CHAPTER 41

ソフトウェア、ライセンス、および設定の管理

この章では、セキュリティ アプライアンスのソフトウェア、ライセンス、およびコンフィギュレーションの管理について説明します。この章では、次の項目について説明します。

ライセンスの管理

ソフトウェアをインストールすると、元のイメージから既存のアクティベーション キーが抽出され、セキュリティ アプライアンス ファイル システムのファイル内に保存されます。

アクティベーション キーの取得

アクティベーション キーを取得するには、製品許可キーが必要です。これは、シスコの代理店から購入できます。製品許可キーの取得後、アクティベーション キーを取得するための登録を Web サイトで行います。手順は次のとおりです。

ステップ 1 次のコマンドを入力して、セキュリティ アプライアンス のシリアル番号を取得します。

```
hostname> show version | include Number
```

コマンドの一部としてパイプ記号（|）を入力します。

ステップ 2 Web ブラウザを次のいずれかの Web サイトに接続します（URL は大文字と小文字が区別されます）。

Cisco.com 登録ユーザの場合は、次の Web サイトを使用します。

```
http://www.cisco.com/go/license
```

Cisco.com 登録ユーザでない場合は、次の Web サイトを使用します。

```
http://www.cisco.com/go/license/public
```

ステップ 3　プロンプトが表示されたら、次の情報を入力します。

- 製品許可キー
- セキュリティ アプライアンス のシリアル番号
- ユーザの電子メール アドレス。

アクティベーション キーが自動的に生成され、入力した電子メール アドレスに送信されます。

新しいアクティベーション キーの入力

アクティベーション キーを入力するには、次のコマンドを入力します。

```
hostname(config)# activation-key key
```

key は、4 つまたは 5 つのエレメントからなる 16 進文字列です。各エレメントは 1 つのスペースで区切られます。有効な形式のキーは、次のとおりです。

0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e

先頭の 0x 指定子は任意です。すべての値が 16 進数と見なされます。

すでにマルチコンテキスト モードになっている場合は、システム実行スペースでこのコマンドを入力します。

アクティベーション キーを入力する前に、フラッシュ メモリ内のイメージと実行イメージが同じであることを確認してください。これは、セキュリティ アプライアンスをリブートしてからアクティベーション キーを入力することで確認できます。

（注）　アクティベーション キーはコンフィギュレーション ファイルに保管されません。キーは、デバイスのシリアル番号に関連付けられます。

実行イメージの変更を反映するには、新しいアクティベーション キーの入力後セキュリティ アプライアンスを再起動します。

次に、セキュリティ アプライアンス でアクティベーション キーを変更する例を示します。

```
hostname(config)# activation-key 0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```

フラッシュ メモリ内のファイルの表示

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参照できます。

- 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 [flash: | disk0: | disk1:]
```

flash: キーワードは、PIX 500 シリーズ セキュリティ アプライアンスの内部フラッシュ メモリを表します。ASA 5500 シリーズ適応型セキュリティ アプライアンスの内部フラッシュ メモリの場合は、**flash:** または **disk0:** を使用できます。**disk1:** キーワードは、ASA の外部フラッシュ メモリを表します。内部フラッシュ メモリがデフォルトです。

次に例を示します。

```
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（flash:/ または disk0:/）のルート ディレクトリです。

次に例を示します。

```
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取得

ASA IP アドレスの値とファイル名を提供する次の URL との HTTPS 接続を使用して、フラッシュ ディスクから直接ファイルを取得できます。

```
https://ASA_IP/disk0/filename
```

このオプションは、次の作業を行うお客様にとって便利です。

- （バックアップとしての）ASA バイナリ イメージからのコピー
- WebVPN キャプチャ ファイルをコピーする。
- セキュア デスクトップへの別のフラッシュ ファイルのコピー

フラッシュ メモリへのソフトウェアまたはコンフィギュレーション ファイルのダウンロード

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、およびその他のファイルを、TFTP、FTP、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 5500 シリーズ適応型セキュリティ アプライアンス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。

この項では、次のトピックについて取り上げます。

- 「特定の場所へのファイルのダウンロード」（P.41-4）

- 「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.41-5）

特定の場所への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。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する場合は、「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.41-5）を参照してください。

Cisco SSL VPN Client のインストールの詳細については、「SVC ソフトウェアのインストール」（P.38-2）を参照してください。セキュリティ アプライアンスに 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セキュリティ アプライアンスを設定する場合は、「ブートするアプリケーション イメージと ASDM イメージの設定」（P.41-6）を参照してください。

（注） ASDM バージョン 5.0（5）を問題なくフラッシュ メモリにコピーするには、バージョン 7.0 が実行されている必要があります。

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セキュリティ アプライアンスを設定する場合は、「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.41-6）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。

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 {flash:/ | disk0:/ |
  disk1:/}[path/]filename
  ```

  flash:/ キーワードは、PIX 500 シリーズ セキュリティ アプライアンスの内蔵フラッシュ メモリを示します。ASA 5500 シリーズ適応型セキュリティ アプライアンスの内蔵フラッシュ メモリには、**flash:/** または **disk0:/** と入力できます。**disk1:/** キーワードは、ASA の外付けフラッシュ メモリを示します。

- 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 {flash:/ | 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 {flash:/ |
  disk0:/ | disk1:/}[path/]filename
  ```

- セキュア コピーを使用するには、まず SSH をイネーブルにしてから、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、または HTTP（S）サーバから、あるいはフラッシュ 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。

（注） 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。

- 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**}

- 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** {**flash:/** | **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
```

ブートするアプリケーション イメージと ASDM イメージの設定

デフォルトでは、セキュリティ アプライアンスは内部フラッシュ メモリ内で見つけた最初のアプリケーション イメージをブートします。また、内蔵フラッシュ メモリで最初に検出された ASDM イメージまたは、イメージがない場合は次に、外付けフラッシュ メモリで最初に検出されたイメージが起動されます。複数のイメージがある場合は、起動するイメージを指定してください。ASDM イメージの場合、起動するイメージを指定しないと、イメージが 1 つのみインストールされている場合でも、セキュリティ アプライアンスによって **asdm image** コマンドが実行されているコンフィギュレーションに挿入されます。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。

- 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
  ```

  url に次のいずれかを入力します。

  - {**flash:/** | **disk0:/** | **disk1:/**}[*path/*]*filename*

    flash:/ キーワードは、PIX 500 シリーズ セキュリティ アプライアンスの内蔵フラッシュ メモリを示します。ASA 5500 シリーズ適応型セキュリティ アプライアンスの内蔵フラッシュ メモリには、**flash:/** または **disk0:/** と入力できます。**disk1:/** キーワードは、ASA の外付けフラッシュ メモリを示します。

  - **tftp://**[*user*[**:*password***]**@**]*server*[*:port*]/[*path/*]*filename*

    このオプションは、ASA 5500 シリーズ適応型セキュリティ アプライアンスでのみサポートされます。

  最大 4 つの **boot system** コマンド エントリを入力して、ブートする別々のイメージを順番に指定することができます。セキュリティ アプライアンスは、最初に見つけたイメージをブートします。**boot system tftp:** コマンドは 1 つのみ設定でき、最初に設定する必要があります。

- 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 {flash:/ | 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、セキュリティ アプライアンスは、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 {flash:/ | disk0:/ | disk1:/}[path/]filename
```

flash:/ キーワードは、PIX 500 シリーズ セキュリティ アプライアンスの内蔵フラッシュ メモリを示します。ASA 5500 シリーズ適応型セキュリティ アプライアンスの内蔵フラッシュ メモリには、**flash:/** または **disk0:/** と入力できます。**disk1:/** キーワードは、ASA の外付けフラッシュ メモリを示します。

フェールオーバー ペアのゼロ ダウンタイム アップグレードの実行

フェールオーバー コンフィギュレーション内の 2 つの装置は、メジャー（最初の番号）およびマイナー（2 番目の番号）のソフトウェア バージョンが同じになるようにします。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、両方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 41-1 に、フェールオーバー ペアでゼロダウンタイム アップグレードを実行する場合にサポートされる事例を示します。

表 41-1　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。
メジャー リリース	前のバージョンの最後のマイナー リリースから次のメジャー リリースにアップグレードできます。 たとえば、7.9 が 7.x リリースの最後のマイナー バージョンであれば、7.9 から 8.0 にアップグレードできます。

フェールオーバー ペアのソフトウェアをアップグレードする場合の詳細については、次の各項目を参照してください。

- 「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アップグレード」（P.41-7）
- 「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アップグレード」（P.41-8）

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 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。

ステップ 1　両方の装置に新規ソフトウェアをダウンロードし、ロードする新規イメージを **boot system** コマンド（「ブートするアプリケーション イメージと ASDM イメージの設定」（P.41-6）を参照）で指定します。

ステップ 2　アクティブ装置で次のコマンドを入力して、スタンバイ装置をリロードして新規イメージをブートします。

```
active# failover reload-standby
```

ステップ 3　スタンバイ装置がリロードを終了して Standby Ready 状態になったら、アクティブ装置で次のコマンドを入力して、アクティブ装置をスタンバイ装置に強制的にフェールオーバーします。

（注）　**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。

```
active# no failover active
```

ステップ 4　次のコマンドを入力して、前のアクティブ装置（現在の新規スタンバイ装置）をリロードします。

```
newstandby# reload
```

ステップ 5　新しいスタンバイ装置がリロードを終了して Standby Ready 状態になったら、次のコマンドを入力して、元のアクティブ装置をアクティブ ステータスに戻します。

```
newstandby# failover active
```

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。

ステップ 1　両方の装置に新規ソフトウェアをダウンロードし、ロードする新規イメージを **boot system** コマンド（「ブートするアプリケーション イメージと ASDM イメージの設定」（P.41-6）を参照）で指定します。

ステップ 2　プライマリ装置のシステム実行スペースで次のコマンドを入力して、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。

```
primary# failover active
```

ステップ 3　プライマリ装置のシステム実行スペースで次のコマンドを入力して、セカンダリ装置をリロードして新規イメージをブートします。

```
primary# failover reload-standby
```

ステップ 4　セカンダリ装置がリロードを終了し、その装置で両方のフェールオーバー グループが Standby Ready 状態になったら、プライマリ装置のシステム実行スペースで次のコマンドを使用して、セカンダリ装置の両方のフィールオーバー グループをアクティブにします。

（注）　**show failover** コマンドを使用して、セカンダリ装置の両方のフェールオーバー グループが Standby Ready 状態かどうかを検証します。

```
primary# no failover active
```

ステップ 5　プライマリ装置の両方のフェールオーバー グループが Standby Ready 状態になっていることを確認してから、次のコマンドを使用してプライマリ装置をリロードします。

```
primary# reload
```

ステップ 6　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。

コンフィギュレーション ファイルのバックアップ

設定をバックアップするには、次のコマンドのいずれかを入力します。

- 「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.41-9）
- 「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のバックアップ」（P.41-9）
- 「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.41-10）
- 「端末の表示からのコンフィギュレーションのコピー」（P.41-10）

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
  ```

  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のバックアップ

マルチ コンテキスト モードで、次のコマンドの 1 つをシステム実行スペースで入力して、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:[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:[path/]filename 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 {flash:/ | disk0:/ | disk1:/}[path/]filename {flash:/ | disk0:/ |
disk1:/}[path/]newfilename
```

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
```

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。

Auto Update サポートの設定

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 イメージを多数のセキュリティ アプライアンスにダウンロードすることを許可し、中央からのセキュリティ アプライアンス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。

セキュリティ アプライアンスは、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セキュリティ アプライアンスのアップデートを発行します。

（注）　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。

この項では、次のトピックについて取り上げます。

- 「Auto Update サーバとの通信の設定」（P.41-11）
- 「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.41-12）
- 「Auto Update ステータスの表示」（P.41-13）

Auto Update サーバとの通信の設定

セキュリティ アプライアンスを 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　次のコマンドを入力して、AUS の URL を指定します。

```
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* 引数には、AUS への要求の送信時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 の要求は管理アクセスで使用されるのと同じ IPSec VPN トンネルを通過します。

verify-certificate キーワードでは、AUS から返された証明書を確認します。

ステップ 2　（任意）次のコマンドを入力して、AUS との通信時の送信先となる装置 ID を特定します。

```
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**：セキュリティ アプライアンス のシリアル番号を使用します。
- **hostname**：セキュリティ アプライアンス のホスト名を使用します。
- **ipaddress**：指定したインターフェイスの IP アドレスを使用します。インターフェイス名を指定しない場合、AUS との通信に使用するインターフェイスの IP アドレスを使用します。
- **mad-address**：指定したインターフェイスの MAC アドレスを使用します。インターフェイス名を指定しない場合、AUS との通信に使用するインターフェイスの MAC アドレスを使用します。
- **string**：スペースまたは「‘」「“」「>」「&」および「?」の文字を含めることができない、指定のテキスト識別子を使用します。

ステップ 3　（任意）次のコマンドを入力して、設定またはイメージのアップデートがあるかどうかを確認するための AUS へのポーリングの間隔を指定します。

```
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 です。

ステップ 4　（任意）セキュリティ アプライアンスが Auto Update サーバを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 は、Monday、Tuesday、Wednesday、Thursday、Friday、Saturday、および Sunday の中の任意の 1 日または複数日の組み合わせです。その他の指定可能な値は、daily（月曜日から日曜日まで）、weekdays（月曜日から金曜日まで）、および weekend（土曜日と日曜日）です。

time 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 8:00 AM で、20:00 は 8:00 PM です

randomize *minutes* 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 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 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。指定できる範囲は 1 ～ 35791 分です。

ステップ 5　（任意）自動アップデート サーバへのアクセスが一定時間ない場合、次のコマンドを入力して、トラフィックを中断します。

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

period には、タイムアウト期間（分単位）を 1 ～ 35791 の範囲内で指定します。デフォルトは、タイムアウトなし（0）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。

このコマンドを使用して、セキュリティ アプライアンス のイメージと設定が最新のものであることを確認します。この状態は、システム ログ メッセージ 201008 で報告されます。

次に、外部インターフェイスから IP アドレス 209.165.200.224、ポート番号 1742 の AUS にポーリングして証明書を確認するように セキュリティ アプライアンス を設定する例を示します。

デバイス ID として セキュリティ アプライアンスのホスト名を使用するようにも設定されます。毎週金曜日と土曜日の夜 10:00 p.m. と 11:00 p.m. の間の任意の時刻のポーリングを設定します。失敗したポーリング試行で、AUS へ 10 回再接続を試行し、再接続時の各試行間で 3 分間待機します。

```
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 コマンドを使用して、Auto Update クライアントとして設定されたセキュリティ アプライアンスのアップデートをイネーブルにできます。このコマンドでは、ソフトウェア コンポーネントのタイプ（asdm または boot image）、セキュリティ アプライアンスのタイプまたはファミリ、アップデートを適用するリビジョン番号、アップデートの取得元となる URL または IP アドレスを指定できます。

セキュリティ アプライアンスを 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　グローバル コンフィギュレーション モードで、次のコマンドを入力してクライアント更新をイネーブルにします。

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

ステップ 2　次のように、**client-update** コマンドを使用してセキュリティ アプライアンス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。

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

component {**asdm** | **image**} は、ASDM またはセキュリティ アプライアンスのブート 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* は、Auto Update クライアントが自身を識別するために使用する一意の文字列を指定します。最大で 63 文字です。

family *family_name* 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名を指定します。これは、asa、pix、または最大 7 文字のテキスト ストリングです。

rev-nums *rev-nums* 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* 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。リストに含まれるセキュリティ アプライアンスには、次のものがあります。

- pix-515：Cisco PIX 515 Firewall
- pix-515e：Cisco PIX 515E Firewall
- pix-525：Cisco PIX 525 Firewall
- pix-535：Cisco PIX 535 Firewall
- asa5505：Cisco 5505 適応型セキュリティ アプライアンス
- asa5510：Cisco 5510 適応型セキュリティ アプライアンス
- asa5520：Cisco 5520 適応型セキュリティ アプライアンス
- asa5540：Cisco 適応型セキュリティ アプライアンス

url *url-string* は、ソフトウェア イメージまたはファームウェア 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。

特定のタイプのセキュリティ アプライアンス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、セキュリティ アプライアンスのタイプと、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 セキュリティ アプライアンス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、アップデートは不要です。クライアントはそのアップデートを無視します。

次の例では、Cisco 5520 適応型セキュリティ アプライアンスのクライアント アップデートを設定しています。

```
hostname(config)# client-update type asa5520 component asdm url
http://192.168.1.114/aus/asdm501.bin rev-nums 7.2(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
```