Guard モジュールの初期化

この章では、Cisco Anomaly Guard Module（Guard モジュール）をネットワークに接続し、管理するための基本的なタスク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。

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 モジュールの機能を制御できます。Guard モジュールのユーザ 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 3-1 に、ユーザの特権レベルの説明を示します。

表 3-1　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た後、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 コマンドの構文
- CLI のエラー メッセージ

表 3-2 に、CLI コマンドの入力規則をまとめます。

表 3-2　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 3-2　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セーブルにする場合に使用します。ディセ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 コマンドの構文

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 モード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）　このマニュアルでは、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 モジュール 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 を使用する際のヒントになる、次のトピックについて取り上げます。

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 モジュールから 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 モジュール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 モジュールにコピーされます。

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。

例

learning policy-construction * コマンドを発行すると、Guard モジュールに設定された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 モジュールに設定されたすべてのゾーン（scannet や scanserver など）でポリシー作成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 モジュールのインターフェイスの設定

この項では、Guard モジュールのインターフェイスの設定手順を説明します。Guard モジュールは、スーパーバイザ上に 1 つの管理ポートと 2 つのデータ ポートを備えています。

現在のバージョンでは、データ ポートは 1 つだけが使用されています。

Guard モジュールを設定するには、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**]

例

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

Guard モジュールを正しく機能させるためには、Guard モジュール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** コマンドまたは 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

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 モジュールは、次のインターフェイスをサポートします。

- eth1：管理ポート
- giga2：データ ポート

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、eth1 インターフェイスの場合は 576 ～ 16,384 バイトの整数で、giga2 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 3-3 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 3-3　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。
speed	インターフェイスの速度。10、100、または 1000 を、それぞれ 10Mbps、100Mbps、および 1000Mbps として入力します。

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 モジュールをリロードする必要があります。

例

```
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

データ ポートに 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 giga2.*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。

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
```

例

```
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。

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
```

例

```
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
```

デフォルト ゲートウェイの設定

Guard モジュールにデフォルト 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 モジュールのデフォルト ゲートウェイの IP アドレスは、Guard モジュール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 モジュールのネットワーク 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 モジュール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 モジュール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。

例

```
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 モジュールのルーティング 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 モジュールの 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 モジュールのリブート後も削除されません。

Guard モジュールのルーティング 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 3-4 に、**ip route** コマンドの引数を示します。

表 3-4　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 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）。
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。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）。
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。

表 3-4　ip route コマンドの引数（続き）

パラメータ	説明
if-name	（オプション）宛先への到達が可能な Guard モジュールのインターフェイスまたは VLAN。インターフェイスを指定しない場合、使用されるインターフェイスは、Guard モジュールのルーティング テーブルに従ってネクスト ホップ IP アドレスから判別されます。

例

```
user@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 モジュールには、プロキシ IP アドレスを割り当てる必要があります。Guard モジュールのプロキシ 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 モジュールが保護モードのときには、Guard モジュールにプロキシ IP アドレスを割り当てないでください。

警告　**ゾーン保護モードをアクティブにするには、プロキシ IP アドレスを定義する必要があります。**

Guard モジュール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 モジュールのプロキシ IP アドレス間のルートを確認する必要があります。Guard モジュールは、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 モジュールでは、プロキシ IP アドレスを最大 10 個使用できます。

Guard モジュールの管理

スーパーバイザからセッションを確立し、Guard モジュールのネットワーク機能を設定した後は（第 2 章「スーパーバイザ エンジンへの Guard モジュールの設定」と P.3-8 の「Guard モジュール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 モジュールにアクセスし、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.3-19 の「SSH を使用した Guard モジュールへのアクセス」を参照してください。
- Web ベース管理（WBM）を使用した Guard モジュールへのアクセス。詳細については、P.3-18 の「Web ベース管理による Guard モジュールの管理」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 モジュールの管理

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 モジュールを管理できます。

Guard モジュールの 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 モジュール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 Module-ip-address*/

Guard Module-ip-address 引数は、Guard モジュールの IP アドレスです。

Guard モジュールの 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。

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。

例

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

SSH を使用した Guard モジュールへのアクセス

セキュリティ保護されたシェル（SSH）の接続を使用して、Guard モジュールにアクセスすることができます。この項では、Guard モジュールの 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 モジュールへの 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 IP アドレスから Guard モジュール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 モジュールの 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.4-31 の「SSH 鍵の管理」を参照してください。