Image Manager の使用

Image Manager は、ネットワークの内部およびエッジファイアウォールデバイスでのイメージの配布と管理を簡素化するツールです。このツールにより、次のことが可能になります。

さまざまなタイプおよびバージョンのイメージのリポジトリをダウンロードして維持する

イメージを評価する

ネットワーク内のデバイスへのイメージのアップグレードの影響を分析する

アップグレードを準備し計画する

組み込みフォールバックおよびリカバリメカニズムを十分に使用した信頼性の高い方法でデバイスをアップグレードし、ネットワークのダウンタイムを最小限にする

この章は次のトピックで構成されています。

- イメージ マネージャの使用開始　（1 ページ）
- イメージの操作　（12 ページ）
- バンドルの操作　（16 ページ）
- デバイスの使用　（20 ページ）
- Image Manager を使用したデバイスでのイメージの更新について　（25 ページ）
- ジョブの操作　（40 ページ）
- イメージ管理のトラブルシューティング　（46 ページ）

イメージ マネージャの使用開始

Image Manager には、イメージの管理、更新が必要なデバイスの操作、およびそれらのデバイスにおけるイメージのインストールの実行に使用されるセクションが含まれています。

Image Manager 上の該当する領域の詳細については、次の項目を参照してください。

- イメージの操作　（12 ページ）
- バンドルの操作　（16 ページ）
- デバイスの使用　（20 ページ）

• ジョブの操作 （40 ページ）

Image Manager を使用する前に、次のセクションを確認する必要があります。

- この機能でサポートされているプラットフォーム
- 機能の動作を制御するために変更可能な設定
- デバイスが Image Manager と連動するように設定されていることを確認するために必要な手順

ここでは、次の内容について説明します。

- Image Manager のサポートされるプラットフォームおよびバージョン （2 ページ）
- Image Manager によってサポートされるデバイス設定 （5 ページ）
- Image Manager でサポートされるイメージタイプ （6 ページ）
- Image Manager での管理設定 （8 ページ）
- Image Manager 用のデバイスのブートストラップ （10 ページ）

Image Manager のサポートされるプラットフォームおよびバージョン

注意 バージョン 4.18 以降、Cisco Security Manager では、ASA 5512、ASA 5506、ASA 5506H、および ASA 5506W モデルの ASA 9.10(1) 以降の SFR はサポートされないため、Image Manager を介して 9.10(1) にアップグレードすると、既存の SFR 設定が失われます。

Image Manager は、ASA デバイスでのみ使用できます。次のデバイスは、Image Manager をサポートしています。

- すべてのレガシー ASA モデル：ASA 5505/10/20/40/50/80
- ASA 5585
- ASA 5515/25/35/45/55
- Catalyst 6000 の ASA-SM モジュール
- 5516-X
- 適応型セキュリティ仮想アプライアンス（ASAv）

Cisco Security Manager 4.20 以降、Image Manager は、ASA 9.13(1) 以降のデバイスで実行されている、アプライアンスモードで動作する次の Firepower デバイスをサポートしています。

- Cisco Firepower 1140 セキュリティ アプライアンス
- Cisco Firepower 1150 セキュリティ アプライアンス

- Cisco Firepower 1010 セキュリティアプライアンス
- Cisco Firepower 2140 セキュリティアプライアンス
- Cisco Firepower 2120 セキュリティアプライアンス
- Cisco Firepower 1120 セキュリティ アプライアンス
- Cisco Firepower 2110 セキュリティアプライアンス
- Cisco Firepower 2130 セキュリティアプライアンス

Cisco Security Manager 4.25 以降、Image Manager は、ASA 9.18(1) 以降のデバイスで実行されている次の Secure Firewall 3100 デバイスをサポートしています。

- Cisco FPR-3110
- Cisco FPR-3120
- Cisco FPR-3130
- Cisco FPR-3140

Cisco Security Manager 4.27 以降、Image Manager は、ASA 9.20(1) 以降のデバイスで実行されている次の Secure Firewall 4200 デバイスをサポートしています。

- Cisco FPR-4215
- Cisco FPR-4225
- Cisco FPR-4245

次のデバイスはサポートされておらず、Image Manager の統合ビューのデバイスタブでは除外されます。

- PIX ファイアウォール
- FWSM ブレード
- AUS によって管理される ASA デバイス
- Security Manager で管理されていないデバイス
- その他のデバイスタイプ：IPS およびルーター

Image Manager は、バージョン 7.x 以降の ASA デバイスのイメージアップグレードをサポートしています。アップグレードに使用できる対象イメージのバージョンに制限はありません。Security Manager 4.4 でサポートされている最新バージョンの ASA（ASA バージョン 9.0(1) および 9.1(1)）へのイメージアップグレードがテストされています。

4.9 より前のバージョンの Image Manager アプリケーションでは、サポートされているデバイスタイプのすべてのイメージがリストされていました。そこで、必要なイメージを選択してダウンロードしていました。バージョン 4.9 以降の Image Manager アプリケーションでは、特定のバージョンのイメージのみがリストされます。

Image Manager には ASDM、†リモートアクセスプラグイン、およびホストスキャンの最新のイメージがリストされます。AnyConnect バージョン 3.x および 4.x では、最新のイメージがリストされます。

ASA デバイスでは、次のイメージがリストされます。

ASA デバイスのモデル	Image Manager にリストされる ASA イメージ
5512-x、5515-x、5525-x、5545-x、5585x	9.4.1 9.3.3 9.3.2 9.3.1.SMP 9.2.3.SMP 9.2.2.4.SMP 9.2.1.SMP.ED 9.1.4.SMP.ED 9.1.5.SMP.ED 9.1.6.SMP.ED 9.1.2.SMP.ED 9.0.4.SMP.ED 8.4.6.SMP.ED
5580-x	9.1.6.SMP 9.1.5.SMP.ED 9.1.4.SMP.ED 9.1.2.SMP.ED 9.0.4.SMP.ED 8.4.6.SMP.ED
5555-x	9.4.1 9.3.3 9.3.2 9.3.1.SMP 9.2.3.SMP 9.2.2.4.SMP 9.2.1.SMP.ED 9.1.2.SMP.ED 9.0.4.SMP.ED

ASA デバイスのモデル	Image Manager にリストされる ASA イメージ
5505、5510、5520、5540、5550	9.1.6 9.1.5.ED 9.1.4.ED 9.1.2.ED 9.0.4.ED 8.4.6.ED
5506-X	9.4.1、9.3.3、9.3.2
5506H-X	9.4.1
5506W-X	9.4.1
5516-X	9.4.1
適応型セキュリティ仮想アプライアンス（ASAv）	9.3.1、9.3.2、9.4.1

（注） Image Manager の ASA イメージアップグレードは、Firepower シリーズのアプライアンス モード デバイスでサポートされます。

危険 イメージのダウングレードは制限されていませんが、ユーザー責任で実施してください。ダウングレードでは Image Manager による検証は実行されません。

Image Manager によってサポートされるデバイス設定

スタンドアロン ASA デバイスでのイメージ更新のサポートに加えて、Image Manager は、ファイルシステムを管理し、高可用性と拡張性を目指して特別に設定された ASA デバイスのシームレスなイメージ更新をサポートします。次の構成がサポートされています。

- [マルチコンテキストモード（Multiple context mode）]：単一の ASA を複数の仮想デバイス/ファイアウォールに分割できるマルチコンテキストモードの ASA。http://www.cisco.com/en/US/docs/security/asa/asa91/configuration/general/ha_contexts.html [英語] を参照してください。該当する各仮想ファイアウォールは、Security Manager では独立したデバイスとして扱われます。Image Manager が、これらの仮想デバイスをホストする物理ユニットのイメージを更新すると、すべての仮想デバイスのデバイスプロパティが新しいイメージ情報で更新されます。
- [フェールオーバー構成（Failover configuration）]：高可用性のためにフェールオーバーするように設定された 2 台の同一の ASA デバイス。これらのデバイスは、アクティブ/アク

ティブまたはアクティブ/スタンバイフェールオーバーになるように構成できます。http://www.cisco.com/en/US/docs/security/asa/asa91/configuration/general/ha_overview.html [英語] を参照してください。アクティブ/アクティブ フェールオーバー ペアでのイメージの更新は、Image Manager ではサポートされていません。Image Manager を使用してアクティブ/アクティブ フェールオーバー ペアのイメージを更新するには、1 つのユニットですべてのフェールオーバーグループをアクティブにし、他方のユニットで対応するフェールオーバーグループをスタンバイにすることによって、アクティブ/アクティブ フェールオーバー ペアを一時的にアクティブ/スタンバイに変換する必要があります。アップグレード後に、フェールオーバーペアをアクティブ/アクティブに戻すことができます。

- [クラスタ構成（Cluster configuration）]：複数の ASA（最大 8 つの ASA）を**クラスタ**と呼ばれる単一の論理ユニットとしてグループ化して、スループットと冗長性を向上させることができます。デバイスをクラスタリングする目的は、管理を簡素化し、処理速度を向上させることです。クラスタを使用することで、接続を負荷分散するために連携して動作する多数の同時接続に拡張できます。クラスタリング機能は、ASA バージョン 9.0(1) から導入されました。詳細については、http://www.cisco.com/en/US/docs/security/asa/asa91/configuration/general/ha_cluster.html [英語] を参照してください。

（注） クラスタリングは ASA 5580 と SSA 5585 のみでサポートされています。

リリース 4.4 以降、Security Manager はクラスタリングをサポートしています。Configuration Manager と Image Manager では、クラスタまたはフェールオーバーペアのすべてのデバイス/メンバーが単一のデバイスとして管理されます。つまり、制御ユニットの設定を変更すると、その変更はクラスタ内のすべてのデバイスに対して自動的に実行されます。同様に、Image Manager は、フェールオーバーまたはクラスタの一部である各物理ユニットのイメージを 1 回の操作で更新します。

マルチコンテキスト ASA のイメージ管理

バージョン 4.12 以降、Image Manager のデバイスツリービューには、ASA ソフトウェアバージョン 9.6(2) 以降を実行しているマルチコンテキスト ファイアウォール デバイスのすべてのユーザーコンテキスト（管理コンテキストとユーザーコンテキスト）が表示されます。

ユーザーコンテキストを選択し、選択したコンテキストの storage-url 情報を [ストレージ（Storage）] タブで表示できます。

[互換性のあるイメージ（Compatible Images）] タブでは、選択したユーザーコンテキストの Secure Client イメージのみを表示できます。ただし、システムコンテキストについては、すべてのイメージタイプが表示されます。

Image Manager でサポートされるイメージタイプ

Image Manager は、次のタイプのイメージをサポートしています。

- ASA システムソフトウェア
- ASDM イメージ
- VPN イメージ（Cisco Secure Desktop（CSD）、Secure Client、および Hostscan を含む）
- SSLVPN プラグインのイメージ（例：RDP、SSH、ICA など）

Image Manager は、ASA システムソフトウェアと ASA デバイス上の ASDM イメージを完全に管理します。つまり、イメージのロード、設定の変更によるイメージのアクティブ化、さらには、イメージのアップグレードプロセスを完了するために必要なデバイスのリロードを実行します。

ユーザーコンテキスト デバイスの場合、Security Manager は、コピーおよびインストール用の Secure Client イメージのみをサポートします。

Image Manager は ASA–CX イメージをサポートしていません。これには、asacx-sys-9.1.1-1.pkg などのシステムイメージと、asacx-5500x-boot-9.1.1-1.img などのブートイメージの両方が含まれます。Image Manager を使用して CX イメージを Image Manager リポジトリに追加したり、CX イメージをデバイスにプッシュしたりすることはできません。

SSL VPN イメージの取り扱い

Image Manager は、SSL VPN イメージを ASA デバイスに確実にコピーすることだけを行います。Image Manager によって SSL VPN イメージに設定コマンドまたはアクティベーションコマンドが追加されることはありません。イメージの設定は、Configuration Manager を使用して行う必要があります。

次のファイルは Image Manager では管理されないため、以前のバージョンの Security Manager と同様に、Configuration Manager から設定および展開する必要があります。

- CSD コンフィギュレーション XML
- セキュアクライアント プロファイルファイル
- DAP コンフィギュレーション XML
- フルカスタマイズ XML ファイル

Image Manager を使用して SSL VPN イメージをデバイスにコピーした後、これらのイメージを使用できるように、Configuration Manager でリモートアクセス VPN ポリシーを設定する必要があります。設定する必要があるリモートアクセス VPN ポリシーは、Configuration Manager の次のパスにあります。

- CSD パッケージ：[リモートアクセスVPN（Remote Access VPN）] > [ダイナミックアクセス（Dynamic Access）] > [Cisco Secure Desktop] グループボックス
- HostScan パッケージ：[リモートアクセスVPN（Remote Access VPN）] > [ダイナミックアクセス（Dynamic Access）] > [Cisco Secure Desktop] グループボックス

- [Secure Clientイメージ（Secure Client Image）]：[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN（SSL VPN）] > [その他の設定（Other Settings）] > [クライアント設定（Client Settings）] タブ
- プラグイン：[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）] > [プラグイン（Plug-in）] タブ

SSL VPN バイナリファイルは、VPN ポリシーで参照する前にデバイスフラッシュに存在している必要があります。そうでない場合、Security Manager は、設定を展開する前に、Image Manager を使用してこれらのファイルをデバイスに確実にプッシュする設定についてユーザーに通知する、アクティビティ検証警告を表示します。ユーザーがアクティブ化の警告を無視して続行すると、Configuration Manager はデフォルトで古い動作に戻り、これらのファイルを参照する構成を展開する前に、以前のバージョンの Security Manager で実行されていたように、イメージまたはファイルをプッシュします。ただし、ユーザーは、Image Manager を使用してこれらのファイルをコピーした場合に得られる次の利点を活用できません。

1. disk1 のような外部ディスクを使用してファイルをコピーする機能。Configuration Manager は、ファイルを disk0 にのみコピーし、外部ディスクを認識またはサポートしません。
2. Image Manager は、選択したイメージをコピーするのに十分な空き領域がディスク上にあることを検証することにより、イメージコピー中のエラーを未然に防ぎ、イメージをコピーするための十分な領域がない限り、ジョブの作成を許可しません。ユーザーは、Image Manager を使用して不要なイメージを削除することでスペースを空けることができます。

（注） Image Manager は、ASA にプッシュされる SSL VPN ファイルの互換性を検証しません。ただし、リモートアクセス VPN ポリシーで互換性のないファイルが参照されている場合、Configuration Manager はエラーを示します。

Image Manager での管理設定

Image Manager には、新しい管理設定が導入されました。これらの管理設定は、Configuration Manager の一部として設定する必要があります。

Cisco.com 証明書の設定

バージョン 4.4 以降、Security Manager には証明書信頼管理機能があります。この機能は、Cisco.com 証明書の処理改善に役立ちます。この機能の詳細については、証明書信頼管理を参照してください。

Image Manager の管理設定をするには、次の手順を実行します。

ステップ 1 [Configuration Manager] > [ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] に移動します。

Cisco Security Manager - [管理（Administration）] ページが表示されます。

ステップ 2 Workflow を設定します。

ヒント Workflow 制御設定については、Configuration Manager のマニュアルを参照してください。

a) [Workflow] を選択します。

b) インストールジョブをデバイスにインストールする前に、割り当てられた承認者がインストールジョブを明示的に承認するよう要求するには、[展開とインストールイメージの承認が必要（Require Deployment & Install Image Approval）] を選択します。このオプションを選択する場合は、適切な電子メール通知を設定してください。詳細については、『[Workflow] ページ』を参照してください。

（注） 送信者が展開ジョブを承認できるようにするには、[送信者が展開ジョブを承認可能（Submitter can Approve Deployment Job）] を選択します。

c) [保存（Save）] をクリックします。

ステップ 3 デバッグの設定をします。

a) [デバッグオプション（Debug Options）] を選択し、[Image Manager のデバッグレベル（ Image Manager Debug Level）] のドロップダウンリストから、必要なデバッグレベルを選択します。

ヒント レベルには、重大、エラー、警告、情報、およびデバッグが含まれます。デフォルトのログ レベルはエラーです。

（注） ログファイルは次のように保存されます。

- サーバーログは、**%NMSROOT%\MDC\log\operation\vmssharedsvcs.log** および **%NMSROOT%\MDC\tomcat\logs\stdout.log** にあります。
- クライアントログは **<Client Install Dir>\logs*.log** にあります。

b) [保存（Save）] をクリックします。

ステップ 4 Cisco.com のログイン情報を設定します。

a) [Image Manager] を選択します。

[Image Manager] ページが表示されます。

b) [ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] > [IPSの更新（IPS Updates）] > [サーバーの更新（Update Server）] ですでに設定されている Cisco.com に接続するためのログイン情報があり、それを Image Manager で再利用する場合は、[IPS更新設定を使用（Use IPS Updates Settings）] チェックボックスをオンにします。これはデフォルトの動作です。

（注） Cisco.com のみがサポートされ、ローカルサーバーはサポートされません。

c) [Image Manager] ページで、Image Manager のログイン情報のセットを明示的に指定する場合は、[IPS更新設定を使用（Use IPS Updates Settings）] チェック ボックスをオフにします。

[Image Manager] ページのフィールドが操作可能になります。

d) 次のフィールドに入力します。

- ユーザ名
- パスワード

- 確認

e) 必要に応じて、プロキシサーバー設定を完了して、プロキシを設定します。

1. [プロキシの有効化（Enable Proxy）] チェックボックスをオンにします。
2. 次のフィールドに入力して、プロキシを定義します。
3. IP またはホスト名（IP or Hostname）
4. ポート
5. ユーザ名
6. パスワード
7. （パスワードの）確認

f) [テスト接続（Test Connection）] をクリックして、設定した Cisco.com への接続をテストします。

g) [保存（Save）] をクリックします。

ステップ 5 イメージインストールジョブのパージ間隔の設定

a) [Image Manager] を選択します。

b) [これより古いジョブをパージ（Purge Jobs Older Than）] フィールドにパージ値を入力して、パージとパージの間に経過すべき日数を指定します。

（注） [今すぐパージ（Purge Now）] ボタンを押すと、パージ間隔基準を満たすイメージインストールジョブが即座にパージされます。

ステップ 6 イメージバックアップを設定します。

a) [Image Manager] を選択します。

b) 標準バックアップの一部としてリポジトリを含めるには、[リポジトリを含める（Include Repository）] を選択します。

注意 イメージファイルは多くの容量を消費するため、Security Manager サーバーに十分なハードディスク容量があることを確認してください。

（注） [リセット（Reset）] ボタンをクリックすると、値を、現在の変更の前に最後に保存された値にリセットできます。

c) [保存（Save）] をクリックします。

ステップ 7 [閉じる（Close）] をクリックして管理ウィンドウを閉じます。

Image Manager 用のデバイスのブートストラップ

Image Manager でのブートストラップは、ASA デバイスに対して Configuration Manager で実行するものと本質的に同じです。

イメージ管理のためにデバイスをブートストラップするには、次の手順を実行します。

ステップ 1 デバイスで HTTPS を設定して、Security Manager で ASA を管理します。

a) HTTP サーバがイネーブルであることを確認します。

b) デバイスでの HTTP 管理のために、Security Manager サーバーの IP アドレスを許可ホストとして追加します。

ステップ 2 コンフィギュレーション レジスタの設定が、実行コンフィギュレーションのイメージリストを使用してブートするように設定されていることを確認します。

a) レジスタ値：0x1、0x3、0x5、0x7、0x9

（注） レジスタ値：0x1 が推奨設定です。

b) **rommon** モードで起動するように設定しないでください（設定すると、デバイスは再起動されず、イメージのアップグレードは中止されます）。

ステップ 3 Security Manager で、[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [デバイス通信（Device Communication）] > [SSL証明書パラメータ（SSL Certificate Parameters）] に移動します。[SSL証明書パラメータ（SSL Certificate Parameters）] 領域で、[PIX/ASA/FWSMデバイス認証証明書（PIX/ASA/FWSM Device Authentication Certificates）] を [証明書認証を使用しない（Do not use certificate authentication）] に設定します。

ステップ 4 デバイスのフラッシュメモリに、ロードするイメージを保持するための十分なスペースがあることを確認します。

ヒント 必要に応じて、使用する予定のない他のイメージをデバイスから削除できます。

ステップ 5 次のように、ASA のブートイメージ/設定ポリシーを管理対象外にすることをお勧めします。

a) Security Manager で、[ツール（Tools）] > [管理（Administration）] > [ポリシー管理（Policy Management）] に移動します。

b) [ブートイメージ（Boot Image）]/[設定ポリシー（Configuration policy）] の選択をオフにします

（注） Image Manager は、イメージインストールジョブの一部としてブートイメージと ASDM イメージを構成します。したがって、ブートイメージ/構成ポリシーが管理対象外ではない場合、イメージのインストール後に設定を展開すると、Image Manager によって追加されたこれらのブートコマンドが削除されます。これを防ぐには、ブートイメージ/設定ポリシーを Security Manager で管理対象外にする必要があります。これは、[Security Managerの管理設定（Security Manager administration settings）] -> [デバイス例外設定（Device Exception Settings）] -> [ファイアウォールポリシー（Firewall Policies）] ノードから実行できます。

ステップ 6 デバイスを HPM の優先監視対象デバイスとして設定しないことをお勧めします。

ステップ 7 デバイスのすべての設定変更が送信され、展開されていることを確認します。

イメージの操作

Image Manager は、Cisco.com 上のイメージへのアクセスに加え、ネットワーク上のイメージへのアクセスも提供します。イメージにリポジトリの場所が示されている場合は、そのイメージがすでにダウンロードされていることを意味します（Cisco.com またはローカルファイルシステムから）。逆に、場所が Cisco.com であることが示されているイメージは、リポジトリにダウンロードされていません。セレクタの [イメージ（Images）] セクションで [リポジトリイメージ（Repository Images）] に移動すると、すべてのイメージが示されたリストを調べることができます。利用可能なイメージをフィルタリング、並べ替え、検索することもできます。特に、フィルタリングは、Image Manager 内の移動に使えるため便利です。すべてのイメージを始め、メインリポジトリビューの見出しを使用して、名前、バージョン、タイプなどのさまざまな属性でイメージを見つけることができます。

Image Manager は ASA-CX イメージを管理しません。Cisco.com で入手可能な CX イメージは、ダウンロード用に Image Manager に表示されません。また、ファイルシステムから CX イメージを追加することもできません。

（注） イメージリポジトリにダウンロードされたイメージのみを、イメージ アップグレード ジョブに使用できます。

（注） Security Manager リリース 4.4 以降、Security Manager が Cisco.com に接続してイメージを更新するか、イメージの更新が利用可能かどうかを確認するときに、追加の証明書検証が実行されます。最新の証明書を受け入れていない場合、更新またはダウンロードは失敗します。他の操作を続行する前に、最新の証明書を取得、表示、および受け入れる必要があります。証明書の詳細については、デバイス通信設定および証明書の管理を参照してください。

ここでは、次の内容について説明します。

- すべてのイメージの表示 （12 ページ）
- イメージのリポジトリへのダウンロード （14 ページ）

すべてのイメージの表示

最初に Image Manager を開いたとき、またはセレクタから [すべてのイメージ（All Images）] を選択したとき、システムはイメージの完全なリストを表示します。このリストには、リポジトリ内のイメージと Cisco.com 上のイメージ（まだダウンロードされていない）の両方が含まれています。一部の VPN イメージファイルは、Security Manager のインストールにバンドルされており、最初からリポジトリに表示されます。Image Manager クライアントが最初に起動したとき、またはクレデンシャルが Image Manager の Security Manager 管理設定で設定されるまで、Image Manager はクレデンシャルが設定されていないことに関する警告を表示します。

（注） Security Manager の以前のリリースでは、Image Manager リポジトリにすでに存在するパッケージ済みの SSL-VPN イメージのみが表示されていました。Security Manager リリース 4.4 以降、新しくインストールされた Security Manager でリポジトリに接続していない場合、Image Manager は、リポジトリ内の事前にパッケージ化された SSL-VPN イメージを表示するだけでなく、Cisco.com で利用可能なサポート対象の ASA イメージも一覧表示します。事前にパッケージ化されたファイルは、CSMRoot>\MDC\athena\ccometadata で入手できます。したがって、Cisco.com への初期接続を実行していない場合でも、Security Manager のリリース時点で利用可能になっていた最新のイメージを表示できます。Cisco.com で最新の更新を確認するか、Cisco.com からイメージをダウンロードするか、またはその両方を行うには、Cisco.com への接続が必要であり、Cisco.com へのクレデンシャルを設定する必要があります。イメージの可用性に関する事前にパッケージ化されたこの情報により、Cisco.com に接続していないユーザーでも、Cisco.com で入手可能な最新のイメージ（少なくとも Security Manager リリースによって Cisco.com で公開されたもの）を表示できます。この機能により、特定のデバイスタイプ/プラットフォームに互換性のあるイメージを表示することもできます。

（注） CSM は、サポートされているすべての最新のイメージを [すべてのイメージ（All Images）] ウィンドウに一覧表示します。インストールエラーやデバイスのシャットダウンを回避するには、デバイスのリストから適切なイメージインストールを使用する必要があります。

このビューは、リストされているイメージ属性のいずれかを基準にして並べ替えることができます。たとえば、イメージをサイズ別に一覧表示できます。並べ替えの基準にできる属性は次のとおりです。

- ダウンロード状態：これは最初の列であり、アイコンとして表示されます。アイコンは操作可能で、この列のアイコンをダブルクリックして、Cisco.com からのイメージのダウンロードを開始したり、進行中のイメージのダウンロードを中止したり、リポジトリからイメージを削除したりできます。これらのアクションのたびにアイコンが変化することに留意してください（緑色の矢印は Cisco.com 上の画像を示し、赤色の十字はすでにダウンロードされている画像を示し、別のアイコンはダウンロードが進行中であることを示しています）。
- イメージ（名前）
- タイプ（Type）
- バージョン
- 参照先
- Size
- 説明
- コメント（イメージについてのコメントを追加および編集できます）。

すべてのイメージを表示するには、次の手順を実行します。

ステップ 1 Cisco.com で利用可能な新しいイメージを確認します。

a) [ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] > [Image Manager] に移動して、Cisco.com にアクセスするためのクレデンシャルを設定します。

b) 右上隅にある二重矢印の [更新の確認（Check for Updates）] アイコンをクリックします。

c) CCO アカウントに暗号化イメージをダウンロードする権限があることを確認します。権限がない場合は、リンクに移動して契約に同意してから、操作を再試行してください。

更新をチェックしている間、システムには「**Updating（更新中）**」と表示されます。完了すると、「**Last updated at: <timestamp>（最終更新日時：<timestamp>）**」と表示され、[すべてのイメージ（All Images）] ビューで利用可能な新しいイメージを表示できるようになります。

ステップ 2 最近発行された Cisco.com 証明書をまだ承認していない場合、システムは、Image Manager による Cisco.com との通信が発生する前に、最新の証明書を取得、表示、および承認する必要があることを通知します。

ステップ 3 セレクタで [すべてのイメージ（All Images）] をクリックします。

イメージリストが表示されます。

ステップ 4 リストを並べ替えるには、いずれかの列見出しをクリックします。

イメージのリストは、選択した属性に従って並べ替えられます。

ステップ 5 リストをフィルタリングするには、Image Manager の検索ウィンドウを使用してキー文字列を入力します。たとえば、バージョン番号の数字を入力できます。

（注） また、一部の列見出しのフィルタ設定を使用して、表示されるリストをフィルタリングすることもできます。

（注） Cisco Secure Firewall 4200 シリーズデバイスの最新のイメージを表示するには、[更新（Refresh）] アイコンをクリックします。

イメージのリポジトリへのダウンロード

Cisco.com またはローカルファイルシステムからリポジトリにイメージをダウンロードできます。

（注） バージョン 4.4 以降、Security Manager には証明書信頼管理機能があります。この機能は、Cisco.com 証明書の処理改善に役立ちます。この機能の詳細については、証明書信頼管理を参照してください。続行するには、Cisco.com のイメージダウンロードサイトからの最新の証明書を承認している必要があります。イメージをダウンロードするサイトの証明書は、イメージに関する最新のメタデータ情報を取得するために「更新の確認」のために接続されるサイトとは異なる場合があります。そのため、「Image Meta-data Locator」URL からの証明書を承認した場合でも、イメージダウンロード URL の証明書を承認する際にエラーが発生して、イメージのダウンロードに失敗する場合があります。イメージのダウンロードを続行するには、エラーメッセージに示されたダウンロード URL からの証明書を取得して承認する必要があります。

（注） バージョン 4.9 以降、Security Manager では、cisco.com からイメージをダウンロードする前に、エンドユーザライセンス契約（EULA）を読んで同意することが義務付けられています。

Cisco Security Manager の以前のバージョンでは、すべてのイメージのダウンロードに対して、シスコ エンドユーザー ライセンス契約（EULA）と K9 プロンプトに同意する必要がありました。バージョン 4.23 以降では、イメージをダウンロードするたびに EULA および K9 のプロンプトは表示されません。

ヒント イメージは、[互換イメージ（Compatible Images）] タブからダウンロードすることもできます。詳細については、デバイス上のイメージの管理 （22 ページ）を参照してください。

イメージファイルを Security Manager リポジトリに追加するには、次の手順を実行します。

ステップ 1 Cisco.com からイメージをダウンロードするには、次の手順を実行します。

a) [すべてのイメージ（All Images）] ビューで、最初の列にある [ダウンロードの開始（Start Download）] アイコンをダブルクリックします。

ヒント Cisco.com へのログイン情報が設定されており、イメージをダウンロードする権限があることを確認してください。

（注） ダウンロードするイメージがリポジトリにすでに存在する場合、Image Manager はエラーメッセージを表示します。ファイル名とチェックサムが同じ場合、システムはダウンロードをスキップします。

ダウンロードの進行状況を示す [ダウンロード（Downloads）] ウィンドウが表示されます。

ヒント ダウンロードの進行に応じて、進行状況アイコンが変化する場合があります。緑色のチェックアイコンに [展開済み（Deployed）] という単語が付いている場合、成功を示します。赤いXアイコンは失敗を示します。失敗した場合は、[ダウンロード（Downloads）] ウィンドウでそのイメージの失敗の原因を表示できます。メッセージをダブルクリックして、エラーの完全な詳細を表示できます。

b) 完了したら、[リポジトリイメージ（Repository Images）] を選択し、リストにイメージを表示します。

ヒント 複数のイメージを選択して、それらを右クリックしてコンテキストメニューを使用して一度にダウンロードすることもできます。

ヒント 更新時刻でリストをソートすることで、最新のイメージを簡単に見ることができます。

ステップ 2 ローカルファイルシステムからイメージをダウンロードするには、次の手順を実行します。

a) [リポジトリイメージ（Repository Images）] ビューのツールバーから、[イメージをファイルシステムからダウンロード（Download image from file system）] アイコン（左端）をクリックします。

[ファイルシステムからダウンロード（Download from File System）] ダイアログボックスが表示されます。

b) 参照機能を使用して、インポート場所を選択し、インポートするイメージを選択します。
c) [OK] をクリック
d) [イメージをファイルシステムからダウンロード（Download image from file system）] ダイアログボックスで [OK] をクリックします。
e) ダウンロードの経過表示を監視します。

（注） ダウンロードするイメージがリポジトリにすでに存在する場合、システムはエラーを表示します。

f) 完了したら、Security Manager でデバイスグループを選択し、リストのイメージを表示します。

ヒント 更新時刻でリストをソートすることで、最新のイメージを簡単に見ることができます。

g) または、ドラッグアンドドロップ方法を使用してイメージファイルをダウンロードすることもできます。たとえば、1つまたは複数のファイルをデスクトップからドラッグして、Image Managerアプリケーションにドロップするだけです。

バンドルの操作

バンドルとは、ユーザーが定義する互換性のあるイメージのグループです。バンドルを使用すると、事前に検証されたイメージをグループ化して論理グループとしてまとめて機能させることで、反復的な操作を簡素化できます。たとえば、ASA と ASDM のペアを反映するバンドルを定義して、1 回の操作で両方のタイプを展開することができます。次のタイプのイメージをバンドルの一部にすることができます。

- ASA システムソフトウェア

- ASDM イメージ
- VPN イメージ（csd、Secure Client、Hostscan を含む）
- プラグイン（rdp、ssh、ica、owa などを含む）

複数のシステム ソフトウェア イメージを同じバンドルに含めることはできません。

注意 Image Manager は、バンドルの一部として互換性のないイメージを追加することを阻止しません。この互換性はユーザーが判断する必要があります。ASA と ASDM の互換性マトリックスは、http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html#wp42231 にあります。

ヒント Image Manager 全体で、1 つのイメージ、複数のイメージ、または（事前定義された）イメージのバンドルを適用するように選択できる操作があります。

ここでは、次の内容について説明します。

- バンドルの作成 （17 ページ）
- バンドル別のイメージの表示 （18 ページ）
- バンドルの名前変更 （19 ページ）
- バンドルの削除 （19 ページ）
- バンドルからのイメージの削除 （19 ページ）

バンドルの作成

イメージのバンドルを定義して、 Image Managerを簡素化できます。バンドルは、定期的に操作するイメージのグループがある場合に特に便利です。

バンドルを作成するには、次の手順を実行します。

ステップ 1 セレクタの [バンドル（Bundles）] 見出しから、[バンドルの追加（Add Bundle）]（プラス記号）アイコンをクリックします。

ステップ 2 表示される [バンドルの作成（Create Bundle）] ダイアログボックスに、新しいバンドルの名前を入力します。

ステップ 3 [OK] をクリック

バンドルは、セレクタの [バンドル（ Bundles）] 見出しの下に一覧表示されます。

ステップ 4 セレクタの [イメージ（Images）] セクションから、バンドルするイメージを選択します。次に、[リリースノート（Release Notes）] タブをクリックします。最後に、該当するリリースノートの互換性テーブルを調べて、バンドルする他のイメージとの競合がないことを確認します。

注意 Image Manager は、バンドルの一部として互換性のないイメージを追加することを阻止しません。この互換性を判断するのはユーザの責任です。ASA と ASDM の互換性マトリックスは、http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html#wp42231 にあります。

ステップ 5 互換性を判断したら、各イメージをバンドルにドラッグアンドドロップします。

（注）
- 複数のシステム ソフトウェア イメージを同じバンドルに含めることはできません。
- すべてのデバイスで、バンドルに追加された同じイメージセットへのアップグレードが必要な場合は、バンドルを任意の数のデバイスに割り当てることができます。

ヒント ドラッグアンドドロップするイメージの範囲を選択するには、範囲の最初のイメージを選択し、Shift キーを押しながら範囲の最後のイメージを選択します。Ctrl キーを押しながらイメージをクリックすると、複数の画像を選択できます。イメージの範囲を選択してから、Ctrl キーを使用して選択した範囲にイメージを追加することもできます。複数のイメージを 1 つのバンドルに移動するには、マウスの右ボタンを使用してドラッグします。

バンドル別のイメージの表示

バンドルに追加されたイメージを表示できます。

バンドル内のイメージを表示するには、次のいずれかを実行します。

ステップ 1 すべてのバンドルに含まれるイメージを表示するには、次のように操作します。

a) セレクタの [バンドル（Bundles）] 見出しの下で、最上位の [バンドル（Bundles）] フォルダをクリックします。

すべてのバンドルが、それぞれに含まれるイメージとともにリストされます。

b) バンドルを展開したり折りたたんだりして、見やすくすることができます。すべてのバンドルを展開するか、すべてのバンドルを折りたたむには、メインウィンドウの上部にある [すべて展開（Expand All）] ボタンと [すべて折りたたむ（Collapse All）] ボタンを使用します。

ステップ 2 特定のバンドルの画像を表示するには、次のように操作します。

a) セレクタの [バンドル（Bundles）] 見出しの下で、バンドルを選択します。

選択したバンドルのイメージの一覧がメインウィンドウに表示されます。

ステップ 3 特定のバンドルを表示するには、次のように操作します。

a) セレクタの [バンドル（Bundles）] セクションで、[検索（Search）]（拡大鏡のアイコン）をクリックします。

b) [バンドル（Bundles）] バナーの下の検索フィールドにバンドル名を入力します。

バンドルのリストには、指定されたバンドルのみが表示されます。

バンドルの名前変更

バンドルの名前を簡単に変更して、編成を改善したり、バンドルの内容をより正確に反映したりできます。

バンドルの名前を変更するには、次の手順を実行します。

ステップ 1 セレクタの [バンドル（Bundles）] 見出しから、バンドルを選択します。

ステップ 2 バンドル名を右クリックし、ドロップダウンリストから [バンドル名の変更（Rename Bundle）] を選択します。

[名前の変更（Rename）] ダイアログボックスが表示されます。

ステップ 3 新しいバンドル名を入力します。

ステップ 4 [OK] をクリックします。

バンドルの下のセレクタに新しいバンドル名が表示されます。

バンドルの削除

不要になったバンドルは削除できます。

バンドルを削除するには、次の手順を実行します。

ステップ 1 バンドルを選択します。

ステップ 2 セレクタの [バンドル（Bundles）] 見出しから、[削除（Delete）]（赤い X アイコン）をクリックします。または、選択したバンドルを右クリックして、[バンドルの削除（Delete Bundle）] を選択します。

バンドルからのイメージの削除

バンドルの内容を変更する場合は、バンドルの一部として定義されているイメージを削除できます。

バンドルからイメージを削除するには、次の手順を実行します。

ステップ 1 バンドルを選択します。

ステップ 2 削除するイメージを右クリックします。

ステップ 3 [バンドルからイメージを削除（Delete Image from Bundle）] を選択します。または、テーブルの最上部にある [削除（Delete）] ボタンをクリックします。

デバイスの使用

次のトピックでは、Image Manager でのデバイスの操作方法について説明します。

（注） クラスタの場合、ストレージからのファイルのダウンロードをサポートしているのは制御ユニットだけです。

ここでは、次の内容について説明します。

- デバイス インベントリの表示 （20 ページ）
- デバイス上のイメージの管理 （22 ページ）
- デバイスメモリの表示 （23 ページ）
- イメージのインストール場所の設定 （24 ページ）

デバイス インベントリの表示

[デバイスの概要（Device Summary）] ページを使用して、ネットワーク上のデバイスとその属性をすばやく表示できます。

左側のセレクターパネル内には、[デバイス（Devices）] と呼ばれる領域があります。その領域から、[すべて（All）] を選択すると、すべてのデバイスを表示できます（または、定義した場所またはデバイスのグループを選択できます）。デバイス選択の範囲を選択すると、対応するデバイスが [デバイスの概要（Device Summary）] ページの上部パネルに表示されます。[デバイスの概要（Device Summary）] ページの上部ウィンドウには、必要に応じて、各デバイスの次の属性が表示されます。

- デバイスの表示名
- モード（たとえば、スタンドアロン、アクティブ-アクティブ。アクティブ-スタンバイ、クラスタ）
- システムの SW バージョン
- ASDM のバージョン
- Secure Client バージョン
- セキュアデスクトップのバージョン
- Hostscanのバージョン

[デバイスの概要（Device Summary）]テーブルには、[モード（Mode）]列が含まれます。この列では、クラスタ、スタンドアロン、アクティブ-アクティブ、アクティブ-スタンバイなどのモードを指定します。

フェールオーバーやクラスタ設定のように、複数の物理デバイスがグループ化されている設定の場合、各物理ユニット/メンバーには独自のファイルシステムがあります。また、これらのファイルシステムは異なる場合があります。各物理デバイス/メンバーのファイルシステムの詳細は、Image Manager 内で表示できます。

ストレージやイメージのステータスなど、個々のクラスタメンバーの詳細は、Security Manager ユーザーインターフェイスに表示されます。イメージ管理インベントリデータの検出中に、各クラスタメンバーのストレージに関する詳細と実行中のイメージの詳細が検出されます。

[デバイスの概要（Device Summary）]ページでフェールオーバーまたはクラスタデバイスを選択すると、グループ内の個々の物理メンバーが中央のデバイスビューテーブルに表示されます。クラスタデバイスのデバイスビューテーブルには、クラスタメンバーに関する次の情報が表示されます。

- [名前（Name）]：デバイスまたはクラスタメンバーの名前。
- [ID]：クラスタメンバー ID。
- [ステータス（Status）]：クラスタ内のメンバーのロール。たとえば、クラスタコントロールまたはクラスタデータ。
- [シリアル番号（Serial Number）]：クラスタデバイスのシリアル番号。
- [実行中のOSバージョン（Running OS Version）]：特定のメンバーの OS のバージョン。
- [CCL IP]：クラスタリンクの IP アドレス。
- [CCL MAC]：クラスタリンクの MAC アドレス。
- [サイトID（Site ID）]：クラスタデバイスのサイト ID。

フェールオーバーデバイスのデバイスビューテーブルには、名前、ステータス（スタンバイまたはアクティブなど）、シリアル番号、RAM サイズ、および実行中の OS バージョンを含む列があります。フェールオーバー デバイス テーブルには、フェールオーバー ペア ノードのプライマリデバイスとセカンダリデバイスごとにこれらの要素が一覧表示されます。

[デバイスの概要（device summary）] ページで特定のデバイスを選択すると、下部のウィンドウに、そのデバイスの詳細に関する次のタブ付きページが表示されます。

- [概要（Summary）]：表示名、デバイスタイプ、IP アドレス、ホスト名、ドメイン名、シリアル番号、実行中の OS バージョン、ターゲット OS バージョン、RAM、フェイルオーバーモード、イメージのインストール場所
- [互換性のあるイメージ（Compatible Images）]：デバイスと互換性のあるオメージ（イメージ、タイプ、バージョン、場所、サイズ、説明、コメント）。
- [履歴（History）]：デバイスで実行されたイメージのインストールジョブおよび設定展開ジョブの時系列ビュー（ジョブ名、変更者、状態、最後のアクション、チケット）

中央の [デバイスビュー（Device View）] でフェールオーバーまたはクラスタデバイスの特定のメンバーを選択すると、下部のウィンドウに、その物理デバイスに関する次のタブ付きの詳細が表示されます。

- [概要（Summary）]：実行中の OS バージョン、ターゲット OS バージョン、RAM
- [ストレージ（Storage）]：フラッシュメモリユニットの数とキャパシティ。名前、サイズ、パス、タイプ、ディスク使用量
- [実行中のイメージ（Running Images）]：現在動作中のイメージ。名前、タイプ、バージョン、パス、サイズ

デバイス上のイメージの管理

[イメージ管理（Image Management）] ツールを使用して、選択した ASA デバイス上のイメージを確認、ダウンロード、および削除できます。

デバイス上の ASA イメージを確認、ダウンロード、または削除するには、次の手順を実行します。

ステップ 1 セレクタパネルの [デバイス（Devices）] 領域でデバイスグループを選択します。

メインウィンドウにデバイスの概要が表示されます。デバイスの概要には、デバイスおよび関連するシステムソフトウェアのバージョンが一覧表示されます。

ヒント または、[デバイス（Devices）] バナーから検索機能（虫眼鏡アイコン）を選択し、表示される検索フィールドにデバイス名を入力することもできます。

ステップ 2 [デバイスの概要（Device Summary）] ページの上部ペインから、デバイスを選択します。

（注） 特定のデバイスがクラスタの一部である場合、クラスタ内を移動してデバイスの詳細を表示できます。

下部ペインに、選択したデバイスの詳細が表示されます。

ステップ 3 下部ペインで [ストレージ（Storage）] タブを選択し、[ディスク使用量（Disk Usage）] に表示される空き容量を確認します。

（注） 特定のデバイスがクラスタの一部である場合、クラスタ内を移動してストレージの詳細を表示できます。

ヒント デバイスには、disk1 などの複数のストレージ領域がある場合があります。 下にスクロールして、セカンダリ（フラッシュ）ストレージ容量を確認してください。

ステップ 4 デバイスで使用可能なディスク領域を確認します。

ステップ 5 デバイスから 1 つまたは複数のイメージを削除してスペースを解放するには、[ストレージ（Storage）] タブで 1 つまたは複数の画像を選択し、[ストレージ（Storage）] タブの上部にある [削除（Delete）] をクリックします。

ヒント　または、1つまたは複数のイメージを選択し、右クリックして[削除（Delete）]をクリックします。

ヒント　現在アクティブであり参照されているイメージを削除すると、Image Managerに警告メッセージが表示されます。

ステップ 6　デバイスからイメージをダウンロードするには、イメージを選択し、[ストレージ（Storage）] タブの上部にある[ダウンロード（Download）]をクリックします。イメージのダウンロード先のローカルファイルシステム上の場所を選択し、[OK] をクリックします。

（注）　クラスタデバイスの場合、イメージのダウンロードは制御ユニットでのみサポートされます。同様に、フェールオーバーデバイスの場合、イメージのダウンロードは、ペアのアクティブデバイスでのみサポートされます。

デバイスからのダウンロードの進行状況を示すダイアログが表示されます。ダウンロードが完了すると、ダウンロードしたイメージがエクスプローラに表示されます。

ステップ 7　下のペインで [互換性のあるイメージ（Compatible Images）] タブを選択します。

デバイスと互換性のあるイメージが表示されます。

ステップ 8　互換性のあるイメージをデバイスにインストールするには、次の手順を実行します。

a) デバイスに追加するイメージを選択します。
b) ダウンロードアイコンをダブルクリックします。

イメージがリポジトリにダウンロードされます。

c) イメージを選択し、コンテキストメニューから [インストール（Install）] を選択します。

インストールウィザードが表示され、イメージがインストールされます。詳細については、互換性のあるイメージのデバイスへのインストール （38 ページ）を参照してください。

デバイスメモリの表示

Image Manager を使用して、ネットワーク内のデバイスのメモリ容量とアプリケーションを判断できます。

（注）　メモリ容量は物理デバイスのみで表示でき、クラスタでは表示できません。

デバイスのメモリの詳細を表示するには、次の手順を実行します。

ステップ 1　セレクタパネルの [デバイス（Devices）] 領域から、調べるデバイスを選択します。

選択したデバイスの詳細は、[デバイスの概要（Device Summary）] ページの上部のウィンドウに表示されます。

ステップ 2 上部のパネルで、RAM のリストを調べます。

注意 新しいイメージをロードするのに十分な RAM がデバイスに存在しない場合、Image Manager は警告を表示します。ただし、システムはそのようなイメージアップグレードの実行を停止しません（これは、RAM が不足している場合に展開ジョブが停止する設定展開とは対照的です）。

イメージのインストール場所の設定

ASA デバイスには、すべてのイメージが存在するデフォルトのフラッシュ（disk0）があります。デフォルトでは、Image Manager はイメージを ASA デバイスの disk0 にコピーします。ASA デバイスが外部ディスク（つまり、disk1）で構成されている場合、Image Manager では、ASA デバイスにイメージをロードするときに、2 つのディスク（disk0 または disk1）のいずれかを選択できます。

（注） 外部ディスクにイメージをロードする機能は、Secure Client 用や CSD 用などの大きなイメージを保存する場合に非常に役立ちます。これは、これらの大きなイメージがいくつかあるだけで disk0 の領域がすぐに不足する可能性があるためです。

外部ディスクを使用するように Image Manager を設定するには、次の手順を実行します。

ステップ 1 セレクタの [デバイス（Devices）] 領域でデバイスを選択します。

ステップ 2 右側のペインには、概要情報が表示されます。

デバイスで使用可能なディスクは、[イメージのインストール場所（ Image Install Location）] ドロップダウンリストに表示されます。外部ディスクを備えたデバイスの場合、disk0 と disk1 がリストされます。

ステップ 3 [イメージのインストール場所（ Image Install Location）] ドロップダウンリストから外部ディスク disk1 を選択し、[適用（Apply）] をクリックします。ユーザコンテキスト デバイスの場合、共有ラベルまたはプライベートラベルを選択して、デフォルトのインストール場所を適用できます。

このデバイスの今後のすべてのイメージインストールジョブでは、イメージは disk1 にロードされます。

ヒント 外部ディスクの構成は、イメージインストール操作を実行することで確認できます。ジョブが完了したら、Image Managerで、デバイスの [ストレージ（Storage）] タブの disk1 の内容を確認します。新しくインストールされたイメージが一覧表示されます。

（注） クラスタデバイスとフェールオーバーデバイス、およびマルチコンテキストデバイスの場合、一部の物理メンバーデバイスに、イメージのインストール場所として選択されたディスクがない場合、イメージをコピーまたはインストールしようとすると、検証エラーが発生します。イメージのコピーまたはインストールを続行するには、すべてのメンバーデバイスに存在するディスクをイメージのインストール場所として選択する必要があります。

Image Manager を使用したデバイスでのイメージの更新について

Image Manager が ASA デバイスのイメージを更新する仕組み

Image Manager は、標準の文書化された手順に従って、信頼性の高いイメージアップグレードを保証するためのいくつかの組み込みチェックを使用して、スタンドアロン ASA デバイスをアップグレードします。イメージのアップグレード手順については、http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a008067e9f9.shtml#maintask2 を参照してください。

（注） Image Manager が cisco.com に接続できるようにするには、最新の Cisco.com 証明書を受け入れている必要があります。イメージのダウンロードを正常に開始するには、「イメージメタデータロケータ」サイトとイメージのダウンロードサイトの両方からの証明書を受け入れる必要があります（[Image Manager] ページを参照）。

Image Manager は、HTTPS プロトコルを使用してイメージを ASA デバイスにコピーし、設定変更を実行して新しいイメージをアクティブ化し（エラーが発生した場合の古いイメージへのフォールバックを保証）、最後に、必要に応じて新しいイメージでデバイスをリロードします。

Image Manager がフェールオーバー用に設定された ASA のイメージを更新する仕組み

アクティブ/スタンバイ フェールオーバー ペアのイメージを更新するには、ペアのアクティブ デバイスでイメージ アップグレード ジョブを作成し、そのイメージ アップグレード ジョブを実行します。

アクティブ/アクティブ フェールオーバー ペアでのイメージの更新は、Image Manager ではサポートされていません。アクティブ/アクティブ フェールオーバー ペアの場合は、一方のユニットですべてのフェールオーバーグループをアクティブにし、他方のユニットで対応するフェールオーバーグループをスタンバイにすることによって、アクティブ/スタンバイに変換する必要があります。その後にのみ、Image Manager は、デバイスのペアのイメージを更新できます。

アクティブ/アクティブ フェールオーバー ペアのデバイスをアップグレードするには、次の手順を実行します。

1. すべてのフェールオーバーグループを一方のデバイスで**アクティブ**にし、他方のデバイスで**スタンバイ**にすることによって、ペアをアクティブ/スタンバイに手動で変換します。

（注） Security Manager でデバイスを検出しないでください。

（注） アクティブ/アクティブ フェールオーバー ペアをアクティブ/スタンバイに変換する方法の詳細については、http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a0080b20f35.shtml#Actact を参照してください。

2. ペアのアクティブデバイスでイメージアップグレードジョブを作成し、そのイメージアップグレード ジョブを実行します。
3. アップグレードの実行後に、必要なフェールオーバーグループを一方のユニットでアクティブにし、残りのフェールオーバーグループを他方の物理ユニットでアクティブにして、アップグレード前と同じように、ペアを手動でアクティブ/アクティブ構成に戻します。
4. Security Manager で、スタンバイに変換したユニットのデバイスインベントリのみを再検出します。

Image Manager は、http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a0080b20f35.shtml で説明されているアップグレード手順に従います。イメージが両方のユニットにコピーされ、設定変更が実行されて、両方のユニットに同期されたイメージがアクティブ化されます。最初に、スタンバイがアクティブユニットを介してリロードされ、スタンバイが新しいバージョンに正常にアップグレードされたことが確認された後に、現在のアクティブがリロードされます。両方のユニットが新しいバージョンにアップグレードされると、フェールオーバーペアまたはクラスタのアップグレードは成功とマークされます。

（注） 現在のアクティブのリロード中は、スタンバイ ASA が引き継ぐまで、フェールオーバーペアを通過するトラフィックが影響を受けます。

フェールオーバー ASA ペアでのイメージアップグレードには制限があります。Image Manager を使用してフェールオーバー ASA ペアまたはクラスタでイメージアップグレードを実行するときは、次の制限が満たされていることの確認をお勧めします。

- フェールオーバー コンフィギュレーション内の 2 つの装置は、メジャー（最初の番号）およびマイナー（2 番目の番号）のソフトウェア バージョンが同じになるようにします。
- **メンテナンスリリース**：任意のメンテナンスリリースを、マイナーリリース内の他のメンテナンスリリースにアップグレードできます。たとえば、中間のメンテナンス リリースをあらかじめインストールしなくても、7.0（1）から 7.0（4）にアップグレードできます。
- **マイナーリリース**：マイナーリリースから次のマイナーリリースにアップグレードできます。**マイナー リリースはスキップできません。**たとえば、7.0 から 7.1 にアップグレードできます。ただし、ゼロダウンタイム アップグレードでは 7.0 から 7.2 への直接のアップグレードはサポートされておらず、まず 7.1 にアップグレードする必要があります。

- **メジャーリリース**：前のバージョンの最後のマイナーリリースから次のメジャーリリースにアップグレードできます。たとえば、7.9 が 7.x リリースの最後のマイナー バージョンであれば、7.9 から 8.0 にアップグレードできます。

Image Manager が ASA クラスタのイメージを更新する仕組み

イメージの更新では、ヒットレスアップグレードのために以前に確立された手順に従います。これにより、確実に、トラフィックフローに影響を与えることなく、クラスタのすべてのメンバーが 1 回のユーザー操作で新しいバージョンにアップグレードされます。イメージのアップグレード時には、次のような動作が実行されます。

- クラスタのデータユニットには、最初に、制御ユニットから新しいイメージがロードされます。制御ユニットのみに接続されている場合、イメージがクラスタのすべてのメンバーにコピーされます。クラスタを介したそのような伝播では、各デバイスのスイッチオーバーによってユニットのステータスを制御する必要がないため、トラフィックの中断が最小限に抑えられます。
- 新しいイメージをロードする起動コマンドを追加するために、制御ユニットで設定が変更されます。制御ユニットで設定が変更されると、すべてのデータユニットで自動的に同期されます。
- すべてのデータユニットが、制御ユニットを介して新しいイメージで順番に再起動します。
- すべてのデータユニットがオンラインになり、クラスタに再参加します。
- その後、制御ユニットがデータユニットになります（次のデータユニットが制御ユニットの役割を引き継ぎます）。
- 新しい制御ユニットを介して、古い制御ユニットに新しいイメージが再ロードされます。

Image Manager がこのイメージ更新手順に従うことで、スイッチオーバーが最小限になり、トラフィックの中断が最小限になります。

イメージ更新中および更新後のデバイス状態の変化

イメージのアップグレードは重要な操作であるため、すべてのイメージ更新操作が視覚的に表現され、ユーザーに通知される必要があります。そのため、次の 3 つの新しいデバイス状態が導入されました。

- [アップグレード中（Upgrade In Progress）]：デバイスでイメージインストールジョブが開始されるたびに、デバイスはこの状態になります。デバイスでイメージ更新操作が完了すると、この状態はシステムによって自動的にリセットされます。
- [メンテナンス（Maintenance）]：デバイスでイメージインストールジョブが失敗し、イメージインストール操作後にデバイスに到達できなくなると、デバイスはメンテナンス状態になります。アップグレードによって発生した問題を手動で修正するかイメージをロールバックすることによって、デバイスをオンラインに戻すために必要な手順を実行した後に、この状態を手動で正常/動作状態にリセットする必要があります。

- [設定が必要（Configuration Required）]：特定のケースのイメージアップグレード（ASA 8.2 から ASA 8.3 など）では、イメージアップグレードの一部としてデバイス設定が大幅に変更されるため、Security Manager のポリシー設定モデルがデバイス設定との互換性をなくします。このような場合は、イメージアップグレード操作が成功しても、アップグレード後に Security Manager の設定ポリシーモデルとデバイス設定が連携していることを確認するために、デバイスの再検出などのいくつかの操作を実行する必要があります。そのため、イメージのアップグレード後に、デバイスを動作させるために Configuration Manager で追加の設定が必要である場合、デバイスは [設定が必要（Configuration Required）] 状態になります。Image Manager を使用して VPN イメージが展開されている場合でも、ユーザーは Configuration Manager を使用して VPN ポリシーでこれらのイメージを設定する必要があるため、デバイスは [設定が必要（Configuration Required）] 状態になります。[設定が必要（Configuration Required）] 状態は、イメージ更新操作後にデバイスを Security Manager で機能させるために Configuration Manager で変更を行う必要があることを示しています。提示される変更を行うことができ、設定の変更に問題がないことを確認できたら、デバイスを手動で [動作（Operational）] 状態に戻すことができます。

（注） デバイスを [設定が必要（Configuration Required）] モードにできる他のシナリオについては、イメージ管理のトラブルシューティング （46 ページ）を参照してください。

デバイスの状態がこれらの 3 つの状態のいずれかに変化するたびに、その状態がデバイスセレクタに明示的なアイコンで示されます。このデバイス状態の変化は、Configuration Manager と Image Manager の両方で確認できます。デバイスでイメージ更新操作がないときのデバイスの正常な状態は [動作（Operational）] 状態です。

ヒント デバイスの状態を正常な状態（つまり、[動作（Operational）]状態）に手動でリセットするには、Configuration Manager または Image Manager のデバイスセレクタでデバイスを選択し、右クリックして、[デバイスを動作させる（Make Device Operational）] を選択します。

ここでは、次の内容について説明します。

- デバイスで提案されたイメージの更新を検証する （29 ページ）
- Image Installation ウィザードを使用してデバイスにイメージをインストールする （32 ページ）
- バンドルされたイメージをデバイスにインストールする （38 ページ）
- 互換性のあるイメージのデバイスへのインストール （38 ページ）
- 選択したデバイスにイメージをインストールする （39 ページ）

デバイスで提案されたイメージの更新を検証する

実際に実行する前に、1 つ以上のデバイスでイメージ更新ジョブを検証できます。次のリストは、実行されるさまざまな検証の詳細を示しています。

- ASA デバイスに選択したイメージを収容するための十分なディスクスペースがありません。

この場合、エラーが表示されます。そのデバイスの [ストレージ（Storage）] タブに移動し、1 つ以上のイメージを削除してスペースを確保する必要があります。次に、アップグレードの検証操作を再試行します。

（注） クラスタ内の各メンバー、およびフェールオーバー内のアクティブユニットとスタンバイユニットの両方のディスクスペースについて、選択されたイメージを収容するのに十分なスペースがあるかどうかが評価されます。1 つのメンバーまたはデバイスに十分なスペースがない場合、エラーが表示され、そのデバイスでのジョブの作成に進むことができません。その特定のメンバーの [ストレージ（Storage）] タブに移動し、1 つ以上の不要なイメージを削除してスペースを確保する必要があります。

- デバイスで新しいイメージを実行するのに十分な RAM がありません（Cisco ASA 5500 シリーズ 8.4(x) のリリースノートでの推奨による）。

（注） 新しいイメージをロードするのに十分な RAM がデバイスにない場合、Image Manager は警告を表示します。ただし、これによってイメージのアップグレードの実行が停止することはありません。これとは対照的に、設定展開では RAM が不足している場合に展開ジョブが停止します。

- イメージのインストール場所として選択されたフラッシュデバイス（disk0 または disk1）が、クラスタ/フェールオーバー セットアップのデバイス/メンバーのいずれにも存在しない場合、エラーが表示され、ジョブは中止されます。
- 送信されたがまだデバイスに展開されていない設定変更。これらの変更は、イメージ更新ジョブを開始する前に展開する必要があります。そうしないと、設定の変更とデバイス上のアップグレードされたイメージバージョンの互換性がなくなる可能性があります。
- 選択したイメージがデバイスタイプと互換性がない場合、たとえば、非 SMP イメージが ASA 5585 デバイスタイプに選択されている場合、警告を行います。

（注） この警告は、ドラッグアンドドロップ方法を使用している場合にのみ発生します。他のフローの場合、互換性のないイメージ/デバイスは、イメージ インストール ウィザードのステップ 2 で除外されます。

（注） Cisco Security Manager 4.3 では、MDF ID と互換性のある Cisco.com 上のイメージに関するメタデータ情報が利用できないことが原因で更新のチェックが実行されない場合、この検証はスキップされていました。Cisco Security Manager 4.4 では、メタデータ情報は Cisco Security Manager のインストールに事前にパッケージ化されているため、更新のチェックが実行されていない場合でも、イメージマネージャーはデバイスタイプのイメージの互換性を検証し、互換性のないイメージとデバイスの組み合わせが選択された場合は、ユーザーに警告します。

- デバイスが Security Manager でサポートされていないバージョンに更新されている場合、警告を行います。
- 新しいイメージバージョンがデバイスで実行されているバージョンと同じまたはそれより低い場合、警告を行います。
- 下位バージョンから ASA バージョン 8.3 へのイメージアップグレードでは、デバイスを Security Manager で再検出する必要があります。ASA バージョン 8.3 で導入された NAT 設定では、以前の ASA バージョンと互換性のない大きな変更が加えられています。同様に、バージョン 8.3 の Security Manager では、NAT ポリシーモデルが大きく変更されています。したがって、デバイスが ASA 8.3 にアップグレードされると、そのデバイスは設定が必要な状態になり、デバイスを動作させるには Configuration Manager でいくつかの変更を加える必要があることが、 Configuration ユーザーに示されます。Security Manager でデバイスを再検出した後、デバイスツリーでデバイスを右クリックし、[デバイスを動作させる（Make Device Operational）] を選択して、デバイスを通常の状態に戻すことができます。
- ASA バージョン 8.3.x から 8.4.2 以降のバージョンへのイメージアップグレードでも、ASA バージョン 8.4.2 の PAT 設定の変更に互換性がないため、Security Manager でデバイスを再検出する必要があります。この場合も、イメージのアップグレード後にデバイスの状態が設定が必要な状態に変更されます。
- ASA バージョン 8.x から 9.0.1 以降へのイメージアップグレードでは、ユニファイドアクセスルール、インスペクション、および NAT ルールの変更に互換性がないため、Security Manager でデバイスを再検出する必要があります。
- ASA バージョン 7.x から 8.x へのイメージアップグレードにより、デバイスと Security Manager の両方の SSLVPN 設定に大きな変更が導入されます。これらの変更に互換性がないため、イメージのアップグレード後にデバイスを Security Manager から削除してから、再度追加する必要があります。デバイスは設定が必要な状態になり、これらの警告に対処するようにユーザーに通知されます。
- Secure Client、CSD、または Hostscan イメージなどの VPN イメージが Image Manager を使用してロードされる場合、既存の VPN イメージが現在のデバイスまたは他のデバイスに割り当てられている共有ポリシーの一部であると、ユーザーに警告が発行されます。新しいイメージを共有ポリシーが割り当てられているすべてのデバイスにもコピーするよう警告が発行されます。そうすることで、ポリシー共有を失うことなく、すべてのデバイスに対して共有ポリシーをシームレスに更新できるようになります。

- フェールオーバーペアのスタンバイユニットに到達できない場合、警告を行います。これは、ジョブの中止を引き起こすエラーです。
- アクティブ/スタンバイ フェールオーバー ペアのアップグレードに関する警告。アップグレードされるバージョンは、ASA/PIX：CLIを使用してフェールオーバーペアのソフトウェアイメージをアップグレードする方法[英語]の推奨事項に準拠している必要があります。

（注） 同じ警告は、クラスタ設定の ASA にも当てはまります。

- アクティブ/アクティブ フェールオーバー ペアのアップグレードに関する警告。ペアがアクティブ/スタンバイに変換されない限り（つまり、1 つの物理ユニットですべてのフェールオーバーグループがアクティブである場合）、イメージ更新ジョブが中止されます。

（注） 指定された制御ユニットである「デバイス」には、追加の検証が必要です。アクティブ/スタンバイフェールオーバーの場合と同様のチェックに加えて、クラスタイメージがサポートされているプラットフォームと互換性があるかどうかもチェックします。クラスターを 9.x 未満のバージョンにダウングレードすることはできません。

イメージのインストールを検証するには、次の手順を実行します。

ステップ 1 [ファイル（File）] メニューの [検証（Validate）] を選択します。

[イメージ割り当ての検証（Validate Image Assignments）] ウィンドウが開きます。

ステップ 2 [ロール割り当ての追加（Add role assignment）] をクリックします。

[イメージの割り当て（Image Assignments）] ウィンドウが開きます。

ステップ 3 [イメージの割り当て（Image Assignments）] ウィンドウで、ドロップダウンリストから次のいずれかを選択します。

- イメージを選択してデバイスに割り当て（Select Images and Assign to Devices）
- デバイスを選択してイメージに割り当て（Select Devices and Assign to Images）

ヒント イメージをデバイスに割り当てても、デバイスをイメージに割り当てても、得られる結果は同じです。

ステップ 4 1 つ以上のアイテム（イメージまたはデバイス）を右側のウィンドウに移動して選択します。

ヒント [バンドル（Bundles）] をクリックしてバンドルを選択すると、イメージではなく事前定義されたバンドルを使用できます。

ステップ 5 [次へ（Next）] をクリックして、他の項目（イメージまたはデバイス）を割り当てます。

[割り当ての確認（Confirm Assignments）] ウィンドウが表示されます。

ステップ 6 指定した割り当てを確認し、確定します。

ヒント 必要に応じて、引き続き割り当てを追加または削除できます。

ステップ 7 [終了（Finish）] をクリックします。

[割り当ての検証（Validate Assignments）] ウィンドウが表示されます。

ステップ 8 [検証の開始（Start Validation）] をクリックします。

割り当ての検証ステータスは、[検証（Validation）] 列に表示されます。警告、成功、またはエラーのいずれかが表示されます。

ステップ 9 警告、成功、またはエラーの表示をクリックします。

ウィンドウの下側ペインが開きます。

ステップ 10 検証ステータスに従って、次のいずれかを実行します。

- エラー — エラーの考えられる原因を調べ、必要に応じて修正します。
- 警告 — 警告の潜在的な理由を調べ、必要に応じて修正します。
- 成功 — 対処不要です。

ヒント 右側のウィンドウスライダーバーを使用して、すべてのエラーまたは警告を表示して確認してください。

ステップ 11 表示された警告またはエラーに対処したら、[イメージのインストール（Image Install）] ウィザードを使用してジョブの作成に進むことができます。

ステップ 12 必要に応じて、[イメージ割り当ての検証（Validate Image Assignments）] ウィンドウで割り当て要素を右クリックし、続行する前に変更または削除できます。

ステップ 13 割り当てを右クリックして、[テーブルのコピー（Copy Table）] を選択することもできます。これにより、割り当ての詳細および検証ステータスとメモがコピーされます。その後、その内容をメモ帳などのプログラムに CSV ファイルとして貼り付けて、参照することができます。

Image Installation ウィザードを使用してデバイスにイメージをインストールする

この機能を使用して、デバイスにイメージを割り当ててインストールするジョブを作成できます。割り当ては、インストールジョブを定義するイメージとデバイスの単純な関連付けです。

（注） ワークフロー機能をイネーブルにしている場合は、インストールを完了する前に、説明されている追加の手順を実行して承認を取得する必要があります。

（注） 任意のデバイス セットを操作するように選択できます。

デバイスにイメージをインストールするジョブを作成するには、次の手順を実行します。

ステップ 1 [ファイル（Files）] > [イメージのインストールウィザードを開く（Open Image Installation Wizard）] に移動します。

イメージのインストール（Image Installation）ウィザードが表示されます。

ヒント イメージのインストール（Image Installation）ウィザードは、いくつかの方法で呼び出すことができます。ここで説明したメニューからのウィザードの呼び出しに加えて、次のいずれかを実行するときにウィザードを呼び出すことができます。（1）ドラッグアンドドロップによるイメージのインストール。（2）デバイスまたはバンドルを右クリックする。または（3）デバイスを選択し、[互換性のあるイメージ（Compatible Image）] タブに移動し、テーブルから 1 つ以上のイメージを選択して右クリックし、[インストール（Install）] オプションを選択する。

ステップ 2 左下の [割り当ての追加（Add Assignment）] をクリックします。

[イメージの割り当て（Image Assignments）] ダイアログボックスが表示されます。

ステップ 3 上部のドロップダウンリストから、イメージをデバイスに割り当てるか、デバイスにイメージを割り当てるかを選択します。

ステップ 4 項目（デバイスまたはイメージ）を左側のリストから右側の選択済みアイテムのリストに移動します。次に、[次へ（Next）] をクリックします。[バンドル（Bundles）] タブをクリックして、イメージの代わりにバンドルを選択することもできます。

ヒント 割り当てを定義するためにイメージとデバイスをペアリングする場合、イメージの後にデバイスを、またはデバイスの後にイメージを操作できます。この選択の順序は重要ではありません。

ステップ 5 [割り当ての確認（Confirm Assignments）] ダイアログボックスで割り当ての定義を確認し、[完了（Finish）] をクリックします。

ヒント この時点で、必要に応じて、[割り当ての追加（Add Assignment）] をクリックして、割り当てペアをさらに追加することもできます。

ステップ 6 割り当ての定義が終了したら、[検証の開始（Start Validation）] をクリックします。[検証の完了（Validation Complete）] が表示されるまで待ちます。

ステップ 7 [ウィザード（Wizard）] ダイアログボックスの [割り当て（Assignments）] タブにある [検証（Validation）] 列のステータスを調べます。警告、成功、またはエラーのいずれかが表示されます。

ステップ 8 ステータスに応じて必要な手順を決定します。

- エラー — エラーの考えられる原因を調べ、必要に応じて修正します。
- 警告 — 警告の潜在的な理由を調べ、必要に応じて修正します。

- 成功 — 対処不要です。

ステップ 9 その他のオプションについては、割り当てを右クリックします。

- [上に移動（Move Up）]/[下に移動（Move Down）]：デバイスが更新される順序を変更する場合は、複数デバイスのジョブに対してこれらのオプションを選択します。[イメージをデバイスにインストール（Install Images to Devices）] ジョブオプションが [逐次（Sequential）] に設定されている場合、この機能を使用して、デバイスの順序付けを行うことができます。
- [削除（Delete）]/[すべて削除（Delete All）]：これらのオプションを選択して、1 つまたはすべてのデバイスをイメージ アップグレード ジョブから削除します。
- [テーブルをコピー（Copy Table）]：これを使用して、警告メッセージをテキストエディタまたはスプレッドシートプログラムにコピーして参照します。
- [ファイルコピーのテスト（Test File copy）]：このオプションを使用して、https プロトコルを使用して Security Manager イメージリポジトリと ASA デバイスのフラッシュの間でファイルをコピーできるかどうかを確認します。

ヒント 右側のウィンドウスライダバーを使用して、すべてのエラーまたは警告を表示して確認してください。

ステップ 10 特定の時刻にインストール ジョブをスケジュールする場合は、[スケジュール（Schedule）] タブを選択し、日付と時刻を指定します。

ステップ 11 インストールジョブのプロパティを設定するには、[プロパティ（Properties）] タブを選択します。

a) 必要に応じて、[名前（Name）] を編集します（デフォルトは Image install Job—<timestamp>）。

b) 必要に応じて、[説明（Description）] を追加します。

c) 必要に応じて、[チケットID（Ticket ID）] を選択します。

ヒント リリース 4.4 以降、Image Manager の [チケットID（Ticket ID）] フィールドは Config Manager から切り離されました。現在は単なる「タグ」であり、任意の文字列にすることができます。[チケットID（Ticket ID）] フィールドは、Image Manager と Configuration Manager の両方で以前に作成されたチケットを表示するオートコンプリート機能付きの編集可能なコンボ ボックスです。また、[チケットID（Ticket ID）] フィールドについては、Configuration Manager のチケットモードに依存しません。[チケットID（Ticket ID）] はオプションのフィールドで、空白のままにすることができます。Configuration Manager のグローバル検索は、Image Manager で使用されるチケットもサポートし、チケットが関連付けられているイメージインストールジョブを一覧表示します。

d) [エラー時（On Error）] オプションを設定します（デフォルトは [インストールの停止（Stop Installation）]、代替は [操作の続行（Continue Operation）] です）。

e) [現在のイメージをバックアップ（Backup Current Image）] オプションを設定します（デフォルトは [はい（Yes）]、代替は [いいえ（No）] ）。

ヒント これは、システム ソフトウェア イメージにのみ適用されます。

f) [イメージをデバイスにインストールする方法（Install images to devices in）] オプションを設定します（デフォルトは [並列（Parallel）]、代替は [逐次（Sequential）]）。

g) 次の 3 つの操作のいずれかを選択します。

- イメージのインストールとデバイスの再起動
- イメージをインストールするが、デバイスを再起動しない
- イメージのデバイスへのコピーのみ
  - [非侵入型：フェールオーバーをトリガーしない（Non-Intrusive: Does not trigger failover）] チェックボックスをオンにして、フェールオーバー デバイスを切り替えずにイメージをコピーします。

h) ワークフローを使用している場合は、オプションで次の承認オプションを構成できます。

ヒント これらは、ジョブのジョブプロパティの上部フレームにあります。

- [アクション（Action）] :
- 承認（Approve）
- 拒否（Reject）
- [展開（Deploy）]
- 送信

ジョブを拒否すると、ステータスは [拒否（Rejected）] に設定され、その後ジョブは破棄されます。ジョブを破棄すると、ステータスは [破棄（Discarded）] として表示され、ジョブのすべてのアクションボタンが無効になります。

ジョブを承認すると、ステータスは [承認済み（Approved）] に設定されます。次に、[展開（Deploy）] をクリックして、イメージ アップグレード ジョブを開始する必要があります。

i) バージョン 4.12 以降、Security Manager には、ソフトウェアバージョン 9.6(2) 以降を実行している ASA マルチコンテキストデバイスのストレージ URL を選択するオプションが用意されています。選択したユーザコンテキストに対して、共有またはプライベートの ストレージ URL を選択できます。デフォルトでは、[共有（Shared）] が選択されています。

ヒント [詳細（Details）]タ ブを選択して [進行状況を表示（Show Progress）] をクリックすると、実行中の状況を確認できます。

ジョブを展開すると、ジョブのステータスが [展開済み（Deployed）] または [失敗（Failed）] として表示されます。下部ペインの [履歴（History）] タブ（選択したジョブの情報）のみが WF モードでアクティブ化され、次の 2 つのジョブアクションフローのいずれかが表示されます。

- 作成/編集中/送信済み/却下済み/破棄済み
- 作成/編集中/送信済み/承認済み/展開中/展開済み（または失敗）
- [ジョブを送信（Submit the job）] : これはデフォルトでオンになっています

- [承認者の電子メール（Approver email）]：承認者の電子メールアドレスリスト
- [送信元の電子メール（Submitter email）]：ジョブを送信する担当者の電子メールアドレス。

j) [編集（Edit）] をクリックして、ジョブのプロパティを変更できます。

k) その他のジョブ表示オプションについては、インストールジョブの表示 （42 ページ）を参照してください。

ステップ 12 [Install（インストール）] をクリックします。

[ジョブ（Jobs）] ページが表示され、インストールジョブのステータスが [展開中（Deploying）] として表示されます。

（注） ジョブのスケジュールが選択されている場合、ジョブの状態は[スケジュール済み（Scheduled）] と表示されます。ジョブはスケジュールされた時刻に展開を開始し、その時点でジョブの状態が [展開中（Deploying）] に変わります。

（注） イメージインストールジョブに対してワークフローがイネーブルになっている場合、ジョブの状態は [送信済み（Submitted）] または [編集中（Edit-in-Use）] のいずれかに変更されます。このモードでは、承認された後にのみジョブを展開できます。ワークフローモードでのジョブの状態については、イメージインストールジョブの承認ワークフロー （44 ページ）を参照してください。

ヒント [中断（Abort）] をクリックすると、ジョブを中断できます。インストールジョブの中断に関する重要な情報については、イメージインストールジョブの中止 （43 ページ）を参照してください。[破棄（Discard）] をクリックすると、スケジュールされた実行時間の前にジョブを破棄できます。

ステップ 13 ジョブの展開が開始されると、Configuration Manager および Image Manager のデバイスツリーで、デバイスの状態が [更新処理中（Update in progress）] 状態に変化することに注意してください。デバイスツリーのデバイスの横に、緑色の進行状況アイコンが表示されます。

ステップ 14 ジョブが展開中の状態の間、ジョブの詳細と進行状況を表示します。詳細については、インストールジョブの表示 （42 ページ）を参照してください。

ステップ 15 ジョブが完了するまで待ちます。

すべてのデバイスが正常に更新されると、ジョブの状態が [展開済み（Deployed）] に変わります。ジョブの 1 つ以上のデバイスが失敗した場合、ジョブの状態は [失敗（Failed）] に変更されます。

ステップ 16 ジョブが完了した後、デバイスツリー内のデバイスの状態の変化に注目してください。

イメージの更新が成功し、Configuration Manager でそれ以上の構成変更が必要ない場合、デバイスは [動作中（Operational）] 状態に戻ります。更新後にデバイスで構成の変更が必要な場合、デバイスは [構成が必要（Configuration Required）] 状態に移行します。デバイスツリーでデバイスをクリックすると、状態の詳細とデバイスの状態を [動作中（Operational）] に戻すために実行する必要があるアクションを含むバルーンヒントが表示されます。デバイスでイメージの更新が失敗し、イメージの更新中にデバイスが到達不能状態になった場合、デバイスは [メンテナンス（Maintenance）] 状態になります。

ステップ 17 イメージの更新を検証します。

a) Image Manager のデバイスツリーでデバイスをクリックします。

b) [概要（Summary）] タブに移動して、更新された実行中の OS バージョンを表示します。
c) [実行中のイメージ（Running Images）] タブに移動して、イメージ更新後の新しい実行中のイメージを表示します。
d) Configuration Manager でデバイスを選択します。
e) デバイスを右クリックして、[デバイスのプロパティ（Device Properties）] を選択します。
f) [実行中のOSバージョン（Running OS Version）] フィールドで、更新された新しいイメージバージョンを確認します。
g) [Configuration Manager] > [管理（Manage）] > [構成アーカイブ（Configuration Archive）] に移動します。
h) デバイス CLI から、**sh ver** と入力します。

   更新された OS バージョンが表示されます。

i) 左側のデバイスツリーでデバイスを選択します。
j) 右側のペインで構成アーカイブのバージョンを表示し、アーカイブソースが Image Manager である最新のエントリを確認します。
k) アーカイブされたエントリを選択し、[View（表示）] をクリックします。
l) このエントリを以前のアーカイブバージョンと比較して、イメージの更新中に Image Manager によって行われた構成の変更を表示します。新しい ASA システム ソフトウェア イメージの先頭に追加されているブートコマンドや、新しい ASDM イメージに追加されている ASDM イメージコマンドを表示できます。
m) Image Manager の管理設定で電子メール通知が設定されている場合、イメージアップグレードジョブのステータスが含まれた電子メール通知が、設定された受信者に送信されます。

ステップ 18 イメージの更新操作後にデバイスが [構成が必要（Configuration Required）] または [メンテナンス（Maintenance）] の状態に設定されている場合は、次の手順に従って Configuration Manager でイメージ更新後に必要な操作を完了して、デバイスが機能するようにします。

a) Configuration Manager または Image Manager のデバイスツリーでデバイスをクリックします。

   デバイス情報を示すバルーンヒントが表示されます。

b) バルーンヒントの内容を確認します。デバイスが [構成が必要（Configuration Required）] または [メンテナンス（Maintenance）] 状態に設定されている理由を確認します。推奨される措置も確認します。
c) 推奨される処置を実行します。
d) デバイスツリーでデバイスを右クリックし、[デバイスを動作状態にする（Make Device(s) Operational）] を選択します。

   デバイスは [動作中（Operational）] 状態に移行し、デバイスツリーのデバイスの横にあるアイコンが削除されます。

   （注） アプライアンスモードで動作している Cisco Firepower 1000 および 2000 シリーズ デバイスのインストールジョブを開始する前に、[プロパティ（Properties）] パネルの [現在のイメージをバックアップ（Backup Current Image）] フィールドで [いいえ（No）] オプションを選択する必要があります。

バンドルされたイメージをデバイスにインストールする

Image Manager ツールを使用して、バンドルとしてグループ化された互換性のあるイメージを割り当ててインストールできます。バンドルによって、反復操作が簡素化されるとともに、デバイスのグループでの一貫したアクションの実行を可能にします。

デバイスまたはデバイスグループにイメージバンドルを選択的にインストールするには、次の手順を実行します。

ステップ 1 バンドルをデバイスまたはデバイスグループにドラッグアンドドロップします。

[デバイスにイメージをインストール（Install images on devices）] ダイアログボックスが表示され、バンドル内のデバイスとイメージが事前に割り当てられます。バンドルをデバイスグループにドロップすると、グループ内のすべてのデバイスが自動的に選択され、バンドル内のイメージに割り当てられます。

ステップ 2 [デバイスにイメージをインストール（Install images on devices）] ダイアログボックスに表示されている割り当て検証エラーまたは警告を調査します。

ヒント ジョブをスケジュールし、ジョブのデフォルトプロパティを変更することもできます。ジョブのスケジュール設定とジョブプロパティの設定の詳細については、Image Installation ウィザードを使用してデバイスにイメージをインストールする （32 ページ）を参照してください。

ステップ 3 警告が修正されたら（または警告が重要ではないと判断したら）、[インストール（Install）] をクリックします。

（注） または、バンドルを右クリックして [インストール（Install）] を選択し、バンドルが事前に選択された状態でイメージインストール ウィザードを起動することもできます。次に、デバイスを選択し、[インストール（Install）] をクリックして、選択したデバイスにバンドルをインストールします。

互換性のあるイメージのデバイスへのインストール

Image Manager を使用して、互換性のあるイメージをデバイスにインストールできます。

デバイスまたはデバイスグループに 1 つ以上の互換性のあるイメージを選択的にインストールするには、次の手順を実行します。

ステップ 1 セレクタの [デバイス（Devices）] 領域でデバイスを選択し、[互換性のあるイメージ（Compatible Images）] タブに移動します。

ステップ 2 [互換性のあるイメージ（Compatible Images）] タブで、 リポジトリイメージを 1 つ以上選択します。

ステップ 3 選択したイメージを右クリックして、[インストール（Install）] をクリックします。

イメージのインストール（Image Installation）ウィザードが表示されます。選択したイメージが事前に割り当てられているか、[イメージの選択（Select Image）] ページの右側のペインに移動されています。

ステップ 4 [次へ（Next）] をクリックします。

ウィザードの [デバイスの選択（Select Devices）] ページが表示されます。

ステップ 5 インストール先のデバイスを選択し、[次へ（Next）] をクリックします。

ウィザードの [割り当ての確認（Confirm Assignments）] ページが表示されます。

ステップ 6 デバイスとイメージの割り当てを確認し、[完了（Finish）] をクリックします。

[選択したデバイスにイメージをインストール（Install images on selected devices）] ダイアログボックスが表示されます。デバイスとイメージが割り当てられています。

ステップ 7 [割り当て（Assignments）] タブの右上隅にある [検証の開始（Start Validation）] をクリックします。[デバイスにイメージをインストール（Install images on devices ）] ダイアログボックスに表示されている割り当て検証エラーまたは警告を調査します。

バージョン 4.9 以降の Security Manager には、デバイスにイメージをインストールするための拡張された検証手順があります。

- Image Manager を使用して CCO からイメージをダウンロードした場合は、イメージをデバイスにインストールする前に、デバイスのシリアル番号がサービス契約に対して検証されます。デバイスに有効なサービス契約がある場合、イメージのインストールまたはアップグレードプロセスが続行されます。デバイスに有効なサービス契約がない場合、イメージのインストールまたはアップグレードプロセスは続行されません。
- ローカルファイルシステムから Image Manager にイメージをコピーした場合、サービス契約の検証はデバイスに対して実行されず、デバイスへのイメージのインストールに進むことができます。

ヒント ジョブをスケジュールし、ジョブのデフォルトプロパティを変更することもできます。ジョブのスケジュール設定とジョブプロパティの設定の詳細については、Image Installation ウィザードを使用してデバイスにイメージをインストールする （32 ページ）を参照してください。

ステップ 8 警告が修正されたら（または警告が重要ではないと判断したら）、[インストール（Install）] をクリックします。

イメージのインストールジョブが作成されます。ジョブの進行状況を監視し、イメージの更新を確認するための残りの手順については、Image Installation ウィザードを使用してデバイスにイメージをインストールする （32 ページ）を参照してください。

（注） または、デバイスまたはデバイスグループに 1 つ以上のイメージをインストールするには、リポジトリビューから複数のイメージをドラッグし、デバイスまたはデバイスグループにドロップします。次に、[インストール（Install）] をクリックして、選択したイメージを選択したデバイスにインストールします。

選択したデバイスにイメージをインストールする

Image Manager を使用して、選択した一連のデバイスのイメージをアップグレードできます。

選択した一連のデバイスにイメージをインストールするには、次の手順を実行します。

ステップ 1 セレクタの [デバイス（Devices）] 領域でデバイスグループを選択します。

ステップ 2 右側のペインにグループ内のデバイスのリストを表示します。

ステップ 3 リストから 1 つ以上のデバイスを選択します。

ヒント 複数のデバイスを選択するには、Shift キーと Ctrl キーを使用します。

ステップ 4 選択したデバイスを右クリックして、[インストール（Install）] をクリックします。

Image Installation ウィザードが表示されます。選択したデバイスが事前に割り当てられているか、[デバイスの選択（Select Devices）] ページの右側のペインに移動されています。

ステップ 5 [次へ（Next）] をクリックします。

ウィザードの [イメージの選択（Select Images）] ページが表示されます。

ステップ 6 インストールするイメージを選択し、[次へ（Next）] をクリックします。

ヒント [バンドル（Bundles）] タブでバンドルを選択することもできます。

ウィザードの [割り当ての確認（Confirm Assignments）] ページが表示されます。

ステップ 7 デバイスとイメージの割り当てを確認し、[完了（Finish）] をクリックします。

[選択したデバイスにイメージをインストール（Install Images on selected devices）] ダイアログボックスが表示されます。デバイスとイメージが割り当てられています。

ステップ 8 [割り当て（Assignments）] タブの右上隅にある [検証の開始（Start Validation）] をクリックします。[デバイスにイメージをインストール（Install images on devices）] ダイアログボックスに表示されている割り当て検証エラーまたは警告を調査します。

ヒント ジョブをスケジュールし、ジョブのデフォルトプロパティを変更することもできます。ジョブのスケジュール設定とジョブプロパティの設定の詳細については、Image Installation ウィザードを使用してデバイスにイメージをインストールする （32 ページ）を参照してください。

ステップ 9 警告が修正されたら（または警告が重要ではないと判断したら）、[インストール（Install）] をクリックします。

イメージのインストールジョブが作成されます。ジョブの進行状況を監視し、イメージの更新を確認するための残りの手順については、Image Installation ウィザードを使用してデバイスにイメージをインストールする （32 ページ）を参照してください。

ジョブの操作

このセクションでは、イメージのインストールジョブの実行を支援する一連の機能について詳しく説明します。イメージのインストールジョブは、すぐに実行することも、指定した日時に

実行するようにスケジュールすることもできます。Image Manager のジョブは時間がかかる傾向があるため、ジョブ管理機能を使用すると、これらの操作をバックグラウンドで実行できます。Image Manager には、一意のチケット ID を使用してジョブを簡単に検索できるオプションのチケットシステムが組み込まれています。

特定のジョブの詳細は、実行前に定義および検証されることを理解しておく必要があります。

ここでは、次の内容について説明します。

- イメージインストールジョブの概要の表示 （41 ページ）
- インストールジョブの表示 （42 ページ）
- イメージインストールジョブの中止 （43 ページ）
- 失敗したイメージインストールジョブの再試行 （43 ページ）
- 展開されたジョブをロールバックする （44 ページ）
- イメージインストールジョブの承認ワークフロー （44 ページ）

イメージインストールジョブの概要の表示

Image Manager ツールを使用して、イメージのインストールおよび展開ジョブを監視できます。Image Manager が実行したジョブの履歴とステータス、および特定のジョブの概要、詳細、または履歴を表示できます。

（注） ジョブの状態変更の包括的な詳細は、Configuration Manager で確認できます（Workflow 以外のモードでのジョブの状態またはWorkflow モードでのジョブの状態を参照）。監査レポートの場合は、[Configuration Manager] > [管理（Manage）] > [監査レポート（Audit Report）] に移動します。

イメージインストールジョブの概要を表示するには、次の手順を実行します。

ステップ 1 セレクタの [ジョブ（Jobs）] で、[ジョブのインストール（Install Jobs）] をクリックします。

メイン ウィンドウの上部ペインに [ジョブ（Jobs）] リストが表示されます。

ステップ 2 [ジョブ（Jobs）] リストの詳細を調べます。次の項目が含まれる可能性があります。

- [名前（Name）]：ジョブの名前。デフォルトでは、名前にタイムスタンプが含まれています。
- [最後のアクション（Last Action）]：最後のアクションの日付。
- [ステータス（Status）]：ジョブのステータス（展開済み、失敗、または進行中）。
- [変更者（Changed By）]：ジョブを開始したユーザー。
- [説明（Description）]：ジョブの説明。

- [スケジュール（Schedule）]：ジョブスケジュール。
- [チケットID（Ticket ID(s)）]：チケットは、変更を追跡するために Image Manager ジョブに添付されるタグです。チケットは、Configuration Manager で作成されたチケットである可能性もあります。

ステップ 3 必要に応じて、1 つのジョブを見つけて選択し、そのジョブに関する詳細情報を下部のペインに表示できます。次の機能が含まれています。

- [概要（Overview）]
- 詳細（Details）
- 履歴（History）

ヒント 下部のペインにある [詳細（Details）] タブを表示しているときに、デバイスを選択し、右下部のペインでジョブのログを表示できます。

（注） それらはドッキング可能なウィンドウです。デフォルトのビューはカスタマイズできます。

インストールジョブの表示

特定のイメージ管理ジョブに関連付けられた詳細を表示できます。

ジョブに関連付けられた詳細を表示するには、次の手順を実行します。

ステップ 1 セレクタの [ジョブ（Jobs）] で、[ジョブのインストール（Install Jobs）] をクリックします。

ヒント ジョブセレクタの [ステータス（Status）] 列には、ジョブのステータス（[送信済み（Submitted）]、[承認済み（Approved）]、[展開済み（Deployed）]、[進行中（In Progress）]、または [失敗（Failed）]）が表示されます。

メイン ウィンドウの上部ペインに [ジョブ（Jobs）] リストが表示されます。

ステップ 2 調べるジョブを選択します。

ヒント 特定のジョブを見つける場合、[名前（Name）]、[最後のアクション（時系列）（Last Action (chronology)）]、[ステータス（Status）]（[展開済み（Deployed）]、[失敗（Failed）] など）、[説明（Description）] など、いずれかの列見出しで [ジョブ（Jobs）] リストをソートできます。検索ウィンドウを使用してフィルタリング文字列を入力し、特定のジョブを検索することもできます。

（注） ジョブフォルダの場所は、CSM-ROOT\files\vms\jobs ディレクトリです。

ステップ 3 下部のペインで [概要（Summary）] をクリックして、ジョブの概要情報を調べます。

下部のペインには、[イメージ管理ジョブ名（Image Management Job Name）]、[展開されるデバイス（Devices to be Deployed）]、[正常に展開されたデバイス（Devices Deployed Successfully）]、[展開時にエラーが発生したデバイス（Devices Deployed with Errors）] など、ジョブの概要情報が表示されます。

ステップ 4 下部のペインで [詳細（Details）] をクリックして、ジョブの概要の詳細を調べます。

デバイスの詳細、新しいイメージ、古いイメージ、およびデバイスステータスが表示されます。

ステップ 5 右端にある縦の [注釈（Commentary）] タブをクリックして、ジョブのデバイスに関する注釈を調べます。注釈には、デバイスでのイメージインストール操作の進行状況が示されます。

ステップ 6 右端にある縦の [トランスクリプト（Transcript）] タブをクリックして、ジョブ内のデバイスのトランスクリプトを調べます。トランスクリプトには、デバイスで実行されたコマンドとその応答が時系列で示されます。

ステップ 7 下部のペインで [履歴（History）] をクリックして、ジョブ履歴の詳細を調べます。ジョブの状態遷移の履歴が示されます。

（注） この情報は、Workflow モードでのみ表示されます。

イメージインストールジョブの中止

[ジョブ（Jobs）] ページで [中止（Abort）] をクリックすると、イメージインストールジョブを中止できます。このオプションは、マルチデバイスジョブに対してのみ有効です。

（注） ジョブに 1 つのデバイスが含まれる場合、ジョブの開始後に停止しても効果がなく、ジョブは必ず完了するまで実行されます。

- [順次（Sequential）] オプションが選択されている場合、ジョブがまだ開始されていないすべてのデバイスが中止されます。
- [並列（Parallel）] が選択されている場合、そのバッチまでのすべてのデバイスでイメージのアップグレードが行われます。次のバッチ以降のすべてのデバイスは中止されます。

失敗したイメージインストールジョブの再試行

1 つ以上のデバイスにイメージを展開しようとして失敗した場合は、ジョブを再試行できます。ただし、失敗したステップから単純に続行しようとしないでください。ジョブ全体を再試行する必要があります。

失敗したジョブを再試行するには、次の手順を実行します。

ステップ 1 インストールジョブが失敗したことを確認するには、セレクタの [ジョブ（Jobs）] セクションに移動し、[インストールジョブ（Install Jobs）] をクリックします。

[ジョブ（Jobs）] ページが表示されます。

ステップ 2 [ステータス（Status）] 列を調べて、問題のジョブのステータスを判断します。

ヒント 緑色のチェックアイコンに [展開済み（Deployed）] という単語が付いている場合、成功を示します。赤い X アイコンは失敗を示します。

ステップ 3 ジョブが失敗した考えられる原因を調査します。

ステップ 4 ジョブリストから失敗したイメージインストールジョブを選択し、上部ペインのツールバーから [再試行（Retry）] をクリックします。

[デバイス（Devices）] ウィンドウにインストールイメージが表示されます。通常のインストールジョブの場合と同様に、検証警告を確認できます。

ステップ 5 必要に応じて、使用するイメージ、デバイス、スケジュール、またはジョブのプロパティを変更できます。

ステップ 6 [デバイスにイメージをインストール（Install Images on Devices）] ウィンドウで、[インストール（Install）] をクリックします。

ステップ 7 新しく作成されたジョブを観察して、再試行が成功したことを確認します。

展開されたジョブをロールバックする

展開されたイメージインストールジョブから変更をロールバックできます。

展開されたジョブをロールバックするには、次の手順を実行します。

ステップ 1 ジョブリストから、ロールバックするイメージインストールジョブを選択し、上部ペインのツールバーから [ロールバック（Rollback）] をクリックします。

[デバイス（Devices）] ウィンドウにインストールイメージが表示されます。通常のインストールジョブの場合と同様に、検証警告を確認できます。

ステップ 2 必要に応じて、ロールバックで使用するイメージ、デバイス、スケジュール、またはジョブのプロパティを変更できます。

ステップ 3 [デバイスにイメージをインストール（ Install Images on Devices）] ウィンドウで、[インストール（Install ）] をクリックします。

ステップ 4 新しく作成されたジョブをモニタリングして、ロールバックの試行が成功したことを確認します。

イメージインストールジョブの承認ワークフロー

イメージの更新は、デバイスやネットワークのダウンタイムを引き起こす可能性のある重要な操作です。そのため、イメージインストール操作の変更制御と管理は非常に重要です。イメージインストールジョブの変更管理は、Configuration Manager の展開ワークフローフレームワー

クを使用して行われます。これにより、すべてのイメージインストールジョブについて、実行または展開前の承認の必要性が確保されます。

イメージインストールジョブでワークフローを使用するには、次の手順を実行します。

ステップ 1 イメージインストールジョブのワークフローを有効にします。

a) Configuration Manager で、[ツール（Tools）] > [Security Manager の管理（Security Manager Administration）] > [ワークフロー（Workflow）] を選択します。

b) ワークフローがまだ有効になっていない場合は、[ワークフローの有効化（Enable Workflow）] を選択します。

c) [イメージの展開およびインストールに承認が必要（Require Deployment & Install Image Approval）] を選択します。

d) [ジョブ/スケジュール承認者（Job/Schedule Approver）] フィールドで、イメージインストールジョブを承認する担当者の電子メールアドレスを設定します。詳細については、[Workflow] ページを参照してください。

e) [保存（Save）] をクリックし、[閉じる（Close）] をクリックします。

f) Image Manager を起動し、[ジョブのインストール（Install Jobs）] に移動します。メニューバーで、ワークフローモードにおいてジョブの状態を変更するための新しいボタン（[送信（Submit）]、[承認（Approve）]、[拒否（Reject）]、[展開（Deploy）]）が使用可能になります。

ステップ 2 ワークフローを有効にしてイメージインストールジョブを作成して実行するには、次の手順を実行します。

a) 以前に説明した手順のいずれかを使用して、イメージインストールジョブを作成します。Image Manager を使用したデバイスでのイメージの更新について （25 ページ）を参照してください。

（注） [プロパティ（Properties）] タブには、ジョブを送信するための追加のオプションがあります。ジョブの作成後に承認のためにジョブを自動送信するには、このオプションをオンにします。

b) イメージインストールジョブを作成したら、イメージインストール ジョブ ビューでジョブの状態を確認します。

c) ジョブの作成時に自動送信オプションが選択されていない場合は、ジョブを選択し、[送信（Submit）] をクリックして承認のためにジョブを送信します。

ジョブ承認者（承認者のロール/権限を持つユーザー）は、ジョブを承認するための電子メール通知を受信します。

d) 承認者は、Security Manager にログインし、Image Manager を起動して、ジョブに移動できます。

e) 承認者は、アップグレードの詳細（アップグレードに使用されるイメージ、ジョブのプロパティ、スケジュールなど）を確認した後、[承認（Approve）] をクリックしてジョブを承認します。

ジョブの状態が [承認済み（Approved）] に変更されます。ジョブの作成者は、ジョブが承認されたことを通知する電子メールを受信します。これでジョブを展開できます。

f) 承認者がジョブの詳細を確認し、納得できない場合は、[拒否（Reject）] をクリックしてジョブを拒否できます。

ジョブの状態が [拒否（Rejected）] に変更されます。ジョブの作成者は、ジョブが拒否されたことを通知する電子メールを受信します。拒否されたジョブは展開されません。

（注） 拒否されたジョブは展開されません。編集して承認のために再送信することができます。または、破棄します。

g) ジョブが承認されたら、[展開（Deploy）] をクリックしてジョブを展開できます。

ジョブの状態が [展開中（Deploying）] に変更され、イメージインストールジョブの実行が開始されます。

h) ジョブが拒否された場合またはジョブに追加の変更を加える必要がある場合は、[編集（Edit）] をクリックしてジョブを編集できます。

ウィザードの [イメージの割り当て（Image Assignments）] ページが表示され、すべてのデバイスおよびイメージが示されます。ユーザーは、ジョブのプロパティを変更したり、イメージへのデバイスの割り当てをスケジュール（場合によっては削除）したり、[送信（Submit）] をクリックして承認のためにジョブを再送信することができます。

i) ジョブの実行が開始されていない場合、ユーザーは、[破棄（Discard）] をクリックしてジョブを破棄できます。

ジョブの状態が [破棄（Discarded）] に変更されます。破棄されたジョブは実行されず、編集したり他の状態に変更することもできません。

j) 承認者は、変更されたジョブが受け入れ可能である場合、そのジョブを承認できます。前述のように、このジョブは展開できます。

k) ジョブの展開が完了すると、イメージのインストールが成功した場合は状態が [展開済み（Deployed）] に変更され、イメージのインストールが失敗した場合は状態が [失敗（Failed）] に変更されます。

イメージ管理のトラブルシューティング

このセクションでは、特定の症状に応じてイメージ管理をトラブルシューティングするために実行できる手順について説明します。

設定されている再起動時間が原因で、イメージインストールジョブに失敗したと表示される場合があります。

クラスタデバイスとフェールオーバーデバイスの場合、スタンバイデバイスとプライマリデバイスの間の再起動時間は、デフォルトで 15 分に設定されています。デバイスの構成が大規模な場合、設定されている再起動時間が原因で、イメージインストールジョブに失敗したと表示されることがあります。設定の完了後、デバイスはイメージを使用して更新されます。ところが、再起動時間の不一致により、Security Manager はジョブを失敗として表示します。

再起動時間を変更するには、次の手順を実行します。

プライマリデバイスまたはクラスタデバイスの ##MAX_RELOAD_WAIT_TIME

#デフォルトの時間は 15 分（15*60*1000）

reloadTime = 900000

Security Manager のアップグレード後、Image Manager にはデバイスのデータが存在しません。デバイスに対して最初に実行される次の操作のいずれかによって、デバイスのイメージインベントリが収集されます。

- デバイスインベントリのみを検出することを選択してデバイスを再検出します。
- デバイスへのライブ展開を実行します。
- デバイスへのイメージインストール操作を実行する

Cisco.com からのイメージのダウンロードに失敗する

- [Configuration Manager] > [ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] に移動します。
- [Image Manager] を選択します。
- [接続のテスト（Test Connection）] をクリックして、サーバーに到達できることを確認します。
- [%NMSROOT%/MDC/athena/config/****-CCOMetaData.xml] で、特定の MDF ID のメタデータ情報をダウンロードした際のエラーを確認してください。

証明書の不一致、使用不能であること、有効期限、またはその他の原因により、更新またはイメージのダウンロードが失敗します。

- エラーメッセージに示されている推奨アクションを実行します。エラーメッセージで、ダウンロードに失敗した URL を使用して証明書を取得します。
- [%NMSROOT%/MDC/certificates/*.ser] に保存されている証明書を表示します（シリアル化されたオブジェクトやファイルの内容は判読不能であり、どのエディタでも表示できません）。

Cisco.com からのイメージのダウンロード時に次のメッセージが表示されて失敗する：「ユーザーにはファイルをダウンロードする権限がありません（User not authorized to download file）」

- [Configuration Manager] > [ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] に移動します。
- [Image Manager] を選択します。
- [接続のテスト（Test Connection）] をクリックして、サーバーに到達できることを確認します。
- Cisco Encryption Software Usage Handling and Distribution Policy への同意を登録してください。

ヒント　このポリシーは、http://tools.cisco.com/legal/k9/controller/do/k9Check.x?eind=Y で閲覧できます。

Cisco.com からのイメージのダウンロードが遅い

- プロキシが設定されていることを確認します。
- Security Manger から Cisco.com へのルートをトレースします。

更新の確認に失敗する

Security Manager の管理設定ページに移動し、Cisco.com への接続をテストします。[%NMSROOT%/MDC/athena/config/****-CCOMetaData.xml] で、特定の MDF ID のメタデータ情報をダウンロードした際のエラーを確認してください。

メッセージ：「ユーザーにはファイルをダウンロードする権限がありません（User not authorized to download file）」Security Manager の管理設定ページに移動し、Cisco.com への接続をテストします。http://tools.cisco.com/legal/k9/controller/do/k9Check.x?eind=Y で、暗号化についての合意事項を承認してください。

外部ファイルシステムまたはネットワークファイル共有からのイメージのダウンロードが失敗する

- 外部ファイルシステムまたはファイル共有への適切なアクセス権限/ログイン情報があることを確認します。
- クライアントでファイル共有を開き、イメージをドラッグして Image Manager にドロップします。

Image Install ウィザードに互換性のあるイメージが表示されない

- Image Manager は、Cisco.com の情報を使用して MDF ID のイメージの互換性を判断します。[更新の確認（Check for Updates）] を実行して、Cisco.com で入手可能な最新のイメージをダウンロードしてください。イメージが Cisco.com で入手可能で、プラットフォームとの互換性があると表示されている場合は、デバイスの該当するイメージが Image Install ウィザードおよびデバイスの [互換性のあるイメージ（Compatible Images）] タブに表示されるようになりました。
- デバイスの [互換性のあるイメージ（Compatible Images）] タブに、デバイスと実際に互換性のある一部のイメージが表示されないこともあります。
- Cisco.com に接続していないか、Cisco.com で該当するプラットフォーム向けにイメージが更新されていないため、依然として Install ウィザードにイメージが表示されない場合は、デバイス上でドラッグアンドドロップを使用してイメージをインストールできます。イメージに互換性がないという警告が表示される可能性がありますが、操作を続行し、イメージをデバイスにドラッグアンドドロップしてジョブを作成することで、イメージをインストールできます。

イメージコピーの失敗：「HTTP 413 エラー（HTTP 413 Error）」

- [Image Manager] > [テストファイルをデバイスにコピー（Test File Copy To Device）] で [デバイス（Device）] を右クリックします。

- vmssharedsvcs.log のエラーメッセージを確認します。
- HTTP 413 エラーが発生した場合は、ジョブを分割して、1 つのジョブに含まれるイメージの数を減らします

イメージコピーの失敗：「ディスクに十分な容量がありません（Not enough space on disk）」

- [デバイス（Device）] > [ストレージビュー（Storage View）] をチェックして、デバイス上のファイルと、イメージのインストール場所の空き容量を確認します。
- [デバイス（Device）] > [ストレージビュー（Storage View）] にファイルが表示されている場合は、ストレージからファイルを削除して容量を確保し、再試行します。
- ファイルが新規のデバイスであるか、Security Manager アップグレードセットアップであるために、[デバイス（Device）] > [ストレージビュー（Storage View）] にファイルが表示されない場合は、デバイス上のデバイスインベントリのみを再検出し、その後 [ストレージビュー（Storage View）] からファイルを削除して容量を確保します。

イメージインストールジョブの失敗：エラー：「フラッシュデバイスが無効です（Invalid flash device）」

- デバイスにフラッシュが存在するかどうかを確認します。
  - [IM] > [テストファイルをデバイスにコピー（Test File Copy To Device）] でデバイスを右クリックします。
  - デバイスに接続し、それが Security Manager でシングル コンテキスト デバイスとして管理されているマルチコンテキスト デバイスかどうかを確認します。
  - [システムコンテキスト（System Context）] の検出を選択しているデバイスを再検出します。その後、イメージインストールジョブを再試行します。

アクティブ/スタンバイペアのイメージ アップグレード ジョブが失敗する

- エラー：「このホストはフェールオーバーペアの「アクティブ」デバイスではありません（This host is not the 'active' device in the failover pair）」。フェールオーバーペアが、スタンバイデバイスの IP アドレスではなく、フェールオーバーペアのアクティブデバイスの IP アドレスを使用して Security Manager で管理されていることを確認します。
- エラー：「セカンダリデバイスがスタンバイ準備完了状態になっていません（Secondary device is not in standby-ready state）」。フェールオーバーペアのデバイスが稼働しており、スタンバイデバイスがスタンバイ準備完了状態になっていることを確認します。スタンバイデバイスに障害が発生している場合、ジョブは中止されます。

イメージインストールジョブの失敗：エラー：「SWIM1114：アップグレード後にデバイスに到達できませんでした（SWIM1114: Device could not be reached after upgrade）」

- デバイスに到達可能かどうかを手動で確認します。解決策：イメージのアップグレード後、デバイスを Security Manager に再度追加するか、管理オプションを [証明書の認証を確認しない（Do not check certificate authentication）] に変更する必要があります。
- [ツール（Tools）] > [管理（Admin）] > [デバイス通信（Device Communication）] > [SSL証明書パラメータ（SSL Certificate Parameters）] > [PIX/ASA/FWSMデバイス認証証明書（PIX/ASA/FWSM Device Authentication Certificates）] が [デバイスの追加中に再取得（Retrieve while adding devices）] に設定されているかどうか確認します。
- イメージのアップグレード後、デバイスが Security Manager に再度追加されていることを確認します。それ以外の場合は、管理オプションを [証明書の認証を確認しない（Do not check certificate authentication）] に変更します。

（注） Image Manager が cisco.com に接続できるようにするには、最新の Cisco.com 証明書を受け入れている必要があります。イメージのダウンロードを正常に開始するには、「イメージメタデータロケータ」サイトとイメージのダウンロードサイトの両方からの証明書を受け入れる必要があります（[Image Manager] ページを参照）。

Security Manager のアップグレード後、Image Manager にデバイスのデータが存在しない

- デバイスインベントリのみを検出することを選択してデバイスを再検出します。
- デバイスへのライブ展開を実行します。
- デバイスへのイメージインストール操作を実行します。

ジョブを再試行またはロールバックしようとすると失敗する

- ジョブ内のいずれかのデバイスが Security Manager から削除されているかどうかを確認します。
- 再試行またはロールバックするすべてのイメージが Security Manager で使用できるかどうかを確認します。イメージを Security Manager リポジトリに追加して、操作を再試行します。

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。