# デバイス インベントリの管理

次の項では、デバイス インベントリを管理する方法について説明します。



## デバイス インベントリについて

Security Manager は、管理対象のデバイスのインベントリを保持します。インベントリにはデバイスを特定してログインするために必要な情報が格納されており、ログインしたデバイスにポリシーを展開できます。次の項では、デバイスインベントリに関連する一般概念について説明します。



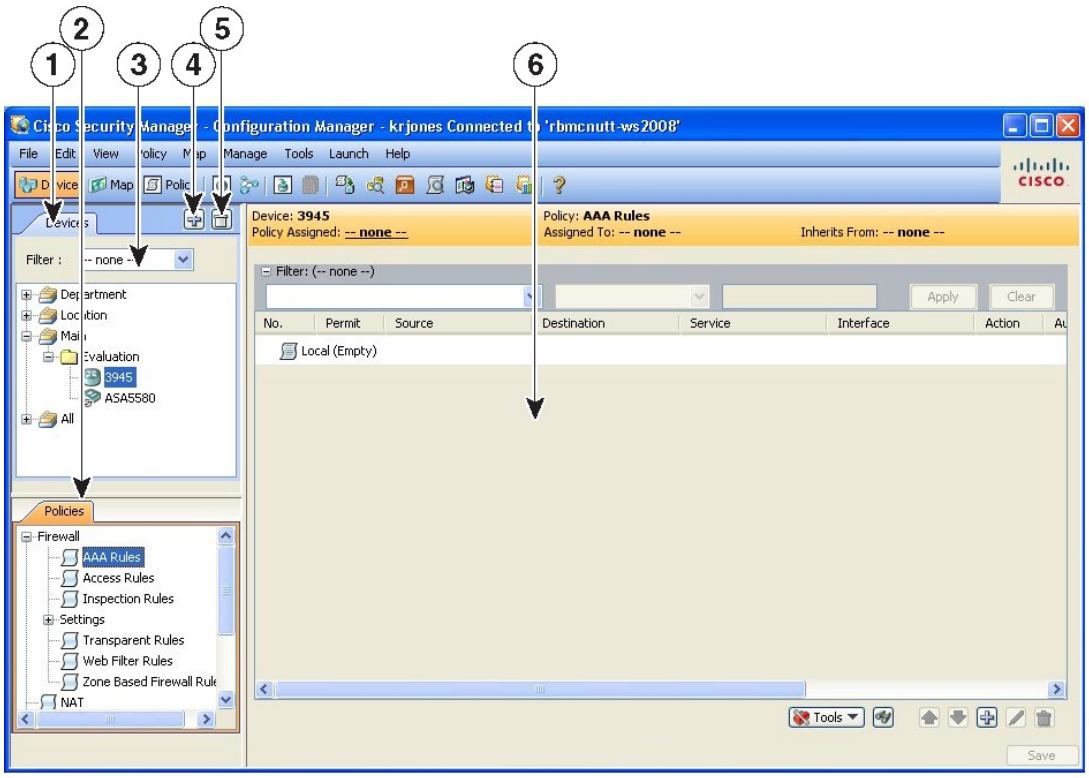
### デバイス ビューについて

[Device View] ボタンを押すと、[Devices] ページが開きます。ここでは、Security Manager インベントリに対するデバイスの追加と削除、デバイスのポリシー、プロパティ、およびインターフェイスの一元管理を行うことができます。

これはデバイス中心のビューであり、すべての管理対象デバイスを表示したり、特定のデバイスを選択してそのプロパティの表示や設定とポリシーの定義を行うことができます。特定のデバイスにセキュリティ ポリシーをローカルに定義できます。その後、そのポリシーを共有して、他のデバイスにグローバルに割り当てることができます。

[Devices] ページには、ペインが 2 つあります。左ペインには要素が 2 つあり、左上にデバイス セレクタ、左下にポリシーセレクタが配置されています。右ペインはメインのコンテンツ領域です。次の図に、[Devices] ページを示します。

**図 *1 : [Devices]* ページ**




**デバイスセレクタ（1、3、4、5）**：次の要素が含まれています。

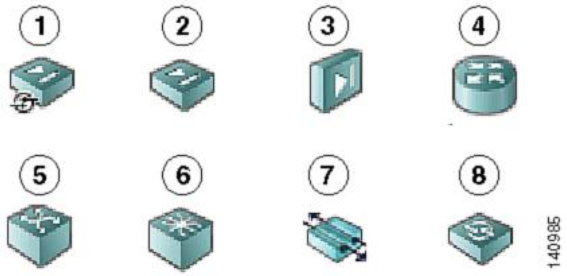
- [Add]/[Delete] ボタン（4、5）：Security Manager インベントリに対してデバイスの追加と削除を行うことができます。
- [Filter] フィールド（3）：独自に定義したフィルタリング基準に基づいて、デバイスのサブセットを表示できます。詳細については、セレクタ内の項目のフィルタリングを参照してください。
- [Device] ツリー：システムに存在するデバイス グループおよびデバイスを一覧表示します。各デバイス タイプが、アイコンで表されます。アイコンについては、図 2 : デバイスのアイコン を参照してください。

マウスのポインタをデバイスの上に置くと、デバイスに関する詳細情報がポップアップ ウィンドウに表示されます。情報は、デバイスプロパティの概要です（[デバイスのプロパティ（Device Properties）] : [全般（General）] ページ （52 ページ）を参照）。

（注） バージョン 4.8 以降、Security Manager は、Auto Update Server（AUS）を使用してアップグレードされたデバイスの更新されたバージョン情報を表示します。この機能を有効にするには、AUS ユーザーインターフェイスで Security Manager の詳細情報を設定する必要があります。デバイスにマウスのカーソルを合わせると、AUS がデバイスバージョンを正常に更新した場合、次のメッセージが表示されます。

「State Description: Version update is successfully completed by Auto Update Server. Check if any other configuration changes are required in Security Manager.」（状態の説明：Auto Update Server によるバージョンの更新が正常に完了しました。Security Manager で他の設定変更が必要かどうかを確認してください）

**図 *2:* デバイスのアイコン**




| | | | |
|---|---|---|---|
| 1 | Adaptive Security Appliance（ASA） | 5 | Catalyst スイッチ |
| 2 | PIX ファイアウォール | 6 | Catalyst 7600 シリーズ ルータ |
| 3 | Catalyst セキュリティ サービス モジュール：Firewall Services Module（FWSM; ファイアウォール サービス モジュール）および ASA-SM | 7 | VPN 3000 コンセントレータ |
| 4 | Cisco IOS ルータ | 8 | 侵入防御システム（IPS） |

- ショートカット メニュー オプション：デバイスまたはデバイス グループを右クリックすると、そのデバイスまたはグループに関連するコマンドのメニューが表示されます。これらのコマンドは、通常のメニューで使用できるコマンドへのショートカットです。

**ポリシーセレクタ（2）**：次の要素が含まれています。

- ポリシー グループ：選択されたデバイス タイプでサポートされているポリシー グループを一覧表示します。表示されるポリシー グループは、次の 4 つの要因によって決まります。
  - デバイス セレクタで選択されているデバイスのタイプ。
  - デバイスで実行されているオペレーティング システム。

- 生成した設定に使用できるコマンドを決定するために選択したターゲットのオペレーティング システム バージョン。
- サポートされているサービス モジュールがデバイスに含まれているかどうか。

詳細については、ポリシーについてを参照してください。

- ショートカット メニュー オプション：ポリシーを右クリックすると、そのポリシーに関連するコマンドのメニューが表示されます。これらのコマンドは、通常のメニューで使用できるコマンドへのショートカットです。

**[コンテンツ（Contents）] ペイン（6）**：メインのコンテンツ領域。

この領域に表示される情報は、デバイス セレクタから選択しているデバイスおよびポリシー セレクタから選択しているオプションによって異なります。

# デバイス名およびデバイスと見なされる要素について

Security Manager では、従来のデバイスの管理のほか、あるタイプのセキュリティ デバイスに定義できる仮想デバイスも管理できます。このような仮想デバイスは、デバイス インベントリでは独立したデバイスとして扱われ、デバイス セレクタには独立したエントリとして表示されます。仮想デバイスは実際にはホストとなる物理デバイス上にあるため、展開など多くのアクションにはホスト デバイスだけでなく仮想デバイスも含める必要があります。

物理デバイスはすべて、デバイス セレクタに表示されます。また、デバイス セレクタに表示されるタイプの仮想デバイスでもあります。

- セキュリティ コンテキスト：PIX ファイアウォール、FWSM デバイス、ASA デバイスにセキュリティ コンテキストを定義できます。セキュリティ コンテキストは、仮想ファイアウォールとして機能します。デフォルトでは、セキュリティコンテキストは、*host-display-name_context-name* という命名ルールに基づいてデバイスセレクタに表示されます。*host-display-name* はコンテキストが定義されているデバイスの表示名で、*context-name* はセキュリティコンテキストの名前です。たとえば、firewall12 というデバイスにある admin セキュリティ コンテキストの場合は firewall12_admin となります。

ヒント [検出設定（Discovery settings）] ページ（[Discovery] ページを参照）の [セキュリティコンテキスト名を生成するときにデバイス名を先頭に追加する（Prepend Device Name when Generating Security Context Names）] プロパティを使用して、表示名をコンテキスト名に追加するかどうかを制御できます。ただし、表示名を追加しないと、コンテキストをホストしているデバイスを特定するのが容易ではなく、コンテキスト名がホストデバイスでソートされません（コンテキスト名が、ホストデバイスに付加されるフォルダに表示されません）。表示名を追加しないと、複数のコンテキストが同じ名前でインベントリに追加されている場合には、Security Manager がコンテキスト名に数値のサフィックスを追加します（たとえば、admin_01、admin_02）。このような数値は、ホスト デバイスとは関連がありません。

- 仮想センサー：IPS デバイスに仮想センサーを定義できます。仮想センサーは、*host-display-name_virtual-sensor-name* という命名ルールでデバイスセレクタに表示されます。この命名ルールを制御するための検出設定はありません。

ヒント　デバイスのプロパティでは、仮想センサー、セキュリティコンテキスト、または他のデバイスのタイプの表示名をいつでも変更できます。

仮想デバイスの命名ルールのほか、さまざまなタイプのデバイス名間の関係についても理解する必要があります。

- 表示名：表示名は、単にデバイス セレクタの Security Manager 内に表示される名前です。実際にデバイスに定義されている名前に関連している必要はありません。デバイスをインベントリに追加する際、入力した DNS 名または IP アドレスに基づいて表示名が提案されますが、任意の命名ルールを使用できます。
- DNS 名：デバイスに定義する DNS 名は、Security Manager サーバ向けの DNS サーバによって解決可能である必要があります。
- IP アドレス：デバイスに定義する IP アドレスは、そのデバイスの管理 IP アドレスである必要があります。
- ホスト名：デバイスを検出すると、デバイスプロパティに表示されるホスト名プロパティがデバイスの設定から取得されます。設定ファイルを使用してデバイスを追加する場合に、ファイルにホスト名コマンドが含まれていないと、設定ファイルの名前が初期ホスト名となります。

ただし、デバイスでホスト名を変更しても、ホスト名デバイスプロパティは更新されません。デバイス プラットフォーム ポリシー領域に [Hostname] ポリシーがあり、この [Hostname] ポリシーによってデバイスに定義されるホスト名が決まります。

# デバイス クレデンシャルについて

Security Manager では、デバイスにログインする際にクレデンシャルが必要になります。デバイス クレデンシャルは次の 2 つのタイミングで提供できます。

- 手動またはネットワーク検出からデバイスを追加するとき。詳細については、次の項を参照してください。
  - ネットワークからのデバイスの追加　（14 ページ）
  - 手動定義によるデバイスの追加　（30 ページ）
- デバイス プロパティを編集するとき。詳細については、デバイス プロパティの表示または変更　（51 ページ）を参照してください。

次のデバイス クレデンシャルを指定できます。

- プライマリ クレデンシャル：SSH または Telnet を使用してデバイスにログインするためのユーザ名およびパスワード。デバイス通信には、この情報が必要です。
- HTTP クレデンシャル：HTTP 接続または HTTPS 接続を許可するデバイスもあれば、その接続を必要とするデバイス（IPS デバイスなど）もあります。デフォルトでは、Security Manager は HTTP/HTTPS アクセスにプライマリ クレデンシャルを使用しますが、一意の HTTP/HTTPS クレデンシャルを設定できます。
- Rx-Boot モード：（任意）Cisco ルータの中にはフラッシュ メモリから実行されるように設計されているものがあり、フラッシュの最初のファイルからだけ起動されます。つまり、フラッシュ イメージをアップグレードするには、フラッシュ内のイメージ以外のイメージを実行する必要があります。そのイメージが、Rx-Boot と呼ばれるサイズを小さくしたコマンド セット イメージ（ROM ベースのイメージ）です。
- SNMP クレデンシャル：（任意）簡易ネットワーク管理プロトコル（SNMP）を使用すると、ネットワーク デバイス間で管理情報を容易に交換できます。SNMP を使用すると、ネットワーク管理者は、ネットワークのパフォーマンスを管理し、ネットワークの問題を検出および解決し、ネットワークの拡大に対する計画を策定できます。

（注） PIX、ASA、および FWSM デバイスでは、ユーザ名を 4 文字以上にする必要があります。パスワードには、3 ～ 32 文字を使用できますが、8 文字以上にすることを推奨します。ソフトウェア バージョン 9.6(1) 以降を実行している ASA デバイスの場合、最大 127 文字のパスワードを入力できます。

デバイス ベースのクレデンシャルを使用するのではなく、Security Manager にログインするときに使用するクレデンシャルを使用するように、Security Manager を設定できます。その後、AAA サーバーのアカウンティング機能を使用して、ユーザーによる設定変更を追跡することができます。ユーザ ログイン クレデンシャルが適しているのは、次の基準に従って、ご使用の環境が設定されている場合だけです。

- 変更の監査に TACACS+ または RADIUS を使用します。ユーザ ログイン クレデンシャルが、このようなアカウンティング レコードに反映されます。デバイス クレデンシャルを使用した場合は、Security Manager でのすべての変更が、どのユーザがその変更を加えたかに関係なく、同じアカウントによるものとなります。
- ユーザ アカウントは AAA サーバに設定されており、設定変更を実行するために必要なデバイス レベルのアクセス権が付与されています。
- 認可に AAA サーバを使用するように Security Manager および管理対象デバイスを設定します。AAA を使用するように Cisco Security Manager を設定する方法の詳細については、Cisco Security Manager インストレーションガイド [英語] を参照してください。
- ワンタイム パスワードは使用しません。

ネットワーク設定でユーザー ログイン クレデンシャルをサポートしている場合は、**[ツール（Tools）] > [Security Manager管理（Security Manager Administration）]** を選択して、そのクレデンシャルを使用するように Security Manager を設定できます。コンテンツテーブルから [デ

バイス通信（Device Communication）] を選択し、[デバイスへの接続方法（Connect to Device Using）] フィールドで [Security Managerのユーザーログイン資格情報（Security Manager User Login Credentials）] を選択します。デフォルトでは、すべてのデバイス アクセスにデバイス クレデンシャルが使用されます。

### 関連項目

- [Device Credentials] ページ （58 ページ）
- デバイス インベントリへのデバイスの追加 （8 ページ）
- [Device Communication] ページ

# デバイス プロパティについて

デバイスを Security Manager に追加するときには、デバイス プロパティを定義します。デバイス プロパティは、デバイス、クレデンシャル、デバイスが割り当てられているグループ、およびポリシー オーバーライドに関する一般的な情報です。デバイス アイデンティティやプライマリ クレデンシャルなど一部のデバイス プロパティ情報はデバイスを追加するときに指定する必要がありますが、[Device Properties] ダイアログボックスからプロパティを追加または編集できます。

デバイス プロパティを表示するには、デバイス セレクタで次のどちらかを実行します。

- デバイスをダブルクリックします。
- デバイスを右クリックして、[デバイスのプロパティ（Device Properties）] を選択します。
- デバイスを選択して、[ツール（Tools）] > [デバイスのプロパティ（Device Properties）] の順に選択します。

[Device Properties] ダイアログボックスには、ペインが 2 つあります。左ペインにはコンテンツ テーブルがあり、次の項目が含まれています。

- [General]：デバイス アイデンティティ、デバイスで実行されているオペレーティング システム、およびデバイス通信設定など、デバイスに関する一般的な情報が含まれています。
- [Credentials]：デバイス プライマリ クレデンシャル（ユーザ名、パスワード、およびイネーブル パスワード）、SNMP クレデンシャル、Rx-Boot モード クレデンシャル、および HTTP クレデンシャルが含まれています。
- [Device Groups]：デバイスが割り当てられているグループが含まれています。
- [クラスタ情報（Cluster Information）]：クラスタ グループの詳細情報が含まれています（存在する場合）。
- [ライセンス情報（License Information）]：FPR-3100 シリーズ デバイスのライセンス ステータス、ライセンスの有効期限、およびライセンスの取得日に関する情報が含まれています。

（注） ライセンス情報パネルは、CSM 4.24 の FPR-3100 シリーズデバイスに対してのみ表示されます。

- [Policy Object Overrides]：再利用可能なポリシー オブジェクトのグローバル設定のうち、このデバイス用に上書きできるものが含まれています。

コンテンツ テーブルで項目を選択すると、対応する情報が右ペインに表示されます。

### 注記

- Security Manager は、[Device Properties] ページに表示される DNS ホスト名が、デバイスに設定したホスト名と同じであるとは想定していません。
- デバイスを Security Manager に追加するときには、管理 IP アドレスまたは DNS ホスト名を入力する必要があります。設定ファイルから検出するときには管理インターフェイスを特定できず、そのため管理 IP アドレスも特定できないため、設定ファイルに記載されたホスト名が DNS ホスト名として使用されます。設定ファイルの CLI にホスト名が見当たらない場合は、設定ファイル名が DNS ホスト名として使用されます。
- ネットワークからデバイスを検出するときには、[Device Properties] ページの DNS ホスト名が、デバイスに設定されたホスト名で更新されません。このため、デバイスの DNS ホスト名を指定する場合は、デバイスを Security Manager または [Device Properties] ページに追加するときに手動でそのホスト名を指定する必要があります。

デバイス プロパティの詳細については、デバイス プロパティの表示または変更 （51 ページ）を参照してください。

# デバイス インベントリへのデバイスの追加

デバイスを Security Manager に追加するときには、DNS 名や IP アドレスなど、デバイスの識別情報を指定します。この情報は、デバイス検出時に追加されます。ポリシー検出を開始して、デバイスに関連付けられた既存のネットワーク設定を取り込むこともできます。ポリシー検出の詳細については、ポリシーの検出を参照してください。追加したデバイスは、Security Manager デバイス インベントリに表示されます。

New Device ウィザードに従うと、デバイスをインベントリに追加するプロセスを実行できます。多種多様な追加元からデバイスを追加できます。ウィザードに至るパスは、使用する方法によって大きく異なります。

（注） Cisco Security Manager 4.21 以降では、ASA ソフトウェアの拡張機能とバグ修正は引き続きサポートされていますが、Cisco IOS ソフトウェアのサポートが終了しているため、ルータのハードウェアサポートは提供されません。

New Device ウィザードを起動するには、デバイスビューで [ファイル（File）] > [新規デバイス（New Device）] を選択するか、またはデバイスセレクタの [追加（Add）] ボタンをクリックします。

（注） デバイスを追加するには、他の方法もあります。デバイスインベントリだけではなく、割り当てられたポリシーおよびポリシーオブジェクトも含む .dev ファイルを別の Security Manager サーバーからエクスポートした場合、[ファイル（File）] > [インポート（Import）] コマンドを使用して、ファイルをインポートできます。詳細については、ポリシーまたはデバイスのインポートを参照してください。

### デバイスおよびサービス モジュールの追加に関するヒント

- PIX ファイアウォール、FWSM デバイス、および ASA デバイスがフェールオーバーに対応するように設定されている場合、アクティブ装置だけを Security Manager に追加します。デバイスに管理 IP アドレスを設定し、その IP アドレスを検出に使用するようにします。フェールオーバー対応のサービスモジュール（FWSM または ASA-SM）が複数含まれている Catalyst スイッチを検出するときは、画面の指示に従って、フェールオーバーモジュールに対して [モジュールを検出しない（Do Not Discover Module）] を選択します。Security Manager は、プライマリまたはセカンダリのどちらのフェールオーバー サービス モジュールが追加されたにかかわらず、常にアクティブな管理コンテキストを管理します。
- Security Manager は、ASA 設定ガイドで定義されている CLI ブートストラップを使用して ASA クラスタを 1 つのクラスタとして設定した後、ASA クラスタを管理できます（http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html [英語] を参照）。クラスタのすべてのメンバーには、ブートストラッププロセスの際に個別の IP アドレスが割り当てられます。クラスタを Security Manager に追加するときは、メインクラスタの IP アドレスを使用してクラスタを検出します。メインクラスタの IP アドレスは、そのクラスタの固定アドレスであり、常に現在の制御ユニットに属します。これは制御ユニットの個別の IP アドレスではありません。クラスタの詳細については、デバイスクラスタの使用 （11 ページ）を参照してください。
- サービス モジュールは、独立したデバイスとして扱われます。ほとんどのモジュールでは、ホスト デバイスとは別にサービス モジュールを追加する必要があります。ただし、Security Manager では Catalyst 6500 デバイスの FWSM モジュールまたは IDSM モジュールを自動的に検出できるため、親デバイスを追加するだけで十分です。（ASA-SM は、親デバイスの検出中に検出できません。ASA-SM を個別に追加する必要があります）この唯一の例外は、HTTPS（SSL）にデフォルト以外のポートを使用するように FWSM モジュールまたは IDSM モジュールを設定する場合です。この場合、モジュールを個別に追加する必要があります。
- セキュリティ コンテキストが複数ある ASA-SM または FWSM を追加するときには（これらはマルチ コンテキスト モードで動作しています）、それぞれの管理 IP アドレスを使用してセキュリティ コンテキストを個別に追加しないでください。その代わりに、管理コンテキストの管理アドレスを使用してデバイスを追加します（これにより、個々のコンテキストも追加されます）。次に、Security Manager でマルチ コンテキストの FWSM に設定を

展開する方法の変更の説明に従って、マルチ コンテキスト デバイスに設定をシリアルに展開するように Security Manager を設定します。

- Security Manager ライセンスに定義されているデバイス制限を超えてデバイスを追加することはできません。たとえば、50 台のデバイスのライセンスを保有し、インベントリに 45 台のデバイスがある場合、セキュリティ コンテンツが 6 個あるマルチ コンテキスト ASA を追加しようとすると、デバイスの追加と検出が失敗します。

次の項では、デバイスを追加するさまざまな方法について説明します。

- [ネットワークからのデバイスの追加（Add Device from Network）]：ネットワークで現在アクティブなデバイスを追加するには、ネットワークからのデバイスの追加 （14 ページ）を参照してください。Security Manager は、デバイスに直接かつ安全に接続し、その識別情報およびプロパティを検出します。
  - **長所**：デバイスに関する最小限の情報を指定すればよく、Security Manager がデバイスから直接詳細な情報を取得して正確性を保ちます。
  - **短所**：追加できるデバイスは一度に 1 つだけです。ダイナミック IP アドレスが付与されているデバイスを追加するには、デバイスの現在の IP アドレスを特定し、そのアドレスを使用してデバイスを追加し、デバイスを管理している Configuration Engine を特定するように Security Manager でデバイスプロパティを更新する必要があります。
- [構成ファイルからの追加（Add from Configuration File）]：デバイス構成ファイルのコピーを使用してデバイスを追加するには、設定ファイルからのデバイスの追加 （26 ページ）を参照してください。
  - **長所**：一度に複数のデバイスを追加できます。
  - **短所**：この方法では、Catalyst 6500/7600 デバイスおよび IPS デバイスを追加できません。設定ファイルをいくつかまとめて追加するときには、そのどちらのファイルも同じデバイス タイプである必要があります。

また、デバイスとの接続を必要とするポリシーを正常に検出できません。たとえば、ポリシーがデバイスに存在するファイルを指している場合、構成ファイルを使用してデバイスを追加すると、Security Manager がデバイスから参照先のファイルを取得できないため、Security Manager 設定に **no** 形式のコマンドが含まれることになります。たとえば、Web VPN の **svc image** コマンドが無効になることがあります。

- [新規デバイスの追加（Add New Device）]：ネットワークにまだ存在しないデバイスを追加して Security Manager でそのデバイスを事前プロビジョニングできるようにするには、手動定義によるデバイスの追加 （30 ページ）を参照してください。デバイス ハードウェアを設置する前に、システムでデバイスを作成し、ポリシーをデバイスに割り当て、設定ファイルを生成できます。
  - **長所**：ネットワークにまだ存在しないデバイスを事前プロビジョニングできます。
  - **短所**：他の方法よりも詳細な情報を指定する必要があります。Catalyst 6500 デバイス、または IPS モジュールが含まれているルータを作成する場合、[ポリシー（Policy）]>

[デバイス上のポリシーを検出する（Discover Policies on Device）] を選択して、そのモジュールを検出する必要があります。

- [ファイルからのデバイスの追加（Add Device from File）]：カンマ区切り値（CSV）形式のインベントリファイルからデバイスを追加するには、インベントリ ファイルからのデバイスの追加 （37 ページ）を参照してください。
  - **長所**：タイプの異なる複数のデバイスを一度に追加できます。CiscoWorks Common Services、Cisco Security Monitoring, Analysis and Response System（CS-MARS）、その他の Security Manager サーバなど、他のネットワーク管理アプリケーションのインベントリ リストを再利用できます。別の Security Manager サーバからエクスポートされたファイルを使用する場合は、ポリシーを検出するせずに任意でデバイスを追加できます。これは、オフライン デバイスまたはスタンバイ デバイスを追加する場合に便利です。
  - **短所**：この方法では、インベントリですでに定義されているデバイスのプロパティを更新できません。また、100 を超えるデバイスを一度にインポートしようとすると、ポリシー検出が失敗することがあり、それより少ない数でも失敗する可能性があります。IPS デバイスの場合には、ポリシー検出の失敗を避けるため、5 台以上の IPS デバイスを一度に追加しないでください。

# デバイスクラスタの使用

クラスタリングを利用すると、複数のデバイスをグループ化して 1 つの論理デバイスとすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。クラスタリングは、9.0(1) 以降を実行している ASA 5580 および 5585 デバイス、および 9.1(4) 以降を実行している ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X デバイスでサポートされています。

（注） CSM 4.27 以降では、ASA 9.20(1) で実行されている Cisco Secure Firewall 4200 シリーズデバイスクラスタを検出して展開できます。

Security Manager は、ASA 設定ガイドで定義されている CLI ブートストラップを使用して ASA クラスタを 1 つのクラスタとして設定した後、ASA クラスタを管理できます（http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html [英語] を参照）。

クラスタのすべてのメンバーには、ブートストラッププロセスの際に個別の IP アドレスが割り当てられます。クラスタを Security Manager に追加するときは、メインクラスタの IP アドレスを使用してクラスタを検出します。メインクラスタの IP アドレスは、そのクラスタの固定アドレスであり、常に現在の制御ユニットに属します。これは制御ユニットの個別の IP アドレスではありません。

（注） 必要なCLIブートストラップを実行した後にデバイスを再検出しても、スタンドアロンデバイスを Security Manager のクラスタに変換することはできません。最初に Security Manager からデバイスを削除する必要があります。次に、必要なCLIブートストラップを実行した後で、クラスタを新しいデバイスとして Security Manager に追加できます。

Security Manager ではクラスタは単一のデバイスとして表されます。クラスタが Security Manager に追加されたら、クラスタインターフェイスやセキュリティポリシーなどのクラスタ設定の構成を完了することができます。

（注） クラスタリングには、設定に関する特定の要件および制限があります。要件、設定の推奨事項、およびパフォーマンス情報の詳細については、http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html にある ASA のドキュメントを参照してください。

### ASA クラスタでサポートされない機能

これらの機能は、クラスタリングがイネーブルのときは設定できず、コマンドは拒否されます。

- ユニファイド コミュニケーション
- リモート アクセス VPN（SSL VPN および IPSec VPN）
- 次のアプリケーション インスペクション：
  - CTIQBE
  - GTP
  - H323、H225、および RAS
  - IPsec パススルー
  - MGCP
  - MMP
  - RTSP
  - SIP
  - SCCP（Skinny）
  - WAAS
  - WCCP
- ボットネット トラフィック フィルタ
- Auto Update Server

- DHCP クライアント、サーバ、リレー、およびプロキシ
- VPN ロード バランシング
- フェールオーバー
- ASA CX モジュール

### 中央集中型機能

次の機能は、制御ユニット上だけでサポートされます。クラスタの場合もスケーリングされません。たとえば、8 ユニット（5585-X と SSP-60）から成るクラスタがあるとします。Other VPN ライセンスでは、1 台の ASA 5585-X と SSP-60 に対して許可される IPSec トンネルの最大数は 10,000 です。8 ユニット クラスタ全体で使用できるトンネル数は 10,000 までです。この機能はスケーリングしません。

（注） 中央集中型機能のトラフィックは、メンバーユニットから制御ユニットに、クラスタ制御リンクを介して転送されます。クラスタ制御リンク用に十分な帯域幅を確保するには、ASA ドキュメントの「クラスタ制御リンクのサイジング」を参照してください。再分散機能を使用する場合は、中央集中型機能のトラフィックが中央集中型機能として分類される前に再分散が行われて、制御ユニット以外のユニットに転送されることがあります。この場合は、トラフィックが制御ユニットに送り返されます。中央集中型機能については、制御ユニットで障害が発生するとすべての接続がドロップされるので、新しい制御ユニット上で接続を再確立する必要があります。

- サイト間 VPN
- 次のアプリケーション インスペクション：
  - DCERPC
  - NetBios
  - PPTP
  - RADIUS
  - RSH
  - SUNRPC
  - TFTP
  - XDMCP
- ダイナミック ルーティング（スパンド EtherChannel モードのみ）
- マルチキャスト ルーティング（個別インターフェイス モードのみ）
- スタティック ルート モニタリング

- IGMP マルチキャスト コントロール プレーン プロトコル処理（データ プレーン転送はクラスタ全体に分散されます）
- PIM マルチキャスト コントロール プレーン プロトコル処理（データ プレーン転送はクラスタ全体に分散されます）
- ネットワーク アクセスの認証および許可。アカウンティングは非集中型です。
- フィルタリング サービス

### 個々のユニットに適用される機能

これらの機能は、クラスタ全体ではなく、個々の ASA ユニットに適用されます。

- QoS：QoS ポリシーは、コンフィギュレーション複製の一部としてクラスタ全体で同期されます。ただし、ポリシーは、各ユニットに対して個別に適用されます。たとえば、出力に対してポリシングを設定する場合は、適合レートおよび適合バースト値は、特定の ASA から出て行くトラフィックに適用されます。8 ユニットから成るクラスタがあり、トラフィックが均等に分散している場合は、適合レートは実際にクラスタのレートの 8 倍になります。
- 脅威検出：脅威検出は、各ユニットに対して個別に機能します。たとえば、上位統計情報は、ユニット別です。たとえば、ポート スキャン検出が機能しないのは、スキャン トラフィックが全ユニット間で分散されるので、1 つのユニットがすべてのトラフィックを読み取ることはないからです。
- リソース管理：マルチ コンテキスト モードでのリソース管理は、ローカル使用状況に基づいて各ユニットに個別に適用されます。
- IPS モジュール：IPS モジュール間でのコンフィギュレーションの同期や状態の共有は行われません。IPS シグニチャによっては、IPS が複数の接続にわたって状態を保持することが必要になります。たとえば、ポート スキャン シグニチャが使用されるのは、同じ人物が同じサーバーへの多数の接続を、それぞれ異なるポートを使用して開いていることを IPS モジュールが検出した場合です。クラスタリングでは、これらの接続は複数の ASA デバイス間で分散されます。これらのデバイスそれぞれに専用の IPS モジュールがあります。これらの IPS モジュールはステート情報を共有しないので、結果としてのポート スキャンをクラスタが検出できない場合があります。

### 関連項目

- [グループ情報（Group Information）] ページ （64 ページ）

# ネットワークからのデバイスの追加

デバイスをインベントリに追加する最も簡単で最も信頼性の高い方法の 1 つに、ネットワークでアクティブであるデバイスを特定するというものがあります。デバイスの IP アドレス（または DNS ホスト名）およびデバイスへのログインに必要なクレデンシャルを提供すると、

Security Manager では必要な情報の多くをデバイスから直接取得して、情報の精度を確保できます。

### はじめる前に

この手順を開始する前に、次の準備が完了していることを確認してください。

- Security Manager で管理されるデバイスを準備します。詳細については、デバイスを管理するための準備を参照してください。
- 認証に ACS を使用する場合は、ACS でデバイスを定義します。『Installation Guide for Cisco Security Manager』を参照してください。

### 関連項目

- デバイス ビューについて （1 ページ）
- デバイス グループの使用 （79 ページ）
- デバイス プロパティの表示または変更 （51 ページ）

---

**ステップ 1** デバイスビューで [ファイル（File）] > [新規デバイス（New Device）] を選択するか、デバイスセレクタの [追加（Add）] ボタンをクリックします。[Choose Method] ページに New Device ウィザードが開きます。

**ステップ 2** [方式を選択（Choose Method）] ページで、[ネットワークからのデバイスの追加（Add Device from Network）] を選択し、[次へ（Next）] をクリックして [デバイス情報（Device Information）] ページを開きます。

**ステップ 3** [Device Information] ページで、少なくとも次のフィールドに値を入力します。すべてのフィールドの詳細については、 [Device Information] ページ - [Add Device from Network] （17 ページ）を参照してください。

- ホスト名と DNS 名、または IP アドレス（あるいはその両方）を入力します。
- 表示名を入力します。この名前は Security Manager のデバイス セレクタに表示されます。
- 正しいオペレーティング システムとバージョンを選択します。Catalyst スイッチまたは 7600 ルータを設定している場合は、[IOS - Catalyst Switch/7600] を選択し、それ以外の IOS エントリは選択しません。
- Security Manager に定義されているデフォルトとは異なるプロトコルを使用するようにデバイスが設定されている場合には、デバイスにログインするのに使用するトランスポート プロトコルを選択します。デフォルトは、[Device Communication] 管理ページに設定されています（[Device Communication] ページを参照）。

[次へ（Next）] をクリックします。

**ステップ 4** [Device Credentials] ページで、デバイスへのログインに必要なユーザ名およびパスワードを入力します。少なくともプライマリ デバイス クレデンシャルを入力します。これは、従来のユーザ EXEC モードと特権 EXEC モードのパスワードです。

クレデンシャルの各種タイプについては、 [Device Credentials] ページ （58 ページ）を参照してください。

**ヒント** [Device Credentials] ページで [Next] または [Finished] をクリックすると、Security Manager はデバイスに接続できるかどうかをテストします。テストが正常に完了しないかぎり、デバイスは追加できません。詳細については、デバイス接続のテストを参照してください。

**ステップ 5** （任意）[次へ（Next）] をクリックして [デバイスのグルーピング（Device Grouping）] ページを開き、インポートしたデバイスの追加先となるデバイスグループを選択します（ [Device Groups] ページ （63 ページ）を参照）。

**ステップ 6** [終了（Finish）] をクリックします。Security Manager が [Discovery Status] ダイアログボックスを開きます。ここでは、デバイス検出およびポリシー分析のステータスを参照できます（[Discovery Status] ダイアログボックスを参照）。

**ヒント** デバイスの追加中にポリシーを検出している場合は、提示されているメッセージをよくお読みください。これらのメッセージには、次に実行する手順に関する重要な推奨事項が含まれている場合があります。Security Manager が設定の所有権を引き継ぐことができるように、検出した設定をファイルにすぐに展開することを推奨します。展開方法の詳細については、展開方法についてを参照してください。

**ステップ 7** モジュールが含まれているデバイスを追加し、Security Manager がそのタイプのデバイスでモジュールの検出をサポートしている場合、デバイスシャーシの検出が完了したときに通知され、デバイスのモジュールを検出するかどうかを確認されます。[はい（Yes）] をクリックすると、次の情報の入力を要求されます。

- Catalyst 6500 サービス モジュール：[Service Module Credentials] ダイアログボックスが開き、シャーシに含まれているモジュールに基づいて次の情報の入力が要求されます。詳細については、 [Service Module Credentials] ダイアログボックス （22 ページ）を参照してください。
  - FWSM：管理 IP アドレス（推奨する）、ユーザ名とパスワード、および実行する検出のタイプ。FWSM がフェールオーバーペアの 2 番めのデバイスである場合は、フェールオーバーモジュールの [モジュールを検出しない（Do Not Discover Module）] を選択します。（Security Manager は、プライマリまたはセカンダリのどちらのフェールオーバー サービスモジュールが追加されたにかかわらず、常にアクティブな管理コンテキストを管理します）。
  - IDSM：ユーザ名とパスワード、および実行する検出のタイプ。
  - ASA-SM：Catalyst 6500 で、シャーシ経由での ASA サービス モジュールの検出はサポートされません。ASA-SM は、ASA-SM の管理 IP アドレスを使用して直接追加する必要があります。

    （注） Cisco Security Manager 4.21 以降では、ASA ソフトウェアの拡張機能とバグ修正は引き続きサポートされていますが、Cisco IOS ソフトウェアのサポートが終了しているため、ルータのハードウェア サポートは提供されません。

- IPS ルータ モジュール：実行する検出のタイプ、管理 IP アドレス、ユーザ名とパスワード、およびその他の SSL 接続情報。詳細については、 [IPS Module Discovery] ダイアログボックス （24 ページ）を参照してください。

Security Manager で管理しないモジュールの検出をスキップできます。

[OK] をクリック [Discovery Status] ダイアログボックスに戻り、サービス モジュールの検出の経過を表示できます。完了したらウィンドウを閉じます。デバイスがインベントリ リストに追加されます。リストに掲載するすべてのデバイスのアクティビティ（たとえば、ASA デバイスに定義されている個々のセキュリティ コンテキスト）を送信する必要がある場合には、メッセージにその説明が示されます。

**ステップ 8** デバイスセレクタでデバイスを選択して Auto Update Server または Configuration Engine によって管理されているデバイスを追加した場合は、[ツール（Tools）] > [デバイスのプロパティ（Device Properties）] を選

択します。[Auto Update] または [Configuration Engine] 設定で、デバイスで使用するサーバを選択します。サーバがリストにない場合は追加できます。詳細については、Auto Update Server または Configuration Engine の追加、編集、または削除 （45 ページ）を参照してください。

## [Device Information] ページ - [Add Device from Network]

ネットワークからデバイスを追加する場合は、New Device ウィザードの [デバイス情報（Device Information）] ページを使用して、デバイスの識別情報を指定します。

（注） バージョン 4.21 以降、Cisco Security Manager は、すべてのアグリゲーション サービス ルータ、統合サービスルータ、組み込みサービスルータ、および Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体を終了します。

### ナビゲーション パス

New Device ウィザードを起動するには、デバイスビューで [ファイル（File）] > [新規デバイス（New Device）] を選択するか、デバイスセレクタの [追加（Add）] ボタンをクリックします。

### 関連項目

- デバイス ビューについて （1 ページ）
- ネットワークからのデバイスの追加 （14 ページ）
- [Device Credentials] ページ （58 ページ）
- [Device Groups] ページ （63 ページ）
- ポリシーの検出
- [Device Communication] ページ

### フィールド リファレンス

**表 *1* : ネットワークからデバイスを追加する場合に使用する *New Device* ウィザードの *[Device Information]* ページ**

| 要素 | 説明 |
|---|---|
| ID | |

| 要素 | 説明 |
|---|---|
| IP タイプ（IP Type） | デバイスの IP アドレスをスタティックにする（デバイスで定義する）か、またはダイナミックにする（DHCP サーバから取得する）かを指定します。選択した IP タイプによって、表示されるフィールドが異なります。<br>スタティック IP アドレスを持つデバイスだけを追加できます。<br>（DHCP サーバから提供される）ダイナミック アドレスを使用するデバイスを追加するには、デバイスの現在の IP アドレスを特定し、そのアドレスを使用します。デバイスを追加したあと、そのプロパティで [IP Type] を [Dynamic] に変更し、デバイスを管理している AUS または Configuration Engine を特定します。<br>（注） バージョン 4.12 以降、ASA デバイスに対する Cisco Security Manager サーバーからデバイスへの通信は、IPv6 アドレスまたは IPv4 アドレスのいずれかでサポートされます。IPv6 アドレスは 128 ビットの一意のアドレスです。IPv6 アドレスについては、スタティック IP タイプのみがサポートされています。ダイナミック IP タイプは、IPv6 アドレスではサポートされません。 |
| ホストネーム | デバイスの DNS ホスト名。IP アドレスが不明な場合に、DNS ホスト名を入力します。<br>（注） DNS ホスト名と IP アドレスのどちらか一方、または両方を入力する必要があります。 |
| ドメイン名 | デバイスの DNS ドメイン名。 |
| IP Address | デバイスの管理 IP アドレス。IP アドレスは、10.64.3.8 というように、ドット付きの 4 つの数字列でなければなりません。<br>（注） IP アドレスと DNS ホスト名のどちらか一方、または両方を入力する必要があります。<br>（注） バージョン 4.12 以降、ASA デバイスに対する Cisco Security Manager サーバーからデバイスへの通信は、IPv6 アドレスまたは IPv4 アドレスのいずれかでサポートされます。デバイスがデュアルスタックで設定されている場合、Security Manager は、Security Manager に追加されたデバイスの IP アドレスに基づいてデバイスと通信します。IPv6 アドレスは 128 ビットの一意のアドレスです。 |
| 表示名 | Security Manager のデバイス セレクタに表示する名前。ホスト名または IP アドレスを入力した場合は、そのホスト名または IP アドレスがこのフィールドに自動的に入力されますが、変更することもできます。<br>最大長は 70 文字です。有効な文字は、0 ～ 9、大文字の A ～ Z、小文字の a ～ z、_ - . :、およびスペースです。<br>（注） 2 つのデバイスに同じ表示名を設定することはできません。 |

| 要素 | 説明 |
|---|---|
| OS タイプ | デバイスで実行されているオペレーティング システムのファミリ。慎重に正しいタイプを選択する必要があります。選択内容が、Security Manager がデバイスにログインし、デバイスの設定を取得する方法に影響を与えるためです。次のオプションがあります。<br>• [IOS 12.3+]：Cisco IOS ソフトウェアリリース 12.3 以降を実行している Cisco ルータの場合。Catalyst 6500/7600 または他の Catalyst デバイスの場合には選択しないでください。<br>ヒント Aggregation Services Router（ASR; アグリゲーション サービス ルータ）の場合は、バージョン 12.2 を実行中であっても、このオプションを選択します。ASR IOS リリースは、上位のリリースとして扱われます。<br>• [IOS - Catalystスイッチ/7600（IOS - Catalyst Switch/7600）]：すべての Catalyst スイッチおよび 7600 デバイスの場合。<br>• [ASA]：すべての ASA デバイスの場合。<br>• [FWSM]：すべての FWSM デバイスの場合。<br>• [IPS]：IPS ソフトウェアを実行しているすべてのデバイスの場合。<br>• [PIX]：すべての PIX デバイスの場合。<br>（注） バージョン 4.12 以降、ASA デバイスに対する Cisco Security Manager サーバーからデバイスへの通信は、IPv6 アドレスまたは IPv4 アドレスのいずれかでサポートされます。この機能は、オペレーティングシステムのタイプが ASA または FWSM であるデバイスでのみ使用できます。 |
| トランスポートプロトコル（Transport Protocol） | デバイスに接続するときに Security Manager で使用するプロトコル。デバイスに設定され、かつクレデンシャルを提供できるプロトコルを選択します。各デバイス タイプにはデフォルト プロトコルがあり、通常この方法がそれぞれのデバイスで使用されます。 |

| 要素 | 説明 |
|---|---|
| システムコンテキスト | マルチ コンテキスト モードで実行されている PIX ファイアウォール 7 デバイス、ASA デバイス、または FWSM デバイスのシステム実行スペースを検出するかどうかを指定します。複数のセキュリティ コンテキストをホストするデバイスを検出している場合は、このチェックボックスをオンにするかどうかが、Security Manager でデバイスを設定する方法に重要な意味を持ちます。デバイスで検出される対象も、[セキュリティコンテキストのポリシーを検出（Discover Policies for Security Contexts）] チェックボックスをオンにするかどうかによって異なります。<br>• [システムコンテキスト（System Context）] と [セキュリティコンテキストのポリシーを検出（Discover Policies for Security Contexts）] のどちらもオン：これが推奨する選択です。Security Manager は、デバイスに定義されているシステム実行スペースおよびすべてのセキュリティ コンテキストを検出して、デバイス セレクタに一覧表示します。[Discovery] ページ（[Discovery] ページを参照）に設定されたデフォルトの命名ルールを変更していないかぎり、基本表示名はシステム実行スペースを表したもの（たとえば、10.10.11.24）であり、セキュリティ コンテキストはノードではコンテキスト名をデバイス名に付加したもの（たとえば、10.10.11.24_admin）として表されます。<br>• [システムコンテキスト（System Context）] はオン、[セキュリティコンテキストのポリシーを検出（Discover Policies for Security Contexts）] はオフ：システム実行スペースが検出されて、デバイスセレクタに追加されます。あとでセキュリティ コンテキストのポリシーを検出できます。この方法は、インベントリを検出するユーザ グループと、さらにもう 1 つポリシーを検出するグループがある場合に適しています。<br>• どちらのチェックボックスもオフ：管理コンテキストだけが検出されて、デバイス セレクタに追加されます。他のセキュリティ コンテキストは検出できず、管理もできません。 |
| デバイス設定の検出 | |

| 要素 | 説明 |
|---|---|
| 検出 | 検出してインベントリに追加する要素のタイプ。次のオプションがあります。<br>• [Policies and Inventory]：ポリシー、インターフェイス、およびサービス モジュール（該当する場合）を検出します。これがデフォルトであり、推奨オプションです。<br><br>ポリシーの検出が開始されると、デバイス上の設定が分析され、設定されているサービスとプラットフォームのポリシーがインポートされます。インベントリの検出が開始されると、デバイス上のインターフェイスが分析され、インターフェイス リストがインポートされます。デバイスが複合デバイスの場合は、デバイス内のすべてのサービス モジュールが検出され、インポートされます。<br><br>このオプションを選択すると、下のチェックボックスがアクティブになり、それらのチェックボックスを使用して、検出されるポリシーのタイプを制御できます。<br><br>（注） 検出中に非アクティブな ACL をインポートすると、その ACL は Security Manager に無効な状態で表示されます。同じ ACL を展開すると、その ACL は Security Manager によって削除されます。<br><br>• [Inventory Only]：インターフェイスとサービス モジュール（該当する場合）を検出します。<br><br>• [No Discovery]：すべての検出がスキップされます。デバイスのポリシー、インターフェイス、またはサービス モジュール情報はデバイス インベントリに追加されません。 |
| プラットフォーム設定 | プラットフォーム固有のポリシー ドメインとも呼ばれるプラットフォーム設定を検出するかどうかを指定します。プラットフォーム固有のポリシー ドメインは、ファイアウォール デバイスと Cisco IOS ルータ上にあります。これらのドメインには、選択したプラットフォームに固有の機能を設定するポリシーが含まれています。詳細については、サービスポリシーとプラットフォーム固有のポリシーを参照してください。 |
| ファイアウォール ポリシー | ファイアウォール サービスとも呼ばれるファイアウォール ポリシーを検出するかどうかを指定します。ファイアウォール サービスには、アクセル ルール、インスペクション ルール、AAA ルール、Web フィルタ ルール、トランスペアレント ルールなどのポリシーが含まれます。詳細については、ファイアウォール サービスの概要を参照してください。 |
| IPS ポリシー | シグニチャや仮想センサーなどの IPS ポリシーを検出するかどうかを指定します。詳細については、IPS 設定の概要またはCisco IOS IPS 設定の概要を参照してください。 |

| 要素 | 説明 |
|---|---|
| RA VPN ポリシー | IKE プロポーザルや IPsec プロポーザルなどの IPSec および SSL リモート アクセス VPN ポリシーを検出するかどうかを指定します。デバイスがリモート アクセス VPN 設定をサポートしていない場合、このオプションはディセーブルになります。詳細については、リモート アクセス VPN の管理の基礎を参照してください。 |
| Discover Policies for Security Contexts | セキュリティ コンテキストのポリシーを検出するかどうかを指定します。セキュリティ コンテキストは、PIX ファイアウォール デバイス、ASA デバイス、または FWSM デバイスに適用されます。このフィールドは、[IPタイプ（IP Type）] に [スタティック（Static）] を選択し、[システムコンテキスト（System Context）] をオンにした場合にのみアクティブになります。 |

## [Service Module Credentials] ダイアログボックス

[Service Module Credentials] ダイアログボックスは、Catalyst デバイスのサポート対象のサービス モジュールにログインするときに必要なクレデンシャルを追加する場合に使用します。

このダイアログボックスではサポート対象のモジュールが各スロットにまとめられており、モジュールのタイプが示されています。たとえば、グループが **Slot 3 (IDSM) Credentials** という名前である場合、シャーシの 3 番めのスロットに IDSM があることを示しています。

（注） Security Manager は VPN モジュールを検出しますが、その検出はシャーシ経由で実施され、クレデンシャルは必要ありません。ASA サービスモジュール（ASA-SM）は、シャーシを介して検出できません。それらは個別に追加する必要があります。

### ナビゲーション パス

サービス モジュールを含めることができる Catalyst シャーシでポリシーを検出すると、そのサービス モジュールを検出するかどうかが確認されます。[はい（Yes）] をクリックすると、このダイアログボックスが表示されます。次のいずれかの方法を使用してポリシー検出を実行できます。

- ネットワークからデバイスを追加する場合。 ネットワークからのデバイスの追加 （14 ページ）を参照してください。
- エクスポート ファイルからデバイスを追加する場合。 インベントリ ファイルからのデバイスの追加 （37 ページ）を参照してください。
- インベントリにすでにあるデバイスでポリシー検出を実行する場合。Security Manager にすでに存在するデバイス上のポリシーの検出を参照してください。

## フィールド リファレンス

**表 *2 : [Service Module Credentials]* ダイアログボックス**

| 要素 | 説明 |
|---|---|
| Discovery Mode | このモジュールのために検出するポリシーのタイプ。<br>• [Discover Inventory and Policies]：インベントリとセキュリティ ポリシーを検出します。これは推奨オプションです。<br>• [Discover Inventory Only]：セキュリティ ポリシーは検出しませんが、VLAN 設定、セキュリティ コンテキスト、インターフェイスなどのインベントリは検出します。サービスモジュールを右クリックし、[デバイスでポリシーを検出（Discover Policies on Device）] を選択して、あとでポリシー設定を検出できます。<br>• [Do Not Discover Module]：このモジュールに対する検出をスキップし、このモジュールをインベントリに追加しません。 |
| Connect to FWSM | Security Manager が FWSM にアクセスする方法。<br>• [Directly]：FWSM の管理 IP アドレスを使用して、FWSM に接続します。この方法を推奨します。フェールオーバー デバイスに接続している場合には必須の方法となります。それ以外の場合、Security Manager はフェールオーバー後にスタンバイ FWSM に接続することがあります。<br>• [via Chassis]：シャーシ経由で FWSM に接続します。この方法には、FWSM に定義されているセキュリティ コンテキストの数が 20 個未満であるという制約があります。Security Manager は、SSH 経由で Catalyst デバイスに接続し、その後 **session** コマンドで FWSM に接続します。Catalyst デバイスでは同時 SSH セッションの数が制限されており、デフォルト値は 5 です。ポリシー検出ではセキュリティ コンテキストごとに 1 つの SSH セッションを使用するため、コンテキストの数が多くなると接続が失敗することがあります。[直接アクセス（Directly）] を選択した場合、Security Manager が SSL で FWSM に接続するため、同時セッションの制限が大きくなります。 |
| 管理 IP（Management IP） | サービス モジュールの管理 IP アドレス。<br>FWSM の場合、接続方法に [シャーシ経由（via Chassis）] を選択したときには、このフィールドは使用できません。 |

| 要素 | 説明 |
|---|---|
| ユーザー名 | サービス モジュールのユーザ名。<br>マルチコンテキストモードで動作するFWSMの場合、どのコンテキストのユーザー名およびパスワードを入力すればよいかが脚注に示されます。システムコンテキストか管理コンテキストのいずれかになります。スイッチのシャーシ経由でマルチコンテキストモードのデバイスに接続している場合は、システム実行スペースと管理コンテキストのいずれにも同じユーザ名およびパスワードを設定し、このダイアログボックスにそのクレデンシャルを指定する必要があります。<br>ユーザ名は、4 文字以上にします。パスワードには、3 ～ 32 文字を使用できますが、8 文字以上にすることを推奨します。ソフトウェア バージョン 9.6(1) 以降を実行している ASA デバイスの場合、最大 127 文字のパスワードを入力できます。 |
| パスワード | サービス モジュールのユーザ EXEC モード パスワード。[Confirm] フィールドに、パスワードを再入力します。 |
| パスワードを有効にする（Enable Password）<br>（FWSM 専用） | サービス モジュールの特権 EXEC モード パスワード。[Confirm] フィールドに、パスワードを再入力します。 |

# [IPS Module Discovery] ダイアログボックス

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしますが、拡張機能はサポートしていません。

[IPS Module Discovery] ダイアログボックスは、インベントリに追加しているルータで AIM-IPS や NME などの IPS モジュールへのログインに必要なクレデンシャルを追加する場合に使用します。

### ナビゲーション パス

IPS モジュールが含まれているルータ シャーシでポリシーを検出すると、そのモジュールを検出するかどうかが確認されます。[はい（Yes）] をクリックすると、このダイアログボックスが表示されます。次のいずれかの方法を使用してポリシー検出を実行できます。

- ネットワークからデバイスを追加する場合。ネットワークからのデバイスの追加 （14 ページ）を参照してください。
- インベントリ ファイルからデバイスを追加する場合。インベントリ ファイルからのデバイスの追加 （37 ページ）を参照してください。

- ネットワークにすでにあるデバイスでポリシー検出を実行する場合。Security Manager にすでに存在するデバイス上のポリシーの検出を参照してください。

## フィールド リファレンス

**表 3 : [IPS Module Discovery] ダイアログボックス**

| 要素 | 説明 |
|---|---|
| 検出 | このモジュールの検出のタイプ。<br>• [Discover Inventory and Policies]：インベントリとセキュリティ ポリシーを検出します。これは推奨オプションです。<br>• [Discover Inventory Only]：セキュリティ ポリシーは検出しませんが、仮想センサーやインターフェイスなどのインベントリは検出します。モジュールを右クリックし、[デバイスでポリシーを検出する（Discover Policies on Device）] を選択して、あとでポリシー設定を検出できます。<br>• [Do Not Discover Module]：このモジュールに対する検出をスキップし、このモジュールをインベントリに追加しません。 |
| IPアドレス | モジュールの管理 IP アドレス。 |
| **HTTP Credentials Group**<br>モジュールへのログインに必要なクレデンシャル。 | |
| ユーザー名 | モジュールのユーザ名。 |
| パスワード | 指定したユーザ名のパスワード。[Confirm] フィールドに、パスワードを再入力します。 |
| HTTP ポート（HTTP Port） | モジュールへの HTTP アクセス用に設定されたポート。デフォルトは 80 です。 |
| HTTPS ポート（HTTPS Port） | モジュールへの SSL（HTTPS）アクセス用に設定されたポート。デフォルトは、[デバイス通信（Device Communication）] ページ（[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] >[デバイス通信（Device Communication）]。詳細については、[Device Communication] ページを参照してください）に定義されています。通常使用されるポートは 443 です。<br>デフォルトを上書きするには、[デフォルトの使用（Use Default）] の選択を解除し、適切なポート番号を入力します。 |
| IPS RDEP Mode | イベント モニタリングのために RDEP または SDEE 接続を確立するときに、IPS デバイスへのアクセスに使用する接続方法。 |

| 要素 | 説明 |
|---|---|
| Certificate Common Name | 証明書に割り当てられる名前。共通名は、証明書に割り当てられた個人、システム、またはその他のエンティティの名前にすることができます。[Confirm] フィールドに、共通名を再入力します。 |

# 設定ファイルからのデバイスの追加

Security Manager にデバイス設定を処理させることにより、デバイスにログインせずにデバイスをインベントリに追加できます。デバイスごとに、デバイス設定をファイルにコピーし、そのファイルを Security Manager サーバに配置する必要があります。

この手順を使用して、IPS デバイスまたは Catalyst 6500/7600 デバイスをインベントリに追加することはできません。

### はじめる前に

この手順を開始する前に、次の準備が完了していることを確認してください。

- Security Manager で管理されるデバイスを準備します。詳細については、デバイスを管理するための準備を参照してください。
- 認証に ACS を使用する場合は、ACS でデバイスを定義します。『Installation Guide for Cisco Security Manager』を参照してください。
- Security Manager サーバ上のディレクトリにデバイス設定ファイルをコピーします。マウントしたドライブを使用することはできません。各設定に適切なデバイス タイプを容易に選択できるような命名ルールを使用してください。

（注） バージョン 4.21 以降、Cisco Security Manager は Cisco Identity Services Engine（ISE）を介した TACACS+ 認証のみをサポートします。これは、ACS のサポートが終了しているためです。

### 関連項目

- デバイス ビューについて （1 ページ）
- デバイス グループの使用 （79 ページ）
- デバイス プロパティの表示または変更 （51 ページ）

**ステップ 1** デバイスビューで [ファイル（File）] > [新規デバイス（New Device）] を選択するか、デバイスセレクタの [追加（Add）] ボタンをクリックします。[Choose Method] ページに New Device ウィザードが開きます。

**ステップ 2** [方式を選択（Choose Method）] ページで、[設定ファイルから追加（Add from Configuration File）] を選択し、[次へ（Next）] をクリックして [デバイス情報（Device Information）] ページを開きます（ [Device Information] ページ - [Configuration File] （27 ページ）を参照）。

**ステップ 3** デバイス タイプ セレクタから設定ファイルのデバイス タイプを選択し、適切なシステム オブジェクト ID を選択します。複数のデバイス タイプに対してそれぞれ設定ファイルがある場合は、デバイス タイプに基づいてそれらの設定ファイルを一括して追加します。

（注） バージョン 4.26 以降、Firepower デバイスモデル FPR4K-SM-12、FPR4K-SM-24、FPR4K-SM-36、FPR4K-SM-44、FPR9K-SM-24、FPR9K-SM-24-NEB、FPR9K- SM-36 および FPR9K-SM-44 は CSM ではサポートされていません。

**ステップ 4** [参照（Browse）] をクリックし、追加する（指定したタイプの）デバイスが含まれている設定ファイルを選択します。

**ステップ 5** どのタイプのポリシーを検出するかを示す適切な検出オプションを選択します。

**ステップ 6** （任意）[次へ（Next）] をクリックし、新規デバイスを所属させるデバイスグループを選択します。

**ステップ 7** [終了（Finish）] をクリックします。Security Manager が [Discovery Status] ダイアログボックスを開きます。ここでは、設定ファイル分析のステータスを参照できます（[Discovery Status] ダイアログボックスを参照）。完了したらウィンドウを閉じます。デバイスがインベントリ リストに追加されます。

ヒント ポリシーの検出中に予期しないエラーが返された場合は、設定ファイルに主要な Cisco IOS ソフトウェア バージョンだけが含まれ、ポイント リリース情報が含まれていないことが原因である可能性があります。デバイスに定義されているポリシーによっては、ポイント リリースで使用できるようになった機能を使用しているものがあります。つまり、Security Manager がその機能をサポート対象であると認識していない可能性があります。この問題を解決するには、デバイスを追加したあと、デバイス セレクタでそのデバイスを選択し、右クリックして [デバイスのプロパティ（Device Properties）] を選択します。[全般（General）] ページで、デバイスで実行されているバージョンに最も近く、かつそのバージョンより新しいものではないソフトウェア バージョンで [ターゲット OS バージョン（Target OS Version）] フィールドを更新します（バージョン番号を取得するには、デバイスの CLI で **show version** コマンドを使用します）。その後、右クリックし、[デバイスでポリシーを検出（Discover Policies on Device）] を選択して、ポリシーを再検出できます。

**ステップ 8** デバイス セレクタでデバイスを選択して Auto Update Server または Configuration Engine によって管理されているデバイスを追加した場合は、[ツール（Tools）] > [デバイスのプロパティ（Device Properties）] を選択します。[Auto Update] または [Configuration Engine] 設定で、デバイスで使用するサーバを選択します。サーバがリストにない場合は追加できます。詳細については、Auto Update Server または Configuration Engine の追加、編集、または削除 （45 ページ）を参照してください。

## [Device Information] ページ - [Configuration File]

構成ファイルからデバイスを追加する場合は、New Device ウィザードの [デバイス情報（Device Information）] ページを使用して、構成ファイルを選択し、ポリシー検出オプションを指定します。

### ナビゲーション パス

New Device ウィザードを起動するには、デバイス ビューで [ファイル（File）] > [新規デバイス（New Device）] を選択するか、デバイス セレクタの [追加（Add）] ボタンをクリックします。

## 関連項目

- デバイス ビューについて （1 ページ）
- 設定ファイルからのデバイスの追加 （26 ページ）
- [Device Groups] ページ （63 ページ）
- ポリシーの検出
- [Discovery Status] ダイアログボックス

## フィールド リファレンス

表 *4:* 設定ファイルからデバイスを追加する場合に使用する *New Device* ウィザードの *[Device Information]* ページ

| 要素 | 説明 |
|---|---|
| Device Type selector | デバイスをデバイス タイプ別およびデバイス ファミリ別に整理します。新しいデバイスのデバイス タイプを選択します。追加する設定ファイルに適切なデバイス タイプを選択する必要があります。 |
| System Object ID | デバイス タイプ セレクタから選択したデバイス タイプのシステム オブジェクト ID。デバイスの正しい ID を選択します。 |
| コンフィギュレーション ファイル | インベントリに追加するデバイスの設定ファイル。複数の設定ファイルを指定できますが、そのいずれもデバイス タイプが同じものである必要があります。ファイル名はカンマで区切ります。<br><br>複数のセキュリティ コンテキストを持つ ASA、PIX、および FWSM デバイスでは、各セキュリティ コンテキストおよびシステム実行スペース（システム コンテキスト）に対して別々の設定ファイルが存在することを覚えておいてください。システム実行スペースの設定ファイルを選択して、基本デバイスを追加します。<br><br>[参照（Browse）] をクリックして、Security Manager サーバーからファイルを選択するか、または手動で（フルパスの）ファイル名を入力します。ファイルの選択の詳細については、Cisco Security Manager でのファイルまたはディレクトリの選択または指定を参照してください。 |
| オプション | デバイスで使用可能な追加オプション。デバイスで IPS 機能を使用できる場合は、[IPS] を選択します。 |

| 要素 | 説明 |
|---|---|
| フェールオーバーのライセンスサポート<br>（ASA 5505、5510 専用） | オプションのフェールオーバー ライセンスがデバイスにインストールされているかどうかを示します。オプションは、ASA 5505 および 5510 デバイスのみでアクティブになります。Security Manager は、このオプションが選択されている場合のみ、フェールオーバー ポリシーをデバイスに展開します。<br>**ヒント** デバイスからポリシーを検出した場合、Security Manager はライセンス ステータスを判定し、このオプションを適切に設定します。 |
| デバイス設定の検出 | |
| 検出 | 検出してインベントリに追加する要素のタイプ。次のオプションがあります。<br>• [Policies and Inventory]：ポリシー、インターフェイス、およびサービス モジュール（該当する場合）を検出します。これがデフォルトであり、推奨オプションです。<br>ポリシーの検出が開始されると、設定ファイルが分析され、設定されているサービスとプラットフォームのポリシーがインポートされます。インベントリの検出が開始されると、設定ファイルに定義されているインターフェイスが分析され、インターフェイス リストがインポートされます。<br>このオプションを選択すると、下のチェックボックスがアクティブになり、それらのチェックボックスを使用して、検出されるポリシーのタイプを制御できます。<br>（注） 検出中に非アクティブな ACL をインポートすると、その ACL は Security Manager に無効な状態で表示されます。同じ ACL を展開すると、その ACL は Security Manager によって削除されます。<br>• [Inventory Only]：インターフェイスとサービス モジュール（該当する場合）を検出します。<br>• [No Discovery]：すべての検出がスキップされます。デバイスのポリシー、インターフェイス、またはサービス モジュール情報はデバイス インベントリに追加されません。 |
| プラットフォーム設定 | プラットフォーム固有のポリシー ドメインとも呼ばれるプラットフォーム設定を検出するかどうかを指定します。プラットフォーム固有のポリシー ドメインは、ファイアウォール デバイス上にあります。これらのドメインには、選択したプラットフォームに固有の機能を設定するポリシーが含まれています。詳細については、サービスポリシーとプラットフォーム固有のポリシーを参照してください。 |

| 要素 | 説明 |
|---|---|
| ファイアウォール ポリシー | ファイアウォール サービスとも呼ばれるファイアウォール ポリシーを検出するかどうかを指定します。ファイアウォールサービスには、アクセルルール、インスペクション ルール、AAA ルール、Web フィルタ ルール、トランスペアレント ルールなどのポリシーが含まれます。詳細については、ファイアウォール サービスの概要を参照してください。 |
| IPS ポリシー | シグニチャや仮想センサーなどの IPS ポリシーを検出するかどうかを指定します。詳細については、IPS 設定の概要またはCisco IOS IPS 設定の概要を参照してください。 |
| RA VPN ポリシー | IKE プロポーザルや IPsec プロポーザルなどの IPSec および SSL リモートアクセス VPN ポリシーを検出するかどうかを指定します。デバイスがリモート アクセス VPN 設定をサポートしていない場合、このオプションはディセーブルになります。詳細については、リモート アクセス VPN の管理の基礎を参照してください。 |

# 手動定義によるデバイスの追加

ネットワークでデバイスがまだアクティブではない場合は、そのデバイスを Security Manager に追加し、デバイスの設定を事前プロビジョニングできます。一般に、ネットワークに存在するデバイスは手動定義しないでください。他のいずれかの手法でデバイスを追加するほうが、はるかに簡単だからです。

### はじめる前に

この手順を開始する前に、次の準備が完了していることを確認してください。

- Security Manager で管理されるデバイスを準備します。詳細については、デバイスを管理するための準備を参照してください。
- 認証に ACS を使用する場合は、ACS でデバイスを定義します。『Installation Guide for Cisco Security Manager』を参照してください。

### 関連項目

- デバイス ビューについて （1 ページ）
- デバイス グループの使用 （79 ページ）
- デバイス プロパティの表示または変更 （51 ページ）

**ステップ 1** デバイスビューで [ファイル（File）] > [新規デバイス（New Device）] を選択するか、デバイスセレクタの [追加（Add）] ボタンをクリックします。[Choose Method] ページに New Device ウィザードが開きます。

**ステップ 2** [方式を選択（Choose Method）] ページで、[新規デバイスの追加（Add New Device）] を選択し、[次へ（Next）] をクリックして [デバイス情報（Device Information）] ページを開きます。

**ステップ 3** [Device Information] ページで、少なくとも次のフィールドに値を入力します。すべてのフィールドの詳細については、[Device Information] ページ - [New Device] （32 ページ）を参照してください。

- ページの左側にあるデバイス タイプ セレクタからデバイス タイプを選択し、デバイス タイプ セレクタの一番下にあるシステム オブジェクト ID を選択します。
- [IP Type] フィールドでは、デバイスがスタティック アドレス（IP アドレスはデバイスに定義されます）を使用するのか、ダイナミック アドレス（IP アドレスは DHCP サーバから提供されます）を使用するのかを選択します。
- スタティック アドレスを使用するデバイスの場合、DNS ホスト名とドメイン名、または IP アドレスのいずれか（あるいはその両方）を入力します。
- 表示名を入力します。この名前は Security Manager のデバイス セレクタに表示されます。
- 正しいオペレーティング システムおよびバージョンが選択されていることを確認します。
- サーバを使用してデバイスの設定を管理する場合は、デバイスに対するダイナミックなアドレス指定が必要であり、そのためデバイスを管理する Auto Update Server または Configuration Engine を選択し、サーバがデバイスに使用するデバイス アイデンティティ文字列を入力します。サーバーが表示されていない場合は、[サーバーの追加（Add Server）] を選択し、そのサーバーをインベントリに追加します。サーバーの追加の詳細については、Auto Update Server または Configuration Engine の追加、編集、または削除 （45 ページ）を参照してください。

デバイス情報を入力したら、[次へ（Next）] をクリックして [デバイスのログイン情報（Device Credentials）] ページに進みます。

**ステップ 4** （任意）[Device Credentials] ページで、デバイスへのログインに必要なユーザ名およびパスワードを入力します。一般に、プライマリ デバイス クレデンシャルを入力する必要があります。これは、従来のユーザ EXEC モードと特権 EXEC モードのパスワードです。クレデンシャルを入力しない場合は、あとで [Device Properties] ページでクレデンシャルを追加できます。

クレデンシャルの各種タイプについては、[Device Credentials] ページ （58 ページ）を参照してください。

[次へ（Next）] をクリックします。

**ステップ 5** （任意）[Device Grouping] ページで、デバイスを所属させるグループを選択します。[Device Groups] ページ （63 ページ）を参照してください。

**ステップ 6** [終了（Finish）] をクリックします。デバイスがインベントリに追加されます。

**ヒント** PIX、ASA、FWSM のいずれかのデバイスを追加している場合は、デバイスの出荷時のデフォルト設定とそのセキュリティ コンテキストを検出する必要があります。詳細については、Security Manager にすでに存在するデバイス上のポリシーの検出を参照してください。

# [Device Information] ページ - [New Device]

（ネットワークにまだ存在しない）新規デバイスを追加する場合は、新規デバイス（New Device）ウィザードの [デバイス情報（Device Information）] ページを使用して、デバイスの識別情報を指定します。

## ナビゲーション パス

New Device ウィザードを起動するには、デバイスビューで [ファイル（File）] > [新規デバイス（New Device）] を選択するか、デバイスセレクタの [追加（Add）] ボタンをクリックします。

## 関連項目

- デバイス ビューについて （1 ページ）
- 手動定義によるデバイスの追加 （30 ページ）
- [Device Credentials] ページ （58 ページ）
- [Device Groups] ページ （63 ページ）

## フィールド リファレンス

**表 *5:* 新規デバイスを追加する場合に使用する *New Device* ウィザードの *[Device Information]* ページ**

| 要素 | 説明 |
|---|---|
| デバイスタイプ（Device Type） | |
| Device Type selector | デバイスをデバイス タイプ別およびデバイス ファミリ別に整理します。新しいデバイスのデバイス タイプを選択します。<br>（注） バージョン 4.26 以降、Firepower デバイスモデル FPR4K-SM-12、FPR4K-SM-24、FPR4K-SM-36、FPR4K-SM-44、FPR9K-SM-24、FPR9K-SM-36、および FPR9K-SM- 44 は CSM ではサポートされていません。<br>Cisco Secure Firewall 3105 デバイスのサポートは、CSM の ASA 9.19(1) 以降のデバイスに導入されました。 |
| System Object ID | デバイス タイプ セレクタから選択したデバイス タイプのシステム オブジェクト ID。デバイスの正しい ID を選択します。 |
| ID | |

| 要素 | 説明 |
|---|---|
| IP タイプ（IP Type） | デバイスのIPアドレスをスタティックにする（デバイスで定義する）か、またはダイナミックにする（DHCPサーバから取得する）かを指定します。選択した IP タイプによって、表示されるフィールドが異なります。<br>（注） バージョン 4.12 以降、ASA デバイスに対する Cisco Security Manager サーバーからデバイスへの通信は、IPv6 アドレスまたはIPv4アドレスのいずれかでサポートされます。IPv6アドレスは128ビットの一意のアドレスです。IPv6アドレスについては、スタティック IP タイプのみがサポートされています。ダイナミック IP タイプは、IPv6 アドレスではサポートされません。 |
| ホストネーム<br>（スタティック IP 専用） | デバイスのDNSホスト名。IPアドレスが不明な場合に、DNSホスト名を入力します。<br>最大長は 70 文字です。有効な文字は、0 ～ 9、大文字の A ～ Z、小文字の a ～ z、およびハイフン（-）です。<br>（注） DNSホスト名とIPアドレスのどちらか一方、または両方を入力する必要があります。<br>2 つのデバイスに同じ DNS ホスト名とドメイン名の組み合わせを使用することはできません。 |
| ドメイン名<br>（スタティック IP 専用） | デバイスの DNS ドメイン名。<br>最大長は 70 文字です。有効な文字は、0 ～ 9、大文字の A ～ Z、小文字の a ～ z、ピリオド（.）、およびハイフン（-）です。 |
| IPアドレス<br>（スタティック IP 専用） | デバイスの管理IPアドレス。IPアドレスは、10.64.3.8というように、ドット付きの 4 つの数字列でなければなりません。<br>（注） IPアドレスとDNSホスト名のどちらか一方、または両方を入力する必要があります。<br>（注） バージョン 4.12 以降、ASA デバイスに対する Cisco Security Manager サーバーからデバイスへの通信は、IPv6 アドレスまたはIPv4アドレスのいずれかでサポートされます。デバイスがデュアルスタックで設定されている場合、Security Manager は、Security Manager に追加されたデバイスの IP アドレスに基づいてデバイスと通信します。IPv6 アドレスは 128 ビットの一意のアドレスです。 |

| 要素 | 説明 |
|---|---|
| 表示名 | Security Manager のデバイス セレクタに表示する名前。ホスト名または IP アドレスを入力した場合は、そのホスト名または IP アドレスがこのフィールドに自動的に入力されますが、変更することもできます。<br>最大長は 70 文字です。有効な文字は、0 ～ 9、大文字の A ～ Z、小文字の a ～ z、_ - . :、およびスペースです。<br>（注） 2 つのデバイスに同じ表示名を設定することはできません。 |
| オペレーティング システム | |
| OS タイプ | オペレーティング システムのタイプ。デバイス タイプに基づいて、OS タイプが自動的に選択されます。<br>（注） バージョン 4.12 以降、ASA デバイスに対する Cisco Security Manager サーバーからデバイスへの通信は、IPv6 アドレスまたは IPv4 アドレスのいずれかでサポートされます。この機能は、オペレーティングシステムのタイプが ASA または FWSM であるデバイスでのみ使用できます。 |
| イメージ名（Image Name） | デバイスで実行されるイメージの名前。 |
| ターゲット OS バージョン | 設定を適用するターゲット OS バージョン。この選択によって、Security Manager が設定ファイルを生成するときに使用されるコマンドのタイプが決まります。 |
| オプション | デバイスで使用可能な追加オプション。デバイスで IPS 機能を使用できる場合は、[IPS] を選択します。 |
| コンテキスト | デバイスで 1 つのセキュリティ コンテキストをホストするか（[Single]）、または複数のセキュリティ コンテキストをホストするか（[Multi]）を指定します。このフィールドが表示されるのは、OS タイプが FWSM、ASA、または PIX ファイアウォール 7.0 の場合だけです。 |

| 要素 | 説明 |
|---|---|
| 動作モード（Operational Mode） | デバイスの動作モード。このフィールドが表示されるのは、OS タイプが FWSM、ASA、または PIX ファイアウォール 7.0 以降の場合だけです。使用可能なオプションは[トランスペアレント（Transparent）] または[ルータ（Router）] です。[コンテキスト（Contexts）] で[マルチ（Multi）] を選択する場合、このモードのデフォルト設定は [混合（Mixed）] になります。[混合（Mixed）] は、ASA 9.0 以降および FWSM 3.1 以降のデバイスと ASA-SM にのみ適用されます。<br>（注） Cisco Security Manager 4.21 以降では、ASA ソフトウェアの拡張機能とバグ修正は引き続きサポートされていますが、Cisco IOS ソフトウェアのサポートが終了しているため、ルータのハードウェア サポートは提供されません。 |
| FXOS モード | デバイスが動作している FXOS モード。使用可能なオプションは [プラットフォーム（Platform）] および [アプライアンス（Appliance）] です。[アプライアンス（Appliance）]モードを選択する場合は、CLI、オンボックスデバイス（ASDM など）、またはマルチデバイスマネージャ（Cisco Security Manager など）のいずれかから、すべてのエンドユーザー設定を実行できます。[プラットフォーム（Platform）] モードオプションは、Firepower 2000 シリーズ アプライアンスに対してのみ表示されます。<br>（注） バージョン 4.20 以降、Security Manager は、Firepower 2000 および 1000 シリーズ アプライアンスに対して [アプライアンス（Appliance）] モードをサポートしています。 |

**[Auto Update] または [Configuration Engine]**

このグループは、選択するデバイス タイプに応じて名前が異なります。

- [Auto Update]：PIX ファイアウォールおよび ASA デバイスの場合。
- [Configuration Engine]：Cisco IOS ルータの場合。

これらのフィールドは、デバイスを管理するサーバ（ある場合）を識別するために使用します。ダイナミック IP アドレスを持つデバイスには、サーバが必須です。Catalyst 6500/7600 デバイスまたは FWSM デバイスのサーバは定義できません。

（注） バージョン 4.21 以降、Cisco Security Manager では、すべてのアグリゲーション サービス ルータ、統合サービスルータ、埋め込み型サービスルータ、および Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体が終了します。

| 要素 | 説明 |
|---|---|
| サーバー（Server） | デバイスを管理する Auto Update Server または Configuration Engine。<br><br>サーバーをリストに追加するには、[サーバーの追加（Add Server）] を選択します。[サーバーのプロパティ（Server Properties）] ダイアログボックスが開きます（[Server Properties] ダイアログボックス （47 ページ）を参照）。[サーバーの編集（Edit Server）] を選択して [使用可能なサーバー（Available Servers）] ダイアログボックスを開き、サーバーのプロパティを編集することもできます（[Available Servers] ダイアログボックス （49 ページ）を参照）。<br><br>このサーバ リストの管理の詳細については、Auto Update Server または Configuration Engine の追加、編集、または削除 （45 ページ）を参照してください。 |
| デバイスアイデンティティ | Auto Update Server または Configuration Engine でデバイスを一意に識別する文字列。 |
| その他のフィールド | |
| Cisco Security Manager での管理 | Security Manager でデバイスを管理するかどうかを指定します。このチェックボックスは、デフォルトでオンになっています。<br><br>追加しようとしているデバイスの唯一の機能が VPN エンドポイントとして機能することである場合は、このチェックボックスをオフにします。Security Manager は設定を管理せず、このデバイスの設定をアップロードまたはダウンロードしません。詳細については、管理対象外デバイスまたは非シスコ デバイスの VPN への組み込みを参照してください。 |

| 要素 | 説明 |
|---|---|
| 管理対象外のデバイスのセキュリティ コンテキスト | 親（PIX ファイアウォール デバイス、ASA デバイス、または FWSM デバイス）が Security Manager によって管理されていないセキュリティ コンテキストを管理するかどうかを指定します。<br>このフィールドがアクティブになるのは、デバイス セレクタで選択したデバイスが PIX ファイアウォール、ASA、FWSM などのファイアウォールデバイスで、かつそのファイアウォールデバイスがセキュリティ コンテキストをサポートしている場合だけです。<br>1 つの PIX ファイアウォール、ASA、または FWSM のパーティションを、セキュリティ コンテキストとも呼ばれる複数のセキュリティ ファイアウォールに分けることができます。各コンテキストは、それぞれに独自の設定およびポリシーを持つ独立したシステムです。このようなスタンドアロンのコンテキストは、親デバイスが管理対象外であっても、Security Manager で管理できます。詳細については、ファイアウォール デバイスでのセキュリティ コンテキストの設定を参照してください。<br>（注） このチェックボックスをオンにした場合、セキュリティ モジュールに使用可能なターゲット OS バージョンが [Target OS Version] フィールドに表示されます。 |
| フェールオーバーのライセンスサポート<br>（ASA 5505、5510 専用） | オプションのフェールオーバー ライセンスがデバイスにインストールされているかどうかを示します。オプションは、ASA 5505 および 5510 デバイスのみでアクティブになります。Security Manager は、このオプションが選択されている場合のみ、フェールオーバー ポリシーをデバイスに展開します。<br>ヒント デバイスからポリシーを検出した場合、Security Manager はライセンス ステータスを判定し、このオプションを適切に設定します。 |

# インベントリ ファイルからのデバイスの追加

Comma-Separated Value（CSV; カンマ区切り値）形式のインベントリ ファイルからデバイスを追加できます。たとえば、CiscoWorks Common Services Device Credential Repository（DCR）または別の Security Manager サーバからエクスポートしたインベントリ ファイルや、Cisco Security Monitoring, Analysis and Response System（CS-MARS）で使用したシード ファイルなどです。インベントリ ファイル形式の詳細については、インベントリのインポートまたはエクスポートでサポートされている CSV 形式を参照してください。

**ヒント**

- この手順では、デバイスのインポートに CSV ファイルを使用する方法について説明します。インベントリだけではなく、デバイスに割り当てられたポリシーおよびポリシー オブジェクトも含む .dev ファイルがある場合は、この手順を使用できません。代わりに、**[ファ**

**イル（File）]>[インポート（Import）]**コマンドを使用して、ポリシーまたはデバイスのインポートの指示に従います。

- インベントリ ファイルを手作業で構築する場合、最も簡単な方法は Security Manager インベントリを目的の形式でエクスポートし、そのファイルを目的のインベントリ ファイルの基礎として使用することです。
- インポートするデバイスは、デバイスインベントリにすでに存在するデバイスと重複していてはいけません。たとえば、デバイスを再インポートして、インベントリのデバイス情報を更新することはできません。

### はじめる前に

この手順を開始する前に、次の準備が完了していることを確認してください。

- Security Manager で管理されるデバイスを準備します。詳細については、デバイスを管理するための準備を参照してください。
- 認証に ACS を使用する場合は、ACS でデバイスを定義します。『Installation Guide for Cisco Security Manager』を参照してください。
- 使用するインベントリ ファイルを Security Manager サーバに配置します。クライアント システム上のファイルからデバイスをインポートすることはできません。
- デバイスのタイプに非標準の通信プロトコルを使用している場合は、グローバルデバイス通信プロパティを更新して正しいプロトコルを指定します。詳細については、[Device Communication] ページを参照してください。

### 関連項目

- デバイス ビューについて （1 ページ）
- デバイス グループの使用 （79 ページ）
- デバイス プロパティの表示または変更 （51 ページ）

---

**ステップ 1** デバイスビューで [ファイル（File）]>[新規デバイス（New Device）] を選択するか、デバイスセレクタの [追加（Add）] ボタンをクリックします。[Choose Method] ページに New Device ウィザードが開きます。

**ステップ 2** [方式を選択（Choose Method）] ページで、[ファイルから追加（Add from File）] を選択し、[次へ（Next）] をクリックして [デバイス情報（Device Information）] ページを開きます（[Device Information] ページ - [Add Device from File] （40 ページ）を参照）。

**ステップ 3** [参照（Browse）] をクリックし、インポートするデバイスが含まれているインベントリファイルを選択します。ファイルの形式を示す正しいファイル タイプを選択していることを確認します。

Security Manager は、インベントリ ファイルの内容を評価し、インポート テーブルにデバイス リストを表示します。ステータスが [Ready to Import] であるすべてのデバイスが自動的に選択されます。このリストから、選択されていないデバイスがなぜインポートできないかがわかります。インポートしないデバイスは、選択を解除できます。

デバイスに関する詳細な情報を参照するには、インポート テーブルでそのデバイスを選択します。詳細が一番下のペインに表示されます。デバイスごとに異なる検出オプションまたは転送設定を選択できます。

ヒント　Security Manager形式のインベントリ ファイルを選択した場合は、ポリシー検出を実行せずにデバイスをインポートすることもできます。これにより、ネットワークで現在アクティブでないデバイスを追加できるようになります。デバイスでポリシー検出を実行する場合は、デバイスを選択し、一番下のパネルで [デバイスディスカバリの実行（Perform Device Discovery）] を選択し、目的の検出オプションを選択します。個々のデバイスではなくフォルダを選択して、そのフォルダ内のすべてのデバイスのポリシー検出設定を選択できます。他のCSV形式では、インポート時にポリシー検出を実行する必要があります。

リストを分析し、検出設定および転送設定に必要な変更を加えたら、[次へ（Next）] をクリックしてグループを選択する任意の手順を続けるか、または [終了（Finish）] をクリックしてウィザードを完了します。いずれにしても、Security Manager 形式で CSV ファイルを使用し、かつ検出を実行しないようにしている場合を除き、Security Managerは各デバイスにログインし、選択された検出を実行しようとします。他の形式の場合、Security Managerはデバイスにログインしてインベントリにそのデバイスを追加できる必要があります。ステータスが [Discovery Status] ダイアログボックスに表示されます（[Discovery Status] ダイアログボックスを参照）。

ヒント　デバイスの追加中にポリシーを検出している場合は、提示されているメッセージをよくお読みください。これらのメッセージには、次に実行する手順に関する重要な推奨事項が含まれている場合があります。Security Managerが設定の所有権を引き継ぐことができるように、検出した設定をファイルにすぐに展開することを推奨します。展開方法の詳細については、展開方法についてを参照してください。

**ステップ 4**　（任意）[Device Grouping] ページで、インポートしたデバイスの追加先となるデバイス グループを選択します（ [Device Groups] ページ （63 ページ）を参照）。

[終了（Finish）] をクリックします。

**ステップ 5**　モジュールが含まれているデバイスを追加し、デバイス検出を実行し、さらにSecurity Managerがそのタイプのデバイスでモジュールの検出をサポートしている場合、デバイスシャーシの検出が完了したときに通知され、デバイスのモジュールを検出するかどうかを確認されます。[はい（Yes）] をクリックすると、次の情報の入力を要求されます。

- Catalyst 6500 サービス モジュール：[Service Module Credentials] ダイアログボックスが開き、シャーシに含まれているモジュールに基づいて次の情報の入力が要求されます。詳細については、 [Service Module Credentials] ダイアログボックス （22 ページ）を参照してください。
  - FWSM：管理IPアドレス（推奨）、ユーザ名とパスワード、および実行する検出のタイプ。FWSMがフェールオーバーペアの 2 番めのデバイスである場合は、フェールオーバーモジュールの [モジュールを検出しない（Do Not Discover Module）] を選択します。（Security Manager は、プライマリまたはセカンダリのどちらのフェールオーバーサービスモジュールが追加されたにかかわらず、常にアクティブな管理コンテキストを管理します）。
  - IDSM：ユーザ名とパスワード、および実行する検出のタイプ。
  - ASA-SM：Catalyst 6500 で、シャーシ経由での ASA サービス モジュールの検出はサポートされません。ASA-SM は、ASA-SM の管理 IP アドレスを使用して直接追加する必要があります。

- IPS ルータ モジュール：実行する検出のタイプ、管理 IP アドレス、ユーザ名とパスワード、およびその他の SSL 接続情報。詳細については、[IPS Module Discovery] ダイアログボックス （24 ページ）を参照してください。

Security Manager で管理しないモジュールの検出をスキップできます。

[OK] をクリック[Discovery Status] ダイアログボックスに戻り、サービス モジュールの検出の経過を表示できます。

## [Device Information] ページ - [Add Device from File]

インベントリファイルからデバイスを追加するには、New Device ウィザードの [デバイス情報（Device Information）] ページを使用して、インベントリファイルを選択し、ポリシー検出オプションを指定します。インベントリ ファイルは、Security Manager サーバに存在する必要があります。クライアント システム上にあるインベントリ ファイルは使用できません。

インベントリ ファイルに使用できる形式については、インベントリのインポートまたはエクスポートでサポートされている CSV 形式で説明します。一般に、インベントリ ファイルは、別の Security Manager サーバまたは CiscoWorks Common Services サーバからエクスポートされたものであるか、または Cisco Security Monitoring, Analysis and Response System（CS-MARS）サーバのインベントリを読み込むときに使用されるシード ファイルとなります。

.dev ファイルを使用してデバイスをインポートしようとしている場合は、このページの代わりに [File] > [Import] コマンドを使用する必要があります。詳細については、ポリシーまたはデバイスのインポートを参照してください。

**ヒント** モジュールが含まれているデバイス、たとえばFWSMがあるCatalystスイッチを追加している場合は、[完了（Finish）] をクリックするとモジュール検出情報の入力を求められます。

### ナビゲーション パス

New Device ウィザードを起動するには、デバイスビューで [ファイル（File）] > [新規デバイス（New Device）] を選択するか、デバイスセレクタの [追加（Add）] ボタンをクリックします。

### 関連項目

- デバイス ビューについて （1 ページ）
- インベントリ ファイルからのデバイスの追加 （37 ページ）
- [Device Groups] ページ （63 ページ）
- ポリシーの検出
- [Device Communication] ページ
- [Discovery Status] ダイアログボックス

## フィールド リファレンス

**表 *6:* インベントリ ファイルからデバイスを追加する場合に使用する *New Device* ウィザードの *[Device Information]* ページ**

| 要素 | 説明 |
|---|---|
| デバイスのインポート元 | インポートするデバイスが含まれているインベントリ ファイル。[参照（Browse）] をクリックして、Security Manager サーバー上のファイルを選択します。<br>ファイルを選択するときは、Security Manager が Comma-Separated Value（CSV; カンマ区切り値）ファイルを正しく評価できるように、正しいファイル タイプも選択する必要があります。 |
| **デバイスインポートテーブル**<br>ファイルを選択すると、Security Manager はその内容を評価し、ファイルに定義されているデバイス リストをページ上部のペインのテーブルに表示します。Security Manager は、ステータスが [Ready to Import] であるすべてのデバイスを自動的に選択します。一般には、デバイス インベントリにまだ存在しないデバイスとなります。<br>テーブルには、次のカラムがあります。 | |
| インポート | デバイスをインベントリに追加するには、このチェックボックスをオンにします。フォルダを選択または選択解除して、そのフォルダ内のすべてのデバイスを選択または選択解除できます。 |
| 表示名 | Security Manager のデバイス セレクタに表示する名前。 |
| ホスト名 | デバイスに定義されているホスト名。 |
| トランスポート（Transport） | デバイスへの接続に使用するトランスポート プロトコル。 |
| ステータス | Security Manager でデバイスをインポートできるかどうかを指定します。デバイスは、ステータスが [Ready to Import] である場合にだけインポートできます。デバイスのステータスの詳細については、デバイスを選択し、ページ右下隅の [ステータス（Status）] テキストボックスでステータス情報を展開してお読みください。 |
| デバイスタイプ | デバイスのタイプ。 |

| 要素 | 説明 |
|---|---|
| **[詳細（Details）] ペイン**<br>デバイス インポート テーブルの下に、テーブルで選択されているデバイスの詳細を表示するペインがあります。アイデンティティ情報には、テーブルのフィールドがそのまま表示されます。[Status] テキスト ボックスには、インポート ステータスの詳しい説明が表示されます。<br>[Discover Device Settings] グループおよび [Transport] グループでは、Security Manager でのデバイスのインポート方法を指定できます。デバイスではなくフォルダを選択した場合、選択した設定はフォルダ内のすべてのデバイスに適用されます。設定については、次に説明します。 | |
| デバイス設定の検出 | |
| デバイス ディスカバリの実行 | デバイスから直接ポリシーを検出するかどうかを指定します。<br>• インベントリ ファイルが Security Manager 形式である場合は、[Perform Device Discovery] を選択して、インベントリおよびポリシーを検出する必要があります（それ以外の場合、デバイスは評価されずに追加されます）。オフライン デバイスまたはスタンバイ デバイスを追加している場合は、このオプションをオフにしておいても、容易にデバイスをインベントリに追加できます。<br>• 他のすべてのインベントリ ファイル タイプでは、デバイス検出が必要です。 |
| システム コンテキスト | 選択したデバイスがマルチ コンテキスト モードで動作するデバイス上のシステム実行スペースであるかどうか（つまり、複数のセキュリティ コンテキストがデバイスに定義されているかどうか）を指定します。デバイスがシステム実行スペースである場合は、検出が正しく完了するようにこのオプションを選択する必要があります。 |

| 要素 | 説明 |
|---|---|
| 検出 | 検出してインベントリに追加する要素のタイプ。次のオプションがあります。<br>• [Policies and Inventory]：ポリシー、インターフェイス、およびサービス モジュール（該当する場合）を検出します。これがデフォルトであり、推奨オプションです。<br><br>ポリシーの検出が開始されると、デバイス上の設定が分析され、設定されているサービスとプラットフォームのポリシーがインポートされます。インベントリの検出が開始されると、デバイス上のインターフェイスが分析され、インターフェイス リストがインポートされます。デバイスが複合デバイスの場合は、デバイス内のすべてのサービス モジュールが検出され、インポートされます。<br><br>このオプションを選択すると、下のチェックボックスがアクティブになり、それらのチェックボックスを使用して、検出されるポリシーのタイプを制御できます。<br><br>（注） 検出中に非アクティブなACLをインポートすると、その ACL は Security Manager に無効な状態で表示されます。同じ ACL を展開すると、その ACL は Security Manager によって削除されます。<br><br>• [Inventory Only]：インターフェイスとサービス モジュール（該当する場合）を検出します。 |
| プラットフォーム設定 | プラットフォーム固有のポリシー ドメインとも呼ばれるプラットフォーム設定を検出するかどうかを指定します。プラットフォーム固有のポリシー ドメインは、ファイアウォール デバイスと Cisco IOS ルータ上にあります。これらのドメインには、選択したプラットフォームに固有の機能を設定するポリシーが含まれています。詳細については、サービスポリシーとプラットフォーム固有のポリシーを参照してください。 |
| ファイアウォール ポリシー | ファイアウォール サービスとも呼ばれるファイアウォール ポリシーを検出するかどうかを指定します。ファイアウォール サービスには、アクセル ルール、インスペクション ルール、AAA ルール、Web フィルタ ルール、トランスペアレント ルールなどのポリシーが含まれます。詳細については、ファイアウォール サービスの概要を参照してください。 |
| IPS ポリシー | シグニチャや仮想センサーなどのIPSポリシーを検出するかどうかを指定します。詳細については、IPS 設定の概要またはCisco IOS IPS 設定の概要を参照してください。 |

| 要素 | 説明 |
|---|---|
| RA VPN ポリシー | IKE プロポーザルや IPsec プロポーザルなどの IPSec および SSL リモート アクセス VPN ポリシーを検出するかどうかを指定します。デバイスがリモート アクセス VPN 設定をサポートしていない場合、このオプションはディセーブルになります。詳細については、リモート アクセス VPN の管理の基礎を参照してください。 |
| セキュリティコンテキストのポリシーの検出 | マルチ コンテキスト モードで動作するデバイスの場合、複数のセキュリティ コンテキストが定義されています。ここには、それらのセキュリティ コンテキストを検出するかどうかを指定します。 |
| **トランスポート**<br>転送設定によって、Security Manager がデバイスへの問い合わせに使用する方法が決まります。各デバイス タイプにはデフォルトの方法がありますが、任意の転送方法を選択できます。デバイスは、選択した方法に応答するように設定する必要があります。デバイス検出を実行していない場合は、デバイスへの問い合わせが行われません。 | |
| プロトコル | デバイスに接続するときに Security Manager で使用するプロトコル。 |
| サーバー（Server） | Auto Update Server（AUS）または Configuration Engine サーバを使用するデバイスの場合、デバイスが設定更新を取得する際に使用するそのサーバの名前を指定します。このようなサーバを使用するデバイスをインポートするには、サーバが Security Manager にすでに定義されているか、またはインポート リストからサーバを選択する必要があります。 |
| デバイスアイデンティティ | サーバを使用するデバイスの場合、Auto Update Server または Configuration Engine でデバイスを一意に識別する文字列を指定します。 |

# デバイス インベントリの使用

次の項では、デバイス インベントリの管理に関連するタスクについて説明します。


- Auto Update Server または Configuration Engine の追加、編集、または削除 （45 ページ）
- インターフェイス モジュールの追加または変更 （50 ページ）
- デバイス プロパティの表示または変更 （51 ページ）
- 重要なデバイス プロパティの変更 （70 ページ）
- デバイスに含まれている要素の表示 （75 ページ）

- デバイスの複製 （75 ページ）
- Security Manager インベントリからのデバイスの削除 （77 ページ）

これらの項に加え、関連する次の項を参照してください。

- デバイス インベントリへのデバイスの追加 （8 ページ）
- デバイス インベントリのエクスポート
- ポリシーまたはデバイスのインポート

# Auto Update Server または Configuration Engine の追加、編集、または削除

他のサーバを使用して設定を管理するデバイスを Security Manager で管理する場合（たとえば、DHCP サーバからダイナミック IP アドレスが提供されるデバイス。デバイスをリブートすると前回と同じアドレスが提供されるとはかぎりません）、Security Manager でその使用するサーバを識別する必要があります。次に、使用できるサーバを示します。

- Auto Update Server（AUS）。自動更新機能を使用する PIX ファイアウォールおよび ASA デバイス上のデバイス設定ファイルをアップグレードする場合に使用されます。
- Cisco Configuration Engine。Configuration Engine 機能を使用する Cisco IOS ルータ、ASA デバイス、および PIX ファイアウォール上のデバイス設定ファイルをアップグレードする場合に使用されます。

Security Manager は、DHCP を使用してインターフェイス アドレスを取得するデバイスとの直接通信を開始できません。そのデバイスの IP アドレスが事前にはわからないためです。また、管理システムが変更を加える必要があるときに、デバイスが動作中でなかったり、ファイアウォールおよび NAT 境界の背後に配置されていたりする場合があります。このようなデバイスは、Auto Update Server または Configuration Engine に接続して、デバイス情報を取得します。

デバイスを手動で追加したり、デバイス プロパティを表示したりするときに、AUS および Configuration Engine サーバをデバイス インベントリに追加できます。このようなサーバのいずれかを使用するデバイスのプロパティを追加または表示する必要はありません。適切なフィールドに移動して、このようなサーバを追加、編集、または削除するためのコントロールにアクセスします。

また、CiscoWorks Common Services Device Credential Repository（DCR）または別の Security Manager サーバからエクスポートされたインベントリ ファイルからこれらのサーバをインポートする場合は、該当するサーバを追加することもできます。サーバをインポートする場合は、ここで説明する手順をスキップします。デバイスのインポートの詳細については、インベントリ ファイルからのデバイスの追加 （37 ページ）を参照してください。

### はじめる前に

デバイスの追加に関係なく、Security Manager インベントリに AUS および Configuration Engine サーバーのリストを読み込む場合、最善の方法は New Device ウィザードを使用し、追加方法

として [新規デバイスの追加（Add New Device）] を選択することです。この方法については、次の手順で説明します。

また、デバイスセレクタでデバイスを選択し、[ツール（Tools）]>[デバイスプロパティ（Device Properties）] をクリックして、サーバーを追加または編集することもできます。デバイスプロパティのコンテンツテーブルで [全般（General）] をクリックします。[Server] フィールドは、[Auto Update] グループまたは [Configuration Engine] グループのいずれかにあります。グループ名で識別されるサーバのタイプだけを追加または編集できます。

ヒント　Security Manager では、Configuration Engine を追加するときに Configuration Engine で実行されているソフトウェア バージョンを特定できません。ただし、Security Manager は、設定を Configuration のすべてのバージョンに正しく展開できるとはかぎりません。Configuration Engine がサポートされているリリースを実行していることを確認してください（サポートされている Configuration Engine バージョンについては、http://www.cisco.com/en/US/products/ps6498/prod_release_notes_list.html にあるこの製品バージョンのリリースノートを参照してください）。

**関連項目**

- ネットワークからのデバイスの追加　（14 ページ）
- 手動定義によるデバイスの追加　（30 ページ）
- デバイス プロパティの表示または変更　（51 ページ）

**ステップ 1**　デバイス インベントリで AUS エントリまたは Configuration Engine エントリを識別および管理できるフィールドの場所を特定します。

a) [ファイル（File）]>[新規デバイス（New Device）] を選択して [新規デバイス（New Device）] ウィザードを開き、[方法の選択（Choose Method）] ページで [新規デバイスの追加（Add New Device）] を選択し、[次へ（Next）] をクリックします。

b) [Device Information] ページで、デバイス タイプ セレクタから ASA デバイスを選択します。たとえば、Cisco ASA-5580 Adaptive Security Appliance などです。[自動更新（Auto Update）] グループの [サーバー（Server）] フィールドには、ドロップダウンリストに [サーバーの追加（Add Server）] が含まれています。すでに定義されたサーバーがある場合は、[サーバーの編集（Edit Server）] も含まれています。このようなエントリに特定のサーバ タイプ（たとえば、Add Auto Update Server や Add Configuration Engine）がある場合、追加、編集、または削除の対象がそのタイプのサーバに制限されます（この場合、適切なサーバ タイプを探すには、他のタイプのデバイスを選択します）。

**ステップ 2**　新規 AUS または Configuration Engine サーバーを追加するには、[サーバー（Server）] ドロップダウンリストから [サーバーの追加（Add Server）] を選択して [サーバープロパティ（Server Properties）] ダイアログボックスを開きます（[Server Properties] ダイアログボックス　（47 ページ）を参照）。

**ステップ 3**　サーバーを編集するには、[サーバー（Server）] ドロップダウンリストから [サーバーの編集（Edit Server）] を選択して [利用可能なサーバー（Available Servers）] ダイアログボックスを開きます（[Available Servers] ダイアログボックス　（49 ページ）を参照）。その後、サーバーを選択し、[編集（Edit）] をクリックして [サーバープロパティ（Server Properties）] ダイアログボックスを開き、変更を加えることができます。

[Available Servers] ダイアログボックスでは、次の操作も実行できます。

- [作成（Create）] をクリックして、サーバーを追加します。
- サーバーを選択し、[削除（Delete）] をクリックして、インベントリからそのサーバーを削除します。削除の確認が求められます。サーバがインベントリのデバイスによって使用されていないことを確認します。

## [Server Properties] ダイアログボックス

[Server Properties] ダイアログボックスは、Auto Update Server または Configuration Engine のプロパティを指定する場合に使用します。

このダイアログボックスでは、その開く方法に応じてタイトルにサーバのタイプを指定できます（たとえば、Auto Update Server Properties や Configuration Engine Properties）。ダイアログボックスは基本的には同じです。

ヒント Security Manager では、Configuration Engine を追加するときに Configuration Engine で実行されているソフトウェア バージョンを特定できません。ただし、Security Manager は、設定を Configuration のすべてのバージョンに正しく展開できるとはかぎりません。Configuration Engine がサポートされているリリースを実行していることを確認してください（サポートされている Configuration Engine バージョンについては、http://www.cisco.com/en/US/products/ps6498/prod_release_notes_list.html にあるこの製品バージョンのリリースノートを参照してください）。

### ナビゲーション パス

このダイアログボックスを開くには、次のいずれかを実行します。

- デバイスを手動で追加するときには、新規デバイス（New Device）ウィザードの [デバイス情報（Device Information）] ページで、[Auto Update Server] グループまたは [Configuration Engine] グループの [サーバー（Server）] フィールドから [サーバーの追加...（Add Server...）] を選択します。選択肢は、[Add Auto Update Server] または [Add Configuration Engine] と表示される場合もあります。
- [デバイスのプロパティ（Device Properties）] - [全般（General）] ページで、[Auto Update Server] グループまたは [Configuration Engine] グループの [サーバー（Server）] フィールドから [サーバーの追加...（Add Server...）] を選択します。選択肢は、[Add Auto Update Server] または [Add Configuration Engine] と表示される場合もあります。
- [使用可能なサーバー（Available Servers）] ダイアログボックスで、[作成（Create）] をクリックするか、サーバーを選択し、[編集（Edit）] をクリックします（[Available Servers] ダイアログボックス （49 ページ）を参照）。

## 関連項目

- [Available Servers] ダイアログボックス （49 ページ）
- [Device Information] ページ - [New Device] （32 ページ）
- [Device Information] ページ - [Add Device from Network] （17 ページ）
- Auto Update Server または Configuration Engine の追加、編集、または削除 （45 ページ）
- デバイス プロパティの表示または変更 （51 ページ）

## フィールド リファレンス

表 *7 : [Server Properties]* ダイアログボックス

| 要素 | 説明 |
|---|---|
| タイプ | 定義しているサーバのタイプ。Auto Update Server または Configuration Engine。<br>このフィールドが表示されるのは、サーバを追加している場合だけです。既存のサーバのタイプは変更できません。<br>新規サーバの場合、ダイアログボックスのタイトルに追加対象のサーバのタイプが指定されているときにも、このフィールドは表示されません。 |
| サーバー名（Server Name） | サーバの DNS ホスト名。 |
| ドメイン名 | サーバの DNS ドメイン名。 |
| [IPアドレス（IP Address）] | サーバの IP アドレス。 |
| 表示名 | サーバの Security Manager に表示する名前。 |
| ユーザー名 | サーバにログインするためのユーザ名。 |
| パスワード | サーバにアクセスするためのパスワード。[Confirm] フィールドに、パスワードを再入力します。 |
| [ポート（Port）] | Auto Update Server または Configuration Engine によって管理されたデバイスがサーバと通信するときに使用するポート番号。通常、ポート番号は 443 です。 |

| 要素 | 説明 |
|---|---|
| URN | このフィールドは、Auto Update Server の場合にだけ表示されます。<br>Auto Update Server のユニフォーム リソース名。URN は、インターネット上のリソースを識別する名前です。URN は URL の一部で、/autoupdate/AutoUpdateServlet などとなります。完全な URL は、https://: *server ip* :443/autoupdate/AutoUpdateServle のようになります。<br>引数の説明<br>• *server ip* は、Auto Update Server の IP アドレスです。<br>• 443 は、Auto Update Server のポート番号です。<br>• /autoupdate/AutoUpdateServlet は、Auto Update Server の URN です。 |

## [Available Servers] ダイアログボックス

[Available Servers] ダイアログボックスは、Auto Update Server または Configuration Engine を追加、編集、または削除する場合に使用します。

このダイアログボックスでは、その開く方法に応じてタイトルにサーバのタイプを指定できます（たとえば、Available Auto Update Server や Available Configuration Engine）。ダイアログボックスは基本的には同じです。

各行が 1 台のサーバを表し、Security Manager でのサーバの表示名、IP アドレス、および DNS ホスト名とドメイン名が表示されます。ダイアログボックスのタイトルにサーバタイプが含まれていない場合、[Type] フィールドには [AUS] または [CE (Configuration Engine)] を指定します。

- サーバーを追加するには、[作成（Create）] ボタンをクリックし、[サーバープロパティ（Server Properties）] ダイアログボックスに値を入力します（[Server Properties] ダイアログボックス （47 ページ）を参照）。
- サーバーのプロパティを編集するには、サーバーを選択し、[編集（Edit）]ボタンをクリックします。
- サーバーを削除するには、サーバーを選択し、[削除（Delete）]ボタンをクリックします。削除の確認が求められます。

### ナビゲーション パス

このダイアログボックスを開くには、次のいずれかを実行します。

- デバイスを手動で追加するときには、[新規デバイス（New Device）] ウィザードの [デバイス情報（Device Information）] ページで、[自動更新サーバー（Auto Update Server）]または [設定エンジン（Configuration Engine）] グループの [サーバー（Server）] フィールドから [サーバーの編集...（Edit Server...）] を選択します。選択肢は、[Edit Auto Update Server] または [Edit Configuration Engine] と表示される場合もあります。

- [デバイスプロパティ（Device Properties）] - [全般（General）] ページで、[自動更新サーバー（Auto Update Server）] または [設定エンジン（Configuration Engine）] グループの [サーバー（Server）] フィールドから [サーバーの編集...（Edit Server...）] を選択します。選択肢は、[Edit Auto Update Server] または [Edit Configuration Engine] と表示される場合もあります。

### 関連項目

- [Device Information] ページ - [New Device] （32 ページ）
- [Device Information] ページ - [Add Device from Network] （17 ページ）
- Auto Update Server または Configuration Engine の追加、編集、または削除 （45 ページ）
- デバイス プロパティの表示または変更 （51 ページ）

# インターフェイス モジュールの追加または変更

多くのデバイスでは、インターフェイスモジュールを追加または変更できます。デバイスでホストされたインターフェイスモジュールに変更を加えるときは、そのデバイスのインベントリを変更します。

インターフェイス カードを追加または変更する場合は、デバイスでインベントリを再検出する必要があります。インベントリを再検出すると、[Interfaces] ポリシー（ルータの場合、[Interfaces] > [Interfaces policy]）が置換され、デバイスで使用可能なインターフェイスの機能が Security Manager に正しく表示されるようになります。

（注） インベントリの再検出は、4 GB イーサネット ファイバ インターフェイス カードを取り付けている ASA 5580 デバイスには特に重要です。他のタイプのデバイスの場合、通常、[Interfaces] ポリシーに手動で変更を加えることができますが、インベントリを再検出する方が簡単であり、信頼性にも優れています。

**ステップ 1** デバイスを右クリックし、[デバイスでポリシーを検出（Discover Policies on Device）] を選択します。

**ステップ 2** [検出タスクの作成（Create Discovery Task）] ダイアログボックスで、少なくとも次に挙げる項目を選択し、[OK] をクリックして再検出を開始します。

- [ライブデバイス（Live Device）] からの検出。
- 検出するポリシー：[インベントリ（Inventory）]。

**ステップ 3** 検出が完了したら、[Interfaces] または [Interfaces] > [Interfaces policy] を必要に応じて編集し、ポリシーに目的の設定が反映されていることを確認します。

# デバイス プロパティの表示または変更

デバイスをインベントリに追加するときは、名前やログイン情報など、デバイスのプロパティをいくつか指定します。インベントリに存在するデバイスの場合、デバイス プロパティを表示および変更できます。

**関連項目**

- デバイス ビューについて （1 ページ）
- デバイス プロパティについて （7 ページ）
- ポリシーについて
- 重要なデバイス プロパティの変更 （70 ページ）

**ステップ 1** デバイス ビューのデバイス セレクタで次のいずれかを実行し、[Device Properties] ダイアログボックスを開きます。

- デバイスをダブルクリックします。
- デバイスを右クリックして、[デバイスのプロパティ（Device Properties）] を選択します。
- デバイスを選択して、[ツール（Tools）] > [デバイスのプロパティ（Device Properties）] の順に選択します。

**ステップ 2** [Device Properties] ダイアログボックスで、左ペインにあるコンテンツ テーブルで対応するエントリをクリックして、プロパティを表示または変更します。別のページに移動する前に、[保存（Save）] をクリックする必要があります。

- [General]：デバイス アイデンティティ、デバイスで実行されているオペレーティング システム、転送設定など、デバイスに関する一般的な情報。これらのフィールドについては、[デバイスのプロパティ（Device Properties）] : [全般（General）] ページ （52 ページ）を参照してください。
- [Credentials]：デバイスへのログインに必要なデバイス クレデンシャル。これらのフィールドについては、 [Device Credentials] ページ （58 ページ）を参照してください。
- [Device Groups]：デバイスが属しているグループ。これらのフィールドについては、 [Device Groups] ページ （63 ページ）を参照してください。
- [Group Information]：グループのグループ詳細（ある場合）。これらのフィールドについては、[グループ情報（Group Information）] ページ （64 ページ）を参照してください。
- [License Information]：FPR-3100 シリーズデバイスのライセンスの詳細。フィールドの詳細については、[ライセンス情報（License Information）] ページを参照してください。

  （注） ライセンス情報パネルは、CSM 4.24 の FPR-3100 シリーズデバイスに対してのみ表示されます。

- [Policy Object Overrides]：デバイスのポリシー オブジェクトに対するローカルなオーバーライド。[Policy Object Overrides] は、デバイスに使用できるさまざまなポリシー オブジェクト タイプが含まれている

フォルダです。特定のポリシー オブジェクト タイプをクリックすると、デバイスで使用されているそのタイプのポリシー オブジェクトが表示され、オーバーライドもあれば表示されます。フィールドの詳細については、ポリシー オブジェクト オーバーライドのページ （69 ページ）を参照してください。

## [デバイスのプロパティ（Device Properties）]：[全般（General）] ページ

[Device Properties] の [General] ページは、デバイスの基本的なプロパティに関する情報を追加または編集する場合に使用します。

### ナビゲーション パス

- デバイスセレクタから、デバイスを右クリックし、[デバイスのプロパティ（Device Properties）] を選択し、[全般（General）] をクリックします。
- デバイスセレクタから、デバイスをダブルクリックし、[全般（General）] をクリックします。
- デバイスを選択し、[ツール（Tools）] > [デバイスのプロパティ（Device Properties）] を選択し、[全般（General）] をクリックします。

### 関連項目

- デバイス プロパティについて （7 ページ）
- [Device Credentials] ページ （58 ページ）
- [Device Groups] ページ （63 ページ）
- ポリシー オブジェクト オーバーライドのページ （69 ページ）

### フィールド リファレンス

***表 8 : [Device Properties] の [General] ページ***

| 要素 | 説明 |
|---|---|
| ID | |
| デバイス タイプ | デバイスのタイプ。 |

| 要素 | 説明 |
|---|---|
| IP タイプ（IP Type） | デバイスの IP アドレスをスタティックにする（デバイスで定義する）か、またはダイナミックにする（DHCP サーバから取得する）かを指定します。選択した IP タイプによって、表示されるフィールドが異なります。<br>（注） バージョン 4.12 以降、ASA デバイスに対する Cisco Security Manager サーバーからデバイスへの通信は、IPv6 アドレスまたは IPv4 アドレスのいずれかでサポートされます。IPv6 アドレスは 128 ビットの一意のアドレスです。IPv6 アドレスについては、スタティック IP タイプのみがサポートされています。ダイナミック IP タイプは、IPv6 アドレスではサポートされません。 |
| ホストネーム<br>（スタティック IP 専用） | デバイスの DNS ホスト名。<br>これは、デバイスにホスト名として設定される名前と同じである必要はありません。このプロパティは、[Hostname] デバイス プロパティに指定されているホスト名で更新されません。また、デバイスを再検出する場合には、デバイス設定に定義されている名前でも更新されません。<br>設定ファイルを追加してデバイスを Security Manager に追加した場合は、ホスト名が当初設定ファイルに指定されている名前に設定されます。ホスト名が設定に指定されていない場合は、ファイルの名前が DNS ホスト名として使用されます。 |
| ドメイン名<br>（スタティック IP 専用） | デバイスの DNS ドメイン名。 |
| IP Address<br>（スタティック IP 専用） | デバイスの管理 IP アドレス。192.168.3.8 など。<br>（注） IP アドレスと DNS ホスト名のどちらか一方、または両方を入力する必要があります。<br>（注） バージョン 4.12 以降、ASA デバイスに対する Cisco Security Manager サーバーからデバイスへの通信は、IPv6 アドレスまたは IPv4 アドレスのいずれかでサポートされます。デバイスがデュアルスタックで設定されている場合、Security Manager は、Security Manager に追加されたデバイスの IP アドレスに基づいてデバイスと通信します。IPv6 アドレスは 128 ビットの一意のアドレスです。 |
| 表示名 | Security Manager のデバイス セレクタに表示する名前。<br>最大長は 70 文字です。有効な文字は、0 ～ 9、大文字の A ～ Z、小文字の a ～ z、_ - . :、およびスペースです。 |

| 要素 | 説明 |
|---|---|
| オペレーティング システム | |
| OS タイプ | オペレーティング システムのタイプ。デバイス タイプに基づいて、OS タイプが自動的に選択されます。<br>（注） バージョン 4.12 以降、ASA デバイスに対する Cisco Security Manager サーバーからデバイスへの通信は、IPv6 アドレスまたは IPv4 アドレスのいずれかでサポートされます。この機能は、オペレーティング システムのタイプが ASA または FWSM であるデバイスでのみ使用できます。 |
| イメージ名（Image Name） | デバイスで実行されているイメージの名前。イメージ名は、デバイスに展開するか、またはポリシーを再検出するたびに更新されます。 |
| 実行中 OS のバージョン | デバイスで実行されているオペレーティング システムのバージョン。 |
| ターゲット OS バージョン | デバイスの設定が基づく OS バージョン。設定しているルールを使用して設定ファイルを作成するとき、Security Manager はターゲット OS バージョンで使用できるコマンドを使用します。このフィールドは、IPS デバイスの読み取り専用です。<br>ターゲット OS バージョンを、デバイスに使用できる機能セットが大きく変更されているバージョンに変更することはできません。詳細については、Security Manager の機能セットを変更する変更 （72 ページ）を参照してください。 |
| オプション | 値が [NONE] または [IPS] である読み取り専用のフィールド。値 [IPS] は、IPS 機能がデバイスで使用可能であることを示します。 |
| IPS 実行中 OS のバージョン | ルータで実行中の IOS IPS のバージョンを表示する読み取り専用のフィールド。[Options] フィールドの値が [NONE] の場合、このフィールドは表示されません。 |
| IPS ターゲット OS バージョン | ルータで実行中の IOS IPS のターゲット バージョンを表示する読み取り専用のフィールド。[Options] フィールドの値が [NONE] の場合、このフィールドは表示されません。 |
| コンテキスト | デバイスで 1 つのセキュリティ コンテキストをホストするか（[Single]）、または複数のセキュリティ コンテキストをホストするか（[Multi]）を指定します。このフィールドが表示されるのは、OS タイプが FWSM、ASA、または PIX ファイアウォール 7.0 の場合だけです。 |

| 要素 | 説明 |
|---|---|
| 動作モード（Operational Mode） | デバイスの動作モード。このフィールドが表示されるのは、OS タイプが FWSM、ASA、または PIX ファイアウォール 7.0 以降の場合だけです。使用可能なオプションは [トランスペアレント（Transparent）] または [ルータ（Router）] です。[コンテキスト（Contexts）] で [マルチ（Multi）] を選択する場合、このモードのデフォルト設定は [混合（Mixed）] になります。[混合（Mixed）] は、ASA 9.0 以降および FWSM 3.1 以降のデバイスと ASA-SM にのみ適用されます。 |
| FXOS モード | デバイスが動作している FXOS モード。使用可能なオプションは [プラットフォーム（Platform）] および [アプライアンス（Appliance）] です。[アプライアンス（Appliance）] モードを選択する場合は、CLI、オンボックスデバイス（ASDM など）、またはマルチデバイスマネージャ（Cisco Security Manager など）のいずれかから、すべてのエンドユーザー設定を実行できます。[プラットフォーム（Platform）] モードオプションは、Firepower 2000 シリーズアプライアンスに対してのみ表示されます。<br>（注） バージョン 4.20 以降、Security Manager は、Firepower 2000 および 1000 シリーズ アプライアンスに対して [アプライアンス（Appliance）] モードをサポートしています。 |
| デバイス通信設定 | |
| トランスポート プロトコル（Transport Protocol） | Security Manager がデバイスにアクセスするとき、または設定をデバイスに展開するときに使用するトランスポートプロトコル。[デフォルトを使用（Use Default）] を選択した場合は、[デバイス通信（Device Communication）] ページ（[ツール（Tools）] > [Security Manager 管理（Security Manager Administration）] > [デバイス通信（Device Communication）]）のトランスポート プロトコル セットが使用されます（[Device Communication] ページを参照）。デバイスがデフォルト プロトコルを使用するように設定されていない場合は、別のプロトコルを選択できます。<br>使用可能なトランスポート プロトコルは、どのデバイス タイプをサポートするかによって異なります。ASA など一部のデバイス タイプでは、オプションが 1 つだけであるため、フィールドはグレー表示されます。 |
| CS-MARS モニタリング | |

| 要素 | 説明 |
|---|---|
| モニタリング実施サーバ | このデバイスがモニタ対象である場合には、モニタを実施する CS-MARS サーバ。<br><br>[CS-MARS の検出（Discover CS-MARS）] をクリックして、Security Manager でどの CS-MARS サーバーがデバイスをモニターしているかを確認します。1 つの CS-MARS サーバだけがデバイスをモニタしている場合、このフィールドはそのサーバ名で更新されます。複数のサーバがある場合は、使用する CS-MARS サーバを選択するように要求されます。デバイスのポリシー ルール テーブルにファイアウォール アクセス ルールまたは IPS シグニチャを表示しているときに、CS-MARS が収集した syslog またはイベントを表示しようとした場合、ここで選択した内容によってアクセスされるサーバが決まります。<br><br>デバイスの CS-MARS サーバを検出する場合は、事前に [CS-MARS] 管理ページ（[Tools] > [Security Manager Administration] > [CS-MARS]）でサーバを Security Manager に登録しておく必要があります。詳細については、[CS-MARS] ページを参照してください。 |
| **[Auto Update] または [Configuration Engine]**<br><br>このグループは、デバイス タイプに応じて名前が異なります。<br><br>• [Auto Update]：PIX ファイアウォールおよび ASA デバイスの場合。<br><br>• [Configuration Engine]：Cisco IOS ルータの場合。<br><br>これらのフィールドは、デバイスを管理するサーバ（ある場合）を識別するために使用します。ダイナミック IP アドレスを持つデバイスには、サーバが必須です。 | |
| サーバー（Server） | デバイスを管理する Auto Update Server または Configuration Engine。AUS の場合、このサーバは AUS ポリシーに定義されているサーバと一致する必要があります（[AUS] ページを参照）。<br><br>サーバーをリストに追加するには、[サーバーの追加（Add Server）] を選択します。[サーバーのプロパティ（Server Properties）] ダイアログ ボックスが開きます（[Server Properties] ダイアログボックス （47 ページ）を参照）。[サーバーの編集（Edit Server）] を選択して [使用可能なサーバー（Available Servers）] ダイアログボックスを開き、サーバーのプロパティを編集することもできます（[Available Servers] ダイアログボックス （49 ページ）を参照）。<br><br>このサーバ リストの管理の詳細については、Auto Update Server または Configuration Engine の追加、編集、または削除 （45 ページ）を参照してください。<br><br>展開時にこのようなサーバを使用する方法の詳細については、Auto Update Server または CNS Configuration Engine を使用した設定の展開を参照してください。 |

| 要素 | 説明 |
|---|---|
| デバイスアイデンティティ | Auto Update Server または Configuration Engine でデバイスを一意に識別する文字列。AUS の場合、この ID は AUS ポリシーに定義されている ID と一致する必要があります（[AUS] ページを参照）。 |
| [ASA-CX/FirePOWER モジュール（ASA-CX/FirePOWER Module）] | |
| 管理 IP（Management IP） | ASA の CX または FirePOWER モジュールの管理 IP アドレス。デバイスの検出時またはデバイスへのモジュールの追加後に検出されます。詳細については、ASA CX モジュールおよび FirePOWER モジュールの検出を参照してください。<br>このフィールドは、Security Manager によってすでに検出されている ASA CX または FirePOWER モジュールについてのみ使用できます。 |
| Manager Address | ASA-CX または FirePOWER モジュールの設定および管理に使用される Cisco Prime Security Manager（PRSM）または FireSIGHT Management Center の IP アドレス。デバイスの検出時またはデバイスへのモジュールの追加後に検出されます。詳細については、Cisco Prime Cisco Security Manager または FireSIGHT Management Center の起動を参照してください。<br>このアドレスは編集できます。ただし、Security Manager は、アドレスの検証を実行せず、再検出または再検出によってこのアドレスが変更される可能性があります。<br>このフィールドは、Security Manager によってすでに検出されている ASA CX または FirePOWER モジュールについてのみ使用できます。 |
| Cisco Security Manager での管理 | Security Manager でデバイスを管理するかどうかを指定します。Security Manager は設定を管理せず、このデバイスの設定をアップロードまたはダウンロードしません。<br>次の理由では、インベントリに管理されていないデバイスを含めることができます。<br>• VPN エンド ポイントとして機能することがデバイスの唯一の機能である場合。<br>• デバイスがフェールオーバーに使用するセキュリティ コンテキストである場合。実際にデバイス自身からコンテキストを削除しないかぎり、管理対象デバイスのセキュリティ コンテキストを削除できません。このため、フェールオーバー コンテキストを管理対象外にする必要があります。 |

| 要素 | 説明 |
|---|---|
| フェールオーバーのライセンスサポート<br>（ASA 5505、5510 専用） | オプションのフェールオーバー ライセンスがデバイスにインストールされているかどうかを示します。オプションは、ASA 5505 および 5510 デバイスのみでアクティブになります。Security Manager は、このオプションが選択されている場合のみ、フェールオーバー ポリシーをデバイスに展開します。<br>ヒント　デバイスからポリシーを検出した場合、Security Manager はライセンス ステータスを判定し、このオプションを適切に設定します。 |

## [Device Credentials] ページ

[Device Credentials] ページは、デバイス アクセスに必要なユーザ名およびパスワードを追加または変更する場合に使用します。デバイス クレデンシャルの詳細については、デバイス クレデンシャルについて （5 ページ）を参照してください。

[クレデンシャル（Credentials）] ページは、（新規デバイス（New Device）ウィザードで）新規デバイスを追加しているか、既存のデバイスのプロパティを表示しているかにかかわらず同じです。

新規デバイスを追加するときには、手動またはネットワークからデバイスを追加する場合にだけクレデンシャルの入力を求められます。

ヒント　新規デバイス（New Device）ウィザードで、ネットワークからデバイスを追加するときに [次へ（Next）] または [完了（Finish）] をクリックした場合、Security Manager はこのようなクレデンシャルを使用してデバイスに接続できるかどうかをテストします。テストの進行中、[Device Connectivity Test] ダイアログボックスが開いたままになります（[Device Connectivity Test] ダイアログボックスを参照）。テストが失敗した場合は、[詳細（Details）] をクリックして詳細なエラー情報を表示します。モジュールが含まれているデバイス、たとえばFWSM がある Catalyst スイッチを追加している場合は、モジュール検出情報の入力を求められます。

重要　Cisco Security Manager 管理対象デバイスの場合、[デバイスのプロパティ（Device Properties）] ページでパスワードを変更する場合は、[ユーザーアカウント（User Accounts）] ページでも同じように更新してください。同じように更新しないと、Cisco Security Manager とデバイス間の通信の初期フェーズは成功し、[接続のテスト（Test Connectivity）] も正常に検証されますが、展開は失敗します。これは、[ユーザーアカウント（User Accounts）] ページで設定されたパスワードが [デバイスのプロパティ（Device Properties）] ページで更新されるためです。したがって、ログイン情報の更新が [デバイスのプロパティ（Device Properties）] ページと [ユーザーアカウント（User Accounts）] ページで並行して実行されるようにすることを推奨します。

## ナビゲーション パス

- 新規デバイスの場合、デバイスビューで[ファイル（File）]>[新規デバイス（New Device）]を選択するか、またはデバイスセレクタの [追加（Add）] ボタンをクリックします。
- 既存のデバイスの場合、デバイスプロパティを開くには、デバイスセレクタでデバイスをダブルクリックし、[デバイスのプロパティ（Device Properties）] ページで [クレデンシャル（Credentials）] をクリックします。

## 関連項目

- デバイス クレデンシャルについて （5 ページ）
- ネットワークからのデバイスの追加 （14 ページ）
- 手動定義によるデバイスの追加 （30 ページ）
- [Device Communication] ページ
- デバイス プロパティについて （7 ページ）
- デバイス プロパティの表示または変更 （51 ページ）
- デバイス通信設定および証明書の管理
- [Discovery Status] ダイアログボックス

## フィールド リファレンス

***表 9 : [Device Credentials] ページ***

| 要素 | 説明 |
|---|---|
| **Primary Credentials**<br>すべてのデバイス タイプに必須です。[HTTP] グループで [プライマリ クレデンシャルを使用（Use Primary Credentials）] を選択した場合、このようなクレデンシャルが SSH 接続と Telnet 接続、および HTTP 接続と HTTPS 接続に使用されます。<br>デバイス ポリシーで、指定したユーザに対するパスワード、またはイネーブル パスワードを変更する場合、Security Manager は、その展開中には古いパスワードをログインに使用します。展開が正常に完了すると、デバイス クレデンシャルのパスワードが、新しく展開されたパスワードに更新されます。これらのパスワードに関連するデバイス ポリシーを更新する方法については、次の項を参照してください。<br>• ASA/PIX/FWSM デバイス：デバイス クレデンシャルの設定<br>• IPS デバイス：IPS ユーザ アカウントの設定<br>• IOS デバイス：アカウントおよびクレデンシャル ポリシーの定義 | |

| 要素 | 説明 |
|---|---|
| ユーザー名 | デバイスにログインするためのユーザ名。ユーザは特権レベル 15 が必要です。<br>デバイスがその設定のみにイネーブルパスワードを必要としている場合、[Username] フィールドおよび [Password] フィールドをブランクのままにし、[Enable Password] だけを入力できます。<br>（注） PIX、ASA、およびFWSMデバイスでは、ユーザ名を4文字以上にする必要があります。パスワードには、3 ～ 32 文字を使用できますが、8 文字以上にすることを推奨します。ソフトウェアバージョン9.6(1)以降を実行しているASAデバイスの場合、最大127文字のパスワードを入力できます。 |
| パスワード | デバイスにログインするためのパスワード（ユーザ EXEC モード）。[Confirm] フィールドに、パスワードを再入力します。 |
| パスワードを有効にする（Enable Password） | イネーブル モード（特権 EXEC モード）がデバイスに設定されている場合に、そのデバイスでイネーブルモードをアクティブにするパスワード。[Confirm] フィールドに、パスワードを再入力します。 |
| **HTTP Credentials**<br>デバイスへのHTTP接続またはHTTPS接続を確立するためのクレデンシャル。デバイスの中には、このタイプの接続をサポートするものもあれば、（IPS デバイスのように）必須とするものもあります。 | |
| Use Primary Credentials<br>ユーザ名<br>パスワード | Security Manager が HTTP 接続および HTTPS 接続に設定済みのプライマリ クレデンシャルを使用するかどうかを指定します。デバイスがHTTP/HTTPS接続に異なるクレデンシャルを使用している場合は、[プライマリクレデンシャルを使用（Use Primary Credentials）] の選択を解除し、HTTP/HTTPS 用に設定されたユーザ名およびパスワードを入力します。[Confirm] フィールドにパスワードを再入力します。<br>（注） PIX、ASA、およびFWSMデバイスでは、ユーザ名を4文字以上にする必要があります。パスワードには、3 ～ 32 文字を使用できますが、8 文字以上にすることを推奨します。ソフトウェアバージョン9.6(1)以降を実行しているASAデバイスの場合、最大127文字のパスワードを入力できます。 |
| HTTP ポート（HTTP Port） | HTTP 接続に使用するポート。デフォルトのポートは 80 です。この設定値は、デフォルトとは異なるポートで HTTP 接続を受け付けるようにデバイスが設定されている場合にだけ変更します。 |

| 要素 | 説明 |
|---|---|
| HTTPS ポート（HTTPS Port） | HTTPS 接続に使用するポート。デフォルトのポートは 443 です（Security Manager デバイス通信設定に別のデフォルトが設定されていない場合）。デフォルトを変更するには、まず [デフォルトを使用（Use Default）] の選択を解除します。この設定値は、デフォルトとは異なるポートで HTTPS 接続を受け付けるようにデバイスが設定されている場合にだけ変更します。<br>（注） ローカル HTTP ポリシーを共有ポリシーとなるように設定して複数のデバイスに割り当てた場合、共有ポリシーが割り当てられるすべてのデバイスを対象に、[Device Credentials] ページに設定されたポート番号が共有ポリシーの HTTPS ポート番号設定で上書きされます。 |
| IPS RDEP Mode | イベント モニタリングのために RDEP または SDEE 接続を確立するときに、IPS デバイスへのアクセスに使用する接続方法。 |
| Certificate Common Name | 証明書に割り当てられる名前。共通名は、証明書に割り当てられた個人、システム、またはその他のエンティティの名前にすることができます。[Confirm] フィールドに、共通名を再入力します。 |
| その他のフィールドおよびボタン | |
| Authentication Certificate Thumbprint<br>（デバイス プロパティ専用） | Security Manager 証明書データ ストアに保存できるデバイスの証明書サムプリント。デバイスから現在の証明書を取得し、Security Manager に格納されている証明書に置き換えるには、[デバイスから取得（Retrieve From Device）] をクリックします。<br>IPS デバイスでは、IPS 証明書の管理で説明するように、証明書を管理するための追加オプションがあります。 |
| [RX-Boot Mode] ボタン | [RX-Boot Mode Credentials] ダイアログボックス （62 ページ）を開きます。ここでは、縮小コマンド セット イメージ（RX-Boot）からルータを起動するためのクレデンシャルを入力できます。<br>そのクレデンシャルがフラッシュ メモリから実行する Cisco ルータ用のものである場合（ルータはフラッシュの最初のファイルからだけ起動します）、フラッシュにあるイメージ以外のイメージを実行してフラッシュ イメージをアップグレードする必要があります。Rx-Boot クレデンシャルは、そのような他のイメージを実行するためのものです。 |
| [SNMP] ボタン | [SNMP Credentials] ダイアログボックス （62 ページ）を開きます。ここでは、デバイスに定義されている SNMP コミュニティ ストリングを指定できます。 |

| 要素 | 説明 |
|---|---|
| [Test Connectivity] ボタン<br>（デバイス プロパティおよび手動によるデバイス追加専用） | 入力したクレデンシャルおよび設定済みの転送方法を使用して Security Manager がデバイスに接続できるかどうかをテストします。デバイス接続のテストの詳細については、デバイス接続のテストを参照してください。 |

## [RX-Boot Mode Credentials] ダイアログボックス

[RX-Boot Mode Credentials] ダイアログボックスは、Rx-Boot モード クレデンシャルを追加する場合に使用します。このクレデンシャルは、縮小コマンド セット イメージ（Rx-Boot）からルータを起動するときに使用されます。Rx-Boot モードのユーザ名およびパスワードを入力します。[Confirm] フィールドに、パスワードを再度入力します。

### ナビゲーション パス

[RX-Bootモードログイン情報（RX-Boot Mode Credentials）] ダイアログボックスを開くには、New Device ウィザード（デバイスを手動またはネットワークから追加する場合）または [デバイスのプロパティ（Device Properties）] ページで、[Device Credentials] ページ （58 ページ）にある [RX-Bootモード（RX-Boot Mode）] をクリックします。

## [SNMP Credentials] ダイアログボックス

[SNMP Credentials] ダイアログボックスは、SNMP クレデンシャルを追加する場合に使用します。

### ナビゲーション パス

[SNMPログイン情報（SNMP Credentials）] ダイアログボックスを開くには、New Device ウィザード（デバイスを手動またはネットワークから追加する場合）または[デバイスのプロパティ（Device Properties）] ページで、[Device Credentials] ページ （58 ページ）の [SNMP] をクリックします。

### フィールド リファレンス

***表 10 : [SNMP Credentials] ダイアログボックス***

| 要素 | 説明 |
|---|---|
| **SNMP V2C**<br>SNMP バージョン 2 を実行しているデバイスのクレデンシャルです。 | |
| RO Community String | 読み取り専用のコミュニティ ストリング。[Confirm] フィールドに、コミュニティ ストリングを再入力します。 |
| RW Community String | 読み書き可能なコミュニティ ストリング。[Confirm] フィールドに、コミュニティ ストリングを再入力します。 |

| 要素 | 説明 |
|---|---|
| **SNMP V3**<br>SNMP バージョン 3 を実行しているデバイスのクレデンシャルです。 | |
| ユーザー名 | SNMP バージョン 3 の認証ユーザー名。 |
| パスワード | SNMP バージョン 3 の認証ユーザーパスワード。[Confirm] フィールドに、パスワードを再入力します。 |
| 認証アルゴリズム（Auth Algorithm） | パスワードを暗号化するための認可アルゴリズム。MD5 または SHA-1 を選択できます。 |
| プライバシー パスワード（Privacy Password） | SNMP バージョン 3 の暗号化ユーザーパスワード。[Confirm] フィールドに、パスワードを再入力します。 |
| プライバシーアルゴリズム（Privacy Algorithm） | 暗号化アルゴリズムとバージョンを選択して、暗号化レベルを指定します。<br>• DES：56 ビットキーを使用して、Data Encryption Standard（DES; データ暗号規格）暗号アルゴリズムを適用します。<br>• 3DES：トリプル DES を使用します。Data Encryption Standard（DES; データ暗号規格）暗号アルゴリズムは、各パケットに 3 回適用されます。<br>• AES128：128 ビットキーで Advanced Encryption Standard を使用します。<br>• AES192：192 ビットキーで Advanced Encryption Standard を使用します。<br>• AES256：256 ビットキーで Advanced Encryption Standard を使用します。 |
| エンジンID（Engine ID） | デバイスの SNMP v3 認証エージェントの 16 進数の識別子を入力します。 |

## [Device Groups] ページ

[Device Groups] ページは、デバイスをデバイス グループに割り当てる場合に使用します。このページからデバイス グループを編集または削除することもできます。

### ナビゲーション パス

- 新規デバイスの場合、デバイスビューで [ファイル（File）]>[新規デバイス（New Device）] を選択するか、またはデバイスセレクタの [追加（Add）] ボタンをクリックします。

- 既存のデバイスの場合、デバイスプロパティを開くには、デバイスセレクタでデバイスをダブルクリックし、[デバイスプロパティ（Device Properties）] ページで [デバイスグループ（Device Groups）] をクリックします。

### 関連項目

- デバイスのグループ化について （79 ページ）
- デバイス インベントリへのデバイスの追加 （8 ページ）
- デバイス プロパティについて （7 ページ）
- [Discovery Status] ダイアログボックス

### フィールド リファレンス

***表 11 : [Device Grouping] ページ***

| 要素 | 説明 |
|---|---|
| [Department] や [Location] などの [Group Types] | Security Manager に定義されているグループ タイプ。[Department] や [Location] など。各フィールドには、そのグループ タイプ内に定義されたデバイス グループのリストが含まれています。デバイスを所属させるデバイス グループを選択します。<br><br>新規デバイスグループまたはグループタイプを作成する場合は、いずれかの既存グループタイプのドロップダウンリストから [グループの編集（Edit Groups）] を選択します。これにより、[Edit Device Groups] ページが開きます。ここでは、新規グループおよびグループ タイプを作成または削除できます（[Edit Device Groups] ダイアログボックス （81 ページ）を参照）。 |
| Set values as default | 選択したグループをデフォルト グループとして設定するかどうかを指定します。このオプションを選択した場合、他に追加しようとしているデバイスもそのグループに自動的に追加されます。 |

## [グループ情報（Group Information）] ページ

[デバイスプロパティのグループ情報（Device Properties Group Information）] ページを使用して、グループの詳細を表示します。

### ナビゲーション パス

- デバイスセレクタから、デバイスを右クリックし、[デバイスのプロパティ（Device Properties）] を選択し、[グループ情報（Group Information）] をクリックします。
- デバイスセレクタから、デバイスをダブルクリックし、[グループ情報（Group Information）] をクリックします。

- デバイスを選択し、[ツール（Tools）]>[デバイスのプロパティ（Device Properties）] を選択し、[グループ情報（Group Information）] をクリックします。

## 関連項目

- デバイスクラスタの使用 （11 ページ）
- デバイス プロパティについて （7 ページ）
- [Device Credentials] ページ （58 ページ）
- [Device Groups] ページ （63 ページ）
- ポリシー オブジェクト オーバーライドのページ （69 ページ）

## フィールド リファレンス

表 *12 : [デバイスプロパティのグループ情報（Device Properties Group Information）]ページ*

| 要素 | 説明 |
|---|---|
| グループの詳細（Group Details） | |
| デバイスタイプ | デバイスのタイプ。 |
| グループ名（Group Name） | グループに割り当てられた名前。 |
| Group Control | 制御ユニットとして機能するデバイスのグループメンバー名。<br>（注） 制御ユニットへの変更は、Security Manager に自動的には反映されません。 |
| デバイスから取得（Retrieve From Device） | [デバイスから取得（Retrieve From Device）] を使用して、制御ユニット情報を更新します。 |
| インターフェイス モード | インターフェイスがレイヤ 2 ロードバランシング（スパンド EtherChannel）またはレイヤ 3 ロードバランシング（単独）用のどちら設定されているか。 |

| 要素 | 説明 |
|---|---|
| 管理IPプール範囲（Management IP Pool Range） | クラスタの管理に使用する IP アドレスプールを入力します。ユーザコンテキストのデバイスにこの値を指定できます。マルチコンテキスト ASA クラスタの syslog をモニターするために Event Viewer が使用されている場合、このフィールドは必須です。<br>このフィールドを空白のままにするか、正しくない IP アドレスプールを入力すると、Event Viewer は syslog を特定のコンテキストに分類できず、syslog イベントをドロップします。<br>（注） 有効な IP アドレスを入力していることを確認してください。Cisco Security Manager は、入力された IP アドレスプールを検証しません。 |
| CSMでの最終更新（Last Update in CSM） | このグループのグループ情報が Security Manager によって最後に更新された日時。 |
| グループVPNモード（Group VPN Mode） | Cisco Security Manager 4.16 以降では、グループ デバイスを検出した後、グループ VPN モードが表示されます。この値は [集中型（Centralized）]または[分散型（Distributed）] です。<br>（注） この値は、デバイスセレクタビューでデバイスの上にマウスポインタを置いたときに表示されるポップアップウィンドウにも表示されます。 |
| グループVPNバックアップ（Group VPN Backup） | Cisco Security Manager 4.16 以降では、[グループVPNバックアップ（Group VPN Backup）] が表示されます。<br>分散型モードでは、次のいずれかの値が表示されます 。<br>• [フラット（Flat）] : グループ VPN バックアップが他のメンバーに存在する場合<br>• [リモートシャーシ（Remote Chassis）] : グループ VPN バックアップが別のシャーシに存在する場合<br>グループ VPN バックアップの情報は、集中型 VPN モードでは表示されません。集中型 VPN モードでのこのフィールドの値は N/A です。<br>（注） この値は、デバイスセレクタビューでデバイスの上にマウスポインタを置いたときに表示されるポップアップウィンドウにも表示されます。 |
| **グループノードの詳細（Group Node Details）**<br>[グループノードの詳細（Group Node Details）] テーブルには、グループ内の各デバイスの詳細が一覧表示されます。 | |

| 要素 | 説明 |
|---|---|
| グループ ID（Group ID） | グループノードのグループ ID。 |
| ノード名 | グループノードのメンバー名。 |
| シリアル番号 | グループノードのシリアル番号。 |
| CCL IP | グループノードのグループ制御リンク IP アドレス。 |
| CCL MAC | グループノードのグループ制御リンク MAC アドレス。 |
| サイト ID（Site ID） | 現在のグループメンバーが属するサイト。サイト ID を設定すると、MAC アドレスのフラッピングが防止されます。 |

## [ライセンス情報（License Information）] ページ

[デバイスプロパティ（Device properities）] ウィンドウで、FPR-3100 シリーズ デバイスのプラットフォームライセンスのサブスクリプション ステータス、ライセンスの有効期限、およびライセンスの取得日をモニタリングできます。

### CSM ライセンススケジューラ

CSM ライセンススケジューラは毎日実行され、デバイスからプラットフォームライセンスの詳細を取得し、CSM データベースで同じ情報を更新します。これは 24 時間ごとに 1 回実行されるバックグラウンドプロセスであり、デフォルトの時刻は午前 4 時です。CSM プロパティファイルのライセンススケジューラの時刻はカスタマイズ可能です。CSM プロパティファイルは、..\CSCOpx\MDC\athena\configcsm.properties にあります。ライセンススケジューラでは、次の 3 つのモードがサポートされています。

- [AM]：0 ～ 11 の任意の時刻を入力でき、スケジューラは毎朝特定の時刻に実行されます。
- [PM]：1 ～ 12 の任意の時刻を入力でき、スケジューラは午後の特定の時刻に実行されます。
- [AMPM]：24 時間形式で設定する場合に使用します。スケジューラは指定した特定の時刻に実行されます。

（注） ライセンススケジューラは、サービスまたはシステムの再起動時に開始され、停止することはできません。

更新されたライセンス情報は、CSM の [ライセンス情報（License Information）] タブの [ポリシーヘッダー（Policy Header）] と [デバイスプロパティ（Device Properties）] に反映されます。

### ナビゲーション パス

- デバイスセレクタから、FPR-3100 シリーズ デバイスを右クリックし、[デバイスプロパティ（Device Properties）] を選択して、[ライセンス情報（License Information）] をクリックします。
- デバイスセレクタから、FPR-3100 シリーズデバイスをダブルクリックして、[ライセンス情報（License Information）] をクリックします。
- FPR-3100 シリーズ デバイスを選択し、[ツール（Tools）] > [デバイスプロパティ（Device Properties）] を選択してから、[ライセンス情報（License Information）] をクリックします。

（注） プラットフォームライセンス情報のライセンス取得時刻は、DST 中には表示されません。

### [デバイスプロパティ（Device Properties）] のライセンス サブスクリプション ステータス

FPR-3100 シリーズ デバイスで、CSM はプラットフォーム ライセンス サブスクリプションのさまざまなステータスを処理します。[ライセンスの詳細（License Details）] は、[デバイスプロパティ（Device Properties）] ページの [ライセンス情報（License Information）] に表示されます。サポートされているライセンス サブスクリプションのステータスは次のとおりです。

| ステータス（Status） | 説明 |
|---|---|
| 新規インストール | インストール後のライセンスの変更はありません。 |
| 評価モード | 設定の変更が完了し、ライセンス機能階層の標準が設定されました。利用可能なライセンスの有効期限は 90 日間です。 |
| 評価モードの期限切れ | 評価モードの有効期限が切れています。 |
| Compliant | Firepower デバイスはアカウントに登録されており、十分なライセンスがあります。 |
| 猶予期間 | 登録されているデバイスの数に比べて、アカウントのライセンス数が不足しています。設定変更の展開は 90 日間有効です。 |
| 猶予期間の期限切れ | 猶予期間の期限が切れています。<br>ヒント アカウントに接続して修正するか、不要なデバイスを登録解除します。 |

（注） プラットフォームライセンスが期限切れになっている FPR-3100 シリーズ デバイスは、展開時にアクティビティ検証エラーをトリガーします。アクティビティ検証エラーにより、デバイスを管理できないため、ライセンスをアップグレードして展開を実行するか、CSM からデバイスを削除する必要があります。[インベントリを使用した再検出（Re-discovery via inventory）] オプションを使用して、CSM のプラットフォームライセンスの詳細を一度に更新します。

### ポリシーヘッダーのライセンス サブスクリプション ステータス

FPR-3100 シリーズ デバイスの [プラットフォームライセンス（Platform License）] は、CSM のポリシーヘッダー GUI にカラーコードで表示されます。ライセンス詳細のカラーコードは次のとおりです。

- 承認：黒
- 猶予期間：オレンジ
- 評価モード：オレンジ
- 評価モードの期限切れ：赤
- 猶予期間の期限切れ：赤
- 使用中のライセンスなし：黒

（注） ポリシービューには、FPR-3100 シリーズデバイスのライセンスステータスが表示されません。

## ポリシー オブジェクト オーバーライドのページ

選択したデバイスの [Device Properties] ウィンドウから、多くのタイプのポリシー オブジェクトのグローバル設定を上書きできます。これにより、そのデバイスにあるオブジェクトの定義をカスタマイズできます。詳細については、個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。

コンテンツ テーブルの [Policy Object Overrides] フォルダには、特定のデバイス タイプのオーバーライドを作成できるあらゆるタイプのオブジェクトが含まれています。オブジェクト タイプを選択すると、デバイスのオーバーライドを許可するように設定されている既存のポリシー オブジェクトがあれば、右ペインのテーブルに表示されます。オブジェクトにデバイスに対するオーバーライドがすでに定義されている場合、[値がオーバーライドされているか（Value Overridden?）] カラムにチェックマークが付けられます。

このようなオブジェクトのオーバーライドを作成および管理できます。オブジェクトを選択し、次の手順を実行できます。

- オーバーライドを作成するには、[Create Override] ボタンをクリックします。これにより、そのタイプのオブジェクトを編集するためのダイアログボックスが開きます。オブジェクト固有の情報については、[Help] ボタンをクリックしてください。
- 既存のオーバーライドを編集するには、[Edit Override] ボタンをクリックします。
- オーバーライドを削除するには、[Delete Override] ボタンをクリックします。

### ナビゲーション パス

デバイスセレクタでデバイスをダブルクリックし、左ペインのコンテンツテーブルにある [ポリシーオブジェクトオーバーライド（Policy Object Overrides）] フォルダで目的のポリシーオブジェクトタイプをクリックします。

### 関連項目

- [Policy Object Overrides] ウィンドウ
- ポリシー オブジェクトの上書きの許可
- 単一デバイスのオブジェクト オーバーライドの作成または編集
- デバイスレベルのオブジェクト オーバーライドの削除
- テーブルのフィルタリング

# 重要なデバイス プロパティの変更

デバイスのイメージ バージョン、デバイス タイプ、または Security Manager によって管理される FWSM デバイスおよび ASA デバイスのセキュリティ コンテキストまたは動作モードを変更するときには、注意が必要です。このような変更を加えると、デバイスの別の機能セットがイネーブルになる場合があります。その結果、Security Manager でデバイスに設定したポリシーの一部が適用されなく可能性があります。

主要なデバイス変更、その変更が Security Manager のポリシーに及ぼす影響、およびこのようなデバイス変更を実装する際の手順については、以降の項で説明します。

- Security Manager の機能セットを変更しないイメージ バージョン変更 （70 ページ）
- Security Manager の機能セットを変更する変更 （72 ページ）

## Security Manager の機能セットを変更しないイメージ バージョン変更

次のイメージバージョン変更は、Security Manager で該当するデバイスに使用できるポリシーのタイプに影響しません。

- 1 つの IOS 個別リリース番号から、同じ Cisco IOS リリース内の別の個別リリース番号へのアップグレード（たとえば IOS 12.3(10) から 12.3(13) へのアップグレード）。
- 任意の IOS 12.1 イメージから任意の 12.2 イメージへのアップグレード。

- 任意の IOS 12.2 イメージから任意の 12.3 イメージへのアップグレード。
- 任意の IOS 15.0 イメージから任意の 15.1 イメージへのアップグレード。
- 任意の IOS 15.2 イメージから任意の 15.3 イメージへのアップグレード。
- 任意の PIX 6.x イメージから別の PIX 6.x イメージへのアップグレード。
- 任意の PIX 7.x イメージから別の PIX 7.x イメージへのアップグレード（同じセキュリティ コンテキストおよびモード設定を保持）。
- 任意の ASA 7.x イメージから別の ASA 7.x イメージへのアップグレード（同じセキュリティ コンテキストおよびモード設定を保持）。
- 任意の ASA 8.0(x) ～ 8.2(x) イメージから別の ASA 8.0(x) ～ 8.2(x) イメージへのアップグレード（同じセキュリティ コンテキストおよびモード設定を保持）。
- 任意の FWSM 2.x イメージから別の 2.x FWSM イメージへのアップグレード（同じセキュリティ コンテキストおよびモード設定を保持）。
- 任意の FWSM 3.x イメージから別の 3.x FWSM イメージへのアップグレード（同じセキュリティ コンテキストおよびモード設定を保持）。
- 任意の IOS 12.x イメージから別の IOS 12.x イメージへの Catalyst 6500/7600 シャーシのアップグレード。

（注） このリストは、Security Manager がサポートするイメージにだけ適用されます。サポートされるイメージのリストについては、次の URL にあるこの製品バージョンの『*Supported Devices and Software Versions for Cisco Security Manager*』を参照してください（http://www.cisco.com/en/US/products/ps6498/products_device_support_tables_list.html [英語]）。

このような場合、次の手順を使用してイメージ バージョンを変更します。

**関連項目**

- デバイス ビューについて （1 ページ）
- デバイス プロパティについて （7 ページ）
- ポリシーについて
- Security Manager の機能セットを変更する変更 （72 ページ）

**ステップ 1** デバイスのイメージ バージョンをアップグレードします。

**ステップ 2** デバイス ビューのデバイス セレクタで次のいずれかを実行し、[Device Properties] ダイアログボックスを開きます。

- デバイスをダブルクリックします。

- デバイスを右クリックして、[デバイスのプロパティ（Device Properties）] を選択します。
- デバイスを選択して、[ツール（Tools）] > [デバイスのプロパティ（Device Properties）] の順に選択します。

**ステップ 3** [デバイスプロパティ（Device Properties）] ダイアログボックスで、[全般（General）] ページにある [ターゲットOSバージョン（Target OS Version）] プロパティを更新後のバージョン番号に変更し、[保存（Save）] をクリックします。

## Security Manager の機能セットを変更する変更

デバイスに使用できるポリシー フィーチャ セットに影響を与える主要なタイプのデバイス変更です。

- イメージ バージョン変更：次のイメージ バージョン変更は、Security Manager でそのデバイスに使用できるポリシーのタイプに影響を与えます。
  - ASA 8.3(x) 以下のリリースから ASA 8.4(x) 以降のリリースへのアップグレード。
  - ASA 8.2(x) 以下のリリースから ASA 8.3(x) 以降のリリースへのアップグレード。
  - ASA、PIX、FWSM、IPS の各デバイスのメジャー バージョン番号の変更。たとえば、8.x から 9.x への ASA のアップグレード、または 7.x から 6.x への IPS デバイスのダウングレード。
  - IOS 12.1 イメージまたは 12.2 イメージから IOS 12.3 イメージまたは 12.4 イメージへのアップグレード。
  - IOS 12.3 イメージまたは 12.4 イメージから IOS 12.1 イメージまたは 12.2 イメージへのダウングレード。
  - IOS 12.3 以前のリリースから IOS 15.2 以降へのアップグレード。

このような変更を加えた場合でも、その変更の影響を受けるポリシーをまだ定義していなければ、デバイスのターゲット OS バージョンを変更できる可能性があります。管理対象デバイスのターゲット OS バージョンを別のバージョンに変更すると、そのデバイスに使用できるポリシーのタイプが変更される場合、Security Manager ではそのような変更が許可されません。そのような変更を加えることができない場合には（問題のポリシーを特定したうえで）通知されます。このため、まず Security Manager からデバイスを削除し、イメージの変更を実行してから、デバイスを追加し直す必要があります。

アクセスルールなどポリシーのタイプによっては、イメージバージョンまたはプラットフォーム タイプの変更の影響を受けないものがあります。

8.3 および 9.0.1 ASA リリースで導入された NAT ポリシーの変更では、NAT ポリシーを Security Manager で再検出する必要があります。これは、以下で説明するように、デバイスを削除してから Security Manager に再度追加することで実現できます。または、デバイスのポリシーの検出機能を使用して NAT ポリシーのみを再検出することもできます。デバイスのポリシーの検

出機能については、Security Manager にすでに存在するデバイス上のポリシーの検出を参照してください。

（注） ASA デバイスが Security Manager の外で現在のバージョンから上位または下位のバージョンにアップグレードまたはダウングレードされた場合は、デバイスを削除してから、Security Manager に再度追加する必要があります。

- セキュリティ コンテキストおよび動作モードの変更：FWSM デバイスまたは ASA デバイスのセキュリティ コンテキストおよび動作モード設定に変更を加えると、そのデバイスで別の機能セットがイネーブルになります。このような変更は、次のようにデバイスを変更すると発生します。
  - 単一のコンテキストから複数のコンテキスト（またはその逆）。
  - ルーテッド モードからトランスペアレント モード（またはその逆）。

Security Manager では、管理対象デバイスのセキュリティ コンテキストまたは動作モード設定を変更できません。このため、まず Security Manager からデバイスを削除し、コンテキストまたはモードを変更してから、デバイスを追加し直す必要があります。

ポリシー タイプによっては（たとえば、Banner、Clock、Console Timeout、HTTP）、動作モードの変更の影響を受けないものがあります。このほか（Banner および Clock に加えて ICMP、SSH、TFTP のように）セキュリティ コンテキスト設定の変更の影響を受けないものもあります。

- デバイス ハードウェアの交換：特定のデバイスを交換しても、元の連絡先情報（IP アドレスなど）を保持できる場合があります。
  - PIX ファイアウォールを Cisco IOS ルータに交換する場合。
  - PIX ファイアウォールを ASA デバイスに交換する場合。
  - ルータをファイアウォール デバイスに交換する場合。
  - ルータを別のモデルの新規ルータに交換する場合。

このいずれの場合でも、新規デバイスにより、Security Manager でそのデバイスに使用できるポリシーのタイプが変更されます。Security Manager では、既存のデバイスのハードウェア モデルを変更できません。このため、まず Security Manager からデバイスを削除し、物理デバイスを変更してから、デバイスを追加し直す必要があります。

ポリシー タイプによっては（たとえば、アクセル ルール）は、デバイス タイプの変更の影響を受けないものがあります。

変更の影響を受けないデバイスを Security Manager から削除する前に、そのデバイスに設定されたポリシーを共有することを推奨します。このようにすると、Security Manager を追加し直したあと、ポリシーをデバイスに（継承およびポリシー オブジェクト参照はそのままにして）再び割り当てることができるため便利です。次の手順では、その方法について説明します。

### 関連項目

- デバイス ビューについて （1 ページ）
- デバイス プロパティについて （7 ページ）
- ポリシーについて
- Security Manager の機能セットを変更しないイメージ バージョン変更 （70 ページ）

---

**ステップ 1** Security Manager でデバイスに設定したすべての変更を送信し、展開します。これにより、イメージのアップグレードよりも前に、目的の設定がデバイスに配置されます。

**ステップ 2** デバイスに定義されているローカル ポリシーを共有します。

a) デバイスセレクタでデバイスを右クリックし、[デバイスポリシーの共有（Share Device Policies）] を選択します。デフォルトでは、Share Policies ウィザードでの共有対象として、デバイスに設定されたすべてのポリシー（ローカルおよび共有）が選択されます。

b) ポリシー アイコンに手の形で示されている既存の各共有ポリシーの横にあるチェックボックスをオフにします。この操作が必要になるのは、すでに存在する共有ポリシーのコピーを作成する必要がないためです。イメージ バージョンのアップグレード後に、既存の共有ポリシーを再び割り当てます。

c) 共有ポリシーの名前を入力します。デバイス名を便利な識別手段として使用することを推奨します。たとえば、デバイス名が MyRouter である場合、各共有ポリシーには MyRouter という名前が付与されます。このために、作成しているすべてのポリシーを書き留めます。

d) [終了（Finish）] をクリックします。選択したローカル ポリシーが共有ポリシーになります。

**ステップ 3** Security Manager からデバイスを削除します。

**ステップ 4** デバイスに目的の変更を加えます。たとえば、イメージ バージョンのアップグレード、動作モードの変更、デバイスの交換などです。

**ステップ 5** デバイスを Security Manager に追加し直し、ポリシー検出を実行します。

**ステップ 6** デバイスにポリシーを再び割り当てます。

a) デバイスポリシーセレクタに表示された最初のポリシータイプを右クリックし、[共有ポリシーの割り当て（Assign Shared Policy）] を選択します。

b) [Assign Shared Policy] ダイアログボックスで、次のいずれかを実行します。

- ローカルポリシーがデバイスで以前に定義されている場合は、この手順のために作成した共有ポリシーを選択し、[OK] をクリックします。
- このタイプの共有ポリシーがデバイスに以前に割り当てられていた場合は、そのポリシーを選択し、[OK] をクリックします。

c) （ローカルポリシーのみ）デバイスポリシーセレクタで再度ポリシータイプを右クリックし、[ポリシーの共有解除（Unshare Policy）] を選択します。

d) デバイスの設定に関連するポリシータイプごとに、この手順を繰り返します。共有ポリシーが使用できない場合は、これが以前のイメージバージョンに使用できなかったポリシー タイプであることを示します。

**ステップ 7** （任意）この手順のために作成した共有ポリシーをポリシー ビューから削除します。

a) [表示（View）]>[ポリシービュー（Policy View）]を選択するか、またはツールバーの[ポリシービュー（Policy View）]アイコンをクリックします。
b) 削除するポリシーのいずれかを選択し、作業領域の[割り当て（Assignments）]タブをクリックして、ポリシーがどのデバイスにも割り当てられていないことを確認します。
c) 共有ポリシーセレクタの下にある[ポリシーの削除（Delete Policy）]ボタンをクリックして、ポリシーを削除します。
d) 削除するポリシー タイプごとに、この手順を繰り返します。

# デバイスに含まれている要素の表示

サービス モジュール、セキュリティ コンテキスト、および仮想センサーを含んでいるデバイスを対象に、それぞれの内容を表示できます。デバイスのタイプに基づいて、このようにデバイスに含まれている要素を表示できます。

- Catalyst 6500 デバイス：IDSM および FWSM サービス モジュール、セキュリティ コンテキスト、および仮想センサー。
- FWSM、PIX ファイアウォール 7.0、および ASA デバイスの場合：デバイスに定義されているセキュリティ コンテキスト。セキュリティ コンテキストの詳細については、ファイアウォール デバイスでのセキュリティ コンテキストの設定を参照してください。
- IPS デバイス：デバイスに定義されている仮想センサー。

含まれている項目を表示するには、デバイスビューで、該当するタイプのデバイスのいずれかを選択し、[ツール（Tools）]>[内容の表示（Show Containment）]を選択するか、またはデバイスを右クリックし、[内容の表示（Show Containment）]を選択します。[Composite View]ダイアログボックスが開き、選択したデバイスに含まれる要素があれば表示されます。

# デバイスの複製

複製した（重複する）デバイスでは、複製元のデバイスの設定およびプロパティが共有されます。デバイスを複製すると、新規デバイスの設定およびプロパティを再作成する必要がないため、時間の節約になります。

複製したデバイスは、デバイスのオペレーティング システム バージョン、クレデンシャル、およびグループ化属性を複製元のデバイスと共有しますが、表示名、IPアドレス、ホスト名、ドメイン名など独自の一意のアイデンティティもあります。一度に複製できるデバイスは、1つだけです。

（注） Catalyst スイッチまたは Catalyst 6500/7600 デバイスは複製できません。

**関連項目**

- デバイス ビューについて （1 ページ）

- デバイス間でのポリシーのコピー

**ステップ 1** 次のいずれかを実行します。

- （デバイスビュー）デバイスを選択し、**[ファイル（File）] > [デバイスの複製（Clone Device）]** を選択するか、またはデバイスセレクタでデバイスを右クリックし、[デバイスの複製（Clone Device] を選択します。
- （マップビュー）デバイスを右クリックし、[デバイスの複製（Clone Device] を選択します。

[Create a Clone of Device] ダイアログボックスが表示されます。

**ステップ 2** 複製の IP アドレスおよび名前をそれぞれ該当するフィールドに入力します。次に、使用可能な属性を示します。

- [IPタイプ（IP Type）]：デバイスでスタティック IP アドレスが使用されるのか、（DHCP から提供される）ダイナミック IP アドレスが使用されるのかを指定します。デバイスを複製するときには、IP タイプは変更できません。
- [ホスト名（Hostname）]：（スタティック IP のみ）。複製したデバイスの DNS ホスト名。
- [ドメイン名（Domain Name）]：（スタティック IP のみ）。複製したデバイスの DNS ドメイン名。ドメイン名を指定しないと、Security Manager ではサーバに設定されたデフォルトのドメイン名が使用されます。
- [IPアドレス（IP Address）]：複製したデバイスの管理 IP アドレス（10.10.100.1 など）。IP アドレスがわからない場合は、[Hostname] フィールドに DNS ホスト名を入力します。スタティック IP アドレスが設定されたデバイスの IP アドレスまたはホスト名を入力する必要があります。

（注） バージョン 4.12 以降、ASA デバイスに対する Cisco Security Manager サーバーからデバイスへの通信は、IPv6 アドレスまたは IPv4 アドレスのいずれかでサポートされます。

- [表示名（Display Name）]：Cisco Security Manager デバイスリストに表示される名前。最大長は 70 文字です。有効な文字は、0 ～ 9、大文字の A ～ Z、小文字の a ～ z、_ - . :、およびスペースです。
- [デバイスID（Device Identity）]：（ダイナミック IP のみ）。Auto Update Server または Configuration Engine でデバイスを一意に識別する文字列値。このフィールドは、このようなサーバのいずれかを使用するようにデバイスが設定されている場合にだけ表示されます。
- [VPN割り当ての複製（Clone VPN Assignments）]：デバイスに対して定義されている VPN 割り当てをコピーするかどうかを指定します。このフィールドは、デバイスが VPN 割り当てをサポートする場合にだけ表示されます。

ハブアンドスポーク設定のスポークとなっているデバイス、または完全メッシュ トポロジに参加しているデバイスの VPN 割り当てを複製できます。スポーク デバイスを複製した場合、新規デバイスは複製元と同じポリシーで VPN に新規スポークとして追加されます。完全メッシュ VPN のデバイスを複製した場合、新規デバイスは複製元と同じポリシーで完全メッシュ VPN に追加されます。ポイントツーポイント VPN トポロジのデバイスは複製できません。

**ステップ 3** [OK] をクリック複製元のデバイスの複製が、一意の表示名でデバイス セレクタに作成されます。

# Security Manager インベントリからのデバイスの削除

あるデバイスをこれ以上 Security Manager で管理しないことにした場合は、そのデバイスをインベントリから削除できます。デバイスを Security Manager から削除しても、デバイスの設定は変更されません。

**ヒント** そのデバイスに別のユーザがポリシーを設定中であった場合は、ロックが機能してデバイスは削除できません。

デバイスのタイプによっては削除する際に特殊な考慮事項があります。

- デバイスが VPN に参加している場合、デバイスを削除すると VPN からデバイスが削除されます。ただし、デバイスの削除によって VPN トポロジが無効になる場合は、デバイスを削除したときに VPN トポロジ全体も削除されます。このことが警告され、デバイスの削除をキャンセルすることもできます。
- マルチ コンテキスト モードで動作する ASA、PIX、FWSM の各デバイスの場合、または仮想センサーが含まれている IPS デバイスの場合、デバイスを削除するとセキュリティ コンテキストまたは仮想センサーもすべて削除されます。この手順では個々のセキュリティ コンテキストまたは仮想センサーは削除できません。代わりに、目的のセキュリティ コンテキストまたは仮想センサーを削除するように、ホスティング デバイスで適切なポリシーを変更する必要があります。
- 管理対象のサービス モジュールが含まれているデバイスを削除した場合は、その含まれていたデバイスも削除されます。たとえば、FWSM を含めて Catalyst スイッチを追加していた場合に、Catalyst スイッチを削除すると、FWSM も削除されます。含まれているデバイスも削除されることが警告されます。

**ヒント** デバイスの削除には、データベースから多数の情報を削除する処理が伴います。一度に多数のデバイスを削除すると、処理が完了するまでに時間がかかることがあります。多数のデバイスを削除する場合には、いくつかのグループに分けて削除することを推奨します。

**ステップ 1** デバイス ビューで、次のいずれかを実行します。

- 削除するデバイスを選択するか、またはデバイス グループ内のデバイスをすべて削除する場合にはそのグループを選択し、右クリックして、[デバイスの削除（Delete Devices）] を選択します。デバイス セレクタの上部にある [デバイスの削除（Delete Devices）] ボタン（ゴミ箱アイコン）をクリックすることもできます。

- **[ファイル（File）]>[デバイスの削除（Delete Devices）]** を選択し、[デバイスセレクタ（Device Selector）] ダイアログボックスで削除するデバイスを選択し、[>>] をクリックしてデバイスを選択済みデバイス リストに移動します（リストには、デバイスツリーで選択したデバイスが含まれています）。デバイス グループを選択して、グループのメンバーであるデバイスをすべて削除できます。完了したら、[OK] をクリックします。

ヒント　デバイス グループを選択すると、そのグループ内のデバイスだけが削除され、グループ自体は削除されません。デバイス グループの削除の詳細については、デバイス グループまたはグループ タイプの削除　（83 ページ）を参照してください。

**ステップ 2**　デバイスを削除するかどうかの確認が求められます。

確認すると、Security Manager はデバイスが削除できるかどうかを検証します。問題または潜在的な問題が明らかになった場合は、その問題が [Device Delete Validation] ダイアログボックス　（78 ページ）に記載されます。このダイアログボックスには、（削除できないデバイスを示す）エラーのほか、警告と情報メッセージも表示されます。

警告または情報メッセージがあるデバイスも、メッセージに説明されている結果を受け入れるのであれば削除できます。ダイアログボックスには、選択したすべてのデバイスの削除を続行できる場合は [OK] ボタンが表示され、エラーメッセージがある場合は [続行（Continue）] ボタンが表示されます。[続行（Continue）] をクリックすると、エラー状態でないデバイスだけが削除されます。確認が求められます。

## [Device Delete Validation] ダイアログボックス

[Device Delete Validation] ダイアログボックスは、デバイスの削除中に発行されたエラー、警告、および情報メッセージを表示する場合に使用します。デバイスの削除の詳細については、Security Manager インベントリからのデバイスの削除　（77 ページ）を参照してください。

各行が、デバイスを削除しようとしたときに検証で問題が発生したデバイスを表します。表示されるのは、メッセージ重大度アイコン、デバイス表示名、および検証の結果です。検証結果には、デバイスを削除できない理由か、またはデバイスの削除によってもたらされる予期しない結果に関する警告または情報が示されます。メッセージがないデバイスはリストに表示されません。

行をダブルクリックするか、行を選択して [詳細（Details）] ボタンをクリックすると、詳細なメッセージが表示されます。情報がさらに読みやすい形式で [Device Delete Validation Details] ダイアログボックスに表示されます。

メッセージ重大度は次のいずれかになります。

- エラー：デバイスの削除を妨げる問題が検出されました。たとえば、別のユーザがデバイスをロックしています。
- 警告：今後の操作に注意を喚起します。たとえば、デバイスを削除すると、VPN トポロジが無効になり、続行した場合には VPN トポロジも削除されます。
- 情報：小さな問題が発生しています。たとえば、デバイスを削除すると、VPN からデバイスが削除されます。

デバイスの削除を続行するには、[OK] ボタンまたは [Continue] ボタンをクリックします。両者は実質的に同じボタンです。

- [OK] が表示されている場合、このボタンをクリックすると、削除対象に選択したすべてのデバイスが削除されます。
- [続行（Continue）] が表示されている場合、選択したデバイスの中にエラーがあるものがあります。[Continue] をクリックすると、エラーがないデバイスだけが削除されます。

選択したすべてのデバイスにエラーがある場合は、ボタンがグレーになり、[Cancel] をクリックする必要があります。デバイスを削除する前に、エラーを残らず解決します。

### ナビゲーション パス

このダイアログボックスが表示されるのは、デバイスを削除しようとしたものの、Security Manager によってその削除に問題があると判断された場合だけです。

# デバイス グループの使用

デバイス グループを作成すると、効率よくデバイスを管理できるようにデバイスを編成できます。次の項では、デバイス グループとその使用方法について説明します。



## デバイスのグループ化について

デバイス グループは簡素かつ任意に編成したデバイスの集まりであり、効率よくネットワークを可視化できます。ポリシーを共有するエンティティではありません。各種のポリシー オブジェクト グループ（たとえば AAA サーバ グループ オブジェクトやユーザ グループ オブジェクト）とは異なるものです。ポリシー オブジェクトの詳細については、ポリシー オブジェクトの管理を参照してください。

**ヒント** デバイスの数が多い場合、グループ化すると、変更をデバイスに展開するときに対象となるデバイスを選択するのが容易になります。たとえば、いくつかのデバイスに同時に変更を展開する場合、それらのデバイスを単一のデバイス グループにまとめておくと、そのグループを選択するだけで展開ジョブを完了できます。ポリシー展開の詳細については、展開の管理を参照してください。

デバイスをグループ化すると、インベントリ内のデバイスのサブセットを表示できます。デバイス グループ階層には、次の 2 つのタイプのフォルダがあります。

- デバイス グループ タイプ：グループ タイプが階層の最上位となります。グループ タイプには特定のデバイス グループを含めることができますが、インベントリのすべてのデバイスが含まれる All グループ タイプを除き、デバイスを含めることはできません。Security Manager には、グループ タイプとして Department と Location があらかじめ定義されていますが、必ず使用しなければならないものではなく、削除することもできます。最大 10 個のグループ タイプを作成できます。
- デバイス グループ：デバイス グループは、グループ タイプ フォルダ内のサブフォルダです。複数レベルのネスト デバイス グループを作成できます。デバイス グループ内にデバイスを配置できます。ただし、デバイスを配置できるのはグループ タイプ内の 1 つのグループだけです。たとえば、図 3 : デバイス グループ（Device Groups） では、グループ タイプ Location の下で、routerx を San Jose に割り当てることはできますが、routerx を San Jose と California に割り当てることはできません。

図 3 : デバイス グループ（Device Groups） は、デバイスがいくつかのグループに配置されている、ネストされたデバイスグループの一例を示しています。図を見るとわかるように、1 つのデバイスが複数のグループに存在できます。この例では、routerx が（[Department] グループ タイプの下の）[Finance] グループと、Location > United States > California > San Jose ネスト グループに属しています。これらの所属先のいずれかで routerx を選択した場合、単一のデバイスを設定していることになります（設定は、グループ化とは関連付けられていません）。

**図 *3*: デバイス グループ（*Device Groups*）**


Security Manager では、グループおよびグループ タイプを作成または削除できるほか、インターフェイス内のさまざまな場所でデバイスをグループに配置できます。

- デバイスをインベントリに追加するとき：New Device ウィザードには、[Device Grouping] ページが含まれています。ここでは、デバイス グループ タイプを作成し、新規に追加したデバイスのグループを選択できます。また、デフォルト グループを選択して、そこにすべての新規デバイスを追加することもできます。
- デバイス ビューでデバイス インベントリを表示したとき：[File] > [Edit Device Groups] コマンドを選択すると、ダイアログボックスが開き、グループおよびグループ タイプを作成

または削除できます。デバイス セレクタでグループまたはグループ タイプを選択した場合、[File] メニューと右クリックのショートカット メニューにはグループを追加するためのコマンドまたはデバイスをグループに追加するためのコマンドが表示されます。

グループにデバイスを追加したり、グループからデバイスを削除したりするには、グループを選択し、**[ファイル（File）] > [グループへのデバイスの追加（Add Devices to Group）]** を選択します。

- デバイスのプロパティを表示したとき：[Device Grouping] ページでは、デバイスが属するグループを選択し、インベントリに追加したデバイスのデフォルトを設定できます。これは、デバイス グループからデバイスを削除できる唯一の場所となります。デバイス セレクタでデバイスをダブルクリックして、デバイス プロパティを開きます。
- 管理ページを使用しているとき：**[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [デバイスグループ（Device Groups）]** を選択して、デバイスグループの管理ページを開きます。ここでは、グループおよびグループタイプを作成または削除できますが、グループにデバイスを追加することはできません。

### 関連項目

- デバイス グループ タイプの作成 （82 ページ）
- デバイス グループの作成 （83 ページ）
- デバイス グループまたはグループ タイプの削除 （83 ページ）
- デバイス グループに対するデバイスの追加と削除 （84 ページ）

## [Edit Device Groups] ダイアログボックス

[Edit Device Groups] ダイアログボックスは、デバイス インベントリに定義されているデバイス グループおよびグループ タイプを管理する場合に使用します。

### ナビゲーション パス

次のいずれかを実行します。

- デバイスセレクタでデバイスグループタイプまたはデバイスグループを右クリックし、[デバイスグループの編集（Edit Device Groups）] を選択します。
- **[ファイル（File）] > [デバイスグループの編集（Edit Device Groups）]** を選択します。
- New Device ウィザードの [デバイスのグループ化（Device Grouping）] ページで、または既存のデバイスの場合はデバイスのプロパティで、グループタイプリストから [グループの編集（Edit Groups）] を選択します。 [Device Groups] ページ （63 ページ） を参照してください。

### 関連項目

- デバイスのグループ化について （79 ページ）
- デバイス グループの使用 （79 ページ）

### フィールド リファレンス

**表 *13 : [Edit Device Groups]* ダイアログボックス**

| 要素 | 説明 |
|---|---|
| Groups | デバイス グループとグループ タイプを表示します。<br>グループ名またはタイプ名を変更するには、グループまたはタイプを選択し、もう一度クリックしてテキストを編集可能にします。新しい名前を入力し、Enter を押します。 |
| [Add Type] ボタン | 新しいグループ タイプを作成するには、このボタンをクリックします。タイプはデフォルト名で追加されます。名前を上書き入力し、Enter を押します。<br>最大 10 個のグループ タイプを設定できます。 |
| [Add Group to Type] ボタン | デバイス グループを選択したデバイス グループまたはグループ タイプに追加するには、このボタンをクリックします。 |
| [Delete] ボタン（ゴミ箱） | 選択したデバイス グループまたはグループ タイプとその中に含まれているすべてのデバイス グループを削除するには、このボタンをクリックします。デバイス グループまたはグループ タイプを削除しても、その中に含まれているデバイスは削除されません。 |

# デバイス グループ タイプの作成

この手順では、デバイス グループ タイプを作成する最も直接的な方法について説明します。グループ タイプを追加する他の方法の詳細については、デバイスのグループ化について （79 ページ）を参照してください。

デバイス グループ タイプは、デバイス グループ階層の最上位にあるカテゴリです。デバイス グループを追加する場合は、デバイス グループ タイプの作成 （82 ページ）を参照してください。

### 関連項目

- デバイスのグループ化について （79 ページ）
- デバイス グループまたはグループ タイプの削除 （83 ページ）
- デバイス グループに対するデバイスの追加と削除 （84 ページ）

**ステップ 1** [ファイル（File）] > [デバイスグループの編集（Edit Device Groups）] を選択します。

[Edit Device Groups] ページが開きます（[Edit Device Groups] ダイアログボックス （81 ページ）を参照）。

**ステップ 2** [タイプの追加（Add Type）] をクリックします。新規デバイス グループ タイプ エントリがセレクタに追加されます。

**ステップ 3** グループタイプの名前を入力し、[入力（Enter）] を押します。

**ステップ 4** [OK] をクリックして、[デバイスグループの編集（Edit Device Groups）] ページを閉じます。

# デバイス グループの作成

この手順では、デバイス グループを作成する最も直接的な方法について説明します。グループを追加する他の方法の詳細については、デバイスのグループ化について （79 ページ）を参照してください。

デバイス グループはデバイス グループ階層の下位のカテゴリであり、デバイス グループ タイプ（最上位）内または別のデバイス グループ内に追加されます。デバイス タイプ グループを追加する場合は、デバイス グループ タイプの作成 （82 ページ）を参照してください。

**関連項目**

- デバイスのグループ化について （79 ページ）
- デバイス グループに対するデバイスの追加と削除 （84 ページ）
- デバイス グループまたはグループ タイプの削除 （83 ページ）

**ステップ 1** デバイスセレクタでデバイスグループまたはグループタイプを選択し、[ファイル（File）]>[新規デバイスグループ（New Device Group）] を選択するか、または右クリックして [新規デバイスグループ（New Device Group）] を選択します。

[Add Group] ダイアログボックスが表示されます。

**ステップ 2** デバイスグループの名前を入力し、[OK] をクリックします。新規デバイス グループがデバイス セレクタに追加されます。

# デバイス グループまたはグループ タイプの削除

不要になったデバイス グループまたはグループ タイプは削除できます。ただし、グループ タイプの中で All グループだけは削除できません。

グループまたはグループ タイプを削除すると、そのグループに含まれるグループが削除されます。ただし、デバイスは削除されません。グループに存在するデバイスはインベントリに残っ

ており、所属先の他のグループに存在していることを確認できます（All グループにはすべてのデバイスがあります）。

デバイス グループおよびグループ タイプを削除するには、さまざまな方法があります。この手順では、最も直接的な方法について説明します。他の方法の詳細については、デバイスのグループ化について （79 ページ）を参照してください。

**ステップ 1** [デバイス（Device）] ビューで、[ファイル（File）] > [デバイスグループの編集（Edit Device Groups）] を選択します。[Edit Device Groups] ページが開きます（[Edit Device Groups] ダイアログボックス （81 ページ）を参照）。

**ステップ 2** 削除するグループタイプまたはグループを選択し、[削除（Delete）] ボタンをクリックします。削除の確認が求められます。

# デバイス グループに対するデバイスの追加と削除

デバイス グループにデバイスを追加するには、そのグループを作成する必要があります。グループを作成するには、デバイス グループの作成 （83 ページ）を参照してください。

**関連項目**

- デバイスのグループ化について （79 ページ）
- セレクタ内の項目のフィルタリング

**ステップ 1** デバイスセレクタでデバイスグループを選択し、右クリックし、[グループへのデバイスの追加（Add Devices to Group）] を選択します。[Add Devices to Group] ダイアログボックスが表示されます。

**ステップ 2** デバイスをグループに追加するには、使用可能なデバイスセレクタでデバイスを選択し、[>>] をクリックして [選択されたデバイス（Selected Devices）] リストに移動します。

デバイスを削除するには、[選択されたデバイス（Selected Devices）] リストでデバイスを選択して、[<<] をクリックします。

**ステップ 3** [OK] をクリックデバイス グループ メンバーシップが、[Selected Devices] リストに表示されていたデバイスを含めるように調整されます。

# [デバイスステータスビュー（Device Status View）] の使用

[デバイスステータスビュー（Device Status View）] を使用して、Cisco Security Manager インベントリ内のデバイスのステータスを迅速に確認できます。[デバイスステータスビュー（Device Status View）] ウィンドウには、Cisco Security Manager 内の複数のアプリケーションおよびツー

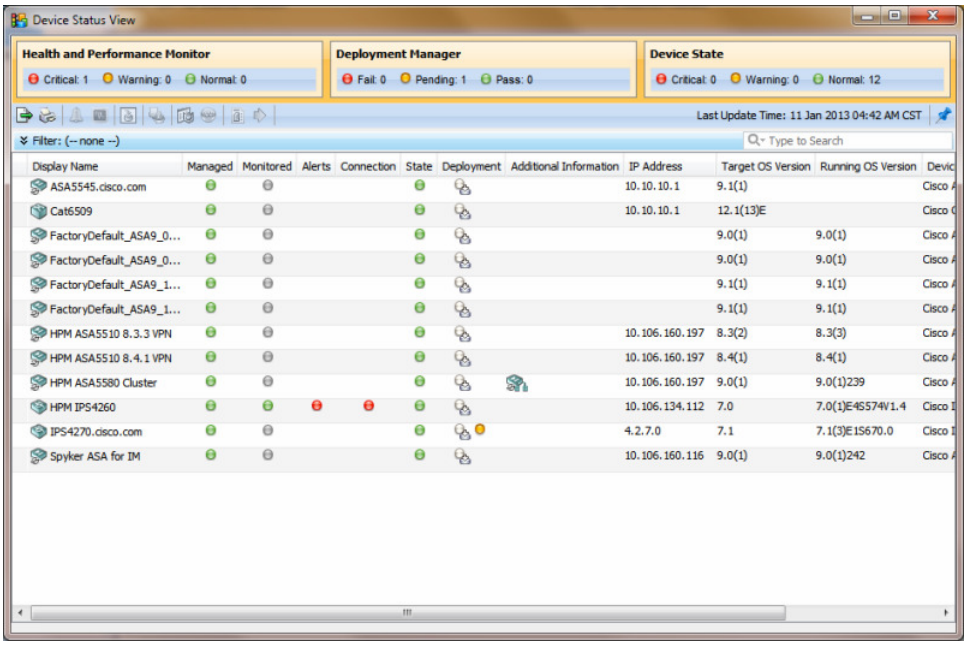
ルからの情報が集約されています。[デバイスステータスビュー（Device Status View）] を使用して、すべてのデバイスまたは特定のデバイスグループのステータスを迅速に確認し、その情報に基づいて操作する必要がある Cisco Security Manager の領域に簡単に移動できます。

**注意** 場合によっては、特定のデバイスについて、Health and Performance Monitor に[クリティカル（Critical）] デバイスステータスが表示され、Configuration Manager に [正常（Normal）] デバイスステータスが表示されることがあります。サービスまたはサーバーを再起動しても、この不一致は解消されません。このため、Configuration Manager に加えて HPM でデバイスのステータスを監視する必要があります。

### ナビゲーション パス

- [表示（View）] > [デバイスステータスビュー（Device Status View）] を選択します。[デバイスステータスビュー（Device Status View）] ウィンドウが開き、すべてのデバイスの情報が表示されます。
- デバイスセレクタでデバイスグループを選択します。[デバイスステータスビュー（Device Status View）] ウィンドウが開き、そのデバイスグループまたはサブグループの一部であるデバイスの情報が表示されます。

**図 *4 : デバイスステータスビュー（Device Status View）***



## フィールド リファレンス

表 *14* : デバイスステータスビュー（*Device Status View*）

| 要素 | 説明 |
|---|---|
| [デバイスステータス（Device Status）] の概要ボックス<br>[デバイスステータス（Device Status）] の概要ボックスには、[デバイスステータスビュー（Device Status View）] におけるデバイスの全体的なステータスの概要が表示されます。概要ボックスに表示される数には、現在選択されているデバイスグループ内のデバイスのステータスが反映されています。[表示（View）]>[デバイスステータスビュー（Device Status View）] を選択するか、[すべて（All）] のデバイスグループを選択すると、概要ボックスにすべてのデバイスの数が反映されます。<br>（注） [デバイスステータスビュー（Device Status View）] ウィンドウでデバイスリストをフィルタリングしても、[デバイスステータス（Device Status）] の概要ボックスのカウントには影響しません。 | |
| [Health and Performance Monitor] 概要ボックス | [クリティカル（Critical）]（赤）、[警告（Warning）]（黄）、および [正常（Normal）]（緑）のアラートステータスのデバイス数を示します。 |
| Deployment Manager の概要ボックス | [失敗（Fail）]（赤）、[保留中（Pending）]（黄）、および [成功（Pass）]（緑）の展開ステータスのデバイス数を示します。 |
| デバイス状態の概要ボックス | [クリティカル（Critical）]（赤）、[警告（Warning）]（黄）、および [正常（Normal）]（緑）のデバイス状態のデバイス数を示します。 |
| [デバイスステータスビュー（Device Status View）] ツールバー<br>[デバイスステータスビュー（Device Status View）] ツールバーには、次のボタンがあります。<br>（注） 以下のオプションはすべて、デバイスの右クリックメニューからも選択できます。 | |
|  | デバイスのステータス情報を PDF ファイルにエクスポートできます。 |
|  | デバイスのステータス情報を印刷できます。 |
|  | Health and Performance Monitor アプリケーションで選択したデバイスのアラートステータス情報を表示します。<br>詳細については、ヘルスとパフォーマンスのモニタリングを参照してください。 |

| 要素 | 説明 |
|---|---|
|  | Health and Performance Monitor アプリケーションで選択したデバイスのモニタリング情報を表示します。<br>詳細については、ヘルスとパフォーマンスのモニタリングを参照してください。 |
|  | Deployment Manager を開きます。<br>詳細については、展開の管理を参照してください。 |
|  | 選択したデバイスの Image Manager アプリケーションを開きます。<br>詳細については、Image Manager の使用を参照してください。 |
|  | 選択されているデバイスのデバイスマネージャを開きます。<br>詳細については、デバイス マネージャの起動を参照してください。 |
|  | 選択したデバイスの Cisco Prime Security Manager（PRSM）アプリケーションを起動します。詳細については、Cisco Prime Cisco Security Manager または FireSIGHT Management Center の起動を参照してください。 |
|  | 選択したデバイスの [デバイスのプロパティ（Device Properties）] ダイアログボックスを開きます。詳細については、デバイス プロパティの表示または変更 （51 ページ）を参照してください。 |
|  | [デバイスステータスビュー（Device Status View）] ウィンドウから選択したデバイスに移動できます。詳細については、デバイス ビューについて （1 ページ）を参照してください。 |
|  | 現在のページのオンライン ヘルプを開きます。<br>詳細については、オンライン ヘルプの利用方法を参照してください。 |
|  | [デバイスステータスビュー（Device Status View）] ウィンドウを切り離すと、ウィンドウを開いた状態で他の製品機能を使用できます。 |
|  | [デバイスステータスビュー（Device Status View）] ウィンドウをドッキングします。<br>（注） デバイスセレクタで選択が変更されている場合、[デバイスステータスビュー（Device Status View）] ウィンドウがドッキングされているときに、現在の選択が作業領域に反映されます。 |

| 要素 | 説明 |
|---|---|
| **テーブルフィルタ**<br>[デバイスステータスビュー（Device Status View）] テーブルに表示されるデバイスのリストをフィルタ処理して、特定の条件を満たす項目を検索できます。詳細については、テーブルのフィルタリングを参照してください。 | |
| [デバイスステータス（Device Status）] テーブル | |
| 表示名 | デバイスの表示名。これは、Cisco Security Manager デバイスセレクタでの表示に使用される名前であり、デバイスのホスト名と必ずしも同じではありません。 |
| 管理対象 | Security Manager でデバイスを管理するかどうかを指定します。 |
| 監視対象 | デバイスが Health and Performance Monitor によって監視されているかどうかを示します。 |
| Alerts | デバイスの現在のアラートレベル（[正常（Normal）]（緑）、[警告（Warning）]（黄）、または[クリティカル（Critical）]（赤））を示します。アラートインジケータにカーソルを合わせると、詳細を表示できます。 |
| Connection | HPM がデバイスに接続可能またはデバイスをポーリング可能かどうかを示します（[接続済み（Connected）]、[認証エラー（Authentication Error）]、[証明書の不一致エラー（Certificate Mismatch Error）]、[接続エラー（Connection error）]、[読み取り操作中のタイムアウト（Timeout during Read operation）]、または[サービスが利用できません（Service unavailable）]）。アラートインジケータにカーソルを合わせると、詳細を表示できます。<br>（注） デバイスが HPM（[ツール（Tools）] > [デバイスセレクタ（Device Selector）]）で通常または優先監視対象デバイスとして選択されていない場合、このステータスは適用されません。監視対象デバイスの選択に対する変更が有効になり、画面に反映されるまで数分かかる場合があります。 |

| 要素 | 説明 |
|---|---|
| 状態 | デバイスの現在の状態を示します。アラートインジケータにカーソルを合わせると、詳細を表示できます。<br><br>Health and Performance Monitor によって監視されている ASA デバイスの場合、アウトオブバンド変更の可能性が検出されると、[状態（State）] 列にもアラートが表示されます。Health and Performance Monitor でデバイスを監視する前に発生したアウトオブバンド変更は、[状態（State）] 列に反映されません。アウトオブバンド変更の詳細については、アウトオブバンド変更の処理方法についておよびアウトオブバンド変更の検出および分析を参照してください。 |
| 展開 | デバイスの展開方法と現在の展開ステータスを示します。展開ステータスは、[失敗（Fail）]（赤）、[保留中（Pending）]（黄）、および[成功（Pass）]（緑）です。アラートインジケータにカーソルを合わせると、詳細を表示できます。 |
| その他の情報 | デバイスの追加情報（デバイスがクラスタモードかどうかなど）を表示します。アラートインジケータにカーソルを合わせると、詳細を表示できます。 |
| IPアドレス | デバイスの管理 IP アドレス。192.168.3.8 など。 |
| Hostname.Domain | デバイスの DNS ホスト名とドメイン名。 |
| ターゲット OS バージョン | デバイスの設定の基となる OS バージョン。 |
| 実行中 OS のバージョン | デバイスで実行されているオペレーティングシステムのバージョン。 |
| デバイスタイプ | デバイスのタイプ。 |

## 関連項目

- ヘルスとパフォーマンスのモニタリング
- Image Manager の使用
- 展開の管理

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。