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、スーパーバイザ エンジンで Cisco Traffic Anomaly Detector Module（Detector モジュール）を設定する方法について説明します。

Cisco Traffic Anomaly Detector Module（Detector モジュール）は、次のいずれかの製品に設置できる Cisco IOS アプリケーション モジュールです。

- Supervisor Engine 720（SUP720）、または Multilayer Switch Feature Card 2（MSFC2; マルチレイヤ スイッチ フィーチャ カード 2）を備えた Supervisor Engine 2（SUP2）が搭載された、Cisco Catalyst 6500 シリーズ スイッチ。Catalyst 6500 で Detector モジュールをサポートするには、IOS 12.2(18)SXD3 以降が必要です。
- SUP720 が搭載された Cisco 7600 シリーズ ルータ。7600 シリーズ ルータで Detector モジュールをサポートするには、IOS 12.2(18)SXE 以降が必要です。

この章は、次の項で構成されています。

スーパーバイザで 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。

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 シャーシに 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 CardType ModelSerial 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.fe0b3.07.2(1)4.0(0.10)Ok
...
Sup#
```

（注）　Detector モジュールが初めて設置された場合、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の時間として、少なくとも 5 分間見込んでおいてください。

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-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 コマンドの引数

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）。
vlan_number	管理に使用する VLAN ID を設定します。

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-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 eth1 を設定する。詳細については、P.3-9 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。詳細については、P.3-8 の「Detector 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。

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。

- SPAN：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する。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.2-9 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。これは、同じ目的での SPAN の使用に代わる方法です。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.2-6 の「VACL の設定」を参照してください。

SPAN の詳細については、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/span.htm
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_2/confg_gd/span.htm

VACL の詳細については、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/vacl.htm
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_82/confg_gd/acc_list.htm#1053650

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。

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。

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 list（ACL; アクセス リスト）を定義し、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。次のコマンドを入力します。

```
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　VLAN アクセス マップを定義します。次のコマンドを入力します。

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

```
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 を選択します。有効な値は、1 ～ 199 および 1300 ～ 2699 です。
acl_name	IP ACL を名前で選択します。

ステップ 4　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。次のコマンドを入力します。

```
action forward capture
```

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

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

表 2-4 で、**vlan filter** コマンドの引数について説明します。

表 2-4　vlan filter コマンドの引数

パラメータ	説明
map_name	VLAN アクセス マップ タグ。
vlan_list	VLAN リスト。有効な値は、1 ～ 4094 です。

ステップ 6　（オプション）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。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。

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*

表 2-5 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 2-5　anomaly-detector module allowed-vlan コマンドの引数

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_number	データ用に使用するポートの番号。Detector モジュールでは、データ用にポート *2* がサポートされています。
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）。

ステップ 7　Detector モジュールでキャプチャ機能をイネーブルにします。

次のコマンドを入力します。

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

表 2-6 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 2-6　anomaly-detector module コマンドの引数

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_number	データ用に使用するポートの番号。Detector モジュールでは、データ用にポート *1* がサポートされています。

（注）　Detector モジュールのデータ ポートを SPAN 宛先ポートとキャプチャ ポートの両方として設定することはできません。

次の例を参考にしてください。

```
Sup (config)# ip access-list extended 10
Sup (config-ext-nacl)# vlan access-map Detector 10
Sup (config-ext-nacl)# match ip address 10
Sup (config-ext-nacl)# action forward capture
Sup (config-ext-nacl)# exit
Sup (config)# vlan filter Detector vlan-list 85
Sup (config)# anomaly-detector module 8 data-port 2 capture
```

SPAN の設定

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（監視される）ポートと宛先（監視する）ポートを指定します。

（注）　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。

ステップ 1　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。次のコマンドを入力します。

```
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 source 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。
interface-id	監視対象の送信元ポート。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）が含まれます。
, | -	（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を指定します。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。両方を指定すると、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るため、パフォーマンスが低下する可能性があります。 • **rx**：受信トラフィックを監視します。 • **tx**：送信トラフィックを監視します。

ステップ 2　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。次のコマンドを入力します。

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

表 2-8 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 2-8　monitor session destination コマンドの引数

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。
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	データのキャプチャに使用するポートの番号。 Detector モジュールでは、データ用にポート 1 がサポートされています。

ステップ 3　特権 EXEC モードに戻ります。次のコマンドを入力します。

```
end
```

ステップ 4　エントリを確認します。次のコマンドを入力します。

```
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。双方向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 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 またはコンソールで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** コマンドの引数について説明します。

表 2-9　session slot コマンドの引数

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_number	Detector モジュールのプロセッサの番号。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。

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 3　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「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。このマニュアルでは、表記法としてこのプロンプトを使用します。**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 レベルで reload コマンドを発行すると、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.11-6 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。

  次の例を参考にしてください。

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

（注）　スイッチがリブートすると、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。このコマンドは通常、アップグレード プロセスで、AP イメージと MP イメージとの切り替え、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。*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.11-7 の「Detector モジュールのバージョンのアップグレード」を参照してください。

次の例を参考にしてください。

```
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、次のコマンドを入力します。

  power enable module *slot_number*

  次の例を参考にしてください。

  ```
  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 maintenance partition（MP; メンテナンス パーティション）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）からブートできるようにするには、次のコマンドを入力します。

  no boot device module *slot_number* cf:1

  次の例を参考にしてください。

  ```
  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.11-6 の「Detector モジュールのリブート」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入力します。

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

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_number	ポート番号。ポート 1 だけが使用されています。
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。

次の例を参考にしてください。

```
Sup# show anomaly-detector module 7 data-port 1 state
```