CHAPTER 6

インターフェイス パラメータの設定

この章では、各インターフェイスに名前、セキュリティ レベル、IP アドレスを設定する方法について説明します。さらにトランスペアレント ファイアウォールでは、各インターフェイスのペアにブリッジ グループの設定が必要です。

この章では、次の内容について説明します。

セキュリティ レベルの概要

各インターフェイスに 0（最下位）～ 100（最上位）のセキュリティ レベルを設定する必要があります。たとえば、内部ホスト ネットワークなど、最もセキュアなネットワークにはレベル 100 を割り当てる必要があります。一方、インターネットなどに接続する外部ネットワークにはレベル 0 が割り当てられる場合があります。DMZ など、その他のネットワークはその中間に設定できます。複数のインターフェイスを同じセキュリティ レベルに割り当てることができます。詳細については、「同一セキュリティ レベルのインターフェイス間の通信の許可」（P.6-10）を参照してください。

レベルによって、次の動作が制御されます。

- インスペクション エンジン：一部のインスペクション エンジンは、セキュリティ レベルに依存します。同じセキュリティ レベルのインターフェイス間では、インスペクション エンジンは発信と着信のいずれのトラフィックに対しても適用されます。
  - NetBIOS インスペクション エンジン：発信接続に対してのみ適用されます。
  - OraServ インスペクション エンジン：ホストのペア間に OraServ ポートへの制御接続が存在する場合は、FWSM 経由での着信データ接続のみが許可されます。
- フィルタリング：HTTP(S) および FTP フィルタリングは発信接続にだけ適用されます。同じセキュリティ レベルのインターフェイス間では、発信と着信のいずれのトラフィックもフィルタリングできます。
- NAT コントロール：NAT コントロールをイネーブルにする場合、高いセキュリティ レベルのインターフェイス（内部）上のホストから低いセキュリティ レベルのインターフェイス（外部）上のホストにアクセスするときは、内部インターフェイスのホストに NAT を設定する必要があります。

NAT コントロールをイネーブルにしない場合、または同じセキュリティ レベルのインターフェイス間においては、任意のインターフェイス間で NAT を使用することも、使用しないこともできます。外部インターフェイスに NAT を設定する場合は、特別なキーワードが必要になることがあります。

- **established** コマンド：このコマンドを使用すると、高いレベルのホストから低いレベルのホストへの接続がすでに確立されている場合、低いセキュリティ レベルのホストから高いセキュリティ レベルのホストへの戻り接続が許可されます。

  同一セキュリティ レベルのインターフェイス間の通信をイネーブルにする場合（「同一セキュリティ レベルのインターフェイス間の通信の許可」（P.6-10）を参照）、双方向に **established** コマンドを設定できます。

ルーテッド ファイアウォール モードのインターフェイスの設定

ここでは、次の内容について説明します。

注意事項および制約事項

インターフェイスを設定する場合は、次のガイドラインを参照してください。

マルチ コンテキスト モードのガイドライン

- 設定できるのは、**allocate-interface** コマンドを使用してシステム コンフィギュレーションでコンテキストにすでに割り当てられているコンテキスト インターフェイスだけです。
- システム実行スペース内でのインターフェイスの状態にかかわらず、すべての割り当て済みのインターフェイスがデフォルトでイネーブルになっています。ただし、トラフィックがインターフェイスを通過するためには、そのインターフェイスもシステム実行スペース内でイネーブルになっている必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。「インターフェイスのオン / オフ」（P.6-12）を参照してください。
- 各コンテキスト内からコンテキスト インターフェイスを設定します。
- システム コンフィギュレーションでフェールオーバー インターフェイスを設定します。フェールオーバー インターフェイスは、この手順で設定しないでください。詳細については、第 14 章「フェールオーバーの設定」を参照してください。

VLAN ID に関するガイドライン

コンフィギュレーションにはあらゆる VLAN ID を追加できますが、トラフィックを転送できるのはスイッチによって FWSM に割り当てられた VLAN だけです。**show vlan** コマンドを使用して、FWSM に割り当てられたすべての VLAN を表示します。

スイッチによって FWSM にまだ割り当てられていない VLAN にインターフェイスを追加した場合、そのインターフェイスはダウン ステートになります。FWSM に VLAN を割り当てた時点で、インターフェイスはアップ ステートに変化します。インターフェイス ステートの詳細については、**show interface** コマンドを参照してください。

フェールオーバー ガイドライン

フェールオーバーを使用している場合は、フェールオーバー通信およびステートフル フェールオーバー通信に予約されているインターフェイスには、この方法で名前を付けないでください。フェールオーバーおよびステート リンクの設定については、第 14 章「フェールオーバーの設定」を参照してください。

インターフェイスの設定

トラフィックに FWSM の通過を許可するには、事前にインターフェイス名と IP アドレスを設定しておく必要があります。また、セキュリティ レベルをデフォルトの 0 から変更する必要があります。インターフェイスに名前「inside」を付けて、明示的にセキュリティ レベルを設定しないと、FWSM はセキュリティ レベルを 100 に設定します。

インターフェイスを設定する手順は、次のとおりです。

ステップ 1　設定するインターフェイスを指定するには、次のコマンドを入力します。

```
hostname(config)# interface {vlan number | mapped_name}
```

マルチコンテキスト モードの場合、マップ名が **allocate-interface** コマンドを使用して割り当てられていれば、そのマップ名を入力します。

たとえば、次のコマンドを入力します。

```
hostname(config)# interface vlan 101
```

ステップ 2　インターフェイスに名前を付けるには、次のコマンドを入力します。

```
hostname(config-if)# nameif name
```

name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。その名前を参照するすべてのコマンドが削除されるため、**no** 形式は入力しないでください。

（注）　インターフェイスの名前を設定すると、セキュリティ レベルは自動的に 0 に変更されます。ただし、名前が「内部」の場合、セキュリティ レベルは 100 になります。

ステップ 3　次のコマンドを入力して、セキュリティ レベルを設定します。

```
hostname(config-if)# security-level number
```

number には、0（最下位）～ 100（最上位）の整数を指定します。

インターフェイスのセキュリティ レベルを変更する場合、既存の接続がタイムアウトするのを待たずに新しいセキュリティ情報を使用するときは、**clear local-host** コマンドを使用して接続をクリアできます。

ステップ 4　次のコマンドを入力して、IP アドレスを設定します。

```
hostname(config-if)# ip address ip_address [mask] [standby ip_address]
```

フェールオーバーには、**standby** キーワードとアドレスを使用します。詳細については、第 14 章「フェールオーバーの設定」を参照してください。

（注）　IPv6 アドレスの設定については、「インターフェイス上での IPv6 の設定」（P.10-2）を参照してください。

次に、VLAN 101 のパラメータの設定例を示します。

```
hostname(config)# interface vlan 101
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
```

次に、マルチコンテキスト モードでコンテキスト コンフィギュレーションにパラメータを設定する例を示します。インターフェイス ID はマップ名です。

```
hostname/contextA(config)# interface int1
hostname/contextA(config-if)# nameif outside
hostname/contextA(config-if)# security-level 100
hostname/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
```

トランスペアレント ファイアウォール モードのインターフェイスの設定

ここでは、次の内容について説明します。

- 「トランスペアレント モードのインターフェイスの概要」（P.6-4）
- 「通過するトラフィックのトランスペアレント ファイアウォール インターフェイスの設定」（P.6-6）
- 「IP アドレスのブリッジ グループへの割り当て」（P.6-7）
- 「管理インターフェイスの追加」（P.6-8）

トランスペアレント モードのインターフェイスの概要

ここでは、次の内容について説明します。

- 「ブリッジ グループの概要」（P.6-5）
- 「デバイス管理の概要」（P.6-5）
- 「注意事項および制約事項」（P.6-5）

ブリッジ グループの概要

トランスペアレント ファイアウォールは、その内部インターフェイスと外部インターフェイスで同じネットワークを接続します。インターフェイスの各ペアは、ブリッジ グループに属します。ブリッジ グループには、管理 IP アドレスを割り当てる必要があります。2 つのインターフェイスそれぞれの最大 8 つのブリッジ グループを設定できます。各ブリッジ グループは、別々のネットワークに接続します。ブリッジ グループのトラフィックは他のブリッジ グループから隔離され、トラフィックは FWSM 内の他のブリッジ グループにはルーティングされません。また、トラフィックは外部ルータから FWSM 内の他のブリッジ グループにルーティングされる前に、FWSM から出る必要があります。

セキュリティ コンテキストのオーバーヘッドを防ぐ場合、またはセキュリティ コンテキストの使用を最大限にする場合、複数のブリッジ グループを使用することがあります。ブリッジング機能はブリッジ グループごとに分かれていますが、その他の多くの機能はすべてのブリッジ グループ間で共有されます。たとえば、すべてのブリッジ グループはシステム ログ サーバまたは AAA サーバのコンフィギュレーションを共有します。セキュリティ ポリシーを完全に分離するには、各コンテキスト内に 1 つのブリッジ グループにして、セキュリティ コンテキストを使用します。

（注） FWSM では、セカンダリ ネットワーク上のトラフィックはサポートされていません。管理 IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。

デバイス管理の概要

デバイス管理については、次のメカニズムを使用できます。

- 任意のブリッジ グループ管理アドレス：管理ステーションがあるブリッジ グループ ネットワークに接続します。
- 個別の管理インターフェイス：管理インターフェイスは、どのブリッジ グループにも属しません。このインターフェイスは、特に、マルチ コンテキストでシングル管理インターフェイスを共有できるマルチ コンテキスト モードで役に立ちます。

  管理インターフェイスについては、次のガイドラインを参照してください。

  - シングル モードまたはコンテキストごとに使用できる管理インターフェイスは 1 つだけです。各コンテキストで管理インターフェイスを 1 つだけ使用する限り、コンテキストによって異なるインターフェイスを使用できます。
  - 管理インターフェイス IP アドレスは、任意のブリッジ グループ ネットワークとは別のネットワークのものも、ブリッジ グループ ネットワークと同じネットワークのものも使用できます。
  - マルチ コンテキストでインターフェイスを共有する場合、インターフェイス IP アドレスは、各コンテキストで同じネットワークになければなりません。
  - 管理 VLAN は、マルチ トランスペアレント コンテキストのみで共有できます。この VLAN は、ルーテッド コンテキストと共有できません。

注意事項および制約事項

インターフェイスを設定する場合は、次のガイドラインを参照してください。

マルチ コンテキスト モードのガイドライン

- 設定できるのは、**allocate-interface** コマンドを使用してシステム コンフィギュレーションでコンテキストにすでに割り当てられているコンテキスト インターフェイスだけです。

- システム実行スペース内でのインターフェイスの状態にかかわらず、すべての割り当て済みのインターフェイスがデフォルトでイネーブルになっています。ただし、トラフィックがインターフェイスを通過するためには、そのインターフェイスもシステム実行スペース内でイネーブルになっている必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。
- 各コンテキスト内からコンテキスト インターフェイスを設定します。
- システム コンフィギュレーションでフェールオーバー インターフェイスを設定します。フェールオーバー インターフェイスは、この手順で設定しないでください。詳細については、第 14 章「フェールオーバーの設定」を参照してください。

VLAN ID に関するガイドライン

コンフィギュレーションにはあらゆる VLAN ID を追加できますが、トラフィックを転送できるのはスイッチによって FWSM に割り当てられた VLAN だけです。**show vlan** コマンドを使用して、FWSM に割り当てられたすべての VLAN を表示します。

スイッチによって FWSM にまだ割り当てられていない VLAN にインターフェイスを追加した場合、そのインターフェイスはダウン ステートになります。FWSM に VLAN を割り当てた時点で、インターフェイスはアップ ステートに変化します。インターフェイス ステートの詳細については、**show interface** コマンドを参照してください。

フェールオーバー ガイドライン

フェールオーバーを使用している場合は、フェールオーバー通信およびステートフル フェールオーバー通信に予約されているインターフェイスには、この方法で名前を付けないでください。フェールオーバーおよびステート リンクの設定については、第 14 章「フェールオーバーの設定」を参照してください。

通過するトラフィックのトランスペアレント ファイアウォール インターフェイスの設定

インターフェイスをブリッジ グループに割り当てて、名前とセキュリティ レベルを設定する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、インターフェイスを識別します。

```
hostname(config)# interface {vlan number | mapped_name}
```

マルチコンテキスト モードの場合、マップ名が **allocate-interface** コマンドを使用して割り当てられていれば、そのマップ名を入力します。

ステップ 2　次のコマンドを入力して、インターフェイスをブリッジ グループに割り当てます。

```
hostname(config-if)# bridge-group number
```

number は、1 ～ 100 の整数です。1 つのブリッジ グループには 2 つのインターフェイスしか割り当てることができません。同一インターフェイスを複数のブリッジ グループに割り当てることはできません。

ステップ 3　インターフェイスに名前を付けるには、次のコマンドを入力します。

```
hostname(config-if)# nameif name
```

name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。その名前を参照するすべてのコマンドが削除されるため、**no** 形式は入力しないでください。インターフェイスに名前「inside」を付けて、明示的にセキュリティ

レベルを設定しないと、FWSM はセキュリティ レベルを 100 に設定します。

ステップ 4　次のコマンドを入力して、セキュリティ レベルを設定します。

```
hostname(config-if)# security-level number
```

number には、0（最下位）～ 100（最上位）の整数を指定します。デフォルトでは、インターフェイスに名前を付けると、セキュリティ レベルは FWSM によって 0 に設定されます。

IP アドレスのブリッジ グループへの割り当て

トランスペアレント ファイアウォールは、IP ルーティングに参加しません。FWSM に必要な IP 設定は、各ブリッジ グループに管理 IP アドレスを設定することだけです。このアドレスが必要なのは、FWSM がシステム ログ メッセージ、AAA サーバとの通信など、FWSM が発信元となるトラフィックの送信元アドレスとしてこのアドレスを使用するからです。リモート管理アクセスにこのアドレスを使用することもできます（FWSM を別の方法で管理するには、「管理インターフェイスの追加」（P.6-8）を参照してください）。

管理 IP アドレスを設定する手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、ブリッジ グループを識別します。

```
hostname(config)# interface bvi bridge_group_number
```

ステップ 2　次のコマンドを入力して、IP アドレスを指定します。

```
hostname(config-if)# ip address ip_address [mask] [standby ip_address]
```

トランスペアレント ファイアウォールにホスト アドレス（/32 または 255.255.255.255）を割り当てないでください。また、/30 サブネットなど（255.255.255.252）、ホスト アドレスが 3 つ未満（アップストリーム ルータ、ダウンストリーム ルータ、トランスペアレント ファイアウォールにそれぞれ 1 つずつ）の他のサブネットを使用しないでください。FWSM は、サブネットの先頭アドレスと最終アドレスとの間で送受信されるすべての ARP パケットをドロップします。このため、/30 サブネットを使用し、このサブネットからアップストリーム ルータに予約済みアドレスを割り当てると、FWSM はダウンストリーム ルータからアップストリーム ルータへの ARP 要求を廃棄します。

FWSM では、セカンダリ ネットワーク上のトラフィックはサポートされていません。管理 IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。

フェールオーバーには、**standby** キーワードとアドレスを使用します。詳細については、第 14 章「フェールオーバーの設定」を参照してください。

次に、VLAN 300 および 301 をブリッジ グループ 1 に割り当てて、ブリッジ グループ 1 の管理アドレスおよびスタンバイ アドレスを設定する例を示します。

```
hostname(config)# interface vlan 300
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# bridge-group 1

hostname(config-if)# interface vlan 301
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# bridge-group 1

hostname(config-if)# interface bvi 1
```

```
hostname(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
```

管理インターフェイスの追加

各ブリッジ グループ管理 IP アドレスのほか、どのブリッジ グループにも属さず、FWSM への管理トラフィックのみを許可する別個の管理インターフェイスを追加できます。詳細については、「デバイス管理の概要」（P.6-5）を参照してください。

管理インターフェイスを設定するには、次の手順を実行します。

ステップ 1　設定するインターフェイスを指定するには、次のコマンドを入力します。

```
hostname(config)# interface {vlan number | mapped_name}
```

マルチコンテキスト モードの場合、マップ名が **allocate-interface** コマンドを使用して割り当てられていれば、そのマップ名を入力します。

たとえば、次のコマンドを入力します。

```
hostname(config)# interface vlan 101
```

ステップ 2　インターフェイスに名前を付けるには、次のコマンドを入力します。

```
hostname(config-if)# nameif name
```

name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。その名前を参照するすべてのコマンドが削除されるため、**no** 形式は入力しないでください。

ステップ 3　次のコマンドを入力して、セキュリティ レベルを設定します。

```
hostname(config-if)# security-level 100
```

このインターフェイスは、レベル 100 に設定する必要があります。

ステップ 4　次のコマンドを入力して、IP アドレスを設定します。

```
hostname(config-if)# ip address ip_address [mask] [standby ip_address]
```

フェールオーバーには、**standby** キーワードとアドレスを使用します。詳細については、第 14 章「フェールオーバーの設定」を参照してください。

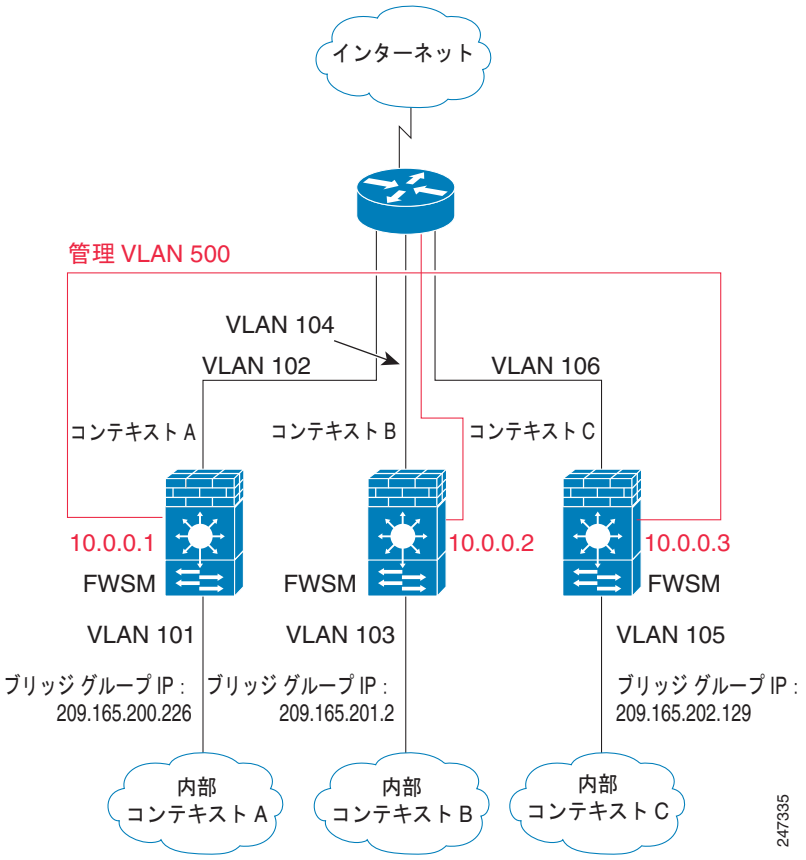
ステップ 5　このインターフェイスを management-only に設定するには、次のコマンドを入力します。

```
hostname(config-if)# management-only
```

このコマンドは必須です。**management-only** コマンドを使用しないインターフェイスは無視されます。

次に、それぞれにブリッジ グループが 1 つある 3 つのコンテキストと共有管理 VLAN のインターフェイスを設定する例を示します（図 6-1 を参照）。

図 6-1　　共有管理 VLAN



コンテキスト A

```
hostname(config)# interface vlan500
hostname(config-if)# nameif mgmt
hostname(config-if)# security-level 0
hostname(config-if)# management-only
hostname(config-if)# ip address 10.0.0.1 255.0.0.0

hostname(config-if)# interface vlan101
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# bridge-group 10

hostname(config-if)# interface vlan102
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# bridge-group 10

hostname(config-if)# interface bvi 10
hostname(config-if)# ip address 209.165.200.226 255.255.255.224
```

コンテキスト B

```
hostname(config)# interface vlan500
hostname(config-if)# nameif mgmt
hostname(config-if)# security-level 0
hostname(config-if)# management-only
hostname(config-if)# ip address 10.0.0.2 255.0.0.0

hostname(config-if)# interface vlan103
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# bridge-group 20

hostname(config-if)# interface vlan104
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# bridge-group 20

hostname(config-if)# interface bvi 20
hostname(config-if)# ip address 209.165.201.2 255.255.255.224
```

コンテキスト C

```
hostname(config)# interface vlan500
hostname(config-if)# nameif mgmt
hostname(config-if)# security-level 0
hostname(config-if)# management-only
hostname(config-if)# ip address 10.0.0.3 255.0.0.0

hostname(config-if)# interface vlan105
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# bridge-group 30

hostname(config-if)# interface vlan106
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# bridge-group 30

hostname(config-if)# interface bvi 30
hostname(config-if)# ip address 209.165.202.129 255.255.255.224
```

同一セキュリティ レベルのインターフェイス間の通信の許可

デフォルトでは、NAT とアクセス リストを設定しても、同一セキュリティ レベルのインターフェイスは相互に通信できません。また、デフォルトでは、トラフィックは同一インターフェイスに入って出ることはできません。ここでは、インターフェイス間通信およびインターフェイス内通信を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。

インターフェイス間通信の設定

同一セキュリティ レベルのインターフェイス間での通信を許可すると、101 を超える通信インターフェイスを設定できます。各インターフェイスで異なるセキュリティ レベルを使用したときに、同一のセキュリティ レベルにインターフェイスを割り当てないと、各レベル（0 ～ 100）に 1 つのインターフェイスしか設定できません。

（注） NAT 制御をイネーブルにする場合、同一セキュリティ レベルのインターフェイス間では NAT を設定する必要がありません。NAT および同一セキュリティ レベルのインターフェイスの詳細については、「NAT および同一セキュリティ レベルのインターフェイス」（P.16-15）を参照してください。

同じセキュリティ インターフェイス通信をイネーブルにした場合でも、異なるセキュリティ レベルで通常どおりインターフェイスを設定できます。

同一セキュリティ レベルのインターフェイスが相互に通信できるようにするには、次のコマンドを入力します。

```
hostname(config)# same-security-traffic permit inter-interface
```

この設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

（注） 外部インターフェイスと内部インターフェイスの両方に同一セキュリティ レベルのインターフェイスを使用する場合、必要に応じて **xlate-bypass** コマンドをイネーブルにできます。状況によっては、そのコンフィギュレーションで xlate の最大数を超えてもかまいません（制限については、「管理対象のシステム リソース」（P.A-5）を参照してください）。たとえば、**xlate-bypass** を使用しない場合、（NAT を設定していなくても）すべての接続に対して xlate が作成されます。同一セキュリティ トラフィックのコンフィギュレーションでは、xlate を作成する目的で、「内部」インターフェイスとなる同一セキュリティ レベルのインターフェイスがランダムに選択されます。FWSM が外部の同一セキュリティ レベル インターフェイスを「内部」インターフェイスと見なしてしまうと、そのインターフェイスを介してアクセスされるすべてのインターネット ホスト用に xlate が作成されます。数千のインターネット ホストをスキャンするアプリケーション（またはウィルス）が内部ネットワーク上に存在する場合、xlate テーブル内のすべてのエントリがすぐに使い果たされる可能性があります。

インターフェイス内通信の設定

同一インターフェイス上の 2 つのホスト間の通信をイネーブルにするように FWSM を設定できます。この機能をイネーブルにするには、まず、パケットがスイッチ経由で宛先ホストに直接送信されるのではなく、FWSM MAC アドレスに送信されるように、MSFC を正しく設定する必要があります。図 6-2 に、同一インターフェイス上のホストが通信する必要があるネットワークを示します。次に、図 6-2 に示すネットワークの MSFC 上でポリシー ルーティングをイネーブルにするために使用される **route-map** コマンドの出力例を示します。

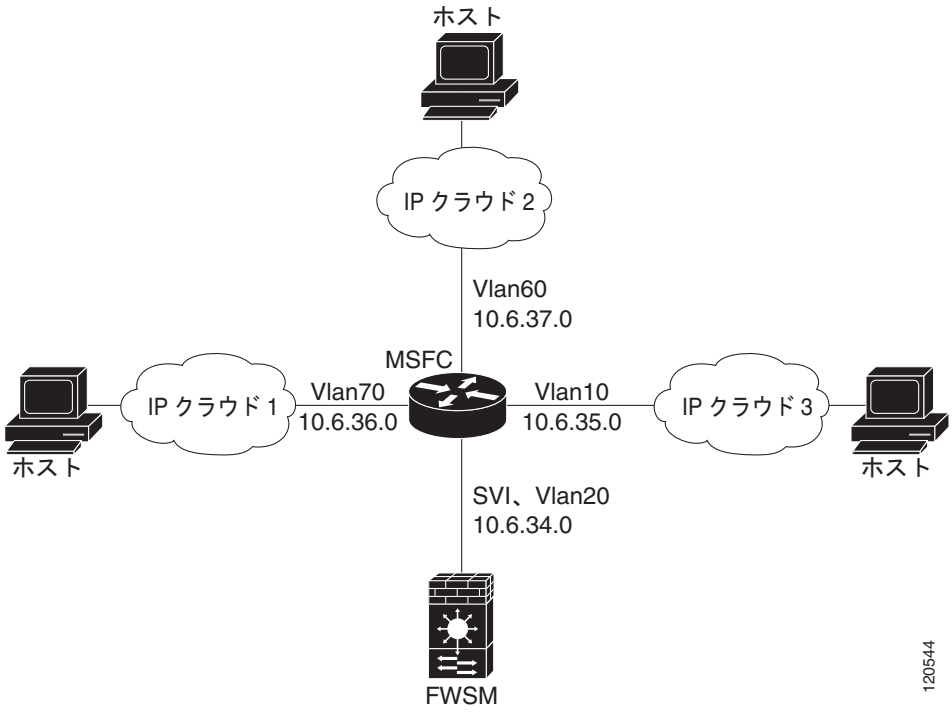
```
Router(config)# route-map intra-inter3 permit 0
Router(config-route-map)# match ip address 103
Router(config-route-map)# set interface Vlan20
Router(config-route-map)# set set ip next-hop 10.6.34.7

Router(config)# route-map intra-inter2 permit 20
Router(config-route-map)# match ip address 102
Router(config-route-map)# set interface Vlan20
Router(config-route-map)# set set ip next-hop 10.6.34.7

Router(config)# route-map intra-inter1 permit 10
```

```
Router(config-route-map)# match ip address 101
Router(config-route-map)# set interface Vlan20
Router(config-route-map)# set set ip next-hop 10.6.34.7
```

図 6-2　同一インターフェイス上のホスト間の通信



同一インターフェイス上の 2 つのホスト間の通信をイネーブルにする場合は、次の要件に注意してください。

- 外部 NAT はサポートされていません。
- 同一セキュリティ レベルのインターフェイス間にスタティック ルートを設定できます。

同一セキュリティ レベルのホスト間の通信をイネーブルにするには、次のコマンドを入力します。

```
hostname(config)# same-security-traffic permit intra-interface
```

これらの設定をディセーブルにするには、コマンドの前に **no** を追加します。

インターフェイスのオン/オフ

デフォルトでは、すべてのインターフェイスがイネーブルです。コンテキスト内でインターフェイスをディセーブルにした場合、または再度イネーブルにした場合、影響を受けるのは、そのコンテキストのインターフェイスだけです。ただし、システム実行スペースでインターフェイスをディセーブルにした場合、または再度イネーブルにした場合は、全コンテキストに対応するその VLAN インターフェイスに影響します。

インターフェイスをディセーブルにする、または再度イネーブルにする手順は、次のとおりです。

ステップ 1　次のコマンドを入力して、インターフェイス コンフィギュレーション モードを開始します。

```
hostname(config)# interface {vlan number | mapped_name}
```

マルチ コンテキスト モードの場合、マップ名が **allocate-interface** コマンドを使用して割り当てられていれば、そのマップ名を入力します。

ステップ 2　次のコマンドを入力して、インターフェイスをディセーブルにします。

```
hostname(config)# shutdown
```

ステップ 3　次のコマンドを入力して、インターフェイスを再度イネーブルにします。

```
hostname(config)# no shutdown
```