CHAPTER 11

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。この章には、次の項があります。

設定のエクスポート

Guard の設定ファイルを FTP サーバや SFTP 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（running-config）をリモート サーバにエクスポートすると、次のことが可能になります。

- 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** *server full-file-name login*

（注）　**copy reports** コマンドを入力する前に、Guard が SFTP 通信に使用する SSH 鍵を設定する必要があります。詳細については、P.3-36 の「SFTP 接続のための鍵の設定」を参照してください。

表 11-1 で、**copy running-config ftp** コマンドの引数について説明します。

表 11-1　copy running-config ftp コマンドの引数

パラメータ	説明
zone-name	（オプション）ゾーン名。ゾーンの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	設定を FTP サーバにエクスポートします。
sftp	設定を SFTP サーバにエクスポートします。
server	サーバの IP アドレス。
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 ディレクトリにファイルを保存します。

表 11-1　copy running-config ftp コマンドの引数（続き）

パラメータ	説明
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。パスワードを挿入しない場合、Guard によってパスワードを要求されます。

次の例を参考にしてください。

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

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。次の目的で設定をインポートします。

- 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）　既存の設定が新しい設定で上書きされます。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入力します。

- **copy ftp running-config** *server full-file-name* [*login* [*password*]]
- **copy sftp running-config** *server full-file-name login*

（注）　**copy reports** コマンドを入力する前に、Guard が SFTP 通信に使用する SSH 鍵を設定する必要があります。詳細については、P.3-36 の「SFTP 接続のための鍵の設定」を参照してください。

表 11-2 で、**copy ftp running-config** コマンドの引数について説明します。

表 11-2　copy ftp running-config コマンドの引数

パラメータ	説明
zone-name	（オプション）ゾーン名。ゾーンの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。
ftp	設定を FTP サーバからインポートします。
sftp	設定を SFTP サーバからインポートします。
server	サーバの IP アドレス。
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。パスワードを挿入しない場合、Guard によってパスワードを要求されます。

次の例を参考にしてください。

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

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。

ディスク スペースの管理

Guard は、アクティビティ ログおよびゾーン攻撃レポートを保持します。ディスクの使用率が 75% を超えている場合、または Guard に多数のゾーン（500 を超える）が定義されている場合は、ファイル履歴パラメータの値を小さくすることをお勧めします。使用されているディスク スペースがディスクの最大キャパシティの約 80% に達すると、Guard は syslog に警告メッセージを入力します。このような場合は、次のいずれかを行うことができます。

1. Guard またはゾーンのログを FTP サーバにエクスポートする：P.10-11 の「ログ ファイルのエクスポート」を参照

   Guard のレポート リストを FTP サーバにエクスポートする：P.9-19 の「攻撃レポートのエクスポート」を参照

   ゾーン攻撃レポートを FTP サーバにエクスポートする：P.9-19 の「攻撃レポートのエクスポート」を参照
2. ログ ファイルをクリアする：P.10-12 の「ログ ファイルのクリア」を参照
3. ログ ファイルおよび攻撃レポートの履歴サイズを小さくする：P.11-8 の「ログとレポートの履歴の設定」を参照

Guard のレコードを FTP サーバに定期的に格納してから、ログをクリアすることをお勧めします。

（注）　ディスク使用率がディスクの最大キャパシティの 80% に達すると、Guard は情報を消去して、ディスク使用率を約 75% に減らします。

ディスク使用率を表示するには、次のコマンドを入力します。

show disk-usage

次の例を参考にしてください。

```
user@GUARD# show disk-usage
2%
```

ログとレポートの履歴の設定

Guard が Guard とゾーンの両方のログおよび攻撃レポートを記録しておく期間を設定できます。

レポートおよびログの履歴を設定するには、次のコマンドを入力します。

history {logs | reports} *days* **[enforce-now]**

表 11-3 で、**history** コマンドの引数とキーワードについて説明します。

表 11-3　history コマンドの引数とキーワード

パラメータ	説明
logs	Guard およびゾーンのログの履歴パラメータを設定します。
reports	ゾーン攻撃レポートの履歴パラメータを設定します。
days	履歴期間。ログの履歴期間は 1 ～ 7 日です。レポートの履歴期間は 1 ～ 60 日です。 デフォルトの履歴期間は、ログの場合 7 日、レポートの場合 30 日です。
enforce-now	(オプション) 記録されたログおよびレポートの履歴キャパシティを、現在のコマンド パラメータにすぐに適合させます（必要に応じてログおよびレポートを消去します)。

履歴を短い期間に設定した場合は、ログ ファイルおよびレポート ファイルのサイズを小さくして、新しく設定したサイズに合せます。次のいずれかを行うことができます。

- **enforce-now** オプションを使用する。

  または

- 後で、新しく設定したサイズに合うように、格納されているログおよびレポートを消去するため、**disk-clean** コマンドを使用する。

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 の設定をリロードできます。

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

Guard をリブートするには、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 の電源オフ

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 の電源をオフにするには、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 ON/OFF ボタンを押して、Guard の電源を切ります。緑色の電源 LED が消えます。

注意　**poweroff** コマンドを発行せずに OFF 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 のバージョンのアップグレード

管理者は、Guard のソフトウェア バージョンをアップグレードできます。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。詳細については、P.11-2 の「設定のエクスポート」を参照してください。

ステップ 2　Guard ソフトウェアのアップデートされたバージョンを FTP サーバまたは SFTP サーバからダウンロードします。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 ftp new-version** *server full-file-name* [*login* [*password*]]
- **copy sftp new-version** *server full-file-name login*

（注）　**copy reports** コマンドを入力する前に、Guard が SFTP 通信に使用する SSH 鍵を設定する必要があります。詳細については、P.3-36 の「SFTP 接続のための鍵の設定」を参照してください。

表 11-4 で、**copy ftp new-version** コマンドの引数について説明します。

表 11-4　copy ftp 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。
server	サーバの IP アドレス。
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 ディレクトリからファイルをコピーします。

表 11-4　copy ftp new-version コマンドの引数（続き）

パラメータ	説明
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。パスワードを挿入しない場合、Guard によってパスワードを要求されます。

ステップ 3　ダウンロードしたバージョンをインストールします。次のコマンドを入力します。

```
install new-version
```

install new-version コマンドを発行すると、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 プロセスが完了すると、Guard で次のメッセージが表示されます。

```
Press Enter to close this CLI session.
```

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。

ステップ 4　Guard との新しいセッションを確立して、ソフトウェア バージョンを確認します。**show version** コマンドを使用します。

次の例を参考にしてください。

```
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.
```

AP をアップグレードすると、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 バージョン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）を発行すると、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 をリロードします。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 コマンドを発行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。

次の例を参考にしてください。

```
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

この項では、ルート ユーザのパスワードを復旧する方法について説明します。Guard は、この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。

この手順を実行するには、Guard コンソールに接続する必要があります。

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、reboot と入力します。

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　次のように入力し、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。

次の例を参考にしてください。

```
[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　**reboot** コマンドを使用し、Guard を再起動して通常の動作モードに入ります。

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、元の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。この機能は、Guard に前から存在する好ましくない設定を削除するときに役立ちます。従来の Guard の設定がとても複雑になっている場合や、Guard をネットワーク間で移動する場合などです。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.11-2 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。

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入力します。

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。

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。

次の例を参考にしてください。

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