展開の管理

Security Manager に定義する設定およびポリシーは、ネットワークに実装できるようにデバイスに展開する必要があります。設定をデバイスに展開するための手順は、Workflow モードまたは Workflow 以外のモードのいずれを使用しているのかによって異なります。Workflow 以外のモードが Security Manager の操作のデフォルト モードですが、社内で必要な場合には Workflow モードを使用できます。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。

ここでは、各 Workflow モードで設定をデバイスに展開する方法について説明します。

展開について

展開ジョブでは、設定変更をデバイスに送信する方法を定義します。展開ジョブでは、設定を展開するデバイスや設定をデバイスに展開するための方法など、パラメータをいくつか定義できます。また、展開スケジュールを作成して、一定の間隔で展開ジョブを自動的に生成できます。

以降のトピックは、展開ジョブの理解を深めて、効果的に使用するのに役立ちます。

展開プロセスの概要

展開とは、大まかに言うと、3つの手順からなるプロセスです。各手順を次の表で説明します。

表 *1:* 展開プロセスの概要

手順	導入手順
ステップ 1	Security Manager は、デバイスの現在の設定を取得し、その設定を Security Manager に保存されているデバイスの最新のポリシーと比較します。Security Manager で現在の設定と見なされるものは、デバイスのタイプ、展開方法、および展開プリファレンスの設定によって異なります。次に、ソースになりうるものと、そのソースが使用される条件を示します。 • デバイスから現在実行中の設定を取得します。 実行コンフィギュレーションは、展開方法が AUS、TMS、または CNS でないかぎり、デバイスに展開するときに使用されます。展開の環境設定として（**[ツール（Tools）] > [Security Manager管理（Security Manager Administration）]** を選択し、[展開（Deployment）] を選択） [デバイスへの展開時に次の場所から参照設定を取得：設定アーカイブ（When Deploying to Device Get Reference Config from: Config Archive）] を選択すると、Security Manager で強制的に Configuration Archive を使用できます。 • Security Manager Configuration Archive から最後の完全な設定を取得します。Configuration Archive は、次の場合に使用されます。 • ファイルを展開する場合。ただし、展開の環境設定として [デバイスへの展開時に次の場所から参照設定を取得：デバイス（When Deploying to File Get Reference Config from: Device] を選択した場合を除きます。 • 展開方法が TMS または CNS である場合。 • デバイスが Security Manager によって管理されていない場合。 • デバイスに展開する場合（ただし、失敗したデバイスから設定をアップロードする場合）。Configuration Archive は、ライブ デバイスから設定を取得するためのバックアップとして使用されます。 • プレビュー設定の場合。 • 工場出荷時のデフォルト設定を使用します。 工場出荷時のデフォルト設定は、AUS 展開方法を使用する場合に、PIX デバイスまたは ASA デバイスで使用されます。展開および設定プレビューに使用されます。
ステップ 2	Security Manager は、デルタ設定を構築します。デルタ設定には、デバイス設定と割り当てられたポリシーの一貫性を確保できるよう、デバイス設定を更新するために必要なコマンドが含まれています。このほか、完全なデバイス設定も構築します。

手順	導入手順
ステップ 3：	デバイスに展開している場合、Security Manager は使用している展開方法に応じてデルタ設定または完全な設定を展開します。ファイルに展開している場合、Security Manager は次の 2 つのファイルを作成します。デルタ設定用の *device_name*_delta.cfg と、完全な設定用の *device_name*_full.cfg です。どちらの場合も、設定は Configuration Archive にも追加されます。次に、展開方法に基づいた処理を示します。 • SSL（HTTPS）、SSH、または Telnet：Security Manager は直接デバイスに問い合わせて、デルタ設定をそのデバイスに送信します。 • PIX デバイスおよび ASA デバイスの Auto Update Server（スタンドアロンまたは Configuration Engine で稼働）：Security Manager は Auto Update Server にすべての設定を送信し、デバイスはサーバから設定を取得します。デルタ設定は送信されません。 • IOS デバイスの Configuration Engine：Security Manager は Configuration Engine にデルタ設定を送信し、デバイスはエンジンから設定を取得します。 • TMS：Security Manager は TMS サーバにデルタ設定を送信します。サーバから eToken に設定をダウンロードし、デバイス上にロードできます。

展開中に、デバイスの設定が最後に展開された設定と異なることを Security Manager が確認した場合、デフォルトでは変更が上書きされます。この動作は、展開の環境設定を使用して制御できます。そのためには、**[ツール（Tools）] > [Security Manager管理（Security Manager Administration）]** を選択し、[展開（Deployment）] を選択し、[アウトオブバンド変更の検出時（When Out of Band Changes Detected）] 設定を探します。ジョブの展開方法を編集して、特定の展開ジョブのためにこの動作を制御することもできます。

Security Manager の管理外でデバイス設定に変更を加えた場合、その変更を Security Manager に反映させるには 2 つの選択肢があります。

1. デバイスでポリシーを再検出できます。その場合、デバイスのすべてのポリシーがローカル ポリシーになり、デバイスに割り当てていた共有ポリシーがあればすべて削除されます。
2. Security Manager で必要な変更を加えて、デバイスに再展開できます。展開中は、アウトオブバンド変更がデバイスで見つかった場合に強制的にエラーにするオプションを選択しないでください。この方法を推奨します。

アウトオブバンド変更が展開に与える影響の詳細については、アウトオブバンド変更の処理方法について （14 ページ）を参照してください。

設定の展開後、Security Manager が制御する設定に変更を加えるときには、Security Manager だけを使用してください。Security Manager が制御する設定は、オペレーティング システムによって異なります。IPS デバイスの場合、Security Manager は設定全体を制御します。IOS、ASA、PIX、FWSM の各デバイスの場合、Security Manager が制御するデバイス設定のさまざまな側面を柔軟に制御できます。Security Manager でルーティング ポリシーなど機能のポリシーを作成しない場合、Security Manager はデバイスでその機能を制御しません。機能のポリシーを作成

すると、Security Managerに定義した設定でデバイスの設定が上書きされます。管理設定では、デバイスに使用可能なポリシーのタイプを制御して、Security Manager で機能のポリシーを表示または変更できないようにすることができます。使用可能な機能を参照し、Security Managerでの管理対象にするかどうかを制御するには、**[ツール（Tools）] > [Security Manager管理（Security Manager Administration）]** を選択し、[ポリシー管理（Policy Management）] を選択します。Security Manager は、VPN 関連のポリシーを管理します。

関連項目

- Workflow 以外のモードでの展開 （4 ページ）
- Workflow モードでの展開タスク フロー （6 ページ）
- [Deployment] ページ
- [Policy Management] ページ

Workflow 以外のモードでの展開

以降のトピックは、Workflow 以外のモードで展開を理解するのに役立ちます。

- Workflow 以外のモードでの展開 （4 ページ）
- Workflow 以外のモードでのジョブの状態 （5 ページ）

Workflow 以外のモードでの展開タスク フロー

Workflow 以外のモードでの展開タスク フローは、3 つの簡単な手順で構成されています。

1. **ジョブの作成**：次のいずれかを実行すると、展開ジョブが作成されます。
   - [メイン（Main）] ツールバーの [変更の送信と展開（Submit and Deploy Changes）] ボタンをクリックするか、**[ファイル（File）] > [送信して展開（Submit and Deploy）]** を選択します。

（注） これらのオプションは、チケット管理が有効になっている場合は使用できません。

   - **[ファイル（File）] > [展開（Deploy）]** を選択します。
   - **[管理（Manage）] > [展開（Deployments）]** を選択し、[展開（Deploy）] をクリックします。

1. **ジョブの定義**：どのデバイスに設定を展開するのか、直接デバイスに展開するのかファイルに展開するのかなど、パラメータを指定します。

   この手順では、設定をプレビューし、その設定を以前に展開した設定またはデバイスで現在実行中の設定と比較することもできます。

（注） あるジョブのために選択したデバイスをそれ以外のジョブに含めることはできません。この制約により、ポリシーを展開する順序が常に正しいものとなります。ただし、展開スケジュールに指定されているデバイスは含めることができます。

2. **ジョブの展開**：ジョブを展開すると、生成したCLIが直接または中間転送サーバー（AUS、CNS、TMSなど）経由でデバイスに送信されるか、または出力ファイルに送信されます。宛先（デバイスまたはファイル）は、ジョブを定義するときに選択します。転送サーバはデバイスのプロパティで指定します。展開方式と転送サーバを定義する方法については、展開方法について （10 ページ）を参照してください。

Workflow 以外のモードでのジョブの状態

Workflow 以外のモードでは、[Deployment Manager] ウィンドウの [Status] 列に、各ジョブの状態が表示されます。次の表に、Workflow 以外のモードでのジョブの有効な状態とその説明を示します。詳細については、[Deployment Manager] ウィンドウ （19 ページ）を参照してください。

表 *2 : Workflow* 以外のモードでのジョブの状態

状態	説明
導入済み	ジョブに含まれるすべてのデバイスの設定が、デバイスまたは設定ファイルに正常に展開されました。これで、ジョブに含まれるデバイスを別のジョブに追加できます。
展開	ジョブに生成された設定を、デバイスまたは Security Manager サーバのディレクトリに展開しています。[Deployment Status] ウィンドウがまだ開かれていない場合には、[Deployment Manager] ウィンドウでジョブの経過表示をモニタできます。
中断	ジョブが手動で停止されました。これで、ジョブに含まれるデバイスを別のジョブに追加できます。
失敗しました（Failed）	ジョブに含まれる 1 つまたは複数のデバイスへの展開に失敗しました。これで、ジョブに含まれるデバイスを別のジョブに追加できます。
Rolling Back	Security Manager は、展開ジョブに含まれるデバイスの以前の設定に復帰し、その設定を展開しています。[Rolling Back] 状態にあるジョブは中断可能です。
Rolled Back	Security Manager は、展開ジョブに含まれるデバイスの以前の設定に復帰し、その設定の展開に成功しました。

Workflow モードでの展開

以降のトピックは、Workflow モードで展開を理解するのに役立ちます。

Workflow モードでの展開タスク フロー

次に、Workflow モードでの代表的なタスク フローを示します（図 1 : ワークフローモードでの展開タスクフロー （7 ページ）を参照）。

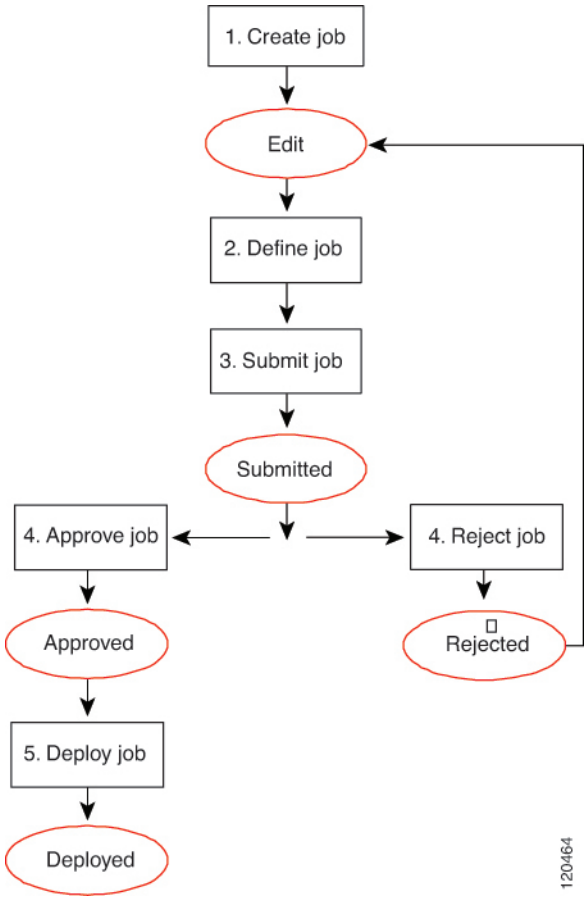
1. **ジョブの作成**：設定をデバイスに展開する前に、展開ジョブを作成する必要があります。
2. **ジョブの定義**：ジョブを作成するときは、どのデバイスに設定を展開するのか、直接デバイスに展開するのかファイルに展開するのか、いつジョブを実行するのかなどのパラメータを指定します。
3. **ジョブの送信**：組織によっては、適切な権限を持つ別のユーザがジョブを承認しなければジョブを展開できないようになっていることがあります。この場合、展開ジョブのアプルーバによって Workflow モードがイネーブルになり、送信者はこのユーザにジョブを送信して確認してもらう必要があります。アプルーバはジョブを確認し、承認または拒否を行います。
4. **ジョブの承認または拒否**：展開ジョブのアプルーバを割り当てて Workflow モードで作業している場合は、アプルーバがジョブを確認し、承認または拒否の決定を下します。ジョブが承認された場合、送信者はジョブを展開できます。ジョブが拒否された場合、送信者はジョブを廃棄し、ジョブを最初からやり直すかまたは修正を加えてから再送信します。

アプルーバを割り当てずに Workflow モードで作業している場合は、ジョブを自分自身で承認できます。

- **ジョブの展開**：ジョブを展開すると、生成したCLIがデバイス、中間転送サーバー（AUS、CNS、TMS など）、またはファイルに送信されます。宛先（デバイスまたはファイル）は、ジョブを定義するときに選択します。転送サーバはデバイスのプロパティで指定します。展開方式と転送サーバを定義する方法については、 展開方法について （10 ページ）を参照してください。

（図 1 : ワークフローモードでの展開タスクフロー （7 ページ）に赤で表示される）ジョブの状態については、 Workflow モードでのジョブの状態 （7 ページ）を参照してください。

図 *1 :* ワークフローモードでの展開タスクフロー



Workflow モードでのジョブの状態

Workflow モードでは、[Deployment Manager] ウィンドウの [Status] 列に、各ジョブの状態が表示されます。次の表に、ジョブの有効な状態とその説明を示します。[Deployment Manager] ウィンドウの詳細については、[Deployment Manager] ウィンドウ （19 ページ）を参照してください。

表 *3 : Workflow* モードでのジョブの状態

状態	説明
Edit	ジョブは作成されましたが、現在編集中ではありません。ジョブが [Edit] 状態であるときは、ジョブを開く、承認する（自動承認モード）、廃棄するという操作を実行できます。
Edit-In Use	ジョブは編集用に開いています。ジョブが [Edit Open] 状態であるときは、ジョブを閉じる、承認する、廃棄する、送信するという操作を実行できます。

状態	説明
送信済み（Submitted）	ジョブは確認のために送信されました。ジョブが [Submitted] 状態であるときは、ジョブを表示できますが、編集はできません。[Submitted] 状態の場合、ジョブを表示する、廃棄する、拒否する、承認するという操作を実行できます。この状態になるのは、展開ジョブの承認が必要な場合に Workflow モードがイネーブルになった場合だけです。
承認（Approved）	ジョブは承認され、展開する準備ができています。ジョブが [承認（Approved）] 状態であるときは、ジョブを展開できます。
拒否	ジョブは拒否されました。ジョブが [Rejected] 状態であるときは、ジョブを開いて編集または廃棄できます。この状態になるのは、展開ジョブの承認が必要な場合に Workflow モードがイネーブルになった場合だけです。
破棄（Discarded）	ジョブは廃棄されました。これ以上ジョブに変更を加えることができません。ジョブは、システムから削除されるまで、[Discarded] 状態となってこれまでどおり [Deployment] テーブルに残ります。ジョブに含まれるデバイスを別のジョブに追加できます。
導入済み	ジョブに含まれるすべてのデバイスの設定が、デバイスまたは設定ファイルに正常に展開されました。これで、ジョブに含まれるデバイスを別のジョブに追加できます。
展開	ジョブに生成された設定を、デバイスまたは Security Manager サーバのディレクトリに展開しています。[Deployment Manager] ウィンドウでジョブの経過表示をモニタできます。
中断	ジョブが手動で停止されました。これで、ジョブに含まれるデバイスを別のジョブに追加できます。
失敗しました（Failed）	ジョブに含まれる 1 つまたは複数のデバイスへの展開に失敗しました。これで、ジョブに含まれるデバイスを別のジョブに追加できます。
Scheduled to run at [date]	ジョブは、指定の日時に展開するようにスケジューリングされます。
Rolling Back	Security Manager は、展開ジョブに含まれるデバイスの以前の設定に復帰し、その設定を展開しています。[Rolling Back] 状態にあるジョブは中断可能です。
Rolled Back	Security Manager は、展開ジョブに含まれるデバイスの以前の設定に復帰し、その設定の展開に成功しました。

展開ジョブの承認

デフォルトでは、Security Manager は Workflow 以外のモードで動作します。展開ジョブは、背後で処理され、ユーザはジョブまたはその承認を意識する必要はありません。Workflow モードを使用している場合は、展開ジョブ アプルーバを割り当てるかどうかを選択できます。

アプルーバを割り当てないことにした場合は、ジョブを定義し、承認する権限が与えられます。

新規の設定または変更を加えた設定をデバイスに展開してよいかどうかを、自分よりも強い権限を持つ別のユーザが承認するようになっている場合は、展開ジョブアプルーバを割り当てて Workflow モードを使用します。展開ジョブ アプルーバを割り当てて Workflow モードを使用する場合は、適切な権限を持つ担当者がジョブを確認してそのジョブを承認するか拒否するかを判断する必要があります。この承認プロセスにより、不適切な設定がネットワーク デバイスに到達しなくなり、展開ジョブが効率よくスケジューリングされるようになります。

（注） 展開ジョブの承認は、[Tools] > [Security Manager Administration] > [Workflow] からイネーブルおよびディセーブルにできます。詳細については、[Workflow] ページを参照してください。

展開ジョブと複数のユーザ

個々の展開ジョブ内のパラメータまたはデバイスを定義または変更できるのは、一度に 1 人のユーザだけです。ただし、複数のユーザが同じ展開ジョブに対して順に作業することはできます。あるユーザが展開ジョブを閉じれば、別のユーザがそのジョブを開いて変更を加えることができます。複数のユーザが、それぞれ異なる展開ジョブを並行して作業できます。

展開ジョブまたは展開スケジュールにデバイスを含める操作

展開ジョブまたは展開スケジューリングを作成するときは、そのジョブまたはスケジュールに含めるデバイスを選択します。デバイスを含めると、他のジョブまたはスケジュールでのそのデバイスの使用方法に影響を与えます。特定のジョブのデバイスを選択すると、そのジョブが展開、拒否（Workflow モード）、廃棄、または中断されるまで、選択したデバイスは他のジョブに選択できません。このメカニズムにより、複数のユーザが変更を同じデバイスに同時に展開できなくなり、ポリシーがデバイスに正しい順序で展開されます。

一方、デバイスは展開スケジューリングに含め、特定の展開ジョブに選択できます。展開ジョブが実行されている間、デバイスはロックされます。展開ジョブが実行されている間、デバイスを他のジョブに含めることができません。

展開ジョブを作成すると、Security Manager にはポリシーに変更が加えられたものの、まだ展開されていないデバイスが表示されます。このようなデバイスに展開し、ジョブに含めるデバイスをさらに選択できます。必要な数だけデバイスを展開ジョブに追加できます（制限はありません）が、実用上の理由からジョブあたりのデバイス数を制限することを推奨します。多数のデバイスを選択した場合や、大きな設定ファイルがあるデバイスをいくつか選択した場合に

は、展開ジョブが失敗することがあります。展開で障害が発生した場合は、選択されたデバイスの数を減らしてジョブを送信し直してください。

VPN の場合、Security Manager は、ジョブに選択したデバイスに定義されているポリシーの影響を受けるデバイスに対してコマンドを生成する必要があります。そのため、VPN を構成するデバイスを選択すると、Security Manager は他の関連するデバイスをジョブに追加します。たとえば、スポークでトンネルポリシーを定義し、ジョブ用にそのスポークを選択した場合、Security Manager はスポークに割り当てられたハブをジョブに追加します。ジョブの生成中、VPN 設定が完了し、トンネルを確立できるように、Security Manager は両方のピア用のコマンドを生成します。VPN に関連付けられたデバイスのいずれも選択しない場合、Security Manager はデバイスを取り外すと VPN が正しく機能しなくなることを警告します。

展開方法について

Security Manager では、主に 3 つの方法で設定をデバイスに展開できます。直接デバイスに展開する方法、設定ファイルに展開する方法（その後手動でデバイスに適用する必要があります）、および中間サーバに展開する方法（直接デバイスに展開する方法と同じように処理されます）です。システムにデフォルトの展開方法は、直接デバイスに展開する方法です。

デバイスを Security Manager に追加するときに、そのデバイスで使用する展開方法を選択します。これにより、（ファイルではなく）デバイスへの展開に使用する方法が決まります。展開ジョブを作成すると、展開方法のデフォルトが一体的にジョブに適用されます。これにより、設定ファイルを作成するかどうか、あるいはデバイスに選択した方法で設定をデバイスに送信するかどうかが決まります。このデフォルトは、管理設定で制御します（**[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）]** を選択し、[展開（Deployment）] を選択。[Deployment] ページを参照）。展開ジョブを作成する際に、[ジョブの作成（Create Job）] ウィンドウで [展開方法の編集（Edit Deploy Method）] をクリックして、デバイスごとに展開先をファイルまたはデバイスに変更することもできます。Workflow 以外のモードを使用している場合は、Workflow 以外のモードでの設定の展開 （35 ページ）を参照してください。Workflow モードを使用している場合は、展開ジョブの作成および編集 （44 ページ）を参照してください。

使用する方法は、組織が採用するプロセスおよび手順、および特定のデバイス タイプでサポートされているトランスポート プロトコルによって異なります。Configuration Engine（CNS）または Auto Update Server（AUS）を使用している場合は、それぞれの展開方法を使用してください。ダイナミック IP アドレスを使用するデバイスには、これらのいずれかを使用する必要があります。スタティック IP アドレスを使用するデバイスの場合、IOS、PIX、ASA、IPS、スタンドアロン FWSM の各デバイスには SSL（HTTPS）、および Catalyst シャーシ経由の FWSM には SSH を使用します。一部のデバイスに Token Management Server（TMS）を使用している場合は、Security Manager とともにその方法も使用できます。

以降のトピックでは、展開方法についてさらに詳しく説明します。

- デバイスへの直接展開 （11 ページ）
- 中間サーバを使用したデバイスへの展開 （12 ページ）
- ファイルへの展開 （13 ページ）

• アウトオブバンド変更の処理方法について （14 ページ）

デバイスへの直接展開

デバイスに直接展開することを選択した場合、Security Manager はそのデバイスのデバイスプロパティに定義されているトランスポートプロトコルを使用します（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）。プロトコルは一般に、Security Manager 管理設定の [デバイス通信（Device Communication）] ページに定義されているデフォルトプロトコルです（[Device Communication] ページを参照）。表 4 : デフォルトの展開トランスポート プロトコル （11 ページ）には、デフォルトのトランスポートプロトコル設定の一部が一覧表示されます。

展開方法として [Device] を選択した場合、デバイスに AUS や Configuration Engine などの転送サーバを設定すると、展開に影響が及びます。中間転送サーバを使用している場合、設定展開はサーバを通過します。中間サーバの使用方法の詳細については、中間サーバを使用したデバイスへの展開 （12 ページ）を参照してください。

前回の展開以降にアウトオブバンド変更をデバイスに加えた場合には、展開にも影響が及ぶことがあります。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 （14 ページ）を参照してください。

展開中、Security Manager は前回の展開以降に加えられた変更だけをデバイスに送信します。

注意 デバイスに展開する前に、そのデバイスで少なくとも 1 つのポリシーを設定する必要があります。ポリシーを 1 つも割り当てずにデバイスに展開すると、そのデバイスの現在の設定が空の設定で上書きされます。

表 *4 :* デフォルトの展開トランスポート プロトコル

デバイスタイプ	トランスポートプロトコル（Transport Protocol）	説明
ASA、IOS 12.3 以降のルータ、FWSM、PIX ファイアウォール、IPS センサー	SSL（HTTPS）（デフォルト）	Security Manager は、HTTPS とも呼ばれる Secure Socket Layer（SSL）プロトコルを使用して、設定をデバイスに展開します。Security Manager は、このプロトコルを使用して、設定ファイルを暗号化してからデバイスに送信します。

デバイスタイプ	トランスポートプロトコル（Transport Protocol）	説明
Catalyst 6500/7600 およびその他の Catalyst スイッチ	SSH	Security Manager は、Secure Shell（SSH; セキュアシェル）を使用して、設定をデバイスに展開します。これにより、セキュアでないチャネルでも強固な認証と安全な通信を確保できます。Security Manager は、SSHv1.5 と SSHv2 の両方をサポートします。デバイスに接続されると、Security Manager はどのバージョンを使用するかを決定し、そのバージョンを使用してダウンロードします。
IOS 12.2 ルータおよび 12.1 ルータ	Telnet	Security Manager は、Telnet プロトコルを使用して、設定をデバイスに展開します。

関連項目

- デバイス通信設定および証明書の管理
- デバイス OS バージョン不一致の処理 （15 ページ）

中間サーバを使用したデバイスへの展開

Auto Update Server（AUS）、Cisco Networking Services（CNS）Configuration Engine、Token Management Server（TMS）などの中間サーバを介して設定を展開する操作は、直接デバイスに展開する操作を若干変更したものです。展開方法を選択するときに、[Device] を選択します。Security Manager は、設定更新を中間サーバに送信します。この中間サーバで、デバイスがその更新を取得するか（AUS および CNS の場合）、またはユーザがその更新を eToken にダウンロードできます（TMS の場合）。

デバイス インターフェイスにダイナミック IP アドレスを使用している場合（つまり、IP アドレスを DHCP サーバから取得する場合）には、中間サーバを使用する必要があります。中間サーバは、スタティック IP アドレスでも使用できます。ただし、対話形式の CLI コマンドを使用する機能を設定する場合には、Configuration Engine ではダイナミック IP アドレスを持つ IOS デバイスを管理できません。次の機能に影響が及びます。

- 証明書登録：
  - **crypto pki trustpoint**
  - **crypto isakmp client configuration group**
  - **crypto key generate rsa**
- IPS シグニチャ設定（**ip ips signature-category**）

- IP Authproxy バナー（**ip auth-proxy-banner**）
- Catalyst デバイス インターフェイス スイッチポート（**interface switchport**）

中間サーバを使用するようにデバイスを設定した場合、Security Manager はその中間サーバを使用します。以降のトピックでは、中間サーバを使用する場合に必要な設定手順について説明します。

- Auto Update Server または CNS Configuration Engine を使用した設定の展開 （52 ページ）
- Token Management Server への設定の展開 （54 ページ）

前回の展開以降にアウトオブバンド変更をデバイスに加えた場合には、展開に影響が及ぶことがあります。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 （14 ページ）を参照してください。

展開中、Security Manager はサーバのタイプに基づいて設定変更を送信します。

- PIX デバイスおよび ASA デバイスの Auto Update Server（スタンドアロンまたは Configuration Engine で稼働）：Security Manager は Auto Update Server にすべての設定を送信し、デバイスはサーバから設定を取得します。デルタ設定は送信されません。
- IOS デバイスの Configuration Engine：Security Manager は Configuration Engine にデルタ設定を送信し、デバイスはエンジンから設定を取得します。
- TMS：Security Manager は TMS サーバにデルタ設定を送信します。サーバから eToken に設定をダウンロードし、デバイス上にロードできます。

関連項目

- デバイス通信設定および証明書の管理
- [Device Communication] ページ

ファイルへの展開

設定を構成ファイルに展開することを選択した場合、Security Manager は 2 つのファイルを作成します。デルタ設定用の *device_name* _delta.cfg と、完全な設定用の *device_name* _full.cfg です。展開スケジューリングから生成されたジョブによってファイルが作成された場合、その名前にはタイム スタンプが含まれています。設定ファイルは、TFTP を使用してデバイスにアップロードできるように、TFTP 形式になっています。

ヒント IPS デバイスの場合には、設定をファイルに展開できません。

ファイルに展開する場合は、ユーザ自身が設定をデバイスに転送します。Security Manager は、ユーザがこの転送を完了したものと想定するため、次回同じデバイスに展開すると、生成される差分コマンドは前回の展開の設定に基づくものになります。何らかの理由で前回の変更がデ

バイスに適用されなかった場合、新規デルタ設定ではデバイス設定がデバイスに展開されず、Security Manager に反映されません。

注意 Security Manager は、ユーザがデルタ設定を適用したことを想定している一方、デルタが展開されたかどうかを判断できないことも想定しています。このため、Security Manager はデバイスに直接実行された最新の展開に基づいた設定の内部ビューを維持します。デルタを適用すると、デルタの変更はアウトオブバンド変更と見なされます。次回のデバイスへの展開時に、アウトオブバンド変更設定によって展開がキャンセルされる場合があります。ファイルへの展開とデバイスへの展開を混在させる場合は、デバイスにファイルの展開を適用したあとにポリシーを再検出する必要があります。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 （14 ページ）を参照してください。

ファイル展開用のデフォルトディレクトリを設定するには、[ツール（Tools）]>[Security Manager 管理（Security Manager Administration）] を選択し、[展開（Deployment）] を選択します（[Deployment] ページを参照）。デフォルトの展開方法に [File] を選択した場合は、そのデフォルトディレクトリも選択します。展開ジョブを作成するときに、そのジョブ用のこのディレクトリを変更できます。

設定をファイルに展開する処理は、デバイスがネットワークにまだ配置されていない場合（グリーンフィールド展開と呼ばれます）、独自のメカニズムで設定をデバイスに転送する場合、または遅延展開を採用する場合に便利です。ファイルに展開するとき、多数のデバイスを選択した場合や、大きな設定ファイルがあるデバイスをいくつか選択した場合には、展開ジョブが失敗することがあります。展開で障害が発生した場合は、選択されたデバイスの数を減らしてジョブを送信し直してください。

ヒント ファイルに展開するときは、展開中にデバイスとの対話を必要とするコマンドを使用しないでください。展開前に設定をプレビューして、そのようなコマンドがファイルにないことを確認することを推奨します。詳細については、設定のプレビュー （55 ページ）を参照してください。

アウトオブバンド変更の処理方法について

Security Manager は、アウトオブバンド変更を手動または Security Manager の管理外でデバイスに加えられた変更であると見なします。たとえば、デバイスに直接ログインし、CLI を介してコンフィギュレーションコマンドを入力した場合などが相当します。ところが、アウトオブバンド変更には、デバイスではなくファイルに設定を展開する際に Security Manager が作成するデルタ変更のアプリケーションも含まれます。

（ファイルではなく）デバイスに展開する際に、新規設定がデバイス上の現在の設定と比較されるようになっている展開方法を選択した場合は、[アウトオブバンド変更動作（Out of Band Change Behavior）] 設定でアウトオブバンド変更が検出されたときに、その変更をどのように処理するかを指定できます。ファイルへの展開では、設定値は適用されません。

新規デバイス設定を Security Manager Configuration Archive に格納されている最新のバージョンと比較する場合は、この設定値は無視されます。アウトオブバンド変更のデフォルトの処理方法は、[Tools] > [Security Manager Administration] > [Deployment] に設定されます。詳細については、[Deployment] ページを参照してください。[デバイス参照設定の展開（Deploy to Device Reference Configuration）] および [アウトオブバンド変更の検出時（When Out of Band Changes Detected）] の設定を探します。

アウトオブバンド変更の処理に関するオプションは次のとおりです。

- [変更を上書きして警告を表示（Overwrite changes and show warning）]：設定が展開されると、Security Manager はデバイスの現在の設定をアップロードし、自身のデータベースに格納されている設定と比較します。デバイスに手動で変更が加えられていた場合、Security Manager は展開を続行し、展開の続行を通知する警告を表示します。アウトオブバンド変更は、デバイスから削除されます。
- [展開のキャンセル（Cancel deployment）]：設定が展開されると、Security Manager はデバイスの現在の設定をアップロードし、自身のデータベースに格納されている設定と比較します。デバイスに手動で変更が加えられていた場合、Security Manager は展開を取り消し、展開の取り消しを通知する警告を表示します。設定変更をデバイスに展開するには、アウトオブバンド変更を手動で削除するか、または Security Manager で同じ設定を行う必要があります。
- [変更を確認しない（Do not check for changes）]：Security Manager は、変更を確認せずに、変更をデバイスに展開します。警告が表示されずに、アウトオブバンド変更がデバイス設定から削除されます。

設定を展開する前に、デバイスにアウトオブバンド変更があるかどうかを検出し、そのような変更があれば Security Manager ポリシーに再作成するのか、Security Manager に変更の上書きを許可するのかを分析することを推奨します。詳細については、アウトオブバンド変更の検出および分析 （57 ページ）を参照してください。

関連項目

- デバイスへの直接展開 （11 ページ）
- 中間サーバを使用したデバイスへの展開 （12 ページ）
- ファイルへの展開 （13 ページ）

デバイス OS バージョン不一致の処理

変更を加えた設定ファイルを直接デバイスに展開する前に、Security Manager は通常、デバイスから現在実行中の設定ファイルをアップロードし、デバイスで実行されている OS バージョンを Security Manager データベースに格納されている OS バージョンと照合します（デバイスの設定ではなく、アーカイブされた設定が使用されように設定できます）。Security Manager は、OS バージョンが相互に一致するのか異なるのかに応じて処理を実行します。

Security Manager は設定を展開し、警告を表示する場合もあれば、設定を展開できない場合もあります。Security Manager が設定を展開するのは、次の場合です。

- デバイスに新しいマイナー バージョンがある場合。たとえば、Security Manager に示されている ASA 8.1(1) ではなく ASA 8.1(2) であるなど。
- デバイスに下位のマイナー バージョンがある場合。たとえば、ASA 8.1(2) ではなく ASA 8.1(1) であるなど。

デバイスが OS の新規メジャー バージョンを実行しているとき（たとえば、Security Manager に示されている ASA 7.2 ではなく ASA 8.0 など）や、デバイスが下位メジャー バージョン（8.0 ではなく 7.2）を実行している場合には、Security Manager は設定を展開しません。

次の表に、OS バージョンが相互に一致するのか異なるのかに応じて Security Manager が実行する処理を示します。表では、一例として ASA デバイスを使用していますが、処理はすべてのサポート対象デバイス タイプに適用されます。

表 *5: OS* バージョンが一致するか異なるかに応じた展開処理

シナリオ	**Security Manager** データベースに格納された **OS** バージョン	デバイス上の **OS** バージョン	展開に使用される **OS** バージョン	操作
バージョンの一致	ASA 8.2(1)	ASA 8.2(1)	ASA 8.2(1)	何の警告もなく、展開が進みます。
デバイスに新しいマイナー OS バージョンがある。	ASA 8.1(1)	ASA 8.1(2)	ASA 8.1(2)	Security Manager データベースの OS バージョンと異なる OS バージョンが、デバイスで検出されたことを警告します。 Security Manager は、デバイスで稼働している OS バージョンに基づいて CLI を生成します。
デバイスに新しいマイナー OS バージョンがあるが、そのバージョンは Security Manager で直接サポートされていない。	ASA 8.0(2)	ASA 8.0(4)	ASA 8.0(3)	Security Manager データベースの OS バージョンと異なる OS バージョンが、デバイスで検出されたことを警告します。 Security Manager は、実行中の OS バージョンと下位互換性があるサポート対象の OS バージョンに基づいて、CLI を生成します。

シナリオ	Security Manager データベースに格納された OS バージョン	デバイス上の OS バージョン	展開に使用される OS バージョン	操作
デバイスに新規メジャーOSバージョンがある。	ASA 7.2(4)	ASA 8.2(1)	なし。展開に失敗。	Security Manager データベースの OS バージョンと異なる OS バージョンが、デバイスで検出されたことを示すエラーを報告します。 このミスマッチを修正するまで、Security Manager は処理を継続できません。インベントリからデバイスを削除し、再度追加してからデバイスポリシーを検出してください。
デバイスに古いマイナーOSバージョンがある。	ASA 8.1(2)	ASA 8.1(1)	ASA 8.1(1)	Security Manager データベースの OS バージョンと異なる OS バージョンが、デバイスで検出されたことを警告します。 Security Manager は、デバイスで稼働している OS バージョンに基づいて CLI を生成します。
デバイスに古いメジャーOSバージョンがある。	ASA 8.2(1)	ASA 7.2(4)	なし。展開に失敗。	Security Manager データベースの OS バージョンと異なる OS バージョンが、デバイスで検出されたことを示すエラーを報告します。 このミスマッチを修正するまで、Security Manager は処理を継続できません。インベントリからデバイスを削除し、再度追加してからデバイスポリシーを検出してください。

Deployment Manager および Configuration Archive の概要

Deployment Manager および Configuration Archive は、展開およびデバイス設定を管理するときに使用する主要なツールです。以降のトピックでは、これらのツールの概要を示します。

• Deployment Manager でできること （18 ページ）
• [Deployment Manager] ウィンドウ （19 ページ）

- [Deployment Schedules] タブ、Deployment Manager （25 ページ）
- [Configuration Archive] ウィンドウ （29 ページ）

Deployment Manager でできること

Deployment Manager では、展開ジョブおよび展開スケジュールを作成および管理します。次の利点があります。

- 設定のプレビューと比較：設定ファイルをデバイスに展開する前に、提示された設定ファイルをプレビューできます。また、提示された設定ファイルを、デバイスから前回インポートされたファイルまたはデバイスで現在実行中のファイルと比較することもできます。

デバイスへの展開が成功したあと、ダウンロードした設定コマンドのトランスクリプトとデバイスの応答を表示できます。詳細については、 設定のプレビュー （55 ページ）を参照してください。

- 展開ジョブの中断：実行中の場合も含め展開ジョブを停止できます。ただし、実行中のジョブを中断しても、デバイスにすでに再設定された設定およびデバイスに現在再設定中の設定はロールバックされません。展開がまだ開始されていないデバイスだけが再設定できません。詳細については、 展開ジョブの中断 （69 ページ）を参照してください。
- 以前の設定へのロールバック：設定をデバイスに展開し、その後新しい設定に何か問題があることが明らかになった場合は、そのデバイスの以前の設定に戻って展開できます。詳細については、 Deployment Manager を使用したデバイスへの設定のロールバック （88 ページ）を参照してください。
- 展開ジョブの状態の表示：エラーに関する情報、提示された設定、ダウンロードのトランスクリプトなど、特定のデバイスへの展開に関する情報を表示できます。詳細については、 ジョブおよびスケジュールの展開ステータスおよび展開履歴の表示 （32 ページ）を参照してください。
- 展開ジョブのスケジューリング：展開スケジュールを作成して、一定の間隔で展開ジョブを生成できます。Workflow モードでは、ジョブを展開するときに、将来の時刻に開始するように展開ジョブをスケジューリングすることもできます。ジョブをスケジューリングすると、デバイスでのトラフィックが少ない時間に展開を実施できます。詳細については、次の項を参照してください。
  - 展開スケジュールの作成または編集 （70 ページ）
  - Workflow モードでの展開ジョブの展開 （50 ページ）
- 展開ジョブ履歴のロギング（Workflow モード限定）：ジョブのトランザクションの履歴を表示できます。トランザクションには、ジョブの承認などさまざまなユーザが開始したジョブ状態の変更と、その状態変更に関連するコメントが表示されます。詳細については、 ジョブおよびスケジュールの展開ステータスおよび展開履歴の表示 （32 ページ）を参照してください。

[Deployment Manager] ウィンドウ

[Deployment Manager] ウィンドウは、展開ジョブおよび展開スケジュールを管理するときに使用します。展開ジョブのリストを表示し、ジョブ詳細を参照し、設定をデバイスに展開および再展開できます。また、展開ジョブを中断し、選択したデバイスで以前の設定にロールバックし、スケジュールを作成して展開ジョブを自動的に生成できます。このほか、展開ジョブおよび展開スケジュールに加えた変更を追跡することもできます。

（注） Deployment Manager で使用できるボタンは、使用している Workflow モードによって異なります。

ナビゲーション パス

[メイン（Main）] ツールバーの [展開マネージャ（Deployment Manager）] ボタンをクリックするか、または[管理（Manage）] > [展開（Deployments）] を選択します。

関連項目

- 展開プロセスの概要 （2 ページ）
- ジョブおよびスケジュールの展開ステータスおよび展開履歴の表示 （32 ページ）
- Workflow 以外のモードでの設定の展開 （35 ページ）
- Workflow モードでの展開ジョブの展開 （50 ページ）
- Auto Update Server または CNS Configuration Engine を使用した設定の展開 （52 ページ）
- Token Management Server への設定の展開 （54 ページ）
- デバイス通信設定および証明書の管理

フィールド リファレンス

表 *6 : [Deployment Manager]* ウィンドウ（*Workflow* モード）

要素	説明
[展開ジョブ（Deployment Job）] タブ このタブには、個々の展開ジョブが表示されます。上部ペインでジョブを選択すると、その詳細が下部ペインのタブに表示されます。 フィルター オプション（Filter Options） 4.14 以降、Cisco Security Manager には、名前（展開ジョブ名）、ステータス、変更者、およびデバイス名に基づいて展開ジョブを検索するためのフィルタオプションが用意されています。フィルタ条件を指定したら、[適用（Apply）] をクリックします。グリッドに検索結果が表示されます。テーブル内のジョブを選択すると、その詳細が下部ペインのタブに表示されます。	
名前	ジョブの名前。
直前のアクション	ジョブまたは状態が変更された日付と時刻。クライアントのタイム ゾーンではなく、サーバのタイム ゾーンに基づきます。
ステータス	各ジョブの状態。有効な状態は、Workflow モードによって異なります。状態については、次のトピックを参照してください。 • Workflow 以外のモードでのジョブの状態 （5 ページ） • Workflow モードでのジョブの状態 （7 ページ）
Changed By	ジョブを変更したユーザの名前。
説明	ジョブの説明。個別のダイアログボックスで説明を表示するには、アイコンをダブルクリックします。
ジョブ タイプ（Job Type）	スケジュールの点から見たジョブのタイプ。**one time** ジョブは定期的に繰り返されるジョブから作成されたものではありませんが、**recurring** ジョブは作成されたものです。
[Create] ボタン （Workflow モード限定）	Workflow モードでは、新規ジョブを作成するには、このボタンをクリックしします。[Create a Job] ダイアログボックスが開きます。 展開ジョブの作成および編集 （44 ページ）を参照してください。
[Open] ボタン （Workflow モード限定）	Workflow モードでは、選択したジョブを開くには、このボタンをクリックします。[Edit a Job] ダイアログボックスが開きます。 展開ジョブの作成および編集 （44 ページ）を参照してください。

要素	説明
[Close] ボタン （Workflow モード限定）	Workflow モードでは、選択したジョブを閉じ、ジョブを開いていた間に加えたすべての変更を保存するには、このボタンをクリックします。[Edit Open] 状態または [Submit Open] 状態であるときは、ジョブを閉じることができます。通常、ジョブを閉じる必要はありません。一般に、展開対象のジョブは送信、承認、展開、またはスケジューリングすることになるためです。ただし、Security Manager サーバが突然使用不可能になったり、ログイン セッションがタイムアウトしたりした場合は、ジョブが [Edit Open] 状態のままになることがあります。この場合、ジョブを選択し、[Close]をクリックして、手動でジョブを閉じることができます。
\[Submit\] ボタン[Submit ぼたん] （Workflow モード限定）	Workflow モードでは、承認のために選択したジョブを送信するには、このボタンをクリックします。ジョブは、[Edit] 状態または [Edit Open] 状態にある場合に送信できます。[Submit Deployment Job] ダイアログボックスが開きます。 展開ジョブの送信 （48 ページ）を参照してください。 このボタンは、展開ジョブ アプルーバを割り当てて Workflow モードを使用している場合にだけアクティブになります。
[Reject] ボタン （Workflow モード限定）	Workflow モードでは、デバイス用に生成された設定に満足できない場合、このボタンをクリックして、選択したジョブを拒否します。展開ジョブ アプルーバを割り当てて Workflow モードを使用している場合にだけ、ジョブを拒否できます。ジョブを拒否したあと、そのジョブを開いて編集または廃棄できます。 展開ジョブの承認と拒否 （49 ページ）を参照してください。 任意で、ジョブを拒否する理由を入力できます。
[Approve] ボタン （Workflow モード限定）	Workflow モードでは、選択したジョブを承認するには、このボタンをクリックします。ジョブを承認したあと、そのジョブを展開できます。 展開ジョブの承認と拒否 （49ページ）を参照してください。 任意で、ジョブを承認する理由を入力できます。
[Discard] ボタン （Workflow モード限定）	Workflow モードでは、選択したジョブを廃棄するには、このボタンをクリックします。[Deployed]、[Deployment Failed]、[Aborted] を除く任意の状態である場合に、ジョブを廃棄できます。いったん廃棄したジョブは、編集、送信、承認、および展開できません。ジョブが [Workflow 設定（Workflow settings）] ページの設定に従って自動的にシステムから削除されるか、または手動でシステムから削除するまで、ジョブ状態は「Discarded」として表示されます（詳細については、[Workflow] ページを参照してください）。 任意で、ジョブを廃棄する理由を入力できます。 展開ジョブの廃棄（51 ページ）を参照してください。

要素	説明
[Deploy] ボタン （すべてのモード）	生成されたCLIコマンドをデバイスまたはファイルに展開するには、このボタンをクリックします。このボタンの動作は、Workflowモードによって異なります。 • （Workflow以外のモード）展開ジョブを作成するには、このボタンをクリックします。まだ送信していない変更がある場合は、まず、その変更を送信するように求められます。[Deploy Saved Changes] ダイアログボックスが開き、どのデバイスをジョブに含めるかを選択できます。このボタンは、テーブルで選択されている展開ジョブには機能しないことに注意してください。その代わり、新規に展開ジョブを作成します。 Workflow以外のモードでの設定の展開 （35ページ）を参照してください。 • （Workflowモード）選択したジョブを展開するには、このボタンをクリックします。ジョブが [Approved] 状態である場合は、[Deploy Job] ダイアログボックスが開きます（ Workflowモードでの展開ジョブの展開 （50ページ）を参照）。 ジョブが [Deployed]、[Failed]、[Aborted] のいずれかの状態である場合は、[Redeploy Job] ダイアログボックスが開きます。 デバイスへの設定の再展開 （67ページ）を参照してください。
[Generate Report] ボタン （すべてのモード）	選択したジョブの展開ステータス 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HTMLおよびPDFフォーマットで生成できます。ジョブは [Deployed]、[Failed]、[Rolled Back]、または [Aborted] のいずれかの状態である必要があります。 展開ステータスレポートには、ジョブの概要および完全な設定とデルタ設定、およびジョブのトランスクリプトが含まれます。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 （すべてのモード）	Security Managerサーバからジョブ情報をリロードするには、このボタンをクリックします。テーブルの下に [自動リフレッシュがオン（Auto Refresh is On）] というメッセージが表示された場合は、ジョブリストが定期的に自動リフレッシュされます。 （注） 自動リフレッシュ設定は、展開の管理設定で設定します。[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [展開（Deployment）] の順に選択してください。

要素	説明
[Redeploy] ボタン （Workflow 以外のモード限定）	Workflow 以外のモードでは、選択したジョブを再展開するには、このボタンをクリックします。これにより、同じ CLI コマンドが生成されて、元のジョブで選択されていたのと同じデバイスまたはファイルに展開されます。[Redeploy Job dialog box] ダイアログボックスが開きます。デバイスへの設定の再展開 （67 ページ）を参照してください。 （Workflow モードでは、[Deploy] ボタンをクリックすると、選択したジョブの設定が再展開されます）
[Abort] ボタン （すべてのモード）	[Deploying]、[Scheduled]、[Rolling Back] のいずれかの状態である場合は、このボタンをクリックすると、選択したジョブが中断します。処理を確認するように求める警告が表示されます。展開ジョブの中断 （69 ページ）を参照してください。
[Rollback] ボタン （すべてのモード）	このボタンをクリックして、以前に展開した設定を選択したジョブのデバイスに展開します。[Deployment Rollback] ダイアログボックスが開きます（Deployment Manager を使用したデバイスへの設定のロールバック （88 ページ）を参照）。
[サマリー（Summary）] タブ	選択した展開ジョブの状態に関する要約情報を表示します。具体的には、ジョブの状態、展開ジョブの名前、ジョブに含まれているデバイスの数、正常に展開されたデバイスの数、展開時にエラーが発生したデバイスの数などです。

要素	説明
[Details] タブ	選択したジョブの詳細な情報を表示します。表には、ジョブに含まれている各デバイス、展開が正常に完了したか失敗したか、デバイスのジョブの一部である変更が含まれるチケット、およびデバイスの警告、エラー、失敗の数をまとめた一覧が表示されます。表でデバイスを選択すると、そのデバイスの結果が表示されます。 • [Config] 列のアイコンをダブルクリックすると、設定が表示されます（設定のプレビュー （55 ページ）を参照）。インベントリからデバイスを削除した場合は、設定およびトランスクリプトが使用できないことがあります。 • デバイスに展開していた場合は、[トランスクリプト（Transcripts）] カラムのアイコンをダブルクリックすると、デバイスに送信されるコマンドのトランスクリプトとデバイスの応答が表示されます。 展開トランスクリプトの表示 （78 ページ）を参照してください。 • チケット管理が有効になっている場合、[最終チケット（Last Ticket(s)）] カラムには、デバイスの展開の一部である変更を含むチケットのチケット ID が表示されます。チケット ID をクリックして、作成者や最終更新日など、チケットに関する追加情報を表示できます。外部チケット管理システムへのリンクが設定されている場合は、チケットの詳細からそのシステムに移動することもできます（[チケット管理（Ticket Management）] ページを参照）。 • デバイスを選択すると、左下にある [Messages] ボックスに、展開に関して生成されたメッセージの概要が表示されます。項目を選択すると、右側にその説明が表示されます。ウィンドウを拡大しないと、[Description] ボックスが表示されないことがあります。問題を解決するために実行した処理があれば、その処理に関する情報も表示されます。
[履歴（History）] タブ（Workflow モード限定）	選択したジョブにこれまで加えられた変更のログを表示します。ログの内容は、状態の変更、変更を行ったユーザ、変更日時（Security Manager サーバの時間が基準）、およびユーザが入力した変更を説明するコメントです。
[Deployment Schedules] タブ このタブは、定期的な展開ジョブをスケジューリングする場合に使用します。このタブの詳細については、 [Deployment Schedules] タブ、Deployment Manager （25 ページ）を参照してください。	

[Deployment Workflow Commentary] ダイアログボックス

Workflow モードを使用している場合に Deployment Manager で処理を実行すると、処理の説明を入力するように求められます。入力した説明は、ジョブまたはスケジュールの履歴に保持されます。

ダイアログボックスのタイトルは、実行している処理を示します。任意でコメントを入力し、[OK] をクリックして処理を実行します。

ナビゲーション パス

Workflow モードでは、Deployment Manager でジョブまたはスケジュールを選択し、適切なボタンをクリックして目的の処理を実行します。

[Deployment Schedules] タブ、Deployment Manager

[Deployment Manager] ウィンドウの [Deployment Schedules] タブは、定期的に繰り返される展開ジョブを作成する場合に使用します。スケジュールに指定した展開時刻になるたびに、スケジューリングしたジョブに基づいて、Security Manager が特定の展開ジョブを作成します。

ナビゲーション パス

[メイン（Main）] ツールバーの [Deployment Manager] ボタンをクリックするか、または **[管理（Manage）] > [展開（Deployments）]** を選択し、上部ペインにある [展開スケジュール（Deployment Schedules）] タブをクリックします。

関連項目

- 展開プロセスの概要　（2 ページ）
- 展開スケジュールの作成または編集　（70 ページ）
- 展開スケジュールの一時停止または再開　（74 ページ）

フィールド リファレンス

表 7 : [Deployment Schedules] タブ、[Deployment Manager] ウィンドウ

要素	説明
[Deployment Schedule] テーブル このテーブルには、展開ジョブ スケジュールが表示されます。テーブル内のスケジュールを選択すると、その詳細が下部ペインのタブに表示されます。 フィルター オプション（Filter Options） 4.14 以降、Cisco Security Manager には、名前（展開スケジュール名）、ステータス、およびデバイス名に基づいて展開スケジュールを検索するためのフィルタオプションが用意されています。フィルタ条件を指定したら、[適用（Apply）] をクリックします。グリッドに検索結果が表示されます。テーブル内のスケジュールを選択すると、その詳細が下部ペインのタブに表示されます。	
名前	ジョブ スケジュールの名前。このスケジュールから作成されたジョブが、この名前とタイム スタンプを使用します。
ステータス	スケジュールの状態。 • [Edit]：Workflow モードでは、スケジュールが作成中です。スケジュールを開き、その設定を変更できます。編集中のスケジュールからはジョブが作成されません。 • [Active]：このスケジュールに従って展開ジョブが作成されます。 • [Suspended]：スケジュールは一時停止されました。そのスケジュールで作成中のジョブはありません。スケジュールを再開するには、そのスケジュールを選択し、[再開（Resume）] をクリックします。
定例（Recurrence）	このスケジュールから展開ジョブが作成される頻度。
Next Run	次回このスケジュールから展開ジョブが作成される日付と時刻。
前回の実行	このスケジュールから最近作成された展開ジョブの日付と時刻。
Schedule End	スケジュールがアクティブではなくなった日付と時刻。スケジュールに終了日がない場合は、[Active Indefinitely] が示されます。
説明	ジョブ スケジュールの説明。説明を表示するには、アイコンをダブルクリックします。
[Create] ボタン	展開ジョブ スケジュールを作成するには、このボタンをクリックします。[Schedule] ダイアログボックスが開き、スケジュールを作成できます（[Schedule] ダイアログボックス （71 ページ）を参照）。

要素	説明
[Open] ボタン	選択したスケジュールを開くには、このボタンをクリックします。[Schedule] ダイアログボックスが開き、スケジュールを表示または変更できます（[Schedule] ダイアログボックス （71 ページ）を参照）。 Workflow以外のモードでは、スケジュールを変更しても、その状態は変更されません。Workflow モードでは、状態が [Edit] に変わり、承認のため再送信する必要があります。
[Close] ボタン （Workflow モード限定）	スケジュールを閉じ、スケジュールを開いていた間に加えたすべての変更を保存するには、このボタンをクリックします。[Edit Open] 状態または[Submit Open] 状態であるときは、スケジュールを閉じることができます。一般に、スケジュールを閉じる必要があるのは、スケジュールが開いたままの状態で Security Manager サーバが使用できなくなった場合だけです。
\[Submit\] ボタン[Submit ぼたん] （Workflow モード限定）	アプルーバを割り当てて Workflow モードを使用している場合は、承認のため、このボタンをクリックして、選択したスケジュールを送信します。[Edit] 状態または [Edit Open] 状態にある場合に、スケジュールを送信できます。任意で、送信の説明を入力できます。Workflowモードでは、電子メールが生成されてアプルーバに送信されます。
[Reject] ボタン （Workflow モード限定）	選択したスケジュールを拒否するには、このボタンをクリックします。任意で、拒否の説明を入力できます。Workflowモードでは、電子メールが生成されてアプルーバおよび送信者に送信されます。
[Approve] ボタン （Workflow モード限定）	選択したスケジュールを承認するには、このボタンをクリックします。任意で、承認の説明を入力できます。Workflowモードでは、電子メールが生成されてアプルーバおよび送信者に送信されます。
[Discard] ボタン	選択したスケジュールを廃棄するには、このボタンをクリックします。スケジュールは、そのスケジュールから作成されたアクティブな展開ジョブがある場合を除き、廃棄できます（ジョブが完了するまで待つか、またはジョブを中断してから、スケジュールを廃棄できます）。 任意で、廃棄の説明を入力できます。Workflow モードでは、電子メールが生成されてアプルーバおよび送信者に送信されます。

要素	説明
[Refresh] ボタン	Security Manager サーバからスケジュール情報をリロードするには、このボタンをクリックします。テーブルの下に [自動リフレッシュがオン（Auto Refresh is On）] というメッセージが表示された場合は、スケジュールリストが定期的に自動リフレッシュされます。 （注） 自動リフレッシュ設定は、展開の管理設定で設定します。[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [展開（Deployment）] の順に選択してください。
[Suspend] ボタン	選択したスケジュールを一時停止するには、このボタンをクリックします。スケジュールを一時停止してもスケジュールは削除されませんが、そのスケジュールに基づいて展開ジョブを作成できなくなります。一時停止を説明するコメントの入力を要求されます。また、電子メールが生成されて、Workflow モードでアプルーバに送信されます。
[再開（Resume）] ボタン	一時停止したスケジュールを再アクティブ化するには、このボタンをクリックします。一時停止を説明するコメントの入力を要求されます。また、電子メールが生成されて、Workflow モードでアプルーバに送信されます。
[サマリー（Summary）] タブ	選択したスケジュールに関する要約情報を表示します。テーブルに表示されるフィールドのほか、要約情報にはスケジュールに含まれているデバイスの数、最後にスケジュールを変更したユーザの ID などがあります。
[Devices] タブ	選択したスケジュールに含まれているデバイスを表示します。ここに表示されるのは、スケジュールから展開ジョブが作成されたときに設定が展開されるデバイスです。デバイスリストを変更するには、[開く（Open）] をクリックし、[スケジュール（Schedule）] ダイアログボックスで [デバイスの追加（Add Devices）] をクリックします。
[履歴（History）] タブ	選択したスケジュールにこれまで加えられた変更のログを表示します。ログの内容は、状態の変更、変更を行ったユーザ、変更日時（Security Manager サーバの時間が基準）、およびユーザが入力した変更を説明するコメントです。

要素	説明
[Jobs] タブ	選択したスケジュールに基づいてこれまで作成された展開ジョブのリストを表示します。情報には、ジョブの名前、ジョブを作成した日付と時刻（クライアント時間ではなくサーバ時間に基づいた時間）、ジョブの状態などがあります。ジョブを選択し、[展開ジョブ（Deployment Job）] タブをクリックすると、選択したジョブが強調表示され、ジョブの詳細を表示できます。 ジョブの状態の詳細については、次の項を参照してください。 • Workflow モードでのジョブの状態 （7 ページ） • Workflow 以外のモードでのジョブの状態 （5 ページ）

[Configuration Archive] ウィンドウ

Configuration Archive は、Security Manager によって管理される各デバイスの設定バージョンを格納します。Cisco Security Manager からデバイスを削除すると、そのデバイスの設定はすべて Configuration Archive からも削除されます。

Configuration Archive は次の場合に使用できます。

- 選択したデバイスの設定展開のトランスクリプトを表示します。
- 設定バージョンを表示し、比較します。
- 展開された設定バージョン間での CLI の相違点を表示します。
- 設定がそのデバイスから作成されたものである場合に、以前の設定バージョンにロールバックします。設定をロールバックするのは、極端な状況にある場合だけとしてください。詳細については、次の項を参照してください。
  - 設定のロールバックについて （80 ページ）
  - ロールバックを使用したアーカイブ済み設定の展開 （89 ページ）
- デバイスで現在実行中の設定をアーカイブに追加します。

デバイスの設定バージョンのリストをソートするには、ソート基準となる列見出しをクリックします。列見出しをクリックすると、行のソートが昇順と降順との間で切り替わります。表示されるフィールドを制御することもできます。そのためには、任意の列見出しを右クリックし、[Show Columns] コマンドの下で目的の列名を選択または選択解除します。

ナビゲーション パス

[管理（Manage）] > [Configuration Archive] を選択します。

関連項目

- [Configuration Archive] ページ
- アーカイブされた設定バージョンの表示および比較 （75 ページ）
- 設定のロールバックについて （80 ページ）
- ロールバックを使用したアーカイブ済み設定の展開 （89 ページ）
- マルチ コンテキスト モードのデバイスのロールバックについて （82 ページ）
- フェールオーバー デバイスのロールバックについて （82 ページ）
- Catalyst 6500/7600 デバイスのロールバックについて （83 ページ）
- IPS および IOS IPS のロールバックについて （84 ページ）
- デバイスの設定バージョンの Configuration Archive への追加 （75 ページ）
- セレクタ内の項目のフィルタリング

フィールド リファレンス

表 8 : [Configuration Archive] ウィンドウ

要素	説明
Device Selector	デバイスインベントリのデバイスを一覧表示します。デバイスを選択すると、アーカイブで使用できるデバイスの設定バージョンが表示されます。次に挙げる情報が右ペインに表示されます。
バージョン ID（Version ID）	設定バージョンのバージョン番号。デフォルトでは、この列は表示されません。この列を表示するには、任意の列見出しを右クリックし、**[列の表示（Show Columns）] > [バージョンID（Version ID）]** を選択します。
作成日（Created On）	設定バージョンがアーカイブされた日付と時刻。
Created By	設定バージョンをアーカイブに追加する操作に関連付けられたユーザ ID またはシステム ID。 username1（username2）という形式で 2 つの名前がある場合、最初の名前が要求を開始したユーザーで、カッコ内の名前がシステム アイデンティティ ユーザーです。システムアイデンティティ信頼ユーザーの詳細については、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。
Archival Source	アーカイブ イベントの発生元（たとえば、ユーザ要求、展開、プロビジョニング、検出）。
Creation Comment	設定バージョンを作成した方法と理由に関する説明。

要素	説明
[Transcript] アイコン	ダブルクリックすると、デバイスに展開された設定バージョンのトランスクリプトが表示されます。 トランスクリプトとは、展開処理またはロールバック処理の間にキャプチャされた、Security Manager とデバイス間のトランザクション ログ ファイルです。この中には、展開要求またはロールバック要求が出た時点からサーバとデバイス間で送受信されたコマンドは含まれていますが、展開の初期検出フェーズである、Security Manager がデバイスから現在の設定を取得するときに行われた通信は含まれていません。
[表示（View）] ボタン	選択した設定を [Config Version Viewer] ウィンドウに表示するには、このボタンをクリックします（[Configuration Version Viewer] （76 ページ）を参照）。ここで、その設定を他の設定バージョンと比較することもできます。
[Rollback] ボタン	デバイス設定を選択した設定バージョンにロールバックするには、このボタンをクリックします。ただし、設定がそのデバイスから作成されたものである場合にかぎります。設定をロールバックするのは、極端な状況にある場合だけとしてください。詳細については、次の項を参照してください。 • 設定のロールバックについて （80 ページ） • ロールバックを使用したアーカイブ済み設定の展開 （89 ページ）
[Add from Device] ボタン	Security Manager を使用して、デバイスから現在実行中の設定を取得し、それを設定バージョンとしてアーカイブに追加するには、このボタンをクリックします。これは、デバイスの中に設定がデバイスの CLI で直接変更された可能性があるものがある場合に便利です。 設定バージョンの追加方法については、デバイスの設定バージョンの Configuration Archive への追加 （75 ページ）を参照してください。

展開および Configuration Archive の使用

ここでは、展開の管理と Configuration Archive の使用について説明します。

ジョブおよびスケジュールの展開ステータスおよび展開履歴の表示

Deployment Manager では、展開ジョブおよび展開スケジュールのステータスおよび履歴情報の表示、さらに展開ジョブおよび展開スケジュールの作成および管理ができます。[Deployment Manager] ウィンドウを開くには、[管理（Manage）] > [展開（Deployments）] を選択します。

ジョブとスケジュールは、独立したタブに表示されます。ただし、展開スケジューリングに基づいてジョブを作成すると、そのジョブは定期的なジョブのリストに表示されます。ジョブまたはスケジュールのリストを表示するには、対応するタブをクリックします。リストでは、次の情報を参照できます。

- 展開ジョブ：上部ペインには、展開ジョブのリストが表示されます。ジョブを選択すると、さらに詳細な情報が下部ペインに表示されます。
  - [Summary] タブ：[Summary] タブには、ジョブの状態、正常に展開されたデバイスの数、展開時にエラーが発生したデバイスの数などが表示されます。
  - [Details] タブ：[Details] タブには、展開対象の各デバイスの状態の詳細が表示されます。
  - [History] タブ（Workflow モード限定）：[History] タブには、選択したジョブが作成されてから、そのジョブに対して実施されたトランザクションが表示されます。テーブルの各行には、実行された処理、処理を実行したユーザ、処理を実行した日付と時刻、ユーザが入力したコメントが表示されます。
- 展開スケジュール：上部ペインには、展開スケジュールのリストが表示されます。スケジュールを選択すると、さらに詳細な情報が下部ペインに表示されます。
  - [Summary] タブ：[Summary] タブには、スケジュール、スケジュールから次にジョブが作成される時間、スケジュールに基づいてジョブが最後に実行された時間、スケ

ジュールに含まれているデバイスの数、スケジュールを最後に変更したユーザのユーザ ID などが表示されます。

- [Devices] タブ：[Devices] タブには、スケジュールに含まれているデバイスのリストが表示されます。
- [History] タブ：[History] タブには、スケジュールの状態変更および関連するコメントが表示されます。処理ごとにどのユーザが実行したかを追跡できます。
- [Jobs] タブ：[Jobs] タブには、スケジュールから作成された展開ジョブとその状態を記載したリストが表示されます。これらのジョブは、[Deployment Jobs] タブでも参照できます。

[Deployment Manager] ウィンドウに表示される状態情報は、[Security Manager Administration Deployment] ページ（[Tools] > [Security Manager Administration] > [Deployment]）で自動リフレッシュをオフにしていないかぎり、自動的にリフレッシュされます。ジョブまたはスケジュールのテーブルの下にあるメッセージを参照すると、自動リフレッシュがオンになっているかどうかがわかります。オフの場合、状態情報をリフレッシュするには、[リフレッシュ（Refresh）] をクリックします。

関連項目

- 展開プロセスの概要　（2 ページ）
- Workflow 以外のモードでの設定の展開　（35 ページ）
- Workflow モードでの展開ジョブの展開　（50 ページ）
- Auto Update Server または CNS Configuration Engine を使用した設定の展開　（52 ページ）
- Token Management Server への設定の展開　（54 ページ）
- 設定のプレビュー　（55 ページ）
- デバイスへの設定の再展開　（67 ページ）
- 展開ジョブの中断　（69 ページ）
- Deployment Manager を使用したデバイスへの設定のロールバック　（88 ページ）
- 展開スケジュールの作成または編集　（70 ページ）
- 展開スケジュールの一時停止または再開　（74 ページ）

展開ジョブを正常に完了するためのヒント

展開が正常に完了するかどうかは、展開のトラブルシューティングに説明するように多くの要因で決まります。展開ジョブのデバイスを選択するときや、ジョブを開始するときに、ネットワーク通信およびデバイスの正常な機能に関する要因に加えて、次のヒントを念頭に置いておくと、展開の結果をよい方向に導くことができます。

- デバイスに展開する前に、そのデバイスで少なくとも 1 つのポリシーを設定する必要があります。ポリシーを 1 つも割り当てずにデバイスに展開すると、そのデバイスの現在の設定が空の設定で上書きされ、デバイスは機能しません。
- ファイアウォール デバイス限定：ファイアウォール デバイスを（手動定義によるデバイスの追加の説明に従って）手動で追加した場合は、そのデバイスに展開する前に、そのデバイスの出荷時のデフォルト ポリシーを検出（インポート）することを強く推奨します。このようなポリシーを Security Manager に導入すると、初めてそのデバイスに展開するときに知らないうちにポリシーを削除してしまうミスを防ぐことができます。ファイアウォール デバイスの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。ポリシーをインポートする方法の詳細については、ポリシーの検出を参照してください。
- 展開にかかる時間は、展開ジョブに含まれるデバイスの数に応じて数分から 1 時間以上となる場合があります。
- VPN に含まれるデバイスのサブセットを変更すると、VPN が動作しなくなることがあります。展開ジョブを作成するときに VPN に含まれるデバイスのサブセットを選択した場合は、警告が表示され、VPN 内の他のデバイスを選択する機会が与えられます。 警告 - [Partial VPN Deployment] ダイアログボックス （39 ページ）を参照してください。
- 他の展開ジョブに含まれていて現在アクティブな状態（[Edit]、[Edit Open]、および [Approved]）であるデバイスは選択できません。他の展開ジョブに含まれていて現在 [Deployed]、[Failed]、[Discarded]、[Aborted] の状態であるデバイスは選択できます。
- Firewall Service Module（FWSM; ファイアウォール サービス モジュール）および Intrusion Detection System Service Module（IDSM; 侵入検知システム サービス モジュール）には、仮想デバイスが含まれています。Security Manager は、モジュールおよび仮想デバイスを独立したデバイスであると見なします。
- FWSM に加えた変更によっては、Catalyst Multiservice Function Card（MSFC; マルチサービス機能カード）の更新が必要になることもあります。このようなタイプの変更を加えた FWSM を選択した場合、Security Manager は展開ジョブに MSFC を含める必要があることを通知し、自動的に MSFC デバイスを選択します。ただし、MSFC がすでに別のアクティブな展開ジョブに含まれている場合は、現在の展開ジョブにその MSFC を含めることはできません。他の展開ジョブから MSFC を削除するか、他の展開ジョブを廃棄するか、または他の展開ジョブに FWSM を含める必要があります。
- Catalyst 6500/7600 デバイスへの展開の状態は、デバイスへの展開を示すほか、インターフェイス コンテキスト（子デバイス）に影響を与えるインターフェイス コマンドがポリシー変更に含まれているときには、そのインターフェイス コンテキストも示します。たとえば、スイッチが参加している VLAN に影響を与えるポリシー変更を展開するときや、インターフェイス コンテキストを追加または削除するなどしてインベントリを更新するときです。

関連項目

- 展開プロセスの概要 （2 ページ）

Workflow 以外のモードでの設定の展開

設定を展開するとき、デバイスに設定を転送するには、直接転送する方法か、ネットワーク内の別の転送サーバ（AUS、CNS、または TMS など）に転送する方法があります。あるいは、Security Manager サーバのディレクトリに、設定ファイルとして作成することもできます。詳細については、 展開方法について （10 ページ）を参照してください。

（注） デバイスの RAVPN ポリシー（DAP、グループポリシーなど）で使用される Policy Object Manager を介して統合 ACL エントリに変更を加えた場合、デバイスとチケットは[保存した変更の展開（Deploy Saved Changes）] ウィンドウに表示されません。[他のデバイスを追加（Add other devices）] をクリックして、デバイスを手動で追加する必要があります。

ヒント 展開ジョブを作成する前に、 展開ジョブを正常に完了するためのヒント （33 ページ）を参照してください。この項には、展開ジョブを作成する場合に留意する必要のあるヒントと注意が記載されています。

注意 デバイスに展開する前に、そのデバイスで少なくとも 1 つのポリシーを設定する必要があります。ポリシーを 1 つも割り当てずにデバイスに展開すると、そのデバイスの現在の設定が空の設定で上書きされます。

（注） 仮想センサーを使用している場合、IPS デバイスおよびそのデバイス上のすべての仮想センサーは、グループとして展開する必要があります。仮想センサーに変更を加えてから展開した場合、Security Manager は親デバイスとその関連するすべての仮想センサーを展開します。

はじめる前に

- デバイスがブートストラップされていることを確認します。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。
- AUS、CNS、または TMS などの転送サーバに展開する場合は、サーバ、Security Manager 設定、およびデバイスが正しく設定されていることを確認します。

関連項目

- 展開プロセスの概要 （2 ページ）
- 展開ジョブまたは展開スケジュールにデバイスを含める操作 （9 ページ）
- 展開方法について （10 ページ）
- Auto Update Server または CNS Configuration Engine を使用した設定の展開 （52 ページ）
- Token Management Server への設定の展開 （54 ページ）
- デバイス通信設定および証明書の管理
- アウトオブバンド変更の処理方法について （14 ページ）

ステップ 1 Workflow 以外のモードでは、次のいずれかを実行します。

- **[ファイル（File）] > [送信して展開（Submit and Deploy）]** を選択するか、またはツールバーの [変更の送信と展開（Submit and Deploy Changes）] ボタンをクリックします。

（注） これらのオプションは、チケット管理が有効になっている場合は使用できません。

- **[ファイル（File）] > [展開（Deploy）]** を選択します。
- [メイン（Main）] ツールバーの [Deployment Manager] ボタンをクリックし、[展開ジョブ（Deployment Job）] タブがアクティブでない場合にはクリックします。[展開（Deploy）] をクリックします。

Security Manager は、前回の展開以降に加えられたすべてのポリシー変更を検証します。検証でエラーが発生した場合は、エラーを解決してから展開を再試行してください。警告メッセージまたは情報メッセージだけが表示される場合は、[OK] をクリックして [保存された変更の展開（Deploy Saved Changes）] ダイアログボックスに進みます。

ステップ 2 [Deploy Saved Changes] ダイアログボックスで、次の手順を実行します。

- 設定の展開先デバイスを選択します。デバイス セレクタには、ポリシーは変更されたが展開がまだ済んでいないデバイスがすべて表示されます。また、展開する変更デバイスは最初からすべて選択されています。

変更されたデバイスを含むすべてのデバイス グループが表示され、デバイス グループ フォルダを使用して、デバイスを選択または選択解除できます。複数のグループに表示されたデバイスを選択または選択解除すると、そのデバイスはすべてのグループで選択または選択解除されます。ただし、ジョブに含まれるデバイスが展開されるのは 1 回だけです。すべてのフォルダを開くには、[すべて展開（Expand All）] を右クリックして選択します。

[保存された変更の展開（Deploy Saved Changes）] ダイアログボックスには、選択したデバイスの展開に含まれる、変更に関連付けられた日付、時刻、およびユーザーが表示されます。この情報は、展開のために選択したデバイスに基づいて変化します。チケット管理を有効にしている場合、展開する変更に関連するチケットも表示されます。チケットIDをクリックしてチケットの詳細を表示し、設定されている場合は外部チケット管理システムに移動できます（[チケット管理（Ticket Management）] ページを参照）。

アウトオブバンド変更が検出された場合、[OOB Changes] ダイアログボックスを閉じるときに、結果に基づいてデバイス名が色分けされます。緑はアウトオブバンド変更、赤は検出プロセス中のエラー、色に変更がない場合はアウトオブバンド変更がないことを示しています。

- ポリシー変更のないデバイスを展開ジョブに追加する場合は、[他のデバイスを追加（Add other devices）] をクリックして、他のデバイスを追加（Add other devices）] ダイアログボックスを開きます（[Add Other Devices] ダイアログボックス （73 ページ）を参照）。変更されていないデバイスを追加するのは、デバイスが手動で変更されたときに、そのデバイスを以前の設定（Security Managerデータベースに格納されている設定）に戻す場合などがあります。
- （オプション）設定の展開方式を変更するには、[展開方式の編集（Edit Deploy Method）] をクリックして、[展開方式の編集（Edit Deploy Method）] ダイアログボックスを開きます（[Edit Deploy Method] ダイアログボックス （38 ページ）を参照）。展開方式にはシステム デフォルト（各組織で選択した方式）が存在するため、方式を変更する必要がない場合があります。選択できる方式は次のとおりです。
  - [Device]：設定をデバイスに直接展開するか、またはデバイスに指定された転送メカニズムに展開します。詳細については、 デバイスへの直接展開 （11 ページ）または 中間サーバを使用したデバイスへの展開 （12 ページ）を参照してください。
  - [File]：Security Managerサーバ上の選択したディレクトリに設定ファイルを展開します。詳細については、 ファイルへの展開 （13 ページ）を参照してください。

展開を行う前に、次の作業を実行できます。

- 提示された設定を確認し、最後に展開された設定または現在実行中の設定と比較する。デバイスを右クリックして、[設定のプレビュー（Preview Config）] を選択します。詳細については、 設定のプレビュー （55 ページ）を参照してください。
- [OOBの変更を検出（Detect OOB Changes）] ボタンをクリックし、デバイスを分析してアウトオブバンド変更の有無を調べます。詳細については、 アウトオブバンド変更の検出および分析 （57 ページ）および [OOB (Out of Band) Changes] ダイアログボックス （61 ページ）を参照してください。

ステップ 3 [展開（Deploy）] をクリックして、選択したデバイスの展開ジョブを開始します。これにより、必要な設定ファイルが生成され、選択した展開方法に従って適用されます。

[Deployment Status Details] ダイアログボックスが開き、展開ステータスを参照できます。このダイアログボックスには、ジョブの概要情報、各デバイスへの展開ステータス、および展開に失敗した理由を示すメッセージが表示されます。

[Deployment Details] テーブルで、デバイスに対応する行を選択すると、特にそのデバイス向けの展開ステータス メッセージが表示されます。詳細については、 [Deployment Status Details] ダイアログボックス （40 ページ）を参照してください。

デバイスへの展開が失敗した場合は、その失敗したデバイスに設定を再展開できます。詳細については、デバイスへの設定の再展開 （67 ページ）を参照してください。

[Edit Deploy Method] ダイアログボックス

[Edit Deploy Method] ダイアログボックスは、生成した設定を直接ネットワーク内のデバイスに展開するのか、Security Manager サーバ上のディレクトリに設定ファイルを作成するのかを指定する場合に使用します。

ナビゲーション パス

[適用（Deployment）]—[ジョブの作成（Create a job）] ダイアログボックス、または[ジョブの編集（Edit a job）]ダイアログボックス（Workflow モード）、または [保存した変更の展開（Deploy Saved Changes）] ダイアログボックス（Workflow 以外のモード）で、[展開方法の編集（Edit Deploy Method）] をクリックします。手順については、次を参照してください。

- 展開ジョブの作成および編集 （44 ページ）
- Workflow 以外のモードでの設定の展開 （35 ページ）

関連項目

- 展開方法について （10 ページ）
- Workflow モードでの設定の展開 （43 ページ）
- Auto Update Server または CNS Configuration Engine を使用した設定の展開 （52 ページ）
- Token Management Server への設定の展開 （54 ページ）
- デバイス通信設定および証明書の管理

フィールド リファレンス

表 *9 : [Edit Deploy Method]* ダイアログボックス

要素	説明
デバイス	デバイスの名前。

要素	説明
方法	使用する展開方法。 • [Device]：設定をデバイスに直接展開するか、またはデバイスに指定された転送メカニズムに展開します。詳細については、デバイスへの直接展開 （11 ページ）または中間サーバを使用したデバイスへの展開 （12 ページ）を参照してください。 • [File]：Security Manager サーバ上のディレクトリに設定ファイルを展開します。[File] を選択する場合は、設定ファイルの展開先ディレクトリを [Destination] カラムで指定します。IPS デバイスではファイル展開を使用できません。詳細については、ファイルへの展開 （13 ページ）を参照してください。 （注） 複数のデバイスの展開方法を一度に設定するには、目的の行を選択して右クリックし、[選択した展開方法の編集（Edit Selected Deploy Method）] を選択します。[Edit Selected Deploy Method] ダイアログボックスが開き、ここで選択を行うことができます。
[接続先（Destination）]	[Method] フィールドで [File] を選択した場合は、設定ファイルを展開するディレクトリを入力します。使用可能なディレクトリのリストから選択するには、[参照（Browse）] をクリックします。
[Preview Config] ボタン	選択したデバイスに対して提示された設定変更を表示するには、このボタンをクリックします。最後に展開された設定または現在実行中の設定と比較できます。詳細については、設定のプレビュー （55 ページ）を参照してください。
Out of Band Change Behavior	CLI を使用してデバイスに直接変更を加えた場合に、Security Manager が実行する処理に対応するオプション ボタンをクリックします。アウトオブバンド変更を処理する方法および使用可能なオプションの意味の詳細については、アウトオブバンド変更の処理方法について （14 ページ）を参照してください。

警告 - [Partial VPN Deployment] ダイアログボックス

[Partial VPN Deployment] ダイアログボックスは、設定を展開する VPN に含まれる他のデバイスを選択する場合に使用します。

展開ジョブを作成し、そのジョブに VPN 内のデバイスが含まれる場合は、その VPN 内のすべてのデバイスを選択する必要があります。デバイスのサブセットを選択し、それらのデバイスにだけ展開しようとした場合は、このダイアログボックスが表示され、VPNに含まれる他のデバイスを選択できます。

ナビゲーション パス

- Workflow 以外のモード：[保存された変更内容の展開（Deploy Saved Changes）] ダイアログボックスで VPN 内のデバイスのサブセットを選択する場合は、[展開（Deploy）] 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。
- Workflow モード：[ジョブの作成または編集（Create or Edit a Job）] ダイアログボックスで VPN 内のデバイスのサブセットを選択する場合は、[OK] 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。

関連項目

- 展開ジョブの作成および編集　（44 ページ）
- Workflow 以外のモードでの設定の展開　（35 ページ）
- Workflow モードでの設定の展開　（43 ページ）

フィールド リファレンス

表 10 : [Partial VPN Deployment Warning] ダイアログボックス

要素	説明
VPN	VPN の名前。
Missing Devices	展開先として選択しなかった VPN 内のすべてのデバイス。
Is Device in Other Job	欠落しているデバイスが別の展開ジョブに含まれているかどうかを示します。
[Deploy to All Devices in VPN] ボタン	VPN 内のすべてのデバイスを展開するには、このボタンをクリックします。 VPN内のすべてのデバイスに展開できるのは、そのいずれのデバイスも他の展開ジョブに含まれていない場合だけです。
[Deploy to Selected Devices] ボタン	[Create or Edit a Job] ダイアログボックスまたは [Deploy Saved Changes] ダイアログボックスで選択されているデバイスにだけ展開するには、このボタンをクリックします。

[Deployment Status Details] ダイアログボックス

選択したデバイスに設定が展開されているときには、[Deployment Status Details] 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、ジョブの概要情報、各デバイスへの展開ステータス、および展開に失敗した理由を示すメッセージが表示されます。

[Deployment Details] テーブルで、デバイスに対応する行を選択すると、そのデバイスの展開ステータス メッセージが表示されます。

（注） [閉じる（Close）] をクリックして、このダイアログボックスを閉じ、展開を続けながら Security Manager での作業を続けることができます。

ナビゲーション パス

[保存した変更を展開する（Deploy Saved Changes）] ダイアログボックスから、[展開（Deploy）] をクリックします。

関連項目

- 展開プロセスの概要　（2 ページ）
- Workflow 以外のモードでの設定の展開　（35 ページ）
- 展開ジョブを正常に完了するためのヒント　（33 ページ）
- デバイス通信設定および証明書の管理
- [Device Communication] ページ

フィールド リファレンス

表 *11 : [Deployment Status Details]* ダイアログボックス

要素	説明
Deployment Status Details	
Progress Status Bar	正常に更新されたデバイスを視覚的に表現し、その割合を示したもの。
ステータス	展開の状態。有効な状態は、[Deploying]、[Aborted]、[Successful]、および [Failed] です。これらの状態の説明については、 Workflow モードでのジョブの状態　（7 ページ）を参照してください。
Deployment Job Name	展開ジョブの名前。
Devices To Be Deployed	展開ジョブに含まれるデバイスの合計数。
Devices Deployed Successfully	正常に更新されたデバイスの数。
Devices Deployed With Errors	更新に失敗したデバイスの数。
展開の詳細 この表には、展開ジョブに含まれるデバイスの一覧が表示されます。	

要素	説明
デバイス	デバイスの名前。
ステータス	デバイスへの展開の状態。これらの状態の説明については、Workflow 以外のモードでのジョブの状態 （5 ページ）を参照してください。
[概要（Overview）]	デバイスの警告、エラー、および失敗の数。
方法	デバイスへの展開の方法。有効な方法は、[File] と [Device] です。
Config	デバイス設定ファイル。アイコンをダブルクリックすると、デバイスの設定がプレビューされます。詳細については、設定のプレビュー（55 ページ）を参照してください。
Transcript	（ファイルへの展開ではなく）デバイスに展開している場合、展開中に Security Manager がデバイスに発行したコマンドおよびデバイスからの応答。アイコンをダブルクリックすると、デバイスのトランスクリプトが表示されます。
Last Ticket(s)	デバイスの展開の一部である変更を含むチケット。チケット ID をクリックして、作成者や最終更新日など、チケットに関する追加情報を表示できます。外部チケット管理システムへのリンクが設定されている場合は、チケットの詳細からそのシステムに移動することもできます（[Device Communication] ページを参照）。
メッセージ	重大度アイコンで示された、警告、エラー、および失敗のメッセージ。 項目を選択すると、右側の [Description] ボックスに詳細なメッセージが表示されます。右側の [Action] ボックスには、問題の修正方法が表示されます。
[Generate Report] ボタン	このジョブの展開ステータス 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 HTML および PDF フォーマットで生成できます。レポートには、ジョブの概要および完全な設定とデルタ設定、およびジョブのトランスクリプトが含まれます。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	ステータス情報を更新するには、このボタンをクリックします。

要素	説明
[Abort] ボタン	展開ジョブを中断するには、このボタンをクリックします。中断可能な展開ジョブは、[Deploying]、[Scheduled]、または [Rolling Back] の状態にあるジョブだけです。ジョブを中断すると、保留中のデバイスへの設定ファイルの展開が停止しますが、展開が進行中のデバイス（コマンドがデバイスに現在書き込まれています）や、展開がすでに正常に完了したデバイスには影響が及びません。

Workflow モードでの設定の展開

Workflow モードで設定を展開する作業は、いくつかの手順からなるプロセスです。展開ジョブを作成し、承認を得てから、展開する必要があります。このプロセスにより、作業を何名かで分担していても、各人の作業を一元的に管理できます。

設定を展開するとき、デバイスに設定を転送するには、直接転送する方法か、ネットワーク内の別の転送サーバ（AUS、CNS、または TMS など）に転送する方法があります。あるいは、Security Manager サーバのディレクトリに、設定ファイルとして作成することもできます。詳細については、展開方法について （10 ページ）を参照してください。

ヒント　展開ジョブを作成する前に、展開ジョブを正常に完了するためのヒント （33 ページ）を参照してください。この項には、展開ジョブを作成する場合に留意する必要のあるヒントと注意が記載されています。

はじめる前に

- デバイスがブートストラップされていることを確認します。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。
- AUS、CNS、または TMS などの転送サーバに展開する場合は、サーバ、Security Manager 設定、およびデバイスが正しく設定されていることを確認します。

関連項目

- 展開プロセスの概要 （2 ページ）
- 展開ジョブまたは展開スケジュールにデバイスを含める操作 （9 ページ）
- 展開方法について （10 ページ）
- Auto Update Server または CNS Configuration Engine を使用した設定の展開 （52 ページ）
- Token Management Server への設定の展開 （54 ページ）
- デバイス通信設定および証明書の管理
- アウトオブバンド変更の処理方法について （14 ページ）

ステップ 1 [メイン（Main）] ツールバーで [展開マネージャ（Deployment Manager）] ボタンをクリックします。

[Deployment Manager] ウィンドウが表示されます。[展開ジョブ（Deployment Jobs）] タブがアクティブでない場合は、このタブをクリックします。

ステップ 2 展開ジョブを作成します。[作成（Create）] をクリックし、ジョブのプロパティを入力します。手順については、展開ジョブの作成および編集 （44 ページ）を参照してください。

ジョブの作成後、そのジョブを送信するかどうかを選択できます。展開ジョブ アプルーバを使用しない場合は、ジョブを自動的に送信し、承認し、展開することもできます。その場合、このプロセスの他の手順を完了する必要はありません。

ステップ 3 （アプルーバを使用したワークフロー）ジョブを送信します。ジョブを送信しなかった場合は、[Deployment Manager] ウィンドウでそのジョブを選択し、[送信（Submit）] をクリックします。電子メールが、アプルーバに送信されます。詳細については、展開ジョブの送信 （48 ページ）を参照してください。

ステップ 4 （アプルーバを使用したワークフローまたは使用しないワークフロー）ジョブを承認します。作成時にジョブを承認しなかった場合は、[Deployment Manager] ウィンドウでそのジョブを選択し、[承認（Approve）] をクリックします。ジョブを承認する担当者が別にいる場合は、その担当者がこの手順を実行する必要があります。詳細については、展開ジョブの承認と拒否 （49 ページ）を参照してください。

ステップ 5 （アプルーバを使用したワークフローまたは使用しないワークフロー）ジョブを展開します。作成時にジョブを展開しなかった場合は、[Deployment Manager] ウィンドウでそのジョブを選択し、[展開（Deploy）] をクリックします。ジョブを開始する時刻として将来の時刻を指定したり、すぐにジョブを開始したりできます。設定は、ジョブのプロパティに従って展開されます。詳細については、Workflow モードでの展開ジョブの展開 （50 ページ）を参照してください。

（注） 展開ジョブは、展開する前であればいつでも廃棄できます。詳細については、展開ジョブの廃棄（51 ページ）を参照してください。

展開ジョブの作成および編集

Workflow モードでは、ポリシー設定をデバイスに展開する前に、展開ジョブを作成する必要があります。ジョブを作成するときは、設定を展開するデバイス、直接デバイスに展開するのか出力ファイルに展開するのか、およびいつジョブを実行するのかを選択します。

（注） デバイスの RAVPN ポリシー（DAP、グループポリシーなど）で使用される Policy Object Manager を介して統合 ACL エントリに変更を加えた場合、デバイスとチケットは [展開-ジョブの作成（Deployment- Create a Job）] ウィンドウに表示されません。[他のデバイスを追加（Add other devices）] をクリックして、デバイスを手動で追加する必要があります。

ヒント 展開ジョブを作成する前に、展開ジョブを正常に完了するためのヒント （33 ページ）を参照してください。この項には、展開ジョブを作成する場合に留意する必要のあるヒントと注意が記載されています。

注意 デバイスに展開する前に、そのデバイスで少なくとも 1 つのポリシーを設定する必要があります。ポリシーを 1 つも割り当てずにデバイスに展開すると、そのデバイスの現在の設定が空の設定で上書きされます。

はじめる前に

- デバイスがブートストラップされていることを確認します。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。
- AUS、CNS、または TMS などの転送サーバに展開する場合は、サーバ、Security Manager 設定、およびデバイスが正しく設定されていることを確認します。

関連項目

- 展開プロセスの概要 （2 ページ）
- 展開ジョブまたは展開スケジュールにデバイスを含める操作 （9 ページ）
- 展開方法について （10 ページ）
- アウトオブバンド変更の処理方法について （14 ページ）
- Workflow モードでのジョブの状態 （7 ページ）

ステップ 1 [メイン（Main）] ツールバーで [展開マネージャ（Deployment Manager）] ボタンをクリックします。

[Deployment Manager] ウィンドウが表示されます。[展開ジョブ（Deployment Jobs）] タブがアクティブでない場合は、このタブをクリックします。

ステップ 2 次のいずれかを実行します。

- [作成（Create）] をクリックして、新規ジョブを作成します。
- 編集可能なジョブを選択し、[開く（Open）] をクリックしてジョブを編集します。すでに展開したジョブは編集できません。

[Create a Job] ダイアログボックスまたは [Edit a Job] ダイアログボックスが開きます。

ステップ 3 ダイアログボックスで、次の手順を実行してジョブの内容を定義します。

- [ジョブの名前と説明（Job Name and Description）]：デフォルトのジョブ名をそのまま使用するか、またはそのジョブが何であるかがよくわかる名前を入力します。ジョブ名を入力すると各ジョブを区別

できるため、ジョブの内容を反映する名前を割り当てることを推奨します。いったん作成したジョブの名前は変更できません。任意で、ジョブの説明を入力できます。

- 設定の展開先デバイスを選択します。デバイス セレクタには、ポリシーは変更されたが展開がまだ済んでいないデバイスがすべて表示されます。また、展開する変更デバイスは最初からすべて選択されています。

変更されたデバイスを含むすべてのデバイス グループが表示され、デバイス グループ フォルダを使用して、デバイスを選択または選択解除できます。複数のグループに表示されたデバイスを選択または選択解除すると、そのデバイスはすべてのグループで選択または選択解除されます。ただし、ジョブに含まれるデバイスが展開されるのは 1 回だけです。すべてのフォルダを開くには、[すべて展開（Expand All）] を右クリックして選択します。

アウトオブバンド変更が検出された場合、[OOB Changes] ダイアログボックスを閉じるときに、結果に基づいてデバイス名が色分けされます。緑はアウトオブバンド変更、赤は検出プロセス中のエラー、色に変更がない場合はアウトオブバンド変更がないことを示しています。

- ポリシー変更のないデバイスを展開ジョブに追加する場合は、[他のデバイスを追加（Add other devices）] をクリックして、[他のデバイスを追加（Add other devices）] ダイアログボックスを開きます（[Add Other Devices] ダイアログボックス （73 ページ）を参照）。変更されていないデバイスを追加するのは、デバイスが手動で変更されたときに、そのデバイスを以前の設定（Security Manager データベースに格納されている設定）に戻す場合などがあります。
- （任意）設定の展開方式を変更するには、[展開方式の編集（Edit Deploy Method）] をクリックして、[展開方式の編集（Edit Deploy Method）] ダイアログボックスを開きます（[Edit Deploy Method] ダイアログボックス （38 ページ）を参照）。展開方式にはシステム デフォルト（各組織で選択した方式）が存在するため、方式を変更する必要がない場合があります。選択できる方式は次のとおりです。
  - [Device]：設定をデバイスに直接展開するか、またはデバイスに指定された転送メカニズムに展開します。詳細については、デバイスへの直接展開 （11 ページ）または 中間サーバを使用したデバイスへの展開 （12 ページ）を参照してください。
  - [File]：Security Manager サーバ上の選択したディレクトリに設定ファイルを展開します。詳細については、ファイルへの展開 （13 ページ）を参照してください。

展開を行う前に、次の作業を実行できます。

- 提示された設定を確認し、最後に展開された設定または現在実行中の設定と比較する。デバイスを右クリックして、[設定のプレビュー（Preview Config）] を選択します。詳細については、設定のプレビュー （55 ページ）を参照してください。
- [OOBの変更を検出（Detect OOB Changes）] ボタンをクリックし、デバイスを分析してアウトオブバンド変更の有無を調べます。詳細については、アウトオブバンド変更の検出および分析 （57 ページ）および [OOB (Out of Band) Changes] ダイアログボックス （61 ページ）を参照してください。

ステップ 4 ダイアログボックスを閉じたときのジョブの処理方法を選択します。使用できるオプションは、展開ジョブ アプルーバを割り当てて Workflow モードを使用しているかどうかによって異なります。

- **承認者なし**：別の承認者を使用しない場合は、次のオプションを使用できます。

- [ジョブを閉じる（Close the job）]：ジョブを閉じ、編集状態のままにします。ジョブにさらに変更を加えることがわかっている場合には、このオプションを選択します。
- [ジョブを承認する（Approve the job）]：ジョブを閉じて承認しますが、まだ展開しません。次を設定します。
- [コメント（Comments）]：（任意）ジョブの承認に関するコメント。
- [送信者（Submitter）]：承認のためにジョブを送信する担当者の電子メールアドレス。ジョブ状態変更の通知が、このアドレスに送信されます。このアドレスには当初、Security Manager へのログインに使用したユーザアカウントに関連付けられた電子メールアドレスが設定されます。このアドレスが正しいアドレスであると、通知を受信できます。
- [ジョブを展開する（Deploy the job）]：ジョブを閉じ、承認し、展開します。次を設定します。
- [オプション（Options）]：[今すぐ展開（Deploy Now）] または [スケジュール（Schedule）]。[Schedule] を選択した場合、他にいくつかフィールドが表示され、ジョブを実行する日付と時刻を指定できます。時間は 24 時間形式で、Security Manager サーバーのタイムゾーンに基づきます。必ずしも現在使用しているタイムゾーンと同じであるとはかぎりません。指定する時刻は、少なくとも 5 分先である必要があります。
- [コメント（Comments）]：（任意）ジョブの展開に関するコメント。
- [展開ステータス通知を送信する（Send Deployment Status Notification）]：ジョブステータスが変更されるたびに、Security Manager から電子メール通知を送信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は、通知を受信する担当者の電子メールアドレスを [Job Completion Recipients] フィールドに入力します。複数のアドレスを入力する場合は、各アドレスをカンマで区切ります。このフィールドには当初、デフォルトのアプルーバと自分の電子メール アドレスが入力されています。

- **承認者あり**：別の承認者を使用する場合は、次のオプションを設定できます。
  - [ジョブを送信する（Submit the job）]：承認のためにジョブを送信するかどうかを指定します。デフォルトでは、このチェックボックスはオンになっています。
  - [承認者の電子メール（Approver E-mail）]：承認のためにジョブを送信する場合は、承認者の電子メールアドレスを指定します。デフォルトのアプルーバ電子メール アドレスがフィールドに入力されていますが、このアドレスは変更できます。
  - [コメント（Comments）]：（任意）承認者に送信するコメント（ある場合）。
  - [送信者の電子メール（Submitter E-mail）]：送信者の電子メールアドレス。このフィールドには当初、ログインに使用したユーザアカウントに関連付けられた電子メールアドレスが入力されていますが、別のアドレスに変更できます。

ステップ 5 [OK] をクリック

ジョブの処理方法に関する選択内容によっては、さらにジョブの送信、承認、および展開が必要になることがあります。詳細については、次のトピックを参照してください。

- 展開ジョブの送信　（48 ページ）

• 展開ジョブの承認と拒否 （49 ページ）
• Workflow モードでの展開ジョブの展開 （50 ページ）

展開ジョブの送信

一部の組織では、ジョブを展開する前に、適切な権限を持つ別のユーザがジョブを承認する必要があります。この場合、展開ジョブのアプルーバによって Workflow モードがイネーブルになり、送信者はこのユーザにジョブを送信して確認してもらう必要があります。アプルーバはジョブを確認し、承認または拒否を行います。

展開ジョブアプルーバを割り当てずに Workflow モードを使用している場合は、自分自身でジョブを確認して承認できます。このモードでは、ジョブを送信しません。詳細については、展開ジョブの承認と拒否 （49 ページ）を参照してください。

（注） 展開ジョブの承認は、[Tools] > [Security Manager Administration] > [Workflow] からイネーブルおよびディセーブルにできます。詳細については、[Workflow] ページを参照してください。

この手順では、ジョブをすでに作成したものと想定しています。作成時にジョブを送信することもできます。そのためには、[ジョブの作成（Create a Job）] ダイアログボックスで [ジョブの送信（Submit the job）] チェックボックスをオンにします。

関連項目

• [Deployment Manager] ウィンドウ （19 ページ）
• Workflow モードでのジョブの状態 （7 ページ）

ステップ 1 [メイン（Main）] ツールバーで [展開マネージャ（Deployment Manager）] ボタンをクリックします。

[Deployment Status] ウィンドウが表示されます。[展開ジョブ（Deployment Jobs）] タブがアクティブでない場合は、このタブをクリックします。

ステップ 2 送信するジョブを選択します。

ステップ 3 [送信（Submit）] をクリックします。

[Submit Deployment Job] ダイアログボックスが開きます。

ステップ 4 次の情報を入力します。

- [アプルーバ（Approver）]：ジョブ送信を通知する担当者の電子メールアドレス。デフォルトのアプルーバ電子メール アドレスがフィールドに入力されていますが、このアドレスは変更できます。
- [コメント（Comments）]：（任意）アプルーバに送信するコメント。

- [送信者（Submitter）]：展開ジョブを送信する担当者の電子メールアドレス。このフィールドには当初、Security Managerへのログインに使用したユーザ名に関連付けられた電子メールアドレスが入力されていますが、別の電子メール アドレスに変更できます。

ステップ 5 [OK] をクリック

ジョブ状態が [Submitted] に変わります。ジョブを展開するには、アプルーバがそのジョブを承認する必要があります。

展開ジョブの承認と拒否

一部の組織では、ジョブを展開する前に、適切な権限を持つ別のユーザがジョブを承認する必要があります。展開ジョブアプルーバを割り当てたWorkflowモードでは、あるユーザーがジョブを送信し、別のユーザーがそのジョブをプレビューし、承認または拒否の判断を下します。

展開ジョブ アプルーバを割り当てない Workflow モードでは、ジョブを作成し、同時にジョブを承認できます。詳細については、展開ジョブの作成および編集 （44 ページ）を参照してください。

ジョブを拒否すると、そのジョブに含まれるデバイスはすぐに他のジョブに含めることができるようになります。拒否されたジョブは展開できませんが、開いて表示および編集できます。

（注） 展開ジョブの承認は、**[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [ワークフロー（Workflow）]** からイネーブルおよびディセーブルにできます。詳細については、[Workflow] ページを参照してください。

関連項目

- [Deployment Manager] ウィンドウ （19 ページ）
- Workflow モードでのジョブの状態 （7 ページ）

ステップ 1 [メイン（Main）] ツールバーで [展開マネージャ（Deployment Manager）] ボタンをクリックします。

[Deployment Manager] ウィンドウが表示されます。[展開ジョブ（Deployment Jobs）] タブがアクティブでない場合は、このタブをクリックします。

ステップ 2 送信されるジョブを選択し、次のいずれかを実行します。

- [承認（Approve）] をクリックします。
- [却下（Reject）] をクリックします。

任意で処理のコメントを入力できます。入力したコメントは、ジョブの履歴に保持されます。コメントを送信すると、電子メール通知が送信され（電子メール通知を設定している場合）、ジョブ状態が [Approved]

または [Rejected] に適宜変わります。これでジョブを展開できます（Workflow モードでの展開ジョブの展開 （50 ページ）を参照）。

Workflow モードでの展開ジョブの展開

Workflowモードで作業している場合、設定をデバイスに展開するには、展開ジョブを作成し、その承認を得る必要があります。アプルーバを別途割り当てずに作業している場合は、自分自身でジョブを承認して展開できます。それ以外の場合、ジョブをアプルーバに送信する必要があります。

Workflowモードで展開ジョブを展開すると、それだけでジョブが開始されます。展開中、ジョブの内容は変更できません。

（注） 展開にかかる時間は、展開ジョブに含まれるデバイスの数に応じて数分から 1 時間以上となる場合があります。

はじめる前に

- デバイスがブートストラップされていることを確認します。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。
- AUS、CNS、または TMS などの転送サーバに展開する場合は、サーバ、Security Manager 設定、およびデバイスが正しく設定されていることを確認します。
- ジョブを作成します。詳細については、展開ジョブの作成および編集 （44 ページ）を参照してください。
- 展開ジョブ アプルーバを割り当てて Workflow モードを使用している場合は、ジョブを送信します。詳細については、展開ジョブの送信 （48 ページ）を参照してください。
- ジョブを承認します。詳細については、展開ジョブの承認と拒否 （49 ページ）を参照してください。

関連項目

- 展開プロセスの概要 （2 ページ）
- [Deployment Manager] ウィンドウ （19 ページ）
- 展開ジョブまたは展開スケジュールにデバイスを含める操作 （9 ページ）
- 展開方法について （10 ページ）
- デバイス通信設定および証明書の管理

ステップ 1 [メイン（Main）] ツールバーで [Deployment Manager] ボタンをクリックします。

[Deployment Manager] ウィンドウが表示されます。[展開ジョブ（Deployment Jobs）] タブがアクティブでない場合は、このタブをクリックします。

ステップ 2 展開するジョブを選択します。

ステップ 3 [展開（Deploy）] をクリックします。

[Deploy Job] ダイアログボックスが開きます。

ステップ 4 [Deploy Job] ダイアログボックスで、次の選択を行います。

- [オプション（Options）]：ジョブを実行する方法。将来のある時点でジョブを実行するには、[スケジュール（Schedule）] を選択します。ジョブを今すぐに実行するには、[今すぐ展開（Deploy Now）] を選択します。将来の時刻にジョブをスケジューリングする場合は、そのジョブで展開される変更は、ジョブの実行時ではなくジョブの作成時点で実施されていた変更に基づきます。

[Schedule] を選択した場合は、日付と時刻のフィールドが表示されます。

- カレンダー アイコンをクリックして、ジョブを実行する日付を選択します。
- [Time] フィールドに、ジョブを開始する時間を 24 時間形式で入力します。時間は、Security Manager サーバのタイム ゾーンのものである必要があります。現在使用中のタイム ゾーンと同じものになるとはかぎりません。指定する時刻は、少なくとも 5 分先である必要があります。
- [コメント（Comments）]：（任意）ジョブを展開する理由の説明。
- [展開ステータス通知の要求、ジョブ完了通知受信者（Require Deployment Status Notifications, Job Completion Recipients）]：ジョブ状態が変化したときに、Security Manager から電子メールを送信するかどうかを指定します。

ステータス通知の送信を選択した場合は、受信者の電子メールアドレスを入力します。このフィールドには当初、ログインに使用したユーザーアカウントに関連付けられている電子メールアドレスが含まれています。複数のアドレスを入力するには、コンマで区切ります。

ステップ 5 [OK] をクリック

[Deployment Manager] ウィンドウに戻ります。ジョブ状態が [Deploying] に変わります。展開が完了すると、ジョブ状態が [Deployed] に変わります。

展開ジョブの廃棄

Workflow モードでは、ジョブは [Deployed]、[Deployment Failed]、[Aborted] を除く任意の状態である場合に廃棄できます。ジョブが [Workflow Management] ページでの設定に従って自動的にシステムから削除されるか、または手動でシステムから削除するまで、ジョブ状態は [Discarded] として表示されます。

関連項目

- [Deployment Manager] ウィンドウ （19 ページ）
- Workflow モードでのジョブの状態 （7 ページ）

ステップ 1 [メイン（Main）] ツールバーで [展開マネージャ（Deployment Manager）] ボタンをクリックします。

[Deployment Manager] ウィンドウが表示されます。[展開ジョブ（Deployment Jobs）] タブがアクティブでない場合は、このタブをクリックします。

ステップ 2 廃棄するジョブを選択します。

ステップ 3 [破棄（Discard）] をクリックします。任意で、ジョブを廃棄する理由を入力できます。

Auto Update Server または CNS Configuration Engine を使用した設定の展開

組織が Auto Update Server（AUS）または Cisco Networking Services（CNS）Configuration Engine を使用してネットワーク デバイスへの設定の展開を管理している場合、Security Manager でこのような中間サーバを使用できます。このタイプの展開を実行するには、デバイス、AUS か Configuration Engine、および Security Manager を正しくセットアップする必要があります。この手順では、実行する必要のあるタスクについて説明します。

ヒント AUS を使用するために Security Manager が他のファイルをデバイスにダウンロードする必要がある場合、その AUS には設定を正常に展開できません。たとえば、リモート アクセス VPN ポリシーによっては、プラグイン、Anyconnect クライアント、および Cisco Secure Desktop 設定を設定できます。このようなファイルは AUS に送信されません。このようなタイプのポリシーを設定する場合は、AUS を使用しないでください。

関連項目

- 展開プロセスの概要　（2 ページ）
- デバイスを管理するための準備
- 展開ジョブまたは展開スケジュールにデバイスを含める操作　（9 ページ）
- 展開方法について　（10 ページ）
- デバイス通信設定および証明書の管理

ステップ 1 AUS または Configuration Engine をそれぞれの製品のマニュアルに従ってセットアップします。

ステップ 2 サーバを使用するようにデバイスを設定します。以降のトピックでは、サーバのタイプおよび目的のセットアップごとに設定手順を示します。

- PIX ファイアウォールおよび ASA デバイスでの AUS の設定

ステップ 3 デバイスを Security Manager に追加するときに、選択した方法で可能であればデバイスに AUS または Configuration Engine を選択します。AUS または Configuration Engine が Security Manager にまだ定義されていない場合は、ネットワーク デバイスを追加するときに Security Manager が AUS または Configuration Engine を識別するようにできます。詳細な手順については、次のトピック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
- 設定ファイルからのデバイスの追加
- 手動定義によるデバイスの追加
- インベントリ ファイルからのデバイスの追加
- Auto Update Server または Configuration Engine の追加、編集、または削除

ヒント デバイスを Security Manager インベントリに追加すると、割り当てるサーバをデバイス プロパティで変更できます。デバイスを右クリックして、[デバイスプロパティ（Device Properties）] を選択します。デバイスを追加するときにサーバを特定できなかった場合は、デバイス プロパティを使用してサーバを設定します。

ステップ 4 デバイスで AUS を使用している場合は、Security Manager にそのデバイスの AUS ポリシーを設定します。次のいずれかを実行します。

- 単一のデバイスのポリシーを設定します。デバイスビューで、デバイスを選択し、次にデバイスポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [AUS] を選択します。
- 同じ AUS を共有する多くのデバイスに割り当てることができる共有ポリシーを設定します。ポリシービューで、ポリシータイプセレクタから [PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [AUS] を選択します。[AUS] を右クリックし、[新規AUSポリシー（New AUS Policy）] を選択してポリシーを作成するか、またはポリシーセレクタから既存のポリシーを選択してポリシーを変更します。[Assignments] タブを選択して、ポリシーを特定のデバイスに割り当てます。

このポリシーで特定するサーバは、デバイス プロパティで特定するサーバでもある必要があります。デバイス プロパティでは Security Manager が設定を送信するサーバを特定し、AUS ポリシーではデバイスが問い合わせるサーバを定義します。

ヒント AUS サーバを変更した場合、デバイスは新しい設定を受け取るまで現在の設定内に定義されている AUS サーバを引き続き使用することに留意してください。したがって、AUS ポリシーは変更しますが、設定の展開には前の AUS サーバを使用する必要があります。展開が正常に完了したあとで、新しいサーバを指し示すようにデバイス プロパティを変更します。

ステップ 5 Security Manager で、[デバイスへの展開（Deploy to Device）] 展開方式を使用して設定を展開します。Security Manager は、設定を AUS または Configuration Engine に送信し、そこでネットワーク デバイスがその設定を取得します。

使用する Workflow モードに応じて、次の手順を実行します。

- Workflow 以外のモードでの設定の展開 （35 ページ）

- Workflow モードでの設定の展開 （43 ページ）

Token Management Server への設定の展開

組織が Token Management Server（TMS）を使用して設定更新をルータに適用する必要がある場合は、TMS プロセスで Security Manager を使用できます。このタイプの展開を実行するには、デバイス、TMS、および Security Manager を正しくセットアップする必要があります。この手順では、実行する必要のあるタスクについて説明します。

関連項目

- 展開プロセスの概要 （2 ページ）
- デバイスを管理するための準備
- 展開ジョブまたは展開スケジュールにデバイスを含める操作 （9 ページ）
- 展開方法について （10 ページ）
- デバイス通信設定および証明書の管理

ステップ 1 TMS を FTP サーバとしてセットアップします。Security Manager は、FTP を使用して設定ファイルを TMS に展開します。その TMS から設定ファイルを eToken にダウンロードし、暗号化できます。次に、eToken をルータの USB ポートに接続し、設定をダウンロードできます。詳細については、TMS 製品のマニュアルを参照してください。

ステップ 2 Security Manager で、**[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [トークンの管理（Token Management）]** を選択して、Security Manager への TMS サーバーを特定します。

デフォルトでは、Security Manager は Security Manager サーバを TMS として使用しますが、別のサーバを指定できます。ホスト名かIPアドレス、TMS のユーザ名とパスワード、設定ファイルのコピー先となるディレクトリ、および公開キー ファイルの場所を Security Manager に入力する必要があります。詳細については、[チケット管理（Ticket Management）] ページを参照してください。

ステップ 3 Cisco IOS ルータに使用するトランスポート プロトコルとして TMS を指定します。

このパラメータをすべての Cisco IOS ルータ用にグローバルに設定することも、特定のデバイス用に設定することもできます。

- グローバル：**[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [デバイス通信（Device Communication）]** を選択し、**[トランスポートプロトコル（IOSルータ12.3以降）（Transport Protocol (IOS Routers 12.3 and above)）]** で [TMS] を選択します。
- デバイス：デバイスセレクタでデバイスを右クリックし、[デバイスのプロパティ（Device Properties）] を選択します。[General] タブの [Device Communications Group] で、トランスポート プロトコルとして [TMS] を選択します。すべてのルータが TMS をサポートするわけではないため、デバイスによっては TMS を設定できないことがあります。

ステップ 4 Security Manager で、[デバイスへの展開（Deploy to Device）] 展開方式を使用して設定を展開します。Security Manager は、デルタ設定を TMS サーバに送信します。

使用する Workflow モードに応じて、次の手順を実行します。

- Workflow 以外のモードでの設定の展開　（35 ページ）
- Workflow モードでの設定の展開　（43 ページ）

ステップ 5 TMS を使用して、設定を eToken にダウンロードします。詳細については、TMS 製品のマニュアルを参照してください。

ステップ 6 設定を eToken からルータにダウンロードし、設定をデバイスに保存します。eToken をルータに接続し、次のコマンドを入力して設定をルータにダウンロードします。*usb_token_id* には、使用した USB ポートに応じて、**usbtoken0** または **usbtoken1** を指定します。デフォルトの PIN は 1234567890 です。

例：

```
router# crypto pki token
usb_token_id
login
PIN

router# config terminal

router(config)# crypto pki token default secondary config CCCD

router(config)# exit

router# write memory
```

ヒント　CCCD は eToken のプライベート セクターで、ここに設定ファイルが保存されます。**crypto pki token default secondary config CCCD** コマンドを入力すると、eToken の CLI がルータの CLI とマージされます。

設定のプレビュー

デバイス設定をプレビューするには、さまざまな方法があります。デバイスセレクタからデバイスを選択してから **[ツール（Tools）] > [設定のプレビュー（Preview Configuration）]** を選択することも、いくつかのダイアログボックスで [設定のプレビュー（Preview Config）] ボタンをクリックすることもできます。

ヒント　マップビューでデバイスを右クリックし、[設定のプレビュー（Preview Configuration）] を選択することもできます。

設定をプレビューすると、設定が [Config Version Viewer] ダイアログボックスに表示されます。提示された設定が左側に表示されます。デルタ設定を表示するのか（前回の展開以降の変更を表示します）、完全な設定を表示するのかを選択できます。右ペインでは、その設定を最後にデバイスに展開した設定または現在実行中の設定と比較することもできます。

提示される設定の内容は、その内容を参照している場所によって異なります。

- **[ツール（Tools）] > [設定のプレビュー（Preview Configuration）]** を使用した場合、またはデバイスセレクタでデバイスを右クリックし、[設定のプレビュー（Preview Configuration）] を選択した場合、提示された設定にはデータベースにまだ送信していない変更が含まれています。
- 展開ジョブの作成中に設定をプレビューした場合、提示された設定にはデータベースに送信した変更だけが含まれています。この設定に含まれている変更が、展開ジョブを開始した場合にデバイスに展開される変更です。

設定をプレビューすると、デバイスを設定するときに使用する実際のデバイス コマンドを表示できます。CLI に習熟している場合は、これにより、設定が想定どおりのものであることを容易に確認できます。CLI に習熟していない場合でも、プレビューされた情報を使用して、Cisco.com でオペレーティング システムのコマンド リファレンスを参照し、詳細な情報を探すことができます。

（注） デバイスでネットワークオブジェクトを設定した後で、Cisco Security Manager を介して ASA 8.2.3 デバイスを再検出すると、新しいオブジェクトが作成されます。プレビュー設定で生成されるこれらの新しいオブジェクトの CLI は無視してください。

次に、設定をプレビューするためのヒントを示します。

- 設定オプションの多くは、1 つ以上のインターフェイスに固有のものです。ポリシーにインターフェイス名を指定する必要がある場合、プレビューした設定にポリシーのコマンドが含まれるのは、[Interfaces] ポリシーにその指定したインターフェイスを定義している場合だけです。設定をプレビューする前に、[Interfaces] ポリシーを設定していることを確認してください。
- 仮想センサーの設定をプレビューした場合は、表示されるプレビューは仮想センサーではなく親デバイスのものとなります。仮想センサーの設定は親デバイスに保存されているためです。
- ポリシーにどのコマンドが設定されるかを確認するだけである場合は、ダミーのデバイスを追加し、そのデバイスのポリシーを設定することを検討してみてください。これにより、リアルデバイスで意図しない設定変更が実施されるのを容易に防ぐことができます。ダミーのデバイスを追加するには、手動定義によるデバイスの追加で説明する手順を使用してください。
- 設定を表示するには、ポリシーを検証する必要があります。検証は、プレビューするデバイスだけでなく、すべてのデバイスを対象に実施されます。このため、目的のデバイスとは異なるデバイスに適用されるエラーおよび警告が表示されることがあります。エラーまたは警告が発生した場合は、[Preview Messages] ダイアログボックスが表示されます。ダイアログボックスには、すべてのメッセージがその重大度と有効な解決策を含めて表示されます。[OK] をクリックして、[Config Version Viewer] ダイアログボックスに進みます。[詳細（Details）] をクリックして、問題に関する詳細な情報を表示します。

次の表に、設定のプレビューに使用される [Config Version Viewer] ウィンドウのフィールドを示します。

表 *12 : [Config Version Viewer (Preview Configuration)]* ダイアログボックス

要素	説明
Proposed Config Type	表示する設定のタイプ。たとえば、完全な設定を表示することも、デルタ（最後に設定を展開してから加えられた変更）だけを表示することもできます。提示された設定は、左ペインに表示されます。
Compare to Version	提示された設定と比較する設定を選択します。選択した設定は、右ペインに表示されます。 • [None]：参照設定を空白のままにします。 • [Last Deployed]：最後にデバイスに展開した設定を表示し、その設定と提示された設定とを比較します。 • [Running Config]：デバイスで現在実行中の設定を表示し、その設定と提示された設定とを比較します。デバイスは、現在実行中の設定を取得できるようになっている必要があります。
[First Difference] ボタン	提示された設定と参照設定との間で指摘された最初の違いにカーソルを移動します。
[Previous Difference] ボタン	提示された設定と参照設定との間で指摘された 1 つ前の違いにカーソルを移動します。
[Current Difference] ボタン	現在選択されている差異をページの中央に移動します。
[Next Difference] ボタン	提示された設定と参照設定との間で指摘された 1 つあとの違いにカーソルを移動します。
[Last Difference] ボタン	提示された設定と参照設定との間で指摘された最後の違いにカーソルを移動します。
[Print] ボタン	設定を印刷します。

アウトオブバンド変更の検出および分析

設定をデバイスに展開すると、Security Manager は展開設定に基づいてアウトオブバンド変更を削除するか、または展開を取り消します（アウトオブバンド変更および展開時のその処理方法の詳細については、アウトオブバンド変更の処理方法について （14 ページ）を参照してください）。

Security Manager が展開中にアウトオブバンド変更を削除するという状況はよく発生します。ただし、Security Manager の管理外でそのような変更をデバイスに加えたのには妥当な理由が

あることもあります。このため、設定を展開する前に、アウトオブバンド変更についてデバイスを分析するようにすると効果的です。これにより、保持しておくべき設定変更をプロアクティブに再作成する機会が得られます。

（注） コンソールからデバイスを再起動すると、Config_mod 値が 0 になります。Config_mod パラメータ値は、検出または展開が完了するとすぐに保存されます。CSM で 5 分ごとにデバイスをポーリングして、config_mod パラメータ値の変更をチェックし、OOB を検出するのが理想的です。

前回のデバイスへの展開以降にデバイス設定に加えたアウトオブバンド変更があるかどうかを検出するには、さまざまな方法があります。（別のデバイス管理アプリケーションまたはCLIでの直接更新による）変更があった場合は、その変更をプレビューして、展開前にデバイスポリシーを更新するのか、展開を実施してそのようなアウトオブバンド変更を上書きするのかを判断できます（アウトオブバンド変更は、Cisco Security Manager では OOB 変更と呼ばれることもあります）。一部のシナリオでは、OOB の変更が検出されません。このような例外の処理については、アウトオブバンド変更検出の例外 （60 ページ）を参照してください。

ヒント アウトオブバンド変更を検出できるのは、IOS、ASA、PIX、FWSM の各デバイスとセキュリティコンテキストだけです。IPS デバイスでは検出できません。ただし、展開中にアウトオブバンド変更を処理するための設定は、IPS デバイスにも適用されます。その違いは、IPS デバイスでは展開前にこのような変更をプロアクティブに分析できないことです。

1つ以上のデバイスでアウトオブバンド変更があったかどうかを判断するには、デバイスビューで次のいずれかを実行します。

- **[ツール（Tools）] > [アウトオブバンド変更の検出（Detect Out of Band Changes）]** を選択します。アウトオブバンド変更について評価するデバイスを選択するように求められます。デバイスまたはデバイスグループを選択し、[>>] をクリックして選択済みリストに移動し、[OK] をクリックします。デバイスの選択の詳細については、セレクタの使用を参照してください。
- 1 つ以上のデバイスまたはデバイスグループを選択し、右クリックして [アウトオブバンド変更の検出（Detect Out of Band Changes）] を選択します。選択したデバイスが変更について評価されます。
- 展開中に、展開に含めるデバイスを選択し、[OOB変更の検出（Detect OOB Changes）] ボタンをクリックします（このボタンは [保存した変更の展開（Deploy Saved Changes）] ダイアログボックスおよび [展開：ジョブの作成または編集（Deployment—Create or Edit a Job）] ダイアログボックスにあり、現在使用中の Workflow モードによって異なります）。選択したデバイスが変更について評価されます。

展開手順の詳細については、次の情報を参照してください。

- Workflow 以外のモードでの設定の展開 （35 ページ）

- 展開ジョブの作成および編集　（44 ページ）

検出プロセスを開始すると、[OOB (Out of Band) Changes] ダイアログボックス　（61 ページ）が開き、その結果を参照できます。現在実行中の設定を取得し、Configuration Archive に格納されている最新の設定と比較することによって、選択した各デバイスが評価されます。Security Manager は、設定間の違いを評価する際、管理対象外のポリシー タイプを考慮しません。

ヒント　展開中の場合、現在実行中の設定は展開対象に提示している設定と比較されないため、アウトオブバンド変更を検出する場合は、提示された設定をプレビューして、Cisco Security Manager ポリシーに同じ変更をすでに実装しているか確認することを推奨します。展開のダイアログボックスでデバイスを右クリックし、[設定のプレビュー（Preview Config）] を選択します。提示された設定を現在実行中の設定と比較できます。詳細については、設定のプレビュー　（55 ページ）を参照してください。

[OOB Changes] ダイアログボックスには、変更検出の結果が表示されます。デバイスにアウトオブバンド変更がある場合は、デバイスセレクタのデバイスのアイコンが緑色に変わります。[OOB Details] タブの左ペインでデバイスを選択すると、Configuration Archive に最新の設定に加えられた変更が表示されます。ウィンドウの一番下にあるボタンを使用すると、変更間を移動できます。一番下にある凡例では、変更の説明に使用されるカラーコーディングについて説明しています。

変更を評価するときは、次の点を考慮してください。

- 変更を保持する場合は、Security Manager の該当するポリシーを更新してポリシーを再作成します。preview config を使用すると、ポリシーに変更を加えて目的の結果を得ることができます。Security Manager で使用される命名ルールが異なることがあるため、ポリシーがまったく同じテキストであるかどうかではなく、同じ結果をもたらすものであるかどうかを検討してください。アウトオブバンド変更の検出では、意味の違いではなく、構文の違いが検出されることに留意してください。
- 別のアプリケーションを使用して特定のポリシーのタイプを設定する場合、Security Manager ではそのポリシー タイプを管理対象外にすることを検討してください。Security Manager は、管理対象外のポリシーに関連するコンフィギュレーション コマンドを無視します。詳細については、[Policy Management] ページを参照してください。

（注）　config_mod パラメータ値は、デバイスの検出または展開が実行されるたびに保存されます。CSM では 5 分ごとにポーリングして、config_mod パラメータ値の変更をチェックし、OOB の変更が検出されます。コンソールから ASA デバイスをリロードすると、config_mod パラメータ値が 0 になり、そのデバイスは OOB 状態としてマークされます。

ヒント　展開中にアウトオブバンド変更を検出する場合、[OOB Changes] ダイアログボックスを閉じるときに、結果に基づいて展開のダイアログボックスのデバイス名が色分けされます。緑はアウトオブバンド変更、赤は検出プロセス中のエラー、色に変更がない場合はアウトオブバンド変更がないことを示しています。

アウトオブバンド変更検出の例外

変更が行われたアクティビティを承認していない場合、Cisco Security Manager データベースは更新されません。これにより、（OOB 機能が使用する）Cisco Security Manager 設定アーカイブと Cisco Security Manager データベースとの間に不一致が生じます。アクティビティを承認しない場合、Cisco Security Manager は、デバイスに適用されているアウトオブバンド（OOB）の変更を検出しません。その結果、OOB の変更が検出されたときに展開をキャンセルするように Cisco Security Manager を設定した場合でも、Cisco Security Manager は展開を停止しません（OOB の変更を上書きします）（アウトオブバンド変更の処理方法について （14 ページ）を参照）。このセクションでは、この例外とその対処方法について説明します。

ポリシーの再検出が開始されると、次のタスクが Cisco Security Manager（ワークフローモード）で実行されます。

ステップ 1　再検出後（Security Manager にすでに存在するデバイス上のポリシーの検出）、新しいデバイス設定が Cisco Security Manager 設定アーカイブに書き込まれます。

ステップ 2　ポリシーの再検出が実行されるアクティビティを承認しない場合、Cisco Security Manager データベースは新しいデバイス設定で更新されず、古い設定データを引き続き使用します。したがって、設定アーカイブと Cisco Security Manager データベースの間に不一致が生じます。これにより、デバイス上の OOB の変更が Cisco Security Manager によって上書きされる可能性があります。これは、OOB の変更が検出されたときに展開をキャンセルするように設定した場合でも発生します（アウトオブバンド変更の処理方法について （14 ページ）を参照）。

（注）　ポリシーの再検出アクティビティが承認されない場合、アウト オブ バンド（OOB）の変更は、Cisco Security Manager データベースとデバイス上の設定との間では検出されません。これは、OOB の変更は、デバイスから検出された設定で更新された Cisco Security Manager 設定アーカイブを使用して検出されるためです（上記のステップ 1 （60 ページ））。一方、アクティビティが承認されていないため、Cisco Security Manager データベースにはデバイスの以前の設定が残っています。

次のタスク

さらに、アクティビティが承認される前に検出されたデバイスに対して 設定のプレビュー （55 ページ）を実行していると、設定のプレビューに正しい設定変更が表示されません。正しい相違を確認するには、最初にアクティビティを承認するか、別のアクティビティから設定をプレビューする必要があります。

アウトオブバンド変更検出の例外

これらの例外を克服するには、次の手順を実行します。

ステップ 1 再検出のための新しいアクティビティを作成します。

ステップ 2 ポリシーの再検出が完了したら、アクティビティを送信して承認します。アクティビティが承認されているかどうかを確認します。

ステップ 3 再検出されたデバイスの設定変更が期待どおりに表示されるかどうかを確認するには、デバイスに対して設定のプレビュー （55 ページ）を実行します。

ステップ 4 必要に応じて、変更を Cisco Security Manager からデバイスに展開します。

[OOB (Out of Band) Changes] ダイアログボックス

[OOB Changes] ダイアログボックスは、デバイスのアウトオブバンド変更を表示および分析する場合に使用します。アウトオブバンド変更とは、デバイスで現在実行中の設定と、Configuration Archive に格納されている最新のデバイスの設定との違いのことです。Security Manager は、設定間に違いがあるかどうかを評価する際、管理対象のポリシータイプだけを考慮することに注意してください。

ヒント 設定は、意味の違いではなく、構文の違いが比較されます。このため、機能の等しい設定がアウトオブバンド変更であると見なされることがあります。

ヒント 例として、セマンティクスを変更せずにデバイス設定で設定行を入れ替える単純なケースを考えてみましょう。この単純な例の場合: 1) Security Manager の行番号 100 にオブジェクトグループがあり、2) ASA 設定の 100 以外の行番号に同じオブジェクトグループが存在する場合、3) Security Manager は OOB として変更を検出して報告します。この単純な例を要約すると、この数個の設定行の順序の変更によってセマンティクスがまったく変わらないとしても、Security Manager は OOB 変更を報告します。

このダイアログボックスには、タブが 2 つあります。

- [OOBの詳細（OOB Detail）]：このタブには、詳細な結果と検出プロセスの経過が表示されます。そのフィールドについては次で説明します。
- [OOBの概要（OOB Summary）]：このタブには検出結果の概要が表示されます。選択したすべてのデバイスで検出プロセスが完了して初めて使用可能になります。情報はデバイス別になっています。タイムスタンプ（日付、時刻、タイムゾーン）のほか、追加、削除、および変更を示す差異データが、関連する設定の行番号とともに表示されます。このタブでテキストを選択し、Ctrl を押しながらクリックしてクリップボードにコピーし、別のアプリケーション（メモ帳など）に貼り付けることができます。

アウトオブバンド変更の検出および分析の詳細については、アウトオブバンド変更の検出および分析 （57 ページ）を参照してください。展開中のアウトオブバンド変更の処理の詳細については、アウトオブバンド変更の処理方法について （14 ページ）を参照してください。

バージョン 4.7 以降の Security Manager には、アウトオブバンドの変更を再同期するのに役立つツールがあります。この新しいツールの詳細については、OOB 再同期Tool （63 ページ）を参照してください。

ナビゲーション パス

アウトオブバンド変更検出プロセスを開始する方法がいくつかあります。**[ツール（Tools）] > [アウトオブバンド変更の検出（Detect Out of Band Changes）]** コマンドを使用する方法もあれば、1 つ以上のデバイスを選択して右クリックし、[アウトオブバンド変更の検出（Detect Out of Band Changes）] を選択する方法もあります。このほか、次の手順での説明に従って、[保存した変更を展開する（Deploy Saved Changes）] ダイアログボックスおよび[展開（Deployment）]—[ジョブの作成（Create a job）] ダイアログボックス、または[ジョブの編集（Edit a job）]ダイアログボックスで [OOBの変更を検出（Detect OOB Changes）] ボタンをクリックする方法もあります。

- Workflow モードでの設定の展開 （43 ページ）
- 展開ジョブの作成および編集 （44 ページ）

関連項目

- 設定のプレビュー （55 ページ）
- セレクタ内の項目のフィルタリング

フィールド リファレンス

表 13 : [OOB Changes] ダイアログボックス

要素	説明
[Selected Devices] リスト（左ペイン）	このリストには、アウトオブバンド変更について評価するために選択したすべてのデバイスが記載されています。デバイス グループがある場合には、デバイスはデバイス グループ別に編成されます。 デバイスを選択すると、右ペインにその結果が表示されます。 デバイスのアイコンは、検出プロセスの結果に基づいて色が変わります。 • 緑：アウトオブバンド変更があります。 • 赤：アウトオブバンド変更検出プロセスが何らかの理由で失敗しました。 • 色変更なし：アウトオブバンド変更はありません。

要素	説明
設定比較（右ペイン）	右ペインには、選択したデバイスの変更検出プロセスの結果が表示されます。メッセージを参照すると、OOB 検出が進行中であるのか、変更がないのか、変更検出を中断させるエラーが発生したのかがわかります。 変更がある場合、右ペインにはデバイスから取得した現在実行中の設定と、Configuration Archive に格納されている最新のデバイス設定の両方が表示されます。ウィンドウの一番下にある凡例は、変更を示すのに使用されるカラー コーディングについて説明しています。次のボタンを使用して、変更間を移動できます。
[First Difference] ボタン	設定間で指摘された最初の違いにカーソルを移動します。
[Previous Difference] ボタン	設定間で指摘された 1 つ前の違いにカーソルを移動します。
[Current Difference] ボタン	現在選択されている差異をページの中央に移動します。
[Next Difference] ボタン	設定間で指摘された 1 つあとの違いにカーソルを移動します。
[Last Difference] ボタン	設定間で指摘された最後の違いにカーソルを移動します。

OOB 再同期Tool

Security Manager 4.7 の新機能である OOB 再同期ツールは、アウトオブバンドデータの再同期または調整に役立ちます。OOB 再同期ツールは、Security Manager 4.6 およびそれ以前のバージョンで利用可能な OOB 検出ツールの拡張機能であり、4.7 でも継続されています。

ヒント　この分析の後、[再同期の概要（Re-Sync Summary）] タブがアクティブになります。OOB データが発生すると、結果的にデバイスの CLI を更新する必要があります。OOB データは次のような理由で発生します。1）（主に ACL の）緊急要件。不明な検証エラーが展開をブロックしているため、Security Manager を使用してワークフロープロセスを完了させる時間がない。2）同じデバイスを管理するために Security Manager 以外の管理アプリケーションを使用する。3）ASA の Security Manager による機能サポートが完全でない場合、一部の ASA 機能を CLI を使用して管理する必要がある。サードパーティツールを使用してデバイスに加えられた変更と、デバイスに加えられた CLI の変更を合計したものが OOB データとなります。

OOB 再同期ツールは、以前に確立したポリシー構造を保持しながら、デバイス上の OOB データを Security Manager インストールに取り込むプロセスを自動化することを目的としています。

OOB 再同期ツールがないと、展開中に OOB データが検出された場合、Security Manager（バージョン 4.6 以前）は次の管理オプションしか使用できません。

- OOB 変更を警告し、オーバーライドする（デフォルト）：Cisco Security Manager は展開中に OOB 変更を検出し、ユーザーに OOB 変更を警告しますが、そのまま処理を進めて OOB 変更を取り消しまたは消去します。
- 展開を停止：OOB 変更が検出されると、展開を中止します。
- OOB 変更をチェックしない：OOB 変更は展開中に検出されず、デバイスでオーバーライドされます。

OOB 再同期ツールでは次のオブジェクトがサポートされています。

- ネットワークオブジェクト/Object-group
- セキュリティグループ
- サービス オブジェクト グループ
- ユーザーグループ
- 時間範囲オブジェクト

（注） OOB 再同期ツールは、ルータの OOB 変更をサポートしていません。

OOB 再同期ツールは、すべてのオブジェクト/ACL を再同期しません。アクセスルールと統合アクセスルールは再同期しますが、IPv6 アクセスルールなどは再同期しません。次のリストに示すポリシーの詳細に注意してください。

- アクセスルール（統合）はサポートされています
- IPv4 アクセスルールはサポートされています
- IPv6 のみのアクセスルールはサポートされていません
- Ethertype ACL はサポートされていません。
- 標準 ACL はサポートされていません。

OOB 再同期ツールのワークフローは簡単です。

1. 次のいずれかの方法を使用して既存のツールを実行することで、OOB 変更を検出します。
   - **[Configuration Manager] > [ツール（Tools）] > [アウトオブバンド変更の検出（Detect Out Of Band Changes）]**... 。
   - [Configuration Manager] > ツールバー > [OOB変更の検出（Detect OOB Changes）] アイコン
   - [Configuration Manager > [デバイスビュー（Device View）] > デバイスを右クリック > [アウトオブバンド変更の検出（Detect Out Of Band Changes）] をクリックします。
   - [保存した変更を展開する（Deploy Saved Changes）] ダイアログボックスで、[ODBの検出（Detect OOB）] をクリックします。

2. アウトオブバンド変更が検出されると、[OOBの詳細（OOB Details）] タブの [OOB （アウトオブバンド）変更（OOB (Out of Band) Changes）] ダイアログボックスの右側のペインに表示されます。[OOBの詳細（OOB Details）] タブには、変更のレポートと、ターゲットルール番号、共有ポリシー、セクション、影響を受けるデバイス、およびCLI が表示されます。

   また、アウトオブバンド変更が検出されると、 [OOB （アウトオブバンド）変更（OOB (Out of Band) Changes）] ダイアログボックスの右側のペインにある [再同期の概要（Re-Sync Summary）] タブがアクティブになります。

   既存の OOB 検出ツールによって OOB 変更が検出されたら、[評価（Evaluate）] をクリックします。その後、Security Manager は、デバイスで実行されている設定と Security Manager で使用可能な設定の違いをさらに分析します。この分析の後、[再同期の概要（Re-Sync Summary）] タブがアクティブになります。このタブで、Security Manager は、ACE、追加または削除されるオブジェクト、ルールの場所などの、追加の詳細を表示します。

（注） また、Security Manager は、デバイスビューとポリシービューの両方で、Policy Object Manager のオブジェクトについて、ポリシールールテーブルに注釈を付けます。

3. [再同期の概要（Re-Sync Summary）] タブがアクティブになると、レポートを生成し、OOB 機能でサポートされていない CLI があるかどうかを確認するオプションを選択できます。レポートを確認した後、[承認（Accept）] をクリックして変更の受け入れを選択できます。デバイスで ACL またはオブジェクトの変更の永続化操作が正常に行われた場合は、「成功」メッセージが表示されます。

（注） 共有ポリシーの一部であるアクセスルールを変更した場合、この特定のケースで、OOB 再同期ツールは実際に変更されたルールとそのすぐ上のルールの両方に注釈を付けます。これは次の場合に発生します。1）共有ポリシーの一部である少なくとも 2 つのアクセスルールを変更し、2）OOB 再同期ツールを実行し、3）変更を承認した。この場合、OOB 再同期ツールは、変更したルールに加えて、一部のルールの OOB 状態を報告します。ルール自体と共有ポリシーには悪影響がないことを理解することが重要です。

4. 左ペインの [OOBの詳細（OOB Detail）] タブで、.pdf 形式のレポートを要求できます。これを実行するには、[レポートの作成（Generate Report）] ボタンをクリックします。このレポートは必ず生成し、保存して必要に応じてトラブルシューティングに役立てることをお勧めします。

ヒント　次の例では、OOB再同期ツールを使用して、OOB再同期ツールでサポートされていないデバイスの変更と、サポートされているアクセスルールの変更を探すシナリオについて、簡単に説明します。このシナリオでは、IPv4 と IPv6 の両方を使用する ASA があるとします。**[ツール（Tools）] > [アウトオブバンド変更の検出（Detect Out of Band Changes）]** を使用してOOB 変更を見つけた場合、OOB 再同期ツールを使用する OOB 変更の再同期を選択する前に、IPv6 の変更を手動で調整する必要があります。

OOB 再同期ツールを使用する場合は、いくつかの注意事項があります。それらは次の表に記載しています。

表 *14*：警告

インターフェイスロール	インターフェイスロールに関連付けられたアクセスルールと複数のインターフェイスルールは吸収されません。ただし、ルールには注釈が付けられ、ユーザーが OOB 再同期レポートから OOB ルールをコピーし、適切なルールの場所で「ルールのインポート」を実行して OOB CLI を吸収できるようにします。
Shared Policies	共有ポリシーに影響する OOB 変更は、他のデバイスに影響するため、再同期されません。ルールには、ユーザーによるルールのインポートに役立つように注釈が付けられます。
オブジェクト	OOB 再同期プロセスでは、常にオブジェクトのオーバーライドが作成されます。ただし、そのオブジェクトのオブジェクトオーバーライドが選択的に無効になっている場合、ユーザーがそのオブジェクトのデバイスオーバーライドを有効にするまで、再同期は許可されません。
サポートされていないアクセスリスト	統合アクセスリストの導入前に存在していた IPv6 専用アクセスリストは、再同期ではサポートされません Ether Type アクセスリストの再同期はサポートされていません
OOBアクセスグループ CLI	アクセスグループ CLI の OOB 変更は吸収できません。この警告に関する詳しい説明： • このような状況（アクセスグループ CLI での OOB 変更）では、評価を選択できません。つまり、OOB 変更の再同期を選択することはできません。 • 1）OOB再同期ツールが再同期できるOOB変更と、2）アクセスグループ CLI の変更の両方が含まれる場合、 OOB 変更の再同期を選択する前に、access-group コマンドに関する変更を解決する必要があります。

コメントの条件付き再同期	アクセスリスト CLI で作成されたアウトオブバンドに追加された ACL コメントは、ルールの再同期の一部として、再同期中に吸収されます。ただし、ACL コメント単独のランダムな OOB 変更は、再同期中に吸収されません。
ルール分割	ルールは、結合されたルール内で行われた OOB 変更の再同期中に分割されます。ユーザーは、フラット化されたルールで「ルールの結合」を実行して再同期し、可能であれば元のルールに復元する必要があります。

関連項目

- アウトオブバンド変更の検出および分析 （57 ページ）
- アウトオブバンド変更の処理方法について （14 ページ）

デバイスへの設定の再展開

必要に応じて、展開ジョブを再展開できます。これは、[Failed] 状態または [Aborted] 状態のジョブに特に有益です。ジョブに含まれるすべてのデバイスに再展開することも、特定のデバイス（展開が失敗したデバイスなど）を選択することもできます。

交換したデバイスへの設定の再展開に関するヒント

ハードウェア障害などのためにデバイスを交換する必要がある場合、そのデバイスの最後の展開ジョブを再展開することはできません。Security Manager では、そのデバイスが実際は新規のデバイスであることが認識されないためです。古いデバイスの設定を新規のデバイスに展開する場合、次の選択肢があります。

- 新規デバイスのモデルとオペレーティング システム バージョンが交換対象のデバイスとまったく同じである場合は、デバイスセレクタで古いデバイスを選択して右クリックし、[設定のプレビュー（Preview Configuration）] を選択し、完全な設定を新規デバイスにコピーして貼り付けることができます。ただし、この方法では、古いデバイスの証明書が新規デバイスに移行されません。自分自身でデバイスを再登録するか、または証明書を更新する必要があります。
- 新規デバイスが古いデバイスと同じものではない場合は、Security Manager の機能セットを変更する変更で説明する手順に従ってください。

はじめる前に

- デバイスがブートストラップされていることを確認します。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。
- AUS、CNS、または TMS などの転送サーバに展開する場合は、サーバ、Security Manager 設定、およびデバイスが正しく設定されていることを確認します。

関連項目

- 展開プロセスの概要 （2 ページ）
- Workflow 以外のモードでの設定の展開 （35 ページ）
- Workflow モードでの設定の展開 （43 ページ）
- Auto Update Server または CNS Configuration Engine を使用した設定の展開 （52 ページ）
- Token Management Server への設定の展開 （54 ページ）
- デバイス通信設定および証明書の管理
- 展開方法について （10 ページ）
- Workflow 以外のモードでのジョブの状態 （5 ページ）
- Workflow モードでのジョブの状態 （7 ページ）

ステップ 1 [メイン（Main）] ツールバーで [Deployment Manager] ボタンをクリックします。

[Deployment Manager] ウィンドウが表示されます。[展開ジョブ（Deployment Jobs）] タブがアクティブでない場合は、このタブをクリックします。

ステップ 2 設定を再展開するデバイスが含まれているジョブを選択し、次のいずれかを実行します。

- Workflow 以外のモードでは、[再展開（Redeploy）] をクリックします。
- Workflow モードでは、[展開（Deploy）] をクリックします。

[Redeploy a Job] ダイアログボックスが開きます。ダイアログボックスには展開ジョブに含まれるデバイスが一覧表示され、デバイス名、使用される展開方法、前回の展開の状態、およびデバイスを更新した展開ジョブの名前が表示されます。

ステップ 3 [Redeploy a Job] ダイアログボックスで、次の作業を行います。

- [選択（Selection）] 列：[選択（Selection）] 列のチェックボックスにチェックマークを付けて、設定を再展開するデバイスを選択します。当初は失敗したすべてのデバイスが選択されています。
- [展開方法（Deployment Method）]、[接続先(Destination）]：（任意）個々のデバイスの設定を展開するのに使用する方法を変更できます。当初は、ジョブに使用されている方法が選択されています。選択できる方式は次のとおりです。
  - [デバイス（Device）]：設定をデバイスに直接展開するか、またはデバイスに指定された転送メカニズムに展開します。 詳細については、 デバイスへの直接展開 （11 ページ）または 中間サーバを使用したデバイスへの展開 （12 ページ）を参照してください。
  - [ファイル（File）]：Security Manager サーバー上のディレクトリに構成ファイルを展開します。[File] を選択する場合は、設定ファイルの展開先ディレクトリを [Destination] カラムで指定します。使用可能なディレクトリのリストから選択するには、[参照（Browse）] をクリックします。IPS デバイスではファイル展開を使用できません。詳細については、ファイルへの展開 （13 ページ）を参照してください。

（注） 複数のデバイスの展開方法を一度に設定するには、各デバイスを選択し、右クリックして、[選択した展開方法の編集（Edit Selected Deploy Method）] を選択します。[Edit Selected Deploy Method] ダイアログボックスが開き、ここで選択を行うことができます。

- [アウトオブバンド変更の動作（Out of Band Change Behavior）]：（任意）Security Manager 以外のユーザーによってデバイスに変更が加えられたことを検出した場合に、Security Manager がどのように応答するかを選択します（このような変更はアウトオブバンド変更と呼ばれます）。アウトオブバンド変更を処理する方法および使用可能なオプションの意味の詳細については、アウトオブバンド変更の処理方法について （14 ページ）を参照してください。

（注） 展開を進める前に、提示された設定を確認し、最後に展開された設定または現在実行中の設定と比較できます。デバイスの行を強調表示し、[設定のプレビュー（Preview Config）] をクリックします。詳細については、設定のプレビュー （55 ページ）を参照してください。

ステップ 4 [OK] をクリックします。

展開ジョブの中断

設定を展開しない場合または展開を延期する場合は、展開ジョブを停止できます。

中断可能な展開ジョブは、[Deploying]、[Scheduled]、または [Rolling Back] の状態にあるジョブだけです。ジョブを中断すると、保留中のデバイスへの設定の展開が停止しますが、展開が進行中のデバイス（コマンドがデバイスに現在書き込まれています）や、展開がすでに正常に完了したデバイスには影響が及びません。

ジョブを中断するには、次のいずれかを実行します。

- アクティブなジョブの稼働状態を表示しているときに、[Deployment Status] ダイアログボックスで [Abort] をクリックします。[Deployment Status Details] ダイアログボックス （40 ページ）を参照してください。
- **[管理（Manage）] > [展開（Deployments）]** を選択して [Deployment Manager] ウィンドウを開き、[展開ジョブ（Deployment Jobs）] タブでジョブを選択し、[中止（Abort）] をクリックします。

[Abort the Job] ダイアログボックスが開き、ジョブ中断の確認が求められます。[OK] をクリックして確認します。

ジョブを中断すると、保留中のデバイスの展開状態が [Aborted] に変わります。

展開を再開するには、ジョブを再展開します。詳細については、デバイスへの設定の再展開 （67 ページ）を参照してください。

関連項目

- ジョブおよびスケジュールの展開ステータスおよび展開履歴の表示 （32 ページ）
- Workflow 以外のモードでのジョブの状態 （5 ページ）

- Workflow モードでのジョブの状態 （7 ページ）

展開スケジュールの作成または編集

展開スケジュールを作成して、一定の間隔で展開ジョブを作成できます。スケジュールを使用すると、選択したデバイスで設定を定期的に更新できるようになります。

ヒント　スケジュールにデバイスを含めると、デバイス設定に変更が加えられ、その変更がデータベースにコミットされた場合にだけ、スケジュールから生成された展開ジョブにデバイスが含められます。このため、スケジューリングされた展開にデバイスが含まれていなくても、その変更をまだ送信していない場合（または Workflow モードで独立したアプルーバを使用しているときに、変更を送信したものの、まだ承認が得られていない場合）には、デバイス設定をプレビューしたときに変更が表示されることがあります。

関連項目

- 展開プロセスの概要 （2 ページ）
- ジョブおよびスケジュールの展開ステータスおよび展開履歴の表示 （32 ページ）
- 展開スケジュールの一時停止または再開 （74 ページ）

ステップ 1　[メイン（Main）] ツールバーで [展開マネージャ（Deployment Manager）] ボタンをクリックします。

[Deployment Manager] ウィンドウが表示されます。展開スケジュールがアクティブになっていない場合は、[展開スケジュール（Deployment Schedules）] タブをクリックします（[Deployment Schedules] タブ、Deployment Manager （25 ページ）を参照）。

ステップ 2　次のいずれかを実行します。

- 新規スケジュールを作成する場合は、[作成（Create）] をクリックします。
- 既存のスケジュールを編集する場合は、[展開スケジュール（Deployment Schedule）] 表でそのスケジュールを選択し、[開く（Open）] をクリックします。

[Schedule] ダイアログボックスが開きます（[Schedule] ダイアログボックス （71 ページ）を参照）。

ステップ 3　[Schedule] ダイアログボックスに少なくとも次の情報を入力します。

- スケジュールの名前。
- アプルーバを割り当てて Workflow モードを使用している場合は、アプルーバの電子メール アドレスが正しいことを確認します。また、自分の電子メールアドレスを（[Submitter] フィールドで）確認し、ジョブ状態が変わるたびに通知を受け取るかどうかを選択します。

- スケジュールを開始する最初の日付と時刻を定義し、スケジュールに基づいてどのくらいの頻度で展開ジョブを生成するかを選択します。また、スケジュールに終了日を設定し、その日以降は新規にジョブを作成しないようにするかどうかを決定します。
- [デバイスの追加（Add Devices）] をクリックし、展開ジョブに含めるデバイスをすべて選択します。デバイスを含めても、ユーザは引き続きそのデバイスに変更を加えることができ、他の展開ジョブまたは展開スケジュールにそのデバイスを含めることができます。

ユーザ ログイン クレデンシャルを使用してデバイスにアクセスするように Security Manager が設定されている場合は、スケジュール作成中にユーザ名とパスワードがキャプチャされます。パスワードを変更する場合は、スケジュールを作成し直す必要があります。

ステップ 4 [OK] をクリックスケジュールは、[Deployment Schedule] 表に追加されます。

ステップ 5 （Workflow モード限定）Workflow モードで作業している場合、さらに次の手順を完了する必要があります。

- 展開ジョブのアプルーバを使用している場合は、テーブルでスケジュールを選択し、[送信（Submit）] をクリックしてスケジュールをアプルーバに送信します。アプルーバの電子メール アドレスを確認し、アプルーバによるスケジュールの評価に役立つコメントを入力するように求められます。アプルーバがスケジュールを承認しないと、そのスケジュールはアクティブになりません。
- アプルーバを使用しない場合は、テーブルでスケジュールを選択し、[承認（Approve）] をクリックして自分自身でスケジュールを承認し、スケジュールをアクティブにします。

[Schedule] ダイアログボックス

[Schedule] ダイアログボックスは、定期的に繰り返される展開ジョブを作成する場合に使用します。

ナビゲーション パス

[管理（Manage）] > [展開（Deployments）] を選択して [Deployment Manager] ウィンドウを開き、上部ペインの [展開スケジュール（Deployment Schedules）] タブをクリックし、次のいずれかを実行します。

- [作成（Create）] をクリックして、新規スケジュールを作成します。
- スケジュールを選択し、[開く（Open）] をクリックしてそのプロパティを表示または変更します。

関連項目

- 展開スケジュールの作成または編集 （70 ページ）
- 展開スケジュールの一時停止または再開 （74 ページ）

フィールド リファレンス

表 *15 : [Schedule]* ダイアログボックス

要素	説明
Schedule Name Group このグループでは、ジョブの名前およびジョブの通知要件を定義します。	
名前	ジョブの名前。このスケジュールから個々の展開ジョブを作成すると、タイム スタンプがジョブ名に追加されます。
説明	ジョブの目的の説明。
Approver Email （Workflow 限定）	スケジュールを承認する担当者の電子メール アドレス。
説明 （Workflow 限定）	（任意）このスケジュールを保存すると、アプルーバがスケジュールを評価します。その評価に役立つ情報を指定します。
Submitter Email （Workflow 限定）	承認のためにこのスケジュールを送信している担当者の電子メール アドレス。このフィールドには当初、Security Manager へのログインに使用したユーザ アカウントに関連付けられた電子メール アドレスが入力されていますが、別のアドレスに変更できます。
Require Deployment Status Notifications （Workflow 限定）	ジョブ スケジューリングまたはそのスケジュールから作成されたジョブのジョブ状態が変わった場合に、電子メール メッセージを送信するかどうかを指定します。メッセージは、アプルーバと送信者に送信されます。
Recurrence Pattern Group このグループのフィールドには、ジョブ スケジュールを定義します。	
[開始日（Start Date）]	スケジュールの最初の日付。カレンダー アイコンをクリックして、カレンダーから日付を選択します。
Time (Start)	スケジュールを実行する日付の時刻。時間は 24 時間形式で、クライアントのタイム ゾーンではなくサーバのタイム ゾーンに基づいています。

要素	説明
定例（Recurrence）	このスケジュールに基づいて、どのくらいの頻度で展開ジョブを作成するかを指定します。 • [One time]：開始日として指定された日付の指定した開始時間にこのジョブを一度だけ実行します。 • [Hourly]：時間単位のスケジュールでこのジョブを実行します。展開ジョブの実行間隔を時間数で指定します。 • [Daily]：日次スケジュールでこのジョブを実行します。展開ジョブの実行間隔を日数で指定します。 • [Weekly]：指定した曜日にこのジョブを実行します。 • [Monthly]：月次スケジュールでこのジョブを実行します。ジョブを実行する日にちを選択し、展開ジョブの実行間隔を月数で指定します。
Run Indefinitely End Date and Time	スケジュールの有効期限日付と時刻。この時刻を過ぎると、展開ジョブは作成されません。スケジュールが期限切れにならないようにするには、[Run Indefinitely] を選択します。
Devices To Deploy Group この表には、展開ジョブに含まれるデバイスの一覧が表示されます。デバイスをリストに追加したり、リストからデバイスを削除したりするには、[デバイスの追加（Add Devices）] をクリックして、[他のデバイスの追加（Add Other Devices）] ダイアログボックスを開きます（[Add Other Devices] ダイアログボックス （73 ページ）を参照）。 ユーザ ログイン クレデンシャルを使用してデバイスにアクセスするように Security Manager が設定されている場合は、スケジュール作成中にユーザ名とパスワードがキャプチャされます。パスワードを変更する場合は、スケジュールを作成し直す必要があります。	

[Add Other Devices] ダイアログボックス

[Add Other Devices] ダイアログボックスは、展開ジョブまたは展開スケジューリングのデバイスを選択するときに使用します。リストには、実際にはポリシーが変更されていないデバイスも含まれることがあります。デバイスに手動で変更を加えたものの、デバイスを以前の設定（Security Manager データベースに格納されている設定）に戻す場合には、ジョブを作成するときに、ポリシー変更がないデバイスを追加することを推奨します。

- [使用可能なデバイス（Available Devices）] リストでジョブまたはスケジュールに含めるデバイスを選択し、[>>] をクリックしてそのデバイスを [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。

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。

- （Workflow 以外のモード）[保存した変更の展開（Deploy Saved Changes）] ダイアログボックスから、[他のデバイスの追加（Add other devices）] をクリックします。 Workflow 以外のモードでの設定の展開 （35 ページ）を参照してください。
- （Workflow モード）[展開：ジョブの作成または編集（Deployment: Create or Edit a Job）] ダイアログボックスから、[他のデバイスの追加（Add other devices）] をクリックします。 展開ジョブの作成および編集 （44 ページ）を参照してください。
- （すべてのモード） [Schedule] ダイアログボックス （71 ページ）から、[デバイスの追加（Add Devices）] をクリックします。

関連項目

- 展開ジョブまたは展開スケジュールにデバイスを含める操作 （9 ページ）
- 展開スケジュールの作成または編集 （70 ページ）
- セレクタ内の項目のフィルタリング>

展開スケジュールの一時停止または再開

アクティブな展開スケジューリングを廃棄せずに一時停止し、あとでスケジュールに基づいてジョブの作成を再開するときに再アクティブ化できます。これにより、スケジュールを一時的に無効にできます。

関連項目

- ジョブおよびスケジュールの展開ステータスおよび展開履歴の表示 （32 ページ）
- 展開スケジュールの作成または編集 （70 ページ）

ステップ 1 [メイン（Main）] ツールバーで [Deployment Manager] ボタンをクリックします。

[Deployment Manager] ウィンドウが表示されます。展開スケジュールがアクティブになっていない場合は、[展開スケジュール（Deployment Schedules）] タブをクリックします（[Deployment Schedules] タブ、Deployment Manager （25 ページ）を参照）。

ステップ 2 次のいずれかを実行します。

- アクティブなスケジュールを一時停止するには、そのスケジュールを選択し、[一時停止（Suspend）] をクリックします。

- 一時停止したスケジュールを再開するには、そのスケジュールを選択し、[再開（Resume）] をクリックします。

デバイスの設定バージョンの Configuration Archive への追加

Configuration Archive は、設定をデバイスにロールバックするときも含め、設定がデバイスまたはファイルに展開されるときには必ず新規設定バージョンで更新されます。

また、デバイスから直接設定を取得して、Configuration Archive に追加することもできます。これは、直接デバイス設定に変更が加えられたときに便利です（この変更はアウトオブバンド変更と呼ばれます）。

（注） AUS によって管理されるデバイス、およびダイナミック IP アドレスが設定されているデバイスからは、設定を取得できません。

この手順を使用すると、デバイスから設定を取得してアーカイブに追加できます。

関連項目

- アーカイブされた設定バージョンの表示および比較 （75 ページ）

ステップ 1 **[管理（Manage）] > [Configuration Archive]** を選択して、Configuration Archive を開きます（[Configuration Archive] ウィンドウ （29 ページ）を参照）。

ステップ 2 デバイス セレクタで、設定を取得するデバイスを選択します。アーカイブされた設定が右側のペインに表示されます。

ステップ 3 [デバイスから追加（Add from Device）] をクリックします。Security Manager がデバイスにログインし、現在実行中の設定を取得してアーカイブに追加します。

アーカイブされた設定バージョンの表示および比較

Configuration Archive では、デバイスの以前の設定を表示し、設定のバージョンを比較し、設定展開に関連するトランスクリプトを表示できます。Configuration Archive ウィンドウを開くには、**[管理（Manage）] > [Configuration Archive]** を選択します。

デバイスの設定バージョンを表示するには、デバイス セレクタでデバイスを選択します。アーカイブされたすべてのバージョンが右ペインに表示されます。次を実行できます。

- 設定を表示するには、その設定を選択し、[表示（View）] をクリックします。[Config Version Viewer] ダイアログボックスが開き、設定が左ペインに表示されます（ダイアログボックスの詳細については、[Configuration Version Viewer] （76 ページ）を参照してください）。

選択したバージョンに使用できる設定のタイプが複数ある場合は、[設定タイプ（Config Type）] フィールドを使用して、どのタイプを表示するかを選択できます。[フル（Full）] バージョンは設定がすべて含まれたもので、[デルタ（Delta）] バージョンはこのバージョンと、デバイスの前回の完全な設定との間で異なるコマンドだけが含まれたものです。デルタ設定には、ネガティブ コマンドが含まれることがあります。

- 設定を比較するには、その設定を選択し、[表示（View）] をクリックします。[Config Version Viewer] ウィンドウの [バージョンを比較（Compare with Version）] フィールドで比較する設定を選択します。2 つめのバージョンが右ペインに表示され、相違点がカラー コーディングで示されます。カラー コーディングについては、表示領域の下にあるキャプションを参照してください。
- 設定の展開に関連付けられたトランスクリプトを表示するには、次のいずれかを実行します。
  - [Configuration Archive] ウィンドウから、目的の設定の [Transcript] 列のアイコンをダブルクリックします。
  - [Config Version Viewer] ダイアログボックスの左ペインに設定を表示するときは、[トランスクリプトビュー（Transcript View）] をクリックします。

トランスクリプトとは、展開処理またはロールバック処理の間にキャプチャされた、Security Manager とデバイス間のトランザクション ログ ファイルです。この中には、展開要求またはロールバック要求が出た時点からサーバとデバイス間で送受信されたコマンドは含まれていますが、展開の初期検出フェーズである、Security Manager がデバイスから現在の設定を取得するときに行われた通信は含まれていません。ロールバックが失敗した場合、ロールバックまたは展開が失敗した段階によっては一部のトランスクリプトが生成されることがあります。トランスクリプトは、[Transcript Viewer] ウィンドウに表示されます（展開トランスクリプトの表示 （78 ページ）を参照）。

[Configuration Archive] 設定ページでは、アーカイブする設定バージョンの数を設定できます（[Configuration Archive] ページを参照）。

関連項目

- デバイスの設定バージョンの Configuration Archive への追加 （75 ページ）

[Configuration Version Viewer]

（Configuration Archive から開いた）[Config Version Viewer] ウィンドウは、デバイスの以前の設定を表示し、アーカイブされた他の設定と比較する場合に使用します。どのバージョンも、選択したデバイスのアーカイブにある他のバージョンと比較できます。選択したバージョンが左ペインに表示され、このウィンドウの右上にあるリストから比較対象の別のバージョンを選択できます。バージョンの表示および比較の詳細については、アーカイブされた設定バージョンの表示および比較 （75 ページ）を参照してください。

ナビゲーション パス

[管理（Manage）] > [Configuration Archive] を選択し、設定を表示するデバイスを選択します。次に、設定を選択し、[表示（View）] をクリックします。

関連項目

- [Configuration Archive] ウィンドウ （29 ページ）
- 展開トランスクリプトの表示 （78 ページ）
- アーカイブされた設定バージョンの表示および比較 （75 ページ）
- デバイスの設定バージョンの Configuration Archive への追加 （75 ページ）

フィールド リファレンス

表 *16 : [Configuration Version Viewer]* ウィンドウ（*Configuration Archive*）

要素	説明
バージョン ID（Version ID）	左ペインに表示する設定バージョン。 • [Previous]：現在選択しているバージョンよりも 1 つ前にあるバージョンを表示します。 • [Next]：現在選択しているバージョンよりも 1 つあとにあるバージョンを表示します。 • [Last]：リストの最後にあるバージョンを表示します。 • [Specific Date and Time]：指定の日付と時刻に作成されたバージョンを表示します。
Compare with version	バージョンを比較する場合は、左ペインで選択されているバージョンと比較する設定バージョン。設定は、右ペインに表示されます。相違点がまとめられ、カラー コーディングで示されます。カラー コーディングについては、ペインの下にあるキャプションを参照してください。

要素	説明
Config Type	表示できる設定のタイプ。設定のタイプは、デバイスのタイプによって異なります。タイプは [Full] または [Delta] となり、次の意味があります。 • [Full Configuration]：選択したデバイスの完全な設定で、Configuration Archive には完全な設定で保存されています。デバイスの完全な設定を比較できます。 • [Delta Configuration]：展開中に Security Manager が生成するファイルで、[Version ID] フィールドで選択されている設定と前回展開されたバージョンとの間に見られるポリシー変更を表します。 （注） アウトオブバンド変更（CLI での変更など）の場合、設定バージョンが生成され、[デバイスから追加（Add from Device）] を使用してそのバージョンを Configuration Archive に追加できますが、デルタ設定ファイルは生成されません。
[First Difference] ボタン	設定バージョン間で指摘された最初の違いにカーソルを移動します。
[Previous Difference] ボタン	設定バージョン間で指摘された 1 つ前の違いにカーソルを移動します。
[Current Difference] ボタン	カーソルを使用して、ウィンドウで現在選択している違いにフォーカスします。
[Next Difference] ボタン	設定バージョン間で指摘された 1 つあとの違いにカーソルを移動します。
[Last Difference] ボタン	設定バージョン間で指摘された最後の違いにカーソルを移動します。
[Transcript View] ボタン	[Transcript Viewer] ウィンドウを開くには、このボタンをクリックします。このウィンドウには、この設定に関連付けられたデバイス通信トランスクリプトが表示されます。
[Print] ボタン	設定を印刷するには、このボタンをクリックします。

展開トランスクリプトの表示

[Transcript Viewer] ウィンドウは、Security Manager とデバイスとの間で交換されたメッセージの記録を表示する場合に使用します。トランスクリプトとは、展開処理またはロールバック処理の間にキャプチャされた、Security Manager とデバイス間のトランザクション ログ ファイルです。この中には、展開要求またはロールバック要求が出た時点からサーバとデバイス間で送受信されたコマンドは含まれていますが、展開の初期検出フェーズである、Security Manager がデバイスから現在の設定を取得するときに行われた通信は含まれていません。詳細については、アーカイブされた設定バージョンの表示および比較 （75 ページ）を参照してください。

ナビゲーション パス

- Configuration Archive：[管理（Manage）] > [Configuration Archive] を選択して、Configuration Archive を開き、トランスクリプトを表示するデバイスを選択し、目的の設定バージョンの行にある [トランスクリプト（Transcript）] アイコンをダブルクリックします。

アーカイブされた設定を調べるときには、[Configuration Version Viewer] ウィンドウから [トランスクリプトの表示（Transcript View）] ボタンをクリックすることもできます（[Configuration Version Viewer] （76 ページ）を参照）。

- Deployment Manager：[管理（Manage）] > [展開（Deployments）] を選択して、Deployment Manager を開き、目的のデバイス展開が含まれている展開ジョブを選択します。次に、下部ペインで [詳細（Details）] タブを選択し、目的のデバイスの行にある [トランスクリプト（Transcript）] アイコンをダブルクリックします。

関連項目

- [Configuration Archive] ウィンドウ （29 ページ）
- [Deployment Manager] ウィンドウ （19 ページ）

フィールド リファレンス

表 *17 : [Transcript Viewer]* ウィンドウ

要素	説明
バージョン ID（Version ID）	トランスクリプトを表示する設定バージョン。 • [Previous]：現在選択しているバージョンよりも 1 つ前にあるバージョンのトランスクリプトを表示します。 • [Next]：現在選択しているバージョンよりも 1 つあとにあるバージョンのトランスクリプトを表示します。 • [Last]：リストの最後にあるバージョンのトランスクリプトを表示します。 • [Specific Date and Time]：指定の日付と時刻に作成されたバージョンのトランスクリプトを表示します。
Transcript Type	表示するトランスクリプトのタイプ。設定バージョンによっては、複数のトランスクリプトが関連付けられていることがあります。このフィールドを使用して、どのトランスクリプトを表示するかを選択します。

要素	説明
[Transcript] ウィンドウ	選択したトランスクリプトを表示します。テキストを選択し、クリップボードにコピーできます（Ctrl を押した状態で C を押します）。コピーしたテキストは、テキスト エディタに貼り付けることができます。
[表示（View）] ボタン	[Config Version Viewer] ウィンドウに関連する設定を表示するには、このボタンをクリックします（[Configuration Version Viewer]（76 ページ）を参照）。
[Print] ボタン	トランスクリプトを印刷するには、このボタンをクリックします。

設定のロールバック

新規設定をデバイスに展開したあと、その新規設定が正しく機能しないことがわかった場合は、設定を古いバージョンにロールバックできます。ただし、通常は、Security Manager で設定を修正し、修正された設定を展開するようにしてください。設定をロールバックすると、Security Manager に定義されている設定と、デバイスで実行中の設定が異なるという状況が発生します。設定をロールバックするのは、極端な状況にある場合だけとしてください。

以降のトピックは、設定のロールバックの理解を深めて、効果的に使用するのに役立ちます。

- 設定のロールバックについて （80 ページ）
- Deployment Manager を使用したデバイスへの設定のロールバック （88 ページ）
- ロールバックを使用したアーカイブ済み設定の展開 （89 ページ）
- ファイルへの展開時のロールバックの実行 （91 ページ）

設定のロールバックについて

展開方法として [Device] を使用して設定をデバイスに展開した場合、設定を直接デバイスに展開しようと、中間サーバに展開しようと、その新規設定が正しく機能しないことがわかったときには、設定を古いバージョンにロールバックできます。ファイルに展開された設定にはロールバックできません。

注意 通常は、Security Manager で設定を修正し、修正された設定を展開するようにしてください。設定をロールバックすると、Security Manager に定義されている設定と、デバイスで実行中の設定が異なるという状況が発生します。ロールバックを実行したあとはデバイスのポリシーを再検出し、デバイスの設定と Security Manager に格納されている設定を一致させる必要があります。設定をロールバックするのは、極端な状況にある場合だけとしてください。

次のツールを使用して、設定をロールバックできます。

- Deployment Manager：最後の正常時の設定がファイルではなくデバイスに展開されたものであれば、展開をその設定にロールバックできます。Deployment Manager を開くには、**[管理（Manage）] > [展開（Deployments）]** を選択します。
- Configuration Archive：アーカイブされた設定がデバイスに展開されたものか、デバイスから作成されたものであれば、その設定に展開をロールバックできます。Configuration Archive を開くには、**[管理（Manage）] > [Configuration Archive]** を選択します。

設定をロールバックすると、Security Manager は次の処理を実行します。

- PIX ファイアウォール、ASA デバイス、および FWSM デバイスの場合、Cisco Security Manager はデバイスの SSL インターフェイスで **replace config** オプションを使用して、リロードと同等の操作を実行します（xlate はクリアされ、IPsec トンネルは終了するなど）。
- IOS 12.3(7)T 以降が稼働するデバイスの場合、Cisco Security Manager は **configure replace** コマンドを使用して、現在実行中の設定を設定ファイルの内容に置換します。このコマンドのサポートは、デバイスにインストールされている IOS バージョンによって異なります。
  - IOS 12.3(7)T 以降が稼働するデバイスの場合、Cisco Security Manager は **configure replace** コマンドを実行する前に、構成ファイルをスタートアップ コンフィギュレーションにコピーします。設定置換操作が失敗した場合、Cisco Security Manager は **reload** コマンドを発行し、スタートアップ コンフィギュレーションの内容を使用してオペレーティングシステムをリロードします。reload コマンドは、システムを再起動するため、一時的にネットワークが停止することがあります。
  - 12.3(7)T よりも前のバージョンが稼働するルータの場合、Cisco Security Manager は構成ファイルをスタートアップ コンフィギュレーションにコピーし、**reload** コマンドを発行してシステムを再起動します。この方法を使用している場合、Security Manager は [Configuration Archive] 設定ページ（[Configuration Archive] ページを参照）に指定されている TFTP サーバおよびディレクトリを使用します。
- ロールバックされた設定は、そのデバイスの Configuration Archive で別のアーカイブされたバージョンになります。

ヒント 設定のロールバックには、ユーザ アカウント ポリシーが含まれません。設定をロールバックしても、ユーザ アカウントの既存の状態は変わりません。これにより、ユーザはこれまでどおりデバイスにログインできます。

デバイス タイプおよび設定によっては、ロールバックに特殊な考慮事項が適用されます。詳細については、次の各項を参照してください。

- マルチ コンテキスト モードのデバイスのロールバックについて （82 ページ）
- フェールオーバー デバイスのロールバックについて （82 ページ）

• Catalyst 6500/7600 デバイスのロールバックについて （83 ページ）
• IPS および IOS IPS のロールバックについて （84 ページ）
• ロールバック後、競合を発生させる可能性があるコマンド （86 ページ）
• ロールバック後、フェールオーバー設定ミスから復旧するためのコマンド （87 ページ）

関連項目

• Deployment Manager を使用したデバイスへの設定のロールバック （88 ページ）
• ロールバックを使用したアーカイブ済み設定の展開 （89 ページ）

マルチ コンテキスト モードのデバイスのロールバックについて

ロールバックしようとしているシステム実行スペースの設定にセキュリティ コンテキストへの接続オプション（vlan config など）が指定され、かつロールバック対象として選択した設定とセキュリティ コンテキストで現在実行中の設定との間に不一致がある場合、Security Manager はセキュリティ コンテキストに接続できないことがあります。そのような場合は、システム実行スペースの設定をロールバックする前に、セキュリティコンテキストの設定をロールバックすることを推奨します。

マルチコンテキストモードで動作するデバイスのシステム実行スペースの設定をセキュリティ コンテキストのセットが異なる設定にロールバックした場合、ロールバック後、デバイス上のセキュリティ コンテキストが、Security Manager で管理されていてデバイス セレクタに表示されているセキュリティ コンテキストに一致しなくなることがあります。

関連項目

• Deployment Manager を使用したデバイスへの設定のロールバック （88 ページ）
• ロールバックを使用したアーカイブ済み設定の展開 （89 ページ）
• ロールバック後、競合を発生させる可能性があるコマンド （86 ページ）
• ロールバック後、フェールオーバー設定ミスから復旧するためのコマンド （87 ページ）

フェールオーバー デバイスのロールバックについて

フェールオーバー ポリシーが含まれているセキュリティ コンテキストの設定をロールバックすると、Security Manager は当初システム実行スペースでフェールオーバーをディセーブルにし、両方のデバイスがアクティブになります。ロールバックの完了後、どちらのデバイスもそれぞれのフェールオーバー設定に戻ります。

ロールバック中にスイッチオーバーが発生した場合、またはアクティブ装置とスタンバイ装置との間で接続が失われた場合は、ロールバックの完了後、ブートストラップ設定をスタンバイ装置にコピーします。詳細については、[Bootstrap Configuration for LAN Failover] ダイアログ ボックスを参照してください。

Security Manager は、次の条件が満たされた場合にのみ、ロールバックアクションを続行できます。

- プライマリユニットとセカンダリユニットの両方がアクティブ状態である必要があります。
- リンク上で構成されている場合、リンクが稼働している必要があります。
- LAN 上で構成されている場合は、インターフェースが稼働している必要があります。

関連項目

- Deployment Manager を使用したデバイスへの設定のロールバック （88 ページ）
- ロールバックを使用したアーカイブ済み設定の展開 （89 ページ）
- ロールバック後、競合を発生させる可能性があるコマンド （86 ページ）
- ロールバック後、フェールオーバー設定ミスから復旧するためのコマンド （87 ページ）

Catalyst 6500/7600 デバイスのロールバックについて

サービス モジュールへの接続オプション（vlan config など）を指定する Catalyst 6500/7600 デバイスに設定をロールバックするときに、ロールバック対象として選択した設定と現在実行中の設定との間に不一致がある場合、Security Manager はサービス モジュールに接続できないことがあります。設定を Catalyst 6500/7600 シャーシにロールバックする前に、サービス モジュールの設定をロールバックすることを推奨します。

したがって、Catalyst 6500/7600 デバイスでロールバックを実行するための正しい順序は次のようになります。

1. セキュリティ コンテキスト。
2. サービス モジュール。
3. シャーシ。

ロールバック操作の完了後、再検出を実行することを推奨します。

FWSM 展開をロールバックしている場合、デバイスの追加時にセキュリティ証明書を取得するようにシステムが設定されていると、ロールバック操作の完了後、証明書を取得することが必要になる場合があります。このためには、次のいずれかの方法を使用します。

- デバイス プロパティからデバイス単位で証明書を取得します。
- ロールバック後に自動的に証明書を取得するように Security Manager を設定します。このためには、[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [デバイス通信（Device Communication）] を選択し、（[SSL証明書パラメータ（SSL Certificate Parameters）] の）[PIX/ASA/FWSMデバイス認証証明書（PIX/ASA/FWSM Device Authentication Certificates）] フィールドで [デバイスを追加時に取得（Retrieve while adding devices）] を選択します。

関連項目

- Deployment Manager を使用したデバイスへの設定のロールバック （88 ページ）
- ロールバックを使用したアーカイブ済み設定の展開 （89 ページ）
- ロールバック後、競合を発生させる可能性があるコマンド （86 ページ）
- ロールバック後、フェールオーバー設定ミスから復旧するためのコマンド （87 ページ）

IPS および IOS IPS のロールバックについて

（注） バージョン 4.17 以降、Cisco Security Manager は FWSM、IPS、および PIX デバイスをサポートしていません。さらに、このリリース以降、Cisco Security Manager は機能拡張を提供していません。

IPS デバイスおよび IOS IPS デバイスのロールバックには、特殊な考慮事項が適用されます。IPS デバイスおよび IOS IPS デバイスの場合、ロールバックにはセンサー更新またはシグニチャ更新のロールバックが含まれることがあります。このようになるのは、IPS デバイスおよび IOS IPS デバイスの場合、Security Manager は設定の管理をサポートするだけでなく、手動および自動によるアップグレードとシグニチャ更新という形でイメージ管理もサポートするためです。ロールバックを実施するときは、センサー更新やシグニチャ更新ではなく、設定をロールバックすることに留意してください。センサー更新とシグニチャ更新がダウングレードされるのは、どちらの更新もダウングレードしないと設定をロールバックできない場合だけです。

ロールバックは、Configuration Archive によって実施されます。IPS デバイスおよび IOS IPS デバイスの場合、現在の設定だけがアーカイブされます。あるデバイス バージョン（バージョン X など）の現在の設定が、別のデバイス バージョン（バージョン Y など）には有効でないことがあります。Security Manager は、バージョン X の設定がバージョン Y に有効であるかぎり、バージョン X の設定をバージョン Y のセンサーにロールバックします。

X の設定が Y に有効である場合、ロールバックが開始され、Security Manager は確認のダイアログボックスを表示します。X の設定が Y に有効ではない場合、Security Manager は警告ダイアログボックスを表示し、ロールバック中にセンサーをダウングレードするためのオプションを示します。ただし、このようなダウングレードがロールバックの完了に有用である場合にかぎります。

注意 IPS デバイスをダウングレードすると、IPS デバイスの一部の機能が削除されます。たとえば、エンジンをダウングレードすると、最新のシグニチャ更新を適用できなくなります。シグニチャ更新を最新の状態に維持せずに IPS デバイスを操作すると、IPS デバイスの有効性が減少します。

展開ジョブのロールバックの場合、警告ダイアログボックスには次のタイプの警告が 1 つ以上含まれています。

- Security Manager は、センサー バージョンをダウングレードしないとロールバックを実行できない IPS デバイスについて警告します。
- Security Manager は、シグニチャ レベルが変更された IOS IPS デバイスについて警告します。このようなデバイスの場合、設定の IPS 以外のセクションだけをロールバックできます。
- Security Manager は、レベルを 2 つ以上ダウングレードする必要がある IPS デバイスについて警告します。Security Manager では、このようなダウングレードは実行できません。このようなダウングレードには、Cisco IPS CLI を使用する必要があります。警告ダイアログボックスには、どのバージョンにデバイスを再イメージ化またはダウングレードする必要があるかが表示されます。

（注） IOS IPS デバイスはダウングレードをサポートしていないため、ロールバック中に IOS IPS デバイスをダウングレードするためのオプションは使用できません。

ロールバック中にセンサーをダウングレードするためのオプションがロールバックの完了に有用でない場合は、ロールバックが実行できないことと、ロールバックするデバイスでイメージを手動で再インストールする必要があることを通知するエラー メッセージが返されます。最近デバイスにインストールされた更新パッケージだけがダウングレードできるため、次のような場合にはダウングレードは有用ではありません。

- 複数の更新パッケージをデバイスにダウンロードする必要がある展開（シグニチャ更新）をロールバックする場合。
- 複数のアップグレードを実行したあとに続くロールバックの古い展開または設定を選択する場合。
- ダウングレードできないアップグレードをロールバックする場合。表 18 : センサーの有効なアップグレード タイプのダウングレード サポート （85 ページ）に示すように、メジャー、マイナー、およびほとんどのサービス パックのアップグレードはダウングレードできません。

設定のロールバックで Cisco IPS 5.1(4) よりも前のバージョンにダウングレードする必要がある場合、Security Manager は自動ダウングレードをサポートしません。指定のバージョンにデバイスを手動でダウングレードしてから、ロールバックを続行する必要があります。

表 *18* : センサーの有効なアップグレード タイプのダウングレード サポート

アップグレード タイプ	ダウングレード サポート
メジャー アップグレード	ダウングレードはサポートされません。
マイナー アップグレード	ダウングレードはサポートされません。
サービス パック更新	Cisco IPS 5.1(4) 以降からのダウングレードはサポートされません。

アップグレード タイプ	ダウングレード サポート
パッチ更新	ダウングレードがサポートされます。
シグニチャ アップデート	ダウングレードがサポートされます。
エンジン更新	ダウングレードがサポートされます。
再パッケージ（メジャー更新、マイナー更新、およびサービス パック更新に適用可能）。	5.1(4) よりも前のサービス パックの再パッケージはダウングレードできます。

注意 デバイスがダウングレードされている場合、そのデバイスで実施された Outbreak Prevention 更新が失われることがあります。

ロールバック中、デバイスに対するアウトオブバンド変更があるためにロールバックを実施できないことが検出された場合は、ロールバックが実施できないことを通知するエラーメッセージが返されます。

関連項目

- Deployment Manager を使用したデバイスへの設定のロールバック （88 ページ）
- ロールバックを使用したアーカイブ済み設定の展開 （89 ページ）

ロールバック後、競合を発生させる可能性があるコマンド

次のコマンドは、ロールバック後、競合を発生させる可能性があります。

- **http server enable** *port***http** *ip_address net_mask interface_name*

セキュリティ コンテキストだけに適用できます（システム実行スペースには適用できません）。

- **allocate-interface** {*physical_interface* | *subinterface* } **[map_name] [visible | invisible]**

context サブコマンドのシステム実行スペースだけに適用できます。

- **config-url** *diskX:/path/filename*

context サブコマンドのシステム実行スペースだけに適用できます。

- **join -failover-group** *group_number*

アクティブ/アクティブ フェールオーバーと context サブコマンドのシステム実行スペースだけに適用できます。フェールオーバー グループは、指定されていない場合、デフォルトではグループ 1 となります。

- **フェールオーバー**

システム実行スペースだけに適用できます。failover をイネーブルにすると、ピア間で設定同期がトリガーされます。

- **failover lan enable**

システム実行スペースだけに適用できます。このコマンドを省略した場合、PIX プラットフォームではシリアル ケーブル フェールオーバーを設定したことになり、ASA および FWSM ではフェールオーバー設定警告が不完全なものになります。

- **failover lan unit** {*primary* | *secondary* }

システム実行スペースだけに適用できます。このコマンドを指定していない場合、デフォルトでは両方の装置がセカンダリになります。誤った装置でロールバックが実行された場合、両方の装置がプライマリになり、どちらの装置が最初にアクティブになるかに影響を与えます。

- **failover group** *group_number*

システム実行スペースだけに適用できます。このコマンドは、アクティブ/アクティブ フェールオーバーをイネーブルにします。このコマンドを省略した場合は、アクティブ/スタンバイがイネーブルになります。

- **preempt** *delay*

システム実行スペースと failover group サブコマンドだけに適用できます。両方の装置が同時に起動するか、または指定の遅延内にプライマリが起動しない場合は、アクティブになるフェールオーバー グループが強制的に指定されます。

- **monitor-interface** *interface_name*

セキュリティ コンテキストだけに適用でき、重要なインターフェイスのヘルス モニタリングをイネーブルする場合に使用されます。このインターフェイスが「バウンス」されるか、または失敗した場合は、スイッチオーバーが発生することがあります。

関連項目

- Deployment Manager を使用したデバイスへの設定のロールバック （88 ページ）
- ロールバックを使用したアーカイブ済み設定の展開 （89 ページ）
- ロールバック後、フェールオーバー設定ミスから復旧するためのコマンド （87 ページ）

ロールバック後、フェールオーバー設定ミスから復旧するためのコマンド

ロールバック中にスイッチオーバーが発生し、2 つの装置が同期しなくなった場合は、次のコマンドを使用して復旧することが必要になることがあります。

- **failover active** *group_number*
- **failover reset** *group_number*
- **failover reload-standby**
- **clear configure failover**

これらのコマンドの詳細については、セキュリティ アプライアンスのコマンド リファレンスを参照してください。

関連項目

- Deployment Manager を使用したデバイスへの設定のロールバック （88 ページ）
- ロールバックを使用したアーカイブ済み設定の展開 （89 ページ）
- ロールバック後、競合を発生させる可能性があるコマンド （86 ページ）

Deployment Manager を使用したデバイスへの設定のロールバック

設定をデバイスに展開し、その後新しい設定に何か問題があることが明らかになった場合は、そのデバイスの以前の設定に戻って展開できます。Configuration Archive に以前の設定がない場合は、以前の設定にロールバックできません。

設定は、ファイルではなくデバイスに展開された設定にだけロールバックできます。ファイルに展開された設定をロールバックする方法の詳細については、ファイルへの展開時のロールバックの実行 （91 ページ）を参照してください。

また、Configuration Archive ツールを使用すると、デバイスからアーカイブされた設定にロールバックすることもできます。詳細については、ロールバックを使用したアーカイブ済み設定の展開 （89 ページ）を参照してください。

⚠

注意 設定をロールバックするのは、極端な状況にある場合だけとしてください。通常は、Security Manager で設定を修正し、修正された設定を展開するようにしてください。設定をロールバックすると、Security Manager に定義されている設定と、デバイスで実行中の設定が異なるという状況が発生します。ロールバックを実行したあとはデバイスのポリシーを再検出し、デバイスの設定と Security Manager に格納されている設定を一致させる必要があります。設定をロールバックするのは、極端な状況にある場合だけとしてください。処理を開始する前に、次のトピックを読んでください。

- 設定のロールバックについて （80 ページ）
- マルチ コンテキスト モードのデバイスのロールバックについて （82 ページ）
- フェールオーバー デバイスのロールバックについて （82 ページ）
- Catalyst 6500/7600 デバイスのロールバックについて （83 ページ）
- IPS および IOS IPS のロールバックについて （84 ページ）
- ロールバック後、競合を発生させる可能性があるコマンド （86 ページ）
- ロールバック後、フェールオーバー設定ミスから復旧するためのコマンド （87 ページ）

はじめる前に

設定をロールバックする場合、そのアクションはアクティビティまたは設定セッションの一部としては実行されません。つまり、デバイスはロックされません。したがって、2 人のユーザがデバイスの設定を同時にロールバックできるため、予期しない問題が発生する可能性があります。設定をロールバックする前に、[Deployment Manager] ウィンドウにデバイスのアクティブな展開ジョブがないことを確認してください。

関連項目

- ジョブおよびスケジュールの展開ステータスおよび展開履歴の表示 （32 ページ）
- Workflow 以外のモードでのジョブの状態 （5 ページ）
- Workflow モードでのジョブの状態 （7 ページ）

ステップ 1 [メイン（Main）] ツールバーで [展開マネージャ（Deployment Manager）] ボタンをクリックします。[展開ジョブ（Deployment Jobs）] タブがアクティブでない場合は、このタブをクリックします。

ステップ 2 展開ジョブ（[展開済み（Deployed）] 状態または [失敗（Failed）] 状態である必要があります）を選択し、[ロールバック（Rollback）] をクリックします。

[Rollback a Job] ダイアログボックスが開きます。ダイアログボックスには、ジョブに含まれているすべてのデバイスが表示されます。デバイスの名前、展開方法（ファイルまたはデバイス）、前回の展開の状態、デバイスを最後に更新した展開ジョブの名前なども表示されます。

ステップ 3 [Selection] 列のチェックボックスをオンにして、設定をロールバックするデバイスを選択します。デバイスへの展開を使用したデバイスだけを選択できます。デフォルトでは、[Succeeded] 状態のデバイスがすべて選択されます。

デバイスの行を強調表示し、[設定のプレビュー（Preview Config）] ボタンをクリックして、デバイスに展開する設定を表示できます。最後に展開された設定または現在実行中の設定と比較できます。詳細については、 設定のプレビュー （55 ページ）を参照してください。

ステップ 4 [OK] をクリックします。処理の確認が求められます。

ステップ 5 （任意）Security Manager に定義されている設定とデバイスで実行中の設定を一致させるには、デバイス ポリシーを再検出します（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）。

ロールバックを使用したアーカイブ済み設定の展開

Configuration Archive にある設定バージョンをその設定バージョンがアーカイブされているデバイスにロールバックできます。ただし、設定バージョンがデバイスに展開されたか、または設定がデバイスから作成された場合にかぎります。ロールバックされた設定は、そのデバイスのリストで別のアーカイブされたバージョンになります。ファイルに展開された設定をロールバックする方法の詳細については、 ファイルへの展開時のロールバックの実行 （91 ページ）を参照してください。

はじめる前に

ヒント 設定をロールバックする場合、そのアクションはアクティビティまたは設定セッションの一部としては実行されません。つまり、デバイスはロックされません。したがって、2人のユーザがデバイスの設定を同時にロールバックできるため、予期しない問題が発生する可能性があります。設定をロールバックする前に、Deployment Manager を参照して、デバイスのアクティブな展開ジョブがないことを確認してください（[管理（Manage）]> [展開（Deployments）] を選択）。

設定をロールバックするのは、極端な状況にある場合だけとしてください。設定をロールバックする前に、次のトピックを丁寧に読んでください。

- 設定のロールバックについて （80 ページ）
- マルチ コンテキスト モードのデバイスのロールバックについて （82 ページ）
- フェールオーバー デバイスのロールバックについて （82 ページ）
- Catalyst 6500/7600 デバイスのロールバックについて （83 ページ）
- IPS および IOS IPS のロールバックについて （84 ページ）
- ロールバック後、競合を発生させる可能性があるコマンド （86 ページ）
- ロールバック後、フェールオーバー設定ミスから復旧するためのコマンド （87 ページ）

関連項目

- Deployment Manager を使用したデバイスへの設定のロールバック （88 ページ）
- デバイスの設定バージョンの Configuration Archive への追加 （75 ページ）
- 展開の管理 （1 ページ）
- アーカイブされた設定バージョンの表示および比較 （75 ページ）

ステップ 1 **[管理（Manage）] > [Configuration Archive]** を選択して、Configuration Archive を開きます（[Configuration Archive] ウィンドウ （29 ページ）を参照）。

ステップ 2 デバイス セレクタで、別の設定バージョンにロールバックするデバイスを選択します。アーカイブされた設定が右側のペインに表示されます。

ステップ 3 ロールバックする設定バージョンを選択します。アーカイブされた設定がデバイスに展開されたものか、デバイスから作成されたものであれば、その設定にだけ展開をロールバックできます。ファイルに展開された設定にはロールバックできません。

ヒント ロールバックの前に設定バージョンを表示するには、[表示（View）] をクリックします。

ステップ 4 選択した設定バージョンをデバイスに展開するには、[ロールバック（Rollback）] をクリックします。経過を表示するボックスが表示され、その後設定バージョンが正常に展開されると、通知メッセージが表示されます。

ステップ 5 （任意）Security Manager に定義されている設定とデバイスで実行中の設定を一致させるには、デバイス ポリシーを再検出します（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）。

ただし、通常はデバイスのポリシーを修正し、更新した設定を再展開する方が効率的です。これにより、変更内容およびデバイスの共有ポリシー設定が保持されます。このようにしないと、ポリシーを再検出した場合に、変更内容も共有ポリシー設定も削除されます。

ファイルへの展開時のロールバックの実行

デバイスではなくファイルに展開するときには、ロールバックを直接には実行できません。ファイルに展開しているときに、以前に保存した設定に戻すための手順は次のとおりです。

関連項目

- 設定のロールバックについて （80 ページ）
- マルチ コンテキスト モードのデバイスのロールバックについて （82 ページ）
- フェールオーバー デバイスのロールバックについて （82 ページ）
- Catalyst 6500/7600 デバイスのロールバックについて （83 ページ）
- IPS および IOS IPS のロールバックについて （84 ページ）
- ロールバック後、フェールオーバー設定ミスから復旧するためのコマンド （87 ページ）
- ロールバック後、競合を発生させる可能性があるコマンド （86 ページ）

ステップ 1 **[管理（Manage）] > [Configuration Archive]** を選択して、Configuration Archive を開きます（[Configuration Archive] ウィンドウ （29 ページ）を参照）。

ステップ 2 デバイス セレクタで、別の設定バージョンにロールバックするデバイスを選択します。アーカイブされた設定が右側のペインに表示されます。

ステップ 3 ロールバックする設定バージョンを選択し、[表示（View）] をクリックします。

ステップ 4 [Configuration Version Viewer] ウィンドウで、[Config Type] を [Full] に設定します。

ステップ 5 左ペイン内をクリックし、Ctrl を押した状態で A を押し、続いて Ctrl を押した状態で C を押して、選択した設定を Windows クリップボードにコピーします。

ステップ 6 メモ帳などのテキスト エディタを開き、Ctrl を押した状態で V を押して、クリップボードの内容をテキスト ファイルに貼り付けます。

ステップ 7 ファイルを保存します。このファイルを使用して、手動でロールバックを実行できます。

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。