CHAPTER 10

Guard の診断とメンテナンス

この章では、Guard の一般的なケアや保守用の作業を行う方法、および Cisco Guard（Guard）に関する統計情報や診断を表示する方法について説明します。この章には、次の項があります。

ゾーンの表示

Guard でゾーンの概要を表示して、アクティブなゾーンやゾーンの現在のステータスを確認できます。ゾーンのリストを表示するには、グローバル プロンプトで **show** コマンドを使用します。表 10-1 で、さまざまなゾーン ステータスについて説明します。

表 10-1　ゾーンのステータス

ステータス	説明
Auto Protection mode	ゾーンは自動保護モードです。ユーザの介入なしに動的フィルタがアクティブになります。
Interactive Protection mode	ゾーンはインタラクティブ保護モードです。動的フィルタは手動でアクティブにされます。
Threshold Tuning phase	ゾーンはしきい値調整ラーニング フェーズです。Guard は、ゾーンのトラフィックを分析して、ポリシー構築フェーズ中に構築されたポリシーのしきい値を定義します。
Policy Construction phase	ゾーンはポリシー構築フェーズです。ゾーンのポリシーが作成されます。
Standby	ゾーンはアクティブではありません。

例

```
admin@GUARD# show
```

Guard のログの表示

Guard は、システムのアクティビティおよびイベントを自動的にログに記録します。Guard のログを表示して、Guard のアクティビティを確認および追跡できます。

表 10-2 に、イベント ログのレベルを示します。

表 10-2　イベント ログのレベル

イベント レベル	数値コード	説明
Emergencies	0	システムを使用できません。
Alerts	1	緊急のアクションが必要です。
Critical	2	危険な状態。
Errors	3	エラー状態。
Warnings	4	警告状態。
Notifications	5	正常だが、重要な状態。
Informational	6	情報メッセージ。
Debugging	7	デバッグ メッセージ。

ログ ファイルには、すべてのログ レベル（emergencies、alerts、critical、errors、warnings、notification、informational、debugging）が表示されます。Guard のログ ファイルには、emergencies、alerts、critical、errors、warnings、および notification という重大度を持つゾーン イベントが含まれます。

イベント ログは、ローカルで表示することも、リモート サーバから表示することもできます。

- イベントのリアルタイム ロギング：P.10-4 の「オンライン イベント ログの表示」を参照してください。
- ログ ファイル：P.10-6 の「ログ ファイルの表示」を参照してください。

オンライン イベント ログの表示

Guard のモニタリング メカニズムをアクティブにして、リアルタイムのイベント ログを表示できます。この設定により、Guard のイベントのオンライン ロギングを表示できます。次のコマンドを入力します。

event monitor

次の例を参考にしてください。

```
admin@GUARD# event monitor
```

画面はイベントで常にアップデートされます。

（注）　モニタリング メカニズムを非アクティブにするには、**no event monitor** コマンドを使用してください。

オンライン イベント ログのエクスポート

Guard のオンライン イベント ログをエクスポートして、Guard のログ ファイルに記録されている Guard の動作を表示できます。Guard のイベントは Guard のログ ファイルにオンラインで記録されるため、リモート ホストからそのイベントを表示できます。Guard のログ ファイルは、syslog メカニズムを使用してエクスポートされ、複数の Syslog サーバにエクスポートできます。1 つのサーバがオフラインになったときに別のサーバでメッセージを受信できるように、追加のサーバを指定できます。

（注）　Guard のオンライン イベント ログは、syslog サーバだけにエクスポートできます。リモート syslog サーバが使用できない場合は、**copy log** コマンドを使用して、Guard のログ ファイルをエクスポートしてください。

syslog メッセージの形式は、次のとおりです。

<イベントの日付><イベントの時刻><Guard の IP アドレス><Guard のモジュール><ゾーン名><イベントの重大度><イベントのタイプ><イベントの説明>

イベント ログの例は、次のとおりです。

```
Sep 11 16:34:40 10.4.4.4 cm: scannet, 5 threshold-tuning-start: Zone
activation completed successfully.
```

オンライン イベント ログを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　（オプション）ロギング パラメータを設定します。次のコマンドを入力します。

```
logging {facility | trap}
```

表 10-3 で、**logging** コマンドのキーワードについて説明します。

表 10-3　logging コマンドのキーワード

パラメータ	説明
facility	エクスポート syslog ファシリティ。使用できるファシリティは、local0 ～ local7 です。デフォルトは local4 です。
trap	リモート syslog に送信する syslog トラップの重大度。重大度のトラップ レベルには、それより高い重大度のレベルが含まれます。たとえば、トラップ レベルを **warning** に設定すると、error、critical、alerts、および emergencies も送信されます。指定できるトラップ レベルは、高い方から順に emergencies、alerts、critical、errors、warnings、notification、informational、debugging です。デフォルトは notification です。

（注）　動的フィルタの追加および削除に関するイベントを受信するには、トラップ レベルを informational に変更してください。

ステップ 2　リモート syslog サーバの IP アドレスを設定します。次のコマンドを入力します。

logging host *remote-syslog-server-ip*

または

export log *remote-syslog-server-ip*

引数 *remote-syslog-server-ip* には、リモート Syslog サーバの IP アドレスを指定します。

（注）　ロギング メッセージを受信する syslog サーバのリストを作成するには、このコマンドを複数回入力してください。

次の例を参考にしてください。

```
admin@GUARD-conf# logging facility local3
admin@GUARD-conf# logging trap notifications
admin@GUARD-conf# logging host 10.0.0.191
```

オンライン イベント ログのエクスポート設定を表示するには、**show logging** コマンドまたは **show log export-ip** コマンドを使用します。

ログ ファイルの表示

診断または監視のために Guard のログを表示できます。Guard のログ ファイルには、emergencies、alerts、critical、errors、warnings、および notification という重大度を持つゾーン イベントが含まれます。

Guard のログを表示するには、次のコマンドを入力します。

show log

ゾーンのログを表示して、指定したゾーンだけに関連するイベントを確認できます。

次の例を参考にしてください。

```
admin@GUARD# show log
```

ログ ファイルのエクスポート

監視または診断のために、Guard のログ ファイルを FTP サーバにエクスポートできます。次のコマンドを入力します。

copy [zone *zone-name***] log ftp** *server full-file-name* [*login*] [*password*]

表 10-4 で、**copy log ftp** コマンドの引数とキーワードについて説明します。

表 10-4　copy log 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。ゾーンのログ ファイルをエクスポートします。デフォルトでは、Guard のログ ファイルがエクスポートされます。
server	FTP 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 ディレクトリにファイルを保存します。
login	（オプション）FTP サーバのログイン名。 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、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。

```
admin@GUARD# copy log ftp 10.0.0.191 log.txt user <password>
```

ログ ファイルのクリア

Guard またはゾーンのログ ファイルのすべてのエントリを消去できます。

ヒント　Guard またはゾーンのログ ファイルが大きい場合、またはテストを行う予定で、ログ ファイルがテスト セッションからの情報だけを反映するようにしたい場合は、ログ ファイルをクリアしてください。

次のコマンドを入力します。

clear [zone *zone-name***] log**

引数 *zone-name* には、ゾーン名を指定します。デフォルトでは、Guard のログがクリアされます。

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.10-7 の「ログ ファイルのエクスポート」を参照
2. Guard のレポート リストを FTP サーバにエクスポートする：P.9-17 の「攻撃レポートのエクスポート」を参照
3. ゾーン攻撃レポートを FTP サーバにエクスポートする：P.9-17 の「攻撃レポートのエクスポート」を参照
4. ログ ファイルをクリアする：P.10-8 の「ログ ファイルのクリア」を参照
5. ファイル履歴サイズを小さくする：P.10-10 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、次のように入力します。

show disk-usage

次の例を参考にしてください。

```
admin@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、次のように入力します。

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

表 10-5 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 10-5　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わせます。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。**disk-clean** コマンドを使用します。

Guard の設定のコピー

Guard の設定ファイルを FTP 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 FTP 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。

設定のエクスポート

Guard の設定ファイルをエクスポートするには、次のコマンドを入力します。

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

表 10-6 で、**copy running-config ftp** コマンドの引数について説明します。

表 10-6　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。
server	FTP 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 ディレクトリにファイルを保存します。
login	（オプション）FTP サーバのログイン名。 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、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。

```
admin@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。

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。

（注）　ゾーンの設定は、Guard の設定の一部です。**copy ftp running-config** コマンドは、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 を再設定するために使用されます。

Guard の設定ファイルをインポートするには、次のコマンドを入力します。

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

表 10-7 で、**copy ftp running-config** コマンドの引数について説明します。

表 10-7　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。
server	FTP 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 ディレクトリにファイルを保存します。
login	（オプション）FTP サーバのログイン名。 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、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。

```
admin@GUARD# copy ftp running-config 10.0.0.191 scannet-conf
```

Guard の診断

この項では、Guard の診断に役立つコマンドのグループについて説明します。これらのコマンドは、次のような機能を実行します。

- 一般的な診断データの表示
- メモリ消費量の表示
- CPU 使用率の表示
- ARP キャッシュの操作
- Netstat
- Traceroute
- Ping
- デバッグ情報の取得

一般的な診断データの表示

Guard の一般的な診断データを表示できます。

一般的な診断データを表示するには、次のコマンドを入力します。

show diagnostic-info

診断データは、次の情報で構成されます。

- **Accelerator card CPU speed**:アクセラレータ カードの CPU 速度を示します。
- **Accelerator card revision**:アクセラレータ カードのリビジョン番号を示します。
- **Accelerator card serial**：アクセラレータ カードのシリアル番号を示します。
- **CFE version**：CFE のバージョン番号。

（注）　CFE のバージョンを変更するには、新しいフラッシュ バージョンをインストールする必要があります。CFE の新しいバージョンを焼き付けるには、**flash-burn** コマンドを使用してください。

- **Recognition Average Sample Loss**：認識モジュールの、計算されたパケット サンプル損失。
- **Forward failures (no resources)**：システム リソースが不足しているために転送されなかったパケット数。

（注）　**Recognition Average Sample Loss** または **Forward failures** の値が大きい場合は、テクニカルサポートに連絡してください。

- **Fan Speeds**：搭載されている各ファンの速度。この値は、最大 RPM のパーセンテージです。
- **Maximum Fans**：システムがサポートするファンの最大数。
- **Installed Fans**：システムに現在搭載されているファンの数。
- **Running Fans**：動作中のファンのリスト。
- **System uptime**：システムに電源が入っている時間数。
- **The number of system restarts**：システムが再起動された回数。
- **Blue Light state**：青い LED 状態。
- **System UUID**：システムの Universal Unique ID（UUID）。
- **CPU Temperature**：搭載されている各 CPU の現在の温度（摂氏）。
- **DASD Temperature**：ハード ディスク ドライブの現在の温度（摂氏）。
- **Ambient Temperature**：システムの周囲温度（摂氏）。

Guard には、内部のステータスを示すいくつかの LED があります。これらの LED は、通常、オフになっています。オンになった場合は、ハードウェアの障害を示します。そのような場合は、Guard が syslog メッセージと SNMP トラップを発行し、問題を通知します。

メモリ消費量の表示

Guard のメモリ消費量を表示できます。Guard は、メモリ使用量を KB 単位で表示します。さらに、Guard は、認識モジュールが使用しているメモリのパーセンテージも表示します。認識モジュールのメモリ使用率は、アクティブなゾーンの数、および各ゾーンが監視するサービスの数に影響されます。

（注）　認識モジュールのメモリ使用率が 90% を超えた場合は、アクティブなゾーンの数を減らすことを強くお勧めします。

次のコマンドを入力します。

show memory

次の例を参考にしてください。

```
admin@GUARD# show memory
              total    used    free    shared   buffers   cached
  In KBytes:  2065188  146260  1918928    0     2360      69232

  Recognition Used Memory: 0.3%
```

（注）　Guard の空きメモリの合計量は、**free** メモリと **cached** メモリの合計です。

CPU 使用率の表示

現在の CPU 使用率（パーセンテージ）を表示できます。Guard は、ユーザ モード、システム モード、ナイス値が負のタスク、およびアイドル状態の CPU 時間のパーセンテージを表示します。ナイス値が負のタスクは、システム時間およびユーザ時間にもカウントされるため、CPU 使用率の合計が 100% を超えることがあります。

次のコマンドを入力します。

show cpu

次の例を参考にしてください。

```
admin@GUARD# show cpu
Host CPU:  0.0% user,  0.1% system,  0.0% nice, 99.0% idle
```

ARP キャッシュの操作

ARP キャッシュを表示または操作して、アドレス マッピング エントリを消去または手動で定義できます。次のいずれかを入力します。

arp [**-evn**] [**-H** *type*] [**-i** *if*] **-a** [*hostname*]

arp [**-v**] [**-i** *if*] **-d** *hostname* [**pub**]

arp [**-v**] [**-H** *type*] [**-i** *if*] **-s** *hostname hw_addr* [**temp**]

arp [**-v**] [**-H** *type*] [**-i** *if*] **-s** *hostname hw_addr* [**netmask** *nm*] **pub**

arp [**-v**] [**-H** *type*] [**-i** *if*] **-Ds** *hostname* ifa [**netmask** *nm*] **pub**

arp [**-vnD**] [**-H** *type*] [**-i** *if*] **-f** [*filename*]

表 10-8 で、**arp** コマンドの引数とキーワードについて説明します。

表 10-8　arp コマンドの引数とキーワード

パラメータ	説明
-v、**--verbose**	出力を詳細に表示します。
-n、**--numeric**	数値アドレスを表示します。
-H *type*、**--hw-type** *type*、**-t** *type*	Guard がチェックするエントリのクラスを指定します。このパラメータのデフォルト値は、ether（IEEE 802.3 10Mbps イーサネットに対応するハードウェア コード 0x01）です。
-a [*hostname*]、**--display** [*hostname*]	指定したホストのエントリを代替（BSD）形式で表示します。デフォルトでは、すべてのエントリが表示されます。
-d *hostname*、**--delete** *hostname*	指定したホストのエントリを削除します。
-D、**--use-device**	インターフェイス ifa のハードウェア アドレスを使用します。
-e	エントリをデフォルトの形式で表示します。

表 10-8　arp コマンドの引数とキーワード（続き）

パラメータ	説明
-i *If*、**--device** *If*	インターフェイスを指定します。ARP キャッシュをダンプすると、指定したインターフェイスに一致するエントリだけが出力されます。永続的または一時的な ARP エントリを設定する場合、このインターフェイスがそのエントリに関連付けられます。このオプションを使用しない場合、Guard はルーティングテーブルに基づいて推測します。pub エントリの場合、これは ARP 要求に応えるインターフェイスです。これは、IP データグラムのルーティング先のインターフェイスとは異なる必要があります。
-s *hostname hw_addr*、**--set** *hostname*	ハードウェア アドレスを *hw_addr* クラスに設定して、ホスト *hostname* の ARP アドレス マッピング エントリを作成します。ほとんどのクラスでは、通常の表現を使用できます。
-f *filename*、**--file** *filename*	ARP アドレス マッピング エントリを作成します。情報は、ファイル *filename* から取得されます。ファイル形式は、ホスト名とハードウェア アドレスが空白で区切られた ASCII テキスト行です。pub、temp、および netmask フラグを使用することもできます。ホスト名を入力するどの場所にも、ドット区切り 10 進表記で IP アドレスを入力できます。

注意　Guard の ARP キャッシュを設定するには、Guard システムとネットワークの知識が必要です。

次の例を参考にしてください。

```
admin@GUARD# arp -e

Address         HWtype  HWaddress           Flags Mask  Iface
10.10.1.254     ether   00:02:B3:C0:61:67   C           eth1
10.10.8.11      ether   00:02:B3:45:B9:F1   C           eth1
10.10.8.253     ether   00:D0:B7:46:72:37   C           eth1
10.10.10.54     ether   00:03:47:A6:44:CA   C           eth1
```

Netstat

ネットワーク接続、ルーティング テーブル、インターフェイス統計情報、マスカレード接続、およびマルチキャスト メンバシップを表示できます。次のいずれかを入力します。

netstat [*address_family_options*] [**--tcp**|**-t**] [**--udp**|**-u**] [**--raw**|**-w**] [**--listening**|**-l**] [**--all**|**-a**] [**--numeric**|**-n**] [**--numeric-hosts**][**--numeric-ports**][**--numeric-ports**] [**--symbolic**|**-N**] [**--extend**|**-e**[**--extend**|**-e**]][**--timers**|**-o**] [**--program**|**-p**] [**--verbose**|**-v**] [**--continuous**|**-c**] [*delay*]

netstat {**--route**|**-r**} [*address_family_options*] [**--extend**|**-e**[**--extend**|**-e**]] [**--verbose**|**-v**] [**--numeric**|**-n**] [**--numeric-hosts**][**--numeric-ports**][**--numeric-ports**] [**--continuous**|**-c**] [*delay*]

netstat {**--interfaces**|**-i**} [*iface*] [**--all**|**-a**] [**--extend**|**-e**[**--extend**|**-e**]] [**--verbose**|**-v**] [**--program**|**-p**] [**--numeric**|**-n**] [**--numeric-hosts**][**--numeric-ports**][**--numeric-ports**] [**--continuous**|**-c**] [*delay*]

netstat {**--groups**|**-g**} [**--numeric**|**-n**] [**--numeric-hosts**][**--numeric-ports**][**--numeric-ports**] [**--continuous**|**-c**] [*delay*]

netstat {**--masquerade**|**-M**} [**--extend**|**-e**] [**--numeric**|**-n**] [**--numeric-hosts**][**--numeric-ports**][**--numeric-ports**] [**--continuous**|**-c**] [*delay*]

netstat {**--statistics**|**-s**} [**--tcp**|**-t**] [**--udp**|**-u**] [**--raw**|**-w**] [*delay*]

netstat {**--version**|**-V**}

netstat {**--help**|**-h**}

（注）　アドレス ファミリを指定しない場合、Guard は設定されているすべてのアドレス ファミリのアクティブなソケットを表示します。

表 10-9 で、**netstat** コマンドの引数とキーワードについて説明します。

表 10-9　netstat コマンドの引数とキーワード

パラメータ	説明
address_family_options	[--protocol={inet,unix,ipx,ax25,netrom,ddp}[,...]][--unix|-x] [--inet|--ip] [--ax25] [--ipx] [--netrom] [--ddp]
--route、-r	Guard のルーティング テーブルを表示します。
--groups、-g	IPv4 および IPv6 のマルチキャスト グループ メンバシップ情報を表示します。
--interface、-i *iface*	すべてのネットワークインターフェイスまたはインターフェイス *iface* のテーブルを表示します。
--masquerade、-M	マスカレード接続のリストを表示します。
--statistics、-s	各プロトコルのサマリー統計情報を表示します。
-v、--verbose	出力を詳細に表示します。
-n、--numeric	数値アドレスを表示します。
--numeric-hosts	数値ホスト アドレスを表示します。これは、ポート名およびユーザ名の解決に影響を及ぼしません。
--numeric-ports	数値ポート番号を表示します。これは、ホスト名およびユーザ名の解決に影響を及ぼしません。
--numeric-users	数値ユーザ ID を表示します。これは、ホスト名およびポート名の解決に影響を及ぼしません。
--protocol、-A *family*	接続を表示するアドレス低レベル プロトコル（ファミリ）を指定するカンマ区切りリスト。アドレス ファミリ inet には、raw、udp、および tcp プロトコル ソケットが含まれます。
-c、--continuous	選択した情報を 1 秒ごとに継続的に表示します。
-e、--extend	追加情報を表示します。最も詳しい情報を表示するには、このオプションを 2 回使用します。

表 10-9　netstat コマンドの引数とキーワード（続き）

パラメータ	説明
-o、--timers	ネットワーキング タイマーに関連する情報を表示します。
-p、--program	各ソケットが属するプログラムの PID および名前を表示します。
-l、--listening	リスニング ソケットだけを表示します。デフォルトでは、リスニング ソケットは省略されます。
-a、--all	リスニング ソケットと非リスニング ソケットの両方を表示します。
-F	FIB からのルーティング情報を表示します。
-C	ルート キャッシュからのルーティング情報を表示します。
delay	*delay* 秒ごとに、Netstat が統計情報からの出力を繰り返します。

次の例を参考にしてください。

```
admin@GUARD# netstat -v
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address   Foreign Address         State
tcp        0      0 localhost:1111  localhost:32777    ESTABLISHED
tcp        0      0 localhost:8200  localhost:32772    ESTABLISHED
.
.
.
tcp        0      0 localhost:33464 localhost:8200     TIME_WAIT
tcp        1      0 localhost:1113  localhost:33194    CLOSE_WAIT
.
.
.
Active UNIX domain sockets (w/o servers)
unix  2      [ ]         STREAM     CONNECTED     928
unix  3      [ ]         STREAM     CONNECTED     890  /tmp/.zserv
.
.
.
admin@GUARD#
```

Traceroute

パケットがネットワーク ホストに到達するまでのルートを出力できます。次のように入力します。

traceroute *ip-address* [**-F**] [**-f** *first_ttl*] [**-g** *gateway*] [**-i** *iface*] [**-m** *max_ttl*] [**-p** *port*] [**-q** *nqueries*] [**-s** *src_addr*] [**-t** *tos*] [**-w** *waittime*] [*packetlen*]

（注）　**traceroute** コマンドでは IP アドレスだけが表示され、名前は表示されません。

表 10-10 で、**traceroute** コマンドの引数とキーワードについて説明します。

表 10-10　traceroute コマンドの引数とキーワード

パラメータ	説明
ip-address	どの IP アドレスへのルートをトレースするか。
-f	最初の発信プローブ パケットで使用される最初の存続可能期間を設定します。
-F	*don't fragment* ビットを設定します。
-g	ルース ソース ルート ゲートウェイを指定します（最大 8 個）。
-i	発信プローブ パケットの送信元 IP アドレスを取得するネットワーク インターフェイスを指定します。これは、通常、マルチホーム ホストだけに役立ちます。
-m	発信プローブ パケットで使用される最大存続可能期間（最大ホップ数）を設定します。デフォルトは 30 ホップです。
-p	プローブで使用されるベース UDP ポート番号を設定します。デフォルトは 33434 です。
packetlen	プローブのパケットの長さを設定します。
-s	この後に指定する IP アドレスを発信プローブ パケットで送信元 IP アドレスとして使用します。

表 10-10　traceroute コマンドの引数とキーワード（続き）

パラメータ	説明
-t	プローブ パケットのサービス タイプを、この後に指定する値に設定します。デフォルトはゼロです。
-w	プローブに対する応答を待つ時間（秒）を設定します。デフォルトは 5 秒です。

次の例を参考にしてください。

```
admin@GUARD# traceroute 10.10.10.34
traceroute to 10.10.10.34 (10.10.10.34), 30 hops max, 38 byte packets
 1 10.10.10.34 (10.10.10.34) 0.577 ms  0.203 ms  0.149 ms
```

Ping

ネットワーク ホストに ICMP ECHO_REQUEST を送信して、接続性を確認できます。次のように入力します。

ping *ip-address* [**-c** *count*] [**-i** *interval*] [**-l** *preload*] [**-s** *packetsize*] [**-t** *ttl*] [**-w** *deadline*] [**-F** *flowlabel*] [**-I** *interface*] [**-Q** *tos*] [**-T** *timestamp option*] [**-W** *timeout*]

表 10-11 で、**ping** コマンドの引数とキーワードについて説明します。

表 10-11　ping コマンドの引数とキーワード

パラメータ	説明
ip-address	宛先 IP アドレス。
-c *count*	*count* 個の ECHO_REQUEST パケットを送信します。deadline オプションが指定されている場合、ping はタイムアウトになるまでこの数の ECHO_REPLY パケットを待ちます。
-F *flow label*	エコー要求パケットに 20 ビットのフロー ラベルを割り当てて設定します（ping6 のみ）。値がゼロの場合は、ランダムなフロー ラベルが使用されます。

表 10-11　ping コマンドの引数とキーワード（続き）

パラメータ	説明
-i *interval*	パケットの送信間隔を *interval* 秒に設定します。デフォルトでは、1 秒に設定されます。
-I *interface*	送信元 IP アドレスを、指定したインターフェイス アドレスに設定します。
-l *preload*	応答を待たずに *preload* 個のパケットを送信します。
-Q *tos*	ICMP データグラムに Quality of Service 関連のビットを設定します。
-s *packetsize*	送信するデータ バイト数を指定します。デフォルトは 56 です。
-t ttl	IP 存続可能時間を設定します。
-T *timestamp option*	特別な IP タイムスタンプ オプションを設定します。
-w *deadline*	送受信されたパケット数に関係なく ping が終了するまでのタイムアウト（秒）を指定します。
-W *timeout*	応答を待つ時間（秒）。

次の例を参考にしてください。

```
admin@GUARD# ping 10.10.10.30 -n 1
```

デバッグ情報の取得

Guard に動作上の問題が発生した場合は、シスコのテクニカルサポートがお客様に内部デバッグ情報を送信するようお願いすることがあります。

デバッグ情報を FTP サーバに抽出するには、次のように入力します。

copy debug-core *time* **ftp** *server* ***full-file-name*** [***login***] [***password***]

表 10-12 で、**copy debug-core** コマンドの引数とキーワードについて説明します。

表 10-12　copy debug-core コマンドの引数

パラメータ	説明
time	デバッグ情報が必要となった原因のイベントの時刻。時刻の文字列では、*MMDDhhmm*[[*CC*]*YY*][*.ss*] という形式を使用します。 • *MM*：月（数値）。 • *DD*：日。 • *hh*：時（24 時間表記）。 • *mm*：分。 • *CC*：年の最初の 2 桁（オプション）。 • *YY*：年の最後の 2 桁（オプション）。 • *.ss*：秒（オプション）。ピリオドが必要です。
server	FTP サーバの IP アドレス。
full-file-name	バージョン 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）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）FTP サーバのパスワード。パスワードを入力しない場合、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。

```
admin@GUARD# copy debug-core ftp 10.0.0.191 debug-file user <password>
```

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　Guard ソフトウェアのアップデートされたバージョンを FTP サーバからダウンロードします。次のように入力します。

```
copy ftp new-version server full-file-name [login] [password]
```

表 10-13 で、**copy ftp new-version** コマンドの引数とキーワードについて説明します。

表 10-13　copy ftp new-version コマンドの引数

パラメータ	説明
server	FTP 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	（オプション）FTP サーバのログイン名。 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、パスワードを要求されます。

ステップ 2　ダウンロードしたバージョンをインストールします。次のように入力します。

```
install new-version
```

注意　**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。

新しいバージョンでファームウェア（CFE）のアップデートが必要となることがあります。詳細については、各バージョン リリースに付属のリリース ノートを参照してください。CFE が適合していない場合、Guard 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.10-28 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 3　Guard をリブートします。次のように入力します。

```
reboot
```

ステップ 4　バージョン番号を表示して、アップグレード プロセスの結果を確認できます。次のように入力します。

```
show version
```

次の例を参考にしてください。

```
admin@GUARD# copy ftp new-version 10.0.0.191
/home/Versions/R3.i386.rpm user <password>
FTP in progress...

admin@GUARD# install new-version

.

.

.

Press Enter to close this CLI session.
```

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。

CFE が適合していない場合は、**install new-version** コマンドを発行すると、Guard が次のメッセージを表示します。

```
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 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。

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　プロンプト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
```

```
For example:
admin@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。