



ASA FirePOWER モジュール ソフトウェアの更新

シスコでは、ルールの更新や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

この項では、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の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、を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、次の各項を参照してください。

- [更新のタイプについて \(43-1 ページ\)](#)
- [ソフトウェア更新の実行 \(43-2 ページ\)](#)
- [ソフトウェアアップデートのアンインストール \(43-7 ページ\)](#)
- [脆弱性データベースの更新 \(43-8 ページ\)](#)
- [ルールの更新とローカルルールファイルのインポート \(43-10 ページ\)](#)
- [位置情報データベースの更新 \(43-21 ページ\)](#)

更新のタイプについて

ライセンス:任意

シスコでは、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 \(39-1 ページ\)](#) および [再帰的なルール更新の使用 \(43-14 ページ\)](#) を参照してください。

表 43-1 ASA FirePOWER モジュールの更新タイプ

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
パッチの適用	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)。	はい	はい
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)。	はい	はい
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 1 桁目または 2 桁目に変更されます)。	いいえ	いいえ
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データベースに影響します。	はい	いいえ
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。	はい	いいえ
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。	はい	いいえ

ただし、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、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ません。を、FireSIGHT システムの新しいメジャーバージョンおよび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。

ソフトウェア更新の実行

ライセンス:任意

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**。その後更新を開始することができます。更新が正常に終了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\(43-3 ページ\)](#)
- [更新プロセスについて\(43-3 ページ\)](#)
- [ASA FirePOWER モジュールソフトウェアの更新\(43-5 ページ\)](#)
- [メジャーな更新のステータスのモニタリング\(43-7 ページ\)](#)

更新の計画

ライセンス:任意

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が記載されています。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

適切なソフトウェア バージョンを実行していることを確認してください。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 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。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。

設定のバックアップのガイドライン

シスコでは、メジャーな更新を開始する前に、ASA FirePOWER モジュール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、それらのバックアップを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があります。[バックアップと復元の使用 \(45-1 ページ\)](#) 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の調査 およびトラフィック フロー、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、シスコ では、保守を行っている間、または中断が及ぼす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:任意

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。

[製品アップデート (Product Updates)] ページ ([設定 (Configuration)] > [ASA FirePOWER 設定 (ASA FirePOWER Configuration)] > [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、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 アップデートのアンインストール \(43-7 ページ\)](#) を参照してください。このページには VDB の更新も一覧表示されます。



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 \(39-7 ページ\)](#) 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、次の機能に影響を及ぼすことがあります。

- 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 トラフィック中断の動作と期間は、ASA FirePOWER モジュール の設定方法と展開方法、およびASA FirePOWER モジュール が再起動されるかどうかに応じて異なります。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。

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、ASA FirePOWER モジュール を使用して、更新のモニタリング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 ASA FirePOWER モジュール を使用することを阻止するとともに、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 インターフェイスは合理化されています。タスク キュー([モニタリング(Monitoring)]>[ASA FirePOWER モニタリング(ASA FirePOWER Monitoring)]>[タスクのステータス(Task Status)])で、マイナーな更新の進行状況をモニタできます。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。

マイナーな更新であっても、更新プロセス中は ASA FirePOWER モジュール を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、これは予想される動作です。



注意

(更新に失敗した場合や、[更新ステータス(Update Status)] ページを手動更新しても進捗が表示されない場合など)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**。

更新後に行う最も重要なタスクは、アクセス コントロール ポリシーを再適用することです。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:任意

更新のタイプ、および ASA FirePOWER モジュール がインターネットへアクセスできるかどうかに応じて、ASA FirePOWER モジュール ソフトウェアを次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 ヘアアップロードすることもできます。ASA FirePOWER モジュール がインターネットにアクセスできない場合や、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させます。

更新前のタスクには、たとえば、次のような項目の確認が含まれます。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か、更新を実行するための十分な空きディスク領域があるか、更新を実行するために十分な時間を確保しているか、設定データをバックアップしたか。

ステップ 2 更新をアップロードします。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応じて、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において、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、**[設定 (Configuration)] > [ASA FirePOWER の設定 (ASA FirePOWER Configuration)] > [更新 (Updates)]** を選択し、**[アップデートのダウンロード (Download Updates)]** をクリックして、次のサポート 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>)
- 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>)
- **[設定 (Configuration)] > [ASA FirePOWER 設定 (ASA FirePOWER Configuration)] > [更新 (Updates)]** の順に選択し、**[アップデートのアップロード (Upload Update)]** をクリックします。**[ファイルの選択 (Choose File)]** をクリックし、更新を選択して **[アップロード (Upload)]** をクリックします。



(注) [製品アップデート (Product Updates)] タブで [アップデートのダウンロード (Download Updates)] 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。

更新がアップロードされます。

ステップ 3 [モニタリング (Monitoring)] > [ASA FirePOWER モニタリング (ASA FirePOWER Monitoring)] > [タスクのステータス (Task Status)] を選択してタスク 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。

更新の開始時に実行中だったタスクは停止され、再開できません。これらのタスクは更新の完了後にタスク 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。実行時間の長いタスクがある場合は、それらが完了するまで待ってから、更新を開始する必要があります。

ステップ 4 [設定 (Configuration)] > [ASA FirePOWER 設定 (ASA FirePOWER Configuration)] > [更新 (Updates)] を選択します。
[製品アップデート (Product Updates)] ページが表示されます。

ステップ 5 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。

更新プロセスが開始されます。更新をモニタする方法は、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は、タスク キュー ([モニタリング (Monitoring)] > [ASA FirePOWER モニタリング (ASA FirePOWER Monitoring)] > [タスクのステータス (Task Status)]) で、更新の進行状況をモニタできます。
- メジャーな更新の場合は、タスク キューで更新の進捗のモニタリングを開始できます。ただし、ASA FirePOWER モジュールによる更新前の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、[アップグレード ステータス (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モニタリング \(43-7 ページ\)](#)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 モジュールを使用しないでください。必要な場合は、ASA FirePOWER モジュールを再起動してください。詳細については、[更新時の ASA FirePOWER モジュールの使用 \(43-4 ページ\)](#)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 サイトの利用可能なルール更新が、ASA FirePOWER モジュールで使用している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、[ルールの更新とローカルルール ファイルのインポート \(43-10 ページ\)](#)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ずに通過する可能性があります。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 サイトの利用可能な VDB が、最も新たにインストールした VDB よりも新しい場合は、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ずに通過する可能性があります。詳細については、[脆弱性データベースの更新 \(43-8 ページ\)](#)を参照してください。

メジャーな更新のステータスのモニタリング

ライセンス:任意

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に、簡潔なインターフェイスが提供されます。この簡潔なインターフェイスでは、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。更新の進行状況のモニタリングは、タスク キュー([モニタリング (Monitoring)]>[ASA FirePOWER モニタリング (ASA FirePOWER Monitoring)]>[タスクのステータス (Task Status)])で開始できます。ただし、ASA FirePOWER モジュールが更新前の必要なチェックを完了すると、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(簡潔な更新ページが表示されます)。

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、現在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、[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。

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。



注意

更新で他の問題が生じた場合(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)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。

更新が完了すると、ASA FirePOWER モジュールは正常終了メッセージを表示し、再起動します。ASA FirePOWER モジュールの再起動が完了したら、更新後の必須手順を完了させます。

ソフトウェアアップデートのアンインストール

ライセンス:任意

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、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シスコ ソフトウェアのバージョンは、更新パスに応じて異なります。たとえば、バージョン 5.0 からバージョン 5.0.0.2 に直接更新した場合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ていなくても、バージョン 5.0.0.1 が残ります。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)

メジャーな更新では、アンインストール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、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。

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、トラフィックのインスペクションとトラフィック フロー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、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。

パッチまたは機能の更新をアンインストールするには、次の手順を実行します。

ステップ 1 [設定 (Configuration)] > [ASA FirePOWER 設定 (ASA FirePOWER Configuration)] > [更新 (Updates)] の順に選択します。

[製品アップデート (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 を再起動します。

アンインストール プロセスが開始されます。タスク キュー ([モニタリング (Monitoring)] > [ASA FirePOWER モニタリング (ASA FirePOWER Monitoring)] > [タスクのステータス (Task Status)]) で、進行状況をモニタできます。



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。必要な場合は、ASA FirePOWER モジュール を起動してください。詳細については、[更新時の ASA FirePOWER モジュールの使用 \(43-4 ページ\)](#) 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:任意

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、[製品アップデート (Product Updates)] ページを使用します。



(注)

検出の更新とともに VDB アップデート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リング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には、次の手順を実行します。

-
- 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、更新でが含まれています。
- ステップ 2** **[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [更新(Updates)]** の順に選択します。
[製品アップデート(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、**[アップデートのダウンロード(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 **[アップデートのアップロード(Upload Update)]** をクリックします。**[ファイルの選択(Choose File)]** をクリックして、その更新に移動して選択し、**[アップロード(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) 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。

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。
[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。
- ステップ 5** **[インストール(Install)]** をクリックします。



注意 更新プロセスが開始されます。タスク キュー (**[モニタリング(Monitoring)] > [ASA FirePOWER モニタリング(ASA FirePOWER Monitoring)] > [タスクのステータス(Task Status)]**) で、更新の進行状況をモニタできます。更新で問題が発生した場合(更新に失敗したことがタスク キューに示されている場合など)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。

VDB の更新を有効にするには、失効したアクセス 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。

ルールの更新とローカルルールファイルのインポート

ライセンス:任意

新しい脆弱性が判明すると、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ます。ルール更新を実装するには、最初にそれを 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 ポリシー、ネットワーク分析ポリシー、侵入ポリシーを適用します。

ルール更新は累積されていくので、シスコで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ことがあるので、ルール更新をダウンロードしてインストールするプロセスが、各自のセキュリティ ポリシーに合致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もあるため、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。

ルールの更新によって以下が提供される場合があります。

- 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。

ルールの更新がポリシーを変更するタイミングについて

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。

- システム付属:** システム付属のネットワーク分析ポリシーと侵入ポリシーへの変更、およびアクセス コントロールの詳細設定への変更は、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 ポリシーごとを実装) 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**。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 \(16-4 ページ\)](#) を参照してください。

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、ポリシーとキャッシュされている変更が表示されます。詳細については、[競合の解決とポリシー変更の確定 \(15-15 ページ\)](#) 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。これは、ルールの更新によってシステムにより提供される基本ポリシーが変更されることを許可する場合に特に役立ちます。

- アクセス コントロール ポリシーを再適用すると、関連する ネットワーク分析ポリシーと ファイル 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更新されます。ネットワーク分析ポリシーを単独で適用することはできないため、ネットワーク分析ポリシーでプリプロセッサ設定を更新する場合は、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**。
- 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。侵入ポリシーをアクセス コントロール ポリシーとともに再適用することができます。または、侵入ポリシーのみを適用して、他のアクセス コントロールの設定を更新することなく侵入ルールを更新することができます。

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は、インポート後に初めてアクセス コントロールまたは侵入ポリシーを適用したときに、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 packets が検査されずに通過することがあります。要件、他の影響、および推奨事項など、アクセス コントロール ポリシーおよび侵入ポリシーの適用の詳細については、[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、以下を参照してください。

- [ワンタイム ルール更新の使用 \(43-11 ページ\)](#) 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 \(43-14 ページ\)](#) 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して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 \(43-16 ページ\)](#) 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 \(43-17 ページ\)](#) 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:任意

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 \(43-12 ページ\)](#) 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。
- [自動ワンタイム ルール更新の使用 \(43-13 ページ\)](#) では、自動機能を使用してサポート 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:任意

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役立ちます。

手動でルール更新をインポートするには、次の手順を実行します。

-
- 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** [ダウンロード(Download)] をクリックし、[ルール(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。
- ルールの更新は累積されます。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。
- 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** [設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [更新(Updates)] の順に選択し、[ルールの更新(Rule Updates)] タブを選択します。の順に選択します。[ルールのアップデート(Rule Updates)] ページが表示されます。



ヒント

[ルール エディタ (Rule Editor)] ページ([設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [侵入ポリシー(Intrusion Policy)] > [ルール エディタ (Rule Editor)]) で [ルールのインポート (Import Rules)] をクリックすることもできます。

- ステップ 6** 必要に応じて、[すべてのローカルルールを削除(Delete All Local Rules)] をクリックして、[OK] をクリックし、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削除済みフォルダに移動します。詳細については、[カスタム ルールの削除\(27-109 ページ\)](#) を参照してください。
- ステップ 7** [アップロードおよびインストールするルールアップデートまたはテキスト ルール ファイル (Rule Update or text rule file to upload and install)] を選択し、[ファイルの選択(Choose File)] をクリックして、ルール更新ファイルに移動して選択します。
- ステップ 8** 必要に応じて、更新の完了後にポリシーを再適用します。
- 侵入ポリシーを自動的に再適用するには、[ルール更新のインポート完了後に侵入ポリシーを再適用する (Reapply intrusion policies after the rule update import completes)] を選択します。他のアクセス コントロールの設定を更新せずに、ルールと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は、このオプションだけを選択します。侵入ポリシーをアクセス コントロール ポリシーとともに再適用するには、このオプションを選択する **必要があります**。この場合、アクセス コントロール ポリシーを再適用しても、完全な適用は実行されません。
 - アクセス コントロール ポリシーとそれに関連するネットワーク分析ポリシーおよびファイル ポリシーを自動的に再適用し、侵入ポリシーを再適用しない場合は、[ルール更新のインポート完了後にアクセス コントロール ポリシーを再適用する (Reapply access control policies after the rule update import completes)] を選択します。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。ネットワーク分析ポリシーを親のアクセス コントロール ポリシーから切り離して適用することはできないため、ネットワーク分析ポリシーでプリプロセッサ設定を更新する場合は、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**。

ステップ 9 [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。[ルール アップデートのインポート ログ (Rule Update Import Log)] 詳細ビューについて (43-20 ページ) を参照してください。また、システムは前の手順で指定した通りに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 (23-8 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。

自動ワнтаイムルール更新の使用

ライセンス:任意

次の手順では、サポートサイトに自動的に接続して、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には、次の手順を実行します。

ステップ 1 [設定 (Configuration)] > [ASA FirePOWER 設定 (ASA FirePOWER Configuration)] > [更新 (Updates)] の順に選択し、[ルールの更新 (Rule Updates)] タブを選択します。の順に選択します。[ルールのアップデート (Rule Updates)] ページが表示されます。



ヒント

[ルール エディタ (Rule Editor)] ページ ([設定 (Configuration)] > [ASA FirePOWER 設定 (ASA FirePOWER Configuration)] > [ポリシー (Policies)] > [侵入ポリシー (Intrusion Policy)] > [ルール エディタ (Rule Editor)]) で [ルールのインポート (Import Rules)] をクリックすることもできます。

ステップ 2 必要に応じて、[すべてのローカルルールを削除 (Delete All Local Rules)] をクリックして、[OK] をクリックし、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削除済みフォルダに移動します。詳細については、[カスタムルールの削除 \(27-109 ページ\)](#) を参照してください。

ステップ 3 [サポートサイトから新しいルールアップデート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 4 必要に応じて、更新の完了後にポリシーを再適用します。

- 侵入ポリシーを自動的に再適用するには、[ルール更新のインポート完了後に侵入ポリシーを再適用する (Reapply intrusion policies after the rule update import completes)] を選択します。他のアクセスコントロールの設定を更新せずに、ルールと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は、このオプションだけを選択します。侵入ポリシーをアクセスコントロールポリシーとともに再適用するには、このオプションを選択する **必要があります**。この場合、アクセスコントロールポリシーを再適用しても、完全な適用は実行されません。
- アクセスコントロールポリシー、ネットワーク分析ポリシー、およびファイルポリシーを自動的に再適用し、侵入ポリシーを再適用しない場合は、[ルール更新のインポート完了後にアクセスコントロールポリシーを再適用する (Reapply access control policies after the rule update import completes)] を選択します。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。ネットワーク分析ポリシー

を親のアクセス コントロール ポリシーから切り離して適用することはできないため、ネットワーク分析ポリシーでプリプロセッサ設定を更新する場合は、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**。

ステップ 5 [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。[\[ルール アップデートのインポート ログ \(Rule Update Import Log\)\] 詳細ビューについて \(43-20 ページ\)](#) を参照してください。また、システムは前の手順で指定した通りに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 \(23-8 ページ\)](#) 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:任意

[ルールのアップデート (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該当するサブタスクは、ダウンロード、インストール、ベース ポリシーの更新、ポリシーの再適用の順序で実行されます。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。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だけ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には、次の手順を実行します。

ステップ 1 [設定 (Configuration)] > [ASA FirePOWER 設定 (ASA FirePOWER Configuration)] > [更新 (Updates)] の順に選択し、[ルールの更新 (Rule Updates)] タブを選択します。の順に選択します。
[ルールのアップデート (Rule Updates)] ページが表示されます。



ヒント

[ルール エディタ (Rule Editor)] ページ([設定 (Configuration)] > [ASA FirePOWER 設定 (ASA FirePOWER Configuration)] > [ポリシー (Policies)] > [侵入ポリシー (Intrusion Policy)] > [ルール エディタ (Rule Editor)]) で [\[ルールのインポート \(Import Rules\)\]](#) をクリックすることもできます。

ステップ 2 必要に応じて、[すべてのローカルルールを削除 (Delete All Local Rules)] をクリックして、[OK] をクリックし、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削除済みフォルダに移動します。詳細については、[カスタムルールの削除 \(27-109 ページ\)](#) を参照してください。

ステップ 3 [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)] を選択します。

ページが展開され、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。[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。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、[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 ボックスをオフにして [保存 (Save)] をクリックします。

ステップ 4 [インポート頻度 (Import Frequency)] フィールドで、ドロップダウンリストから [日次 (Daily)]、[週次 (Weekly)]、または [月次 (Monthly)] を選択します。

インポート間隔として週次または月次を選択した場合は、表示されるドロップダウンリストで、ルールの更新をインポートする曜日または日付を選択します。選択項目をクリックするか、または選択項目の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 [インポート頻度 (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 必要に応じて、更新の完了後にポリシーを再適用します。

- 侵入ポリシーを自動的に再適用するには、[ルール更新のインポート完了後に侵入ポリシーを再適用する (Reapply intrusion policies after the rule update import completes)] を選択します。他のアクセス コントロールの設定を更新せずに、ルールと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は、このオプションだけを選択します。侵入ポリシーをアクセス コントロール ポリシーとともに再適用するには、このオプションを選択する **必要があります**。この場合、アクセス コントロール ポリシーを再適用しても、完全な適用は実行されません。
- アクセス コントロール ポリシーとネットワーク分析ポリシーおよびファイル ポリシーを自動的に再適用し、侵入ポリシーを再適用しない場合は、[ルール更新のインポート完了後にアクセス コントロール ポリシーを再適用する (Reapply access control policies after the rule update import completes)] を選択します。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。ネットワーク分析ポリシーを親のアクセス コントロール ポリシーから切り離して適用することはできないため、ネットワーク分析ポリシーでプリプロセス設定を更新する場合は、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**。

ステップ 7 [保存 (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。

[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。予定時刻になると、前の手順で指定した通りにシステムはルールの更新をインストールし、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 \(23-8 ページ\)](#) を参照してください。

インポート前やインポート中は、ログオフすることも、他のタスクを実行することもできます。インポート中に [ルールアップデート 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、[ルールアップデート 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。詳細については、[ルール更新ログの表示 \(43-17 ページ\)](#) 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:任意

ローカルルールは、ASCII または UTF-8 エンコードのプレーン テキスト ファイルとしてローカル マシンからインポートされるカスタムの 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。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、[ルール エディタ (Rule Editor)] ページを表示し、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、ルールの横にある [編集 (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 と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することで、削除したローカルルールを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。

削除したローカルルールのリビジョン番号を表示するには、[ルール エディタ (Rule Editor)] ページを表示し、削除したルールのカテゴリをクリックしてフォルダを展開し、ルールの横にある [編集 (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。
- インポートしたローカルルールのステータスは常に無効に設定されます。これらのローカルルールを侵入ポリシーで使用するには、事前に手動でそのステータス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 \(24-21 ページ\)](#) 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、単一のシャープ文字(#)で始まるローカルルールをインポートします。
- また、二重のシャープ文字(##)で始まるローカルルールは無視し、インポートしません。
- 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。詳細については、[イベントしきい値の設定 \(24-23 ページ\)](#) 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には、次の手順を実行します。

ステップ 1 [設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [更新(Updates)] の順に選択し、[ルールの更新(Rule Updates)] タブを選択します。

[ルールのアップデート(Rule Updates)] ページが表示されます。

ステップ 2 [アップロードおよびインストールするルール アップデートまたはテキスト ルール ファイル(Rule Update or text rule file to upload and install)] を選択し、[ファイルの選択(Choose File)] をクリックして、ルール ファイルに移動します。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

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 ファイルのみをインポートできます。

ステップ 3 [インポート(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、ユーザの侵入ポリシーが適用され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:任意

ASA FirePOWER モジュールは、インポートされたルール更新と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 ログ(Rule Update Log)] で実行できる操作を次の表で説明します。

表 43-2 [ルール アップデート ログ(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	[ルール アップデート ログ(Rule Update Log)] の表について(43-18 ページ)で詳細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。

表 43-2 [ルールアップデートログ(Rule Update Log)] のアクション(続き)

目的	操作
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、次の各項を参照してください。

- [ルールアップデートログ(Rule Update Log)] の表について(43-18 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。
- [ルールアップデートのインポートログ(Rule Update Import Log)] の詳細の表示(43-19 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。
- [ルールアップデートのインポートログ(Rule Update Import Log)] 詳細ビューについて(43-20 ページ)では、[ルールアップデートログ(Rule Update Log)] 詳細ビューの各フィールドについて説明します。

[ルールアップデートログ(Rule Update Log)] を表示するには、次の手順を実行します。

- ステップ 1** [設定 (Configuration)] > [ASA FirePOWER 設定 (ASA FirePOWER Configuration)] > [更新 (Updates)] の順に選択し、[ルールの更新 (Rule Updates)] タブを選択します。の順に選択します。
[ルールのアップデート (Rule Updates)] ページが表示されます。



ヒント

[ルール エディタ (Rule Editor)] ページ([設定 (Configuration)] > [ASA FirePOWER 設定 (ASA FirePOWER Configuration)] > [ポリシー (Policies)] > [侵入ポリシー (Intrusion Policy)] > [ルール エディタ (Rule Editor)]) で [ルールのインポート (Import Rules)] をクリックすることもできます。

- ステップ 2** [ルールアップデートログ (Rule Update Log)] をクリックします。
[ルールアップデートログ (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。

[ルールアップデートログ (Rule Update Log)] の表について

ライセンス:任意

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 43-3 [ルールアップデートログ(Rule Update Log)] のフィールド

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。

表 43-3 [ルールアップデートログ(Rule Update Log)] のフィールド(続き)

フィールド	説明
ステータス (Status)	<p>インポートの状態を表します</p> <ul style="list-style-type: none"> 正常終了 (🟢) 失敗、または実行中 (🔴) <p>ヒント 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。</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 [ルールアップデートログ (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。

[ルールアップデートのインポートログ (Rule Update Import Log)] の詳細の表示

ライセンス:任意

[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。

次の表では、[ルールアップデートのインポートログ (Rule Update Import Log)] 詳細ビューので実行できる特定のアクションについて説明します。

表 43-4 [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	[ルールアップデートのインポートログ (Rule Update Import Log)] 詳細ビューについて(43-20 ページ) で詳細を参照してください。

[ルールアップデートのインポートログ (Rule Update Import Log)] 詳細ビューを表示するには、次の手順を実行します。

- ステップ 1 [設定 (Configuration)] > [ASA FirePOWER 設定 (ASA FirePOWER Configuration)] > [更新 (Updates)] の順に選択し、[ルールの更新 (Rule Updates)] タブを選択します。の順に選択します。[ルールのアップデート (Rule Updates)] ページが表示されます。



ヒント [ルールエディタ (Rule Editor)] ページ([設定 (Configuration)] > [ASA FirePOWER 設定 (ASA FirePOWER Configuration)] > [ポリシー (Policies)] > [侵入ポリシー (Intrusion Policy)] > [ルールエディタ (Rule Editor)]) で [ルールのインポート (Import Rules)] をクリックすることもできます。

- ステップ 2 [ルール アップデート ログ (Rule Update Log)] をクリックします。
 [ルール アップデート ログ (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。

[ルール アップデートのインポート ログ (Rule Update Import Log)] 詳細ビューについて

ライセンス:任意

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、[ルール アップデート ログ (Rule Update Log)] 詳細ビューのフィールドについて説明します。

表 43-5 [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
時刻 (Time)	インポートが開始された日時。
[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、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。
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。 <ul style="list-style-type: none"> [ルール更新コンポーネント (rule update component)] (ルール バックやポリシー バ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侵入ポリシーを再適用する (Reapply intrusion policies after the rule update import completes)] オプションが有効だった場合)
アクション (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。 <ul style="list-style-type: none"> [新規 (new)] (ルール用。この ASA FirePOWER モジュール にルールが初めて格納された場合) [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。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)] (ルール更新の編集用。プリプロセッサ、ルール、またはその他の機能がシステム付属ポリシーで有効になっている場合) [無効 (disabled)] (ルール用。システム付属ポリシーでルールが無効になっている場合) [ドロップ (drop)] (ルール用。システム付属ポリシーで、ルールが [ドロップしてイベントを生成する (Drop and Generate Events)] に設定されている場合) [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侵入ポリシーを再適用する (Reapply intrusion policies after the Rule Update import completes)] オプションが有効だった場合)

表 43-5 [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(続き)

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。
GID	ルールのジェネレータ ID。例:1(標準テキストルール)、3(共有オブジェクトのルール)。
SID	ルールの SID。
Rev	ルールのリビジョン番号。
ポリシー(Policy)	インポートされたルールの場合、このフィールドには [すべて(All)] が表示されます。これは、そのルールがすべてのシステム付属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。
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。
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 [Count] フィールドが表示されます。

位置情報データベースの更新

ライセンス:任意

シスコ位置情報データベース(GeoDB)は、ルート可能な IP アドレスに関連する位置情報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。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。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、[位置情報の更新(Geolocation Updates)] ページを使用します([設定(Configuration)]>[ASA FirePOWER 設定(ASA FirePOWER Configuration)]>[更新(Updates)]>[位置情報の更新(Geolocation Updates)])。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。

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。

この項では、手動による GeoDB の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\(39-6 ページ\)](#)を参照してください。

位置情報データベースを更新するには、次の手順を実行します。

ステップ 1 [設定(Configuration)]>[ASA FirePOWER 設定(ASA FirePOWER Configuration)]>[更新(Updates)]の順に選択します。

[製品アップデート(Product Updates)] ページが表示されます。

ステップ 2 [位置情報の更新(Geolocation Updates)] タブをクリックします。

[位置情報の更新(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、[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)] をクリックして、以下のサポート 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、[位置情報の更新をアップロードおよびインストールする (Upload and install geolocation update)] をクリックします。[ファイルの選択 (Choose File)] をクリックして、その更新に移動して選択し、[インポート (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) [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。

更新プロセスが開始されます。更新のインストールには、平均で 30 ~ 40 分かかります。タスクキュー ([モニタリング (Monitoring)] > [ASA FirePOWER モニタリング (ASA FirePOWER Monitoring)] > [タスクのステータス (Task Status)]) で、更新の進行状況をモニタできます。

ステップ 4 更新が終了したら [位置情報の更新 (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。