CHAPTER 7

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に名前、セキュリティ レベル、および IP アドレスを設定する方法について説明します。シングル コンテキスト モードでは、第 5 章「イーサネット設定および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設定をこの章の手順で継続します。マルチ コンテキスト モードでは、第 5 章「イーサネット設定およびサブインターフェイスの設定」の手順を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。

（注） ASA 5505 適応型セキュリティ アプライアンスのインターフェイスを設定するには、第 4 章「Cisco ASA 5505 適応型セキュリティ アプライアンス用スイッチ ポートおよび VLAN インターフェイスの設定」を参照してください。

この章は、次の項で構成されています。

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、「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」（P.7-6）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。

- ネットワーク アクセス：デフォルトで、高いセキュリティ レベルのインターフェイスから低いセキュリティ レベルのインターフェイスへの通信（発信）は暗黙的に許可されます。高いセキュリティ レベルのインターフェイス上のホストは、低いセキュリティ レベルのインターフェイス上の任意のホストにアクセスできます。インターフェイスにアクセス リストを適用することによって、アクセスを制限できます。

  同じセキュリティ レベルのインターフェイスの通信をイネーブルにすると（「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」（P.7-6）を参照）、同じセキュリティ レベルまたはそれより低いセキュリティ 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は、暗黙的に許可されます。

- インスペクション エンジン：一部のアプリケーション 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。
  - SQL*Net インスペクション 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、着信データ接続だけがセキュリティ 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) および FTP フィルタリングは、（高いレベルから低いレベルへの）発信接続にのみ適用されます。

  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、発信と着信の両方の接続に対して **established** コマンドを設定できます。

インターフェイスの設定

物理インターフェイスは、デフォルトではすべてシャットダウンされます。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。

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、セキュリティ アプライアンス はセキュリティ レベルを 100 に設定します。

（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。

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。

- 各コンテキスト内からコンテキスト 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。
- 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 の設定のみができます。ただし、フェールオーバー インターフェイスは例外です。この手順ではフェールオーバー インターフェイスを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のタイプには、次のものがあります。

- **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（例：**gigabitethernet0/1**）。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、4GE SSM のインターフェイスはスロット 1 に割り当てられます。ASA 5550 適応型セキュリティ アプライアンスでは、最大のスループットを得るために、2 つのインターフェイス スロット間でトラフィックのバランスを取るようにします。たとえば、内部インターフェイスをスロット 1 に、外部インターフェイスをスロット 0 に割り当てます。

ASA 5510 以降の適応型セキュリティ アプライアンスには、次のタイプも含まれます。

- **management**

  管理インターフェイスは、管理トラフィック専用のファスト イーサネット インターフェイスであり、**management0/0** のように指定します。ただし、必要に応じて通過トラフィック用に使用することもできます（**management-only** コマンドを参照）。トランスペアレント ファイアウォール モードでは、通過トラフィックに許可されている 2 つのインターフェイスに加えて、管理インターフェイスを使用できます。また、管理インターフェイスにサブインターフェイスを追加して、マルチ コンテキスト モードの各セキュリティ コンテキストでの管理を実現できます。

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 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。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　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
```

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　（任意）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 5510 以降の適応型セキュリティ アプライアンスには、Management 0/0 という専用の管理インターフェイスが含まれ、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するようになっています。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 の場合、管理専用モードをディセーブルにできるため、このインターフェイスは他のインターフェイスと同じくトラフィックを通過させることができます。

（注）　トランスペアレント ファイアウォール モードでは、2 つのインターフェイスだけがトラフィックを通過させることができます。ただし、ASA 5510 以降の適応型セキュリティ アプライアンスの場合、Management 0/0 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のいずれか）を管理トラフィック用に 3 台目のインターフェイスとして使用できます。この場合モードは設定不可となり、常に管理専用にする必要があります。

ステップ 5　IP アドレスを設定するには、次のいずれかのコマンドを入力します。

ルーテッド ファイアウォール モードでは、すべてのインターフェイスに対する IP アドレスを設定します。トランスペアレント ファイアウォール 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設定します。トラフィックを通過させない Management 0/0 管理専用インターフェイスの場合は例外となります。トランスペアレント ファイアウォール モードの管理 IP アドレスを設定する方法については、「透過ファイアウォールの管理 IP アドレスの設定」（P.8-5）を参照してください。Management 0/0 インターフェイスまたはサブインターフェイスの IP アドレスを設定するには、次のいずれかのコマンドを使用します。

IPv6 アドレスの設定については、「インターフェイスでの IPv6 の設定」（P.12-3）を参照してください。

フェールオーバーの場合、IP アドレスとスタンバイ アドレスを手動で設定する必要があります。DHCP および PPPoE はサポートされません。

- 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]
  ```

  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。

- 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]
  ```

  DHCP リースをリセットし、新規リースを要求するには、このコマンドを再入力します。

  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なかった場合、DHCP 要求が送信されないことがあります。

- PPPoE サーバからの IP アドレスの取得については、第 35 章「PPPoE クライアントの設定」を参照してください。

ステップ 6　（任意）プライベート MAC アドレスをこのインターフェイスに割り当てるには、次のコマンドを入力します。

```
hostname(config-if)# mac-address mac_address [standby mac_address]
```

mac_address は、H.H.H 形式で指定します。H は 16 ビットの 16 進数です。たとえば、MAC アドレスが 00-0C-F1-42-4C-DE であれば、000C.F142.4CDE と入力します。

デフォルトでは、物理インターフェイスはバーンドイン MAC アドレスを使用し、物理インターフェイスのすべてのサブインターフェイスは同じバーンドイン MAC アドレスを使用します。

フェールオーバーで使用する場合は、**スタンバイ** MAC アドレスを設定します。アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古いアクティブ装置はスタンバイ アドレスを使用します。

マルチ コンテキスト モードでは、コンテキスト間でインターフェイスを共有している場合、固有の MAC アドレスをそれぞれのコンテキストのインターフェイスに割り当てることができます。この機能を使用すると、セキュリティ アプライアンスはパケットを適切なコンテキストに容易に分類できます。固有の MAC アドレスがなくても共有インターフェイスを使用できますが、制限があります。詳細については、「セキュリティ アプライアンスによるパケットの分類方法」（P.3-3）を参照してください。コンテキストの共有インターフェイスには、手動で各 MAC アドレスを割り当てることも、自動生成することもできます。MAC アドレスの自動生成については、「コンテキスト インターフェイスへの MAC アドレスの自動割り当て」（P.6-11）を参照してください。MAC アドレスを自動的に生成する場合、**mac-address** コマンドを使用して、生成されたアドレスを上書きできます。

シングル コンテキスト モード、またはマルチ コンテキスト モードで共有されないインターフェイスの場合は、固有の MAC アドレスをサブインターフェイスに割り当てることを推奨します。たとえば、サービス プロバイダーによっては、MAC アドレスに基づいてアクセス コントロールを実行する場合があります。

ステップ 7　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。

次に、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する例を示します。

```
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
```

次に、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する例を示します。

```
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)# mac-address 000C.F142.4CDE standby 020C.F142.4CDE
hostname(config-subif)# no shutdown
```

次に、システム コンフィギュレーション用にマルチ 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コンテキスト A に割り当てる例を示します。

```
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
```

次に、コンテキスト コンフィギュレーション用にマルチ コンテキスト モードでパラメータを設定する例を示します。

```
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)# mac-address 030C.F142.4CDE standby 040C.F142.4CDE
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同士は通信できません。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 より多い数の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。

- 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 および同じセキュリティ レベルのインターフェイス」（P.17-13）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。

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。