ルールを使用した侵入ポリシーの調整

この章では Short 3 のカスタムルール、侵入ルールアクション、侵入ポリシー内の侵入イベント通知のフィルタ、Snort 2 カスタムルールの Snort 3 への変換、およびカスタムルールのあるルールグループの侵入ポリシーへの追加について説明します。

侵入ルールの調整の概要

共有オブジェクトルール、標準テキストルール、およびインスペクタルールにはルールの状態などを設定できます。

ルールを有効にするには、ルールの状態を [アラート（Alert）] または [ブロック（Block）] に設定します。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。また、[ブロック（Block）]に設定したルールが一致するトラフィック上でイベントを生成したり、ドロップするように侵入ポリシーを設定することもできます。

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インスペクタ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 Web インターフェイスではインスペクタが無効のままになりますが、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。

侵入ルールのタイプ

侵入ルールとは、ネットワーク内の脆弱性を不正利用する試みを検出するためにシステムが使用する、指定されたキーワードと引数のセットのことです。システムはネットワークトラフィックを分析する際に、パケットを各ルールに指定された条件に照らし合わせ、データパケットがルールに指定されたすべての条件を満たす場合、そのルールをトリガーします。

侵入ポリシーには以下の構成要素があります。

- 侵入ルール。共有オブジェクト ルールと標準テキスト ルールに分割されます。
- インスペクタルール。パケットデコーダの検出オプション、またはシステムに付属のインスペクタの 1 つに関連付けられます

次の表に、以上のルール タイプの属性を要約します。

表 *1*: 侵入ルールのタイプ

タイプ	ジェネレータ ID（GID）	Snort ID（SID）	ソース	コピーの可否	編集の可否
共有オブジェクトルール	3	1000000 未満	Cisco Talos Intelligence Group（Talos）	はい	制限付き
標準テキストルール	1（グローバル ドメインまたはレガシー GID）	1000000 未満	Talos	はい	制限付き
	1000～2000（子孫ドメイン）	1000000 以上	ユーザが作成またはインポート	はい	はい
プリプロセッサルール	デコーダまたはプリプロセッサに固有	1000000 未満	Talos	いいえ	いいえ
		1000000 以上	オプション設定時にシステムにより生成	いいえ	いいえ

Talos によって作成されたルールへの変更は保存できませんが、変更したルールのコピーをカスタムルールとして保存することはできます。ルールで使用される変数またはルールヘッダー情報（送信元と宛先のポートやIPアドレスなど）を変更できます。マルチドメイン展開では、

Talosによって作成されるルールはグローバルドメインに属します。子孫ドメインの管理者は、ルールのローカル コピーを保存してから、ルールを編集できます。

Talos によって作成されるルールには、各デフォルト侵入ポリシー内でデフォルトのルール状態が割り当てられます。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行わせる場合は、これらのルールを有効にする必要があります。

ネットワーク分析と侵入ポリシーの前提条件

Snort検査エンジンが侵入およびマルウェア分析のトラフィックを処理できるようにするには、Threat Defense デバイスに対して IPS ライセンスを有効にする必要があります。

ネットワーク分析、侵入ポリシーを管理し、移行タスクを実行するには、管理者ユーザーである必要があります。

Snort 3 のカスタムルール

カスタム侵入ポリシーは、ローカルルールファイルをインポートすることによって作成できます。ルールファイルの拡張子は、`.txt` または `.rules` です。作成方法に関わらず、システムはカスタム ルールをローカル ルールに分類して保存します。カスタムルールはルールグループに属している必要があります。ただし、カスタムルールは複数のグループの一部になることもできます。

カスタム侵入ルールを作成すると、システムは一意のルール番号（番号の形式は`GID:SID:Rev`）を割り当てます。この番号には次の要素が含まれます。

- **GID**：ジェネレータ ID。カスタムルールの場合、GIDを指定する必要はありません。システムは、ルールのアップロード中にグローバルドメインまたはサブドメインのどちらにいるかに基づいて GID を自動的に生成します。標準テキスト ルールでは、グローバルドメインの値は 2000 です。
- **SID**：Snort ID。ルールがシステム ルールのローカル ルールであるかどうかを示します。新しいルールを作成する場合は、一意の SID をルールに割り当てます。

  ローカル ルールの SID 番号は 1000000 から始まり、新しいローカル ルールにつき番号が 1 ずつ増えます。
- **Rev**：リビジョン番号。新しいルールのリビジョン番号は 1 です。カスタムルールを変更するたびに、リビジョン番号は 1 ずつ増える必要があります。

カスタム標準テキスト ルールでは、ルール ヘッダー設定、ルール キーワード、およびルール引数を設定できます。特定のプロトコルを使用する、特定の IP アドレスまたはポートを行き来するトラフィックだけをルールで照合するよう、ルール ヘッダーを設定できます。

（注） Snort 3 カスタムルールは編集できません。カスタムルールに、ルールテキスト内の `classtype` の有効な分類メッセージがあることを確認します。分類または誤分類なしでルールをインポートする場合は、ルールを削除してから再作成します。

Snort 3 の機密データの検出

社会保障番号、クレジットカード番号、E メールなどの機密データは、インターネットに意図的に、または誤って漏洩される可能性があります。機密データの検出は、機密データの漏洩の可能性を検出してイベントを生成するために使用されます。イベントは、大量の個人識別情報（PII）データが転送された場合にのみ生成されます。機密データの検出ではイベントの出力で PII をマスクできます。

sd_pattern オプション

PII を検出してフィルタリングするには、`sd_pattern` IPS オプションを使用します。この情報には、クレジットカード番号、米国社会保障番号、電話番号、電子メールアドレスが含まれます。独自の PII を定義するために、正規表現（regex）構文を使用できます。

sd_pattern オプションには、次の設定があります。

- [パターン（Pattern）]：PDU で検索する正規表現を指定する暗黙の必須設定。正規表現は、PCRE 構文で記述する必要があります。
- [しきい値（Threshold）]：イベントの生成に必要な PDU 内の一致数を指定する明示的なオプション設定。

  IPS ルールオプションとしての `sd_pattern` は、追加のインスペクタの要件なしで Snort で使用できます。ルールオプションの構文は次のとおりです。

  ```
  sd_pattern: "<pattern>"[, threshold <count>];
  ```

  次に例を示します。

  ```
  sd_pattern:"credit_card";
  ```

組み込みパターン

機密データには 5 つの組み込みパターンがあります。「パターン」設定で組み込みパターンを使用するには、照合する必要がある PII タイプの名前を指定する必要があり、必要な正規表現で置き換えられます。PII 名と正規表現のマッピングまたはパターンは次のとおりです。

- credit_card：

  ```
  \d{4}\D?\d{4}\D?\d{2}\D?\d{2}\D?\d{3,4}
  ```

- us_ Social：

  ```
  [0-8]\d{2}-\d{2}-\d{4}
  ```

- us_social_nodashes：

  ```
  [0-8]\d{8}
  ```

- Email：

```
[a-zA-Z0-9!#$%&'*+\/=?^_`{|}~-]+(?:\.[a-zA-Z0-9!#$%&'*+\/=?^_`{|}~-]+)*@(?:[a-zA-Z0-9](?:[a-zA-Z0-9-]*[a-zA-Z0-9])?\.)+[a-zA-Z0-9](?:[a-zA-Z0-9-]*[a-zA-Z0-9])?
```

- us_phone：

```
(?:\+?1[-\.\s]?)?\(?([2-9][0-8]\d)\)?[-\.\s]([2-9]\d{2})[-\.\s](\d{4})
```

PII 名	パターン
credit_card	`\d{4}\D?\d{4}\D?\d{2}\D?\d{2}\D?\d{3,4}`
us_social	`[0-8]\d{2}-\d{2}-\d{4}`
us_social_nodashes	`[0-8]\d{8}`
email	`[a-zA-Z0-9!#$%&'*+\/=?^_`{\|}~-]+(?:\.[a-zA-Z0-9!#$%&'*+\/=?^_`{|}~-]+)*@(?:[a-zA-Z0-9](?:[a-zA-Z0-9-]*[a-zA-Z0-9])?\.)+[a-zA-Z0-9](?:[a-zA-Z0-9-]*[a-zA-Z0-9])?`
us_phone	`(?:\+?1[-\.\s]?)?\(?([2-9][0-8]\d)\)?[-\.\s]([2-9]\d{2})[-\.\s](\d{4})`

これらのパターンに一致するデータのマスキングは、クレジットカードと米国社会保障番号、電子メール、および米国の電話番号のシステム提供ルールまたは組み込みパターンでのみ機能します。マスキングは、カスタムルールまたはユーザー定義のPIIパターンでは機能しません。ルールは、機密データ用の Lightweight Security Package（LSP）gid:13 で使用できます。デフォルトでは、どのポリシーにも含まれていません。

LSP の機密データルールは、すべての組み込みパターンを対象とし、次のしきい値があります。

- credit_card：2
- us_ social：2
- us_ social_nodashes：20
- email：20
- us_phone：20

sd_pattern オプションを使用すると、カスタムルールを作成したり、既存のルールを変更できます。これを行う場合は、Snort 3 侵入ポリシーインターフェイスを使用します。

カスタムパターンとしきい値を使用した sd_pattern を含むルールの例：

alert tcp (sid: 1000000001; sd_pattern:"[\w-\.]+@([\w-]+\.)+[\w-]{2,4}",threshold 4; msg: "email, threshold 4")

例

機密データ検出を使用したカスタムルールの例：

組み込みパターンを使用したルール：

```
alert tcp (
        msg:"SENSITIVE-DATA Email";
        flow:only_stream;
```

```
        pkt_data;
        sd_pattern:"email", threshold 5;
        service:http, smtp, ftp-data, imap, pop3;
        sid:1000001;
)
```

カスタムパターンを使用したルール：

```
alert tcp (
        msg:"SENSITIVE-DATA US phone numbers";
        flow:only_stream;
        file_data;
       sd_pattern:"+?3?8?(0[\s\.-]\d{2}[\s\.-]\d{3}[\s\.-]\d{2}[\s\.-]\d{2})", threshold
 2;
        service:http, smtp, ftp-data, imap, pop3;
        sid:1000002;
)
```

次に、組み込み機密データパターンを使用した完全な Snort IPS ルールの例をいくつか示します。

- alert tcp (sid:1; msg:"Credit Card"; sd_pattern:"credit_card";)
- alert tcp (sid:2; msg:"US Social Number"; sd_pattern:"us_social";)
- alert tcp (sid:3; msg:"US Social Number No Dashes"; sd_pattern:"us_social_nodashes";)
- alert tcp (sid:4; msg:"US Phone Number"; sd_pattern:"us_phone";)
- alert tcp (sid:5; msg:"Email"; sd_pattern:"email";)

データマスキングの無効化は、Cisco Secure Firewall Management Center および Cisco Secure Firewall Device Manager ではサポートされていません。

侵入ポリシーの Snort 3 侵入ルールの表示

侵入ポリシー内のルールの表示方法を調整できます。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。

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 3 ルールを表示している間、以下を実行できます。

- ルールをフィルタ処理します。
- ルールグループを選択すると、そのグループに関連するルールが表示されます。
- 侵入ルールの詳細を表示します。
- ルールのコメントを表示します。
- ルールのドキュメンテーションを表示します。

これらのタスクの実行の詳細については、「Snort 3 侵入ポリシーの編集」を参照してください。

侵入ルールアクション

侵入ルールアクションでは、個々の侵入ポリシー内のルールを有効または無効にできるだけでなく、モニター対象の条件がルールをトリガーした場合にシステムが実行するアクションを指定できます。

Cisco Talos Intelligence Group（Talos）が各デフォルトポリシーの侵入およびインスペクタルールごとにデフォルトアクションを設定します。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。Talos 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アクションを変更する場合もあります。ルール更新でのベース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）のデフォルトアクション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アクションの変更も許可することになります。ただし、ルールアクションを変更している場合は、ルール更新でその変更がオーバーライドされないことに注意してください。

侵入ルールを作成すると、そのルールは、ポリシーの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アクションを継承します。

侵入ルールアクションのオプション

侵入ポリシーでは、ルールのアクションを次の値に設定できます。

アラート（Alert）

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。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。悪意のあるパケットはその対象に到達しますが、イベントロギングによって通知されます。

ブロック（Block）

システムで特定の侵入試行を検出して、その攻撃を含むパケットをドロップし、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。悪意のあるパケットはその対象に到達せず、イベントロギングによって通知されます。

無効（Disable）

システムで一致するトラフィックを評価しない場合。

（注） [アラート（Alert）] または [ブロック（Block）] オプションを選択すると、ルールが有効になります。[無効（Disable）] を選択すると、ルールが無効になります。

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**推奨します。すべてのルールが有効になっている場合は、管理対象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。

侵入ルールアクションの設定

侵入ルールアクションはポリシーに固有です。

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

ステップ 2 編集する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。

ヒント　このページには、次の合計数が表示されます。

- 無効なルール
- [アラート（Alert）] に設定された有効なルール
- [ブロック（Block）] に設定された有効なルール
- オーバーライドされたルール

ステップ 3 ルールアクションを設定する 1 つ以上のルールを選択します。

ステップ 4 [ルールアクション（Rule Action）] ドロップダウンリストからルールアクションのいずれかを選択します。さまざまなルールアクションの詳細については、「Snort 3 侵入ポリシーの編集」を参照してください。

ステップ 5 [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。設定変更の展開を参照してください。

侵入ポリシーの侵入イベント通知フィルタ

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。

侵入イベントしきい値

指定した期間内にイベントを生成する回数に基づいて、システムが侵入イベントをログに記録して表示する回数を制限するには、個別のルールのしきい値を設定します。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。共有オブジェクトルール、標準テキストルール、またはインスペクタルールごとにしきい値を設定できます。

侵入イベントしきい値の設定

しきい値を設定するには、最初にしきい値のタイプを指定します。

表 *2:* しきい値設定オプション

オプション	説明
制限（Limit）	指定された数のパケット（count 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 [制限（Limit）] に、[カウント（Count）] を 10 に、[秒（Seconds）] を 60 に設定し、14 個のパケットがルールをトリガーとして使用した場合、システムはその 1 分の間に発生した最初の 10 個を表示した後、イベントの記録を停止します。
しきい値（Threshold）	指定された数のパケット（count 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 [しきい値（Threshold）] に、[カウント（Count）] を 10 に、[秒（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、[秒（Seconds）] と [カウント（Count）] のカウンタを 0 にリセットします。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。
両方（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 [両方（Both）] に、[カウント（Count）] を 2 に、[秒（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 回目にトリガーとして使用されたときにしきい値が満たされる）。 • 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します。これにより、イベントしきい値が送信元 IP アドレス単位と宛先 IP アドレス単位のどちらで計算されるかが決まります。

表 *3: IP* しきい値設定オプション

オプション	説明
ソース（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。

オプション	説明
接続先（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 *4*: 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
カウント（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。
秒（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 [制限（limit）] に、トラッキングを [送信元IP（Source IP）] に、[カウント（count）] を [10] に、[秒（seconds）] を [10] に設定した場合は、システムが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 のイベントを記録して表示します。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。

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ます。

ヒント 侵入イベントのパケット ビューでしきい値を追加することもできます。

Snort 3 での侵入ルールのしきい値の設定

[ルールの詳細（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。

ステップ 1 **[オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）]** をクリックします。

ステップ 2 [Snort 3 のすべてのルール（Snort 3 All Rules）] タブをクリックします。

ステップ 3 侵入ルールの [アラート設定（Alert Configuration）] 列で、[なし（None）] リンクをクリックします。

ステップ 4 **[編集（Edit）]**（）をクリックします。

ステップ 5 [アラート設定（Alert Configuration）] ウィンドウで、[しきい値（Threshold）] タブをクリックします。

ステップ 6 [タイプ（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、[制限（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、[しきい値（Threshold）] を選択します。
- 指定されたイベント インスタンス数に達した後で、期間あたり 1 回ずつ通知を提供する場合は、[両方（Both）] を選択します。

ステップ 7 [追跡対象（Track By）] フィールドで [送信元（Source）] または [宛先（Destination）] を選択し、イベントインスタンスの追跡を送信元 IP アドレスで行うか、宛先の IP アドレスで行うかを指定します。

ステップ 8 [カウント（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 9 [秒数（Seconds）] フィールドに、イベントインスタンスを追跡する期間（秒数）を指定する数値を入力します。

ステップ 10 [保存（Save）] をクリックします。

追加のサポートと情報については、「Snort 3 の抑制としきい値」ビデオ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

ルールのしきい値の既存の設定を表示または削除するには、[ルールの詳細（Rules Details）] ビューを使用して、しきい値の構成済み設定を表示し、それらがシステムに適切かどうかを確認します。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。

ステップ 1 **[オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）]** をクリックします。

ステップ 2 [Snort 3 のすべてのルール（Snort 3 All Rules）] タブをクリックします。

ステップ 3 [アラート設定（Alert Configuration）] 列に表示されるしきい値が設定されているルールを選択します（[アラート設定（Alert Configuration）] 列には、ルールのリンクとして [しきい値（Threshold）] が表示されます）。

ステップ 4 ルールのしきい値を削除するには、[アラート設定（Alert Configuration）] 列の [しきい値（Threshold）] リンクをクリックします。

ステップ 5 をクリックします。

ステップ 6 [しきい値（Threshold）] タブをクリックします。

ステップ 7 [リセット（Reset）] をクリックします。

ステップ 8 [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。設定変更の展開を参照してください。

侵入ポリシー抑制の設定

特定の IP アドレスまたは IP アドレスの範囲でインスペクタの特定のルール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、特定のエクスプロイトのように見えるパケットを伝送しているメールサーバが存在する場合は、そのメールサーバによってトリガーとして使用されたイベントに関するイベント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。

侵入ポリシー抑制タイプ

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構成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。

ヒント　侵入イベントのパケット ビュー内から抑制を追加できます。侵入ルールエディタページ（**[オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）] > [Snort 3 のすべてのルール（Snort 3 All Rules）]**）の [アラート設定（Alert Configuration）] 列を使用して、抑制設定にアクセスすることもできます

Snort 3 での侵入ポリシーの抑制の設定

侵入ポリシーのルールに対して 1 つ以上の抑制を設定できます。

始める前に

送信元または宛先の抑制に追加する必要があるネットワークオブジェクトを作成していることを確認します。

ステップ 1　**[オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）]** をクリックします。

ステップ 2　[Snort 3 のすべてのルール（Snort 3 All Rules）] タブをクリックします。

ステップ 3　侵入ルールの [アラート設定（Alert Configuration）] 列の [なし（None）] リンクをクリックします。

ステップ 4　**[編集（Edit）]**（  ）をクリックします。

ステップ 5　[抑制（Suppressions）] タブで、次のオプションの横にある追加アイコン（+）をクリックします。

- 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、[送信元ネットワーク（Source Networks）] 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、[宛先ネットワーク（Destination Networks）] を選択します。

ステップ 6　[ネットワーク（Network）] ドロップダウンリストからプリセットネットワークを選択します。

ステップ 7　[保存（Save）] をクリックします。

ステップ 8 （任意）必要に応じて、最後の 3 つの手順を繰り返します。

ステップ 9 [アラート設定（Alert Configuration）] ウィンドウで [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。設定変更の展開を参照してください。

抑制条件の表示と削除

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、メールサーバがエクスプロイト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。

ステップ 1 **[オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）]** をクリックします。

ステップ 2 [Snort 3 のすべてのルール（Snort 3 All Rules）] タブをクリックします。

ステップ 3 抑制を表示または削除するルールを選択します。

ステップ 4 [アラート設定（Alert Configuration）] 列の [抑制（Suppression）] をクリックします。

ステップ 5 をクリックします。

ステップ 6 [抑制（Suppressions）] タブをクリックします。

ステップ 7 抑制の横にある [クリア（Clear）]（×）をクリックして、抑制を削除します。

ステップ 8 [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。設定変更の展開を参照してください。

侵入ルールのコメントの追加

侵入ポリシーのルールにコメントを追加できます。このようにして追加されたコメントはポリシー専用のコメントとなります。よって、ある侵入ポリシーのルールに追加したコメントは、他の侵入ポリシーでは表示されません。

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

ステップ 2 編集する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 3 すべてのルールがリストされているページの右側で、コメントを追加するルールを選択します。

ステップ 4 [コメント（Comments）]列の下にある**コメント**（[コメント（comment）]アイコン[コメント（comment）]アイコン） をクリックします。

ステップ 5 [コメント（Comments）] フィールドに、ルールコメントを入力します。

ステップ 6 [コメントを追加（Add a Comment）] をクリックします。

ステップ 7 [保存（Save）] をクリックします。

ヒント [コメント（Comments）] 列のルールの横に [コメント（Comment）] （）が表示されます。

次のタスク

設定変更を展開します。設定変更の展開を参照してください。

Snort 2 カスタムルールの Snort 3 への変換

カスタムルールを使用している場合は、Snort 2 から Snort 3 に変換する前に、Snort 3 のルールセットを管理する準備ができていることを確認してください。サードパーティベンダーのルールセットを使用している場合は、そのベンダーに連絡して、そのルールが Snort 3 に正常に変換されることを確認するか、または Snort 3 用にネイティブに作成された置換ルールセットを取得します。独自に作成したカスタムルールがある場合は、変換前に Snort 3 ルールの作成に慣れておくと、変換後の Snort 3 検出を最適化するようにルールを更新できます。Snort 3 でのルールの作成の詳細については、次のリンクを参照してください。

- https://blog.snort.org/2020/08/how-rules-are-improving-in-snort-3.html
- https://blog.snort.org/2020/10/talos-transition-to-snort-3.html

Snort 3 ルールの詳細については、https://blog.snort.org/ にある他のブログを参照してください。

システム付属のツールを使用して Snort 2 ルールを Snort 3 ルールに変換するには、Snort 2 カスタムルールの Snort 3 への変換 （14 ページ）を参照してください。

重要 Snort 2 ネットワーク分析ポリシー（NAP）の設定を Snort 3 に自動的にコピーすることはできません。NAP 設定は、Snort 3 で手動で複製する必要があります。

すべての侵入ポリシーのすべての Snort 2 カスタムルールの Snort 3 への変換

ステップ 1 **[オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）]** をクリックします。

ステップ 2 [Snort 3 のすべてのルール（Snort 3 All Rules）] タブをクリックします。

ステップ 3 左側のペインで [すべてのルール（All Rules）] が選択されていることを確認します。

ステップ 4 [タスク（Tasks）] ドロップダウンリストから値を選択します。

- **[Snort 2ルールの変換とインポート（Convert Snort 2 rules and import）]**：すべての侵入ポリシーのすべての Snort 2 カスタムルールを Snort 3 に自動的に変換し、それらを Snort 3 カスタムルールとして Management Center にインポートします。
- **[Snort 2ルールの変換とダウンロード（Convert Snort 2 rules and download）]**：すべての侵入ポリシーのすべての Snort 2 カスタムルールを Snort 3 に自動的に変換し、それらをローカルシステムにダウンロードします。

ステップ 5 [OK] をクリックします。

（注）
- 前の手順で [変換してインポート（Convert and import）] を選択した場合は、変換されたすべてのルールが、[ローカルルール（Local Rules）] の下に新しく作成されたルールグループ [すべての Snort 2 をグローバルに変換（All Snort 2 Converted Global）] の下に保存されます。
- 前の手順で [変換してダウンロード（Convert and download）] を選択した場合は、ルールファイルをローカルに保存します。ダウンロードしたファイル内の変換済みのルールを確認します。後でルールグループへのカスタムルールの追加 （16 ページ）の手順に従ってアップロードできます。

追加のサポートと情報については、「Snort 2 ルールの Snort 3 への変換」ビデオを参照してください。

次のタスク

設定変更を展開します。設定変更の展開を参照してください。

単一の侵入ポリシーの Snort 2 カスタムルールの Snort 3 への変換

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）] タブで、[Snort 3同期ステータスの表示（Show Snort 3 Sync status）] をクリックします。

ステップ 3 侵入ポリシーの [同期（Sync）] アイコン（ ）をクリックします。

（注） 侵入ポリシーの Snort 2 バージョンと Snort 3 バージョンが同期されている場合は、[同期（Sync）] アイコンが緑色の で表示されます。変換するカスタムルールがないことを示します。

ステップ 4 サマリーを読み、[カスタムルール（Custom Rules）] タブをクリックします。

ステップ 5 次のどちらかを選択します。

- [変換後のルールをこのポリシーにインポートする（Import converted rules to this policy）]：侵入ポリシーの Snort 2 カスタムルールを Snort 3 に変換し、Snort 3 カスタムルールとして Management Center にインポートします。
- [変換後のルールのダウンロード（Download converted rules）]：侵入ポリシーのSnort 2カスタムルールをSnort 3に変換し、ローカルシステムにダウンロードします。ダウンロードしたファイル内の変換後のルールを確認し、後でアップロードアイコンをクリックしてファイルをアップロードできます。

ステップ 6 [再同期（Re-Sync）] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開を参照してください。

ルールグループへのカスタムルールの追加

Management Center でカスタムルールをアップロードすると、ローカルで作成したカスタムルールがすべての Snort 3 ルールのリストに追加されます。

ステップ 1 **[オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）]** をクリックします。

ステップ 2 [Snort 3 のすべてのルール（Snort 3 All Rules）] タブをクリックします。

ステップ 3 [タスク（Tasks）] ドロップダウンリストをクリックします。

ステップ 4 [Snort 3ルールのアップロード（Upload Snort 3 Rules）] をクリックします。

ステップ 5 作成した Snort 3 カスタムルールを含む `.txt` または `.rules` ファイルをドラッグアンドドロップします。

ステップ 6 [OK] をクリックします。

（注） 選択したファイルにエラーがある場合、それ以上先に進むことはできません。エラーファイルをダウンロードし、エラーを修正した後に [ファイルの置換（Replace File）] リンクをクリックし、ファイルのバージョン 2 をアップロードできます。

ステップ 7 ルールをルールグループに関連付けて、そのグループに新しいルールを追加します。

新しいカスタムルールグループを作成し（[新しいカスタムルールグループの作成（Create New Custom Rule Group）] リンクをクリック）、新しいグループにルールを追加することもできます。

（注） 既存のローカルルールグループがない場合は、[新しいカスタムルールグループの作成（Create New Custom Rule Group）] をクリックして続行します。新しいルールグループの [名前（Name）] を入力して、[保存（Save）] をクリックします。

ステップ 8 次のいずれかを選択します。

- [ルールのマージ（Merge Rules）] は、追加する新しいルールをルールグループ内の既存のルールとマージします。

- [グループ内のすべてのルールをファイルの内容に置換（Replace all rules in the group with file contents）] は、既存のすべてのルールを追加する新しいルールに置換します。

（注） 前の手順で複数のルールグループを選択した場合は、使用できるオプションは[ルールのマージ（Merge Rules）] のみになります。

ステップ 9 [次へ（Next）] をクリックします。

サマリーを確認して、追加する新しいルール ID を確認し、必要に応じてダウンロードします。

ステップ 10 [終了（Finish）] をクリックします。

重要 アップロードされたすべてのルールのルールアクションは無効な状態になっています。ルールをアクティブにするために必要な状態に変更する必要があります。

次のタスク

- Management Center でカスタムルールをアップロードすると、作成したカスタムルールがすべての Snort 3 ルールのリストに追加されます。これらのカスタムルールをトラフィックに適用するには、必要な侵入ポリシーでこれらのルールを追加して有効にします。カスタムルールを含むルールグループを侵入ポリシーに追加する方法については、カスタムルールを含むルールグループの侵入ポリシーへの追加 （17ページ）を参照してください。カスタムルールを有効にする方法については、Snort 3 でのカスタムルールの管理 （18ページ）を参照してください。
- 設定変更を展開します。設定変更の展開を参照してください。

カスタムルールを含むルールグループの侵入ポリシーへの追加

システムにアップロードされたカスタムルールを侵入ポリシーで有効にし、それらのルールをトラフィックに適用する必要があります。Management Center にカスタムルールをアップロードした後、侵入ポリシーに新しいカスタムルールを含むルールグループを追加します。

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

ステップ 2 [侵入ポリシー（Intrusion Policies）] タブで、侵入ポリシーの [Snort 3 バージョン（Snort 3 Version）] をクリックします。

ステップ 3 [ルールグループ（Rule Groups）] 検索バーの横にある [追加（Add）] （+）をクリックします。

ステップ 4 [ルールグループの追加（Add Rule Groups）] ウィンドウで、ルールグループの横にある [>] アイコンをクリックして、ローカルルールグループを展開します。

ステップ 5 アップロードしたカスタムルールグループの横にあるチェックボックスをオンにします。

ステップ 6 [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。設定変更の展開を参照してください。

Snort 3 でのカスタムルールの管理

システムにアップロードしたカスタムルールを侵入ポリシーに追加し、それらのルールを有効にしてトラフィックに適用する必要があります。アップロードされたカスタムルールは、すべてのポリシーで有効にすることも、個々のポリシーで選択して有効にすることもできます。

次の手順に従って、1 つ以上の侵入ポリシーでカスタムルールを有効にします。

ステップ 1 **[オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）]** をクリックします。

ステップ 2 [Snort 3 のすべてのルール（Snort 3 All Rules）] タブをクリックします。

ステップ 3 [ローカルルール（Local Rules）] を展開します。

ステップ 4 必要なルールグループを選択します。

ステップ 5 ルールの横にあるチェックボックスをオンにしてルールを選択します。

ステップ 6 [ルールアクション（Rule Actions）] ドロップダウンリストから [侵入ポリシーごと（Per Intrusion Policy）] を選択します。

ステップ 7 次のどちらかを選択します。

- [すべてのポリシー（All Policies）]：追加するすべてのルールに対して同じルールアクションを設定します。
- [侵入ポリシーごと（Per Intrusion Policy）]：侵入ポリシーごとに異なるルールアクションを設定します。

ステップ 8 ルールアクションを次のように設定します。

- 前の手順で [すべてのポリシー（All Policies）] を選択した場合は、[オーバーライド状態の選択（Select Override state）] ドロップダウンリストから必要なルールアクションを選択します。
- 前の手順で [侵入ポリシーごと（Per Intrusion Policy）] を選択した場合は、ポリシー名に [ルールアクション（Rule Action）] を選択します。さらにポリシーを追加するには、[別のポリシーの追加（Add Another）] をクリックします。

ステップ 9 必要に応じて、[コメント（Comments）] テキストボックスにコメントを追加します。

ステップ 10 [保存（Save）] をクリックします。

次のタスク

デバイスに変更を展開します。設定変更の展開を参照してください。.

カスタムルールの削除

ステップ 1 **[オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）]** をクリックします。

ステップ 2 [Snort 3 のすべてのルール（Snort 3 All Rules）] タブをクリックします。

ステップ 3 左側のペインの [ローカルルール（Local Rules）] を展開します。

ステップ 4 削除するルールのチェックボックスをオンにします。

ステップ 5 選択したすべてのルールのルールアクションが [無効（Disable）] であることを確認します。

必要に応じて次の手順に従い、選択した複数のルールのルールアクションを無効にします。

a) [ルールアクション（Rule Actions）] ドロップダウンボックスから、[侵入ポリシーごと（Per Intrusion Policy）] を選択します。
b) [すべてのポリシー（All Policies）] オプションボタンを選択します。
c) [オーバーライド状態の選択（Select Override state）] ドロップダウンリストから [無効（Disable）] を選択します。
d) [保存（Save）] をクリックします。
e) 削除するルールのチェックボックスをオンにします。

ステップ 6 [ルールアクション（Rule Actions）] ドロップダウンリストから、[削除（Delete）] を選択します。

ステップ 7 [ルールの削除（Delete Rules）] ポップアップウィンドウで [削除（Delete）] をクリックします。

次のタスク

設定変更を展開します。設定変更の展開を参照してください。

ルールグループの削除

始める前に

含めたすべての侵入ポリシーから削除するルールグループを除外します。侵入ポリシーからルールグループを除外する手順については、Snort 3 侵入ポリシーの編集を参照してください。

ステップ 1 **[オブジェクト（Objects）] > [侵入ルール（Intrusion Rules）]** をクリックします。

ステップ 2 [Snort 3 のすべてのルール（Snort 3 All Rules）] タブをクリックします。

ステップ 3 左側のペインの [ローカルルール（Local Rules）] を展開します。

ステップ 4 削除するルールグループを選択します。

ステップ 5 続行する前に、グループ内のすべてのルールのルールアクションが [無効（Disable）] に設定されていることを確認します。

いずれかのルールのルールアクションが [無効（Disable）] 以外の場合、ルールグループは削除できません。必要に応じて、次の手順に従ってすべてのルールのルールアクションを無効にします。

a) [ルールアクション（Rule Actions）] ドロップダウンリストの下にあるチェックボックスをオンにして、グループ内のすべてのルールを選択します。
b) [ルールアクション（Rule Actions）] ドロップダウンボックスから、[侵入ポリシーごと（Per Intrusion Policy）] を選択します。
c) [すべてのポリシー（All Policies）] オプションボタンを選択します。
d) [オーバーライド状態の選択（Select Override state）] ドロップダウンリストから [無効（Disable）] を選択します。
e) [保存（Save）] をクリックします。

ステップ 6 ルールグループの横にある **[削除（Delete）]**（）をクリックします。

ステップ 7 [ルールグループの削除（Delete Rule Group）] ポップアップウィンドウで [OK] 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。