CHAPTER 13

メンテナンス タスクの実行

この章では、Cisco Guard（Guard）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 ファイルをエクスポートしたり、Guard 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 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 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 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.3-40 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 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 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 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 の設定パラメータを別の Guard に実装する。
- Guard の設定をバックアップする。

Guard 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 が使用する鍵を設定していない場合、Guard はパスワードの入力を要求します。Guard 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.3-40 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。ゾーン名を指定すると、Guard 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 の設定ファイルがエクスポートされます。
running-config	Guard 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 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
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い場合、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 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 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。
destination-file-name	リモート サーバ上の設定ファイルの名前。Guard 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 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 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 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 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 の既存の設定ファイルに基づいて Guard を設定する。
- Guard の設定を復元する。

ゾーンの設定は、Guard 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 にコピーし、それに応じて Guard 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 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。Guard では、ゾーン設定をインポートする前に、ゾーンが非アクティブになります。

Guard 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 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 は安全な通信を SSH に依存しているので、**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 が使用する鍵を設定していない場合、Guard はパスワードの入力を求めます。Guard 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.3-40 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い場合、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 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 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。Guard 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パスにファイルの名前を追加します。

次の例は、Guard 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 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された設定をインポートすると、Guard では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 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 が次のメッセージを表示します。

  ```
  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 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 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.12-25 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

  ゾーンに対する攻撃が終了すると、Guard から任意のゾーンのレポートがエクスポートされます。詳細については、P.11-20 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 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.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、Guard 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 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。Guard 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.12-16 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。ゾーンに対する攻撃が終了すると、Guard から任意のゾーンのレポートがエクスポートされます。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.11-20 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 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 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 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 をリロードする必要があります。

- Guard と Network Time Protocol（NTP; ネットワーク タイム プロトコル）サーバの同期
- **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
- **no shutdown** コマンドを使用した、giga0 インターフェイスのイネーブル化
- 新しいフラッシュの組み込み

Guard のリブートおよびゾーンの非アクティブ化

Guard をリブートするには、グローバル モードで次のコマンドを入力します。

reboot

Guard のデフォルトの動作では、すべてのゾーンが非アクティブな動作状態でロードされます。このため、Guard では、リブート前のゾーンの動作状態に関係なく、リブート後のゾーンの保護やラーニング プロセスはイネーブルになりません。

デフォルトの動作を変更して、リブート プロセスの前にアクティブであったゾーンを自動的にアクティブにするには、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 のシャットダウン

完全なシャットダウンにより、Guard は重要な情報を保存することができます。

Guard をシャットダウンするには、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ます。

```
poweroff
```

ステップ 2　コマンド プロンプトで **yes** と入力し、プロセスを確認します。

ステップ 3　Guard の電源制御ボタンを押して、電源を切ります。

緑色の電源 LED が消えます。

注意　**poweroff** コマンドを入力せずに電源制御ボタンを押すと、重大なデータの損失につながる恐れがあります。

Guard のソフトウェア バージョンのアップグレード

Guard のソフトウェア バージョン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 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.11-21 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.11-23 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.12-13 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.12-26 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　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、SFTP または SCP でアクセスできる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　グローバル モードで次のいずれかのコマンドを入力して、ネットワーク サーバから Guard ソフトウェアにソフトウェア バージョンをコピーします。

- **copy ftp new-version** *server full-file-name* [*login* [*password*]]
- **copy** {**sftp** | **scp**} **new-version** *server full-file-name login*

SFTP および SCP は安全な通信を SSH に依存しているので、**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 が使用する鍵を設定していない場合、Guard はパスワードの入力を求めます。Guard 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.3-40 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 13-5 に、**copy new-version** コマンドの引数を示します。

表 13-5　copy new-version コマンドの引数

パラメータ	説明
ftp	FTP サーバからバージョン ファイルをダウンロードします。
sftp	SFTP サーバからバージョン ファイルをダウンロードします。
scp	SCP サーバからバージョン ファイルをダウンロードします。
server	サーバの IP アドレス。
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 ディレクトリからファイルをコピーします。
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い場合、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 によってパスワードを要求されます。

ステップ 5　次のコマンドを入力して、ダウンロードしたバージョンをインストールします。

```
install new-version
```

install new-version コマンドを入力すると、ラーニング プロセスと保護プロセスが非アクティブになります。

注意　バージョンをアップグレードしている間は、Guard に安定して電源が供給されるようにし、かつ Guard を動作させないようにする必要があります。アップグレード プロセスが完了した後、Guard は「Press Enter to close this CLI session.」というメッセージを表示します。上記の制限に対応できない場合、アップグレードが失敗したり、Guard にアクセスできなくなる可能性があります。

ステップ 6　**show version** コマンドを入力して、Guard との新しいセッションを確立し、ソフトウェア バージョンを確認します。

次の例は、新しいソフトウェア バージョン ファイルを Guard にコピーして、ソフトウェア バージョンをアップグレードする方法を示しています。

```
user@GUARD# copy ftp new-version 10.0.0.191 /home/Versions/R3.i386.rpm
user <password>
FTP in progress...
user@GUARD# install new-version
.
.
.
Press Enter to close this CLI session.
```

ソフトウェアのバージョンをアップグレードすると、Guard の自己保護設定が自動的に新しくアップデートされます。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。

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 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、**install new-version** コマンド（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 バージョンを示す）を入力すると、Guard から次のメッセージが表示されます。「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 に安定して電源が供給されるようにし、かつ Guard 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 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 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 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 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
```

忘失パスワードの復旧

Guard は、ルート パスワードを使用してルート アクセスを制御します。ルート パスワードは暗号化されているため、新しいパスワードで置き換えることしかできません。

ルート 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 にキーボードとモニタを接続します。

ステップ 2　ログインして、**reboot** コマンドを入力します。

ステップ 3　Guard の起動中、Shift キーを押して、そのまま押し続けます。

Guard が次のプロンプトを表示します。

```
Lilo:
```

ステップ 4　次のコマンドを入力し、1 つのユーザ イメージをロードします。

```
Cisco 1
```

（注）　3.0.8 より前のバージョンを実行している場合は、**Riverhead 1** と入力してください。実行しているバージョンが分からない場合は、**Tab** キーを押して、イメージのリストを表示してください。

ステップ 5　パスワード プロンプトで **Enter** キーを押して、ヌル パスワードを入力します。

Guard がルート プロンプトに入ります。

ステップ 6　ルートのパスワードを変更するには、**passwd** コマンドを使用します。
New password プロンプトで、新しいパスワードを入力します。Retype new password プロンプトで新しいパスワードを再度入力し、選択を確認します。

次の例は、ルート パスワードを変更する方法を示しています。

```
[root@GUARD root]# passwd
    Changing password for user root.
    New password: <new password typed in here>
    Retype new password: <new password typed in here>
    passwd: all authentication tokens updated successfully.
```

ステップ 7　通常の動作モードで **reboot** コマンドを使用して、Guard を再起動します。

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 の設定を、工場出荷時のデフォルト設定に戻し、工場出荷時のデフォルト設定にリセットするほうが有効な場合があります。これは、設定が複雑になった場合や、Guard 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 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 を工場出荷時のデフォルトにリセットして、新しい Guard 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 の設定をバックアップすることをお勧めします。P.13-4 の「設定のエクスポート」を参照してください。

Guard をリロードするまでは、インバンド インターフェイスの設定（eth0）を利用できます。

注意　Guard 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 をリロードした場合、Guard への接続は失われます。

Guard 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 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
```