CHAPTER 14

メンテナンス タスクの実行

この章では、Cisco Anomaly Guard Module（Guard モジュール）の一般的なケアや保守用の作業を行う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。

ファイル サーバの設定

Guard モジュール ファイルをエクスポートしたり Guard モジュールにファイルをインポートできるネットワーク サーバを設定すると、IP アドレス、通信方式、およびログインの詳細などのネットワーク サーバ アトリビュートを一度に設定できます。その後で、後の操作でネットワーク サーバ アトリビュートを指定しないで、ネットワーク サーバの名前を使用することができます。

ネットワーク サーバを設定したら、次に export コマンドまたは import コマンドを設定する必要があります。たとえば、export reports コマンドを使用すると、Guard モジュールが攻撃レポートをネットワーク サーバにエクスポートするように設定できます。

ネットワーク サーバを設定するには、設定モードで次のいずれかのコマンドを使用します。

- **file-server** *file-server-name description* **ftp** *server remote-path login password*
- **file-server** *file-server-name description* [**sftp** | **scp**] *server remote-path login*

Secure FTP（SFTP）および Secure Copy（SCP）は、セキュアな通信を行うために Secure Shell（SSH; セキュア シェル）に依存するため、Guard モジュールが SFTP 通信および SCP 通信に使用する SSH 鍵を設定する必要があります。Guard モジュールがセキュアな通信のために使用する鍵を設定する方法の詳細については、P.4-38 の「SFTP 接続および SCP 接続用の鍵の設定」を参照してください。

表 14-1 に、**file-server** コマンドの引数とキーワードを示します。

表 14-1　file-server コマンドの引数とキーワード

パラメータ	説明
file-server-name	ネットワーク サーバの名前。1 ～ 63 文字の英数字文字列を入力します。文字列にアンダースコア（_）を含めることはできますが、スペースを含めることはできません。
description	ネットワーク サーバを説明する文字列。文字列の長さは最大 80 文字です。式にスペースを使用する場合は、式を引用符（" "）で囲みます。
ftp	ネットワーク サーバで FTP を使用するように定義します。

表 14-1　file-server コマンドの引数とキーワード（続き）

パラメータ	説明
sftp	ネットワーク サーバで SFTP を使用するように定義します。
scp	ネットワーク サーバで SCP を使用するように定義します。
server	ネットワーク サーバの IP アドレス。IP アドレスをドット区切り 10 進表記で入力します（たとえば 192.168.10.2）。
remote-path	ファイルの保存先ディレクトリまたはファイルをインポートするディレクトリの完全パス。
login	ネットワーク サーバのログイン名。
password	ネットワーク サーバのパスワード。 このオプションは FTP サーバに対してだけ有効です。Guard モジュールは公開鍵を使用して SFTP および SCP を使用するネットワーク サーバを認証します。

次の例は、IP アドレス 10.0.0.191 を使用して FTP サーバを定義する方法を示しています。

```
user@GUARD-conf# file-server CorpFTP-Server "Corp's primary FTP
server" ftp 10.0.0.191 /root/ConfigFiles <user> <password>
```

ネットワーク サーバを削除するには、設定モードで **no file-server** [*file-server-name* | *] コマンドを使用します。

ネットワーク サーバのリストを表示するには、グローバル モードまたは設定モードで **show file-servers** コマンドを使用します。

設定のエクスポート

Guard モジュールの設定ファイルまたはゾーン設定ファイル（running-config）をネットワーク サーバにエクスポートできます。Guard モジュールまたはゾーンの設定ファイルをリモート サーバにエクスポートすることで、次を実行できます。

- Guard モジュールの設定パラメータを別の Guard モジュールに実装する。
- Guard モジュールの設定をバックアップする。

Guard モジュールの設定ファイルをエクスポートするには、グローバル モードで次のいずれかのコマンドを入力します。

- **copy** [**zone** *zone-name*] **running-config ftp** *server full-file-name* [*login* [*password*]]
- **copy** [**zone** *zone-name*] **running-config** {**sftp** | **scp**} *server full-file-name login*
- **copy** [**zone** *zone-name*] **running-config** *file-server-name dest-file-name*

SFTP および SCP はセキュアな通信を SSH に依存しているため、**sftp** オプションまたは **scp** オプションを使用して **copy** コマンドを入力する前に、Guard モジュールが使用する鍵を設定していない場合、Guard モジュールはパスワードの入力を要求します。Guard モジュールがセキュアな通信のために使用する鍵を設定する方法の詳細については、P.4-38 の「SFTP 接続および SCP 接続用の鍵の設定」を参照してください。

表 14-2 に、**copy running-config ftp** コマンドの引数とキーワードを示します。

表 14-2　copy running-config ftp コマンドの引数とキーワード

パラメータ	説明
zone *zone-name*	（オプション）ゾーン名。ゾーン名を指定すると、Guard モジュールはゾーン設定ファイルをエクスポートします。デフォルトでは、Guard モジュールの設定ファイルがエクスポートされます。
running-config	Guard モジュールのすべての設定、または指定されたゾーンの設定をエクスポートします。
ftp	FTP を使用しているネットワーク サーバに設定をエクスポートします。
sftp	SFTP を使用しているネットワーク サーバに設定をエクスポートします。

表 14-2　copy running-config ftp コマンドの引数とキーワード

パラメータ	説明
scp	SCP を使用しているネットワーク サーバに設定をエクスポートします。
server	ネットワーク サーバの IP アドレス。IP アドレスをドット区切り 10 進表記で入力します（たとえば 192.168.10.2）。
full-file-name	ファイルの完全な名前。パスを指定しない場合、サーバはユーザのホーム ディレクトリにファイルを保存します。
login	サーバのログイン名。 *login* 引数は、FTP サーバを定義するときは省略可能です。ログイン名を入力しなかった場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
password	（オプション）リモート FTP サーバのパスワード。パスワードを入力しない場合、Guard モジュールによってパスワードを要求されます。
file-server-name	設定ファイルをエクスポートするネットワーク サーバの名前。**file-server** コマンドを使用してネットワーク サーバを設定する必要があります。 SFTP または SCP を使用してネットワーク サーバを設定する場合は、Guard モジュールが SFTP 通信および SCP 通信で使用する SSH 鍵を設定する必要があります。 詳細については、P.14-2 の「ファイル サーバの設定」を参照してください。
destination-file-name	リモート サーバ上の設定ファイルの名前。Guard モジュールは、**file-server** コマンドを使用してネットワーク サーバに対して定義したディレクトリの宛先ファイル名を使用してネットワーク サーバ上に設定ファイルを保存します。

次の例は、Guard モジュールの設定ファイルを FTP サーバにエクスポートする方法を示しています。

```
user@GUARD# copy running-config ftp 10.0.0.191 run-conf.txt <user>
<password>
```

次の例は、Guard モジュール設定ファイルをネットワーク サーバにエクスポートする方法を示しています。

```
user@GUARD# copy running-config CorpFTP Configuration-12-11-05
```

設定のインポートとアップデート

Guard モジュールまたはゾーンの設定ファイルを FTP サーバからインポートし、新しく転送されたファイルに応じて Guard モジュールを再設定できます。設定をインポートするには、次のいずれかのタスクを行います。

- Guard モジュールの既存の設定ファイルに基づいて Guard モジュールを設定する。
- Guard モジュールの設定を復元する。

ゾーンの設定は、Guard モジュールの設定の一部です。**copy ftp running-config** コマンドを使用して、両方のタイプの設定ファイルを Guard モジュールにコピーし、それに応じて Guard モジュールを再設定します。

（注） 既存の設定を新しい設定で置き換えます。新しい設定を有効にするには、Guard モジュールをリロードする必要があります。

すべてのゾーンを非アクティブにしてからインポート プロセスを開始することをお勧めします。ゾーン設定をインポートする前に、Guard モジュールによってゾーンは非アクティブになります。

Guard モジュールでは、古いバージョンの自己保護設定はデフォルトで無視されます。自己保護設定を古い設定で上書きしないでください。古い設定は現在の設定と互換性がない場合があります。

Guard モジュールの設定ファイルをインポートするには、グローバル モードで次のいずれかのコマンドを使用します。

- **copy ftp running-config** *server full-file-name* [*login* [*password*]]
- **copy** {**sftp** | **scp**} **running-config** *server full-file-name login*
- **copy** *file-server-name* **running-config** *source-file-name*

SFTP および SCP は安全な通信の SSH に従うので、Guard モジュールは **sftp** オプションまたは **scp** オプションを使用して **copy** コマンドを入力する前に Guard モジュールが使用する鍵を設定しない場合、パスワードの入力を求めます。Guard モジュールがセキュアな通信のために使用する鍵を設定する方法の詳細については、P.4-38 の「SFTP 接続および SCP 接続用の鍵の設定」を参照してください。

表 14-3 に、**copy ftp running-config** コマンドの引数を示します。

表 14-3　copy ftp running-config コマンドの引数

パラメータ	説明
ftp	FTP を使用して、ネットワーク サーバから設定をインポートします。
sftp	SFTP を使用して、ネットワーク サーバから設定をインポートします。
scp	SCP を使用して、ネットワーク サーバから設定をインポートします。
server	ネットワーク サーバの IP アドレス。IP アドレスをドット区切り 10 進表記で入力します（たとえば 192.168.10.2）。
remote-path	ファイルの完全な名前。パスを指定しない場合、サーバはユーザのホーム ディレクトリでファイルを検索します。
login	サーバのログイン名。 *login* 引数は、FTP サーバを定義するときは省略可能です。ログイン名を入力しなかった場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
password	（オプション）リモート FTP サーバのパスワード。パスワードを入力しない場合、Guard モジュールによってパスワードを要求されます。

表 14-3　copy ftp running-config コマンドの引数（続き）

パラメータ	説明
file-server-name	ネットワーク サーバの名前。**file-server** コマンドを使用してネットワーク サーバを設定する必要があります。 SFTP または SCP を使用してネットワーク サーバを設定する場合は、Guard モジュールが SFTP 通信および SCP 通信で使用する SSH 鍵を設定する必要があります。 詳細については、P.14-2 の「ファイル サーバの設定」を参照してください。
source-file-name	インポートするファイルの名前。Guard モジュールは、**file-server** コマンドを使用して、ネットワーク サーバとして定義したパスにファイルの名前を追加します。

次の例は、Guard モジュール設定ファイルを FTP サーバからインポートする方法について示しています。

```
user@GUARD# copy ftp running-config 10.0.0.191
/root/backup/conf/scannet-conf <user> <password>
```

次の例は、Guard モジュールの設定ファイルをネットワーク サーバからインポートする方法について示しています。

```
user@GUARD# copy CorpFTP running-config scannet-conf
```

古いバージョンからエクスポートした設定をインポートすると、Guard モジュールによって次のメッセージが表示されます。

```
WARNING: The configuration file includes a self-protection definition
that is incompatible with the current version and will be ignored.
Continue? [yes|no]
```

次のいずれかのオプションを入力します。

- **yes :** 古い自己保護設定を無視します。Guard モジュールは次のように動作します。
  - 古い自己保護設定を無視し、インポートしない。
  - ゾーン、インターフェイス、サービス設定など、他の設定をすべてインポートする。
- **no**：古い自己保護設定をインポートできます。Guard モジュールによって次のメッセージが表示されます。

```
You can abort the import process or import the old self-protection
definition as-is.
WARNING: The self-protection definitions are incompatible with the
current version.
Abort? [yes|no]
```

注意　自己保護設定を古い設定で上書きしないでください。古い設定は現在のソフトウェアの設定と互換性がない場合があります。

古い自己保護設定をインポートするには、**no** を入力します。

インポート プロセスを中断するには、**yes** を入力します。

ファイルを自動的にエクスポートする方法

Guard モジュールが次のファイルをネットワーク サーバへ自動的にエクスポートするように設定できます。

- パケットダンプ キャプチャ ファイル

  Guard モジュールは、キャプチャ バッファのサイズが 50MB に到達するか、または 10 分が経過すると、パケットダンプ キャプチャ ファイルをエクスポートします。詳細については、P.13-24 の「パケットダンプ キャプチャ ファイルの自動エクスポート」を参照してください。

- 攻撃レポート

  Guard モジュールは、ゾーンに対する攻撃が終了すると、いずれかのゾーンのレポートをエクスポートします。詳細については、P.12-19 の「攻撃レポートの自動エクスポート」を参照してください。

Guard モジュールはパケットダンプ キャプチャ ファイルと攻撃レポートを Extensible Markup Language（XML）形式でエクスポートします。ソフトウェア バージョンには、XML スキーマを記述した xsd ファイルが付属しています。次の URL にある Cisco.com のソフトウェア センターから xsd ファイルをダウンロードできます。

http://www.cisco.com/public/sw-center/

ファイルをネットワークサーバへ自動的にエクスポートするには、次の手順を実行します。

ステップ 1　ファイルをエクスポートできるネットワーク サーバを定義します。

詳細については、P.14-2 の「ファイル サーバの設定」を参照してください。

ステップ 2　次のコマンドを入力することにより、Guard モジュールがファイルを自動的にエクスポートするように設定します。

```
export {packet-dump | reports} file-server-name
```

表 14-4 に、**export** コマンドの引数とキーワードを示します。

表 14-4　export コマンドの引数とキーワード

パラメータ	説明
packet-dump	パケットダンプ バッファの内容がローカル ファイルに保存されるたびに、パケットダンプ キャプチャ ファイルをエクスポートします。Guard モジュールは、「gzip」（GNU zip）プログラムで圧縮および符号化されたパケットダンプ キャプチャ ファイルを（記録されたデータを記述する XML 形式のファイルとともに）PCAP 形式でエクスポートします。XML スキーマについては、このバージョンに付属の Capture.xsd ファイルを参照してください。パケットダンプ キャプチャ ファイルの詳細については、P.13-16 の「ネットワーク トラフィックの監視と攻撃シグニチャの抽出」を参照してください。
reports	攻撃が終了したら、攻撃レポートを XML 形式でエクスポートします。Guard モジュールは、ゾーンに対する攻撃が終了すると、いずれかのゾーンのレポートをエクスポートします。XML　　スキーマについては、このバージョンに付属の ExportedReports.xsd ファイルを参照してください。詳細については、P.12-19 の「攻撃レポートのエクスポート」を参照してください。
file-server-name	ファイルを保存できるネットワーク サーバの名前。**ile-server** コマンドを使用してネットワーク サーバを設定する必要があります。

次の例は、IP アドレス 10.0.0.191 を使用して FTP サーバを定義し、攻撃の最後でそのサーバへ自動的にレポートを XML 形式でエクスポートするように Guard モジュールを設定する方法を示しています。

```
user@GUARD-conf# file-server CorpFTP-Server "Corp's primary FTP
server" ftp 10.0.0.191 /root/ConfigFiles <user> <password>
user@GUARD-conf# export reports CorpFTP-Server
```

ネットワーク サーバへのファイルの自動エクスポートをディセーブルにするには、このコマンドの **no** 形式を使用します。

Guard モジュールのリロード

reload コマンドを使用すると、マシンをリブートすることなく Guard モジュールの設定を再ロードできます。

次の変更内容を反映するには、Guard モジュールをリロードする必要があります。

- **shutdown** コマンドを使用した、物理インターフェイスの非アクティブ化またはアクティブ化
- 新しいフラッシュの組み込み

Guard モジュールのリブートおよびゾーンの非アクティブ化

デフォルトの動作では、Guard モジュールはすべてのゾーンを非アクティブの動作状態でロードします。そのため、リブート前のゾーンの動作状態に関係なく、Guard モジュールはリブート後にゾーン保護またはラーニング プロセスをイネーブルにしません。

リブート プロセス前にアクティブであったゾーンが Guard モジュールによって自動的にアクティブになるように、デフォルトの動作を変更するには、設定モードで次のコマンドを入力します。

boot reactivate-zones

注意　ゾーンのラーニング フェーズは、リブート後に再起動されます。

Guard モジュールのソフトウェアのアップグレード

Guard モジュールが動作するためには、次の 2 つのソフトウェア コンポーネントが必要です。

- Supervisor エンジン 2 または Supervisor エンジン 720 を使用する Cisco IOS ソフトウェア
- Guard モジュール ソフトウェア

（注）　Guard モジュール ソフトウェアをアップグレードするには、Supervisor エンジン モジュールにログインする必要があります。

Supervisor エンジン 2 または Supervisor エンジン 720 を使用する IOS ソフトウェア

1 つ目のソフトウェア コンポーネントは、Catalyst 6500 Supervisor エンジン 2 または Supervisor エンジン 720 を使用する Cisco IOS ソフトウェア イメージです。スーパーバイザ エンジン上のイメージは、Guard モジュールおよびそのプロセッサを認識して初期化します。Guard モジュールをサポートする Cisco IOS ソフトウェア リリースを使用する必要があります。

Guard モジュール ソフトウェア

Guard モジュール ソフトウェアは、プロセッサ制御複合体に統合された Compact Flash（CF; コンパクト フラッシュ）カードに常駐します。コンパクト フラッシュには、ソフトウェア イメージのパーティションが 2 つあります。それぞれには独自のオペレーティング システム（イメージ）が用意されています。

- メンテナンス　パーティション（MP）：基本モジュールの初期化およびドーター カードの制御の機能のために必要なソフトウェア（cf:1 と呼ばれる）
- アプリケーション パーティション（AP）：Guard モジュール アプリケーションに付属するイメージ（cf:4 と呼ばれる）

コンパクト フラッシュ カード上の Guard モジュール ソフトウェアは、スーパーバイザ エンジン コンソールを使用してアップグレードできます。このアップグレード プロセスでは、最新バージョンの AP イメージや MP イメージを Cisco Software Center から FTP サーバまたは TFTP サーバにダウンロードし、コンパクト フラッシュ カードにインストールします。

Guard モジュールでは、次の 3 つのアップグレード手順を使用できます。

- AP　のアップグレード手順：アプリケーション　イメージを使用可能な最新バージョンにアップグレードします。この手順は MP から実行し、モジュールをリセットする必要があります。P.14-16 の「AP イメージのアップグレード」を参照してください。
- MP のアップグレード手順 : メンテナンス パーティションをアップグレードします。MP イメージは、アップグレードの必要がほとんどありません。この手順は、ソフトウェア リリースに付属のリリース ノートで指示されている場合にのみ使用してください。P.14-20 の「AP イメージのアップグレード」を参照してください。
- インライン イメージのアップグレード手順：アプリケーション イメージまたはメンテナンス イメージをアップグレードします。この手順は MP から実行します。P.14-23 の「AP および MP イメージをインラインにアップグレード」を参照してください。

アップグレード時の注意事項

この項では、AP および MP のバージョンをアップグレードする際のガイドラインを示します。

- AP および MP のバージョンをアップグレードするには、スーパーバイザ エンジンにログインします。Guard モジュールのフラッシュ（CFE）をアップグレードするには、Guard モジュールにログインします。
- AP イメージと MP イメージの両方をアップグレードする場合は、MP イメージを先にアップグレードする必要があります。
- MP に切り替えるには、**hw-module module** *slot_number* **reset cf:1** コマンドを使用します。MP モードで操作する主な目的は、AP イメージをアップグレードすることです。
- AP に切り替えるには、**hw-module module** *slot_number* **reset cf:4** コマンドを使用します。AP が通常の動作モードです。

- **show module** コマンドを使用すると、実行しているパーティション イメージのソフトウェア バージョンを表示できます。AP イメージを実行している場合、**show module** コマンド を使用すると AP イメージのバージョンが表示されます。AP イメージ バージョンのサンプル形式は、5.1（0.12）です。MP イメージを実行している場合は、MP イメージのバージョンが表示されます。MP イメージ バージョンのサンプル形式は、5.1（0.0）m です。
- MP イメージ ファイル名は、c6svc-mp.5-0-3.bin 形式です。
- AP イメージ ファイル名は、c6svc-agm-k9.5-0-3.bin 形式です。
- MP は Guard モジュールと同じネットワーク設定を使用します。Guard モジュールのイメージをアップグレードする前に、ネットワークの設定を行う必要があります。詳細については、第 2 章「スーパーバイザ エンジンへの Guard モジュールの設定」および第 3 章「Guard モジュールの初期化」を参照してください。
- AP をアップグレードするときに、Guard モジュールは自己保護設定を新しい設定で更新します。自己保護設定を古い設定で上書きしないでください。古い設定は現在の設定と互換性がない場合があります。

（注） スーパーバイザ エンジンで **logging console** コマンドをグローバルに設定して、アップグレード手順の詳細な出力を表示することを強くお勧めします。コンソールではなく Telnet セッションから接続している場合、コンソール メッセージを表示するには **terminal monitor** コマンドを使用します。

AP イメージのアップグレード

アプリケーション イメージ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　アップグレード プロセスを開始する前に、**copy running-config** コマンドを使用して、Guard モジュールの設定をバックアップします。バックアップすることにより既存の設定を保存できるため、必要な場合は、設定を現在の状態に迅速に復元できます。詳細については、P.14-4 の「設定のエクスポート」を参照してください。

ステップ 2　保存するファイルをエクスポートします。次のファイルをエクスポートできます。

- **copy reports** コマンドまたは **copy zone** *zone-name* **reports** コマンドを使用することで、保存したい攻撃レポートをエクスポートできます。詳細については、P.12-20 の「すべてのゾーンの攻撃レポートのエクスポート」および P.12-21 の「ゾーン レポートのエクスポート」を参照してください。
- **copy log** コマンドを使用して、保存するログをエクスポートします。詳細については、P.13-13 の「ログ ファイルのエクスポート」を参照してください。
- **copy zone** *zone-name* **packet-dump captures** コマンドを使用して、保存するパケットダンプ キャプチャ ファイルをエクスポートします。詳細については、P.13-24 の「パケットダンプ キャプチャ ファイルの手動エクスポート」を参照してください。

ステップ 3　アプリケーション イメージを使用可能な最新のソフトウェア リリースにアップグレードするには、まず、次の場所にある Cisco.com の Software Center でイメージを見つけます。

http://www.cisco.com/public/sw-center/

FTP または TFTP にアクセス可能なディレクトリにソフトウェア イメージをコピーします。

ステップ 4　Guard モジュールをリセットし、MP イメージをロードします（この処理には約 3 分かかります）。すでに MP イメージを実行している場合は、このステップを省略します。

スーパーバイザ エンジンで次のコマンドを入力します。

```
hw-module module slot_number reset cf:1
```

slot_number 引数は、モジュールをシャーシに装着するためのスロットの番号です。

ステップ 5　MP がブートされ、Guard モジュールのステータスが OK であることを確認します。次のコマンドを入力します。

```
show module slot_number
```

ステップ 6　AP イメージをコンパクト フラッシュにインストールします。この処理には数分かかる場合があります。次のコマンドを入力します。

```
copy tftp://path/filename pclc#slot_number-fs:
```

path/filename 引数には、FTP の場所とイメージ ファイルの名前を指定します。FTP サーバが匿名ユーザを許可しない場合は、ftp-url の値に *ftp://user@host/absolute-path/filename* という構文を使用します。パスワードを要求されたら入力します。

FTP サーバから目的のバージョンをダウンロードすることもできます。

アプリケーション イメージのダウンロードの所要時間は、接続の速度によって異なりますが、最大で約 30 分です。

注意　Guard モジュールのコンソールに「You can now reset the module.」のメッセージが表示されるまでは、モジュールをリセットしないでください。このメッセージが表示される前にモジュールをリセットすると、アップグレードが失敗します。

ステップ 7　Guard モジュールを AP にリセットするには、次のコマンドを入力します。

```
hw-module module slot_number reset cf:4
```

ステップ 8　次のコマンドを入力して、コピーした AP イメージが **show module** コマンドの出力に表示されることを確認します。

```
show module slot_number
```

（注） 新しいバージョンで Common Firmware Environment（CFE）のアップデートが必要になることがあります。詳細については、各ソフトウェア リリースに対応するリリース ノートを参照してください。CFE が適合していない場合、AP イメージのアップグレードの後でユーザが最初に Guard モジュールへのセッションを確立すると、Guard モジュールは次のメッセージを表示します。「Bad CFE version (*X*).This version requires version *Y*.」

詳細については、P.14-27 の「新しいフラッシュ バージョンの焼き付け」を参照してください。

次の例は、AP イメージをアップグレードする方法を示しています。

```
Sup# hw-module module 8 reset cf:1
Device BOOT variable for reset = <cf:1>
Warning:Device list is not verified. <<< This message is informational

Proceed with reload of module? [confirm]

% reset issued for module 8
Sup# copy tftp:images/ap/agm-APUpgrade-4.0.0.x.bin pclc#8-fs:
Address or name of remote host [10.56.36.2]?
Source filename [images/ap/agm-APUpgrade-4.0.0.x.bin]?
Destination filename [agm-APUpgrade-4.0.0.x.bin]?
.
.
.
19:50:06: %SVCLC-SP-5-STRRECVD: mod 8: <Application upgrade has
started>
19:50:06: %SVCLC-SP-5-STRRECVD: mod 8: <Do not reset the module till
upgrade completes!!>

......<<< Wait

19:59:58: %SVCLC-SP-5-STRRECVD: mod 8: <Application upgrade has
succeeded>
19:59:58: %SVCLC-SP-5-STRRECVD: mod 8: <You can now reset the module>

Sup# hw-module module 8 reset cf:4 <<<<< Resets Guard module to AP
Device BOOT variable for reset = <cf:4>
Proceed with reload of module? [confirm]
...
%OIR-SP-6-INSCARD:Card inserted in slot 8, interfaces are now online
```

AP イメージのアップグレード

MP イメージは、アップグレードの必要がほとんどありません。MP ソフトウェアをアップデートするようソフトウェア リリースに付属のリリース ノートで指示されている場合、次の手順を実行します。

ステップ 1　最新のソフトウェア リリースにアップグレードするには、次の URL にある Cisco.com のソフトウェア センターにあるソフトウェア イメージを確認します。

http://www.cisco.com/public/sw-center/

FTP または TFTP にアクセス可能なディレクトリにソフトウェア イメージをコピーします。

Guard モジュールをリセットし、MP イメージをロードするには（この処理には約 3 分かかります）、スーパーバイザ エンジンで次のコマンドを入力します。

hw-module module *slot_number* reset cf:1

すでに MP イメージを実行している場合は、このステップを省略します。

slot_number 引数は、モジュールをシャーシに装着するためのスロットの番号です。

ステップ 2　次のコマンドを入力して、MP がブートされ、Guard モジュールのステータスが OK であることを確認します。

show module *slot_number*

ステップ 3　MP イメージをコンパクト フラッシュにコピーします。スーパーバイザ エンジンで次のコマンドを入力することにより、Guard モジュールが MP または AP にリセットされているときに、MP イメージをコピーできます。

copy tftp://*path***/***filename* **pclc#***slot_number***-fs:**

path/filename 引数には、FTP の場所とイメージ ファイルの名前を指定します。

FTP サーバが匿名ユーザを許可しない場合は、ftp-url の値に ftp://user@host/absolute-path/filename という構文を使用します。パスワードを要求されたら入力します。

アプリケーション イメージのダウンロードの所要時間は、接続の速度によって異なりますが、最大で約 30 分です。

注意　Guard モジュールのコンソールに「You can now reset the module.」のメッセージが表示されるまでは、モジュールをリセットしないでください。このメッセージが表示される前にモジュールをリセットすると、アップグレードが失敗します。

FTP サーバから目的のバージョンをダウンロードすることもできます。

MP コマンドの詳細については、P.14-29 の「MP コマンドの使用」を参照してください。

ステップ 4　次のコマンドを入力して、コピーした MP イメージが **show module** コマンドの出力に表示されることを確認します。

```
show module slot_number
```

ステップ 5　Guard モジュールを AP にリセットするには、次のコマンドを入力します。

```
hw-module module slot_number reset cf:4
```

次の例は、MP イメージをアップグレードする方法を示しています。

```
Sup# hw-module module 8 reset cf:1
Device BOOT variable for reset = <cf:1>
Warning:Device list is not verified. <<< This message is informational

Proceed with reload of module? [confirm]

% reset issued for module 8
Sup# copy tftp:images/mp/MPUpgrade-4.0.0.0.bin pclc#8-fs:
Address or name of remote host [10.56.36.2]?
Source filename [images/ap/MPUpgrade-4.0.0.0.bin]?
Destination filename [MPUpgrade-4.0.0.0.bin]?
.
.
.
3d19h:%SVCLC-SP-5-STRRECVD:mod 8:<Upgrade of MP was successful.>
3d19h:%SVCLC-SP-5-STRRECVD:mod 8:<You can now reset the module>
Sup# show module 8
.
The Following output shows MP image name because Guard module is reset
to MP (cf:1)
.
Mod MAC addressesHwFwSwStatus
--- ------------------------------------ ------- ----------- -------
8   000f.348d.d7f0 to 000f.348d.d7f70.3017.2(1)4.0(0.0)mOther
...
Sup# hw-module module 8 reset cf:4 <<< Resets Guard module to AP
(normal operation)
Device BOOT variable for reset = <cf:4>
Proceed with reload of module? [confirm]
...
%OIR-SP-6-INSCARD:Card inserted in slot 8, interfaces are now online
```

AP および MP イメージをインラインにアップグレード

インライン イメージのアップグレード手順は、AP イメージおよび MP イメージをアップグレードする代替の方法です。

ソフトウェア イメージ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　アップグレード プロセスを開始する前に、**copy running-config** コマンドを使用して、Guard モジュールの設定をバックアップします。バックアップすることにより既存の設定を保存できるため、必要な場合は、設定を現在の状態に迅速に復元できます。詳細については、P.14-4 の「設定のエクスポート」を参照してください。

ステップ 2　保存するファイルをエクスポートします。次のファイルをエクスポートできます。

- **copy reports** コマンドまたは **copy zone** *zone-name* **reports** コマンドを使用することで、保存したい攻撃レポートをエクスポートできます。詳細については、P.12-20 の「すべてのゾーンの攻撃レポートのエクスポート」および P.12-21 の「ゾーン レポートのエクスポート」を参照してください。
- **copy log** コマンドを使用して、保存するログをエクスポートします。詳細については、P.13-13 の「ログ ファイルのエクスポート」を参照してください。
- **copy zone** *zone-name* **packet-dump captures** コマンドを使用して、保存するパケットダンプ キャプチャ ファイルをエクスポートします。詳細については、P.13-24 の「パケットダンプ キャプチャ ファイルの手動エクスポート」を参照してください。

ステップ 3　イメージを使用可能な最新バージョンにアップグレードするには、次の場所にある Cisco.com の Software Center でイメージを見つけます。

http://www.cisco.com/public/sw-center/

FTP にアクセス可能なディレクトリにソフトウェア イメージをコピーします。

MP コマンドの詳細については、P.14-27 の「新しいフラッシュ バージョンの焼き付け」を参照してください。

ステップ 4　コンソール ポートまたは Telnet セッションを介してスーパーバイザ エンジンにログインします。

ステップ 5　Guard モジュールをメンテナンス イメージで実行している場合は、ステップ 7 に進みます。Guard モジュールをメンテナンス イメージで実行していない場合は、スーパーバイザ エンジンで次のコマンドを入力します。

```
hw-module module slot_number reset cf:1
```

slot_number 引数は、モジュールをシャーシに装着するためのスロットの番号です。

ステップ 6　Guard モジュールがオンラインに戻ったら、Guard モジュールとのコンソール セッションを確立し、ルート アカウントにログインします。アカウントのデフォルト パスワードは *cisco* です。

ステップ 7　次のコマンドを入力することで、ソフトウェア イメージをアップグレードします。

```
upgrade ftp://path/filename
```

path/filename 引数には、FTP の場所とイメージ ファイルの名前を指定します。

FTP サーバが匿名ユーザを許可しない場合は、ftp-url の値に ftp://user@host/absolute-path/filename という構文を使用します。パスワードを要求されたら入力します。

AP ソフトウェア イメージをアップグレードするには、AP ソフトウェア イメージのファイル名を入力します。MP ソフトウェア イメージをアップグレードするには、MP ソフトウェア イメージのファイル名を入力します。詳細については、P.14-15 の「アップグレード時の注意事項」を参照してください。

注意　Guard モジュールのコンソールに次のメッセージが表示されるまでは、モジュールをリセットしないでください。「Application image upgrade complete.You can boot the image now.」このメッセージが表示される前にモジュールをリセットすると、アップグレードが失敗します。

ステップ 8　アップグレードが完了したら、**exit** コマンドを入力して、Guard モジュールからログアウトします。

ステップ 9　Guard モジュールを AP ソフトウェア イメージにリセットするには、次のコマンドを入力します。

```
hw-module module slot_number reset cf:4
```

（注）　新しいソフトウェア リリースにアップグレードすることで Common Firmware Environment（CFE）のアップデートが必要になることがあります。詳細については、各ソフトウェア リリースに対応するリリース ノートを参照してください。CFE が適合していない場合、AP イメージのアップグレードの後でユーザが最初に Guard モジュールへのセッションを確立すると、Guard モジュールは次のメッセージを表示します。「Bad CFE version (*X*).This version requires version *Y*」。詳細については、P.14-27 の「新しいフラッシュ バージョンの焼き付け」を参照してください。

ステップ 10　Guard モジュールがリブートしたら、**show version** コマンドを入力して、ソフトウェア バージョンを確認します。

次の例は、Guard モジュールのアプリケーション ソフトウェアをアップグレードする方法を示しています。

```
Sup# hw-module module 8 reset cf:1
.
.
.
Proceed with reload of module? [confirm]
% reset issued for module 9
.
.
.
Sup# session slot 8 proc 1
.
.
.
login:root
Password:
.
.
.
root@localhost.cisco.com# upgrade
ftp://psdlab-pc1/pub/images/ap/agm-APUpgrade-4.0.0.x.bin


Downloading the image. This may take several minutes...
.
.
.
Upgrading will wipe out the contents on the storage media.
Do you want to proceed installing it [y|N]:



Proceeding with upgrade. Please do not interrupt.
If the upgrade is interrupted or fails, boot into
Maintenance image again and restart upgrade.
.
.
.
Application image upgrade complete. You can boot the image now.
root@hostname.cisco.com# exit
logout
                                                                [  OK  ]
[Connection to 127.0.0.91 closed by foreign host]
Sup# hw-module module 8 reset cf:4
```

新しいフラッシュ バージョンの焼き付け

現在の Common Firmware Environment（CFE）とソフトウェア リリースが適合していない場合にだけ、新しいフラッシュ バージョンを焼き付けることができます。不適合は、Guard モジュール ソフトウェアをアップデートするときに発生する場合があります。

CFE との不適合が検出された場合、ソフトウェア リリースのアップグレード後に Guard モジュールとの最初のセッションを確立するときに、Guard モジュールは次のメッセージを表示します（X は古いフラッシュ バージョンを示し、Y は新しいフラッシュ バージョンを示します）。「Bad CFE version (X).This version requires version Y.」

注意　新しいフラッシュ バージョンを焼き付けている間は、Guard モジュールに安定して電源が供給されるようにし、かつ Guard モジュールを動作させないようにする必要があります。上記の制限に対応できない場合、アップグレードは正常に終了せず、Guard モジュールにアクセスできなくなる可能性があります。

新しいフラッシュ バージョンを焼き付けるには、次の手順を実行します。

ステップ 1　設定モードで次のコマンドを入力します。

```
flash-burn
```

CFE と Guard モジュールのソフトウェア バージョンが適合している場合に新しいフラッシュを焼き付けようとすると、操作が失敗します。

ステップ 2　Guard モジュールをリロードするには、次のコマンドを入力します。

```
reload
```

新しいフラッシュ バージョンを焼き付けた後、**reload** コマンドを入力する必要があります。Guard モジュールは、**reload** コマンドを実行した後でないと完全に機能しません。

次の例は、新しいフラッシュ バージョンを焼き付ける方法を示しています。

```
user@GUARD-conf# flash-burn
Please note: DON'T PRESS ANY KEY WHILE IN THE PROCESS!
. . .
Burned firmware successfully
SYSTEM IS NOT FULLY OPERATIONAL. Type 'reload' to restart the system
```

MP コマンドの使用

ユーザは、Guard モジュールを MP からブートすることができます。Guard モジュールを管理および診断するため、インターフェイスのセットを MP で使用できます。MP の主要な特徴の 1 つは、新しい AP イメージをインストールする機能を提供することです。

MP からブートするには、**hw_module module reset** コマンドを使用した後、**session slot** コマンドを入力して、MP にログインします。

表 14-5 は MP コマンドを要約したものです。

表 14-5　MP 関連のコマンド

コマンド	説明
clear ap password	Guard モジュールに定義されたすべてのパスワードを消去します。
clear ap config	Guard モジュールをデフォルト設定に戻します。このコマンドは Guard モジュールの設定、ログ、およびレポートをすべて削除します。
ip address [*ip address*] [*subnet*]	Guard モジュールが外部ネットワークへのアクセスに使用する IP アドレスを設定します。
ip gateway [*default-gateway*]	ネットワークのデフォルト ゲートウェイを指定します。
passwd	現行ユーザのパスワードを変更します。
passwd-guest	ゲスト アカウントのパスワードを変更します。
ping {*host-name* | *ip address*}	ネットワーク上の特定のホストに ping を実行し、ネットワーク パラメータが正しく設定されていることを確認します。
show images	アプリケーション パーティションに格納されているイメージを表示します。
show ip	Guard モジュールのネットワーク パラメータを表示します。

表 14-5　MP 関連のコマンド（続き）

コマンド	説明
upgrade *ftp-url*	イメージをアップグレードします。ftp-url は、イメージおよびイメージへのパスを含む FTP サーバを指定する URL です。パスの形式は ftp://user:password@server-name/path です。 FTP サーバの名前または IP アドレスを指定できます。

忘失パスワードの復旧

忘失したパスワードを復旧するには、次の手順を実行します。

ステップ 1　Guard モジュールを MP にリセットするには、スーパーバイザ エンジン上で次のコマンドを入力します。

```
hw-module module slot_number reset cf:1
```

slot_number 引数は、モジュールをシャーシに装着するためのスロットの番号です。

ステップ 2　Guard モジュールがオンラインに戻ったら、Guard モジュールとのセッションを確立し、ルート アカウントにログインします。

ステップ 3　次のコマンドを入力することで、Guard モジュール上に設定されたすべてのパスワードを削除します。

```
clear ap password
```

ステップ 4　Guard モジュールを AP にリセットするには、次のコマンドを入力します。

```
hw-module module slot_number reset cf:4
```

ステップ 5　Guard モジュールに設定されたユーザに、新しいパスワードを設定します。P.4-10 の「自分のパスワードの変更」を参照してください）。Guard モジュールのユーザのリストを表示するには、**show running-config** コマンドを使用します。

ヒント　**show running-config** コマンド出力の表示を Guard モジュールのユーザのリストだけが含まれるように絞り込むには、**show running-config | include username** コマンドを使用します。

工場出荷時のデフォルト設定へのリセット

状況によっては、Guard モジュールの設定を、工場出荷時のデフォルト設定に戻したい場合があります。工場出荷時のデフォルト設定にリセットすることは、設定が複雑になった場合や、Guard モジュールをあるネットワークから別のネットワークに移動させる場合に、Guard モジュールに前から存在する不要な設定を削除するときに役立ちます。Guard モジュールを工場出荷時のデフォルトにリセットして、新しい Guard モジュールとして設定できます。

工場出荷時のデフォルト設定にリセットする前に、**copy running-config** コマンドを使用して、Guard モジュールの設定をバックアップすることをお勧めします。P.14-4 の「設定のエクスポート」を参照してください。

管理インターフェイスの設定（eth1）は、Guard モジュールをリロードするまで使用できます。

注意　Guard モジュールの設定を工場出荷時のデフォルトにリセットして、コンソールに接続していないときに Guard モジュールをリロードした場合、Guard モジュールへの接続は失われます。

Guard モジュールを工場出荷時のデフォルト設定にリセットするには、設定モードで次のコマンドを使用します。

clear config all

設定した変更内容は、リセットをした後に有効になります。

次の例は、Guard モジュールを工場出荷時のデフォルト設定にリセットする方法を示しています。

```
user@GUARD-conf# clear config all
```