CHAPTER 46

ソフトウェアとコンフィギュレーションの管理

この章では、ASA のソフトウェアおよびコンフィギュレーションの管理方法について説明します。この章は、次の項で構成されています。

ソフトウェアのアップグレード

ここでは、最新のバージョンにアップグレードする方法について説明します。説明する項目は次のとおりです。

（注） CLI の手順については、ASA のマニュアルを参照してください。

アップグレード パスと移行

- 8.3 より前のリリースからアップグレードする場合、
  - 設定の移行に関する重要な情報については、「*Cisco ASA 5500 Migration Guide to Version 8.3 and Later*」を参照してください。

- 9.0 より前のリリースからアップグレードする場合は、設定の移行については 9.0 リリース ノートの移行の章を参照してください。
- ゼロ ダウンタイム アップグレードのためのソフトウェア バージョン要件

  フェールオーバー構成や ASA クラスタのすべての装置の、ソフトウェアのメジャー バージョン（最初の番号）とマイナー バージョン（2 番目の番号）が同じである必要があります。ただし、アップグレード プロセス中に装置のバージョン パリティを維持する必要はありません。それぞれの装置で実行されるソフトウェアのバージョンが異なっていても、フェールオーバーのサポートを維持できます。長期の互換性および安定性を確保するために、すべての装置をできるだけ早く同じバージョンにアップグレードすることをお勧めします。

  表 46-1 に、ゼロ ダウンタイム アップグレードの実行がサポートされるシナリオを示します。

表 46-1　ゼロダウンタイム アップグレードのサポート

アップグレードのタイプ	サポート
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。特定のマイナー リリースでサポートされないモデルの場合は、そのマイナー リリースをスキップできます。たとえば ASA 5585-X の場合は、8.2 から 8.4 にアップグレードできます（このモデルは 8.3 ではサポートされていません）。
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、7.2 が 7.x リリース シリーズ最後のマイナー バージョンであれば、7.2 から 8.0 にアップグレードできます。 **（注）** ゼロ ダウン タイムのアップグレードは、機能の設定が 8.2 から 8.3 などに移行されていても可能です。

現在のバージョンの表示

ソフトウェア バージョンは ASDM ホーム ページに表示されます。ASA のソフトウェア バージョンを確認するには、ホーム ページを参照してください。

Cisco.com からのソフトウェアのダウンロード

アップグレード ウィザード ASDM を使用している場合は、事前ダウンロード ソフトウェアは必要ありません。フェールオーバー アップグレードなど手動でのアップグレードの場合は、ローカル コンピュータにイメージをダウンロードします。

Cisco.com のログインをお持ちの場合は、次の Web サイトから OS および ASDM のイメージを入手できます。

http://www.cisco.com/cisco/software/navigator.html?mdfid=279513386

スタンドアロン ユニットのアップグレード

（注）　ここでは、ASDM とオペレーティング システム（OS）イメージのインストール方法を説明します。ASA でバージョン 8.0 以降が実行されてい場合は、OS をアップグレードする前に ASDM の最新バージョン（実行には接続の切断と再接続が必要）にアップグレード可能です。例外は、ASA 8.5 など、最新の ASDM バージョンがサポートしていない ASA バージョンです。この場合は、8.0 よりも前のバージョン（ASDM 5.2 以前）の手順に従ってください。

ASA で 8.0 より前のバージョンが実行されている場合は、インストール済みバージョンの ASDM を使用して最新バージョンの OS および ASDM の両方をアップグレードし、リロードします。

ローカル コンピュータ（ASDM 6.0 以降）からのアップグレード

Upgrade Software from Local Computer ツールにより、コンピュータからフラッシュ メモリにイメージ ファイルをアップロードし、ASA をアップグレードできます。

コンピュータからソフトウェアをアップグレードするには、次の手順を実行します。

ステップ 1　（設定の移行の場合）ASDM で、[Tools] > [Backup Configurations] ツールにより、現在の設定をバック アップします。

ステップ 2　メイン ASDM アプリケーション ウィンドウで、[Tools] > [Upgrade Software from Local Computer] の順に選択します。

[Upgrade Software] ダイアログボックスが表示されます。

ステップ 3　[Image to Upload] ドロップダウン リストから、[ASDM] を選択します。

ステップ 4　[Local File Path] フィールドにコンピュータ上のファイルへのローカル パスを入力するか、[Browse Local Files] をクリックして PC 上のファイルを検索します。

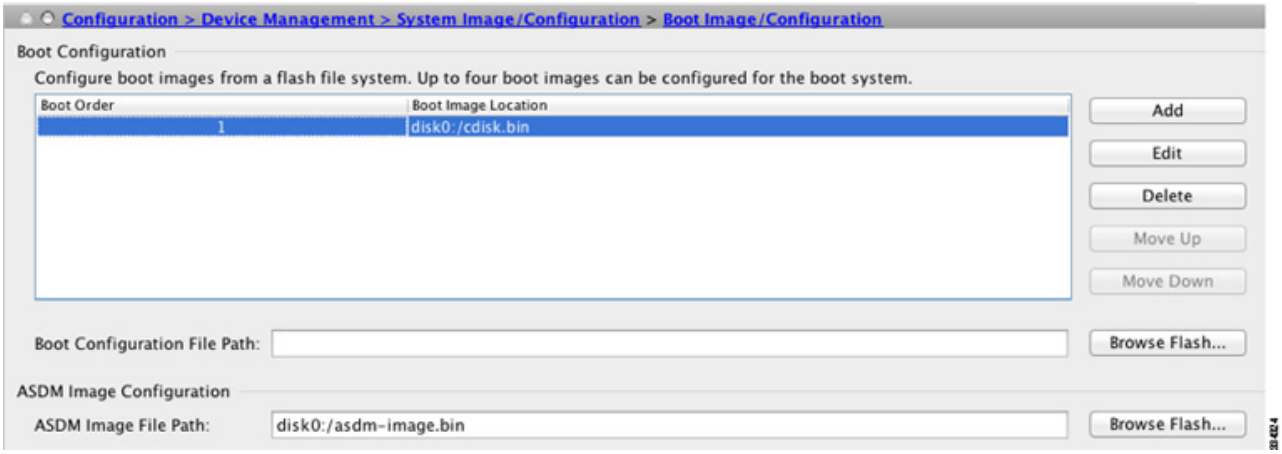
ステップ 5　[Flash File System Path] フィールドにフラッシュ ファイル システムへのパスを入力するか、[Browse Flash] をクリックしてフラッシュ ファイル システム上のディレクトリまたはファイルを検索します。

ステップ 6　[Upload Image] をクリックします。アップグレード プロセスには数分かかる場合があります。

ステップ 7　ステップ 2からステップ 6を繰り返し、[Image to Upload] ドロップダウン リストで [ASA] を選択します。この手順は、その他のタイプのファイルのアップロードでも同じです。

ステップ 8　ASA を設定して、新しいイメージを使用します。

a. [Configuration] > [Device Management] > [System Image/Configuration] > [Boot Image/Configuration] の順に選択します。



b. ブート設定テーブルで [Add] をクリックして、新しいイメージ（表示されているイメージが 4 つ未満の場合）を追加します。既存のイメージを選択し、[Edit] をクリックして新しいイメージに変更することもできます。

イメージを指定しない場合は、ASA が内部フラッシュ メモリからブート用に有効な最初のイメージを検索します。特定のイメージからのブートを推奨します。

c. [Browse Flash] をクリックし、OS イメージを選択して、[OK] をクリックします。

d. [OK] をクリックして、[Boot Image/Configuration] ペインに戻ります。

e. 必要に応じて [Move Up] ボタンを使用して、新しいイメージがテーブルの最初のイメージであることを確認します。

f. [ASDM Image Configuration] 領域で、[Browse Flash] をクリックし、ASDM イメージを選択して、[OK] をクリックします。

g. [Apply] をクリックします。

ステップ 9　[File] > [Save Running Configuration to Flash] を選択して、設定変更を保存します。

ステップ 10　[Tools] > [System Reload] を選択して、ASA をリロードします。

リロードの詳細の確認を求める新しいウィンドウが表示されます。[Save the running configuration at the time of reload] オプション ボタンをクリックし、リロードする時刻（[Now] など）を選択して、[Schedule Reload] をクリックします。

リロードが開始されると、[Reload Status] ウィンドウにリロードの進行状況が表示されます。ASDM を終了するオプションもあります。

ステップ 11　ASA のリロード後、ASDM を再起動します。

Cisco.com Wizard （ASDM 6.3 以降）を使用したアップグレード

Upgrade Software from Cisco.com Wizard により、ASDM および ASA を最新のバージョンに自動的にアップグレードできます。

このウィザードでは、次の操作を実行できます。

- アップグレード用の ASA イメージ ファイルまたは ASDM イメージ ファイルを選択する。

（注）　ASDM は最新のイメージ バージョンをダウンロードし、そこにはビルド番号が含まれています。たとえば、8.4（2）をダウンロードした場合、そのダウンロードは 8.4（2.8）になります。この動作は想定されているため、計画したアップグレードを続行できます。

- 実行したアップグレードの変更点を確認する。
- イメージをダウンロードし、インストールする。
- インストールのステータスを確認する。
- インストールが正常に完了した場合は、ASA を再起動して、コンフィギュレーションを保存し、アップグレードを完了する。

手順の詳細

ステップ 1　（設定の移行の場合）ASDM で、[Tools] > [Backup Configurations] ツールにより、現在の設定をバック アップします。

ステップ 2　[Tools] > [Check for ASA/ASDM Updates] を選択します。

マルチ コンテキスト モードでは、システムからこのメニューにアクセスします。

[Cisco.com Authentication] ダイアログボックスが表示されます。

ステップ 3　割り当てられている Cisco.com ユーザ名、および Cisco.com パスワードを入力し、[Login] をクリックします。

[Cisco.com Upgrade Wizard] が表示されます。

（注）　利用可能なアップグレードがない場合は、ダイアログボックスが表示されます。ウィザードを終了するには、[OK] をクリックします。

ステップ 4　[Next] をクリックして [Select Software] 画面を表示します。

現在の ASA バージョンおよび ASDM バージョンが表示されます。

ステップ 5　ASA バージョンおよび ASDM バージョンをアップグレードするには、次の手順を実行します。

a.　[ASA] 領域で、[Upgrade to] チェックボックスをオンにしてから、アップグレードする ASA バージョンをドロップダウン リストから選択します。

b.　[ASDM] 領域で、[Upgrade to] チェックボックスをオンにしてから、アップグレードする ASDM バージョンをドロップダウン リストから選択します。

ステップ 6　[Next] をクリックして [Review Changes] 画面を表示します。

ステップ 7　次の項目を確認します。

- ダウンロードした ASA イメージ ファイルや ASDM イメージ ファイルが正しいファイルであること。
- アップロードする ASA イメージ ファイルや ASDM イメージ ファイルが正しいファイルであること。
- 正しい ASA ブート イメージが選択されていること。

ステップ 8　[Next] をクリックして、アップグレード インストールを開始します。

アップグレード インストールの進行状況を示すステータスを表示できます。

[Results] 画面が表示され、アップグレード インストール ステータス（成功または失敗）など、追加の詳細が示されます。

バージョン 8.2（1）からバージョン 8.3（1）へのアップグレード プロセス時に、次のファイルがフラッシュ メモリに自動的に保存されます。

- スタートアップ コンフィギュレーション
- コンテキストごとのコンフィギュレーション
- 移行メッセージが含まれるブートアップ エラー ログ

コンフィギュレーション ファイルを保存するにはメモリが不足している場合は、ASA のコンソール上にエラー メッセージが表示され、ブートアップ エラー ログ ファイルに保存されます。また、以前保存されたすべてのコンフィギュレーション ファイルは削除されます。

ステップ 9　アップグレード インストールが成功した場合に、アップグレード バージョンを有効にするには、[Save configuration and reload device now] チェックボックスをオンにして、ASA を再起動し、ASDM を再起動します。

ステップ 10　[Finish] をクリックして、ウィザードを終了し、コンフィギュレーションに対して行った変更を保存します。

（注）　次に高いバージョン（存在する場合）にアップグレードするには、ウィザードを再起動する必要があります。

Cisco.com Wizard（ASDM 6.0 ～ ASDM 6.2）を使用したアップグレード

手順の詳細

ステップ 1　（設定の移行の場合）ASDM で、[Tools] > [Backup Configurations] ツールにより、現在の設定をバック アップします。

ステップ 2　[Tools] メニューから、[Tools] > [Upgrades Software from Cisco.com] を選択します。

マルチ コンテキスト モードでは、システムからこのメニューにアクセスします。

[Upgrade Software from Cisco.com Wizard] が表示されます。

ステップ 3　[Next] をクリックします。

[Authentication] 画面が表示されます。

ステップ 4　Cisco.com のユーザ名とパスワードを入力し、[Next] をクリックします。

[Image Selection] 画面が表示されます。

ステップ 5　[Upgrade the ASA version] チェックボックスと [Upgrade the ASDM version] チェックボックスをオンにして、アップグレードしたい最新のイメージを指定し、[Next] をクリックします。

[Selected Images] 画面が表示されます。

ステップ 6　選択したイメージ ファイルが正しいことを確認し、[Next] をクリックしてアップグレードを開始します。

アップグレードに数分かかることを示すメッセージがウィザードに表示されます。アップグレードの進行状況を示すステータスを表示できます。

[Results] 画面が表示されます。この画面では、アップグレードが失敗したか、設定を保存して ASA をリロードするかなどの詳細も提供します。

ASA バージョンのアップグレードに成功したら、設定を保存して ASA をリロードするためのオプションが表示されます。

ステップ 7　[Yes] をクリックします。

アップグレード バージョンを有効にするには、コンフィギュレーションを保存して ASA をリロードし、ASDM を再起動する必要があります。

ステップ 8　アップグレードが終了したら、[Finish] をクリックしてウィザードを終了します。

ステップ 9　ASA のリロード後、ASDM を再起動します。

ローカル コンピュータ（ASDM 5.2 以前）からのアップグレード

手順の詳細

ステップ 1　（設定の移行の場合）ASDM、現在の設定をバック アップします。たとえば、[File] > [Show Running Configuration in New Window] を選択して、HTML ページに設定を開きます。[File] > [Save Running Configuration] オプションの 1 つを使う方法もあります。

ステップ 2　[Tools] > [Upgrade Software] を選択します。

ステップ 3　[Image to Upload] ドロップダウン リストから、[ASDM] を選択します。

ステップ 4　[Browse Local Files] をクリックして、Cisco.com からダウンロードした ASDM イメージに移動します。

ステップ 5　[Browse Flash] をクリックして、新しい ASDM イメージのインストール場所を決定します。

[Browse Flash] ダイアログボックスが表示されます。新しい場所を選択し、[OK] をクリックします。現在のイメージと新しいイメージの両方を置く容量がない場合は、現在のイメージに上書きインストールできます。

ステップ 6　[Upload Image] をクリックします。

イメージがアップロードされるのを待ちます。アップロードが成功したことを示す [Information] ウィンドウが表示されます。

ステップ 7　ステップ 2 から ステップ 6 を繰り返し、[Image to Upload] ドロップダウン リストで [ASA] を選択します。

ステップ 8　[Close] をクリックして、[Upgrade Software] ダイアログボックスから出ます。

ステップ 9　新しいイメージを使用するには、ASA を設定します。

a.　[Configuration] > [Properties] > [Device Administration] > [Boot Image/Configuration] を選択します。

b. ブート設定テーブルで [Add] をクリックして、新しいイメージ（表示されているイメージが 4 つ未満の場合）を追加します。既存のイメージを選択し、[Edit] をクリックして新しいイメージに変更することもできます。

   イメージを指定しない場合は、ASA が内部フラッシュ メモリからブート用に有効な最初のイメージを検索します。特定のイメージからのブートを推奨します。

c. [Browse Flash] をクリックし、OS イメージを選択して、[OK] をクリックします。

d. [OK] をクリックして、[Boot Image/Configuration] ペインに戻ります。

e. 必要に応じて [Move Up] ボタンを使用して、新しいイメージがテーブルの最初のイメージであることを確認します。

f. [ASDM Image Configuration] 領域で、[Browse Flash] をクリックし、ASDM イメージを選択して、[OK] をクリックします。

g. [Apply] をクリックします。

ステップ 10　[File] > [Save Running Configuration to Flash] を選択して、設定変更を保存します。

ステップ 11　[Tools] > [System Reload] を選択して、ASA をリロードします。

リロードの詳細の確認を求める新しいウィンドウが表示されます。[Save the running configuration at the time of reload] オプション ボタンをクリックし、リロードする時刻（[Now] など）を選択して、[Schedule Reload] をクリックします。

リロードが開始されると、[Reload Status] ウィンドウにリロードの進行状況が表示されます。ASDM を終了するオプションもあります。

ステップ 12　ASA のリロード後、ASDM を再起動します。

フェールオーバー ペアまたは ASA クラスタのアップグレード

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

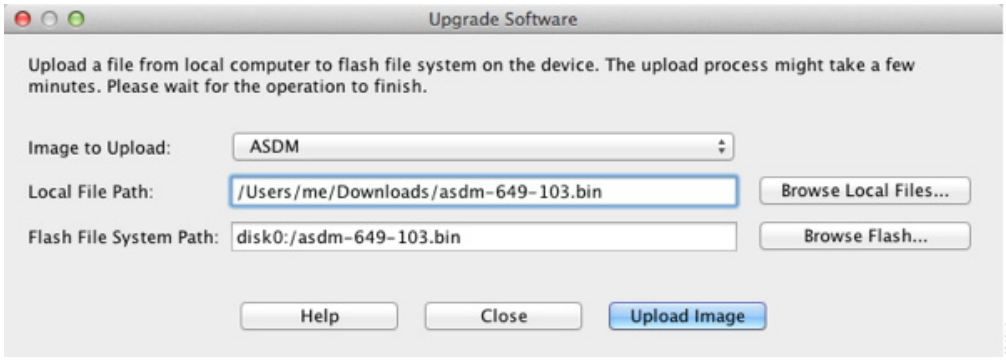
アクティブ/スタンバイ フェールオーバー ペアをアップグレードするには、次の手順を実行します。

手順の詳細

ステップ 1　（設定の移行の場合）ASDM で、[Tools] > [Backup Configurations] ツールにより、現在の設定をバック アップします。

ステップ 2　アクティブ装置のメイン ASDM アプリケーション ウィンドウで、[Tools] > [Upgrade Software from Local Computer] を選択します。

[Upgrade Software] ダイアログボックスが表示されます。



ステップ 3　[Image to Upload] ドロップダウン リストから、[ASDM] を選択します。

ステップ 4　[Local File Path] フィールドにコンピュータ上のファイルへのローカル パスを入力するか、[Browse Local Files] **をクリックして PC 上のファイルを検索します。**

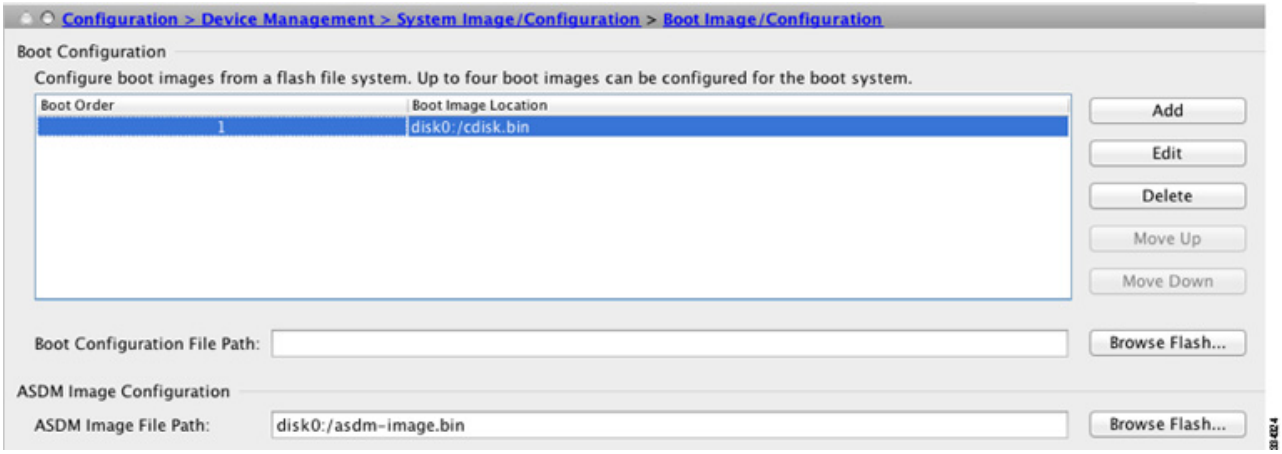
ステップ 5　[Flash File System Path] フィールドにフラッシュ ファイル システムへのパスを入力するか、[Browse Flash] をクリックしてフラッシュ ファイル システム上のディレクトリまたはファイルを検索します。

ステップ 6　[Upload Image] をクリックします。アップグレード プロセスには数分かかる場合があります。

ステップ 7　ステップ 2 から ステップ 6 を繰り返し、[Image to Upload] ドロップダウン リストで [ASA] を選択します。

ステップ 8　ASA を設定して、新しいイメージを使用します。

a.　[Configuration] > [Device Management] > [System Image/Configuration] > [Boot Image/Configuration] の順に選択します。



b.　ブート設定テーブルで [Add] をクリックして、新しいイメージ（表示されているイメージが 4 つ未満の場合）を追加します。既存のイメージを選択し、[Edit] をクリックして新しいイメージに変更することもできます。

イメージを指定しない場合は、ASA が内部フラッシュ メモリからブート用に有効な最初のイメージを検索します。特定のイメージからのブートを推奨します。

c.　[Browse Flash] をクリックし、OS イメージを選択して、[OK] をクリックします。

d.　[OK] をクリックして、[Boot Image/Configuration] ペインに戻ります。

e. 必要に応じて [Move Up] ボタンを使用して、新しいイメージがテーブルの最初のイメージであることを確認します。

f. [ASDM Image Configuration] 領域で、[Browse Flash] をクリックし、ASDM イメージを選択して、[OK] をクリックします。

g. [Apply] をクリックします。

ステップ 9　[File] > [Save Running Configuration to Flash] を選択して、設定変更を保存します。

ステップ 10　ASDM を*スタンバイ*装置に接続し、ステップ 2からステップ 7に従って ASA および ASDM ソフトウェアをアップロードします。このとき、アクティブ装置と同じ場所にファイルを置きます。

ステップ 11　[Tools] > [System Reload] を選択して、スタンバイ ASA をリロードします。

リロードの詳細の確認を求める新しいウィンドウが表示されます。[Save the running configuration at the time of reload] オプション ボタンをクリックし、リロードする時刻（[Now] など）を選択して、[Schedule Reload] をクリックします。

リロードが開始されると、[Reload Status] ウィンドウにリロードの進行状況が表示されます。ASDM を終了するオプションもあります。

ステップ 12　スタンバイ ASA のリロード後、ASDM を再起動し、スタンバイ装置に接続して、実行注であることを確認します。

ステップ 13　再度 ADSM を*アクティブ*装置に接続します。

ステップ 14　[Monitoring] > [Properties] > [Failover] > [Status] を選択して、アクティブ装置をスタンバイ装置にフェールオーバーし、[Make Standby] をクリックします。

ステップ 15　[Tools] > [System Reload] を選択して、（旧）アクティブ ASA をリロードします。

リロードの詳細の確認を求める新しいウィンドウが表示されます。[Save the running configuration at the time of reload] オプション ボタンをクリックし、リロードする時刻（[Now] など）を選択して、[Schedule Reload] をクリックします。

リロードが開始されると、[Reload Status] ウィンドウにリロードの進行状況が表示されます。ASDM を終了するオプションもあります。

ASA を起動すると、スタンバイ装置になります。

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

アクティブ/アクティブ フェールオーバー コンフィギュレーションの 2 つの装置をアップグレードするには、次の手順を実行します。

要件

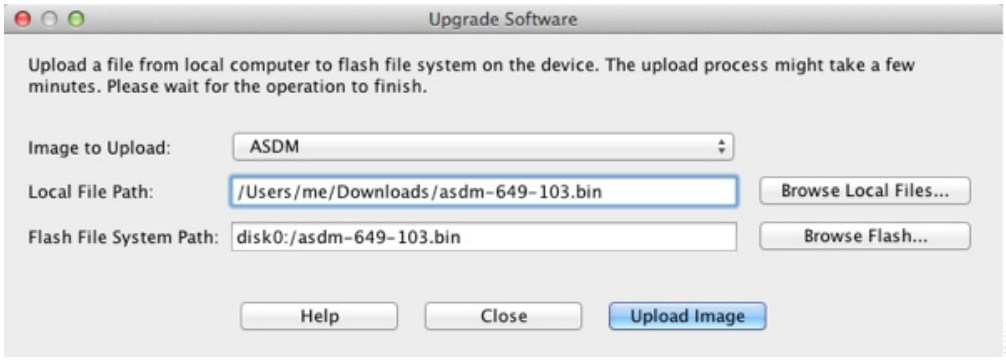
これらの手順をシステム実行スペース で実行します。

手順の詳細

ステップ 1　（設定の移行の場合）ASDM で、[Tools] > [Backup Configurations] ツールにより、現在の設定をバック アップします。

ステップ 2　プライマリ装置のメイン ASDM アプリケーション ウィンドウで、[Tools] > [Upgrade Software from Local Computer] を選択します。

[Upgrade Software] ダイアログボックスが表示されます。



ステップ 3　[Image to Upload] ドロップダウン リストから、[ASDM] を選択します。

ステップ 4　[Local File Path] フィールドにコンピュータ上のファイルへのローカル パスを入力するか、[Browse Local Files] をクリックして PC 上のファイルを検索します。

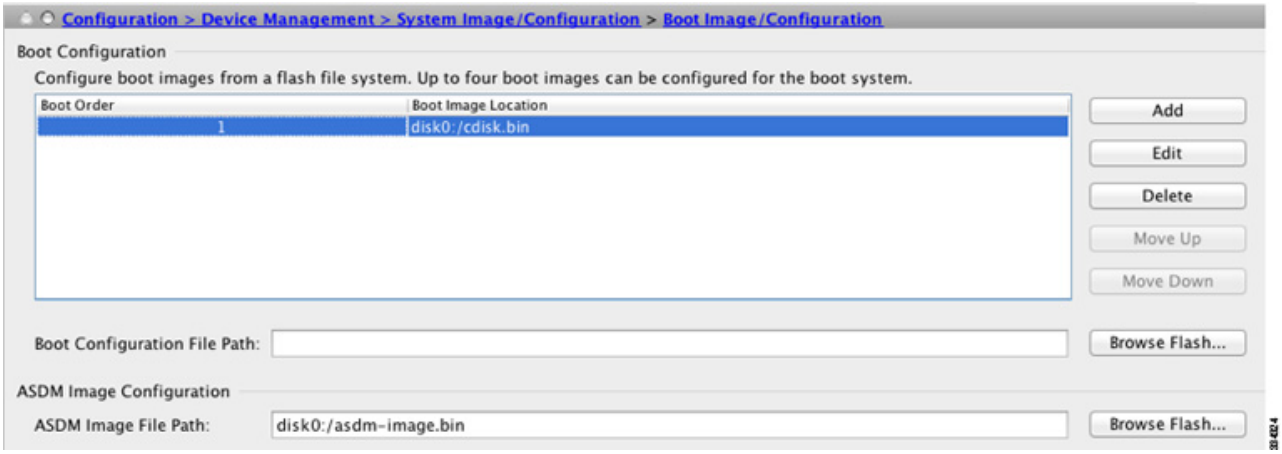
ステップ 5　[Flash File System Path] フィールドにフラッシュ ファイル システムへのパスを入力するか、[Browse Flash] をクリックしてフラッシュ ファイル システム上のディレクトリまたはファイルを検索します。

ステップ 6　[Upload Image] をクリックします。アップグレード プロセスには数分かかる場合があります。

ステップ 7　ステップ 2 から ステップ 6 を繰り返し、[Image to Upload] ドロップダウン リストで [ASA] を選択します。

ステップ 8　ASA を設定して、新しいイメージを使用します。

a.　[Configuration] > [Device Management] > [System Image/Configuration] > [Boot Image/Configuration] の順に選択します。



b.　ブート設定テーブルで [Add] をクリックして、新しいイメージ（表示されているイメージが 4 つ未満の場合）を追加します。既存のイメージを選択し、[Edit] をクリックして新しいイメージに変更することもできます。

イメージを指定しない場合は、ASA が内部フラッシュ メモリからブート用に有効な最初のイメージを検索します。特定のイメージからのブートを推奨します。

c.　[Browse Flash] をクリックし、OS イメージを選択して、[OK] をクリックします。

d.　[OK] をクリックして、[Boot Image/Configuration] ペインに戻ります。

e. 必要に応じて [Move Up] ボタンを使用して、新しいイメージがテーブルの最初のイメージであることを確認します。

f. [ASDM Image Configuration] 領域で、[Browse Flash] をクリックし、ASDM イメージを選択して、[OK] をクリックします。

g. [Apply] をクリックします。

ステップ 9　[File] > [Save Running Configuration to Flash] を選択して、設定変更を保存します。

ステップ 10　[Monitoring] > [Failover] > [Failover Group #] をクリックして、プライマリ装置上の両方のフェールオーバー グループをアクティブにします。ここで # は、プライマリ装置に移動するフェールオーバー グループ数です。[Make Active] をクリックします。

ステップ 11　ASDM を*セカンダリ*装置に接続し、ステップ 2からステップ 7に従って ASA および ASDM ソフトウェアをアップロードします。このとき、アクティブ装置と同じ場所にファイルを置きます。

ステップ 12　[Tools] > [System Reload] を選択して、セカンダリ ASA をリロードします。

リロードの詳細の確認を求める新しいウィンドウが表示されます。[Save the running configuration at the time of reload] オプション ボタンをクリックし、リロードする時刻（[Now] など）を選択して、[Schedule Reload] をクリックします。

リロードが開始されると、[Reload Status] ウィンドウにリロードの進行状況が表示されます。ASDM を終了するオプションもあります。

ステップ 13　ASDM を*プライマリ*装置に接続して、[Monitoring] > [Failover] > [System] の順に選択し、セカンダリ装置がリロードされたことを確認します。

ステップ 14　セカンダリ装置起動したら、[Monitoring] > [Properties] > [Failover] > [System] の順に選択して、プライマリ装置をセカンダリ装置にフェールオーバーし、[Make Standby] をクリックします。

ステップ 15　[Tools] > [System Reload] を選択して、（旧）アクティブ ASA をリロードします。

リロードの詳細の確認を求める新しいウィンドウが表示されます。[Save the running configuration at the time of reload] オプション ボタンをクリックし、リロードする時刻（[Now] など）を選択して、[Schedule Reload] をクリックします。

リロードが開始されると、[Reload Status] ウィンドウにリロードの進行状況が表示されます。ASDM を終了するオプションもあります。

フェールオーバー グループは、[Preempt Enabled] を使用して設定されると、プリエンプト遅延の経過後、指定された装置で自動的にアクティブになります。[Preempt Enabled] でフェールオーバー グループが設定されていない場合は、[Monitoring] > [Failover] > [Failover Group #] ペインを使用して、指定された装置上でアクティブ ステータスに戻すことができます。

ASA クラスタのアップグレード

ASA クラスタ内のすべての装置をアップグレードするには、マスター装置で次の手順を実行します。マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。

手順の詳細

ステップ 1　マスター装置で ASDM を起動します。

ステップ 2　（設定の移行の場合）ASDM で、[Tools] > [Backup Configurations] ツールにより、現在の設定をバック アップします。

ステップ 3　メイン ASDM アプリケーション ウィンドウで、[Tools] > [Upgrade Software from Local Computer] の順に選択します。

[Upgrade Software from Local Computer] ダイアログボックスが表示されます。

ステップ 4　[All devices in the cluster] オプション ボタンをクリックします。

ステップ 5　[Image to Upload] ドロップダウン リストから、新しいイメージ ファイルを選択します。

ステップ 6　[Local File Path] フィールドにコンピュータ上のファイルへのローカル パスを入力するか、[Browse Local Files] をクリックして PC 上のファイルを検索します。

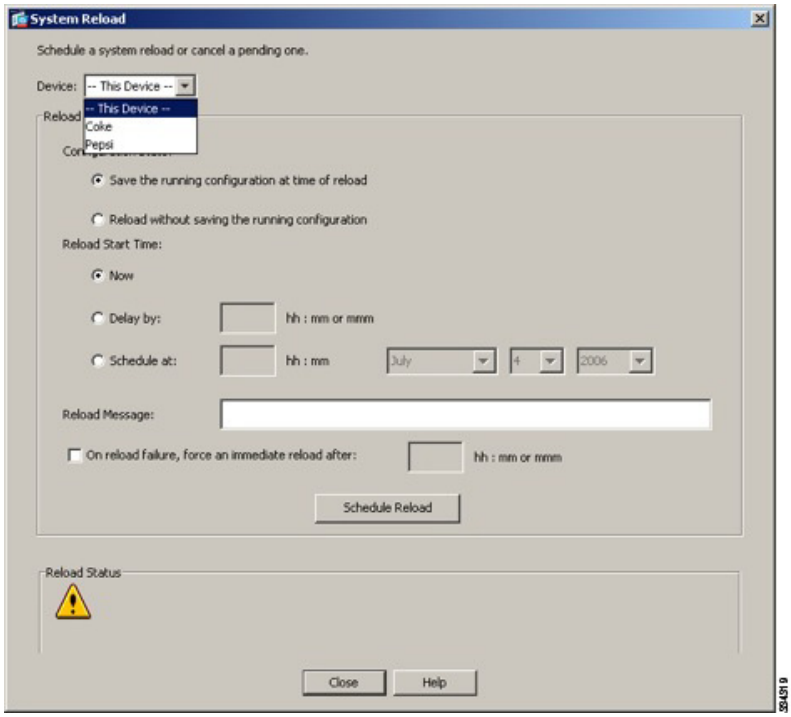
ステップ 7　[Flash File System Path] フィールドにフラッシュ ファイル システムへのパスを入力するか、[Browse Flash] をクリックしてフラッシュ ファイル システム上のディレクトリまたはファイルを検索します。

ステップ 8　[Upload Image] をクリックします。アップグレード プロセスには数分かかる場合があります。必ず終了するまでお待ちください。

ステップ 9　[Tools] > [System Reload] を選択します。

[System Reload] ダイアログボックスが表示されます。

ステップ 10　[Device] ドロップダウン リストでスレーブ装置名を選択して、各スレーブ装置を 1 台ずつリロードし、続いて [Schedule Reload] をクリックして装置をすぐにリロードします。



接続損失を回避しトラフィックを安定させるために、各装置が起動するまで（約 5 分）次の装置のリロードを待ちます。装置がクラスタに再接続したことを確認するには、[Monitoring] > [ASA Cluster] > [Cluster Summary] ペインを表示します。

ステップ 11　すべてのスレーブ装置のリロードが完了したら、[Configuration] > [Device Management] > [High Availability and Scalability] > [ASA Cluster] を選択して、マスター装置のクラスタリングをディセーブルにします。続いて [Participate ASA cluster] チェックボックスをオフにして、[Apply] をクリックします。

新しいマスターが選択されトラフィックが安定するまでに、5 分間かかります。それまでマスターであった装置がクラスタに再参加すると、その装置はスレーブとなります。

設定は保存しないでください。マスター装置がリロードしたら、そこでクラスタリングをイネーブルにします。

ステップ 12　[Tools] > [System Reload] を選択し、[Device] ドロップダウン リストから [--This Device--] を選択して [System Reload] ダイアログボックスからマスター装置をリロードします。

ステップ 13　ASDM を停止および再起動します。新しいマスター装置に再接続できます。

ファイルの管理

ASDM には、基本的なファイル管理タスクを実行するのに便利なファイル管理ツール セットが用意されています。ファイル管理ツールにより、フラッシュ メモリに保存されているファイルの表示、移動、コピー、および削除、ファイルの転送、およびリモート ストレージ デバイス（マウント ポイント）のファイルの管理を行うことができます。

（注）　マルチコンテキスト モードの場合、このツールはシステムのセキュリティ コンテキストでだけ使用できます。

ファイル管理ツールへのアクセス

ファイル管理ツールを使用するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [File Management] の順に選択します。

[File Management] ダイアログボックスが表示されます。

- [Folders] ペインには、ディスク上にあるフォルダが表示されます。
- [Flash Space] は、フラッシュ メモリの合計容量と、使用可能なメモリ容量を示します。
- [Files] 領域には、選択したフォルダのファイルについて次の情報が表示されます。
  - パス
  - ファイル名

- サイズ（バイト単位）
- 修正時刻
- 選択したファイルの種類（ブート コンフィギュレーション、ブート イメージ ファイル、ASDM イメージ ファイル、SVC イメージ ファイル、CSD イメージ ファイル、または APCF イメージ ファイル）を示す、ステータス

ステップ 2　選択したファイルをブラウザに表示するには、[View] をクリックします。

ステップ 3　選択したファイルを切り取って別のディレクトリに貼り付けるには、[Cut] をクリックします。

ステップ 4　選択したファイルをコピーして別のディレクトリに貼り付けるには、[Copy] をクリックします。

ステップ 5　コピーしたファイルを選択した場所に貼り付けるには、[Paste] をクリックします。

ステップ 6　選択したファイルをフラッシュ メモリから削除するには、[Delete] をクリックします。

ステップ 7　ファイルの名前を変更するには、[Rename] をクリックします。

ステップ 8　ファイルを保存するディレクトリを新規作成するには、[New Directory] をクリックします。

ステップ 9　[File Transfer] ダイアログボックスを開くには、[File Transfer] をクリックします。詳細については、「ファイル転送」（P.46-18）を参照してください。

ステップ 10　[Manage Points] ダイアログボックスを開くには、[Mount Points] をクリックします。詳細については、「マウント ポイントの管理」（P.46-15）を参照してください。

マウント ポイントの管理

この機能により、CIFS または FTP 接続を使用して、ネットワーク ファイル システムのリモート ストレージ（マウント ポイント）を設定できます。このダイアログボックスには、マウント ポイント、接続タイプ、サーバ名または IP アドレス、およびイネーブルにされた設定（yes または no）の一覧が表示されます。マウント ポイントは、追加、編集、または削除できます。詳細については、「CIFS/FTP マウント ポイントの追加または編集」（P.46-15）を参照してください。作成後に、CIFS マウント ポイントにアクセスできます。詳細については、「CIFS マウント ポイントのアクセス」（P.46-16）を参照してください。

この項では、次のトピックについて取り上げます。

CIFS/FTP マウント ポイントの追加または編集

CIFS マウント ポイントを追加するには、次の手順を実行します。

ステップ 1　[Add] をクリックし、[CIFS Mount Point] を選択します。

[Add CIFS Mount Point] ダイアログボックスが表示されます。

[Enable mount point] チェックボックスは、デフォルトで自動的にオンになります。

ステップ 2　該当するフィールドに、マウント ポイント、サーバ名または IP アドレス、および共有名を入力します。

ステップ 3　[Authentication] セクションで、NT ドメイン、ユーザ名、およびパスワードを入力し、続いてパスワードを確認します。

ステップ 4　[OK] をクリックします。

FTP マウント ポイントを追加するには、次の手順を実行します。

ステップ 1　[Add] をクリックし、[FTP Mount Point] を選択します。

[Add FTP Mount Point] ダイアログボックスが表示されます。

[Enable mount point] チェックボックスは、デフォルトで自動的にオンになります。

ステップ 2　該当するフィールドに、マウント ポイント名と、サーバ名または IP アドレスを入力します。

ステップ 3　[FTP Mount Options] 領域で、[Active Mode] または [Passive Mode] オプションをクリックします。

ステップ 4　リモート ストレージをマウントするパスを入力します。

ステップ 5　[Authentication] 領域で、NT ドメイン、ユーザ名、およびパスワードを入力し、続いてパスワードを確認します。

ステップ 6　[OK] をクリックします。

CIFS マウント ポイントを編集するには、次の手順を実行します。

ステップ 1　変更する CIFS マウント ポイントを選択し、[Edit] をクリックします。

[Edit CIFS Mount Point] ダイアログボックスが表示されます。

（注）　CIFS マウント ポイントは変更できません。

ステップ 2　残りの設定に変更を加え、変更が済んだら [OK] をクリックします。

FTP マウント ポイントを編集するには、次の手順を実行します。

ステップ 1　変更する FTP マウント ポイントを選択し、[Edit] をクリックします。

[Edit FTP Mount Point] ダイアログボックスが表示されます。

（注）　FTP マウント ポイントは変更できません。

ステップ 2　残りの設定に変更を加え、変更が済んだら [OK] をクリックします。

CIFS マウント ポイントのアクセス

作成後に CIFS マウント ポイントにアクセスするには、次の手順を実行します。

ステップ 1　ASA CLI を起動します。

ステップ 2　**mount** *name of mount* **type cifs** コマンドを入力し、マウントを作成します。

ステップ 3　**show run mount** コマンドを入力します。

次の出力が表示されます。

（注）　この例では、マウント名は win2003 です。

```
server kmmwin2003
share sharefolder
username webvpnuser2
password ********
status enable
```

ステップ 4　**dir** コマンドを入力し、イネーブルになっているすべてのマウントをサブディレクトリとして表示します。これは、Windows PC でドライブをマウントするのに似ています。たとえば、次の出力結果（FTP2003:、FTPLINUX:、および win2K:）は設定されたマウントです。

次に、**dir** コマンドの出力例を示します。

```
FTP2003: Directory or file name
FTPLINUX: Directory or file name
WIN2003: Directory or file name
all-filesystems List files on all filesystems
disk0: Directory or file name
disk1: Directory or file name
flash: Directory or file name
system: Directory or file name
win2K: Directory or file name
```

ステップ 5　そのマウントに対して **dir** コマンドを入力します（たとえば、**dir WIN2003**）。そして、フラッシュ メモリ（disk0:）からリストされたマウントのいずれかへ、またはマウントからフラッシュメモリへファイルをコピーします。

次に、**dir WIN2003** コマンドの出力例を示します。

```
Directory of WIN2003:/
---- 14920928 08:33:36 Apr 03 2009 1_5_0_01-windows-i586-p.exe
---- 33 11:27:16 Jun 07 2007 AArenameIE70
---- 28213021 15:15:22 Apr 03 2009 atest2(3).bin
---- 61946730 12:09:40 Mar 17 2009 atest2.bin
---- 5398366 14:52:10 Jul 28 2008 atest222.bin
---- 2587728 10:07:44 Dec 06 2005 cCITRIXICA32t.exe
---- 1499578 15:26:50 Dec 02 2005 ccore.exe
---- 61946728 11:40:36 Dec 09 2005 CIFSTESTT.bin
---- 2828 13:46:04 May 11 2009 ClientCert.pfx
d--- 16384 14:48:28 Mar 20 2007 cookiefolder
---- 4399 15:58:46 Jan 06 2006 Cookies.plist
---- 2781710 12:35:00 Dec 12 2006 coreftplite1.3.exe
---- 0 10:22:52 Jul 13 2007 coreftplite1.3.exe.download
---- 245760 15:13:38 Dec 21 2005 Dbgview.exe
---- 1408249 11:01:34 Dec 08 2005 expect-5.21r1b1-setup.exe
d--- 16384 14:49:14 Jul 28 2008 folder157
---- 101 09:33:48 Dec 12 2005 FxSasser.log
---- 2307104 09:54:12 Dec 12 2005 ica32t.exe
---- 8732552 10:14:32 Apr 29 2009 iclientSetup_IFen_flex51.exe
d--- 16384 08:32:46 Apr 03 2009 IE8withVistaTitan
---- 15955208 08:34:18 Aug 14 2007 j2re.exe
---- 16781620 13:38:22 Jul 23 2008 jre-1_5_0_06-windows-i586-p.exe
<--- More --->
```

ファイル転送

File Transfer ツールにより、ローカルにあるファイルとリモートにあるファイルを転送できます。PC またはフラッシュ ファイル システムのローカル ファイルを ASA との間で転送できます。HTTP、HTTPS、TFTP、FTP、または SMB を使用して、ASA との間でファイルを転送できます。

（注） IPS SSP ソフトウェア モジュールの場合、IPS ソフトウェアを disk0 にダウンロードする前に、フラッシュ メモリに少なくとも 50% の空きがあることを確認してください。IPS をインストールするときに、IPS のファイル システム用に内部フラッシュ メモリの 50% が予約されます。

- 「ローカル PC とフラッシュ間でのファイル転送」（P.46-18）
- 「リモート サーバとフラッシュ間でのファイル転送」（P.46-18）

ローカル PC とフラッシュ間でのファイル転送

ローカル PC とフラッシュ ファイル システムとの間でファイルを転送するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [File Management] の順に選択します。

[File Management] ダイアログボックスが表示されます。

ステップ 2　[File Transfer] の横にある下矢印をクリックし、続いて [Between Local PC and Flash] をクリックします。

[File Transfer] ダイアログボックスが表示されます。

ステップ 3　ローカル PC またはフラッシュ ファイル システムのどちらかで、アップロードまたはダウンロードしたいファイルを選択し、目的の場所に *ドラッグ*します。または、ローカル PC またはフラッシュ ファイル システムのどちらかで、アップロードまたはダウンロードしたいファイルを選択し、右矢印または左矢印をクリックし、目的の場所にファイルを転送します。

ステップ 4　完了したら [Close] をクリックします。

リモート サーバとフラッシュ間でのファイル転送

リモート サーバとフラッシュ ファイル システムとの間でファイルを転送するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [File Management] の順に選択します。

[File Management] ダイアログボックスが表示されます。

ステップ 2　[File Transfer] ドロップダウン リストで下矢印をクリックし、[Between Remote Server and Flash] をクリックします。

[File Transfer] ダイアログボックスが表示されます。

ステップ 3　リモート サーバからファイルを転送するには、[Remote server] オプションをクリックします。

ステップ 4　転送対象になるソース ファイルを定義します。

a.　サーバの IP アドレスを含めたファイルの場所へのパスを選択します。

（注）　ファイル転送は IPv4 および IPv6 のアドレスをサポートしています。

b. FTP の場合はリモート サーバのタイプを、HTTP または HTTPS の場合はリモート サーバのポート番号を入力します。有効な FTP タイプは次のとおりです。

- ap：パッシブ モードの ASCII ファイル
- an：非パッシブ モードの ASCII ファイル
- ip：パッシブ モードのバイナリ イメージ ファイル
- in：非パッシブ モードのバイナリ イメージ ファイル

ステップ 5　フラッシュ ファイル システムからファイルを転送するには、[Flash file system] オプションを選択します。

ステップ 6　ファイルの場所へのパスを入力するか、[Browse Flash] をクリックしてファイルの場所を指定します。

ステップ 7　また、CLI により、スタートアップ コンフィギュレーション、実行コンフィギュレーション、または SMB ファイル システムからファイルをコピーすることもできます。**copy** コマンドの使用方法については、『CLI 設定ガイド』を参照してください。

ステップ 8　転送するファイルの宛先を定義します。

a. フラッシュ ファイル システムにファイルを転送するには、[Flash file system] オプションを選択します。

b. ファイルの場所へのパスを入力するか、[Browse Flash] をクリックしてファイルの場所を指定します。

ステップ 9　リモート サーバにファイルを転送するには、[Remote server] オプションを選択します。

a. ファイルの場所へのパスを入力します。

b. FTP 転送の場合はタイプを入力します。有効なタイプは次のとおりです。

- ap：パッシブ モードの ASCII ファイル
- an：非パッシブ モードの ASCII ファイル
- ip：パッシブ モードのバイナリ イメージ ファイル
- in：非パッシブ モードのバイナリ イメージ ファイル

ステップ 10　[Transfer] をクリックしてファイル転送を開始します。

[Enter Username and Password] ダイアログボックスが表示されます。

ステップ 11　リモート サーバのユーザ名、パスワード、ドメイン（必要な場合）が表示されます。

ステップ 12　[OK] をクリックし、ファイル転送を続行します。

ファイル転送プロセスには数分かかる場合があります。必ず終了するまでお待ちください。

ステップ 13　ファイル転送が完了したら [Close] をクリックします。

使用するイメージおよびスタートアップ コンフィギュレーションの設定

デフォルトでは、ASA によって内部フラッシュ メモリ内で検出された最初のアプリケーション イメージがブートされます。また、内部フラッシュ メモリ内で最初に検出された ASDM イメージもブートされます。ASDM イメージが内部フラッシュ メモリに存在しない場合は、外部フラッシュ メモリ内が検索されます。複数のイメージがある場合は、ブートするイメージを指定する必要があります。ASDM イメージについては、ブートするイメージが指定されていない場合、インストールされているイメージが 1 つしかなくても、ASA がイメージを実行コンフィギュレーションに定義します。Auto Update（設定されている場合）の問題を避けるため、また起動時ごとのイメージ検索を回避するため、ブートする ASDM イメージをスタートアップ コンフィギュレーションで指定する必要があります。

[Configuration] > [Device Management] > [System Image/Configuration] > [Boot Image/Configuration] を選択します。

起動イメージとして使用するバイナリ イメージ ファイルは、ローカルから 4 つまで指定できます。また TFTP サーバのイメージを 1 つ指定し、そこからデバイスをブートできます。TFTP サーバに格納されているイメージを指定する場合は、そのファイルをリスト内の先頭に配置する必要があります。デバイスが、イメージのロード元の TFTP サーバに到達できない場合は、フラッシュ メモリに保存されているリスト内の次のイメージ ファイルのロードが試行されます。

ブート変数を指定しなければ、内部フラッシュ メモリの先頭にある有効なイメージからシステムがブートされます。[Boot Image/Configuration] ペインには、次のフィールドがあります。

- [Boot Order]：ブート時に使用されるバイナリ イメージ ファイルの順序を表示します。
- [Boot Image Location]：ブート ファイルの物理的な場所とパスを表示します。
- [Boot Configuration File Path]：コンフィギュレーション ファイルの場所を表示します。
- [Add]：ブート プロセスで使用するフラッシュ メモリまたは TFTP サーバのブート イメージ エントリを追加します。詳細については、「ブート イメージの追加」（P.46-20）を参照してください。
- [Edit]：フラッシュ メモリまたは TFTP サーバのイメージ エントリを編集します。
- [Delete]：フラッシュ メモリまたは TFTP サーバの選択されたイメージ エントリを削除します。
- [Move Up]：フラッシュ メモリまたは TFTP サーバの選択されたイメージ エントリの、ブート順序を上に移動します。
- [Move Down]：フラッシュ メモリまたは TFTP サーバの選択されたイメージ エントリの、ブート順序を下に移動します。
- [Browse Flash]：ブート イメージ ファイルまたはコンフィギュレーション ファイルの場所を指定します。
- [ASDM Image File Path]：起動時に使用するコンフィギュレーション ファイルの場所を表示します。

ブート イメージの追加

ブート イメージ エントリをブート順序リストに追加するには、[Boot Image/Configuration] ペインの [Add] をクリックします。

フラッシュ メモリまたは TFTP サーバのイメージを選択して、ブート イメージをブート順序リストに追加できます。

イメージのパスを入力するか [Browse Flash] をクリックして、イメージの場所を指定します。TFTP の場合、イメージの場所のパスを入力する必要があります。

- [Flash Image]：フラッシュ ファイル システムのブート イメージを選択して追加します。

  - [Path]：フラッシュ ファイル システムにあるブート イメージのパスを指定します。
- [TFTP Image]：TFTP サーバのブート イメージを選択して追加します。
  - [Path]：サーバの IP アドレスを含む、TFTP サーバ上のブート イメージ ファイルのパスを入力します。
- [OK]：変更内容を受け入れて、前のペインに戻ります。
- [Cancel]：変更内容を破棄して、前のペインに戻ります。
- [Help]：詳細情報を表示します。

設定 その他のファイルのバックアップおよびリストア

[Tools] メニューの [Backup and Restore] 機能オプションを使用して、ASA 実行コンフィギュレーション、スタートアップ コンフィギュレーション、インストールされたアドオン イメージ、SSL VPN クライアントのイメージとプロファイルをバックアップおよび復元できます。

ASDM の [Backup Configurations] 画面では、バックアップするファイル タイプを選択し、それらを単一の zip ファイルに圧縮し、その zip ファイルをコンピュータ上の選択したディレクトリに転送できます。同様に、ファイルを復元するには、コンピュータ上で転送元となる zip ファイルを選択し、復元するファイル タイプを選択します。

（注） これらのツールは、シングル コンテキスト モードでのみ使用可能です。

- 「コンフィギュレーションのバックアップ」（P.46-21）
- 「ローカル CA サーバのバックアップ」（P.46-24）
- 「コンフィギュレーションの復元」（P.46-25）
- 「TFTP サーバへの実行コンフィギュレーションの保存」（P.46-28）

コンフィギュレーションのバックアップ

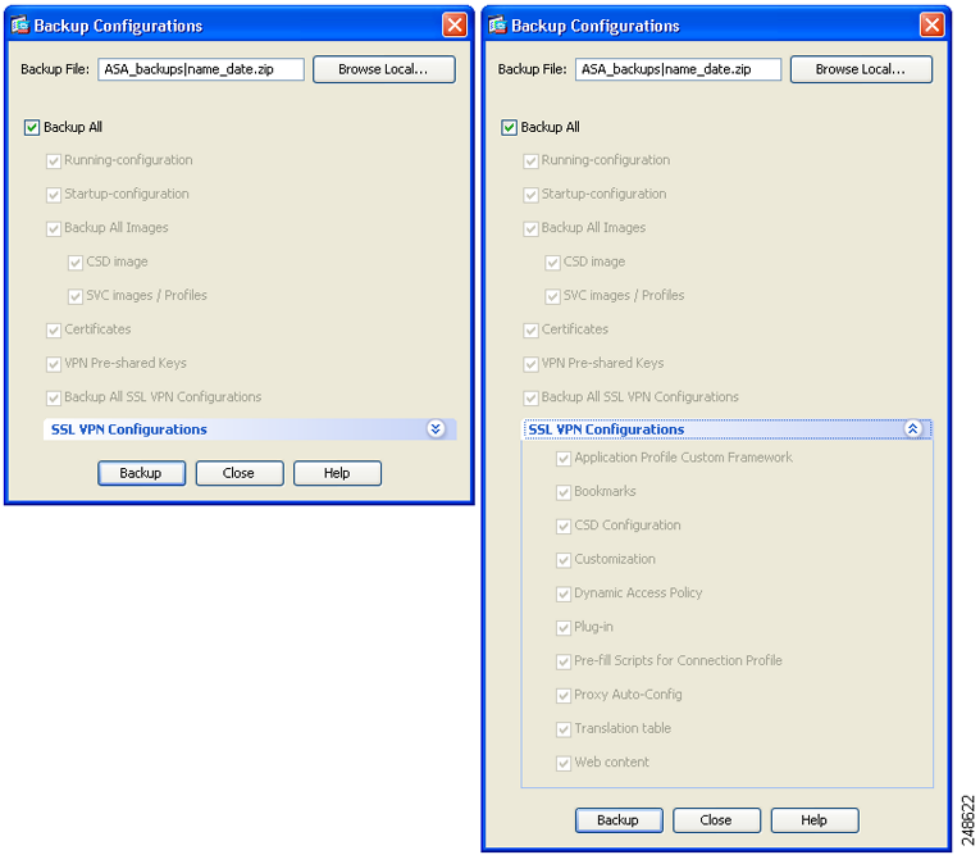
この手順では、コンフィギュレーションおよびイメージを .zip ファイルにバックアップし、それをローカル コンピュータに転送する方法について説明します。

注意 ASA にマスター パスフレーズを設定している場合は、この手順で作成したバックアップ コンフィギュレーションの復元時にそのマスター パスフレーズが必要となります。ASA のマスター パスフレーズが不明な場合は、「マスター パスフレーズの設定」（P.16-5）を参照して、バックアップを続行する前に、マスター パスフレーズをリセットする方法を確認してください。

ステップ 1　コンピュータ上にフォルダを作成し、バックアップ ファイルを保存します。こうすると、後で復元するときに探しやすくなります。

ステップ 2　[Tools] > [Backup Configurations] を選択します。

[Backup Configurations] ダイアログボックスが表示されます。[SSL VPN Configuration] 領域の下矢印をクリックし、SSL VPN コンフィギュレーションのバックアップ オプションを確認します。デフォルトでは、すべてのコンフィギュレーション ファイルがチェックされ、利用できる場合にはバックアップされます。リスト内のすべてのファイルをバックアップするには、手順 5 に進みます。



ステップ 3　バックアップするコンフィギュレーションを選択する場合は、[Backup All] チェックボックスをオフにします。

ステップ 4　バックアップするオプションの横にあるチェックボックスをオンにします。

ステップ 5　**[Browse Local] をクリックして、バックアップ .zip ファイルのディレクトリおよびファイル名を指定**します。

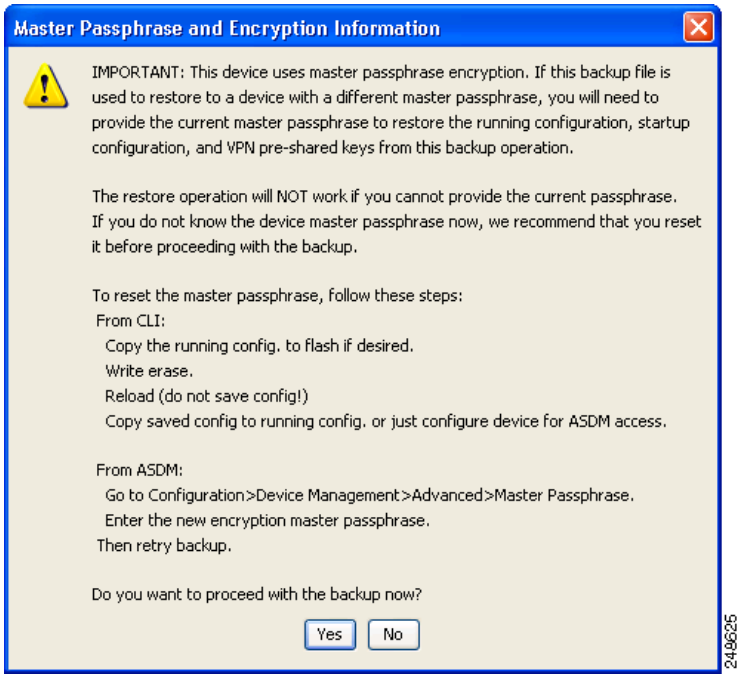
ステップ 6　[Select] ダイアログボックスで、バックアップ ファイルを格納するディレクトリを選択します。

ステップ 7　[Select] をクリックします。[Backup File] フィールドにパスが表示されます。

ステップ 8　ディレクトリ パスの後にバックアップ ファイルの宛先の名前を入力します。バックアップ ファイルの名前の長さは、3 ～ 232 文字の間である必要があります。

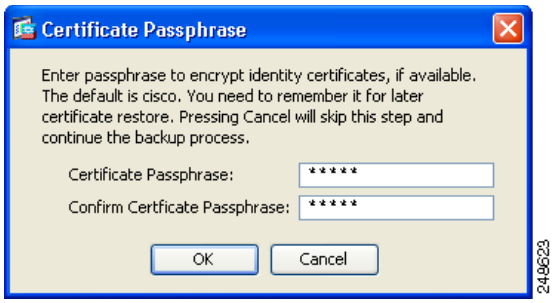
ステップ 9　[Backup] をクリックします。証明書をバックアップする場合や、ASA でマスター パスフレーズを使用している場合を除き、すぐにバックアップが続行されます。

ステップ 10　ASA でマスター パスフレーズを設定し、イネーブルにしている場合、バックアップを続行する前に、マスター パスフレーズが不明な場合は変更することを推奨する警告メッセージが表示されます。マスター パスフレーズがわかっている場合は、[Yes] をクリックしてバックアップを続行します。ID 証明書をバックアップする場合を除き、すぐにバックアップが続行されます。



ステップ 11　ID 証明書をバックアップする場合は、証明書を PKCS12 形式でエンコーディングするために使用する別のパスフレーズを入力するように求められます。パスフレーズを入力するか、またはこの手順をスキップすることができます。

（注）　このプロセスで ID 証明書はバックアップされますが、認証局の証明書はバックアップされません。CA 証明書のバックアップ手順については、「ローカル CA サーバのバックアップ」（P.46-24）を参照してください。

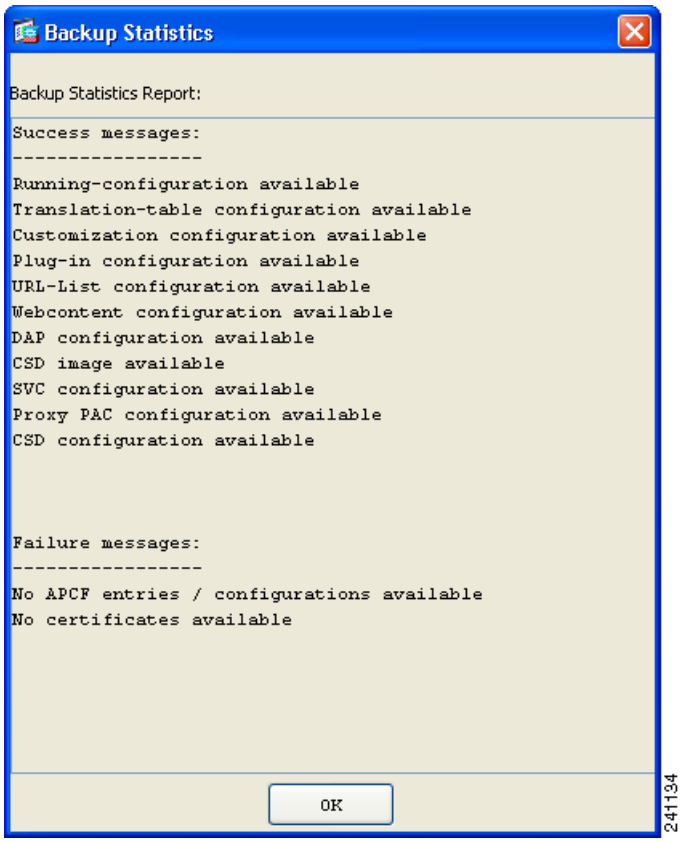


- 証明書を暗号化するには、[Certificate Passphrase] ダイアログボックスで証明書のパスフレーズを入力および確認し、[OK] をクリックします。証明書の復元時に必要となるため、このダイアログボックスに入力したパスワードを覚えておく必要があります。
- [Cancel] をクリックすると、この手順がスキップされ、証明書はバックアップされません。

[OK] をクリックするか、またはキャンセルすると、すぐにバックアップが開始されます。

ステップ 12　バックアップが完了すると、ステータス ウィンドウが閉じ、[Backup Statistics] ダイアログボックスが表示され、成功または失敗のメッセージが示されます。

（注）　バックアップの「失敗」メッセージは多くの場合、指定されたタイプの既存のコンフィギュレーションが存在しない場合に表示されます。



ステップ 13　[OK] をクリックし、[Backup Statistics] ダイアログボックスを閉じます。

ローカル CA サーバのバックアップ

ASDM バックアップを実行した場合、ローカル CA サーバ データベースは含まれていないため、サーバ上の CA 証明書はバックアップされません。ローカル CA サーバをバックアップする場合は、ASA CLI による次の手動プロセスを使用します。

ステップ 1　**show run crypto ca server** コマンドを入力します。

```
crypto ca server
 keysize server 2048
 subject-name-default OU=aa,O=Cisco,ST=ca,
 issuer-name CN=xxx,OU=yyy,O=Cisco,L=Bxb,St=Mass
 smtp from-address abcd@cisco.com
 publish-crl inside 80
 publish-crl outside 80
```

ステップ 2　**crypto ca import** コマンドを使用して、ローカル CA PKCS12 ファイルをインポートして LOCAL-CA-SERVER トラストポイントを作成し、キーペアを復元します。

```
crypto ca import LOCAL-CA-SERVER pkcs12 <passphrase> (paste the pkcs12
base64 data here)
```

（注）　この手順では、正確な名前「LOCAL-CA-SERVER」を必ず使用してください。

ステップ 3　LOCAL-CA-SERVER ディレクトリが存在しない場合、**mkdir LOCAL-CA-SERVER** を入力して作成する必要があります。

ステップ 4　ローカル CA ファイルを LOCAL-CA-SERVER ディレクトリにコピーします。

```
copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.ser
disk0:/LOCAL-CA-SERVER/

copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.cdb
disk0:/LOCAL-CA-SERVER/

copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.udb
disk0:/LOCAL-CA-SERVER/

copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.crl
disk0:/LOCAL-CA-SERVER/

copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.p12
disk0:/LOCAL-CA-SERVER/
```

ステップ 5　**crypto ca server** コマンドを入力して、ローカル CA サーバをイネーブルにします。

```
crypto ca server
 no shutdown
```

ステップ 6　**show crypto ca server** コマンドを入力して、ローカル CA サーバが起動し、動作していることを確認します。

ステップ 7　設定を保存します。

コンフィギュレーションの復元

zip ファイルからローカル PC に復元するコンフィギュレーションやイメージを指定します。

続行する前に、次のその他の制約事項に注意してください。

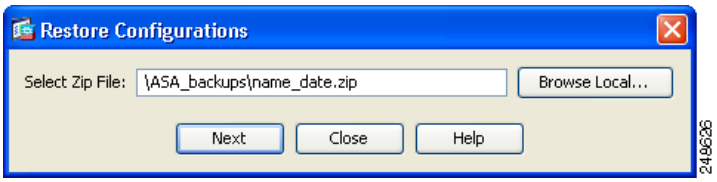
- 復元する zip ファイルは、[Tools] > [Backup Configurations] オプションを選択して作成したものである必要があります。
- マスター パスフレーズをイネーブルにしてバックアップを実行した場合、作成したバックアップから実行コンフィギュレーション、スタートアップ コンフィギュレーション、および VPN 事前共有キーを復元するときにそのマスター パスフレーズが必要になります。ASA のマスター パスフレーズが不明な場合、復元プロセス時にこれらの項目は復元されません。マスター パスフレーズの詳細については、「マスター パスフレーズの設定」（P.16-5）を参照してください。
- バックアップ時に証明書パスフレーズを指定した場合は、証明書を復元するためにそのパスフレーズを指定するよう求められます。デフォルトのパスフレーズは cisco です。
- DAP コンフィギュレーションは、実行中の特定のコンフィギュレーション、URL リスト、CSD コンフィギュレーションに依存することがあります。

- CSD コンフィギュレーションは、CSD イメージのバージョンに依存することがあります。
- 同じ ASA タイプから作成したバックアップを使用して、コンポーネント、イメージ、およびコンフィギュレーションを復元できます。ASDM アクセスを許可する基本コンフィギュレーションで起動する必要があります。

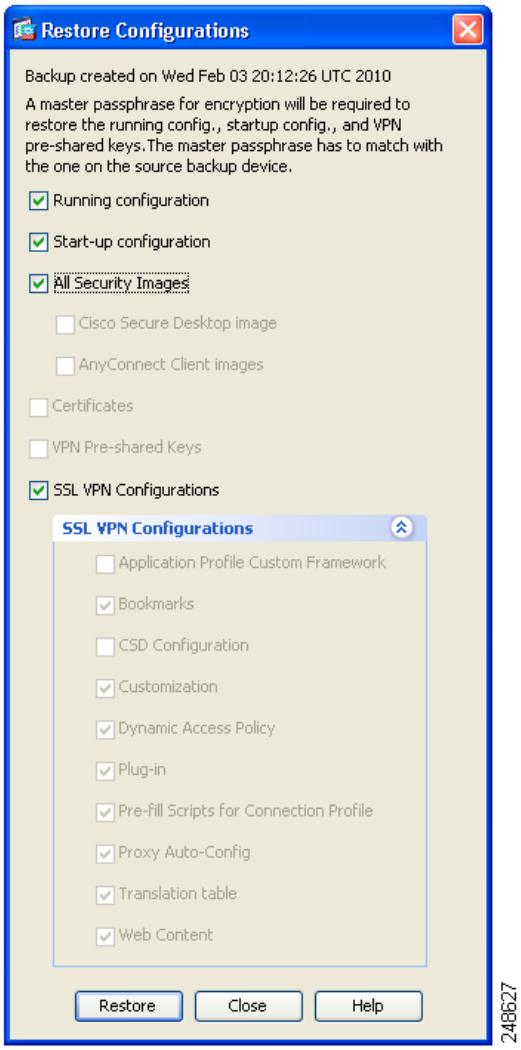
ASA コンフィギュレーションの選択されたエレメント、Cisco Secure Desktop イメージ、SSL VPN Client イメージとプロファイルを復元するには、次の手順を実行します。

ステップ 1　[Tools] > [Restore Configurations] を選択します。

ステップ 2　[Restore Configurations] ダイアログボックスで、[Browse Local Directory] をクリックし、ローカル コンピュータ上の、復元するコンフィギュレーションが含まれている zip ファイルを選択し、[Select] をクリックします。[Local File] フィールドにパスと zip ファイル名が表示されます。



ステップ 3　[Next] をクリックします。2 つ目の [Restore Configuration] ダイアログボックスが表示されます。復元するコンフィギュレーションの横にあるチェックボックスをオンにします。使用可能なすべての SSL VPN コンフィギュレーションがデフォルトで選択されています。



ステップ 4　[Restore] をクリックします。

ステップ 5　バックアップ ファイルの作成時に、証明書の暗号化に使用する証明書パスフレーズを指定している場合は、このパスフレーズを入力するように ASDM から求められます。

ステップ 6　実行コンフィギュレーションの復元を選択した場合、実行コンフィギュレーションを結合するか、実行コンフィギュレーションを置換するか、または復元プロセスのこの部分をスキップするかを尋ねられます。

- コンフィギュレーションの結合では、現在の実行コンフィギュレーションとバックアップされた実行コンフィギュレーションが結合されます。
- 実行コンフィギュレーションの置換では、バックアップされた実行コンフィギュレーションのみが使用されます。
- この手順をスキップすると、バックアップされた実行コンフィギュレーションは復元されません。

ASDM では、復元操作が完了するまでステータス ダイアログボックスが表示されます。

ステップ 7　実行コンフィギュレーションを置換または結合した場合は、ASDM を閉じてから再起動します。実行コンフィギュレーションを復元しなかった場合は、ASDM セッションをリフレッシュして、変更を有効にします。

TFTP サーバへの実行コンフィギュレーションの保存

この機能により、現在の実行コンフィギュレーション ファイルのコピーを TFTP サーバに保存します。

実行コンフィギュレーションを TFTP サーバに保存するには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[File] > [Save Running Configuration to TFTP Server] の順に選択します。

[Save Running Configuration to TFTP Server] ダイアログボックスが表示されます。

ステップ 2　TFTP サーバの IP アドレスと、コンフィギュレーション ファイルの保存先となる TFTP サーバ上のファイル パスを入力して、[Save Configuration] をクリックします。

（注）　デフォルトの TFTP 設定を行うには、[Configuration] > [Device Management] > [Management Access] > [File Access] > [TFTP Client] の順に選択します。この設定を行った後は、このダイアログボックスに、TFTP サーバの IP アドレスと TFTP サーバ上でのファイル パスが自動的に表示されます。

システム再起動のスケジュール

System Reload ツールにより、システムの再起動をスケジュールしたり、現在の再起動をキャンセルしたりできます。

再起動をスケジュールするには、次の手順を実行します。

ステップ 1　メイン ASDM アプリケーション ウィンドウで、[Tools] > [System Reload] の順に選択します。

ステップ 2　[Reload Scheduling] 領域で、次の設定を定義します。

a. [Configuration State] では、再起動時に実行コンフィギュレーションを保存するか、破棄するかのどちらかを選択します。

b. [Reload Start Time] では、次のオプションから選択します。

- 再起動をただちに実行するには、[Now] をクリックします。

- 指定した時間だけ再起動を遅らせるには、[Delay by] をクリックします。再起動開始までの時間を、時間と分単位、または分単位だけで入力します。
- 指定した時刻と日付に再起動を実行するようにスケジュールするには、[Schedule at] をクリックします。再起動の実行時刻を入力し、再起動のスケジュール日を選択します。

c. [Reload Message] フィールドに、再起動時に ASDM の開いているインスタンスに送信するメッセージを入力します。

d. 再起動を再試行するまでの経過時間を時間と分単位で、または分単位だけで表示するには、[On reload failure force immediate reload after] チェックボックスをオンにします。

e. 設定に従って再起動をスケジュールするには、[Schedule Reload] をクリックします。

[Reload Status] 領域には、再起動のステータスが表示されます。

ステップ 3　次のいずれかを選択します。

- スケジュールされた再起動を停止するには、[Cancel Reload] をクリックします。
- スケジュールされた再起動の終了後に [Reload Status] 表示をリフレッシュするには、[Refresh] をクリックします。
- スケジュールされた再起動の詳細を表示するには、[Details] をクリックします。

ソフトウェアのダウングレード

バージョン 8.3 にアップグレードすると、コンフィギュレーションが移行されます。既存のコンフィギュレーションは、自動的にフラッシュ メモリに保存されます。たとえば、バージョン 8.2（1）から 8.3（1）にアップグレードすると、古い 8.2（1）コンフィギュレーションはフラッシュ メモリ内の 8_2_1_0_startup_cfg.sav というファイルに保存されます。

（注）　ダウングレードする前に、古いコンフィギュレーションを手動で復元する必要があります。

この項では、ダウングレードする方法について説明します。次の項目を取り上げます。

- 「アクティベーション キーの互換性に関する情報」（P.46-29）
- 「ダウングレードの実行」（P.46-30）

アクティベーション キーの互換性に関する情報

任意の旧バージョンから最新バージョンにアップグレードした場合、アクティベーション キーの互換性は存続します。ただし、ダウングレード機能の維持には問題が生じる場合があります。

- バージョン 8.1 以前のバージョンにダウングレードする場合：アップグレード後に、*8.2 よりも前*に導入された追加の機能ライセンスをアクティブ化すると、ダウングレードした場合でも旧バージョンに対するアクティベーション キーの互換性は存続します。ただし、バージョン 8.2 以降のバージョンで導入された機能ライセンスをアクティブ化した場合は、アクティベーション キーの下位互換性がなくなります。互換性のないライセンス キーがある場合は、次のガイドラインを参照してください。
  - 旧バージョンでアクティベーション キーを入力した場合は、そのキーが ASA で使用されます（バージョン 8.2 以降のバージョンでアクティブ化した新しいライセンスがない場合）。

  - 新しいシステムで、以前のアクティベーション キーがない場合は、旧バージョンと互換性のある新しいアクティベーション キーを要求する必要があります。
- バージョン 8.2 以前のバージョンにダウングレードする場合：バージョン 8.3 では、よりロバストな時間ベース キーの使用およびフェールオーバー ライセンスの変更が次のとおり導入されました。
  - 複数の時間ベースのアクティベーション キーがアクティブな場合、ダウングレード時には一番最近アクティブ化された時間ベース キーのみがアクティブになれます。他のキーはすべて非アクティブ化されます。
  - フェールオーバー ペアに不一致のライセンスがある場合、ダウングレードによりフェールオーバーはディセーブルになります。キーが一致した場合でも、使用するライセンスは、結合されたライセンスではなくなります。

ダウングレードの実行

コンフィギュレーションの移行の詳細については、「[Tools] メニューの [Backup and Restore] 機能オプションを使用して、ASA 実行コンフィギュレーション、スタートアップ コンフィギュレーション、インストールされたアドオン イメージ、SSL VPN クライアントのイメージとプロファイルをバックアップおよび復元できます。」（P.46-21）を参照してください。

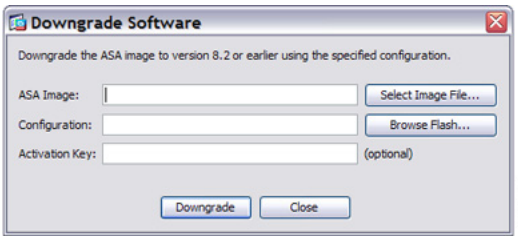
バージョン 8.3 からダウングレードするには、次の手順を実行します。

手順の詳細

ステップ 1　[Tools] > [Downgrade Software] を選択します。

[Downgrade Software] ダイアログボックスが表示されます。

図 46-1　Downgrade Software



ステップ 2　ASA イメージの場合、[Select Image File] をクリックします。

[Browse File Locations] ダイアログボックスが表示されます。

ステップ 3　次のいずれかのオプション ボタンをクリックします。

- [Remote Server]：ドロップダウン リストで [ftp]、[smb]、[http] のいずれかを選択し、以前のイメージ ファイルのパスを入力します。
- [Flash File System]：[Browse Flash] をクリックして、ローカル フラッシュ ファイル システムにある以前のイメージ ファイルを選択します。

ステップ 4　[Configuration] で [Browse Flash] をクリックし、移行前の設定ファイルを選択します（デフォルトでは disk0 に保存されています）。

ステップ 5　（任意）バージョン 8.3 よりも前のアクティベーション キーに戻す場合は、[Activation Key] フィールドで以前のアクティベーション キーを入力します。

詳細については、「アクティベーション キーの互換性に関する情報」（P.46-29）を参照してください。

ステップ 6　[Downgrade] をクリックします。

このツールは、次の機能を実行するためのショートカットです。

1. ブート イメージ コンフィギュレーションのクリア（**clear configure boot**）。
2. 古いイメージへのブート イメージの設定（**boot system**）。
3. （任意）新たなアクティベーション キーの入力（**activation-key**）。
4. 実行コンフィギュレーションのスタートアップ コンフィギュレーションへの保存（**write memory**）。これにより、BOOT 環境変数を古いイメージに設定します。このため、リロードすると古いイメージがロードされます。
5. 古いコンフィギュレーションのスタートアップ コンフィギュレーションへのコピー（**copy** *old_config_url* **startup-config**）。
6. リロード（**reload**）。

Auto Update の設定

この項では、次のトピックについて取り上げます。

- 「Auto Update に関する情報」（P.46-31）
- 「注意事項と制約事項」（P.46-35）
- 「Auto Update サーバとの通信の設定」（P.46-35）

Auto Update に関する情報

Auto Update は、Auto Update サーバがコンフィギュレーションおよびソフトウェア イメージを多数の ASA にダウンロードすることを許可し、中央からの ASA の基本的なモニタリングを提供するプロトコル仕様です。

- 「Auto Update クライアントまたはサーバ」（P.46-31）
- 「自動更新の利点」（P.46-31）
- 「フェールオーバー コンフィギュレーションでの Auto Update サーバ サポート」（P.46-32）

Auto Update クライアントまたはサーバ

ASA は、クライアントまたはサーバとして設定できます。Auto Update クライアントとして動作する場合は、ソフトウェア イメージおよびコンフィギュレーション ファイルへのアップデートのため、Auto Update サーバを定期的にポーリングします。Auto Update サーバとして動作する場合は、Auto Update クライアントとして設定された ASA のアップデートを発行します。

自動更新の利点

Auto Update は、次のように、管理者が ASA の管理で直面するさまざまな問題を解決できる便利な機能です。

- ダイナミック アドレッシングおよび NAT に関する問題点の解決。
- コンフィギュレーションの変更を 1 つのアクションでコミット。

- ソフトウェア更新用の信頼度の高い方式の提供。
- ハイ アベイラビリティ用の十分実績のある方式の活用（フェールオーバー）。
- オープン インターフェイスによる柔軟性の提供。
- サービス プロバイダー環境のセキュリティ ソリューションの簡素化。

Auto Update 仕様は、中央、または複数の場所から、リモート管理アプリケーションにより ASA のコンフィギュレーションやソフトウェア イメージをダウンロードしたり、基本的なモニタリング機能を実行したりする場合に必要なインフラストラクチャです。

Auto Update 仕様に従うと、Auto Update サーバから ASA にコンフィギュレーション情報をプッシュしたり、要求を送信して情報を取得したりすることも、ASA から Auto Update サーバに定期的にポーリングすることによって、最新のコンフィギュレーション情報を引き出す（プルする）こともできます。また、Auto Update サーバはいつでも ASA にコマンドを送信し、ただちにポーリング要求を送信させることもできます。Auto Update サーバと ASA の通信では、通信パスとローカル CLI コンフィギュレーションをすべての ASA に設定する必要があります。

フェールオーバー コンフィギュレーションでの Auto Update サーバ サポート

Auto Update サーバを使用して、ソフトウェア イメージとコンフィギュレーション ファイルを、アクティブ/スタンバイ フェールオーバー コンフィギュレーションの ASA に配置できます。アクティブ/スタンバイ フェールオーバー コンフィギュレーションで Auto Update をイネーブルにするには、フェールオーバー ペアのプライマリ装置に Auto Update サーバのコンフィギュレーションを入力します。

フェールオーバー コンフィギュレーションの Auto Update サーバ サポートには、次の制限と動作が適用されます。

- アクティブ/スタンバイ コンフィギュレーションがサポートされるのは、シングル モードだけです。
- 新しいプラットフォーム ソフトウェア イメージをロードする際、フェールオーバー ペアはトラフィックの転送を停止します。
- LAN ベースのフェールオーバーを使用する場合、新しいコンフィギュレーションによってフェールオーバー リンクのコンフィギュレーションが変更されてはいけません。フェールオーバー リンクのコンフィギュレーションが変更されると、装置間の通信は失敗します。
- Auto Update サーバへの Call Home を実行するのはプライマリ装置だけです。Call Home を実行するには、プライマリ装置がアクティブ状態である必要があります。そうでない場合、ASA は自動的にプライマリ装置にフェールオーバーします。
- ソフトウェア イメージまたはコンフィギュレーション ファイルをダウンロードするのは、プライマリ装置だけです。その後、ソフトウェア イメージまたはコンフィギュレーション ファイルはセカンダリ装置にコピーされます。
- インターフェイス MAC アドレスとハードウェアのシリアル番号は、プライマリ装置のものです。
- Auto Update サーバまたは HTTP サーバに保存されたコンフィギュレーション ファイルは、プライマリ装置専用です。

Auto Update プロセスの概要

次に、フェールオーバー コンフィギュレーションでの Auto Update プロセスの概要を示します。このプロセスは、フェールオーバーがイネーブルであり、動作していることを前提としています。装置がコンフィギュレーションを同期化している場合、SSM カードの不具合以外の理由でスタンバイ装置に障害が発生している場合、または、フェールオーバー リンクがダウンしている場合、Auto Update プロセスは実行できません。

1. 両方の装置は、プラットフォームおよび ASDM ソフトウェア チェックサムとバージョン情報を交換します。
2. プライマリ装置は Auto Update サーバにアクセスします。プライマリ装置がアクティブ状態でない場合、ASA はプライマリ装置にフェールオーバーした後、Auto Update サーバにアクセスします。
3. Auto Update サーバは、ソフトウェア チェックサムと URL 情報を返します。
4. プライマリ装置が、アクティブまたはスタンバイ装置のプラットフォーム イメージ ファイルをアップデートする必要があると判断した場合は、次の処理が実行されます。
   a. プライマリ装置は、Auto Update サーバの URL を使用して、HTTP サーバから適切なファイルを取得します。
   b. プライマリ装置は、そのイメージをスタンバイ装置にコピーしてから、自身のイメージをアップデートします。
   c. 両方の装置に新しいイメージがある場合は、セカンダリ（スタンバイ）装置が最初にリロードされます。
   - セカンダリ装置のブート時にヒットレス アップグレードが可能な場合は、セカンダリ装置がアクティブ装置になり、プライマリ装置がリロードされます。リロードが終了すると、プライマリ装置がアクティブ装置になります。
   - スタンバイ装置のブート時にヒットレス アップグレードができない場合は、両方の装置が同時にリロードされます。
   d. セカンダリ（スタンバイ）装置だけに新しいイメージがある場合は、セカンダリ装置だけがリロードされます。プライマリ装置は、セカンダリ装置のリロードが終了するまで待機します。
   e. プライマリ（アクティブ）装置だけに新しいイメージがある場合は、セカンダリ装置がアクティブ装置になり、プライマリ装置がリロードされます。
   f. もう一度アップデート プロセスが手順 1 から開始されます。
5. ASA が、プライマリまたはセカンダリ装置の ASDM ファイルをアップデートする必要があると判断した場合は、次の処理が実行されます。
   a. プライマリ装置は、Auto Update サーバから提供された URL を使用して、HTTP サーバから ASDM イメージ ファイルを取得します。
   b. プライマリ装置は、必要に応じてそのイメージをスタンバイ装置にコピーします。
   c. プライマリ装置は、自身の ASDM イメージをアップデートします。
   d. もう一度アップデート プロセスが手順 1 から開始されます。
6. プライマリ装置が、コンフィギュレーション ファイルをアップデートする必要があると判断した場合は、次の処理が実行されます。
   a. プライマリ装置は、指定された URL を使用して、からコンフィギュレーション ファイルを取得します。
   b. 両方の装置で同時に、古いコンフィギュレーションが新しいコンフィギュレーションに置換されます。
   c. もう一度アップデート プロセスが手順 1 から開始されます。

7. チェックサムがすべてのイメージおよびコンフィギュレーション ファイルと一致している場合、アップデートは必要ありません。このプロセスは、次のポーリング時間まで中断されます。

Auto Update プロセスのモニタリング

debug auto-update client または **debug fover cmd-exe** コマンドを使用して、Auto Update プロセスで実行される処理を表示できます。次に、**debug auto-update client** コマンドの出力例を示します。ターミナル セッションから **debug** コマンドを実行します。

```
Auto-update client: Sent DeviceDetails to /cgi-bin/dda.pl of server 192.168.0.21
Auto-update client: Processing UpdateInfo from server 192.168.0.21
   Component: asdm, URL: http://192.168.0.21/asdm.bint, checksum:
0x94bced0261cc992ae710faf8d244cf32
   Component: config, URL: http://192.168.0.21/config-rms.xml, checksum:
0x67358553572688a805a155af312f6898
   Component: image, URL: http://192.168.0.21/cdisk73.bin, checksum:
0x6d091b43ce96243e29a62f2330139419
Auto-update client: need to update img, act: yes, stby yes
name
ciscoasa(config)# Auto-update client: update img on stby unit...
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 2001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 2501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 3001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 3501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 4001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 4501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 5001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 5501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 6001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 6501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 7001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 7501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 8001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 8501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 9001, len = 1024
auto-update: Fover file copy waiting at clock tick 6129280
fover_parse: Rcvd file copy ack, ret = 0, seq = 4
auto-update: Fover filecopy returns value: 0 at clock tick 6150260, upd time 145980 msecs
Auto-update client: update img on active unit...
fover_parse: Rcvd image info from mate
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
Beginning configuration replication: Sending to mate.
auto-update: HA safe reload: reload active waiting with mate state: 50
auto-update: HA safe reload: reload active waiting with mate state: 50
```

```
auto-update: HA safe reload: reload active waiting with mate state: 80
        Sauto-update: HA safe reload: reload active unit at clock tick: 6266860
Auto-update client: Succeeded: Image, version: 0x6d091b43ce96243e29a62f2330139419
```

Auto Update プロセスが失敗すると、次の syslog メッセージが生成されます。

```
%ASA4-612002: Auto Update failed: file version: version reason: reason
```

失敗したアップデートに応じて、*file* は「image」、「asdm」、または「configuration」になります。*version* は、アップデートのバージョン番号です。*reason* は、アップデートが失敗した原因です。

注意事項と制約事項

- ASA のコンフィギュレーションが Auto Update で更新されても、ASDM には通知されません。[Refresh] または [File] > [Refresh **ASDM** with the Running Configuration on the Device] を選択して、最新のコンフィギュレーションを取得する必要があります。また、ASDM でコンフィギュレーションに加えた変更は失われます。
- Auto Update サーバと通信するためのプロトコルとして HTTPS が選択されている場合は、ASA は SSL を使用します。これは、ASA が DES または 3DES ライセンスを保有していることを必要とします。
- Auto Update は、シングル コンテキスト モードでのみサポートされます。

Auto Update サーバとの通信の設定

手順の詳細

Auto Update 機能を設定するには、[Configuration] > [Device Management] > [System Image/Configuration] > [Auto Update] を選択します。[Auto Update] ペインには、[Auto Update Servers] テーブルの他に [Timeout] 領域と [Polling] 領域があります。

[Auto Update Servers] テーブルで、Auto Update サーバにすでに設定されているパラメータを確認できます。ASA は、テーブルの一番上にあるサーバを最初にポーリングします。テーブル内のサーバの順序を変更するには、[Move Up] または [Move Down] をクリックします。[Auto Update Servers] テーブルには次のカラムがあります。

- [Server]：Auto Update サーバの名前または IP アドレス。
- [User Name]：Auto Update サーバのアクセス時に使用されるユーザ名。
- [Interface]：Auto Update サーバへの要求送信時に使用されるインターフェイス。
- [Verify Certificate]：Auto Update サーバが返した証明書を、ASA で CA のルート証明書と照合して確認するかどうかを指定します。Auto Update サーバおよび ASA は同じ CA を使用する必要があります。

[Auto Update Server] テーブルの行のいずれかをダブルクリックすると、[Edit Auto Update Server] ダイアログボックスが開き、Auto Update サーバのパラメータを変更できます。ここで行った変更はただちにテーブルに反映されますが、コンフィギュレーションに保存するには [Apply] をクリックする必要があります。

[Timeout] エリアでは、ASA が Auto Update サーバのタイムアウトを待つ時間を設定できます。[Timeout] 領域には次のフィールドがあります。

- [Enable Timeout Period]：ASA が Auto Update サーバから応答を受信しなかった場合にタイムアウトするには、オンにします。

- [Timeout Period (Minutes)]：Auto Update サーバから応答がなかった場合の ASA のタイムアウト時間（分単位）を指定します。

[Polling] エリアで、ASA から Auto Update サーバの情報をポーリングする頻度を設定できます。[Polling] 領域には次のフィールドがあります。

- [Polling Period (minutes)] : ASA から Auto Update サーバに新しい情報をポーリングするときの待ち時間（分単位）。
- [Poll on Specified Days]：ポーリングのスケジュールを指定します。
- [Set Polling Schedule] : [Set Polling Schedule] ダイアログボックスが表示され、Auto Update サーバをポーリングする日付と時刻を設定できます。
- [Retry Period (minutes)]：サーバのポーリングに失敗した場合、ASA から Auto Update サーバに新しい情報をポーリングするまでの待ち時間（分単位）。
- [Retry Count]：ASA から Auto Update サーバに新しい情報をポーリングするときの再試行回数。

Auto Update サーバの追加または編集

[Add/Edit Auto Update Server] ダイアログボックスには次のフィールドがあります。

- [URL]：Auto Update サーバが ASA と通信する際に使用する HTTP または HTTPS のプロトコルと Auto Update サーバへのパスです。
- [Interface]：Auto Update サーバに要求を送信する際に使用するインターフェイスです。
- [Verify Certificate] : ASA が Auto Update サーバにより返された証明書を CA のルート証明書と比較して検証できるようにする場合にクリックします。Auto Update サーバおよび ASA は同じ CA を使用する必要があります。

[User] 領域には次のフィールドがあります。

- [User Name (Optional)]：Auto Update サーバのアクセス時に必要なユーザ名を入力します。
- [Password]：Auto Update サーバのユーザ パスワードを入力します。
- [Confirm Password]：Auto Update サーバのユーザ パスワードを再入力します。
- [Use Device ID to uniquely identify the ASA] : デバイス ID による認証をイネーブルにします。デバイス ID により、ASA が Auto Update サーバを一意に識別できます。
- [Device ID]：使用するデバイス ID のタイプ。
  - [Hostname]：ホストの名前。
  - [Serial Number]：デバイスのシリアル番号。
  - [IP Address on interface]：選択したインターフェイスの IP アドレス。ASA を Auto Update サーバが一意に識別する場合に使用します。
  - [MAC Address on interface]：選択したインターフェイスの MAC アドレス。ASA を Auto Update サーバが一意に識別する場合に使用します。
  - [User-defined value]：一意のユーザ ID。

ポーリング スケジュールの設定

[Set Polling Schedule] ダイアログボックスでは、ASA から Auto Update サーバをポーリングする特定の日付と時刻を設定できます。

[Set Polling Schedule] ダイアログボックスには次のフィールドがあります。

[Days of the Week] : ASA から Auto Update サーバをポーリングする曜日のチェックボックスを選択します。

[Daily Update] ペイン グループでは、ASA が Auto Update サーバをポーリングする時刻を設定できます。次のフィールドがあります。

- [Start Time]：Auto Update のポーリング開始時刻を入力します。
- [Enable randomization]：ASA から Auto Update サーバをランダムに選択した時刻にポーリングするには、オンにします。