ポリシーの管理

ここでは、Cisco Security Manager におけるポリシーの概念およびポリシーの使用方法や管理方法について説明します。

ポリシーについて

Security Manager におけるポリシーとは、ネットワークの特定の設定項目を定義した一連のルールまたはパラメータのことです。ネットワークを設定するには、デバイス（個々のデバイス、サービス モジュール、セキュリティ コンテキスト、仮想センサーなど）のポリシーおよび複数のデバイスで構成される VPN トポロジを定義し、これらのポリシーで定義された設定をこれらのデバイスに展開します。

特定のソリューションを設定するためにさまざまなタイプのポリシーが必要になる場合があります。たとえば、サイト間 VPN を設定するには、IPsec、IKE、GRE などの複数のポリシーを設定することが必要になる場合があります。

ポリシーは、1 つ以上のデバイスに割り当てられます。ポリシーがデバイスに割り当てられたあとでポリシー定義を変更すると、デバイスの動作が変わります。

ここでは、ポリシーについて詳しく説明します。

- ポリシーのロックについて （9 ページ）
- ルータおよびファイアウォール デバイスのポリシー管理のカスタマイズ （13 ページ）

設定ベースのポリシーとルールベースのポリシー

Security Manager のポリシーは、ルールベースまたは設定ベースのポリシーとして構造化されます。

ルールベースのポリシー

ルールベースのポリシーには、選択されたデバイス上のトラフィックの処理方法を制御する 1 つ以上のルールが含まれます。たとえば、ファイアウォール サービスの一部として定義されたアクセス ルールやインスペクション ルールなどがあります。ルールベースのポリシーには、テーブルに配置された数百または数千のルールを含めることができ、それぞれのルールで同じパラメータ セットに異なる値を定義できます。トラフィック フローには、定義がフローと一致する最初のルール（最初の一致と呼ばれる）が割り当てられるため、ルールの順序は非常に重要です。

ルール テーブルの構造は、ローカル ポリシーまたは共有ポリシー（ローカルポリシーと共有ポリシー （3 ページ）を参照）のどちらを設定するかによって異なります。単一デバイスにルールベースのローカル ポリシーを設定した場合、ポリシーにはローカル ルールのフラットなテーブルが含まれます。デバイス ビューまたはポリシー ビューでルールベースの共有ポリシーを設定した場合、テーブルは [Mandatory] セクションと [Default] セクションの 2 つに分割されます。必須ルールは、常にデフォルト ルールよりも優先され、ローカル ルールやデフォルト ルールで上書きできません。[Default] セクションには、必須ルールやローカル ルールで上書きできるルールが含まれます。ルールを [Mandatory] セクションまたは [Default] セクションで定義したり、カットアンドペーストを使用して2つのセクション間でルールを移動したりできます。

ファイアウォール サービス ポリシーなどの特定タイプのルールベースのポリシーを定義する場合は、ポリシーを階層化することができます。この階層では、下位レベルのルールは上位レベルのルールからプロパティを取得します。これはルールの継承と呼ばれます。たとえば、すべてのファイアウォールにグローバルに適用される一連のインスペクション ルールを定義し、デバイスのサブセットに適用できる追加ルールでこれらのルールを補足できます。親ポリシーで共通のルールを保持すると、継承によって、展開失敗の原因となる設定エラーの発生を抑えることができます。詳細については、 ルールの継承について （5 ページ）を参照してください。

設定ベースのポリシー

設定ベースのポリシーには、セキュリティまたはデバイス動作の側面を定義した一連の関連パラメータが含まれます。たとえば、Cisco IOS ルータを設定する場合、Quality of Service（QoS）ポリシーを定義して、ポリシーに含めるインターフェイス、QoS を適用するトラフィックのタイプ、およびトラフィックのキューイング方法やシェーピング方法を定義できます。同じパラメータ セットの値を含む数百のルールを格納できるルールベースのポリシーとは異なり、デバイスに定義される各設定ベースのポリシーには1つのパラメータ セットしか定義できません。

関連項目

- ポリシーについて （1 ページ）

サービスポリシーとプラットフォーム固有のポリシー

Security Manager のポリシーは、いくつかのドメインに分割され、各ドメインは主なポリシー カテゴリを表します。これらのドメインは、サービス ポリシーおよびプラットフォーム固有のポリシーという 2 つのカテゴリに分類できます。

サービス ポリシーは、次のポリシー ドメインに分割されます。

- ファイアウォール
- サイト間 VPN
- リモート アクセス VPN
- IPS サービス ポリシー

たとえば、ファイアウォール ポリシー ドメインには、アクセル ルール、インスペクション 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。サイト間 VPN ポリシー ドメインには、IKE プロポーザル、IPsec プロポーザル、事前共有キーなどのポリシーが含まれます。サービス ポリシーは、プラットフォームにかかわらず任意の種類のデバイスに適用できますが、ポリシー定義はデバイス タイプによって異なる場合があります。

プラットフォーム固有のポリシー 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。すべてのプラットフォーム固有のポリシーがセキュリティに直接関連付けられるわけではありません。たとえば、ルータ ポリシー ドメインには、ルーティング ポリシー、アイデンティティ ポリシー（ネットワーク アドミッション コントロールおよび 802.1x）、デバイス管理に関連するポリシー（DHCP、SNMP、デバイス アクセス）、および QoS や NAT などのその他のポリシーが含まれます。

ルータおよびファイアウォール（ASA、PIX、FWSM）の場合は、管理するプラットフォーム固有のポリシーを選択できます。詳細については、ルータおよびファイアウォール デバイスのポリシー管理のカスタマイズ （13 ページ）を参照してください。

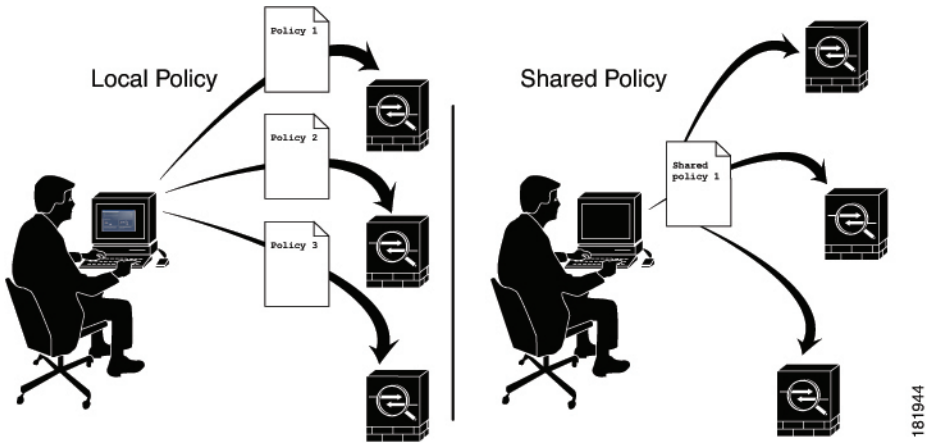
ローカルポリシーと共有ポリシー

デバイスには、ローカル ポリシーまたは共有ポリシーを設定できます。ローカル ポリシーとは、単一デバイスに定義されるポリシーのことです。ローカル ポリシーに加えた変更は、そのデバイスだけに反映されます。ローカル ポリシーは、小規模ネットワークや標準以外の設定を必要とするデバイスに適しています。たとえば、ネットワーク内の他のルータで使用されるポリシーとは異なる OSPF ルーティング ポリシーを必要とするルータにローカル ポリシーを設定します。ローカル ポリシーに対して実行できるアクションの詳細については、基本的なポリシー管理の実行 （39 ページ）を参照してください。

デバイスごとにローカル ポリシーを保持している場合は、ネットワークが拡大するにつれ、ポリシーを包括的かつ効率的に管理するために必要な作業が増加します。この問題に対処するた

めに、Security Managerにはポリシー共有という機能が用意されています。ポリシー共有では、1 つのポリシーを作成し、そのポリシーを複数のデバイスに割り当てることができます。詳細については、ローカル ポリシーの共有 （53 ページ）を参照してください。

図 *1:* ローカルポリシーと共有ポリシー



たとえば、ネットワーク内のすべてのCisco IOSルータで同じNetwork Admission Control（NAC; ネットワーク アドミッション コントロール）ポリシーを実装する場合は、1 つの NAC ポリシーだけを定義し、そのポリシーを共有します。その後、1 つのアクションでネットワーク内のすべてのルータに共有ポリシーを割り当てることができます。詳細については、デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシー割り当ての変更 （63 ページ）を参照してください。

共有ポリシーに加えた変更は、そのポリシーが割り当てられているすべてのデバイスに自動的に適用されます。このため、共有ポリシーを使用すると、ポリシー作成プロセスを合理化して、デバイス設定の一貫性や同一性を保持することができます。

共有ポリシーに対して実行できるアクションの詳細については、デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用 （47 ページ）を参照してください。

ヒント

- 共有ポリシーをグループ化して、ポリシーバンドルを形成できます。ポリシーバンドルを使用すると、特に多数のデバイスを操作する場合に、共有ポリシーの割り当てを簡単に管理できます。詳細については、ポリシーバンドルの管理 （72 ページ）を参照してください。
- ポリシーの共有以外に、同じタイプの別のポリシーを定義するときに、ルールベースのポリシーのルールを継承することもできます。これにより、たとえば、すべてのファイアウォール デバイスに適用される一連の企業アクセス ルールを保持しながら、必要に応じて個々のデバイスに追加ルールを定義するという柔軟性が得られます。詳細については、ルールの継承について （5 ページ）を参照してください。
- 複数の Security Manager サーバーを使用する場合、プライマリサーバーから定期的に共有ポリシーをエクスポートし、他のサーバーにインポートすることで、サーバー間で一貫性のあるポリシーセットを維持できます。公式のポリシー ソースとして使用するサーバを決

定する必要があります。詳細については、共有ポリシーのエクスポートおよび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。

- バージョン 4.7 では、Cisco Security Manager に、デバイスフィルタで使用可能なフィルタリングの選択肢に新しいオプションが追加されました。この新しいオプションは、共有ポリシーが適用されているデバイスのフィルタを提供します。Security Manager GUI でこれを表示するには、[ドロップダウンリスト内（in the dropdown list）] で、[表示（View）] > [デバイス表示（Device View）]>[フィルタ：（Filter:）]>[フィルタの作成（Create Filter）]... に移動します。[フィルタの作成（Create Filter）] ダイアログボックスが表示されたら、ドロップダウンリストを使用して、「Device,」「has,」「Shared Policy,」を選択すると、結果として「Device has 'Shared Policy」フィルタが設定されます。

共有ポリシーと VPN

共有ポリシーを使用すると、デバイス設定の場合と同様に、VPN の設定も簡単に行うことができます。たとえば、共有 IPsec プロポーザル ポリシーを作成し、そのポリシーを複数のサイト間 VPN に割り当てることができます。共有ポリシーに加えた変更は、そのポリシーが割り当てられているすべての VPN に反映されます。

共有ポリシーは、Site-to-Site VPN Manager を使用して、既存の VPN に割り当てることができます。そのためには、共有可能なポリシーを右クリックし、[共有ポリシーの割り当て（Assign Shared Policy）] を選択します。これは、デバイス ビューで共有ポリシーを割り当てる方法とほぼ同じです。VPN デフォルト ポリシーについて、および VPN デフォルト ポリシーの設定で説明しているように、共有ポリシーを Create VPN ウィザードで使用するデフォルト ポリシーとして設定することもできます。

関連項目

- ポリシーについて （1 ページ）

ルールの継承について

ローカルポリシーと共有ポリシー （3 ページ）で説明しているように、共有ポリシーを使用すると、共通のポリシー定義を設定して複数のデバイスに割り当てることができます。ルールの継承では、この機能がさらに拡張されており、共有ポリシーに定義されているルールをデバイスに含めるだけでなく、そのデバイスに固有のローカルルールを含めることもできます。Security Manager では、継承を使用することにより、階層の下位レベルのポリシー（子ポリシーと呼ばれる）が、上位レベルで定義されているポリシー（親ポリシーと呼ばれる）のルールを継承するという階層構造を適用できます。

（注） ポリシーバンドルに他の共有ポリシーから継承する共有ポリシーが含まれている場合、継承されたルールは、ポリシーバンドルが適用されるすべてのデバイスにも適用されます。

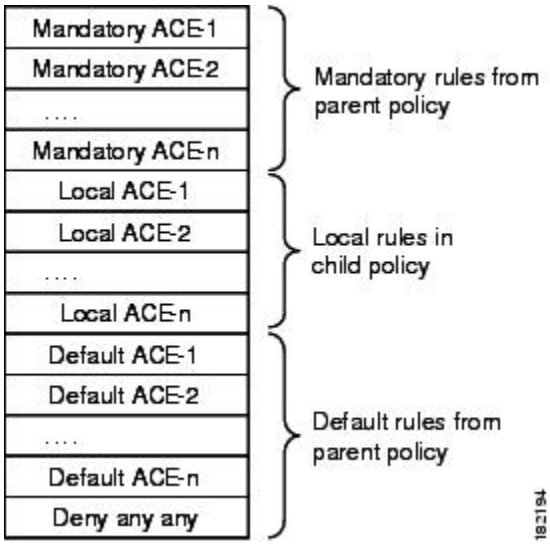
継承使用時のルールの順序

アクセス ルールについてで説明しているように、アクセス コントロール リスト（ACL）は、テーブルに配置されたルール（アクセス コントロール エントリ（ACE）とも呼ばれる）で構成されます。着信パケットは、ACL内の最初のルールと照合されます。パケットは、そのルールと一致する場合、ルールに従って許可または拒否されます。一致しない場合、パケットは、一致するルールが見つかって実行されるまでテーブル内の次のルールと照合されます。

この最初の一致方式では、テーブル内のルールの順序が非常に重要になります。共有アクセス ルール ポリシーを作成すると、Security Manager はルール テーブルを複数のセクション（[Mandatory] と [Default]）に分割します。[Mandatory] セクションには、子ポリシーで定義されているローカル ルールによって上書きできないルールが含まれます。[デフォルト（Default）] セクションには、ローカル ルールでオーバーライドできるルールが含まれます。

次の図に、継承使用時のルールテーブルにおけるルールの順序付けを示します。

図 *2:* 継承使用時のルール順序



継承を使用する利点

ルールベースのポリシーを階層構造で定義すると、ルールセットを定義するときの柔軟性が大幅に向上します。また、階層レベルを必要な数だけ増やすことができます。たとえば、ブランチ オフィスにあるデバイスのアクセス ルール ポリシーを定義します。このポリシーは、地域レベルのアクセスを決定する親ポリシーからルールを継承します。一方、この親ポリシーは、企業レベルでルールを設定する階層最上位のグローバル アクセス ルール ポリシーからルールを継承します。

この例では、ルールは次のようにルール テーブルで順序付けられています。

```
Mandatory corporate access rules
    Mandatory regional access rules
        Local rules on branch device
    Default regional access rules
Default corporate access rules
```

ブランチ デバイスに対して定義されているポリシーは、地域ポリシーの子であり、企業ポリシーの孫です。このように継承を構造化すると、すべてのデバイスに適用されるが、階層下位レベルのルールによって上書きされない、企業レベルの必須ルールを定義できます。同時に、ルールの継承により、必要に応じて特定のデバイスのローカル ルールを柔軟に追加できます。

デフォルトルールを使用すると、ルールテーブルで上位に表示される必須ルールとデフォルトルールにギャップがある場合に、「deny any any」などのグローバルデフォルトルールを定義できます。グローバルデフォルトルールは、すべてのアクセスルールリストの最後に表示され、最終的なセキュリティ手段となります。

継承の例

たとえば、企業アクセス ルール ポリシーに必須のワーム軽減ルールを定義して、1 つのエントリですべてのデバイスに対するワームを軽減またはブロックできます。地域アクセス ルール ポリシーが設定されたデバイスは、ワーム軽減ルールを企業ポリシーから継承し、一方で地域レベルに適用されるルールを追加できます。たとえば、特定の地域のすべてのデバイスには FTP トラフィックを許可するが、他のすべての地域のデバイスにはFTPをブロックするというルールを作成できます。ただし、企業レベルの必須ルールは、常にアクセス ルール リストの最上位に表示されます。子ポリシーで定義した必須ルールは、親ポリシーで定義された必須ルールのあとに配置されます。

デフォルト ルールでは、順序は逆になります。つまり、子ポリシーで定義されたデフォルト ルールは、親ポリシーから継承されたデフォルト ルールの前に表示されます。デフォルト ルールはデバイスに定義されたローカル ルールのあとに表示されるため、デフォルト ルールを上書きするローカル ルールを定義できます。たとえば、特定の地域のデフォルト ルールで、ある宛先リストに対する FTP トラフィックが拒否されている場合、この宛先のうちの 1 つには FTP を許可するローカル ルールを定義できます。

IPS ポリシーの継承

IPS デバイスのイベント アクション フィルタ ポリシーでは、継承を使用して、親ポリシーに定義されたルールを特定のデバイスに定義されたローカル ルールに追加することもできます。唯一の違いは、アクティブ ルールと非アクティブ ルールは Security Manager インターフェイスに表示されますが、すべての非アクティブ ルールは継承されたデフォルト ルールのあとで最後に展開される点です。

IPS デバイスのシグニチャ ポリシーでは、シグニチャごとに適用できる別の継承タイプが使用されます。シグニチャの設定 を参照してください。

関連項目

- 設定ベースのポリシーとルールベースのポリシー　(2 ページ)
- アクセス ルールについて
- グローバル アクセス ルールについて
- 継承と割り当て　(8 ページ)
- ルールの継承または継承の解除　(60 ページ)

継承と割り当て

ルールの継承とポリシーの割り当ての違いを理解しておくことが重要です。

- 継承：選択したポリシーからルールを継承した場合、デバイスにすでに設定されているローカル ルールは上書きされません。代わりに、継承されたルールがローカルルールに追加されます。継承されたルールが必須ルールの場合、ローカル ルールの前に追加されます。継承されたルールがデフォルトルールの場合、ローカルルールのあとに追加されます。継承されたルールに対して親ポリシー内で変更を加えると、このルールを継承するポリシーにも反映されます。

（注） IPS シグニチャ ポリシーとシグニチャ イベント アクションでは、継承の動作は異なります。詳細については、シグニチャ継承についてを参照してください。

- 割り当て：共有ポリシーをデバイスに割り当てると、デバイスにすでに設定されているポリシーは、選択したポリシーに置き換わります。これは、デバイスにローカルポリシーまたは別の共有ポリシーがすでに設定されていたかどうかにかかわらず、あてはまります。

したがって、アクセス ルールなどのルールベースのポリシーを使用する場合は、これらのオプションを慎重に選択する必要があります。継承は、デバイス上のローカル ルールを、親ポリシーからの追加ルールで補足する場合に使用します。割り当ては、デバイス上のポリシーを、選択した共有ポリシーに置き換える場合に使用します。

ヒント ローカル ルールを誤って上書きしないように、Security Manager では、ルールベースのポリシーに対して [Assigned Shared Policy] オプションを選択するときに警告メッセージが表示されます。このメッセージには、ポリシーを割り当てる代わりにポリシーのルールを継承するオプションがあります。ローカル ルールを保持する場合は、継承オプションを選択します。

関連項目

- ルールの継承について （5 ページ）
- ルールの継承または継承の解除 （60 ページ）
- ローカルポリシーと共有ポリシー （3 ページ）
- 設定ベースのポリシーとルールベースのポリシー （2 ページ）

ポリシー管理とオブジェクト

オブジェクトを使用すると、必要なときにいつでも適用できる論理的な覚えやすい名前を一連の値に付けることによって、Security Manager で簡単にポリシーを設定できます。たとえば、

ネットワークの一連の IP アドレスが含まれる、MyNetwork というネットワーク/ホスト オブジェクトを定義できます。このアドレスを必要とするポリシーを設定するときは、MyNetwork オブジェクトを参照するだけで済むため、毎回手動でアドレスを入力する必要がありません。

ポリシーを定義するときに、値としてオブジェクトを受け入れるフィールドの横にある [選択（Select）]ボタンをクリックして、すぐにオブジェクトを作成できます。詳細については、ポリシーのオブジェクトの選択を参照してください。Policy Object Managerで、システム全体のオブジェクトを作成したり管理したりすることもできます。

すでにデバイスに存在するポリシーが検出された場合にも、ポリシー オブジェクトが作成されます。 ポリシーの検出 （15 ページ）で説明しているように、デバイスを Security Manager インベントリに追加するときにポリシーを検出したり、インベントリにすでに存在するデバイス上のポリシーを検出したりできます。新しく検出されたポリシーに対して、すでに定義されているポリシー オブジェクトを再利用するように Security Manager を設定できます。検出用のポリシー オブジェクト設定の詳細については、[Discovery] ページを参照してください。

特定のタイプのオブジェクトを使用すると、定義済みの値をデバイス レベルで上書きできるため、ポリシーでオブジェクトを使用しながら、特定の値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。

オブジェクトの詳細およびポリシーの定義時にオブジェクトを使用する方法の詳細については、ポリシー オブジェクトの管理を参照してください。

関連項目

- ポリシーについて （1 ページ）

ポリシーのロックについて

Security Manager には、ポリシーのロック メカニズムがあります。これは、複数のユーザが設定を変更する権限を持つ組織で役立ちます。複数のユーザが同じデバイス、ポリシー、ポリシーの割り当て、またはオブジェクトを同時に変更する可能性がある状況を回避できます。ロックを適用すると、そのデバイスまたはポリシーにアクセスする他のユーザに対して、作業領域の上部にメッセージが表示されます。

ヒント ユーザが特定のアクションを実行すると、Security Manager はポリシー ロックよりも適用範囲が広いアクティビティ（または設定セッション）ロックを取得します。詳細については、アクティビティとロッキングを参照してください。

ロック タイプ

Security Manager は、次の 2 つの異なるロック タイプを使用します。

- ポリシー コンテンツ ロック：特定のポリシーのコンテンツをロックします。作業領域の上に表示されるバナーは次のようになります。

This data for this policy is locked by activity/user: <name>.

コンテンツ ロックにより、他のユーザはロックされたポリシーの設定を変更できなくなります。

- 割り当てロック：特定のデバイスに対するポリシータイプの割り当てをロックします。作業領域の上に表示されるバナーは次のようになります。

The assignment of this policy is locked by activity/user: <name>.

ローカルポリシーの場合は、割り当てロックが適用されると、他のユーザはポリシーの割り当てを解除したり、ローカルポリシーの代わりに同じタイプの共有ポリシーを割り当てたりすることができなくなります。共有ポリシーの場合は、割り当てロックが適用されると、他のユーザはすでに割り当てられているポリシーの代わりに同じタイプの別の共有ポリシーを割り当てることができなくなります。

これらのロックは、ユーザによって実行されるアクションに応じて、連携して機能するか、相互に独立して機能します。両方のロックが同時にアクティブになった場合、作業領域の上に表示されるバナーは次のようになります。

This policy is locked by activity/user: <name>.

実行可能なアクションに対するロックの効果の概要については、ロックとポリシーについて（11 ページ）を参照してください。

ロックの解除

ロックをイネーブルにすると、変更を送信するか（Workflow 以外のモードでの作業時）またはアクティビティを送信および承認する（Workflow モードでの作業時）までロックは解除されません。アクティビティを廃棄すると、そのアクティビティによって生成されたロックも廃棄されます。ワークフローモードの詳細については、ワークフローおよびアクティビティの概要を参照してください。

次の点を考慮してください。

- ロックは、デバイスの IP アドレスではなくデバイス名に基づきます。そのため、Security Manager では、IP アドレスが同じで名前が異なる 2 つのデバイスを定義しないことを推奨します。特に同時に両方のデバイスに展開しようとすると、予期しない結果が発生します。
- ロックは異なる操作にまたがって適用されることはありません。たとえば、あるユーザが、別のユーザによって検出されたデバイスと同じデバイスに対して展開することをロックで防ぐことはできません。

ロックの詳細については、次の項を参照してください。

- ロックとポリシーについて （11 ページ）
- ロックと VPN トポロジについて （12 ページ）
- ロックとオブジェクトについて （12 ページ）

ロックとポリシーについて

次のテーブルに、Security Manager におけるポリシーロックの効果の概要を示します。

（注） ポリシーやポリシーの割り当てを変更できるかどうかは、ユーザに割り当てられているユーザ権限によって決まります。『Installation Guide for Cisco Security Manager』を参照してください。

表 *1:* ロックの概要

別のユーザまたはアクティビティによる処理	不可能な操作	可能な操作
ポリシー定義を変更する。	• ポリシーを変更したり、他のデバイスに割り当てたりする。 • ポリシーの割り当てを解除する（ローカル ポリシーの場合）。	デバイスからポリシーの割り当てを解除する（共有ポリシーの場合）。
子孫を持つルールベースのポリシーの定義を変更する。	• 親ポリシーまたはその子孫のいずれかを変更する。 • 親ポリシーまたはその子孫のいずれかを追加デバイスに割り当てる。 • 親ポリシーまたはその子孫のいずれかのルール継承を変更する。	デバイスからポリシーの割り当てを解除する。
ポリシーの割り当てを、その定義を変更しないで変更する。	ポリシーを変更する。 （注） ポリシー ビューでは、コンテンツ ロックはポリシーに適用されます。デバイス ビューでは、割り当てロックは割り当てが他のユーザによって変更されるデバイスに適用されます。	ポリシーを割り当てたり、他のデバイスからポリシーの割り当てを解除したりする。
ポリシー定義を変更し、その割り当てを変更する。	ポリシーを変更したり、他のデバイスに割り当てたりする。	デバイスからポリシーの割り当てを解除する。

関連項目

- ポリシーのロックについて （9 ページ）
- ポリシーについて （1 ページ）

ロックと VPN トポロジについて

VPN トポロジのデバイス割り当てを変更したり、特定の VPN ポリシーを変更したりする場合、ロックは VPN トポロジ全体、およびポリシーが共有される他のトポロジに適用されます。つまり、他のユーザはデバイス割り当てを変更したり、VPN トポロジに定義されている VPN ポリシーを変更したりすることはできません。

サイト間 VPN ポリシーを表示したり変更したりするには、VPN トポロジ内の各デバイスに対する権限が必要です。また、デバイスを VPN トポロジに追加するための権限も必要です。VPN トポロジ内のデバイスに対して異なるレベルの権限を持っている場合は、最低の権限レベルがトポロジ全体に適用されます。たとえば、ハブアンドスポーク トポロジ内のスポークに対する読み取り/書き込み権限があり、ハブとして機能するデバイスに対する読み取り専用権限がある場合、ハブアンドスポーク トポロジ内のポリシーとデバイスに対する読み取り専用権限が与えられます。権限の詳細については、『Installation Guide for Cisco Security Manager』を参照してください。

（注） VPN トポロジからデバイスの割り当てを解除すると、VPN トポロジ内にデバイス ロックが作成されます。つまり、これらのデバイスはインベントリから削除できません。影響を受けるすべてのデバイス（削除するデバイスなど）に設定を展開するまでは、他のユーザはトポロジのデバイス割り当てを編集できません。デバイスは、設定が展開されるまで実際にはトポロジから削除されません。

関連項目

- ポリシーのロックについて （9 ページ）
- サイト間 VPN の管理：基本

ロックとオブジェクトについて

再利用可能なオブジェクトを作成または変更すると、そのオブジェクトはロックされ、他のユーザは同じオブジェクトを変更または削除できなくなります。オブジェクトのロックに関するその他のルールは次のとおりです。

- オブジェクトのロックによって、そのオブジェクトを使用するポリシーの定義や割り当てを変更できなくなることはありません。
- ポリシーに適用されたロックによって、そのポリシー定義に含まれているオブジェクトを変更できなくなることはありません。
- オブジェクトの定義は、権限を持たないデバイスに割り当てられたポリシーの一部である場合でも、変更できます。
- オブジェクトが他のオブジェクト（ネットワーク/ホスト オブジェクト、AAA サーバ グループ オブジェクトなど）を利用する場合、オブジェクトのロックによって、別のユーザがそれらの他のオブジェクトを変更できなくなることはありません。たとえば、AAA サーバ グループ オブジェクトを変更する場合、そのオブジェクトのロックによって、AAA

サーバ グループを構成する AAA サーバを別のユーザが変更できなくなることはありません。

オブジェクトがロックされると、そのオブジェクトを変更しようとするユーザには、関連するダイアログボックスの読み取り専用バージョンが表示されます。Workflow モードで作業している場合、メッセージにオブジェクトをロックしているアクティビティが示されます。

関連項目

- ポリシーのロックについて （9 ページ）
- ポリシー オブジェクトの管理

ルータおよびファイアウォールデバイスのポリシー管理のカスタマイズ

Cisco IOS ルータまたはASA、PIX、FWSM ファイアウォールデバイスを管理する場合、Security Manager で管理するポリシー タイプや管理対象外にするポリシー タイプを選択できます。ポリシー タイプの管理とは、Security Manager がポリシーの設定を管理し、データベースに格納するそのポリシーの情報を必要な設定であると認識することを意味します。Security Manager では、管理対象外のポリシータイプを設定したり、他の方法で設定されたこれらのタイプの設定を追跡したりはしません。たとえば、SNMP ポリシーを管理しない場合、CLI コマンドを使用して設定した SNMP 設定は Security Manager に認識されません。

注意 AUS または CNS を使用して設定を ASA または PIX デバイスに展開する場合は、デバイスが AUS または CNS から完全な設定をダウンロードする点に注意してください。そのため、Security Manager で管理されているポリシーを減らすと、実際にはデバイスから設定が削除されます。管理対象の一部の ASA/PIX ポリシーを選択解除し、Security Manager とともに他のアプリケーションを使用してデバイスを設定する場合は、AUS または CNS を使用しないでください。

ルータおよびファイアウォールにおけるポリシー管理をカスタマイズして、たとえば Security Manager を使用して DHCP および NAT ポリシーを管理し、一方で EIGRP や RIP などのルーティング プロトコル ポリシーを管理対象外のままにすることができます。これらの設定は、管理権限を持つユーザだけが変更でき、すべての Security Manager ユーザに影響します。

管理対象外のポリシーは、デバイス ビューとポリシー ビューの両方から削除されます。そのタイプの既存のポリシー（ローカルまたは共有）は、Security Manager データベースから削除されます。

ルータとファイアウォールのポリシー管理をカスタマイズするには、**[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [ポリシー管理（Policy Management）]**を選択して[Policy Management] ページを開きます。ポリシー タイプはフォルダに整理され、ルータとファイアウォール（すべての ASA、PIX、および FWSM デバイスを含む）は別々に処理されます。必要に応じてポリシータイプを選択または選択解除し、[保存

（Save）] をクリックします。その後の処理は、ポリシー タイプを管理対象にするか管理対象外にするかによって異なります。

- [ポリシータイプを管理対象外にする（Unmanaging a policy type）]：ポリシータイプを管理対象外にするときに、そのタイプのいずれかのデバイスにそのポリシーが設定されている場合は、管理対象外にする前にポリシーの割り当てを解除する必要があります。Security Manager によって、そのタイプのポリシーが割り当てられているすべてのデバイスのリスト（ポリシー名、デバイス名、およびポリシーをロックしているユーザまたはアクティビティを含む）が表示されます。[はい（Yes）] をクリックしてポリシーを管理対象外にすると、Security Manager は必要なロックを取得し、ポリシーの割り当てを解除してポリシータイプを管理対象外にします。

1 つでもデバイスのロックを取得できなかった場合、ポリシーの割り当ては解除されず、ポリシータイプは管理対象外になりません。この場合、問題が通知されます。その後、影響を受けるデバイスから手動でポリシーの割り当てを解除するか、ユーザまたはアクティビティのロックを解除し、ポリシー タイプを管理対象外にする操作を再試行できます。

（注） ポリシーを管理対象外にしても、デバイスで実行されているアクティブな設定に影響はありません。つまり、Security Manager はデバイスから設定を削除しません。代わりに、ポリシーがデータベースから削除され、Security Manager ではデバイス設定のその部分が考慮されなくなります。

- [以前に管理対象外にしたポリシータイプを管理する（Managing a previously-unmanaged policy type）]：以前に Security Manager で管理しなかったポリシータイプの管理を開始する場合は、デバイス上のアクティブな設定に、新たに管理対象にしたポリシータイプによって制御されるコマンドが含まれている可能性があります。**したがって、そのタイプのすべてのデバイス（すべてのルータまたはすべての ASA、PIX、FWSM デバイス）上のポリシーを再検出することが重要です**。これにより、Security Manager はこれらのポリシーに関する現在の設定を保持できます。

ポリシーを再検出せず、新たに管理対象にしたポリシーを未設定のままにすると、デバイスへの次の展開時に、デバイスに定義されている既存の設定が削除されます。すでに管理対象になっているデバイス上のポリシーの検出については、Security Manager にすでに存在するデバイス上のポリシーの検出 （19 ページ）を参照してください。

（注） Security Manager によって管理対象外にされた機能は、CLI コマンドまたは FlexConfig を使用して手動で変更できます。FlexConfig の詳細については、FlexConfig の管理を参照してください。

ポリシーの検出

ポリシー検出を使用すると、既存のネットワーク設定を Security Manager に取り込んで管理できます。ポリシー検出は、動作中のデバイスの設定をインポートするか、または設定ファイルをインポートすることによって実行できます。構成ファイルをインポートする場合、ファイルはデバイスで（たとえば、Cisco IOS ソフトウェアデバイスで **show run** コマンドを使用して）生成されている必要があります。他の形式の構成ファイルは検出できません。

ポリシー検出は、New Device ウィザードで関連するオプションを選択してデバイスを追加するときに開始できます。詳細については、デバイスインベントリへのデバイスの追加を参照してください。

デバイス ビューから既存のデバイスのポリシー検出を開始することもできます。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 （19 ページ）を参照してください。

デバイスのポリシー検出を開始すると、そのデバイス上の設定が分析され、デバイスを管理できるように Security Manager ポリシーおよびポリシー オブジェクトに変換されます。インポートした設定によって一部のポリシーだけが定義される場合、警告が表示されます。追加の設定が必要な場合は、Security Manager インターフェイスの関連するページに移動して、ポリシー定義を完了する必要があります。インポートした設定が無効な場合も、警告とエラーが表示されます。

ポリシー検出の実行後、変更を送信して（または、Workflow モードで作業している場合はアクティビティを承認して）、情報を変更レポートに含め、情報を他のユーザが使用できるようにする必要があります。検出されたポリシーを変更した場合は、変更を有効にするためにデバイスに展開する必要があります。詳細については、展開の管理を参照してください。

ヒント　すべてのデバイスに適用される検出関連の設定を行うには、[Security Manager Administration] ウィンドウを使用します。詳細については、[Discovery] ページを参照してください。

ポリシー検出と VPN

Security Manager では、個々のデバイスに対して検出を実行する以外に、ネットワークにすでに展開されている VPN を検出できます。VPN の検出方法は、検出対象の VPN のタイプによって異なります。

- サイト間 VPN：ウィザードに従って検出手順を実行します。詳細については、サイト間 VPN ディスカバリを参照してください。

ヒント　サイト間VPNの検出後すぐにファイルに展開することを推奨します。これにより、Security Manager はデバイスで設定されている、関連する CLI コマンドを完全に管理できます。

- IPSec および SSL リモート アクセス VPN：デバイスをインベントリに追加する場合、またはインベントリにすでに存在するデバイスのポリシーを検出する場合は、デバイスのポリシーを検出するときに IPSec および SSL VPN を検出できます。これらの VPN に関連するポリシーは、通常のデバイス ポリシーとして扱われます。ただし、検出オプションを選択するときに、RA VPN ポリシーを検出するように選択する必要があります。リモート アクセス VPN ポリシー検出の詳細については、リモート アクセス VPN ポリシーの検出を参照してください。ポリシー検出の実行の詳細については、デバイス インベントリへのデバイスの追加および Security Manager にすでに存在するデバイス上のポリシーの検出 （19 ページ）を参照してください。

（注） 設定ファイルを使用してデバイスを追加し、デバイスの追加中にセキュリティ ポリシーを検出する場合、Security Manager では、検出対象のデバイスからファイルをダウンロードする必要があるポリシーを正常に検出できません。これは、特に SSL VPN 設定に **svc image** コマンドを含むデバイスに影響します。Security Manager のデータベースには参照先ファイルはないため、検出された設定に対して **no** 形式のコマンドが生成されます。

ポリシー検出および Cisco IOS ルータと Catalyst デバイス

Security Manager では、Cisco IOS ソフトウェアで使用可能なすべてのコマンドのサブセットがサポートされ、そのほとんどはセキュリティ関連のコマンドです。サポートされているすべての Cisco IOS コマンドを検出できます。サポートされていないコマンドは、Security Manager で設定されているポリシーと直接競合しないかぎり、そのまま残されます。Cisco IOS ルータに対するポリシー検出の実行の詳細については、ルータ ポリシーの検出を参照してください。Catalyst デバイスに対するポリシー検出の実行の詳細については、Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータにおけるポリシーの検出を参照してください。

ヒント Cisco IOS ルータまたは Catalyst デバイスの検出後すぐにファイルに展開することを推奨します。これにより、Security Manager はデバイスで設定されている、関連する CLI コマンドを完全に管理できます。

ポリシー検出およびファイアウォール セキュリティ コンテンツ

セキュリティ コンテキストを含むデバイスを追加する場合、すべてのコンテキストとポリシーを同時に検出する必要があります。それ以外の場合、各コンテキストのポリシーを別々に検出する必要があります。デバイスを追加するときに、コンテキストとして [MULTI] を選択します。[管理対象外デバイスのセキュリティコンテキスト（Security Context of Unmanaged Device）] は選択しません（このオプションを選択すると、管理コンテキストだけがインポートされますが、管理コンテキストにはデバイス上の他のセキュリティコンテキストとの関連性がありません。このオプションは、セキュリティコンテキストを親デバイスとは無関係に管理する場合に選択してください）。デバイスの追加方法によっては、セキュリティコンテキストを検出するオプションを選択しなければならない場合があります。検出中、Security Manager はセキュリティコンテキスト名を親の名前の末尾に付加して、各セキュリティコンテキストを識別し、個別のデバイスとしてデバイスリストに追加します。たとえば、親が pix_141 の場合、管理コン

テキストはpix_141_adminとなります（セキュリティ コンテキストの命名ルールを制御できます。詳細については、[Discovery] ページを参照してください）。新しいセキュリティ コンテキストを作成したり、既存のコンテキストを削除したりする以外に、それらのコンテキストのポリシーを作成または削除することもできます。

Catalyst 6500デバイスに含まれるFWSMの複数のセキュリティ コンテキストを作成し、シャーシでIOS ソフトウェアを実行する場合は、シャーシのSSH クレデンシャルを使用してシャーシ デバイスを追加します。その後、Security Managerはシャーシの各FWSMを識別し、それぞれを追加するためのオプションを表示できます。FWSMの検出中、Security ManagerはFWSMや各コンテキストのポリシーなど、各FWSMのセキュリティ コンテキストを検出します。ただし、デバイスでCatalyst OSを使用する場合は、各FWSMを個別に検出する必要があります。

デバイスをインベントリに追加する方法の詳細については、デバイスインベントリへのデバイスの追加を参照してください。

ポリシー検出およびIPSデバイス

IPSデバイスのポリシーを検出すると、そのデバイスに定義されている仮想センサーが、その仮想センサーに定義されているポリシーとともに検出されます。複数の仮想センサーで同じポリシーが使用される場合、そのポリシーは共有ポリシーとして作成され、仮想センサーに割り当てられます。1つの仮想センサーに定義されたポリシーまたは親デバイスだけに定義されたポリシーは、ローカルポリシーとして作成されます。個々の仮想センサーだけのポリシーは検出できません。検出できるのは、親デバイス上のポリシーだけです。仮想センサーに割り当てられていない親デバイス上のポリシーが検出された場合、それらのポリシーはデバイスまたは仮想センサーに割り当てられない共有ポリシーとして作成されます。

仮想センサーを含むIPSデバイスの検出後、仮想センサーをデバイス セレクタに表示するには、変更をデータベースに送信する必要があります。

ポリシー検出とオブジェクトグループ

ポリシー検出を実行すると、PIX、ASA、FWSM、およびIOS 12.4(20)T+デバイスにすでに設定されているオブジェクト グループは、ポリシー オブジェクトとしてSecurity Managerに取り込まれます。Security Managerのポリシー オブジェクトがオブジェクト グループに変換される方法およびその逆の方法の詳細については、ポリシー オブジェクトがオブジェクト グループとしてプロビジョニングされる方法を参照してください。

さらに、ASA 8.3+デバイス上の[オブジェクトネットワーク（Object Network）]設定と[オブジェクトサービス（Object Service）]設定は、ホスト、ネットワーク、またはアドレス範囲ネットワーク/ホストオブジェクトあるいは（サービス グループ オブジェクトではなく）サービス オブジェクトとしてSecurity Managerに取り込まれます。唯一の例外として、範囲の開始と終了に同じアドレスを持つアドレス範囲オブジェクトは、代わりにホスト ネットワーク/ホスト オブジェクトとして作成されます。

（注） IOSデバイスの場合、ACLオブジェクトとして検出されたアクセス コントロール リストで使用されている検出済みオブジェクトは、その後の展開時にオブジェクトのコンテンツによって置き換えられます。ACLオブジェクトで使用されるオブジェクト グループは保持されませんが、Security Managerポリシー オブジェクトとして検出されます。

ポリシー検出および Security Manager ポリシー オブジェクト

ポリシー検出を実行すると、Security Manager は Security Manager ですでに作成されているポリシーオブジェクトを再利用しようとします。デバイス設定のコンテンツに基づいて、次のアクションが実行される可能性があります。

- 設定内の名前付きポリシー オブジェクト：既存のポリシー オブジェクトのコンテンツがデバイス上の設定と一致する場合は、そのオブジェクトが再利用されます。

  名前付きポリシーオブジェクトのコンテンツが一致しない場合は、ポリシーオブジェクトが再利用され、[検出（Discovery）] 管理ページで [検出されたポリシーオブジェクトのデバイスオーバーライドを許可（Allow Device Override for Discovered Policy Objects）] が選択されていれば、デバイスレベルのオーバーライドが作成されます。詳細については、次の項を参照してください。

  - 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
  - [Discovery] ページ

- 設定内の名前のないポリシー オブジェクト：既存のポリシー オブジェクトのコンテンツがデバイス上の設定と一致する場合は、そのオブジェクトが使用されます。この動作は、[検出（Discovery）] 管理ページの [ポリシーオブジェクトをインライン値に再利用する（Reuse Policy Objects for Inline Values）] 設定の値を変更することによって制御できます。
- 冗長なオブジェクトを検出するために定義した設定にかかわらず、既存のオブジェクトと同じ定義を持つオブジェクトを検出できます。この設定の詳細については、[Policy Objects] ページを参照してください。

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。

ポリシー検出およびアクセス制御リスト

Security Manager のポリシーには、標準 ACL だけをサポートするもの、または拡張 ACL だけをサポートするものがあります。これは、CLI で両方のタイプがサポートされている場合でも同様です。このような場合、ポリシー検出は次のように機能します。

- Security Manager のポリシーで拡張 ACL だけがサポートされる場合（たとえば、ファイアウォール サービス ポリシー）、そのポリシー用にデバイスで設定されている標準 ACL は、拡張 ACL としてインポートされます。
- Security Manager のポリシーで標準 ACL だけがサポートされる場合（たとえば、IOS ルータ上の SNMP トラップ）、そのポリシー用にデバイスで設定されている拡張 ACL は、標準 ACL としてインポートされます。

検出プロセス中、Security Manager には、インポートされた非アクティブな ACL は無効な状態で表示されます。あとでこれらの無効な ACL を展開すると、ACL はデバイス設定から削除されます。

関連項目

- ポリシー検出に関する FAQ （34 ページ）

• ポリシー検出タスクのステータスの表示 （28 ページ）
• 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

Security Manager にすでに存在するデバイス上のポリシーの検出

インベントリにデバイスを追加する場合、デバイスの追加と同時にポリシーを検出できます。ただし、ポリシー検出をスキップしてあとで実行したり、デバイスの追加後にポリシーを再検出したりすることもできます。

既存のデバイスに対してポリシー検出を開始できるのは、次のような場合です。

- device upgrade などの CLI コマンドを使用してデバイス設定を変更します。このような場合、Security Manager データベースに最新の情報が格納されるように、デバイス上の既存のポリシーを再検出できます。再検出を実行するよりも Security Manager でアウトオブバンド変更を入力することを推奨します。ただし、バージョン4.13以降では、単一の検出アクションですべてのポリシーが適切に検出されます（ASA 8.x から 9.x へのアップグレードに適用可能）。
- Security Managerに最初にデバイスを追加するときに検出されなかったポリシーのサブセット（プラットフォーム固有の設定など）を検出する場合。
- ファイアウォールデバイスの出荷時のデフォルト設定をインポートする場合。詳細については、ファイアウォールのデフォルト設定を参照してください。

注意 Security Manager でポリシーを設定した後に、変更を展開するまでにデバイスに対してポリシー検出を実行すると、検出されたポリシーによって、未展開の変更が上書きされます。たとえば、プラットフォーム固有の設定を検出するオプションを選択した場合、検出された設定によって、Security Manager で設定したプラットフォーム固有の未展開のポリシーが上書きされます。検出された設定に、設定した固有のプラットフォームポリシーが含まれていない場合でも、上書きされます。たとえば、プラットフォーム固有の設定を検出すると、検出された設定にルーティング情報が含まれていない場合でも、Security Manager でこのデバイス用に設定したルーティング ポリシーが上書きされます。また、再検出の結果、デバイスに設定された共有ポリシーが検出されたローカル ポリシーに置き換えられる場合もあります。

⚠

注意 特定の条件下では、Security Manager がシステムコンテキストで ASA インターフェイスを検出できない場合があります。具体的には、「インベントリ」をチェック（選択）せずにマルチコンテキスト ASA のシステム コンテキストで再検出/展開が行われた場合、Security Manager は他のセキュリティコンテキストのインターフェイスを検出できない可能性があります。これにより、その後の展開で Security Manager が他のコンテキストのインターフェイス設定を変更するか、完全に削除する可能性があります。この問題を回避するには、システムコンテキストの再検出を行うときに、必ず「インベントリ」を選択してください。

はじめる前に

デバイスにポリシーを設定しているユーザやデバイスに設定を展開しているユーザがいないことを確認します。展開ジョブによってデバイスに設定が展開されている間にデバイスのポリシーを再検出すると、再検出後に、展開された変更が表示されないことがあります。ポリシーを再検出する前に、Deployment Manager を使用して、該当デバイスを含むアクティブなジョブがないかどうかを確認してください（**[管理（Manage）] > [展開（Deployments）]** を選択）。展開ジョブ中に間違ってポリシーを再検出した場合は、展開ジョブが完了するまで待ってから再度ポリシーを検出して、Security Manager がデバイスと同期されるようにします。

関連項目

- ポリシー検出タスクのステータスの表示 （28 ページ）
- ポリシーの検出 （15 ページ）
- ポリシー検出に関する FAQ （34 ページ）
- ポリシーについて （1 ページ）
- デバイス ビューおよび Site-to-Site VPN Manager におけるポリシーの管理 （38 ページ）
- ポリシー ビューにおける共有ポリシーの管理 （64 ページ）

ステップ 1 単一デバイス上のポリシーを検出するかどうか、または一度に複数のデバイス上のポリシーを検出するかどうかを決定します。ポリシー検出オプションは、検出プロセスの開始方法によって異なります。

- **単一デバイスの検出**：次のいずれかに関連するポリシーを検出する必要がある場合は、単一デバイスの検出だけを使用してポリシーを検出できます（単一デバイスの検出は、インベントリにデバイスを追加するときに実行される検出タイプです）。
  - マルチコンテキストモードで実行されている ASA、PIX、および FWSM デバイスのセキュリティコンテキスト設定
  - IPS デバイスの仮想センサー設定
  - Catalyst デバイスのサービス モジュール情報
  - 設定ファイルからのポリシー検出

- 出荷時のデフォルト設定からのポリシー検出

- **バルク再検出**：複数のデバイスのポリシーを検出する必要がある場合は、バルク再検出を実行できます。ただし、バルク再検出は、動作中のデバイス（つまり、ネットワークで現在稼働し、アクセス可能なデバイス）に対してだけ実行できます。セキュリティ コンテキスト、仮想センサー、またはCatalyst サービス モジュール設定は検出できません（サービス モジュールを含むデバイスを選択するのではなく、サービス モジュールを直接選択した場合は、サービス モジュールを検出できます）。

ステップ 2 **単一デバイスの検出を実行する場合は**、次の手順を実行します。

a) デバイスビューまたはマップビューで、1 つのデバイスだけが選択されていることを確認し、右クリックして [デバイスでポリシーを検出（Discover Policies on Device）] を選択します。[Create Discovery Task] ダイアログボックスが開きます。

ヒント：[バルク再検出（Bulk Rediscovery）] ダイアログボックスが表示された場合は、ダイアログボックスを閉じて再試行する必要があります。1 つのデバイスだけが選択されていることを確認し、コマンドを再発行します。右クリック メニューを使用する必要があります。これが単一デバイスの検出を実行する唯一の方法です。

b) 必要に応じて検出タスク名を変更し、次の検出オプションを選択します。詳細については、[Create Discovery Task] および [Bulk Rediscovery] ダイアログボックス （23 ページ）を参照してください。

- [検出元（Discover From）]：動作中のデバイス（ネットワークでアクティブであり、アクセス可能なデバイス）から検出するか、設定ファイルから検出するか（[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）、または出荷時のデフォルト設定（出荷時のデフォルト設定が存在する OS バージョンを実行している ASA、PIX、および FWSM デバイス）から検出するかを指定します。シングルコンテキスト モードで実行されているデバイスまたは個々のセキュリティ コンテキストだけのデフォルト設定を検出できます。

ヒント：PIX、ASA、および FWSM デバイスを手動で追加する場合は（手動定義によるデバイスの追加を参照）、[工場出荷時のデフォルト設定（Factory Default Configuration）] 設定を使用することを推奨します。シングルコンテキスト モードのデバイスおよびマルチ コンテキスト モードのデバイスの各セキュリティ コンテキストのデフォルト設定を検出する必要があります。出荷時のデフォルト ポリシーの詳細については、ファイアウォールのデフォルト設定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を検出（Discover Policies for Security Contexts）]：マルチコンテキストモードで実行されているファイアウォールデバイスに定義されているセキュリティコンテキストのポリシーを検出する場合は、このオプションを選択します。

c) 検出するポリシーのタイプを選択します。ポリシー タイプ間の相違の詳細については、サービスポリシーとプラットフォーム固有のポリシー （3 ページ）を参照してください。

- [ASA-CX/FirePOWERモジュールの検出（Detect ASA-CX/FirePOWER Module）]：CX モジュールまたは FirePOWER モジュールがインストールされているかどうかを確認します。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。

- [Inventory]：デバイスの基本情報（ホスト名、ドメイン名など）、インターフェイス、およびマルチコンテキスト モードで実行されているデバイス上のセキュリティ コンテキストを検出します。

Cisco IOS ルータでは、DSL、PPP、PVC ポリシーなどのすべてのインターフェイス関連ポリシーも検出されます。

- [Platform Settings]：ルーティング ポリシーなどのプラットフォーム固有のポリシーを検出します。
- [Firewall Services]：すべてのプラットフォーム上にある、アクセス ルールやインスペクション ルールなどのファイアウォール サービス ポリシーを検出します。
- [NATポリシー（NAT Policies）]：アドレスプール、スタティック変換ルール、ダイナミック NAT/PAT といったネットワークアドレス変換（NAT）ポリシーを検出します。NAT ポリシーの検出は、ASA、ASA-SM、PIX、および FWSM デバイスでサポートされています。
- [ルーティングポリシー（Routing Policies）]：ASA デバイスのルーティングポリシーを検出します。
- [SSL ポリシー（SSL Policy）]：ASA デバイスの SSL ポリシーを検出します。
- [RA VPNポリシー（RA VPN Policies）]：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 ポリシーを検出します。
- [IPS]：シグニチャや仮想センサーなどの IPS ポリシーを検出します。

詳細については、[Create Discovery Task] および [Bulk Rediscovery] ダイアログボックス （23 ページ）を参照してください。

d) [OK] をクリックします。検出タスクが開始され、[Discovery Status] ダイアログボックスが開くため、タスク ステータスを表示できます（[Discovery Status] ダイアログボックス （29 ページ）を参照）。検出の進行中は Security Manager で他のタスクを実行できません。

ステップ 3 **バルク再検出を実行する場合は**、次の手順を実行します。

a) デバイス ビューで、次のいずれかを実行します。

- デバイスグループまたは複数のデバイスを選択し、右クリックして [デバイスでポリシーを検出（Discover Policies on Device）] を選択します。[Bulk Rediscovery] ダイアログボックスが開くことを確認します。

ヒント：[ディスカバリタスクの作成（Create Discovery Task）] ダイアログボックスが表示された場合は、ダイアログボックスを閉じて再試行する必要があります。デバイス グループまたは複数のデバイスが選択されていることを確認し、コマンドを再発行します。

- **[ポリシー（Policy）] > [デバイスでポリシーを検出（Discover Policies on Device）]**を選択します。[Device Selector] ダイアログボックスが開きます。[使用可能なデバイス（Available Devices）] リストから検出するデバイスを選択し、[>>] 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。[次へ（Next）] をクリックします。

（注） 右クリック コマンドを使用する場合、Security Manager は目的のデバイスが選択されていると見なします。いつでも [戻る（Back）] ボタンをクリックして [デバイスセレクタ（Device Selector）] 画面に戻り、デバイスリストを変更できます。

b) 必要に応じて検出タスク名を変更し、検出オプションを選択します。詳細については、[Create Discovery Task] および [Bulk Rediscovery] ダイアログボックス （23 ページ）を参照してください。

デバイスはデバイス タイプに従ってグループにまとめられ、各タイプ内にデバイス グループ（ある場合）が表示されます。

- 特定のタイプのデバイスすべてに対するオプションを変更するには、デバイス タイプのフォルダを選択し、[Discover Device Settings] オプションを変更します。[Discover] ドロップダウン リストに [Multiple Values] が表示される場合は、そのタイプのデバイスに異なる検出オプションが選択されています。値を変更すると、その変更はすべてのデバイスに適用されます。前述の単一デバイスの検出で説明したポリシー タイプのチェックボックスは、[Policies and Inventory] を選択した場合だけ使用できます。選択したグループ内のすべてのデバイスに使用できるオプションだけが表示されます。そのため、最も適切なオプション セットを選択するには、個々のデバイスを別々に選択する必要があります。
- 単一デバイスのオプションを変更するには、デバイスが見つかるまでフォルダの横にある [+] アイコンをクリックして開き、デバイスを選択して検出オプションを選択します。

（注） オプションのリストが展開されていない場合、すべてのポリシー、すなわちプラットフォーム設定、ファイアウォールポリシー、NAT ポリシー、および RA VPN が検出されます。ただし、オプションのリストを展開すると、使用可能なリストから選択したオプションに基づいて検出が行われます。

c) [終了（Finish）] をクリックします。検出タスクが開始され、[Discovery Status] ダイアログボックスが開くため、タスク ステータスを表示できます（[Discovery Status] ダイアログボックス （29 ページ）を参照）。検出の進行中は Security Manager で他のタスクを実行できません。

[Create Discovery Task] および [Bulk Rediscovery] ダイアログボックス

デバイス インベントリにすでに存在するデバイスのポリシーを Security Manager で検出するには、[Create Discovery Task] ダイアログボックスを使用します。一度に複数のデバイスのポリシーを検出するには、[Bulk Rediscovery] ダイアログボックスを使用します。ポリシー検出のオプションは、使用するダイアログボックスによって異なります。これらの各ダイアログボックスを開く方法など、手順の詳細については、Security Manager にすでに存在するデバイス上のポリシーの検出 （19 ページ）を参照してください。

インベントリにデバイスを追加するときにポリシーを検出することもできます。デバイスの追加の詳細については、デバイス インベントリへのデバイスの追加を参照してください。

ナビゲーション パス

デバイス ビューで、デバイス セレクタからデバイスを選択し、次のいずれかを実行します。

- [ポリシー（Policy）] > [デバイスでポリシーを検出（Discover Policies on Device）] を選択して、バルク再検出を実行します。
- デバイスセレクタで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。単一デバイスを選択した場合は、[Create Discovery Task] ダイアログボックスが表示されます。それ以外の場合は、バルク再検出を実行します。

ヒント　マップビューで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）] を選択することもできます。

関連項目

- ポリシーの検出　（15 ページ）
- ポリシー検出タスクのステータスの表示　（28 ページ）
- 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
- [Discovery Status] ダイアログボックス　（29 ページ）

フィールド リファレンス

表 2 : [Create Discovery Task] ダイアログボックス

要素	説明
Discovery Task Name	検出タスクに割り当てられる名前。タスクの名前は、現在の日時に基づいて自動的に生成されますが、必要に応じてこの名前を変更できます。
[Selected Devices] テーブル （バルク再検出だけ）	再検出対象として選択したデバイス。デバイスはデバイス タイプに従ってグループにまとめられ、各タイプ内にデバイス グループ（ある場合）が表示されます。 • 特定のタイプのデバイスすべてに対するオプションを変更するには、デバイス タイプのフォルダを選択し、[Discover Device Settings] オプションを変更します。[Discover] ドロップダウン リストに [Multiple Values] が表示される場合は、そのタイプのデバイスに異なる検出オプションが選択されています。値を変更すると、その変更はすべてのデバイスに適用されます。前述の単一デバイスの検出で説明したポリシー タイプのチェックボックスは、[Policies and Inventory] を選択した場合だけ使用できます。選択したグループ内のすべてのデバイスに使用できるオプションだけが表示されます。そのため、最も適切なオプションセットを選択するには、個々のデバイスを別々に選択する必要があります。 • 単一デバイスのオプションを変更するには、デバイスが見つかるまでフォルダの横にある [+] アイコンをクリックして開き、デバイスを選択して検出オプションを選択します。 **ヒント**：再検出対象として選択したデバイスを変更するには、[戻る（Back）] をクリックして [デバイスセレクタ（Device Selector）] ダイアログボックスに移動します。

要素	説明
Discover From Config. ファイル（File） （バルク再検出には使用不可）	検出するポリシー情報のソース： • [Live Device]：デバイスから直接ポリシーを検出します。 • [Config File]：設定ファイルからポリシーを検出します。[設定ファイル（Config File）] フィールドにファイルの場所を指定します。[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。 デバイスで（たとえば、**show run** コマンドを使用して）生成された設定ファイルからだけポリシーを検出できます。詳細については、設定ファイルからのデバイスの追加を参照してください。 • [Factory Default Configuration]：ファイアウォール デバイスの出荷時のデフォルト設定を含むファイルを使用して、そのデバイスに対して検出を実行します。Security Manager によって、選択したデバイスに適切なファイル（[Config File] 編集ボックスに表示される）が自動的に選択されます。このオプションは、Security Manager に ASA、PIX、または FWSM デバイスで実行されている OS バージョンのデフォルト設定がある場合だけ使用できます。シングルコンテキスト モードで実行されているデバイスまたは個々のセキュリティ コンテキストだけのデフォルト設定を検出できます。詳細については、ファイアウォールのデフォルト設定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 （バルク再検出には使用不可）	マルチ コンテキスト モードで実行されているファイアウォール デバイスに設定されている各セキュリティ 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。このフィールドは、PIX、ASA、およびFWSMデバイスだけに適用されます。 選択を解除すると、Security Manager はデバイス全体をシングルコンテキスト モードで設定された単一のポリシー セットを持っているものとして処理します。 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。

要素	説明
Policies to Discover（単一デバイスの検出の場合） Discover Device Settings（バルク再検出の場合）	

要素	説明
	選択したデバイス上の検出するポリシー タイプ。 （注） バルク再検出の場合、[検出（Discover）] ドロップダウンメニューから [ポリシーとインベントリ（Policies and Inventory）] を選択し、[インベントリのみ（Inventory Only）]（他のポリシータイプを検出しないでインベントリを検出する場合）または [ASA-CX/FirePOWER モジュールの検出（Detect ASA-CX/FirePOWER Module）]（他のポリシーを検出せずに CX または FirePOWER モジュールがインストールされるかどうかを確認する場合）をオンにします。ドロップダウンリストで [複数の値（Multiple Values）] が選択されている場合は、選択したグループ内のデバイスで別の検出オプションが選択されています。選択を変更すると、変更はグループ内のすべてのデバイスに適用されます。 次の検出オプションがあります。 • [ASA-CX/FirePOWER モジュールの検出（Detect ASA-CX/FirePOWER Module）]：CX モジュールまたは FirePOWER モジュールがインストールされているかどうかを確認します。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。 • [Inventory]：ホスト名、ドメイン名などのデバイス情報、インターフェイス、およびマルチコンテキストモードで実行されているファイアウォール デバイスのセキュリティ コンテキストが含まれます。Cisco IOS ルータでは、DSL、PPP、PVC ポリシーなどのすべてのインターフェイス関連ポリシーも検出されます。 • [Platform Settings]：選択したデバイスに設定できるすべてのプラットフォーム固有のポリシーが含まれます。 • [Firewall Services]：すべてのファイアウォール サービス 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。 • [NAT ポリシー（NAT Policies）]：アドレスプール、スタティック変換ルール、ダイナミック NAT/PAT といった、選択したデバイスで設定されているすべてのネットワークアドレス変換（NAT）ポリシーが含まれます。NAT ポリシーの検出は、ASA、ASA-SM、PIX、および FWSM デバイスでサポートされています。詳細については、ネットワーク アドレス変換の設定を参照してください。 • [ルーティングポリシー（Routing Policies）]：ASA デバイスのルーティングポリシーを検出します。詳細については、ファイアウォール デバイスでのルーティング ポリシーの設定を参照してください。 • [SSL ポリシー（SSL Policy）]：ASA デバイスの SSL ポリシーを検出します。

要素	説明
	• [RA VPN Policies]：選択したデバイスに設定されているすべての IPSec および SSL リモート アクセス VPN ポリシーが含まれます。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。 • [IPS Policies]：選択したデバイスに設定されているすべての IPS ポリシーが含まれます。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。
	（注） • [ルーティングポリシー（Routing Policies）] オプションと [SSL ポリシー（SSL Policy）] オプションは、適応型セキュリティアプライアンス（ASA）デバイスにのみ適用されます。 • 検出するポリシーとして [プラットフォーム設定（Platform Settings）] を選択する場合、[プラットフォーム設定（Platform Settings）] のサブオプションである [ルーティングポリシー（Routing Policies）] と [SSL ポリシー（SSL Policy）] の選択は解除できません。 • ルーティングポリシーと SSL ポリシーのいずれかまたは両方を検出するには、[プラットフォーム設定（Platform Settings）] オプションの選択を解除し、[ルーティングポリシー（Routing Policies）] と [SSL ポリシー（SSL Policy）] のいずれかまたは両方を選択して、それらのポリシーのみを検出します。 • 非 ASA デバイスの場合、[ルーティングポリシー（Routing Policies）] オプションおよび [SSL ポリシー（SSL Policy）] オプションが表示される場合がありますが、常に選択できません。 • バルク再検出では、トランスペアレントモードおよびシステムコンテキストの場合、[ルーティングポリシー（Routing Policies）] オプションを選択できますが、検出は行われません。

ポリシー検出タスクのステータスの表示

ポリシー検出を開始すると、検出タスクが作成されます。検出対象のデバイスの数にかかわらず、ポリシー検出の開始ごとにタスクが 1 つだけ作成されます。

現在のポリシー検出タスクのステータスは、タスクの開始時に自動的に開く [Discovery Status] ダイアログボックスで確認できます。このダイアログボックスには、タスクに関する概要情報や検出対象の各デバイスに関する詳細など、検出タスクに関する更新されたステータス情報が表示されます。

必要に応じて検出タスクを中断できます。単一デバイスに対してポリシー検出を実行する場合、タスクを中断すると、検出は不完全になります。このような場合は、情報を削除し、検出を再度開始することを推奨します。複数のデバイスに対してポリシー検出を実行する場合、操作を中断する前に検出が完了したデバイスは完全に検出されます。検出が不完全なデバイスの情報は、Security Manager によって自動的に廃棄されます。

検出プロセス中に問題が発生した場合は、[Discovery Status] ダイアログボックスに該当する警告やエラー メッセージも表示されます。たとえば、設定ファイル内の CLI コマンドで完全な Security Manager ポリシーが定義されていない場合は、関連する Security Manager ポリシー ページでポリシー定義を完了する必要があることを示す警告メッセージが表示されます。

詳細については、[Discovery Status] ダイアログボックス （29 ページ）を参照してください。

以前の検出タスクに関する情報を表示するには、**[管理（Manage）] > [ポリシー検出ステータス（Policy Discovery Status）]** を選択して、[ポリシー検出ステータス（Policy Discovery Status）] ウィンドウを開きます。ウィンドウの上部のペインで検出タスクを選択すると、タスクの結果が下部のペインに表示されます。[Policy Discovery Status] ウィンドウの使用法の詳細については、[Policy Discovery Status] ページ （31 ページ）を参照してください。

関連項目

- Security Manager にすでに存在するデバイス上のポリシーの検出 （19 ページ）
- ポリシー検出に関する FAQ （34 ページ）
- ポリシーの検出 （15 ページ）

[Discovery Status] ダイアログボックス

[Discovery Status] ダイアログボックスでは、現在のポリシー検出タスクに関する詳細情報を表示します。このダイアログボックスには、タスクのステータスに関する一般情報および検出対象のデバイスによって生成された警告やエラーに関する詳細情報が表示されます。

[Discovery Status] ダイアログボックスは、既存のデバイスに対して検出タスクを開始するとき、およびネットワーク、設定ファイル、またはエクスポート ファイルからデバイスを追加するときに自動的に開きます。検出タスクの開始の詳細については、Security Manager にすでに存在するデバイス上のポリシーの検出 （19 ページ）を参照してください。

関連項目

- ポリシー検出タスクのステータスの表示 （28 ページ）
- ポリシーの検出 （15 ページ）
- ネットワークからのデバイスの追加
- ネットワークからのデバイスの追加
- インベントリ ファイルからのデバイスの追加

フィールド リファレンス

表 *3 : [Discovery Status]* ダイアログボックス

要素	説明
進行状況バー	現在のデバイスに対する検出タスクの何 % が完了したかを示します。
ステータス	検出タスクの現在の状態。
Devices to be discovered	このタスクで検出するデバイスの合計数。この数には、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が含まれます。
Devices discovered successfully	エラーが発生することなく検出されたデバイスの数。
Devices discovered with errors	検出中にエラーを生成したデバイスの数。

[Discovery Details] テーブル	検出対象のデバイス。デバイスを選択すると、概要リストの下にあるメッセージ リストに、そのデバイスの検出中に生成されたメッセージが表示されます。デバイス名以外にテーブルに含まれる情報は次のとおりです。
	• [Severity]：検出タスクの全体の重大度。たとえば、検出タスクが正常に完了した場合は、情報アイコンが表示されます。タスクが失敗した場合は、エラー アイコンが表示されます。
	• [State]：選択したデバイスにおけるポリシー検出タスクの現在の状態。
	  • [Device Added]：デバイスが Security Manager に追加されましたが、ポリシー検出はまだ開始されていません。
	  • [Discovery Started]：ポリシー検出が開始されました。
	  • [Reading and Parsing Device Config]：ポリシー検出タスクによってデバイス設定が解釈されています。
	  • [Importing Objects]：ポリシー検出タスクによって設定からオブジェクトがインポートされています。
	  • [Importing Policies]：ポリシー検出タスクによって設定からポリシーがインポートされています。
	  • [Discovery Complete]：ポリシー検出が正常に完了しました。
	  • [Discovery Failed]：ポリシー検出がエラーにより失敗しました。
	• [Discovered From]：ポリシー情報のソース。たとえば、設定ファイルからの検出時は、このフィールドにファイルの名前とパスが表示されます。

要素	説明
Messages list	選択したデバイスの検出中に生成されたメッセージ。メッセージを選択すると、リストの右側のフィールドに詳細情報が表示されます。
説明	[Message list] で選択されたメッセージに関する詳細情報。
操作	説明されている問題を解決するために実行する必要がある手順。
[Generate Report] ボタン	このジョブの検出ステータス レポートを作成するには、このボタンをクリックします。レポートは、ジョブの概要を含む PDF ファイルとして、クライアント システムに保存されます。ユーザはこのレポートを独自の目的で使用したり、Cisco TAC の問題のトラブルシューティングに使用したりできます。詳細については、展開ステータス レポートまたは検出ステータス レポートの生成を参照してください。
[Abort] ボタン	検出タスクを中断します。 単一デバイスに対するポリシー検出の実行時にタスクを中断すると、そのデバイスの検出は不完全になります。このような場合は、情報を削除し（たとえば、アクティビティを廃棄して）、検出を再度開始することを推奨します。 複数のデバイスに対するポリシー検出の実行時にタスクを中断すると、検出が不完全なデバイスの情報は自動的に廃棄されます。操作を中断する前に検出が完了したデバイスは完全に検出されます。

[Policy Discovery Status] ページ

[Policy Discovery Status] ページでは、以前のポリシー検出タスクやデバイス追加タスクのステータスを表示します。

ナビゲーション パス

[管理（Manage）] > [ポリシー検出ステータス（Policy Discovery Status）] を選択します。

関連項目

- ポリシー検出タスクのステータスの表示　（28 ページ）

フィールド リファレンス

表 *4 : [Policy Discovery Status]* ページ

要素	説明
[Task] テーブル ウィンドウの上部に、以前のポリシー検出タスクまたはデバイス追加タスクが表示されます。タスクを選択すると、ウィンドウの下部にそのタスクに関する詳細情報が表示されます。テーブルのカラムには、タスクの全体的なステータス情報が表示されます。 セキュリティ コンテキストを含むデバイスを追加すると、コンテキスト検出が個別のポリシー検出タスクとして表示されます。	
名前	検出タスクまたはデバイス追加タスクの名前。これは、システムによって生成された名前またはデバイス ポリシーの再検出時に指定した名前です。
タイプ（Type）	タスクのタイプ。[Policy Discovery]（デバイス ポリシーを再検出する場合）、または [Add Device]（New Device ウィザードを使用してデバイスを追加し、ポリシーの検出を選択した場合）。
開始時刻	タスクが開始された時刻。
終了時間（End Time）	タスクが終了した時刻。
ステータス	タスクの全体のステータス。次のいずれかです。 • [Completed successfully]：タスクは成功しました。 • [Completed with errors]：タスクは部分的に成功しました。一部のポリシーが検出されなかった場合、またはデバイスが追加されてポリシーが検出されなかった場合は、このステータスが表示されます。 • [Completed with warnings]：タスクは成功しましたが、軽微な問題が発生しました。 • [Failed]：タスクは失敗しました。エラーまたは検出の中断により、ポリシーが検出されなかったか、またはデバイスが追加されませんでした。

要素	説明
[Generate Report] ボタン	選択したジョブの検出ステータス レポートを作成するには、このボタンをクリックします。 レポートは、ジョブの概要を含む PDF ファイルとして、クライアント システムに保存されます。ユーザはこのレポートを独自の目的で使用したり、Cisco TAC の問題のトラブルシューティングに使用したりできます。詳細については、展開ステータス レポートまたは検出ステータス レポートの生成を参照してください。
[Refresh] ボタン	このボタンをクリックすると、タスク リストがリフレッシュされ、バックグラウンドで実行されているタスクがある場合、または新しいタスクが作成された場合に情報が更新されます。
[削除（Delete）] ボタン	このボタンをクリックすると、選択したタスクがデータベースから削除されます。古いタスクを削除しても、関連するデバイスや検出されたポリシーに影響しません。
[Discovery Details] または [Import Details] テーブル これらのテーブルには、選択したタスクに含まれるデバイスが表示されます。テーブル名は、タスクのタイプによって異なります（ポリシー検出タスクの場合は [Discovery Details]、デバイスの追加タスクの場合は [Import Details]）。 デバイスを選択すると、テーブルの下にあるメッセージ リストに、そのデバイスに対するタスクの実行中に生成されたメッセージが表示されます。	
デバイス	デバイスの名前。名前のあとに (deleted) が続く場合、デバイスは Security Manager インベントリに存在しません。
Config File （[Import Details] だけ）	設定ファイルの場所。このフィールドは、設定ファイルからインポートする場合だけ表示されます。
タスク タイプ（Task Type） （[Import Details] だけ）	次のいずれかです。 • [Import only]：デバイスを Security Manager に追加します。 • [Import and Discover]：デバイスを追加してポリシーとインベントリを検出するか、またはデバイスを追加してポリシーを検出します。
重大度	次のいずれかのアイコンが表示されます。 • エラー：デバイスの追加またはポリシー検出が失敗しました。 • 情報：デバイスが正常に追加されたか、またはポリシー検出が成功しました。

要素	説明
状態 詳細（Details）	これらのフィールドは、[Discovery Details] テーブルと [Import Details] テーブルで異なる名前が使用されますが、意味は同じです。デバイスに対するタスクのステータスが表示されます。 • [Device Added]：デバイスは正常にインベントリに追加されました。 • [Device Add Failed]：デバイスはインベントリに追加されませんでした。 • [Discovery Completed]：検出は成功し、検出されたポリシーが Security Manager データベースに追加されました。 • [Discovery Failed]：エラーが発生したため、ポリシーは検出されませんでした。
Discovered From （[Discovery Details] だけ）	次のいずれかです。 • [Live Device]：Security Manager は、デバイスに接続して設定とポリシー情報を取得しました。 • [File]：Security Manager は、設定ファイルから設定とポリシー情報を取得しました。
Messages list	選択したデバイスに対するタスクの実行中に生成されたメッセージ。メッセージを選択すると、リストの右側のフィールドに詳細情報が表示されます。重大度アイコンには、次の意味があります。 • エラー：問題が検出されました。 • 警告：検出中に軽微な問題が発生しました。 • 情報：選択したデバイスに関する情報メッセージ。
説明	[Message list] で選択されたメッセージに関する詳細情報。
操作	説明されている問題を解決するために実行する必要がある手順。

ポリシー検出に関する FAQ

次の質問と回答では、ポリシー検出によってデバイス設定を Security Manager ポリシーに取り込む方法について説明します。

質問：ポリシー検出はどのように動作しますか。

回答：ポリシー、設定、およびインターフェイス（インベントリ）を検出するデバイスを選択すると、Cisco Security Manager は動作中のデバイスから実行コンフィギュレーションを取得す

るか、または指定された設定（構成ファイルからの検出時）を取得し、CLI を Cisco Security Manager のポリシーとオブジェクトに変換します。インポートされた設定は、デバイスの初期設定として Configuration Archive に追加されます。検出後、検出されたポリシーとオブジェクトを確認したり、データベースにコミットするかどうかを決定したりできます。検出されたポリシーやオブジェクトが適切でない場合は、廃棄できます。コミットと廃棄は検出されたすべてのデバイス全体に影響し、デバイス単位で実行することはできません。

質問：どのようなときにポリシーを検出する必要がありますか。

回答：通常は、デバイスを Cisco Security Manager に追加するときにポリシーを検出します。ただし、動作中のデバイスまたは設定ファイルをインポートするのではなく、Security Manager でデバイスを作成する場合は、デバイスの追加後にポリシー検出を実行する必要があります。また、たとえば CLI を使用してデバイスに加えられたアウトオブバンド変更と Security Manager を同期する場合にも、ポリシー検出を実行する必要があります。

質問：検出結果はどのように確認すればよいですか。

回答：検出タスクを開始すると、ウィンドウが開き、検出のステータスと結果が表示されます。[ポリシー検出スタータス（Policy Discovery Status）] ページ（**[管理（Manage）] > [ポリシー検出スタータス（Policy Discovery Status）]** を選択）で検出タスク結果の履歴を表示することもできます。

質問：検出されないコマンドは Cisco Security Manager に表示されますか。また、それらのコマンドにはどう対処すればよいですか。

回答：検出ステータスウィンドウの [メッセージの概要（Message Summary）] セクションに移動し、[未検出のコマンド（Commands Not Discovered）] を選択します。[Description] フィールドに検出されなかったコマンドが表示されます。コマンドをデバイスから削除して検出プロセスを繰り返すか、またはそのまま続行できます。続行すると、Security Manager によって次回の展開時にサポートされないコマンドが削除されます。

デバイスで見つかったコマンドが Security Manager でサポートされていない場合、一般に検出は中断されません。ただし、デバイスにサポートされていないオブジェクト グループを参照するアクセス コントロール エントリ（ACE）がある場合、検出は中断されます。「**User groups not supported**」などのその他のエラーメッセージにも、検出されなかったコマンドに関する詳細が示される場合があります。推奨対処については、[Action] ボックス内の情報を参照してください。

質問：検出されたポリシーは、ユーザーインターフェイスにどのように反映されますか。

回答：Cisco Security Manager によってデバイスコマンドがポリシーに変換されます。デバイス設定から検出されたポリシーと、Security Manager で直接定義されたポリシーの間に、表示上の違いはありません。

質問：PIX または ASA デバイスに Auto Update Server を使用しています。ポリシーを検出するにはどうすればよいですか。

回答：デバイスにスタティック IP アドレスが割り当てられている場合は、デバイスからポリシーを検出できます。デバイスにダイナミック IP アドレスが割り当てられている場合は、デバイスの構成ファイルから（オフラインで）ポリシーを検出する必要があります。

質問：Cisco Secure ACS を使用して Cisco Security Manager に対する認証と認可を管理しています。これはポリシー検出にどのように影響しますか。

回答：ポリシー検出を実行して Cisco Security Manager で該当デバイスを管理する前に、すべての管理対象デバイスを Cisco Secure ACS に追加する必要があります。これには、PIX/ASA/FWSM デバイス上のセキュリティ コンテキストが含まれます。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。

質問：VPN またはルータ プラットフォーム ポリシーを検出したあと、何をすればよいですか。

回答：これらの機能の検出方法では、Cisco Security Manager は、検出された VPN ポリシーやルータ プラットフォーム ポリシーを展開するまで、ポリシーを管理しません。つまり、ルータを検出してから、いずれかのポリシーの割り当てを解除して展開すると、ルータの設定からコマンドは削除されません。そのため、VPN ポリシーまたはルータ プラットフォーム ポリシーを検出後すぐにファイルへの展開を実行し、その後これらのポリシーに変更を加えることを推奨します。最初の展開後、必要に応じてこれらのポリシーを再設定したり、変更を展開したりできます。

質問：デバイス上のポリシーを検出し、変更しないで Cisco Security Manager から展開した場合、デバイス上の元の設定と展開後の設定にはどのような違いがありますか。

回答：一般に、サポートされていない CLI コマンドの FlexConfig を設定した場合、新しい設定と元の設定の間に違いはありません。ただし、ACL またはオブジェクト グループの命名方式が多少変更になる場合があります。詳細については、ポリシー オブジェクトがオブジェクト グループとしてプロビジョニングされる方法を参照してください。さらに、ポリシーで使用されていない検出済みオブジェクトは設定から削除されます。新しい設定が古い設定と機能的に同じであっても、同じコマンドが使用されない場合もあります。

質問：Cisco Security Manager では、ACL やオブジェクトグループの現在の CLI 命名方式はどのように処理されますか。

回答：デバイスからポリシーを検出すると、Cisco Security Manager は使用されているポリシーと同じ名前を使用しようとします。ただし、命名方式によっては、デバイスに対して定義したポリシーと検出により作成されたポリシーの間に若干の違いが生じることがあります。さらに、デバイス上の既存の ACL やオブジェクトと、新しいポリシーやオブジェクトに必要な名前の間に、名前の競合が発生する可能性があります。この場合、デバイスが誤って設定されないように、Security Manager によって別の名前が生成されます。たとえば、検出されたオブジェクトの名前が、Security Manager にすでに存在する同じタイプのオブジェクトと競合する場合は、新しいオブジェクトの名前にサフィックスが追加されて一意の名前が生成されるか、またはデバイス レベルのオーバーライドが作成されます。

質問：Cisco Security Manager では、すべてのコンフィギュレーション コマンドが検出されて、取り込まれますか。

回答：Cisco Security Manager ですべてのデバイス コンフィギュレーション コマンドが検出されるわけではありません。代わりに、セキュリティ ポリシーが検出されます。検出されなかったコンフィギュレーション コマンドについては、FlexConfig 機能を使用して、Security Manager でサポートされていないコマンドを追加します。

質問：すでに Cisco Security Manager に存在するデバイス上のポリシーを再検出した場合、デバイスに割り当てられているポリシーはどうなりますか。

回答：すでに Cisco Security Manager で管理されているデバイス上のポリシーを再検出すると、デバイスに割り当てられているポリシーは、新たに検出されたポリシーに置き換えられます。Security Manager データベース内のポリシーとは異なるデバイス上のポリシーだけでなく、選択したポリシー ドメイン内のすべてのポリシー（ファイアウォール サービス、プラットフォーム設定、またはこれらの両方）が置き換えられます。デバイスに共有ポリシーが割り当てられている場合は、割り当てが解除され、共有ポリシーは変更されません（そのため、共有ポリシーを使用する他のデバイスは影響を受けません）。ポリシー検出後、デバイスに割り当てられているすべてのポリシーは、そのデバイス固有になります。つまり、他のデバイスと共有されません。デバイスで共有ポリシーを使用する場合は、ポリシー検出後に割り当てをやり直す必要があります。

さらに、ローカルポリシーに対して行われたカスタマイズも失われます。たとえば、セクションを使用してルールベースのファイアウォールポリシーを編成した場合、セクションは削除され、再検出されたポリシーはエントリのフラットリストになります。

質問：Cisco Security Manager は、ポリシー検出中に既存のポリシーやオブジェクトを使用しますか。

回答：ポリシー検出中、Cisco Security Manager はデバイスのポリシーを作成するときに既存のポリシーオブジェクト（Cisco Security Manager ですでに定義されているオブジェクト）を使用します。ただし、Security Manager は既存のポリシーを再利用しません。検出中に作成されたすべてのポリシーは検出対象のデバイスに対してローカルになります。したがって、Security Manager にデバイスを追加する前に、ネットワーク オブジェクトなどのポリシー オブジェクトを定義すると役立つ場合があります。

質問：デバイスを追加してポリシーを検出したあと、変更をデータベースに送信できません。その代わりに、「Connection Policies Not Set」などの警告が表示されます。デバイスの追加を完了するにはどうすればよいですか。

回答：デバイスを追加してポリシーを検出すると（特に構成ファイルからデバイスを追加する場合）、作成される構成が不完全でデバイスを正しく管理できなくなる場合に Cisco Security Manager から警告が表示されます。たとえば、接続ポリシーは、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（ユーザ名およびパスワード）と、その他の接続関連の設定（HTTP 設定など）である場合があります。これらの設定がなければ設定が無効になるか、または Security Manager があとでデバイスに接続してデバイスを管理できなくなるため、変更をデータベースに送信できません。これらの設定が完了し、設定が有効であることを確認して、変更をデータベースに再送信してください。

質問：AAA ポリシーにデバイスで検出した AAA 設定が表示されないのはなぜですか。

回答：AAA ポリシーには、認証、許可、およびアカウンティングのデフォルト設定が含まれています。特定のリスト名を指定する他の AAA コマンドは、それらのコマンドを参照するポリシーにマッピングされます。リスト名は、ポリシーによって参照されない場合は検出されません。

質問：ルータに設定されている AAA 方式リストの定義の一部が検出されないのはなぜですか。

回答：Cisco Security Manager では、if-needed などの特定のキーワードがサポートされていません。これらのキーワードを含む方式リストは、キーワードなしに検出されます。デバイス上の

デフォルトの AAA 定義にサポートされていないキーワードが含まれる場合、コマンド全体が検出されません。

質問：server-private コマンドを使用して設定された、IOS ソフトウェアを実行しているデバイスで AAA サーバーを検出できますか。

回答：はい。AAA サーバーを検出できます。ただし、Security Manager によって標準の AAA サーバに変換されます。これらのサーバは、グローバルに使用したり、複数の AAA サーバ グループで使用したりできます。server-private コマンドはサポートされません。

質問：検出とデバイスホスト名について知っておくべきことは何ですか。

回答：デバイスを検出すると、デバイスで検出されたホスト名がホスト名ポリシーに読み込まれます。ただし、[Device Properties] に表示されているホスト名は、この値で更新されません。デバイス プロパティで定義されたホスト名がデバイスの正しい DNS 名であることを確認してください。詳細については、デバイス プロパティについてを参照してください。

質問：検出された ASA ポリシーからポリシーマップのポリシーに関する説明が CSM によって削除されるのはなぜですか。

回答：ポリシーの検出中、CSM では、ポリシーマップの説明はポリシーからデータベースに移動されないため、設定をプレビューすると、ポリシーマップ内の説明は空白になります。展開後、ASA は、CSM によって展開されたポリシーマップを説明なしで表示します。

デバイス ビューおよび Site-to-Site VPN Manager におけるポリシーの管理

次の項で説明するように、デバイス ビューまたは Site-to-Site VPN Manager を使用して、ローカル ポリシーと共有ポリシーの両方を管理できます。

- ポリシー ステータス アイコン （39 ページ）
- 基本的なポリシー管理の実行 （39 ページ）
- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用 （47 ページ）

デバイスビューにアクセスするには、[ビュー（View）] > [デフォルトビュー（Device View）] を選択するか、またはツールバーの [デバイスビュー（Device View）] ボタンをクリックします。Site-to-Site VPN Manager にアクセスするには、[管理（Manage）] > [サイト間VPN（Site-to-Site VPNs）] を選択するか、またはツールバーの [サイト間VPN Manager（Site-to-Site VPN Manager）] ボタンをクリックします。

関連項目

- デバイス インベントリについて
- ポリシー ビューにおける共有ポリシーの管理 （64 ページ）

- ポリシーについて （1 ページ）

ポリシー ステータス アイコン

ポリシー名の横に表示されるアイコンを確認すると、ひと目で Security Manager のポリシーのステータスがわかります。

表 *5:* ポリシー ステータス アイコン

アイコン	ステータス（Status）
147969	ポリシーが設定されていません。展開時に、デバイス上にすでに存在するこのタイプのポリシーが削除されます。
147967	ローカル ポリシーが設定されています。このポリシーの定義は、このポリシーが設定されているデバイスまたは VPN トポロジだけに影響します。
147968	共有ポリシーが設定されています。このポリシーの定義に加えた変更は、このポリシーが割り当てられているすべてのデバイスまたは VPN トポロジに影響します。
	ポリシーバンドルが設定されています。このポリシーの定義を変更すると、これらのポリシーが同じポリシーバンドル、共有ポリシーを含む別のポリシーバンドルを使用して割り当てられているか、共有ポリシーがポリシーバンドル経由ではなく直接割り当てられているかにかかわらず、このポリシーが割り当てられているすべてのデバイスまたは VPN トポロジに影響します。

関連項目

- ポリシーについて （1 ページ）

基本的なポリシー管理の実行

ここでは、デバイス ビューでローカル ポリシーに対して実行できる操作について説明します。ローカル ポリシーとは、そのポリシーが設定されているデバイスまたは VPN トポロジに固有のポリシーのことです。他のネットワーク要素によって共有されることはありません。

- デバイス ビューにおけるローカル ポリシーの設定 （40 ページ）
- デバイス間でのポリシーのコピー （42 ページ）
- ポリシーの割り当て解除 （46 ページ）（この項は、Site-to-Site VPN Manager にも適用されます）

関連項目

- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用 （47 ページ）
- ポリシー ビューにおける共有ポリシーの管理 （64 ページ）
- ポリシーについて （1 ページ）

デバイス ビューにおけるローカル ポリシーの設定

個々のデバイスのローカル プラットフォームやサービス ポリシーを設定するには、デバイス ビューを使用します。各ポリシーでは、NAT、OSPF ルーティング、インスペクション ルールなどのデバイスで実行できる特定の設定やセキュリティ タスクを定義します。ローカル ポリシーとは、そのポリシーが定義されている個々のデバイスに固有の、名前のないポリシーのことです。ローカル ポリシーに加えた変更は、Security Manager で管理されている他のデバイスには反映されません。

ポリシーを設定すると、そのポリシーにロックが適用され、他のユーザは同じポリシーを同時に変更できなくなります。 ポリシーのロックについて （9 ページ）を参照してください。

特定のデバイスに割り当てられたローカルポリシーを変更できるのは、ポリシーを変更する権限とそのデバイスにアクセスする権限がある場合です。権限の詳細については、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。

ポリシーの設定後、デバイス上で変更を有効にするには、そのデバイスに変更を展開する必要があります。詳細については、展開の管理を参照してください。

関連項目

- デバイス ビューについて
- デバイス ビューおよび Site-to-Site VPN Manager におけるポリシーの管理 （38 ページ）
- デバイス間でのポリシーのコピー （42 ページ）
- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用 （47 ページ）

ステップ 1 デバイス ビューで、デバイス セレクタからデバイスを選択し、デバイス ポリシー セレクタからそのデバイスのポリシーを選択します。ポリシーの詳細は作業領域に表示されます。

ステップ 2 必要に応じてポリシーの定義を変更します。[Help] ボタンをクリックすると、選択したポリシーに固有の情報が表示されます。詳細については、以下を参照してください。

- サイト間 VPN の管理：基本
- リモート アクセス VPN の管理の基礎
- ファイアウォール サービスの概要
- IPS 設定の概要

- Cisco IOS IPS 設定の概要
- ルータの管理
- ファイアウォール デバイスの管理
- Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータの管理

ステップ 3 [保存（Save）] をクリックして変更を保存します。

この特定のデバイスにこのポリシーを設定するのが初めての場合は、選択したポリシーの横にあるアイコンが変わり、ポリシーが設定されてデバイスにローカルに割り当てられたことを示します。ポリシー ステータス アイコンの詳細については、を参照してください。

ポリシーを保存すると、ポリシーは設定されますが、変更を表示できるのは自分だけです。変更をコミットしてデバイスに展開するには、追加手順を実行します。変更は、Workflow モードで作業しているか、または Workflow 以外のモードで作業しているかによって異なります。追加手順を実行する前に、展開するすべてのポリシーを設定します。ポリシーの変更を一度に 1 つずつ展開する必要はありません。

実行する必要がある追加手順の概要を次に示します。

- 変更を送信します。送信すると、Security Manager サーバ上のデータベースが変更で更新されます。
  - Workflow 以外のモードで、[ファイル（File）] > [送信（Submit）] を選択して変更を送信します。[ファイル（File）] > [送信と展開（Submit and Deploy）] を選択して、1 つの手順で変更の送信と展開を実行することもできます。
  - Workflow モードでは、アクティビティ アプルーバと連携している場合、アクティビティを送信します。アクティビティが承認されると変更がコミットされます。アクティビティ アプルーバと連携していない場合は、自分で自分のアクティビティを承認すると、変更がコミットされます。詳細については、承認のためのアクティビティの送信（アクティビティ アプルーバを使用する Workflow モード）およびアクティビティの承認または拒否（Workflow モード）を参照してください。

Workflow モードと Workflow 以外のモードの両方において、ポリシーは送信時に検証されます。検証の詳細については、アクティビティ/チケットの検証を参照してください。

- 変更を展開します。展開すると、デバイスが直接新しい設定で更新されるか、自分で展開できる設定ファイルが作成されるか、またはデバイスが更新を取得する中間サーバ（Auto Update Server、Configuration Engine、または Token Management Server）に設定ファイルがコピーされます。使用する方法は、組織の要件によって決まり、デバイスごとに異なる方法を選択できます。展開の一般情報については、展開および Configuration Archive の使用を参照してください。Workflow モードに基づく特定の手順および展開方法については、次の各項を参照してください。
  - Workflow 以外のモードでの設定の展開
  - Workflow モードでの展開ジョブの展開
  - Auto Update Server または CNS Configuration Engine を使用した設定の展開
  - Token Management Server への設定の展開

- デバイスへの直接展開
- 中間サーバを使用したデバイスへの展開
- ファイルへの展開

デバイス間でのポリシーのコピー

複数のポリシーまたはポリシー一式を、あるデバイスから、選択したポリシーをサポートする他のデバイスにコピーすることによって、デバイス設定を合理化できます。これにより、たとえば、既存のファイアウォールデバイスに設定されているのと同じポリシーを新しいファイアウォール デバイスにすばやく簡単に設定できます。

デバイス間でポリシーをコピーすると、ソース デバイス上のローカル ポリシーはターゲット デバイスにローカルにコピーされます。ソース デバイスに割り当てられた共有ポリシーは、ターゲット デバイスにも共有ポリシーとしてコピーされます。

ヒント

- 1 つの共有ポリシーを追加デバイスに割り当てる場合は、ポリシーのコピーではなく、割り当て機能を使用することを推奨します。デバイス ビューにおけるポリシーの共有の詳細については、デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシー割り当ての変更 （63 ページ）を参照してください。
- ソース デバイスと同じ設定やプロパティ（オペレーティング システムのバージョン、クレデンシャル、グループ化属性など）を共有する同じタイプの新しいデバイスを作成するには、[Clone Device] 機能を使用します。詳細については、デバイスの複製を参照してください。

関連項目

- デバイス ビューおよび Site-to-Site VPN Manager におけるポリシーの管理 （38 ページ）
- デバイス ビューにおけるローカル ポリシーの設定 （40 ページ）
- デバイス ビューについて
- ポリシー ステータス アイコン （39 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 ビューで、次のいずれかを実行します。

- [ポリシー（Policy）] > [デバイス間でポリシーをコピー（Copy Policies Between Devices）] を選択します。Copy Policies ウィザードが起動し、手順 1 の [Copy Policies from this Device] ページが表示されます。コピーするポリシーを含むデバイスを選択し、[次へ（Next)] をクリックします。

- デバイスセレクタでデバイスを右クリックし、[デバイス間でポリシーをコピー（Copy Policies Between Devices）] を選択します。Copy Policies ウィザードによってデバイスがソース デバイスとして選択され、手順 2 の [Select Policies to Copy] ページが表示されます。[戻る（Back）] をクリックしてソースデバイスを変更できます。

ヒント マップビューでデバイスを右クリックし、[デバイス間でポリシーをコピー（Copy Policies Between Devices）] を選択することもできます。

ステップ 2 [Select Policies to Copy] ページでコピーするポリシーを選択します。最初は、ソース デバイスのコピー可能なほとんどのポリシー（ローカルと共有の両方）が選択されます。選択を変更できますが、別のポリシーに依存するポリシーを選択する場合は、従属するポリシーを選択する必要があります。選択が有効でない場合は、選択するように求められます。

ポリシーを選択する場合は、次の点を考慮してください。

- ポリシー グループのチェックボックスをオンにすると、そのグループ内のすべてのポリシーが選択されます。
- ファイアウォールデバイス（ASA、PIX、FWSM）間でポリシーをコピーする場合、フェールオーバーポリシーをコピーすると自動的にインターフェイス ポリシーがコピーされ、その逆も同様にコピーされます。
- 通常は、インターフェイス ポリシーをコピーしないことを推奨します。これらのポリシーには固有の IP アドレスが含まれている場合があるからです。コピー前に慎重に検討する必要があるその他のポリシー タイプとして、IOS デバイス上の NAT、ルーティング、または IPS ポリシーがあります。
- セキュリティ コンテキスト ポリシー（FWSM、PIX ファイアウォール、または ASA デバイスの場合）を選択する場合は、コンテキストがデバイス セレクタに表示されるように、デバイスをコピーしたあとで変更を送信する必要があります。Workflow 以外のモードで、[ファイル（File）]>[送信（Submit）] を選択します。Workflow モードでは、アクティビティを送信します。

ステップ 3 ポリシーオブジェクトのコピーオプションを使用して、ポリシーオブジェクトの処理方法を指定します。これらのオプションは相互に排他的ではありません。選択する組み合わせには、ターゲット デバイスでのポリシーの定義方法に関連する重要な意味があります。

選択可能なオプションの組み合わせとその意味を次に示します。

- ターゲットデバイスにソースデバイスと同じポリシーオブジェクト設定を適用するには、[ポリシーオブジェクトのグローバル値をコピーする（Copy the Global Values of Policy Objects）] と [ポリシーオブジェクトのオーバーライド値をコピーする（Copy the Overridden Values of Policy Objects] の両方を選択します。
- ポリシーオブジェクトをターゲットデバイスで使用する場合に値がオーバーライドされないようにするには、**どちらの**オプションも選択しません。選択したポリシーでポリシーオブジェクトが使用され、ターゲットデバイス上の対応するポリシーで同じポリシーオブジェクトが使用される場合、ターゲットデバイスで定義されているポリシーオブジェクトの値が保持されます。ターゲットデバイスでポリシーオブジェクトが使用されない場合、ポリシーはポリシーオブジェクトのグローバル値を使用してソースデバイスにコピーされます（ソースデバイス上のオーバーライドは無視されます）。

- ターゲットデバイス上のすべてのポリシーオブジェクトが、ポリシーオブジェクトのグローバル値を使用するには、[ポリシーオブジェクトのグローバル値をコピーする（Copy the Global Values of Policy Objects）] を選択し、[ポリシーオブジェクトのオーバーライド値をコピーする（Copy the Overridden Values of Policy Objects] の選択を解除します。ソース デバイスにポリシー オブジェクトを使用するポリシーが含まれている場合は、ポリシー オブジェクトにグローバル値を使用するポリシーだけがコピーされます。ターゲットデバイスが、ポリシーオブジェクトのローカル値を使用する同等のポリシーをもつ場合、ローカル値はポリシーオブジェクトのグローバル値に置き換えられます。
- ソースデバイス上のローカル値を持つポリシーオブジェクトだけをターゲットデバイスにコピーするには、[ポリシーオブジェクトのグローバル値をコピーする（Copy the Global Values of Policy Objects）] の選択を解除し、[ポリシーオブジェクトのオーバーライド値をコピーする（Copy the Overridden Values of Policy Objects] を選択します。ソースデバイスにポリシーオブジェクトを使用するポリシーが含まれている場合は、ポリシーオブジェクトのグローバル値をオーバーライドするポリシーのみがコピーされます。ターゲットデバイスは、ソースデバイスのポリシーオブジェクトのオーバーライド値を取得します。

次の表は、2 つのオプションのどちらが選択されているかに応じて、ポリシーオブジェクトをコピーした場合に生じ得る結果を示しています。

送信元デバイス	ターゲットデバイス	ユーザ オプション	ターゲットデバイス（コピーの結果）
グローバル定義	参照しない	任意（Any）	グローバル定義
グローバル定義	グローバル定義	任意（Any）	グローバル定義
グローバル定義	デバイスレベルのオーバーライド	どちらのオプションも選択しない	ターゲットデバイスのオーバーライドを保持
		[ポリシーオブジェクトのグローバル値のみをコピーする（Copy the Global Values of Policy Objects）]	グローバル定義
		[ポリシーオブジェクトのオーバーライド値のみをコピーする（Copy the Overridden Values of Policy Objects）]	ターゲットデバイスのオーバーライドを保持
		両方のオプションを選択	グローバル定義

送信元デバイス	ターゲットデバイス	ユーザ オプション	ターゲットデバイス（コピーの結果）
デバイスレベルのオーバーライド	参照しない	どちらのオプションも選択しない	グローバル定義
		[ポリシーオブジェクトのグローバル値 のみをコピーする（Copy the Global Values of Policy Objects）]	グローバル定義
		[ポリシーオブジェクトのオーバーライド値のみをコピーする（Copy the Overridden Values of Policy Objects]	ソースデバイスのオーバーライドを使用
		両方のオプションを選択	ソースデバイスのオーバーライドを使用
デバイスレベルのオーバーライド	グローバル定義	どちらのオプションも選択しない	グローバル定義
		[ポリシーオブジェクトのグローバル値のみをコピーする（Copy the Global Values of Policy Objects）]	グローバル定義
		[ポリシーオブジェクトのオーバーライド値のみをコピーする（Copy the Overridden Values of Policy Objects]	ソースデバイスのオーバーライドを使用
		両方のオプションを選択	ソースデバイスのオーバーライドを使用
デバイスレベルのオーバーライド	デバイスレベルのオーバーライド	どちらのオプションも選択しない	ターゲットデバイスのオーバーライドを保持
		[ポリシーオブジェクトのグローバル値のみをコピーする（Copy the Global Values of Policy Objects）]	ターゲットデバイスのオーバーライドを保持
		[ポリシーオブジェクトのオーバーライド値のみをコピーする（Copy the Overridden Values of Policy Objects]	ソースデバイスのオーバーライドを使用
		両方のオプションを選択	ソースデバイスのオーバーライドを使用

[次へ（Next）] をクリックします。

ステップ 4 [Copy Policies to these Devices] ページで、ポリシーのコピー先のターゲット デバイスを選択します。デバイス グループのチェックボックスをオンにすると、そのグループ内のすべてのデバイスが選択されます。

デバイス セレクタには、コピー対象として選択したすべてのポリシーをサポートするデバイスだけが表示されます。ポリシーのコピー先のデバイスが一部表示されない場合は、ポリシー選択ページに戻って制約

の厳しいポリシーの選択を解除します。次に、もう一度ウィザードを使用して、制約の厳しいポリシーを、そのポリシーをサポートするデバイスのサブセットにコピーします。

インベントリ内に、選択したすべてのポリシーをサポートできる他のデバイスがない場合、デバイス リストは空になります。

ヒント　デバイスの選択後、[プレビュー（Preview）] ボタンをクリックすると、コピーするポリシーの概要が表示されます。概要には、選択したデバイス、それらのデバイスにコピーされるポリシー、およびポリシーのコピーにより作成、更新、または削除されるオーバーライドが表示されます。

ステップ 5　[終了（Finish）] をクリックします。ポリシーのコピーを確認するように求められます。

ポリシーは、ターゲットデバイスにコピーされます。ターゲットデバイスに対するコピー操作が失敗すると、成功したデバイスに対するコピーは取り消され、問題のある各デバイスでコピーが失敗した原因のリストが表示されます。一般に、コピーが失敗するのは、他のユーザがポリシーまたはデバイスをロックしたか、またはデバイスに対する必要な権限がないことが原因です。

ポリシーの割り当て解除

すでにデバイスに展開されているポリシーの割り当てを解除すると、ほとんどの場合、ポリシーに定義された値が消去され、デバイスの計画設定からポリシーが削除されます。展開を実行すると、デバイスにすでに存在するこの機能の設定が削除されます。

正確な動作は、割り当てを解除するポリシーのタイプによって異なります。

- ファイアウォール サービス ポリシー：ポリシーの割り当てを解除すると、デバイスからポリシーが消去されます。
- VPN ポリシー：
  - サイト間 VPN ポリシー：必須のサイト間 VPN ポリシーは、トポロジ内のデバイスから割り当て解除できません。必須ポリシーの共有を解除すると、影響を受けるデバイスにデフォルト値が割り当てられます。オプション ポリシーの割り当てを解除すると、デバイスから設定が消去されます。詳細については、サイト間 VPN の必須ポリシーおよびオプションのポリシーについてを参照してください。
  - IPSec リモート アクセス VPN ポリシー：ポリシーの割り当てを解除すると、必須ポリシーの場合でもデバイスからポリシーが消去されます。ほとんどの場合、必須ポリシーの新しい定義を作成しなければ展開は失敗します。展開が失敗しない場合は、デバイスで VPN トンネルを確立できません。
  - SSL VPN ポリシー：ポリシーの割り当てを解除すると、デバイスからポリシーが消去されます。
- Catalyst 6500/7600 または Catalyst スイッチ ポリシー：インターフェイスおよび VLAN ポリシーは共有または割り当て解除できません。プラットフォーム ポリシー（IDSM 設定、VLAN アクセス リストなど）の割り当てを解除すると、デバイスからポリシーが削除されます。

- IPS ポリシー：すべての IPS デバイスおよびサービス ポリシーでは、デフォルトのポリシーがデバイスに割り当てられます。
- PIX/ASA/FWSM ポリシー：他のデバイスと共有できないポリシーは、そのポリシーが作成されたデバイスから割り当て解除できません。これには、インターフェイス、フェールオーバー、セキュリティ コンテキスト、およびリソース ポリシーが含まれます。その他のポリシー タイプ（タイムアウト ポリシーなど）については、Security Manager は可能なかぎりデバイス上のシステム デフォルト設定を復元します。
- IOS ルータ ポリシー：基本的なインターフェイス設定やアカウントなどのコア接続ポリシーとクレデンシャルポリシーは、それらのポリシーが作成されたデバイスから割り当て解除できません。デバイスを設定するためのパスワードの定義に使用されたデバイス アクセス ポリシーの割り当てを解除すると、Security Manager はそのデバイスを今後設定できなくなる可能性があります。詳細については、Cisco IOS ルータにおけるユーザ アカウントおよびデバイス クレデンシャルを参照してください。

VTY またはコンソール ポリシーの割り当てを解除すると、Security Manager はデフォルト設定を復元して、デバイスとの通信が継続されるようにします。その他のすべてのポリシータイプの場合、ポリシーの割り当てを解除すると、デバイスから設定が消去されます。

関連項目

- デバイス ビューにおけるローカル ポリシーの設定 （40 ページ）
- デバイス間でのポリシーのコピー （42 ページ）
- デバイス ビューおよび Site-to-Site VPN Manager におけるポリシーの管理 （38 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイス ビュー）割り当てを解除するポリシーが含まれているデバイスを選択します。
- （Site-to-Site VPN Manager）割り当てを解除するポリシーが含まれている VPN トポロジを選択します。

ステップ 2 ローカルポリシーを右クリックし、[ポリシーの割り当て解除（Unassign Policy）] を選択します。

（注） ロールに割り当て権限がマップされている場合にのみ、ポリシーの共有を解除できます。Cisco Security Manager は認証のエラーメッセージを表示します。

現在のポリシーの割り当てを解除することを確認するように求められます。

デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用

共有ポリシーを使用すると、複数のデバイスに共通のポリシーを設定できます。これにより、ポリシー定義の一貫性が維持され、管理作業が合理化されます。共有ポリシーに加えた変更

は、そのポリシーが割り当てられているすべてのデバイスおよび VPN トポロジに反映されます。これにより、たとえば、Cisco IOS ルータに割り当てられている共有 Quality of Service ポリシーを更新して、これらのすべてのデバイスを新しい Quality of Service ポリシーで簡単に更新できます。

デバイス ビューまたは Site-to-Site VPN Manager で作業する場合、ローカル ポリシー（デバイス検出中に作成されたポリシーなど）を取得して共有できます。その後、共有ポリシー（別のユーザによってロックされていない場合（ポリシーのロックについて （9ページ）を参照））を必要な数のデバイスや VPN トポロジに割り当てたり、これらの割り当てをいつでも変更したりできます。ローカルポリシーから作成されたこれらの共有ポリシーを取得して、ポリシーバンドルに追加することもできます。ポリシーバンドルの詳細については、ポリシーバンドルの管理 （72 ページ）を参照してください。

ヒント　他のデバイスを作成するためのテンプレートとして使用しているデバイスがある場合は、テンプレートデバイスに基づくデバイス設定に使用できるポリシーバンドルをすばやく作成できます。作成するには、最初にデバイス共有ポリシーですべてのポリシーを作成し（選択したデバイスの複数のポリシーの共有 （54 ページ）を参照）、次にそれらの共有ポリシーからポリシーバンドルを作成します。

さらに、デバイスまたは VPN トポロジに割り当てられている共有ポリシーを取得し、それを特定のデバイスまたはトポロジのローカルポリシーにすることができます。これにより、そのデバイスまたはトポロジだけに反映される特別な設定を作成できます。共有ポリシーが割り当てられている他のデバイスやトポロジは、前と同じように共有ポリシーを使用し続けます。

ローカル ポリシーを共有する代わりに、ポリシー ビューを使用して新しい共有ポリシーを作成し、そのポリシーをネットワーク レベルで管理できます。詳細については、ポリシー ビューにおける共有ポリシーの管理 （64 ページ）を参照してください。ポリシー ビューで共有ポリシーを作成し、デバイスまたは VPN トポロジに割り当てたら、デバイス ビューまたは Site-to-Site VPN Manager に戻って、次の項で説明するようにポリシーに対して追加操作を実行できます。デバイス ビューまたは Site-to-Site VPN Manager で作成したすべての共有ポリシーは、ポリシー ビューに自動的に共有ポリシーとして表示されます。

ヒント　デバイス ビューまたは Site-to-Site VPN Manager で共有ポリシーを編集すると、変更はそのポリシーを共有するすべてのデバイスまたは VPN に適用されます。したがって、ポリシー ビューに移動して共有ポリシーを編集する必要はありません。共有ポリシーを編集しようとすると、目的以外のデバイスやトポロジに誤って変更を加えることがないように、警告が表示されます。1 つのデバイスまたはトポロジだけのポリシーを変更する必要がある場合は、ポリシーの共有解除 （56ページ）で説明しているように、そのポリシーを編集する前にポリシーの共有を解除できます。

次の項では、ポリシーの共有方法およびデバイス ビューまたは Site-to-Site VPN Manager でそれらのポリシーに対して実行できる操作について説明します。

- ポリシー バナーの使用 （49 ページ）

- デバイス ビューおよび Site-to-Site VPN Manager におけるポリシー ショートカット メニュー コマンド （51 ページ）
- ローカル ポリシーの共有 （53 ページ）
- 選択したデバイスの複数のポリシーの共有 （54 ページ）
- ポリシーの共有解除 （56 ページ）
- デバイスまたは VPN トポロジへの共有ポリシーの割り当て （57 ページ）
- 共有ポリシーへのローカル ルールの追加 （58 ページ）
- ルールの継承または継承の解除 （60 ページ）
- 共有ポリシーのクローニング（コピー） （61 ページ）
- 共有ポリシー名の変更 （61 ページ）
- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシー定義の変更 （62 ページ）
- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシー割り当ての変更 （63 ページ）

関連項目

- ポリシーまたはデバイスのインポート
- ポリシーについて （1 ページ）
- デバイス ビューおよび Site-to-Site VPN Manager におけるポリシーの管理 （38 ページ）

ポリシー バナーの使用

デバイス ビューでデバイス ポリシーを表示する場合、または Site-to-Site VPN Manager でサイト間 VPN ポリシーを表示する場合は、作業領域のポリシー コンテンツの上にバナーが表示されます。バナーには、ポリシーがデバイスに対してローカルであるか、または共有ポリシーであるかに関する情報が含まれます。共有ポリシーの場合、バナーは、そのポリシーを使用するデバイスの数も示します。継承を許可するポリシーの場合、バナーには継承に関する情報が含まれます。

バナーの下に、次の内容のメッセージが表示される場合があります。

- ポリシーは他のユーザによってロックされています。他のユーザが変更を送信（および承認）するか、編集をキャンセルするか、または変更を廃棄するまで、ポリシーへの変更を保存できません。
- 共有ポリシーがインポートされました。ポリシーが異なるサーバで管理されている場合、インポートされたポリシーは今後、再度インポートされる可能性があります。ポリシーに加えた変更は、ポリシーが再度インポートされた場合には削除されます。ポリシーを編集する前に、ポリシー管理およびインポート用に組織で使用されているプロトコルを確実に

理解してください。[Tools] > [Security Manager Administration] > [Policy Management] ページのオプションを使用して、このメッセージを表示するかどうかを制御できます（[Policy Management] ページを参照）。

バナーのリンクを使用して、共有ポリシーを作成または割り当てたり、ポリシーの継承を設定したりできます。次の図に、デバイスのポリシー マナーの例を示します。

ポリシー バナーのフィールドには、次の意味と用途があります。

- [Policy Assigned]：このデバイスまたは VPN に割り当てられているポリシーの名前。名前がリンクになっている場合は、そのリンクをクリックして共有ポリシーを要素に割り当てることができます。リンクがない場合は、共有ポリシーをこの特定のタイプのポリシーに割り当てることはできません。
  - [Local]：ポリシーは共有ポリシーではなくローカル ポリシー（このデバイスのみに設定されたポリシー）です。
  - 特定のポリシー名：デバイス ポリシーに共有ポリシーが割り当てられています。
- [Assigned To]：共有ポリシーが割り当てられている場合は、ポリシーが割り当てられているデバイスまたは VPN の数。共有ポリシーが割り当てられていない場合は、[ローカルデバイス（local device）] または [このVPN（this VPN）] が表示されます。名前がリンクになっている場合は、次の操作を実行できます。
  - [Local Device] または [This VPN] リンク：リンクをクリックして、このローカル ポリシーから共有ポリシーを作成します。作成した共有ポリシーは、他のデバイスまたは VPN に割り当てることができます。
  - デバイスまたは VPN の数のリンク：リンクをクリックして、共有ポリシーに割り当てられているデバイスまたは VPN を変更します。
- [Inherits From]：このポリシーがルールを継承するポリシーの名前。このフィールドは、継承を許可するポリシーに対してだけ表示されます。リンクをクリックして、ポリシーがルールを継承するポリシーまたはポリシーのセットを指定します。継承の詳細については、ルールの継承について （5 ページ）を参照してください。

  このフィールドには、次のエントリが含まれる可能性があります。
  - [None]：ポリシーは他のポリシーからルールを継承しません。
  - 1 つのポリシー名：ポリシーはこのポリシーからルールを継承します。
  - > 記号で区切られた複数のポリシー名：ポリシーは表示されたポリシーの階層からルールを継承します。
- [割り当て済みのポリシーバンドル（Policy Bundle Assigned）]：このデバイスまたは VPN に割り当てられているポリシーバンドルの名前。

関連項目

- ポリシーについて （1 ページ）
- デバイス ビューおよび Site-to-Site VPN Manager におけるポリシーの管理 （38 ページ）
- ローカル ポリシーの共有 （53 ページ）
- デバイスまたは VPN トポロジへの共有ポリシーの割り当て （57 ページ）
- 共有ポリシーへのローカル ルールの追加 （58 ページ）
- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシー割り当ての変更 （63 ページ）
- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシー定義の変更 （62 ページ）
- 継承と割り当て （8 ページ）
- ポリシーのロックについて （9 ページ）
- ポリシーまたはデバイスのインポート

デバイス ビューおよび Site-to-Site VPN Manager におけるポリシー ショートカット メニュー コマンド

デバイス ビューまたは Site-to-Site VPN Manager でポリシーを右クリックすると、ポリシーに対して使用できるコマンドのリストが表示されます。このショートカット コマンド リストには、選択したポリシーに使用できるコマンドだけが含まれるため、リストは選択したポリシーによって異なります。

使用できるコマンドは、ポリシーの次の状態によって決まります。

- ポリシーが割り当てられているかどうか。
- ポリシーに特定のデバイスまたは VPN トポロジのローカル ポリシーが含まれているかどうか。
- ポリシーに複数のデバイスまたは VPN トポロジに割り当てることができる共有ポリシーが含まれているかどうか。
- ポリシーを共有できるかどうか。デバイスまたはトポロジ間で共有できないポリシーにはショートカット コマンドがありません。

ポリシー名の横に表示されるアイコンで各ポリシータイプの現在のステータスが示されます。ポリシー ステータス アイコン （39 ページ）を参照してください。

次の表に、表示されるコマンドの一覧を示します。

表 *6:* ポリシー ショートカット コマンド

メニュー コマンド	説明
ローカルポリシーと共有ポリシーの両方で使用できるコマンド	
Assign Shared Policy	選択したデバイスまたは VPN トポロジに既存の共有ポリシーを割り当てます。ポリシーがすでに共有ポリシーとして割り当てられている場合は、選択によって既存のポリシーの代わりに新しい共有ポリシーが割り当てられます。 デバイスまたは VPN トポロジへの共有ポリシーの割り当て （57 ページ）を参照してください。
Inherit Rules	ルールの継承元の共有ポリシーを特定できます。または、子ポリシーから継承を削除します。子ポリシーは、親ポリシーに定義されている必須ルールとデフォルト ルールの両方を継承します。 ルールの継承または継承の解除 （60 ページ）を参照してください。
その他のローカル ポリシー コマンド	
Share Policy	ローカル ポリシーを共有して、他のデバイスや VPN トポロジに割り当てることができるようにします。 ローカル ポリシーの共有 （53 ページ）を参照してください。
Unassign Policy	デバイスまたはVPN トポロジからポリシーの割り当てを解除します。展開時に、このポリシーに定義されている設定に対応する設定がデバイスまたはトポロジ内のデバイスから削除されます。 ポリシーの割り当て解除 （46 ページ）を参照してください。
その他の共有ポリシー コマンド	
Unshare Policy	共有ポリシーのローカル コピーを作成し、共有ポリシーの代わりにデバイスまたは VPN トポロジに割り当てます。 ポリシーの共有解除 （56 ページ）を参照してください。
Edit Policy Assignments	現在表示しているデバイスまたは VPN トポロジだけでなく、このポリシーに割り当てられているデバイスまたは VPN トポロジを変更できます。 デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシー割り当ての変更 （63 ページ）を参照してください。
ポリシーの複製	新しい名前でポリシーのコピーを作成します。このオプションは、作成時のポリシーと同じ定義を持つ新しいポリシーを作成し、そのポリシーを編集できるようにする場合に使用します。 共有ポリシーのクローニング（コピー） （61 ページ）を参照してください。
Rename Policy	選択したポリシーの名前を変更します。 共有ポリシー名の変更 （61 ページ） を参照してください。

ローカル ポリシーの共有

ネットワークが拡大するにつれて、ローカル ポリシーを、複数のデバイスまたは VPN トポロジに割り当て可能な共有ポリシーに変換することが必要になってくる可能性があります（ローカルポリシーと共有ポリシー （3 ページ）を参照）。ポリシーを共有すると、ポリシーに割り当てられているすべてのデバイスまたはトポロジの設定の一貫性を保持できる合理的な管理が可能になります。たとえば、一連のファイアウォール インスペクション ルールを特定のデバイスに設定し、そのデバイスのインスペクション ルール ポリシーを共有すると、そのポリシーを他のデバイスに割り当てられるため、各デバイスを個別に設定する必要がなくなります。デバイスまたは VPN トポロジへの共有ポリシーの割り当て （57 ページ）を参照してください。

さらに、共有ポリシーを使用すると、割り当てられている各デバイスまたはトポロジの設定を一度に更新できるため、時間を短縮したり、一連の管理対象デバイスの一貫性を向上させることができます。

ポリシーを共有する場合は、ポリシーに名前を付ける必要があります（ローカルポリシーは単一のデバイスまたはトポロジにのみ関連付けられているため、名前は付けません）。名前を付けることで、ポリシービューで共有ポリシーを管理するときにポリシーを識別できます。

関連項目

- デバイス ビューについて
- ポリシー ステータス アイコン （39 ページ）
- ポリシー バナーの使用 （49 ページ）
- デバイスまたは VPN トポロジへの共有ポリシーの割り当て （57 ページ）
- ポリシーの共有解除 （56 ページ）
- 共有ポリシーへのローカル ルールの追加 （58 ページ）
- 選択したデバイスの複数のポリシーの共有 （54 ページ）
- ルールの継承または継承の解除 （60 ページ）
- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用 （47 ページ）

ステップ 1 デバイス ビューまたは Site-to-Site VPN Manager で、ポリシー セレクタからポリシーを選択し、次のいずれかを実行します。

- （デバイスビューのみ）**[ポリシー（Policy）] > [ポリシーの共有（Share Policy）]** を選択します。
- ポリシーを右クリックし、[ポリシーの共有（Share Policy）] を選択します。
- ポリシーバナーの [割り当て先（Assigned To）] フィールドの [ローカルデバイス/このVPN（local device/this VPN）] リンクをクリックします。「Local Policies Cannot Be Assigned to Multiple Devices」と

いうメッセージを含む警告ダイアログボックスが開き、ローカル ポリシーを表示していることが示されます。[ポリシーの共有（Share Policy）] をクリックして続行します。

[Share Policy] ダイアログボックスが表示されます。

ステップ 2 共有ポリシーの名前を入力し、[OK] をクリックします。

ポリシー名は、スペースや特殊文字を含めて最大 255 文字です。

選択したデバイスの複数のポリシーの共有

1 つの手順で、特定のデバイスに設定されている複数のポリシーを共有できます。この手順を実行すると、デバイスに設定されているすべてのポリシーを共有するか、またはその一部のポリシーだけを共有するかを選択できます。たとえば、ASA デバイスに定義されているすべてのファイアウォール サービス ポリシーを取得して共有できます。

最初は、生成される共有ポリシーは手順を実行したデバイスにだけ割り当てられます。ただし、これらの共有ポリシーを必要に応じて他のデバイスに割り当てることができます。デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシー割り当ての変更 （63 ページ）を参照してください。

この機能により、単一デバイスに設定されたポリシーを簡単に取得し、同様のデバイスを設定するためのテンプレートとしてこのポリシーを使用できます。たとえば、ブランチ オフィスのデバイスの検出後に、1 つの手順で同様のデバイスに設定されているローカル アクセス ルールをすべて取得し、それらのルールを共有して、ブランチ オフィスのデバイスに割り当てることができます。

ヒント この手順を使用して、デバイス上のポリシーを共有ポリシーにして、これらの共有ポリシーからポリシー バンドルを作成できます。その後、このポリシー バンドルを使用して、テンプレート デバイスに基づいて新しいデバイスをすばやく構成できます。

ヒント ソース デバイスと同じ設定やプロパティ（デバイスのオペレーティング システムのバージョン、クレデンシャル、グループ化属性など）を共有する同じタイプの新しいデバイスを作成するには、デバイスの複製を作成します。詳細については、デバイスの複製を参照してください。

関連項目

- デバイス ビューについて
- デバイス間でのポリシーのコピー （42 ページ）
- ローカル ポリシーの共有 （53 ページ）

- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用 （47 ページ）
- ポリシーの共有解除 （56 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 ビューで、次のいずれかを実行します。

- **[ポリシー（Policy）] > [デバイスポリシーの共有（Share Device Policies）]** を選択します。Share Policies ウィザードが開き、[Share Policies from this Device] ページ（手順 1）が表示されます。ポリシーを共有するデバイスを選択し、[次へ（Next）] をクリックします。
- 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。ポリシーの共有（Share Policies）ウィザードが開き、[共有するポリシーを選択（Select Policies to Share）] ページ（手順 2）が表示されます。必要に応じて [戻る（Back）] をクリックして手順 1 に戻り、別のデバイスを選択できます。

ヒント マップビュー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）] を選択することもできます。

ステップ 2 [Select Policies to Share] ページで、共有するすべてのポリシーを選択します。最初は、デバイスに設定されているすべての共有可能なポリシー（ローカルまたは共有）が選択されています。共有しない各ポリシーの横にあるチェックボックスをオフにします。

次にいくつかのヒントを示します。

- チェックボックスをオフにしたローカル ポリシーは、選択したデバイスに対してローカルのままです。
- すでに共有されているポリシーを選択すると、ウィザードで定義した名前を使用して、そのポリシーのコピーが作成されます。
- ポリシー グループのチェックボックスをオンにすると、そのグループ内のすべてのポリシーが選択されます。
- デバイスにポリシーが設定されており、そのポリシーを選択できない（チェックボックスがグレーになっている）場合、そのポリシーは共有不可能なポリシーです。

ステップ 3 共有ポリシーの名前を入力します。すべてのポリシーに同じ名前が付けられます。あとで個々のポリシーの名前を変更できます。詳細については、 共有ポリシー名の変更 （61 ページ）を参照してください。

すでに共有されているポリシーを選択すると、この名前を使用して、そのポリシーのコピーが作成されます。

ステップ 4 [終了（Finish）] をクリックします。選択したポリシーは共有ポリシーになり、必要に応じて他のデバイスに割り当てることができます。詳細については、デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシー割り当ての変更 （63 ページ）を参照してください。

ポリシーの共有解除

特定のデバイスまたはVPNトポロジに割り当てられている共有ポリシーの共有を解除すると、そのデバイスまたはポリシーのローカルポリシーになるコピーが作成されます。つまり、その後ローカル ポリシーに加えた変更は、この特定のデバイスまたはトポロジだけに反映されます。元の共有ポリシーが割り当てられている他のデバイスやトポロジは、これまでと同様に共有ポリシーを使用し続けます。

（注） ロールに割り当て権限が定義されている場合にのみ、ポリシーの共有を解除できます。Cisco Security Manager は認証のエラーメッセージを表示します。

（注） ポリシーバンドルの一部としてデバイスに割り当てられているポリシーは共有解除できません。デバイスからポリシーバンドルの割り当てを解除するか、デバイスに割り当てられているポリシーバンドルから共有ポリシーを削除する必要があります。

たとえば、Security Manager が、20 台のルータに割り当てられている MyBGP という BGP ルーティング ポリシーを管理しているとします。そのうち 1 台のルータ（ルータ 1）でこのポリシーの変更が必要な場合、デバイスを選択し、ポリシーの共有を解除して、そのルータに必要な変更を行うことができます。それ以降、ルータ 1 にはローカル BGP ポリシーが割り当てられ、他の 19 台のルータは引き続き MyBGP という元の共有ポリシーを使用します。

関連項目

- デバイス ビューについて
- ローカル ポリシーの共有 （53 ページ）
- デバイス ビューおよび Site-to-Site VPN Manager におけるポリシーの管理 （38 ページ）
- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用 （47 ページ）
- ポリシー ステータス アイコン （39 ページ）

ステップ 1 デバイス ビューまたは Site-to-Site VPN Manager で、ポリシー セレクタからポリシーを選択し、次のいずれかを実行します。

- （デバイスビューのみ）**[ポリシー（Policy）] > [ポリシーの共有解除（Unshare Policy）]** を選択します。
- 共有ポリシーを右クリックし、[ポリシーの共有解除（Unshare Policy）] を選択します。

（注） ロールに割り当て権限がマップされている場合にのみ、ポリシーの共有を解除できます。Cisco Security Manager は認証のエラーメッセージを表示します。

ステップ 2 [OK] をクリック共有ポリシーは、選択したデバイスまたは VPN トポロジのローカル ポリシーに変換されます。ポリシー セレクタの共有ポリシー アイコンは、ローカル ポリシー アイコンに置き換わります。

デバイスまたは VPN トポロジへの共有ポリシーの割り当て

デバイス ビューまたは Site-to-Site VPN Manager で割り当てた共有可能なポリシー（ローカルまたは共有）を同じタイプの既存の共有ポリシーに置き換えることができます。たとえば、Cisco IOS ルータにローカル NAT ポリシーが割り当てられている場合、そのポリシーの代わりに共有 NAT ポリシーを割り当てることができます。同様に、ルータに共有 NAT ポリシーが割り当てられている場合、そのポリシーを別の共有NATポリシーに置き換えることができます。

ヒント 複数のバンドル共有ポリシーを一緒に使用して、それらのポリシーの割り当てを容易にすることができます。詳細については、ポリシーバンドルの管理 （72 ページ）を参照してください。

ルールベースのローカル ポリシー（インスペクション ルール ポリシーなど）に代えて共有ポリシーを割り当てる場合、設定済みのローカル ルールは共有ポリシーに定義されているルールに置き換えられます。警告メッセージが表示され、ローカル ポリシーの代わりに共有ポリシーを割り当てるのではなく、共有ポリシーのルールを継承することによって、ローカル ルールを保持することもできます。詳細については、継承と割り当て （8 ページ）を参照してください。

ヒント 共有ポリシーに定義されているルールを使用し、ローカル ルールを保持する場合は、ポリシーを割り当てるのではなく、[Inherit Rules] オプションを選択することを推奨します。詳細については、ルールの継承または継承の解除 （60 ページ）を参照してください。

（注） IPS シグニチャ ポリシーとシグニチャ イベント アクションを継承することもできますが、継承の動作はルールベースのポリシーとは異なります。詳細については、シグニチャ継承についてを参照してください。

関連項目

- デバイス ビューについて
- ポリシー バナーの使用 （49 ページ）
- ポリシーの割り当て解除 （46 ページ）
- 共有ポリシーへのローカル ルールの追加 （58 ページ）
- デバイス間でのポリシーのコピー （42 ページ）

- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用 （47 ページ）

ステップ 1 デバイス ビューまたは Site-to-Site VPN Manager で、ポリシー セレクタからポリシーを選択し、次のいずれかを実行します。

- （デバイスビューのみ）[ポリシー（Policy）] > [共有ポリシーの割り当て（Assign Shared Policy）] を選択します。
- ポリシーセレクタでポリシーを右クリックし、[共有ポリシーの割り当て（Assign Shared Policy）] を選択します。
- ポリシー バナーの [Policy Assigned] フィールドのリンクをクリックします。

割り当て可能な共有ポリシーがある場合は、[Assign Shared Policy] ダイアログボックスが表示されます。

ステップ 2 表示されたリストからデバイスまたは VPN トポロジに割り当てる共有ポリシーを選択し、[OK] をクリックします。ポリシーで継承が許可されていない場合は、選択したデバイスに共有ポリシーが割り当てられ、終了します。

ステップ 3 ポリシーで継承が許可されている場合は、現在のポリシーが共有ポリシーに置き換えられることを示す警告が表示され、[ローカルポリシーが置き換えられる（Local Policy Will Be Replaced）] ダイアログボックスにルールを継承するためのオプションが表示されます。[Customize Desktop] ページ

選択できるオプションは、次のとおりです。

- [Assign Policy]：既存のローカル ポリシーを置き換える共有ポリシーを割り当てます。割り当てを選択した場合は、すべてのローカル ルールが削除され、取得できなくなります。
- [Inherit From Policy]：共有ポリシーのルールを継承します。継承を選択した場合は、継承されたルールがデバイスのローカルポリシーですでに定義されているローカルルールに追加されます。定義済みの一連のローカル ルールをデバイスで保持する必要がある場合は、割り当てではなく継承を使用します。

ヒント [次回から表示しない（Do not show this again）] を選択して選択内容を保存し、今後ルールベースのポリシーを割り当てるときに常にこの設定を適用できます。このオプションを選択しない場合は、ポリシーを割り当てるたびにメッセージが表示されるため、状況に応じて異なる選択を行うことができます。このオプションを選択した場合、[Customize Desktop] 管理設定ページ（を参照）でリセットすると、このオプションをオフにすることができます。

共有ポリシーへのローカル ルールの追加

アクセス ルールなどのルールベースの共有ポリシーをデバイスに割り当てると、そのデバイスに対してローカルなポリシーに追加ルールを定義できます。このオプションを選択すると、継承関係が作成され、デバイスに定義されているポリシーは共有ポリシーからルールを継承し、この特定のデバイスだけに影響するルールを追加できます。継承の詳細については、ルールの継承について （5 ページ）を参照してください。

デバイスに追加したローカル ルールは、デバイスが残りのルールを継承する共有ポリシーには影響しません。たとえば、共有ポリシー Access_Rules_South を 5 台のデバイスに割り当てて、このうち 1 台のデバイスにローカル ルールを定義した場合、そのデバイスのアクセス ルール ポリシーは Access_Rules_South とローカル ルールで構成されます。他の 4 台のデバイスは引き続き Access_Rules_South に定義されているルールだけを使用します。

はじめる前に

デバイスまたは VPN トポロジへの共有ポリシーの割り当て （57 ページ）の説明に従って、ルールベースの共有ポリシーをデバイスに割り当てます。

関連項目

- デバイス ビューについて
- 共有ポリシーのクローニング（コピー） （61 ページ）
- デバイスまたは VPN トポロジへの共有ポリシーの割り当て （57 ページ）
- ポリシーの共有解除 （56 ページ）
- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用 （47 ページ）

ステップ 1 デバイス ビューで、デバイス セレクタからデバイスを選択し、デバイス ポリシー セレクタからそのデバイスに割り当てられている共有ポリシーを選択します。アクセス ルールなどのルールベースのポリシーを選択する必要があります。ポリシーの詳細は作業領域に表示されます。

ステップ 2 次のいずれかを実行します。

- [ポリシー（Policy）] > [ローカルルールの追加（Add Local Rules）] を選択します。
- ポリシーを右クリックし、[ローカルルールの追加（Add Local Rules）] を選択します。

このデバイスのポリシーが共有ポリシーからルールを継承する子ポリシーとして定義されることを示すメッセージが表示されます。その共有ポリシーが別の共有ポリシーからルールを継承する場合は、それらのルールも自動的に継承されます。

（注） このポリシーがルールを継承する親ポリシーを変更する場合は、ルールの継承または継承の解除（60 ページ）を参照してください。

ステップ 3 [OK] をクリックして確認します。作業領域で、共有ポリシーから継承された必須ルールとデフォルト ルールに加えて、ローカルの必須ルールとデフォルト ルールの見出しが追加されます。

デバイス ポリシー セレクタで、ステータス アイコンがローカル ポリシーのアイコンに変わります。詳細については、 ポリシー ステータス アイコン （39 ページ）を参照してください。

ステップ 4 必要に応じてローカル ルールを定義します。

ヒント　ローカル ルールの追加後に共有ポリシーを割り当てると、継承されたルールとローカル ルールの両方が、選択した共有ポリシーに置き換えられます。

ルールの継承または継承の解除

ここでは、特定タイプのルールベースのポリシー（アクセス ルールなど）が同じタイプの共有ポリシーからルールを継承する方法について説明します。子ポリシーは、親ポリシーに定義されている必須ルールとデフォルト ルールの両方を継承します。

デバイス ビューで作業する場合、選択したデバイスに対してローカルな追加ルールを定義できます。詳細については、共有ポリシーへのローカル ルールの追加　（58 ページ）を参照してください。

デバイス ビューまたはポリシー ビューからルールの継承を編集できます。

関連項目

- デバイス ビューについて
- ポリシー ビューにおける共有ポリシーの管理　（64 ページ）
- デバイスまたは VPN トポロジへの共有ポリシーの割り当て　（57 ページ）
- ルールの継承について　（5 ページ）
- 継承と割り当て　（8 ページ）
- ポリシー バナーの使用　（49 ページ）
- ポリシーについて　（1 ページ）

ステップ 1　デバイスビューまたはポリシービューでルールベースのローカルまたは共有ポリシーを選択し、次のいずれかを実行します。

- **[ポリシー（Policy）] > [ルールの継承（Inherit Rules）]** を選択します。
- ポリシーを右クリックし、[ルールの継承（Inherit Rules）] を選択します。
- （デバイス ビューだけ）ポリシー バナーの [Inherits From] フィールドのリンクをクリックします。

[Inherit Rules] ダイアログボックスが表示されます。このダイアログボックスには、継承関係を含む、選択したタイプの共有ポリシーすべてのリストが表示されます。

ステップ 2　ルールを継承するポリシーを選択するか、または [継承なし（No Inheritance）] を選択して子ポリシーから継承を削除します。親ポリシーの名前がセレクタの下に表示されます。

たとえば、West Coast というアクセス ルール ポリシーを選択した場合、アクセス ポリシーは West Coast ポリシーのルールを継承します。West Coast ポリシーが US という別のアクセス ルール ポリシーの子ポリシーである場合、ポリシーは US ポリシーのプロパティを継承する West Coast ポリシーのプロパティを継承します。

ステップ 3 [OK] をクリックして定義を保存します。作業領域の親ポリシー名の下に継承されたルールが表示され、定義されている場合はローカル ルールが元の共有ポリシー名の下に表示されます。

共有ポリシーのクローニング（コピー）

既存の共有ポリシーを複製できます。これにより、既存のポリシーに似た新しいポリシーを簡単に作成できます。複製の作成後、必要に応じて複製を変更できます。

継承が適用されたルールベースのポリシーを複製した場合、新しいポリシーには作成元のポリシーと同じ継承プロパティが含まれます。詳細については、ルールの継承について （5 ページ）を参照してください。

ヒント デバイス ビューまたは Site-to-Site VPN Manager でポリシーを複製すると、新しいポリシーは選択したデバイスまたは VPN トポロジに割り当てられます。ポリシーの割り当てを変更しないでポリシーを複製する場合は、ポリシー ビューで複製を作成します。

関連項目

- デバイス ビューについて
- ポリシー ビューにおける共有ポリシーの管理 （64 ページ）
- 共有ポリシー名の変更 （61 ページ）
- 共有ポリシーの削除 （71 ページ）

ステップ 1 デバイス ビュー、ポリシー ビュー、または Site-to-Site VPN Manager で共有ポリシーを選択し、次のいずれかを実行します。

- （デバイスビューまたはポリシービューのみ）**[ポリシー（Policy）]>[ポリシーの複製（Clone Policy）]** を選択します。
- 共有ポリシーを右クリックし、[ポリシーの複製（Clone Policy）] を選択します。

[Clone Policy] ダイアログボックスが表示されます。

ステップ 2 新しいポリシーの名前を入力し、[OK] をクリックします。

名前は、スペースや特殊文字を含めて最大 255 文字です。

共有ポリシー名の変更

共有ポリシーの名前を変更できます。新しい名前は、ポリシーが割り当てられているすべてのデバイスまたは VPN トポロジにすぐに反映されます。

関連項目

- デバイス ビューについて
- ポリシー ビューにおける共有ポリシーの管理 （64 ページ）
- 共有ポリシーのクローニング（コピー） （61 ページ）
- 共有ポリシーの削除 （71 ページ）

ステップ 1 デバイス ビュー、ポリシー ビュー、または Site-to-Site VPN Manager で共有ポリシーを選択し、次のいずれかを実行します。

- （デバイスビューまたはポリシービュー）[ポリシー（Policy）]>[ポリシーの名前変更（Rename Policy）] を選択します。
- ポリシーを右クリックし、[ポリシーの名前変更（Rename Policy）] を選択します。

[Rename Policy] ダイアログボックスが表示されます。

ステップ 2 選択したポリシーの新しい名前を入力し、[OK] をクリックします。

名前は、スペースや特殊文字を含めて最大 255 文字です。

デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシー定義の変更

デバイス ビューまたは Site-to-Site VPN Manager で共有ポリシーを変更できます。変更するには、ポリシーが割り当てられているいずれかのデバイスまたは VPN トポロジを選択し、必要な変更を加えてその変更を Security Manager サーバに保存します。デバイス ビューまたは Site-to-Site VPN Manager で共有ポリシーに加えた変更は、共有ポリシーが割り当てられているすべてのデバイスに自動的に反映されます。

ヒント 変更するデバイスまたは VPN トポロジだけに変更を適用するには、まずポリシーの共有を解除する必要があります（ポリシーの共有解除 （56 ページ）を参照）。このアクションによって、ポリシーがローカル ポリシーに変換され、変更が他のデバイスやトポロジに反映されなくなります。

関連項目

- デバイス ビューについて
- ポリシー バナーの使用 （49 ページ）
- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシー割り当ての変更 （63 ページ）
- デバイス ビューにおけるローカル ポリシーの設定 （40 ページ）

- デバイス ビューおよび Site-to-Site VPN Manager におけるポリシーの管理 （38 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイス ビュー）変更する共有ポリシーが含まれているデバイスを選択します。
- （Site-to-Site VPN Manager）変更する共有ポリシーが含まれている VPN トポロジを選択します。

ステップ 2 必要に応じてポリシーを再定義します。

ステップ 3 [保存（Save）] をクリックします。ポリシーが割り当てられているすべてのデバイスまたはトポロジに変更が適用されることを示す警告が表示され、変更の保存を確認するように求められます。

デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシー割り当ての変更

特定の共有ポリシーが割り当てられているデバイスまたは VPN トポロジのリストを必要に応じて変更できます。ポリシー割り当てからデバイスまたはトポロジを削除すると、そのポリシーはデバイスまたはトポロジの計画設定から削除されます。展開時には、デバイスまたはトポロジに存在するそのタイプの設定が削除されます。ポリシーの割り当て解除の意味の詳細については、 ポリシーの割り当て解除 （46 ページ）を参照してください。

注意 ポリシー割り当てを解除すると、その設定がデバイスまたはトポロジから削除され、予期しない結果が発生するおそれがあるため、ポリシー割り当て機能は慎重に使用してください。たとえば、Cisco IOS ルータからデバイス アクセス ポリシーの割り当てを解除し、その変更を展開すると、Security Manager は今後そのデバイスを設定できなくなる可能性があります（Cisco IOS ルータにおけるユーザ アカウントおよびデバイス クレデンシャルを参照）。

ポリシー割り当ては、ポリシー ビューから変更することもできます。詳細については、 ポリシー ビューにおけるポリシー割り当ての変更 （70 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
- ポリシー バナーの使用 （49 ページ）
- デバイスまたは VPN トポロジへの共有ポリシーの割り当て （57 ページ）
- ポリシーの割り当て解除 （46 ページ）
- デバイス間でのポリシーのコピー （42 ページ）
- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用 （47 ページ）
- 継承と割り当て （8 ページ）

- ルールの継承または継承の解除 （60 ページ）

ステップ 1 デバイス ビューまたは Site-to-Site VPN Manager で、ポリシー セレクタから共有ポリシーを選択し、次のいずれかを実行します。

- （デバイスビューのみ）**[ポリシー（Policy）] > [ポリシー割り当ての編集（Edit Policy Assignments）]** を選択します。
- ポリシーを右クリックし、[ポリシー割り当ての編集（Edit Policy Assignments）] を選択します。
- ポリシーバナーの [割り当て先（Assigned To）] フィールドの [nデバイス/VPN（n device/VPN）] リンクをクリックします。

ステップ 2 次のように、ポリシーが割り当てられているデバイスまたは VPN トポロジのリストを変更します。

- 選択したポリシーを追加のデバイスまたはトポロジに割り当てるには、[使用可能なデバイス/VPN（Available Devices/VPNs）] リストからデバイスまたはトポロジを選択し、[>>] をクリックして [割り当て済みデバイス（Assigned Devices）] リストに移動します。
- デバイスまたはトポロジから選択したポリシーの割り当てを解除するには、[割り込み済みデバイス/VPN（Assigned Devices/VPNs）] リストからデバイスまたはトポロジを選択し、[<<] をクリックして [利用可能なデバイス/VPN（Available Devices/VPNs）] リストに戻します。ポリシーの割り当てが解除されたデバイスまたはトポロジは、展開時にこのポリシーを実行コンフィギュレーションから削除します。

ヒント ポリシーをデバイスグループ内のすべてのデバイスに割り当てるには、デバイスグループの名前を選択してから、[>>] をクリックします。

ステップ 3 [OK] をクリックして割り当ての変更を保存します。

ポリシー ビューにおける共有ポリシーの管理

Security Manager で設定されたすべての共有ポリシーをグローバルに管理するには、ポリシー ビューを使用します。選択したデバイスに設定されているすべてのポリシーを管理するためのデバイス ビューとは異なり、ポリシー ビューでは、デバイスにかかわらず特定のタイプの共有ポリシーをすべて管理できます。

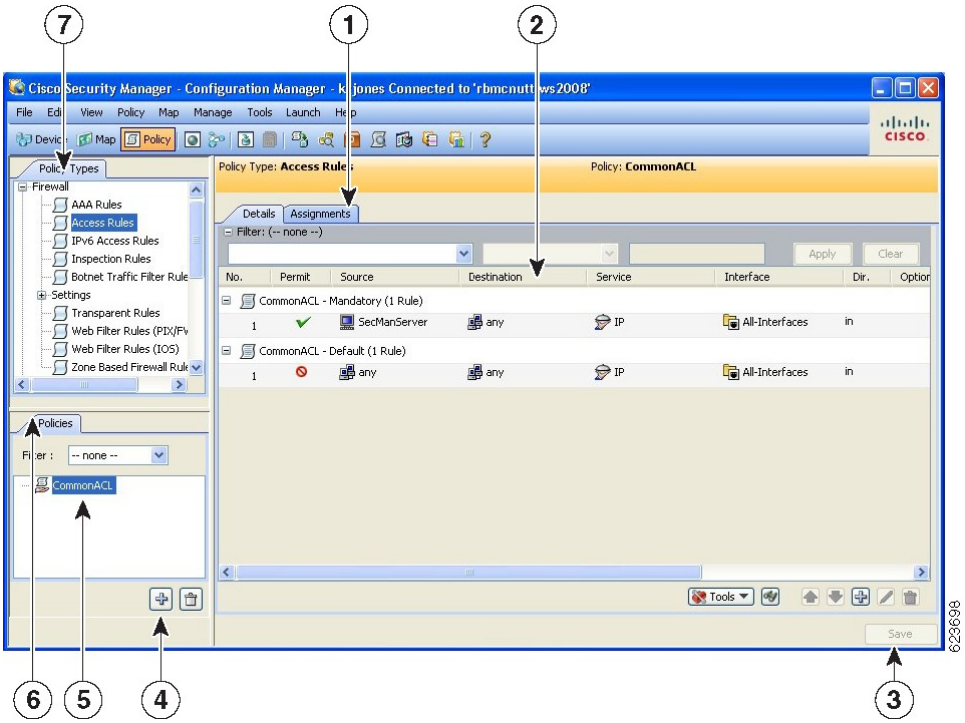
ポリシー ビューでは、次の操作を実行できます。

- 新しい共有ポリシーの作成
- ポリシー設定の編集
- 共有ポリシーが割り当てられているデバイスまたは VPN のリストの変更
- どのデバイスまたは VPN にも割り当てられていない共有ポリシーの削除

ポリシー ビューにアクセスするには、**[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。

下の図は、ポリシービューのメイン領域を示します。

図 *3 : Policy View*



1	**[Assignments] タブ**	5	**共有ポリシー セレクタ**
2	作業領域と [Details] タブ	6	共有ポリシー フィルタ
3	[Save] ボタン	7	ポリシー タイプ セレクタ
4	[Create a Policy] および [Delete a Policy] ボタン		

- （7）ポリシータイプセレクタ：Security Manager で使用できるポリシータイプがカテゴリ別に表示されます。セレクタでポリシー タイプをクリックすると、共有ポリシー セレクタにそのタイプに定義されているすべての共有ポリシーが表示されます。新しいポリシーを作成するには、ポリシータイプを右クリックし、[新規[ポリシータイプ]ポリシー（New [policy type] Policy）] を選択するか、または共有ポリシーセレクタで [ポリシーの作成（Create a Policy）] ボタンをクリックします。詳細については、ポリシー ビューのセレクタ （66 ページ）を参照してください。
- （4、5、6）共有ポリシーセレクタ：選択したタイプに定義されている共有ポリシーが表示されます。セレクタでポリシーをクリックすると、作業領域にポリシーの定義と割り当てが表示されます。詳細については、ポリシー ビューのセレクタ （66 ページ）を参照してください。

セレクタでポリシーを右クリックし、ポリシーに対してアクションを実行します。使用可能なコマンドの詳細については、ポリシー ビュー - 共有ポリシー セレクタのオプション （68 ページ）を参照してください。

セレクタに表示されるポリシーのリストをフィルタリングするには、[Filter] フィールドを使用します。フィルタの作成の詳細については、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。

- （1、2、3）作業領域：次の 2 つのタブがあります。
  - [Details]：選択したポリシーの定義を表示および編集する場合に使用します。必要に応じて定義を変更できます。作業領域で [保存（Save）] をクリックして変更を保存します。変更は、ポリシーが割り当てられているすべてのデバイスまたは VPN トポロジに反映されます。[Details] タブに表示される情報は、デバイス ビューまたは Site-to-Site VPN Manager に表示される情報と同じであり、まったく同じ方法で変更できます。ポリシー ビューのセレクタ （66 ページ）を参照してください。
  - [Assignments]：共有ポリシーが割り当てられているデバイスまたは VPN のリストを表示および編集する場合に使用します。詳細については、ポリシー ビューにおけるポリシー割り当ての変更 （70 ページ）を参照してください。

関連項目

- ポリシーまたはデバイスのインポート
- デバイス ビューおよび Site-to-Site VPN Manager におけるポリシーの管理 （38 ページ）
- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用 （47 ページ）

ポリシー ビューのセレクタ

ポリシー ビューには 2 つのセレクタがあります。上部のセレクタには、選択したポリシー ドメインの使用可能なポリシー タイプがすべて表示されます。ポリシー タイプ セレクタのルートは、ポリシー ドメイン名です。別のポリシー ドメインのポリシー タイプを表示するには、ツリーのルートをクリックし、リストから別のドメインを選択します。

ポリシー ドメインは次のとおりです。

- [Firewall]：ファイアウォール サービスを設定するためのすべてのポリシー タイプが表示されます。ファイアウォール サービスの概要を参照してください。
- [NAT (PIX/ASA/FWSM)]：PIX、ASA、および FWSM デバイスに設定されているすべての NAT ポリシーが表示されます。セキュリティ デバイスの NAT ポリシーを参照してください。
- [NAT (Router)]：Cisco IOS ルータに設定されているすべての NAT ポリシーが表示されます。Cisco IOS ルータにおける NAT ポリシーを参照してください。

- [Site-to-Site VPN]：サイト間 VPN を設定するためのすべてのポリシー タイプが表示されます。サイト間 VPN の管理：基本を参照してください。
- [Remote Access VPN]：リモート アクセス IPSec および SSL VPN を設定するためのすべてのポリシー タイプが表示されます。リモート アクセス VPN の管理の基礎を参照してください。
- [Catalyst Platform]：Catalyst スイッチおよび 7600 ルータを設定するためのすべてのポリシー タイプが表示されます。Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータの管理を参照してください。
- [IPS]：IPS デバイスを設定するためのすべてのポリシー タイプが表示されます。IPS 設定の概要を参照してください。
- [IPS (Router)]：IOS ルータに Cisco IOS IPS ポリシーを設定するためのすべてのポリシー タイプが表示されます。Cisco IOS IPS 設定の概要を参照してください。
- [PIX/ASA/FWSM Platform]：PIX/ASA/FWSM プラットフォーム固有のポリシーを設定するためのすべてのポリシー タイプが表示されます。ファイアウォール デバイスの管理を参照してください。
- [Router Interfaces]：プラットフォーム固有の Cisco IOS ルータ インターフェイス ポリシーを設定するためのすべてのポリシータイプが表示されます。ルータの管理を参照してください。
- [Router Platform]：プラットフォーム固有の Cisco IOS ルータ ポリシーを設定するためのすべてのポリシー タイプが表示されます。ルータの管理を参照してください。
- [FlexConfigs]：すべての FlexConfig ポリシーが表示されます。FlexConfig の管理を参照してください。

セレクタを必要に応じて展開および縮小して、使用可能なすべてのポリシータイプとサブタイプを表示できます。新しいポリシーを作成するには、ポリシータイプを右クリックし、[新規[ポリシータイプ]ポリシー（New [policy type] Policy）] を選択するか、または共有ポリシーセレクタで [ポリシーの作成（Create a Policy）] ボタンをクリックします。

ポリシー タイプ セレクタからポリシー タイプを選択すると、共有ポリシー セレクタにそのタイプのすべての共有ポリシーが表示されます。デバイス ビューで設定されたローカル ポリシーは表示されません。

たとえば、NAT 変換ルールなどの設定ポリシー タイプを選択すると、共有ポリシー セレクタにそのタイプの各共有ポリシーを含むフラットなリストが表示されます。ファイアウォール アクセス ルールなどのルールベースのポリシー タイプを選択すると、共有ポリシー セレクタに共有ポリシーの階層ツリーが表示されます。これにより、さまざまなポリシー間の継承関係を確認できます。共有ポリシーセレクタには、そのポリシーに対して実行できるアクション（名前の変更など）のオプションを含むショートカット メニューがあります。

ヒント　フィルタを作成して割り当てることにより、共有ポリシーセレクタに表示されるポリシーのリストを短くすることができます。フィルタの詳細については、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。

ポリシー ビュー - 共有ポリシー セレクタのオプション

ポリシー ビューの共有ポリシー セレクタでポリシーを右クリックすると、選択したポリシーに対して機能を実行するためのショートカット メニューが表示されます。

関連項目

- ポリシー ビューのセレクタ （66 ページ）
- ポリシー ビューにおける共有ポリシーの管理 （64 ページ）

フィールド リファレンス

表 7: 共有ポリシー セレクタのオプション

メニュー コマンド	説明
ポリシーの複製	複製時のポリシーと同じ定義を持つ新しい共有ポリシーを作成します。 共有ポリシーのクローニング（コピー） （61 ページ）を参照してください。
Rename Policy	選択したポリシーの名前を変更します。 共有ポリシー名の変更 （61 ページ）を参照してください。
ポリシーバンドルに追加（Add to Policy Bundle）	選択した共有ポリシーをポリシーバンドルに追加できます。 ポリシーバンドルの管理 （72 ページ）を参照してください。
Inherit Rules	アクセス ルールなどのルールベースのポリシーだけに適用されます。 ルールベースのポリシーは同じタイプの別の共有ポリシーのルールを継承します。 ルールの継承または継承の解除 （60 ページ）を参照してください。
[New [policy type] Policy]	選択したタイプの新しい共有ポリシーを作成します。 新しい共有ポリシーの作成 （69 ページ）を参照してください。
Delete Policy	選択した共有ポリシーを削除します。 共有ポリシーの削除 （71 ページ） を参照してください。

新しい共有ポリシーの作成

新しい共有ポリシーを作成するには、ポリシー ビューを使用します。ほとんどの場合、新しいポリシーは最初は未定義の状態ですが、特定の場合には（IPsec プロポーザルや GRE モードなどの多くのサイト間 VPN ポリシーなど）デフォルト値が指定されます。いずれの場合でも、新しいポリシーは最初はデバイスに割り当てられていません。新しいポリシーが、継承をサポートするルールベースのポリシーである場合は、同じタイプの既存の共有ポリシーの子として作成できます。詳細については、ルールの継承について （5 ページ）を参照してください。

ヒント デバイス ビューでローカル ポリシーを変換して共有ポリシーを作成することもできます。詳細については、ローカル ポリシーの共有 （53 ページ）を参照してください。

関連項目

- ポリシーまたはデバイスのインポート
- ポリシー ビューにおける共有ポリシーの管理 （64 ページ）
- 共有ポリシーの削除 （71 ページ）

ステップ 1 ポリシー ビューで、ポリシー タイプ セレクタからポリシー タイプを選択します。

ステップ 2 次のいずれかを実行します。

- ポリシータイプセレクタでポリシータイプを右クリックし、[新規[ポリシータイプ]ポリシー（New [policy type] Policy）] を選択します。
- 共有ポリシーセレクタでポリシーを右クリックし、[新規[ポリシータイプ]ポリシー（New [policy type] Policy）]を選択します。
- 共有ポリシーセレクタの下にある [ポリシーの作成（eate a Policy）] ボタンをクリックします。

[Create a Policy] ダイアログボックスが表示されます。

ステップ 3 新しいポリシーの名前を入力します。ポリシー名は、スペースや特殊文字を含めて最大 255 文字です。

セキュリティデバイス（PIX/ASA/FWSM）で NAT ルールの変換ルールポリシーを作成する場合は、デバイスのソフトウェアバージョンとして **PIX/ASA 6.3-8.2** または **ASA 8.3 & 以降**を選択する必要があります。

ステップ 4 [OK] をクリック新しいポリシーが共有ポリシー セレクタに表示されます。

新しい共有ポリシーの定義を設定するには、[Details] タブが開いている状態でツールバーの [Help] ボタンをクリックして、作成するポリシーのタイプに固有の情報を表示します。新しい共有ポリシーを割り当てるには、ポリシー ビューにおけるポリシー割り当ての変更 （70 ページ）を参照してください。

ポリシー ビューにおけるポリシー割り当ての変更

ポリシー ビューの [Assignments] タブでは、選択した共有ポリシーが割り当てられているデバイスまたは VPN トポロジのリストを変更します。[割り当て（Assignments）] タブには、選択した共有ポリシーが現在割り当てられているすべてのデバイスのリストが表示されます。また、継承によってポリシーが割り当てられているデバイスも表示されます。

ポリシーをデバイスまたは VPN に割り当てると、Security Manager で以前にデバイスに割り当てられた同じタイプのポリシー（ローカルまたは共有）が上書きされます。展開すると、新たに割り当てられたポリシーは、すでにデバイスに設定されている同じタイプのポリシーを上書きします。このポリシーは、Security Manager を使用して設定されたか、または CLI などの別の方法を使用して設定されたかにかかわらず上書きされます。

デバイスまたは VPN トポロジから共有ポリシーの割り当てを解除すると、そのデバイスまたは VPN トポロジの計画設定からポリシーが削除されます。ポリシーによって定義された設定を展開すると、すでにデバイス（VPN トポロジ内のデバイスを含む）に設定されている同じタイプの設定は削除されます。詳細については、ポリシーの割り当て解除 （46 ページ）を参照してください。

したがって、特定のデバイスまたは VPN トポロジに別の共有ポリシーを割り当てるために割り当てを解除する場合は、置換ポリシーを選択し、展開を実行する前に割り当てを実行することが重要です。

ヒント 置換ポリシーの割り当ては、特にデバイス アクセス ポリシーを使用して Cisco IOS ルータのイネーブル パスワードまたはイネーブル シークレット パスワードを設定する場合に重要です。このポリシーの割り当てを解除したときに、展開前に別のパスワードを定義しなかった場合、Security Manager は今後このデバイスを設定できなくなる可能性があります。詳細については、Cisco IOS ルータにおけるユーザ アカウントおよびデバイス クレデンシャルを参照してください。

このほか、デバイス ビューに戻って、デバイスに割り当てられている共有ポリシーを別の共有ポリシーに置き換える方法もあります。詳細については、デバイスまたは VPN トポロジへの共有ポリシーの割り当て （57 ページ）を参照してください。

（注） IKE プロポーザル ポリシーなどの必須のサイト間 VPN ポリシーの割り当てを解除すると、そのポリシーは Security Manager によって自動的にデフォルト ポリシーに置き換えられます。必須のリモート アクセス VPN ポリシーの割り当てを解除すると、その同じタイプの新しいポリシーを手動で設定する必要があります。そうしなければ展開は失敗します。

関連項目

- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシー割り当ての変更 （63 ページ）

• ポリシー ビューにおける共有ポリシーの管理 （64 ページ）

ステップ 1 ポリシー ビューで、ポリシー タイプ セレクタからポリシー タイプを選択し、共有ポリシー セレクタからポリシーを選択します。これらのセレクタの使用に関する詳細については、 ポリシー ビューのセレクタ（66 ページ）を参照してください。

ステップ 2 作業領域で [割り当て（Assignments）] タブをクリックします。

[割り当て（Assignments）] タブには、選択した共有ポリシーが現在割り当てられているすべてのデバイスのリストが表示されます。また、継承によってポリシーが割り当てられているデバイスも表示されます。

ステップ 3 次のように、ポリシーが割り当てられているデバイスまたは VPN のリストを変更します。

- 選択したポリシーを追加のデバイスまたはVPNに割り当てるには、[利用可能なデバイス/VPN（Available Devices/VPNs）] リストから 1 つ以上の項目を選択し、[>>] をクリックして [割り当て済みデバイス/VPN（Assigned Devices/VPNs）] リストに移動します。

ヒント ポリシーをデバイスグループ内のすべてのデバイスに割り当てるには、デバイスグループの名前を選択してから、[>>] をクリックします。

- デバイスまたは VPN から選択したポリシーの割り当てを解除するには、[割り当て済みデバイス/VPN（Assigned Devices/VPNs）] リストから 1 つ以上の項目を選択し、[<<] をクリックして [利用可能なデバイス/VPN（Available Devices/VPNs）] リストに戻します。

（注） Security Manager 4.4 およびバージョン 9.0 以降の ASA のリリースより前は、IPv4 および IPv6 ファイアウォールルールとポリシーを設定するための個別のページ、ポリシー、およびポリシーオブジェクトが提供されていました。Security Manager 4.4 および ASA 9.0+ では、これらのポリシーとポリシーオブジェクトが結合または統合されました。ただし、以前の ASA バージョンでは、IPv6 アクセスルールの別のページが引き続きデバイスビューで提供されますが、ポリシービューでは、AAA ルール、アクセスルール、およびインスペクションルールのポリシータイプの IPv4 および統合バージョンが提供されます。IPv4 AAA ルール、アクセスルール、またはインスペクションルール共有ポリシーを 9.0 以降のデバイスに割り当てると、これらのポリシーの統合バージョンをそのデバイスに割り当てることはできなくなります。同様に、統合AAA ルール、アクセスルール、またはインスペクションルール共有ポリシーを 9.0 以降のデバイスに割り当てると、これらの共有ポリシーの IPv4 バージョンをそのデバイスに割り当てることはできなくなります。そのデバイスは、共有ポリシーの [割り当て（Assignments）] タブの使用可能なデバイスのリストには含まれません。

ステップ 4 [保存（Save）] をクリックして割り当ての変更を保存します。

共有ポリシーの削除

Security Manager から共有ポリシーを削除するには、ポリシー ビューを使用します。

共有ポリシーを削除する前に、そのポリシーを使用するデバイスからポリシーの割り当てを解除し、そのデバイスの置換ポリシーを設定する必要があります。共有ポリシーがデバイスに割

り当てられている場合、そのポリシーを削除すると、削除した共有ポリシー用に設定されているポリシーがデバイスから削除されます。ただし、そのポリシータイプのデフォルトは存在する可能性があります。割り当ての削除の詳細については、ポリシー ビューにおけるポリシー割り当ての変更 （70 ページ）を参照してください。

（注） 共有ポリシーが、デバイスに割り当てられているポリシーバンドルの一部である場合、共有ポリシーを削除する前に割り当てを解除する必要があります。

関連項目

- 新しい共有ポリシーの作成 （69 ページ）
- 共有ポリシーのクローニング（コピー） （61 ページ）
- ポリシー ビューにおける共有ポリシーの管理 （64 ページ）

ステップ 1 ポリシー ビューで、ポリシー タイプ セレクタからポリシー タイプを選択し、共有ポリシー セレクタから削除するポリシーを選択します。これらのセレクタの使用に関する詳細については、ポリシー ビューのセレクタ （66 ページ）を参照してください。

ステップ 2 次のいずれかを実行します。

- ポリシーを右クリックして、[ポリシーの削除（Delete Policy）] を選択します。
- 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ます。

削除の確認が求められます。

ポリシーバンドルの管理

ポリシーバンドルは、グループとして管理できる共有ポリシーのコレクションです。ポリシーバンドルを使用すると、バンドルを1回作成してから、バンドル内のすべてのポリシーを新しいデバイスに一度に割り当てることができるため、共有ポリシーの管理が容易になります。バンドルの一部である共有ポリシーは、他の共有ポリシーと同じように機能し、バンドルの一部である共有ポリシーを変更すると、直接またはポリシーバンドルを介してそのポリシーが割り当てられているすべてのデバイスに影響します。

ポリシーバンドルを作成するときは、各タイプの共有ポリシーを1つだけポリシーバンドルに割り当てることができます。ポリシーバンドルのポリシータイプが重複しない限り、複数のポリシーバンドルをデバイスに割り当てることができます。

ポリシーバンドルをデバイスに割り当てるときに、そのデバイスのローカルポリシーがポリシーバンドルに含まれているものと同じポリシータイプである場合、既存のポリシーを継承するか、置き換えるかを選択できます。

（注） ポリシーバンドルの割り当てを解除すると、そのバンドルの一部であるすべてのポリシーがデバイスから削除されます。ローカルポリシーは失われ、取得できなくなります。

ここでは、次の内容について説明します。

- 新しい共有ポリシーの作成 （69 ページ）
- ポリシーバンドルの複製 （74 ページ）
- ポリシーバンドルの名前変更 （75 ページ）
- ポリシーバンドルのデバイスへの割り当て （75 ページ）

新規ポリシーバンドルの作成

ポリシーバンドルビューを使用して、新しいポリシーバンドルを作成できます。ポリシーバンドルを作成するとき、各タイプの共有ポリシーを1つだけポリシーバンドルに割り当てることができます。

関連項目

- ポリシーバンドルの管理 （72 ページ）
- ポリシーバンドルの複製 （74 ページ）
- ポリシーバンドルの名前変更 （75 ページ）
- ポリシーバンドルのデバイスへの割り当て （75 ページ）

ステップ 1 次のいずれかの方法を使用して、ポリシーバンドルを作成できます。

- ポリシーバンドルビューで、次のいずれかを実行します。
  - [すべての共有ポリシー（All Shared Policies）] ビューから、バンドルする共有ポリシーを選択し、選択した共有ポリシーを右クリックして [ポリシーバンドルの作成（Create Policy Bundle）] を選択します。
  - ポリシーバンドルセレクタで既存のポリシーバンドルを右クリックし、[ポリシーバンドルの作成（Create Policy Bundle）] を選択します。
  - 共有ポリシーバンドルセレクタの下にある [ポリシーバンドルの作成（Create a Policy Bundle）] ボタンをクリックします。
- デバイス上のすべての共有ポリシーを含む新しいポリシーバンドルを作成するには、デバイスビューのデバイスセレクタでデバイスを右クリックし、[ポリシーバンドルの作成（Create Policy Bundle）] を選択します。

[ポリシーバンドルの作成（Create Policy Bundle）] ダイアログボックスが表示されます。

ステップ 2 新しいポリシーバンドルの名前を入力します。

ステップ 3 [OK] をクリック

ポリシーバンドルは、ポリシーバンドルビューの [ポリシーバンドル（policy bundles）] リストに追加されます。

ステップ 4 ポリシー バンドルの定義を設定するには、次のいずれかを実行します。

- ポリシーバンドルビューで：
  - 共有ポリシーをバンドルに追加するには、ポリシーバンドルセレクタで [すべての共有ポリシー（All Shared Policies）] を選択し、必要な共有ポリシーをポリシーバンドルにドラッグアンドドロップします。
  - バンドルから共有ポリシーを削除するには、ポリシーバンドルセレクタでバンドルを選択します。[ポリシーバンドルビュー（Policy Bundle View）] ウィンドウの [詳細（Details）] タブで削除する共有ポリシーを選択し、[削除（Delete）] をクリックします。
- ポリシービューで、ポリシーバンドルに追加する共有ポリシーを右クリックし、[ポリシーバンドルに追加（Add to Policy Bundle）] を選択してから、共有ポリシーを追加するバンドルを選択します。

ポリシーバンドルの複製

ポリシーバンドルビューを使用して、既存のバンドルを複製して新しいポリシーバンドルを作成できます。

関連項目

- ポリシーバンドルの管理　（72 ページ）
- 新しい共有ポリシーの作成　（69 ページ）
- 共有ポリシー名の変更　（61 ページ）
- ポリシーバンドルのデバイスへの割り当て　（75 ページ）

ステップ 1 ポリシーバンドルビューのポリシーバンドルセレクタで既存のポリシーバンドルを右クリックし、[ポリシーバンドルの複製（Clone Policy Bundle）] を選択します。

[ポリシーバンドルの複製（Clone Policy Bundle）] ダイアログボックスが表示されます。

ステップ 2 新しいポリシーバンドルの名前を入力します。

ステップ 3 [OK] をクリック

新しいポリシーバンドルが共有ポリシーバンドルセレクタに表示されます。

ポリシーバンドルの名前変更

ポリシーバンドルビューから既存のポリシーバンドルの名前を変更できます。ポリシーバンドルの名前を変更しても、デバイスの割り当てには影響しません。

関連項目

- ポリシーバンドルの管理 （72 ページ）
- 新しい共有ポリシーの作成 （69 ページ）
- ポリシーバンドルの複製 （74 ページ）
- ポリシーバンドルのデバイスへの割り当て （75 ページ）

ステップ 1 ポリシーバンドルビューのポリシーバンドルセレクタで既存のポリシーバンドルを右クリックし、[ポリシーバンドルの名前変更（Rename Policy Bundle）] を選択します。

[ポリシーバンドルの名前変更（Rename Policy Bundle）] ダイアログボックスが表示されます。

ステップ 2 ポリシーバンドルの新しい名前を入力します。

ステップ 3 [OK] をクリック

ポリシーバンドルセレクタでポリシーバンドル名が更新されます。

ポリシーバンドルのデバイスへの割り当て

特定のポリシーバンドルが割り当てられているデバイスのリストを必要に応じて変更できます。ポリシーバンドルのポリシータイプが重複しない限り、複数のポリシーバンドルをデバイスに割り当てることができます。ポリシーバンドルをデバイスに割り当てるときに、そのデバイスのローカルポリシーがポリシーバンドルに含まれているものと同じポリシータイプである場合、既存のポリシーを継承するか、置き換えるかを選択できます。

（注） ポリシーバンドルに含まれるいずれかのポリシーに、割り当てようとしているデバイスとの互換性がない場合、そのバンドルを割り当てることはできません。

ポリシーバンドルの割り当てからデバイスを削除すると、そのバンドルに含まれるすべてのポリシーが、デバイスの計画中の設定から完全に削除されます。ローカルポリシーは失われ、取得できなくなります。展開時に、デバイスに存在するそのタイプの設定が削除されます。ポリシーの割り当て解除の意味の詳細については、ポリシーの割り当て解除 （46 ページ）を参照してください。

⚠

注意 ポリシーバンドルの割り当てを解除すると、その設定がデバイスから削除され、予期しない結果が発生するおそれがあるため、ポリシーバンドル割り当て機能は慎重に使用してください。たとえば、Cisco IOS ルータからデバイス アクセス ポリシーの割り当てを解除し、その変更を展開すると、Security Manager は今後そのデバイスを設定できなくなる可能性があります（Cisco IOS ルータにおけるユーザ アカウントおよびデバイス クレデンシャルを参照）。

関連項目

- ポリシーバンドルの管理 （72 ページ）
- 新しい共有ポリシーの作成 （69 ページ）
- ポリシーバンドルの複製 （74 ページ）
- ポリシーバンドルの名前変更 （75 ページ）

ステップ 1 ポリシーバンドルビューのポリシーバンドルセレクタで、既存のポリシーバンドルを選択します。

ポリシーバンドルの詳細は、ポリシーバンドルのメインウィンドウに表示されます。

ステップ 2 [割り当て（Assignment）] タブをクリックします。

ステップ 3 次のように、ポリシーバンドルが割り当てられているデバイスのリストを変更します。

- 選択したポリシーバンドルを追加のデバイスに割り当てるには、[使用可能なデバイス（Available Devices）] リストからデバイスを選択し、[>>] をクリックして [割り当て済みデバイス（Assigned Devices）] リストに移動します。
- デバイスから選択したポリシーバンドルの割り当てを解除するには、[割り当て済みデバイス（Assigned Devices）] リストからデバイスを選択し、[<<] をクリックして [使用可能なデバイス/VPN（Available Devices/VPNs）] リストに戻します。ポリシーの割り当てが解除されたデバイスまたはトポロジは、展開時にこのポリシーを実行コンフィギュレーションから削除します。

ヒント ポリシーをデバイスグループ内のすべてのデバイスに割り当てるには、デバイスグループの名前を選択してから、[>>] をクリックします。

ステップ 4 [OK] をクリックして割り当ての変更を保存します。

ポリシーバンドル名がポリシーバンドルセレクタで更新されます。

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。