CHAPTER 15

IDSM-2 の設定

この章では、IDSM-2 の設定に固有の手順について説明します。

（注） Catalyst 6500 シリーズ スイッチは、6500 シリーズ スイッチおよび 7600 シリーズ ルータの両方を指す一般名として使用されます。

この章は、次の項で構成されています。

コンフィギュレーション シーケンス

IDSM-2 を設定するには、次のタスクを実行します。

1. IDSM-2 へのコマンド / コントロール アクセスのために Catalyst 6500 シリーズ スイッチを設定します。

   手順については、P.15-6 の「IDSM-2 へのコマンド / コントロール アクセスのための Catalyst 6500 シリーズ スイッチの設定」を参照してください。

2. IDSM-2 にログインします。

   IDSM-2 に対してセッションを開始する手順については、P.2-6 の「IDSM-2 へのログイン」を参照してください。

3. IDSM-2 を初期化します。

   setup コマンドを実行して、IDSM-2 を初期化します。

   手順については、P.3-3 の「センサーの初期化」を参照してください。

4. トラフィックを取り込んで侵入分析を行うように IDSM-2 を設定します。

   手順については、P.15-9 の「IDSM-2 用の Catalyst 6500 シリーズ スイッチの混合モードでの設定」および P.15-21 の「IDSM-2 用の Catalyst 6500 シリーズ スイッチのインライン モードでの設定」を参照してください。混合モードまたはインライン モードで実行するように IDSM-2 を設定する手順については、第 5 章「インターフェイスの設定」を参照してください。TCP リセット インターフェイスの詳細については、P.15-9 の「TCP リセット インターフェイスの使用方法」を参照してください。Cisco IOS ソフトウェアを使用して IDSM-2 のロード バランスを設定するための手順については、P.15-25 の「EtherChanneling の設定」を参照してください。

5. サービス アカウントを作成します。

   手順については、P.4-16 の「サービス アカウントの作成」を参照してください。

6. ユーザや信頼できるホストの追加など、その他の初期タスクを実行します。

   手順については、第 4 章「初期コンフィギュレーション タスク」を参照してください。

7. 侵入防御を設定します。

   手順については、第 6 章「イベント アクション ルールの設定」、第 7 章「シグニチャの定義」、および第 10 章「ブロッキングとレート制限のための ARC の設定」を参照してください。

8. 各種タスクを実行して、IDSM-2 が円滑に実行し続けるようにします。

   手順については、第 13 章「センサーの管理タスク」および P.15-30 の「IDSM-2 の管理タスク」を参照してください。

9. 新規シグニチャ アップデートとサービス パックで IPS ソフトウェアをアップグレードします。

   詳細については、P.18-2 の「Cisco IPS ソフトウェアの入手方法」を参照してください。

10. 必要に応じて、アプリケーション パーティションとメンテナンス パーティションのイメージを再作成します。

    手順については、P.17-31 の「IDSM-2 システム イメージのインストール」を参照してください。

IDSM-2 取り付けの確認

スイッチが IDSM-2 を認識し、オンラインにしたことを確認します。

取り付けを確認するには、次の手順を実行します。

ステップ 1　コンソールにログインします。

ステップ 2　Catalyst ソフトウェアの場合、次のように入力します。

```
cat6k> (enable) show module
Mod Slot Ports Module-Type                Model               Sub Status
--- ---- ----- ------------------------- ------------------- --- --------
1   1    2     1000BaseX Supervisor      WS-X6K-SUP1A-2GE    yes ok
15  1    1     Multilayer Switch Feature WS-F6K-MSFC         no  ok
2   2    48    10/100BaseTX Ethernet     WS-X6248-RJ-45      no  ok
3   3    48    10/100/1000BaseT Ethernet WS-X6548-GE-TX      no  ok
4   4    16    1000BaseX Ethernet        WS-X6516A-GBIC      no  ok
6   6    8     Intrusion Detection Mod   WS-SVC-IDSM2        yes ok

Mod Module-Name          Serial-Num
--- -------------------- -----------
1                        SAD041308AN
15                       SAD04120BRB
2                        SAD03475400
3                        SAD073906RC
4                        SAL0751QYN0
6                        SAD062004LV

Mod MAC-Address(es)                         Hw     Fw          Sw
--- --------------------------------------- ------ ----------- ------------------
1   00-d0-c0-cc-0e-d2 to 00-d0-c0-cc-0e-d3 3.1    5.3.1       8.4(1)
    00-d0-c0-cc-0e-d0 to 00-d0-c0-cc-0e-d1
    00-30-71-34-10-00 to 00-30-71-34-13-ff
15  00-30-7b-91-77-b0 to 00-30-7b-91-77-ef 1.4    12.1(23)E2 12.1(23)E2
2   00-30-96-2b-c7-2c to 00-30-96-2b-c7-5b 1.1    4.2(0.24)V 8.4(1)
3   00-0d-29-f6-01-98 to 00-0d-29-f6-01-c7 5.0    7.2(1)      8.4(1)
4   00-0e-83-af-15-48 to 00-0e-83-af-15-57 1.0    7.2(1)      8.4(1)
6   00-e0-b0-ff-3b-80 to 00-e0-b0-ff-3b-87 0.102  7.2(0.67)   5.0(0.30)

Mod Sub-Type                Sub-Model           Sub-Serial  Sub-Hw Sub-Sw
--- ----------------------- ------------------- ----------- ------ ------
1   L3 Switching Engine     WS-F6K-PFC          SAD041303G6 1.1
6   IDS 2 accelerator board WS-SVC-IDSUPG       .           2.0
cat6k> (enable)
```

ステップ 3　Cisco IOS ソフトウェアの場合、次のように入力します。

```
switch# show module
Mod Ports Card Type                                Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  1    48  48 port 10/100 mb RJ-45 ethernet       WS-X6248-RJ-45     SAD0401012S
  2    48  48 port 10/100 mb RJ45                 WS-X6348-RJ-45     SAL04483QBL
  3    48  SFM-capable 48 port 10/100/1000mb RJ45 WS-X6548-GE-TX     SAD073906GH
  6    16  SFM-capable 16 port 1000mb GBIC        WS-X6516A-GBIC     SAL0740MMYJ
  7     2  Supervisor Engine 720 (Active)         WS-SUP720-3BXL     SAD08320L2T
  9     1  1 port 10-Gigabit Ethernet Module      WS-X6502-10GE      SAD071903BT
 10     3  Anomaly Detector Module                WS-SVC-ADM-1-K9    SAD084104JR
 11     8  Intrusion Detection System             WS-SVC-IDSM2       SAD05380608
 13     8  Intrusion Detection System             WS-SVC-IDSM-2      SAD072405D8

Mod MAC addresses                       Hw     Fw           Sw           Status
--- ----------------------------------- ------ ------------ ------------ -------
  1  00d0.d328.e2ac to 00d0.d328.e2db   1.1    4.2(0.24)VAI 8.5(0.46)ROC Ok
  2  0003.6c14.e1d0 to 0003.6c14.e1ff   1.4    5.4(2)       8.5(0.46)ROC Ok
  3  000d.29f6.7a80 to 000d.29f6.7aaf   5.0    7.2(1)       8.5(0.46)ROC Ok
  6  000d.ed23.1658 to 000d.ed23.1667   1.0    7.2(1)       8.5(0.46)ROC Ok
  7  0011.21a1.1398 to 0011.21a1.139b   4.0    8.1(3)       12.2(PIKESPE Ok
  9  000d.29c1.41bc to 000d.29c1.41bc   1.3    Unknown      Unknown      PwrDown
 10  000b.fcf8.2ca8 to 000b.fcf8.2caf   0.101  7.2(1)       4.0(0.25)    Ok
 11  00e0.b0ff.3340 to 00e0.b0ff.3347   0.102  7.2(0.67)    5.0(1)       Ok
 13  0003.feab.c850 to 0003.feab.c857   4.0    7.2(1)       5.0(1)       Ok

Mod Sub-Module                  Model              Serial       Hw     Status
--- --------------------------- ------------------ ------------ ------- -------
  7 Policy Feature Card 3       WS-F6K-PFC3BXL     SAD083305A1  1.3    Ok
  7 MSFC3 Daughterboard         WS-SUP720          SAD083206JX  2.1    Ok
 11 IDS 2 accelerator board     WS-SVC-IDSUPG      .            2.0    Ok
 13 IDS 2 accelerator board     WS-SVC-IDSUPG      0347331976   2.0    Ok

Mod Online Diag Status
--- -------------------
  1 Pass
  2 Pass
  3 Pass
  6 Pass
  7 Pass
  9 Unknown
 10 Not Applicable
 11 Pass
 13 Pass
switch#
```

（注）　IDSM-2　を初めて取り付けたときに、ステータスが「other」を示すのは正常な動作です。IDSM-2 が診断ルーチンを完了してオンラインになった後で、ステータスは ok を示します。IDSM-2 がオンラインになるまでの時間としては、最長で 5 分間みてください。

IDSM-2 の取り付け確認後、全メモリ テストをイネーブルにするための詳細については、P.15-30 の「全メモリ テストのイネーブル化」を参照してください。

サポートされている IDSM-2 の設定

表 15-1 にサポートされている IDSM-2 の設定を示します。

表 15-1　サポートされている設定

スーパーバイザ	SPAN/ RSPAN	VACL キャプチャ	VACL ブロッキング	RACL ブロッキング	Catalyst ソフトウェア	Cisco IOS ソフトウェア
スーパーバイザ 1A	X	—	—	—	7.5(1)	—
PFC1 組み込みのスーパーバイザ 1A	X	X	X	—	7.5(1)	—
PFC1 または MSFC1 組み込みのスーパーバイザ 1A	X	X	X[1]	X	7.5(1)	[2]
スーパーバイザ 1A-PFC2 または MSFC2	X	X	X[3]	X	7.5(1)	12.1(19)E1
PFC2 組み込みのスーパーバイザ 2	X	X	X	—	7.5(1)	—
PFC2 または MSFC2 組み込みのスーパーバイザ 2	X	X	X[4]	X	7.5(1)	12.1(19)E、12.2(14)SY
スーパーバイザ 720（PFC3 および MSFC3 統合）	X	X	[5]	X	—	12.2(14)SX1

1. IDSM-2 による VACL ブロッキングは、Catalyst ソフトウェアでサポートされていますが、この設定に関しては Cisco IOS ではサポートされていません。
2. Cisco IOS は PFC1 または MSFC1 組み込みのスーパーバイザ 1A でサポートされています。しかし、IDSM-2 はこの設定ではサポートされていません。
3. IDSM-2 による VACL ブロッキングは、Catalyst ソフトウェアでサポートされていますが、この設定に関しては Cisco IOS ではサポートされていません。
4. IDSM-2 による VACL ブロッキングは、Catalyst ソフトウェアでサポートされていますが、この設定に関しては Cisco IOS ではサポートされていません。
5. Cisco IOS 組み込みのスーパーバイザ 720 は VACL の deny 文をサポートしています。しかし、IDSM-2 は、Cisco IOS 形式の VACL でブロックを実行できません。

注意　スーパーバイザ 1A と PFC2 の組み合せはサポートされていません。PFC2 または MSFC2 が組み込まれていないスーパーバイザ 2 は、Catalyst ソフトウェアや Cisco IOS ソフトウェアではサポートされていません。

IDSM-2 へのコマンド / コントロール アクセスのための Catalyst 6500 シリーズ スイッチの設定

IDSM-2 にコマンド / コントロール アクセスを行うように Catalyst 6500 シリーズ スイッチを設定する必要があります。

この項では、次のトピックについて説明します。

Catalyst ソフトウェア

IDSM-2 へのコマンド / コントロール アクセスのために Catalyst 6500 シリーズ スイッチを設定するには、次の手順を実行します。

ステップ 1　コンソールにログインします。

ステップ 2　特権モードに入ります。

```
cat6k> enable
```

ステップ 3　コマンド / コントロール ポートを正しい VLAN に置きます。

```
cat6k> (enable) set vlan command_and_control_vlan_number
idsm2_slot_number/command_and_control_port_number
```

例

```
cat6k> (enable) set vlan 147 6/2
VLAN 147 modified.
VLAN 146 modified.
VLAN  Mod/Ports
---- ----------------------
147   2/5,2/16-18
      6/2
```

コマンド / コントロール ポート番号は、常に 2 です。

ステップ 4　IDSM-2 に対してセッションを開始し、ネットワーク IP アドレスを ping します。

```
cat6k> session slot_number
idsm-2# ping network_ip_address
```

例

```
console> (enable) session 6
Trying IDS-6...
Connected to IDS-6.
Escape character is '^]'.

login: cisco
Password:
Last login: Thu Mar 3 09:40:53 from 127.0.0.11
***NOTICE***
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco
cryptographic products does not imply third-party authority to import, export,
distribute or use encryption. Importers, exporters, distributors and users are
responsible for compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable to comply with
U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license to obtain a new license or install a
license.
idsm-2# ping 10.89.149.126
PING 10.89.149.126 (10.89.149.126): 56 data bytes
64 bytes from 10.89.149.126: icmp_seq=0 ttl=255 time=0.3 ms
64 bytes from 10.89.149.126: icmp_seq=1 ttl=255 time=0.3 ms
64 bytes from 10.89.149.126: icmp_seq=2 ttl=255 time=0.3 ms
64 bytes from 10.89.149.126: icmp_seq=3 ttl=255 time=0.3 ms
--- 10.89.149.126 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.3/0.3/0.3 ms
idsm-2# exit
cat6k> (enable)
```

ステップ 5　IDSM-2 を初期化します。

手順については、P.3-3 の「センサーの初期化」を参照してください。

ステップ 6　IDSM-2 のデフォルト ルータを ping します。

ステップ 7　管理ステーションが IDSM-2 に対して ping、SSH または Telnet 接続、および Web ブラウザでの参照ができることを確認します。

Cisco IOS ソフトウェア

IDSM-2 へのコマンド / コントロール アクセスのために Catalyst 6500 シリーズ スイッチを設定するには、次の手順を実行します。

ステップ 1　コンソールにログインします。

ステップ 2　グローバル コンフィギュレーション モードに入ります。

```
switch# configure terminal
```

ステップ 3　コマンド / コントロール ポートを正しい VLAN に置きます。

```
switch (config)# intrusion-detection module module_number management-port access-vlan
vlan_number
```

例

```
switch (config)# intrusion-detection module 11 management-port access-vlan 146
```

ステップ 4　IDSM-2 に対してセッションを開始し、ネットワーク IP アドレスを ping して、接続できることを確認します。

```
switch# session slot module_number processor 1
idsm-2# ping network_ip_address
```

例

```
switch# session slot 11 processor 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.91 ... Open

login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco
cryptographic products does not imply third-party authority to import, export,
distribute or use encryption. Importers, exporters, distributors and users are
responsible for compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable to comply with
U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.
idsm-2# ping 10.89.149.254
PING 10.89.149.254 (10.89.149.254): 56 data bytes
64 bytes from 10.89.149.254: icmp_seq=0 ttl=255 time=0.2 ms
64 bytes from 10.89.149.254: icmp_seq=1 ttl=255 time=0.2 ms
64 bytes from 10.89.149.254: icmp_seq=2 ttl=255 time=0.2 ms
64 bytes from 10.89.149.254: icmp_seq=3 ttl=255 time=0.2 ms
--- 10.89.149.254 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.2 ms
idsm-2# exit
[Connection to 127.0.0.91 closed by foreign host]
switch#
```

ステップ 5　IDSM-2 をまだ初期化していない場合は、初期化します。

手順については、P.3-3 の「センサーの初期化」を参照してください。

IDSM-2 用の Catalyst 6500 シリーズ スイッチの混合モードでの設定

トラフィックは、SPAN または VACL キャプチャを使用して、IDSM-2 上での混合分析のために取り込まれます。ポート 1（GigabitEthernet0/1）は TCP リセット ポートとして、ポート 2（GigabitEthernet0/2）はコマンド / コントロール ポートとして、およびポート 7 とポート 8（GigabitEthernet0/7 と GigabitEthernet0/8）はモニタリング ポートとして、それぞれ使用されます。両方のモニタリング ポートを、SPAN 宛先ポートまたは VACL キャプチャ ポートのいずれかとして設定できます。

注意　両方のポートをモニタリング ポートに設定する場合は、必ずこれらのポートが別のトラフィックを監視するように設定してください。

注意　IDSM-2 はトラフィックを受信しないので、IDSM-2 データ ポートを SPAN 宛先ポートと VACL キャプチャ ポートの両方として設定しないでください。このデュアル コンフィギュレーション（SPAN および VACL）を行うと、スイッチで問題が発生し、トラフィックが適切に送信されなくなります。

この項では、次のトピックについて説明します。

TCP リセット インターフェイスの使用方法

IDSM-2 には TCP リセット インターフェイス（ポート 1）があります。IDSM-2 は、センシング ポートに TCP リセットを送信できないので、専用の TCP リセット インターフェイスが用意されています。

IDSM-2 においてリセット上の問題が発生した場合は、次の手順を試してください。

- センシング ポートがアクセス ポート（1 つの VLAN）である場合、リセット ポートが同じ VLAN に存在するように設定する必要があります。
- センシング ポートが dot1q トランク ポート（マルチ VLAN）である場合、このセンシング ポートとリセット ポートはすべて同じネイティブ VLAN を持つ必要があり、リセット ポートは両方のセンシング ポートによってトランク接続されている VLAN すべてにトランク接続されている必要があります。

SPAN の設定

IDSM-2 はイーサネットまたはファースト イーサネット SPAN ソース ポートからのイーサネット VLAN トラフィックを分析できます。つまり、イーサネット VLAN を SPAN ソースとして指定できます。

この項では、次のトピックについて説明します。

Catalyst ソフトウェア

IDSM-2 に対して SPAN をイネーブルにするには、特権モードで **set span** コマンドを使用します。

（注）　IDSM-2 ポート番号は、7 または 8 に限られます。

次のオプションが適用されます。

- **disable**：ポート モニタリングをディセーブルにします。
- *module/port*：送信元モジュール番号およびポート番号。
- *vlan*：送信元 VLAN 番号。
- *module/port*：宛先モジュール番号およびポート番号。
- **both**：トラフィックの受信および転送の両方。
- **filter**：VLAN にフィルタを適用します。
- **inpkts**：宛先ポートへのパケット着信をイネーブル / ディセーブルにします。
- **learning**：MAC アドレス ラーニングをイネーブル / ディセーブルにします。
- **multicast**：マルチキャスト トラフィックをイネーブル / ディセーブルにします。
- **rx**：トラフィックの受信。
- **session**：SPAN セッションのセッション番号。
- **tx**：トラフィックの送信。

IDSM-2 上の SPAN 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　コンソールにログインします。

ステップ 2　特権モードに入ります。

```
cat6k> enable
```

ステップ 3　IDSM-2 に対して SPAN をイネーブルにします。

- 送信元ポートから

```
cat6k> (enable) set span 3/3 13/7
Destination     : Port 13/7
Admin Source    : Port 3/3
Oper Source     : Port 3/3
Direction       : transmit/receive
Incoming Packets: disabled
Learning        : enabled
Multicast       : enabled
Filter          : -

Session Number  : 1

cat6k> (enable)
```

（注）　送信元トランク ポートで特定の VLAN のトラフィックを監視するには、**filter** キーワードを使用します。

- VLAN から

```
cat6k> (enable) set span 650 13/7 rx

Destination : Port 13/7
Admin Source : VLAN 650
Oper Source : Port 11/1,13/1
Direction : receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -

Session Number : 1

cat6k> (enable)
```

ステップ 4　SPAN セッションを表示します。

```
cat6k> (enable) show span

Destination     : Port 13/7
Admin Source    : VLAN 650
Oper Source     : Port 11/1,13/1
Direction       : receive
Incoming Packets: disabled
Learning        : enabled
Multicast       : enabled
Filter          : -

Session Number  : 1

Total local span sessions:  1
cat6k> (enable)
```

ステップ 5　IDSM-2 にトラフィックを送信している SPAN セッションをディセーブルにするには、次のように入力します。

```
cat6k> (enable) set span disable session 1
This command will disable your span session.
Do you want to continue (y/n) [n]? y
Disabled Port 13/7 to monitor receive traffic of VLAN 650
cat6k> (enable)
```

（注）　SPAN の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

Cisco IOS ソフトウェア

IDSM-2 上で SPAN をイネーブルにするには、グローバル コンフィギュレーション モードで **monitor session** コマンドを使用します。

（注）　IDSM-2 データ ポート番号には、1 または 2 を使用します。

次のオプションが適用されます。

- **interface**：SPAN 送信元インターフェイス
- **remote**：SPAN 送信元リモート
- **vlan**：SPAN 送信元 VLAN
- **GigabitEthernet**：ギガビット イーサネット IEEE 802.3z
- **Port-channel**：インターフェイスのイーサネット チャネル
- **,**：インターフェイスの別の範囲を指定
- **--**：インターフェイスの範囲を指定
- **both**：受信および送信トラフィックを監視
- **rx**：受信トラフィックのみを監視
- **tx**：送信トラフィックのみを監視
- **intrusion-detection-module**：SPAN 宛先侵入検出モジュール
- **destination**：SPAN 宛先インターフェイスまたは VLAN
- **filter**：SPAN フィルタ VLAN
- **source**：SPAN 送信元インターフェイス、VLAN
- **type**：モニタ セッションのタイプ

IDSM-2 上の SPAN 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　コンソールにログインします。

ステップ 2　グローバル コンフィギュレーション モードに入ります。

```
switch# configure terminal
```

ステップ 3　モニタ セッションの送信元インターフェイスを設定します。

```
switch (config)# monitor session (session_number) source interface
interface/port_number [, | - | rx | tx | both]
```

例

```
switch (config)# monitor session 1 source interface GigabitEthernet2/23 both
```

ステップ 4　IDSM-2 データ ポートを SPAN 宛先としてイネーブルにします。

```
switch (config)# monitor session (session_number) destination
intrusion-detection-module module_number data-port data_port_number
```

例

```
switch (config)# monitor session 1 destination intrusion-detection-module 9 data-port
1
```

ステップ 5　（オプション）モニタ セッションをディセーブルにするには、次のように入力します。

```
switch (config)# no monitor session session_number
```

ステップ 6　（オプション）スイッチ ポート トランクから特定の VLAN のみが見えるように SPAN セッションをフィルタリングするには、次のように入力します。

```
switch (config)# monitor session (session_number) {filter vlan {vlan_ID} [, | - ]}
```

例

```
switch (config)# monitor session 1 filter vlan 146
```

ステップ 7　コンフィギュレーション モードを終了します。

```
switch (config)# exit
```

ステップ 8　現在のモニタ セッションを表示するには、次のように入力します。

```
switch # show monitor session session_number
```

例

```
switch # show monitor session 1
    Session 1
    ---------
    Type                   : Local Session
    Source Ports           :
        Both               : Gi2/23
    Destination Ports      : intrusion-detection-module 9 data-port 1
```

（注）　SPAN の詳細については、『*Catalyst 6500 Series Cisco IOS Command Reference*』を参照してください。

VACL の設定

Cisco IOS ソフトウェアを使用している場合、1 つの VLAN または複数の VLAN から、あるいは 7600 ルータの FLexWAN2 ポートから IPS 用のトラフィックを取り込むように VACL を設定できます。

この項では、次のトピックについて説明します。

- Catalyst ソフトウェア（P.15-14）
- Cisco IOS ソフトウェア（P.15-16）

Catalyst ソフトウェア

（注）　ポート 1 は、TCP リセット ポートとして設定されます。ポート 7 および 8 は、センシング ポートで、セキュリティ ACL キャプチャ ポートとして設定できます。Catalyst Software 8.4(1) 以前のリリースでは、デフォルトで、ポート 7 および 8 はトランク ポートとして設定され、セキュリティ ACL にキャプチャ機能が適用されたすべての VLAN にトランク接続します。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 をクリアして、ポート 7 および 8 にトランク接続されないようにする必要があります。

セキュリティ ACL キャプチャ ポートを設定するには、**set security acl** コマンドを使用します。

次のオプションが適用されます。

- **ACL**：セキュリティ ACL 機能を設定します。
  - **capture-port**：ACL キャプチャ用のポートを設定します。
  - **cram**：セキュリティ ACL クラムを設定します。
  - **ip**：IP セキュリティ ACL 機能を設定します。
  - **ipx**：IPX セキュリティ ACL 機能を設定します。
  - **mac**：MAC セキュリティ ACL 機能を設定します。
  - **map**：セキュリティ ACL を VLAN マッピングに設定します。
- **permit**：転送するパケットを指定します。
- **deny**：拒否するパケットを指定します。
- **redirect**：ポートに転送するパケットを指定します。

- **before**：編集バッファ内の指定された ACE の前に ACE を挿入します。
- **capture**：このフローのコピーをキャプチャ ポートに作成します。
- **modify**：編集バッファ内の指定された ACE を変更します。

VLAN 上の IPS トラフィックを取り込むように VACL を設定するには、次の手順を実行します。

ステップ 1　コンソールにログインします。

ステップ 2　特権モードに入ります。

```
cat6k> enable
```

ステップ 3　トラフィックを取り込むために VACL を作成します。許可、拒否、および取り込むトラフィックを指定します。

```
cat6k> (enable) set security acl ip acl_name permit ip [permit (...) | deny (...)]
capture
```

（注）　許可したトラフィックのみを取り込むことができます。トラフィックを許可するが、取り込まない場合は、**capture** キーワードを使用しないでください。

例

```
console> (enable) set security acl ip CAPTUREALL permit ip any any capture
CAPTUREALL editbuffer modified. Use 'commit' command to apply changes.
```

ステップ 4　VACL を適用します。

```
console> (enable) commit security acl CAPTUREALL
ACL commit in progress.
```

VACL を適用すると、VACL および関連 ACE が NVRAM に書き込まれます。

ステップ 5　VACL を VLAN にマッピングします。

```
console> (enable) set security acl map acl_name vlan_number
```

例

```
console> (enable) set security acl map CAPTUREALL 650
Mapping in progress.

ACL CAPTUREALL successfully mapped to VLAN 650.
```

ステップ 6　IDSM-2 ポート（ポート 7 または 8）をキャプチャ ポートとして設定します。

```
console> (enable) set security acl capture module_number/port_number
```

例

```
console> (enable) set security acl capture 2/13
Successfully set 2/13 to capture ACL traffic.
```

（注）　トランク　ポートおよび ACL の詳細については、『*Catalyst 6500 Series Switch Command Reference*』を参照してください。

Cisco IOS ソフトウェア

VLAN 上の IPS トラフィックを取り込むように VACL を設定するには、次のコマンドを使用します。

次のオプションが適用されます。

- **ip access-list**：名前付きアクセス リスト
  - **extended**：拡張アクセス リスト
  - **hardware**：ハードウェア フラグメント処理のイネーブル化
  - **log-update**：アクセス リスト ログのアップデートの制御
  - **logging**：アクセス リストのロギングの制御
  - **resequence**：アクセス リストの再シーケンス
  - **standard**：標準アクセス リスト

VLAN 上の IPS トラフィックを取り込むように VACL を設定するには、次の手順を実行します。

ステップ 1　コンソールにログインします。

ステップ 2　グローバル コンフィギュレーション モードに入ります。

```
switch# configure terminal
```

ステップ 3　ACL を定義します。

```
switch (config)# ip access-list [standard | extended] acl_name
```

例

```
switch(config)# ip access-list standard CAPTUREALL
switch(config-std-nacl)# exit
```

ステップ 4　VLAN アクセス マップを定義します。

```
switch(config)# vlan access-map map_name [0-65535]
```

ステップ 5　VLAN アクセス マップ シーケンスに match 句を設定します。

```
switch (config-access-map)# match [ip address {1-199 | 1300-2699 | acl_name}]
```

ステップ 6　VLAN アクセス マップ シーケンスに action 句を設定して、先行する match 句に付加します。

```
switch(config-access-map)# action forward capture
```

ステップ 7　VLAN アクセス マップを指定された VLAN に適用します。

```
switch (config)# vlan filter map_name vlan-list vlan_list
```

ステップ 8　取り込まれたフラグ付きトラフィックを取り込むように IDSM-2 データ ポートを設定します。

```
switch (config)# intrusion-detection module module_number data-port data_port_number
capture allowed-vlan capture_vlans
```

（注）　スイッチでトラフィックをルーティングしている場合は、ルーティングされる VLAN すべてを監視するように IDSM-2 を設定します。VACL を FlexWan2 ポートに適用する場合は、すべての VLAN を監視するように IDSM-2 を設定する必要があります。

ステップ 9　IDSM-2 上のキャプチャ機能をイネーブルにします。

```
switch (config)# intrusion-detection module module_number data-port data_port_number
capture
```

次の例は、**show run** コマンドの出力を示します。

```
switch# show run
intrusion-detection module 4 data-port 1 capture allowed-vlan 450,1002-1005
intrusion-detection module 4 data-port 1 capture
.
.
.
vlan access-map CAPTUREALL 10
match ip address MATCHALL
action forward capture
.
.
.
ip access-list extended MATCHALL
permit ip any any
switch#
```

mls ip ids コマンドの設定

この項では、**mls ip ids** コマンドを使用して IPS トラフィックを取り込む方法について説明します。

この項では、次のトピックについて説明します。

Catalyst ソフトウェア

MSFC で Cisco IOS ファイアウォールを動作させている場合は、VACL を使用して IDSM-2 のトラフィックを取り込むことはできません。これは、Cisco IOS ファイアウォールの IP 検査ルールを適用した VLAN には VACL が適用できないからです。しかし、**mls ip ids** コマンドを使用して、取り込むパケットを指定することはできます。ACL によって許可されたパケットが取り込まれます。ACL によって拒否されたパケットは取り込まれません。permit/deny パラメータは、宛先ポートへのパケットの転送に影響を与えません。そのルータ インターフェイスに到着するパケットが IPS ACL に照らしてチェックされ、それらを取り込むかどうかが判断されます。**mls ip ids** コマンドは、スーパーバイザ コンフィギュレーションではなく、MSFC コンフィギュレーションの一部として適用されます。**mls ip ids** コマンドでは、着信トラフィックのみが取り込まれます。**mls ip ids** コマンドは、クライアント側のルータ インターフェイスとサーバ側のルータ インターフェイスの両方で使用する必要があります。これにより、接続の両方向で取り込まれるようになります。

mls ip ids コマンドを使用して IPS トラフィックを取り込むには、次の手順を実行します。

ステップ 1　MSFC にログインします。

ステップ 2　特権モードに入ります。

```
cat6k> enable
```

ステップ 3　コンフィギュレーション モードに入ります。

```
switch# configure terminal
```

ステップ 4　ACL を設定して、取り込むパケットを指定します。

```
switch(config)# ip access-list extended word
```

ステップ 5　取り込んだパケットを伝送するインターフェイスを選択します。

```
switch(config)# interface interface_name
```

ステップ 6　ステップ 4 で作成した ACL を、ステップ 5 で選択したインターフェイスに適用します。

```
switch(config-if)# mls ip ids word
```

ステップ 7　スーパーバイザ エンジンにログインします。

ステップ 8　特権モードに入ります。

```
cat6k> enable
```

ステップ 9　スーパーバイザ エンジンで、IDSM-2 モニタ ポート（ポート 7 または 8）を VACL キャプチャ リストに追加します。

```
cat6k> (enable) set security acl capture module_number/port_number
```

注意　IDSM-2 が、**mls ip ids** コマンドによってマークが付けられたパケットすべてを取り込むには、IDSM-2 のポート 7 または 8 が、パケットのルーティング先の VLAN すべてのメンバーでなければなりません。

Cisco IOS ソフトウェア

ポートを、スイッチ ポートではなく、ルータ インターフェイスとして使用している場合は、VACL を適用する VLAN はありません。

mls ip ids コマンドを使用すると、取り込むパケットを指定することができます。ACL によって許可されたパケットが取り込まれます。ACL によって拒否されたパケットは取り込まれません。permit/deny パラメータは、宛先ポートへのパケットの転送に影響を与えません。そのルータ インターフェイスに到着するパケットが IPS ACL に照らしてチェックされ、それらを取り込むかどうかが判断されます。

mls ip ids コマンドを使用して IDS トラフィックを取り込むには、次の手順を実行します。

ステップ 1　コンソールにログインします。

ステップ 2　グローバル コンフィギュレーション モードに入ります。

```
switch# configure terminal
```

ステップ 3　ACL を設定して、取り込むパケットを指定します。

```
switch(config)# ip access-list extended word
```

ステップ 4　取り込んだパケットを伝送するインターフェイスを選択します。

```
switch(config)# interface interface_name
```

ステップ 5　キャプチャ VLAN を指定します。

```
switch(config)# intrusion-detection module module_number data-port data_port_number
capture allowed-vlan capture_vlans
```

例

```
switch(config)# intrusion-detection module 4 data-port 1 capture allowed-vlan 165
```

ステップ 6　ステップ 4 で作成した ACL を、ステップ 5 で選択したインターフェイスに適用します。

```
switch(config-if)# mls ip ids word
```

注意　IDSM-2 が、**mls ip ids** コマンドによってマークされたすべてのパケットを取り込むには、IDSM-2 のデータ ポート 1 または 2 が、パケットのルーティング先の VLAN すべてのメンバーでなければなりません。

IDSM-2 用の Catalyst 6500 シリーズ スイッチのインライン モードでの設定

IDM または CLI を使用して、2 つの離れた VLAN（IDM-2 の両側それぞれに 1 つの VLAN）の間でインライン モードで動作するように IDSM-2 を設定できます。インライン モード用の IDSM-2 を準備するには、スイッチと IDSM-2 を設定する必要があります。まずスイッチを設定して、その後インライン モード用の IDSM-2 インターフェイスを設定します。混合モードまたはインライン モードで動作するように IDSM-2 を設定するための手順については、第 5 章「インターフェイスの設定」を参照してください。

この項では、次のトピックについて説明します。

Catalyst ソフトウェア

IDSM-2 モニタリング ポートを、Supervisor Engine 1a、Supervisor Engine 2、Supervisor Engine 32、または Supervisor Engine 720 を備えた Catalyst ソフトウェア 8.4(1) 以上に対するインライン動作用のトランク ポートとして設定します。ネイティブ VLAN はトランク接続される唯一の VLAN と同じであるので、トラフィックは 802.1q カプセル化されていません。

注意　IDSM-2 ポート 7 および 8 のデフォルト コンフィギュレーションでは、すべての VLAN 1 ～ 4094 をトランク接続します。IDSM-2 コンフィギュレーションをクリアすると（**clear configuration** *module_number*）、IDSM-2 はすべての VLAN をトランク接続します。IDSM-2 インターフェイスがインライン用に設定されている場合、スパニング ツリー ループが作成されてストームが発生する可能性があります。ストームとは数多くのパケットのループであり、それらのパケットが宛先に到達することはありません。

IDSM-2 上にインライン モード用のモニタリング ポートを設定するには、次の手順を実行します。

ステップ 1　コンソールにログインします。

ステップ 2　特権モードに入ります。

```
cat6k> enable
```

ステップ 3　各 IDSM-2 モニタリング ポートにネイティブ VLAN を設定します。

```
cat6k (enable)> set vlan vlan_number slot_number/port_number
```

例

```
cat6k (enable)> set vlan 651 9/7
cat6k (enable)> set vlan 652 9/8
```

ステップ 4　各 IDSM-2 モニタリング ポートからすべての VLAN をクリアします。ただし、各ポートのネイティブ VLAN（ポート 7 の場合は 651、ポート 8 の場合は 652）は除きます。

```
cat6k (enable)> clear trunk slot_number/port_number vlan_range
```

例

```
cat6k (enable)> clear trunk 9/7 1-650,652-4094
cat6k (enable)> clear trunk 9/8 1-651,653-4094
```

ステップ 5　IDSM-2 モニタリング ポートの Bpdu スパンツリー フィルタリングをイネーブルにします。

```
cat6k (enable)> set spantree bpdu-filter 6/7-8 enable
```

（注）　IPS 5.0(2) の場合は、このステップは省略します。

Cisco IOS ソフトウェア

（注）　Supervisor Engine 720 を備えた Cisco IOS ソフトウェア 12.2(18)SXE は、2 つの VLAN 間では 1 つの IDSM-2 インラインのみをサポートします。

IDSM-2 モニタリング ポートをインライン動作用のアクセス ポートとして設定します。

（注）　Etherchannelling インライン IDSM-2 は、Cisco IOS ではまだサポートされていません。

インライン VLAN を設定するには、次の手順を実行します。

ステップ 1　コンソールにログインします。

ステップ 2　グローバル コンフィギュレーション モードに入ります。

```
switch# configure terminal
```

ステップ 3　インライン IDSM-2 のそれぞれの側に 1 つずつ、2 つの VLAN を作成します。

```
switch(config)# vlan vlan_number
switch(config)# name vlan_name
switch(config)# exit
switch# exit
```

ステップ 4　各インライン VLAN 上の各インターフェイスに IOS アクセス ポートをまだ設定していない場合は、設定します。

a. グローバル コンフィギュレーション モードに入ります。

```
switch# configure terminal
```

b. 設定する IOS インターフェイスを選択します。

```
switch(config)# interface interface_name
```

c. インターフェイスの目的が分かるように説明を入力します。

```
switch(config-if)# description description
```

d. インターフェイスをレイヤ 2 スイッチ ポートとして設定します。

```
switch(config-if)# switchport
```

e. アクセス モード VLAN を設定します。

```
switch(config-if)# switchport access vlan vlan_number
```

f. アクセス ポートとするインターフェイス / ポートを設定します。

```
switch(config-if)# switchport mode access
```

g. グローバル コンフィギュレーション モードを終了します。

```
switch(config-if)# exit
switch# exit
```

ステップ 5　ステップ 3 で作成した 2 つの VLAN それぞれの上に 1 つの IDSM-2 データ ポートを設定します。

```
switch# configure terminal
switch(config)# intrusion-detection module slot_number data-port data_port_number
access-vlan vlan_number
switch(config)# exit
```

ステップ 6　コンフィギュレーションを確認します。

（注）　次の例では、スロット 13 の IDSM-2 は、VLAN 661 および 662 の間でインラインです。IDSM-2 データ ポート 1 は VLAN 661 上にあり、データ ポート 2 は VLAN 662 上にあります。

a. IDSM-2 侵入検出設定を確認します。

```
switch# show run | include intrusion-detection
intrusion-detection module 13 management-port access-vlan 147
intrusion-detection module 13 data-port 1 access-vlan 661
intrusion-detection module 13 data-port 2 access-vlan 662
switch#
```

b. IDSM-2 データ ポート 1 が VLAN 661 上のアクセス ポートであることを確認します。

```
switch# show intrusion-detection module slot_number data-port data_port_number
state
```

例

```
switch# show intrusion-detection module 13 data-port 1 state
Intrusion-detection module 13 data-port 1:

Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q Operational Trunking Encapsulation:
native Negotiation of Trunking: Off Access Mode VLAN: 661 (inline-vlan-1) Trunking
Native Mode VLAN: 1 (default) Trunking VLANs Enabled: NONE Pruning VLANs Enabled:
2-1001 Vlans allowed on trunk:661 Vlans allowed and active in management domain:
661 Vlans in spanning tree forwarding state and not pruned: 661
Administrative Capture Mode: Disabled
Administrative Capture Allowed-vlans: <empty>
```

c. VLAN 番号を確認します。

```
switch# show vlan id vlan_number
```

例

```
switch# show vlan id 661
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------

661  ward-attack3                     active    Gi3/2, Gi13/d1

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
661  enet  100661     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
switch#
```

EtherChanneling の設定

この項では、IDSM-2 に Cisco IOS ソフトウェア用の EtherChanneling を設定する方法について説明します。取り上げる事項は次のとおりです。

概要

Catalyst 6500 シリーズ シャーシのスーパーバイザ エンジンは、IPS 5.0 を EtherChannel デバイスとして実行している IDSM-2 デバイスを認識します。これによって、最大 8 個の IDSM-2 デバイスを同一シャーシに取り付けることができます。

Catalyst 6500 シリーズ スイッチの IDSM-2 には、8 個の内部ポートがあります。これらのポートのうち、4 個のみが使用されます。ポート 1 は、TCP/IP リセット ポートです。ポート 2 は、コマンド / コントロール ポートです。ポート 7 および 8 は Catalyst ソフトウェア用のセンシング ポートで、データ ポート 1 および 2 は Cisco IOS ソフトウェア用です。その他のポートは使用されません。

バックプレーンは 1000 Mbps です。これが、IDSM-2 は約 600 Mbps のパフォーマンスしか処理できない場合でも、IDSM-2 が 1000 Mbps を示す理由です。EtherChannel 機能により、最大 8 台の IDSM-2 デバイスが、ポート 7 または 8 のいずれかのロード バランシングに参加できるようになります。

（注）　IDSM-2 の EtherChannel ロード バランシングは、Cisco IOS ソフトウェアでのみサポートされています。Cisco Catalyst ソフトウェア用の EtherChannel ロード バランシングを IDSM-2 に設定するための手順については、これをサポートする Catalyst リリースが使用可能になるときに提供されます。

EtherChanneling のイネーブル化

（注）　EtherChannel ロード バランシングを IDSM-2 に設定するには、Cisco IOS 12.2(18)SXE をインストールし、Supervisor Engine 720 を装備する必要があります。Cisco IOS は、VACL キャプチャ（SPAN でも監視でもない）を使用する混合 DSM-2 EtherChanneling のみをサポートします。

EtherChannel は、フレーム内のアドレスから形成されるバイナリ パターンの部分を、チャネル内のリンクの 1 つを選択する数値に縮小して、EtherChannel 内のリンクを越えてトラフィック ロードをバランスさせます。

EtherChannel ロード バランシングでは、MAC アドレス、IP アドレス、またはレイヤ 4 ポート番号が使用できます。アドレスまたはポートは、送信元または宛先のアドレスまたはポートでも、送信元および宛先の両方のアドレスまたはポートでもかまいません。選択されたモードがスイッチに設定されている EtherChannel すべてに適用されます。EtherChannel ロード バランシングでは、MPLS レイヤ 2 情報も使用できます。

使用しているコンフィギュレーションにおいて非常に多様なバランス基準を与えるオプションが使用できます。たとえば、EtherChannel 上のトラフィックが 1 つの MAC アドレスだけに送信され、その宛先 MAC アドレスを EtherChannel ロード バランシングの基準とする場合、EtherChannel は常にその EtherChannel 内の同じリンクを選択します。送信元アドレスまたは IP アドレスを使用すると、ロード バランシングが向上する場合があります。

EtherChanneling の詳細については、『*Catalyst 6500 Series Cisco IOS Software Configuration Guide, 12.2SX*』を参照してください。

EtherChannel ロード バランシングを IDSM-2 に設定するには、次の手順を実行します。

ステップ 1　混合動作用に各 IDSM-2 を設定します。

手順については、第 5 章「インターフェイスの設定」を参照してください。

（注）　IDSM-2 EtherChanneling を設定する前に、IDSM-2 VACL キャプチャ、あるいは SPAN またはモニタ コンフィギュレーションの行がすべて、削除されていることを確認します。

ステップ 2　コンソールにログインします。

ステップ 3　グローバル コンフィギュレーション モードに入ります。

```
switch# configure terminal
```

ステップ 4　VACL を作成します。

```
switch(config)# ip access-list extended vacl_name
```

ステップ 5　任意のアクセス コントロール エントリ（たとえば、`permit any any`）を追加します。

```
switch(config-ext-nacl)# permit ip any any
```

ステップ 6　少なくとも 1 つの VLAN アクセス マップ シーケンスを作成します。

```
switch(config-ext-nacl)# vlan access-map vlan_access_map_name sequence_number
switch(config-access-map)# match ip address vacl_name
switch(config-access-map)# action forward capture
```

ステップ 7　VLAN アクセス マップを VLAN に適用します。

```
switch(config-access-map)# vlan filter vlan_access_map_name vlan-list vlan_list
```

ステップ 8　各 IDSM-2 に対して、目的のデータ ポートを目的の EtherChannel に追加します。

```
switch(config)# intrusion-detection module module_number data-port data_port_number
channel-group channel_number
```

各 EtherChannel には、番号付きのポート チャネル インターフェイスがあります。最大 64 個のポート チャネル インターフェイス（1 ～ 256 の番号を付けて）を設定できます。

ステップ 9　EtherChannel ロード バランシングを設定します。

```
switch(config)# port-channel load-balance [dst-ip | dst-mac | dst-port | mpls |
src-dst-ip | src-dst-mac | src-dst-port | src-ip | src-mac | src-port]
```

次のオプションが適用されます。

- **dst-ip**：宛先 IP アドレス
- **dst-mac**：宛先 MAC アドレス
- **dst-port**：宛先 TCP/UDP ポート
- **mpls**：MPLS パケットのロード バランシング
- **src-dst-ip**：送信元および宛先 IP アドレス
- **src-dst-mac**：送信元および宛先 MAC アドレス
- **src-dst-port**：送信元および宛先 TCP/UDP ポート
- **src-ip**：送信元 IP アドレス
- **src-mac**：送信元 MAC アドレス
- **src-port**：送信元 TCP/UDP ポート

  デフォルトは **src-dst-ip** です。これは、EtherChannel が、配布方法として、送信元と宛先の IP アドレスの組み合せを使用することを意味します。

ステップ 10　ロード バランシングを確認します。

```
cat6k# show etherchannel load-balance
EtherChannel Load-Balancing Configuration:
        src-dst-ip

EtherChannel Load-Balancing Addresses Used Per-Protocol:
Non-IP: Source XOR Destination MAC address
  IPv4: Source XOR Destination IP address
  IPv6: Source XOR Destination IP address
  MPLS: Label or IP
```

ステップ 11　取り込む VLAN を EtherChannel に設定します。

```
switch(config)# intrusion-detection port-channel channel_number capture allowed-vlan
vlan_list
```

ステップ 12　EtherChannel に対してキャプチャをイネーブルにします。

```
switch(config)# intrusion-detection port-channel channel_number capture
```

ステップ 13　グローバル コンフィギュレーション モードを終了します。

```
switch(config)# exit
```

ステップ 14 変更内容を保存するには、次のように入力します。

```
switch# write memory
```

EtherChanneling のディセーブル化

IDSM-2 EtherChanneling をディセーブルにするには、次の手順を実行します。

ステップ 1　コンソールにログインします。

ステップ 2　グローバル コンフィギュレーション モードに入ります。

```
switch# configure terminal
```

ステップ 3　EtherChannel から 1 つの IDSM-2 を削除するには、次のように入力します。

```
switch(config)# no intrusion-detection module module_number data-port
data_port_number channel-group channel_number
```

ステップ 4　EtherChannel 全体を削除するには、次のように入力します。

（注）　IDSM-2 用の VACL キャプチャ コマンドは残ります。

```
switch(config)# no intrusion-detection module port-channel channel_number
```

EtherChanneling の確認

IDSM-2 EtherChannel コンフィギュレーションを確認するには、次の手順を実行します。

ステップ 1　コンソールにログインします。

ステップ 2　すべての EtherChannel を表示するには、次のように入力します。

```
switch# show etherchannel
                Channel-group listing:
                ----------------------

Group: 10
----------
Group state = L2
Ports: 0   Maxports = 8
Port-channels: 1 Max Port-channels = 1
Protocol:    -

cat6k#
```

ステップ 3　特定の EtherChannel のステータスを表示するには、次のように入力します。

```
switch# show etherchannel 1 [summary | detail | port | port-channel | protocol]
```

例

```
switch# show etherchannel 1 summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        u - unsuitable for bundling
Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+----------------------------

switch#
```

ステップ 4　EtherChannel ロード バランスの設定を表示するには、次のように入力します。

```
switch# show etherchannel load-balance
EtherChannel Load-Balancing Configuration:
        src-dst-ip
        mpls label-ip

EtherChannel Load-Balancing Addresses Used Per-Protocol:
Non-IP: Source XOR Destination MAC address
  IPv4: Source XOR Destination IP address
  IPv6: Source XOR Destination IP address
  MPLS: Label or IP
switch#
```

ステップ 5　IDSM-2 データ ポート情報を表示するには、次のように入力します。

```
switch# show intrusion-detection module module_number data-port data_port_number state
Intrusion-detection module 11 data-port 2:

Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 662 (ward-victim3)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: NONE
Pruning VLANs Enabled: 2-1001
Vlans allowed on trunk:none
Vlans allowed and active in management domain: none
Vlans in spanning tree forwarding state and not pruned:
   none
Administrative Capture Mode: Disabled
Administrative Capture Allowed-vlans: empty
```

IDSM-2 の管理タスク

この項では、IDSM-2 の管理タスクに役立つ手順について説明します。取り上げる事項は次のとおりです。

全メモリ テストのイネーブル化

IDSM-2 を最初にブートするときに、デフォルトでは部分的なメモリ テストが実行されます。Catalyst ソフトウェアおよび Cisco IOS ソフトウェアで全メモリ テストをイネーブルにできます。

この項では、次のトピックについて説明します。

Catalyst ソフトウェア

全メモリ テストをイネーブルにするには、**set boot device** *boot_sequence module_number* **mem-test-full** コマンドを使用します。全メモリ テストには約 12 分かかります。

全メモリ テスト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　コンソールにログインします。

ステップ 2　特権モードに入ります。

```
cat6k> enable
```

ステップ 3　全メモリ テストをイネーブルにします。

```
cat6k> (enable) set boot dev cf:1 3 mem-test-full
Device BOOT variable = cf:1
Memory-test set to FULL
Warning: Device list is not verified but still set in the boot string.
console> (enable) set boot dev hdd:1 3 mem-test-full
Device BOOT variable = hdd:1
Memory-test set to FULL
Warning: Device list is not verified but still set in the boot string.
cat6k> (enable)
```

set boot device コマンドには、**cf:1** または **hdd:1** を指定できます。

ステップ 4　IDSM-2 をリセットします。

手順については、P.15-31 の「IDSM-2 のリセット」を参照してください。

全メモリ テストを実行します。

（注）　全メモリ テストは、部分的なメモリ テストよりも完了に時間がかかります。

Cisco IOS ソフトウェア

全メモリ テストをイネーブルにするには、**hw-module module** *module_number* **reset mem-test-full** コマンドを使用します。全メモリ テストには約 12 分かかります。

全メモリ テスト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　コンソールにログインします。

ステップ 2　全メモリ テストをイネーブルにします。

```
switch# hw-module module 9 reset mem-test-full
    Device BOOT variable for reset = <empty>
    Warning: Device list is not verified.

    Proceed with reload of module?[confirm]
    % reset issued for module 9
switch#
```

ステップ 3　IDSM-2 をリセットします。

手順については、P.15-31 の「IDSM-2 のリセット」を参照してください。

全メモリ テストを実行します。

（注）　全メモリ テストは、部分的なメモリ テストよりも完了に時間がかかります。

IDSM-2 のリセット

何らかの理由で、SSH、Telnet、またはスイッチの **session** コマンドを使用して IDSM-2 と通信できない場合は、スイッチ コンソールから IDSM-2 をリセットする必要があります。リセット処理には数分かかります。

この項では、次のトピックについて説明します。

Catalyst ソフトウェア

CLI から IDSM-2 をリセットするには、次の手順を実行します。

ステップ 1　コンソールにログインします。

ステップ 2　特権モードに入ります。

```
cat6k> enable
```

ステップ 3　アプリケーション パーティションまたはメンテナンス パーティションに IDSM-2 をリセットします。

```
cat6k> (enable) reset module_number [hdd:1 | cf:1]
```

（注）　アプリケーション パーティション（hdd:1 デフォルト）もメンテナンス パーティション（cf:1）も指定しないと、IDSM-2 はブート デバイス変数を使用します。

次の例は、**reset** コマンドの出力を示します。

```
cat6k> (enable) reset 3
2003 Feb 01 00:18:23 %SYS-5-MOD_RESET: Module 3 reset from console//
Resetting module 3... This may take several minutes.
2003 Feb 01 00:20:03 %SYS-5-MOD_OK: Module 3 is online.
cat6k> (enable)
```

注意　IDSM-2 を先にシャットダウンしないでスイッチ シャーシから取り外した場合、またはシャーシの電源が切れた場合は、IDSM-2 のリセットを複数回行うことが必要な場合があります。リセット操作を 3 回繰り返しても IDSM-2 が反応しない場合は、メンテナンス パーティションをブートし、アプリケーション パーティションの復元手順を実行してください。手順については、P.17-31 の「IDSM-2 システム イメージのインストール」を参照してください。

Cisco IOS ソフトウェア

（注）　リセット処理には数分かかります。

CLI から IDSM-2 をリセットするには、次の手順を実行します。

ステップ 1　コンソールにログインします。

ステップ 2　IDSM-2 をリセットします。

```
switch# hw-module module module_number reset [hdd:1 | cf:1]
```

（注）　アプリケーション パーティション（hdd:1 デフォルト）もメンテナンス パーティション（cf:1）も指定しないと、IDSM-2 はブート デバイス変数を使用します。

次の例は、**reset** コマンドの出力を示します。

```
switch# hw-module module 8 reset
Device BOOT variable for reset =
Warning: Device list is not verified.
Proceed with reload of module? [confirm]
% reset issued for module 8
switch#
```

Catalyst および Cisco IOS ソフトウェアのコマンド

この項では、IDSM-2 に関係する Catalyst ソフトウェアおよび Cisco IOS ソフトウェアのコマンドを示します。

（注）　Catalyst および Cisco IOS ソフトウェア コマンドの詳細については、Cisco.com にあるコマンド リファレンスを参照してください。これらの文書の検索方法については、IDSM-2 に付属する『*Documentation Roadmap for Cisco Intrusion Prevention System 5.1*』を参照してください。

この項では、次のトピックについて説明します。

Catalyst ソフトウェア

この項では、サポートされている Catalyst ソフトウェア コマンドとサポートされていない Catalyst ソフトウェア コマンドを示します。取り上げる事項は次のとおりです。

サポートされているスーパーバイザ エンジン コマンド

IDSM-2 は、次のスーパーバイザ エンジン CLI コマンドもサポートしています。このコマンドの詳細は、Catalyst 6500 シリーズのコマンド リファレンスに記載されています。

- **clear config** *module_number*

  指定された IDSM-2 に関連付けられたスーパーバイザ エンジンのコンフィギュレーションをクリアします。
- **clear log** *module_number*

  指定された IDSM-2 に関するエラー ログのエントリをすべて削除します。
- **session** *slot_number*

  スイッチ コンソールから IDSM-2 のコンソールにログインします。
- **set module** コマンド（他のすべての **set module** コマンドはエラー メッセージを返します）。
  - **set module name** *module_number*

    モジュールの名前を設定します。
  - **set module power** *module_number* [**up** | **down**]

    指定された IDSM-2 の電源をイネーブルまたはディセーブルにします。

- **set port name** *module_number*

  指定された IDSM-2 ポートの名前を設定します。
- **set span**

  ポート 1 を SPAN 宛先ポートとして設定します。IDSM-2 上のポート 1 は、SPAN 発信元ポートとして使用できません。
- **set trunk**

  トランク ポートを設定します。
- **set vlan**

  VLAN キャプチャ ポートを設定します。
- **show config**

  スーパーバイザ エンジン NVRAM コンフィギュレーションを表示します。
- **show log**

  指定された IDSM-2 のエラー ログを表示します。
- **show mac** *module_number*

  指定された IDSM-2 の MAC カウンタを表示します。
- **show module** *module_number*

  IDSM-2 が取り付けられている場合は、Module-Type に「Intrusion Detection System Module」が表示されます。
- **show port** *module_number*

  指定された IDSM-2 のポート ステータスを表示します。
- **show port capabilities** [*module* | *module_number*]

  モジュールおよびポートの機能を表示します。
- **show test**

  SPAN ポート（ポート 1）および管理ポート（ポート 2）の両方の診断テストから報告されたエラーと、BIOS および CMOS のブート結果を表示します。

サポートされていないスーパーバイザ エンジン コマンド

次のスーパーバイザ エンジン CLI コマンドは、IDSM-2 ではサポートされていません。

- **set module** [**enable** | **disable**] *module_number*
- **set port broadcast**
- **set port channel**
- **set port cops**
- **set port disable**
- **set port enable**
- **set port flowcontrol**
- **set port gmrp**
- **set port gvrp**
- **set port host**
- **set port inlinepower**
- **set port jumbo**
- **set port membership**
- **set port negotiation**
- **set port protocol**

- **set port qos**
- **set port rsvp**
- **set port security**
- **set port speed**
- **set port trap**
- **set protocolfilter**
- **set rgmp**
- **set snmp**
- **set spantree**
- **set udld**
- **set vtp**

Cisco IOS ソフトウェア

この項では、IDSM-2 がサポートしている Cisco IOS ソフトウェア コマンドを示します。これらのコマンドは、モードに従ってグループ化されています。

この項では、次のトピックについて説明します。

- EXEC コマンド（P.15-35）
- コンフィギュレーション コマンド（P.15-36）

EXEC コマンド

次のコマンドはすべて、EXEC モードで実行されます。

- **clock read-calendar**

  クロック時刻をカレンダ時刻にアップデートします。
- **clock set** *time date*

  現在の時刻と日付を設定します。
- **clock update-calendar**

  カレンダ時刻をクロック時刻にアップデートします。
- **hw-module module** *slot_number* **reset**

  IDSM-2 を、ブート デバイス変数で指定されたパーティションにリセットします。ブート デバイス変数が設定されていなかった場合、IDSM-2 はデフォルトでアプリケーション パーティションにリセットされます。ブート デバイス変数の現在の設定を表示するには、**show boot device module** *module_number* コマンドを使用します。
- **hw-module module** *slot_number* **reset cf:1**

  モジュールをメンテナンス パーティションにリセットします。
- **hw-module module** *slot_number* **shutdown**

  モジュールをシャットダウンして、シャーシから安全に取り外しできるようにします。
- **reload**

  スイッチ全体をリロードします。
- **session slot** *slot_number* **processor** *processor_number*

  スイッチ コンソールから IDSM-2 のコンソールにログインします。
- **show intrusion-detection module** *module_number* **data-port** *data_port_number* **state**

  指定された IDSM-2 データ ポートの状態を表示します。

- **show intrusion-detection module** *module_number* **data-port** *data_port_number* **traffic**

  IDSM-2 データ ポート トラフィックのトラフィック統計情報を表示します。
- **show intrusion-detection module** *module_number* **management-port state**

  IDSM-2 管理ポートの状態を表示します。
- **show intrusion-detection module** *module_number* **management-port traffic**

  IDSM-2 管理ポートのトラフィック統計情報を表示します。
- **show ip access-lists**

  現在のアクセス リストを表示します。
- **show module**

  取り付けられているモジュール、バージョン、および状態を表示します。
- **show running-config**

  現在動作しているコンフィギュレーションを表示します。
- **show startup-config**

  保存されているコンフィギュレーションを表示します。
- **show vlan access-map**

  現在の VLAN アクセス マップをすべて表示します。

コンフィギュレーション コマンド

次のコンフィギュレーション コマンドはすべて、グローバル コンフィギュレーション モード、インターフェイス コンフィギュレーション モード、または VACL コンフィギュレーション サブモードのいずれかで実行されます。

- グローバル コンフィギュレーション モード
  - **clock calendar valid**

    現在のカレンダ時刻をブートのスイッチ時刻として設定します。
  - **clock summer-time** *zone* **recurring**

    サマータイム設定を使用するようにスイッチを設定します。
  - **clock timezone** *zone offset*

    スイッチ /IDSM-2 の時間帯を設定します。
  - **intrusion-detection module** *module_number* **management-port access-vlan** *access_vlan_number*

    IDSM-2 コマンド / コントロール ポートのアクセス VLAN を設定します。
  - **intrusion-detection module** *module_number* **data-port** *data_port_number* **capture allowed-vlan** *allowed_capture_vlan(s)*

    VACL キャプチャ用の VLAN を設定します。
  - **intrusion-detection module** *module_number* **data-port** *data_port_number* **capture**

    指定された IDSM-2 データ ポートの VACL キャプチャをイネーブルにします。
  - **ip access-list extended** *word*

    VACL マップで使用するアクセス リストを作成します。
  - **monitor session** *session* {**destination** {**interface** *interface interface-number*} [, | -] {**vlan** *vlan-id*}}

    SPAN セッションの宛先を設定します。
  - **monitor session** *session* {**source** {**interface** *interface interface-number*} | {**vlan** *vlan-id*}} [, | - | **rx** | **tx** | **both**]

    SPAN セッションの送信元を設定します。
  - **no power enable module** *slot_number*

    IDSM-2 をシャットダウンして、電源を切ります。

- **power enable module** *slot_number*

  IDSM-2 の電源がまだオンでない場合は、オンにします。
- **vlan access-map** *map_name_sequence*

  VACL マップを作成します。
- **vlan filter** *map_name* **vlan-list** *vlans*

  VACL マップを VLAN にマッピングします。

- インターフェイス コンフィギュレーション モード
  - **switchport**

    インターフェイスをスイッチ ポートとして設定します。
  - **switchport access vlan** *vlan*

    インターフェイスのアクセス VLAN を設定します。
  - **switchport capture**

    インターフェイスをキャプチャ ポートとして設定します。
  - **switchport mode access**

    インターフェイスをアクセス ポートとして設定します。
  - **switchport mode trunk**

    インターフェイスをトランク ポートとして設定します。
  - **switchport trunk allowed vlan** *vlans*

    トランク用の許可された VLAN を設定します。
  - **switchport trunk encapsulation dot1q**

    dot1q をカプセル化タイプとして設定します。
  - **switchport trunk native vlan** *vlan*

    トランク ポート用のネイティブ VLAN を設定します。
- VACL コンフィギュレーション サブモード
  - **action forward capture**

    一致したパケットを取り込むことを指定します。
  - **match ip address** [*1-199* | *1300-2699* | *acl_name*]

    VACL でのフィルタリングを指定します。