# システム ソフトウェアの更新

次のトピックでは、FirePOWER ソフトウェアを更新する方法について説明します。



## FirePOWER の更新について

シスコは、以下を含む各種のアップデートを配信します。

- システム ソフトウェア自体に対するメジャーおよびマイナー アップグレード
- 侵入ルールの更新（SRU）
- 地理位置情報データベース（GeoDB）の更新
- 脆弱性データベース（VDB）の更新

メジャーアップグレードを除いて、更新のダウンロードとインストールをスケジュールすることができます。

**注意** この章では、システムの更新に関する全般的な情報について説明します。VDB、GeoDB、侵入ルールを含め、更新を実行する前に、更新に付随しているリリース ノートまたはアドバイザリ テキストを必ずお読みください。リリース ノートでは、サポートされるプラットフォーム、互換性、前提条件、警告、特定のインストールおよびアンインストールの手順など重要なデータが提供されます。

（注） 更新には、Firepower Management Center から管理対象デバイスへの大量のデータ転送が必要になる場合があります。開始する前に、管理ネットワークに、転送を正常に実行するために十分な帯域幅があることを確認してください。https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212043-Guidelines-for-Downloading-Data-from-the.html で、トラブルシューティングのテクニカル ノートを参照してください。

**表 *1 : Firepower* の更新**

| 更新のタイプ | 説明 | スケジュールを行うか | アンインストールをするか | [ドメイン（Domain）] |
|---|---|---|---|---|
| システム ソフトウェア自体に対するメジャー アップグレード。 | システム ソフトウェアに対するメジャー アップグレードには新機能が含まれており、製品の大規模な変更を伴うことがあります。この場合、バージョン番号の 1、2、または 3 番目の桁が変更されます。<br>メジャー アップグレードでは、シスコ エンド ユーザ ライセンス契約（EULA）の再承認が必要な場合があります。 | — | — | グローバルだけ |
| システム ソフトウェアに対するパッチ | パッチには限られた範囲の修正が含まれています。バージョン番号の 4 番目の桁が更されます。 | ○ | ○ | グローバルだけ |
| 脆弱性データベース（VDB） | VDB の更新は、オペレーティング システム、アプリケーション、クライアントによって検出された脆弱性、およびFirepower システムによって報告された脆弱性に影響を与えます。 | ○ | — | グローバルだけ |
| 侵入ルール | 侵入ルールの更新には、新規および更新された侵入ルールとプリプロセッサ ルール、既存のルールの変更されたステータス、変更されたデフォルト侵入ポリシーの設定が含まれています。ルールの更新では、ルールが削除されたり、新しいルール カテゴリとデフォルトの変数が提供されたり、デフォルトの変数値が変更されたりすることもあります。 | ○ | — | シスコ提供：グローバルのみ<br>ローカル インポート：任意 |

| 更新のタイプ | 説明 | スケジュールを行うか | アンインストールをするか | [ドメイン（Domain）] |
|---|---|---|---|---|
| 位置情報データベース（GeoDB） | GeoDB の更新には、物理的な場所や接続タイプなど、検出されたルート可能な IP アドレスにシステムが関連付けることができるものに関する更新情報が含まれています。位置情報データは、アクセス コントロール ルールとして使用できます。位置情報の詳細を表示するには、GeoDB をインストールする必要があります。 | ○ | — | グローバルだけ |

パッチおよび他のマイナーな更新はアンインストールできますが、VDB、GeoDB、または侵入ルールに対するメジャーな更新をアンインストールしたり、前のバージョンに戻したりすることはできないことに注意してください。自分のアプライアンスを新しいメジャーバージョンに更新した場合、および古いバージョンに戻す必要がある場合は、サポートに連絡してください。

リリース ノートまたはアドバイザリ テキストに特に記載されていない限り、アプライアンスを更新しても設定は変更されず、アプライアンスの設定はそのまま保持されます。

# FirePOWER ソフトウェアのアップグレード

Firepower Management Center 展開のアップグレードは、複雑なプロセスになることがあります。誤りを避けるには、注意深い計画と準備が役立ちます。アップグレード プロセスの一部として、アップグレードスクリプトを呼び出す機械的な手順を実際に実行することと同じくらい、計画と準備を検討する必要があります。

このプロセスの最初の手順は、展開を評価し、アップグレードパス、すなわちアップグレードするアプライアンス、アップグレードするコンポーネント、およびその順序の詳細な計画を作成することです。アップグレード パスは、次の条件を満たす必要があります。

- マネージャとデバイスの互換性を維持します。
- 必要に応じて、オペレーティング システムとホスティング環境のアップグレードを含めます。
- バックアップ、パッケージのダウンロード、準備状況チェック、帯域幅とディスク容量のチェック、アップグレード前後の設定変更などの、その他のタスクを含めます。
- トラフィック フローおよびインスペクションでの潜在的な中断を特定します。

Firepower Management Center 展開のアップグレードを準備して正常に完了する方法の詳細については、『Firepower Management Center アップグレード ガイド』を参照してください。

# Firepower システムのソフトウェア アップデートのアンインストール

パッチまたは機能の更新を適用すると、更新プロセスによってアンインストーラが作成されます。これにより、Webインターフェイスを使用してアプライアンスから更新を削除することができます。

更新をアンインストールした場合、結果として保持されるバージョンは、アプライアンスの更新パスに応じて異なります。たとえば、アプライアンスをバージョン6.0からバージョン6.0.0.2へ直接更新した場合のシナリオについて考えてみます。バージョン6.0.0.2のパッチをアンインストールすると、バージョン 6.0.0.1 の更新をインストールしたことがなくても、バージョン6.0.0.1を実行するアプライアンスが結果として生成されます。更新をアンインストールしたときに結果として生成される Firepower ソフトウェアのバージョンの詳細については、リリースノートを参照してください。

⚠

**注意** メジャーな更新では、Webインターフェイスからのアンインストールはサポートされていません。アプライアンスを Firepower システムの新しいメジャー バージョンに更新して、古いバージョンに戻す必要がある場合は、サポートに連絡してください。

### アンインストールの順序

更新は、インストールと逆の順序でアンインストールします。つまり、最初に管理対象デバイスから更新をアンインストールしてから、Firepower Management Center からアンインストールします。

### ローカル Web インターフェイスを使用した更新のアンインストール

更新をアンインストールするにはローカルWebインターフェイスを使用する必要があります。Firepower Management Center を使用して、管理対象デバイスから更新をアンインストールすることはできません。ローカル Web インターフェイスを持たないデバイス（NGIPSv デバイスなど）からパッチをアンインストールする場合の詳細については、リリース ノートを参照してください。

### ハイ アベイラビリティ ペアからの 7000 および 8000 シリーズ デバイスのアンインストール

ハイ アベイラビリティ ペアの 7000 または 8000 シリーズ デバイスは、同じバージョンの Firepowerシステムを実行する必要があります。アンインストールプロセスは自動フェールオーバーをトリガーしますが、不一致のハイ アベイラビリティ ペアの 7000 または 8000 シリーズ デバイスは、設定情報を共有せず、同期の一部として更新をインストールまたはアンインストールすることもありません。冗長デバイスから更新をアンインストールする必要がある場合は、即時および連続的にアンインストールを実行するように計画します。

アンインストールによって、これらのデバイスが、ハイ アベイラビリティへのスタックの設定がサポートされないバージョンに戻される場合は、ハイ アベイラビリティ ペアとして設定されたスタックの 7000 または 8000 シリーズ デバイスから更新をアンインストールできません。

運用の継続性を保証するために、ハイ アベイラビリティ ペアのデバイスから一度に 1 つずつ更新をアンインストールします。まず、セカンダリ デバイスから更新をアンインストールします。アンインストール プロセスが完了するまで待ってから、すぐにプライマリ デバイスから更新をアンインストールします。

**注意** ハイ アベイラビリティ ペアのデバイスでのアンインストール プロセスが失敗した場合は、アンインストールを再開したり、ピアの設定を変更したり**しないで**ください。代わりに、サポートに連絡してください。

### スタック構成のデバイスからの更新のアンインストール

スタック内のすべてのデバイスが、同じバージョンの Firepower システムを実行する必要があります。スタック構成のデバイスのいずれかから更新をアンインストールすると、そのスタックではデバイスが限定的な、バージョンが混在する状態になります。

展開への影響を最小にするために、スタック構成のデバイスから更新を同時にアンインストールします。スタック内のすべてのデバイスで更新が完了すると、スタックは通常の動作を再開します。

アンインストールによって、これらのデバイスが、ハイ アベイラビリティへのスタックの設定がサポートされないバージョンに戻される場合は、ハイ アベイラビリティ ペアとして設定されたスタックの 7000 または 8000 シリーズ デバイスから更新をアンインストールできません。

### トラフィック フローとインスペクション

管理対象デバイスから更新をアンインストールすると、トラフィックのインスペクション、トラフィック フロー、およびリンク ステートに影響を及ぼすことがあります。特定の更新に対してネットワーク トラフィックがいつ、どのように影響を受けるかについての情報は、リリース ノートを参照してください。

### アンインストール後

更新をアンインストールした後で、展開が正しく機能していることを確認するために、いくつかの手順を実行する必要があります。これらはアンインストールが成功したこと、および展開のすべてのアプライアンスが正常に通信していることを確認することが含まれます。それぞれの更新に特定の情報については、リリース ノートを参照してください。

# Firepower システムのソフトウェア更新のアンインストール

| スマート ライセンス | 従来のライセンス | サポートされるデバイス | サポートされるドメイン | アクセス |
|---|---|---|---|---|
| 任意（Any） | 任意（Any） | 任意（Any） | グローバルだけ | Admin |

この手順は、Firepower Management Center と 7000 & 8000 シリーズ デバイスで実行できます。

### 始める前に

- アプライアンスを Firepower System の新しいメジャー バージョンに更新した後に、古いバージョンに戻す必要が生じた場合は、サポートに連絡してください。メジャー更新では、Web インターフェイスからのアンインストールはサポートされていません。

### 手順

**ステップ 1** **[システム（System）] > [更新（Updates）]**を選択します。

**ステップ 2** 削除する更新のアンインストーラの隣にあるインストールアイコンをクリックします。プロンプトが表示されたら、更新をアンインストールすることを確認して、アプライアンスをリブートします。

- Firepower Management Center で、[アップデートをインストール（Install Update）] ページが表示されます。Firepower Management Center を選択し、[インストール（Install）] をクリックします。
- 管理対象デバイスには、操作のページがありません。

**注意** アンインストールが完了するまで、更新の監視以外のタスクを実行するために Web インターフェイスを使用**しないで**ください。必要に応じて、アプライアンスをリブートします。

**ステップ 3** 必要に応じて、タスクのステータスをモニタします（タスク メッセージの表示を参照）。

**ステップ 4** アンインストールが完了したら、必要に応じてアプライアンスにログインします。

**ステップ 5** ブラウザのキャッシュを消去し、ブラウザを強制的にリロードします。そうしない場合、ユーザ インターフェイスが予期しない動作を示すことがあります。

**ステップ 6** **[ヘルプ（Help）] > [バージョン情報（About）]** を選択し、ソフトウェアのバージョンが正しく示されていることを確認します。

### 次のタスク

- パッチをアンインストールしたアプライアンスが正常に管理対象デバイスと通信していること（Firepower Management Center の場合）、または管理元のFirepower Management Centerと通信していること（管理対象デバイスの場合）を確認します。

- アンインストールが成功したこと、および展開環境のすべてのアプライアンスが正常に通信していることを確認します。それぞれの更新に特定の情報については、リリース ノートを参照してください。

# 脆弱性データベース（VDB）の更新

| スマート ライセンス | 従来のライセンス | サポートされるデバイス | サポートされるドメイン | アクセス |
|---|---|---|---|---|
| 任意（Any） | 任意（Any） | 任意（Any） | グローバルだけ | Admin |

シスコ脆弱性データベース（VDB）は、オペレーティング システム、クライアント、およびアプリケーションのフィンガープリントだけでなく、ホストが影響を受ける可能性がある既知の脆弱性のデータベースです。システムでは、VDB を使用して、特定のホストで感染のリスクが高まるかどうかを判断します。

Cisco Talos Security Intelligence and Research Group（Talos） では、VDB の定期的な更新を配布しています。Firepower Management Center で VDB と関連付けられたマッピングの更新にかかる時間は、ネットワーク マップ内のホストの数によって異なります。一般的に、更新の実行にかかるおおよその時間（分）を判断するには、ホストの数を 1000 で割ります。

⚠

**注意** 脆弱性データベース（VDB）の更新プログラムを直ちにインストールすると、すべての管理対象デバイスで Snort プロセスが再起動します。また、VDB の内容によっては、VDB のインストール後の最初の展開により Snort が再起動する場合があります。どちらのシナリオでも、再起動によってトラフィックのインスペクションが中断されます。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。詳細については、Snort® の再起動によるトラフィックの動作を参照してください。

次の手順を使用して手動でVDBを更新します。VDB更新を自動化するには、タスク スケジュールを使用します（**[システム（System）]** > **[ツール（Tools）]** > **[スケジューリング（Scheduling）]**）。

### 始める前に

- Firepower Management Center でインターネット アクセスができない、または VDB 更新を手動で Firepower Management Center へアップロードする場合は、更新をダウンロードします（https://www.cisco.com/go/firepower-software）。
- Snort の再起動が発生するため、トラフィック フローとインスペクションに更新による影響があることを考慮します。メンテナンス ウィンドウ期間に更新を実行することをお勧めします。

### 手順

**ステップ 1** **[システム（System）] > [更新（Updates）]** を選択し、[製品の更新（Product Updates）] タブをクリックします。

**ステップ 2** VDB 更新の Firepower Management Center へのアップロード方法を選択します。

- Cisco.com から直接ダウンロード：[アップデートのダウンロード（Download Updates）] をクリックします。シスコ サポートおよびダウンロード サイトにアクセスできる場合、Firepower Management Center は最新の VDB をダウンロードします。Firepower Management Centerは、アプライアンスが現在実行しているバージョンに関連付けられている各パッチとホットフィックスのパッケージもダウンロードする点に注意してください（ただし、メジャー リリースは含まれない）。
- 手動でアップロード：[更新のアップロード（Upload Update）] をクリックして、[ファイルの選択（Choose File）] をクリックします。ダウンロードした更新を参照して、[アップロード（Upload）] をクリックします。

VDB 更新は、Firepower ソフトウェアのアップグレードおよびアンインストーラ パッケージと同じページに表示されます。

**ステップ 3** 更新をインストールします。

a) [脆弱性およびフィンガープリント データベースの更新（Vulnerability and Fingerprint Database update）] の横にある [Install（インストール）] アイコンをクリックします。
b) Firepower Management Center を選択します。
c) [Install（インストール）] をクリックします。

**ステップ 4** （オプション）メッセージ センターで更新の進行状況をモニタします。

更新が完了するまで、マッピングされた脆弱性に関連するタスクを実行しないでください。メッセージセンターに進行状況が数分間表示されない、または更新が失敗したことが示されている場合でも、更新を再開しないでください。代わりに、Cisco TAC にお問い合わせください。

更新の完了およびSnortの再起動後に、システムで新しい脆弱性情報が使用されます。ただし、更新されたアプリケーション ディテクタとオペレーティング システム フィンガープリントを有効にするために、展開する必要があります。

**ステップ 5** （オプション）メッセージ センターで更新の進行状況をモニタします。

更新が完了するまで、マッピングされた脆弱性に関連するタスクを実行しないでください。メッセージセンターに進行状況が数分間表示されない、または更新が失敗したことが示されている場合でも、更新を再開しないでください。代わりに、Cisco TAC にお問い合わせください。

更新の完了およびSnortの再起動後に、システムで新しい脆弱性情報が使用されます。ただし、更新されたアプリケーション ディテクタとオペレーティング システム フィンガープリントを有効にするために、展開する必要があります。

**ステップ 6** 更新が成功したことを確認します。

現在の VDB バージョンを表示するには、**[ヘルプ（Help）]** > **[バージョン情報（About）]** を選択します。

### 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。

# 地理位置情報データベース（GeoDB）の更新

シスコ地理位置情報データベース（GeoDB）は、ルーティング可能な IP アドレスと関連付けられた地理的データ（国、都市、座標など）および接続関連のデータ（インターネット サービス プロバイダー、ドメイン名、接続タイプなど）のデータベースです。検出された IP アドレスと一致する GeoDB 情報が検出された場合は、その IP アドレスに関連付けられている位置情報を表示できます。国や大陸以外の位置情報の詳細を表示するには、システムに GeoDB をインストールする必要があります。シスコでは、GeoDB の定期的な更新を提供しています。

GeoDB を更新するには、Firepower Management Center で [位置情報の更新（Geolocation Updates）] ページ（**[システム（System）]** > **[更新（Updates）]** > **[位置情報の更新（Geolocation Updates）]**）を使用します。サポートまたは自身のアプライアンスから取得した GeoDB の更新をアップロードすると、それらがこのページに表示されます。

（注） [位置情報の更新（Geolocation Updates）] ページで [位置情報の更新をサポート サイトからダウンロードおよびインストールする（Download and install geolocation update from the Support Site）] をクリックするか、または手動でサポート サイトから更新を直接ダウンロードします。電子メールで更新ファイルを転送すると、破損する可能性があります。

GeoDB の更新にかかる時間はアプライアンスによって異なります。インストールには通常、30 ～ 40 分かかります。GeoDB の更新によって他のシステム機能（進行中の位置情報収集など）が中断されることはありませんが、更新が完了するまでシステム リソースが消費されます。更新を計画する場合には、この点について考慮してください。

GeoDB を更新すると、GeoDB の以前のバージョンが上書きされ、すぐに有効になります。GeoDB を更新すると、Firepower Management Center により、管理対象デバイス上の関連データが自動的に更新されます。GeoDB の更新が展開全体で有効になるまでに数分かかることがあります。更新後に再度展開する必要はありません。

## 手動による GeoDB の更新（インターネット接続）

| スマート ライセンス | 従来のライセンス | サポートされるデバイス | サポートされるドメイン | アクセス（Access） |
|---|---|---|---|---|
| 任意（Any） | 任意（Any） | 任意（Any） | グローバルだけ | Admin |

新しい GeoDB 更新プログラムは、アプライアンスがインターネットにアクセスできる場合にのみ、サポート サイトに接続することで自動的にインポートできます。

**手順**

**ステップ 1** **[システム（System）] > [更新（Updates）]**を選択します。

**ステップ 2** [位置情報の更新（Geolocation Updates）] タブをクリックします。

**ステップ 3** [サポート サイトから地理位置情報の更新をダウンロードしてインストールする（Download and install geolocation update from the Support Site）] を選択します。

**ステップ 4** [インポート（Import）] をクリックします。
システムは [地理位置情報の更新（Geolocation Update）] タスクをキューに入れます。このタスクは、最新の更新について、シスコ サポート サイト（http://www.cisco.com/cisco/web/support/index.html）で確認します。

**ステップ 5** 必要に応じて、タスクのステータスをモニタします。タスク メッセージの表示を参照してください。

**ステップ 6** 更新が終了したら、[地理位置情報の更新（Geolocation Updates）] ページに戻るか、**[ヘルプ（Help）] > [バージョン情報（About）]** を選択して、GeoDB のビルド番号がインストールした更新と一致していることを確認します。

# 地理位置情報データベース（GeoDB）の手動更新：インターネット接続なし

| スマート ライセンス | 従来のライセンス | サポートされるデバイス | サポートされるドメイン | アクセス |
|---|---|---|---|---|
| 任意（Any） | 任意（Any） | 任意（Any） | グローバルだけ | Admin |

Firepower Management Center がインターネットにアクセスできない場合は、シスコ サポート サイトからネットワーク上のローカル マシンに GeoDB の更新をダウンロードして、その更新を手動で Firepower Management Center にアップロードできます。

**手順**

**ステップ 1** シスコ サポート サイト（http://www.cisco.com/cisco/web/support/index.html）から、手動で更新をダウンロードします。

**ステップ 2** **[システム（System）] > [更新（Updates）]**を選択します。

**ステップ 3** [位置情報の更新（Geolocation Updates）] タブをクリックします。

**ステップ 4** [地理位置情報の更新のアップロードとインストール（Upload and install geolocation update）] を選択します。

**ステップ 5** ダウンロードした更新を参照して、[アップロード（Upload）] をクリックします。

**ステップ 6** [インポート（Import）] をクリックします。

**ステップ 7** 必要に応じて、タスクのステータスをモニタします。タスク メッセージの表示を参照してください。

**ステップ 8** 更新が終了したら、[地理位置情報の更新（Geolocation Updates）] ページに戻るか、**[ヘルプ（Help）] > [バージョン情報（About）]** を選択して、GeoDB のビルド番号がインストールした更新と一致していることを確認します。

# GeoDB 更新のスケジューリング

| スマート ライセンス | 従来のライセンス | サポートされるデバイス | サポートされるドメイン | アクセス |
|---|---|---|---|---|
| 任意（Any） | 任意（Any） | 任意（Any） | グローバルだけ | Admin |

Firepower Management Center でインターネット アクセスができる場合、週ごとの GeoDB 更新をお勧めします。

### 始める前に

Firepower Management Center でインターネットにアクセスできることを確認します。

### 手順

**ステップ 1** **[システム（System）] > [更新（Updates）]** を選択し、[ジオロケーションの更新（Geolocation Updates）] タブをクリックします。

**ステップ 2** [位置情報の定期更新（Recurring Geolocation Updates）] で、[週ごとの定期更新を有効にする（Enable Recurring Weekly Updates）] をオンにします。

**ステップ 3** [開始時刻の更新（Update Start Time）] を指定します。

**ステップ 4** [保存（Save）] をクリックします。

# 侵入ルールの更新

新しい脆弱性が明らかになるのに伴い、Cisco Talos Security Intelligence and Research Group（Talos）は侵入ルールの更新をリリースします。これらの更新を Firepower Management Center にインポートして、変更後の設定を管理対象デバイスに導入することで、侵入ルールの更新を実装できます。それらの更新は、侵入ルール、プリプロセッサ ルール、およびルールを使用するポリシーに影響を及ぼします。

侵入ルール更新は更新を累積されていくものなので、常に最新の更新をインポートすることをお勧めします。現在インストールされているルールのバージョン以前の侵入ルールの更新をインポートすることはできません。

侵入ルールの更新では、次のものを提供します。

- **新規または変更されたルールおよびルール状態**：ルール更新は、新規および更新された侵入ルールとプリプロセッサ ルールを提供します。新規ルールの場合は、システム付属の各侵入ポリシーでルール ステータスが異なることがあります。たとえば、新規ルールが、Security over Connectivity 侵入ポリシーでは有効になっており、Connectivity over Security 侵入ポリシーでは無効になっていることがあります。ルールの更新では、既存のルールのデフォルトの状態が変更されたり、既存のルールが完全に削除されたりすることもあります。
- **新しいルール カテゴリ**：ルール更新には、常に追加される新しいルール カテゴリが含まれている場合があります。
- **変更されたプリプロセッサおよび詳細設定**：ルール更新によって、システム提供の侵入ポリシーの詳細設定、およびシステム提供のネットワーク分析ポリシーのプリプロセッサ設定が変更されることがあります。また、アクセス コントロール ポリシーの高度な前処理およびパフォーマンスのオプションのデフォルト値も変更される場合があります。
- **新規および変更された変数**：ルール更新によって、既存のデフォルト変数のデフォルト値が変更されることがありますが、ユーザによる変更は上書きされません。新しい変数が常に追加されます。

マルチドメイン展開では、ローカル侵入ルールを任意のドメインにインポートできますが、グローバル ドメイン内の Talos からでなければ、侵入ルールの更新をインポートすることはできません。

⚠

**注意** 侵入ルールの更新をインポートした後の最初の展開により Snort プロセスが再起動され、トラフィックのインスペクションが中断されます。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。詳細については、Snort® の再起動によるトラフィックの動作を参照してください。

### 侵入ルールの更新によってポリシーが変更されるタイミングについて

侵入ルールの更新は、システムが提供するネットワーク分析ポリシーとカスタム ネットワーク分析ポリシーの両方だけでなく、すべてのアクセス コントロール ポリシーにも影響する場合があります。

- **システム提供**：システムが提供するネットワーク解析および侵入ポリシーへの変更は、その他のアクセス コントロールの詳細設定と同様に、更新後にポリシーを再適用すると自動的に有効になります。

- **カスタム**：すべてのカスタム ネットワーク分析ポリシーと侵入ポリシーは、システム付属ポリシーをそのベースとして、またはポリシー チェーンの根本的ベースとして使用しているので、ルール更新によってカスタム ネットワーク分析ポリシーと侵入ポリシーが影響を受けることがあります。ただし、ルール更新によるこれらの自動的な変更は回避することができます。これにより、ルール更新のインポートとは関係ないスケジュールで、システムによって提供される基本ポリシーを手動で更新できます。ユーザによる選択（カスタム ポリシーごとに実装）とは関係なく、システム付属ポリシーに対する更新によって、カスタマイズ済みの設定が上書きされることは**ありません**。

ルール更新をインポートすると、ネットワーク分析ポリシーと侵入ポリシーのキャッシュされていた変更がすべて廃棄されるので注意してください。便宜のために、[ルールの更新（Rule Updates）]ページには、キャッシュされている変更があるポリシー、および変更を行ったユーザが表示されます。

### 侵入ルールの更新の展開

侵入ルールの更新によって行われた変更を有効にするには、設定を再導入する必要があります。侵入ルールの更新をインポートする際に、影響を受けるデバイスに自動的に再導入するようシステムを設定できます。この手法が特に役立つのは、侵入ルールの更新によるシステム提供の基本侵入ポリシーの変更を許可する場合です。

### 侵入ルールの更新の繰り返し

[ルールの更新（Rule Updates）]ページを使用して、ルール更新を日次、週次、または月次ベースでインポートすることができます。

展開に高可用性ペアの Firepower Management Center が含まれる場合は、プライマリ側だけに更新をインポートします。セカンダリ Firepower Management Center は、通常の同期プロセスの一環としてルールの更新を受け取ります。

侵入ルールの更新のインポートに適用されるサブタスクは、ダウンロード、インストール、ベース ポリシーの更新、設定の展開の順で実行されます。1 つのサブタスクが完了すると、次のサブタスクが開始されます。

スケジュールされた時間になると、システムはルールの更新をインストールして、前のステップで指定したように変更後の設定を展開します。インポートの前、またはインポート中にログオフすることも、Web インターフェイスを使用して他のタスクを実行することもできます。インポート中に [ルールの更新ログ（Rule Update Log）] にアクセスすると、赤色のステータス アイコン（  ）が表示され、[ルールの更新ログ（Rule Update Log）] 詳細ビューに表示されるメッセージを確認できます。ルール更新のサイズと内容によっては、ステータス メッセージが表示されるまでに数分かかることがあります。

### ローカル侵入ルールのインポート

ローカル侵入ルールは、ASCII または UTF-8 エンコーディングによるプレーン テキスト ファイルとしてローカル マシンからインポートするカスタム標準テキスト ルールです。Snort ユーザ マニュアル（http://www.snort.org で入手可能）の指示に従って、ローカル ルールを作成することができます。

マルチドメイン展開では、任意のドメインにローカル侵入ルールをインポートできます。現在のドメインと親ドメインにインポートされたローカル侵入ルールを表示できます。

# 侵入ルールのワンタイム手動更新

| スマート ライセンス | 従来のライセンス | サポートされるデバイス | サポートされるドメイン | アクセス（Access） |
|---|---|---|---|---|
| 任意（Any） | 任意（Any） | 任意（Any） | グローバルだけ | Admin |

Firepower Management Center にインターネット アクセスがない場合、新しい侵入ルールの更新を手動でインポートします。

⚠

**注意** 侵入ルールの更新をインポートした後の最初の展開により Snort プロセスが再起動され、トラフィックのインスペクションが中断されます。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。詳細については、Snort® の再起動によるトラフィックの動作を参照してください。

**手順**

**ステップ 1** シスコのサポート サイト（http://www.cisco.com/cisco/web/support/index.html）から更新を手動でダウンロードします。

**ステップ 2** **[システム（System）] > [更新（Updates）]** を選択し、[ルールの更新（Rule Updates）] タブをクリックします。

**ステップ 3** 削除されるフォルダに作成またはインポートしたすべてのユーザ定義ルールを移動する場合、ツールバーで [すべてのローカル ルールの削除（Delete All Local Rules）] をクリックして [OK] をクリックする必要があります。

**ステップ 4** [アップロードおよびインストールするルールの更新またはテキスト ルール ファイル（Rule Update or text rule file to upload and install）] を選択し、[参照（Browse）] をクリックして、ルール アップデート ファイルを選択します。

**ステップ 5** 更新が完了した後に、ポリシーを管理対象デバイスに自動的に再展開する場合、[ルールの更新のインポートが完了した後にすべてのポリシーを再適用する（Reapply all policies after the rule update import completes）] をオンにします。

**ステップ 6** [インポート（Import）]をクリックします。ルールの更新がインストールされ、[ルール アップデート ログ（Rule Update Log）] 詳細ビューが表示されます。

（注） ルール更新のインストール中にエラー メッセージが表示された場合は、サポートに連絡してください。

# 侵入ルールのワンタイム自動更新

| スマート ライセンス | 従来のライセンス | サポートされるデバイス | サポートされるドメイン | アクセス |
|---|---|---|---|---|
| 任意（Any） | 任意（Any） | 任意（Any） | グローバルだけ | Admin |

新しい侵入ルールの更新を自動的にインポートするには、サポート サイトに接続するためのインターネット アクセスがアプライアンスで必要になります。

**注意** 侵入ルールの更新をインポートした後の最初の展開により Snort プロセスが再起動され、トラフィックのインスペクションが中断されます。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。詳細については、Snort® の再起動によるトラフィックの動作を参照してください。

### 始める前に

- Firepower Management Center にインターネット アクセス権があることを確認してください（セキュリティ、インターネット アクセス、および通信ポート を参照）。

### 手順

**ステップ 1** **[システム（System）] > [更新（Updates）]**を選択します。

**ステップ 2** [ルールの更新（Rule Updates）] タブをクリックします。

**ステップ 3** 削除されるフォルダに作成またはインポートしたすべてのユーザ定義ルールを移動する場合、ツールバーで [すべてのローカル ルールの削除（Delete All Local Rules）] をクリックして [OK] をクリックします。

**ステップ 4** [サポート サイトから新しいルールの更新をダウンロードする（Download new Rule Update from the Support Site）] を選択します。

**ステップ 5** 更新が完了した後に、変更した設定を管理対象デバイスに自動的に再展開する場合、[ルールの更新のインポートが完了した後にすべてのポリシーを再適用する（Reapply all policies after the rule update import completes）] チェックボックスをオンにします。

**ステップ 6** [インポート（Import）] をクリックします。
ルールの更新がインストールされ、[ルール アップデート ログ（Rule Update Log）] 詳細ビューが表示されます。

**注意** ルール更新のインストール中にエラー メッセージが表示された場合は、サポートに連絡してください。

# 定期的な侵入ルール更新の設定

| スマート ライセンス | 従来のライセンス | サポートされるデバイス | サポートされるドメイン | アクセス |
|---|---|---|---|---|
| 任意（Any） | 任意（Any） | 任意（Any） | グローバルだけ | Admin |

**注意** 侵入ルールの更新をインポートした後の最初の展開により Snort プロセスが再起動され、トラフィックのインスペクションが中断されます。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。詳細については、Snort® の再起動によるトラフィックの動作を参照してください。

## 手順

**ステップ 1** **[システム（System）] > [更新（Updates）]**を選択します。

**ステップ 2** [ルールの更新（Rule Updates）] タブをクリックします。

**ステップ 3** 作成した、または削除されたフォルダにインポートしたすべてのユーザ定義ルールを移動するには、ツールバーで [すべてのローカル ルールの削除（Delete All Local Rules）] をクリックし、[OK] をクリックします。

**ステップ 4** [ルール アップデートの再帰的なインポートを有効にする（Enable Recurring Rule Update Imports）] チェックボックスをオンにします。

[ルール アップデートの再帰的なインポート（Recurring Rule Update Imports）] セクションの見出しの下に、インポート ステータスに関するメッセージが表示されます。

**ステップ 5** [インポート頻度（Import Frequency）] フィールドで、次を指定します。

- 更新の頻度（[日次（Daily）]、[週次（Weekly）]、または [月次（Monthly）]）。
- 更新が必要な曜日または日付。
- 更新を開始する時刻。

**ステップ 6** 更新の完了後、変更された設定を管理対象デバイスに自動的に再展開するには、[ルール更新の完了後、更新されたポリシーを管理対象デバイスに展開する（Deploy updated policies to targeted devices after rule update completes）] チェックボックスをオンにします。

**ステップ 7** [保存（Save）] をクリックします。

**注意** 侵入ルール更新のインストール中にエラー メッセージが表示された場合は、サポートに連絡してください。

[ルール アップデートの再帰的なインポート（Recurring Rule Update Imports）] セクションの見出しの下のステータス メッセージが変わり、ルールの更新がまだ実行されていないことが示されます。

# ローカル侵入ルールのインポートのガイドライン

ローカル ルール ファイルをインポートする際には次のガイドラインに従います。

- ルールのインポータには、すべてのカスタム ルールが ASCII または UTF-8 でエンコードされるプレーン テキスト ファイルにインポートされることが必要です。
- テキストファイル名には英数字とスペースを使用できますが、下線（_）、ピリオド（.）、ダッシュ（-）以外の特殊記号は使用できません。
- システムは、単一のポンド文字（#）で始まるローカル ルールをインポートしますが、これらには削除のフラグが立てられます。
- 単一のポンド文字（#）で始まるローカル ルールはインポートされますが、2 つのポンド文字（##）で始まるローカル ルールはインポートされません。
- ルールにはエスケープ文字を含めることはできません。
- ローカル ルールをインポートするときにはジェネレータ ID（GID）を指定する必要はありません。指定する場合は、標準テキスト ルールに GID 1 のみを指定します。
- ルールを初めてインポートするときには、Snort ID（SID）またはリビジョン番号を指定しないでください。これにより、削除されたルールを含むその他のルールの SID の競合を回避できます。システムはルールに対して、1000000 以上の次に使用できるカスタム ルール SID 、およびリビジョン番号 の 1 を自動的に割り当てます。

  SID を持つルールをインポートする必要がある場合、SID は 1,000,000 ～ 9,999,999 の間の一意の数字でなければなりません。

  マルチドメイン展開では、SID が Firepower Management Center 上のすべてのドメインによって使用される共有プールからインポートされたルールに割り当てられます。複数の管理者がローカル ルールを同時にインポートする場合、個々のドメイン内の SID が連続していないように見える場合があります。これは、シーケンス内の途中の数字が別のドメインに割り込んで指定されたためです。
- 以前にインポートしたローカル ルールの更新バージョンをインポートするとき、または削除したローカル ルールを元に戻すときは、システムによって指定された SID および現在のリビジョン番号より大きいリビジョン番号を含める必要があります。ルールを編集して、現在のルールまたは削除されたルールのリビジョン番号を判別できます。

（注） ローカル ルールを削除すると、システムは自動的にリビジョン番号を増やします。これは、ローカル ルールを元に戻すための方法です。削除されたすべてのローカル ルールは、ローカル ルール カテゴリから、削除されたルール カテゴリへ移動されます。

- SID 番号の問題を回避するには、ハイ アベイラビリティ ペアのプライマリ Firepower Management Center でローカル ルールをインポートします。
- ルールに次のいずれかが含まれていると、インポートに失敗します。
  - 2147483647 より大きい SID。
  - 64 文字よりも長い送信元ポートまたは宛先ポートのリスト。
- 非推奨の `threshold` キーワードと侵入イベントしきい値機能を組み合わせて使用しているローカル ルールをインポートして、侵入ポリシーで有効にすると、ポリシーの検証に失敗します。
- インポートされたすべてのローカル ルールは、ローカル ルール カテゴリに自動的に保存されます。
- システムによって、インポートしたローカル ルールは常に無効なルール状態に設定されます。ローカル ルールを侵入ポリシーで使用できるようにするには、ローカル ルールの状態を手動で設定する必要があります。

## ローカル侵入ルールのインポート

- ローカル ルール ファイルが、ローカル侵入ルールのインポートのガイドライン （17 ページ）に記載されているガイドラインに従っていることを確認します。
- ローカル侵入ルールのインポート プロセスが、自身のセキュリティ ポリシーに適合していることを確認します。
- 帯域幅の制約や Snort の再起動が発生するため、トラフィック フローとインスペクションにインポートによる影響があることを考慮します。メンテナンス ウィンドウ期間にルール更新をスケジュールすることをお勧めします。

| スマート ライセンス | 従来のライセンス | サポートされるデバイス | サポートされるドメイン | アクセス |
|---|---|---|---|---|
| 任意（Any） | 任意（Any） | 任意（Any） | 任意（Any） | Admin |

ローカル侵入ルールをインポートするには、次の手順を使用します。インポートされた侵入ルールは、無効状態でローカル ルール カテゴリに表示されます。

### 手順

**ステップ 1** **[システム（System）] > [更新（Updates）]** を選択し、[ルールの更新（Rule Updates）] タブをクリックします。

**ステップ 2** （オプション）既存のローカル ルールを削除します。

[すべてのローカルルールの削除（Delete All Local Rules）] をクリックして、すべての作成およびインポートされた侵入ルールを削除フォルダに移動することを確認します。

**ステップ 3** [ワンタイムルール更新/ルールインポート（One-Time Rule Update/Rules Import）] で、[ルールの更新またはテキストルールファイル...（Rule update or text rule file...）] を選択して、[ファイルの選択（Choose File）] をクリックしたら、ローカル ルール ファイルを参照します。

**ステップ 4** [インポート（Import）] をクリックします。

**ステップ 5** メッセージ センターでインポートの進行状況をモニタします。

メッセージセンターを表示するには、メニュー バーの [システムステータス（System Status）] アイコンをクリックします。メッセージセンターに進行状況が数分間表示されない、またはインポートが失敗したことが示されている場合でも、インポートを再起動しません。代わりに、Cisco TAC に連絡してください。

### 次のタスク

- 侵入ポリシーを編集し、インポートしたルールを有効にします。
- 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。

# ルールの更新ログ

Firepower Management Center は、ユーザがインポートする各ルール更新およびローカル ルール ファイルごとに 1 つのレコードを生成します。

各レコードにはタイム スタンプ、ファイルをインポートしたユーザの名前、およびインポートが正常に終了したか失敗したかを示すステータス アイコンが含まれています。ユーザは、インポートしたすべてのルール更新とローカル ルール ファイルのリストを管理したり、リストからレコードを削除したり、インポートしたすべてのルールとルール更新コンポーネントに関する詳細レコードにアクセスすることができます。

[ルール アップデートのインポート ログ（Rule Update Import Log）] 詳細ビューには、ルール更新またはローカル ルール ファイルにインポートされた各オブジェクトの詳細レコードが表示されます。表示されるレコードのうち、自分のニーズに合う情報のみを含むカスタム ワークフローまたはレポートを作成することもできます。

# 侵入ルール更新のログ テーブル

表 *2:* 侵入ルール更新のログ フィールド

| フィールド | 説明 |
|---|---|
| 要約 | インポート ファイルの名前。インポートが失敗した場合は、ファイル名の下に、失敗した理由の簡単な説明が表示されます。 |
| 時刻（Time） | インポートが開始された日時。 |
| ユーザ ID（User ID） | インポートをトリガーとして使用したユーザ名。 |
| ステータス（Status） | インポートの状態を表します<br>• 正常終了（）<br>• 失敗、または実行中（）<br>インポート中には [ルールアップデートログ（Rule Update Log）] ページで、正常終了しなかった、または完了していないことを示す赤いステータス アイコンが表示され、インポートが正常終了した場合のみこれが緑色のアイコンに変わります。 |

ヒント　侵入ルール更新のインポートの進行中に示される、インポートの詳細を表示することができます。

# 侵入ルールの更新ログの表示

| スマート ライセンス | 従来のライセンス | サポートされるデバイス | サポートされるドメイン | アクセス |
|---|---|---|---|---|
| 任意（Any） | 任意（Any） | 任意（Any） | 任意（Any） | Admin |

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

**手順**

ステップ 1　**[システム（System）]** > **[更新（Updates）]**を選択します。

ヒント　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）]**）の [インポート ページ（Import Rules）] をクリックすることもできます。

**ステップ 2**　[ルールの更新（Rule Updates）] タブをクリックします。

**ステップ 3**　[ルールアップデートログ（Rule Update Log）] をクリックします。

**ステップ 4**　次の 2 つの対処法があります。

- 詳細の表示：ルールの更新またはローカル ルール ファイルにインポートされる各オブジェクトの詳細を表示するには、表示するファイルの横にある表示アイコン（）をクリックします（侵入ルールの更新インポート ログの詳細の表示 （24 ページ）を参照）。
- 削除：インポート ログからインポート ファイル レコード（ファイルに含まれるすべてのオブジェクトに関する詳細レコードを含む）を削除するには、インポート ファイル名の横にある削除アイコン（）をクリックします。

（注）　ログからファイルを削除しても、インポート ファイルにインポートされているオブジェクトはいずれも削除されませんが、インポート ログ レコードのみは削除されます。

## 侵入ルール更新ログのフィールド

ヒント　1 つのインポート ファイルのレコードのみが表示されている [ルール アップデートのインポート ログ（Rule Update Import Log）] 詳細ビューからツールバーの [検索（Search）] をクリックして検索を開始した場合でも、[ルール アップデートのインポート ログ（Rule Update Import Log）]データベースの全体が検索されます。検索の対象とするすべてのオブジェクトが含まれるように、時間制限が設定されていることを確認します。

表 *3 : [*ルール アップデートのインポート ログ（***Rule Update Import Log***）*]* 詳細ビューのフィールド

| フィールド | 説明 |
|---|---|
| 操作（Action） | オブジェクト タイプについて、次のいずれかが発生していることを示します。<br>• [新規（new）]（ルールで、このアプライアンスにルールが最初に格納された場合）<br>• [変更済み（changed）]（ルール更新コンポーネントまたはルール用。ルール更新コンポーネントが変更された場合、またはルールのリビジョン番号が大きく、GID と SID が同じ場合）<br>• [競合（collision）]（ルール更新コンポーネントまたはルールに関して、アプライアンス上の既存のコンポーネントまたはルールとリビジョンが競合しているため、インポートがスキップされた場合）<br>• [削除済み（deleted）]（ルール用。ルール更新からルールが削除された場合）<br>• [有効（enabled）]（ルール更新の編集で、プリプロセッサ、ルール、または他の機能が、システムで提供されるデフォルト ポリシーで有効になっていた場合）<br>• [無効（disabled）]（ルールで、システム提供のデフォルト ポリシーでルールが無効になっていた場合）<br>• [ドロップ（drop）]（ルールで、システムで提供されるデフォルト ポリシーで、ルールが [ドロップおよびイベントの生成（Drop and Generate Events）] に設定されていた場合）<br>• [エラー（error）]（ルール更新またはローカル ルール ファイル用。インポートに失敗した場合）<br>• [適用（apply）]（インポートに対して [ルール更新のインポート完了後にすべてのポリシーを再適用する（Reapply all policies after the rule update import completes）] オプションが有効だった場合） |
| デフォルト アクション（Default Action） | ルールの更新によって定義されたデフォルトのアクション。インポートされたオブジェクトのタイプが [ルール（rule）] の場合、デフォルトのアクションは [通過（Pass）]、[アラート（Alert）]、または [ドロップ（Drop）] になります。インポートされた他のすべてのオブジェクト タイプには、デフォルトのアクションはありません。 |

| フィールド | 説明 |
|---|---|
| 詳細（Details） | コンポーネントまたはルールに対する一意の文字列。ルールの場合、変更されたルールの GID、SID、および旧リビジョン番号は、`previously (GID:SID:Rev)` と表示されます。変更されていないルールについては、このフィールドは空白です。 |
| ドメイン（Domain） | 侵入ポリシーで更新されたルールを使用できるドメイン。子孫ドメインの侵入ポリシーもルールを使用できます。このフィールドは、マルチドメイン展開の場合にのみ存在します。 |
| GID | ルールのジェネレータ ID。たとえば、`1`（標準テキスト ルール）または `3`（共有オブジェクト ルール）。 |
| [名前（Name）] | インポートされたオブジェクトの名前。ルールの場合はルールの [メッセージ（Message）] フィールドに対応した名前で、ルール更新コンポーネントの場合はコンポーネント名です。 |
| ポリシー | インポートされたルールの場合、このフィールドには [すべて（All）] が表示されます。これは、インポートされたルールがデフォルトのすべての侵入ポリシーに含まれていたことを意味します。インポートされた他のタイプのオブジェクトについては、このフィールドは空白です。 |
| Rev | ルールのリビジョン番号。 |
| ルール アップデート（Rule Update） | ルール更新のファイル名。 |
| SID | ルールの SID。 |
| 時刻（Time） | インポートが開始された日時。 |

| フィールド | 説明 |
|---|---|
| タイプ（Type） | インポートされたオブジェクトのタイプで、有効な値は次のいずれかです。<br>• [ルール更新コンポーネント（rule update component）]（ルール パックやポリシー パックなどのインポートされたコンポーネント）<br>• [ルール（rule）]（ルール用。新しいルールまたは更新されたルール。バージョン 5.0.1 では、廃止された `update` 値の代わりにこの値が使用されます）。<br>• [ポリシー適用（policy apply）]（インポートに対して [ルール更新のインポート完了後にすべてのポリシーを再適用する（Reapply all policies after the rule update import completes）] オプションが有効だった場合） |
| メンバー数（Count） | 各レコードのカウント（1）。テーブルが制限されており、[ルール アップデート ログ（Rule Update Log）] 詳細ビューがデフォルトでルール更新レコードに制限されている場合は、テーブル ビューに [メンバー数（Count）] フィールドが表示されます。このフィールドは検索できません。 |

## 侵入ルールの更新インポート ログの詳細の表示

| スマート ライセンス | 従来のライセンス | サポートされるデバイス | サポートされるドメイン | アクセス |
|---|---|---|---|---|
| 任意（Any） | 任意（Any） | 任意（Any） | 任意（Any） | Admin |

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

**手順**

**ステップ 1** **[システム（System）] > [更新（Updates）]**を選択します。

**ステップ 2** [ルールの更新（Rule Updates）] タブをクリックします。

**ステップ 3** [ルールアップデートログ（Rule Update Log）] をクリックします。

**ステップ 4** 表示する詳細レコードが含まれているファイルの隣にある表示アイコン（  ）をクリックします。

**ステップ 5** 次のいずれかの処理を実行できます。

- ブックマーク：現在のページをブックマークするには、[このページをブックマーク（Bookmark This Page）] をクリックします。
- 検索の編集：現在の単一制約が事前入力されている検索ページを開くには、検索制約の横にある [検索の編集（Edit Search）] または [検索の保存（Save Search）] を選択します。
- ブックマークの管理：ブックマークの管理ページに移動するには、[レポート デザイナ（Report Designer）] をクリックします。
- レポート：現在のビューのデータに基づいてレポートを生成するには、[レポート デザイナ（Report Designer）] をクリックします。
- 検索：ルールの更新インポート ログ データベース全体でルールの更新インポート レコードを検索するには、[検索（Search）] をクリックします。
- ソート：現在のワークフローページでレコードをソートしたり制約したりするには、詳細についてドリルダウン ページの使用を参照してください。
- ワークフローの切り替え：別のワークフローを一時的に使用するには、[(ワークフローの切り替え)（(switch workflows)）] をクリックします。