Snort 2 から Snort 3 への移行

「Snort 2 から Snort 3 への移行」の章では、Snort 2 から Snort 3 への移行のさまざまな側面について説明します。また、Snort 3 の有効化と無効化、および Snort 2 ルールの Snort 3 との同期についても説明します。

Snort 2 と Snort 3 の比較

Snort 3 はアーキテクチャが再設計され、Snort 2 と比較すると同等のリソースでより多くのトラフィックを検査します。Snort 3 では、トラフィックパーサーを簡単かつ柔軟に挿入できます。Snort 3 には、ルールの記述を容易にし、同等の共有オブジェクトルールを表示できる新しいルールシンタックスも用意されています。

次の表に、検査エンジン機能に関する Snort 2 バージョンと Snort 3 バージョンの違いを示します。

機能	Snort 2	Snort 3
パケットスレッド	プロセスごとに 1 つ	プロセスごとに任意の数
コンフィギュレーション メモリの使用	プロセス数 X *x* GB	合計 *x* GB。より多くのメモリをパケットに使用可能
設定のリロード	低速	より高速。1つのスレッドを個別のコアにピン留め可能
ルールのシンタックス	一貫性がなく、改行が必要	任意の空白を含む均一なシステム

機能	Snort 2	Snort 3
ルールのコメント	コメントのみ	#、#begin、および #end マーク。C 言語スタイル

追加リファレンス：Firepower の Snort 2 と Snort 3 の違い。

FMC 管理対象の FTD での Snort 3 の機能制限

次の表に、Snort 2 でサポートされているが、FMC 管理対象の FTD デバイスの Snort 3 ではサポートされていない機能を示します。

表 *1 : Snort 3* の機能制限

ポリシー/領域	サポートされない機能
アクセス コントロール ポリシー	次のアプリケーション設定。 • Safe Search • YouTube EDU

脅威インテリジェンスディテクタ	IPv4 または IPv6 のトラフィックが次の場合：
	• ブロック済み：
	  • TID インシデントなし
	  • SI イベントなし
	• モニター対象：
	  • ITD インシデントなし

侵入ポリシー	• Firepower 推奨 • ポリシー層 • グローバルルールのしきい値 • ロギングの設定： • SNMP • SRU ルールの更新（Snort 3 は LSP ルールの更新のみをサポートしているため）

Snort 2 から Snort 3 への移行

ポリシー/領域	サポートされない機能
アプリケーションの検出	Snort 3 では、デフォルトですべてのネットワークに対してアプリケーション検出が有効になっています。Snort 2 とは異なり、ネットワーク検出ポリシーのネットワークフィルタを使用して、特定のネットワークのみに対するアプリケーション検出の有効化または無効化を制御することはできません。詳細については、『Firepower Management Center Configuration Guide』の最新バージョンの「Application Detection in Snort 2 and Snort 3」のトピックを参照してください。
ネットワーク検出/RNA	• ホストポート/サービス ID（ネットワークマップに表示） • OS フィンガープリント（侵入ポリシーを自分のネットワークマップに合わせて調整することはできません）
その他の機能	FQDN 名によるイベントのロギング

Snort 2 から Snort 3 への移行

Snort 2 から Snort 3 に移行するには、FTD 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。バージョン 7.0 以降のデバイスのみが Snort 3 をサポートしていることに注意してください。

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。サポートされているデバイスで Snort 3 を有効にするには、Snort 3 の有効化と無効化 （4 ページ）を参照してください。

Snort 2 カスタムルール用の変換ツール

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 のカスタムルールの Snort 3 への変換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。

Snort 3 の有効化と無効化

Snort 3 は、バージョン 7.0 以降の新規登録 FTD 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 FTD 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 FTD デバイスをバージョン 7.0 以降にアップグレードすると、検査エンジンは Snort 2 に残ります。バージョン 7.0 以降のアップグレードされた FTD 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。必要に応じて Snort 3 から Snort 2 にいつでも戻すことができます。

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。

個々のデバイス上での Snort 3 の有効化と無効化

始める前に

手順の実行が可能なサポートされているユーザロールは次のとおりです。

- 管理者
- 侵入管理者

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。

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。

複数のデバイスでの Snort 3 の有効化と無効化

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 FTD 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。

始める前に

手順の実行が可能なサポートされているユーザロールは次のとおりです。

- 管理者
- 侵入管理者

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。

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。

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

これは、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ためのユーティリティです。

- FMC が 7.0 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された場合、システムは設定を同期します。FMC が新しい 7.0 バージョン以降の場合、より高いバージョンにアップグレードでき、システムはアップグレード中にコンテンツを同期しません。

  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。

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 に引き継がれるように、FMC が同期機能を提供します。同期は、Snort 2 ルールのオーバーライド設定とカスタムルールに役立ちます。これらは過去数か月または数年にわたってすでに変更されたり、追加されている可能性があり、それらを Snort 3 バージョンで複製しなければなりません。

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。