システム ソフトウェアの更新

次のトピックでは、Firepower の展開を更新する方法について説明します。

FirePOWER の更新について

シスコでは、Firepower の展開に対していくつかの種類のアップグレードと更新を配信しています。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、更新しても設定は変更されません。メジャー アップグレードはアンインストールできません。また、VDB、GeoDB、SRU を前のバージョンに戻すこともできません。

表 *1 : Firepower* のアップグレードと更新

更新のタイプ	説明	ドメイン
メジャー アップグレード	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。 新規インストールまたは復元はできますが、アンインストールはできません。 オペレーティング システムを個別にアップグレードするデバイスの場合、付随するオペレーティング システムのアップグレードを伴うことがあります。 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。	グローバルのみ

更新のタイプ	説明	ドメイン
マイナー アップグレード（パッチ）	限られた範囲の修正が含まれています。 アンインストールできますが、新規インストールまたは復元はできません。メジャー バージョンに復元してからマイナー バージョンにアップグレードする必要があります。	グローバルのみ
脆弱性データベース（VDB）	動的分析の対象となる脆弱性、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、およびファイル タイプの検出を更新します。	グローバルのみ
侵入ルールの更新（SRU）	新規および更新された侵入ルールおよびプリプロセッサ ルール、既存のルールの変更後のステータス、デフォルト侵入ポリシーの変更後の設定が提供されます。 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 ローカル インポート：任意
位置情報データベース（GeoDB）	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 アドレスに関連付けることができるものに関する情報を更新します。GeoDB をインストールして地理的位置情報の詳細を表示するか、または地理的位置情報ベースのアクセス制御を実行します。	グローバルのみ

Firepower 更新のガイドラインおよび制限事項

更新する前に

Firepower 展開のいずれかのコンポーネント（VDB、GeoDB、SRU など）を更新する前に、更新に付属しているリリース ノートまたはアドバイザリ テキストを読んでおく必要があります。これらは、互換性、前提条件、新機能、動作の変更、警告など、重要かつリリースに固有の情報を提供します。

Firepower Management Center 展開のシステム ソフトウェア 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、『Cisco Firepower Management Center Upgrade Guide』を参照してください。

帯域幅のガイドライン

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。

Firepower システム 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。慎重に計画および準備することで、失敗を回避することができます。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とプッシュ、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、『Cisco Firepower Management Center Upgrade Guide』を参照してください。

脆弱性データベース（VDB）の手動による更新

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数	サポートされるドメイン数	アクセス
任意	任意	任意	グローバルのみ	管理者

Cisco Vulnerability Database（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 Intelligence 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。

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、この手順を使用します。VDB 更新を自動化するには、タスクのスケジューリング（**[システム（System）]**>**[ツール（Tools）]**>**[スケジューリング（Scheduling）]**）を使用します。詳細は、脆弱性データベースの更新の自動化を参照してください。

重要 自動 VDB 更新をスケジュールしない場合は、これらの更新を定期的にチェックする必要があります。更新は毎日 1 回だけ実行され、https://www.cisco.com/go/firepower-software の適切な子ページに掲載されます。

注意 脆弱性データベース（VDB）の更新のインストールを開始するために Firepower Management Center を選択すると警告が表示される場合は、VDB のインストール後に設定を展開し、Snort プロセスの展開を再開する必要があります。Firepower Threat Defense デバイスへの展開の保留に関する追加の警告が展開ダイアログに表示されます。展開の中断中にインスペクションを続行せずにトラフィックをドロップするか、パスするかは、対象デバイスによるトラフィックの処理方法によって異なります。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。Firepower Management Center にのみ適用される VDB の更新では再起動が行われないため、更新を展開できません。

始める前に

- https://www.cisco.com/go/firepower-software から更新プログラムをダウンロードします。
- 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。

ステップ 1 **[System]** > **[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 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。

設定を展開

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、ファイルが破損することがあります。

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 の更新は他のシステムの機能（実行中の地理情報の収集など）を中断することはありませんが、更新が完了するまでシステムのリソースを消費します。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数	サポートされるドメイン数	アクセス
任意	任意	任意	グローバルのみ	管理者

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。

ステップ 1 **[System]** > **[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数	サポートされるドメイン数	アクセス
任意	任意	任意	グローバルのみ	管理者

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。

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 **[System]** > **[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数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（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。

ステップ 1 **[System]** > **[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 Intelligence 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。新しいルールについては、ルールの状態がそれぞれのシステム提供の侵入ポリシーで異なる場合があります。たとえば、Security over Connectivity の侵入ポリシーでは新しいルールが有効になっており、Connectivity over Security の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状態が変更されたり、既存のルールそのものが削除されることもあります。
- **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。

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**：カスタムのネットワーク解析および侵入ポリシーは、いずれもシステム提供のポリシーをベースとして使用するか、ポリシー チェーン中でのイベント ベースとして使用しているので、ルール更新がカスタムのネットワーク解析および侵入ポリシーにも影響を与えることがあります。ただし、ルール更新によるこれらの自動的な変更が行われないように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

択とは関係なく（カスタムポリシーごとに実装）システム提供のポリシーに対する更新では、ユーザがカスタマイズした設定は上書き**されません**。

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。インポート中にアクセスした場合は、[Rule Update Log] に赤いステータスのアイコン（  ）が表示され、[Rule Update Log] 詳細ビューでは表示された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数	サポートされるドメイン数	アクセス
任意	任意	任意	グローバルだけ。	管理者

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。

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 **[System]** > **[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数	サポートされるドメイン数	アクセス
任意	任意	任意	グローバルのみ	管理者

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。

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）。

ステップ 1 **[System]** > **[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 [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数	サポートされるドメイン数	アクセス
任意	任意	任意	グローバルのみ	管理者

ステップ 1 **[System]** > **[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。
- マルチドメイン展開では、グローバル ドメインにインポートまたは作成されたルールに 1 の GID が割り当てられ、他のすべてのドメインには 1000 ～ 2000 の間のドメイン固有 GID が割り当てられます。
- 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 には 1,000,000 以上の一意の番号を指定できます。

  マルチドメイン展開で、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。
  - マルチドメイン展開でグローバル ドメインにインポートする場合、GID:SID の組み合わせでは、別のドメインに既に存在する GID 1 と SID を使用します。これは、バージョン 6.2.1 より前に組み合わせが存在していたことを示します。GID 1 と固有の SID を使用してルールを再インポートできます。
- 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 （12 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数	サポートされるドメイン数	アクセス
任意	任意	任意	任意	管理者

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。

ステップ 1 **[System]** > **[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名、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。

[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
Summary	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。
Time	インポートが開始された日時。
User ID	インポートをトリガーとして使用したユーザ名。
Status	インポートの状態を表します • 正常終了（） • 失敗、または実行中（） 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数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（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。

ステップ 1　**[System]** > **[Updates]** を選択します。

ヒント　侵入ルール エディタ ページ（**[Objects]** > **[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 （18 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
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。 • [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） • [changed]（ルール更新コンポーネントまたはルールで、ルール更新コンポーネントが変更された場合、ルールのリビジョン番号が大きく、GID と SID が同じだった場合） • [collision]（ルール更新コンポーネントまたはルールで、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の競合によりインポートがスキップされた場合） • [deleted]（ルール用。ルール更新からルールが削除された場合） • [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） • [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） • [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 [Drop and Generate Events] に設定されていた場合） • [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） • [apply]（インポートに対して [Reapply all policies after the rule update import completes] オプションが有効だった場合）
Default Action	ルールの更新によって定義されている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 [rule] の場合、デフォルトのアクションは [Pass]、[Alert]、または [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。
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、GID、SID、および変更されたルールの以前のリビジョン番号については、`previously (GID:SID:Rev)` のように表示されます。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。
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、グローバル ドメインまたは従来の GID）または `3`（共有オブジェクト ルール）。
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 [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。
Policy	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。つまり、ルールが正常にインポートされ、適切なデフォルト侵入ポリシーすべてで有効にすることができます。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。

フィールド	説明
Rule Update	ルール更新のファイル名。
SID	ルールの SID。
Time	インポートが開始された日時。
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。 • [rule update component]（ルール パックまたはポリシー パックなどの、インポートされたコンポーネント） • [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）。 • [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）
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数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（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。

ステップ 1 **[System]** > **[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。

エアギャップ展開の維持

Firepower システムがインターネットに接続されていない場合、必要な更新は自動的に実行されません。

それらの更新を手動で取得してインストールする必要があります。次の情報を参照してください。

- 脆弱性データベース（VDB）の手動による更新 （3 ページ）
- 侵入ルールのワンタイム手動更新 （10 ページ）
- 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 （6ページ）
- *Firepower Management Center Software Upgrade Guide*
  https://www.cisco.com/c/en/us/td/docs/security/firepower/upgrade/fpmc-upgrade-guide.html