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作業を行う方法について説明します。

（注） 1 Gbps で動作する Guard モジュールと 3 Gbps で動作する Guard モジュールでは、動作と設定に違いがあります。この章では、1 Gbps 動作と 3 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モードの動作に適用されます。詳細については、P.1-12 の「1 Gbps と 3 Gbps の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

Guard モジュールでネットワーク サーバを定義し、Guard モジュールとそのサーバの間でファイルのインポートおよびエクスポートを行うことができます。Guard モジュールにより、ネットワーク サーバのプロファイルを作成し、その中で、IP アドレス、通信方式、およびログイン詳細などのネットワーク サーバのアトリビュートを定義できます。ネットワーク サーバのプロファイルを作成することにより、ファイルのインポートまたはエクスポート時にサーバ名を指定できます。

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）に依存するので、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.4-37 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 文字の英数字の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。英数字の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。

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
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。
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。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 に依存しています。したがって、**copy** コマンドに **sftp** または **scp** オプションを指定して入力する前に、Guard モジュールで使用される鍵を設定していない場合、Guard モジュールからパスワードの入力を求められます。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.4-37 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）ゾーン名を指定します。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（続き）

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	（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、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。
dest-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 はセキュアな通信を SSH に依存しています。したがって、**copy** コマンドに **sftp** または **scp** オプションを指定して入力する前に、Guard モジュールで使用される鍵を設定していない場合、Guard モジュールからパスワードの入力を求められます。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.4-37 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、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	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。

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

パラメータ	説明
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.13-27 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。xsd ファイルは www.cisco.com から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.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、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.13-19 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。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。**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 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

デフォルトにより、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。Guard モジュールは、リブート前のゾーンの動作状態に関係なく、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だったゾーンを Guard モジュールによって自動的にアクティブにできるようにするには、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

この項では、Guard モジュールが動作するために必要な次のソフトウェア コンポーネントについて説明します。

- Supervisor エンジン 2 または Supervisor エンジン 720 をサポートする Cisco IOS リリース
- Guard 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）

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。

この項では、次のトピックについて取り上げます。

Supervisor エンジン 2 または Supervisor エンジン 720 の Cisco IOS ソフトウェア

Cisco IOS ソフトウェア イメージは、Catalyst 6500 シリーズのスイッチまたは Cisco 7600 シリーズのルータの Supervisor エンジン 2 あるいは Supervisor エンジン 720 に常駐します。スーパーバイザ エンジンのイメージは、Guard モジュールとそのプロセッサを認識および初期化します。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 フラッシュは次のパーティションに分割され、それぞれに Guard モジュール ソフトウェア イメージがあります。

- 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 カードの制御機能で必要とされる Guard モジュールのメンテナンス ソフトウェア イメージが含まれています。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）：Guard　モジュールのアプリケーション ソフトウェア イメージが含まれています。スーパーバイザ エンジンは AP を cf:4 として識別します。

ソフトウェア イメージの一方または両方は、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 File Transfer Protocol（FTP; ファイル転送プロトコル）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）　Guard モジュール ソフトウェアをアップグレードして 1 Gbps から 3 Gbps に帯域幅を増大する場合は、P.14-29 の「1 Gbps から 3 Gbps への帯域幅のアップグレード」を参照してください。

Guard モジュールでは、次のアップグレード手順を使用できます。

- AP イメージ アップグレード手順：スーパーバイザ エンジン CLI を使用して AP イメージをアップグレードします。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 イメージ アップグレード手順：スーパーバイザ エンジン 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.14-19 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：Guard モジュール 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.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。
- Common Firmware Environment（CFE）：Guard モジュールの CFE をアップグレードします。新しい AP または MP イメージのインストール プロセスによって CFE もアップグレードされるため、CFE はアップグレードの必要がほとんどありません。CFE のアップグレードが必要になるのは、現在の CFE

と新しい MP または AP イメージの間に不適合があることを示すエラー メッセージが Guard モジュールに表示された場合だけです。P.14-27 の「新しいフラッシュ バージョンの焼き付けによる Common Firmware Environment のアップグレード」を参照してください。

アップグレード時の注意事項

AP と MP のソフトウェア イメージおよび CFE をアップグレードする場合は、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、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します。
- Guard モジュールを MP 動作モードに切り替えるには、**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。
- Guard モジュールを通常の動作モードである AP 動作モードに切り替えるには、**hw-module module** *slot_number* **reset cf:4** コマンドを使用します。
- **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。Guard モジュールが AP 動作モードで実行されている場合は、**show module** コマンドを実行すると AP イメージ 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。Guard モジュールが MP 動作モードで実行されている場合には、MP イメージ 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 ファイル名では、c6svc-agm-k9.5-0-3.bin 形式を使用します。
- 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

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 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.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.13-16 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.13-28 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、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。

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。接続速度に応じて、この操作には最大で 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。

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　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による Common Firmware Environment のアップグレード」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
```

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バージョンのソフトウェア リリースをダウンロードします。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 2　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 3　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 4　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、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　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。

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.14-34 の「MP 関連コマンドの使用」を参照してください。

ステップ 5　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 6　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。インライン イメージのアップグレードを実行する場合は、スーパーバイザ エンジンからではなく Guard 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、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.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.13-16 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.13-28 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、最新バージョンのソフトウェア イメージを入手します。ソフトウェア イメージを FTP にアクセス可能なディレクトリにコピーします。

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　Guard モジュールがメンテナンス イメージで動作している場合は、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。ルート アカウントのデフォルト 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、Guard モジュールをシャーシに装着するためのスロット番号（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、Guard モジュール プロセッサの番号です。Guard モジュールは、プロセッサ 1 を使用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による Common Firmware Environment のアップグレード」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による Common Firmware Environment のアップグレード

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、Guard 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。

Guard モジュールは、CFE との不適合を検出すると、ソフトウェア リリースのアップグレード後にユーザが Guard モジュールとの最初のセッションを確立するときに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） 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。

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
```

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
```

1 Gbps から 3 Gbps への帯域幅のアップグレード

Guard モジュールが現在、最大帯域幅 1 Gbps で動作している場合は、XG バージョンのソフトウェア イメージ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り、帯域幅を 3 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、Guard モジュールとスーパーバイザ エンジンの間の 3 つのインターフェイス ポートすべてをデータ トラフィックおよびインバンド管理トラフィックに対してアクティブにします。1 Gbps ソフトウェア イメージでは、データ トラフィック用に 1 つのインターフェイスのみを使用します。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化されます。詳細については、P.1-12 の「1 Gbps と 3 Gbps の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すると、対応するソフトウェア ライセンスをインストールし、3 Gbps 動作で必要な設定の変更を行うまで、Guard モジュールは動作しません。設定の変更には、次の項目が含まれます。

- インターフェイス設定：スーパーバイザ エンジンと Guard モジュールの新しいインターフェイスで、IP アドレスと VLAN を設定します。
- プロキシ：Guard モジュールの新しいインターフェイスでプロキシを設定します。
- SSL 証明書：Guard モジュールおよび関連付けられたすべての Detector 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、Guard モジュールの次の項目に影響はありません。

- ゾーン設定：既存のゾーン設定情報は変更されません。
- 管理アクセス：1 Gbps 動作の eth1 で設定した設定パラメータは、3 Gbps 動作の giga1 に自動的に割り当てられます。

この項では、次のトピックについて取り上げます。

3 Gbps 動作の XG ソフトウェア イメージの入手とインストール

XG ソフトウェア イメージのコピーを入手して Guard モジュールにインストールするには、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。

XG ソフトウェア イメージがロードされている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ている場合は、ソフトウェア バージョン番号の後に XG と表示されます。

XG ソフトウェア イメージ ライセンス キーの入手とインストール

XG ソフトウェア イメージのアクティブ化に必要なライセンス キーは、XG ソフトウェア イメージが常駐する Guard モジュールの Media Access Control（MAC; メディア アクセス制御）アドレスと結び付いています。この項では、XG ソフトウェア ライセンス キーを注文する際のプロセスについて説明します。

（注） 対応するライセンスを注文およびインストールする前に、ご使用の Guard モジュールに XG バージョン 6.0（以降）のオペレーティング ソフトウェアをインストールしておく必要があります。ご使用の Guard モジュールに現在ロードされている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ている場合は、ソフトウェア バージョン番号に -XG 接尾辞が付きます（たとえば、バージョン 6.0(0.39)-XG）。

3 Gbps ライセンスを入手して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　Guard モジュールから **show license-key unique-identifier** コマンド（このコマンドでは、管理者特権レベルが必要です）を入力し、Guard モジュールの MAC アドレスを表示します。

ステップ 2　3 Gbps 動作ライセンスの注文時に必要になるため、MAC アドレス情報を控えておきます。

ステップ 3　cisco.com で利用可能な シスコの注文ツールのいずれかを使用して、lic-agm-3g-k9 ライセンスを注文します。

ステップ 4　シスコから Software License Claim Certificate を受け取ったら、指示に従って次の cisco.com Web サイトにアクセスします。

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

ステップ 5　購入の証明として、Software License Claim Certificate に記載されている Product Authorization Key（PAK）番号を入力します。

ステップ 6　要求される情報すべてを入力してライセンス キーを生成します。

システムによってライセンス キーが生成されると、ライセンス ファイルとインストールの指示を添付したライセンス キー E メールが送信されます。今後必要が生じる場合に備えて、そのライセンス キー E メールを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、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　Guard 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。CLI に、ライセンス キー行の入力を求める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内容（ライセンス キーを含む）を貼り付け、**Enter** キーを押します。

ステップ 10　空白行を入力して **Enter** キーを押します。Guard モジュールに以前にインストールされたライセンスが含まれている場合は、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）と入力します。XG ソフトウェア イメージがアクティブになり、3 Gbps 動作の準備が整います。

ステップ 12　（オプション）**show license-key** コマンドを入力して、キーが正しくロードされ、有効になっていることを確認します。

3 Gbps 動作に向けた既存ポートとインターフェイス設定のアップデート

XG ソフトウェア イメージをインストールしてアクティブにすることにより、スーパーバイザ エンジンと Guard モジュールの間のデータ トラフィックは、1 つのインターフェイス ポートだけでなく 3 つのインターフェイス ポートを使用して移動できます。3 Gbps 動作をアクティブ化するより前に、スーパーバイザ エンジンと Guard モジュールに 1 つのインターフェイス ポートのインターフェイス設定がすでに存在していた場合は、両方のデバイスでインターフェイス設定をアップデートし、2 つの追加インターフェイスを組み込む必要があります。3 つのインターフェイス ポートを設定するには、次のタスクを実行します。

- スーパーバイザ エンジンから、**anomaly-guard module** コマンドを使用して Guard モジュールに VLAN を割り当てます。データ トラフィック VLAN を Guard モジュールに割り当てる場合は、3 つのスーパーバイザ エンジン ポートすべてに VLAN を割り当てる必要があります。詳細については、P.2-5 の「管理およびデータ トラフィックの VLAN の設定」を参照してください。
- Guard モジュールで、次のタスクを実行します。
  - 設定モードで **interface** コマンドを使用し、次にインターフェイス設定モードで **ip address** コマンドを使用することによって、3 つの物理インターフェイスすべてに IP アドレスを設定します。IP アドレスは、インターフェイスごとに固有であり、すべて同じサブネットに属する必要があります。インターフェイス設定モードで **no shutdown** コマンドを使用することにより、インターフェイスをアクティブにします。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。
  - 設定モードで **interface** コマンドを使用し、次にインターフェイス設定モードで **ip address** コマンドを使用することによって、3 つの物理インターフェイスすべてにおいて各データ トラフィック VLAN を定義します。インターフェイス設定モードで **no shutdown** コマンドを使用することにより、インターフェイスをアクティブにします。詳細については、P.3-14 の「Guard モジュールのインターフェイスでの VLAN の設定」を参照してください。

3 Gbps 動作のインターフェイスでのプロキシの設定

設定モードで **proxy** コマンドを使用することにより、Guard モジュールの各インターフェイスに最低でも 1 つのスプーフィング防止プロキシ IP アドレスを設定します。詳細については、P.3-20 の「プロキシ IP アドレスの設定」を参照してください。

（注） 3 つのインターフェイス ポートを設定し、インターフェイスのそれぞれでプロキシを定義したら、グローバル モードまたは設定モードで **validate network-config** コマンドを入力することにより、トラフィックの宛先変更用に 3 つのインーフェイスが正しく設定されていることを確認します（P.5-33 の「Guard モジュールのネットワーク設定の検証」を参照）。

3 Gbps 動作の SSL 証明書の再生成

Guard モジュールは、Secure Sockets Layer（SSL）証明書を使用して、関連付けられた Detector との安全な通信チャネルを確立します。1 Gbps ソフトウェア イメージを 3 Gbps ソフトウェア イメージにアップグレードすると、Guard モジュールから既存の SSL 証明書がすべて削除されます。3 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は、安全な通信チャネルを確立するために Guard モジュールおよび関連付けられた Detector が使用する SSL 証明書を再生成する必要があります。関連付けられた Detector の場合、新しい証明書を生成する前に、まず既存の SSL 証明書を削除する必要があります。

詳細については、P.4-28 の「SSL 通信チャネルの設定」を参照してください。

MP 関連コマンドの使用

ユーザは、Guard モジュールを MP に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 にブートするには、**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 関連の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	Guard モジュールをデフォルト設定に戻します。このコマンドにより、すべての Guard モジュール設定、ログ、レポート、および（インストールされている場合は）ライセンス キーが削除されます。
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。

表 14-5　MP 関連のコマンド（続き）

コマンド	説明
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。
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状態に戻す必要が生じます。設定を工場出荷時の状態に戻す処理は、Guard モジュールの不要な設定を削除する場合や設定が複雑になってしまった場合、またはネットワークから別のネットワークに Guard モジュールを移動する場合に役立ちます。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。

注意　アウトオブバンド コンソール接続（使用可能な場合）を使用して、clear config all コマンドを実行します。Guard モジュールで clear config コマンドを実行すると、設定がクリアされ、続いてリブート要求の確認後にリブートが実行されます。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 プロセスの間は切断され、Guard モジュールがリブートしません。その後、スーパーバイザ エンジンに接続して Guard モジュールを手動でリブートする必要があります。

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
```