インターフェイス コンフィギュレーションの実行（トランスペアレント モード、8.3 以前）

この章では、トランスペアレント ファイアウォール モードですべてのモデルのインターフェイス コンフィギュレーションを実行するためのタスクについて説明します。

バージョン 8.4 以降については、第 15 章「インターフェイス コンフィギュレーションの実行（トランスペアレント モード、8.3 以前）」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。

（注） マルチ コンテキスト モードでは、この項のタスクをコンテキスト実行スペースで実行してください。[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

トランスペアレント モードでのインターフェイス コンフィギュレーションの実行について（8.3 以前）

この項では、次のトピックについて取り上げます。

グローバル管理 IP アドレスについて

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。ASA に必要な唯一の IP コンフィギュレーションは、管理 IP アドレスを設定することです。このアドレスが必要になるのは、ASA がシステム メッセージや AAA サーバとの通信など ASA で発信され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ためです。このアドレスは、リモート管理アクセスにも使用できます。

IPv4 トラフィックの場合、すべてのトラフィックを通過させるには、管理 IP アドレスが必要です。IPv6 トラフィックの場合は、少なくとも、トラフィックを通過させるリンクローカル アドレスを設定する必要があります。リモート管理などの管理操作を含めたフル機能を実現するために、グローバル管理アドレスを設定することを推奨します。

（注） また、デバイスの管理 IP アドレス以外に、管理インターフェイスの IP アドレスを設定できます。この IP アドレスは、メインの管理 IP アドレスとは別のサブネットに設定できます。

他のインターフェイスの IPv4 アドレスまたはグローバル IPv6 アドレスは設定しませんが 「一般的なインターフェイス パラメータの設定」（P.15-10）に従って、セキュリティ レベルとインターフェイス名を設定する必要があります。

セキュリティ レベル

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、「同じセキュリティ レベルの通信の許可」（P.15-18）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（「同じセキュリティ レベルの通信の許可」（P.15-18）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 ASA 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の通信をイネーブルにすると、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。

- **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。

  セキュリティ レベルが同じインターフェイス間の通信をイネーブルにすると、両方向に対して **established** コマンドを設定できます。

トランスペアレント モードでインターフェイス コンフィギュレーションを実行するためのライセンス要件

モデル	ライセンス要件
すべてのモデル	基本ライセンス

注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

- マルチ コンテキスト モードでは、第 11 章「インターフェイス コンフィギュレーションの開始（ASA 5510 以降）」に従って、システム実行スペースで物理インターフェイスを設定します。次に、この章に従って、コンテキスト実行スペースで論理インターフェイス パラメータを設定します。
- 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。

ファイアウォール モードのガイドライン

- IPv4 の場合は、管理トラフィックと、ASA を通過するトラフィックの両方に対し、管理 IP アドレスが必要です。

  インターフェイスごとに IP アドレスが必要なルーテッド モードと異なり、トランスペアレント ファイアウォールではデバイス全体に IP アドレスが割り当てられます。ASA は、この IP アドレスを、システム メッセージや AAA 通信など、ASA で発信されるパケットの送信元アドレスとして使用します。グローバル管理アドレスのほか、オプションで、管理インターフェイスを設定できます。詳細については、「管理インターフェイス」（P.11-2）を参照してください。

  管理 IP アドレスは、接続されているネットワークと同じサブネット内にある必要があります。サブネットにホスト サブネット（255.255.255.255）を設定することはできません。ASA 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。管理 IP サブネットの詳細については、「トランスペアレント ファイアウォールの管理 IP アドレスの設定（8.3 以前）」（P.15-4）を参照してください。
- IPv6 の場合は、少なくとも通過トラフィック用に各インターフェイスにリンクローカル アドレスを設定する必要があります。ASA の管理を含むフル機能のためには、グローバル IPv6 アドレスを設定する必要があります。

- マルチ コンテキスト モードでは、各コンテキストが別個のインターフェイスを使用する必要があります。コンテキスト間でインターフェイスを共有することはできません。
- マルチ コンテキスト モードでは、通常、各コンテキストが別個のサブネットを使用します。重複するサブネットを使用することもできますが、ルーティング スタンドポイントから可能にするため、ネットワーク トポロジにルータと NAT コンフィギュレーションが必要です。

フェールオーバーのガイドライン

フェールオーバー インターフェイスの設定は、この章の手順では完了しません。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 9 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、フェールオーバー インターフェイスがシステム コンフィギュレーションに設定されます。

IPv6 のガイドライン

- IPv6 をサポートします。
- トランスペアレント モードでは IPv6 エニーキャスト アドレスをサポートしません。

デフォルト設定

この項では、工場出荷時のデフォルト コンフィギュレーションが設定されていない場合のインターフェイスのデフォルト設定を示します。工場出荷時のデフォルト コンフィギュレーションについては、「工場出荷時のデフォルト コンフィギュレーション」（P.3-19）を参照してください。

デフォルトのセキュリティ レベル

デフォルトのセキュリティ レベルは 0 です。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、ASA はセキュリティ レベルを 100 に設定します。

（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。

トランスペアレント ファイアウォールの管理 IP アドレスの設定（8.3 以前）

この項では、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説明します。次の項目を取り上げます。

- 「IPv4 アドレスの設定」（P.15-5）
- 「IPv6 アドレスの設定」（P.15-5）

IPv4 アドレスの設定

この項では、IPv4 アドレスの設定方法について説明します。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [Management IP Address] の順に選択します。

ステップ 2　[IPv4 Address] 領域の [Management IP Address] フィールドに IP アドレスを入力します。

このアドレスは、上流のルータおよび下流のルータと同じサブネットに存在する必要があります。サブネットにホスト サブネット（255.255.255.255）を設定することはできません。フェールオーバーには、**standby** キーワードおよびアドレスを使用します。

ステップ 3　[Subnet Mask] ドロップダウン リストからサブネット マスクを選択するか、サブネット マスクをフィールドに直接入力します。

ステップ 4　[Apply] をクリックします。

IPv6 アドレスの設定

この項では、グローバル アドレスまたはリンクローカル アドレスの設定方法について説明します。説明する内容は次のとおりです。

IPv6 に関する情報

ここでは、IPv6 を設定する手順について説明します。内容は次のとおりです。

IPv6 アドレス指定

次の 2 種類の IPv6 のユニキャスト アドレスを設定できます。

- グローバル：グローバル アドレスは、パブリック ネットワークで使用可能なパブリック アドレスです。このアドレスは、インターフェイスごとではなく、デバイスごとまたはコンテキストごとに設定する必要があります。また、管理インターフェイスのグローバルな IPv6 アドレスを設定することもできます。

- リンクローカル：リンクローカル アドレスは、直接接続されたネットワークだけで使用できるプライベート アドレスです。ルータは、リンクローカル アドレスを使用してパケットを転送するのではなく、特定の物理ネットワーク セグメント上で通信だけを行います。ルータは、アドレス設定またはアドレス解決およびネイバー探索などの ND 機能に使用できます。リンクローカル アドレスは 1 つのセグメント上だけで使用可能であり、インターフェイスの MAC アドレスに関連付けられているため、インターフェイスごとにリンクローカル アドレスを設定する必要があります。

最低限、IPv6 が動作するようにリンクローカル アドレスを設定する必要があります。グローバル アドレスを設定する場合、各インターフェイスにリンクローカル アドレスが自動的に設定されるため、特にリンクローカル アドレスを設定する必要はありません。グローバル アドレスを設定しない場合は、リンクローカル アドレスを自動的にするか、手動で設定する必要があります。

重複アドレス検出

ステートレスな自動設定プロセス中、新しいユニキャスト IPv6 アドレスは重複アドレス検出（DAD）によって固有であることが検証されてから、インターフェイスに割り当てられます（重複アドレス検出の実行中、新しいアドレスは仮の状態となります）。重複アドレス検出は、最初に新しいリンクローカル アドレスに対して行われます。リンクローカル アドレスが固有であることが検証されたら、次にインターフェイス上のその他すべての IPv6 ユニキャスト アドレスに対して重複アドレス検出が行われます。

重複アドレス検出は、管理上ダウンしているインターフェイスでは停止します。インターフェイスが管理上ダウンしている間、そのインターフェイスに割り当てられたユニキャスト IPv6 アドレスは保留状態に設定されます。管理上アップ状態に復帰したインターフェイスでは、重複アドレス検出がインターフェイス上のすべてのユニキャスト IPv6 アドレスに対して再開されます。

重複アドレスが検出されると、そのアドレスの状態は DUPLICATE に設定され、アドレスは使用対象外となり、次のエラー メッセージが生成されます。

```
%ASA-4-325002: Duplicate address ipv6_address/MAC_address on interface
```

重複アドレスがインターフェイスのリンクローカル アドレスであれば、インターフェイス上で IPv6 パケットの処理はディセーブルになります。重複アドレスがグローバル アドレスであれば、そのアドレスは使用されません。ただし、その重複アドレスに関連付けられたすべてのコンフィギュレーション コマンドは、アドレスの状態が DUPLICATE に設定されている間、設定されたままになります。

インターフェイスのリンクローカル アドレスが変更された場合、新しいリンクローカル アドレスで重複アドレス検出が実行され、インターフェイスに関連付けられた他のすべての IPv6 アドレスが再生成されます（重複アドレス検出は新規のリンクローカル アドレスでのみ実行されます）。

ASA は、ネイバー送信要求メッセージを使用して、重複アドレス検出を実行します。デフォルトでは、インターフェイスが重複アドレス検出を行う回数は 1 回です。

Modified EUI-64 インターフェイス ID

RFC 3513「Internet Protocol Version 6 (IPv6) Addressing Architecture」（インターネット プロトコル バージョン 6 アドレッシング アーキテクチャ）では、バイナリ値 000 で始まるものを除き、すべてのユニキャスト IPv6 アドレスのインターフェイス識別子部分は長さが 64 ビットで、Modified EUI-64 形式で組み立てることが要求されています。ASA では、ローカル リンクに接続されたホストにこの要件を適用できます。

この機能がインターフェイスでイネーブルになっていると、そのインターフェイス ID が Modified EUI-64 形式を採用していることを確認するために、インターフェイスで受信した IPv6 パケットの送信元アドレスが送信元 MAC アドレスに照らして確認されます。IPv6 パケットがインターフェイス ID に Modified EUI-64 形式を採用していない場合、パケットはドロップされ、次のシステム ログ メッセージが生成されます。

```
%ASA-3-325003: EUI-64 source address check failed.
```

アドレス形式の確認は、フローが作成される場合にのみ実行されます。既存のフローからのパケットは確認されません。また、アドレスの確認はローカル リンク上のホストに対してのみ実行できます。ルータの背後にあるホストから受信したパケットは、アドレス形式の検証に失敗してドロップされます。これは、その送信元 MAC アドレスがルータの MAC アドレスであり、ホストの MAC アドレスではないためです。

サポートされていないコマンド

次の IPv6 コマンドにはルータ機能が必要であるため、トランスペアレント ファイアウォール モードではサポートされません。

- **ipv6 address autoconfig**
- **ipv6 nd prefix**
- **ipv6 nd ra-interval**
- **ipv6 nd ra-lifetime**
- **ipv6 nd suppress-ra**

トランスペアレント モードが VPN をサポートしていないため、**ipv6 local pool** VPN コマンドはサポートされません。

グローバル アドレスの設定

管理 IPv6 アドレスを設定するには、次の手順を実行します。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [Management IP Address] の順に選択します。

ステップ 2　[IPv6 Addresses] 領域で、[Add] をクリックします。

[Add IPv6 Management Address] ダイアログボックスが表示されます。

ステップ 3　[IP Address] フィールドに、IPv6 アドレスを入力します。

たとえば、「2001:0DB8::BA98:0:3210」のように入力します。IPv6 アドレッシングの詳細については、「IPv6 アドレス」（P.48-5）を参照してください。

ステップ 4　[Prefix Length] フィールドに、プレフィックスの長さを入力します。

たとえば 48 と入力します。IPv6 アドレッシングの詳細については、「IPv6 アドレス」（P.48-5）を参照してください。

ステップ 5　[OK] をクリックします。

ステップ 6　追加のアドレスを設定するには、ステップ 2 から ステップ 5 を繰り返します。

ステップ 7　[Apply] をクリックします。

リンクローカル アドレスの自動設定

リンクローカル アドレスだけを設定する必要があり、その他の IPv6 アドレスを割り当てない場合は、リンクローカル アドレスをインターフェイスの MAC アドレス（Modified EUI-64 形式）に基づいて生成できます。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [Management IP Address] の順に選択します。

ステップ 2　[IPv6 configuration] 領域で、[Enable IPv6] をオンにします。

このオプションでは、すべてのインターフェイスで IPv6 をイネーブルにし、インターフェイスの MAC アドレスに基づく Modified EUI-64 インターフェイス ID を使用してリンクローカル アドレスを自動的に生成します。

（注）　IPv6 アドレス（グローバルまたはリンクローカル）を設定する場合は、このオプションをオンにする必要はありません。IPv6 アドレスを割り当てるとただちに、IPv6 サポートが自動的にイネーブルになります。また、IPv6 アドレスを設定した場合は、このオプションをオフにしても IPv6 はディセーブルになりません。

この領域に表示される IPv6 DAD パラメータを設定する場合については、「DAD 設定の指定」（P.15-8）を参照してください。

ステップ 3　[Apply] をクリックします。

インターフェイスでのリンクローカル アドレスの手動設定

リンクローカル アドレスだけを設定し、その他の IPv6 アドレスを割り当てない場合は、リンクローカル アドレスを手動で定義できます。

手順の詳細

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。

ステップ 2　インターフェイスを選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

ステップ 3　[IPv6] タブをクリックします。

ステップ 4　（任意）ローカル リンクの IPv6 アドレスに Modified EUI-64 形式のインターフェイス識別子の使用を適用するには、[Enforce EUI-64] チェックボックスをオンにします。

インターフェイス識別子が Modified EUI-64 形式に準拠していない場合は、エラー メッセージが表示されます。詳細については、「Modified EUI-64 インターフェイス ID」（P.15-6）を参照してください。

ステップ 5　リンクローカル アドレスを設定するには、[Link-local address] フィールドにアドレスを入力します。

リンクローカル アドレスは、FE8、FE9、FEA、または FEB で始まっている必要があります。たとえば fe80::20d:88ff:feee:6a82 のようになります。IPv6 アドレッシングの詳細については、「IPv6 アドレス」（P.48-5）を参照してください。

ステップ 6　[OK] をクリックします。

DAD 設定の指定

DAD は、割り当てられる前に、新しいユニキャスト IPv6 アドレスの一意性を検証し、ネットワークに重複する IPv6 アドレスが検出されていないかをリンクベースで確認します。

Enable IPv6 パラメータに関する情報については、「リンクローカル アドレスの自動設定」（P.15-7）を参照してください。

手順の詳細

ステップ 1　[Configuration] > [Device Management] > [Management Access] > [Management IP Address] の順に選択します。

ステップ 2　[IPv6 configuration] 領域の [DAD attempts] フィールドに、許可される DAD の試行回数を入力します。

この設定では、DAD が IPv6 アドレスで実行されている間に、インターフェイスに連続して送信されるネイバー送信要求メッセージの数を設定します。0 ～ 600 の範囲の値を指定できます。この値がゼロの場合、指定されたインターフェイスでの DAD 処理がディセーブルになります。デフォルトは 1 メッセージです。

ステップ 3　[NS Interval] フィールドに、ネイバー送信要求メッセージの間隔を入力します。

ネイバー送信要求メッセージは、ターゲット ノードのリンク層アドレスを要求します。有効値の範囲は、1000 ～ 3600000 ミリ秒です。デフォルトは 1000 ミリ秒です。

ステップ 4　[Reachable Time] フィールドに、到達可能性確認イベントの発生後、リモート IPv6 ノードが到達可能と見なされる秒単位の時間を入力します。

有効値の範囲は、1000 ～ 3600000 ミリ秒です。デフォルトは 0 です。設定時間によって、使用不可のネイバーを検知できます。時間を短く設定すればするほど、速く検知できますが、通常の IPv6 の動作では、極端に短い時間を設定することはお勧めしません。

ステップ 5　[Apply] をクリックします。

トランスペアレント モードでのインターフェイス コンフィギュレーションの実行（8.3 以前）

この項では、トランスペアレント モードのすべてのモデルのインターフェイス コンフィギュレーションを実行するためのタスクについて説明します。

（注）　マルチ コンテキスト モードでは、この項のタスクをコンテキスト実行スペースで実行してください。[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

この項では、次のトピックについて取り上げます。

インターフェイス コンフィギュレーションを実行するためのタスク フロー

ステップ 1　「インターフェイス コンフィギュレーションの開始（ASA 5510 以降）」（P.11-15）または「ASA 5505 インターフェイス コンフィギュレーションの開始」（P.12-6）の手順を実行します。

ステップ 2　（マルチ コンテキスト モード）[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

ステップ 3　インターフェイス名、セキュリティ レベルなどの一般的なインターフェイス パラメータを設定します。「一般的なインターフェイス パラメータの設定」（P.15-10）を参照してください。

ステップ 4　（任意）管理インターフェイスを設定します。「管理インターフェイスの設定（ASA 5510 以降）」（P.15-12）を参照してください。

ステップ 5　（任意）MAC アドレスと MTU を設定します。「MAC アドレス、MTU、TCP MSS の設定」（P.15-15）を参照してください。

ステップ 6　（任意）2 つのインターフェイス間の通信を許可するか、またはトラフィックが同じインターフェイスに入って同じインターフェイスから出ることを許可することで、同じセキュリティ レベルの通信を許可します。「同じセキュリティ レベルの通信の許可」（P.15-18）を参照してください。

一般的なインターフェイス パラメータの設定

この手順は、トランスペアレント インターフェイスの名前、セキュリティ レベル、およびブリッジ グループを設定する方法について説明します。

別の管理インターフェイスを設定する方法については、「管理インターフェイスの設定（ASA 5510 以降）」（P.15-12）を参照してください。

ASA 5510 以降では、次のインターフェイス タイプのインターフェイス パラメータを設定する必要があります。

- 物理インターフェイス
- VLAN サブインターフェイス
- 冗長インターフェイス

ASA 5505 では、次のインターフェイス タイプのインターフェイス パラメータを設定する必要があります。

- VLAN インターフェイス

注意事項と制約事項

- コンテキストごとに最大 2 つのインターフェイスを設定できます。
- ASA 5550ASA 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。
- セキュリティ レベルについては、「セキュリティ レベル」（P.15-2）を参照してください。
- 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 9 章「フェールオーバーの設定」を参照してください。

前提条件

- 第 11 章「インターフェイス コンフィギュレーションの開始（ASA 5510 以降）」または第 12 章「インターフェイス コンフィギュレーションの開始（ASA 5505）」の手順を実行します。
- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システムからコンテキスト コンフィギュレーションに変更するには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順の詳細

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。

マルチ コンテキスト モードでは、システム実行スペースでコンテキストに割り当てられたインターフェイスだけがテーブルに表示されます。

ステップ 2　インターフェイスの行を選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

ステップ 3　[Interface Name] フィールドに、名前を 48 文字以内で入力します。

ステップ 4　[Security level] フィールドに、0（最低）～ 100（最高）のレベルを入力します。

詳細については、「セキュリティ レベル」（P.15-2）を参照してください。

ステップ 5　インターフェイスがまだイネーブルでない場合は、[Enable Interface] チェックボックスをオンにします。

ステップ 6　（任意）[Description] フィールドに、このインターフェイスの説明を入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。フェールオーバーまたはステート リンクの場合、説明は、「LAN Failover Interface」、「STATE Failover Interface」、「LAN/STATE Failover Interface」などの固定の値になります。この説明は編集できません。このインターフェイスをフェールオーバーまたはステート リンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。

（注）　（ASA 5510 以降、シングル モード）[Configure Hardware Properties] ボタンに関する情報については、「物理インターフェイスのイネーブル化およびイーサネット パラメータの設定」（P.11-26）を参照してください。

ステップ 7　[OK] をクリックします。

次の作業

- （任意）管理インターフェイスを設定します。「管理インターフェイスの設定（ASA 5510 以降）」（P.15-12）を参照してください。
- （任意）MAC アドレスと MTU を設定します。「MAC アドレス、MTU、TCP MSS の設定」（P.15-15）を参照してください。

管理インターフェイスの設定（ASA 5510 以降）

1 つの管理インターフェイスをネットワーク インターフェイスとは独立してシングル モードまたはコンテキストごとに設定できます。管理*スロット/ポート*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）を個別の管理インターフェイスとして使用できます。他のインターフェイス タイプは管理インターフェイスとして使用できません。詳細については、「管理インターフェイス」（P.11-2）を参照してください。

この項では、次のトピックについて取り上げます。

一般パラメータおよび IPv4 アドレスの設定

この項では、管理インターフェイスの名前、セキュリティ レベル、および IPv4 アドレスを設定する方法について説明します。

前提条件

- 第 11 章「インターフェイス コンフィギュレーションの開始（ASA 5510 以降）」または第 12 章「インターフェイス コンフィギュレーションの開始（ASA 5505）」の手順を実行します。
- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システムからコンテキスト コンフィギュレーションに変更するには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順の詳細

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。

マルチ コンテキスト モードでは、システム実行スペースでコンテキストに割り当てられたインターフェイスだけがテーブルに表示されます。

ステップ 2　管理インターフェイスまたはサブインターフェイスの行を選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

ステップ 3　[Interface Name] フィールドに、名前を 48 文字以内で入力します。

ステップ 4　[Security level] フィールドに、0（最低）～ 100（最高）のレベルを入力します。

詳細については、「セキュリティ レベル」（P.15-2）を参照してください。

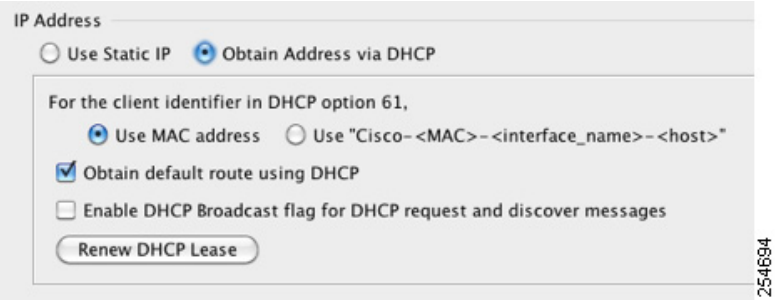
（注）　[Dedicate this interface to management only] チェックボックスは、デフォルトでイネーブルであり、設定することはできません。

ステップ 5　インターフェイスがまだイネーブルでない場合は、[Enable Interface] チェックボックスをオンにします。

ステップ 6　IP アドレスを設定するには、次のいずれかのオプションを使用します。

（注）　フェールオーバーとともに使用する場合は、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 はサポートされません。[Configuration] > [Device Management] > [High Availability] > [Failover] > [Interfaces] タブのスタンバイ 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、[Use Static IP] オプション ボタンをクリックして IP アドレスとマスクを入力します。
- DHCP サーバから IP アドレスを取得するには、[Obtain Address via DHCP] オプション ボタンをクリックします。



a. MAC アドレスがオプション 61 の DHCP 要求パケット内に保存されるようにするには、[Use MAC Address] オプション ボタンをクリックします。

いくつかの ISP はインターフェイスの MAC アドレスにオプション 61 が必要です。MAC アドレスが DHCP 要求パケットに含まれていない場合、IP アドレスは割り当てられません。

b. オプション 61 用に生成された文字列を使用するには、[Use "Cisco-<MAC>-<interface_name>-<host>"] をクリックします。

c. （任意）DHCP サーバからデフォルト ルートを取得するには、[Obtain Default Route Using DHCP] をオンにします。

d. （任意）DHCP クライアントが IP アドレス要求の探索を送信する場合に、DHCP パケット ヘッダーでブロードキャスト フラグを 1 に設定するには、[Enable DHCP Broadcast flag for DHCP request and discover messages] をオンにします。

DHCP サーバはこのブロードキャスト フラグをリッスンし、フラグが 1 に設定されている場合は応答パケットをブロードキャストします。

e. （任意）リースを更新するには、[Renew DHCP Lease] をクリックします。

ステップ 7　（任意）[Description] フィールドに、このインターフェイスの説明を入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。

（注）　（ASA 5510 以降、シングル モード）[Configure Hardware Properties] ボタンに関する情報については、「物理インターフェイスのイネーブル化およびイーサネット パラメータの設定」（P.11-26）を参照してください。

ステップ 8　[OK] をクリックします。

グローバル IPv6 アドレスとその他のオプションの設定

管理インターフェイスのグローバル IPv6 アドレスおよびその他のオプションを設定するには、次の手順を実行します。

（注）　グローバル アドレスを設定すると、リンクローカル アドレスは自動的に設定されるため、別々に設定する必要はありません。

制約事項

ASA は、IPv6 エニーキャスト アドレスはサポートしません。

前提条件

- 第 11 章「インターフェイス コンフィギュレーションの開始（ASA 5510 以降）」または第 12 章「インターフェイス コンフィギュレーションの開始（ASA 5505）」の手順を実行します。
- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システムからコンテキスト コンフィギュレーションに変更するには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

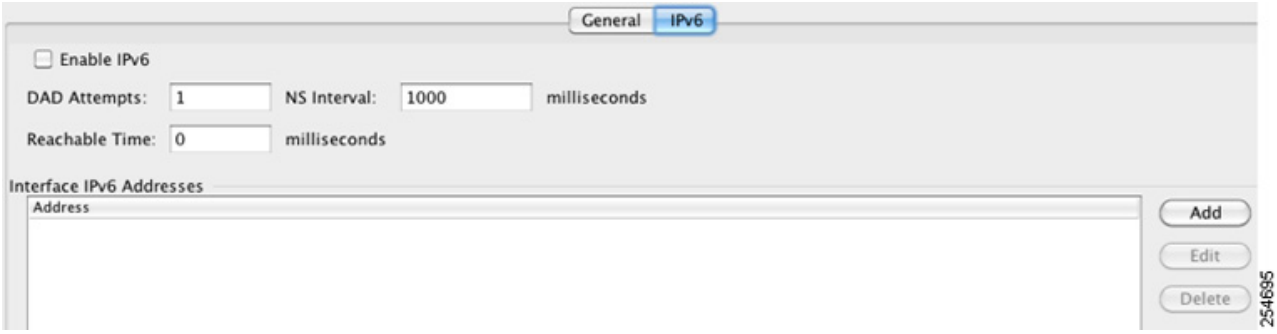
手順の詳細

ステップ 1　[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。

ステップ 2　管理インターフェイスを選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

ステップ 3　[IPv6] タブをクリックします。



ステップ 4　（任意）ローカル リンクの IPv6 アドレスに Modified EUI-64 形式のインターフェイス識別子の使用を適用するには、[Enforce EUI-64] チェックボックスをオンにします。

詳細については、「Modified EUI-64 インターフェイス ID」（P.15-6）を参照してください。

ステップ 5　グローバル IPv6 アドレスを設定する場合：

a.　[Interface IPv6 Addresses] エリアで、[Add] をクリックします。

[Add IPv6 Address for Interface] ダイアログボックスが表示されます。

b. [Address/Prefix Length] フィールドに、グローバル IPv6 アドレスと IPv6 プレフィックスの長さを入力します。たとえば、「2001:0DB8::BA98:0:3210/48」のように入力します。IPv6 アドレッシングの詳細については、「IPv6 アドレス」（P.48-5）を参照してください。

c. [OK] をクリックします。

ステップ 6　（任意）最上部のエリアで、次のオプションを設定して IPv6 設定をカスタマイズします。

- [DAD Attempts]：この設定では、DAD が IPv6 アドレスで実行されている間に、インターフェイスに連続して送信されるネイバー送信要求メッセージの数を設定します。0 ～ 600 の範囲の値を指定できます。この値がゼロの場合、指定されたインターフェイスでの DAD 処理がディセーブルになります。デフォルトは 1 メッセージです。
- [NS Interval]：ネイバー送信要求メッセージの間隔を入力します。ネイバー送信要求メッセージは、ターゲット ノードのリンク層アドレスを要求します。有効値の範囲は、1000 ～ 3600000 ミリ秒です。デフォルトは 1000 ミリ秒です。
- [Reachable Time]：到達可能性確認イベントの発生後、リモート IPv6 ノードが到達可能と見なされる秒単位の時間を入力します。有効値の範囲は、0 ～ 3600000 ミリ秒です。デフォルトは 0 です。設定時間によって、使用不可のネイバーを検知できます。時間を短く設定すればするほど、速く検知できますが、通常の IPv6 の動作では、極端に短い時間を設定することはお勧めしません。

ステップ 7　[OK] をクリックします。

[Configuration] > [Device Setup] > [Interfaces] ペインに戻ります。

次の作業

（任意）MAC アドレスと MTU を設定します。「MAC アドレス、MTU、TCP MSS の設定」（P.15-15）を参照してください。

MAC アドレス、MTU、TCP MSS の設定

ここでは、インターフェイスの MAC アドレスの設定方法、MTU の設定方法、TCP MSS の設定方法を説明します。

MAC アドレスに関する情報

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。

冗長インターフェイスは、追加した最初の物理インターフェイスの MAC アドレスを使用します。コンフィギュレーションでメンバ インターフェイスの順序を変更すると、MAC アドレスは、リストの最初になったインターフェイスの MAC アドレスと一致するように変更されます。このコマンドを使用して冗長インターフェイスに MAC アドレスを割り当てると、メンバ インターフェイスの MAC アドレスに関係なく、割り当てた MAC アドレスが使用されます。

EtherChannel の場合は、そのチャネル グループに含まれるすべてのインターフェイスが同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワーク アプリケーションとユーザに対してトランスペアレントになります。ネットワーク アプリケーションやユーザから見えるのは 1 つの論理接続のみであり、個々のリンクのことは認識しないからです。ポート チャネル インターフェイスは、最も小さいチャネル グループ インターフェイスの MAC アドレスをポート チャネル MAC アドレスとして使用します。または、ポートチャネル インターフェイスの MAC アドレスを手動で設定することもできます。マルチ コンテキスト モードでは、EtherChannel ポート インターフェイスを含め、固有の MAC アドレスをインターフェイスに自動的に割り当てることができます。グループ チャネル

インターフェイスのメンバーシップを変更する場合は、固有の MAC アドレスを手動で設定するか、またはマルチ コンテキスト モードで自動的に設定することを推奨します。ポートチャネル MAC アドレスを提供していたインターフェイスを削除すると、そのポートチャネルの MAC アドレスは次に番号が小さいインターフェイスに変わるため、トラフィックが分断されます。

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、ASA 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、「ASA によるパケットの分類方法」（P.8-3）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.8-24）を参照してください。MAC アドレスを自動生成する場合、この手順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。

MTU および TCP MSS に関する情報

「最大伝送単位および TCP 最大セグメント サイズのフラグメンテーションの制御」（P.11-8）を参照してください。

前提条件

- 第 11 章「インターフェイス コンフィギュレーションの開始（ASA 5510 以降）」または第 12 章「インターフェイス コンフィギュレーションの開始（ASA 5505）」の手順を実行します。
- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システムからコンテキスト コンフィギュレーションに変更するには、[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順の詳細

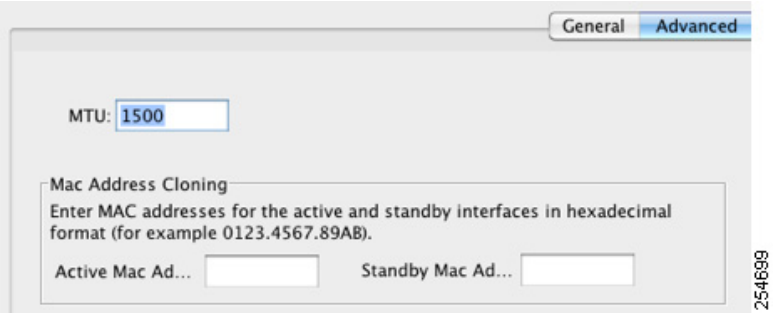
ステップ 1　[Configuration] > [Device Setup] > [Interfaces] ペインを選択します。

BVI は、物理インターフェイス、サブインターフェイス、冗長インターフェイス、EtherChannel ポートチャネル インターフェイスとともにテーブルに表示されます。マルチ コンテキスト モードでは、システム実行スペースでコンテキストに割り当てられたインターフェイスだけがテーブルに表示されます。

ステップ 2　物理インターフェイス、サブインターフェイス、冗長インターフェイス、または EtherChannel ポート インターフェイスの行を選択して、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが、[General] タブが選択された状態で表示されます。

ステップ 3　[Advanced] タブをクリックします。



ステップ 4　MTU を設定する、またはジャンボ フレームのサポート（サポートされているモジュール）をイネーブルにするには、[MTU] フィールドに 300 ～ 65,535 バイトの範囲の値を入力します。

デフォルトは 1500 バイトです。

（注）　冗長インターフェイスまたはポートチャネル インターフェイスに MTU を設定すると、ASA は、この設定をすべてのメンバ インターフェイスに適用します。

- ジャンボ フレームをサポートする、シングル モードのモデルの場合：いずれかのインターフェイスに 1500 を超える値を入力すると、ジャンボ フレーム サポートがすべてのインターフェイスに対して自動的にイネーブルになります。すべてのインターフェイスの MTU の設定を 1500 未満に戻すと、ジャンボ フレーム サポートがディセーブルになります。
- ジャンボ フレームをサポートしているモジュールの場合：いずれかのインターフェイスに 1500 を超える値を入力する場合は、必ずシステム コンフィギュレーションのジャンボ フレーム サポートをイネーブルにしてください。「ジャンボ フレーム サポートのイネーブル化（サポート対象のモデル）」（P.11-41）を参照してください。

（注）　ジャンボ フレーム サポートをイネーブルまたはディセーブルにするには、ASA をリブートする必要があります。

ジャンボ フレームとは、標準的な最大値 1518 バイト（レイヤ 2 ヘッダーおよび FCS を含む）より大きく、9216 バイトまでのイーサネット パケットのことです。ジャンボ フレームでは、処理を行うためにさらにメモリが必要となります。また、ジャンボ フレームに割り当てるメモリが多くなると、アクセス リストなどの他の機能が制限され最大限に利用できなくなる場合があります。

ステップ 5　MAC アドレスをこのインターフェイスに手動で割り当てるには、[Active Mac Address] フィールドに MAC アドレスを H.H.H 形式（H は 16 ビットの 16 進数）で入力します。

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。自動生成された MAC アドレスも使用する場合、手動で割り当てる MAC アドレスの最初の 2 バイトには A2 を使用できません。

ステップ 6　フェールオーバーを使用する場合、[Standby Mac Address] フィールドにスタンバイ MAC アドレスを入力します。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。

ステップ 7　TCP MSS を設定するには、[Configuration] > [Firewall] > [Advanced] > [TCP Options] の順に選択します。次のオプションを設定します。

- [Force Maximum Segment Size for TCP]：最大 TCP セグメント サイズを 48 から最大数の範囲のバイト数で設定します。デフォルト値は 1380 バイトです。この機能は、0 バイトに設定することによってディセーブルにできます。

- [Force Minimum Segment Size for TCP] : 48 から最大数の間で、ユーザが設定したバイト数未満にならないように最大セグメント サイズを上書きします。この機能は、デフォルトでディセーブルです（0 に設定）。

同じセキュリティ レベルの通信の許可

デフォルトでは、同じセキュリティ レベルのインターフェイスは相互に通信することができません。また、パケットは同じインターフェイスを出入りすることができません。ここでは、複数のインターフェイスが同じセキュリティ レベルの場合にインターフェイス間通信をイネーブルにする方法について説明します。

インターフェイス間通信に関する情報

同じセキュリティ レベルのインターフェイスが互いに通信できるようにすると、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する場合に便利です。

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。

手順の詳細

同じセキュリティ 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には、[Configuration] > [Interfaces] ペインで、[Enable traffic between two or more interfaces which are configured with same security level] をオンにします。

インターフェイスのモニタリング

モニタリング画面の詳細については、「インターフェイスのモニタリング」（P.14-24）を参照してください。

トランスペアレント モードのインターフェイスの機能履歴

表 15-1 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 15-1　トランスペアレント モードのインターフェイスの機能履歴

機能名	プラットフォーム リリース	機能情報
VLAN 数の増加	7.0(5)	次の制限値が増加されました。 • ASA 5510 基本ライセンスの VLAN 数が 0 から 10 に増えました。 • ASA 5510 Security Plus ライセンスの VLAN 数が 10 から 25 に増えました。 • ASA 5520 の VLAN 数が 25 から 100 に増えました。 • ASA 5540 の VLAN 数が 100 から 200 に増えました。
VLAN 数の増加	7.2(2)	ASA 5505 ASA 上の Security Plus ライセンスに対する VLAN 最大数が、5（3 つのフル機能インターフェイス、1 つのフェールオーバー インターフェイス、1 つのバックアップ インターフェイスに制限されるインターフェイス）から 20 のフル機能インターフェイスに増加されました。また、トランク ポート数も 1 から 8 に増加されました。フル機能のインターフェイスの数が 20 になり、バックアップ ISP インターフェイスを停止するために backup interface コマンドを使用する必要がなくなりました。つまり、バックアップ ISP インターフェイス用にフル機能のインターフェイスを使用できるようになりました。backup interface コマンドは、これまでどおり Easy VPN 設定用に使用できます。 VLAN の制限値も変更されました。ASA 5510 ASA の基本ライセンスでは 10 から 50 に、Security Plus ライセンスでは 25 から 100 に、ASA 5520 ASA では 100 から 150 に、ASA 5550 ASA では 200 から 250 に増えています。
ASA 5510 Security Plus ライセンスに対するギガビット イーサネット サポート	7.2(3)	ASA 5510 ASA は、GE（ギガビット イーサネット）を Security Plus ライセンスのあるポート 0 および 1 でサポートするようになりました。ライセンスを Base から Security Plus にアップグレードした場合、外部 Ethernet 0/0 および Ethernet 0/1 ポートの容量は、元の FE（ファスト イーサネット）の 100 Mbps から GE の 1000 Mbps に増加します。インターフェイス名は Ethernet 0/0 および Ethernet 0/1 のままです。
ASA 5505 に対するネイティブ VLAN サポート	7.2(4)/8.0(4)	ネイティブ VLAN を ASA 5505 トランク ポートに割り当てることができるようになりました。 次の画面が変更されました。[Configuration] > [Device Setup] > [Interfaces] > [Switch Ports] > [Edit Switch Port]。

表 15-1　トランスペアレント モードのインターフェイスの機能履歴 （続き）

機能名	プラットフォーム リリース	機能情報
ASA 5580 に対するジャンボ パケット サポート	8.1(1)	Cisco ASA 5580 はジャンボ フレームをサポートしています。ジャンボ フレームとは、標準的な最大値 1518 バイト（レイヤ 2 ヘッダーおよび FCS を含む）より大きく、9216 バイトまでのイーサネット パケットのことです。イーサネット フレームを処理するためのメモリ容量を増やすことにより、すべてのインターフェイスに対してジャンボ フレームのサポートをイネーブルにできます。ジャンボ フレームに割り当てるメモリを増やすと、他の機能（アクセス リストなど）の最大使用量が制限される場合があります。 次の画面が変更されました。[Configuration] > [Device Setup] > [Interfaces] > [Add/Edit Interface] > [Advanced]。
ASA 5580 の VLAN 数の増加	8.1(2)	ASA 5580 上でサポートされる VLAN 数が 100 から 250 に増加されました。
トランスペアレント モードの IPv6 のサポート	8.2(1)	トランスペアレント ファイアウォール モードの IPv6 サポートが導入されました。
ASA 5580 10 ギガビット イーサネット インターフェイスでのフロー制御のポーズ フレームのサポート	8.2(2)	フロー制御のポーズ（XOFF）フレームをイネーブルにできるようになりました。 次の画面が変更されました。 （シングル モード）[Configuration] > [Device Setup] > [Interfaces] > [Add/Edit Interface] > [General] （マルチ モード、システム）[Configuration] > [Interfaces] > [Add/Edit Interface]
トランスペアレント モードのブリッジ グループ（第 14 章「インターフェイス コンフィギュレーションの実行（トランスペアレント モード、8.4 以降)」を参照）	8.4(1)	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、インターフェイスをブリッジ グループにグループ化し、各ネットワークに 1 つずつ複数のブリッジ グループを設定できます。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ます。シングル モードまたはコンテキストごとに、それぞれ 4 つのインターフェイスからなる最大 8 個のブリッジ グループを設定できます。 次の画面が変更または導入されました。 [Configuration] > [Device Setup] > [Interfaces] [Configuration] > [Device Setup] > [Interfaces] > [Add/Edit Bridge Group Interface] [Configuration] > [Device Setup] > [Interfaces] > [Add/Edit Interface]