IPS センサーの管理

日常的なセンサー管理を実行するには、通常 IPS Device Manager（IDM）などのデバイス マネージャを使用する必要があります。Security Manager はポリシーとイベントの管理に焦点を置いています。

ただし、次の項では、Security Manager を使用して実行できる管理作業について説明します。

IPS ライセンスの管理

次の項では、IPS デバイスのライセンスを管理する方法について説明します。

IPS ライセンス ファイルの更新

Security Manager を使用して、IPS デバイスのライセンスを更新できます。ここでは、Cisco.com、または Security Manager サーバのライセンス ファイルからライセンスを手動で取得することにより、ライセンスを手動で更新する方法について説明します。自動ライセンス更新のセットアップの詳細については、IPS ライセンス ファイル更新の自動化　（3 ページ）を参照してください。

はじめる前に

Cisco.com を使用する場合、ユーザ名とパスワードを指定できるように、最初に IPS 更新サーバを Cisco.com として設定する必要があります。デバイスによっては、ライセンス取得に Cisco.com を使用する必要があります。たとえば、IPS 4270 や ASA デバイス内の AIP SSM-40

デバイスでは、Cisco.com アカウントが必要です。Cisco.com を IPS 更新サーバとして設定する方法の詳細については、IPS 更新サーバの設定 （5 ページ）を参照してください。

ローカル ライセンスを使用する場合、Security Manager サーバ ファイル システムに直接ダウンロードする必要があります。この作業は Security Manager では実行できません。サーバ上で Windows にログインして、ライセンスをダウンロードする必要があります。

関連項目

- IPS ライセンス ファイルの再展開 （3 ページ）

ステップ 1 [ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、目次から [ライセンス（Licensing）] を選択します。

ステップ 2 [IPS] タブをクリックします（[IPS] タブ、[Licensing] ページを参照）。

表に、デバイス インベントリ内のすべての IPS デバイスおよびそのライセンス ステータスが表示されます。ステータスは、[valid]、[invalid]、[expired]、[no license]、または [trial license] です。ライセンスの有効期限も表示されます。[ライセンスの更新（Refresh License）] をクリックすると、デバイスの最新ライセンス情報で表が更新されます（1 つ以上のデバイスを選択して、更新の範囲を制限できます）。

ライセンスを更新するには、次のいずれかを実行します。

- Cisco.com から直接取得したライセンスでデバイスを更新する場合は、更新するデバイスを選択し、[CCO経由で選択内容を更新（Update Selected via CCO）] をクリックします。ダイアログボックスが開き、Cisco.com から更新可能なデバイスが表示されます。選択したすべてのデバイスが表示されるとは限りません。リストを確認し、[OK] をクリックします。[License Update Status Details] ダイアログボックスに更新作業のステータスが表示されます（[License Update Status Details] ダイアログボックスを参照）。

この方法でライセンスを更新するには、選択したデバイスのシリアル番号が含まれる Cisco.com サポート契約を締結する必要があります。

ヒント ライセンスが格納されたシスコのソフトウェア ライセンス サーバ（SWIFT）は、同じサーバから 3 分間に 10 ライセンス以上の要求があると、その要求をブロックする場合があります。そのため、手動でライセンス更新を実行するときは、一度に選択するデバイスを 8 つ以下にしてください。

- Cisco Security Manager サーバーにコピーしたライセンスでデバイスを更新するには、[ライセンスファイルから更新（Update from License File）] をクリックします。ライセンス ファイルを選択するためのダイアログボックスが開きます。[参照（Browse）] をクリックして、Cisco Security Manager ローカル ファイルシステムからライセンスファイルを選択します。複数のライセンス ファイルを選択できます。目的のファイルを選択したら、[OK] をクリックして、選択したファイルをデバイスに適用します。

IPS ライセンス ファイルの再展開

IPS ライセンス更新をデバイスに適用しようとして失敗した場合は、更新を再展開できます。再展開を実行できるのは、すでに更新を試行し、ライセンス ファイルが IPS デバイスに関連付けられている場合だけです。

関連項目

- IPS ライセンス ファイルの更新 （1 ページ）
- IPS ライセンス ファイル更新の自動化 （3 ページ）

ステップ 1 [ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、コンテンツ テーブルから [ライセンス（Licensing）] を選択します。

ステップ 2 [IPS] タブをクリックします（[IPS] タブ、[Licensing] ページを参照）。

ステップ 3 ライセンスを再展開するデバイスを選択し、[選択したライセンスの再展開（Redeploy Selected Licenses）] をクリックします。ライセンスを再展開するデバイスが表示されたダイアログボックスが開きます。[OK] をクリックして、更新を実行します。

[License Update Status Details] ダイアログボックスに更新作業のステータスが表示されます（[License Update Status Details] ダイアログボックスを参照）。

IPS ライセンス ファイル更新の自動化

Security Manager は、IPS ライセンス更新を定期的に IPS デバイスに自動適用できます。自動更新を設定するには、IPS デバイスのシリアル番号が含まれる Cisco.com サポート契約を締結する必要があります。

ヒント Security Manager は、置き換えられるライセンスよりも未来の有効期限がダウンロードされたライセンスに設定されている場合、またはライセンス情報が異なる場合に、新しいライセンスを適用します。

はじめる前に

Cisco.com ユーザ名とパスワードを指定できるように、最初に IPS 更新サーバを Cisco.com として設定する必要があります。Cisco.com を IPS 更新サーバとして設定する方法の詳細については、 IPS 更新サーバの設定 （5 ページ）を参照してください。

関連項目

- IPS ライセンス ファイルの更新 （1 ページ）
- IPS ライセンス ファイルの再展開 （3 ページ）

ステップ 1 [ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、目次から [ライセンス（Licensing）] を選択します。

ステップ 2 [IPS] タブをクリックします（[IPS] タブ、[Licensing] ページを参照）。

ステップ 3 [ラインセンスのダウンロードと適用（Download and apply licenses）] を選択して、次の設定値を設定します。

- [有効期限までの日数（Days before the expiration date）]：Cisco Security Manager が更新されたライセンスをダウンロードする必要がある、ライセンスの有効期限までの日数を選択します。デフォルトは 1 日です。
- [毎日のデバイスの検出時刻（Discover devices daily at）]：Cisco Security Manager がライセンスをダウンロードする時刻を選択します。選択した時刻になると、Security Manager はデバイスのライセンス ステータスを確認し、ライセンスが存在しないデバイス、ライセンスの有効期限が切れているデバイス、または設定した日数の間にライセンスの有効期限が切れるデバイスに対して、新しいライセンスを Cisco.com に問い合わせます。
- [ライセンスの更新結果を電子メールで送信する（Email License Update Results）]：Cisco Security Manager がライセンス更新結果の電子メール通知を送付するかどうかを選択します。ライセンス有効期限ステータスが記載された電子メールと、ライセンス更新ジョブ結果に関する電子メールが送信されます。このオプションを選択した場合は、[電子メール通知（Email Notification）] フィールドに 1 つ以上の電子メールアドレスを入力します。カンマで複数のアドレスを区切ります。

電子メールを送信するには、電子メール通知用の SMTP サーバおよびデフォルト アドレスの設定の説明に従って SMTP サーバを設定する必要があります。

ステップ 4 [保存（Save）] をクリックして変更を保存します。

IPS 更新の管理

Security Manager を使用すると、センサーおよびシグニチャの更新を IPS デバイスおよび共有ポリシーに適用できます。Security Manager を使用して、更新をダウンロードした後、自動更新をセットアップするか、または手動で更新を適用できます。

シグニチャの更新は、IPS 5.1(4) 以降でのみ使用可能です。

ヒント パッチ、サービス パック、またはシグニチャの更新の適用中に問題が発生する場合は、IPS センサーの時刻を確認します。センサーの時刻が、関連付けられている証明書の時刻よりも進んでいる場合、証明書は拒否されます。この場合、更新が失敗する可能性があります。IPS センサーの時刻を正確に保つには、ネットワーク タイム プロトコル（NTP）を使用します。センサーで NTP を設定する方法の詳細については、NTP サーバの識別を参照してください。

Security Manager に含まれる IPS パッケージには、IPS デバイスの更新に必要なパッケージ ファイルは含まれていません。更新を適用する前に、Cisco.com またはローカル更新サーバから IPS パッケージをダウンロードする必要があります。ダウンロードされたバージョンにはすべての必要なパッケージ ファイルが含まれ、Security Manager の初期インストールに含まれていた部分的なファイルと置き換えられます。

ここでは、Security Manager を使用して IPS 更新を管理する方法について説明します。

IPS 更新サーバの設定

IPS センサーおよびシグニチャの更新を適用するには、Security Manager で、指定された IPS 更新サーバから Security Manager サーバに更新をダウンロードする必要があります。

Cisco.com を IPS 更新サーバとして使用できます。Cisco.com を使用すると、最新の更新をすぐに入手できます。ただし、何らかの理由で Cisco.com を使用できない場合、独自のローカル IPS 更新 Web サーバをセットアップして、そのサーバに手動で更新をダウンロードし、ローカル サーバからの更新を取得するように Security Manager を設定できます。

ヒント ライセンスの更新に Cisco.com ログインを必要とするデバイス（IPS 4270 や ASA デバイス内の AIP SSM-40 など）を使用している場合は、IPS 更新サーバを Cisco.com として設定する必要があります。ローカル サーバを使用することはできません。

関連項目

• IPS 更新の自動化 （7 ページ）
• IPS 更新の手動適用 （9 ページ）

ステップ 1 [ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] を選択し、コンテンツテーブルから [IPS更新（IPS Updates）] を選択して、[IPS更新（IPS Updates）] ページを開きます（[IPS Updates] ページを参照）。

ステップ 2 [サーバーの更新（Update Server）] 領域で、[設定の編集（Edit Settings）] をクリックして [更新サーバー設定の更新の編集（Edit Update Server Settings）] ダイアログボックスを開きます（[Edit Update Server Settings] ダイアログボックスを参照）。

ステップ 3 サーバの識別情報を入力します。[Update From] フィールドで選択したサーバ タイプに基づいて、次の操作を実行します。

- [Cisco.com]：Cisco.comユーザ名およびパスワードを入力します。指定するユーザアカウントで強化暗号化ソフトウェアをダウンロードできる必要があります。アカウントに適切な権限があることを確認するには、Cisco.com にアクセスして、IPS 更新パッケージのダウンロードを試行してください。アカウントがまだ認定されていない場合は、適切な契約に合意するように求められます。
- [Local server]：サーバの IP アドレスまたは DNS ホスト名、ユーザ名とパスワード（アクセス許可の前にログインの必要がある場合）、およびファイルが含まれるフォルダへのパスを入力します。パスには、URL 全部ではなく URL のパス部分だけを入力します（たとえば、http://servername/IPSpath の中のパスは IPSpath です）。また、次のように IIS 設定を追加します。
  - ホーム ディレクトリのリストがイネーブルになっている必要があります。
  - ドキュメントの [Default Content Page] がディセーブルになっている必要があります。

証明書情報を入力します。IPS パッケージをダウンロードする前に、Cisco.com 証明書を承認する必要があります。イメージのダウンロードを正常に開始するには、「イメージメタデータロケータ」サイトと IPS パッケージのダウンロードサイトの両方からの証明書を受け入れる必要があります（[Edit Update Server Settings] ダイアログボックスを参照）。

Security Manager サーバーから IPS 更新サーバーに接続するために、ネットワークでプロキシサーバーが必要な場合、[プロキシサーバーの有効化（Enable Proxy Server）] を選択し、プロキシサーバーの情報を入力します。

[OK] をクリックして変更を保存します。

ステップ 4 [IPS更新（IPS Updates）] ページで [保存（Save）] をクリックします。[保存（Save）] をクリックするまで、変更は完全には保存されません。

ステップ 5 [最新の更新をダウンロード（Download Latest Updates）] をクリックして、IPS 更新サーバーへの接続をテストします。ダイアログボックスが表示されます。[開始（Start）] をクリックすると、Security Manager が更新サーバーにログインし、新しい更新を確認してダウンロードします。ダイアログボックスに操作の結果が表示されます。

Cisco.com を使用しているときにダウンロードが失敗する場合は、ユーザ アカウントを再度確認して、強化暗号化ソフトウェアをダウンロードできるかどうかを確認してください。

IPS 更新の確認とダウンロード

Security Manager を使用して、IPS センサーとシグニチャの更新を確認し、Security Manager サーバにダウンロードできます。これらの更新は、Security Manager サーバで IPS デバイスおよびポリシーに適用できます。

手動で IPS 更新をダウンロードすることも、IPS 更新のダウンロードを自動化することもできます。または、手動で IPS 更新をデバイスに適用するときに更新をダウンロードすることもできます。ここでは、手動で更新を確認してダウンロードする方法について説明します。自動ダウンロードの設定方法の詳細については、IPS 更新の自動化 （7 ページ）を参照してくださ

い。更新をデバイスまたはポリシーに手動で適用するときに更新をダウンロードする方法の詳細については、IPS 更新の手動適用 （9 ページ）を参照してください。

はじめる前に

IPS 更新サーバの設定 （5 ページ）の説明に従って IPS 更新サーバを設定する必要があります。

関連項目

- IPS 更新の自動化 （7 ページ）
- IPS 更新の手動適用 （9 ページ）

ステップ 1 [ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] を選択し、コンテンツテーブルから [IPS更新（IPS Updates）] を選択して、[IPS更新（IPS Updates）] ページを開きます（[IPS Updates] ページを参照）。

ステップ 2 [Update Status] グループ内のステータス情報を確認し、次のいずれかを実行します。

- [更新の確認（Check for Updates）] をクリックします。操作の結果を示すダイアログボックスが開きます。[開始（Start）] をクリックすると、Security Manager が IPS 更新サーバーにログインし、更新を確認します。
- [最新の更新をダウンロード（Download Latest Updates）] をクリックします。操作の結果を示すダイアログボックスが開きます。[開始（Start）] をクリックすると、Security Manager が IPS 更新サーバーにログインし、更新を確認して Security Manager サーバーにダウンロードします。

ヒント Cisco.com からのダウンロードに失敗する場合は、使用しているアカウントで強化暗号化ソフトウェアをダウンロードできることを確認してください。詳細については、[Edit Update Server Settings] ダイアログボックスの [User Name] の説明を参照してください。

IPS 更新の自動化

センサーイメージとシグニチャを常に最新に保つために、それらの更新を互換性のある IPS デバイスに自動的に適用できます。必要に応じて、更新を部分的に自動化して、プロセスに対する制御を必要なレベルに保つことができます。

ヒント 後でシグニチャの更新を適用する必要はなかったと判断した場合は、デバイスで [シグネチャ（Signatures）] ポリシーを選択し、[更新レベルの表示（View Update Level）] ボタンをクリックしてから [元に戻す（Revert）] をクリックすることで、直前の更新レベルに戻すことができます。

ヒント　IPSデバイスを管理しない場合は、次のパフォーマンス調整手順の実行を検討してください。*$NMSROOT*\MDC\ips\etc\sensorupdate.properties の packageMonitorInterval の値を、初期デフォルト値の 30,000 ミリ秒から、より頻度の低い値である 600,000 ミリ秒に変更します。この手順を実行することにより、いくらかパフォーマンスが向上します。*$NMSROOT* は、Common Services インストールディレクトリ（デフォルトは C:\Program Files\CSCOpx）のフルパス名です。

はじめる前に

IPS 更新サーバの設定　（5 ページ）の説明に従って IPS 更新サーバを設定する必要があります。

関連項目

- IPS 更新の確認とダウンロード　（6 ページ）
- IPS 更新の手動適用　（9 ページ）
- IPS ネットワーク検知について
- Workflow 以外のモードでの設定の展開
- Workflow モードでの設定の展開

ステップ 1　[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] を選択し、コンテンツテーブルから [IPS更新（IPS Updates）] を選択して、[IPS更新（IPS Updates）] ページを開きます（[IPS Updates] ページを参照）。

ステップ 2　ページ下部の [Auto Update Settings] グループで自動更新モードを選択して、自動化のレベルを設定します。次のオプションがあります。

- [Download, Apply, and Deploy Updates]：Security Manager はスケジュールに従って更新を確認し、更新を Security Manager サーバにダウンロードしてから、選択されたデバイスおよびポリシーに適用します。続いて、展開ジョブを開始して、影響を受けるデバイスを更新します。これを選択すると、運用スタッフの労力を最小限に抑えて、デバイスの最新の更新が確実に実行されます。
- [Disable Auto Update]：Security Manager は、IPS 更新の自動処理を実行しません。
- [Check for Updates]：Security Manager はスケジュールに従って更新を確認し、[Update Status] グループ内の情報を更新します。デバイスもポリシーも更新されません。
- [Download Updates]：Security Manager はスケジュールに従って更新を確認し、新しい更新を Security Manager サーバにダウンロードします。
- [Download and Apply Updates]：Security Manager はスケジュールに従って更新を確認し、更新をダウンロードして、選択されたデバイスおよびポリシーに適用します。影響を受けるデバイスに変更を展開する展開ジョブは、個別に作成する必要があります。

ステップ 3 [更新スケジュールの編集（Edit Update Schedule）] をクリックして、操作のスケジュールを指定できるダイアログボックスを開きます。開始日を選択し、開始時刻を 24 時間形式（hh:mm）で入力し、スケジュールをどの単位で指定するか（時間、日、週、月、または 1 回限りのイベント）を選択します。[OK] をクリックして、スケジュールを保存します。

ステップ 4 （任意）[Notify Email] フィールドに電子メール アドレスを入力します。Security Manager は、パッケージがダウンロード可能になったとき、あるいはパッケージのダウンロード、適用、または展開が完了したときに、このユーザに通知します。複数のアドレスをカンマで区切って入力できます。

ステップ 5 [Apply Update To] セレクタで、自動で更新するデバイスおよび共有ポリシーを選択します。ローカル ポリシー（デバイスの場合）と共有ポリシーを切り替えるには、[Type] フィールドを使用します。

デバイスまたはポリシーを選択するには、セレクタ内のデバイスまたはポリシーをクリックし、[行の編集（Edit Row）] ボタン（セレクタの下の鉛筆アイコン）をクリックします。この処理により、[Edit Auto Update Settings] ダイアログボックスが開きます。適用する更新のタイプ（[minor sensor updates and service packs] または [service packs only]）およびシグニチャ更新のレベルを選択します。[OK] をクリックして変更を保存します。ポリシーの適用先のデバイスが、[Devices to be Auto Updated] リストに追加されます。メッセージに、変更を有効にするために変更を送信する必要があるかどうかが示されます。

ステップ 6 [保存（Save）] をクリックします。

IPS 更新の手動適用

Apply IPS Update ウィザードを使用すると、イメージおよびシグニチャの更新を互換性のある IPS デバイスに手動で適用できます。この手順は、自動更新が設定されていないポリシーおよびデバイスに対して使用してください（IPS 更新の自動化 （7 ページ）を参照）。

シグニチャ更新を適用するときに、このウィザードには、更新内のシグニチャのうち対象の IPS デバイス上に設定されていないものが表示されます。新しいシグニチャは、適用前に設定できます。

イメージおよびシグニチャの更新を適用する際は、更新を適用できるデバイスだけが選択可能になります。適用できないデバイスはグレー表示されます。グレー表示されているデバイスにマウスポインタを合わせると、デバイスがグレー表示されている理由がツールチップに表示されます。必要なエンジンアップグレードまたは汎用パッケージを利用できない場合、シグネチャの更新がデバイスに適用されていても、デバイスがグレー表示されることがあります。以下に、デバイスがグレー表示される例と、対応するツールチップラベルを示します。

- 選択したシグネチャまたはセンサーパッケージのバージョンがターゲット IPS デバイスのバージョンよりも低い場合、Cisco Security Manager によりデバイスがグレー表示され、マウスオーバーのツールチップに「選択されたパッケージは適用できません（Selected package is inapplicable）」というメッセージが表示されます。
- Cisco Security Manager を使用して、SNMP ポリシーが設定されているバージョン 7.2.2 からバージョン 7.3.1 に IPS デバイスをアップグレードしようとすると、マウスオーバーのツールチップに「選択されたアップグレードは推奨されません（Selected upgrade is not recommended）。デバイスの SNMP ポリシーの割り当てを解除して展開し、7.3.1 へのアップグレードを続行してください（Unassign the SNMP policy on the device and deploy it to

continue with the upgrade to 7.3.1）」と表示されます。これは、SNMPv3 が IPS バージョン 7.3.1 でサポートされていないためです。

- Cisco Security Manager を使用して、デバイスに適用されている 1 つ以上の脅威プロファイルが含まれていないシグネチャの更新を実行しようとすると、Cisco Security Manager によりデバイスがグレー表示され、マウスオーバーのツールチップに「現在適用されている脅威プロファイルは、このシグネチャバージョンには適用されません（Currently applied threat profile is not applicable to this signature version）」というメッセージが表示されます。この場合、シグネチャの更新は正常に適用できません。既存の脅威プロファイルを削除してから、シグネチャの更新を続行する必要があります。

ヒント　後にシグネチャの更新を適用する必要はなかったと判断した場合は、デバイスで [シグネチャ（Signatures）] ポリシーを選択し、[更新レベルの表示（View Update Level）] ボタンをクリックしてから [元に戻す（Revert）] をクリックすることで、直前の更新レベルに戻すことができます。

はじめる前に

IPS 更新サーバの設定　（5 ページ）の説明に従って IPS 更新サーバを設定します。

関連項目

- IPS 更新の確認とダウンロード　（6 ページ）
- Cisco IOS IPS のシグニチャ カテゴリの選択

（注）　ここでは、IPS 7.1.3 の更新パッケージと以前のバージョンで使用されたパッケージの違いについて説明します。Apply IPS Update ウィザード（[ツール（Tools）] > [IPS更新の適用（Apply IPS Update）]）を開くと、ウィザードの最初のページに、使用可能なセンサーおよびシグネチャの更新パッケージが一覧表示されます。IPS 7.1.3 以降は、IPS-4270 や ASA-SSE-AIP-85 など、サポートされているすべてのプラットフォームに単一の更新パッケージ（IPS-CSM-K9-7.1.3.zip など）が使用されます。IPS 7.1.3 より前は、サポートされているプラットフォームごとに個別のパッケージ（IPS-CS-MGR-SSC_5-K9-6.2-4-E4.zip など）が使用されていました。

ステップ 1　[ツール（Tools）] > [IPS更新の適用（Apply IPS Update）] を選択して、Apply IPS Update ウィザードを開きます。

ステップ 2　ウィザードの最初のページで、適用する更新を選択します。このページに、使用可能なセンサーおよびシグニチャの更新が表示されます。このページで、次の操作を実行します。

- パッケージのリストを更新するには、[最新の更新をダウンロード（Download Latest Updates）] をクリックします。Security Manager は IPS 更新サーバにログインし、最後のダウンロード以降に使用可能になった更新をダウンロードします。これは、IPS 更新サーバの設定　（5 ページ）の説明に従って

更新サーバを設定した場合のみ実行されます。また、次の操作を実行して、パッケージのリストを更新することもできます。

- [IPS更新（IPS Updates）] ページ（**[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] > [IPS更新（IPS Updates）]** を選択）で自動ダウンロードを設定します。詳細については、[IPS Updates] ページを参照してください。
- Security Manager サーバ上の製品インストール フォルダ（通常は Program Files）内の CSCOpx\MDC\ips\updates フォルダに更新を手動でダウンロードします。

また、[更新の確認（Check for Updates）] をクリックすることで、ダウンロードせずに更新を確認できます。[Update Status] 情報は、[IPS Updates] ページの説明と同じです。

- [Updates Downloaded] テーブルで、IPS デバイスに適用するシグニチャまたはセンサーの更新を選択します。更新のタイプを切り替えるには、[タイプ（Type）] フィールドを使用します（適用する更新は 1 つだけ選択できます）。
  - [センター更新（Sensor Updates）]：ファイル名、メジャー、マイナー、サービスパック、パッチ バージョン、およびサポートされているエンジンリリースが表示されます。メジャー センサー更新はすべて適用する必要があります。ただし、マイナー更新は累積的です。
  - [シグネチャの更新（Signature Updates）]：ファイル名、シグネチャ番号、およびサポートされているエンジンリリースが表示されます。シグニチャ更新は累積的ですが、ネットワークの特定の要件に合わせて更新を調整しようとする場合、これらの更新を個別のパッケージとして適用すると、より管理しやすい単位に作業を分割できます。

（注） エンジン パッケージは更新ページに表示されません。ただし、上位のエンジン バージョンが必要となるシグニチャ更新の場合、Security Manager は暗黙的にエンジン パッケージをプッシュします（この処理は、エンジン パッケージで必要となる特定のバージョンでデバイスを更新する場合のみ実行されます）。

[次へ（Next）] をクリックして続行します。

ステップ 3 ウィザードの 2 ページめで、[Apply Updates To] リストから、更新対象となる（共有シグニチャ ポリシーに割り当てられていないデバイスを表す）ローカル シグニチャ ポリシーおよび共有シグニチャ ポリシーを選択します。ポリシーのタイプを切り替えるには、[タイプ（Type）] フィールドを使用します。ローカル ポリシーと共有ポリシーを自由に組み合わせて選択できます。ポリシーを選択すると、そのポリシーを使用するデバイスが更新対象として選択されます。

適用可能なすべてのデバイスまたは共有ポリシーを選択するには、[すべて選択（Select All）] をクリックします。選択内容を消去して最初からやり直すには、[すべて選択解除（Deselect All）] をクリックします。これらのボタンは、表示されているリストにだけ適用されます。

更新が適用されない IPS デバイスは、[Apply Updates To] リストでグレー表示されるため、選択できません。更新可能なデバイスを選択すると、[Devices Assigned to Selected Policies] リストにそのデバイスが示されます。更新されるのは、これらのデバイスだけです。共有ポリシーを選択すると、そのポリシーを使用しているすべてのデバイスが、[selected policies] リストに表示されますが、更新が適用されないデバイスはグレー表示されます。

ヒント　センサー更新の対象として選択できるデバイスは、エンジン リリースによって決まります。つまり、更新は、リリース バージョンに関係なく、同じエンジン バージョンを使用するデバイスだけに適用できます。たとえば、デバイスが 6.0(5) E3 を実行している場合、6.1(1) E3 には更新できますが、6.1(1) E2 には更新できません。また、6.1(1) E2 を実行しているデバイスに 6.1(1) E3 更新を適用することもできません。エンジン バージョンを更新する場合は、上位のエンジン バージョンを持つシグニチャ更新を選択します。これにより、Security Manager は、シグニチャの更新中に自動的にエンジン レベルを更新します。たとえば、デバイスのバージョンが 6.1(1) E2 の場合、E3 エンジン パッケージを適用する必要があれば、E3 エンジンを必要とするシグニチャ パッケージを選択してデバイスに適用します。これにより、シグニチャの更新中に自動的にエンジン パッケージがデバイスに適用されます。このため、更新する必要のあるデバイスがグレー表示されている場合は、[戻る（Back）] をクリックし、更新の選択内容を変更します。

シグネチャの更新を適用する際に、適用前にシグネチャを編集する場合は、[次へ（Next）] をクリックして続行します。それ以外の場合は、[終了（Finish）] をクリックして更新をポリシーに適用します。

ステップ 4　（任意）ウィザードの 3 ページ目で、必要に応じてシグニチャを変更します。

シグニチャ リストに、選択した更新のシグニチャ レベルから、選択したデバイス間で最も下位のシグニチャ レベルまでの間で、新規のシグニチャおよび変更されたシグニチャが表示されます。選択したデバイスに IPS センサーと Cisco IOS IPS デバイスの両方が含まれている場合、これらのデバイスのシグニチャは別々のタブに表示されます。

ID 番号内のリンクをクリックして、Cisco.com のシグニチャの説明を読みます。[Status] カラムは、シグニチャが新規のものか変更されたものかを示します（ウィザード ページのアイコンの説明図を参照）。

シグニチャを編集するには、表内のシグニチャを選択し、表の下にある [Edit] ボタン（鉛筆アイコン）をクリックします。シグネチャの説明については、[編集（Edit）] ボタンを押すと開くダイアログボックス内の [ヘルプ（Help）] をクリックして確認してください。

使用可能なシグニチャ情報の詳細については、[Signatures] ページを参照してください。[Signature Summary Table] ではカスタム シグニチャの追加やシグニチャの削除ができますが、Apply IPS Update ウィザードのこのページではこれらの操作を実行できません。

[終了（Finish）] をクリックして、更新をポリシーに適用し、編集を保存します。

ステップ 5　変更を送信し、デバイスに展開します。展開ジョブの作成方法の詳細については、次の各項を参照してください。

- Workflow 以外のモードでの設定の展開
- Workflow モードでの設定の展開

IPS 証明書の管理

IPS デバイスとの通信に SSL（HTTPS）を使用するように Cisco Security Manager を設定する場合、デバイスに設定されている証明書が Cisco Security Manager の証明書ストアに保存されてい

る証明書と一致している必要があります。証明書が一致していないと、ポリシー検出または展開時に通信が失敗します。

IPS デバイスは、約 2 年間の固定の有効期間が設定された自己署名証明書を使用します。証明書の有効期限が切れた場合は、証明書を再生成し、新しい証明書で証明書ストアを更新する必要があります。

Security Manager には、デバイスに定義されている証明書との証明書ストアの同期、有効期限が切れた証明書の再生成、および管理する IPS デバイス上に存在する証明書のステータス（有効期限を含む）の表示ができるユーティリティが含まれています。

ヒント IPS デバイスとの通信に HTTP を使用している場合、証明書は使用されず、証明書を管理することもできません。IPS デバイスの通信の設定値は、[Security Manager Administration Device Communication] ページで設定します（[Device Communication] ページを参照）。

ここでは、Security Manager を使用して IPS 証明書を管理する方法について説明します。

関連項目

- テーブル カラムおよびカラム見出しの機能
- テーブルのフィルタリング
- HTTPS 通信を使用するデバイスでの SSL 証明書の手動追加
- デバイス検出時にセキュリティ証明書が拒否される
- デバイス検出中の無効な証明書のエラー

ステップ 1 [管理（Manage）] > [IPS] > [IPS証明書（IPS Certificates）] を選択して、[IPS証明書（IPS Certificates）] ダイアログボックスを開きます。

ヒント このダイアログボックスに表示されるリストは、自動的には更新されません。ダイアログボックスを開くたびに [更新（Refresh）] をクリックして、最新の証明書の有効期限情報を参照してください。

ダイアログボックスには、インベントリにあるすべての IPS センサーが Security Manager の表示名のとおりに表示されます。すべてのカラムが表示されるわけではありません（他のカラムを選択するには、任意のセルの見出しを右クリックします）。主要なカラムは次のとおりです。

- [証明書の不一致（Certificate Mismatch?）]：デバイスに定義されている証明書が Cisco Security Manager の証明書と同一かどうかを示します。証明書が使用できない、または取得できない場合は、このフィールドはブランクになります。証明書が取得できた場合は、次のいずれかの値になります。
  - [いいえ（No）]：デバイスと Cisco Security Manager は同一の証明書を保持しています。特に対処の必要はありません。

- [はい（Yes）]：デバイスと Cisco Security Manager は異なる証明書を保持しています。証明書の有効期限が切れていない場合、デバイスを選択し、[証明書の同期（Sync Certificates）] をクリックして、Cisco Security Manager の証明書ストアの証明書をデバイスの証明書と置き換えます。

- [デバイスの有効期限最終日（Valid Until on Device）]、[デバイスの有効期限開始日（Valid From on Device）]：この 2 つの列には、証明書が有効である日付の範囲が表示されます。[Valid Until] の日付を迎えると、証明書の有効期限は切れます。この日付が近づいてきたら、証明書の再生成を検討してください。

- [デバイスの証明書ステータス（Certificate Status on Device）]：デバイスに存在する証明書の現在のステータスを示します。
  - [有効な証明書（Valid Certificate）]：証明書は正常で、有効期間内です。
  - [期限切れの証明書（Expired Certificate）]：[有効期限最終日（Valid Until）] の日付が過ぎ、証明書は有効期限が切れています。デバイスを選択し、[証明書の再生成（Regenerate Certificate）] をクリックすると、デバイス上に新しい有効な証明書が作成され、Cisco Security Manager の証明書ストアに証明書がロードされます。
  - [有効期限前の証明書（Certificate Not Yet Valid）]：証明書は [有効期限開始日（Valid From）] の日付に達していないため、まだ使用できません。デバイス上の時刻設定と Security Manager サーバの時刻設定との間に不一致がある可能性があります。時刻設定が同一であることを確認してください（NTP サーバの使用を検討してください）。証明書の再生成を検討してください。
  - [使用不可：更新して証明書情報を取得する（Unavailable – Refresh to get Cert Info）]：証明書は現在 Cisco Security Manager の証明書ストアに存在しません。[更新（Refresh）] をクリックして、Cisco Security Manager がデバイスから証明書を取得し、証明書ストアにロードするようにします。
  - [取得不可能：証明書情報を利用できない（Nonretrievable – Cert Info not available）]：Cisco Security Manager はデバイスにログインして証明書を取得できませんでした。または、通信に HTTP を使用しています。デバイスを選択して、[更新（Refresh）] をクリックします。

更新により問題が解決されない場合、デバイスが正常に動作していること（つまり、ダウンしていないこと）を確認してください。次に、デバイスのプロパティを確認して、正しいクレデンシャルがアクセスのために設定されていることを確認してください（デバイス プロパティの表示または変更を参照）。クレデンシャルに問題がない場合、デバイスに設定されている Allowed Hosts ポリシーも確認して、Security Manager サーバが許可ホストとして含まれていることを確認してください（許可ホストの識別を参照）。また、Security Manager サーバ上の Windows にログインし、ping を使用してサーバと IPS デバイスとの間にルートが存在するかどうかを確認することもできます。

- [CSMのサムプリント（Thumbprint on CSM）]、[デバイスのサムプリント（Thumbprint on Device）]：これらの列には、証明書ストア内とデバイス上にある証明書のサムプリントが表示されます。

ステップ 2 次のいずれかのボタンを使用して、指示されたアクションを実行します。指示されている箇所を除いて、デバイスを 1 つも選択せずにボタンをクリックした場合、表示されているすべてのデバイスにアクションが実行されます。この操作は、多くの IPS デバイスが存在する場合に、時間がかかる可能性があります。操作がすべてのデバイスに実行される前に警告が表示され、操作を中止するオプションが表示されます。

- [証明書の同期（Sync Certificate）]：Cisco Security Manager の証明書ストア内の証明書情報と、デバイスの証明書を同期します。デバイスの証明書によって、証明書ストア内の証明書が置き換えられます。
- [証明書の再生成（Regenerate Certificate）]：デバイス上に新しい証明書を生成し、新しい証明書を証明書ストア内にロードします。
- [更新（Refresh）]：Cisco Security Manager がデバイスに問い合わせて、有効期限などの証明書情報を取得し、証明書ストア内の証明書とデバイスの証明書を比較することで、ステータス情報を更新します。このアクションによって [Certificate Status on Device] カラムが更新され、証明書の不一致があるかどうかも判断します。
- [エクスポート（Export）]：証明書テーブル全体をカンマ区切り値（CSV）ファイルにエクスポートします。テーブル全体より小さな単位でのエクスポートはできません。Security Manager サーバ上のファイル名とフォルダの入力を求められます。

IPS センサーのリブート

Security Manager から IPS センサーをリブートできます。

センサーをリブートするには、[デバイス（Device）] ビューでセンサーを選択して、[デバイスのリブート（Reboot Device）] を右クリックして選択します。リブートを確認するように求められます。

Security Manager はリブート プロセスのステータス情報を表示しません。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。