Snort 2 から Snort 3 への移行

次のシナリオで 脅威に対する防御 デバイスを移行できます。

- Snort 2 脅威に対する防御 デバイスバージョン 6.7 以前を使用しており、Snort 3 脅威に対する防御 バージョン 7.0 以降に移行する。
- Snort 2 脅威に対する防御 デバイスバージョン 7.0 以降を使用しており、デバイスを Snort 3 にアップグレードする。

Snort 3 検査エンジン

Snort 3 は、バージョン 7.0 以降の新規登録 脅威に対する防御 デバイスのデフォルト検査エンジンです。ただし、下位バージョンの 脅威に対する防御 デバイスでは、Snort 2 がデフォルトの検査エンジンです。管理対象の 脅威に対する防御 デバイスをバージョン 7.0 以降にアップグレードしても、検査エンジンは Snort 2 のままです。バージョン 7.0 以降のアップグレードされた 脅威に対する防御 で Snort 3 を使用するには、明示的に有効にする必要があります。Snort 3 をデバイスの検査エンジンとして有効にすると、（アクセス コントロール ポリシーを介して）デバイスに適用される侵入ポリシーの Snort 3 バージョンがアクティブ化され、デバイスを通過するすべてのトラフィックに適用されます。

必要に応じて Snort のバージョンを切り替えることができます。Snort 2 と Snort 3 の侵入ルールがマッピングされ、マッピングはシステムによって実行されます。ただし、Snort 2 と Snort 3 のすべての侵入ルールの 1 対 1 のマッピングが見つからない場合があります。Snort 2 で 1 つのルールのルールアクションを変更した場合、Snort 2 と Snort 3 を同期せずに Snort 3 に切り替えると、その変更は保持されません。同期の詳細については、Snort 2 のルールと Snort 3 の同期 （6 ページ）を参照してください。

Snort 2 から Snort 3 への移行方法

Snort 2 から Snort 3 に移行するには、脅威に対する防御 デバイスの検査エンジンを Snort 2 から Snort 3 に切り替える必要があります。

要件に応じて、Snort 2 から Snort 3 へのデバイスの移行を完了するためのタスクを次の表に示します。

ステップ	タスク	手順へのリンク
1	Snort 3 の有効化	• 個々のデバイス上での Snort 3 の有効化 （3 ページ） • 複数のデバイスでの Snort 3 の有効化 （3 ページ）
2	Snort 2 のカスタムルールの Snort 3 への変換	• 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 （4 ページ） • 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 （5 ページ）
3	Snort 2 のルールと Snort 3 の同期	Snort 2 のルールと Snort 3 の同期 （6 ページ）

Snort 2 から Snort 3 への移行の前提条件

移行手順を実行可能なサポートされているユーザーロールは次のとおりです。

- 管理者
- 侵入管理者

以下は、デバイスを Snort 2 から Snort 3 に移行する前に考慮する必要がある推奨される前提条件です。

- Snort の実用的な知識を持っている。Snort 3 アーキテクチャの詳細については、Snort 3 Adoption を参照してください。
- Management Center をバックアップする。「Backup the Management Center」を参照してください。
- 侵入ポリシーをバックアップする。「Exporting Configurations」を参照してください。
- 侵入ポリシーを複製する。複製する場合、既存のポリシーをベースポリシーとして使用して、侵入ポリシーのコピーを作成できます。

個々のデバイス上での Snort 3 の有効化

重要 展開プロセス中に現在の検査エンジンをシャットダウンする必要があるため、一時的なトラフィック損失が発生します。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択します。

ステップ 2 デバイスをクリックして、デバイスのホームページに移動します。

（注） デバイスは Snort 2 または Snort 3 としてマークされ、デバイスの現在のバージョンが表示されます。

ステップ 3 [デバイス（Device）] タブをクリックします。

ステップ 4 [検査エンジン（Inspection Engine）] セクションで、[アップグレード（Upgrade）] をクリックします。

（注） Snort 3 を無効にするには、[検査エンジン（Inspection Engine）] セクションで [Snort 2 に戻す（Revert to Snort 2）] をクリックします。

ステップ 5 [はい（Yes）] 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。.

選択した Snort バージョンとの互換性を得るため、システムは展開プロセス中にポリシー設定を変換します。

複数のデバイスでの Snort 3 の有効化

複数のデバイスで Snort 3 を有効にするには、必要なすべての 脅威に対する防御 デバイスがバージョン 7.0 以降であることを確認します。

重要 展開プロセス中に現在の検査エンジンをシャットダウンする必要があるため、一時的なトラフィック損失が発生します。

ステップ 1 **[デバイス（Devices）] > [デバイス管理（Device Management）]** の順に選択します。

ステップ 2 Snort 3 を有効または無効にするすべてのデバイスを選択します。

（注） デバイスは Snort 2 または Snort 3 としてマークされ、デバイスの現在のバージョンが表示されます。

ステップ 3 [一括アクションの選択（Select Bulk Action）] 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 へのアップグレード（Upgrade to Snort 3）] をクリックします。

（注） Snort 3 を無効にするには、[Snort 2 へのダウングレード（Downgrade to Snort 2）] をクリックします。

ステップ 5 [はい（Yes）] 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。.

選択した Snort バージョンとの互換性を得るため、システムは展開プロセス中にポリシー設定を変換します。

Snort 2 のカスタム IPS ルールの Snort 3 への変換

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。

システム提供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、次の手順を参照してください。

- 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 （4 ページ）
- 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 （5 ページ）

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。

- [変換してインポート（Convert 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、Snort 3 カスタムルールとして Management Center にインポートします。
- [変換してダウンロード（Convert 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。後でカスタム ルールのアップロード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（  ）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。

Snort 2 と Snort 3 のベースポリシーのマッピングの表示

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 [IPS マッピング（IPS Mapping）] をクリックします。

Snort 2 のルールと Snort 3 の同期

Snort 2 のバージョン設定とカスタムルールが保持され、Snort 3 に引き継がれるための同期機能が Management Center によって提供されます。同期することで、過去数か月または数年にわたって変更または追加されている可能性がある、Snort 2 ルールのオーバーライド設定とカスタムルールを Snort 3 バージョンで複製できます。このユーティリティは、Snort 2 バージョンのポリシー設定を Snort 3 バージョンと同期して、同様の対象範囲で開始するのに役立ちます。

Management Center を 6.7 より前のバージョンから 7.0 以降のバージョンにアップグレードすると、設定が同期されます。Management Center が新しい 7.0 移行のバージョンの場合、より高いバージョンにアップグレードできますが、アップグレード中にコンテンツは同期されません。

デバイスを Snort 3 にアップグレードする前に、Snort 2 バージョンで変更が行われた場合は、このユーティリティを使用して Snort 2 バージョンから Snort 3 バージョンに最新の同期を行うことができ、同様の対象範囲で開始できます。

（注） Snort 3 への移行時に、Snort 3 バージョンのポリシーを別個に管理し、通常の運用としてこのユーティリティを使用しないことを推奨します。

重要

- Snort 2 ルールのオーバーライドとカスタムルールのみが Snort 3 にコピーされ、その逆は行われません。Snort 2 と Snort 3 のすべての侵入ルールの 1 対 1 のマッピングが見つからない場合があります。次の手順を実行すると、両方のバージョンに存在するルールのルールアクションに対する変更が同期されます。
- 同期では、カスタムまたはシステムによって提供されるルールのしきい値と抑制の設定は Snort 2 から Snort 3 に移行されません。

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

ステップ 2 [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 [Snort 3 の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 4 同期していない侵入ポリシーを特定します。

ステップ 5 [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（）で表示されます。

ステップ 6 サマリーを読み、必要に応じてサマリーのコピーをダウンロードします。

ステップ 7 [再同期（Re-Sync）] をクリックします。

（注）
- 同期された設定は、Snort 3 侵入エンジンがデバイスに適用され、展開が成功した後にのみ適用されます。
- Snort 2 カスタムルールは、システム付属のツールを使用して Snort 3 に変換できます。Snort 2 カスタムルールがある場合は、[カスタムルール（Custom Rules）] タブをクリックし、画面の指示に従ってルールを変換します。詳細については、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 （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。