



ASA FirePOWER モジュール ソフトウェアの更新

シスコは、ルール of 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) の更新だけでなく、ASA FirePOWER モジュール ソフトウェア本体のメジャーおよびマイナーの更新など、さまざまなタイプの更新を電子的に配布しています。



注意

このセクションでは、ASA FirePOWER モジュールの更新に関する全般的な情報について説明します。VDB、GeoDB、侵入ルールを含め、更新を実行する前に、更新に付随しているリリースノートまたはアドバイザリテキストを**必ず**お読みください。リリースノートには、前提条件、警告、および特定のインストールとアンインストールの手順など、重要な情報が記載されています。

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

詳細については、次の項を参照してください。

- [更新のタイプについて \(45-1 ページ\)](#)
- [ソフトウェア更新の実行 \(45-2 ページ\)](#)
- [ソフトウェア更新のアンインストール \(45-7 ページ\)](#)
- [脆弱性データベースの更新 \(45-8 ページ\)](#)
- [ルール更新およびローカルルールファイルのインポート \(45-9 ページ\)](#)
- [地理位置情報データベースの更新 \(45-21 ページ\)](#)

更新のタイプについて

ライセンス:すべて

シスコは、侵入ルールの更新や VDB の更新だけでなく、ASA FirePOWER モジュール ソフトウェア本体のメジャーおよびマイナーの更新など、さまざまなタイプの更新を電子的に配布しています。

次の表で、シスコが提供している更新のタイプについて説明します。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。[タスクのスケジュール \(41-1 ページ\)](#) および [再帰的なルール更新の使用 \(45-14 ページ\)](#) を参照してください。

表 45-1 ASA FirePOWER モジュールの更新タイプ

Update Type	説明	スケジュール	アンインストール
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、5.4.0.1 のようにバージョン番号の 4 桁目に変更されます)。	yes	yes
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、5.4.1 のようにバージョン番号の 3 桁目に変更されます)。	yes	yes
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、大規模な変更が含まれることがあります(通常は、5.3 または 5.4 のようにバージョン番号の最初の桁または 2 桁目に変更されます)。	no	no
VDB	VDB の更新は、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に影響します。	yes	no
侵入ルール	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セッサルール、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。	yes	no
地理情報データベース (GeoDB)	GeoDB の更新により、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情報が提供されます。地理情報データを、アクセス コントロールルールとして使用することができます。地理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

パッチおよび他のマイナーな更新はアンインストールできますが、VDB、GeoDB、または侵入ルールに対するメジャーな更新をアンインストールしたり、前のバージョンに戻したりすることはできないことに注意してください。新しいメジャーバージョンに更新してから古いバージョンに戻すことが必要になった場合は、サポートに連絡してください。

ソフトウェア更新の実行

ライセンス:すべて

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、更新の準備として、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しておく**必要があります**。次に、更新を開始できます。更新が成功したことを確認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。

詳細については、次の項を参照してください。

- [更新の計画\(45-3 ページ\)](#)
- [更新プロセスについて\(45-3 ページ\)](#)
- [ASA FirePOWER モジュール ソフトウェアの更新\(45-5 ページ\)](#)
- [メジャーな更新のステータスの監視\(45-7 ページ\)](#)

更新の計画

ライセンス:すべて

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、新しい機能、および既知の問題と解決済みの問題について説明されています。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。

以降の項では、更新の計画で検討しなければならない要素の概要を提供します。

ソフトウェア バージョンの要件

正しいソフトウェア 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。

時間とディスク領域の要件

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。リリース ノートには、領域と時間の要件が示されています。

設定のバックアップのガイドライン

シスコでは、メジャーの更新を開始する前に、外部の場所へコピーした後にASA FirePOWER モジュール上に残っているバックアップをすべて削除することを推奨しています。更新のタイプに関係なく、現行の設定データを外部の場所にバックアップしておく必要もあります。[バックアップと復元の使用\(47-1 ページ\)](#)を参照してください。

更新を実行するタイミング

更新プロセスはトラフィック インспекションおよびトラフィック フローに影響を与えることがあります。更新を行っている間は **Data Correlator** が無効になるため、シスコでは、保守期間内、または中断の影響が最も少ない時間に更新を行うことを推奨しています。

更新プロセスについて

ライセンス:すべて

ASA FirePOWER モジュールを更新するには、ASA FirePOWER モジュール インターフェイスを使用します。

[Product Updates] ページ ([Configuration] > [ASA FirePOWER Configuration] > [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、ソフトウェアの再起動が更新の一環として必要です。サポートから取得した更新を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。[ソフトウェア更新のアンインストール\(45-7 ページ\)](#)を参照してください。このページでは、VDBの更新もリストできます。



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。[ソフトウェア更新の自動化\(41-5 ページ\)](#)を参照してください。

トラフィックフローとインスペクション

更新をインストールまたはアンインストールすると、次の機能に影響を与えることがあります。

- トラフィックのインスペクション(アプリケーションおよびユーザの認識とコントロール、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、侵入検出と防御、接続のログギングなど)
- トラフィックフロー

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がどのように中断されるか、およびその期間は、ASA FirePOWER モジュールの設定と展開の方法、および更新でASA FirePOWER モジュールがリブートされるかどうかによって依存しています。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。

更新時の ASA FirePOWER モジュールの使用

更新のタイプに関係なく、更新のモニタ以外のタスクを実行するために ASA FirePOWER モジュールを使用しないでください。

メジャーな更新中にユーザが ASA FirePOWER モジュール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、ASA FirePOWER モジュールのインターフェイスが合理化されています。マイナーな更新の進捗は、タスクキュー([Monitoring] > [ASA FirePOWER Monitoring] > [Task Status]) でモニタできます。マイナーな更新中に ASA FirePOWER モジュール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。

マイナーな更新の場合でも、ASA FirePOWER モジュールが更新処理中に使用できなくなることがあります。これは想定されている動作です。そのような場合は、再びASA FirePOWER モジュールにアクセスできるようになるまで待機します。まだ更新が実行中の場合は、更新が完了するまで ASA FirePOWER モジュールを使用しないでください。更新中は、ASA FirePOWER モジュールが2回リブートされることがありますが、これも予想される動作です。



注意

更新で問題が発生した場合には(たとえば更新が失敗した、または [Update Status] ページの手動更新に進捗が表示されないなど)、更新を再開しないでください。代わりに、サポートへ連絡してください。

更新後

リリースノートに記載されている更新後のすべてのタスクを完了し、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。

最も重要な更新後作業は、アクセスコントロールポリシーの再適用です。アクセスコントロールポリシーを適用すると、トラフィックフローと処理が一時的に停止することがあります。また、いくつかのパケットが検査されない場合があります。[設定変更の展開\(4-12 ページ\)](#)を参照してください。

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
- 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

ASA FirePOWER モジュールソフトウェアの更新

ライセンス:すべて

更新のタイプ、および ASA FirePOWER モジュールがインターネットにアクセスできるかどうかによって、ASA FirePOWER モジュールソフトウェアを次の 2 つのいずれかの方法で更新します。

- ASA FirePOWER モジュール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更新を取得できます。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更新を手動でダウンロードして、ASA FirePOWER モジュールへアップロードすることもできます。ASA FirePOWER モジュール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、このオプションを選択します。

メジャーな更新の場合は、ASA FirePOWER モジュールを更新すると、以前の更新のアンインストールが削除されます。

ASA FirePOWER モジュールソフトウェアを更新するには、次の手順を実行します。

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します。

更新前のタスクには、ASA FirePOWER モジュールがシスコ ソフトウェアの正しいバージョンを実行している、更新を実行するための十分な空きディスク領域がある、更新を実行するために十分な時間を確保している、設定データをバックアップした、などの確認が含まれています。

ステップ 2 更新をアップロードします。ここで、更新のタイプによって、および ASA FirePOWER モジュールがインターネットにアクセスできるかどうかによって、2 つのオプションがあります。

- メジャーな更新を除くすべての更新で、ASA FirePOWER モジュールがインターネットにアクセスできる場合は、[Configuration] > [ASA FirePOWER Configuration] > [Updates] の順に選択し、[Download Updates] をクリックして、次のいずれかのサポート サイトで最新の更新をチェックします。
 - Sourcefire: (<https://support.sourcefire.com/>)
 - シスコ: (<http://www.cisco.com/cisco/web/support/index.html>)
- メジャーな更新の場合、または ASA FirePOWER モジュールがインターネットにアクセスできない場合は、最初に次のいずれかのサポート サイトから更新を手動でダウンロードする必要があります。
 - Sourcefire: (<https://support.sourcefire.com/>)
 - シスコ: (<http://www.cisco.com/cisco/web/support/index.html>)
- [Configuration] > [ASA FirePOWER Configuration] > [Updates] の順に選択し、[Upload Update] をクリックします。[Choose File] をクリックして、その更新に移動して選択し、[Upload] をクリックします。



(注) サポートサイトから、手動でまたは [Product Updates] タブで [Download Updates] をクリックして、更新を直接ダウンロードします。電子メールで更新ファイルを転送すると、ファイルが破損することがあります。

更新がアップロードされます。

ステップ 3 [Monitoring] > [ASA FirePOWER Monitoring] > [Task Status] の順に選択して、タスク キューを表示し、進行中のジョブがないことを確認します。

更新を開始したときに実行されているタスクは停止され、再開できません。更新が完了した後で、タスク キューから手動で削除する必要があります。タスク キューは 10 秒ごとに自動的にリフレッシュされます。更新を始める前に、長時間実行しているタスクが完了するまで待機する必要があります。

ステップ 4 [Configuration] > [ASA FirePOWER Configuration] > [Updates]の順に選択します。
[Product Updates] ページが表示されます。

ステップ 5 ユーザがアップロードする更新の隣にあるインストールアイコンをクリックします。

更新プロセスが開始されます。更新を監視する方法は、更新がメジャーかマイナーかによって異なります。更新のタイプを判断するには、[ASA FirePOWER モジュールの更新タイプ](#)の表およびリリース ノートを参照してください。

- マイナーな更新の場合、更新の進捗は、タスク キュー ([Monitoring] > [ASA FirePOWER Monitoring] > [Task Status]) でモニタできます。
- メジャーな更新については、タスク キューで更新の進捗の監視を開始できます。ただし、ASA FirePOWER モジュールによる更新前の必要なチェックが完了すると、ユーザはモジュール インターフェイスからロックアウトされます。再度アクセスすると、[Upgrade Status] ページが表示されます。詳細については、[メジャーな更新のステータスの監視 \(45-7 ページ\)](#)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、更新のモニタ以外のタスクを実行するために ASA FirePOWER モジュールを使用しないでください。必要な場合は、ASA FirePOWER モジュールをリブートします。詳細については、[更新時の ASA FirePOWER モジュールの使用 \(45-4 ページ\)](#)を参照してください。

ステップ 6 更新が完了したら、ASA FirePOWER モジュール インターフェイスにアクセスし、ページを更新します。そうしない場合、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。メジャーな更新の後、最初にインターフェイスにアクセスしたユーザに対してエンド 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。

ステップ 7 サポート サイトで利用できるルール更新が、自身の ASA FirePOWER モジュール上のルールよりも新しい場合は、新しいルールをインポートします。
詳細については、[ルール更新およびローカル ルール ファイルのインポート \(45-9 ページ\)](#)を参照してください。

ステップ 8 アクセス コントロール ポリシーを再適用します。

アクセス コントロール ポリシーを適用すると、トラフィック フローと処理が一時的に停止することがあります。また、いくつかのパケットが検査されない場合があります。詳細については、[設定変更の展開 \(4-12 ページ\)](#)を参照してください。

ステップ 9 サポート サイトにある利用可能な VDB が、最後にインストールした VDB よりも新しい場合は、その最新の VDB をインストールします。

VDB の更新をインストールすると、トラフィック フローと処理が一時的に停止することがあります。また、いくつかのパケットが検査されない場合があります。詳細については、[脆弱性データベースの更新 \(45-8 ページ\)](#)を参照してください。

メジャーな更新のステータスの監視

ライセンス:すべて

メジャーな更新では、ASA FirePOWER モジュールは、更新プロセスを簡単にモニタできるような、簡潔なインターフェイスを提供します。この簡潔なインターフェイスではまた、更新のモニタリング以外のタスクを実行するために ASA FirePOWER モジュールを使用することはできません。タスク キューでの更新の進捗についてモニタを開始できます ([Monitoring] > [ASA FirePOWER Monitoring] > [Task Status])。ただし、ASA FirePOWER モジュールによる更新前の必要なチェックが完了すると、簡潔な更新ページが表示されるまで、ユーザはユーザ インターフェイスからロックアウトされます。

簡潔なインターフェイスには、更新前のバージョン、更新後のバージョン、および更新を開始してから経過時間が表示されます。また進捗バーが表示され、実行中のスクリプトに関する詳細が示されます。



ヒント

更新ログを表示するには、[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、[hide log for current script]をクリックします。

何らかの理由で更新が失敗すると、ページにはエラー 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、およびサポートへ連絡するための方法が示されます。更新を再開しないでください。



注意

更新で他の問題(ページの手動更新で長時間経過しても進捗が表示されない、など)が生じた場合も、更新を再開しないでください。代わりに、サポートへ連絡してください。

更新が完了すると、ASA FirePOWER モジュールは成功メッセージ表示して再起動します。ASA FirePOWER モジュールがリブートを終了したら、更新後の必要な手順をすべて実行します。

ソフトウェア更新のアンインストール

ライセンス:すべて

パッチまたは機能の更新を適用すると、更新プロセスにより、更新を削除できるアンインストーラが作成されます。

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シスコソフトウェアのバージョンは、どのような経路で更新したかによって異なります。たとえば、バージョン 5.0 からバージョン 5.0.0.2 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 5.0.0.2 のパッチをアンインストールすると、バージョン 5.0.0.1 の更新をインストールしたことがなくても、バージョン 5.0.0.1 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シスコ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

アンインストールは、メジャーな更新ではサポートされていません。新しいメジャーバージョンに更新してから古いバージョンに戻すことが必要になった場合は、サポートに連絡してください。


トラフィック フローとインスペクション

更新をアンインストールすると、トラフィック インスペクションとトラフィック フローが影響を受ける可能性があります。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ら、アンインストールが成功したことを確認します。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。

パッチまたは機能更新のアンインストール方法:

-
- ステップ 1** [Configuration] > [ASA FirePOWER Configuration] > [Updates]の順に選択します。
[Product Updates] ページが表示されます。
- 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、ASA FirePOWER モジュールをリブートします。
アンインストール プロセスが開始されます。その進捗は、タスク キュー([Monitoring] > [ASA FirePOWER Monitoring] > [Task Status]) でモニタできます。
-  **注意** アンインストールが完了するまで、タスクを実行するために ASA FirePOWER モジュール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、ASA FirePOWER モジュールをリブートします。詳細については、[更新時の ASA FirePOWER モジュールの使用 \(45-4 ページ\)](#) を参照してください。
-
- ステップ 3** ページを更新します。そうしない場合、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。
-

脆弱性データベースの更新

ライセンス:すべて

シスコ脆弱性データベース (VDB) は、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。シスコ脆弱性調査チーム (VRT) は、VDB を定期的に更新します。VDB を更新するには、[Product Updates] ページを使用します。

**注**

検出の更新とともに VDB 更新をインストールすると、トラフィックフローと処理が一時的に停止し、いくつかのパケットが検査なしで通過する場合があります。システムのダウンタイムの影響を最小限に抑えるために、システムの使用率が低い時間に合わせて更新をスケジュールすることもできます。

**注**

VDB の更新完了後に、古くなったすべてのアクセス コントロール ポリシーを再適用します。VDB のインストールまたはアクセス コントロール ポリシーの再適用を行うと、トラフィックフローと処理が一時的に停止することがあり、また、いくつかのパケットが検査されずに通過する場合がありますので注意してください。詳細については、[設定変更の展開 \(4-12 ページ\)](#) を参照してください。

この項では、手動による VDB 更新を計画および実行する方法について説明します。

脆弱性データベースを更新する方法:

- 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 VDB に加えられた変更に関する情報が含まれています。
- ステップ 2 [Configuration] > [ASA FirePOWER Configuration] > [Updates]の順に選択します。
[Product Updates] ページが表示されます。
- ステップ 3 更新をアップロードします。
- ASA FirePOWER モジュールがインターネットにアクセスできる場合は、[Download Updates] をクリックして、次のいずれかのサポート サイトで最新の更新を確認します。
 - Sourcefire: (<https://support.sourcefire.com/>)
 - シスコ: (<http://www.cisco.com/cisco/web/support/index.html>)
 - ASA FirePOWER モジュールがインターネットにアクセスできない場合は、次のいずれかのサポート サイトから更新を手動でダウンロードして [Upload Update] をクリックします。
[Choose File] をクリックして、その更新に移動して選択し、[Upload] をクリックします。
 - Sourcefire: (<https://support.sourcefire.com/>)
 - シスコ: (<http://www.cisco.com/cisco/web/support/index.html>)



(注) サポート サイトから、手動でまたは [Download Updates] をクリックして、更新を直接ダウンロードします。電子メールで更新ファイルを転送すると、ファイルが破損することがあります。

更新がアップロードされます。

- ステップ 4 VDB 更新の隣にあるインストール アイコンをクリックします。
[Install Update] ページが表示されます。
- ステップ 5 [Install] をクリックします。
更新プロセスが開始されます。更新の進捗は、タスク キュー ([Monitoring] > [ASA FirePOWER Monitoring] > [Task Status]) でモニタできます。



注意

更新で問題が発生した場合には(たとえばタスク キューに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、サポートへ連絡してください。

VDB 更新を有効にするには、古くなったすべてのアクセス コントロール ポリシーを再適用する必要があります。「設定変更の展開(4-12 ページ)」を参照してください。

ルール更新およびローカルルールファイルのインポート

ライセンス:すべて

新しい脆弱性に関する情報が判明すると、シスコ脆弱性調査チーム(VRT)からルール更新がリリースされるので、これを最初にASA FirePOWER モジュールにインポートしてから、影響を受けるアクセス コントロール、ネットワーク解析、および侵入ポリシーを適用することで、その実装ができます。

ルール更新は累積的なので、シスコは常に最新の更新をインポートすることを推奨しています。現在インストールされているルールのバージョンに一致するルール更新、またはそれより前のバージョンのルール更新をインポートすることはできません。



注

ルール更新には新しいバイナリが含まれている場合があるので、これらのダウンロードおよびインストールのプロセスが、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てください。また、ルールの更新は量が多くなることがあるため、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。

ルール更新では、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の状態:** ルール更新は、新規または更新された侵入およびプリプロセッサのルールを提供します。新しいルールについては、ルールの状態がそれぞれのシステム提供の侵入ポリシーで異なる場合があります。たとえば、Security over Connectivity の侵入ポリシーでは新しいルールが有効になっており、Connectivity over Security の侵入ポリシーでは無効になっていることがあります。ルールの更新では、既存のルールのデフォルト状態が変更されたり、既存のルールそのものが削除されることもあります。
- **新しいルール カテゴリ:** ルール更新には、常に追加される新しいルール カテゴリが含まれている場合があります。
- **変更されたプリプロセッサおよび詳細設定:** ルール更新は、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解析ポリシーのプリプロセッサ設定を変更することがあります。また、アクセス コントロール ポリシーにおける高度な前処理やパフォーマンス オプションに関するデフォルト値を更新することもあります。
- **新規の変数および変数の変更:** ルール更新は、既存のデフォルト変数のデフォルト値を変更す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。新しい変数は常に追加されています。

ルール更新でポリシーが変更されるタイミングの概要

ルール更新は、すべてのアクセス コントロール ポリシーと同様に、システム提供およびカスタムのネットワーク解析ポリシーの両方に影響を与えます。

- **システム提供:** システムが提供するネットワーク解析および侵入ポリシーへの変更は、その他のアクセス コントロールの詳細設定と同様に、更新後にポリシーを再適用すると自動的に有効になります。
- **カスタム:** カスタムのネットワーク解析および侵入ポリシーは、いずれもシステム提供のポリシーをベースとして使用するか、ポリシー チェーン中でのイベント ベースとして使用しているので、ルール更新がカスタムのネットワーク解析および侵入ポリシーにも影響を与えることがあります。ただし、ルール更新によるこれらの自動的な変更が行われないようにすることができます。その場合、ルール更新のインポートとは独立したスケジュールに従って、システム提供の基本ポリシーを手動で更新することができます。ユーザによる選択とは関係なく(カスタム ポリシーごとに実装)システム提供のポリシーに対する更新では、ユーザがカスタマイズした設定は上書きされません。詳細については、[ルール更新がシステムによって提供される基本ポリシーを変更することを許可する\(18-4 ページ\)](#)を参照してください。

ルールの更新をインポートすると、ネットワーク解析および侵入ポリシーのキャッシュされていた変更は、すべて廃棄されることに注意してください。便宜のために、[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がリストされます。詳細については、[競合の解決とポリシー変更の確定\(17-16 ページ\)](#)を参照してください。

ポリシーの再適用

ルール更新による変更を反映させるには、変更されたすべてのポリシーを再適用する必要があります。ルール更新をインポートする際には、侵入またはアクセス コントロール ポリシーを自動的に再適用するように、システムを設定できます。この機能が特に役立つのは、ルール更新によるシステム提供の基本ポリシーの変更を許可する場合です。

- アクセス コントロール ポリシーを再適用すると、関連付けられた SSL、ネットワーク解析、ファイルのポリシーも再適用されますが、侵入ポリシーは再適用されません。また、変更された詳細設定のデフォルト値もすべて更新されます。ネットワーク解析のポリシーは個別に適用できないので、ネットワーク解析ポリシーのプリプロセッサ設定を更新するには、アクセス コントロール ポリシーの再適用が必要です。
- 侵入ポリシーを再適用すると、ルールおよびその他の変更された侵入ポリシーの設定も更新することができます。侵入ポリシーの再適用はアクセス コントロール ポリシーとあわせて行うこともできますが、その他のアクセス コントロールの設定は更新せずに、侵入ポリシーの適用で侵入ルールだけを更新することもできます。

ルールの更新に共有オブジェクトのルールが含まれている場合に、インポートの後で初めてアクセス コントロールまたは侵入ポリシーを適用すると、トラフィック フローと処理が一時的に停止し、いくつかのパケットが検査されずに通過する場合があります。アクセス コントロールおよび侵入ポリシーの適用における、要件、その他の影響、および推奨事項などを含めた詳細については「[設定変更の展開 \(4-12 ページ\)](#)」を参照してください。

ルール更新のインポートの詳細については、次の解説を参照してください。

- [ワンタイム ルール更新の使用 \(45-11 ページ\)](#) では、サポート サイトから 1 つのルール更新をインポートする方法について説明しています。
- [再帰的なルール更新の使用 \(45-14 ページ\)](#) では、自動機能を使用して、サポート サイトからルールの更新をダウンロードおよびインストールする方法について説明しています。
- [ローカル ルール ファイルのインポート \(45-15 ページ\)](#) では、ローカル マシンで作成した標準テキスト ルール ファイルのコピーをインポートする方法について説明しています。
- [ルール更新ログの表示 \(45-17 ページ\)](#) では、ルール更新のログについて説明しています。

ワンタイム ルール更新の使用

ライセンス:すべて

ワンタイム ルール更新では次の 2 つの方法を使用することができます。

- [手動によるワンタイム ルール更新の使用 \(45-11 ページ\)](#) では、サポート サイトから手動でルール更新をダウンロードし、それを手動でインストールする方法について説明しています。
- [自動によるワンタイム ルール更新の使用 \(45-13 ページ\)](#) では、自動機能を使用し、サポート サイトで新しいルール更新を検索し、それをアップロードする方法について説明しています。

手動によるワンタイム ルール更新の使用

ライセンス:すべて

次の手順では、新しいルール更新を手動でインポートする方法について説明します。この手順は、ASA FirePOWER モジュールがインターネットにアクセスできない場合に特に有用です。

手動でルール更新をインポートする方法:

ステップ 1 インターネットにアクセスできるコンピュータから、次のサイトのいずれかへアクセスします。

- **Sourcefire:** (<https://support.sourcefire.com/>)
- **シスコ:** (<http://www.cisco.com/cisco/web/support/index.html>)

ステップ 2 [Download] をクリックし、[Rules] をクリックします。

ステップ 3 最新のルール更新へ移動します。

ルール更新は累積的です。現在インストールされているルールのバージョンに一致するルール更新、またはそれより前のバージョンのルール更新をインポートすることはできません。

ステップ 4 ダウンロードするルール更新ファイルをクリックし、そのファイルをコンピュータに保存します。

ステップ 5 [Configuration] > [ASA FirePOWER Configuration] > [Updates] の順に選択し、[Rule Updates] タブを選択します。

[Rule Updates] ページが表示されます。



ヒント

[Rule Editor] ページ([Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] > [Rule Editor]) で、[Import Rules] をクリックすることもできます。

ステップ 6 オプションで [Delete All Local Rules] をクリックし、[OK] をクリックして、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します。詳細については、「[カスタム ルールの削除\(29-109 ページ\)](#)」を参照してください。

ステップ 7 [Rule Update or text rule file to upload and install] を選択し、[Choose File] をクリックしてナビゲートし、ルール更新ファイルを選択します。

ステップ 8 オプションで、更新の完了後にポリシーを再適用します。

- [Reapply intrusion policies after the rule update import completes] を選択すると、侵入ポリシーが自動的に再適用されます。このオプションを選択するのは、その他のアクセス コントロールのユーザ設定は更新せずに、ルールおよびその他の変更された侵入ポリシーの設定を更新する場合だけです。このオプションの選択が**必要となる**のはアクセス コントロール ポリシーとあわせて侵入ポリシーを再適用する場合であり、そうしたケースではアクセス コントロール ポリシーを再適用しても完全には適用されません。
- [Reapply access control policies after the rule update import completes] を選択すると、アクセス コントロール ポリシーとその関連の SSL、ネットワーク解析、ファイルのポリシーも自動的に再適用されますが、侵入ポリシーは再適用されません。このオプションを選択すると、変更されたアクセス コントロールの詳細設定のデフォルト値もすべて更新されます。ネットワーク解析のポリシーは親となるアクセス コントロール ポリシーと個別には適用できないので、ネットワーク解析ポリシーのプリプロセスサ設定を更新するには、アクセス コントロール ポリシーの再適用が**必要**です。

ステップ 9 [Import] をクリックします。

システムはルール更新をインストールし、[Rule Update Log] 詳細ビューを表示します。「[\[Rule Update Import Log\] 詳細ビューについて\(45-19 ページ\)](#)」を参照してください。システムは、前のステップで指定したポリシーも適用します。「[設定変更の展開\(4-12 ページ\)](#)」および「[侵入ポリシーの適用\(25-8 ページ\)](#)」を参照してください。



(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。

自動によるワンタイムルール更新の使用

ライセンス:すべて

次の手順では、サポートサイトに自動で接続して、新しいルール更新をインポートする方法について説明します。この手順は、ASA FirePOWER モジュールがインターネットにアクセスできる場合のみ使用できます。

自動でルール更新をインポートする方法:

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Updates]の順に選択し、[Rule Updates] タブを選択します。

[Rule Updates] ページが表示されます。



ヒント

[Rule Editor] ページ([Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] > [Rule Editor])で、[Import Rules] をクリックすることもできます。

ステップ 2 オプションで [Delete All Local Rules] をクリックし、[OK] をクリックして、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します。詳細については、「[カスタム ルールの削除 \(29-109 ページ\)](#)」を参照してください。

ステップ 3 [Download new Rule Update from the Support Site] を選択します。

ステップ 4 オプションで、更新の完了後にポリシーを再適用します。

- [Reapply intrusion policies after the rule update import completes] を選択すると、侵入ポリシーが自動的に再適用されます。このオプションを選択するのは、その他のアクセス コントロールのユーザ設定は更新せずに、ルールおよびその他の変更された侵入ポリシーの設定を更新する場合だけです。このオプションの選択が**必要となる**のはアクセス コントロール ポリシーとあわせて侵入ポリシーを再適用する場合であり、そうしたケースではアクセス コントロール ポリシーを再適用しても完全には適用されません。
- [Reapply access control policies after the rule update import completes] を選択すると、アクセス コントロール ポリシー、ネットワーク解析ポリシー、ファイル ポリシーは自動的に再適用されますが、侵入ポリシーは再適用されません。このオプションを選択すると、変更されたアクセス コントロールの詳細設定のデフォルト値もすべて更新されます。ネットワーク解析のポリシーは親となるアクセス コントロール ポリシーと個別には適用できないので、ネットワーク解析ポリシーのプリプロセッサ設定を更新するには、アクセス コントロール ポリシーの再適用が**必要です**。

ステップ 5 [Import] をクリックします。

システムはルール更新をインストールし、[Rule Update Log] 詳細ビューを表示します。「[\[Rule Update Import Log\] 詳細ビューについて \(45-19 ページ\)](#)」を参照してください。システムは、前のステップで指定したポリシーも適用します。「[設定変更の展開 \(4-12 ページ\)](#)」および「[侵入ポリシーの適用 \(25-8 ページ\)](#)」を参照してください。



(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。

再帰的なルール更新の使用

ライセンス:すべて

[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。

ルール更新のインポートにおける適用可能なサブタスクは、ダウンロード、インストール、ベースポリシーの更新、およびポリシーの再適用の順序で生じます。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。適用できるのは、再帰的なインポートが設定されているASA FirePOWER モジュールで以前に適用されたポリシーのみであることを注意してください。

再帰的なルール更新をスケジュールする方法:

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Updates]の順に選択し、[Rule Updates] タブを選択します。

[Rule Updates] ページが表示されます。



ヒント

[Rule Editor] ページ([Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] > [Rule Editor])で、[Import Rules] をクリックすることもできます。

ステップ 2 オプションで [Delete All Local Rules] をクリックし、[OK] をクリックして、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します。詳細については、「[カスタム ルールの削除\(29-109 ページ\)](#)」を参照してください。

ステップ 3 [Enable Recurring Rule Update Imports] を選択します。

ページが拡張され、再帰的なインポートを設定するためのオプションが表示されます。

[Recurring Rule Update Imports] セクション見出しの下に、インポート ステータスのメッセージが表示されます。設定を保存すると、再帰的なインポートが有効になります。



ヒント

再帰的なインポートを無効にするには、[Enable Recurring Rule Update Imports] チェック ボックスをオフにして [Save] をクリックします。

ステップ 4 [Import Frequency] フィールドで、ドロップダウン リストから [Daily]、[Weekly]、または [Monthly] を選択します。

週次または月次インポート間隔を選択した場合は、表示されるドロップダウン リストを使用して、ルールの更新をインポートする曜日または月の日を選択します。選択する内容をクリックするか、または最初の文字または数字を1回以上入力して、Enter を押すことで、再帰タスクのドロップダウン リストから選択できます。

ステップ 5 [Import Frequency] フィールドで、再帰的なルール更新のインポートを開始するタイミングを指定します。

ステップ 6 オプションで、更新の完了後にポリシーを再適用します。

- [Reapply intrusion policies after the rule update import completes] を選択すると、侵入ポリシーが自動的に再適用されます。このオプションを選択するのは、その他のアクセスコントロールのユーザ設定は更新せずに、ルールおよびその他の変更された侵入ポリシーの設定を更新する場合だけです。このオプションの選択が**必要となる**のはアクセスコントロールポリシーとあわせて侵入ポリシーを再適用する場合であり、そうしたケースではアクセスコントロールポリシーを再適用しても完全には適用されません。

- [Reapply access control policies after the rule update import completes]を選択すると、アクセスコントロールポリシーとその関連のSSL、ネットワーク解析、ファイルのポリシーも自動的に再適用されますが、侵入ポリシーは再適用されません。このオプションを選択すると、変更されたアクセスコントロールの詳細設定のデフォルト値もすべて更新されます。ネットワーク解析のポリシーは親となるアクセスコントロールポリシーと個別には適用できないので、ネットワーク解析ポリシーのプリプロセッサ設定を更新するには、アクセスコントロールポリシーの再適用が**必要**です。

ステップ 7 [Save]をクリックし、設定を使用した再帰的なルール更新のインポートを有効にします。

[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。スケジュールされた時間になるとシステムは、前のステップで指定したルール更新をインストールしてポリシーを適用します。「[設定変更の展開 \(4-12 ページ\)](#)」および「[侵入ポリシーの適用 \(25-8 ページ\)](#)」を参照してください。

インポートの前またはインポート中にも、ログオフしたり、他のタスクを実行したりできます。インポート中にアクセスした場合は、[Rule Update Log] に赤いステータスのアイコン(❗)が表示され、[Rule Update Log] 詳細ビューでは表示されたメッセージを確認できます。ルールの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。詳細については、[ルール更新ログの表示 \(45-17 ページ\)](#)を参照してください。



(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。

ローカルルールファイルのインポート

ライセンス:すべて

ローカルルールはカスタム標準テキストルールで、ユーザがローカルマシンからASCIIまたはUTF-8 エンコードのプレーンテキストファイルとしてインポートします。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。

ローカルルールのインポートについて、次の点に注意してください。

- 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。
- ジェネレータ ID(GID)を指定する必要はありません。GID を指定する場合は、標準テキストルールに対しては GID 1、機密データルールに対しては 138 のみ指定できます。
- 初めてルールを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、他のルールのSIDとの競合が回避されます。

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。

- 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場合には、システムによって割り当てられたSID、および現在のリビジョン番号よりも大きいリビジョン番号を含める必要があります。

現行のローカルルールのリビジョン番号を表示するには、[Rule Editor] ページ([Policies] > [Intrusion] > [Rule Editor])を表示し、ローカルルールのカテゴリをクリックしてフォルダを展開し、ルールの隣にある [Edit] をクリックします。

- システムによって割り当てられた SID、および現行のリビジョン番号よりも大きいリビジョン番号を使用してルールをインポートして削除したローカルルールは、元に戻すことができます。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すことに注意してください。これは、ローカルルールを元に戻すための方法です。
削除されたローカルルールのリビジョン番号を表示するには、[Rule Editor] ページ ([Policies] > [Intrusion Policy] > [Rule Editor]) を表示し、削除されたルールカテゴリをクリックしてフォルダを展開し、ルールの隣にある [Edit] をクリックします。
- 2147483647 よりも大きい SID を持つルールが含まれているルールファイルはインポートできません。この場合、インポートが失敗します。
- 64 文字を超える送信元または宛先のポートのリストが含まれているルールをインポートすると、そのインポートは失敗します。
- システムは常に、ユーザがインポートするローカルルールを無効なルール状態に設定します。これらを侵入ポリシーで使用するには、その前に手動でローカルルールの状態を設定する必要があります。詳細については、「[ルール状態の設定 \(26-21 ページ\)](#)」を参照してください。
- ファイル内のルールに、エスケープ文字が含まれていないことを確認する必要があります。
- ルールインポータでは、すべてのカスタムルールを ASCII または UTF-8 エンコードでインポートする必要があります。
- 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。
- 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。
- 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。
- また、二重のポンド文字 (##) で始まるローカルルールは無視し、インポートしません。
- 侵入ポリシーで、侵入イベントのしきい値機能と組み合わせて非推奨の threshold キーワードを使用しているローカルルールをインポートして有効にすると、ポリシーの検証は失敗します。詳細については、「[イベントしきい値の設定 \(26-23 ページ\)](#)」を参照してください。

ローカルルールファイルをインポートする方法:

ステップ 1 [Policies] > [Intrusion Policy] > [Rule Editor] の順に選択します。

[Rule Editor] ページが表示されます。

ステップ 2 [Import Rules] をクリックします。

[Import Rules] ページが表示されます。



ヒント

[System] > [Updates] を選択して、[Rule Updates] タブを選択することもできます。

ステップ 3 [Rule Update or text rule file to upload and install] を選択して、[Choose File] をクリックし、ルールファイルにナビゲートします。この方法でアップロードされたすべてのルールは、ローカルルールカテゴリに保存されることに注意してください。



ヒント

インポートできるのは、ASCII または UTF-8 エンコードのプレーンテキストファイルだけです。

ステップ 4 [Import] をクリックします。

ルールファイルがインポートされます。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。影響を受けるポリシーが次に適用されるまで、ルールはアクティブにはなりません。



(注) システムは、侵入ポリシーを適用するまで、インスペクションに対して新しいルールセットを使用しません。手順については、[設定変更の展開 \(4-12 ページ\)](#) を参照してください。



ルール更新ログの表示

ライセンス:すべて

ASA FirePOWER モジュールは、ユーザがインポートする各ルール更新およびローカルルールファイルごとに1つのレコードを生成します。

各レコードにはタイムスタンプ、ファイルをインポートしたユーザ名、およびインポートが正常に終了したか失敗したかを示すステータスアイコンが含まれています。ユーザは、自分がインポートするすべてのルール更新およびローカルルールファイルのリストを管理する、リストからレコードを削除する、インポートしたすべてのルールおよびルール更新のコンポーネントについての詳細レコードにアクセスする、といったことができます。[\[Rule Update Log\]](#) で実行できる操作を次の表で説明します。

表 45-2 [\[Rule Update Log\]](#) のアクション

目的	操作
テーブルのカラムの内容について詳しく調べる	詳細については、 [Rule Update Log] の表について(45-18 ページ)を参照してください。
インポートログからインポートファイルレコード(ファイルに含まれているすべてのオブジェクトについて削除されたレコードも含めて)を削除する	インポートファイルでファイル名の隣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。
ルール更新またはローカルルールファイルにインポートされている各オブジェクトの詳細を表示する	インポートファイルでファイル名の隣にある表示アイコン()をクリックします。

詳細については、次の項を参照してください。

- [\[Rule Update Log\]](#) の表について(45-18 ページ)では、インポートするルール更新およびローカルルールファイルのリスト内のフィールドについて説明します。
- [\[Rule Update Import Log\]](#) の詳細の表示(45-19 ページ)では、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について説明します。
- [\[Rule Update Import Log\]](#) 詳細ビューについて(45-19 ページ)では、[\[Rule Update Log\]](#) 詳細ビューの各フィールドについて説明します。

[Rule Update Log] を表示する方法:

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Updates]の順に選択し、[Rule Updates] タブを選択します。

[Rule Updates] ページが表示されます。



ヒント

[Rule Editor] ページ([Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] > [Rule Editor])で、[Import Rules] をクリックすることもできます。

ステップ 2 [Rule Update Log]をクリックします。

[Rule Update Log] ページが表示されます。このページには、インポートされた各ルール更新とローカルルールファイルが示されています。

[Rule Update Log] の表について

ライセンス:すべて

次の表で、ユーザがインポートするルール更新およびローカルルールファイルのリストのフィールドについて説明します。

表 45-3 **[Rule Update Log] のフィールド**

フィールド	説明
Summary	インポートファイルの名前。インポートが失敗した場合は、ファイル名の下に、失敗した理由の簡単な説明が表示されます。
Time	インポートが開始された日時。
User ID	インポートをトリガーとして使用したユーザ名。
Status	インポートの状態を表します <ul style="list-style-type: none"> 正常終了(🟢) 失敗した、または実行中(🔴) <p>ヒント インポート中には [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。</p>

ルール更新またはファイル名の隣にある表示アイコン(🔍)をクリックして、ルール更新またはローカルルールファイルの [Rule Update Log] 詳細ページを表示するか、または削除アイコン(🗑️)をクリックして、ファイルレコード、およびファイルと一緒にインポートされたすべての詳細オブジェクトレコードを削除します。



ヒント

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。

[Rule Update Import Log] の詳細の表示

ライセンス:すべて

[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。

次の表では、[Rule Update Import Log] 詳細ビューで実行できる特定のアクションについて説明します。

表 45-4 [Rule Update Import Log] 詳細ビューのアクション

目的	操作
テーブルのカラムの内容について詳しく調べる	詳細については、 [Rule Update Import Log] 詳細ビューについて (45-19 ページ) を参照してください。

[Rule Update Import Log] 詳細ビューを表示する方法:

ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Updates] の順に選択し、[Rule Updates] タブを選択します。

[Rule Updates] ページが表示されます。



ヒント

[Rule Editor] ページ ([Configuration] > [ASA FirePOWER Configuration] > [Policies] > [Intrusion Policy] > [Rule Editor]) で、[Import Rules] をクリックすることもできます。

ステップ 2 [Rule Update Log] をクリックします。

[Rule Update Log] ページが表示されます。

ステップ 3 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。

詳細レコードのテーブルビューが表示されます。

[Rule Update Import Log] 詳細ビューについて

ライセンス:すべて

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を表示することができます。以下の表で、[Rule Update Log] 詳細ビューのフィールドについて説明します。

表 45-5 [Rule Update Import Log] 詳細ビューのフィールド

フィールド	説明
Time	インポートが開始された日時。
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、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。

表 45-5 [Rule Update Import Log] 詳細ビューのフィールド(続き)

フィールド	説明
Type	<p>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。</p> <ul style="list-style-type: none"> [ruleupdate 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) [rule](新しいルールまたは更新されたルールの場合。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)。 [policyapply](インポートで [Reapply intrusion policies after the Rule Update import completes] オプションが有効だった場合)
Action	<p>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。</p> <ul style="list-style-type: none"> [new](ルールで、この ASA FirePOWER モジュール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、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](ルールで、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、システム提供ポリシーで有効になっている場合) [disabled](ルールで、システム提供ポリシーでルールが無効になっている場合) [drop](ルールで、システム提供ポリシーでルールが [Drop] または [Generate Events] に設定されている場合) [error](ルール更新またはローカルルール ファイルで、インポートが失敗した場合) [apply](インポートで [Reapply intrusion policies after the Rule Update import completes] オプションが有効だった場合)
Default Action	<p>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。</p>
GID	<p>ルールのジェネレータ ID。例:1 (標準テキスト ルール)や 3(共有オブジェクトのルールなど)。</p>
SID	<p>ルールの SID。</p>
Rev	<p>ルールのリビジョン番号。</p>
Policy	<p>インポートされたルールの場合、このフィールドには [All]が表示されます。これは、そのインポートされたルールがすべてのシステム提供侵入ポリシーに含まれていたことを示しています。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。</p>
Details	<p>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。</p>
Count	<p>各レコードのカウント(1)。テーブルが制限されており、[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 [Count] フィールドが表示されます。</p>

地理位置情報データベースの更新

ライセンス:すべて

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データのデータベースです。ASA FirePOWER モジュールでは、国および大陸を使用できます。システムで、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地理情報を表示することができます。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、[Geolocation Updates] ページ ([Configuration] > [ASA FirePOWER Configuration] > [Geolocation Updates]) を使用します。GeoDB の更新をアップロードすると、このページに表示されます。

インストールには通常 30 ~ 40 分かかります。GeoDB の更新は他のシステムの機能 (実行中の地理情報の収集など) を中断することはありませんが、更新が完了するまでシステムのリソースを消費します。更新を計画する場合には、この点について考慮してください。

この項では、手動による GeoDB 更新を計画および実行する方法について説明します。自動更新機能を利用して GeoDB の更新をスケジュールすることもできます。詳細については、[位置情報データベースの更新の自動化\(41-5 ページ\)](#)を参照してください。

地理情報データベースを更新する方法:

- ステップ 1 [Configuration] > [ASA FirePOWER Configuration] > [Updates]の順に選択します。
[Product Updates] ページが表示されます。
- ステップ 2 [Geolocation Updates]タブをクリックします。
[Geolocation Updates] ページが表示されます。
- ステップ 3 更新をアップロードします。
 - ASA FirePOWER モジュールがインターネットにアクセスできる場合は、[Download and install geolocation update from the Support Site] をクリックして、サポートサイトのいずれかで最新の更新を確認します。
 - Sourcefire: (<https://support.sourcefire.com/>)
 - シスコ: (<http://www.cisco.com/cisco/web/support/index.html>)
 - ASA FirePOWER モジュールがインターネットにアクセスできない場合は、以下のサポートサイトのいずれかから更新を手動でダウンロードして、[Upload and install geolocation update] をクリックします。[Choose File] をクリックして、その更新に移動して選択し、[Import] をクリックします。
 - Sourcefire: (<https://support.sourcefire.com/>)
 - シスコ: (<http://www.cisco.com/cisco/web/support/index.html>)



(注) 手動で、または [Geolocation Updates] ページで [Download and install geolocation update from the Support Site] 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、ファイルが破損することがあります。

更新プロセスが開始されます。更新インストールの平均時間は 30 ~ 40 分です。更新の進捗は、タスクキュー ([Monitoring] > [ASA FirePOWER Monitoring] > [Task Status]) でモニタできます。

ステップ 4 更新が終了したら、[Geolocation Updates] ページに戻り、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 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。展開全体で GeoDB の更新が有効になるには数分かかることがあります。更新した後にアクセスコントロールポリシーを再適用する必要はありません。
