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。さらに透過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。

この章で説明する内容は、次のとおりです。

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、最もセキュアにする必要があるネットワークには、レベル 100 を割り当てる必要があります。一方、インターネットに接続する外部ネットワークのレベルは 0 でかまいません。DMZ などその他のネットワークは範囲内の任意のレベルにできます。同じセキュリティ レベルに複数のインターフェイスを割り当てることもできます。詳細については、「同じセキュリティ レベルのインターフェイス間の通信の許可」（p.6-8）を参照してください。

このレベルでは、次の動作を制御します。

- 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。同一セキュリティ レベルのインターフェイスの場合、インスペクション エンジンはどちらの方向のトラフィックにも適用されます。
  - NetBIOS インスペクション エンジン — 発信接続だけに適用されます。
  - OraServ インスペクション エンジン — ホスト ペア間に OraServ ポート用の制御接続がある場合、着信データ接続だけが FWSM の通過を許可されます。
- 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のみ適用されます。同一セキュリティ レベルのインターフェイスの場合、どちらの方向のトラフィックもフィルタリングできます。
- NAT 制御 — NAT 制御をイネーブルにする場合、セキュリティの高いインターフェイス（内部）上のホストがセキュリティの低いインターフェイス（外部）上のホストにアクセスするときに NAT 制御を設定する必要があります。

  NAT 制御を行わない場合、または同一セキュリティ レベルのインターフェイスの場合、すべてのインターフェイス間で NAT を使用することも、NAT を使用しないことも選択できます。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となります。
- **established** コマンド — このコマンドを使用すると、セキュリティ レベルが上位のホストから下位のホストへの接続がすでに確立されている場合に、下位のホストから上位のホストへの戻り接続が可能になります。

  同一セキュリティ レベルのインターフェイスの場合、どちらの方向にも **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

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「内部」という名前を付けて、セキュリティ レベルを明示的に設定しない場合、セキュリティ レベルは 100 に設定されます。

（注） フェールオーバーを使用する場合、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用に確保するインターフェイスには、ここで紹介する手順で名前を設定しないでください。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 13 章「フェールオーバーの設定」を参照してください。

マルチコンテキスト モードに関する注意事項は、次のとおりです。

- 各コンテキスト内でコンテキスト インターフェイスを設定します。
- 設定できるのは、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。
- フェールオーバー インターフェイスはシステム コンフィギュレーションでのみ設定可能です。この手順ではフェールオーバー インターフェイスは設定しないでください。詳細については、第 13 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セキュリティ レベルを変更し、既存の接続がタイムアウトする前に新しいセキュリティ情報を使用する必要がある場合は、**clear local-host** コマンドを使用して、接続を消去します。

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。

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　次のコマンドを入力して、設定するインターフェイスを指定します。

```
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。

コマンドの入力例を示します。

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

ステップ 2　次のコマンドを入力して、インターフェイスに名前を付けます。

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

name は最大 48 文字の文字列です。大文字と小文字は区別されません。名前を変更する場合は、新しい値を使用してコマンドを再入力します。**no** 形式での入力は行わないでください。この名前を参照するすべてのコマンドが削除されます。

（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 は、0（最小）～ 100（最大）の整数です。

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 13 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.9-3）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
```

透過ファイアウォール モードの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、セキュリティ レベル、およびブリッジ グループ アソシエーションを設定しておく必要があります。最後に、各ブリッジ グループに管理 IP アドレスを割り当てます。ここでは、次の内容について説明します。

透過ファイアウォール インターフェイスのパラメータの設定

透過ファイアウォールは内部および外部インターフェイス上の同一ネットワークに接続します。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。このブリッジ 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（「IP アドレスのブリッジ グループへの割り当て」[p.6-7] を参照）。2 つのインターフェイスそれぞれに、8 つまでブリッジ 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避けたい場合、またはセキュリティ コンテキストを最大限に使用したい場合、複数のブリッジ グループを使用できます。ブリッジング機能はブリッジ グループごとに別々ですが、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、各コンテキストで単一ブリッジ グループのセキュリティ コンテキストを使用します。

（注）　フェールオーバーを使用する場合、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用に確保するインターフェイスには、ここで紹介する手順で名前を設定しないでください。

マルチコンテキスト モードでのインターフェイスの設定に関する注意事項は、次のとおりです。

- 各コンテキスト内でコンテキスト インターフェイスを設定します。
- 設定できるのは、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。
- フェールオーバー インターフェイスはシステム コンフィギュレーションでのみ設定可能です。この手順ではフェールオーバー インターフェイスは設定しないでください。
- インターフェイスのセキュリティ レベルを変更し、既存の接続がタイムアウトする前に新しいセキュリティ情報を使用する必要がある場合は、**clear local-host** コマンドを使用して、接続を消去します。

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。

インターフェイスをブリッジ グループに割り当てるには、名前とセキュリティ レベルを設定して、次の手順を実行します。

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　次のコマンドを入力して、インターフェイスに名前を付けます。

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

name は最大 48 文字の文字列です。大文字と小文字は区別されません。名前を変更する場合は、新しい値を使用してコマンドを再入力します。**no** 形式での入力は行わないでください。この名前を参照するすべてのコマンドが削除されます。インターフェイスに「内部」という名前を付けて、セキュリティ レベルを明示的に設定しない場合、セキュリティ レベルは 100 に設定されます。

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 は、0（最小）～ 100（最大）の整数です。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 0 になります。

IP アドレスのブリッジ グループへの割り当て

透過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 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。

管理 IP アドレスを設定するには、次の手順を実行します。

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]
```

透過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、透過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、サブネットの最初と最後のアドレスへの（またはアドレスからの）すべての ARP パケットを廃棄します。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。

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 13 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
```

同じセキュリティ 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、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。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レベルを使用し、同一セキュリティ レベルにインターフェイスを割り当てない場合、1 つのレベル（0 ～ 100）に 1 つのインターフェイスのみ設定できます。

（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.12-13）を参照してください。

セキュリティ レベルが同じインターフェイス間で通信できるようにした場合でも、通常どおり、さまざまなセキュリティ レベルでインターフェイスを設定できます。

同じセキュリティ 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。

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
```