システムソフトウェアの更新

シスコは、システム ソフトウェア本体のメジャーおよびマイナー更新に加えて、ルールの更新や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 この章では、FireSIGHT 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。VDB、GeoDB、侵入ルールなど、FireSIGHT システム のいずれかの部分を更新する前に、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。

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。

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

ライセンス：任意（Any）

シスコは、システム ソフトウェア本体のメジャーおよびマイナー更新に加えて、侵入ルールの更新や VDB 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（62-1 ページ）および再帰的なルール更新の使用（66-21 ページ）を参照してください。

表 66-1　FireSIGHT システム更新のタイプ

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
FireSIGHT システム へのパッチの適用	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 桁目が変更されます)。	Yes	Yes
FireSIGHT 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、5.4.1 のようにバージョン番号の 3 桁目が変更されます)。	Yes	Yes
FireSIGHT システム の主要な更新(メジャーおよびマイナー バージョン リリース)	主要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、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 桁目が変更されます)。	No	No
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、およびクライアントによって検出された脆弱性、および FireSIGHT 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
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
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。 DC500 防御センター はこの機能をサポートしません。	Yes	No

ただし、FireSIGHT システム の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、および侵入ルールの主要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、FireSIGHT システム の新しいメジャーバージョンに更新した場合、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(Any)

FireSIGHT 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 防御センター をすべて更新し、次にこれら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。

詳細については、次の項を参照してください。

更新の計画

ライセンス：任意（Any）

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。

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。

FireSIGHT システム バージョン要件

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、FireSIGHT 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。仮想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、『*FireSIGHT システムVirtual Installation Guide*』を参照してください。Blue Coat X-Series 向け Cisco NGIPS 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、『*Blue Coat X-Series 向け Cisco NGIPS 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、防御センター 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

シスコでは、主要な（メジャーな）更新を開始する前に、バックアップを外部の場所へコピーし、アプライアンス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。また、更新のタイプに関係なく、現行のイベントおよび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。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**。

防御センター を使用して、それ自身、および管理対象のイベントと設定データをバックアップすることができます。バックアップと復元の使用（70-1 ページ）を参照してください。

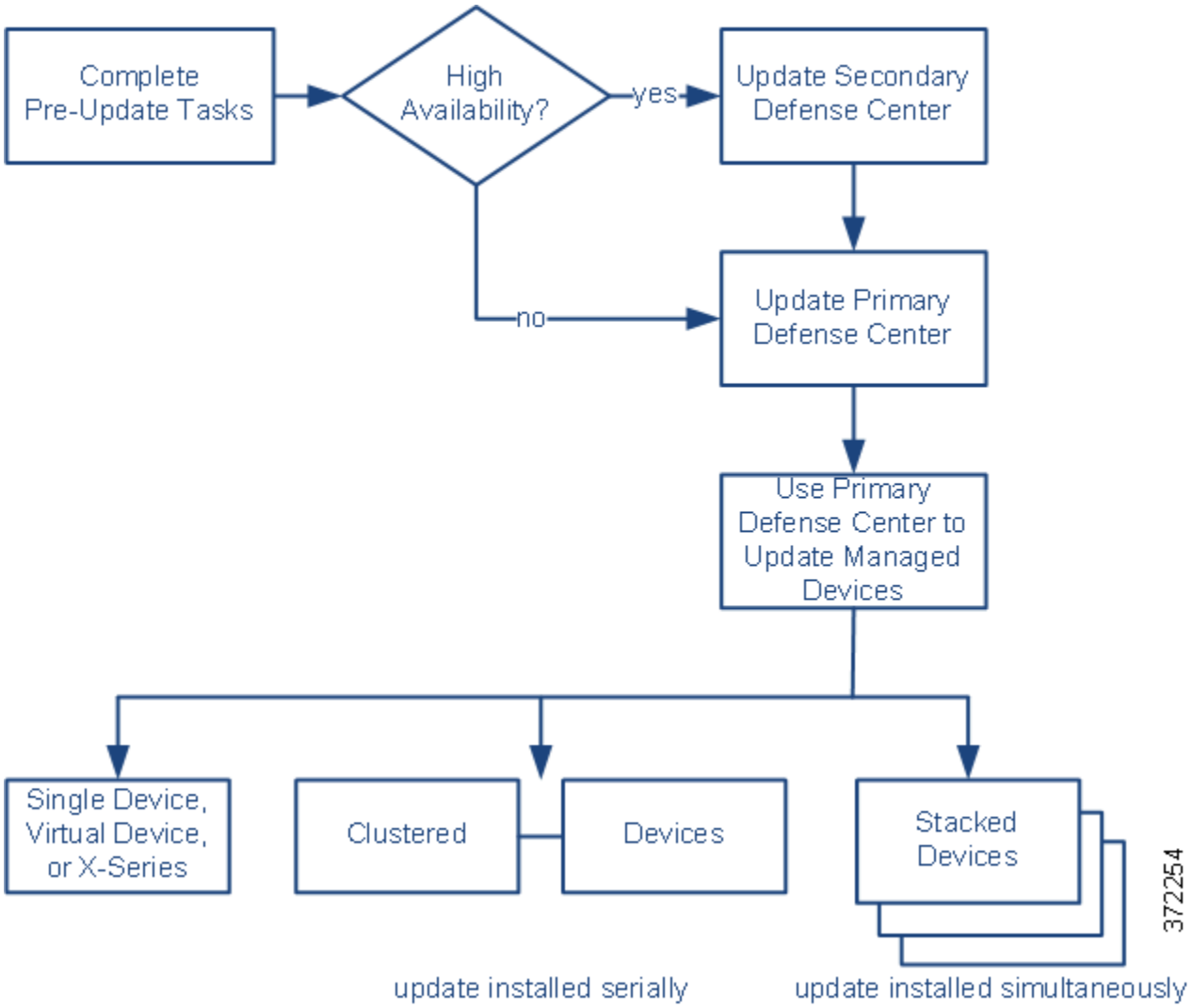
更新を実行するタイミング

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 ステートに影響を与えることがあり、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：任意（Any）

次の図は、更新プロセスの概要を示しています。



更新の順序

使用している 防御センター 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**。

防御センターを使用した更新の実行

シスコでは、防御センター の Web インターフェイスを使用して、それ自身だけでなく、管理対象のデバイスも更新することを推奨しています。仮想デバイスや Blue Coat X-Series 向け Cisco NGIPS など、Web インターフェイスを持たない管理対象デバイスを更新するには、防御センターを使用する**必要があります**。Blue Coat X-Series 向け Cisco NGIPS に対するメジャーな更新では、前のバージョンをアンインストールしてから新しいバージョンをインストールする必要がある場合もあります。詳細については、『*Blue Coat X-Series 向け Cisco NGIPS Installation Guide*』を参照してください。

[製品の更新(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。ソフトウェア アップデートのアンインストール(66-12 ページ)を参照してください。防御センター で、ページに VDB 更新を表示できます。

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(62-12 ページ)を参照してください。

ペアの 防御センター の更新

高可用性ペアの片方の 防御センター の更新を開始すると、もう一方の 防御センター がプライマリになります(まだプライマリになっていなかった場合)。また、ペアの 防御センター が設定情報の共有を停止し、ペアの 防御センター は通常の同期プロセスの一環としてソフトウェア更新を受信しません。

運用の継続性を保証するには、ペアの 防御センター を同時に更新**しないでください**。まず、セカンダリ 防御センター の更新手順を完了してからプライマリを更新してください。

クラスタ デバイスの更新

クラスタ デバイスまたはクラスタ 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。次に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、同じプロセスに従います。

クラスタ スタックのデバイスを更新するには、クラスタのすべてのメンバー上で同時に、管理している 防御センター から更新を実行する必要があります。デバイスから更新を直接実行することはできません。

スタック構成デバイスの更新

スタック構成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バージョンが混在する制限付き状態で動作します。
- 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(スイッチング、ルーティング、および関連する機能を含む)
- 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 FireSIGHT 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　クラスタ 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、更新の監視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監視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。タスク キュー（[システム（System）] > [モニタリング（Monitoring）] > [タスクのステータス（Task Status）]）でマイナーな更新の進捗を監視することができます。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監視するには、防御センター でタスク キューを使用します。

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 インターフェイスが使用不可になるか、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。そのような場合は、もう一度ログインしてタスク キューを表示します。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 回再起動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、タスク キューの手動更新または [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**。

更新後に行う最も重要なタスクは、防御センター を更新した後と、管理対象デバイスを更新した後の両方で、アクセス コントロール ポリシーを再適用することです。

注意　アクセス コントロール ポリシーの適用時に、リソース需要が生じる結果として、少数のパケットがインスペクションなしでドロップされることがあります。さらに、構成の一部を適用するときに、Snort プロセスの再開が要求され、これにより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。アクセス コントロール ポリシーの適用（12-17 ページ）および Snort プロセスを再開する構成（1-8 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
- 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

防御センター の更新

ライセンス: 任意（Any）

更新のタイプ、および 防御センター がインターネットへアクセスできるかどうかによって、防御センター を次のいずれかの方法で更新します。

- 防御センター がインターネットにアクセスできる場合は、防御センター を使用して、サポート サイトから直接更新を取得します。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 サイトから更新を手動でダウンロードして、防御センターへアップロードすることもできます。防御センター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。

注意　操作の継続性を保証するために、ペアの 防御センター を同時に更新**しないでください**。ペアの防御センター の更新（66-5 ページ）を参照してください。

メジャーな更新の場合は、防御センターを更新すると、以前の更新のアンインストーラが削除されます。

防御センター を更新する方法:

アクセス: 管理

手順 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。

更新前のタスクとして、防御センター 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こと、更新を実行するための十分な空きディスク領域があること、更新を実行するための十分な時間を確保していること、イベントおよび設定データをバックアップしたことなどを確認します。

手順 2　防御センター に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、および防御センター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、防御センター がインターネットにアクセスできる場合は、[システム（System）] > [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、最新の更新をチェックします。メジャーな更新の場合、または 防御センター がインターネットにアクセスできない場合は、最初に更新を手動でダウンロードする必要があります。次のサポート サイトのいずれかから更新をダウンロードします。
  - **すべての Sourcefire の更新:**（https://support.sourcefire.com/）
  - **シスコの更新**:

Physical Defense Center
(http://software.cisco.com/download/navigator.html?mdfid=278875421)
Virtual Defense Center_
(http://software.cisco.com/download/type.html?mdfid=286259687&catid=null)

- [システム(System)] > [更新(Updates)] を選択して [アップデートのアップロード(Upload Update)] をクリックします。更新を参照し、[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。

防御センター に更新がアップロードされます。

手順 3　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。

手順 4　[システム(System)] > [モニタリング(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。

手順 5　[システム(System)] > [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。

手順 6　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。

[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。

手順 7　防御センター を選択して [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 防御センター をリブートします。

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、FireSIGHT システム更新のタイプの表およびリリース ノートを参照してください。

- マイナーな更新については、タスク キュー([システム(System)] > [モニタリング(Monitoring)] > [タスクのステータス(Task Status)]) で更新の進捗を監視することができます。
- 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、防御センター による更新前のチェックが完了すると、ユーザはログアウトされます。再度ログインすると、[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(66-11 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、防御センター をリブートします。詳細については、更新中の Web インターフェイスの使用(66-6 ページ)を参照してください。

手順 8　更新が完了したら、必要に応じて 防御センター にログインします。

メジャーな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。

手順 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。

手順 10　[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。また、防御センター のルール更新と VDB のバージョンもメモしてください。この情報は後で必要になります。

手順 11　すべての管理対象デバイスが、防御センター と正常に通信していることを確認します。

手順 12　サポート サイトで利用可能なルール更新が、ご使用の 防御センターのルールより新しい場合は、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（66-16 ページ）を参照してください。

手順 13　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 ポリシーの適用時に、リソース需要が生じる結果として、少数のパケットがインスペクションなしでドロップされることがあります。さらに、構成の一部を適用するときに、Snort プロセスの再開が要求され、これにより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。アクセス コントロール ポリシーの適用（12-17 ページ）および Snort プロセスを再開する構成（1-8 ページ）を参照してください。

手順 14　サポート サイトで利用可能な VDB が、ご使用の 防御センター の VDB より新しい場合は、最新の VDB をインストールします。

注意　VDB の更新をインストールすると、アクセス コントロール ポリシーの適用時に 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 の再開によるトラフィックへの影響（1-9 ページ）と脆弱性データベースの更新（66-14 ページ）を参照してください。

手順 15　次の項、管理対象デバイスの更新へ進んで、防御センター が管理するデバイス上で シスコ ソフトウェアを更新します。

管理対象デバイスの更新

ライセンス：任意（Any）

シスコでは、更新後の 防御センター を使用して、管理対象のデバイスを更新することを推奨しています。仮想デバイスや Blue Coat X-Series 向け Cisco NGIPS など、Web インターフェイスを持たない管理対象デバイスを更新するには、防御センター を使用する**必要があります**。Blue Coat X-Series 向け Cisco NGIPS に対するメジャーな更新では、前のバージョンをアンインストールしてから新しいバージョンをインストールする必要がある場合もあります。

管理対象デバイスの更新は、2 段階のプロセスです。最初に、以下のいずれかのサポート サイトから更新をダウンロードし、それを管理元の 防御センター へアップロードします。

- **Sourcefire：**（https://support.sourcefire.com/）
- **シスコ：**（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)　トラフィックのインスペクション、トラフィック フロー、およびリンク状態は、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。

管理対象デバイスを更新するには、次の手順を実行します。

アクセス: 管理

手順 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。

更新前のタスクとして、管理元の 防御センター を更新し、イベントおよび設定データをバックアップします。さらにデバイスが 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こと、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、更新を実行するのに十分な空きディスク領域があること、更新を実行するための十分な時間を確保していることなどを確認します。

手順 2　デバイスの管理元の 防御センター で FireSIGHT システム ソフトウェアを更新します。防御センター の更新 (66-7 ページ) を参照してください。

手順 3　次のサポート サイトのいずれかから更新をダウンロードします。

- **すべての Sourcefire の更新:** (https://support.sourcefire.com/)
- **シスコの更新:**

```
physical managed devices:
(http://software.cisco.com/download/navigator.html?mdfid=278875421)
virtual managed devices:
(http://software.cisco.com/download/type.html?mdfid=286259690&flowid=70802)
```

デバイス モデルごとに異なる更新を使用できます。ダウンロードできる更新については、リリース ノートを参照してください。

(注)　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。

手順 4　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。

手順 5　管理元の 防御センター で、[システム (System)] > [更新 (Update)] 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。

手順 6　[更新のアップロード (Upload Update)] をクリックして、ダウンロードした更新を参照し、[アップロード (Upload)] をクリックします。

防御センター に更新がアップロードされます。[製品アップデート (Product Updates)] タブに、アップロードした更新のタイプ、バージョン番号、および生成された日付と時刻が示されます。このページには、再起動が更新の一環として必要かどうかも示されます。

手順 7　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。

[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。

手順 8　更新をインストールするデバイスを選択して [インストール (Install)] をクリックします。同じ更新を使用する場合は、複数のデバイスを一度に更新できます。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リブートします。

更新プロセスが開始されます。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。防御センター のタスク キュー（[システム（System）] > [モニタリング（Monitoring）] > [タスクのステータス（Task Status）]）で更新の進行状況を監視できます。更新中に、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、これは正常な動作です。

注意　（タスク キューに更新が失敗したことが示されている、またはタスク キューの手動更新で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。

手順 9　オプションとして、メジャーな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。

メジャーな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。

手順 10　防御センター で、[デバイス（Devices）] > [デバイス管理（Device Management）] を選択し、更新したデバイスのバージョンが記載されている正しいものであることを確認します。

手順 11　更新したデバイスが、防御センター と正常に通信していることを確認します。

手順 12　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 ポリシーの適用時に、リソース需要が生じる結果として、少数のパケットがインスペクションなしでドロップされることがあります。さらに、構成の一部を適用するときに、Snort プロセスの再開が要求され、これにより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。アクセス コントロール ポリシーの適用（12-17 ページ）および Snort プロセスを再開する構成（1-8 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（Any）

メジャーな更新では、FireSIGHT システムに備わっている簡潔な Web インターフェイスを使用して、更新プロセスを簡単に監視できます。また、この簡潔なインターフェイスを使用すると、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することを防止できます。

タスク キュー（[システム（System）] > [モニタリング（Monitoring）] > [タスク キュー（Task Queue）]）で更新の進捗の監視を開始できます。ただし、アプライアンスで更新前の必要なチェックが完了した後、このユーザおよび他のすべてのユーザが 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。

管理者の場合は、ログインし直すと、簡潔な更新ページが表示されます。

防御センター を使用して管理対象デバイスを更新する場合、シスコでは、防御センター のタスク キューから更新の進捗をモニタすることを推奨しています。ただし、アプライアンスが更新前のチェックを終了した後、デバイスのローカル Web インターフェイスへのログインを試みると、簡潔な更新ページが表示され、これを使用して更新の進捗をモニタすることができます。

このページには、更新前の FireSIGHT システム 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の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、アプライアンスで正常終了のメッセージが表示され、リブートが行われます。アプライアンスのリブートが完了した後で、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。

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（Any）

シスコ アプライアンスへ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シスコ ソフトウェアのバージョンは、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 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 を実行するアプライアンスが結果として生成される可能性があります。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、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。自分のアプライアンスを、FireSIGHT システムの新しいメジャー バージョンに更新した場合、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。

アンインストールの順序

インストールした順序と逆の順序で更新を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、その後に 防御センター 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。防御センター 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（仮想デバイスや Blue Coat X-Series 向け Cisco NGIPS 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。

このプロセスを使用して、Blue Coat X-Series 向け Cisco NGIPS のマイナーな更新をアンインストールできますが、このプロセスを使用して、X-シリーズ プラットフォームから Blue Coat X-Series 向け Cisco NGIPS アプリケーションをアンインストールすることはできないことに注意してください。詳細については、『*Blue Coat X-Series 向け Cisco NGIPS Installation Guide*』を参照してください。

クラスタ アプライアンスまたはペア アプライアンスからの更新のアンインストール

高可用性ペアのクラスタ デバイスおよび 防御センター は、同じバージョンの FireSIGHT システムを実行する必要があります。アンインストール プロセスによりフェールオーバーが自動でトリガーされますが、非対応のペアまたはクラスタ内のアプライアンスは設定情報を共有しません。また、同期の一環としては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。冗長なアプライアンスから更新をアンインストールしなければならない場合は、アンインストールを連続して実行するよう計画してください。

アンインストールによって、これらのデバイスが、クラスタ スタック非対応バージョンに戻される場合は、クラスタ スタックの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には、クラスタ デバイスとペア 防御センター から更新を 1 つずつアンインストールします。まず、セカンダリ アプライアン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 アプライアンスから更新をアンインストールします。

注意　クラスタ デバイスまたはペア 防御センター から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 FireSIGHT システムを実行する必要があります。いずれかのスタック デバイスから更新をアンインストールすると、そのスタック内のデバイスは、バージョンが混在する制限付きの状態になります。

展開への影響を最小にするために、シスコではスタック構成デバイスから更新を同時にアンインストールすることを推奨しています。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、クラスタ スタック非対応バージョンに戻される場合は、クラスタ スタックの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。これには、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の確認が含まれます。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。

ローカル Web インターフェイスを使用してパッチまたは機能の更新をアンインストールする方法:

アクセス:管理

手順 1　[システム(System)] > [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。

手順 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。

- 防御センター 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。防御センター を選択して [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。

いずれの場合も、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。

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([システム(System)] > [モニタリング(Monitoring)] > [タスクのステータス(Task Status)]) で進捗をモニタリングすることができます。

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。詳細については、更新中の Web インターフェイスの使用(66-6 ページ)を参照してください。

手順 3　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。

手順 4　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。

手順 5　[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。

手順 6　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(防御センター の場合)、または管理元の 防御センター 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。

脆弱性データベースの更新

ライセンス:任意(Any)

シスコの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、およびオペレーティング システム、クライアント、アプリケーションのフィンガープリントを格納するデータベースです。FireSIGHT 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。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、防御センター で [製品アップデート(Product Updates)] ページを使用します。サポートから取得した VDB の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 FireSIGHT システムの更新およびそのアンインストーラの更新が示されます。

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。

(注) 更新されたアプリケーション ディテクタおよび VDB 内のオペレーティング システムのフィンガープリントを有効にするには、アクセス コントロール ポリシーの再適用が必要です。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 ポリシーを管理対象デバイスに再適用します。詳細については、アクセス コントロール ポリシーの適用（12-17 ページ）を参照してください。

注意 VDB の更新をインストールすると、アクセス コントロール ポリシーの適用時に 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 の再開によるトラフィックへの影響（1-9 ページ）と脆弱性データベースの更新（66-14 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。自動更新機能を利用して VDB の更新をスケジュールすることもできます。脆弱性データベースの更新の自動化（62-17 ページ）を参照してください。

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。

アクセス：管理

手順 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。

手順 2　[システム（System）] > [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。

手順 3　防御センター に更新をアップロードします。

- 防御センター 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）
- 防御センター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。更新を参照し、[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。

防御センター に更新がアップロードされます。

手順 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。

手順 5　防御センター を選択し、[インストール(Install)] をクリックします。

更新プロセスが開始されます。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。タスク キュー([システム(System)] > [モニタリング(Monitoring)] > [タスクのステータス(Task Status)]) で更新の進行状況を監視できます。

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。(タスク キューに更新が失敗したことが示されている、またはタスク キューの手動更新で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。

手順 6　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。

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。アクセス コントロール ポリシーの適用(12-17 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(Any)

新しい脆弱性に関する情報が判明すると、シスコの脆弱性調査チーム(VRT) からルール更新がリリースされるので、これを最初に 防御センター 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管理対象デバイスに適用することで、その実装ができます。

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。展開に高可用性ペアの防御センター が含まれる場合は、プライマリ側だけに更新をインポートします。セカンダリ 防御センター は、通常の同期プロセスの一環としてルールの更新を受け取ります。

(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**。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（24-5 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。確認用に [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た変更、および変更を行ったユーザが表示されます。詳細については、競合の解決とポリシー変更の確定（23-17 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ターゲット デバイス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。

注意　アクセス コントロール ポリシーまたは侵入ポリシーの適用時に、リソース需要が生じる結果として、少数のパケットがインスペクションなしでドロップされることがあります。また、設定によっては、適用したときに Snort プロセスの再起動が必要になることがあります。これには、新しい（または更新された）共有オブジェクト ルールを含む侵入ルール更新をインポートした後、アクセス コントロール ポリシーまたは侵入ポリシーを適用する場合が含まれます。Snort プロセスを再起動すると、一時的にトラフィック 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 プロセスを再開する構成（1-8 ページ）と Snort の再開によるトラフィックへの影響（1-9 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（66-18 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（66-21 ページ）では、Web インターフェイスで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（66-22 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（66-24 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（Any）

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（66-18 ページ）では、サポート サイトからローカル マシンへ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（66-20 ページ）では、Web インターフェイスで自動機能を使用し、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：任意（Any）

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、防御センター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には、次の手順を実行します。

アクセス：管理

手順 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）

手順 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。

手順 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。

手順 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。

手順 5　アプライアンスの Web インターフェイスにログインします。

手順 6　[システム（System）] > [更新（Updates）] を選択し、[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。

ヒント　または [ルール エディタ（Rule Editor）] ページで [ルールのインポート（Import Rules）] をクリックします（[ポリシー（Policies）] > [侵入（Intrusion）] > [ルール エディタ（Rule Editor）]）。

手順 7　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（36-116 ページ）を参照してください。

手順 8　[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。

手順 9　オプションで、更新の完了後にポリシーを管理対象デバイスに再適用します。

- 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 SSL 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**。

手順 10　[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（66-28 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。アクセス コントロール ポリシーの適用（12-17 ページ）および侵入ポリシーの適用（31-9 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。

自動ワンタイム ルール更新の使用

ライセンス: 任意（Any）

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、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。

アクセス: 管理

手順 1　[システム（System）] > [更新（Updates）] を選択し、[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。

ヒント　または [ルール エディタ（Rule Editor）] ページで [ルールのインポート（Import Rules）] をクリックします（[ポリシー（Policies）] > [侵入（Intrusion）] > [ルール エディタ（Rule Editor）]）。

手順 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（36-116 ページ）を参照してください。

手順 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。

手順 4　オプションで、更新の完了後にポリシーを管理対象デバイスに再適用します。

- 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 SSL 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**。

手順 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（66-28 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。アクセス コントロール ポリシーの適用（12-17 ページ）および侵入ポリシーの適用（31-9 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（Any）

[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。展開に高可用性ペアの 防御センター が含まれる場合は、プライマリ側だけに更新をインポートします。セカンダリ 防御センター は、通常の同期プロセスの一環としてルールの更新を受け取ります。

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、再帰的インポートが設定されているアプライアンスで以前に適用されたポリシーだけであることに注意してください。

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。

アクセス：管理

手順 1　[システム（System）] > [更新（Updates）] を選択し、[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。

ヒント　または [ルール エディタ（Rule Editor）] ページで [ルールのインポート（Import Rules）] をクリックします（[ポリシー（Policies）] > [侵入（Intrusion）] > [ルール エディタ（Rule Editor）]）。

手順 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（36-116 ページ）を参照してください。

手順 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。

手順 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。

手順 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。

手順 6　オプションで、更新の完了後にポリシーを管理対象デバイスに再適用します。

- 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 SSL 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**。

手順 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。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。アクセス コントロール ポリシーの適用（12-17 ページ）および侵入ポリシーの適用（31-9 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 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（66-24 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（Any）

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([ポリシー(Policies)] > [侵入(Intrusion)] > [ルール エディタ(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([ポリシー(Policies)] > [侵入(Intrusion)] > [ルール エディタ(Rule Editor)])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(32-23 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が、これらには削除のフラグが立てられます。
- 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。

- シスコ では、SID の番号付けの問題を回避するために、高可用性ペアのプライマリ 防御センター にローカル ルールをインポートすることを強くお勧めしています。
- 非推奨の `threshold` キーワードと侵入イベントしきい値機能を組み合わせて使用しているローカル ルールをインポートして、侵入ポリシーで有効にすると、ポリシーの検証に失敗します。詳細については、イベントしきい値の設定（32-26 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。

アクセス：管理

手順 1　[ポリシー（Policies）] > [侵入（Intrusion）] > [ルール エディタ（Rule Editor）] の順に選択します。

[ルール エディタ（Rule Editor）] ページが表示されます。

手順 2　[ルールのインポート（Import Rules）] をクリックします。

[ルールのインポート（Import Rules）] ページが表示されます。

ヒント　[システム（System）] > [更新（Updates）] を選択して、[ルールの更新（Rule Updates）] タブを選択することもできます。

手順 3　[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）] を選択して [参照（Browse）] をクリックすると、ルール ファイルにナビゲートできます。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。

手順 4　[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）　管理対象デバイスは、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、アクセス コントロール ポリシーの適用（12-17 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（Any）

防御センターは、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。以下の表で、[ルール アップデート ログ(Rule Update Log)] のフィールドについて説明します。

表 66-2　[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(66-26 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。
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(66-26 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(66-26 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(66-28 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 アップデートのインポート ログ(Rule Update Import Log)] の検索(66-30 ページ)では、インポート ログで検索基準と一致する特定のレコード、またはすべてのレコードを検索する方法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。

アクセス: 管理

手順 1　[システム(System)] > [更新(Updates)] を選択し、[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。

ヒント　または [ルール エディタ(Rule Editor)] ページで [ルールのインポート(Import Rules)] をクリックします。ここには、[ポリシー(Policies)] > [侵入(Intrusion)] > [ルール エディタ(Rule Editor)] を選択してアクセスすることができます。

手順 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（Any）

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 66-3　[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。
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（） 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。

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（Any）

[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）] 詳細ビューのワークフロー ページで実行できる特定のアクションについて説明します。

表 66-4　[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(66-28 ページ)で詳細を参照してください。
現行のワークフロー ページ上でレコードをソートおよび制約する	ドリルダウン ワークフロー ページのソート(58-39 ページ)で詳細を参照してください。
一時的に他のワークフローを使用する	[(ワークフローの切り替え)((switch workflows))] をクリックします。ワークフローの選択については、ワークフローの選択(58-19 ページ)を参照してください。カスタム ワークフローの作成については、カスタム ワークフローの作成(58-44 ページ)を参照してください。
すぐに再表示できるように、現在のページをブックマークする	[このページをブックマーク(Bookmark This Page)] をクリックします。詳細については、ブックマークの使用(58-42 ページ)を参照してください。
ブックマークの管理ページへ移動する	[ブックマークの表示(View Bookmarks)] をクリックします。詳細については、ブックマークの使用(58-42 ページ)を参照してください。
現在のビューのデータに基づいてレポートを生成する	[レポート デザイナ(Report Designer)] をクリックします。詳細については、イベント ビューからのレポート テンプレートの作成(57-10 ページ)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)] データベース全体で、ルール更新のインポート レコードを検索する	[検索(Search)] をクリックします。詳細については、[ルール アップデートのインポート ログ(Rule Update Import Log)] の検索(66-30 ページ)を参照してください。
現行の制約が設定されている検索ページを開く	[制約の検索(Search Constraints)] の隣にある [検索の編集(Edit Search)] または [検索の保存(Save Search)] を選択します。詳細については、テーブル ビューおよびドリルダウン ページの機能の表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。

アクセス:管理

手順 1　[システム(System)] > [更新(Updates)] を選択し、[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。

ヒント　または [ルール エディタ(Rule Editor)] ページで [ルールのインポート(Import Rules)] をクリックします。ここには、[ポリシー(Policies)] > [侵入(Intrusion)] > [ルール エディタ(Rule Editor)] を選択してアクセスすることができます。

手順 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。

手順 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（Any）

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 66-5　[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。
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 66-5　[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
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。 • [新規(new)](ルールで、このアプライアンスにルールが最初に格納された場合) • [変更済み(changed)](ルール更新コンポーネントまたはルール用。ルール更新コンポーネントが変更された場合、またはルールのリビジョン番号が大きく、GID と SID が同じ場合) • [競合(collision)](ルール更新コンポーネントまたはルールに関して、アプライアンス上の既存のコンポーネントまたはルールとリビジョンが競合しているため、インポートがスキップされた場合) • [削除済み(deleted)](ルール用。ルール更新からルールが削除された場合) • [有効(enabled)](ルール更新の編集で、プリプロセッサ、ルール、または他の機能がシスコ提供のデフォルト ポリシーで有効になっている場合) • [無効(disabled)](ルールに関して、シスコ提供のデフォルト ポリシーでルールが無効になっていた場合) • [ドロップ(drop)](ルールに関して、シスコ提供のデフォルト ポリシーでルールが [ドロップ(Drop)] または [イベントを生成する(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)
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)。詳細については、表 41-7(41-44 ページ)を参照してください。
SID	ルールの SID。
Rev	ルールのリビジョン番号。
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。
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 [メンバー数(Count)] フィールドが表示されます。

[ルール アップデートのインポート ログ(Rule Update Import Log)] の検索

ライセンス:任意(Any)

(注) ベータ ユーザ:この機能については、このマニュアルの最終バージョンで詳細に説明します。

インポート ログで検索基準と一致する特定のレコード、またはすべてのレコードを検索することができます。カスタマイズされた検索を作成し、後で再利用できるように保存しておくこともできます。

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。検索の対象となるすべてのオブジェクトが含まれるように、時間制約が設定されていることを確認します。詳細については、検索での時間制約の指定 (60-6 ページ)を参照してください。

次の表で、ユーザが使用できる検索条件について説明します。レコード検索では大文字/小文字が区別されないことに注意してください。たとえば、`RULE` または `rule` の検索では同じ結果が得られます。

表 66-6　[ルール アップデートのインポート ログ(Rule Update Import Log)] の検索基準

検索フィールド (Search Field)	説明	例
時刻(Time)	レコードが生成された日時を指定します。時間入力の構文については、検索での時間制約の指定(60-6 ページ)を参照してください。	`> 2006-01-15 13:30:00` のように指定すると、2006 年 1 月 15 日午後 1:30 より後にインポートされたすべてのルール レコードが返されます。
[名前(Name)]	ルールの [メッセージ(Message)] フィールドのすべてまたは一部の内容を指定します。このフィールドでは、ワイルドカード文字としてアスタリスク(*)を使用できます。	`*dhcp*` のように指定すると、[メッセージ(Message)] フィールドで DHCP という文字列が含まれるすべてのルール レコードが返されます。
タイプ(Type)	レコードのタイプを指定します。[ルール更新コンポーネント(rule update component)]、[ルール(rule)]、または [ポリシー適用(policy apply)] を使用できます。 バージョン 5.0.1 より前にインポートされたルールの検索では、検索で [更新(update)] 検索値を使用できることに注意してください。	[更新(update)] を指定すると、ルール パックやポリシー パックなど、インポートされたルール更新コンポーネントが返されます。[ルール(rule)] を指定すると、新しいルールも含めてルールの更新が返されます。[ポリシー適用(policy apply)] を指定すると、更新の後に侵入ポリシーが自動的に再適用されたルール更新の情報が、表形式の行で返されます。
アクション(Action)	表示するオブジェクトに対するアクションを指定します。指定できるアクションについては、[ルール アップデートのインポート ログ(Rule Update Import Log)] 詳細ビューのフィールドの表を参照してください。	タイプが [ルール(rule)]、[新規(new)] の場合は、アプライアンスに最初にインポートされたすべてのルールが返されます。
GID	ルールのジェネレータ ID を指定します。	`3` を指定すると、すべての 共有オブジェクトのルール が返されます。

表 66-6　[ルール アップデートのインポート ログ(Rule Update Import Log)] の検索基準(続き)

検索フィールド(Search Field)	説明	例
SID	ルールのシグネチャ ID または SID の範囲を指定します。	923 と指定すると、SID 923 を持つルールのレコードが返されます。
Rev	ルールのリビジョン番号を指定します。	3 を指定すると、リビジョン番号 3 のルールが返されます。
ポリシー	ルールがインポートされたデフォルト ポリシーを指定します。	[すべて(All)] を指定すると、すべてのデフォルト ポリシーにインポートされたルールが返されます。
ルール アップデート(Rule Update)	ルール アップデート(Rule Update)ファイルの名前を指定します。	[ファイル名(filename)] と指定すると、指定されたインポート ファイルのすべてのレコードが返されます。
詳細(Details)	インポートされたオブジェクトの詳細を指定します。	previously* と指定すると、変更されたすべてのルールのレコードが返されます。

保存されている検索をロードおよび削除する方法など、検索の詳細については、イベントの検索(60-1 ページ)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)] を検索する方法:

アクセス: Admin/Intrusion Admin

手順 1　[分析(Analysis)] > [検索(Search)] を選択します。

[検索(Search)] ページが表示されます。

手順 2　[テーブル(Table)] ドロップダウン リストから、[ルール アップデートのインポート ログ(Rule Update Import Log)] を選択します。

適切な制約を使用してページがリロードされます。

ヒント　[ルール アップデート ログ(Rule Update Log)] 詳細ビューで [検索(Search)] をクリックすることもできます。[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(66-26 ページ)を参照してください。

手順 3　オプションで、検索を保存する場合は、[名前(Name)] フィールドに検索の名前を入力します。

名前を入力しない場合は、検索が保存されるときに Web インターフェイスで自動的に名前が生成されます。

手順 4　表 [ルール アップデートのインポート ログ(Rule Update Import Log)] の検索基準に記載されているように、該当するフィールドに検索基準を入力します。複数の条件を入力すると、検索によって、すべての基準に一致するレコードが返されます。

手順 5　検索を保存して他のユーザがアクセスできるようにするには、[プライベートとして保存(Save As Private)] チェック ボックスをオフにします。そうではなく、検索をプライベートとして保存するには、このチェック ボックスをオンのままにします。

カスタム ユーザ ロールのデータの制限として検索を使用する場合は、**必ず**プライベート検索として保存する必要があります。

手順 6　次の選択肢があります。

- 検索を開始するには、[検索（Search）] ボタンをクリックします。

  デフォルトの [ルール アップデートのインポート ログ（Rule Update Import Log）] 詳細ビューのワークフローに検索結果が示されます。カスタム ワークフローなどの別のワークフローを使用するには、[ワークフローの切り替え（(switch workflows)）] をクリックします。別のデフォルト ワークフローの指定方法については、イベント ビュー設定の設定（71-3 ページ）を参照してください。
- 既存の検索を変更して、その変更を保存する場合は、[保存（Save）] をクリックします。
- 検索基準を保存する場合は、[新規検索として保存（Save as New Search）] をクリックします。検索が保存され（[プライベートとして保存（Save As Private）] を選択した場合はユーザ アカウントに関連付けられ）、後で実行できます。

位置情報データベースの更新

ライセンス：FireSIGHT

サポートされる防御センター：任意（DC500 を除く）

シスコ地理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（国、都市、緯度と経度の座標など）、および接続関係のデータ（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）からなるデータベースです。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、防御センター 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。サポート担当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。

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。

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（62-10 ページ）を参照してください。地理位置情報の詳細については、地理位置情報の使用（58-24 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。

アクセス：管理

手順 1　[システム（System）] > [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。

手順 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。

手順 3　防御センター に更新をアップロードします。

- 防御センター 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）
- 防御センター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。更新を参照して、[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。これは、アプライアンスのハードウェアによって異なります。タスク キュー（[システム（System）] > [モニタリング（Monitoring）] > [タスクのステータス（Task Status）]）で更新の進行状況を監視できます。

手順 4　更新が終了したら、[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 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、防御センター により、管理対象デバイスが自動的に更新されます。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が、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。