CHAPTER 13

メンテナンス タスクの実行

この章では、Cisco Traffic Anomaly Detector Module（Detector 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。

（注） 1 Gbps 動作の Detector モジュールと 2 Gbps 動作の Detector モジュールの間には、動作および設定上の違いがあります。この章では、1 Gbps 動作と 2 Gbps 動作の違いについて説明します。特に記載がない限り、この章の情報は、両方の動作モードに適用されます。詳細については、P.1-9 の「1 Gbps および 2 Gbps 帯域幅オプションについて」を参照してください。

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

ネットワーク サーバを Detector モジュールで定義すると、そのサーバと Detector モジュールとの間でファイルをインポートおよびエクスポートできます。Detector モジュールでは、IP アドレス、通信方式、ログインの詳細など、ネットワーク サーバのアトリビュートを定義するネットワーク サーバ プロファイルを作成できます。ネットワーク サーバ プロファイルを作成することにより、サーバ名を指定するだけで、ファイルをインポートまたはエクスポートできます。

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、Detector 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 Secure Shell（SSH; セキュア シェル）に依存しているので、SFTP 通信および SCP 通信に Detector モジュールで使用する SSH 鍵を設定する必要があります。Detector 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.4-40 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 13-1 に、**file-server** コマンドの引数とキーワードを示します。

表 13-1　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 文字の英数字です。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 13-1　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のインポート元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。Detector 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@DETECTOR-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

Detector 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。Detector 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。

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

Detector 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*

Cisco Anomaly Guard Module でゾーンを設定するために必要なゾーン設定の一部をエクスポートするには、**copy guard-running-config** コマンドを使用します。詳細については、P.5-28 の「ゾーン設定の手動エクスポート」を参照してください。

SFTP および SCP はセキュアな通信を SSH に依存しているので、**sftp** 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、Detector モジュールで使用する鍵を設定していない場合、Detector モジュールによってパスワードの入力が求められます。Detector 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.4-40 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 13-2 に、**copy running-config ftp** コマンドの引数とキーワードを示します。

表 13-2　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）ゾーン名を指定します。ゾーン名を指定すると、Detector 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、Detector 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	Detector 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	File Transfer Protocol（FTP; ファイル転送プロトコル）を指定します。
sftp	Secure File Transfer Protocol（SFTP; セキュア ファイル転送プロトコル）を指定します。
scp	Secure Copy Protocol（SCP）を指定します。
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	（オプション）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、Detector モジュールによってパスワードを要求されます。

表 13-2　copy running-config ftp コマンドの引数とキーワード（続き）

パラメータ	説明
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、Detector 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.13-2 の「ファイル サーバの設定」を参照してください。
dest-file-name	リモート サーバ上の設定ファイルの名前。 Detector 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、Detector 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@DETECTOR# copy running-config ftp 10.0.0.191 run-conf.txt <user>
<password>
```

次の例は、Detector モジュールの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@DETECTOR# copy running-config CorpFTP Configuration-12-11-05
```

設定のインポートとアップデート

Detector 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 Detector 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。

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

ゾーンの設定は、Detector 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 Detector モジュールにコピーし、それに応じて再設定します。

（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、Detector 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。Detector モジュールはゾーンを非アクティブにしてからゾーンの設定をインポートします。

Detector 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 はセキュアな通信を SSH に依存しているので、**sftp** 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、Detector モジュールで使用する鍵を設定していない場合、Detector モジュールによってパスワードの入力が求められます。Detector 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.4-40 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 13-3 に、**copy ftp running-config** コマンドの引数を示します。

表 13-3　copy ftp running-config コマンドの引数

パラメータ	説明
ftp	FTP を指定します。
sftp	SFTP を指定します。
scp	SCP を指定します。
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 ディレクトリでファイルを検索します。
login	（オプション）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、Detector モジュールによってパスワードを要求されます。
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、Detector 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.13-2 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。Detector 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、Detector 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@DETECTOR# copy ftp running-config 10.0.0.191
/root/backup/conf/scannet-conf <user> <password>
```

次の例は、Detector 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@DETECTOR# copy CorpFTP running-config scannet-conf
```

ファイルを自動的にエクスポートする方法

Detector 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

  Detector モジュールは、キャプチャ バッファのサイズが 50 MB 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.12-26 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

  Detector モジュールは、いずれか 1 つのゾーンのレポートを、そのゾーンに対する攻撃が終了した時点でエクスポートします。詳細については、P.11-11 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。

- ゾーン設定

  ラーニング プロセスのしきい値調整フェーズの結果が受け入れられるたびに、Detector モジュールはゾーンの設定ファイルをエクスポートします。詳細については、P.5-26 の「ゾーン設定の自動エクスポート」を参照してください。

Detector 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。www.cisco.com から xsd ファイルをダウンロードできます。

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.13-2 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、Detector 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 | sync-config} file-server-name
```

表 13-4 に、**export** コマンドの引数とキーワードを示します。

表 13-4　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。Detector モジュールは、gzip（GNU zip）プログラムで圧縮、符号化された PCAP 形式でパケットダンプ キャプチャ ファイルをエクスポートし、記録されたデータを説明する XML のファイルを添付します。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.12-19 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。Detector モジュールは、いずれか 1 つのゾーンのレポートを、そのゾーンに対する攻撃が終了した時点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 ExportedReports.xsd ファイルを参照してください。詳細については、P.11-11 の「攻撃レポートのエクスポート」を参照してください。
sync-config	ラーニング プロセスのしきい値調整フェーズの結果が受け入れられるたびに、ゾーンの設定をエクスポートします。その後、その設定を Guard モジュールにインポートしてアクティブにし、ゾーンを保護することができます。 Detector モジュールがネットワーク サーバにゾーン設定を自動的にエクスポートできるようにするには、Detector モジュールのデフォルトのリモート サーバ リストまたはゾーンのリモート サーバ リストにそのサーバを設定する必要があります。詳細については、P.5-26 の「ゾーン設定の自動エクスポート」を参照してください。

表 13-4　export コマンドの引数とキーワード（続き）

パラメータ	説明
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。**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。

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 Detector モジュールを設定する方法を示しています。

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

Detector モジュールがゾーン設定をエクスポートするネットワーク サーバのデフォルト リストを表示するには、設定モードで **show sync-config file-servers** コマンドを使用します。

ゾーンのリモート サーバ リストを表示するには、ゾーン設定モードで **show sync-config file-servers** コマンドを使用します。

Detector 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 Detector モジュールの設定をリロードできます。

次の変更内容を反映するには、Detector 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

Detector モジュールのリブートおよびゾーンの非アクティブ化

デフォルトでは、Detector モジュールは、リブート プロセスの前にアクティブになっていたゾーンを再度アクティブにします。

非アクティブ動作状態のすべてのゾーンを Detector モジュールがロードす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。

no 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。

Detector モジュール ソフトウェアのアップグレード

この項では、Detector モジュールが動作するために必要な次の 2 つのソフトウェア コンポーネントについて取り上げます。

- Supervisor Engine 2 または Supervisor Engine 720 をサポートする Cisco IOS リリース
- Detector モジュール ソフトウェア（メンテナンス パーティション イメージとアプリケーション パーティション イメージ）

Detector モジュール ソフトウェア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する必要があります。

この項では、次のトピックについて取り上げます。

Supervisor Engine 2 または Supervisor Engine 720 の Cisco IOS ソフトウェア

Cisco IOS ソフトウェア イメージは、Cisco Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータの Supervisor Engine 2 または Supervisor Engine 720 に存在します。スーパーバイザ エンジンに存在するイメージは、Detector モジュールとそのプロセッサを認識し、初期化します。Detector 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。

Detector モジュール ソフトウェア

Detector モジュール ソフトウェアは、プロセッサ制御複合体に組み込まれたコンパクト フラッシュ（CF）カード上に存在します。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 Detector モジュール ソフトウェア 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 Detector モジュールのメンテナンス ソフトウェア イメージを格納しています。スーパーバイザ エンジンは、MP を cf:1 として識別します。

- アプリケーション パーティション（AP）：Detector モジュール アプリケーション ソフトウェア イメージを格納しています。スーパーバイザ エンジンは、AP を cf:4 として識別します。

スーパーバイザ エンジン コンソールで、コンパクト フラッシュ カード上の Detector モジュール ソフトウェアを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 Trivial File Transfer Protocol（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。

（注）　Detector モジュール ソフトウェアをアップグレードして帯域幅のパフォーマンスを 1 Gbps から 2 Gbps に向上させる場合は、P.13-30 の「1 Gbps から 2 Gbps への帯域幅パフォーマンスのアップグレード」を参照してください。

Detector モジュールについては、次のアップグレード手順が利用可能です。

- AP のアップグレード手順：スーパーバイザ エンジンの CLI を使用して AP イメージをアップグレードします。P.13-17 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：スーパーバイザ エンジンの CLI を使用して MP イメージ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.13-21 の「MP 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：Detector モジュールの CLI を使用して、AP または MP イメージをアップグレードします。P.13-24 の「AP および MP イメージのインライン アップグレード」を参照してください。
- Common Firmware Environment（CFE）：Detector モジュールで CFE をアップグレードします。新しい AP または MP イメージをインストールする過程で CFE もアップグレードされるため、CFE のアップグレードの必要はほとんどありません。現在の CFE と新しい MP または AP イメージの不適合を表すエラー メッセージを Detector モジュールが表示した場合にのみ、CFE をアップグレードする必要があります。P.13-28 の「Common Firmware Environment をアップグレードするため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。

アップグレード操作に関する注釈

AP および MP ソフトウェア イメージと CFE をアップグレードするときには、次のガイドラインに従います。

- 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。
- CFE をアップグレードするには、Detector 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。たとえば、AP イメージのバージョン形式は 5.1(0.12) のように表示されます。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。たとえば、MP イメージのバージョン形式は 5.1(0.0)m のように表示されます。
- MP イメージのファイル名の形式は、c6svc-mp.5-0-3.bin です。
- AP イメージのファイル名の形式は、c6svc-adm-k9.5-0-3.bin です。
- MP は、Detector モジュールと同じネットワーク設定を使用します。ネットワーク設定は、Detector モジュールのイメージをアップグレードする前に設定する必要があります。詳細については、第 2 章「スーパーバイザ エンジンでの Detector モジュールの設定」および第 3 章「Detector モジュールの初期化」を参照してください。
- 1 Gbps の帯域幅動作で AP イメージのバージョン 5.x をバージョン 6.x にアップグレードする場合、インストール プロセスによって管理ポート指定子のインスタンスがすべて eth1 から mng に変更されます。

（注）　**logging console** コマンドをスーパーバイザ エンジンに対してグローバルに設定し、アップグレード手順の出力の詳細を表示することをお勧めします。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

AP 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、Detector 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.13-4 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、保存する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.11-12 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.11-13 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.12-16 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.12-27 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　www.cisco.com でイメージを見つけて、アプリケーション イメージを最新の利用可能なソフトウェア リリースにアップグレードします。

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　Detector モジュールをリセットし、MP イメージをロードします（この作業には約 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 引数には、モジュールが挿入されているシャーシ内のスロットの番号を指定します。

ステップ 5　MP がブートしたこと、および Detector 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。接続の速度によって異なりますが、この処理には、最大で 30 分かかります。次のコマンドを入力します。

```
copy ftp://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。

また、TFTP 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。

注意　Detector モジュールのコンソールに「You can now reset the module.」というメッセージが表示されるまで、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、アップグレードは失敗します。

ステップ 7　次のコマンドを入力して、Detector モジュールを AP にリセットします。

```
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てい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（リリース ノートは www.cisco.com にあります）。CFE が不適合な場合、Detector モジュールは、AP イメージのアップグレード後に Detector モジュールへの最初のセッションを確立したときに、「Bad CFE version (*X*). This version requires version *Y*.」というメッセージを表示します。

詳細については、P.13-28 の「Common Firmware Environment をアップグレードするため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/adm-APUpgrade-4.0.0.x.bin pclc#8-fs:
Address or name of remote host [10.56.36.2]?
Source filename [images/ap/adm-APUpgrade-4.0.0.x.bin]?
Destination filename [adm-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 Detector 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
```

MP 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　www.cisco.com でソフトウェア イメージを見つけて、最新のソフトウェア リリースにアップグレードします。

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。

Detector モジュールをリセットし、MP イメージをロードするには（この作業には約 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 引数には、モジュールが挿入されているシャーシ内のスロットの番号を指定します。

ステップ 2　次のコマンドを入力して、MP がブートされ、Detector 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　スーパーバイザ エンジンで次のコマンドを入力して、MP イメージをコンパクト フラッシュにコピーします。

```
copy ftp://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　Detector モジュールのコンソールに「You can now reset the module.」というメッセージが表示されるまで、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、アップグレードは失敗します。

また、TFTP 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.13-34 の「MP 関連のコマンドの使用」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　次のコマンドを入力して、Detector モジュールを AP にリセットします。

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 Detector 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 Detector 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 イメージのインライン 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では、AP イメージおよび MP イメージをアップグレードする別の方法を示します。インライン イメージ アップグレードを実行する場合には、スーパーバイザ エンジンではなく、Detector モジュールからアップグレードを実行します。

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、Detector 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.13-4 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、保存する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.11-12 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.11-13 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.12-16 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.12-27 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　www.cisco.com でイメージを見つけて、イメージを使用可能な最新のバージョンにアップグレードします。

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。

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　メンテナンス イメージで Detector モジュールが稼働中の場合は、ステップ 7 に進みます。メンテナンス イメージで Detector モジュールが稼働中でない場合は、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 引数には、モジュールが挿入されているシャーシ内のスロットの番号を指定します。

ステップ 6　Detector モジュールがオンラインに戻ったら、Detector 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。このルート アカウントのデフォルトのパスワードは *cisco* です。コンソール セッションを確立するには、スーパーバイザ エンジン プロンプトで次のコマンドを入力します。

```
session slot slot_number processor processor_number
```

slot-number は、Detector モジュールが挿入されているシャーシ内のスロットの番号（スイッチまたはルータのモデルに応じて 1 ～ 13）です。*processor_number* は、Detector モジュールのプロセッサの番号です。Detector モジュールは、プロセッサ 1 を介した管理だけをサポートします。

ステップ 7　次のコマンドを入力して、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.13-16 の「アップグレード操作に関する注釈」を参照してください。

注意　Detector モジュールのコンソールに、「Application image upgrade complete. You can boot the image now.」というメッセージが表示されるまで、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、アップグレードは失敗します。

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、Detector モジュールからログアウトします。

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

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

（注）　新しいソフトウェア リリースへアップグレードするために、Common Firmware Environment（CFE）のアップデートが必要となる場合があります。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 が不適合な場合、Detector モジュールは、AP イメージのアップグレード後に Detector モジュールへの最初のセッションを確立したときに、「Bad CFE version (*X*). This version requires version *Y*.」というメッセージを表示します。詳細については、P.13-28 の「Common Firmware Environment をアップグレードするため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　Detector モジュールがリブートされたら、**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、Detector モジュール 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/adm-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
```

Common Firmware Environment をアップグレードするための新しいフラッシュ バージョンの焼き付け

現在の 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、Detector モジュール の AP または MP 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 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 Detector モジュールとのセッションを初めて確立するときに、Detector 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、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） CFE と Detector 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 バージョンを焼き付けようとすると、操作が失敗します。

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、Detector モジュールに安定して電源が供給されるようにし、かつ Detector 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、Detector 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
```

ステップ 2　Detector 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。Detector 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@DETECTOR-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
```

1 Gbps から 2 Gbps への帯域幅パフォーマンスのアップグレード

Detector モジュールが現在最大 1 Gbps の帯域幅で動作している場合には、ソフトウェア イメージの XG バージョンと対応するソフトウェア ライセンス キーをインストールすることによって、帯域幅パフォーマンスを 2 Gbps にアップグレードできます。XG ソフトウェア イメージは、Detector モジュールとスーパーバイザ エンジン間のデータ トラフィックに使用する追加インターフェイス ポートをアクティブにします（1 Gbps ソフトウェア イメージは、データ トラフィックに 1 つのインターフェイスだけを使用します）。ソフトウェア ライセンス キーにより、インストールされた XG ソフトウェア イメージがアクティブになります。詳細については、P.1-9 の「1 Gbps および 2 Gbps 帯域幅オプションについて」を参照してください。

XG ソフトウェア イメージをインストールしても、対応するソフトウェア ライセンスをインストールし、2 Gbps 動作に必要な設定変更を行うまで、Detector モジュールは動作しません。その設定変更として、次の項目があります。

- インターフェイス設定：スーパーバイザ　エンジンで新しいインターフェイスを設定します。
- SSL 証明書：Detector モジュールおよび関連付けられている Guard で新しい SSL 証明書を生成します。

XG ソフトウェア イメージとライセンスをインストールしても、次の Detector モジュールの項目には影響しません。

- ゾーン設定：既存のゾーン設定情報は変わりません。
- 管理アクセス：1 Gbps 動作の場合に mng で設定した設定パラメータは、2 Gbps 動作でも同じです。

この項では、次のトピックについて取り上げます。

- 2 Gbps 動作用 XG ソフトウェア イメージの取得とインストール
- XG ソフトウェア イメージ ライセンス キーの取得とインストール
- 2 Gbps 動作用追加データ ポートのアクティブ化
- 2 Gbps 動作用 SSL 証明書の再生成

2 Gbps 動作用 XG ソフトウェア イメージの取得とインストール

XG ソフトウェア イメージのコピーを取得し、Detector モジュールにソフトウェアをインストールするには、P.13-17 の「AP イメージのアップグレード」を参照してください。

XG ソフトウェア イメージがロードされたことを確認するには、**show version** コマンドを使用します。XG ソフトウェア イメージがロードされると、ソフトウェア バージョン番号の後に XG と表示されます（version 6.0(.0.39)-XG など）。

XG ソフトウェア イメージ ライセンス キーの取得とインストール

XG ソフトウェア イメージをアクティブにするために必要なライセンス キーは、XG ソフトウェア イメージが格納されている Detector モジュールの Media Access Control（MAC; メディア アクセス制御）アドレスと対応付けられます。この項では、XG ソフトウェア ライセンス キーを注文するプロセスについて説明します。

（注）　XG バージョン 6.0 オペレーティング ソフトウェア（またはそれ以降）を Detector モジュールにロードした上で、対応するライセンスを注文およびインストールする必要があります。Detector モジュールに現在ロードされているソフトウェアのバージョンを確認するには、**show version** コマンドを使用します。XG ソフトウェア イメージがロードされると、ソフトウェアのバージョン番号に -XG 接尾辞が付きます（version 6.0(0.39)-XG など）。

2 Gbps ライセンスを取得し、インストールするには、次の手順を実行します。

ステップ 1　Detector モジュールから **show license-key unique-identifier** コマンド（このコマンドを使用するには admin 特権レベルが必要）を入力して、Detector モジュールの MAC アドレスを表示します。

ステップ 2　MAC アドレス情報を記録します。この情報は、2 Gbps 動作ライセンスを注文するときに必要です。

ステップ 3　www.cisco.com で利用可能な Cisco Ordering ツールを使用して、lic-adm-2g-k9 ライセンスを注文します。

ステップ 4　Cisco から Software License Claim Certificate を受け取ったら、次の Cisco.com Web サイトにアクセスする手順に従います。

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

ステップ 5　購入証明として Software License Claim Certificate に記載されている製品認可キー（PAK）番号を入力します。

ステップ 6　要求された情報をすべて入力して、ライセンス キーを生成します。

ライセンス キーが生成されると、ライセンス ファイルが添付され、インストール手順が記載されたライセンス キー電子メールを受信します。ライセンス キー電子メールは、今後必要となる場合に備えて、安全な場所に保存します。

ステップ 7　テキスト エディタを使用してライセンス キー ファイルを開き、その内容をデスクトップ コンピュータのクリップボードにコピーします。

ステップ 8　Detector モジュールから、設定モードで **license-key add** コマンドを入力します。キーの入力を求める CLI プロンプトが表示されます。

ステップ 9　デスクトップ コンピュータのクリップボードの（ライセンス キーを含む）内容を貼り付け、**Enter** キーを押します。

ステップ 10　空行を入力して、**Enter** キーを押します。以前にインストールしたライセンスが Detector モジュールに残っている場合には、新しいライセンスをインストールするかどうかを尋ねる確認メッセージが表示されます。

ステップ 11　**y**（yes）を入力します。これで XG ソフトウェア イメージがアクティブになり、2 Gbps 動作の準備は完了です。

ステップ 12　（オプション）**show license-key** コマンドを入力して、キーが適切にロードされ、有効であることを確認します。

2 Gbps 動作用追加データ ポートのアクティブ化

XG ソフトウェア イメージをインストールし、アクティブ化することにより、スーパーバイザ エンジンと Detector モジュール間のデータ トラフィックが、1 つだけではなく 2 つのインターフェイス ポートを介して移動できるようになります。Detector モジュールで 2 Gbps 動作用の追加データ ポートをアクティブ化するには、インターフェイス設定モードで **no shutdown** コマンドを使用します。

詳細については、P.3-11 の「物理インターフェイスの設定」を参照してください。

2 Gbps 動作用 SSL 証明書の再生成

Detector モジュールは、Secure Sockets Layer（SSL）証明書を使用して、関連付けられている Guard サービスと安全な通信チャネルを確立します。1 Gbps ソフトウェア イメージから 2 Gbps ソフトウェア イメージにアップグレードすると、既存の SSL 証明書が Detector モジュールから削除されます。2 Gbps ソフトウェア イメージとライセンスをインストールした後、Detector モジュールおよび関連付けられている Guard が安全な通信チャネルを確立するために使用する SSL 証明書を再生成する必要があります。関連付けられている Guard については、最初に既存の SSL 証明書を削除した後に、新しい証明書を作成できます。

詳細については、P.4-31 の「SSL 証明書の再生成」を参照してください。

MP 関連のコマンドの使用

Detector モジュールを MP にブートできます。Detector モジュールを管理および診断するためのインターフェイスのセットを MP 上で使用できます。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 にブートするには、**hw_module module reset** コマンドを入力し、その後 **session slot** コマンドを入力して MP にログインします。

表 13-5 で、MP 関連のコマンドの要点を説明します。

表 13-5　MP 関連のコマンド

コマンド	説明
clear ap password	Detector モジュールで定義した次の情報を消去します。 • すべてのユーザ パスワード • すべての TACACS+ 定義
clear ap config	Detector 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、すべての Detector モジュール設定、ログ、レポート、およびライセンス キー（インストールされている場合）を削除します。
ip address [*ip address*] [*subnet*]	Detector 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。

表 13-5　MP 関連のコマンド（続き）

コマンド	説明
show ip	Detector モジュールのネットワーク パラメータを表示します。
upgrade *ftp-url*	イメージをアップグレードします。ここで、ftp-url は、イメージがある FTP サーバとイメージへのパスを指定する 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　スーパーバイザ エンジンで次のコマンドを入力して、Detector モジュールを MP にリセットします。

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

slot_number 引数には、モジュールが挿入されているシャーシ内のスロットの番号を指定します。

ステップ 2　Detector モジュールがオンラインに戻ったら、Detector 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して、Detector　モジュールに設定されているすべてのパスワードを削除します。

```
clear ap password
```

ステップ 4　次のコマンドを入力して、Detector モジュールを AP にリセットします。

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

ステップ 5　Detector　モジュール上に設定されているユーザの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）。Detector 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絞り込んで、Detector モジュール ユーザのリストだけが含まれるようにするには、**show running-config | include username** コマンドを使用してください。

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、Detector モジュールの設定を、工場出荷時のデフォルト設定に戻す必要が生じる場合があります。工場出荷時のデフォルト設定へのリセットは、設定が複雑になった場合や、Detector 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、Detector モジュールに存在する不要な設定を削除するときに役立ちます。Detector モジュールを工場出荷時のデフォルト設定にリセットして、新しい Detector 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、Detector モジュールの設定をバックアップする必要があります。P.13-4 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設定（eth1）は、Detector モジュールをリロードするまで使用可能です。

注意　アウトオブバンド コンソール接続を使用して（利用可能な場合）、clear config all コマンドを実行します。Detector モジュールが clear config コマンドを実行すると設定がクリアされ、ユーザがリブート要求を確認するとリブートします。インライン SSH 接続を使用して clear config all コマンドを実行すると、clear config プロセスの途中で接続が解除され、Detector モジュールがリブートしません。スーパーバイザ エンジンに接続し、手動で Detector モジュールをリブートする必要があります。

Detector 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、Detector 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@DETECTOR-conf# clear config all
```