CHAPTER 2

Guard の初期化

この章は、次の内容で構成されています。

Guard の物理的な仕様

ラックマウント

表 2-1 に、Guard のラックマウントの主要な仕様を示します。

表 2-1　ラックマウントの仕様

寸法	
重量	28.12 Kg（62 ポンド）
高さ	8.53cm（2U、3.36 インチ）
幅	44.45 cm（17.5 インチ）（19 インチ ラックマウント可能）
奥行	69.85cm（27.5 インチ）
電力管理	
電源	350 W
電源タイプ	110 または 220 V ユニバーサル自動検知
インターフェイス	
アウトオブバンド	10/100/1000 BaseT × 2
インバンド	次のいずれかのオプションで構成される 1 つのデュアル ポート NIC • 自動検知半 / 全二重 10/100/1000 Base-T（銅）× 2 • 1000 Base-SX（ファイバ）× 2
シリアル ポート	シリアル DB9 RS-232 ポート × 2
電気関連	
	100 ～ 240 V AC 自動検知自動スイッチ 50 ～ 60 Hz（オプション：デュアル電源）

前面パネル

図 2-1 に、Guard の前面パネルを示します。

図 2-1　Guard の前面パネル

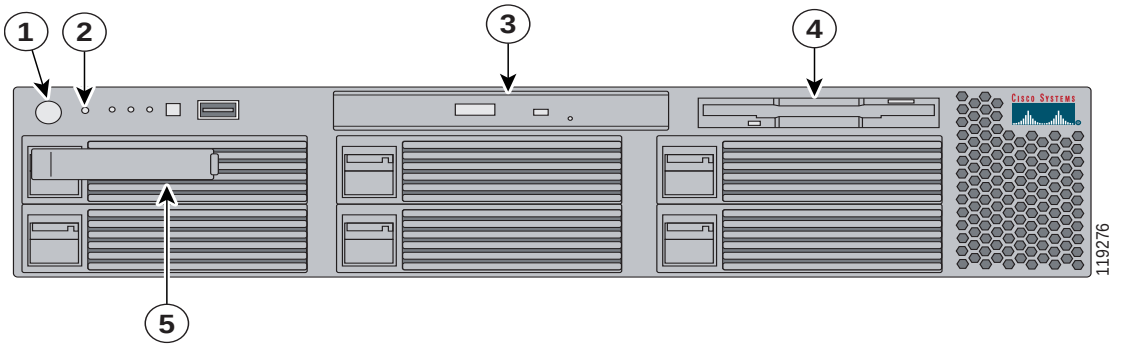

表 2-2 に、Guard の前面パネルの仕様を示します。

表 2-2　前面パネルの仕様

番号	項目	説明	機能
1	ON/OFF ボタン	電源制御ボタン	Guard のオン / オフを切り替えます。 Guard の電源がオンのときには、緑色の LED が点灯します。Guard がオフで、AC 電源に接続されている場合は、LED が点滅します。
2	リセット ボタン	オレンジ色のボタン	サーバをリセットしてパワーオン セルフ テストを実行します。
3	CD-ROM ドライブ	CD-ROM ドライブ	CD 用ドライブ。
4	フロッピーディスク ドライブ	フロッピーディスク ドライブ	フロッピーディスク用ドライブ。
5	ハード ディスク ドライブ	ハード ディスク ドライブ	サーバのハード ディスク用ドライブ。

背面パネル

図 2-2 に、Guard の背面パネルを示します。

図 2-2　Guard の背面パネル

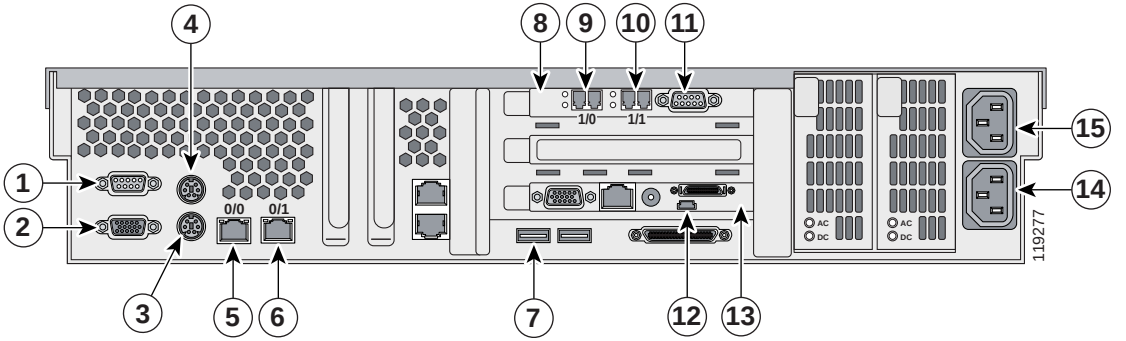

表 2-3 に、Guard の背面パネルの仕様を示します。

表 2-3　背面パネルの仕様

番号	項目	説明	機能
1	シリアル RS-232	シリアル ポート（COM 1）	ユーザ コンソール制御またはコンソール サーバに接続するためのシリアル ポート。
2	モニタ ケーブル ソケット	コンソール モニタのソケット	コンソール モニタ用のソケット。
3	キーボード ケーブル ソケット	コンソールのキーボード ケーブルのソケット	コンソールのキーボード ケーブル用のソケット。
4	マウス ケーブル ソケット	コンソールのマウス ケーブルのソケット	コンソールのマウス ケーブル用のソケット。
5	Eth0 ソケット	10/100/1000 BaseT イーサネット ケーブルのソケット	アウトオブバンド管理ケーブル用のネットワーク インターフェイス ソケット。

表 2-3　背面パネルの仕様（続き）

番号	項目	説明	機能
6	Eth1 ソケット	10/100/1000 BaseT イーサネット ケーブルのソケット	アウトオブバンド管理ケーブル用のネットワーク インターフェイス ソケット。
7	USB ポート	USB ポート	ミニ USB ケーブルをハードウェア診断カードに接続するためのポート。 ⚠ **注意**　このミニ USB ケーブルは、電源を入れる前に接続しておく必要があります。
8	アクセラレータ カード	アクセラレータ カード	シスコ専用アクセラレータ カード。
9	Giga1 ソケット	ネットワーク ソケット	アクセラレータ カードのインバンド ネットワーク インターフェイス ソケット。 ⚠ **注意**　インバンド インターフェイスを 1 つ使用する場合は、このソケットを使用する必要があります。
10	Giga0 ソケット	ネットワーク ソケット	アクセラレータ カードのインバンド ネットワーク インターフェイス ソケット。
11	アクセラレータ カードのシリアル ソケット	アクセラレータ カードのシリアル ソケット	シスコ専用アクセラレータ カードのシリアル ソケット。
12	ハードウェア診断カードの USB ソケット	ハードウェア診断カードの USB ソケット	ミニ USB ケーブルを接続するためのソケット。
13	ハードウェア診断カード	ハードウェア診断カード	このカードによってハードウェア診断データが提供されます。
14	電源ケーブル ソケット 2	電源ケーブル ソケット	サーバの電源 2 に対応する電源ケーブル。
15	電源ケーブル ソケット 1	電源ケーブル ソケット	サーバの電源 1 に対応する電源ケーブル。

（注）　Cisco Guard では、プリインストールのハードウェア アクセラレーション カード（ファイバ ケーブルの場合 P/N X25E02、銅ケーブルの場合 P/N X25E03）が使用されています。屋外設備のリード線への接続は用意されていません。すべての線は室内専用です。

このカードは、メインの Intel CPU による重要なパケット単位の処理の負荷を軽減し、必要とされる高いスループットを実現するために使用されます。カードのブラケットには、前述の 2 つのギガビット イーサネット インターフェイス（Giga0、Giga1（9、10））、およびデバッグを目的とする 1 つのシリアル コネクタ（11）の 3 つのコネクタがあります。カードのブラケット上にないその他のコネクタ（電源コネクタや EJTAG コネクタ）には、ユーザはアクセスできません。シスコの研究所以外ではこれらを使用しないでください。

警告　**カード P/N X25E02 には、クラス 1 レーザー製品が含まれます。このモジュールは、アメリカの FDA/CDRH および国際的な IEC-825 規格に準拠したクラス 1 レーザー安全要件を満たしています。**

Guard の接続

この項では、Guard をネットワークと電源に接続する方法について説明します。

（注）　Guard のコンソール接続は、Guard をローカルに操作するか、コンソールから操作するかによって異なります。詳細については、「コンソールの接続」を参照してください。

ミニ USB ケーブルの接続

注意　ミニ USB ケーブルは、電源を入れる前に接続しておく必要があります。

ミニ USB ケーブルを接続するには、次の手順を実行します。

ステップ 1　ミニ USB ケーブルの小さいプラグをハードウェア診断カードの USB ソケットに接続します（図 2-2 の項目 12 を参照）。

ステップ 2　もう一方のプラグをシャーシの USB ポートのいずれかに接続します（図 2-2 の項目 7 を参照）。

ネットワーク インターフェイスの接続

ネットワーク インターフェイスを接続するには、次の手順を実行します。

ステップ 1　10/100/1000 Base-T イーサネット ケーブルを、Guard の対応するネットワーク ソケットと、適切な管理ネットワーク ソケットに接続します（図 2-2 の項目 5、6 を参照）。

ステップ 2　インバンド ケーブル（銅またはファイバ）を、適切なインバンド ネットワーク ソケット（図 2-2 の項目 9、10 を参照）と、対応するネットワーク ソケットに接続します。Guard では、1 つまたは 2 つのインバンド ネットワーク インターフェイス カードを使用できます。

警告　**インバンド インターフェイスを 1 つ使用する場合は、Giga1 を使用する必要があります（項目 9 を参照）。**

電源の接続

2 つの電源ケーブルを、背面パネルのソケット（図 2-2 の項目 14、15 を参照）と、適切な AC 電源に接続します。緑色のライトの点滅は、ケーブルが正常に接続されたことを示します。

注意　Guard が正しく動作するには、両方のケーブルが AC 電源に接続されている必要があります。

電源ケーブルを、Guard の電源ケーブル ソケット 2（図 2-2 のソケット 7 を参照）に接続し、ケーブルのもう一方の端を適切な AC 電源に接続します。緑色のライトは、接続を示します。

（注）　詳細については、電源ケーブルのソケットのラベルを参照してください。

コンソールの接続

RS-232 ケーブルの一方の端を Guard の RS-232 ソケット（図 2-2 のソケット 1 を参照）に接続し、もう一方の端をシリアル コンソール制御に接続して、ON/OFF ボタン（図 2-1 の ON/OFF ボタンを参照）を押します。

シリアル接続を使用して Guard との通信を確立する場合には、任意の適切なターミナル エミュレータ ソフトウェアを使用できます。このマニュアルの例では、Hilgraeve Inc. が Microsoft 用に作成したソフトウェアである Hyper Terminal を使用しています。

シリアル接続を使用して Guard と通信を確立するには、次の手順を実行します。

ステップ 1　Hyper Terminal を起動します。接続名を入力して、**OK** をクリックします。

ステップ 2　*Connect using* ドロップダウン リストから通信ポートを選択して、**OK** をクリックします。

ステップ 3　次のポート設定を入力して、**OK** をクリックします。

- Bits per second：9600
- Data bits：8
- Parity：None
- Stop bits：1
- Flow control：None

ステップ 4　Hyper Terminal のメイン画面が表示されます。File メニューから **Properties** を選択します。

ステップ 5　Settings 画面のタブを選択します。

ステップ 6　次の値を挿入して、**OK** をクリックします。

- Emulation：VT100
- Telnet terminal ID：VT100
- Backscroll buffer lines：500

Hyper Terminal のメイン画面に Guard のログイン プロンプトが表示されます。

ローカルな接続

Guard をローカルに接続し、操作するには、次の手順を実行します。

ステップ 1　モニタ、キーボード、およびマウスの各ケーブルを、Guard の対応するソケット（図 2-2 の 2、3、および 4 を参照）に接続します。

ステップ 2　ON/OFF ボタン（図 2-1 の ON/OFF ボタンを参照）を押します。2 ～ 3 分するとログイン プロンプトが表示されます。

コマンドライン インターフェイスの使用

CLI を使用して、Guard の機能を制御できます。Guard のユーザ インターフェイスは、多数の異なるコマンド モードに分割されています。任意の時点で使用できるコマンドは、そのときのモードによって異なります。システム プロンプトで **?** と入力すると、各コマンド モードで使用可能なコマンドのリストを取得できます。

CLI へのアクセス権は、ユーザの特権レベルに対応しています。各特権レベルには、独自のコマンドのグループがあります。

表 2-4 に、ユーザの特権レベルの説明を示します。

表 2-4　ユーザの特権レベル

ユーザの特権レベル	コマンド グループ
管理者（admin）	すべてのコマンド グループへの最大限のアクセス
設定（config）	ユーザの定義、削除、変更に関連したコマンドを除くすべてのコマンド グループへの最大限のアクセス
ダイナミック（dynamic）	show コマンド、保護およびラーニング関連コマンド、およびフレックスおよび動的フィルタの設定（下の注を参照）へのアクセス
表示（show）	グローバル コマンド グループのすべての show コマンド

（注）　管理者レベルと設定レベルのユーザがすべてのフィルタ設定手順を実行することを推奨します。これより低いレベルのユーザも、動的フィルタを追加および削除できます。

CLI でのコマンドの発行

表 2-5 に、CLI コマンドの入力規則をまとめます。

表 2-5　CLI の規則

目的の操作	キーボード シーケンス
コマンド履歴をスクロールして変更する	矢印キーを使用する
特定のコマンド モードで使用可能なコマンドを表示する	**Shift+?**
コマンドの補完を表示する	コマンドの最初の部分を入力し、**Tab** キーを押す
コマンド構文の補完を表示する	コマンドを入力して、**Tab** キーを 2 回押す
`more` コマンドを使用してスクロールする	more *number-of-lines* `more` コマンドでは、Space キーを押したときにウィンドウに表示される追加の行数が設定されます。デフォルトは、その端末で表示可能な行数より 2 行少ない行数です。 *number-of-lines*：Space キーを押したときに表示される追加の行数を設定します。
一画面分スクロールする（コマンド出力内）	**Space キー**
一画面分後方にスクロールする（コマンド出力内）	**b キー**
スクロール動作を中止する	**q キー**
文字列を前方に検索する	*/ ストリング*
文字列を後方に検索する	*? ストリング*
アクションをキャンセルするか、パラメータを削除する	そのコマンドの **no** 形を使用する
現在の操作に関連する情報を表示する	**show**

表 2-5　CLI の規則（続き）

目的の操作	キーボード シーケンス
現在のコマンド グループ レベルを終了して上位のグループ レベルに移る	`exit`
すべてのコマンド グループ レベルを終了してルート レベルに戻る	`end`
特定の *文字列*を含む最初の行も含めて、その行からコマンド出力を表示する	| begin *文字列*
特定の *文字列*を含むコマンド出力の行を表示する	| include *文字列*
特定の *文字列*を含まないコマンド出力の行を表示する	| exclude *文字列*

（注）　ルート レベルで **exit** コマンドを発行すると、CLI 環境が終了し、オペレーティング システムのログイン画面に戻ります。

コマンドの no 形の使用

ほとんどすべての設定コマンドには、no 形も存在します。一般に、コマンドの no 形は、特定のフィーチャや機能を無効にする場合に使用します。無効になっているフィーチャや機能を有効にするには、キーワード no のない状態でそのコマンドを使用します。たとえば、**event monitor** コマンドではイベント モニタが有効になり、**no event monitor** コマンドでは無効になります。

コマンド構文の表示

ゾーン コマンド グループ レベルから、ゾーン関連の **show** コマンドを実行できます。また、これらのコマンドは、グローバルまたは設定コマンド グループ レベルからも実行できます。

グローバルまたは設定コマンド グループ レベルの **show** コマンドの構文は、次のとおりです。

show zone *zone-name parameters...*

ゾーン コマンド グループ レベルの `show` コマンドの構文は、次のとおりです。

show *parameters...*

（注）　このガイドでは、表記法として、**ゾーン** コマンド グループ レベルの **show** コマンド構文を使用します。

CLI のエラー メッセージ

Guard CLI では、次の場合にエラー メッセージが表示されます。

- 入力されたコマンドの構文が不完全であるか、間違っている場合。
- 入力されたコマンドがシステムの設定と一致しない場合。
- システムの障害のために操作を実行できなかった場合。この場合は、システムのログにエントリが作成されます。

CLI 使用のヒント

ヘルプ

CLI では、コマンド階層のすべてのレベルで状況依存のヘルプが用意されています。ヘルプの情報では、階層内の現在のレベルで使用可能なコマンドが示され、各コマンドの簡単な説明が提供されます。

ヘルプを取得するには、**?** と入力します。

コマンドのヘルプを表示するには、そのコマンドの後ろに **?** を入力します。

コマンド プロンプトで ? と入力すると、そのモードで使用可能なすべてのコマンドと、その短い説明が表示されます。

ヘルプには、現在のモードで使用可能なコマンドのみが表示されます。

タブ補完

コマンドの一部を入力して Tab キーを押すことにより、コマンドを補完することができます。

複数のオプションを取る値を持ったコマンドを入力し、Tab キーを 2 回押すと、使用可能な入力パラメータが表示されます。この機能は、システム定義パラメータにもユーザ定義パラメータにも使用できます。
たとえば、ゾーンのプロンプトで **policy-template** コマンドを入力し、Tab キーを 2 回押すと、ポリシー テンプレート名のリストが表示されます。設定のプロンプトで **zone** コマンドを入力し、Tab キーを 2 回押すと、定義済みのゾーンが表示されます。

タブ補完で複数のコマンドが一致する場合は、何も表示されず、端末には入力されている現在の行がもう一度表示されます。

タブ補完とヘルプでは、現在のモードで使用可能なコマンドのみが表示されます。

操作の方向の規定

一般に、コマンド名の前に ftp がある場合は、コマンドの方向は Guard から FTP サーバへのコピーになります。コマンドが ftp の前にある場合には、コマンドの方向は FTP サーバから Guard へのコピーになります。たとえば、**copy log ftp** コマンドではログ ファイルが FTP サーバにコピーされます。**copy ftp new-version** コマンドでは、新規バージョンが FTP サーバから Guard にコピーされます。

コマンドの省略

コマンドやキーワードは、一意な省略形を保てる文字数まで短縮できます。

たとえば、**show** コマンドは **sh** まで短縮できます。

ワイルドカード文字

ワイルドカードとして、アスタリスク（*）を使用できます。

次の例を参考にしてください。

learning policy-construction * コマンドを発行すると、Guard のすべてのゾーンでポリシー構築フェーズがアクティブになります。

learning policy-construction scan* コマンドを発行すると、scan で始まる名前を持つ Guard のすべてのゾーン（scannet や scanserver など）でポリシー構築フェーズがアクティブになります。

no zone * コマンドを発行すると、すべてのゾーンが削除されます。

Guard の管理

最初は、コンソールからローカルに Guard を管理することができます。初めて Guard の電源をオンにするときに、コンソール接続を使用して CLI にアクセスし、初期セットアップ プロシージャを実行することができます。詳細については、P.3-10 の「パスワードを使用した特権レベルの割り当て」を参照してください。

Guard のネットワーク機能を設定した後は（P.2-19 の「Guard のインターフェイスの設定」を参照）、次のいずれかの方法を使用して Guard にアクセスし、管理することができます。

- Secured Shell（SSH）セッションを使用したアクセス。詳細については、P.2-34 の「SSH を使用した Guard へのアクセス」を参照してください。
- Web ベース管理（WBM）を使用した Guard へのアクセス。詳細については、P.2-32 の「Web ベース管理による Guard の管理」を参照してください。
- DDoS 検知からのアクセス。DDoS 検知は、接続を確立し、DDoS 対抗システムを形成するネットワーク要素です。詳細については、該当するマニュアルを参照してください。

Guard への初回のアクセス

Guard には、管理者特権を持ったユーザ名が事前設定されています。

Guard に初めてアクセスするときには、次の手順を実行します。

ステップ 1　Guard の ON/OFF ボタンを押して、Guard の電源を入れます。緑色の LED が点灯します。

ステップ 2　管理（ルート）アカウントのパスワードを選択します。パスワードは、6 文字以上の英数字の組み合せである必要があります。

ステップ 3　ユーザ名に **admin** を入力し、パスワードを選択します。パスワードは、スペースを含まず、6 ～ 24 文字である必要があります。

（注）　このパスワードは、いつでも変更できます。詳細については、P.3-8 の「パスワードの変更」を参照してください。

次のプロンプト行が表示されます。admin@GUARD#

Guard を設定するには、設定コマンド レベルに入る必要があります。

設定コマンド レベルに入るには、次のように入力します。

configure [terminal]

次の例を参考にしてください。

```
admin@GUARD# configure
admin@GUARD-conf#
```

（注）　ユーザ名 **riverhead** は、ダイナミック特権を付与します。Detector では、この名前を使用して、Guard をリモートでアクティブにします。

Guard のインターフェイスの設定

この項では、Guard のインターフェイスの設定手順を説明します。Guard には、いくつかのネットワーク インターフェイス カード（NIC）があります。Eth0 と Eth1（ファースト / ギガビット イーサネット）は、管理目的で使用されるアウトオブバンドの NIC を構成します。

Giga0 および Giga1（ギガビット イーサネット）は、Guard の管理およびゾーンのトラフィック送信用のインバンドの NIC を構成します。

（注）　Guard のインバンド インターフェイスは、Giga0 と Giga1 の 2 つに限定されています。1 つまたは両方を設定できます。

Giga0 および Giga1 は、物理インターフェイスを提供し、その上に仮想インターフェイス（VLAN およびトンネル）が設定されます。Guard のインターフェイスの設定は、宛先変更手順の基礎となります（詳細については、第 4 章「ゾーン トラフィックの宛先変更」を参照）。

Guard を正しく機能させるためには、Guard のインターフェイスを設定する必要があります。インターフェイスの特性には、IP アドレスやインターフェイスの Maximum Transmission Unit（MTU; 最大伝送ユニット）などがあります。

注意　同じサブネット上に 2 つの物理インターフェイスを設定しないでください。

多くの機能は、インターフェイス単位で有効になります。**interface** コマンドを入力するときには、インターフェイスのタイプと番号を指定する必要があります。

次の一般的なガイドラインは、すべての物理および仮想インターフェイスの設定プロセスに当てはまります。

- 各インターフェイスには、IP アドレスと IP サブネット マスクを設定する必要があります。

- **no shutdown** コマンドを使用して、各インターフェイスをアクティブにする必要があります。
- インターフェイスに大きな設定変更を行った後は、Guard をリロードする必要があります。

インターフェイスの設定を表示するには、**show** または show running-config コマンドを使用します。

物理インターフェイスの設定

Guard には、4 つの物理インターフェイスがあります。アウトオブバンド インターフェイスには、アウトオブバンド管理用のファースト / ギガビット イーサネット ソケットの Eth0 と Eth1 があります。

インバンド インターフェイスには、銅またはファイバ ソケットの Giga0 と Giga1 があります。

注意　インバンド インターフェイスを 1 つ使用する場合は、Giga1 を使用する必要があります。

物理インターフェイスを設定するには、次の手順を実行します。

ステップ 1　インターフェイス設定モードに入ります。次のように入力します。

```
interface if-name
```

引数 *if-name* には、インターフェイス名を指定します。

次のいずれかを入力します。

- eth0 または eth1：アウトオブバンド インターフェイス
- giga1：最初のインバンド インターフェイス
- giga0：2 番目のインバンド インターフェイス

ステップ 2　インターフェイスの IP アドレスを設定します。次のように入力します。

```
ip address ip-addr ip-mask
```

引数 *ip-addr* および *ip-mask* には、インターフェイスの IP アドレスを指定します。

ステップ 3　（オプション）インターフェイスの MTU を定義します。次のように入力します。

```
mtu integer
```

引数 *integer* は、eth0 および eth1 インターフェイスの場合は 576 ～ 16,384 バイトの整数で、giga0 および giga1 インターフェイスの場合は 576 ～ 1,824 の整数です。

デフォルトの MTU の値は 1,500 バイトです。

ステップ 4　インターフェイスをアクティブにします。次のように入力します。

```
no shutdown
```

大きな変更を行った場合は、Guard の設定をリロードする必要があります。

（注）　Guard の設定をリロードしない場合、設定は変更されますが、設定がリロードされるまでは変更内容が反映されません。

次の例を参考にしてください。

```
admin@GUARD-conf# interface eth1
admin@GUARD-conf-if-eth1#
admin@GUARD-conf-if-eth1# ip address 10.10.10.33 255.255.255.252
admin@GUARD-conf-if-eth1# no shutdown
```

VLAN の設定

インバンド インターフェイスに VLAN を定義できます。

VLAN を定義するには、次の手順を実行します。

ステップ 1　VLAN　インターフェイスが存在する場合は、その設定モードに入ります。または、新しい VLAN を定義します。設定プロンプトで次のように入力します。

```
interface giga x.vlan-id
```

引数 *vlan-id* は、VLAN ID 番号を指定する整数です。VLAN ID は、TAG IEEE 802.1Q に従った番号です。

引数 *x* には、インターフェイスを指定します。インバンド インターフェイスに応じて 0 または 1 を入力します。

ステップ 2　VLAN の IP アドレスを設定します。次のように入力します。

```
ip address ip-addr ip-mask
```

引数 *ip-addr* および *ip-mask* には、インターフェイスの IP アドレスを指定します。

ステップ 3　（オプション）インターフェイスの MTU を定義します。次のように入力します。

```
mtu integer
```

引数 *integer* は、576 ～ 1,824 バイトの整数です。

デフォルトの MTU の値は 1,500 バイトです。

ステップ 4　インターフェイスをアクティブにします。次のように入力します。

```
no shutdown
```

大きな変更を行った場合は、Guard の設定をリロードする必要があります。

（注） Guard の設定をリロードしない場合、設定は変更されますが、設定がリロードされるまでは変更内容が反映されません。

```
For example:
admin@GUARD-conf#interface giga2.2
admin@GUARD-conf-if-giga2.2#
admin@GUARD-conf-if-giga2.2# ip address 192.168.5.8 255.255.255.0
admin@GUARD-conf-if-giga2.2# no shutdown
```

ループバック インターフェイスの設定

ループバック インターフェイスを設定できます。このインターフェイスは、遠隔宛先変更メカニズムに使用されます。

ループバック インターフェイスを設定するには、次の手順を実行します。

ステップ 1　ループバック インターフェイスが存在する場合は、その設定モードに入ります。または、新しいループバック インターフェイスを定義します。次のように入力します。

interface *if-name*

引数 *if-name* には、ループバック インターフェイス名を指定します。インターフェイス名は、**lo:***integer* で、*integer* は 0 ～ 1,023 の整数です。

ステップ 2　ループバック インターフェイスの IP アドレスを設定します。次のように入力します。

ip address *ip-addr ip-mask*

引数 *ip-addr* および *ip-mask* には、インターフェイスの IP アドレスを指定します。

ステップ 3　ループバック　インターフェイスの設定モードを終了します。次のように入力します。

```
exit
```

Guard の設定をリロードする必要があります。

（注）　Guard の設定をリロードしない場合、設定は変更されますが、設定がリロードされるまでは変更内容が反映されません。

次の例を参考にしてください。

```
admin@GUARD-conf# interface lo:0
admin@GUARD-conf-if-lo:0# ip address 1.1.1.1 255.255.255.255
admin@GUARD-conf-if-lo:0# exit
```

トンネルの設定

GRE または IPIP トンネルを定義できます。トンネルは、ゾーンの宛先変更メカニズムに使用できます。

トンネルを定義するには、次の手順を実行します。

ステップ 1　トンネル　インターフェイスが存在する場合は、その設定モードに入ります。または、新しいトンネルを定義します。次のように入力します。

```
interface {greX | ipipY}
```

引数 *X* は、GRE トンネルに割り当てられる 0 ～ 1,024 バイトの整数です。

引数 *Y* は、IPIP トンネルに割り当てられる 0 ～ 1,024 バイトの整数です。

ステップ 2　トンネルの IP アドレスを設定します。次のように入力します。

```
ip address ip-addr [ip-mask]
```

引数 *ip-addr* および *ip-mask* には、インターフェイスの IP アドレスを指定します。デフォルトのサブネット マスクは、255.255.255.255 です。

ステップ 3　トンネルの送信元 IP アドレスを設定します。次のように入力します。

```
tunnel source source ip
```

引数 *source ip* には、トンネルの送信元 IP アドレスを指定します。この IP アドレスは、トンネル内のパケットの送信元アドレスとして使用されます。

ステップ 4　トンネルの宛先 IP アドレスを設定します。次のように入力します。

```
tunnel destination destination-ip
```

引数 *destination ip* には、トンネルの宛先 IP アドレスを指定します。

ステップ 5　（オプション）インターフェイスの MTU を定義します。次のように入力します。

```
mtu integer
```

引数 *integer* は、576 ～ 1,480 の整数です。

IPIP トンネルのデフォルト値は、1,480 バイトです。

GRE トンネルのデフォルト値は、1,476 バイトです。

ステップ 6　インターフェイスをアクティブにします。次のように入力します。

```
no shutdown
```

大きな変更を行った場合は、Guard の設定をリロードする必要があります。

（注）　Guard の設定をリロードしない場合、設定は変更されますが、設定がリロードされるまでは変更内容が反映されません。

次の例を参考にしてください。

```
admin@GUARD-conf# interface gre2
admin@GUARD-conf-if-gre2# ip address 192.168.121.1 255.255.255.0
admin@GUARD-conf-if-gre2# tunnel source 192.168.8.8
admin@GUARD-conf-if-gre2# tunnel destination 192.168.250.2
admin@GUARD-conf-if-gre2# no shutdown
```

GRE トンネルのステータスの確認

GRE トンネルでキープアライブ メッセージを有効にできます。キープアライブ機能が有効になっていると、キープアライブ パケットが指定された間隔で送信され、インターフェイスがアクティブに保たれます。Guard が応答のないキープアライブ パケットの送信を何回試行するとトンネルがダウン状態になるかを指定できます。

キープアライブの間隔を設定することができます。この間隔は、GRE トンネルが活動中であることを確認するために Guard がメッセージを送信する頻度で、1 秒単位で調整が可能です。デフォルトのリトライ値を変更していない場合、キープアライブ パケットを受信せずに 10 回の間隔が過ぎると、GRE トンネルはダウンを宣言されます。

（注）　GRE トンネルがダウンを宣言されると、Guard はそのトンネルを注入に使用することを中止します。トラフィックの注入手段が他に存在しなければ、Guard はゾーンのトラフィックの宛先変更を停止します。

Guard は、GRE トンネルがダウンを宣言されている場合でも、キープアライブ メッセージの送信を続けます。トンネル側がキープアライブ メッセージを返すと、Guard はトンネルをアクティブにし、トラフィックの宛先変更を再開します。

GRE トンネルでキープアライブ メッセージを有効にするには、次のように入力します。

keepalive [*refresh-time* [*retries*]]

表 2-6 に、**keepalive** コマンドの引数を示します。

表 2-6　keepalive コマンドの引数

パラメータ	説明
refresh-time	（オプション）キープアライブ メッセージが送信される間隔（秒）。1 ～ 32,767 の整数を入力します。 デフォルトのリフレッシュ時間は 3 秒です。
retries	（オプション）Guard が応答のないキープアライブ パケットの送信を何回続けるとトンネル インターフェイス プロトコルがダウン状態になるかを指定します。1 ～ 255 の整数を入力します。 デフォルトのリトライ回数は 10 回です。

（注）　キープアライブの設定変更を有効にするには、Guard をリロードする必要があります。

次の例を参考にしてください。

```
admin@GUARD-conf-if-gre2# keepalive 60 5
```

デフォルト ゲートウェイの設定

Guard にデフォルト ゲートウェイを割り当てることができます。ほとんどの場合、Guard のデフォルト ゲートウェイの IP アドレスは、Guard とインターネットの間に存在する隣接ルータです。デフォルト ゲートウェイ アドレスは、Guard のネットワーク インターフェイスの IP アドレスのいずれかと同じネットワーク上にある必要があります。

（注）　Guard が保護モードのときには、デフォルト ゲートウェイに IP アドレスを割り当てないでください。

注意　デフォルト ゲートウェイ アドレスを削除すると、Guard にアクセスできなくなる場合があります。

デフォルト ゲートウェイ アドレスを割り当てるには、次のように入力します。

default-gateway ***ip-addr***

引数 *ip-addr* には、デフォルト ゲートウェイの IP アドレスを指定します。

デフォルト ゲートウェイ アドレスを変更するには、このコマンドを再発行します。

次の例を参考にしてください。

```
admin@GUARD-conf# default-gateway 192.168.100.1
```

ルーティング テーブルへのスタティック ルートの追加

Guard のルーティング テーブルにスタティック ルートを追加できます。スタティック ルートは、Guard の IP インターフェイスに関連付けられたローカル ネットワークの外側にあるサーバやネットワークのルートを指定するために追加します。

スタティック ルートは永続的に追加され、Guard のリブート後も削除されません。

Guard のルーティング テーブルにスタティック ルートを追加するには、次のように入力します。

ip route *ip-addr ip-mask nexthop-ip* [*if-name*]

表 2-7 に、**ip route** コマンドの引数を示します。

表 2-7　ip route コマンドの引数

パラメータ	説明
ip-addr	ルートの宛先ネットワーク。宛先には、IP ネットワーク アドレス（ネットワーク アドレスのホスト ビットは 0 に設定）またはホスト ルートの IP アドレスを指定できます。
ip-mask	宛先ネットワークに関連付けられたサブネット マスク。
nexthop-ip	宛先ネットワークとサブネット マスクによって定義された一連のアドレスへの到達を可能にする転送アドレスまたはネクスト ホップ IP アドレス。ネクスト ホップ IP アドレスは、インターフェイスのサブネット内にある必要があります。ローカル サブネット ルートでは、ネクスト ホップ IP アドレスは、そのサブネットに接続されたインターフェイスに割り当てられている IP アドレスです。1 つ以上のルータをまたいで使用可能なリモート ルートの場合、ネクスト ホップ IP アドレスは、ネイバー ルータに割り当てられている直接到達可能な IP アドレスです。
if-name	（オプション）宛先への到達が可能な Guard のインターフェイス、VLAN、またはトンネル。

（注）　インターフェイスを指定しない場合、Guard はルーティング テーブルに従って、ネクスト ホップ IP アドレスからルートのインターフェイスを判別します。

次の例を参考にしてください。

```
admin@GUARD-conf# ip route 172.16.31.5 255.255.255.255 192.168.100.34
```

ルーティング テーブルを表示するには、**show ip route** コマンドを使用します。

プロキシ IP アドレスの設定

Guard には、プロキシ IP アドレスを割り当てる必要があります。Guard のプロキシ IP アドレスは、プロキシ モードのスプーフィング防止保護メカニズムで必要です。Guard が保護モードのときには、Guard にプロキシ IP アドレスを割り当てないでください。詳細については、P.1-7 の「保護のメカニズム」を参照してください。

警告　**プロキシ IP アドレスが定義されていない場合、ゾーンの保護モードをアクティブにできません。**

Guard のスプーフィング防止用プロキシ IP アドレスを設定するには、次のように入力します。

proxy *ip-addr*

引数 *ip-addr* には、プロキシ IP アドレスを指定します。

各ゾーンと Guard のプロキシ IP アドレス間のルートを確認する必要があります。Guard は、プロキシ IP に対する ping 要求には応答しません。

追加のプロキシ IP アドレスを設定するには、このコマンドを再発行します。

3 ～ 4 個のプロキシ IP アドレスを設定することを推奨します。Guard は、プロキシ IP アドレスを 10 個まで持つことができます。

変更を有効にするには、Guard の設定をリロードする必要があります。

Web ベース管理による Guard の管理

Web ベース管理（WBM）を使用すると、Web ブラウザを使用して Web から Guard を管理できます。

Guard の WBM を有効にするには、次の手順を実行します。

ステップ 1　WBM サービスを有効にします。次のように入力します。

```
service wbm
```

ステップ 2　リモート マネージャの IP アドレスから Guard へのアクセスを許可します。次のように入力します。

permit wbm *ip-addr* [*ip-mask*]

引数 *ip-addr* および *ip-mask* には、リモート マネージャの IP アドレスを指定します。

ステップ 3　ブラウザを開き、次のアドレスを入力します。

https://*Guard-ip-address*/

引数 *Guard-ip-address* には、Guard の IP アドレスを指定します。

Guard の WBM ウィンドウが表示されます。

（注）　Web ベース管理の有効化には、HTTP ではなく HTTPS が使用されます。

ステップ 4　ユーザ名とパスワードを入力して、**OK** をクリックします。

ユーザ名とパスワードを正しく入力すると、Guard のホームページが表示されます。

（注）　TACACS+ 認証が設定されている場合は、ユーザ認証にローカル データベースではなく TACACS+ ユーザ データベースが使用されます。

次の例を参考にしてください。

```
admin@GUARD-conf# service wbm
admin@GUARD-conf# permit wbm 192.168.30.32
```

SSH を使用した Guard へのアクセス

セキュリティ保護されたシェル（SSH）の接続を使用して、Guard にアクセスすることができます。この項では、Guard の SSH 通信設定について説明します。

（注）　SSH サービスは、デフォルトで有効になっています。

Guard への SSH 接続を有効にするには、次の手順を実行します。

ステップ 1　リモート ネットワーク アドレスから Guard へのアクセスを許可します。次のように入力します。

```
permit ssh ip-addr [ip-mask]
```

引数 *ip-addr* および *ip-mask* には、リモート ネットワークの IP アドレスを指定します。

ステップ 2　リモート ネットワーク アドレスから接続を確立し、ログイン名とパスワードを入力します。ログイン名とパスワードを入力せずに SSH 接続を有効にするには、Guard の SSH キー リストにリモート接続の SSH 公開キーを追加します。詳細については、P.3-24 の「SSH キーの管理」を参照してください。

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。

注意　**reload** コマンドを発行すると、Guard の設定の詳細に影響が及び、ラーニングと保護のプロセスが非アクティブになります。

reload コマンドは、Guard のリロードに使用します。

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。

- インターフェイスの IP アドレスの変更
- インターフェイスのアクティブ化と非アクティブ化
- VLAN の ID 番号と IP アドレスの変更
- トンネルのパラメータ（名前、タイプ、送信元および宛先 IP アドレス、およびマスク）の変更
- デフォルト ゲートウェイの IP アドレスの変更
- Guard の TCP プロキシ IP アドレスの変更
- 新しいフラッシュの組み込み
- 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

Guard のリブート

Guard をリブートするには、次のように入力します。

reboot

デフォルトの動作では、Guard は非アクティブ モードのすべてのゾーンをロードします。Guard は、リブート前に保護モードまたはラーニング モードであったゾーンは再びアクティブにしません。

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ようにできます。次のように入力します。

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　次のように入力します。

```
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。緑色の電力 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。