CHAPTER 2

スーパーバイザ エンジンでの Detector モジュールの設定

この章では、Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータのスーパーバイザ エンジンで Cisco Traffic Anomaly Detector モジュール（Detector モジュール）を設定する方法について説明します。Detector モジュールとのセッションを確立してこれを設定する前に、スーパーバイザ エンジンで Detector モジュールを設定しておく必要があります。

スーパーバイザ エンジンで Detector モジュールを設定するには、EXEC 特権を持っており、設定モードである必要があります。

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。

（注） 1 Gbps 動作の Detector モジュールと 2 Gbps 動作の Detector モジュールの間には、動作および設定上の違いがあります。この章では、1 Gbps 動作と 2 Gbps 動作の違いについて説明します。特に記載がない限り、この章の情報は、両方の動作モードに適用されます。詳細については、P.1-9 の「1 Gbps および 2 Gbps 帯域幅オプションについて」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。

Detector モジュールの設置確認

スーパーバイザ エンジンが新しい Detector モジュールを認識してオンラインにしたことを確認します。

（注） Catalyst 6500 シリーズ スイッチに Detector 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　Detector モジュールがオンラインであ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 CardTypeModelSerial No.
--   ---- --------------------------------------------------
1    2   Catalyst 6000 supervisor 2(Active)WS-X6K-SUP2-2GESAL081230TJ
... ...
6    3   Anomaly Detector module ModuleWS-SVC-adm-1-K9SAD081000GG
...
Mod MAC addressesHwFwSwStatus
--- ------------------------------------ ------- ----------- -------
...
6   000e.847f.fe04 to 000e.847f.fe0b1.07.2(1)6.0(0.10)Ok
...
Sup
#
```

（注） Detector　モジュールが初めてインストールされたときは、通常、ステータスは「other」です。Detector 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。Detector モジュールがオンラインになるまでは少なくとも 5 分間はかかります。

Detector モジュール管理の設定

Detector モジュールとのリモート管理セッションを確立するには、Detector モジュールの管理ポートを設定します。

管理のために VLAN を選択するには、次のコマンドを使用します。

anomaly-detector module *module_number* **management-port access-vlan** *vlan_number*

表 2-1 で、**anomaly-detector 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-detector 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挿入するためのスロットの番号（スイッチまたはルータのモデルに応じて 1 ～ 13）。
management-port	スーパーバイザ エンジンと Detector モジュール間で管理トラフィックを転送するポートを指定します。
access-vlan *vlan_number*	管理に使用する VLAN ID を指定します。デフォルトは VLAN 1 です。

現在の管理ポート設定を参照するには、**show anomaly-detector module** コマンドを使用します（P.2-13 の「Detector モジュールの設定の確認」を参照）。

次の例は、シャーシの番号 *4* のスロットに挿入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-detector module 4 management-port access-vlan 5
```

Detector モジュールとのリモート管理セッションを確立するには、Detector モジュールで、次のような設定も必要になります。

- Detector モジュールの管理ポート インターフェイスを設定する。P.3-8 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.3-13 の「Detector モジュールの管理」を参照してください。

トラフィックをキャプチャするためのトラフィックの送信元の設定

ゾーンに送信されるトラフィックをキャプチャし、そのコピーを Detector モジュールに渡すようにスイッチを設定する必要があります。Detector モジュールは、自身を通過するネットワーク トラフィックを分析し、そのトラフィックを監視して、進化し続ける攻撃パターンがないか調べます。

次のいずれかの方法を使用して、ネットワーク トラフィックを Detector モジュールに渡すことができます。

- Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）: 1 つまたは複数の送信元ポートで受信、送信、または送受信されたトラフィックを分析のために宛先ポートにキャプチャします。Detector モジュールは、SPAN セッション用に 1 つの宛先ポートを提供します。詳細については、P.2-7 の「SPAN の設定」を参照してください。
- VLAN access list（VACL; VLAN アクセスリスト）: WAN インターフェイスまたは VLAN から Detector モジュールのデータ ポートにトラフィックを転送します。この方法は、同じ目的での SPAN の使用に代わるものです。1 つの VLAN または複数の VLAN からのトラフィックをキャプチャするように VACL を設定できます。詳細については、P.2-4 の「VACL の設定」を参照してください。

SPAN の詳細については、『*Catalyst 6500 Series Switch Software Configuration Guide*』または『*Cisco 7600 Series Router Software Configuration Guide*』の「Configuring SPAN and RSPAN」を参照してください。

VACL の詳細については、『*Catalyst 6500 Series Switch Software Configuration Guide*』または『*Cisco 7600 Series Router Software Configuration Guide*』の「Configuring VLAN ACLs」を参照してください。

Detector モジュールで監視するために、1 つの VLAN または複数の VLAN からのトラフィックをキャプチャできます。特定の VLAN からのトラフィックだけを監視する場合は、監視しない VLAN をキャプチャ機能から消去する必要があります。

この項では、次のトピックについて取り上げます。

VACL の設定

1 つの VLAN または複数の VLAN からの Detector モジュール用トラフィックをキャプチャするように VACL を設定できます。

（注）　この項の手順は、VLAN 上の Detector モジュール用トラフィックをキャプチャするように VACL を設定するための基本情報です。詳細については、該当する Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータの設定ガイドを参照してください。

VLAN 上の Detector モジュール用トラフィックをキャプチャするように VACL を設定するには、次の手順を実行します。

ステップ 1　Access Control List（ACL; アクセス コントロール リスト）を定義し、次のコマンドを入力して、permit 文および deny 文（あるいはそのいずれか）によって Access Control Entry（ACE; アクセスコントロール エントリ）を追加します。

```
ip access-list {standard | extended} acl-name
```

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

表 2-2　ip access-list コマンドの引数とキーワード

パラメータ	説明
standard	標準の IP アクセスリストを指定します。
extended	拡張 IP アクセスリストを指定します。
acl-name	ACL の名前。名前には、スペースも疑問符も使用できません。また、番号付きアクセスリストと明確に区別するために、名前はアルファベット文字で始める必要があります。

（注）　代わりに、**access-list** コマンドを使用することもできます。

ステップ 2　次のコマンドを入力して、VLAN アクセス マップを定義します。

```
vlan access-map map_name [0-65535]
```

map_name 引数には、アクセス マップの名前タグを指定します。シーケンス番号を指定できます。シーケンス番号を指定しない場合は、番号が自動的に割り当てられます。このコマンドを実行すると、VLAN アクセス マップ設定モードに入ります。

マップ シーケンスごとに 1 つの match 句と 1 つの action 句を入力できます。

ステップ 3　次のコマンドを入力して、VLAN アクセス マップ シーケンスに match 句を設定します。

```
match ip address {acl_number | acl_name}
```

表 2-3 で、**match ip address** コマンドの引数とキーワードについて説明します。

表 2-3　match ip address コマンドの引数

パラメータ	説明
acl_number	VLAN アクセス マップ シーケンス用の 1 つまたは複数の IP ACL。有効な値は、1 ～ 199 および 1300 ～ 2699 です。
acl_name	IP ACL 名。

ステップ 4　次のコマンドを入力して、ネットワーク トラフィックを転送するように、VLAN アクセス マップ シーケンスに action 句を設定します。

```
action forward capture
```

ステップ 5　次のコマンドを入力して、VLAN アクセス マップを VLAN インターフェイスに適用します。

```
vlan filter map_name vlan-list vlan_list
```

表 2-4 に、**vlan filter** コマンドの引数とキーワードを示します。

表 2-4　vlan filter コマンドの引数とキーワード

パラメータ	説明
map_name	VLAN アクセス マップ タグ。
vlan-list *vlan_list*	VLAN リストを指定します。有効な値は、1 ～ 4094 です。

ステップ 6　（オプション）次のコマンドを入力して、キャプチャフラグの付いたトラフィックをキャプチャするように Detector モジュールのデータ ポートを設定します。

次のコマンドを入力します。

```
anomaly-detector module slot_number data-port port_number capture allowed-vlan
vlan_range
```

（注）　データ ポートを指定しない場合、Detector はすべての VLAN からのトラフィックのキャプチャをイネーブルにします。

表 2-5 で、**anomaly-detector module capture** コマンドの引数とキーワードについて説明します。

表 2-5　anomaly-detector module capture 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挿入するためのスロットの番号（スイッチまたはルータのモデルに応じて 1 ～ 13）。
data-port *port_number*	データ用に使用するポートの番号を指定します。データ ポート オプションは次のとおりです。 • 1 Gbps 動作：ポート 1。 • 2 Gbps 動作：ポート 1 と 2。
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 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）。

ステップ 7　次のコマンドを入力して、Detector モジュールでキャプチャ機能をイネーブルにします。

```
anomaly-detector module module_number data-port port_number capture
```

表 2-6 で、**anomaly-detector module capture** 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　anomaly-detector module capture コマンドの引数とキーワード

パラメータ	説明
module_number	モジュールを挿入するためのシャーシ スロットの番号（スイッチまたはルータのモデルに応じて 1 ～ 13）。
data-port *port_number*	データ用に使用するポートの番号を指定します。データ ポート オプションは次のとおりです。 • 1 Gbps 動作：ポート 1。 • 2 Gbps 動作：ポート 1 と 2。コマンドを 2 回（各ポート番号に 1 回）入力して、両方のデータ ポートでキャプチャ機能をイネーブルにする必要があります。

（注）　1 Gbps 動作の場合は、一方のデータ ポートを SPAN 宛先ポートまたはキャプチャ ポートとして設定する必要があります。2 Gbps 動作の場合は、次の方法で 2 つのデータ ポートを設定できます。

- 両方のデータ ポートを SPAN 宛先ポートとして設定
- 両方のデータ ポートをキャプチャ ポートとして設定
- 一方のデータ ポートを SPAN 宛先ポート、もう一方をキャプチャ ポートとして設定

次の 2-Gpbs 動作の例は、VLAN の Detector モジュール トラフィックをキャプチャするための VACL の設定方法を示しています。

```
Sup (config)# ip access-list extended Permit_Any
Sup (config-ext-nacl)# permit ip any any
Sup (config-ext-nacl)# exit
Sup (config)# vlan access-map Detector 10
Sup (config-access-map)# match ip address Permit_Any
Sup (config-access-map)# action forward capture
Sup (config-access-map)# exit
Sup (config)# vlan filter Detector vlan-list 921,931
Sup (config)# anomaly-detector module 6 data-port 1 capture
Sup (config)# anomaly-detector module 6 data-port 1 capture allowed-vlan 921
Sup (config)# anomaly-detector module 6 data-port 2 capture
Sup (config)# anomaly-detector module 6 data-port 2 capture allowed-vlan 931
```

SPAN の設定

SPAN セッションを作成し、送信元（監視される）ポートと宛先（監視する）ポートを指定します。Detector モジュールのポートを SPAN の送信元ポートとして使用することはできません。

（注）　この項の手順は、SPAN　セッションを作成するための基本情報です。詳細については、該当する Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータの設定ガイドを参照してください。

スーパーバイザ エンジン コンソールで特権 EXEC モードから次の手順を実行し、SPAN セッションを作成して、送信元ポートと宛先ポートを指定します。

ステップ 1　次のコマンドを入力して、SPAN セッションおよび送信元ポート（監視されるポート）を指定します。

monitor session *session_number* **source interface** *interface-id* [**,** | **-**] [**rx** | **tx**]

表 2-7 で、**monitor session** コマンドの引数とキーワードについて説明します。

表 2-7　monitor session コマンドの引数とキーワード

パラメータ	説明
session_number	*セッションの識別番号。*
source interface *interface-id*	監視対象の送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスおよびポートチャネル論理インターフェイス（port-channel port-channel-number または VLAN）が含まれます。

表 2-7　monitor session コマンドの引数とキーワード（続き）

パラメータ	説明
, | -	（オプション）一連のインターフェイスまたはインターフェイス範囲。カンマの前後およびハイフンの前後にはスペースを入力します。
rx | tx	（オプション）監視対象のトラフィックの方向を指定します。トラフィックの方向を指定しない場合、送信元インターフェイスは、送信トラフィックと受信トラフィックの両方を送信します。 ⚠ **注意**　Detector モジュールは、指定されたすべての方向のトラフィックのキャプチャを受信します。rx と tx の両方を指定しないでください。パケットの 2 つのコピーが Detector モジュールのポートに転送され、Detector モジュールのパフォーマンスが低下します。 • **rx**：受信トラフィックを監視するように指定します。 • **tx**：送信トラフィックを監視するように指定します。

ステップ 2　次のコマンドを入力して、SPAN セッションおよび宛先ポート（監視するポート）を指定します。

```
monitor session SPAN_session_number destination anomaly-detector-module module_number
[data-port port]
```

表 2-8 で、**monitor session destination** コマンドの引数とキーワードについて説明します。

表 2-8　monitor session destination コマンドの引数とキーワード

パラメータ	説明
SPAN_session_number	*インターフェイスの識別番号*。1 と指定します。
anomaly-detector-module *module-number*	モジュールをシャーシに挿入するためのスロットの番号（スイッチまたはルータのモデルに応じて 1 ～ 13）を指定します。
data-port *port*	データのキャプチャに使用するポートの番号を指定します。データポート オプションは次のとおりです。 • 1 Gbps 動作：ポート 1。 • 2 Gbps 動作：ポート 1 と 2。コマンドを 2 回（各ポート番号に 1 回）入力して、両方のデータ ポートを宛先ポートとして指定する必要があります。

ステップ 3　次のコマンドを入力して、特権 EXEC モードに戻ります。

```
end
```

ステップ 4　次のコマンドを入力して、エントリを確認します。

```
show monitor [session session_number]
```

session_number 引数には、セッション識別番号を指定します。

次の 1 Gbps 動作の例は、SPAN セッションとしてセッション 1 を設定し、送信元ポートから宛先ポートへのトラフィックを監視する方法を示しています。受信トラフィックが送信元ポート 1 から Detector モジュールにミラーリングされます。

```
Sup(config)# monitor session 1 source interface GigabitEthernet 1/2 rx
Sup(config)# monitor session 1 destination anomaly-detector-module 4 data-port 1
```

次の 2 Gbps 動作の例は、SPAN セッションとしてセッション 1 と 2 を設定し、送信元ポートから 2 つの宛先ポートへのトラフィックを監視する方法を示しています。受信トラフィックが送信元ポート 1 と 2 から Detector モジュールのポート 1 と 2 にミラーリングされます。

```
Sup(config)# monitor session 1 source interface GigabitEthernet 1/2 rx
Sup(config)# monitor session 1 destination anomaly-detector-module 4 data-port 1
Sup(config)# monitor session 2 source interface GigabitEthernet 2/2 rx
Sup(config)# monitor session 2 destination anomaly-detector-module 4 data-port 2
```

Detector モジュールとのセッションの確立

Detector 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のログ 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 2-9 で、**session slot** コマンドの引数とキーワードについて説明します。

表 2-9　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挿入するためのスロットの番号（スイッチまたはルータのモデルに応じて 1 ～ 13）。
processor *processor_number*	Detector モジュールのプロセッサの番号を指定します。Detector モジュールは、プロセッサ 1 を介した管理だけをサポートします。

ステップ 3　次のように、Detector モジュールのログイン 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。

Detector モジュールとのセッションを初めて確立している場合は、admin ユーザ アカウントおよび 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 文字の英数字にする必要があります。パスワードは、いつでも変更できます。詳細については、P.4-7 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 プロンプトが user@DETECTOR# と表示されます。**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。

Detector モジュールのリブート

Detector モジュールを制御するために、Cisco IOS には **boot**、**shutdown**、**power enable** および **reset** というコマンド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。Detector モジュールをリロードする方法については、P.13-9 の「Detector モジュールのリロード」を参照してください。

- **shutdown**：オペレーティング システムを正常に停止させ、データが失われないことを保証します。Detector モジュールの破損を防ぐため、Detector モジュールを正常にシャットダウンすることが重要です。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、モジュールが挿入されているシャーシ内のスロットの番号を指定します。

  その後、**hw-module module** *module_number* **reset** コマンドを入力して、Detector モジュールを再起動する必要があります。

  次の例は、Detector 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、Detector 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。このコマンドを使用して、シャットダウンからの復旧や、次の Detector モジュール動作イメージの切り替えを行います。
  - アプリケーション パーティション（AP）：Detector モジュール アプリケーション ソフトウェア イメージ（P.13-10 の「Detector モジュール ソフトウェアのアップグレード」を参照）。
  - メンテナンス パーティション（MP）：基本モジュールの初期化およびドーター カードの制御の機能のために必要なソフトウェア イメージ（P.13-10 の「Detector モジュール ソフトウェアのアップグレード」を参照）。

  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 引数には、モジュールが挿入されているシャーシ内のスロットの番号を指定します。*string* 引数は PC ブート シーケンス用のオプションの文字列です。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.13-10 の「Detector モジュール 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、Detector 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、シャーシから安全に取り外すことが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、モジュールが挿入されているシャーシ内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、Detector 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**：次回電源投入時に Detector モジュールを強制的に MP にブートさせます。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、モジュールが挿入されているシャーシ内のスロットの番号を指定します。

Detector モジュールが次のブート サイクルでデフォルト パーティション（AP）に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 Detector モジュールが AP にブートするための設定方法を示しています。

```
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の詳細については、P.13-9 の「Detector 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。

Detector モジュールの設定の確認

スーパーバイザ エンジンで Detector 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-detector module *slot_number* {**management-port** | **data-port** *port_number*} [**state** | **traffic**]

表 2-10 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 2-10　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挿入するためのスロットの番号（スイッチまたはルータのモデルに応じて 1 ～ 13）。
management-port	管理ポートの情報を指定します。
data-port *port_number*	ポート番号を指定します。データ ポート オプションは次のとおりです。 • 1 Gbps 動作：ポート 1 • 2 Gbps 動作：ポート 1 と 2
state	（オプション）指定のポートの設定を指定します。
traffic	（オプション）指定のポートのトラフィック統計情報を指定します。

次の例は、スーパーバイザ エンジンでの Detector 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-detector module 7 data-port 1 state
```