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。

重要 Management Center、または Threat Defense ソフトウェアやシャーシをアップグレードするには、*Management Center* が現在実行しているバージョンのアップグレードガイド：http://www.cisco.com/go/ftd-fmc-upgradehttp://www.cisco.com/go/ftd-fmc-upgrade-74を参照してください。

管理対象デバイスをアップグレードするには、クラウド提供型 Firewall 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。

システムアップデートについて

Management Center を使用して、FMC 自体と FMC が管理するデバイスのシステムソフトウェアをアップグレードします。アドバンスドサービスを提供するさまざまなデータベースとフィードを更新することもできます。

Management Center がインターネットにアクセスできるときは、多くの場合、システムがシスコから直接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。その他の更新は、自分でスケジュールする必要があります。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*: アップグレードと更新

コンポーネント	説明（Description）	詳細
システム ソフトウェア	メジャー ソフトウェア リリースには、新機能、機能、および拡張機能が含まれます。インフラストラクチャまたはアーキテクチャの変更が含まれる場合があります。 メンテナンスリリースには、一般的なバグとセキュリティ関連の修正が含まれています。動作の変更はまれであり、これらの修正に関連しています。 パッチは、緊急性の高い重要な修正に限定されたオンデマンド更新です。 ホットフィックスは、特定のお客様の問題に対処できます。	**直接ダウンロード**：パッチおよびメンテナンスリリースのみを選択します。通常は、リリースが手動でダウンロードできるようになってからしばらく時間がかかります。遅延の長さは、リリースの種類、リリースの選択、およびその他の要因によって異なります。オンデマンドダウンロードとスケジュールされたダウンロードの両方がサポートされています。 （注） バージョン 7.4.1 では、すべてのリリース（ホットフィックスを除く）のオンデマンド直接ダウンロードのサポートが開始されました。ただし、メンテナンスリリースのスケジュールされたダウンロードのサポートは中止されました。 **スケジュールインストール**：パッチおよびメンテナンスリリースのみを、スケジュールされたタスクとしてインストールします。 **アンインストール**：パッチのみ。 **復元**：Threat Defense のメジャーリリースおよびメンテナンスリリースのみ。Management Center または従来型デバイスでは、復元機能はサポートされていません。 **再イメージ化**：メジャーリリースおよびメンテナンスリリースのみ。 **参照先**： Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
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。	**直接ダウンロード**：あり。 **スケジュール**：あり（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 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 （4 ページ）

コンポーネント	説明（Description）	詳細
位置情報データベース（GeoDB）	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アドレスに関連付けられている地理および接続関連のデータのデータベースです。	**直接ダウンロード**：あり。 **スケジュール**：あり（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（7 ページ）
侵入ルール（SRU/LSP）	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。	**直接ダウンロード**：あり。 **スケジュール**：あり（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 （9 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。	**直接ダウンロード**：あり。 **スケジュール**：あり（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。	**直接ダウンロード**：あり。 **スケジュール**：あり（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

システムアップデートの要件と前提条件

モデルのサポート

任意

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

システムアップデートの注意事項と制約事項

更新する前に

展開のいずれかのコンポーネント（侵入ルール、VDB、GeoDB 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ください。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

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。

重要 スケジュールされた更新が意図したとおりに確実に実行されることの確認を強くお勧めします。

帯域幅のガイドライン

システムソフトウェアをアップグレードしたり準備状況チェックを実行するには、アップグレードパッケージがアプライアンス上に存在する必要があります。アップグレードパッケージには、さまざまなサイズがあります。管理対象デバイスに大容量のデータを転送するための帯域幅があることを確認します。『Guidelines for Downloading Data from the Firepower Management Center to Managed Devices』（トラブルシューティング テクニカルノーツ）を参照してください。

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。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。

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

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 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

Management Center が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ない場合は、ユーザー自身で更新を入手します：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 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 ルール更新ページに移動します。

- バージョン 7.4.0：**システム**（⚙）>**[更新（Updates）]**>**[製品の更新（Product Updates）]**
- バージョン 7.4.1 以降：**システム**（⚙）>**[Content Updates]**>**[VDB Updates]**

ステップ 2 VDB を 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。

（注） バージョン 7.4.0 では、[更新のダウンロード（Download Updates）] をクリックすることでも、環境に適した最新のメンテナンスリリースおよび最新の重要パッチをすぐに取得できます。

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) 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）]**（?）>**[バージョン情報（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。**[ヘルプ（Help）]**（  ）> **[バージョン情報（About）]** で現在のバージョンを確認できます。

システムには IP アドレスを国/大陸にマッピングする GeoDB カントリー コード パッケージが付属しています。また、コンテキストデータを含む IP パッケージも提供されます。これには、追加の場所詳細のほか、ISP、接続タイプ、プロキシタイプ、ドメイン名などの接続情報が含まれます。

- バージョン 7.4.0 ～ 7.4.1 では、システムが（オンデマンドでまたはスケジュールに従って）GeoDB の更新をダウンロードする際、デフォルトで両方のパッケージがダウンロードされます。コンテキストデータが重要でない場合は、IP パッケージを無効化および削除することでディスク容量を節約できます。
- バージョン 7.4.2 以降では、デフォルトで国コードパッケージのみがダウンロードされますが、コンテキストデータが重要であり、十分なディスク容量がある場合は、両方のパッケージをダウンロードするように設定できます。

GeoDB の更新は、以前のバージョンをオーバーライドします。Management Center により、管理対象デバイスが自動的に更新されるため、展開する必要はありません。GeoDB の更新に必要な時間は展開によって異なりますが、更新のサイズによっては最大 45 分かかる場合があります（たとえば、完全な IP パッケージをダウンロードして処理する場合など）。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。

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 （7 ページ）。

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。

始める前に

Management Center で シスコ サポートおよびダウンロード サイト にアクセスできることを確認します。

手順

ステップ 1 GeoDB 更新ページに移動します。

- バージョン 7.4.0：**システム**（⚙）>**[更新（Updates）]**>**[地理位置情報の更新（Geolocation Updates）]**
- バージョン 7.4.1 以降：**システム**（⚙）>**[Content Updates]**>**[Geolocation Updates]**

ステップ 2 [IPパッケージの設定（IP Package Configuration）] で、[IPパッケージのダウンロード（IP Package Download）] オプションを使用して、必要な国コードパッケージのみをダウンロードするか IP パッケージもダウンロードするかを指定します。

IP パッケージを使用しないと、ディスク容量を節約できますが、IP アドレスのコンテキスト地理位置情報データも削除されます。この設定を変更した場合は、[保存（Save）] をクリックします。

ステップ 3 [Recurring Geolocation Updates] で、[Enable Recurring Weekly Updates] をオンにします。。

ステップ 4 [開始時刻の更新（Update Start Time）] を指定します。

ステップ 5 [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

Management Center が シスコ サポートおよびダウンロード サイト にアクセスできない場合は、ユーザー自身で更新を入手します：「Software Download」。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 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。国コードパッケージと、オプションで、IP パッケージをダウンロードします。

手順

ステップ 1 GeoDB 更新ページに移動します。

- バージョン 7.4.0：**システム**（⚙）>**[更新（Updates）]**>**[地理位置情報の更新（Geolocation Updates）]**

- バージョン 7.4.1 以降：**システム**（⚙） > **[Content Updates]** > **[Geolocation Updates]**

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 [IPパッケージの設定（IP Package Configuration）] で、[IPパッケージのダウンロード（IP Package Download）] オプションを使用して、国コードパッケージのみを使用するかIPパッケージも使用するかを指定します。

IP パッケージを使用しないと、ディスク容量を節約できますが、IP アドレスのコンテキスト地理位置データも削除されます。GeoDB パッケージを手動でアップロードする場合でも、IP パッケージのデータが必要ないときは、このオプションを無効にする必要があります。これは、オプションを無効にすると、既存の IP パッケージまたは古い IP パッケージが削除されるためです。

この設定を変更した場合は、[保存（Save）] をクリックします。

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。

ステップ 5 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）]**（❓） > **[バージョン情報（About）]** の両方に現在のバージョンが表示されます。

ステップ 6 （任意）更新を手動でアップロードする場合は、IPパッケージに対してこの手順を繰り返します。

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。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

[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 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（Red Status）] （⛔） 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。

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 （12 ページ）。

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。
- Management Center で シスコ サポートおよびダウンロード サイト にアクセスできることを確認します。

手順

ステップ 1 ルール更新ページに移動します。

- バージョン 7.4.0：**システム**（⚙） > **[更新（Updates）]** > **[ルールの更新（Rule Updates）]**
- バージョン 7.4.1 以降：**システム**（⚙） > **[Content Updates]** > **[Rule Updates]**

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。

- Management Center が シスコ サポートおよびダウンロード サイト にアクセスできない場合は、ユーザー自身で更新を入手します：「Software Download」。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 Management Center に同じ SRU または LSP 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 ルール更新ページに移動します。

- バージョン 7.4.0：**システム**（⚙）> **[更新（Updates）]** > **[ルールの更新（Rule Updates）]**
- バージョン 7.4.1 以降：**システム**（⚙）> **[Content Updates]** > **[Rule Updates]**

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）]**（?）> **[バージョン情報（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。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

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（15 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 ルール更新ページに移動します。

- バージョン 7.4.0：**システム**（⚙）> **[更新（Updates）]** > **[ルールの更新（Rule Updates）]**
- バージョン 7.4.1 以降：**システム**（⚙）> **[Content Updates]** > **[Rule Updates]**
- 任意のバージョン：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、[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 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 （17 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 ルール更新ページに移動します。

- バージョン 7.4.0：**システム**（⚙）> **[更新（Updates）]** > **[ルールの更新（Rule Updates）]**
- バージョン 7.4.1 以降：**システム**（⚙）> **[Content Updates]** > **[Rule Updates]**

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。 • [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） • [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） • [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） • [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） • [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） • [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） • [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） • [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） • [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）

フィールド	説明
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。
詳細	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、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）。
名前	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。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。
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。
Time	インポートが開始された日時。
タイプ	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。 • [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） • [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）
カウント（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

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。

- ソフトウェア アップグレード ガイド：https://cisco.com/go/ftd-fmc-upgrade
- VDB の手動更新 （5 ページ）
- 侵入ルールの手動更新 （12 ページ）
- 地理位置情報データベース（GeoDB）の手動更新 （8 ページ）

システムアップデートの履歴

表 *3 :* バージョン *7.4.1* の機能

機能	最小 Management Center	最小 Threat Defense	詳細
Threat Defense のアップグレード			
FXOS アップグレードに含まれるファームウェアのアップグレード。	任意（Any）	任意（Any）	**シャーシ/FXOS アップグレードの影響。ファームウェアのアップグレードにより、余分な再起動が発生します。** Firepower 4100/9300 の場合、バージョン 2.14.1 への FXOS アップグレードにファームウェアのアップグレードが含まれるようになりました。デバイス上のいずれかのファームウェア コンポーネントが FXOS バンドルに含まれているコンポーネントよりも古い場合、FXOS アップグレードによってファームウェアも更新されます。ファームウェアがアップグレードされると、デバイスは 2 回リブートします。1 回は FXOS 用、1 回はファームウェア用です。 ソフトウェアおよびオペレーティングシステムのアップグレードと同様に、ファームウェアのアップグレード中に設定変更を行ったり、展開したりしないでください。システムが非アクティブに見えても、ファームウェアのアップグレード中は手動で再起動またはシャットダウンしないでください。 参照：Cisco Firepower 4100/9300 FXOS ファームウェア アップグレード ガイド

機能	最小 Management Center	最小 Threat Defense	詳細
マルチインスタンスモードでの Secure Firewall 3100 のシャーシのアップグレード	7.4.1	7.4.1	マルチインスタンスモードの Cisco Secure Firewall 3100 では、コンテナインスタンスのアップグレード（*Threat Defense* のアップグレード）とは別に、オペレーティングシステムとファームウェアがアップグレードの対象（シャーシのアップグレード）になります。 新規/変更された画面： • シャーシのアップグレード：**[デバイス（Devices）]** > **[シャーシのアップグレード（Chassis Upgrade）]** • Threat Defense のアップグレード：**[デバイス（Devices）]** > **[Threat Defenseのアップグレード（Threat Defense Upgrade）]** 参照： Management Center 用 Cisco Secure Firewall Threat Defense アップグレードガイド
Management Center のアップグレード			
Management Center のアップグレード後に設定変更レポートを自動的に生成します。	任意（Any）	任意（Any）	Management Center のメジャーおよびメンテナンスアップグレード後に、設定変更に関するレポートを自動的に生成できます。このレポートは、展開しようとしている変更を理解するのに役立ちます。レポートが生成されたら、メッセージセンターの [タスク（Tasks）] タブからレポートをダウンロードできます。 その他のバージョンの制限：バージョン 7.4.1 以降の Management Center のアップグレードでのみサポートされます。バージョン 7.4.1 以前のバージョンへのアップグレードはサポートされていません。 新規/変更された画面：**システム（⚙）** > **[設定（Configuration）]** > **[設定のアップグレード（Upgrade Configuration）]** > **[アップグレード後のレポートの有効化（Enable Post-Upgrade Report）]**

表 *4* : バージョン *7.4.0* の機能

機能	最小 Management Center	最小 Threat Defense	詳細
Management Center のアップグレード：廃止された機能			

機能	最小 Management Center	最小 Threat Defense	詳細
一時的に廃止された機能。	7.4.0	機能に依存	バージョン 7.2.6 以降を実行している場合、バージョン 7.4.0 にアップグレードすると、次のアップグレード関連機能が削除されます。 • アップグレードの開始ページとパッケージ管理が改善されました。 • Threat Defense のアップグレードウィザードからの復元の有効化。 • Threat Defense アップグレードウィザードから詳細なアップグレードステータスを表示します。 • 推奨リリースの通知。 • Management Center の新しいアップグレードウィザード。 • 同期を一時停止することなく、高可用性管理センターでホットフィックスを利用できます。 • ソフトウェアアップグレードの直接ダウンロードに関するインターネットアクセス要件を更新しました。アップグレードの影響。 • 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。アップグレードの影響。

表 *5* : バージョン *7.3.0* の機能

機能	最小 Management Center	最小 Threat Defense	詳細
廃止された機能			

機能	最小 Management Center	最小 Threat Defense	詳細
一時的に廃止された機能。	任意	機能に依存	バージョン 7.2.6 以降を実行している場合、バージョン 7.3.x にアップグレードすると、次のアップグレード関連機能が削除されます。 • アップグレードの開始ページとパッケージ管理が改善されました。 • Threat Defense のアップグレードウィザードからの復元の有効化。 • Threat Defense アップグレードウィザードから詳細なアップグレードステータスを表示します。 • 推奨リリースの通知。 • Management Center の新しいアップグレードウィザード。 • 同期を一時停止することなく、高可用性管理センターでホットフィックスを利用できます。 • ソフトウェアアップグレードの直接ダウンロードに関するインターネットアクセス要件を更新しました。 • 国コードの地理位置情報パッケージのみをダウンロードします。 • 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。 アップグレードはサポートされていますが、現在のバージョンに含まれている重要な修正および機能拡張が削除されます。バージョン 7.4.1 以降に直接アップグレードすることをお勧めします。
Threat Defense のアップグレード			
シスコからアップグレードパッケージを選択して、Management Center に直接ダウンロードします。	7.3.0	いずれか	Management Center に直接ダウンロードする Threat Defense アップグレードパッケージを選択できるようになりました。 > **[更新（Updates）]** > **[製品の更新（Product Updates）]** の新しい [の更新のダウンロード（Download Threat Defense Updates）] サブタブを使用します。 その他のバージョンの制限：バージョン 7.2.6/7.4.1 では、この機能は改善されたパッケージ管理システムに置き換えられています。 参照：Management Center を含むアップグレードパッケージのダウンロード

機能	最小 Management Center	最小 Threat Defense	詳細
Threat Defense のウィザードを使用してアップグレードパッケージを Management Center にアップロードします。	7.3.0	いずれか	ウィザードを使用して、脅威防御アップグレードパッケージをアップロードしたり、場所を指定したりできるようになりました。以前は（バージョンに応じて）、**システム**（⚙）>**[更新（Updates）]**または**システム**（⚙）>**[製品のアップグレード（Product Upgrades）]**を使用していました。 その他のバージョンの制限：バージョン 7.2.6/7.4.1 では、この機能は改善されたパッケージ管理システムに置き換えられています。 参照：脅威防御のアップグレード
Threat Defense のアップグレード完了後の Snort 3 への自動アップグレードはオプションではなくなりました。	7.3.0	いずれか	**アップグレードの影響。** Threat Defence をバージョン 7.3 以降にアップグレードする場合、[Snort 2からSnort 3にアップグレードする（Upgrade Snort 2 to Snort 3）] オプションは無効化できなくなりました。 ソフトウェアのアップグレード後、設定を展開すると、対象となるすべてのデバイスが Snort 2 から Snort 3 にアップグレードされます。個々のデバイスを元に戻すことはできますが、Snort 2 は将来のリリースで非推奨になるため、今すぐ使用を停止することを強く推奨します。 カスタム侵入ポリシーやネットワーク分析ポリシーを使用しているためにデバイスが自動アップグレード対象外になる場合は、検出とパフォーマンスを向上させるために、手動で Snort 3 にアップグレードすることを強く推奨します。移行のサポートについては、お使いのバージョンの Cisco Secure Firewall Management Center Snort 3 Configuration Guide を参照してください。

機能	最小 Management Center	最小 Threat Defense	詳細
Cisco Secure Firewall 3100 の統合アップグレードおよびインストールパッケージ。	7.3.0	7.3.0	

機能	最小 Management Center	最小 Threat Defense	詳細
			再イメージ化の影響。 バージョン 7.3 では、次のように、Secure Firewall 3100 の Threat Defense のインストールおよびアップグレードパッケージを組み合わせました。 • バージョン 7.1 ～ 7.2 インストールパッケージ：isco-ftd-fp3k.*version*.SPA • バージョン 7.1 ～ 7.2 アップグレードパッケージ：Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar • バージョン 7.3 以降の統合パッケージ：Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar Threat Defense は問題なくアップグレードできますが、古い Threat Defense および ASA バージョンから Threat Defense バージョン 7.3 以上に直接再イメージ化することはできません。これは、新しいイメージタイプに必要な ROMMON アップデートが原因です。これらの古いバージョンから再イメージ化するには、古い ROMMON でサポートされているだけでなく新しい ROMMON への更新も行う、ASA 9.19 以上を「通過」する必要があります。個別の ROMMON アップデータはありません。 Threat Defense バージョン 7.3 以上にするには、次のオプションがあります。 • Threat Defense バージョン 7.1 または 7.2 からのアップグレード — 通常のアップグレードプロセスを使用します。 該当するアップグレードガイドを参照してください。 • Threat Defense バージョン 7.1 または 7.2 からの再イメージ化 — 最初に ASA 9.19 以上に再イメージ化してから、Threat Defense バージョン 7.3 以上に再イメージ化します。 『Cisco Secure Firewall ASA および Secure Firewall Threat Defense 再イメージ化ガイド』の「Threat Defense→ASA: Firepower 1000, 2100; Secure Firewall 3100」、次に「ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100」を参照してください。 • ASA 9.17 または 9.18 からの再イメージ化 — 最初に ASA 9.19 以上にアップグレードしてから、Threat Defense バージョン 7.3 以上に再イメージ化します。 『Cisco Secure Firewall ASA アップグレードガイド』を参照し、次に『Cisco Secure Firewall ASA および Secure Firewall Threat Defense

機能	最小 Management Center	最小 Threat Defense	詳細
			再イメージ化ガイド』の「ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100」を参照してください。 • Threat Defense バージョン 7.3 以上からの再イメージ化 — 通常の再イメージ化プロセスを使用します。 『Cisco FXOS トラブルシューティング ガイド（Firepower Threat Defense を実行している Firepower 1000/2100 および Cisco Secure Firewall 3100/4200 向け）』の「Reimage the System with a New Software Version」を参照してください。
コンテンツの更新（Content Updates）			
自動 VDB ダウンロード。	7.3.0	いずれか	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 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るようになりました。 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**（⚙）> **[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。

表 *6 :* バージョン *7.2.0* の機能

機能	詳細
Threat Defense のアップグレード	
デバイス間のアップグレードパッケージのコピー（「ピアツーピア同期」）。	Management Center や内部 Web サーバーから各デバイスにアップグレードパッケージをコピーする代わりに、Threat Defense CLI を使用してデバイス間でアップグレード パッケージをコピーできます（「ピアツーピア同期」）。この安全で信頼性の高いリソース共有は、管理ネットワークを経由しますが、Management Center には依存しません。各デバイスは、5 つのパッケージの同時転送に対応できます。 この機能は、同じバージョン 7.2.x ー 7.4.x のスタンドアロン Management Center によって管理されるバージョン 7.2 以降のスタンドアロンデバイスでサポートされています。次の場合はサポートされていません。 • コンテナインスタンス。 • デバイスの高可用性ペアとクラスタ。これらのデバイスは通常の同期プロセスの一部として、相互にパッケージを取得します。アップグレードパッケージを 1 つのグループメンバーにコピーすると、自動的にすべてのグループメンバーと同期されます。 • 高可用性 Management Center によって管理されるデバイス。 • クラウド提供型 Firewall Management Center によって管理されるが、分析モードでオンプレミス Management Center に追加されたデバイス。 • 異なるドメインのデバイス、または NAT ゲートウェイによって分離されたデバイス。 • Management Center のバージョンに関係なく、バージョン 7.1 以前からアップグレードするデバイス。 新規/変更された CLI コマンド：**configure p2psync enable**、**configure p2psync disable**、**show peers**、**show peer details**、**sync-from-peer**、**show p2p-sync-status**

機能	詳細
Threat Defense のアップグレード完了後の Snort 3 への自動アップグレード。	バージョン 7.2 以降の Management Center を使用して Threat Defense をバージョン 7.2 以降にアップグレードする場合、**Snort 2 から Snort 3 へのアップグレード**を実行するかどうかを選択できるようになりました。 ソフトウェアのアップグレード後、設定を展開すると、対象のデバイスが Snort 2 から Snort 3 にアップグレードされます。カスタム侵入ポリシーやネットワーク分析ポリシーを使用しているためにデバイスがアップグレード対象外になる場合は、検出とパフォーマンスを向上させるために、手動で Snort 3 にアップグレードすることを強く推奨します。ヘルプについては、ご使用のバージョンの Cisco Secure Firewall Management Center Snort 3 Configuration Guide を参照してください。 バージョンの制限：Threat Defense のバージョン 7.0.x または 7.1.x へのアップグレードはサポートされていません。
単一ノードクラスタのアップグレード。	デバイスのアップグレードページ（[デバイス（Devices）] > [デバイスのアップグレード（Device Upgrade）]）を使用して、アクティブノードが 1 つだけのクラスタをアップグレードできるようになりました。非アクティブ化されたノードもアップグレードされます。以前は、このタイプのアップグレードは失敗していました。この機能は、システムの更新ページ（**システム**（⚙）**[更新（Updates）]**）ではサポートされていません。 この場合、ヒットレスアップグレードもサポートされません。トラフィックフローと検査の中断は、スタンドアロンデバイスと同様に、アクティブユニットのインターフェイス設定に依存します。 サポートされるプラットフォーム：Firepower 4100/9300、Secure Firewall 3100
CLI からの Threat Defense アップグレードの復元。	Management Center とデバイス間の通信が中断された場合、デバイスの CLI から Threat Defense のアップグレードを元に戻すことができるようになりました。高可用性や拡張性の展開では、すべてのユニットを同時に復元すると、復元が成功する可能性が高くなります。CLI を使用して復元する場合は、すべてのユニットでセッションを開き、それぞれで復元が可能であることを確認してから、プロセスを同時に開始します。 **注意** CLI から復元すると、アップグレード後に行った変更によっては、デバイスと Management Center 間で設定が同期されないことがあります。これにより、後に通信と展開の問題が発生する可能性があります。 新規/変更された CLI コマンド：**upgrade revert**、**show upgrade revert-info**。
Management Center のアップグレード	

機能	詳細
Management Center のアップグレードでは、トラブルシューティング ファイルは自動的に生成されません。	時間とディスク容量を節約するために、管理センターのアップグレードプロセスでは、アップグレードの開始前にトラブルシューティング ファイルを自動的に生成しなくなりました。デバイスのアップグレードは影響を受けず、引き続きトラブルシューティング ファイルが生成される点に注意してください。 管理センターのトラブルシューティング ファイルを手動で生成するには、**システム**（⚙）>**[正常性（Health）]**>**[モニタ（Monitor）]** を選択し、左側のパネルで [Firewall Management Center] をクリックし、[View System & Troubleshoot Details]、[Generate Troubleshooting Files] を選択します。
コンテンツの更新（Content Updates）	
GeoDB を 2 つのパッケージに分割。	2022 年 5 月、バージョン 7.2 リリースの直前に、GeoDB が 2 つのパッケージに分割されました。IP アドレスを国/大陸にマッピングする国コードパッケージと、ルーティング可能な IP アドレスに関連付けられた追加のコンテキストデータを含む IP パッケージです。IP パッケージのコンテキストデータには、追加のロケーションの詳細に加えて、ISP、接続タイプ、プロキシタイプ、ドメイン名などの接続情報を含めることができます。 バージョン 7.2.0 から 7.2.5 までの Management Center にインターネットアクセスがあり、定期的な更新を有効にしている場合、または シスコ サポートおよびダウンロード サイト から 1 回限りの更新を手動で開始した場合、両方のパッケージが自動的に取得されます。バージョン 7.2.6 以降または 7.4.0 以降では、システムに IP パッケージを取得させるかどうかを設定できます。 エアギャップ展開などで更新を手動でダウンロードする場合、パッケージを個別にインポートする必要があります。 • 国コードパッケージ：Cisco_GEODB_Update-*date-build*.sh.REL.tar • IP パッケージ：Cisco_IP_GEODB_Update-*date-build*.sh.REL.tar **[ヘルプ（Help）]**（?）>**[バージョン情報（About）]** には、システムで現在使用されているパッケージのバージョンが一覧表示されます。

表 *7*：バージョン *7.1.0* の機能

機能	詳細
Threat Defense のアップグレード	

機能	詳細
正常なデバイスアップグレードを元に戻します。	メジャーおよびメンテナンスアップグレードを FTD に戻すことができるようになりました。復元すると、ソフトウェアは、最後のアップグレードの直前の状態に戻ります（スナップショットとも呼ばれます）。パッチのインストール後にアップグレードを元に戻すと、パッチだけでなく、メジャーアップグレードやメンテナンスアップグレードも元に戻されます。 **重要** 元に戻す必要がある可能性があると思われる場合は、**システム**（⚙）> **[更新（Updates）]** ページを使用して FTD をアップグレードする必要があります。[システムの更新（System Updates）] ページは、[アップグレード後の復元を有効にする（Enable revert after successful upgrade）] オプションを有効にできる唯一の場所です。このオプションでは、アップグレードの開始時に復元スナップショットを保存するようにシステムが設定されます。これは、[デバイス（Devices）]>[デバイスのアップグレード（Device Upgrade）] ページでウィザードを使用する通常の推奨とは対照的です。 この機能は、コンテナインスタンスではサポートされません。 必要最低限の FTD：7.1
クラスタ化された高可用性デバイスのアップグレードワークフローの改善。	クラスタ化された高可用性デバイスのアップグレードワークフローが次のように改善されました。 • アップグレードウィザードは、個々のデバイスとしてではなく、グループとして、クラスタ化された高可用性ユニットを正しく表示するようになりました。システムは、発生する可能性のあるグループ関連の問題を特定し、報告し、事前に修正を要求できます。たとえば、Firepower Chassis Manager で非同期の変更を行った場合は、Firepower 4100/9300 のクラスタをアップグレードできません。 • アップグレードパッケージをクラスタおよび高可用性ペアにコピーする速度と効率が向上しました。以前は、FMC はパッケージを各グループメンバーに順番にコピーしていました。これで、グループメンバーは通常の同期プロセスの一部として、相互にパッケージを取得できるようになりました。 • クラスタ内のデータユニットのアップグレード順序を指定できるようになりました。コントロールユニットは常に最後にアップグレードされます。

表 *8* : バージョン *7.0.0* の機能

機能	詳細
Threat Defense のアップグレード	

機能	詳細
FTDのアップグレードパフォーマンスとステータスレポートの改善。	FTD のアップグレードがより簡単かつ確実に、より少ないディスク容量で実行できるようになりました。メッセージセンターの新しい [アップグレード（Upgrades）] タブでは、アップグレードステータスとエラーレポートがさらに強化されています。

機能	詳細
FTDデバイスのわかりやすいアップグレードワークフロー。	FMC の新しいデバイス アップグレード ページ（[デバイス（Devices）] > [デバイスアップグレード（Device Upgrade）]）には、バージョン 6.4 以降の FTD デバイスをアップグレードするためのわかりやすいウィザードがあります。アップグレードするデバイスの選択、アップグレードパッケージのデバイスへのコピー、互換性と準備状況の確認など、アップグレード前の重要な段階を順を追って説明します。 開始するには、[デバイス管理（Device Management）] ページ（[デバイス（Devices）] > [デバイス管理（Device Management）] > [アクションの選択（Select Action）]）で新しい [Firepower ソフトウェアのアップグレード（Upgrade Firepower Software）] アクションを使用します。 続行すると、選択したデバイスに関する基本情報と、現在のアップグレード関連のステータスが表示されます。表示内容には、アップグレードできない理由が含まれます。あるデバイスがウィザードの 1 つの段階に「合格」しない場合、そのデバイスは次の段階には表示されません。 ウィザードから移動しても、進行状況は保持されます。ただし、管理者アクセス権を持つ他のユーザーはウィザードをリセット、変更、または続行できます。 （注） FTD のアップグレードパッケージの場所をアップロードまたは指定するには、引き続き **システム**（⚙）> **[更新（Updates）]**を使用する必要があります。また、[システム更新（System Updates）]ページを使用して、FMC 自体、およびすべての非 FTD 管理対象デバイスをアップグレードする必要があります。 （注） バージョン 7.0 では、ウィザードにクラスタまたは高可用性ペアのデバイスが正しく表示されません。これらのデバイスは 1 つのユニットとして選択してアップグレードする必要がありますが、ウィザードにはスタンドアロンデバイスとして表示されます。デバイスのステータスとアップグレードの準備状況は、個別に評価および報告されます。つまり、1 つのユニットが「合格」して次の段階に進んでいるように見えても、他のユニットは合格していない可能性があります。ただし、それらのデバイスはグループ化されたままです。1 つのユニットで準備状況チェックを実行すると、すべてのユニットで実行されます。1 つユニットでアップグレードを開始すると、すべてのユニットで開始されます。 時間がかかるアップグレードの失敗を回避するには、[次へ（Next）] をクリックする前に、すべてのグループメンバーがウィザードの次のステップに進む準備ができていることを手動で確認します。

機能	詳細
多くのFTDデバイスを一度にアップグレードします。	FTD アップグレードウィザードでは、次の制限が解除されます。 • デバイスの同時アップグレード。 一度にアップグレードできるデバイスの数は、同時アップグレードを管理するシステムの機能ではなく、管理ネットワークの帯域幅によって制限されます。以前は、一度に 5 台を上回るデバイスをアップグレードしないことを推奨していました。 **重要** この改善は、FTD バージョン 6.7 以降へのアップグレードでのみ確認できます。デバイスを古いFTDリリースにアップグレードする場合は、新しいアップグレードウィザードを使用している場合でも、一度に 5 台のデバイスに制限することをお勧めします。 • デバイスモデルによるアップグレードのグループ化。 システムが適切なアップグレードパッケージにアクセスできる限り、すべての FTD モデルのアップグレードを同時にキューに入れて呼び出すことができます。 以前は、アップグレードパッケージを選択し、そのパッケージを使用してアップグレードするデバイスを選択していました。つまり、アップグレードパッケージを共有している場合にのみ、複数のデバイスを同時にアップグレードできました。たとえば、2 台の Firepower 2100 シリーズデバイスは同時にアップグレードできますが、Firepower 2100 シリーズと Firepower 1000 シリーズはアップグレードできません。

表 *9* : バージョン *6.7.0* の機能

機能	詳細
Threat Defense のアップグレード	
アップグレードでディスク容量を節約するためにPCAPファイルが削除される。	アップグレードにより、ローカルに保存された PCAP ファイルが削除されるようになりました。アップグレードするには、十分な空きディスク容量が必要です。これがない場合、アップグレードは失敗します。

機能	詳細
FTDアップグレードステータス レポートとキャンセル/再試行オプションの改善。	[デバイス管理（Device Management）] ページで、進行中の FTD デバイスアップグレードと準備状況チェックのステータス、およびアップグレードの成功/失敗の 7 日間の履歴を確認できるようになりました。メッセージセンターでは、拡張ステータスとエラーメッセージも提供されます。 デバイス管理とメッセージセンターの両方からワンクリックでアクセスできる新しい [Upgrade Status] ポップアップに、残りのパーセンテージ/時間、特定のアップグレード段階、成功/失敗データ、アップグレードログなどの詳細なアップグレード情報が表示されます。 また、このポップアップで、失敗したアップグレードまたは進行中のアップグレードを手動でキャンセル（[Cancel Upgrade]）することも、失敗したアップグレードを再試行（[Retry Upgrade]）することもできます。アップグレードをキャンセルすると、デバイスはアップグレード前の状態に戻ります。 （注） 失敗したアップグレードを手動でキャンセルまたは再試行できるようにするには、FMC を使用して FTD デバイスをアップグレードするときに表示される新しい自動キャンセルオプションを無効にする必要があります（[Automatically cancel on upgrade failure and roll back to the previous version]）。オプションを有効にすると、アップグレードが失敗した場合、デバイスは自動的にアップグレード前の状態に戻ります。 パッチの自動キャンセルはサポートされていません。HA またはクラスタ展開では、自動キャンセルは各デバイスに個別に適用されます。つまり、1 つのデバイスでアップグレードが失敗した場合、そのデバイスだけが元に戻ります。 新規/変更された画面： • FTD アップグレードパッケージの **システム**（⚙） > **[更新（Updates）]** > **[製品の更新（Product Updates）]** > **[使用可能な更新（Available Updates）]** > **[インストール（Install）]** アイコン • **[Devices]** > **[Device Management]** > **[Upgrade]** • **[Message Center] > [Tasks]** 新規/変更された CLI コマンド：**show upgrade status detail**、**show upgrade status continuous**、**show upgrade status**、**upgrade cancel**、**upgrade retry**
コンテンツの更新（Content Updates）	

機能	詳細
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。	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**（⚙） > **[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。

表 *10 :* バージョン *6.6.0* の機能

機能	詳細
Threat Defense のアップグレード	
内部 Web サーバーから FTD アップグレードパッケージを取得します。	FTD デバイスは、FMC からではなく、独自の内部 Web サーバーからアップグレードパッケージを取得できるようになりました。これは、FMC とそのデバイスの間の帯域幅が制限されている場合に特に役立ちます。また、FMC 上の領域も節約できます。 （注） この機能は、バージョン 6.6+ を実行している FTD デバイスでのみサポートされています。バージョン 6.6 へのアップグレードではサポートされておらず、FMC または従来のデバイスでもサポートされていません。 新規/変更された画面：アップグレードパッケージをアップロードするページに、[ソフトウェアアップデートソースの指定（Specify software update source）] オプションを追加しました。
コンテンツの更新（Content Updates）	
初期セットアップ中の自動VDB更新。	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。

表 *11* : バージョン *6.5.0* の機能

機能	詳細
コンテンツの更新（Content Updates）	
ソフトウェアの自動ダウンロードとGeoDB の更新。	新規または再イメージ化されたFMC を設定すると、システムは自動的に次のスケジュールを設定します。 • FMC とその管理対象デバイスの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。 • GeoDB の週次更新。 タスクはUTC でスケジュールされるため、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、タスクは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タスクは、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。自動スケジュール設定を確認し、必要に応じて調整することをお勧めします。

表 *12* : バージョン *6.4.0* の機能

機能	詳細
Management Center のアップグレード	
アップグレードがスケジュールされたタスクを延期する。	Management Center のアップグレードプロセスによって、スケジュールされたタスクが延期されるようになりました。アップグレード中に開始するようにスケジュールされたタスクは、アップグレード後の再起動の 5 分後に開始されます。 （注） アップグレードを開始する前に、実行中のタスクが完了していることを確認する必要があります。アップグレードの開始時に実行中のタスクは停止し、失敗したタスクとなり、再開できません。 この機能は、サポートされているバージョンからのすべてのアップグレードでサポートされていることに注意してください。これには、バージョン6.4.0.10 以降のパッチ、バージョン 6.6.3 以降のメンテナンスリリース、およびバージョン 6.7.0 以降が含まれます。この機能は、サポートされていないバージョンからサポートされているバージョンへのアップグレードではサポートされていません。
コンテンツの更新（Content Updates）	

機能	詳細
署名済みのSRU、VDB、およびGeoDBの更新。	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。 シスコ サポートおよびダウンロードサイトから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。

表 *13 :* バージョン *6.2.3* の機能

機能	詳細
デバイスのアップグレード	
アップグレードの前に、アップグレードパッケージを管理対象デバイスにコピーします。	実際のアップグレードを実行する前に、FMC から管理対象デバイスにアップグレードパッケージをコピー（またはプッシュ）できるようになりました。帯域幅の使用量が少ない時間帯やアップグレードのメンテナンス期間外でプッシュできるため、この機能は便利です。 高可用性デバイス、クラスタデバイス、またはスタック構成デバイスにプッシュすると、アップグレードパッケージは最初にアクティブ/コントロール/プライマリに送信され、次にスタンバイ/データ/セカンダリに送信されます。 新規/変更された画面：**システム**（⚙）>**[更新（Updates）]**
コンテンツの更新（Content Updates）	

機能	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。	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。

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。