スーパーバイザ エンジンへの Guard モジュールの設定

この章では、スーパーバイザ エンジンへの Cisco Anomaly Guard Module（Guard モジュール）の設定方法について説明します。Guard モジュールとの新しいセッションを確立して設定を行う前に、スーパーバイザエンジン上の Guard モジュールの設定を行う必要があります。

Catalyst 6500 シリーズ スイッチまたは 7600 シリーズ ルータに Cisco Anomaly Guard Module（Guard モジュール）をインストールできます。詳細については、P.1-2 の「Cisco Anomaly Guard Module について」を参照してください。

この章は、次の項で構成されています。

- Guard モジュールの設置の確認
- Guard モジュールの管理の設定
- VLAN の設定
- Guard モジュールとのセッションの確立
- Guard モジュールのリブート
- Guard モジュールの設定の確認
- 1 つのスイッチまたはルータに複数の Guard モジュールを設定

スーパーバイザ エンジンに Guard モジュールを設定するには、EXEC 特権を保有し、設定モードに入る必要があります。

フラッシュ メモリへの設定変更をすべて保存するには、特権 EXEC モードで **write memory** コマンドを使用します。

Guard モジュールの設置の確認

スーパーバイザ エンジンで新しい Guard モジュールが認識され、オンラインになっていることを確認します。

（注） Catalyst 6500 シリーズ スイッチに Guard モジュールを設置する方法については、『*Cisco Anomaly Guard Module and Traffic Anomaly Detector Module Installation Note*』を参照してください。

設置を確認するには、次の手順を実行します。

ステップ 1　スーパーバイザ エンジン コンソールにログインします。

ステップ 2　Guard モジュールがオンラインになっていることを確認します。次のコマンドを入力します。

```
show module
```

次の例は、**show module** コマンドの出力を示しています。

```
Sup# show module
Mod Ports CardType ModelSerial No.
—-  —-- ————————————————————-
1   2 Catalyst 6000 supervisor 2(Active)WS-X6K-SUP2-2GESAL081230TJ
... ...
6   3 Anomaly Guard module ModuleWS-SVC-agm-1-K9SAD081000GG
Mod MAC addressesHwFwSwStatus
--- ----------------------------------- ------- ----------- -------
...
6   000e.847f.fe04 to 000e.847f.fe0b3.07.2(1)4.0(0.10)Ok
...
Sup
#
```

（注）　Guard モジュールを初めて設置した場合、ステータスは通常「other」になります。Guard モジュールが診断ルーチンを完了してオンラインになると、ステータスは「OK」になります。

Guard モジュールの管理の設定

Guard モジュールとリモート管理セッションを確立するには、Guard モジュールの管理ポートを設定する必要があります。

管理のために VLAN を選択するには、次のコマンドを入力します。

anomaly-guard module *module_number* **port** *port_number* [**allowed-vlan** *vlan_range* | **native-vlan** *vlan_id*]

表 2-1 で、**anomaly-guard module** コマンドの引数とキーワードについて説明します。

表 2-1　anomaly-guard モジュール コマンドの引数とキーワード

パラメータ	説明
module_number	モジュールをシャーシに装着するためのスロットの番号（1 ～ 9）。
port *port_number*	管理用に使用するポートの番号。Guard モジュールでは、管理用にポート 1 がサポートされています。
allowed-vlan *vlan_range*	VLAN の範囲またはカンマ区切りリストで指定するいくつかの VLAN（スペース文字を入力することはできません）。
native-vlan *vlan_id*	802.1Q トランキング モードにおけるトランクのネイティブ VLAN を設定します。デフォルトのネイティブ VLAN は 1 です。

次の例は、シャーシの番号 4 のスロットに装着されたモジュールについて、管理のために VLAN *5* を選択する方法を示しています。

```
Sup(config)# anomaly-guard module 4 port 1 allowed-vlan 5
```

Guard モジュールとリモート管理セッションを確立するには、次の事項も Guard モジュールに設定する必要があります。

- Guard モジュールの管理ポート インターフェイス eth1 を設定する。P.3-11 の「物理インターフェイスの設定」を参照してください。
- 関連するサービスをイネーブルにする。P.3-21 の「Guard モジュールの管理」を参照してください。

VLAN の設定

トラフィックを Guard モジュールに転送するためのスーパーバイザ エンジンに VLAN を設定するには、次の手順を実行します。

ステップ 1　トラフィックを Guard モジュールに転送するためのスーパーバイザ エンジンに VLAN を設定します。詳細については、P.2-5 の「スーパーバイザ エンジンへの VLAN の設定」を参照してください。

ステップ 2　Guard モジュールに VLAN を割り当てます。詳細については、P.2-6 の「Guard モジュールへの VLAN の割り当て」を参照してください。

ステップ 3　（オプション）VLAN にレイヤ 3 インターフェイスを設定します。詳細については、P.2-7 の「VLAN へのレイヤ 3 インターフェイスの設定」を参照してください。

ステップ 4　Guard モジュールのインターフェイスを設定します。詳細については、P.3-10 の「Guard モジュールのインターフェイスの設定」を参照してください。

スーパーバイザ エンジンへの VLAN の設定

トラフィックを Guard モジュールに転送するには、スーパーバイザ エンジンに VLAN を設定する必要があります。スーパーバイザ エンジン上に VLAN を作成するには、次のコマンドを入力し、Guard モジュールに割り当てる VLAN 範囲を定義します。

vlan *vlan_range*

vlan_range 引数には、単一の番号、VLAN の範囲、またはカンマ区切りリスト形式の複数の VLAN を指定します（スペース文字を入力することはできません）。vlan_range は、1 つまたは複数の VLAN（1 ～ 4,094）となります。

次の例は、VLAN を定義する方法を示しています。

```
Sup(config)# vlan 86-89,99
```

Guard モジュールへの VLAN の設定方法については、P.3-13 の「VLAN の設定」を参照してください。

Guard モジュールへの VLAN の割り当て

Guard モジュールに VLAN を割り当てるには、Guard モジュールとイーサネット ポート間のマッピングについて理解する必要があります。このイーサネット ポートとは、Guard モジュールをスイッチ ファブリックに接続するものを指します。

Guard モジュールに VLAN を割り当てるには、スーパーバイザ エンジン プロンプトで次のコマンドを使用します。

anomaly-guard module *module_number* **port** *port_number* [**allowed-vlan** *vlan_range* | **native-vlan** *vlan_id*]

表 2-2 に、**anomaly-guard module** コマンドの引数とキーワードを示します。

表 2-2　anomaly-guard module コマンドの引数とキーワード

パラメータ	説明
module_number	モジュールをシャーシに装着するためのスロットの番号（1 ～ 9）。
port *port_number*	ポート番号（1 ～ 3）。ポート 1 は管理用に、ポート 2 はデータ用に使用されます。ポート 3 は現在使用されていません。
allowed-vlan *vlan_range*	VLAN の範囲、またはカンマ区切りリストで指定するいくつかの VLAN（スペース文字を入力することはできません）。
native-vlan *vlan_id*	802.1Q トランキング モードにおけるトランクのネイティブ VLAN を設定します。デフォルトのネイティブ VLAN は 1 です。 使用可能な VLAN の 1 つは、管理 VLAN である必要があります。デフォルトでは、VLAN 1 になっています。

次の例は、VLAN を Guard モジュールに割り当てる方法を示しています。

```
Sup# anomaly-guard module 7 port 2 allowed-vlan 1,3,6-15
```

（注）　VLAN の割り当てだけでなく、Guard モジュール上の管理ポートとデータ ポートも設定する必要があります。詳細については、P.3-11 の「物理インターフェイスの設定」を参照してください。

VLAN へのレイヤ 3 インターフェイスの設定

アプリケーションで必要な場合は、VLAN にレイヤ 3 インターフェイスを設定できます。

（注）　レイヤ 3 インターフェイスを設定する前に、Guard モジュールに VLAN を割り当てる必要があります。

レイヤ 3 VLAN 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　スーパーバイザ エンジン プロンプトで次のコマンドを入力し、VLAN インターフェイス設定モードに入ります。

interface vlan *vlan-id*

vlan-id 引数には、VLAN の番号を指定します。有効な値は 1 ～ 4,094 です。

ステップ 2　次のコマンドを入力して、VLAN IP アドレスを設定します。

ip address *ip_address subnet_mask*

ip-addr 引数および *subnet-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。

ステップ 3　次のコマンドを入力して、インターフェイスをアクティブにします。

```
no shutdown
```

次の例は、レイヤ 3 VLAN インターフェイスを設定する方法を示しています。

```
sup (config)# interface vlan 5
sup (config-if)# ip address 192.168.89.100 255.255.255.0
sup (config-if)# no shutdown
```

Guard モジュールとのセッションの確立

Guard モジュールにログインするには、次の手順を実行します。

ステップ 1　Telnet セッションまたはコンソール セッションを確立して、スイッチにログインします。

ステップ 2　スーパーバイザ エンジン プロンプトで次のコマンドを入力します。

```
session slot slot_number processor processor_number
```

表 2-3 に、**session slot** コマンドの引数とキーワードを示します。

表 2-3　session slot コマンドの引数とキーワード

パラメータ	説明
slot-number	モジュールをシャーシに装着するためのスロットの番号（1 ～ 9）。
processor *processor_number*	Guard モジュールのプロセッサの番号。Guard モジュールは、プロセッサ 1 を使用した管理だけをサポートします。

ステップ 3　Guard モジュール ログイン プロンプトでログインします。

```
login: admin
```

ステップ 4　パスワードを入力します。

Guard モジュールとセッションを初めて確立する場合は、admin ユーザ アカウントと riverhead ユーザ アカウントのパスワードを選択する必要があります。パスワードは、スペースを含まず、6 ～ 24 文字の長さである必要があります。パスワードは、いつでも変更できます。詳細については、P.4-10 の「自分のパスワードの変更」を参照してください。

ログインに成功すると、コマンドライン プロンプトの表示が user@GUARD# になります。**hostname** コマンドを入力することにより、このプロンプトを変更できます。

Guard モジュールのリブート

Cisco IOS には、Guard モジュールを制御するコマンドとして、**boot**、**shutdown**、**power enable**、および **reset** が用意されています。

注意　スーパーバイザ エンジン プロンプトで reload コマンドを入力すると、シャーシ全体でリロードが発生し、そのシャーシ内のすべてのモジュールが影響を受けます。Guard モジュールをリロードする方法については、P.14-13 の「Guard モジュールのリロード」を参照してください。

- **shutdown**：すべてのデータを確保して、オペレーティング システムを正しくシャットダウンします。Guard モジュールの破損を避けるには、Guard モジュールを正しくシャットダウンする必要があります。スーパーバイザ エンジン プロンプトで次のコマンドを入力します。

  hw-module module *slot_number* **shutdown**

  slot_number 引数には、モジュールをシャーシに装着するためのスロットの番号を指定します。

  次に、Guard モジュールを再起動するには、**hw-module module** *module_number* **reset** コマンドを入力する必要があります。

  次の例は、Guard モジュールをシャットダウンする方法を示しています。

  ```
  Sup# hw-module module 8 shutdown
  ```

（注）　スイッチをリブートすると、Guard モジュールがリブートします。

- **reset**：モジュールをリセットします。このコマンドは通常、アップグレード プロセスで、アプリケーション パーティション（AP）イメージとメンテナンス パーティション（MP）イメージとの切り替えのため、またはシャットダウンからの復旧のために使用します。**hw-module reset** コマンドは、モジュールの電源をいったん切った後で入れ、モジュールをリセットします。リセット プロセスには数分かかります。スーパーバイザ エンジン プロンプトで次のコマンドを入力します。

  hw-module module *slot_number* reset [*string*]

  slot_number 引数は、モジュールをシャーシに装着するためのスロットの番号です。*string* 引数は、PC ブート シーケンス用のオプション文字列です。MP にリセットするには **cf:1** を、AP にリセットするには **cf:4** を入力します。詳細については、P.14-14 の「Guard モジュールのソフトウェアのアップグレード」を参照してください。

  次の例は、Guard モジュールをリセットする方法を示しています。

  ```
  Sup# hw-module module 8 reset
  ```

- **no power enable**：モジュールをシャットダウンして、シャーシから安全に除去できるようにします。スーパーバイザ エンジン プロンプトで次のコマンドを入力します。

  no power enable module *slot_number*

  slot_number 引数には、モジュールをシャーシに装着するためのスロットの番号を指定します。

  モジュールをもう一度オンにするには、次のコマンドを使用します。

  power enable module *slot_number*

  次の例は、Guard モジュールをシャットダウンする方法を示しています。

  ```
  Sup (config)# no power enable module 8
  ```

- **boot**：次回の電源投入時に Guard モジュールを MP からブートさせます。スーパーバイザ エンジン プロンプトで次のコマンドを入力します。

  boot device module *slot_number* cf:1

  slot_number 引数には、モジュールをシャーシに装着するためのスロットの番号を指定します。

  次回のブート サイクルで Guard モジュールをデフォルト パーティション（AP）からブートできるようにするには、スーパーバイザ エンジン プロンプトで次のコマンドを使用します。

  no boot device module *slot_number* cf:1

次の例は、次のブート サイクルで Guard モジュールが AP からブートするように設定する方法を示します。

```
Sup# boot device module 8 cf:1
```

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。リブート後のゾーンのデフォルト動作に関する詳細については、P.14-13 の「Guard モジュールのリブートおよびゾーンの非アクティブ化」を参照してください。

Guard モジュールの設定の確認

スーパーバイザ エンジンに対する Guard モジュールの設定を確認するには、スーパーバイザ エンジン プロンプトで次のコマンドを使用します。

show anomaly-guard module *slot_number* port *port_number* [**state** | **traffic**]

表 2-4 で、**show module** コマンドの引数とキーワードについて説明します。

表 2-4　show module コマンドの引数とキーワード

パラメータ	説明
slot-number	モジュールをシャーシに装着するためのスロットの番号（1 ～ 9）。
port *port_number*	ポート番号（1 ～ 3）。ポート 1 は管理用に、ポート 2 はデータ用に使用されます。
state	指定のポートの設定を表示します。
traffic	指定のポートのトラフィック統計情報を表示します。

次の例は、スーパーバイザ エンジン上に Guard モジュールの設定を表示する方法を示しています。

```
Sup# show anomaly-guard module 8 port 2 state
```

1 つのスイッチまたはルータに複数の Guard モジュールを設定

スーパーバイザ エンジンが少なくとも 1 つ設置されていれば、1 つの Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータに複数の Guard モジュールを設置できます。モジュールの正確な数については、最新のリリース ノートを参照してください。

（注）　Guard モジュールの最新をリリース ノートを表示するには、次の URL を参照してください。

http://www.cisco.com/en/US/products/hw/modules/ps2706/prod_release_notes_list.html

次の設定のどちらかに複数の Guard モジュールを設定できます。

- ロード シェアリング
- 冗長性と高いアベイラビリティ

ロード シェアリング

ゾーン トラフィックを処理するための複数の Guard モジュールを設定できます。同じ宛先に対する複数のルートのコストが等しい場合、スーパーバイザ エンジンは必ずトラフィックを Guard モジュール間に均等に分散させます。

ロード シェアリング用に複数の Guard モジュールを設定するには、次の操作を行います。

- すべての Guard モジュールにゾーンを定義する。詳細については、P.6-10 の「ゾーンのアトリビュートの設定」を参照してください。
- すべての Guard モジュールに、同じ宛先変更ハイジャックの重みを割り当てる。詳細については、P.5-12 の「ハイジャックの設定」を参照してください。
- すべての Guard モジュールで、ゾーンに対する Guard モジュールのラーニング プロセスを同時にアクティブにする。詳細については、P.6-15 の「Guard モジュールの Cisco Traffic Anomaly Detector Module とのゾーン設定の同期」を参照してください。

- すべての Guard モジュールのゾーンの保護をアクティブ化する。詳細については、第 10 章「ゾーンの保護」を参照してください。

（注）　半分以上の Guard モジュールにおいて機能が停止した場合、残りの Guard モジュールは、正当なトラフィックをゾーンに対する攻撃と見なす場合があります。

冗長性と高いアベイラビリティ

高いアベイラビリティを実現するために、2 つの Guard モジュール（または Guard モジュールのグループ）を設定できます。このようにすると、アクティブな Guard モジュールが使用不能になった場合に、スーパーバイザ エンジンがゾーン トラフィックをスタンバイ状態の Guard モジュールに宛先変更します。

スーパーバイザ エンジンは、より低コストのルート（重みが最小のルート）にトラフィックを転送します。スーパーバイザ エンジンが、アクティブな Guard へのルートがダウンしていることを検出した場合に限り、冗長ルートにトラフィックを転送します。

冗長設定で Guard モジュールを設定するには、次の操作を行います。

- 両方の Guard モジュールに同じゾーンを定義する。詳細については、P.6-10 の「ゾーンのアトリビュートの設定」を参照してください。
- アクティブな Guard モジュールに、より小さい宛先変更ハイジャックの重みを割り当てる。詳細については、P.5-12 の「ハイジャックの設定」を参照してください。
- 冗長 Guard モジュールに、より大きい宛先変更ハイジャックの重みを割り当てる。詳細については、P.5-12 の「ハイジャックの設定」を参照してください。
- アクティブな Guard モジュールのラーニング プロセスをアクティブにする。詳細については、P.6-15 の「Guard モジュールの Cisco Traffic Anomaly Detector Module とのゾーン設定の同期」を参照してください。
- ゾーン設定を冗長 Guard モジュールにコピーする。詳細については、P.14-4 の「設定のエクスポート」および P.14-7 の「設定のインポートとアップデート」を参照してください。
- 両方の Guard モジュールのゾーンの保護をアクティブ化する。詳細については、P.10-1 の「ゾーンの保護」を参照してください。