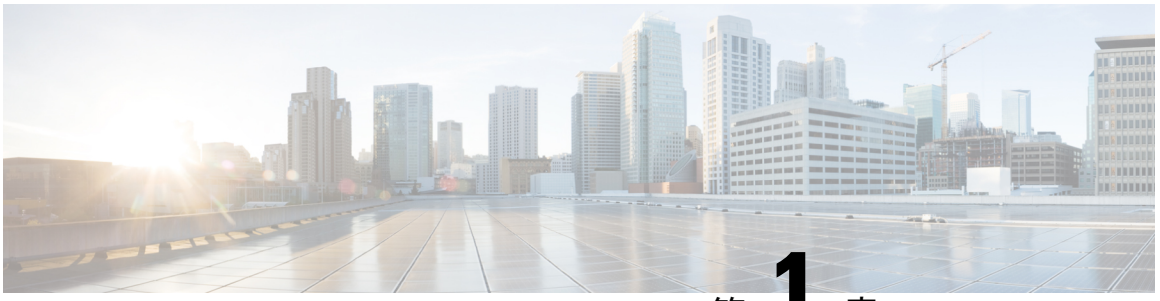
Cisco ASA with FirePOWER Services バージョン 7.0 ローカル管理設定 ガイド

初版：2021 年 4 月 12 日

最終更新：2021 年 5 月 24 日

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

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



第 1 章

ASA with FirePOWER Services の使用開始

Cisco ASA FirePOWER モジュールは、一部の Cisco ASA 5500-X シリーズ アプライアンスに展開できます。詳細については、*Cisco FirePOWER* 互換性ガイドを参照してください。モジュールは、ユーザ組織のセキュリティ ポリシーに準拠した方法でネットワーク トラフィックを処理するように設計されています。

このガイドでは、Adaptive Security Device Manager（ASDM）を使用してアクセス可能な ASA FirePOWER モジュールの機能の設定方法について説明します。

また、Firepower Management Center を使用した ASA with FirePOWER Services デバイスの管理方法については、*Cisco Firepower Management Center* コンフィギュレーション ガイドを参照してください。

クイック スタート：基本設定

ASA with FirePOWER Services デバイスの設定を開始する場合は、Cisco ASA FirePOWER モジュール クイック スタート ガイドを参照してください。クイック スタート ガイドには、以下を含む、セットアップ プロセス全体の説明が含まれています。

1. ASA with FirePOWER Services の導入。

（注） ASDM を使用して ASA with FirePOWER Services を管理するための Firepower Management Center への ASA with FirePOWER Services の登録セクションはスキップします。

注意 Firepower Management Center または ADSM を使用して、特定のアプライアンスを管理できますが、両方を使用することはできません。管理方式を切り替えると、既存のアプライアンスの設定が削除されます。

2. ASDM の開始。
3. ASA with FirePOWER Services の設定。

ポリシーと基本設定の設定

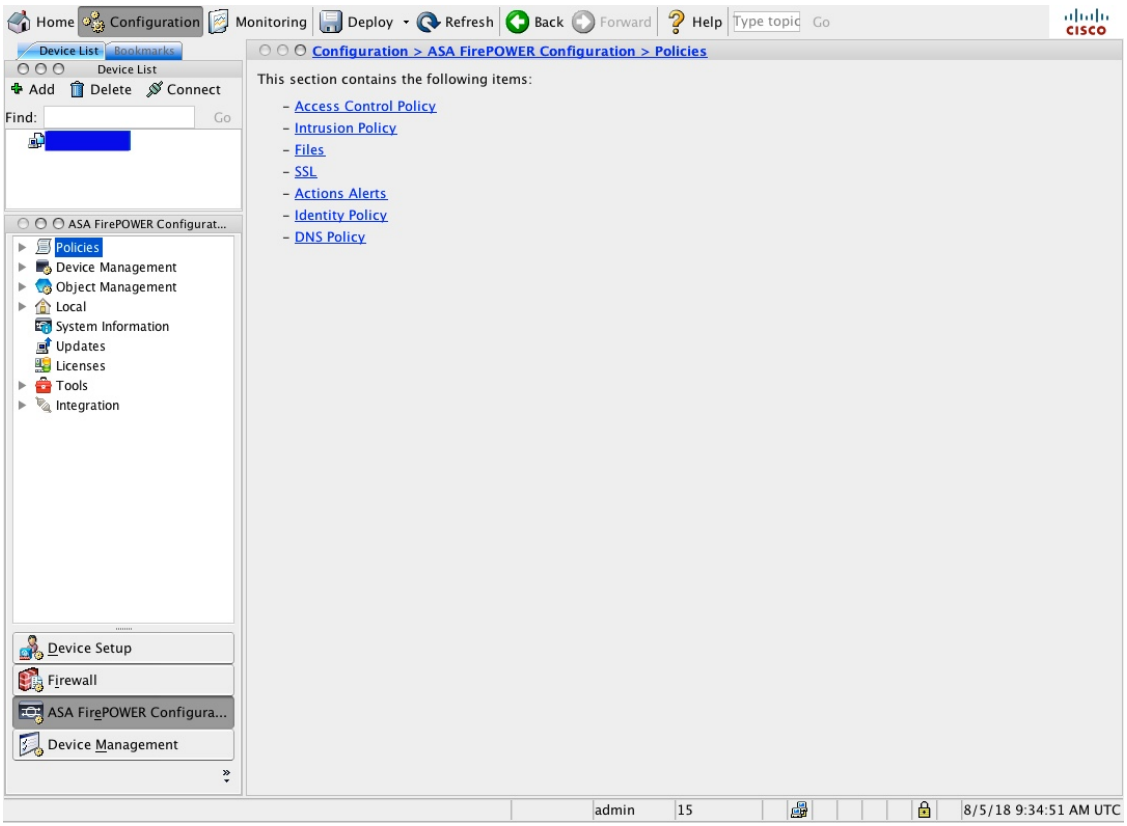
始める前に

クイック スタート：基本設定 （1 ページ）の説明に従い、最初に ASA with FirePOWER Services モジュールを設定します。

ステップ 1 クイック スタート ガイドの説明に従い、ASDM を起動して、ASA with FirePOWER Services モジュールにログインします。

ステップ 2 上部のナビゲーション バーで、[Configuration] をクリックします。

ステップ 3 サイドのナビゲーション バーで、[ASA FirePOWER Configuration] をクリックします。
次のような [Configuration] ページが表示されます。

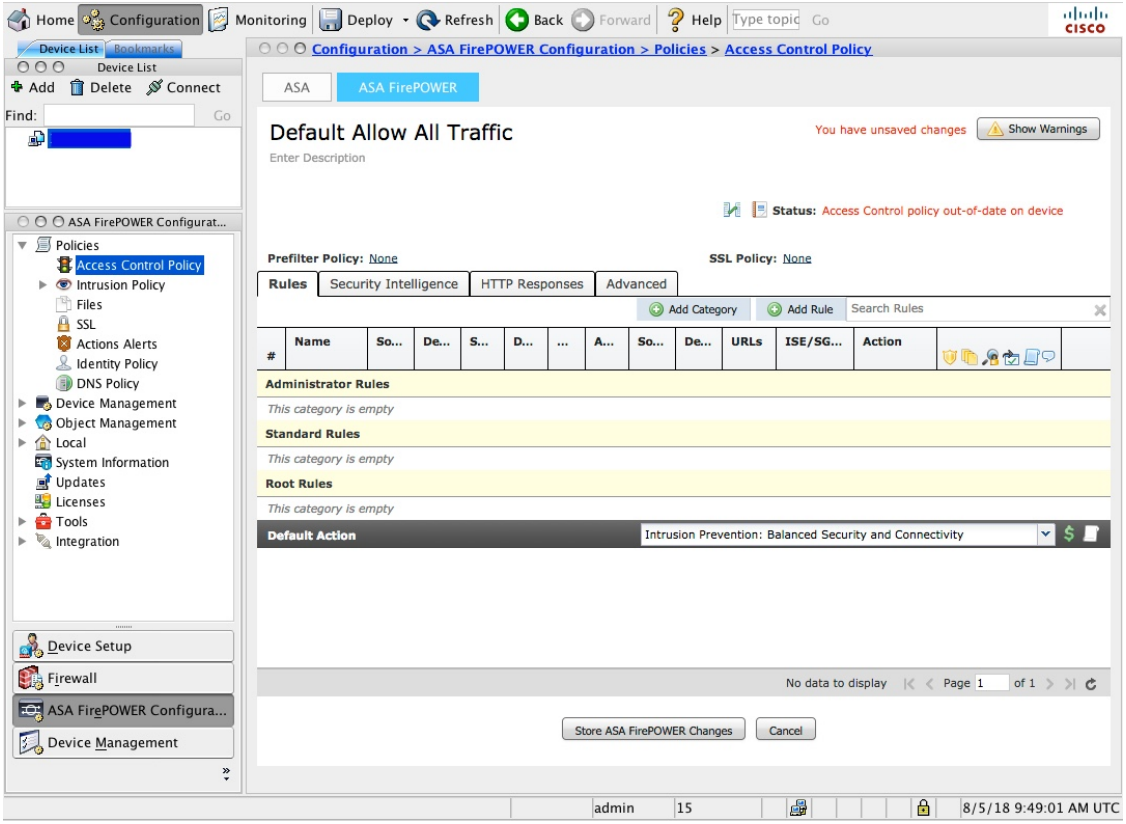


ステップ 4 基本的なアクセス コントロール ポリシーの作成 （81 ページ）の説明に従い、アクセス コントロール ポリシーを作成します。

a) [Policies] を展開します。

b) [Access Control Policy] をクリックします。

c) [ASA with FirePOWER] をクリックします。
次のような [Policy] ページが表示されます。



d) ほとんどの場合、[Default Action] では、[Intrusion Prevention: Balanced Security and Connectivity] を選択することをお勧めします。

ステップ 5 その他の共通の設定をカスタマイズします。

a) ASA FirePOWER モジュール インターフェイスの管理
b) アプライアンスのアクセス リストの設定
c) アプライアンス情報の表示と変更
d) Advanced Malware Protection を使用する場合、クラウド通信の有効化
e) 外部のアラートを使用した Syslog アラート応答の作成または SNMP アラート応答の作成へのログのストリーミング
f) バックアップ ジョブの自動化
g) ソフトウェア ダウンロードの自動化
h) ソフトウェア インストールの自動化
i) 再帰的なルール更新の使用
j) URL フィルタリング更新の自動化
k) 位置情報データベースの更新の自動化

次のタスク

Cisco Adaptive Security Device Manager コンフィギュレーション ガイドの説明に従い、ASA オプションを設定します。

ASA With FirePOWER Services デバイス

ASA with FirePOWER Services デバイスは、次世代侵入防御システム（NGIPS）デバイスと呼ばれることもあります。これらのデバイスは、ASA デバイス上で NGIPS ソフトウェアを実行します。

ASA デバイスは最も重要なシステム ポリシーを提供し、検出およびアクセス コントロールのためにトラフィックを ASA FirePOWER モジュールに渡します。

ASA FirePOWER には ASA プラットフォームに固有のユーザ インターフェイスとコマンド ライン インターフェイス（CLI）があります。これらの ASA 固有のツールを使用して、システムをインストールしたり、プラットフォーム固有の他の管理タスクを実行したりすることができます。

ASA FirePOWER は次の Firepower 機能をサポートしていません。

- Firepower ハードウェアの機能：ASA CLI および ASDM を使用して、デバイスのハイ アベイラビリティ、スタッキング、スイッチング、ルーティング、VPN、NAT などを設定します。詳細については、ASA のマニュアルを参照してください。
- インターフェイスの設定：Firepower Management Center の Web インターフェイスを使用して ASA FirePOWER インターフェイスを設定することはできません。ASA FirePOWER が SPAN ポート モードで展開されている場合、Firepower Management Center には ASA インターフェイスは表示されません。
- プロセス管理：Firepower Management Center を使用して、ASA FirePOWER プロセスのシャットダウン、再起動、その他の管理を行うことはできません。

ASA With FirePOWER Services の機能

このセクションでは、一般的に使用される ASA With FirePOWER Services の機能をいくつか示します。

アプライアンスおよびシステム管理の機能

不明なドキュメントを探す場合は、ドキュメント ロードマップを参照してください。

目的	設定	参照場所
アプライアンスのデータをバックアップする	バックアップと復元	バックアップと復元の使用（605 ページ）

目的	設定	参照場所
新しいソフトウェア バージョンへのアップグレード	ソフトウェア アップデート	ASA FirePOWER モジュール ソフトウェアの更新（573ページ）
アプライアンスを基準に合わせる	工場出荷時の初期状態に復元（再イメージ化）する	• Cisco ASA および Firepower Threat Defense 再イメージ化ガイド • Cisco Adaptive Security Device Manager コンフィギュレーション ガイドの FirePOWER モジュールの再イメージ化に関するセクション
アプライアンスの動作の継続性を確保する	ハイ アベイラビリティ	Cisco Adaptive Security Device Manager Configuration Guides
VDB を更新する、侵入ルールを更新する、またはアプライアンスの GeoDB を更新する	脆弱性データベース（VDB）の更新、侵入ルールの更新、地理位置情報データベース（GeoDB）の更新	更新のタイプについて （573ページ）
ライセンス制御機能を利用するためにライセンスを適用する	移行が可能	ライセンスについて （567ページ）
複数のインターフェイス間のトラフィックをルーティングするようにデバイスを設定する	ルーティング	ASDM コンフィギュレーション ガイド
インターネット接続のプライベート アドレスをパブリック アドレスに変換する	ネットワーク アドレス変換（NAT）	Cisco Adaptive Security Device Manager Configuration Guides

潜在的な脅威を検出、防御、および処理するための機能

不明なドキュメントを探す場合は、ドキュメント ロードマップを参照してください。

目的	設定	参照場所
ネットワーク トラフィックのインスペクション、記録、およびアクションを実行する	アクセス コントロール ポリシー、他のいくつかのポリシーの親	アクセス コントロール ポリシーの開始 （79 ページ）

目的	設定	参照場所
IP アドレス、URL、またはドメイン名との間の接続をブロックする	アクセス コントロール ポリシー内のセキュリティ インテリジェンス	セキュリティ インテリジェンス戦略の選択 （104 ページ）
ネットワーク上の悪意のあるトラフィックと侵入をモニタする	侵入ポリシー	侵入ポリシーについて （341 ページ）
インスペクションを実行せずに、暗号化されたトラフィックをブロックする 暗号化または複合されたトラフィックのインスペクション	SSL ポリシー	トラフィック復号の概要 （205 ページ）
ネットワーク上のファイルを許可またはブロックする	ファイル ポリシー	侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御 （171 ページ）
ユーザの認知およびユーザ制御を実行するためにパッシブまたはアクティブなユーザ認証を設定する	ユーザ認識、ユーザ アイデンティティ、アイデンティティ ポリシー	アイデンティティ データの概要 （401 ページ）

外部ツールとの統合

不明なドキュメントを探す場合は、ドキュメント ロードマップを参照してください。

目的	設定	参照場所
カスタム開発されたクライアント アプリケーションにイベント データをストリーミングする	eStreamer 統合	高度なデバイス設定について （14 ページ）

Firepowerのオンラインヘルプ、ハウツー、およびドキュメント

オンライン ヘルプには、Web インターフェイスからアクセスできます。

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

ハウツーは、Firepower Management Center 上でタスク間を移動するためのウォークスルーを提供するウィジェットです。ウォークスルーでは、タスクを実行するために移動する必要があるかもしれない各種 UI 画面かどうかを問わず、各ステップを順次体験することでタスクを完遂するために必要なステップを実行します。デフォルトで [How To] ウィジェットは有効になっています。ウィジェットを無効にするには、ユーザ名の下にあるドロップダウンリストから [User Preferences] を選択し、[How-To Settings] にある [Enable How-Tos] チェックボックスをオフにします。

（注） 通常、ウォークスルーはすべての UI ページで利用でき、ユーザ ロールは区別されていません。ただし、ユーザの権限によっては Firepower Management Center のインターフェイスに表示されないメニュー項目もあります。そのため、そのようなページではウォークスルーは実行されません。

Firepower Management Center では次のウォークスルーを使用できます。

- [Cisco スマート アカウントへの FMC の登録（Register FMC with Cisco Smart Account）]：このウォークスルーでは、Cisco スマート アカウントに Firepower Management Center を登録する手順について説明します。
- [デバイスのセットアップと FMC への追加（Set up a Device and add it to FMC）]：このウォークスルーでは、デバイスをセットアップし、そのデバイスを Firepower Management Center に追加する手順について説明します。
- [日付と時刻の設定（Configure Date and Time）]：このウォークスルーでは、プラットフォーム設定ポリシーを使用して Firepower Threat Defense デバイスの日付と時刻を設定する手順について説明します。
- [インターフェイスの設定（Configure Interface Settings）]：このウォークスルーでは、Firepower Threat Defense デバイス上のインターフェイスを設定する手順について説明します。
- [アクセス コントロール ポリシーの作成（Create an Access Control Policy）]：アクセス コントロール ポリシーは上から下へと評価される、順序付けられた一連のルールから構成されています。このウォークスルーでは、アクセス コントロール ポリシーを作成する手順について説明します。
- [アクセス コントロール ルールの追加（Add an Access Control Rule）] - 機能のウォークスルー：このウォークスルーでは、アクセス コントロール ルールのコンポーネントと、Firepower Management Center でのそれらの使用方法について説明します。
- [ルーティングの設定（Configure Routing Settings）]：Firepower Threat Defense ではさまざまなルーティング プロトコルがサポートされています。スタティック ルートは、特定の宛先ネットワークのトラフィックの送信先を定義します。このウォークスルーでは、デバイスのスタティック ルーティングを設定する手順について説明します。

- [NAT ポリシーの作成（Create a NAT Policy）] - 機能のウォークスルー：このウォークスルーでは、NAT ポリシーを作成する手順とともに、NAT ルールのさまざまな機能について説明します。

ドキュメントのロードマップを使用して Firepower システムに関連する他のドキュメントについてはhttp://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html を参照してください。

関連資料

このセクションに記載されているドキュメントは、ASA with FirePOWER Services アプライアンスを設定する際に役立つことがあります。

ハードウェア ガイドとデータシート

次のガイドには、ASA with FirePOWER Services ハードウェアに関する詳細な情報が記載されています。

- https://www.cisco.com/c/en/us/support/security/asa-firepower-services/tsd-products-support-series-home.html
- https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html
- https://www.cisco.com/c/en/us/td/docs/security/asa/quick_start/sfr/firepower-qsg.html

詳細情報

一部のトピックは、Firepower Management Center コンフィギュレーション ガイドで詳細に説明されているため、このガイドには含まれていません。次の表に、このガイドで詳細情報が説明されていないトピックを示します。以下も参照してください。 関連資料 （9 ページ）

詳細情報の項目	FMC コンフィギュレーション ガイドのパート > 章を参照
アクセス コントロール ルール	**Access Control** > **Access Control Rules**
侵入ポリシー	**Intrusion Detection and Prevention** > **Getting Started with Intrusion Policies**
トラブルシューティング ツール	**System Monitoring and Troubleshooting** > **Troubleshooting the System**
ユーザ制御用のレルム	**Discovery and Identity** > **Create and Manage Realms**
アイデンティティ ポリシー	**Discovery and Identity** > **Create and Manage Identity Policies**
内部認証局（CA）	**Deployment Management** > **Reusable Objects**

詳細情報の項目	FMC コンフィギュレーション ガイドのパート > 章を参照
信頼できる CA	**Deployment Management** > **Reusable Objects**
地理位置情報データベースの更新	**Deployment Management** > **Reusable Objects**

ドキュメント内のサポート対象デバイスに関する記述

章または項目の先頭に記載されているサポート対象デバイスに関する記述は、ある機能が特定のデバイス シリーズ、ファミリ、またはモデルでのみサポートされていることを示しています。たとえば、多くの機能は Firepower Threat Defense デバイスのみでサポートされています。

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

ドキュメント内のアクセス ステートメント

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

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

Firepower システムの IP アドレス表記法

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

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

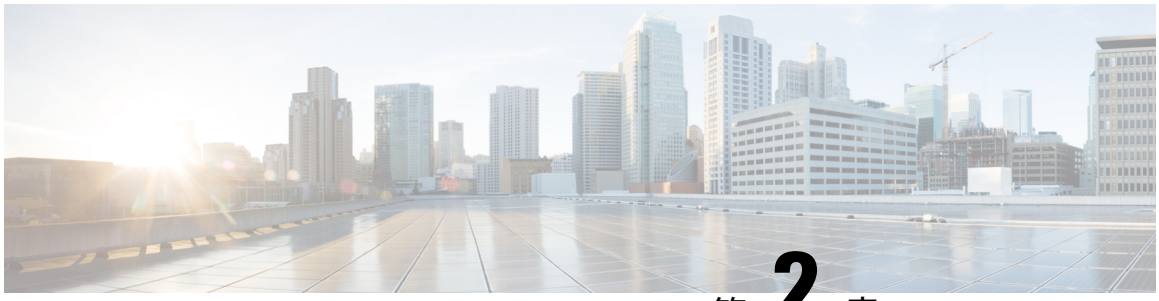
つまり、Cisco では CIDR またはプレフィックス長の表記を使用する場合に、ビット境界上でネットワーク IP アドレスを使用する標準の方法を推奨していますが、Firepower システムではこれは必要ありません。

関連リソース

ファイアウォール コミュニティは、参考資料の包括的リポジトリで、シスコの広範にわたるドキュメンテーションを補完します。これには、シスコのハードウェアの3Dモデル、ハードウェア構成セレクタ、製品販促アイテム、設定例、トラブルシューティングに関するテクニカル ノート、トレーニング ビデオ、ラボおよび Cisco Live セッション、ソーシャル メディア チャネル、Cisco ブログおよび技術文書チームによって公開されたすべてのドキュメンテーションへのリンクが含まれます。

管理人等、コミュニティ サイトや動画共有サイトに情報を掲載する個人が、シスコの社員であることがあります。それらのサイトおよび対応するコメントで表明される意見は、投稿者本人の個人的意見であり、シスコの意見ではありません。掲載内容は、情報の提供のみを目的としており、シスコや他の関係者による推奨または異議を目的としたものではありません。

（注） ファイアウォール コミュニティ の動画、テクニカル ノート、および参考資料の中には、古いバージョンの Firepower Management Center に言及しているものがあります。ご使用のバージョンの Firepower Management Center と動画やテクニカル ノートで参照されているバージョンとではユーザ インターフェイスに違いがあるために、手順も異なる場合があります。



第 2 章

デバイス設定の管理

[Device Management] ページでは、ASA FirePOWER モジュールのデバイスおよびインターフェイスの設定を管理できます。

注意 フェールオーバー ペアで ASA を設定した場合、ASA FirePOWER の設定は、セカンダリ デバイス上の ASA FirePOWER モジュールとは自動的に同期されません。変更を加えるたびに、プライマリから ASA FirePOWER の設定を手動でエクスポートしてセカンダリにインポートする必要があります。

デバイス設定の編集

[Device Management] ページの [Device] タブには、ASA FirePOWER モジュールに適用されたときの詳細なデバイス設定と情報が表示されます。さらにこれにより、表示されるモジュール名や管理設定の変更など、デバイス設定のいくつかの部分に変更を加えることができます。

一般的なデバイス設定の編集

ライセンス：任意

[Device] タブの [General] セクションにはモジュール名が表示されます。モジュール名は変更できます。

一般的なデバイス設定を編集するには、次の手順を実行します。

ステップ 1 **[Configuration]** > **[ASA FirePOWER Configuration]** > **[Device Management]** > **[Device]** をクリックします。

[Device] ページが表示されます。

ステップ 2 [General] セクションで（編集）をクリックします。

ステップ 3 [Name]フィールドに、モジュールに割り当てる新しい名前を入力します。英数字と特殊文字を入力できます。ただし、+、(、)、{、}、#、&、\、<、>、?、‘、および“ の文字は無効です。

ステップ 4 [**Save**] をクリックします。

これにより、変更内容が保存されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイス設定への変更の適用 （16 ページ）を参照してください）。

デバイス システム設定の表示

ライセンス：任意

[Device] タブの [System] セクションには、システム情報の読み取り専用テーブルが表示されます。以下の表に、表示される情報をリストします。

表 *1 : [*システム（*System***）*]* セクション テーブルのフィールド**

フィールド	説明
Model	デバイスのモデル名と番号。
Serial	デバイスのシャーシのシリアル番号。
Time	デバイスの現在のシステム時刻。
Version	ASA FirePOWER モジュールに現在インストールされているソフトウェアのバージョン。
Policy	ASA FirePOWER モジュールに現在適用されているシステム ポリシーへのリンク。

高度なデバイス設定について

[Device] タブの [Advanced] セクションには、次の表に示すように、構成時の詳細設定が表示されます。

表 *2 : [*詳細設定（*Advanced***）*]* セクションのテーブルのフィールド**

フィールド	説明
Application Bypass	モジュールでの Automatic Application Bypass の状態。
Bypass Threshold	自動アプリケーションバイパスのしきい値（ミリ秒）。

上記の設定は、いずれも [詳細設定（Advanced）] セクションを使用して編集できます。詳細については、次の項を参照してください。

自動アプリケーション バイパス

ライセンス：任意

Automatic Application Bypass（AAB）機能は、インターフェイスでのパケット処理時間に制限を設け、この時間を超過した場合、パケットに検出のバイパスを許可します。この機能は任意の展開で使用できますが、インライン展開ではとりわけ価値があります。

パケット処理の遅延は、ネットワークで許容できるパケット レイテンシとバランスを取って調整します。Snort 内での不具合やデバイスの誤った設定が原因で、トラフィックの処理時間が指定のしきい値を超えると、AAB により、その障害発生から 10 分以内に Snort が再起動され、トラブルシューティング データが生成されます。このデータを分析することで、過剰な処理時間の原因を調査できます。

このオプションが選択されている場合は、バイパスしきい値を変更できます。デフォルト設定は 3000 ミリ秒（ms）です。有効な範囲は 250 ms ～ 60,000 ms です。

（注） AAB がアクティブ化されるのは、単一パケットに過剰な処理時間がかかっている場合のみです。AAB がアクティブになると、システムはすべての Snort プロセスをキルします。

自動アプリケーションバイパスを有効にしてバイパスしきい値を設定する方法の詳細については、詳細なデバイス設定の編集 （15 ページ）を参照してください。

詳細なデバイス設定の編集

[Devices] タブの [Advanced] セクションを使用して、Automatic Application Bypass を変更できます。

高度なデバイス設定を変更するには、以下を行います。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration]> [Device Management] > [Device] の順に選択します。

[Device] ページが表示されます。

ステップ 2 [Advanced] セクションの横にある編集アイコン（）をクリックします。

[Advanced] ポップアップ ウィンドウが表示されます。

ステップ 3 ネットワークがレイテンシの影響を受けやすい場合は、必要に応じて、[Automatic Application Bypass] を選択します。Automatic Application Bypass は、インライン展開でとりわけ役立ちます。詳細については、自動アプリケーション バイパス （15 ページ）を参照してください。

ステップ 4 [Automatic Application Bypass] オプションを選択すると、[Bypass Threshold] にバイパスしきい値（ミリ秒）を入力できます。デフォルト設定は 3000 ms です。有効な範囲は 250 ms ～ 60,000 ms です。

ステップ 5 [**Save**] をクリックします。

変更が保存されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイス設定への変更の適用 （16 ページ）を参照してください）。

ASA FirePOWER モジュール インターフェイスの管理

ライセンス：Control、Protection

ASA FirePOWER インターフェイスを編集する際には、ASA FirePOWER モジュールからインターフェイスのセキュリティ ゾーンのみ設定できます。詳細については、「セキュリティ ゾーンの操作 （64 ページ）」を参照してください。

ASDM および CLI を使用してインターフェイスを設定します。

ASA FirePOWER インターフェイスを編集するには、次の手順を実行します。

ステップ 1 **[Configuration]** > **[ASA FirePOWER Configuration]** > **[Device Management]** > **[Interfaces]** の順に選択します。

[Interfaces] ページが表示されます。

ステップ 2 編集するインターフェイスの横にある編集アイコン（  ）をクリックします。

[Edit Interface] ポップアップ ウィンドウが表示されます。

ステップ 3 [Security Zone] ドロップダウン リストから既存のセキュリティ ゾーンを選択するか、または [New] を選択して、新しいセキュリティ ゾーンを追加します。

ステップ 4 [Store ASA FirePOWER Changes] をクリックします。

セキュリティ ゾーンが設定されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください（詳しくはデバイス設定への変更の適用 （16 ページ）を参照してください）。

デバイス設定への変更の適用

ライセンス：任意

デバイスの ASA FirePOWER 設定に変更を加えたら、それらの変更を適用してモジュール全体に変更を反映する必要があります。デバイスが変更適用前の状態でなければ、このオプションは無効になります。

インターフェイスを編集してデバイス ポリシーを再適用すると、編集したインターフェイス インスタンスだけでなく、デバイス上のすべてのインターフェイス インスタンスで Snort が再起動することに注意してください。

変更をデバイスに適用するには、以下を行います。

ステップ 1 **[Configuration]** > **[ASA FirePOWER Configuration]** > **[Device Management]** > **[Device]** または **[Configuration]** > **[ASA FirePOWER Configuration]** > **[Device Management]** > **[Interfaces]** の順に選択します。

[Device Management] ページが表示されます。

ステップ 2 [Apply ASA FirePOWER Changes] をクリックします。

ステップ 3 プロンプトが出されたら、[適用（Apply）] をクリックします。

デバイスの変更が適用されます。

ヒント 必要に応じて、[Apply Device Changes] ダイアログボックスで [View Changes] をクリックします。新しいウィンドウに [Device Management Revision Comparison Report] ページが表示されます。詳細については、デバイス管理のリビジョン比較レポートの使用 （17ページ）を参照してください。

ステップ 4 [OK] をクリックします。

[Device Management] ページに戻ります。

デバイス管理のリビジョン比較レポートの使用

ライセンス：任意

デバイス管理の比較レポートを使用して、変更を確認してから、アプライアンスに適用できます。このレポートには、現在のアプライアンスの設定と、変更適用後のアプライアンスの設定との間の差異がすべて表示されます。これにより、設定の潜在的なエラーを検出することができます。

変更適用前と適用後のアプライアンスを比較するには、以下を行います。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Device Management] > [Device] または [Configuration] > [ASA FirePOWER Configuration] > [Device Management] > [Interfaces] の順に選択します。

[Device Management] ページが表示されます。

ステップ 2 [Apply Changes] をクリックします。

[Apply Device Changes] ポップアップ ウィンドウが表示されます。アプライアンスが変更適用前の状態でなければ、[Apply Changes] ボタンは無効のままになります。

ステップ 3 [変更の表示（View Changes）] をクリックします。

新しいウィンドウに [Device Management Revision Comparison Report] ページが表示されます。

ステップ 4 [Previous] と [Next] をクリックして、現在のアプライアンスの設定と変更適用後のアプライアンスの設定との間のすべての差異を確認します。

ステップ 5 必要に応じて、レポートの PDF バージョンを生成するには、[Comparison Report] をクリックします。

リモート管理の設定

ライセンス：任意

ある Firepower システム アプライアンスで別のアプライアンスを管理できるようにするには、2 つのアプライアンスの間に双方向の SSL 暗号化通信チャネルをセットアップする必要があります。このチャネルを使用して、両方のアプライアンスが設定とイベント情報を共有します。ハイ アベイラビリティ ピアも、このチャネルを使用します。このチャネルは、デフォルトではポート 8305/tcp に位置します。

管理対象のアプライアンス、つまり Firepower Management Center で管理するデバイス上にはリモート管理を設定する必要があります。リモート管理を設定した後、管理側アプライアンスの Web インターフェイスを使用して、管理対象アプライアンスを展開環境に追加できます。

（注） リモート管理を設定し、Cisco ASA with FirePOWER Services を Firepower Management Center に登録したら、ASDM の代わりに Firepower Management Center から ASA FirePOWER モジュールを管理する必要があります。アプライアンスを Firepower Management Center に登録すると、ASDM コンソールを使用して Cisco ASA with FirePOWER Services をリモート管理することはできません。

2 つのアプライアンス間の通信を可能にするためには、アプライアンスが互いを認識する手段を提供しなければなりません。Firepower システムでは 3 つの基準を使用して通信を許可します。

- 通信を確立する対象のアプライアンスのホスト名または IP アドレス

NAT 環境では、ルーティング可能なアドレスがもう一方のアプライアンスにないとしても、リモート管理を設定する際、または管理対象アプライアンスを追加する際には、ホスト名または IP アドレスのいずれかを指定する必要があります。

- 接続を識別するために自己生成される、最大 37 文字の英数字による登録キー
- Firepower システムが NAT 環境で通信を確立するために利用できるオプションの一意の英数字による NAT ID。

NAT ID は、管理対象アプライアンスを登録するために使用されているすべての NAT ID の間で一意でなければなりません。

管理対象デバイスを Firepower Management Center に登録すると、選択したアクセス コントロール ポリシーがデバイスに適用されます。ただし、選択したアクセス コントロール ポリシーで使用される機能に必要なライセンスがデバイスで有効になっていなければ、アクセス コントロール ポリシーの適用は失敗します。

ローカル アプライアンスのリモート管理を設定するには、以下を行います。

アクセス：管理者

ステップ 1 **[Configuration]** > **[ASA FirePOWER Configuration]** > **[Integration]** > **[Remote Management]** の順に選択します。

[Remote Management] ページが表示されます。

ステップ 2 [マネージャの追加（Add Manager）] をクリックします。

[Add Remote Management] ページが表示されます。

ステップ 3 [Management Host] に、このアプライアンスを管理するために使用するアプライアンスの IP アドレスまたはホスト名を入力します。

ホスト名は、完全修飾ドメイン名またはローカル DNS で有効な IP アドレスに解決される名前です。

NAT 環境では、管理対象アプライアンスを追加する際に IP アドレスまたはホスト名を指定する予定の場合、ここで IP アドレスまたはホスト名を指定する必要はありません。その場合、Firepower システムは後で指定される NAT ID を使用して、管理対象 ASA FirePOWER モジュール インターフェイス上のリモートマネージャを識別します。

注意 ネットワークで IP アドレスの割り当てに DHCP を使用している場合は、IP アドレスではなく、ホスト名を使用します。

ステップ 4 [Registration Key] フィールドに、アプライアンス間の通信をセットアップするために使用する登録キーを入力します。

ステップ 5 NAT 環境の場合は、[Unique NAT ID] フィールドに、アプライアンス間の通信をセットアップするために使用する、英数字による**一意**の NAT ID を入力します。

ステップ 6 [**Save**] をクリックします。

アプライアンスが相互に通信できることを確認すると、ステータスとして [登録保留（Pending Registration）] が表示されます。

ステップ 7 管理側アプライアンスの Web ユーザインターフェイスを使用して、このアプライアンスを展開環境に追加します。

（注） デバイスのリモート管理を有効にする場合、NAT を使用する一部のハイアベイラビリティ展開では、セカンダリ Firepower Management Center をマネージャとして追加する必要がある場合があります。詳細については、サポートにお問い合わせください。

リモート管理の編集

ライセンス：任意

管理側アプライアンスのホスト名または IP アドレスを編集するには、以下の手順を使用します。また、管理側アプライアンスの表示名を変更することもできます。表示名は、Firepower システムのコンテキスト内でのみ使用されます。ホスト名をアプライアンスの表示名として使用することもできますが、別の表示名を入力してもホスト名は変更されません。

リモート管理を編集するには、以下を行います。

アクセス：管理者

ステップ 1 **[Configuration]** > **[ASA FirePOWER Configuration]** > **[Integration]** > **[Remote Management]** の順に選択します。

[Remote Management] ページが表示されます。

ステップ 2 リモート管理設定を編集するマネージャの横にある編集アイコン（  ）をクリックします。

[Edit Remote Management] ページが表示されます。

ステップ 3 [Name] フィールドで、管理側アプライアンスの表示名を変更します。

ステップ 4 [Host] フィールドで、管理側アプライアンスの IP アドレスまたはホスト名を変更します。

ホスト名は、完全修飾ドメイン名またはローカル DNS で有効な IP アドレスに解決される名前です。

ステップ 5 [**Save**] をクリックします。

変更が保存されます。

eStreamer サーバでの eStreamer の設定

ライセンス：FireSIGHT + Protection

eStreamer サーバとして使用するアプライアンスで eStreamer イベントの外部クライアントへのストリームを開始するには、その前に、イベントをクライアントに送信するように eStreamer サーバを設定し、クライアントに関する情報を指定して、通信を確立するときに使用する認証クレデンシャルを生成する必要があります。

eStreamer イベント タイプの設定

要求したクライアントに eStreamer サーバが送信できるイベント タイプを制御できます。

管理対象デバイスまたは Firepower Management Center のいずれかで使用可能なイベント タイプは以下のとおりです。

- 侵入イベント
- 侵入イベント パケット データ
- 侵入イベント追加データ

eStreamer によって送信されるイベントのタイプを設定するには、次の手順を実行します。

ステップ 1 **[Configuration]** > **[ASA FirePOWER Configuration]** > **[Integration]** > **[eStreamer]** の順に選択します。

[eStreamer Event Configuration] ページが表示されます。

ステップ 2 [eStreamer Event Configuration] の下で、eStreamer から要求元のクライアントに転送するイベントのタイプの横にあるチェックボックスをオンにします。

管理対象デバイスまたは Firepower Management Center で次の一部またはすべてを選択することができます。

- [Intrusion Events]：侵入イベントを送信します。
- [侵入イベント パケット データ（Intrusion Event Packet Data）]：侵入イベントに関連付けられたパケットを送信します。
- [Intrusion Event Extra Data]：HTTP プロキシまたはロード バランサ経由で Web サーバに接続しているクライアントの発信元 IP アドレスのような侵入イベントに関連付けられた追加データを送信します。

（注） これは、eStreamer サーバが送信できるイベントを制御することに注意してください。クライアントは、eStreamer サーバに送信する要求メッセージで受信するイベント タイプを具体的に要求する必要があります。詳細については、*Firepower* システム *eStreamer* 統合ガイドを参照してください。

ステップ 3 [**Save**] をクリックします。

eStreamer クライアントの認証の追加

eStreamer がクライアントに eStreamer イベントを送信するには、その前に、eStreamer ページから eStreamer サーバのピア データベースにクライアントを追加しておく必要があります。また、eStreamer サーバによって生成された認証証明書をクライアントにコピーする必要もあります。

eStreamer クライアントを追加するには、次の手順を実行します。

ステップ 1 **[Configuration]** > **[ASA FirePOWER Configuration]** > **[Integration]** > **[Remote Management]** の順に選択します。

[Registration] ページが表示されます。

ステップ 2 [eStreamer] タブを選択します。

[eStreamer] ページが表示されます。

ステップ 3 [Create Client] をクリックします。

[Create Client] ページが表示されます。

ステップ 4 [ホスト名（Hostname）] フィールドに、eStreamer クライアントを実行しているホストのホスト名または IP アドレスを入力します。

（注） ホスト名を使用する場合、eStreamer サーバはホストを IP アドレスに解決できる必要があります。DNS 解決を設定していない場合、最初に設定するか、IP アドレスを使用する必要があります。

ステップ 5 証明書ファイルを暗号化するには、[Password] フィールドにパスワードを入力します。

ステップ 6 [**Save**] をクリックします。

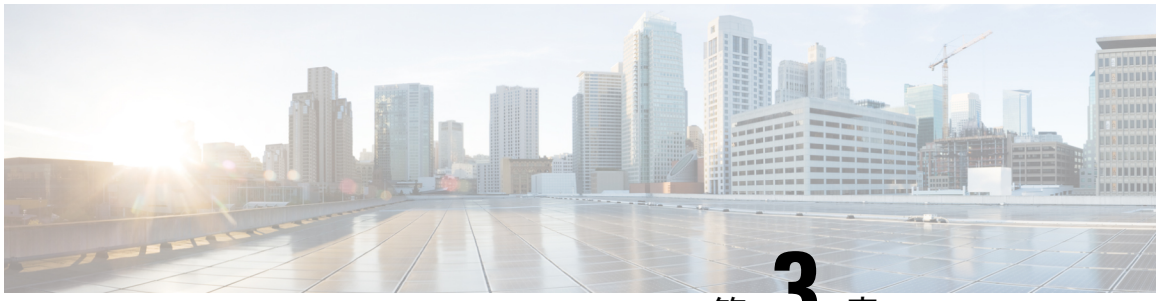
これで、eStreamer サーバは、ホストが eStreamer サーバ上のポート 8302 にアクセスすることを許可し、クライアント/サーバ認証時に使用する認証証明書を作成します。新しいクライアントが [Hostname] の下に表示された状態で、[eStreamer] ページが再表示されます。

ステップ 7 クライアントのホスト名の横にあるダウンロードアイコン（）をクリックして、証明書ファイルをダウンロードします。

ステップ 8 SSL 認証のためにクライアントが使用する適切なディレクトリに証明書ファイルを保存します。

これで、クライアントは eStreamer サーバに接続できます。eStreamer サービスを再起動する必要はありません。

ヒント クライアントのアクセスを取り消すには、削除するホストの横にある削除アイコン（）をクリックします。eStreamerサービスを再起動する必要はありません。アクセスはただちに取り消されます。



第 3 章

再使用可能オブジェクトの管理

柔軟性を高めて使用しやすくするために、ASA FirePOWER モジュールでは名前付きオブジェクトを作成できます。これは、名前を値と関連付ける再使用可能な設定であり、値を使用する必要がある場合、代わりに名前付きオブジェクトを使用できます。

次のタイプのオブジェクトを作成できます。

- IP アドレスとネットワーク、ポートとプロトコルのペア、セキュリティ ゾーン、および送信側と宛先の国（地理位置情報）を表すネットワークベースのオブジェクト
- セキュリティ インテリジェンス フィードとリスト、アプリケーション フィルタ、URL、ファイル リスト、および侵入ポリシーの変数セットを含む、非暗号化および復号化されたトラフィックを処理するためのオブジェクト

これらのオブジェクトは、アクセス コントロール ポリシー、ネットワーク分析ポリシー、侵入ポリシー、レポート、ダッシュボードなど、ASA FirePOWER モジュールのさまざまな場所で使用できます。

オブジェクトをグループ化すると、複数のオブジェクトを 1 つの設定で参照できます。ネットワーク、ポート、URL、および公開キー インフラストラクチャ（PKI）オブジェクトをグループ化できます。

（注） ほとんどの場合、ポリシーで使用されるオブジェクトを編集するには、変更を有効にするために設定の再展開が必要になります。

オブジェクト マネージャの使用

ライセンス：任意

オブジェクト マネージャ（**[Configuration] > [ASA FirePOWER Configuration] > [Object Management]**）を使用して、アプリケーション フィルタ、変数セット、およびセキュリティ ゾーンなどのオブジェクトを作成および管理します。ネットワーク、ポート、URL、および PKI オブジェクトをグループ化できます。さらに、オブジェクトおよびオブジェクト グループのリストをソート、フィルタ、参照することもできます。

オブジェクトのグループ化

ライセンス：任意

ネットワーク、ポート、PKI、およびURLのオブジェクトをグループ化できます。システムでは、オブジェクトおよびオブジェクト グループを交互に使用することができます。たとえば、ポート オブジェクトを使用する場合はいつでも、ポート オブジェクト グループも使用できます。同じタイプのオブジェクトおよびオブジェクト グループには、同じ名前を付けることはできません。

ポリシーで使用されるオブジェクト グループ（たとえば、アクセス コントロール ポリシーで使用されるネットワーク オブジェクト グループ）を編集する場合、変更を有効にするために設定を再展開する必要があります。設定変更の導入 （92 ページ）を参照してください。

グループを削除しても、グループ内のオブジェクトは削除されず、相互の関連性だけが削除されます。さらに、使用中のグループは削除できません。たとえば、保存されたアクセス コントロール ポリシーの URL 条件で使用している URL グループは削除できません。

再利用可能なオブジェクトをグループ化するには、次の手順を実行します。

ステップ 1 **[Configuration] > [ASA FirePOWER Configuration] > [Object Management]** の順に選択します。

ステップ 2 グループ化するオブジェクト タイプ [Network]、[Port]、[URL]、[PKI]、または [Distinguished Name] で、[Object Groups] を選択します。

ステップ 3 グループ化するオブジェクトに対応する [Add] ボタンをクリックします。

ステップ 4 [Name] にグループの名前を入力します。中カッコ（{}）を除く、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5 1 つ以上のオブジェクトを選択し、[Add] をクリックします。

- 複数のオブジェクトを選択するには、Shift と Ctrl を使用するか、右クリックして [Select All] を選択します。
- 含める既存のオブジェクトを検索するには、フィルタ フィールド（）を使用します。このフィールドは入力に従って更新され、一致する項目が表示されます。検索文字列をクリアするには、検索フィールドの上にあるリロードアイコン（）をクリックするか、検索フィールド内のクリアアイコン（）をクリックします。
- 既存のオブジェクトがニーズを満たさない場合、すぐにオブジェクトを作成するには、追加アイコン（）をクリックします。

ステップ 6 [Store ASA FirePOWER Changes] をクリックします。

オブジェクトの参照、ソート、およびフィルタ

ライセンス：任意

オブジェクト マネージャには、ページあたり 20 のオブジェクトまたはグループが表示されます。オブジェクトまたはグループのタイプが 20 を超える場合は、ページ下部のナビゲーション リンクを使用して追加ページを表示します。特定のページにアクセスしたり、更新アイコン（）にアクセスしてビューを更新したりすることもできます。

デフォルトでは、オブジェクトとグループはページで、アルファベット順に名前でリストされます。ただし、表示されている任意の列でオブジェクトまたはグループの各タイプをソートできます。列見出しの横にある上または下矢印は、ページがその列でその方向にソートされていることを示します。ページのオブジェクトは、名前または値でフィルタすることもできます。

オブジェクトまたはグループをソートする方法：

1. カラムの見出しをクリックします。反対方向でソートするには、見出しを再度クリックします。

オブジェクトまたはグループをフィルタする方法：

1. [Filter] フィールドのフィルタ条件を入力します。

   ページは入力に従って更新され、一致する項目が表示されます。フィールドには、ワイルドカードとして 1 つ以上のアスタリスク（*）を使用できます。

オブジェクトの参照、ソート、およびフィルタ

デフォルトでは、オブジェクトとグループはページで、アルファベット順に名前でリストされます。ただし、表示されている任意の列でオブジェクトまたはグループの各タイプをソートできます。列見出しの横にある上または下矢印は、ページがその列でその方向にソートされていることを示します。ページのオブジェクトは、名前または値でフィルタすることもできます。

オブジェクトまたはグループをソートする方法：

カラムの見出しをクリックします。反対方向でソートするには、見出しを再度クリックします。

オブジェクトまたはグループをフィルタする方法：

a) [Filter] フィールドのフィルタ条件を入力します。

ページは入力に従って更新され、一致する項目が表示されます。フィールドは、ワイルドカードとして 1 つ以上のアスタリスク（*）を受け入れます。

ネットワーク オブジェクトの操作

ライセンス：任意

ネットワーク オブジェクトは、個別に、またはアドレス ブロックとして指定できる 1 つ以上の IP アドレスを表します。ネットワーク オブジェクトおよびグループ（オブジェクトのグループ化 （24 ページ）を参照）は、アクセス コントロール ポリシー、ネットワークの変数、レポートなど、ASA FirePOWER モジュールのさまざまな場所で使用できます。

また、使用中のネットワーク オブジェクトは削除できません。さらに、アクセス コントロールまたは侵入ポリシーで使用されるネットワーク オブジェクトを編集した場合は、変更を有効にするためにポリシーを再適用する必要があります。

ネットワーク オブジェクトを作成する方法：

ステップ 1 **[Configuration]** > **[ASA FirePOWER Configuration]** > **[Object Management]** の順に選択します。

ステップ 2 [Network] で、[Individual Objects] を選択します。

ステップ 3 [Add Network] をクリックします。

ステップ 4 [Name] にネットワーク オブジェクトの名前を入力します。中カッコ（{}）を除く、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5 ネットワーク オブジェクトに追加する IP アドレスまたはアドレス ブロックごとに、値を入力して [Add] をクリックします。

ステップ 6 [Store ASA FirePOWER Changes] をクリックします。

アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の導入 （92 ページ）を参照してください。

セキュリティ インテリジェンス リストとフィードの操作

ライセンス：Protection

セキュリティ インテリジェンス機能を使用すると、アクセス コントロール ポリシーごとに、送信元または宛先 IP アドレスに基づいてネットワークをトラバースできるトラフィックを指定できます。これは、トラフィックがアクセス制御ルールによって分析される前に、特定の IP アドレスをブロックする（トラフィックの送受信を拒否する）場合に特に役立ちます。同様に、IP アドレスをブロックなしリストに追加し、アクセス制御を使用してシステムに接続を強制的に処理させることができます。

特定の IP アドレスをブロックするかどうか決めていない場合は、「モニタのみ」の設定を使用できます。この設定では、システムがアクセス制御ルールを使用して接続を処理でき、接続の一致がセキュリティ インテリジェンスのブロックリストに記録されます。

グローバルブロックなしリストとグローバルブロックリストは、デフォルトですべてのアクセス コントロール ポリシーに含まれており、すべてのゾーンに適用されます。また、各アクセス コントロール ポリシー内で、ネットワークオブジェクトとグループの組み合わせを使用して個別のブロックなしリストとブロックリストや、セキュリティインテリジェンスのリストとフィードを作成できます。ユーザはこれらすべてをセキュリティゾーン別に制約することができます。

フィードとリストの比較

セキュリティ インテリジェンス フィードは、ユーザが設定した間隔でシステムが HTTP または HTTPS サーバからダウンロードする IP アドレスの動的コレクションです。フィードは定期的に更新されるため、システムは最新の情報を使用してネットワーク トラフィックをフィルタ処理できます。ASA FirePOWER モジュールには、ブロックリストの作成に役立つインテリジェンスフィードがあります。このフィードは、VRT によってレピュテーションが低いと判断された IP アドレスを表します。

フィードの更新が反映されるまで数分かかる場合がありますが、フィードの作成または変更後、またはスケジュールされたフィードの更新後に、ポリシーを展開する必要はありません。

（注） システムがインターネットからフィードをダウンロードするタイミングを厳密に制御する場合は、そのフィードの自動更新を無効にすることができます。ただし、シスコでは自動更新を許可することを推奨しています。オンデマンド更新は手動でも実行できますが、システムが定期的にフィードをダウンロードするようにすれば、最新の関連データを入手できます。

フィードとは対照的に、セキュリティ インテリジェンス リストは、手動でシステムにアップロードする IP アドレスの単純な静的リストです。フィードやグローバルブロックなしリストとブロックリストを増やしたり、微調整したりするには、カスタムリストを使用します。カスタムリストの編集（ネットワークオブジェクトの編集およびグローバルブロックなしリストま

たはブロックリストからの IP アドレスの削除）を行う場合、変更を有効にするために設定を再展開する必要があることに注意してください。

フィード データの書式設定や破損

フィードとリストのソースは、1 行につき 1 つの IP アドレスまたはアドレス ブロックを持つ、最大 500 MB の単純なテキスト ファイルでなければなりません。コメント行は # 文字で始める必要があります。リストのソース ファイルは、.txt 拡張子を使用する必要があります。

システムが破損したフィードまたは認識不能な IP アドレスを持つフィードをダウンロードした場合、システムは古いフィードデータを引き続き使用します（これが初回のダウンロードである場合を除く）。ただし、システムがフィード内の IP アドレスを 1 つでも認識できる場合、システムは認識できるアドレスを更新します。

インターネット アクセスおよびハイ アベイラビリティ

システムは、ポート 443/HTTPS を使用してインテリジェンス フィードをダウンロードし、443/HTTP または 80/HTTP を使用してカスタムまたはサードパーティのフィードをダウンロードします。フィードを更新するには、デバイスでインバウンドとアウトバウンドの両方の適切なポートを開く必要があります。フィードサイトに直接アクセスできない場合、システムはプロキシ サーバを使用できます。

システムでは、カスタム フィードのダウンロード時にピア SSL 証明書の検証は行われません。また、証明書のバンドルまたは自己署名証明書を使用したリモート ピアの検証もサポートされていません。

フィードとリストの管理

[Security Intelligence] リストとフィード（総称してセキュリティ インテリジェンス オブジェクトと呼ばれる）は、オブジェクト マネージャの [Security Intelligence] ページを使用して作成および管理します。

保存または適用されているアクセス コントロール ポリシーで現在使用されているカスタム リストまたはフィードは削除できないことに注意してください。さらに、個別の IP アドレスは削除できますが、グローバル リストは削除できません。同様に、インテリジェンス フィードは削除できませんが、編集することによって更新の頻度を無効にしたり、変更したりできます。

セキュリティ インテリジェンス オブジェクトのクイック リファレンス

次の表に、セキュリティインテリジェンスのフィルタリングを実行する場合に使用できるオブジェクトのクイック リファレンスを示します。

表 *3:* セキュリティ インテリジェンス

機能	ブローバルブロックなしリストまたはブロックリスト	インテリジェンス フィード	カスタム フィード	カスタム リスト	ネットワーク オブジェクト
使用方法	デフォルトで、アクセス コントロール ポリシーで	ブロックなしリストまたはブロックリストのいずれかのオブジェクトとして任意のアクセス コントロール ポリシーで			
セキュリティ ゾーンで制約することができるか	いいえ（No）	あり	あり	あり	あり
削除できるか	いいえ（No）	いいえ（No）	はい（保存または適用されているアクセス コントロール ポリシーで現在使用されている場合を除く）		
オブジェクト マネージャの編集機能	IP アドレスのみを削除する	更新の頻度を無効にするか、変更する	完全に変更する	変更されたリストのみをアップロードする	完全に変更する
変更されたときに設定の再展開が必要か	削除する場合は「はい」（IP アドレスを追加する場合は、再展開する必要はありません）	いいえ（No）	いいえ（No）	あり	あり

グローバルブロックなしリストとブロックリストの操作

ライセンス：**Protection**

システムのグローバルブロックなしリストとブロックリストは、デフォルトですべてのアクセス コントロール ポリシーに含まれており、すべてのゾーンに適用されます。ポリシーごとに、これらのグローバル リストを使用しないことを選択できます。

グローバル リストにIPアドレスを追加した後は、設定を再展開する必要はありません。逆に、グローバルブロックなしリストまたはブロックリストから IP アドレスを削除した後は、変更を有効にするために設定を再展開する必要があります。

ネットマスク /0 のネットワークオブジェクトはブロックなしリストまたはブロックリストに追加できますが、ネットマスク /0 を使用したアドレスブロックは無視され、これらのアドレ

スに基づいたブロックなしリストおよびブロックリストフィルタリングは行われないことに注意してください。セキュリティ インテリジェンス フィードからのネットマスク /0 のアドレスブロックも無視されます。すべてのトラフィックをモニタまたはブロックする場合は、セキュリティインテリジェンスフィルタリングの代わりに、[Monitor] または [Block] ルールアクションでアクセス コントロール ルールを使用し、[Source Networks] および [Destination Networks] の [any] のデフォルト値をそれぞれ使用します。

IP アドレスをグローバルブロックなしリストまたはブロックリストから削除する方法：

ステップ 1 オブジェクトマネージャの [Security Intelligence] ページで、グローバルブロックなしリストまたはブロックリストの横にある編集アイコン（）をクリックします。

ステップ 2 リストから削除する IP アドレスの横にある削除アイコン（）をクリックします。

複数の IP アドレスを同時に削除するには、Shift キーおよび Ctrl キーを使用して IP アドレスを選択し、右クリックして [Delete] を選択します。

ステップ 3 [Store ASA FirePOWER Changes] をクリックします。

アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の導入（92 ページ）を参照してください。

インテリジェンス フィードの操作

ライセンス：Protection

ASA FirePOWER モジュールには、ブロックリストの作成に役立つインテリジェンスフィードがあります。このフィードは、VRT によってレピュテーションが低いと判断された IP アドレスの定期的に更新される複数のリストから成ります。フィードの各リストは、オープンリレー、既知の攻撃者、bogus IP アドレス（bogon）などの、特定のカテゴリを表します。アクセス コントロール ポリシーでは、カテゴリのいずれかまたはすべてをブロックできます。

インテリジェンスフィードは定期的に更新されるため、システムは最新の情報を使用してネットワーク トラフィックをフィルタ処理できます。ただし、セキュリティに対する脅威（マルウェア、スパム、ボットネット、フィッシングなど）を表す不正な IP アドレスが現れては消えるペースが速すぎて、新しいポリシーを更新して展開するには間に合わないこともあります。

インテリジェンスフィードは削除できませんが、編集することによって更新の頻度を変更できます。デフォルトで、フィードは 2 時間ごとに更新されます。

インテリジェンス フィードの更新頻度を変更するには、次の手順を実行します。

ステップ 1 オブジェクト マネージャの [Security Intelligence] ページで、インテリジェンス フィードの横にある編集アイコン（）をクリックします。

ステップ 2 [Update Frequency] を編集します。

2 時間から 1 週間までの範囲で、さまざまな間隔から選択できます。フィードの更新を無効にすることもできます。

ステップ 3 [Store ASA FirePOWER Changes] をクリックします。

カスタム セキュリティ インテリジェンス フィードの操作

ライセンス：Protection

カスタムまたはサードパーティのセキュリティ インテリジェンス フィードを使用すると、インターネット上で定期的に更新される他の信頼できるブロックなしリストやブロックリストによって、インテリジェンスフィードを増やすことができます。また、内部フィードを設定することもできます。

フィードを設定する場合は、URL を使用して場所を指定します。この URL は Punycode でエンコードすることはできません。デフォルトでは、システムは設定された間隔でフィード ソース全体をダウンロードします。

オプションで、md5 チェックサムを使用して、更新フィードをダウンロードするかどうか判断するようにシステムを設定できます。モジュールが最後にフィードをダウンロードした後にチェックサムが変更されていない場合、システムによるチェックサムの再ダウンロードは不要です。特に内部フィードが大きい場合には、md5 チェックサムを使用することができます。md5 チェックサムは、チェックサムのみを含む単純なテキスト ファイルに保存する必要があります。コメントはサポートされていません。

セキュリティ インテリジェンス フィードを設定する方法：

ステップ 1 オブジェクト マネージャの [Security Intelligence] ページで、[Add Security Intelligence] をクリックします。

ステップ 2 フィードの名前を [Name] に入力します。中カッコ（{}）を除く、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 3 [Type] ドロップダウンリストから、[Feed] を設定することを指定します。

ステップ 4 [Feed URL] を指定し、オプションで [MD5 URL] を指定します。

ステップ 5 [Update Frequency] を指定します。

2 時間から 1 週間までの範囲で、さまざまな間隔から選択できます。フィードの更新を無効にすることもできます。

ステップ 6 [Store ASA FirePOWER Changes] をクリックします。

セキュリティ インテリジェンス フィードのオブジェクトが作成されます。フィードの更新を無効にした場合を除き、システムはフィードをダウンロードして検証しようとします。これで、アクセス コントロール ポリシーでフィード オブジェクトを使用できるようになりました。

手動によるセキュリティ インテリジェンス フィードの更新

ライセンス：Protection

手動でセキュリティ インテリジェンス フィードを更新すると、インテリジェンス フィードを含め、すべてのフィードが更新されます。

すべてのセキュリティ インテリジェンス フィードを更新する方法：

ステップ 1 オブジェクト マネージャの [Security Intelligence] ページで、[Update Feeds] をクリックします。

ステップ 2 すべてのフィードを更新することを確認します。

更新が有効になるまで数分かかる可能性があることが警告されます。

ステップ 3 [OK] をクリックします。

フィードの更新をダウンロードして検証したら、システムはその更新されたフィードを使用してトラフィックのフィルタリングを開始します。

カスタム セキュリティ インテリジェンスのリストの操作

ライセンス：Protection

セキュリティ インテリジェンスのリストは、手動でアップロードする IP アドレスおよびアドレス ブロックのシンプルな静的リストです。カスタム リストは、フィードやグローバル リストの 1 つを増やしたり、微調整したりする場合に役立ちます。

アドレス ブロックのネットマスクは、IPv4 および IPv6 の場合、それぞれ 0 から 32、または 0 から 128 までの整数になることに注意してください。

たとえば、信頼できるフィードが重要なリソースへのアクセスを誤ってブロックしていても、そのフィードが組織にとって全体的に有用である場合、セキュリティ インテリジェンス フィード オブジェクトをアクセス コントロール ポリシーのブロックリストから削除する代わりに、誤って分類された IP アドレスだけを含むカスタムブロックなしリストを作成できます。

セキュリティ インテリジェンスのリストを変更するには、ソース ファイルを変更して、新しいコピーをアップロードする必要があることに注意してください。詳細については、セキュリティ インテリジェンス リストの更新 （33 ページ）を参照してください。

新しいセキュリティ インテリジェンスをアップロードする方法：

ステップ 1 オブジェクト マネージャの [Security Intelligence] ページで、[Add Security Intelligence] をクリックします。

ステップ 2 リストの名前を [Name] に入力します。中カッコ（{}）を除く、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 3 [Type] ドロップダウンリストから、[List] をアップロードすることを指定します。

ステップ 4 [Browse] をクリックして list.txt ファイルを参照し、[Upload] をクリックします。

リストがアップロードされます。ポップアップ ウィンドウに、リストで検出されたIPアドレスとアドレスブロックの総数が表示されます。

番号が予期したものでない場合は、ファイルの書式設定を調べ、再試行してください。

ステップ 5 [Store ASA FirePOWER Changes] をクリックします。

セキュリティ インテリジェンス リストの更新

ライセンス：Protection

セキュリティ インテリジェンス リストを編集するには、ソース ファイルを変更して、新しいコピーをアップロードする必要があります。ASDMを使用してファイルの内容を変更することはできません。ソース ファイルへのアクセス権がない場合は、ASDM インターフェイスを使用してコピーをダウンロードできます。

セキュリティ インテリジェンス リストを変更する方法：

ステップ 1 オブジェクトマネージャの [Security Intelligence] ページで、更新するリストの横にある編集アイコン（）をクリックします。

ステップ 2 編集するリストのコピーが必要な場合、[Download] をクリックして、プロンプトに従ってリストをテキスト ファイルとして保存します。

必要に応じてリストを変更します。

ステップ 3 [Security Intelligence] ポップアップ ウィンドウで、[Browse] をクリックして変更されたリストを参照し、[Upload] をクリックします。

ステップ 4 [Store ASA FirePOWER Changes] をクリックします。

アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の導入（92ページ）を参照してください。

ポート オブジェクトの操作

ライセンス：任意

ポート オブジェクトは、異なるプロトコルをそれぞれ少し異なる方法で表します。

- TCP および UDP の場合、ポート オブジェクトは、カッコ内にプロトコル番号が記載されたトランスポート層プロトコルと、オプションの関連ポートまたはポート範囲を表します。例：TCP(6)/22。
- ICMP および ICMPv6（IPv6 ICMP）の場合、ポート オブジェクトはインターネット層プロトコルおよびオプションのタイプとコードを表します。例：ICMP(1):3:3

- ポート オブジェクトは、ポートを使用しない他のプロトコルを表すこともできます。

システムが既知のポート用にデフォルトのポート オブジェクトを提供することに注意してください。これらのオブジェクトは変更または削除できますが、代わりにカスタム ポート オブジェクトを作成することを推奨します。

ポート オブジェクトおよびグループ（オブジェクトのグループ化 （24 ページ）を参照）は、アクセス コントロール ポリシーやポートの変数など、ASA FirePOWER モジュールのさまざまな場所で使用できます。

使用中のポート オブジェクトは削除できません。さらに、ポート オブジェクトを編集または削除した後に、アクティブ ポリシーがオブジェクトを参照する場合、変更を有効にするには設定を再展開する必要があります。設定変更の導入 （92 ページ）を参照してください。

アクセス コントロール ルールの送信元ポートの条件には TCP/UDP 以外のプロトコルを追加できないことに注意してください。さらに、送信元ポートと宛先ポートの両方のポート条件をルールで設定する場合、トランスポート プロトコルを混在させることはできません。

送信元ポートの条件で使用されるポート オブジェクト グループにサポート対象外のプロトコルを追加した場合、使用場所のルールはポリシー展開には適用されません。さらに、TCP と UDP の両方のポートを含むポート オブジェクトを作成してから、ルールの送信元ポートの条件としてそのポート オブジェクトを追加した場合、宛先ポートを追加することはできません。その逆もまた同様です。

ポート オブジェクトを作成する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 [Port] で、[Individual Objects] を選択します。

ステップ 3 [Add Port] をクリックします。

ステップ 4 [Name] にポート オブジェクトの名前を入力します。中カッコ（{}）を除く、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5 [Protocol] を選択します。

[TCP]、[UDP]、[IP]、[ICMP]、または [IPv6 ICMP] から選択するか、[Other] ドロップダウンリストを使用して別のプロトコルまたは [All] プロトコルを選択できます。

ステップ 6 オプションで、[Port] またはポート範囲を使用して TCP または UDP ポート オブジェクトを制限します。

1 ～ 65535 までの任意のポートを指定するか、すべてのポートと一致するように [any] を指定できます。ポートの範囲を指定するには、ハイフンを使用します。

ステップ 7 必要に応じて、[Type] および関連する [Code]（該当する場合）を使用して、ICMP または IPV6 ICMP ポート オブジェクトを制限します。

ICMP または IPv6 ICMP オブジェクトを作成する場合、タイプおよびコード（該当する場合）を指定できます。ICMP のタイプとコードの詳細については、
http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml および
http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml を参照してください。任意のタイプ

と一致するようにタイプに any を設定するか、指定したタイプの任意のコードと一致するようにコードに any を設定できます。

ステップ 8 オプションで、[Other] を選択し、ドロップダウン リストからプロトコルを選択します。[All] プロトコルを選択した場合は、[Port] フィールドにポート番号を入力します。

ステップ 9 [Store ASA FirePOWER Changes] をクリックします。

URL オブジェクトの操作

ライセンス：任意

設定した各 URL オブジェクトは、単一の URL または IP アドレスを表します。アクセス コントロール ポリシーでは、URL オブジェクトとグループを使用できます（オブジェクトのグループ化 （24 ページ）を参照）。たとえば、特定の URL をブロックするアクセス コントロール ルールを作成することもできます。

HTTPS トラフィックをブロックするには、トラフィックの Secure Sockets Layer（SSL）証明書から URL を入力できることに注意してください。証明書から URL を入力する場合は、ドメイン名を入力し、サブドメイン情報を省略します。（たとえば、www.example.com の代わりに example.com と入力します。）証明書の URL に基づいてトラフィックをブロックする場合、その Web サイトへの HTTP トラフィックと HTTPS トラフィックの両方がブロックされます。

使用中の URL オブジェクトは削除できません。さらに、URL オブジェクトを編集または削除した後に、アクティブ ポリシーがオブジェクトを参照する場合、変更を有効にするには設定を再展開する必要があります。設定変更の導入 （92 ページ）を参照してください。

URL オブジェクトを作成する方法：

ステップ 1 [Configuration] > > [ASA FirePOWER Configuration] > > [Object Management] の順に選択します。

ステップ 2 [URL] で、[Individual Objects] を選択します。

ステップ 3 [Add URL] をクリックします。

ステップ 4 [Name] に URL オブジェクトの名前を入力します。中カッコ（{}）を除く、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5 URL オブジェクトの [URL] または IP アドレスを入力します。

ステップ 6 [Store ASA FirePOWER Changes] をクリックします。

アプリケーション フィルタの操作

ライセンス：任意

ASA FirePOWER モジュールは IP トラフィックを分析するときに、ネットワーク上でよく使用されているアプリケーションを特定しようとします。アプリケーション認識は、アプリケーション ベースのアクセス コントロールの実行には不可欠です。システムは多くのアプリケーションに対応するディテクタとともに提供されており、シスコでは頻繁に更新を行い、システムおよび脆弱性データベース（VDB）の更新を通じてディテクタを追加しています。

アプリケーション フィルタは、アプリケーションのリスク、ビジネスとの関連性、タイプ、カテゴリ、およびタグに関連付けられている条件に従ってアプリケーションをグループ化します。アプリケーション フィルタを使用すると、アプリケーションを個別に検索および追加する必要がないため、アクセス コントロール ルール用のアプリケーション条件を素早く作成できます。詳細については、トラフィックとアプリケーション フィルタの一致（141 ページ）を参照してください。

アプリケーション フィルタを使用する別の利点は、新しいアプリケーションを変更または追加する場合にフィルタを使用するアクセス コントロール ルールを更新する必要がないことです。たとえば、すべてのソーシャル ネットワーキング アプリケーションをブロックするようにアクセス コントロール ポリシーを設定し、VDB の更新に新しいソーシャル ネットワーキング アプリケーション ディテクタが含まれる場合、ポリシーは VDB の更新時に更新されます。システムが新しいアプリケーションをブロックする前に、変更された設定を再展開する必要がありますが、アプリケーションをブロックするアクセス コントロール ルールを更新する必要はありません。

システム提供のアプリケーション フィルタがユーザのニーズに応じてアプリケーションをグループ化しない場合、独自のフィルタを作成することができます。ユーザ定義のフィルタでは、システム提供のフィルタをグループ化して結合できます。たとえば、非常にリスクが高く、ビジネス関連性が低いアプリケーションをすべてブロックするフィルタを作成することができます。個々のアプリケーションを手動で指定することによってもフィルタを作成できますが、これらのフィルタは、モジュール ソフトウェアまたは VDB を更新しても自動的に更新されないことを覚えておいてください。

システム提供のアプリケーション フィルタと同様、ユーザ定義のアプリケーション フィルタもアクセス コントロール ルールで使用できます。

アプリケーション フィルタを作成および管理する場合は、オブジェクト マネージャ（[Configuration] > [ASA FirePOWER Configuration] > [Object Management]）を使用します。アプリケーションの条件をアクセス コントロール ルールに追加しながら、アプリケーション フィルタをすぐに作成できることに注意してください。

[Application Filters] リストには、独自のフィルタを作成するために選択できるシステム提供のアプリケーション フィルタが含まれています。表示されるフィルタは検索文字列を使用することによって抑制できます。これは、カテゴリとタグの場合に特に役立ちます。

[Available Applications] リストには、選択したフィルタ内の個別のアプリケーションが含まれます。また、検索ストリングを使用して、表示されるアプリケーションを抑制することもできます。

システムは、OR 演算を使用して同じフィルタ タイプの複数のフィルタをリンクします。中リスク フィルタに 100 のアプリケーションが含まれており、高リスク フィルタに 50 のアプリケーションが含まれているシナリオについて考えてみてください。両方のフィルタを選択すると、システムは使用可能な 150 のアプリケーションを表示します。

システムは、AND 演算を使用して異なるタイプのフィルタをリンクします。たとえば、中リスクおよび高リスクのフィルタと中レベルおよび高レベルのビジネス関連性のフィルタを選択した場合、システムは、中リスクまたは高リスクで、かつ中レベルおよび高レベルのビジネス関連性があるアプリケーションを表示します。

ヒント 関連するアプリケーションの詳細については、情報アイコン（）をクリックします。詳細情報を表示するには、情報ポップアップにあるいずれかのインターネット検索リンクをクリックします。

フィルタに追加するアプリケーションを決定したら、それらを個別に追加するか、アプリケーション フィルタを選択した場合は、[All apps matching the filter] を追加することができます。[Selected Applications and Filters] リストにあるアイテムの合計数が 50 を超えない限り、複数のフィルタおよび複数のアプリケーションを任意の組み合わせで追加できます。

アプリケーション フィルタを作成すると、オブジェクト マネージャの [Application Filters] ページに一覧表示されます。このページには、各フィルタを構成する条件の合計数が表示されます。

表示されるアプリケーション フィルタのソートとフィルタの詳細については、オブジェクト マネージャの使用 （24 ページ）を参照してください。使用中のアプリケーション フィルタは削除できないことに注意してください。さらに、アプリケーション フィルタ オブジェクトを編集または削除した後に、アクティブポリシーがオブジェクトを参照する場合、変更を有効にするには設定を再展開する必要があります。設定変更の導入 （92 ページ）を参照してください。

アプリケーション フィルタを作成する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 [Application Filters] をクリックします。

ステップ 3 [Add Application Filter] をクリックします。

ステップ 4 [Name] を入力します。中カッコ（{}）を除く、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5 必要に応じて、[Application Filters] リストにあるシステム提供のフィルタを使用して、フィルタに追加するアプリケーションのリストを絞り込みます。

- リストを展開および縮小するには、各フィルタ タイプの横にある矢印をクリックします。
- フィルタ タイプを右クリックし、[Check All] または [Uncheck All] をクリックします。このリストには、各タイプで選択したフィルタ数が示されることに注意してください。
- 表示されるフィルタを絞り込むには、[Search by name] フィールドに検索文字列を入力します。これは、カテゴリとタグの場合に特に有効です。検索をクリアするには、クリア アイコン（）をクリックします。
- フィルタのリストを更新し、選択したフィルタをすべてクリアするには、リロード アイコン（）をクリックします。

- すべてのフィルタと検索フィールドをクリアするには、[Clear All Filters] をクリックします。

選択したフィルタに一致するアプリケーションが [Available Applications] リストに表示されます。リストには一度に 100 のアプリケーションが表示されます。

ステップ 6 [Available Applications] リストから、フィルタに追加するアプリケーションを選択します。

- 前の手順で指定した制約を満たすすべてのアプリケーションを追加するには、[All apps matching the filter] を選択します。
- 表示される個別のアプリケーションを絞り込むには、[Search by name] フィールドに検索文字列を入力します。検索をクリアするには、クリア アイコン（×）をクリックします。
- 使用可能な個別のアプリケーションのリストを参照するには、リストの下部にあるページング アイコンをクリックします。
- 複数の個別のアプリケーションを選択するには、Shift キーおよび Ctrl キーを使用します。現在表示されている個別のアプリケーションをすべて選択するには、右クリックして [Select All] を選択します。
- アプリケーションのリストを更新し、選択したアプリケーションをすべてクリアするには、リロード アイコン（↻）をクリックします。

個別のアプリケーションと [All apps matching the filter] は同時に選択できません。

ステップ 7 選択したアプリケーションをフィルタに追加します。クリックしてドラッグするか、[Add to Rule] をクリックできます。

結果は次のもので構成されています。

- 選択したアプリケーション フィルタ
- 選択した個別の使用可能なアプリケーション、または [All apps matching the filter]

フィルタには最大 50 のアプリケーションおよびフィルタを追加できます。選択したアプリケーションからアプリケーションまたはフィルタを削除するには、該当する削除アイコン（🗑）をクリックします。1 つ以上のアプリケーションおよびフィルタを選択するか、または右クリックして [Select All] を選択してから、右クリックして [Delete Selected] を選択することもできます。

ステップ 8 [Store ASA FirePOWER Changes] をクリックします。

変数セットの操作

ライセンス：Protection

変数は、侵入ルールで一般的に使用される値を表し、送信元および宛先の IP アドレスおよびポートを識別します。侵入ポリシーにある変数を使用して、ルール抑制、適応プロファイル、および動的ルール状態にある IP アドレスを表すこともできます。

ヒント　プリプロセッサルールは、侵入ルールで使用されるネットワーク変数で定義されたホストにかかわらず、イベントをトリガーできます。

変数セットを使用して、変数を管理、カスタマイズ、およびグループ化します。ASA FirePOWER モジュール提供のデフォルトの変数セットを使用するか、独自のカスタムセットを作成することができます。いずれのセットでも、定義済みのデフォルトの変数を変更したり、ユーザ定義の変数を追加および変更したりできます。

ASA FirePOWER モジュール提供の共有オブジェクト ルールと標準テキスト ルールの大部分では、定義済みのデフォルト変数を使用してネットワークとポート番号を定義します。たとえば、ルールの大半は、保護されたネットワークを指定するために変数 $HOME_NET を使用して、保護されていない（つまり外部の）ネットワークを指定するために変数 $EXTERNAL_NET を使用します。さらに、特殊なルールでは、他の定義済みの変数がしばしば使用されます。たとえば、Web サーバに対するエクスプロイトを検出するルールは、$HTTP_SERVERS 変数および $HTTP_PORTS 変数を使用します。

ルールがより効率的なのは、変数がユーザのネットワーク環境をより正確に反映する場合です。少なくとも、事前定義されたデフォルト変数の最適化 （39 ページ） で説明されているように、デフォルトのセットにあるデフォルトの変数を変更する必要があります。$HOME_NET などの変数がネットワークを正しく定義し、$HTTP_SERVERS にネットワーク上のすべての Web サーバが含まれるようにするには、処理は最適化され、疑わしいアクティビティがないかどうかすべての関連システムが監視されます。

変数を使用するには、変数セットをアクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルト アクションに関連付けられている侵入ポリシーにリンクします。デフォルトでは、デフォルトの変数セットは、アクセス コントロール ポリシーによって使用されるすべての侵入ポリシーにリンクされています。

事前定義されたデフォルト変数の最適化

デフォルトでは、ASA FirePOWER モジュールには、定義済みのデフォルト変数から成る単一のデフォルト変数セットがあります。脆弱性調査チーム（VRT）はルールの更新を使用して、デフォルト変数を含む、新規および更新された侵入ルール、および他の侵入ポリシー要素を提供します。詳細については、「ルール更新とローカル ルール ファイルのインポート （582 ページ）」を参照してください。

ASA FirePOWER モジュールで提供される多くの侵入ルールでは定義済みのデフォルト変数が使用されるため、それらの変数に対して適切な値を設定する必要があります。変数セットを使用してネットワーク上のトラフィックを特定する方法によっては、任意またはすべての変数セットにあるこれらのデフォルト変数の値を変更することができます。詳細については、「変数の追加と編集 （48 ページ）」を参照してください。

注意：アクセス コントロールまたは侵入ポリシーをインポートすると、デフォルトの変数セットにある既存のデフォルト変数が、インポートしたデフォルト変数で上書きされます。既存のデフォルト変数セットに、インポートされたカスタム変数セットに存在しないカスタム変数が

含まれる場合、一意的な変数が保持されます。詳細については、設定のインポート（620ページ）を参照してください。

次の表に、ASA FirePOWER モジュールで提供される変数に関する説明、および通常変更する変数を示します。変数をご使用のネットワークに合わせて調整する方法を決定するには、プロフェッショナル サービスまたはサポートに問い合わせてください。

表 *4 : ASA FirePOWER* モジュールで提供される変数（続き）

変数名	説明	変更しますか
$AIM_SERVERS	既知の AOL Instant Messenger（AIM）サーバを定義し、チャット ベースのルールおよびAIM エクスプロイトを検索するルールで使用されます。	不要。
$DNS_SERVERS	ドメイン ネーム サービス（DNS）サーバを定義します。DNS サーバに特に影響するルールを作成する場合、$DNS_SERVERS 変数を宛先または送信元 IP アドレスとして使用できます。	現在のルール セットでは不要です。
$EXTERNAL_NET	ASA FirePOWER モジュールに非保護ネットワークとして表示され、外部ネットワークを定義するために多くのルールで使用されるネットワークを定義します。	はい。$HOME_NET を適切に定義してから、$EXTERNAL_NET の値として $HOME_NET を除外する必要があります。
$FILE_DATA_PORTS	ネットワーク ストリームでファイルを検出する侵入ルールで使用される、暗号化されていないポートを定義します。	不要。
$FTP_PORTS	ネットワーク上の FTP サーバのポートを定義し、FTP サーバのエクスプロイト ルールに使用されます。	FTP サーバがデフォルト ポート以外のポートを使用する場合は変更します（モジュール インターフェイスでデフォルト ポートを確認できます）。

変数名	説明	変更しますか
$GTP_PORTS	パケット デコーダが GTP（General Packet Radio Service（GPRS）トンネリング プロトコル）PDU 内部でペイロードを取得するデータ チャネル ポートを定義します。	不要。
$HOME_NET	関連した侵入ポリシーが監視するネットワークを定義し、内部ネットワークを定義するために多くのルールで使用されます。	内部ネットワークの IP アドレスを指定する場合は変更します。
$HTTP_PORTS	ネットワーク上の Web サーバのポートを定義し、Web サーバのエクスプロイト ルールに使用されます。	Web サーバがデフォルト ポート以外のポートを使用する場合は変更します（モジュール インターフェイスでデフォルト ポートを確認できます）。
$HTTP_SERVERS	ネットワーク上の Web サーバを定義します。Web サーバのエクスプロイト ルールで使用されます。	HTTP サーバを実行する場合は変更します。
$ORACLE_PORTS	ネットワーク上で Oracle データベース サーバのポートを定義し、Oracle データベースでの攻撃をスキャンするルールで使用されます。	Oracle サーバを実行する場合は変更します。
$SHELLCODE_PORTS	システムにシェル コードのエクスプロイトをスキャンさせるポートを定義し、シェル コードを使用するエクスプロイトを検出するルールで使用されます。	不要。
$SIP_PORTS	ネットワーク上の SIP サーバのポートを定義し、SIP のエクスプロイト ルールに使用されます。	不要。

変数名	説明	変更しますか
$SIP_SERVERS	ネットワーク上で SIP サーバを定義し、SIP をターゲットとしたエクスプロイトを解決するルールで使用されます。	はい。SIP サーバを実行している場合は、$HOME_NET を適切に定義してから、$SIP_SERVERS の値として $HOME_NET を含める必要があります。
$SMTP_SERVERS	ネットワーク上で SMTP サーバを定義し、メール サーバをターゲットとするエクスプロイトを解決するルールで使用されます。	SMTP サーバを実行する場合は変更します。
$SNMP_SERVERS	ネットワーク上で SNMP サーバを定義し、SNMP サーバでの攻撃をスキャンするルールで使用されます。	SNMP サーバを実行する場合は変更します。
$SNORT_BPF	後に、バージョン 5.3.0 以降にアップグレードされるバージョン 5.3.0 以前の ASA FirePOWER モジュール ソフトウェア リリースのシステム上に存在する場合にのみ表示されるレガシー拡張変数を特定します。拡張変数について（58 ページ）を参照してください。	変更しません。この変数は表示または削除のみが可能です。削除後に、編集または復元することはできません。
$SQL_SERVERS	ネットワーク上でデータベース サーバを定義し、データベースをターゲットとしたエクスプロイトを解決するルールで使用されます。	SQL サーバを実行する場合は変更します。
$SSH_PORTS	ネットワーク上の SSH サーバのポートを定義し、SSH サーバのエクスプロイト ルールに使用されます。	SSH サーバがデフォルト ポート以外のポートを使用する場合は変更します（モジュール インターフェイスでデフォルト ポートを確認できます）。

変数名	説明	変更しますか
$SSH_SERVERS	ネットワーク上で SSH サーバを定義し、SSH をターゲットとしたエクスプロイトを解決するルールで使用されます。	はい。SSH サーバを実行している場合は、$HOME_NET を適切に定義してから、$SSH_SERVERS の値として $HOME_NET を含める必要があります。
$TELNET_SERVERS	ネットワーク上で既知の Telnet サーバを定義し、Telnet サーバをターゲットとしたエクスプロイトを解決するルールで使用されます。	Telnet サーバを実行する場合は変更します。
$USER_CONF	本来はモジュール インターフェイスを介して使用できない 1 つ以上の機能を設定できる一般ツールを提供します。拡張変数について （58 ページ）を参照してください。 **注意** $USER_CONF の設定が競合または重複していると、システムは停止します。拡張変数について （58 ページ）を参照してください。	機能の説明で指示されている場合や、サポートによる指示があった場合を除き、変更しません。

変数セットについて

ライセンス：Protection

変数を任意のセットに追加すると、それはすべてのセットに追加されます。つまり、各変数セットは、システムで現在設定されているすべての変数のコレクションになります。いずれの変数セットでも、ユーザ定義の変数を追加したり、任意の変数の値をカスタマイズしたりできます。

ASA FirePOWER モジュールでは、初めに定義済みのデフォルト値から成る単一のデフォルトの変数セットが提供されます。デフォルト設定では、各変数は最初はそのデフォルト値に設定されています。定義済みの変数の場合、このデフォルト値は VRT によって設定され、ルール更新で提供される値です。

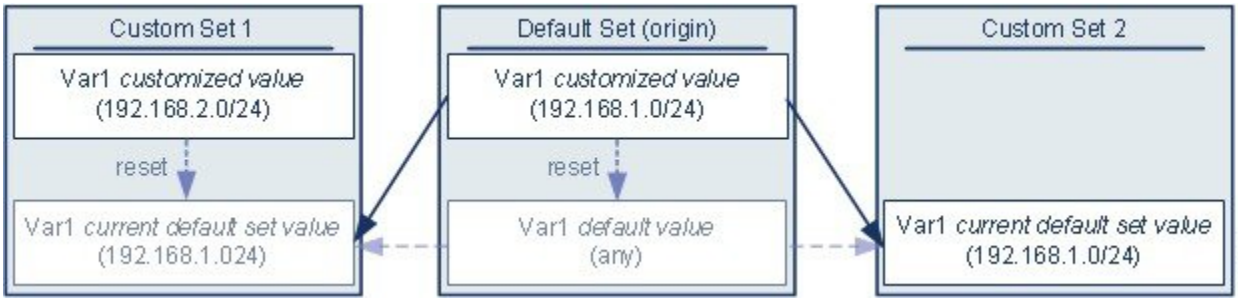
定義済みのデフォルト変数は、デフォルト値のままにすることもできますが、事前定義されたデフォルト変数の最適化 （39 ページ）の説明に従い、定義済みの変数のサブセットを変更することを推奨します。

変数はデフォルトセットでのみ使用できますが、多くの場合、1つ以上のカスタム設定を追加し、異なるセットで異なる変数の値を設定し、場合によっては新しい変数を追加することによって、最大限に活用できます。

複数のセットを使用する場合は、デフォルトのセットにある任意の変数の現在値によって、他のすべてのセットの変数のデフォルト値が決まることに注意してください。

例：デフォルト セットにユーザ定義変数を追加する

次の図は、値が 192.168.1.0/24 のデフォルト セットにユーザ定義変数 Var1 を追加した場合のセットのインタラクションを示しています。



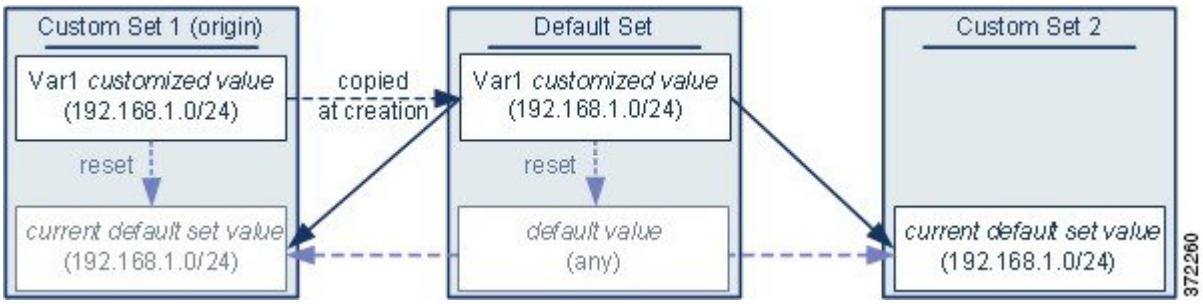
オプションで、任意のセットの Var1 値をカスタマイズできます。Var1 がカスタマイズされていない Custom Set 2 では、この値は 192.168.1.0/24 です。Custom Set 1 では、Var1 のカスタマイズ値 192.168.2.0/24 はデフォルト値をオーバーライドします。デフォルト セット内のユーザ定義変数をリセットすると、すべてのセットのデフォルト値が any にリセットされます。

この例では、Custom Set 2 で Var1 を更新しなかった場合、デフォルト セットで Var1 をカスタマイズまたはリセットすると、Custom Set 2 の現在のデフォルト値 Var1 が更新され、変数セットにリンクされているすべての侵入ポリシーに影響を与えることに注意してください。

この例では示されていませんが、セット間のインタラクションは、デフォルトセットのデフォルト変数をリセットすると現在のルールの更新でシステムによって設定された値にリセットされること以外は、ユーザ定義変数およびデフォルト変数で同じであることに注意してください。

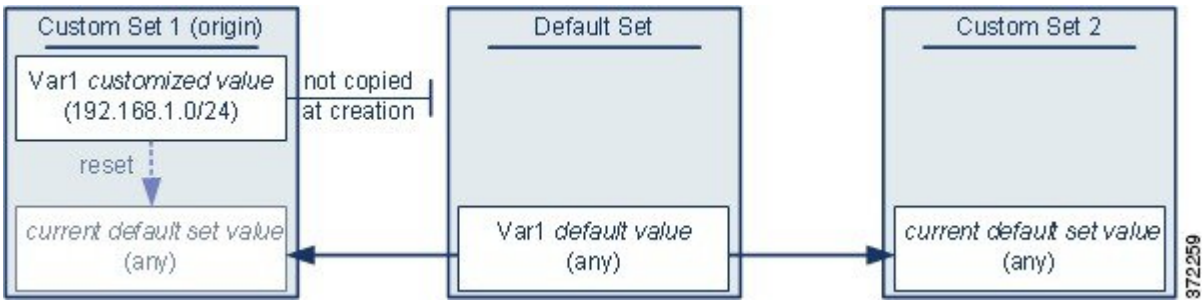
例：カスタム セットにユーザ定義変数を追加する

次の2つの例は、カスタムセットにユーザ定義変数を追加した場合の変数セットのインタラクションを示しています。新しい変数を保存すると、設定値を他のセットのデフォルト値として使用するかどうかを尋ねるプロンプトが出されます。次の例では、設定値を使用するという選択がなされています。



Custom Set 1 からの Var1 の発信元を除き、この例は Var1 をデフォルト セットに追加した上述の例と同じであることに注意してください。Var1 のカスタマイズ値 192.168.1.0/24 を Custom Set 1 に追加すると、値はデフォルト値 any を持つカスタマイズ値としてデフォルト セットにコピーされます。その後、Var1 の値とインタラクションは、Var1 をデフォルト セットに追加した場合と同じになります。前述の例と同様、デフォルト セットで Var1 をカスタマイズまたはリセットすると、Custom Set 2 の現在のデフォルト値 Var1 が更新され、変数セットにリンクされているすべての侵入ポリシーに影響を与えることに注意してください。

次の例では、前述の例にあるように値が 192.168.1.0/24 の Var1 を Custom Set 1 に追加しますが、Var1 の設定値を他のセットのデフォルト値として使用しないことを選択します。



このアプローチでは、Var1 をデフォルト値 any を持つすべてのセットに追加します。Var1 を追加したら、任意のセットでその値をカスタマイズできます。このアプローチの利点は、デフォルト セットで Var1 を最初にカスタマイズしないことによって、デフォルト セットの値をカスタマイズし、Var1 をカスタマイズしていない Custom Set 2 などのセット内の現在の値を意図せずに変更してしまうリスクが軽減されます。

変数セットの管理

ライセンス：Protection

[Object Manager] ページ（[Configuration] > > [ASA FirePOWER Configuration] > > [Object Management] > ）で [Variable Sets] を選択した場合、オブジェクト マネージャは、デフォルトの変数セットとユーザが作成したカスタム セットをリストします。

新しくインストールされたシステムでは、デフォルトの変数セットは、デフォルトのシステム提供変数だけで構成されます。

各変数セットには、システム提供のデフォルト変数と、任意の変数セットから追加したすべてのカスタム変数が含まれます。デフォルト設定は編集できますが、デフォルトセットの名前を変更したり、削除したりすることはできないことに注意してください。

次の表に、変数セットを管理するために実行できるアクションを要約します。

表 5: 変数セットの管理アクション

目的	操作
変数セットを表示する	[Configuration] > [ASA FirePOWER Configuration] > [Object Management] を選択し、[Variable Set] を選択します。
変数セットを名前でフィルタする	名前の入力を開始します。入力するにつれて、ページが更新され、一致する名前が表示されます。
名前のフィルタリングをクリアする	フィルタ フィールドのクリア アイコン（×）をクリックします。
カスタム変数セットを追加する	[Add Variable Set] をクリックします。 便宜を図るため、新しい変数セットには、現在定義されているすべてのデフォルト変数とカスタマイズ変数が含まれます。
変数セットを編集する	編集する変数セットの横にある編集アイコン（）をクリックします。 変数セットの行内で右クリックし、[Edit] を選択することもできます。
カスタム変数セットを削除する	変数セットの横にある削除アイコン（）をクリックしてから、[Yes] をクリックします。デフォルトの変数セットは削除できません。削除する変数セットで作成された変数は、他のセットで削除されたり他の方法で影響を受けたりしないことに注意してください。 変数セットの行内で右クリックし、[Delete] を選択してから、[Yes] をクリックすることもできます。複数のセットを選択するには、Ctrl キーと Shift キーを使用します。

変数セットを設定した後、それを侵入ポリシーにリンクできます。

変数セットを編集または作成する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 [Variable Set] を選択します。

ステップ 3 変数セットを作成したり、既存のセットを編集したりするには、以下の手順に従います。

- 変数セットを作成するには、[Add Variable Set] をクリックします。
- 変数セットを作成するには、変数セットの横にある編集アイコン（）をクリックします。

変数セット内の変数を追加および編集する方法の詳細については、変数の追加と編集 （48 ページ）を参照してください。

アクティブポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の導入 （92 ページ）を参照してください。

変数の管理

ライセンス：Protection

変数セット内の新規の変数セット ページ、または変数セットの編集ページで変数を管理します。すべての変数セットの変数ページでは、変数は [Customized Variables] ページ領域と [Default Variables] ページ領域に分かれています。

デフォルト変数は、ASA FirePOWER モジュールによって提供される変数です。デフォルト変数の値をカスタマイズすることができます。デフォルト変数の名前変更または削除はできません。また、デフォルト値を変更することもできません。

カスタマイズされた変数は、次のいずれかになります。

- カスタマイズされたデフォルト変数

デフォルト変数の値を編集すると、その変数は [Default Variables] 領域から [Customized Variables] 領域に移動します。デフォルト セットの変数値によってカスタム セットの変数のデフォルト値が決まるため、デフォルト セットのデフォルト変数をカスタマイズすると、他のすべてのセットの変数のデフォルト値が変更されます。

- ユーザ定義変数

独自の変数を追加および削除したり、異なる変数セット内の値をカスタマイズしたり、カスタマイズされた変数をそのデフォルト値にリセットしたりできます。ユーザ定義変数をリセットした場合、その変数は [Customized Variables] 領域に残ります。

次の表に、変数を作成または編集するために実行できるアクションを要約します。

表 *6*：変数の管理アクション（続き）

目的	操作
変数のページを表示する	変数セット ページで、[Add Variable Set] をクリックして新しい変数セットを作成するか、編集する変数セットの横にある編集アイコン（）をクリックします。
変数セットに名前を付け、オプションで説明を加える	[Name] および [Description] フィールドに、スペースや特殊文字を含む、英数字文字列を入力します。
変数を追加する	[Add] をクリックします。 詳細については、「変数の追加と編集 （48 ページ）」を参照してください。

変数を編集する	編集する変数の横にある編集アイコン（  ）をクリックします。 詳細については、「変数の追加と編集 （48 ページ）」を参照してください。
変更された変数をデフォルト値にリセットする	変更された変数の横にあるリセットアイコン（  ）をクリックします。影付きリセット アイコンは、現在の値がすでにデフォルト値であることを示します。
ユーザ定義のカスタマイズされた変数を削除する	変数セットの横にある削除アイコン（  ）をクリックします。変数の追加後に変数セットを保存した場合は、[Yes] をクリックして変数の削除を確認します。 デフォルト変数は削除できません。また、侵入ルールまたは他の変数によって使用されているユーザ定義変数は削除できません。
変数セットへの変更を保存する	変数セットがアクセス コントロール ポリシーで使用されている場合は [Store ASA FirePOWER Changes] をクリックしてから、[Yes] をクリックして変更を保存することを確認します。 デフォルト セットの現在の値によって他のすべてのセットのデフォルト値が決まるため、デフォルト セットの変数を変更またはリセットすると、デフォルト値がカスタマイズされていない他のセットの現在の値が変更されます。

変数セットの変数を表示する方法：

ステップ 1 [Configuration] > > [ASA FirePOWER Configuration] > > [Object Management] の順に選択します。

ステップ 2 [Variable Set] を選択します。

ステップ 3 変数セットを作成したり、既存のセットを編集したりするには、以下の手順に従います。

- 変数セットを作成するには、[Add Variable Set] をクリックします。
- 変数セットを作成するには、変数セットの横にある編集アイコン（  ）をクリックします。

ステップ 4 変数を作成したり、既存の変数を編集したりするには、以下の手順に従います。

- 変数を作成するには、[Add] をクリックします。
- 変数を編集するには、変数の横にある編集アイコン（  ）をクリックします。

変数セット内の変数を追加および編集する方法の詳細については、変数の追加と編集 （48 ページ）を参照してください。

変数の追加と編集

ライセンス：**Protection**

任意のカスタム セットで変数を変更できます。

カスタム標準テキスト ルール を作成する場合はさらに、独自のユーザ定義変数を作成して、トラフィックをより正確に反映したり、ショートカットとしてルール作成プロセスを単純化したりできます。たとえば、「緩衝地帯」（つまり DMZ）でのみトラフィックを検査するルールを作成する場合、公開されているサーバの IP アドレスが値にリストされる変数 $DMZ を作成できます。こうして、この地帯で作成された任意のルールで $DMZ 変数を使用できます。

変数セットに変数を追加すると、他のすべてのセットにもその変数が追加されます。以下に説明されている 1 つの例外を除き、変数はデフォルト値として他のセットに追加され、その後ユーザはそれをカスタマイズできます。

カスタム セットから変数を追加する場合は、設定値をデフォルト セットのカスタマイズ値として使用するかどうかを選択する必要があります。

- 設定値（たとえば、192.168.0.0/16）を使用する場合、変数は、デフォルト値 any を持つカスタマイズ値として設定値を使用するデフォルトセットに追加されます。デフォルトセットの現在の値によって他のセットのデフォルト値が決まるため、他のカスタムセットの初期のデフォルト値は設定値（この例では 192.168.0.0/16）になります。
- 設定値を使用しない場合、変数はデフォルト値 any のみを使用してデフォルトセットに追加され、こうして、他のカスタム セットの初期のデフォルト値は any になります。

詳細については、変数セットについて （43 ページ）を参照してください。

変数セット内の変数の追加は [New Variable] ページで行い、既存の変数の編集は [Edit Variable] ページで行います。これら 2 つのページは、既存の変数を編集する場合に、変数名または変数タイプを変更できないこと以外は、同じように使用します。

各ページは主に次の 3 つのウィンドウで構成されます。

- 既存のネットワークまたはポート変数、オブジェクト、およびネットワーク オブジェクト グループを含む、使用可能な項目
- 変数定義に包含するネットワークまたはポート
- 変数定義から除外するネットワークまたはポート

次の 2 種類の変数を作成または編集できます。

- ネットワーク変数は、ネットワーク トラフィックのホストの IP アドレスを指定します。ネットワーク変数の作業 （53 ページ）を参照してください。
- ポート 変数は、ネットワーク トラフィックの TCP または UDP ポートを指定するもので、いずれかのタイプを意味する値 any を指定することもできます。ポート変数の操作 （55 ページ）を参照してください。

ネットワーク変数タイプを追加するのか、ポート変数タイプを追加するのかを指定すると、ページが更新され、使用可能な項目がリストされます。リストの上部にある検索フィールドを使用してリストを制約できます。これは、入力するにつれて更新されます。

項目のリストから使用可能な項目を選択してドラッグし、包含または除外することができます。また、項目を選択し、[Include] または [Exclude] ボタンをクリックすることもできます。複数の項目を選択するには、Ctrl キーと Shift キーを使用します。包含または除外された項目の

リストの下にある設定フィールドを使用して、ネットワーク変数にリテラル IP アドレスおよびアドレス ブロック、およびポート変数にポートおよびポート範囲を指定できます。

ネットワーク変数の場合、包含または除外する項目のリストは、リテラル文字列や既存の変数、オブジェクト、およびネットワーク オブジェクト グループの任意の組み合わせで構成できます。

次の表に、変数を作成または編集するために実行できるアクションを要約します。

表 7: 変数の編集アクション（続き）

目的	操作
変数のページを表示する	変数セットのページで、[Add] をクリックして新しい変数を追加するか、既存の変数の横にある編集アイコン（  ）をクリックします。
変数に名前を付ける	[Name] フィールドに、下線文字（_）以外の特殊文字を含まない、大文字と小文字を区別した一意の英数字文字列を入力します。 変数名は大文字と小文字を区別することに注意してください。たとえば、var と Var はそれぞれ一意です。
ネットワーク変数またはポート変数を指定する	[Type] ドロップダウンリストから [Network] または [Port] を選択します。 ネットワーク変数およびポート変数の使用および設定方法の詳細については、ネットワーク変数の作業 （53 ページ）およびポート変数の操作 （55 ページ）を参照してください。
利用可能なネットワークのリストから選択できるように、個別のネットワーク オブジェクトを追加する	[Type] ドロップダウンリストから [Network] を選択し、追加アイコン（  ）をクリックします。オブジェクトマネージャを使用してネットワーク オブジェクトを追加する方法の詳細については、ネットワーク オブジェクトの操作 （26 ページ） を参照してください。
利用可能なポートのリストから選択できるように、個別のポート オブジェクトを追加する	[Type] ドロップダウンリストから [Port] を選択し、追加アイコン（）をクリックします。 任意のポート タイプを追加できますが、いずれかのタイプを意味する値 any を含め、TCP および UDP ポートだけが有効な変数値であり、使用可能なポートのリストにはこれらの値タイプを使用する変数のみが表示されます。オブジェクトマネージャを使用してポート オブジェクトを追加する方法の詳細については、ポート オブジェクトの操作 （33 ページ）を参照してください。
使用可能なポート項目またはネットワーク項目を名前で検索する	使用可能な項目のリストの上にある検索フィールドに名前を入力します。入力するに従ってページが更新され、一致する名前が表示されます。
名前の検索をクリアする	検索フィールドの上のリロード アイコン（  ）、または検索フィールド内のクリア アイコン（）をクリックします。

使用可能な項目を区別する	変数アイコン（）、ネットワーク オブジェクト アイコン（）、ポート アイコン（）、およびオブジェクト グループ アイコン（）の横にある項目を探します。 ポート グループではなく、ネットワーク グループだけが使用可能であることに注意してください。
変数定義に含める（または除外する）オブジェクトを選択する	使用可能なネットワークまたはポートのリストにあるオブジェクトをクリックします。複数のオブジェクトを選択するには、Ctrl キーと Shift キーを使用します。
含まれる（または除外される）ネットワークまたはポートのリストに、選択した項目を追加する	選択した項目をドラッグアンドドロップします。あるいは、[Include] または [Excluede] をクリックします。 使用可能な項目のリストから、ネットワークやポートの変数とオブジェクトを追加できます。また、ネットワーク オブジェクト グループを追加することもできます。
リテラル ネットワークまたはポートを含める（または除外する）ために、ネットワークまたはポートのリストに追加する	クリックして [literal Network] または [Port] フィールドからプロンプトを削除し、ネットワーク変数の場合はリテラル IP アドレスまたはアドレス ブロック、ポート変数の場合はリテラル ポートまたはポート範囲を入力して、[Add] をクリックします。 ドメイン名やリストを入力できないことに注意してください。複数の項目を追加するには、それぞれを個別に追加します。
値が any の変数を追加する	変数に名前を付け、変数タイプを選択してから、値を設定せずに [Store ASA FirePOWER Changes] をクリックします。
包含/除外リストから変数またはオブジェクトを削除する	変数の横にある削除アイコン（）をクリックします。
新規または変更された変数を保存する	[Store ASA FirePOWER Changes] をクリックします。カスタム セットから変数を追加している場合は、[Yes] をクリックすると設定値が他のセットのデフォルト値として使用され、[No] をクリックするとデフォルト値 any が使用されます。

変数を編集した後に、アクティブ ポリシーがオブジェクトを参照する場合、変更を有効にするには設定を再展開する必要があります。設定変更の導入 （92 ページ）を参照してください。

変数を作成または編集する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 [Variable Set] を選択します。

ステップ 3 変数セットを作成したり、既存のセットを編集したりするには、以下の手順に従います。

- 変数セットを作成するには、[Add Variable Set] をクリックします。

- 既存の変数セットを編集するには、変数セットの横にある編集アイコン（）をクリックします。

ステップ 4 新しい変数を作成したり、既存の変数を編集したりするには、以下の手順に従います。

- 新しい変数を作成するには、[Add] をクリックします。
- 既存の変数を編集するには、変数の横にある編集アイコン（）をクリックします。

ステップ 5 新しい変数を作成するには、以下の手順に従います。

- [Name] に一意の変数名を入力します。

英数字およびアンダースコア（_）文字を使用できます。

- ドロップダウンリストから、変数の [Type] として [Network] または [Port] を選択します。

ステップ 6 オプションで、使用可能なネットワークまたはポートのリストから、包含または除外項目リストに項目を移動します。

1 つ以上の項目を選択してから、ドラッグ アンド ドロップするか、[Include] または [Exclude] をクリックできます。複数の項目を選択するには、Ctrl キーと Shift キーを使用します。

ヒント ヒント：ネットワーク変数またはポート変数の包含リストと除外リストにあるアドレスやポートが重複している場合、除外されているアドレスまたはポートが優先されます。

ステップ 7 オプションで、1 つのリテラル値を入力し、[Add] をクリックします。

ネットワーク変数の場合、単一の IP アドレスまたはアドレス ブロックを入力できます。ポート変数の場合、単一ポートまたはポート範囲を追加できます。ポート範囲は上限値と下限値をハイフン（-）で区切ります。

複数のリテラル値を入力する場合は、必要に応じてこの手順を繰り返します。

ステップ 8 [Store ASA FirePOWER Changes] をクリックして変数を保存します。カスタム セットから新しい変数を追加する場合、次のオプションがあります。

- [Yes] をクリックすると、設定値を使用する変数がデフォルト セットのカスタマイズ値として追加され、結果として他のカスタム セットのデフォルト値として追加されます。
- [No] をクリックすると、変数はデフォルト セットのデフォルト値 any として追加され、結果として他のカスタム セットのデフォルト値として追加されます。

ステップ 9 変更を終えたら、変数セットを保存するために [Store ASA FirePOWER Changes] をクリックして、[Yes] をクリックします。

アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の導入（92 ページ）を参照してください。

ネットワーク変数の作業

ライセンス：Protection

ネットワーク変数で表される IP アドレスを、侵入ポリシーで有効になった侵入ルール、侵入ポリシー ルール抑制、動的ルール状態、および適応型プロファイルで使用することができます。ネットワーク変数はネットワーク オブジェクトやネットワーク オブジェクト グループとは異なります。ネットワーク変数は、侵入ポリシーや侵入ルールに固有のものですが、ネットワーク オブジェクトおよびグループは、アクセス コントロール ポリシー、ネットワーク変数、レポートなど、ASA FirePOWER モジュールのさまざまな場所で IP アドレスを表すために使用できます。詳細については、「ネットワーク オブジェクトの操作 （26 ページ）」を参照してください。

次の設定でネットワーク変数を使用して、ネットワーク上のホストの IP アドレスを指定できます。

- 侵入ルール

侵入ルールの [Source IPs] および [Destination IPs] 見出し フィールドを使用すると、パケット インスペクションを、特定の送信元または宛先 IP アドレスを持つパケットに制限することができます。

- 抑制

送信元または宛先の侵入ルール抑制の [Network] フィールドを使用すると、特定の 1 つの IP アドレスまたは IP アドレス範囲が侵入ルールやプリプロセッサをトリガーした場合の侵入イベント通知を抑制できます。侵入ポリシーごとの抑制の設定（385ページ）を参照してください。

- 動的ルール状態

送信元または宛先の動的ルール状態の [Network] フィールドを使用すると、指定時間内に発生した侵入ルールやプリプロセッサ ルールの一致数が多すぎる場合に、それを検出できます。動的ルール状態の追加 （388 ページ）を参照してください。

- 適応型プロファイル

適応型プロファイルの [Networks] フィールドは、パッシブ展開でのパケット フラグメントと TCP ストリームの再構築リアセンブリを改善させる必要があるネットワーク内のホストを特定します。ルールを使用した侵入ポリシーの調整 （355 ページ）を参照してください。

このセクションで示されるフィールドで変数を使用する場合、侵入ポリシーにリンクされた変数セットは、侵入ポリシーを使用するアクセス コントロール ポリシーで処理されるネットワーク トラフィックでの変数値を決定します。

次のネットワーク設定を任意に組み合わせて変数に追加できます。

- 使用可能なネットワーク リストから選択したネットワーク変数、ネットワーク オブジェクト、およびネットワーク オブジェクト グループの任意の組み合わせ

オブジェクト マネージャを使用して個別のネットワーク オブジェクトとグループ ネットワーク オブジェクトを作成する方法については、ネットワーク オブジェクトの操作 （26 ページ）を参照してください。

- [New Variable] または [Edit Variable] ページから追加した個々のネットワーク オブジェクト（独自の変数、他の既存の変数、今後の変数に追加可能）
- リテラルの単一 IP アドレスまたはアドレス ブロック

それぞれを個別に追加することにより、複数のリテラル IP アドレスとアドレス ブロックをリストできます。IPv4 および IPv6 アドレスとアドレス ブロックを単独で、または任意に組み合わせてリストできます。IPv6 アドレスを指定するときには、RFC 4291 で定義された任意のアドレス指定規則を使用できます。

追加する変数での包含ネットワークのデフォルト値は any で、これは任意の IPv4 または IPv6 アドレスを示します。除外ネットワークのデフォルト値は none で、これは「ネットワークなし」を示します。また、リテラル値の中でアドレス :: を指定すると、包含ネットワーク リストで任意の IPv6 アドレスを指定でき、除外リストでは IPv6 アドレスなしを指定できます。

除外リストにネットワークを追加すると、指定されたアドレスおよびアドレス ブロックが拒否されます。つまり、除外された IP アドレスやアドレス ブロックを除き、任意の IP アドレスに一致させることができます。

たとえば、リテラル アドレス 192.168.1.1 を除外すると 192.168.1.1 以外の任意の IP アドレスが指定され、2001:db8:ca2e::fa4c を除外すると 2001:db8:ca2e::fa4c 以外の任意の IP アドレスが指定されます。

リテラル ネットワークまたは使用可能なネットワークを任意に組み合わせて、除外で使用できます。たとえば、リテラル値 192.168.1.1 および 192.168.1.5 を除外すると、192.168.1.1 と 192.168.1.5 以外の任意の IP アドレスが含まれます。つまり、システムはこの構文を「192.168.1.1 でも、192.168.1.5 でもない」と解釈し、大カッコ内に列挙されたものを除くすべての IP アドレスに一致させます。

ネットワーク変数を追加または編集するときには、次の点に注意してください。

- 論理的に言って、値 any を除外することはできません。any を除外すると「アドレスなし」を意味することになります。たとえば、除外ネットワーク リストに、値 any を持つ変数を追加することはできません。
- ネットワーク変数は、指定された侵入ルールおよび侵入ポリシー機能に関するトラフィックを識別します。プリプロセッサ ルールは、侵入ルールで使われているネットワーク変数で定義されたホストとは無関係に、イベントをトリガーできることに注意してください。
- 除外される値は、包含される値のサブセットに解決される必要があります。たとえば、アドレス ブロック 192.168.5.0/24 を包含し、192.168.6.0/24 を除外することはできません。エラー メッセージが表示され、問題となっている変数が明示されます。包含される値の範囲外となる値を除外した場合は、変数セットを保存できません。

ネットワーク変数の追加および編集の詳細については、変数の追加と編集 （48 ページ）を参照してください。

ポート変数の操作

ライセンス：Protection

ポート変数は、侵入ポリシーで有効になった侵入ルールの [Source Port] および [Destination Port] 見出し フィールドで使用できる TCP ポートと UDP ポートを表します。ポート変数とポート オブジェクトおよびポート オブジェクト グループとの相違点は、ポート変数が侵入ルール固有のものであることです。TCP および UDP 以外のプロトコル用にポート オブジェクトを作成して、ポート変数とアクセス コントロール ポリシーでポート オブジェクトを使用できます。詳細については、「ポート オブジェクトの操作 （33 ページ）」を参照してください。

侵入ルールの [Source Port] および [Destination Port] 見出し フィールドでポート変数を使用すると、パケット インスペクションを、特定の送信元または宛先 TCP/UDP ポートを持つパケットに制限することができます。

これらのフィールドで変数を使用した場合、アクセス コントロール ルールまたはポリシーに関連付けられた侵入ポリシーにリンクされる変数セットは、システムによりアクセス コントロール ポリシーが適用されるネットワーク トラフィックでのこれらの変数の値を決定します。

次のポート設定を任意に組み合わせて変数に追加できます。

- 使用可能なポート リストから選択したポート変数およびポート オブジェクトの任意の組み合わせ

使用可能なポート リストには、ポート オブジェクト グループが表示されず、したがってこれらを変数に追加できないことに注意してください。オブジェクト マネージャを使用してポート オブジェクトを作成する方法については、ポート オブジェクトの操作 （33 ページ）を参照してください。

- [New Variable] または [Edit Variable] ページから追加した個々のポート オブジェクト（独自の変数、他の既存の変数、今後の変数に追加可能）

有効な変数値は TCP および UDP ポートのみです（どちらのタイプでも値 any を含む）。新しい変数のページまたは変数の編集ページを使用して、有効な変数値ではない有効なポート オブジェクトを追加した場合、オブジェクトはシステムに追加されますが、使用可能なオブジェクト リストには表示されません。オブジェクト マネージャを使用して、変数で使われるポート オブジェクトを編集する場合、有効な変数値にのみ値を変更できます。

- 単一のリテラル ポート値とポート範囲

ポート範囲はダッシュ（-）を使って区切る必要があります。下位互換性のために、コロンで指定されるポート範囲もサポートされていますが、作成するポート変数ではコロンを使用できません。

複数のリテラル ポートの値および範囲をリストするには、それぞれを個別に追加して任意に組み合わることができます。

ポート変数を追加または編集するときには、次の点に注意してください。

- 追加する変数での包含ポートのデフォルト値は any で、これは任意のポートまたはポート範囲を示します。除外ポートのデフォルト値は none で、これは「ポートなし」を示します。

ヒント　値 any を持つ変数を作成するには、特定の値を追加せずに変数に名前を付けて保存します。

- 論理的に言って、値 any を除外することはできません。any を除外すると「ポートなし」を意味することになります。たとえば、値 any を持つ変数を除外ポートリストに追加した場合、変数セットを保存することはできません。
- 除外リストにポートを追加すると、指定されたポートおよびポート範囲が拒否されます。つまり、除外されたポートまたはポート範囲を除き、任意のポートに一致させることができます。
- 除外される値は、包含される値のサブセットに解決される必要があります。たとえば、ポート範囲 10 から 50 を包含し、ポート 60 を除外することはできません。エラーメッセージが表示され、問題となっている変数が明示されます。包含される値の範囲外となる値を除外した場合は、変数セットを保存できません。

.

ポート変数の追加および編集の詳細については、変数の追加と編集 （48 ページ）を参照してください。

変数のリセット

ライセンス：Protection

変数セットの新しい変数ページまたは変数の編集ページで、変数をデフォルト値にリセットできます。次の表に、変数をリセットするときの基本原則を要約します。

表 *8:* 変数のリセット値

リセットする変数のタイプ	それが含まれるセット タイプ	リセット後の値
デフォルト	デフォルト	ルール更新値
ユーザ定義	デフォルト	任意
デフォルトまたはユーザ定義	カスタム	現在のデフォルト セット値（変更/未変更にかかわらず）

カスタム セットの変数をリセットすると、単にデフォルト セット内のその変数の現在値にリセットされます。

逆に、デフォルト セットの変数の値をリセットまたは変更すると、すべてのカスタム セット内のその変数のデフォルト値が常に更新されます。リセットアイコンがグレー表示され、その

変数をリセットできないことを示している場合、そのセットでは変数のカスタマイズ値が存在しないことを意味します。カスタム セット内の変数の値をすでにカスタマイズした場合を除き、デフォルト セットの変数を変更すると、変数セットがリンクされた侵入ポリシーで使われている値が更新されます。

（注） デフォルト セット内の変数を変更する際は、リンクされたカスタム セットの変数を使用している侵入ポリシーが、その変更によってどのような影響を受けるかを評価することをお勧めします（特に、カスタム セット内の変数値をまだカスタマイズしていない場合）。

カスタマイズされた値とリセット値が同じである場合は、次のいずれかを示しています。

- カスタム セットまたはデフォルト セットの中で、値 any を持つ変数を追加した
- カスタムセットの中で、明示的な値を持つ変数を追加し、設定した値をデフォルト値として使用することを選択した

侵入ポリシーへの変数セットのリンク

ライセンス：Control

デフォルトでは、ASA FirePOWER モジュールは、アクセス コントロール ポリシーで使用されるすべての侵入ポリシーにデフォルト変数セットをリンクします。侵入ポリシーを使用するアクセス コントロール ポリシーを展開すると、その侵入ポリシー内で有効になった侵入ルールは、リンクされた変数セットの変数値を使用します。

アクセス コントロール ポリシー内の侵入ポリシーで使用されるカスタム変数セットを変更すると、[Access Control] ページに、そのポリシーのステータスが「失効」と表示されます。変数セットの変更を実装するには、設定を展開する必要があります。デフォルト セットを変更すると、侵入ポリシーを使用するすべてのアクセス コントロール ポリシーのステータスが「失効」と表示され、変更を実装するには設定を再展開する必要があります。

情報については、次の各項を参照してください。

- デフォルト セット以外の変数セットをアクセス コントロール ルールにリンクさせるには、「侵入防御を実行するアクセス コントロール ルールの設定」（144 ページ）の手順を参照してください。 侵入防御を実行するアクセス コントロール ルールの設定 （175 ページ）
- デフォルト セット以外の変数セットをアクセス コントロール ポリシーのデフォルト アクションにリンクさせるには、デフォルトの処理の設定およびネットワーク トラフィックのインスペクション （83 ページ）を参照してください。
- 変数セットを侵入ポリシーにリンクさせるポリシーを含むアクセス コントロール ポリシーを展開するには、設定変更の導入 （92 ページ）を参照してください。

拡張変数について

ライセンス：Protection

拡張変数を使用すると、他の方法ではモジュールインターフェイスで設定できない機能を設定することができます。現在、ASA FirePOWER モジュールには 2 つの拡張変数だけがあり、USER_CONF 拡張変数のみ編集できます。

USER_CONF

USER_CONF は、モジュールインターフェイスで通常設定できない 1 つ以上の機能を設定するための汎用ツールです。

⚠

注意 機能の説明またはサポート担当の指示に従う場合を除き、拡張変数 USER_CONF を使用して侵入ポリシー機能を設定しないでください。競合または重複する設定が存在すると、システムが停止します。

USER_CONF を編集するときには、1 行に合計 4096 文字まで入力できます。行は自動的に折り返します。変数の最大長 8192 文字、またはディスク スペースなどの物理制限に達するまで、任意の数の有効な指示または行数を含めることができます。コマンドディレクティブでは、完全な引数の後にバックスラッシュ（\）行連結文字を使用します。

USER_CONF をリセットすると、空になります。

シンクホール オブジェクトの操作

ライセンス：Protection

シンクホール オブジェクトは、シンクホール内のすべてのドメイン名にルーティング不可アドレスを付与する DNS サーバ、またはサーバに解決しない IP アドレスのいずれかを表します。DNS ポリシー ルール内のシンクホール オブジェクトを参照して、一致するトラフィックをシンクホールにリダイレクトできます。このオブジェクトには IPv4 アドレスと IPv6 アドレスの両方を割り当てる必要があります。

使用中のシンクホール オブジェクトは削除できません。さらに、DNS ポリシーで使用されるシンクホール オブジェクトを編集した後に、変更を有効にするには、設定を再展開する必要があります。設定変更の導入 （92 ページ）を参照してください。

シンクホール オブジェクトを作成する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 オブジェクト タイプのリストから [Sinkhole] を選択します。

ステップ 3 [Add Sinkhole] をクリックします。

ステップ 4 [Name] を入力します。

ステップ 5 シンクホールの [IPv4 アドレス（IPv4 Address）] と [IPv6 アドレス（IPv6 Address）] を入力します。

ステップ 6 次の選択肢があります。

- シンクホール サーバにトラフィックをリダイレクトする場合は、[Log Connections to Sinkhole] を選択します。
- 非解決 IP アドレスにトラフィックをリダイレクトする場合は、[Block and Log Connections to Sinkhole] を選択します。

ステップ 7 [Indication of Compromise (IoC)] タイプをシンクホールに割り当てる場合は、[Type] ドロップダウンからいずれかを選択します。

ステップ 8 [Store ASA FirePOWER Changes] をクリックします。

ファイル リストの操作

ライセンス：Malware

ネットワークベースの高度なマルウェア防御（AMP）を使用していて、Collective Security Intelligence クラウドによってファイルの性質が誤って識別される場合は、SHA256 ハッシュ値を使用してそのファイルをファイル リストに追加し、以降のファイル検出精度を向上できます。ファイル リストのタイプに応じて、次の操作を実行できます。

- クラウドがクリーンの性質を割り当てた場合と同じ方法でファイルを扱うには、クリーン リストにファイルを追加します。
- クラウドがマルウェアの性質を割り当てた場合と同じ方法でファイルを扱うには、カスタム検出リストにファイルを追加します。

これらのファイルのブロッキング動作は手動で指定されるため、そのファイルがクラウドによってマルウェアと識別されるような場合でも、システムはマルウェア クラウド ルックアップを実行しません。ファイルの SHA 値を計算するには、マルウェア クラウド ルックアップ アクションとブロック マルウェア アクションのいずれか、および一致するファイル タイプを使用して、ファイル ポリシー内のルールを設定する必要があります。詳細については、「ファイル ルールの操作 （461 ページ）」を参照してください。

システムのクリーン リストとカスタム検出リストは、デフォルトですべてのファイル ポリシーに含まれています。ポリシーごとに、いずれかまたは両方のリストを使用しないことを選択できます。

注意 実際にマルウェアであるファイルをこのリストに含めないでください。クラウドによってファイルのマルウェアの性質が割り当てられている場合、またはファイルをカスタム検出リストに追加した場合でも、システムはそれらのファイルをブロックしません。

各ファイル リストには、一意の SHA-256 値を最大 10000 個まで含めることができます。ファイルをファイル リストに追加するには、次の操作を実行できます。

- ファイルをアップロードする。これにより、システムはそのファイルの SHA256 値を計算して追加できます。
- ファイルの SHA-256 値を直接入力する。
- 複数の SHA-256 値を含むコンマ区切り値（CSV）ソース ファイルを作成してアップロードする。重複しないすべての SHA-256 値がこのファイル リストに追加されます。

ファイル リストにファイルを追加したり、ファイル リスト内の SHA-256 値を編集したり、ファイル リストから SHA-256 値を削除したりする場合、変更を有効にするには、設定を再展開する必要があります。設定変更の導入 （92 ページ）を参照してください。

ファイル リストに複数の SHA-256 値をアップロードする

ライセンス：Malware

SHA-256 値のリストと説明を含むコンマ区切り値（CSV）ソース ファイルをアップロードすることで、複数の SHA-256 値をファイル リストに追加できます。システムはその内容を検証し、有効な SHA-256 値をファイル リストに入れます。

ソース ファイルは、ファイル名拡張子 .csv の単純なテキスト ファイルである必要があります。見出しはポンド記号（#）で始まる必要があります。これはコメントとして処理され、アップロードされません。各エントリには、1 つの SHA-256 値の後に（最大 256 個の英文字または特殊文字からなる）説明が含まれる必要があり、LF または CR+LF 改行文字で終わる必要があります。システムはエントリ内のこれ以外の情報をすべて無視します。

次の点に注意してください。

- ファイル リストからソース ファイルを削除すると、それに関連付けられているすべての SHA-256 ハッシュもファイル リストから削除されます。
- ソース ファイルのアップロードに成功した結果、10000 個を超える個別の SHA-256 値がファイル リストに含まれる場合は、複数のファイルをファイル リストにアップロードすることはできません。
- システムは、アップロード時に 256 文字を超える説明を最初の 256 文字で切り捨てます。説明にコンマを含める場合は、エスケープ文字（\）を使用する必要があります。説明が含まれていない場合、代わりにソース ファイル名が使用されます。
- すでにファイル リストに存在する SHA-256 値を含むソース ファイルをアップロードした場合、新たにアップロードした値によって既存の SHA-256 値が変更されることはありません。SHA-256 値に関連するキャプチャ済みファイル、ファイル イベント、またはマルウェア イベントを表示するとき、個々の SHA-256 値から脅威名または説明が得られます。
- システムはソース ファイル内の無効な SHA-256 値をアップロードしません。
- アップロードされた複数のソース ファイルに同じ SHA-256 値のエントリが含まれている場合は、最新の値が使用されます。

- 1 つのソース ファイル内に同じ SHA-256 値のエントリが複数含まれる場合、システムは最後のものを使用します。
- オブジェクト マネージャ内でソース ファイルを直接編集することはできません。変更を行うには、最初にソースファイルを直接変更し、システム上のコピーを削除した後、変更済みソース ファイルをアップロードする必要があります。詳細については、「ファイル リストからソース ファイルをダウンロードする （63 ページ）」を参照してください。

ソース ファイルをファイル リストにアップロードする方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 [File List] をクリックします。

ステップ 3 ソース ファイルからの値の追加先となるファイル リストの横にある編集アイコン（  ）をクリックします。

ステップ 4 [Add by] フィールドから [List of SHAs] を選択します。

ステップ 5 オプションで、[Description] フィールドにソース ファイルの説明を入力します。

説明を入力しない場合、システムはファイル名を使用します。

ステップ 6 [Browse] をクリックしてソース ファイルを参照してから、[Upload and Add List] をクリックしてリストを追加します。

ソース ファイルがファイル リストに追加されます。[SHA-256] カラムには、ファイルに含まれる SHA-256 値の数が表示されます。

ステップ 7 [Store ASA FirePOWER Changes] をクリックします。

アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の導入 （92 ページ）を参照してください。

設定が展開されると、システムはファイル リスト内のファイルに対してマルウェア クラウド ルックアップを実行しなくなります。

個別のファイルをファイル リストにアップロードする

ライセンス：**Malware**

ファイル リストに追加するファイルのコピーがある場合、分析用にファイルをシステムにアップロードできます。システムはファイルの SHA-256 値を計算して、ファイルをリストに追加します。SHA-256 を計算する場合、ファイル サイズは制限されません。

システムに SHA-256 値を計算させることによってファイルを追加するには、次の手順を実行します。

ステップ 1 オブジェクト マネージャの [File List] ページで、ファイルの追加場所となるクリーン リストまたはカスタム検出リストの横にある編集アイコン（  ）をクリックします。

ステップ 2 [Add by] フィールドから [Calculate SHA] を選択します。

ステップ 3 オプションで、[Description] フィールドにファイルの説明を入力します。

説明を入力しない場合、アップロード時にファイル名が説明として使用されます。

ステップ 4 [Browse] をクリックしてソース ファイルを参照してから、[Calculate and Add SHA] をクリックしてリストを追加します。

ステップ 5 [Store ASA FirePOWER Changes] をクリックします。

アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の導入（92 ページ）を参照してください。

設定が展開されると、システムはファイル リスト内のファイルに対してマルウェア クラウド ルックアップを実行しなくなります。

ファイル リストに SHA-256 値を追加する

ライセンス：Malware

ファイルの SHA-256 値を送信して、その値をファイル リストに追加できます。重複する SHA-256 値は追加できません。

ファイルの SHA-256 値を手動で入力してファイルを追加するには、次の手順を実行します。

ステップ 1 オブジェクト マネージャの [File List] ページで、ファイルの追加先となるクリーン リストまたはカスタム検出リストの横にある編集アイコン（  ）をクリックします。

ステップ 2 [Add by] フィールドから [Enter SHA Value] を選択します。

ステップ 3 [Description] フィールドにソース ファイルの説明を入力します。

ステップ 4 ファイルの SHA-256 値全体を入力するか、貼り付けます。システムでは値の部分的な一致はサポートされません。

ステップ 5 ファイルを追加するには、[Add] をクリックします。

ステップ 6 [Store ASA FirePOWER Changes] をクリックします。

アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の導入（92 ページ）を参照してください。

設定の展開後には、システムはファイル リスト内のファイルに対してマルウェア クラウド ルックアップを実行しなくなります。

ファイル リスト上のファイルの変更

ライセンス：**Malware**

ファイル リストの個々の SHA-256 値を編集または削除できます。オブジェクト マネージャ内でソース ファイルを直接編集できないことに注意してください。変更を行うには、最初にソース ファイルを直接変更し、システム上のコピーを削除した後、変更済みソース ファイルをアップロードする必要があります。詳細については、「ファイル リストからソース ファイルをダウンロードする （63 ページ）」を参照してください。ファイル リスト上のファイルを編集する方法：

ステップ 1 オブジェクト マネージャの [File List] ページで、変更するファイルがあるクリーン リストまたはカスタム検出リストの横にある編集アイコン（  ）をクリックします。

ステップ 2 編集する SHA-256 値の横にある編集アイコン（  ）をクリックします。

ヒント リストからファイルを削除することもできます。削除するファイルの横にある削除アイコン（  ）をクリックします。

ステップ 3 [SHA-256] 値または [Description] を更新します。

ステップ 4 [**Save**] をクリックします。

ステップ 5 [Store ASA FirePOWER Changes] をクリックします。

アクティブ ポリシーがオブジェクトを参照する場合は、設定変更を展開します。設定変更の導入 （92 ページ）を参照してください。

設定の展開後には、システムはファイル リスト内のファイルに対してマルウェア クラウド ルックアップを実行しなくなります。

ファイル リストからソース ファイルをダウンロードする

ライセンス：**Malware**

ファイル リスト上の既存のソース ファイル エントリを表示、ダウンロード、または削除できます。いったんアップロードされたソース ファイルを編集することはできません。まずファイル リストからソース ファイルを削除し、更新後のファイルをアップロードする必要があります。ソース ファイルをアップロードする方法については、ファイル リストに複数の SHA-256 値をアップロードする （60 ページ）を参照してください。

ソース ファイルに関連付けられたエントリ数とは、個別の SHA-256 値の数です。ファイル リストからソース ファイルを削除すると、ファイル リストに含まれる SHA-256 エントリの合計数は、ソース ファイル内の有効なエントリ数だけ減少します。

ソース ファイルをダウンロードする方法：

ステップ 1 オブジェクト マネージャの [File List] ページで、ソースファイルのダウンロード対象となるクリーン リストまたはカスタム検出リストの横にある編集アイコン（  ）をクリックします。

ステップ 2 ダウンロードするソース ファイルの横にある表示アイコン（  ）をクリックします。

ステップ 3 [Download SHA List] をクリックし、プロンプトに従ってソース ファイルを保存します。

ステップ 4 [閉じる（**Close**）] をクリックします。

セキュリティ ゾーンの操作

ライセンス：任意

サポートされるデバイス：任意

セキュリティ ゾーンは、1 つ以上の ASA インターフェイスからなるグループです。これを使用すると、さまざまなポリシーと設定でトラフィック フローを管理および分類できます。単一のデバイス上に複数のゾーンを設定できます。これにより、ネットワークを複数セグメントに分割でき、システムによりさまざまなポリシーを適用できるようになります。トラフィックをセキュリティ ゾーンと照合するには、少なくとも 1 つのインターフェイスをそのセキュリティ ゾーンに割り当てる必要があり、各インターフェイスは 1 つのゾーンのみに属することができます。

セキュリティ ゾーンを使用してインターフェイスをグループ化することに加え、ゾーンはアクセス コントロール ポリシーでも使用できます。たとえば、特定の送信元または宛先ゾーンだけに適用されるアクセス コントロール ルールを作成することもできます。

オブジェクト マネージャの [Security Zones] ページには、ASA FirePOWER モジュールで設定されたゾーンが一覧表示されます。

使用中のセキュリティ ゾーンは削除できません。ゾーンでのインターフェイスの追加または削除の後に、アクティブ ポリシーがオブジェクトを参照する場合は、変更を有効にするために設定を展開する必要があります。設定変更の導入 （92 ページ）を参照してください。

セキュリティ ゾーンを作成する手順：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 [Security Zones] を選択します。

ステップ 3 [Add Security Zone] をクリックします。

ステップ 4 [Name] にゾーンの名前を入力します。中カッコ（{}）とポンド記号（#）を除く、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5 [Type] で、ゾーンのインターフェイスのタイプを選択します。

セキュリティ ゾーンの作成後に、タイプを変更することはできません。

ステップ 6 1 つ以上のインターフェイスを選択します。

複数のオブジェクトを選択するには、Ctrl キーと Shift キーを使用します。インターフェイスをまだ設定していない場合は、空のゾーンを作成し、後でそこにインターフェイスを追加できます。ステップ 9 に進みます。

ステップ 7 [Add] をクリックします。

ステップ 8 他のデバイスのインターフェイスをゾーンに追加するには、手順 6 から 8 までを繰り返します。

ステップ 9 [Store ASA FirePOWER Changes] をクリックします。

暗号スイート リストの操作

ライセンス：任意

暗号スイート リストは複数の暗号スイートからなるオブジェクトです。定義済みの各暗号スイートの値は、SSL または TLS 暗号化セッションのネゴシエーションに使用される暗号スイートを表しています。暗号スイートおよび暗号スイート リストを SSL ルールで使用すると、クライアントとサーバが暗号スイートを使って SSL セッションをネゴシエートしたかどうかに基づいて暗号化トラフィックを制御できます。SSL ルールに暗号スイート リストを追加すると、リスト内のいずれかの暗号スイートでネゴシエートされた SSL セッションがルールに一致します。

（注） ASDM インターフェイスでは暗号スイート リストと同じ場所で暗号スイートを使用できますが、暗号スイートを追加、変更、削除することはできません。

使用中の暗号スイート リストは削除できません。さらに、暗号スイート リストを編集した後に、アクティブ ポリシーがオブジェクトを参照する場合、変更を有効にするには設定を再展開する必要があります。設定変更の導入 （92 ページ）を参照してください。

暗号スイート リストを作成する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 [Cipher Suite List] を選択します。

ステップ 3 [Add Cipher Suites] をクリックします。

ステップ 4 [Name] に、暗号スイート リストの名前を入力します。縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5 1 つ以上の暗号スイートを選択して、[Add] をクリックします。

- Shift および Ctrl を使用して複数の暗号スイートを選択するか、右クリックして [Select All] を選択します。
- 含める既存の暗号スイートを検索するには、フィルタ フィールド（🔍）を使用します。このフィールドは入力に従って更新され、一致する項目が表示されます。検索文字列をクリアするには、検索フィー

ルドの上にあるリロードアイコン（）をクリックするか、検索フィールド内のクリアアイコン（）をクリックします。

ステップ 6 [Store ASA FirePOWER Changes] をクリックします。

識別名オブジェクトの操作

ライセンス：任意

各識別名オブジェクトは、公開鍵証明書のサブジェクトまたは発行元の識別名リストを表します。SSL ルールで識別名オブジェクトとグループ（オブジェクトのグループ化 （24 ページ）を参照）を使用すると、サブジェクトまたは発行元として識別名を含むサーバ証明書を使ってクライアントとサーバが SSL セッションをネゴシエートしたかどうかに基づき、暗号化トラフィックを制御できます。

識別名オブジェクトには、共通名属性（CN）を含めることができます。「CN=」を含まない共通名を追加すると、オブジェクトを保存する前に「CN=」が名前の前に追加されます。

さらに、次の表にリストされている、コンマで区切られた属性を含む識別名を追加することもできます。

表 *9:* 識別名の属性

属性	説明	使用可能な値
C	国番号	2 つの英字
CN	共通名	最大 64 文字の英数字、バックスラッシュ（/）、ハイフン（-）、引用符（"）、アスタリスク（*）、スペース文字
O	組織	
OU	組織単位	

ワイルドカードとして 1 つ以上のアスタリスク（*）を属性に定義できます。共通名属性では、ドメイン名ラベルごとに 1 つ以上のアスタリスクを定義できます。ワイルドカードはそのラベル内でのみ照合されますが、ワイルドカードを使用して複数のラベルを定義できます。例については、以下の表を参照してください。

表 *10 :* 共通名属性のワイルドカードの例

属性	一致する	一致しない
CN=”*ample.com”	example.com	mail.example.com example.text.com ampleexam.com
CN=”exam*.com”	example.com	mail.example.com example.text.com ampleexam.com
CN=”*xamp*.com”	example.com	mail.example.com example.text.com ampleexam.com
CN=”*.example.com”	mail.example.com	mail.example.com example.text.com ampleexam.com
CN=”*.com”	example.com ampleexam.com	mail.example.com example.text.com
CN=”*.*.com”	mail.example.com example.text.com	example.com ampleexam.com

使用中の識別名オブジェクトは削除できません。さらに、識別名オブジェクトを編集した後に、アクティブポリシーがオブジェクトを参照する場合、変更を有効にするには設定を展開する必要があります。設定変更の導入 （92 ページ）を参照してください。

識別名オブジェクトを作成する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 [Distinguished Name] の下で、[Individual Objects] を選択します。

ステップ 3 [Add Distinguished Name] をクリックします。

ステップ 4 [Name] に、識別名オブジェクトの名前を入力します。縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5 [DN] フィールドに、識別名または共通名の値を入力します。次の選択肢があります。

- 識別名を追加する場合は、[Distinguished Name Attributes] テーブルにリストされている、コンマで区切られた属性を含める必要があります。
- 共通名を追加する場合は、複数のラベルとワイルドカードを含めることができます。

ステップ 6 [Store ASA FirePOWER Changes] をクリックします。

PKI オブジェクトの操作

ライセンス：任意

PKI オブジェクトは、SSL インスペクション展開をサポートするために必要な公開鍵証明書、およびペアになった秘密鍵を表します。内部 CA オブジェクトおよび信頼できる CA オブジェクトは、認証局（CA）証明書で構成されます。また、内部 CA オブジェクトには、証明書とペアになった秘密鍵も含まれます。内部証明書オブジェクトおよび外部証明書オブジェクトは、サーバ証明書で構成されます。また、内部証明書オブジェクトには、証明書とペアになった秘密鍵も含まれます。SSL のルールでこれらのオブジェクトを使用すると、次のものを復号化できます。

- 発信トラフィック：内部 CA オブジェクトを使用してサーバ証明書を再署名することで復号化します
- 受信トラフィック：内部証明書オブジェクトにある既知の秘密鍵を使用して復号化します

さらに、SSL ルールを作成して、次のものを使って暗号化されたトラフィックを照合することができます。

- 外部証明書オブジェクト内の証明書
- 信頼できる CA オブジェクトの CA によって署名された証明書、または信頼できる CA チェーン内で署名された証明書

証明書とキーの情報を手動で入力し、その情報を含むファイルをアップロードします。場合によっては、新しい CA 証明書や秘密キーを生成することができます。

オブジェクト マネージャで PKI オブジェクトのリストを表示すると、証明書のサブジェクト識別名がオブジェクト値として表示されます。証明書の完全なサブジェクト識別名を表示するには、値の上にポインタを移動してください。その他の証明書の詳細を表示するには、PKI オブジェクトを編集します。

（注） ASA FirePOWER モジュールは、内部 CA オブジェクトと内部証明書オブジェクトに保存されるすべての秘密キーを、ランダムに生成されたキーを使用して暗号化してから保存します。パスワード保護されている秘密キーをアップロードすると、アプライアンスはユーザ提供のパスワードを使用して秘密キーを復号化し、ランダムに生成されたキーを使用して再暗号化してから保存します。

内部認証局オブジェクトの操作

ライセンス：任意

設定されたそれぞれの内部認証局（CA）オブジェクトは、組織で制御されるCAのCA公開鍵証明書を表します。このオブジェクトは、オブジェクト名、CA証明書、およびペアになった秘密鍵からなります。SSLルールで内部CAオブジェクトとグループ（オブジェクトのグループ化 （24 ページ）を参照）を使用すると、内部CAでサーバ証明書を再署名することで、発信される暗号化トラフィックを復号化できます。

（注） [Decrypt - Resign] SSLルールで内部CAオブジェクトを参照する場合、ルールが暗号化セッションに一致すると、SSLハンドシェイクのネゴシエート中は証明書を信頼できないという警告がユーザのブラウザに表示されることがあります。これを回避するには、信頼できるルート証明書のクライアントまたはドメイン リストに内部CAオブジェクト証明書を追加します。

次の方法で内部CAオブジェクトを作成できます。

- 既存のRSAベースまたは楕円曲線ベースのCA証明書と秘密キーをインポートする
- 新しいRSAベースの自己署名CA証明書と秘密キーを生成する
- RSAベースの未署名のCA証明書と秘密キーを生成する。内部CAオブジェクトを使用する前に、証明書に署名するために証明書署名要求（CSR）を別のCAに送信する必要があります。

署名付き証明書を含む内部CAオブジェクトを作成した後で、CA証明書と秘密鍵をダウンロードできるようになります。システムは、ダウンロードされた証明書と秘密キーをユーザ提供のパスワードで暗号化します。

システム生成の場合でも、ユーザ作成の場合でも、内部CAオブジェクトの名前は変更できますが、オブジェクトの他のプロパティは変更できません。

使用中の内部CAオブジェクトは削除できません。さらに、内部CAオブジェクトを編集した後に、アクティブポリシーがオブジェクトを参照する場合、変更を有効にするには設定を展開する必要があります。設定変更の導入 （92 ページ）を参照してください。

CA証明書および秘密キーのインポート

ライセンス：任意

X.509 v3 CA証明書と秘密キーをインポートすることによって、内部CAオブジェクトを設定できます。サポートされる次のいずれかの形式でエンコードされたファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

秘密キーファイルがパスワード保護されている場合は、復号化パスワードを提供できます。証明書とキーが PEM 形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

適切な証明書またはキーの情報を含んでいる、相互にペアになっているファイルのみをアップロードできます。システムはオブジェクトを保存する前にペアを検証します。

（注） ルールに [Decrypt - Resign] アクションを設定すると、そのルールでは、設定されているすべてのルール条件に加えて、参照される内部 CA 証明書の暗号化アルゴリズムのタイプに基づいてトラフィックが照合されます。たとえば、楕円曲線ベースのアルゴリズムで暗号化された発信トラフィックを復号化するには、楕円曲線ベースの CA 証明書をアップロードする必要があります。詳細については、「復号化アクション：さらに検査するためにトラフィックを復号化（253 ページ）」を参照してください。

内部 CA 証明書と秘密鍵をインポートする方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 [PKI] で、[Internal CAs] を選択します。

ステップ 3 [Import CA] をクリックします。

ステップ 4 [Name] に、内部 CA オブジェクトの名前を入力します。縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5 [Certificate Data] フィールドの上部にある [Browse] をクリックして、DER または PEM でエンコードされた X.509 v3 CA 証明書ファイルをアップロードします。

ステップ 6 [Key] フィールドの上部にある [Browse] をクリックして、DER または PEM でエンコードされたペアの秘密キー ファイルをアップロードします。

ステップ 7 アップロード ファイルがパスワード保護されている場合は、[Encrypted, and the password is:] チェック ボックスをオンにして、パスワードを入力します。

ステップ 8 [Store ASA FirePOWER Changes] をクリックします。

内部 CA オブジェクトが追加されます。

新しい CA 証明書と秘密キーの生成

ライセンス：任意

識別情報を提供することで、RSA ベースの自己署名 CA 証明書と秘密キーを生成するように内部 CA オブジェクトを設定できます。次の表に、証明書を生成するために提供する識別情報について説明します。

表 *11* : 生成される内部 *CA* の属性

フィールド	使用可能な値	必須
国名（Country Name）（2 文字コード）	2 つの英字	2 つの英字
州または地域、都道府県（State or Province）	最大 64 文字の英数字、バックスラッシュ（/）、ハイフン（-）、引用符（"）、アスタリスク（*）、ピリオド（.）、スペース文字	いいえ
市区町村（Locality or City）		
組織（Organization）		
組織単位（Organizational Unit）		
共通名（Common Name）		

生成される CA 証明書の有効期間は 10 年です。[Valid From] の日付は生成の一週間前です。

自己署名 CA 証明書を生成するには、次の手順を実行します。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 [PKI] で、[Internal CAs] を選択します。

ステップ 3 [Generate CA] をクリックします。

ステップ 4 [Name] に、内部 CA オブジェクトの名前を入力します。縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5 表「生成される内部 CA 属性」の説明に従い、識別属性を入力します。

ステップ 6 [Generate self-signed CA] をクリックします。

新しい署名付き証明書の取得およびアップロード

ライセンス：任意

署名付き証明書を CA から取得することによって、内部 CA オブジェクトを設定できます。これは、次の 2 段階からなります。

- 内部 CA オブジェクトを設定するための識別情報を指定します。これにより、未署名の証明書およびペアになった秘密鍵が生成され、指定した CA に対する証明書署名要求（CSR）が作成されます。
- CA により署名付き証明書が発行されたら、それを内部 CA オブジェクトにアップロードして、未署名の証明書と置き換えます。

署名付き証明書が含まれている場合にのみ、SSL ルールで内部 CA オブジェクトを参照できます。

未署名の CA 証明書と CSR を作成する方法：

ステップ 1 内部 CA オブジェクトを設定するための識別情報を指定します。

a) [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。
b) [PKI] で、[Internal CAs] を選択します。
c) [Generate CA] をクリックします。
d) [Name] に、内部 CA オブジェクトの名前を入力します。縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。
e) 新しい CA 証明書と秘密キーの生成 （70 ページ）の説明に従い、識別属性を入力します。
f) [Generate CSR] をクリックします。
g) CA に送信するために CSR をコピーします。
h) [Store ASA FirePOWER Changes] をクリックします。

ステップ 2 CA から署名証明書をアップロードします。

a) [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。
b) [PKI] で、[Internal CAs] を選択します。
c) CSR を待機している未署名の証明書を含む CA オブジェクトの横にある編集アイコン（）をクリックします。
d) [Install Certificate] をクリックします。
e) [Certificate Data] フィールドの上部にある [Browse] をクリックして、DER または PEM でエンコードされた X.509 v3 CA 証明書ファイルをアップロードします。
f) アップロード ファイルがパスワード保護されている場合は、[Encrypted, and the password is:] チェックボックスをオンにして、パスワードを入力します。
g) [Store ASA FirePOWER Changes] をクリックします。

CA オブジェクトに署名付き証明書が含まれ、SSL ルールでこれを参照できます。

CA 証明書および秘密キーのダウンロード

ライセンス：任意

証明書および鍵の情報を含むファイルを内部 CA オブジェクトからダウンロードすることにより、CA 証明書およびペアになった秘密鍵をバックアップまたは転送できます。

⚠

注意 ダウンロードされた鍵情報は必ず安全な場所に保存してください。

システムは、内部 CA オブジェクトに保存されている秘密鍵をディスクに保存する前に、ランダムに生成された鍵を使って暗号化します。証明書および秘密鍵を内部 CA オブジェクトからダウンロードすると、システムはまず情報を復号化してから、証明書および秘密鍵の情報を含むファイルを作成します。その後、ダウンロードファイルを暗号化するためにシステムで使われるパスワードを提供する必要があります。

注意 システムバックアップの一部としてダウンロードされる秘密鍵は、復号化されてから、非暗号化バックアップ ファイルに保存されます。詳細については、バックアップ ファイルの作成（606 ページ）を参照してください。

内部 CA 証明書と秘密鍵をダウンロードする方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 [PKI] で、[Internal CAs] を選択します。

ステップ 3 証明書および秘密キーをダウンロードする対象となる内部CAオブジェクトの横にある編集アイコン（）をクリックします。

ステップ 4 [Download] をクリックします。

ステップ 5 [Password] および [Confirm Password] フィールドに、暗号化パスワードを入力します。

ステップ 6 [Store ASA FirePOWER Changes] をクリックします。

ファイルを保存するように指示するメッセージが表示されます。

信頼できる認証局オブジェクトの操作

ライセンス：任意

設定済みの、信頼できる認証局（CA）オブジェクトはそれぞれ、組織外の信頼できる CA に属する CA 公開鍵証明書を表します。このオブジェクトは、オブジェクト名と CA 公開鍵証明書からなります。SSL ポリシーで外部 CA オブジェクトとグループ（オブジェクトのグループ化 （24 ページ）を参照）を使用すると、信頼できる CA またはトラスト チェーン内の任意の CA によって署名された証明書を使って暗号化されたトラフィックを制御できます。

信頼できる CA オブジェクトを作成した後で、その名前を変更したり、証明書失効リスト（CRL）を追加したりすることはできますが、他のオブジェクトプロパティを変更することはできません。オブジェクトに追加できるCRLの数には制限がありません。オブジェクトにアップロード済みの CRL を変更するには、オブジェクトをいったん削除して再作成する必要があります。

使用中の信頼できる CA オブジェクトを削除することはできません。さらに、信頼できる CA オブジェクトを編集した後に、アクティブポリシーがオブジェクトを参照する場合、変更を有効にするには設定を展開する必要があります。設定変更の導入 （92 ページ）を参照してください。

信頼できる CA オブジェクトの追加

ライセンス：任意

外部 CA オブジェクトは、X.509 v3 CA 証明書をアップロードすることによって設定できます。次のサポートされている形式のいずれかでエンコードしたファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

ファイルがパスワード保護されている場合は、復号化パスワードを提供する必要があります。証明書が PEM 形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

ファイルに適切な証明書情報が含まれる場合にのみ、CA 証明書をアップロードできます。システムはオブジェクトを保存する前に証明書を検証します。

信頼できる CA 証明書をインポートする方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 [PKI] で、[Trusted CAs] を選択します。

ステップ 3 [Add Trusted CAs] をクリックします。

ステップ 4 [Name] に、信頼できる CA オブジェクトの名前を入力します。縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5 [Certificate Data] フィールドの上部にある [Browse] をクリックして、DER または PEM でエンコードされた X.509 v3 CA 証明書ファイルをアップロードします。

ステップ 6 ファイルがパスワード保護されている場合は、[Encrypted, and the password is:] チェックボックスをオンにして、パスワードを入力します。

ステップ 7 [Store ASA FirePOWER Changes] をクリックします。

信頼できる CA オブジェクトへの証明書失効リストの追加

ライセンス：**任意**

信頼できる CA オブジェクトに CRL をアップロードできます。信頼できる CA オブジェクトを SSL ポリシーの中で参照すると、セッションの暗号化証明書を発行した CA がその後で証明書を取り消したかどうかに基づいて、暗号化されたトラフィックを制御できます。サポートされる次のいずれかの形式でエンコードされたファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

CRL を追加した後、失効した証明書のリストを表示することができます。オブジェクトにアップロード済みの CRL を変更するには、オブジェクトをいったん削除して再作成する必要があります。

適切な CRL を含んでいるファイルのみをアップロードできます。信頼できる CA オブジェクトに追加できる CRL の数には制限がありません。ただし、CRL をアップロードした場合、別の CRL を追加する前に、オブジェクトをその都度保存する必要があります。

CRL をアップロードする方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。
ステップ 2 [PKI] で、[Trusted CAs] を選択します。
ステップ 3 信頼できる CA オブジェクトの横にある編集アイコン（）をクリックします。
ステップ 4 [Add CRL] をクリックして、DER または PEM でエンコードされた CRL ファイルをアップロードします。
ステップ 5 [Store ASA FirePOWER Changes] をクリックします。

外部証明書オブジェクトの操作

ライセンス：任意

設定済みのそれぞれの外部証明書オブジェクトは、組織に属さないサーバ公開鍵証明書を表します。このオブジェクトは、オブジェクト名と証明書からなります。SSL ルールで外部証明書オブジェクトとグループ（オブジェクトのグループ化 （24 ページ）を参照）を使用すると、サーバ証明書で暗号化されたトラフィックを制御できます。たとえば、信頼できる自己署名サーバ証明書はアップロードできますが、信頼できる CA 証明書を使用して検証することはできません。

X.509 v3 サーバ証明書をアップロードすることによって、外部証明書オブジェクトを設定できます。サポートされている次のいずれかの形式のファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

適切なサーバ証明書情報を含んでいるファイルだけをアップロードできます。システムはオブジェクトを保存する前にファイルを検証します。証明書が PEM 形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

外部証明書オブジェクトを作成した後、その名前を変更することはできますが、他のオブジェクト プロパティを変更することはできません。

使用中の外部証明書オブジェクトは削除できません。さらに、外部証明書オブジェクトを編集した後に、アクティブ ポリシーがオブジェクトを参照する場合、変更を有効にするには設定を展開する必要があります。設定変更の導入 （92 ページ）を参照してください。

外部証明書オブジェクトを作成する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。
ステップ 2 [PKI] で、[External Certs] を選択します。

ステップ 3 [Add External Cert] をクリックします。

ステップ 4 [Name] に、外部証明書オブジェクトの名前を入力します。縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5 [Certificate Data] フィールドの上部にある [Browse] をクリックして、DER または PEM でエンコードされた X.509 v3 サーバ証明書ファイルをアップロードします。

ステップ 6 [Store ASA FirePOWER Changes] をクリックします。

内部証明書オブジェクトの操作

ライセンス：任意

設定済みのそれぞれの内部証明書オブジェクトは、組織に属するサーバ公開鍵証明書を表します。このオブジェクトは、オブジェクト名、公開鍵証明書、およびペアになった秘密鍵からなります。SSL ルールで内部証明書オブジェクトとグループ（オブジェクトのグループ化 （24 ページ）を参照）を使用すると、既知の秘密キーを使用して組織のいずれかのサーバに着信するトラフィックを復号化できます。

X.509 v3 RSA ベースまたは楕円曲線ベースのサーバ証明書およびペアの秘密キーをアップロードすることで、内部証明書オブジェクトを設定できます。サポートされている次のいずれかの形式のファイルをアップロードできます。

- 識別符号化規則（DER）
- プライバシー強化電子メール（PEM）

ファイルがパスワード保護されている場合は、復号化パスワードを提供する必要があります。証明書とキーが PEM 形式でエンコードされている場合は、情報をコピーして貼り付けることもできます。

適切な証明書またはキーの情報を含んでいる、相互にペアになっているファイルのみをアップロードできます。システムはオブジェクトを保存する前にペアを検証します。

内部証明書オブジェクトを作成した後、その名前を変更することはできますが、他のオブジェクト プロパティを変更することはできません。

使用中の内部証明書オブジェクトは削除できません。さらに、内部証明書オブジェクトを編集した後に、アクティブポリシーがオブジェクトを参照する場合、変更を有効にするには設定を展開する必要があります。設定変更の導入 （92 ページ）を参照してください。

内部証明書オブジェクトを作成する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 [PKI] で、[Internal Certs] を選択します。

ステップ 3 [Add Internal Cert] をクリックします。

ステップ 4 [Name] に、内部証明書オブジェクトの名前を入力します。縦線（|）と中カッコ（{}）を除き、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5 [Certificate Data] フィールドの上部にある [Browse] をクリックして、DER または PEM でエンコードされた X.509 v3 サーバ証明書ファイルをアップロードします。

ステップ 6 [Key] フィールドの上部にある [Browse] をクリックして、DER または PEM でエンコードされたペアの秘密キー ファイルをアップロードします。

ステップ 7 アップロードした秘密キー ファイルがパスワード保護されている場合は、[Encrypted, and the password is:] チェックボックスをオンにして、パスワードを入力します。

ステップ 8 [Store ASA FirePOWER Changes] をクリックします。

次のタスク

- CA 証明書および秘密キーのインポート （69 ページ）
  新しい CA 証明書と秘密キーの生成 （70 ページ）
  新しい署名付き証明書の取得およびアップロード （71 ページ）
  CA 証明書および秘密キーのダウンロード （72 ページ）

地理位置情報オブジェクトの操作

ライセンス：任意

設定済みの位置情報（ジオロケーション）オブジェクトは、管理対象ネットワーク上のトラフィックの送信元または宛先としてシステムで識別された 1 つ以上の国または大陸を表します。アクセス コントロール ポリシーまたは SSL ポリシーでは、地理位置情報オブジェクトを使用できます。たとえば、特定の国が送信元/宛先であるトラフィックをブロックするアクセス コントロール ルールを作成できます。地理的な場所によるトラフィックのフィルタリングについては、ネットワークまたは地理的位置によるトラフィックの制御 （131 ページ）を参照してください。

常に最新の情報を使用してネットワーク トラフィックをフィルタ処理できるように、地理位置情報データベース（GeoDB）を定期的に更新することを強くお勧めします。GeoDB の更新をダウンロードおよびインストールする方法については、地理情報データベースについて （595 ページ）を参照してください。

使用中の位置情報オブジェクトは削除できません。さらに、アクセス コントロール ポリシーまたはSSLポリシーで使用される地理位置情報オブジェクトを編集した後、変更を有効にするには、ポリシーを再適用する必要があります。

地理位置情報オブジェクトを作成する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 [Geolocation] を選択します。

ステップ 3 [Add Geolocation] をクリックします。

ステップ 4 [Name] に、地理位置情報オブジェクトの名前を入力します。中カッコ（{}）を除く、印字可能な任意の標準 ASCII 文字を使用できます。

ステップ 5 位置情報オブジェクトに含める国および大陸のチェック ボックスを選択します。

大陸を選択すると、その大陸内のすべての国、およびGeoDB 更新によってその大陸に今後追加されるすべての国が選択されます。大陸の下でいずれかの国を選択解除すると、その大陸が選択解除されます。国と大陸を任意に組み合わせて選択できます。

ステップ 6 [Store ASA FirePOWER Changes] をクリックします。

セキュリティ グループ タグ オブジェクトの操作

ライセンス：任意

セキュリティ グループ タグ（SGT）オブジェクトは、単一の SGT 値を指定します。この値はアクセス コントロール ルールでカスタム SGT 条件として使用できます。SGT オブジェクトをグループ化することはできません。

ISE/ISE-PIC をアイデンティティ ソースとして設定すると、システムはオブジェクト マネージャの [セキュリティ グループ タグ（Security Group Tag）] オプションを自動的に無効にします。ISE/ISE-PIC 接続を無効にしない限り、新規 SGT オブジェクトの追加、既存 SGT オブジェクトの編集、またはルール条件としての SGT オブジェクトの使用はできません。カスタム SGT と ISE SGT の違いの詳細については、ISE SGT およびカスタム SGT ルール条件 （167 ページ）を参照してください。

SGT オブジェクトを編集または削除した後に、アクティブ ポリシーがオブジェクトを参照する場合、変更を有効にするには設定を再展開する必要があります。設定変更の導入 （92 ページ）を参照してください。

SGT オブジェクトを作成する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Object Management] の順に選択します。

ステップ 2 [Security Group] タグを選択します。

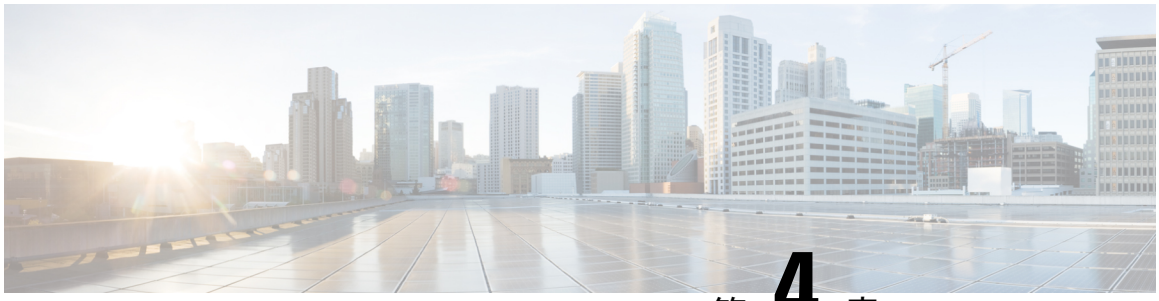
ステップ 3 [Add Security Group Tag] をクリックします。

ステップ 4 [Name] を入力します。

ステップ 5 （任意）[Description] に説明を入力します。

ステップ 6 [Tag] フィールドに、単一の SGT を入力します。

ステップ 7 [Store ASA FirePOWER Changes] をクリックします。



第 4 章

アクセス コントロール ポリシーの開始

アクセス コントロール ポリシーは、システムがネットワーク上のトラフィックを処理する方法を決定します。各 ASA FirePOWER モジュールには、現在適用されている 1 つのポリシーを設定できます。

この章では、単純なアクセス コントロール ポリシーを作成して適用する方法について説明します。また、アクセス コントロール ポリシーの管理に関する基本情報（編集、更新、比較など）も含まれています。

アクセス コントロール ポリシーについて

最も単純なアクセス コンロトール ポリシーは、そのデフォルト アクションを使用してすべてのトラフィックを処理します。このデフォルト アクションは、詳細な検査を行わずにすべてのトラフィックをブロックまたは信頼するように設定することも、侵入についてトラフィックを検査するように設定することもできます。

インライン展開された ASA FirePOWER モジュールだけがトラフィックのフローに影響を与える場合があることに注意してください。トラフィックをブロックまたは変更するように設定されたアクセス コントロール ポリシーをパッシブに展開されたデバイスに適用すると、予期しない結果になることがあります。場合によっては、パッシブに展開された ASA FirePOWER モジュールへのインライン設定の適用がシステムにより阻止されることがあります。

より複雑なアクセス コントロール ポリシーはセキュリティ インテリジェンス データに基づいてトラフィックをブロックすることができ、また、アクセス制御ルールを使用してネットワーク トラフィックのロギングおよび処理を細かく制御することができます。これらのルールは単純または複雑にすることができ、複数の基準を使用してトラフィックを照合および検査できます。高度なアクセス コントロール ポリシー オプションは、復号化、前処理、パフォーマンス、および他の一般設定を制御します。

基本的なアクセス コントロール ポリシーを作成した後に、固有の展開環境に合わせて調整する方法については、次の章を参照してください。

- セキュリティ インテリジェンスの IP アドレス レピュテーションを使用したトラフィックのブロック（103 ページ）では、最新のレピュテーション インテリジェンスに基づいて接続を直ちにブロックする方法について説明します。
- ネットワーク分析ポリシーと侵入ポリシーについて（297 ページ）では、システムの侵入検知および防止機能の一部として、ネットワーク分析および侵入ポリシーがパケットを前処理し確認する方法について説明します。
- アクセス コントロール ルールを使用したトラフィック フローの調整（111 ページ）では、複数の ASA FirePOWER モジュールで、アクセス コントロール ルールがネットワーク トラフィックを処理する詳細な方法について説明します。
- 侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御（171 ページ）では、侵入、禁止されたファイルおよびマルウェアを検出しオプションでブロックすることによって、トラフィックがその宛先に許可される前に、最後の防衛ラインを侵入ポリシーおよびファイル ポリシーが提供する方法について説明します。

アクセス コントロールのライセンスおよびロール要件

アクセス コントロールのライセンス要件

アクセス コントロール ポリシーは、ASA FirePOWER モジュールのどのライセンスでも作成できますが、アクセス コントロールのある側面では、ポリシーを適用する前に、特定のライセンス機能を有効にする必要があります。

警告アイコンおよび確認ダイアログ ボックスは、ご使用の展開環境でサポートされない機能を示します。

次の表に、アクセス コントロール ポリシーを適用する際のライセンス要件を記載します。

表 *12 :* アクセス コントロールのライセンス要件

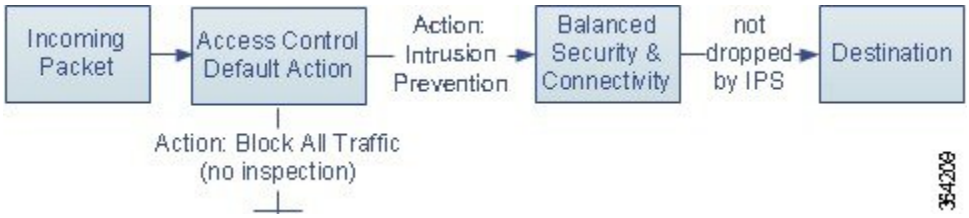
以下を実行するアクセス コントロール ポリシーを適用する場合	ライセンス
ゾーン、ネットワーク、またはポートに基づいてアクセス コントロールを実行する リテラル URL および URL オブジェクトを使用して URL フィルタリングを実行する	任意
位置情報データ（発信元または宛先の国/大陸）に基づいてアクセス コントロールを実行する	任意
侵入検知および侵入防御、ファイル コントロール、またはセキュリティ インテリジェンス フィルタリングを実行するポリシー	Protection
高度なマルウェア防御としてネットワークベースのマルウェア検出およびブロッキングを実行するポリシー	Malware
ユーザ制御またはアプリケーション制御を実行するポリシー	Control
カテゴリとレピュテーション データを使用して URL フィルタリングを実行するポリシー	URL Filtering

基本的なアクセス コントロール ポリシーの作成

ライセンス：任意

アクセス コントロール ポリシーには一意の名前が必須であり、デフォルト アクションを指定する必要があります。この時点で、デフォルト アクションにより、ASA FirePOWER モジュールの暗号化されていないすべてのトラフィックの処理方法が決まります。トラフィック フローに影響するその他の設定は後で追加します。

次の図に示すように、追加のインスペクションなしですべてのトラフィックをブロックするか、または侵入がないかどうかトラフィックを検査するようにデフォルト アクションを設定できます。



ヒント 最初にアクセス コントロール ポリシーを作成するときに、デフォルト アクションとしてトラフィックを信頼するように選択することはできません。すべてのトラフィックをデフォルトで信頼する場合は、ポリシーを作成した後にデフォルト アクションを変更します。

新規のアクセス コントロール ポリシーを作成したり、既存のアクセス コントロール ポリシーを管理したりするには、[Access Control Policy] ページ（[Policies] > [Access Control]）を使用します。

必要に応じて、当初からシステムに付属している Default Trust All Traffic という名前のポリシーを使用および変更できます。

アクセス コントロール ポリシーの作成方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。

[Access Control Policy] ページが表示されます。

ヒント この ASA FirePOWER モジュールから既存のポリシーをコピーしたり、別の ASA FirePOWER モジュールからポリシーをインポートしたりできます。ポリシーをコピーするには、コピー アイコンをクリックします。ポリシーをインポートするには、設定のインポートおよびエクスポート（617 ページ） を参照してください。

ステップ 2 [Name] に一意のポリシー名を入力し、オプションで [Description] にポリシーの説明を入力します。

印刷可能なすべての文字を使用できます。スペースと特殊文字も含まれますが、番号記号（#）、セミコロン（;）、波カッコ（{}）は使用できません。名前には少なくとも 1 つのスペース以外の文字が含まれている必要があります。

ステップ 3 初期デフォルト アクションを指定します。

- [すべてのトラフィックをブロック（Block All Traffic）] を選択すると、[アクセス コントロール：すべてのトラフィックをブロック（Access Control: Block All Traffic）] をデフォルト アクションとするポリシーが作成されます。
- [侵入防御（Intrusion Prevention）] を選択すると、[侵入防御：バランスの取れたセキュリティと接続（Intrusion Prevention: Balanced Security and Connectivity）] をデフォルト アクションとするポリシーが作成されます。

最初のデフォルト アクションを選択する手順、および後でそれを変更する手順については、デフォルトの処理の設定およびネットワーク トラフィックのインスペクション （83 ページ） を参照してください。

ステップ 4 [Store ASA FirePOWER Changes] をクリックします。

アクセス コントロール ポリシー エディタが表示されます。新しいポリシーの設定方法については、アクセス コントロール ポリシーの編集 （86 ページ） を参照してください。ポリシーを有効にするには適用する必要があることに注意してください。設定変更の導入 （92 ページ）を参照してください。

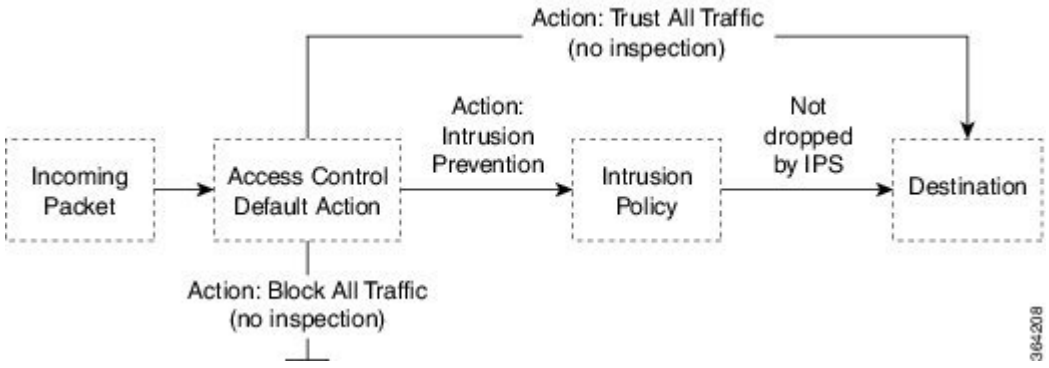
デフォルトの処理の設定およびネットワークトラフィックのインスペクション

ライセンス：任意

アクセス コントロール ポリシーを作成する場合は、デフォルト アクションを選択する必要があります。アクセス コントロール ポリシーのデフォルト アクションは、次の復号化されたまたは暗号化されていないトラフィックをシステムで処理する方法を決定します。

- セキュリティ インテリジェンスによってブロックされない
- ポリシー内のルールのいずれにも一致しないトラフィック（トラフィックの照合とロギングは行うが、処理または検査はしないモニタ ルールを除く）

したがって、アクセス コントロール ルールまたはセキュリティ インテリジェンスの設定が含まれておらず、暗号化されたトラフィックの処理に SSL ポリシーを呼び出さないアクセス コントロール ポリシーを適用する場合、デフォルト アクションにより、ネットワーク上のすべてのトラフィックがどのように処理されるかが決まります。追加のインスペクションなしですべてのトラフィックをブロックまたは信頼するか、または侵入がないかトラフィックを検査できます。オプションを次の図に示します。

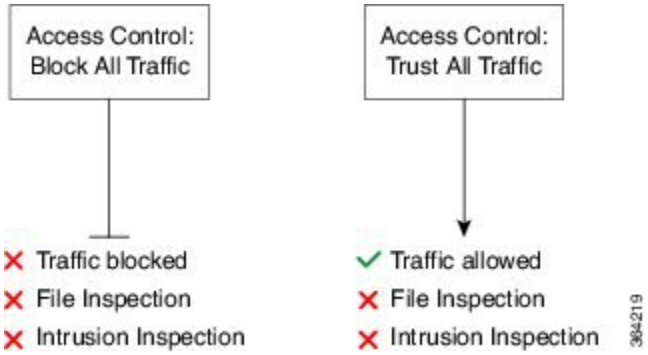


次の表に、さまざまなデフォルトアクションがトラフィックを処理する方法を示し、各デフォルト アクションで処理されるトラフィックで実行できるインスペクションのタイプを示します。デフォルトアクションで処理されるトラフィックでは、ファイルまたはマルウェアのインスペクションを実行**できない**ことに注意してください。詳細については、侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御 （171 ページ）を参照してください。

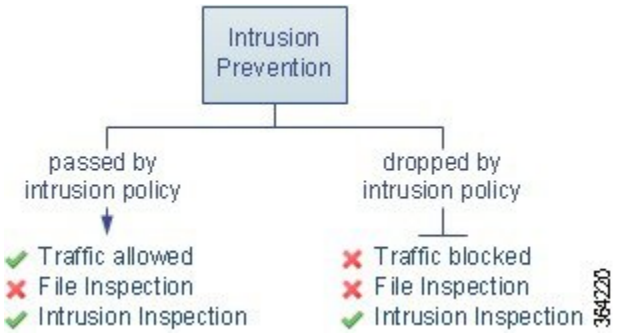
表 *13*：アクセス コントロール ポリシーのデフォルト アクション

デフォルト アクション	トラフィックに対して行う処理	インスペクションのタイプとポリシー
Access Control: Block All Traffic	それ以上のインスペクションは行わずにブロックする	なし
Access Control: Trust All Traffic	信頼（追加のインスペクションなしで最終宛先に許可）	なし
Intrusion Prevention	ユーザが指定した侵入ポリシーに合格する限り、許可する（Protection ライセンスが必要）	侵入、指定した侵入ポリシーおよび関連する変数セットを使用

次の図は、**すべてのトラフィックをブロック**および**すべてのトラフィックを信頼**デフォルト アクションを示しています。



以下の図は、**侵入防御**デフォルト アクションを示しています。



初めてアクセス コントロール ポリシーを作成する際、デフォルト アクションで処理される接続のロギングはデフォルトで無効になっています。侵入インスペクションを実行するデフォルトアクションを選択すると、システムはデフォルトの侵入変数セットを選択した侵入ポリシーに自動的に関連付けます。ポリシーを作成した後に、これらのオプションのどちらか、およびデフォルト アクション自体を変更できます。

アクセス コントロール ポリシーのデフォルト アクションと関連オプションを変更するには、次の手順を実行します。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。

[Access Control Policy] ページが表示されます。

ステップ 2 設定するアクセス コントロール ポリシーの横にある編集アイコンをクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3 [Default Action] を選択します。

- すべてのトラフィックをブロックする場合は、[Access Control: Block All Traffic] を選択します

  .
- すべてのトラフィックを信頼する場合は、[Access Control: Trust All Traffic] を選択します

  .
- すべてのトラフィックを侵入ポリシーを使用して検査する場合は、侵入ポリシーを選択します。侵入ポリシーは、いずれも Intrusion Prevention というラベルで始まります。侵入ポリシーによってトラフィックがブロックされる可能性があることに注意してください

  .

注意 シスコの担当者から指示された場合を除き、Experimental Policy 1は使用しないでください。シスコでは、試験用にこのポリシーを使用します。

ステップ 4 [Intrusion Prevention] のデフォルト アクションを選択した場合は、変数アイコンをクリックし、選択した侵入ポリシーに関連付けられている変数セットを変更します。

表示されるポップアップ ウィンドウで、新しい変数セットを選択して [OK] をクリックします。編集アイコンをクリックして、選択されている変数セットを新しいウィンドウで編集することもできます。変数セットを変更しない場合、システムはデフォルトのセットを使用します。詳細については、変数セットの操作（38 ページ）を参照してください。

ステップ 5 ロギング アイコンをクリックして、デフォルト アクションによって処理される接続のロギング オプションを変更します。

一致する接続は、その開始時と終了時にログに記録できます。システムはブロックされたトラフィックの終了をロギングできないことに注意してください。ASA FirePOWER モジュール イベント ビューア、外部のシステム ログ（Syslog）、または SNMP トラップ サーバへの接続をログに記録できます。詳細については、アクセス コントロールの処理に基づく接続のロギング （477 ページ）を参照してください。

アクセス コントロール ポリシーの管理

ライセンス：任意

[Access Control Policy] ページ（[Configuration] > [ASA FirePOWER Configuration] > [Policies]> [Access Control]）で、ポリシーの適用状態に関する情報とともに、現在のカスタム アクセス コントロール ポリシーを確認できます。

ユーザが作成したカスタム ポリシーに加えて、カスタム ポリシー Default Allow All Traffic がシステムによって提供され、それを編集して使用することができます。

[Access Control Policy] ページ上のオプションを使用して、次の表にあるアクションを実行できます。

表 *14*：アクセス コントロール ポリシーの管理操作

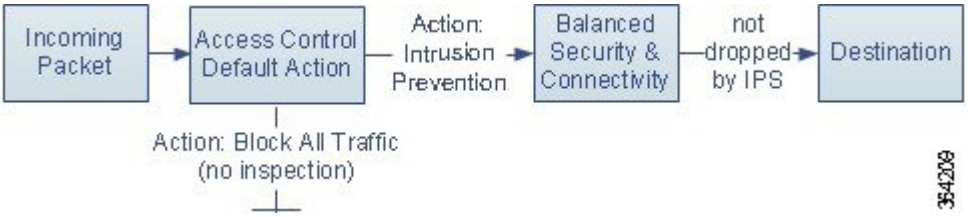
目的	操作	参照先
新しいアクセス コントロール ポリシーを作成する	[New Policy] をクリックします。	基本的なアクセス コントロール ポリシーの作成 （81 ページ）
既存のアクセス コントロール ポリシーを編集する	編集アイコンをクリックします。	アクセス コントロール ポリシーの編集 （86 ページ）
アクセス コントロール ポリシーを再適用する	適用アイコンをクリックします。	設定変更の導入 （92 ページ）
アクセス コントロール ポリシーをエクスポートして別の ASA FirePOWER モジュールにインポートする	エクスポート アイコンをクリックします。	設定のインポートおよびエクスポート （617 ページ）
アクセス コントロール ポリシーの現行の設定をリストする PDF を表示する	レポート アイコンをクリックします。	現在のアクセス コントロール設定のレポートの生成 （97 ページ）
アクセス コントロール ポリシーを比較する	[Compare Policies] をクリックします。	アクセス コントロール ポリシーを比較する （98 ページ）
アクセス コントロール ポリシーを削除する	削除アイコンをクリックし、ポリシーを削除することを確認します。適用済みのアクセス コントロール ポリシーや現在適用しているポリシーは削除できません。	

アクセス コントロール ポリシーの編集

ライセンス：任意

新しいアクセス コントロール ポリシーを初めて作成する場合、アクセス コントロール ポリシー エディタが表示され、[Rules] タブに焦点が置かれています。次の図に、新しく作成されたポリシーを示します。新しいポリシーにはルールやその他の設定がまだ存在しないため、デ

フォルトアクションはすべての暗号化されていないトラフィックを処理します。この場合、デフォルト アクションは、最終宛先に許可する前に、システムによって提供される [バランスの取れたセキュリティと接続（Balanced Security and Connectivity）] 侵入ポリシーを使用してトラフィックを検査します。



ルールの追加や編成などを行うには、アクセス コントロール ポリシー エディタを使用します。次のリストでは、変更可能なポリシー設定に関する情報を提供します。

名前と説明

ポリシーの名前と説明を変更するには、該当するフィールドをクリックし、新しい名前または説明を入力します。

セキュリティ インテリジェンス

セキュリティ インテリジェンスは、悪意のあるインターネット コンテンツに対する最初の防御ラインです。この機能を使用すると、最新のレピュテーションインテリジェンスに基づいて接続を直ちにブロックすることができます。重要なリソースへの継続的なアクセスを確保するために、ブロックリストをカスタムブロックなしリストでオーバーライドできます。このトラフィック フィルタリングは、ルールやデフォルト アクションを含む、他のどのポリシーベースのインスペクション、分析、またはトラフィック処理よりも**前に**行われます。詳細については、レピュテーションベースのルールによるトラフィックの制御 （139 ページ）を参照してください。

ルール

ルールでは、ネットワーク トラフィックを処理する詳細な方法が提供されます。アクセス コントロール ポリシー内の各ルールには、1 から始まる番号が付きます。システムは、ルール番号の昇順で先頭から順にアクセス コントロール ルールをトラフィックと照合します。

ほとんどの場合、システムは、すべてのルールの条件がトラフィックに一致する場合、最初のアクセス コントロール ルールに従ってネットワーク トラフィックを処理します。これらの条件には、セキュリティ ゾーン、ネットワークまたは地理的位置、ポート、アプリケーション、要求されたURL、またはユーザが含まれています。条件は単純または複雑にできます。条件の使用は特定のライセンスによって異なります。

ルールを追加、分類、有効化、無効化、フィルタリング、または管理するには、[Rules] タブを使用します。詳細については、アクセス コントロール ルールを使用したトラフィック フローの調整 （111 ページ）を参照してください。

デフォルト アクション

デフォルトアクションは、セキュリティインテリジェンスによってブロックされず、いずれのアクセス制御ルールにも一致しないトラフィックをシステムが処理する方法を決定します。デフォルト アクションを使用して、追加のインスペクションなしですべてのトラフィックをブ

ロックまたは信頼でき、または侵入がないかトラフィックを検査できます。デフォルト アクションによって処理される接続のロギングを有効または無効にできます。

詳細については、デフォルトの処理の設定およびネットワーク トラフィックのインスペクション （83 ページ）およびアクセス コントロールの処理に基づく接続のロギング （477 ページ）を参照してください。

HTTP 応答

ユーザの Web サイト要求をシステムがブロックした場合にブラウザに表示する内容を指定できます。一般的なシステム提供の応答ページを表示するか、カスタム HTML を入力するかを指定できますユーザに警告するページを表示することもできますが、ユーザはボタンをクリックして最初に要求されたサイトをロードするためにページの続行または更新を行うことも可能です。詳細については、ブロックされた URL のカスタム Web ページの表示 （157 ページ）を参照してください。

アクセス コントロールの詳細オプション

通常、アクセス コントロール ポリシーの詳細設定を変更する必要はほとんど、あるいはまったくありません。デフォルト設定は、ほとんどの展開環境に適しています。変更できる詳細設定には次のものがあります。

- ユーザが要求した各 URL に対し、ASA FirePOWER モジュール データベースに保存する文字数。を参照してください。 接続で検出された URL のロギング （481 ページ）
- ユーザが最初のブロックをバイパスした後に Web サイトを再度ブロックするまでの時間間隔。ブロックされた Web サイトのユーザー バイパス タイムアウトの設定 （157 ページ）を参照してください。
- ネットワーク分析ポリシーおよび侵入ポリシーの設定。この設定では、ネットワークおよびゾーンに対する多くの前処理オプションを調整し、デフォルトの侵入インスペクション動作を設定できます。
- トランスポートおよびネットワーク プリプロセッサの詳細設定。この設定は、アクセス コントロール ポリシーを適用するすべてのネットワークおよびゾーンにグローバルに適用されます。
- ユーザのネットワークのホスト オペレーティング システムに基づいて、パッシブ展開でパケット フラグメントおよび TCP ストリームの再構成を改善する適応型プロファイル。ルールを使用した侵入ポリシーの調整 （355 ページ） を参照してください。
- 侵入インスペクション、ファイル制御、および高度なマルウェア防御のパフォーマンス オプション。侵入防御パフォーマンスの調整 （177 ページ）およびファイルおよびマルウェア インスペクション パフォーマンスおよびストレージの調整 （190 ページ）を参照してください。

アクセス コントロール ポリシーを編集すると、変更がまだ保存されていないことを示すメッセージが表示されます。変更を維持するには、ポリシー エディタを終了する前にポリシーを保存する必要があります。変更を保存しないでポリシー エディタを終了しようとすると、変更がまだ保存されていないことを警告するメッセージが表示されます。この場合、変更を破棄してポリシーを終了するか、ポリシー エディタに戻るかを選択できます。

セッションのプライバシーを保護するために、ポリシー エディタで 60 分間操作が行われないと、ポリシーの変更が破棄されて、[Access Control Policy] ページに戻ります。30 分間操作が行われなかった時点で、変更が破棄されるまでの分数を示すメッセージが表示されます。以降、このメッセージは定期的に更新されて残りの分数を示します。ページで何らかの操作を行うと、タイマーがキャンセルされます。

アクセス コントロール ポリシーの編集方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。

[Access Control Policy] ページが表示されます。

ステップ 2 設定するアクセス コントロール ポリシーの横にある編集アイコンをクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3 ポリシーを編集します。上記に要約されているいずれかの操作を実行します。

ステップ 4 設定を保存または廃棄します。

- 変更を保存し、編集を続行する場合は、[Store ASA FirePOWER Changes] をクリックします。
- 変更を保存し、ポリシーを適用するには、[Apply ASA FirePOWER Changes] をクリックします。設定変更の導入 （92 ページ）を参照してください。
- 変更を廃棄する場合は、[Cancel] をクリックし、プロンプトが出たら [OK] をクリックします。

アクセス制御への他のポリシーの関連付け

ライセンス：任意

次のサブポリシーのいずれかとアクセス コントロール ポリシーとを関連付けるには、アクセス コントロール ポリシーの詳細設定を使用します。

- SSL ポリシー：セキュア ソケット レイヤ（SSL）または Transport Layer Security（TLS）で暗号化されたアプリケーション層プロトコル トラフィックをモニター、復号化、ブロック、または許可します。
- アイデンティティ ポリシー：トラフィックに関連付けられているレルムと認証方式に基づいて、ユーザ認証を実行します。

注意 SSL またはアイデンティティ ポリシーの関連付け、またはそれ以降の [None] を選択することによるポリシー関連付け解除により、設定変更の展開時に Snort プロセスは再開し、トラフィックの検査が一時的に中断されます。この検査中にトラフィックがドロップされるか、それ以上検査が行われずに受け渡されるかは、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。

他のポリシーとアクセス コントロール ポリシーを関連付ける方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。

ステップ 2 設定するアクセス コントロール ポリシーの横にある編集アイコンをクリックします。

ステップ 3 [Advanced] タブをクリックします。

ステップ 4 適切な [Policy Settings] 領域の編集アイコンをクリックします。

ステップ 5 ドロップダウン リストからポリシーを選択します。

ユーザが作成したポリシーを選択した場合、編集アイコンをクリックして、ポリシーを編集できます。

ステップ 6 [OK] をクリックします。

ステップ 7 設定を保存または廃棄します。

- 変更を保存し、編集を続行する場合は、[Store ASA FirePOWER Changes] をクリックします。
- 変更を保存し、ポリシーを適用するには、[Apply ASA FirePOWER Changes] をクリックします。設定変更の導入 （92 ページ）を参照してください。
- 変更を廃棄する場合は、[Cancel] をクリックし、プロンプトが出たら [OK] をクリックします。

失効したポリシーの警告について

ライセンス：任意

[Access Control Policy] ページ（[Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control]）では、失効したポリシーには、赤色のステータステキストが付いています。

ほとんどの場合、アクセス コントロール ポリシーを変更した場合は、変更を有効にするために再度適用する必要があります。アクセス コントロール ポリシーが他のポリシーを呼び出したり、または他の設定に依存する場合、それらを変更すると、アクセス コントロール ポリシーを再度適用する必要があります（または、侵入ポリシーの変更の場合は、侵入ポリシーだけを再度適用できます）。

ポリシーの再適用が必要な設定変更には次のものがあります。

- アクセス コントロール ポリシー自体の変更：アクセス コントロール ルール、デフォルト アクション、セキュリティ インテリジェンス フィルタリング、NAP ルールなどの詳細オプションの変更。
- アクセス コントロール ポリシーが呼び出す侵入およびファイル ポリシーのいずれかの変更：SSLポリシー、ネットワーク分析ポリシー、侵入ポリシー、およびファイルポリシー。
- アクセス コントロール ポリシーで使用される再利用可能なオブジェクトまたは設定、またはアクセスコントロールポリシーが呼び出すポリシーの変更：ネットワーク、ポート、URL、および位置情報オブジェクト、セキュリティ インテリジェンスのリストとフィード、アプリケーションフィルタまたはディテクタ、侵入ポリシーの変数セット、ファイルリスト、復号化関連オブジェクト、セキュリティ ゾーンなど。
- システム ソフトウェア、侵入ルール、または脆弱性データベース（VDB）の更新。

これらの設定の一部は、ASA FirePOWER モジュール インターフェイスの複数の場所から変更できることに留意してください。たとえば、セキュリティ ゾーンはオブジェクト マネージャ（[Configuration] > [ASA FirePOWER Configuration] > [Object Management]）を使用して変更できます。

次の更新では、ポリシーの再適用は必要**ありません**。

- URL フィルタリング データへの自動更新
- スケジュールされた位置情報データベース（GeoDB）の更新

アクセス コントロール ポリシーまたは侵入ポリシーが失効した理由を確認するには、比較ビューアを使用します。

アクセス コントロール ポリシーが失効した理由を確認するには、次の手順を実行します。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。

[Access Control Policy] ページが表示されます。失効したポリシーには、ASA FirePOWER モジュールがポリシーの更新を必要としていることを示す赤色のステータス テキストが付いています。

ステップ 2 失効したポリシーのポリシー ステータスをクリックします。

詳細な [Apply Access Control Policy] ポップアップ ウィンドウが表示されます。

ステップ 3 該当する変更されたコンポーネントの横にある [Out-of-date] をクリックします。

ポリシーの比較レポートが新しいウィンドウに表示されます。詳細については、アクセス コントロール ポリシーを比較する （98 ページ）および2 つの侵入ポリシーまたはリビジョンの比較 （351 ページ）を参照してください。

ステップ 4 オプションで、ポリシーを再度適用します。「設定変更の導入 （92 ページ）」を参照してください。

設定変更の導入

ライセンス：任意

ASA FirePOWER モジュールを使用して展開環境の設定を行った後で、その設定に変更を加える場合は、常に新しい設定を展開する必要があります。

この導入アクションにより、次の設定コンポーネントが配布されます。

- アクセスコントロールポリシーとすべての関連ポリシー：DNS、ファイル、アイデンティティ、侵入、ネットワーク分析、SSL
- 導入されたポリシーに関連付けられているすべての関連ルール設定とオブジェクト
- 侵入ルール更新
- デバイスとインターフェイスの設定

⚠

注意 特殊なケースとして、設定変更を展開すると、トラフィック フローと処理が一時的に停止したり、いくつかのパケットが検査されないまま通過したりすることがあります。利用できない時間を最小限にするために、導入は変更時間帯に実行します。

設定変更を展開するには、次のようにします。

ステップ 1 [Deploy] をクリックして、[Deploy FirePOWER Changes] を選択します。

ステップ 2 [Deploy] をクリックします。

ステップ 3 変更の展開時にエラーまたは警告が出された場合には、次の選択肢があります。

- [Proceed] をクリックして、エラーまたは警告条件を解決しないで導入を続行します。
- [Cancel] をクリックして、展開を実行せずに終了します。エラーおよび警告状態を解決し、設定の再展開を試行します。

アクセス コントロール ポリシーとルールのトラブルシューティング

ライセンス：任意

アクセス コントロール ポリシーの適切な設定、特に、アクセス コントロール ルールの作成と順序付けは複雑なタスクです。しかし、これは効果的な展開を構築するために必要なタスクです。ポリシーを慎重に計画しないと、ルールが他のルールをプリエンプション処理したり、

ルールに無効な設定が含まれる場合があります。ルールおよび他のポリシー設定にはどちらも追加ライセンスが必要な場合があります。

システムが想定どおりにトラフィックを確実に処理できるように、アクセス コントロール ポリシー インターフェイスには強力なフィードバック システムがあります。アクセス コントロール ポリシーおよびルール エディタのアイコンは、警告とエラーを示します。表「アクセス コントロールのエラー アイコン」を参照。

ヒント アクセス コントロール ポリシー エディタで、ポリシーのすべての警告を表示するポップアップ ウィンドウを表示するには [Show Warnings] をクリックします。

また、トラフィックの分析およびフローに影響を与える可能性がある問題の適用時には、システムによって警告が表示されます。

表 *15*：アクセス コントロールのエラー アイコン

アイコン	説明	詳細
	エラー	ルールまたは設定にエラーがある場合、影響を受けるルールを無効にしても、問題を修正するまでポリシーを適用できません。
	警告	ルールまたはその他の警告を表示するアクセス コントロール ポリシーを適用できます。しかし、警告とマークされている誤った設定には影響しません。 たとえば、プリエンプション処理されたルールまたは誤った設定（空のオブジェクト グループを使用した条件、アプリケーションに一致しないアプリケーション フィルタ、クラウド通信を有効にしないまま行った URL 条件の設定など）によってトラフィックを照合できないルールを含むポリシーを適用できます。これらのルールは、トラフィックを評価しません。警告が出されているルールを無効にすると、警告アイコンが消えます。潜在する問題を修正せずにルールを有効にすると、警告アイコンが再表示されます。 別の例としては、多くの機能で特定のライセンスが必要です。アクセス コントロール ポリシーは、対象のデバイスのみに正常に適用されます。
	情報	情報アイコンには、トラフィックのフローに影響する可能性がある設定に関する有用な情報が表示されます。これらの問題によってポリシーの適用が阻まれることはありません。 たとえば、アプリケーション制御または URL フィルタリングを実行している場合、システムはその接続でアプリケーションまたは Web トラフィックを識別するまで、接続の最初の数パケットを複数のアクセス コントロール ルールと照合するのをスキップする場合があります。これにより、アプリケーションと HTTP 要求が識別されるように接続が確立されます。詳細については、アプリケーション制御の制限（146 ページ）およびURL の検出とブロッキングのガイドラインと制限事項（153 ページ）を参照してください。

アクセス コントロール ポリシーおよびルールを適切に設定することで、ネットワーク トラフィックの処理に必要なリソースも減らすことができます。複雑なルールの作成、多数のさま

ざまな侵入ポリシーの呼び出し、およびルールの誤った順序付けはすべて、パフォーマンスに影響する可能性があります。

パフォーマンスを向上させるためのルールの簡素化

複雑なアクセス コントロール ポリシーおよびルールは、重要なリソースを消費する可能性があります。アクセス コントロール ポリシーを適用すると、システムはすべてのルールをまとめて評価し、ネットワーク トラフィックを評価するために ASA FirePOWER モジュールが使用する条件の拡張セットを作成します。サポートされるアクセス コントロール ルールまたは侵入ポリシーの最大数を超えていることを警告するポップアップ ウィンドウが表示される場合があります。

アクセス コントロール ルールの簡素化

次のガイドラインは、アクセス コントロール ルールを簡素化し、パフォーマンスを向上させるのに役立ちます。

- ルールを構築するときは、条件内で使用する個々の要素は可能な限り少なくします。たとえばネットワーク条件であれば、個別の IP アドレスではなく、IP アドレス ブロックを使用します。ポート条件では、ポート範囲を使用します。アプリケーション制御および URL フィルタリングを実行する場合はアプリケーション フィルタと URL カテゴリおよびレピュテーションを使用し、ユーザ制御を実行する場合は LDAP ユーザ グループを使用します。

アクセス コントロール ルールの条件で使用する要素をオブジェクトに組み合わせてもパフォーマンスは向上しないことに注意してください。たとえば、50 の個別の IP アドレスを含むネットワーク オブジェクトを使用しても、その条件内のそれらの IP アドレスに対するものを含む、組織的な（パフォーマンスではない）利点が個別に与えられるだけです。

- できるだけセキュリティ ゾーンでルールを制限します。デバイスのインターフェイスが、ゾーン制限されたルールのどのゾーンにも属さない場合、そのデバイスのパフォーマンスにルールは影響を与えません。
- ルールを過度に設定しないようにします。1 つの条件が処理するトラフィックに一致するのに十分な場合は、2 つ使用しないでください。

侵入ポリシーと変数セットの急増の回避

アクセス コントロール ポリシーでトラフィックを検査するために使用できる一意の侵入ポリシーの数は、ポリシーの複雑度によって異なります。1 つの侵入ポリシーを各許可ルールおよびインタラクティブ ブロック ルール、さらにデフォルト アクションに関連付けることができます。侵入ポリシーと変数セットの固有の**ペア**はすべて、1 つのポリシーとしてカウントされます。アクセス コントロール ポリシー全体で、侵入ポリシーを 3 つしか選択できない場合があります。

サポートされる侵入ポリシーの数を超えた場合、アクセス コントロール ポリシーを再評価してください。複数の侵入ポリシーまたは変数セットを統合すると、複数のアクセス コントロール ルールに 1 つの侵入ポリシーと変数セットのペアを関連付けることができます。

アクセス コントロール ポリシーの次の場所のそれぞれで、選択したポリシーの数と、それらのポリシーが使用する変数セットの数を確認します。アクセス コントロール ポリシーの詳細設定の [Intrusion Policy used before Access Control rule is determined] オプション、アクセス コントロール ポリシーのデフォルト アクション、およびポリシー内のアクセス コントロール ルールのインスペクション設定。

ルールのプリエンプションと無効な設定の警告について

ライセンス：任意

アクセス コントロール ルール（および、高度な展開ではネットワーク分析ルール）の適切な設定と順序付けは、効果的な展開を構築するために必須です。アクセス コントロール ポリシー内では、アクセス コントロール ルールが他のルールをプリエンプション処理したり、ルールに無効な設定が含まれている場合があります。同様に、アクセス コントロール ポリシーの詳細設定を使用して設定するネットワーク分析ルールにも同じ問題が存在する可能性があります。システムは、警告とエラーのアイコンを使用してこれらをマークします。

ルールのプリエンプションの警告について

アクセス コントロール ルールの条件が後続のルールよりも優先して適用され、後続のルールによるトラフィックの照合が回避される場合があります。次に例を示します。

```
Rule 1: allow Admin users
Rule 2: block Admin users
```

上記の最初のルールによってトラフィックは事前に許可されているため、2番目のルールによってトラフィックがブロックされることはありません。

次の点に注意してください。

- どのようなタイプのルール条件でも、後続のルールを回避する可能性があります。
- あるルールとその後続のルールがまったく同じで、いずれもすべて同じ条件が設定されている場合、後続のルールは回避されます。
- 条件が 1 つでも異なる場合は、後続のルールが回避されることはありません。

無効な設定の警告について

アクセス コントロール ポリシーが依存する外部の設定は変更される可能性があるため、有効であったアクセス コントロール ポリシー設定が無効になる場合があります。次の例について考えてみます。

- ルールの送信元ポートにポート グループを追加し、その後そのポート グループを変更して ICMP ポートを含めると、そのルールは無効になり、横に警告アイコンが表示されます。ポリシーをまだ適用することはできますが、ルールはネットワーク トラフィックに影響を与えません。

- ルールにユーザを追加した後、LDAP ユーザ認識設定を変更してそのユーザを除外すると、ユーザはアクセス コントロールの対象ユーザではなくなるため、そのルールは影響しなくなります。

パフォーマンスを向上させプリエンプションを回避するためのルールの順序付け

ライセンス：任意

アクセス コントロール ポリシー内の各ルールには、1 から始まる番号が付きます。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。Monitor ルールを除き、トラフィックが最初に一致するルールが、当該トラフィックを処理するためのルールになります。

アクセス コントロール ルールの順序を適切にすることで、ネットワーク トラフィックの処理に必要なリソースが減り、ルールのプリエンプションを回避できます。ユーザーが作成するルールはすべての組織と展開に固有のものですが、ユーザーのニーズに対処しながらもパフォーマンスを最適化できるルールを順序付けする際に従うべきいくつかの一般的なガイドラインがあります。

ルール条件は高いものから低いものに順序付ける

最初に、組織のニーズに適する順番でルールを配置します。すべてのトラフィックに適用する必要があるプライオリティ ルールをポリシーの先頭部分付近に配置します。たとえば、ある 1 人のユーザからのトラフィックに侵入がないかを検査する（許可ルールを使用）が、部門内の他のすべてのユーザは信頼する（信頼ルールを使用）場合は、その順序で 2 つのアクセス コントロール ルールを配置します。

特定のルールから一般的なルールへの順序付け

具体的なルール、つまり処理するトラフィックの定義を絞り込むルールを先に設定することで、パフォーマンスを向上させることができます。これは、広範な条件を持つルールが多くのさまざまなタイプのトラフィックを照合し、後でより多くの特定のルールをプリエンプション処理することができるという理由からも重要です。

ほとんどのソーシャル ネットワーキング サイトをブロックする一方で、特定の他の部分へのアクセスを許可する場合のシナリオを考えます。たとえば、グラフィック デザイナーに Creative Commons Flickr および deviantART コンテンツへのアクセスを許可したいが、Facebook や Google+ などの他のサイトへのアクセスは許可したくない場合があります。この場合はルールを次のように順序付けする必要があります。

```
Rule 1: Allow Flickr, deviantART for the “Design” LDAP user group
Rule 2: Block social networking
```

ルールを入れ替える場合は次のようになります。

```
Rule 1: Block social networking
Rule 2: Allow Flickr, deviantART for the “Design” LDAP user group
```

最初のルールは、Flickr および deviantART を含むすべてのソーシャル ネットワーキング トラフィックをブロックします。トラフィックが2番目のルールに一致しないため、利用可能にしたかったコンテンツにデザイナーはアクセスできません。

トラフィックを後で検査するルールの配置

侵入、ファイルおよびマルウェアのインスペクションにはリソースの処理が必要なため、トラフィックのインスペクションを行うルール（許可、インタラクティブ ブロック）の前にトラフィックを検査しないルール（信頼、ブロック）を配置することで、パフォーマンスを向上させることができます。これは、信頼ルールおよびブロック ルールは、システムが別の方法で検査をした可能性があるトラフィックを迂回させることができるためです。他の要素がすべて同等、つまり、より重要なものがなくプリエンプションが問題ではない場合にルールのセットを与えると仮定すると、次の順序でルールを配置することを検討します。

- 一致する接続はロギングするが、トラフィックで他のアクションは実行しないモニタ ルール
- 追加のインスペクションなしでトラフィックを処理する信頼ルールおよびブロック ルール
- トラフィックの追加のインスペクションを行わない許可ルールおよびインタラクティブ ブロック ルール
- マルウェア、侵入、またはその両方がないか任意でトラフィックを検査する許可ルールおよびインタラクティブ ブロック ルール

現在のアクセス コントロール設定のレポートの生成

ライセンス：任意

アクセス コントロール ポリシー レポートとは、特定の時点でのポリシーおよびルールの設定を記録したものです。このレポートには、次の情報が含まれており、監査目的や現在の設定を調べるために使用できます。

表 *16*：アクセス コントロール ポリシー レポートのセクション

セクション	説明
Policy Information	ポリシーの名前と説明、ポリシーを最後に変更したユーザの名前、ポリシーが最後に変更された日時が記載されます。
HTTP Block Response HTTP Interactive Block Response	ポリシーを使用して Web サイトをブロックするときにユーザに表示されるページの詳細が提供されます。
Security Intelligence	ポリシーのセキュリティ インテリジェンスのブロックなしリストとブロックリストの詳細が提供されます。

セクション	説明
Default Action	デフォルト アクションと関連する変数セット（存在する場合）が示されます。
Rules	ポリシーの各アクセス コントロール ルールが示され、その設定の詳細が提供されます。
Advanced Settings	次のようなポリシーの詳細設定の情報 • アクセス コントロール ポリシーのトラフィックを前処理するために使用されるネットワーク分析ポリシー、およびグローバル前処理オプション • パッシブ展開用の適合型プロファイル設定 • ファイル、マルウェア、および侵入を検出するためのパフォーマンス設定 • 他のポリシー全体の設定
Referenced Objects	侵入ポリシーの変数セットおよび SSL ポリシーで使用されるオブジェクトなど、アクセス コントロール ポリシーによって参照される再利用可能なオブジェクトに関する詳細が提供されます。

また、ポリシーを現在適用されているポリシーや別のポリシーと比較する、アクセス コントロール比較レポートを生成することもできます。詳細については、アクセス コントロール ポリシーを比較する （98 ページ）を参照してください。

アクセス コントロール ポリシー レポートの表示方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。

[Access Control Policy] ページが表示されます。

ステップ 2 レポートの生成対象とするポリシーの横にあるレポート アイコンをクリックします。アクセス コントロール ポリシー レポートを生成する前に、必ずすべての変更を保存してください。レポートには、保存された変更のみが表示されます。

システムによってレポートが生成されます。コンピュータにレポートを保存するように求められます。

アクセス コントロール ポリシーを比較する

ライセンス：任意

組織の標準に準拠しているかを確認する目的や、システム パフォーマンスを最適化する目的でポリシーの変更を検討するために、2 つのアクセス コントロール ポリシーの差異を調べること

ができます。任意の2つのポリシーを比較することも、現在適用されているポリシーを別のポリシーと比較することもできます。オプションで、比較した後に PDF レポートを生成することで、2 つのポリシーの間の差異を記録できます。

ポリシーを比較するために使用できるツールは 2 つあります。

- 比較ビューは、2 つのポリシーを左右に並べて表示し、その差異のみを示します。比較ビューの左右のタイトル バーに、それぞれのポリシーの名前が示されます。。ただし、[Running Configuration] を選択した場合、現在アクションなポリシーは空白のバーで表されます。

このツールを使用すると、モジュールインターフェイスで2つのポリシーを表示してそれらに移動するときに、差異を強調表示することができます。

- 比較レポートは、ポリシー レポートと同様の形式ですが、2つのポリシーの間の差異だけが、PDF 形式で記録されます。

これを使用して、ポリシーの比較の保存、コピー、出力、共有を行って、さらに検証することができます。

アクセス コントロール ポリシー比較ビューの使用

ライセンス：任意

比較ビューには、両方のポリシーが左右に並べて表示されます。それぞれのポリシーは、比較ビューの左右のタイトルバーに示される名前で特定されます。現在実行されている設定ではない 2 つのポリシーを比較する場合、最後に変更された日時とその変更を行ったユーザがポリシー名と共に表示されます。

2 つのポリシー間の違いは次のように強調表示されます。

- 青色は強調表示された設定が2つのポリシーで異なることを示し、差異は赤色で示されます。
- グリーンは、強調表示されている設定項目が一方のポリシーに含まれ、もう一方のポリシーには含まれないことを示します。

次の表に、実行できる操作を記載します。

表 *17*：アクセス コントロール ポリシー比較ビューの操作

目的	操作
変更に個別にナビゲートする	またはタイトルバーの上にある [Previous] または [Next] をクリックします。 左側と右側の間にある二重矢印アイコン（）が移動し、[Difference] 番号が調整されて、表示中の差異が示されます。

目的	操作
新しいポリシー比較ビューを生成する	[New Comparison] をクリックします。 [Select Comparison] ウィンドウが表示されます。詳細については、「アクセス コントロール ポリシー比較レポートの使用（100 ページ）」を参照してください。
ポリシー比較レポートを生成する	[Comparison Report] をクリックします。 ポリシー比較レポートは、2 つのポリシーの間の差異だけをリストした PDF ドキュメントです。

アクセス コントロール ポリシー比較レポートの使用

ライセンス：任意

アクセス コントロール ポリシー比較レポートとは、ポリシー比較ビューで識別された、2 つのアクセス コントロール ポリシーの間、またはポリシーと現在適用中のポリシーの間にあるすべての差異を、PDF 形式で記録したものです。このレポートを使用することで、2 つのポリシー設定の間の違いをさらに調べ、調査結果を保存して共有できます。

ユーザは、アクセス権限が与えられている任意のポリシーの比較ビューから、アクセス コントロール ポリシー比較レポートを生成できます。ポリシー レポートを生成する前に、必ずすべての変更を保存してください。レポートには、保存されている変更だけが表示されます。

ポリシー比較レポートの形式は、ポリシー レポートと同様です。唯一異なる点は、ポリシー レポートにはポリシーのすべての設定が記載される一方、ポリシー比較レポートにはポリシー間で異なる設定だけがリストされることです。アクセス コントロール ポリシー比較レポートには、「現在のアクセス コントロール設定のレポートの生成」で説明されているセクションが含まれています。

ヒント 同様の手順を使用して、SSL、ネットワーク分析ポリシー、侵入ポリシー、ファイル ポリシー、またはシステム ポリシーを比較できます。

2 つのアクセス コントロール ポリシーを比較する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。

[Access Control Policy] ページが表示されます。

ステップ 2 [Compare Policies] をクリックします。

[Select Comparison] ウィンドウが表示されます。

ステップ 3 [Compare Against] ドロップダウン リストから、比較するタイプを次のように選択します。

- 異なる 2 つのポリシーを比較するには、[Other Policy] を選択します。

ページが更新されて、[Policy A] と [Policy B] という 2 つのドロップダウン リストが表示されます。

- 現在アクティブなポリシーと別のポリシーを比較するには、[Running Configuration] を選択します。

ページが更新されて、[Target/Running Configuration A] と [Policy B]という 2 つのドロップダウンリストが表示されます。

ステップ 4 選択した比較タイプに応じて、次のような選択肢があります。

- 2 つの異なるポリシーを比較する場合、[Policy A] ドロップダウン リストと [Policy B] ドロップダウン リストから比較するポリシーを選択します。
- 現在実行されている設定を別のポリシーと比較する場合は、[Policy B] ドロップダウン リストから 2 つ目のポリシーを選択します。

ステップ 5 ポリシー比較ビューを表示するには、[OK] をクリックします。

比較ビューが表示されます。

ステップ 6 必要に応じて、アクセス コントロール ポリシー比較レポートを生成するには [Comparison Report] をクリックします。

アクセス コントロール ポリシー比較レポートが表示されます。コンピュータにレポートを保存するように求められます。

アクセス コントロール ポリシーでの詳細設定の使用

通常、アクセス コントロール ポリシーの詳細設定を変更する必要はほとんど、あるいはまったくありません。デフォルト設定は、ほとんどの展開環境に適しています。アクセス コントロール ポリシーでの前処理およびパフォーマンスの詳細オプションの多くは、ルールの更新で変更される場合があることに注意してください。

一般設定

ユーザが要求した各 URL に対し、ASA FirePOWER モジュール データベースに保存する文字数をカスタマイズするには、接続で検出された URL のロギング（481 ページ）を参照してください。

ユーザが最初のブロックをバイパスした後に Web サイトを再度ブロックするまでの時間間隔をカスタマイズするには、ユーザが URL ブロックをバイパスすることを許可する （155 ページ） を参照してください。

ネットワーク分析ポリシーと侵入ポリシー

ネットワーク分析ポリシーおよび侵入ポリシーの詳細設定によって、以下が可能になります。

- システムがトラフィックを検査する方法を正確に決定する前に、最初にそのトラフィックを検査するために使用される、アクセス コントロール ポリシーのデフォルトの侵入ポリシーと関連付けられている変数セットの変更。
- 多くの前処理オプションを制御する、アクセス コントロール ポリシーのデフォルト ネットワーク分析ポリシーの変更。
- カスタム ネットワーク分析ルールおよびネットワーク分析ポリシーを使用した、特定のセキュリティ ゾーンおよびネットワークに対する前処理オプションの調整。

ファイルおよびマルウェアの設定

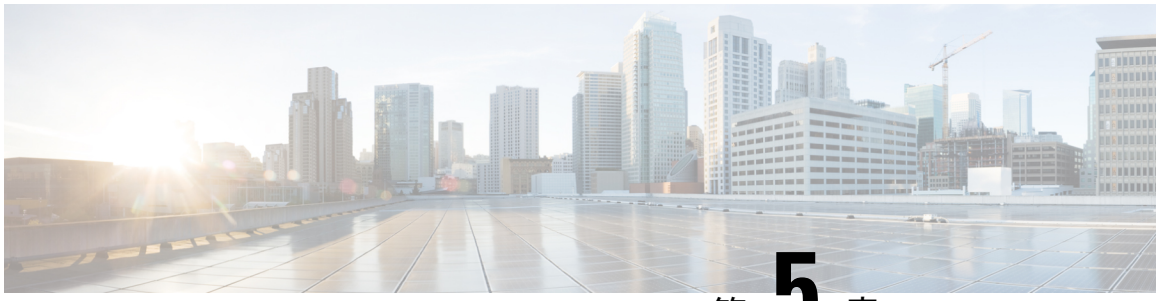
ファイルおよびマルウェアの詳細設定では、ファイル制御および高度なマルウェア防御のためのパフォーマンス オプションを設定できます。詳細については、許可されたトラフィックに対する侵入およびマルウェアの有無のインスペクション （172 ページ）を参照してください。

トランスポート層とネットワーク層のプリプロセッサの設定

トランスポートおよびネットワークのプリプロセッサの詳細設定は、アクセス コントロール ポリシーを適用するすべてのネットワーク、ゾーン、および VLAN にグローバルに適用されます。高度なプリプロセッサの詳細については、お使いのバージョンの *Firepower Management Center* コンフィギュレーション ガイドの「Advanced NetworkAnalysis and Preprocessing」を参照してください。

パフォーマンス設定および遅延ベースのパフォーマンス設定

パケットおよび侵入ルール遅延しきい値の設定 （181 ページ） では、侵入行為についてトラフィックを分析する際のシステムのパフォーマンスを向上させるための情報を提供しています。



第 5 章

セキュリティ インテリジェンスの IP アドレス レピュテーションを使用したトラフィックのブロック

悪意のあるインターネットコンテンツに対する第一の防衛ラインとして、ASA FirePOWER モジュールにはセキュリティインテリジェンス機能があります。この機能により、最新のレピュテーションインテリジェンスに基づいて接続を直ちにブロックすることができ、リソースを集中的に使用する詳細な分析が不要になります。セキュリティインテリジェンスのフィルタリングを行うには、Protection ライセンスが必要です。

セキュリティ インテリジェンスは、既知の好ましくないレピュテーションが含まれる IP アドレスを送信元/宛先とするトラフィックをブロックすることにより機能します。このトラフィック フィルタリングは、他のどのポリシーベースのインスペクション、分析、またはトラフィック処理よりも前に行われます。

IP アドレスでトラフィックを手動で制限することで、セキュリティ インテリジェンス フィルタリングと同様の機能を実行するアクセス コントロール ルールを作成することができます。ただし、アクセス コントロール ルールは対象範囲が広く、設定の難易度が高いだけでなく、動的フィードを使用した自動更新に対応できません。

セキュリティインテリジェンスによってブロックされたトラフィックは直ちにブロックされるため、他のさらなる（侵入、エクスプロイト、マルウェアなどの）インスペクションの対象にはなりません。オプションで、セキュリティ インテリジェンス フィルタリングには「モニタ専用」設定を使用できます。パッシブ展開環境では、この設定が推奨されます。この設定では、ブロックされたであろう接続をシステムが分析できるだけでなく、ブロックリストに一致する接続がログに記録され、接続終了セキュリティ インテリジェンス イベントが生成されます。

便宜上、 シスコではインテリジェンス フィードを提供しています。インテリジェンス フィードは、VRT によってレピュテーションが低いと判断された、複数の定期的に更新される IP アドレスのコレクションで構成されます。インテリジェンス フィードは、オープン リレー、既知の攻撃者、偽の IP アドレス（bogon）などを追跡します。この機能を組織の固有のニーズに適するようにカスタマイズできます。例を次に示します。

- サードパーティ フィード：インテリジェンス フィードをサードパーティのレピュテーション フィードで補足できます。それらのフィードはシスコのフィードと同様に自動的に更新できます。
- カスタムブロックリスト：ユーザのニーズに応じてさまざまな方法で特定の IP アドレスを手動でブロックできます。
- セキュリティゾーン別のブロックの適用：パフォーマンスを向上させるために、電子メールトラフィックを処理するゾーンにスパムのブロックを制限するなどして、適用対象を絞れます。
- ブロックに代わるモニタリング：特にパッシブ展開や、実装前にフィードをテストする場合に便利です。違反しているセッションをブロックする代わりにモニタするだけで、接続終了イベントを生成できます。
- 誤検出をなくすためのブロックなしリストの使用：ブロックリストの範囲が広すぎる場合、または（たとえば、重要なリソースに）許可するトラフィックを誤ってブロックした場合、ブロックリストをカスタムブロックなしリストでオーバーライドできます。

- セキュリティ インテリジェンス戦略の選択 （104 ページ）
- セキュリティ インテリジェンスのブロックリストとブロックしないリストの作成 （106 ページ）

セキュリティ インテリジェンス戦略の選択

ライセンス：Protection

ブロックリストを作成する最も簡単な方法は、オープンリレーとなることが分かっている IP アドレス、既知の攻撃者、不正な IP アドレス（bogon）などを追跡するインテリジェンスフィードを使用することです。インテリジェンス フィードは定期的に更新されるため、インテリジェンス フィードを使用することで、システムは最新の情報を使用してネットワーク トラフィックをフィルタ処理できます。ただし、セキュリティに対する脅威（マルウェア、スパム、ボットネット、フィッシングなど）を表す不正な IP アドレスが現れては消えるペースが速すぎて、新しいポリシーを更新して適用するには間に合わないこともあります。

したがって、インテリジェンス フィードを補完するために、次の場合にサードパーティの IP アドレスのリストとフィードを使用してセキュリティ インテリジェンス フィルタリングを実行できるようになっています。

- リストとは、ASA FirePOWER モジュールにアップロードする IP アドレスの静的リストのことです。
- フィードとは、 ASA FirePOWER モジュールが定期的にインターネットからダウンロードする、IP アドレスの動的リストのことです。インテリジェンス フィードは特殊なタイプのフィードです。

インターネット アクセス要件を含め、セキュリティ インテリジェンスのリストとフィードを設定する方法の詳細については、セキュリティ インテリジェンス リストとフィードの操作（27 ページ）を参照してください。

セキュリティ インテリジェンスのグローバルブロックリストの使用

分析中に、グローバルブロックリストを作成できます。たとえば、エクスプロイトの試行に関連した侵入イベントでルーティング可能な IP アドレスのセットに気づいた場合、それらの IP アドレスをブロックリストに追加することができます。ASA FirePOWER モジュールは、すべてのアクセス コントロール ポリシーでこのグローバルブロックリスト（および関連するグローバルブロックなしリスト）を使用してセキュリティ インテリジェンス フィルタリングを行います。これらのグローバル リストを管理する方法の詳細については、グローバルブロックなしリストとブロックリストの操作 （29 ページ）を参照してください。

（注） グローバルブロックリスト（またはグローバルブロックなしリスト。以下を参照）のフィードの更新および追加では、展開環境全体にわたって自動的にその変更が実装されますが、セキュリティ インテリジェンス オブジェクトに対するその他の変更には、アクセス コントロール ポリシーの再適用が必要になります。

ネットワーク オブジェクトの使用

さらに、ブロックリストを作成するもう 1 つの簡単な方法として、IP アドレス、IP アドレス ブロック、あるいは IP アドレスのコレクションを表すネットワークオブジェクトまたはネットワーク オブジェクト グループ を使用することもできます。ネットワーク オブジェクトの作成および変更の詳細については、ネットワーク オブジェクトの操作 （26 ページ）を参照してください。

セキュリティ インテリジェンスのブロックなしリストの使用

ブロックリストに加え、各アクセス コントロール ポリシーにはブロックなしリストが関連付けられます。これらには、セキュリティ インテリジェンス オブジェクトを取り込むことができます。ポリシーでは、ブロックなしリストがブロックリストをオーバーライドします。つまり、システムは、ブロックなしリストに登録されている送信元または宛先の IP アドレスを、そのIPアドレスがブロックリストにも登録されているとしても、アクセス制御ルールを使用して評価します。通常、ブロックリストがまだ有用であっても、その適用範囲があまりにも広く、インスペクション対象のトラフィックを誤ってブロックする場合には、ブロックなしリストを使用してください。

たとえば、信頼できるフィードにより、重要なリソースへのアクセスが不適切にブロックされても、そのフィードが全体としては組織にとって有用である場合は、そのフィード全体をブロックリストから削除するのではなく、不適切に分類された IP アドレスのみをブロックなしリストに追加するという方法を取ることができます。

セキュリティ ゾーンを基準としたセキュリティ インテリジェンス フィルタリングの適用

さらに細かく制御するには、接続の送信元または宛先 IP アドレスが特定のセキュリティ ゾーン内にあるかどうかに基づいて、セキュリティ インテリジェンス フィルタリングを適用することができます。

上述のブロックなしリストの例を拡張するには、不適切に分類された IP アドレスをブロックなしリストに追加した後、組織でそれらの IP アドレスにアクセスする必要があるユーザが使用しているセキュリティゾーンを使用して、オブジェクトを制限するという方法が考えられます。この方法では、ビジネスニーズを持つユーザだけが、それらの IP アドレスにアクセスできます。別の例として、サードパーティのスパムフィードを使用して、電子メールサーバのセキュリティゾーンのトラフィックをブロックすることができます。

接続のモニタリング（ブロッキングではなく）

特定の IP アドレスまたは一連のアドレスをブロックする必要があるかどうかわからない場合は、「モニタのみ」の設定を使用できます。この設定では、システムが一致する接続をアクセス制御ルールに渡せるだけでなく、ブロックリストと一致する接続がログに記録され、接続終了セキュリティインテリジェンスイベントが生成されます。注意点として、グローバルブロックリストをモニタのみに設定することはできません。

たとえば、サードパーティのフィードを使用したブロッキングを実装する前に、そのフィードをテストする必要があるとします。フィードをモニタ専用に設定すると、ブロックされるはずの接続をシステムで詳細に分析できるだけでなく、そのような接続のそれぞれをログに記録して、評価することもできます。

パッシブ展開環境では、パフォーマンスを最適化するために、Cisco では常にモニタ専用の設定を使用することを推奨しています。パッシブに展開されたデバイスはトラフィック フローに影響を与える可能性がないため、トラフィックをブロックするようにシステムを構成しても何のメリットもありません。また、ブロックされた接続はパッシブ展開で実際にはブロックされないため、システムにより、ブロックされた各接続に対し複数の接続開始イベントが報告される場合があります。

セキュリティ インテリジェンスのブロックリストとブロックしないリストの作成

ライセンス：Protection

ブロックリストとホワイトリストを作成するには、ネットワークオブジェクトとグループの任意の組み合わせに加え、セキュリティゾーン別に制約できるセキュリティインテリジェンスのフィードとリストを入力します。

デフォルトでは、アクセスコントロールポリシーは、任意のゾーンに適用する ASA FirePOWER モジュールのグローバルブロックしないリストおよびブロックリストを使用します。これらのリストは、アナリストによって入力されます。ポリシーのそれぞれについて、これらのグローバル リストを使用しないように選択することができます。

（注） 入力したグローバル ブロックしないリストとブロックリストを使用するアクセス コントロール ポリシーは Protection ライセンスのないデバイスには適用できません。いずれかのグローバル リストに IP アドレスを追加した場合は、ポリシーのセキュリティ インテリジェンス設定から空でないリストを削除**してからでないと**、ポリシーを適用できません。詳細については、グローバルブロックなしリストとブロックリストの操作 （29 ページ）を参照してください。

ブロックしないリストとブロックリストを作成した後は、ブロックした接続をログに記録できます。また、フィードとリストを含めてブロックした個々のオブジェクトをモニタのみに設定することもできます。これにより、システムはアクセス制御を使用してブロックした IP アドレスを含む接続を処理できるだけでなく、ブロックリストと一致する接続をログイに記録することもできます。

ブロックなしリスト、ブロックリスト、およびロギングのオプションを設定するには、アクセス コントロール ポリシーの [Security Intelligence] タブを使用します。このページには、ブロックなしリストまたはブロックリストのいずれかで使用できるオブジェクトのリスト（[Available Objects]）と、ブロックなしリストとブロックリストのオブジェクトの制約に使用できるゾーンのリスト（[Available Zones]）が表示されます。オブジェクトまたはゾーンのタイプは、異なるアイコンによって見分けられるようになっています。シスコのアイコンでマークされたオブジェクトは、インテリジェンス フィードの各種カテゴリを表します。

ブロックリストでは、ブロックするように設定されたオブジェクトはブロックアイコンでマークされ、モニタのみのオブジェクトはモニタアイコンでマークされます。ブロックなしリストがブラックリストをオーバーライドするため、両方のリストに同じオブジェクトを追加すると、ブロックリストに登録されたオブジェクトに取り消し線が表示されます。

ブロックなしリストとブロックリストには、最大 255 個のオブジェクトを追加できます。つまり、ブロックなしリストのオブジェクトとブロックリストのオブジェクトを合計した数は 255 以下でなければなりません。

ネットマスク /0 のネットワークオブジェクトはブロックなしリストまたはブロックリストに追加できますが、ネットマスク /0 を使用したアドレスブロックは無視され、これらのアドレスに基づいたブロックなしリストおよびブロックリストフィルタリングは行われないことに注意してください。セキュリティ インテリジェンス フィードからのネットマスク /0 のアドレスブロックも無視されます。すべてのトラフィックを監視またはブロックする場合は、セキュリティ インテリジェンス フィルタリングの代わりに、[Monitor] または [Block] ルール アクションでアクセス コントロール ルールを使用し、[Source Networks] および [Destination Networks] の [any] のデフォルト値をそれぞれ使用します。

アクセス コントロール ポリシーのセキュリティ インテリジェンスのブロックなしリストおよびブロックリストを作成する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。

[Access Control Policy] ページが表示されます。

ステップ 2 設定するアクセス コントロール ポリシーの横にある編集アイコンをクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3 [Security Intelligence] タブを選択します。

アクセス コントロール ポリシーのセキュリティ インテリジェンス設定が表示されます。

ステップ 4 必要に応じて、ブロックされた接続をログに記録するには、ロギングアイコンをクリックします。

ロギングを有効にしてからでないと、ブロックされたオブジェクトをモニタのみに設定することはできません。詳細については、セキュリティ インテリジェンスによる判断のロギング （475 ページ）を参照してください。

ステップ 5 1 つ以上の使用可能なオブジェクトを選択して、ブロックなしリストとブロックリストの作成を開始します。

Ctrl キーまたは Shift キーを押しながらクリックして複数のオブジェクトを選択し、右クリックして [Select All] を選択します。

ヒント リストに含める既存のオブジェクトを検索できます。組織のニーズを満たす既存のオブジェクトがない場合は、その場でオブジェクトを作成することもできます。詳細については、ブロックなしリストまたはブロックリストに追加するオブジェクトの検索 （109 ページ）を参照してください。

ステップ 6 オプションで、**使用可能なゾーン**を選択して、ゾーン別に選択したオブジェクトを制約します。

デフォルトでは、オブジェクトに制約はありません。つまり、オブジェクトのゾーンは [Any] に設定されます。[Any] を使用しない場合、制約の基準にできるゾーンは 1 つだけです。複数のゾーンでオブジェクトのセキュリティ インテリジェンス フィルタリングを適用するには、ゾーンごとにオブジェクトをブロックなしリストまたはブロックリストに追加する必要があります。また、グローバルブロックなしリストまたはブロックリストをゾーンによって制約することはできません。

ステップ 7 **[Add to Do-Not-Block List]** または **[Add to Block List]** をクリックします。

また、オブジェクトをクリックして選択し、いずれかのリストにドラッグすることもできます。

選択したオブジェクトは、ブロックなしリストまたはブロックリストに追加されます。

ヒント オブジェクトをリストから削除するには、そのオブジェクトの削除アイコンをクリックします。Ctrl キーまたは Shift キーを押しながらクリックして複数のオブジェクトを選択するか、または右クリックして [Select All]]を選択した後、右クリックして [Delete Selected] を選択します。グローバル リストを削除する場合は、選択した操作を確認する必要があります。ブロックなしリストまたはブロックリストからオブジェクトを削除しても、そのオブジェクトは ASA FirePOWER モジュールからは削除されません。

ステップ 8 オブジェクトをブロックなしリストまたはブロックリストに追加し終わるまで、ステップ ステップ 5 ～ ステップ 7 を繰り返します。

ステップ 9 必要に応じて、ブロックされたオブジェクトをモニタのみに設定するには、**[Add to Block List]** で該当するオブジェクトを右クリックし、[Monitor-only (do not block)] を選択します。

パッシブ展開環境の場合は、ブロックされたすべてのオブジェクトをモニタのみに設定することを推奨します。ただし、グローバルブロックリストをモニタのみに設定することはできません。

ステップ 10 [Store ASA FirePOWER Changes] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（設定変更の導入（92 ページ）を参照してください）。

ブロックなしリストまたはブロックリストに追加するオブジェクトの検索

ライセンス：Protection

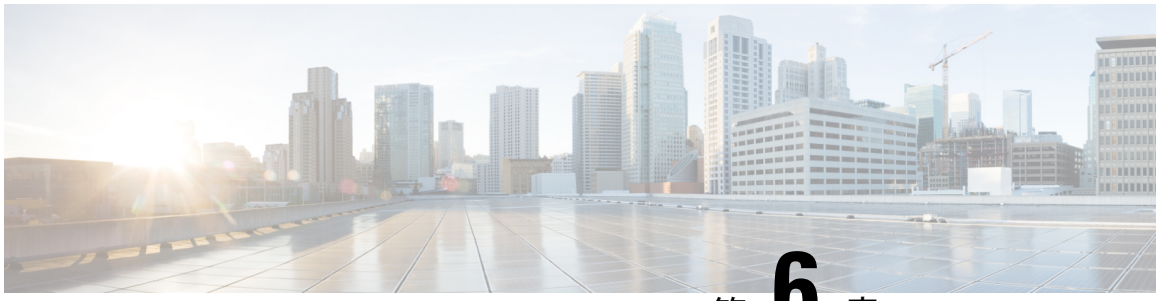
複数のネットワークオブジェクト、グループ、フィード、およびリストを使用する場合は、検索機能を使用して、ブロックなしリストまたはブロックリストに追加するオブジェクトを絞り込むことができます。

リストに追加するオブジェクトを検索する方法：

[Search by name or value] フィールドにクエリを入力します。

入力すると、[Available Objects] リストが更新されて、一致する項目が表示されます。検索文字列をクリアするには、検索フィールドの上のリロードアイコンをクリックするか、検索フィールド内のクリアアイコンをクリックします。

ネットワーク オブジェクトの名前、またはネットワーク オブジェクトに設定されている値を基準に検索できます。たとえば、Texas Office という名前で 192.168.3.0/24 という設定値を持つ個別ネットワーク オブジェクトがあり、そのオブジェクトが US Offices というグループ オブジェクトに含まれている場合、検索文字列の一部（Tex など）または全部を入力するか、3 などの値を入力することで、両方のオブジェクトを表示できます。



第 6 章

アクセス コントロール ルールを使用したトラフィック フローの調整

アクセス コントロール ポリシーでは、アクセス コントロール ルールによってネットワーク トラフィックの詳細な処理方法が提供されます。

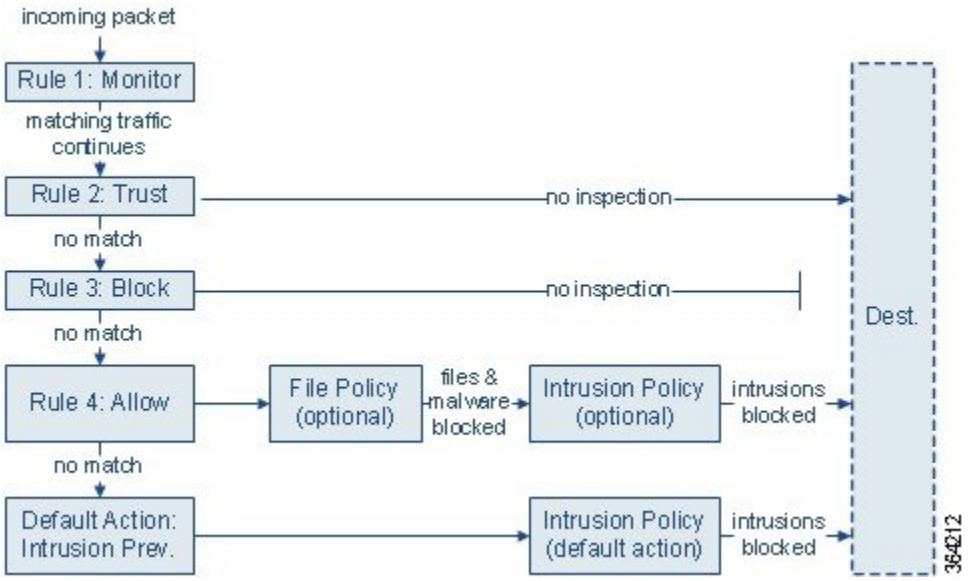
（注） セキュリティ インテリジェンス ベースのトラフィック フィルタリング、および一部の復号化と前処理は、ネットワーク トラフィックがアクセス コントロール ルールによって評価される前に行われます。また、*SSL* インスペクション機能を設定し、暗号化されたトラフィックをアクセス コントロール ルールが評価する前にブロックまたは復号化することができます。

アクセス コントロール ルールによるトラフィックの評価

システムは、指定した順にアクセス コントロール ルールをトラフィックと照合します。ほとんどの場合、システムは、すべてのルールの条件がトラフィックに一致する場合、最初のアクセス コントロール ルールに従ってネットワーク トラフィックを処理します。条件は単純または複雑にできます。セキュリティ ゾーン、ネットワークまたは地理的位置、ポート、アプリケーション、要求された URL、およびユーザごとにトラフィックを制御できます。

各ルールには、一致するトラフィックをモニタ、信頼、ブロック、または許可するかどうかを決定するアクションも含まれています。トラフィックを許可するときは、システムが侵入ポリシーまたはファイル ポリシーを使用してトラフィックを最初に検査し、アセットに到達したりネットワークを出る前に、エクスプロイト、マルウェア、または禁止されたファイルをブロックするように指定できます。ただし、システムはトラフィックを信頼またはブロックした後は、追加のインスペクションを実行しません。

次のシナリオでは、インラインの侵入防御展開環境で、アクセス コントロール ルールによってトラフィックを評価できる方法を要約しています。



このシナリオでは、トラフィックは次のように評価されます。

- **ルール 1**：**モニタ**はトラフィックを最初に評価します。モニタ ルールはネットワーク トラフィックを追跡してログに記録しますが、トラフィック フローには影響しません。システムはトラフィックと追加ルールの照合を継続して、許可するか拒否するかを決定します。
- **ルール 2**：**信頼**はトラフィックを 2 番目に評価します。一致するトラフィックは、追加のインスペクションなしでその宛先への通過を許可されます。一致しなかったトラフィックは、次のルールへと進められます。
- **ルール 3**：**ブロック**はトラフィックを 3 番目に評価します。一致したトラフィックは、それ以上のインスペクションは行わずに、ブロックされます。一致しないトラフィックは、引き続き最後のルールと照合されます。
- **ルール 4**：**許可**は最後のルールです。このルールの場合、一致するトラフィックは許可されますが、そのトラフィック内の禁止されたファイル、マルウェア、侵入およびエクスプロイトは検出されてブロックされます。残りの禁止されていない悪意のないトラフィックは宛先に許可されます。ファイルインスペクションのみを実行する、または侵入インスペクションのみを実行する、もしくは両方とも実行しない追加の許可ルールを割り当てることができることに留意してください。
- **デフォルト アクション**はルールのいずれにも一致しないすべてのトラフィックを処理します。このシナリオでは、デフォルトアクションは、悪意のないトラフィックの通過を許可する前に侵入防御を実行します。別の展開では、追加のインスペクションなしですべてのトラフィックを信頼またはブロックするデフォルト アクションが存在する場合があります。（デフォルトアクションで処理されるトラフィックでは、ファイルまたはマルウェアのインスペクションを実行できません）。

アクセス コントロール ルールの作成および編集

ライセンス：任意

アクセスコントロールポリシー内で、アクセスコントロールルールはネットワークトラフィックを処理する詳細な方法を提供しています。一意の名前に加え、各アクセスコントロールルールには次の基本コンポーネントがあります。

状態

デフォルトでは、ルールが有効状態になります。無効にしたルールはネットワークトラフィックの評価には使用されなくなり、そのルールの場合の警告とエラーの生成が停止されます。

位置

アクセス コントロール ポリシー内の各ルールには、1 から始まる番号が付きます。システムは、ルール番号の昇順で上から順に、ルールをトラフィックと照合します。Monitor ルールを除き、トラフィックが最初に一致するルールが、当該トラフィックを処理するためのルールになります。

条件

条件は、ルールで処理する特定のトラフィックを指定します。条件は、セキュリティゾーン、ネットワークまたは地理的位置、ポート、アプリケーション、要求されたURL、またはユーザ別にトラフィックを照合できます。条件は単純または複雑にできます。条件の使用はライセンスによって異なります。

アクション

ルールのアクションは、一致したトラフィックの処理方法を決定します。一致するトラフィックをモニタ、信頼、ブロック、または許可（追加のインスペクションあり/なしで）することができます。システムは、信頼されたトラフィックとブロックされたトラフィックに対してインスペクションを実行**しない**ことに注意してください。

インスペクション

アクセス コントロール ルールのインスペクション オプションは、何も行われなければユーザが許可していたであろう悪意のあるトラフィックをシステムが検査およびブロックする方法を制御します。ルールを使用してトラフィックを許可するときは、システムが侵入ポリシーまたはファイル ポリシーを使用してトラフィックを最初に検査し、アセットに到達したりネットワークを出る前に、エクスプロイト、マルウェア、または禁止されたファイルをブロックするように指定できます。

ロギング

ルールのロギング設定は、システムが処理するトラフィックのレコードの維持を制御します。各ルールに一致したトラフィックのレコードを維持できます。一般に、接続の開始時および終了時にセッションをログに記録できます。接続のログは、ASA FirePOWER モジュールの他に、システム ログ（syslog）または SNMP トラップ サーバに記録できます。

注

アクセス コントロール ルールで変更を保存するたびに、コメントを追加できます。

アクセス コントロール ルールを追加および編集するには、アクセス コントロール ルール エディタを使用します。アクセス コントロール ポリシー エディタの [Rules] タブからルール エディタにアクセスします。ルール エディタで、次の操作を実行します。

- エディタの上部で、ルールの名前、状態、位置、アクションなどの基本的なプロパティを設定します。
- エディタの左下にあるタブを使用して、条件を追加します。
- インスペクションおよびロギングのオプションを設定し、さらにルールにコメントを追加するには、右下にあるタブを使用します。便宜上、どのタブを表示しているかに関係なく、エディタにはルールのインスペクションおよびロギングのオプションがリストされます。

（注） アクセス コントロール ルールの適切な作成と順序付けは複雑なタスクですが、効果的な展開を構築するためには必須なものです。慎重なポリシーの設計を怠ると、他のルールをプリエンプション処理したり、追加ライセンスが必要となったり、無効な設定を含んだルールになる可能性があります。システムが想定どおりにトラフィックを確実に処理できるように、アクセス コントロール ポリシー インターフェイスにはルールに対する強力な警告およびエラーのフィードバック システムがあります。詳細については、アクセス コントロール ポリシーとルールのトラブルシューティング （92 ページ）を参照してください。

アクセス コントロール ルールを作成または変更するには、次の手順を実行します。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。

ステップ 2 ルールの追加先にするアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

ステップ 3 次の選択肢があります。

- 新しいルールを追加するには、[Add Rule] をクリックします。
- 既存のルールを編集するには、そのルールの横にある編集アイコン（）をクリックします。

ステップ 4 規則の**名前**を入力します。

各ルールには一意の名前が必要です。30 文字までの印刷可能文字を使用できます。スペースや特殊文字を含めることができますが、コロン（:）は使用できません。

ステップ 5 前述の説明に従い、ルール コンポーネントを設定します。次の設定をするか、デフォルト設定をそのまま使用することができます。

- ルールを有効にするかどうか [Enabled] を指定します。
- ルールの位置を指定します。を参照してください。 ルールの評価順序の指定 （115 ページ）

- ルールの [Action] を指定します。ルール アクションを使用したトラフィック処理とインスペクションの決定 （119 ページ）を参照してください。
- ルールの条件を設定します。 ルールが処理するトラフィックを指定するための条件の使用 （116 ページ）
- 許可ルールおよびインタラクティブ ブロック ルールの場合は、ルールの [Inspection] オプションを設定します。 侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御 （171 ページ）を参照してください。
- [Applications] タブで、[Safe Search]（）または [YouTube EDU] アイコン（）をクリックして、コンテンツ制限の設定を行います。アイコンが淡色表示の場合、ルールに対してコンテンツ制限は無効になっています。詳細については、アクセス コントロール ルールを使用したコンテンツ制限の実施 （202 ページ）を参照してください。
- [Logging] オプションを指定します。ネットワーク トラフィックの接続のロギング （467 ページ）を参照してください。
- コメントを追加します。ルールにコメントを追加する （123 ページ） を参照してください。

ステップ 6 [Store FirePOWER Changes] をクリックしてルールを保存します

.

ルールが保存されます。削除アイコン（）をクリックすると、ルールを削除できます。変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります。を参照してください。 設定変更の導入 （92 ページ）

ルールの評価順序の指定

ライセンス：任意

最初にアクセス コントロール ルールを作成するときに、ルール エディタで [Insert] ドロップダウンリストを使用してその位置を指定します。アクセス コントロール ポリシー内の各ルールには、1 から始まる番号が付きます。システムは、ルール番号の昇順で先頭から順にアクセス コントロール ルールをトラフィックと照合します。

ほとんどの場合、システムは、すべてのルールの条件がトラフィックに一致する場合、最初のアクセス コントロール ルールに従ってネットワーク トラフィックを処理します。モニタ ルール（トラフィックをログに記録するがトラフィック フローには影響しないルール）の場合を除き、システムは、そのトラフィックがルールに一致した後、追加の優先順位の低いルールに対してトラフィックを評価し続けることは**ありません**。

ヒント　アクセス コントロール ルールの順序を適切にすることで、ネットワーク トラフィックの処理に必要なリソースが減り、ルールのプリエンプションを回避できます。ユーザーが作成するルールはすべての組織と展開に固有のものですが、ユーザーのニーズに対処しながらもパフォーマンスを最適化できるルールを順序付けする際に従うべきいくつかの一般的なガイドラインがあります。詳細については、パフォーマンスを向上させプリエンプションを回避するためのルールの順序付け （96 ページ）を参照してください。

ルールは数値で順序付けするだけでなく、カテゴリ別にグループ化することもできます。デフォルトで、システムには3つのカテゴリ（管理者、標準、ルート）があります。カスタム カテゴリを追加できますが、 シスコ提供のカテゴリは削除したり、順序を変更したりできません。既存のルールの位置またはカテゴリの変更の詳細については、を参照してください。ルールの位置またはカテゴリの変更 （127 ページ）

ルールの編集や作成中にルールをカテゴリに追加する手順：

アクセス コントロール ルール エディタで、[Insert] ドロップダウンリストから [Into Category] を選択し、使用するカテゴリを選択します。

ルールを保存すると、そのカテゴリの最後に配置されます。

ルールの評価順序の指定

ルールの編集や作成中にルールの位置を数値で指定する手順：

アクセス コントロール ルール エディタで、[Insert] ドロップダウンリストから [above rule] または [below rule] を選択し、適切なルール番号を入力します。

ルールを保存すると、指定した場所に配置されます。

ルールが処理するトラフィックを指定するための条件の使用

ライセンス：機能に応じて異なる

アクセス コントロール ルールの条件によって、ルールが処理するトラフィックのタイプが識別されます。条件は単純または複雑にできます。セキュリティ ゾーン、ネットワークまたは地理的位置、ポート、アプリケーション、要求されたURL、およびユーザごとにトラフィックを制御できます。

条件をアクセス コントロール ルールに追加する場合は、次の点に注意してください。

- 1つのルールにつき複数の条件を設定できます。ルールがトラフィックに適用されるには、トラフィックがそのルールの**すべての**条件に一致する必要があります。たとえば、特定のホストのURLフィルタリング（URL条件）を実行する単一のルールを使用できます（ゾーンまたはネットワーク条件）。
- ルールの条件ごとに、最大 50 の基準を追加できます。条件の基準の**いずれかに**一致するトラフィックはその条件を満たします。たとえば、単一のルールを使用して、最大 50 のユーザおよびグループのユーザ制御を実行できます。

最大 50 の送信元の基準と最大 50 の宛先の基準を使用して、送信元と宛先ごとにゾーンおよびネットワークの条件を制約できます。送信元基準と宛先基準の両方をゾーンまたはネットワーク条件に追加する場合、一致するトラフィックは指定された送信元ゾーン/ネットワークの 1 つから発生し、宛先ゾーン/ネットワークの 1 つを通って出力する必要があります。つまり、システムは、同じタイプの複数の条件基準を OR 演算でリンクし、複数の条件タイプを AND 演算でリンクします。たとえば、次のようなルール条件の場合、

```
Source Networks: 10.0.0.0/8, 192.168.0.0/16
Application Category: peer to peer
```

ルールは、プライベートな IPv4 ネットワークの 1 つでホストからのピアツーピア アプリケーション トラフィックを照合します。パケットはいずれか一方**または**他の送信元ネットワークから発生し、ピアツーピア アプリケーション トラフィックを表す必要があります。次の接続の両方がルールをトリガーします。

```
10.42.0.105 to anywhere, using LimeWire
192.168.42.105 to anywhere, using Kazaa
```

ルールに対し特定の条件を設定しない場合、システムはその基準に基づいてトラフィックを照合しません。たとえば、ネットワーク条件を持つがアプリケーション条件を持たないルールは、セッションで使用されるアプリケーションに関係なく、送信元または宛先に基づいてトラフィックを評価します。

（注） アクセス コントロール ポリシーを適用すると、システムはすべてのルールを評価し、ネットワーク トラフィックを評価するために ASA FirePOWER モジュールが使用する条件の拡張セットを作成します。複雑なアクセス コントロール ポリシーおよびルールは、重要なリソースを消費する可能性があります。アクセス コントロール ルールを簡素化するヒントと、パフォーマンスを改善する他の方法については、 を参照してください。 アクセス コントロール ポリシーとルールのトラブルシューティング （92 ページ）

アクセス コントロール ルールを追加または編集するときは、ルール エディタの左下にあるタブを使用してルール条件を追加および編集します。次の表に、追加できる条件のタイプを示します。表のタイトル：アクセス コントロール ルール条件のタイプ

条件	照合されるトラフィック	詳細
ゾーン	特定のセキュリティ ゾーンにあるインターフェイスを経由したデバイスへの着信または発信	セキュリティ ゾーンとは、展開やセキュリティ ポリシーに従って 1 つまたは複数のインターフェイスを論理的にグループ化したものです。ゾーン条件の作成については、を参照してください。 セキュリティ ゾーンによるトラフィックの制御 （130 ページ）
ネットワーク	その送信元または宛先の IP アドレス、国、または大陸による	明示的に IP アドレスまたはアドレス ブロックを指定できます。位置情報の機能では、送信元または宛先となる国や大陸を基準にしたトラフィック制御もできます。ネットワーク条件の作成については、を参照してください。 ネットワークまたは地理的位置によるトラフィックの制御 （131 ページ）
ポート	送信元ポートまたは宛先ポート	TCP および UDP の場合、トランスポート層プロトコルに基づいてトラフィックを制御できます。ICMP および ICMPv6（IPv6 ICMP）の場合、インターネット層プロトコルと、オプションのタイプおよびコードに基づいてトラフィックを制御できます。ポート条件を使用して、ポートを使用しない他のプロトコルでトラフィックを制御することもできます。ポート条件の作成については、を参照してください。 ポートおよび ICMP コードによるトラフィックの制御 （134 ページ）
アプリケーション	セッションで検出されるアプリケーション	基本的な特性であるタイプ、リスク、ビジネス関連性、カテゴリ、タグに応じて、個々のアプリケーションへのアクセスやフィルタ アクセスを制御できます。アプリケーション条件の作成については、を参照してください。 アプリケーション トラフィックの制御 （140 ページ）
URL	セッションで要求された URL による	ネットワーク上のユーザが個別にまたは URL の一般的な分類とリスク レベルに基づいてアクセスできる Web サイトを制限できます。URL 条件の作成については、を参照してください。 URL のブロッキング （147 ページ）
ユーザ	セッションに参加しているユーザ	モニタ対象セッションに参加するホストにログインした LDAP ユーザに基づいてトラフィックを制御できます。Microsoft Active Directory サーバから取得された個別ユーザまたはグループに基づいてトラフィックを制御できます。 アクセス コントロール ルール：レルムとユーザ（161 ページ）を参照してください。

任意のライセンスを使ってアクセス コントロール ルールを作成できますが、ルール条件によっては、ポリシーを適用する前に、特定のライセンス機能を有効にする必要があることに注意し

てください。詳細については、アクセス コントロールのライセンス要件 （81 ページ）を参照してください。

ルールアクションを使用したトラフィック処理とインスペクションの決定

ライセンス：任意

すべてのアクセス コントロール ルールには、一致するトラフィックについて次のことを決定するアクションがあります。

- 処理：まず第一に、ルールアクションは、システムがルールの条件に一致するトラフィックをモニタ、信頼、ブロック、または許可するかどうかを制御します。
- インスペクション：特定のルール アクションでは、適切にライセンス付与されている場合、通過を許可する前に一致するトラフィックをさらに検査することができます。
- ロギング：ルールアクションによって、一致するトラフィックの詳細をいつ、どのようにログに記録できるかが決まります。

アクセス コントロール ポリシーのデフォルト アクションは、モニタ アクセス コントロール ルール以外のどの条件にも一致しないトラフィックを処理します（デフォルトの処理の設定およびネットワーク トラフィックのインスペクション （83 ページ）を参照）。

インライン展開されたデバイスのみがトラフィックをブロックまたは変更できることに留意してください。パッシブに展開されたデバイスは、トラフィックのフローを分析およびログに記録できますが、影響を与えることはありません。

モニタ アクション：アクションの延期とロギングの確保

ライセンス：任意

モニタ アクションはトラフィック フローに影響を与えません。つまり、一致するトラフィックが直ちに許可または拒否されることはありません。その代わり、追加のルールに照らしてトラフィックが照合され、許可/拒否が決定されます。モニタ ルール以外の一致する最初のルールが、トラフィック フローおよび追加のインスペクションを決定します。さらに一致するルールがない場合、システムはデフォルト アクションを使用します。

モニタ ルールの主な目的はネットワーク トラフィックのトラッキングなので、システムはモニタ対象トラフィックの接続終了イベントを自動的にログに記録します。つまり、トラフィックが他のルールに一致せず、デフォルト アクションでロギングが有効になっていない場合でも、接続はログに記録されます。詳細については、モニタされる接続のロギングについて （471 ページ）を参照してください。

信頼アクション：インスペクションなしでのトラフィックの通過

ライセンス：任意

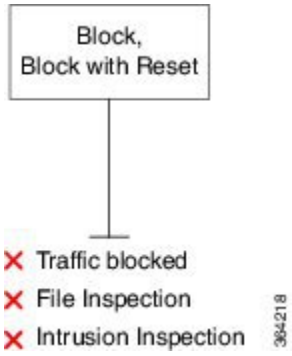
信頼アクションでは、トラフィックはいかなる種類の追加のインスペクションなしで通過を許可されます。

信頼されたネットワーク トラフィックは、接続の開始および終了の両方でログに記録できます。詳細については、信頼されている接続のロギングについて（472ページ）を参照してください。

ブロッキング アクション：インスペクションなしでトラフィックをブロック

ライセンス：任意

ブロック アクションおよび**リセット付きブロック** アクションはトラフィックを拒否し、いかなる種類の追加のインスペクションも行われません。リセット付きブロック ルールでは接続のリセットも行います。



復号化された HTTP トラフィックの場合、システムが Web 要求をブロックすると、デフォルトのブラウザまたはサーバのページを、接続が拒否されたことを説明するカスタム ページでオーバーライドできます。このカスタム ページはHTTP応答ページと呼ばれています。ブロックされた URL のカスタム Web ページの表示 （157 ページ） を参照してください。

ブロックされたネットワーク トラフィックは、接続の開始時にのみログに記録できます。インラインで展開されたデバイスのみがトラフィックをブロックできることに注意してください。ブロックされた接続はパッシブ展開で実際にはブロックされないため、システムにより、ブロックされた各接続に対し複数の接続開始イベントが報告される場合があります。詳細については、ブロックされた接続およびインタラクティブにブロックされた接続のロギングについて（472 ページ）を参照してください。

注意 サービス妨害（DoS）攻撃の間にブロックされたTCP接続をロギングすると、複数の同様のイベントによってシステム パフォーマンスが影響を受ける可能性があります。ブロック ルールに対してロギングを有効にする前に、そのルールがインターネット側のインターフェイスまたはDoS 攻撃を受けやすい他のインターフェイス上のトラフィックをモニタするかどうかを検討します。

インタラクティブ ブロッキング アクション：ユーザが Web サイト ブロックをバイパスすることを許可する

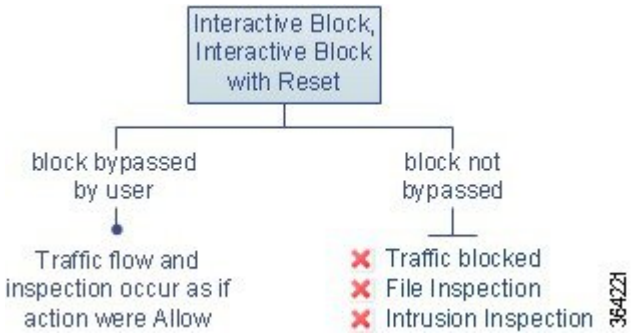
ライセンス：任意

復号化されたHTTP トラフィックの場合、[Interactive Block] アクションおよび [Interactive Block with reset] アクションを使用すると、ユーザはカスタマイズ可能な警告ページ（HTTP 応答ページと呼ばれます）をクリックスルーすることで、Web サイトのブロックをバイパスできます。リセット付きインタラクティブ ブロック ルールでは接続のリセットも行います。

Web トラフィックを復号化する SSL インスペクションを設定し、そのトラフィックがインタラクティブ ブロック ルールに一致する場合、システムは応答ページを暗号化し、再度暗号化された SSL 応答ストリームの最後にそのページを送信します。

インタラクティブにブロックされたすべてのトラフィックに対し、システムの処理、インスペクション、およびロギングは、ユーザがブロックをバイパスするかどうかによって異なります。

- ユーザがブロックをバイパスしない（できない）場合は、ルールはブロック ルールを模倣します。一致するトラフィックは追加のインスペクションなしで拒否され、接続の開始のみをロギングできます。これらの接続開始イベントには、Interactive Block または Interactive Block with Reset アクションが付きます。
- ユーザがブロックをバイパスする場合は、ルールは許可ルールを模倣します。このため、一方のタイプのインタラクティブ ブロック ルールをファイルおよび侵入ポリシーに関連付け、このユーザ許可されたトラフィックを検査できます。さらにシステムは、接続イベントの開始と終了の両方をログに記録できます。これらの接続イベントには Allow アクションが付きます



許可アクション：トラフィックの許可および検査

ライセンス：任意

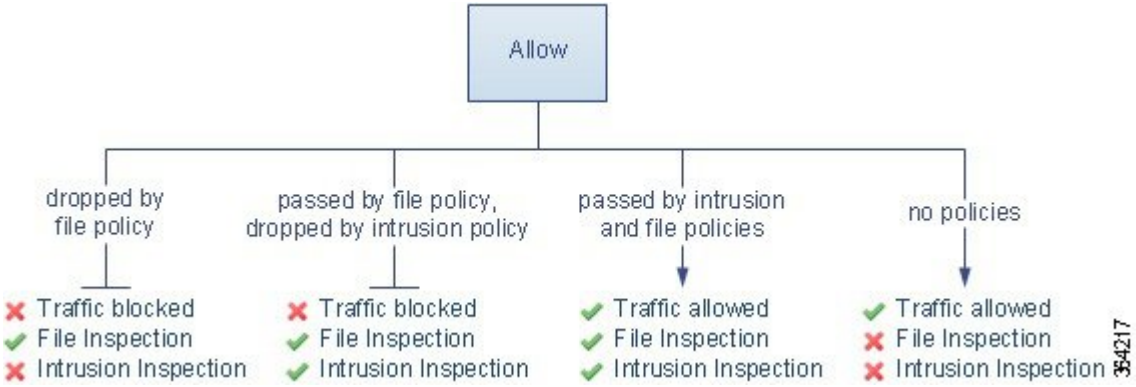
許可アクションにより、一致するトラフィックの通過が許可されます。トラフィックを許可すると、関連付けられた侵入ポリシーまたはファイル ポリシー（またはその両方）を使用して、暗号化されていないまたは復号化されたネットワーク トラフィックをさらに検査してブロックすることができます。

- Protection ライセンスを使用すると、侵入ポリシーを使用して、侵入検知および防御の設定に従ってネットワーク トラフィックを分析し、必要に応じて、有害なパケットをドロップできます。
- また、Protection ライセンスを使用すると、ファイル ポリシーを使用してファイル制御を実行できます。ファイル制御により、ユーザが特定のアプリケーション プロトコルを介して特定のタイプのファイルをアップロード（送信）またはダウンロード（受信）するのを検出およびブロックすることができます。
- Malware ライセンスを使用すると、同じくファイル ポリシーを使用して、ネットワークベースの高度なマルウェア防御（AMP）を実行できます。ネットワークベースの AMP は、マルウェアの有無についてファイルを検査し、必要に応じて検出されたマルウェアをブロックできます。

侵入ポリシーまたはファイル ポリシーをアクセス コントロール ルールに関連付ける方法については、を参照してください。侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御 （171 ページ）

下の図に、許可ルールの条件（またはユーザによりバイパスされるインタラクティブ ブロック ルール（インタラクティブ ブロッキング アクション：ユーザが Web サイト ブロックをバイパスすることを許可する （121 ページ）を参照）の条件）を満たすトラフィックに対して実行されるインスペクションの種類を示します。侵入インスペクションの前にファイル インスペクションが行われることに注意してください。そこでブロックされたファイルに対しては、侵入関連の exploit は検査されません。

単純化のために、侵入ポリシーとファイル ポリシーの両方がアクセス コントロール ルールに関連付けられている状態（またはどちらも関連付けられていない状態）のトラフィック フローを図に示しています。ただし、いずれか一方を設定して他方は設定なしにすることもできます。ファイル ポリシーがない場合、トラフィック フローは侵入ポリシーによって決定されます。侵入ポリシーがない場合、トラフィック フローはファイル ポリシーによって決定されます。



許可されたネットワーク トラフィックは、接続の開始および終了の両方でログに記録することができます。

ルールにコメントを追加する

ライセンス：任意

アクセス コントロール ルールを作成または編集するときは、コメントを追加できます。たとえば、他のユーザーのために設定全体を要約したり、ルールの変更時期と変更理由を記載することができます。あるルールの全コメントのリストを表示し、各コメントを追加したユーザーやコメント追加日を確認することができます。

ルールを保存すると、最後に保存してから追加されたすべてのコメントは読み取り専用になります。

コメントをルールに追加する方法：

ステップ 1 アクセス コントロール ルール エディタで、[Comments] タブを選択します。

[Comments] ページが表示されます。

ステップ 2 [New Comment] をクリックします。

[New Comment] ポップアップ ウィンドウが表示されます。

ステップ 3 コメントを入力し、[OK] をクリックします。

コメントが保存されます。ルールを保存するまでこのコメントを編集または削除できます。

ステップ 4 ルールを保存するか、編集を続けます。

ポリシー内のアクセス コントロール ルールの管理

ライセンス：任意

次の図に示すアクセス コントロール ポリシー エディタの [Rules] タブでは、ポリシー内のアクセス コントロール ルールを追加、編集、検索、移動、有効化、無効化、削除、または管理できます。

各ルールで、ポリシー エディタには、ルールの名前、条件の概要、ルール アクション、およびルールのインスペクションおよびロギングのオプションを示すアイコンが表示されます。その他のアイコンは、次の表で説明するように、コメント、警告、エラー、およびその他の重要な情報を表します。無効なルールはグレーで表示され、ルール名の下に [(disabled)] というマークが付きます。

表 *18*：アクセス コントロール ポリシー エディタについて

アイコン	説明	操作
	侵入インスペクション	ルールのインスペクション オプションを編集するには、アクティブな（黄色）インスペクション アイコンをクリックします（侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御 （171 ページ）を参照）。アイコンが非アクティブ（白色）の場合、そのタイプのポリシーはルールに対して選択されていません。
	ファイルおよびマルウェアのインスペクション	
	ロギング	ルールのロギング オプションを編集するには、アクティブな（青色）ロギング アイコンをクリックします（アクセス コントロールの処理に基づく接続のロギング （477 ページ）を参照）。アイコンが非アクティブ（白色）の場合、そのルールの接続ロギングは無効になっています。
	コメント	ルールにコメントを追加するには、コメント列の数字をクリックします（ルールにコメントを追加する （123 ページ）を参照）。数字は、ルールにすでに含まれているコメントの数を示しています。

アイコン	説明	操作
	warning	アクセス コントロール ポリシー エディタで [Show Warnings] をクリックすると、ポップアップ ウィンドウが表示されて、ポリシーに関するすべての警告が一覧表示されます（アクセス コントロール ポリシーとルールのトラブルシューティング （92 ページ）を参照）。
	エラー	
	情報	

アクセス コントロール ルールの管理については、以下を参照してください。

- アクセス コントロール ルールの作成および編集 （113 ページ）
- アクセス コントロール ルールの検索 （125 ページ）
- ルールのイネーブル化とディセーブル化 （126 ページ）
- ルールの位置またはカテゴリの変更 （127 ページ）

アクセス コントロール ルールの検索

ライセンス：任意

スペースおよび印刷可能な特殊文字を含む英数字文字列を使用して、アクセス コンロトール ルールのリストで一致する値を検索できます。この検索では、ルール名およびルールに追加したルール条件が検査されます。ルール条件の場合は、条件タイプ（ゾーン、ネットワーク、アプリケーションなど）ごとに追加できる任意の名前または値が検索照合されます。これには、個々のオブジェクト名または値、グループ オブジェクト名、グループ内の個々のオブジェクト名または値、およびリテラル値が含まれます。

検索文字列のすべてまたは一部を使用できます。照合ルールごとに、一致する値のカラムが強調表示されます。たとえば、 100Bao という文字列のすべてまたは一部を基準に検索すると、少なくとも、100Bao アプリケーションを追加した各ルールの [Applications] カラムが強調表示されます。100Bao という名前のルールもある場合は、[Name] カラムと [Applications] カラムの両方が強調表示されます。

1 つ前または次の照合ルールに移動することができます。ステータス メッセージには、現行の一致および合計一致数が表示されます。

複数ページのルール リストでは、どのページでも一致が検出される可能性があります。最初の一致が検出されたのが最初のページではない場合は、最初の一致が検出されたページが表示されます。最後の一致が現行の一致となっている場合、次の一致を選択すると、最初の一致が表示されます。また、最初の一致が現行の一致となっている場合、前の一致を選択すると、最後の一致が表示されます。

ルールの検索方法：

ステップ 1 検索するポリシーのアクセス コントロール ポリシー エディタで、[Search Rules] プロンプトをクリックして検索文字列を入力し、Enter を押します。検索を開始するには、Tab キーを使用するか、ページの空白部分をクリックします。

一致する値を含むルールのカラムが強調表示されます。表示されている（最初の）一致は、他とは区別できるように強調表示されます。

ステップ 2 目的のルールを探すには次の操作が利用できます。

- 照合ルールの間を移動するには、次の一致アイコン（▼）または前の一致アイコン（▲）をクリックします。
- ページを更新して、検索文字列や強調表示をクリアするには、クリア アイコン（✖）をクリックします。

ルールのイネーブル化とディセーブル化

ライセンス：任意

アクセス コントロール ルールを作成すると、デフォルトで有効になります。無効にしたルールはネットワーク トラフィックの評価には使用されなくなり、そのルールについての警告とエラーが停止されます。アクセス コントロール ポリシーでルールのリストを表示するとき、無効状態のルールはグレーで表示されますが、変更は可能です。また、ルール エディタを使用してアクセス コントロール ルールを有効化または無効化することもできます。を参照してください。 アクセス コントロール ルールの作成および編集 （113 ページ）

アクセス コントロール ルールの状態を変更するには、次の手順を実行します。

ステップ 1 有効化または無効化するルールを含むポリシーのアクセス コントロール ポリシー エディタで、ルールを右クリックして、ルールの状態を選択します。

- 非アクティブなルールをイネーブルにするには、[State] > [Enable] を選択します。
- アクティブなルールを無効にするには、[State] > [Disable] を選択します。

ステップ 2 [Store FirePOWER Changes] をクリックして、ポリシーを保存します。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります。を参照してください。 設定変更の導入 （92 ページ）

ルールの位置またはカテゴリの変更

ライセンス：任意

アクセス コントロール ルールを整理しやすくするために、すべてのアクセス コントロール ポリシーにはシステムによって提供された3つのルール カテゴリ（管理者ルール、標準ルール、ルート ルール）があります。これらのカテゴリの移動、削除、名前変更はできませんが、カスタム カテゴリの作成は可能です。

ルールの移動

ライセンス：任意

アクセス コントロール ルールの順序を適切に設定することで、ネットワーク トラフィック処理に必要なリソースを削減して、ルールのプリエンプションを回避できます。

次の手順では、アクセス コントロール ポリシー エディタを使用して 1 つ以上のルールを同時に移動する方法について説明します。ルール エディタを使用して個々のアクセス コントロール ルールを移動することもできます。を参照してください。アクセス コントロール ルールの作成および編集 （113 ページ）

規則を移動するには、次の手順を実行します。

ステップ 1 移動するルールを含むポリシーのアクセス コントロール ポリシー エディタで、各ルールの空白領域をクリックしてルールを選択します。複数のルールを選択するには、Ctrl キーと Shift キーを使用します。

選択したルールは強調表示されます。

ステップ 2 ルールを移動します。カットアンドペーストおよびドラッグアンドドロップを使用することもできます。

新しい場所にルールをカット アンド ペーストするには、選択したルールを右クリックし、[Cut] を選択します。次に、貼り付けたい位置に隣接するルールの空白部分を右クリックし、[Paste above] または [Paste below] を選択します。2 つの異なるアクセス コントロール ポリシー間ではアクセス コントロール ルールをコピー アンド ペーストできないことに注意してください。

ステップ 3 [Store FirePOWER Changes] をクリックして、ポリシーを保存します。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります。を参照してください。設定変更の導入 （92 ページ）

新しいルール カテゴリの追加

ライセンス：任意

アクセス コントロール ルールを整理しやすくするために、すべてのアクセス コントロール ポリシーにはシステムによって提供された3つのルール カテゴリ（管理者ルール、標準ルール、ルート ルール）があります。これらのカテゴリの移動、削除、名前変更はできませんが、Standard Rules と Root Rules 間でのカスタム カテゴリの作成は可能です。

カスタム カテゴリを追加すると、追加のポリシーを作成しなくても、ルールをさらに細かく編成できます。追加したカテゴリは、名前変更と削除ができます。これらのカテゴリの移動はできませんが、ルールのカテゴリ間およびカテゴリ内外への移動は可能です。

新しいカテゴリを追加するには、次の手順に従います。

ステップ 1 ルール カテゴリを追加するポリシーのアクセス コントロール ポリシー エディタで、[Add Category] をクリックします。

ヒント ポリシーにルールがすでに含まれている場合は、既存のルールの行の空白部分をクリックして、新しいカテゴリを追加する前にその位置を設定できます。既存のルールを右クリックし、[Insert new category] を選択することもできます。

[Add Category] ポップアップ ウィンドウが表示されます。

ステップ 2 [Name] に、一意のカテゴリ名を入力します。

最大 30 文字の英数字の名前を入力できます。名前には、スペース、および印刷可能な特殊文字を含めることができます。

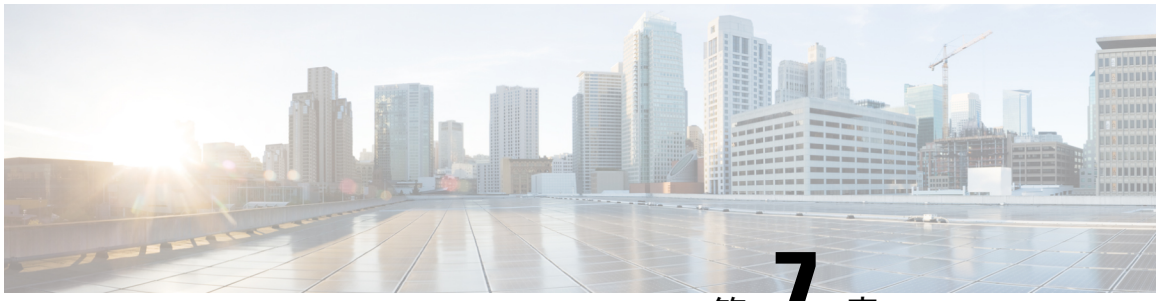
ステップ 3 次の選択肢があります。

- 既存のカテゴリのすぐ上に新しいカテゴリを配置する場合は、最初の [Insert] ドロップダウンリストから [above Category] を選択した後、2 番目のドロップダウンリストからカテゴリを選択します。ここで選択したカテゴリの上にルールが配置されます。
- 既存のルールの下に新しいカテゴリを配置する場合は、ドロップダウン リストから [below rule] を選択した後、既存のルール番号を入力します。このオプションが有効なのは、ポリシーに少なくとも 1 つのルールが存在する場合のみです。
- 既存のルールの上にルールを配置する場合は、ドロップダウン リストから [above rule] を選択した後、既存のルール番号を入力します。このオプションが有効なのは、ポリシーに少なくとも 1 つのルールが存在する場合のみです。

ステップ 4 [OK] をクリックします。

カテゴリが追加されます。カテゴリ名を編集するには、カスタム カテゴリの横にある編集アイコン（  ）をクリックします。カテゴリを削除するには、削除アイコン（  ）をクリックします。削除するカテゴリに含まれるルールは、その上にあるカテゴリに追加されます。

ステップ 5 [Store FirePOWER Changes] をクリックして、ポリシーを保存します。



第 7 章

ネットワークベースのルールによるトラフィックの制御

アクセス コントロール ポリシー内のアクセス コントロール ルールは、ネットワーク トラフィックのロギングや処理の詳細な制御を行います。ネットワークベースの条件によって、次の条件の 1 つ以上を使用してネットワークを通過するトラフィックを管理できます。

- 送信元と宛先のセキュリティ ゾーン
- 送信元と宛先の IP アドレスまたは地理的位置
- トランスポート層プロトコルおよびICMP コードオプションを含む、送信元と宛先のポート

ネットワークベースの条件を互いに組み合わせたり、他のタイプの条件と組み合わせて、アクセス コントロール ルールを作成することができます。これらのアクセス コントロール ルールは単純にも複雑にも設定でき、複数の条件を使用してトラフィックを照合および検査できます。アクセス コントロール ルールの詳細については、アクセス コントロール ルールを使用したトラフィック フローの調整 （111 ページ） を参照してください。

（注） セキュリティ インテリジェンス ベースのトラフィック フィルタリング、および一部の復号化と前処理は、ネットワーク トラフィックがアクセス コントロール ルールによって評価される**前に**行われます。また、*SSL* インスペクション機能を設定し、暗号化されたトラフィックをアクセス コントロール ルールが評価する前にブロックまたは復号化することができます。

表 *19*：ネットワークベースのアクセス コントロール ルールのライセンス要件

要件	位置情報制御	他のすべてのネットワークベースの制御
ライセンス	いずれか（Any）	いずれか（Any）

• ポートおよび ICMP コードによるトラフィックの制御 （134 ページ）

セキュリティ ゾーンによるトラフィックの制御

ライセンス：任意

アクセス コントロール ルール内のゾーン条件によって、その送信元および宛先セキュリティ ゾーン別にトラフィックを制御することができます。セキュリティ ゾーンは、1 つ以上のインターフェイスのグループです。

単純な例として、内部と外部の 2 つのゾーンを作成し、デバイスの最初のインターフェイスのペアをそれらのゾーンに割り当てることができます。内部側のネットワークに接続されたホストは、保護されている資産を表します。

このシナリオを拡張するには、追加で同様に設定されたデバイスを配置して、複数の異なるロケーションで同様のリソースを保護することができます。これらの各デバイスも、内部セキュリティ ゾーンのアセットを保護します。

ヒント 内部（または外部）のすべてのインターフェイスを 1 つのゾーンにグループ化する必要はありません。導入ポリシーおよびセキュリティ ポリシーが意味をなすグループ化を選択します。ゾーン作成の詳細については、セキュリティ ゾーンの操作 （64 ページ）を参照してください。

この展開では、これらのホストにインターネットへの無制限アクセスを提供できますが、それでもやはり、着信トラフィックで侵入およびマルウェアの有無を検査することでホストを保護したい場合があります。

アクセス コントロールを使用してこれを実現するには、[Destination Zone] が [Internal] に設定されているゾーン条件を持つアクセス コントロール ルールを設定します。この単純なアクセス コントロール ルールは、内部ゾーンの任意のインターフェイスからデバイスを離れるトラフィックを照合します。

一致するトラフィックが侵入やマルウェアについて確実に検査されるようにするには、ルール アクションとして Allow を選択し、そのルールを侵入ポリシーとファイル ポリシーに関連付けます。

より複雑なルールを作成する場合は、1 つのゾーン条件で [Source Zones] および [Destination Zones] それぞれに対し、最大 50 のゾーンを追加できます。

- ゾーン内のインターフェイスからデバイスを離れるトラフィックを照合するには、そのゾーンを [Destination Zones] に追加します。

パッシブに展開されたデバイスはトラフィックを送信しないため、パッシブなインターフェイスで構成されるゾーンを**宛先ゾーン**条件で使用することはできません。

- ゾーン内のインターフェイスからデバイスに入るトラフィックを照合するには、そのゾーンを [Source Zones] に追加します。

- 送信元ゾーン条件と宛先ゾーン条件の両方をルールに追加する場合、一致するトラフィックは指定された送信元ゾーンの 1 つから発生し、宛先ゾーンの 1 つを通って出力する必要があります。

ゾーン条件を作成する際、警告アイコンは無効な設定を示します。詳細は、アクセス コントロール ポリシーとルールのトラブルシューティング （92 ページ）を参照してください。

ゾーン別にトラフィックを制御するには、次の手順を実行します。

ステップ 1 ゾーン別にトラフィックを制御するアクセス コントロール ポリシーで、新しいアクセス コントロール ルールを作成するか、または既存のルールを編集します。

詳細な手順については、アクセス コントロール ルールの作成および編集 （113 ページ）を参照してください。

ステップ 2 ルール エディタで、[Zones] タブを選択します。

[Zones] タブが表示されます。

ステップ 3 [Available Zones] から追加するゾーンを見つけて選択します。

追加するゾーンを検索するには、[Available Zones] リストの上にある [Search by name] プロンプトをクリックし、ゾーン名を入力します。入力すると、リストが更新されて一致するゾーンが表示されます。

クリックすると、ゾーンを選択できます。複数のゾーンを選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [Select All] を選択します。

ステップ 4 [Add to Source] または [Add to Destination] をクリックして、選択したゾーンを適切なリストに追加します。

選択したゾーンをドラッグ アンド ドロップすることもできます。

ステップ 5 ルールを保存するか、編集を続けます。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（設定変更の導入 （92 ページ）を参照してください）。

ネットワークまたは地理的位置によるトラフィックの制御

ライセンス：機能に応じて異なる

アクセス コントロール ルール内のネットワーク条件によって、その送信元および宛先 IP アドレス別にトラフィックを制御することができます。次のいずれかの操作を実行できます。

- 制御するトラフィックの送信元および宛先 IP アドレスを明示的に指定します。または、

- IP アドレスを地理的位置に関連付ける位置情報機能を使用して、その送信元または宛先の国または大陸に基づいてトラフィックを制御します。

ネットワークベースのアクセス コントロール ルールの条件を作成するには、IP アドレスと地理的位置を手動で指定できます。または、名前を 1 つ以上の IP アドレス、アドレス ブロック、国、大陸などに関連付ける再利用可能なネットワーク オブジェクトおよび地理位置情報オブジェクトを使用してネットワーク条件を設定できます。

ヒント ネットワーク オブジェクトや位置情報オブジェクトを作成しておくと、それを使用してアクセス コントロール ルールを作成したり、モジュール インターフェイスのさまざまな場所で IP アドレスを表すオブジェクトとして使用したりできます。詳細については、再使用可能オブジェクトの管理 （23 ページ）を参照してください。

地理的位置別にトラフィックを制御するルールを作成する場合は、確実に最新の地理位置情報データを使用してトラフィックをフィルタ処理するために、 ASA FirePOWER モジュールで地理位置情報データベース（GeoDB）を定期的に更新することを強くお勧めします。地理情報データベースについて （595 ページ）を参照してください。

表 *20*：ネットワーク条件のライセンス要件

要件	位置情報制御	IP アドレス制御
ライセンス	いずれか（Any）	いずれか（Any）

1 つのネットワーク条件で [Source Networks] および [Destination Networks] それぞれに対し、最大 50 の項目を追加でき、ネットワークベースの設定と位置情報ベースの設定を組み合わせることができます。

- IP アドレスまたは地理的位置からのトラフィックを照合するには、[Source Networks] を設定します。
- IP アドレスまたは地理的位置へのトラフィックを照合するには、[Destination Networks] を設定します。

送信元ネットワーク条件と宛先ネットワーク条件の両方をルールに追加する場合、一致するトラフィックは指定された IP アドレスの 1 つから発生**し、**宛先 IP アドレスの 1 つに向かう必要があります。

ネットワーク条件を作成する際、警告アイコンは無効な設定を示します。詳細については、アクセス コントロール ポリシーとルールのトラブルシューティング （92 ページ）を参照してください。

ネットワーク条件により、元のクライアントに基づいてプロキシトラフィックを処理することもできます。送信元ネットワーク条件を使用してプロキシサーバを指定し、次に元のクライアント制約を追加して元のクライアント IP アドレスを指定します。システムはパケットの

X-Forwarded-For（XFF）、True-Client-IP、またはカスタム定義HTTPヘッダー フィールドを使用して、元のクライアント IP を判別します。

プロキシの IP アドレスがルールの送信元ネットワークの制約と一致する場合、トラフィックはルールに一致し、元のクライアントの IP アドレスは、ルールの元のクライアント制約に一致します。たとえば、特定の元のクライアント アドレスからのトラフィックを許可するものの、それが特定のプロキシを使用している場合のみに限定するには、以下の3つのルールを作成します。

ルール 1：特定の IP アドレス（209.165.201.1）からの非プロキシ トラフィックをブロックします。

送信元ネットワーク：209.165.201.1

元のネットワーク クライアント：none または any

アクション：ブロック

ルール 2：同じ IP アドレスからのプロキシ トラフィックを許可します。ただし、そのトラフィックのプロキシ サーバが、選択したもの（209.165.200.225 または 209.165.200.238）である場合に限ります。

送信元ネットワーク：209.165.200.225 および 209.165.200.238

元のクライアント ネットワーク：209.165.201.1

アクション：許可

ルール 3：同じ IP アドレスからのプロキシ トラフィックを、それが他のプロキシ サーバを使用する場合はブロックします。

[Source Networks]：any

元のクライアント ネットワーク：209.165.201.1

アクション：ブロック

ネットワークまたは地理的位置別にトラフィックを制御するには、次の手順を実行します。

ステップ 1 ネットワーク別にトラフィックを制御するアクセス コントロール ポリシーで、新しいアクセス コントロール ルールを作成するか、または既存のルールを編集します。アクセス コントロール ルールの作成および編集 （113 ページ）を参照してください。

ステップ 2 ルール エディタで、[Networks] タブを選択します。

ステップ 3 [Available Networks] から、次のように追加するネットワークを見つけて選択します。

- 追加するネットワーク オブジェクトとグループを表示するには [Networks] タブをクリックします。地理位置情報オブジェクトを表示するには [Geolocation] タブをクリックします。
- ネットワーク オブジェクト（後で条件に追加可能）をその場で追加するには、[Available Networks] リストの上にある追加アイコン（  ）をクリックします。ネットワーク オブジェクトの操作 （26 ページ）を参照してください。

- 追加するネットワーク オブジェクトまたは位置情報オブジェクトを検索するには、適切なタブを選択し、[Available Networks] リストの上にある [Search by name or value] プロンプトをクリックして、オブジェクト名またはオブジェクトのいずれかの値を入力します。入力を開始するとリストが更新され、一致するオブジェクトが表示されます。

オブジェクトを選択するには、そのオブジェクトをクリックします。複数のオブジェクトを選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [Select All] を選択します。

ステップ 4 プロキシ トラフィックをフィルタリングするには、以下の手順に従います。

- [Source] サブタブをクリックして、送信元ネットワーク制約を指定します。
- [Original Client] サブタブをクリックして、元のクライアント ネットワーク制約を指定します。プロキシ接続では、元のクライアントの IP アドレスは、ルールに一致するネットワークの 1 つと一致する必要があります。

ステップ 5 [Add to Source]、[Add to Original Client]、または [Add to Destination] をクリックして、選択したオブジェクトを適切なリストに追加します。

選択したオブジェクトをドラッグ アンド ドロップでリストに追加することもできます。

ステップ 6 手動で指定する送信元または宛先 IP アドレスまたはアドレス ブロックを追加します。

[送信元ネットワーク（Source Networks）] リストまたは [宛先ネットワーク（Destination Networks）] リストの下にある [IP アドレスの入力（Enter an IP address）] プロンプトをクリックし、1 つの IP アドレスまたはアドレス ブロックを入力して [追加（Add）] をクリックします。

ステップ 7 ルールを保存するか、編集を続けます。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（設定変更の導入（92 ページ）を参照してください）。

ポートおよび ICMP コードによるトラフィックの制御

ライセンス：任意

アクセス コントロール ルール内のネットワーク条件によって、その送信元および宛先ポート別にトラフィックを制御することができます。このコンテンツでは、「ポート」は次のいずれかを示します。

- TCP および UDP の場合、トランスポート層プロトコルに基づいてトラフィックを制御できます。システムは、カッコ内に記載されたプロトコル番号+オプションの関連ポートまたはポート範囲を使用してこの設定を表します。例：TCP(6)/22。
- ICMP および ICMPv6（IPv6 ICMP）の場合、インターネット層プロトコルと、オプションのタイプおよびコードに基づいてトラフィックを制御できます。例：ICMP(1):3:3
- ポートを使用しない他のプロトコルを使用してトラフィックを制御できます。

ポート ベースのアクセス コントロール ルールの条件を作成するときは、手動でポートを指定できます。または、名前を1つ以上のポートに関連付ける再利用可能なポート オブジェクトを使用してポート条件を設定できます。

ヒント ポート オブジェクトを作成しておくと、それを使用してアクセス コントロール ルールを作成したり、システムのモジュール インターフェイスのさまざまな場所でポートを表すオブジェクトとして使用したりできます。ポート オブジェクトは、オブジェクト マネージャを使用して作成するか、またはアクセス コントロール ルールの設定時にその場で作成できます。詳細については、このセクションの後半の手順を参照してください。

1 つのネットワーク条件で [Selected Source Ports] および [Selected Destination Ports] それぞれに対し、最大 50 の項目を追加できます。

- ポートからのトラフィックを照合するには、[Selected Source Ports] を設定します。

送信元ポートだけを条件に追加する場合は、異なるトランスポート プロトコルを使用するポートを追加できます。たとえば、DNS over TCP および DNS over UDP の両方を 1 つのアクセス コントロール ルールの送信元ポート条件として追加できます。

- ポートへのトラフィックを照合するには、[Selected Destination Ports] を設定します。

宛先ポートだけを条件に追加する場合は、異なるトランスポート プロトコルを使用するポートを追加できます。

- 特定の**選択した送信元ポート**から発生し、特定の**選択した宛先ポート**に向かうトラフィックを照合するには、両方設定します。

送信元ポートと宛先ポートの両方を条件に追加する場合は、単一のトランスポート プロトコル（TCP または UDP）を共有するポートのみを追加できます。たとえば、送信元ポートとして DNS over TCP を追加する場合は、宛先ポートとして Yahoo Messenger Voice Chat（TCP）を追加できますが、Yahoo Messenger Voice Chat （UDP）は追加できません。

ポート条件を作成する際は、次の点に注意します。

- タイプ 0 が設定された宛先 ICMP ポート、またはタイプ 129 が設定された宛先 ICMPv6 ポートを追加すると、アクセス コントロール ルールは要求されていないエコー応答だけを照合します。ICMP エコー要求への応答として送信される ICMP エコー応答は無視されます。ルールですべての ICMP エコーに一致させるには、ICMP タイプ 8 または ICMPv6 タイプ 128 を使用してください。
- 宛先ポート条件としてGRE（47）プロトコルを使用する場合、アクセス コントロール ルールに追加できるのは、他のネットワークベースの条件（つまりゾーンおよびネットワーク条件）のみです。レピュテーションまたはユーザ ベースの条件を追加する場合は、ルールを保存できません。

ポート条件を作成する際、警告アイコンは無効な設定を示します。たとえば、既存のポート オブジェクトをオブジェクト マネージャで編集すると、それらのオブジェクト グループを使用

するルールが無効になります。詳細については、ポート オブジェクトの操作 （33 ページ）を参照してください。

ポート別にトラフィックを制御するには、次の手順を実行します。

ステップ 1 ポート別にトラフィックを制御するアクセス コントロール ポリシーで、新しいアクセス コントロール ルールを作成するか、または既存のルールを編集します。

詳細な手順については、アクセス コントロール ルールを使用したトラフィック フローの調整 （111 ページ）を参照してください。

ステップ 2 ルール エディタで、[Ports] タブを選択します。

[Ports] タブが表示されます。

ステップ 3 [Available Ports] から、次のように追加するポートを見つけて選択します。

- ポート オブジェクト（後で条件に追加可能）をその場で追加するには、[Available Ports] リストの上にある追加アイコンをクリックします。ポート オブジェクトの操作 （33 ページ）を参照してください。
- 追加するポート オブジェクトおよびグループを検索するには、[Available Ports] リストの上にある [Search by name or value] プロンプトをクリックし、オブジェクトの名前またはオブジェクト内のポートの値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。たとえば、「80」と入力すると、ASA FirePOWER モジュールにシスコ提供の HTTP ポート オブジェクトが表示されます。

オブジェクトを選択するには、そのオブジェクトをクリックします。複数のオブジェクトを選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [Select All] を選択します。

ステップ 4 [Add to Source] または [Add to Destination] をクリックして、選択したオブジェクトを適切なリストに追加します。

選択したオブジェクトをドラッグ アンド ドロップでリストに追加することもできます。

ステップ 5 手動で指定する送信元ポートまたは宛先ポートを追加します。

- 送信元ポートの場合は、[Selected Source Ports] リストの下の [Protocol] ドロップダウンリストから [TCP] または [UDP] を選択します。次に、**ポート**を入力します。0 ～ 65535 の値を持つ 1 つのポートを指定できます。
- 宛先ポートの場合は、[Selected Destination Ports] リストの下の [Protocol] ドロップダウンリストからプロトコル（すべてのプロトコルの場合は [All]）を選択します。リストに表示されない割り当てられていないプロトコルの数字を入力することもできます。

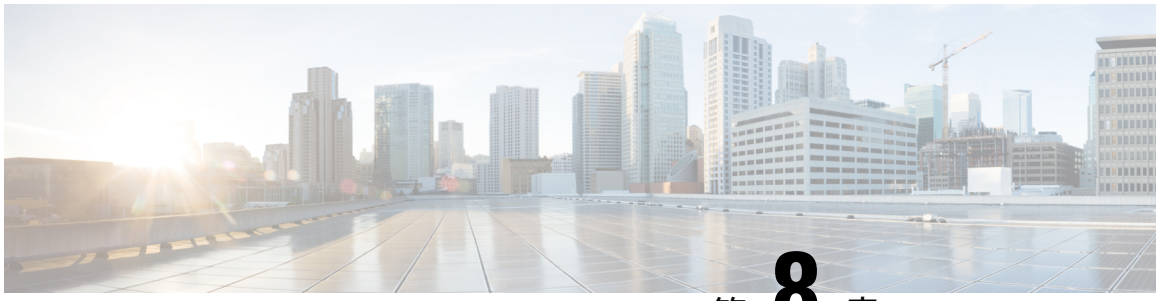
[ICMP] または [IPv6-ICMP] を選択すると、ポップアップ ウィンドウが表示され、タイプと関連するコードを選択できます。詳細については、IANA サイト ICMP types and codes または ICMP v6 types and codes を参照してください。

プロトコルを指定しない場合、またはオプションで TCP または UDP を指定した場合は、**ポート**を入力します。0 ～ 65535 の値を持つ 1 つのポートを指定できます。

[Add] をクリックします。ASA FirePOWER モジュールでは、無効な設定となるルール条件にはポートが追加されません。

ステップ 6 ルールを保存するか、編集を続けます。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（設定変更の導入（92 ページ）を参照してください）。



第 8 章

レピュテーションベースのルールによるトラフィックの制御

アクセス コントロール ポリシー内のアクセス コントロール ルールは、ネットワーク トラフィックのロギングや処理の詳細な制御を行います。アクセス コントロール ルールのレピュテーションベースの条件を使用することで、ネットワーク トラフィックを文脈によって解釈可能にし、必要に応じて制限することで、ネットワークを通過できるトラフィックを管理できます。アクセス コントロール ルールは、次のタイプのレピュテーション ベースの制御を管理します。

- アプリケーション条件を使用することで、アプリケーション制御を実行できます。これによって、個々のアプリケーションだけでなく、アプリケーションの基本的な特性であるタイプ、リスク、ビジネスとの関連性、カテゴリ、およびタグに基づいてアプリケーション トラフィックが制御されます。
- URL 条件を使用することで、URL フィルタリングを実行できます。これによって、個々の Web サイトだけでなく、Web サイトのシステムによって割り当てられたカテゴリおよびレピュテーションに基づいて Web トラフィックが制御されます。

レピュテーションベースの条件を互いに組み合わせたり、他のタイプの条件と組み合わせて、アクセス コントロール ルールを作成することができます。これらのアクセス コントロール ルールは単純にも複雑にも設定でき、複数の条件を使用してトラフィックを照合および検査できます。アクセス コントロール ルールの詳細については、アクセス コントロール ルールを使用したトラフィック フローの調整 （111 ページ） を参照してください。

（注） セキュリティ インテリジェンス ベースのトラフィック フィルタリング、および一部の復号化と前処理は、ネットワーク トラフィックがアクセス コントロール ルールによって評価される**前に**行われます。また、*SSL* インスペクション機能を設定し、暗号化されたトラフィックをアクセス コントロール ルールが評価する前にブロックまたは復号化することができます。

レピュテーション ベースのアクセス コントロールには、次のライセンスが必要です。

表 *21 :* レピュテーション ベースのアクセス コントロール ルールのライセンス要件

要件	アプリケーション管理	URL フィルタリング（cat. & rep.）	URL フィルタリング（手動）
ライセンス	Control	URL フィルタリング	いずれか（Any）

ASA FirePOWER モジュールは、他のタイプのレピュテーション ベースの制御を実行できますが、アクセス コントロール ルールを使用してそれらを設定しないでください。詳細については、セキュリティ インテリジェンスの IP アドレス レピュテーションを使用したトラフィックのブロック （103 ページ）を参照してください。ここでは、最初の防御ラインとして、接続の発信元または宛先のレピュテーションに基づいてトラフィックを制限する方法について説明されています。侵入防御パフォーマンスの調整（177 ページ）では、マルウェアおよび他のタイプの禁止されたファイルの送信を検出、追跡、保存、分析、およびブロックする方法について説明されています。

- アプリケーション トラフィックの制御 （140 ページ）
- URL のブロッキング （147 ページ）

アプリケーション トラフィックの制御

ライセンス：Control

ASA FirePOWER モジュールは、IP トラフィックを分析する際に、ネットワークで一般的に使用されているアプリケーションを識別および分類することができます。

アプリケーション制御について

アクセスコントロールルールのアプリケーション条件を使用することで、このアプリケーション制御を実行できます。1 つのアクセス コントロール ルール内には、トラフィックを制御するアプリケーションを指定する方法がいくつかあります。

- カスタム アプリケーションなどの個々のアプリケーションを選択できます。
- システム提供のアプリケーション フィルタを使用できます。このフィルタは、アプリケーションの基本的な特性であるタイプ、リスク、ビジネスとの関連性、カテゴリ、およびタグに基づいて編成されたアプリケーションの名前付きセットです。
- 選択したアプリケーション（カスタム アプリケーションを含む）をグループ化するカスタム アプリケーション フィルタを作成し、使用できます。

アプリケーションフィルタを使用することで、アクセスコントロールルールに対しアプリケーション条件をすぐに作成することができます。このフィルタによって、ポリシーの作成と管理が簡素化され、システムは Web トラフィックを想定通りに確実に制御します。たとえば、リスクが高く、ビジネスとの関連性が低いアプリケーションをすべて認識してブロックするアクセス コントロール ルールを作成できます。ユーザがそれらのアプリケーションの 1 つを使用しようとすると、セッションがブロックされます。

また、 シスコでは、システムおよび脆弱性データベース（VDB）の更新を通じて頻繁にディテクタを更新および追加しています。アプリケーションの特性に基づいたフィルタを使用することで、システムが最新のディテクタを使用してアプリケーション トラフィックをモニタすることが保証されます。

アプリケーション条件の作成

トラフィックがアプリケーション条件を持つアクセス コントロール ルールに一致するには、トラフィックが [Selected Applications and Filters] リストに追加したフィルタまたはアプリケーションの 1 つに一致している必要があります。

1 つのアプリケーション条件において、最大 50 の項目を [Selected Applications and Filters] リストに追加できます。以下はそれぞれ 1 つの項目としてカウントされます。

- 個別またはカスタムな組み合わせの、[Application Filters] リストからの 1 つ以上のフィルタ。この項目は、特性を基準にグループ化されたアプリケーションのセットです。
- [Available Applications] リストでアプリケーションの検索を保存することで作成されるフィルタ。この項目は、アプリケーション名の一部の一致によってグループ化されたアプリケーションのセットです。
- [Available Applications] リストからの個々のアプリケーション。

モジュール インターフェイスでは、条件に追加されたフィルタは上部にリストされ、個別に追加されたアプリケーションとは分けられます。

アプリケーション条件を持つ各ルールに対し、アクセス コントロール ポリシーを展開すると、システムは一意のアプリケーションのリストを生成して照合することに留意してください。つまり、完全なカバレッジを確保するために、重複フィルタおよび個々に指定されたアプリケーションを使用できます。

（注） 暗号化されたトラフィックの場合、システムは [SSL Protocol] とタグ付けされたアプリケーションだけを使用して、トラフィックを識別およびフィルタリングできます。このタグがないアプリケーションは、暗号化されていないまたは復号化されたトラフィックでのみ検出できます。

トラフィックとアプリケーション フィルタの一致

ライセンス：Control

アクセス コントロール ルールでアプリケーション条件を作成するときは、[Application Filters] リストを使用して、特性によってグループ化されたトラフィックを照合するアプリケーションのセットを作成します。

アクセス コントロール ルール内でアプリケーションをフィルタリングするメカニズムは、オブジェクト マネージャを使用して再利用可能なカスタム アプリケーション フィルタを作成するメカニズムと同じです。アプリケーション フィルタの操作 （35 ページ） を参照してください。また、アクセス コントロール ルールの設定時に作成する各種のフィルタを、新規のフィ

ルタとして保存して再利用することもできます。ユーザが作成したフィルタはネストすることができないため、別のユーザが作成したフィルタを含むフィルタは保存できません。

フィルタの組み合わせ方について

フィルタを単独または組み合わせて選択すると、[Available Applications] リストが更新され、基準を満たすアプリケーションのみが表示されます。システムによって提供されるフィルタは組み合わせて選択できますが、カスタム フィルタはできません。

システムは、OR 演算を使用して同じフィルタ タイプの複数のフィルタをリンクします。たとえば、Risks（リスク）タイプの下の Medium（中）および High（高）フィルタを選択すると、結果として次のようなフィルタになります。

```
Risk: Medium OR High
```

Medium フィルタに 110 個のアプリケーション、High フィルタに 82 個のアプリケーションが含まれる場合、システムはこれら 192 個のアプリケーションすべてを [Available Applications] リストに表示します。

システムは、AND 演算を使用して異なるタイプのフィルタをリンクします。たとえば Risks タイプで Medium および High フィルタを選択し、Business Relevance（業務との関連性）タイプで Medium および High フィルタを選択した場合、結果として次のようなフィルタになります。

```
Risk: Medium OR HighANDBusiness Relevance: Medium OR High
```

この場合、システムは Medium または High Risk タイプと Medium または High Business Relevance タイプの両方に含まれるアプリケーションだけを表示します。

フィルタの検索および選択

フィルタを選択するには、フィルタ タイプの横にある矢印をクリックしてそれを展開し、アプリケーションを表示/非表示にする各フィルタの横のチェック ボックスを選択/選択解除します。システム提供のフィルタ タイプ（[Risks]、[BusinessRelevance]、[Types]、[Categories]、または[Tags]）を右クリックして、[CheckAll] または [Uncheck All] を選択することもできます。

フィルタを検索するには、[Available Filters] リストの上にある [Search by name] プロンプトをクリックし、名前を入力します。入力していくと、リストが更新されて一致するフィルタが表示されます。

フィルタを選択したら、[Available Applications] リストを使用してそのフィルタをルールに追加します。個々のアプリケーションからのトラフィックの照合（142 ページ） を参照してください。

個々のアプリケーションからのトラフィックの照合

ライセンス：Control

アクセス コントロール ルールでアプリケーション条件を作成するときは、[Available Applications] リストを使用して、トラフィックを照合するアプリケーションを作成します。

アプリケーションのリストの参照

条件の作成を初めて開始するときは、リストは制約されておらず、システムが検出するすべてのアプリケーションを一度に 100 個ずつ表示します。

- アプリケーションを順次確認するには、リストの下にある矢印をクリックします。
- アプリケーションの特性に関する概要情報と参照可能なインターネット検索リンクを含むポップアップウィンドウを表示するには、アプリケーションの横にある情報アイコン（  ）をクリックします。

一致するアプリケーションの検索

照合するアプリケーションを見つけやすくするために、[Available Applications] リストを次のように制約できます。

- アプリケーションを検索するには、リスト上部にある [Search by name] プロンプトをクリックし、名前を入力します。入力していくと、リストが更新されて一致するアプリケーションが表示されます。
- フィルタを適用してアプリケーションを制約するには、[Application Filters] リストを使用します（トラフィックとアプリケーションフィルタの一致（141 ページ） を参照）。フィルタを適用すると、[Available Applications] リストが更新されます。

制約されると、[All apps matching the filter] オプションが [Available Applications] リストの上部に表示されます。このオプションを使用して、制約されたリスト内のすべてのアプリケーションを [Selected Applications and Filters] リストにすべて一度に追加できます。

（注） [アプリケーション フィルタ（Application Filters）] リストで 1 つ以上のフィルタを選択し、さらに [使用可能なアプリケーション（Available Applications）] リストも検索すると、選択内容と検索フィルタ適用後の [使用可能なアプリケーション（Available Applications）] リストが AND 演算を使用して結合されます。つまり [All apps matching the filter] 条件には、[Available Applications] リストに現在表示されている個々のすべての条件と、[Available Applications] リストの上で入力された検索文字列が含まれます。

条件内で照合する単一アプリケーションの選択

照合するアプリケーションを検索したら、それをクリックして選択します。複数のアプリケーションを選択するには、Shift キーまたは Ctrl キーを使用します。表示されているすべてのアプリケーションを選択するには、右クリックして [Select All] を選択します。

単一のアプリケーション条件では、それらを個別に選択することで、最大 50 のアプリケーションを照合できます。50 を超えるアプリケーションを追加するには、複数のアクセス コントロール ルールを作成するか、またはフィルタを使用してアプリケーションをグループ化します。

条件のフィルタに一致するすべてのアプリケーションの選択

[Application Filters] リストで検索またはフィルタを使用して制約されると、[All apps matching the filter] オプションが [Available Applications] リストの上部に表示されます。

このオプションを使用すると、制限した [Available Applications] リストに表示されているすべてのアプリケーションをまとめて [Selected Applications and Filters] リストに追加できます。アプリケーションを個別に追加するのとは対照的に、このアプリケーションのセットを追加すると、そのセットを構成する個々のアプリケーションの数にかかわらず、最大 50 のアプリケーションに対してただ 1 つのアイテムとしてカウントされます。

この方法でアプリケーション条件を作成すると、[Selected Applications and Filters] リストに追加したフィルタに「フィルタ タイプ + 各タイプの最大 3 フィルタの名前」形式の名前が付きます。同じタイプのフィルタが 3 個を超える場合は、その後に省略記号（...）が表示されます。たとえば次のフィルタ名には、Risks タイプの 2 つのフィルタと Business Relevance タイプの 4 つのフィルタが含まれています。

```
Risks: Medium, High Business Relevance: Low, Medium, High,...
```

[All apps matching the filter] で追加したフィルタでは表されないフィルタ タイプは、追加するフィルタの名前に含まれません。それらのファイル タイプは [any] に設定されます。つまり、それらのフィルタ タイプはフィルタを制約せず、任意の値を使用できるということです。

[All apps matching the filter] の複数のインスタンスをアプリケーション条件に追加でき、各インスタンスは [Selected Applications and Filters] リストで個別の項目としてカウントされます。たとえば、リスクが高いすべてのアプリケーションを 1 つの項目として追加し、選択内容をクリアしてから、ビジネスとの関連性が低いすべてのアプリケーションを別の項目として追加できます。このアプリケーション条件は、リスクが高いアプリケーションまたはビジネスとの関連性が低いアプリケーションに一致します。

アクセス コントロール ルールへのアプリケーション条件の追加

ライセンス：Control

トラフィックがアプリケーション条件を持つアクセス コントロール ルールに一致するには、トラフィックが [Selected Applications and Filters] リストに追加したフィルタまたはアプリケーションの 1 つに一致している必要があります。

1 つの条件に最大 50 の項目を追加することができ、条件に追加したフィルタが個別に追加したアプリケーションの上に一覧表示されます。無効なアプリケーション条件が検出されると、警告アイコンが表示されます。詳細については、アクセス コントロール ポリシーとルールのトラブルシューティング （92 ページ）を参照してください。

アプリケーション トラフィックを制御するには、次の手順を実行します。

ステップ 1 アプリケーション別にトラフィックを制御するアクセス コントロール ポリシーで、新しいアクセス コントロール ルールを作成するか、または既存のルールを編集します。

詳細な手順については、アクセス コントロール ルールの作成および編集 （113 ページ）を参照してください。

ステップ 2 ルール エディタで、[Applications] タブを選択します。

ステップ 3 必要に応じて、セーフサーチ（）または YouTube EDU（）の淡色表示アイコンをクリックし、関連オプションを設定して、コンテンツ制限機能を有効にします。追加の設定要件については、アクセス コントロール ルールを使用したコンテンツ制限の実施 （202 ページ）を参照してください。

たいていの場合、コンテンツ制限を有効にすると、条件の [Selected Applications and Filters] リストに適切な値が入力されます。コンテンツ制限を有効にするときに、コンテンツ制限に関係するアプリケーションまたはフィルタがすでにリスト内に存在している場合には、システムはリストに自動的に値を入力することはしません。

アプリケーションを絞り込んで選択内容をフィルタする手順を続行するか、またはスキップしてルールの保存に進みます。

ステップ 4 オプションで、フィルタを使用して [Available Applications] リストに表示されるアプリケーションのリストを制約します。

[Application Filters] リストで 1 つ以上のフィルタを選択します。詳細については、トラフィックとアプリケーション フィルタの一致 （141 ページ）を参照してください。

ステップ 5 [Available Applications] リストから追加するアプリケーションを見つけて選択します。

個々のアプリケーションを検索して選択したり、リストの表示を制限した場合は [All apps matching the filter] をクリックしてすべてを選択したりできます。詳細については、個々のアプリケーションからのトラフィックの照合 （142 ページ）を参照してください。

ステップ 6 [Add to Rule] をクリックして、選択したアプリケーションを [Selected Applications and Filters] リストに追加します。

選択したアプリケーションとフィルタをドラッグアンドドロップすることもできます。フィルタは [Filters] という見出しの下に表示され、アプリケーションは [Applications] という見出しの下に表示されます。

ヒント このアプリケーション条件に別のフィルタを追加する場合は、[Clear All Filters] をクリックして既存の選択をクリアしておきます。

ステップ 7 必要に応じて、[Selected Applications and Filters] リストの上にある追加アイコンをクリックすると、リストに現在含まれているすべての個々のアプリケーションとフィルタから成るカスタム フィルタを保存できます。

臨機応変に作成されたこのフィルタを管理するには、オブジェクト マネージャを使用します。アプリケーション フィルタの操作 （35 ページ） を参照してください。別のユーザが作成したフィルタを含むフィルタは保存できないことに注意してください。ユーザが作成したフィルタはネストできません。

ステップ 8 ルールを保存するか、編集を続けます。

変更を反映させるには、アクセス コントロール ポリシーを展開する必要があります（設定変更の導入 （92 ページ）を参照してください）。

アプリケーション制御の制限

ライセンス：Control

アプリケーション制御を実行する場合は、次の点に注意してください。

アプリケーション識別の速度

システムは、以下の動作の前にアプリケーション制御を実行することはできません。

- モニタ対象の接続がクライアントとサーバの間で確立される前
- システムがセッションでアプリケーションを識別する前

この識別は 3 ～ 5 パケット以内で、またはトラフィックが暗号化されている場合は、SSL ハンドシェイクのサーバ証明書交換の後に発生する必要があります。これらの最初のパケットの 1 つがアプリケーション条件を含むアクセス コントロール ルール内の他のすべての条件に一致するが、識別が完了していない場合、アクセス コントロール ポリシーはパケットの通過を許可します。この動作により接続が確立され、こうしてアプリケーションの識別が可能になります。便宜上、影響を受けるルールは情報アイコン（）でマークされます。

許可されたパケットは、アクセスコントロールポリシーのデフォルトの侵入ポリシー（デフォルトアクション侵入ポリシーでも、ほぼ一致するルールの侵入ポリシーでもない）により検査されます。

システムは識別を終えると、アクセス コントロール ルール アクションおよび関連付けられている侵入ポリシーおよびファイルポリシーをそのアプリケーション条件に一致する残りのセッション トラフィックに適用します。

暗号化されたトラフィックの処理

システムは、SMTPS、POP、FTPS、TelnetS および IMAPS など StartTLS を使用して、暗号化されるようになる暗号化されていないアプリケーション トラフィックを識別し、フィルタリングできます。また、TLS クライアントの hello メッセージ内の Server Name Indication、またはサーバ証明書のサブジェクト識別名の値に基づいて、特定の暗号化されたアプリケーションを識別できます。

これらのアプリケーションは、[SSL Protocol] とタグ付けされています。このタグがないアプリケーションは、暗号化されていないまたは復号されたトラフィックでのみ検出できます。

ペイロードのないアプリケーション トラフィック パケットの処理

システムは、アプリケーションが識別される接続内にペイロードがないパケットに対してデフォルト ポリシー アクションを適用します。

参照されるトラフィックの処理

Web サーバによって参照されるトラフィック（たとえばアドバタイズメント トラフィック）を処理するルールを作成するには、参照元アプリケーションではなく、参照されるアプリケーションに関する条件を追加します。

複数のプロトコルを使用するアプリケーション トラフィックの制御（Skype）

システムは、Skype の複数のタイプのアプリケーション トラフィックを検出できます。Skype のトラフィックを制御するためのアプリケーション条件を作成する場合は、個々のアプリケーションを選択するのではなく、[Application Filters] リストから [Skype] タグを選択します。これにより、システムは同じ方法で Skype のすべてのトラフィックを検出して制御できるようになります。詳細については、トラフィックとアプリケーションフィルタの一致（141 ページ）を参照してください。

URL のブロッキング

ライセンス：機能に応じて異なる

アクセス コントロール ルールの URL 条件を使用することで、ネットワーク上のユーザがアクセスできる Web サイトを制限することができます。この機能は、URL フィルタリングと呼ばれます。アクセス コントロールを使用してブロックする（または逆に許可する）URL を指定するには 2 つの方法があります。

- 各ライセンスを使用して、個々の URL または URL のグループを手動で指定することで、Web トラフィックへのきめ細かなカスタム コントロールを実現できます。
- URL Filtering ライセンスを使用して、URL の一般的な分類、またはカテゴリ、およびリスク レベル、またはレピュテーションに基づいて、Web サイトへのアクセスを制御することもできます。システムは接続ログ、侵入イベント、およびアプリケーションの詳細にこのカテゴリとレピュテーション データを表示します。

（注） イベントで URL カテゴリおよびレピュテーション情報を表示するには、URL 条件を使用して少なくとも 1 つのアクセス コントロール ルールを作成する必要があります。

Web サイトをブロックするときは、ユーザのブラウザにデフォルト動作を許可するか、またはシステムによって提供される一般的なページまたはカスタム ページを表示できます。また、警告ページをクリック スルーすることで Web サイトのブロックをバイパスする機会をユーザに与えることができます。

表 *22 : URL* フィルタリングのライセンス要件

要件	カテゴリおよびレピュテーションベース	手動
ライセンス	URL フィルタリング	いずれか（Any）

URL カテゴリとレピュテーションに基づく URL のブロッキング

ライセンス：URL Filtering

URL Filtering を使用して、ASA FirePOWER モジュールが Cisco Cloud から取得する要求された URL のカテゴリおよびレピュテーションに基づいて、Web サイトへのユーザのアクセスを制御できます。

- URL カテゴリとは、URL の一般的な分類です。たとえば ebay.com は [Auctions] カテゴリ、monster.com は [Job Search] カテゴリに属します。1 つの URL は複数のカテゴリに属することができます。

  URL カテゴリの説明は https://www.talosintelligence.com/categories を参照してください。

  すべてのカテゴリを表示するには、[Threat Categories] タブをクリックしてください。

- URL レピュテーションは、URL が悪意のあるものである可能性を表します。URL のリスクは、**[Untrusted]**（レベル 1）から **[Trusted]**（レベル 5）まであります。

  URL レピュテーションのレベルの説明は、https://talosintelligence.com/reputation_center/support を参照してください。[Common Questions] セクションを確認します。

（注） カテゴリとレピュテーションベースの URL 条件を持つアクセス制御ルールを有効にする前に、URL フィルタリングライセンスを追加し、Cisco Cloud との通信を有効にする必要があります。これで、ASA FirePOWER モジュールが URL データを取得できるようになります。詳細については、「URL フィルタリングとマルウェア検出のクラウドコミュニケーションのオプション（563 ページ）」を参照してください。

レピュテーション ベースの URL ブロッキングの利点

URL のカテゴリおよびレピュテーションにより、アクセス コントロール ルールの URL 条件をすぐに作成することができます。たとえば、**[Illegal Drugs]** カテゴリの **[Untrusted]** のすべての URL を識別し、ブロックするアクセス制御ルールを作成できます。ユーザがそのカテゴリとレピュテーションの組み合わせで URL を閲覧しようとすると、セッションがブロックされます。

Cisco Cloud のカテゴリ データとレピュテーション データを使用することで、ポリシーの作成と管理も簡素化されます。この方法では、システムが Web トラフィックを想定通りに確実に制御します。最後に、クラウドは新しい URL だけでなく、既存の URL に対する新しいカテゴリとリスクで常に更新されるため、システムは確実に最新の情報を使用して要求された URL をフィルタ処理できます。マルウェア、スパム、ボットネット、フィッシングなど、セキュリティに対する脅威を表す悪意のあるサイトは、組織でポリシーを更新したり新規ポリシーを展開したりするペースを上回って次々と現れては消える可能性があります。

次に例をいくつか示します。

- すべてのギャンブルサイトをルールでブロックする場合は、新しいドメインが登録されて [Gambling] に分類されると、それらのサイトはシステムで自動的にブロックされます。
- ルールですべてのマルウェアサイトをブロックしており、あるブログのページがマルウェアに感染した場合、クラウドは **[Online Communities]** の URL を [Malware] に分類し、そのサイトをシステムでブロックできます。

- ルールでリスクの高いソーシャル ネットワーキング サイトをブロックし、ある参加者がプロファイルページに悪意のあるペイロードへのリンクを含むリンクを掲載すると、クラウドはそのページのレピュテーションを **[Favorable]** から **[Untrusted]** に変更でき、システムはそのページをブロックできます。

なお、URL のカテゴリやレピュテーションがクラウドで不明な場合、または ASA FirePOWER モジュールがクラウドと通信できない場合は、カテゴリまたはレピュテーションベースの URL 条件を含むアクセス コントロール ルールが URL によってトリガーされないことに注意してください。URL にカテゴリやレピュテーションを手動で割り当てることはできません。

URL 条件の作成

1 つの URL 条件で、照合する最大 50 の項目を [Selected URLs] に追加できます。任意でレピュテーションによって制限された各 URL カテゴリは、1 つの項目としてカウントされます。URL 条件でリテラル URL および URL オブジェクトを使用することもできますが、これらの項目はレピュテーションで制限できないことに注意してください。詳細については、手動による URL ブロッキングの実行 （151 ページ）を参照してください。

レピュテーションでリテラル URL または URL オブジェクトを制限できないことに注意してください。

URL 条件を作成する際、警告アイコンは無効な設定を示します。詳細については、アクセス コントロール ポリシーとルールのトラブルシューティング （92 ページ）を参照してください。

カテゴリ データおよびレピュテーション データを使用した要求された URL によるトラフィックの制御

ステップ 1 Cisco Cloud から URL カテゴリとレピュテーションデータを取得するようにアプライアンスを設定します。

クラウド通信の有効化 （565 ページ）を参照してください。

ステップ 2 URL 別にトラフィックを制御するアクセス コントロール ポリシーで、新しいアクセス コントロール ルールを作成するか、または既存のルールを編集します。

詳細な手順については、アクセス コントロール ルールの作成および編集 （113 ページ）を参照してください。

ステップ 3 ルール エディタで、[URLs] タブを選択します。

[URLs] タブが表示されます。

ステップ 4 [Categories and URLs] リストから追加する URL のカテゴリを見つけて選択します。カテゴリに関係なく Web トラフィックを照合するには、[Any] カテゴリを選択します。

追加するカテゴリを検索するには、[Categories and URLs] リストの上にある [Search by name or value] プロンプトをクリックして、カテゴリ名を入力します。入力を開始するとリストが更新され、一致するカテゴリが表示されます。

カテゴリを選択するには、そのカテゴリをクリックします。複数のカテゴリを選択するには、Shift キーおよび Ctrl キーを使用します。

ヒント 右クリックして、すべてのカテゴリを選択することもできますが、すべてのカテゴリを追加すると、1 つのアクセス コントロール ルールに対する項目の最大値 50 を超えます。代わりに [Any] を使用してください。

ルールの目的がマルウェアからの保護である場合は、https://www.talosintelligence.com/categoriesの説明に従ってすべての脅威カテゴリを選択してください。

カテゴリのページが複数存在する場合があります。カテゴリリストの下にある矢印をクリックして、すべてのページにアクセスしていることを確認します。

ステップ 5 オプションで、[レピュテーション（Reputations）] リストからレピュテーション レベルをクリックして、カテゴリの選択内容を制限します。レピュテーションレベルを指定しなかった場合、システムはデフォルトで [Any]（レピュテーションが未知のサイトを含むすべてのレベル）に設定します。

必要に応じて、[不明なレピュテーションに適用（Apply to unknown reputation）] をオンにします。

選択できるレピュテーション レベルは 1 つだけです。レピュテーション レベルを選択すると、アクセス コントロール ルールはその目的に応じて異なる動作をします。

- ルールによって Web アクセスをブロックまたはモニタする場合（ルールアクションが [Block]、[Block with reset]、[Interactive Block]、[Interactive Block with reset]、または [Monitor]）、レピュテーション レベルを選択すると、そのレベルよりも厳しいレピュテーションもすべて選択されます。たとえば、[Questionable sites]（レベル 2）をブロックまたはモニタするルールを設定した場合、**[Untrusted]**（レベル 1）サイトも自動的にブロックまたはモニタされます。
- ルールによって Web アクセスがそれを信頼またはさらに検査するかどうかを許可する場合（ルールアクションが [Allow] または [Trust]）、レピュテーション レベルを選択すると、そのレベルよりも厳しさが弱いレピュテーションもすべて選択されます。たとえば、[Favorable] サイト（レベル 4）を許可するルールを設定した場合、**[Trusted]**（レベル 5）サイトも自動的に許可されます。

ルールのアクションを変更した場合、システムは、上記の点に従って URL 条件のレピュテーション レベルを自動的に変更します。

ステップ 6 [Add to Rule] をクリックするか、または選択した項目をドラッグ アンド ドロップして、[Selected URLs] リストに追加します。

ステップ 7 ルールを保存するか、編集を続けます。

変更を反映させるには、アクセス コントロール ポリシーを展開する必要があります（設定変更の導入（92 ページ）を参照してください）。

URL カテゴリを変更する場合

URL フィルタリング カテゴリのセットは、新しい Web のトレンドと進化する使用パターンに合わせてときどき変更されます。

これらの変更は、ポリシーとイベントに関連するアクティビティの両方に影響します。

このトピックの説明どおりに設定された URL カテゴリへの更新は、新しい URL を単純に追加したり、誤って分類された URL を再マッピングする変更とは異なります。このトピックは個々の URL のカテゴリ変更には適用されません。

イベントへの影響

トラフィックが検出された時点で一致した URL カテゴリがすべてのイベントにあります。レガシーカテゴリはそのようにラベル付けされます。時間が経過するとともに、レガシーカテゴリを持つイベントはシステムからエージアウトします。

処理された時点で URL にレピュテーションがない場合は、イベント ビューア内の URL レピュテーションは空になります。

手動による URL ブロッキングの実行

URL を手動で指定してブロックし、カテゴリとレピュテーションによって URL のフィルタリングを補完または選択的に上書きすることができます。

また、この手順を例として使用して、設定によってブロックされる URL へのトラフィックを手動で許可することもできます。

手動で URL のフィルタリングを実行する方法はいくつかあります。指定した URL 文字列が URL 内の何らかの部分に一致する場合は、ほとんどのメソッドが一致します。これは、たとえば、これらのメソッドを使用して「cisco.com」へのトラフィックを許可する場合は URL の任意の部分に「cisco.com」がある他のドメインへのトラフィックを誤って許可する可能性があることを意味します。

そのため、この手順では、この目的でドメインに一致する URL をアンカーするセキュリティ インテリジェンス リストを使用する手順を示します。

暗号化された Web トラフィックの手動ブロッキングに関する注意事項

アクセス コントロール ルールの URL 条件は以下を行います。

- Web トラフィック（HTTP または HTTPS）の暗号化プロトコルを無視します。

たとえば、アクセス コントロール ルールは、http://example.com/ へのトラフィックを https://example.com/ へのトラフィックと同じものとして処理します。HTTP または HTTPS トラフィックのみに一致するアクセス コントロール ルールを設定するには、アプリケーション条件をルールに追加します。詳細については、URL のブロッキング（147 ページ）を参照してください。

- トラフィックを暗号化するために使用された公開キー証明書のサブジェクト共通名に基づいて HTTPS トラフィックを照合し、また、サブジェクト共通名に含まれるサブドメインを無視します。

手動で HTTPS トラフィックをフィルタリングする場合は、サブドメイン情報を含めないでください。

URL 条件を作成する際、警告アイコンは無効な設定を示します。詳細については、アクセス コントロール ポリシーとルールのトラブルシューティング （92 ページ）を参照してください。

ステップ 1 ブロックする URL を含むカスタム セキュリティ インテリジェンス リストを作成して追加します。

a) ファイル名拡張子が .txt の新しいテキストファイルを作成します。

ファイル名に「Block」と「URL」を含めることをお勧めします。

b) 各行で、1 つまたは複数の URL をファイルに追加します。

リストの詳細な要件とガイドラインについては、https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html から入手可能な『Firepower Management Center Configuration Guide for version 6.6』の「Custom Security Intelligence Lists」のトピックを参照してください。

ステップ 2 カスタム セキュリティ インテリジェンス リストとしてテキストファイルを追加します。

a) [Object Management] > [Security Intelligence] > [URL Lists and Feeds] に移動します。

b) カスタム セキュリティ インテリジェンスのリストの操作 （32 ページ）の手順に従ってリストを追加します。

ステップ 3 アクセス コントロール ポリシーで、ブロックアクションを指定したルール内に新しいリストを指定します。

a) アクセスコントロールルールで、[URLs] タブをクリックします。

b) [URLs] タブで、[URLs] サブタブをクリックします。

c) 上で作成した新しいカスタム セキュリティ インテリジェンス リストを選択します。

d) [Add to Rule] をクリックします。

e) [追加（Add）] をクリックします。

ステップ 4 ポリシーを保存します。

次のタスク

- （任意）この手順を例として使用して、手動で許可する URL トラフィックのカスタム セキュリティ インテリジェンス リストを作成します。

  たとえば、組織に適していない Web サイトのカテゴリをブロックする一方で、アクセスできるようにする必要がある Web サイトがそのカテゴリに含まれている場合に、このようなリストを使用できます。

  このリストでは、ファイル名に「Allow」と「URL」を使用することをお勧めします。許可アクションを使用してアクセスコントロールルールにリストを追加します。リスト上の URL をブロックするルールの上にルールを配置します。

- 変更を展開します。

- カスタム セキュリティ インテリジェンス リストに URL を追加するには、セキュリティ インテリジェンス リストの更新 （33 ページ）を参照してください。

URL の検出とブロッキングのガイドラインと制限事項

ライセンス：任意

URL の検出とブロッキングを実行する際は、次の点に注意してください。

脅威カテゴリ

ポリシーが既知の悪意のあるサイトを識別する脅威カテゴリに明確に対応していることを確認してください。

詳細については、URL カテゴリとレピュテーションに基づく URL のブロッキング （147 ページ）の URL にある [脅威カテゴリ（Threat Categories）] タブを参照してください。

一部のパケットは URL の識別前に通過することが必要

システムは以下の動作の前に URL をフィルタリングできません。

- モニタ対象の接続がクライアントとサーバの間で確立される前
- システムがセッションで HTTP または HTTPS アプリケーションを識別する前
- システムが要求された URL を識別する前（クライアントの hello メッセージまたはサーバ証明書から暗号化されたセッションの場合）

この識別は 3 ～ 5 パケット以内で、またはトラフィックが暗号化されている場合は、SSL ハンドシェイクのサーバ証明書交換の後に発生する必要があります。これらの最初のパケットの 1 つが URL 条件を含むアクセス コントロール ルール内の他のすべての条件に一致するが、識別が完了していない場合、アクセス コントロール ポリシーはパケットの通過を許可します。この動作により接続が確立され、こうして URL の識別が可能になります。便宜上、影響を受けるルールは情報アイコン（）でマークされます。

許可されたパケットは、アクセス コントロール ポリシーのデフォルトの侵入ポリシー（デフォルト アクション侵入ポリシーでも、ほぼ一致するルールの侵入ポリシーでもない）により検査されます。**重要**この侵入ポリシーが設定されていることを確認します。

システムは識別を終えると、アクセス コントロール ルール アクションおよび関連付けられている侵入ポリシーおよびファイル ポリシーをその URL 条件に一致する残りのセッション トラフィックに適用します。

未分類/レピュテーションのない URL

URL ルールを作成するときは、まず一致させるカテゴリを選択します。[未分類（Uncategorized）] URL を明示的に選択した場合は、レピュテーションによりさらに制約を追加することはできません。

信頼できないレピュテーションの未分類 URL は、[悪意のあるサイト（Malicious Sites）] カテゴリによって処理されます。他のレピュテーション レベルを使用する未分類サイトをブロックする場合は、すべての未分類サイトをブロックする必要があります。

URL のカテゴリおよびレピュテーションが不明な場合、Web サイトの閲覧は、カテゴリおよびレピュテーションベースの URL 条件を持つルールには一致しません。カテゴリとレピュテーションを手動で URL に割り当てることはできませんが、特定の URL はブロックできます。手動による URL ブロッキングの実行 （151 ページ）を参照してください。

暗号化された Web トラフィックの処理

URL 条件を持つアクセス コントロール ルールを使用して暗号化された Web トラフィックを評価する際、システムは以下を行います。

- 暗号化プロトコルを無視します。ルールに URL 条件はあるがプロトコルを指定するアプリケーション条件はない場合、アクセス コントロール ルールは HTTPS および HTTP 両方のトラフィックを照合します。
- トラフィックを暗号化するために使用された公開キー証明書のサブジェクト共通名に基づいて HTTPS トラフィックを照合し、サブジェクト共通名に含まれるサブドメインを無視します。
- HTTP 応答ページを表示しません（設定したとしても）。

URL での検索クエリ パラメータ

システムでは、URL 条件の照合に URL 内の検索クエリ パラメータを使用しません。たとえば、すべてのショッピング トラフィックをブロックする場合を考えます。amazon.com を探すために Web 検索を使用してもブロックされませんが、amazon.com を閲覧しようとするとブロックされます。

手動による URL フィルタリングのガイドライン

手動で URL を入力するか、URL オブジェクトまたはグループを使用して URL フィルタリングを指定すると、それらの URL は単純な文字列一致を使用してトラフィックを照合します。たとえば、トラフィックの通過を許可するルールに「cisco.com」を入力すると、URL 内の何らかの部分に「cisco.com」を持つすべてのドメインに対するトラフィックが許可されることを意味します。一方で、個別の URL を指定するためにカスタム セキュリティ インテリジェンス リストまたはフィードを使用すると、ドメイン名に一致している URL がアンカーされます。

URL カテゴリまたはレピュテーションの不一致

ライセンス：URL Filtering

URL に誤ったカテゴリまたはレピュテーション レベルが割り当てられていると思われる場合は、疑われるエラーをシスコに報告できます。

始める前に

シスコ アカウントのクレデンシャルが必要になります。

ステップ 1 接続イベントのリストに移動します。

ステップ 2 報告するイベントを右クリックし、[Dispute URL Category] または [Dispute URL Reputation] を選択します。

ブラウザのウィンドウに新しいページが開きます。

ステップ 3 シスコアカウントのクレデンシャルを使用して Talos の Web サイトにサインインします。

ステップ 4 ページに表示される指示に従います。

このページにはチケットのステータスを表示するリンクが含まれています。この情報は後で追跡できるようにメモします。

ユーザが URL ブロックをバイパスすることを許可する

ライセンス：任意

アクセス コントロール ルールを使用してユーザの HTTP Web 要求をブロックする場合は、ルール アクションを [Interactive Block] または [Interactive Block with reset] に設定することで、ユーザは警告 HTTP 応答ページをクリック スルーすることによりブロックをバイパスできます。システムによって提供される汎用応答ページを表示するか、またはカスタム HTML を入力できます。

デフォルトでは、システムによってユーザは後続のアクセスで警告ページを表示することなく、10 分（600 秒）間ブロックをバイパスすることができます。期間を 1 年に設定したり、ユーザに毎回ブロックをバイパスするように強制できます。

ユーザがブロックをバイパスしない場合、一致するトラフィックは追加のインスペクションなしで拒否されます。また、接続をリセットすることもできます。一方、ユーザがブロックをバイパスすると、システムによってトラフィックが許可されます。このトラフィックを許可するということは、侵入、マルウェア、および禁止されているファイルの有無について暗号化されていないペイロードを引き続き検査できることを意味します。ブロックをバイパスした後、ロードされなかったページの要素をロードするために、ページを更新しなければならない場合があることに注意してください。

インタラクティブ HTTP 応答ページは、ブロック ルールに設定する応答ページとは別に設定することに注意してください。たとえば、インタラクションなしでセッションがブロックされたユーザにはシステムによって提供されるページを表示できますが、クリックして続行できるユーザにはカスタム ページを表示できます。詳細については、ブロックされた URL のカスタム Web ページの表示 （157 ページ）を参照してください。

SSL インスペクション機能によって復号化された Web トラフィックをブロックすると、システムは応答ページを暗号化し、再度暗号化された SSL ストリームの最後にそのページを送信します。

ヒント アクセス コントロール ポリシーのすべてのルールに対してインタラクティブ ブロッキングを素早く無効にするには、システムによって提供されるページもカスタム ページも表示しないでください。これにより、システムはインタラクションなしでインタラクティブ ブロック ルールに一致するすべての接続をブロックします。

ユーザに Web サイト ブロックをバイパスするように許可するには、次の手順を実行します。

ステップ 1 URL 条件を持つ Web トラフィックに一致するアクセス コントロール ルールを作成します。

URL カテゴリとレピュテーションに基づく URL のブロッキング （147 ページ） および手動による URL ブロッキングの実行 （151 ページ） を参照してください。

ステップ 2 アクセス コントロール ルール アクションが [Interactive Block] または [Interactive Block with reset] であることを確認します。

ルール アクションを使用したトラフィック処理とインスペクションの決定 （119 ページ） を参照してください。

ステップ 3 ユーザがブロックをバイパスし、ルールに対してインスペクションおよびロギング オプションを必要に応じて選択すると仮定します。許可ルールと同様に次のようになります。

- 一方のタイプのインタラクティブ ブロック ルールをファイルおよび侵入ポリシーに関連付けることができます。詳細については、侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御 （171 ページ） を参照してください。
- インタラクティブ ブロックされるトラフィックに関するロギング オプションは、許可されたトラフィックに関するオプションと同じですが、ユーザがインタラクティブ ブロックをバイパスしない場合、システムがログに記録できるのは接続開始イベントだけであることに注意してください。

システムは最初にユーザに警告すると、ロギングされた接続開始イベントを Interactive Block または Interactive Block with reset アクションでマークすることに留意してください。ユーザがブロックをバイパスすると、セッションが記録される追加の接続イベントに Allow アクションが付きます。詳細については、アクセス コントロールの処理に基づく接続のロギング （477 ページ） を参照してください。

ステップ 4 オプションで、システムが警告ページを再表示する前にユーザがブロックをバイパスしてから経過する時間を設定します。

ブロックされた Web サイトのユーザー バイパス タイムアウトの設定 （157 ページ） を参照してください。

ステップ 5 オプションで、ユーザにブロックをバイパスすることを許可するために表示するカスタム ページを作成し、使用します。

「ブロックされた URL のカスタム Web ページの表示 （157 ページ） 」を参照してください。

ブロックされた Web サイトのユーザー バイパス タイムアウトの設定

ライセンス：任意

デフォルトでは、システムによってユーザは後続のアクセスで警告ページを表示することなく、10 分（600 秒）間インタラクティブ ブロックをバイパスすることができます。期間を 1 年に設定したり、ゼロに設定してユーザに毎回ブロックをバイパスするように強制できます。この制限は、ポリシー内のすべてのインタラクティブ ブロック ルールに適用されます。ルールごとに制限を設定することはできません。

ユーザ バイパスの期限が切れるまでの時間の長さをカスタマイズするには、次の手順を実行します。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。

[Access Control Policy] ページが表示されます。

ステップ 2 設定するアクセス コントロール ポリシーの横にある編集アイコンをクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3 [Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定が表示されます。

ステップ 4 [General Settings] の横にある編集アイコンをクリックします。

[General Settings] ポップアップ ウィンドウが表示されます。

ステップ 5 [Allow an Interactive Block to bypass blocking for (seconds)] フィールドに、ユーザ バイパスの期限が切れるまでの経過時間を秒数で入力します。

0 ～ 31536000（1 年）の間の任意の秒数を指定できます。ゼロを指定すると、ユーザはブロックを毎回強制的にバイパスします。

ステップ 6 [OK] をクリックします。

アクセス コントロール ポリシーの詳細設定が表示されます。

ステップ 7 [Store ASA FirePOWER Changes] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを展開する必要があります。詳細については、設定変更の導入 （92 ページ）を参照してください。

ブロックされた URL のカスタム Web ページの表示

ライセンス：任意

システムによってユーザの HTTP Web 要求がブロックされたときに、ユーザのブラウザに表示される内容は、アクセス コントロール ルールのアクションを使用して、セッションをどのようにブロックするかによって異なります。次から選択できます。

- 接続を拒否するには、[Block] または [Block with reset]。ブロックされたセッションがタイム アウトすると、システムは [リセットしてブロック（Block with reset）] の接続をリセットします。ただし、いずれのブロック アクションの場合でも、デフォルトのブラウザまたはサーバのページを、接続が拒否されたことを説明するカスタム ページでオーバーライドすることができます。このカスタム ページは HTTP 応答ページと呼ばれています。
- ユーザに警告するインタラクティブ *HTTP* 応答ページを表示する一方、ユーザがボタンをクリックすることで、処理を続行あるいはページを最新表示して、要求された元のサイトをロードできるようにする場合は、[Interactive Block] または [Interactive Block with reset] を選択します。応答ページをバイパスした後、ロードされなかったページの要素をロードするために、ページを最新表示しなければならない場合があります。

システムによって提供される汎用応答ページを表示するか、またはカスタム HTML を入力できます。カスタム テキストを入力する際には、使用した文字数がカウンタで示されます。

各アクセス コントロール ポリシーで、インタラクティブ HTTP 応答ページは、インタラクションなしで、つまりブロック ルールを使用してトラフィックをブロックするために使用する応答ページとは別に設定します。たとえば、インタラクションなしでセッションがブロックされたユーザにはシステムによって提供されるページを表示できますが、クリックして続行できるユーザにはカスタム ページを表示できます。

HTTP 応答ページをユーザに確実に表示できるかは、ネットワーク設定、トラフィック負荷、およびページのサイズによって異なります。カスタム応答ページを作成する場合は、より小さいページが正常に表示されやすいことに留意してください。

HTTP 応答ページの設定方法：

ステップ 1 Web トラフィックをモニタするアクセス コントロール ポリシーを編集します。アクセス コントロール ポリシーの編集 （86 ページ）を参照してください。

ステップ 2 [HTTP Responses] タブをクリックします。

ステップ 3 [Block Response Page] および [Interactive Block Response Page] の場合は、ドロップダウンリストから応答を選択します。各ページには、次の選択肢があります。

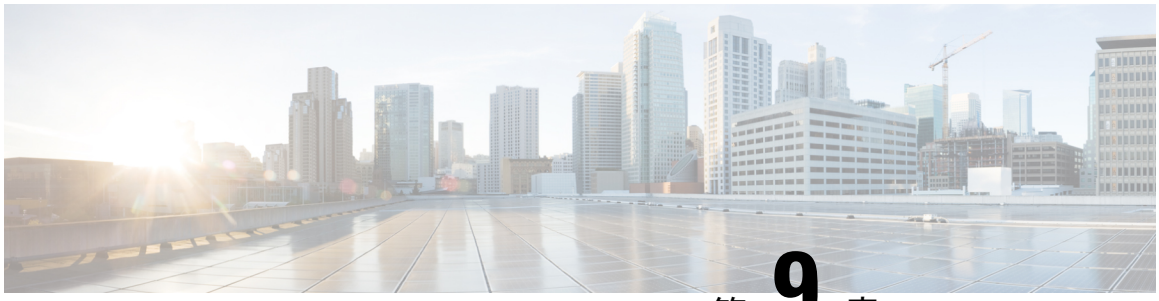
- [System-provided]：一般的な応答を表示します。表示アイコンをクリックすると、このページのコードが表示されます。
- [Custom]：カスタム応答ページを作成します。

ポップアップ ウィンドウが表示されます。このウィンドウに事前入力されているシステムによって提供されるコードを置換または変更できます。完了したら、変更を保存します。カスタム ページは、編集アイコンをクリックすると編集できます。

- [None]：応答ページを無効にして、インタラクションや説明なしでセッションをブロックします。 インタラクティブにブロックされるセッションに対してこのオプションを選択すると、ユーザはクリックして続行することができなくなります。セッションはインタラクションなしでブロックされます。

ステップ 4 [Store ASA FirePOWER Changes] をクリックします。

変更を有効にするには、設定を再展開する必要があります。詳細については、設定変更の導入 （92 ページ）を参照してください。



第 9 章

アクセス コントロール ルール：レルムとユーザ

ライセンス：Control

ユーザ制御を実行する（レルム全体、個々のユーザ、ユーザ グループ、またはISE属性に基づいてアクセス コントロール ルール条件を作成する）前に、次のことを行う必要があります。

- モニタ対象の Microsoft Active Directory または LDAP サーバのそれぞれに対し、レルムを設定する。レルムに対してユーザのダウンロードを有効にすると、FirePOWER Management Centerは定期的および自動的に、新規に報告されたかすでに報告済みの、権限のあるユーザおよびユーザ グループのメタデータをダウンロードするようサーバに照会します。

（注） SGT ISE 属性条件の設定を計画しているものの、ユーザ、グループ、レルム、エンドポイント ロケーション、またはエンドポイント プロファイルの条件の設定は計画していない場合、レルムの設定はオプションです。

- レルムを認証方式に関連付けるために、アイデンティティ ポリシーを作成する。
- 1 つ以上のユーザ エージェントまたは ISE/ISE-PIC デバイス、あるいはキャプティブ ポータルを設定する。ISE 属性の条件を使用するには、ISE を設定する必要があります。

ユーザ エージェント、ISE/ISE-PIC およびキャプティブ ポータルは、アクセス コントロール ルール条件でユーザ制御に使用できる、権限のあるユーザ データを収集します。アイデンティティ ソースは、指定したユーザがホストにログイン、ログアウトしたり、LDAP または AD クレデンシャルを使用して認証する際にモニタします。

（注） ユーザ エージェントまたはISE/ISE-PICデバイスのモニタ対象に多くのユーザ グループを設定した場合、またはネットワークでホストにマップされるユーザ数が非常に多い場合、Firepower Management Center のユーザ制限が原因で、グループに基づいてユーザ マッピングがドロップされることがあります。その結果、レルム、ユーザ、またはユーザ グループ条件を持つアクセス コントロール ルールが、想定どおりに適用されない可能性があります。

1 つのユーザ条件で、最大 50 のレルム、ユーザおよびグループを [Selected Users] に追加できます。ユーザ グループを持つ条件は、そのグループのメンバー（サブグループのメンバーを含む）のいずれかが送信元/宛先であるトラフィックを照合します。ただし、個別に除外されたユーザと、除外されたサブグループのメンバーは含まれません。

ユーザ グループを含めると、すべてのセカンダリ グループのメンバーを含む、そのグループのすべてのメンバーが自動的に含められます。ただし、アクセス コントロール ルールでセカンダリ グループを使用する場合は、明示的にセカンダリ グループを含める必要があります。

（注） アクセス コントロール ルールがネットワーク トラフィックを評価する前に、ハードウェアベースの高速パス ルール、セキュリティ インテリジェンス ベースのトラフィック フィルタリング、SSL インスペクション、ユーザ識別、および一部の復号化と前処理が行われます。

- ユーザ アクセス コントロール ルールに関する問題のトラブルシューティング （162 ページ）
- アクセス コントロール ルールへのレルム、ユーザ、またはユーザ グループ条件の追加 （163 ページ）
- ISE 属性条件の設定 （164 ページ）

ユーザ アクセス コントロール ルールに関する問題のトラブルシューティング

ライセンス：Control

ユーザ アクセス コントロール ルールの予期しない動作に気付いたら、ルール、アイデンティティ ソース、またはレルムの設定を調整することを検討してください。

レルム、ユーザ、またはユーザ グループに対するアクセス コントロール ルールが適用されない

ユーザ エージェントまたはISE/ISE-PICデバイスのモニタ対象に多くのユーザ グループを設定した場合、またはネットワークでホストにマップされるユーザ数が非常に多い場合、FirePOWER Management Center のユーザ制限が原因で、システムがユーザ レコードをドロップすることがあります。その結果、レルムまたはユーザ条件を使用するアクセス コントロール ルールが想定どおりに適用されない可能性があります。

ユーザ グループまたはユーザ グループ内のユーザに対するアクセス コントロール ルールが想定どおりに適用されない

ユーザ グループ条件を含むアクセス コントロール ルールを設定する場合は、LDAP または Active Directory サーバでユーザ グループを設定している必要があります。サーバが基本的なオブジェクト階層でユーザを編成している場合、FirePOWER Management Center はユーザ グループ制御を実行できません。

セカンダリ グループ内のユーザに対するアクセス コントロール ルールが想定どおりに適用されない

Active Directory サーバのセカンダリ グループのメンバーであるユーザを含めるか除外するユーザ グループ条件を含むアクセス コントロール ルールを設定する場合、サーバは報告するユーザの数を制限していることがあります。

デフォルトでは、Active Directory サーバはセカンダリ グループから報告するユーザの数を制限します。この制限は、セカンダリ グループ内のすべてのユーザが FirePOWER Management Center に報告され、ユーザ条件を含むアクセス コントロール ルールでの使用に適するようにカスタマイズする必要があります。

アクセス コントロール ルールが、初めて表示されたユーザに一致していない

システムは、以前に表示されていないユーザからのアクティビティを検出すると、サーバから情報を取得します。システムがこの情報を正常に取得するまで、このユーザに表示されるアクティビティは、一致するアクセス コントロール ルールによって処理されません。代わりに、ユーザ セッションは、一致する次のアクセス コントロール ルール（またはアクセス コントロール ポリシーのデフォルト アクション）によって処理されます。

たとえば、次のような状況が考えられます。

- ユーザ グループのメンバーであるユーザが、ユーザ グループ条件を含むアクセス コントロール ルールに一致しない。
- ユーザ データ取得に使用されたサーバが Active Directory サーバである場合に、ISE/ISE-PIC またはユーザ エージェントによって報告されたユーザがアクセス コントロール ルールに一致しない。

これにより、システムがユーザ データをイベント ビューおよび分析ツールに表示するのが遅れる可能性があることに注意してください。

アクセス コントロール ルールへのレルム、ユーザ、またはユーザ グループ条件の追加

ライセンス：Control

はじめる前に

- ユーザ アイデンティティ ソース （429 ページ）の説明に従って、1 つ以上の権限のあるユーザ アイデンティティ ソースを設定します。
- レルムの作成 （409 ページ）の説明に従って、レルムを設定します。アクセス コントロール ルールでレルム、ユーザ、またはユーザ グループの条件を設定する前に、ユーザによるダウンロード（自動またはオンデマンド）が実行される必要があります。

ステップ 1 アクセス コントロール ルール エディタで、[Users] タブを選択します。
ステップ 2 [Available Realms] リストで、名前または値で検索してレルムを選択します。
ステップ 3 [Available Users] リストで、名前または値で検索してレルムを選択します。
ステップ 4 [Add to Rule] をクリックするか、ドラッグ アンド ドロップします。
ステップ 5 ルールを保存するか、編集を続けます。

ISE 属性条件の設定

ライセンス：Control

はじめる前に

- レルムの作成 （409 ページ）の説明に従って、レルムを設定します。アクセス コントロール ルールで ISE 属性条件を設定するには、その前にユーザによるダウンロード（自動またはオンデマンド）が実行される必要があります。

（注） SGT ISE 属性条件の設定を計画しているものの、ユーザ、グループ、レルム、エンドポイント ロケーション、またはエンドポイント プロファイルの条件の設定は計画していない場合、レルムの設定はオプションです。

- ISE/ISE-PIC 接続の設定 （436 ページ）の説明に従って ISE を設定します。

（注） ISE-PIC アイデンティティ ソースでは、ISE 属性データを提供しません。ISE を設定する必要があります。

ステップ 1 アクセス コントロール ルール エディタで、[SGT/ISE Attributes] タブをクリックします。
ステップ 2 [Available Attributes] リストで、名前または値で検索して属性を選択します。
ステップ 3 [Available Metadata] リストで、名前または値で検索してメタデータを選択します。
ステップ 4 [Add to Rule] をクリックするか、ドラッグ アンド ドロップします。

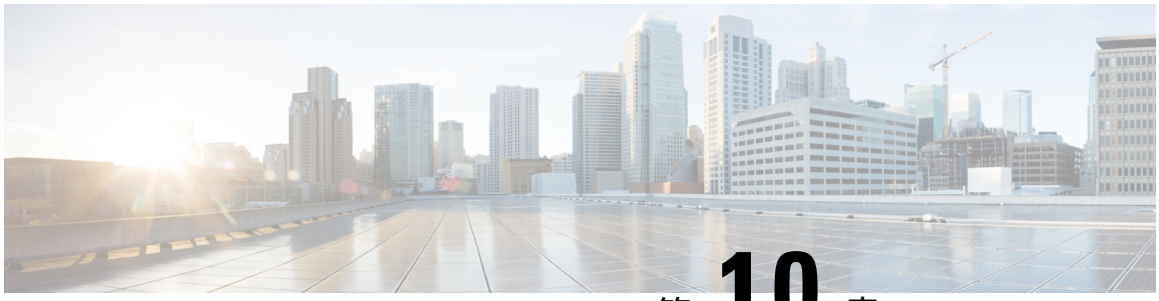
ステップ 5 [Add a Location IP Address] フィールドで、IP アドレスによりルールを制約します。

（注） ISE 属性条件を制約するために、ISE 割り当てセキュリティ グループ タグ（SGT）を使用できます。アクセス コントロール ルールでカスタム SGT を使用するには、ISE SGT およびカスタム SGT ルール条件 （167 ページ）を参照してください。

ステップ 6 ルールを保存するか、編集を続けます。

次のタスク

- 設定変更を展開します。設定変更の導入 （92 ページ）を参照してください。



第 10 章

アクセス コントロール ルール：カスタム セキュリティ グループ タグ

セキュリティ グループ タグ（SGT）は、信頼ネットワーク内におけるトラフィックの送信元の権限を指定します。ユーザが TrustSec または ISE でセキュリティ グループを追加すると、セキュリティ グループ アクセス（Cisco TrustSec と Cisco ISE の両方に共通の機能）が自動的に SGT を生成します。SGA は、パケットがネットワークに入ると、SGT 属性を適用します。ISE をアイデンティティ ソースとして設定するかまたはカスタム SGT オブジェクトを作成することで、アクセス コントロール用に SGT を使用できます。

カスタム SGT 条件により、カスタム SGT オブジェクトに基づいてアクセス コントロール ルールを設定できます。カスタム SGT オブジェクトの FirePOWER システムへの追加は、ISE を介して SGT を取得するのではなく、手動で行います。

カスタム SGT 条件を使用できるのは、アイデンティティ ソースとしての ISE/ISE-PIC を無効にしている場合のみです。

ISE SGT およびカスタム SGT ルール条件

ISE をアイデンティティ ソース（ISE SGT）として設定するかまたはカスタム SGT オブジェクト（custom SGT）を作成することで、アクセス コントロール用に SGT を使用できます。システムによる ISE SGT とカスタム SGT ルール条件の扱いは、次のように異なります。

ISE SGT：設定済みの ISE 接続がある

アクセス コントロール ルールでは、ISE SGT は ISE 属性条件として使用できます。[SGT/ISE Attributes] タブの [Available Attributes] リストから [Security Group Tag] を選択すると、システムは使用可能なタグを ISE に照会して、[Available Metadata] リストに入力します。パケットに SGT 属性が存在するかしないかにより、システムの応答が次のように決まります。

- SGT 属性がパケット内に存在している場合、システムはその値を抽出し、それをアクセス コントロール ルール内の ISE SGT 条件と比較します。
- SGT 属性がパケットにない場合、システムはパケットのソース IP アドレスと関連付けられている SGT が ISE で既知であるかどうかを判別し、SGT をアクセス コントロール ルール内の ISE SGT 条件と比較します。

カスタム SGT：設定済みの ISE 接続がない

カスタム SGT オブジェクトを作成し、それをアクセス コントロール ルール内の条件として使用できます。[SGT/ISE Attributes] タブの [Available Attributes] リストから [Security Group Tag] を選択すると、システムは [Available Metadata] リストに、ユーザが追加した SGT オブジェクトを入力します。パケットに SGT 属性が存在するかしないかにより、システムの応答が次のように決まります。

- SGT 属性がパケット内に存在している場合、システムはその値を抽出し、それをアクセス コントロール ルール内のカスタム SGT 条件と比較します。
- SGT 属性がパケット内にない場合、システムはパケットをアクセス コントロール ルール内のカスタム SGT 条件と照合しません。

カスタム SGT から ISE SGT ルール条件への自動移行

カスタム SGT オブジェクトを条件として使用してアクセス コントロール ルールを作成した後に ISE/ISE-PIC をアイデンティティ ソースとして設定した場合のシステムの動作は、次のとおりです。

- オブジェクト マネージャの [セキュリティ グループ タグ（Security Group Tag）] オブジェクト オプションを無効にします。ISE/ISE-PIC 接続を無効にしない限り、新規 SGT オブジェクトの追加、既存 SGT オブジェクトの編集、または新規条件としての SGT オブジェクトの追加はできません。
- 既存の SGT オブジェクトを保持します。これら既存のオブジェクトは変更できません。それらは、それらを条件として使用する既存のアクセス コントロール ルールのコンテキストでのみ表示できます。
- カスタム SGT 条件がある既存のアクセス コントロール ルールを保持します。カスタム SGT オブジェクトは手動編集でしか更新できないため、シスコはこれらのルールを削除するか、または無効にすることをお勧めしています。代わりに、SGT を ISE 属性条件として使用するルールを作成してください。システムは ISE 属性条件の SGT メタデータを更新するように ISE を自動的に照会しますが、手動編集ではカスタム SGT オブジェクトしか更新できません。

カスタム SGT 条件の設定

ライセンス：任意

カスタム セキュリティ グループ タグ（SGT）を設定する方法：

ステップ 1 アクセス コントロール ルール エディタで、[SGT/ISE Attributes] タブをクリックします。

ステップ 2 [Available Attributes] リストから [Security Group Tag] を選択します。

ステップ 3 [Available Metadata] リストで、カスタム SGT オブジェクトを見つけて選択します。

選択すると、ルールはSGT属性があるすべてのトラフィックと一致します。たとえば、この値は、TrustSec向けに構成されていないホストからのトラフィックをブロックするルールが必要な場合に選択できます。

ステップ 4 [Add to Rule] をクリックするか、ドラッグ アンド ドロップします。

ステップ 5 ルールを保存するか、編集を続けます。

次のタスク

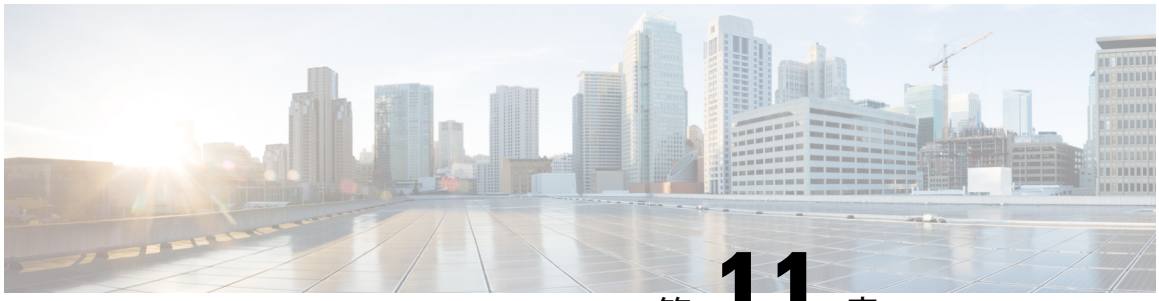
- 設定変更を展開します。設定変更の導入 （92 ページ）を参照してください。

カスタム SGT 条件のトラブルシューティング

予期しないルールの動作に気付いたら、カスタム SGT オブジェクトの設定を調整することを検討してください。

使用不可のセキュリティ グループ タグ オブジェクト

カスタム SGT オブジェクトは、ISE/ISE-PIC をアイデンティティ ソースとして設定していない場合にのみ使用できます。詳細については、カスタム SGT から ISE SGT ルール条件への自動移行 （168 ページ）を参照してください。



第 11 章

侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御

侵入ポリシーとファイルポリシーは連携し、トラフィックがその宛先に許可される前の最後の防御ラインとして機能します。

- **侵入ポリシー**は、システムの侵入防御機能を制御します。ネットワーク分析ポリシーと侵入ポリシーについて （297 ページ） を参照してください。
- **ファイル ポリシー**は、システムのネットワークベースのファイル制御および高度なマルウェア防御（AMP）機能を制御します。ファイル ポリシーの概要と作成 （453 ページ） を参照してください。

セキュリティインテリジェンスベースのトラフィックフィルタリング（ブロッキング）、SSL インスペクションベースの決定、およびトラフィックの復号化と前処理は、ネットワークトラフィックが侵入、禁止されたファイル、およびマルウェアの有無について検査される前に行われます。アクセス コントロール ルールおよびアクセス コントロールのデフォルト アクションによって、侵入ポリシーおよびファイル ポリシーで検査されるトラフィックが決まります。

侵入ポリシーまたはファイル ポリシーをアクセス コントロール ルールに関連付けることで、アクセスコントロールルールの条件に一致するトラフィックを通過させる前に、侵入ポリシーまたはファイルポリシー（またはその両方）を使ってトラフィックを検査するよう、システムに指示できます。

侵入防御および AMP では、次の表で説明されている特定のライセンス機能を有効にする必要があります。

表 *23* : 侵入インスペクションおよびファイル インスペクションのライセンス要件

機能	説明	License
侵入防御	侵入およびエクスプロイトを検出し、任意でブロックします	Protection
ファイル制御	ファイルタイプの伝送を検出し、任意でブロックします	Protection

機能	説明	License
高度なマルウェア防御（AMP）	マルウェアの伝送を検出、追跡し、任意でブロックします	Malware

侵入、禁止されたファイル、およびマルウェアの有無についてトラフィックを検査する詳細については、以下を参照してください。

- 許可されたトラフィックに対する侵入およびマルウェアの有無のインスペクション （172 ページ）
- 侵入防御パフォーマンスの調整 （177 ページ）
- ファイルおよびマルウェアのインスペクション パフォーマンスおよびストレージの調整 （190 ページ）

許可されたトラフィックに対する侵入およびマルウェアの有無のインスペクション

ライセンス：Protection または Malware

侵入ポリシーおよびファイル ポリシーは、トラフィックがその宛先に許可される前の最後の防衛ラインとして、システムの侵入防御、ファイル制御、およびAMP機能を制御します。セキュリティ インテリジェンス ベースのトラフィック フィルタリング、SSL インスペクションの決定（復号化を含む）、復号化および前処理、およびアクセス コントロール ルールの選択は、侵入およびファイルのインスペクションの**前に**発生します。

侵入ポリシーまたはファイル ポリシーをアクセス コントロール ルールに関連付けることで、アクセス コントロール ルールの条件に一致するトラフィックを通過させる前に、侵入ポリシーまたはファイル ポリシー（またはその両方）を使ってトラフィックを検査するよう、システムに指示できます。アクセス コントロール ルールの条件は単純または複雑のどちらにもできます。セキュリティ ゾーン、ネットワークまたは地理的位置、ポート、アプリケーション、要求された URL、およびユーザごとにトラフィックを制御できます。

システムは、指定した順にアクセス コントロール ルールをトラフィックと照合します。ほとんどの場合、システムは、すべてのルールの条件がトラフィックに一致する場合、最初のアクセス コントロール ルールに従ってネットワーク トラフィックを処理します。アクセス コントロール ルールのアクションによって、システムが一致するトラフィックをどのように処理するかが決まります。一致するトラフィックをモニタ、信頼、ブロック、または許可（追加のインスペクションあり/なし）することができます。を参照してください。 ルール アクションを使用したトラフィック処理とインスペクションの決定 （119 ページ）

インタラクティブ ブロック ルールには、許可ルールと同じインスペクション オプションがあることに留意してください。これにより、あるユーザが警告ページをクリック スルーすることによってブロックされた Web サイトをバイパスした場合に、悪意のあるコンテンツがないかトラフィックを検査できます。詳細については、インタラクティブブロッキングアクション：ユーザが Web サイト ブロックをバイパスすることを許可する （121 ページ）を参照してください。

ポリシー内のモニタ以外のアクセス コントロール ルールのいずれにも一致しないトラフィックは、デフォルトアクションによって処理されます。システムはデフォルトアクションによって許可されたトラフィックに対し侵入の有無を検査できますが、禁止されたファイルまたはマルウェアの有無は検査できないことに注意してください。アクセス コントロールのデフォルト アクションにファイル ポリシーを関連付けることは**できません**。

（注） 場合によっては、接続がアクセス コントロール ポリシーによって分析される場合、システムはトラフィックを処理するアクセス コントロール ルール（存在する場合）を決定する前に、その接続の最初の数パケットを処理し**通過を許可する**必要があります。しかし、これらのパケットは検査されないまま宛先に到達することはないので、デフォルト侵入ポリシーと呼ばれる侵入ポリシーを使用して、パケットを検査し侵入イベントを生成できます。

上記のシナリオの詳細と、ファイルポリシーおよび侵入ポリシーをアクセス コントロール ルールおよびアクセス コントロールのデフォルト アクションに関連付ける手順については、以下を参照してください。

ファイルインスペクションおよび侵入インスペクションの順序について

ライセンス：Protection または Malware

（注） 侵入防御のデフォルトアクションによって許可されたトラフィックは、侵入の有無について検査されますが、禁止されたファイルまたはマルウェアの有無については検査されません。アクセス コントロールのデフォルト アクションにファイル ポリシーを関連付けることは**できません**。

同じルールでファイルインスペクションと侵入インスペクションの両方を実行する必要はありません。許可ルールまたはインタラクティブ ブロック ルールに一致する接続の場合：

- ファイル ポリシーがない場合、トラフィック フローは侵入ポリシーによって決まります
- 侵入ポリシーがない場合、トラフィック フローはファイル ポリシーによって決まります

ヒント システムは、信頼されたトラフィックに対してはどんなインスペクションも実行しません。

アクセス コントロール ルールによって処理される単一接続の場合、ファイル インスペクションは侵入インスペクションの前に行われます。つまり、システムは侵入の有無についてファイル ポリシーによってブロックされたファイルを検査しません。ファイル インスペクション内では、タイプによる単純なブロッキングの方が、マルウェア インスペクションおよびブロッキングよりも優先されます。

（注） ファイルがセッションで検出されブロックされるまで、セッションからのパケットは侵入インスペクションの対象になります。

たとえば、アクセス コントロール ルールで定義された特定のネットワーク トラフィックを正常に許可するシナリオを考えてください。ただし、予防措置として、実行可能ファイルのダウンロードをブロックし、ダウンロードされた PDF のマルウェア インスペクションを行って検出された場合はブロックし、トラフィックに対して侵入インスペクションを実行する必要があるとします。

一時的に許可するトラフィックの特性に一致するルールを持つアクセス コントロール ポリシーを作成し、それを侵入ポリシーとファイル ポリシーの両方に関連付けます。ファイル ポリシーはすべての実行可能ファイルのダウンロードをブロックし、マルウェアを含む PDF の検査およびブロックも行います。

- まず、システムはファイル ポリシーで指定された単純なタイプ マッチングに基づいてすべての実行可能ファイルのダウンロードをブロックします。これはすぐにブロックされるため、これらのファイルは、マルウェア クラウド ルックアップの対象にも侵入インスペクションの対象にもなりません。
- 次に、システムは、ネットワーク上のホストにダウンロードされた PDF に対するマルウェア クラウド ルックアップを実行します。マルウェア ファイルの性質を持つ PDF はすべてブロックされ、侵入インスペクションの対象にはなりません。
- 最後に、システムはアクセス コントロール ルールに関連付けられている侵入ポリシーを使用して、ファイル ポリシーでブロックされなかったファイルを含む残りのトラフィック全体を検査します。

AMP またはファイル制御を実行するアクセス コントロール ルールの設定

ライセンス：Protection または Malware

アクセス コントロール ポリシーは、複数のアクセス コントロール ルールをファイル ポリシーに関連付けることができます。ファイル インスペクションを許可アクセス コントロール ルールまたはインタラクティブ ブロック アクセス コントロール ルールに設定でき、これによって、トラフィックが最終宛先に到達する前に、異なるファイルおよびマルウェアのインスペクション プロファイルをネットワーク上のさまざまなタイプのトラフィックと照合できます。

システムはファイル ポリシーの設定に従って禁止されたファイル（マルウェアを含む）を検出すると、イベントを自動的にロギングします。ログファイルまたはマルウェア イベントが必要ない場合は、アクセス コントロール ルールごとにこのロギングを無効にできます。アクセス コントロール ルールにファイル ポリシーを関連付けた後、アクセス コントロール ルール エディタの [Logging] タブで [Log Files] チェックボックスをオフにします。詳細については、許可された接続のファイルおよびマルウェア イベント ロギングの無効化（473 ページ）を参照してください。

また、システムは、呼び出し元のアクセス コントロール ルールのロギング設定に関係なく、関連付けられた接続の終了をロギングします。「ファイル イベントとマルウェア イベントに関連付けられた接続（自動）」を参照してください。

アクセス コントロール ルールにファイル ポリシーを関連付けるには、次の手順を実行します。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control] の順に選択します。

[Access Control Policy] ページが表示されます。

ステップ 2 アクセス コントロール ルールを使用して AMP またはファイル制御を設定するアクセス コントロール ポリシーの横にある編集アイコン（✎）をクリックします。

ステップ 3 新しいルールを作成するか、または既存のルールを編集します。を参照してください。アクセス コントロール ルールの作成および編集 （113 ページ）

アクセス コントロール ルール エディタが表示されます。

ステップ 4 ルール アクションが [Allow]、[Interactive Block]、または [Interactive Block with reset] のいずれかに設定されていることを確認します。

ステップ 5 [Inspection] タブを選択します。

[Inspection] タブが表示されます。

ステップ 6 アクセス コントロール ルールに一致するトラフィックを検査する場合は [File Policy] を選択し、または一致するトラフィックに対するファイル インスペクションを無効にする場合は [None] を選択します。

表示される編集アイコン（✎）をクリックして、ポリシーを編集できます。ファイル ポリシーの作成（460 ページ）を参照してください。

ステップ 7 [Add] をクリックしてルールを保存します。

ルールが保存されます。変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。を参照してください。 設定変更の導入 （92 ページ）

侵入防御を実行するアクセス コントロール ルールの設定

ライセンス：Protection

アクセス コントロール ポリシーは、複数のアクセス コントロール ルールを侵入ポリシーに関連付けることができます。侵入インスペクションを許可アクセス コントロール ルールまたはインタラクティブ ブロック アクセス コントロール ルールに設定でき、これによって、トラフィックが最終宛先に到達する前に、異なる侵入インスペクション プロファイルをネットワーク上のさまざまなタイプのトラフィックと照合できます。

システムが侵入ポリシーを使用してトラフィックを評価する場合、関連付けられた変数セットが使用されます。セット内の変数は、侵入ルールで一般的に使用される値を表し、送信元およ

び宛先の IP アドレスおよびポートを識別します。侵入ポリシーにある変数を使用して、ルール抑制および動的ルール状態にある IP アドレスを表すこともできます。

ヒント　システム提供の侵入ポリシーを使用する場合であっても、正確にネットワーク環境を反映するためにシステムの侵入変数を設定することを**強く**推奨します。少なくとも、デフォルトのセットにあるデフォルトの変数を変更します。を参照してください。事前定義されたデフォルト変数の最適化 （39 ページ）

異なる侵入ポリシー変数セットのペアを各許可ルールおよびインタラクティブ ブロック ルール（およびデフォルト アクション）と関連付けることができますが、ターゲット デバイスが設定されたとおりにインスペクションを実行するのに必要なリソースを不足している場合は、アクセス コントロール ポリシーを適用できません。詳細については、パフォーマンスを向上させるためのルールの簡素化 （94 ページ）を参照してください。

システムによって提供される侵入ポリシーとカスタム侵入ポリシーについて

シスコでは ASA FirePOWER モジュールで複数の侵入ポリシーを提供しています。システムによって提供される侵入ポリシーを使用することで、シスコ脆弱性調査チーム（VRT）の経験を活用できます。これらのポリシーでは、VRT は侵入ルールおよびプリプロセッサ ルールの状態を設定し、詳細設定の初期設定も提供します。システムによって提供されるポリシーをそのまま使用するか、またはカスタム ポリシーのベースとして使用できます。カスタム ポリシーを作成すれば、環境内のシステムのパフォーマンスを向上させ、ネットワーク上で発生する悪意のあるトラフィックやポリシー違反に焦点を当てたビューが提供されます。

お客様が独自に作成するカスタム ポリシーに加えて、システムは初期インライン ポリシーと初期パッシブ ポリシーの 2 つのカスタム ポリシーを提供しています。これらの 2 つの侵入ポリシーは、基本ポリシーとして「Balanced Security and Connectivity」侵入ポリシーを使用します。両者の唯一の相違点は [Drop When Inline] の設定です。インライン ポリシーではドロップ動作が有効化され、パッシブ ポリシーでは無効化されています。詳細については、システムによって提供されるポリシーとカスタム ポリシーの比較 （305 ページ）を参照してください。

接続イベントおよび侵入イベントのロギング

アクセス コントロール ルールで呼び出された侵入ポリシーは、侵入を検出すると、侵入イベントを生成します。また、システムはアクセス コントロール ルールのロギング設定に関係なく、侵入が発生した接続の終了を自動的にロギングします。「侵入に関連付けられた接続（自動）」を参照してください。

アクセス コントロール ルールに侵入ポリシーを関連付けるには、次の手順を実行します。

ステップ 1　[Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。

[Access Control Policy] ページが表示されます。

ステップ 2　アクセス コントロール ルールを使用して侵入インスペクションを設定するアクセス コントロール ポリシーの横にある編集アイコン（  ）をクリックします。

ステップ 3 新しいルールを作成するか、または既存のルールを編集します。を参照してください。 アクセス コントロール ルールの作成および編集 （113 ページ）

アクセス コントロール ルール エディタが表示されます。

ステップ 4 ルール アクションが [Allow]、[Interactive Block]、または [Interactive Block with reset] のいずれかに設定されていることを確認します。

ステップ 5 [Inspection] タブを選択します。

[Inspection] タブが表示されます。

ステップ 6 システムによって提供されるまたはカスタムの**侵入ポリシー**を選択するか、またはアクセス コントロール ルールに一致するトラフィックに対する侵入インスペクションを無効にするには [None] を選択します。

カスタム侵入ポリシーを選択する場合は、表示される編集アイコン（）をクリックして、ポリシーを編集できます。侵入ポリシーの編集 （345 ページ）を参照してください。

注意 シスコの担当者から指示された場合を除き、[Experimental Policy 1] を選択しないでください。シスコでは、試験用にこのポリシーを使用します。

ステップ 7 オプションで、侵入ポリシーに関連付けられている**変数セット**を変更します。

表示される編集アイコン（）をクリックして、変数セットを編集できます。変数セットの操作 （38 ページ）を参照してください。

ステップ 8 [Save] をクリックしてルールを保存します。

ルールが保存されます。変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。を参照してください。 設定変更の導入 （92 ページ）

侵入防御パフォーマンスの調整

ライセンス：Protection

Cisco では、侵入行為のトラフィックを分析する際のシステムのパフォーマンスを向上するための機能を提供しています。これらのパフォーマンス設定は、各アクセス コントロール ポリシーごとに設定し、その設定はその親のアクセス コントロール ポリシーによって呼び出されるすべての侵入ポリシーに適用されます。

侵入に関するパターン一致の制限

ライセンス：Protection

イベント キューで許可するパケット数を指定できます。また、ストリーム再構成の前後に、より大きなストリームに再構築されるパケットのインスペクションを有効または無効にできます。

イベント キューの設定：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。

[Access Control Policy] ページが表示されます。

ステップ 2 編集するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3 [Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4 [Performance Settings] の横にある編集アイコン（）をクリックし、表示されるポップアップ ウィンドウで [Pattern Matching Limits] タブを選択します。

ステップ 5 次のオプションを修正できます。

- [Maximum Pattern States to Analyze Per Packet] フィールドに、キューに含めるイベントの最大数の値を入力します。
- ストリーム再構成の前後で、データのより大きなストリームに再構築されるパケットを検査するには、[Disable Content Checks on Traffic Subject to Future Reassembly] を選択します。再構成の前後の検査はより多くの処理オーバーヘッドを必要とするため、パフォーマンスが低下する可能性があります。
- ストリーム再構成の前後で、データのより大きなストリームに再構築されるパケットのインスペクションを無効にするには、[Disable Content Checks on Traffic Subject to Future Reassembly] をオフにします。検査を無効にすると、ストリームの検査の処理オーバーヘッドが減少し、パフォーマンスが向上する場合があります。

ステップ 6 [OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。を参照してください。設定変更の導入 （92 ページ）

侵入ルールの正規表現制限のオーバーライド

ライセンス：Protection

パケット ペイロードの内容を検査するための侵入ルールで使用される PCRE のデフォルトの一致および再帰の制限をオーバーライドできます。デフォルトの制限によってパフォーマンスの最低レベルが確保されます。これらの制限をオーバーライドすると、セキュリティが向上する可能性がありますが、非効率的な正規表現に対してパケット評価を許可することで、パフォーマンスが著しく影響を受ける可能性もあります。

⚠

注意 非効率的なパターンの影響に関する知識があり、侵入ルールの作成経験が豊富であるユーザ以外は、デフォルトの PCRE の制限をオーバーライドしないでください。

次の表に、デフォルトの制限をオーバーライドするように設定できるオプションを示します。

表 *24*：正規表現の制約オプション

オプション	説明
Match Limit State	[Match Limit] をオーバーライドするかどうかを指定します。次の選択肢があります。 • [デフォルト（Default）] を選択して、[制限に合わせる（Match Limit）] に設定した値を使用する • [Unlimited] を選択して、無制限の数の試行を許可する • [カスタム（Custom）] を選択して、[制限に合わせる（Match Limit）] に対して 1 以上の制限を指定するか、または PCRE の一致の評価を完全に無効化するために 0 を指定する
Match Limit	PCRE 正規表現で定義されたパターンに一致することを試行する回数を指定します。
Match Recursion Limit State	[Match Recursion Limit] をオーバーライドするかどうかを指定します。次の選択肢があります。 • [Default] を選択して、[Match Recursion Limit] に設定した値を使用する • [Unlimited] を選択して、無制限の数の再帰を許可する • [Custom] を選択して、[Match Recursion Limit] に対して 1 以上の制限を指定するか、または PCRE の再帰を完全に無効化するために 0 を指定する [Match Recursion Limit] が意味を持つためには、[Match Limit] よりも小さい必要があることに注意してください。
Match Recursion Limit	パケット ペイロードに対して PCRE 正規表現を評価する際の再帰数を指定します。

PCRE オーバーライドの設定：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。
[Access Control Policy] ページが表示されます。

ステップ 2 編集するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。
アクセス コントロール ポリシー エディタが表示されます。

ステップ 3 [Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4 [Performance Settings] の横にある編集アイコン（）をクリックし、表示されるポップアップ ウィンドウで [Regular Expression Limits] タブを選択します。

ステップ 5 表「正規表現の制約オプション」にあるオプションはすべて変更できます。

ステップ 6 [OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。を参照してください。 設定変更の導入 （92 ページ）

パケットごとに生成される侵入イベントの制限

ライセンス：Protection

ルール エンジンがルールに対してトラフィックを評価する場合、特定のパケットまたはパケット ストリームに生成されたイベントをイベント キューに配置し、キュー内の上位のイベントをユーザ インターフェイスに報告します。複数のイベントが発生した場合、ルール エンジンが 1 個のパケットまたはパケット ストリームに対して複数のイベントを記録するように選択できます。これらのイベントのロギングにより、報告されたイベントを超えて情報を収集することができます。このオプションを設定する場合、キュー内に配置可能なイベントの数および記録されるイベントの数を指定できます。また、キュー内のイベントの順序を決定する条件を選択できます。

次の表に、1 個のパケットまたはストリームに対して記録されるイベントの数を決定するために設定できるオプションを示します。

表 *25 :* 侵入イベント ロギング制限のオプション

オプション	説明
Maximum Events Stored Per Packet	特定のパケットまたはパケット ストリームに対して保存できるイベントの最大数。
Maximum Events Logged Per Packet	特定のパケットまたはパケット ストリームに対して記録されるイベントの数。これは、[Maximum Events Stored Per Packet] の値を超えてはいけません。

オプション	説明
Prioritize Event Logging By	イベント キュー内のイベントの順序を決定するために使用する値。最上位のイベントがユーザ インターフェイスから報告されます。次の中から選択できます。 • [priority]：イベントの優先順位によってキュー内のイベントを並べ替えます。 • [content_length]：最も長い識別コンテンツの一致によってイベントを並べ替えます。イベントがコンテンツ長によって並べ替えられる場合、ルール イベントは常にデコーダ イベントおよびプリプロセッサ イベントよりも優先されます。

1 個のパケットまたはストリームに対して記録されるイベント数の設定：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。

[Access Control Policy] ページが表示されます。

ステップ 2 編集するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3 [Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4 [Performance Settings] の横にある編集アイコン（）をクリックし、表示されるポップアップ ウィンドウで [Intrusion Event Logging Limits] タブを選択します。

ステップ 5 表「侵入イベント ロギング制限のオプション」の任意のオプションを変更できます。

ステップ 6 [OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。を参照してください。 設定変更の導入 （92 ページ）

パケットおよび侵入ルール遅延しきい値の設定

ライセンス：Protection

デバイスの遅延をパケットおよびルール遅延しきい値構成の許容レベルで保持する必要性とともにセキュリティのバランスを保つことができます。

パケット遅延しきい値構成について

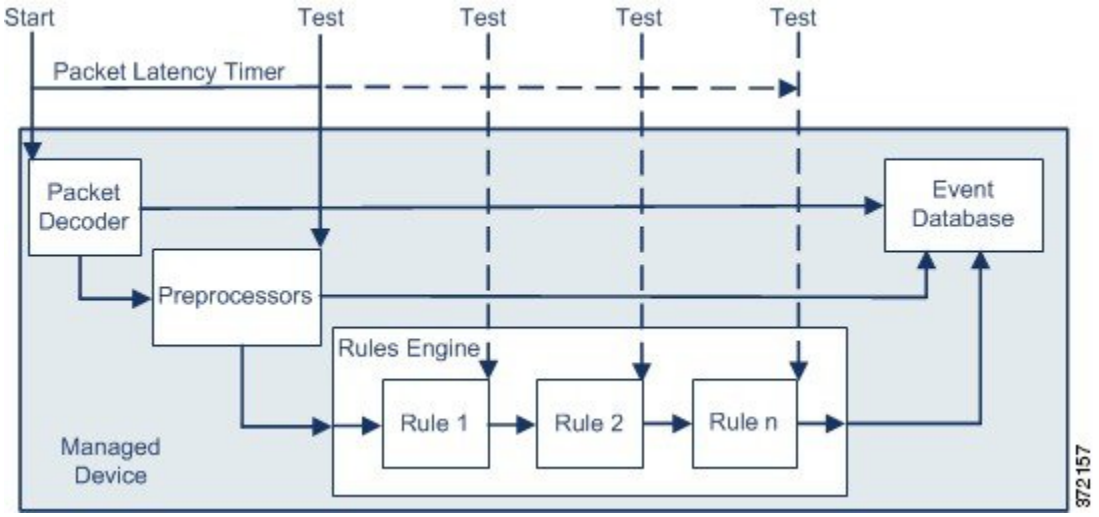
ライセンス：Protection

パケット遅延しきい値構成を有効にすることで、遅延を許容レベルで保持する必要性とセキュリティのバランスを取ることができます。パケット遅延しきい値構成は、該当するデコーダ、プリプロセッサ、およびルールによるパケット処理の総経過時間を測定し、処理時間が設定可能なしきい値を超えるとパケットのインスペクションを終了します。

パケット遅延しきい値構成は、ルールがパケットを処理する際に必要な実際の時間をより正確に反映するために、処理時間のみでなく、経過時間を測定します。ただし、遅延しきい値構成は、厳密なタイミングを強制しないソフトウェア ベースの遅延実装です。

遅延しきい値構成から生じるパフォーマンスと遅延のメリットに関するトレードオフは、未検査パケットに攻撃が含まれる可能性があることです。ただし、パケット遅延しきい値構成では、セキュリティと接続性のバランスを取るために使用可能なツールが用意されています。

デコーダの処理の開始時に各パケットのタイマーが起動します。タイミングは、パケットのすべての処理が終了するか、または処理時間がタイミング テスト ポイントでしきい値を超えるまで継続します。



上の図に示すように、パケット遅延タイミングは次のテスト ポイントでテストされます。

- すべてのデコーダおよびプリプロセッサの処理の完了後、ルールの処理が開始される前
- 各ルールによる処理の後

処理時間がいずれかのテスト ポイントでしきい値を超えると、パケット インスペクションは終了します。

ヒント パケットの合計処理時間にルーチン TCP ストリームまたは IP フラグメント再構成の時間は含まれません。

パケット遅延しきい値構成は、パケットを処理するデコーダ、プリプロセッサ、またはルールによってトリガーされるイベントに影響を与えません。該当するデコーダ、プリプロセッサ、またはルールは、パケットが完全に処理されるか、または遅延しきい値を超えたためにパケッ

ト処理が終了されるか、どちらか先に発生した時点まで通常通りトリガーされます。廃棄ルールがインライン展開の侵入を検知すると、その廃棄ルールがイベントをトリガーし、パケットは廃棄されます。

（注） パケット遅延しきい値違反のためにパケットの処理が終了した後は、ルールに対してパケットは評価されません。イベントを引き起こす可能性があったルールはそのイベントをトリガーできず、廃棄ルールに対してパケットを廃棄できません。

廃棄ルールの詳細については、を参照してください。 ルール状態の設定 （377 ページ）

パケット遅延しきい値構成は、パッシブとインラインの両方の展開でシステムのパフォーマンスを向上することができます。また、過剰な処理時間を必要とするパケットのインスペクションを停止することで、インライン展開の遅延を減らすことができます。これらのパフォーマンスのメリットは、たとえば次の場合に得られる可能性があります。

- パッシブ展開およびインライン展開の両方で、複数のルールによるパケットの順次検査に長時間かかる場合
- インライン展開で、ユーザが非常に大きなファイルをダウンロードするときなど、ネットワーク パフォーマンスの低下がパケット処理を遅らせる場合

パッシブ展開では、パケットの処理を停止しても、処理が単に次のパケットに移るだけで、ネットワーク パフォーマンスの回復につながらない可能性があります。

パケット遅延しきい値の設定

ライセンス：Protection

次の表に、パケット遅延しきい値構成でユーザが設定できるオプションを示します。

表 *26 :* パケット遅延しきい値構成オプション

オプション	説明
しきい値（マイクロ秒）	パケットのインスペクションが終了する時間をマイクロ秒単位で指定します。推奨される最小しきい値の設定については、表「最小のパケット遅延しきい値設定」を参照してください。

ルール 134:3 を有効にして、パケット遅延しきい値を超えたためにシステムがパケットのインスペクションを終了するイベントを生成できます。詳細については、「ルール状態の設定 （377 ページ）」を参照してください。

システムパフォーマンスおよびパケット遅延の測定に影響する要因は、CPU速度、データ レート、パケット サイズ、プロトコル タイプなど多数あります。このためシスコは、ユーザ独自の計算によってご自身のネットワーク環境に合った設定を行うまで、次の表のしきい値設定を使用することを推奨します。

表 *27:* 最小のパケット遅延しきい値設定

データ レート	最小しきい値設定（マイクロ秒）
1 Gbps	100
100 Mbps	250
5 Mbps	1000

独自の設定を計算する場合は、次の項目を決定します。

- 1 秒あたりの平均パケット数
- 1 パケットあたりの平均マイクロ秒数

パケットインスペクションを不必要に中断することがないように、ネットワークの1パケットあたりの平均マイクロ秒数に重要な安全係数を乗算します。

たとえば、表「最小のパケット遅延しきい値設定」では、1 ギガビット環境で 100 マイクロ秒の最小パケット遅延しきい値を推奨しています。この最小推奨値は、1 秒あたり平均 250,000 パケットを示すテストデータに基づいています。これは、1マイクロ秒あたり 0.25パケット、言い換えると 1 パケットあたり 4 マイクロ秒に相当します。25 倍すると推奨最小しきい値の 100 マイクロ秒が得られます。

パケット遅延しきい値の設定：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。

[Access Control Policy] ページが表示されます。

ステップ 2 編集するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3 [Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4 [Latency-Based Performance Settings] の横にある編集アイコン（）をクリックし、表示されるポップアップ ウィンドウで [Packet Handling] タブを選択します。

ステップ 5 推奨される最小しきい値の設定については、表「最小のパケット遅延しきい値設定」を参照してください。

ステップ 6 [OK] をクリックします。

変更を反映させるには、アクセスコントロールポリシーを保存して適用する必要があります。を参照してください。 設定変更の導入 （92 ページ）

ルール遅延しきい値構成について

ライセンス：Protection

ルール遅延しきい値構成を有効にすることで、遅延を許容レベルで保持する必要性とセキュリティのバランスを取ることができます。ルールの遅延しきい値構成は、各ルールが個別のパケットの処理に費やした時間を測定し、処理時間がルールの遅延しきい値を設定可能な回数を連続して超えた場合は、そのルールに違反した処理を、関連するルールのグループとともに指定された期間中断し、中断期間終了後にルールを回復します。

ルール遅延しきい値構成は、ルールがパケットを処理する際に必要な実際の時間をより正確に反映するために、処理時間のみでなく、経過時間を測定します。ただし、遅延しきい値構成は、厳密なタイミングを強制しないソフトウェア ベースの遅延実装です。

遅延しきい値構成から生じるパフォーマンスと遅延のメリットに関するトレードオフは、未検査パケットに攻撃が含まれる可能性があることです。ただし、ルール遅延しきい値構成では、セキュリティと接続性のバランスを取るために使用可能なツールが用意されています。

パケットがルールのグループに対して処理されるたびに、タイマーが処理時間を測定します。ルール処理時間が指定されたルール遅延しきい値を超えると、システムでカウンタが増加します。連続したしきい値違反の数が指定した数に達すると、システムは次のアクションを実行します。

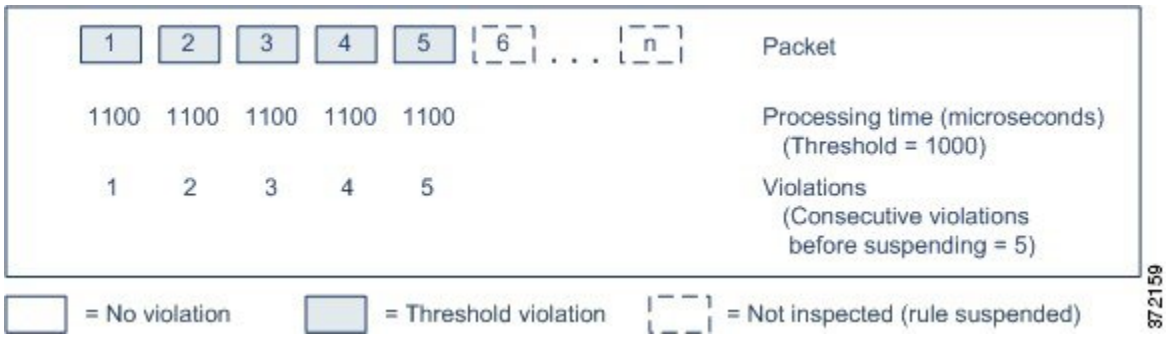
- 指定された時間、ルールを一時停止する
- ルールが一時停止されたことを示すイベントをトリガーとして使用する
- 一時停止期間が過ぎたらルールを再度有効にする
- ルールが再び有効になったことを示すイベントをトリガーとして使用する

ルールのグループが一時停止しているか、またはルール違反が連続していない場合は、カウンタがゼロになります。ルールを一時停止する前に連続する違反の一部を許可することにより、パフォーマンスへの影響がわずかであると考えられる散発的なルール違反を無視し、繰り返しルール遅延しきい値を超えるルールのより重大な影響に焦点を当てることができます。

次の例は、ルールが一時停止にならない、5 つの連続したルール処理時間を示します。

上の例で、最初の 3 個の各パケットの処理に必要な時間は 1000 マイクロ秒というルール遅延しきい値に違反し、違反カウンタは各違反のたびに増加します。4 個目のパケット処理はしきい値に違反しないので、違反カウンタはゼロにリセットされます。5 個目のパケットはしきい値に違反し、違反カウンタは 1 から再開します。

次の例は、ルールが一時停止になる、5 つの連続したルール処理時間を示します。



2 番目の例で、5 個のパケットのそれぞれの処理に必要な時間は 1000 マイクロ秒というルール遅延しきい値に違反します。各パケットの 1100 マイクロ秒というルール処理時間が指定された連続する 5 回の違反に対する 1000 マイクロ秒というしきい値に違反するため、ルールのグループは一時停止されます。図中のパケット 6 から n で表される後続のパケットは、一時停止期間が経過するまで、一時停止されたルールに対して検査されません。ルールが再有効化された後にさらにパケットが発生すると、違反カウンタはゼロから再開されます。

ルール遅延しきい値構成は、パケットを処理するルールによってトリガーされる侵入イベントに影響を及ぼしません。ルール処理時間がしきい値を超えるかどうかにかかわらず、パケット内で検出されるすべての侵入に対して、ルールはイベントをトリガーします。侵入を検知するルールがインライン展開の廃棄ルールである場合、パケットは廃棄されます。廃棄ルールがパケット内で侵入を検出し、その結果ルールが一時停止されると、廃棄ルールは侵入イベントをトリガーし、パケットは廃棄され、そのルールと関連するすべてのルールが一時停止されます。廃棄ルールの詳細については、を参照してください。 ルール状態の設定 （377 ページ）

（注） パケットは一時停止されたルールに対して評価されません。イベントを引き起こす可能性があった一時停止ルールはそのイベントをトリガーできず、廃棄ルールに対してパケットを廃棄できません。

ルール遅延しきい値構成は、パッシブとインラインの両方の展開でシステムのパフォーマンスを向上することができます。また、パケットの処理に最も多くの時間を必要とするルールを一時停止することで、インライン展開の遅延を減らすことができます。設定可能な時間が過ぎるまで、パケットは一時停止されたルールに対して再度評価されず、過負荷のデバイスに回復の時間が与えられます。これらのパフォーマンスのメリットは、たとえば次の場合に得られる可能性があります。

- 短期間で作成され、ほとんどテストされていないルールが過剰な処理時間を必要とする場合
- ユーザが非常に大きなファイルをダウンロードするときなど、ネットワーク パフォーマンスの低下がパケット インスペクションを遅らせる場合

ルール遅延しきい値の設定

ライセンス：Protection

ルール遅延しきい値、一時停止されるルールの一時停止時間、ルールを一時停止する前に発生する必要がある連続したしきい値違反の回数を変更することができます。

ルールによるパケット処理時間が、[Consecutive Threshold Violations Before Suspending Rule] で指定された回数連続して [Threshold] を超えると、ルール遅延しきい値構成は [Suspension Time] で指定された時間、ルールを一時停止します。

ルール 134:1 を有効にして、ルールが一時停止されるときにイベントを生成できます。また、ルール 134:2 を有効にして、一時停止されたルールが有効化されるときにイベントを生成できます。詳細については、ルール状態の設定 （377 ページ）を参照してください。

次の表に、ルール遅延しきい値構成でユーザが設定できるオプションを示します。

表 *28 :* ルール遅延しきい値構成のオプション

オプション	説明
しきい値	ルールがパケットを検査する際に超えることができない時間をマイクロ秒単位で指定します。推奨される最小しきい値の設定については、表「最小のルール遅延しきい値設定」を参照してください。
Consecutive Threshold Violations Before Suspending Rule	ルールが一時停止される前に、ルールによるパケットの検査時間が [Threshold] で設定された時間を超えることができる、連続した回数を指定します。
Suspension Time	ルールのグループを一時停止する秒数を指定します。

システム パフォーマンスの測定に影響する要因は、CPU 速度、データ レート、パケット サイズ、プロトコル タイプなど多数あります。このためシスコは、ユーザ独自の計算によってご自身のネットワーク環境に合った設定を行うまで、次の表のしきい値設定を使用することを推奨します。

表 *29 :* 最小のルール遅延しきい値設定

データ レート	最小しきい値設定（マイクロ秒）
1 Gbps	500
100 Mbps	1250
5 Mbps	5000

独自の設定を計算する場合は、次の項目を決定します。

- 1 秒あたりの平均パケット数
- 1 パケットあたりの平均マイクロ秒数

ルールを不必要に一時停止することがないように、ネットワークの1パケットあたりの平均マイクロ秒数に重要な安全係数を乗算します。

ルール遅延しきい値の設定：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。

[Access Control Policy] ページが表示されます。

ステップ 2 編集するアクセス コントロール ポリシーの横にある編集アイコン（✎）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3 [Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4 [Latency-Based Performance Settings] の横にある編集アイコン（✎）をクリックし、表示されるポップアップ ウィンドウで [Rule Handling] タブを選択します。

ステップ 5 表「ルール遅延しきい値構成のオプション」の任意のオプションを設定できます。

推奨される最小しきい値の設定については、表「最小のルール遅延しきい値設定」を参照してください。

ステップ 6 [OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。を参照してください。 設定変更の導入 （92 ページ）

侵入パフォーマンス統計情報のロギングの設定

ライセンス：Protection

デバイスがそのパフォーマンスを監視および報告する動作に関する基本的なパラメータを設定できます。これにより、次のオプションを設定することで、システムがデバイスのパフォーマンス統計情報を更新する間隔を指定できます。

[Sample time (seconds)] と [Minimum number of packets]

パフォーマンス統計情報の各更新の間で指定した秒数が経過すると、システムは指定したパケット数を分析したかを検証します。分析していた場合、システムはパフォーマンス統計情報を更新します。それ以外の場合、システムは指定したパケット数を分析するまで待機します。

Troubleshooting Options：**Log Session/Protocol Distribution**

トラブルシューティングの電話中に、プロトコル分布、パケット長、およびポートの統計情報のログを取るようにサポートから依頼される場合があります。

注意 このトラブルシューティング オプションの設定を変更するとパフォーマンスに影響するので、必ずガイダンスに従って実行してください。

Troubleshooting Options：**Summary**

トラブルシューティングの電話中に、Snortプロセスのシャットダウンまたは再起動時に限り、パフォーマンス統計情報を計算するようにシステムを設定するようにサポートから依頼される場合があります。このオプションを有効にするには、[Log Session/Protocol Distribution] トラブルシューティング オプションも有効にする必要があります。

注意 このトラブルシューティング オプションの設定を変更するとパフォーマンスに影響するので、必ずガイダンスに従って実行してください。

基本的なパフォーマンス統計情報パラメータの設定：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。

[Access Control Policy] ページが表示されます。

ステップ 2 編集するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3 [Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4 [Performance Settings] の横にある編集アイコン（）をクリックし、表示されるポップアップ ウィンドウで [Performance Statistics] タブを選択します。

ステップ 5 前述のように、[Sample time] または [Minimum number of packets] を変更します。

ステップ 6 任意で、サポートによって求められた場合にのみ、[Troubleshoot Options] セクションを展開し、そのオプションを変更します。

ステップ 7 [OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。設定変更の導入 （92 ページ） を参照してください。

ファイルおよびマルウェアのインスペクションパフォーマンスおよびストレージの調整

ライセンス：Protection または Malware

ファイル制御、またはマルウェアの検出あるいはブロッキングを行うためにファイルポリシーを使用する場合は、次の表にリストするオプションを設定できます。ファイルサイズを増やすと、システムのパフォーマンスに影響を与える可能性があることに注意してください。

表 *30*：アクセス コントロール ファイルおよびマルウェア検出の詳細オプション

フィールド	説明	デフォルト値	範囲	注意
Limit the number of bytes inspected when doing file type detection	ファイルタイプを検出するときに検査するバイト数を指定します。	1460 バイト、または TCP パケットの最大セグメント サイズ	0 ～ 4294967295（4 GB）	制限を取り除くには、0 に設定します。 ほとんどの場合、システムは最初のパケットによって、一般的なファイル タイプを特定できます。
Do not calculate SHA-256 hash values for files larger than (in bytes)	システムが一定のサイズを超えるファイルを保管すること、ファイルで Collective Security Intelligence クラウドルックアップを実行すること、またはカスタム検出リストに追加されたファイルをブロックすることを防止します。	10485760（10MB）	0 ～ 4294967295（4 GB）	制限を取り除くには、0 に設定します。
Allow file if cloud lookup for Block Malware takes longer than (seconds)	マルウェア クラウドルックアップの実行中に、システムが [Block Malware] ルールに一致し、性質がキャッシュに入れられていないファイルを保持する期間を指定します。システムが性質を取得する前にこの期間が満了すると、ファイルが渡されます。「使用不可」の性質はキャッシュに入れられません。	2 秒	0 ～ 30 秒	このオプションは最大 30 秒に設定できますが、デフォルト値を使用して、接続の障害によってトラフィックがブロックされないようにすることを推奨します。サポートに連絡することなく、このオプションを 0 に設定しないでください。

ファイルおよびマルウェアのインスペクションパフォーマンスおよびストレージを設定するには、次の手順を実行します。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。

[Access Control Policy] ページが表示されます。

ステップ 2 編集するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3 [Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定ページが表示されます。

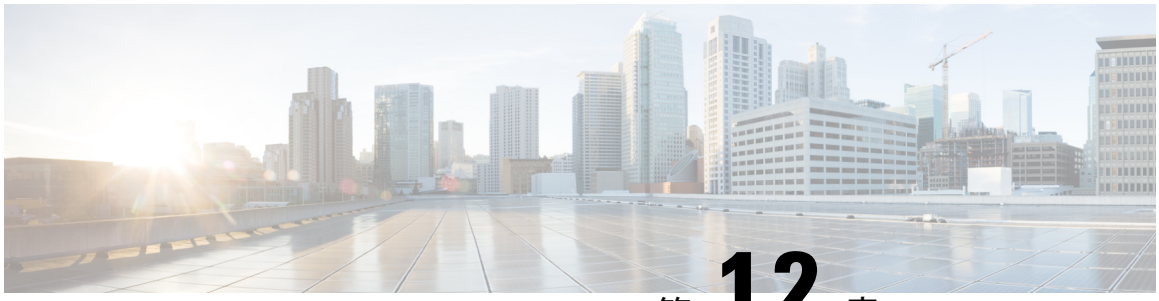
ステップ 4 [Files and Malware Settings] の横にある編集アイコン（）をクリックします。

[Files and Malware Settings] ポップアップ ウィンドウが表示されます。

ステップ 5 表「アクセス コントロール ファイルおよびマルウェア検出の詳細オプション」の任意のオプションを設定できます。

ステップ 6 [OK] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを保存して適用する必要があります。を参照してください。 設定変更の導入 （92 ページ）



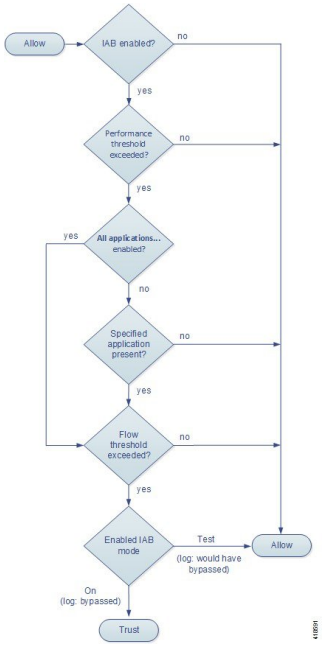
第 12 章

インテリジェント アプリケーション バイパス（IAB）

インテリジェントアプリケーションバイパス（IAB）は、パフォーマンスとフローのしきい値を超過した場合に追加のインスペクションなしでネットワークを通過する信頼するアプリケーションを特定します。たとえば、毎晩のバックアップがシステムパフォーマンスに大きく影響する場合、しきい値を超えてもバックアップアプリケーションが生成したトラフィックを信頼するように設定できます。オプションで、インスペクションパフォーマンスしきい値を超過したときに、IABが、いずれかのフローバイパスしきい値を超えるすべてのトラフィックをアプリケーションのタイプに関係なく信頼するようにIABを設定できます。

システムはトラフィックがディープインスペクションの対象となる前に、アクセスコントロール ルールまたはアクセス コントロール ポリシーのデフォルトのアクションで許可されたトラフィック上でIABを実行します。テストモードでは、しきい値を超えているかどうかを判断し、超えていた場合は、IABバイパスモードを有効にした場合にバイパスされたアプリケーションフローを特定できます。

次の図に、IAB意思決定プロセスを示します。



IAB オプション

状態（State）

IAB を有効または無効にします。

パフォーマンス サンプル インターバル（Performance Sample Interval）

IAB パフォーマンス サンプリング スキャンの間隔を秒で指定します。この間隔で、システムは、IAB パフォーマンスしきい値と比較するためのシステム パフォーマンス測定値を収集します。値を 0 にすると、IAB は無効になります。

バイパス可能なアプリケーションとフィルタ（Bypassable Applications and Filters）

この機能には、相互に排他的な、次の 2 つのオプションがあります。

アプリケーション/フィルタ（Applications/Filters）

バイパス可能なアプリケーションおよびアプリケーションのセット（フィルタ）を指定できるエディタを提供します。指定の方法は、アクセス コントロール ルールでアプリケーション条件を指定するときとほぼ同じです。詳細については、アプリケーション トラフィックの制御（140 ページ）を参照してください。

未確認アプリケーションを含むすべてのアプリケーション（All applications including unidentified application）

インスペクションパフォーマンスしきい値を超過すると、アプリケーションのタイプに関係なく、いずれかのフロー バイパスしきい値を超過するすべてのトラフィックを信頼します。

検査パフォーマンスしきい値（Inspection Performance Thresholds）

インスペクションパフォーマンスしきい値は、侵入インスペクションのパフォーマンスの限界を定めるもので、この限界を超えると、フローしきい値のインスペクションがトリガーされます。IAB では、0 に設定された インスペクション パフォーマンスしきい値は使用しません。

（注） インスペクション パフォーマンスしきい値とフロー バイパスしきい値は、デフォルトでは無効化されています。IAB がトラフィックを信頼するには、少なくともいずれか 1 つを有効化し、いずれか1つを超過している必要があります。インスペクションパフォーマンスしきい値またはフローバイパスしきい値を複数有効にした場合、IABがトラフィックを信頼するには、いずれか 1 つのみを超過する必要があります。

ドロップ率（Drop Percentage）

高価な侵入ルール、ファイルポリシー、圧縮解除などによるパフォーマンスのオーバーロードのためにパケットがドロップされたときの、パケット全体に対する割合としてドロップされた平均パケット数。これは、侵入ルールなどの通常の設定によってドロップされたパケットを参照するものではありません。1 より大きい整数を指定すると、指定されたパーセンテージのパケットがドロップされたときにIABがアクティブ化することに注意が必要です。1 を指定すると、0 ～ 1 までのパーセンテージによって IAB がアクティブ化します。これにより、少ないパケット数で IAB がアクティブ化します。

プロセッサ使用率（Processor Utilization Percentage）

使用されたプロセッサ リソースの平均比率。

パケット遅延

マイクロ秒単位の平均パケット遅延。

フロー レート（Flow Rate）

1 秒あたりのフロー数で測定される、システムによるフロー処理率。このオプションを使用すると、フロー数ではなくフロー レートを測定するように IAB が設定されることに注意してください。.

フロー バイパスしきい値（Flow Bypass Thresholds）

フローバイパスしきい値はフローの限界を定めるもので、この限界を超えると、IABは、バイパス モードではバイパス可能なアプリケーションを信頼し、テスト モードでは、アプリケーション トラフィックを許可してさらなるインスペクションの対象にします。IAB では、0 に設定された フロー バイパスしきい値は使用しません。

（注） インスペクション パフォーマンスしきい値とフロー バイパスしきい値は、デフォルトでは無効化されています。IAB がトラフィックを信頼するには、少なくともいずれか 1 つを有効化し、いずれか1つを超過している必要があります。インスペクション パフォーマンスしきい値またはフローバイパスしきい値を複数有効にした場合、IABがトラフィックを信頼するには、いずれか 1 つのみを超過する必要があります。

フローあたりのバイト数（Bytes per Flow）

フローに含めることができる最大キロバイト数。

フローあたりのパケット数（Packets per Flow）

フローに含めることができる最大パケット数。

フロー継続時間（Flow Duration）

フローを開いたままにできる最大秒数。

フロー速度（Flow Velocity）

最大転送速度（KB/秒）。

IAB の設定

注意 すべての展開にIABが必要なわけではありません。IABを使用する展開では、限定的な方法でIAB を使用する場合があります。ネットワーク トラフィック、特にアプリケーション トラフィックと、予測可能なパフォーマンスの問題の原因を含むシステム パフォーマンスの専門知識がない場合は、IABを有効にしないでください。IABをバイパス モードで実行する場合は、指定したトラフィックを信頼することでリスクが生じないことを事前に確認してください。

しきい値を超過する場合に、信頼できるものとしてネットワークを通過させるアプリケーションを指定する方法：

ステップ 1 アクセス コントロール ポリシー エディタで [Advanced] タブをクリックし、[Intelligent Application Bypass Settings] の横にある編集アイコンをクリックします。

代わりに表示アイコンが表示される場合、設定は先祖ポリシーから継承され、設定の変更権限はありません。設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ 2 IAB の各オプションを設定します。

- [State]：IAB を [Off] または [On]、あるいは [Test] モードで有効にします。
- [Performance Sample Interval]：IAB のパフォーマンス サンプリング スキャン間の時間を秒単位で入力します。IAB を有効にする場合は、テスト モードであっても、0 以外の値を入力します。0 を入力すると、IAB が無効化されます。

- バイパス可能なアプリケーションとフィルタ（Bypassable Applications and Filters）：次のいずれかを実行します。
  - バイパスするアプリケーションとフィルタの数をクリックし、トラフィックをバイパスするアプリケーションを指定します。これは、アクセス コントロール ルールでアプリケーション条件を指定するときとほぼ同じ方法です。詳細については、アプリケーション トラフィックの制御 （140 ページ）を参照してください。
  - [All applications including unidentified applications] をクリックし、インスペクション パフォーマンスしきい値を超過したときに、IAB が、いずれかのフロー バイパスしきい値を超えるすべてのトラフィックをアプリケーションのタイプに関係なく信頼するように設定します。
- [Inspection Performance Thresholds]：[Configure] をクリックし、1 つ以上のしきい値を入力します。
- [Flow Bypass Thresholds]：[Configure] をクリックし、1 つ以上のしきい値を入力します。

少なくとも 1 つのインスペクション パフォーマンスしきい値と 1 つのフロー バイパスしきい値を指定する必要があります。IAB がトラフィックを信頼するには、両方を超過する必要があります。各タイプのしきい値を複数入力した場合は、各タイプの 1 つのみを超過する必要があります。詳細については、IAB オプション （194 ページ）を参照してください。

ステップ 3 [OK] をクリックして IAB 設定を保存します。

ステップ 4 [Save] をクリックしてポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入 （92 ページ）を参照してください。

IAB のロギングと分析

IAB は、接続ロギングを有効にしたかどうかを問わず、バイパスされたフローやバイパスされることが予想されるフローをロギングする接続終了イベントを強制します。接続イベントは、バイパス モードでバイパスされたフロー、またはテスト モードでバイパスされることが予想されるフローを示します。接続イベントに基づいたカスタムのダッシュボード ウィジェットやレポートでは、バイパスされたフローおよびバイパスされることが予想されるフローの長期的な統計情報を表示できます。

IAB の接続イベント

アクション（Action）

[Reason] に [Intelligent App Bypass] が含まれる場合：

Allow：適用されている IAB 設定がテスト モードであり、[アプリケーション プロトコル（Application Protocol）] によって指定されたアプリケーションのトラフィックはインスペクション可能な状態のままであることを示します。

Trust：適用されている IAB 設定がバイパス モードであり、[アプリケーション プロトコル（Application Protocol）] によって指定されたアプリケーションのトラフィックが信頼され、さらなるインスペクションなしでネットワークを通過したことを示します。

理由（Reason）

[インテリジェント アプリケーション バイパス（Intelligent App Bypass）] は、IAB がバイパス モードまたはテスト モードでイベントをトリガーしたことを示します。

アプリケーション プロトコル（Application Protocol）

このフィールドには、イベントをトリガーしたアプリケーション プロトコルが表示されます。

例

次の省略された図では、一部のフィールドが省かれています。図は、2 つの別個のアクセス コントロール ポリシーの異なる IAB 設定から生成された 2 つの接続イベントの [アクション（Action）]、[理由（Reason）]、および [アプリケーション プロトコル（Application Protocol）] フィールドを示しています。

最初のイベントの場合、[信頼する（Trust）] アクションは、IAB がバイパス モードで有効にされており、Bonjour プロトコル トラフィックが信頼されているため、それ以上インスペクションが行われずに受け渡されることを示します。

2 番目のイベントの場合、[Allow] アクションは、IAB がテスト モードで有効にされているため、Ubuntu Update Manager トラフィックはさらにインスペクションが行われる必要がありますが、IAB がバイパス モードであればバイパスされることが予想されることを示します。

Action	Reason	Application Protocol
Trust	Intelligent App Bypass	Bonjour
Allow	Intelligent App Bypass	Ubuntu Update Manager

404433

例

次の省略された図では、一部のフィールドが省かれています。2 番目のイベントのフローはどちらもバイパス（[Action]：[Trust]、[Reason]：[Intelligent App Bypass]）されており、侵入ルール（[Reason]：[Intrusion Monitor]）によって検査されています。[Intrusion Monitor] の理由は、[Generate Events] に設定された侵入ルールが検出されたが、接続時にエクスプロイトがブロックされなかったことを示しています。この例では、これはアプリケーションが検出される前に発生しました。アプリケーションが検出された後、IAB は、アプリケーションがバイパス可能であると認識し、フローを信頼しました。

Last Packet	Action	Reason	Application Protocol
2015-06-12 10:53:09	Trust	Intelligent App Bypass	Skype Probe
2015-06-12 10:53:08	Trust	Intelligent App Bypass, Intrusion Monitor	HTTP

404541

IAB のカスタム ダッシュボード ウィジェット

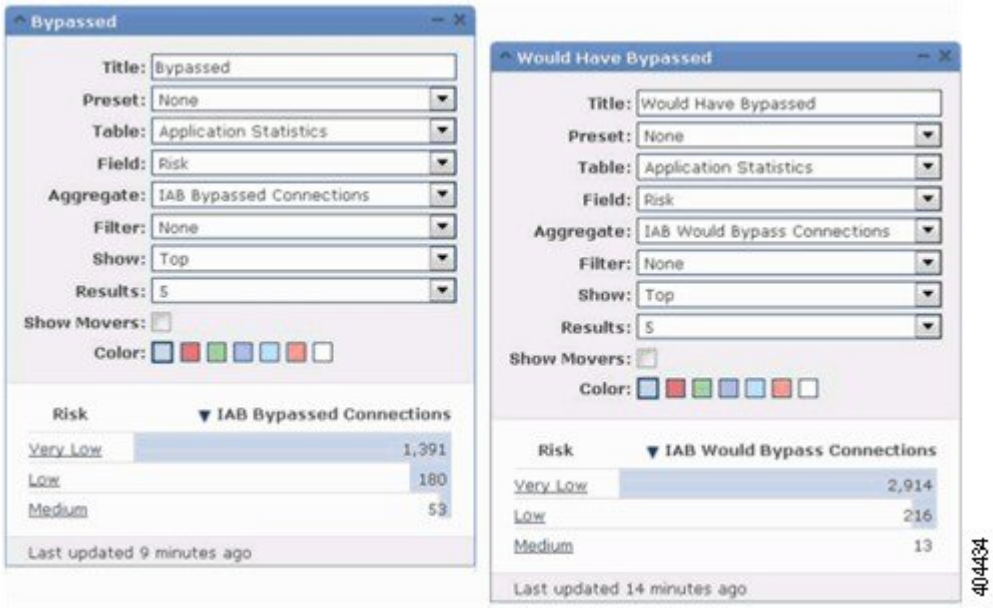
接続イベントに基づいて長期的なIABの統計情報を表示するカスタム分析ダッシュボードウィジェットを作成できます。ウィジェットを作成する際には、次の項目を指定します。

- [Preset]：[None]
- [Table]：[Application Statistics]
- フィールド（Field）：任意（any）
- 集約（Aggregate）：次のいずれか
  - IAB が接続をバイパスした（IAB Bypassed Connections）
  - IAB が接続をバイパスすることが予想された（IAB Would Bypass Connections）
- フィールド（Field）：任意（any）

例

次のカスタム分析ダッシュボード ウィジェットの例では、次のようになっています。

- 「*Bypassed*」の例は、アプリケーションがバイパス可能として指定され、IAB が展開済みのアクセス コントロール ポリシーにおいてバイパス モードで有効になっているためにバイパスされたアプリケーション トラフィックの統計を示しています。
- 「*Would Have Bypassed*」の例は、アプリケーションがバイパス可能として指定され、IAB が展開済みのアクセス コントロール ポリシーにおいてテスト モードで有効になっているためにバイパスされることが予想されたアプリケーショントラフィックの統計を示しています。



IAB のカスタム レポート

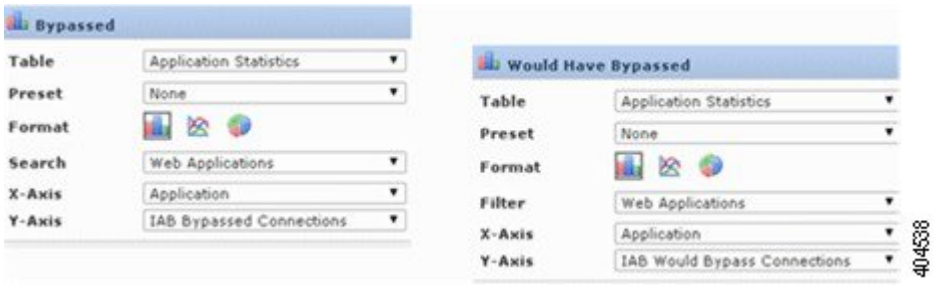
接続イベントに基づいて長期的な IAB の統計情報を表示するカスタム レポートを作成できます。レポートを作成する際には、次の項目を指定します。

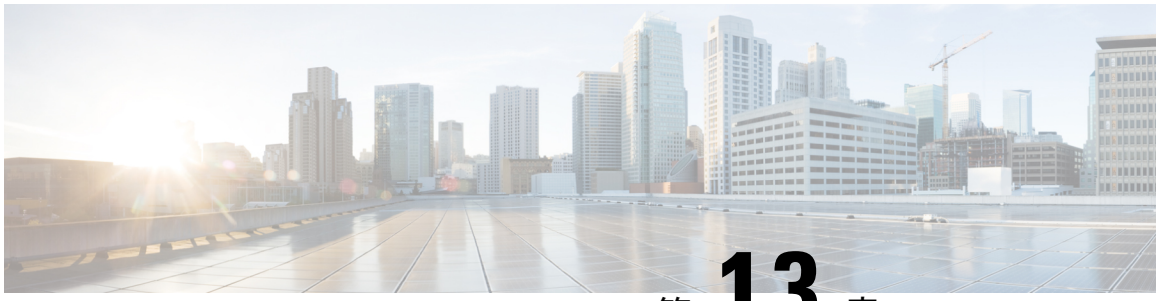
- [Table]：[Application Statistics]
- [Preset]：[None]
- フィールド（Field）：任意（any）
- X 軸（X-Axis）：任意（any）
- Y 軸（Y-Axis）：以下のいずれか
  - IAB が接続をバイパスした（IAB Bypassed Connections）
  - IAB が接続をバイパスすることが予想された（IAB Would Bypass Connections）

例

次の図は、2 つのレポートの例の抜粋を示します。

- [Bypassed] の例は、アプリケーションがバイパス可能として指定され、IAB が展開済みのアクセス コントロール ポリシーにおいてバイパス モードで有効になっているためにバイパスされたアプリケーション トラフィックの統計を示しています。「*Would Have Bypassed*」の例は、アプリケーションがバイパス可能として指定され、IAB が展開済みのアクセス コントロール ポリシーにおいてテスト モードで有効になっているためにバイパスされることが予想されたアプリケーション トラフィックの統計を示しています。





第 13 章

コンテンツ制限を使用したアクセス制御

主要な検索エンジンやコンテンツ配信サービスは、検索結果と Web サイトのコンテンツを制限できる機能を提供しています。たとえば学校では、「子どもをインターネットから保護する法律」（CIPA）を順守するために、コンテンツ制限機能を使用します。

コンテンツ制限機能は、検索エンジンやコンテンツ配信サービスで実行する場合には、個々のブラウザやユーザを対象にしか実施できません。FirePOWER システムは、これらの機能をご使用のネットワーク全体に拡大できます。

このシステムにより、以下を実施できます。

- セキュア検索：多くの主要な検索エンジンでサポートされているこのサービスは、特定の環境（ビジネス、行政、教育など）で不愉快であると分類されている、露骨なアダルト向けコンテンツを除外します。システムは、サポートされている検索エンジンのホームページへのユーザのアクセス機能は制限しません。YouTube 制限付きモードは、セーフサーチのサブ機能であることに注意してください。
- YouTube EDU：このサービスは、教育環境向けに YouTube コンテンツをフィルタリングします。これにより学校は、教育的なコンテンツへのアクセスを設定しながら、非教育的なコンテンツへのアクセスを制限できます。YouTube EDU は YouTube 制限付きモードとは別の機能であり、Google のセーフサーチ機能の一部として YouTube 検索に対する制限を実施します。YouTube EDU を使用すると、ユーザは標準の YouTube ホームページではなく、YouTube EDU ホームページにアクセスします。

コンテンツ制限機能は、検索またはコンテンツ照会の制限状態を、要求 URI の要素、関連する Cookie、またはカスタム HTTP ヘッダー要素により通信します。システムがトラフィックを処理するときに、これらの要素を変更するためのアクセス コントロール ルールを設定できます。

コンテンツ制限を実施するために、SSL ポリシーを有効にする必要もありますが、これはパフォーマンスに影響を与えることに注意してください。

これらのアクセス コントロール ルールに対して接続イベントのロギングを有効にすると、システムは [Reason] が [Content Restriction] の関連イベントをログに記録します。

- アクセス制御ルールのセーフサーチ オプション （202 ページ）
- アクセス コントロール ルールを使用したコンテンツ制限の実施 （202 ページ）
- アクセス制御ルールの YouTube EDU オプション （204 ページ）

• コンテンツ規制ルールの順序 （204 ページ）

アクセス制御ルールのセーフサーチ オプション

Firepower System は、特定の検索エンジンのセーフサーチ フィルタリングにのみ対応しています。サポートされる検索エンジンのリストについては、アクセス コントロール ルール エディタの [Applications] タブにある、[safesearch supported] とタグ付けされているアプリケーションを参照してください。サポートされない検索エンジンのリストについては、[safesearch unsupported] とタグ付けされているアプリケーションを参照してください。

アクセス コントロール ルールに対してセーフサーチを有効にするには、次のパラメータを設定します。

セーフサーチを有効にする

このルールに一致するトラフィックに対して、セーフサーチ フィルタリングを有効にします。

サポートされない検索トラフィック

サポートされていない検索エンジンからのトラフィックを処理するときにシステムが取るアクションを指定します。[Block] または [Block with Reset] を選択した場合は、システムが制限付きコンテンツをブロックしたときに表示する HTTP 応答ページも設定できます。ブロックされた URL のカスタム Web ページの表示 （157 ページ）を参照してください。

アクセス コントロール ルールを使用したコンテンツ制限の実施

ライセンス：任意

注意 ルールのプリエンプションを避けるため、SSL とアクセス コントロール ポリシーの両方で、YouTube EDU を制御するルールは、セーフサーチを制御するルールの上に配置します。詳細については、コンテンツ規制ルールの順序 （204 ページ）を参照してください。

アクセス コントロール ルールを使用してコンテンツ制限を実施する方法：

ステップ 1 SSL ポリシーを作成します。基本 SSL ポリシーの作成 （224 ページ）を参照してください。

ステップ 2 セーフサーチと YouTube EDU のトラフィックを処理するための SSL ルールを追加します。

- ルールの [Action] として [Decrypt - Resign] を選択します。システムは、コンテンツ制限処理にこれ以外のアクションは許可しません。
- [Applications] タブで、選択内容を [Selected Applications and Filters] リストに追加します。

- セーフサーチ：[safesearch supported] フィルタを追加します。
- YouTube EDU：[Available Applications] リストで「YouTube」を検索し、結果のアプリケーションを追加します。

詳細については、アプリケーション ベースの暗号化トラフィックの制御 （274 ページ）を参照してください。

ステップ 3 追加した SSL ルールのための、ルールの位置を設定します。クリックしてドラッグするか、または右クリック メニューを使用してカット アンド ペーストを実行します。

ステップ 4 アクセス コントロール ポリシーを作成または編集して、SSL ポリシーとアクセス コントロール ポリシーを関連付けます。アクセス制御への他のポリシーの関連付け （89 ページ）を参照してください。

ステップ 5 アクセス コントロール ポリシーでは、セーフサーチと YouTube EDU トラフィックを処理するためのルールを追加し、セーフサーチ ルールを YouTube EDU ルールの後に配置します。

- ルールの [Action] として [Allow] を選択します。システムは、コンテンツ制限処理にこれ以外のアクションは許可しません。
- [Applications] タブで、セーフサーチ（）または YouTube EDU（）のいずれかの淡色表示されているアイコンをクリックして、関連オプションを設定します。ルールに [Allow] 以外の [Action] を選択すると、これらのアイコンは淡色表示されるのではなく無効になります。

（注） 同じアクセス コントロール ルールに対してセーフサーチと YouTube EDU の制限を有効にすることはできません。

- [Applications] タブで、[Selected Applications and Filters] リストのアプリケーション選択を絞り込みます。

たいていの場合、セーフサーチまたは YouTube EDU を有効にすると、[Selected Applications and Filters] リストに適切な値が入力されます。セーフサーチまたは YouTube アプリケーションを有効にしたときにそれらの機能がすでにリストにある場合、システムはリストへの自動入力を行いません。予期したとおりにアプリケーションが入力を行わない場合は、それらを以下のように手動で追加します。

- セーフサーチ：検索エンジンフィルタを追加します。
- YouTube EDU：[Available Applications] リストで「YouTube」を検索し、結果のアプリケーションを追加します。

詳細については、アクセス コントロール ルールへのアプリケーション条件の追加 （144 ページ）を参照してください。

ステップ 6 追加したアクセス コントロール ルールに対してルールの位置を設定します。クリックしてドラッグするか、または右クリック メニューを使用してカット アンド ペーストを実行します。

ステップ 7 システムが制限付きコンテンツをブロックするときに表示する**ブロック応答ページ**を設定します。ブロックされた URL のカスタム Web ページの表示 （157 ページ）を参照してください。

次のタスク

次の作業

設定変更を展開します。設定変更の導入 （92 ページ）を参照してください。

アクセス制御ルールの YouTube EDU オプション

アクセス コントロール ルールに対して YouTube EDU を有効にするには、次のパラメータを設定します。

YouTube EDU の有効化

このルールに一致するトラフィックに対して、YouTube EDU フィルタリングを有効にします。

カスタム ID

学校または地域のネットワークを固有に識別する値を YouTube EDU イニシアチブに指定します。YouTube は、学校または地域が YouTube EDU アカウントの登録をすると、この ID を提供します。

（注） [Enable YouTube EDU] をオンにした場合は、[Custom ID] を入力する必要があります。この ID は、YouTube によって外部に定義されます。システムは、YouTube システムに対するユーザの入力内容は検証しません。無効な ID を入力すると、YouTube EDU の制限が予期したとおりに実行されない場合があります。

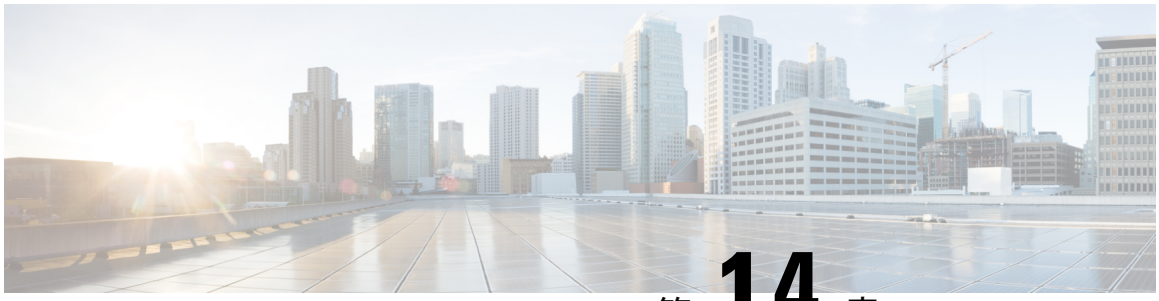
コンテンツ規制ルールの順序

SSL とアクセス コントロール ポリシーの両方でルールのプリエンプションを避けるため、YouTube の制限を制御するルールは、セーフサーチ制限を制御するルールの上に配置します。

アクセス コントロール ルールに対してセーフサーチを有効にする場合、システムは検索エンジンのカテゴリを [Selected Applications and Filters] リストに追加します。このアプリケーション カテゴリには YouTube が含まれます。結果として、YouTube EDU がさらに上位の評価優先順位を持つルールで有効にされていない限り、YouTube トラフィックはセーフサーチ ルールに一致します。

同様のルールのプリエンプションは、セーフサーチ サポート フィルタを持つ SSL ルールを、評価順序内で特定の YouTube アプリケーション条件を持つ SSL ルールよりも高い順序に配置した場合に生じます。

詳細については、パフォーマンスを向上させプリエンプションを回避するためのルールの順序付け （96 ページ）を参照してください。



第 14 章

トラフィック復号の概要

デフォルトでは、ASA FirePOWER モジュールはセキュア ソケット レイヤ（SSL）プロトコルまたはその後継である Transport Layer Security（TLS）プロトコルで暗号化されたトラフィックを検査できません。アクセス コントロールの一部として SSL インスペクション機能を使用すると、暗号化トラフィックを検査せずにブロックしたり、暗号化または復号化されたトラフィックをアクセス コントロールで検査したりできます。暗号化されたセッションをモジュールが処理するときは、トラフックの詳細がログに記録されます。暗号化トラフィックのインスペクションと暗号化セッションのデータ分析を組み合わせることで、ネットワーク内の暗号化されたアプリケーションやトラフィックをより詳細に把握したり制御したりできます。

トラフィック復号について

SSL インスペクションは、ポリシーベースの機能です。FirePOWER システムでは、アクセス コントロール ポリシーは、SSL ポリシーを含む、サブポリシーおよびその他の設定を呼び出すマスター設定です。アクセス コントロールと SSL ポリシーを関連付ければ、システムはアクセス コントロール ルールで評価する前に、その SSL ポリシーを使用して暗号化セッションを処理します。SSL インスペクションを設定していない場合、またはデバイスがサポートしていない場合、アクセス コントロール ルールは、すべての暗号化トラフィックを処理します。

暗号化されたトラフィックの通過が SSL インスペクション設定で許可される場合、そのトラフィックがアクセス コントロール ルールによって処理されることにも注意してください。ただし、一部のアクセス コントロール ルールの条件では暗号化されていないトラフィックを必要とするため、暗号化されたトラフィックに一致するルール数が少なくなる場合があります。また、デフォルトでは、システムは暗号化されたペイロードの侵入およびファイルのインスペクションを無効にしていますこれにより、侵入およびファイルインスペクションが設定されたアクセス コントロール ルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。詳細については、アクセス コントロール ルールの作成および編集 （113 ページ）を参照してください。

モジュールで TCP 接続での SSL または TLS ハンドシェイクが検出されると、そのトラフィックを復号化できるかどうかが判定されます。復号できない場合は、設定されたアクションが適用されます。以下のアクションを設定できます。

- 暗号化されたトラフィックをブロックし、オプションで TCP 接続をリセットする。
- 暗号化されたトラフィックを復号化しない。

モジュールによるトラフィックの復号化が可能な場合、それ以上のインスペクションなしでトラフィックをブロックするか、復号化されていないトラフィックをアクセス コントロールによって評価するか、または次のいずれかの方法を使用して復号化します。

- 既知の秘密キーを使用して復号する。外部ホストがネットワーク上のサーバとの SSL ハンドシェイクを開始すると、交換されたサーバ証明書とアプライアンスにアップロード済みのサーバ証明書が照合されます。次に、アップロード済みの秘密キーを使用してトラフィックを復号化します。
- サーバ証明書の再署名によって復号する。ネットワーク上のホストが外部サーバとの SSL ハンドシェイクを開始すると、システムによって、交換されたサーバ証明書が、アップロード済みの認証局（CA）証明書で再署名されます。次に、アップロード済みの秘密キーを使用してトラフィックを復号します。

復号化されたトラフィックに対しては、はじめから暗号化されていないトラフィックと同じ処理と分析が行われます。これには、ネットワーク、レピュテーション、ユーザベースのアクセス コントロール、侵入の検知と防止、および高度なマルウェア防御が該当します。システムで、復号されたトラフィックのポスト分析をブロックしない場合、トラフィックを再暗号化してから宛先ホストに渡します。

（注） トラフィックのブロックや発信トラフィックの復号化など、いくつかの SSL インスペクション アクションはトラフィックのフローを変更します。インライン展開された ASA FirePOWER モジュールは、これらのアクションを実行できます。パッシブ展開された ASA FirePOWER モジュールは、トラフィック フローを変更できません。ただし、これらのデバイスでも着信トラフィックを復号化することは可能です。詳細については、例：パッシブ展開でのトラフィック復号化 （214 ページ）を参照してください。

SSL ハンドシェイク処理

このマニュアルでは、SSL ハンドシェイクという用語は SSL プロトコルとその後継プロトコルである TLS の両方の暗号化セッションを開始する、2 ウェイ ハンドシェイクを表します。

パッシブ展開では、FirePOWER システムはハンドシェイクのコピーを確認しますが、実際のハンドシェイクを処理しません。インライン展開では、FirePOWER システムは SSL ハンドシェイクを処理し、ClientHello メッセージを修正する可能性があり、セッションの TCP プロキシ サーバとして機能します。

（正常に TCP 3 ウェイ ハンドシェイクが完了した後）クライアントがサーバとの TCP 接続を確立すると、管理対象デバイスは TCP セッションでの暗号化されたセッションの開始の試行をモニタします。SSL ハンドシェイクは、クライアントとサーバ間の特殊なパケットの交換によって、暗号化セッションを確立します。SSL と TLS プロトコルでは、これらの特殊なパケットはハンドシェイク メッセージと呼ばれます。ハンドシェイク メッセージは、クライアントとサーバの両方がサポートする暗号化属性を伝えます。

- ClientHello：クライアントは各暗号化属性に複数のサポートされる値を指定します。
- ServerHello：サーバはシステムがセキュリティで保護されたセッション中に使用する暗号化方式を決定する、各暗号化属性に 1 つのサポートされる値を指定します。

セッション中に伝送されるデータは暗号化されますが、ハンドシェイク メッセージは暗号化されません。

SSL ハンドシェイクが完了すると、管理対象デバイスは暗号化セッションデータをキャッシュに保存し、それによりフル ハンドシェイクを必要とせずにセッションを再開できます。管理対象デバイスもサーバ証明書データをキャッシュに保存し、それにより後続のセッションでのより速いハンドシェイクの処理が可能になります。

ClientHello メッセージ処理

セキュアな接続が確立できる場合、クライアントはパケットの宛先として機能するサーバに ClientHello メッセージを送信します。クライアントは SSL ハンドシェイクを開始するメッセージを送信するか、または、宛先サーバからの Hello Request メッセージへの応答に含めます。

SSL インスペクションを設定した場合、管理対象デバイスが ClientHello メッセージを受信すると、システムはそのメッセージを **Decrypt - Resign** アクションを含む SSL ルールと照合しようとします。照合は ClientHello メッセージからのデータとキャッシュされたサーバ証明書データからのデータに依存します。考えられるデータには次のものがあります。

SSL ルールの条件のデータの可用性

SSL ルールの条件	データの存在場所
ゾーン	ClientHello
Networks	ClientHello
VLAN タグ	ClientHello
ポート	ClientHello
ユーザ	ClientHello
アプリケーション	ClientHello（サーバ名インジケータの拡張機能）
カテゴリ	ClientHello（サーバ名インジケータの拡張機能）
Certificate	サーバ証明書（キャッシュされている可能性あり）

SSL ルールの条件	データの存在場所
Distinguished Names	サーバ証明書（キャッシュされている可能性あり）
証明書のステータス	サーバ証明書（キャッシュされている可能性あり）
暗号スイート	ServerHello
Versions	ServerHello

ClientHello メッセージが Decrypt - Resign ルールに一致しない場合、システムはメッセージを変更しません。次に、メッセージがアクセス コントロール評価（ディープ インスペクションを含めることができる）で合格するかどうかを決定します。メッセージが合格すれば、システムはそれを宛先サーバに送信します。

メッセージが Decrypt - Resign ルールに一致したら、システムは ClientHello メッセージを次のように変更します。

- 圧縮方法：クライアントがサポートする圧縮方法を指定する、compression_methods 要素を削除します。FirePOWER システムは圧縮されたセッションを復号化することはできません。この変更により、復号化できないトラフィックの圧縮されたセッション タイプが削減されます。
- 暗号スイート：FirePOWER システムがサポートしない場合、cipher_suites 要素から暗号スイートを削除します。FirePOWER システムが指定した暗号スイートのいずれもサポートしない場合、システムは、元の変更されていない要素を送信します。この変更により、復号化できないトラフィックのサポートされない暗号スイートと不明な暗号スイートが削減されます。
- セッション識別子：キャッシュされたセッション データと一致しない SessionTicket 拡張機能と Session Identifier 要素から値を削除します。ClientHello 値がキャッシュされたデータと一致した場合、一時停止したセッションは、クライアントとサーバが完全な SSL ハンドシェイクを実行せずに、中断したセッションを再開できます。この変更は、セッション再開の可能性を高め、復号化できないトラフィックのセッションが未キャッシュのタイプを削減します。
- 楕円曲線：FirePOWER システムがサポートしない場合、サポートされる楕円曲線拡張機能から楕円曲線を削除します。FirePOWER システムが指定した楕円曲線のいずれもサポートしない場合、管理対象デバイスは拡張機能を削除し、cipher_suites 要素から関連する暗号スイートを削除します。
- ALPN 拡張機能：FirePOWER システムでサポートされていないアプリケーション層プロトコル ネゴシエーション（ALPN）拡張機能から値を削除します（たとえば、SPDY と HTTP/2 プロトコル）。この変更は、メッセージがコンテンツ制限機能に関連付けられた SSL ルールに一致した場合にのみ実行されます。詳細については、コンテンツ制限を使用したアクセス制御 （201 ページ）を参照してください。
- 他の拡張機能：Extended Master Secret、Next Protocol Negotiation（NPN）、および TLS チャネル ID 拡張機能を削除します。

（注） システムはデフォルトでClientHelloの変更を実行します。SSLポリシーが正しく設定されていると、このデフォルトの動作により、トラフィックの復号化がより頻繁に発生します。各ネットワークにおけるデフォルトの動作を調整するには、サポートにお問い合わせください。

システムが ClientHello メッセージを変更した後、メッセージがアクセス コントロール評価（ディープインスペクションを含めることができる）を合格するかどうかを決定します。メッセージが合格すれば、システムはそれを宛先サーバに送信します。

メッセージを変更した後はクライアントおよびサーバで計算されたメッセージ認証コード（MAC）が一致しなくなるため、SSLハンドシェイク時のクライアントとサーバの間の直接通信はできなくなります。すべての後続のハンドシェイク メッセージ（および一度設定された暗号化セッションに対し）、管理対象デバイスは、中間者（MITM）として機能します。ここでは 2 つの SSL セッションが作成され、1 つはクライアントと管理対象デバイスの間、もう 1 つは管理対象デバイスとサーバの間で使用されます。その結果、暗号セッションの詳細はセッションごとに異なります。

（注） FirePOWER システムが復号化できる暗号スイートは頻繁に更新されるので、SSL ルールの条件で使用可能な暗号スイートと直接対応しません。現在、復号できる暗号スイートのリストについては、サポートに連絡してください。

ServerHello とサーバ証明書メッセージの処理

ServerHello メッセージは、正常な SSL ハンドシェイクの ClientHello メッセージへの応答です。

管理対象デバイスが ClientHello メッセージを処理し、宛先サーバに送信した後、サーバはクライアントがメッセージで指定した復号属性をサポートするかどうかを決定します。その属性をサポートしない場合、サーバはクライアントにハンドシェイクの失敗のアラートを送信します。その属性をサポートする場合、サーバは ServerHello メッセージを送信します。同意済みキー交換方式が認証に証明書を使用する場合、サーバ証明書メッセージはすぐに ServerHello メッセージに続きます。

管理対象デバイスがこれらのメッセージを受信すると、SSLルールとの一致を試みます。これらのメッセージには、ClientHello メッセージまたはセッション データ キャッシュにはなかった情報が含まれます。具体的には、システムは、識別名、証明書のステータス、暗号スイート、およびバージョン条件でのこれらのメッセージと一致する可能性があります。

メッセージがSSLルールと一致しない場合、管理対象デバイスは、SSLポリシーのデフォルトのアクションを実行します。詳細については、基本SSLポリシーの作成（224ページ）を参照してください。

メッセージがSSLルールに一致する場合、管理対象デバイスは、必要に応じて次に進みます。

アクション：Monitor

SSL ハンドシェイクは完了に進みます。管理対象デバイスは追跡およびログに記録しますが、暗号化トラックを復号化しません。

アクション：Block または Block with Reset

管理対象デバイスは、SSLセッションをブロックします。必要に応じて、TCP接続もリセットします。

アクション：Do Not Decrypt

SSL ハンドシェイクは完了に進みます。管理対象デバイスは、SSL セッションの間で交換されるアプリケーション データを復号化しません。

まれに、システムでは ClientHello メッセージと Decrypt - Resign ルールが一致してメッセージを変更しますが、関連する ServerHello メッセージは Do Not Decrypt ルールに一致することがあります。このような場合、クライアントから更新されたハンドシェイクをトリガーするために、システムは TCP 接続をリセットします。更新された ClientHello メッセージは Decrypt - Resign ルールに一致しなくなり、SSL セッションは復号化せずに進みます。

アクション：Decrypt - Known Key

管理対象デバイスは、サーバ証明書データを以前にアップロードされたサーバ証明書と照合しようとします。

証明書が以前に生成された証明書と一致した場合、SSL ハンドシェイクは完了に進みます。管理対象デバイスはアップロードされた秘密キーを使用して、SSL セッション中に交換されたアプリケーション データを復号化および再暗号化します。

まれに、システムでは、サーバ証明書メッセージが以前に生成された証明書と一致しないことがあります。たとえば、サーバはクライアントとの最初の接続と後続の接続の間に証明書を変更することがあります。この場合、システムはSSL接続をブロックし、クライアントが再接続して、システムが新しい証明書データとのハンドシェイクを処理できるようにします。

アクション：Decrypt - Resign

管理対象デバイスは、サーバ証明書メッセージを処理し、以前にアップロードされた認証局（CA）証明書で交換されるサーバ証明書を再署名します。SSL ハンドシェイクは完了に進みます。管理対象デバイスはアップロードされた秘密キーを使用して、SSL セッション中に交換されたアプリケーション データを復号化および再暗号化します。

ServerHello および証明書メッセージの処理中、管理対象デバイスは識別名と証明書データをキャッシュし、再確立されたセッションと、後続のSSLセッションの両方でハンドシェイクが高速で処理されるようにします。

SSL インスペクションの要件

ライセンス：機能に応じて異なる

構成設定やライセンスに加え、デバイスをネットワーク上にどのように展開しているかにより、暗号化トラフィックの制御や復号化に適用できるアクションが異なります。

SSL インスペクションの一部の機能では、公開キー証明書と秘密キーのペアが必要です。暗号化セッションの特性に応じてトラフィックを復号化したり制御したりするためには、証明書および秘密キーのペアを ASA FirePOWER モジュールにアップロードする必要があります。

SSL インスペクションをサポートする ASA FirePOWER モジュールの導入

ライセンス：任意

設定済みのインライン展開された ASA FirePOWER モジュールは、トラフィック フローを変更できます。これらのデバイスでは、着信および発信トラフィックのモニタリング、ブロック、許可、および復号化を行えます。

設定済みのパッシブ展開された ASA FirePOWER モジュールは、トラフィック フローを変更できません。これらのデバイスで行えるのは、着信トラフィックのモニタリング、許可、および復号だけです。パッシブ展開では、一時 Diffie-Hellman（DHE）および楕円曲線 Diffie-Hellman（ECDHE）の暗号スイートを使用した暗号化トラフィックの復号はサポートされません。

最適な展開タイプを決定するときは、マッピングされたアクション、既存のネットワーク展開、および全体的な要件のリストを確認してください。詳細については、「SSL インスペクション アプライアンス展開の分析 （213 ページ）」を参照してください。

SSL インスペクションのライセンス要件

ライセンス：機能に応じて異なる

ライセンスによっては、いくつかの条件を組み合わせて暗号化トラフィックの処理方法を決定できます。ASA FirePOWER モジュールでは、警告アイコン（  ）および確認ダイアログ ボックスを使用して、展開環境でサポートされない機能が示されます。警告アイコンの上にポインタを置くと詳細が表示されます。

アクセス コントロール ポリシーの一部として SSL ポリシーを適用すると、SSL ポリシーで復号化されたトラフィックがこのアクセス コントロール ポリシーにより検査されます。アクセス コントロールのライセンスの詳細については、アクセス コントロールのライセンスおよびロール要件 （81 ページ）を参照してください。

次の表に、アクセス コントロール ポリシーの一部として SSL ポリシーを適用するためのライセンス要件を示します。

表 *31 : SSL* インスペクションのライセンス要件

SSL ポリシーの機能	ライセンス
ゾーン、ネットワーク、ポート、または SSL 関連の基準に基づいて、暗号化されたトラフィックを処理する	任意

SSL ポリシーの機能	ライセンス
位置情報のデータを使用して暗号化トラフィックを処理する	任意
アプリケーションまたはユーザの条件を使用して暗号化トラフィックを処理する	Control
URL カテゴリおよびレピュテーションデータを使用して暗号化されたトラフィックをフィルタ処理する	URL Filtering

SSL ルールを設定するために必要な情報の収集

ライセンス：機能に応じて異なる

SSL インスペクションは、サポートする公開キー インフラストラクチャ（PKI）の多くの情報に依存しています。照合ルールの条件を設定するときは、その組織におけるトラフィック パターンについて検討する必要があります。次の表に示す情報を収集しておく必要があります。

表 *32 : SSL* ルール条件の設定に必要な情報

一致対象	必要な情報
自己署名サーバ証明書を含む、検出されたサーバ証明書	サーバ証明書
信頼できるサーバ証明書	CA 証明書
検出されたサーバ証明書のサブジェクトまたは発行元	サーバ証明書のサブジェクト DN または発行元 DN

詳細については、SSL ルールを使用したトラフィック復号化の調整（265 ページ）を参照してください。

ルールの適用先となる暗号化トラフィックの復号化、ブロック、モニタリングが不要かどうか、または復号化が必要かどうかについて検討します。その結果を、SSL ルールのアクション、復号化できないトラフィックのアクション、および SSL ポリシーのデフォルト アクションに反映させます。トラフィックを復号化する場合は、次の表に示す情報を収集しておく必要があります。

表 *33 : SSL* 復号に必要な情報

復号化の対象	必要な情報
制御対象のサーバへの着信トラフィック	サーバ証明書のファイルと秘密キー ファイルのペア
外部サーバへの発信トラフィック	CA 証明書のファイルと秘密キー ファイルのペア CA 証明書と秘密キーを生成することもできます。

詳細については、ルールアクションを使用した暗号化トラフィックの処理と検査の決定（248 ページ）を参照してください。

これらの情報を収集したら、システムにアップロードして、再利用可能なオブジェクトを設定します。詳細については、「再使用可能オブジェクトの管理 （23 ページ）」を参照してください。

SSL インスペクション アプライアンス展開の分析

ライセンス：機能に応じて異なる

ここでは Life Insurance Example, Inc.（LifeIns）という架空の生命保険会社で使われる複数のシナリオを例にして、同社のプロセス監査で利用されている暗号化トラフィックの SSL インスペクションについて解説します。LifeIns はそのビジネス プロセスに基づいて、以下の展開を計画しています。

- カスタマー サービス部門では、単一の ASA FirePOWER デバイスをパッシブ展開する
- 契約審査部門では、単一の ASA FirePOWER デバイスをインライン展開する

カスタマー サービスのビジネス プロセス

LifeIns はすでに顧客対応用の Web サイトを構築済みです。LifeIns は、保険契約に関する加入見込み客からの暗号化された質問や要求を、この Web サイトおよび電子メールで受け取ります。LifeIns のカスタマー サービスは、これらの要求を処理して 24 時間以内に必要な情報を返信しなければなりません。カスタマー サービスでは、着信するコンタクト メトリックのコレクションを拡張したいと思っています。LifeIns では、すでにカスタマー サービスに対する内部監査用のレビューが確立されています。

また、LifeIns は暗号化された申請書もオンラインで受信します。カスタマー サービス部門は申請書を 24 時間以内に処理し、申請書類のファイルを契約審査部門に送信しなければなりません。カスタマー サービスでは、オンライン フォームからの不正な申請をすべて除外するようにしていますが、この作業が同部門での作業のかなりの部分を占めています。

契約審査部門のビジネス プロセス

LifeIns の契約審査担当者は、Medical Repository Example, LLC（MedRepo）という医療データリポジトリに、オンラインで暗号化された医療情報要求を送信します。MedRepo はこれらの要求を評価し、LifeIns に暗号化されたレコードを 72 時間以内に送信します。その後は契約審査担当者が申請書類を査定し、保険契約および保険料に関連する判定を送信します。契約審査部門では、そのメトリック コレクションを拡張したいと思っています。

最近、不明な送信元からのスプーフィング（なりすまし）応答が LifeIns に送られてくるようになりました。LifeIns の契約審査担当者はインターネット使用に関する適切なトレーニングを受けていますが、LifeIns の IT 部門はまず、医療応答の形式で送られてくる暗号化トラフィックをすべて分析し、すべてのスプーフィング行為をブロックしたいと思っています。

LifeInsでは、経験の浅い契約審査担当者に対して6ヵ月のトレーニング期間を設けています。最近、こうした契約審査担当者がMedRepoのカスタマー サービス部門への暗号化された医療規制リクエストの送信を正しく行わない事例がありました。そのためMedRepoからLifeInsに複数の苦情が提出されています。LifeInsは、新任の契約審査担当者用のトレーニング期間を延長し、契約審査担当者からMedRepoへの要求についても監査を入れることを計画しています。

例：パッシブ展開でのトラフィック復号化

ライセンス：機能に応じて異なる

LifeInsのビジネス要件では、カスタマー サービスに次の要求をしています。

- すべての要求と申請書類を24時間以内に処理する。
- 着信するコンタクト メトリックのコレクション プロセスを改善する。
- 着信した不正な申請書類を特定して廃棄する。

カスタマー サービス部門では、追加の監査用レビューを必要としません。

LifeInsではカスタマー サービス デバイスのパッシブ展開を計画しています。

外部ネットワークからのトラフィックはLifeInsのルータに送信されます。ルータはトラフィックをカスタマー サービス部門にルーティングし、検査用にトラフィックのコピーをASA FirePOWERモジュールにミラーリングします。

ASA FirePOWERモジュールでは、アクセス コントロールおよびSSLエディタのカスタム ロールを持つユーザが、次のSSLインスペクションの設定を行います。

- カスタマー サービス部門に送信された暗号化トラフィックをすべてログに記録する。
- オンラインの申請フォームからカスタマーサービスに送信された暗号化トラフィックを復号化する。
- カスタマー サービスに送信された他の暗号化トラフィックは、オンライン リクエスト フォームからのトラフィックも含め、すべて復号化しない。

さらに、復号化された申請フォーム トラフィック中に偽の申請データが含まれていないかを検査し、検出された場合はログに記録するためのアクセス コントロールも設定します。

次のシナリオでは、ユーザからカスタマー サービスにオンライン フォームが送信されます。ユーザのブラウザは、サーバとのTCP接続を確立してから、SSLハンドシェイクを開始します。ASA FirePOWERモジュールは、このトラフィックのコピーを受信します。クライアントとサーバがSSLハンドシェイクを完了することで、暗号化されたセッションが確立されます。システムは、ハンドシェイクと接続の詳細に応じて、接続ログの記録および、暗号化トラフィックのコピーを処理します。

パッシブ展開で暗号化トラフィックをモニタする

ライセンス：任意

システムは、カスタマー サービスに送信されるすべての SSL 暗号化トラフィックに関する接続のログを記録します。

次のステップが実行されます。

1. ユーザがプレーンテキストの要求（info）を送信します。クライアントがこの要求（AaBb）を暗号化し、カスタマー サービスに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、カスタマー サービス部門のサーバにルーティングします。また、ASA FirePOWER モジュールにコピーをミラーリングします。
3. カスタマー サービス部門のサーバが暗号化された情報の要求（AaBb）を受信し、プレーン テキスト（info）に復号化します。
4. モジュールはトラフィックを復号化しません。

アクセス コントロール ポリシーが暗号化トラフィックの処理を続行し、これを許可します。セッション終了後、モジュールは接続イベントを生成します。

1. ASA FirePOWER モジュールは接続イベントを受信します。

パッシブ展開で暗号化トラフィックを復号化しない

ライセンス：任意

保険契約に関する要求を含むすべての SSL 暗号化トラフィックは復号化されずに許可され、接続のログが記録されます。

次のステップが実行されます。

1. ユーザがプレーンテキストの要求（info）を送信します。クライアントがこの要求（AaBb）を暗号化し、カスタマー サービスに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、カスタマー サービス部門のサーバにルーティングします。また、ASA FirePOWER モジュールにコピーをミラーリングします。
3. カスタマー サービス部門のサーバが暗号化された情報の要求（AaBb）を受信し、プレーン テキスト（info）に復号化します。
4. ASA FirePOWER モジュールはトラフィックを復号化しません。

アクセス コントロール ポリシーが暗号化トラフィックの処理を続行し、これを許可します。セッション終了後、モジュールは接続イベントを生成します。

1. ASA FirePOWER モジュールは接続イベントを受信します。

パッシブ展開で暗号化トラフィックを秘密キーで検査する

ライセンス：任意

申請フォームのデータを含むすべてのSSL暗号化トラフィックは復号され、接続のログが記録されます。

（注） パッシブ展開の場合、DHEまたはECDHE暗号スイートで暗号化されたトラフィックは、既知の秘密キーを使って復号化することはできません。

有効な申請フォームの情報を含むトラフィックについては、接続のログが記録されます。

次のステップが実行されます。

1. ユーザがプレーンテキストの要求（form）を送信します。クライアントがこの要求（AaBb）を暗号化し、カスタマー サービスに暗号化トラフィックを送信します。
2. LifeInsのルータが暗号化トラフィックを受信し、カスタマーサービス部門のサーバにルーティングします。また、ASA FirePOWER モジュールにコピーをミラーリングします。
3. カスタマー サービス部門のサーバが暗号化された情報の要求（AaBb）を受信し、プレーン テキスト（form）に復号化します。
4. ASA FirePOWER モジュールは、アップロードされた既知の秘密キーで取得したセッション キーを使用して、暗号化トラフィックをプレーン テキスト（form）に復号化します。

アクセス コントロール ポリシーは、復号化されたトラフィックの処理を継続します。偽の申請書であることを示す情報は検出されません。セッション終了後、モジュールは接続イベントを生成します。

1. ASA FirePOWERモジュールは、暗号化および復号化されたトラフィックの情報とともに、接続イベントを受信します。

これに対し、復号化されたトラフィックに偽の申請データが含まれていた場合、接続および偽のデータについてのログが記録されます。

次のステップが実行されます。

1. ユーザがプレーンテキストの要求（fake）を送信します。クライアントがこの要求（CcDd）を暗号化し、カスタマー サービスに暗号化トラフィックを送信します。
2. LifeInsのルータが暗号化トラフィックを受信し、カスタマーサービス部門のサーバにルーティングします。また、デバイスにコピーを送信します。
3. カスタマー サービス部門のサーバが暗号化された情報の要求（CcDd）を受信し、プレーン テキスト（fake）に復号化します。
4. ASA FirePOWER モジュールは、アップロードされた既知の秘密キーで取得したセッション キーを使用して、暗号化トラフィックをプレーン テキスト（fake）に復号化します。

アクセス コントロール ポリシーは、復号化されたトラフィックの処理を継続して、偽の申請書であることを示す情報を検出します。モジュールは侵入イベントを生成します。セッション終了後、デバイスは接続イベントを生成します。

1. ASA FirePOWER モジュールは、暗号化および復号化されたトラフィックの情報とともに、接続イベントおよび偽の申請データの侵入イベントを受信します。

例：インライン展開でのトラフィック復号化

ライセンス：機能に応じて異なる

LifeIns のビジネス要件では、契約審査部門に次の要求をしています。

- 新採用および経験の浅い契約審査担当者を監査し、MedRepo への情報要求が適切なすべての規則に準じていることを検証する。
- その契約審査によるメトリック コレクション プロセスを改善する。
- MedRepo が送信元と思われるすべての要求を調査し、スプーフィング行為を排除する。
- 契約審査部門から MedRepo のカスタマー サービス部門へのすべての不適切な規制要求を排除する。
- 経験豊富な契約審査担当者は監査しない。

LifeIns の契約審査部門では、デバイスのインライン展開を計画しています。

MedRepo のネットワークからのトラフィックは、MedRepo のルータに流されます。そこから LifeIns のネットワークにトラフィックがルーティングされます。デバイスはトラフィックを受信し、許可されたトラフィックを LifeIns のルータに転送して、ASA FirePOWER モジュールにイベントを送信します。LifeIns のルータは、トラフィックを宛先ホストにルーティングします。

ASA FirePOWER モジュールでは、ユーザが次の SSL インスペクションの設定を行います。

- 契約審査部門に送信された暗号化トラフィックをすべてログに記録する。
- LifeIns の契約審査部門から MedRepo のカスタマー サービス部門に不正に送信された暗号化トラフィックをすべてブロックする。
- MedRepo から LifeIns の契約審査部門宛て、および LifeIns の経験の浅い契約審査担当者から MedRepo のリクエスト部門宛てに送信される暗号化トラフィックをすべて復号化する。
- 経験豊富な契約審査担当者から送信される暗号化トラフィックは復号化しない。

さらに、カスタムの侵入ポリシーと以下の設定を使用して、復号化トラフィックを検査するアクセス コントロールを設定します。

- 復号化トラフィックでスプーフィング行為が検出された場合はそのトラフィックをブロックし、スプーフィング行為をログに記録する。

- 規制に準拠しない情報を含んでいる復号化トラフィックをブロックし、不適切な情報をログに記録する。
- 他の暗号化および復号化されたトラフィックをすべて許可する。

許可された復号化トラフィックは、再暗号化されて宛先ホストに転送されます。

次のシナリオでは、ユーザが情報をオンラインでリモートサーバに送信します。ユーザのブラウザは、サーバとの TCP 接続を確立してから、SSL ハンドシェイクを開始します。モジュールはこのトラフィックを受信し、ハンドシェイクと接続の詳細に応じて、システムが接続をログに記録し、トラフィックを処理します。システムがトラフィックをブロックした場合、TCP 接続も切断されます。トラフィックがブロックされない場合、クライアントとサーバが SSL ハンドシェイクを完了することで、暗号化されたセッションが確立されます。

インライン展開で暗号化トラフィックをモニタする

ライセンス：任意

契約審査部門で送受信されるすべての SSL 暗号化トラフィックについて、接続のログが記録されます。

次のステップが実行されます。

1. ユーザがプレーンテキストの要求（help）を送信します。クライアントがこの要求（AaBb）を暗号化し、MedRepo のリクエスト部門のサーバに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、リクエスト部門のサーバにルーティングします。
3. ASA FirePOWER モジュールはトラフィックを復号化しません。

アクセス コントロール ポリシーが暗号化トラフィックの処理を続行してこれを許可し、セッション終了後に接続イベントを生成します。

1. 外部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
2. 契約審査部門のサーバは、暗号化された情報の要求（AaBb）を受信し、プレーン テキスト（help）に復号化します。
3. ASA FirePOWER モジュールは接続イベントを受信します。

インライン展開で特定ユーザからの暗号化トラフィックを許可する

ライセンス：Control

経験豊富な契約審査担当者から送信されるすべての SSL 暗号化トラフィックは復号化されずに許可され、接続のログが記録されます。

次のステップが実行されます。

1. ユーザがプレーンテキストの要求（help）を送信します。クライアントがこの要求（AaBb）を暗号化し、MedRepo のリクエスト部門のサーバに暗号化トラフィックを送信します。
2. LifeIns のルータが暗号化トラフィックを受信し、リクエスト部門のサーバにルーティングします。
3. ASA FirePOWER モジュールはこのトラフィックを復号化しません。

アクセス コントロール ポリシーが暗号化トラフィックの処理を続行してこれを許可し、セッション終了後に接続イベントを生成します。

1. 外部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
2. リクエスト部門のサーバは、暗号化された情報の要求（AaBb）を受信し、プレーン テキスト（help）に復号化します

   .
3. ASA FirePOWER モジュールは接続イベントを受信します。

インライン展開で暗号化トラフィックをブロックする

ライセンス：任意

LifeIns の契約審査部門から MedRepo のカスタマー サービス部門に不正に送信されるすべての SMTPS 電子メール トラフィックは SSL ハンドシェイク時にブロックされ、追加の検査なしで接続のログが記録されます。

次のステップが実行されます。

1. カスタマー サービス部門のサーバは、クライアント ブラウザから SSL ハンドシェイクの確立要求を受信すると、SSLハンドシェイクの次のステップとして、サーバ証明書（cert）を LifeIns の契約審査担当者に送信します。
2. MedRepo のルータが証明書を受信し、これを LifeIns の契約審査担当者にルーティングします。
3. ASA FirePOWER モジュールは追加の検査を行わずにトラフィックをブロックし、TCP 接続を終了します。これにより、接続イベントが生成されます。
4. 内部ルータは、ブロックされたトラフィックを受信しません。
5. 契約審査担当者は、ブロックされたトラフィックを受信しません。
6. ASA FirePOWER モジュールは接続イベントを受信します。

インライン展開で暗号化トラフィックを秘密キーで検査する

ライセンス：任意

MedRepo から LifeIns の契約審査部門に送信されるすべての SSL 暗号化トラフィックは復号され、接続のログが記録されます。復号には、アップロードされたサーバ秘密キーを使って取得されたセッション キーが使用されます。正規のトラフィックは許可され、再暗号化されて契約審査部門に送信されます。

次のステップが実行されます。

1. ユーザがプレーン テキストの要求（stats）を送信します。クライアントがこの要求（AaBbC）を暗号化し、契約審査部門のサーバに暗号化トラフィックを送信します。
2. 外部ルータがトラフィックを受信し、これを契約審査部門のサーバにルーティングします。
3. ASA FirePOWER モジュールは、アップロードされた既知の秘密キーで取得したセッション キーを使用して、このトラフィックをプレーン テキスト（stats）に復号化します。

アクセス コントロール ポリシーは、カスタムの侵入ポリシーを使用して復号化トラフィックの処理を継続します。スプーフィング行為は検出されません。デバイスは暗号化トラフィック（AaBbC）を転送し、セッション終了後に接続イベントを生成します。

1. 内部ルータがトラフィックを受信し、これを契約審査部門のサーバにルーティングします。
2. 契約審査部門のサーバは、暗号化された情報（AaBbC）を受信し、プレーン テキスト（stats）に復号化します。
3. ASA FirePOWER モジュールは、暗号化および復号化されたトラフィックの情報とともに、接続イベントを受信します。

これに対し、スプーフィング行為の復号化トラフィックはすべてドロップされ、接続およびスプーフィング行為についてのログが記録されます。

次のステップが実行されます。

1. ユーザがプレーン テキストの要求（spoof）を送信しますが、このトラフィックは、発信元が MedRepo, LLC であるかのように改変されています。クライアントがこのトラフィック（FfGgH）を暗号化し、契約審査部門のサーバに暗号化トラフィックを送信します。
2. ASA FirePOWER モジュールは、アップロードされた既知の秘密キーで取得したセッション キーを使用して、このトラフィックをプレーン テキスト（spoof）に復号化します。

アクセス コントロール ポリシーは、カスタムの侵入ポリシーを使用して復号化トラフィックの処理を継続し、スプーフィング行為を検出します。ASA FirePOWER モジュールはトラフィックをブロックし、侵入イベントを生成します。セッション終了後、接続イベントを生成します。

1. 内部ルータは、ブロックされたトラフィックを受信しません。
2. 契約審査部門のサーバは、ブロックされたトラフィックを受信しません。

3. ASA FirePOWERモジュールは、暗号化および復号化されたトラフィックの情報とともに、接続イベントおよびスプーフィング行為の侵入イベントを受信します。

インライン展開で特定ユーザの暗号化トラフィックを再署名証明書で検査する

ライセンス：Control

新任および経験の浅い契約審査担当者から MedRepo のリクエスト部門に送信されるすべての SSL 暗号化トラフィックは復号され、接続のログが記録されます。復号には、再署名されたサーバ証明書を使って取得されたセッション キーが使用されます。正規のトラフィックは許可され、再暗号化されて MedRepo に送信されます。

（注） インライン展開においてサーバ証明書の再署名によりトラフィックを復号化する場合、ASA FirePOWER モジュールは中間者として機能します。2 つの SSL セッションが作成されます。1 つはクライアントと ASA FirePOWER モジュール間、もう 1 つは ASA FirePOWER モジュールとサーバ間のセッションです。その結果、暗号セッションの詳細はセッションごとに異なります。

次のステップが実行されます。

1. ユーザがプレーンテキストの要求（help）を送信します。クライアントがこの要求（AaBb）を暗号化し、リクエスト部門のサーバに暗号化トラフィックを送信します。
2. 内部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
3. ASA FirePOWERモジュールは、再署名されたサーバ証明書と秘密キーで取得したセッション キーを使用して、このトラフィックをプレーン テキスト（help）に復号化します。

アクセス コントロール ポリシーは、カスタムの侵入ポリシーを使用して復号化トラフィックの処理を継続します。不適切な要求は検出されません。モジュールはトラフィック（CcDd）を再暗号化して、送信を許可します。セッション終了後、接続イベントを生成します。

1. 外部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
2. リクエスト部門のサーバは、暗号化された情報（CcDd）を受信し、プレーン テキスト（help）に復号化します。
3. ASA FirePOWERモジュールは、暗号化および復号化されたトラフィックの情報とともに、接続イベントを受信します。

（注） 再署名されたサーバ証明書で暗号化されたトラフィックにより、信頼できない証明書についての警告がクライアントのブラウザに表示されます。この問題を避けるには、組織のドメインルートにある信頼できる証明書ストアまたはクライアントの信頼できる証明書ストアにCA証明書を追加します。

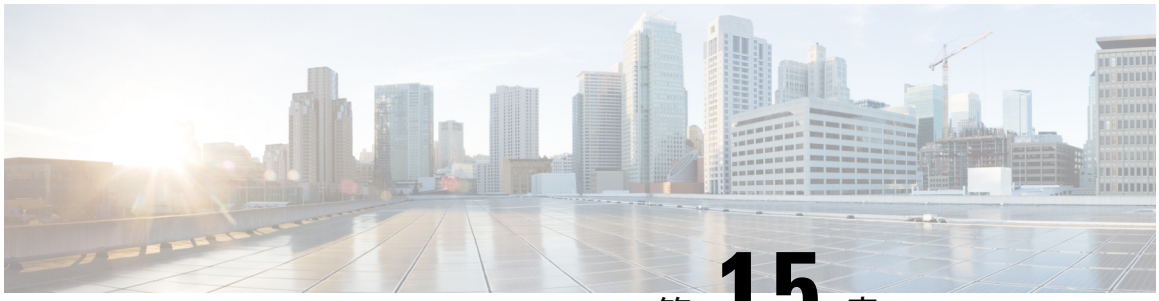
これに対し、規制要件を満たさない情報を含んでいる復号化トラフィックは、すべてドロップされます。接続および非準拠情報についてのログが記録されます。

次のステップが実行されます。

1. ユーザが規制要件に準拠していないプレーン テキストの要求（regs）を送信します。クライアントがこの要求（EeFf）を暗号化し、リクエスト部門のサーバに暗号化トラフィックを送信します。
2. 内部ルータがトラフィックを受信し、これをリクエスト部門のサーバにルーティングします。
3. ASA FirePOWERモジュールは、再署名されたサーバ証明書と秘密キーで取得したセッション キーを使用して、このトラフィックをプレーン テキスト（regs）に復号化します。

アクセス コントロール ポリシーは、カスタムの侵入ポリシーを使用して復号化トラフィックの処理を継続し、不適切な要求を検出します。モジュールはトラフィックをブロックし、侵入イベントを生成します。セッション終了後、接続イベントを生成します。

1. 外部ルータは、ブロックされたトラフィックを受信しません。
2. リクエスト部門のサーバは、ブロックされたトラフィックを受信しません。
3. ASA FirePOWERモジュールは、暗号化および復号化されたトラフィックの情報とともに、接続イベントおよび不適切な要求の侵入イベントを受信します。



第 15 章

SSL ポリシーの開始

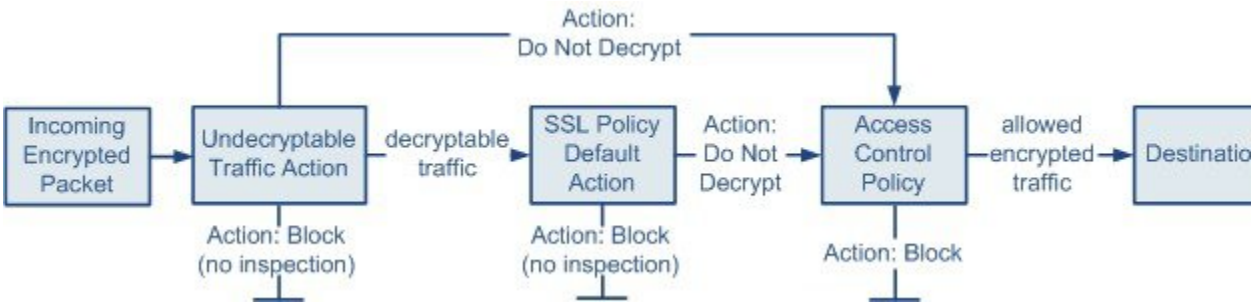
この章では、単純なSSLポリシーを作成して適用する方法について説明します。また、編集、更新、比較などの SSL ポリシー管理の基本情報も含まれています。

SSL ポリシーについて

SSL ポリシーは、ネットワーク上の暗号化トラフィックをシステムがどのように処理するかを決定します。SSL ポリシーを、1 つまたは複数設定できます。SSL ポリシーをアクセス コントロール ポリシーに関連付け、そのアクセス コントロール ポリシーを適用します。ASA FirePOWER モジュールで TCP ハンドシェイクが検出されると、アクセス コントロール ポリシーは最初にトラフィックの処理と検査を行います。次に TCP 接続上で SSL 暗号化セッションが識別された場合は、SSL ポリシーが引き継いで、暗号化トラフィックの処理および復号を行います。同時に適用できる SSL ポリシーは 1 つのみです。

最も単純な SSL ポリシーは、次の図のように、単一のデフォルト アクションで暗号化トラフィックを処理するように適用先のデバイスに指示します。デフォルトアクションは、それ以上のインスペクションなしで復号可能なトラフィックをブロックするか、あるいは復号可能なトラフィックを復号化されていない状態でアクセスコントロールによって検査するように設定できます。システムは、暗号化されたトラフィックを許可するか、またはブロックできます。ASA FirePOWER モジュールは復号化できないトラフィックを検出すると、トラフィックをそれ以上検査しないでブロックするか、または復号化しないでアクセスコントロールによる検査

を行います。



より複雑なSSLポリシーでは、各種の復号化できないトラフィックをさまざまなアクションで処理することが可能であり、認証局（CA）が証明書を発行したか、または暗号化証明書を信頼するかどうかに応じてトラフィックを制御したり、SSLルールを使ってきめ細かな暗号化トラフィックの制御およびログの記録を行ったりできます。これらのルールには、単純なものや複雑なものがあり、複数の基準を使用して暗号化トラフィックの照合および検査を行います。基本的なSSLポリシーの作成後は、個々の展開環境に応じた調整法の詳細について、次の章を参照してください。

- 再使用可能オブジェクトの管理 （23 ページ） では、再利用可能な公開キー インフラストラクチャ（PKI）オブジェクトおよびその他の SSL インスペクション関連オブジェクトを設定して、暗号化トラフィックの制御やトラフィックの復号化を強化する方法を説明しています。
- 「ネットワーク トラフィックの接続のロギング （467 ページ）」では、復号可能および復号化できない暗号化トラフィックに対するログの設定法を説明しています。
- 「アクセス コントロールを使用した復号化設定の適用 （232 ページ）」では、SSL ポリシーをアクセス コントロール ポリシーに関連付ける方法を説明しています。
- 「アクセス コントロール ポリシーの開始 （79 ページ）」では、アクセス コントロール ポリシーをデバイスに適用する方法を説明しています。
- 「アクセス コントロール ルールを使用したトラフィック フローの調整 （111 ページ）」では、復号化トラフィックを検査するアクセス コントロール ルールの設定法を説明しています。
- 「SSL ルールの開始 （239 ページ）」では、暗号化トラフィックの処理とログを記録する SSL ルールの設定法を説明しています。
- 「SSL ルールを使用したトラフィック復号化の調整 （265 ページ）」では、特定の暗号化トラフィックと SSL ルール条件の一致度を向上させる設定法を説明しています。

基本 SSL ポリシーの作成

ライセンス：任意

新しいSSLポリシーを作成するために最低限必要な操作は、そのポリシーに一意の名前を付けて、ポリシーのデフォルト アクションを指定することです。新しいポリシーのデフォルト アクションを選択する際には、次のオプションがあります。

- **Do not decrypt** は Do not decrypt デフォルト アクションでポリシーを作成します。
- **Block** は Block デフォルト アクションでポリシーを作成します。
- **Block with reset** は Block with reset デフォルト アクションでポリシーを作成します。

デフォルト アクションは、SSL ポリシーを作成した後で変更できます。デフォルト アクションの選択に関するガイダンスについては、暗号化トラフィックのデフォルトの処理と検査の設定 （226 ページ）を参照してください。

新しい SSL ポリシーにはシステムが復号化できないトラフィックのデフォルト アクションも含まれています。ユーザが復号化できないトラフィックに対して選択したデフォルトアクションを継承する、ブロックする、あるいはトラフィックを復号化せずアクセス コントロールで検査するなどのアクションです。復号化できないトラフィックに対するアクションは、SSL ポリシーの作成後に変更できます。復号できないトラフィック アクションの選択に関するガイダンスについては、復号できないトラフィックのデフォルト処理の設定 （227 ページ）を参照してください。

SSL ポリシーのページ（[Configuration] > [ASA FirePOWER Configuration] > [Policies] > [SSL]）で、オプションの説明とともに、現在のすべてのSSLポリシーを名前別に表示できます。このページのオプションを使用して、さまざまな操作を行うことができます。具体的には、ポリシーの比較、新規ポリシーの作成、ポリシーのコピー、各ポリシーに最近保存された設定をすべてリストするレポートの表示、ポリシーの編集、ポリシーの削除などです。

次の表で、SSLポリシーのページでポリシーを管理するために実行可能なアクションについて説明します。

表 *34 : SSL* ポリシー管理アクション

目的	操作
新しい SSL ポリシーを作成する	[New Policy] をクリックします。詳細については、「基本 SSL ポリシーの作成 （224 ページ）」を参照してください。
既存の SSL ポリシーの設定を変更する	編集アイコン（）をクリックします。詳細については、「SSL ポリシーの編集 （230 ページ）」を参照してください。
SSL ポリシーを比較する	[Compare Policies] をクリックします。詳細については、「SSL ポリシーの比較 （235 ページ）」を参照してください。
SSL ポリシーをコピーする	コピーアイコン（）をクリックします。コピーしたポリシーの編集の詳細については、SSL ポリシーの編集 （230 ページ）を参照してください。
SSL ポリシーの現在の設定を示す PDF レポートを表示する	レポートアイコン（）をクリックします。詳細については、「現在のトラフィック復号化設定のレポートの生成 （234 ページ）」を参照してください。

目的	操作
SSL ポリシーを削除する	削除アイコン（）をクリックし、[OK] をクリックします。続行するかどうかを尋ねるプロンプトで、ポリシー内に別のユーザの未保存の変更が存在するかどうかも通知されます。

SSL ポリシーを作成する手順：

ステップ 1 [Configuration] > > [ASA FirePOWER Configuration] > [Policies] > [SSL] の順に選択します。

[SSL Policy] ページが表示されます。

ステップ 2 [名前（Name）] に一意のポリシー名を入力し、オプションで [説明（Description）] にポリシーの説明を入力します。

スペース、特殊文字、を含めて、印刷可能なすべての文字を使用できます。

ステップ 3 [Default Action] で、デフォルト アクションを指定します。

選択したデフォルト アクションは、SSL ポリシーの作成後に変更できることに注意してください。詳細については、「暗号化トラフィックのデフォルトの処理と検査の設定 （226ページ）」を参照してください。

ステップ 4 [Store ASA FirePOWER Changes] をクリックします。

[SSL Policy Editor] ページが表示されます。詳細については、「SSL ポリシーの編集 （230 ページ）」を参照してください。

暗号化トラフィックのデフォルトの処理と検査の設定

ライセンス：任意

SSLポリシーのデフォルトアクションは、ポリシーのモニタ以外のルールと一致しない復号可能な暗号化トラフィックについてシステムがどのように処理するかを決定します。SSLルールがまったく含まれないSSLポリシーを適用する場合、ネットワーク上のすべての復号可能トラフィックの処理方法を、デフォルトアクションが決定します。システムが復号化できない暗号化トラフィックを処理する方法の詳細については、トラフィック復号の概要 （205ページ）を参照してください。

次の表に、選択可能なデフォルトアクションとそれが暗号化トラフィックに対して行う処理をリストします。デフォルトアクションでブロックされた暗号化トラフィックに対しては、システムはいかなる種類のインスペクションも行わないことに注意してください。

：

表 *35 : SSL* ポリシーのデフォルト アクション

デフォルトアクション	暗号化トラフィックに対して行う処理
Block	それ以上のインスペクションは行わずに SSL セッションをブロックする。
Block with reset	それ以上のインスペクションは行わずに SSL セッションをブロックし、TCP 接続をリセットする。
Do not decrypt	アクセス コントロールを使用して暗号化トラフィックを検査する。

SSL ポリシーを最初に作成する場合、デフォルト アクションによって処理される接続のログは、デフォルトでは無効化されています。デフォルト アクションと同様に、この設定もポリシー作成後に変更できます。

次の手順で、ポリシーの編集の際に SSL ポリシーのデフォルト アクションを設定する方法を説明します。SSL ポリシーを編集するための詳細な手順についてはSSL ポリシーの編集 （230 ページ）を参照してください。

SSL ポリシーのデフォルト アクションを設定する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [SSL] の順に選択します。

[SSL Policy] ページが表示されます。

ステップ 2 設定する SSL ポリシーの横にある編集アイコンをクリックします。

SSL ポリシー エディタが表示されます。

ステップ 3 [Default Action] を選択します。詳細については、暗号化トラフィックのデフォルトの処理と検査の設定（226 ページ）の表を参照してください。

ステップ 4 暗号化された接続および復号化できない接続のデフォルトのロギング設定（484 ページ）の説明に従って、デフォルト アクションのロギング オプションを設定します。

ステップ 5 [Store ASA FirePOWER Changes] をクリックします。

[SSL Policy Editor] ページが表示されます。詳細については、「SSL ポリシーの編集 （230 ページ）」を参照してください。

復号できないトラフィックのデフォルト処理の設定

ライセンス：任意

システムによる復号化や検査ができない特定タイプの暗号化トラフィックの処理については、SSL ポリシー レベルで、復号化できないトラフィック用のアクションを設定できます。SSL ルールがまったく含まれない SSL ポリシーを適用する場合、ネットワーク上のすべての復号化

できない暗号化トラフィックの処理方法は、復号化できないトラフィック用のアクションが決定します。

復号化できないトラフィックのタイプによって、次の選択ができます。

- 接続をブロックする。
- 接続をブロックした後でリセットする。
- アクセス コントロールを使用して暗号化トラフィックを検査する。
- SSL ポリシーのデフォルト アクションを継承する。

次の表に、復号化できないトラフィックのタイプを示します。

表 *36*：復号化できないトラフィック タイプ

タイプ	Description	デフォルト アクション	利用可能なアクション
圧縮されたセッション（Compressed Session）	SSLセッションはデータ圧縮メソッドを適用します。	デフォルト アクションを継承（Inherit default action）	Do not decrypt Block Block with reset デフォルト アクションを継承（Inherit default action）
SSLv2 Session	セッションは SSL バージョン 2 で暗号化されます。 トラフィックが復号可能となるのは、クライアントの HELLO メッセージが SSL 2.0 で、送信トラフィックの残りが SSL 3.0 である場合なので注意してください。	デフォルト アクションを継承（Inherit default action）	Do not decrypt Block Block with reset デフォルト アクションを継承（Inherit default action）
Unknown Cipher Suite	システムが認識できない暗号スイートです。	デフォルト アクションを継承（Inherit default action）	Do not decrypt Block Block with reset デフォルト アクションを継承（Inherit default action）
Unsupported Cipher Suite	検出された暗号スイートに基づく復号化を、システムはサポートしていません。	デフォルト アクションを継承（Inherit default action）	Do not decrypt Block Block with reset デフォルト アクションを継承（Inherit default action）

タイプ	Description	デフォルト アクション	利用可能なアクション
セッションが未キャッシュ（Session not cached）	SSL セッションでセッションの再利用が有効化されており、クライアントとサーバがセッション識別子を使ってセッションを再確立しているのに、システムでセッション識別子がキャッシュされていません。	デフォルト アクションを継承（Inherit default action）	Do not decrypt Block Block with reset デフォルト アクションを継承（Inherit default action）
ハンドシェイク エラー（Handshake Errors）	SSL ハンドシェイクのネゴシエーション中にエラーが発生しました。	デフォルト アクションを継承（Inherit default action）	Do not decrypt Block Block with reset デフォルト アクションを継承（Inherit default action）
Decryption Errors	トラフィックの復号化中にエラーが発生しました。	Block	Block Block with Reset

SSL ポリシーを最初に作成する場合、デフォルト アクションによって処理される接続のログは、デフォルトでは無効化されています。復号化できないトラフィックの処理ではデフォルト アクションのログ設定も適用されるため、復号化できないトラフィック用のアクションで処理される接続のログは、デフォルトでは無効化されています。デフォルトのロギング設定の詳細については、「SSL ルールを使用した復号可能接続のロギング （483 ページ）」を参照してください。

（注） クライアントとデバイスの間に HTTP プロキシがあり、クライアントとサーバが CONNECT HTTP メソッドを使用してトンネル SSL 接続を確立する場合、システムはトラフィックを復号化できません。このトラフィックのシステムによる処理法は、ハンドシェイク エラー（**Handshake Errors**）の復号化できないアクションが決定します。詳細については、「復号化アクション：さらに検査するためにトラフィックを復号化 （253 ページ）」を参照してください。

ブラウザが証明書ピニングを使用してサーバ証明書を確認する場合は、サーバ証明書に再署名しても、このトラフィックを復号化できないことに注意してください。このトラフィックはアクセス コントロールを使用して引き続き検査できるため、復号化できないトラフィック アクションでは処理されません。このトラフィックを許可するには、サーバ証明書の共通名または識別名と突き合わせるように、Do not decrypt アクションを使用して SSL ルールを設定します。

復号化できないトラフィックのデフォルト処理を設定する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [SSL] の順に選択します。

[SSL Policy] ページが表示されます。

ステップ 2 設定する SSL ポリシーの横にある編集アイコン（）をクリックします。

SSL ポリシー エディタが表示されます。

ステップ 3 [Undecryptable Actions] タブを選択します。

[Undecryptable Actions] タブが表示されます。

ステップ 4 各フィールドで、復号化できないトラフィック タイプで実行するアクションを選択するか、あるいは SSL ポリシーのデフォルト アクションを適用するかを指定します。詳細については、表 35 : SSL ポリシーのデフォルト アクション （227 ページ） の表を参照してください。

ステップ 5 [Store ASA FirePOWER Changes] をクリックします。

変更を反映させるには、関連付けたアクセス コントロール ポリシーを適用する必要があります（設定変更の導入 （92 ページ）を参照してください）。

SSL ポリシーの編集

ライセンス：任意

SSL ポリシー エディタでは、ポリシーの設定と SSL ルールの編成ができます。SSL ポリシーの設定では、ポリシーに一意の名前を付け、デフォルト アクションを指定する必要があります。次のことも実行できます。

- SSL ルールの追加、編集、削除、有効化/無効化
- 信頼できる CA 証明書を追加する
- システムが復号化できない暗号化トラフィックに対する処理の指定
- デフォルト アクションおよび復号化できないトラフィック アクションで処理されるトラフィックのログ

SSL ポリシーの作成または変更後は、SSL ポリシーをアクセス コントロール ポリシーに関連付け、そのアクセス コントロール ポリシーを適用します。カスタム ユーザ プロファイルを作成して、ユーザごとに、ポリシーの設定、編成、適用のための異なる権限を割り当てることもできます。

次の表は、SSL ポリシー エディタで実行可能な設定アクションを示しています。

表 *37 : SSL* ポリシーの設定アクション

目的	操作
ポリシーの名前または説明を変更する	[Name] フィールドまたは [Description] フィールドをクリックして、必要に応じて文字を削除し、新しい名前または説明を入力します。

目的	操作
デフォルト アクションを設定する	詳細については、暗号化トラフィックのデフォルトの処理と検査の設定（226 ページ）を参照してください。
復号化できないトラフィックのデフォルト処理を設定する	詳細については、復号できないトラフィックのデフォルト処理の設定（227 ページ）を参照してください。
デフォルト アクションと復号化できないトラフィック アクションの接続をログに記録する	詳細については、SSL ルールを使用した復号可能接続のロギング（483 ページ）を参照してください。
信頼できる CA 証明書を追加する	詳細については、外部認証局の信頼（289 ページ）を参照してください。
ユーザごとに異なる権限を割り当てる	詳細については、SSL ルールを設定するために必要な情報の収集（212 ページ）を参照してください。
ポリシーの変更を保存する	[保存（Save）] をクリックします。
ポリシーの変更をキャンセルする	[Cancel] をクリックします。変更を行った場合は、次に [OK] をクリックします。
ポリシーにルールを追加する	[Add Rule] をクリックします。詳細については、「SSL ルールの概要と作成（242 ページ）」を参照してください。 **ヒント** ルールの行の空白部分を右クリックし、[Insert new rule] を選択することもできます。
既存のルールを編集する	ルールの横にある編集アイコン（）をクリックします。詳細については、SSL ルールの概要と作成（242 ページ）を参照してください。 **ヒント** ルールを右クリックして、[Edit] を選択することもできます。
ルールを削除する	ルールの横にある削除アイコン（）をクリックし、[OK] をクリックします。 **ヒント** 選択したルールの行の空白部分を右クリックして [Delete] を選択した後、[OK] をクリックして、選択した 1 つ以上のルールを削除するという方法もあります。
既存のルールを有効または無効にする	選択したルールを右クリックして [State] を選択した後、[Disable] または [Enable] を選択します。無効なルールはグレーで表示され、ルール名の下に [(disabled)] というマークが付きます。
特定のルール属性の設定ページを表示する	ルールの行で、該当する条件のカラムに示されている名前、値、またはアイコンをクリックします。たとえば、[Source Networks] カラムに示されている名前または値をクリックすると、選択したルールの [Networks] ページが表示されます。詳細については、「SSL ルールを使用したトラフィック復号化の調整（265 ページ）」を参照してください。

設定を変更すると、変更がまだ保存されていないことを通知するメッセージが表示されます。変更を維持するには、ポリシーエディタを終了する前にポリシーを保存する必要があります。変更を保存しないでポリシーエディタを終了しようとすると、変更がまだ保存されていないことを警告するメッセージが表示されます。この場合、変更を破棄してポリシーを終了するか、ポリシー エディタに戻るかを選択できます。

セッションのプライバシーを保護するために、ポリシー エディタで 60 分間操作が行われないと、ポリシーの変更が破棄されて、[SSL Policy] ページに戻されます。30 分間操作が行われなかった時点で、変更が破棄されるまでの分数を示すメッセージが表示されます。以降、このメッセージは定期的に更新されて残りの分数を示します。ページで何らかの操作を行うと、タイマーがキャンセルされます。

複数のユーザが同じポリシーを同時に編集する際、ポリシーエディタに変更を保存していない他のユーザを特定するメッセージが表示されます。いずれかのユーザが変更を保存しようとすると、その変更によって他のユーザの変更が上書きされることを警告するメッセージが表示されます。同一のポリシーを複数のユーザが保存する場合、最後に保存された変更が維持されます。

SSL ポリシーを編集する手順：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [SSL] の順に選択します。

[SSL Policy] ページが表示されます。

ステップ 2 次の選択肢があります。

- ポリシーを設定する場合は、暗号化トラフィックのデフォルトの処理と検査の設定 （226ページ）SSL ルールの開始 （239 ページ）の表で説明されているすべての操作を使用できます。
- ポリシー ルールを編成する場合は、SSL ルールの順序指定によるパフォーマンス向上とプリエンプション回避 （259 ページ）の表で説明されているすべての操作を使用できます。

ステップ 3 設定を保存または廃棄します。次の選択肢があります。

- 変更を保存し、編集を続行する場合は、[Store ASA FirePOWER Changes] をクリックします。
- 変更を廃棄する場合は、[Cancel] をクリックし、プロンプトが出たら [OK] をクリックします。

変更は廃棄され、[SSL Policy] ページが表示されます。

アクセス コントロールを使用した復号化設定の適用

ライセンス：任意

SSL ポリシーに何らかの変更をした後は、関連付けられたアクセス コントロール ポリシーの適用が必要です。詳細については、設定変更の導入 （92 ページ）を参照してください。

SSL ポリシーを適用する場合は、次の点に注意してください。

- 適用された SSL ポリシー、または現在適用されている SSL ポリシーを削除することはできません。
- アクセス コントロール ポリシーを適用すると、関連付けられた SSL ポリシーが自動的に適用されます。SSL ポリシーを個別に適用することはできません。

（注） パッシブ展開では、システムがトラフィック フローに影響を与えることはありません。適用するアクセス コントロール ポリシーが参照する SSL ポリシーが、暗号化トラフィックをブロックするか、またはサーバ証明書を再署名することでトラフィックを復号化するように設定されている場合、システムから警告が表示されます。また、パッシブ展開では、一時 Diffie-Hellman（DHE）および楕円曲線 Diffie-Hellman（ECDHE）暗号スイートを使用した暗号化トラフィックの復号化をサポートしていません。

SSL ポリシーとアクセス コントロール ポリシーを関連付ける方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。

[Access Control Policy] ページが表示されます。

ステップ 2 設定するアクセス コントロール ポリシーの横にある編集アイコン（）をクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3 [Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定が表示されます。

ステップ 4 [General Settings] の横にある編集アイコン（）をクリックします。

[General Settings] ポップアップ ウィンドウが表示されます。

ステップ 5 [SSL Policy to use for inspecting encrypted connections] ドロップダウンから SSL ポリシーを選択します。

ステップ 6 [OK] をクリックします。

アクセス コントロール ポリシーの詳細設定が表示されます。

ステップ 7 [Store ASA FirePOWER Changes] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（設定変更の導入（92 ページ）を参照してください）。

現在のトラフィック復号化設定のレポートの生成

ライセンス：任意

SSL ポリシー レポートは、特定の時点でのポリシーとルール設定の記録です。このレポートは、監査目的や、現行の設定を調べるために使用できます。

ヒント　また、ポリシーを現在適用されているポリシーまたは別のポリシーと比較する SSL 比較レポートを生成することもできます。詳細については、SSL ポリシーの比較 （235 ページ）を参照してください。

SSL ポリシー レポートには、次の表で説明するセクションが含まれます。

表 *38 : SSL* ポリシー レポートのセクション

セクション	説明
Title Page	ポリシー レポートの名前、ポリシーが最後に変更された日時、その変更を行ったユーザの名前が記載されます。
Table of Contents	レポートの内容が記載されます。
Policy Information	ポリシーの名前と説明、ポリシーを最後に変更したユーザの名前、ポリシーが最後に変更された日時が記載されます。
Default Action	デフォルト アクションが記載されます。
Default Logging	デフォルト接続ログの設定が記載されます。
Rules	ルール カテゴリ別に、ポリシーに含まれる各ルールのルール アクションおよび条件が記載されます。
Trusted CA Certificates	自動的に信頼できる CA 証明書が記載されます。該当するのは、検出されたトラフィックの暗号化にそうした証明書が使用されている場合、あるいは信頼のチェーン内にある他の証明書が使用されている場合です。
Undecryptable Actions	復号化できないトラフィック タイプが検出された場合に適用されるアクションが記載されます。

セクション	説明
Referenced Objects	ポリシーで使用されている個々のすべてのオブジェクトおよびグループ オブジェクトの名前と設定が、各オブジェクトが設定されている条件タイプ別（ネットワーク、ポート、タグなど）に記載されます。

SSL ポリシー レポートを表示する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [SSL] の順に選択します。

[SSL Policy] ページが表示されます。

ステップ 2 レポートの生成対象とするポリシーの横にあるレポートアイコン（  ）をクリックします。SSL ポリシーレポートを生成する前に、すべての変更を保存してください。保存された変更のみがレポートに表示されます。

システムによってレポートが生成されます。ブラウザの設定によっては、レポートがポップアップ ウィンドウに表示されることがあります。または、コンピュータにレポートを保存するかどうか確認するプロンプトが出される場合があります。

SSL ポリシーの比較

ライセンス：任意

ポリシー変更が組織の標準に準拠しているかどうかを確認するため、またはシステムのパフォーマンスを最適化するために、2 つの SSL ポリシーの違いを確認することができます。任意の 2 つのポリシーを比較することも、現在適用されているポリシーを別のポリシーと比較することもできます。オプションで、比較した後に PDF レポートを生成することで、2 つのポリシーの間の差異を記録できます。

ポリシーを比較するために使用できるツールは 2 つあります。

- 比較ビューは、2 つのポリシーを左右に並べて表示し、その差異のみを示します。比較ビューの左右のタイトル バーに、それぞれのポリシーの名前が示されます。。ただし、[Running Configuration] を選択した場合、現在アクションなポリシーは空白のバーで表されます。

このツールを使用すると、Web インターフェイスで 2 つのポリシーを表示してそれらに移動するときに、差異を強調表示することができます。

- 比較レポートは、ポリシー レポートと同様の形式ですが、2 つのポリシーの間の差異だけが、PDF 形式で記録されます。

これを使用して、ポリシーの比較の保存、コピー、出力、共有を行って、さらに検証することができます。

SSL ポリシー比較ビューの使用

ライセンス：任意

比較ビューには、両方のポリシーが左右に並べて表示されます。それぞれのポリシーは、比較ビューの左右のタイトルバーに示される名前で特定されます。現在実行されている設定ではない 2 つのポリシーを比較する場合、最後に変更された日時とその変更を行ったユーザがポリシー名と共に表示されます。2 つのポリシー間の違いは次のように強調表示されます。

- 青色は強調表示された設定が 2 つのポリシーで異なることを示し、差異は赤色で示されます。
- グリーンは、強調表示されている設定項目が一方のポリシーに含まれ、もう一方のポリシーには含まれないことを示します。

次の表に、実行できる操作を記載します。

表 *39 : SSL* ポリシー比較のビューのアクション

目的	操作
変更に個別にナビゲートする	またはタイトル バーの上にある [Previous] または [Next] をクリックします。 左側と右側の間にある二重矢印アイコン（）が移動し、[Difference] 番号が調整されて、表示中の差異が示されます。
新しいポリシー比較ビューを生成する	[New Comparison] をクリックします。 [Select Comparison] ウィンドウが表示されます。SSL ポリシー比較レポートの使用を参照してください。
ポリシー比較レポートを生成する	[Comparison Report] をクリックします。 ポリシー比較レポートは、2 つのポリシーの間の差異だけをリストした PDF ドキュメントです。

SSL ポリシー比較レポートの使用

ライセンス：任意

SSL ポリシー比較レポートは、ポリシー比較ビューによって示される 2 つの SSL ポリシー間または 1 つのポリシーと現在適用されているポリシーの間のすべての差異を PDF 形式で表示する記録です。このレポートを使用することで、2 つのポリシー設定の間の違いをさらに調べ、調査結果を保存して共有できます。

アクセス可能な任意のポリシーに関して、比較ビューからSSLポリシー比較レポートを生成できます。ポリシー レポートを生成する前に、必ずすべての変更を保存してください。レポートには、保存されている変更だけが表示されます。

ポリシー比較レポートの形式は、ポリシー レポートと同様です。唯一異なる点は、ポリシー レポートにはポリシーのすべての設定が記載される一方、ポリシー比較レポートにはポリシー間で異なる設定だけがリストされることです。SSL ポリシー比較レポートには、「表 38 : SSL ポリシー レポートのセクション （234 ページ）」で説明しているセクションが含まれます。

ヒント 同様の手順を使用して、アクセス コントロール ポリシー、ネットワーク解析ポリシー、侵入ポリシー、ファイル ポリシー、システム ポリシー、またはヘルス ポリシーを比較できます。

2 つの SSL ポリシーを比較する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [SSL] の順に選択します。

[SSL Policy] が表示されます。

ステップ 2 [Compare Policies] をクリックします。

[Select Comparison] ウィンドウが表示されます。

ステップ 3 [Compare Against] ドロップダウン リストから、比較するタイプを次のように選択します。

- 異なる 2 つのポリシーを比較するには、[Other Policy] を選択します。

ページが更新されて、[Policy A] と [Policy B] という 2 つのドロップダウン リストが表示されます。

- 現在アクティブなポリシーと別のポリシーを比較するには、[Running Configuration] を選択します。

ページが更新されて、[Target/Running Configuration A] と [Policy B]という 2 つのドロップダウンリストが表示されます。

ステップ 4 選択した比較タイプに応じて、次のような選択肢があります。

- 2 つの異なるポリシーを比較することを選択した場合は、[Policy A] および [Policy B] ドロップダウン リストのそれぞれから、比較するポリシーを選択します。
- 現在実行されている設定を別のポリシーと比較する場合は、[Policy B] ドロップダウン リストから 2 つ目のポリシーを選択します。

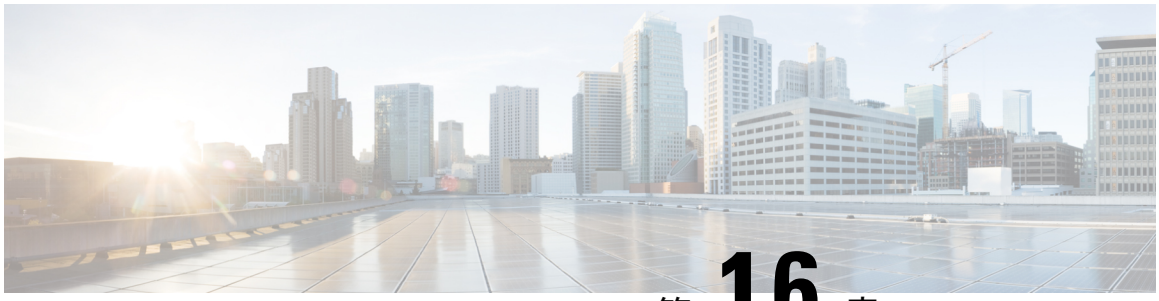
ステップ 5 ポリシー比較ビューを表示するには、[OK] をクリックします。

比較ビューが表示されます。

ステップ 6 オプションで、[Comparison Report] をクリックして、SSL ポリシー比較レポートを生成します。

SSL ポリシー比較レポートが表示されます。ブラウザの設定によっては、レポートがポップアップ ウィンドウに表示されることがあります。または、コンピュータにレポートを保存するかどうか確認するプロンプトが出される場合があります。

次のタスク



第 16 章

SSL ルールの開始

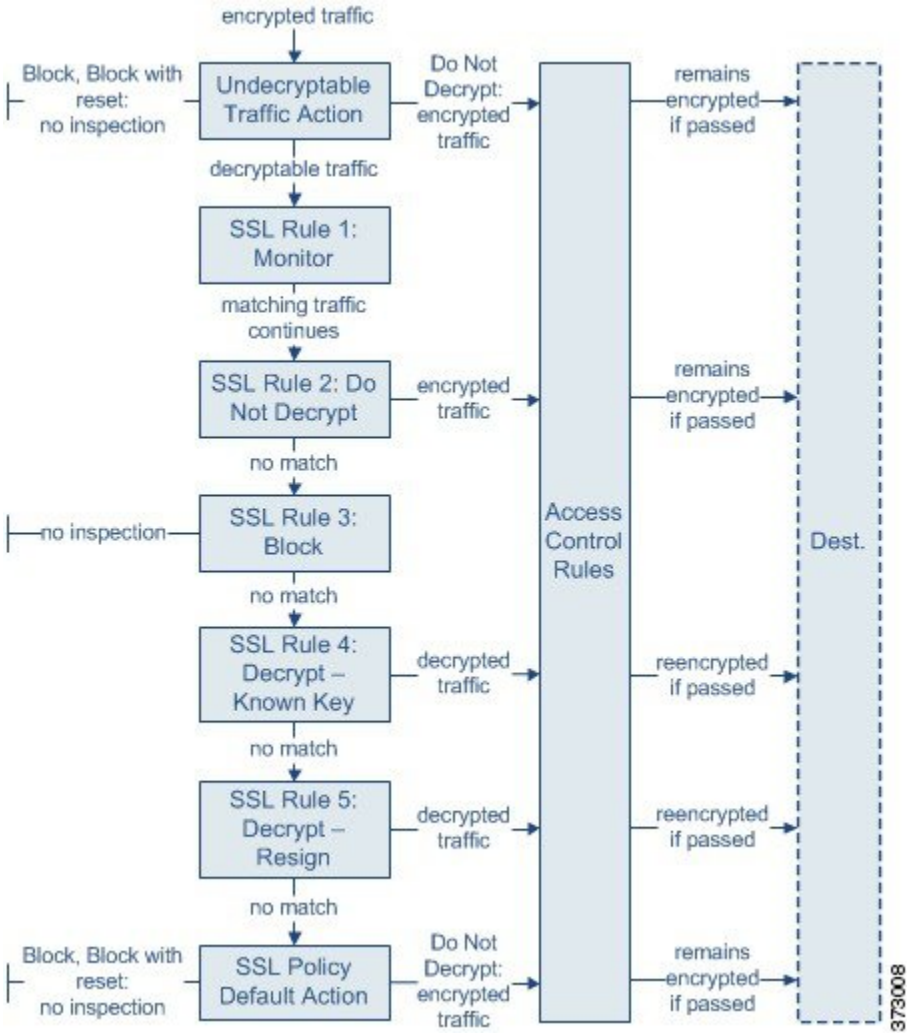
SSL ポリシー内に、各種の *SSL* ルールを設定することで、それ以上のインスペクションなしでトラフィックをブロックする、トラフィックを復号化せずにアクセスコントロールで検査する、あるいはアクセスコントロールの分析用にトラフィックを復号するなど、きめ細やかな暗号化トラフィックの処理メソッドを構築できます。

SSL ルールについて

ASA FirePOWER モジュールは、ユーザが指定した順序で SSL ルールをトラフィックと照合します。ほとんどの場合、モジュールによる暗号化トラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の SSL ルールに従って行われます。こうした条件には、単純なものと複雑なものがあります。セキュリティゾーン、ネットワークまたは地理的位置、ポート、アプリケーション、要求された URL、ユーザ、証明書、証明書の識別名、証明書ステータス、暗号スイート、暗号化プロトコルバージョンなどによってトラフィックを制御できます。

また、各ルールには 1 つのアクションがあり、このアクションにより、一致するトラフィックの復号化後にオプションでモニタするか、ブロックするか、または一致したトラフィックをアクセスコントロールで検査するかが決まります。システムがブロックした暗号化トラフィックは、それ以上のインスペクションが**行われない**ことに注意してください。暗号化されたトラフィックおよび復号できないトラフィックは、アクセス コントロールを使用して検査します。ただし、一部のアクセス コントロール ルールの条件では暗号化されていないトラフィックを必要とするため、暗号化されたトラフィックに一致するルール数が少なくなる場合があります。またデフォルトでは、モジュールは暗号化ペイロードの侵入およびファイルのインスペクションを無効化します。

次のシナリオは、インライン展開での SSL ルールによるトラフィックの処理を要約しています。



このシナリオでは、トラフィックは次のように評価されます。

- **復号できないトラフィック アクション（Undecryptable Traffic Action**）は、暗号化されたトラフィックを最初に評価します。復号化できないトラフィックについて、モジュールはそれ以上のインスペクションなしでブロックするか、あるいはアクセス コントロールによるインスペクション用に渡します。一致しなかった暗号化トラフィックは、次のルールへと進められます。
- **SSL ルール 1**：**モニタ（SSL Rule 1: Monitor**）は、暗号化トラフィックを次に評価します。モニタ ルールは、暗号化トラフィックのログ記録と追跡を行いますが、トラフィック フローには影響しません。モジュールは引き続きトラフィックを追加のルールと照合し、許可するか拒否するかを決定します。
- **SSL ルール 2**：**復号化しない（SSL Rule 2: Do Not Decrypt**）は、暗号化トラフィックを 3 番目に評価します。一致したトラフィックは復号されません。モジュールはこのトラフックをアクセス コントロールにより検査しますが、ファイルや侵入インスペクションは行いません。一致しないトラフィックは、引き続き次のルールと照合されます。

- **SSL ルール 3**：**ブロック**（**SSL Rule 3: Block**）は、暗号化トラフィックを 4 番目に評価します。一致したトラフィックは、それ以上のインスペクションは行わずに、ブロックされます。一致しなかったトラフィックは、次のルールへと進められます。
- **SSL ルール 4**：**復号化 - 既知のキー**（**SSL Rule 4: Decrypt - Known Key**）は、暗号化トラフィックを 5 番目に評価します。ネットワークへの着信トラフィックで一致したものは、ユーザのアップロードする秘密キーを使用して復号化されます。復号化トラフィックはその後、アクセス コントロール ルールで評価されます。アクセス コントロール ルールは、復号されたトラフィックと暗号化されていないトラフィックで同じ処理をします。この追加のインスペクションの結果、そのモジュールがトラフィックをブロックする場合があります。他のすべてのトラフィックは、宛先への送信が許可される前に再暗号化されます。SSL ルールに一致しなかったトラフィックは、次のルールへと進められます。
- **SSL ルール 5**：**復号化 - 再署名**（**SSL Rule 5: Decrypt - Resign**）は、最後のルールです。トラフィックがこのルールに一致した場合、モジュールはアップロードされた CA 証明書を使用してサーバ証明書を再署名してから、中間者としてトラフィックを復号化します。復号化トラフィックはその後、アクセス コントロール ルールで評価されます。アクセス コントロール ルールは、復号されたトラフィックと暗号化されていないトラフィックで同じ処理をします。この追加のインスペクションの結果、そのモジュールがトラフィックをブロックする場合があります。他のすべてのトラフィックは、宛先への送信が許可される前に再暗号化されます。SSL ルールに一致しなかったトラフィックは、次のルールへと進められます。
- **SSL ポリシーのデフォルト アクション**（**SSL Policy Default Action**）は、他の SSL ルールに一致しなかったすべてのトラフィックを処理します。デフォルトアクションでは、暗号化トラフィックをそれ以上のインスペクションなしでブロックするか、あるいは復号化しないままにして、アクセス コントロールによる検査を行います。

サポートする検査情報の設定

ライセンス：任意

暗号化セッションの特性に基づいた暗号化トラフィックの制御および暗号化トラフィックの復号化には、再利用可能な公開キー インフラストラクチャ（PKI）オブジェクトの作成が必要です。この情報の追加は、信頼できる認証局（CA）の証明書の SSL ポリシーへのアップロード、SSL ルール条件の作成、およびプロセスでの関連オブジェクトの作成時に、臨機応変に実行できます。ただし、これらのオブジェクトを事前に設定しておくと、不適切なオブジェクトが作成される可能性を抑制できます。

証明書とキー ペアによる暗号化トラフィックの復号化

セッションの暗号化に使用するサーバ証明書と秘密キーをアップロードして内部証明書オブジェクトを設定している場合、ASA FirePOWER モジュールは着信する暗号化トラフィックを復号化できます。**Decrypt - Known Key** のアクションが設定された SSL ルールでそのオブジェクトを参照し、当該ルールにトラフィックが一致すると、モジュールはアップロードされた秘密キーを使用してセッションを復号化します。

CA 証明書と秘密キーをアップロードして内部 CA オブジェクトを設定した場合、モジュールは発信トラフィックの復号化もできます。[Decrypt - Resign] のアクションが設定された SSL ルールでそのオブジェクトを参照し、当該ルールにトラフィックが一致すると、モジュールはクライアントブラウザに渡されたサーバ証明書を再署名した後、中間者としてセッションを復号化します。

暗号化セッションの特性に基づいたトラフィック制御

ASA FirePOWER モジュールによる暗号化トラフィックの制御は、セッションのネゴシエートに使用される暗号スイートまたはサーバ証明書に基づいて実行できます。複数の異なる再利用可能オブジェクトの 1 つを設定し、SSL ルール条件でオブジェクトを参照しトラフィックを照合することができます。次の表に、設定できる再利用可能なオブジェクトのタイプを示します。

設定する内容	暗号化トラフィック制御に使用する条件
1 つまたは複数の暗号スイートが含まれる暗号スイートのリスト	暗号化セッションのネゴシエートに使う暗号スイートが、暗号スイート リストにある暗号スイートのいずれかに一致する。
組織の信頼する CA 証明書のアップロードによる信頼できる CA オブジェクト	この信頼できる CA は、次のいずれかにより、セッションの暗号化に使用されたサーバ証明書を信頼する。 • CA が証明書を直接発行した。 • サーバ証明書を発行した中間 CA に CA が証明書を発行した。
サーバ証明書のアップロードによる外部証明書オブジェクト	セッションの暗号化に使用されたサーバ証明書が、アップロードされたサーバ証明書と一致する。
発行元の識別名または証明書サブジェクトを含む識別名オブジェクト	セッション暗号化に使用された証明書で、サブジェクトまたは発行元の共通名、国、組織、組織単位のいずれかが、設定された識別名に一致する。

詳細については、次の各項を参照してください。

- 地理位置情報オブジェクトの操作 （77 ページ）
- 信頼できる認証局オブジェクトの操作 （73 ページ）
- 外部証明書オブジェクトの操作 （75 ページ）
- 識別名オブジェクトの操作 （66 ページ）

SSL ルールの概要と作成

ライセンス：任意

SSLポリシー内で、SSLルールによってネットワーク トラフィックを処理するためのきめ細かなメソッドが提供されます。各SSLルールには、一意の名前以外にも、次の基本コンポーネントがあります。

状態

デフォルトでは、ルールが有効状態になります。ルールを無効にすると、モジュールはネットワーク トラフィックの評価にそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。

位置

SSL ポリシーのルールには 1 から始まる番号が付いています。モジュールは、ルール番号の昇順で、ルールを上から順にトラフィックと照合します。Monitor ルールを除き、トラフィックが最初に一致するルールが、当該トラフィックを処理するためのルールになります。

条件

条件は、ルールで処理する特定のトラフィックを指定します。こうした条件では、セキュリティゾーン、ネットワークまたは地理的位置、ポート、アプリケーション、要求されたURL、ユーザ、証明書、証明書のサブジェクトまたは発行元、証明書ステータス、暗号スイート、暗号化プロトコルバージョンなどによってトラフィックを照合できます。条件には、単純なものと複雑なものがあり、デバイスのライセンスによって用途が異なります。

アクション

ルールのアクションによって、一致するトラフィックをモジュールがどのように処理するかが決まります。一致したトラフィックに対して行うことができ処理は、モニタ、信頼、ブロック、または復号です。復号したトラフィックには、さらにインスペクションが適用されます。モジュールは、ブロックされた暗号化トラフィックと信頼された暗号化トラフィックに対してインスペクションを実行**しない**ことに注意してください。

ロギング

ルールのロギング設定によって、モジュールが処理するトラフィックについて記録するレコードが管理されます。各ルールに一致したトラフィックのレコードを維持できます。SSL ポリシーでの設定に従って、モジュールが暗号化セッションをブロックするか、あるいはインスペクションなしで渡すことを許可するときに、その接続をログに記録できます。アクセス コントロール ルールに従ってより詳細な評価を行うために復号化した接続をログに記録するようにモジュールを強制することも可能です。これはその後でどのようなトラフィックの処理や検査がなされるかに関係なく行うことができます。接続のログは、モジュール ログ（syslog）または SNMP トラップ サーバに記録できます。

ヒント SSL ルールを適切に作成して順序付けることは複雑な作業ですが、これは効果的な展開を構築する上で不可欠な要素です。慎重なポリシーの設計を怠ると、他のルールをプリエンプション処理したり、追加ライセンスが必要となったり、無効な設定を含んだルールになる可能性があります。予期したとおりにモジュールでトラフィックが確実に処理されるようにするために、SSL ポリシー インターフェイスには、ルールに関する強力な警告およびエラーのフィードバック システムが用意されています。詳細については、SSL ルールのトラブルシューティング （258 ページ）を参照してください。

SSL ルールを作成または変更する手順：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [SSL] の順に選択します。

[SSL Policy] ページが表示されます。

ステップ 2 ルールを追加する SSL ポリシーの横にある編集アイコン（）をクリックします。

SSL ポリシー エディタが表示され、[Rules] タブにフォーカスが移動します。

ステップ 3 次の選択肢があります。

- 新しいルールを追加するには、[Add Rule] をクリックします。
- 既存のルールを編集するには、そのルールの横にある編集アイコン（）をクリックします。

SSL ルール エディタが表示されます。

ステップ 4 [Name] にルールの名前を入力します。

各ルールには一意の名前が必要です。30 文字までの印刷可能文字を使用できます。スペースや特殊文字を含めることができますが、コロン（:）は使用できません。

ステップ 5 前述の説明に従い、ルール コンポーネントを設定します。次の設定をするか、デフォルト設定をそのまま使用することができます。

- ルールを有効にするかどうか [Enabled] を指定します。
- ルールの位置を指定します。を参照してください。 SSL ルールの評価順序の指定 （245 ページ）

  .
- ルールの [Action] を選択します。「ルール アクションを使用した暗号化トラフィックの処理と検査の決定 （248 ページ）」を参照してください。
- ルールの条件を設定します。「条件を使用したルールによる暗号化トラフィックの処理の指定 （246 ページ）」を参照してください。
- [Logging] オプションを指定します。「SSL ルールを使用した復号可能接続のロギング （483 ページ）」を参照してください。

ステップ 6 [Save] をクリックしてルールを保存します。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（設定変更の導入 （92 ページ）を参照してください）。

SSL ルールの評価順序の指定

ライセンス：任意

SSL ルールを最初に作成するときに、ルール エディタの [Insert] ドロップダウン リストを使用して、その位置を指定します。SSL ポリシーの SSL ルールには 1 から始まる番号が付いています。ASA FirePOWER モジュールは、ルール番号の昇順で、SSL ルールを上から順にトラフィックと照合します。

ほとんどの場合、モジュールによるネットワーク トラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の SSL ルールに従って行われます。モニタ ルール（トラフィックをログに記録するが、トラフィック フローには影響しない）の場合を除き、モジュールは、そのトラフィックがルールに一致した後、追加の優先順位の低いルールに対してトラフィックの評価を続けることはありません。

ヒント 適切な SSL ルールの順序は、ネットワーク トラフィックの処理に必要なリソースを軽減し、ルールのプリエンプションを回避します。ユーザが作成するルールはすべての組織と展開に固有のものですが、ユーザのニーズに対処しながらもパフォーマンスを最適化できるルールを順序付けする際に従うべきいくつかの一般的なガイドラインがあります。詳細については、SSL ルールの順序指定によるパフォーマンス向上とプリエンプション回避 （259 ページ）を参照してください。

ルールは数値で順序付けするだけでなく、カテゴリ別にグループ化することもできます。デフォルトで、システムには 3 つのカテゴリ（管理者、標準、ルート）があります。カスタム カテゴリを追加できますが、 ASA FirePOWER モジュール提供のカテゴリを削除したり、カテゴリの順序を変更したりはできません。既存のルールの位置またはカテゴリの変更の詳細については、「SSL ルールの位置またはカテゴリの変更 （256 ページ）」を参照してください。

ルールの編集や作成中にルールをカテゴリに追加する手順：

SSL ルール エディタの [Insert] ドロップダウン リストで [Into Category] を選択し、使用するカテゴリを選択します。

ルールを保存すると、そのカテゴリの最後に配置されます。

SSL ルールの評価順序の指定

ルールの編集や作成中にルールの位置を数値で指定する手順：

SSL ルール エディタの [Insert）] ドロップダウンリストで、[above rule] または [below rule] を選択して、適切なルール番号を入力します。

ルールを保存すると、指定した場所に配置されます。

条件を使用したルールによる暗号化トラフィックの処理の指定

ライセンス：機能に応じて異なる

SSL ルールの条件は、ルールで処理する暗号化トラフィックのタイプを特定します。条件には、単純なものと複雑なものがあり、ルールごとに複数の条件タイプを指定できます。トラフィックにルールが適用されるのは、トラフィックがルールの条件をすべて満たしている場合だけです。

ルールに対し特定の条件を設定しない場合、モジュールはその基準に基づいてトラフィックを照合しません。たとえば、証明書の条件が設定され、バージョンの条件が設定されていないルールは、セッションSSLまたはTLSのバージョンにかかわりなく、セッションのネゴシエーションに使用されるサーバ証明書に基づいてトラフィックを評価します。

SSLルールを追加および編集するときは、ルールエディタ下部の左側にあるタブを使用して、ルール条件の追加と編集を行います。SSL ルールに追加できる条件を次の表に示します。

表 *40 : SSL* ルールの条件タイプ

条件	一致する暗号化トラフィック	詳細
ゾーン	特定のセキュリティ ゾーンにあるインターフェイスを経由したデバイスへの着信または発信	セキュリティ ゾーンとは、展開やセキュリティ ポリシーに従って 1 つまたは複数のインターフェイスを論理的にグループ化したものです。ゾーン条件の作成については、「ネットワーク ゾーンによる暗号化トラフィックの制御 （266 ページ）」を参照してください。
ネットワーク	その送信元または宛先の IP アドレス、国、または大陸による	明示的に IP アドレスを指定できます。位置情報の機能では、送信元または宛先となる国や大陸を基準にしたトラフィック制御もできます。ネットワーク条件を作成するには、ネットワークまたは地理的位置による暗号化トラフィックの制御 （268 ページ） を参照してください。
ポート	送信元ポートまたは宛先ポート	TCP ポートに基づいて暗号化トラフィックを制御できます。ポート条件の作成については、「ポートによる暗号化トラフィックの制御 （270 ページ）」を参照してください。

条件	一致する暗号化トラフィック	詳細
ユーザ	セッションに参加しているユーザ	暗号化されたモニタ対象セッションの関連ホストにログインしている LDAP ユーザに基づいて暗号化トラフィックを制御できます。Microsoft Active Directory サーバから取得された個別ユーザまたはグループに基づいてトラフィックを制御できます。ユーザ条件の作成については、「ユーザ ベースの暗号化トラフィックの制御 （272 ページ）」を参照してください。
アプリケーション	セッションで検出されるアプリケーション	タイプ、リスク、ビジネスとの関連性、カテゴリの基本的な特性に従って、フィルタアクセスまたは暗号化セッションの各アプリケーションへのアクセスを制御できます。アプリケーション条件の作成については、「アプリケーションベースの暗号化トラフィックの制御 （274 ページ）」を参照してください。
カテゴリ	証明書サブジェクトの識別名に基づいてセッションで要求される URL	URL の一般分類とリスク レベルに基づいて、ネットワークのユーザがアクセスできる Web サイトを制限できます。URL 条件の作成については、「URL カテゴリおよびレピュテーションによる暗号化トラフィックの制御 （280 ページ）」を参照してください。
識別名	暗号化セッションのネゴシエートに使用されたサーバ証明書のサブジェクトまたは発行元の識別名	サーバ証明書を発行した CA またはサーバ証明書ホルダーに基づいて、暗号化トラフィックを制御できます。識別名条件の作成については、「証明書の識別名による暗号化トラフィックの制御 （284 ページ）」を参照してください。
証明書	暗号化セッションのネゴシエートに使用されるサーバ証明書	暗号化セッションのネゴシエート用にユーザのブラウザに渡されるサーバ証明書に基づいて、暗号化されたトラフィックを制御できます。証明書条件の作成については、「証明書ステータスによる暗号化トラフィックの制御 （289 ページ）」を参照してください。
証明書のステータス	暗号化セッションのネゴシエートに使用されるサーバ証明書のプロパティ	サーバ証明書のステータスに基づいて、暗号化トラフィックを制御できます。証明書ステータス条件の作成については、「証明書ステータスによる暗号化トラフィックの制御 （289 ページ）」を参照してください。
暗号スイート	暗号化セッションのネゴシエートに使用する暗号スイート	暗号化セッションのネゴシエート用にサーバで選択された暗号スイートに基づいて、暗号化トラフィックを制御できます。暗号スイート条件の作成については、「暗号スイートによる暗号化トラフィックの制御 （294 ページ）」を参照してください。
バージョン	セッションの暗号化に使用される SSL または TLS のバージョン	セッションの暗号化に使用される SSL または TLS のバージョンに基づいて、暗号化トラフィックを制御できます。バージョン条件の作成については、「暗号化プロトコルのバージョンによるトラフィックの制御 （295 ページ）」を参照してください。

暗号化トラフィックの制御と検査は可能ですが、トラフィックの制御に検出されたアプリケーション、URL カテゴリ、またはユーザを使用するには追加ライセンスが必要です。また過度に

複雑なルールは、多くのリソースを消費し、状況によってはポリシーを適用できなくなる場合があります。詳細については、SSL ルールのトラブルシューティング （258 ページ）を参照してください。

ルールアクションを使用した暗号化トラフィックの処理と検査の決定

ライセンス：任意

すべての SSL ルールには、一致する暗号化トラフィックに対して次の判定をする関連アクションがあります。

- 処理：まず、ルール アクションは、ASA FirePOWER モジュールがルールの条件に一致する暗号化トラフィックに対して、モニタ、信頼、ブロック、または復号化を行うかどうかを判定します。
- ロギング：ルールアクションは一致する暗号化トラフィックの詳細をいつ、どのようにログに記録するかを判定します。

SSL インスペクション設定では、次のように復号化されたトラフィックの処理、検査、ログ記録を行います。

- SSL ポリシーの復号化できないアクションは、ASA FirePOWER モジュールが復号化できないトラフィックを処理します。復号できないトラフィックのデフォルト処理の設定 （227 ページ）を参照してください。
- ポリシーのデフォルト アクションは、モニタ以外のどの SSL ルールの条件にも一致しないトラフィックを処理します。暗号化トラフィックのデフォルトの処理と検査の設定 （226 ページ）を参照してください。

ASA FirePOWER モジュールが暗号化セッションをブロックまたは信頼したときに、接続イベントをログに記録できます。アクセス コントロール ルールに従ってより詳細な評価を行うために復号化した接続をログに記録するようにモジュールを強制することも可能です。これはその後でどのようなトラフィックの処理や検査がなされるかに関係なく行うことができます。暗号化セッションの接続ログには、セッションの暗号化に使用される証明書など、暗号化の詳細が含まれます。ただし次の場合は、接続終了イベントだけをログに記録できます。

- ブロックされた接続（Block、Block with reset）の場合、システムは即座にセッションを終了してイベントを生成します
- 信頼された接続（Do not decrypt）の場合、システムはセッション終了後にイベントを生成します

モニタ アクション：アクションの延期とロギングの確保

ライセンス：任意

モニタ アクションは暗号化トラフィック フローに影響を与えません。つまり、一致するトラフィックがただちに許可または拒否されることはありません。その代わり、追加のルールが存

在する場合はそのルールに照らしてトラフィックが照合され、信頼するか、ブロックするか、復号化するかが決定されます。モニタ ルール以外の一致する最初のルールが、トラフィック フローおよび追加のインスペクションを決定します。さらに一致するルールがない場合、ASA FirePOWER モジュールはデフォルトのアクションを使用します。

Monitor ルールの主な目的はネットワーク トラフィックのトラッキングなので、モジュールはモニタ対象トラフィックの接続終了イベントを自動的にログに記録します。つまり、ルールのロギング設定または後で接続を処理するデフォルト アクションとは無関係に、モジュールは接続の終了時に常にログに記録します。言い換えると、パケットが他のルールに一致せず、デフォルト アクションでロギングが有効になっていない場合でも、パケットがモニタ ルールに一致すれば必ず接続がロギングされます。

復号化しない（Do Not Decrypt）アクション：暗号化トラフィックを検査なしで転送

ライセンス：任意

復号化しない（**Do Not Decrypt**）アクションは、アクセス コントロール ポリシーのルールおよびデフォルト アクションに従って暗号化トラフィックを評価するため転送します。一部のアクセス コントロール ルールの条件では暗号化されていないトラフィックを必要とするため、こうしたトラフィックに一致するルール数が少なくなる場合があります。侵入やファイル インスペクションなど、暗号化トラフィックのディープ インスペクションは実行できません。

ブロッキング（Block）アクション：検査なしで暗号化トラフィックをブロック

ライセンス：任意

[Block] および [Block with reset] アクションは、アクセス コントロール ルールの [Block] と [Block with reset] アクションに類似しています。これらのアクションは、クライアントとサーバによる SSL 暗号化セッションの確立と暗号化トラフィックの転送を防止します。リセット付きブロック ルールでは接続のリセットも行います。

ブロックされた暗号化トラフィックに対しては、ASA FirePOWER モジュールは設定された応答ページを表示しないことに注意してください。その代わりに、ユーザの要求する禁止された URL の接続は、リセットまたはタイムアウトされます。詳細については、「ブロックされた URL のカスタム Web ページの表示 （157 ページ）」を参照してください。

ヒント パッシブまたはインライン（タップ モード）展開では、デバイスがトラフィックを直接検査しないので、Block および Block with reset アクションを使用できないことに注意してください。パッシブまたはインライン（タップ モード）インターフェイスを含むセキュリティ ゾーン条件内で、Block および Block with reset アクションを使用したルールを作成すると、ポリシー エディタでルールの横に警告アイコン（⚠）が表示されます。

復号化アクション：さらに検査するためにトラフィックを復号化

ライセンス：任意

[Decrypt - Known Key] および [Decrypt - Resign] アクションは、暗号化トラフィックを復号します。ASA FirePOWER モジュールは、アクセス コントロールを使用して復号化されたトラフィックを検査します。アクセス コントロール ルールは、復号化されたトラフィックと暗号化されていないトラフィックで同じ処理をします。ここでは、侵入、禁止ファイル、マルウェアの検出とブロックができます。モジュールは許可されたトラフィックを再暗号化してから宛先に渡します。

Decrypt - Known アクションを設定した場合は、1 つまたは複数のサーバ証明書と秘密キー ペアをアクションに関連付けることができます。トラフィックがルールに一致して、トラフィックの暗号化に使用された証明書とアクションに関連付けられた証明書が一致した場合、モジュールは適切な秘密キーを使用してセッションの暗号化と復号化キーを取得します。秘密キーへのアクセスが必要なため、このアクションが最も適しているのは、組織の管理下にあるサーバへの入力トラフィックを復号する場合です。

同様に [Decrypt - Resign] アクションには、1 つの認証局証明書と秘密キーを関連付けることができます。トラフィックがこのルールに一致した場合、モジュールは CA 証明書を使用してサーバ証明書を再署名してから、中間者として機能します。ここでは、1 つはクライアントとデバイスの間、もう 1 つはデバイスとサーバの間をつなぐ、2 つの SSL セッションが作成されます。各セッションには、さまざまな暗号セッションの詳細が含まれており、モジュールはこれを使用することでトラフィックの復号化と再暗号化が行えます。このアクションは、証明書の秘密キーを各自の管理下にあるキーに置き換えてセッション キーを取得するため、発信トラフィックに適しています。

サーバ証明書の再署名では、証明書の公開キーを CA 証明書の公開キーに置き換えるか、あるいは証明書全体が置き換えられます。通常、サーバ証明書全体を置き換える場合は、SSL 接続が確立された時点で、証明書が信頼できる認証局によって署名されていないことがクライアント ブラウザで警告されます。ただし、その CA をクライアント ブラウザで信頼できることがポリシーに設定されている場合、ブラウザは証明書が信頼できないことの警告をしません。オリジナルのサーバ証明書が自己署名の場合、ASA FirePOWER モジュールは証明書全体を置き換えて、再署名する CA を信頼しますが、ユーザのブラウザは証明書が自己署名であることを警告しません。この場合、サーバ証明書の公開キーを交換するだけで、クライアントブラウザは証明書が自己署名であることを警告します。

Decrypt - Resign アクションを設定した場合、ルールによるトラフィックの照合は、設定したすべてのルール条件に加えて、参照される内部CA証明書の署名アルゴリズム タイプに基づいて実施されます。各 **Decrypt - Resign** アクションにはそれぞれ 1 つの CA 証明書が関連付けられるので、暗号化の署名アルゴリズムが異なる複数タイプの発信トラフィックを復号化する SSL ルールは作成できません。また、ルールに追加する暗号スイートと外部証明書のオブジェクトのすべては、関連する CA 証明書の暗号化アルゴリズム タイプに一致する必要があります。

たとえば、楕円曲線暗号（EC）アルゴリズムで暗号化された発信トラフィックが [Decrypt - Resign] ルールに一致するのは、アクションが EC ベースの CA 証明書を参照している場合だけです。証明書と暗号スイートのルール条件を作成する場合は、EC ベースの外部証明書と暗号

スイートをルールに追加する必要があります。同様に、RSA ベースの CA 証明書を参照する [Decrypt - Resign] ルールは、RSA アルゴリズムで暗号化された発信トラフィックとのみ一致します。EC アルゴリズムで暗号化された発信トラフィックは、設定されている他のルール条件がすべて一致したとしても、このルールには一致しません。

次の点に注意してください。

- SSL 接続の確立に使用される暗号スイートが Diffie-Hellman Ephemeral（DHE）または楕円曲線 Diffie-Hellman Ephemeral（ECDHE）キー交換アルゴリズムを適用している場合、パッシブ展開では [Decrypt - Known Key] アクションを使用できません。SSL ポリシーの対象がパッシブまたはインライン（タップモード）インターフェイスであり、そのポリシーに含まれる [Decrypt - Known Key] ルールで DHE または ECDHE 暗号スイートを含む暗号スイート条件が使用されている場合、ASA FirePOWER モジュールによりルールの横に情報アイコンが表示されます。パッシブまたはインライン（タップモード）インターフェイスを含む SSL ルールに後からゾーンを追加すると、モジュールにより警告アイコンが表示されます。

- デバイスはトラフィックを直接検査しないため、パッシブまたはインライン（タップモード）展開では [Decrypt - Resign] アクションを使用できません。セキュリティ ゾーン内にパッシブまたはインライン（タップ モード）インターフェイスを含む [Decrypt - Resign] アクションを使用したルールを作成した場合、ポリシーエディタによりルールの横に警告アイコンが表示されます。SSL ポリシーの対象がパッシブまたはインライン（タップ モード）インターフェイスであり、そのポリシーに **Decrypt - Resign** ルールが含まれる場合、モジュールによりルールの横に情報アイコン（）が表示されます。パッシブまたはインライン（タップ モード）インターフェイスを含む SSL ルールに後からゾーンを追加すると、モジュールにより警告アイコン（）が表示されます。パッシブまたはインライン（タップ モード）インターフェイスを含むデバイスに、[Decrypt - Resign] ルールを含む SSL ポリシーを適用した場合、このルールに一致する SSL セッションはすべて失敗します。

- サーバ証明書の再署名に使用する CA をクライアントが信頼していない場合、証明書が信頼できないという警告がユーザに出されます。これを防止するには、クライアントの信用できる CA ストアに CA 証明書をインポートします。または組織にプライベート PKI がある場合は、組織の全クライアントで自動的に信頼されるルート CA が署名する中間 CA 証明書を発行して、その CA 証明書をデバイスにアップロードすることもできます。

- SSL ルールの**暗号スイート**条件に匿名の暗号スイートを追加できますが、次の点に注意してください。

  - システムは ClientHello 処理中に自動的に匿名の暗号スイートを削除します。ルールを使用するシステムでは、ClientHello の処理を防止するために SSL ルールを設定する必要があります。詳細については、SSL ルールの順序指定によるパフォーマンス向上とプリエンプション回避 （259 ページ）を参照してください。

  - システムでは、匿名の暗号スイートで暗号化されたトラフィックは復号化できないため、ルールに **Decrypt - Resign** または **Decrypt - Known Key** アクションを使用できません。

- クライアントとデバイスの間にHTTPプロキシがあり、クライアントとサーバがCONNECT HTTP メソッドを使用してトンネル SSL 接続を確立する場合、ASA FirePOWER モジュールはトラフィックを復号化できません。モジュールによるこのトラフィックの処理法は、**ハンドシェイク エラー**の復号化できないアクションが決定します。詳細については、「復号できないトラフィックのデフォルト処理の設定（227ページ）」を参照してください。
- SSL ルールに **Decrypt - Known Key** アクションを付けて作成した場合、**Distinguished Name** または **Certificate** 条件による照合はできません。ここでの前提は、このルールがトラフィックと一致する場合、証明書、サブジェクト DN、および発行元 DN は、ルールに関連付けられた証明書とすでに一致済みであることです。詳細については、ルールアクションを使用した暗号化トラフィックの処理と検査の決定（248 ページ）を参照してください。

  .
- 内部 CA オブジェクトを作成して証明書署名要求（CSR）の生成を選択した場合、オブジェクトに署名付き証明書をアップロードするまで、この CA は **Decrypt - Resign** アクションに使用できません。詳細については、新しい署名付き証明書の取得およびアップロード（71 ページ）を参照してください。
- [Decrypt - Resign] アクションのルールを設定して、1 つまたは複数の外部証明書オブジェクトまたは暗号スイートで署名アルゴリズム タイプの不一致が生じた場合、ポリシー エディタによりルールの横に情報アイコンが表示されます。すべての外部証明書オブジェクトまたはすべての暗号スイートで署名アルゴリズム タイプの不一致が生じた場合、ポリシーによりルールの横に警告アイコンが表示され、SSL ポリシーに関連付けたアクセス コントロール ポリシーは適用できません。詳細については、証明書による暗号化トラフィックの制御（287ページ）および暗号スイートによる暗号化トラフィックの制御（294ページ）を参照してください。
- [Interactive Block] または [Interactive Block with reset] アクションのアクセス コントロール ルールと復号化トラフィックが一致する場合、ASA FirePOWER モジュールは一致する接続をインタラクションなしでブロックし、応答ページを表示しません。
- インライン正規化プリプロセッサで **Normalize Excess Payload** オプションをイネーブルにすると、プリプロセッサによる復号化トラフィックの標準化時に、パケットがドロップされてトリミングされたパケットに置き換えられる場合があります。これは SSL セッションを終了させません。トラフィックが許可された場合、SSL セッションの一部としてトリミングされたパケットは暗号化されます。
- ブラウザが証明書ピニングを使用してサーバ証明書を確認する場合は、サーバ証明書に再署名しても、このトラフィックを復号化できません。このトラフィックを許可するには、サーバ証明書の共通名または識別名と突き合わせるように、Do not decrypt アクションを使用して SSL ルールを設定します。

着信トラフィックを復号化するルールを設定する場合：

アクセス：管理者/アクセス管理者/ネットワーク管理者

ステップ 1 着信トラフィックを復号化するポリシーの SSL ポリシー エディタでは、次のオプションを利用できます。

- 新しいルールを追加するには、[Add Rule] をクリックします。
- 既存のルールを編集するには、編集するルールの横にある編集アイコンをクリックします。

SSL ルール エディタが表示されます。

ステップ 2 [Action] ドロップダウン リストから、[Decrypt - Known Key] を選択します。
[Click to select decryption certs] フィールドが表示されます。

ステップ 3 [Click to select decryption certs] フィールドをクリックします。
証明書の選択ポップアップ ウィンドウが表示されます。

ステップ 4 [Available Certificates] リストにある内部証明書オブジェクトをクリックします。複数の条件を選択するには Shift キーと Ctrl キーを使用するか、右クリックして [Select All] をクリックします。
選択した証明書が強調表示されます。

ステップ 5 次の選択肢があります。

- [Add to Rule] をクリックします。
- 選択した条件を [Selected Certificates] リストにドラッグ アンド ドロップします。

選択した条件が追加されます。

ステップ 6 [OK] をクリックします。
SSL ルール エディタが表示されます。

ステップ 7 [Save] をクリックしてルールを保存します。
変更を反映させるには、SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります。

次のタスク

発信トラフィックを復号化するルールを設定する場合：

復号化アクション：さらに検査するためにトラフィックを復号化

アクセス：管理者/アクセス管理者/ネットワーク管理者

ステップ 1 着信トラフィックを復号化するポリシーの SSL ポリシー エディタでは、次のオプションを利用できます。

- 新しいルールを追加するには、[Add Rule] をクリックします。
- 既存のルールを編集するには、編集するルールの横にある編集アイコンをクリックします。

SSL ルール エディタが表示されます。

ステップ 2 [Action] ドロップダウン リストから、[Decrypt - Resign] を選択します。

追加のフィールドが表示されます。

ステップ 3 ドロップダウン リストから内部 CA 証明書のオブジェクトを選択します。

ステップ 4 オプションとして [Replace Key] を選択すると、証明書全体を置き換える代わりに証明書の公開キーが置き換えられます。

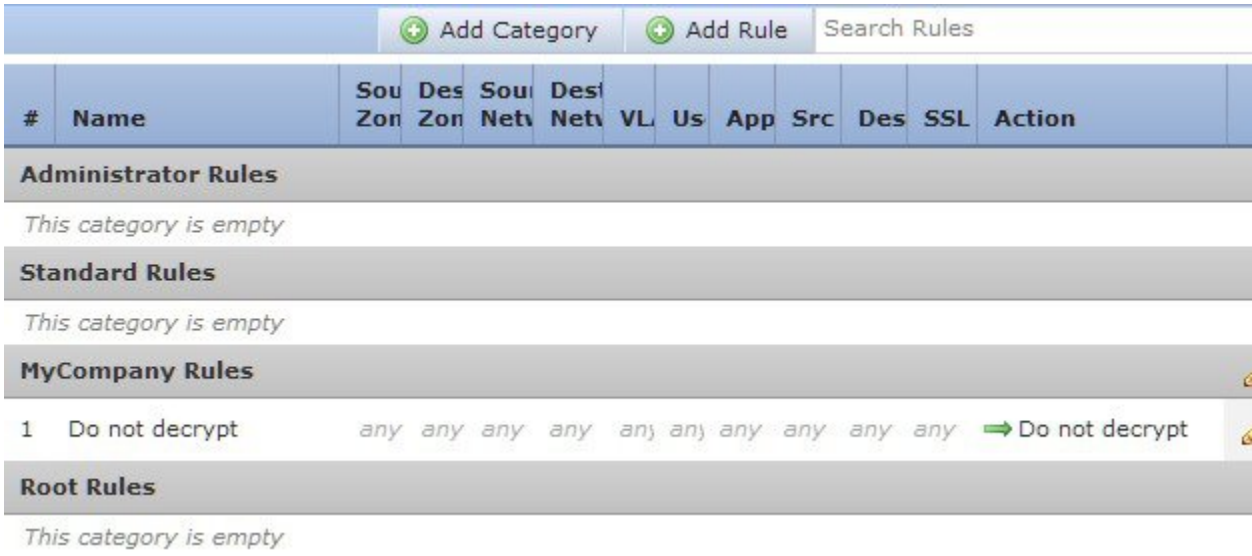
ステップ 5 [Save] をクリックしてルールを保存します。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（設定変更の導入 （92 ページ）を参照してください）。

ポリシー内の SSL ルールの管理

ライセンス：任意

SSL ポリシー エディタの [Rules] タブでは、以下の図に示すように、ポリシー内の SSL ルールの追加、編集、検索、移動、有効化、無効化、削除、およびその他の管理ができます。



各ルールについて、ポリシー エディタでは、その名前、条件のサマリー、およびルール アクションが表示されます。警告、エラー、その他の重要な情報がアイコンで示されます。無効なルールはグレーで表示され、ルール名の下に [(disabled)] というマークが付きます。アイコンの詳細については、「SSL ルールのトラブルシューティング （258 ページ）」を参照してください。

SSL ルールの検索

ライセンス：任意

スペースおよび印刷可能な特殊文字を含む英数字文字列を使用して、SSL ルールのリストで一致する値を検索できます。この検索では、ルール名およびルールに追加したルール条件が検査されます。ルール条件の場合は、条件タイプ（ゾーン、ネットワーク、アプリケーションなど）ごとに追加できる任意の名前または値が検索照合されます。これには、個々のオブジェクト名または値、グループ オブジェクト名、グループ内の個々のオブジェクト名または値、およびリテラル値が含まれます。

検索文字列のすべてまたは一部を使用できます。照合ルールごとに、一致する値のカラムが強調表示されます。たとえば、 100Bao という文字列のすべてまたは一部を基準に検索すると、少なくとも、100Bao アプリケーションを追加した各ルールの [Applications] カラムが強調表示されます。100Bao という名前のルールもある場合は、[Name] カラムと [Applications] カラムの両方が強調表示されます。

1 つ前または次の照合ルールに移動することができます。ステータス メッセージには、現行の一致および合計一致数が表示されます。

複数ページのルール リストでは、どのページでも一致が検出される可能性があります。最初の一致が検出されたのが最初のページではない場合は、最初の一致が検出されたページが表示されます。最後の一致が現行の一致となっている場合、次の一致を選択すると、最初の一致が表示されます。また、最初の一致が現行の一致となっている場合、前の一致を選択すると、最後の一致が表示されます。

ルールの検索方法：

ステップ 1 検索するポリシーの SSL ポリシー エディタで、[Search Rules] プロンプトをクリックし、検索文字列を入力してから Enter を押します。検索を開始するには、Tab キーを使用するか、ページの空白部分をクリックします。

一致する値を含むルールのカラムが強調表示されます。表示されている（最初の）一致は、他とは区別できるように強調表示されます。

ステップ 2 目的のルールを探すには次の操作が利用できます。

- 照合ルールの間を移動するには、次の一致（▼）または前の一致（▲）をクリックします。
- ページを更新して、検索文字列および強調表示をクリアするには、クリア アイコン（×）をクリックします。

SSL ルールの有効化と無効化

ライセンス：任意

作成した SSL ルールは、デフォルトでイネーブルになっています。ルールを無効にすると、ASA FirePOWER モジュールはネットワーク トラフィックの評価にそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。SSL ポリシーのルール リストを表示すると、無効なルールはグレー表示されますが、変更は可能です。またはルール エディタを使用し

てSSLルールをイネーブルまたはディセーブルにできることに注意してください。「SSL ルールの概要と作成 （242 ページ）」を参照してください。

SSL ルールの状態を変更するには、次の手順を実行します。

ステップ 1 有効または無効にするルールを含むポリシーのSSL ポリシーエディタで、ルールを右クリックして、ルールの状態を選択します。

- 非アクティブなルールをイネーブルにするには、[State] > [Enable] を選択します。
- アクティブなルールを無効にするには、[State] > [Disable] を選択します。

ステップ 2 [Store ASA FirePOWER Changes] をクリックします。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（設定変更の導入 （92 ページ）を参照してください）。

SSL ルールの位置またはカテゴリの変更

ライセンス：任意

SSL ルールを編成しやすいように、SSL ポリシーには、管理者ルール、標準ルール、ルートルールという、ASA FirePOWER モジュールが提供する 3 つのルール カテゴリが用意されています。これらのカテゴリの移動、削除、名前変更はできませんが、カスタム カテゴリの作成は可能です。

SSL ルールの移動

ライセンス：任意

適切なSSLルールの順序を指定することで、ネットワーク トラフィックの処理に必要なリソースが削減され、ルールのプリエンプションを回避できます。

次の手順は、SSL ポリシーエディタを使用して1つまたは複数のルールを同時に移動する方法を説明しています。またはルール エディタを使用して個々の SSL ルールを移動することもできます。「SSL ルールの概要と作成 （242 ページ）」を参照してください。

規則を移動するには、次の手順を実行します。

ステップ 1 移動するルールを含むポリシーのSSL ポリシーエディタで、ルールごとに空白部分をクリックして、ルールを選択します。複数のルールを選択するには、Ctrl キーと Shift キーを使用します。

選択したルールは強調表示されます。

ステップ 2 ルールを移動します。カットアンドペーストおよびドラッグアンドドロップを使用することもできます。

新しい場所にルールをカット アンド ペーストするには、選択したルールを右クリックし、[Cut] を選択します。次に、貼り付けたい位置に隣接するルールの空白部分を右クリックし、[Paste above] または [Paste

below] を選択します。2 つの異なる SSL ポリシーの間では、SSL ルールのコピー アンド ペーストはできないことに注意してください。

ステップ 3 [Store ASA FirePOWER Changes] をクリックします。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（設定変更の導入 （92 ページ）を参照してください）。

新しい SSL ルール カテゴリの追加

ライセンス：任意

SSL ルールを編成しやすいように、SSL ポリシーには、管理者ルール、標準ルール、ルート ルールという、ASA FirePOWER モジュールが提供する 3 つのルール カテゴリが用意されています。これらのカテゴリの移動、削除、名前変更はできませんが、Standard Rules と Root Rules 間でのカスタム カテゴリの作成は可能です。

カスタム カテゴリを追加すると、追加のポリシーを作成しなくても、ルールをさらに細かく編成できます。追加したカテゴリは、名前変更と削除ができます。これらのカテゴリの移動はできませんが、ルールのカテゴリ間およびカテゴリ内外への移動は可能です。

新しいカテゴリを追加するには、次の手順に従います。

ステップ 1 ルール カテゴリを追加するポリシーの SSL ポリシー エディタで、[Add Category] をクリックします。

ヒント ポリシーにルールがすでに含まれている場合は、既存のルールの行の空白部分をクリックして、新しいカテゴリを追加する前にその位置を設定できます。既存のルールを右クリックし、[Insert new category] を選択することもできます。

[Add Category] ポップアップ ウィンドウが表示されます。

ステップ 2 [Name] に、一意のカテゴリ名を入力します。

最大 30 文字の英数字の名前を入力できます。名前には、スペース、および印刷可能な特殊文字を含めることができます。

ステップ 3 次の選択肢があります。

- 既存のカテゴリのすぐ上に新しいカテゴリを配置する場合は、最初の [Insert] ドロップダウンリストから [above Category] を選択した後、2 番目のドロップダウンリストからカテゴリを選択します。ここで選択したカテゴリの上にルールが配置されます。
- 既存のルールの下に新しいカテゴリを配置する場合は、ドロップダウン リストから [below rule] を選択した後、既存のルール番号を入力します。このオプションが有効なのは、ポリシーに少なくとも 1 つのルールが存在する場合のみです。
- 既存のルールの上にルールを配置する場合は、ドロップダウン リストから [above rule] を選択した後、既存のルール番号を入力します。このオプションが有効なのは、ポリシーに少なくとも 1 つのルールが存在する場合のみです。

ステップ 4 [OK] をクリックします。

カテゴリが追加されます。カテゴリ名を編集するには、カスタム カテゴリの横にある編集アイコンをクリックします。カテゴリを削除するには、削除アイコンをクリックします。削除するカテゴリに含まれるルールは、その上にあるカテゴリに追加されます。

ステップ 5 [Store ASA FirePOWER Changes] をクリックしてポリシーを保存します。

SSL ルールのトラブルシューティング

ライセンス：任意

SSL ルールを適切に作成して順序付けることは複雑な作業ですが、これは効果的な展開を構築する上で不可欠な要素です。慎重なポリシーの設計を怠ると、他のルールをプリエンプション処理したり、追加ライセンスが必要となったり、無効な設定を含んだルールになる可能性があります。ASA FirePOWER モジュールでトラフィックが想定どおりに処理されるようにするために、SSL ポリシー インターフェイスには、ルールに関する強力な警告およびエラーのフィードバック システムが用意されています。

各ルールについては、次の表に示すように、ポリシー エディタのアイコンによる警告とエラーの表示がされます。アイコンにポインタを合わせると、警告、エラー、情報の内容を示すテキストを確認できます。

表 *41 : SSL* のエラー アイコン

アイコン	説明	詳細
	警告	問題によっては、ルールやその他の警告を示している SSL ポリシーであっても、適用が可能な場合があります。この場合、間違いのある設定は機能しません。たとえば、プリエンプションされたルールはトラフィックを評価しません。ただし、警告アイコンがライセンス エラーまたはモデルの不一致を示している場合は、問題が解消されるまでそのポリシーは適用できません。 警告が出されているルールを無効にすると、警告アイコンが消えます。潜在する問題を修正せずにルールを有効にすると、警告アイコンが再表示されます。
	エラー	ルールまたはその他の SSL ポリシー設定にエラーがある場合、問題が解消されるまでそのポリシーは適用できません。
	情報	情報アイコンは、トラフィックのフローに影響する可能性がある設定に関する有用な情報を伝送します。これらの問題は重大ではなく、ポリシーの適用を妨げません。

SSLルールを適切に設定することは、ネットワーク トラフィックの処理に必要なリソースの軽減にも寄与します。複雑なルールを作成したりルールの順番が不適切であると、パフォーマンスに影響する場合があります。

ルールのプリエンプションと無効な設定の警告について

ライセンス：任意

SSLルールを適切に設定して順序付けることは、効果的な展開を構築する上で不可欠な要素です。SSLポリシーの内部では、SSLルールで他のルールのプリエンプションが発生したり、無効な設定が含まれたりする場合があります。これらの問題を示すために、モジュールでは警告およびエラーのアイコンを使用します。

ルールのプリエンプションの警告について

SSLルールの条件が後続のルールによるトラフィックの照合をプリエンプション処理する場合があります。次に例を示します。

```
Rule 1: do not decrypt Administrators
Rule 2: block Administrators
```

上記の最初のルールによってトラフィックは事前に許可されているため、2番目のルールによってトラフィックがブロックされることはありません。

無効な設定の警告について

SSL ポリシーが依存する外部の設定は変更される可能性があるため、有効であった SSL ポリシー設定が無効になる場合があります。次の例について考えてみます。

- URL カテゴリ条件を含むルールは、URL Filtering ライセンスを持たないモジュールをターゲットにするまで有効な場合があります。その時点で、ルールの横にエラーアイコンが表示され、ポリシーをそのデバイスに適用できなくなります。適用可能にするには、このルールを編集または削除するか、ポリシーのターゲットを変更するか、または適切なライセンスを有効にする必要があります。
- Decrypt - Resign ルールを作成し、後でパッシブ インターフェイスでセキュリティ ゾーンをゾーン条件に追加した場合、ルールの横に警告アイコンが表示されます。パッシブ展開では証明書の再署名によるトラフィックの復号はできないので、パッシブインターフェイスをルールから削除するか、またはルール アクションを変更するまで、このルールには効果がありません。
- ルールにユーザを追加した後、LDAP ユーザ認識設定を変更してそのユーザを除外すると、そのユーザはアクセス コントロールの対象ではなくなるため、そのルールの影響を受けなくなります。

SSL ルールの順序指定によるパフォーマンス向上とプリエンプション回避

ライセンス：任意

SSL ポリシーのルールには 1 から始まる番号が付いています。ASA FirePOWER モジュールは、ルール番号の昇順で、ルールを上から順にトラフィックと照合します。Monitor ルールを除き、トラフィックが最初に一致するルールが、当該トラフィックを処理するためのルールになります。

適切な SSL ルールの順序は、ネットワーク トラフィックの処理に必要なリソースを軽減し、ルールのプリエンプションを回避します。ユーザが作成するルールはすべての組織と展開に固有のものですが、ユーザのニーズに対処しながらもパフォーマンスを最適化できるルールを順序付けする際に従うべきいくつかの一般的なガイドラインがあります。

ルール条件は高いものから低いものに順序付ける

最初に、組織のニーズに適する順番でルールを配置します。すべてのトラフィックに適用する必要があるプライオリティ ルールをポリシーの先頭部分付近に配置します。たとえば、ある 1 人のユーザからの発信トラフィックは詳細な分析用に復号化するが（Decrypt - Resign ルールを使用）、その部門の他のすべてのユーザからのトラフィックは復号化しない（Do not decrypt ルールを使用）場合は、この順序で 2 つの SSL ルールを配置します。

特定のルールから一般的なルールへの順序付け

具体的なルール、つまり処理するトラフィックの定義を絞り込むルールを先に設定することで、パフォーマンスを向上させることができます。これは、広範な条件を持つルールが多くのさまざまなタイプのトラフィックを照合し、後でより多くの特定のルールをプリエンプション処理することができるという理由からも重要です。

ここで 1 つのシナリオとして、信頼できる CA（Good CA）が悪意のあるエンティティ（Bad CA）に間違って CA 証明書を発行してしまい、その証明書を取り消していない状況を考えてみましょう。信頼できない CA によって発行された証明書で暗号化されたトラフィックはブロックしたいが、信頼できる CA の信頼チェーン内にあるそれ以外のトラフィックは許可したいとします。ここで必要となるのは、CA 証明書およびすべての中間 CA 証明書をアップロードし、その後に次のようにルールを順序付けることです。

```
Rule 1: Block issuer CN=www.badca.com
Rule 2: Do not decrypt issuer CN=www.goodca.com
```

ルールを入れ替える場合は次のようになります。

```
Rule 1: Do not decrypt issuer CN=www.goodca.com
Rule 2: Block issuer CN=www.badca.com
```

最初のルールは Good CA によって信頼されたすべてのトラフィックに一致し、その中には Bad CA によって信頼されたトラフィックも含まれます。どのトラフィックも 2 番目のルールに一致しないため、悪意のあるトラフィックはブロックされずに許可される可能性があります。

証明書でピニングしたサイトからのトラフィックを許可するルールの配置

証明書のピニングを行うと、SSL セッションが確立される前に、サーバの公開キー証明書が、サーバに既に関連付けられているブラウザの証明書と一致しているかどうかを、クライアントのブラウザが強制的に確認します。Decrypt - Resign アクションにはサーバ証明書を変更してか

らクライアントに渡すという動作が含まれているため、ブラウザが既にその証明書をピニングしている場合は、変更された証明書が拒否されます。

たとえば、クライアント ブラウザが、証明書のピニングを使用するサイト windowsupdate.microsoft.com に接続されていて、そのトラフィックと一致する SSL ルールを [Decrypt - Resign] アクションを使用して設定すると、ASA FirePOWER モジュールはサーバ証明書に再署名してから、クライアントブラウザに渡します。この変更されたサーバ証明書は、ブラウザでピニングした windowsupdate.microsoft.com の証明書と一致しないため、クライアント ブラウザは接続を拒否します。

このトラフィックを許可するには、サーバ証明書の共通名または識別名と突き合わせるように、Do not decrypt アクションを使用して SSL ルールを設定します。SSL ポリシーでは、このルールを、トラフィックと一致するすべての Decrypt - Resign ルールの前に配置してください。Web サイトに正常に接続された後で、クライアント ブラウザから、ピニングされた証明書を取得できます。接続が成功した場合も、失敗した場合も、ログに記録された接続イベントから証明書を表示できます。

トラフィックを復号化するルールは後方に配置する

トラフィックの復号化はリソースを必要とする処理なので、トラフィックの復号化を実行しないルール（Do not decrypt、Block）を、実行するルール（Decrypt - Known Key、Decrypt - Resign）より前に配置することで、パフォーマンスが向上する可能性があります。この理由は、トラフィック復号化のコマンドには多量のリソースを消費するものがあるからです。また、Block ルールにより、ASA FirePOWER モジュールで復号化やインスペクションの対象となるはずのトラフィックが迂回されることがあります。他の要素がすべて同等、つまり、より重要なものがなくプリエンプションが問題ではない場合にルールのセットを与えると仮定すると、次の順序でルールを配置することを検討します。

- 一致する接続はロギングするが、トラフィックで他のアクションは実行しないモニタ ルール
- それ以上のインスペクションなしでトラフィックをブロックする Block ルール
- 暗号化トラフィックを復号化しない Do not decrypt ルール
- 既知の秘密キーを使用して着信トラフィックを復号する Decrypt - Known Key ルール
- サーバ証明書の再署名によって発信トラフィックを復号化する Decrypt-Resign ルール

ClientHello の変更の優先順位付け

ClientHello の変更を優先順位付けするには、ServerHello またはサーバ証明書条件に一致するルールの前に、ClientHello メッセージで使用可能な条件に一致するルールを配置します。

管理対象デバイスが SSL ハンドシェイクを処理するときに、ClientHello メッセージを変更して、復号化の可能性を高めることができます。たとえば、FirePOWER システムは圧縮されたセッションを復号化できないので、圧縮メソッドを削除できます。

システムは Decrypt - Resign アクションを含む SSL ルールに最終的に一致させることができる場合、ClientHello メッセージを変更するのみです。システムが新しいサーバへの暗号化セッ

ションを最初に検出したときは、サーバ証明書データを ClientHello の処理には使用できません。これは復号化されていない最初のセッションとなる可能性があります。同じクライアントからの後続の接続で、システムはサーバ証明書条件を含むルールに ClientHello メッセージを最終的に一致させ、メッセージを処理して、復号化の可能性を最大化できます。

ServerHello またはサーバ証明書条件（証明書、識別名、証明書のステータス、暗号スイート、バージョン）と一致するルールを、ClientHello 条件（ゾーン、ネットワーク、VLAN タグ、ポート、ユーザ、アプリケーション、URL カテゴリ）と一致するルールの前に配置する場合、ClientHello の変更をプリエンプション処理し、復号されないセッションの数を増やすことができます。

パフォーマンスを改善する SSL インスペクション設定

ライセンス：任意

複雑な SSL ポリシーおよびルールのコマンドには、多量のリソースを消費するものがあります。SSL ポリシーを適用すると、ASA FirePOWER モジュールはすべてのルールをまとめて評価し、ネットワーク トラフィックの評価にデバイスが使用する条件の拡張セットを作成します。デバイスでサポートされる SSL ルールの最大数を超えていることを警告するポップアップ ウィンドウが表示される場合があります。この最大値は、デバイスの物理メモリやプロセッサ数などの、さまざまな要因によって異なります。

ルールの単純化

次のガイドラインは、SSL ルールの単純化とパフォーマンスの向上に役立ちます。

- ルールを構築するときは、条件内で使用する個々の要素は可能な限り少なくします。たとえばネットワーク条件であれば、個別の IP アドレスではなく、IP アドレス ブロックを使用します。ポート条件では、ポート範囲を使用します。アプリケーション制御および URL フィルタリングを実行する場合はアプリケーション フィルタと URL カテゴリおよびレピュテーションを使用し、ユーザ制御を実行する場合は LDAP ユーザ グループを使用します。

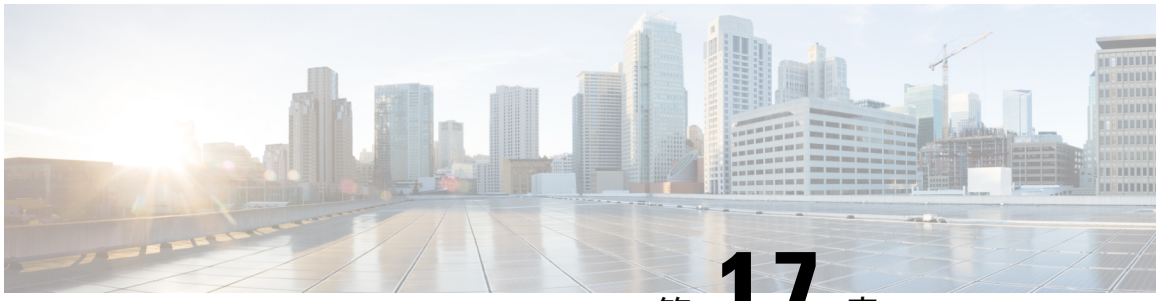
SSL ルール条件で使用するオブジェクトに要素を結合してもパフォーマンスは向上しないことに注意してください。たとえば、50 の個別の IP アドレスを含むネットワーク オブジェクトを使用しても、その条件内のそれらの IP アドレスに対するものを含む、組織的な（パフォーマンスではない）利点が個別に与えられるだけです。

- できるだけセキュリティ ゾーンでルールを制限します。デバイスのインターフェイスが、ゾーン制限されたルールのどのゾーンにも属さない場合、そのデバイスのパフォーマンスにルールは影響を与えません。
- ルールを過度に設定しないようにします。1 つの条件が処理するトラフィックに一致するのに十分な場合は、2 つ使用しないでください。

トラフィック復号化の設定

トラフィック復号化を設定する際は、次の注意事項に従ってください。

- トラフィックの復号化は、トラフィックを復号化してアクセス コントロールによるチェックを実行するため、リソースを必要とする処理です。処理対象を絞り込んだ復号化ルールを作成すると、処理対象が広範な復号化ルールより、ASA FirePOWER モジュールが復号化するトラフィック量が減るため、結果として、トラフィックの復号化に必要な処理リソースも削減されます。トラフィックをいったん復号化した後にアクセス コントロール ルールを使用して許可またはブロックするのではなく、暗号化トラフィックはできるだけブロックするか復号化しないことを選択するようにします。
- ルート発行元 CA に基づいてトラフィックを信頼するように証明書ステータスの条件を設定する場合は、ルート CA 証明書およびルート CA 信頼チェーン内のすべての中間 CA 証明書を SSL ポリシーにアップロードするようにします。信頼できる CA の信頼チェーン内のすべてのトラフィックは復号化なしで許可されるようになり、不要な復号化は実施されません。



第 17 章

SSLルールを使用したトラフィック復号化の調整

ASA FirePOWER モジュールで検査されるすべての暗号化トラフィックに対するルール アクションには、基本的なSSLルールが適用されます。暗号化トラフィックをより詳細に復号化および制御するには、特定タイプのトラフィックの処理およびログ記録を制御するルール条件を設定します。各 SSL ルールには 0 個、1 個、または複数の条件を設定できますが、トラフィックにSSLルールが適用されるのは、そのルールのすべての条件にトラフィックが一致する場合のみです。

（注） トラフィックがルールに一致すると、ASA FirePOWERモジュールはその設定ルールのアクションをトラフィックに適用します。ログの記録が設定されている場合、接続が終了した時点でモジュールではトラフィックに関するログが記録されます。詳細については、アクセス コントロールおよび SSL ルール アクションがどのようにロギングに影響を及ぼすかについて （471 ページ）およびアクセス コントロールの処理に基づく接続のロギング （477 ページ）を参照してください。

各ルール条件には、照合するトラフィックのプロパティを1つまたは複数指定できます。たとえば、以下のプロパティを指定できます。

- 通過するセキュリティ ゾーン、IP アドレスおよびポート、送信元または宛先の国などのトラフィック フロー
- 検出された IP アドレスに関連付けられたユーザ
- トラフィックで検出されたアプリケーションなどのトラフィック ペイロード
- 接続の暗号化に使用された SSL/TLS プロトコル バージョン、暗号スイート、サーバ証明書などの接続暗号化
- サーバ証明書の識別名に指定された URL のカテゴリおよびレピュテーション

- TLS/SSL 復号化：再署名のガイドライン （266 ページ）
- ネットワークベースの条件による暗号化トラフィックの制御 （266 ページ）

TLS/SSL 復号化：再署名のガイドライン

場合によっては、アクセス制御の信頼ルールアクションが一致する TLS/SSL トラフィックをブロックすることがあります。この問題は、ASA 5555-X デバイスなど、FirePOWER サービスを備えた ASA を実行できるすべての ASA デバイスに限定されます。

次の注意事項に従ってください。

- [Decrypt - Resign] または [Do Not Decrypt] のルールのアクションのいずれかと一致する TLS/SSL トラフィックの場合は、アクセス制御の許可ルールのアクションが信頼ルールのアクションよりも前に配置されていることを確認します。
- SSL ポリシーがない場合は、アクセス制御の信頼ルールのアクションに問題はありません。

FirePOWER サービスを備えた ASA を実行できるデバイスのリストについては、Cisco ASA の互換性の「ASA and ASA FirePOWER Module Compatibility」の項を参照してください。

ネットワークベースの条件による暗号化トラフィックの制御

ライセンス：任意

SSL ポリシーに追加する SSL ルールにより、暗号化トラフィックの処理やログ記録を詳細に制御できます。ネットワークベースの条件を使用して、ネットワークを通過する暗号化トラフィックを管理できます。以下の条件を使用できます。

- 送信元と宛先のセキュリティ ゾーン
- 送信元と宛先 IP アドレスまたは地理的位置
- 送信元と宛先のポート

ネットワークベースの複数の条件を組み合わせたり、他のタイプの条件と組み合わせたりして、SSL ルールを作成できます。これらの SSL ルールは単純にも複雑にも設定でき、複数の条件を使用してトラフィックを照合および検査できます。SSL ルールの詳細については、SSL ルールの開始 （239 ページ）を参照してください。

ネットワーク ゾーンによる暗号化トラフィックの制御

ライセンス：任意

SSL ルールでゾーン条件を設定すると、暗号化トラフィックの送信元および宛先のセキュリティ ゾーンに応じてそのトラフィックを制御できます。

セキュリティ ゾーンは、1 つ以上のインターフェイスのグループです。検出モードと呼ばれる、デバイスの初期セットアップ時に選択するオプションによって、ASA FirePOWER モジュールによるデバイスのインターフェイスの初期設定の方法、およびデバイスのインターフェイスがセキュリティ ゾーンに属するかどうかが決まります。

単純な例として、デバイスをインライン検出モードに登録する場合、ASA FirePOWER モジュールにより内部と外部の 2 つのゾーンが作成され、そのデバイスの最初のインターフェイスのペアがそれらのゾーンに割り当てられます。内部側のネットワークに接続されたホストは、保護されている資産を表します。

ヒント 内部（または外部）のすべてのインターフェイスを 1 つのゾーンにグループ化する必要はありません。導入ポリシーおよびセキュリティ ポリシーが意味をなすグループ化を選択します。ゾーン作成の詳細については、セキュリティ ゾーンの操作 （64 ページ）を参照してください。

この展開では、これらのホストにインターネットへの無制限アクセスを提供できますが、着信する暗号化トラフィックを復号化および検査してホストを保護しなければなりません。

SSL インスペクションでこれを実現するには、[Destination Zone] を [Internal] に設定したゾーン条件を SSL ルールに定義します。この単純な SSL ルールでは、内部ゾーンのいずれかのインターフェイスからデバイスを離れるトラフィックが照合されます。

より複雑なルールを作成する場合は、1 つのゾーン条件で [Source Zones] および [Destination Zones] それぞれに対し、最大 50 のゾーンを追加できます。

- 特定のゾーンのインターフェイスからデバイスを離れる暗号化トラフィックを照合するには、そのゾーンを [Destination Zones] に追加します。

パッシブに展開されたデバイスはトラフィックを送信しないので、パッシブインターフェイスで構成されるゾーンを [Destination Zones] 条件で使用することはできません。

- 特定のゾーンのインターフェイスからデバイスに入る暗号化トラフィックを照合するには、そのゾーンを [Source Zones] に追加します。

送信元（Source）ゾーン条件と宛先（Destination）ゾーン条件の両方をルールに追加する場合、送信元ゾーンから発信され**かつ**宛先ゾーンを介して出力されるトラフィックにルールが適用されます。

ゾーン内のすべてのインターフェイスが同じタイプ（インライン、パッシブ、スイッチド、またはルーテッド）である必要があるため、SSL ルールのゾーン条件で使用されているすべてのゾーンが同じタイプでなければならないことに注意してください。つまり、異なるタイプのゾーンを送信元/宛先とする暗号化トラフィックを照合する単一ルールを定義することはできません。

ゾーンにインターフェイスが含まれていないなど、無効な設定が検出されると、警告アイコンが表示されます。アイコンの上にポインタを置くと詳細が表示されます。

ゾーン条件に基づいて暗号化トラフィックを制御するには、次の手順を実行します。

ステップ 1 ゾーンに応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの開始 （239 ページ）を参照してください。

ステップ 2 SSL ルール エディタで、[Zones] タブを選択します。

[Zones] タブが表示されます。

ステップ 3 [Available Zones] から追加するゾーンを見つけて選択します。

追加するゾーンを検索するには、[Available Zones] リストの上にある [Search by name] プロンプトをクリックし、ゾーン名を入力します。入力すると、リストが更新されて一致するゾーンが表示されます。

クリックすると、ゾーンを選択できます。複数のゾーンを選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [Select All] を選択します。

ステップ 4 [Add to Source] または [Add to Destination] をクリックして、選択したゾーンを適切なリストに追加します。

選択したゾーンをドラッグ アンド ドロップすることもできます。

ステップ 5 ルールを保存するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（設定変更の導入 （92 ページ）を参照してください）。

ネットワークまたは地理的位置による暗号化トラフィックの制御

ライセンス：任意

SSL ルールでネットワーク条件を設定すると、暗号化トラフィックの送信元および宛先の IP アドレスに応じてそのトラフィックを制御および復号化できます。次のいずれかの操作を実行できます。

- 制御する暗号化トラフィックの送信元および宛先の IP アドレスを明示的に指定する。
- IP アドレスを地理的位置に関連付ける位置情報機能を使用して、その送信元または宛先の国または大陸に基づいて暗号化トラフィックを制御する。

ネットワークベースの SSL ルールの条件を作成する場合、IP アドレスと地理的位置を手動で指定できます。または、名前を 1 つ以上の IP アドレス、アドレス ブロック、国、大陸などに関連付ける再利用可能なネットワーク オブジェクトおよび地理位置情報オブジェクトを使用してネットワーク条件を設定できます。

ヒント　ネットワーク オブジェクトや位置情報オブジェクトを作成しておくと、それを使用して SSL ルールを作成したり、モジュール インターフェイスのさまざまな場所で IP アドレスを表すオブジェクトとして使用したりできます。これらのオブジェクトはオブジェクトマネージャを使用して作成できます。また、SSL ルールの設定時にネットワーク オブジェクトをオンザフライで作成することもできます。詳細については、再使用可能オブジェクトの管理 （23 ページ）を参照してください。

地理的位置別にトラフィックを制御するルールを作成する場合は、確実に最新の地理位置情報データを使用してトラフィックをフィルタ処理するために、 ASA FirePOWER モジュールで地理位置情報データベース（GeoDB）を定期的に更新することを強くお勧めします。地理情報データベースについて （595 ページ）を参照してください。

次の図は、内部ネットワークから発信され、ケイマン諸島（Cayman Islands）または海外にある持ち株会社のサーバ（182.16.0.3）のリソースにアクセスしようとする暗号化接続をブロックする SSL ルールのネットワーク条件を示しています。

この例では、持ち株会社のサーバの IP アドレスを手動で指定し、ケイマン諸島の IP アドレスを表す ASA FirePOWER モジュール提供の地理位置情報オブジェクト Cayman Island を使用しています。

1 つのネットワーク条件で [Source Networks] および [Destination Networks] それぞれに最大 50 の項目を追加でき、ネットワークベースの設定と位置情報ベースの設定を組み合わせることができます。

- 特定の IP アドレスまたは地理的位置からの暗号化トラフィックを照合するには、[Source Networks] を設定します。
- 特定の IP アドレスまたは地理的位置への暗号化トラフィックを照合するには、[Destination Networks] を設定します。

送信元（Source）ネットワーク条件と宛先（Destination）ネットワーク条件の両方をルールに追加する場合、送信元 IP アドレスから発信され**かつ**宛先 IP アドレスに送信される暗号化トラフィックにルールが適用されます。

無効なネットワーク条件設定が検出されると、警告アイコンが表示されます。アイコンの上にポインタを置くと詳細が表示されます。

ネットワークまたは地理的位置の条件に応じてトラフィックを制御するには、次の手順を実行します。

アクセス：管理者/アクセス管理者/ネットワーク管理者

ステップ 1 ネットワークに応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成 （242 ページ）を参照してください。

ステップ 2 SSL ルール エディタで、[Networks] タブを選択します。

[Networks] タブが表示されます。

ステップ 3 [Available Networks] から、次のように追加するネットワークを見つけて選択します。

- 追加するネットワーク オブジェクトとグループを表示するには [Networks] タブをクリックします。地理位置情報オブジェクトを表示するには [Geolocation] タブをクリックします。
- ここでネットワーク オブジェクトを作成してリストに追加するには、[Available Networks] リストの上にある追加アイコン（）をクリックし、ネットワーク オブジェクトの操作 （26 ページ）の手順に従います。
- 追加するネットワーク オブジェクトまたは位置情報オブジェクトを検索するには、適切なタブを選択し、[Available Networks] リストの上にある [Search by name or value] プロンプトをクリックして、オブジェクト名またはオブジェクトのいずれかの値を入力します。入力を開始するとリストが更新され、一致するオブジェクトが表示されます。

オブジェクトを選択するには、そのオブジェクトをクリックします。複数のオブジェクトを選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [Select All] を選択します。

ステップ 4 [Add to Source] または [Add to Destination] をクリックして、選択したオブジェクトを適切なリストに追加します。

選択したオブジェクトをドラッグ アンド ドロップでリストに追加することもできます。

ステップ 5 手動で指定する送信元または宛先 IP アドレスまたはアドレス ブロックを追加します。

[送信元ネットワーク（Source Networks）] リストまたは [宛先ネットワーク（Destination Networks）] リストの下にある [IP アドレスの入力（Enter an IP address）] プロンプトをクリックし、1 つの IP アドレスまたはアドレス ブロックを入力して [追加（Add）] をクリックします。

ステップ 6 ルールを保存するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（設定変更の導入 （92 ページ）を参照してください）。

ポートによる暗号化トラフィックの制御

ライセンス：任意

SSL ルールでポート条件を設定すると、暗号化トラフィックの送信元および宛先の TCP ポートに応じてそのトラフィックを制御できます。ポートベースの SSL ルールの条件を作成すると

きは、手動で TCP ポートを指定できます。または、名前を 1 つ以上のポートに関連付ける再利用可能なポート オジェクトを使用してポート条件を設定できます。

ヒント ポート オブジェクトを作成しておくと、それを使用して SSL ルールを作成したり、モジュール インターフェイスのさまざまな場所でポートを表すオブジェクトとして使用したりできます。ポート オブジェクトは、オブジェクト マネージャを使用して作成できます。また、SSL ルールの設定時に作成することもできます。詳細については、ポート オブジェクトの操作（33 ページ）を参照してください。

1 つのネットワーク条件で [Selected Source Ports] および [Selected Destination Ports] リストそれぞれに対し、最大 50 の項目を追加できます。

- 特定の TCP ポートからの暗号化トラフィックを照合するには、[Selected Source Ports] を設定します。
- 特定の TCP ポートへの暗号化トラフィックを照合するには、[Selected Destination Ports] を設定します。
- [Selected Source Ports] および [Selected Destination Ports] の両方を設定すると、特定の送信元（Source）TCP ポートから発信されかつ特定の宛先（Destination）TCP ポートに送信される暗号化トラフィックが照合されます。

[Selected Source Ports] および [Selected Destination Ports] リストで設定できるのは TCP ポートだけです。非 TCP ポートを含むポート オブジェクトは、[使用可能ポート（Available Ports）] リストではグレイで表示されます。

ポート条件を作成する際、警告アイコンは無効な設定を示します。たとえば、既存のポート オブジェクトをオブジェクト マネージャで編集すると、それらのオブジェクト グループを使用するルールが無効になります。アイコンの上にポインタを置くと詳細が表示されます。

ポート条件に基づいてトラフィックを制御するには、次の手順を実行します。

ステップ 1 TCP ポートに応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成 （242 ページ）を参照してください。

ステップ 2 SSL ルール エディタで、[Ports] タブを選択します。

[Ports] タブが表示されます。

ステップ 3 [Available Ports] で、追加する TCP ポートを選択します。

- ここで TCP ポート オブジェクトを作成してリストに追加するには、[Available Ports] リストの上にある追加アイコン（  ）をクリックし、ポート オブジェクトの操作 （33 ページ）の手順に従います。
- 追加する TCP ベースのポート オブジェクトおよびグループを検索するには、[利用可能なポート（Available Ports）] リストの上にある [名前または値で検索（Search by name or value）] プロンプトをクリックし、オブジェクトの名前またはオブジェクトのポートの値を入力します。入力を開始すると

リストが更新され、一致するオブジェクトが表示されます。たとえば、「443」と入力すると、ASA FirePOWER モジュールに ASA FirePOWER モジュール提供の HTTP ポート オブジェクトが表示されます。

TCP ベースのポート オブジェクトを 1 つ選択するには、それをクリックします。複数の TCP ベースのポート オブジェクトを選択するには、Shift キーおよび Ctrl キーを使用します。または、右クリックして [Select All] を選択します。非 TCP ベースのポートを含んでいるオブジェクトは、ポート条件に追加できません。

ステップ 4 [Add to Source] または [Add to Destination] をクリックして、選択したオブジェクトを適切なリストに追加します。

選択したオブジェクトをドラッグ アンド ドロップでリストに追加することもできます。

ステップ 5 送信元または宛先のポートを手動で指定するには、[Selected Source Ports] または [Selected Destination Ports] リストの下にある [Port] にポート番号を入力します。0 ～ 65535 の値を持つ 1 つのポートを指定できます。

ステップ 6 [Add] をクリックします。

ASA FirePOWER モジュールでは、無効な設定となるルール条件にはポートが追加されません。

ステップ 7 ルールを保存するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（設定変更の導入 （92 ページ）を参照してください）。

ユーザ ベースの暗号化トラフィックの制御

ライセンス：Control

SSL ルールでユーザ条件を設定すると、Microsoft Active Directory サーバから取得されるユーザに応じてそのトラフィックを制御できます。SSL ルールのユーザ条件では、ホストにログインしている LDAP ユーザに基づいてトラフィックを制限することで、ネットワークを通過するトラフィックを管理するユーザ制御が可能になります。

ユーザ制御は、アクセス制御されたユーザと IP アドレスを関連付けることによって機能します。この機能では、ホストにログインまたはホストからログアウトするとき、または他の理由で Active Directory 認証を行うときに、特定のユーザをモニタするエージェントを展開します。たとえば、アプリケーションやサービスでの認証を Active Directory で一元管理している組織では、このトラフィック制御方法を検討できます。

ユーザ条件を設定した SSL ルールとトラフィックを一致させるには、モニタ対象のセッションにおける送信元または宛先ホストの IP アドレスと、ログインする「アクセス制御されたユーザ」を関連付ける必要があります。この機能では、特定のユーザまたはユーザ グループに基づいてトラフィックを制御できます。

複数のユーザ条件を組み合わせたり、他のタイプの条件と組み合わせたりして、SSL ルールを作成できます。これらの SSL ルールは単純にも複雑にも設定でき、複数の条件を使用してトラ

フィックを照合および検査できます。SSL ルールの詳細については、SSL ルールの概要と作成（242 ページ）を参照してください。

ユーザ制御機能を使用するには、Control ライセンスが必要です。また、ユーザ エージェントのモニタリング Microsoft Active Directory サーバによって報告されるログインおよびログアウトのレコードを使用している、LDAP ユーザおよびグループ（アクセス制御されたユーザ）に対してのみサポートされます。

ユーザ条件を含む SSL ルールを作成する前に、ASA FirePOWER モジュールと組織内の少なくとも 1 つの Microsoft Active Directory サーバとの間の接続を設定しておく必要があります。この設定は認証オブジェクトと呼ばれ、サーバの接続設定と認証フィルタ設定が含まれています。また、ユーザ条件で使用できるユーザも指定されます。

さらに、ユーザ エージェントをインストールする必要もあります。エージェントは、Active Directory クレデンシャルで認証するユーザをモニタし、それらのログイン レコードを ASA FirePOWER モジュールに送信します。これらのレコードによりユーザが IP アドレスに関連付けられ、これに基づいてユーザ条件を含んでいる SSL ルールが照合可能になります。

ユーザ条件に基づいて暗号化トラフィックを制御するには、次の手順を実行します。

ステップ 1 ユーザに応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成 （242 ページ）を参照してください。

ステップ 2 SSL ルール エディタで、[Users] タブを選択します。

[Users] タブが表示されます。

ステップ 3 追加するユーザを検索するには、[Available Users] リストの上にある [Search by name or value] プロンプトをクリックし、ユーザ名を入力します。入力を開始するとリストが更新され、一致するユーザが表示されます。

ユーザをクリックして選択します。複数のユーザを選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [Select All] を選択します。

ステップ 4 [Add to Rule] をクリックして、選択したユーザを [Selected Users] リストに追加します。

選択したユーザをドラッグ アンド ドロップでリストに追加することもできます。

ステップ 5 ルールを保存するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（を参照してください）。設定変更の導入 （92 ページ）

レピュテーションによる暗号化トラフィックの制御

ライセンス：Control または URL Filtering

SSL ルールでレピュテーション ベース条件を設定すると、ネットワーク トラフィックをコンテキスト化して状況に応じて制限することで、ネットワーク通過を許可する暗号化トラフィックを管理できます。SSLルールでのレピュテーションベースの制御には、以下のタイプがあります。

- アプリケーション条件によるアプリケーション制御では、個々のアプリケーションだけでなく、アプリケーションの基本的な特性（タイプ、リスク、ビジネスとの関連性、およびカテゴリ）に基づいてアプリケーション トラフィックを制御できます。
- URL 条件では、Web サイトに割り当てられたカテゴリおよびレピュテーションに基づいて Web トラフィックを制御できます。

レピュテーションベースの複数の条件を組み合わせたり、他のタイプの条件と組み合わせたりして、SSLルールを作成できます。これらのSSLルールは単純にも複雑にも設定でき、複数の条件を使用してトラフィックを照合および検査できます。

アプリケーション ベースの暗号化トラフィックの制御

ライセンス：Control

Firepower システムは、暗号化された IP トラフィックを分析するときに、ネットワーク上で一般的に使用されている暗号化アプリケーションを識別および分類してから暗号化セッションを復号化します。ASA FirePOWER モジュールでは、この検出ベースのアプリケーション認識機能を使用して、ネットワーク上の暗号化されたアプリケーション トラフィックを制御できます。

SSL ルールのアプリケーション条件により、このアプリケーション制御を実行できます。1 つのルールにおいて、トラフィックの制御対象とするアプリケーションを複数の方法で指定できます。

- 各アプリケーションを個別に選択する（カスタム アプリケーションを含む）。
- ASA FirePOWER モジュール提供のアプリケーション フィルタを使用する。このフィルタは、基本的な特性（タイプ、リスク、ビジネスとの関連性、およびカテゴリ）に応じて構成された名前付きのアプリケーション セットです。
- カスタム アプリケーション フィルタを作成して使用する。このフィルタでは、任意の方法でアプリケーションをグループ化できます（カスタム アプリケーションを含む）。

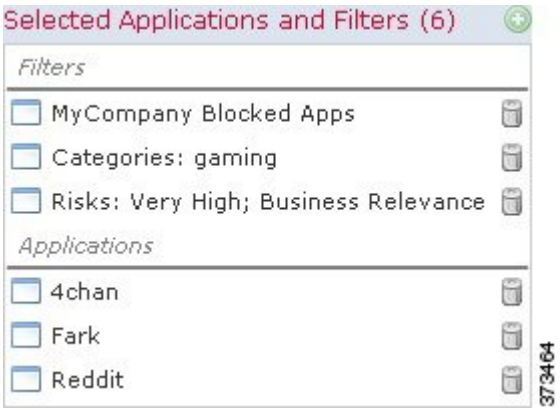
（注） アクセス コントロール ルールを使用してアプリケーション トラフィックをフィルタ処理する場合、フィルタ条件としてアプリケーションタグを使用できます。ただし、暗号化トラフィックはアプリケーション タグでフィルタ処理できません。ASA FirePOWER モジュールが暗号化トラフィックで検出できるアプリケーションはすべてタグ付きのSSLプロトコルです。このタグが付いていないアプリケーションは、暗号化されていないトラフィックまたは復号化されたトラフィックでのみ検出できます。

アプリケーションフィルタを利用すると、SSL ルールのアプリケーション条件を簡単に作成できます。このフィルタによって、ポリシーの作成と管理が簡素化され、モジュールは Web トラフィックを期待通りに確実に制御します。たとえば、暗号化トラフィックのリスクが高くビジネスとの関連性の低いアプリケーションをすべて識別して復号する SSL ルールを作成できます。ユーザがこれらのアプリケーションの使用を試みると、アクセス コントロールによってセッションが復号化されて検査されます。

また、 シスコでは、システムおよび脆弱性データベース（VDB）の更新を通じて頻繁にディテクタを更新および追加しています。独自のディテクタを作成し、そのディテクタが検出するアプリケーションに特性（リスク、関連性など）を割り当てることもできます。アプリケーションの特性に基づいたフィルタを使用することで、モジュールは最新のディテクタを使用してアプリケーション トラフィックをモニタします。

アプリケーション条件を設定した SSL ルールとトラフィックを一致させるには、[選択済みのアプリケーションとフィルタ（Selected Applications and Filters）] リストに追加したいずれかのアプリケーションまたはフィルタにトラフィックが一致する必要があります。

次の図は、MyCompany のアプリケーション、リスクが高くビジネスとの関連性の低いすべてのアプリケーション、ゲームアプリケーション、およびいくつかの指定アプリケーションからなるカスタム グループを復号化する、SSL ルールのアプリケーション条件を示しています。



1 つのアプリケーション条件において、最大 50 の項目を [Selected Applications and Filters] リストに追加できます。以下はそれぞれ 1 つの項目としてカウントされます。

- 個別またはカスタムな組み合わせの、[Application Filters] リストからの 1 つ以上のフィルタ。この項目は、特性を基準にグループ化されたアプリケーションのセットです。
- [Available Applications] リストにあるアプリケーションの検索結果を保存することで作成されたフィルタ。この項目は、アプリケーション名の一部の一致によってグループ化されたアプリケーションのセットです。
- [Available Applications] リストからの個々のアプリケーション。

モジュール インターフェイスでは、条件に追加されたフィルタは上部にリストされ、個別に追加されたアプリケーションとは分けられます。

SSL ポリシーの適用時には、アプリケーション条件を持つルールごとに、ASA FirePOWER モジュールによって一致する固有のアプリケーションのリストが生成されます。つまり、完全な

カバレッジを確保するために、重複フィルタおよび個々に指定されたアプリケーションを使用できます。

アプリケーション フィルタと暗号化トラフィックの照合

ライセンス：Control

SSL ルールのアプリケーション条件を作成するには、[Application Filters] リストを使用して、照合するトラフィックの特性を基にアプリケーションをグループ化します。

便宜上、ASA FirePOWER モジュールは、指定された基準を使用して、検出した各アプリケーションを特徴付けます。これらの基準をフィルタとして使用したり、独自の組み合わせでカスタム フィルタを作成したりしてアプリケーションを制御できます。

SSL ルールでのアプリケーション フィルタの機能は、オブジェクト マネージャを使用した再利用可能なカスタム アプリケーション フィルタの作成と同じです（アプリケーション フィルタの操作 （35 ページ）を参照してください）。また、アクセス コントロール ルールの設定時に作成する各種のフィルタを、新規のフィルタとして保存して再利用することもできます。ユーザが作成したフィルタはネストすることができないため、別のユーザが作成したフィルタを含むフィルタは保存できません。

フィルタの組み合わせ方について

フィルタを単独または組み合わせて選択すると、[Available Applications] リストが更新され、基準を満たすアプリケーションのみが表示されます。ASA FirePOWER モジュール提供のフィルタは組み合わせて選択できますが、カスタム フィルタを組み合わせることはできません。

モジュールは、OR 演算を使用して同じフィルタ タイプの複数のフィルタをリンクします。たとえば、Risks（リスク）タイプの下の Medium（中）および High（高）フィルタを選択すると、結果として次のようなフィルタになります。

```
Risk: Medium OR High
```

Medium（中）フィルタに 110 個のアプリケーション、High（高）フィルタに 82 個のアプリケーションが含まれる場合、[Available Applications] リストには、これら 192 個のアプリケーションがすべて表示されます。

モジュールは、AND 演算を使用して異なるタイプのフィルタをリンクします。たとえば Risks（リスク）タイプで Medium（中）および High（高）フィルタを選択し、Business Relevance（ビジネスとの関連性）タイプで Medium（中）および High（高）フィルタを選択した場合、結果として次のようなフィルタになります。

```
Risk: Medium OR HighANDBusiness Relevance: Medium OR High
```

この場合、モジュールは Medium（中）または High（高）の Risk（リスク）タイプと Medium（中）または High（高）の Business Relevance（ビジネスとの関連性）タイプの両方に含まれるアプリケーションだけを表示します。

フィルタの検索および選択

フィルタを選択するには、フィルタ タイプの横にある矢印をクリックしてそれを展開し、アプリケーションを表示/非表示にする各フィルタの横のチェック ボックスを選択/選択解除しま

す。また、Cisco 提供のフィルタ タイプ（[リスク（Risks）]、[ビジネスとの関連性（Business Relevance）]、[タイプ（Types）]、または [カテゴリ（Categories）]）を右クリックして、[すべて選択（Check All）] または [すべて選択解除（Uncheck All）] を選択することもできます。

フィルタを検索するには、[Available Filters] リストの上にある [Search by name] プロンプトをクリックし、名前を入力します。入力していくと、リストが更新されて一致するフィルタが表示されます。

フィルタを選択したら、[Available Applications] リストを使用してそのフィルタをルールに追加します。個々のアプリケーションからのトラフィックの照合（277ページ）を参照してください。

個々のアプリケーションからのトラフィックの照合

ライセンス：Control

SSL ルールのアプリケーション条件を作成するには、[Available Applications] リストを使用して、照合するトラフィックのアプリケーションを選択します。

アプリケーションのリストの参照

条件の作成を初めて開始するときは、リストは制約されておらず、モジュールが検出するすべてのアプリケーションを一度に 100 個ずつ表示します。

- アプリケーションを確認していくには、リストの下にある矢印をクリックします。
- アプリケーションの特性に関するサマリー情報と参照できるインターネットの検索リンクが示されているポップアップ ウィンドウを表示するには、アプリケーションの横にある情報アイコン（  ）をクリックします。

一致するアプリケーションの検索

照合するアプリケーションを見つけやすくするために、[Available Applications] リストを次のように制約できます。

- アプリケーションを検索するには、リスト上部にある [Search by name] プロンプトをクリックし、名前を入力します。入力していくと、リストが更新されて一致するアプリケーションが表示されます。
- フィルタを適用してアプリケーションを制約するには、[Application Filters] リストを使用します（アプリケーション フィルタと暗号化トラフィックの照合（276ページ）を参照）。フィルタを適用すると、[Available Applications] リストが更新されます。

制約されると、[All apps matching the filter] オプションが [Available Applications] リストの上部に表示されます。このオプションを使用して、制約されたリスト内のすべてのアプリケーションを [Selected Applications and Filters] リストにすべて一度に追加できます。

（注） [アプリケーション フィルタ（Application Filters）] リストで 1 つ以上のフィルタを選択し、さらに [使用可能なアプリケーション（Available Applications）] リストも検索すると、選択内容と検索フィルタ適用後の [使用可能なアプリケーション（Available Applications）] リストが AND 演算を使用して結合されます。つまり [All apps matching the filter] 条件には、[Available Applications] リストに現在表示されている個々のすべての条件と、[Available Applications] リストの上で入力された検索文字列が含まれます。

条件内で照合する単一アプリケーションの選択

照合するアプリケーションを検索したら、それをクリックして選択します。複数のアプリケーションを選択するには、Shift キーまたは Ctrl キーを使用します。表示されているすべてのアプリケーションを選択するには、右クリックして [Select All] を選択します。

1 つのアプリケーション条件において、アプリケーションの個別選択で追加できる最大数は 50 です。50 を超えるアプリケーションを追加するには、複数の SSL ルールを作成するか、フィルタを使用してアプリケーションをグループ化する必要があります。

条件のフィルタに一致するすべてのアプリケーションの選択

[Application Filters] リストで検索またはフィルタを使用して制約されると、[All apps matching the filter] オプションが [Available Applications] リストの上部に表示されます。

このオプションを使用すると、制限した [Available Applications] リストに表示されているすべてのアプリケーションをまとめて [Selected Applications and Filters] リストに追加できます。アプリケーションを個別に追加するのとは異なり、このアプリケーションのセットは、含まれているアプリケーションの数にかかわらず 1 項目としてカウントされます。このため、結果的に 50 を超える数のアプリケーションを条件に追加できます。

この方法でアプリケーション条件を作成すると、[Selected Applications and Filters] リストに追加したフィルタに「フィルタ タイプ + 各タイプの最大 3 フィルタの名前」形式の名前が付きます。同じタイプのフィルタが 3 個を超える場合は、その後に省略記号（...）が表示されます。たとえば次のフィルタ名には、Risks タイプの 2 つのフィルタと Business Relevance タイプの 4 つのフィルタが含まれています。

```
Risks: Medium, High Business Relevance: Low, Medium, High,...
```

[All apps matching the filter] で追加するフィルタに表されないフィルタ タイプは、追加するフィルタの名前に含まれません。[Selected Applications and Filters] リスト内のフィルタ名の上にポインタを置いたときに表示される説明テキストは、それらのフィルタ タイプが [any] に設定されていることを示します。つまり、それらのフィルタ タイプはフィルタを制約しないため、任意の値が許可されます。

[All apps matching the filter] の複数のインスタンスをアプリケーション条件に追加でき、各インスタンスは [Selected Applications and Filters] リストで個別の項目としてカウントされます。たとえば、リスクが高いすべてのアプリケーションを 1 つの項目として追加し、選択内容をクリアしてから、ビジネスとの関連性が低いすべてのアプリケーションを別の項目として追加でき

ます。このアプリケーション条件は、リスクが高いアプリケーションまたはビジネスとの関連性が低いアプリケーションに一致します。

SSL ルールにアプリケーション条件を追加する

ライセンス：Control

アプリケーション条件を設定した SSL ルールと暗号化トラフィックを一致させるには、[Selected Applications and Filters] リストに追加したいずれかのアプリケーションまたはフィルタにトラフィックが一致する必要があります。

1 つの条件に最大 50 の項目を追加することができ、条件に追加したフィルタが個別に追加したアプリケーションの上に一覧表示されます。無効なアプリケーション条件が検出されると、警告アイコンが表示されます。アイコンの上にポインタを置くと詳細が表示されます。

アプリケーション条件に基づいて暗号化トラフィックを制御するには、次の手順を実行します。

ステップ 1 アプリケーションに応じたトラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成 （242 ページ）を参照してください。

ステップ 2 SSL ルール エディタで、[Applications] タブを選択します。

[Applications] タブが表示されます。

ステップ 3 オプションで、フィルタを使用して [Available Applications] リストに表示されるアプリケーションのリストを制約します。

[Application Filters] リストで 1 つ以上のフィルタを選択します。詳細については、アプリケーション フィルタと暗号化トラフィックの照合 （276 ページ）を参照してください。

ステップ 4 [Available Applications] リストから追加するアプリケーションを見つけて選択します。

個々のアプリケーションを検索して選択したり、リストの表示を制限した場合は [All apps matching the filter] をクリックしてすべてを選択したりできます。詳細については、個々のアプリケーションからのトラフィックの照合 （277 ページ）を参照してください。

ステップ 5 [Add to Rule] をクリックして、選択したアプリケーションを [Selected Applications and Filters] リストに追加します。

選択したアプリケーションとフィルタをドラッグアンドドロップすることもできます。フィルタは [Filters] という見出しの下に表示され、アプリケーションは [Applications] という見出しの下に表示されます。

ヒント このアプリケーション条件に別のフィルタを追加する場合は、[Clear All Filters] をクリックして既存の選択をクリアしておきます。

ステップ 6 ルールを保存するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（設定変更の導入 （92 ページ）を参照してください）。

暗号化されたアプリケーションの制御に関する制限事項

ライセンス：Control

アプリケーション制御を実行する場合は、次の点に注意してください。

暗号化されたアプリケーションの識別

ASA FirePOWER モジュールは、StartTLS を使用して暗号化される、暗号化されていないアプリケーションを識別できます。これには、SMTPS、POPS、FTPS、TelnetS、IMAPS などのアプリケーションが含まれます。また、サーバ証明書サブジェクトの識別名の値または TLS クライアントの hello メッセージの Server Name Indication に基づいて、特定の暗号化アプリケーションを識別します。

アプリケーション識別の速さ

ASA FirePOWER モジュールは、以下の内容が完了するまで暗号化トラフィックのアプリケーション制御を実行できません。

- 暗号化された接続がクライアントとサーバ間で確立される。
- 暗号化セッション内のアプリケーションがモジュールにより識別される

この識別が行われるのは、サーバ証明書が交換された後です。ハンドシェイク中に交換されるトラフィックでアプリケーションの識別が完了する前に、アプリケーション条件を含んでいる SSL ルール内の他のすべての条件に一致してしまうと、SSL ポリシーによりそのパケットの通過が許可されます。このため、アプリケーションを識別できるように接続が確立されます。便宜を図るため、影響を受けるルールは情報アイコン（）でマークされます。

モジュールによる識別が完了すると、アプリケーション条件に一致する残りのセッション トラフィックに SSL ルールのアクションが適用されます。

URL カテゴリおよびレピュテーションによる暗号化トラフィックの制御

ライセンス：URL Filtering

SSL ルールの URL 条件では、ネットワーク上のユーザからアクセス可能な暗号化 Web サイト トラフィックの処理と復号を行います。要求された URL は、SSL ハンドシェイク時に提供される情報に基づいて検出されます。URL Filtering ライセンスを使用して、URL の一般的な分類、またはカテゴリ、およびリスク レベル、またはレピュテーションに基づいて、Web サイトへのアクセスを制御することができます。

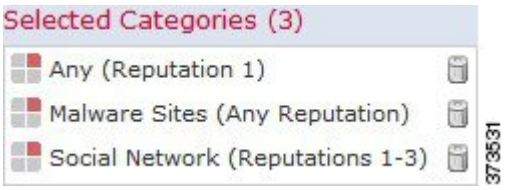
（注） 特定の URL に対するトラフィックの処理と復号化は、識別名の SSL ルール条件を定義することで行えます。証明書のサブジェクト識別名にある共通名属性には、サイトの URL が含まれています。詳細については、証明書の識別名による暗号化トラフィックの制御 （284 ページ）を参照してください。

カテゴリとレピュテーションに基づく暗号化 URL のブロック

ライセンス：URL Filtering

URL フィルタリングライセンスでは、要求された URL のカテゴリとレピュテーションに基づいて、Web サイトへのユーザのアクセスを制御できます。暗号化された接続を使用する URL をブロックするには、SSL ルールでカテゴリルールを使用します。URL フィルタリング機能の詳細については、URL カテゴリとレピュテーションに基づく URL のブロッキング （147 ページ）を参照してください。

次の図に、すべてのマルウェアサイト、すべての信頼できないサイト、レピュテーションレベルが [Neutral] 以下のすべてのソーシャル ネットワーキング サイトをブロックする SSL ルールの URL の条件をします。



次の表では、上記の条件をどのように設定するかを示しています。レピュテーションでリテラル URL または URL オブジェクトを制限できないことに注意してください。

表 *42 :* 例：*URL* 条件の作成

ブロックする対象	選択するカテゴリまたは URL オブジェクト	選択するレピュテーション
マルウェア サイト（レピュテーションに関係なく）	https://www.talosintelligence.com/categories の [Threat] タブに表示されるすべての脅威カテゴリ。	いずれか（Any） [Apply to unknown reputation] も選択します。
信頼できない URL（レベル 1）	いずれか（Any）	1：[信頼できない（Untrusted）] 必要に応じて、[不明なレピュテーションに適用（Apply to unknown reputation）] をオンにします。

ブロックする対象	選択するカテゴリまたは URL オブジェクト	選択するレピュテーション
レピュテーションレベルが [Neutral] よりも低いソーシャル ネットワーキング サイト（レベル 1 ～ 3）	Social Network	3：[ニュートラル（Newtral）]

無効な URL 条件が検出されると、警告アイコンが表示されます。詳細については、アイコンの上にポインタを置き、アクセス コントロール ポリシーとルールのトラブルシューティング（92 ページ） を参照してください。

ヒント トラフィックを復号化してからアクセス コントロールでブロックする場合、ユーザは警告ページをクリックして閉じることでブロックをバイパスできます。詳細については、「インタラクティブ ブロッキング アクション：ユーザが Web サイト ブロックをバイパスすることを許可する（121 ページ）」を参照してください。

カテゴリ データおよびレピュテーション データを使用した要求された URL によるトラフィックの制御

ステップ 1 URL に応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（242 ページ）を参照してください。

ステップ 2 SSL ルール エディタで、[Categories] タブを選択します。

ステップ 3 [Categories] リストで、追加する URL カテゴリを選択します。カテゴリを指定せずにすべての暗号化 Web トラフィックと一致させるには、[Any] カテゴリを選択します。

追加可能なカテゴリを検索するには、[Categories] リストの上にある [Search by name or value] プロンプトをクリックし、カテゴリ名を入力します。入力を開始するとリストが更新され、一致するカテゴリが表示されます。

カテゴリを選択するには、そのカテゴリをクリックします。複数のカテゴリを選択するには、Shift キーおよび Ctrl キーを使用します。

ヒント 右クリックして、すべてのカテゴリを選択することもできますが、すべてのカテゴリを追加すると、1 つのアクセス コントロール ルールに対する項目の最大値 50 を超えます。代わりに [Any] を使用してください。

ルールの目的がマルウェアからの保護である場合は、https://www.talosintelligence.com/categoriesの説明に従ってすべての脅威カテゴリを選択してください。

カテゴリのページが複数存在する場合があります。カテゴリリストの下にある矢印をクリックして、すべてのページにアクセスできることを確認します。

ステップ 4 オプションで、[レピュテーション（Reputations）] リストからレピュテーション レベルをクリックして、カテゴリの選択内容を制限します。レピュテーションレベルを指定しなかった場合、モジュールはデフォルトで [Any]（レピュテーションが未知のサイトを含むすべてのレベル）に設定します。

選択できるレピュテーション レベルは 1 つだけです。レピュテーションのレベルを選択すると、SSL ルールはその目的に応じて異なる動作をします。

- ルールで Web アクセスのブロックまたはトラフィックの復号化を行う場合（ルール アクションが、**Block**、**Block with reset**、**Decrypt - Known Key**、**Decrypt - Resign**、または **Monitor**の場合）、選択したレピュテーション レベルよりも厳しいすべてのレピュテーションも自動的に選択されます。たとえば、[Questionable] サイト（レベル 2）をブロックするルールを設定した場合は、**[Untrusted]**（レベル 1）のサイトも自動的にブロックします。
- ルールで Web アクセスを許可して、アクセス コントロールに従わせる場合（ルール アクションが **Do not decrypt** の場合）、選択したレピュテーション レベルよりも厳しくないすべてのレピュテーションも自動的に選択されます。たとえば、[Favorable] サイト（レベル 4）を許可するルールを設定した場合、**[Trusted]**（レベル 5）サイトも自動的に許可されます。

ルールに対するルールアクションを変更すると、モジュールは上記の点に従ってカテゴリの条件のレピュテーションレベルを自動的に変更します。

必要に応じて、[不明なレピュテーションに適用（Apply to unknown reputation）] をオンにします。

ステップ 5 [ルールに追加（Add to Rule）] をクリックして、選択した項目を [選択したカテゴリ（Selected Categories）] リストに追加します。

選択した項目をドラッグ アンド ドロップでリストに追加することもできます。

ステップ 6 ルールを保存するか、編集を続けます。

次のタスク

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（設定変更の導入 （92 ページ）を参照してください）。

URL 検出とブロッキングの制約事項

ライセンス：URL Filtering

URL の検出とブロッキングを実行する際は、次の点に注意してください。

URL 識別の速度

モジュールによる URL のカテゴリ分類は、以下のことが行われるまで実行されません。

- モニタしている接続がクライアントとサーバ間で確立される。
- セッション内の HTTPS アプリケーションがモジュールにより識別される
- 要求された URL をモジュールがクライアントの hello メッセージまたはサーバ証明書に基づいて識別する

この識別が行われるのは、サーバ証明書が交換された後です。ハンドシェイク中に交換されるトラフィックで URL 識別が完了する前に、URL 条件を含んでいる SSL ルール内の他のすべての条件に一致してしまうと、SSL ポリシーによりそのパケットの通過が許可されます。このため、URL を識別できるように接続が確立されます。便宜を図るため、影響を受けるルールは情報アイコン（）でマークされます。

モジュールによる識別が完了すると、URL 条件に一致する残りのセッション トラフィックに SSL ルールのアクションが適用されます。

URL での検索クエリ パラメータ

モジュールでは、URL 条件の照合に URL 内の検索クエリ パラメータを使用しません。たとえば、すべてのショッピング トラフィックをブロックする場合を考えます。amazon.com を探すために Web 検索を使用してもブロックされませんが、amazon.com を閲覧しようとするとブロックされます。

サーバ証明書の特性に基づいたトラフィック制御

ライセンス：任意

サーバ証明書の特性に基づいて暗号化トラフックの処理および復号化を行う SSL ルールを作成できます。セッションの暗号化に使用されている暗号スイートまたはプロトコルバージョンを検出して、それに応じてトラフィックを処理できます。また、サーバ証明書を検出して、以下のサーバ証明書の特性に基づいてトラフィックを処理することもできます。

- サーバ証明書自体。
- 証明書の発行元。証明書が CA で発行されているか、自己署名されているか。
- 証明書のホルダー。
- 証明書ステータス。証明書が有効であるか、発行元の CA により無効にされているかなど。

複数の暗号スイートを 1 つのルールで検出したり、証明書の発行元や証明書ホルダーを検出する場合は、再利用可能な暗号スイートのリストおよび識別名オブジェクトを作成してルールに追加できます。サーバ証明書および特定の証明書ステータスを検出するには、ルール用の外部証明書と外部 CA オブジェクトの作成が必要です。

証明書の識別名による暗号化トラフィックの制御

ライセンス：任意

SSL ルールで識別名条件を設定すると、証明書ホルダーまたはサーバ証明書を発行した CA に応じて暗号化トラフィックを処理および検査できます。発行元の識別名を基準にすると、サイトのサーバ証明書を発行した CA に基づいてトラフィックを処理できます。サブジェクトの識別名には Web サイトの URL が含まれているので、特定の URL を送信元または宛先とする暗号化トラフィックの処理もできます。

ルール条件を設定する場合は、手動でリテラル値を指定するか、識別名オブジェクトを参照するか、または複数のオブジェクトを含んでいる識別名グループを参照できます。

（注） **Decrypt - Known Key** アクションを選択した場合、識別名条件を設定することはできません。このアクションでは、トラフィック復号化用のサーバ証明書の選択が必要であり、トラフィックの照合はすでにこの証明書で行われることになります。詳細については、「復号化アクション：さらに検査するためにトラフィックを復号化 （253 ページ）」を参照してください。

複数のサブジェクトおよび発行元の識別名との一致を単一の証明書ステータスのルール条件で行うことも可能ですが、ルールとの照合で一致する必要があるのは1つの共通名または識別名だけです。

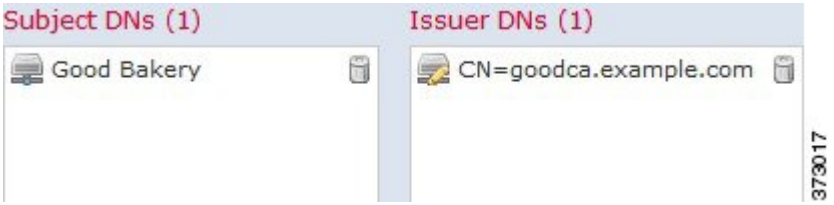
識別名を手動で追加する場合、共通名属性（**CN**）を含めることができます。「CN=」なしで共通名を追加すると、オブジェクトの保存時に「CN=」が追加されます。

さらに、次の表にリストされている、コンマで区切られた属性を含む識別名を追加することもできます。

表 *43* : 識別名の属性

属性	説明	使用可能な値
C	国番号	2 つの英字
CN	共通名	最大 64 個の英数字、バックスラッシュ（\）、ハイフン（-）、引用符（"）、アスタリスク（*）、ピリオド（.）、またはスペース文字
O	組織	
OU	組織単位	

次の図は、goodbakery.example.com に対して発行された証明書および goodca.example.com によって発行された証明書を検索する識別名ルール条件を示しています。これらの証明書で暗号化されたトラフィックは許可され、アクセス コントロールにより制御されます。



次の図は、badbakery.example.com および関連ドメインに対して発行された証明書および badca.example.com によって発行された証明書を検索する識別名ルール条件を示しています。こ

れらの証明書で暗号化されたトラフィックは、再署名された証明書を使用して復号されます。

1 つの識別名条件で、[Subject DNs] リストおよび [Issuer DNs] リストにそれぞれ最大 50 のリテラル値および識別名オブジェクトを追加できます。

ASA FirePOWER モジュール提供の識別名オブジェクト グループである Sourcefire Undecryptable Sites には、モジュールで復号化できないトラフィックの Web サイトが含まれています。このグループを識別名条件に追加すると、該当する Web サイトとのトラフィックがブロックしたり復号化を無効にしたりでき、これらのトラフィックの復号化に使用されるシステム リソースの浪費を回避できます。グループ内の各エントリは変更できますが、このグループを削除することはできません。システムによる更新によりこのリストのエントリが変更されることがありますが、モジュールではユーザによる変更が保持されます。

システムが新しいサーバへの暗号化セッションを最初に検出したときは、DN データを ClientHello の処理には使用できません。これは復号化されていない最初のセッションとなる可能性があります。最初のセッション後に、管理対象デバイスは、サーバの証明書メッセージからのデータをキャッシュします。同じクライアントからの後続の接続で、システムは識別名条件を含むルールに ClientHello メッセージを最終的に一致させ、メッセージを処理して、復号化の可能性を最大化できます。

証明書のサブジェクトまたは発行元の識別名に基づいて暗号化トラフィックを検査するには、次の手順を実行します。

ステップ 1 証明書のサブジェクトまたは発行元の識別名に応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成 （242 ページ）を参照してください。

ステップ 2 SSL ルール エディタで、[DN] タブを選択します。

[DN] タブが表示されます。

ステップ 3 [Available DNs] で、追加する識別名を選択します。

- 識別名オブジェクトをその場で追加するには（後で条件に追加可能）、[Available DNs] リストの上にある追加アイコンをクリックします。識別名オブジェクトの操作 （66 ページ）を参照してください。
- 追加する識別名オブジェクトおよびグループを検索するには、[Available DNs] リストの上にある [Search by name or value] プロンプトをクリックし、オブジェクトの名前またはオブジェクトの値を入力します。入力を開始するとリストが更新され、一致するオブジェクトが表示されます。

オブジェクトを選択するには、そのオブジェクトをクリックします。複数のオブジェクトを選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [Select All] を選択します。

ステップ 4 次の選択肢があります。

- [Add to Subject] をクリックして、選択したオブジェクトを [Subject DNs] リストに追加します。
- [Add to Issuer] をクリックして、選択したオブジェクトを [Issuer DNs] リストに追加します。

選択したオブジェクトをドラッグ アンド ドロップでリストに追加することもできます。

ステップ 5 手動で指定するリテラル共通名または識別名がある場合は、それらを追加します。

[Subject DNs] または [Issuer DNs] リストの下にある [Enter DN or CN] プロンプトをクリックし、共通名または識別名を入力して [Add] をクリックします。

ステップ 6 ルールを追加するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（設定変更の導入 （92 ページ）を参照してください）。

証明書による暗号化トラフィックの制御

ライセンス：任意

SSL ルールで証明書条件を設定すると、トラフィックの暗号化に使用されているサーバ証明書に応じて暗号化トラフィックを処理および検査できます。1 つの条件に 1 つまたは複数の証明書を設定でき、トラフィックの証明書がいずれかの条件の証明書と一致するとそのルールが適用されます。

証明書ベースの SSL ルール条件を作成する場合、サーバ証明書をアップロードしたり、証明書を再利用可能な外部証明書オブジェクトとして保存して、名前をサーバ証明書と関連付けたりできます。また、既存の外部証明書オブジェクトやオブジェクト グループを使用して証明書条件を設定することもできます。

ルール条件の [Available Certificates] フィールドでは、外部証明書オブジェクトやオブジェクト グループを証明書の識別名に関する以下の特性に基づいて検索できます。

- サブジェクトまたは発行元の共通名（CN）
- サブジェクトまたは発行元の組織（O）
- サブジェクトまたは発行元の組織単位（OU）

1 つの証明書のルール条件で複数の証明書に一致させることもでき、トラフィックの暗号化に使用されている証明書がアップロードされた証明書のいずれかと一致した場合、その暗号化トラフィックはルールに一致したと判定されます。

1 つの証明書条件で、[Selected Certificates] リストに最大 50 の外部証明書オブジェクトおよび外部証明書オブジェクト グループを追加できます。

次の点に注意してください。

- **Decrypt - Known Key** アクションを選択した場合、証明書条件を設定することはできません。このアクションでは、トラフィック復号化用のサーバ証明書の選択が必要であり、トラフィックの照合はすでにこの証明書で行われることになります。詳細については、「復号化アクション：さらに検査するためにトラフィックを復号化（253 ページ）」を参照してください。
- 証明書条件に外部証明書オブジェクトを設定する場合、暗号スイート条件に追加する暗号スイートまたは **Decrypt - Resign** アクションに関連付ける内部 CA オブジェクトのいずれかが、外部証明書の署名アルゴリズム タイプと一致する必要があります。たとえば、ルールの証明書条件で EC ベースのサーバ証明書を参照する場合は、追加する暗号スイート、または [Decrypt - Resign] アクションに関連付ける CA 証明書も EC ベースでなければなりません。署名アルゴリズム タイプの不一致が検出されると、ポリシー エディタでルールの横に警告アイコンが表示されます。詳細については、暗号スイートによる暗号化トラフィックの制御（294 ページ）および復号化アクション：さらに検査するためにトラフィックを復号化（253 ページ）を参照してください。
- システムが新しいサーバへの暗号化セッションを最初に検出したときは、証明書データを ClientHello の処理には使用できません。これは復号化されていない最初のセッションとなる可能性があります。最初のセッション後に、管理対象デバイスは、サーバの証明書メッセージからのデータをキャッシュします。同じクライアントからの後続の接続で、システムは証明書条件を含むルールに ClientHello メッセージを最終的に一致させ、メッセージを処理して、復号化の可能性を最大化できます。

サーバ証明書に基づいて暗号化トラフィックを検査するには、次の手順を実行します。

ステップ 1 サーバ証明書に応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成（242 ページ）を参照してください。

ステップ 2 SSL ルール エディタで、[Certificate] タブを選択します。

[Certificate] タブが表示されます。

ステップ 3 [Available Certificates] で、追加するサーバ証明書を選択します。

- ここで外部証明書オブジェクトを作成してリストに追加するには、[Available Certificates] リストの上にある追加アイコン（）をクリックし、識別名オブジェクトの操作（66 ページ）の手順に従います。
- 追加する証明書オブジェクトおよびグループを検索するには、[Available Certificates] リストの上にある [Search by name or value] プロンプトをクリックし、オブジェクトの名前またはオブジェクトの値を入力します。入力を開始するとリストが更新され、一致するオブジェクトが表示されます。

オブジェクトを選択するには、そのオブジェクトをクリックします。複数のオブジェクトを選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [Select All] を選択します。

ステップ 4 [Add to Rule] をクリックして、選択したオブジェクトを [Subject Certificates] リストに追加します。

選択したオブジェクトをドラッグ アンド ドロップでリストに追加することもできます。

ステップ 5 ルールを追加するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（設定変更の導入 （92 ページ）を参照してください）。

証明書ステータスによる暗号化トラフィックの制御

ライセンス：任意

SSL ルールで証明書ステータス条件を設定すると、トラフィックの暗号化に使用されているサーバ証明書のステータス（有効、失効済み、有効期限切れ、未有効化、自己署名、信頼できる CA によって署名済みなど）に応じて暗号化トラフィックを処理および検査できます。

CA が証明書を発行したか失効したかを確認するには、ルートおよび中間 CA 証明書とその CRL をオブジェクトとしてアップロードする必要があります。その後で SSL ポリシーの信頼できる CA 証明書のリストに、これらの信頼できる CA のオブジェクトを追加します。

証明書ステータスの SSL ルール条件では、各ステータスの有無を基準にしたトラフィックの照合ができます。1 つのルール条件で複数のステータスを選択でき、いずれかのステータスと証明書が一致すれば、ルールとトラフィックが一致したと判定されます。

外部認証局の信頼

ライセンス：任意

SSL ポリシーでルートおよび中間 CA 証明書を追加することで信頼できる CA が設定され、トラフィックの暗号化に使用されているサーバ証明書の検証に、これらの信頼できる CA を使用できるようになります。検証されたサーバ証明書には、信頼できる CA によって署名された証明書が含まれます。

信頼できる CA 証明書の中にアップロードされた証明書失効リスト（CRL）が含まれている場合は、信頼できる CA により暗号化証明書が失効されているかどうかも確認できます。詳細については、「信頼できる CA オブジェクトへの証明書失効リストの追加 （74 ページ）」を参照してください。

SSL ポリシーに信頼できる CA 証明書を追加した後は、トラフィックと一致させるさまざまな証明書ステータス条件を SSL ルールに設定することができます。詳細については、信頼できる認証局オブジェクトの操作 （73 ページ）および証明書ステータスによる暗号化トラフィックの制御 （289 ページ）を参照してください。

ヒント 信頼できるルート CA の信頼チェーン内にあるすべての証明書を、信頼できる CA 証明書のリストにアップロードしますが、これにはルート CA 証明書およびすべての中間 CA 証明書が含まれます。これを行わないと、中間 CA から発行された信頼できる証明書の検出が困難になります。

SSL ポリシーを作成すると、ASA FirePOWER モジュールにより、[Trusted CA Certificates] タブにデフォルトの信頼できる CA オブジェクト グループ「Cisco Trusted Authorities」が入力されます。このグループ内の各エントリは変更が可能で、SSL ポリシーにこのグループを含めるかどうかを選択できます。このグループを削除することはできません。システムによる更新によりこのリストのエントリが変更されることがありますが、ユーザによる変更は保持されます。詳細については、「基本 SSL ポリシーの作成 （224 ページ）」を参照してください。

ポリシーに信頼できる CA を追加するには、次の手順を実行します。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [SSL] の順に選択します。 > >

[SSL Policy] ページが表示されます。

ステップ 2 設定する SSL ポリシーの横にある編集アイコン（）をクリックします。

SSL ポリシー エディタが表示されます。

ステップ 3 [Trusted CA Certificates] タブを選択します。

[Trusted CA Certificates] ページが表示されます。

ステップ 4 [Available Trusted CAs] で,追加する信頼できる CA を選択します。

- その場で信頼できる CA オブジェクト（後で条件に追加可能）を作成するには、[Available Trusted CAs] リストの上にある追加アイコン（）をクリックします。信頼できる認証局オブジェクトの操作 （73 ページ）を参照してください。
- 追加する信頼できる CA オブジェクトおよびグループを検索するには、[Available Trusted CAs] リストの上にある [Search by name or value] プロンプトをクリックし、オブジェクトの名前またはオブジェクトの値を入力します。入力を開始するとリストが更新され、一致するオブジェクトが表示されます。

オブジェクトを選択するには、そのオブジェクトをクリックします。複数のオブジェクトを選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [Select All] を選択します。

ステップ 5 [Add to Rule] をクリックして、選択したオブジェクトを [Selected Trusted CAs] リストに追加します。

選択したオブジェクトをドラッグ アンド ドロップでリストに追加することもできます。

ステップ 6 ルールを追加するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（信頼できる認証局オブジェクトの操作 （73 ページ）を参照してください）。

証明書ステータスでのトラフィックの照合

ライセンス：任意

証明書ステータスベースのルール条件を設定すると、トラフィックの暗号化に使用されているサーバ証明書のステータスに基づいて暗号化トラフィックを照合できます。次の作業を実行できます。

- サーバ証明書のステータスをチェックする。
- 証明書にステータスがないことをチェックする。
- 証明書ステータスの有無のチェックをスキップする。

複数の証明書ステータスの有無との一致を単一の証明書ステータスのルール条件で選択することも可能ですが、ルールとの照合で証明書が一致する必要があるのは 1 つの基準だけです。

次の表は、暗号化用のサーバ証明書のステータスに基づいて、ASA FirePOWER モジュールが暗号化トラフィックを評価する方法を示しています。

表 *44*：証明書ステータスのルール条件の基準

ステータスチェック	Yes を設定	No を設定
Revoked	ポリシーは、サーバ証明書を発行した CA を信頼しており、ポリシーにアップロードされた CA 証明書にはそのサーバ証明書を失効させる CRL が含まれています。	ポリシーは、サーバ証明書を発行した CA を信頼しており、ポリシーにアップロードされた CA 証明書にはこのサーバ証明書を失効させる CRL が含まれていません。
Self-signed	検出されたサーバ証明書が、同じサブジェクトと発行元の識別名を含んでいます。	検出されたサーバ証明書が、異なるサブジェクトと発行元の識別名を含んでいます。
Valid	以下のすべてを満たしています。 • 証明書を発行した CA をポリシーが信頼しています。 • 署名が有効です。 • 発行元が有効です。 • ポリシーの信頼できる CA のいずれも証明書を失効させていません。 • 現在の日付が証明書の有効期限の開始日と終了日の範囲内にあります。	以下の 1 つ以上を満たしています。 • 証明書を発行した CA をポリシーが信頼していません。 • 署名が無効です。 • 発行元が無効です。 • ポリシーの信頼できる CA の 1 つが証明書を失効させています。 • 現在の日付が証明書の有効期限の開始日より前です。 • 現在の日付が証明書の有効期限の終了日より後です。
Invalid signature	証明書の内容に対して証明書の署名が適切に検証されません。	証明書の内容に対して証明書の署名が適切に検証されます。
Invalid issuer	発行元の CA 証明書が、ポリシーの信頼できる CA 証明書のリストに登録されていません。	発行元の CA 証明書が、ポリシーの信頼できる CA 証明書のリストに登録されています。

ステータス チェック	Yes を設定	No を設定
Expired	現在の日付が証明書の有効期限の終了日より後です。	現在の日付が証明書の有効期限の終了日であるかそれより前です。
Not yet valid	現在の日付が証明書の有効期限の開始日より前です。	現在の日付が証明書の有効期限の開始日であるかそれより後です。

次の例について考えてみます。組織は Verified Authority という認証局を信頼しています。組織は Spammer Authority という認証局を信頼していません。システム管理者は、Verified Authority の証明書、および Verified Authority の発行した中間 CA 証明書をモジュールにアップロードします。Verified Authority が以前に発行した証明書の 1 つを失効させたため、システム管理者は Verified Authority から配布された CRL をアップロードします。

次の図は、有効な証明書をチェックする証明書ステータスのルール条件を示しています。これにより、Verified Authority から発行されたが CRL には登録されておらず、現状で有効期限の開始日と終了日の範囲内にあるかどうかがチェックされます。この設定では、これらの証明書で暗号化されたトラフィックはアクセス コントロールにより復号化および検査されません。

次の図は、ステータスの不在をチェックする証明書ステータスのルール条件を示しています。この設定では、期限切れになっていない証明書を使用して暗号化されたトラフィックに一致し、そのトラフィックをモニタします。

次の図は、さまざまなステータスの有無に一致する証明書ステータスのルール条件を示しています。この設定でルールが一致するのは、着信トラフィックを暗号化した証明書が無効なユー

ザが発行元、自己署名、無効、または期限切れであった場合で、そうしたトラフィックを既知のキーで復号します。

1 つの証明書が複数のステータスに一致する場合でも、ルールがトラフィックに行うアクションは一度に 1 つだけであることに注意してください。

（注） システムが新しいサーバへの暗号化セッションを最初に検出したときは、証明書ステータスを ClientHello の処理には使用できません。これは復号化されていない最初のセッションとなる可能性があります。最初のセッション後に、管理対象デバイスは、サーバの証明書メッセージからのデータをキャッシュします。同じクライアントからの後続の接続で、システムは証明書ステータス条件を含むルールに ClientHello メッセージを最終的に一致させ、メッセージを処理して、復号化の可能性を最大化できます。

サーバ証明書のステータスで暗号化トラフィックを検査するには、次の手順を実行します。

ステップ 1 サーバ証明書のステータスに応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成 （242 ページ）を参照してください。

ステップ 2 SSL ルール エディタで、[Cert Status] タブを選択します。

[Cert Status] タブが表示されます。

ステップ 3 各証明書ステータスには次のオプションがあります。

- 該当する証明書ステータスが存在するときに一致させる場合は [Yes] を選択します。
- 該当する証明書ステータスが存在しないときに一致させる場合は [No] を選択します。
- 該当する証明書ステータスと照合させない場合は [Do Not Match] を選択します。

ステップ 4 ルールを追加するか、編集を続けます。

変更を反映させるには、SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります。設定変更の導入 （92 ページ）を参照してください。

暗号スイートによる暗号化トラフィックの制御

ライセンス：任意

SSL ルールで暗号スイート条件を設定すると、暗号化セッションのネゴシエートに使用される暗号スイートに応じて暗号化トラフィックを処理および検査できます。Cisco では、暗号スイートのルール条件に追加できる事前定義の暗号スイートを提供しています。複数の暗号スイートを含む、暗号スイートのリストのオブジェクトを追加することもできます。暗号スイートのリストの詳細については、地理位置情報オブジェクトの操作（77 ページ）を参照してください。

（注） 新しい暗号スイートを追加することはできません。定義済みの暗号スイートは変更も削除もできません。

1 つの暗号スイート条件で、[Selected Cipher Suites] リスト最大 50 の暗号スイートおよび暗号スイート リストを追加できます。

次の点に注意してください。

- 展開でサポートされていない暗号スイートを追加した場合、その SSL ポリシーに関連付けられたアクセス コントロール ポリシーを適用することはできません。たとえば、パッシブ展開では、一時 Diffie-Hellman（DHE）および一時的楕円曲線 Diffie-Hellman（ECDHE）暗号スイートを使用したトラフィックの復号がサポートされません。これらの暗号スイートでルールを作成した場合、アクセス コントロール ポリシーは適用できません。
- 暗号スイート条件に暗号スイートを設定する場合、証明書条件に追加する外部証明書オブジェクトまたは **Decrypt - Resign** アクションに関連付ける内部 CA オブジェクトのいずれかが、暗号スイートの署名アルゴリズム タイプと一致する必要があります。たとえば、ルールの暗号スイート条件で EC ベースの暗号スイートを参照する場合、追加するサーバ証明書または **[Decrypt - Resign]** アクションに関連付ける CA 証明書も EC ベースである必要があります。署名アルゴリズム タイプの不一致が検出されると、ポリシー エディタでルールの横に警告アイコンが表示されます。詳細については、暗号スイートによる暗号化トラフィックの制御（294 ページ）および復号化アクション：さらに検査するためにトラフィックを復号化（253 ページ）を参照してください。
- SSL ルールの暗号スイート条件に匿名の暗号スイートを追加できますが、次の点に注意してください。
  - システムは ClientHello 処理中に自動的に匿名の暗号スイートを削除します。ルールを使用するシステムでは、ClientHello の処理を防止するために SSL ルールを設定する必要があります。詳細については、SSL ルールの順序指定によるパフォーマンス向上とプリエンプション回避（259 ページ）を参照してください。
  - システムでは、匿名の暗号スイートで暗号化されたトラフィックは復号化できないため、ルールに **Decrypt - Resign** または **Decrypt - Known Key** アクションを使用できません。

- 暗号スイーをルール条件として指定する際、ルールをClientHelloメッセージで指定された暗号スイートの完全なリストではなく、ServerHelloメッセージのネゴシエートされた暗号スイートと照合することを検討してください。ClientHelloの処理中に、管理対象デバイスはClientHelloメッセージからサポートされていない暗号スイートを削除します。ただし、これにより指定されたすべての暗号スイートが削除されることになる場合、システムでは元のリストを保持します。システムがサポートされていない暗号スイートを保持する場合、後続の評価は復号化されないセッションになります。

暗号化トラフィックを暗号スイートで検査するには、次の手順を実行します。

ステップ 1 暗号スイートに応じた暗号化トラフィック制御を設定するSSLポリシーで、新しいSSLルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成 （242 ページ）を参照してください。

ステップ 2 SSL ルール エディタで、[Cipher Suite] タブを選択します。

[Cipher Suite] タブが表示されます。

ステップ 3 [Available Cipher Suites] で、追加する暗号スイートを選択します。

- その場で暗号スイート リスト（後で条件に追加可能）を追加するには、[Available Cipher Suites] リストの上にある追加アイコンをクリックします。地理位置情報オブジェクトの操作 （77 ページ）を参照してください。
- 追加する暗号スイートおよびリストを検索するには、[Available Cipher Suites] リストの上にある [Search by name or value] プロンプトをクリックし、暗号スイートの名前または暗号スイートの値を入力します。入力を開始するとリストが更新され、一致する暗号スイートが表示されます。

暗号スイートをクリックして選択します。複数の暗号スイートを選択するには、Shift キーおよび Ctrl キーを使用するか、または右クリックして [Select All] を選択します。

ステップ 4 [Add to Rule] をクリックして、選択した暗号スイートを [Selected Cipher Suites] リストに追加します。

選択した暗号スイートをドラッグ アンド ドロップでリストに追加することもできます。

ステップ 5 ルールを追加するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（設定変更の導入 （92 ページ）を参照してください）。

暗号化プロトコルのバージョンによるトラフィックの制御

ライセンス：任意

SSLルールでセッション条件を設定すると、トラフィックの暗号化に使用されているSSLまたはTLSのバージョンに応じて暗号化トラフィックを検査できます。SSL バージョン 3.0 または TLS バージョン 1.0、1.1、1.2 のいずれかで暗号化されたトラフィックとの照合を選択できま

す。デフォルトでは、ルールの作成時にすべてのプロトコルのバージョンが選択されます。複数のバージョンが選択されている場合、いずれかのバージョンと一致する暗号化トラフィックがルールに一致したと判定されます。ルール条件を保存するには、最低1つのプロトコルバージョンを選択する必要があります。

（注） バージョンのルール条件で SSL バージョン 2.0 を選択することはできません。これは、ASA FirePOWER モジュールが SSL バージョン 2.0 で暗号化されたトラフィックの復号化をサポートしていないためです。復号化できないアクションを設定すれば、それ以上のインスペクションなしで、これらのトラフィックを許可またはブロックできます。詳細については、SSL ルールを使用した復号可能接続のロギング （483 ページ）を参照してください。

暗号化トラフィックを SSL または TLS のバージョンで検査するには、次の手順を実行します。

ステップ 1 暗号化プロトコルのバージョンに応じた暗号化トラフィック制御を設定する SSL ポリシーで、新しい SSL ルールを作成するか既存のルールを編集します。

詳細な手順については、SSL ルールの概要と作成 （242 ページ）を参照してください。

ステップ 2 SSL ルール エディタで、[Version] タブを選択します。

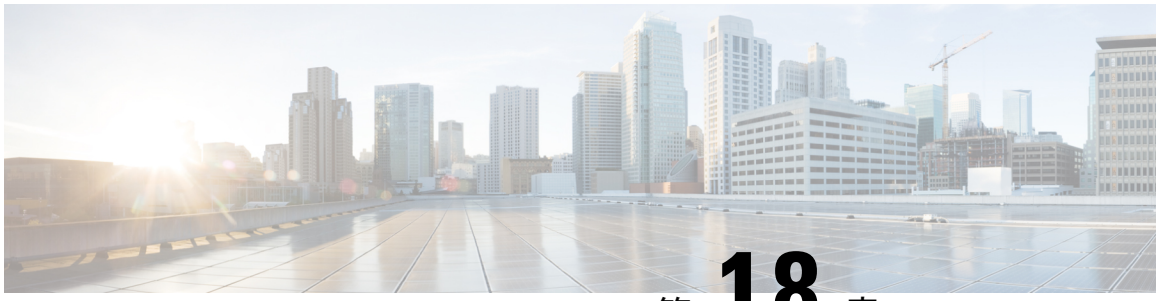
[Version] タブが表示されます。

ステップ 3 照合するプロトコル バージョンを選択します。**SSL v3.0**、**TLS v1.0**、**TLS v1.1**、または **TLS v1.2** を選択できます。

ステップ 4 ルールを追加するか、編集を続けます。

変更を反映させるには、その SSL ポリシーに関連付けたアクセス コントロール ポリシーを適用する必要があります（設定変更の導入 （92 ページ）を参照してください）。

次のタスク



第 18 章

ネットワーク分析ポリシーと侵入ポリシーについて

ネットワーク分析ポリシーと侵入ポリシーは、ASA FirePOWER モジュールの侵入検知および防御機能の一部として連携して動作します。侵入検知という用語は、一般に、ネットワーク トラフィックへの侵入の可能性を受動的に分析し、セキュリティ分析用に攻撃データを保存するプロセスを指します。侵入防御という用語には、侵入検知の概念が含まれますが、ネットワークを通過する悪意のあるトラフィックをブロックまたは変更する機能も加味されます。

ネットワーク分析ポリシーと侵入ポリシーについて

ASA FirePOWER モジュールは、ネットワーク分析ポリシーと侵入ポリシーを使用して侵入検知と防御機能を処理します。

侵入防御展開では、システムがパケットを検査するときに、以下が実行されます。

- ネットワーク分析ポリシーは、トラフィックのデコードと前処理の方法を管理し、特に、侵入を試みている兆候がある異常なトラフィックについて、さらに評価できるようにします。
- 侵入ポリシーでは侵入およびプリプロセッサ ルール（総称して「侵入ポリシー ルール」とも呼ばれる）を使用し、パターンに基づき、デコードされたパケットを検査して攻撃の可能性を調べます。侵入ポリシーは変数セットとペアになっているため、名前付き値を使用してネットワーク環境を正確に反映できます。

ネットワーク分析ポリシーと侵入ポリシーは、どちらも親のアクセス コントロール ポリシーによって呼び出されますが、呼び出されるタイミングが異なります。システムでトラフィック

ネットワーク分析ポリシーと侵入ポリシーについて

が分析される際には、侵入防御（追加の前処理と侵入ルール）フェーズよりも前に、別にネットワーク分析（デコードと前処理）フェーズが実行されます。ネットワーク分析ポリシーと侵入ポリシーを一緒に使用すると、広範囲で詳細なパケットインスペクションを行うことができます。これらのポリシーは、ホストとそのデータの可用性、整合性、機密性を脅かす可能性のあるネットワーク トラフィックの検知、アラート、防御に役立ちます。

ASA FirePOWER モジュールには、同様の名前（Balanced Security and Connectivity など）が付いた複数のネットワーク分析ポリシーと侵入ポリシーが付属しており、それらのポリシーは相互に補完して連携します。システムによって提供されるポリシーを使用することで、シスコ脆弱性調査チーム（VRT）の経験を活用できます。これらのポリシーでは、VRT は侵入ルールおよびプリプロセッサルールの状態を設定し、プリプロセッサおよび他の詳細設定の初期設定も提供します。

また、カスタムのネットワーク分析ポリシーや侵入ポリシーも作成できます。カスタム ポリシー内の設定は、ユーザにとって最も意味のある方法でトラフィックを検査するように調整できます。

同様のポリシーエディタを使用し、ネットワーク分析ポリシーや侵入ポリシーを作成、編集、保存、管理します。いずれかのタイプのポリシーを編集するときには、ユーザインターフェイスの左側にナビゲーションパネルが表示され、右側にさまざまな設定ページが表示されます。

この章では、ネットワーク分析ポリシーおよび侵入ポリシーによって管理される各種設定の概要、ポリシーが連携してトラフィックを検査し、ポリシー違反のレコードを生成するしくみ、および、ポリシーエディタの基本的な操作方法について説明します。また、カスタムポリシーとシステム付属ポリシーを比較して、それらの使用上の利点と制約についても説明します。侵入防御展開をカスタマイズするには、以下の該当する手順を参照してください。

- 変数セットの操作 （38 ページ） には、ネットワーク環境を正確に反映させるためのシステムの侵入変数の設定方法が記載されています。カスタム ポリシーを使用しない場合でも、デフォルトの変数セットのデフォルト変数を変更することを強く推奨します。上級ユーザはカスタム変数セットを作成して、1 つ以上のカスタム侵入ポリシーと組合わせることができます。

- 侵入ポリシーについて （341 ページ） では、単純なカスタム侵入ポリシーを作成および編集する方法について説明します。

- 侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御 （171 ページ） には、親アクセス コントロール ポリシーに侵入ポリシーを関連付け、侵入ポリシーを使用して目的のトラフィックのみを検査するためのシステムの設定方法が記載されています。また、侵入ポリシーの高度なパフォーマンス オプションの設定方法も記載されています。

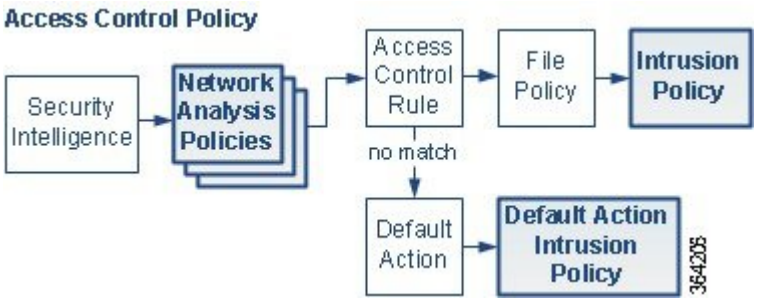
- ネットワーク分析ポリシーまたは侵入ポリシー レイヤでのレイヤの使用 （317 ページ） では、大規模な組織や複雑な展開環境で、ポリシー階層と呼ばれる構成要素を使用して、複数のネットワーク分析ポリシーや侵入ポリシーをより効率的に管理する方法が説明されています。

ポリシーが侵入の有無についてトラフィックをどのように検査するかについて

ライセンス：Protection

システムがアクセス コントロール展開の一部としてトラフィックを分析する際には、侵入防御（侵入ルールと詳細設定）フェーズよりも前に、別にネットワーク分析（デコードと前処理）フェーズが実行されます。

次の図は、インラインの侵入防御および高度なマルウェア防御（AMP）展開におけるトラフィック分析の順序を簡略的に示しています。アクセス コントロール ポリシーが他のポリシーを呼び出してトラフィックを検査するしくみ、およびそれらのポリシーが呼び出される順序を示しています。ネットワーク分析ポリシーと侵入ポリシーの選択フェーズは強調表示されています。



同様に、プロセスの各ステップで、パケットによってシステムがイベントを生成する場合があります。侵入およびプリプロセッサイベント（総称して「侵入イベント」と呼ばれることもある）は、パケットまたはそのコンテンツがセキュリティ リスクを含んでいる可能性を示しています。

単一の接続の場合は、図に示すように、アクセス コントロール ルールよりも前にネットワーク分析ポリシーが選択されますが、いくつかの前処理（特にアプリケーション層の前処理）はアクセス コントロール ルールの選択後に実行されます。これは、カスタム ネットワーク分析ポリシーでの前処理の設定方法に**影響しません**。

復号化、正規化、前処理：ネットワーク分析ポリシー

ライセンス：Protection

デコードと前処理を実行しないと、プロトコルの相違によってパターンマッチングを行えなくなるので、侵入についてシステムでトラフィックを適切に評価できなくなります。ポリシーが侵入の有無についてトラフィックをどのように検査するかについて（299ページ）の図に示すように、ネットワーク分析ポリシーは、次のように、これらのトラフィック処理タスクを制御します。

- 暗号化トラフィックがセキュリティ インテリジェンスによってフィルタリングされた後

- ファイルまたは侵入ポリシーによってトラフィックを検査できるようになる前

ネットワーク分析ポリシーは、フェーズでのパケット処理を制御します。最初に、システムは最初の3つのTCP/IP層を通ったパケットを復号化し、次にプロトコル異常の正規化、前処理、および検出に進みます。

- パケット デコーダは、パケット ヘッダーとペイロードを、プリプロセッサや以降の侵入ルールで簡単に使用できる形式に変換します。TCP/IP スタックの各レイヤのデコードは、データリンク層から開始され、ネットワーク層、トランスポート層へと順番に行われます。パケット デコーダは、パケット ヘッダーからさまざまな異常動作を検出します。
- インライン展開では、インライン正規化プリプロセッサは、攻撃者が検出を免れる可能性を最小限にするために、トラフィックを再フォーマット（正規化）します。その他のプリプロセッサや侵入ルールによる検査に向けてパケットを準備し、システムで処理されるパケットがネットワーク上のホストで受信されるパケットと同じものになるようにします。
- ネットワーク層とトランスポート層のさまざまなプリプロセッサは、IPフラグメントを悪用する攻撃を検出したり、チェックサム検証を実行したり、TCP および UDP セッションの前処理を実行したりします。

トランスポートおよびネットワーク プリプロセッサの一部の詳細設定は、アクセス コントロール ポリシーで処理されるすべてのトラフィックにグローバルに適用されます。これらの詳細設定は、ネットワーク分析ポリシーではなくアクセス コントロール ポリシーで設定します。

- 各種のアプリケーション層プロトコル デコーダは、特定タイプのパケット データを侵入ルール エンジンで分析可能な形式に正規化します。アプリケーション層プロトコルのエンコードを正規化することにより、システムはデータ表現が異なるパケットに同じコンテンツ関連の侵入ルールを効果的に適用し、大きな結果を得ることができます。詳細については、
- Modbus と DNP3 のプリプロセッサは、トラフィックの異常を検出し、データを侵入ルールに提供します。Supervisory Control and Data Acquisition（SCADA）プロトコルは、製造、水処理、配電、空港、輸送システムなどの工業プロセス、インフラストラクチャ プロセス、および設備プロセスからのデータをモニタ、制御、取得します。
- 一部のプリプロセッサでは、Back Orifice、ポートスキャン、SYN フラッドおよび他のレート ベース攻撃など、特定の脅威を検出できます。

侵入ポリシーで、ASCIIテキストのクレジット カード番号や社会保障番号などの機密データを検出する機密データ プリプロセッサを設定することに注意してください。

新たに作成されたアクセス コントロール ポリシーでは、1 つのデフォルト ネットワーク分析ポリシーが、同じ親アクセス コントロール ポリシーによって呼び出されるすべての侵入ポリシー向けのすべてのトラフィックについて、前処理を制御します。最初に、デフォルトでは Balanced Security and Connectivity ネットワーク分析ポリシーが使用されますが、別のシステム付属ポリシーやカスタム ネットワーク分析ポリシーに変更できます。より複雑な展開では、上級ユーザは、一致したトラフィックの前処理にさまざまなカスタム ネットワーク分析ポリシーを割り当てることによって、特定のセキュリティ ゾーンおよびネットワークに合わせてトラ

フィックの前処理オプションを調整できます。詳細については、システムによって提供されるポリシーとカスタム ポリシーの比較 （305 ページ）を参照してください。

表 *45*：復号化されたパケット

TCP/IP 層	復号化されたパケット
データ リンク	• イーサネット • 仮想ローカル エリア ネットワーク（VLAN） • マルチプロトコル ラベル スイッチング（MPLS）
ネットワーク	• Encapsulated Remote Switched Port Analyzer（ERSPAN）タイプ II、タイプ III • インターネット プロトコル バージョン 4（IPv4） • インターネット プロトコル バージョン 6（IPv6） • Internet Control Message Protocol バージョン 4（ICMPv4） • Internet Control Message Protocol バージョン 6（ICMPv6） • Point-to-Point Protocol (PPP) • Point-to-Point Protocol over Ethernet（PPPoE） • Generic Routing Encapsulation (GRE) • カプセル化セキュリティ プロトコル（ESP） • Teredo トンネリング • GPRS Tunneling Protocol（GTP）
トランスポート	• 伝送制御プロトコル（TCP） • ユーザ データグラム プロトコル（UDP）

アクセス コントロール ルール：侵入ポリシーの選択

ライセンス：Protection

最初の前処理の後、トラフィックはアクセス コントロール ルール（設定されている場合）によって評価されます。ほとんどの場合、パケットが一致した最初のアクセスコントロールルールがそのトラフィックを処理することになります。ユーザは一致したトラフィックをモニタ、信頼、ブロック、または許可することができます。

アクセス コントロール ルールでトラフィックを許可すると、マルウェア、禁止ファイル、侵入について、この順序でトラフィックを検査できます。アクセス コントロール ルールに一致

しないトラフィックは、アクセス コントロール ポリシーのデフォルト アクションによって処理されます。デフォルト アクションでは、侵入についても検査できます。

（注） どのネットワーク分析ポリシーによって前処理されるかに関わらず、すべてのパケットは、設定されているアクセス コントロール ルールと上から順に照合されます（したがって、侵入ポリシーによる検査の対象となります）。詳細については、カスタム ポリシーの制限（310 ページ）を参照してください。

ポリシーが侵入の有無についてトラフィックをどのように検査するかについて（299 ページ）の図は、インラインの侵入防御およびAMP展開でデバイスを通過する、次のようなトラフィックのフローを示しています。

- アクセス コントロール ルールによって、一致したトラフィックを続行できます。次にトラフィックは、ファイル ポリシーによって禁止ファイルとマルウェアについて検査され、侵入ポリシーによって侵入について検査されます。
- このシナリオでは、アクセス コントロール ポリシーのデフォルト アクションは一致したトラフィックを許可します。次にトラフィックは侵入ポリシーによって検査されます。アクセス コントロール ルールまたはデフォルト アクションに侵入ポリシーを関連付けるときに、必要に応じて、別の侵入ポリシーを使用できます。

ブロックされたトラフィックや信頼済みトラフィックは検査されないので、図の例には、ブロック ルールや信頼ルールは含まれていません。詳細については、ルール アクションを使用したトラフィック処理とインスペクションの決定（119 ページ）およびデフォルトの処理の設定およびネットワーク トラフィックのインスペクション（83 ページ）を参照してください。

侵入インスペクション：侵入ポリシー、ルール、変数セット

ライセンス：Protection

トラフィックが宛先に向かうことを許可する前に、システムの最終防御ラインとして侵入防御を使用できます。侵入ポリシーは、セキュリティ違反に関するトラフィックの検査方法を制御し、インライン展開では、悪意のあるトラフィックをブロックまたは変更することができます。侵入ポリシーの主な機能は、有効にする侵入ルールとプリプロセッサ ルールの選択および設定方法を管理することです。

侵入ルールとプリプロセッサ ルール

侵入ルールはキーワードと引数のセットとして指定され、ネットワーク上の脆弱性を悪用する試みを検出します。システムは侵入ルールを使用してネットワーク トラフィックを分析し、トラフィックがルールの条件に合致しているかどうかをチェックします。システムが各ルール内で指定された条件とパケットを照らし合わせます。そして、パケット データとルール内で指定されたすべての条件が一致した場合に、ルールがトリガーとして使用されます。

システムには、VRT により作成された次のようなタイプのルールが含まれています。

- 共有オブジェクト侵入ルール：コンパイルされているため変更できません（送信元と宛先のポートや IP アドレスなどのルール ヘッダー情報を除く）。
- 標準テキスト侵入ルール：ルールの新しいカスタムインスタンスとして保存および変更できます。
- プリプロセッサ ルール：これは、ネットワーク分析ポリシーのプリプロセッサおよびパケット デコーダの検出オプションに関連付けられるルールです。プリプロセッサ ルールはコピーまたは編集できません。ほとんどのプリプロセッサルールはデフォルトで無効になっています。プリプロセッサを使用してイベントを生成したり、インライ展開で違反パケットをドロップするには、これらのルールを有効にする必要があります。

システムで侵入ポリシーに従ってパケットを処理するとき、最初にルール オプティマイザが、基準（トランスポート層、アプリケーション プロトコル、保護されたネットワークへの入出力方向など）に基づいて、サブセット内のすべてのアクティブなルールを分類します。次に、侵入ルール エンジンが、各パケットに適用する適切なルールのサブセットを選択します。最後に、マルチルール検索エンジンが 3 種類の検索を実行して、トラフィックがルールに一致するかどうかを検査します。

- プロトコル フィールド検索は、アプリケーション プロトコル内の特定のフィールドでの一致を検索します。
- 汎用コンテンツ検索は、パケット ペイロードの ASCII またはバイナリ バイトでの一致を検索します。
- パケット異常検索では、特定のコンテンツが含まれているかどうかではなく、確立されたプロトコルに違反しているパケット ヘッダーやペイロードが検索されます。

カスタム侵入ポリシーでは、ルールを有効化および無効化し、独自の標準テキスト ルールを記述および追加することで、検出を調整できます。

変数セット

システムが侵入ポリシーを使用してトラフィックを評価する場合、関連付けられた変数セットが使用されます。大部分の変数は、侵入ルールで一般的に使用される値を表し、送信元および宛先の IP アドレスおよびポートを識別します。侵入ポリシーにある変数を使用して、ルール抑制および動的ルール状態にある IP アドレスを表すこともできます。

システムには、定義済みのデフォルト変数から構成される 1 つのデフォルト変数セットが含まれています。システム提供の共有オブジェクト ルールと標準テキスト ルールは、これらの定義済みのデフォルト変数を使用してネットワークおよびポート番号を定義します。たとえば、ルールの大半は、保護されたネットワークを指定するために変数 $HOME_NET を使用して、保護されていない（つまり外部の）ネットワークを指定するために変数 $EXTERNAL_NET を使用します。さらに、特殊なルールでは、他の定義済みの変数がしばしば使用されます。たとえば、Web サーバに対するエクスプロイトを検出するルールは、$HTTP_SERVERS 変数および $HTTP_PORTS 変数を使用します。

ヒント　システム提供の侵入ポリシーを使用する場合でも、デフォルトセットの主要なデフォルト変数を変更することを強く推奨します。ネットワーク環境を正確に反映する変数を使用すると、処理が最適化され、システムによって疑わしいアクティビティに関連するシステムをモニタできます。上級ユーザはカスタム変数セットを作成して、1 つ以上のカスタム侵入ポリシーと組合わせることができます。詳細については、事前定義されたデフォルト変数の最適化 （39 ページ）を参照してください。

侵入イベントの生成

ライセンス：Protection

システムは侵入の可能性を特定すると、侵入イベントまたはプリプロセッサイベント（総称して「侵入イベント」とも呼ばれる）を生成します。このデータを表示して、ネットワーク アセットに対する攻撃についてさらに理解することができます。インライン展開では、システムは、有害であると判明しているパケットをドロップまたは置き換えることがきます。

各侵入イベントにはイベント ヘッダーがあり、イベント名と分類、送信元と宛先の IP アドレス、ポート、イベントを生成したプロセス、およびイベントの日時に関する情報が含まれています。パケット ベースのイベントの場合、システムは復号化されたパケット ヘッダーとイベントをトリガーしたパケット（複数の場合あり）のペイロードのコピーもログに記録します。

パケット デコーダ、プリプロセッサ、および侵入ルール エンジンはすべて、システムによるイベントの生成を引き起こします。次に例を示します。

- （ネットワーク分析ポリシーで設定された）パケット デコーダが 20 バイト（オプションやペイロードのない IP データグラムのサイズ）未満の IP パケットを受け取った場合、デコーダはこれを異常なトラフィックと解釈します。以降、パケットを検査する侵入ポリシーで付随するデコーダ ルールが有効な場合は、システムによってプリプロセッサ イベントが生成されます。
- IP 最適化プリプロセッサが重複する一連の IP フラグメントを検出した場合、プリプロセッサはこれを潜在的な攻撃と解釈し、付随するプリプロセッサ ルールが有効な場合はシステムによってプリプロセッサ イベントが生成されます。
- 侵入ルール エンジン内では、ほとんどの標準テキスト ルールおよび共有オブジェクト ルールはパケットによってトリガーされた場合に侵入イベントを生成するように記述されます。

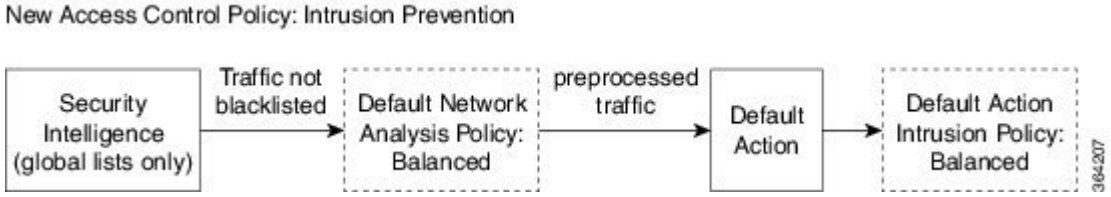
デバイスに侵入イベントが蓄積されると、ユーザは攻撃の可能性について分析を開始できます。システムは、ユーザが侵入イベントを確認し、ネットワーク環境とセキュリティ ポリシーのコンテキストでそのイベントが重要であるかどうかを評価するために必要なツールを提供します。

システムによって提供されるポリシーとカスタム ポリシーの比較

ライセンス：Protection

ASA FirePOWER モジュールを使用してトラフィック フローを管理する最初のステップの 1 つは、新しいアクセス コントロール ポリシーの作成です。デフォルトでは、新たに作成されたアクセス コントロール ポリシーは、システム付属のネットワーク分析ポリシーと侵入ポリシーを呼び出してトラフィックを検査します。

次の図は、インラインの侵入防御展開で、新たに作成されたアクセス コントロール ポリシーが最初にトラフィックを処理するしくみを示しています。前処理および侵入防御のフェーズが強調表示されています。



以下の点に注意してください。

- デフォルトのネットワーク分析ポリシーによって、アクセス コントロール ポリシーで処理されるすべてのトラフィックの前処理が制御されます。最初は、システム付属の *Balanced Security and Connectivity* ネットワーク分析ポリシーがデフォルトになります。
- アクセス コントロール ポリシーのデフォルト アクションは、システムによって提供される Balanced Security and Connectivity 侵入ポリシーによって判定された悪意のないすべてのトラフィックを許可します。
- ポリシーはデフォルトのセキュリティ インテリジェンス オプション（グローバルブロックなしリストとブロックリストのみ）を使用し、SSL ポリシーによる暗号化トラフィックの復号化や、アクセス制御ルールによるネットワーク トラフィックの特別な処理やインスペクションを実行しません。

侵入防御展開を調整するために実行できる簡単な手順は、システム付属のネットワーク分析ポリシーと侵入ポリシーの別のセットをデフォルトとして使用することです。シスコでは ASA FirePOWER モジュールで、これらのポリシーのペアを複数提供しています。

または、カスタム ポリシーを作成して使用することで、侵入防御展開を調整できます。それらのポリシーに設定されたプリプロセッサ オプション、侵入ルール、およびその他の詳細設定が、ネットワークのセキュリティ ニーズに適合しない場合があります。設定できるネットワーク分析ポリシーおよび侵入ポリシーを調整することにより、システムがネットワーク上のトラフィックを処理して侵入の有無について検査する方法を非常にきめ細かく設定できます。

システムによって提供されるポリシーについて

ライセンス：Protection

シスコでは ASA FirePOWER モジュールで、ネットワーク分析ポリシーと侵入ポリシーのペアを複数提供しています。システムによって提供されるネットワーク分析ポリシーと侵入ポリシーを使用することで、シスコ脆弱性調査チーム（VRT）の経験を活用できます。これらのポリシーに対して、VRT は侵入およびプリプロセッサ ルールの状態を設定し、プリプロセッサと他の詳細設定の初期設定も行います。システムによって提供されるポリシーをそのまま使用するか、またはカスタム ポリシーのベースとして使用できます。

ヒント システム付属のネットワーク分析ポリシーと侵入ポリシーを使用する場合でも、ネットワーク環境を正確に反映するように、システムの侵入変数を設定する必要があります。少なくとも、デフォルトセットの主要なデフォルト変数を変更してください（事前定義されたデフォルト変数の最適化 （39 ページ）を参照）。

新たな脆弱性が発見されると、VRT は侵入ルールのアップデートをリリースします。これらのルールアップデートにより、システム付属のネットワーク分析ポリシーや侵入ポリシーが変更され、侵入ルールとプリプロセッサ ルールの新規作成または更新、既存ルールの状態の変更、およびデフォルトのポリシー設定の変更が実施されます。ルールアップデートでは、システム付属のポリシーからルールが削除されたり、新しいルール カテゴリが提供されたり、さらにデフォルトの変数セットが変更されることもあります。

ルールの更新によって展開が影響を受けると、システムは影響を受けた侵入ポリシーやネットワーク分析ポリシー、およびそれらの親のアクセス コントロール ポリシーを失効とマークします。変更を有効にするには、更新されたポリシーを再適用する必要があります。

便宜を図るために、影響を受けた侵入ポリシーを単独でまたは影響を受けたアクセス コントロール ポリシーと組み合わせて、自動的に再適用するように、ルール アップデートを設定できます。これにより、展開を自動的に最新な状態に保ち、新たに検出されたエクスプロイトや侵入から保護することができます。

前処理の設定を確実に最新の状態にするには、アクセス コントロール ポリシーを再適用する必要があります。これにより、現在実行されているものとは異なる関連する SSL ポリシー、ネットワーク分析ポリシー、ファイル ポリシーが再適用され、高度な前処理とパフォーマンス オプションのデフォルト値も更新できます。詳細については、「ルール更新とローカル ルール ファイルのインポート （582 ページ）」を参照してください。

シスコでは ASA FirePOWER モジュールで、次のネットワーク分析ポリシーと侵入ポリシーを提供しています。

[バランスのとれたセキュリティと接続性（Balanced Security and Connectivity）] ネットワーク分析ポリシーおよび侵入ポリシー

これらのポリシーは、速度と検出の両方を目的として作成されています。一緒に使用すると、ほとんどの組織にとって最適な出発点となります。ほとんどの場合、システムは Balanced Security and Connectivity のポリシーおよび設定をデフォルトとして使用します。

Connectivity Over Security ネットワーク分析ポリシーおよび侵入ポリシー

これらのポリシーは、接続（すべてのリソースに到達可能な）の方がネットワークインフラストラクチャのセキュリティより優先される組織向けに作られています。この侵入ポリシーは、Security over Connectivity ポリシー内で有効になっているルールよりもはるかに少ないルールを有効にします。トラフィックをブロックする最も重要なルールだけが有効にされます。

[接続性よりもセキュリティを優先（Security over Connectivity）] ネットワーク分析ポリシーおよび侵入ポリシー

これらのポリシーは、ネットワークインフラストラクチャのセキュリティがユーザの利便性より優先される組織向けに作られています。この侵入ポリシーは、正規のトラフィックにアラートを発したり、それらのトラフィックをドロップする可能性のある膨大な数のネットワーク異常侵入ルールを有効にします。

No Rules Active 侵入ポリシー

No Rules Active 侵入ポリシーでは、すべての侵入ルールと詳細設定が無効化されます。このポリシーは、他のシステム付属ポリシーのいずれかで有効になっているルールに基づくのではなく、独自のポリシーを作成する場合の出発点となります。

注意 シスコでは、試験用に別のポリシー Experimental Policy 1 を使用しています。シスコの担当者から指示された場合を除き、このポリシーは使用しないでください。

カスタム ポリシーの利点

ライセンス：Protection

システム付属のネットワーク分析ポリシーと侵入ポリシーに設定されているプリプロセッサオプション、侵入ルール、およびその他の詳細設定が、組織のネットワークのセキュリティニーズに完全に合致しない場合があります。

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

すべてのカスタムポリシーには基本ポリシー（別名「基本レイヤ」）があり、それによって、ポリシー内のすべてのコンフィギュレーションのデフォルト設定が定義されます。レイヤは、複数のネットワーク分析ポリシーや侵入ポリシーを効率的に管理するために使用できる基本構成要素です（ネットワーク分析ポリシーまたは侵入ポリシー レイヤでのレイヤの使用 （317 ページ）を参照）。

ほとんどの場合、カスタムポリシーはシステム付属のポリシーに基づきますが、別のカスタムポリシーを使用することもできます。ただし、すべてのカスタム ポリシーには、ポリシーチェーンの最終的なベースとしてシステム付属ポリシーが含まれています。システム付属のポ

リシーはルールアップデートによって変更される可能性があるので、カスタムポリシーを基本として使用している場合でも、ルールアップデートをインポートするとポリシーに影響が及びます。ルール更新によってポリシーが影響を受けると、モジュールインターフェイスでは影響を受けたポリシーが失効とマークされます。詳細については、ルールアップデートによるシステム付属基本ポリシーの変更を許可する （320 ページ）を参照してください。

カスタム ネットワーク分析ポリシーの利点

ライセンス：Protection

デフォルトでは、1つのネットワーク分析ポリシーによって、アクセス コントロール ポリシーで処理されるすべての暗号化されていないトラフィックが前処理されます。これは、侵入ポリシー（および侵入ルールセット）に関係なく、すべてのパケットが同じ設定に基づいてデコードされ、処理されることを意味します。

初期段階では、システムによって提供される Balanced Security and Connectivity ネットワーク分析ポリシーがデフォルトです。前処理を調整する簡単な方法は、デフォルトとしてカスタム ネットワーク分析ポリシーを作成して使用することです。

使用可能な調整オプションはプリプロセッサによって異なりますが、プリプロセッサおよびデコーダを調整できる方法には次のものがあります。

- モニタしているトラフィックに適用されないプリプロセッサを無効にします。たとえば、HTTP Inspect プリプロセッサは HTTP トラフィックを正規化します。ネットワークに Microsoft インターネット インフォメーション サービス（IIS）を使用する Web サーバが含まれていないことが確実な場合は、IIS 特有のトラフィックを検出するプリプロセッサ オプションを無効にすることで、システム処理のオーバーヘッドを軽減できます。

（注） カスタム ネットワーク分析ポリシーではプリプロセッサが無効に設定されているものの、後にパケットを有効化されている侵入ルールまたはプリプロセッサ ルールと照合して評価するためにプリプロセッサを使用する必要がある場合、システムは、自動的にプリプロセッサを有効化して使用します。ただし、ネットワーク分析ポリシーのユーザインターフェイスでは、プリプロセッサは無効のままになります。

- 必要に応じて、特定のプリプロセッサのアクティビティを集中させるポートを指定します。たとえば、DNS サーバの応答や暗号化 SSL セッションをモニタするための追加ポートを特定したり、Telnet、HTTP、RPC トラフィックを復号化するポートを特定したりできます。

複雑な環境内の上級ユーザの場合は、複数のネットワーク分析ポリシーを作成して、それぞれが異なる方法でトラフィックを処理するように調整できます。次に、システムがこれらのポリシーを使用し、異なるセキュリティ ゾーンまたはネットワークを使用してトラフィックの前処理を制御するように、システムを設定します。

（注） カスタム ネットワーク分析ポリシー（特に複数のネットワーク分析ポリシー）を使用して前処理を調整することは、高度なタスクです。前処理と侵入インスペクションは非常に密接に関連しているため、単一のパケットを検査するネットワーク分析ポリシーと侵入ポリシーが相互補完することを許可する場合は、注意する**必要があります**。詳細については、カスタム ポリシーの制限 （310 ページ）を参照してください。

カスタム侵入ポリシーの利点

ライセンス：Protection

侵入防御を実行するように設定されている、新規に作成されたアクセス コントロール ポリシーでは、デフォルト アクションはすべてのトラフィックを許可しますが、最初にシステム付属の Balanced Security and Connectivity 侵入ポリシーでトラフィックをチェックします。アクセス コントロール ルールを追加するか、デフォルト アクションを変更しない限り、すべてのトラフィックがその侵入ポリシーによって検査されます。システムによって提供されるポリシーとカスタム ポリシーの比較 （305 ページ）の図を参照してください。

侵入防御の展開をカスタマイズするために、複数のネットワーク分析ポリシーを作成し、それぞれがトラフィックを異なる方法で処理するように調整できます。次に、どのポリシーがどのトラフィックを検査するかを指定するルールを、アクセス コントロール ポリシーに設定します。アクセス コントロール ルールは単純でも複雑でもかまいません。セキュリティ ゾーン、ネットワークまたは地理的位置、ポート、アプリケーション、要求された URL、またはユーザなど、複数の基準を使用してトラフィックを照合および検査します。ポリシーが侵入の有無についてトラフィックをどのように検査するかについて （299 ページ）のシナリオは、トラフィックが 2 つの侵入ポリシーの一方によって検査される展開を示しています。

侵入ポリシーの主な機能は、次のように、どの侵入ルールおよびプリプロセッサ ルールを有効にしてどのように設定するかを管理することです。

- 各侵入ポリシーで、環境に適用されるすべてのルールが有効であることを確認し、環境に適用されないルールを無効化することによって、パフォーマンスを向上させます。インライン展開では、どのルールによって悪質なパケットをドロップまたは変更するかを指定できます。詳細については、ルール状態の設定 （377 ページ）を参照してください。
- 必要に応じて、既存のルールの変更や、新しい標準テキスト ルールの作成により、新たなエクスプロイトの検出やセキュリティ ポリシーの適用が可能です。

侵入ポリシーに対して行えるその他のカスタマイズは次のとおりです。

- 機密データ プリプロセッサは、ASCII テキストのクレジット カード番号や社会保障番号などの機密データを検出します。特定の脅威（Back Orifice 攻撃、何種類かのポートスキャン、および過剰なトラフィックによってネットワークを過負荷状態に陥らせようとするレート ベース攻撃）を検出するプリプロセッサは、ネットワーク分析ポリシーで設定します。
- グローバルしきい値を設定すると、侵入ルールに一致するトラフィックが、指定期間内に特定のアドレスまたはアドレス範囲で送受信される回数に基づいて、イベントが生成され

ます。これにより、大量のイベントによってシステムに過剰な負荷がかかることを回避できます。詳細については、侵入イベントの記録の制限（395ページ）を参照してください。

- また、個々のルールまたは侵入ポリシー全体に対して、侵入イベント通知を抑制し、しきい値を設定することで、大量のイベントによってシステムに過剰な負荷がかかることを回避することもできます。詳細については、ポリシー単位の侵入イベント通知のフィルタ処理（380 ページ）を参照してください。
- 侵入イベントに加えて、syslogファシリティへのロギングを有効にしたり、イベントデータを SNMP トラップ サーバに送信したりできます。ポリシーごとに、侵入イベントの通知限度を指定したり、外部ロギング ファシリティに対する侵入イベントの通知をセットアップしたり、侵入イベントへの外部応答を設定したりできます。詳細については、侵入ルールに関する外部アラートの設定（511 ページ）を参照してください。

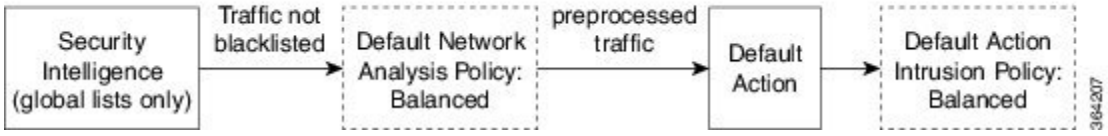
カスタム ポリシーの制限

ライセンス：Protection

前処理と侵入インスペクションは非常に密接に関連しているため、単一のパケットを処理および検査する、ネットワーク分析ポリシーと侵入ポリシーが相互補完することを設定で許可する場合は、注意する**必要があります**。

デフォルトでは、システムは1つのネットワーク分析ポリシーを使用してすべてのトラフィックを前処理します。次の図は、インラインの侵入防御展開で、新たに作成されたアクセス コントロール ポリシーが最初にトラフィックを処理するしくみを示しています。前処理および侵入防御のフェーズが強調表示されています。

New Access Control Policy: Intrusion Prevention



デフォルトのネットワーク分析ポリシーがアクセス コントロール ポリシーによって処理されるすべてのトラフィックの前処理を制御する仕組みに注目してください。初期段階では、システムによって提供される Balanced Security and Connectivity ネットワーク分析ポリシーがデフォルトです。

前処理を調整する簡単な方法は、カスタム ネットワーク分析ポリシーを作成し、それをデフォルトとして使用することです（カスタム ネットワーク分析ポリシーの利点（308ページ）の概要を参照）。ただし、カスタム ネットワーク分析ポリシーでプリプロセッサが無効化されているときに、システムが前処理されたパケットを有効な侵入ルールまたはプリプロセッサ ルールと照合して評価する必要がある場合、システムはプリプロセッサを有効にして使用します。この場合、ネットワーク分析ポリシーのユーザインターフェイスではプリプロセッサは無効のままになります。

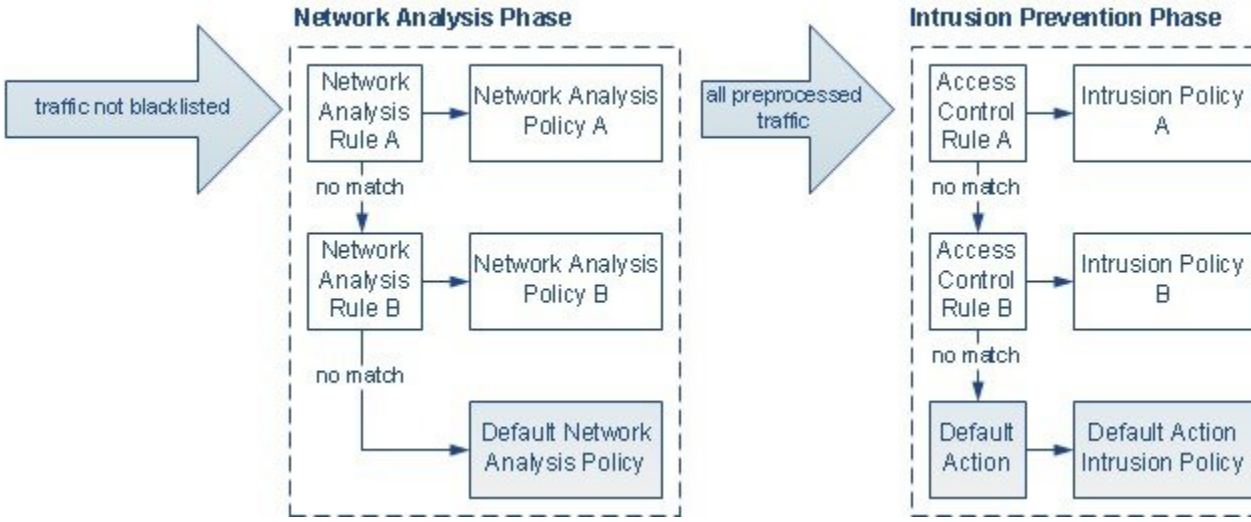
（注） プリプロセッサを無効化してパフォーマンスを向上させるには、どの侵入ポリシーでもプリプロセッサを要求するルールが有効になっていないことを確認する**必要があります**。

複数のカスタム ネットワーク分析ポリシーを使用する場合は、さらに課題があります。複雑な展開内の上級ユーザの場合は、一致したトラフィックの前処理にカスタム ネットワーク分析ポリシーを割り当てることによって、特定のセキュリティ ゾーンおよびネットワークに合わせて前処理を調整できます。これを実現するには、アクセス コントロール ポリシーにカスタム ネットワーク分析ルールを追加します。各ルールには、ルールに一致したトラフィックの前処理を制御するネットワーク分析ポリシーが関連付けられています。

ヒント アクセス コントロール ポリシーの詳細設定としてネットワーク分析ルールを設定します。ASA FirePOWER モジュールの他のタイプのルールとは異なり、ネットワーク分析ルールは、ネットワーク分析ポリシーに含まれているのではなく、ネットワーク分析ポリシーを呼び出します。

システムは、ルール番号の昇順で、設定済みネットワーク分析ルールとパケットを照合します。ネットワーク分析ルールーに一致しなかったトラフィックは、デフォルトのネットワーク分析ポリシーによって前処理されます。これにより非常に柔軟にトラフィックを前処理できます。ただし、留意すべき点として、パケットがどのネットワーク分析ポリシーによって前処理されるかに**関係なく**、すべてのパケットは、アクセス コントロール ルール独自のプロセスで引き続きアクセス コントロール ルールと照合されます（つまり、侵入ポリシーにより検査される可能性があります）。つまり、特定のネットワーク分析ポリシーでパケットを前処理しても、そのパケットが確実に特定の侵入ポリシーで検査されるわけでは**ありません**。適切なネットワーク分析ポリシーと侵入ポリシーを呼び出して特定のパケットを評価するように、注意してアクセス コントロール ポリシーを設定する**必要があります**。

次の図は、侵入防御（ルール）フェーズよりも前に、別にネットワーク分析ポリシー（前処理）の選択フェーズが発生するしくみを詳細に示しています。簡略化するために、図ではファイル/マルウェア インスペクション フェーズが省かれています。また、デフォルトのネットワーク分析ポリシーとデフォルト アクションの侵入ポリシーは強調表示されています。



このシナリオでは、アクセス コントロール ポリシーは、2 つのネットワーク分析ルールとデフォルトのネットワーク分析ポリシーで設定されています。

- ネットワーク分析ルール A は、ネットワーク分析ポリシー A とトラフィックとの照合を前処理します。その後、このトラフィックを侵入ポリシー A によって検査できます。
- ネットワーク分析ルール B は、ネットワーク分析ポリシー B とトラフィックとの照合を前処理します。その後、このトラフィックを侵入ポリシー B によって検査できます。
- 残りのトラフィックはすべて、デフォルトのネットワーク分析ポリシーにより前処理されます。その後、アクセス コントロール ポリシーのデフォルト アクションに関連付けられている侵入ポリシーによってこのトラフィックを検査できます。

システムはトラフィックを前処理した後、侵入についてトラフィックを検査できます。図は、2つのアクセス コントロール ルールとデフォルト アクションが設定されたアクセス コントロール ポリシーを示しています。

- アクセス コントロール ルール A は、一致したトラフィックを許可します。その後、トラフィックは侵入ポリシー A により検査されます。
- アクセス コントロール ルール B は、一致したトラフィックを許可します。その後、トラフィックは侵入ポリシー B により検査されます。
- アクセス コントロール ポリシーのデフォルト アクションは一致したトラフィックを許可します。その後、トラフィックはデフォルトアクションの侵入ポリシーによって検査されます。

各パケットの処理は、ネットワーク分析ポリシーと侵入ポリシーのペアにより制御されますが、このペアはユーザに合わせて調整**されません**。アクセス コントロール ポリシーが誤って設定されているため、ネットワーク分析ルール A とアクセス コントロール ルール A が同じトラフィックを処理しない場合を想定してください。たとえば、特定のセキュリティ ゾーンのトラフィックの処理を制御するポリシー ペアを意図していた場合に、誤って、異なるゾーンを使用するように 2 つのルールの条件を設定したとします。この誤設定により、トラフィックが誤って前処理される可能性があります。このような理由から、ネットワーク分析ルールとカスタム ポリシーを使用して前処理を調整することは、**高度な**タスクです。

単一の接続の場合、アクセス コントロール ルールよりも前にネットワーク分析ポリシーが選択されますが、いくつかの前処理（特にアプリケーション層の前処理）はアクセス コントロール ルールの選択後に実行されます。これは、カスタム ネットワーク分析ポリシーでの前処理の設定方法に**影響しません**。

ナビゲーション パネルの使用方法

ライセンス：Protection

ネットワーク分析ポリシーと侵入ポリシーは、同様のユーザインターフェイスを使用して、設定に対する変更を編集して保存します。を参照してください。侵入ポリシーの編集（345 ページ）

いずれかのタイプのポリシーを編集するときに、ユーザ インターフェイスの左側にナビゲーション パネルが表示されます。次の図は、ネットワーク分析ポリシー（左）と侵入ポリシー（右）のナビゲーション パネルを示しています。

ナビゲーションパネルは境界線によって複数のポリシー設定項目リンクに分割されており、ポリシー層との直接対話により（下側）または直接対話なしで（上側）ポリシー設定項目を設定できます。いずれかの設定ページに移動するには、ナビゲーションパネル内の名前をクリックします。ナビゲーションパネルで影付きで強調表示されている項目は、現在の設定ページを示しています。たとえば、上の図では、[Policy Information] ページがナビゲーション パネルの右側に表示されます。

Policy Information

[Policy Information] ページには、一般的に使用される設定の設定オプションが表示されます。上記のネットワーク分析ポリシーパネルの図に示されているように、ポリシーに未保存の変更がある場合は、ナビゲーション パネルの [Policy Information] の横にポリシー変更アイコンが表示されます。このアイコンは、変更を保存すると表示されなくなります。

Rules（侵入ポリシーのみ）

侵入ポリシーの [Rules] ページでは、共有オブジェクト ルール、標準テキスト ルール、およびプリプロセッサ ルールのルール ステータスとその他の設定項目を設定できます。詳細については、ルールを使用した侵入ポリシーの調整 （355 ページ）を参照してください。

Settings（ネットワーク分析ポリシーのみ）と Advanced Settings（侵入ポリシーのみ）

ネットワーク分析ポリシーの [Settings] ページでは、プリプロセッサとアクセス プリプロセッサの設定ページを有効または無効にすることができます。[Settings] リンクを展開すると、ポリシー内で有効になっているすべてのプリプロセッサを個々に設定する設定ページへのサブリンクが表示されます。

侵入ポリシーの [Advanced Settings] ページでは、詳細設定ページと詳細設定のアクセス設定ページを有効または無効にすることができます。[Advanced Settings] リンクを展開すると、ポリシー内で有効になっているすべての詳細設定を個々に設定する設定ページへのサブリンクが表示されます。詳細については、侵入ポリシーの詳細設定 （348 ページ）を参照してください。

Policy Layers

[Policy Layers] ページには、ネットワーク分析ポリシーまたは侵入ポリシーを構成するレイヤの要約が表示されます。[Policy Layers] リンクを展開すると、ポリシー内のレイヤに関するサマリ ページへのサブリンクが表示されます。各レイヤのサブリンクを展開すると、レイヤで有効になっているすべてのルール、プリプロセッサ、または詳細設定を個々に設定する設定ページへのサブリンクが表示されます。詳細については、ネットワーク分析ポリシーまたは侵入ポリシー レイヤでのレイヤの使用 （317 ページ）を参照してください。

競合の解決とポリシー変更の確定

ライセンス：Protection

ネットワーク分析ポリシーまたは侵入ポリシーを編集する場合、変更をシステムに認識させるには、その変更を保存（またはコミット）する必要があります。

（注） 保存後は、変更を反映させるためにネットワーク分析ポリシーまたは侵入ポリシーを適用する必要があります。保存しないでポリシーを適用すると、最後に保存された設定が使用されます。侵入ポリシーは個別に再適用できますが、ネットワーク分析ポリシーは親アクセス コントロール ポリシーで適用されます。

編集の競合の解決

[Network Analysis Policy] ページおよび [Intrusion Policy] ページには、各ポリシーの未保存の変更の有無が表示されます。侵入ポリシーの編集 （345 ページ）を参照してください。

シスコでは、同時に 1 人だけがポリシーを編集することを推奨します。同一ユーザとして複数のユーザ インターフェイス経由で同じネットワーク分析ポリシーまたは侵入ポリシーを編集し、1 つのインスタンスの変更を保存すると、他のインスタンスの変更を保存できなくなります。

設定の依存関係の解決

特定の分析を実行する場合、多くのプリプロセッサ ルールとセキュリティ ルールでは、最初に特定の方法でトラフィックをデコードまたは前処理するか、他の依存関係を割り当てる必要があります。ネットワーク分析ルールまたは侵入ポリシーを保存すると、システムは必要な設定を自動的に有効にするか、または警告を発して、設定を無効化してもトラフィックに影響がないことを示します。

- SNMP ルール アラートを追加しても、SNMP アラートを設定しなかった場合は、侵入ポリシーを保存できません。SNMP アラートを設定するかルール アラートを無効化してから、再度保存する必要があります。
- 侵入ポリシーに有効なセンシティブ データ ルールが含まれているときに、センシティブ データ プリプロセッサが有効になっていない場合は、侵入ポリシーを保存できません。システムがプリプロセッサを有効化してポリシーを保存することを許可するか、ルールを無効化して再度保存する必要があります。
- ネットワーク分析ポリシーで必要なプリプロセッサを無効化しても、まだポリシーを保存できます。ただし、ネットワーク分析ポリシーのユーザインターフェイスでプリプロセッサは無効になっていても、システムは無効になっているプリプロセッサを自動的に現在の設定で使用します。詳細については、カスタム ポリシーの制限 （310 ページ）を参照してください。
- ネットワーク分析ポリシーでインライン モードを無効にして、インライン正規化プリプロセッサを有効化した場合は、ポリシーを保存できます。ただし、正規化設定が無視されることが警告されます。インライン モードを無効化すると他の設定が無視されるので、プリプロセッサは、チェックサム検証やレート ベース攻撃の防御を含めて、トラフィックを変更またはブロックできます。

ポリシー変更のコミット、破棄、およびキャッシュ

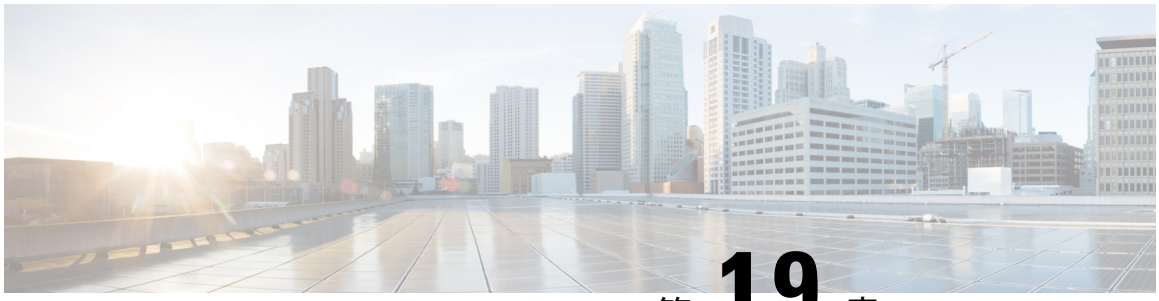
ネットワーク分析ポリシーまたは侵入ポリシーの編集時に、変更を保存しないでポリシー エディタを終了した場合、それらの変更はシステムによってキャッシュされます。変更は、システムからログアウトしたり、システム クラッシュが発生したりした場合でもキャッシュされます。システム キャッシュには、1 つのネットワーク分析ポリシーと 1 つの侵入ポリシーの未保存の変更しか格納されないため、同じタイプの別のポリシーを編集する場合は、その前に、行った変更を確定または破棄する必要があります。最初のポリシーに対する変更を保存せずに別のポリシーを編集した場合や、侵入ルールのアップデートをインポートした場合は、キャッシュされている変更が破棄されます。

ネットワーク分析ポリシーまたは侵入ポリシーのエディタの [Policy Information] ページで、ポリシーの変更をコミットまたは破棄できます。侵入ポリシーの編集（345ページ）を参照してください。

次の表は、ネットワーク分析ポリシーまたは侵入ポリシーへの変更を保存または破棄する方法を要約して示しています。

表 *46*：ネットワーク分析ポリシーまたは侵入ポリシーへの変更の確定

目的	[Policy Information] ページでは、次の操作を実行できます
ポリシーへの変更を保存する	[Commit Changes] をクリックします。 任意で、コメントを入力します。[OK] をクリックしてコミットを続行します。
すべての未保存の変更を破棄する	[Discard Changes] をクリックしてから [OK] をクリックし、変更を破棄して、[Intrusion Policy] ページに移動します。変更を破棄しない場合は、[Cancel] をクリックして [Policy Information] ページに戻ります。
ポリシーを終了し、変更をキャッシュする	任意のメニューまたは別のページへの他のパスを選択します。終了時に、表示されたプロンプトで[ページを移動（Leave page）] をクリックするか、[ページを移動しない（Stay on page）] をクリックして高度なエディタに残ります。



第 19 章

ネットワーク分析ポリシーまたは侵入ポリシー レイヤでのレイヤの使用

多数の ASA FirePOWER モジュールが存在する大規模な組織では、さまざまな部署や事業部門、場合によっては異なる企業の固有のニーズに対応するために、多数の侵入ポリシーやネットワーク分析ポリシーが存在することがあります。両方のポリシータイプでの設定はレイヤと呼ばれる構成要素に含まれており、それを使用することで効率的に複数のポリシーを管理することができます。

侵入ポリシーとネットワーク分析ポリシーのレイヤは、基本的に同じように動作します。どちらのポリシータイプも、レイヤを意識せずに作成したり編集することができます。ポリシーの設定は変更でき、ポリシーにユーザ レイヤを追加していない場合は、1つの設定可能なレイヤ（最初は「My Changes」という名前が付けられています）にその変更が自動的に取り込まれます。必要に応じて、最大200のレイヤを追加できます。それらのレイヤでは、任意の設定項目を組み合わせて設定することができます。ユーザ レイヤのコピー、マージ、移動、削除を実行できます。最も重要な点は、個々のユーザ レイヤを同じタイプの他のポリシーと共有できることです。

- レイヤ スタックについて （317 ページ）
- レイヤの管理 （322 ページ）

レイヤ スタックについて

ライセンス：Protection

レイヤが追加されていないネットワーク分析ポリシーや侵入ポリシーには、組み込みの読み取り専用の基本ポリシー レイヤと、ユーザが設定可能な単一のレイヤ（最初は「My Changes」という名前が付けられています）が含まれています。ユーザ設定可能なレイヤは、コピー、マージ、移動、または削除を行うことができます。また、任意のユーザ設定可能なレイヤが同じタイプの他のポリシーと共有されるように設定することもできます。

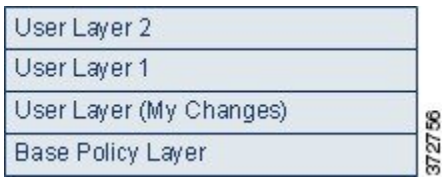
各ポリシー レイヤには、ネットワーク分析ポリシーのすべてのプリプロセッサの全設定、または、侵入ポリシーの侵入ルールと詳細設定がすべて含まれています。最下位の基本ポリシー レイヤには、ポリシーの作成時に選択した基本ポリシーのすべての設定が含まれています。上位

レイヤの設定は、下位レイヤの同じ設定よりも優先されます。レイヤで明示的に設定されていない機能は、明示的に設定されている次に上位のレイヤの設定を継承します。

システムはレイヤをフラット化します。つまり、ネットワーク トラフィックの処理時にすべての設定の蓄積効果のみを適用します。

ヒント 侵入またはネットワークの分析ポリシーは、基本ポリシーのデフォルト設定のみに基づいて作成できます。

次の図は、基本ポリシー レイヤと初期設定の My Changes レイヤの他に、2 つのユーザが設定可能な追加レイヤ「User Layer 1」と「User Layer 2」を含むレイヤ スタックの例を示しています。この図では、ユーザが追加したユーザ設定可能な各レイヤは、スタックの最上位のレイヤに配置されていることに注目してください。図の User Layer 2 は、最後に追加され、スタックの最上位にあります。



複数のレイヤを使用する場合は、次の点に注意してください。

- 以下のいずれかを実行する場合、ポリシー内の最上位のレイヤが読み取り専用レイヤであるか、またはポリシー間でのレイヤの共有 （327ページ）で説明されてる共有レイヤであるときに、ユーザ設定可能なレイヤが最上位のレイヤとして侵入ポリシーに自動的に追加されます。
  - 侵入ポリシーの [Rules] ページでルールのアクション（ルール状態、イベント フィルタリング、動的状態、または警告）を変更する。詳細については、「ルールを使用した侵入ポリシーの調整 （355 ページ）」を参照してください。
  - プリプロセッサ、侵入ルール、あるいは詳細設定を有効化、無効化、または変更する。

システムによって追加されたレイヤの設定は、新しいレイヤで生じた変更を除いてすべて継承されます。

- 最上位レイヤが共有レイヤの場合、次のいずれかの操作を実行するとレイヤが追加されます。
  - 他のポリシーと最上位レイヤを共有する
  - ポリシーにレイヤを追加する
- ルール アップデートによるポリシーの変更を許可しているかどうかに関わらず、ルール アップデートによる変更は、ユーザがレイヤで行った変更を上書きしません。これは、ルール アップデートよる変更は、基本ポリシー レイヤのデフォルト設定を決定する基本

ポリシーに対して行われるからです。ユーザによる変更はより上位のレイヤで行われるので、その変更によって、ルール アップデートによる基本ポリシーの変更が上書きされます。詳細については、「ルール更新とローカル ルール ファイルのインポート （582 ページ）」を参照してください。

基本レイヤについて

ライセンス：Protection

侵入ポリシーまたはネットワーク分析ポリシーの基本レイヤ（基本ポリシーとも呼ばれる）は、ポリシーのすべての設定のデフォルト設定を定義し、ポリシーの最下位に位置します。新しいポリシーを作成し、新しいレイヤを追加しないで設定を変更すると、その変更はMy Changesレイヤに保存され、基本ポリシーの設定を変更するのではなく、上書きます。

システムによって提供される基本ポリシーについて

ライセンス：Protection

シスコではASA FirePOWERモジュールで、ネットワーク分析ポリシーと侵入ポリシーのペアを複数提供しています。システムによって提供されるネットワーク分析ポリシーと侵入ポリシーを使用することで、シスコ脆弱性調査チーム（VRT）の経験を活用できます。これらのポリシーに対して、VRTは侵入およびプリプロセッサ ルールの状態を設定し、プリプロセッサと他の詳細設定の初期設定も行います。これらのシステム付属のポリシーはそのまま使用することも、カスタム ポリシーの基本として使用することもできます。

システム付属のポリシーを基本として使用する場合は、ルールアップデートをインポートすると基本ポリシーの設定が変更されます。ただし、カスタムポリシーで、システム付属の基本ポリシーが自動的に変更されないように設定できます。これにより、ルールアップデートのインポートとは別に、スケジュールに基づいて、システム付属の基本ポリシーを手動で変更できます。いずれの場合も、ルールアップデートによって基本ポリシーが変更されても、My Changesや他のレイヤの設定は変更されず、上書きもされません。詳細については、ルールアップデートによるシステム付属基本ポリシーの変更を許可する （320 ページ）を参照してください。

システム付属の侵入ポリシーとネットワーク分析ポリシーには同じような名前が付いていますが、異なる設定が含まれています。たとえば、「Balanced Security and Connectivity」ネットワーク分析ポリシーと「Balanced Security and Connectivity」侵入ポリシーは連携して動作し、どちらも侵入ルールのアップデートで更新できます。詳細については、システムによって提供されるポリシーについて （306 ページ）を参照してください。

カスタム基本ポリシーについて

ライセンス：Protection

ネットワーク分析ポリシーまたは侵入ポリシーでシステムによって提供されるポリシーを基本ポリシーとして使用しない場合は、カスタムポリシーをベースとして使用できます。カスタムポリシーの設定を調整することで、最も役立つ方法でトラフィックを検査できます。これによって、デバイスのパフォーマンスが向上し、ユーザは生成されたイベントにさらに効率的に対応できるようになります。

最大 5 つのカスタム ポリシーをチェーンすることができます。5 つのうちの 4 つのポリシーで事前に作成されたポリシーが基本ポリシーとして使用され、5つ目のポリシーでシステムによって提供されたポリシーをベースとして使用する必要があります。

別のポリシーの基本として使用しているカスタム ポリシーに加えた変更は、それを使用しているポリシーのデフォルト設定として自動的に使用されます。また、すべてのポリシーにはポリシーチェーンの最終的なベースとしてシステム付属のポリシーがあるため、カスタム基本ポリシーを使用している場合でも、ルールアップデートをインポートするとポリシーに影響が及びます。チェーンの最初のカスタムポリシー（システム付属のポリシーを基本として使用しているポリシー）で、ルール アップデートによる基本ポリシーの変更が許可されている場合は、ユーザのポリシーが影響を受ける可能性があります。この設定の変更の詳細については、ルールアップデートによるシステム付属基本ポリシーの変更を許可する （320 ページ）を参照してください。

変更の内容に関係なく、また、ルールアップデートによる変更であるか、基本ポリシーとして使用しているカスタムポリシーの変更であるかを問わず、ユーザの基本ポリシーに対する変更は、My Changes や他のレイヤの設定を変更せず、上書きもしません。

基本ポリシーの変更

ライセンス：Protection

ネットワーク分析ポリシーや侵入ポリシーに対して別の基本ポリシーを選択できます。または必要に応じて、上位レイヤでの変更に影響を与えることなく、ルールアップデートによってシステム付属の基本ポリシーを変更できます。

基本ポリシーの変更方法：

ステップ 1 ポリシーの編集中に、ナビゲーション パネルで [Policy Information] をクリックします。

[Policy Information] ページが表示されます。

ステップ 2 [Base Policy] ドロップダウン リストから基本ポリシーを選択します。

ステップ 3 （任意）システム付属の基本ポリシーを選択する場合は、[Manage Base Policy] をクリックして、侵入ルールのアップデートによって基本ポリシーを自動的に変更できるかどうかを指定します。

詳細については、ルール アップデートによるシステム付属基本ポリシーの変更を許可する （320 ページ）を参照してください。

ステップ 4 ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。詳細については、競合の解決とポリシー変更の確定 （314 ページ）を参照してください。

ルール アップデートによるシステム付属基本ポリシーの変更を許可する

ライセンス：Protection

インポートするルール更新によって、変更済みのネットワーク分析プリプロセッサの設定、変更済みの侵入ポリシーの詳細設定、新規および更新済みの侵入ルール、および既存ルールの変更済みの状態が、システム提供ポリシーに提供されます。ルール更新では、ルールを削除したり、新しいルールカテゴリとデフォルト変数を提供したりすることもできます。詳細については、「ルール更新とローカルルールファイルのインポート（582ページ）」を参照してください。

ルール更新は、プリプロセッサ、詳細設定およびルールの変更とともに、システムによって提供されるポリシーを常に変更します。デフォルト変数とルールカテゴリに対する変更はシステム レベルで処理されます。詳細については、「システムによって提供される基本ポリシーについて（319ページ）」を参照してください。

システム提供のポリシーを基本ポリシーとして使用する場合、ルール更新による基本ポリシー（この場合はシステム提供ポリシーのコピー）の変更を許可できます。ルール更新で基本ポリシーの更新を許可する場合は、新しいルール更新によって、基本ポリシーとして使用するシステム提供のポリシーに対する変更と同じ変更が基本ポリシーにも加えられます。対応する設定を変更しなかった場合は、基本ポリシー内の設定によって、新しいポリシー内の設定が決定されます。ただし、ユーザがポリシーに加えた変更は、新しいルールアップデートによって上書きされません。

ルール更新で基本ポリシーの更新を許可しない場合は、1つ以上のルール更新のインポート後に、基本ポリシーを手動で更新できます。

ルール アップデートでは、侵入ポリシー内のルール状態や、ルール アップデートによる基本ポリシーの更新が許可されているかどうかに関係なく、VRTが削除したルールは必ず削除されるので注意してください。ネットワークトラフィックに変更が再適用されるまで、現在適用されている侵入ポリシー内のルールは次のように動作します。

- 無効になっているルールは無効のままになります。
- [Generate Events] に設定されたルールは、トリガーされると引き続きイベントを生成します。
- [Drop and Generate Events] に設定されたルールは、トリガーされると引き続きイベントを生成し、違反パケットをドロップします。

次の両方の条件が満たされていない場合、ルールアップデートはカスタム基本ポリシーを変更しません。

- ルール アップデートによる親ポリシーのシステム付属基本ポリシー（カスタム基本ポリシーの元となるポリシー）の変更が許可されている。
- 親の基本ポリシー内の対応する設定が上書きされる親ポリシー内の変更を実施していない。

両方の条件が満たされている場合は、親ポリシーを保存したときに、ルール更新内の変更が子ポリシー（つまり、カスタム基本ポリシーを使用したポリシー）に渡されます。

たとえば、無効化されていた侵入ルールがルールアップデートによって有効化され、親となる侵入ポリシーのルールの状態がユーザによって変更されていない場合は、親ポリシーの保存時に、変更されたルール状態が基本ポリシーに渡されます。

同様に、ルールアップデートによってデフォルトのプリプロセッサ設定が変更され、親となるネットワーク分析ポリシーの設定がユーザによって変更されていない場合は、親ポリシーの保存時に、変更された設定が基本ポリシーに渡されます。

詳細については、「基本ポリシーの変更 （320 ページ）」を参照してください。

ルール アップデートによるシステム付属基本ポリシーの変更を許可するには：

ステップ 1 システム提供のポリシーを基本ポリシーとして使用するポリシーの編集時に、ナビゲーション パネルで [Policy Information] をクリックします。

[Policy Information] ページが表示されます。

ステップ 2 [Manage Base Policy] をクリックします。

[Base Policy summary] ページが表示されます。

ステップ 3 [Update when a new Rule Update is installed] チェック ボックスをオンまたはオフにします。

このチェックボックスをオフにしてポリシーを保存してから、ルールアップデートをインポートすると、[Base Policy] 概要ページに [Update Now] ボタンが表示され、そのページ上のステータス メッセージが更新されて、ポリシーが期限切れであることが示されます。必要に応じて、[Update Now] をクリックして、最近インポートしたルール更新内の変更で基本ポリシーを更新できます。

ステップ 4 ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。詳細については、競合の解決とポリシー変更の確定 （314 ページ）を参照してください。

レイヤの管理

ライセンス：Protection

[Policy Layers] ページには、ネットワーク分析ポリシーまたは侵入ポリシーの完全なレイヤ スタックの概要が 1 ページで表示されます。このページでは、共有レイヤや非共有レイヤを追加したり、レイヤをコピー、マージ、移動、削除したり、各レイヤの概要ページにアクセスすることができます。また、各レイヤ内の設定を有効化、無効化、上書きするための設定ページにもアクセスできます。

各レイヤについて、次の情報が表示されます。

- レイヤが組み込み型レイヤ、共有ユーザ レイヤ、または非共有ユーザ レイヤであるかどうか
- どのレイヤが、最も上位の（つまり、効率的な）プリプロセッサまたは詳細設定を含んでいるか（機能名別に表示）
- 侵入ポリシーにおける、レイヤに状態が設定されている侵入ルールの数、および各ルール状態に対して設定されているルールの数。

サマリに表示される各レイヤの機能名は、次のように、レイヤで有効化、無効化、上書き、継承されている設定を示しています。

このページには、すべての有効なプリプロセッサ（ネットワーク分析）または詳細設定（侵入）、および侵入ルール（侵入ポリシーの場合）の実質的な効果の概要も表示されます。

機能の状態	機能名
レイヤで有効	プレーン テキストで表示
レイヤで無効	取り消し線が引かれる
上位レイヤの設定によって上書きされる	イタリック テキストで表示
下位レイヤから継承される	表示されない

次の表に、[Policy Layers] ページで使用できるアクションを示します。

表 47 : ネットワーク分析ポリシーおよび侵入ポリシーの設定操作

目的	操作
[ポリシー情報（Policy Information）] ページの表示	[Policy Summary] をクリックします。 [Policy Information] ページで実行できる操作については、ルールを使用した侵入ポリシーの調整（355 ページ）および侵入ポリシーについて（341 ページ）を参照してください。
レイヤのサマリ ページを表示する	該当するレイヤの行でレイヤ名をクリックするか、またはユーザ レイヤの横にある編集アイコンをクリックします。表示アイコンをクリックして、共有レイヤの読み取り専用サマリ ページにアクセスすることもできます。 レイヤのサマリ ページで実行できる操作については、ポリシー間でのレイヤの共有（327 ページ）、層のプリプロセッサと詳細の設定（333 ページ）、およびレイヤでの侵入ルールの設定（329 ページ）を参照してください。
レイヤレベルのプリプロセッサまたは詳細設定の設定ページへのアクセス	該当するレイヤの行で機能名をクリックします。基本ポリシーと共有レイヤでは、設定ページが読み取り専用であることに注意してください。詳細については、「層のプリプロセッサと詳細の設定（333 ページ）」を参照してください。
ルール状態のタイプ別にフィルタリングされた、レイヤレベルのルール設定ページにアクセスする	レイヤのサマリで、イベントのドロップおよび生成アイコン（  ）、イベントの生成アイコン（  ）、または無効化アイコン（）をクリックします。選択したルール状態に設定されているルールがレイヤに含まれていない場合、ルールは表示されません。
ポリシーへのレイヤの追加	レイヤの追加（324 ページ）を参照してください。
別のポリシーからの共有レイヤの追加	ポリシー間でのレイヤの共有（327 ページ）を参照してください。

目的	操作
レイヤの名前または説明を変更する	レイヤの名前および説明の変更 （325 ページ）を参照してください。
レイヤを移動、コピー、または削除する	レイヤの移動、コピー、削除 （325 ページ）を参照してください。
すぐ下のレイヤとのレイヤのマージ	レイヤのマージ （326 ページ）を参照してください。

[Policy Layers] ページの使用方法：

ステップ 1 ポリシーの編集中に、ナビゲーション パネルで [Policy Layers] をクリックします。

[Policy Layers] サマリ ページが表示されます。

ステップ 2 表「ネットワーク分析レイヤおよび侵入ポリシー レイヤの設定操作」のいずれかの操作を実行できます。#unique_328 unique_328_Connect_42_Table （323 ページ）

ステップ 3 ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。詳細については、競合の解決とポリシー変更の確定 （314 ページ）を参照してください。

レイヤの追加

ライセンス：Protection

最大200のレイヤをネットワーク分析ポリシーまたは侵入ポリシーに追加できます。レイヤを追加すると、そのレイヤがポリシーの最上位レイヤとして表示されます。すべての機能の初期状態が継承され、侵入ポリシーでは、イベント フィルタリング、動的状態、アラート ルール アクションは設定されません。

ネットワーク分析ポリシーまたは侵入ポリシーへのレイヤの追加方法：

ステップ 1 ポリシーの編集中に、ナビゲーション パネルで [Policy Layers] をクリックします。

[Policy Layers] ページが表示されます。

ステップ 2 ユーザ レイヤの横にあるレイヤの追加アイコン（  ）をクリックします。

[Add Layer] ポップアップ ウィンドウが表示されます。

ステップ 3 [Name] に一意のレイヤ名を入力し、[OK] をクリックします。

新しいレイヤが、ユーザ レイヤの最上位のレイヤとして表示されます。

ステップ 4 ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。詳細については、競合の解決とポリシー変更の確定 （314 ページ）を参照してください。

レイヤの名前および説明の変更

ライセンス：Protection

ネットワーク分析ポリシーまたは侵入ポリシーのユーザ設定可能レイヤの名前は変更できます。必要に応じて、レイヤの編集時に表示される説明を追加または変更することもできます。

レイヤ名の変更方法および説明の追加/変更方法：

ステップ 1 ポリシーの編集中に、ナビゲーション パネルで [Policy Layers] をクリックします。

[Policy Layers] ページが表示されます。

ステップ 2 編集するユーザ レイヤの横にある編集アイコンをクリックします。

レイヤのサマリ ページが表示されます。

ステップ 3 次の操作を実行できます。

- レイヤの**名前**の変更
- レイヤの**説明**の追加または変更

ステップ 4 ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。詳細については、競合の解決とポリシー変更の確定 （314 ページ）を参照してください。

レイヤの移動、コピー、削除

ライセンス：Protection

初期の My Changes レイヤを含め、ネットワーク分析ポリシーまたは侵入ポリシーのユーザ レイヤはコピー、移動、削除することができます。以下の点に注意してください。

- レイヤをコピーすると、そのコピーが最上位レイヤとして表示されます。
- 共有レイヤをコピーすると、非共有のコピーが作成されます。このコピーは、必要に応じて他のポリシーと共有できます。
- 共有レイヤは削除できません。共有が有効になっているレイヤが他のポリシーと共有されていない場合、そのレイヤは共有レイヤではありません。

レイヤのコピー、移動、削除方法：

ステップ 1 ポリシーの編集中に、ナビゲーション パネルで [Policy Layers] をクリックします。

[Policy Layers] ページが表示されます。

ステップ 2 次の操作を実行できます。

- レイヤをコピーするには、コピーするレイヤのコピー アイコンをクリックします。

ページが更新され、レイヤのコピーが最上位のレイヤとして表示されます。

- [User Layers] ページ領域内でレイヤを上下に移動するには、レイヤ サマリ内の任意の空領域をクリックし、位置矢印（▶）が移動するレイヤの上または下の行を指すまでドラッグします。

画面が更新され、レイヤが新しい場所に表示されます。

- レイヤを削除するには、削除するレイヤの削除アイコンをクリックし、[OK] をクリックします。

ページが更新され、レイヤは削除されます。

ステップ 3 ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。詳細については、競合の解決とポリシー変更の確定 （314 ページ）を参照してください。

レイヤのマージ

ライセンス：Protection

ネットワーク分析ポリシーまたは侵入ポリシー内のユーザ設定可能なレイヤを、その下にある次のユーザ レイヤとマージできます。マージされたレイヤは、どちらかのレイヤに固有だったすべての設定を保持します。また、両方のレイヤに同じプリプロセッサ、侵入ルールまたは詳細設定の設定が含まれている場合は、上位のレイヤの設定を受け入れます。マージされたレイヤでは、下位レイヤの名前が保持されます。

ポリシーで共有レイヤを作成して他のポリシーに追加する場合、作成元のポリシーでは、その共有レイヤをすぐ上の非共有レイヤとマージできますが、下の非共有レイヤとマージすることはできません。

ポリシーで共有レイヤを作成して他のポリシーに追加する場合、追加先のポリシーでは、その共有レイヤをすぐ下の非共有レイヤとマージできますが、マージ後のレイヤは共有されなくなります。共有レイヤを上の非共有レイヤとマージすることはできません。

ユーザ レイヤをその下のユーザ レイヤとマージする方法：

ステップ 1 ポリシーの編集中に、ナビゲーション パネルで [Policy Layers] をクリックします。

[Policy Layers] ページが表示されます。

ステップ 2 2 つのレイヤの上部にあるマージ アイコン（）をクリックし、[OK] をクリックします。

ページが更新され、レイヤがその下のレイヤとマージされます。

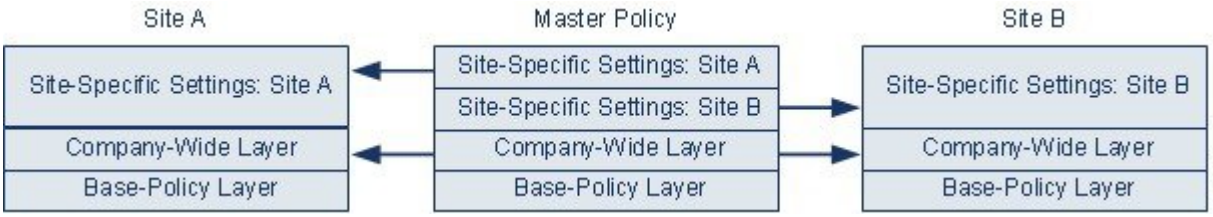
ステップ 3 ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。詳細については、競合の解決とポリシー変更の確定 （314 ページ）を参照してください。

ポリシー間でのレイヤの共有

ライセンス：Protection

ユーザ設定可能なレイヤは同じタイプの他のポリシー（侵入またはネットワーク分析）と共有できます。共有レイヤ内の設定を変更し、変更を確定すると、共有レイヤを使用するすべてのポリシーが更新され、影響を受けたすべてのポリシーのリストが表示されます。レイヤを作成したポリシーでのみ、共有レイヤの機能設定を変更できます。

次の図は、サイト固有のポリシーのソースとして機能するマスターポリシーの例を示しています。



図内のマスター ポリシーには、Site A と Site B のポリシーに適用可能な設定を持つ全社的レイヤが含まれています。また、各ポリシーのサイト固有のレイヤも含まれています。たとえば、ネットワーク分析ポリシーの場合、サイト A にはモニタ対象ネットワークに Web サーバがないため、保護したり、HTTP インスペクション プリプロセッサのオーバーヘッドを処理したりする必要はありませんが、両方のサイトで TCP ストリームの前処理が必要になる場合があります。両方のサイトで共有する全社的レイヤで TCP ストリーム処理を有効にし、サイト A で共有するサイト固有のレイヤで HTTP Inspect プリプロセッサを無効にして、サイト B で共有するサイト固有のレイヤで HTTP Inspect プリプロセッサを有効にできます。サイト固有のポリシーで上位レイヤの設定を編集することで、必要に応じて、設定の調整によって各サイトのポリシーをさらに調整することもできます。

この例のマスターポリシーでフラット化された設定値そのものがトラフィックをモニタするのに役立つわけではありませんが、サイト固有のポリシーを設定および更新する際に時間が節約されるため、ポリシー階層で活用することができます。

その他にも多くのレイヤ設定が可能です。たとえば、企業、部門、またはネットワークごとにポリシーのレイヤを定義できます。侵入ポリシーの場合は、一方のレイヤに詳細設定を含め、もう一方にルール設定を含めることもできます。

ヒント　基本ポリシーが共有対象のレイヤが作成されたカスタムポリシーである場合は、ポリシーに共有レイヤを追加できません。変更を保存しようとすると、ポリシーに循環依存関係が含まれていることを示すエラーメッセージが表示されます。詳細については、「カスタム基本ポリシーについて （319 ページ）」を参照してください。

他のポリシーとレイヤを共有するには、次の手順を実行します。

- 共有するレイヤのサマリ ページで共有を有効にします。
- レイヤを共有するポリシーの [Policy Layers] ページに、共有するレイヤを追加します。

ポリシー間でのレイヤの共有

別のポリシーで使用されているレイヤの共有を無効にすることはできません。まずそのレイヤを他のポリシーから削除するか、他のポリシーを削除する必要があります。

他のポリシーとのレイヤ共有を有効化/無効化する方法：

ステップ 1　ポリシーの編集中に、ナビゲーション パネルで [Policy Layers] をクリックします。

[Policy Layers] ページが表示されます。

ステップ 2　他のポリシーと共有するレイヤの横にある編集アイコンをクリックします。

レイヤのサマリ ページが表示されます。

ステップ 3　[Sharing] チェックボックスをオン（有効）またはオフ（無効）にします。

ステップ 4　ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。

詳細については、競合の解決とポリシー変更の確定 （314 ページ） を参照してください。

ポリシーへの共有レイヤの追加方法：

ステップ 5　ポリシーの編集中に、ナビゲーション パネルで [Policy Layers] をクリックします。

[Policy Layers] ページが表示されます。

ステップ 6　[Add Shared Layer] ドロップダウンリストから追加する共有レイヤを選択し、[OK] をクリックします。

[Policy Layers] サマリ ページが表示され、選択した共有レイヤがポリシー内の最上位レイヤとして表示されます。

その他のポリシーに共有レイヤがない場合、ドロップダウンリストは表示されません。ポップアップ ウィンドウで [OK] または [Cancel] をクリックすると、[Policy Layers] サマリ ページに戻ります。

ステップ 7　ユーザ レイヤの横にある共有レイヤ追加アイコン（）をクリックします。

[Add Shared Layer] ポップアップ ウィンドウが表示されます。

ステップ 8 ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。

詳細については、競合の解決とポリシー変更の確定 （314 ページ）を参照してください。

レイヤでの侵入ルールの設定

ライセンス：Protection

侵入ポリシーでは、すべてのユーザ設定可能なレイヤのルールに対して、ルール状態、イベント フィルタリング、動的状態、アラート、およびルール コメントを設定できます。変更を加えるレイヤにアクセスした後、侵入ポリシーの [Rules] ページでの操作と同様に、そのレイヤの [Rules] ページに設定を追加します（ルールを使用した侵入ポリシーの調整 （355 ページ）を参照）。

レイヤの [Rules] ページで個々の設定を表示することも、[Rules] ページのポリシー ビューですべての設定の実質的な効果を表示することもできます。[Rules] ページのポリシー ビューのルール設定を変更する場合、ポリシーの最上位のユーザ設定可能なレイヤを変更します。[Rules] ページにあるレイヤ ドロップダウン リストを使用して、別のレイヤに切り替えることができます。

次の表では、複数のレイヤで同じ種類の設定を構成した場合の結果について説明しています。

表 *48 :* レイヤ ルールの設定

設定可能なレイヤ数	設定の種類	目的
1	ルール状態	下位レイヤのルールに対して設定されたルール状態を上書きします。また、下位レイヤで設定されたそのルールのすべてのしきい値、抑制、レートベースのルール状態、およびアラートを無視します。詳細については、「ルール状態の設定 （377 ページ）」を参照してください。 基本ポリシーまたは下位レイヤのルール状態をルールに継承させる場合は、ルール状態を [Inherit] に設定します。ただし、侵入ポリシーの [Rules] ページで作業している場合は、ルール状態を [Inherit] に設定できません。 特定のレイヤの [Rules] ページでルール状態を表示すると、ルール状態が色分け表示されます。有効状態が下位レイヤで設定されているルールは黄色で、上位レイヤで設定されているルールは赤色で強調表示されます。有効状態が現在のレイヤで設定されているルールは強調表示されません。侵入ポリシーの [Rules] ページはすべてのルール設定の最終的な効果の複合ビューであるため、ルール状態はこのページでは色分けされません。

設定可能なレイヤ数	設定の種類	目的
1	しきい値 SNMP アラート	下位レイヤのルールの同じ種類の設定を上書きします。しきい値を設定すると、レイヤのルールの既存のしきい値が上書きされることに注意してください。詳細については、イベントしきい値の設定（380ページ）およびSNMPアラートの追加（392ページ）を参照してください。
1 つ以上	抑制レートベースのルール状態	選択した各ルールの同じ種類の設定を、ルール状態がそのルールに対して設定された最初の下位レイヤまで累積的に組み合わせます。ルール状態が設定されているレイヤより下の設定は無視されます。詳細については、侵入ポリシーごとの抑制の設定（385ページ）および動的ルール状態の追加（388ページ）を参照してください。
1 つ以上	コメント	ルールにコメントを追加します。コメントは、ポリシー固有またはレイヤ固有ではなく、ルール固有です。任意のレイヤの 1 つのルールに 1 つ以上のコメントを追加できます。詳細については、「動的ルール状態の追加（388ページ）」を参照してください。

たとえば、あるレイヤでルール状態を [Drop and Generate Events] に設定し、それよりも上位のレイヤで [Disabled] に設定した場合、侵入ポリシーの [Rules] ページには、ルールが無効であることが示されます。

別の例として、あるレイヤでルールの送信元ベースの抑制を 192.168.1.1 に設定し、別のレイヤでそのルールの宛先ベースの抑制を 192.168.1.2 に設定した場合、[Rules] ページには、送信元アドレス 192.168.1.1 と宛先アドレス 192.168.1.2 に関するイベントを抑制する累積的な結果が示されます。抑制およびレートベースのルール状態の設定では、選択した各ルールの同じ種類の設定が、ルール状態がそのルールに対して設定された最初の下位レイヤまで累積的に組み合わせられることに注意してください。ルール状態が設定されているレイヤより下の設定は無視されます。

レイヤでのルールの変更方法：

ステップ 1 侵入ポリシーの編集中に、ナビゲーション パネルで [Policy Layers] を展開し、変更するポリシー レイヤを展開します。

ステップ 2 変更するポリシー レイヤのすぐ下にある [Rules] をクリックします。

レイヤの [Rules] ページが表示されます。

表「レイヤ ルールの設定」のいずれかの設定を変更できます。#unique_330 unique_330_Connect_42_Table（329ページ）侵入ルールの設定の詳細については、ルールを使用した侵入ポリシーの調整（355ページ）を参照してください。

編集可能なレイヤから個々の設定を削除するには、そのレイヤの [Rules] ページでルール メッセージをダブルクリックしてルールの詳細を表示します。削除する設定の横にある [Delete] をクリックして [OK] を 2 回クリックします。

ステップ 3 ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。詳細については、競合の解決とポリシー変更の確定 （314 ページ）を参照してください。

マルチレイヤ ルールの設定の削除

ライセンス：Protection

侵入ポリシーの [Rules] ページで 1 つ以上のルールを選択して、侵入ポリシーの複数のレイヤから特定タイプのイベント フィルタ、動的状態、またはアラートを同時に削除できます。

システムは、すべての設定を削除するか、ルール状態がルールに対して設定されているレイヤに遭遇するまで、下位方向にある各レイヤの同じ種類の設定を削除します。レイヤにルール状態が設定されている場合は、レイヤからその設定が削除され、その設定タイプの削除は中止されます。

共有レイヤまたは基本ポリシーに指定されたタイプの設定があり、ポリシーの最上位レイヤが編集可能である場合は、ルールの残りの設定とルール状態がその編集可能なレイヤにコピーされます。そうではない場合、ポリシーの最上位のレイヤが共有レイヤであれば、システムは新しい編集可能なレイヤをその共有レイヤの上に作成し、そのルールの残りの設定およびルール状態をその編集可能なレイヤにコピーします。

（注） 共有レイヤまたは基本ポリシーに由来するルール設定を削除すると、下位レイヤまたは基本ポリシーにおけるこのルールへの変更は無視されます。下位レイヤまたは基本ポリシーにおける変更が無視されないようにするには、最上位レイヤのサマリ ページでルール状態を [Inherit] に設定します。詳細については、「ルール状態の設定 （377 ページ）」を参照してください。

複数のレイヤのルール設定を削除する方法：

ステップ 1 侵入ポリシーの編集中に、ナビゲーション パネルで [Policy Information] のすぐ下にある [Rules] をクリックします。

ヒント また、任意のレイヤの [Rules] ページでレイヤのドロップダウン リストから [Policy] を選択するか、[Policy Information] ページの [Manage Rules] を選択することもできます。

侵入ポリシーの [Rules] ページが表示されます。

ステップ 2 複数の設定を削除するルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェック ボックスをオンにします。

ルールの検索については、侵入ポリシー内のルール フィルタ処理について （366 ページ）および侵入ポリシー内のルール フィルタの設定 （375 ページ）を参照してください。

ステップ 3 次の選択肢があります。

- ルールのすべてのしきい値を削除するには、[Event Filtering] > [Remove Thresholds] を選択します。
- ルールのすべての抑制を削除するには、[Event Filtering] > [Remove Suppressions] を選択します。
- ルールのレートベースのルール状態をすべて削除するには、[Dynamic State] > [Remove Rate-Based Rule States] の順に選択します。
- ルールのすべての SNMP アラート設定を削除するには、[Alerting] > [Remove SNMP Alerts] を選択します。

確認ポップアップ ウィンドウが表示されます。

（注） 共有レイヤまたは基本ポリシーに由来するルール設定を削除すると、下位レイヤまたは基本ポリシーにおけるこのルールへの変更は無視されます。下位レイヤまたは基本ポリシーにおける変更が無視されないようにするには、最上位レイヤのサマリ ページでルール状態を [Inherit] に設定します。詳細については、「ルール状態の設定 （377 ページ）」を参照してください。

ステップ 4 [OK] をクリックします。

システムは選択された設定を削除し、ルールの残りの設定をポリシーの最上位の編集可能なレイヤにコピーします。システムが残りの設定をコピーする方法に影響を与える条件については、この手順の概要を参照してください。

ステップ 5 ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。詳細については、競合の解決とポリシー変更の確定 （314 ページ）を参照してください。

カスタム基本ポリシーからのルール変更の受け入れ

ライセンス：Protection

レイヤを追加していないカスタム ネットワーク分析ポリシーまたは侵入ポリシーで、ベース ポリシーとして別のカスタム ポリシーを使用するときは、以下の場合にルール状態を継承するようにルールを設定する必要があります。

- 基本ポリシー ルールに対するイベント フィルタ、動的状態、または SNMP アラートを削除する。および
- 基本ポリシーとして使用している他のカスタム ポリシーで、ルールに対して加える以降の変更をルールが受け入れるようにする

次の手順は、これを完了させる方法を示しています。階層を追加したポリシーでこれらのルールの設定を受け入れるには、マルチレイヤ ルールの設定の削除 （331 ページ）を参照してください。

レイヤを追加しなかったポリシー内でのルール変更を受け入れるには：

ステップ 1 侵入ポリシーの編集中に、ナビゲーション パネルで [Policy Layers] リンクを展開し、[My Changes] を展開します。

ステップ 2 [My Changes] のすぐ下にある [Rules] リンクをクリックします。

My Changes レイヤの [Rules] ページが表示されます。

ステップ 3 設定を受け入れるルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェック ボックスをオンにします。

ルールの検索については、侵入ポリシー内のルール フィルタ処理について （366 ページ）および侵入ポリシー内のルール フィルタの設定 （375 ページ）を参照してください。

ステップ 4 [Rule State] ドロップダウン リストから、[Inherit] を選択します。

ステップ 5 ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。詳細については、競合の解決とポリシー変更の確定 （314 ページ）を参照してください。

層のプリプロセッサと詳細の設定

ライセンス：Protection

ネットワーク分析ポリシーでのプリプロセッサの設定および侵入ポリシーでの詳細設定の設定と同様の方法を使用します。ネットワーク分析の [Settings] ページでプリプロセッサを有効化/無効化したり、侵入ポリシーの [Advanced Settings] ページで侵入ポリシーの詳細設定を有効化/無効化することができます。これらのページには、すべての関連機能の有効状態の概要も表示されます。たとえば、ネットワーク分析 SSL プリプロセッサが、あるレイヤで無効になっており、そのレイヤよりも上位のレイヤで有効になっている場合、[Settings] ページではそのプリプロセッサが有効であると表示されます。このページで加えられる変更は、ポリシーの最上位のレイヤに表示されます。

また、プリプロセッサまたは詳細設定を有効化または無効化したり、ユーザ設定可能なレイヤのサマリ ページの設定ページにアクセスしたりできます。このページで、レイヤの名前と説明を変更したり、同じタイプの他のポリシーとレイヤを共有するかどうかを設定できます。詳細については、ポリシー間でのレイヤの共有 （327 ページ）を参照してください。ナビゲーション パネルの [Policy Layers] の下にあるレイヤの名前を選択することによって、別のレイヤのサマリ ページに切り替えることができます。

プリプロセッサまたは詳細設定を有効にすると、ナビゲーション パネルのレイヤ名の下にその機能の設定ページへのサブリンクが表示され、レイヤのサマリ ページの機能の横に編集アイコンが表示されます。これらは、レイヤで機能を無効化するか、[Inherit] に設定すると表示されなくなります。

プリプロセッサまたは詳細設定の状態（有効または無効）を設定すると、下位レイヤでこの機能の状態と設定が上書きされます。プリプロセッサまたは詳細設定に、基本ポリシーまたは下位レイヤの状態と設定を継承させる場合は、状態を [Inherit] に設定します。[Settings or Advanced Settings] ページで作業するときは、[Inherit] の選択が表示されません。

各レイヤのサマリ ページは次のように色分けされており、有効な設定が上位レイヤ、下位レイヤ、または現在のレイヤのいずれにあるかが示されます。

- 赤：有効な設定は上位レイヤにあります
- 黄色：有効な設定は下位レイヤにあります
- 強調表示なし：有効な設定は現在のレイヤにあります

[Settings] および [Advanced Settings] ページは、関連するすべての設定の複合ビューであるため、これらのページでは有効な設定の位置を示すためのカラー コーディングは使用されません。

システムでは、設定が有効になっている最も上位のレイヤの設定が使用されます。設定を明示的に変更しなかった場合は、デフォルト設定が使用されます。たとえば、ネットワーク分析 DCE/RPC プリプロセッサをあるレイヤで有効にして変更し、それよりも上位のレイヤでは有効にするが、変更しない場合は、上位レイヤのデフォルト設定が使用されます。

次の表に、ユーザ設定可能なレイヤのサマリ ページで実行できる操作を示します。

表 *49*：レイヤのサマリ ページの操作

目的	操作
レイヤの名前または説明の変更	[名前（Name）] または [説明（Description）] の新しい値を入力します。
他の侵入ポリシーとのレイヤの共有	[他のポリシーによるこのレイヤの使用を許可（Allow this layer to be used by other policies）] を選択します。 詳細については、「ポリシー間でのレイヤの共有 （327ページ）」を参照してください。
現在のレイヤのプリプロセッサ/詳細設定を有効化/無効化する	機能の横にある [Enabled] または [Disabled] をクリックします。 有効にすると、ナビゲーション パネルのレイヤ名の下に設定ページへのサブリンクが表示され、サマリ ページの機能の横に編集アイコンが表示されます。 無効にすると、サブリンクと編集アイコンが削除されます。
現在のレイヤの下にある最も上位のレイヤの設定から、プリプロセッサ/詳細設定の状態と設定を継承する	[Inherit] をクリックします。 ページが更新され、機能が有効だった場合は、ナビゲーション パネルの機能のサブリンクおよび編集アイコンが表示されなくなります。

目的	操作
有効なプリプロセッサ/詳細設定の設定ページにアクセスする	編集アイコンまたは機能のサブリンクをクリックして、現在の設定を変更します。 Back Orifice プリプロセッサにユーザ設定可能なオプションがないことに注意してください。

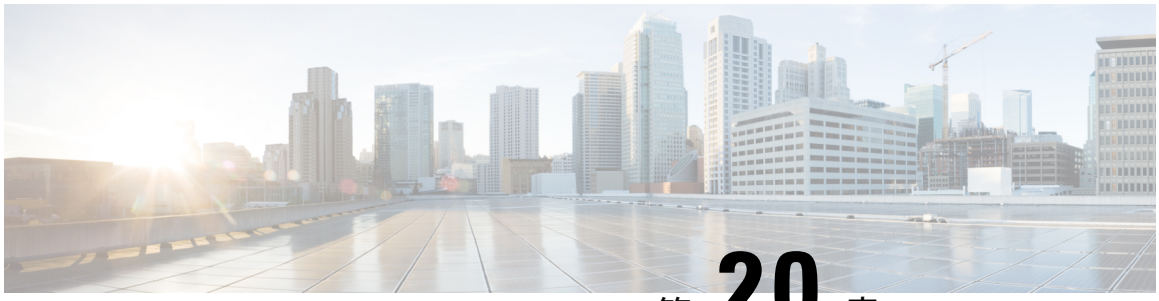
ユーザ レイヤのプリプロセッサ/詳細設定を変更する方法：

ステップ 1 侵入ポリシーの編集中に、ナビゲーション パネルで [Policy Layers] を展開し、変更するレイヤの名前をクリックします。

レイヤのサマリ ページが表示されます。

ステップ 2 表「レイヤのサマリ ページの操作」のいずれかの操作を実行できます。

ステップ 3 ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了するのいずれかを行います。詳細については、競合の解決とポリシー変更の確定 （314 ページ）を参照してください。



第 20 章

パッシブ展開における前処理の調整

通常、システムはネットワーク分析ポリシーの静的な設定を使用して、トラフィックの前処理と分析を行います。ただし、適応型プロファイル機能により、トラフィックをホスト情報と関連付けて処理することにより、ネットワーク トラフィックに対応できます。

ホストがトラフィックを受信すると、ホストで実行されているオペレーティング システムは IP フラグメントを再構成します。再構成に使用する順序は、オペレーティング システムによって異なります。同様に、各オペレーティング システムはさまざまな方法で TCP を実装することがあるため、TCP ストリームの再構成の方法も異なる可能性があります。プリプロセッサが宛先ホストのオペレーティング システムで使用されているものとは異なる形式を使用してデータを再構成すると、受信ホストでの再構成時に悪意のある可能性があるコンテンツをシステムが見逃す可能性があります。

ヒント パッシブ展開の場合、シスコではアダプティブ プロファイルを設定することを推奨しています。インライン展開の場合、シスコでは、インライン正規化プリプロセッサの設定で [Normalize TCP Payload] オプションを有効にすることを推奨しています。

- アダプティブ プロファイルについて （337 ページ）
- 適応型プロファイルの設定 （338 ページ）

アダプティブ プロファイルについて

ライセンス：Protection

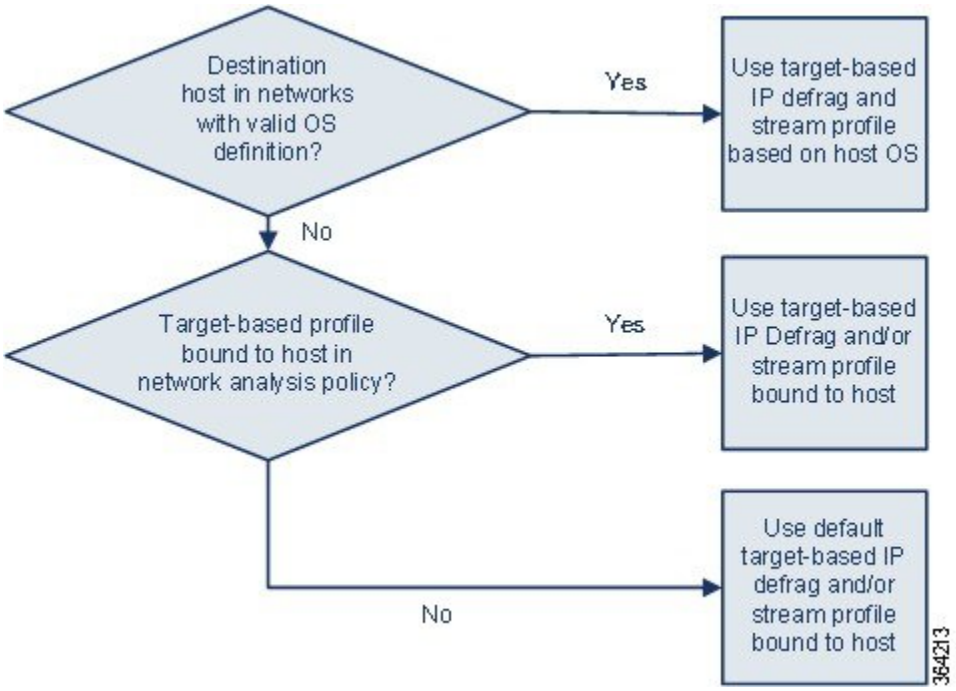
アダプティブ プロファイルは、IP 最適化と TCP ストリームの前処理に最適なオペレーティング システム プロファイルの使用を可能にします。

プリプロセッサでのアダプティブ プロファイルの使用

ライセンス：Protection

適応型プロファイルによって、ターゲット ホストのオペレーティング システムと同じ方法で IP パケットが最適化され、ストリームが再構成されます。その後、侵入ルール エンジンは宛先ホストによって使用されるものと同じ形式でデータを分析します。

適応型プロファイルは、次の図に示すように、ターゲット ホストのホスト プロファイルのオペレーティング システムに基づいて、適切なオペレーティング システム プロファイルに切り替わります。



たとえば、10.6.0.0/16 サブネットにアダプティブ プロファイルを設定し、Linux にデフォルトの IP 最適化ターゲット ベース ポリシーを設定します。設定を行う ASA FirePOWER モジュールには、10.6.0.0/16 サブネットが含まれます。

デバイスは、10.6.0.0/16 サブネットにないホスト A からのトラフィックを検出すると、Linux ターゲット ベース ポリシーを使用して IP フラグメントを再構成します。ただし、10.6.0.0/16 サブネットにあるホスト B からのトラフィックを検出した場合、デバイスはホスト B のオペレーティング システムのデータを取得します。ここでホスト B は、Microsoft Windows XP Professional を実行しています。システムは、Windows ターゲットベース プロファイルを使用して、ホスト B に送信されるトラフィックの IP 最適化を実行します。

適応型プロファイルの設定

ライセンス：Protection

ホスト情報を使用して IP 最適化および TCP ストリームの前処理に使用するターゲット ベース プロファイルを判別するために、適応型プロファイルを設定できます。

適応型プロファイルを設定する際、適応型プロファイルを特定のネットワークにバインドする必要があります。適応型プロファイルを正常に使用するには、そのネットワークがデバイスによってモニタされるセグメント内にある必要があります。

IP アドレス、アドレスのブロック、またはアクセス コントロール ポリシーのデフォルトの侵入ポリシーにリンクされた変数セットにおいて、設定された適切な値を使用したネットワーク変数を指定することで、トラフィックの処理に適応型プロファイルが使用される、ネットワーク内のホストを指定できます。

これらのアドレス指定方法を単独で使用したり、次の例に示すように、IPアドレス、アドレスブロック、または変数をカンマで区切ったリストとして組み合わせて使用したりすることができます。

```
192.168.1.101, 192.168.4.0/24, $HOME_NET
```

ヒント any という値の変数を使用するか、またはネットワーク値として 0.0.0.0/0 を指定することにより、アダプティブ プロファイルをネットワーク内のすべてのホストに適用できます。

適合型プロファイルの設定：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。
[Access Control Policy] ページが表示されます。

ステップ 2 編集するアクセス コントロール ポリシーの横にある編集アイコンをクリックします。
アクセス コントロール ポリシー エディタが表示されます。

ステップ 3 [Advanced] タブを選択します。
アクセス コントロール ポリシーの詳細設定ページが表示されます。

ステップ 4 [Detection Enhancement Settings] の横にある編集アイコンをクリックします。
[Detection Enhancement Settings] ポップアップ ウィンドウが表示されます。

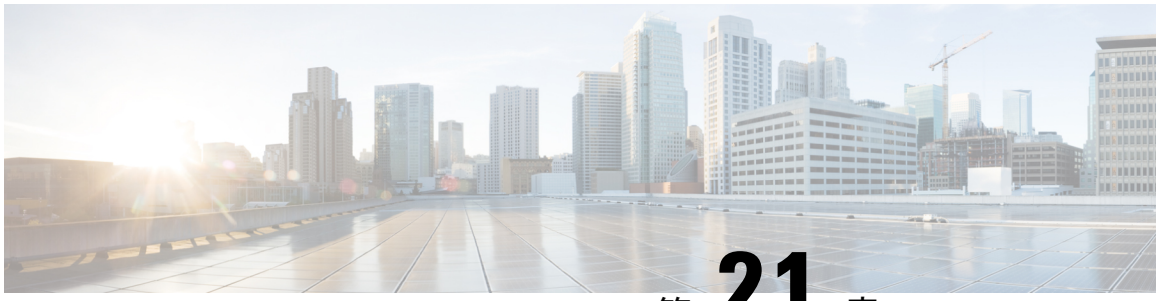
ステップ 5 [Adaptive Profiles - Enabled] を選択して、アダプティブ プロファイルを有効にします。

ステップ 6 必要に応じて、[Adaptive Profiles - Attribute Update Interval] フィールドに、同期に必要な経過時間（分）を入力します。

（注） このオプションの値を大きくすると、大規模なネットワークのパフォーマンスを向上できます。

ステップ 7 [Adaptive Profiles - Networks] フィールドに、適応型プロファイルを使用するネットワーク内のホストを識別する、特定のIPアドレス、アドレスブロック、または変数、またはこれらのアドレス指定方法を含むカンマ区切りのリストを入力します。
変数の設定の詳細については、変数セットの操作 （38 ページ）を参照してください。

ステップ 8 [OK] をクリックして設定内容を維持します。



第 21 章

侵入ポリシーの開始

この章では、単純なカスタム侵入ポリシーの作成方法について説明します。この章には、侵入ポリシーの管理（編集、比較など）に関する基本情報も記載されています。

侵入ポリシーについて

侵入ポリシーは定義済みの侵入検知のセットであり、セキュリティ違反についてトラフィックを検査し、インライン展開の場合は、悪意のあるトラフィックをブロックまたは変更することができます。侵入ポリシーは、アクセス コントロール ポリシーによって呼び出され、システムの最終防御ラインとして、トラフィックが宛先に到達することを許可するかどうかを判定します。

シスコでは ASA FirePOWER モジュールで複数の侵入ポリシーを提供しています。システムによって提供されるポリシーを使用することで、シスコ脆弱性調査チーム（VRT）の経験を活用できます。これらのポリシーに対して、VRT は侵入およびプリプロセッサ ルールの状態（有効または無効）を設定し、他の詳細設定の初期設定も行います。ルールを有効にすると、ルールに一致するトラフィックに対して侵入イベントが生成されます（さらに、必要に応じてトラフィックがブロックされます）。ルールを無効にすると、ルールの処理が停止されます。

ヒント システム付属の侵入ポリシーとネットワーク分析ポリシーには同じような名前が付いていますが、異なる設定が含まれています。たとえば、「Balanced Security and Connectivity」ネットワーク分析ポリシーと「Balanced Security and Connectivity」侵入ポリシーは連携して動作し、どちらも侵入ルールのアップデートで更新できます。ただし、ネットワーク分析ポリシーは主に前処理オプションを管理し、侵入ポリシーは主に侵入ルールを管理します。ネットワーク分析ポリシーと侵入ポリシーについて（297ページ）には、ネットワーク分析ポリシーと侵入ポリシーが連携してトラフィックを検査するしくみの概要、およびナビゲーション パネルの使用、競合の解決、変更のコミットに関する基本事項が記載されています。

カスタム侵入ポリシーを作成すると、以下を実行できます。

- ルールを有効化/無効化することに加え、独自のルールを作成して追加し、検出を調整する。
- 外部アラート、センシティブ データの前処理、グローバル ルールのしきい値設定など、さまざまな詳細設定を設定する。
- レイヤを基本構成要素として使用し、複数の侵入ポリシーを効率的に管理する。

留意事項として、侵入ポリシーを調整する場合（特にルールを有効化して追加する場合）、一部の侵入ルールでは、最初に特定の方法でトラフィックをデコードまたは前処理する必要があります。侵入ポリシーによって検査される前に、パケットはネットワーク分析ポリシーの設定に従って前処理されます。必要なプリプロセッサを無効にすると、システムは自動的に現在の設定でプリプロセッサを使用します。ただし、ネットワーク分析ポリシーのユーザ インターフェイスではプリプロセッサは無効のままになります。

（注） 前処理と侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは、相互補完する**必要があります**。前処理の調整、特に複数のカスタム ネットワーク分析ポリシーを使用して調整することは、**高度な**タスクです。詳細については、カスタム ポリシーの制限 （310 ページ）を参照してください。

カスタム侵入ポリシーを設定した後、それを 1 つ以上のアクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルト アクションに関連付けることによって、カスタム侵入ポリシーをアクセス コントロール設定の一部として使用できます。これによって、システムは、最終宛先に渡す前に、特定の許可されたトラフィックを侵入ポリシーによって検査します。変数セットを侵入ポリシーと組み合わて使用することにより、ホーム ネットワークと外部ネットワークに加えて、必要に応じてネットワーク上のサーバを正確に反映させることができます。詳細については、侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御 （171 ページ）を参照してください。

カスタム侵入ポリシーの作成

ライセンス：Protection

新しい侵入ポリシーを作成する場合は、、一意の名前を付けて基本ポリシーを指定し、ドロップ動作を指定する必要があります。

基本ポリシーは侵入ポリシーのデフォルト設定を定義します。新しいポリシーの設定の変更は、基本ポリシーの設定を変更するのではなく、オーバーライドします。システム付属のポリシーまたはカスタムポリシーを基本ポリシーとして使用できます。詳細については、基本レイヤについて （319 ページ）を参照してください。

侵入ポリシーのドロップ動作、または[Drop when Inline]の設定によって、廃棄ルール（ルール状態が[Drop and Generate Events]に設定されている侵入ルールまたはプリプロセッサルール）、およびトラフィックに影響を与えるその他の侵入ポリシー設定のシステムにおける処理方法が決まります。悪意のあるパケットをドロップまたは置き換える場合は、インライン展開でドロップ動作を有効にする必要があります。パッシブ展開では、ドロップ動作に関わらず、システムはトラフィック フローに影響を与えることはできません。詳細については、インライン展開でのドロップ動作の設定 （347 ページ）を参照してください。

侵入ポリシーを作成するには、以下を行います。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ヒント 別の ASA FirePOWER モジュールからポリシーをインポートすることもできます。設定のインポートおよびエクスポート （617 ページ）参照してください。

ステップ 2 [Create Policy] をクリックします。

別のポリシー内に未保存の変更が存在する場合は、[Intrusion Policy] ページに戻るかどうか尋ねられたときに [Cancel] をクリックします。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定 （314 ページ）を参照してください。

[Create Intrusion Policy] ポップアップ ウィンドウが表示されます。

ステップ 3 [Name] に一意のポリシー名を入力し、オプションで [Description] にポリシーの説明を入力します。

ステップ 4 [Base Policy] で最初の基本ポリシーを指定します。

システム付属のポリシーまたはカスタム ポリシーを基本ポリシーとして使用できます。

注意 シスコの担当者から指示された場合を除き、Experimental Policy 1は使用しないでください。シスコでは、試験用にこのポリシーを使用します。

ステップ 5 インライン展開でのシステムのドロップ動作を設定します。

- 侵入ポリシーによるトラフィックへの影響およびイベントの生成を許可するには、[Drop when Inline] を有効にします。

- 侵入ポリシーによるトラフィックへの影響を回避し、イベントの生成のみを許可するには、[Drop when Inline] を無効にします。

ステップ 6 ポリシーを作成します。

- 新しいポリシーを作成して、[Intrusion Policy] ページに戻るには、[Create Policy] をクリックします。新しいポリシーには基本ポリシーと同じ設定項目が含まれています。
- ポリシーを作成し、高度な侵入ポリシー エディタでそれを開いて編集するには、[Create and Edit Policy] をクリックします（侵入ポリシーの編集 （345 ページ）を参照）。

侵入ポリシーの管理

ライセンス：Protection

[Intrusion Policy] ページ（[Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy]）で、現在のカスタム侵入ポリシーを次の情報とともに確認できます。

- ポリシーが最終変更された日時（ローカル タイム）
- インライン展開でトラフィックをドロップおよび変更できる [Drop when Inline] 設定を有効にするかどうか
- トラフィックの検査に侵入ポリシーを使用しているアクセス コントロール ポリシー
- ポリシーに保存されていない変更があるかどうか

[Intrusion Policy] ページのオプションを使用して、次の表のアクションを実行できます。

表 *50* : 侵入ポリシー管理操作

目的	操作	参照先
新しい侵入ポリシーを作成する	[Create Policy] をクリックします。	カスタム侵入ポリシーの作成 （343 ページ）
既存の侵入ポリシーを編集する	編集アイコン（  ）をクリックします。	侵入ポリシーの編集 （345 ページ）
侵入ポリシーを再適用する	適用アイコン（  ）をクリックします。	侵入ポリシーの適用 （349 ページ）
侵入ポリシーをエクスポートして別の ASA FirePOWER モジュールにインポートする	エクスポートアイコン（  ）をクリックします。	設定のエクスポート （617 ページ）

目的	操作	参照先
侵入ポリシーの現在の設定を示す PDF レポートを表示する	レポートアイコン（  ）をクリックします。	現在の侵入設定のレポートの生成 （350 ページ）
2 つの侵入ポリシーまたは同じポリシーの 2 つのリビジョンの設定を比較する	[Compare Policies] をクリックします。	2 つの侵入ポリシーまたはリビジョンの比較 （351 ページ）
侵入ポリシーを削除する	削除アイコン（  ）をクリックし、ポリシーを削除することを確認します。アクセス コントロール ポリシーが参照している侵入ポリシーは削除できません。	

侵入ポリシーの編集

ライセンス：Protection

新しい侵入ポリシーポリシーを作成すると、そのポリシーには基本ポリシーと同じ侵入ルールと詳細設定が含まれます。次の表では、侵入ポリシーの編集時に実行する最も一般的な操作について説明しています。

表 *51* : 侵入ポリシーの編集操作

目的	操作	参照先
インライン展開での別のドロップ動作を指定する	[Policy Information] ページの [Drop when Inline] チェック ボックスをオンまたはオフにします。	インライン展開でのドロップ動作の設定 （347 ページ）
基本ポリシーを変更する	[Policy Information] ページの [Base Policy] ドロップダウン リストから、基本ポリシーを選択します。	基本ポリシーの変更 （320 ページ）
基本ポリシーの設定を表示する	[Policy Information] ページで [Manage Base Policy] をクリックします。	基本レイヤについて （319 ページ）
侵入ルールを表示または設定する	[Policy Information] ページで [Manage Rules] をクリックします。	侵入ポリシー内のルールの表示 （357 ページ）
現在のルール状態によってフィルタリングした侵入ルールのビューを表示し、必要に応じて、これらのルールを設定する	[Policy Information] ページで、[Manage Rules] の下の [Generate Events] または [Drop and Generate Events] に設定されているルールの番号の横にある [View] をクリックします。	侵入ポリシー内のルールのフィルタ処理 （365 ページ）

目的	操作	参照先
詳細設定を有効化、無効化、または編集する	ナビゲーション パネルで [Advanced Settings] をクリックします。	侵入ポリシーの詳細設定 （348 ページ）
ポリシー層を管理する	ナビゲーション パネルで [Policy Layers] をクリックします。	ネットワーク分析ポリシーまたは侵入ポリシー レイヤでのレイヤの使用 （317 ページ）

留意事項として、侵入ポリシーを調整する場合（特にルールを有効化して追加する場合）、一部の侵入ルールでは、最初に特定の方法でトラフィックをデコードまたは前処理する必要があります。侵入ポリシーによって検査される前に、パケットはネットワーク分析ポリシーの設定に従って前処理されます。必要なプリプロセッサを無効にすると、システムは自動的に現在の設定でプリプロセッサを使用します。ただし、ネットワーク分析ポリシーのユーザ インターフェイスではプリプロセッサは無効のままになります。

（注） 前処理と侵入インスペクションは非常に密接に関連しているため、単一パケットを検査するネットワーク分析ポリシーと侵入ポリシーは、相互補完する**必要があります**。前処理の調整、特に複数のカスタム ネットワーク分析ポリシーを使用して調整することは、**高度な**タスクです。詳細については、カスタム ポリシーの制限 （310 ページ）を参照してください。

システムは、1 つの侵入ポリシーをキャッシュします。侵入ポリシーの編集中に、任意のメニューまたは別のページへの他のパスを選択した場合、変更内容はそのページを離れてもシステム キャッシュにとどまります。上の表に示す実行可能アクションの他に、ネットワーク分析ポリシーと侵入ポリシーについて （297 ページ）では、競合の解決および変更の確定に関する情報を記載しています。

侵入ポリシーの編集方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2 設定する侵入ポリシーの横にある編集アイコン（）をクリックします。

侵入ポリシー エディタが開き、[Policy Information] ページとその左端にナビゲーション パネルが表示されます。

ステップ 3 ポリシーを編集します。上記に要約されているいずれかの操作を実行します。

ステップ 4 ポリシーの保存、編集の続行、変更の破棄を行うか、またはシステム キャッシュで変更をそのままにしながら終了します。詳細については、競合の解決とポリシー変更の確定 （314 ページ）を参照してください。

インライン展開でのドロップ動作の設定

ライセンス：Protection

インライン展開では、侵入ポリシーによってトラフィックを変更したりブロックすることができます。

- 廃棄ルールを使用すると、一致したパケットをドロップして、侵入イベントを生成できます。侵入またはプリプロセッサの廃棄ルールを設定するには、そのステータスを [Drop and Generate Events] に設定します（ルール状態の設定 （377 ページ）を参照）。
- 侵入ルールでは、replace キーワードを使用して悪意のあるコンテンツを置き換えることができます。

侵入ルールがトラフィックに影響を与える場合、廃棄ルールおよびコンテンツを置換するルールを正しく設定し、システムをインラインで正しく展開する必要があります。最後に、侵入ポリシーのドロップ動作、または [Drop when Inline] 設定を有効にする必要があります。

（注） FTP を介してマルウェア ファイルの転送をブロックするには、ネットワーク ベースの高度なマルウェア防御（AMP）を設定するだけではなく、アクセス コントロール ポリシーのデフォルトの侵入ポリシーで [Drop when Inline] を有効にする必要があります。

実際にトラフィックに影響を与えることなく、設定がインライン展開でどのように機能するかを評価する必要がある場合は、ドロップ動作を無効化できます。その場合、システムは侵入イベントを生成しますが、廃棄ルールをトリガーしたパケットをドロップしません。結果を確認したら、ドロップ動作を有効化できます。

パッシブ展開では、ドロップ動作に関わらず、システムはトラフィックに影響を与える可能性はありません。つまり、パッシブ展開では、[Drop and Generate Events] に設定されたルールは [Generate Events] に設定されたルールと同様に動作します。システムは侵入イベントを生成しますが、パケットをドロップできません。

侵入イベントを表示すると、ワークフローにインライン結果が含まれている場合があり、トラフィックが実際にドロップされたか、または単にドロップされるはずだったかが示されます。パケットが廃棄ルールに一致した場合、インライン結果は次のようになります。

- [Dropped]：ドロップ動作が有効な適切に設定されたインライン展開でパケットがドロップされた場合。
- [Would have dropped]：デバイスがパッシブ展開されているか、ドロップ動作が無効化されているために、パケットがドロップされなかった場合。展開に関係なく、システムがプルーニングしている間に検出されるパケットのインライン結果は、常に Would have dropped です。

インライン展開での侵入ポリシーのドロップ動作の設定方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2 編集するポリシーの横にある編集アイコンをクリックします。

[Policy Information] ページが表示されます。

ステップ 3 ポリシーのドロップ動作を設定します。

- 侵入ルールによるトラフィックへの影響およびイベントの生成を許可するには、[Drop when Inline] を有効にします。
- 侵入ルールによるトラフィックへの影響を回避し、イベントの生成のみを許可するには、[Drop when Inline] を無効にします。

ステップ 4 ポリシーの保存、編集の続行、変更の破棄を行うか、またはシステム キャッシュで変更をそのままにしながら終了します。詳細については、競合の解決とポリシー変更の確定（314ページ）を参照してください。

侵入ポリシーの詳細設定

ライセンス：Protection

侵入ポリシーの詳細設定を設定するには、特定の専門知識が必要です。デフォルトで有効になる詳細設定や、詳細設定ごとのデフォルトは、侵入ポリシーの基本ポリシーに応じて決まります。

侵入ポリシーのナビゲーション パネルで [Advanced Settings] を選択すると、ポリシーの詳細設定がタイプ別に一覧表示されます。[Advanced Settings] ページでは、侵入ポリシーの詳細設定を有効または無効にしたり、詳細設定の設定ページにアクセスすることができます。

詳細設定を行うには、それを有効にする必要があります。詳細設定を有効にすると、その詳細設定に関する設定ページへのサブリンクがナビゲーション パネル内の [Advanced Settings] リンクの下に表示され、この設定ページへの [Edit] リンクが [Advanced Settings] ページ上の詳細設定の横に表示されます。

ヒント 詳細設定の設定を基本ポリシーの設定に戻すには、詳細設定の設定ページで [Revert to Defaults] をクリックします。プロンプトが表示されたら、復元することを確認します。

詳細設定を無効にすると、サブリンクと [Edit] リンクは表示されなくなりますが、設定は保持されます。侵入ポリシーの一部の設定（センシティブ データ ルール、侵入ルールの SNMP アラート）では、詳細設定を有効化して適切に設定する必要があります。このように誤って設定された侵入ポリシーは保存できません（競合の解決とポリシー変更の確定（314ページ）を参照）。

詳細設定を変更する場合、変更する設定と、その変更がネットワークに及ぼす可能性のある影響について理解していることが必要です。次の項では、詳細設定ごとに固有の設定の詳細情報へのリンクを記述します。

特定の脅威の検出（Specific Threat Detection）

機密データ プリプロセッサは、ASCII テキストのクレジット カード番号や社会保障番号などの機密データを検出します。

特定の脅威（Back Orifice 攻撃、何種類かのポートスキャン、および過剰なトラフィックによってネットワークを過負荷状態に陥らせようとするレートベース攻撃）を検出するプリプロセッサは、ネットワーク分析ポリシーで設定します。

侵入ルールしきい値（Intrusion Rule Thresholds）

グローバル ルールのしきい値を設定すると、しきい値を使用して、システムが侵入イベントを記録したり表示したりする回数を制限できるので、多数のイベントでシステムが圧迫されないようにすることができます。詳細については、を参照してください。

外部レスポンス（External Responses）

ユーザインターフェイス内での侵入イベントをさまざまな形式で表示することに加えて、システムログ（syslog）ファシリティへのロギングを有効にしたり、イベント データを SNMP トラップ サーバに送信したりできます。ポリシーごとに、侵入イベントの通知限度を指定したり、外部ロギング ファシリティに対する侵入イベントの通知をセットアップしたり、侵入イベントへの外部応答を設定したりできます。

侵入ポリシーの適用

ライセンス：Protection

アクセス コントロールを使用して侵入ポリシーを適用した場合は（設定変更の導入 （92 ページ）を参照）、その侵入ポリシーをいつでも再適用できます。これにより、アクセス コントロール ポリシーを再適用せずに、監視対象ネットワーク上で侵入ポリシーを変更できます。再適用中は、比較レポートを表示して、最後に侵入ポリシーが適用されてから加えられた変更を確認できます。

侵入ポリシーを再適用する際は次の点に注意してください。

- 侵入ポリシーの再適用タスクは、定期的に実行するようにスケジュールできます（侵入ポリシーの適用の自動化 （539 ページ）を参照）。
- ルール更新をインポートするときに、インポートの完了後に自動的に侵入ポリシーを適用できます。このオプションを有効にしなかった場合は、ルール更新によって変更されたポリシーを手動で再適用する必要があります。詳細については、「ルール更新とローカル ルール ファイルのインポート （582 ページ）」を参照してください。

侵入ポリシーを再適用するには、以下を行います。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2 再適用するポリシーの横にある適用アイコン（）をクリックします。

[Reapply Intrusion Policy] ウィンドウが表示されます。

ステップ 3 [Reapply] をクリックします。

ポリシーが再適用されます。タスク キューを使用して適用のステータスをモニタできます（[Monitoring] > [ASA FirePOWER Monitoring] > [Task Status]）。詳細については、「タスク キューの表示 （625 ページ）」を参照してください。

現在の侵入設定のレポートの生成

ライセンス：Protection

侵入ポリシー レポートは、特定の時点におけるポリシー設定の記録です。システムは、基本ポリシー内の設定とポリシー層の設定を統合して、基本ポリシーに起因する設定とポリシー層に起因する設定を区別しません。

このレポートは監査目的に使用したり、現行の設定を調べるために使用できます。レポートには次の情報が含まれています。

表 *52*：侵入ポリシー レポートのセクション

セクション	説明
Policy Information	ポリシーの名前と説明、侵入ポリシーを最後に変更したユーザの名前、ポリシーが最後に変更された日時が記載されます。インライン展開でのパケットのドロップが有効になっているか無効になっているか、現在のルール更新のバージョン、基本ポリシーが現在のルール更新にロックされているかどうかも記載されます。
Advanced Settings	すべての有効化されている侵入ポリシーの設定項目およびその設定を一覧表示します。
Rules	有効になっているすべてのルールとその動作を一覧表示します。

また、2 つの侵入ポリシーまたは同じ侵入ポリシーの 2 つのリビジョンを比較する比較レポートを生成することもできます。詳細については、2 つの侵入ポリシーまたはリビジョンの比較（351 ページ）を参照してください。

侵入ポリシー レポートを表示するには、以下を行います。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2 レポートを生成する侵入ポリシーの横にあるレポート アイコン（  ）をクリックします。侵入ポリシー レポートを生成する前に未確定の変更をコミットするのを忘れないでください。コミットされた変更だけがレポートに表示されます。

システムが侵入ポリシー レポートを生成します。コンピュータにレポートを保存するように求められます。

2 つの侵入ポリシーまたはリビジョンの比較

ライセンス：Protection

ポリシー変更が組織の標準に準拠しているかどうかを確認するため、またはシステムのパフォーマンスを最適化するために、2 つの侵入ポリシーの違いを確認することができます。アクセス可能な侵入ポリシーの場合は、2 つの侵入ポリシーまたは同じ侵入ポリシーの 2 つのリビジョンを比較できます。比較した後に、必要に応じて、2 つのポリシーまたはポリシー リビジョン間の違いを記録した PDF レポートを生成できます。

侵入ポリシーを比較するために使用できるツールは 2 つあります。

- 比較ビューには、2 つの侵入ポリシーまたは侵入ポリシー リビジョン間の違いだけが並べて表示されます。各ポリシーの名前は比較ビューの左右のタイトル バーに表示されます。

これを使用して、ユーザ インターフェイスで相違点を強調表示したまま、両方のポリシーのリビジョンを表示し移動することができます。

- 比較レポートは、2 つの侵入ポリシーまたは侵入ポリシー リビジョン間の違いのみを記録したもので、PDF であるという以外は、侵入ポリシー レポートと類似した形式になっています。

これは、ポリシー比較を保存、コピー、出力、および共有して、詳しく調査するために使用できます。

侵入ポリシー比較ビューの使用

ライセンス：Protection

比較ビューには、両方の侵入ポリシーまたはポリシー リビジョンが並べて表示されます。それぞれのポリシーまたはポリシー リビジョンは、比較ビューの左右のタイトル バーに表示された名前で識別されます。最終変更時刻と最終変更ユーザが、ポリシー名の右側に表示されます。[Intrusion Policy] ページにはポリシーが最後に変更された時刻が現地時間で表示されますが、侵入ポリシー レポートでは変更時刻が UTC でリストされることに注意してください。2 つの侵入ポリシーまたはポリシー リビジョン間の違いが強調表示されます。

- 青色は強調表示された設定が 2 つのポリシーまたはポリシー リビジョンで違うことを意味します。違いは赤色のテキストで表示されます。

- 緑色は強調表示された設定が1つのポリシーまたはポリシー リビジョンにだけ存在することを意味します。

次の表内の操作を実行できます。

表 *53*：侵入ポリシー比較ビューの操作

目的	操作
変更に個別にナビゲートする	またはタイトル バーの上にある [Previous] または [Next] をクリックします。
新しい侵入ポリシー比較ビューを生成する	[New Comparison] をクリックします。 [Select Comparison] ウィンドウが表示されます。詳細については、「侵入ポリシー比較レポートの使用 （352ページ）」を参照してください。
侵入ポリシー比較レポートを生成する	[Comparison Report] をクリックします。 ポリシー比較レポートは、2つのポリシーまたはリビジョンの相違点だけがリストされた PDF です。

侵入ポリシー比較レポートの使用

ライセンス：Protection

侵入ポリシー比較レポートは、PDF で提供される、侵入ポリシー比較ビューで特定された2つの侵入ポリシー間または同じ侵入ポリシーの2つのリビジョン間のすべての違いを記録したものです。このレポートは、2 つの侵入ポリシー構成間の違いをさらに調査し、その結果を保存して共有するために使用できます。

侵入ポリシー比較レポートは、アクセス可能な任意の侵入ポリシーの比較ビューから生成できます。侵入ポリシー レポートを生成する前に未確定の変更をコミットするのを忘れないでください。コミットされた変更だけがレポートに表示されます。

侵入ポリシー比較レポートの形式は1つの例外（侵入ポリシー レポートには侵入ポリシー内のすべての設定が含まれる）を除いて侵入ポリシー レポートと同じであり、侵入ポリシー比較レポートにはポリシー間で異なる設定のみがリストされます。

構成に応じて、侵入ポリシー比較レポートに表 52：侵入ポリシー レポートのセクション （350ページ）の表に示す 1 つ以上のセクションを含めることができます。

ヒント 同様の手順を使用して、SSL ポリシー、アクセス コントロール ポリシー、ネットワーク分析ポリシー、ファイル ポリシー、またはシステム ポリシーを比較できます。

- 2 つの侵入ポリシーまたは同じポリシーの 2 つのリビジョンを比較するには、以下を行います。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2 [Compare Policies] をクリックします。

[Select Comparison] ウィンドウが表示されます。

ステップ 3 [Compare Against] ドロップダウン リストから、比較するタイプを次のように選択します。

- 異なる 2 つのポリシーを比較するには、[Other Policy] を選択します。
- 同じポリシーの 2 つのリビジョンを比較するには、[Other Revision] を選択します。

侵入ポリシー レポートを生成する前に変更をコミットするのを忘れないでください。コミットされた変更だけがレポートに表示されます。

ステップ 4 選択した比較タイプに応じて、次のような選択肢があります。

- 異なる 2 つのポリシーを比較する場合、[Policy A] および [Policy B] ドロップダウン リストから比較するポリシーを選択します。
- 同じポリシーの 2 つのリビジョンを比較する場合は、[Policy] ドロップダウン リストからポリシーを選択してから、[Revision A] ドロップダウン リストと [Revision B] ドロップダウン リストから比較するリビジョンを選択します。

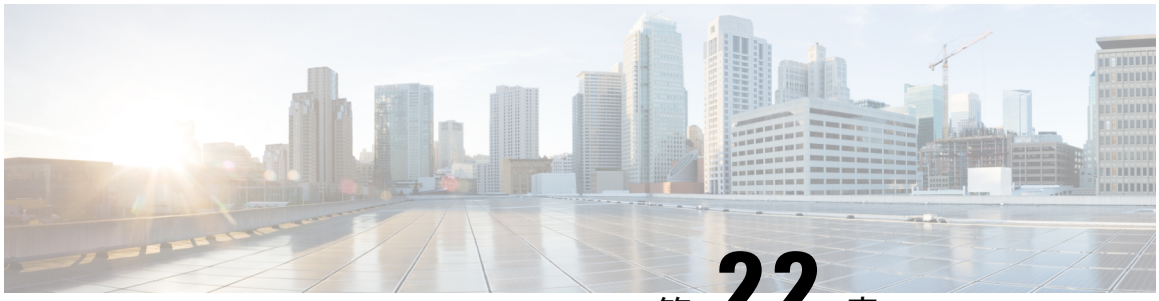
ステップ 5 侵入ポリシー比較ビューを表示するには、[OK] をクリックします。

比較ビューが表示されます。

ステップ 6 侵入ポリシー比較レポートを生成するには、[Comparison Report] をクリックします。

ステップ 7 侵入ポリシー レポートが表示されます。コンピュータにレポートを保存するように求められます。

次のタスク



第 22 章

ルールを使用した侵入ポリシーの調整

侵入ポリシーの [Rules] ページを使用して、共有オブジェクト ルール、標準テキスト ルール、プリプロセッサ ルールに関するルール状態とその他の設定を構成できます。

ルールは、ルール状態を [Generate Events] または [Drop and Generate Events] に設定することによって有効にします。ルールを有効にすると、システムがそのルールと一致するトラフィックに対するイベントを生成します。ルールを無効にすると、ルールの処理が停止されます。オプションで、インライン展開で [Drop and Generate Events] に設定されたルールによって、一致するトラフィックに対するイベントが生成され、そのトラフィックが破棄されるように、侵入ポリシーを設定できます。詳細については、「インライン展開でのドロップ動作の設定（347ページ）」を参照してください。パッシブ展開では、[Drop and Generate Events] に設定されたルールによって、一致するトラフィックに対するイベントが生成されるだけです。

ルールのサブセットを表示するようにルールをフィルタ処理することによって、ルール状態やルール設定を変更するルールのセットを正確に選択できます。

侵入ルールまたはルールの引数がプリプロセッサの無効化を必要とする場合、ネットワーク分析ポリシーのユーザインターフェイスではプリプロセッサが無効化されたままになりますが、システムは自動的に現在の設定でプリプロセッサを使用します。詳細については、カスタム ポリシーの制限（310 ページ）を参照してください。

詳細については、次の項を参照してください。

- 侵入防御ルール タイプについて（356ページ）では、侵入ポリシーで表示または設定可能な侵入ルールとプリプロセッサ ルールについて説明します。
- 侵入ポリシー内のルールの表示（357ページ）では、[Rules] ページでルールの順序を変更したり、ページ上のアイコンを解釈したり、ルール詳細に焦点を当てたりするための方法について説明します。
- 侵入ポリシー内のルールのフィルタ処理（365 ページ）では、ルール フィルタを使用して、ルール設定を適用するルールを見つける方法について説明します。
- ルール状態の設定（377ページ）では、[Rules] ページでルールを有効化または無効化する方法について説明します。

- ポリシー単位の侵入イベント通知のフィルタ処理（380ページ）では、特定のルールに対するイベントフィルタリングしきい値の設定方法と特定のルールの抑制方法について説明します。
- 動的ルール状態の追加（388ページ）では、一致するトラフィックでレート異常が検出されたときに動的にトリガーとして使用されるルール状態の設定方法について説明します。
- SNMP アラートの追加（392 ページ）では、SNMP アラートを特定のルールに関連付ける方法について説明します。
- ルール コメントの追加（393ページ）では、侵入ポリシー内のルールにコメントを追加する方法について説明します。

- 侵入防御ルール タイプについて （356 ページ）
- 侵入ポリシー内のルールの表示 （357 ページ）
- 侵入ポリシー内のルールのフィルタ処理 （365 ページ）
- ルール状態の設定 （377 ページ）
- ポリシー単位の侵入イベント通知のフィルタ処理 （380 ページ）
- 動的ルール状態の追加 （388 ページ）
- SNMP アラートの追加 （392 ページ）
- ルール コメントの追加 （393 ページ）

侵入防御ルール タイプについて

ライセンス：Protection

侵入ポリシーには、侵入ルールとプリプロセッサ ルールという 2 つのルール タイプが含まれています。

侵入ルールは、ネットワーク上の脆弱性を悪用する試みを検出するキーワードと引数の指定されたセットで、ネットワーク トラフィックを分析してルール内の基準が満たされているかどうかをチェックします。システムが各ルール内で指定された条件とパケットを照らし合わせます。そして、パケットデータとルール内で指定されたすべての条件が一致した場合に、ルールがトリガーとして使用されます。システムには、シスコ脆弱性調査チーム（VRT）が作成した次の2種類の侵入ルールがあります。共有オブジェクト ルールは、コンパイルされているため変更できません（送信元ポート、宛先ポート、IP アドレスなどのルール見出し情報を除く）。標準テキスト ルールは、ルールの新しいカスタム インスタンスとして保存および変更できます。

システムには、プリプロセッサに関連付けられたルールであるプリプロセッサ ルールとパケット デコーダ検出オプションも付属しています。プリプロセッサ ルールはコピーまたは編集できません。ほとんどのプリプロセッサルールがデフォルトで無効になっているため、システムにプリプロセッサルールに対するイベントの生成とインライン展開での違反パケットの破棄を指示する場合は、これらのルールを有効にする（つまり、[Generate Events] または [Drop and Generate Events] に設定する）必要があります。

VRT が、システムに付属のデフォルト侵入ポリシー用のシスコの共有オブジェクト ルール、標準テキスト ルール、およびプリプロセッサ ルールのデフォルト ルールの状態を決定します。

次の表に、ASA FirePOWER モジュールに付属している各ルール タイプの説明を示します。

表 *54 :* ルール タイプ

タイプ	Description
共有オブジェクトのルール	C ソース コードからコンパイルされたバイナリ モジュールとして配布される、シスコ脆弱性調査チーム（VRT）によって作成された侵入ルール。共有オブジェクト ルールを使用すると、標準テキスト ルールではできない方法で攻撃を検出できます。共有オブジェクト ルール内のルール キーワードと引数は変更できません。実行できるのは、ルールで使用されている変数の変更、送信元ポート、宛先ポート、IP アドレスなどの要素の変更、およびルールの新しいインスタンスのカスタム共有オブジェクトとしての保存だけです。共有オブジェクト ルールの GID（ジェネレータ ID）は 3 です。
標準テキスト ルール	VRT によって作成された侵入ルール、コピーされて新しいカスタム ルールとして保存された侵入ルール、ルール エディタを使用して作成された侵入ルール、またはユーザがローカル マシン上で作成してインポートしたローカル ルールとしてインポートされた侵入ルール。VRT によって作成された標準ルール内のルール キーワードと引数は変更できません。実行できるのは、ルールで使用されている変数の変更、送信元ポート、宛先ポート、IP アドレスなどの要素の変更、およびルールの新しいインスタンスのカスタム標準ルールとしての保存だけです。詳細については、ローカル ルール ファイルのインポート （589 ページ）を参照してください。VRT によって作成された標準テキスト ルールの GID（ジェネレータ ID）は 1 です。ルール エディタを使用して作成した、またはローカル ルールとしてインポートしたカスタム標準テキストルールには 1000000 以上の SID（シグニチャ ID）が割り当てられます。
プリプロセッサ ルール	パケット デコーダの検出オプション、または ASA FirePOWER モジュールに付属のプリプロセッサの 1 つに関連付けられたルール。プリプロセッサ ルールによってイベントを生成するには、プリプロセッサ ルールを有効にする必要があります。このルールには、デコーダ固有またはプリプロセッサ固有の GID（ジェネレータ ID）が割り当てられます。

侵入ポリシー内のルールの表示

ライセンス：Protection

侵入ポリシー内のルールの表示方法を調整したり、複数の条件によってルールをソートできます。特定のルールの詳細を表示して、ルール設定、ルール ドキュメント、およびその他のルール仕様を確認することもできます。

[Rules] ページには次の 4 つの主な機能領域があります。

- フィルタリング機能：詳細については、侵入ポリシー内のルールのフィルタ処理 （365 ページ）を参照してください。

- ルール属性メニュー：詳細については、ルール状態の設定 （377ページ）、ポリシー単位の侵入イベント通知のフィルタ処理 （380ページ）動的ルール状態の追加 （388ページ）、SNMP アラートの追加 （392 ページ）、およびルール コメントの追加 （393 ページ）を参照してください。
- ルール一覧：詳細については、表 55 : [Rules] ページの列 （358 ページ）の表を参照してください。
- ルールの詳細：詳細については、ルール詳細の表示 （360ページ）を参照してください。

さまざまな基準に基づいてルールをソートすることもできます。詳細については、ルール画面のソート （359 ページ）を参照してください。

カラム見出しとして使用されているアイコンは、設定項目にアクセスするためのメニューバー内のメニューに対応していることに注意してください。たとえば、[Rule State] メニューは、[Rule State] カラムと同じアイコン（  ）でマークされています。

次の表に、[Rules] ページのカラムの説明を示します。

表 *55 : [Rules]* ページの列

見出し	説明	詳細情報の参照先
GID	ルールのジェネレータ ID（GID）を表す整数。	イベントの表示 （487 ページ）
SID	ルールの一意の識別子として機能する Snort ID （SID）を表す整数。	イベントの表示 （487 ページ）
Message	このルールによって生成されるイベントに含まれるメッセージ。ルールの名前としても機能します。	
	ルールのルール状態。次の 3 つの中のいずれか。 • drop and generate events  > • generate events  • disable  ルール状態アイコンをクリックすることによって、ルールの [Set rule state] ダイアログボックスにアクセスできることに注意してください。	ルール状態の設定 （377 ページ）
	ルールに適用されるイベントしきい値やイベント抑制などのイベント フィルタ。	ポリシー単位の侵入イベント通知のフィルタ処理 （380 ページ）
	ルールの動的ルール状態。指定されたレート異常が発生した場合に有効になります。	動的ルール状態の追加 （388 ページ）

見出し	説明	詳細情報の参照先
	ルールに対して設定されたアラート（現在はSNMPアラートのみ）。	SNMPアラートの追加（392ページ）
	ルールに追加されたコメント。	ルール コメントの追加（393ページ）

階層ドロップダウン リストを使用して、ポリシー内の他の階層の [Rules] ページに切り替えることもできます。ポリシーに階層を追加しなかった場合にドロップダウンリストに表示される編集可能なビューはポリシーの [Rules] ページと、元は My Changes という名前だったポリシー階層の [Rules] ページだけです。これらのビューの一方を変更すると、もう一方も同じように変更されることに注意してください。詳細については、ネットワーク分析ポリシーまたは侵入ポリシー レイヤでのレイヤの使用（317ページ）を参照してください。ドロップダウン リストには、読み取り専用の基本ポリシーの [Rules] ページも表示されます。基本ポリシーの詳細については、基本レイヤについて（319 ページ）を参照してください。

侵入ポリシー内のルールを表示する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（314 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3 [Policy Information] ページで [Rules] をクリックします。

[Rules] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ナビゲーション パネルの境界線の上にある [Rules] を選択すると、同じルール一覧が表示されることに注意してください。このビューでポリシー内のすべてのルール属性を表示して設定できます。

ルール画面のソート

ライセンス：Protection

[Rules] ページでは、見出しタイトルまたはアイコンをクリックすることによって、ルールをいずれかのカラムでソートできます。

見出しまたはアイコン上の上矢印（）または下矢印（）は、そのカラムを基準として、その方向にソートが実行されることを意味していることに注意してください。

侵入ポリシー内でルールをソートする方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2 編集するポリシーの横にある編集アイコンをクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定 （314 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3 [Rules] をクリックします。

[Rules] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ステップ 4 ソートの基準とする列の一番上のタイトルまたはアイコンをクリックします。

ルールがそのカラムのカラム見出しに表示された矢印が示す方向でソートされます。反対方向でソートするには、見出しを再度クリックします。ソート順と矢印が反転します。

ルール詳細の表示

ライセンス：Protection

[Rule Detail] ビューで、ルール ドキュメントおよびルール オーバーヘッドを表示できます。また、ルール固有の機能を表示および追加できます。

脆弱性にマップされていないローカル ルールにはオーバーヘッドがないことに注意してください。

表 *56* : ルールの詳細

アイテム	説明	詳細情報の参照先
Summary	ルールの概要。ルール ベースのイベントでは、ルール ドキュメントに概要情報が含まれている場合にこのローが表示されます。	イベントの表示 （487 ページ）
Rule State	ルールの現在のルール状態。ルール状態が設定された階層も示します。	ルール状態の設定 （377 ページ）、ネットワーク分析ポリシーまたは侵入ポリシー レイヤでのレイヤの使用 （317 ページ）
Thresholds	このルールに現在設定されているしきい値と、ルールのしきい値を追加するための機能。	ルールのしきい値の設定 （361 ページ）

アイテム	説明	詳細情報の参照先
Suppressions	このルールに現在設定されている抑制設定と、ルールの抑制を追加するための機能。	ルールの抑制の設定 （362 ページ）
Dynamic State	このルールに現在設定されているレート ベースのルール状態と、ルールの動的ルール状態を追加するための機能。	ルールの動的ルール状態の設定 （363 ページ）
Alerts	このルールに現在設定されているアラートと、ルールのアラートを追加するための機能。現時点では、SNMPアラートのみがサポートされています。	SNMP アラートの追加 （392 ページ）
Comments	このルールに追加されたコメントと、ルールのコメントを追加するための機能。	ルール コメントの追加 （393 ページ）
Documentation	シスコ脆弱性調査チーム（VRT）から提供される現在のルールのルール ドキュメント。	イベントの表示 （487 ページ）

ルール詳細を表示する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定 （314 ページ） を参照してください。

[Policy Information] ページが表示されます。

ステップ 3 [Rules] をクリックします。

[Rules] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ステップ 4 ルール詳細を表示するルールを強調表示します。

ステップ 5 [Show details] をクリックします。

[Rule Detail] ビューが表示されます。詳細を再度非表示にするには、[Hide details] をクリックします。

ヒント [Rules] ビューでルールをダブルクリックして、[Rule Detail] を開くこともできます。

ルールのしきい値の設定

ライセンス：Protection

[Rule Detail] ページで、ルールの単一のしきい値を設定できます。しきい値を追加すると、ルールの既存のしきい値が上書きされます。しきい値設定の詳細については、イベントしきい値の設定 （380 ページ）を参照してください。

無効な値を入力するとフィールドに復元アイコン（）が表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

ルール詳細でしきい値を設定する方法：

ステップ 1 [Thresholds] の横にある [Add] をクリックします。

[Set Threshold] ダイアログボックスが表示されます。

ステップ 2 [Type] ドロップダウンリストから、設定するしきい値のタイプを選択します。

- 指定された期間あたりのイベント インスタンス数に通知を制限する場合は、[Limit] を選択します。
- 指定された期間あたりのイベント インスタンス数ごとに通知を提供する場合は、[Threshold] を選択します。
- 指定されたイベント インスタンス数後に期間あたり 1 回ずつ通知を提供する場合は、[Both] を選択します。

ステップ 3 [Track By] ドロップダウンリストから、[Source] または [Destination] を選択し、送信元または宛先のいずれの IP アドレスでイベント インスタンスを追跡するかを指定します。

ステップ 4 [Count] フィールドに、しきい値として使用するイベント インスタンスの数を入力します。

ステップ 5 [Seconds] フィールドに、イベント インスタンスを追跡する秒単位の期間として 0 ～ 2147483647 の数値を入力します。

ステップ 6 [OK] をクリックします。

システムが、しきい値を追加し、[Event Filtering] カラムのルールの横にイベント フィルタ アイコン（  ）を表示します。ルールに複数のイベント フィルタを追加すると、アイコン上にイベント フィルタの数が表示されます。

ルールの抑制の設定

ライセンス：Protection

[Rule Detail] ページで、ルールの 1 つまたは複数の抑制を設定できます。抑制の詳細については、ルールの抑制の設定 （362 ページ） を参照してください。

無効な値を入力するとフィールドに復元アイコン（）が表示されます。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

ルール詳細で抑制を設定する方法：

ステップ 1 [Suppressions] の横にある [Add] をクリックします。

[Add Suppression] ダイアログボックスが表示されます。

ステップ 2 [Suppression Type] ドロップダウンリストから、次のいずれかのオプションを選択します。

- 選択したルールのイベントを完全に抑制する場合は、[Rule] を選択します。
- 指定した送信元 IP アドレスから送信されるパケットによって生成されるイベントを抑制する場合は、[Source] を選択します。
- 指定した宛先 IP アドレスに送信されるパケットによって生成されるイベントを抑制する場合は、[Destination] を選択します。

ステップ 3 抑制タイプとして [Source] または [Destination] を選択すると、[Network] フィールドが表示されます。[Network] フィールドに、IP アドレス、アドレス ブロック、またはこれらを任意に組み合わせたカンマ区切りのリストを入力します。侵入ポリシーがアクセス コントロール ポリシーのデフォルト アクションに関連付けられている場合は、デフォルト アクション変数セットでネットワーク変数を指定または列挙することもできます。

IPv4 CIDR および IPv6 プレフィックス長アドレス ブロックの使用の詳細については、お使いのバージョンの *Firepower Management Center* コンフィギュレーション ガイドで「Firepower System IP Address Conventions」を参照してください。

ステップ 4 [OK] をクリックします。

抑制条件が追加され、抑制するルールの横にある [Event Filtering] カラムのルールの横にイベント フィルタ アイコンが表示されます。ルールに複数のイベント フィルタを追加した場合は、アイコン上の数字がフィルタの数を示します。

ルールの動的ルール状態の設定

ライセンス：Protection

[Rule Detail] ページで、ルールの 1 つまたは複数の動的ルール状態を設定できます。最初に表示される動的ルール状態に最も高いプライオリティが割り当てられます。2 つの動的ルール状態が競合している場合は、最初のアクションが実行されることに注意してください。動的ルール状態の詳細については、動的ルール状態について （388 ページ）を参照してください。

無効な値を入力するとフィールドに復元アイコン（）が表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

ルール詳細で動的ルール状態を設定する方法：

ステップ 1 [Dynamic State] の横にある [Add] をクリックします。

[Add Rate-Based Rule State] ダイアログボックスが表示されます。

ステップ 2 [Track By] ドロップダウンリストから、ルール一致の追跡方法を指定するオプションを選択します。

- 特定の送信元または送信元のセットからのそのルールのヒット数を追跡する場合は、[Source] を選択します。
- 特定の宛先または宛先のセットへのそのルールのヒット数を追跡する場合は、[Destination] を選択します。
- そのルールのすべての一致を追跡する場合は、[Rule] を選択します。

ステップ 3 オプションで、[Track By] を [Source] または [Destination] に設定した場合は、[Network] フィールドに追跡する各ホストの IP アドレスを入力します。

ステップ 4 [Rate] の隣で、攻撃レートを設定する期間あたりのルール一致の数を指定します。

- [Count] フィールドで、0 ～ 2147483647 の整数を使用して、しきい値として使用するルール一致の数を指定します。
- [Seconds] フィールドで、0 ～ 2147483647 の整数を使用して、攻撃を追跡する期間を表す秒数を指定します。

ステップ 5 [New State] ドロップダウンリストから、条件を満たしたときに実行される新しいアクションを選択します。

- イベントを生成する場合は、[Generate Events] を選択します。
- インライン展開でイベントを生成し、イベントをトリガーしたパケットを破棄する場合、または、パッシブ展開でイベントを生成する場合は、[Drop and Generate Events] を選択します。
- アクションを実行しない場合は、[Disabled] を選択します。

ステップ 6 [Timeout] フィールドに、1 ～ 2147483647（約 68 年）の整数を使用して、新しいアクションを有効にしておく秒数を入力します。タイムアウトが発生すると、ルールが元の状態に戻ります。新しいアクションがタイムアウトしないようにする場合は、0 を指定します。

ステップ 7 [OK] をクリックします。

動的ルール状態が追加され、[Dynamic State] カラムのルールの横に動的状態アイコン（  ）が表示されます。ルールに複数の動的ルール状態フィルタを追加した場合は、アイコン上の数字がフィルタの数を示します。

必須フィールドを空白にした場合は、フィールドに値を入力する必要があることを伝えるエラーメッセージが表示されます。

ルールの SNMP アラートの設定

ライセンス：Protection

[Rule Detail] ページで、ルールの SNMP アラートを設定できます。SNMP アラートの詳細については、SNMP 応答の使用 （512 ページ）を参照してください。

ルール詳細で SNMP アラートを追加する方法：

[Alerts] の横にある [Add SNMP Alert] をクリックします。

アラートが追加され、[Alerting] カラムのルールの横にアラート アイコン（）が表示されます。ルールに複数のアラートを追加した場合は、アイコン上にアラートの数が表示されます。

ルールに関するルール コメントの追加

ライセンス：Protection

[Rule Detail] ページで、ルールに関するルール コメントを追加できます。ルール コメントの詳細については、ルール コメントの追加 （393 ページ）を参照してください。

ルール詳細でコメントを追加する方法：

ステップ 1 [Comments] の横にある [Add] をクリックします。

[Add Comment] ダイアログボックスが表示されます。

ステップ 2 [Comment] フィールドに、ルールに関するコメントを入力します。

ステップ 3 [OK] をクリックします。

コメントが追加され、[Comments] カラムのルールの横にコメント アイコン（）が表示されます。ルールに複数のコメントを追加した場合は、アイコン上の数字がコメントの数を示します。

ヒント ルール コメントを削除するには、ルール コメント セクションで [Delete] をクリックします。侵入ポリシーの変更がコミットされずにコメントがキャッシュされている場合にだけ、コメントを削除できることに注意してください。侵入ポリシーの変更がコミットされた後は、ルール コメントを削除できなくなります。

侵入ポリシー内のルールのフィルタ処理

ライセンス：Protection

[Rules] ページに表示するルールは、1 つの基準または 1 つ以上の基準の組み合わせに基づいてフィルタ処理できます。

作成したフィルタが [Filter] テキスト ボックスに表示されます。フィルタ パネルでキーワードとキーワード引数をクリックしてフィルタを作成できます。複数のキーワードを選択した場合は、システムがそれらを AND ロジックを使用して結合し、複合検索フィルタを生成します。たとえば、[Category] で [preprocessor] を選択してから、[Rule Content] > [GID] の順に選択して「116」と入力すると、プリプロセッサ ルールで、かつ GID が 116 のすべてのルールを取得する「Category: “preprocessor” GID:”116”」というフィルタが返されます。

Category、Microsoft Vulnerabilities、Microsoft Worms、Platform Specific、Preprocessor、および Priority の各フィルタ グループを使用すれば、カンマで区切られたキーワードの複数の引数を送信できます。たとえば、Shift キーを押しながら、[Category] から [os-linux] と [os-windows] を選択すると、os-linux カテゴリまたは os-windows カテゴリ内のルールを取得する「Category:"os-windows,os-linux"」というフィルタを作成できます。

フィルタ パネルを表示するには、表示アイコン（  ）をクリックします。

フィルタ パネルを非表示にするには、非表示アイコンをクリックします。 

侵入ポリシー内のルール フィルタ処理について

ライセンス：Protection

ルール フィルタ キーワードは、ルール状態やイベント フィルタなどのルール設定を適用するルールを見つけやすくします。[Rules] ページのフィルタ パネルで必要な引数を選択することによって、キーワードでフィルタ処理すると同時に、キーワードの引数を選択することができます。

侵入ポリシー ルール フィルタを作成するためのガイドライン

ライセンス：Protection

ほとんどの場合、フィルタを作成するときに、侵入ポリシー内の [Rules] ページの左側にあるフィルタ パネルを使用して必要なキーワード/引数を選択できます。

フィルタ パネルでは、ルール フィルタがルール フィルタ グループに分類されます。多くのルール フィルタ グループにサブ基準が含まれているため、探している特定のルールを簡単に見つけることができます。一部のルール フィルタには複数のレベルが設定されているので、それを展開して個別のルールにドリルダウンできます。

フィルタ パネル内の項目は、場合によって、フィルタ タイプ グループを表したり、キーワードを表したり、キーワードの引数を表したりします。次の経験則をフィルタの作成に役立ててください。

- キーワード（Rule Configuration、Rule Content、Platform Specific、および Priority）以外のフィルタ タイプ グループ見出しを選択すると、そのグループが展開して使用可能なキーワードが一覧表示されます。

基準リスト内のノードをクリックしてキーワードを選択すると、フィルタ処理する引数を指定するためのポップアップ ウィンドウが表示されます。

そのキーワードがすでにフィルタで使用されていた場合は、そのキーワードの既存の引数が指定した引数に置き換えられます。

- キーワード（Category、Classifications、Microsoft Vulnerabilities、Microsoft Worms、Priority、および Rule Update）になっているフィルタ タイプ グループ見出しを選択すると、使用可能な引数が一覧表示されます。

このタイプのグループから項目を選択すると、適用される引数とキーワードがすぐにフィルタに追加されます。キーワードがすでにフィルタ内に存在していた場合は、そのグループに対応するキーワードの既存の引数が置き換えられます。

たとえば、フィルタ パネルの [Category] で [os-linux] をクリックすると、「Category:"os-linux"」がフィルタ テキスト ボックスに追加されます。その後、[Category] で [os-windows] をクリックすると、フィルタが「Category:"os-windows"」に変わります。

- [Rule Content] の下の [Reference] はキーワードであり、その下に特定の参照 ID タイプが列挙されます。いずれかの参照キーワードを選択すると、引数を指定するためのポップアップ ウィンドウが表示され、既存のフィルタにそのキーワードが追加されます。キーワードがすでにフィルタ内で使用されていた場合は、既存の引数が指定した新しい引数に置き換えられます。

たとえば、フィルタ パネルで [Rule Content] > [Reference] > [CVE ID] の順にクリックすると、ポップアップ ウィンドウが開いて CVE ID を指定するよう示されます。「2007」と入力すると、「CVE:”2007”」がフィルタ テキスト ボックスに追加されます。別の例では、フィルタ パネルで [Rule Content] > [Reference] の順にクリックすると、ポップアップ ウィンドウが開いて、参照を指定するよう示されます。「2007」と入力すると、「Reference:”2007”」がフィルタ テキスト ボックスに追加されます。

- 複数のグループからルール フィルタ キーワードを選択した場合は、各フィルタ キーワードがフィルタに追加され、既存のキーワードが維持されます（同じキーワードの新しい値で上書きされなかった場合）。

たとえば、フィルタ パネルの [Category] で [os-linux] をクリックすると、「Category:"os-linux"」がフィルタ テキスト ボックスに追加されます。その後、[Microsoft Vulnerabilities] で [MS00-006] をクリックすると、フィルタが「Category:"os-linux" MicrosoftVulnerabilities:"MS00-006"」に変わります。

- 複数のキーワードを選択した場合は、システムがそれらを AND ロジックを使用して結合し、複合検索フィルタを生成します。たとえば、[Category] で [preprocessor] を選択してから、[Rule Content] > [GID] の順に選択して「116」と入力すると、プリプロセッサ ルールで、かつ GID が 116 のすべてのルールを取得する「Category: “preprocessor” GID:”116”」というフィルタが返されます。

- Category、Microsoft Vulnerabilities、Microsoft Worms、Platform Specific、および Priority の各フィルタ グループを使用すれば、カンマで区切られたキーワードの複数の引数を送信できます。たとえば、Shift キーを押しながら、[Category] から [os-linux] と [os-windows] を選択すると、os-linux カテゴリまたは os-windows カテゴリ内のルールを取得する「Category:"os-windows,app-detect"」というフィルタを作成できます。

複数のフィルタ キーワード/引数のペアで同じルールが取得される場合があります。たとえば、ルールを [dos] カテゴリによってフィルタ処理する場合や [High] 優先度でフィルタ処理する場合は、DOS Cisco 試行ルール（SID 1545）が表示されます。

（注） Cisco VRT がルール アップデート メカニズムを使用してルール フィルタを追加または削除する場合があります。

[Rules] ページ上のルールは、共有オブジェクト ルール（ジェネレータ ID 3）または標準テキスト ルール（ジェネレータ ID 1）のどちらかであることに注意してください。次の表に、さまざまなルール フィルタの説明を示します。

表 57：ルール フィルタ グループ

フィルタ グループ	説明	複数の引数をサポートするか	見出し	リスト内の項目
Rule Configuration	ルールの設定に基づいてルールを検索します。ルール構成フィルタについて （369 ページ）を参照してください。	いいえ	グループ	キーワード
Rule Content	ルールの内容に基づいてルールを検索します。ルール コンテンツ フィルタについて （371 ページ）を参照してください。	いいえ	グループ	キーワード
Category	ルール エディタで使用されるルール カテゴリに基づいてルールを検索します。ローカル ルールはローカル サブグループに表示されることに注意してください。ルール カテゴリについて （374 ページ）を参照してください。	はい	キーワード	引数
Classifications	ルールによって生成されるイベントのパケット画面内に表示される攻撃分類に基づいてルールを検索します。.	いいえ	キーワード	引数
Microsoft Vulnerabilities	Microsoft セキュリティ情報番号に従ってルールを検索します。	はい	キーワード	引数
Microsoft Worms	Microsoft Windows ホストに影響する特定のワームに基づいてルールを検索します。	はい	キーワード	引数
Platform Specific	オペレーティング システムの特定のバージョンとの関連性に基づいてルールを検索します。 ルールが複数のオペレーティング システムまたは 1 つのオペレーティング システムの複数のバージョンに影響する場合があることに注意してください。たとえば、SID 2260 を有効にすると、Mac OS X、IBM AIX、およびその他のオペレーティング システムの複数のバージョンに影響します。	はい	キーワード	引数 サブリストからいずれかの項目を選択すると、引数に修飾子が追加されることに注意してください。

フィルタ グループ	説明	複数の引数をサポートするか	見出し	リスト内の項目
Preprocessors	個別のプリプロセッサのルールを検索します。 プリプロセッサが有効になっている場合にプリプロセッサ オプションに対するイベントを生成するには、そのオプションに関連付けられているプリプロセッサ ルールを有効にする必要があります（ルール状態の設定（377 ページ）を参照）。	はい	グループ	サブグループ
Priority	高、中、および低の優先度に基づいてルールを検索します。 ルールに割り当てられた分類によってその優先度が決定されます。これらのグループは、さらにルール カテゴリに分類されます。ローカル ルール（つまり、ユーザが作成したルール）は優先度グループに表示されないことに注意してください。	はい	キーワード	引数 サブリストからいずれかの項目を選択すると、引数に修飾子が追加されることに注意してください。
Rule Update	特定のルール更新を通して追加または変更されたルールを検索します。ルール更新ごとに、更新内のすべてのルール、更新でインポートされた唯一の新しいルール、または更新によって変更された唯一の既存のルールを表示します。	いいえ	キーワード	引数

ルール構成フィルタについて

ライセンス：Protection

[Rules] ページに表示されたルールをいくつかのルール構成設定でフィルタ処理できます。

基準リスト内のノードをクリックしてキーワードを選択すると、フィルタ処理する引数を指定するためのポップアップ ウィンドウが表示されます。

そのキーワードがすでにフィルタで使用されていた場合は、そのキーワードの既存の引数が指定した引数に置き換えられます。

フィルタ処理に使用可能なルール構成設定に関する詳細については、次の手順を参照してください。

ステップ 1 ルール状態フィルタを使用する方法：

a) [Rule Configuration] で、[Rule State] をクリックします。

b) [Rule State] ドロップダウンリストから、フィルタ条件のルール状態を選択します。

- イベントを生成するだけのルールを検索するには、[Generate Events] を選択して、[OK] をクリックしてします。

- イベントを生成して一致するパケットをドロップするルールを検索するには、[Drop and Generate Events] を選択して、[OK] をクリックします。
- 無効になっているルールを検索するには、[Disabled] を選択して、[OK] をクリックします。

最新のルール状態に基づいてルールを表示するように [Rules] ページが更新されます。

ステップ 2 しきい値フィルタを使用する方法：

a) [Rule Configuration] で [Threshold] をクリックします。
b) [Threshold] ドロップダウンリストから、フィルタ条件のしきい値設定を選択します。

- しきい値タイプが limit のルールを検索するには、[Limit] を選択して、[OK] をクリックします。
- しきい値タイプが threshold のルールを検索するには、[Threshold] を選択して、[OK] をクリックします。
- しきい値タイプが both のルールを検索するには、[Both] を選択して、[OK] をクリックします。
- しきい値が source によって追跡されるルールを検索するには、[Source] を選択して、[OK] をクリックします。
- しきい値が destination によって追跡されるルールを検索するには、[Destination] を選択して、[OK] をクリックします。
- しきい値が設定されているすべてのルールを検索するには、[All] を選択して、[OK] をクリックします。

[Rules] ページが更新されて、フィルタで指定されたしきい値のタイプがルールに適用されているルールが表示されます。

ステップ 3 抑制フィルタを使用する方法：

a) [Rule Configuration] で、[Suppression] をクリックします。
b) [Suppression] ドロップダウンリストから、フィルタ条件の抑制設定を選択します。

- ルールの検査対象のパケットに対してイベントを抑制するルールを検索するには、[By Rule] を選択して、[OK] をクリックします。
- トラフィックの送信元に基づいてイベントを抑制するルールを検索するには、[By Source] を選択して、[OK] をクリックします。
- トラフィックの宛先に基づいてイベントを抑制するルールを検索するには、[By Destination] を選択して、[OK] をクリックします。
- 抑制が設定されているすべてのルールを検索するには、[All] を選択して、[OK] をクリックします。

.

[Rules] ページが更新されて、フィルタで指定された抑制のタイプがルールに適用されているルールが表示されます。

ステップ 4 動的状態フィルタを使用する方法：

a) [Rule Configuration] で、[Dynamic State] をクリックします。
b) [Dynamic State] ドロップダウンリストから、フィルタ条件の抑制設定を選択します。

- ルールの検査対象のパケットに対して動的状態を設定するルールを検索するには、[By Rule] を選択して、[OK] をクリックします。
- トラフィックの送信元に基づいてパケットに動的状態を設定するルールを検索するには、[By Source] を選択して、[OK] をクリックします。
- トラフィックの宛先に基づいて動的状態を設定するルールを検索するには、[By Destination] を選択して、[OK] をクリックします。
- Generate Events の動的状態が設定されたルールを検索するには、[Generate Events] を選択して、[OK] をクリックします。
- Drop and Generate Events の動的状態が設定されたルールを検索するには、[Drop and Generate Events] を選択して、[OK] をクリックします。
- Disabled の動的状態が設定されたルールを検索するには、[Disabled] を選択して、[OK] をクリックします。
- 抑制が設定されているすべてのルールを検索するには、[All] を選択して、[OK] をクリックします。

フィルタで指定された動的ルール状態がルールに適用されているルールを表示するように [Rules] ページが更新されます。

ステップ 5 アラート フィルタの使用方法：

a) [Rule Configuration] で [Alert] をクリックします。
b) [Alert] ドロップダウンリストから、SNMP 別にフィルタ処理するアラート設定を選択します。
c) [OK] をクリックします。

[Rules] ページが更新され、アラート フィルタを適用したルールが表示されます。

ステップ 6 コメント フィルタを使用する方法：

a) [Rule Configuration] で、[Comment] をクリックします。
b) [Comment] フィールドにフィルタ条件に関するコメント文字列を入力し、[OK] をクリックします。

[Rules] ページが更新され、ルールに適用されるコメントにフィルタで指定された文字列が含まれているルールが表示されます。

ルール コンテンツ フィルタについて

ライセンス：Protection

[Rules] ページに表示されたルールをいくつかのルール コンテンツ項目でフィルタ処理できます。たとえば、ルールの SID を検索することによって、ルールをすばやく取得できます。特定

の宛先ポートに送信されるトラフィックを検査するすべてのルールを検索することもできます。

基準リスト内のノードをクリックしてキーワードを選択すると、フィルタ処理する引数を指定するためのポップアップ ウィンドウが表示されます。

そのキーワードがすでにフィルタで使用されていた場合は、そのキーワードの既存の引数が指定した引数に置き換えられます。

たとえば、フィルタ パネルの [Rule Content] で [SID] をクリックすると、ポップアップ ウィンドウが開いてSIDの入力が促されます。「1045」と入力すると、「SID:"1045"」がフィルタ テキスト ボックスに追加されます。その後、再度 [SID] をクリックして、SIDフィルタを「1044」に変更すると、フィルタが「SID:"1044"」に変わります。

フィルタ処理に使用可能なルール コンテンツの詳細については、次の表を参照してください。

表 *58 :* ルール コンテンツ フィルタ

このフィルタを使用する場合のクリック対象	次の操作	結果
Message	フィルタ条件となるメッセージ文字列を入力して、[OK] をクリックします。	メッセージ フィールドで指定された文字列を含むルールを検索します。
SID	フィルタ条件となる SID 番号を入力して、[OK] をクリックします。	指定されたSIDが割り当てられたルールを検索します。
GID	フィルタ条件となる GID 番号を入力して、[OK] をクリックします。	指定されたGIDが割り当てられたルールを検索します。
Reference	フィルタ条件となる参照文字列を入力して、[OK] をクリックします。 フィルタ条件となる特定の参照タイプの文字列を入力するには、[CVE ID]、[URL]、[Bugtraq ID]、[Nessus ID]、[Arachnids ID]、または [Mcafee ID] を選択し、[OK] をクリックします。	参照フィールドで指定された文字列を含むルールを検索します。
Action	フィルタ処理するアクションを選択します。 • アラート ルールを検索するには、[Alert] を選択して、[OK] をクリックします。 • パス ルールを検索するには、[Pass] を選択して、[OK] をクリックします。	alert または pass で始まるルールを検索します。
Protocol	[ICMP]、[IP]、[TCP]、または [UDP] からフィルタ条件となるプロトコルを選択し、[OK] をクリックします。	選択されたプロトコルを含むルールを検索します。

このフィルタを使用する場合のクリック対象	次の操作	結果
Direction	フィルタ処理する方向設定を選択します。 • 特定の方向に移動するトラフィックを検査するルールを検索するには、[Directional] を選択して、[OK] をクリックします。 • 送信元と宛先の間を双方向に移動するトラフィックを検査するルールを検索するには、[Bidirectional] を選択して、[OK] をクリックしてします。	ルールに、指定された方向設定が含まれているかどうかに基づいてルールを検索します。
Source IP	フィルタ条件となる送信元 IP アドレスを入力して、[OK] をクリックします。 有効な IP アドレス、CIDR ブロック/プレフィクス長、または $HOME_NET や $EXTERNAL_NET などの変数を使用してフィルタ処理できることに注意してください。	ルール内の送信元 IP アドレス宛先に指定されたアドレスまたは変数を使用するルールを検索します。
Destination IP	フィルタ条件となる宛先 IP アドレスを入力して、[OK] をクリックします。 有効な IP アドレス、CIDR ブロック/プレフィクス長、または $HOME_NET や $EXTERNAL_NET などの変数を使用してフィルタ処理できることに注意してください。	ルール内の送信元 IP アドレス宛先に指定されたアドレスまたは変数を使用するルールを検索します。
Source Port	フィルタ条件となる送信元ポートを入力して、[OK]をクリックします。 ポート値は、1 ～ 65535 の整数またはポート変数にする必要があります。	指定された送信元ポートを含むルールを検索します。
Destination port	フィルタ条件となる宛先ポートを入力して、[OK] をクリックします。 ポート値は、1 ～ 65535 の整数またはポート変数にする必要があります。	指定された宛先ポートを含むルールを検索します。
ルールのオーバーヘッド	[Low]、[Medium]、[High]、または [Very High] からフィルタ条件となるルールのオーバーヘッド量を選択し、[OK] をクリックします。	選択されたルール オーバーヘッドを伴うルールを検索します。
メタデータ	フィルタ条件となるメタデータ キーと値のペアをスペースで区切って入力し、[OK] をクリックします。 たとえば、HTTP アプリケーションプロトコルに関連するメタデータを使用したルールを検索するには、「metadata:”service http”」と入力します。	一致するキーと値のペアを含むメタデータを使用したルールを検索します。

ルール カテゴリについて

ライセンス：Protection

ASA FirePOWER モジュールは、ルールが検出するトラフィックのタイプに基づいてカテゴリにルールを配置します。[Rules] ページで、ルール カテゴリでフィルタ処理することによって、カテゴリ内のすべてのルールにルール属性を設定できます。たとえば、ネットワーク上に Linux ホストが存在しない場合は、**os-linux** カテゴリでフィルタ処理してから、表示されたすべてのルールを無効にすることによって、**os-linux** カテゴリ全体を無効にすることができます。

（注） Cisco VRT がルール アップデート メカニズムを使用してルール カテゴリを追加または削除する場合があります。

ルール フィルタの直接編集

ライセンス：Protection

フィルタ パネルでフィルタをクリックしたときに入力される特殊なキーワードとその引数を変更するようにフィルタを編集できます。[Rules] ページのカスタム フィルタはルール エディタで使用されるものと同様に機能しますが、フィルタ パネルを通してフィルタを選択したときに表示される構文を使用して、[Rules] ページのフィルタに入力されたキーワードのいずれかを使用することもできます。今後使用するキーワードを決定するには、右側のフィルタ パネルで該当する引数をクリックします。フィルタ キーワードと引数構文がフィルタ テキスト ボックスに表示されます。

特定の値のみをサポートするキーワードの引数のリストを表示するには、ルール構成フィルタについて （369 ページ）、ルール コンテンツ フィルタについて （371 ページ）、およびルール カテゴリについて （374 ページ）を参照してください。キーワードのカンマ区切りの複数の引数は Category と Priority のフィルタ タイプでしかサポートされないことに注意してください。

引用符内のキーワードと引数、文字列、およびリテラル文字列と一緒に、複数のフィルタ条件を区切るスペースを使用できます。ただし、正規表現、ワイルドカード文字、または否定文字（!）、大なり記号（>）、小なり記号（<）などの特殊な演算子を含めることはできません。キーワードなし、キーワードの先頭文字の大文字表記なし、または引数の周りの引用符なしの検索語を入力すると、検索が文字列検索として扱われ、[Category]、[Message]、および [SID] の各フィールドで指定された単語が検索されます。

キーワード、キーワード引数、および文字列では、いずれも大文字と小文字が区別されません。gid キーワードと sid キーワードを除き、すべての引数と文字列は部分的な文字列として扱われます。gid と sid の引数は完全一致のみを返します。

各ルール フィルタに、次の形式で 1 つ以上のキーワードを含めることができます。

```
Keyword:"argument"
```

ここで、keyword は表 54 : ルール タイプ （357 ページ）の表に示すフィルタ グループ内のキーワードのいずれかです。また、argument は二重引用符で囲まれた単一の英数字文字列で、大文

字と小文字の区別がなく、キーワードに関連する特定のフィールド内の検索に使用されます。キーワードは先頭文字を大文字にして入力する必要があることに注意してください。

gid と sid を除くすべてのキーワードの引数が部分文字列として扱われます。たとえば、引数 123 は、「12345」、「41235」、「45123」などを返します。gid と sid の引数は完全一致のみを返します。たとえば、sid:3080 の場合、SID 3080 だけが返されます。

各ルール フィルタに、1 つ以上の英数字文字列を含めることもできます。文字列はルールの [Message] フィールド、シグニチャ ID、およびジェネレータ ID を検索します。たとえば、文字列 123 を指定するとルール メッセージ内の文字列「Lotus123」」、「123mania」などが返され、さらに SID 6123、SID 12375 なども返されます。1 つ以上の文字列でフィルタ処理することによって、SID を部分的に検索できます。

すべての文字列で大文字と小文字が区別されず、部分文字列として扱われます。たとえば、文字列 ADMIN、admin、または Admin はすべて、「admin」、「CFADMIN」、「Administrator」などを返します。

文字列を引用符で囲むと、完全一致を返すことができます。たとえば、引用符付きのリテラル文字列 "overflow attempt" は完全一致のみを返しますが、引用符なしの 2 つの文字列 overflow と attempt で構成されるフィルタは「overflow attempt」、「overflow multipacket attempt」、「overflow with evasion attempt」などを返します。

複数のキーワード、文字列、またはその両方をスペースで区切って任意に組み合わせて入力することで、フィルタ結果を絞り込むことができます。結果には、すべてのフィルタ条件に一致するルールが含まれます。

複数のフィルタ条件を任意の順序で入力できます。たとえば、次のフィルタはそれぞれ同じルールを返します。

- url:at login attempt cve:200
- login attempt cve:200 url:at
- login cve:200 attempt url:at

侵入ポリシー内のルール フィルタの設定

ライセンス：Protection

[Rules] ページで、ルールのサブセットを表示するようにルールをフィルタ処理できます。それから任意のページ機能を使用できます。これは、特定のカテゴリのすべてのルールのしきい値を設定する場合などに便利です。フィルタ処理されたリスト内のルールとフィルタ処理されていないリスト内のルールで同じ機能を使用できます。たとえば、新しいルール状態を、フィルタ処理されたリスト内のルールまたはフィルタ処理されていないリスト内のルールに適用できます。

侵入ポリシー内の [Rules] ページの左側にあるフィルタ パネルから事前定義のフィルタ キーワードを選択できます。フィルタを選択すると、ページに、すべての一致するルールが表示されるか、どのルールも一致しなかったことが表示されます。

使用可能なすべてのキーワードと引数の詳細と、フィルタ パネルでのフィルタの作成方法については、侵入ポリシー内のルール フィルタ処理について （366ページ）を参照してください。

フィルタにキーワードを追加してさらに絞り込むことができます。入力されたすべてのフィルタが、ルールデータベース全体を検索して、一致するすべてのルールを返します。ページに前回のフィルタ結果が表示されている状態でフィルタを入力すると、ページが消去され、代わりに新しいフィルタの結果が返されます。

また、フィルタを選択したとき、または、フィルタを選択後にその中の引数値を変更したときに指定したものと同じキーワードと引数の構文を使用してフィルタを入力することもできます。キーワードなし、キーワードの先頭文字の大文字表記なし、または引数の周りの引用符なしの検索語を入力すると、検索が文字列検索として扱われ、[Category]、[Message]、および [SID] の各フィールドで指定された単語が検索されます。

侵入ポリシー内の特定のルールに対してフィルタ処理する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定 （314 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3 [Rules] をクリックします。

[Rules] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ステップ 4 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。フィルタ内に存在するキーワードの引数をクリックすると、既存の引数が置き換えられることに注意してください。

ページが、すべての一致するルールを表示するように更新され、フィルタと一致するルールの数がフィルタ テキスト ボックスの上に表示されます。

ステップ 5 新しい設定を適用する 1 つ以上のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェック ボックスをオンにします。

ステップ 6 オプションで、通常ページで行うような変更をルールに対して行えます。詳細については、次の項を参照してください。

- [Rules] ページ上でルールを有効または無効にする方法については、ルール状態の設定 （377 ページ）を参照してください。

- ルールにしきい値設定と抑制を追加する方法については、ポリシー単位の侵入イベント通知のフィルタ処理 （380 ページ）を参照してください。
- 一致するトラフィックでレート異常が発生したときにトリガされる動的ルール状態を設定する方法については、動的ルール状態の追加 （388 ページ）を参照してください。
- 特定のルールに SNMP アラートを追加する方法については、SNMP アラートの追加 （392 ページ）を参照してください。
- ルールにルール コメントを追加する方法については、ルール コメントの追加 （393 ページ）を参照してください。

ステップ 7 ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。

詳細については、「侵入ポリシーの管理 （344 ページ）」と「侵入ポリシーの編集 （345 ページ）」を参照してください。

ルール状態の設定

ライセンス：Protection

シスコ脆弱性調査チーム（VRT）が、各デフォルト ポリシー内の侵入ルールとプリプロセッサ ルールのデフォルト状態を設定します。たとえば、ルールを Security over Connectivity デフォルト ポリシーでは有効にして、Connectivity over Security デフォルト ポリシーでは無効にすることができます。作成された侵入ポリシー ルールは、作成時に使用されたデフォルト ポリシー内のルールのデフォルト状態を継承します。

ルールを [Generate Events]、[Drop and Generate Events]、または [Disable] に個別に設定することも、状態を変更するルールを選択するためのさまざまな要素でルールをフィルタ処理することもできます。インライン展開では、インライン侵入展開で [Drop and Generate Events] ルール状態を使用して悪意のあるパケットをドロップできます。パッシブ展開では、[Drop and Generate Events] ルール状態が設定されたルールは、イベントを生成してもパケットはドロップしないことに注意してください。ルールを [Generate Events] または [Drop and Generate Events] に設定すると、ルールが有効になります。ルールを [Disable] に設定すると、ルールが無効になります。

2 つのシナリオについて考えてみます。最初のシナリオでは、特定のルールのルール状態が [Generate Events] に設定されます。悪意のあるパケットがネットワークを通過してルールをトリガーすると、そのパケットが宛先に送信され、システムが侵入イベントを生成します。2 つ目のシナリオでは、同じルールのルール状態が、インライン展開で [Drop and Generate Events] に設定されていると仮定します。この場合は、悪意のあるパケットがネットワークを通過すると、システムがそのパケットをドロップして、侵入イベントを生成します。パケットがターゲットに到達することはありません。

侵入ポリシーでは、ルールの状態を次のいずれかに設定できます。

- システムで特定の侵入試行を検出して、一致したトラフィックが見つかった時点で侵入イベントを生成する場合は、ルール状態を [Generate Events] に設定します。
- システムで特定の侵入試行を検出してから、インライン展開で一致するトラフィックが見つかった時点で攻撃を含むパケットをドロップし、侵入イベントを生成する場合、あるいはパッシブ展開で一致するトラフィックが見つかった時点で侵入イベントを生成する場合は、ルール状態を [Drop and Generate Events] に設定します。

システムでパケットをドロップする場合は、インライン展開で侵入ポリシーを廃棄ルールに設定する必要があることに注意してください。詳細については、インライン展開でのドロップ動作の設定 （347 ページ）を参照してください。

- システムで一致するトラフィックを評価しない場合は、ルール状態を [Disable] に設定します。

廃棄ルールを使用するには、次の手順を実行する必要があります。

- 侵入ポリシーで [Drop when Inline] オプションを有効にします。
- ルールと一致するすべてのパケットをドロップする必要があるすべてのルールのルール状態を [Drop and Generate Events] に設定します。
- 侵入ポリシーに関連付けられたアクセス コントロール ルールを含むアクセス コントロール ポリシーを、インライン展開で適用します。

[Rules] ページのルールのフィルタ処理は、廃棄ルールとして設定するルールを探すときに役立ちます。詳細については、侵入ポリシー内のルールのフィルタ処理（365 ページ）を参照してください。

VRT がルール更新を使用してデフォルト ポリシー内の 1 つ以上のルールのデフォルト状態を変更する場合があります。ルール更新での基本ポリシーの更新を許可すると、ポリシーの作成時に使用されたデフォルト ポリシー（または基礎となるデフォルト ポリシー）のデフォルト状態が変更されたときの、そのポリシー内のルールのデフォルト状態の変更も許可することになります。ただし、ルール状態を変更している場合は、ルール更新でその変更が上書きされないことに注意してください。

1 つ以上のルールのルール状態を変更する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定 （314 ページ）を参照してください。

[Policy Information] ページが表示されます。

このページには、有効なルールの総数、[Generate Events] に設定された有効なルールの総数、および [Drop and Generate Events] に設定された有効なルールの総数が表示されることに注意してください。また、パッシブ展開では、[Drop and Generate Events] に設定されたルールで行われるのはイベントの生成だけです。

ステップ 3 [Rules] をクリックします。

[Rules] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ステップ 4 ルール状態を設定するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、侵入ポリシー内のルール フィルタ処理について （366 ページ）および侵入ポリシー内のルール フィルタの設定 （375 ページ）を参照してください。

ページが更新され、一致するすべてのルールが表示されます。

ステップ 5 ルール状態を設定する 1 つ以上のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェック ボックスをオンにします。

ステップ 6 次の選択肢があります。

- トラフィックが選択されたルールと一致したときにイベントを生成するには、[Rule State] > [Generate Events] の順に選択します。
- インライン展開でトラフィックが選択されたルールと一致したときにイベントを生成し、そのトラフィックをドロップするには、[Rule State] > [Drop and Generate Events] の順に選択します。 >
- 選択されたルールと一致するトラフィックを検査しないようにするには、[Rule State] > [Disable] の順に選択します。

（注） シスコでは、侵入ポリシー内のすべての侵入ルールを有効に**しない**ことを**強く**推奨しています。すべてのルールが有効になっている場合は、デバイスのパフォーマンスが低下する可能性があります。代わりに、できるだけネットワーク環境に合わせてルール セットを調整してください。

ステップ 7 ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。詳細については、「侵入ポリシーの管理 （344 ページ）」と「侵入ポリシーの編集 （345 ページ）」を参照してください。

ポリシー単位の侵入イベント通知のフィルタ処理

ライセンス：Protection

侵入イベントの重要度は、発生頻度、送信元 IP アドレス、または宛先 IP アドレスに基づいて設定できます。イベントが特定の回数発生するまで注意が必要ない場合もあります。たとえば、何者かがサーバにログインしようとしても、特定の回数失敗するまで、気にする必要はありません。一方、ほんの少数の発生を見れば、広範な問題があることを理解できる場合もあります。たとえば、Web サーバに対して DoS 攻撃が行われた場合は、少数の侵入イベントの発生を確認しただけで、その状況に対処しなければならないことが分かります。同じイベントが何百回も確認されれば、システムの機能が麻痺します。

イベントしきい値の設定

ライセンス：Protection

指定された期間内にイベントが生成された回数に基づいて、システムが侵入イベントを記録して表示する回数を制限するための個別のルールのしきい値を侵入ポリシー単位で設定できます。これにより、大量の同じイベントが原因で機能が麻痺するのを避けることができます。共有オブジェクトのルール、標準テキスト ルール、またはプリプロセッサ ルールごとにしきい値を設定できます。

イベントしきい値の設定について

ライセンス：Protection

まず、しきい値タイプを指定する必要があります。次の表に示すオプションの中から選択できます。

表 *59 :* しきい値設定オプション

オプション	説明
Limit	指定された数のパケット（カウント引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、イベントを記録して表示します。たとえば、タイプを [Limit] に、[Count] を 10 に、[Seconds] を 60 に設定し、14 個のパケットがルールをトリガーする場合、システムはその 1 分間に発生した最初の 10 個を表示して、イベントの記録を停止します。
Threshold	指定された数のパケット（カウント引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、1 つのイベントを記録して表示します。イベントのしきい値カウントに達し、システムがそのイベントを記録した後、時間のカウンタは再び開始されることに注意してください。たとえば、タイプを [Threshold] に、[Count] を 10 に、[Seconds] を 60 に設定して、ルールが 33 秒間で 10 回トリガーされたとします。システムは、1 個のイベントを生成してから、[Seconds] と [Count] のカウンタをリセットします。次の 25 秒間にルールがさらに 10 回トリガーされたとします。33 秒でカウンタが 0 にリセットされたため、システムが別のイベントを記録します。

オプション	説明
Both	指定された数（カウント）のパケットがルールをトリガーとして使用した後で、指定された期間ごとに 1 回イベントを記録して表示します。たとえば、タイプを [Both] に、[Count] を 2 に、[Seconds] を 10 に設定した場合、イベント数は以下のようになります。 • ルールが 10 秒間に 1 回トリガーされた場合、システムはイベントを生成しません（しきい値が満たされていない）。 • ルールが 10 秒間に 2 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回トリガーとして使用した場合、しきい値が満たされるため）。 • ルールが 10 秒間に 4 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回目にトリガーとして使用されたときにしきい値に達し、それ以降のイベントは無視される）。

次に、トラッキングを指定する必要があります。これにより、イベントしきい値を送信元 IP アドレスごとに計算するか、宛先IPアドレスごとに計算するか決まります。次の表の中から、システムがイベントインスタンスを追跡する方法を指定するためのオプションの1つを選択します。

表 *60 : IP* しきい値設定オプション

オプション	説明
Source	送信元 IP アドレス単位でイベント インスタンス カウントを計算します。
Destination	宛先 IP アドレス単位でイベント インスタンス カウントを計算します。

最後に、しきい値を定義するインスタンスの数と期間を指定します。

表 *61 :* インスタンス/時間のしきい値設定オプション

オプション	説明
Count	しきい値を満たすために必要な、追跡する IP アドレス単位で指定された期間単位のイベント インスタンスの数。
Seconds	カウントがリセットされるまでの秒数。しきい値タイプを [limit] に、トラッキングを [Source IP] に、[count] を 10 に、[seconds] を 10 に設定した場合、システムは指定された送信元ポートから 10 秒間に発生した最初の 10 個のイベントを記録して表示します。最初の 10 秒間に 7 つのイベントしか発生しなかった場合は、システムがそれらのイベントを記録して表示します。最初の 10 秒間に 40 のイベントが発生した場合は、システムが 10 のイベントを記録して表示してから 10 秒後にカウントを再開します。

侵入イベントのしきい値設定は、単独で使用することも、レート ベースの攻撃防御、detection_filter キーワード、および侵入イベント抑制のいずれかと組み合わせて使用すること

もできることに注意してください。詳細については、動的ルール状態の追加（388ページ）および侵入ポリシーごとの抑制の設定（385ページ）を参照してください。

侵入イベントしきい値の追加と変更

ライセンス：Protection

1つ以上の特定のルールのしきい値を設定できます。既存のしきい値設定を個別にまたは同時に変更することもできます。それぞれに1つずつのしきい値を設定できます。しきい値を追加すると、ルールの既存のしきい値が上書きされます。

しきい値設定の表示方法と削除方法については、侵入イベントしきい値の表示と削除（383ページ）を参照してください。

また、すべてのルールとプリプロセッサ生成イベントにデフォルトで適用されるグローバルしきい値を変更することもできます。詳細については、侵入イベントの記録の制限（395ページ）を参照してください。

無効な値を入力するとフィールドに復元アイコン（  ）が表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

イベントしきい値を追加または変更する方法：

ステップ1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ2 編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定（314ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ3 [Rules] をクリックします。

[Rules] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ステップ4 しきい値を設定するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、侵入ポリシー内のルール フィルタ処理について（366ページ）および侵入ポリシー内のルール フィルタの設定（375ページ）を参照してください。

ページが更新され、一致するすべてのルールが表示されます。

ステップ 5 しきい値を設定する 1 つまたは複数のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェック ボックスをオンにします。

ステップ 6 [Event Filtering] > [Threshold] の順に選択します。

[thresholding] ポップアップ ウィンドウが表示されます。

ステップ 7 [Type] ドロップダウンリストから、設定するしきい値のタイプを選択します。

- 指定された期間あたりのイベント インスタンス数に通知を制限する場合は、[Limit] を選択します。
- 指定された期間あたりのイベント インスタンス数ごとに通知を提供する場合は、[Threshold] を選択します。
- 指定されたイベント インスタンス数後に期間あたり 1 回ずつ通知を提供する場合は、[Both] を選択します。

ステップ 8 [Track By] ドロップダウンリストから、イベント インスタンスが送信元 IP アドレスまたは宛先 IP アドレスのどちらによって追跡されるかを選択します。

ステップ 9 [Count] フィールドで、しきい値として使用するイベント インスタンスの数を指定します。

ステップ 10 [Seconds] フィールドで、イベント インスタンスを追跡する期間を表す秒数を指定します。

ステップ 11 [OK] をクリックします。

しきい値が追加され、[Event Filtering] カラムのルールの横にイベント フィルタ アイコン（  ）が表示されます。ルールに複数のイベント フィルタを追加した場合は、アイコン上の数字がイベント フィルタの数を示します。

ステップ 12 ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。

詳細については、「侵入ポリシーの管理 （344 ページ）」と「侵入ポリシーの編集 （345 ページ）」を参照してください。

侵入イベントしきい値の表示と削除

ライセンス：Protection

既存のしきい値設定を表示または削除することができます。[Rules Details] ビューを使用してしきい値の既存の設定を表示することによって、それらがシステムに適切かどうかを確認できます。そうでない場合は、新しいしきい値を追加して既存の値を上書きすることができます。

すべてのルールとプリプロセッサ生成イベントにデフォルトで適用されるグローバルしきい値を変更することもできることに注意してください。詳細については、侵入イベントの記録の制限 （395 ページ）を参照してください。

しきい値を表示または削除する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定 （314 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3 [Rules] をクリックします。

[Rules] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ステップ 4 表示または削除する、しきい値が設定されたルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、侵入ポリシー内のルール フィルタ処理について （366 ページ）および侵入ポリシー内のルール フィルタの設定 （375 ページ）を参照してください。

ページが更新され、一致するすべてのルールが表示されます。

ステップ 5 表示または削除する、しきい値が設定された 1 つまたは複数のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェック ボックスをオンにします。

ステップ 6 選択したルールのしきい値を削除するには、[Event Filtering] > [Remove Thresholds] の順に選択します。表示される確認のポップアップ ウィンドウで [OK] をクリックします。

ヒント 特定のしきい値を削除するために、ルールを強調表示して、[Show Details] をクリックすることもできます。しきい値設定を展開して、削除するしきい値設定の横にある [Delete] をクリックします。[OK] をクリックして、設定の削除を確認します。

ページが更新され、しきい値が削除されます。

ステップ 7 ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。詳細については、「侵入ポリシーの管理 （344ページ）」と「侵入ポリシーの編集 （345ページ）」を参照してください。

侵入ポリシーごとの抑制の設定

ライセンス：Protection

特定の IP アドレスまたは IP アドレスの範囲が特定のルールまたはプリプロセッサをトリガーしたときの侵入イベント通知を抑制できます。これは、誤検出を回避するのに役立ちます。たとえば、ユーザのメールサーバが特定のエクスプロイトのように見えるパケットを送信している場合、そのメールサーバによってイベントがトリガーされたされたときに、そのイベントに関する通知を抑制できます。ルールはすべてのパケットに対してトリガーとして使用されますが、本物の攻撃に対するイベントだけが表示されます。

侵入イベント抑制は、単独で使用することも、レート ベースの攻撃防御、detection_filter キーワード、および侵入イベントしきい値のいずれかと組み合わせて使用することもできることに注意してください。詳細については、動的ルール状態の追加 （388ページ）およびイベントしきい値の設定 （380 ページ）を参照してください。

侵入イベントの抑制

ライセンス：Protection

ルールに関する侵入イベント通知を抑制できます。ルールに関する通知が抑制されると、ルールはトリガーとして使用されますが、イベントは生成されません。ルールの 1 つまたは複数の抑制を設定できます。リスト内の最初の抑制に最も高いプライオリティが割り当てられます。2 つの抑制が競合している場合は、最初の抑制のアクションが実行されることに注意してください。

無効な値を入力するとフィールドに復元アイコン（  ）が表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

イベント表示を抑制する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定 （314 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3 [Rules] をクリックします。

[Rules] ページが表示されます。デフォルトで、このページにはルールがメッセージのアルファベット順に表示されます。

ステップ 4 抑制を設定するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、侵入ポリシー内のルール フィルタ処理について （366 ページ）および侵入ポリシー内のルール フィルタの設定 （375 ページ）を参照してください。

ページが更新され、一致するすべてのルールが表示されます。

ステップ 5 抑制条件を設定する 1 つまたは複数のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェック ボックスをオンにします。

ステップ 6 [Event Filtering] > [Suppression] の順に選択します。

[suppression] ポップアップ ウィンドウが表示されます。

ステップ 7 次の [Suppression Type] オプションのいずれかを選択します。

- 選択したルールのイベントを完全に抑制する場合は、[Rule] を選択します。
- 指定した送信元 IP アドレスから送信されるパケットによって生成されるイベントを抑制する場合は、[Source] を選択します。
- 指定した宛先 IP アドレスに送信されるパケットによって生成されるイベントを抑制する場合は、[Destination] を選択します。

ステップ 8 抑制タイプとして [Source] または [Destination] を選択した場合は、[Network] フィールドに、IP アドレス、アドレス ブロック、または送信元 IP アドレスまたは宛先 IP アドレスとして指定する変数、あるいは、これらの任意の組み合わせで構成されたカンマ区切りのリストを入力します。

ステップ 9 [OK] をクリックします。

抑制条件が追加され、抑制するルールの横にある [Event Filtering] カラムのルールの横にイベント フィルタ アイコン（  ）が表示されます。ルールに複数のイベント フィルタを追加した場合は、アイコン上の数字がイベント フィルタの数を示します。

ステップ 10 ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。

詳細については、「侵入ポリシーの管理 （344 ページ）」と「侵入ポリシーの編集 （345 ページ）」を参照してください。

抑制条件の表示と削除

ライセンス：Protection

既存の抑制条件を表示または削除することもできます。たとえば、メールサーバが悪用のように見えるパケットを普段から送信しているという理由で、そのメール サーバの IP アドレスから送信されたパケットに関するイベント通知を抑制できます。その後、そのメールサーバが使用停止になり、その IP アドレスが別のホストに再割り当てされたら、その送信元 IP アドレスの抑制条件を削除する必要があります。

定義された抑制条件を表示または削除する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定 （314 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3 [Rules] をクリックします。

[Rules] ページが表示されます。デフォルトで、ページにはルールがメッセージのアルファベット順に一覧表示されます。

ステップ 4 抑制を表示または削除するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、侵入ポリシー内のルール フィルタ処理について （366 ページ）および侵入ポリシー内のルール フィルタの設定 （375 ページ）トピックを参照してください。

ページが更新され、一致するすべてのルールが表示されます。

ステップ 5 抑制を表示または削除する 1 つまたは複数のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェック ボックスをオンにします。

ステップ 6 次の 2 つのオプションから選択できます。

- ルールのすべての抑制を削除するには、[Event Filtering] > [Remove Suppressions] の順に選択します。表示される確認のポップアップ ウィンドウで [OK] をクリックします。
- 特定の抑制設定を削除するには、ルールを強調表示して、[Show Details] をクリックします。抑制設定を展開して、削除する抑制設定の横にある [Delete] をクリックします。[OK] をクリックして、選択した設定の削除を確認します。

ページが更新され、抑制設定が削除されます。

ステップ 7 ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。詳細については、侵入ポリシーの管理 （344 ページ）および侵入ポリシーの編集 （345 ページ）を参照してください。

動的ルール状態の追加

ライセンス：Protection

レート ベースの攻撃は、ネットワークまたはホストに過剰なトラフィックを送信することによって、低速化または正規の要求の拒否を引き起こし、ネットワークまたはホストを混乱させようとします。レートベースの防御を使用して、特定のルールの過剰なルール一致に対応してルール アクションを変更することができます。

動的ルール状態について

ライセンス：Protection

一定期間に多すぎる数のルールの一致が発生した時点を検出するレートベースのフィルタを含めるように侵入ポリシーを設定できます。インライン展開されたデバイス上でこの機能を使用して、指定された時刻のレートベースの攻撃をブロックしてから、ルール一致がイベントを生成するだけでトラフィックをドロップしないルール状態に戻すことができます。

レート ベースの攻撃防御は、異常なトラフィック パターンを識別し、正規の要求に対するそのトラフィックの影響を最小限に抑えようとします。特定の宛先 IP アドレスに送信されるトラフィックまたは特定の送信元 IP アドレスから送信されるトラフィックの過剰なルール一致を識別できます。また、検出されたすべてのトラフィックを通して特定のルールの過剰な一致に対処することもできます。

侵入ポリシーでは、侵入ルールまたはプリプロセッサ ルールのレート ベースのフィルタを設定できます。レート ベースのフィルタは次の 3 つの要素で構成されます。

- 特定の秒数以内のルール一致のカウントとして設定されるルール一致率
- レートを超えた時点で実行される新しいアクション（Generate Events、Drop and Generate Events、および Disable の 3 種類がある）
- タイムアウト値として設定されるアクションの継続期間

新しいアクションは、開始されると、レートがその期間内に設定されたレートを下回っても、タイムアウトに達するまで継続されることに注意してください。タイムアウトに達したときに、レートがしきい値を下回っている場合は、ルールのアクションが初期設定に戻ります。

インライン展開のレートベースの攻撃防御は、攻撃を一時的または永続的にブロックするように設定できます。レート ベースの設定を使用しない場合、[Generate Events] に設定されたルールはイベントを生成しますが、システムはそのようなルールに関するパケットをドロップしま

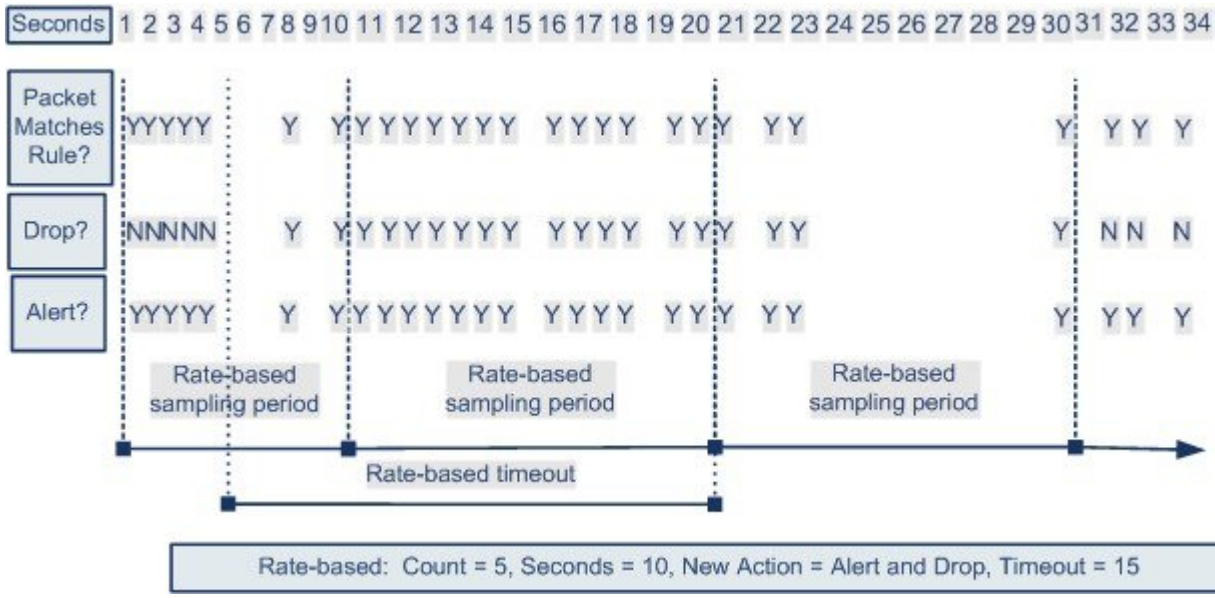
せん。ただし、攻撃トラフィックが、レートベースの基準が設定されたルールと一致した場合は、そのようなルールが最初から [Drop and Generate Events] に設定されていなかったとしても、レート アクションがアクティブな期間にパケットのドロップが実行されます。

（注） レート ベースのアクションは、無効なルールを有効にしたり、無効なルールと一致したトラフィックをドロップしたりできません。

同じルールに対して複数のレートベースのフィルタを定義できます。侵入防御ポリシーで最初にリストされているフィルタに、最大のプライオリティが割り当てられます。2 つのレートベースのフィルタ アクションが競合している場合は、最初のレート ベースのフィルタのアクションが実行されることに注意してください。

次の図は、攻撃者がホストにアクセスしようとしている例を示しています。繰り返しパスワードを特定しようとする試みが、レート ベースの攻撃防御が設定されたルールをトリガーします。レートベースの設定は、ルール一致が 10 秒間に 5 回発生した時点で、ルール属性を [Drop and Generate Events] に変更します。新しいルール属性は 15 秒後にタイムアウトします。

タイムアウト後も、そのパケットは後続のレートベースのサンプリング期間にドロップされることに注意してください。サンプリング レートが現在または過去のサンプリング期間のしきい値を上回っている場合は、新しいアクションが継続されます。新しいアクションは、サンプリング レートがしきい値レートを下回るサンプリング期間の終了後にのみ、[Generate Events] に戻ります。



動的ルール状態の設定

ライセンス：Protection

ルールと一致したすべてのパケットをドロップするのではなく、指定された期間に特定の一致率に達した場合にルールと一致したパケットをドロップするために、ルールを[Drop and Generate Events] 状態に設定しない場合があります。動的ルール状態を使用すれば、ルールのアクションの変更をトリガーするレート、あるレートに達したときに変更すべきアクション、および新しいアクションの継続時間を設定できます。

アクションの変更をトリガーする特定のヒット数に対して、必要なカウントと期間（秒数）を指定することによって、そのルールのヒット数を設定します。加えて、タイムアウトが発生したらアクションをルールの以前の状態に戻すタイムアウトを設定できます。

同じルールに対して複数の動的状態フィルタを定義できます。侵入ポリシー内のルール詳細に列挙された最初のフィルタに最も高い優先度が割り当てられます。2つのレートベースのフィルタ アクションが競合している場合は、最初のレート ベースのフィルタのアクションが実行されることに注意してください。

無効な値を入力するとフィールドに復元アイコンが表示されることに注意してください。そのアイコンをクリックすると、そのフィールドの最後の有効値に戻るか、以前の値が存在しない場合はフィールドが空になります。

（注） 動的ルール状態は、無効なルールを有効にしたり、無効なルールと一致したトラフィックをドロップしたりできません。

動的ルール状態を追加する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2 編集するポリシーの横にある編集アイコン（✎）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定 （314 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3 [Rules] をクリックします。

[Rules] ページが表示されます。

ステップ 4 動的ルール状態を追加するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。

ページが更新され、一致するすべてのルールが表示されます。

ステップ 5 動的ルール状態を追加する 1 つまたは複数のルールを選択します。次の選択肢があります。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェック ボックスをオンにします。

ステップ 6 [Dynamic State] > [Add Rate-Based Rule State] の順に選択します。

[Add Rate-Based Rule State] ダイアログボックスが表示されます。

ステップ 7 [Track By] ドロップダウンリストから、ルール一致の追跡方法を選択します。

- 特定の送信元または送信元のセットからのそのルールのヒット数を追跡する場合は、[Source] を選択します。
- 特定の宛先または宛先のセットへのそのルールのヒット数を追跡する場合は、[Destination] を選択します。
- そのルールのすべての一致を追跡する場合は、[Rule] を選択します。

ステップ 8 [Track By] を [Source] または [Destination] に設定した場合は、[Network] フィールドに追跡する各ホストのアドレスを入力します。

単一の IP アドレス、アドレスブロック、変数、またはこれらの任意の組み合わせで構成されたカンマ区切りのリストを指定できます。

ステップ 9 [Rate] の隣で、攻撃レートを設定する期間あたりのルール一致の数を指定します。

- [Count] フィールドで、1 ～ 2147483647 の整数を使用して、しきい値として使用するルール一致の数を指定します。
- [Seconds] フィールドで、1 ～ 2147483647 の整数を使用して、攻撃を追跡する期間を表す秒数を指定します。

ステップ 10 [New State] ドロップダウンリストから、条件を満たしたときに実行される新しいアクションを指定します。

- イベントを生成する場合は、[Generate Events] を選択します。
- インライン展開でイベントを生成し、イベントをトリガーしたパケットをドロップする場合、または、パッシブ展開でイベントを生成する場合は、[Drop and Generate Events] を選択します。
- アクションを実行しない場合は、[Disabled] を選択します。

ステップ 11 [Timeout] フィールドに、新しいアクションを有効にしておく秒数を入力します。タイムアウトが発生すると、ルールが元の状態に戻ります。新しいアクションのタイムアウトを阻止する場合は、[0] を指定するか、[Timeout] フィールドを空白のままにします。

ステップ 12 [OK] をクリックします。

動的ルール状態が追加され、[Dynamic State] カラムのルールの横に動的状態アイコン（）が表示されます。ルールに複数の動的ルール状態フィルタを追加した場合は、アイコン上の数字がフィルタの数を示します。

必須フィールドを空白にした場合は、フィールドに値を入力する必要があることを伝えるエラーメッセージが表示されます。

ヒント 一連のルールからすべての動的ルール設定を削除するには、[Rules] ページでルールを選択してから、[Dynamic State] > [Remove Rate-Based States] の順に選択します。また、ルールのルール詳細から個別のレート ベースのルール状態フィルタを削除するには、ルールを選択して、[Show Details] をクリックしてから、削除するレート ベースのフィルタのそばにある [Delete] をクリックします。

ステップ 13 ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。

詳細については、「侵入ポリシーの管理 （344 ページ）」と「侵入ポリシーの編集 （345 ページ）」を参照してください。

SNMP アラートの追加

ライセンス：Protection

ASA FirePOWER モジュールの SNMP アラートを設定する場合は、ルールがイベントを生成したときに SNMP アラートを表示する特定のルールを設定できます。詳細については、「SNMP 応答の使用 （512 ページ）」を参照してください。

SNMP アラートを設定する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定 （314 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3 [Rules] をクリックします。

[Rules] ページが表示されます。

ステップ 4 SNMP アラートを設定するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、侵入ポリシー内のルール フィルタ処理について （366 ページ）および侵入ポリシー内のルール フィルタの設定 （375 ページ）を参照してください。

ページが更新され、一致するすべてのルールが表示されます。

ステップ 5 SNMP アラートを設定する 1 つまたは複数のルールを選択します。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェック ボックスをオンにします。

ステップ 6 [Alerting] > [Add SNMP Alert] の順に選択します。

アラートが追加され、[Alerting] カラムのルールの横にアラート アイコンが表示されます。ルールに複数のアラート タイプを追加した場合は、アイコン上の数字がアラート タイプの数を示します。

ヒント ルールから SNMP アラートを削除するには、そのルールの横にあるチェックボックスをクリックして、[Alerting] > [Remove SNMP Alerts] の順に選択し、[OK] をクリックして削除を確認します。

ステップ 7 ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。詳細については、「侵入ポリシーの管理 （344 ページ）」と「侵入ポリシーの編集 （345 ページ）」を参照してください。

ルール コメントの追加

ライセンス：Protection

ルールにコメントを追加することができます。追加したコメントは、[Rules] ページ上の [Rule Details] ビューで確認できます。

コメントを含む侵入ポリシーの変更をコミットしてから、ルールの [Edit] ページで [Rule Comment] をクリックしてコメントを表示することもできます。

コメントをルールに追加する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定 （314 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3 [Rules] をクリックします。

[Rules] ページが表示されます。

ステップ 4 コメントを追加するルールを探します。次の選択肢があります。

- 現在の画面をソートするには、カラム見出しまたはアイコンをクリックします。ソートを反転させるには、再度クリックします。
- 左側のフィルタ パネルでキーワードまたは引数をクリックしてフィルタを構築します。詳細については、侵入ポリシー内のルール フィルタ処理について （366 ページ）および侵入ポリシー内のルール フィルタの設定 （375 ページ）を参照してください。

ページが更新され、一致するすべてのルールが表示されます。

ステップ 5 コメントを追加する 1 つまたは複数のルールを選択します。

- 特定のルールを選択するには、そのルールの横にあるチェック ボックスをオンにします。
- 現在のリスト内のすべてのルールを選択するには、カラムの一番上にあるチェック ボックスをオンにします。

ステップ 6 [Comments] > [Add Rule Comment] の順に選択します。

[Add Comment] ダイアログボックスが表示されます。

ステップ 7 [Comment] フィールドに、ルールに関するコメントを入力します。

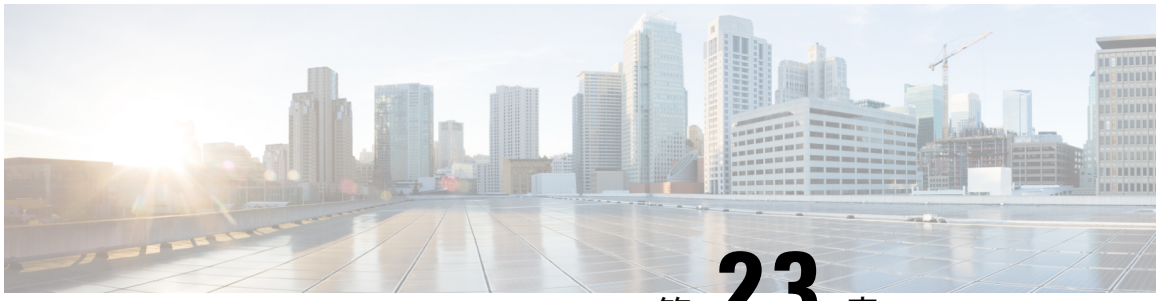
ステップ 8 [OK] をクリックします。

コメントが追加され、[Comments] カラムのルールの横にコメント アイコン（）が表示されます。ルールに複数のコメントを追加した場合は、アイコン上の数字がコメントの数を示します。

ヒント ルールのコメントを削除するには、そのルールを強調表示して [Show Details] をクリックし、[Comments] セクションで [Delete] をクリックします。侵入ポリシーの変更がコミットされずにコメントがキャッシュされている場合にだけ、コメントを削除できることに注意してください。侵入ポリシーの変更がコミットされた後は、ルール コメントを削除できなくなります。

ステップ 9 ポリシーの保存、編集の継続、変更の破棄、またはシステム キャッシュに変更を残したままの終了を実行します。

詳細については、「侵入ポリシーの管理 （344 ページ）」と「侵入ポリシーの編集 （345 ページ）」を参照してください。



第 23 章

侵入イベントの記録のグローバルな制限

システムが侵入イベントを記録して表示する回数を制限するしきい値を使用できます。この章は、次のセクションで構成されています。

侵入イベントの記録の制限

侵入ポリシーの一部としてしきい値を設定すると、ルールに一致するトラフィックが、指定期間内に特定のアドレスまたはアドレス範囲で送受信される回数に基づいて、イベントが生成されます。これにより、多数のイベントでいっぱいなることを回避できます。この機能を使用するには Protection ライセンスが必要です。

イベント通知しきい値は、次の 2 種類の方法で設定できます。

- すべてのトラフィックに対するグローバルしきい値を設定して、指定された期間に特定の送信元または宛先からのイベントが記録され表示される頻度を制限できます。詳細については、しきい値について （395ページ）およびグローバルなしきい値の設定 （397ページ）を参照してください。
- 侵入ポリシーの設定では、共有オブジェクト ルール、標準テキスト ルール、またはプリプロセッサ ルールごとにしきい値を設定できます。イベントしきい値の設定 （380 ページ）を参照してください。

しきい値について

ライセンス：Protection

デフォルトでは、侵入ポリシーごとに、グローバル ルールしきい値が含まれます。デフォルトのしきい値では、各ルールのイベント生成が、同じ宛先に送られるトラフィックで 60 秒あたり 1 つのイベントに制限されます。このグローバルしきい値は、デフォルトですべての侵入

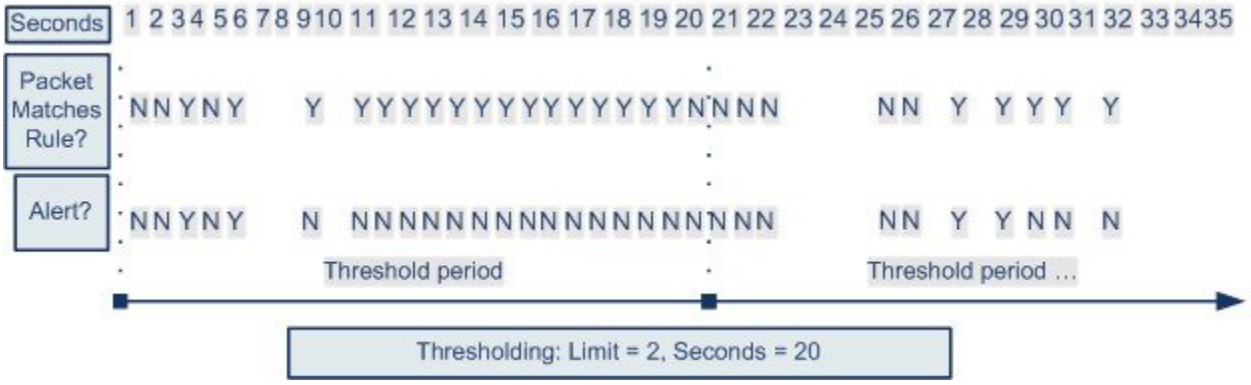
ルールとプリプロセッサルールに適用されます。しきい値は侵入ポリシーの [Advanced Settings] ページで無効にできることに注意してください。

特定のルールで個々のしきい値を設定することにより、このしきい値を上書きすることもできます。たとえば、グローバル制限しきい値を 60 秒ごとに 5 個のイベントに設定してから、SID 1315 について特定のしきい値として 60 秒ごとに 10 個のイベントに設定できます。他のすべてのルールでは 60 秒ごとに 6 個以上のイベントは生成されませんが、SID 1315 では 60 秒ごとに最大 10 個のイベントが生成されます。

ルールベースのしきい値の設定の詳細については、イベントしきい値の設定（380 ページ）を参照してください。

次の図は、特定のルールに関して攻撃を受けている例を示します。グローバル制限しきい値では、各ルールのイベント生成が、20 秒あたり 2 つのイベントに制限されます。

期間は 1 秒で始まり 21 秒で終わることに注意してください。期間が終了すると、サイクルが再び開始され、次の 2 つのルール一致によってイベントが生成されます。その後、その期間にさらにイベントが生成されることはありません。



しきい値のオプションについて

ライセンス：Protection

しきい値を使用して、期間内に特定数のイベントのみが生成されるように制限するか、イベントセットごとに 1 つのイベントが生成されるように制限することで、侵入イベントの生成を制限できます。グローバルしきい値を設定する際は、最初にしきい値のタイプを指定する必要があります。以下の表を参照してください。

表 *62*：しきい値設定オプション

オプション	説明
Limit	指定された数のパケット（カウント引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、イベントを記録して表示します。たとえば、タイプを [Limit] に、[Count] を 10 に、[Seconds] を 60 に設定し、14 個のパケットがルールをトリガーする場合、システムはその 1 分間に発生した最初の 10 個を表示して、イベントの記録を停止します。

オプション	説明
Threshold	指定された数のパケット（カウント引数によって指定される）が、指定された期間内にルールをトリガーとして使用した場合に、1 つのイベントを記録して表示します。イベントのしきい値カウントに達し、システムがそのイベントを記録した後、時間のカウンタは再び開始されることに注意してください。たとえば、タイプを [Threshold] に、[Count] を 10 に、[Seconds] を 60 に設定して、ルールが 33 秒間で 10 回トリガーされたとします。イベントが 1 つ生成されて、[Seconds] と [Count] のカウンタが 0 にリセットされます。次の 25 秒間にルールがさらに 10 回トリガーされたとします。33 秒でカウンタが 0 にリセットされたため、システムが別のイベントを記録します。
Both	指定された数（カウント）のパケットがルールをトリガーとして使用した後で、指定された期間ごとに 1 回イベントを記録して表示します。たとえば、タイプを [Both] に、[Count] を 2に、[Seconds] を 10 に設定した場合、イベント数は以下のようになります。 • ルールが 10 秒間に 1 回トリガーされた場合、システムはイベントを生成しません（しきい値が満たされていない）。 • ルールが 10 秒間に 2 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回トリガーとして使用した場合、しきい値が満たされるため）。 • ルールが 10 秒間に 4 回トリガーされた場合、システムは 1 つのイベントを生成します（ルールが 2 回トリガーされると、しきい値が満たされ、以後のイベントは無視されるため）。

次に、イベント インスタンスの数を、送信元 IP アドレスまたは宛先 IP アドレスのどちらに基づいて計算するかを決定する、トラッキングを指定します。最後に、しきい値を定義するインスタンスの数と期間を指定します。

表 *63* : インスタンス/時間のしきい値設定オプション

オプション	説明
Count	しきい値を満たすために必要な、トラッキング IP アドレスまたはアドレス範囲ごとの、指定された期間でのイベント インスタンスの数。
Seconds	カウントがリセットされるまでの秒数。しきい値タイプを [Limit] に、トラッキングを [Source] に、[Count] を 10 に、[Seconds] を 10 に設定した場合、特定のソース ポートで 10 秒間に発生した最初の 10 のイベントを記録し表示します。最初の 10 秒で 7 個のイベントだけが発生した場合、システムはそれらを記録して表示します。最初の 10 秒で 40 個のイベントが発生した場合、システムは 10 個を記録して表示し、10 秒経過してからカウントを再度開始します。

グローバルなしきい値の設定

ライセンス：Protection

一定の期間に各ルールによって生成されるイベントの数を管理するために、グローバルしきい値を設定できます。グローバルしきい値を設定すると、特定のしきい値を上書きしない各ルールでそのしきい値が適用されます。しきい値の設定の詳細については、しきい値について （395 ページ）を参照してください。

デフォルトでは、ユーザのシステムにグローバルしきい値が設定されます。デフォルト値は次のとおりです。

- **Type** — Limit
- **Track By** — Destination
- **Count** — 1
- **Seconds** — 60

グローバルしきい値の設定方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定 （314 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3 左側のナビゲーション パネルにある [Advanced Settings] をクリックします。

[Advanced Settings] ページが表示されます。

ステップ 4 [Intrusion Rule Thresholds] の [Global Rule Thresholding] が有効になっているかどうかに応じて、以下の 2 つの選択肢があります。

- 設定が有効な場合、[Edit] をクリックします。
- 設定が無効である場合、[Enabled] をクリックし、[Edit] をクリックします。

[Global Rule Thresholding] ページが表示されます。ページ下部のメッセージは、設定を含む侵入ポリシー層を示します。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシー レイヤでのレイヤの使用（317 ページ）」を参照してください。

ステップ 5 [Type] オプション ボタンから、seconds 引数で指定された時間内に適用するしきい値のタイプを選択します。詳細については、表 62 : しきい値設定オプション （396 ページ）の表を参照してください。

- count 引数で指定された制限を超えるまで、ルールをトリガーとして使用したパケットごとにイベントを記録して表示する場合、[制限（Limit）] を選択します。
- ルールをトリガーとして使用し、カウント引数で設定されたしきい値と同じかその倍数であるインスタンスを表すパケットごとに 1 つのイベントを記録して表示する場合、[Threshold] を選択します。

- count 引数によって指定された数のパケットがルールをトリガーとして使用した後に 1 つのイベントを記録して表示する場合、[両方（Both）] を選択します。

ステップ 6 [Track By] ドロップダウン リストからトラッキング方法を選択します。

- 特定の送信元 IP アドレスからのトラフィックでルールの一致を識別するには、[送信元（Source）] を選択します。
- 特定の宛先 IP アドレスへのトラフィックでルールの一致を識別するには、[宛先（Destination）] を選択します。

ステップ 7 [Count] フィールドで以下を実行します。

- [Limit] しきい値では、しきい値を満たすために必要なトラッキング IP アドレスごとに、指定期間ごとのイベント インスタンスの数を指定します。
- [Threshold] しきい値では、しきい値として使用するルールの一致回数を指定します。

ステップ 8 [Seconds] フィールドで以下を実行します。

- [Limit] しきい値では、攻撃を追跡する期間の秒数を指定します。
- [Threshold] しきい値では、カウントをリセットするまでの経過時間（秒数）を指定します。指定された秒数が経過する前であっても、[カウント（Count）] フィールドで示されている数のルールが一致すると、カウントはリセットされるのでご注意ください。

ステップ 9 ポリシーの保存、編集の続行、変更の破棄を行うか、またはシステム キャッシュで変更をそのままにしながら終了します。詳細については、「競合の解決とポリシー変更の確定 （314 ページ）」を参照してください。

グローバルしきい値の無効化

ライセンス：Protection

デフォルトでは、グローバル制限しきい値は、宛先へのトラフィックでのイベントの数を 60 秒あたり 1 個のイベントに制限しています。デフォルトで特定のルールに関するイベントにしきい値を適用し、すべてのルールにしきい値を適用しない場合、最高位のポリシー階層でグローバルしきい値を無効にできます。

グローバルしきい値の無効化：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2 編集するポリシーの横にある編集アイコン（  ）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定 （314 ページ）を参照してください。

[Policy Information] ページが表示されます。

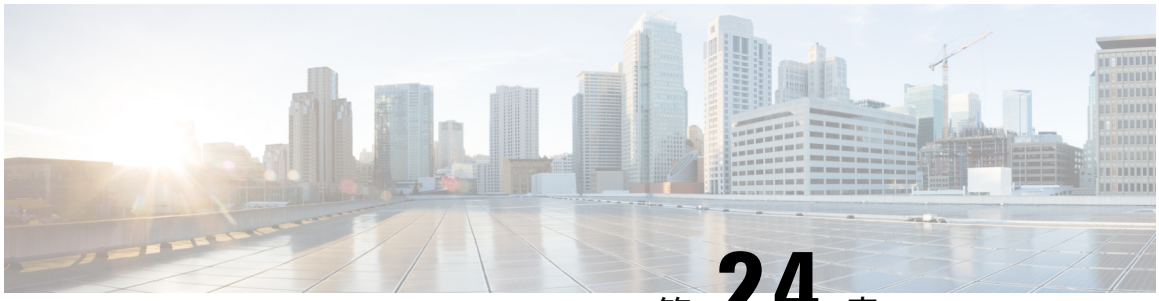
ステップ 3 左側のナビゲーション パネルで [Settings] をクリックします。

[Settings] ページが表示されます。

ステップ 4 [Intrusion Rule Thresholds] で、[Global Rule Thresholding] を無効化します。

ステップ 5 ポリシーの保存、編集の続行、変更の破棄を行うか、またはシステム キャッシュで変更をそのままにしながら終了します。詳細については、「競合の解決とポリシー変更の確定 （314 ページ）」を参照してください。

次のタスク



第 24 章

アイデンティティ データの概要

アイデンティティ ポリシーは、ユーザ エージェント、ISE/ISE-PIC デバイス、またはキャプティブ ポータルを使用して、ネットワーク上のユーザに関するデータを取得するように設定できます。詳細については、ユーザ アイデンティティ ソース （429 ページ）を参照してください。

アイデンティティ データの用途

アイデンティティ データを収集することにより、以下を含む多くの機能を活用できます。

- レルム、ユーザ、ユーザ グループ、および ISE 属性条件を使用してアクセス コントロール ルールを作成することにより、ユーザ制御を実行します。
- 特定のインパクト フラグが設定された侵入イベントをシステムが生成すると、電子メール、SNMP トラップ、または syslog により警告が出されます。

ユーザ検出の基本

アイデンティティ ポリシーを使用してネットワーク上のユーザ活動をモニタできます。これにより、脅威、エンドポイント、およびネットワーク インテリジェンスをユーザ ID 情報に関連付けることができます。ネットワーク動作、トラフィック、およびイベントを個別のユーザに直接リンクすることによって、ポリシー違反、攻撃、またはネットワークの脆弱性の発生源の特定に役立てることができます。たとえば、以下について決定できます。

- 脆弱（レベル 1：赤）影響レベルの侵入イベントの対象になっているホストの所有者
- 内部攻撃またはポートスキャンを開始した人物
- ホスト重要度の高いサーバの不正アクセスを試みている人物

- 不合理な容量の帯域幅を使用している人物
- 重要なオペレーティング システム更新を適用しなかった人物
- 会社の IT ポリシーに違反してインスタント メッセージング ソフトウェアまたはピアツーピア ファイル共有アプリケーションを使用している人物

この情報を利用して ASA FirePOWER モジュールの他の機能を使用すると、リスクを軽減し、アクセス コントロールを実行し、その他の機能を中断から保護するアクションを実行できます。これらの機能により、監査制御が大幅に改善され、規制の順守が促進されます。

ユーザ アイデンティティ ソースを設定したら、ユーザ対応とユーザ制御を実行できます。

ユーザ対応

ユーザ データの表示や分析ができます。

ユーザ制御

ユーザ アクセス コントロール ルール条件を設定して、ユーザ対応から引き出した結論に基づいて、ネットワーク上のトラフィックでユーザやユーザ アクティビティをブロックできます。

ユーザ データは、正規のアイデンティティ ソース（アイデンティティ ポリシーにより参照される）から取得できます。

アイデンティティ ソースは、信頼できるサーバによりユーザ ログインが検証済みであれば、正規のものになります。正規のログインから取得されるデータを使用して、ユーザ対応とユーザ制御を実行できます。正規のユーザ ログインは、パッシブ認証とアクティブ認証から取得されます。

- パッシブ認証は、ユーザが外部サーバで認証するときに実行されます。ASA FirePOWER モジュールでサポートされているパッシブ認証方式は、ユーザ エージェントと ISE/ISE-PIC だけです。
- アクティブ認証は、ユーザが FirePOWER デバイスにより認証するときに実行されます。ASA FirePOWER モジュールでサポートされているアクティブ認証方式は、キャプティブ ポータルだけです。

次の表に、ASA FirePOWER モジュールでサポートされているユーザ アイデンティティ ソースの概要を示します。

ユーザ アイデンティティ ソース	サーバ要件	ソース タイプ	認証タイプ	ユーザ認識	ユーザ アクセス コントロール	詳細情報の参照先
ユーザ エージェント	Microsoft Active Directory	正規のログイン	パッシブ	対応	対応	ユーザー エージェントのアイデンティティ ソース （432 ページ）

ユーザ アイデンティティ ソース	サーバ要件	ソース タイプ	認証タイプ	ユーザ認識	ユーザ アクセス コントロール	詳細情報の参照先
ISE/ISE-PIC	Microsoft Active Directory	正規のログイン	パッシブ	対応	対応	ISE/ISE-PIC アイデンティティ ソース（433ページ）
キャプティブ ポータル	LDAP または Microsoft Active Directory	正規のログイン	アクティブ	対応	対応	キャプティブ ポータル アクティブ認証のアイデンティティ ソース（436ページ）

展開するアイデンティティ ソースを選択するには、以下を考慮します。

- キャプティブ ポータルを使用して、失敗した認証アクティビティを記録する必要があります。失敗認証試行で新しいユーザがデータベース内のユーザのリストに追加されることはありません。
- キャプティブ ポータルを使用するために、センシング インターフェイス（ルーテッド インターフェイスなど）の IP アドレスがあるアプライアンスを展開する必要があります。

ユーザ アイデンティティの展開

システムが任意のアイデンティティ ソースからのユーザ データをユーザ ログイン時に検出すると、そのログインのユーザは、ユーザ データベース内のユーザのリストに照らして確認されます。ログイン ユーザが既存のユーザと一致した場合は、ログインからのデータがそのユーザに割り当てられます。ログインが SMTP トラフィック内に存在しない場合は、既存のユーザと一致しないログインによって新しいユーザが作成されます。SMTP トラフィック内の一致しないログインは破棄されます。

ユーザ活動データベース

デバイス上のユーザ アクティビティ データベースには、設定済みのすべてのアイデンティティ ソースにより報告された、ネットワーク上のユーザ アクティビティのレコードが含まれています。システムは次の状況でイベントを記録します。

- 個別のログインまたはログオフを検出したとき
- 新しいユーザを検出したとき
- 手動でユーザが削除されたとき
- データベース内に存在しないユーザをシステムが検出したものの、ユーザ制限に達したためにそのユーザを追加できなかったとき

ユーザ データベース

ユーザ データベースには、設定済みのアイデンティティ ソースにより報告された、各ユーザのレコードが含まれています。

デバイスが保存できるユーザの合計数は、モデルごとに異なります。制限に達した場合は、ユーザを（手動またはデータベースの消去により）削除して、新規ユーザを追加できるようにする必要があります。

アイデンティティ ソースが特定のユーザ名を除外するように設定されている場合、それらのユーザ名のユーザ アクティビティ データは ASA FirePOWER モジュールに報告されません。これらの除外されたユーザ名はデータベースに残りますが、IP アドレスに関連付けられません。

現在のユーザ アイデンティティ

異なる複数のユーザによる同じホストへの複数のログインがシステムにより検出されると、特定のホストに同時にログインできるのは1ユーザのみであり、ホストの現在のユーザが最新の正式なユーザ ログインであると見なされます。複数のユーザがリモート セッション経由でログインしている場合は、サーバによって報告された最後のユーザが ASA FirePOWER モジュールに報告されるユーザです。

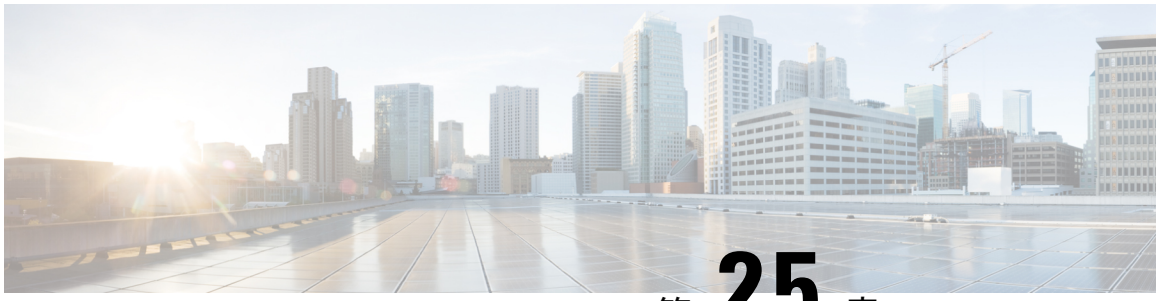
同じユーザによる同じホストへの複数のログインがシステムにより検出されると、システムは指定のホストへのユーザの最初のログインを記録し、それ以降のログインは無視します。あるユーザが特定のホストにログインしている唯一の人物の場合は、システムが記録する唯一のログインがオリジナルのログインです。

ただし、そのホストに別のユーザがログインした時点で、システムは新しいログインを記録します。その後で、オリジナルのユーザが再度ログインすると、その人物の新しいログインが記録されます。

ユーザ データベースの制限

デバイス モデルにより、モニタできるユーザの数、およびユーザ制御を実行するために使用できるユーザ数が決定されます。

ASDM によって管理される ASA FirePOWER モジュールを展開する場合、最大 2,000 の正規ユーザをユーザ データベースに保存できます。



第 25 章

レルムとアイデンティティ ポリシー

この章は、次のセクションで構成されています。

サーバとレルムについて

ライセンス：任意

レルムは、ASA FirePOWER モジュールとモニタリングの対象サーバ間の接続を確立します。レルムでは、サーバの接続設定と認証フィルタの設定を指定します。レルムでは次のことを実行できます。

- アクティビティをモニタするユーザとユーザ グループを指定する。
- 権限のあるユーザに関するユーザ メタデータについてサーバをクエリする。

レルム内のディレクトリとして複数のサーバを追加できますが、同じ基本レルム情報を共有する必要があります。レルム内のディレクトリは、LDAP サーバのみ、または AD サーバのみである必要があります。レルムを有効にすると、保存された変更は次回 ASA FirePOWER モジュールがサーバをクエリするときに適用されます。

ユーザ認識を行うには、サポートされるすべてのサーバタイプのレルムを設定する必要があります。モジュールはこれらの接続を使用して、POP3 および IMAP ユーザに関連付けられているデータについてサーバを照会します。モジュールは、POP3 および IMAP ログイン内の電子メール アドレスを使用して、Active Directory、OpenLDAP、または Oracle Directory Server

Enterprise Edition サーバ上の LDAP ユーザに関連付けます。たとえば、LDAP ユーザと電子メール アドレスが同じユーザの POP3 ログインをデバイスが検出すると、モジュールは LDAP ユーザのメタデータをそのユーザに関連付けます。

ユーザのアクセス コントロールを実行するために、以下を設定できます。

- ユーザ エージェントまたは ISE/ISE-PIC デバイス用に設定された AD サーバのレルム。

（注） SGT ISE 属性条件を設定することを計画しているものの、ユーザ、グループ、レルム、エンドポイント ロケーション、エンドポイント プロファイルの条件の設定は計画していない場合、レルムの設定はオプションです。

- キャプティブ ポータル用に設定された Oracle または OpenLDAP サーバのレルム。

（ユーザ認識またはユーザ制御のために）レルムを設定してユーザをダウンロードする場合、ASA FirePOWER モジュールはサーバを定期的にクエリして、前回のクエリ以降にアクティビティが検出された新規ユーザおよび更新されたユーザのメタデータを取得します。

ユーザ アクティビティ データはユーザ アクティビティ データベースに保存され、ユーザ アイデンティティ データはユーザ データベースに保存されます。アクセス コントロールで保存できる使用可能なユーザの最大数は、デバイス モデルによって異なります。含めるユーザとグループを選択するときは、ユーザの総数がモデルの上限より少ないことを確認してください。アクセス コントロール パラメータの範囲が広すぎる場合、ASA FirePOWER モジュールはできるだけ多くのユーザに関する情報を取得し、取得できなかったユーザ数をタスク キューで報告します。

（注） モジュールによって検出されたユーザを LDAP サーバから削除しても、ASA FirePOWER モジュールではユーザ データベース内の該当ユーザは削除されないため、手動で削除する必要があります。ただし、LDAP に対する変更は、ASA FirePOWER モジュールが権限のあるユーザのリストを次に更新したときにアクセス コントロール ルールに反映されます。

レルムがサポートされているサーバー

ライセンス：任意

次のタイプのサーバには、ASA FirePOWER モジュールからの TCP/IP アクセスがあれば、レルムを設定して接続できます。 <Table Title:Supported Servers for Realms>

サーバ タイプ	ユーザ認識によるデータ取得のサポート	ユーザ エージェントによるデータ取得のサポート	ISE/ISE-PIC によるデータ取得のサポート	キャプティブ ポータルによるデータ取得のサポート
Windows Server 2003、Windows Server 2008、および Windows Server 2012 上の Microsoft Active Directory	対応	対応	対応	対応（NTLM キャプティブ ポータルを使用する場合、Windows Server 2003 を除く）
Windows Server 2003 と Windows Server 2008 上の Oracle Directory Server Enterprise Edition 7.0	対応	非対応	非対応	対応
Linux 上の OpenLDAP	対応	非対応	非対応	対応

サーバ グループの設定に関して次の点に注意してください。

- ユーザ グループまたはグループ内のユーザに対してユーザ制御を実行する場合、サーバでユーザ グループを設定する必要があります。サーバの基本的なオブジェクト階層でユーザが編成されている場合、ASA FirePOWER モジュールはユーザ グループ制御を実行できません。

LDAP または AD サーバ グループのサイズを制限し、含めるユーザ数を最大で 1500 とすることを推奨します。サイズ超過のグループを含める（または除外する）ようにレルムを設定したり、サイズ超過のユーザ グループをターゲットにしたアクセス コントロール ルールを作成したりすると、パフォーマンス上の問題が生じる可能性があります。

- デフォルトでは、AD サーバはセカンダリ グループから報告するユーザの数を制限します。この制限は、セカンダリ グループのすべてのユーザが ASA FirePOWER モジュールに報告されるようにカスタマイズする必要があります。

サポートされるサーバ フィールド名

ライセンス：任意

レルムのサーバでは、ASA FirePOWER モジュールがサーバからユーザ メタデータを取得できるように、次の表に記載されているフィールド名を使用する必要があります。サーバ上のフィールド名が正しくない場合、ASA FirePOWER モジュールはそのフィールドの情報を使用してデータベースに入力できなくなります。

表 *64 : ASA FirePOWER* フィールドへのサーバ フィールドのマッピング

メタデータ	ASA FirePOWER モジュール	Active Directory	Oracle Directory Server	OpenLDAP
LDAP ユーザー名	Username	samaccountname	cn uid	cn uid
名	First Name	givenname	givenname	givenname
姓	Last Name	sn	sn	sn
電子メール アドレス	Email	mail userprincipalname（mail に値が設定されていない場合）	mail	mail
department	department	department distinguishedname（department に値が設定されていない場合）	department	ou
telephone number	Phone	telephonenumber	該当なし	telephonenumber

レルムに関する問題のトラブルシューティング

ライセンス：任意

予期しないサーバ接続の動作に気付いたら、レルム設定、デバイス設定、またはサーバ設定の調整を検討してください。

予期しない時間にユーザ タイムアウトが発生する

予期しない間隔でユーザ タイムアウトが行われていることに気付いたら、ユーザ エージェントまたは ISE/ISE-PIC デバイスの時間が ASA FirePOWER モジュールの時間と同期されていることを確認します。アプライアンスが同期されていないと、予想外の間隔でユーザのタイムアウトが実行される可能性があります。

レルム設定で指定したようにユーザが含まれない、または除外されない

Active Directory サーバのレルムを、Active Directory サーバのセカンダリ グループのメンバーであるユーザを含めるかまたは除外するように設定する場合、報告するユーザ数をサーバが制限することがあります。

デフォルトでは、Active Directory サーバはセカンダリ グループから報告するユーザの数を制限します。この制限は、セカンダリ グループのすべてのユーザが ASA FirePOWER モジュールに報告されるようにカスタマイズする必要があります。

ユーザのダウンロードが遅い

ユーザのダウンロードが遅いことに気付いたら、LDAPおよびADサーバグループに最大1500のユーザが含まれることを確認します。サイズ超過のユーザグループを含めるか除外するようにレルムを設定すると、パフォーマンスの問題が発生する可能性があります。

アイデンティティ ポリシーの基礎

ライセンス：任意

アイデンティティ ポリシーには、アイデンティティ ルールが含まれます。アイデンティティ ルールでは、トラフィックのセットを、レルムおよび認証方式（パッシブ認証、アクティブ認証、または認証なし）と関連付けます。

アイデンティティ ルールで呼び出す前に、使用するレルムおよび認証方式を完全に設定しておく必要があります。

- [Configuration] > [ASA FirePOWER Configuration] > [Integration] > [Realms] でアイデンティティ ポリシー外のレルムを設定します。
- [Configuration] > [ASA FirePOWER Configuration] > [Integration] > [Identity Sources] で、パッシブ認証のアイデンティティ ソース、ユーザ エージェント、およびISE/ISE-PICを設定します。
- アイデンティティ ポリシー内で、アクティブ認証のアイデンティティ ソース、キャプティブ ポータルを設定します。

1つ以上のアイデンティティ ポリシーを設定した後、アクセス コントロール ポリシーの1つのアイデンティティ ポリシーを呼び出す必要があります。ネットワークのトラフィックがアイデンティティ ルールの条件と一致し、認証方式がパッシブまたはアクティブであるとき、モジュールは指定されたレルムとトラフィックとを関連付け、指定されたアイデンティティ ソースを使用してトラフィックのユーザを認証します。

アイデンティティ ポリシーを設定しない場合、モジュールはユーザ認証を実行しません。

レルムの作成

ライセンス：Control

レルムの作成方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Integration] の順に選択します。 > > >

ステップ 2 [Realms] をクリックします。

ステップ 3 [New Realm] をクリックします。

ステップ 4 の説明に従って、基本的なレルム情報を設定します。 基本的なレルム情報の設定 （412 ページ）

ステップ 5 の説明に従って、ディレクトリを設定します。 レルム ディレクトリの設定 （413 ページ）

ステップ 6 の説明に従って、ユーザとユーザ グループのダウンロード（アクセス コントロールに必要）を設定します。 ユーザの自動ダウンロードの設定 （413 ページ）

ステップ 7 レルム設定を保存します。

ステップ 8 必要に応じて、の説明に従ってレルムを編集し、デフォルトのユーザセッション タイムアウトの設定を変更します。 レルム ユーザ セッション タイムアウトの設定 （414 ページ）

ステップ 9 レルム設定を保存します。

次のタスク

次の作業

- レルムの有効化または無効化 （426 ページ）の説明に従って、レルムを有効にします。
- 必要に応じて、タスクのステータスをモニタします。[Task Status] ページ（[Monitoring] > > [ASA FirePOWER Monitoring] > > [Task Status]）を参照してください。

レルム フィールド

ライセンス：任意

次のフィールドを使用して、レルムを設定します。

レルムの設定フィールド

AD Primary Domain

AD レルムのみの場合に、ユーザを認証する必要がある Active Directory サーバのドメイン。

AD Join Username および AD Join Password

Kerberos キャプティブ ポータル アクティブ認証を意図した AD レルムの場合、クライアントをドメインに参加させる適切な権限を持つユーザの識別用のユーザ名とパスワード。

Kerberos（または Kerberos をオプションとする場合に HTTP ネゴシエート）を、アイデンティティ ルールの [Authentication Type] として選択する場合、選択する [Realm] は、Kerberos キャプティブ ポータル認証を実行できるように、[AD Join Username] と [AD Join Password] を使用して設定する必要があります。

Description

（任意）レルムの説明。

Directory Username および Directory Password

取得するユーザ情報に適切な権限を持っているユーザの識別用のユーザ名とパスワード。

Base DN

ASA FirePOWER モジュールがユーザ データの検索を開始するサーバのディレクトリ ツリー。

通常、ベースDNには、企業ドメインおよび部門を示す基本構造があります。たとえば、Example 社のセキュリティ（Security）部門のベース DN は、ou=security,dc=example,dc=com となります。

Group DN

ASA FirePOWER モジュールがグループ属性を持つユーザを検索するサーバのディレクトリ ツリー。

Group Attribute

サーバのグループ属性：[Member]、[Unique Member]、[Custom]。

Name

レルムの一意の名前。

Type

レルム、AD、または LDAP のタイプ。

User Session Timeout: Authenticated Users

ユーザ セッションがタイムアウトするまでの最大時間（分単位）。

パッシブ認証されたユーザのセッションがタイムアウトした場合、ユーザは[Unknown] と識別され、現在のセッションはアクセス コントロール ルールの設定に応じて許可またはブロックされます。モジュールは、次回ログイン時にユーザを再度識別します。

アクティブ認証された（キャプティブ ポータル）ユーザのセッションがタイムアウトした場合、ユーザは再認証を要求されます。

User Session Timeout: Failed Authentication Users

アクティブ認証の試行失敗後にユーザのセッションがタイムアウトとなる時間（分単位）。認証に失敗したユーザのセッションがタイムアウトすると、ユーザは再認証を要求されます。

User Session Timeout: Guest Users

アクティブ認証された（キャプティブ ポータル）ゲスト ユーザのセッションがタイムアウトされるまでの最大時間（分単位）。ユーザのセッションがタイムアウトすると、ユーザは再認証を要求されます。

レルムのディレクトリ フィールド

これらの設定は、レルム内の個々のサーバ（ディレクトリ）に適用されます。

Encryption

サーバ接続に使用する暗号化方式。暗号化方式を指定する場合、このフィールドにホスト名を指定する必要があります。

Hostname / IP Address

サーバのホスト名または IP アドレス。

Port

サーバ接続に使用するポート。

SSL Certificate

サーバへの認証に使用する SSL 証明書。SSL 証明書を使用するには、[Encryption] タイプを設定する必要があります。

認証に証明書を使用する場合、証明書のサーバー名は、サーバーの [Hostname/IP Address] と一致する必要があります。たとえば、IP アドレスとして 10.10.10.250 を使用し、証明書内で computer1.example.com を使用した場合は、接続が失敗します。

ユーザのダウンロード フィールド

Download for access control

このチェックボックスをオンにすると、ユーザ データの自動ダウンロードが設定されます。ユーザ認識と、状況によっては、ユーザのアクセス コントロールのためにデータを使用できます。

ダウンロードの頻度を設定するには、[Begin automatic download at] および [Repeat every] ドロップダウン メニューを使用します。

基本的なレルム情報の設定

ライセンス：Control

基本的なレルム情報の設定方法：

ステップ 1 [Add New Realm] ページで、[Name] および、必要に応じて [Description] を入力します。

ステップ 2 ドロップダウン リストから [Type] を選択します。

ステップ 3 AD レルムを設定する場合は、[AD Primary Domain] を入力します。

ステップ 4 Kerberos キャプティブ ポータル アクティブ認証を意図した AD レルムを設定する場合、ユーザの識別用の [AD Join Username] と [AD Join Password] を、クライアントをドメインに参加させるための適切な権限で入力します。

ステップ 5 取得するユーザ情報に適切な権限を持っているユーザの識別用の [Directory Username] と [Directory Password] を入力します。

ステップ 6 ディレクトリの [Base DN] を入力します。
ステップ 7 ディレクトリの [Group DN] を入力します。
ステップ 8 オプションで、ドロップダウン リストから [Group Attribute] を選択します。
ステップ 9 [OK] をクリックします。

次のタスク

- の説明に従って、レルム ディレクトリを設定します。 レルム ディレクトリの設定 （413 ページ）

レルム ディレクトリの設定

ライセンス：Control

レルム ディレクトリの設定方法：

ステップ 1 [Directory] タブで、[Add Directory] をクリックします。
ステップ 2 サーバのホスト名/IP アドレスとポートを入力します。
ステップ 3 [暗号化モード（Encryption Mode）] を選択します。
ステップ 4 オプションで、ドロップダウン リストから SSL 証明書を選択します。追加アイコン（）をクリックすると、オブジェクトを即座に作成することができます。
ステップ 5 接続をテストする場合は、[Test] をクリックします。
ステップ 6 [OK] をクリックします。

ユーザの自動ダウンロードの設定

ライセンス：Control

含めるグループを指定しなかった場合、ASA FirePOWER モジュールは指定されたパラメータと一致するすべてのグループのユーザ データを取得します。パフォーマンス上の理由から、アクセス コントロールに使用するユーザを表すグループだけを明示的に含めることをお勧めします。

ユーザの自動ダウンロードの設定方法：

ステップ 1 [User Download] タブで、[Download users and groups (required for user access control)] チェックボックスをオンにします。
ステップ 2 ドロップダウン リストから [Begin automatic download at] の時間を選択します。
ステップ 3 [Repeat Every] ドロップダウン リストから、ダウンロード間隔を選択します。

ステップ 4 ダウンロードからユーザ グループを含めるか除外するには、[Available Groups] 列からユーザ グループを選択し、[Add to Include] または [Add to Exclude] をクリックします。

ステップ 5 個々のユーザを含めるか除外するには、[Groups to Include] または [Groups to Exclude] の下のフィールドにユーザを入力し、[Add] をクリックします。

（注） ダウンロードからユーザを除外すると、そのユーザを条件として使用するアクセス コントロール ルールを作成できなくなります。複数のユーザはカンマで区切ります。このフィールドでは、アスタリスク（*）をワイルドカード文字として使用できます。

レルム ユーザ セッション タイムアウトの設定

ライセンス：Control

（注） 予期しない間隔でモジュールがユーザ タイムアウトを行っていることに気付いたら、ユーザ エージェントまたは ISE/ISE-PIC デバイスの時間が ASA FirePOWER モジュールの時間と同期されていることを確認します。

レルム ユーザ セッション タイムアウトを設定する方法：

ステップ 1 [Realm Configuration] タブを選択します。

ステップ 2 [Authenticated Users]、[Failed Authentication Users]、および [Guest Users] にユーザ セッション タイムアウト値を入力します。

ステップ 3 [Save] をクリックするか、レルムの編集を続けます。

アイデンティティ ポリシーの設定

ライセンス：Control

はじめる前に

- の説明に従って、1 つ以上のレルムを作成し、有効にします。レルムの作成（409 ページ）

アイデンティティ ポリシーの設定方法：

アクセス：管理者/アクセス管理者/ネットワーク管理者

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Identity Policy] の順に選択します。

ステップ 2 [Name] を入力し、任意で [Description] を入力します。

ステップ 3 ポリシーにルールを追加する場合は、アイデンティティ ルールの作成（418 ページ）の説明に従って、[Add Rule] をクリックします。

ステップ 4 ルール カテゴリを追加する場合は、アイデンティティ ルール カテゴリの追加（427 ページ）の説明に従って、[Add Category] をクリックします。

ステップ 5 キャプティブ ポータルを使用するアクティブ認証を設定する場合は、キャプティブ ポータル（アクティブ認証）の設定（415 ページ）の説明に従って、[Active Authentication] をクリックします。

キャプティブ ポータル（アクティブ認証）フィールド

ライセンス：任意

次のフィールドを使用して、キャプティブ ポータルを設定します。

Server Certificate

キャプティブ ポータル デーモンが示すサーバ証明書。

Port

キャプティブ ポータル接続に使用するポート番号。このフィールドのポート番号は、captive-portal CLI コマンドを使用して ASA FirePOWER デバイスで設定したポート番号と一致している必要があります。

Maximum login attempts

ユーザのログイン要求がモジュールによって拒否されるまでに許容されるログイン試行失敗の最大数。

Active Authentication Response Page

キャプティブ ポータル ユーザに対して表示される、システム提供またはカスタムの HTTP 応答ページ。アイデンティティ ポリシーのアクティブ認証で [Active Authentication Response Page] を選択したら、HTTP 応答ページで 1 つ以上のアイデンティティ ルールを認証タイプとして設定する必要があります。

システム提供の HTTP 応答ページには、[Username] と [Password] フィールドに加え、[Login as guest] ボタンがあり、ユーザはゲストとしてネットワークにアクセスできます。ログイン方法を 1 つだけ表示する場合は、カスタム HTTP 応答ページを設定します。

キャプティブ ポータル（アクティブ認証）の設定

ライセンス：Control

キャプティブ ポータル ユーザを表示するために、システム提供またはカスタムのいずれかの HTTP 応答ページを選択できます。システム提供の HTTP 応答ページには、[Username] と [Password] のフィールドに加え、[Login as guest] ボタンがあり、ユーザはゲストとしてネット

ワークにアクセスできます。単一のログイン方法を表示するには、カスタムHTTP応答ページを設定します。

キャプティブ ポータルの詳細については、を参照してください。 キャプティブ ポータル アクティブ認証のアイデンティティ ソース （436 ページ）

はじめる前に

- デバイスが管理している 1 つ以上の ASA FirePOWER デバイスが、ルーテッド モードでバージョン 9.5(2) 以降を実行していることを確認します。
- キャプティブ ポータルに使用するポート宛てのトラフィックを許可するようにアクセス コントロール ルールを設定します。
- HTTPS トラフィックでキャプティブ ポータルを使用してアクティブ認証を実行する場合は、キャプティブ ポータルを使用して認証するユーザから送信されたトラフィックを復号する SSL ルールを作成する必要があります。
- キャプティブ ポータル接続でトラフィックを復号する場合、キャプティブ ポータルに使用するポート宛てのトラフィックを復号する SSL ルールを作成します。
- **captive-portal ASA** CLI コマンドを使用してアクティブ認証のキャプティブ ポータルを有効にし、ASA Firewall コンフィギュレーション ガイド（バージョン 9.5(2) 以降）（https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html）の説明に従い、ポートを定義します。

キャプティブ ポータルの設定方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Identity Policy] の順に選択し、アイデンティティ ポリシーを編集します。 > > >

ステップ 2 [Active Authentication] をクリックします。

ステップ 3 ドロップダウン リストから、該当する [Server Certificate] を選択します。必要に応じて、追加アイコン（  ）をクリックして、オブジェクトをその場で作成します。

ステップ 4 [Port] を入力し、[Maximum login attempts] を指定します。

ステップ 5 オプションで、HTTP 応答ページでユーザを認証するには、[Active Authentication Response Page] を選択します。

ステップ 6 [**Save**] をクリックします。

ステップ 7 アイデンティティ ルールの作成 （418 ページ）の説明に従って、[Action] として [Active Authentication] を使用するアイデンティティ ルールを設定します。ステップ 5 で応答ページを選択した場合は、[Authentication Type] として HTTP 応答ページを選択する必要もあります。

次のタスク

- 設定変更を展開します。を参照してください。 設定変更の導入 （92 ページ）

アクティブ認証からのアプリケーションの除外

ライセンス：Control

アプリケーション（HTTP ユーザエージェント文字列によって指定される）を選択し、キャプティブ ポータル（アクティブ認証）から除外することができます。これにより、選択されたアプリケーションからのトラフィックが認証を受けずにアイデンティティ ポリシーを通過できるようになります。

アプリケーションをアクティブ認証から除外する方法：

ステップ 1 アイデンティティ ルール エディタ ページの [Realm & Settings] タブで、[Application Filters] リストにあるシスコ提供のフィルタを使用して、フィルタに追加するアプリケーションのリストを絞り込みます。

- リストを展開および縮小するには、各フィルタ タイプの横にある矢印をクリックします。
- フィルタ タイプを右クリックし、[Check All] または [Uncheck All] をクリックします。このリストには、各タイプで選択したフィルタ数が示されることに注意してください。
- 表示されるフィルタを絞り込むには、[Search by name] フィールドに検索文字列を入力します。これは、カテゴリとタグの場合に特に有効です。検索をクリアするには、クリア アイコン（×）をクリックします。
- フィルタのリストを更新し、選択したフィルタをすべてクリアするには、リロード アイコン（↻）をクリックします。
- すべてのフィルタと検索フィールドをクリアするには、[すべてのフィルタをクリア（Clear All Filters）] をクリックします。

（注） リストには一度に 100 のアプリケーションが表示されます。

ステップ 2 [Available Applications] リストから、フィルタに追加するアプリケーションを選択します。

- 前の手順で指定した制約を満たすすべてのアプリケーションを追加するには、[All apps matching the filter] を選択します。
- 表示される個別のアプリケーションを絞り込むには、[Search by name] フィールドに検索文字列を入力します。検索をクリアするには、クリア アイコン（×）をクリックします。

.

- 使用可能な個別のアプリケーションのリストを参照するには、リストの下部にあるページング アイコンを使用します。
- アプリケーションのリストを更新し、選択したアプリケーションをすべてクリアするには、リロード アイコン（↻）をクリックします。

ステップ 3 外部認証から除外する、選択したアプリケーションを追加します。クリックしてドラッグするか、[ルールに追加（Add to Rule）] をクリックできます。結果は次のもので構成されています。

- 選択したアプリケーション フィルタ

- 選択した個別の使用可能なアプリケーション、または [All apps matching the filter]

次のタスク

- の説明に従って、アイデンティティ ルールの設定を続けます。 アイデンティティ ルールの作成 （418 ページ）

アイデンティティ ポリシーとアクセス コントロール ポリシーの関連付け

ライセンス：Control

ASA FirePOWER モジュールには、現在適用されている 1 つのアイデンティティ ポリシーを設定できます。アイデンティティ ポリシーを個別に適用することはできません。適用されたアイデンティティ ポリシー、または現在適用されているアイデンティティ ポリシーを削除することはできません。

アイデンティティ ポリシーとアクセス コントロール ポリシーを関連付ける方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。
ステップ 2 [Advanced] タブを選択します。
ステップ 3 [Identity Policy Settings] の横にある編集アイコン（）をクリックします。
ステップ 4 ドロップダウンからアイデンティティ ポリシーを選択します。
ステップ 5 [OK] をクリックします。
ステップ 6 [Store ASA FirePOWER Changes] をクリックして変更を保存します。

アイデンティティ ルールの作成

ライセンス：Control

アイデンティティ ルールの作成方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Identity Policy] の順に選択します。 > > >
ステップ 2 [Add Rule] をクリックします。
ステップ 3 の説明に従って、アイデンティティ ルールの基本的な情報を設定します。 基本的なアイデンティティ ルール情報の設定 （421 ページ）
ステップ 4 必要に応じて、の説明に従って、ゾーン条件を追加します。 アイデンティティ ルールへのゾーン条件の追加 （423 ページ）

（注） キャプティブ ポータルにルールを設定していて、キャプティブ ポータル デバイスにインライン インターフェイスとルーテッド インターフェイスが含まれている場合は、デバイス上のルーテッド インターフェイスのみを対象とするゾーン条件を設定する必要があります。

ステップ 5 必要に応じて、の説明に従って、ネットワークまたは地理位置情報の条件を追加します。 アイデンティティ ルールへのネットワークまたは位置情報条件の追加 （422 ページ）

ステップ 6 必要に応じて、の説明に従って、ポート条件を追加します。 アイデンティティ ルールへのポート条件の追加 （422 ページ）

ステップ 7 の説明に従って、ルールをレルムに関連付けます。 アイデンティティ ルールでのレルムの関連付けとアクティブ認証設定の設定 （424 ページ）

ステップ 8 [Add] をクリックします。

ステップ 9 [Store ASA FirePOWER Changes] をクリックします。

次のタスク

- 設定変更を展開します。を参照してください。 設定変更の導入 （92 ページ）

アイデンティティ ルール フィールド

次のフィールドを使用して、アイデンティティ ルールを設定します。

Enabled

このオプションを選択すると、アイデンティティ ポリシーのアイデンティティ ルールが有効になります。このオプションの選択を解除すると、アイデンティティ ルールが無効になります。

Action

指定された**レルム**でユーザに実行する認証のタイプ。パッシブ認証（ユーザエージェントまたは ISE/ISE-PIC）、アクティブ認証（キャプティブ ポータル）、または認証なしを選択できます。アイデンティティ ルールのアクションとして選択する前に、認証方式、またはアイデンティティ ソースを完全に設定する必要があります。

Realm

指定された**アクション**の実行対象になるユーザが含まれるレルム。アイデンティティ ルールのレルムとして選択する前に、レルムを完全に設定する必要があります。

Kerberos（または Kerberos をオプションとする場合に HTTP ネゴシエート）を、アイデンティティ ルールの [Authentication Type] として選択する場合、選択する [Realm] は、Kerberos キャプティブ ポータル認証を実行できるように、[AD Join Username] と [AD Join Password] を使用して設定する必要があります。

Use active authentication if passive authentication cannot identify user

このオプションを選択すると、パッシブ認証でユーザを識別できない場合にアクティブ認証を使用してユーザが認証されます。このオプションを選択するには、アクティブ認証（キャプティブ ポータル）を設定する必要があります。

このオプションを無効にすると、パッシブ認証で識別できないユーザは [Unknown] と識別されます。このフィールドを表示するには、パッシブ認証に対するルールアクションを設定する必要があります。

Identify as Special Identities/Guest if authentication cannot identify user

このオプションを選択すると、ASDM インターフェイスのすべてのエリアで不明ユーザが**特別 ID/ゲスト**として識別されます。このフィールドを表示するには、ルールアクションをアクティブ認証に設定するか、[Use active authentication if passive authentication cannot identify user] を選択する必要があります。

Authentication Type

アクティブ認証を実行するために使用する方法です。選択は、レルム、LDAP、または AD のタイプによって異なります。

- 暗号化されていない HTTP 基本認証（BA）接続を使用してユーザを認証するには、[HTTP Basic] を選択します。ユーザはブラウザのデフォルトの認証ポップアップ ウィンドウを使用してネットワークにログインします。

ほとんどの Web ブラウザは、HTTP 基本ログインからクレデンシャルをキャッシュし、古いセッションがタイムアウトした後にシームレスに新しいセッションを開始するためにそのクレデンシャルを使用します。

- NT LAN Manager（NTLM）接続を使用してユーザを認証する場合は、[NTLM] を選択します。この選択は、AD レルムを選択するときにのみ使用できます。ユーザはブラウザのデフォルトの認証ポップアップ ウィンドウを使用してネットワークにログインします。アイデンティティ ルール認証タイプとして [NTLM] を選択した場合、アイデンティティ ルールのレルムとして Windows Server 2003 を使用することはできません。
- Kerberos 接続を使用してユーザを認証する場合は、[Kerberos] を選択します。この選択は、セキュア LDAP（LDAPS）が有効になっているサーバに対して AD レルムを選択する場合にのみ可能です。透過的な認証がユーザのブラウザで設定されている場合、ユーザは自動的にログインします。透過的な認証が設定されていない場合、ユーザは各自のブラウザでデフォルトの認証ポップアップ ウィンドウを使用してネットワークにログインします。

選択する [Realm] は、Kerberos キャプティブ ポータル認証を実行するために、[AD Join Username] および [AD Join Password] を使用して設定する必要があります。

（注） 設定済みの DNS 解決があり、Kerberos（または Kerberos をオプションとする場合は HTTP ネゴシエート）キャプティブ ポータルを実行するアイデンティティ ルールを作成する場合は、キャプティブ ポータル デバイスの完全修飾ドメイン名（FQDN）を解決するように DNS サーバを設定する必要があります。FQDN は、DNS 設定時に指定したホスト名と一致する必要があります。ASA with FirePOWER Services デバイスの場合、FQDN は、キャプティブ ポータルに使用されるルーテッド インターフェイスの IP アドレスに解決される必要があります。

- キャプティブ ポータル サーバが認証接続に HTTP 基本認証、Kerberos、または NTLM を選択できるようにするには、[HTTP Negotiate] を選択します。この選択は、AD レルムを選択するときにのみ使用できます。ユーザはブラウザのデフォルトの認証ポップアップ ウィンドウを使用してネットワークにログインします。

選択する [Realm] は、Kerberos キャプティブ ポータル認証を実行するために、[AD Join Username] および [AD Join Password] を使用して設定する必要があります。

HTTP ネゴシエート キャプティブ ポータルを実行するアイデンティティ ルールを作成しようとしており、DNS 解決は設定済みである場合、キャプティブ ポータル デバイスのホスト名を解決する DNS サーバを設定する必要があります。キャプティブ ポータルに使用するデバイスのホスト名は、DNS の設定時に入力したホスト名と一致している必要があります。

- ASA FirePOWER モジュール提供のページ、またはカスタムの HTTP 応答ページを使用してユーザを認証する場合は、[HTTP Response Page] を選択します。ユーザは設定された応答ページを使用してネットワークにログインします。

システム提供の HTTP 応答ページには、[Username] と [Password] のフィールドに加え、[Login as guest] ボタンがあり、ユーザはゲストとしてネットワークにアクセスできます。単一のログイン方法を表示するには、カスタム HTTP 応答ページを設定します。

ゲストとしてログインするユーザは、Web インターフェイス上ではユーザ名 [ゲスト（Guest）] で表示され、そのレルムはアイデンティティ ルールで指定されたレルムになります。

基本的なアイデンティティ ルール情報の設定

ライセンス：Control

基本的なアイデンティティ ルール情報の設定方法：

ステップ 1 アイデンティティ ルール エディタ ページで、[Name] を入力します。

ステップ 2 ルールを有効にするかどうか [Enabled] を指定します。

ステップ 3 ルール カテゴリにルールを追加するには、を参照してください。アイデンティティ ルール カテゴリの追加 （427 ページ）

ステップ 4 ドロップダウン リストからルールの [Action] を選択します。

ステップ 5 [Add] をクリックするか、ルールの編集を続けます。

アイデンティティルールへのネットワークまたは位置情報条件の追加

ライセンス：Control

アイデンティティ ルールにネットワークまたは地理位置情報条件を追加する方法：

ステップ 1 アイデンティティ ルール エディタ ページで、[Networks] タブを選択します。

ステップ 2 [Available Networks] から、次のように追加するネットワークを見つけます。

- ネットワーク オブジェクト（後で条件に追加可能）をその場で追加するには、[Available Networks] リストの上にある追加アイコン（）をクリックします。
- 追加するネットワーク オブジェクトまたは地理位置情報オブジェクトを検索するには、適切なタブを選択し、[Available Networks] リストの上にある [Search by name or value] プロンプトをクリックして、オブジェクトのコンポーネントの 1 つのオブジェクト名または値を入力します。入力を開始するとリストが更新され、一致するオブジェクトが表示されます。

ステップ 3 オブジェクトを選択するには、そのオブジェクトをクリックします。すべてのオブジェクトを選択するには、右クリックして [Select All] を選択します。

ステップ 4 [Add to Source] または [Add to Destination] をクリックします。

ステップ 5 手動で指定する送信元または宛先 IP アドレスまたはアドレス ブロックを追加します。[送信元ネットワーク（Source Networks）] リストまたは [宛先ネットワーク（Destination Networks）] リストの下にある [IP アドレスの入力（Enter an IP address）] プロンプトをクリックし、1 つの IP アドレスまたはアドレス ブロックを入力して [追加（Add）] をクリックします。

ステップ 6 [Add] をクリックするか、ルールの編集を続けます。

アイデンティティ ルールへのポート条件の追加

ライセンス：Control

アイデンティティ ルールにポート条件を追加する方法：

ステップ 1 アイデンティティ ルール エディタ ページで、[Ports] タブを選択します。

ステップ 2 [Available Ports] から、追加する TCP ポートを次のように探します。

- TCP ポート オブジェクト（後で条件に追加可能）をその場で追加するには、[Available Ports] リストの上にある追加アイコン（）をクリックします。
- 追加する TCP ベースのポート オブジェクトおよびグループを検索するには、[Available Ports] リストの上にある [Search by name or value] プロンプトをクリックし、オブジェクトの名前またはオブジェク

トのポートの値を入力します。入力を開始するとリストが更新され、一致するオブジェクトが表示されます。たとえば、「443」と入力すると、ASA FirePOWER モジュールに提供されている HTTP ポート オブジェクトが表示されます。

ステップ 3 TCP ベースのポート オブジェクトを 1 つ選択するには、それをクリックします。TCP ベースのポート オブジェクトをすべて選択するには、右クリックして [Select All] を選択します。非 TCP ベースのポートを含んでいるオブジェクトは、ポート条件に追加できません。

ステップ 4 [Add to Source] または [Add to Destination] をクリックします。

ステップ 5 送信元または宛先のポートを手動で指定するには、[Selected Source Ports] または [Selected Destination Ports] リストの下にある [Port] にポート番号を入力します。0 ～ 65535 の値を持つ 1 つのポートを指定できます。

ステップ 6 [Add] をクリックします。

（注） ASA FirePOWER モジュールでは、無効な設定となるルール条件にはポートが追加されません。

ステップ 7 [Add] をクリックするか、ルールの編集を続けます。

アイデンティティ ルールへのゾーン条件の追加

ライセンス：Control

キャプティブ ポータルに使用する予定のデバイスにインライン インターフェイスとルーテッド インターフェイスの両方が含まれる場合、キャプティブ ポータル デバイス上でルーテッド インターフェイスだけを対象とするようにキャプティブ ポータル アイデンティティ ルールでゾーン条件を設定する必要があります。

セキュリティ ゾーンの詳細については、を参照してください。セキュリティ ゾーンの操作（64 ページ）

アイデンティティ ルールにゾーン条件を追加する方法：

ステップ 1 アイデンティティ ルール エディタ ページで、[Zones] タブを選択します。

ステップ 2 [Available Zones] から、追加するゾーンを見つけます。追加するゾーンを検索するには、[Available Zones] リストの上にある [Search by name] プロンプトをクリックし、ゾーン名を入力します。入力すると、リストが更新されて一致するゾーンが表示されます。

ステップ 3 クリックすると、ゾーンを選択できます。すべてのゾーンを選択するには、右クリックして [Select All] を選択します。

ステップ 4 [Add to Source] または [Add to Destination] をクリックします。

ステップ 5 [Add] をクリックするか、ルールの編集を続けます。

アイデンティティルールでのレルムの関連付けとアクティブ認証設定の設定

ライセンス：Control

アイデンティティ ルールをレルムに関連付け、オプションで、アクティブ認証の追加設定を設定します。

アイデンティティ ルールをレルムに関連付ける方法：

ステップ 1 アイデンティティ ルール エディタ ページで、[Realm & Settings] タブを選択します。

ステップ 2 ドロップダウン リストから [Realm] を選択します。

ステップ 3 オプションで、[Use active authentication if passive authentication cannot identify user] チェックボックスをオンにします。このチェックボックスは、パッシブ認証ルールを設定するときにのみ表示されます。

ステップ 4 ステップ 3 でチェックボックスをオンにした場合、またはこれがアクティブ認証ルールである場合、ステップ 4 に進みます。それ以外の場合は、ステップ 8 に進みます。

ステップ 5 オプションで、[Identify as Special Identities/Guest if authentication cannot identify user] チェックボックスを選択します。

ステップ 6 ドロップダウン リストから [Authentication Type] を選択します。

ステップ 7 必要に応じて、[Exclude HTTP User-Agents] を使用し、アクティブ認証からのアプリケーションの除外 （417 ページ）の説明に従って、特定のアプリケーション トラフィックをアクティブ認証から除外します。

ステップ 8 [Add] をクリックするか、ルールの編集を続けます。

レルムの管理

ライセンス：Control

レルムの管理方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Integration] > [Realms] の順に選択します。 > > >

ステップ 2 レルムを削除する場合は、削除アイコン（）をクリックします。

ステップ 3 レルムを編集する場合は、レルムの横にある編集アイコン（）をクリックし、レルムの作成 （409 ページ）の説明に従って変更を行います。

ステップ 4 レルムを有効または無効にするには、レルムの有効化または無効化 （426 ページ）の説明に従って、有効または無効にするレルムの横の [State] スライダをクリックします。

ステップ 5 ユーザとユーザ グループをオンデマンドでダウンロードする場合は、オンデマンドでのユーザとユーザ グループのダウンロード （425 ページ）の説明に従ってダウンロード アイコン（）をクリックします。

ステップ 6 レルムをコピーする場合は、コピー アイコン（）をクリックします。

ステップ 7 レルムを比較する場合は、レルムの比較 （425 ページ）を参照してください。

レルムの比較

ライセンス：Control

レルムの比較方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Integration] > [Realms] の順に選択します。
ステップ 2 [Compare Realms] をクリックします。
ステップ 3 [Compare Against] ドロップダウン リストから [Compare Realm] を選択します。
ステップ 4 [Realm A] および [Realm B] ドロップダウン リストから、比較するレルムを選択します。
ステップ 5 [OK] をクリックします。
ステップ 6 個々の変更を選択する場合は、タイトル バーの上の [Previous] または [Next] をクリックします。
ステップ 7 必要に応じて、[Comparison Report] をクリックして、レルム比較レポートを生成します。
ステップ 8 必要に応じて、[New Comparison] をクリックして、新しいレルム比較ビューを生成します。

オンデマンドでのユーザとユーザ グループのダウンロード

ライセンス：Control

レルムのユーザまたはグループ ダウンロード パラメータを変更する場合、またはサーバでユーザまたはグループを変更して、変更をユーザ制御にすぐに反映させる場合は、サーバからのオンデマンド ユーザ ダウンロードの実行を ASA FirePOWER モジュールに強制できます。

ASA FirePOWER モジュールがサーバから取得可能なユーザの最大数はデバイス モデルによって異なります。レルムのダウンロード パラメータの範囲が広すぎる場合、ASA FirePOWER モジュールはできるだけ多くのユーザに関する情報を取得し、取得できなかったユーザ数をタスク キューで報告します。

はじめる前に

- レルムの有効化または無効化 （426 ページ）の説明に従って、レルムを有効にします。

ユーザとユーザ グループをオンデマンドでダウンロードする方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Integration] > [Realms] の順に選択します。 > > >
ステップ 2 ユーザとユーザ グループをダウンロードするレルムの横のダウンロード アイコン（）をクリックします。

次のタスク

- 必要に応じて、タスクのステータスをモニタします。[Task Status] ページ（[Monitoring] > > [ASA FirePOWER Monitoring] > > [Task Status]）を参照してください。

レルムの有効化または無効化

ライセンス：Control

ASA FirePOWER モジュールがサーバにクエリできるのは、有効になっているレルムだけです。問い合わせを停止するには、レルムを無効にします。

レルムを有効または無効にする方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Integration] > [Realms] の順に選択します。 > > >

ステップ 2 有効または無効にするレルムの横にある [State] スライダをクリックします。

次のタスク

- 必要に応じて、タスクのステータスをモニタします。[Task Status] ページ（[Monitoring] > [ASA FirePOWER Monitoring] > [Task Status]）を参照してください。 > >

アイデンティティ ポリシーの管理

ライセンス：Control

アイデンティティ ポリシーの管理方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Identity Policy] の順に選択します。

ステップ 2 ポリシーをコピーする場合は、コピー アイコン（  ）をクリックします。

ステップ 3 ポリシーのレポートを生成する場合は、レポート アイコン（  ）をクリックします。

アイデンティティ ルールの管理

ライセンス：Control

アイデンティティ ルールを管理する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Identity Policy] の順に選択します。

ステップ 2 アイデンティティ ルールを編集する場合は、編集アイコン（）をクリックし、アイデンティティ ルールの作成 （418 ページ）の説明に従って変更を行います。

ステップ 3 アイデンティティ ルールを削除する場合は、削除アイコン（）をクリックします。

ステップ 4 [Store ASA FirePOWER Changes] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の導入 （92 ページ）を参照してください。

アイデンティティ ルール カテゴリの追加

ライセンス：Control

アイデンティティ ルール カテゴリを追加する方法：

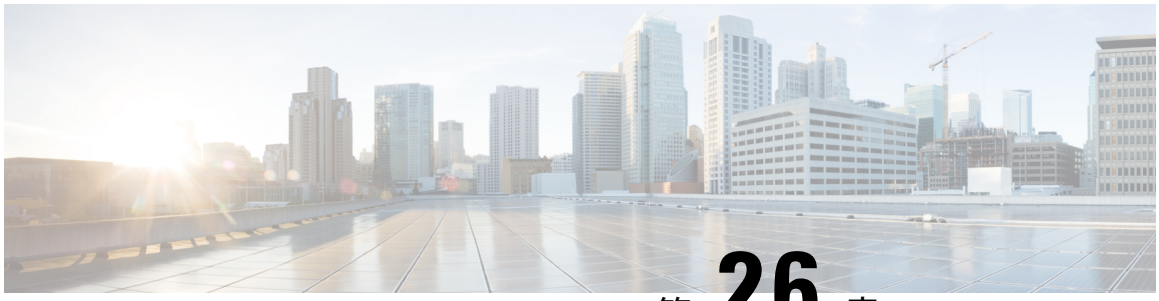
ステップ 1 アイデンティティ ルール エディタ ページでは、次の選択肢があります。

- 最初の [Insert] ドロップダウン リストから [above Category] を選択した後、2 番目のドロップダウン リストからカテゴリを選択します。ここで選択したカテゴリの上にルールが配置されます。
- ドロップダウン リストから [below rule] を選択し、既存のルール番号を入力します。このオプションが有効なのは、ポリシーに少なくとも 1 つのルールが存在する場合のみです。
- ドロップダウン リストから [above rule] を選択し、既存のルール番号を入力します。このオプションが有効なのは、ポリシーに少なくとも 1 つのルールが存在する場合のみです。

ステップ 2 [OK] をクリックします。

（注） 削除するカテゴリに含まれるルールは、その上にあるカテゴリに追加されます。

ステップ 3 [Add] をクリックするか、ルールの編集を続けます。



第 26 章

ユーザ アイデンティティ ソース

ASA FirePOWER モジュールは、次のアイデンティティ ソースをサポートしています。

- 権限のあるユーザ エージェント レポートは、ユーザ認識とユーザ アクセス コントロールに関するユーザ データを収集します。ホストにログインまたはホストからログアウトするとき、または Active Directory クレデンシャルで認証するときにユーザをモニタするようにユーザ エージェントを設定するには、ユーザー エージェントのアイデンティティ ソース（432 ページ）を参照してください。
- 権限のあるレポートは、Identity Services Engine（ISE）または ISE-PIC レポートは、ユーザ認識とユーザ アクセス コントロールに関するユーザ データを収集します。ISE/ISE-PIC が展開されていて、Active Directory ドメイン コントローラ（DC）を使用した認証時にユーザをモニタするように ISE/ISE-PIC を設定する場合は、ISE/ISE-PIC アイデンティティ ソース （433 ページ）を参照してください。
- 権限のあるキャプティブ ポータル認証は、アクティブにネットワークのユーザを認証し、ユーザ認識とユーザ制御に関するユーザ データを収集します。キャプティブ ポータル認証を実行するために仮想ルータまたは FirePOWER Threat Defense デバイスを設定する場合は、キャプティブ ポータル アクティブ認証のアイデンティティ ソース （436 ページ）を参照してください。

これらのアイデンティティ ソースからのデータは、ASA FirePOWER モジュール ユーザ データベースおよびユーザ アクティビティ データベースに保存されます。データベース サーバ クエリを設定すると、モジュールに新しいデータを自動的にダウンロードできます。

ASA FirePOWER モジュールでのユーザ検出の詳細については、ユーザ検出の基本 （401 ページ）を参照してください。

ユーザアイデンティティ ソースに関する問題のトラブルシューティング

ライセンス：任意

ユーザ アイデンティティ ソースに関する問題のトラブルシューティングについては、次の各項を参照してください。

ユーザ エージェント

ユーザ エージェントの接続に関する問題が発生した場合は、*Firepower* ユーザ エージェント コンフィギュレーション ガイドを参照してください。

ユーザ エージェントによって報告されるユーザ データに関する問題が発生した場合は、次の点に注意してください。

- システムはデータがまだデータベースにないユーザ エージェント ユーザのアクティビティを検出すると、サーバからそれらに関する情報を取得します。状況によっては、システムが Active Directory サーバからこの情報を正常に取得するために 60 分かかることもあります。データ取得が成功するまで、ユーザ エージェント ユーザから見えるアクティビティはアクセス コントロール ルールで処理され、Web インターフェイスに表示されません。

ISE/ISE-PIC

ISE/ISE-PIC 接続に問題が起こった場合は、次のことを確認してください。

- ISE と FirePOWER システムを正常に統合するには、ISE 内の pxGrid アイデンティティ マッピング機能を有効にする必要があります。
- すべての ISE システム証明書と FirePOWER Management Center 証明書には、**serverAuth** と **clientAuth** 拡張キー使用値が含まれている必要があります。
- ISE デバイスの時間は、FirePOWER Management Center の時間と同期されている必要があります。アプライアンスが同期されていないと、予想外の間隔でユーザのタイムアウトが実行される可能性があります。
- 展開にプライマリとセカンダリの pxGrid ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。
- 展開にプライマリとセカンダリの MNT ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。

ISE/ISE-PIC によって報告されるユーザ データに関する問題が発生した場合は、次の点に注意してください。

- システムはデータがまだデータベースにない ISE ユーザのアクティビティを検出すると、サーバからそれらに関する情報を取得します。状況によっては、システムが Active Directory サーバからこの情報を正常に取得するために 60 分かかることもあります。データ取得が

成功するまで、ISEユーザから見えるアクティビティはアクセス コントロール ルールで処理され、Web インターフェイスに表示されません。

- LDAP、RADIUS、または RSA ドメイン コントローラで認証された ISE ユーザに対するユーザ制御は実行できません。
- ASA FirePOWER モジュールは、ISE ゲスト サービス ユーザのユーザ データは受信しません。
- 使用する ISE バージョンと設定は、FirePOWER システムでの ISE の使用方法に影響を与えます。詳細については、ISE/ISE-PIC アイデンティティ ソース （433 ページ）を参照してください。
- ISE-PIC は ISE 属性のデータを提供しません。

キャプティブ ポータル

キャプティブ ポータル認証に関する問題が発生した場合は、次の点に注意してください。

- キャプティブ ポータル サーバの時刻は、ASA FirePOWER モジュールの時刻と同期している必要があります。
- 設定済みの DNS 解決があり、Kerberos（または Kerberos をオプションとする場合は HTTP ネゴシエート）キャプティブ ポータルを実行するアイデンティティ ルールを作成する場合は、キャプティブ ポータル デバイスの完全修飾ドメイン名（FQDN）を解決するように DNS サーバを設定する必要があります。FQDN は、DNS 設定時に指定したホスト名と一致する必要があります。

ASA with FirePOWER Services デバイスの場合、FQDN は、キャプティブ ポータルに使用されるルーテッド インターフェイスの IP アドレスに解決される必要があります。

- Kerberos（または Kerberos をオプションとする場合は HTTP ネゴシエート）をアイデンティティ ルールの [認証タイプ（Authentication Type）] として選択する場合は、選択する [レルム（Realm）] には、Kerberos キャプティブ ポータル アクティブ認証を実行できるようにするため、[AD 参加ユーザ名（AD Join Username）] および [AD 参加パスワード（AD Join Password）] が設定されている必要があります。
- アイデンティティ ルールの [認証タイプ（Authentication Type）] として [HTTP 基本（HTTP Basic）] を選択した場合、ネットワーク上のユーザはセッションがタイムアウトしたことを認識しない場合があります。ほとんどの Web ブラウザは、HTTP 基本ログインからクレデンシャルをキャッシュし、古いセッションがタイムアウトした後にシームレスに新しいセッションを開始するためにそのクレデンシャルを使用します。
- キャプティブ ポータルに使用する予定のデバイスにインライン インターフェイスとルーテッドインターフェイスの両方が含まれる場合、キャプティブ ポータル デバイス上でルーテッドインターフェイスだけを対象とするようにキャプティブ ポータル アイデンティティ ルールでゾーン条件を設定する必要があります。

ユーザー エージェントのアイデンティティ ソース

ライセンス：任意

ユーザ エージェントはパッシブ認証方式で、ASA FirePOWER モジュールでサポートされる権限のあるアイデンティティ ソースの 1 つです。ASA FirePOWER モジュールと統合すると、エージェントは、ホストにログインまたはホストからログアウトするとき、あるいは Active Directory クレデンシャルで認証するときにユーザをモニタします。ユーザ エージェントは失敗したログイン試行を報告しません。ユーザエージェントから取得されたデータは、ユーザ認識とユーザ制御に使用できます。パッシブ認証はアイデンティティ ポリシーで呼び出します。

ユーザ エージェントをインストールして使用することで、ユーザ制御を実行できます。つまり、エージェントがユーザと IP アドレスを関連付け、これによりユーザの条件によるアクセス コントロール ルールをトリガーできるようになります。1 つのエージェントを使用して最大 5 つの Active Directory サーバ上のユーザ活動を監視できます。

ユーザ エージェントは段階的な設定が必要であり、以下が含まれます。

- エージェントがインストールされたコンピュータまたはサーバ。
- ASA FirePOWER モジュールおよびエージェントがインストールされたコンピュータまたは Active Directory サーバ間の接続。
- ASA FirePOWER モジュールおよびアイデンティティ レルム内のディレクトリとして設定されたモニタ対象 LDAP サーバ間の接続。

段階的なユーザ エージェントの設定とサーバ要件の詳細については、ユーザ エージェント コンフィギュレーション ガイドを参照してください。

ASA FirePOWER モジュール接続は、ログインとログオフがユーザ エージェントによって検出されたユーザのメタデータを取得可能にするだけでなく、アクセス コントロール ルール内で使用するユーザとグループを指定するためにも使用されます。エージェントが特定のユーザ名を除外するように設定されている場合、該当ユーザ名のログイン データは ASA FirePOWER モジュールに報告されません。ユーザ エージェント データは、デバイスのユーザ データベースとユーザ アクティビティ データベースに保存されます。

（注） ユーザ エージェントは $ 記号で終わる Active Directory ユーザ名を ASA FirePOWER モジュールに送信できません。これらのユーザをモニタする場合は、最後の $ の文字を削除する必要があります。

複数のユーザがリモート セッションを使用してホストにログインしている場合は、エージェントがそのホストからのログインを正確に検出しない場合があります。これを回避する方法については、ユーザ エージェント コンフィギュレーション ガイドを参照してください。

ユーザ エージェント接続の設定

ライセンス：Control

はじめる前に

ユーザ アクセス コントロールを実装する場合は、レルムの作成 （409 ページ）の説明に従って、ユーザ エージェント接続用の Active Directory レルムを設定して有効にします。

ユーザ エージェント接続の設定方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Integration]> [Identity Sources] の順に選択します。 > >

ステップ 2 [Service Type] に [User Agent] を選択し、ユーザ エージェント接続を有効にします。

（注） 接続を無効にするには、[None] を選択します。

ステップ 3 [Add New Agent] ボタンをクリックして、新しいエージェントを追加します。

ステップ 4 エージェントをインストールするコンピュータの [Hostname] または [Address] を入力します。IPv4 アドレスを使用する必要があります。IPv6 アドレスを使用してユーザ エージェントに接続するように ASA FirePOWER モジュールを設定することはできません。

ステップ 5 [Add] をクリックします。

ステップ 6 接続を削除するには、削除アイコンをクリックして、削除を確認します。

次のタスク

- *Firepower* ユーザエージェント コンフィギュレーション ガイドの説明に従い、ユーザ エージェントの設定を続行します。

ISE/ISE-PIC アイデンティティ ソース

ライセンス：任意

Cisco Identity Services Engine（ISE）または ISE Passive Identity Connector（ISE-PIC）の展開を ASA FirePOWER モジュールと統合して、ISE/ISE-PIC をパッシブ認証に使用できます。パッシブ認証はアイデンティティ ポリシーで呼び出します。

ISE/ISE-PIC は、信頼できるアイデンティティ ソースで、Active Directory（AD）、LDAP、RADIUS、または RSA によって認証するユーザに関するユーザ認識データを提供します。さらに、AD ユーザのユーザ制御を行えます。ISE/ISE-PIC は、ISE ゲスト サービス ユーザの失敗したログイン試行またはアクティビティは報告しません。

（注） システムではマシンの認証とユーザが関連付けられないため、ASA FirePOWER モジュールは、AD 認証と同時に 802.1x マシン認証をサポートすることはできません。802.1x アクティブ ログインを使用する場合は、802.1x アクティブ ログイン（マシンとユーザの両方）だけを報告するように ISE を設定します。このように設定すれば、マシン ログインはシステムに 1 回だけ報告されます。

Cisco ISE/ISE-PIC の詳細については、*Cisco Identity Services Engine* 管理者ガイドおよび *Identity Services Engine Passive Identity Connector*（*ISE-PIC*）のインストールおよび管理者ガイドを参照してください。

ご使用の ISE/ISE-PIC バージョンと設定は、次のように ASA FirePOWER モジュールとの統合や相互作用に影響を与えます。

- ISE/ISE-PIC サーバと ASA FirePOWER モジュールの時刻を同期させます。そうしないと、システムが予期しない間隔でユーザのタイムアウトを実行する可能性があります。
- 多数のユーザ グループをモニタするように ISE/ISE-PIC を設定した場合、システムはメモリ制限のためにグループに基づいてユーザ マッピングをドロップすることがあります。その結果、レルムまたはユーザ条件を使用するアクセス コントロール ルールが想定どおりに適用されない可能性があります。
- ISE のバージョン 2.0 パッチ 4 には、IPv6 対応エンドポイントのサポートが含まれています。
- ISE-PIC は ISE 属性のデータを提供しません。

このバージョンの ASA FirePOWER モジュールと互換性がある特定のバージョンの ISE/ISE-PIC については、*Cisco Firepower* 互換性ガイドを参照してください。

ISE 接続を設定すると、ISE 属性データが ASA FirePOWER モジュール データベースに入力されます。ユーザ認識とユーザ制御に使用できる ISE 属性は、次のとおりです。これは、ISE-PIC ではサポートされません。

セキュリティ グループ タグ（SGT）

セキュリティ グループ タグ（SGT）は、信頼ネットワーク内におけるトラフィックの送信元の権限を指定します。ユーザが TrustSec または ISE でセキュリティ グループを追加すると、セキュリティ グループ アクセス（Cisco TrustSec と Cisco ISE の両方に共通の機能）が自動的に SGT を生成します。SGA は、パケットがネットワークに入ると、SGT 属性を適用します。ISE をアイデンティティ ソースとして設定するかまたはカスタム SGT オブジェクトを作成することで、アクセス コントロール用に SGT を使用できます。詳細については、ISE SGT およびカスタム SGT ルール条件 （167 ページ）を参照してください。

SGT ISE 属性ルール条件は、ポリシー内で関連するアイデンティティ ポリシーの有無にかかわらず設定できます。

エンドポイント ロケーション（ロケーション IP とも呼ばれる）

[Endpoint Location] 属性は Cisco ISE によって適用され、エンドポイント デバイスの IP アドレスを特定します。

関連付けられたアイデンティティ ポリシーがあるポリシー内では、ロケーション IP を ISE 属性ルール条件としてのみ設定できます。

エンドポイント プロファイル（デバイス タイプとも呼ばれる）

[Endpoint Profile] 属性は Cisco ISE によって適用され、各パケットのエンドポイント デバイス タイプを特定します。

関連付けられたアイデンティティ ポリシーがあるポリシー内では、デバイス タイプを ISE 属性ルール条件としてのみ設定できます。

ISE/ISE-PIC フィールド

次のフィールドを使用して ISE/ISE-PIC への接続を設定します。

Primary and Secondary Host Name/IP Address

プライマリ（およびオプションでセカンダリ）ISE サーバのホスト名または IP アドレス。

pxGrid Server CA

pxGrid フレームワークの認証局。展開にプライマリとセカンダリの pxGrid ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。

MNT Server CA

一括ダウンロード実行時の ISE 証明書の認証局。展開にプライマリとセカンダリの MNT ノードがある場合、両方のノードの証明書が同じ認証局によって署名されている必要があります。

MC Server Certificate

ISE への接続時、または一括ダウンロードの実行時に ASA FirePOWER モジュールが ISE に提供する必要がある証明書およびキー。

MC サーバ証明書には、**clientAuth** 拡張キー使用値が含まれている必要があります。そうでない場合、拡張キー使用値は含まれていてはなりません。

ISE Network Filter

ISE がモニタするネットワークを制限するために設定できるオプション フィルタ。フィルタを指定する場合、ISE はそのフィルタ内のネットワークをモニタします。次の方法でフィルタを指定できます。

- すべて指定する場合はフィールドを空白のままにします。
- CIDR 表記を使用して単一の IPv4 アドレス ブロックを入力します。

- CIDR 表記を使用して IPv4 アドレス ブロックのリストをカンマで区切って入力します。

（注） このバージョンの Firepower システムは、ISE のバージョンに関係なく、IPv6 アドレスを使用したフィルタリングをサポートしません。

ISE/ISE-PIC 接続の設定

ライセンス：Control

はじめる前に

- レルムの作成（409 ページ）の説明に従って、レルムを設定します。アクセス コントロール ルールで ISE 属性条件を設定するには、その前にユーザによるダウンロード（自動またはオンデマンド）が実行される必要があります。

（注） SGT ISE 属性条件の設定を計画しているものの、ユーザ、グループ、レルム、エンドポイント ロケーション、またはエンドポイント プロファイルの条件の設定は計画していない場合、レルムの設定はオプションです。

ISE/ISE-PIC 接続を設定するには

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Integration]> [Identity Sources] の順に選択します。 > > >

ステップ 2 [サービス タイプ（Service Type）] に [Identity Services Engine] を選択し、ISE/ISE-PIC 接続を有効にします。

（注） 接続を無効にするには、[None] を選択します。

ステップ 3 [Primary Host Name/IP Address] と、オプションで [Secondary Host Name/IP Address] を入力します。

ステップ 4 [pxGrid Server CA]、[MNT Server CA]、および [MC Server Certificate] ドロップダウンリストから適切な証明書を選択します。必要に応じて、追加アイコンをクリックして、オブジェクトをその場で作成します。

ステップ 5 オプションで、CIDR ブロック表記を使用して **ISE ネットワーク フィルタ** を入力します。

ステップ 6 接続をテストする場合は、[Test] をクリックします。

キャプティブ ポータル アクティブ認証のアイデンティティ ソース

ライセンス：任意

キャプティブ ポータルは、ASA FirePOWER モジュールでサポートされる権限のあるアイデンティティ ソースの 1 つです。これは ASA FirePOWER モジュールでサポートされる唯一のアクティブな認証方式であり、ユーザはデバイスを介してネットワークに対する認証を行うことができます。

キャプティブ ポータル経由のアクティブ認証は、HTTP および HTTPS トラフィックのみで実行されます。HTTPS トラフィックでキャプティブ ポータルを実行する場合は、キャプティブ ポータルを使用して認証するユーザから送信されたトラフィックを復号するための、SSL ルールを作成する必要があります。

設定して展開すると、指定レルムのユーザはバージョン 9.5(2) 以降を実行しているルーテッド モードの ASA FirePOWER デバイス経由で認証されます。キャプティブ ポータルから取得された認証データは、ユーザ認識とユーザ制御に使用できます。

キャプティブ ポータルはまた、失敗した認証の試行を記録します。失敗した試行によって新しいユーザーがデータベース内のユーザーのリストに追加されることはありません。キャプティブ ポータルで報告される失敗した認証アクティビティのユーザー アクティビティ タイプは、[Failed Auth User] です。

ASA ファイアウォール コンフィギュレーション ガイドの説明に従い、captive-portal ASA CLI コマンドを使用してアクティブ認証のキャプティブ ポータルを有効にします。

アイデンティティ ポリシーのキャプティブ ポータルの設定を続け、アイデンティティ ルールのアクティブ認証を呼び出します。アイデンティティ ポリシーは、アクセス コントロール ポリシーで呼び出されます。詳細については、キャプティブポータル（アクティブ認証）の設定（415 ページ）を参照してください。

キャプティブ ポータルは、設定された 1 つ以上のルーテッド インターフェイスがあるデバイスによってのみ実行できます。

アクセス コントロール ルールおよび SSL ルールの次の要件に注意してください。

- HTTPS トラフィックでキャプティブ ポータルを使用してアクティブ認証を実行する場合は、キャプティブ ポータルを使用して認証するユーザから送信されたトラフィックを復号する SSL ルールを作成する必要があります。
- キャプティブ ポータル接続でトラフィックを復号する場合、キャプティブ ポータルに使用するポート宛てのトラフィックを復号する SSL ルールを作成する必要があります。
- キャプティブ ポータルに使用する IP アドレスおよびポート宛てのトラフィックを許可するようにアクセス コントロール ルールを設定する必要があります。宛先ポートがアクセス コントロール ポリシーで許可されない場合、トラフィックはキャプティブ ポータルを使用して認証できません。

ASA FirePOWER モジュール サーバのダウンロード

ライセンス：任意

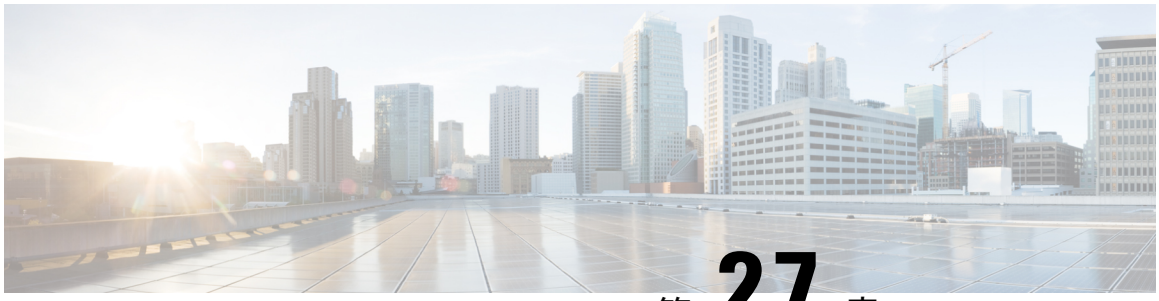
ASA FirePOWER モジュールと LDAP または AD サーバ間の接続により、特定の検出されたユーザの、ユーザおよびユーザ グループのメタデータを取得できます。

- キャプティブ ポータルで認証されたか、あるいはユーザ エージェントまたは ISE/ISE-PIC で報告された LDAP および AD のユーザ。このメタデータは、ユーザ認識とユーザ制御に使用できます。
- トラフィック ベースの検出により検出された POP3 と IMAP ユーザ ログイン（ユーザが LDAP または AD ユーザと同じ電子メール アドレスを持つ場合）。このメタデータは、ユーザ認識に使用できます。

ASA FirePOWER モジュール ユーザ データベース サーバ接続は、レルム内のディレクトリとして設定します。ユーザ認識とユーザ制御のためにレルムのユーザおよびユーザ グループ データをダウンロードするには、[Download users and user groups for access control] チェックボックスをオンにする必要があります。

ASA FirePOWER モジュールは、ユーザごとに次の情報とメタデータを取得します。

- LDAP ユーザ名
- 姓と名
- 電子メール アドレス
- 部門
- 電話番号



第 27 章

DNS ポリシー

ライセンス：任意

DNS ベースのセキュリティ インテリジェンスにより、クライアントが要求したドメイン名に基づいてトラフィックをブロックしたり、ブロック対象から除外したりできます。シスコが提供するドメイン名のインテリジェンスを使用して、トラフィックをフィルタリングできます。また、環境に合わせて、ドメイン名のカスタム リストやフィードを設定することも可能です。DNS ベースのセキュリティ インテリジェンスによるフィルタリングが実行されるタイミングは、ハードウェア レベルの処理およびトラフィックの復号が行われた後で、かつ、他のほとんどのポリシー ベースのインスペクション、分析、トラフィック処理が行われる前です。

DNS ポリシーによってブロックされたトラフィックは直ちにブロックされるため、他の詳細なインスペクション（侵入、エクスプロイト、マルウェアの有無など）の対象にはなりません。ブロックなしリストに追加することでブロックをオーバーライドしてアクセス制御ルールの評価を適用することができます。また、「モニタのみ」の設定をセキュリティ インテリジェンス フィルタリングに使用できます。パッシブ展開環境では、この設定が推奨されます。この設定では、ブロックされた可能性がある接続を ASA FirePOWER モジュールが分析できるだけでなく、ブロックリストに一致する接続がログに記録され、接続終了セキュリティ インテリジェンス イベントが生成されます。

DNS ポリシーと、関連する DNS ルールを使用して、DNS ベースのセキュリティ インテリジェンスを設定します。展開するには、DNS ポリシーとアクセス コントロール ポリシーとを関連付け、次に設定を展開する必要があります。

- DNS ポリシーの構成要素 （439 ページ）
- DNS ルール （441 ページ）
- DNS ポリシーの導入 （448 ページ）

DNS ポリシーの構成要素

ライセンス：任意

DNS ポリシーを使用すると、ドメイン名ベースの接続をブロック（またはブロックから除外）できます。以下のリストでは、DNS ポリシーの作成後に変更できる設定を説明しています。

名前と説明

各 DNS ポリシーには一意の名前が必要です。説明は任意です。

ルール

ルールは、ドメイン名に基づいてネットワーク トラフィックを処理するための詳細な方法を提供します。DNS ポリシーのルールには 1 から始まる番号が付いています。ASA FirePOWER モジュールは、ルール番号の昇順で、DNS ルールを上から順にトラフィックと照合します。

DNS ポリシーを作成すると、ASA FirePOWER モジュールはそのポリシーをデフォルトのグローバル DNS ブロックなしリストのルールとデフォルトのグローバル DNS ブロックリストのルールに入力します。各ルールは、それぞれのカテゴリで先頭の位置に固定されます。ルールは変更できませんが、無効にすることはできます。モジュールはルールを、以下の順序で評価します。

- グローバル DNS ブロックなしリストのルール（有効になっている場合）
- ブロックなしのルール
- Global DNS ブロックのルール（有効になっている場合）
- ブロックとモニタのルール

通常、モジュールはドメイン名ベースのネットワーク トラフィックを、すべてのルールの条件がトラフィックと一致する最初の DNS ルールに従って処理します。トラフィックと一致する DNS ルールがない場合、モジュールは、関連するアクセス コントロール ポリシーのルールに基づいてトラフィックの評価を続行します。DNS ルールの条件は、単純なものにも複雑なものにもできます。

DNS ポリシーの編集

ライセンス：Protection

DNS ポリシーを同時に編集できるのは 1 ユーザのみであり、使用できるのは単一のブラウザ ウィンドウのみです。複数のユーザが同じポリシーを保存しようとすると、最初に保存された変更のセットのみが保持されます。

セッションのプライバシーを保護するために、ポリシー エディタで活動が行われずに 30 分が経過すると、警告が表示されます。60 分経過すると、モジュールは変更内容を破棄します。

DNS ポリシーを編集する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [DNS Policy] の順に選択します。

ステップ 2 DNS ポリシーを次のように編集します。

- 名前と説明：名前または説明を変更するには、フィールドをクリックして新しい情報を入力します。
- ルール：DNS ルールを追加、分類、有効化、無効化、または管理する場合は、[Rules] タブをクリックして、DNS ルールの作成と編集 （442 ページ）の説明に従って続行します。

ステップ 3 [Store ASA FirePOWER Changes] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の導入 （92 ページ）を参照してください。

DNS ルール

ライセンス：任意

DNS ルールは、ホストにより要求されるドメイン名に基づいてトラフィックを処理します。セキュリティ インテリジェンスの一部として、この評価はすべてのトラフィック復号の後、およびアクセス コントロールの評価の前に実行されます。

ASA FirePOWER モジュールは、ユーザが指定した順序で DNS ルールをトラフィックと照合します。ほとんどの場合、モジュールによるネットワーク トラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の DNS ルールに従って行われます。DNS ルールの作成時に、モジュールはブロックなしのルールをモニタのルールやブロックのルールよりも前に配置し、最初にブロックなしのルールと照合してトラフィックを評価します。

.

各 DNS ルールには、一意の名前以外にも、次の基本コンポーネントがあります。

状態

デフォルトでは、ルールが有効状態になります。ルールを無効にすると、ASA FirePOWER モジュールはネットワーク トラフィックの評価にそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。

位置

DNS ポリシーのルールには 1 から始まる番号が付いています。ASA FirePOWER モジュールは、ルール番号の昇順で、ルールを上から順にトラフィックと照合します。Monitor ルールを除き、トラフィックが最初に一致するルールが、当該トラフィックを処理するためのルールになります。

条件

条件は、ルールで処理する特定のトラフィックを指定します。DNS ルールは、DNS フィードまたはリスト条件が含まれていなければならず、セキュリティ ゾーンまたはネットワークを基準にしてトラフィックと突き合わせることもできます。

アクション

ルールのアクションによって、ASA FirePOWER モジュールによる一致するトラフィックの処理方法が決まります。

- ブロックなしリストにあるトラフィックが許可され、さらにアクセス制御インスペクションを受けます。
- モニタされるトラフィックは、残りのDNSブロックのルールによりさらに評価されます。トラフィックが DNS ブロックのルールに一致しない場合、アクセス制御ルールによりインスペクションを受けます。モジュールは、トラフィックのセキュリティインテリジェンス イベントをログに記録します。
- ブロックされたトラフィックは、それ以上のインスペクションは行われずにドロップされます。[Domain Not Found] 応答を返したり、DNS クエリをシンクホール サーバにリダイレクトしたりすることもできます。

DNS ルールの作成と編集

ライセンス：Protection

DNS ポリシーで、合計で最大 32,767 の DNS リストをブロックなしリストとブロックリストのルールに追加できます。つまり、DNS ポリシーのリスト数は、32767 より多くすることはできません。

DNS ルールを作成または編集する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [DNS Policy] の順に選択します。

ステップ 2 次の選択肢があります。

- 新しいルールを追加するには、[Add DNS Rule] をクリックします。
- 既存のルールを編集するには、編集アイコンをクリックします。

ステップ 3 [Name] を入力します。

ステップ 4 ルール コンポーネントを設定するか、またはデフォルトを受け入れます。

- [Action]：ルールのアクションを選択します。DNS ルールのアクション （444 ページ）を参照してください。
- [Conditions]：ルールの条件を設定します。DNS ルールの条件 （445 ページ）を参照してください。
- [Enabled]：ルールを有効にするかどうかを指定します。

ステップ 5 [追加（Add）] または [OK] をクリックします。

ステップ 6 [Store ASA FirePOWER Changes] をクリックします。

DNS ルールの管理

ライセンス：任意

DNS ポリシー エディタの [Rules] タブでは、ポリシー内の DNS ルールの追加、編集、移動、有効化、無効化、削除、その他の管理が行えます。

各ルールについて、ポリシー エディタでは、その名前、条件のサマリー、およびルール アクションが表示されます。他のアイコンには、警告、エラー、その他の重要な情報が表示されます。無効なルールは淡色表示され、ルール名の下に [（disabled）] というマークが付きます。

DNS ルールの有効化と無効化

ライセンス：Protection

作成した DNS ルールは、デフォルトでイネーブルになっています。ルールを無効にすると、ASA FirePOWER モジュールはネットワーク トラフィックの評価にそのルールを使用せず、そのルールに対する警告とエラーの生成を停止します。DNS ポリシーのルール リストを表示すると、無効なルールは淡色表示されますが、変更は可能です。DNS ルール エディタを使用して DNS ルールをイネーブルまたはディセーブルにできることにも注意してください。

DNS ルールのイネーブル化とディセーブル化の方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [DNS Policy] の順に選択します。

ステップ 2 有効化または無効化するルールを含む DNS ポリシー エディタで、ルールを右クリックして、ルールの状態を選択します。

ステップ 3 [OK] をクリックします。

ステップ 4 [Store ASA FirePOWER Changes] をクリックします。

次のタスク

- 設定変更を展開します。設定変更の導入 （92 ページ）を参照してください。

DNS ルールの評価順序

ライセンス：任意

DNS ポリシーのルールには 1 から始まる番号が付いています。ASA FirePOWER モジュールは、ルール番号の昇順で、DNS ルールを上から順にトラフィックと照合します。ほとんどの場合、モジュールによるネットワーク トラフィックの処理は、すべてのルールの条件がトラフィックに一致する最初の DNS ルールに従って行われます。

- モニタ ルールの場合、モジュールはトラフィックをログに記録し、優先度が低い DNS ブロックリストのルールと照合してトラフィックの評価を続行します。
- 非モニタ ルールの場合、トラフィックがルールに一致したら、モジュールは追加の優先度が低い DNS ルールに突き合わせた評価を続行しません。

ルールの順序に関して、次の点に注意してください。

- グローバルブロックなしリストは常に最初に使用され、他のすべてのルールに優先します。
- [Do-Not-Block] セクションは [Block] セクションに優先します。ブロックなしのルールは常に他のルールに優先します。
- グローバルブロックリストは[Blocklist] セクション内で常に最初に使用され、他のすべてのモニタのルールやブロックリストのルールに優先します。
- [Blocklist] セクションには、モニタのルールとブロックリストのルールが含まれます。
- DNS ルールの最初の作成時に、モジュールはそれを、**[Do-Not-Block]** のアクションを割り当てる場合には [Do-Not-Block] セクションの末尾に配置し、その他のアクションを割り当てる場合は [Block] セクションの末尾に配置します。

それらを並べ替えて評価順序を変更するルールをドラッグ アンド ドロップできます。

DNS ルールのアクション

ライセンス：任意

すべての DNS ルールには、一致するトラフィックについて次のことを決定するアクションがあります。

- 処理：第一に、ルールアクションはルールの条件に一致するトラフィックをモジュールがモニタするか、またはブロックするか、あるいは処理の次段階に渡すことを許可するかを制御します。
- ロギング：ルールアクションによって、一致するトラフィックの詳細をいつ、どのようにログに記録できるかが決まります。

インライン展開されたデバイスのみがトラフィックをブロックできることに留意してください。パッシブに展開されたデバイスは、トラフィックの受け渡しやロギングはできますが、影響を与えることはありません。

ブロックなしのアクション

[Do-Not-Block] のアクションにより、一致するトラフィックの通過が許可されます。このオプションを選択した場合は、一致するアクセス制御ルール、またはアクセス コントロール ポリシーのデフォルトアクションのいずれかによって、トラフィックはさらにインスペクションを受けます。

モジュールはブロックなしの一致をログに記録しません。これらの接続のロギングは、その接続の最終的な傾向によって異なります。

モニタ アクション

[Monitor] のアクションはトラフィックフローに影響を与えません。つまり、一致するトラフィックが直ちに受け渡されるか、またはブロックされることはありません。その代わり、追加のルールに照らしてトラフィックが照合され、許可/拒否が決定されます。一致する最初の非モ

ニタ DNS ルールにより、モジュールがトラフィックをブロックするかどうかが決まります。追加の一致ルールがない場合、トラフィックはアクセス コントロール評価に従います。

DNS ポリシーによってモニタされる接続の場合、ASA FirePOWER モジュールは、接続終了セキュリティ インテリジェンス イベントと接続イベントをログに記録します。

ブロックのアクション

これらのアクションは、どんな種類のインスペクションもなく、トラフィックをブロックします。

- [Drop] アクションはトラフィックをドロップします。
- [Domain Not Found] アクションは、存在しないインターネット ドメイン応答を DNS クエリに返します。これによりクライアントは DNS 要求を解決できなくなります。
- [Sinkhole] アクションは、シンクホール オブジェクトの IPv4 または IPv6 アドレスを DNS クエリに応答して返します。シンクホール サーバは、IP アドレスへの後続の接続をログに記録するか、ログに記録してブロックすることができます。[Sinkhole] アクションを設定する場合、シンクホール オブジェクトも設定する必要があります。

[Drop] または **[Domain Not Found]** のアクションに基づいてブロックされた接続の場合は、モジュールが接続開始のセキュリティ インテリジェンス イベントと接続イベントをログに記録します。ブロックされたトラフィックは追加のインスペクションなしですぐに拒否されるため、ログに記録できる固有の接続終了イベントはありません。

[Sinkhole] のアクションに基づいてブロックされる接続の場合、ロギングはシンクホールオブジェクトの設定に応じて決まります。シンクホール オブジェクトを、シンクホール接続のログ記録のみを実行するように設定した場合、モジュールは後続の接続の「接続の終わり」接続イベントをログに記録します。シンクホール オブジェクトを、シンクホール接続のログ記録およびブロックを実行するように設定した場合、モジュールは後続の接続の「接続の開始」接続イベントをログに記録し、それから接続をブロックします。

DNS ルールの条件

ライセンス：任意

DNS ルールの条件は、ルールで処理するトラフィックのタイプを特定します。条件は単純なものにも複雑なものにもできます。DNS フィードまたはリスト条件を定義する必要があります。セキュリティ ゾーンまたはネットワークでトラフィックをさらに制御できます。

条件を DNS ルールに追加するには、以下の手順に従います。

- ルールに対し特定の条件を設定しない場合、モジュールはその基準に基づいてトラフィックを照合しません。
- 1 つのルールにつき複数の条件を設定できます。ルールがトラフィックに適用されるには、トラフィックがそのルールの**すべての**条件に一致する必要があります。

- ルールの条件ごとに、最大 50 の基準を追加できます。条件の基準の**いずれかに**一致するトラフィックはその条件を満たします。たとえば、最大で 50 DNS のリストとフィードに基づいてトラフィックをブロックする単一のルールを使用できます。

DNS およびセキュリティ ゾーンに基づくトラフィックの制御

ライセンス：Protection

DNS ルールでゾーン条件を設定すると、トラフィックの送信元および宛先のセキュリティ ゾーンに応じてそのトラフィックを制御できます。セキュリティ ゾーンは、1 つ以上のインターフェイスのグループです。検出モードと呼ばれる、デバイスの初期セットアップ時に選択するオプションによって、モジュールが最初にデバイスのインターフェイスをどのように設定するか、およびこれらのインターフェイスがセキュリティ ゾーンに属するかどうかが決定します。

DNS とセキュリティ ゾーンに基づいてトラフィックを制御する方法：

ステップ 1 DNS ルール エディタで、[Zones] タブをクリックします。

ステップ 2 [Available Zones] から追加するゾーンを見つけて選択します。追加するゾーンを検索するには、[Available Zones] リストの上にある [Search by name] プロンプトをクリックし、ゾーン名を入力します。入力すると、リストが更新されて一致するゾーンが表示されます。

ステップ 3 セキュリティ ゾーンをクリックするか、または右クリックして、[Select All] を選択します。

ステップ 4 [Add to Source] をクリックします。

ヒント 選択したゾーンをドラッグ アンド ドロップすることもできます。

ステップ 5 ルールを保存するか、編集を続けます。

次のタスク

- 設定変更を展開します。設定変更の導入 （92 ページ）を参照してください。

DNS およびネットワークに基づくトラフィックの制御

ライセンス：Protection

DNS ルール内のネットワーク条件によって、その送信元 IP アドレス別にトラフィックを制御することができます。制御するトラフィックの送信元 IP アドレスを明示的に指定できます。

DNS とネットワークに基づいてトラフィックを制御する方法：

ステップ 1 DNS ルール エディタで、[Networks] タブをクリックします。

ステップ 2 [Available Networks] から、次のように追加するネットワークを見つけて選択します。

- ネットワーク オブジェクト（後で条件に追加可能）をその場で追加するには、[Available Networks] リストの上にある追加アイコンをクリックし、ネットワーク オブジェクトの操作 （26 ページ）の説明に従って続行します。
- 追加するネットワーク オブジェクトを検索するには、[Available Networks] リストの上にある [Search by name or value] プロンプトをクリックし、オブジェクトのコンポーネントの 1 つのオブジェクト名または値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

ステップ 3 [Add to Source] をクリックします。

ヒント 選択したオブジェクトをドラッグ アンド ドロップすることもできます。

ステップ 4 手動で指定する送信元 IP アドレスまたはアドレス ブロックを追加します。[Source Networks] リストの下にある [Enter an IP address] プロンプトをクリックし、1 つの IP アドレスまたはアドレス ブロックを入力して [Add] をクリックします。

ステップ 5 ルールを保存するか、編集を続けます。

次のタスク

- 設定変更を展開します。設定変更の導入 （92 ページ）を参照してください。

DNS リスト、フィード、またはカテゴリに基づくトラフィックの制御

ライセンス：Protection

DNS リスト、フィード、またはカテゴリにクライアントにより要求されたドメイン名が含まれる場合、DNS ルール内の DNS 条件によりトラフィックを制御できます。DNS ルール内で DNS 条件を定義する必要があります。

グローバルまたはカスタムのブロックなしリストまたはブラックリストを DNS 条件に追加するかどうかに関係なく、ASA FirePOWER モジュールは設定済みのルールアクションをトラフィックに適用します。たとえば、グローバルブロックなしリストをルールに追加し、[Drop] アクションを設定した場合、モジュールは追加のアセスメント用に渡されるはずだったすべてのトラフィックをブロックします。

DNS リスト、フィード、またはカテゴリに基づいてトラフィックを制御する方法：

ステップ 1 DNS ルール エディタで、[DNS] タブをクリックします。

ステップ 2 追加する DNS リストとフィードを、以下のように [DNS Lists and Feeds] から見つけて選択します。

- DNS リストまたはフィード（後で条件に追加可能）をその場で追加するには、[DNS Lists and Feeds] リストの上にある追加アイコンをクリックし、インテリジェンス フィードの操作 （30 ページ）の説明に従って続行します。
- 追加する DNS リスト、フィード、またはカテゴリを検索するには、[DNS Lists and Feeds] リストの上にある [Search by name or value] プロンプトをクリックし、オブジェクトのコンポーネントの 1 つのオ

ブジェクト名または値を入力します。入力すると、リストが更新されて一致するオブジェクトが表示されます。

ステップ 3 [Add to Rule] をクリックします。

ヒント 選択したオブジェクトをドラッグ アンド ドロップすることもできます。

ステップ 4 ルールを保存するか、編集を続けます。

次のタスク

- 設定変更を展開します。設定変更の導入 （92 ページ）を参照してください。

DNS ポリシーの導入

ライセンス：任意

DNS ポリシー設定の更新が終了したら、変更を有効にするために、それをアクセス コントロール ポリシーの一部として展開する必要があります。次の手順を実行する必要があります。

- セキュリティ インテリジェンスのブロックリストとブロックしないリストの作成 （106 ページ）の説明に従って、DNS ポリシーとアクセス コントロール ポリシーを関連付けます。
- 設定変更を展開します。設定変更の導入 （92 ページ）を参照してください。

第 28 章

マルウェアおよび禁止されたファイルのブロッキング

悪意のあるソフトウェア、つまりマルウェアは、複数のルートで組織のネットワークに入る可能性があります。マルウェアの影響を特定して軽減するために、ASA FirePOWER モジュールのファイル制御、および高度なマルウェア防御の各コンポーネントを使用すると、ネットワーク トラフィックで伝送されるマルウェアやその他の種類のファイルを検出、追跡、保存、分析し、必要に応じてブロックできます。

全体的なアクセス制御設定の一部として、マルウェア対策とファイル制御を実行するようにシステムを設定できます。作成してアクセス コントロール ルールに関連付けたファイル ポリシーは、ルールに一致するネットワーク トラフィックを処理します。

ファイル ポリシーはどのライセンスでも作成可能ですが、マルウェア防御とファイル制御の一部の操作を行うには、次の表に示すように、ライセンス供与される特定の機能を ASA FirePOWER モジュールで有効にする必要があります。

表 *65* : 侵入インスペクションおよびファイル インスペクションのライセンスおよびアプライアンスの要件

機能	説明	追加する必要のあるライセンス
侵入防御	侵入およびエクスプロイトを検出し、任意でブロックします	Protection
ファイル制御	ファイル タイプの伝送を検出し、任意でブロックします	Protection
高度なマルウェア防御（AMP）	マルウェアの伝送を検出、追跡し、任意でブロックします	Malware

- マルウェア防御とファイル制御について （450 ページ）
- ファイル ポリシーの概要と作成 （453 ページ）

マルウェア防御とファイル制御について

ライセンス：Protection、Malware、または任意

高度なマルウェア防御機能を使用すると、ネットワークで伝送されるマルウェア ファイルを検出、追跡、分析し、必要に応じてブロックするように ASA FirePOWER モジュールを設定できます。

システムは、PDF、Microsoft Office 文書など多数のファイル タイプに潜むマルウェアを検出し、オプションでブロックできます。ASA FirePOWER モジュールは、特定のアプリケーション プロトコル ベースのネットワーク トラフィックで、これらのファイル タイプの伝送をモニタします。ASA FirePOWER モジュールは該当するファイルを検出し、ファイルの SHA256 ハッシュ値を使用してマルウェア クラウド ルックアップを実行します。その結果に基づき、Cisco Cloud は ASA FirePOWER モジュールにファイルの性質を返します。

クラウドにあるファイルの性質が不正確だとわかっている場合、次のようにして、ファイルの SHA-256 値をファイル リストに追加できます。

- クラウドがクリーンの性質を割り当てた場合と同じ方法でファイルを扱うには、クリーン リストにファイルを追加します。
- クラウドがマルウェアの性質を割り当てた場合と同じ方法でファイルを扱うには、カスタム検出リストにファイルを追加します。

あるファイルの SHA-256 値がファイル リスト内で検出されると、システムはマルウェア ルックアップの実行もファイルの性質の検査も行わずに、適切なアクションを実行します。ファイルの SHA 値を計算するには、**マルウェア クラウド ルックアップ** アクションと**マルウェア ブロック** アクションのどちらか、および一致するファイルタイプを使用して、ファイルポリシー内のルールを設定する必要があることに注意してください。ファイルポリシーごとに、クリーン リストまたはカスタム検出リストの使用を有効にできます。

ファイルを検査またはブロックするには、ASA FirePOWER モジュールで Protection ライセンスを有効にする必要があります。ファイルをファイル リストに追加するには、Malware ライセンスも有効にする必要があります。

ファイルの性質について

システムは、Cisco Cloud から返される性質に基づいてファイルの性質を決定します。ファイル リストへの追加操作の結果、または脅威スコアに応じて、Cisco Cloud クラウドから返されるファイルの性質は次のいずれかになります。

- Malware：クラウドがマルウェアとしてファイルを分類したことを示します。
- Clean は、クラウドでそのファイルがクリーンとして分類されているか、ユーザがファイルをクリーン リストに追加したことを示します。
- Unknown は、クラウドが性質を割り当てる前にマルウェア クラウド ルックアップが行われたことを示します。クラウドはそのファイルをまだ分類していません。

- [Custom Detection] は、ファイルをユーザがカスタム検出リストに追加したことを示します。
- Unavailable：ASA FirePOWER モジュールがマルウェア クラウド ルックアップを実行できなかったことを示します。この性質で見られるイベントはごくわずかである可能性があります。これは予期された動作です。

ヒント 高速連続で複数のUnavailableマルウェア イベントが発生した場合は、クラウド接続およびポート設定を確認してください。詳細については、「セキュリティ、インターネット アクセス、および通信ポート （629 ページ）」を参照してください。

ファイルの性質に基づいて、ASA FirePOWER モジュールはファイルをブロックするか、またはファイルのアップロードやダウンロードをブロックします。パフォーマンス向上のために、SHA256 値に基づくファイルの性質がすでにわかっている場合、アプライアンスは Cisco Cloud にクエリする代わりに、キャッシュ済みの性質を使用します。

ファイルの性質は変更される可能性があることに注意してください。たとえば、クラウドによる判定の結果、以前はクリーンであると考えられていたファイルが今はマルウェアとして識別されるようになったり、その逆、つまりマルウェアと識別されたファイルが実際にはクリーンであったりする可能性があります。あるファイルに関するマルウェア ルックアップを前の週に実行した後、そのファイルの性質が変更された場合、クラウドから ASA FirePOWER モジュールに通知が送信されるため、そのファイルの伝送が次回検出されたときにシステムは適切なアクションを実行できます。変更されたファイルの性質は、レトロスペクティブな性質と呼ばれます。

マルウェア クラウド ルックアップから戻されたファイルの性質には、存続可能時間（TTL）値が割り当てられます。ファイルの性質が更新されないまま、TTL 値で指定された期間にわたって保持された後は、キャッシュ情報が消去されます。性質には、次の TTL 値があります。

- [Clean]：4 時間
- [Unknown]：1 時間
- [Malware]：1 時間

キャッシュに照らしたマルウェア クラウド ルックアップの結果、キャッシュ済み性質がタイムアウトになったことが識別されると、システムはファイルの性質を判別するために新しいルックアップを実行します。

ファイル制御について

マルウェア ファイル伝送のブロックに加えて、（マルウェアを含むかどうかにかかわらず）特定のタイプのすべてのファイルをブロックする必要がある場合は、ファイル制御機能により防御網を広げることができます。マルウェア防御の場合と同様に、ASA FirePOWER モジュールはネットワーク トラフィック内で特定のファイル タイプの伝送をモニタし、そのファイルをブロックまたは許可します。

システムでマルウェアを検出できるすべてのファイル タイプだけでなく、さらに多数のファイル タイプに対するファイル制御がサポートされています。これらのファイル タイプは、マルチメディア（swf、mp3）、実行可能ファイル（exe、トレント）、PDF などの基本的なカテゴリにグループ分けされます。ファイル制御はマルウェア防御とは異なり、Cisco Cloud へのクエリを必要としないことに注意してください。

マルウェア防御とファイル制御の設定

ライセンス：Protection または Malware

ファイル ポリシーをアクセス コントロール ルールに関連付けることで、全体的なアクセス制御設定の一部として、マルウェア対策とファイル制御を設定します。この関連付けにより、アクセス コントロール ルールの条件と一致するトラフィック内のファイルを通過させる前に、システムは必ずファイルを検査するようになります。

ファイル ポリシーには、親アクセス コントロール ポリシーと同様に、各ルールの条件に一致するファイルの処理方法を決定するルールがいくつか含まれています。ファイル タイプ、アプリケーション プロトコル、転送方向の違いに応じて異なるアクションを実行する別個のファイル ルールを設定できます。

あるファイルがルールに一致する場合、ルールで以下を実行できます。

- 単純なファイル タイプ照合に基づいてファイルを許可またはブロックする
- マルウェア ファイルの性質に基づいてファイルをブロックする

さらに、ファイル ポリシーは、クリーン リストまたはカスタム検出リストのエントリに基づいて、ファイルがクリーンまたはマルウェアである場合と同じように自動的にファイルを扱うことができます。

単純な例として、ユーザによる実行可能ファイルのダウンロードをブロックするファイル ポリシーを導入できます。ファイル ポリシーについて、およびファイル ポリシーとアクセス コントロール ルールとの関連付けについての詳細は、ファイル ポリシーの概要と作成 （453 ページ） を参照してください。

マルウェア防御とファイル制御に基づくイベントのロギング

ライセンス：Protection または Malware

ASA FirePOWER モジュールは、システムによるファイル インスペクションの記録、ファイル イベントおよびマルウェア イベント処理の記録をログに記録します。

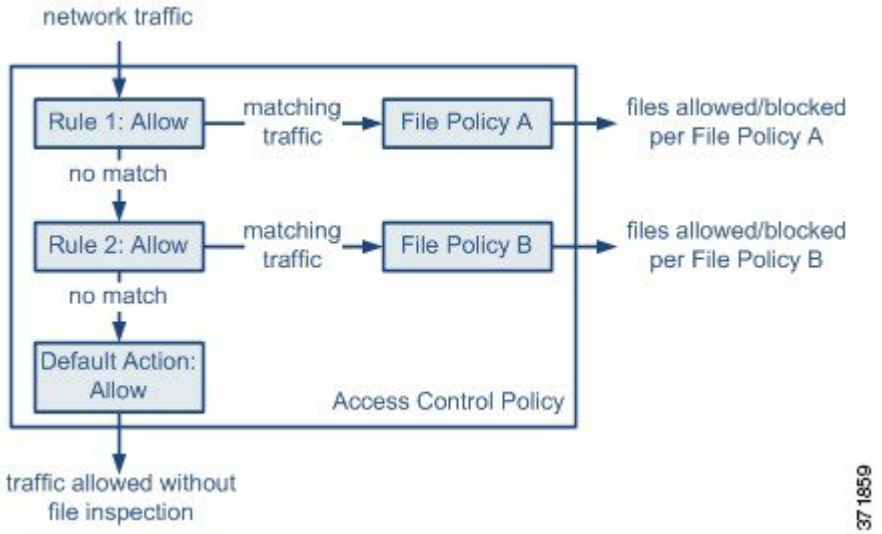
- ファイル イベントは、システムがネットワーク トラフィック内で検出した（さらにオプションでブロックした）ファイルを表します。
- マルウェア イベントは、システムがネットワーク トラフィック内で検出した（さらにオプションでブロックした）マルウェア ファイルを表します。
- 遡及的マルウェア イベントは、マルウェア ファイルの性質が変更されたファイルを表します。

システムがネットワーク トラフィックでのマルウェアの検出またはブロックに基づいてマルウェア イベントを生成する場合、ファイル イベントも生成します。ファイル内のマルウェアを検出するために、システムはまずファイル自体を検出する必要があるからです。

ファイル ポリシーの概要と作成

ライセンス：Protection または Malware

ファイルポリシーは、システムが全体的なアクセス制御設定の一環として、高度なマルウェア防御とファイル制御を実行するために使用する一連の設定です。



このポリシーには 2 つのアクセス コントロール ルールがあり、両方とも許可アクションを使用し、ファイル ポリシーに関連付けられています。このポリシーのデフォルト アクションもまた「トラフィックの許可」ですが、ファイル ポリシー インスペクションはありません。このシナリオでは、トラフィックは次のように処理されます。

- Rule 1 に一致するトラフィックは File Policy A で検査されます。
- Rule 1 に一致しないトラフィックは Rule 2 に照らして評価されます。Rule 2 に一致するトラフィックはFile Policy B で検査されます。
- どちらのルールにも一致しないトラフィックは許可されます。デフォルト アクションにファイル ポリシーを関連付けることはできません。

ファイル ポリシーには、親アクセス コントロール ポリシーと同様に、各ルールの条件に一致するファイルの処理方法を決定するルールがいくつか含まれています。ファイルタイプ、アプリケーションプロトコル、転送方向の違いに応じて異なるアクションを実行する別個のファイル ルールを設定できます。

ファイルがルールに一致する場合、ルールで以下を実行できます。

- 単純なファイル タイプ照合に基づいてファイルを許可またはブロックする

- マルウェア ファイルの性質に基づいてファイルをブロックする

さらに、ファイル ポリシーは、クリーン リストまたはカスタム検出リストのエントリに基づいて、ファイルがクリーンまたはマルウェアである場合と同じように自動的にファイルを扱うことができます。

1 つのファイル ポリシーを、**許可**、**インタラクティブ ブロック**、または **リセット付きインタラクティブ ブロック** アクションを含むアクセス コントロール ルールに関連付けることができます。その後、システムはそのファイル ポリシーを使用して、アクセス コントロール ルールの条件を満たすネットワーク トラフィックを検査します。異なるファイル ポリシーを個々のアクセス コントロール ルールに関連付けることにより、ネットワークで伝送されるファイルを識別/ブロックする方法をきめ細かく制御できます。ただし、アクセス制御のデフォルト アクションによって処理されるトラフィックを検査するためにファイル ポリシーを使用**できない**ことに注意してください。詳細については、許可されたトラフィックに対する侵入およびマルウェアの有無のインスペクション （172 ページ）を参照してください。

ファイル ルール

ファイル ポリシーの中でファイル ルールを設定します。次の表に、ファイル ルールのコンポーネントを示します。

表 *66 :* ファイル ルールのコンポーネント

ファイル ルールのコンポーネント	説明
アプリケーション プロトコル	システムは、FTP、HTTP、SMTP、IMAP、POP3、NetBIOS-ssn（SMB）を介して伝送されるファイルを検出し、検査できます。パフォーマンスを向上させるには、ファイル ルールごとに、これらのアプリケーション プロトコルのうち 1 つだけでファイルを検出するよう限定できます。
転送の方向	ダウンロードされるファイルに対して、FTP、HTTP、IMAP、POP3、および NetBIOS-ssn（SMB）の着信トラフィックを検査できます。アップロードされるファイルに対しては、FTP、HTTP、SMTP、および NetBIOS-ssn（SMB）の発信トラフィックを検査できます。

ファイル ルールのコンポーネント	説明
ファイルのカテゴリとタイプ	システムは、さまざまなタイプのファイルを検出できます。これらのファイル タイプは、マルチメディア（swf、mp3）、実行可能ファイル（exe、トレント）、PDF などの基本的なカテゴリにグループ分けされます。個々のファイル タイプを検出したり、ファイル タイプ カテゴリ全体を検出したりするよう、ファイル ルールを設定できます。 たとえば、すべてのマルチメディア ファイルをブロックしたり、Shockwave Flash（swf）ファイルのみをブロックしたりできます。または、ユーザが BitTorrent（torrent）ファイルをダウンロードしたときにアラートを出すよう、システムを設定できます。 **注意** 頻繁にトリガーされるファイル ルールは、システム パフォーマンスに影響を与える可能性があります。たとえば、HTTP トラフィックでマルチメディア ファイルを検出しようとすると（たとえばYouTubeは多量のFlashコンテンツを伝送します）、膨大な数のイベントが生成される可能性があります。
ファイル ルール アクション	ファイル ルール アクションは、ルールの条件に一致するトラフィックがシステムによってどのように処理されるかを決定します。 （注） 複数のファイル ルールは（数値順ではなく）ルール アクション順に評価されます。詳細については、次の「ファイル ルール アクションと評価順序」を参照してください。

ファイル ルール アクションと評価順序

各ファイル ルールには、ルールの条件に一致するトラフィックがシステムによってどのように処理されるかを決定する 1 つのアクションが関連付けられます。1 つのファイル ポリシー内に、ファイル タイプ、アプリケーション プロトコル、転送方向の違いに応じて異なるアクションを実行する別々のルールを設定できます。複数のルール アクションは、以下のようなルール アクション順になります。

- ファイル ブロック ルールを使用すると、特定のファイル タイプをブロックできます。
- マルウェア ブロック ルールを使用すると、特定のファイル タイプの SHA-256 ハッシュ値を計算した後、クラウド ルックアップ プロセスを使用して、ネットワークを通過するファイルにマルウェアが含まれているかどうかまず判断し、脅威を示すファイルをブロックできます。
- マルウェア クラウド ルックアップ ルールを使用すると、ネットワークを通過するファイルの伝送を許可しながら、クラウド ルックアップに基づいてそのファイルのマルウェアの性質をログに記録できます。
- ファイル検出ルールを使用すると、ファイルの伝送を許可しながら、特定のファイル タイプの検出をログに記録できます。

各ファイル ルール アクションに対して、ファイル転送がブロックされると接続をリセットするというオプションを設定できます。次の表に、各ファイルアクションで使用可能なオプションの詳細を示します。

表 *67 :* ファイル ルール アクション

アクション	接続をリセットするか
ファイル ブロック（Block Files）	はい（推奨）
マルウェア ブロック（Block Malware）	はい（推奨）
ファイル検出（Detect Files）	いいえ
マルウェア クラウドルックアップ（Malware Cloud Lookup）	いいえ

ファイルとマルウェアの検出、キャプチャ、およびブロッキングに関する注意事項と制約事項

ファイルとマルウェアの検出、キャプチャ、およびブロッキングの動作に関して、以下の詳細および制限に注意してください。

- ファイルがセッションで検出されブロックされるまで、セッションからのパケットは侵入インスペクションの対象になる場合があります。
- ファイルの終わりを示す End of File マーカーが検出されない場合、転送プロトコルとは無関係に、そのファイルは**マルウェア ブロック** ルールでもカスタム検出リストでもブロックされません。システムは、End of File マーカーで示されるファイル全体の受信が完了するまでファイルのブロックを待機し、このマーカーが検出された後にファイルをブロックします。
- FTP ファイル転送で End of File マーカーが最終データ セグメントとは別に伝送される場合、マーカーがブロックされ、ファイル転送失敗が FTP クライアントに表示されますが、実際にはそのファイルは完全にディスクに転送されます。
- FTP は、さまざまなチャネルを介してコマンドおよびデータを転送します。パッシブ展開では、FTP データ セッションとその制御セッションからのトラフィックが同じ Snort に負荷分散されない場合があります。
- ファイルがアプリケーション プロトコル条件を持つルールに一致する場合、ファイル イベントの生成は、システムがファイルのアプリケーションプロトコルを正常に識別した後に行われます。識別されていないファイルは、ファイル イベントを生成しません。
- FTP に関する [マルウェア ブロック（Block Malware）] ルールを持つファイル ポリシーを使用するアクセス コントロール ポリシーでは、[インライン時にドロップ（Drop when Inline）] を無効にした侵入ポリシーをデフォルトアクションに設定した場合、システムはルールに一致するファイルやマルウェアの検出でイベントを生成しますが、ファイルをドロップしません。FTP ファイア転送をブロックし、ファイル ポリシーを選択するアクセス コントロール ポリシーのデフォルトアクションとして侵入ポリシーを使用するには、[Drop when Inline] を有効にした侵入ポリシーを選択する必要があります。

- [ファイル ブロック（Block Files）] アクションおよび [マルウェア ブロック（Block Malware）] アクションを持つファイル ルールでは、最初のファイル転送試行後 24 時間で検出される、同じファイル、URL、サーバ、クライアントアプリケーションを使った新しいセッションをブロックすることにより、HTTP 経由のファイル ダウンロードの自動再開をブロックします。
- まれに、HTTP アップロードセッションからのトラフィックが不適切である場合、システムはトラフィックを正しく再構築できなくなり、トラフィックのブロックやファイルイベントの生成を行いません。
- **ファイル ブロック** ルールでブロックされる NetBios-ssn 経由ファイル転送（SMB ファイル転送など）の場合、宛先ホストでファイルが見つかることがあります。ただし、ダウンロード開始後にファイルがブロックされ、結果としてファイル転送が不完全になるため、そのファイルは使用できません。
- （SMB ファイル転送など）NetBios-ssn 経由で転送されるファイルを検出またはブロックするファイル ルールを作成した場合、ファイル ポリシーを呼び出すアクセス コントロール ポリシーの適用前に開始された、確立済み TCP または SMB セッションで転送されるファイルに対しては、検査が行われません。このため、これらのファイルは検出/ブロックされません。
- パッシブ展開でファイルをブロックするよう設定されたルールは、一致するファイルをブロックしません。接続ではファイル伝送が続行されるため、接続の開始をログに記録するルールを設定した場合、この接続に関して複数のイベントが記録されることがあります。
- POP3、POP、SMTP、または IMAP セッションでのすべてのファイル名の合計バイト数が 1024 を超えると、セッションのファイル イベントでは、ファイル名バッファがいっぱいになった後で検出されたファイルの名前が正しく反映されないことがあります。
- SMTP 経由でテキストベースのファイルを送信すると、一部のメール クライアントは改行を CRLF 改行文字標準に変換します。MAC ベースのホストはキャリッジ リターン（CR）文字を使用し、Unix/Linux ベースのホストはライン フィード（LF）文字を使用するので、メール クライアントによる改行変換によってファイルのサイズが変更される場合があります。一部のメール クライアントは、認識できないファイル タイプを処理する際に改行変換を行うようデフォルト設定されていることに注意してください。
- シスコでは、[Block Files] アクションと [Block Malware] アクションで [Reset Connection] を有効にすることを推奨しています。これにより、ブロックされたアプリケーション セッションが TCP 接続リセットまで開いたままになることを防止できます。接続をリセットしない場合、TCP 接続が自身をリセットするまで、クライアント セッションが開いたままになります。
- マルウェア クラウド ルックアップ アクションまたは マルウェア ブロック アクションを使用してファイル ルールが設定されている場合、ASA FirePOWER モジュールがクラウドとの接続を確立できないと、クラウド接続が復元されるまで、システムは設定済みルール アクション オプションを実行できません。

ファイル ルールの評価例

番号順にルールが評価されるアクセス コントロール ポリシーとは異なり、ファイル ポリシーでは「ファイル ルール アクションと評価順序」に従ってファイルが処理されます。つまり、（優先度の高い順に）単純なブロッキング、次にマルウェア インスペクションとブロッキング、さらにその次に単純な検出とロギングとなります。例として、1つのファイルポリシー内に、PDF ファイルを処理する 4 つのルールがあるとします。モジュール インターフェイスで表示される順序に関係なく、これらのルールは次の順序で評価されます。

表 *68 :* ファイル ルールの評価順序の例

アプリケーションプロトコル	方向	アクション	アクションのオプション	結果
SMTP	アップロード	ファイルブロック	接続のリセット	ユーザが電子メールで PDF ファイルを送信することをブロックし、接続をリセットします。
FTP	ダウンロード	マルウェア ブロック	接続のリセット	ファイル転送によるマルウェア PDF ファイルのダウンロードをブロックし、接続をリセットします。
POP3 IMAP	ダウンロード	マルウェア クラウドルックアップ	なし	電子メールで受信した PDF ファイルについてマルウェアを検査します。
いずれか（Any）	いずれか（Any）	ファイル検出	なし	ユーザが Web 上で（つまり HTTP 経由で）PDF ファイルを表示すると、それを検出してログに記録しますが、トラフィックは許可します。

ASA FirePOWER モジュールでは、矛盾するファイル ルールを示すために警告アイコンが使用されます。

システムで検出されるすべてのファイル タイプに対してマルウェア分析を実行できるわけではないことに注意してください。[Application Protocol] 、[Direction of Transfer]、および [Action] ドロップダウン リストで値を選択すると、システムはファイル タイプのリストを限定します。

ファイル イベント、マルウェア イベント、およびアラートのロギング

ファイル ポリシーをアクセス コントロール ルールに関連付けると、一致するトラフィックに関するファイル イベントとマルウェア イベントのロギングが自動的に有効になります。ファイルを検査するときに、システムは次のタイプのイベントを生成できます。

- ファイル イベント：検出またはブロックされたファイル、および検出されたマルウェア ファイルを表します。

- マルウェア イベント：検出されたマルウェア ファイルを表します。
- レトロスペクティブ マルウェア イベント：以前に検出されたファイルに関するマルウェア ファイルの性質が変更された場合に生成されます。

ファイル ポリシーでファイル イベントまたはマルウェア イベントが生成されるか、ファイルがキャプチャされると、システムは（起動元のアクセス コントロール ルールにおけるロギング設定とは無関係に）関連する接続の終了を自動的に記録します。

（注） NetBIOS-ssn（SMB）トラフィックの検査によって生成されるファイル イベントは、即座には接続イベントを生成しません。これは、クライアントとサーバが持続的接続を確立するためです。システムはクライアントまたはサーバがセッションを終了した後に接続イベントを生成します。

これらの接続イベントごとに、

- [Files] フィールドには、接続で検出されたファイル数（マルウェア ファイルを含む）を示すアイコン（）が含まれます。このアイコンをクリックすると、それらのファイルのリスト、およびマルウェア ファイルの性質が表示されます。
- [Reason] フィールドには、接続イベントがログに記録された理由が示されます。これはファイル ルール アクションに応じて次のように異なります。
  - [File Monitor]：ファイル検出ルールおよびマルウェア クラウド ルックアップ ルールの場合、およびクリーン リスト内のファイルの場合
  - [File Block]：ファイル ブロック ルールまたはマルウェア ブロック ルールの場合
  - [File Custom Detection]： カスタム検出リストにあるファイルをシステムが検出した場合
  - [File Resume Allow]：ファイル ブロック ルールまたはマルウェア ブロック ルールによってファイル伝送が最初にブロックされた場合。ファイルを許可する新しいアクセス コントロール ポリシーが適用された後、HTTP セッションが自動的に再開しました。
  - [File Resume Block]：ファイル検出ルールまたはマルウェア クラウド ルックアップ ルールによってファイル伝送が最初に許可された場合。ファイルをブロックする新しいアクセス コントロール ポリシーが適用された後、HTTP セッションが自動的に停止しました。
- ファイルやマルウェアがブロックされた接続の場合、[Action] は [Block] です。

ファイル イベントやマルウェア イベントは、ASA FirePOWER モジュールによって生成される各種イベントと同じように表示できます。また、SNMP や syslog によって警告されたマルウェア イベントを使用することもできます。

インターネット アクセス

システムはポート 443 を使用して、ネットワークベース AMP 用のマルウェア クラウド ルックアップを実行します。ASA FirePOWER モジュールで発信ポートを開く必要があります。

ファイル ポリシーの管理

[File Policies] ページ（[Policies] > [Files]）でファイル ポリシーの作成、編集、削除、および比較を行います。このページには既存のファイル ポリシーのリストと、ポリシーの最終更新日が表示されます。

ファイル ポリシーの適用アイコンをクリックするとダイアログボックスが表示され、そのファイル ポリシーを使用するアクセス コントロール ポリシーが示された後、[Access Control Policy] ページにリダイレクトされます。これは、ファイル ポリシーが親アクセス コントロール ポリシーの一部と見なされ、ファイル ポリシーを単独で適用できないためです。新しいファイル ポリシーを使用したり、既存のファイル ポリシーの変更内容を適用したりするには、親アクセス コントロール ポリシーを適用/再適用する必要があります。

保存済みまたは適用済みのアクセス コントロール ポリシーで使われているファイル ポリシーは削除できないことに注意してください。

ファイル ポリシーの作成

ライセンス：Protection または Malware

ファイル ポリシーを作成して、その中でルールを設定すると、それをアクセス コントロール ポリシーで使用できるようになります。

ヒント 既存のファイル ポリシーのコピーを作成するには、コピー アイコンをクリックして、表示されるダイアログボックスで新しいポリシーの一意の名前を入力します。その後、そのコピーを変更できます。

ファイル ポリシーを作成する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Files] の順に選択します。

[File Policies] ページが表示されます。

新しいポリシーの場合、ポリシーが使用中でないことがモジュール インターフェイスに示されます。使用中のファイル ポリシーを編集している場合は、そのファイル ポリシーを使用しているアクセス コントロール ポリシーの数がモジュール インターフェイスに示されます。どちらの場合も、テキストをクリックすると [Access Control Policies] ページに移動できます（アクセス コントロール ポリシーの開始 （79 ページ）を参照）。

ステップ 2 新しいポリシーの [Name] とオプションの [Description] を入力してから、[Save] をクリックします。

[File Policy Rules] タブが表示されます。

ステップ 3 ファイル ポリシーに 1 つ以上のルールを追加します。

ファイル ルールを使用すると、ロギング、ブロック、またはマルウェア スキャンの対象となるファイル タイプを詳細に制御できます。ファイル ルールの追加については、ファイル ルールの操作 （461 ページ）を参照してください。

ステップ 4 詳細オプションを設定します。詳細については、「ファイル ポリシーの詳細オプション（General）の設定（463 ページ）」を参照してください。

ステップ 5 [Store ASA FirePOWER Changes] をクリックします。

新しいポリシーを使用するには、アクセス コントロール ルールにファイル ポリシーを追加してから、アクセス コントロール ポリシーを適用する必要があります。既存のファイル ポリシーを編集している場合は、そのファイル ポリシーを使用するすべてのアクセス コントロール ポリシーを再適用する必要があります。

ファイル ルールの操作

ライセンス：Protection または Malware

効果を発揮するには、ファイル ポリシーに 1 つ以上のルールが含まれている必要があります。新しいファイル ポリシーを作成するとき、または既存のポリシーを編集するときに表示される [File Policy Rules] ページで、ルールを作成、編集、および削除します。このページには、ポリシー内のすべてのルールがリストされ、各ルールの基本的な特性も示されます。

また、このページでは、このファイル ポリシーを使用するアクセス コントロール ポリシーの数も通知されます。この通知をクリックすると、親ポリシーのリストが表示され、オプションで [Access Control Policies] ページに進むことができます。

ファイル ルールを作成する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Files] を選択します。

[File Policies] ページが表示されます。

ステップ 2 次の選択肢があります。

- 新しいポリシーにルールを追加するには、[New File Policy] をクリックして、新しいポリシーを作成します（ファイル ポリシーの作成 （460 ページ）を参照）。
- 既存のポリシーにルールを追加するには、ポリシーの横にある編集アイコンをクリックします。

ステップ 3 表示される [File Policy Rules] ページで、[Add File Rule] をクリックします。

[Add File Rule] ダイアログボックスが表示されます。

ステップ 4 ドロップダウンリストから、[Application Protocol] を選択します。

デフォルトの [Any] は、HTTP、SMTP、IMAP、POP3、FTP、および NetBIOS-ssn（SMB）トラフィック内のファイルを検出します。

ステップ 5 ドロップダウンリストから [Direction of Transfer] を選択します。

ダウンロードされるファイルに関して、以下のタイプの着信トラフィックを検査できます。

- HTTP
- IMAP
- POP3
- FTP
- NetBIOS-ssn（SMB）

アップロードされるファイルに関して、以下のタイプの発信トラフィックを検査できます。

- HTTP
- FTP
- SMTP
- NetBIOS-ssn（SMB）

[Any] を使用すると、ユーザが送信しているか受信しているかには関係なく、多数のアプリケーション プロトコルを介したファイルが検出されます。

ステップ 6 ファイル ルールの [Action] を選択します。詳細については、表「ファイル ルール アクション」を参照してください。

[Block Files] または [Block Malware] を選択すると、[Reset Connection] がデフォルトで有効になります。ファイル転送のブロックが発生した接続をリセット**しない**ようにするには、[Reset Connection] チェックボックスをクリアします。

（注） シスコでは、[Reset Connection] を有効のままにしておくことを推奨しています。これにより、ブロックされたアプリケーションセッションが TCP 接続リセットまで開いたままになることを防止できます。

ファイル ルールのアクションの詳細については、「ファイル ルール アクションと評価順序」を参照してください。

ステップ 7 [File Types] を 1 つ以上選択します。複数のファイル タイプを選択するには、Shift キーと Ctrl キーを使用します。ファイル タイプのリストを、次のようにフィルタ処理できます。

- [File Type Categories] を 1 つ以上選択します。
- 名前または説明でファイル タイプを検索します。たとえば、Microsoft Windows 固有のファイルのリストを表示するには、[Search name and description] フィールドに「Windows」と入力します。

ファイル ルールで使用できるファイル タイプは、[Application Protocol] 、[Direction of Transfer] 、および [Action] での選択内容に応じて変化します。

たとえば、[Direction of Transfer] で [Download] を選択すると、ファイル イベントが過剰になるのを防止するために、[Graphics] カテゴリから [GIF]、[PNG]、[JPEG]、[TIFF]、および [ICO] が削除されます。

ステップ 8 選択したファイル タイプを [Selected Files Categories and Types] リストに追加します。

- [Add] をクリックすると、選択したファイル タイプがルールに追加されます。
- 1 つ以上のファイル タイプを [Selected Files Categories and Types] リストの中にドラッグ アンド ドロップします。
- カテゴリを選択して [All types in selected Categories] をクリックしてから、[Add] をクリックするか、選択項目を [Selected Files Categories and Types] リストの中にドラッグ アンド ドロップします。

ステップ 9 [Store ASA FirePOWER Changes] をクリックします。

ファイル ルールがポリシーに追加されます。既存のファイル ポリシーを編集している場合、変更内容を有効にするには、そのファイル ポリシーを使用するすべてのアクセス コントロール ポリシーを再適用する必要があります。

ファイル ポリシーの詳細オプション（General）の設定

ライセンス：Malware

ファイル ポリシーでは、[General] セクションにある以下の詳細オプションを設定できます。

表 *69 :* ファイル ポリシーの詳細オプション（*General*）

フィールド	説明	デフォルト値
Enable Custom Detection List	これを選択すると、カスタム検出リストにあるファイルが検出されたときに、そのファイルをブロックします。	有効（enabled）
Enable Clean List	これを選択すると、クリーン リストにあるファイルが検出されたときに、そのファイルを許可します。	有効（enabled）

ファイル ポリシーの詳細オプション（General）を設定するには、次の手順を実行します。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Files] の順に選択します。

[File Policies] ページが表示されます。

ステップ 2 編集するポリシーの横にある編集アイコンをクリックします。

[File Policy Rule] ページが表示されます。

ステップ 3 [Advanced] タブを選択します。

[Advanced] タブが表示されます。

ステップ 4 表「ファイル ポリシーの詳細オプション（General）」の説明に従い、オプションを変更します。

ステップ 5 [Store ASA FirePOWER Changes] をクリックします。

編集したファイル ポリシーを使用するすべてのアクセス コントロール ポリシーを再適用する必要があります。

2 つのファイル ポリシーの比較

ライセンス：Protection

変更後のポリシーが組織の標準に準拠することを確かめたり、システム パフォーマンスを最適化したりする目的で、任意の 2 つのファイル ポリシー間の違いや、同じポリシーの 2 つのリビジョン間の違いを調べることができます。

ファイル ポリシーの比較ビューには、2 つのポリシーまたはリビジョンが並んで表示され、各ポリシー名の横には最終変更時刻と最後に変更したユーザが表示されます。2 つのポリシー間の違いは次のように強調表示されます。

- 青色は強調表示された設定が 2 つのポリシーで異なることを示し、差異は赤色で示されます。
- グリーンは、強調表示されている設定項目が一方のポリシーに含まれ、もう一方のポリシーには含まれないことを示します。

[Previous] と [Next] をクリックすると、前後の相違箇所に移動できます。左側と右側の間にある二重矢印アイコンが移動し、[Difference] 番号が調整されて、表示中の差異が示されます。必要に応じて、ファイル ポリシーの比較レポートを生成できます。これは PDF 版の比較ビューです。

2 つのファイル ポリシーを比較する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Files] の順に選択します。

[File Policies] ページが表示されます。

ステップ 2 [Compare Policies] をクリックします。

[Select Comparison] ダイアログボックスが表示されます。

ステップ 3 [Compare Against] ドロップダウン リストから、比較するタイプを次のように選択します。

- 2 つの異なるポリシーを比較するには、[Running Configuration] または [Other Policy] を選択します。この 2 つのオプションの違いは、[Running Configuration] を選択した場合、現在適用されている一連のファイル ポリシーの中からのみ、比較対象の 1 つを選択できます。
- 同じポリシーのバージョン間を比較するには、[Other Revision] を選択します。

ダイアログ ボックスの表示が更新され、比較オプションが示されます。

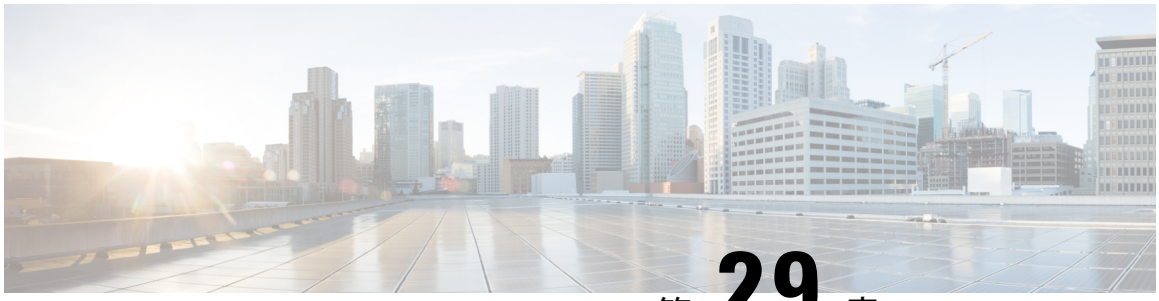
ステップ 4 選択した比較タイプに応じて、次の選択肢があります。

- 2 つの異なるポリシーを比較する場合、比較対象のポリシーとして [Policy A] または [Target/Running Configuration A] のどちらかと、[Policy B] とを選択します。
- 同じポリシーのバージョン間を比較する場合、対象の [Policy] を選択してから、2 つのリビジョン [Revision A] と [Revision B] を選択します。リビジョンは、日付とユーザ名別にリストされます。

ステップ 5 [OK] をクリックします。

比較ビューが表示されます。

ステップ 6 オプションで、[Comparison Report] をクリックして、ファイル ポリシー比較レポートを生成します。コンピュータにレポートを保存するように求められます。



第 29 章

ネットワーク トラフィックの接続のロギング

デバイスがネットワーク上でホストによって生成されたトラフィックをモニタするとき、デバイスは検出した接続のログを生成できます。アクセス コントロールおよび SSL ポリシーでさまざまな設定を行うことで、ロギングする接続の種類、接続をロギングする時期、およびデータを保存する場所をきめ細かく制御することができます。また、アクセス コントロール ルールの特定のロギング設定では、接続に関連するファイル イベントとマルウェア イベントをログに記録するかどうかも決定します。

ほとんどの場合、接続の開始時および終了時に接続をログに記録できます。接続をログに記録すると、システムによって接続イベントが生成されます。接続がレピュテーションベースのセキュリティ インテリジェンス機能によってブロックされる場合は、セキュリティ インテリジェンス イベントと呼ばれる特別な種類の接続イベントをログに記録することもできます。

接続イベントには、検出されたセッションに関するデータが含まれています。

組織のセキュリティ上およびコンプライアンス上の要件に従って接続をロギングしてください。

どの接続をログに記録するかの決定

ライセンス：任意

アクセス コントロール ポリシーと SSL ポリシーのさまざまな設定を使用して、ASA FirePOWER モジュールがモニタする接続をログに記録できます。ほとんどの場合、接続の開始時および終了時に接続をログに記録できます。ただし、ブロックされたトラフィックは追加のインスペクションなしですぐに拒否されるため、システムがログに記録できるのはブロックされたトラ

フィックの接続開始イベントのみです。ログに記録できる固有の接続終了イベントはありません。

接続イベントをログに記録すると、イベント ビューアで表示できます。または、外部 syslog あるいは SNMP トラップ サーバに接続データを送信できます。

ヒント　ASA FirePOWER モジュールを使用して接続データの詳細な分析を実行するために、シスコではクリティカルな接続の終了をログに記録することを推奨しています。

クリティカルな接続のロギング

ライセンス：任意

組織のセキュリティ上およびコンプライアンス上の要件に従って接続をロギングしてください。目標が生成するイベントの数を抑えパフォーマンスを向上させることである場合は、分析のために重要な接続のロギングのみを有効にします。しかし、プロファイリングの目的でネットワーク トラフィックの広範な表示が必要な場合は、追加の接続のロギングを有効にできます。アクセス コントロールおよび SSL ポリシーでさまざまな設定を行うことで、ロギングする接続の種類、接続をロギングする時期、およびデータを保存する場所をきめ細かく制御することができます。

注意　サービス妨害（DoS）攻撃の間にブロックされたTCP接続をロギングすると、類似の複数のイベントによってシステムが過負荷になる可能性があります。ブロック ルールに対してロギングを有効にする前に、そのルールがインターネット側のインターフェイスまたは DoS 攻撃を受けやすい他のインターフェイス上のトラフィックをモニタするかどうかを検討します。

設定するロギングに加えて、システムは禁止されたファイル、マルウェア、または侵入の試みを検出した場合に、ほとんどの接続を自動的にログに記録します。システムはこれらの接続終了イベントを、さらに分析するために保存します。すべての接続イベントは、自動的にログ記録された理由を [Action] および [Reason] フィールドで反映します。

セキュリティ インテリジェンスによるブロックの決定（オプション）

接続がレピュテーションベースのセキュリティインテリジェンス機能によってブロックされる場合は、その接続をログに記録できます。オプションで、セキュリティインテリジェンスフィルタリングにはモニター専用設定を使用できます。パッシブ展開環境では、この設定が推奨されます。この設定では、ブロックされるはずの接続をシステムがさらに分析できるだけでなく、一致する接続をログに記録することもできます。

セキュリティ インテリジェンスのロギングを有効にすると、ブロックリストに一致するトラフィックによってセキュリティ インテリジェンス イベントと接続イベントが生成されます。セキュリティ インテリジェンス イベントは特殊なタイプの接続イベントで、個別に表示および分析できるだけでなく、個別に保存およびプルーニングできます。詳細については、セキュリティ インテリジェンスによる判断のロギング （475 ページ）を参照してください。

アクセス コントロールの処理（任意）

接続がアクセス コントロール ルールまたはアクセス コントロールのデフォルト アクションによって処理される場合は、その接続をログに記録できます。このロギングはアクセス コントロール ルールごとに設定し、クリティカルな接続のみをログに記録できるようにします。詳細については、アクセス コントロールの処理に基づく接続のロギング（477 ページ）を参照してください。

侵入に関連付けられた接続（自動）

アクセス コントロール ルールによって呼び出された侵入ポリシー（アクセス コントロール ルールを使用したトラフィック フローの調整（111 ページ）を参照）が侵入を検出して侵入イベントを生成すると、システムはルールのロギング設定に関係なく、侵入が発生した接続の終了を自動的にロギングします。

しかし、アクセス コントロールのデフォルト アクションに関連付けられた侵入ポリシー（デフォルトの処理の設定およびネットワーク トラフィックのインスペクション（83 ページ）を参照）によって侵入イベントが生成された場合、システムは関連する接続の終了を自動的にログに記録**しません**。代わりに、デフォルトのアクション接続のロギングを明示的に有効にする必要があります。これは、接続データをログに記録する必要がない、侵入防御専用の展開環境で役立ちます。

侵入がブロックされた接続では、接続ログ内の接続のアクションは Block、理由は Intrusion Block ですが、侵入インスペクションを実行するには、許可ルールを使用する必要があります。

ファイル イベントとマルウェア イベントに関連付けられた接続（自動）

アクセス コントロール ルールによって呼び出されたファイル ポリシーが禁止されたファイル（マルウェアを含む）を検出してファイル イベントまたはマルウェア イベントを生成すると、システムはアクセス コントロール ルールのロギング設定に関係なく、ファイルが検出された接続の終了をデータベースに自動的にロギングします。このロギングを無効にすることはできません。

（注） NetBIOS-ssn（SMB）トラフィックの検査によって生成されるファイル イベントは、即座には接続イベントを生成しません。これは、クライアントとサーバが持続的接続を確立するためです。システムはクライアントまたはサーバがセッションを終了した後に接続イベントを生成します。

ファイルがブロックされた接続では、接続ログ内の接続のアクションは [Block] ですが、ファイルおよびマルウェアのインスペクションを実行するには、許可ルールを使用する必要があります。接続の原因は、File Monitor（ファイル タイプまたはマルウェアが検出された）、あるいは Malware Block または File Block（ファイルがブロックされた）です。

接続の開始および終了のロギング

ライセンス：任意

システムが接続を検出すると、ほとんどの場合、その開始および終了をログに記録できます。

ただし、ブロックされたトラフィックは追加のインスペクションなしですぐに拒否されるため、多くの場合、ユーザがログに記録できるのはブロックされたトラフィックの接続開始イベントのみです。ログに記録できる固有の接続終了イベントはありません。

（注） 単一のブロックされていない接続の場合、接続終了イベントには、接続開始イベントに含まれるすべての情報に加えて、セッション期間中に収集された情報も含まれます。

何らかの理由で接続をモニタすると、接続終了ロギングが強制されることに注意してください。モニタされる接続のロギングについて （471 ページ） を参照してください。

次の表では、接続開始イベントと接続終了イベントの違い（それぞれをロギングする利点を含む）を詳細に説明します。

コンテキスト	接続開始イベント	接続終了イベント
次の場合に生成可能です	システムが接続の開始を検出した場合（または、イベントの生成がアプリケーションまたは URL の識別に依存する場合は最初の数パケットの後）	システムが以下の場合 • 接続のクローズを検出した場合 • 一定期間後に接続の終了を検出しない場合 • メモリ制約によりセッションを追跡できなくなった場合
次のものについてロギングが可能です	セキュリティインテリジェンスまたはアクセス コントロール ルールで評価されているすべての接続	すべての接続は構成可能。ただしシステムはブロックされている接続の終了をログに記録できない
次を含みます	最初のパケット（または、イベントの生成がアプリケーションまたは URL の識別に依存する場合は最初の数パケット）で判別できる情報のみ	接続開始イベント内のすべての情報と、セッション期間を通してトラフィックを検査して判別された情報（たとえば伝送されたデータ総量、接続の最後のパケットのタイムスタンプなど）
次の場合に有用です	次のものをロギングする場合 • セキュリティインテリジェンスによるブロッキングの決定を含む、ブロックされた接続	次を実行する場合 • セッションの期間にわたって収集された情報であらゆる種類の詳細な分析を実行する場合 • グラフィカル形式での接続データの表示

ASA FirePOWER モジュールまたは外部サーバへの接続のロギング

ライセンス：任意

接続イベントのログは、ASA FirePOWER モジュールの他に、外部の syslog または SNMP トラップ サーバに記録できます。外部サーバに接続データを記録する前に、そのサーバにアラート応答という接続を設定する必要があります。アラート応答の使用 （504 ページ）を参照してください。

アクセス コントロールおよび SSL ルール アクションがどのようにロギングに影響を及ぼすかについて

ライセンス：機能に応じて異なる

すべてのアクセス コントロールおよび SSL ルールにはアクションがあり、それによってシステムがルールに一致するトラフィックを検査および処理する方法だけでなく、一致するトラフィックに関する詳細をユーザがロギングできる時期と方法が決まります。

モニタされる接続のロギングについて

ライセンス：機能に応じて異なる

システムは、ルールのロギング設定や、後で接続を処理するデフォルト アクションとは関係なく、次の接続の終了を ASA FirePOWER モジュールに常にロギングします。

- モニタに設定されたセキュリティ インテリジェンスのブロックリストに一致する接続
- アクセス コントロールのモニタ ルールに一致する接続

つまり、パケットが他のルールに一致せず、デフォルトのアクションでロギングが有効になっていない場合でも、パケットがモニタのルールまたはセキュリティ インテリジェンスのモニタ対象のブロックリストに一致すれば、必ず接続がログに記録されます。セキュリティ インテリジェンスのフィルタリングの結果、システムが接続イベントをロギングすると、一致するセキュリティ インテリジェンス イベントもロギングされます。そのイベントは特殊なタイプの接続イベントで、個別に表示および分析できます。セキュリティ インテリジェンスによる判断のロギング （475 ページ）を参照してください。

モニタ対象のトラフィックは、必ず後で別のルールまたはデフォルト アクションによって処理されるため、モニタ ルールが原因でロギングされる接続に関連するアクションは、決して Monitor にはなりません。代わりに、後で接続を処理するルールまたはデフォルト アクションの操作が反映されます。

システムは、1 つの接続が 1 つの SSL またはアクセス コントロールのモニタ ルールに一致するたびに 1 つの別個のイベントを生成するわけではありません。1 つの接続が複数のモニタ ルールに一致する可能性があるため、ASA FirePOWER モジュールにロギングされる各接続イベントには、接続が一致する最初の 8 つのモニタ アクセス コントロール ルールに関する情報だけでなく、最初に一致するモニタ SSL ルールに関する情報を含めて表示できます。

同様に、外部 syslog または SNMP トラップ サーバに接続イベントを送る場合、システムは 1 つの接続が 1 つのモニタ ルールに一致するたびに 1 つの別個のアラートを送信するわけではありません。代わりに、接続の終了時にシステムから送られるアラートに、接続が一致したモニター ルールの情報が含まれます。

信頼されている接続のロギングについて

ライセンス：機能に応じて異なる

信頼されている接続は、信頼アクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルト アクションによって処理される接続です。これらの接続の開始と終了をロギングできますが、暗号化されているかどうかにかかわらず、信頼されている接続は、侵入や、禁止されているファイルおよびマルウェアについて検査されないことに注意してください。したがって、信頼されている接続の接続イベントには、限られた情報が含まれます。

ブロックされた接続およびインタラクティブにブロックされた接続のロギングについて

ライセンス：機能に応じて異なる

トラフィックをブロックするアクセス コントロール ルールおよびアクセス コントロール ポリシーのデフォルト アクション（インタラクティブなブロッキング ルールを含む）の場合は、システムは接続開始イベントをロギングします。一致するトラフィックは、追加のインスペクションなしで拒否されます。

アクセス コントロールまたは SSL ルールでブロックされたセッションの接続イベントには、Block または Block with reset アクションがあります。ブロックされた暗号化接続の理由は SSL Block です。

インタラクティブ ブロッキング アクセス コントロール ルール（禁止されている Web サイトをユーザが参照するとシステムによって警告ページが表示される）は、接続の終了をログに記録します。その理由は、警告ページをユーザがクリック スルーすると、その接続は新規の、許可された接続と見なされ、システムによってモニタとロギングができるためです。許可された接続のロギングについて （473 ページ） を参照してください。

したがって、インタラクティブ ブロック ルールまたはリセット付きインタラクティブ ブロック ルールにパケットが一致する場合、システムは以下の接続イベントを生成できます。

- ユーザの要求が最初にブロックされ警告ページが表示されたときの接続開始イベント。このイベントにはアクション [インタラクティブ ブロック（Interactive Block）] または [リセットしてインタラクティブ ブロック（Interactive Block with reset）] が関連付けられます。
- 複数の接続開始または終了イベント（ユーザが警告ページをクリックスルーし、要求した最初のページをロードした場合。これらのイベントには Allow アクションおよび理由 User Bypass が関連付けられます）

インラインで展開されたデバイスのみがトラフィックをブロックできることに注意してください。ブロックされた接続はパッシブ展開で実際にはブロックされないため、システムにより、ブロックされた各接続に対し複数の接続開始イベントが報告される場合があります。

⚠

注意 サービス妨害（DoS）攻撃の間にブロックされたTCP接続をロギングすると、類似の複数のイベントによってシステムが過負荷になる可能性があります。ブロック ルールに対してロギングを有効にする前に、そのルールがインターネット側のインターフェイスまたはDoS 攻撃を受けやすい他のインターフェイス上のトラフィックをモニタするかどうかを検討します。

許可された接続のロギングについて

ライセンス：機能に応じて異なる

[Decrypt] SSL ルール、[Do not decrypt] SSL ルール、および [Allow] アクセス コントロール ルールは、一致するトラフィックを許可し、インスペクションおよびトラフィック処理の次のフェーズへと通過させます。

アクセス コントロール ルールでトラフィックを許可すると、関連付けられた侵入ポリシーまたはファイル ポリシー（またはその両方）を使用して、トラフィックをさらに検査し、トラフィックが最終宛先に到達する前に、侵入、禁止されたファイル、およびマルウェアをブロックすることができます。

許可アクセス コントロール ルールに一致するトラフィックの接続は次のようにロギングされます。

- アクセス コントロール ルールによって呼び出された侵入ポリシーが侵入を検出して侵入イベントを生成すると、システムはルールのロギング設定に関係なく、侵入が発生した接続の終了を ASA FirePOWER モジュールに自動的にロギングします。
- アクセス コントロール ルールによって呼び出されたファイル ポリシーが禁止されたファイル（マルウェアを含む）を検出してファイル イベントまたはマルウェア イベントを生成すると、システムはアクセス コントロール ルールのロギング設定に関係なく、ファイルが検出された接続の終了を ASA FirePOWER モジュールに自動的にロギングします。
- 任意で、システムが安全と見なすトラフィックや、侵入ポリシーまたはファイル ポリシーで検査をしないトラフィックなど、許可されたトラフィックに対して接続の開始および終了のロギングを有効にできます。

結果として生じるすべての接続イベントで、[Action] および [Reason] フィールドにイベントがロギングされた理由が反映されます。次の点に注意してください。

- アクション Allow は、最終宛先に到達した明示的に許可され、ユーザがバイパスしたインタラクティブにブロックされた接続を表します。
- アクション Block は、アクセス コントロール ルールによって初めは許可されたが、侵入、禁止されたファイル、またはマルウェアが検出された接続を表します。

許可された接続のファイルおよびマルウェア イベント ロギングの無効化

ライセンス：Protection または Malware

アクセス コントロール ルールで暗号化されていないまたは復号化されたトラフィックを許可すると、関連付けられたファイル ポリシーを使用して、送信されたファイルを検査し、そのトラフィックが宛先に到達する前に禁止されたファイルおよびマルウェアをブロックできます。侵入防御パフォーマンスの調整 （177 ページ）を参照してください。

システムは禁止されたファイルを検出すると、次のタイプのイベントの 1 つを ASA FirePOWER モジュールに自動的にロギングします。

- ファイル イベント：検出またはブロックされたファイル（マルウェア ファイルを含む）を表します。
- マルウェア イベント：検出またはブロックされたマルウェア ファイルのみを表します。
- レトロスペクティブ マルウェア イベント：以前に検出されたファイルに関するマルウェアの性質が変化した場合に生成されます。

ファイル イベントまたはマルウェア イベントをロギングしない場合は、アクセス コントロール ルール エディタの [Logging] タブの [Log Files] チェックボックスをオフにすることで、アクセス コントロール ルールごとにロギングを無効にできます。

（注） Cisco では、ファイル イベントおよびマルウェア イベントのロギングを有効のままにすることを推奨しています。

ファイル イベントおよびマルウェア イベントを保存するかどうかに関係なく、ネットワーク トラフィックがファイル ポリシーに違反すると、呼び出し元のアクセス コントロール ルールのロギング設定に関係なく、システムは関連付けられた接続の終了を ASA FirePOWER モジュールに自動的にロギングします。ファイル イベントとマルウェア イベントに関連付けられた接続（自動） （469 ページ）を参照してください。

接続ロギングのライセンス要件

ライセンス：機能に応じて異なる

アクセス コントロール ポリシーおよび SSL ポリシーで接続ロギングを設定する前に、これらのポリシーが正常に処理できる任意の接続をロギングできます。

アクセス コントロール ポリシーおよび SSL ポリシーは、 ASA FirePOWER モジュールのどのライセンスでも作成できますが、アクセス コントロールの一部の操作を行うには、ポリシーを適用する前に、特定のライセンス機能を有効にする必要があります。

次の表では、アクセス コントロールを正常に設定し、アクセス コントロール ポリシーによって処理される接続をロギングするために必要なライセンスについて説明します。

表 *70*：アクセス コントロール ポリシーにおける接続ロギングのライセンス要件

次の接続をロギングするには	ライセンス
ネットワーク、ポート、またはリテラル URL 基準を使用して処理されるトラフィック用	任意
位置情報データを使用して処理されるトラフィック用	任意
関連付ける対象 • レピュテーションが低い IP アドレス（セキュリティ インテリジェンスのフィルタリング） • 暗号化されていないまたは復号化されたトラフィックの侵入または禁止されたファイル	Protection
暗号化されていないまたは復号化されたトラフィックで検出されたマルウェアに関連付けられる	Malware
ユーザ制御またはアプリケーション制御によって処理されるトラフィック用	Control
URL カテゴリおよびレピュテーションデータを使用してシステムがフィルタリングするトラフィック用、およびモニタ対象ホストによって要求される URL の URL カテゴリおよび URL レピュテーション情報を表示するため	URL Filtering

セキュリティ インテリジェンスによる判断のロギング

ライセンス：Protection

悪意のあるインターネットコンテンツに対する第一の防衛ラインとして、ASA FirePOWER モジュールにはセキュリティインテリジェンス機能があります。この機能により、最新のレピュテーションインテリジェンスに基づいて接続を直ちにブロックすることができ、リソースを集中的に使用する詳細な分析が不要になります。このトラフィック フィルタリングは、他のどのポリシーベースのインスペクション、分析、またはトラフィック処理よりも前に行われます。

オプションで、セキュリティ インテリジェンス フィルタリングにはモニタ専用設定を使用できます。パッシブ展開環境では、この設定が推奨されます。この設定では、ブロックされるはずの接続をシステムがさらに分析できるだけでなく、一致する接続をログに記録することもできます。

セキュリティ インテリジェンスのロギングを有効にすると、アクセス コントロール ポリシーによって処理されるすべてのブロックされた接続およびモニタされた接続がロギングされます。ただし、システムはブロックなしリストの一致はログに記録しません。これらの接続のロギングは、その接続の最終的な傾向によって異なります。

セキュリティインテリジェンスのフィルタリングの結果、システムが接続イベントをロギングすると、一致するセキュリティ インテリジェンス イベントもロギングされます。そのイベン

トは特殊なタイプの接続イベントで、個別に表示および分析できます。どちらのタイプのイベントも、[Action] フィールドと [Reason] フィールドを使用して、ブロックリストの一致を反映します。さらに、接続でブロックされた IP アドレスを特定できるように、イベントビューアではブロックされた IP アドレスとモニタされた IP アドレスの横にあるアイコンの表示は若干異なっています。

ブロックされた接続のロギング

ブロックされた接続の場合、システムは接続開始セキュリティ インテリジェンス イベントと接続イベントをロギングします。ブロックされたトラフィックは追加のインスペクションなしですぐに拒否されるため、ログに記録できる固有の接続終了イベントはありません。これらのイベントの場合、アクションは Block で、理由は IP Block です。

IP Block 接続イベントのしきい値は、開始側と応答側の固有のペアあたり 15 秒です。つまり、システムは接続をブロックしてイベントを生成した時点から 15 秒の間、この 2 つのホスト間で接続がブロックされたとしても、ポートやプロトコルの違いに関わらず、別の接続イベントを生成しません。

モニタされた接続のロギング

セキュリティインテリジェンスによって（ブロックされるのではなく）モニタされた接続の場合、システムは接続終了セキュリティ インテリジェンス イベントと接続イベントを、ASA FirePOWER モジュールにロギングします。このロギングは、接続が後で SSL ポリシー、アクセス コントロール ルール、またはアクセス コントロールのデフォルト アクションによってどのように処理されるかにかかわらず発生します。

これらの接続イベントの場合、アクションは接続の最終的な傾向によって異なります。[Reason] フィールドには、IP Monitor と、接続がロギングされている可能性がある他の理由が含まれています。

ただし、モニタされる接続の場合、以降に接続を処理するアクセス コントロール ルールやデフォルトアクションでのロギング設定によっては、接続開始イベントが生成されることもあります。

ブロックされた接続をログに記録する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。

[Access Control Policy] ページが表示されます。

ステップ 2 設定するアクセス コントロール ポリシーの横にある編集アイコンをクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3 [Security Intelligence] タブを選択します。

アクセス コントロール ポリシーのセキュリティ インテリジェンス設定が表示されます。

ステップ 4 ロギング アイコンをクリックします。

[Block Options] ポップアップウィンドウが表示されます。

ステップ 5 [Log Connections] チェックボックスをオンにします。

ステップ 6 接続イベントとセキュリティ インテリジェンス イベントの送信先を指定します。次の選択肢があります。

- ASA FirePOWER モジュールにイベントを送信するには、[Event Viewer] を選択します。
- イベントを外部 syslog サーバに送信するには、[Syslog] を選択して、ドロップダウンリストから syslog アラート応答を選択します。必要に応じて、追加アイコンをクリックして syslog アラート応答を追加することもできます（Syslog アラート応答の作成 （506 ページ）を参照）。
- 接続イベントを SNMP トラップ サーバに送信する場合は、[SNMP Trap] を選択し、ドロップダウン リストから SNMP アラート応答を選択します。必要に応じて、追加アイコンをクリックして SNMP アラート応答を追加することもできます（SNMP アラート応答の作成 （504 ページ）を参照）。

ブロックされたオブジェクトをモニタのみに設定する場合、またはセキュリティ インテリジェンス フィルタリングによって生成された接続イベントで他の ASA FirePOWER モジュール ベースの分析を行う場合は、イベントをイベント ビューアに送信する必要があります。詳細については、ASA FirePOWER モジュールまたは外部サーバへの接続のロギング （471 ページ）を参照してください。

ステップ 7 [OK] をクリックしてロギング オプションを設定します。

[Security Intelligence] タブが再表示されます。

ステップ 8 [Store ASA FirePOWER Changes] をクリックします。

変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（設定変更の導入 （92 ページ）を参照してください）。

アクセス コントロールの処理に基づく接続のロギング

ライセンス：任意

アクセス コントロール ポリシー内で、アクセス コントロール ルールはネットワーク トラフィックを処理する詳細な方法を提供しています。クリティカルな接続のみをロギングできるように、アクセス コントロール ルールごとに接続ロギングを有効にします。あるルールに対して接続ロギングを有効にすると、システムはそのルールによって処理されるすべての接続をロギングします。

アクセス コントロール ポリシーのデフォルト アクションによって処理されるトラフィックの接続をログに記録することもできます。デフォルト アクションによって、システムがポリシー内のアクセス コントロール ルールのいずれにも一致しないトラフィックを処理する方法が決まります（トラフィックに一致しロギングするが、処理または検査はしないモニタ ルールを除く）。

すべてのアクセス コントロール ルールおよびデフォルト アクションのロギングを無効にしても、接続がアクセス コントロール ルールに一致し、侵入の試み、禁止されたファイル、またはマルウェアが含まれている場合、またはシステムによって復号化され、SSL ポリシーで接続

のロギングを有効にした場合は、接続終了イベントは引き続き ASA FirePOWER モジュールにロギングされる場合があることに注意してください。

ルールまたはデフォルトのポリシー アクション、および設定した関連するインスペクション オプションによって、ロギング オプションは異なります。

アクセス コントロール ルールに一致する接続のロギング

ライセンス：任意

クリティカルな接続のみをロギングするには、アクセス コントロール ルールごとに接続ロギングを有効にします。あるルールに対しロギングを有効にすると、システムはそのルールによって処理されたすべての接続をロギングします。

ルール アクションおよびそのルールの侵入およびファイルのインスペクション設定によって、ロギング オプションは異なります。アクセス コントロールおよび SSL ルール アクションがどのようにロギングに影響を及ぼすかについて（471 ページ）を参照してください。また、アクセス コントロール ルールに対してロギングを無効にしても、接続が以下に当てはまる場合は、そのルールに一致する接続の接続終了イベントは引き続き ASA FirePOWER モジュールにロギングされる場合があることに注意してください。

- 侵入の試み、禁止されたファイル、またはマルウェアが含まれている場合
- 以前に少なくとも 1 つのアクセス コントロールのモニタ ルールに一致した場合

接続、ファイル、およびマルウェア情報をログに記録するアクセス コントロール ルールを設定する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] の順に選択します。

[Access Control Policy] ページが表示されます。

ステップ 2 変更するアクセス コントロール ポリシーの横にある編集アイコンをクリックします。

アクセス コントロール ポリシー エディタが表示され、[Rules] タブに焦点が置かれています。

ステップ 3 ロギングを設定するルールの横にある編集アイコンをクリックします。

アクセス コントロール ルール エディタが表示されます。

ステップ 4 [Logging] タブを選択します。

[Logging] タブが表示されます。

ステップ 5 [Log at Beginning and End of Connection]、[Log at End of Connection] を選択して、接続の開始時と終了時または終了時のみにログに記録することを指定するか、または [No Logging at Connection] を選択して、接続時にはログに記録しないことを指定します。

単一のブロックされていない接続の場合、接続終了イベントには、接続開始イベントに含まれるすべての情報に加えて、セッション期間中に収集された情報も含まれます。ブロックされたトラフィックは追加の検査なしで即座に拒否されるので、ブロック ルールについては接続開始イベントだけがログに記録されま

す。このため、ルール アクションを [Block] または [Block with reset] に設定すると、**接続の開始時点でロギングを行う**よう指示するプロンプトが表示されます。

ステップ 6 接続に関連しているファイルイベントとマルウェアイベントをすべてログに記録するかどうか指定するには、[Log Files] チェック ボックスを使用します。

ユーザがファイル ポリシーをルールに関連付けてファイル制御または AMP を実行すると、システムはこのオプションを自動的に有効にします。シスコでは、このオプションを有効のままにすることを推奨しています。許可された接続のファイルおよびマルウェア イベント ロギングの無効化 （473 ページ）を参照してください。

ステップ 7 接続イベントの送信先を指定します。次の選択肢があります。

- ASA FirePOWER モジュールに接続イベントを送信するには、[Event Viewer] を選択します。このオプションは、モニタ ルールに対して無効にできません。
- イベントを外部 syslog サーバに送信するには、[Syslog] を選択して、ドロップダウンリストから syslog アラート応答を選択します。必要に応じて、追加アイコンをクリックして syslog アラート応答を追加することもできます（Syslog アラート応答の作成 （506 ページ）を参照）。
- イベントを SNMP トラップ サーバに送信するには、[SNMP Trap]を選択し、ドロップダウンリストから SNMP アラート応答を選択します。必要に応じて、追加アイコンをクリックして SNMP アラート応答を追加することもできます（SNMP アラート応答の作成 （504 ページ）を参照）。

接続イベントで ASA FirePOWER モジュール ベースの分析を実行する場合は、イベントをイベント ビューアに送信する必要があります。詳細については、ASA FirePOWER モジュールまたは外部サーバへの接続のロギング （471 ページ）を参照してください。

ステップ 8 [Store ASA FirePOWER Changes] をクリックしてルールを保存します。

ルールが保存されます。変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（設定変更の導入 （92 ページ）を参照してください）。

アクセス コントロールのデフォルト アクションによって処理される接続のロギング

ライセンス：任意

アクセス コントロール ポリシーのデフォルト アクションによって処理されるトラフィックの接続をログに記録することができます。デフォルトアクションは、ポリシー内のどのアクセス コントロール ルール（トラフィックの照合とロギングは行うが、処理または検査はしないモニタ ルールを除く）にも一致しないトラフィックをシステムがどのように処理するかを決定します。デフォルトの処理の設定およびネットワーク トラフィックのインスペクション （83 ページ） を参照してください。

ポリシーのデフォルトアクションによって処理された接続のメカニズムとオプションは、次の表で示すように、個々のアクセス コントロール ルールによって処理された接続のロギング オ

プションとほとんど同じです。つまり、ブロックされたトラフィックを除き、システムは接続の開始と終了をログに記録し、接続イベントを ASA FirePOWER モジュール、または外部の syslog や SNMP トラップ サーバに送信できます。

表 *71*：アクセス コントロールのデフォルト アクションのロギング オプション

デフォルト アクション	比較対象	参照先
Access Control: Block All Traffic	ブロック ルール	ブロックされた接続およびインタラクティブにブロックされた接続のロギングについて （472 ページ）
Access Control: Trust All Traffic	信頼ルール	信頼されている接続のロギングについて （472 ページ）
Intrusion Prevention	関連付けられた侵入ポリシーを持つ許可ルール	許可された接続のロギングについて （473 ページ）

しかし、アクセス コントロール ルールによって処理された接続のロギングとデフォルト アクションによって処理された接続のロギングにはいくつかの違いがあります。

- デフォルト アクションにはファイル ロギング オプションはありません。デフォルト アクションを使用して、ファイル制御または AMP を実行することはできません。
- アクセス コントロールのデフォルト アクションに関連付けられた侵入ポリシーによって侵入イベントが生成された場合、システムは、そのイベントに関連する接続の終了を自動的にログに記録**しません**。このことは、接続データをログに記録する必要がない、侵入検知および侵入防御専用の展開環境に役立ちます。

ただし、デフォルトアクションに対して接続開始および接続終了ロギングを有効にした場合は例外です。この場合、関連付けられた侵入ポリシーがトリガーされると、システムは接続の開始だけでなく、接続の終了もログに記録します。

デフォルトアクションに対してロギングを無効にしても、接続が以前に少なくとも 1 つのアクセス コントロールのモニタ ルールに一致した場合、または SSL ポリシーによって検査およびロギングされた場合は、そのルールに一致する接続の接続終了イベントは引き続き ASA FirePOWER モジュールにロギングされる場合があることに注意してください。

アクセス コントロールのデフォルト アクションによって処理されたトラフィックの接続をログに記録するには、次の手順を実行します。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。

[Access Control Policy] ページが表示されます。

ステップ 2 変更するアクセス コントロール ポリシーの横にある編集アイコンをクリックします。

アクセス コントロール ポリシー エディタが表示され、[Rules] タブに焦点が置かれています。

ステップ 3 [Default Action] ドロップダウンリストの横にあるロギング アイコンをクリックします。

[Logging] ポップアップ ウィンドウが表示されます。

ステップ 4 [Log at Beginning and End of Connection]、[Log at End of Connection] を選択して、接続の開始時と終了時または終了時のみにログに記録することを指定するか、または [No Logging at Connection] を選択して、接続時にはログに記録しないことを指定します。

単一のブロックされていない接続の場合、接続終了イベントには、接続開始イベントに含まれるすべての情報に加えて、セッション期間中に収集された情報も含まれます。ブロックされたトラフィックは追加のインスペクションなしで即座に拒否されるので、システムは [Block All Traffic] デフォルト アクションの接続開始イベントのみをログに記録します。このため、デフォルト アクションを [Access Control: Block All Traffic] に設定すると、**接続の開始時点でロギングを行う**よう指示するプロンプトが表示されます。

ステップ 5 接続イベントの送信先を指定します。次の選択肢があります。

- ASA FirePOWER モジュールに接続イベントを送信するには、[Event Viewer] を選択します。このオプションは、モニタ ルールに対して無効にできません。
- イベントを外部 syslog サーバに送信するには、[Syslog] を選択して、ドロップダウンリストから syslog アラート応答を選択します。必要に応じて、追加アイコンをクリックして syslog アラート応答を追加することもできます（Syslog アラート応答の作成 （506 ページ）を参照）。
- イベントを SNMP トラップ サーバに送信するには、[SNMP Trap]を選択し、ドロップダウンリストから SNMP アラート応答を選択します。必要に応じて、追加アイコンをクリックして SNMP アラート応答を追加することもできます（SNMP アラート応答の作成 （504 ページ）を参照）。

接続イベントで ASA FirePOWER モジュール ベースの分析を実行する場合は、イベントをイベント ビューアに送信する必要があります。詳細については、ASA FirePOWER モジュールまたは外部サーバへの接続のロギング （471 ページ）を参照してください。

ステップ 6 [Store ASA FirePOWER Changes] をクリックしてポリシーを保存します。

ポリシーが保存されます。変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（設定変更の導入 （92 ページ）を参照してください）。

接続で検出された URL のロギング

ライセンス：任意

HTTP トラフィックで、接続終了イベントを ASA FirePOWER モジュールにロギングすると、システムはセッション中にモニタ対象ホストにより要求された URL を記録します。

デフォルトでは、システムは URL の最初の 1024 文字を接続ログに保管します。しかし、モニタ対象のホストが要求する完全な URL が取り込まれるように、URL ごとに最大 4096 文字を保管するようにシステムを設定することができます。または、アクセスされた個々の URL を知る必要がない場合は、保管する文字数をゼロに設定して、URL の保管を無効にすることもできます。ネットワーク トラフィックによっては、URL の保管を無効にするか、あるいは保管する URL の文字数を制限すると、システム パフォーマンスが向上する可能性があります。

URL のロギングを無効にしても、URL フィルタリングには影響しないことに注意してください。アクセス コントロール ルールにより、要求された URL、そのカテゴリ、およびレピュテーションに基づいて、トラフィックが適切にフィルタリングされます。システムが、これらのルールによって処理されたトラフィックで要求された個々の URL を記録しないだけです。詳細については、URL のブロッキング （147 ページ）を参照してください。

保存する URL の文字数をカスタマイズするには、次の手順を実行します。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Access Control Policy] の順に選択します。

[Access Control Policy] ページが表示されます。

ステップ 2 設定するアクセス コントロール ポリシーの横にある編集アイコンをクリックします。

アクセス コントロール ポリシー エディタが表示されます。

ステップ 3 [Advanced] タブを選択します。

アクセス コントロール ポリシーの詳細設定が表示されます。

ステップ 4 [General Settings] の横にある編集アイコンをクリックします。

[General Settings] ポップアップ ウィンドウが表示されます。

ステップ 5 **接続イベントで保存する URL の最大文字数**を入力します。

1 ～ 4096 の値を指定できます。保管する文字数をゼロにすると、URL フィルタリングを無効にすることなく URL の保管が無効になります。

ステップ 6 [OK] をクリックします。

アクセス コントロール ポリシーの詳細設定が表示されます。

ステップ 7 [Store ASA FirePOWER Changes] をクリックしてポリシーを保存します。

ポリシーが保存されます。変更を反映させるには、アクセス コントロール ポリシーを適用する必要があります（設定変更の導入 （92 ページ）を参照してください）。

暗号化された接続のロギング

ライセンス：任意

アクセス コントロールの一部として、*SSL* インスペクション機能を使用することで、SSL ポリシーを使用してアクセス コントロール ルールによるさらなる評価のために暗号化されたトラフィックを復号化できます。システムがトラフィックを後でどのように処理または検査するかにかかわらず、これらの復号化された接続のログを記録するようにシステムに強制できます。また、暗号化されたトラフィックをブロックするとき、または復号化せずにトラフィックがア

クセス コントロール ルールに渡されることを許可するときに、接続をロギングすることもできます。

暗号化セッションの接続ログには、セッションの暗号化に使用される証明書など、暗号化の詳細が含まれます。クリティカルな接続のみをログに記録するように、SSL ポリシーの暗号化されたセッションの接続ロギングは SSL ルールごとに設定します。

SSL ルールを使用した復号可能接続のロギング

ライセンス：任意

SSL ポリシー内では、SSL ルールは複数の管理対象デバイス間で暗号化されたトラフィックを処理する詳細な方法を提供します。クリティカルな接続のみをロギングできるように、SSL ルールごとに接続ロギングを有効にします。あるルールに対して接続ロギングを有効にすると、システムはそのルールによって処理されるすべての接続をロギングします。

SSL ポリシーによって検査される暗号化された接続の場合、接続イベントのログは、外部の syslog や SNMP トラップ サーバに記録できます。ただし次の場合は、接続終了イベントだけをログに記録できます。

- ブロックされた接続（[Block]、[Block with reset]）の場合、システムは即座にセッションを終了し、イベントを生成します。
- モニタ対象の接続（[Monitor]）およびアクセス コントロール ルールに渡す接続（[Decrypt]、[Do not decrypt]）の場合、アクセス コントロール ルールまたはそのセッションを後で処理するデフォルト アクションのロギング設定に関係なく、システムはセッション終了時にイベントを生成します。

詳細については、アクセス コントロールおよび SSL ルール アクションがどのようにロギングに影響を及ぼすかについて （471 ページ）を参照してください。

復号化できる接続をログに記録するには、次の手順を実行します。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [SSL] の順に選択します。

[SSL Policy] ページが表示されます。

ステップ 2 ロギングを設定するルールの横にある編集アイコンをクリックします。

SSL ルール エディタが表示されます。

ステップ 3 [Logging] タブを選択します。

[Logging] タブが表示されます。

ステップ 4 [Log at End of Connection] を選択します。

ステップ 5 接続イベントの送信先を指定します。次の選択肢があります。

- イベントを外部の syslog に送信するには、[Syslog] を選択して、ドロップダウンリストから syslog アラート応答を選択します。必要に応じて、追加アイコンをクリックして syslog アラート応答を追加することもできます（Syslog アラート応答の作成 （506 ページ）を参照）。
- イベントを SNMP トラップ サーバに送信するには、[SNMP Trap]を選択し、ドロップダウンリストから SNMP アラート応答を選択します。必要に応じて、追加アイコンをクリックして SNMP アラート応答を追加することもできます（SNMP アラート応答の作成 （504 ページ）を参照）。

ステップ 6 [Add] をクリックして変更を保存します。

変更を反映させるには、SSL ポリシーが関連付けられているアクセス コントロール ポリシーを適用する必要があります。設定変更の導入 （92 ページ） を参照してください。

暗号化された接続および復号化できない接続のデフォルトのロギング設定

ライセンス：SSL

SSL ポリシーのデフォルト アクションによって処理されるトラフィックの接続をログに記録できます。これらのロギング設定では、システムが復号化できないセッションをどのようにログに記録するかも管理されます。

SSL ポリシーのデフォルト アクションは、ポリシー内のどの SSL ルール（トラフィックの照合とロギングは行うが、処理または検査はしないモニタ ルールを除く）にも一致しない暗号化されたトラフィックをシステムがどのように処理するかを決定します。SSL ポリシーに SSL ルールが含まれていない場合、デフォルト アクションは、ネットワーク上のすべての暗号化セッションがどのようにログに記録されるかを決定します。詳細については、暗号化トラフィックのデフォルトの処理と検査の設定 （226 ページ）を参照してください。

接続イベントを外部の syslog や SNMP トラップ サーバにロギングするように、SSL ポリシーのデフォルト アクションを設定できます。ただし次の場合は、接続終了イベントだけをログに記録できます。

- ブロックされた接続[Block with reset] の場合、システムは即座にセッションを終了してイベントを生成します。
- 暗号化されていない接続をアクセス コントロールに渡すことを許可する接続の場合（[Do not decrypt]）、システムはセッションの終了時にイベントを生成します。

SSL ポリシーのデフォルト アクションのロギングを無効にしても、接続が以前に少なくとも 1 つの SSL モニタ ルールに一致していた場合、または後でアクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルト アクションに一致する場合は、接続終了イベントが引き続きロギングされる可能性があることに注意してください。

暗号化されたトラフィックおよび復号化できないトラフィックのデフォルトの処理を設定するには、次の手順を実行します。

アクセス：管理者/アクセス管理者/ネットワーク管理者/セキュリティ承認者

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [SSL] の順に選択します。

[SSL Policy] ページが表示されます。

ステップ 2 [Default Action] ドロップダウンリストの横にあるロギング アイコンをクリックします。

[Logging] ポップアップ ウィンドウが表示されます。

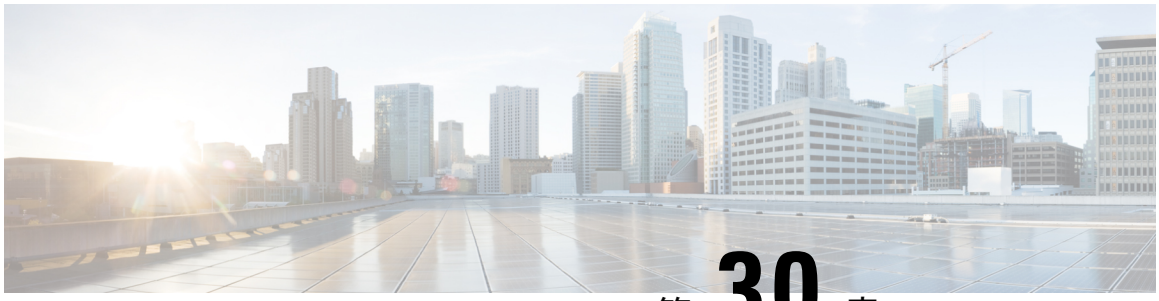
ステップ 3 [Log at End of Connection] を選択して、接続イベントのロギングを有効にします。

ステップ 4 接続イベントの送信先を指定します。次の選択肢があります。

- イベントを外部 syslog サーバに送信するには、[Syslog] を選択して、ドロップダウンリストから syslog アラート応答を選択します。必要に応じて、追加アイコンをクリックして syslog アラート応答を設定することもできます（Syslog アラート応答の作成 （506 ページ）を参照）。
- イベントを SNMP トラップ サーバに送信するには、[SNMP Trap]を選択し、ドロップダウンリストから SNMP アラート応答を選択します。必要に応じて、追加アイコンをクリックして SNMP アラート応答を設定することもできます（SNMP アラート応答の作成 （504 ページ）を参照）。

ステップ 5 [OK] をクリックして変更を保存します。

変更を反映させるには、SSL ポリシーが関連付けられているアクセス コントロール ポリシーを適用する必要があります。設定変更の導入 （92 ページ） を参照してください。



第 30 章

イベントの表示

ASA FirePOWER モジュールによって検査されたトラフィックに対してロギングされたリアルタイム イベントを表示できます。

（注） モジュールがメモリにキャッシュするのは直近の 100 個のイベントのみです。

ASA FirePOWER リアルタイム イベントへのアクセス

いくつかの定義済みイベント ビューで ASA FirePOWER モジュールによって検出されたイベントを表示できます。または、カスタム イベント ビューを作成して選択したイベント フィールドを表示することができます。

（注） モジュールがメモリにキャッシュするのは直近の 100 個のイベントのみです。

ASA FirePOWER イベントを表示するには、次の手順を実行します。

ステップ 1 [Monitoring] > [ASA FirePOWER Monitoring] > [Real-time Eventing] の順に選択します。

ステップ 2 次の 2 つの選択肢があります。

- 接続イベント、セキュリティ インテリジェンス イベント、侵入イベント、ファイル イベント、またはマルウェア イベントから表示するイベントのタイプの既存のタブをクリックします。
- カスタム イベント ビューを作成し、ビューに含めるイベント フィールドを選択するには [+] アイコンをクリックします。

詳細については、ASA FirePOWER イベント タイプについて （488 ページ）およびASA FirePOWER イベントのイベント フィールド （490 ページ）を参照してください。

ASA FirePOWER イベント タイプについて

ASA FirePOWER モジュールでは、5 つのイベント タイプ（接続イベント、セキュリティ インテリジェンス イベント、侵入イベント、ファイル イベント、およびマルウェア イベント）からのイベント フィールドを表示するリアルタイム イベント ビューが提供されます。

Connection Events

接続イベントと呼ばれる接続ログには、検出されたセッションに関するデータが含まれています。個々の接続イベントで入手可能な情報はいくつかの要因によって決まりますが、一般的には次のものがあります。

- タイムスタンプ、送信元と宛先の IP アドレス、入出力ゾーン、接続を処理したデバイスなど、基本的な接続特性
- アプリケーション、要求されるURL、または接続に関連付けられているユーザなど、システムによって検出または推測される追加の接続特性
- ポリシーがトラフィックを処理したアクセス コントロール ルール（または他の設定）、接続が許可またはブロックされているかどうかなど、接続がログに記録された理由に関するメタデータ

アクセスコントロールでさまざまな設定を行うことで、ログする接続の種類、接続をログする時期、およびデータを保存する場所のきめ細かい制御を行うことができます。アクセスコントロールポリシーが正常に処理できる接続をログに記録できます。接続のロギングは、次の状況で有効にできます。

- 接続がレピュテーションベースのセキュリティインテリジェンス機能によってブロックまたはモニタされる場合
- 接続がアクセス コントロール ルールまたはアクセス コントロールのデフォルト アクションによって処理された場合

設定するロギングに加えて、システムは禁止されたファイル、マルウェア、または侵入の試みを検出した場合に、ほとんどの接続を自動的にログに記録します。

Security Intelligence Events

セキュリティ インテリジェンス ロギングを有効にすると、ブロックリストの一致によってセキュリティ インテリジェンス イベントおよび接続イベントが自動的に生成されます。セキュリティ インテリジェンス イベントは特殊なタイプの接続イベントで、個別に表示および分析できます。セキュリティインテリジェンスによるブロックの決定を含む、接続ロギングの設定

の詳細については、ネットワーク トラフィックの接続のロギング（467ページ）を参照してください。

ヒント　特に明記されていない限り、接続イベントに関する一般情報もまたセキュリティ インテリジェンス イベントに関連します。セキュリティ インテリジェンスの詳細については、レピュテーションベースのルールによるトラフィックの制御 （139 ページ） を参照してください。

Intrusion Events

システムは、ホストとそのデータの可用性、整合性、および機密性に影響する可能性のある悪意のあるアクティビティについて、ネットワークを通過するパケットを検査します。システムは、潜在的な侵入を特定すると侵入イベントを生成します。これは、エクスプロイトの日付、時間、タイプ、および攻撃元とそのターゲットに関するコンテキスト情報の記録です。

File Events

ファイル イベントは、システムがネットワーク トラフィック内で検出した（さらにオプションでブロックした）ファイルを表します。

システムは、現在適用されているファイル ポリシーのルールに従って、管理対象デバイスがネットワーク トラフィック内のファイルを検出またはブロックしたときに生成されたファイル イベントを記録します。

Malware Events

マルウェア イベントは、システムがネットワーク トラフィック内で検出した（さらにオプションでブロックした）マルウェア ファイルを表します。

マルウェア ライセンスを使用すると、ASA FirePOWER モジュールは全体的なアクセス コントロール設定の一部として、ネットワーク トラフィック内のマルウェアを検出できます。ファイル ポリシーの概要と作成 （453 ページ） を参照してください。

以下のシナリオでは、マルウェア イベントが生成される可能性があります。

- 管理対象デバイスが一連の特定のファイル タイプのいずれかを検出すると、ASA FirePOWER モジュールはマルウェア クラウド ルックアップを実行します。これにより、ファイル性質として Malware、Clean、または Unknown が ASA FirePOWER モジュールに返されます。
- ASA FirePOWER モジュールがクラウドとの接続を確立できない場合や、その他の理由でクラウドが使用できない場合、ファイル性質は Unavailable になります。この性質で見られるイベントはごくわずかである可能性があります。これは予期された動作です。
- クリーン リストに含まれているファイルを管理対象デバイスが検出した場合、ASA FirePOWER モジュールはファイル性質として Clean をそのファイルに割り当てます。

ASA FirePOWER モジュールは他のコンテキスト データとともに、ファイルの検出と性質のレコードをマルウェア イベントとして記録します。

ネットワーク トラフィックで検出され、ASA FirePOWER モジュールによってマルウェアとして識別されたファイルは、ファイル イベントとマルウェア イベントの両方を生成します。これは、ファイル内のマルウェアを検出するために、システムはまずそのファイル自体を検出する必要があるためです。

ASA FirePOWER イベントのイベント フィールド

Action

接続イベントまたはセキュリティ インテリジェンス イベントの場合、接続をロギングしたアクセス コントロール ルールまたはデフォルト アクションに関連付けられたアクション。

- [許可（Allow）] は、明示的に許可されてユーザがバイパスする、インタラクティブにブロックされる接続を表します。
- [Trust] は、信頼できる接続を表します。最初のパケットが信頼ルールによって検出された TCP 接続のみ、接続終了イベントを生成します。システムは、最後のセッション パケットの 1 時間後にイベントを生成します。
- [Block] と [Block with reset] は、ブロックされた接続を表します。さらにシステムは、ブロックアクションを、セキュリティインテリジェンスによってブロックされた接続、侵入ポリシーによってエクスプロイトが検出された接続、およびファイルポリシーによってファイルがブロックされた接続にも関連付けます。
- [Interactive Block] と [Interactive Block with reset] は、システムが Interactive Block ルールを使用して最初にユーザの HTTP 要求をブロックしたときにロギングできる接続開始イベントを示します。システムが表示する警告ページでユーザがクリック操作をすると、そのセッションについてロギングするその他の接続イベントは、アクションが [Allow] になります。
- [Default Action] は、接続がデフォルト アクションによって処理されたことを示します。
- セキュリティ インテリジェンスによって監視されている接続の場合、そのアクションは、接続によってトリガーされる最初の監視以外のアクセス コントロール ルールのアクションか、デフォルト アクションです。同様に、モニタ ルールに一致するトラフィックは常に後続のルールまたはデフォルト アクションによって処理されるため、モニタ ルールによってロギングされた接続に関連付けられたアクションが [Monitor] になることはありません。

ファイル イベントまたはマルウェア イベントの場合、ファイルが一致したルールのルール アクションに関連付けられているファイル ルール アクションと、関連するファイル ルール アクションのオプション。

Allowed Connection

システムがイベントのトラフィック フローを許可したかどうか。

Application

接続で検出されたアプリケーション。

Application Business Relevance

接続で検出されたアプリケーショントラフィックに関連付けられたビジネスとの関連性：[Very High]、[High]、[Medium]、[Low]、[Very Low]。接続で検出されたアプリケーションのタイプごとに、関連するビジネス関連性があります。このフィールドでは、それらのうち最も低いもの（関連が最も低い）が表示されます。

Application Categories

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示すカテゴリ。

Application Risk

接続で検出されたアプリケーション トラフィックに関連付けられたリスク：[Very High]、[High]、[Medium]、[Low]、[Very Low]。接続で検出されたアプリケーションのタイプごとに、関連するリスクがあります。このフィールドでは、それらのうち最も高いものが表示されます。

Application Tag

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示すタグ。

Block Type

イベントのトラフィック フローと一致するアクセス コントロール ルールで指定されたブロックのタイプ。[Block] または [Interactive Block]。

Client

接続で検出されたクライアント アプリケーション。

接続に使用されている特定のクライアントをシステムが特定できない場合、このフィールドには汎用的な名称としてアプリケーションプロトコル名の後に client を付加した形で、FTP client などと表示されます。

Client Business Relevance

接続で検出されたクライアント トラフィックに関連付けられたビジネスとの関連性：[Very High]、[High]、[Medium]、[Low]、[Very Low]。接続で検出されたクライアントのタイプごとに、ビジネスとの関連性が関連付けられています。このフィールドは、最も低いもの（関連性が最も低い）を表示します。

Client Categories

クライアントの機能を理解するのに役立つ、トラフィックで検出されたクライアントの特性を示すカテゴリ。

Client Risk

接続で検出されたクライアント トラフィックに関連付けられたリスク：[Very High]、[High]、[Medium]、[Low]、[Very Low]。接続で検出されたクライアントのタイプごとに、リスクが関連付けられています。このフィールドは、最も高いものを表示します。

Client Tag

クライアントの機能を理解するのに役立つ、トラフィックで検出されたクライアントの特性を示すタグ。

Client Version

接続で検出されたクライアントのバージョン。

Connection

内部的に生成されたトラフィック フローの固有 ID。

Connection Blocktype Indicator

イベントのトラフィック フローと一致するアクセス コントロール ルールで指定されたブロックのタイプ。[Block] または [Interactive Block]。

Connection Bytes

接続の合計バイト数。

Connection Time

接続の開始時刻。

Connection Timestamp

接続が検出された時刻。

Context

トラフィックが通過したセキュリティ コンテキストを識別するメタデータ。マルチ コンテキスト モードのデバイスでは、システムはこのフィールドにのみ入力することに注意してください。

Denied Connection

システムがイベントのトラフィック フローを拒否したかどうか。

Destination Country and Continent

受信ホストの国および大陸。

Destination IP

受信ホストが使用する IP アドレス。

Destination Port, Destination Port Icode, Destination Port/ICMP Code

セッション レスポンダが使用する宛先ポートまたは ICMP コード。

Direction

ファイルの送信方向。

Disposition

以下のファイル性質のいずれかです。

- Malware：クラウドがマルウェアとしてファイルを分類したことを示します。
- Clean は、クラウドでそのファイルがクリーンとして分類されているか、ユーザがファイルをクリーン リストに追加したことを示します。
- Unknown は、クラウドが性質を割り当てる前にマルウェア クラウド ルックアップが行われたことを示します。ファイルは分類されていません。
- [Custom Detection] は、ファイルをユーザがカスタム検出リストに追加したことを示します。
- Unavailable：ASA FirePOWER モジュールがマルウェア クラウド ルックアップを実行できなかったことを示します。この性質で見られるイベントはごくわずかである可能性があります。これは予期された動作です。
- N/A：ファイル検出またはファイル ブロック ルールがファイルを処理し、ASA FirePOWER モジュールがマルウェア クラウド ルックアップを行わなかったことを示します。

Egress Interface

接続に関連付けられた出力インターフェイス。展開環境に非同期のルーティング設定が含まれている場合は、入力と出力のインターフェイスが同じインターフェイス セットに属する場合があることに注意してください。

Egress Security Zone

接続に関連付けられた出力セキュリティ ゾーン。

Event

イベントのタイプ。

Event Microseconds

イベントが検出された時刻（マイクロ秒単位）。

Event Seconds

イベントが検出された時刻（秒単位）。

Event Type

イベントのタイプ。

File Category

ファイルタイプの一般的なカテゴリ（Office ドキュメント、アーカイブ、マルチメディア、実行可能ファイル、PDF ファイル、エンコード ファイル、グラフィック、システム ファイルなど）。

File Event Timestamp

ファイルまたはマルウェア ファイルが作成された日時。

File Name

ファイルまたはマルウェア ファイルの名前。

File SHA256

ファイルの SHA-256 ハッシュ値。

File Size

ファイルまたはマルウェア ファイルのサイズ（KB 単位）。

File Type

ファイルまたはマルウェア ファイルのファイル タイプ（HTMLや MSEXE など）。

File/Malware Policy

イベントの生成に関連付けられているファイル ポリシー。

Filelog Blocktype Indicator

イベントのトラフィック フローと一致するファイル ルールで指定されたブロックのタイプ。[Block] または [Interactive Block]。

Firewall Policy Rules/SI Category

接続でブロックされた IP アドレスを表すか、またはそれを含むオブジェクトの名前。セキュリティ インテリジェンスのカテゴリは、ネットワークオブジェクトまたはグループ、グローバルブロックリスト、カスタム セキュリティ インテリジェンスのリストまたはフィード、あるいはインテリジェンスフィードのカテゴリのいずれかの名前にできます。[Reason] が [IP Block] または [IP Monitor] の場合にのみ、このフィールドに値が入力されることに注意してください。セキュリティ インテリジェンスイベントのビューでは、エントリに必ず原因が表示されます。

Firewall Rule

接続を処理したアクセス コントロール ルールまたはデフォルト アクションと、その接続に一致した最大 8 つの Monitor ルール。

First Packet

セッションの最初のパケットが検出された日時。

HTTP Referrer

接続で検出された HTTP トラフィックの要求 URL の参照元を示す HTTP 参照元（他の URL へのリンクを提供した Web サイト、他の URL からリンクをインポートした Web サイトなど）。

IDS Classification

イベントを生成したルールが属する分類。ルールの分類名と番号のリストについては、表 72 : ルールの分類 （501 ページ）の表を参照してください。

Impact

このフィールドの影響レベルは、侵入データ、ネットワーク検出データ、脆弱性情報との関係を示します。

Impact Flag

「Impact」を参照してください。

Ingress Interface

接続に関連付けられた入力インターフェイス。展開環境に非同期のルーティング設定が含まれている場合は、入力と出力のインターフェイスが同じインターフェイス セットに属する場合があることに注意してください。

Ingress Security Zone

接続に関連付けられた入力セキュリティ ゾーン。

Initiator Bytes

セッション イニシエータが送信した合計バイト数。

Initiator Country and Continent

ルーティング可能な IP が検出された場合の、セッションを開始したホスト IP アドレスに関連付けられた国および大陸。

Initiator IP

セッション レスポンダを開始したホスト IP アドレス（および DNS 解決が有効化されている場合はホスト名）。

Initiator Packets

セッション イニシエータが送信した合計パケット数。

Inline Result

次のいずれかが必要です。

- 黒い下矢印。ルールをトリガーとして使用したパケットをシステムがドロップしたことを示します
- 灰色の下矢印。[Drop when Inline] ポリシー オプション（インライン展開環境）を有効にした場合、またはシステムがプルーニングしている間に [Drop and Generate] ルールがイベントを生成した場合、IPS がパケットをドロップしたことを示します
- ブランク。トリガーとして使用されたルールが [Drop and Generate Events] に設定されてないことを示します
- 侵入ポリシーのルールの状態またはインライン ドロップ動作にかかわらず、インライン インターフェイスがタップ モードになっている場合を含め、パッシブ展開環境ではシステムはパケットをドロップしないことに注意してください。

IPS Blocktype Indicator

イベントのトラフィック フローと一致する侵入ルールのアクション。

Last Packet

セッションの最後のパケットが検出された日時。

MPLS Label

この侵入イベントをトリガーしたパケットと関連付けられているマルチプロトコル ラベル スイッチング ラベル。

Malware Blocktype Indicator

イベントのトラフィック フローと一致するファイル ルールで指定されたブロックのタイプ。[Block] または [Interactive Block]。

Message

イベントを説明するテキスト。

ルールベースの侵入イベントの場合、イベント メッセージはルールから取得されます。デコーダベースおよびプリプロセッサベースのイベントの場合は、イベント メッセージはハードコーディングされています。

マルウェア イベントの場合は、マルウェア イベントに関連付けられている追加情報。ネットワークベースのマルウェア イベントの場合、このフィールドにデータが入れられるのは、性質が変更されたファイルだけです。

Monitor Rules

その接続で一致する 8 つまでのモニタ ルール。

Netbios Domain

セッションで使用された NetBIOS ドメイン。

Num Ioc

侵入イベントをトリガーとして使用したトラフィックが、接続に関係するホストに対する侵入の痕跡（IOC）もトリガーとして使用したかどうか。

Original Client Country and Continent

元のクライアントの IP アドレスが属する国。この値を取得するために、システムは元のクライアント IP アドレスを X-Forwarded-For（XFF）、True-Client-IP、またはカスタム定義の HTTP ヘッダーから抽出し、それを地理位置情報データベース（GeoDB）を使用して国にマップします。このフィールドに入力するには、元のクライアントに基づいてプロキシ トラフィックを処理するアクセス コントロール ルールを有効にする必要があります。

Original Client IP

X-Forwarded-For（XFF）、True-Client-IP、またはカスタム定義の HTTP ヘッダーからの、元のクライアント IP アドレス。このフィールドに入力するには、元のクライアントに基づいてプロキシ トラフィックを処理するアクセス コントロール ルールを有効にする必要があります。

Policy

イベントの生成に関連付けられているアクセス コントロール ポリシー、侵入ポリシー、またはネットワーク分析ポリシー（NAP）（ある場合）。

Policy Revision

イベントの生成に関連付けられているアクセス コントロール ポリシー、侵入ポリシー、またはネットワーク分析ポリシー（NAP）（ある場合）のリビジョン。

Priority

Cisco VRT で指定されたイベントの優先順位。

Protocol

接続で検出されたプロトコル。

Reason

次の場合に接続がロギングされた 1 つまたは複数の原因。

- [User Bypass] は、システムが最初はユーザの HTTP 要求をブロックしたが、ユーザが警告ページでクリック操作をして、最初に要求していたサイトへ進むことを選択したことを示します。[User Bypass] の原因は必ず [Allow] のアクションとペアになります。

- [IP Block] は、システムがセキュリティ インテリジェンス データに基づいて、インスペクションなしで接続を拒否したことを示します。[IP Block] の原因は必ず [Block] のアクションとペアになります。
- [IP Monitor] は、システムがセキュリティ インテリジェンス データに基づいて接続を拒否するはずでしたが、ユーザが接続を拒否せず監視するように設定したことを示します。
- [File Monitor] は、システムが接続において特定のファイルの種類を検出したことを示します。
- [File Block] は、ファイルまたはマルウェア ファイルが接続に含まれており、システムがその送信を防いだことを示します。[File Block] の原因は必ず [Block] のアクションとペアになります。
- [File Custom Detection] は、カスタム検出リストにあるファイルが接続に含まれており、システムがその送信を防いだことを示します。
- [File Resume Allow] は、ファイル送信がはじめにファイル ブロックまたはマルウェア ブロック ファイル ルールによってブロックされたことを示します。そのファイルを許可する新しいアクセス コントロール ポリシーが適用された後で、HTTP セッションは自動的に再開しました。この原因は、インライン構成のみで表示されることに注意してください。
- [File Resume Block] は、ファイル送信がはじめにファイル検出または マルウェア クラウド ルックアップ ファイル ルールによって許可されたことを示します。そのファイルをブロックする新しいアクセス コントロール ポリシーが適用された後で、HTTP セッションは自動的に停止しました。この原因は、インライン構成のみで表示されることに注意してください。
- [Intrusion Block] は、接続で検出されたエクスプロイト（侵入ポリシー違反）をシステムがブロックしたか、ブロックするはずだったことを示します。[侵入ブロック（Intrusion Block）] の理由は、ブロックされたエクスプロイトの場合は [ブロック（Block）]、ブロックされるはずだったエクスプロイトの場合は [許可（Allow）] のアクションと対として組み合わされます。
- [Intrusion Monitor] は、接続で検出されたエクスプロイトをシステムが検出したものの、ブロックしなかったことを示します。これは、トリガーされた侵入ルールの状態が [Generate Events] に設定されている場合に発生します。
- コンテンツ制限は、セーフサーチまたは YouTube EDU 機能のいずれかに関連したコンテンツ制限を実施するために、システムがパケットを変更したことを示します。

Receive Times

宛先ホストまたはレスポンダがイベントに応答した時刻。

Referenced Host

接続のプロトコルが DNS、HTTP、または HTTPS の場合、このフィールドにはそれぞれのプロトコルが使用していたホスト名が表示されます。

Responder Bytes

セッション レスポンダが送信した合計バイト数。

Responder Country and Continent

ルーティング可能な IP が検出された場合の、セッション レスポンダのホスト IP アドレスに関連付けられた国および大陸。

Responder Packets

セッション レスポンダが送信した合計パケット数。

Responder IP

セッション イニシエータに応答したホスト IP アドレス（および DNS 解決が有効化されている場合はホスト名）。

Security Group Tag Name

接続に関係するパケットのセキュリティ グループ タグ（SGT）属性。SGT は、信頼ネットワーク内での、トラフィックの送信元の権限を指定します。セキュリティ グループ アクセス（Cisco TrustSec と Cisco ISE の両方に共通の機能）は、パケットがネットワークに入るときに属性を適用します。

Signature

イベントのトラフィックと一致する侵入ルールのシグネチャ ID。

Source Country and Continent

送信元ホストの国および大陸。

Source IP

侵入イベントで送信元ホストが使用する IP アドレス。

Source or Destination

イベントの接続を送信元/宛先とするホスト。

Source Port, Source Port Type, Source Port/ICMP Type

セッション イニシエータが使用する送信元ポートまたは ICMP タイプ。

TCP Flags

接続で検出された TCP フラグ。

URL

セッション中に監視対象のホストによって要求された URL。

URL Category

セッション中に監視対象のホストによって要求されたURLに関連付けられているカテゴリ（使用可能な場合）。

URL Reputation

セッション中に監視対象のホストによって要求された URL に関連付けられているレピュテーション（使用可能な場合）。

URL Reputation Score

セッション中に監視対象のホストによって要求された URL に関連付けられているレピュテーション スコア（使用可能な場合）。

User

イベントが発生したホスト（**受信 IP**）のユーザ

User Agent

接続で検出された HTTP トラフィックから取得したユーザ エージェント アプリケーションの情報。

VLAN

イベントをトリガーしたパケットに関連付けられている最内部 VLAN ID。

Web App Business Relevance

接続で検出された Web アプリケーション トラフィックに関連付けられているビジネスとの関連性：[Very High]、[High]、[Medium]、[Low]、[Very Low]。接続で検出された Web アプリケーションのタイプごとに、ビジネスとの関連性が関連付けられています。このフィールドは、最も低いもの（関連性が最も低い）を表示します。

Web App Categories

Web アプリケーションの機能を理解するのに役立つ、トラフィックで検出された Web アプリケーションの特性を示すカテゴリ。

Web App Risk

接続で検出されたWebアプリケーション トラフィックに関連付けられたリスク：[Very High]、[High]、[Medium]、[Low]、[Very Low]。接続で検出された Web アプリケーションのタイプごとに、リスクが関連付けられています。このフィールドは、最も高いものを表示します。

Web App Tag

Web アプリケーションの機能を理解するのに役立つ、トラフィックで検出された Web アプリケーションの特性を示すタグ。

Web Application

トラフィックで検出された Web アプリケーション。

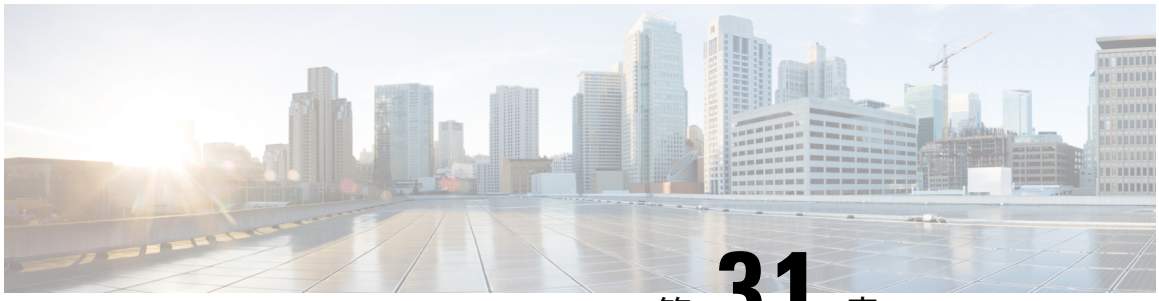
侵入ルールの分類

侵入ルールには、攻撃の分類が含まれています。次の表に、それぞれの分類の名前と番号を示します。

表 *72 :* ルールの分類

番号	分類名	説明
1	not-suspicious	不審ではないトラフィック
2	unknown	不明なトラフィック
3	bad-unknown	有害な可能性のあるトラフィック
4	attempted-recon	情報漏えいが試行された
5	successful-recon-limited	情報漏えいが発生
6	successful-recon-largescale	大規模な情報漏えい
7	attempted-dos	サービス拒否が試行された
8	successful-dos	サービス拒否が発生
9	attempted-user	ユーザ特権の獲得が試行された
10	unsuccessful-user	ユーザ特権の獲得が失敗した
11	successful-user	ユーザ特権の獲得に成功
12	attempted-admin	管理者特権の獲得が試行された
13	successful-admin	管理者特権の獲得に成功
14	rpc-portmap-decode	RPC クエリのデコード
15	shellcode-detect	実行可能コードが検出された
16	string-detect	疑わしい文字列が検出された
17	suspicious-filename-detect	疑わしいファイル名が検出された
18	suspicious-login	疑わしいユーザ名を使用したログイン試行が検出された
19	system-call-detect	システム コールが検出された

番号	分類名	説明
20	tcp-connection	TCP 接続が検出された
21	trojan-activity	ネットワーク トロイの木馬が検出された
22	unusual-client-port-connection	通常とは異なるポートをクライアントが使用していた
23	network-scan	ネットワーク スキャンの検出
24	denial-of-service	サービス拒否攻撃の検出
25	non-standard-protocol	標準的でないプロトコルまたはイベントの検出
26	protocol-command-decode	一般的なプロトコル コマンド デコード
27	web-application-activity	脆弱な可能性のある Web アプリケーションへのアクセス
28	web-application-attack	Web アプリケーション攻撃
29	misc-activity	その他のアクティビティ
30	misc-attack	その他の攻撃
31	icmp-event	一般的な ICMP イベント
32	inappropriate-content	不適切な内容が検出された
33	policy-violation	企業プライバシー侵害の可能性
34	default-login-attempt	デフォルトのユーザ名とパスワードによるログイン試行
35	sdf	機密データ
36	malware-cnc	既知のマルウェア コマンドと制御トラフィック
37	client-side-exploit	既知のクライアント側 exploit 試行
38	file-format	既知の有害ファイルまたはファイル ベースの exploit



第 31 章

外部アラートの設定

ASA FirePOWER モジュールではイベントのさまざまなビューをモジュール インターフェイス内で提供されますが、重要なシステムの継続的なモニタリングを容易にするために外部イベント通知を設定することもできます。次のいずれかが生成されたときに、SNMP トラップの使用または syslog への書き込みによって通知するアラートを生成するようにモジュールを設定できます。

- ネットワークベースのマルウェア イベントまたはレトロスペクティブ マルウェア イベント
- 特定のアクセス コントロール ルールによってトリガーされる接続イベント

ASA FirePOWER モジュールでこれらのアラートが送信されるようにするには、まずアラート応答を作成する必要があります。アラート応答は、アラートの送信先にする予定の外部システムとモジュールが連携できるようにする一連の設定です。それらの設定では、たとえば、SNMP アラート パラメータまたは syslog ファシリティおよびプライオリティを指定する場合があります。

アラート応答を作成した後、アラートをトリガーとして使用するために使用するイベントに関連付けます。アラート応答とイベントを関連付けるための処理は、次のように、イベントのタイプによって異なることに注意してください。

- アラート応答をマルウェア イベントと関連付ける場合は、独自の設定ページを使用します。
- SNMP および syslog アラート応答を接続のログ記録と関連付ける場合は、アクセス コントロール ルールとポリシーを使用します。

ASA FirePOWER モジュールには、実行可能なもう 1 つのタイプのアラートがあります。このアラートでは、個々の侵入イベントに対して、SNMP および syslog による侵入イベント通知を設定します。これらの通知は侵入ポリシーで設定します。侵入ルールに関する外部アラートの設定 （511 ページ）およびSNMP アラートの追加 （392 ページ）を参照してください。次の表では、アラート生成に必要なライセンスについて説明します。

表 *73:* アラートを生成するためのライセンス要件

アラートを生成する条件	必要なライセンス
侵入イベント	Protection
ネットワークベースのマルウェアイベント	Malware
接続イベント	接続をログに記録するために必要なライセンス

• アラート応答の使用 （504 ページ）

アラート応答の使用

ライセンス：任意

外部アラートを設定する際の最初の手順は、アラート応答を作成することです。アラート応答とは、アラートの送信先とする予定の外部システムと ASA FirePOWER モジュールが連携できるようにする一連の設定です。Syslog への書き込みによって、SNMP トラップを使用してアラートを送信するアラート応答を作成することができます。

アラートで受け取る情報は、アラートをトリガーしたイベントのタイプによって異なります。

作成したアラート応答は自動的に有効になります。有効なアラート応答のみがアラートを生成できます。アラートの生成を停止するには、設定を削除する代わりに、一時的にアラート応答を無効にすることができます。

アラート応答は [Alerts] ページ（[ASA FirePOWER Configuration] > [Policies] > [Actions Alerts]）で管理します。各アラート応答の横のスライダは有効かどうかを示します。有効なアラート応答のみがアラートを生成できます。このページは、たとえば、アクセス コントロール ルールの接続をログに記録するための設定でアラート応答が使用されているかどうかも示します。該当する列見出しをクリックして、名前、タイプ、使用中ステータス、および有効または無効のステータスでアラート応答をソートできます。列見出しを再度クリックすると、順序が反転します。

SNMP アラート応答の作成

ライセンス：任意

SNMPv1、SNMPv2、または SNMPv3 を使用して SNMP アラート応答を作成できます。

（注） SNMP で 64 ビット値を監視する場合は、SNMPv2 または SNMPv3 を使用する必要があります。SNMPv1 は 64 ビットのモニタリングをサポートしていません。

SNMP アラート応答を作成する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Actions Alerts] の順に選択します。

[Alerts] ページが表示されます。

ステップ 2 [Create Alert] ドロップダウン メニューから、[Create SNMP Alert] を選択します。

[Create SNMP Alert Configuration] ポップアップ ウィンドウが表示されます。

ステップ 3 [Name] フィールドに、SNMP 応答を識別するために使用する名前を入力します。

ステップ 4 [Trap Server] フィールドに、英数字を使用して SNMP トラップ サーバのホスト名または IP アドレスを入力します。

このフィールドに無効な IPv4 アドレス（192.169.1.456 など）を入力した場合でも、システムからの警告が**ない**ことに注意してください。無効なアドレスはホスト名として扱われます。

ステップ 5 [Version] ドロップダウン リストから、使用する SNMP バージョンを選択します。

SNMP v3 がデフォルトです。SNMP v1 または SNMP v2 を選択すると、異なるオプションが表示されます。

ステップ 6 どのバージョンの SNMP を選択したかに応じて、以下のようにします。

- SNMP v1 または SNMP v2 の場合、英数字または特殊文字（* または $）を使用して、[Community String] フィールドに SNMP コミュニティの名前を入力し、ステップ 12 に進みます。
- SNMP v3 の場合、[User Name] フィールドに SNMP サーバで認証するユーザの名前を入力し、次のステップに進みます。

ステップ 7 [Authentication Protocol] ドロップダウン リストから、認証に使用するプロトコルを選択します。

ステップ 8 [Authentication Password] フィールドに、SNMP サーバの認証に必要なパスワードを入力します。

ステップ 9 [Privacy Protocol] リストから、[None] を選択してプライバシー プロトコルを使用しないか、または [DES] を選択してプライバシー プロトコルにデータ暗号規格を使用します。

ステップ 10 [Privacy Password] フィールドに、SNMP サーバに必要なプライバシー パスワードを入力します。

ステップ 11 [Engine ID] フィールドに、SNMP エンジンの識別子を偶数桁の 16 進表記で入力します。

SNMPv3 を使用する場合、メッセージの符号化には Engine ID 値が使用されます。SNMP サーバでは、メッセージを復号化するためにこの値が必要です。

ASA FirePOWER モジュールの IP アドレスの 16 進数バージョンを使用することを推奨します。たとえば、ASA FirePOWER モジュールの IP アドレスが 10.1.1.77 の場合は、0a01014D0 を使用します。

ステップ 12 [Store ASA FirePOWER Changes] をクリックします。

アラート応答が保存され、自動的に有効になります。

Syslog アラート応答の作成

ライセンス：任意

syslog アラート応答を設定する際、syslog サーバーで確実に正しく処理されるようにするために、syslog メッセージに関連付けられる重大度とファシリティを指定できます。ファシリティはメッセージを作成するサブシステムを示し、重大度はメッセージの重大度を定義します。ファシリティと重大度は syslog に示される実際のメッセージには表示されませんが、syslog メッセージを受信するシステムに対して、メッセージの分類方法を指示するために使用されます。

ヒント　syslog の機能とその設定方法の詳細については、ご使用のシステムのマニュアルを参照してください。UNIX システムでは、syslog および syslog.conf の man ページで概念情報および設定手順が説明されています。

syslog アラート応答の作成時に任意のタイプのファシリティを選択できますが、syslog サーバに基づいて意味のあるものを選択する必要があります。すべての syslog サーバがすべてのファシリティをサポートしているわけではありません。UNIX syslog サーバの場合、syslog.conf ファイルで、どのファシリティがサーバ上のどのログ ファイルに保存されるかを示す必要があります。

次の表に、選択可能な syslog ファシリティを示します。

表 *74 :* 使用可能な *syslog* ファシリティ

ファシリティ	説明
ALERT	アラート メッセージ。
AUDIT	監査サブシステムによって生成されるメッセージ。
AUTH	セキュリティと承認に関連するメッセージ。
AUTHPRIV	セキュリティと承認に関連する制限付きアクセス メッセージ。多くのシステムで、これらのメッセージはセキュア ファイルに転送されます。
CLOCK	クロック デーモンによって生成されるメッセージ。 Windows オペレーティング システムを実行している syslog サーバは CLOCK ファシリティを使用することに注意してください。
CRON	クロック デーモンによって生成されるメッセージ。 Linux オペレーティング システムを実行している syslog サーバは CRON ファシリティを使用することに注意してください。
DAEMON	システム デーモンによって生成されるメッセージ。
FTP	FTP デーモンによって生成されるメッセージ。

ファシリティ	説明
KERN	カーネルによって生成されるメッセージ。多くのシステムでは、これらのメッセージは表示されるときにコンソールに出力されます。
LOCAL0-LOCAL7	内部プロセスによって生成されるメッセージ。
LPR	印刷サブシステムによって生成されるメッセージ。
MAIL	メール システムで生成されるメッセージ。
NEWS	ネットワーク ニュース サブシステムによって生成されるメッセージ。
NTP	NTP デーモンによって生成されるメッセージ。
SYSLOG	syslog デーモンによって生成されるメッセージ。
USER	ユーザー レベルのプロセスによって生成されるメッセージ。
UUCP	UUCP サブシステムによって生成されるメッセージ。

次の表に、選択可能な標準の syslog 重大度レベルを示します。

表 *75 : syslog* 重大度レベル

レベル	説明
ALERT	ただちに修正する必要がある状態。
CRIT	クリティカルな状態。
DEBUG	デバッグ情報を含むメッセージ。
EMERG	すべてのユーザに配信されるパニック状態。
ERR	エラー状態。
INFO	情報メッセージです。
NOTICE	エラー状態ではないが、注意が必要な状態。
WARNING	警告メッセージ。

syslog アラートの送信を開始する前に、syslog サーバがリモート メッセージを受信できることを確認してください。

syslog アラートを作成する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Actions Alerts] の順に選択します。

[Alerts] ページが表示されます。[Create Alert] ドロップダウン メニューから、[Create Syslog Alert] を選択します。

[Create Syslog Alert Configuration] ポップアップ ウィンドウが表示されます。

ステップ 2 [Name] フィールドに、保存される応答を識別するために使用する名前を入力します。

ステップ 3 [Host] フィールドに、syslog サーバのホスト名または IP アドレスを入力します。

このフィールドに無効な IPv4 アドレス（192.168.1.456 など）を入力した場合でも、システムからの警告が**ない**ことに注意してください。無効なアドレスはホスト名として扱われます。

ステップ 4 [Port] フィールドに、サーバが syslog メッセージに使用するポートを入力します。

この値はデフォルトで 514 です。

ステップ 5 [Facility] リストから、ファシリティを選択します。

使用可能なファシリティの一覧については、表「使用可能な syslog ファシリティ」を参照してください。

ステップ 6 [Severity] リストから、重大度を選択します。

使用可能な重大度の一覧については、表「Syslog の重大度レベル」を参照してください。

ステップ 7 [Tag] フィールドに、syslog メッセージとともに表示するタグ名を入力します。

タグ名には英数字のみを使用します。スペースまたは下線は使用**できません**。

たとえば、syslog に送信されるすべてのメッセージの前に From MC を付ける場合は、フィールドに「From MC」と入力します。

ステップ 8 [Store ASA FirePOWER Changes] をクリックします。

アラート応答が保存され、自動的に有効になります。

アラート応答の変更

ライセンス：任意

ほとんどのタイプのアラートについて、アラート応答が有効で使用中の場合、アラート応答への変更はすぐに反映されます。ただし、接続イベントをログに記録するアクセス コントロール ルールで使用されるアラート応答の場合、アクセス コントロール ポリシーを再適用するまで変更は有効になりません。

アラート応答を編集する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Actions Alerts] の順に選択します。

[Alerts] ページが表示されます。

ステップ 2 編集するアラート応答の横にある編集アイコンをクリックします。

そのアラート応答の設定ポップアップ ウィンドウが表示されます。

ステップ 3 必要に応じて変更を加えます。

ステップ 4 [Store ASA FirePOWER Changes] をクリックします。

アラート応答が保存されます。

アラート応答の削除

ライセンス：任意

使用中でない任意のアラート応答を削除できます。

アラート応答を削除する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Actions Alerts] の順に選択します。

[Alerts] ページが表示されます。

ステップ 2 削除するアラート応答の横にある削除アイコンをクリックします。

ステップ 3 アラート応答を削除することを確認します。

アラート応答が削除されます。

アラート応答の有効化と無効化

ライセンス：任意

有効なアラート応答のみがアラートを生成できます。アラートの生成を停止するには、設定を削除する代わりに、一時的にアラート応答を無効にすることができます。無効化するときにアラートが使用中の場合は、無効にしても使用中とみなされることに注意してください。

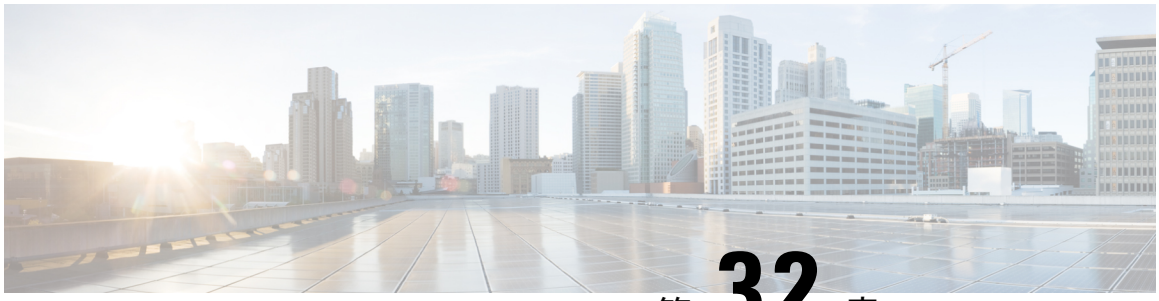
アラート応答を有効または無効にする方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Actions Alerts] の順に選択します。

[Alerts] ページが表示されます。

ステップ 2 有効または無効にするアラート応答の横にある [enable/disable] スライダをクリックします。

アラート応答が有効だった場合は、無効になります。無効だった場合は、有効になります。



第 32 章

侵入ルールに関する外部アラートの設定

ASA FirePOWER モジュールのユーザ インターフェイスには侵入イベントに関するさまざまなビューがありますが、企業によっては、重要なシステムの継続的なモニタリングを容易にするために、外部侵入イベントの通知を定義したいという要望があります。syslog ファシリティへのロギングを有効にしたり、SNMP トラップ サーバにイベント データを送信したりできます。

各侵入ポリシー内では、侵入イベントの通知制限を指定し、外部ロギング ファシリティへの侵入イベント通知をセットアップし、侵入イベントへの外部応答を設定できます。

ヒント　アナリストによっては、同じ侵入イベントに対して複数のアラートを受信することは望まないものの、特定の侵入イベントの発生については、頻度を制限したうえで通知を受信したいと考えています。詳細については、「ポリシー単位の侵入イベント通知のフィルタ処理 （380 ページ）」を参照してください。

侵入ポリシー以外にも、ASA FirePOWER モジュールで実行可能な別のタイプのアラートがあります。特定のアクセス コントロール ルールによって記録された接続イベントなど、他のタイプのイベントに対して、SNMP および syslog アラートによる応答を設定できます。詳細については、外部アラートの設定 （503 ページ）を参照してください。

外部侵入イベント通知の詳細情報については、次の項を参照してください。

- 「SNMP 応答の使用」セクションでは、指定された SNMP トラップ サーバにイベント データを送信する場合に設定可能なオプションや、SNMP アラート オプションを指定する手順が説明されています。
- 「Syslog 応答の使用」セクションでは、外部 syslog にイベント データを送信する場合に設定可能なオプションや、syslog アラート オプションを指定する手順が説明されています。

SNMP 応答の使用

ライセンス：Protection

SNMP トラップは、ネットワーク管理に関する通知です。侵入イベントに関する通知を SNMP トラップ（SNMP アラートとも呼ばれる）として送信するようにデバイスを設定できます。各 SNMP アラートには次のものが含まれます。

- トラップを生成するサーバの名前
- アラートを検出したデバイスの IP アドレス
- アラートを検出したデバイスの名前
- イベント データ

さまざまな SNMP アラート パラメータを設定できます。使用可能なパラメータは、使用する SNMP のバージョンによって異なります。SNMP アラートを有効化および無効化する方法の詳細については、侵入ポリシーの詳細設定 （348 ページ）を参照してください。

ヒント ネットワーク管理システムで Management Information Base（MIB）ファイルが必要な場合は、ASA FirePOWER モジュール（/etc/sf/DCEALERT.MIB）から入手できます。

SNMP v2 オプション

SNMP v2 の場合、次の表で説明されているオプションを指定できます。

表 *76 : SNMP v2* オプション

オプション	説明
Trap Type	アラートに表示される IP アドレスに使用するトラップ タイプ。 ネットワーク管理システムによって INET_IPV4 アドレス タイプが正常にレンダリングされた場合は、[as Binary] を選択できます。そうでない場合は、[as String] を選択します。たとえば、HP Openview では文字列タイプが必要になります。
Trap Server	SNMP トラップ通知を受信するサーバ。 単一の IP アドレスまたはホスト名を指定できます。
Community String	コミュニティ名。
Sensor ID	侵入イベントを SNMP トラップとして送信する管理対象デバイスを表す、ユーザ定義の整数。

SNMP v3 オプション

SNMP v3 の場合、次の表で説明されているオプションを指定できます。

（注） SNMP v3 を使用する場合、アプライアンスは Engine ID 値を使用してメッセージをエンコードします。SNMP サーバでは、メッセージを復号化するためにこの値が必要です。現在、この Engine ID 値は常に、文字列の末尾に 01 が付く、アプライアンスの IP アドレスの 16 進数バージョンになります。たとえば、SNMP アラートを送信するアプライアンスの IP アドレスが 172.16.1.50 の場合、Engine ID は 0xAC10013201 です。また、アプライアンスの IP アドレスが 10.1.1.77 の場合、Engine ID として 0x0a01014D01 が使用されます。

オプション	説明
Trap Type	アラートに表示される IP アドレスに使用するトラップ タイプ。 ネットワーク管理システムによって INET_IPV4 アドレス タイプが正常にレンダリングされた場合は、[as Binary] を選択できます。そうでない場合は、[as String] を選択します。たとえば、HP Openview では文字列タイプが必要になります。
Trap Server	SNMP トラップ通知を受信するサーバ。 単一の IP アドレスまたはホスト名を指定できます。
Authentication Password	認証に必要なパスワード。SNMP v3 は、設定に応じて Message Digest 5（MD5）ハッシュ関数または Secure Hash Algorithm（SHA）ハッシュ関数のいずれかを使用し、このパスワードを暗号化します。 認証パスワードを指定すると、認証が有効になります。
Private Password	プライバシー用の SNMP キー。SNMP v3 は Data Encryption Standard（DES）ブロック暗号を使用して、このパスワードを暗号化します。 プライベート パスワードを指定すると、プライバシーが有効になります。プライベートパスワードを指定する場合は、認証パスワードも指定する必要があります。
User Name	SNMP ユーザ名。

SNMP アラートの設定の詳細については、SNMP 応答の使用 （512 ページ）を参照してください。

SNMP 応答の設定

ライセンス：Protection

侵入ポリシーで SNMP アラートを設定できます。アクセス コントロール ポリシーの一部としてポリシーを適用すると、システムは SNMP トラップで検出した侵入イベントをすべて通知す

るようになります。SNMP アラートの詳細については、SNMP 応答の設定 （513 ページ）を参照してください。

SNMP アラート オプションを設定するには、次の手順を実行します。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定 （314 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3 左側のナビゲーション パネルにある [Advanced Settings] をクリックします。

[Advanced Settings] ページが表示されます。

ステップ 4 外部応答の [SNMP Alerting] が有効かどうかに応じて、次の 2 つの選択肢があります。

- 設定が有効な場合、[Edit] をクリックします。
- 設定が無効である場合、[Enabled] をクリックし、[Edit] をクリックします。

[SNMP Alerting] ページが表示されます。

ページ下部のメッセージは、設定を含む侵入ポリシー層を示します。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシー レイヤでのレイヤの使用 （317 ページ）」を参照してください。

ステップ 5 IP アドレスに使用するトラップ タイプの形式を [as Binary] または [as String] のいずれかに指定します。

（注） ネットワーク管理システムによって INET_IPV4 アドレス タイプが正常にレンダリングされた場合は、[as Binary] オプションを使用できます。正常にレンダリングされなかった場合は、[as String] オプションを使用します。たとえば、HP OpenView では [as String] オプションが必要になります。

ステップ 6 [SNMP v2] または [SNMP v3] を選択します。

- SNMP v2 を設定するには、使用するトラップ サーバの IP アドレスとコミュニティ名を対応するフィールドに入力します。SNMP v2 オプション （512 ページ） を参照してください。
- SNMP v3 を設定するには、使用するトラップ サーバの IP アドレス、認証パスワード、プライベート パスワード、およびユーザ名を対応するフィールドに入力します。詳細については、「SNMP v3 オプション （513 ページ）」を参照してください。

（注） [SNMP v2] または [SNMP v3] を選択する必要があります。

（注） SNMP v3 パスワードを入力すると、パスワードは初期設定時にはプレーンテキストで表示されますが、暗号化形式で保存されます。

ステップ 7 ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、「競合の解決とポリシー変更の確定 （314 ページ）」を参照してください。

Syslog 応答の使用

ライセンス：Protection

システム ログ、つまり *syslog* は、ネットワーク イベント ロギングの標準ロギング メカニズムです。侵入イベントの通知である syslog アラートをアプライアンスの syslog に送信できます。syslog では、syslog 内の情報を優先順位別およびファシリティ別に分類することができます。優先順位はアラートの重大度を反映し、ファシリティはアラートを生成したサブシステムを示します。ファシリティおよび優先順位は syslog の実際のメッセージに表示されませんが、その代わりに、syslog メッセージを受信するシステムにそれを分類する方法を指示するために使用されます。

syslog アラートには次の情報が含まれます。

- アラート生成の日時
- イベント メッセージ
- イベント データ
- トリガー イベントのジェネレータ ID
- トリガー イベントの Snort ID
- リビジョン

侵入ポリシーでは、syslog アラートを有効にして、syslog の侵入イベントの通知に関連付けられている syslog の優先順位およびファシリティを指定できます。アクセス コントロール ポリシーの一部として侵入ポリシーを適用した場合、システムは、検出した侵入イベントの syslog アラートをローカル ホストまたはポリシーで指定されたロギング ホストの syslog ファシリティに送信します。アラートを受信したホストは、syslog アラートの設定時に設定されたファシリティおよび優先順位に関する情報を使用して、アラートを分類します。

次の表には、syslog アラートを設定する場合に選択できるファシリティを示します。使用するリモート syslog サーバの設定に基づいて、効果のあるファシリティの設定を行ってください。リモート システムにある syslog.conf ファイル（UNIX または Linux ベースのシステムに syslog メッセージをロギングしている場合）は、サーバのどのログ ファイルにどのファシリティが保存されるかを示します。

表 *77*：使用可能な *syslog* ファシリティ

ファシリティ	説明
AUTH	セキュリティと承認に関連するメッセージ。

ファシリティ	説明
AUTHPRIV	セキュリティと承認に関連する制限付きアクセス メッセージ。多くのシステムで、これらのメッセージはセキュア ファイルに転送されます。
CRON	クロック デーモンによって生成されるメッセージ。
DAEMON	システム デーモンによって生成されるメッセージ。
FTP	FTP デーモンによって生成されるメッセージ。
KERN	カーネルによって生成されるメッセージ。多くのシステムでは、これらのメッセージは表示されるときにコンソールに出力されます。
LOCAL0-LOCAL7	内部プロセスによって生成されるメッセージ。
LPR	印刷サブシステムによって生成されるメッセージ。
MAIL	メール システムで生成されるメッセージ。
NEWS	ネットワーク ニュース サブシステムによって生成されるメッセージ。
SYSLOG	syslog デーモンによって生成されるメッセージ。
USER	ユーザー レベルのプロセスによって生成されるメッセージ。
UUCP	UUCP サブシステムによって生成されるメッセージ。

このアラートで生成されるすべての通知を表示するには、次の標準的なsyslogの優先順位レベルのいずれかを選択します。

表 *78 : syslog* の優先順位レベル

レベル	説明
EMERG	すべてのユーザにブロードキャストするパニック状態
ALERT	すぐに修正する必要がある状態
CRIT	重大な状態
ERR	エラー状態
WARNING	警告メッセージ
NOTICE	エラー状態ではないが、注意が必要な状態
INFO	通知メッセージ
DEBUG	デバッグ情報を含むメッセージ

syslog の動作とその設定方法の詳細については、システムに付属の資料を参照してください。UNIX または Linux ベースのシステムの syslog にログインしている場合、syslog.conf man ファイル（コマンドラインで man syslog.conf と入力）および syslog man ファイル（コマンドラインで man syslog と入力）に、syslog の動作とその設定方法に関する情報が示されます。

Syslog 応答の設定

ライセンス：Protection

侵入ポリシーで syslog アラートを設定できます。アクセス コントロール ポリシーの一部としてポリシーを適用すると、システムはsyslog で検出した侵入イベントをすべて通知するようになります。syslog アラートの詳細については、Syslog 応答の使用 （515 ページ）を参照してください。

syslog アラート オプションを設定するには、次の手順を実行します。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] の順に選択します。

[Intrusion Policy] ページが表示されます。

ステップ 2 編集するポリシーの横にある編集アイコン（）をクリックします。

別のポリシーに未保存の変更がある場合は、[OK] をクリックしてそれらの変更を破棄し、処理を続行します。別のポリシーでの未保存の変更の保存方法については、競合の解決とポリシー変更の確定 （314 ページ）を参照してください。

[Policy Information] ページが表示されます。

ステップ 3 左側のナビゲーション パネルにある [Advanced Settings] をクリックします。

[Advanced Settings] ページが表示されます。

ステップ 4 外部応答の [Syslog Alerting] が有効かどうかに応じて、次の 2 つの選択肢があります。

- 設定が有効な場合、[Edit] をクリックします。
- 設定が無効である場合、[Enabled] をクリックし、[Edit] をクリックします。

[Syslog Alerting] ページが表示されます。

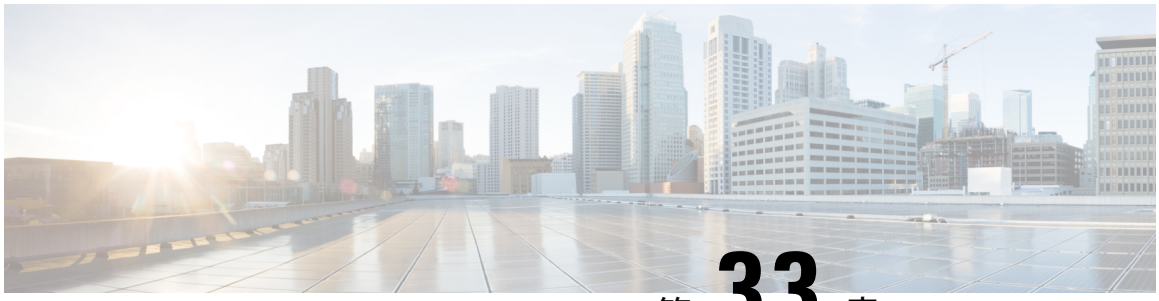
ページ下部のメッセージは、設定を含む侵入ポリシー層を示します。詳細については、「ネットワーク分析ポリシーまたは侵入ポリシー レイヤでのレイヤの使用 （317 ページ）」を参照してください。

ステップ 5 オプションで、[Logging Hosts] フィールドに、ロギング ホストとして指定するリモート アクセス IP アドレスを入力します。複数のホストを指定する場合は、カンマで区切ります。

ステップ 6 ドロップダウン リストからファシリティおよび優先順位のレベルを選択します。

ファシリティおよび優先順位オプションの詳細については、Syslog 応答の使用 （515 ページ）を参照してください。

ステップ 7 ポリシーを保存する、編集を続行する、変更を破棄する、基本ポリシーのデフォルト設定に戻す、変更をシステム キャッシュに残して終了する、のいずれかを行います。詳細については、「競合の解決とポリシー変更の確定 （314 ページ）」を参照してください。



第 33 章

ASA FirePOWER ダッシュボードの使用

ASA FirePOWER モジュール ダッシュボードでは、現在のシステム ステータスを一目で確認できます。ダッシュボードでは、ウィジェットが 3 列のレイアウトで表示されます。ウィジェットとは、ASA FirePOWER モジュールのさまざまな側面に関する情報が提供される自己完結型の小さなコンポーネントです。システムには、事前定義された複数のウィジェットが付属しています。たとえば、Appliance Information ウィジェットには、アプライアンスの名前、モデル、および現在実行中の ASA FirePOWER モジュール ソフトウェアのバージョンが表示されます。

ダッシュボードには、ウィジェットを制約する時間範囲があります。最短で 1 時間前から、最長では 1 年前からの期間を反映するように時間範囲を変更できます。

各アプライアンスは、デフォルト ダッシュボードが付属しています。このダッシュボードには、ASA FirePOWER モジュール展開環境の一般的なシステム ステータス情報が表示されます。

ダッシュボード ウィジェットについて

ライセンス：任意

ダッシュボードには、複数のウィジェットが 3 列のレイアウトで表示されます。ASA FirePOWER モジュールには、事前定義された複数のダッシュボード ウィジェットが付属しています。各ウィジェットには、システムのさまざまな側面に関する情報が表示されます。ウィジェットは、最小化、最大化、並べ替えができます。

ウィジェットの設定について

ライセンス：任意

各ウィジェットには、動作を決定する一連のプリファレンスがあります。

ウィジェットのプリファレンスは単純なものにすることもできます。たとえば、Current Interface Status ウィジェットのプリファレンスを設定できます。これは、内部ネットワークで有効になっているすべてのインターフェイスについて現在のステータスを表示します。このウィジェットでは、アップデートの頻度のみを設定します。

ウィジェットのプリファレンスを変更する方法：

ステップ 1 プリファレンスを変更するウィジェットのタイトルバーで、プリファレンスの表示アイコンをクリックします。

そのウィジェットのプリファレンス セクションが表示されます。

ステップ 2 必要に応じて変更を加えます。

変更はすぐに反映されます。ユーザが個々のウィジェットに指定できるプリファレンスについては、事前定義されたウィジェットについて （520 ページ）を参照してください。

ステップ 3 プリファレンス セクションを非表示にするには、ウィジェットのタイトルバーで、プリファレンスの非表示アイコンをクリックします。

事前定義されたウィジェットについて

ライセンス：任意

ASA FirePOWER モジュールには、現在のシステム ステータスを一目で確認できる複数の事前定義ウィジェットが付属しています。

Appliance Information ウィジェットについて

ライセンス：任意

Appliance Information ウィジェットは、次の情報を提供します。

- アプライアンスの名前、IPv4 アドレス、IPv6 アドレス、およびモデル
- アプライアンスにインストールされている、ASA FirePOWER モジュール ソフトウェア、ルールアップデート、脆弱性データベース（VDB）、および地理位置情報更新のバージョン。

単純なビューまたは高度なビューを表示するようにウィジェットのプリファレンスを変更することで、ウィジェットで表示する情報量を調整できます。プリファレンスでは、ウィジェットをアップデートする頻度を調整することもできます。詳細については、ウィジェットの設定について （519 ページ）を参照してください。

Current Interface Status ウィジェットについて

ライセンス：任意

Current Interface Status ウィジェットは、有効になっているか未使用のアプライアンスのすべてのインターフェイスのステータスを示します。ウィジェットは、各インターフェイスに対して次の情報を提供します。

- インターフェイスの名前
- インターフェイスのリンク状態
- インターフェイスのリンク モード（100Mb 全二重、または 10Mb 半二重など）
- インターフェイスのタイプ（銅線または光ファイバ）
- インターフェイスで受け取ったデータ量（Rx）および送信したデータ量（Tx）

リンクの状態を表すボールの色は、次のように現在のステータスを示します。

- 緑色：リンクはフルスピードでアップ状態です
- 黄色：リンクはアップ状態ですがフルスピードではありません
- 赤色：リンクはアップ状態ではありません
- 灰色：リンクは管理上無効になっています
- 青色：リンク ステート情報は使用可能ではありません（たとえば、ASA）

ウィジェットのプリファレンスでは、ウィジェットをアップデートする頻度を調整します。詳細については、ウィジェットの設定について （519 ページ）を参照してください。

Disk Usage ウィジェットについて

ライセンス：任意

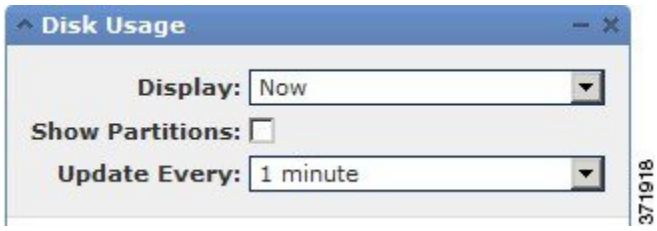
Disk Usage ウィジェットには、ディスク使用率のカテゴリに基づいて、ハードドライブで使用される領域が表示されます。また、アプライアンスのハードドライブの各パーティションで使用される領域および容量も示します。[カテゴリ別（By Category）] スタック バーは、各ディスク使用率のカテゴリを、使用可能な合計ディスク領域に対する使用量の割合として表示します。次の表で、使用可能なカテゴリについて説明します。

表 *79*：ディスク使用率のカテゴリ

Disk Usage のカテゴリ	説明
イベント	システムで記録されたすべてのイベント
Files	システムに格納されたすべてのファイル
Backups	すべてのバックアップ ファイル

Disk Usage のカテゴリ	説明
Updates	ルールのアップデートやシステムのアップデートなど、アップデートに関連するすべてのファイル
Other	システムのトラブルシューティング ファイルおよびその他のファイル
Free	アプライアンス上の残りの空き領域

マルウェア ストレージ パックがインストールされている場合は、ウィジェットのプリファレンスを変更して、By Category スタック バーのみを表示したり、スタック バーと admin（/）、/Volume、および /boot パーティションの使用率、および /var/storage パーティションを表示したりするようにウィジェットを設定できます。



ウィジェットのプリファレンスは、ウィジェットのアップデート頻度、およびダッシュボードの時間範囲で現在のディスク使用率または収集したディスク使用率の統計のいずれかを表示するかも制御します。詳細については、ウィジェットの設定について （519ページ）を参照してください。

Product Licensing ウィジェットについて

ライセンス：任意

Product Licensing ウィジェットには、現在インストールされているデバイスおよび機能のライセンスが表示されます。また、ライセンス契約されているアイテム（ホストやユーザ）の数、許可される残りのライセンス契約アイテム数も示します。

このウィジェットの上部のセクションには、一時的なライセンスも含めて、インストールされているすべてのデバイスおよび機能のライセンスが表示されますが、[Expiring Licenses] セクションには、一時的なライセンスおよび期限の切れたライセンスだけが表示されます。

ウィジェットの背景のバーは、使用中のライセンスのそれぞれのタイプの割合を示しています。このバーは右から左へ読みます。期限の切れたライセンスには、取り消し線が付けられています。

ウィジェットのプリファレンスを変更して、現在ライセンス契約されている機能を表示するか、またはライセンス契約が可能なすべての機能を表示するようにウィジェットを設定することができます。プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。詳細については、ウィジェットの設定について （519 ページ）を参照してください。

任意のライセンス タイプをクリックすると、ローカル設定の [License] ページに移動して、機能ライセンスを追加または削除することができます。詳細については、ASA FirePOWER モジュールのライセンス （567 ページ）を参照してください。

Product Updates ウィジェットについて

ライセンス：任意

Product Updates ウィジェットには、アプライアンスに現在インストールされているソフトウェア（ASA FirePOWER モジュール ソフトウェアおよびルール アップデート）の概要、およびそのソフトウェアに関するダウンロード済みで、まだインストールしていないアップデートの情報が表示されます。

このウィジェットは、ユーザがソフトウェアのアップデートをダウンロード、プッシュ、またはインストールするスケジュールされたタスクを設定していない場合、ソフトウェアの最新バージョンを [Unknown] と表示します。ウィジェットではスケジュールされたタスクを使用して、最新のバージョンを決定するためです。詳細については、タスクのスケジューリング （537 ページ）を参照してください。

ウィジェットは、ソフトウェアを更新できるページへのリンクもあります。

ウィジェットのプリファレンスを変更して、最新のバージョンを非表示にするようウィジェットを設定できます。プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。詳細については、ウィジェットの設定について （519 ページ）を参照してください。

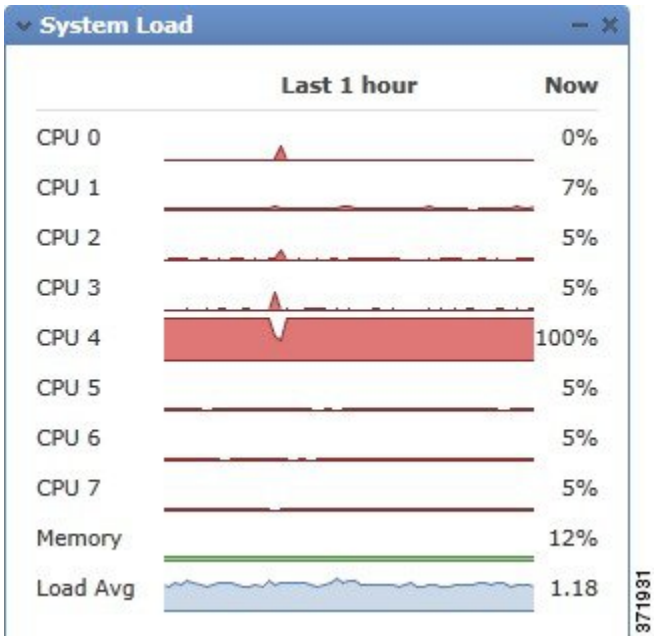
Product Updates ウィジェットでは、次のことができます。

- ASA FirePOWER モジュール ソフトウェア、ルール アップデート、VDB、または地理位置情報アップデートの最新バージョンをクリックすることによる、アプライアンスの手動更新。
- システム ソフトウェア、VDB、または位置情報データベースを更新するには、ASA FirePOWER モジュール ソフトウェアの更新 （577 ページ）を参照してください。
- 最新のルール アップデートをインポートするには、ルール更新とローカル ルール ファイルのインポート （582 ページ）を参照してください。
- 最新バージョンをクリックして、ASA FirePOWER モジュール ソフトウェア、VDB、またはルール アップデートの最新バージョンをダウンロードするためのスケジュールされたタスクの作成。タスクのスケジューリング （537 ページ）を参照してください。

System Load ウィジェットについて

ライセンス：任意

System Load ウィジェットは、アプライアンス上の（各 CPU についての）CPU の使用率、メモリ（RAM）の使用率、およびシステムの負荷（実行を待機しているプロセスの数によって測定され、負荷平均とも呼ばれる）を現在、およびダッシュボードの時間範囲について表示します。

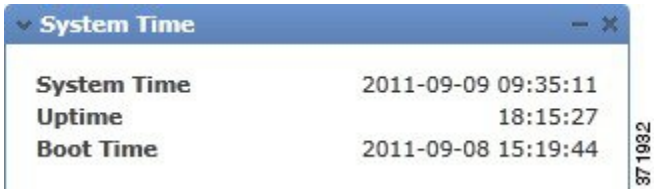


ウィジェットのプリファレンスを変更して、負荷平均を表示または非表示にするようウィジェットを設定できます。プリファレンスでは、ウィジェットをアップデートする頻度も調整されます。詳細については、ウィジェットの設定について （519 ページ）を参照してください。

System Time ウィジェットについて

ライセンス：任意

System Time ウィジェットは、アプライアンスのローカル システム時間、稼動時間、およびブート時間を表示します。



ウィジェットのプリファレンスを変更して、ブート時間を非表示にするようウィジェットを設定できます。プリファレンスは、ウィジェットがアプライアンスの時計と同期する頻度も調整します。詳細については、ウィジェットの設定について （519ページ）を参照してください。

ダッシュボードの操作

ライセンス：任意

ダッシュボードに示されるウィジェットを表示および変更できます。

ダッシュボードの表示

ライセンス：任意

ASA FirePOWER モジュールのダッシュボードは、[Home] > [ASA FirePOWER Dashboard] の順に選択することで、いつでも表示できます。

ダッシュボードには、ウィジェットを制約する時間範囲があります。最短で1時間前（デフォルト）から、最長では1年前からの期間を反映するように時間範囲を変更できます。時間範囲を変更する場合は、時間によって制約される可能性のあるウィジェットが自動でアップデートされ、新しい時間範囲が反映されます。

すべてのウィジェットを時間で制約できるわけではないことに注意してください。たとえば、ダッシュボードの時間範囲は Appliance Information ウィジェットには影響を与えません。このウィジェットには、アプライアンスの名前、モデル、およびASA FirePOWERモジュール ソフトウェアの現在のバージョンを含む情報が表示されます。

ダッシュボードを表示するには、次のようにします。

- [Home] > [ASA FirePOWER Dashboard] の順に選択します。

[ASA FirePOWER] ダッシュボードが表示されます。

ダッシュボードの時間範囲を変更するには、次のようにします。

- [Show the Last] ドロップダウン リストから、ダッシュボードの時間範囲を選択します。

ページ上で該当するすべてのウィジェットが更新され、最新の時間範囲が反映されます。

ダッシュボードの変更

ライセンス：任意

ダッシュボードでは、ウィジェットが3列のレイアウトで表示されます。ウィジェットは、最小化、最大化、並べ替えができます。

ウィジェットの並べ替え

ライセンス：任意

ウィジェットはどれも、場所を変更できます。

ウィジェットを移動するには、次のようにします。

移動するウィジェットのタイトル バーをクリックし、新しい場所へドラッグします。

ウィジェットの最小化と最大化

ライセンス：任意

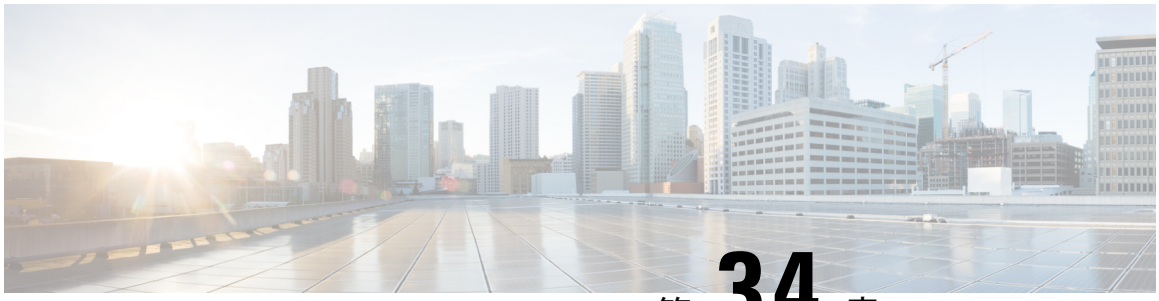
ウィジェットを最小化してビューを単純化したり、その後で最大化してもう一度表示したりできます。

ウィジェットを最小化するには、次のようにします。

ウィジェットのタイトル バーで、最小化アイコンをクリックします。

ウィジェットを最大化するには、次のようにします。

最小化されているウィジェットのタイトル バーで最大化アイコンをクリックします。



第 34 章

ASA FirePOWER レポートの使用

ネットワーク上のトラフィックを分析するため、さまざまな期間のレポートを表示できます。レポートは、ネットワーク トラフィックのさまざまな側面の情報を集計します。ほとんどの場合、一般情報から特定の情報にドリルダウンできます。たとえば、すべてのユーザのレポートを表示し、次に特定のユーザの詳細を表示できます。

概要レポートと詳細レポートには、トップ ポリシーや Web カテゴリなど、複数のレポート コンポーネントがあります。これらのレポートには、表示しているレポートのそのタイプで最も発生頻度の高い項目が示されます。たとえば、特定のユーザの詳細レポートを表示している場合、トップ ポリシーにはそのユーザに最も関連付けられたポリシー ヒットが表示されます。

使用可能なレポートについて

ライセンス：任意

使用可能なレポートには、ASA FirePOWER モジュールで使用可能なメイン レポートが含まれます。それらのレポートは、[ASA FirePOWER Reporting] メニューから表示できます。

一般に、名前、[View More] リンクなど、多くの項目をクリックして、個々の項目または監視するカテゴリ全体に関する詳細な情報を取得できます。

Network Overview

このレポートには、ネットワークのトラフィックに関するサマリー情報が表示されます。この情報は、詳細な分析を必要とするエリアの識別、またはネットワークが一般的な予期内で動作していることの確認に使用します。

Users

このレポートには、ネットワークの上位ユーザが表示されます。アクティブ認証に失敗したユーザは、ユーザ レポートのユーザ名 ANONYMOUS の下に表示されます。ただし、ゲスト アクセスを有効にしてる場合には、ユーザ名が Guest となります。認証の必要がないためマッ

ピングをもたないユーザは、IPアドレスで表示されます。この情報は、ユーザの異常活動の識別に役立ちます。

ヒント　ユーザ名は、ユーザの ID 情報がトラフィック フローに関連付けられている場合に限り使用できます。ユーザ ID が大多数のトラフィックのレポートで使用できるようにする場合は、アクセス コントロール ポリシーでアクティブ認証を使用する必要があります。

Applications

このレポートには、侵入イベントをトリガーしたトラフィックで検出されたHTTP トラフィックの内容または要求されたURL を表すアプリケーションが表示されます。モジュールがHTTP のアプリケーション プロトコルを検出し、特定の Web アプリケーションを検出できなかった場合、モジュールはここで一般的な Web ブラウジング指定を提供することに注意してください。

Web categories

このレポートには、訪問する Web サイトのカテゴリに基づいて、ネットワークで使用されている Web サイトのカテゴリ（ギャンブル、広告、検索エンジン、ポータルなど）が表示されます。ユーザが訪問する上位カテゴリを識別し、アクセス コントロール ポリシーによって望ましくないカテゴリが十分にブロックされているかどうかを判別するために、この情報を使用します。

Policies

このレポートには、アクセス コントロール ポリシーがネットワークのトラフィックにどのように適用されたかが表示されます。ポリシーを削除した場合、名前に「-DELETED」が付きます。この情報を使用すると、ポリシーの効果の評価に役立ちます。

Ingress zones

このレポートには、イベントをトリガーしたパケットの入力セキュリティ ゾーンが表示されます。パッシブ展開環境では、このセキュリティ ゾーン フィールドだけに入力されます。

Egress zones

インライン展開環境の場合、このレポートには、イベントをトリガーとして使用したパケットの出力セキュリティ ゾーンが表示されます。パッシブ展開環境では、このセキュリティ ゾーンのフィールドには入力されません。

Destinations

このレポートには、ネットワーク トラフィックの分析に基づいて、ネットワークで使用中のアプリケーション（Facebook など）が表示されます。この情報を使用すると、ネットワークで使用された上位アプリケーションの識別に役立ち、不要なアプリケーションの使用量を減らすために追加のアクセス コントロール ポリシーが必要かどうかを判断できます。

Attackers

このレポートには、イベントをトリガーした送信元ホストが使用する送信元 IP アドレスが表示されます。

Targets

このレポートには、イベントをトリガーした受信ホストが使用する宛先 IP アドレスが表示されます。

Threats

このレポートには、ネットワークに対し検出された各脅威に割り当てられた固有の識別番号と説明のテキストが表示されます。

Files logs

このレポートには、検出されたファイルのタイプ（たとえばHTMLやMSEXE）が表示されます。

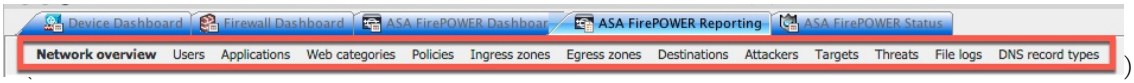
レポートの基本

ライセンス: 任意

ここでは、レポート使用の基本を説明します。以降のトピックは、いずか1つの特定のレポートではなくレポート全般に適用されます。

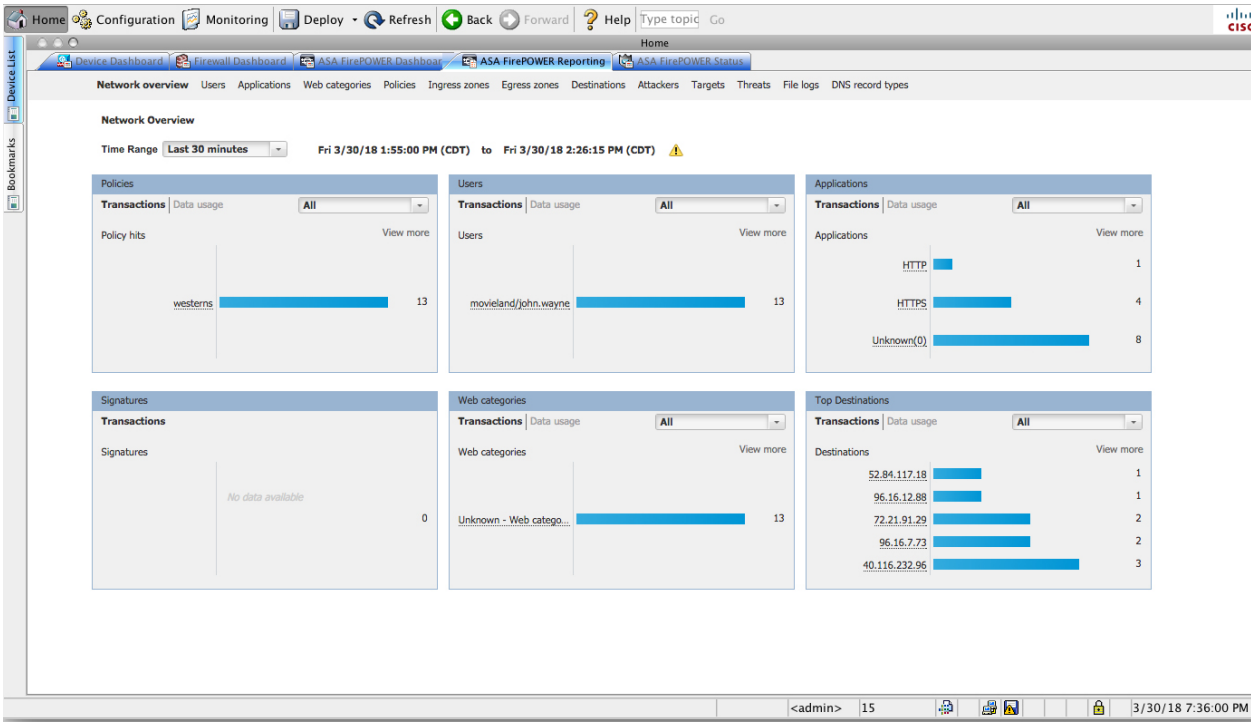
レポートを使用する前に

レポートを実行するには、ASA FirePOWER モジュールにログインして、[ホーム（Home）] > [ASA FirePOWER レポート（ASA FirePOWER Reporting）] をクリックします。使用可能なレポートのタイプは、次の図



に示すように、ウィンドウの上部に表示されます。

ネットワークの概要レポートの例を次に示します。



の詳細情報を取得するには、任意の下線付きテキストをクリックします。

レポート データについて

ライセンス: 任意

レポートデータはデバイスからすぐに収集されるため、レポートに反映されるデータとネットワーク活動の間に時差はほとんどありません。ただし、データを分析するときは次の点に注意してください。

- データは、ASA FirePOWER モジュールに適用されたアクセス コントロール ポリシーに一致するトラフィックについて収集されます。
- データは 5 分バケットで集約されるため、30 分グラフと 1 時間グラフではデータ ポイントは 5 分刻みで表示されます。1 時間の終了時に、5 分バケットが 1 時間バケットに集約され、さらにこれらが日バケットおよび週バケットに集約されます。5 分バケットは 7 日間保持され、1 時間バケットは 31 日間、日バケットは最大 365 日間保持されます。前にさかのぼるほど、データはさらに集約されます。古いデータを照会する場合、これらのデータ バケットが利用できる状態に合わせてクエリーを実行すると最良の結果が得られます。日計算はすべて UTC 時刻に基づきます。サーバやクライアントの時刻は無視されます。

（注） たとえば、5 分間よりも長い間デバイスが到達不能になったなどの理由により、データ ポイントが欠けている場合は、折れ線グラフが途切れます。

レポートのドリルダウン

ライセンス: 任意

レポートには、必要な情報にドリルダウンするための多くのリンクが含まれます。項目の上にマウスを置くと、どの項目でその詳細に進めるかがわかります。

たとえば、一般的なレポート項目において、[View More] リンクをクリックすると、その項目のサマリー レポートに移動できます。

サマリー レポートの項目をクリックして、特定の項目の詳細レポートに移動することもできます。たとえば、アプリケーション サマリー レポートで Hypertext Transfer Protocol (HTTP)をクリックすると、HTTP のアプリケーション詳細レポートに進みます。

レポート時間範囲の変更

ライセンス: 任意

レポートを表示するときは、[Time Range] リストを使用して、レポートに含める情報を定義する時間範囲を変更できます。時間範囲のリストは各レポートの上部に表示され、これを使用して最近 1 時間または 1 週間などの定義済みの時間範囲を選択したり、特定の開始時刻と終了時刻でカスタムの時間範囲を定義できます。選択した時間範囲は、選択を変更するまで、表示する他のすべてのレポートに引き継がれます。

レポートは 10 分ごとに自動的に更新されます。

ヒント モジュールの時間は、ご使用のワークステーションで設定されているタイムゾーンではなく、デバイスで定義されているタイム ゾーンに基づきます。

表 *80 :* レポートの時間範囲

時間範囲	戻されるデータ
直近の 30 分（Last 30 minutes）	5 分間隔で 30 分間と、追加で最大 5 分間。
過去 1 時間（Last hour）	5 分間隔で 60 分間と、追加で最大 5 分間。
直近の 24 時間（Last 24 hours）	直前の時間境界に丸めた、1 時間間隔で最近 24 時間。たとえば、現在時刻が 13:45 の場合、[Last 24 Hour] は昨日の 13:00 から今日の 13:00 までの期間になります。
過去 7 日（Last 7 days）	直前の時間境界に丸めた、1 時間間隔で最近 7 日間。
過去 30 日（Last 30 days）	直前の午前 0 時から始まり、1 日間隔で最近 30 日間。

時間範囲	戻されるデータ
カスタム範囲（Custom Range）	ユーザ定義の時間範囲。開始日、開始時刻、終了日、および終了時刻用に [Edit] ボックスが表示されます。各ボックスをクリックして、目的の値を選択します。作業が完了したら、[Apply] をクリックしてレポートを更新します。 カスタム時間範囲を作成する際、その範囲をデータ バケットの利用可能な範囲に揃える必要があります。過去 7～31 日の範囲の場合、クエリーを時に合わせます。古い範囲の場合は、その日に合わせます。1 年を超える範囲の場合は、週に合わせます。いずれの場合も、UTC 時間を使用して日の境界を規定します。クエリー、サーバ、クライアントの時間帯は、データ バケットに関連しません。たとえば、時間帯が太平洋夏時間（PDT）で、40 前からのデータをクエリーする場合、UTC（PDT に対して 8 時間のオフセット）に合わせて、Day 1 の 4PM、Day 2 の 4PM を使用します。

レポートに表示されるデータの制御

ライセンス：任意

概要レポートと詳細レポートには、トップ ポリシーや Web カテゴリなど、複数の下位レポートがあります。各レポートパネルにあるコントロールを使用すると、データのさまざまな側面を表示できます。次のコントロールを使用できます。

[Transactions] または [Data Usage]

これらのリンクをクリックすると、トランザクション数またはトランザクションのデータ量に基づいたグラフが表示されます。

[All]、[Denied]、[Allowed]

各レポートの右上にあるラベルのないリストに、これらのオプションがあります。これらを使用して、拒否接続のみ、許可接続のみ、あるいは拒否または許可にかかわらずすべての接続の表示に変更します。

[View More]

表示する項目のレポートに移動するには、[View More] リンクをクリックします。たとえば、[Destinations] レポートの [Web Categories] グラフで [View More] をクリックすると、[Web Categories] レポートに進みます。詳細レポートのレポートを表示している場合は、詳細を表示している項目の詳細な [Web Categories] レポートに移動します。

レポート カラムについて

ライセンス：任意

通常、レポートにはグラフ形式で表示される情報の加えて、情報を提供する 1 つ以上のテーブルが含まれています。

- 多くのカラムの意味は、そのカラムを含むレポートによって変わります。たとえば、トランザクションのカラムには、レポートの基準になる項目タイプのトランザクション数が示されます。[Values] または [Percentages] をクリックすることで、未処理の数値で行うか、項目に報告されたすべての未処理値の比率で行うか、値の切り替えを行うこともできます。
- カラム ヘッダーをクリックすると、カラムのソート順を変更できます。

次の表に、各種レポートで使用される標準のカラムの説明を示します。標準カラムはすべてのレポートにあり、可変カラムはその項目のレポートのみに表示されます。

表 *81 :* レポート カラム

カラム	説明
Transactions	報告された項目のトランザクション総数。上位レポートでは、番号がリンクになっています。表示している項目に基づいてフィルタリングされたイベントテーブルとともにイベント ビューアーを表示するには、そのリンクをクリックします。表示されるイベント数がトランザクション数と異なる場合があります。これは、ディスク スペースが不足すると、新しいイベントの到着時にストレージからイベントが削除されるためであり、特に古い期間のクエリで発生します。期間が 30 日間前より古いクエリーは、一致するイベントを返さないことがあります。逆に、トランザクション数よりも多くのイベントが表示されることがあります。これは、項目が対象時間範囲における各 5 分バケットの Top N に含まれない場合、トランザクション数にそれらの期間が含まれないためです。
Transactions allowed	報告された項目で許可されたトランザクションの数。
Transactions denied	報告された項目で（ポリシーに基づいて）ブロックされたトランザクションの数。
Total bytes	報告された項目の送受信バイト数の合計。
Bytes received	報告された項目の受信バイト数。
Total Bytes Sent	報告された項目の送信バイト数。

レポートの例

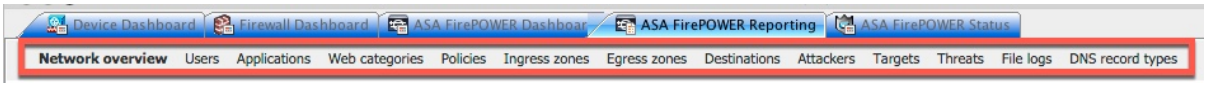
このセクションでは、ポリシー レポートを実行する方法について説明します。この手順で説明したタスクを使用して、別のレポートを実行できます。

レポートを実行するには、次の手順に従います。

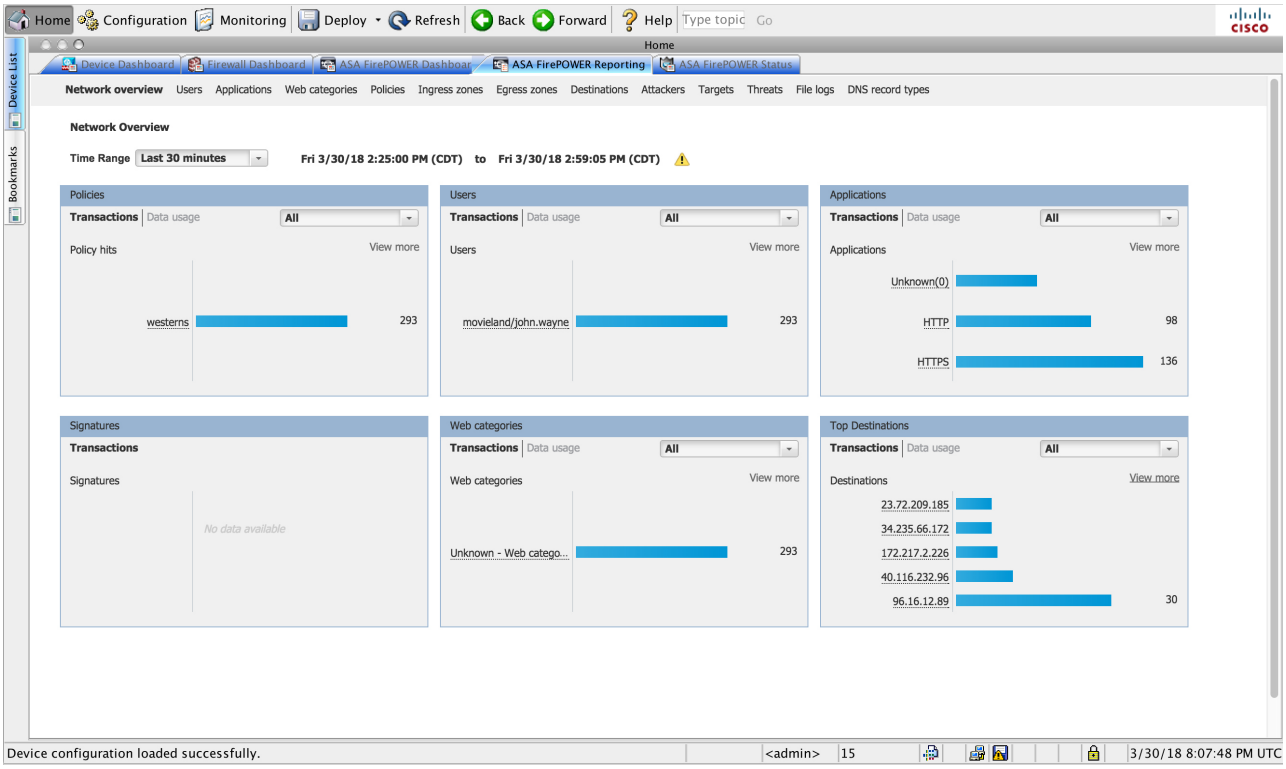
ステップ 1 ASA FirePOWER モジュールにログインします。

ステップ 2 [ホーム（Home）] > [ASA FirePOWER レポート（ASA FirePOWER Reporting）] をクリックします。

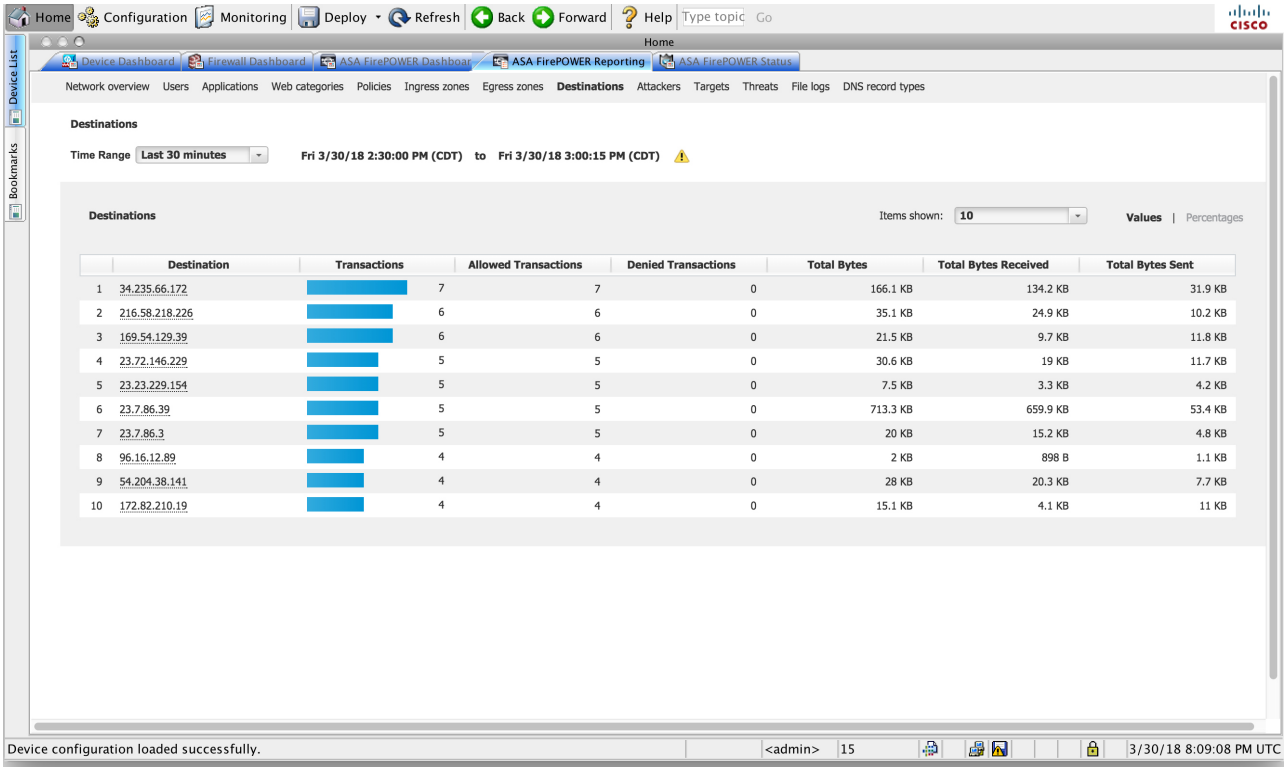
使用可能なレポートのタイプは、次の図に示すように、ウィンドウの上部に表示されます。



ステップ 3 多くのレポートで、レポートに含まれるカテゴリについての詳細を表示できます。たとえば、[ネットワークの概要（Network Overview）] をクリックします。

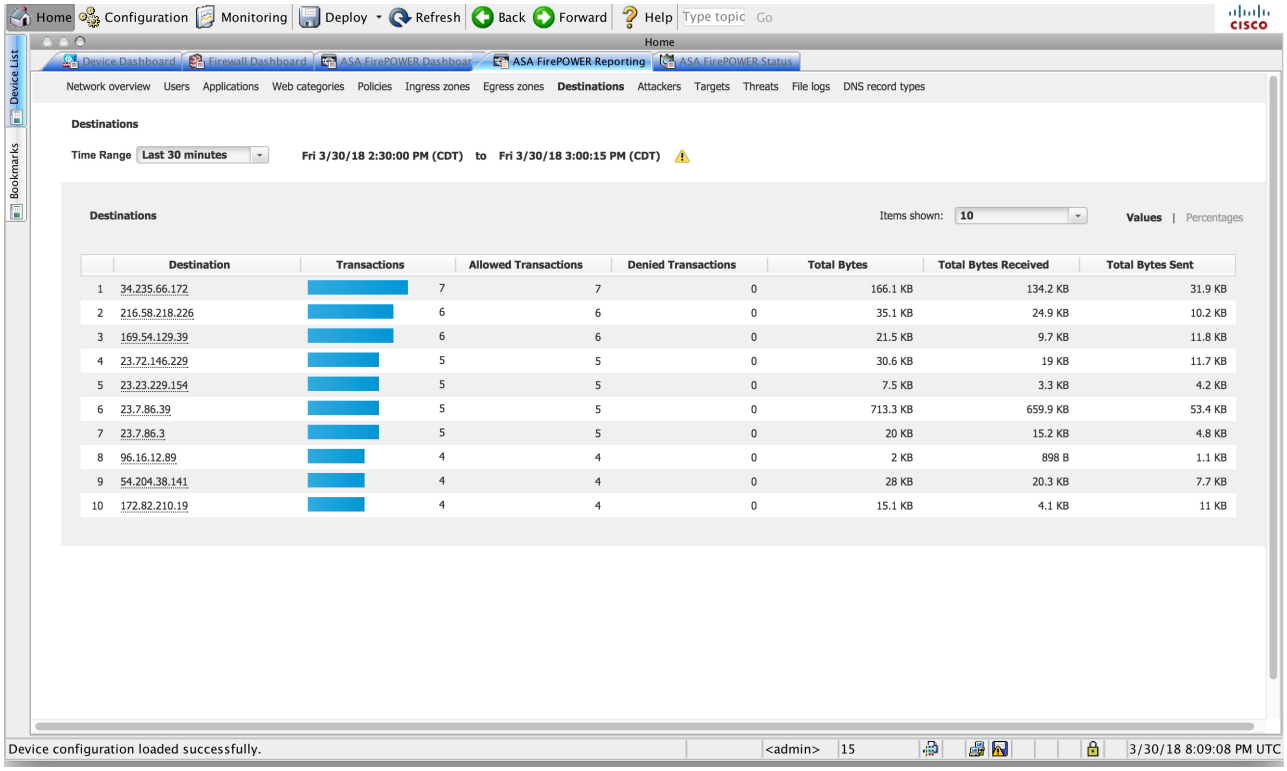


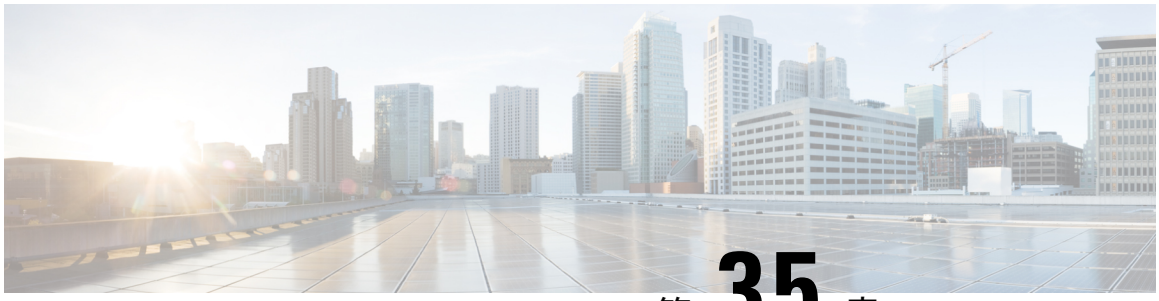
ステップ 4 [ネットワークの概要（Network Overview）] レポートの結果で、上位の宛先の名前をクリックして、宛先に関する詳細情報を取得します。



結果には、宛先についての概要情報と詳細が表示されます。

（オプション）[詳細情報（View More）] をクリックして、さらに詳しい情報を表示します。





第 35 章

タスクのスケジューリング

さまざまな種類の管理タスクを、指定した回数（1 度または繰り返し）実行するようにスケジュールを設定できます。

（注） タスクによっては、低帯域幅のネットワークにかなりの負荷をかける可能性があります（ソフトウェアの自動更新が関係するタスクなど）。ネットワーク使用率が低い時間帯にこのようなタスクを実行するよう、スケジュールしてください。

定期タスクの設定

ライセンス：任意

定期タスクの頻度を設定する際には、すべてのタイプのタスクで同じ手順に従います。

ユーザインターフェイスのほとんどのページに表示される時間はローカル時刻であり、ローカル設定で指定したタイム ゾーンに従ってそれが決定されます。さらに、ASA FirePOWER モジュールは、ローカル時刻の表示をサマータイム（DST）に合わせて自動的に調整します（該当する場合）。ただし、DST から標準時への移行日および元に戻る移行日をまたがる定期タスクは、移行を考慮して調整されません。つまり、標準時の午前 2:00 にタスク スケジュールを作成すると、DST 期間中は午前 3:00 に実行されます。同様に、DST の午前 2:00 にタスク スケジュールを作成すると、標準時には午前 1:00 に実行されます。

定期タスクを設定する方法：

ステップ 1 ASDM で、[Configuration] > [ASA FirePOWER Configuration] > [Tools] > [Scheduling] の順に選択します。

[Scheduling] ページが表示されます。

ステップ 2 [Add Task] をクリックします。

[New Task] ページが表示されます。

ステップ 3 [Job Type] リストから、スケジュールするタスクのタイプを選択します。

スケジュールできるタスク タイプについては、それぞれ該当するセクションで説明します。

ステップ 4 [Schedule task to run] オプションで、定期タスクを指定するために [Recurring] を選択します。

ページがリロードされ、定期タスクのオプションが示されます。

ステップ 5 [Start On] フィールドに、定期タスクを開始する日付を指定します。ドロップダウン リストを使用して月、日、年を選択できます。

ステップ 6 [Repeat Every] フィールドに、タスクを繰り返す頻度を指定します。時間、日、週、または月の数値を指定できます。

数値を入力するか、上矢印アイコン（▲）および下矢印アイコン（▼）をクリックして、間隔を指定できます。たとえば、2 日おきにタスクを実行するには、2 を入力して [Days] を選択します。

ステップ 7 [Run At] フィールドで、定期タスクを開始する時刻を指定します。

ステップ 8 [Repeat Every] で [Weeks] を選択した場合は、[Repeat On] フィールドが表示されます。タスクを実行する曜日の横にあるチェック ボックスを選択してください。

ステップ 9 [Repeat Every] で [Months] を選択した場合は、[Repeat On] フィールドが表示されます。ドロップダウン リストを使用して、タスクを実行する各月の日を選択します。

[New Task] ページ上のその他のオプションは、作成中のタスクに応じて異なります。

バックアップ ジョブの自動化

スケジューラを使用して、ASA FirePOWER モジュールのバックアップを自動化できます。バックアップをスケジュール済みタスクとして設定するには、その前にバックアップ プロファイルを設計する必要があります。詳細については、バックアップ プロファイルの作成 （607 ページ）を参照してください。

バックアップ タスクを自動化する方法：

ステップ 1 ASDM で、[Configuration] > [ASA FirePOWER Configuration] > [Tools] > [Scheduling] の順に選択します。

[Scheduling] ページが表示されます。

ステップ 2 [Add Task] をクリックします。

[New Task] ページが表示されます。

ステップ 3 [Job Type] リストから、[Backup] を選択します。

ページがリロードされ、バックアップのオプションが表示されます。

ステップ 4 バックアップをスケジュールする頻度として、ワンタイム タスクを示す [1 回（Once）] または定期タスクを示す [定期（Recurring）] を指定します。

- ワンタイム タスクの場合、ドロップダウン リストを使用して開始日時を指定します。[Current Time] フィールドには、アプライアンスの現在時刻が示されます。
- 定期タスクの場合、タスクのインスタンスの間隔を設定するオプションがいくつかあります。詳細については、定期タスクの設定 （537 ページ）を参照してください。

ステップ 5 [Job Name] フィールドに、 255 文字以内の英数字、スペース、ハイフンを使用して名前を入力します。

ステップ 6 [Backup Profile] リストから、適切なバックアップ プロファイルを選択します。

新しいバックアップ プロファイルの作成の詳細については、バックアップ プロファイルの作成 （607 ページ）を参照してください。

ステップ 7 オプションで、[Comment] フィールドに、255 文字以内の英数字、スペース、ピリオドを使用してコメントを入力します。

ヒント コメント フィールドはページの [View Tasks] セクションに表示されるので、ある程度短くしてください。

ステップ 8 オプションで、[Email Status To:] フィールドに、タスク ステータス メッセージの送信先となるメール アドレス（またはカンマで区切った複数のメール アドレス）を入力します。

ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。中継ホストの設定の詳細については、メール リレー ホストおよび通知アドレスの設定 （556 ページ）を参照してください。

ステップ 9 [**Save**] をクリックします。

タスクが追加されます。[Task Status] ページで、実行中のタスクの状態を確認できます（実行時間が長いタスクのステータスの表示 （625 ページ）を参照）。

侵入ポリシーの適用の自動化

ライセンス：Protection

ASA FirePOWER モジュールに侵入ポリシーを適用する操作をキューイングすることができます。このタスクの実行時点で、侵入ポリシーを参照するアクセス コントロール ポリシーが ASA

FirePOWERモジュールに適用されている場合のみ、このタスクは侵入ポリシーを適用します。それ以外の場合、このタスクは完了せずに終了します。

このタスクをスケジュールする前に、侵入ポリシーをアクセス コントロール ポリシーに関連付けて、アクセス コントロール ポリシーをデバイスに適用する必要があります。侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御 （171 ページ）を参照してください。

ポリシー適用のキューイング方法：

ステップ 1 ASDM で、[Configuration] > [ASA FirePOWER Configuration] > [Tools] > [Scheduling] の順に選択します。

現在の月のスケジュール カレンダー ページが表示されます。

ステップ 2 [Add Task] をクリックします。

[New Task] ページが表示されます。

ステップ 3 [ジョブ タイプ（Job Type）] リストから、[侵入ポリシー適用のキューイング（Queue Intrusion Policy Apply）] を選択します。

ページがリロードされ、ポリシー適用のキューイングに関するオプションが表示されます。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す[Once]または定期タスクを示す[Recurring]を指定します。

- ワンタイム タスクの場合、ドロップダウン リストを使用して開始日時を指定します。[Current Time]フィールドには、ASA FirePOWER モジュールの現在時刻が示されます。
- 定期タスクの場合、タスクのインスタンスの間隔を設定するオプションがいくつかあります。詳細については、定期タスクの設定 （537 ページ）を参照してください。

ステップ 5 [Job Name] フィールドに、 255 文字以内の英数字、スペース、ハイフンを使用して名前を入力します。

ステップ 6 [Intrusion Policy] フィールドで、次の操作を実行できます。

- ASA FirePOWER モジュールに適用する侵入ポリシーを選択します。
- [All intrusion policies] を選択して、ASA FirePOWER モジュールにすでに適用されているすべての侵入ポリシーを適用します。

ステップ 7 オプションで、[Comment]フィールドに、255 文字以内の英数字、スペース、ピリオドを使用してコメントを入力します。

ヒント スケジュール カレンダー ページの下部の [タスクの詳細（Task Details）] セクションにコメント フィールドが表示されるため、コメントの長さを制限してください。

ステップ 8 オプションで、[Email Status To:] フィールドに、タスク ステータス メッセージの送信先となるメール アドレス（またはカンマで区切った複数のメール アドレス）を入力します。

ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。中継ホストの設定の詳細については、メール リレー ホストおよび通知アドレスの設定 （556 ページ）を参照してください。

ステップ 9 [**Save**] をクリックします。

タスクが追加されます。カレンダー ページの [Task Details] セクションで、実行中のタスクの状態を確認できます（実行時間が長いタスクのステータスの表示 （625 ページ）を参照）。

ステップ 10 保存済みのタスクを編集するには、スケジュール カレンダー ページに表示されているタスクをクリックします。

[Task Details] セクションがページの下部に表示されます。変更を行うには、編集アイコン（）をクリックします。

位置情報データベースの更新の自動化

ライセンス：任意

スケジューラを使用して、位置情報データベース（GeoDB）の定期更新を自動化できます。GeoDB の定期更新は 7 日ごとに 1 度（週 1 回）実行されます。週ごとに更新が繰り返される時刻を設定できます。GeoDB 更新の詳細については、地理情報データベースについて （595 ページ）を参照してください。

位置情報データベースの更新を自動化する方法：

ステップ 1 ASDM で、[Configuration] > [ASA FirePOWER Configuration] > [Updates] を選択します。

[Product Updates] ページが表示されます。

ステップ 2 [Geolocation Updates] タブをクリックします。

[Geolocation Updates] ページが表示されます。

ステップ 3 [Recurring Geolocation Updates] の下で、[Enable Recurring Weekly Updates] チェック ボックスを選択します。

[Update Start Time] フィールドが表示されます。

ステップ 4 [Update Start Time] フィールドで、週ごとに GeoDB 更新を行う曜日と時刻を指定します。

ステップ 5 [**Save**] をクリックします。

タスクが追加されます。[Task Status] ページで、実行中のタスクの状態を確認できます（実行時間が長いタスクのステータスの表示 （625 ページ）を参照）。

ソフトウェア アップデートの自動化

ほとんどのパッチや機能リリースは、自動的にダウンロードして ASA FirePOWER モジュールに適用することができます。

（注） 手動で更新をアップロードしてインストールする必要が生じる状況が2つあります。最初に、ASA FirePOWER モジュールへのメジャー アップデートをスケジュールすることはできません。次に、サポートサイトにアクセスできないアプライアンスの更新や、そのアプライアンスからのプッシュをスケジュールすることはできません。ASA FirePOWER モジュールの手動更新の詳細については、ASA FirePOWER モジュール ソフトウェアの更新 （573 ページ）を参照してください。

このプロセスをより確実に制御するには、更新がリリースされたことがわかった後、[1 回（Once）] オプションを使用してオフピーク時間帯に更新をダウンロードしインストールできます。

ソフトウェア ダウンロードの自動化

Cisco から最新のソフトウェア更新を自動的にダウンロードするスケジュール済みタスクを作成することができます。このタスクを使用すると、手動でインストールする予定の更新のダウンロードをスケジュールできます。

ソフトウェア更新のダウンロードを自動化する方法：

ステップ 1 ASDM で、[Configuration] > [ASA FirePOWER Configuration] > [Tools] > [Scheduling] の順に選択します。

[Scheduling] ページが表示されます。

ステップ 2 [Add Task] をクリックします。

[New Task] ページが表示されます。

ステップ 3 [Job Type] リストから、[Download Latest Update] を選択します。

[New Task] ページがリロードされ、更新オプションが示されます。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [Once] または定期タスクを示す [Recurring] を指定します。

- ワンタイム タスクの場合、ドロップダウン リストを使用して開始日時を指定します。[Current Time] フィールドには、アプライアンスの現在時刻が示されます。
- 定期タスクの場合、タスクのインスタンスの間隔を設定するオプションがいくつかあります。詳細については、定期タスクの設定 （537 ページ）を参照してください。

ステップ 5 [Job Name] フィールドに、 255 文字以内の英数字、スペース、ハイフンを使用して名前を入力します。

ステップ 6 [Update Items] セクションで、[Software] を選択します。

ステップ 7 オプションで、[Comment] フィールドに、255 文字以内の英数字、スペース、ピリオドを使用してコメントを入力します。

ヒント コメント フィールドはページの [View Tasks] セクションに表示されるので、ある程度短くしてください。

ステップ 8 オプションで、[Email Status To:] フィールドに、タスク ステータス メッセージの送信先となるメール アドレス（またはカンマで区切った複数のメール アドレス）を入力します。

ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。中継ホストの設定の詳細については、メール リレー ホストおよび通知アドレスの設定 （556 ページ）を参照してください。

ステップ 9 [**Save**] をクリックします。

タスクが追加されます。[Task Status] ページで、実行中のタスクの状態を確認できます（実行時間が長いタスクのステータスの表示 （625 ページ）を参照）。

ソフトウェア インストールの自動化

注意 インストールする更新によっては、ソフトウェアのインストール後にアプライアンスがリブートする場合があります。

ソフトウェア インストール タスクをスケジュールする方法：

ステップ 1 ASDM で、[Configuration] > [ASA FirePOWER Configuration] > [Tools] > [Scheduling] の順に選択します。

[Scheduling] ページが表示されます。

ステップ 2 [Add Task] をクリックします。

[New Task] ページが表示されます。

ステップ 3 [Job Type] リストから、[Install Latest Update] を選択します。

ページがリロードされ、更新をインストールするためのオプションが表示されます。

ステップ 4 タスクをスケジュールする頻度として、ワンタイム タスクを示す [Once] または定期タスクを示す [Recurring] を指定します。

- ワンタイム タスクの場合、ドロップダウン リストを使用して開始日時を指定します。[Current Time] フィールドには、アプライアンスの現在時刻が示されます。
- 定期タスクの場合、タスクのインスタンスの間隔を設定するオプションがいくつかあります。詳細については、定期タスクの設定 （537 ページ）を参照してください。

ステップ 5 [Job Name] フィールドに、 255 文字以内の英数字、スペース、ハイフンを使用して名前を入力します。

ステップ 6 オプションで、[Comment] フィールドに、255 文字以内の英数字、スペース、ピリオドを使用してコメントを入力します。

ヒント コメント フィールドはページの [View Tasks] セクションに表示されるので、ある程度短くしてください。

ステップ 7 オプションで、[Email Status To:] フィールドに、タスク ステータス メッセージの送信先となるメール アドレス（またはカンマで区切った複数のメール アドレス）を入力します。

ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。中継ホストの設定の詳細については、メール リレー ホストおよび通知アドレスの設定 （556 ページ）を参照してください。

ステップ 8 [**Save**] をクリックします。

タスクが追加されます。[Task Status] ページで、実行中のタスクの状態を確認できます（実行時間が長いタスクのステータスの表示 （625 ページ）を参照）。

URL フィルタリング更新の自動化

ライセンス：URL Filtering

スケジューラを使用して、Collective Security Intelligence クラウドからの URL フィルタリング データの更新を自動化できます。URL フィルタリングを更新するタスクが正しく実行されるには：

- ASA FirePOWER モジュールがインターネットにアクセスできる必要があります。アクセスできない場合は、クラウドと通信できません。
- クラウド通信の有効化 （565 ページ）の説明に従って、URL フィルタリングを有効にする必要があります。

また、URL フィルタリングを有効にする際に、自動更新を有効にできることに注意してください。その場合、URL フィルタリング データの更新を確認するために、ASA FirePOWER モジュールは 30 分ごとにクラウドと通信します。自動更新がすでに有効になっている場合は、URL フィルタリング データを更新するスケジュール済みタスクを作成**しないでください**。

通常、毎日の更新は小規模ですが、最終更新日から 5 日を超えると、帯域幅によっては新しい URL フィルタリング データのダウンロードに最長 20 分かかる場合があります。その場合、アップデート自体の実行にも最大 30 分かかることがあります。

URL フィルタリング データのタスクを自動化する方法：

ステップ 1 ASDM で、[Configuration] > [ASA FirePOWER Configuration] > [Tools] > [Scheduling] の順に選択します。

[Scheduling] ページが表示されます。

ステップ 2 [Add Task] をクリックします。

[New Task] ページが表示されます。

ステップ 3 [Job Type] リストから、[Update URL Filtering Database] を選択します。

ページがリロードされ、URL フィルタリング更新のオプションが示されます。

ステップ 4 更新をスケジュールする頻度として、ワンタイム更新を示す [Once] または定期更新を示す [Recurring] を指定します。

- ワンタイム タスクの場合、ドロップダウン リストを使用して開始日時を指定します。[Current Time] フィールドには、アプライアンスの現在時刻が示されます。
- 定期タスクの場合、タスクのインスタンスの間隔を設定するオプションがいくつかあります。詳細については、定期タスクの設定 （537 ページ）を参照してください。

ステップ 5 [Job Name] フィールドに、 255 文字以内の英数字、スペース、ハイフンを使用して名前を入力します。

ステップ 6 オプションで、[Comment] フィールドに、255 文字以内の英数字、スペース、ピリオドを使用してコメントを入力します。

ヒント コメント フィールドはページの [View Tasks] セクションに表示されるので、ある程度短くしてください。

ステップ 7 オプションで、[Email Status To] フィールドに、タスク ステータス メッセージの送信先となるメール アドレス（またはカンマで区切った複数のメール アドレス）を入力します。

ステータス メッセージを送信するには、有効な電子メール中継サーバが設定されている必要があります。中継ホストの設定の詳細については、メール リレー ホストおよび通知アドレスの設定 （556 ページ）を参照してください。

ステップ 8 [**Save**] をクリックします。

タスクが追加されます。[Task Status] ページで、実行中のタスクの状態を確認できます（実行時間が長いタスクのステータスの表示 （625 ページ）を参照）。

タスクの表示

スケジュール済みタスクを追加した後、それらのタスクを表示したり、状態を評価したりできます。ページの [View Options] セクションで、カレンダーやスケジュール済みタスク リストを使用してスケジュール済みタスクを表示できます。

カレンダーの使用

カレンダー表示オプションを使用すると、どの日にどのスケジュール済みタスクが行われるかを表示できます。

カレンダーを使用してスケジュール済みタスクを表示する方法：

ステップ 1 ASDM で、[Configuration] > [ASA FirePOWER Configuration] > [Tools] > [Scheduling] の順に選択します。

[Scheduling] ページが表示されます。

ステップ 2 カレンダー ビューを使用して、次のタスクを実行できます。

- 二重左矢印アイコン（«）をクリックすると、1 年戻ります。
- 単一の左矢印アイコン（‹）をクリックすると、1 ヵ月戻ります。
- 単一の右矢印アイコン（›）をクリックすると、1 ヵ月進みます。
- 二重右矢印アイコン（»）をクリックすると、1 年進みます。
- [Today] をクリックすると、現在の年月に戻ります。
- [Add Task] をクリックすると、新しいタスクをスケジュールできます。
- 1 つの日付をクリックすると、カレンダーの下にあるタスク リスト表に、特定の日付のスケジュール済みタスクがすべて表示されます。
- ある日付の特定のタスクをクリックすると、カレンダーの下にあるタスク リスト表にそのタスクが表示されます。

（注） タスク リストの使用方法の詳細については、タスク リストの使用法（546 ページ）を参照してください。

タスク リストの使用法

タスク リストには、タスクのリストとその状態が表示されます。タスク リストき、カレンダーを開いたときにカレンダーの下にが表示されます。また、カレンダーで1つの日付またはタスクを選択してアクセスすることもできます。詳細については、「カレンダーの使用（545 ページ）」を参照してください。

表 *82*：タスク一覧のカラム

カラム	説明
Name	スケジュール済みタスクの名前と、関連付けられているコメントを表示します。
Type	スケジュール済みタスクのタイプを表示します。
Start Time	スケジュールされている開始日時を表示します。
Frequency	タスクの実行頻度を表示します。

カラム	説明
Status	スケジュール済みタスクの現在の状態を次のように示します。 • チェックマークアイコン（  ）は、タスクが正常に実行されたことを示します。 • 疑問符アイコン（  ）は、タスクの状態が不明であることを示します。 • 感嘆符アイコン（  ）は、タスクが失敗したことを示します .
Creator	スケジュール済みタスクを作成したユーザの名前を表示します。
Edit	スケジュール済みタスクを編集します。
Delete	スケジュール済みタスクを削除します。

スケジュール済みタスクの編集

以前に作成したスケジュール済みタスクを編集できます。この機能は、パラメータが正しいことを確認するために、スケジュール済みタスクを1度テストする場合に特に役立ちます。タスクが正常に完了したら、あとで定期タスクに変更できます。

既存のスケジュール済みタスクを編集する方法：

ステップ 1 ASDM で、[Configuration] > [ASA FirePOWER Configuration] > [Tools] > [Scheduling] の順に選択します。

[Scheduling] ページが表示されます。

ステップ 2 編集するタスク、またはタスクが表示されている日付をクリックします。

[Task Details] 表に、選択した 1 つ以上のタスクが示されます。

ステップ 3 この表で、編集するタスクを見つけて編集アイコン（  ）をクリックします。

[Edit Task] ページが表示され、選択したタスクの詳細が示されます。

ステップ 4 必要に応じて、タスクの開始時間、ジョブ名、コメント、実行頻度（1 度または繰り返し）などを編集します。ジョブのタイプを変更することはできません。

残りのオプションは、編集中のタスクに応じて異なります。

ステップ 5 [Save] をクリックして編集内容を保存します。

変更が保存され、[Scheduling] ページが再び表示されます。

スケジュール済みタスクの削除

[Schedule View] ページから 2 種類の削除操作を実行できます。まだ実行されていない特定のワンタイムタスク、または定期タスクのすべてのインスタンスを削除できます。定期タスクの1つのインスタンスを削除すると、そのタスクのすべてのインスタンスが削除されます。1 度だけ実行するようスケジュールされているタスクを削除すると、そのタスクだけが削除されます。

以下の項では、タスクを削除する方法について説明します。

- タスクのすべてのインスタンスを削除するには、定期タスクを削除します。
- タスクの 1 つのインスタンスを削除するには、ワンタイム タスクを削除します。

定期タスクの削除

定期タスクの1つのインスタンスを削除すると、そのタスクのすべてのインスタンスが自動的に削除されます。

定期タスクを削除する方法：

ステップ 1 ASDM で、[Configuration] > [ASA FirePOWER Configuration] > [Tools] > [Scheduling] の順に選択します。

[Scheduling] ページが表示されます。

ステップ 2 カレンダーで、削除する定期タスクのインスタンスを 1 つ選択します。

ページがリロードされ、カレンダーの下にタスクの表が表示されます。

ステップ 3 この表で、削除する定期タスクのインスタンスを見つけて、削除アイコン（）をクリックします。

その定期タスクのすべてのインスタンスが削除されます。

ワンタイム タスクの削除

タスク リストを使用して、スケジュール済みのワンタイム タスクを削除したり、以前に実行されたスケジュール済みタスクのレコードを削除したりできます。

1 つのタスク（そのタスクがすでに実行済みの場合はタスク レコード）を削除する方法：

ステップ 1 ASDM で、[Configuration] > [ASA FirePOWER Configuration] > [Tools] > [Scheduling] の順に選択します。

[Scheduling] ページが表示されます。

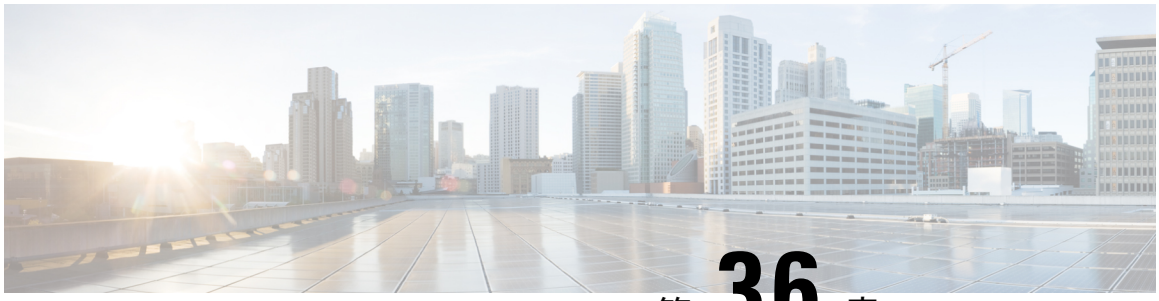
ステップ 2 削除するタスク、またはタスクが表示されている日付をクリックします。

選択した 1 つ以上のタスクを含む表が表示されます。

ステップ 3 この表で、削除するタスクを見つけて、削除アイコン（）をクリックします。

選択したタスクのインスタンスが削除されます。

次のタスク



第 36 章

システム ポリシーの管理

システム ポリシーを使用すると、ASA FirePOWER モジュールで次の管理を行うことができます。

- 監査ログ設定
- メール リレー ホストおよび通知アドレス
- SNMP ポーリング設定
- STIG コンプライアンス

システム ポリシーの作成

ライセンス：任意

システム ポリシーを設定する代わりに、別の ASA FirePOWER モジュールからシステム ポリシーをエクスポートして、ASA FirePOWER モジュールにインポートすることができます。必要に合わせて、インポートされたポリシーを編集してから、それを適用することができます。詳細については、設定のインポートおよびエクスポート （617 ページ）を参照してください。

システム ポリシーを作成する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Local] > [System Policy] の順に選択します。

[System Policy] ページが表示されます。

ステップ 2 ドロップダウン リストから、新しいシステム ポリシーのテンプレートとして使用する既存のポリシーを選択します。

ステップ 3 新しいポリシーの名前を [ポリシー名（Policy Name）] フィールドに入力します。

ステップ 4 新しいポリシーの説明を [ポリシーの説明（Policy Description）] フィールドに入力します。

ステップ 5 [作成（Create）] をクリックします。

システム ポリシーが保存され、[Edit System Policy] ページが表示されます。

システム ポリシーの編集

ライセンス：任意

ASA FirePOWER モジュールに現在適用されているシステム ポリシーを編集する場合は、変更を保存後にポリシーを再適用してください。詳細については、「システム ポリシーの適用 （552 ページ）」を参照してください。

既存のシステム ポリシーを編集する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Local] > [System Policy] の順に選択します。

既存のシステム ポリシーのリストを含む、[System Policy] ページが表示されます。

ステップ 2 システム ポリシーの横にある編集アイコン（  ）をクリックします。

[Edit Policy] ページが表示されます。ポリシー名とポリシーの説明を変更できます。ASA FirePOWER モジュールに適用されているシステム ポリシーを編集する場合は、編集が完了したら、更新したポリシーを再適用してください。システム ポリシーの適用 （552 ページ）を参照してください。

ステップ 3 [Save Policy and Exit] をクリックして変更を保存します。変更が保存され、[System Policy] ページが表示されます。

システム ポリシーの適用

ライセンス：任意

ASA FirePOWER モジュールには、システム ポリシーを適用できます。システム ポリシーがすでに適用されている場合、再適用するまで、ポリシーに加えた変更は有効になりません。

システム ポリシーを適用する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Local] > [System Policy] の順に選択します。

[System Policy] ページが表示されます。

ステップ 2 システム ポリシーの横にある適用アイコン（  ）をクリックします。

ステップ 3 [Apply] をクリックします。

[System Policy] ページが表示されます。メッセージはシステム ポリシーの適用のステータスを示します。

システム ポリシー ルールの削除

ライセンス：任意

システム ポリシー ルールは、ルールが使用中でも削除できます。ルールが使用中の場合は、新しいポリシーが適用されるまでそのルールが使用されます。システム ポリシーは削除できません。

システム ポリシー ルールを削除するには、次の手順を実行します。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Local] > [System Policy] の順に選択します。

[System Policy] ページが表示されます。

ステップ 2 システム ポリシー ルールの横にある削除アイコン（）をクリックします。ルールを削除するには、[OK] をクリックします。

[System Policy] ページが表示されます。ポリシーを削除するかどうか確認するポップアップ メッセージが表示されます。

アプライアンスのアクセス リストの設定

ライセンス：任意

さまざまなシステム ポリシーの設定を行うことができます。アプライアンスのアクセス リストの設定

ライセンス：任意

[Access List] ページを使用して、特定のポートのアプライアンスにコンピュータがアクセスできるかを制御できます。デフォルトでは、Webインターフェイスへのアクセスに使用するポート 443（Hypertext Transfer Protocol Secure（HTTPS））、コマンドラインへのアクセスに使用するポート 22（Secure Shell（SSH））が任意の IP アドレスに対して有効です。ポート 161 を介したSNMPアクセスを追加することもできます。SNMP情報をポーリングするには、使用する任意のコンピュータで SNMP アクセスを追加する必要があることに注意してください。

注意 デフォルトでは、アプライアンスへのアクセスは制限**されません**。よりセキュアな環境でアプライアンスを稼動させるために、特定の IP アドレスに対してアプライアンスへのアクセスを追加してから、デフォルトのオプションすべてを削除することを検討してください。

（注） SSH を介した CLI またはシェルへのログイン試行が 3 回連続して失敗すると、SSH 接続は終了します。

アクセス リストは、システム ポリシーの一部です。新しいシステム ポリシーを作成するか、既存のシステム ポリシーを編集することによって、アクセス リストを指定できます。いずれの場合も、システム ポリシーを適用するまでアクセス リストは有効になりません。

アクセス リストを設定するには、次の手順を実行します。

アクセス：管理者

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Local] > [System Policy] の順に選択します。

[System Policy] ページが表示されます。

ステップ 2 システム ポリシーの横にある編集アイコン（）をクリックします。

ステップ 3 必要に応じて、現在の設定の 1 つを削除するために、削除アイコンをクリックできます。

設定が削除されます。

注意 アプライアンスのインターフェイスへの接続に現在使用されている IP アドレスへのアクセスを削除し、「IP=any port=443」のエントリが存在しない場合、ポリシーを適用した時点でシステムへのアクセスは失われます。

ステップ 4 1 つ以上の IP アドレスへのアクセスを追加するために、[Add Rules] をクリックすることもできます。

[Add IP Address] ページが表示されます。

ステップ 5 [IP Address] フィールドでは、追加する IP アドレスに応じて以下の選択肢があります。

- 正確な IP アドレス（192.168.1.101 など）
- CIDR 表記を使用した IP アドレス ブロック（192.168.1.1/24 など）
- 任意の IP アドレスを示す any

ステップ 6 [SSH]、[HTTPS]、[SNMP]、またはこれらのオプションの組み合わせを選択して、これらの IP アドレスで有効にするポートを指定します。

ステップ 7 [Add] をクリックします。

[Access List] ページが再度表示され、行った変更が反映されます。

ステップ 8 [Save Policy and Exit] をクリックします。

システム ポリシーが更新されます。システム ポリシーを適用するまで変更は有効になりません。詳細については、「システム ポリシーの適用 （552 ページ）」を参照してください。

監査ログの設定

ライセンス：任意

ASA FirePOWER モジュールが外部ホストに監査ログをストリーミングするように、システム ポリシーを設定できます。

（注） 外部ホストが機能していて、監査ログを送信する ASA FirePOWER モジュールからアクセスできることを確認する必要があります。

送信元ホスト名は送信される情報の一部です。ファシリティ、重大度、およびオプションのタグを使用して監査ログ ストリームをより詳細に識別できます。ASA FirePOWER モジュールは、システム ポリシーが適用されるまで監査ログを送信しません。

この機能が有効になっている状態でポリシーが適用され、宛先ホストが監査ログを受け入れるように設定された後で、syslog メッセージが送信されます。次に、出力構造の例を示します。

Date Time Host [**Tag**] Sender: [**User_Name**]@[**User_IP**], [**Subsystem**], [**Action**

現地の日付、時刻、およびホスト名の後に、角括弧で囲まれたオプション タグが続き、送信側デバイス名の後に監査ログ メッセージが続きます。

次に例を示します。

Mar 01 14:45:24 localhost [**TAG**] Dev-DC3000: admin@10.1.1.2, **Operations** > **Monitoring**, **Page View**

監査ログの設定を行うには、次の手順を実行します。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Local] > [System Policy] の順に選択します。

[System Policy] ページが表示されます。

ステップ 2 システム ポリシーの横にある編集アイコン（）をクリックします。

ステップ 3 [Audit Log Settings] をクリックします。

[Audit Log Settings] ページが表示されます。

ステップ 4 [Send Audit Log to Syslog] ドロップダウン メニューから、[Enabled] を選択します。（デフォルト設定では [Disabled] になっています。）

ステップ 5 [Host] フィールドにあるホストの IP アドレスまたは完全修飾名を使用して、監査情報の宛先ホストを指定します。デフォルト ポート（514）が使用されます。

注意 監査ログを受け入れるように設定しているコンピュータが、リモート メッセージを受け入れるようにセットアップされていない場合、ホストは監査ログを受け入れません。

ステップ 6 [Facility] フィールドから syslog ファシリティを選択します。

ステップ 7 [Severity] フィールドから重大度を選択します。

ステップ 8 必要に応じて、[Tag (optional)] フィールドで参照タグを挿入します。

ステップ 9 外部 HTTP サーバに定期的な監査ログの更新を送信するには、[Send Audit Log to HTTP Server] ドロップダウン リストから [Enabled] を選択します。デフォルト設定では [Disabled] になっています。

ステップ 10 [URL to Post Audit] フィールドに、監査情報を送信する URL を指定します。次にリストされている HTTP POST 変数を要求するリスナー プログラムに対応する URL を入力する必要があります。

- subsystem
- actor
- event_type
- message
- action_source_ip
- action_destination_ip
- result
- time
- tag（上記のように定義されている場合）

注意 暗号化されたポストを許可するには、HTTPS URL を使用する必要があります。外部 URL に監査情報を送信すると、システム パフォーマンスに影響を与える場合があるので注意してください。

ステップ 11 [Save Policy and Exit] をクリックします。

システム ポリシーが更新されます。システム ポリシーを適用するまで変更は有効になりません。詳細については、「システム ポリシーの適用 （552 ページ）」を参照してください。

メール リレー ホストおよび通知アドレスの設定

ライセンス：任意

次の処理を行う場合、メール ホストを設定する必要があります。

- イベント ベースのレポートの電子メール送信
- スケジュールされたタスクのステータス レポートの電子メール送信
- 変更調整レポートの電子メール送信
- データ切り捨て通知の電子メール送信

- 侵入イベント アラートについての電子メールの使用

アプライアンスとメール リレー ホストとの間の通信に使用する暗号化方式を選択し、メール サーバの認証資格情報を指定できます（必要な場合）。設定を行った後、指定された設定を使用してアプライアンスとメール サーバとの間の接続をテストできます。

メール リレー ホストを設定するには、次の手順を実行します。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Local] > [System Policy] の順に選択します。

[System Policy] ページが表示されます。

ステップ 2 システム ポリシーの横にある編集アイコン（  ）をクリックします。

ステップ 3 [Email Notification] をクリックします。

[Configure Email Notification] ページが表示されます。

ステップ 4 [Mail Relay Host] フィールドで、使用するメール サーバのホスト名または IP アドレスを入力します。

（注） 入力したメール ホストはアプライアンスからのアクセスを許可している必要があります。

ステップ 5 [Port Number] フィールドに、電子メール サーバで使用するポート番号を入力します。ポートは通常、暗号化を使用しない場合は 25、SSLv3 を使用する場合は 465、TLS を使用する場合は 587 です。

ステップ 6 暗号化方式を選択するには、次のオプションがあります。

- Transport Layer Security を使用してアプライアンスとメール サーバとの間の通信を暗号化するには、[Encryption Method] ドロップダウン リストから [TLS] を選択します。
- セキュア ソケット レイヤを使用してアプライアンスとメール サーバとの間の通信を暗号化するには、[Encryption Method] ドロップダウン リストから [SSLv3] を選択します。
- アプライアンスとメール サーバとの間の非暗号化通信を許可するには、[Encryption Method] ドロップダウン リストから [None] を選択します。

アプライアンスとメール サーバとの間の暗号化された通信では、証明書の検証は不要であることに注意してください。

ステップ 7 アプライアンスによって送信されるメッセージの送信元の電子メール アドレスとして使用する有効な電子メール アドレスを、[From Address] フィールドに入力します。

ステップ 8 必要に応じて、メールサーバに接続する際にユーザ名とパスワードを指定するために、[Use Authentication] を選択します。[Username] フィールドにユーザー名を入力します。パスワードを [Password] フィールドに入力します。

ステップ 9 設定したメール サーバを使用してテスト メールを送信するには、[Test Mail Server Settings] をクリックします。

テストの成功または失敗を示すメッセージがボタンの横に表示されます。

ステップ 10 [Save Policy and Exit] をクリックします。

システム ポリシーが更新されます。システム ポリシーを適用するまで変更は有効になりません。詳細については、「システム ポリシーの適用 （552 ページ）」を参照してください。

SNMP ポーリングの設定

ライセンス：任意

システム ポリシーを使用してアプライアンスの Simple Network Management Protocol（SNMP）ポーリングを有効にできます。SNMP 機能は、SNMP プロトコルのバージョン 1、2、および 3 をサポートします。

システム ポリシー SNMP 機能を有効にすると、アプライアンスで SNMP トラップを送信できなくなり、MIB の情報はネットワーク管理システムによるポーリングでのみ使用可能になることに注意してください。

（注） アプライアンスをポーリングするには、使用する任意のコンピュータで SNMP アクセスを追加する必要があります。詳細については、アプライアンスのアクセス リストの設定 （553 ページ）を参照してください。SNMP MIB にはアプライアンスの攻撃に使用される可能性のある情報も含まれることに注意してください。SNMP アクセスのアクセス リストを MIB のポーリングに使用される特定のホストに制限することをお勧めします。SNMPv3 を使用し、ネットワーク管理アクセスには強力なパスワードを使用することもお勧めします。

SNMP ポーリングを設定するには、次の手順を実行します。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Local] > [System Policy] の順に選択します。

[System Policy] ページが表示されます。

ステップ 2 システム ポリシーの横にある編集アイコン（）をクリックします。

ステップ 3 アプライアンスをポーリングするために使用するコンピュータごとに SNMP アクセスをまだ追加していない場合は、ここで追加してください。詳細については、アプライアンスのアクセス リストの設定 （553 ページ）を参照してください。

ステップ 4 [SNMP] をクリックします。

[SNMP] ページが表示されます。

ステップ 5 [SNMP Version] ドロップダウン リストから、使用する SNMP バージョンを選択します。

ドロップダウン リストに選択したバージョンが表示されます。

ステップ 6 次の選択肢があります。

- [Version 1] または [Version 2] を選択した場合、[Community String] フィールドに SNMP コミュニティ名を入力します。ステップ 15 に進みます。

- [Version 3] を選択した場合、[Add User] をクリックするとユーザ定義ページが表示されます。

ステップ 7 [Username] フィールドにユーザ名を入力します。

ステップ 8 [Authentication Protocol] ドロップダウン リストから、認証に使用するプロトコルを選択します。

ステップ 9 [Authentication Password] フィールドに SNMP サーバの認証に必要なパスワードを入力します。

ステップ 10 [Authentication Password] フィールドのすぐ下にある [Verify Password] フィールドに認証パスワードを再入力します。

ステップ 11 使用するプライバシー プロトコルを [Privacy Protocol] リストから選択するか、プライバシー プロトコルを使用しない場合は [None] を選択します。

ステップ 12 [Privacy Password] フィールドに SNMP サーバで必要な SNMP プライバシー キーを入力します。

ステップ 13 [Privacy Password] フィールドのすぐ下にある [Verify Password] フィールドにプライバシー パスワードを再入力します。

ステップ 14 [Add] をクリックします。

ユーザが追加されます。ステップ 6 ～ 13 までを繰り返して、さらにユーザを追加できます。ユーザを削除するには、削除アイコン（）をクリックします。

ステップ 15 [Save Policy and Exit] をクリックします。

システム ポリシーが更新されます。システム ポリシーを適用するまで変更は有効になりません。詳細については、「システム ポリシーの適用 （552 ページ）」を参照してください。

STIG コンプライアンスの有効化

ライセンス：任意

米国連邦政府内の組織は、Security Technical Implementation Guides（STIG）に示されている一連のセキュリティ チェックリストに準拠しなければならない場合があります。STIG コンプライアンス オプションは、米国国防総省によって定められた特定の要件に準拠することを目的とした設定を有効にします。

STIG コンプライアンスを有効にした場合、適用可能なすべての STIG に対する厳格なコンプライアンスは保証されません。

STIG コンプライアンスを有効にすると、ローカル シェル アクセス アカウントのパスワードの複雑さや維持に関するルールが変わります。さらに、STIG コンプライアンス モードでは、ssh のリモート ストレージを使用できません。

STIG コンプライアンスが有効なシステム ポリシーを適用すると、アプライアンスは強制的にリブートされることに注意してください。STIG が有効なシステム ポリシーをすでに STIG が有効になっているアプライアンスに適用した場合、アプライアンスはリブートしません。STIG が無効なシステム ポリシーを STIG が有効になっているアプライアンスに適用した場合、STIG は引き続き有効であり、アプライアンスはリブートしません。

⚠

注意 サポートからの支援なしでこの設定を無効にすることはできません。また、この設定はシステムのパフォーマンスに大きく影響する可能性があります。シスコでは、米国国防総省（DoD）のセキュリティ要件に準拠する以外の目的で、STIG コンプライアンスを有効にすることを推奨しません。

STIG コンプライアンスを有効にするには、次の手順を実行します。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Local] > [System Policy] の順に選択します。

[System Policy] ページが表示されます。

ステップ 2 システム ポリシーの横にある編集アイコン（✎）をクリックします。

ステップ 3 [STIG Compliance] をクリックします。

[STIG Compliance] ページが表示されます。

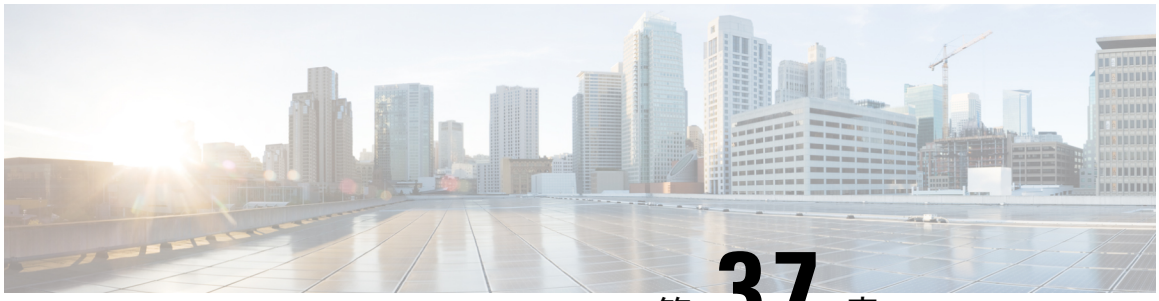
ステップ 4 STIG コンプライアンスをアプライアンスで永続的に有効にする場合は、[Enable STIG Compliance] を選択します。

注意 STIG コンプライアンスが有効なポリシーを適用した後に、STIG コンプライアンスをアプライアンスで無効にすることはできません。コンプライアンスを無効にする必要がある場合は、サポートに連絡してください。

ステップ 5 [Save Policy and Exit] をクリックします。

システム ポリシーが更新されます。システム ポリシーを適用するまで変更は有効になりません。詳細については、「システム ポリシーの適用 （552 ページ）」を参照してください。

アプライアンスに対して STIG コンプライアンスを有効にするシステム ポリシーを適用した場合、アプライアンスがリブートすることに注意してください。STIG が有効なシステム ポリシーをすでに STIG が有効になっているアプライアンスに適用した場合は、アプライアンスはリブートしないことに注意してください。



第 37 章

ASA FirePOWER モジュール設定の構成

次の表は、ASA FirePOWER モジュールのローカル設定をまとめたものです。

表 *83 :* ローカル構成のオプション

オプション	説明
情報	アプライアンスに関する現在の情報が表示されます。アプライアンスの名前を変更することもできます。
[Cisco CSI][クラウドサービス（Cloud Services）]	Collective Security Intelligence クラウドから URL フィルタリングデータをダウンロードしたり、未分類の URL を検索したり、検出されたファイルの診断情報をシスコに送信したりできます。

アプライアンス情報の表示と変更

ライセンス：任意

[Information] ページには、ASA FirePOWER モジュールに関する情報が表示されます。情報には、製品名とモデル番号、オペレーティングシステムとバージョン、現在のシステムポリシーなどの読み取り専用の情報が含まれます。このページには、アプライアンスの名前を変更するオプションも用意されています。

次の表で、各フィールドについて説明します。

表 *84 : Appliance Information*

フィールド	説明
Name	アプライアンスに割り当てられた名前。この名前はASA FirePOWERモジュールのコンテキスト内でのみ使用されます。ホスト名をアプライアンスの名前として使用できますが、このフィールドに別の名前を入力しても、ホスト名は変更されません。
Product Model	アプライアンスのモデル名。
Serial Number	アプライアンスのシャーシのシリアル番号。
Software Version	現在インストールされているソフトウェアのバージョン。
Operating System	アプライアンス上で現在実行されているオペレーティングシステム。
Operating System Version	アプライアンス上で現在実行されているオペレーティング システムのバージョン。
IPv4 Address	アプライアンスのデフォルトの管理インターフェイス（eth0）のIPv4アドレス。アプライアンスでIPv4の管理が無効になっている場合は、このフィールドにそのことが示されます。
IPv6 Address	アプライアンスのデフォルトの管理インターフェイス（eth0）のIPv6アドレス。アプライアンスでIPv6の管理が無効になっている場合は、このフィールドにそのことが示されます。
Current Policies	現在適用されているアプライアンスレベルのポリシー。ポリシーが最後に適用された後で更新されていると、ポリシーの名前がイタリック体で表示されます。
Model Number	アプライアンスのモデル番号。この番号は、トラブルシューティングで重要になる場合があります。

アプライアンスの情報を変更する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Local] > [Configuration] の順に選択します。

[Information] ページが表示されます。

ステップ 2 アプライアンス名を変更するには、[Name] フィールドに新しい名前を入力します。

名前は、英数字である**必要があり**、数字だけで構成することはできません。

ステップ 3 変更を保存するには、[Save] をクリックします。

ページが更新され、変更が保存されます。

URL フィルタリングとマルウェア検出のクラウドコミュニケーションのオプション

ライセンス：URL Filtering または Malware

ASA FirePOWER モジュールは、さまざまな種類の情報を取得するためにシスコの Collective Security Intelligence クラウドにアクセスします。

- アクセス コントロール ルールに関連付けられたファイル ポリシーにより、デバイスは、ネットワーク トラフィックで送信されるファイルを検出できます。ASA FirePOWER モジュールは、Cisco Cloud からのデータを使用して、ファイルがマルウェアに相当するかどうかを判定します。ファイル ポリシーの概要と作成（453 ページ）を参照してください。
- URL フィルタリングを有効にすると、ASA FirePOWER モジュールはよくアクセスされる多くの URL のカテゴリとレピュテーション データを取得し、未分類の URL を検索できます。その後、アクセス コントロール ルールの URL 条件をすばやく作成できます。URL カテゴリとレピュテーションに基づく URL のブロッキング（147 ページ）を参照してください。

ASA FirePOWER モジュールのローカル設定を使用して、次のオプションを指定します。

Enable URL Filtering

カテゴリおよびレピュテーションベースの URL フィルタリングを実行するには、このオプションを有効にする必要があります。

Enable Automatic Updates

システムが定期的にクラウドに接続し、アプライアンスのローカルデータセット内の URL カテゴリとレピュテーションのデータに対する更新を取得できるようにしますクラウドでは通常、データが 1 日に 1 回更新されますが、自動更新を有効にすると、ASA FirePOWER モジュールによるチェックが 30 分ごとに強制的に行われ、常に最新の情報が保持されるようになります。

通常、毎日の更新は小規模ですが、最終更新日から 5 日を超えると、帯域幅によっては新しい URL フィルタリング データのダウンロードに最長 20 分かかる場合があります。その場合、アップデート自体の実行にも最大 30 分かかることがあります。

システムがクラウドに接続するタイミングを厳密に制御する必要がある場合は、URL フィルタリング更新の自動化（544 ページ）で説明しているように、自動更新を無効にして、代わりにスケジューラを使用できます。

（注） Cisco では、自動更新を有効にするか、またはスケジューラを使用して更新をスケジュールすることを推奨しています。手動でオンデマンド更新を実行することもできますが、システムによるクラウドへの定期的な接続を自動化することで、最も関連性の高い最新の URL データを取得できます。

Query Cloud for Unknown URL

監視対象ネットワーク上で誰かがローカル データ セットに存在しない URL を参照しようとしたときに、システムがクラウドを照会できるようにします。

クラウドが URL のカテゴリまたはレピュテーションを識別できない場合や、ASA FirePOWER モジュールがクラウドに接続できない場合、その URL は、カテゴリまたはレピュテーション ベースの URL 条件を含むアクセス コントロール ルールと一致しません。URL にカテゴリやレピュテーションを手動で割り当てることはできません。

プライバシー上の理由などで、未分類の URL を Cisco Cloud でカタログ化したくない場合は、このオプションを無効にします。

キャッシュされた URL の期限切れ

この設定は、[不明 URL を Cisco CSI に問い合わせる（Query Cisco CSI for Unknown URL）][不明 URL を Cisco Cloud に問い合わせる（Query Cisco Cloud for Unknown URLs）] が有効になっている場合にのみ該当します。

古いデータと一致する URL のインスタンスを最小限に抑えるため、キャッシュ内の URL を期限切れに設定できます。脅威データの正確性と即時性を向上させるため、短い有効期限を選択します。

カテゴリおよびレピュテーション データのキャッシングにより、Web ブラウジングが高速化されます。デフォルトでは、最速のパフォーマンスを得るため、URL のキャッシュされたデータの有効期限はありません。

キャッシュされた URL は、指定された時間が経過した後、ネットワーク上のユーザが初めてアクセスした後に更新されます。最初のユーザに更新済みの結果は表示されませんが、この URL に次にアクセスしたユーザには更新済みの結果が表示されます。

Licensing

カテゴリおよびレピュテーションベースの URL フィルタリングとデバイスベースのマルウェア検出を実行するには、ASA FirePOWER モジュールで適切なライセンスを有効にする必要があります（ASA FirePOWER モジュールのライセンス （567 ページ）を参照）。

ASA FirePOWER モジュールに URL Filtering ライセンスがない場合、クラウド接続オプションを設定することはできません。クラウドサービスのローカル設定ページには、ライセンスが供与されているオプションのみが表示されます。ライセンスが期限切れになっている ASA FirePOWER モジュールは、クラウドに接続できません。

ASA FirePOWER モジュールに URL Filtering ライセンスを追加すると、URL フィルタリングの設定オプションが表示されるのに加えて、[Enable URL Filtering] と [Enable Automatic Updates] が自動的に有効になります。必要な場合は、手動でこれらのオプションを無効にすることができます。

Internet Access

Cisco Cloud への接続にはポート 80/HTTP および 443/HTTPS が使用されます。

次の手順では、Cisco Cloud との通信を有効にする方法と、URL データのオンデマンド更新を実行する方法について説明します。更新がすでに進行中である場合は、オンデマンド更新を開始できません。

クラウド通信の有効化

クラウドとの通信を有効にする方法：

ステップ 1 アプライアンスが次のすべての URL で Cisco Cloud と通信できることを確認します。

https://regsvc.sco.cisco.com

https://est.sco.cisco.com

https://updates-talos.sco.cisco.com

http://updates.ironport.com

https://v3.sds.cisco.com

ステップ 2 [Configuration] > [ASA FirePOWER Configuration] > [Integration] > **[Cloud Services]** を選択します。

[Information] ページが表示されます。

ステップ 3 **[Cloud Services]** をクリックします。

[Cloud Services] ページが表示されます。URL Filtering ライセンスがある場合は、このページに URL データの最終更新時間が表示されます。

ステップ 4 上記の説明に従って、クラウド接続のオプションを構成します。

[Enable Automatic Updates] または [Query Cloud for Unknown URLs] を有効にするには、あらかじめ [Enable URL Filtering] を有効にする必要があります。

ステップ 5 [**Save**] をクリックします。

設定が保存されます。URL フィルタリングを有効にした場合、URL フィルタリングが最後に有効になってからの経過時間、または URL フィルタリングを初めて有効にしたかどうかに応じて、ASA FirePOWER モジュールがクラウドから URL フィルタリング データを取得します。

次のタスク

- システムの URL データのオンデマンド更新を実行する方法：

1. [Configuration] > [ASA FirePOWER Configuration] > [Local] > [Configuration] の順に選択します。

   [Information] ページが表示されます。

2. [URL Filtering] をクリックします。

   [URL Filtering] ページが表示されます。

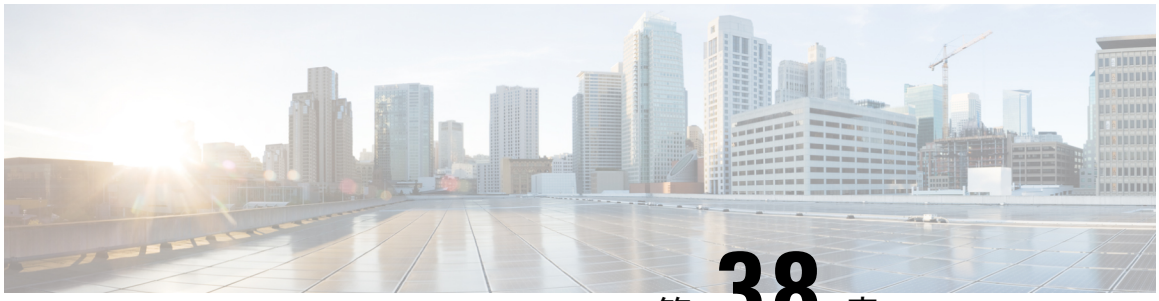
3. [Update Now] をクリックします。

   ASA FirePOWER モジュールがクラウドに接続し、更新が利用可能な場合はその URL フィルタリング データを更新します。

システム情報

時刻（Time）

ASA FirePOWER モジュールの現在時刻と時刻源は、[Time] ページを使用して確認できます。



第 38 章

ASA FirePOWER モジュールのライセンス

ライセンスについて

ライセンス：任意

組織に対して ASA FirePOWER モジュールの最適な展開を実現するために、さまざまな機能のライセンスを付与できます。

ライセンスにより、デバイスは以下を含むさまざまな機能を実行できます。

- 侵入検知および防御
- Security Intelligence フィルタリング
- ファイル制御および拡張マルウェア対策
- アプリケーション、ユーザ、および URL 制御

ASA FirePOWER モジュールでライセンス付き機能にアクセスできなくなる状況がいくつかあります。ライセンス付きの機能は削除できます。いくつかの例外がありますが、期限切れライセンスまたは削除済みライセンスに関連付けられている機能は使用できません。

ここでは、 ASA FirePOWER モジュールの展開環境で使用可能なライセンスのタイプについて説明します。アプライアンス上で有効にできるライセンスは、有効になっている他のライセンスに依存します。

次の表に、ASA FirePOWER モジュール ライセンスの概要を示します。

表 *85 : ASA FirePOWER* モジュール ライセンス

ライセンス	付与される機能	要件
Protection	侵入検知と防御 ファイル制御 Security Intelligence フィルタリング	なし
Control	ユーザおよびアプリケーション制御	プロテクション
Malware	高度なマルウェア防御（ネットワークベースのマルウェアの検出とブロッキング）	Protection
URL フィルタリング	カテゴリとレピュテーションに基づく URL フィルタリング	プロテクション

Protection

ライセンス：Protection

プロテクション ライセンスでは、侵入検知および防御、ファイル制御、およびセキュリティ インテリジェンス フィルタリングを実行できます。

- 侵入検知および防御により、侵入とエクスプロイトを検出するためネットワーク トラフィックを分析できます。またオプションで違反パケットをドロップできます。
- ファイル制御により、特定のアプリケーションプロトコルを介した特定タイプのファイルを検出し、オプションでこれらのファイルのアップロード（送信）またはダウンロード（受信）をブロックできます。Malware ライセンス（Malware （570 ページ）を参照）では、マルウェアの性質に基づいて限られたファイル タイプを検査およびブロックすることもできます。
- セキュリティ インテリジェンス フィルタリングにより、トラフィックをアクセス制御ルールによる分析対象にする前に、特定の IP アドレスをブロック（その IP アドレスとの間のトラフィックを拒否）できます。ダイナミックフィードにより、最新の情報に基づいて接続をただちにブロックできます。オプションで、Security Intelligence フィルタリングに「監視のみ」設定を使用できます。

ライセンスがない状態でも Protection 関連の検査を実行するようにアクセス コントロール ポリシーを設定できますが、最初に Protection ライセンスを ASA FirePOWER モジュールに追加するまではポリシーを適用できません。

ASA FirePOWER モジュールから Protection ライセンスを削除すると、ASA FirePOWER モジュールは侵入イベントとファイル イベントの検出を停止します。また、ASA FirePOWER モジュールはシスコ提供またはサードパーティのセキュリティ インテリジェンス情報を取得するためにインターネットに接続しなくなります。Protection を再度有効にするまで、既存ポリシーは再適用できません。

プロテクション ライセンスは URL フィルタリング、マルウェア、および制御ライセンスに必要であるため、プロテクションライセンスを削除または無効にすると、URL フィルタリング、マルウェア、または制御ライセンスを削除または無効にすることと同じ効果があります。

Control

ライセンス：Control

制御ライセンスでは、アクセス コントロール ルールにユーザとアプリケーションの条件を追加することで、ユーザとアプリケーションの制御を実装できます。Control を有効にするには、Protection も有効にする必要があります。

Control ライセンスがない状態でもアクセス コントロール ルールにユーザ条件とアプリケーション条件を追加できますが、Control ライセンスを ASA FirePOWER モジュールに追加するまで、ポリシーは適用できません。

Control ライセンスを削除する場合、既存のアクセス コントロール ポリシーにユーザ条件またはアプリケーション条件があるルールが含まれていると、それらのポリシーは再適用できません。

URL フィルタリング

ライセンス：URL Filtering

URL フィルタリングを使用すると、監視対象ホストにより要求される URL に基づいてネットワークを移動可能なトラフィックを判別するアクセス コントロール ルールを作成し、ASA FirePOWER モジュールが Cisco Cloud から取得する URL に関する情報に関連付けることができます。URL フィルタリングを有効にするには、Protection ライセンスも有効にする必要があります。

ヒント URL フィルタリング ライセンスがない状態で、許可またはブロックする個別 URL または URL グループを指定できます。これにより、Web トラフィックをカスタムできめ細かく制御できますが、URL カテゴリおよびレピュテーション データをネットワーク トラフィックのフィルタリングに使用することはできません。

URL フィルタリングにはサブスクリプション ベースの URL Filtering ライセンスが必要です。URL Filtering ライセンスがない状態でも、アクセス コントロール ルールにカテゴリ ベースおよびレピュテーション ベースの URL 条件を追加できますが、 ASA FirePOWER モジュールは URL 情報を取得するためにクラウドに接続しません。アクセス コントロール ポリシーは、URL Filtering ライセンスを ASA FirePOWER モジュールに追加するまで適用できません。

ASA FirePOWER モジュールからライセンスを削除すると、URL フィルタリングにアクセスできなくなることがあります。また、URL フィルタリング ライセンスの有効期限が切れることもあります。ライセンスが期限切れになるか、またはライセンスを削除すると、URL 条件を含むアクセス コントロール ルールは URL のフィルタリングをすぐに停止し、ASA FirePOWER モジュールはクラウドにアクセスできなくなります。既存のアクセス制御ポリシーに、カテゴ

リ ベースまたはレピュテーション ベースの URL 条件を含むルールが含まれている場合は、それらのポリシーを再適用することができません。

Malware

ライセンス：Malware

Malware ライセンスでは高度なマルウェア防御を実行できます。つまり、デバイスを使用して、ネットワーク上で送信されるファイルのマルウェアを検出してブロックできます。デバイスの Malware ライセンスを有効にするには、Protection も有効にする必要があります。

ファイル ポリシーの一部としてマルウェア検出を設定し、その後 1 つ以上のアクセス制御ルールを関連付けます。ファイル ポリシーは、特定のアプリケーション プロトコルを使用して特定のファイルをアップロードまたはダウンロードするユーザを検出できます。Malware ライセンスでは、限定された一連のファイル タイプでマルウェアを検査できます。Malware ライセンスでは、ファイル リストに特定のファイルを追加し、そのファイル リストをファイル ポリシー内で有効にすることもできます。これにより、検出時にこれらのファイルを自動的に許可またはブロックできます。

Malware ライセンスがなくてもアクセス コントロール ルールにマルウェア検出ファイル ポリシーを追加できますが、アクセス コントロール ルール エディタでは、そのファイル ポリシーは警告アイコン付きで表示されます。ファイル ポリシー内でも、マルウェア クラウド検索ルールに警告アイコンが付きます。マルウェア検出ファイル ポリシーを含むアクセス コントロール ポリシーを適用する前に、Malware ライセンスを追加する必要があります。後でライセンスを削除すると、マルウェア検出を実行するファイル ポリシーが含まれている既存のアクセス コントロール ポリシーを、これらのデバイスに対して再適用することはできません。

Malware ライセンスを削除するか、またはライセンスが期限切れになると、ASA FirePOWER モジュールはマルウェア クラウド ルックアップの実行を停止し、Cisco Cloud から送信されるレトロスペクティブ イベントの確認も停止します。既存のアクセス コントロール ポリシーにマルウェア検出を実行するファイル ポリシーが含まれている場合、このアクセス コントロール ポリシーを再適用することはできません。Malware ライセンスの期限切れまたは削除後のごく短い時間においては、マルウェア クラウド ルックアップ ファイル ルールで検出されたファイルのキャッシュされた性質を、システムが使用できることに注意してください。この時間枠の経過後は、システムは検索を実行せず Unavailable という性質をこれらのファイルに割り当てます。

ライセンスの表示

ライセンス：任意

ASA FirePOWER モジュールのライセンスを表示するには、[Licenses] ページを使用します。

[Licenses] ページ以外にも、ライセンスとライセンス制限を確認できる方法がいくつかあります。

- [Product Licensing] ダッシュボード ウィジェットにはライセンスの概要が表示されます。

- [Device] ページ（[Configuration] > [ASA FirePOWER Configuration] > [Device Management] > [Device]）には、ライセンスが一覧表示されます。

ライセンスを確認するには、次の手順を実行します。

[Configuration] > [ASA FirePOWER Configuration] > [Licenses] の順に選択します。

[Licenses] ページが表示されます。

ASA FirePOWER モジュールへのライセンスの追加

ライセンス：任意

ASA FirePOWER モジュールにライセンスを追加する前に、ライセンスの購入時にシスコから提供されたアクティベーション キーがあることを確認してください。ライセンス付き機能を使用する前に、**必ず**ライセンスを追加してください。

（注） バックアップが完了した後にライセンスを追加した場合は、このバックアップを復元するときに、それらのライセンスが削除されたり上書きされたりすることはありません。復元の際の競合を防止するためにも、バックアップを復元する前に、これらのライセンスを（それらが使用されている場所をメモした上で）削除し、バックアップを復元した後で、追加して再設定してください。競合が発生した場合は、サポートに連絡してください。

ライセンスを追加するには、次の手順を実行します。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Licenses] の順に選択します。

[Licenses] ページが表示されます。

ステップ 2 [Add New License] をクリックします。

[Add License] ページが表示されます。

ステップ 3 ライセンスを電子メールで受信しましたか?

- 電子メールで受信した場合は電子メールからライセンスをコピーし、[License] フィールドに貼り付け、[Submit License] をクリックします。

ライセンスが正しい場合、ライセンスが追加されます。残りの手順は省略します。

- 電子メールで受信していない場合は、[ライセンスの取得（Get License）] をクリックします。

[Product License Registration] ポータルが表示されます。インターネットにアクセスできない場合は、インターネットにアクセスできるコンピュータに切り替えてください。ページ下部に表示されるライセンスキーを書きとめ、https://www.cisco.com/go/license にアクセスします。

ステップ 4 画面の指示に従ってライセンスを取得します。ライセンスは電子メールで送信されます。

ヒント サポート サイトにログインした後で、[Licenses] タブでライセンスを要求することもできます。

ステップ 5 電子メールからライセンスをコピーし、ASA FirePOWER モジュールの Web ユーザ インターフェイスの [License] フィールドに貼り付け、[Submit License] をクリックします。

ライセンスが有効な場合、ライセンスが追加されます。

ライセンスの削除

ライセンス：任意

何らかの理由でライセンスを削除する必要がある場合は、次の手順を使用します。シスコでは、各 ASA FirePOWER モジュールの一意のライセンス キーに基づきライセンスを生成するため、1 つの ASA FirePOWER モジュールからライセンスを削除して、別の ASA FirePOWER モジュールでそのライセンスを再利用することはできないことに注意してください。

ほとんどの場合、ライセンスを削除すると、そのライセンスによって有効になる機能を使用することができなくなります。詳細については、ライセンスについて（567 ページ）を参照してください。

ライセンスを削除するには、次の手順を実行します。

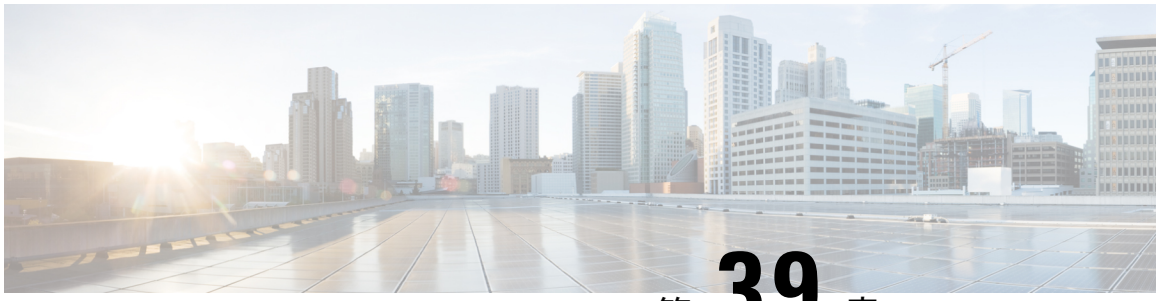
ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Licenses] の順に選択します。

[Licenses] ページが表示されます。

ステップ 2 削除するライセンスの横にある削除アイコン（）をクリックします。

ステップ 3 ライセンスを削除することを確認します。

ライセンスが削除されます。



第 39 章

ASA FirePOWER モジュール ソフトウェアの更新

シスコでは、ルールアップデート、地理位置情報データベース（GeoDB）の更新、脆弱性データベース（VDB）の更新だけでなく、ASA FirePOWER モジュール ソフトウェア本体のメジャーおよびマイナーな更新など、さまざまなタイプの更新を電子的に配布しています。

注意 このセクションでは、ASA FirePOWER モジュールの更新に関する全般的な情報について説明します。VDB、GeoDB、侵入ルールを含め、更新を実行する前に、更新に付随しているリリース ノートまたはアドバイザリ テキストを**必ず**お読みください。リリース ノートには、前提条件、警告、および特定のインストールとアンインストールの手順など、重要な情報が記載されています。

リリース ノートまたはアドバイザリ テキストに特に記載されていない限り、更新しても設定は変更されず、設定はそのまま保持されます。

更新のタイプについて

ライセンス：任意

シスコでは、侵入ルールの更新や VDB の更新だけでなく、ASA FirePOWER モジュール ソフトウェア本体のメジャーおよびマイナーな更新など、さまざまなタイプの更新を電子的に配布しています。

次の表に、シスコが提供している更新のタイプの説明を示します。ほとんどのタイプの更新では、ダウンロードとインストールをスケジュールすることができます。タスクのスケジューリング （537 ページ）および再帰的なルール更新の使用 （587 ページ）を参照してください。

表 *86 : ASA FirePOWER* モジュールの更新タイプ

更新のタイプ	説明	スケジュール	アンインストール
パッチ	パッチには、限定された範囲の修正が含まれています（また通常は、5.4.0.1 のようにバージョン番号の 4 桁目が変更されます）。	あり	あり
機能の更新	機能の更新はパッチよりも包括的であり、通常は新しい機能が含まれています（また通常は、5.4.1 のようにバージョン番号の 3 桁目が変更されます）。	あり	あり
メジャーな更新（メジャーおよびマイナー バージョンのリリース）	メジャーな更新（アップグレードと呼ばれることもある）には新しい機能が含まれており、大規模な変更が含まれることがあります（通常は、5.3 や 5.4 のようにバージョン番号の最初の桁または 2 桁目が変更されます）。	いいえ（No）	いいえ（No）
VDB	VDB の更新は、ホストが影響を受ける可能性がある既知の脆弱性のデータベースに影響します。	はい	いいえ（No）
侵入ルール	侵入ルールを更新すると、更新された新しい侵入ルールおよびプリプロッセサ ルール、既存のルールに対して変更された状態、および変更されたデフォルトの侵入ポリシーの設定が提供されます。ルールの更新では、ルールが削除されたり、新しいルール カテゴリとデフォルトの変数が提供されたり、デフォルトの変数値が変更されたりすることもあります。	はい	いいえ（No）
地理情報データベース（GeoDB）	GeoDB の更新により、物理的な場所や接続タイプなど、検出されたルート可能な IP アドレスにシステムが関連付けることができるものに関する情報が提供されます。地理情報データを、アクセス コントロール ルールとして使用することができます。位置情報の詳細を表示するには、GeoDB をインストールする必要があります。	はい	いいえ（No）

パッチおよび他のマイナーな更新はアンインストールできますが、VDB、GeoDB、または侵入ルールに対するメジャーな更新をアンインストールしたり、前のバージョンに戻したりすることはできないことに注意してください。新しいメジャー バージョンに更新後に、古いバージョンに戻す必要がある場合は、Cisco TAC に連絡してください。

ソフトウェア アップデートの実行

ライセンス：任意

更新するには、いくつかの基本的な手順があります。最初にリリース ノートを参照し、必要な更新前のタスクをすべて完了することで更新の準備を整えておく**必要があります**。次に、更新

を開始できます。更新が成功したことを確認する必要があります。最後に、更新後の必要な手順を完了させます。

更新の計画

ライセンス：任意

更新を開始する前に、リリース ノートをよく読んで理解する必要があります。リリース ノートはサポート サイトからダウンロードすることができます。リリース ノートには、新しい機能、および既知の問題と解決済みの問題について説明されています。また、リリースノートには前提条件、警告、および特別なのインストールおよびアンインストールの手順についての重要な情報が含まれています。

以降の項では、更新の計画で検討しなければならない要素の概要を提供します。

ソフトウェア バージョンの要件

正しいソフトウェアバージョンを実行していることを確認する必要があります。リリースノートには必要なバージョンが示されています。古いバージョンを実行している場合は、サポートサイトから更新を取得することができます。

時間とディスク領域の要件

十分な空きディスク領域があることを確認し、更新のために十分な時間を確保しておく必要があります。リリース ノートには、領域と時間の要件が示されています。

設定のバックアップのガイドライン

メジャーな更新を開始する前に、ASA FirePOWER モジュールに存在するバックアップを外部の場所にコピーしてから、それらのバックアップを削除することをお勧めします。更新のタイプに関係なく、現行の設定データを外部の場所にバックアップしておく必要もあります。バックアップと復元の使用 （605 ページ）を参照してください。

更新を実行するタイミング

更新プロセスはトラフィックの検査およびトラフィック フローに影響を与えることがあり、更新中は Data Correlator が無効になるため、保守時間帯や中断の影響が最も少ない時間に更新を行うことを推奨しています。

更新プロセスについて

ライセンス：任意

ASA FirePOWER モジュールの更新には、ASA FirePOWER モジュール インターフェイスを使用します。

[Product Updates] ページ（[Configuration] > [ASA FirePOWER Configuration] > [Updates]）には、それぞれの更新のバージョン、およびその更新が生成された日時が表示されます。また、ソフトウェアの再起動が更新の一環として必要です。サポートから取得した更新をアップロードす

ると、更新がページに示されます。パッチ機能および機能の更新のアンインストーラも表示されます。ソフトウェア アップデートのアンインストール（580ページ）を参照してください。このページでは、VDB の更新もリストできます。

ヒント　パッチおよび機能の更新では、自動更新機能を利用することができます。ソフトウェア アップデートの自動化（541 ページ）を参照してください。

トラフィック フローとインスペクション

更新をインストールまたはアンインストールすると、次の機能に影響を与えることがあります。

- トラフィックのインスペクション（アプリケーションおよびユーザの認識とコントロール、URL フィルタリング、セキュリティ インテリジェンス フィルタリング、侵入検出と防御、接続のロギングなど）
- トラフィック フロー

Data Correlator は、システムの更新中は動作しません。更新が完了すると再開します。

ネットワーク トラフィックの中断方法と期間は、ASA FirePOWER モジュールの設定および展開方法、更新により ASA FirePOWER モジュールが再起動されるかどうかによって異なります。特定の更新に対してネットワーク トラフィックがいつ、どのように影響を受けるかについての情報は、リリース ノートを参照してください。

更新時の ASA FirePOWER モジュールの使用

更新のタイプに関係なく、更新のモニタ以外のタスクを実行するために ASA FirePOWER モジュールを使用しないでください。

メジャーな更新中にユーザが ASA FirePOWER モジュールを使用するのを防ぎ、メジャーな更新の進捗を簡単にモニタできるようにするために、ASA FirePOWER モジュールのインターフェイスが合理化されています。マイナーな更新の進捗は、タスク キュー（[Monitoring] > [ASA FirePOWER Monitoring] > [Task Status]）でモニタできます。マイナーな更新中に ASA FirePOWER モジュールを使用することは禁止されていませんが、シスコでは推奨していません。

マイナーな更新の場合でも、ASA FirePOWER モジュールが更新プロセス中に使用できなくなることがあります。これは想定されている動作です。その場合は、ASA FirePOWER モジュールに再度アクセスできるようになるまで待機します。まだ更新が実行中の場合は、更新が完了するまで ASA FirePOWER モジュールを使用しないでください。更新中は、ASA FirePOWER モジュールが 2 回再起動されることがありますが、これも想定されている動作です。

注意　更新で問題が発生した場合には（たとえば更新が失敗した、または [Update Status] ページの手動更新に進捗が表示されないなど）、更新を再開**しない**でください。代わりに、サポートに連絡してください。

更新後

リリース ノートに記載されている更新後のタスクをすべて完了し、展開が正常に実行されていることを確認する**必要があります**。

最も重要な更新後作業は、アクセス コントロール ポリシーの再適用です。アクセス コントロール ポリシーを適用すると、トラフィック フローと処理が一時的に停止することがあります。また、いくつかのパケットが検査されない場合があります。設定変更の導入 （92 ページ）を参照してください。

また、次の作業を実行する必要があります。

- 更新が正常に終了したことを確認する
- 必要に応じて侵入ルール、VDB、および GeoDB を更新する
- リリース ノートの情報に基づいて、必要な設定変更を行う
- リリース ノートに記載されている、更新後の追加タスクを実行する

ASA FirePOWER モジュール ソフトウェアの更新

ライセンス：任意

更新のタイプ、および ASA FirePOWER モジュールがインターネットにアクセスできるかどうかによって、ASA FirePOWER モジュール ソフトウェアを次のいずれかの方法で更新できます。

- ASA FirePOWER モジュールがインターネットにアクセスできる場合は、サポート サイトから直接更新を取得できます。このオプションは、メジャーな更新ではサポート**されていません**。
- サポート サイトから更新を手動でダウンロードして、ASA FirePOWER モジュールにアップロードすることもできます。ASA FirePOWER モジュールがインターネットにアクセスできない場合、またはメジャーな更新を実行している場合は、このオプションを選択します。

メジャーな更新の場合は、ASA FirePOWER モジュールを更新すると、以前の更新のアンインストーラが削除されます。

- ASA FirePOWER モジュール ソフトウェアを更新するには、次の手順を実行します。

ステップ 1 リリース ノートを読んで、更新前の必要なタスクを完了します。

更新前のタスクには、ASA FirePOWER モジュールが Cisco ソフトウェアの正しいバージョンを実行している、更新を実行するための十分な空きディスク容量がある、更新を実行するために十分な時間を確保している、設定データをバックアップしているなどの確認が含まれます。

ステップ 2 更新をアップロードします。更新のタイプ、および ASA FirePOWER モジュールがインターネットにアクセスできるかどうかに応じて、2 つのオプションがあります。

ASA FirePOWER モジュール ソフトウェアの更新

- メジャーな更新を除くすべての更新で、ASA FirePOWER モジュールがインターネットにアクセスできる場合は、[Configuration] > [ASA FirePOWER Configuration] > [Updates] の順に選択し、[Download Updates] をクリックして、次のいずれかのサポート サイトで最新の更新を確認します。
  - **Sourcefire**：（https://support.sourcefire.com/）
  - **シスコ**：

    （http://www.cisco.com/cisco/web/support/index.html）
- メジャーな更新の場合、または ASA FirePOWER モジュールがインターネットにアクセスできない場合は、最初に次のいずれかのサポート サイトから更新を手動でダウンロードする必要があります。
  - **Sourcefire**：（https://support.sourcefire.com/）
  - **シスコ**：（http://www.cisco.com/cisco/web/support/index.html）
- [Configuration] > [ASA FirePOWER Configuration] > [Updates] の順に選択し、[Upload Update] をクリックします。[Choose File] をクリックして、その更新に移動して選択し、[Upload] をクリックします。

（注） サポート サイトから、手動でまたは [Product Updates] タブで [Download Updates] をクリックして、更新を直接ダウンロードします。電子メールで更新ファイルを転送すると、ファイルが破損することがあります。

更新がアップロードされます。

ステップ 3 [Monitoring] > [ASA FirePOWER Monitoring] > [Task Status] の順に選択して、タスク キューを表示し、進行中のジョブがないことを確認します。

更新を開始したときに実行されているタスクは停止され、再開できません。更新が完了した後で、タスク キューから手動で削除する必要があります。タスク キューは 10 秒ごとに自動的にリフレッシュされます。更新を始める前に、長時間実行しているタスクが完了するまで待機する必要があります。

ステップ 4 [Configuration] > [ASA FirePOWER Configuration] > [Updates] の順に選択します。

[Product Updates] ページが表示されます。

ステップ 5 アップロードした更新の横にあるインストール アイコンをクリックします。

更新プロセスが開始されます。更新を監視する方法は、更新がメジャーかマイナーかによって異なります。更新のタイプを判断するには、表 86 : ASA FirePOWER モジュールの更新タイプ （574 ページ）の表およびリリース ノートを参照してください。

- マイナーな更新の場合、更新の進捗は、タスク キュー（[Monitoring] > [ASA FirePOWER] > [Monitoring] > [Task Status]）でモニタできます。
- メジャーな更新については、タスク キューで更新の進捗の監視を開始できます。ただし、ASA FirePOWER モジュールによる更新前の必要なチェックが完了すると、ユーザはモジュール インターフェイスからロックアウトされます。再度アクセスすると、[Upgrade Status] ページが表示されます。詳細については、メジャーな更新のステータスの監視 （579 ページ）を参照してください。

注意 更新のタイプに関係なく、更新が完了するまで、更新のモニタ以外のタスクを実行するために ASA FirePOWER モジュールを使用しないでください。必要な場合、ASA FirePOWER モジュールは再起動します。詳細は、更新時の ASA FirePOWER モジュールの使用 （576 ページ）を参照してください。

ステップ 6 更新が完了したら、ASA FirePOWER モジュール インターフェイスにアクセスしてページを更新します。そうしない場合、インターフェイスが予期しない動作を示すことがあります。メジャーな更新の後、最初にインターフェイスにアクセスしたユーザに対してエンド ユーザ ライセンス契約（EULA）が表示されることがあります。EULA を確認して承認し、処理を続行します。

ステップ 7 サポート サイトで利用可能なルール アップデートが、ご使用の ASA FirePOWER モジュールのルールより新しい場合は、新しいルールをインポートします。

詳細については、ルール更新とローカル ルール ファイルのインポート （582 ページ）を参照してください。

ステップ 8 アクセス コントロール ポリシーを再適用します。

アクセス コントロール ポリシーを適用すると、トラフィック フローと処理が一時的に停止することがあります。また、いくつかのパケットが検査されない場合があります。詳細については、設定変更の導入（92 ページ）を参照してください。

ステップ 9 サポート サイトにある利用可能な VDB が、最後にインストールした VDB よりも新しい場合は、その最新の VDB をインストールします。

VDB の更新をインストールすると、トラフィック フローと処理が一時的に停止することがあります。また、いくつかのパケットが検査されない場合があります。詳細については、脆弱性データベースの更新（581 ページ）を参照してください。

メジャーな更新のステータスの監視

ライセンス：任意

メジャーな更新では、ASA FirePOWER モジュール提供の簡潔なインターフェイスを使用して、更新プロセスを簡単にモニタできます。簡潔なインターフェイスでは、更新のモニタリング以外のタスクを実行するために ASA FirePOWER モジュールを使用することもできません。更新の進捗のモニタリングは、タスク キューで開始できます（[Monitoring] > [ASA FirePOWER Monitoring] > [Task Status]）。ただし、ASA FirePOWER モジュールによる更新前の必要なチェックが完了すると、簡潔な更新ページが表示されるまで、ユーザはユーザ インターフェイスからロックアウトされます。

簡潔なインターフェイスには、更新前のバージョン、更新後のバージョン、および更新を開始してからの経過時間が表示されます。また進捗バーが表示され、実行中のスクリプトに関する詳細が示されます。

ヒント 更新ログを表示するには、[show log for current script] をクリックします。ログをもう一度非表示にするには、[hide log for current script] をクリックします。

何らかの理由で更新が失敗すると、ページにはエラーメッセージが表示され、失敗した日時、更新が失敗したときに実行していたスクリプト、およびサポートへ連絡するための方法が示されます。更新を再開**しないで**ください。

注意 更新で他の問題（ページの手動更新で長時間経過しても進捗が表示されない、など）が生じた場合も、更新を再開**しないで**ください。代わりに、サポートへ連絡してください。

更新が完了すると、ASA FirePOWER モジュールは正常終了のメッセージを表示して再起動します。ASA FirePOWER モジュールの再起動が終了したら、更新後の必要な手順をすべて実行します。

ソフトウェア アップデートのアンインストール

ライセンス：任意

パッチまたは機能の更新を適用すると、更新プロセスにより、更新を削除できるアンインストーラが作成されます。

更新をアンインストールした場合、結果として保持される Cisco ソフトウェアのバージョンは更新パスによって異なります。たとえば、バージョン 5.0 からバージョン 5.0.0.2 へ直接更新した場合のシナリオについて考えてみます。バージョン 5.0.0.2 のパッチをアンインストールすると、バージョン 5.0.0.1 の更新をインストールしたことがなくても、バージョン 5.0.0.1 が結果として生成されます。更新をアンインストールした場合に結果として保持される Cisco ソフトウェアのバージョンの詳細については、リリース ノートを参照してください。

（注） アンインストールは、メジャーな更新ではサポートされていません。新しいメジャーバージョンに更新してから古いバージョンに戻すことが必要になった場合は、サポートに連絡してください。

トラフィック フローとインスペクション

更新をアンインストールすると、トラフィック インスペクションとトラフィック フローが影響を受ける可能性があります。特定の更新に対してネットワーク トラフィックがいつ、どのように影響を受けるかについての情報は、リリース ノートを参照してください。

アンインストール後

更新をアンインストールしたら、アンインストールが成功したことを確認します。それぞれの更新に特定の情報については、リリース ノートを参照してください。

パッチまたは機能更新のアンインストール方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Updates] の順に選択します。

[Product Updates] ページが表示されます。

ステップ 2 削除する更新のアンインストーラの隣にあるインストール アイコンをクリックします。

プロンプトが表示されたら、更新をアンインストールすることを確認して、ASA FirePOWER モジュールを再起動します。

アンインストール プロセスが開始されます。その進捗は、タスク キュー（[Monitoring] > [ASA FirePOWER Monitoring] > [Task Status]）でモニタできます。

注意 アンインストールが完了し、必要に応じて、ASA FirePOWER モジュールを再起動するまでタスクを実行するために ASA FirePOWER モジュール インターフェイスを使用しないでください。詳細については、更新プロセスについて （575 ページ）を参照してください。

ステップ 3 ページを更新します。更新しないと、インターフェイスが予期しない動作を示すことがあります。

脆弱性データベースの更新

ライセンス：任意

シスコ脆弱性データベース（VDB）は、ホストが影響を受ける可能性がある既知の脆弱性のデータベースです。シスコ脆弱性調査チーム（VRT）は、VDB を定期的に更新します。VDB を更新するには、[Product Updates] ページを使用します。

（注） 検出の更新とともに VDB 更新をインストールすると、トラフィック フローと処理が一時的に停止し、いくつかのパケットが検査なしで通過する場合があります。システムのダウンタイムの影響を最小限に抑えるために、システムの使用率が低い時間に合わせて更新をスケジュールすることもできます。

（注） VDB の更新完了後に、古くなったすべてのアクセス コントロール ポリシーを再適用します。VDB のインストールまたはアクセス コントロール ポリシーの再適用を行うと、トラフィック フローと処理が一時的に停止することがあり、また、いくつかのパケットが検査されずに通過する場合があるので注意してください。詳細については、設定変更の導入 （92 ページ）を参照してください。

この項では、手動による VDB 更新を計画および実行する方法について説明します。

脆弱性データベースを更新する方法：

ステップ 1 更新用の VDB 更新アドバイザリ テキストを読みます。

このアドバイザリ テキストには、更新で VDB に加えられた変更に関する情報が含まれています。

ステップ 2 [Configuration] > [ASA FirePOWER Configuration] > [Updates] の順に選択します。

[Product Updates] ページが表示されます。

ステップ 3 更新をアップロードします。

- ASA FirePOWER モジュールがインターネットにアクセスできる場合は、[Download Updates] をクリックして、次のいずれかのサポート サイトで最新の更新を確認します。
- **Sourcefire**：（https://support.sourcefire.com/）
- **シスコ**：（http://www.cisco.com/cisco/web/support/index.html）
- ASA FirePOWER モジュールがインターネットにアクセスできない場合は、次のいずれかのサポート サイトから更新を手動でダウンロードして [Upload Update] をクリックします。[Choose File] をクリックして、その更新に移動して選択し、[Upload] をクリックします。
- **Sourcefire**：（https://support.sourcefire.com/）
- **シスコ**：（http://www.cisco.com/cisco/web/support/index.html）

（注） サポート サイトから、手動でまたは [Download Updates] をクリックして、更新を直接ダウンロードします。電子メールで更新ファイルを転送すると、ファイルが破損することがあります。

更新がアップロードされます。

ステップ 4 VDB 更新の隣にあるインストール アイコンをクリックします。

[Install Update] ページが表示されます。

ステップ 5 [Install] をクリックします。

更新プロセスが開始されます。更新の進捗は、タスク キュー（[Monitoring] > [ASA FirePOWER Monitoring] > [Task Status]）でモニタできます。

注意 更新で問題が発生した場合には（たとえばタスク キューに更新が失敗したことが示されているなど）、更新を再開**しない**でください。代わりに、サポートへ連絡してください。

VDB 更新を有効にするには、古くなったすべてのアクセス コントロール ポリシーを再適用する必要があります。「設定変更の導入 （92 ページ）」を参照してください。

ルール更新とローカル ルール ファイルのインポート

ライセンス：任意

新しい脆弱性に関する情報が判明すると、シスコ脆弱性調査チーム（VRT）からルール更新がリリースされます。これは、最初に ASA FirePOWER モジュールにインポートしてから、影響を受けるアクセス コントロール、ネットワーク解析、および侵入ポリシーを適用することで実装できます。

ルール更新は累積的なので、シスコでは常に最新の更新をインポートすることを推奨しています。現在インストールされているルールのバージョンに一致するルール更新、またはそれより前のバージョンのルール更新をインポートすることはできません。

（注） ルール更新には新しいバイナリが含まれている場合があるので、これらのダウンロードおよびインストールのプロセスが、自身のセキュリティ ポリシーに適合していることを確認してください。また、ルールの更新は量が多くなることがあるため、ルールのインポートはネットワークの使用量が少ないときに行うようにしてください。

ルール更新では、次のものを提供します。

1. **新規または変更されたルールおよびルールの状態**：ルール更新は、新規または更新された侵入およびプリプロセッサのルールを提供します。新しいルールについては、ルールの状態がそれぞれのシステム提供の侵入ポリシーで異なる場合があります。たとえば、Security over Connectivity の侵入ポリシーでは新しいルールが有効になっており、Connectivity over Security の侵入ポリシーでは無効になっていることがあります。ルールの更新では、既存のルールのデフォルト状態が変更されたり、既存のルールそのものが削除されることもあります。
2. **新しいルール カテゴリ**：ルール更新には、常に追加される新しいルール カテゴリが含まれている場合があります。
3. **変更されたプリプロセッサおよび詳細設定**：ルール更新は、システム提供の侵入ポリシーの詳細設定および、システム提供のネットワーク解析ポリシーのプリプロセッサ設定を変更することがあります。また、アクセス コントロール ポリシーにおける高度な前処理やパフォーマンス オプションに関するデフォルト値を更新することもあります。
4. **新規の変数および変数の変更**：ルール更新は、既存のデフォルト変数のデフォルト値を変更することがありますが、ユーザによる変更は上書きされません。新しい変数は常に追加されています。

ルール更新でポリシーが変更されるタイミングの概要

ルール更新は、すべてのアクセス コントロール ポリシーと同様に、システム提供およびカスタムのネットワーク解析ポリシーの両方に影響を与えます。

- **システム提供**：システムが提供するネットワーク解析および侵入ポリシーへの変更は、その他のアクセス コントロールの詳細設定と同様に、更新後にポリシーを再適用すると自動的に有効になります。
- **カスタム**：カスタムのネットワーク解析および侵入ポリシーは、いずれもシステム提供のポリシーをベースとして使用するか、ポリシー チェーン中でのイベント ベースとして使

用しているので、ルール更新がカスタムのネットワーク解析および侵入ポリシーにも影響を与えることがあります。ただし、ルール更新によるこれらの自動的な変更が行われないようにすることができます。これにより、ルール更新のインポートとは関係ないスケジュールで、システムによって提供される基本ポリシーを手動で更新できます。ユーザーによる選択とは関係なく（カスタム ポリシーごとに実装）システム提供のポリシーに対する更新では、ユーザーがカスタマイズした設定は上書き**されません**。詳細については、ルール アップデートによるシステム付属基本ポリシーの変更を許可する （320 ページ）を参照してください。

ルールの更新をインポートすると、ネットワーク解析および侵入ポリシーのキャッシュされていた変更は、すべて廃棄されることに注意してください。便宜のために、[Rule Updates] ページには、キャッシュされている変更があるポリシーがリストされます。詳細については、競合の解決とポリシー変更の確定 （314 ページ）を参照してください。

ポリシーの再適用

ルール更新による変更を反映させるには、変更されたすべてのポリシーを再適用する必要があります。ルール更新をインポートする際には、侵入またはアクセス コントロール ポリシーを自動的に再適用するように、システムを設定できます。これは、ルールの更新によってシステムにより提供される基本ポリシーが変更されることを許可する場合に特に役立ちます。

- アクセス コントロール ポリシーを再適用すると、関連付けられた SSL、ネットワーク解析、ファイルのポリシーも再適用されますが、侵入ポリシーは再適用**されません**。また、変更された詳細設定のデフォルト値もすべて更新されます。ネットワーク解析のポリシーは個別に適用できないので、ネットワーク解析ポリシーのプリプロセッサ設定を更新するには、アクセス コントロール ポリシーの再適用が**必要です**。
- 侵入ポリシーを再適用すると、ルールおよびその他の変更された侵入ポリシーの設定も更新することができます。侵入ポリシーの再適用はアクセス コントロール ポリシーとあわせて行うこともできますが、その他のアクセス コントロールの設定は更新せずに、侵入ポリシーの適用で侵入ルールだけを更新することもできます。

ルール更新に共有のオブジェクト ルールが含まれている場合は、インポート後に初めてアクセス コントロールまたは侵入ポリシーを適用したときに、トラフィック フローと処理が一時的に停止し、いくつかのパケットが検査されずに通過することがあります。アクセス コントロールおよび侵入ポリシーの適用における、要件、その他の影響、および推奨事項などを含めた詳細については、設定変更の導入 （92 ページ）を参照してください。

ワンタイム ルール更新の使用

ライセンス：任意

ワンタイム ルール更新では次の 2 つの方法を使用することができます。

- 手動ワンタイム ルール更新の使用：サポート サイトから手動でルール更新をダウンロードし、手動でインストールします。

- 自動ワンタイム ルール更新の使用：自動機能を使用し、サポート サイトで新しいルール更新を検索してアップロードします。

手動によるワンタイム ルール更新の使用

ライセンス：任意

次の手順では、新しいルール更新を手動でインポートする方法について説明します。この手順は、ASA FirePOWER モジュールがインターネットにアクセスできない場合に便利です。

手動でルール更新をインポートするには、次の手順を実行します。

ステップ 1 インターネットにアクセスできるコンピュータから、次のサイトのいずれかへアクセスします。

- **Sourcefire**：（https://support.sourcefire.com/）
- **シスコ**：（http://www.cisco.com/cisco/web/support/index.html）

ステップ 2 [Download] をクリックし、[Rules] をクリックします。

ステップ 3 最新のルール更新へ移動します。

ルール更新は累積的です。現在インストールされているルールのバージョンに一致するルール更新、またはそれより前のバージョンのルール更新をインポートすることはできません。

ステップ 4 ダウンロードするルール更新ファイルをクリックし、そのファイルをコンピュータに保存します。

ステップ 5 [Configuration] > [ASA FirePOWER Configuration] > [Updates] の順に選択し、[Rule Updates] タブを選択します。

[Rule Updates] ページが表示されます。

ヒント [Rule Editor] ページ（[Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] > [Rule Editor]）で、[Import Rules] をクリックすることもできます。

ステップ 6 オプションで [Delete All Local Rules] をクリックし、[OK] をクリックして、作成した、または削除されたフォルダにインポートしたすべてのユーザ定義ルールを移動します。

ステップ 7 [アップロードおよびインストールするルール アップデートまたはテキスト ルール ファイル（Rule Update or text rule file to upload and install）] を選択し、[ファイルの選択（Choose File）] をクリックして、ルール更新ファイルに移動して選択します。

ステップ 8 オプションで、更新の完了後にポリシーを再適用します。

- [Reapply intrusion policies after the rule update import completes] を選択すると、侵入ポリシーが自動的に再適用されます。このオプションを選択するのは、その他のアクセス コントロールのユーザ設定は更新せずに、ルールおよびその他の変更された侵入ポリシーの設定を更新する場合だけです。このオプションの選択が**必要となる**のはアクセス コントロール ポリシーとあわせて侵入ポリシーを再適用する場合であり、そうしたケースではアクセス コントロール ポリシーを再適用しても完全には適用されません。
- [Reapply access control policies after the rule update import completes] を選択すると、アクセス コントロール ポリシーとその関連の SSL、ネットワーク解析、ファイルのポリシーも自動的に再適用されます

が、侵入ポリシーは再適用されません。このオプションを選択すると、変更されたアクセス コントロールの詳細設定のデフォルト値もすべて更新されます。ネットワーク解析のポリシーは親となるアクセス コントロール ポリシーと個別には適用できないので、ネットワーク解析ポリシーのプリプロセッサ設定を更新するには、アクセス コントロール ポリシーの再適用が**必要です**。

ステップ 9 [Import] をクリックします。

システムはルール更新をインストールし、[Rule Update Log] 詳細ビューを表示します。「[Rule Update Import Log] 詳細ビューについて （593 ページ）」を参照してください。システムは、前のステップで指定したポリシーも適用します。「設定変更の導入 （92 ページ）」および「侵入ポリシーの適用 （349 ページ）」を参照してください。

（注） ルール更新のインストール中にエラー メッセージが表示された場合は、サポートに連絡してください。

自動のワンタイム ルール更新の使用

ライセンス：任意

次の手順では、サポート サイトに自動で接続して、新しいルール更新をインポートする方法について説明します。この手順は、ASA FirePOWER モジュールがインターネットにアクセスできる場合にのみ使用できます。

自動でルール更新をインポートする方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Updates] の順に選択し、[Rule Updates] タブを選択します。

[Rule Updates] ページが表示されます。

ヒント [Rule Editor] ページ（[Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] > [Rule Editor]）で、[Import Rules] をクリックすることもできます。

ステップ 2 オプションで [Delete All Local Rules] をクリックし、[OK] をクリックして、作成した、または削除されたフォルダにインポートしたすべてのユーザ定義ルールを移動します。

ステップ 3 [Download new Rule Update from the Support Site] を選択します。

ステップ 4 オプションで、更新の完了後にポリシーを再適用します。

- [Reapply intrusion policies after the rule update import completes] を選択すると、侵入ポリシーが自動的に再適用されます。このオプションを選択するのは、その他のアクセス コントロールのユーザ設定は更新せずに、ルールおよびその他の変更された侵入ポリシーの設定を更新する場合だけです。このオプションの選択が**必要となる**のはアクセス コントロール ポリシーとあわせて侵入ポリシーを再適用する場合であり、そうしたケースではアクセス コントロール ポリシーを再適用しても完全には適用されません。
- [Reapply access control policies after the rule update import completes] を選択すると、アクセス コントロール ポリシー、ネットワーク解析ポリシー、ファイル ポリシーは自動的に再適用されますが、侵入ポリ

シーは再適用されません。このオプションを選択すると、変更されたアクセス コントロールの詳細設定のデフォルト値もすべて更新されます。ネットワーク解析のポリシーは親となるアクセス コントロール ポリシーと個別には適用できないので、ネットワーク解析ポリシーのプリプロセッサ設定を更新するには、アクセス コントロール ポリシーの再適用が**必要です**。

ステップ 5 [Import] をクリックします。

ルール更新がインストールされ、[Rule Update Log] 詳細ビューが表示されます。[Rule Update Import Log] 詳細ビューについて （593 ページ）を参照してください。システムは、前のステップで指定したポリシーも適用します。「設定変更の導入 （92 ページ）」および「侵入ポリシーの適用 （349 ページ）」を参照してください。

（注） ルール更新のインストール中にエラー メッセージが表示された場合は、サポートに連絡してください。

再帰的なルール更新の使用

ライセンス：任意

[ルールのアップデート（Rule Updates）] ページを使用して、ルール更新を日次、週次、または月次ベースでインポートすることができます。

ルール更新のインポートにおける適用可能なサブタスクは、ダウンロード、インストール、ベース ポリシーの更新、およびポリシーの再適用の順序で生じます。1 つのサブタスクが完了すると、次のサブタスクが開始されます。適用できるのは、再帰的なインポートが設定されている ASA FirePOWER モジュールによって以前に適用されたポリシーだけであることに注意してください。

再帰的なルール更新をスケジュールする方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Updates] の順に選択し、[Rule Updates] タブを選択します。

[Rule Updates] ページが表示されます。

ヒント [Rule Editor] ページ（[Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] > [Rule Editor]）で、[Import Rules] をクリックすることもできます。

ステップ 2 オプションで [Delete All Local Rules] をクリックし、[OK] をクリックして、作成した、または削除されたフォルダにインポートしたすべてのユーザ定義ルールを移動します。

ステップ 3 [Enable Recurring Rule Update Imports] を選択します。

ページが拡張され、再帰的なインポートを設定するためのオプションが表示されます。[Recurring Rule Update Imports] セクション見出しの下に、インポート ステータスのメッセージが表示されます。設定を保存すると、再帰的なインポートが有効になります。

ヒント　再帰的なインポートを無効にするには、[Enable Recurring Rule Update Imports] チェック ボックスをオフにして [Save] をクリックします。

ステップ 4　[Import Frequency] フィールドで、ドロップダウン リストから [Daily]、[Weekly]、または [Monthly] を選択します。

週次または月次のインポート間隔を選択した場合は、表示されるドロップダウンリストを使用して、ルール更新をインポートする曜日または月の日を選択します。選択項目をクリックするか、または選択項目の最初の文字または数字を 1 回以上入力して Enter を押すことで、再帰タスクのドロップダウンリストから選択できます。

ステップ 5　[Import Frequency] フィールドで、再帰的なルール更新のインポートを開始するタイミングを指定します。

ステップ 6　オプションで、更新の完了後にポリシーを再適用します。

- [Reapply intrusion policies after the rule update import completes] を選択すると、侵入ポリシーが自動的に再適用されます。このオプションを選択するのは、その他のアクセス コントロールのユーザ設定は更新せずに、ルールおよびその他の変更された侵入ポリシーの設定を更新する場合だけです。このオプションの選択が**必要となる**のはアクセス コントロール ポリシーとあわせて侵入ポリシーを再適用する場合であり、そうしたケースではアクセス コントロール ポリシーを再適用しても完全には適用されません。
- [Reapply access control policies after the rule update import completes] を選択すると、アクセス コントロール ポリシーとその関連の SSL、ネットワーク解析、ファイルのポリシーも自動的に再適用されますが、侵入ポリシーは再適用されません。このオプションを選択すると、変更されたアクセス コントロールの詳細設定のデフォルト値もすべて更新されます。ネットワーク解析のポリシーは親となるアクセス コントロール ポリシーと個別には適用できないので、ネットワーク解析ポリシーのプリプロセッサ設定を更新するには、アクセス コントロール ポリシーの再適用が**必要です**。

ステップ 7　[Save] をクリックし、設定を使用した再帰的なルール更新のインポートを有効にします。

[ルール アップデートの再帰的なインポート（Recurring Rule Update Imports）] セクションの見出しの下のステータス メッセージが変わり、ルールの更新がまだ実行されていないことが示されます。スケジュールされた時間になるとシステムは、前のステップで指定したルール更新をインストールしてポリシーを適用します。「設定変更の導入 （92 ページ）」および「侵入ポリシーの適用 （349 ページ）」を参照してください。

インポートの前またはインポート中にも、ログオフしたり、他のタスクを実行したりできます。インポート中にアクセスした場合は、[Rule Update Log] に赤色のステータス アイコン（  ）が表示され、[Rule Update Log] 詳細ビューに表示されるメッセージを確認できます。ルールの更新のサイズと内容によっては、ステータス メッセージが表示されるまでに数分かかることがあります。詳細については、ルール更新ログの表示 （591 ページ）を参照してください。

（注）　ルール更新のインストール中にエラー メッセージが表示された場合は、サポートに連絡してください。

ローカル ルール ファイルのインポート

ライセンス：任意

ローカル ルールは、ASCII または UTF-8 エンコーディングによるプレーン テキスト ファイルとしてローカル マシンからインポートするカスタム標準テキスト ルールです。Snort ユーザ マニュアル（ http://www.snort.org で入手可能）の指示に従って、ローカル ルールを作成できます。

ローカル ルールのインポートについて、次の点に注意してください。

- テキスト ファイル名には英数字とスペースを使用できますが、下線（_）、ピリオド（.）、ダッシュ（-）以外の特殊文字は使用できません。
- ジェネレータ ID（GID）を指定する必要はありません。GID を指定する場合、標準テキスト ルールには GID 1、センシティブ データ ルールには 138 のみ指定できます。
- 初めてルールをインポートするときには、Snort ID（SID）またはリビジョン番号を指定**しないで**ください。これにより、削除されたルールを含む、他のルールの SID との競合が回避されます。

システムはルールに対して、1000000 以上の次に使用できるカスタム ルール SID、およびリビジョン番号 の 1 を自動的に割り当てます。

- 以前にインポートしたローカル ルールの更新バージョンをインポートする場合には、システムによって割り当てられた SID、および現在のリビジョン番号よりも大きいリビジョン番号を**含める必要があります**。

現行のローカル ルールのリビジョン番号を表示するには、[Rule Editor] ページ（[Policies] > [Intrusion] > [Rule Editor]）を表示し、ローカル ルールのカテゴリをクリックしてフォルダを展開し、ルールの隣にある [Edit] をクリックします。

- システムによって割り当てられた SID、および現行のリビジョン番号よりも大きいリビジョン番号を使用してルールをインポートして削除したローカル ルールは、元に戻すことができます。ローカル ルールを削除すると、システムは自動的にリビジョン番号を増やすことに注意してください。これは、ローカル ルールを元に戻すための方法です。

削除されたローカル ルールのリビジョン番号を表示するには、[Rule Editor] ページ（[Policies] > [Intrusion Policy] > [Rule Editor]）を表示し、削除されたルール カテゴリをクリックしてフォルダを展開し、ルールの隣にある [Edit] をクリックします。

- 2147483647 よりも大きい SID を持つルールが含まれているルール ファイルはインポートできません。この場合、インポートが失敗します。
- 64 文字を超える送信元または宛先のポートのリストが含まれているルールをインポートすると、そのインポートは失敗します。
- システムは常に、ユーザがインポートするローカル ルールを無効なルール状態に設定します。これらを侵入ポリシーで使用するには、その前に手動でローカル ルールの状態を設定

する必要があります。詳細については、「ルール状態の設定 （377 ページ）」を参照してください。

- ファイル内のルールに、エスケープ文字が含まれていないことを確認する必要があります。
- ルール インポータでは、すべてのカスタム ルールを ASCII または UTF-8 エンコードでインポートする必要があります。
- インポートされたすべてのローカル ルールは、ローカル ルール カテゴリに自動的に保存されます。
- 削除されたすべてのローカル ルールは、ローカル ルール カテゴリから、削除されたルール カテゴリへ移動されます。
- システムは、単一のポンド文字（#）で始まるローカル ルールをインポートします。
- また、二重のポンド文字（##）で始まるローカル ルールは無視し、インポートしません。
- 侵入ポリシーで、侵入イベントのしきい値機能と組み合わせて非推奨の threshold キーワードを使用しているローカル ルールをインポートして有効にすると、ポリシーの検証は失敗します。詳細については、「イベントしきい値の設定 （380 ページ）」を参照してください。

ローカル ルール ファイルをインポートする方法：

ステップ 1 [Policies] > [Intrusion Policy] > [Rule Editor] の順に選択します。

[Rule Editor] ページが表示されます。

ステップ 2 [Import Rules] をクリックします。

[Import Rules] ページが表示されます。

ヒント [System] > [Updates] を選択して、[Rule Updates] タブを選択することもできます。

ステップ 3 [Rule Update or text rule file to upload and install] を選択して、[Choose File] をクリックし、ルール ファイルにナビゲートします。この方法でアップロードされたすべてのルールは、ローカル ルール カテゴリに保存されることに注意してください。

ヒント インポートできるのは、ASCII または UTF-8 エンコードのプレーン テキスト ファイルだけです。

ステップ 4 [Import] をクリックします。

ルール ファイルがインポートされます。侵入ポリシーで、適切なルールが有効になっていることを確認してください。影響を受けるポリシーが次に適用されるまで、ルールはアクティブにはなりません。

（注） システムは、侵入ポリシーを適用するまで、インスペクションに対して新しいルール セットを使用**しません**。手順については、設定変更の導入 （92 ページ）を参照してください。

ルール更新ログの表示

ライセンス：任意

ASA FirePOWER モジュールは、インポートされたルール更新とローカル ルール ファイルごとに 1 つのレコードを生成します。

各レコードにはタイム スタンプ、ファイルをインポートしたユーザ名、およびインポートが正常に終了したか失敗したかを示すステータス アイコンが含まれています。ユーザは、インポートしたすべてのルール更新とローカル ルール ファイルのリストを管理したり、リストからレコードを削除したり、インポートしたすべてのルールとルール更新コンポーネントに関する詳細レコードにアクセスすることができます。[Rule Update Log] で実行できる操作を次の表で説明します。

表 *87 : [*ルール アップデート ログ（*Rule Update Log***）*]* のアクション**

目的	操作
テーブルのカラムの内容について詳しく調べる	詳細については、[Rule Update Log] 表について（592 ページ）を参照してください。
インポート ログからインポート ファイル レコード（ファイルに含まれているすべてのオブジェクトについて削除されたレコードも含めて）を削除する	インポート ファイルでファイル名の隣にある削除アイコン（）をクリックします。 （注） ログからファイルを削除しても、インポート ファイルにインポートされているオブジェクトはいずれも削除されませんが、インポート ログ レコードのみは削除されます。
ルール更新またはローカル ルール ファイルにインポートされている各オブジェクトの詳細を表示する	インポート ファイルでファイル名の隣にある表示アイコン（）をクリックします。

[Rule Update Log] を表示する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Updates] の順に選択し、[Rule Updates] タブを選択します。

[Rule Updates] ページが表示されます。

ヒント [Rule Editor] ページ（[Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] > [Rule Editor]）で、[Import Rules] をクリックすることもできます。

ステップ 2 [Rule Update Log] をクリックします。

[Rule Update Log] ページが表示されます。このページには、インポートされた各ルール更新とローカル ルール ファイルが示されています。

[Rule Update Log] 表について

ライセンス：任意

次の表で、ユーザがインポートするルール更新およびローカル ルール ファイルのリストのフィールドについて説明します。

表 *88 : [Rule Update Log]* のフィールド

フィールド	説明
Summary	インポート ファイルの名前。インポートが失敗した場合は、ファイル名の下に、失敗した理由の簡単な説明が表示されます。
Time	インポートが開始された日時。
User ID	インポートをトリガーとして使用したユーザ名。
Status	インポートの状態を表します • succeeded • 失敗、または実行中 **ヒント** インポート中には [Rule Update Log] ページで、正常終了しなかった、または完了していないことを示す赤いステータス アイコンが表示され、インポートが正常終了した場合のみこれが緑色のアイコンに変わります。

ルール更新またはファイル名の隣にある表示アイコン（）をクリックして、ルール更新またはローカル ルール ファイルの [Rule Update Log] 詳細ページを表示するか、または削除アイコン（）をクリックして、ファイル レコード、およびファイルと一緒にインポートされたすべての詳細オブジェクト レコードを削除します。

ヒント ルール更新のインポートの進行中に示される、インポートの詳細を表示することができます。

[Rule Update Import Log] の詳細の表示

ライセンス：任意

[Rule Update Import Log] 詳細ビューには、ルール更新またはローカル ルール ファイルにインポートされた各オブジェクトの詳細レコードが表示されます。表示されるレコードのうち、自分のニーズに合う情報のみを含むカスタム ワークフローまたはレポートを作成することもできます。

次の表では、[Rule Update Import Log] 詳細ビューで実行できる特定のアクションについて説明します。

表 *89 : [Rule Update Import Log]* 詳細ビューのアクション

目的	操作
テーブルのカラムの内容について詳しく調べる	詳細については、[Rule Update Import Log] 詳細ビューについて （593 ページ）を参照してください。

[Rule Update Import Log] 詳細ビューを表示する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Updates] の順に選択し、[Rule Updates] タブを選択します。

[Rule Updates] ページが表示されます。

ヒント [Rule Editor] ページ（[Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] > [Rule Editor]）で、[Import Rules] をクリックすることもできます。

ステップ 2 [Rule Update Log] をクリックします。

[Rule Update Log] ページが表示されます。

ステップ 3 表示する詳細レコードが含まれているファイルの隣にある表示アイコン（🔍）をクリックします。

詳細レコードのテーブル ビューが表示されます。

[Rule Update Import Log] 詳細ビューについて

ライセンス：任意

ルール更新またはローカル ルール ファイルにインポートされた各オブジェクトの詳細レコードを表示することができます。以下の表で、[Rule Update Log] 詳細ビューのフィールドについて説明します。

表 *90 : [*ルール アップデートのインポート ログ（*Rule Update Import Log*）*]* 詳細ビューのフィールド

フィールド	説明
Time	インポートが開始された日時。
Name	インポートされたオブジェクトの名前。ルールの場合はルールの [Message] フィールドに対応した名前で、ルール更新コンポーネントの場合はコンポーネント名です。

フィールド	説明
Type	インポートされたオブジェクトのタイプで、有効な値は次のいずれかです。 • [rule update component]（ルール パックまたはポリシー パックなどの、インポートされたコンポーネント） • [rule]（新しいルールまたは更新されたルールの場合。バージョン 5.0.1 では、廃止された [update] 値の代わりにこの値が使用されます）。 • [policy apply]（インポートで [Reapply intrusion policies after the Rule Update import completes] オプションが有効だった場合）
Action	オブジェクト タイプについて、次のいずれかが発生していることを示します。 • [new]（ルール用。この ASA FirePOWER モジュールにルールが最初に格納された場合） • [changed]（ルール更新コンポーネントまたはルールで、ルール更新コンポーネントが変更された場合、ルールのリビジョン番号が大きく、GID と SID が同じだった場合） • [collision]（ルール更新コンポーネントまたはルールで、既存のコンポーネントまたはルールとリビジョンの競合によりインポートがスキップされた場合） • [deleted]（ルールで、ルール更新からルールが削除された場合） • [enabled]（ルール更新の編集用。プリプロセッサ、ルール、または他の機能がシステム提供ポリシーで有効になっている場合） • [disabled]（ルール用。システム提供ポリシーでルールが無効になっている場合） • [drop]（ルール用。システム提供ポリシーでルールが [Drop] または [Generate Events] に設定されている場合） • [error]（ルール更新またはローカル ルール ファイルで、インポートが失敗した場合） • [apply]（インポートで [Reapply intrusion policies after the Rule Update import completes] オプションが有効だった場合）
Default Action	ルールの更新によって定義されているデフォルトのアクション。インポートされたオブジェクトのタイプが [rule] の場合、デフォルトのアクションは [Pass]、[Alert]、または [Drop] になります。インポートされた他のすべてのオブジェクト タイプには、デフォルトのアクションはありません。
GID	ルールのジェネレータ ID。たとえば、1（標準テキスト ルール）または3（共有オブジェクト ルール）。
SID	ルールの SID。
Rev	ルールのリビジョン番号。
Policy	インポートされたルールの場合、このフィールドには [All] が表示されます。これは、そのインポートされたルールがすべてのシステム提供侵入ポリシーに含まれていたことを示しています。インポートされた他のタイプのオブジェクトについては、このフィールドは空白です。

フィールド	説明
Details	コンポーネントまたはルールに対する一意の文字列。ルール、GID、SID、および変更されたルールの以前のリビジョン番号については、previously (GID:SID:Rev) のように表示されます。変更されていないルールについては、このフィールドは空白です。
Count	各レコードのカウント（1）。テーブルが制限されており、[Rule Update Log] 詳細ビューがデフォルトでルール更新レコードに制限されている場合は、テーブル ビューに [Count] フィールドが表示されます。

地理情報データベースについて

ライセンス：任意

シスコ地理位置情報データベース（GeoDB）は、ルーティング可能な IP アドレスに関連付けられている地理データのデータベースです。ASA FirePOWER モジュールでは、国と大陸が提供されます。システムで、検出された IP アドレスと一致する GeoDB 情報が検出された場合は、その IP アドレスに関連付けられている地理情報を表示することができます。シスコでは、GeoDB の定期的な更新を提供しています。

GeoDB を更新するには、[Geolocation Updates] ページ（[Configuration] > [ASA FirePOWER Configuration] > [Geolocation Updates]）を使用します。GeoDB の更新をアップロードすると、このページに表示されます。

インストールには通常 30 ～ 40 分かかります。GeoDB の更新は他のシステムの機能（実行中の地理情報の収集など）を中断することはありませんが、更新が完了するまでシステムのリソースを消費します。更新を計画する場合には、この点について考慮してください。

この項では、手動による GeoDB 更新を計画および実行する方法について説明します。自動更新機能を利用して GeoDB の更新をスケジュールすることもできます。詳細については、地理情報データベースについて （595 ページ）を参照してください。

地理情報データベースを更新する方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Updates] の順に選択します。

[Product Updates] ページが表示されます。

ステップ 2 [Geolocation Updates] タブをクリックします。

[Geolocation Updates] ページが表示されます。

ステップ 3 更新をアップロードします。

ASA FirePOWER モジュールがインターネットにアクセスできる場合は、[Download and install geolocation update from the Support Site] をクリックして、以下のサポート サイトのいずれかで最新の更新を確認します。

- **Sourcefire**：（https://support.sourcefire.com/）

- シスコ：（http://www.cisco.com/cisco/web/support/index.html）
- ASA FirePOWER モジュールがインターネットにアクセスできない場合は、以下のサポート サイトのいずれかから更新を手動でダウンロードして、[Upload and install geolocation update] をクリックします。[Choose File] をクリックして、その更新に移動して選択し、[Import] をクリックします。
  - **Sourcefire**：（https://support.sourcefire.com/）
  - シスコ：（http://www.cisco.com/cisco/web/support/index.html）

（注） 手動で、または [Geolocation Updates] ページで [Download and install geolocation update from the Support Site] をクリックして、サポート サイトから更新を直接ダウンロードします。電子メールで更新ファイルを転送すると、ファイルが破損することがあります。

更新プロセスが開始されます。更新インストールの平均時間は 30 ～ 40 分です。更新の進捗は、タスク キュー（[Monitoring] > [ASA FirePOWER Monitoring] > [Task Status]）でモニタできます。

ステップ 4 更新が終了したら、[Geolocation Updates] ページに戻り、GeoDB のビルド番号が、インストールした更新と一致していることを確認します。

GeoDB を更新すると、GeoDB の以前のバージョンが上書きされ、すぐに有効になります。展開全体で GeoDB の更新が有効になるには数分かかることがありますが、更新した後にアクセス コントロール ポリシーを再適用する必要はありません。

次のタスク

第 40 章

システムのモニタリング

ASA FirePOWER モジュールでは、日常のシステム管理をサポートする多くの便利なモニタリング機能が単一のページで提供されます。たとえば、[Host Statistics] ページで、基本的なホストの統計情報のモニタができます。

ホスト統計情報の表示

ライセンス：任意

[Statistics] ページには、次の内容の現在のステータスが表示されます。

- 一般的なホスト統計情報。詳細については、表 91 : ホスト統計情報（Host Statistics） （597 ページ）の表を参照してください
- 侵入イベント情報（Protection が必要）。詳細については、イベントの表示 （487 ページ）を参照してください。

次の表に、[統計情報（Statistics）] ページにリストされるホスト統計情報を示します。

表 *91 :* ホスト統計情報（*Host Statistics*）

カテゴリ	説明
Time	システムの現在の時刻。
Uptime	システムが前回起動されてから経過した日数（該当する場合）、時間数、および分数。
Memory Usage	使用中のシステム メモリの割合。

カテゴリ	説明
Load Average	直前の 1 分間、5 分間、15 分間の CPU キュー内の平均プロセス数。
Disk Usage	使用中のディスクの割合。詳細なホスト統計情報を表示するには、矢印をクリックします。詳細については、「システム ステータスとディスク領域使用率のモニタリング （598 ページ）」を参照してください。
Processes	システムで実行されているプロセスの概要。詳細については、「システム ステータスとディスク領域使用率のモニタリング （598 ページ）」を参照してください。

[Statistics] ページを表示する方法：

[Monitoring] > [ASA FirePOWER Monitoring] > [Statistics] の順に選択します。

[Statistics] ページが表示されます。

システムステータスとディスク領域使用率のモニタリング

ライセンス：任意

[Statistics] ページの [Disk Usage] セクションには、カテゴリ別およびパーティション ステータス別に、ディスク使用率の簡単な概要が表示されます。マルウェア ストレージ パックがデバイスにインストールされている場合、そのパーティション ステータスも確認できます。このページを定期的に監視して、システム プロセスおよびデータベースで十分なディスク領域が使用可能であることを確認できます。

ディスク使用量情報にアクセスする方法：

ステップ 1 [Monitoring] > [ASA FirePOWER Monitoring] > [Statistics] の順に選択します。

[Statistics] ページが表示されます。

ディスク使用量カテゴリの詳細については、Disk Usage ウィジェットについて （521 ページ）を参照してください。

ステップ 2 展開するには、[Total] の横にある下矢印をクリックします。

[Disk Usage] セクションが展開され、パーティションの使用状況が表示されます。マルウェア ストレージ パックがインストールされている場合は、/var/storage パーティションの使用状況も表示されます。

システム プロセス ステータスについて

ライセンス：任意

[Host Statistics] ページの [Processes] セクションでは、アプライアンスで現在実行中のプロセスを確認できます。これは、一般的なプロセス情報と、実行中の各プロセスに固有の情報を提供します。

次の表に、プロセス リストに表示される各列を示します。

表 *92 :* プロセス ステータス

カラム	説明
Pid	プロセス ID 番号
Username	プロセスを実行しているユーザまたはグループの名前
Pri	プロセスの優先度
Nice	*nice* 値。プロセスのスケジューリング優先度を示す値です。値は -20（最も高い優先度）から 19（最も低い優先度）までの範囲になります。
Size	プロセスで使用されるメモリ サイズ（値の後ろにメガバイトを表す m がない場合はキロバイト単位）
Res	メモリ内の常駐ページング ファイルの量（値の後ろにメガバイトを表す m がない場合はキロバイト単位）
State	プロセスの状態： • D - プロセスが中断不能スリープ状態（通常は入出力）にある • N - プロセスの nice 値が正の値 • R - プロセスが実行可能である（実行するキュー上で） • S - プロセスがスリープ モードにある • T - プロセスがトレースまたは停止されている • W - プロセスがページングしている • X - プロセスがデッド状態である • Z - プロセスが機能していない • < - プロセスの nice 値が負の値
Time	プロセスが実行されている時間（時間 : 分 : 秒）
Cpu	プロセスが使用している CPU の割合

カラム	説明
コマンド	

システム プロセス ステータスの表示

プロセスの実行可能ファイル名

プロセス リストを展開する方法：

ステップ 1 [Monitoring] > [ASA FirePOWER Monitoring] > [Statistics] の順に選択します。

[Statistics] ページが表示されます。

ステップ 2 [Processes] の横にある下矢印をクリックします。

プロセス リストが展開され、実行中のタスクの数やタイプ、現在の時刻、現在のシステム稼働時間、システムの負荷平均、CPU、メモリ、およびスワップ情報などの、一般的なプロセス ステータス情報と、実行中の各プロセスに関する固有の情報がリストされます。

[Cpu(s)] は、以下の CPU 使用状況情報をリストします。

- ユーザ プロセスの使用状況の割合
- システム プロセスの使用状況の割合
- nice 使用状況の割合（高い優先度を示す、負の nice 値を持つプロセスの CPU 使用状況）

nice 値は、システム プロセスのスケジュールされた優先度を示しており、-20（最も高い優先度）から 19（最も低い優先度）の範囲の値になります。

- アイドル状態の使用状況の割合

[Mem] は、以下のメモリ使用状況情報をリストします。

- メモリ内の合計キロバイト数
- メモリ内の使用キロバイト数の合計
- メモリ内の空きキロバイト数の合計
- メモリ内のバッファに書き出されたキロバイト数の合計

[Swap] は、以下のスワップ使用状況情報をリストします。

- スワップ内の合計キロバイト数
- スワップ内の使用キロバイト数の合計
- スワップ内の空きキロバイト数の合計
- スワップ内のキャッシュされたキロバイト数の合計

（注） アプライアンスで実行されるプロセスのタイプの詳細については、実行可能ファイルおよびシステム ユーティリティについて （602 ページ）を参照してください。

次のタスク

プロセス リストを折りたたむには、次の手順に従います。

[Processes] の横にある上矢印をクリックします。

プロセス リストが折りたたまれます。

実行されるプロセスについて

ライセンス：任意

アプライアンスで実行されるプロセスには、デーモンと実行可能ファイルの 2 種類があります。デーモンは常に実行され、実行可能ファイルは必要に応じて実行されます。

システム デーモンについて

ライセンス：任意

デーモンは、アプライアンスで継続的に実行されます。これにより、サービスが使用可能になり、必要に応じてプロセスが生成されるようになります。次の表では、[Process Status] ページに表示されるデーモンをリストし、その機能について簡単に説明します。

（注） 次の表は、アプライアンスで実行される可能性があるすべてのプロセスの包括的なリストではありません。

表 *93* : システム デーモン

デーモン	説明
crond	スケジュールされたコマンド（cron ジョブ）の実行を管理します
dhclient	ダイナミック ホスト IP アドレッシングを管理します
httpd	HTTP（Apache Web サーバ）プロセスを管理します
httpsd	HTTPS（SSL を使用した Apache Web サーバ）サービスを管理し、SSL および有効な証明書の認証が機能しているかチェックし、アプライアンスへの安全な Web アクセスを提供するためにバックグラウンドで実行します。
keventd	Linux カーネルのイベント通知メッセージを管理します

デーモン	説明
klogd	Linux カーネル メッセージのインターセプションおよびロギングを管理します
kswapd	Linux カーネルのスワップ メモリを管理します
kupdated	ディスクの同期を実行する、Linux カーネルの更新プロセスを管理します
mysqld	ASA FirePOWER モジュール データベース プロセスを管理します
ntpd	Network Time Protocol（NTP）プロセスを管理します
pm	すべてのシスコ プロセスを管理し、必要なプロセスを始動し、予期せずに失敗したプロセスをすべて再始動します
reportd	レポートを管理します
safe_mysqld	データベースのセーフ モード運用を管理し、エラーが発生した場合にはデータベース デーモンを再始動し、ランタイム情報をファイルに記録します
sfmgr	アプライアンスへの sftunnel 接続を使用して、リモートでアプライアンスを管理および設定するための RPC サービスを提供します
sftroughd	着信ソケットで接続をリッスンしてから、正しい実行可能ファイル（通常は、Cisco メッセージ ブローカ sfmb）を呼び出して要求を処理します
sftunnel	リモート アプライアンスとの通信を必要とするすべてのプロセスに対し、安全な通信チャネルを提供します。
sshd	Secure Shell (SSH) プロセスを管理し、アプライアンスへの SSH アクセスを提供するためにバックグラウンドで実行します
syslogd	システム ロギング（syslog）プロセスを管理します

実行可能ファイルおよびシステム ユーティリティについて

ライセンス：任意

システム上には、他のプロセスまたはユーザ操作によって実行される実行可能ファイルが数多く存在します。次の表で、[Process Status] ページに表示される実行可能ファイルについて説明します。

表 *94 :* システムの実行可能ファイルおよびユーティリティ

実行可能	説明
awk	awk プログラミング言語で作成されたプログラムを実行するユーティリティ

実行可能	説明
bash	GNU Bourne-Again シェル
cat	ファイルを読み取り、コンテンツを標準出力に書き込むユーティリティ
chown	ユーザおよびグループのファイル権限を変更するユーティリティ
chsh	デフォルトのログイン シェルを変更するユーティリティ
cp	ファイルをコピーするユーティリティ
df	アプライアンスの空き領域の量をリストするユーティリティ
echo	コンテンツを標準出力に書き込むユーティリティ
egrep	指定された入力を、ファイルおよびフォルダで検索するユーティリティ。標準 grep でサポートされていない正規表現の拡張セットをサポートします
find	指定された入力のディレクトリを再帰的に検索するユーティリティ
grep	指定された入力をファイルとディレクトリで検索するユーティリティ
halt	サーバを停止するユーティリティ
httpsdctl	セキュアな Apache Web プロセスを処理する
hwclock	ハードウェア クロックへのアクセスを許可するユーティリティ
ifconfig	ネットワーク構成実行可能ファイルを示します。MAC アドレスが常に一定になるようにします
iptables	[Access List] ページに加えられた変更に基づいてアクセス制限を処理します。アクセス権の設定の詳細については、アプライアンスのアクセス リストの設定 （553 ページ）を参照してください。
iptables-restore	iptables ファイルの復元を処理します
iptables-save	iptables に対する保存済みの変更を処理します
kill	セッションおよびプロセスを終了するために使用できるユーティリティ
killall	すべてのセッションおよびプロセスを終了するために使用できるユーティリティ
ksh	Korn シェルのパブリック ドメイン バージョン
logger	コマンドラインから syslog デーモンにアクセスする方法を提供するユーティリティ

実行可能	説明
md5sum	指定したファイルのチェックサムとブロック数を印刷するユーティリティ
mv	ファイルを移動（名前変更）するユーティリティ
myisamchk	データベース テーブルの検査および修復を示します
mysql	データベース プロセスを示します。複数のインスタンスが表示されることがあります
openssl	認証証明書の作成を示します。
perl	perl プロセスを示します。
ps	標準出力にプロセス情報を書き込むユーティリティ
sed	1 つ以上のテキスト ファイルの編集に使用されるユーティリティ
sh	Korn シェルのパブリック ドメイン バージョン
shutdown	アプライアンスをシャットダウンするユーティリティ
sleep	指定された秒数のあいだプロセスを中断するユーティリティ
smtpclient	電子メール イベント通知機能が有効な場合に、電子メール送信を処理するメール クライアント
snmptrap	SNMP 通知機能が有効な場合に、指定された SNMP トラップ サーバに SNMP トラップ データを転送します
snort（Protection が必要）	Snort が動作していることを示します
ssh	アプライアンスへの Secure Shell (SSH) 接続を示します
sudo	sudo プロセスを示します。これにより、admin 以外のユーザが実行可能ファイルを実行できるようになります
top	上位の CPU プロセスに関する情報を表示するユーティリティ
touch	指定したファイルへのアクセス時刻や変更時刻を変更するために使用できるユーティリティ
vim	テキスト ファイルの編集に使用されるユーティリティ
wc	指定したファイルの行、ワード、バイトのカウントを実行するユーティリティ

第 41 章

バックアップと復元の使用

バックアップ/復元は、システム保守プランの重要な部分です。各組織のバックアップ計画は高度に個別化されていますが、ASA FirePOWER モジュールにはデータをアーカイブするメカニズムがあり、障害発生時にはデータを復元できます。

バックアップ対象は次のとおりです。

- アクセス ポリシー、侵入ポリシー、およびアイデンティティ ポリシー
- ローカル データベース
- イベント

バックアップと復元に関する次の制限事項に注意してください。

- バックアップは、バックアップを作成した製品バージョンに対してのみ有効です。
- バックアップの復元は、そのバックアップの作成に使用したものと同じバージョンの ASA FirePOWER モジュール ソフトウェアを実行している場合のみ可能です。

注意 ASA FirePOWER モジュール間で設定ファイルをコピーするために、バックアップおよび復元プロセスを使用しないでください。設定ファイルには、ASA FirePOWER モジュールを一意に識別する情報が含まれているため、共有することはできません。

注意 侵入ルールのアップデートを適用した場合、それらのアップデートはバックアップされません。復元**後に**、最新のルールのアップデートを適用する必要があります。

アプライアンスまたはローカル コンピュータにバックアップ ファイルを保存できます。

- バックアップ ファイルの作成 （606 ページ）
- バックアップ プロファイルの作成 （607 ページ）
- ローカル ホストからのバックアップのアップロード （608 ページ）
- バックアップ ファイルからのアプライアンスの復元 （609 ページ）

バックアップ ファイルの作成

ライセンス：任意

ASA FirePOWER モジュールのバックアップは、モジュール インターフェイスを使用して実行できます。既存のシステム バックアップを表示して使用するには、[Backup Management] ページに移動します。イベントデータに加えて、アプライアンスの復元に必要なすべてのコンフィギュレーション ファイルを含むバックアップ ファイルを定期的に保存する必要があります。設定の変更をテストする際にも、システムをバックアップして、必要に応じて保存されている設定に戻せるようにすることができます。バックアップ ファイルを、アプライアンスに保存するか、ローカル コンピュータに保存するかを選択できます。

アプライアンスに十分なディスク スペースがない場合は、バックアップ ファイルを作成できません。バックアップ プロセスが使用可能なディスク スペースの 90% 以上を使用する場合、バックアップは失敗することがあります。必要に応じて、古いバックアップ ファイルを削除するか、古いバックアップ ファイルをアプライアンスの外部に転送してください。

あるいは、バックアップ ファイルが 4GB を超える場合は、SCP 経由でリモート ホストにコピーします。バックアップ ファイルが 4 GB を超えている場合、ローカル コンピュータからのバックアップのアップロードは実行できません。

注意 セキュリティ ゾーンとのインターフェイスのアソシエーションを設定してある場合、それらのアソシエーションはバックアップされません。それらは、復元後に再設定する必要があります。詳細はセキュリティ ゾーンの操作 （64 ページ）を参照してください。

ASA FirePOWER モジュールのバックアップ ファイルを作成するには、次の手順を実行します。

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Tools] > [Backup/Restore] の順に選択します。

[Backup Management] ページが表示されます。

ステップ 2 [Device Backup] をクリックします。

[Create Backup] ページが表示されます。

ステップ 3 [Name] フィールドに、バックアップ ファイルの名前を入力します。英数字、句読記号、およびスペースを使用できます。

ステップ 4 オプションで、バックアップの完了時に通知を受けるためには、[Email] チェック ボックスをオンにして、用意されているテキスト ボックスに電子メール アドレスを入力します。

（注） 電子メール通知を受信するには、メール リレー ホストおよび通知アドレスの設定 （556 ページ）で説明されているように、リレー ホストを設定する必要があります。

ステップ 5 必要に応じて、Secure Copy Protocol（SCP）を使用してバックアップ アーカイブを異なるマシンにコピーするには、[Copy when complete] チェックボックスをオンにしてから、用意されているテキスト ボックスに以下の情報を入力します。

- [Host] フィールド：バックアップのコピー先となるマシンのホスト名または IP アドレス
- [Path] フィールド：バックアップのコピー先となるディレクトリへのパス
- User] フィールド：リモート マシンへのログインに使用するユーザ名
- [Password] フィールド：そのユーザ名のパスワード。パスワードの代わりに SSH 公開キーを使用してリモートマシンにアクセスする場合は、[SSH Public Key] フィールドの内容を、そのマシンの指定ユーザの authorized_keys ファイルにコピーします。

このオプションをオフにする場合、バックアップ中に使用された一時ファイルがシステムによってリモート サーバに保存されます。このオプションをオンにする場合は、一時ファイルはリモート サーバに保存されません。

ヒント Cisco は、システム障害が発生した場合にアプライアンスを復元できるように、バックアップをリモート ロケーションに定期的に保存することを推奨します。

ステップ 6 次の選択肢があります。

- バックアップ ファイルをアプライアンスに保存するには、[Start Backup] をクリックします。

バックアップ ファイルは /var/sf/backup ディレクトリに保存されます。

バックアップ プロセスが完了すると、[Restoration Database] ページでファイルを参照できます。バックアップ ファイルを復元する方法について詳しくは、バックアップ ファイルからのアプライアンスの復元 （609 ページ）を参照してください。

- この設定を後で使用できるバックアップ プロファイルとして保存するには、[Save as New] をクリックします。

バックアップ プロファイルを変更または削除するには、[Configuration] > [ASA FirePOWER Configuration] > [Tools] > [Backup/Restore] の順に選択して、[Backup Profiles] をクリックします。詳細については、「バックアップ プロファイルの作成 （607 ページ）」を参照してください。

バックアップ プロファイルの作成

ライセンス：任意

[Backup Profiles] ページを使用して、さまざまな種類のバックアップに使用する設定値を含むバックアップ プロファイルを作成できます。後にアプライアンスのファイルをバックアップするときに、これらのプロファイルの 1 つを選択できます。

ヒント　バックアップ ファイルの作成 （606 ページ）で説明されているようにバックアップ ファイルを作成すると、バックアップ プロファイルが自動的に作成されます。

バックアップ プロファイルの作成方法：

ステップ 1　[Configuration] > [ASA FirePOWER Configuration] > [Tools] > [Backup/Restore] の順に選択します。

[Backup Management] ページが表示されます。

ステップ 2　[Backup Profiles] タブをクリックします。

[Backup Profiles] ページが開き、既存のバックアップ プロファイルのリストが表示されます。

ヒント　編集アイコンをクリックして既存のプロファイルを変更するか、または削除アイコンをクリックしてリストからプロファイルを削除することができます。

ステップ 3　[Create Profile] をクリックします。

[Create Backup] ページが表示されます。

ステップ 4　バックアップ プロファイルの名前を入力します。英数字、句読記号、およびスペースを使用できます。

ステップ 5　バックアップ プロファイルを必要に合わせて設定します。

このページのオプションについて詳しくは、バックアップ ファイルの作成 （606 ページ）を参照してください。

ステップ 6　バックアップ プロファイルを保存するには、[Save as New] をクリックします。

[Backup Profiles] ページが開き、新しいプロファイルがリストに表示されます。

ローカル ホストからのバックアップのアップロード

ライセンス：任意

表「バックアップ管理」で説明されているダウンロード機能を使用してローカルホストにバックアップ ファイルをダウンロードした場合は、ASA FirePOWER モジュールにそのファイルをアップロードできます。

バックアップ ファイルに PKI オブジェクトが含まれている場合、内部 CA と内部証明書オブジェクトに関連付けられた秘密キーは、アップロードの際にランダムに生成されるキーによって再暗号化されます。

ヒント　ローカルホストからは、4GB より大きいバックアップはアップロードできません。代わりに、バックアップを SCP 経由でリモート ホストにコピーし、そこから取得することができます。

ローカル ホストからバックアップをアップロードする方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Tools] > [Backup/Restore] の順に選択します。

[Backup Management] ページが表示されます。

ステップ 2 [Upload Backup] をクリックします。

[Upload Backup] ページが表示されます。

ステップ 3 [Choose File] をクリックして、アップロードするバックアップ ファイルに移動します。

アップロードするファイルを選択した後に、[Upload Backup] をクリックします。

ステップ 4 [Backup Management] をクリックして、[Backup Management] ページに戻ります。

バックアップ ファイルがアップロードされ、バックアップ リストに表示されます。ASA FirePOWER モジュールによってファイルの整合性が検証されたら、[Backup Management] ページを更新して、詳細なファイル システム情報を確認します。

バックアップ ファイルからのアプライアンスの復元

ライセンス：任意

[Backup Management] ページを使用して、バックアップ ファイルからアプライアンスを復元できます。バックアップを復元するには、バックアップ ファイル内の VDB のバージョンが、アプライアンスの現在の VDB のバージョンと一致している必要があります。復元プロセスが完了したら、シスコの最新のルール アップデートを適用する必要があります。

⚠

注意 仮想 Firepower Management Center で作成されたバックアップを物理 Firepower Management Center に復元しないでください。システム リソースに負荷をかける可能性があります。仮想バックアップを物理 Firepower Management Center に復元する必要がある場合は、サポートに連絡してください。

バックアップ ファイルに PKI オブジェクトが含まれている場合、内部 CA と内部証明書オブジェクトに関連付けられた秘密キーは、アップロードの際にランダムに生成されるキーによって再暗号化されます。

ローカル ストレージを使用する場合、バックアップ ファイルは /var/sf/backup に保存されて、/var パーティションで使用されているディスク領域の量とともに [Backup Management] ページの下部に一覧表示されます。

（注） バックアップが完了した後にライセンスを追加した場合は、このバックアップを復元するときに、それらのライセンスが削除されたり上書きされたりすることはありません。復元の際の競合を防止するためにも、バックアップを復元する前に、これらのライセンスを（それらが使用されている場所をメモした上で）削除し、バックアップを復元した後で、追加して再設定してください。競合が発生した場合は、サポートに連絡してください。

次の表では、[Backup Management] ページの各列とアイコンについて説明します。

表 *95 :* バックアップ管理（*Backup Management*）

機能	説明
System Information	元のアプライアンスの名前、タイプ、バージョン。バックアップを復元できるのは、同一のアプライアンス タイプとバージョンに対してだけであることに注意してください。
Date Created	バックアップ ファイルが作成された日時
File Name	バックアップ ファイルのフルネーム
VDB Version	バックアップ時にアプライアンスで実行されている脆弱性データベース（VDB）のビルド。
Location	バックアップ ファイルの場所
Size (MB)	バックアップ ファイルのサイズ（メガバイト）
View	バックアップ ファイルの名前をクリックすると、圧縮されたバックアップ ファイルに含まれるファイルのリストが表示されます。
Restore	バックアップ ファイルが選択された状態でクリックすると、そのバックアップ ファイルがアプライアンスに復元されます。VDB バージョンがバックアップ ファイルの VDB のバージョンと一致しない場合、このオプションは無効になります。
Download	バックアップ ファイルが選択された状態でクリックすると、そのバックアップ ファイルがローカル コンピュータに保存されます。
Delete	バックアップ ファイルが選択された状態でクリックすると、そのバックアップ ファイルが削除されます。
Move	以前に作成したローカル バックアップを選択した状態でクリックすると、そのバックアップが指定のリモート バックアップ ロケーションに送信されます。

バックアップ ファイルからのアプライアンスの復元方法：

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Tools] > [Backup/Restore] の順に選択します。

[Backup Management] ページが表示されます。

ステップ 2 バック アップ ファイルの内容を確認するには、ファイルの名前をクリックします。

マニフェストが表示され、各ファイルの名前、所有者と権限、およびファイル サイズと日付がリストされます。

ステップ 3 [Backup Management] をクリックして、[Backup Management] ページに戻ります。

ステップ 4 復元するバックアップ ファイルを選択して、[Restore] クリックします。

[Restore Backup] ページが表示されます。

バックアップの VDB バージョンがアプライアンスに現在インストールされている VDB のバージョンと一致しない場合、[Restore] ボタンはグレー表示されることに注意してください。

注意 この手順では、すべての設定ファイルが上書きされます。

ステップ 5 ファイルを復元するには、[Replace Configuration Data] を選択します。

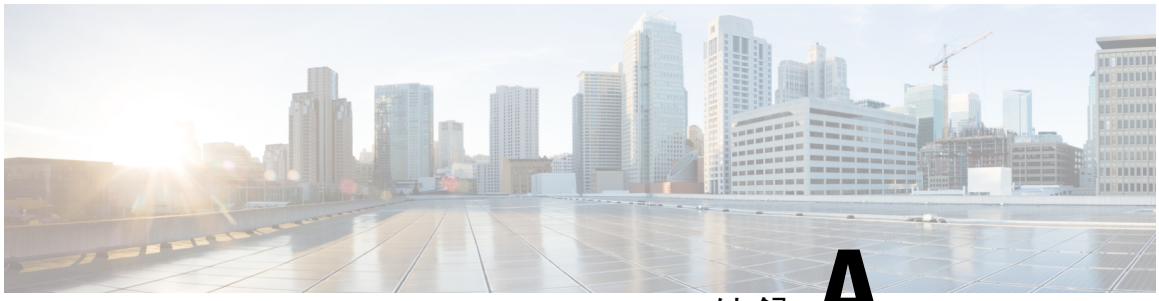
ステップ 6 [Restore] クリックして、復元を開始します。

アプライアンスが、指定したバックアップ ファイルを使用して復元されます。

ステップ 7 アプライアンスをリブートします。

ステップ 8 シスコの最新のルール アップデートを適用して、ルール アップデートを再適用します。

ステップ 9 復元されたシステムにポリシーを展開します。



付録 A

トラブルシューティング ファイルの生成

アプリケーションで問題が発生したときに、サポートから問題の診断を容易にするためにトラブルシューティング ファイルの作成を依頼されることがあります。次の表に示すオプションのいずれかを選択して、ASA FirePOWER モジュールから報告されるトラブルシューティング データをカスタマイズすることができます。

表 *96* : 選択可能なトラブルシュート オプション

オプション	報告内容
Snort Performance and Configuration	アプライアンス上の Snort に関連するデータとコンフィギュレーション設定
Hardware Performance and Logs	アプライアンス ハードウェアのパフォーマンスに関連するデータとログ
System Configuration, Policy, and Logs	アプライアンスの現在のシステム設定に関連するコンフィギュレーション設定、データ、およびログ
Detection Configuration, Policy, and Logs	アプライアンス上の検出に関連するコンフィギュレーション設定、データ、およびログ
Interface and Network Related Data	アプライアンスのインラインセットとネットワーク設定に関連するコンフィギュレーション設定、データ、およびログ
Discovery, Awareness, VDB Data, and Logs	アプライアンス上の現在の検出設定と認識設定に関連するコンフィギュレーション設定、データ、およびログ
Upgrade Data and Logs	アプライアンスの以前のアップグレードに関連するデータとログ
All Database Data	トラブルシュート レポートに含まれるすべてのデータベース関連データ
All Log Data	アプライアンス データベースによって収集されたすべてのログ
Network Map Information	現在のネットワーク トポロジ データ

一部のオプションは報告するデータの観点で重複していますが、どのオプションが選択されたかに関係なく、トラブルシューティング ファイルには冗長なコピーは含まれません。

アプライアンス トラブルシューティング ファイルの生成

ライセンス：任意

次の手順を使用して、サポートに送信可能なカスタマイズされたトラブルシューティング ファイルを生成できます。

トラブルシューティング ファイルを生成する方法：

ステップ 1 ASDM で、[Configuration] > [ASA FirePOWER Configuration] > [Tools] > [Troubleshooting] の順に選択します。

ステップ 2 [Generate Troubleshooting Files] をクリックします。

[Troubleshooting Options] ポップアップ ウィンドウが表示されます。

ステップ 3 [All Data] を選択して可能性のあるすべてのトラブルシューティング データを生成することも、個別のチェック ボックスをオンにしてレポートをカスタマイズすることもできます。詳細については、表 96 : 選択可能なトラブルシュート オプション （613 ページ）の表を参照してください。

ステップ 4 [OK] をクリックします。

ASA FirePOWER モジュールからトラブルシューティング ファイルが生成されます。タスク キュー（[Monitoring] > [ASA FirePOWER Monitoring] > [Task Status]）でファイル生成プロセスをモニタできます。

ステップ 5 次の項（トラブルシューティング ファイルのダウンロード （614 ページ））の手順に進みます。

トラブルシューティング ファイルのダウンロード

ライセンス：任意

次の手順を使用して、生成されたトラブルシューティング ファイルのコピーをダウンロードします。

トラブルシューティング ファイルをダウンロードする方法：

ステップ 1 ASDM で、[Monitoring] > [ASA FirePOWER Monitoring] > [Task Status] の順に選択します。

[Task Status] ページが表示されます。

ステップ 2 生成されたトラブルシューティング ファイルに対応するタスクを探します。

ステップ 3 アプライアンスがトラブルシューティング ファイルを生成し、タスク ステータスが [Completed] に変ったら、[Click to retrieve generated files] をクリックします。

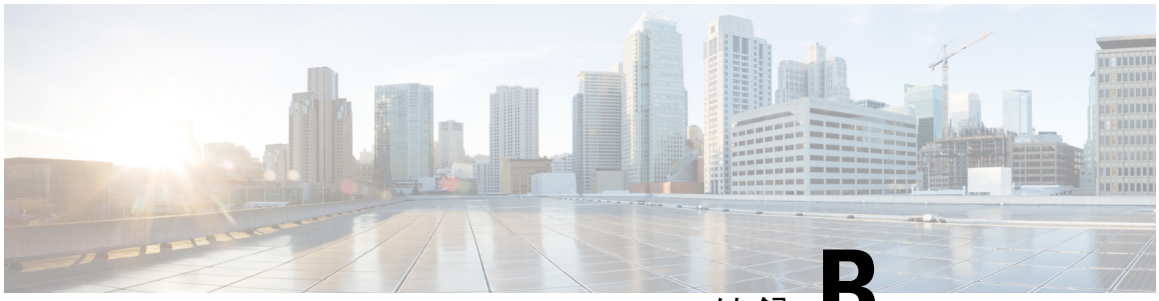
ステップ 4 ブラウザのプロンプトに従ってファイルをダウンロードします。

トラブルシューティング ファイルの生成

ファイルは単一の .tar.gz ファイルとしてダウンロードされます。

ステップ 5 サポートの指示に従って、トラブルシューティング ファイルを Cisco に送信してください。

トラブルシューティング ファイルの生成



付録 B

設定のインポートおよびエクスポート

インポート/エクスポート機能を使用して、ポリシーを含む複数のタイプの設定を、1つのアプライアンスから同じタイプの別のアプライアンスにコピーにできます。設定のインポートおよびエクスポートは、バックアップ ツールとして設計されてはいませんが、新しい ASA FirePOWER モジュールを追加するプロセスを簡素化するために使用できます。

以下の設定をインポートおよびエクスポートできます。

- アクセス コントロール ポリシーとその関連するネットワーク分析ポリシー、SSL ポリシー、およびファイル ポリシー
- 侵入ポリシー
- システム ポリシー
- アラート応答

エクスポートされた設定をインポートするには、両方の ASA FirePOWER モジュールで同じソフトウェア バージョンを実行している必要があります。エクスポートされた侵入ポリシーまたはアクセス コントロール ポリシーをインポートするには、両方のアプライアンスでルール更新のバージョンも一致している必要があります。

（注） バージョンが一致している場合、ASDM で管理された ASA with FirePOWER Services デバイスからエクスポートしたポリシーを、Firepower Management Center で管理されたデバイスにインポートできます。

- 設定のエクスポート （617 ページ）
- 設定のインポート （620 ページ）

設定のエクスポート

ライセンス：任意

設定のインポートおよびエクスポート

単一の設定をエクスポートすることや、（同じタイプまたは異なるタイプの）一連の設定を同時にエクスポートすることができます。後に別のアプライアンスにパッケージをインポートするとき、パッケージ内のどの設定をインポートするかを選択できます。

設定をエクスポートするとき、アプライアンスは、その設定のリビジョン情報もエクスポートします。ASA FirePOWER モジュールはその情報を使用して、別のアプライアンスにその設定をインポートできるかどうかを判別します。アプライアンスにすでに存在する設定リビジョンをインポートすることはできません。

また、設定をエクスポートするときには、その設定が依存するシステム設定も、アプライアンスによってエクスポートされます。

ヒント ASA FirePOWER モジュールの多くのリスト ページ には、リスト項目の横にエクスポート アイコンがあります。このアイコンがある場合は、それを使用することにより、その後のエクスポート操作を簡単に代行させることができます。

以下の設定をエクスポートできます。

- アラート応答：アラート応答は、アラートの送信先とする予定の外部システムと ASA FirePOWER モジュールが対話できるようにするための一連の設定です。
- アクセス コントロール ポリシー：アクセス コントロール ポリシーには、システムがネットワーク トラフィックをどのように管理するかを指定するために設定できる、さまざまなコンポーネントが含まれます。これらのコンポーネントには、アクセス コントロール ルール、関連する侵入ポリシー、ファイル ポリシー、およびネットワーク分析ポリシー、およびSSL ポリシー、および侵入の変数セットを含むルールとポリシーが使用するオブジェクトが含まれています。アクセス コントロール ポリシーをエクスポートすると、そのポリシーのすべての設定とコンポーネントもエクスポートされます。ただし、複数のアプライアンスで同等であり、ユーザが変更できない URL レピュテーションとカテゴリは（それらが存在しても）エクスポートされません。アクセス コントロール ポリシーをインポートするには、エクスポート元とインポート先の ASA FirePOWER モジュールでルール アップデートのバージョンが一致している必要があります。

エクスポートするアクセス コントロール ポリシー、またはそのポリシーが呼び出す SSL ポリシーには、地理位置情報データを参照するルールが含まれている場合、インポート先モジュールの地理位置情報データベース（GeoDB）のアップデート バージョンが使用されます。

- 侵入ポリシー：侵入ポリシーには、ネットワーク トラフィックを検査して侵入やポリシー違反を見つけるように設定できる、さまざまなコンポーネントが組み込まれています。これらのコンポーネントは、プロトコル ヘッダー値、ペイロード コンテンツ、特定のパケット サイズの特性、および他の詳細設定を検査する侵入ルールです。

侵入ポリシーをエクスポートすると、そのポリシーのすべての設定もエクスポートされます。たとえば、イベントを生成するルールを設定するように選択した場合、ルールの SNMP アラートを設定した場合、またはポリシーで機密データ プリプロセッサをオンにした場合は、エクスポートされるポリシー内にそれらの設定値が保持されます。カスタム ルール、カスタム ルールの分類、およびユーザ定義変数も、ポリシーと共にエクスポートされます。

レイヤを使用する侵入ポリシーをエクスポートする場合、そのレイヤが2番目の侵入ポリシーによって共有されているときは、エクスポートするポリシーにその共有レイヤがコピーされて、共有関係はなくなることに注意してください。侵入ポリシーを別のアプライアンスにインポートするときは、インポートするポリシーをニーズに合うように編集できます。レイヤの削除、追加、共有などができます。

1 つの ASA FirePOWER モジュールから別の ASA FirePOWER モジュールに侵入ポリシーをエクスポートする場合、2 つ目の ASA FirePOWER モジュールのデフォルト変数の設定が異なっている場合は、インポートされたポリシーの動作が異なることがあります。

（注） インポート/エクスポート機能を使用して、脆弱性調査チーム（VRT）が作成したルールをアップデートすることはできません。代わりに、最新バージョンのルール アップデートをダウンロードして適用します。ルール更新とローカル ルール ファイルのインポート（582 ページ）を参照してください。

- システム ポリシー：システム ポリシーは、時間設定や SNMP 設定などを含む、展開内の他の ASA FirePOWER モジュールに類似している可能性のある ASA FirePOWER モジュールの側面を制御します。

（注） エクスポートされる設定の数や、それらのオブジェクトが参照する設定の数によっては、エクスポート プロセスに数分かかる場合があります。

一つ以上の設定をエクスポートする方法：

ステップ 1 設定のエクスポート元の ASA FirePOWER モジュールと設定のインポート先の ASA FirePOWER モジュールで、同じバージョンが実行されていることを確認します。侵入ポリシーまたはアクセス コントロール ポリシーをエクスポートする場合は、ルールのアップデート バージョンが一致することを確認します。

ASA FirePOWER モジュールのバージョン（および該当する場合はルールのアップデート バージョン）が一致しない場合、インポートは失敗します。

ステップ 2 [Configuration] > [ASA FirePOWER Configuration] > [Tools] > [Import Export] の順に選択します。 > > >

[Import/Export] ページが開き、ASA FirePOWER モジュール上の設定のリストが表示されます。エクスポートする設定がない設定カテゴリは、このリストに表示されないことに注意してください。

ヒント 設定のリストは、設定タイプの横にある折りたたみアイコンをクリックして折りたたむことができます。設定を確認するには、設定タイプの横にあるフォルダ展開アイコンをクリックします。

ステップ 3 エクスポートする設定の横にあるチェック ボックスを選択して、[Export] をクリックします。

ステップ 4 プロンプトに従って、エクスポートされたパッケージをコンピュータに保存します。

設定のインポート

ライセンス：任意

ASA FirePOWER モジュールから設定をエクスポートした後に、その設定が別のモジュールでもサポートされていれば、そのモジュールにインポートできます。

インポートしている設定のタイプに応じて、以下の点に注意する必要があります。

- 設定のインポート先の ASA FirePOWER モジュールと設定のエクスポートに使用した ASA FirePOWER モジュールで、同じバージョンが実行されていることを確認します。侵入ポリシーまたはアクセス コントロール ポリシーをインポートする場合は、両方のアプライアンスでルールのアップデート バージョンも一致している必要があります。バージョンが一致しない場合、インポートは失敗します。

（注） バージョンが一致している場合、ASDM で管理された ASA with FirePOWER Services デバイスからエクスポートしたポリシーを、Firepower Management Center で管理されたデバイスにインポートできます。

- ゾーンに基づいてトラフィックを評価するアクセス コントロール ポリシーをインポートした場合、インポートしたポリシー内のゾーンを、インポート先の ASA FirePOWER モジュールのゾーンにマッピングする必要があります。ゾーンをマッピングするときは、それらのタイプが一致している必要があります。したがって、インポートを開始する前に、インポート先の ASA FirePOWER モジュールで必要となるゾーン タイプを作成する必要があります。セキュリティ ゾーンについて詳しくは、セキュリティ ゾーンの操作 （64 ページ）を参照してください。
- 既存のオブジェクトやグループと同一の名前を持つオブジェクトやオブジェクト グループを含むアクセス コントロール ポリシーをインポートする場合は、オブジェクトやグループの名前を変更する必要があります。
- アクセス コントロール ポリシーや侵入ポリシーをインポートする場合、インポート プロセスによって、デフォルト変数セットに含まれる既存のデフォルト変数が、インポートされたデフォルト変数に置換されます。既存のデフォルト変数セットに、インポートされたカスタム変数セットに存在しないカスタム変数が含まれる場合、一意的な変数が保持されます。
- 侵入ポリシーをインポートするとき、その侵入ポリシーが 2 番目の侵入ポリシーの共有レイヤを使用していた場合は、エクスポート プロセスによって共有関係が切断されて、それまで共有されていたレイヤがパッケージにコピーされます。つまり、インポートされた侵入ポリシーに共有レイヤは含まれません。

（注） インポート/エクスポート機能を使用して、脆弱性調査チーム（VRT）が作成したルールをアップデートすることはできません。代わりに、最新バージョンのルール アップデートをダウンロードして適用します。ルール更新とローカル ルール ファイルのインポート （582 ページ）を参照してください。

1 つのパッケージで複数の設定をエクスポートできるため、パッケージのインポート時に、パッケージ内のどの設定をインポートするかを選択する必要があります。

設定をインポートしようとすると、ASA FirePOWER モジュールは、その設定がアプライアンスにすでに存在しているかどうかを判別します。競合がある場合は、以下の操作が可能です。

- 既存の設定を維持する、
- 既存の設定を新しい設定に置き換える、
- 最新の設定を維持する、または
- 設定を新しい設定としてインポートする。

設定をインポートした後に、宛先システムで設定を変更してその設定を再インポートすると、保持する設定のバージョンを選択する必要があります。

インポートされる設定の数や、それらのオブジェクトが参照する設定の数によっては、プロセスに数分かかる場合があります。

一つ以上の設定をインポートする方法：

ステップ 1 設定のエクスポート元の ASA FirePOWER モジュールと設定のインポート先のモジュールで、同じバージョンが実行されていることを確認します。侵入ポリシーまたはアクセス コントロール ポリシーをインポートする場合は、ルールのアップデート バージョンが一致することも確認する必要があります。

ASA FirePOWER モジュールのバージョン（および該当する場合はルールのアップデート バージョン）が一致しない場合、インポートは失敗します。

ステップ 2 インポートする設定をエクスポートします。設定のエクスポート （617 ページ）を参照してください。

ステップ 3 設定をインポートするアプライアンスで、[Configuration] > [ASA FirePOWER Configuration] > [Tools] > [Import Export] の順に選択します。 > > >

[Import Export] ページが表示されます。

ヒント 設定のリストを折りたたむには、設定タイプの横にある折りたたみアイコンをクリックします。設定を確認するには、設定タイプの横にあるフォルダ展開アイコンをクリックします。

ステップ 4 [Upload Package] をクリックします。

[Upload Package] ページが表示されます。

ステップ 5 次の 2 つのオプションから選択できます。

- アップロードするパッケージへのパスを入力します。

- [Upload File] をクリックして、パッケージを見つけます。

ステップ 6 [Upload] をクリックします。

アップロードの結果は、パッケージの内容によって異なります。

- パッケージ内の設定およびルールのバージョンが、アプライアンスにすでに存在するバージョンと正確に一致する場合、そのバージョンが存在することを示すメッセージが表示されます。アプライアンスに最新の設定が存在するので、それらをインポートする必要はありません。
- 使用するアプライアンスとパッケージのエクスポート元のアプライアンスとの間に、ASA FirePOWER モジュールまたは（該当する場合）ルールアップデートのバージョンの不一致がある場合、パッケージをインポートできないことを示すメッセージが表示されます。ASA FirePOWER モジュールまたはルール アップデートのバージョンを更新して、プロセスを再試行します。
- アプライアンスに存在しない設定やルールのバージョンがパッケージに含まれている場合、[Package Import] ページが表示されます。次の手順に進んでください。

ステップ 7 インポートする設定を選択して、[Import] をクリックします。

インポート プロセスが解決されて、以下のような結果になります。

- ASA FirePOWER モジュールに、インポートする設定の以前のリビジョンが存在しない場合、インポートは自動的に完了し、成功メッセージが表示されます。残りの手順は省略してください。
- セキュリティ ゾーンを含むアクセス コントロール ポリシーをインポートする場合、[アクセス コントロール インポートの解決（Access Control Import Resolution）] ページが表示されます。ステップ 8 に進みます。
- インポートする設定に対してアプライアンスに以前のリビジョンが存在する場合、[Import Resolution] ページが表示されます。ステップ 9 に進みます。

ステップ 8 取り込まれる各セキュリティ ゾーンの横で、同じタイプの既存のローカル セキュリティ ゾーンをマップ先として選択し、[Import] をクリックします。

ステップ 7 に戻ります。

ステップ 9 各設定を展開して、以下の該当するオプションを選択します。

- アプライアンスの設定を保持するには、[Keep existing] を選択します。
- アプライアンスの設定をインポートした設定に置き換えるには、[Replace existing] を選択します。
- 最新の設定を保持するには、[Keep newest] を選択します。
- インポートした設定を新しい設定として保存するには、[Import as new] を選択し、オプションとして設定名を編集します。

クリーン リストまたはカスタム検出リストが有効になっているファイル ポリシーを含むアクセス コントロール ポリシーをインポートする場合、[Import as new] オプションは使用できません。

- 従属オブジェクトを含むアクセス コントロール ポリシーや保存済み検索をインポートする場合、提案された名前を受け入れるか、またはオブジェクトの名前を変更します。システムは常にこれらの従属オブジェクトを新規としてインポートします。既存のオブジェクトを保存したり置き換えたりするオプションはありません。システムではオブジェクトもオブジェクト グループも同様に処理されることに注意してください。

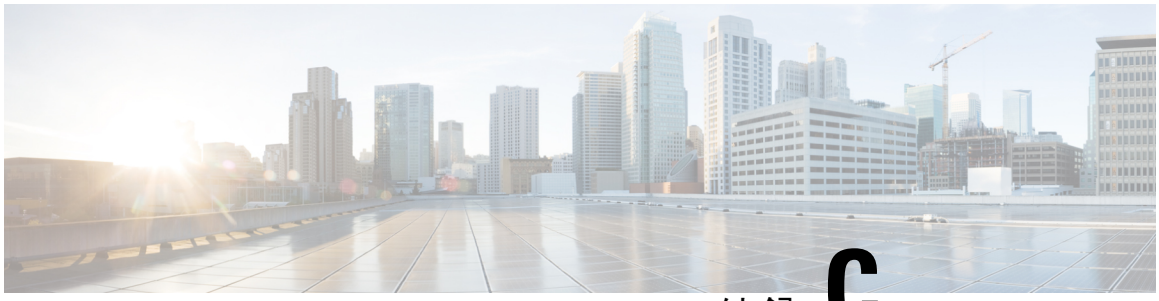
ステップ 10 [Import] をクリックします。

設定がインポートされます。

次のタスク

セキュリティ インテリジェンス フィードを含むアクセス コントロール ポリシーのインポート後、そのポリシーを展開する前にセキュリティ インテリジェンス フィードを更新して最新のデータがダウンロードされるのを待つ必要があります。フィードの内容はエクスポートやインポートのプロセスの一部ではありません。そのため、こうすることで最新のフィードが常に使用されるようにします。

設定のインポートおよびエクスポート



付録 C

実行時間が長いタスクのステータスの表示

ASA FirePOWER モジュールで実行できるタスクの中には、ポリシー適用やアップデート インストールのように、すぐに完了せず実行に時間がかかるものがあります。

このように実行時間が長いタスクの進捗状況を、タスク キューで確認できます。また、これらのタスクが正常に終了したり、異常終了したりした場合にも、タスク キューで報告されます。

タスク キューの表示

ライセンス：任意

ポリシーの適用やアップデートのインストールなど、実行時間が長いタスクを実行すると、これらのタスクのステータスがタスク キューで報告されます。タスク キューは複雑なタスクに関する情報を示し、そのようなタスクが完了したときに報告します。

[Task Status] ページでタスク キューを表示します。このページは 10 秒ごとに自動的に更新されます。

[Job Summary] セクションには、次の表に記載するように、ページに示されているタスクのステータスが表示されます。

表 *97*：タスク キューのタスク タイプ

タスク タイプ	説明
Running	進行中のタスクの数。
Waiting	進行中のいずれかのタスクが完了するのを待機している、実行前のタスクの数。
Completed	正常に完了したタスクの数。

タスク タイプ	説明
Retrying	自動的に再試行されるタスクの数。なお、すべてのタスクの再試行が許可されるわけではありません。
Stopped	システムの更新のために中断されたタスクの数。停止したタスクは再開できません。タスク キューから手動で削除する必要があります。
Failed	正常に終了しなかったタスクの数。

[Jobs] セクションには、各タスクの情報（簡単な説明、タスクがいつ起動されたか、タスクの現在の状態、ステータスが最後に変更されたタイミングなど）が示されます。同じタイプのタスクは、タスク グループにまとめて表示されます。

[Task Status] ページがすばやくロードされるように、ASA FirePOWER モジュールは 過去 1 ヶ月より前に完了/失敗/停止したすべてのタスクを 1 週間に一度、キューから削除します。さらに、1000 個を超えるタスクが含まれるタスク グループから古いタスクを同じ頻度で削除します。なお、手動でキューからタスクを削除することもできます（タスク キューの管理 （626 ページ）の説明を参照してください）。

タスク キューを表示する方法：

次の 2 つのオプションから選択できます。

- 手動でタスクを起動した場合は、タスク起動時に表示された通知ボックスの [Task Status] リンクをクリックします。

ポップアップ ウィンドウに [Task Status] ページが表示されます。

- タスクをスケジュールした場合、または表示されていないページからタスクが起動された場合は、[Monitoring] > [ASA FirePOWER Monitoring] > [Task Status] の順に選択します。

[Task Status] ページが表示されます。

[Task Status] ページで実行できる操作については、タスク キューの管理 （626 ページ）を参照してください。

タスク キューの管理

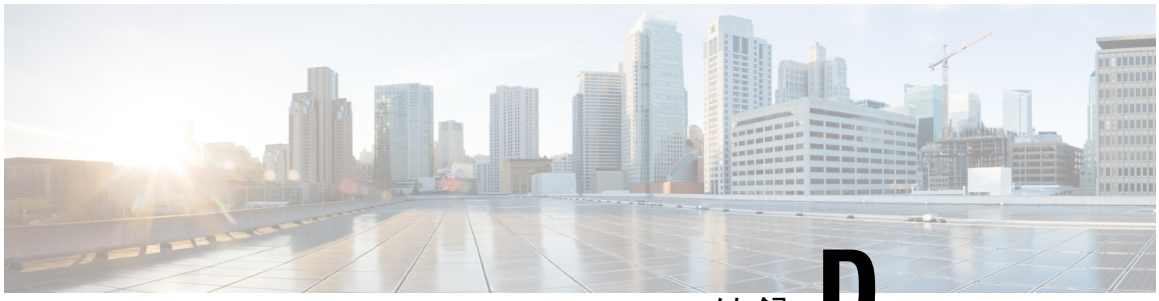
ライセンス：任意

次の表に示すように、タスク キューを表示（タスク キューの表示 （625 ページ）を参照）しているときにいくつかの操作を実行できます。

表 *98 :* タスク キューの操作

目的	操作
完了したすべてのタスクをタスク キューから削除する	[Remove Completed Jobs] をクリックします。
失敗したすべてのタスクをタスク キューから削除する	[Remove Failed Jobs] をクリックします。
タスク キューから 1 つのタスクを削除する	削除するタスクの横にある削除アイコン（）をクリックします。 実行中のタスクは削除できないことに注意してください。実行中のタスクを削除する必要がある場合（例えばタスクが何度も失敗する場合）は、サポート担当にお問い合わせください。
タスク グループを縮小し、タスクを非表示にする	展開されたタスク グループの横にあるオープン フォルダ アイコン（）をクリックします。
タスク グループの中を展開し、タスクを表示する	縮小されたタスク グループの横にあるクローズドフォルダアイコン（）をクリックします。

実行時間が長いタスクのステータスの表示



付録 D

セキュリティ、インターネットアクセス、および通信ポート

ASA FirePOWER モジュールを保護するには、保護された内部ネットワークにインストールする必要があります。ASA FirePOWER モジュールには、使用可能なサービスとポートのうち必要なものだけが設定されていますが、攻撃がファイアウォールの外からモジュールに到達できないことを確認する必要があります。

また、ASA FirePOWER モジュールの機能によってはインターネット接続が必要になります。デフォルトでは、ASA FirePOWER モジュールはインターネットに直接接続するように設定されます。また、システムでは、セキュアなアプライアンスアクセスのため、さらに特定のシステム機能が正しく動作するのに必要なローカルまたはインターネット上のリソースにそれらのシステムがアクセスできるようにするため、特定のポートをオープンしたままにする必要があります。

インターネット アクセス要件

デフォルトでは、ASA FirePOWER モジュールはポート 443/tcp（HTTPS）および 80/tcp（HTTP）でインターネットに直接接続するよう設定されます。これらのポートは、デフォルトで、ASA FirePOWER モジュール上でオープンになっています。通信ポートの要件 （630 ページ）を参照してください。

次の表に、ASA FirePOWER モジュールの特定の機能におけるインターネット アクセス要件を示します。

表 *99 : ASA FirePOWER* モジュール機能のインターネット アクセス要件

機能	インターネット アクセスの用途
侵入ルール、VDB、および GeoDB の更新	侵入ルール、GeoDB、または VDB の更新をアプライアンスに直接ダウンロードするか、ダウンロードをスケジュールします。

機能	インターネット アクセスの用途
ネットワークベースの AMP	マルウェア クラウド検索を実行します。
Security Intelligence フィルタリング	インテリジェンス フィードを含む、外部ソースからのセキュリティ インテリジェンス フィードデータをダウンロードします。
システム ソフトウェアの更新	システム更新をアプライアンスに直接ダウンロードするか、ダウンロードをスケジュールします。
URL フィルタリング	クラウドベースの URL カテゴリおよびレピュテーション データをアクセス制御用にダウンロードし、カテゴライズされていない URL に対してルックアップを実行します。 https://regsvc.sco.cisco.com https://est.sco.cisco.com https://updates-talos.sco.cisco.com http://updates.ironport.com IPV4： • 146.112.62.0/24 • 146.112.63.0/24 • 146.112.255.0/24 • 146.112.59.0/24 IPv6 • 2a04:e4c7:ffff::/48 • 2a04: e4c7: fffe::/48
whois	外部ホストに whois 情報を要求する。

通信ポートの要件

オープン ポートでは、以下が可能です。

- アプライアンスのユーザ インターフェイスにアクセスする
- アプライアンスへのセキュアなリモート接続
- システムの特定の機能が正しく機能するために必要なローカルまたはインターネット上のリソースへのアクセス

一般に、機能関連のポートは、該当する機能を有効化または設定する時点まで、閉じたままになります。

セキュリティ、インターネット アクセス、および通信ポート

注意 開いたポートを閉じると展開にどのような影響が及ぶか理解するまでは、開いたポートを**閉じないでください**。

たとえば、管理デバイス上のポート 25/tcp（SMTP）アウトバウンドを閉じた場合、個別の侵入イベントに関する電子メール通知をデバイスから送信できなくなります（侵入ルールに関する外部アラートの設定 （511 ページ）を参照）。

次の表は、ASA FirePOWER モジュールの機能を最大限に活用するために必要なオープン ポートを示しています。

表 *100 : ASA FirePOWER* モジュールの機能と運用のためのデフォルト通信ポート

ポート	説明	方向	開く目的
22/tcp	SSH/SSL	双方向	アプライアンスへのセキュアなリモート接続を許可します。
25/tcp	SMTP	発信	アプライアンスから電子メール通知とアラートを送信します。
53/tcp	DNS	発信	DNS を使用します。
67/udp 68/udp	DHCP	発信	DHCP を使用します。 （注） これらのポートはデフォルトで**閉じられています**。
		双方向	HTTP経由でのカスタムおよびサードパーティのセキュリティ インテリジェンス フィードの更新。 URL カテゴリおよびレピュテーション データのダウンロード（ポート 443 も必要）。
161/udp	SNMP	双方向	SNMP ポーリング経由でアプライアンスの MIB にアクセスできるようにします。
162/udp	SNMP	発信	リモート トラップ サーバに SNMP アラートを送信します。
389/tcp 636/tcp	LDAP	発信	外部認証用に LDAP サーバと通信します。
389/tcp 636/tcp	LDAP	発信	検出された LDAP ユーザのメタデータの取得。
443/tcp	HTTPS	着信	アプライアンスのユーザ インターフェイスにアクセスする

セキュリティ、インターネット アクセス、および通信ポート

ポート	説明	方向	開く目的
443/tcp	HTTPS クラウド通信	双方向	次のものを取得します。 • ソフトウェア、侵入ルール、VDB、およびGeoDBの更新 • URL カテゴリおよびレピュテーション データ（さらにポート 80 も必要） • インテリジェンス フィードおよび他のセキュアなセキュリティ インテリジェンス フィード • ファイルに関してネットワーク トラフィックで検出されたマルウェアの性質
			デバイスのローカルユーザ インターフェイスを使用してソフトウェア更新をダウンロードします。
514/udp	syslog	発信	リモート syslog サーバにアラートを送信します。
8305/tcp	アプライアンス通信	双方向	展開におけるアプライアンス間で安全に通信します。**必須です。**
8307/tcp	ホスト入力クライアント	双方向	ホスト入力クライアントと通信します。