



CHAPTER 85

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」 (P.85-1)
- 「ファイルの管理」 (P.85-11)
- 「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」 (P.85-14)
- 「イメージをロードするための ROM モニタの使用」 (P.85-15)
- 「コンフィギュレーションまたはその他のファイルのバックアップ」 (P.85-18)
- 「ソフトウェアのダウングレード」 (P.85-27)
- 「Auto Update の設定」 (P.85-28)

ソフトウェアのアップグレード



(注)

以前のどのリリースからでも (ただし、ご使用のモデルに対応している場合に限り)、最新リリースに直接アップグレードできます。バージョン 9.0 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るので、ダウングレードできなくなります。ダウングレードが必要になった場合に備えて、コンフィギュレーションファイルをバックアップしてください。

バージョン 9.0 にアップグレードする場合は、リリース ノートの移行の項に記載されているコンフィギュレーション移行の情報を参照してください。

8.3 よりも前のリリースからアップグレードする場合は、『*Cisco ASA 5500 Migration Guide to Version 8.3 and Later*』に記載されている、コンフィギュレーション移行に関する重要な情報も参照してください。

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。

- 「現在のバージョンの表示」 (P.85-2)
- 「Cisco.com からのソフトウェアのダウンロード」 (P.85-2)
- 「スタンドアロン ユニットのアップグレード」 (P.85-2)
- 「フェールオーバー ペアまたは ASA クラスターのアップグレード」 (P.85-4)



(注) ASDM の手順については、ASDM のマニュアルを参照してください。

現在のバージョンの表示

ASA のソフトウェア バージョンを確認するには、**show version** コマンドを使用します。

Cisco.com からのソフトウェアのダウンロード

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>

この手順は、イメージを TFTP サーバに置くことを前提としていますが、その他のサーバ タイプもサポートされます。

スタンドアロン ユニットのアップグレード

この項では、ASDM およびオペレーティング システム (OS) のイメージをインストールする方法について説明します。この項の手順では、TFTP を使用します。FTP または HTTP の場合は、**copy** コマンドを参照してください。

手順の詳細

	コマンド	目的
ステップ1	<pre>more system:running-config</pre> <p>例:</p> <pre>hostname# more system:running-config</pre>	<p>(コンフィギュレーション移行がある場合) コンフィギュレーションをバックアップできるように、コンフィギュレーションを端末に表示します。このコマンドの出力をコピーし、テキストファイルにコンフィギュレーションを貼り付けます。</p> <p>(注) 8.3 よりも前のバージョンからアップグレードする場合は、実行コンフィギュレーションが自動的にバックアップされます。</p> <p>その他のバックアップ方法については、コンフィギュレーションガイドを参照してください。</p>
ステップ2	<pre>copy tftp://server[/path]/asa_image_name {disk0:/ disk1:/}[path/]asa_image_name</pre> <p>例:</p> <pre>hostname# copy tftp://10.1.1.1/asa901-smp-k9.bin disk0:/asa901-smp-k9.bin</pre>	<p>ASA ソフトウェアをアクティブ装置のフラッシュ メモリにコピーします。TFTP 以外の方法の場合は、copy コマンドを参照してください。</p>

	コマンド	目的
ステップ 3	<pre>copy tftp://server[/path]/asdm_image_name {disk0:/ disk1:/}[path/]asdm_image_name</pre> <p>例:</p> <pre>hostname# copy tftp://10.1.1.1/asdm-701.bin disk0:/asdm-701.bin</pre>	ASDM イメージをアクティブ装置のフラッシュメモリにコピーします。
ステップ 4	<pre>configure terminal</pre> <p>例:</p> <pre>hostname(config)# configure terminal</pre>	まだグローバル コンフィギュレーション モードを開始していない場合は、グローバル コンフィギュレーション モードを開始します。
ステップ 5	<pre>show running-config boot system</pre> <p>例:</p> <pre>hostname(config)# show running-config boot system boot system disk0:/cdisk.bin boot system disk0:/asa841-smp-k9.bin</pre>	設定されている現在のブート イメージを表示します (最大 4 個)。ASA は、表示された順序でイメージを使用します。最初のイメージが使用できない場合は次のイメージが使用され、以下同様です。新しいイメージ URL をリストの先頭に挿入することはできません。新しいイメージが先頭であることを指定するには、既存のエントリをすべて削除してから、次の手順に従ってイメージの URL を目的の順序で入力します。
ステップ 6	<pre>no boot system {disk0:/ disk1:/}[path/]asa_image_name</pre> <p>例:</p> <pre>hostname(config)# no boot system disk0:/cdisk.bin hostname(config)# no boot system disk0:/asa841-smp-k9.bin</pre>	既存のブート イメージ コンフィギュレーションがある場合は削除します。新しいブート イメージを最初の選択肢として入力できるようにするためです。
ステップ 7	<pre>boot system {disk0:/ disk1:/}[path/]asa_image_name</pre> <p>例:</p> <pre>hostname(config)# boot system disk0://asa901-smp-k9.bin</pre>	アップロードした ASA イメージを起動するように設定します。このイメージが使用できない場合に使用するバックアップ イメージに対して、このコマンドを繰り返します。たとえば、前の ステップ 6 で削除したイメージを再入力できます。
ステップ 8	<pre>asdm image {disk0:/ disk1:/}[path/]asdm_image_name</pre> <p>例:</p> <pre>hostname(config)# asdm image disk0:/asdm-701.bin</pre>	アップロードした ASDM イメージを起動するように設定します。使用するように設定できる ASDM イメージは 1 つだけであるため、最初に既存のコンフィギュレーションを削除する必要はありません。
ステップ 9	<pre>write memory</pre> <p>例:</p> <pre>hostname(config)# write memory</pre>	新しい設定をスタートアップ コンフィギュレーションに保存します。
ステップ 10	<pre>reload</pre> <p>例:</p> <pre>hostname# reload</pre>	ASA をリロードします。

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


- 「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」 (P.85-4)
- 「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」 (P.85-4)
- 「ASA クラスタのアップグレード」 (P.85-9)

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 85-1 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 85-1 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せん。マイナー リリースはスキップできません。 たとえば、7.0(1) から 7.1(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(1) から 7.2(1) 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(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 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.X リリースの最後のマイナー バージョンが 7.2(1) ならば、7.2(1) から 8.0(1) にアップグレードできます。  (注) ゼロ ダウンタイム アップグレードは、機能コンフィギュレーションが移行される時（たとえば 8.2(X) から 8.3(X) に）でも可能です。

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

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。

要件

アクティブ装置で次の手順を実行します。

手順の詳細

	コマンド	目的
ステップ1	<pre>more system:running-config</pre> <p>例:</p> <pre>active# more system:running-config</pre>	<p>(コンフィギュレーション移行がある場合) コンフィギュレーションをバックアップできるように、コンフィギュレーションを端末に表示します。このコマンドの出力をコピーし、テキストファイルにコンフィギュレーションを貼り付けます。</p> <p>(注) 8.3 よりも前のバージョンからアップグレードする場合は、実行コンフィギュレーションが自動的にバックアップされます。</p> <p>その他のバックアップ方法については、コンフィギュレーションガイドを参照してください。</p>
ステップ2	<pre>copy tftp://server[/path]/asa_image_name {disk0:/ disk1:/}[path/]asa_image_name</pre> <p>例:</p> <pre>active# copy tftp://10.1.1.1/asa901-smp-k9.bin disk0:/asa901-smp-k9.bin</pre>	<p>ASA ソフトウェアをアクティブ装置のフラッシュメモリにコピーします。TFTP 以外の方法の場合は、copy コマンドを参照してください。</p>
ステップ3	<pre>failover exec mate copy tftp://server[/path]/filename {disk0:/ disk1:/}[path/]filename</pre> <p>例:</p> <pre>active# failover exec mate copy tftp://10.1.1.1/asa901-smp-k9.bin disk0:/asa901-smp-k9.bin</pre>	<p>ソフトウェアをスタンバイ装置にコピーします。アクティブ装置で指定したのと同じパスを指定してください。</p>
ステップ4	<pre>copy tftp://server[/path]/asdm_image_name {disk0:/ disk1:/}[path/]asdm_image_name</pre> <p>例:</p> <pre>active# copy tftp://10.1.1.1/asdm-701.bin disk0:/asdm-701.bin</pre>	<p>ASDM イメージをアクティブ装置のフラッシュメモリにコピーします。</p>
ステップ5	<pre>failover exec mate copy tftp://server[/path]/asdm_image_name {disk0:/ disk1:/}[path/]asdm_image_name</pre> <p>例:</p> <pre>active# failover exec mate copy tftp://10.1.1.1/asdm-701.bin disk0:/asdm-701.bin</pre>	<p>ASDM イメージをスタンバイ装置にコピーします。アクティブ装置で指定したのと同じパスを指定してください。</p>
ステップ6	<pre>configure terminal</pre> <p>例:</p> <pre>active(config)# configure terminal</pre>	<p>まだグローバル コンフィギュレーション モードを開始していない場合は、グローバル コンフィギュレーション モードを開始します。</p>

■ ソフトウェアのアップグレード

	コマンド	目的
ステップ 7	<pre>show running-config boot system</pre> <p>例 : <pre>hostname(config)# show running-config boot system boot system disk0:/cdisk.bin boot system disk0:/asa841-smp-k9.bin</pre></p>	<p>設定されている現在のブートイメージを表示します (最大 4 個)。ASA は、表示された順序でイメージを使用します。最初のイメージが使用できない場合は次のイメージが使用され、以下同様です。新しいイメージ URL をリストの先頭に挿入することはできません。新しいイメージが先頭であることを指定するには、既存のエントリをすべて削除してから、次の手順に従ってイメージの URL を目的の順序で入力します。</p>
ステップ 8	<pre>no boot system {disk0:/ disk1:/}[path/]asa_image_name</pre> <p>例 : <pre>hostname(config)# no boot system disk0:/cdisk.bin hostname(config)# no boot system disk0:/asa841-smp-k9.bin</pre></p>	<p>既存のブート イメージ コンフィギュレーションがある場合は削除します。新しいブート イメージを最初の選択肢として入力できるようにするためです。</p>
ステップ 9	<pre>boot system {disk0:/ disk1:/}[path/]asa_image_name</pre> <p>例 : <pre>hostname(config)# boot system disk0://asa901-smp-k9.bin</pre></p>	<p>アップロードした ASA イメージを起動するように設定します。このイメージが使用できない場合に使用するバックアップ イメージに対して、このコマンドを繰り返します。たとえば、前の ステップ 8 で削除したイメージを再入力できます。</p>
ステップ 10	<pre>asdm image {disk0:/ disk1:/}[path/]asdm_image_name</pre> <p>例 : <pre>hostname(config)# asdm image disk0:/asdm-701.bin</pre></p>	<p>アップロードした ASDM イメージを起動するように設定します。使用するように設定できる ASDM イメージは 1 つだけであるため、最初に既存のコンフィギュレーションを削除する必要はありません。</p>
ステップ 11	<pre>write memory</pre> <p>例 : <pre>active(config)# write memory</pre></p>	<p>新しい設定をスタートアップ コンフィギュレーションに保存します。</p>
ステップ 12	<pre>failover reload-standby</pre> <p>例 : <pre>active# failover reload-standby</pre></p>	<p>スタンバイ装置をリロードして新しいイメージを起動します。スタンバイ装置のロードが完了するまで待ちます。show failover コマンドを使用して、スタンバイ装置が Standby Ready 状態かどうかを検証します。</p>
ステップ 13	<pre>no failover active</pre> <p>例 : <pre>active# no failover active</pre></p>	<p>強制的にアクティブ装置からスタンバイ装置へのフェールオーバーを行います。</p>
ステップ 14	<pre>reload</pre> <p>例 : <pre>active# reload</pre></p>	<p>以前アクティブであった装置 (現在は新しいスタンバイ装置) をリロードします。リロード後にこの装置を再びアクティブにする場合は、failover active コマンドを入力します。</p>

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

これらの手順は、プライマリ装置のシステム実行スペースで実行します。

手順の詳細

	コマンド	目的
ステップ1	<pre>more system:running-config</pre> <p>例:</p> <pre>primary# more system:running-config</pre>	<p>(コンフィギュレーション移行がある場合) コンフィギュレーションをバックアップできるように、コンフィギュレーションを端末に表示します。このコマンドの出力をコピーし、テキストファイルにコンフィギュレーションを貼り付けます。</p> <p>(注) 8.3 よりも前のバージョンからアップグレードする場合は、実行コンフィギュレーションが自動的にバックアップされます。</p> <p>その他のバックアップ方法については、コンフィギュレーションガイドを参照してください。</p>
ステップ2	<pre>copy tftp://server[/path]/asa_image_name {disk0:/ disk1:/}[path/]asa_image_name</pre> <p>例:</p> <pre>primary# copy tftp://10.1.1.1/asa901-smp-k9.bin disk0:/asa901-smp-k9.bin</pre>	<p>ASA ソフトウェアをプライマリ装置のフラッシュ メモリにコピーします。TFTP 以外の方法の場合は、copy コマンドを参照してください。</p>
ステップ3	<pre>failover exec mate copy tftp://server[/path]/filename {disk0:/ disk1:/}[path/]filename</pre> <p>例:</p> <pre>primary# failover exec mate copy tftp://10.1.1.1/asa901-smp-k9.bin disk0:/asa901-smp-k9.bin</pre>	<p>ソフトウェアをセカンダリ装置にコピーします。プライマリ装置で指定したのと同じパスを指定してください。</p>
ステップ4	<pre>copy tftp://server[/path]/asdm_image_name {disk0:/ disk1:/}[path/]asdm_image_name</pre> <p>例:</p> <pre>primary# copy tftp://10.1.1.1/asdm-701.bin disk0:/asdm-701.bin</pre>	<p>ASDM イメージをプライマリ装置のフラッシュ メモリにコピーします。</p>

■ ソフトウェアのアップグレード

	コマンド	目的
ステップ 5	<pre>failover exec mate copy tftp://server[/path]/asdm_image_name {disk0:/ disk1:/}[path/]asdm_image_name</pre> <p>例:</p> <pre>primary# failover exec mate copy tftp://10.1.1.1/asdm-701.bin disk0:/asdm-701.bin</pre>	ASDM イメージをセカンダリ装置にコピーします。アクティブ装置で指定したのと同じパスを指定してください。
ステップ 6	<pre>failover group 1 active failover group 2 active</pre> <p>例:</p> <pre>primary# failover group 1 active primary# failover group 2 active</pre>	プライマリ装置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。
ステップ 7	<pre>configure terminal</pre> <p>例:</p> <pre>primary(config)# configure terminal</pre>	まだグローバル コンフィギュレーション モードを開始していない場合は、グローバル コンフィギュレーション モードを開始します。
ステップ 8	<pre>show running-config boot system</pre> <p>例:</p> <pre>hostname(config)# show running-config boot system boot system disk0:/cdisk.bin boot system disk0:/asa841-smp-k9.bin</pre>	設定されている現在のブート イメージを表示します (最大 4 個)。ASA は、表示された順序でイメージを使用します。最初のイメージが使用できない場合は次のイメージが使用され、以下同様です。新しいイメージ URL をリストの先頭に挿入することはできません。新しいイメージが先頭であることを指定するには、既存のエントリをすべて削除してから、次の手順に従ってイメージの URL を目的の順序で入力します。
ステップ 9	<pre>no boot system {disk0:/ disk1:/}[path/]asa_image_name</pre> <p>例:</p> <pre>hostname(config)# no boot system disk0:/cdisk.bin hostname(config)# no boot system disk0:/asa841-smp-k9.bin</pre>	既存のブート イメージ コンフィギュレーションがある場合は削除します。新しいブート イメージを最初の選択肢として入力できるようにするためです。
ステップ 10	<pre>boot system {disk0:/ disk1:/}[path/]asa_image_name</pre> <p>例:</p> <pre>hostname(config)# boot system disk0://asa901-smp-k9.bin</pre>	アップロードした ASA イメージを起動するように設定します。このイメージが使用できない場合に使用するバックアップ イメージに対して、このコマンドを繰り返します。たとえば、前の ステップ 9 で削除したイメージを再入力できます。
ステップ 11	<pre>asdm image {disk0:/ disk1:/}[path/]asdm_image_name</pre> <p>例:</p> <pre>hostname(config)# asdm image disk0:/asdm-701.bin</pre>	アップロードした ASDM イメージを起動するように設定します。使用するように設定できる ASDM イメージは 1 つだけであるため、最初に既存のコンフィギュレーションを削除する必要はありません。
ステップ 12	<pre>write memory</pre> <p>例:</p> <pre>primary(config)# write memory</pre>	新しい設定をスタートアップ コンフィギュレーションに保存します。

	コマンド	目的
ステップ 13	<code>failover reload-standby</code> 例： primary# failover reload-standby	セカンダリ装置をリロードして新しいイメージを起動します。 セカンダリ装置のロードが完了するまで待ちます。 show failover コマンドを使用して、両方のフェールオーバー グループが Standby Ready 状態であることを確認します。
ステップ 14	<code>no failover group 1 active</code> <code>no failover group 2 active</code> 例： primary# no failover group 1 active primary# no failover group 2 active	セカンダリ装置で、両方のフェールオーバー グループを強制的にアクティブにします。
ステップ 15	<code>reload</code> 例： primary# reload	プライマリ装置をリロードします。フェールオーバー グループは、 preempt コマンド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。フェールオーバー グループが preempt コマンドによって設定されていない場合は、 failover active group コマンドを使用して、指定された装置でそれらのステータスをアクティブ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

	コマンド	目的
ステップ 1	<code>more system:running-config</code> 例： master# more system:running-config	(コンフィギュレーション移行がある場合) コンフィギュレーション ファイルをバックアップします。このコマンドの出力をコピーし、テキスト ファイルにコンフィギュレーションを貼り付けます。 その他のバックアップ方法については、コンフィギュレーション ガイドを参照してください。
ステップ 2	<code>cluster exec copy</code> <code>tftp://server[/path]/asa_image_name</code> <code>{disk0:/ disk1:/}[path/]asa_image_name</code> 例： master# copy tftp://10.1.1.1/asa901-smp-k9.bin disk0:/asa901-smp-k9.bin	ASA ソフトウェアをクラスタ内のすべての装置にコピーします。TFTP 以外の方法の場合は、 copy コマンドを参照してください。
ステップ 3	<code>cluster exec copy</code> <code>tftp://server[/path]/asdm_image_name</code> <code>{disk0:/ disk1:/}[path/]asdm_image_name</code> 例： master# copy tftp://10.1.1.1/asdm-701.bin disk0:/asdm-701.bin	ASDM イメージをクラスタ内のすべての装置にコピーします。

■ ソフトウェアのアップグレード

	コマンド	目的
ステップ 4	<code>configure terminal</code> 例： master(config)# configure terminal	まだグローバル コンフィギュレーション モードを開始していない場合は、グローバル コンフィギュレーション モードを開始します。
ステップ 5	<code>show running-config boot system</code> 例： hostname(config)# show running-config boot system boot system disk0:/cdisk.bin boot system disk0:/asa841-smp-k9.bin	設定されている現在のブート イメージを表示します (最大 4 個)。ASA は、表示された順序でイメージを使用します。最初のイメージが使用できない場合は次のイメージが使用され、以下同様です。新しいイメージ URL をリストの先頭に挿入することはできません。新しいイメージが先頭であることを指定するには、既存のエントリをすべて削除してから、次の手順に従ってイメージの URL を目的の順序で入力します。
ステップ 6	<code>no boot system {disk0:/ disk1:/}[path/]asa_image_name</code> 例： hostname(config)# no boot system disk0:/cdisk.bin hostname(config)# no boot system disk0:/asa841-smp-k9.bin	既存のブート イメージ コンフィギュレーションがある場合は削除します。新しいブート イメージを最初の選択肢として入力できるようにするためです。
ステップ 7	<code>boot system {disk0:/ disk1:/}[path/]asa_image_name</code> 例： hostname(config)# boot system disk0://asa901-smp-k9.bin	アップロードした ASA イメージを起動するように設定します。 このイメージが使用できない場合に使用するバックアップ イメージに対して、このコマンドを繰り返します。たとえば、前の ステップ 6 で削除したイメージを再入力できます。
ステップ 8	<code>asdm image {disk0:/ disk1:/}[path/]asdm_image_name</code> 例： hostname(config)# asdm image disk0:/asdm-701.bin	アップロードした ASDM イメージを起動するように設定します。使用するように設定できる ASDM イメージは 1 つだけであるため、最初に既存のコンフィギュレーションを削除する必要はありません。
ステップ 9	<code>write memory</code> 例： master(config)# write memory	新しい設定をスタートアップ コンフィギュレーションに保存します。
ステップ 10	<code>cluster exec unit slave-unit reload noconfirm</code> 例： master# failover reload-standby	各スレーブ装置をリロードするために、各装置名に対してこのコマンドを繰り返します。接続の切断を防ぐには、各装置が再び稼働状態になるまで待ってから次の装置をリロードします。 メンバ名を一覧表示するには、 cluster exec unit ? と入力するか、 show cluster info コマンドを入力します。
ステップ 11	<code>reload noconfirm</code> 例： master# reload	マスター装置をリロードします。新しいマスターの選定が実行されて、新しいマスター装置が決定します。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。

ファイルの管理

- 「フラッシュ メモリ内のファイルの表示」 (P.85-11)
- 「フラッシュ メモリからのファイルの削除」 (P.85-11)
- 「フラッシュ ファイル システムの消去」 (P.85-12)
- 「ファイルのダウンロード」 (P.85-12)
- 「スタートアップ コンフィギュレーションまたは実行コンフィギュレーションへのファイルのダウンロード」 (P.85-13)

フラッシュ メモリ内のファイルの表示

次のように、フラッシュ メモリ内のファイルを表示して、そのファイルに関する情報を表示することもできます。

- フラッシュ メモリ内のファイルを表示するには、次のコマンドを入力します。

```
hostname# dir [disk0: | disk1:]
```

内部フラッシュ メモリの場合、**disk0:** と入力します。**disk1:** キーワードは外部フラッシュ メモリを表します。デフォルトは、内部フラッシュ メモリです。

例：

```
hostname# dir

Directory of disk0:/
500  -rw-  4958208    22:56:20 Nov 29 2004  cdisk.bin
2513 -rw-   4634      19:32:48 Sep 17 2004  first-backup
2788 -rw-   21601     20:51:46 Nov 23 2004  backup.cfg
2927 -rw-  8670632    20:42:48 Dec 08 2004  asdmfile.bin
```

- 特定のファイルに関する拡張情報を表示するには、次のコマンドを入力します。

```
hostname# show file information [path:] filename
```

デフォルトパスは、内部フラッシュ メモリのルート ディレクトリ (disk0:/) です。

例：

```
hostname# show file information cdisk.bin

disk0:/cdisk.bin:
type is image (XXX) []
file size is 4976640 bytes version 7.0(1)
```

示されているファイル サイズは例にすぎません。

フラッシュ メモリからのファイルの削除

不要になったファイルはフラッシュ メモリから削除できます。フラッシュ メモリからファイルを削除するには、次のコマンドを入力します。

```
hostname# delete disk0: filename
```

パスを指定しないと、デフォルトにより、ファイルは現在の作業ディレクトリから削除されます。ファイルを削除するときは、ワイルドカードを使用できます。削除するファイル名を求めるプロンプトが表示されます。その後、削除を確認する必要があります。

フラッシュ ファイル システムの消去

フラッシュ ファイル システムを消去するには、次の手順を実行します。

-
- ステップ 1** 「[コマンドライン ASA サービス モジュールインターフェイスへのアクセス](#)」 (P.3-2) または「[アプライアンスのコマンドライン インターフェイスへのアクセス](#)」 (P.3-1) の手順に従って、ASA のコンソール ポートに接続します。
 - ステップ 2** ASA の電源を切ってから、投入します。
 - ステップ 3** スタートアップの間に、ROMMON モードに入るようにプロンプト表示されたら、Escape キーを押します。
 - ステップ 4** 非表示のシステム ファイルを含め、すべてのファイルを上書きしてファイル システムを消去する **erase** コマンドを入力します。

```
rommon #1> erase [disk0: | disk1: | flash:]
```

ファイルのダウンロード

この項では、フラッシュ メモリにダウンロードする必要があるアプリケーション イメージ、ASDM ソフトウェア、コンフィギュレーション ファイル、またはその他のファイルをダウンロードする方法について説明します。

アプリケーション イメージ、ASDM イメージ、コンフィギュレーション ファイル、および他のファイルを TFTP、FTP、SMB、HTTP、または HTTPS サーバから内部フラッシュ メモリに、あるいは ASA の場合は外部フラッシュ メモリに、ダウンロードできます。

ガイドライン

- 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。
- 文字の大文字と小文字が異なっても、同じ名前の 2 つのファイルをフラッシュ メモリの同じディレクトリに保存できません。たとえば、**config.cfg** というファイルが存在する場所に **Config.cfg** というファイルをダウンロードしようとする、次のエラー メッセージが表示されます。

```
%Error opening disk0:/Config.cfg (File exists).
```

- Cisco SSL VPN クライアントをインストールする方法の詳細については、『*Cisco AnyConnect VPN Client Administrator Guide*』を参照してください。ASA に Cisco Secure Desktop をインストールする方法の詳細については、『*Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*』を参照してください。

- 複数のイメージがインストールされている場合、または外部フラッシュメモリにイメージがインストールされている場合に特定のアプリケーションイメージまたは ASDM イメージを使用するように ASA を設定する場合は、「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」(P.85-14) を参照してください。
- マルチ コンテキスト モードの場合は、システム実行スペース内にいる必要があります。

手順の詳細

ファイルをフラッシュメモリにダウンロードするには、各ダウンロードサーバタイプ用の次のコマンドを参照してください。

- TFTP サーバからコピーするには、次のコマンドを入力します。

```
hostname# copy tftp://server[/path]/filename {disk0:/ | disk1:/}[path/]filename
```

- FTP サーバからコピーするには、次のコマンドを入力します。

```
hostname# copy ftp://[user[:password]@]server[/path]/filename {disk0:/ | disk1:/}[path/]filename
```

- HTTP または HTTPS サーバからコピーするには、次のコマンドを入力します。

```
hostname# copy http[s]://[user[:password]@]server[:port]/[path]/filename {disk0:/ | disk1:/}[path/]filename
```

- SMB サーバからコピーするには、次のコマンドを入力します。

```
hostname# copy smb://[user[:password]@]server[/path]/filename {disk0:/ | disk1:/}[path/]filename
```

- セキュアコピーを使用するには、最初にセキュアシェル (SSH) をイネーブルにし、次のコマンドを入力します。

```
hostname# ssh scopy enable
```

その後、Linux クライアントから次のコマンドを入力します。

```
scp -v -pw password filename username@asa_address
```

-v は冗長を表します。-pw が指定されていない場合は、パスワードの入力を求めるプロンプトが表示されます。

スタートアップ コンフィギュレーションまたは実行コンフィギュレーションへのファイルのダウンロード

テキストファイルは、TFTP、FTP、SMB、または HTTP (S) サーバから、またはフラッシュメモリから、実行コンフィギュレーションまたはスタートアップ コンフィギュレーションにダウンロードできます。

スタートアップ コンフィギュレーションとして特定のコンフィギュレーションを使用するように ASA を設定する場合は、「スタートアップ コンフィギュレーションとしてブートするファイルの設定」(P.85-15) を参照してください。

ガイドライン

コンフィギュレーションを実行コンフィギュレーションにコピーするには、2つのコンフィギュレーションをマージします。マージによって、新しいコンフィギュレーションから実行コンフィギュレーションに新しいコマンドが追加されます。コンフィギュレーションが同じ場合、変更は発生しません。コマンドが衝突する場合、またはコマンドがコンテキストの実行に影響を与える場合、マージの結果はコマンドによって異なります。エラーが発生することも、予期できない結果が生じることもあります。

手順の詳細

スタートアップ コンフィギュレーションまたは実行コンフィギュレーションにファイルをコピーするには、適切なダウンロード サーバに対して次のコマンドのいずれかを入力します。

- TFTP サーバからコピーするには、次のコマンドを入力します。

```
hostname# copy tftp://server[/path]/filename {startup-config | running-config}
```

- FTP サーバからコピーするには、次のコマンドを入力します。

```
hostname# copy ftp://[user[:password]@]server[/path]/filename {startup-config | running-config}
```

- HTTP または HTTPS サーバからコピーするには、次のコマンドを入力します。

```
hostname# copy http[s]://[user[:password]@]server[:port][/path]/filename {startup-config | running-config}
```

- SMB サーバからコピーするには、次のコマンドを入力します。

```
hostname# copy smb://[user[:password]@]server[/path]/filename {startup-config | running-config}
```

- フラッシュ メモリからコピーするには、次のコマンドを入力します。

```
hostname# copy {disk0:/ | disk1:/}[path/]filename {startup-config | running-config}
```

たとえば、TFTP サーバからコンフィギュレーションをコピーするには、次のコマンドを入力します。

```
hostname# copy tftp://209.165.200.226/configs/startup.cfg startup-config
```

FTP サーバからコンフィギュレーションをコピーするには、次のコマンドを入力します。

```
hostname# copy ftp://admin:letmein@209.165.200.227/configs/startup.cfg startup-config
```

HTTP サーバからコンフィギュレーションをコピーするには、次のコマンドを入力します。

```
hostname# copy http://209.165.200.228/configs/startup.cfg startup-config
```

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 メモリ内を検索されます。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に、インストールされているイメージが 1 つしかなくても、実行コンフィギュレーションに ASA によって **asdm image** コマンドが挿入さ

れます。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。

- 「使用する ASA および ASDM のイメージを設定する」(P.85-15)
- 「スタートアップ コンフィギュレーションとしてブートするファイルの設定」(P.85-15)

使用する ASA および ASDM のイメージを設定する

ブートするアプリケーション イメージを設定するには、次のコマンドを入力します。

```
hostname(config)# boot system url
```

ここで、*url* は次のいずれかです。

- `{disk0:/ | disk1:/}[path/]filename`
- `tftp://[user[:password]@]server[:port]/[path/]filename`



(注) TFTP オプションは、すべてのモデルでサポートされるわけではありません。

最大 4 つの **boot system** コマンド エントリを入力して、複数のイメージをブートする順番に指定することができます。ASA は、最初に検出に成功したイメージをブートします。**boot system** コマンドを入力すると、エントリがリストの最後に追加されます。ブート エントリの順序を変更するには、**clear configure boot system** コマンドを使用してすべてのエントリを削除してから、エントリを目的の順序で再入力する必要があります。設定できる **boot system tftp** コマンドは 1 つだけです。これは、最初に設定する必要があります。



(注) ASA が連続ブートのサイクルから抜け出せない場合は、ASA を ROMMON モードにリポートします。ROMMON モードの詳細については、「デバッグ メッセージの表示」(P.86-1) を参照してください。

ブートする ASDM イメージを設定するには、次のコマンドを入力します。

```
hostname(config)# asdm image {disk0:/ | disk1:/}[path/]filename
```

スタートアップ コンフィギュレーションとしてブートするファイルの設定

デフォルトでは、ASA は、隠しファイルであるスタートアップ コンフィギュレーションからブートします。あるいは、次のコマンドを入力して、任意のコンフィギュレーションをスタートアップ コンフィギュレーションとして設定することもできます。

```
hostname(config)# boot config {disk0:/ | disk1:/}[path/]filename
```

イメージをロードするための ROM モニタの使用

- 「ASA 5500 シリーズに対する ROM モニタの使用」(P.85-16)
- 「ASASM に対する ROM モニタの使用」(P.85-17)

ASA 5500 シリーズに対する ROM モニタの使用

TFTP を使用して ROM モニタ モードから ASA へソフトウェア イメージをロードするには、次の手順を実行します。

- ステップ 1** 「[アプライアンスのコマンドライン インターフェイスへのアクセス](#)」(P.3-1) に従って、ASA のコンソール ポートに接続します。
- ステップ 2** ASA の電源を切ってから、投入します。
- ステップ 3** スタートアップの間に、ROMMON モードに入るようにプロンプト表示されたら、Escape キーを押します。
- ステップ 4** ROMMON モードで、IP アドレス、TFTP サーバアドレス、ゲートウェイ アドレス、ソフトウェア イメージ ファイル、およびポートを含む、ASA に対するインターフェイス設定を次のように定義します。

```
rommon #1> ADDRESS=10.132.44.177
rommon #2> SERVER=10.129.0.30
rommon #3> GATEWAY=10.132.44.1
rommon #4> IMAGE=f1/asa800-232-k8.bin
rommon #5> PORT=Ethernet0/0
Ethernet0/0
Link is UP
MAC Address: 0012.d949.15b8
```



(注) ネットワークへの接続がすでに存在することを確認してください。

- ステップ 5** 設定を検証するには、**set** コマンドを入力します。

```
rommon #6> set
ROMMON Variable Settings:
ADDRESS=10.132.44.177
SERVER=10.129.0.30
GATEWAY=10.132.44.1
PORT=Ethernet0/0
VLAN=untagged
IMAGE=f1/asa840-232-k8.bin
CONFIG=
LINKTIMEOUT=20
PKTTIMEOUT=4
RETRY=20
```

- ステップ 6** **ping server** コマンドを入力して、TFTP サーバを ping します。

```
rommon #7> ping server
Sending 20, 100-byte ICMP Echoes to server 10.129.0.30, timeout is 4 seconds:

Success rate is 100 percent (20/20)
```

- ステップ 7** **tftp** コマンドを入力して、ソフトウェア イメージをロードします。

```
rommon #8> tftp
ROMMON Variable Settings:
ADDRESS=10.132.44.177
SERVER=10.129.0.30
GATEWAY=10.132.44.1
PORT=Ethernet0/0
VLAN=untagged
IMAGE=f1/asa840-232-k8.bin
CONFIG=
LINKTIMEOUT=20
```



```

PKTTIMEOUT=4
RETRY=20

tftp f1/asa840-232-k8.bin@10.129.0.30 via 10.132.44.1

Received 14450688 bytes

Launching TFTP Image...
Cisco ASA Security Appliance admin loader (3.0) #0: Mon Mar 5 16:00:07 MST 2011

```

```
Loading...N
```

ソフトウェア イメージが正常にロードされると、ASA は自動的に ROMMON モードを終了します。

- ステップ 8** 正しいソフトウェア イメージが ASA にロードされたことを検証するには、次のコマンドを入力して、ASA 内のバージョンを確認します。

```
hostname# show version
```

ASASM に対する ROM モニタの使用

TFTP を使用して ROM モニタ モードから ASASM へソフトウェア イメージをロードするには、次の手順を実行します。

- ステップ 1** 「[コマンドライン ASA サービス モジュールインターフェイスへのアクセス](#)」(P.3-2) に従って、ASA のコンソール ポートに接続します。
- ステップ 2** ASASM イメージをリロードすることを確認します。
- ステップ 3** スタートアップの間に、ROMMON モードに入るようにプロンプト表示されたら、**Escape** キーを押します。
- ステップ 4** ROMMON モードで、IP アドレス、TFTP サーバアドレス、ゲートウェイ アドレス、ソフトウェア イメージファイル、ポートおよび VLAN を含む、ASASM に対するインターフェイス設定を次のように定義します。

```

rommon #1> ADDRESS=172.16.145.149
rommon #2> SERVER=172.16.171.125
rommon #3> GATEWAY=172.16.145.129
rommon #4> IMAGE=f1/asa851-smp-k8.bin
rommon #5> PORT=Data0
rommon #6> VLAN=1
Data0
Link is UP
MAC Address: 0012.d949.15b8

```



(注) ネットワークへの接続がすでに存在することを確認してください。

- ステップ 5** 設定を検証するには、**set** コマンドを入力します。

```

rommon #7> set
ROMMON Variable Settings:
ADDRESS=172.16.145.149
SERVER=172.16.171.125
GATEWAY=172.16.145.129
PORT=Data0
VLAN=1
IMAGE=f1/asa851-smp-k8.bin
CONFIG=

```

■ コンフィギュレーションまたはその他のファイルのバックアップ

```
LINKTIMEOUT=20
PKTTIMEOUT=2
RETRY=20
```

ステップ 6 ping server コマンドを入力して、TFTP サーバを ping します。

```
rommon #8> ping server
Sending 20, 100-byte ICMP Echoes to server 172.16.171.125, timeout is 2 seconds:

Success rate is 100 percent (20/20)
```

ステップ 7 tftp コマンドを入力して、ソフトウェア イメージをロードします。

```
rommon #9> tftp
Clearing EOBC receive queue ...
cmostime_set = 1
ROMMON Variable Settings:
ADDRESS=172.16.145.149
SERVER=172.16.171.125
GATEWAY=172.16.145.129
PORT=Data0
VLAN=1
IMAGE=f1/asa851-smp-k8.bin
CONFIG=
LINKTIMEOUT=20
PKTTIMEOUT=2
RETRY=20

tftp f1/asa851-smp-k8.bin@172.16.171.125 via 172.16.145.129
Starting download.Press ESC to abort.
```

ソフトウェア イメージが正常にロードされると、ASASM は自動的に ROMMON モードを終了します。



(注) ROMMON のブート完了後に、システム フラッシュにイメージを個別にダウンロードする必要があります。ROMMON モードにモジュールをブートすると、リロード時にシステム イメージが維持されません。

ステップ 8 正しいソフトウェア イメージが ASASM にロードされたことを検証するには、次のコマンドを入力して、バージョンを確認します。

```
hostname# show version
```

コンフィギュレーションまたはその他のファイルのバックアップ

- 「シングル モード コンフィギュレーションまたはマルチ モード システム コンフィギュレーションのバックアップ」 (P.85-19)
- 「フラッシュ メモリ内のコンテキスト コンフィギュレーションまたはその他のファイルのバックアップ」 (P.85-19)
- 「コンテキスト内でのコンテキスト コンフィギュレーションのバックアップ」 (P.85-20)
- 「端末の表示からのコンフィギュレーションのコピー」 (P.85-20)

- 「[export および import コマンドを使用した追加ファイルのバックアップ](#)」 (P.85-20)
- 「[スクリプトを使用したファイルのバックアップおよび復元](#)」 (P.85-21)

シングル モード コンフィギュレーションまたはマルチ モード システム コンフィギュレーションのバックアップ

シングル コンテキスト モードで、またはマルチモードのシステム コンフィギュレーションから、スタートアップ コンフィギュレーションまたは実行コンフィギュレーションを外部サーバまたはローカル フラッシュ メモリにコピーできます。

- TFTP サーバにコピーするには、次のコマンドを入力します。

```
hostname# copy {startup-config | running-config} tftp://server[/path]/filename
```

- FTP サーバにコピーするには、次のコマンドを入力します。

```
hostname# copy {startup-config | running-config}
ftp://[user[:password]@]server[/path]/filename
```

- ローカル フラッシュ メモリにコピーするには、次のコマンドを入力します。

```
hostname# copy {startup-config | running-config} {flash:/ | disk0:/ |
disk1:/}[/path]/filename
```



(注) 宛先ディレクトリが存在することを確認してください。存在しない場合は、まず **mkdir** コマンドを使用してディレクトリを作成します。

フラッシュ メモリ内のコンテキスト コンフィギュレーションまたはその他のファイルのバックアップ

システム実行スペースで次のいずれかのコマンドを入力することによって、ローカル フラッシュ メモリにあるコンテキスト コンフィギュレーションまたは他のファイルをコピーします。

- TFTP サーバにコピーするには、次のコマンドを入力します。

```
hostname# copy disk{0 | 1}:[/path]/filename tftp://server[/path]/filename
```

- FTP サーバにコピーするには、次のコマンドを入力します。

```
hostname# copy disk{0 | 1}:[/path]/filename
ftp://[user[:password]@]server[/path]/filename
```

- SMB ファイル システムからコピーするには、次のコマンドを入力します。

```
hostname# copy disk{0 | 1}:[/path]/filename
smb://[user[:password]@]server[/path]/filename
```

- HTTPS を使用して ASA からコピーするには、ブラウザで次の URL を入力します。

```
https://ASA_IP/disk{0 | 1}/filename
```

- ローカル フラッシュ メモリにコピーするには、次のコマンドを入力します。

```
hostname# copy disk{0 | 1}:[/path]/filename disk{0 | 1}:[/path]/newfilename
```



(注) 宛先ディレクトリが存在することを確認してください。存在しない場合は、まず **mkdir** コマンドを使用してディレクトリを作成します。

コンテキスト内でのコンテキスト コンフィギュレーションのバックアップ

マルチ コンテキスト モードでは、コンテキスト内から次のバックアップを実行できます。

- (admin コンテキストに接続された) スタートアップ コンフィギュレーション サーバに実行コンフィギュレーションをコピーするには、次のコマンドを入力します。

```
hostname/contexta# copy running-config startup-config
```

- コンテキスト ネットワークに接続された TFTP サーバに実行コンフィギュレーションをコピーするには、次のコマンドを入力します。

```
hostname/contexta# copy running-config tftp:/server[/path]/filename
```

端末の表示からのコンフィギュレーションのコピー

コンフィギュレーションを端末に表示するには、次のコマンドを入力します。

```
hostname# show running-config
```

コマンドから出力をコピーして、コンフィギュレーションをテキスト ファイルに貼り付けます。

export および import コマンドを使用した追加ファイルのバックアップ

コンフィギュレーションに欠かせない追加ファイルは次のとおりです。

- **import webvpn** コマンドを使用してインポートするファイル。現在これらのファイルには、カスタマイゼーション、URL リスト、Web コンテンツ、プラグイン、および言語翻訳などがあります。
- DAP ポリシー (dap.xml)。
- CSD コンフィギュレーション (data.xml)。
- デジタル キーおよびデジタル証明書。
- ローカル CA ユーザ データベース ファイルと証明書ステータス ファイル。

CLI では、**export** コマンドと **import** コマンドを使用して、コンフィギュレーションの個々の要素をバックアップおよび復元できます。

たとえば **import webvpn** コマンドを使用してインポートしたこれらのファイル、または証明書をバックアップするには、次の手順を実行します。

ステップ 1 次のように、適用可能な **show** コマンドを実行します。

```
hostname # show import webvpn plug-in
ica
rdp
ssh, telnet
vnc
```

ステップ 2 バックアップするファイルに対して **export** コマンドを発行します (この例では rdp ファイルです)。

```
hostname # export webvpn plug-in protocol rdp tftp://tftpserver/backupfilename
```

スクリプトを使用したファイルのバックアップおよび復元

スクリプトを使用して、ASA のコンフィギュレーション ファイルをバックアップおよび復元できません。これには、**import webvpn CLI** によってインポートする拡張機能のすべて、CSD コンフィギュレーションの XML ファイル、および DAP コンフィギュレーションの XML ファイルが含まれます。セキュリティ上の理由により、デジタル キーと証明書、またはローカル CA キーの自動バックアップを実行することはお勧めしません。

この項では、自動バックアップの手順について説明します。また、そのまま使用することも、環境要件に合わせて修正することもできるサンプル スクリプトを示します。サンプル スクリプトは Linux システムに固有のスクリプトです。Microsoft Windows システムで使用するには、サンプルのロジックを使用して修正する必要があります。



(注)

既存の CLI では、**copy**、**export**、および **import** コマンドを使用して個々のファイルをバックアップおよび復元できます。ただし、1 回の操作ですべての ASA コンフィギュレーション ファイルをバックアップする機能はありません。スクリプトを実行すると、複数の CLI を使用できます。

この項は、次の内容で構成されています。

- 「前提条件」(P.85-21)
- 「スクリプトの実行」(P.85-21)
- 「サンプル スクリプト」(P.85-22)

前提条件

スクリプトを使用して ASA コンフィギュレーションをバックアップおよび復元するには、まず次の作業を実行します。

- Expect モジュールとともに Perl をインストールする。
- ASA に到達可能な SSH クライアントをインストールする。
- TFTP サーバをインストールして、ASA からバックアップ サイトにファイルを送信する。

別の選択肢としては、市販のツールを使用します。このスクリプトのロジックをそれらのツールに取り入れることができます。

スクリプトの実行

バックアップおよび復元のスクリプトを実行するには、次の手順を実行します。

- ステップ 1** システムの任意の場所に、スクリプト ファイルをダウンロードまたはカットアンドペーストします。
- ステップ 2** コマンドラインで、**Perl scriptname** と入力します。*scriptname* はスクリプト ファイルの名前です。
- ステップ 3** Enter を押します。
- ステップ 4** オプションごとに値を入力するように、プロンプトが表示されます。あるいは、**Perl scriptname** コマンドを入力するときにオプションの値を入力してから、Enter を押すことができます。どちらの方法でも、スクリプトによりオプションごとに値を入力するよう求められます。

- ステップ 5** このスクリプトが実行され、発行されるコマンドが出力されます。この出力は CLI の記録となります。これらの CLI は後で行われる復元に使用できます。特に、ファイルを 1 つまたは 2 つだけ復元する場合に便利です。

サンプル スクリプト

```
#!/usr/bin/perl
#Function: Backup/restore configuration/extensions to/from a TFTP server.
#Description: The objective of this script is to show how to back up
configurations/extensions before the backup/restore command is developed.
# It currently backs up the running configuration, all extensions imported via "import
webvpn" command, the CSD configuration XML file, and the DAP configuration XML file.
#Requirements: Perl with Expect, SSH to the ASA, and a TFTP server.
#Usage: backupasa -option option_value
#       -h: ASA hostname or IP address
#       -u: User name to log in via SSH
#       -w: Password to log in via SSH
#       -e: The Enable password on the security appliance
#       -p: Global configuration mode prompt
#       -s: Host name or IP address of the TFTP server to store the configurations
#       -r: Restore with an argument that specifies the file name.This file is produced
during backup.
#If you don't enter an option, the script will prompt for it prior to backup.
#
#Make sure that you can SSH to the ASA.

use Expect;
use Getopt::Std;

#global variables
%options=();
$restore = 0; #does backup by default
$restore_file = '';
$sasa = '';
$storage = '';
$user = '';
$password = '';
$enable = '';
$prompt = '';
$date = `date +%F`;
chop($date);
my $exp = new Expect();

getopts("h:u:p:w:e:s:r:", \%options);
do process_options();

do login($exp);
do enable($exp);
if ($restore) {
    do restore($exp,$restore_file);
}
else {
    $restore_file = "$prompt-restore-$date.cli";
    open(OUT,">$restore_file") or die "Can't open $restore_file\n";
    do running_config($exp);
    do lang_trans($exp);
    do customization($exp);
    do plugin($exp);
    do url_list($exp);
    do webcontent($exp);
}
```

```

do dap($exp);
do csd($exp);
close(OUT);
}
do finish($exp);

sub enable {
    $obj = shift;
    $obj->send("enable\n");
    unless ($obj->expect(15, 'Password:')) {
        print "timed out waiting for Password:\n";
    }
    $obj->send("$enable\n");
    unless ($obj->expect(15, "$prompt#")) {
        print "timed out waiting for $prompt#\n";
    }
}

sub lang_trans {
    $obj = shift;
    $obj->clear_accum();
    $obj->send("show import webvpn translation-table\n");
    $obj->expect(15, "$prompt#" );
    $output = $obj->before();
    @items = split(/\n+/, $output);

    for (@items) {
        s/^\s+//;
        s/\s+$//;
        next if /show import/ or /Translation Tables/;
        next unless (/^.+\s+.$/);
        ($lang, $transtable) = split(/\s+/, $_);
        $cli = "export webvpn translation-table $transtable language $lang
$storage/$prompt-$date-$transtable-$lang.po";
        $ocli = $cli;
        $ocli =~ s/^export/import/;
        print "$cli\n";
        print OUT "$ocli\n";
        $obj->send("$ocli\n");
        $obj->expect(15, "$prompt#" );
    }
}

sub running_config {
    $obj = shift;
    $obj->clear_accum();
    $cli = "copy /noconfirm running-config $storage/$prompt-$date.cfg";
    print "$cli\n";
    $obj->send("$cli\n");
    $obj->expect(15, "$prompt#" );
}

sub customization {
    $obj = shift;
    $obj->clear_accum();
    $obj->send("show import webvpn customization\n");
    $obj->expect(15, "$prompt#" );
    $output = $obj->before();
    @items = split(/\n+/, $output);

    for (@items) {
        chop;
        next if /^Template/ or /show import/ or /\s*$/;
    }
}

```

```

    $cli = "export webvpn customization $_ $storage/$prompt-$date-cust-$_.xml";
    $ocli = $cli;
    $ocli =~ s/^export/import/;
    print "$cli\n";
    print OUT "$ocli\n";
    $obj->send("$cli\n");
    $obj->expect(15, "$prompt#" );
}
}

sub plugin {
    $obj = shift;
    $obj->clear_accum();
    $obj->send("show import webvpn plug-in\n");
    $obj->expect(15, "$prompt#" );
    $output = $obj->before();
    @items = split(/\n+/, $output);

    for (@items) {
        chop;
        next if /^Template/ or /show import/ or /\s*$/;
        $cli = "export webvpn plug-in protocol $_ $storage/$prompt-$date-plugin-$_.jar";
        $ocli = $cli;
        $ocli =~ s/^export/import/;
        print "$cli\n";
        print OUT "$ocli\n";
        $obj->send("$cli\n");
        $obj->expect(15, "$prompt#" );
    }
}

sub url_list {
    $obj = shift;
    $obj->clear_accum();
    $obj->send("show import webvpn url-list\n");
    $obj->expect(15, "$prompt#" );
    $output = $obj->before();
    @items = split(/\n+/, $output);

    for (@items) {
        chop;
        next if /^Template/ or /show import/ or /\s*$/ or /No bookmarks/;
        $cli="export webvpn url-list $_ $storage/$prompt-$date-urllist-$_.xml";
        $ocli = $cli;
        $ocli =~ s/^export/import/;
        print "$cli\n";
        print OUT "$ocli\n";
        $obj->send("$cli\n");
        $obj->expect(15, "$prompt#" );
    }
}

sub dap {
    $obj = shift;
    $obj->clear_accum();
    $obj->send("dir dap.xml\n");
    $obj->expect(15, "$prompt#" );

    $output = $obj->before();
    return 0 if($output =~ /Error/);

    $cli="copy /noconfirm dap.xml $storage/$prompt-$date-dap.xml";
    $ocli="copy /noconfirm $storage/$prompt-$date-dap.xml disk0:/dap.xml";
    print "$cli\n";
}

```



```

    print OUT "$ocli\n";
    $obj->send("$cli\n");
    $obj->expect(15, "$prompt#" );
}

sub csd {
    $obj = shift;
    $obj->clear_accum();
    $obj->send("dir sdesktop\n");
    $obj->expect(15, "$prompt#" );

    $output = $obj->before();
    return 0 if($output =~ /Error/);

    $cli="copy /noconfirm sdesktop/data.xml $storage/$prompt-$date-data.xml";
    $ocli="copy /noconfirm $storage/$prompt-$date-data.xml disk0:/sdesktop/data.xml";
    print "$cli\n";
    print OUT "$ocli\n";
    $obj->send("$cli\n");
    $obj->expect(15, "$prompt#" );
}

sub webcontent {
    $obj = shift;
    $obj->clear_accum();
    $obj->send("show import webvpn webcontent\n");
    $obj->expect(15, "$prompt#" );
    $output = $obj->before();
    @items = split(/\n+/, $output);

    for (@items) {
        s/^\s+//;
        s/\s+$//;
        next if /show import/ or /No custom/;
        next unless (/^.+s+.+$/);
        ($url, $type) = split(/\s+/, $_);
        $turl = $url;
        $turl =~ s/\/\+//;
        $turl =~ s/\+\/-//;
        $cli = "export webvpn webcontent $url $storage/$prompt-$date-$turl";
        $ocli = $cli;
        $ocli =~ s/^export/import/;
        print "$cli\n";
        print OUT "$ocli\n";
        $obj->send("$cli\n");
        $obj->expect(15, "$prompt#" );
    }
}

sub login {
    $obj = shift;
    $obj->raw_pty(1);
    $obj->log_stdout(0); #turn off console logging.
    $obj->spawn("/usr/bin/ssh $user@$asa") or die "can't spawn ssh\n";
    unless ($obj->expect(15, "password:")) {
        die "timeout waiting for password:\n";
    }

    $obj->send("$password\n");

    unless ($obj->expect(15, "$prompt>")) {
        die "timeout waiting for $prompt>\n";
    }
}
}

```

```
sub finish {
    $obj = shift;
    $obj->hard_close();
    print "\n\n";
}

sub restore {
    $obj = shift;
    my $file = shift;
    my $output;
    open(IN,"$file") or die "can't open $file\n";
    while (<IN>) {
        $obj->send("$_");
        $obj->expect(15, "$prompt#" );
        $output = $obj->before();
        print "$output\n";
    }
    close(IN);
}

sub process_options {
    if (defined($options{s})) {
        $tstr= $options{s};
        $storage = "tftp://$tstr";
    }
    else {
        print "Enter TFTP host name or IP address:";
        chop($tstr=<>);
        $storage = "tftp://$tstr";
    }
    if (defined($options{h})) {
        $asa = $options{h};
    }
    else {
        print "Enter ASA host name or IP address:";
        chop($asa=<>);
    }

    if (defined ($options{u})) {
        $user= $options{u};
    }
    else {
        print "Enter user name:";
        chop($user=<>);
    }

    if (defined ($options{w})) {
        $password= $options{w};
    }
    else {
        print "Enter password:";
        chop($password=<>);
    }
    if (defined ($options{p})) {
        $prompt= $options{p};
    }
    else {
        print "Enter ASA prompt:";
        chop($prompt=<>);
    }
    if (defined ($options{e})) {
        $enable = $options{e};
    }
}
```

```

}
else {
    print "Enter enable password:";
    chop($enable=<>);
}

if (defined ($options{r})) {
    $restore = 1;
    $restore_file = $options{r};
}
}

```

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.85-27)
- 「[ダウングレードの実行](#)」 (P.85-28)

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ります。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

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 次のコマンドを入力します。

```
hostname(config)# downgrade [/noconfirm] old_image_url old_config_url [activation-key
old_key]
```

/noconfirm オプションを指定すると、プロンプトは表示されずにダウングレードされます。*image_url* は、disk0、disk1、tftp、ftp、または smb 上の古いイメージへのパスです。*old_config_url* は、保存されている移行前の設定へのパスです（デフォルトでは、この設定は disk0 に保存されます）。8.3 よりも前のアクティベーション キーに戻る必要がある場合は、そのアクティベーション キーを入力できます。

このコマンドは、次の機能を完了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**)。

たとえば、次のように入力します。

```
hostname(config)# downgrade /noconfirm disk0:/asa821-k8.bin disk0:/8_2_1_0_startup_cfg.sav
```

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.85-29)
- 「Auto Update サーバとの通信の設定」 (P.85-29)
- 「Auto Update サーバとしてのクライアントアップデートの設定」 (P.85-31)
- 「Auto Update ステータスの表示」 (P.85-32)

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。

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。

Auto Update は、次のような、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、基本的な監視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。

注意事項と制限事項

- 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

ASA を Auto Update クライアントとして設定するには、次の手順を実行します。

ステップ 1 Auto Update サーバの URL を指定するには、次のコマンドを入力します。

```
hostname (config) # auto-update server url [source interface] [verify-certificate]
```

ここで、*url* には次の構文があります。

```
http[s]://[user:password@]server_ip[:port]/pathname
```

https を指定すると、SSL が使用されます。URL の *user* 引数と *password* 引数は、サーバにログインするときの基本認証に使用されます。**write terminal**、**show configuration**、または **show tech-support** コマンドを使用してコンフィギュレーションを表示した場合、ユーザとパスワードは「*****」に置換されます。

HTTP のデフォルトポートは 80、HTTPS のデフォルトポートは 443 です。

source interface キーワードおよび引数は、Auto Update サーバに要求を送信するときに使用するインターフェイスを指定します。**management-access** コマンドで指定したインターフェイスと同じインターフェイスを指定すると、Auto Update 要求は管理アクセスに使用されるのと同じ IPsec VPN トンネルを通過します。

verify-certificate キーワードは、Auto Update サーバによって戻される証明書を確認します。

ステップ 2 (任意) Auto Update サーバと通信する際に送信するデバイス ID を識別するには、次のコマンドを入力します。

```
hostname(config)# auto-update device-id {hardware-serial | hostname | ipaddress [if-name] | mac-address [if-name] | string text}
```

使用する ID は、次のいずれかのパラメータによって決まります。

- **hardware-serial** 引数は、ASA のシリアル番号を指定します。
- **hostname** 引数は、ASA のホスト名を指定します。
- **ipaddress** キーワードは、指定のインターフェイスの IP アドレスを指定します。インターフェイス名を指定しない場合、Auto Update サーバとの通信に使用するインターフェイスの IP アドレスが使用されます。
- **mac-address** キーワードは、指定のインターフェイスの MAC アドレスを指定します。インターフェイス名を指定しない場合、Auto Update サーバとの通信に使用するインターフェイスの MAC アドレスが使用されます。
- **string** キーワードは、指定のテキスト識別子を指定します。空白や '、"、>、&、? は使用できません。

ステップ 3 (任意) コンフィギュレーション、またはイメージのアップデートを要求するために Auto Update サーバにポーリングする回数を指定するには、次のコマンドを入力します。

```
hostname(config)# auto-update poll-period poll-period [retry-count [retry-period]]
```

poll-period 引数は、更新を確認する間隔 (分単位) を指定します。デフォルトは 720 分 (12 時間) です。

retry-count 引数は、サーバへの最初の接続に失敗した場合に、再試行する回数を指定します。デフォルトは 0 です。

retry-period 引数は、リトライの間の待機時間 (分単位) を指定します。デフォルトは 5 分です。

ステップ 4 (任意) ASA から Auto Update サーバにポーリングする特定の時刻をスケジュールするには、次のコマンドを入力します。

```
hostname(config)# auto-update poll-at days-of-the-week time [randomize minutes] [retry_count [retry_period]]
```

days-of-the-week 引数は、Monday、Tuesday、Wednesday、Thursday、Friday、Saturday、および Sunday の中の任意の曜日または曜日の組み合わせです。それ以外に、**daily** (月曜日から日曜日)、**weekdays** (月曜日から金曜日)、および **weekend** (土曜日と日曜日) の値が設定可能です。

time 引数は、ポーリングの開始時刻を HH:MM 形式で指定します。たとえば、8:00 は午前 8 時です。午後 8 時は 20:00 と指定します。

randomize minutes キーワードおよび引数は、指定した開始時刻に続いてポーリングをランダムに実行する期間を指定します。範囲は 1 ~ 1439 分です。

retry_count 引数は、最初の接続に失敗したときに、Auto Update サーバへの再接続を試みる回数を指定します。デフォルトは 0 です。

retry_period 引数は、接続の試行から次の試行までの待機時間を指定します。デフォルトは 5 分です。範囲は 1 ~ 35791 分です。

ステップ 5 (オプション) Auto Update サーバに一定期間アクセスがなかった場合にトラフィックの通過を中断するには、次のコマンドを入力します。

```
hostname(config)# auto-update timeout period
```

period 引数は、1 ~ 35791 の範囲で分単位のタイムアウト期間を指定します。デフォルトはタイムアウトなし (0 分) です。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

最新のイメージとコンフィギュレーションが ASA にあることを確認するには、**auto-update timeout** コマンドを使用します。この状態は、システム ログ メッセージ 201008 で報告されます。

次の例では、ASA が外部インターフェイスから証明書の検証付きで、IP アドレス 209.165.200.224、ポート番号 1742 で Auto Update サーバをポーリングするように設定されています。

また、ASA は、デバイス ID としてホスト名を使用し、Auto Update サーバへのポーリングを毎週金曜日と土曜日の 10:00 p.m から 11:00 p.m. の間の任意の時刻に実行するように設定されます。次の例のように、ポーリングに失敗した場合は、ASA によって Auto Update サーバへの再接続が 10 回試みられます。再接続と再接続の間は、3 分間の待機時間が設定されます。

```
hostname(config)# auto-update server
https://jcrichton:farscape@209.165.200.224:1742/management source outside
verify-certificate
hostname (config)# auto-update device-id hostname
hostname (config)# auto-update poll-at Friday Saturday 22:00 randomize 60 2 10
```

Auto Update サーバとしてのクライアント アップデートの設定

client-update コマンドを入力すると、Auto Update クライアントとして設定された ASA のアップデートがイネーブルになり、ソフトウェア コンポーネントのタイプ (ASDM またはブート イメージ)、ASA のタイプまたはファミリー、アップデートが適用されるリビジョン番号、アップデートを取得した URL または IP アドレスを指定できるようになります。

ASA を Auto Update サーバとして設定するには、次の手順を実行します。

ステップ 1 クライアント アップデートをイネーブルにするには、次のコマンドを入力します。

```
hostname(config)# client-update enable
```

ステップ 2 ASA に適用する **client-update** コマンドに、次のパラメータを設定します。

```
client-update {component {asdm | image} | device-id dev_string |
family family_name | type type} url url-string rev-nums rev-nums}
```

component {asdm | image} パラメータは、ASDM または ASA のブート イメージのいずれかをソフトウェア コンポーネントとして指定します。

device-id dev_string パラメータは、Auto Update クライアントが自身を識別するために使用する固有の文字列を指定します。最大長は 63 文字です。

family *family_name* パラメータは、Auto Update クライアントが自身を識別するために使用するファミリー名を指定します。asa、pix、または 7 文字以内のテキスト文字列を指定します。

rev-nums *rev-nums* パラメータは、このクライアントのソフトウェアまたはファームウェアイメージを指定します。最大 4 個のイメージを、任意の順序でカンマで区切って指定します。

type *type* パラメータは、クライアントアップデートを通知するクライアントのタイプを指定します。このコマンドは、Windows クライアントのアップデートでも使用されるため、クライアントのリストには Windows オペレーティングシステムも複数含まれています。リストに含まれる ASA には、次のようなものがあります。

- asa5505: Cisco 5505 ASA
- asa5510: Cisco 5510 ASA
- asa5520: Cisco 5520 ASA
- asa5540: Cisco 5540 ASA

url *url-string* パラメータは、ソフトウェア/ファームウェアイメージの URL を指定します。この URL は、クライアントに適合するファイルを指している必要があります。すべての Auto Update クライアントには、URL のプレフィックスとして「http://」または「https://」プロトコルを使用する必要があります。

特定のタイプの ASA すべてに適用するクライアントアップデートのパラメータを設定します。つまり、ASA のタイプと、アップデートされたイメージの取得元 URL または IP アドレスを指定します。また、リビジョン番号も指定する必要があります。リモートの ASA のリビジョン番号が、指定したリビジョン番号の 1 つと一致する場合は、クライアントのアップデートは不要です。アップデートは無視されます。

Cisco 5520 ASA にクライアントアップデートを設定するには、次のコマンドを入力します。

```
hostname(config)# client-update type asa5520 component asdm url
http://192.168.1.114/aus/asdm601.bin rev-nums 8.0(1)
```

Auto Update ステータスの表示

Auto Update のステータスを表示するには、次のコマンドを入力します。

```
hostname(config)# show auto-update
```

次に、**show auto-update** コマンドの出力例を示します。

```
hostname(config)# show auto-update
```

```
Server: https://*****@209.165.200.224:1742/management.cgi?1276
Certificate will be verified
Poll period: 720 minutes, retry count: 2, retry period: 5 minutes
Timeout: none
Device ID: host name [corporate]
Next poll in 4.93 minutes
Last poll: 11:36:46 PST Tue Nov 13 2004
Last PDM update: 23:36:46 PST Tue Nov 12 2004
```