



CHAPTER 2

ファイアウォール サービス モジュールを使用するためのスイッチの設定

この章では、FWSM と組み合わせて使用できるように、Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータを設定する方法について説明します。この章で説明する作業を行う前に、スイッチに付属のマニュアルに従って、インターフェイスへの VLAN 割り当てをはじめ、スイッチの基本的なプロパティを設定してください。

この章では、次の内容について説明します。

- 「スイッチの概要」(P.2-1)
- 「モジュールの搭載確認」(P.2-2)
- 「ファイアウォール サービス モジュールを通過するトラフィックの確認」(P.2-3)
- 「ファイアウォール サービス モジュールの状態の確認」(P.2-3)
- 「ファイアウォール サービス モジュールへの VLAN の割り当て」(P.2-4)
- 「MSFC へのスイッチ仮想インターフェイスの追加」(P.2-6)
- 「FWSM の内部インターフェイスのカスタマイズ」(P.2-10)
- 「フェールオーバーを使用するためのスイッチの設定」(P.2-11)
- 「ファイアウォール サービス モジュールのブートパーティションの管理」(P.2-12)

スイッチの概要

FWSM は、Cisco 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータに搭載できます。いずれのシリーズも設定が同じであるため、このマニュアルではこれらのシリーズを総称して「スイッチ」と表記しています。このスイッチには、スイッチ（スーパーバイザ エンジン）とルータ（MSFC）があります。

スイッチのスーパーバイザ エンジンと統合型の MSFC ルータの両方で Cisco IOS ソフトウェアがサポートされています。



(注) Catalyst オペレーティング システム ソフトウェアはサポートされていません。

FWSM は独自の OS で動作します。



(注) FWSM は独自のオペレーティング システムで動作するので、Cisco IOS ソフトウェアをアップグレードしても FWSM の動作には影響ありません。

MSFC の詳細については、「[MSFC の使用方法](#)」(P.1-6) を参照してください。

一部の FWSM 機能は Cisco IOS 機能と連携しますが、特定バージョンの Cisco IOS ソフトウェアが必要となります。詳細については、「[スイッチ ハードウェアおよびソフトウェアの互換性](#)」(P.A-1) を参照してください。次の機能には、Cisco IOS ソフトウェアが含まれています。詳細については、各機能に関するセクションを参照してください。

- ルートヘルス注入：「[Route Health Injection の設定](#)」(P.8-36) を参照してください。
- PISA 統合：「[PISA 統合でのアプリケーション タイプの許可または拒否](#)」(P.21-4) を参照してください。
- Virtual Switching System (VSS; 仮想スイッチング システム) サポート：FWSM の設定は必要ありません。



(注) Cisco IOS ソフトウェア Version 12.2(18)SX6 以前では、スイッチ内の FWSM ごとに SPAN リフレクタ機能がイネーブルになっています。この機能により、FWSM から送られてきたマルチキャストトラフィック（および中央の書き換えエンジンを必要とする他のトラフィック）をスイッチングできます。SPAN リフレクタ機能は SPAN セッションを 1 つ使用します。この機能をディセーブルにするには、次のコマンドを入力します。

```
Router(config)# no monitor session servicemodule
```

モジュールの搭載確認

スイッチが FWSM を認識してオンラインにしているかどうかを確認するには、次のコマンドを使用してモジュール情報を表示します。

```
Router> show module [mod-num | all]
```

次に、**show module** コマンドの出力例を示します。

```
Router> show module
Mod Ports Card Type                               Model                               Serial No.
-----
 1     2 Catalyst 6000 supervisor 2 (Active)   WS-X6K-SUP2-2GE                     SAD0444099Y
 2    48 48 port 10/100 mb RJ-45 ethernet     WS-X6248-RJ-45                       SAD03475619
 3     2 Intrusion Detection System             WS-X6381-IDS                         SAD04250KV5
 4     6 Firewall Module                       WS-SVC-FWM-1                         SAD062302U4
```



(注) **show module** コマンドの出力に FWSM の 6 つのポートが示されています。これらのポートは、EtherChannel としてひとまとめにされた内部ポートです。詳細については、「[FWSM の内部インターフェイスのカスタマイズ](#)」(P.2-10) を参照してください。

ファイアウォール サービス モジュールを通過するトラフィックの確認

トラフィックが FWSM を通過するか確認するには、次のコマンドを使用してモジュール情報を表示します。

```
Router> show firewall module [mod-num | traffic]
```

次に、**show firewall module traffic** コマンドの出力例を示します。

```
Router> show firewall module 11 traffic
Firewall module 11:

Specified interface is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 0014.1cd5.bef6 (bia 0014.1cd5.bef6)
  MTU 1500 bytes, BW 6000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Full-duplex, 1000Mb/s, media type is unknown
  input flow-control is on, output flow-control is on
  Members in this channel: Gi11/1 Gi11/2 Gi11/3 Gi11/4 Gi11/5 Gi11/6
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queuing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 10000 bits/sec, 17 packets/sec
    8709 packets input, 845553 bytes, 0 no buffer
    Received 745 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 input packets with dribble condition detected
  18652077 packets output, 1480488712 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```

ファイアウォール サービス モジュールの状態の確認

FWSM の状態を確認するには、次のコマンドを入力してモジュール情報を表示します。

```
Router> show firewall module [mod-num | state]
```

次に、**show firewall module state** コマンドの出力例を示します。

```
Router> show firewall module 11 state
Firewall module 11:
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: 3,6,7,20-24,40,59,85,87-89,99-115,150,188-191,200,250,
  501-505,913,972
Pruning VLANs Enabled: 2-1001
```

■ ファイアウォール サービス モジュールへの VLAN の割り当て

```
Vlans allowed on trunk:
Vlans allowed and active in management domain:
Vlans in spanning tree forwarding state and not pruned:
```

ファイアウォール サービス モジュールへの VLAN の割り当て

ここでは、FWSM に VLAN を割り当てる方法について説明します。FWSM には、外部物理インターフェイスが組み込まれていません。代わりに VLAN インターフェイスを使用します。FWSM への VLAN の割り当ては、スイッチ ポートへの VLAN の割り当てと同様です。FWSM には、Switch Fabric Module (SFM; スイッチ ファブリック モジュール) (搭載されている場合) または共有バスへの内部インターフェイスが組み込まれています。



(注) VLAN をスイッチに追加してスイッチ ポートに割り当てる方法については、スイッチのマニュアルを参照してください。

ここでは、次の内容について説明します。

- 「VLAN の注意事項」(P.2-4)
- 「FWSM への VLAN の割り当て」(P.2-4)

VLAN の注意事項

FWSM で VLAN を使用する際の注意事項は、次のとおりです。

- FWSM では、プライベート VLAN を使用できます。FWSM にプライマリ VLAN を割り当てると、FWSM は自動的にセカンダリ VLAN トラフィックを処理します。
- 予約済みの VLAN は使用できません。
- VLAN 1 は使用できません。
- 同一スイッチ シャーシ内で FWSM フェールオーバーを使用する場合は、フェールオーバーおよびステータスフル通信のために確保してある VLAN (複数可) をスイッチ ポートに割り当てないでください。ただし、シャーシ間でフェールオーバーを使用する場合は、シャーシ間を結ぶトランク ポートに VLAN を組み込む必要があります。
- FWSM に VLAN を割り当てる前に、スイッチに VLAN を追加しなかった場合、VLAN はスーパーバイザ エンジンのデータベースに保管され、スイッチに追加された時点で FWSM に送信されます。

FWSM への VLAN の割り当て

Cisco IOS ソフトウェアでは、ファイアウォール VLAN グループを 16 個まで作成して FWSM に割り当てます。たとえば、すべての VLAN を 1 つのグループに割り当てる、内部グループと外部グループを作成する、またはカスタマーごとにグループを 1 つずつ作成するといったことが可能です。各グループには、VLAN を制限なく割り当てることができます。

同じ VLAN を複数のファイアウォール グループに割り当てることはできませんが、1 つの FWSM への複数のファイアウォール グループの割り当てと複数の FWSM への 1 つのファイアウォール グループの割り当ては可能です。たとえば、複数の FWSM に割り当てる VLAN は、それぞれの FWSM に一意の VLAN とは別のグループに配置できます。

VLAN を FWSM に割り当てる手順は、次のとおりです。

ステップ 1 次のコマンドを入力して、ファイアウォール グループに VLAN を割り当てます。

```
Router(config)# firewall vlan-group firewall_group vlan_range
```

firewall_group 引数には、整数値を指定します。

vlan_range には、次のいずれかの形式で 1 つまたは複数の VLAN (2 ~ 1000 および 1025 ~ 4094) を指定できます。

- 個別の番号 (*n*)
- 範囲 (*n-x*)

番号または範囲はカンマで区切ります。番号の入力例を示します。

```
5,7-10,13,45-100
```



(注)

ルーテッドポートと WAN ポートは内部 VLAN を使用するため、1020 ~ 1100 の範囲に含まれる番号は、すでに使用されている可能性があります。

VLAN を FWSM コンフィギュレーションで設定し、後でこの手順を使用して、VLAN をスイッチの FWSM に割り当てる場合、これらの VLAN は、シャットダウンするように設定されている場合でも、FWSM では管理上アップ状態になります。これらの VLAN をシャットダウンするには、FWSM の CLI で次のコマンドを入力します。

```
interface vlan number  
shutdown
```

ステップ 2 次のコマンドを入力して、FWSM にファイアウォール グループを割り当てます。

```
Router(config)# firewall module module_number vlan-group firewall_group
```

firewall_group は 1 つまたは複数のグループ番号です。

- 個別の番号 (*n*)
- 範囲 (*n-x*)

番号または範囲はカンマで区切ります。番号の入力例を示します。

```
5,7-10
```

次に、3 つのファイアウォール VLAN グループ (各 FWSM 用のグループおよび両方の FWSM に割り当てられた VLAN を含むグループ) を作成する例を示します。

```
Router(config)# firewall vlan-group 50 55-57  
Router(config)# firewall vlan-group 51 70-85  
Router(config)# firewall vlan-group 52 100  
Router(config)# firewall module 5 vlan-group 50,52  
Router(config)# firewall module 8 vlan-group 51,52
```

次に、**show firewall vlan-group** コマンドの出力例を示します。

```
Router# show firewall vlan-group
Group vlans
-----
 50 55-57
 51 70-85
 52 100
```

次に、すべての VLAN グループを示す **show firewall module** コマンドの出力例を示します。

```
Router# show firewall module
Module Vlan-groups
 5      50,52
 8      51,52
```

MSFC へのスイッチ仮想インターフェイスの追加

MSFC 上で定義された VLAN を Switch Virtual Interface (SVI; スイッチ仮想インターフェイス) といいます。FWSM に SVI 用の VLAN を割り当てると (「[ファイアウォール サービス モジュールへの VLAN の割り当て](#)」(P.2-4) を参照)、MSFC は FWSM と他のレイヤ 3 VLAN 間のルーティングを行います。

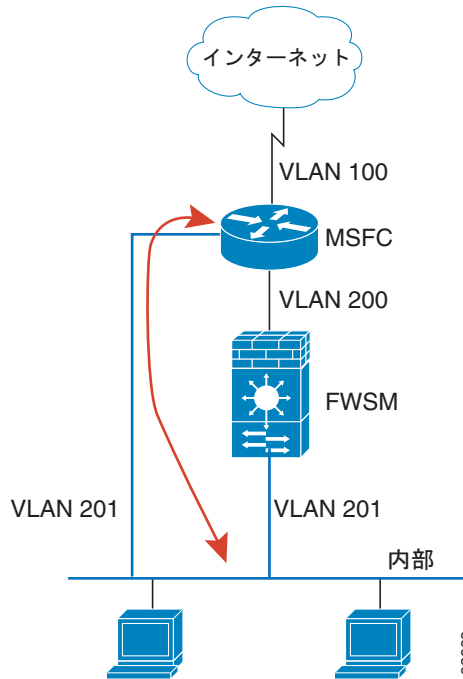
ここでは、次の内容について説明します。

- 「[SVI の概要](#)」(P.2-7)
- 「[複数の SVI の設定](#)」(P.2-9)

SVI の概要

セキュリティ上の理由から、デフォルトでは MSFC と FWSM 間に配置できる SVI は 1 つだけです。たとえば、誤って複数の SVI をシステムに設定した場合は、MSFC に内部 VLAN と外部 VLAN の両方が割り当てられていることによって、トラフィックが偶発的に FWSM をバイパスする可能性があります (図 2-1 を参照)。

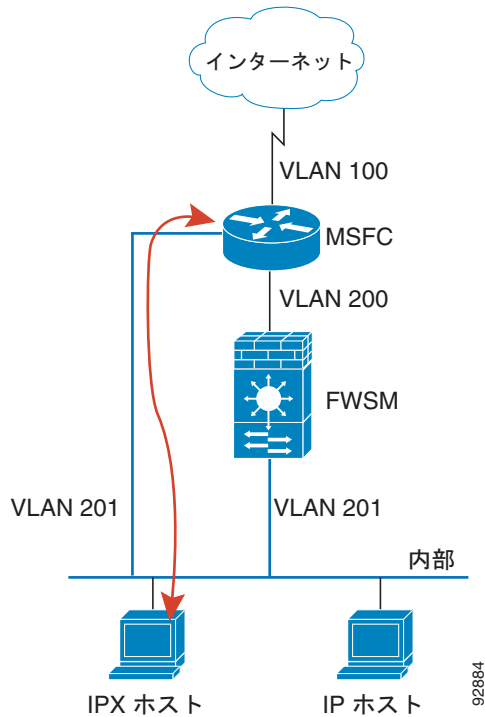
図 2-1 誤設定による複数の SVI



ただし、ネットワーク シナリオの中には、FWSM をバイパスする必要があるものもあります。図 2-2 に、IP ホストと同じイーサネット セグメント上にある IPX ホストを示します。ルーテッドファイアウォールモードの FWSM は IP トラフィックしか処理せず、IPX などの他のプロトコルトラフィックを廃棄するため (トランスペアレント ファイアウォールモードでは IP 以外のトラフィックの通過が任

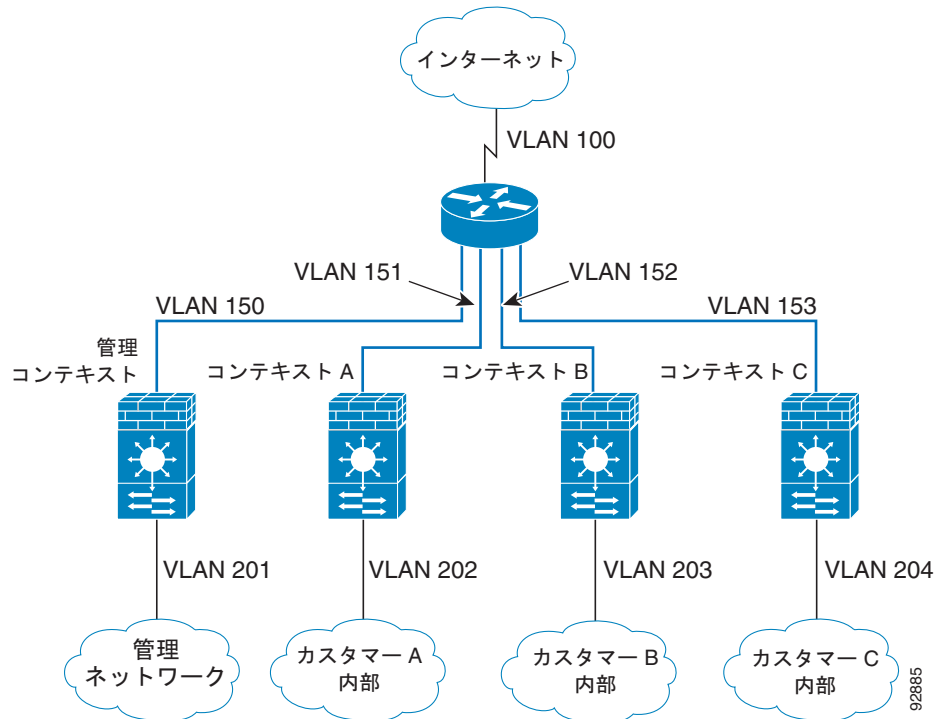
意に許可されます)、IPX トラフィックで FWSM をバイパスする必要があります。この場合は、必ず VLAN 201 を通過できるのが IPX トラフィックに限定されるアクセスリストを使用して MSFC を設定してください。

図 2-2 IPX 対応の複数の SVI



トランスペアレント ファイアウォールがマルチコンテキスト モードの場合、コンテキストごとに対応する外部インターフェイス上に固有の VLAN が必要なので、複数の SVI を使用する必要があります (図 2-3 を参照)。ルーテッド モードの場合でも複数の SVI を使用できるので、外部インターフェイス用に 1 つの VLAN を共有する必要はありません。

図 2-3 マルチコンテキスト モードでの複数の SVI



複数の SVI の設定

MSFC に SVI を追加する手順は、次のとおりです。

-
- ステップ 1** (任意) 次のコマンドを入力して、FWSM に複数の SVI を追加できるようにします。
- ```
Router(config)# firewall multiple-vlan-interfaces
```
- ステップ 2** 次のコマンドを入力して、MSFC に VLAN インターフェイスを追加します。
- ```
Router(config)# interface vlan vlan_number
```
- ステップ 3** 次のコマンドを入力して、MSFC 上でこのインターフェイスに対応する IP アドレスを設定します。
- ```
Router(config-if)# ip address address mask
```
- ステップ 4** 次のコマンドを入力して、インターフェイスをイネーブルにします。
- ```
Router(config-if)# no shutdown
```
-

次に、複数の SVI を使用する一般的な設定例を示します。

```
Router(config)# firewall vlan-group 50 55-57
Router(config)# firewall vlan-group 51 70-85
Router(config)# firewall module 8 vlan-group 50-51
Router(config)# firewall multiple-vlan-interfaces
Router(config)# interface vlan 55
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# interface vlan 56
Router(config-if)# ip address 10.1.2.1 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# end
Router#
```

次に、**show interface** コマンドの出力例を示します。

```
Router# show interface vlan 55
Vlan55 is up, line protocol is up
  Hardware is EtherSVI, address is 0008.20de.45ca (bia 0008.20de.45ca)
  Internet address is 10.1.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type:ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:08, output hang never
  Last clearing of "show interface" counters never
  Input queue:0/75/0/0 (size/max/drops/flushes); Total output drops:0
  Queueing strategy:fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
  L2 Switched:ucast:196 pkt, 13328 bytes - mcast:4 pkt, 256 bytes
  L3 in Switched:ucast:0 pkt, 0 bytes - mcast:0 pkt, 0 bytes mcast
  L3 out Switched:ucast:0 pkt, 0 bytes
    0 packets input, 0 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  4 packets output, 256 bytes, 0 underruns
  0 output errors, 0 interface resets
  0 output buffer failures, 0 output buffers swapped out
```

FWSM の内部インターフェイスのカスタマイズ

FWSM とスイッチ間の接続は 6 GB の 802.1Q トランキンク EtherChannel です。この EtherChannel は、FWSM を搭載した時点で自動的に作成されます。FWSM 側では、2 つの NP がそれぞれ 3 つのギガビットイーサネットインターフェイスに接続され、これらのインターフェイスが EtherChannel を形成します。スイッチはセッション情報に基づき、分散アルゴリズムに従って EtherChannel 内のインターフェイスにトラフィックを分散させます。負荷分散はパケット単位ではなく、フロー単位で行われます。アルゴリズムがインターフェイス間、したがって 2 つの NP 間でトラフィックを均等に割り当てない場合もあります。恒常的な不均衡は、FWSM の処理能力がフル活用されないだけでなく、複数のコンテキストにリソース管理を適用したときに予想外の動作を引き起こす可能性があります（詳細については、「[クラスの設定](#)」(P.4-25) を参照してください)。

負荷分散方式を変更するには、次のコマンドを入力します。

```
Router(config)# port-channel load-balance {dst-ip | dst-mac | dst-port | src-dst-ip |
src-dst-mac | src-dst-port | src-ip | src-mac | src-port}
```

デフォルトは `src-dst-ip` です。

フェールオーバーを使用するためのスイッチの設定

フェールオーバー対応としてスイッチを設定する場合は、次の項を参照してください。

- 「セカンダリファイアウォール サービス モジュールへの VLAN の割り当て」(P.2-11)
- 「プライマリ スイッチとセカンダリ スイッチ間のトランクの追加」(P.2-11)
- 「トランスペアレント ファイアウォール モードとの両立」(P.2-11)
- 「高速リンク障害検出のための自動ステート メッセージングのイネーブル化」(P.2-11)

セカンダリファイアウォール サービス モジュールへの VLAN の割り当て

両方の装置が同じように内部ネットワークと外部ネットワークにアクセスできる必要があるため、スイッチ上の両方の FWSM に同じ VLAN を割り当てる必要があります。「ファイアウォール サービス モジュールへの VLAN の割り当て」(P.2-4) を参照してください。

プライマリ スイッチとセカンダリ スイッチ間のトランクの追加

スイッチ間フェールオーバーを使用している場合（「シャーシ内およびシャーシ間のモジュール配置」(P.14-3) を参照）、2 つのスイッチ間に 802.1Q VLAN トランクを設定してフェールオーバーとステートリンクを処理する必要があります。CoS 値が 5（ハイ プライオリティ）のフェールオーバー VLAN パケットがこれらのポートでハイ プライオリティとして処理されるように、トランクで QoS（Quality Of Service）をイネーブルにしておく必要があります。

EtherChannel とトランクの設定については、スイッチのマニュアルを参照してください。

トランスペアレント ファイアウォール モードとの両立

トランスペアレント モードでフェールオーバーを使用した場合にループが発生しないように、Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) の転送をサポートするスイッチ ソフトウェアを使用してください。トランスペアレント ファイアウォール モードでのスイッチのサポートの詳細については、「スイッチ ハードウェアおよびソフトウェアの互換性」(P.A-1) を参照してください。

FWSM がトランスペアレント モードの場合、スイッチでグローバルに LoopGuard をイネーブルにしないでください。LoopGuard は、スイッチと FWSM 間の内部 EtherChannel に自動的に適用されます。そのため、フェールオーバーおよびフェールバック後、EtherChannel がエラー ディセーブル ステートになるため、LoopGuard によりセカンダリ ユニットが切断されます。

高速リンク障害検出のための自動ステート メッセージングのイネーブル化

Cisco IOS ソフトウェア Release 12.2(18)SXF5 以降を使用している場合は、FWSM の VLAN に関連付けられた物理インターフェイスのステータスに関する自動ステート メッセージをスーパーバイザ エンジンから FWSM に送信できます。たとえば、VLAN に関連付けられたすべての物理インターフェイスが停止すると、VLAN が停止したことを示す自動ステート メッセージが FWSM に届きます。この情報に基づいて FWSM は VLAN が停止していると判断できます。この場合は、いずれの側でリンク

障害が発生したかを判別するのに必要となるインターフェイス モニタリング テストが回避されます。自動ステート メッセージングにより、FWSM がリンク障害を検出するのに要する時間が大幅に短縮されます（自動ステートがサポートされていない場合の最長 45 秒と比較すると、数ミリ秒も短縮されます）。

次の場合に、スイッチのスーパーバイザから FWSM に自動ステート メッセージが送信されます。

- VLAN に属している最後のインターフェイスが停止した
- VLAN に属している最初のインターフェイスが動作を開始した



(注)

スイッチで自動ステート メッセージングがサポートされるのは、シャーシに 1 つの FWSM を搭載した場合だけです。

デフォルトでは、自動ステート メッセージングはディセーブルになっています。Cisco IOS ソフトウェアで自動ステート メッセージングをイネーブルにするには、次のコマンドを入力します。

```
Router (config)# firewall autostate
```

ファイアウォール サービス モジュールのブートパーティションの管理

ここでは、スイッチから FWSM をリセットする方法とフラッシュ メモリ カード上のブートパーティションを管理する方法について説明します。ここでは、次の内容について説明します。

- 「フラッシュ メモリの概要」 (P.2-12)
- 「デフォルト ブートパーティションの設定」 (P.2-13)
- 「FWSM のリセットまたは特定のパーティションからの起動」 (P.2-13)

フラッシュ メモリの概要

FWSM には、OS、コンフィギュレーション、およびその他のデータを保管する 128 MB のフラッシュ メモリ カードが装備されています。フラッシュ メモリには 6 つのパーティションがあります。Cisco IOS ソフトウェアのコマンドでは、**cf:n** で指定します。

- メンテナンス パーティション (**cf:1**) : メンテナンス ソフトウェアが格納されています。メンテナンス ソフトウェアを使用して、アプリケーション パーティションの起動ができない場合に、アプリケーション イメージをアップグレードまたはインストールしたり、アプリケーション イメージのパスワードをリセットしたり、クラッシュ ダンプ情報を表示したりします。
- ネットワーク コンフィギュレーション パーティション (**cf:2**) : メンテナンス ソフトウェアのネットワーク コンフィギュレーションが格納されています。FWSM が TFTP サーバにアクセスしてアプリケーション ソフトウェア イメージをダウンロードできるように、メンテナンス ソフトウェアには IP の設定値が必要となります。
- クラッシュ ダンプ パーティション (**cf:3**) : クラッシュ ダンプ情報が格納されています。
- アプリケーション パーティション (**cf:4** および **cf:5**) : アプリケーション ソフトウェア イメージ、システム コンフィギュレーション、および ASDM が格納されています。デフォルトで、イメージは **cf:4** にインストールされます。**cf:5** はテスト パーティションとして使用できます。たとえば、

ソフトウェアをアップグレードする場合は、新しいソフトウェアを **cf:5** にインストールできますが、問題発生時のバックアップとして旧ソフトウェアを維持しておくこともできます。各パーティションには独自のスタートアップ コンフィギュレーションが設定されています。

- セキュリティ コンテキスト パーティション (**cf:6**) : このパーティション専用として 64 MB が確保されます。セキュリティ コンテキスト コンフィギュレーション (必要な場合) と RSA キーがナビゲーション可能なファイル システムに保管されます。他のパーティションには、ファイルのリスト表示などの一般的な作業を実行できるファイル システムはありません。 **copy** コマンドの使用時には、このパーティションは **ディスク** と呼ばれます。

デフォルト ブート パーティションの設定

FWSM はデフォルトで **cf:4** アプリケーション パーティションから起動します。**cf:5** アプリケーション パーティションからの起動または **cf:1** メンテナンス パーティションへの起動を選択することもできます。アプリケーション パーティションごとに独自のスタートアップ コンフィギュレーションがあります。

デフォルトのブート パーティションを変更するには、次のコマンドを入力します。

```
Router(config)# boot device module mod_num cf:n
```

n は 1 (メンテナンス)、4 (アプリケーション)、または 5 (アプリケーション) です。

現在のブート パーティションを表示するには、次のコマンドを入力します。

```
Router# show boot device [mod_num]
```

次に例を示します。

```
Router# show boot device
[mod:1 ]:
[mod:2 ]:
[mod:3 ]:
[mod:4 ]: cf:4
[mod:5 ]: cf:4
[mod:6 ]:
[mod:7 ]: cf:4
[mod:8 ]:
[mod:9 ]:
```

FWSM のリセットまたは特定のパーティションからの起動

ここでは、FWSM をリセットする方法または特定のパーティションから起動する方法について説明します。CLI または外部 Telnet セッションから FWSM にアクセスできない場合は、FWSM のリセットが必要となります。メンテナンス パーティションにアクセスしなければならない場合、またはバックアップのアプリケーション パーティションに保管されている別のソフトウェア イメージから起動しなければならない場合は、デフォルト以外のブート パーティションからの起動が必要になります。メンテナンス パーティションは、トラブルシューティング時に役立ちます。

リセットすると、完了までに数分間かかることがあります。

FWSM をリセットする場合は、フルメモリ テストの実行を選択することもできます。FWSM の初回起動時には、部分的なメモリ テストが実行されるだけです。フルメモリ テストには、6 分ほどかかります。



(注)

FWSM へのログイン時に FWSM をリロードする場合は、**reload** コマンドまたは **reboot** コマンドを入力します。これらのコマンドでは、デフォルト以外のブートパーティションから起動できません。

FWSM をリセットするには、次のコマンドを入力します。

```
Router# hw-module module mod_num reset [cf:n] [mem-test-full]
```

cf:n 引数はパーティションであり、1 (メンテナンス)、4 (アプリケーション)、または 5 (アプリケーション) のいずれかになります。パーティションを指定しないと、デフォルトのパーティションが使用されます (通常は **cf:4**)。

mem-test-full オプションを指定すると、フルメモリ テストが実行されます。所要時間は約 6 分です。

次に、スロット 9 に搭載された FWSM をリセットする例を示します。デフォルトのブートパーティションが使用されます。

```
Router# hw-module module 9 reset
```

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

```
Router#
00:26:55:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
00:26:55:SP:The PC in slot 8 is shutting down. Please wait ...
```