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およびサブインターフェイスの名前、セキュリティ レベル、IP アドレスの設定方法について説明します。シングルコンテキスト モードの場合は、この章の手順は、第 4 章「イーサネットとサブインターフェイスの設定」で開始したインターフェイスの設定の続きとして実行します。マルチコンテキスト モードの場合は、第 4 章「イーサネットとサブインターフェイスの設定」の手順はシステム実行スペースで実行しますが、この章の手順は各セキュリティ コンテキスト内で実行します。

次の事項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は、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、P.6-7 の「同一セキュリティ レベルにあるインターフェイス間の通信の許可」を参照してください。

各レベルは、次の動作を制御します。

- ネットワーク アクセス：デフォルトでは、高位のセキュリティ インターフェイスから低位のセキュリティ インターフェイス（発信）へのアクセスは、暗黙的に許可されます。高位のセキュリティ インターフェイス上のホストは、それより低いセキュリティ インターフェイス上のホストすべてにアクセスできます。アクセスは、インターフェイスにアクセスリストを適用すると制限できます。

  同じレベルのセキュリティ インターフェイスの場合、同じセキュリティ レベルまたはそれより低いレベルの他のインターフェイスにアクセスするインターフェイスへのアクセスは、暗黙的に許可されます。
- 検査エンジン：一部のアプリケーション検査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の場合、検査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 検査エンジン：発信接続のみに適用されます。
  - SQL*Net 検査エンジン：SQL*Net（旧称 OraServ）ポートとの制御接続が一対のホスト間に存在する場合、着信データ接続のみセキュリティ アプライアンスを通過することが許可されます。
- フィルタリング：HTTP（S）フィルタリングおよび FTP フィルタリングは、発信接続（高位レベルから低位レベルへの接続）に対してのみ適用されます。

  同じセキュリティ レベルのインターフェイスの場合、どちらの方向のトラフィックにもフィルタリングが適用できます。
- NAT 制御：NAT 制御をイネーブルにする場合、低位のセキュリティ インターフェイス（外部）上のホストにアクセスする高位のセキュリティ インターフェイス（内部）上のホストに NAT を設定する必要があります。

  NAT 制御がない場合、または同じレベルのセキュリティ インターフェイスの場合は、任意のインターフェイス間で NAT を使用するように選択することも、NAT を使用しないように選択することもできます。外部インターフェイスに対して NAT を設定すると、特殊なキーワードが必要になる場合があることに留意してください。
- **established** コマンド：このコマンドを使用すると、高位レベルのホストから低位レベルのホストに接続がすでに確立されている場合に、低位のセキュリティのホストから高位のセキュリティのホストへのリターン接続が許可されます。

  同じセキュリティ レベルのインターフェイスでは、両方向に対して **established** コマンドが設定できます。

インターフェイスの設定

デフォルトでは、物理インターフェイスはすべてシャットダウンされています。イネーブルになっているサブインターフェイスをトラフィックが通過できるようにするには、物理インターフェイスを事前にイネーブルにしておく必要があります。マルチコンテキスト モードの場合、物理インターフェイスまたはサブインターフェイスをコンテキストに割り当てると、インターフェイスはデフォルトではそのコンテキスト内でイネーブルになります。ただし、トラフィックがコンテキスト 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をシステム コンフィギュレーションでもイネーブルにする必要があります。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、そのインターフェイスを共有しているすべてのコンテキストでダウンします。

コンフィギュレーションを完了してトラフィックがセキュリティ アプライアンスを通過できるようにするには、事前にインターフェイス名と、ルーテッド モードの場合は IP アドレスを設定する必要があります。また、セキュリティ レベルをデフォルトの 0 から変更する必要もあります。インターフェイス名を「inside」にし、セキュリティ レベルを明示的に設定しない場合は、セキュリティ アプライアンスによってセキュリティ レベルが 100 に設定されます。

（注） 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 リンクおよびステート リンクの設定については、第 11 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 モードでは、次のガイドラインに従ってください。

- 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。
- システム　コンフィギュレーションの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 インターフェイスのみが設定できます。
- システム コンフィギュレーションでは、イーサネット設定および VLAN のみが設定できます。フェールオーバー インターフェイスは例外で、この方法でフェールオーバー 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、フェールオーバーの章を参照してください。

（注） インターフェイスのセキュリティ　レベルを変更したときに、既存の接続がタイムアウトするまで待機せず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クリアできます。

インターフェイスまたはサブ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 {physical_interface[.subinterface] | mapped_name}
```

physical_interface ID には、タイプ、スロット、およびポート番号を *type*[*slot*/]*port* という形式で指定します。

物理インターフェイスには、次のタイプがあります。

- **ethernet**
- **gigabitethernet**

PIX 500 シリーズ セキュリティ アプライアンスでは、タイプの後ろにポート番号を入力します（**ethernet0** など）。

ASA 5500 シリーズ適応型セキュリティ アプライアンスでは、タイプの後ろにスロット / ポートを入力します（**gigabitethernet0/1** など）。シャーシに組み込まれているインターフェイスはスロット 0 に割り当てられていますが、4GE SSM 上のインターフェイスはスロット 1 に割り当てられています。

ASA 5500 シリーズ適応型セキュリティ アプライアンスには、次のタイプもあります。

- **management**

  管理インターフェイスは、管理トラフィックのみを対象に設計されているファースト イーサネット インターフェイスであり、**management0/0** と指定されます。ただし、必要であれば、トラフィックを通すために使用することもできます（**management-only** コマンドを参照）。透過ファイアウォール モードでは、トラフィックの通過を許可する 2 つのインターフェイスの他に、管理インターフェイスを使用できます。サブインターフェイスを管理インターフェイスに追加して、マルチコンテキスト モードのセキュリティ コンテキストごとに管理を提供することもできます。

subinterface ID は、物理インターフェイス ID の後ろに、ピリオド（.）で区切って付加します。

マルチコンテキスト モードで、マッピング名を **allocate-interface** コマンドを使用して割り当てた場合、その名前を入力します。

たとえば、次のコマンドを入力します。

```
hostname(config)# interface gigabitethernet0/1.1
```

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。新しい値を指定してこのコマンドを再入力すると名前を変更することができます。**no** 形式は入力しないでください。このコマンドを入力すると、この名前を参照しているコマンドがすべて削除されます。

ステップ 3　セキュリティ レベルを設定するには、次のコマンドを入力します。

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

ここで、*number* には、0（最下位）～ 100（最上位）の整数を指定します。

ステップ 4　（ルーテッド モードのみ）IP アドレスを設定するには、次のコマンドのいずれかを入力します。

（注）　IPv6 アドレスの設定については、P.9-3 の「インターフェイスでの IPv6 の設定」を参照してください。

透過ファイアウォール モードの管理 IP アドレスを設定するには、P.7-6 の「透過ファイアウォールの管理 IP アドレスの設定」を参照してください。透過モードでは、インターフェイスごとに IP アドレスを設定するのではなく、セキュリティ アプライアンス全体またはコンテキスト全体に IP アドレスを設定します。

- IP アドレスを手動で設定するには、次のコマンドを入力します。

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

  standby キーワードおよびアドレスはフェールオーバーで使用します。詳細については、第 11 章「フェールオーバーの設定」を参照してください。

- DHCP サーバから IP アドレスを取得するには、次のコマンドを入力します。

  ```
  hostname(config-if)# ip address dhcp [setroute]
  ```

  このコマンドを再入力すると、DHCP リースがリセットされて新しいリースが要求されます。

  このコマンドは、**ip address** コマンドと同時には設定できません。

  setroute オプションをイネーブルにする場合は、**static** コマンドを使用してデフォルト ルートを設定しないでください。

  ip address dhcp コマンドを入力する前に **no shutdown** コマンドを使用してインターフェイスをイネーブルにしていない場合は、一部の DHCP 要求が送信されない場合があります。

ステップ 5　インターフェイスを管理専用モードに設定するには、次のコマンドを入力します。

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

ASA 5000 シリーズ適応型セキュリティ アプライアンスには、Management 0/0 と呼ばれる専用の管理インターフェイスが含まれており、このインターフェイスによってセキュリティ アプライアンスへのトラフィックをサポートします。ただし、**management-only** コマンドを使用することで、任意のインターフェイスを管理専用インターフェイスとして設定できます。また、Management 0/0 の管理専用モードをディセーブルにして、他のインターフェイスと同様にトラフィックを通過させることもできます。

（注）　透過ファイアウォール モードでは、2 つのインターフェイスのみがトラフィックを通過させることができます。ただし、ASA 5000 シリーズ適応型セキュリティ アプライアンスでは、専用の管理インターフェイス（物理インターフェイスまたはサブインターフェイス）を管理トラフィック用の第 3 のインターフェイスとして使用できます。モードはこの場合設定不能であり、常に管理専用にする必要があります。

ステップ 6　インターフェイスをイネーブルにするには、次のコマンドを入力します（インターフェイスがまだイネーブルになっていない場合）。

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

インターフェイスをディセーブルにするには、**shutdown** コマンドを入力します。物理インターフェイスに対して **shutdown** コマンドを入力すると、すべてのサブインターフェイスもシャットダウンします。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を共有しているすべてのコンテキストでシャットダウンします。これは、コンテキスト コンフィギュレーションでこのインターフェイスがイネーブルであると表示される場合も例外ではありません。

次の例では、シングルモードで物理インターフェイスのパラメータを設定します。

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

次の例では、シングルモードでサブインターフェイスのパラメータを設定します。

```
hostname(config)# interface gigabitethernet0/1.1
hostname(config-subif)# vlan 101
hostname(config-subif)# nameif dmz1
hostname(config-subif)# security-level 50
hostname(config-subif)# ip address 10.1.2.1 255.255.255.0
hostname(config-subif)# no shutdown
```

次の例では、システム コンフィギュレーションに対してマルチコンテキスト モードでインターフェイス パラメータを設定し、gigabitethernet 0/1.1 サブインターフェイスを contextA に割り当てます。

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# no shutdown
hostname(config-if)# interface gigabitethernet0/1.1
hostname(config-subif)# vlan 101
hostname(config-subif)# no shutdown
hostname(config-subif)# context contextA
hostname(config-ctx)# ...
hostname(config-ctx)# allocate-interface gigabitethernet0/1.1
```

次の例では、コンテキスト コンフィギュレーションに対してマルチコンテキスト モードでパラメータを設定します。

```
hostname/contextA(config)# interface gigabitethernet0/1.1
hostname/contextA(config-if)# nameif inside
hostname/contextA(config-if)# security-level 100
hostname/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
hostname/contextA(config-if)# no shutdown
```

同一セキュリティ レベルにあるインターフェイス間の通信の許可

デフォルトでは、セキュリティ レベルが同じインターフェイスは同士では通信できません。同じセキュリティ レベルのインターフェイス間で通信を許可する利点としては、次のものがあります。

- 101 より多くの通信インターフェイスが設定できます。

  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。
- アクセスリストがなくても同じセキュリティ　レベルのインターフェイスすべての間で自由にトラフィックが流れるようにできます。

（注）　NAT 制御をイネーブルにすると、同じセキュリティ レベルのインターフェイス間で NAT を設定する必要がなくなります。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、P.14-13 の「NAT および同じセキュリティ レベルのインターフェイス」を参照してください。

同じセキュリティ レベルを持つインターフェイス間の通信をイネーブルにした場合でも、異なるセキュリティ レベルのインターフェイスも通常どおりに設定できます。

相互通信を可能にするために同じセキュリティ レベルのインターフェイス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 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。