



Snort 3 侵入ポリシーを開始するには

「Snort 3 侵入ポリシーを開始する」の章では、侵入ポリシーの基礎について洞察します。この章では、カスタム Snort 3 の侵入ポリシーの作成、侵入ポリシーの検査モードの変更、侵入防御を実行するためのアクセス制御ルールの設定について説明します。

- [侵入ポリシーの基本 \(1 ページ\)](#)
- [侵入ポリシーの要件と前提条件 \(3 ページ\)](#)
- [カスタム Snort 3 検査ポリシーの作成 \(3 ページ\)](#)
- [Snort 3 侵入ポリシーの編集 \(4 ページ\)](#)
- [侵入ポリシーのベースポリシーの変更 \(5 ページ\)](#)
- [Snort 2 と Snort 3 の両方のバージョンでの侵入ポリシーの検査モードの変更 \(6 ページ\)](#)
- [侵入ポリシーの管理 \(6 ページ\)](#)
- [侵入防御を実行するためのアクセスコントロールルール設定 \(7 ページ\)](#)
- [設定変更の展開 \(9 ページ\)](#)

侵入ポリシーの基本

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。

各侵入ポリシーの中核となるのは、侵入ルールです。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。

システムによって提供されるいくつかの基本侵入ポリシーにより、Cisco Talos Intelligence Group (Talos) の経験を活用できます。これらのポリシーでは、Talos が侵入ルールとインスペクタールールの状態（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。



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。

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。
- ネットワーク上で検出されたオペレーティングシステム、サーバー、およびクライアントアプリケーションプロトコルをそれらの資産を保護するために明確に書き込まれたルールに関連付けるには、Secure Firewall の推奨事項を使用します。

侵入ポリシーは一致する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ドロップルールを設定するには、その状態を [ブロック (Block)] に設定します。

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。必要なインスペクタを無効にすると、システムは自動的に現在の設定でインスペクタを使用します。ただし、ネットワーク分析ポリシーの Web インターフェイスではインスペクタは無効のままになります。



注意 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。

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。

デフォルトでは、暗号化ペイロードの侵入インスペクションは無効化されます。これにより、侵入インスペクションが設定されているアクセスコントロールルールと暗号化された接続を照合する際の誤検出が減少し、パフォーマンスが向上します。

追加のサポートと情報については、「[Snort 3 侵入ポリシーの概要](#)」ビデオを参照してください。

侵入ポリシーの要件と前提条件

モデルのサポート

Threat Defense

サポートされるドメイン

任意

ユーザの役割

- 管理者
- 侵入管理者

カスタム Snort 3 検査ポリシーの作成

ステップ 1 [ポリシー (Policies)] > [侵入 (Intrusion)] を選択します。

ステップ 2 [ポリシーの作成 (Create Policy)] をクリックします。

ステップ 3 [名前 (Name)] に一意の名前を入力し、オプションで [説明 (Description)] を入力します。

ステップ 4 [検査モード (Inspection Mode)] を選択します。

選択したアクションによって、侵入ルールでブロックしてアラートを発生させるか (**防御モード**)、またはアラートを発生させるのみにするか (**検出モード**) が決まります。

(注) 防御モードを選択する前に、多くの誤検出の原因となるルールを特定できるように、ブロックルールのみアラートを発生させることができます。

ステップ 5 [ベースポリシー (Base Policy)] を選択します。

システムによって提供されるポリシーまたは別のカスタムポリシーをベースポリシーとして使用できます。

ステップ 6 [保存 (Save)] をクリックします。

新しいポリシーにはベースポリシーと同じ設定項目が含まれています。

次のタスク

ポリシーをカスタマイズするには、[Snort 3 侵入ポリシーの編集 \(4 ページ\)](#) を参照してください。

Snort 3 侵入ポリシーの編集

Snort 3 ポリシーを編集している間、すべての変更は即座に保存されます。変更を保存するための追加のアクションは必要ありません。

ステップ 1 [ポリシー (Policies)] > [侵入 (Intrusion)] を選択します。

ステップ 2 [侵入ポリシー (Intrusion Policies)] タブが選択されていることを確認します。

ステップ 3 設定する侵入ポリシーの横にある [Snort 3バージョン (Snort 3 Version)] をクリックします。

ステップ 4 ポリシーを編集します。

ベースポリシーを変更するには、[侵入ポリシーのベースポリシーの変更 \(5 ページ\)](#) を参照してください。

次のタスク

設定変更を展開します。[設定変更の展開 \(9 ページ\)](#) を参照してください。

ルールアクションのロギング

Management Center 7.2.0 以降、[侵入イベント (Intrusion Events)] ページの [インライン結果 (Inline Result)] 列のイベントには、ルールに適用された IPS アクションと同じ名前が表示されるため、ルールに一致するトラフィックに適用されたアクションを確認できます。

IPS アクションについて、次の表に、[侵入イベント (Intrusion Events)] ページの [インライン結果 (Inline Result)] 列と、[統合されたイベント (Unified Events)] ページの [侵入イベントタイプ (Intrusion Event Type)] の [アクション (Action)] 列に表示されるイベントを示します。

IPS アクション (Snort 2)	インライン結果 - Management Center 7.1.0 以前	インライン結果 - Management Center 7.2.0 以降
アラート	成功 (Pass)	アラート

IPS アクション (Snort 3)	インライン結果 - Management Center 7.1.0 以前	インライン結果 - Management Center 7.2.0 以降
アラート	成功 (Pass)	アラート
ブロック	Dropped/Would Have Dropped/Partially Dropped	Block/Would Block/Partial Block
削除 (Drop)	Dropped/Would have dropped	Drop/Would drop
拒否 (Reject)	Dropped/Would have dropped	Reject/Would reject

IPS アクション (Snort 3)	インライン結果 - Management Center 7.1.0 以前	インライン結果 - Management Center 7.2.0 以降
書き換え	[許可 (Allow)]	書き換え



- 重要**
- [置換 (Replace)] オプションのないルールの場合、書き換えアクションは「**Would Rewrite**」と表示されます。
 - また、[置換 (Replace)] オプションが指定されているが、IPS ポリシーが検出モードであるか、デバイスがインライン TAP/パッシブモードである場合に、書き換えアクションは「**Would Rewrite**」と表示されます。




- (注) 後方互換性の場合 (Management Center 7.2.0 が Threat Defense 7.1.0 デバイスを管理している)、言及されているイベントは、[成功 (Pass)] がイベントの [アラート (Alert)] として表示されるアラート IPS アクションにのみ適用されます。他のすべてのアクションについては、Management Center 7.1.0 のイベントが適用されます。

侵入ポリシーのベースポリシーの変更

別の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。

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。

- ステップ 1** [ポリシー (Policies)] > [侵入 (Intrusion)] を選択します。
- ステップ 2** 設定する侵入ポリシーの横にある [編集 (Edit)] () をクリックします。
- ステップ 3** [ベースポリシー (Base Policy)] ドロップダウンリストからポリシーを選択します。
- ステップ 4** [保存 (Save)] をクリックします。

次のタスク

設定変更を展開します。[設定変更の展開 \(9 ページ\)](#) を参照してください。

Snort 2 と Snort 3 の両方のバージョンでの侵入ポリシーの検査モードの変更

既存の侵入ポリシーに対して異なる検査モードを選択できます。展開が正常に完了すると、変更がデバイスに適用されます。侵入ポリシーの Snort 2 と Snort 3 の両方のバージョンの検査モードを変更するには、このトピックの手順を実行します。

ステップ 1 [ポリシー (Policies)] > [侵入 (Intrusion)] を選択します。

ステップ 2 変更する侵入ポリシーの横にある [編集 (Edit)] (✎) をクリックします。

ステップ 3 ポリシーに適用する [検査モード (Inspection Mode)] を選択します。

ステップ 4 [保存 (Save)] をクリックします。

次のタスク

設定変更を展開します。[設定変更の展開 \(9 ページ\)](#) を参照してください。

侵入ポリシーの管理

[侵入ポリシー (Intrusion Policy)] ページ ([ポリシー (Policies)] > [侵入 (Intrusion)]) では、現在のカスタム侵入ポリシーとともに次の情報を表示できます。

- 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 ポリシーとデバイスの数
- マルチドメイン展開では、ポリシーが作成されたドメイン

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。

ステップ 1 [ポリシー (Policies)] > [侵入 (Intrusion)] を選択します。

ステップ 2 侵入ポリシーを管理します。

- 作成 : [ポリシーの作成 (Create Policy)] をクリックします。[カスタム Snort 3 検査ポリシーの作成 \(3 ページ\)](#) を参照してください。
- 削除 : 削除するポリシーの横にある をクリックします。別のユーザが保存していないポリシーの変更がある場合は、システムによって確認と通知のプロンプトが表示されます。[OK] をクリックして確認します。

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

- 侵入ポリシーの詳細の編集：編集するポリシーの横にある [\[名前 \(Name\)\]](#)、[\[検査モード \(Inspection Mode\)\]](#)、および [\[ベースポリシー \(Base Policy\)\]](#) を編集できます。
- 侵入ポリシー設定の編集：[\[Snort 3 バージョン \(Snort 3 Version\)\]](#) をクリックします。[Snort 3 侵入ポリシーの編集 \(4 ページ\)](#) を参照してください。
- エクスポート：侵入ポリシーをエクスポートして別の **Management Center** にインポートする場合は、[\[エクスポート \(Export\)\]](#) をクリックします。最新バージョンの『*Firepower Management Center Configuration Guide*』の「*Exporting Configurations*」のトピックを参照してください。
- 展開：[\[展開 \(Deploy\)\]](#) > [\[展開 \(Deployment\)\]](#) を選択します。[設定変更の展開 \(9 ページ\)](#) を参照してください。
- レポート：[\[レポート \(Report\)\]](#) をクリックします。最新バージョンの『*Firepower Management Center Configuration Guide*』の「*Generate Current Policy Reports*」のトピックを参照してください。ポリシーバージョンごとに1つずつ、2つのレポートを生成します。

侵入防御を実行するためのアクセスコントロールルール設定

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。

システムは侵入ポリシーを使用してトラフィックを評価するたびに、関連する変数セットを使用します。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、デフォルトセットにあるデフォルトの変数を変更します。
-

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

システムには複数の侵入ポリシーが付属しています。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、Cisco Talos インテリジェンスグループ (Talos) の経験を活用できます。これらのポリシーでは、Talos は侵入ルールと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を提供できます。

接続イベントおよび侵入イベントのロギング

アクセス制御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すると、侵入イベントを生成し、そのイベントを Management Center に保存します。また、システムはアクセス制御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も Management Center データベース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設定と侵入ポリシー

1つのアクセスコントロールポリシーで使用可能な一意の侵入ポリシーの数は、ターゲットデバイスのモデルによって異なります。より強力なデバイスは、より多数のポリシーを処理できます。侵入ポリシーと変数セットの固有のペアはすべて、1つのポリシーと見なされます。異なる侵入ポリシーと変数セットのペアをそれぞれの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検査を実行するのに必要なリソースが不足している場合は、アクセスコントロールポリシーを展開できません。

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

このタスクを実行するには、管理者、アクセス管理者、またはネットワーク管理者である必要があります。

- ステップ 1 アクセスコントロールポリシーエディタで、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。最新バージョンの『*Firepower Management Center Configuration Guide*』の「*Access Control Rule Components*」のトピックを参照してください。
- ステップ 2 ルールアクションが [許可 (Allow)]、[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)] に設定されていることを確認します。
- ステップ 3 [検査 (Inspection)] をクリックします。
- ステップ 4 システムによって提供される侵入ポリシーまたはカスタムの侵入ポリシーを選択するか、あるい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検査を無効にするには [なし (None)] を選択します。
- ステップ 5 侵入ポリシーに関連付けられた変数セットを変更するには、[変数セット (Variable Set)] ドロップダウンリストから値を選択します。
- ステップ 6 [保存 (Save)] をクリックしてルールを保存します。

ステップ7 [保存 (Save)] をクリックしてポリシーを保存します。

次のタスク

設定変更を展開します。[設定変更の展開 \(9 ページ\)](#) を参照してください。

設定変更の展開

設定を変更した後に、影響を受けるデバイスに展開します。



- (注) このトピックでは、設定変更を展開する基本的な手順について説明します。手順を進める前に、最新バージョンの『*Firepower Management Center Configuration Guide*』の「*Deploy Configuration Changes*」のトピックを参照して変更を展開する上での前提条件と影響を理解しておくことを強くお勧めします。



- 注意** 展開する際にリソースを要求すると、いくつかのパケットがインスペクションなしでドロップされることがあります。また、一部のコンフィギュレーションを展開すると、トラフィックのインスペクションを中断する Snort プロセスが再開します。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。

ステップ1 Secure Firewall Management Center メニューバーで、[展開 (Deploy)] をクリックし、[展開 (Deployment)] を選択します。

[GUI] ページには、期限切れの設定を持ち、ステータスが保留中のデバイスのリストが表示されます。

- [変更者 (Modified by)] 列には、ポリシーまたはオブジェクトを変更したユーザの一覧が表示されます。デバイスリストを展開すると、ポリシーリストごとのポリシーを変更したユーザが表示されます。

(注) 削除されたポリシーおよびオブジェクトのユーザ名は表示されません。

- [インスペクションの中断 (Inspect Interruption)] 列には、展開時にデバイスでトラフィックインスペクションの中断が発生する可能性があるかどうかが表示されます。

デバイスのこの列のエントリが空白の場合は、展開時にそのデバイス上でのトラフィックインスペクションが中断されないことを示します。

- [最終変更時刻 (Last Modified Time)] 列は、最後に設定変更を行った時刻を指定します。
- [プレビュー (Preview)] 列では、次の展開の変更をプレビューできます。
- [ステータス (Status)] 列には、各展開のステータスが表示されます。

ステップ 2 設定変更を展開するデバイスを特定して選択します。

- [検索 (Search)] : [検索 (Search)] ボックスのデバイス名、タイプ、ドメイン、グループ、またはステータスを検索します。
- [展開 (Expand)] : 展開するデバイス固有の設定変更を表示するには、**展開矢印** ([展開矢印 (expand arrow)] アイコン [展開矢印 (expand arrow)] アイコン) をクリックします。

デバイスのチェックボックスを選択すると、デバイスの下に表示されているデバイスのすべての変更がプッシュされ、展開されます。ただし、**ポリシーの選択** ([ポリシーの選択 (policy selection)] アイコン [ポリシーの選択 (policy selection)] アイコン) を使用して展開する個々のポリシーや特定の設定を選択し、残りの変更は展開せずに保持することができます。

- (注)
- [インスペクションの中断 (Inspect Interruption)] 列のステータスに [あり (Yes)] と表示されている場合は、展開によって脅威に対する防御 デバイスでインスペクションと、場合によってはトラフィックが中断され、展開されたリストには中断の原因となった特定の設定が **インスペクションの中断** ([インスペクションの中断 (inspect interruption)] アイコン [インスペクションの中断 (inspect interruption)] アイコン) で示されます。
 - インターフェイスグループ、セキュリティゾーン、またはオブジェクトに変更がある場合、影響を受けるデバイスは、**Management Center** で失効として表示されます。これらの変更が有効になるようにするには、これらのインターフェイスグループ、セキュリティゾーン、またはオブジェクトを含むポリシーも、これらの変更とともに展開する必要があります。影響を受けるポリシーは、**Management Center** の [Preview] ページに [out-of-date] として表示されます。

ステップ 3 [展開 (Deploy)] をクリックします。

ステップ 4 展開する変更に関するエラーや警告がシステムによって識別された場合は、[検証メッセージ (Validation Messages)] ウィンドウにその内容が表示されます。完全な詳細を表示するには、警告またはエラーの前にある矢印アイコンをクリックします。

次の選択肢があります。

- [展開 (Deploy)] : 警告状態を解決せずに展開を続行します。システムがエラーを確認した場合は続行できません。
- [閉じる (Close)] : 展開せずに終了します。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。

次のタスク

展開中に何らかの理由で展開が失敗した場合、その障害がトラフィックに影響を与える可能性があります。ただし、特定の条件によって異なります。展開に特定の設定変更がある場合、展開の失敗によってトラフィックが中断されることがあります。詳細については、最新バージョンの『*Firepower Management Center Configuration Guide*』の「*Deploy Configuration Changes*」のトピックを参照してください。

翻訳について

このドキュメントは、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。