更新

この章では、コンテンツの更新方法について説明します。

システムソフトウェアのアップグレード

このガイドヘルプには、システム ソフトウェアまたはファイアウォール シャーシのアップグレード方法に関する情報はありません。Firewall Management Center が現在実行しているバージョンの Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド を参照してください。

コンテンツの更新について

システムはインターネットからコンテンツの更新を取得できます。可能な限り、コンテンツの自動更新をスケジュールするか、有効にすることを推奨します。一部の更新は、初期セットアッププロセスによって、または関連機能を有効にすると、自動的に有効になります。初期セットアップ後に、すべての自動更新を確認し、必要に応じて調整することを推奨します。

表 *1*: コンテンツの更新

コンポーネント	説明（Description）	詳細
脆弱性データベース（VDB）	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。	**スケジュール**：スケジュールタスクとして。 **アンインストール**：VDB 357 以降、その Firewall Management Center の基準 VDB までさかのぼって任意の VDB をインストールできます。 **参照先**： 脆弱性データベース（VDB）の更新 （3 ページ）
位置情報データベース（GeoDB）	シスコの地理位置情報データベース（GeoDB）は、IP アドレスを国/大陸にマッピングします。	**スケジュール**：専用の更新ページから **アンインストール**：なし。 **参照先**： 地理位置情報データベース（GeoDB）の更新（6 ページ）
侵入ルール（SRU/LSP）	侵入ルールを更新すると、更新された新しい侵入ルールおよびプリプロッセサルール、既存のルールに対して変更された状態、および変更されたデフォルトの侵入ポリシーの設定が提供されます。 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。	**スケジュール**：専用の更新ページから。 **アンインストール**：なし。 **参照先**： 侵入ルールの更新 （7 ページ）
セキュリティインテリジェンスのフィード	セキュリティ インテリジェンスのフィードは、エントリに一致するトラフィックをすばやくフィルタリングするために使用できるIPアドレス、ドメイン名、およびURLのコレクションです。	**スケジュール**：オブジェクト マネージャから。 **アンインストール**：なし。 **参照先**： Cisco Secure Firewall Management Center デバイス構成ガイド
URL カテゴリとレピュテーション	URL フィルタリングでは、URL の一般的な分類（カテゴリ）およびリスクレベル（レピュテーション）に基づいて、Webサイトへのアクセスを制御することができます。	**スケジュール**：統合/クラウドサービスを設定する場合、またはスケジュール タスクとして。 **アンインストール**：なし。 **参照先**： Cisco Secure Firewall Management Center デバイス構成ガイド

コンテンツ アップデートの要件と前提条件

モデルのサポート

Any

サポートされるドメイン

Global（特に明記のない場合）。

ユーザの役割

管理者

コンテンツの更新のガイドラインと制約事項

リリースノート

コンテンツの更新に付随するリリースノートまたはアドバイザリテキストを読むことをお勧めします。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。

スケジュールされた更新

スケジュールされた更新が意図したとおりに実行されることを確認してください。システムは、タスク（更新を含む）を UTC でスケジュールします。そのため、いつ現地で実行されるかは、日付と場所によって異なります。また、更新はUTCでスケジュールされるため、サマータイムなど、所在地で実施される場合がある季節調整に合わせて調節されることもありません。このような影響を受ける場合、スケジュールされた更新は、現地時間を基準とすると、夏期では冬期の場合よりも 1 時間「遅れて」実行されることになります。

脆弱性データベース（VDB）の更新

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。

シスコでは、VDB に対して定期的に更新を提供しています。Firewall 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。

Firewall Management Center の初期設定では、1 回限りの操作でシスコから最新の VDB が自動的にダウンロードされてインストールされます。また、最新の VDB を含む最新の利用可能なソフトウェアアップデートをダウンロードする週次タスクもスケジュールされます。この週次タスクを確認し、必要に応じて調整することをお勧めします。必要に応じて、VDB を実際に更新し、構成を展開する新しい週次タスクをスケジュールしてください。詳細については、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。

VDB 343 以降では、すべてのアプリケーションディテクタ情報は、Cisco Secure Firewall アプリケーションディテクタから入手できます。このサイトには、アプリケーションディテクタの検索可能なデータベースが含まれています。リリースノートには、特定の VDB リリースの変更に関する情報が記載されています。

VDB の更新のスケジュール

Firewall Management Center でインターネットアクセスができる場合、定期的な VDB 更新をお勧めします。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。

VDB の手動更新

次の手順を使用して手動で VDB を更新します。VDB 357 以降、その Firewall Management Center の基準 VDB までさかのぼって任意の VDB をインストールできます。

注意 VDB の更新中に、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。

ほとんどの場合、VDB 更新後の最初の展開では Snort プロセスが再起動され、トラフィックインスペクションが中断されます。これが発生すると、システムから警告が表示されます（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のフィンガープリントについては再起動が必要ですが、脆弱性情報については不要です）。こ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がドロップされるかパスするどうかは、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。

始める前に

Firewall Management Center がインターネットにアクセスできない場合 、または古い VDB をインストールする場合は、自分で更新を取得してください：https://www.cisco.com/go/firepower-software 。モデルを選択または検索し（または任意のモデルを選択して、すべての Firewall Management Center に同じ VDB を使用します）、[カバレッジおよびコンテンツの更新（Coverage and Content Updates）] ページを参照します。

手順

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

ステップ 2 VDB を Firewall Management Center に取得する方法を選択します。

- 直接ダウンロード：[アップデートのダウンロード（Download Updates）] ボタンすぐにダウンロードできます。
- 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、[ファイルの選択（Choose File）] をクリックして VDB を参照します。ファイルを選択したら、[アップロード（Upload）] をクリックします。

ステップ 3 VDB をインストールします。

a) インストールする [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 [インストール（Install）] アイコン（新しい VDB の場合）または [ロールバック（Rollback）] アイコン（古い VDB の場合）をクリックします。
b) Firewall Management Center を選択します。
c) [Install（インストール）] をクリックします。

Message Center で更新の進行状況をモニターします。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 4 更新が成功したことを確認します。

VDB 更新ページと **[ヘルプ（Help）]**（⚙）> **[概要（About）]** の両方に現在のバージョンが表示されます。

次のタスク

- 設定変更を展開します。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。
- 利用できなくなった脆弱性、アプリケーションディテクタ、またはフィンガープリントに基づいて設定を行っている場合は、それらの設定を調べて、トラフィックが期待どおりに処理されていることを確認します。また、VDB を更新するためのスケジュールされたタスクは、ロールバックを取り消すことができることに注意してください。これを回避するには、スケジュールされたタスクを変更するか、新しい VDB パッケージを削除します。

地理位置情報データベース（GeoDB）の更新

地理位置情報データベース（GeoDB）は、地理的な位置に基づいてトラフィックを表示およびフィルタリングするために利用できるデータベースです。シスコでは GeoDB を定期的に更新しています。正確な地理位置情報を取得するには、GeoDB を定期的に更新する必要があります。初期構成の一環として、システムは週次 GeoDB 更新をスケジュールします。このタスクを確認し、必要に応じ、GeoDB 更新のスケジューリング （6 ページ）。

GeoDB の更新は、以前のバージョンをオーバーライドします。Firewall Management Center は、自動で、管理対象デバイスを更新し、まれなケースですがアップデートにより新しい国が追加されない限り、再デプロイは不要です。**[ヘルプ（Help）]**（?）> **[概要（About）]** で現在のバージョンを確認できます。

GeoDB 更新のスケジューリング

初期構成の一環として、システムは週次 GeoDB 更新をスケジュールします。このタスクを確認し、必要に応じ、この手順。

GeoDB の更新後は、ほとんどの場合不要なため、システムは自動的にデプロイされないことに注意してください。ただし、スケジュールされた GeoDB の更新によって、まれではありますが、新しい国が追加された後は、できるだけ早くデプロイします。これにより、新しい国を大陸の一部として数えることができます。たとえばこの更新で大陸に国が追加された場合、「大陸」ベースでフィルタ処理されるルールは、デプロイするまで国を経由したトラフィックと一致しません。

始める前に

Firewall 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）]（⚙）> **[Content Updates]** > **[Geolocation Updates]** を選択します。

ステップ 2 [Recurring Geolocation Updates] で、[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。

地理位置情報データベース（GeoDB）の手動更新

オンデマンド GeoDB 更新を実行するには、次の手順を実行します。

始める前に

Firewall Management Center がインターネットにアクセスできない場合は、自分で更新情報を取得してください： https://www.cisco.com/go/firepower-software 。モデルを選択または検索し（または任意のモデルを選択して、すべての Firewall Management Center に同じ GeoDB を使用します）、[カバレッジおよびコンテンツの更新（Coverage and Content Updates）] ページを参照します。

手順

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

ステップ 2 [1回限りの地理位置情報更新（One-Time Geolocation Update）] で、GeoDB の更新方法を選択します。

- 直接ダウンロード：[ダウンロードしてインストール...（Download and install...）] を選択します。
- 手動アップロード：**[アップロードしてインストール...（Upload and install...）]** を選択し、**[ファイルを選択（Choose File）]** をクリックして、事前にダウンロードした国コードパッケージを参照します。

ステップ 3 [インポート（Import）] をクリックします。

Message Center で更新の進行状況をモニターします。

ステップ 4 更新が成功したことを確認します。

GeoDB 更新ページと **[ヘルプ（Help）]**（?） > **[概要（About）]** の両方に現在のバージョンが表示されます。

次のタスク

更新プログラムで新しい国が追加されている場合（これはまれです）、ここで展開します。展開するまで、新しい国はその大陸の一部としてカウントされません。たとえばこの更新で大陸に国が追加された場合、「大陸」ベースでフィルタ処理されるルールは、デプロイするまで国を経由したトラフィックと一致しません。

侵入ルールの更新

新たな脆弱性が発見されると、Talos インテリジェンスグループ は侵入ルールの更新をリリースします。侵入ルールの更新は、侵入ルール、プリプロセッサルール、および各ルールを使用するポリシーに影響を及ぼします。侵入ルールの更新は累積的であるため、システムを最新の状態に保つことを推奨します。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分析および侵入ポリシーへの変更は、その他のアクセス制御の詳細設定と同様に、更新後にポリシーを再展開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。ユーザーによる選択（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。

注意 ルールの更新自体は、展開時に Snort プロセスを再起動しませんが、加えた他の変更により再起動する可能性があります。Snort を再起動すると、高可用性/拡張性を備えた構成になっているものを含め、すべてのデバイスでトラフィックフローとインスペクションが一時的に中断されます。インターフェイス設定により、中断中にインスペクションせずにトラフィックをドロップするか受け渡すかが決定されます。Snort を再起動せずに展開すると、リソース要求時にいくつかのパケットが検査なしでドロップされることがあります。

侵入ルールの更新の繰り返し

初期構成の一環として、システムは日次の侵入ルール更新をスケジュールします。このタスクを確認し、必要に応じ、侵入ルールの更新のスケジュール （9 ページ）。頻度を変更したり、ルールインポート後の自動展開を有効にすることができます。高可用性Firewall Management Center の場合は、アクティブユニットに更新をインポートするだけで済みます。

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。

侵入ルールの更新のスケジュール

初期構成の一環として、システムは日次の侵入ルール更新をスケジュールします。このタスクを確認し、必要に応じ、この手順。

始める前に

- 侵入ルールの更新プロセスが、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。
- Firewall 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）]（⚙）>**[Content Updates]**>**[Rule Updates]** を選択します。

ステップ 2 [定期的なルール更新のインポート（Recurring Rule Update Imports）] で、[定期的なルール更新のインポートを有効にする（Enable Recurring Rule Update Imports）] をオンにします。

ステップ 3 [インポート頻度（Import Frequency）] と開始時刻を指定します。

ステップ 4 （オプション）各更新後に展開するには、[...すべてのポリシーを再適用（Reapply all policies...）] をオンにします。

ステップ 5 [保存（Save）] をクリックします。

侵入ルールの手動更新

オンデマンド侵入ルール更新を実行するには、次の手順を実行します。

始める前に

- 侵入ルールの更新プロセスが、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。
- Firewall Management Center がインターネットにアクセスできない場合は、自分で更新情報を取得してください： https://www.cisco.com/go/firepower-software 。モデルを選択または検索し（または任意のモデルを選択して、すべての Firewall Management Center に同じ更新を使用します）、[カバレッジおよびコンテンツの更新（Coverage and Content Updates）] ページを参照します。

手順

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

ステップ 2 [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、侵入ルールの更新方法を選択します。

- 直接ダウンロード：[新しいルール更新をダウンロードする...（Download new rule update...）] を選択します。
- 手動アップロード：[ルール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、[ファイルの選択（Choose File）] をクリックして侵入ルール更新を参照します。

ステップ 3 （任意）更新後に展開するには、[すべてのポリシーを再適用する...（Reapply all policies...）] をオンにします。

ステップ 4 [インポート（Import）] をクリックします。

Message Center で更新の進行状況をモニターします。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。

ステップ 5 更新が成功したことを確認します。

ルール更新ページと **[ヘルプ（Help）]**（⚙）> **[概要（About）]** の両方に現在のバージョンが表示されます。

次のタスク

更新の一部として展開しなかった場合は、ここで展開します。

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。このタスクは、どのドメインでも実行できます。

始める前に

- 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に関するガイドライン（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。

手順

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

侵入ルールエディタ（**[オブジェクト（Objects）]** > **[侵入ルール（Intrusion Rules）]**）で [ルールのインポート（Import Rules）] をクリックすることもできます。

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、[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。

メッセージセンターでインポートの進行状況をモニターできます。メッセージセンターに進行状況が数分間表示されない、または更新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。

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。Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

ローカル侵入ルールのインポートに関するガイドライン

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、高可用性ペアのプライマリ Firewall 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。

侵入ルールの更新ログの表示

システムは、ルールの更新/インポートのログを生成します。これには、タイムスタンプ、ユーザー、および各更新の成功/失敗が示されます。これらのログには、更新されたすべてのルールおよびコンポーネントに関する詳細なインポート情報が含まれています。侵入ルール更新のログの詳細 （14 ページ）を参照してください。ルールインポートログを表示するには、次の手順を実行します。インポートログを削除してもインポートされたオブジェクトは削除されな

いことに注意してください。 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）]（⚙） > **[Content Updates]** > **[Rule Updates]** を選択します。

ステップ 2 [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 3 （任意）ログファイルの横にある [表示（View）]（👁） をクリックして、ルール更新の詳細を表示します。

侵入ルール更新のログの詳細

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 *2:* 侵入ルール更新のログの詳細

フィールド	説明
操作	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。

フィールド	説明
Rev	ルールのリビジョン番号。
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）。 • [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。

エアギャップ展開の維持

Firewall Management Center 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。

詳細については、以下を参照してください。

- VDB の手動更新 （4 ページ）
- 侵入ルールの手動更新 （10 ページ）
- 地理位置情報データベース（GeoDB）の手動更新 （6 ページ）

コンテンツ更新の履歴

表 *3:* コンテンツ更新の履歴

機能	最小の Management Center	最小の Threat Defense	詳細
自動 VDB ダウンロード。	7.3.0	いずれか	Firewall Management Center の初期設定では、最新の脆弱性データベース（VDB）を含むようになった、利用可能な最新のソフトウェア更新をダウンロードするための週次タスクがスケジュールされています。この週次タスクを確認し、必要に応じて調整することをお勧めします。必要に応じて、VDB を実際に更新し、構成を展開する新しい週次タスクをスケジュールしてください。 新規/変更された画面：システムで作成された [週次ソフトウェアダウンロード（Weekly Software Download）] のスケジュールされたタスクで、[脆弱性データベース（Vulnerability Database）] チェックボックスがデフォルトで有効になりました。
任意の VDB をインストールします。	7.3.0	いずれか	VDB 357 以降、その Firewall Management Center の基準 VDB までさかのぼって任意の VDB をインストールできます。 VDB を更新したら、構成の変更を展開します。利用できなくなった脆弱性、アプリケーションディテクタ、またはフィンガープリントに基づいて設定を行っている場合は、それらの設定を調べて、トラフィックが期待どおりに処理されていることを確認します。また、VDB を更新するためのスケジュールされたタスクは、ロールバックを取り消すことができることに注意してください。これを回避するには、スケジュールされたタスクを変更するか、新しい VDB パッケージを削除します。 新しい/変更された画面：**[システム（System）]**（⚙）> **[更新（Updates）]** > **[製品アップデート（Product Updates）]** > **[利用可能なアップデート（Available Updates）]**で、古い VDB をアップロードすると、[インストール（Install）] アイコンの代わりに新しい [ロールバック（Rollback）] アイコンが表示されます。

機能	最小の Management Center	最小の Threat Defense	詳細
スケジュール済みタスクでは、パッチおよびVDB 更新のみダウンロードされます。	7.2.6 7.4.1	任意	**アップグレードの影響。スケジュールされたダウンロードタスクは、メンテナンスリリースの取得を停止します。** [最新の更新のダウンロード（Download Latest Update）] スケジュール済みタスクでは、メンテナンスリリースはダウンロードされなくなり、適用可能な最新のパッチと VDB の更新のみがダウンロードされるようになりました。メンテナンス（およびメジャー）リリースを Firewall Management Center に直接ダウンロードするには、**[システム（System）] > [製品のアップグレード（Product Upgrades）]**を使用します。 バージョンの制限：Firewall Management Center バージョン 7.3.x または 7.4.0 ではサポートされていません。
カスタム侵入ルールのインポートでルール競合の際に警告表示。	6.7.0	いずれか	カスタム（ローカル）侵入ルールをインポートする場合、FMCがルールの競合について警告するようになりました。以前は、システムは競合の原因となるルールをサイレントにスキップしていました。ただし、競合のあるルールのインポートが完全に失敗するバージョン6.6.0.1は除きます。 [ルールの更新（Rule Updates）]ページで、ルールのインポートに競合があった場合は、[ステータス（Status）]列に警告アイコンが表示されます。詳細については、警告アイコンの上にポインタを置いて、ツールチップを参照してください。 既存のルールと同じSID/リビジョン番号を持つ侵入ルールをインポートしようとすると、競合が発生することに注意してください。カスタムルールの更新バージョンには必ず新しいリビジョン番号を付けてください。 新規/変更された画面：[システム（System）]（⚙） > **[更新（Updates）] > [ルールの更新（Rule Updates）]** に警告アイコンが追加されました。
初期セットアップ中の自動 VDB 更新。	6.6.0	任意（Any）	新規または再イメージ化された FMC をセットアップすると、システムは自動的に脆弱性データベース（VDB）の更新を試みます。 これは1回限りの操作です。FMCがインターネットにアクセスできる場合は、自動の定期 VDB 更新のダウンロードとインストールを実行するようにタスクをスケジュールしておくことを推奨します。

機能	最小の Management Center	最小の Threat Defense	詳細
ソフトウェアの自動ダウンロードと GeoDB の更新。	6.5.0	いずれか	新規または再イメージ化された FMC をセットアップすると、システムは自動的に脆弱性データベース（VDB）の更新を試みます。 これは1回限りの操作です。FMCがインターネットにアクセスできる場合は、自動の定期 VDB 更新のダウンロードとインストールを実行するようにタスクをスケジュールしておくことを推奨します。
署名済みの SRU、VDB、および GeoDB の更新。	6.4.0	いずれか	正しい更新ファイルを使用していることが確認できるため、バージョン 6.4 以降では署名済みの更新を侵入ルール（SRU）、脆弱性データベース（VDB）、および地理位置情報データベース（GeoDB）が使用されます。以前のバージョンでは、引き続き未署名の更新が使用されます。 手動で更新をダウンロードしない限り（たとえば、エアギャップ導入環境の場合）、機能の違いはわかりません。ただし、SRU、VDB、および GeoDB の更新を手動でダウンロードしてインストールする場合は、必ず現在のバージョンに対応した正しいパッケージをダウンロードしてください。 署名付きの更新ファイルの先頭は、以下のように「Sourcefire」ではなく「Cisco」で、末尾は .sh ではなく .sh.REL.tar です。 • SRU：Cisco_Firepower_SRU-*date-build*-vrt.sh.REL.tar • VDB：Cisco_VDB_Fingerprint_Database-4.5.0-*version*.sh.REL.tar • GeoDB：Cisco_GEODB_Update-*date-build*.sh.REL.tar シスコは、署名なしの更新を必要とするバージョンのサポートが終了するまで、署名付きと署名なしの両方の更新を提供します。署名付きの（.tar）パッケージは解凍しないでください。古い FMC または ASA FirePOWER デバイスに署名付きの更新を誤ってアップロードした場合は、手動で削除する必要があります。パッケージを残しておくと、ディスク領域が占有されるため、今後のアップグレードで問題が発生する可能性もあります。

機能	最小の Management Center	最小の Threat Defense	詳細
VDB の更新前に、Snort の再起動について FMC から警告されます。	6.2.3	いずれか	脆弱性データベース（VDB）の更新で Snort プロセスが再起動することが、FMCから警告されるようになりました。これにより、トラフィック インスペクションが中断され、管理対象デバイスによるトラフィックの処理方法によっては、トラフィックフローが中断される可能性があります。メンテナンス期間中など、都合の良い期間までインストールをキャンセルすることができます。 次のようなときに警告が表示される可能性があります。 • VDB をダウンロードして手動でインストールした後。 • スケジュールされたタスクを作成して VDB をインストールする場合。 • たとえば、以前にスケジュールされたタスクの実行中に、またはソフトウェアアップグレードの一部として、VDBがバックグラウンドでインストールされる場合。
廃止：地理位置情報の詳細	6.2.3	いずれか（Any）	ルーティング可能なIPアドレスに関連付けられたコンテキストデータを含む地理位置情報IPパッケージは提供されなくなりました。この措置によりディスク容量が節約されますが、地理位置情報ルールやトラフィック処理には影響しません。コンテキストデータはすべて古くなっており、最新のバージョンにアップグレードするとIPパッケージが削除されます。IPパッケージをダウンロードしたり、コンテキストデータを表示したりするオプションは効果がなく、以降のバージョンでは削除されます。

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。