



侵入ポリシーの準備

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。

シスコは、複数の侵入ポリシーを ASA FirePOWER モジュールとともに提供します。システム付属の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

システム提供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けられていますが、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および侵入ポリシーについて \(18-1 ページ\)](#)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 방법으로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 ポリシーに関する制約事項\(18-12 ページ\)](#)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せ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\(11-1 ページ\)](#)を参照してください。

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。詳細については、以下を参照してください。

- [カスタム侵入ポリシーの作成\(26-2 ページ\)](#)
- [侵入ポリシーの管理\(26-4 ページ\)](#)
- [侵入ポリシーの編集\(26-4 ページ\)](#)
- [侵入ポリシーの適用\(26-8 ページ\)](#)
- [現在の侵入設定のレポートの生成\(26-9 ページ\)](#)
- [2 つの侵入ポリシーまたはリビジョンの比較\(26-10 ページ\)](#)

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。システム提供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\(19-2 ページ\)](#)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[インライン時にドロップ(Drop when Inline)]の設定によって、廃棄ルール(ルール状態が[ドロップしてイベントを生成する(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\(26-6 ページ\)](#)を参照してください。

侵入ポリシーを作成する方法:

- 手順 1 [設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [侵入ポリシー(Intrusion Policy)] の順に選択します。
- [侵入ポリシー(Intrusion Policy)] ページが表示されます。



ヒント

また、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\(B-1 ページ\)](#) を参照してください。

- 手順 2 [ポリシーの作成(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、[侵入ポリシー(Intrusion Policy)] ページに戻るかどうか尋ねられたときに [キャンセル(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\(18-16 ページ\)](#) を参照してください。

[侵入ポリシーの作成(Create Intrusion Policy)] ポップアップ ウィンドウが表示されます。

- 手順 3 [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。

- 手順 4 [基本ポリシー(Base Policy)] で最初の基本ポリシーを指定します。
- システム提供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。

- 手順 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、[インライン時にドロップ(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、[インライン時にドロップ(Drop when Inline)] を無効にします。
- 手順 6 ポリシーを作成します。
- 新しいポリシーを作成して、[侵入ポリシー(Intrusion Policy)] ページに戻るには、[ポリシーの作成(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、[ポリシーの作成と編集(Create and Edit Policy)] をクリックします([侵入ポリシーの編集\(26-4 ページ\)](#) を参照)。

侵入ポリシーの管理




ライセンス:Protection

[侵入ポリシー (Intrusion Policy)] ページ ([設定 (Configuration)] > [ASA FirePOWER 設定 (ASA FirePOWER Configuration)] > [ポリシー (Policies)] > [侵入ポリシー (Intrusion Policy)]) では、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。

- ポリシーの最終変更日時(ローカル タイム)
- [インライン時にドロップ(Drop when Inline)] 設定が有効になっているかどうか。この設定が有効な場合、インライン展開でトラフィックをドロップしたり変更することができます。
- トラフィックのインスペクションに当該の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

[侵入ポリシー (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 26-1 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	[ポリシーの作成(Create Policy)] をクリックします。	カスタム侵入ポリシーの作成(26-2 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(26-4 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(26-8 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(B-1 ページ)
侵入ポリシーの現在の構成設定を示す 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(26-9 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	[ポリシーの比較(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(26-10 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付与されます。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 26-2 侵入ポリシーの編集操作

目的	操作	参照先
インライン展開でドロップ動作を指定する	[ポリシー情報 (Policy Information)] ページの [インライン時にドロップ (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 (26-6 ページ)
基本ポリシーを変更する	[ポリシー情報 (Policy Information)] ページの [基本ポリシー (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 (19-4 ページ)
基本ポリシーの設定を表示する	[ポリシー情報 (Policy Information)] ページで [基本ポリシーの管理 (Manage Base Policy)] をクリックします。	基本レイヤについて (19-2 ページ)
侵入ルールを表示または設定する	[ポリシー情報 (Policy Information)] ページで [ルールの管理 (Manage Rules)] をクリックします。	侵入ポリシー内のルールの表示 (27-3 ページ)
現在のルール状態別に侵入ルールのフィルタビューを表示する、またオプションでそれらのルールを設定する	[ポリシー情報 (Policy Information)] ページの [ルールの管理 (Manage Rules)] で、[イベントを生成する (Generate Events)] または [ドロップしてイベントを生成する (Drop and Generate Events)] が設定されているルールの番号の横にある [表示 (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リング (27-11 ページ)
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 [詳細設定 (Advanced Settings)] をクリックします。	侵入ポリシー内の詳細設定の設定 (26-7 ページ)
ポリシー層を管理する	ナビゲーションパネルで [ポリシー層 (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でのレイヤの使用 (19-1 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 방법으로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 ポリシーに関する制約事項 \(18-12 ページ\)](#)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集中に、メニューまたは別のページへのパスを選択すると、そのページから移動しても、変更内容はシステム キャッシュに残ります。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および侵入ポリシーについて \(18-1 ページ\)](#)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:

-
- 手順 1 [設定 (Configuration)] > [ASA FirePOWER 設定 (ASA FirePOWER Configuration)] > [ポリシー (Policies)] > [侵入ポリシー (Intrusion Policy)] の順に選択します。
[侵入ポリシー (Intrusion Policy)] ページが表示されます。
- 手順 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、[ポリシー情報 (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。
- 手順 3 ポリシーを編集します。上に概要を示したいいずれかのアクションを実行します。
- 手順 4 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、[競合の解決とポリシー変更の確定 \(18-16 ページ\)](#) 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 [ドロップしてイベントを生成する (Drop and Generate Events)] に設定します ([ルール状態の設定 \(27-22 ページ\)](#) 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 ([インライン展開でのコンテンツの置き換え \(30-32 ページ\)](#) を参照)。

侵入ルールがトラフィックに影響を与える場合、ドロップのルールおよびコンテンツ置き換えのルールを正しく設定するとともに、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](#) ([インライン時にドロップ (Drop when Inline)] 設定) を有効にします。



(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 [インライン時にドロップ (Drop when Inline)] を有効にする必要があります。デフォルトの侵入ポリシーを確認または変更するには、[アクセス コントロールのデフォルト侵入ポリシーの設定 \(20-1 ページ\)](#) を参照してください。

設定がインライン展開で実際にトラフィックに影響を与えることなくどのように機能するかを評価する場合は、ドロップ動作を無効にできます。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、ドロップ動作に関係なく、システムがトラフィックに影響を与えることはできないことに注意が必要です。つまり、パッシブ展開では、[ドロップしてイベントを生成する (Drop and Generate Events)] に設定されたルールは [イベントを生成する (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際に、ワークフローにインライン結果を含めることができます。インライン結果は、トラフィックが実際にドロップされたのか、あるいはドロップが想定に過ぎなかったのかを示します。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。

- ドロップ動作が有効な正しく設定されたインライン展開によりドロップされたパケットの場合は `Dropped`
- デバイスがパッシブ展開されている、またはドロップ動作が無効化されているため、パケットがドロップされなかった場合は `Would have dropped`。展開に関係なく、システムがブロ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:

-
- 手順 1** [設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [侵入ポリシー(Intrusion Policy)] の順に選択します。
[侵入ポリシー(Intrusion Policy)] ページが表示されます。
- 手順 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。
[ポリシー情報(Policy Information)] ページが表示されます。
- 手順 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、[インライン時にドロップ(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、[インライン時にドロップ(Drop when Inline)] を無効にします。
- 手順 4** 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、[競合の解決とポリシー変更の確定\(18-16 ページ\)](#) を参照してください。
-

侵入ポリシー内の詳細設定の設定

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 [詳細設定(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。[詳細設定(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 [詳細設定(Advanced Settings)] リンクの下に表示され、この設定ページへの [編集(Edit)] リンクが [詳細設定(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 [デフォルトに戻す(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 [編集 (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 \(18-16 ページ\)](#) 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。このプリプロセッサの設定方法については、[センシティブ データ検出 \(28-21 ページ\)](#) を参照してください。

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。詳細については、[特定の脅威の検出 \(28-1 ページ\)](#) を参照してください。

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、[侵入イベントの記録のグローバルな制限 \(29-1 ページ\)](#) 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。詳細については、以下を参照してください。

- [SNMP 応答の設定 \(39-3 ページ\)](#)
- [Syslog 応答の設定 \(39-6 ページ\)](#)

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 ([設定変更の展開 \(4-13 ページ\)](#) を参照) した後は、その侵入ポリシーは、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、モニタ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、定期的に行う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 \(42-4 ページ\)](#) 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、[ルール更新およびローカルルール ファイルのインポート \(46-10 ページ\)](#) を参照してください。

侵入ポリシーを再適用する方法:

- 手順 1 [設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [侵入ポリシー(Intrusion Policy)] の順に選択します。
[侵入ポリシー(Intrusion Policy)] ページが表示されます。
- 手順 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。
[侵入ポリシーの再適用(Reapply Intrusion Policy)] ウィンドウが表示されます。
- 手順 3 [再適用(Reapply)] をクリックします。
ポリシーが再適用されます。適用のステータスは、タスク キューを使用してモニタできます([モニタリング(Monitoring)] > [ASA FirePOWER モニタリング(ASA FirePOWER Monitoring)] > [タスクのステータス(Task Status)])。詳細については、[タスク キューの表示\(C-1 ページ\)](#)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。

このレポートには、次の情報が含まれており、監査目的や現在の設定の調査目的に使用できます。


表 26-3 侵入ポリシー レポートのセクション

セクション	説明
ポリシー情報	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、および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が示されます。
詳細設定 (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。
ルール(Rule)	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\(26-10 ページ\)](#)を参照してください。

侵入ポリシー レポートを表示する方法:

- 手順 1 [設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [侵入ポリシー(Intrusion Policy)] の順に選択します。
[侵入ポリシー(Intrusion Policy)] ページが表示されます。

手順 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。各ポリシーの名前が比較ビューの左右のタイトルバーに表示されます。
これを使用すると、相違点を強調表示したまま、ユーザ インターフェイス上で両方のポリシーのリビジョンを表示し、そこへ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。
これを使用して、ポリシーの比較を保存、コピー、出力、共有して、さらに検証することができます。

侵入ポリシー比較ツールとその使い方の詳細については、以下を参照してください。

- [侵入ポリシー比較ビューの使用 \(26-10 ページ\)](#)
- [侵入ポリシー比較レポートの使用 \(26-11 ページ\)](#)

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。[侵入ポリシー (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一方のポリシーまたはポリシー リビジョンだけにあるが、他方がないことを意味します。

次の表内の操作を実行できます。

表 26-4 侵入ポリシー比較ビューの操作

目的	操作
変更個別にナビゲートする	タイトルバーの上にある [前へ(Previous)] または [次へ(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、表示している違いを示す [差異(Difference)] 番号が変わります。
新しい侵入ポリシー比較ビューを生成する	[新しい比較(New Comparison)] をクリックします。 [比較の選択(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 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	[比較レポート(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[侵入ポリシー レポートのセクション](#)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方法:

- 手順 1 [設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [侵入ポリシー(Intrusion Policy)] の順に選択します。
[侵入ポリシー(Intrusion Policy)] ページが表示されます。
- 手順 2 [ポリシーの比較(Compare Policies)] をクリックします。
[比較の選択(Select Comparison)] ウィンドウが表示されます。
- 手順 3 [比較対象(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つの侵入ポリシーまたはリビジョンの比較

- 異なる 2 つのポリシーを比較するには、[他のポリシー (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、[その他のリビジョン (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。

手順 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は、[ポリシー A (Policy A)] と [ポリシー B (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、[ポリシー (Policy)] ドロップダウンリストからポリシーを選択してから、[リビジョン A (Revision A)] と [リビジョン B (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。

手順 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。

手順 6 侵入ポリシー比較レポートを生成するには、[比較レポート (Comparison Report)] をクリックします。

手順 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。
