システム ソフトウェア更新

ここでは、Firepower システム ソフトウェアを更新する方法について説明します。

- システム ソフトウェア アップデートの概要，1 ページ
- Firepower システムのソフトウェア アップデート，3 ページ
- 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，14 ページ
- 脆弱性データベースの更新，17 ページ
- 侵入ルールの更新，19 ページ
- 地理位置情報データベースの更新，31 ページ

システム ソフトウェア アップデートの概要

Cisco は、以下を含む各種のアップデートを電子的に配信します。

- 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 アップデート
- 侵入ルールの更新
- 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

ほとんどのタイプの更新では、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、Firepower 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。Firepower システムのいずれかの部分（VDB、GeoDB、侵入ルールなど）を更新する前に、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 テキストを読んでおく**必要があります**。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。

表 *1*：*Firepower* システム アップデートのタイプ

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	タブ	ドメイン
Firepower システムに対するパッチ	パッチには、限定された範囲の修正が含まれています（また通常は、6.0.0.1 のようにバージョン番号の 4 桁目が変更されます）。	Yes	Yes	製品の更新	グローバルのみ
Firepower システムの機能の更新	機能の更新はパッチよりも包括的であり、通常は新しい機能が含まれています（また通常は、6.0.1 のようにバージョン番号の 3 桁目が変更されます）。	Yes	Yes	製品の更新	グローバルのみ
Firepower システムに対するメジャーな更新（メジャーおよびマイナー バージョンのリリース）	メジャーな更新はアップグレードと呼ばれることもあります。この更新には新しい機能が含まれており、製品に対する大規模な変更が含まれることがあります（通常は、6.1 または 6.2 のようにバージョン番号の最初の桁または 2 桁目が変更されます）。メジャーな更新では、Cisco 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。	No	No	製品の更新	グローバルのみ
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。	Yes	No	製品の更新	グローバルのみ

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	タブ	ドメイン
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。	Yes	No	ルールの更新	• 侵入ルールの更新：グローバルのみ • ローカル ルールのインポート：任意
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。	Yes	No	地理位置情報の更新	グローバルのみ

ただし、Firepower システムに対するパッチや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、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ません。自分のアプライアンスを、Firepower システムの新しいメジャー バージョンに更新した場合、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 システムのソフトウェア アップデート

Firepower システムの展開を更新するには、いくつかの基本的な手順があります。最初にリリース ノートを参照し、必要な更新前のタスクをすべて完了することで更新の準備を整えておく**必要があります**。その後に更新を開始することができます。まず Firepower Management Center を更新し、

次にこれが管理するデバイスを更新します。更新が完了し、更新が正常に終了したことを確認するまで、更新の進捗状況を監視する必要があります。最後に、更新後の必要な手順を完了させます。

Firepower システムのソフトウェア アップデートの準備

更新を開始する前に、リリース ノートをよく読んで理解する必要があります。リリース ノートはサポートサイトからダウンロードすることができます。リリースノートには、サポートされているプラットフォーム、新しい機能、既知および解決済みの問題、製品の互換性について記載されています。また、リリース ノートには前提条件、警告、および特別なのインストールおよびアンインストールの手順についての重要な情報が含まれています。

Firepower システムのバージョンの要件

アプライアンス（ソフトウェアベースのデバイスを含む）が、Firepower システムの正しいバージョンを実行していることを確認する必要があります。リリース ノートには必要なバージョンが示されています。古いバージョンを実行している場合は、サポート サイトから更新を取得することができます。

オペレーティング システム要件

ソフトウェアベースのデバイスをインストールしたコンピュータが、オペレーティング システムの正しいバージョンを実行していることを確認します。リリース ノートには必要なバージョンが示されています。NGIPSv デバイスでサポートされるオペレーティング システムの詳細については、『*Firepower System Virtual Installation Guide*』を参照してください。

時間とディスク スペース要件

十分な空きディスク領域があることを確認し、更新のために十分な時間を確保しておく必要があります。管理対象デバイスを更新する場合は、Firepower Management Center 上に追加のディスク領域が必要になります。リリース ノートには、ディスク領域と時間の要件が示されています。

設定とイベント バックアップのガイドライン

更新を開始する前に、アプライアンスに残っているバックアップを外部の場所にコピーしてから、アプライアンス上のバックアップを削除することを強く推奨します。また、現在のイベント データと設定データを外部の場所にバックアップする必要があります。Firepower Management Center は、以前の更新でローカルに保存されたバックアップを消去します。イベント データは更新プロセスの一部としてバックアップ**されません**。

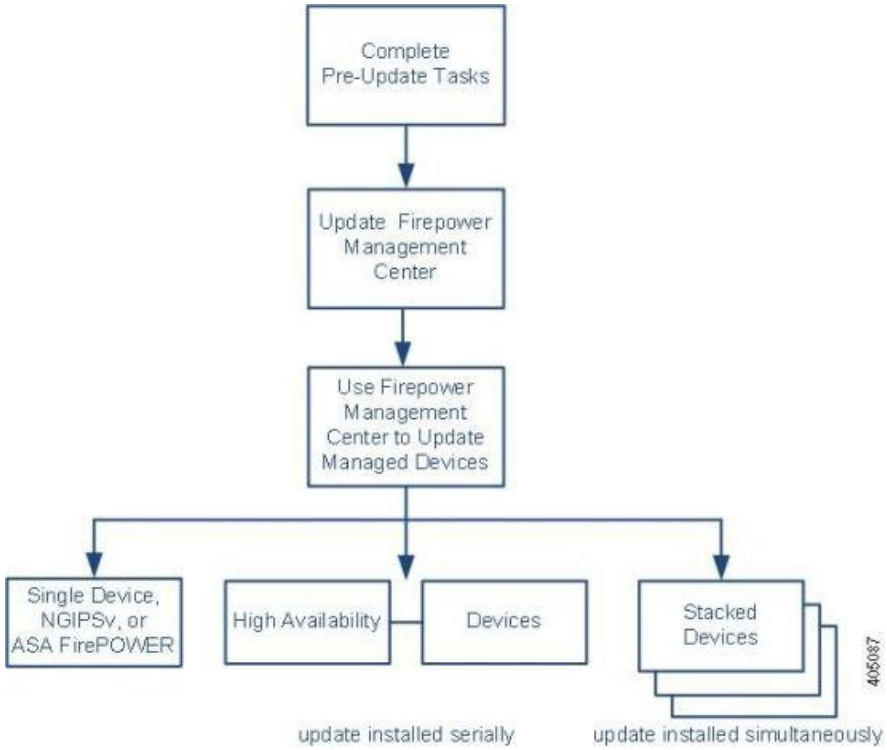
Firepower Management Center を使用して、そのイベント データと設定データ、および管理しているデバイスのイベント データと設定データをバックアップできます。

更新を実行するタイミング

注意 更新プロセスはトラフィックの調査、トラフィック フロー、およびリンク ステートに影響を与えることがあること、および更新を行っている間は Data Correlator が無効になっていることにより、保守を行っている間、または中断が展開に及ぼす影響が最も少ない時間に更新を行うことをお勧めします。

Firepower システムのソフトウェア アップデート プロセス

次のフローチャートは、Firepower システムの更新プロセスを示しています。



更新の順序

使用している Firepower Management Center を更新してから、それらが管理するデバイスを更新する**必要があります**。

Firepower Management Centerを使用した更新の実行

Firepower Management Center の Web インターフェイスを使用して、アプライアンス自体とその管理対象デバイスを更新します。

ヒント パッチおよび機能の更新では、自動更新機能を利用することができます。

管理対象デバイスの更新は、2段階のプロセスです。まず、サポートサイトから更新をダウンロードして、管理元の Firepower Management Center にアップロードします（http://www.cisco.com/cisco/web/support/index.html）。

次に、ソフトウェアをインストールします。

注意 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 ステートは、デバイスがどのように設定および展開されているか、更新がどのコンポーネントに影響を及ぼすか、更新によってデバイスがリブートされるかどうかよって、更新中に影響を受けることがあります。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具体的な情報は、対象の更新のリリース ノートを参照してください。

ハイ アベイラビリティ ペアの 7000 および 8000 シリーズ デバイスの更新

ハイ アベイラビリティ ペアの 7000 または 8000 シリーズ デバイスまたはデバイス スタック上で更新をインストールすると、システムは、複数のデバイスまたはスタック上で同時に更新を実行します。更新を開始すると、システムは最初にバックアップ デバイスまたはスタックに更新を適用し、必要なプロセスが再開され、デバイスまたはスタックがトラフィックを再処理するまでメンテナンス モードになります。システムは、アクティブなデバイスまたはスタックに更新を適用し、同じプロセスを行います。

ハイ アベイラビリティペアのスタック内のデバイスを更新するには、ハイ アベイラビリティ ペアのすべてのメンバー上で同時に、管理している Firepower Management Center から更新を実行する必要があります。デバイスから直接更新を実行することはできません。

スタック内の 8000 シリーズ デバイスの更新

スタック構成のデバイスで更新をインストールする場合、システムは更新を同時に実行します。各デバイスは、更新が完了すると通常の動作を再開します。次の点に注意してください。

- すべてのセカンダリ デバイスの更新が完了する前にプライマリ デバイスの更新が完了すると、すべてのデバイスで更新が完了するまでスタックは限定的な、バージョンが混在している状態で動作します。
- すべてのセカンダリ デバイスの更新が完了した後でプライマリ デバイスの更新が完了した場合は、プライマリ デバイスで更新が完了したときに、スタックは通常の動作を再開します。

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インストールまたはアンインストールすると、次の機能に影響を及ぼすことがあります。

- トラフィック インスペクション（アプリケーションおよびユーザの認識と制御、URL フィルタリング、セキュリティ インテリジェンス フィルタリング、侵入/ファイル/マルウェアのインスペクションと制御、接続のロギングなど）
- トラフィック フロー（スイッチング、ルーティング、NAT、VPN、関連機能など）
- リンク ステート

Data Correlator は、システムの更新中は動作しません。更新が完了すると再開します。

ネットワーク トラフィックの中断の方法と期間は、更新が影響を及ぼす Firepower システムのコンポーネント、デバイスがどのように設定および展開されているか、更新によりデバイスがリブートされるかどうか、によって異なります。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。

ヒント ハイ アベイラビリティ ペア内の 7000 または 8000 シリーズ デバイスを更新する場合、システムは、トラフィックの中断を回避するために、一度に 1 つずつ更新を実行します。

更新中の Web インターフェイスの使用

更新のタイプに関係なく、更新中のアプライアンスの Web インターフェイスを使用して、更新のモニタ以外のタスクを実行**しないで**ください。

メジャーな更新中にユーザがアプライアンスを使用しないようにし、メジャーな更新の進捗をユーザが簡単にモニタできるようにするために、アプライアンスの Web インターフェイスが合理化されています。メッセージ センターでマイナーな更新の進捗をモニタできます。マイナーな更新中に Web インターフェイスを使用することは禁止されていませんが、シスコでは推奨していません。

ヒント 管理対象デバイスの更新をモニタするには、Firepower Management Center でメッセージ センターを使用します。

マイナーな更新であっても、更新プロセス中は、更新しているアプライアンスの Web インターフェイスは使用できないか、またはアプライアンスでユーザがログアウトされることがあります。これは想定されている動作です。これが発生した場合は、再度ログインして、メッセージ センター（マイナー更新の場合）または [更新ステータス（Update Status）] ページ（メジャー更新の場合）を表示します。まだ更新が実行中の場合は、更新が完了するまで Web インターフェイスを使用**しないで**ください。更新中は、管理対象デバイスが 2 回リブートされることがありますが、これは予想される動作です。

注意 （Web インターフェイスに更新が失敗したことが示されている、メッセージ センターまたは [更新ステータス（Update Status）] ページに進捗が表示されないなど）更新で問題が発生した場合には、更新を再開**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。

更新後

リリース ノートに記載されている更新後のタスクをすべて完了し、展開が正常に実行されていることを確認する**必要があります**。

注意 Firepower Management Center の更新後、およびその管理対象デバイスの更新後に**再度**、設定を展開する必要があります。

また、次の作業を実行する必要があります。

- 更新が正常に終了したことを確認する
- 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
- 必要に応じて侵入ルール、VDB、および GeoDB を更新する
- リリース ノートの情報に基づいて、必要な設定変更を行う
- リリース ノートに記載されている、更新後の追加タスクを実行する

Firepower システム ソフトウェア アップデートに関する注意事項

更新のタイプ、および Firepower Management Center がインターネットへアクセスできるかどうかによって、Firepower Management Center の Firepower システム ソフトウェアを次のいずれかの方法で更新できます。

- Firepower Management Center がインターネットにアクセスできる場合は、サポート サイトから直接アップデートを取得します。このオプションは、メジャーな更新ではサポート**されていません**。
- サポート サイトからアップデートを手動でダウンロードして、Firepower Management Center へアップロードします。Firepower Management Center がインターネットへアクセスできない場合、またはメジャーな更新を実行している場合は、この方法を選択します。

（注） 上記のいずれかの方法を使用して、アップデートを取得します。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。

[製品アップデート（Product Updates）]ページ（[システム（System）]>[更新（Updates）]）には、それぞれの更新のバージョン、およびその更新が生成された日時が表示されます。また、更新の一環としてリブートが必要かどうかも示されます。

サポートから取得した更新をアプライアンスへアップロードすると、更新がページに示されます。パッチ機能および機能の更新のアンインストーラも表示されます。Firepower Management Center で、ページに VDB 更新を表示できます。

メジャーな更新の場合は、Firepower Management Center を更新すると、以前の更新のアンインストーラが削除されます。

Firepower Management Center でのソフトウェアの更新

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（**Access**）
任意（Any）	任意（Any）	任意（Any）	グローバルだけ	Admin

はじめる前に

- Firepower Management Center で実行時間が長いタスクの実行を許可します。
- Firepower Management Center に更新をアップロードします。詳細については、Firepower システムのソフトウェア更新のダウンロード，（10 ページ）と Firepower Management Center にソフトウェア更新をアップロードする，（11 ページ）を参照してください。

手順

ステップ 1 リリース ノートを読んで、更新前の必要なタスクを完了させます。

ステップ 2 展開内でデバイスが正常に通信していること、およびヘルス モニタによって問題が報告されていないことを確認します。

ステップ 3 [システム（System）] > [更新（Updates）]を選択します。

ステップ 4 アップロードした更新の横にあるインストール アイコンをクリックします。

ステップ 5 Firepower Management Center を選択し、[インストール（Install）] をクリックします。プロンプトが表示されたら、更新をインストールすることを確認して Firepower Management Center をリブートします。

ステップ 6 オプションで、更新ステータスをモニタします。

- マイナー更新については、タスク メッセージの表示を参照してください。
- メジャー更新については、主要な Firepower システム ソフトウェア更新のモニタリング，（13 ページ）を参照してください。

注意 更新のタイプに関係なく、更新が完了するまで、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。必要な場合は、Firepower Management Center を再起動します。

更新で問題が発生した場合（更新に失敗したことがメッセージ センターに示されている場合、またはメッセージに進捗が表示されない場合など）、更新を再開**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。

ステップ 7 更新が完了したら、必要に応じて Firepower Management Center にログインします。

ステップ 8 メジャー更新の後に最初にログインするユーザの場合、エンド ユーザ ライセンス契約（EULA）を確認して同意し、続行します。

ステップ 9 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 10 システム情報を表示するには、[ヘルプ（Help）] > [バージョン情報（About）]を選択します。

ステップ 11 システム情報ページで、ソフトウェア バージョンが正しくリストされていることを確認し、Firepower Management Center のルールの更新および VDB のバージョンをメモします。これらの情報が後で必要になります。

ステップ 12 すべての管理対象デバイスが、Firepower Management Center と正常に通信していることを確認します。

次の作業

- 新しい侵入ルールの更新があれば、それをインポートします（侵入ルールの更新, （19 ページ）を参照）。
- Firepower Management Center 上の VDB より新しい VDB があれば、サポート サイトからインストールします（脆弱性データベースの更新, （17 ページ）を参照）。
- 管理対象デバイスのシステム ソフトウェアを更新します（ を参照）。
- 設定変更を展開します。設定変更の導入を参照してください。

Firepower システムのソフトウェア更新のダウンロード

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

メジャー アップデートを除くすべてのアップデートについて、Firepower Management Center にソフトウェア アップデートをダウンロードできます。ダウンロードするには、Firepower Management Center がインターネットにアクセスできる必要があります。

はじめる前に

- 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 [アップデートのダウンロード（Download Updates）] をクリックして、Cisco サポート サイト（http://www.cisco.com/cisco/web/support/index.html）の最新の更新を確認します。

ステップ 3 更新をインストールします。詳細については、Firepower Management Center でのソフトウェアの更新, （9 ページ）と 脆弱性データベースの更新, （18 ページ）を参照してください。

Firepower Management Center にソフトウェア更新をアップロードする

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

次の場合に、Firepower Management Center に更新をアップロードする必要があります。

- メジャー更新を実行している。
- Firepower Management Center にインターネットへのアクセスがない。
- 管理対象デバイスを更新している。

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）]を選択します。

ステップ 3 [更新のアップロード（Upload Update）] をクリックします。

ステップ 4 更新を参照し、[アップロード（Upload）] をクリックします。

次の作業

- 更新をインストールします。詳細については、Firepower Management Center でのソフトウェアの更新, （9 ページ）と 脆弱性データベースの更新, （18 ページ）を参照してください。

管理対象デバイスでのソフトウェア更新

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

この手順のすべてのステップは、注記がない限り、Firepower Management Center で実行されます。

はじめる前に

- デバイスを管理する Firepower Management Center で Firepower System ソフトウェアを更新します。詳細については、Firepower システム ソフトウェア アップデートに関する注意事項, （8 ページ）を参照してください。
- Firepower Management Center に更新をアップロードします。詳細については、Firepower Management Center にソフトウェア更新をアップロードする, （11 ページ）を参照してください。

手順

ステップ 1 リリース ノートを読んで、更新前に必要なタスクを完了させます（Firepower システム ソフトウェア アップデートに関する注意事項, （8 ページ）および Firepower システムのソフトウェア アップデートの準備, （4 ページ）を参照）。

ステップ 2 展開内でアプライアンスが正常に通信していること、およびヘルス モニタによって問題が報告されていないことを確認します。

ステップ 3 [システム（System）] > [更新（Updates）]を選択します。

ステップ 4 インストール中の更新の横にあるインストール アイコンをクリックします。

ステップ 5 更新をインストールするデバイスを選択し、[インストール（Install）] をクリックします。
同じ更新が使用される場合、複数のデバイスを一度に更新することができます。プロンプトが表示されたら、更新をインストールすることを確認してデバイスを再起動します。

ファイルのサイズによっては、すべてのデバイスで更新をインストールするのに時間がかかることがあります。更新中に、管理対象デバイスが 2 回再起動されることがありますが、これは正常な動作です。

ステップ 6 オプションで、更新ステータスをモニタします。

- マイナー更新については、タスク メッセージの表示を参照してください。
- メジャー更新については、主要な Firepower システム ソフトウェア更新のモニタリング, （13 ページ）を参照してください。

注意 更新のタイプに関係なく、更新が完了するまで、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。必要な場合は、管理対象デバイスを再起動します。

更新で問題が発生した場合（更新に失敗したことがメッセージ センターに示されている場合、またはメッセージに進捗が表示されない場合など）、更新を再開**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。

ステップ 7 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 8 [デバイス（Devices）] > [デバイス管理（Device Management）] を選択して、更新したデバイスに正しいバージョンがリストされていることを確認します。

ステップ 9 更新したデバイスが、Firepower Management Center と正常に通信していることを確認します。

次の作業

- 設定変更を展開します。設定変更の導入を参照してください。
- オプションで、7000 または 8000 シリーズ デバイスへのメジャー更新の後でデバイスのローカル Web インターフェイスにログインします。メジャー更新の後に最初にログインするユーザには、エンド ユーザ ライセンス契約（EULA）が表示されることがあります。EULA を確認して承認し、処理を続行します。Web インターフェイスではなくコマンドライン インターフェイスを介して最初にログインした場合も EULA が表示されるので、必ず承認してください。

主要な Firepower システム ソフトウェア更新のモニタリング

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（Access）
任意（Any）	任意（Any）	Management Center	グローバルだけ	Admin

この手順は、アプライアンスのローカル Web インターフェイスを使用して実行する必要があります。

手順

ステップ 1 アプライアンスが必要な更新前チェックを完了するまで、メジャー ソフトウェア アップデートの進行を Message Center でモニタします。

この時点で、自分も含めてすべてのユーザは、システムによってWebインターフェイスからログアウトされます。管理者またはメンテナンス ユーザ以外は、更新が完了するまでログインし直すことはできません。

ステップ 2 管理者の場合は、Web インターフェイスにログインし直します。簡略化された更新ページが表示されます。

ステップ 3 更新ログを表示するには、[現在のスクリプトのログを表示する（show log for current script）] をクリックします。ログをもう一度非表示にするには、[現在のスクリプトのログを非表示する（hide log for current script）] をクリックします。

注意 更新で問題が生じた場合は（簡略化された更新ページを手動更新しても長時間にわたって進捗が表示されない場合など）、更新を再開**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。

次の作業

- 何らかの理由で更新に失敗した場合は、このページにエラーメッセージが表示され、失敗した日時、更新が失敗したときに実行していたスクリプト、およびサポートへの連絡方法が示されます。更新は再開**しないで**ください。
- 更新が正常に完了すると、ページに成功メッセージが表示され、アプライアンスがリブートされます。アプライアンスのリブートが完了したら、ページを更新してログインし、更新後の必要な手順を完了します。

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（**Access**）
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。

はじめる前に

- 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。

次の作業

- 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の更新

シスコの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。Firepower システムはフィンガープリントと脆弱性を関連付けて、特定のホストがネットワークの侵害のリスクを増大させているかどうかを判断するのをサポートします。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。

VDB を更新するには、Firepower Management Center で [製品の更新（Product Updates）] ページを使用します。サポートから取得した VDB 更新をアプライアンスへアップロードすると、このページに、アップロードした更新と Firepower システムの更新およびそのアンインストーラの更新が表示されます。

（注） 手動でまたは [アップデートのダウンロード（Download Updates）] をクリックして、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。

脆弱性のマッピングを更新するのにかかる時間は、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。システムのダウンタイムの影響を最小にするために、システムの使用率が低い時間帯に更新をスケジュールすることをお勧めします。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、ネットワーク上のホストの数を 1000 で割ります。

VDB を更新した後、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、設定を展開する必要があります。

注意 VDB アップデートをインストールした後、初めて脆弱性データベース（VDB）アップデートをインストールするか、またはアクセス コントロール ポリシーを展開すると、すぐに 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一時的に中断されます。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、管理対象デバイスのモデルおよびトラフィックの処理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。

自動更新機能を利用して VDB 更新をスケジュールすることができます。

脆弱性データベースの更新

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（**Access**）
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 でしか実行できません。

はじめる前に

- Firepower Management Center に更新をアップロードします。詳細については、Firepower システムのソフトウェア更新のダウンロード, （10 ページ）と Firepower Management Center にソフトウェア更新をアップロードする, （11 ページ）を参照してください。

注意 VDB アップデートをインストールした後、初めて脆弱性データベース（VDB）アップデートをインストールするか、またはアクセス コントロール ポリシーを展開すると、すぐに 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一時的に中断されます。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、管理対象デバイスのモデルおよびトラフィックの処理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 更新用の VDB 更新アドバイザリ テキストを読みます。このアドバイザリ テキストには、更新で作成された VDB に対する変更、および製品の互換性情報が含まれています。

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

ステップ 3 [製品の更新（Product Updates）] タブで、VDB 更新の横にあるインストール アイコンをクリックします。

ステップ 4 Firepower Management Center エントリの横にあるチェックボックスをオンにします。

ステップ 5 [Install（インストール）]をクリックします。ネットワーク マップ内のホストの数によっては、更新のインストールに時間がかかることがあります。

ステップ 6 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）。

注意 更新が完了するまで、マップされた脆弱性に関連する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。更新で問題が発生した場合には（たとえば、メッセージ センターに進捗が表示されない、更新が失敗したことが示されているなど）、更新を再開**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。

ステップ 7 更新が終了したら、[ヘルプ（Help）] > [バージョン情報（About）] を選択して、VDB 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。

次の作業

- 設定変更を展開します。設定変更の導入を参照してください。
- オプションで、VDB 更新をスケジュールします（脆弱性データベースの更新の自動化を参照）。

関連トピック

Snort® の再起動シナリオ

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 ステータス**：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、システム付属侵入ポリシーの詳細設定、およびシステム付属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**：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。

注意 ルール更新をインポートするときには、設定の変更を展開するとSnortプロセスが再起動され、一時的に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、管理対象デバイスのモデルおよびトラフィックの処理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。ルール更新のダウンロードおよびインストール プロセスがセキュリティ ポリシーに従っていることを確認してください。また、侵入ルールの更新のサイズは大きいことがあるため、ルールのインポートはネットワークの使用量が少ないときに行うようにしてください。

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。

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。

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（Access）
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。

はじめる前に

- 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（**Access**）
任意（Any）	任意（Any）	任意（Any）	グローバルだけ	Admin

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 ファイル インポート

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している場合、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。それは、数字が別のドメインにシーケンス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。
- 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 ファイルのインポート

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）	任意（Any）	Admin

次の説明に従ってインポートした進入ルールは、ローカル ルール カテゴリに保存されます。

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 [ルールの更新（Rule Updates）] タブをクリックします。

ステップ 3 [ルールの更新またはアップロードおよびインストールするテキスト ルール ファイル（Rule Update or text rule file to upload and install）] を選択して、ルール ファイルにナビゲートするために [参照（Browse）] 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。

次の作業

- 侵入ポリシーで、適切なルールが有効になっていることを確認してください。
- 設定変更を展開します。設定変更の導入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 • 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	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）	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, （30 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。

ルール アップデートのインポート ログの詳細ビュー

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。 • [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用。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）
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（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）。

フィールド	説明
[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。
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。 • [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。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）
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。

関連トピック

侵入ルールの更新インポート ログの詳細の表示, （30 ページ）

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（Access）
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。

地理位置情報データベースの更新

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（Access）
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（**Access**）
任意（Any）	任意（Any）	任意（Any）	グローバルだけ	Admin

地理位置情報データベース（GeoDB）の定期更新を自動化できます。GeoDB の定期更新は 7 日ごとに 1 度（週 1 回）実行されます。週ごとに更新が繰り返される時刻を設定できます。

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 [位置情報の定期更新（Recurring Geolocation Updates）] の下で、[週ごとの定期更新を有効にする（Enable Recurring Weekly Updates）] チェックボックスをオンにします。

ステップ 4 [更新の開始時刻（Update Start Time）] フィールドで、週ごとに GeoDB 更新を行う曜日と時刻を指定します。

ステップ 5 [保存（Save）] をクリックします。