CHAPTER 20

IDSM2 の設定

（注） すべての IPS プラットフォームで、許可される同時 CLI セッション数は 10 です。

この章では、IDSM2 の設定に固有の手順について説明します。ネットワークからトラフィックを受信するように IDSM2 を設定すると、侵入防御の設定ができるようになります。この章は、次の内容で構成されています。

（注） Catalyst 6500 シリーズ スイッチは、6500 シリーズ スイッチと 7600 シリーズ ルータの総称として使用しています。

IDSM2 設定手順

IDSM2 を設定するには、次のタスクを実行します。

1. Catalyst 6500 シリーズ スイッチで、IDSM2 へのコマンド/コントロール アクセスを設定します。
2. IDSM2 にログインします。
3. モニタするトラフィックが IDSM2 に送信されるようにスイッチを設定します。

4. IDSM2 を初期化します。

   setup コマンドを実行して IDSM2 を初期化します。設定時に、IDSM2 のインターフェイスを設定できます。

5. サービス アカウントを作成します。
6. ユーザの追加、信頼されるホストの追加など、その他の初期タスクを実行します。
7. 侵入防御を設定します。
8. グローバル相関を設定します。
9. IDSM2 をスムーズに実行し続けるためのその他のタスクを実行します。
10. 新しいシグニチャ アップデートおよびサービス パックで IPS ソフトウェアをアップグレードします。
11. 必要に応じて、アプリケーション パーティションのイメージおよびメンテナンス パーティションのイメージを再作成します。

詳細情報

- IDSM2 にセッション接続する手順については、「IDSM2 へのログイン」（P.2-7）を参照してください。
- IDSM2 を初期化する手順については、「IDSM2 の高度な設定」（P.3-20）を参照してください。
- IDSM2 へのコマンド/コントロール アクセスを設定する手順については、「Catalyst 6500 シリーズ スイッチにおける IDSM2 へのコマンド/コントロール アクセスの設定」（P.20-5）を参照してください。
- インターフェイス設定の変更が必要な場合は、第 6 章「インターフェイスの設定」を参照してください。
- サービス アカウントを作成する手順については、「サービス アカウントの作成」（P.4-22）を参照してください。
- センサーを設定する手順については、第 4 章「センサーのセットアップ」を参照してください。
- 侵入防御を設定する手順については、第 7 章「イベント アクション規則の設定」、第 8 章「シグニチャの定義」、第 9 章「異常検出の設定」、および第 14 章「Attack Response Controller でのブロッキングとレート制限の設定」を参照してください。
- グローバル相関を設定する手順については、第 10 章「グローバル相関の設定」を参照してください。
- IDSM2 の管理タスクを実行する手順については、第 17 章「センサーの管理タスク」および「IDSM2 の管理タスク」（P.20-40）を参照してください。
- 最新版の IPS ソフトウェアを入手する方法については、第 22 章「ソフトウェアの入手」を参照してください。
- アプリケーションおよびメンテナンス パーティションのイメージを再作成する手順については、「IDSM2 システム イメージのインストール」（P.23-29）を参照してください。

IDSM2 取り付けの確認

（注）　IDSM2 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。IDSM2 の診断ルーチンが完了し、オンラインになると、ステータスは `ok` を示します。IDSM2 がオンラインになるまで、最大 5 分かかります。

show module コマンドを使用して、スイッチが IDSM2 を認識し、オンラインになっ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　IDSM2 がオンラインであることを確認します。

- Catalyst ソフトウェア

```
console> (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
console> (enable)
```

- Cisco IOS ソフトウェア

```
router# 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-IDSM2      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
router#
```

詳細情報

IDSM2 の取り付けを確認した後、全メモリ テストをイネーブルにする手順については、「全メモリ テストのイネーブル化」（P.20-40）を参照してください。

サポートされている IDSM2 の最小構成

（注）　次の表は、特定のバージョンを推奨するものではなく、サポートされる最小バージョンを示すものです。

表 20-1 に、サポートされている IDSM2 の最小構成を示します。

表 20-1　IDSM2 機能をサポートする Catalyst 6500 ソフトウェアの最小バージョン

Catalyst/IDSM2 機能	Catalyst ソフトウェア				Cisco IOS ソフトウェア			
	Sup1	Sup2	Sup32	Sup720	Sup1	Sup2	Sup32	Sup720
SPAN	7.5(1)	7.5(1)	8.4(1)	8.1(1)	12.1(19)E1	12.1(19)E1 12.2(18)SXF1	12.2(18)SXF1	12.2(14)SX1
VACL キャプチャ[1]	7.5(1)	7.5(1)	8.4(1)	8.1(1)	12.1(19)E1	12.1(19)E1 12.2(18)SXF1	12.2(18)SXF1	12.2(14)SX1

表 20-1　IDSM2 機能をサポートする Catalyst 6500 ソフトウェアの最小バージョン（続き）

Catalyst/IDSM2 機能	Catalyst ソフトウェア				Cisco IOS ソフトウェア			
VACL キャプチャによる ECLB[2]	8.5(1)	8.5(1)	8.5(1)	8.5(1)	該当なし	12.2(18)SXF4	12.2(18)SXF1	12.2(18)SXE1
インライン インターフェイス ペア	8.4(1)	8.4(1)	8.4(1)	8.4(1)	該当なし	12.2(18)SXF4	12.2(18)SXF4	12.2(18)SXE1
インライン インターフェイス ペアによる ECLB	8.5(1)	8.5(1)	8.5(1)	8.5(1)	該当なし	12.2(18)SXF4	12.2(18)SXF4	12.2(18)SXF4
インライン VLAN ペア	8.4(1)	8.4(1)	8.4(1)	8.4(1)	該当なし	12.2(18)SXF4	12.2(18)SXF4	12.2(18)SXF4
インライン VLAN ペアによる ECLB	8.5(1)	8.5(1)	8.5(1)	8.5(1)	該当なし	12.2(18)SXF4	12.2(18)SXF4	12.2(18)SXF4

1. PFC2/3 または MSFC2/3 が必要です。
2. PFC2/3 または MSFC2/3 が必要です。

Catalyst 6500 シリーズ スイッチにおける IDSM2 へのコマンド/コントロール アクセスの設定

Catalyst 6500 シリーズ スイッチが IDSM2 にコマンド/コントロール アクセスできるように設定する必要があります。ここでは、IDSM2 へのコマンド/コントロール アクセスの設定方法について説明します。内容は次のとおりです。

Catalyst ソフトウェア

Catalyst 6500 シリーズ スイッチが IDSM2 にコマンド/コントロール アクセスできるようにするには、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　特権モードを開始します。

```
console> enable
```

ステップ 3　適切な VLAN にコマンド/コントロール ポートを設定します。

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

例

```
console> (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　IDSM2 にセッション接続して、ネットワーク IP アドレスに ping を送信します。

```
console> session slot_number
IDSM2# 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.
IDSM2# 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
IDSM2# exit
console> (enable)
```

ステップ 5　IDSM2 を初期化します。

ステップ 6　IDSM2 のデフォルト ルータに ping を送信します。

ステップ 7　管理ステーションから IDSM2 に対して ping 送信、SSH または Telnet 接続、および Web ブラウズができることを確認します。

詳細情報

setup コマンドを使用して IDSM2 を初期化する手順については、「IDSM2 の高度な設定」（P.3-20）を参照してください。

Cisco IOS ソフトウェア

Catalyst 6500 シリーズ スイッチが IDSM2 にコマンド/コントロール アクセスできるようにするには、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 モードを開始します。

```
router# configure terminal
```

ステップ 3　適切な VLAN にコマンド/コントロール ポートを設定します。

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

例

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

ステップ 4　IDSM2 にセッション接続し、ネットワーク IP アドレスに ping を送信して、接続されていることを確認します。

```
router# session slot module_number processor 1
IDSM2# ping network_ip_address
```

例

```
router# 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.
IDSM2# 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
IDSM2# exit
```

```
[Connection to 127.0.0.91 closed by foreign host]
router#
```

ステップ 5　IDSM2 を初期化します。

詳細情報

setup コマンドを使用して IDSM2 を初期化する手順については、「IDSM2 の高度な設定」（P.3-20）を参照してください。

IDSM2 の検知モード

IDSM2 では、次の 3 つの検知モードがサポートされます。

- 無差別モード：IDSM2 が導入されたとき、IDSM2 でサポートされる唯一の検知モードが無差別モードでした。両方のデータ ポートのデフォルト検知モードです。

  無差別モードでは、IDSM2 は Catalyst スイッチがデータ ポートにコピーしたネットワーク トラフィックをパッシブにモニタします。データ ポートは 802.1q トランクとして動作し、2 つのデータ ポートが同じ VLAN または異なる VLAN をトランク接続するように設定できます。Catalyst スイッチは、SPAN または VACL キャプチャを使用して、特定のトラフィックをデータ ポートにコピーします。2 つのデータ ポートに、同じトラフィックまたは異なるトラフィックを送信できます。このモードでは IDSM2 がパッシブとなるため、パケットをドロップしてネットワーク侵入をブロックすることはできませんが、TCP リセットをネットワーク接続の両側に送信して接続の切断を試行するように設定できます。

  （注）　Catalyst スイッチはキャプチャ宛先ポートからのトラフィックを転送しないため、IDSM2 はデータ ポート経由で TCP リセットを送信して侵入のブロックを試行することができません。そのため、無差別モードでのみ使用できる別のリセット ポートが、この目的で予約されています。

- インライン モード：IPS 5.0(1) 以降では、IDSM2 をインライン インターフェイス ペア モードで、アクティブ ネットワーク デバイスとして設定できます。2 つのデータ ポートが協調して動作し、IDSM2 を通じて 2 つの VLAN がブリッジされます。各データ ポートをアクセス ポートとして設定し、それぞれに異なる VLAN を割り当てることができます。IDSM2 は、2 つのデータ ポート間でトラフィックを転送することによって、2 つの VLAN をブリッジします。各データ ポート上で受信するトラフィックを検査し、そのパケットをペアのもう一方のデータ ポートに転送するか、または侵入の試行が検出された場合はそのパケットをドロップできます。スイッチをインライン モードに設定してから、IDSM2 でインライン インターフェイス ペアを作成する必要があります。
- インライン VLAN ペア モード：IPS 5.1(1) 以降では、IDSM2 をインライン VLAN ペア モードに設定できます。IDSM2 は 802.1q トランクとして動作し、同じデータ ポート内にある VLAN ペア間で VLAN ブリッジングを実行します。IDSM2 は、VLAN ペアの各 VLAN 上で受信するトラフィックを検査し、そのパケットをペアのもう一方の VLAN（または、パケットを受信したデータ ポートと同じデータ ポートの VLAN）に転送するか、または侵入の試行が検出された場合はそのパケットをドロップできます。IDSM2 は、各データ ポート上で最大 255 個の VLAN ペアを同時にブリッジするように設定できます。IDSM2 は、各パケットの 802.1q ヘッダー内の VLAN ID フィールドを、パケットを転送する VLAN の ID に置き換えます。インライン VLAN ペアに割り当てられていない VLAN で受信したパケットはすべてドロップされます。

（注）　インライン VLAN ペアに関連付けられている VLAN も、データ ポート トランクが許可された VLAN になるように、IPS とスイッチの設定を調整する必要があります。

IDSM2 の検知モードは混在できます。たとえば、一方のデータ ポートを無差別モードに設定し、もう一方のデータ ポートをインライン VLAN ペア モードに設定できます。ただし、IDSM2 のデータ ポートは 2 つだけで、インライン モードでは両方のデータ ポートをペアとして使用する必要があるため、インライン モードを他の 2 つのモードのいずれかと混在させることはできません。

詳細情報

- 無差別モードの詳細については、「無差別モードの設定」（P.6-17）を参照してください。
- TCP リセットの詳細については、「TCP リセット インターフェイス」（P.6-4）を参照してください。
- SPAN を設定する手順については、「SPAN の設定」（P.20-10）を参照してください。
- VACL キャプチャを設定する手順については、「VACL キャプチャの設定」（P.20-14）を参照してください。
- インライン インターフェイス モードの詳細については、「インライン インターフェイス モードの設定」（P.6-19）を参照してください。
- インライン インターフェイス モードでのスイッチ設定の詳細については、「インライン モードの IDSM2 用の Catalyst 6500 シリーズ スイッチの設定」（P.20-20）を参照してください。
- インライン インターフェイス モードでの IDSM2 設定の詳細については、「インライン インターフェイス ペアの設定」（P.6-20）を参照してください。
- インライン VLAN ペア モードの詳細については、「インライン VLAN ペア モードの設定」（P.6-24）を参照してください。
- インライン VLAN ペア モード用にスイッチを設定する手順については、「インライン VLAN ペア モードの IDSM2 用の Catalyst 6500 シリーズ スイッチの設定」（P.20-23）を参照してください。
- インライン VLAN ペア モードで IDSM2 を設定する手順については、「インライン VLAN ペアの設定」（P.6-24）を参照してください。

無差別モードの IDSM2 用の Catalyst 6500 シリーズ スイッチの設定

ここでは、スイッチおよび IDSM2 を無差別モード用に設定する方法について説明します。内容は次のとおりです。

無差別モードのスイッチおよび IDSM2 について

トラフィックは、無差別分析のために IDSM2 上で SPAN または VACL キャプチャを使用してキャプチャされます（Cisco IOS Firewall を MSFC で実行している場合、VACL は使用できませんが、**mls ip ids** コマンドを使用できます）。ポート 1（GigabitEthernet0/1）は TCP リセット ポートとして使用され、ポート 2（GigabitEthernet0/2）はコマンド/コントロール ポート、ポート 7 および 8（GigabitEthernet0/7 および GigabitEthernet0/8）はモニタリング ポートになります。どちらのモニタリング ポートも、SPAN の宛先ポートまたは VACL キャプチャ ポートとして設定できます。

注意　両方のポートをモニタリング ポートとして設定する場合は、異なるトラフィックをモニタするように設定する必要があります。

注意　IDSM2 データ ポートを SPAN の宛先ポートと 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。このように設定すると、IDSM2 がトラフィックを受信しなくなります。このデュアル設定（SPAN と VACL）を行うと、スイッチで問題が発生し、トラフィックが正しく送信されなくなります。

（注）　Catalyst ソフトウェア 8.4(3) よりも前は、IDSM2 データ ポートがデフォルトですべての VLAN をトランキングしていました。Catalyst ソフトウェア 8.4(3) 以降では、IDSM2 データ ポートはデフォルトで VLAN をトランキングしないように設定されます。特に 8.4(3) よりも前のバージョンから 8.4(3) 以降にアップグレードしたときは、IDSM2 ポートが正しい VLAN をトランキングすることを確認してください。

TCP リセット インターフェイスの使用方法

IDSM2 には、TCP リセット インターフェイス（ポート 1）があります。IDSM2 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。

IDSM2 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

IDSM2 では、イーサネットまたはファスト イーサネット SPAN 送信元ポートからのイーサネット VLAN トラフィックを分析することも、イーサネット VLAN を SPAN 送信元として指定することもできます。ここでは、IDSM2 で SPAN を使用する方法について説明します。内容は次のとおりです。

Catalyst ソフトウェア

（注）　IDSM2 ポート番号は 7 または 8 のみです。

IDSM2 への 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。

次のオプションが適用されます。

- **disable**：ポートのモニタリングをディセーブルにします。
- *module/port*：送信元モジュールおよびポート番号。
- *vlan*：送信元 VLAN 番号。
- *module/port*：宛先モジュールおよびポート番号。
- **both**：受信トラフィックと送信トラフィックの両方。
- **filter**：VLAN にフィルタを適用します。
- **inpkts**：宛先ポートの着信パケットをイネーブル/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**：受信トラフィック。
- **session**：SPAN セッションのセッション番号。
- **tx**：送信トラフィック。

IDSM2 で 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　特権モードを開始します。

```
console> enable
```

ステップ 3　IDSM2 への SPAN をイネーブルにします。

- 送信元ポートから

```
console> (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

console> (enable)
```

（注）　送信元トランク ポート上の特定の VLAN についてトラフィックをモニタするには、**filter** キーワードを使用します。

- VLAN から

```
console> (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

console> (enable)
```

ステップ 4　SPAN セッションを表示します。

```
console> (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
console> (enable)
```

ステップ 5　IDSM2 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、次の手順を実行します。

```
console> (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
console> (enable)
```

Cisco IOS ソフトウェア

（注）　IDSM2 データ ポート番号には、1 または 2 を使用します。

IDSM2 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。

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**：GigabitEthernet IEEE 802.3z
- **Port-channel**：インターフェイスのイーサネット チャネル
- **,**：別のインターフェイス範囲を指定します
- **-**：インターフェイス範囲を指定します
- **both**：受信トラフィックと送信トラフィックをモニタします
- **rx**：受信トラフィックのみをモニタします
- **tx**：送信トラフィックのみをモニタします
- **intrusion-detection-module**：SPAN 宛先の侵入検知モジュール
- **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

IDSM2 で 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 モードを開始します。

```
router# 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。

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

例

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

ステップ 4　IDSM2 のデータ ポートを SPAN の宛先としてイネーブルにします。

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

例

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

ステップ 5　データ ポートに自動ステートが含まれていることを確認します。

```
router(config)# intrusion-detection module module_number data-port data_port_number
autostate include
```

例

```
router(config)# intrusion-detection module 9 data-port 1 autostate include
```

これによって、データ ポートが VLAN で唯一のポートになっている場合に、スイッチ仮想インターフェイスが稼動状態のままになります。デフォルトは **no include** です。

ステップ 6　（任意）そのデータ ポートの PortFast をイネーブルにします。

```
router(config)# intrusion-detection module module_number data-port data_port_number
portfast
```

例

```
router(config)# intrusion-detection module 9 data-port 1 portfast
```

デフォルトではディセーブルになっています。

ステップ 7　（任意）モニタ セッションをディセーブルにするには、次の手順を実行します。

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

ステップ 8　（任意）SPAN セッションをフィルタ処理して、特定の VLAN だけがスイッチ ポート トランクから認識できるようにします。

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

例

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

ステップ 9　コンフィギュレーション モードを終了します。

```
router(config)# exit
```

ステップ 10　現在のモニタ セッションを表示します。

```
router# show monitor session session_number
```

例

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

詳細情報

自動ステートおよび PortFast の詳細については、『*Catalyst 6500 Series Software Configuration Guide, 8.x*』を参照してください。

VACL キャプチャの設定

Cisco IOS ソフトウェアを使用している場合、単一の VLAN、複数の VLAN、または 7600 ルータの FLexWAN2 ポートからのトラフィックを、IPS のために VACL がキャプチャするように設定できます。ここでは、VACLS を使用してトラフィックをキャプチャする方法について説明します。内容は次のとおりです。

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 ポートであり、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) 以前のリリースの場合、デフォルトでポート 7 および 8 がトランク ポートとして設定され、キャプチャ機能によってセキュリティ ACL が適用されているすべての VLAN にトランク接続されます。特定の VLAN からのトラフィックのみをモニタする場合は、モニタしない VLAN はクリアして、ポート 7 およびポート 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 cram 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 と VLAN のマッピングを設定します
- **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**：ポートにリダイレクトするパケットを指定します
- **before**：editbuffer で指定した ace の前に、ACE を挿入します
- **capture**：キャプチャ ポートに、このフローのコピーを作成します
- **modify**：editbuffer で指定した ACE を変更します

VLAN 上で IPS 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　コンソールにログインします。

ステップ 2　特権モードを開始します。

```
console> enable
```

ステップ 3　トラフィックをキャプチャする VACL を作成します。許可、拒否、およびキャプチャするトラフィックを指定します。

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

（注） キャプチャできるのは、許可されたトラフィックに限られます。あるトラフィックを許可するがキャプチャしない場合は、**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 をコミットします。

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

VACL をコミットすると、VACL およびそれに関連付けられた ACE が NVRAM に書き込まれます。

ステップ 5　VACL を VLAN にマップします。

```
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　IDSM2 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 2/7
Successfully set 2/7 to capture ACL traffic.
```

Cisco IOS ソフトウェア

VLAN 上で IPS 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**：名前付きのアクセス リストを指定します。
  - **extended**：拡張アクセス リスト。
  - **hardware**：ハードウェア フラグメント処理をイネーブルにします。
  - **log-update**：アクセス リスト ログのアップデートを制御します。
  - **logging**：アクセス リストのロギングを制御します。
  - **resequence**：アクセス リストのシーケンス番号を再割り当てします。
  - **standard**：標準アクセス リスト。

VLAN 上で IPS 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　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 モードを開始します。

```
router# configure terminal
```

ステップ 3　ACL を定義します。

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

例

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

ステップ 4　VLAN アクセス マップを定義します。

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

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

```
router(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 シーケンスで action 句を前の match 句に付随するように設定します。

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

ステップ 7　指定した VLAN に VLAN アクセス マップを適用します。

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

ステップ 8　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 IDSM2 データ ポートを設定します。

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

（注）　スイッチがトラフィックをルーティングする場合は、ルーティング対象のすべての VLAN をモニタするように IDSM2 を設定する必要があります。VACL を FlexWan2 ポートに適用する場合は、すべての VLAN をモニタするように IDSM2 を設定する必要があります。

ステップ 9　IDSM2 でキャプチャ機能をイネーブルにします。

```
router(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。

```
router# 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
router#
```

ステップ 10　データ ポートに自動ステートが含まれていることを確認します。

```
router(config)# intrusion-detection module module_number data-port data_port_number
autostate include
```

例

```
router(config)# intrusion-detection module 4 data-port 1 autostate include
```

これによって、データ ポートが VLAN で唯一のポートになっている場合に、スイッチ仮想インターフェイスが稼動状態のままになります。デフォルトは **no include** です。

ステップ 11　（任意）そのデータ ポートの PortFast をイネーブルにします。

```
router(config)# intrusion-detection module module_number data-port data_port_number
portfast
```

例

```
router(config)# intrusion-detection module 4 data-port 1 portfast
```

デフォルトではディセーブルになっています。

詳細情報

自動ステートおよび PortFast の詳細については、『*Catalyst 6500 Series Software Configuration Guide, 8.x*』を参照してください。

mls ip ids コマンドの設定

ここでは、**mls ip ids** コマンドを使用して IPS トラフィックをキャプチャする方法について説明します。次の項目について説明します。

Catalyst ソフトウェア

Cisco IOS Firewall を MSFC で実行している場合、VACL を使用して IDSM2 のトラフィックをキャプチャすることはできません。これは、Cisco IOS ファイアウォール用の IP 検査規則を適用済みの VLAN には、VACL を適用できないためです。しかし、**mls ip ids** コマンドを使用することにより、キャプチャするパケットを指定することはできます。ACL で許可されたパケットがキャプチャされます。ACL によって拒否されたパケットはキャプチャされません。**permit**/**deny** パラメータは、パケットが宛先ポートに転送されるかどうかには影響しません。ルータ インターフェイスに着信するパケットは、IPS ACL と照合されて、キャプチャするかどうかが決定されます。**mls ip ids** コマンドは、スーパーバイザ設定ではなく MSFC 設定の一部として適用されます。**mls ip ids** コマンドは、着信トラフィックのみをキャプチャします。接続の両方向についてキャプチャを行うためには、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 **mls ip ids** コマンドを使用します。

mls ip ids コマンドを使用して IPS トラフィックをキャプチャするには、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　特権モードを開始します。

```
console> enable
```

ステップ 3　コンフィギュレーション モードを開始します。

```
Router# configure terminal
```

ステップ 4　キャプチャするパケットを指定するように ACL を設定します。

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

ステップ 5　キャプチャするパケットが伝送されるインターフェイスを選択します。

```
Router(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。

```
Router(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　特権モードを開始します。

```
console> enable
```

ステップ 9　スーパーバイザ エンジンで、IDSM2 モニタリング ポート（ポート 7 および 8）を VACL キャプチャ リストに追加します。

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

注意　**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 IDSM2 がキャプチャするためには、IDSM2 のポート 7 または 8 が、これらのパケットのルーティング先となるすべての VLAN のメンバーとなっている必要があります。

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 の適用先となる VLAN が存在しません。

mls ip ids コマンドを使用することにより、キャプチャするパケットを指定することはできます。ACL で許可されたパケットがキャプチャされます。ACL によって拒否されたパケットはキャプチャされません。**permit**/**deny** パラメータは、パケットが宛先ポートに転送されるかどうかには影響しません。ルータ インターフェイスに着信するパケットは、IPS ACL と照合されて、キャプチャするかどうかが決定されます。

mls ip ids コマンドを使用して IDS トラフィックをキャプチャするには、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 モードを開始します。

```
router# configure terminal
```

ステップ 3　キャプチャするパケットを指定するように ACL を設定します。

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

ステップ 4　キャプチャするパケットが伝送されるインターフェイスを選択します。

```
router(config)# interface interface_name
```

ステップ 5　キャプチャ VLAN を指定します。

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

例

```
router(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。

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

注意　**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 IDSM2 がキャプチャするためには、IDSM2 のデータ ポート 1 または 2 が、これらのパケットのルーティング先となるすべての VLAN のメンバとなっている必要があります。

インライン モードの IDSM2 用の Catalyst 6500 シリーズ スイッチの設定

IDM または CLI を使用して、別々の VLAN（IDSM2 のそれぞれの側で 1 つずつの VLAN）の間で、インライン モードで動作するように IDSM2 を設定できます。インライン モード用に IDSM2 を準備するには、スイッチも IDSM2 と同様に設定する必要があります。先にスイッチを設定してから、IDSM2 インターフェイスをインライン モードに設定します。ここでは、IDSM2 をインライン モードに設定する方法について説明します。内容は次のとおりです。

Catalyst ソフトウェア

Supervisor Engine 1a、Supervisor Engine 2、Supervisor Engine 32、または Supervisor Engine 720 を搭載した Catalyst ソフトウェア 8.4(1) 以降でインライン動作を行うには、IDSM2 モニタリング ポートをトランク 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 と同じなので、トラフィックは 802.1q カプセル化されません。

注意　Catalyst ソフトウェア 8.4.(3) よりも前は、IDSM2 ポート 7 および 8 のデフォルト設定で、すべての VLAN（1 ～ 4094）がトランク接続されていました。IDSM2 設定をクリアすると（**clear configuration** *module_number*）、IDSM2 によってすべての VLAN がトランク接続されます。IDSM2 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、ストームが発生するおそれがあります。ストームとは、多数のパケットがループし、宛先に到達しないことです。

IDSM2 のモニタリング ポートをインライン動作用に設定するには、次の手順に従います。

ステップ 1　コンソールにログインします。

ステップ 2　特権モードを開始します。

```
console> enable
```

ステップ 3　各 IDSM2 モニタリング ポートにネイティブ VLAN を設定します。

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

例

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

ステップ 4　各 IDSM2 モニタリング ポート（ポート 7 および 8）からすべての VLAN をクリアします。

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

例

```
console (enable)> clear trunk 9/7 1-4094
console (enable)> clear trunk 9/8 1-4094
```

ステップ 5　ステップ 3 で設定した単一のネイティブ VLAN をトランク接続するように、IDSM2 モニタリング ポート 7 および 8 を設定します。

```
console (enable)> set trunk slot_number/port_number vlan_number
```

例

```
console (enable)> set trunk 9/7 651
console (enable)> set trunk 9/8 652
```

ステップ 6　ステップ 3 のインターフェイスを IDSM2 上でペア設定します。

詳細情報

インライン インターフェイスをペア設定する手順については、「インライン インターフェイス ペアの設定」（P.6-20）を参照してください。

Cisco IOS ソフトウェア

IDSM2 モニタリング ポートをインライン操作のアクセス ポートとして設定します。

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 モードを開始します。

```
router# configure terminal
```

ステップ 3　IDSM2 がリンクする VLAN を選択します。

ステップ 4　各 IDSM2 データ ポートをそれぞれ単一の VLAN に設定します。

```
router(config)# intrusion-detection module slot_number data-port {1 | 2} access-vlan
vlan_number
router(config)# exit
```

例

```
router(config)# intrusion-detection module 13 data-port 1 access-vlan 661
router(config)# intrusion-detection module 13 data-port 2 access-vlan 662
router(config)# exit
```

ステップ 5　設定を確認します。

（注）　次の例では、スロット 13 の IDSM2 が、VLAN 661 と 662 の間でインラインになっています。IDSM2 データ ポート 1 が VLAN 661 にあり、データ ポート 2 が VLAN 662 にあります。

a.　IDSM2 の侵入検知設定を確認します。

```
router# 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
router#
```

b. IDSM2 データ ポート 1 が VLAN 661 のアクセス ポートになっていることを確認します。

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

例

```
router# 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。

```
router# show vlan id vlan-number
```

例

```
router# 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
------- --------- ----------------- ------------------------------------------
router#
```

ステップ 6　ステップ 4 のインターフェイスを IDSM2 上でペア設定します。

詳細情報

インライン インターフェイスをペア設定する手順については、「インライン インターフェイス ペアの設定」（P.6-20）を参照してください。

インライン VLAN ペア モードの IDSM2 用の Catalyst 6500 シリーズ スイッチの設定

IDM または CLI を使用して、インライン VLAN ペア モードで動作するように、IDSM2 を設定できます。インライン VLAN ペア モード用に IDSM2 を準備するには、スイッチも IDSM2 と同様に設定する必要があります。先にスイッチを設定してから、IDSM2 インターフェイスをインライン VLAN ペア モードに設定します。ここでは、IDSM-2 をインライン VLAN ペア モードに設定する方法について説明します。内容は次のとおりです。

Catalyst ソフトウェア

Supervisor Engine 1a、Supervisor Engine 2、Supervisor Engine 32、または Supervisor Engine 720 を搭載した Catalyst ソフトウェア 8.4(1) 以降でインライン VLAN ペア モードを使用するには、IDSM2 モニタリング ポートをトランク ポートとして設定します。

IDSM2 のモニタリング ポートをインライン VLAN ペア モード用に設定するには、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　特権モードを開始します。

```
console> enable
```

ステップ 3　IDSM2 モニタリング ポートから、すべての VLAN をクリアします。

```
console (enable)> clear trunk slot_number/port_number 1-4094
```

例

```
console (enable)> clear trunk 9/7 1-4094
```

（注）　Catalyst ソフトウェア 8.4.(3) よりも前は、IDSM2 モニタリング ポートから VLAN をクリアするときの VLAN 範囲の値が 1 ～ 1005、1024 ～ 4094 でした。これ以降のバージョンでは、全 VLAN 範囲の 1 ～ 4094 をクリアできます。

ステップ 4　ペア設定する VLAN をトランク接続するように、IDSM2 モニタリング ポートを設定します。

```
console (enable)> set trunk slot_number/port_number vlans_to_be_paired
```

例

```
console (enable)> set trunk 9/7 651,652
```

ステップ 5　ステップ 4 で使用した VLAN ペア以外の値になるように、IDSM2 モニタリング ポートのネイティブ VLAN を設定します。

```
console (enable)> set vlan vlan-number slot_number/port_number
```

例

```
console (enable)> set vlan 1 9/7
```

デフォルトのネイティブ VLAN は VLAN 1 です。

ステップ 6　IDSM2 モニタリング ポートで、ペア設定するその他の VLAN に対してステップ 4 を繰り返します。

ステップ 7　その他のモニタリング ポートを設定するには、ステップ 3 から 6 を繰り返します。

ステップ 8　ステップ 4 の VLAN を IDSM2 上でペア設定します。

詳細情報

インライン VLAN ペア モードで IDSM2 が実行されるように設定する手順については、「インライン VLAN ペアの設定」（P.6-24）を参照してください。

Cisco IOS ソフトウェア

インライン VLAN ペア動作用に、IDSM2 モニタリング ポートをトランク ポートとして設定します。

インライン VLAN ペアを設定するには、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 モードを開始します。

```
router# configure terminal
```

ステップ 3　ペア設定する VLAN をトランク接続するように、一方の IDSM2 モニタリング ポートを設定します。

```
router(config)# intrusion-detection module slot_number data-port data_port_number trunk
allowed-vlan vlans_to_be_paired
router(config)# exit
```

例

```
router(config)# intrusion-detection module 13 data-port 1 trunk allowed-vlan 661,662
router(config)# exit
```

ステップ 4　設定を確認します。

（注）　次の例では、スロット 13 の IDSM2 のデータ ポート 1 が、VLAN 661 と 662 をトランキングしています。

a. IDSM2 の侵入検知設定を確認します。

```
router# show run | include intrusion-detection
intrusion-detection module 13 management-port access-vlan 147
intrusion-detection module 13 data-port 1 trunk allowed-vlan 661,662
router#
```

b. IDSM2 データ ポートが正しい VLAN をトランキングしていることを確認します。

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

例

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

Switchport: Enabled
Administrative Mode: trunk
```

```
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: 661,662
Pruning VLANs Enabled: 2-1001
Vlans allowed on trunk: 661-662
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
Autostate mode: excluded
Portfast mode: default

router#
```

ステップ 5　ステップ 3 の VLAN を IDSM2 上でペア設定します。

詳細情報

インライン VLAN ペア モードで IDSM2 が実行されるように設定する手順については、「インライン VLAN ペアの設定」（P.6-24）を参照してください。

EtherChannel ロード バランシングの設定

ここでは、IDSM2 上での ECLB の設定方法について説明します。内容は次のとおりです。

EtherChannel のロード バランシングについて

Catalyst 6500 シリーズ シャーシに搭載されているスーパーバイザ エンジンは、IPS 5.*x* 以降を実行している IDSM2 デバイスを EtherChannel デバイスとして認識します。このため、最大 8 台の IDSM2 デバイスを同じ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 IDSM2 には、8 個の内部ポートがあります。使用されるのは、このうちの 4 個だけです。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 ソフトウェアではセンシング ポートで、Cisco IOS ソフトウェアではデータ ポート 1 および 2 になります。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。そのため、IDSM2 が処理できるパフォーマンスは約 600 Mbps ですが、1000 Mbps と表示されます。ECLB により、ポート 7 またはポート 8 で最大 8 台の IDSM2 デバイスをロード バランシングに参加させることができます。

EtherChannel と 3 つの検知モード

EtherChannel は、3 つのすべての検知モードで、複数の IDSM2 の間でのロード バランシングおよびフェイルオーバーを提供します。IDSM2 は、LACP や PAgP などの EtherChannel プロトコルには参加しません。Cisco IOS では、**src-dst-ip** アルゴリズムを使用したロード バランシングだけが可能です。そのため、指定された IP アドレス ペア間のすべてのパケットが常に同じチャネルにマップされます。Catalyst ソフトウェアは、**ip both** アルゴリズムを使用します。そのため、IDSM2 が 2 台のホスト間の接続を正しく追跡できる必要があります。

注意　EtherChannel グループ内で、ポート タイプの異なる IDSM2 データ ポートを混在させることはできません。1 つの EtherChannel グループのすべてのデータ ポートの設定は、同一にする必要があります。

3 つの検知モードで、EtherChannel と IDSM2 は次のように動作します。

- EtherChannel と無差別モード：IDSM2 が無差別モードで動作する場合、2 つのデータ ポートはそれぞれ独立して動作します。データ ポートが同じグループ内の複数の IDSM2 を持つようにスイッチを設定した場合、スイッチは IDSM2 間でトラフィックを分散します。これによって、複数の IDSM2 間でトラフィックの負荷が分散されます。データ ポートが `errDisabled` ステートになった場合、または IDSM2 がシャットダウン、電源オフ、またはリセットされた場合は、チャネルの再バランスを行う必要があります。
- EtherChannel とインライン モード：複数の IDSM2 をインライン モードに設定した場合、各 IDSM2 のデータ ポート 1 をあるチャネル グループに設定し、各 IDSM2 のデータ ポート 2 を別のチャネル グループに設定することによって、IDSM2 間でトラフィックのロード バランスを行うことができます。

注意　各 IDSM2 の 2 つのデータ ポートに同じトラフィックを必ず割り当てるには、EtherChannel グループが異なっていても、各 IDSM2 の両方のデータ ポートに同じ EtherChannel インデックスを割り当てる必要があります。

- EtherChannel とインライン VLAN ペア モード：IDSM2 がインライン on-a-stick モードで動作する場合、2 つのデータ ポートはそれぞれ独立して動作します。無差別モードと同じ制約が適用されます。

ECLB のイネーブル化

ここでは、Cisco IOS および Catalyst ソフトウェアで ECLB をイネーブルにする方法について説明します。次のような構成になっています。

- 「Catalyst ソフトウェア」（P.20-26）
- 「Cisco IOS ソフトウェア」（P.20-28）

Catalyst ソフトウェア

ここでは、Catalyst ソフトウェアの 3 つの検知モードで ECLB をイネーブルにする方法について説明します。次の項目について説明します。

- 「無差別モードおよび VLAN ペア モードの ECLB」（P.20-27）
- 「インライン モードの ECLB」（P.20-27）

無差別モードおよび VLAN ペア モードの ECLB

無差別モードおよびインライン VLAN ペア モードの場合は、各 IDSM2 の単一のポート（ポート 7 またはポート 8）を EtherChannel に追加します。

IDSM2 のモニタリング ポートを無差別モードまたはインライン VLAN ペア モードの ECLB 用に設定するには、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　特権モードを開始します。

```
console> enable
```

ステップ 3　各 IDSM2 を無差別モードまたはインライン VLAN ペア モード用に設定します。

ステップ 4　IDSM2 モニタリング ポートを EtherChannel に追加します。

```
console (enable)> set port channel slot_number/port_number channel_number
```

例

```
console (enable)> set port channel 1/7,7/7 1
```

ステップ 5　分散方式を設定します。

```
console (enable)> set port channel all distribution ip both
Channel distribution is set to ip both.
console (enable)>
```

ステップ 6　ECLB をイネーブルにします。

```
console (enable)> set port channel slot_number/port_number mode on
```

例

```
console (enable)> set port channel 1/7,7/7 mode on
```

詳細情報

インライン VLAN ペアを設定する手順については、「インライン VLAN ペアの設定」（P.6-24）を参照してください。

インライン モードの ECLB

インライン モードの場合、各 IDSM2 の単一のポート 7 を EtherChannel に追加し、各 IDSM2 のポート 8 を別の EtherChannel に追加します。

IDSM2 のモニタリング ポートをインライン モードの ECLB 用に設定するには、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　特権モードを開始します。

```
console> enable
```

ステップ 3　各 IDSM2 をインライン モード用に設定します。

ステップ 4　IDSM2 モニタリング ポート 7 を EtherChannel に追加します。

```
console (enable)> set port channel slot_number/7 channel_A_number
```

例

```
console (enable)> set port channel 1/7,7/7 1
```

ステップ 5　その EtherChannel に対して ECLB をイネーブルにします。

```
console (enable)> set port channel slot_number/7 mode on
```

例

```
console (enable)> set port channel 1/7,7/7 mode on
```

ステップ 6　IDSM2 モニタリング ポート 8 を別の EtherChannel に追加します。

```
console (enable)> set port channel slot_number/8 channel_B_number
```

例

```
console (enable)> set port channel 1/8,7/8 2
```

ステップ 7　その EtherChannel に対して ECLB をイネーブルにします。

```
console (enable)> set port channel slot_number/8 mode on
```

例

```
console (enable)> set port channel 1/8,7/8 mode on
```

ステップ 8　分散方式を設定します。

```
console (enable)> set port channel all distribution ip both
Channel distribution is set to ip both.
console (enable)>
```

詳細情報

インライン VLAN ペアを設定する手順については、「インライン VLAN ペアの設定」（P.6-24）を参照してください。

Cisco IOS ソフトウェア

ここでは、Cisco IOS ソフトウェアの 3 つの検知モードで ECLB をイネーブルにする方法について説明します。内容は次のとおりです。

（注）　インライン モードには、IOS 12.2(18)SXF4 以降が必要です。

デフォルトの復元

指定したデータ ポートのデフォルトを復元するには、**intrusion-detection module** *module_number* **data-port {1 | 2} default** コマンドを使用します。このコマンドによって、許可 VLAN、自動ステート、PortFast、コスト、プライオリティ設定が復元されます。データ ポートがポート チャネルに属している場合、このコマンドは無効です。このコマンドは、ポート チャネル グループにデータ ポートを追加する前に、データ ポートをクリアするときに役立ちます。

このコマンドは、次のコマンドをすべて使用することと同じです。

- **no intrusion-detection module** *module_number* **data-port {1 | 2} trunk allowed-vlan**
- **intrusion-detection module** *module_number* **data-port {1 | 2} access vlan**
- **intrusion-detection module** *module_number* **data-port {1 | 2} autostate include**
- **intrusion-detection module** *module_number* **data-port {1 | 2} portfast**
- **intrusion-detection module** *module_number* **data-port {1 | 2} spanning-tree cost**
- **intrusion-detection module** *module_number* **data-port {1 | 2} spanning-tree priority**

無差別モードの ECLB

（注） IDSM2 で EtherChannel ロード バランシングを行うために必要な Cisco IOS のバージョンおよびスーパーバイザの要件については、表 20-1 を参照してください。

（注） Cisco IOS は（SPAN またはモニタではなく）VACL キャプチャを使用して、無差別 IDSM2 EtherChannel をサポートします

EtherChannel は、フレーム内のアドレスに基づいて形成されたバイナリ パターンの一部を、チャネル内の 1 つのリンクを選択する数値に変換することによって、EtherChannel 内のリンク間でトラフィックの負荷を分散させます。

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 ポート番号を使用できます。これらは、送信元または宛先、あるいはその両方のアドレスまたはポートです。選択したモードは、スイッチ上で設定されているすべての EtherChannel に適用されます。ECLB には MPLS レイヤ 2 情報も使用できます。

使用している設定で最も多様なバランス基準を提供するオプションを使用してください。たとえば、EtherChannel 上のトラフィックが 1 つの MAC アドレスにだけ送信され、かつ ECLB の基準として宛先 MAC アドレスを使用している場合、EtherChannel は常に 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 バランスが向上することがあります。

IDSM2 上で無差別動作をするように ECLB を設定するには、次の手順を実行します。

ステップ 1　各 IDSM2 を無差別動作用に設定します。

（注） IDSM2 用に ECLB を設定する前に、すべての IDSM2 VACL キャプチャ、SPAN、またはモニタの設定行が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 モードを開始します。

```
Router# configure terminal
```

ステップ 4　VACL を作成します。

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

例

```
Router(config)# ip access-list extended idstest
```

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

```
Router(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。

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

例

```
Router(config)# vlan access-map idstestmap 10
Router(config-access-map)# match ip address idstest
Router(config-access-map)# action forward capture
```

ステップ 7　VLAN に VLAN アクセス マップを適用します。

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

例

```
Router(config)# vlan filter idstestmap vlan-list 50-60
```

ステップ 8　各 IDSM2 の目的のデータ ポートを目的の EtherChannel に追加します。

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

例

```
Router(config)# intrusion-detection module 13 data-port 1 channel-group 3
Router(config)# intrusion-detection module 12 data-port 1 channel-group 3
```

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 1 つずつあります。1 ～ 256 の番号のポート チャネル インターフェイスを最大 64 個設定できます。

ステップ 9　ECLB を設定します。

```
Router(config)# port-channel load-balance src-dst-ip
```

IDSM2 でサポートされるデフォルトで唯一のロード バランシング アルゴリズムは **src-dst-ip** です。そのため、EtherChannel が送信元と宛先の IP アドレスの組み合わせを分散方式として使用します。

ステップ 10　ロード バランシングを確認します。

```
Router# 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　EtherChannel にキャプチャされるように VLAN を設定します。

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

例

```
Router(config)# intrusion-detection port-channel 3 capture allowed-vlan 10
```

ステップ 12　EtherChannel へのキャプチャをイネーブルにします。

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

例

```
Router(config)# intrusion-detection port-channel 3 capture
```

ステップ 13　チャネル グループに自動ステートが含まれていることを確認します。

```
Router(config)# intrusion-detection port-channel channel_number autostate include
```

例

```
Router(config)# intrusion-detection port-channel 3 autostate include
```

これによって、データ ポートが VLAN で唯一のポートになっている場合に、スイッチ仮想インターフェイスが稼動状態のままになります。デフォルトは **no include** です。

ステップ 14　（任意）そのチャネル グループの PortFast をイネーブルにします。

```
Router(config)# intrusion-detection port-channel channel_number portfast enable
```

例

```
Router(config)# intrusion-detection port-channel 3 portfast enable
```

デフォルトではディセーブルになっています。

ステップ 15　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。

```
Router(config)# exit
```

ステップ 16　変更内容を保存します。

```
Router# write memory
```

詳細情報

- EtherChannel の詳細については、『*Catalyst 6500 Release 12.2SXF and Rebuilds Software Configuration Guide*』を参照してください。
- 自動ステートおよび PortFast の詳細については、『*Catalyst 6500 Series Software Configuration Guide, 8.x*』を参照してください。
- 無差別モードで IDSM2 を設定する手順については、「無差別モードの IDSM2 用の Catalyst 6500 シリーズ スイッチの設定」（P.20-9）を参照してください。

インライン モードの ECLB

（注）　IDSM2 用に ECLB を設定する前に、すべての IDSM2 VACL キャプチャ、SPAN、またはモニタの設定行が削除されていることを確認します。いずれかのポートでキャプチャをイネーブルにしているときに、チャネル グループをインライン モードに変更しようとすると、エラーが発生します。

IDSM2 上で ECLB をインライン モードに設定するには、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 モードを開始します。

```
router# configure terminal
```

ステップ 3　各 IDSM2 のすべてのデータ ポート 1 を EtherChannel に追加します。

```
router(config)# intrusion-detection module module_number data-port 1 port-channel
channel_number
```

例

```
router(config)# intrusion-detection module 1 data-port 1 port-channel 5
```

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 1 つずつあります。1 ～ 256 の番号のポート チャネル インターフェイスを最大 64 個設定できます。まだ作成されていない場合、このコマンドで、許可 VLAN リストが空のチャネル グループおよびポート チャネルが作成されます。ポート チャネルが存在する場合は、ポート チャネルの許可 VLAN リスト、PortFast、自動ステート、スパニング ツリー コスト、およびプライオリティ設定がデータ ポートに割り当てられます。

（注）　別のポート タイプが含まれているチャネル グループにデータ ポートを追加しようとした場合、または 1 つ以上のデータ ポートが含まれているポート チャネルに別のポート タイプを追加しようとした場合、エラーが発生します。

ステップ 4　各 IDSM2 のすべてのデータ ポート 2 を別の EtherChannel に追加します。

```
router(config)# intrusion-detection module module_number data-port 2 port-channel
channel_number
```

例

```
router(config)# intrusion-detection module 1 data-port 2 port-channel 6
```

ステップ 5　検知モードをアクセス（インライン）に設定し、データ ポート 1 が含まれるチャネル グループのアクセス VLAN を設定します。

```
router(config)# intrusion-detection port-channel channel_number access-vlan vlan_id
```

例

```
router(config)# intrusion-detection port-channel 5 access-vlan 1050
```

（注）　ポート チャネルが存在しない場合、またはポート チャネルがトランクまたはキャプチャ モード用にすでに設定されている場合、エラー メッセージが表示されます。ポート チャネルを作成するか、トランクまたはキャプチャ モードからポート チャネルを削除する必要があります。

ステップ 6　検知モードをアクセス（インライン）に設定し、データ ポート 2 が含まれるチャネル グループのアクセス VLAN を設定します。

```
router(config)# intrusion-detection port-channel channel_number access-vlan vlan_id
```

例

```
router(config)# intrusion-detection port-channel 6 access-vlan 10
```

ステップ 7　ECLB を設定します。

```
router(config)# port-channel load-balance src-dst-ip
```

デフォルトは **src-dst-ip** です。そのため、EtherChannel が送信元と宛先の IP アドレスの組み合わせを分散方式として使用します。

例

```
router(config)# port-channel load-balance src-dst-ip
```

ステップ 8　ECLB の確認

```
router# 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 9　アクセス（インライン）モードの場合は、各チャネル グループを **include** するように自動ステートを設定します。

```
router(config)# intrusion-detection port-channel channel_number autostate include
```

例

```
router(config)# intrusion-detection port-channel 5 autostate include
```

デフォルトは **no include** です。これによって、データ ポートが稼動中で VLAN にある場合に、スイッチ仮想インターフェイスの停止が防止されます。

ステップ 10　（任意）各チャネル グループの PortFast をイネーブルまたはディセーブルにします。

```
router(config)# intrusion-detection port-channel channel_number portfast enable
```

例

```
router(config)# intrusion-detection port-channel 5 portfast enable
```

デフォルトではディセーブルになっています。

ステップ 11　（任意）2 つのチャネル グループのそれぞれについて、スパニング ツリー パス コストを設定します。

```
router(config)# intrusion-detection port-channel channel_number spanning-tree cost
port_cost
```

例

```
router(config)# intrusion-detection port-channel 5 spanning-tree cost 4
```

各 IDSM2 のデータ ポート 1 とデータ ポート 2 が同じステート（フォワーディングまたはブロッキング）になるように、両方のチャネル グループに同じポート コストを設定する必要があります。

ステップ 12　（任意）2 つのチャネル グループのそれぞれについて、スパニング ツリー ポート プライオリティを設定します。

```
router(config)# intrusion-detection port-channel channel_number spanning-tree priority
priority
```

例

```
router(config)# intrusion-detection port-channel 5 spanning-tree priority 16
```

指定できるポート プライオリティ値は、0 ～ 240 の範囲の 16 の倍数です。デフォルトは 32 です。

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。

```
router(config)# exit
```

ステップ 14　変更内容を保存します。

```
router# write memory
```

詳細情報

- 自動ステート、PortFast、スパニング ツリーとポート コストの計算方法、ポート プライオリティの詳細については、『*Catalyst 6500 Series Software Configuration Guide, 8.x*』を参照してください。
- 無差別モードで IDSM2 を設定する手順については、「無差別モードの IDSM2 用の Catalyst 6500 シリーズ スイッチの設定」（P.20-9）を参照してください。

インライン VLAN ペア モードの ECLB

（注）　IDSM2 用に ECLB を設定する前に、すべての IDSM2 VACL キャプチャ、SPAN、またはモニタの設定行が削除されていることを確認します。いずれかのポートで**キャプチャ**をイネーブルにしているときに、チャネル グループをインライン VLAN ペア モードに変更しようとすると、エラーが発生します。

IDSM2 上で ECLB をインライン VLAN ペア モードに設定するには、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 モードを開始します。

```
router# configure terminal
```

ステップ 3　各 IDSM2 のデータ ポート（データ ポート 1 またはデータ ポート 2）を EtherChannel に追加します。

```
router(config)# intrusion-detection module module_number data-port [1:2] port-channel
channel_number
```

例

```
router(config)# intrusion-detection module 1 data-port 1 port-channel 5
```

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 1 つずつあります。1 ～ 256 の番号のポートチャネル インターフェイスを最大 64 個設定できます。まだ作成されていない場合、このコマンドで、許可 VLAN リストが空のチャネル グループおよびポート チャネルが作成されます。ポート チャネルが存在する場合は、ポート チャネルの許可 VLAN リスト、PortFast、自動ステート、スパニング ツリー コスト、およびプライオリティ設定がデータ ポートに割り当てられます。

（注）　別のポート タイプが含まれているチャネル グループにデータ ポートを追加しようとした場合、または 1 つ以上のデータ ポートが含まれているポート チャネルに別のポート タイプを追加しようとした場合、エラーが発生します。

ステップ 4　検知モードをトランク（インライン VLAN ペア）に設定し、データ ポート 1 が含まれるチャネル グループのアクセス VLAN を設定します。ペア設定する VLAN（100 と 200、101 と 201 など）を決定し、すべてのペアのすべての VLAN が含まれるように許可 VLAN リストを設定します。

```
router(config)# intrusion-detection port-channel channel_number trunk allowed-vlan
vlan_list
```

例

```
router(config)# intrusion-detection port-channel 5 trunk allowed-vlans 100,101,200,201
```

（注）　スイッチの許可 VLAN リストには、インライン VLAN ペアとして IDSM2 で組み合わされたすべての VLAN が含まれている必要があります。含まれていない場合、トラフィックがドロップされます。

（注）　ポート チャネルが存在しない場合、またはポート チャネルがトランクまたはキャプチャ モード用にすでに設定されている場合、エラー メッセージが表示されます。ポート チャネルを作成するか、トランクまたはキャプチャ モードからポート チャネルを削除する必要があります。

ステップ 5　ECLB を設定します。

```
router(config)# port-channel load-balance src-dst-ip
```

デフォルトは **src-dst-ip** です。そのため、EtherChannel が送信元と宛先の IP アドレスの組み合わせを分散方式として使用します。

例

```
router(config)# port-channel load-balance src-dst-ip
```

ステップ 6　ECLB の確認

```
router# 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 7　アクセス（インライン）モードの場合は、チャネル グループを **include** するように自動ステートを設定します。

```
router(config)# intrusion-detection port-channel channel_number autostate include
```

例

```
router(config)# intrusion-detection port-channel 5 autostate include
```

デフォルトは **no include** です。これによって、データ ポートが稼動中で VLAN にある場合に、スイッチ仮想インターフェイスの停止が防止されます。

ステップ 8　（任意）チャネル グループの PortFast をイネーブルまたはディセーブルにします。

```
router(config)# intrusion-detection port-channel channel_number portfast enable
```

例

```
router(config)# intrusion-detection port-channel 5 portfast enable
```

デフォルトではディセーブルになっています。

ステップ 9　（任意）チャネル グループのスパニング ツリー ポート コストを設定します。

```
router(config)# intrusion-detection port-channel channel_number spanning-tree cost
port_cost
```

例

```
router(config)# intrusion-detection port-channel 5 spanning-tree cost 4
```

ステップ 10　（任意）チャネル グループのスパニング ツリー ポート プライオリティを設定します。

```
router(config)# intrusion-detection port-channel channel_number spanning-tree priority
priority
```

例

```
router(config)# intrusion-detection port-channel 5 spanning-tree priority 16
```

指定できるポート プライオリティ値は、0 ～ 240 の範囲の 16 の倍数です。デフォルトは 32 です。

ステップ 11　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。

```
router(config)# exit
```

ステップ 12　変更内容を保存します。

```
router# write memory
```

ステップ 13　ステップ 4 の VLAN を IDSM2 上でペア設定します。

詳細情報

- 自動ステート、PortFast、スパニング ツリーとポート コストの計算方法、ポート プライオリティの詳細については、『*Catalyst 6500 Series Software Configuration Guide, 8.x*』を参照してください。
- VLAN をペア設定する手順については、「インライン VLAN ペアの設定」（P.6-24）を参照してください。

ECLB のディセーブル化

ここでは、ECLB をディセーブルにする方法について説明します。内容は次のとおりです。

Catalyst ソフトウェア

ECLB 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　特権モードを開始します。

```
console> enable
```

ステップ 3　ECLB で無差別モードまたはインライン VLAN ペア モードをディセーブルにします。

```
console (enable)> set port channel slot_number/port_number mode off
```

例

```
console (enable)> set port channel 1/7,7/7 mode off
```

ステップ 4　ECLB でインライン モードをディセーブルにします。

a. 一方の EtherChannel の ECLB をディセーブルにします。

```
console (enable)> set port channel slot_number/7 mode off
```

例

```
console (enable)> set port channel 1/7,7/7 mode off
```

b. もう一方の EtherChannel の ECLB をディセーブルにします。

```
console (enable)> set port channel slot_number/8 mode off
```

例

```
console (enable)> set port channel 1/8,7/8 mode off
```

Cisco IOS ソフトウェア

IDSM2 の ECLB 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 モードを開始します。

```
Router# configure terminal
```

ステップ 3　EtherChannel から単一の IDSM2 を削除します。

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

例

```
Router(config)# no intrusion-detection module 1 data-port 1 channel-group 5
```

ステップ 4　EtherChannel 全体を削除します。

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

例

```
Router(config)# no intrusion-detection module port-channel 5
```

（注）　IDSM2 の VACL キャプチャ コマンドは残っています。

ECLB の確認

ここでは、ECLB コンフィギュレーションを確認する方法について説明します。次の項目について説明します。

Catalyst ソフトウェア

ECLB 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　特権モードを開始します。

```
console> enable
```

ステップ 3　すべての EtherChannel を表示します。

```
console (enable)> show channel slot_number/port_number mode off
```

例

```
console> (enable) show channel
Channel Id   Ports
-----------  ------------------------------------------------
1669         1/7,7/7
1698         2/1-6
console> (enable)
```

（注）　この出力では、2 つの IDSM2 データ ポートを持つ ID 1669 の EtherChannel が作成されています。ポート 1/7 は、スロット 1 の IDSM2 のポート 7 で、ポート 7/7 は、スロット 7 の IDSM2 のポート 7 です。どちらの IDSM2 も、無差別動作用に設定されています。2 つの IDSM2 ポート間（各 IDSM2 の 1 ポートずつ）で、ロード バランスが行われます。

ステップ 4　特定の EtherChannel ステータスを表示します。

```
console (enable)> show channel hash channel_id source_ip_addr dest_ip_addr
```

例

```
console> (enable) show channel hash 1669 10.20.2.1 10.20.5.3
Selected channel port: 1/7
console> (enable)
```

（注）　この出力では、10.20.2.1 から 10.20.5.3 へのトラフィックがポート 1/7（スロット 1 の IDSM2 のポート 7）に送信されることが示されています。

Cisco IOS ソフトウェア

IDSM2 ECLB 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 を表示します。

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

Group: 10
----------
```

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

router#
```

ステップ 3　特定の EtherChannel ステータスを表示します。

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

例

```
router# 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
------+-------------+-----------+-----------------------------

router#
```

ステップ 4　ECLB 設定を表示します。

```
router# 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
router#
```

ステップ 5　IDSM2 データ ポート情報を表示します。

```
router# show intrusion-detection module module_number data-port data_port_number state
```

例

```
router# show intrusion-detection module 11 data-port 2 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
```

IDSM2 の管理タスク

ここでは、IDSM2 の管理タスクを実行するときに役立つ手順を示します。次の項目について説明します。

全メモリ テストのイネーブル化

IDSM2 を初めてブートすると、デフォルトで部分メモリ テストが実行されます。Catalyst ソフトウェアおよび Cisco IOS ソフトウェアでは、全メモリ テストをイネーブルにできます。ここでは、全メモリ テストをイネーブルにする方法について説明します。内容は次のとおりです。

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　特権モードを開始します。

```
console> enable
```

ステップ 3　全メモリ テストをイネーブルにします。

```
console> (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.
console> (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　IDSM2 をリセットします。

全メモリ テストが実行されます。

（注）　全メモリ テストは、部分メモリ テストよりも完了までに時間がかかります。

詳細情報

IDSM2 をリセットする手順については、「IDSM2 のリセット」（P.20-41）を参照してください。

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。

```
router# 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
router#
```

ステップ 3　IDSM2 をリセットします。

全メモリ テストが実行されます。

（注）　全メモリ テストは、部分メモリ テストよりも完了までに時間がかかります。

詳細情報

IDSM2 をリセットする手順については、「IDSM2 のリセット」（P.20-41）を参照してください。

IDSM2 のリセット

何らかの理由により、SSH、Telnet、またはスイッチの **session** コマンドによって IDSM2 と通信できないときは、スイッチのコンソールから IDSM2 をリセットする必要があります。リセット プロセスには数分かかります。ここでは、IDSM2 のリセット方法について説明します。内容は次のとおりです。

Catalyst ソフトウェア

CLI から IDSM2 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　特権モードを開始します。

```
console> enable
```

ステップ 3　IDSM2 をアプリケーション パーティションまたはメンテナンス パーティションにリセットします。

```
console> (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、IDSM2 はブート デバイス変数を使用します。

例

```
console> (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.
console> (enable)
```

注意　IDSM2 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、IDSM2 を複数回リセットしなければならないことがあります。リセット操作を 3 回繰り返しても IDSM2 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。

詳細情報

IDSM2 のイメージを再作成する手順については、「IDSM2 システム イメージのインストール」（P.23-29）を参照してください。

Cisco IOS ソフトウェア

IDSM2 をリセットするには、EXEC モードで **hw-module module** *slot_number* **reset** {**hdd:1** | **cf:1**} コマンドを使用します。リセット プロセスには数分かかります。指定したブート パーティションに、IDSM2 がブートします。ブート ストリングを指定しないと、デフォルトの起動設定が使用されます。

CLI から IDSM2 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　IDSM2 をリセットします。

```
router# 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、IDSM2 はブート デバイス変数を使用します。

例

```
router# 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
router#
```

Catalyst および Cisco IOS ソフトウェアのコマンド

（注）　Catalyst および Cisco IOS ソフトウェアの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。これらのマニュアルの検索方法については、『*Documentation Roadmap for Cisco Intrusion Prevention System 7.0*』を参照してください。

ここでは、IDSM2 に関連する Catalyst および Cisco IOS ソフトウェアのコマンドを示します。次の項目について説明します。

Catalyst ソフトウェア

ここでは、Catalyst ソフトウェアでサポートされているコマンドおよびサポートされていないコマンドを示します。次の項目について説明します。

サポートされているスーパーバイザ エンジン コマンド

IDSM2 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。これらの詳細については、Catalyst 6500 シリーズのコマンド リファレンスで説明されています。

- **clear config** *module_number*

  指定した IDSM2 に関連付けられているスーパーバイザ エンジンの設定をクリアします。

- **clear log** *module_number*

  指定した IDSM2 のエラー ログのすべてのエントリを削除します。

- **session** *slot_number*

  スイッチ コンソールから IDSM2 のコンソールにログインします。

- **set module** コマンド（次に示す以外のすべての **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**}

    指定した IDSM2 へ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*

  指定した IDSM2 ポートの名前を設定します。

- **set span**

  ポート 1 を SPAN の宛先ポートとして設定します。IDSM2 のポート 1 は SPAN の送信元ポートとしては使用できません。

- **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 エンジンの NVRAM 設定を表示します。

- **show log**

  指定した IDSM2 のエラー ログを表示します。

- **show mac** *module_number*

  指定した IDSM2 の MAC カウンタを表示します。

- **show module** *module_number*

  IDSM2 が取り付けられている場合に、`Module-Type` の下に `Intrusion Detection System Module` と表示します。

- **show port** *module_number*

  指定した IDSM2 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）と管理ポート（ポート 2）の両方の診断テスト、および BIOS と CMOS のブート結果からレポートされたエラーを表示します。

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、IDSM2 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

ここでは、IDSM2 がサポートしている Cisco IOS ソフトウェアのコマンドを示します。これらのコマンドは、モードに基づいてグループ化されています。ここでは、次の項目について説明します。

- 「EXEC コマンド」（P.20-45）
- 「コンフィギュレーション コマンド」（P.20-47）

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**

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

  現在の日付と時刻を設定します。
- **clock update-calendar**

  カレンダーの時刻をクロックの時刻にアップデートします。
- **hw-module module** *module_number* **reset** {**cf:1** | **hdd:1**}

ブート デバイス変数で指定されたパーティションに IDSM2 をリセットします。ブート デバイス変数が設定されていない場合、IDSM2 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。**cf:1** は、メンテナンス パーティションです。**hdd:1** は、アプリケーション パーティションです。

- **hw-module module** *module_number* **shutdown**

  IDSM2 を安全にシャーシから取り外せるようにシャットダウンします。
- **reload**

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

  スイッチ コンソールから IDSM2 のコンソールにログインします。
- **show boot device module** *module_number*

  指定したモジュールの現在の起動設定を表示します。
- **show diagnostic result module** *module_number*

  IDSM2 が最後に起動されたときに実行されたオンライン診断の結果を表示します。
- **show interface port-channel** *channel_number*

  ポート チャネルのステータスを表示します。
- **show intrusion-detection module** *module_number* **data-port {1 | 2} {state | traffic}**

  指定した IDSM2 データ ポートのステートまたは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 | traffic}**

  IDSM2 管理ポートのステートまたは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 [***module_number* **| all | version]**

  インストールされているモジュールと、そのバージョンおよび状態を表示します。
- **show monitor session** *session_number*

  指定したセッションの SPAN 送信元および宛先を表示します。
- **show running-config**

  現在実行中の設定を表示します。
- **show spanning-tree active**

  アクティブ インターフェイスのスパニング ツリー ステート情報だけを表示します。
- **show spanning-tree detail**

  詳細なスパニング ツリー ステート情報を表示します。
- **show spanning-tree summary [totals]**

  スパニング ツリーの上位のステートを表示します。インターフェイス固有の情報は表示されません。
- **show spanning-tree vlan** *vlan_number*

  指定した VLAN のスパニング ツリー ステート情報を表示します。これらの VLAN が転送またはブロックされるポートのリストが含まれます。

- **show startup-config**

  保存されている設定を表示します。

- **show vlan access-map**

  現在のすべての VLAN アクセス マップを表示します。

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 サブモードで実行できます。

- グローバル コンフィギュレーション モード
  - **boot device module** *number_number* {**cf:1** | **hdd:1**}

    指定したモジュールのデフォルト ブート デバイスを設定します。**cf:1** は MP にブートし、**hdd:1** は AP にブートします。オプションを設定しないと、ブート ストリングがクリアされ、デフォルト ブート デバイスが AP に設定されます。

  - **clock calendar valid**

    起動時に、現在のカレンダー時刻をスイッチの時刻として設定します。

  - **clock summer-time** *zone* **recurring**

    スイッチがサマータイム設定を使用するように設定します。

  - **clock timezone** *zone offset*

    スイッチ/IDSM2 のタイムゾーンを設定します。

  - **fabric switching-mode force busmode**

    パケット再循環をサポートしないサービス モジュールが、スイッチ ファブリックではなく、シャーシ共有バス経由で通信するようにします。これによって、スーパーバイザがパケット再循環を集中的に処理し、サービス モジュールが上記の条件に合った VLAN で適切に通信できるようになります。このコマンドをイネーブルにしても、この問題の影響を受けない他のファブリック対応モジュールは、引き続きスイッチ ファブリックで通信します。

  - **[no] intrusion-detection module** *module_number* **data-port {1 | 2} access vlan** *vlan_id*

    指定したモジュールのデータ ポートをアクセス（インライン）モードに設定し、データ ポートのアクセス VLAN を設定します。

  - **[no] intrusion-detection module** *module_number* **data-port {1 | 2} autostate include**

    指定したデータ ポートを自動ステートの計算に含めます（または計算から除外します）。含めた場合、モジュールのデータ ポートがイネーブルの間、MSFC または WLAN ポートに関連付けられたスイッチ仮想インターフェイスは稼動状態のままになります。除外した場合、指定したモジュールのデータ ポートが VLAN で唯一のアクティブ ポートの場合に、MSFC または WAN ポートに関連付けられたスイッチ仮想インターフェイスがダウンします。デフォルトは **no include** です。

  - **[no] intrusion-detection module** *module_number* **data-port {1 | 2} capture**

    指定したデータ ポートをキャプチャ先ポートに設定します。パケットをキャプチャする前に、**intrusion-detection module** *module_number* **data-port {1 | 2} capture** コマンドを使用して、許可 VLAN リストを設定する必要があります。IDSM2 を無差別モードにしておく必要があります。

  - **[no] intrusion-detection module** *module_number* **data-port {1 | 2} capture allowed-vlan** *vlan_list*

指定したデータ ポートの許可 VLAN をパケット キャプチャに指定します。データ ポートでトラフィックをキャプチャする前に、**intrusion-detection module** *module_number* **data-port {1 | 2} capture** コマンドを使用して、データポートでキャプチャ モードをイネーブルにする必要もあります。

- **intrusion-detection module** *module_number* **data-port {1 | 2} default**

  指定したデータ ポートの許可 VLAN、自動ステート、PortFast、ポート コスト、およびプライオリティ設定をデフォルト値に戻します。このコマンドは、データ ポートをチャネル グループに追加する前に、データ ポートからすべての設定を削除するときに役立ちます。

- **[no] intrusion-detection module** *module_number* **data-port {1 | 2}port-channel** *channel_number*

  指定したモジュールのデータ ポートをチャネル グループに追加し、同じ数字 ID のポート チャネルを作成します。まだ作成されていない場合、このコマンドで、許可 VLAN リストが空のチャネル グループおよびポート チャネルが作成されます。**no** オプションを使用すると、チャネル グループからデータ ポートが削除され、データ ポートの設定がデフォルトに戻り、ポート チャネルが空であれば削除されます。

- **[no] intrusion-detection module** *module_number* **data-port {1 | 2}portfast {enable | disable} [trunk]**

  データ ポート上で PortFast をイネーブルまたはディセーブルにします。PortFast をイネーブルにすると、スパニング ツリーの構築中に、スイッチによってトラフィックが IDSM2 データ ポートに転送されます。ディセーブルの場合、ツリーが構築され、バックプレーン ポートがフォワーディング ステートになるまで、トラフィックは拒否されます。デフォルトではディセーブルになっています。trunk オプションは、データ ポートがトランク（無差別モードまたはインライン VLAN ペア モード）として設定されているときに、PortFast をイネーブルまたはディセーブルにします。

- **[no] intrusion-detection module** *module_number* **data-port {1 | 2} spanning-tree cost** *path_cost*

  指定したモジュールのデータ ポートのスパニング ツリー パス コストを設定します。**no** オプションを使用すると、指定したモジュールのデータ ポートのスパニング ツリー コストがデフォルト コスト値に戻ります。

- **[no] intrusion-detection module** *module_number* **data-port {1 | 2} trunk allowed-vlan** *vlan_list*

  指定したモジュールのデータ ポートをトランキング モードに設定し、データ ポートの許可 VLAN リストを設定します。**no** オプションを使用すると、指定したモジュールのデータ ポートがトランキング モードから削除され、データ ポートの許可 VLAN リストがクリアされます。

- **intrusion-detection module** *module_number* **management-port access-vlan** *vlan_number*

  IDSM2 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 キャプチャを行う VLAN を設定します。

- **intrusion-detection module** *module_number* **data-port** *data_port_number* **capture**

  指定した IDSM2 データ ポートの VACL キャプチャをイネーブルにします。

- [**no**] **intrusion-detection port-channel** *channel_number* **access vlan** *vlan_id*

指定したポート チャネルのすべてのデータ ポートをアクセス モードに設定し、データ ポートのアクセス VLAN を設定します。**no** オプションを使用すると、指定したポート チャネルのすべてのモジュールのデータ ポートの許可 VLAN リストがクリアされます。

- **[no] intrusion-detection port-channel** *channel_number* **autostate include**

  指定したポート チャネルのすべてのデータ ポートを自動ステートの計算に含めるか、計算から除外します。含めた場合、データ ポートがイネーブルの間、MSFC または WLAN ポートに関連付けられた仮想スイッチ インターフェイスは稼動状態のままになります。除外した場合、データ ポートが VLAN で唯一のアクティブ ポートの場合に、MSFC または WAN ポートに関連付けられた仮想スイッチ インターフェイスがダウンします。デフォルトでは、データ ポートは自動ステートの計算から除外されます。

- **[no] intrusion-detection port-channel** *channel_number* **capture**

  チャネル グループのすべてのデータ ポートをキャプチャ ポートとして設定します。**no** オプションを使用すると、チャネル グループのすべてのデータ ポートで、キャプチャ機能がディセーブルになります。

- [**no**] **intrusion-detection port-channel** *channel_number* **capture allowed-vlan** *vlan_id*

  指定したポート チャネルのすべてのモジュールのデータ ポートで、キャプチャ VLAN リストを設定します。このコマンドでは、チャネル グループがキャプチャ モードに設定されません。チャネル グループをキャプチャ モードに設定するには、**intrusion-detection port-channel** *channel_number* **capture** コマンドを使用します。**no** オプションを使用すると、指定したポート チャネルのすべてのモジュールのデータ ポートのキャプチャ VLAN リストがクリアされます。

- **[no] intrusion-detection port-channel** *channel_number* **portfast {enable | disable} [trunk]**

  ポートチャネルのデータ ポート上で PortFast をイネーブルまたはディセーブルにします。PortFast をイネーブルにすると、スパニング ツリーの構築中に、スイッチによってトラフィックがデータ ポートに転送されます。ディセーブルの場合、ツリーが構築され、バックプレーン ポートがフォワーディング ステートになるまで、トラフィックは拒否されます。データ ポートがトランク（無差別モードまたはインライン VLAN ペア モード）として設定されているときに、PortFast をイネーブルまたはディセーブルにするには、**trunk** オプションを使用します。データ ポートがアクセス ポート（インライン モード）として設定されているときは、**trunk** オプションを使用しないでください。portfast および portfast trunk オプションは、デフォルトでディセーブルになっています。

- [**no**] **intrusion-detection port-channel** *channel_number* **spanning-tree cost** *port_cost*

  指定したモジュールのデータ ポートのスパニング ツリー ポート コストを設定します。**no** オプションを使用すると、指定したモジュールのデータ ポートのスパニング ツリー ポート コストがデフォルト値に戻ります。

- [**no**] **intrusion-detection port-channel** *channel_number* **spanning-tree priority** *priority*

  指定したモジュールのデータ ポートのスパニング ツリー ポート プライオリティを設定します。**no** オプションを使用すると、指定したモジュールのデータ ポートのスパニング ツリー ポート プライオリティがデフォルト値に戻ります。

- [**no**] **intrusion-detection port-channel** *channel_number* **trunk allowed-vlan** *vlan_id*

  指定したポート チャネルのすべてのモジュールのデータ ポートで、許可 VLAN リストを設定します。**no** オプションを使用すると、指定したポート チャネルのすべてのモジュールのデータ ポートの許可 VLAN リストがクリアされます。

- **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。

- **[no] monitor session** *session_number* **destination intrusion-detection module** *module_number* **data-port {1 | 2}**

  SPAN 宛先ポートを設定します。標準ラインカード ポートまたは IDSM2 データ ポートを設定できます。

- **[no] monitor session** *session_number* {**source** {**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** *module_number*

  IDSM2 の電源をオフまたはオンにします。

- **[no] spanning tree mode {pvst | mst | rapid-pvst}**

  スイッチでグローバルに使用するスパニング ツリー プロトコル（PVST+、MST、または Rapid-PVST+）を選択します。デフォルトは PVST です。MST は IDSM2 ではサポートされません。**no** オプションを使用すると、スパニング ツリー モードがデフォルトに戻ります。

- **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 にマップします。

- 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*

    許可された VLAN をトランク用に設定します。

  - **switchport trunk encapsulation dot1q**

    dot1q をカプセル化されたタイプとして設定します。

  - **switchport trunk native vlan** *vlan*

    ネイティブ VLAN をトランク ポート用に設定します。

- 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キャプチャするように指定します。

  - **match ip address** [*1-199* | *1300-2699* | *acl_name*]

    VACL 内でのフィルタ処理を指定します。