



Guard の初期化

この章では、Cisco Guard (Guard) をネットワークに接続して管理するために必要な基本的作業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。

- [Guard の物理的な仕様](#)
- [Guard の接続](#)
- [コマンドライン インターフェイスの使用](#)
- [Guard への初回のアクセス](#)
- [Guard のインターフェイスの設定](#)
- [デフォルト ゲートウェイの設定](#)
- [ルーティング テーブルへのスタティック ルートの追加](#)
- [プロキシ IP アドレスの設定](#)
- [Guard の管理](#)

Guard の物理的な仕様

この項では、次のトピックについて取り上げます。

- ラックマウント
- 前面パネル
- 背面パネル

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 <ul style="list-style-type: none"> • 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

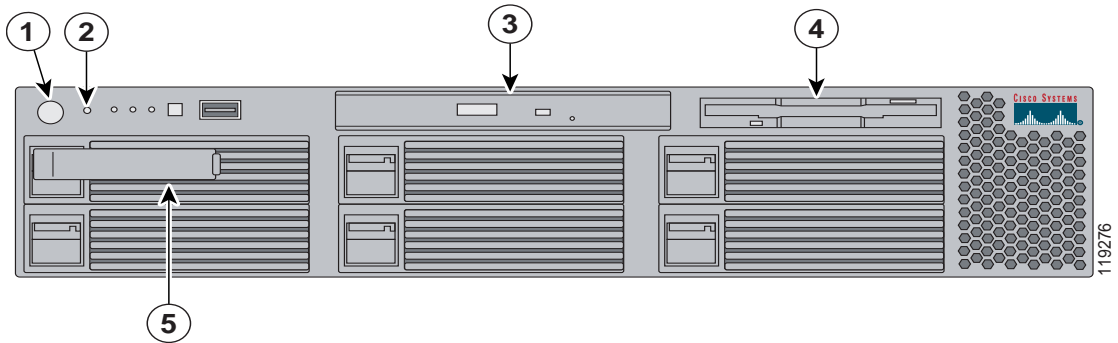


表 2-2 に、Guard の前面パネルの仕様を示します。

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。

Guard の物理的な仕様

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

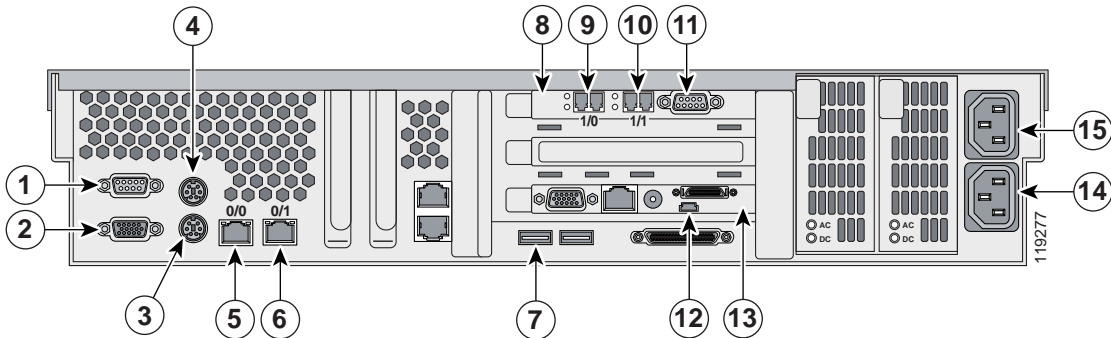




表 2-3 に、Guard の背面パネルの仕様を示します。

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	モニター 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、Gig1 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 14 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	説明
管理者 (admin)	すべての操作にアクセスできます。
設定 (config)	ユーザの定義、削除、および修正に関連する操作を除いて、すべての操作にアクセスできます。
ダイナミック (dynamic)	監視と診断、保護、およびラーニングに関する操作にアクセスできます。dynamic 特権を持つユーザは、フレックスコンテンツ フィルタおよび動的フィルタを設定することもできます。
表示 (show)	監視操作と診断操作にアクセスできます。



(注) フィルタの設定はすべて、管理者の特権レベルまたは設定の特権レベルを持つユーザが実行することをお勧めします。これより下位の特権レベルしか持たないユーザも、動的フィルタを追加および削除できます。

この項では、次のトピックについて取り上げます。

- [CLI でのコマンドの発行](#)
- [CLI 使用のヒント](#)

CLI でのコマンドの発行

この項では、CLI コマンドの入力規則について説明します。

この項では、次のトピックについて取り上げます。

- コマンドの **no** 形の使用
- **show** コマンド構文の表示
- CLI のエラーメッセージ

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 引数は、 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	/ 文字列

表 2-5 CLI の規則 (続き)

目的の操作	キーボード シーケンス
文字列を後方に検索する	? 文字列
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
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** コマンドを使用すると、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デイスーブルにする場合に使用します。デイスーブルになっているフィーチャや機能をイネーブルにするには、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。

show コマンド構文の表示

ゾーン設定モードから、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 モードまたは設定モードからも実行できます。

グローバルまたは設定モードの **show** コマンドの構文は、次のとおりです。

```
show zone zone-name parameters...
```

ゾーン設定モードの **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、明示的な指定がない限り、表記法として、ゾーン設定モードの **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。

- コマンドの構文が不完全であるか、間違っている場合。
- 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

この項では、CLI の使用に関するヒントを提供します。

この項では、次のトピックについて取り上げます。

- [ヘルプ](#)
- [タブ補完](#)
- [操作の方向の規定](#)
- [コマンドの省略](#)
- [ワイルドカード文字](#)

ヘルプ

CLI では、コマンド階層のすべてのモード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、現在のコマンドモード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、ゾーン設定モードで **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。設定モードで **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せん。

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 で設定されている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 で設定されているすべてのゾーン (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 への初回のアクセス

Guard には、管理者のユーザ特権レベル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わせである必要があります。確認のため、新しいパスワードを再入力します。
 - ステップ 3 **admin** ユーザ名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わせである必要があります。確認のため、新しいパスワードを再入力します。
 - ステップ 4 **riverhead** ユーザ名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わせである必要があります。確認のため、新しいパスワードを再入力します。



(注) **admin** および **riverhead** ユーザ名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.3-10](#) の「パスワードの変更」を参照してください。

- ステップ 5 ユーザ名として **admin** を入力し、[ステップ 3](#) で設定したパスワードを入力します。

次のプロンプト行が表示されます。

```
user@GUARD#
```

Guard を設定するには、設定モードに入る必要があります。

次のコマンドを入力します。

configure [terminal]

次の例を参考にしてください。

```
user@GUARD# configure  
user@GUARD-conf#
```

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方法について説明します。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 が管理およびゾーンのトラフィック送信に使用するインバンドの NIC を構成します。



(注)

Guard には、Giga0 と Giga1 の 2 つのインバンド インターフェイスがあります。1 つまたは両方を設定できます。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。

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「トラフィックの宛先変更の設定」](#)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イネーブルになります。**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。設定モードで次のコマンドを入力します。

```
interface if-name
```

if-name 引数には、インターフェイス名を指定します。

Guard では、次のインターフェイスをサポートしています。

- 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。次のコマンドを入力します。

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

ip-addr 引数および *ip-mask* 引数には、インターフェイスの IP アドレスを指定します。IP アドレスとサブネット マスクをドット区切り 10 進表記で入力します (たとえば IP アドレスが 192.168.100.1、サブネット マスクが 255.255.255.0)。

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。次のコマンドを入力します。

```
mtu integer
```

integer 引数は、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 (オプション) インターフェイスの速度とデュプレックス モードを設定します。次のコマンドを入力します。

```
speed {auto | half speed | full speed}
```

表 2-6 で、**speed** コマンドの引数とキーワードについて説明します。

表 2-6 speed コマンドの引数とキーワード

パラメータ	説明
auto	インターフェイスのオートネゴシエーション機能を有効にします。インターフェイスは、ネットワーク設定で使用されているメディア タイプ、およびピア ルータ、ハブ、スイッチの伝送速度などの環境要因に応じて、10 Mbps、100 Mbps、1000 Mbps のいずれか、半二重または全二重で自動的に動作します。 これがデフォルトのモードです。
half	半二重動作を指定します。
full	全二重動作を指定します。
<i>speed</i>	インターフェイスの速度。10Mbps、100Mbps、および 1000Mbps にそれぞれ対応する 10、100、または 1000 を入力します。

ステップ 5 インターフェイスをアクティブにします。次のコマンドを入力します。

```
no shutdown
```

設定の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。

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

物理インターフェイスを非アクティブにするには、**shutdown** コマンドを使用します。

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。設定モードで次のコマンドを入力します。

```
interface gigaX.vlan-id
```

vlan-id 引数は、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。

x 引数には、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。次のコマンドを入力します。

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

ip-addr 引数および *ip-mask* 引数には、インターフェイスの IP アドレスを指定します。IP アドレスとサブネット マスクをドット区切り 10 進表記で入力します (たとえば IP アドレスが 192.168.100.1、サブネット マスクが 255.255.255.0)。

- 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。次のコマンドを入力します。

```
mtu integer
```

integer 引数は、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。次のコマンドを入力します。

```
no shutdown
```

次の例を参考にしてください。

```
user@GUARD-conf#interface giga2.2
user@GUARD-conf-if-giga2.2# ip address 192.168.5.8 255.255.255.0
user@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。設定モードで次のコマンドを入力します。

```
interface if-name
```

if-name 引数には、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。次のコマンドを入力します。

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

ip-addr 引数および *ip-mask* 引数には、インターフェイスの IP アドレスを指定します。IP アドレスとサブネット マスクをドット区切り 10 進表記で入力します (たとえば IP アドレスが 192.168.100.1、サブネット マスクが 255.255.255.0)。

- 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。次のコマンドを入力します。

```
exit
```

次の例を参考にしてください。

```
user@GUARD-conf# interface lo:0
user@GUARD-conf-if-lo:0# ip address 1.1.1.1 255.255.255.255
user@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。設定モードで次のコマンドを入力します。

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

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

Y 引数は、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。次のコマンドを入力します。

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

ip-addr 引数および *ip-mask* 引数には、インターフェイスの IP アドレスを指定します。IP アドレスとサブネット マスクをドット区切り 10 進表記で入力します (たとえば IP アドレスが 192.168.100.1、サブネット マスクが 255.255.255.0)。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。次のコマンドを入力します。

```
tunnel source source ip
```

source ip 引数には、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。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 192.168.100.1)。

ステップ 4 トンネルの宛先 IP アドレスを設定します。次のコマンドを入力します。

```
tunnel destination destination-ip
```

destination ip 引数には、トンネルの宛先 IP アドレスを指定します。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 192.168.100.1）。

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。次のコマンドを入力します。

```
mtu integer
```

integer 引数は、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。次のコマンドを入力します。

```
no shutdown
```

次の例を参考にしてください。

```
user@GUARD-conf# interface gre2
user@GUARD-conf-if-gre2# ip address 192.168.121.1 255.255.255.0
user@GUARD-conf-if-gre2# tunnel source 192.168.8.8
user@GUARD-conf-if-gre2# tunnel destination 192.168.250.2
user@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 メッセージをイネーブルにできます。キープアライブ機能をイネーブルにすると、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 メッセージをイネーブルにするには、次のコマンドを入力します。

```
keepalive [refresh-time [retries]]
```

表 2-7 に、**keepalive** コマンドの引数を示します。

表 2-7 keepalive コマンドの引数

パラメータ	説明
<i>refresh-time</i>	(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 ~ 32767 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。
<i>retries</i>	(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。

次の例を参考にしてください。

```
user@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するには、次のコマンドを入力します。

```
default-gateway ip-addr
```

ip-addr 引数には、デフォルト ゲートウェイの IP アドレスを指定します。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 192.168.100.1)。

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。

```
user@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、次のコマンドを入力します。

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

表 2-8 に、**ip route** コマンドの引数を示します。

表 2-8 ip route コマンドの引数

パラメータ	説明
<i>ip-addr</i>	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 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 192.168.100.1)。
<i>ip-mask</i>	宛先ネットワークに関連付けられたサブネット マスク。サブネット マスクをドット区切り 10 進表記で入力します (たとえば 255.255.255.0)。
<i>nexthop-ip</i>	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。

表 2-8 ip route コマンドの引数 (続き)

パラメータ	説明
<i>if-name</i>	(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。インターフェイスを指定しない場合、Guard のルーティング テーブルに従って、使用されるインターフェイスはネクスト ホップ IP アドレスによって判別されます。

次の例を参考にしてください。

```
user@GUARD-config# 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。



警告

プロキシ IP アドレスを定義しない場合、ゾーン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、次のコマンドを入力します。

proxy ip-addr

ip-addr 引数には、プロキシ IP アドレスを指定します。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 192.168.100.1）。

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 アドレスに対する 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。

ネットワークでロード バランシングを使用してネットワークの過負荷を分散している場合、または多数の同時接続が必要な場合は、プロキシ IP アドレスを 3 つまたは 4 つ設定することをお勧めします。

Guard は、プロキシ IP アドレスを最大で 10 個持つことができます。

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.3-12 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。

- セキュリティ保護されたシェル (SSH) のセッションを使用したアクセス。詳細については、P.2-35 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.2-33 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。

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 をイネーブルにするには、次の手順を実行します。

ステップ 1 WBM サービスをイネーブルにします。次のコマンドを入力します。

```
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。次のコマンドを入力します。

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

ip-addr 引数および *ip-mask* 引数には、リモート マネージャの IP アドレスを指定します。IP アドレスとサブネット マスクをドット区切り 10 進表記で入力します。

ステップ 3 ブラウザを開いて、次のアドレスを入力します。

```
https://Guard-ip-address/
```

Guard-ip-address 引数は、Guard の IP アドレスです。

Guard の WBM ウィンドウが表示されます。



(注) Web ベース管理をイネーブルにするには、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、**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。

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。

```
user@GUARD-conf# service wbm
user@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。

SSH サービスは、デフォルトでイネーブルになっています。

Guard への SSH 接続をイネーブルにするには、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。次のコマンドを入力します。

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

ip-addr 引数および *ip-mask* 引数には、リモート ネットワークの IP アドレスを指定します。IP アドレスとサブネット マスクをドット区切り 10 進表記で入力します。

- 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 接続をイネーブルにするには、Guard の SSH 鍵リストにリモート接続の SSH 公開鍵を追加します。詳細については、[P.3-33](#) の「SSH 鍵の管理」を参照してください。
-

