CHAPTER 13

インターフェイス コンフィギュレーションの実行（ルーテッド モード）

この章では、ルーテッド 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。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。設定するコンテキストに切り替えるには、**changeto context** *name* コマンドを入力します。

ルーテッド 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の概要

この項は、次の内容で構成されています。

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.13-17）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.13-17）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。

デュアル IP スタック（IPv4 および IPv6）

ASA は、1 つのインターフェイス上で IPv6 と IPv4 の両方のコンフィギュレーションをサポートします。そのために特別なコマンドを入力する必要はありません。単純に、IPv4 コンフィギュレーション コマンドと IPv6 コンフィギュレーション コマンドを通常と同じように入力します。IPv4 と IPv6 の両方で、デフォルト ルートを設定してください。

ルーテッド モード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ライセンス要件

モデル	ライセンス要件
ASA 5505	VLAN： 基本ライセンス：3（2 つの正規ゾーンともう 1 つの制限ゾーンだけが他の 1 つのゾーンと通信可能） Security Plus ライセンス：20 VLAN トランク： 基本ライセンス：なし。 Security Plus ライセンス：8 すべての種類のインターフェイス[1]： 基本ライセンス：52。 Security Plus ライセンス：120。

1. VLAN、物理、冗長、およびブリッジ グループ インターフェイスなど、すべてを合わせたインターフェイスの最大数。

モデル	ライセンス要件
ASA 5510	VLAN： 基本ライセンス：50 Security Plus ライセンス：100 インターフェイス速度： 基本ライセンス：すべてのインターフェイスがファスト イーサネット。 Security Plus ライセンス：Ethernet 0/0 および 0/1：ギガビット イーサネット、その他すべてはファスト イーサネット。 すべての種類のインターフェイス[1]： 基本ライセンス：52 Security Plus ライセンス：120
ASA 5520	VLAN： 基本ライセンス：150 すべての種類のインターフェイス[1]： 基本ライセンス：640
ASA 5540	VLAN： 基本ライセンス：200 すべての種類のインターフェイス[1]： 基本ライセンス：840

モデル	ライセンス要件
ASA 5550	VLAN： 基本ライセンス：400 すべての種類のインターフェイス[1]： 基本ライセンス：1640
ASA 5580	VLAN： 基本ライセンス：1024 すべての種類のインターフェイス[1]： 基本ライセンス：4176
ASA 5512-X	VLAN： 基本ライセンス：50 すべての種類のインターフェイス[1]： 基本ライセンス：328
ASA 5515-X	VLAN： 基本ライセンス：100 すべての種類のインターフェイス[1]： 基本ライセンス：528
ASA 5525-X	VLAN： 基本ライセンス：200 すべての種類のインターフェイス[1]： 基本ライセンス：928
ASA 5545-X	VLAN： 基本ライセンス：300 すべての種類のインターフェイス[1]： 基本ライセンス：1328
ASA 5555-X	VLAN： 基本ライセンス：500 すべての種類のインターフェイス[1]： 基本ライセンス：2128
ASA 5585-X	VLAN： 基本ライセンス：1024 SSP-10 および SSP-20 のインターフェイス速度： 基本ライセンス：ファイバ インターフェイスの場合 1 ギガビット イーサネット 10 GE I/O ライセンス（Security Plus）：ファイバ インターフェイスの場合 10 ギガビット イーサネット （SSP-40 および SSP-60 は 10 ギガビット イーサネットをデフォルトでサポートします）。 すべての種類のインターフェイス[1]： 基本ライセンス：4176

1. VLAN、物理、冗長、ブリッジ グループ、および EtherChannel インターフェイスなど、すべてを合わせたインターフェイスの最大数。

モデル	ライセンス要件
ASASM	VLAN： 基本ライセンス：1000

ガイドラインと制限事項

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 モードでの ASA 5510 以降の場合、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。マルチ コンテキスト モードの ASASM の場合は、スイッチのスイッチポートおよび VLAN を設定し、第 2 章「ASA サービス モジュール を使用するためのスイッチの設定」に従って VLAN を ASASM に割り当てます。

  ASA 5505 はマルチ コンテキスト モードをサポートしません。

- マルチ コンテキスト モードで設定できるのは、「マルチ コンテキストの設定」（P.6-15）に従ってシステム 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。

- PPPoE は、マルチ コンテキスト モードではサポートされていません。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードでサポートされています。トランスペアレント モードの場合は、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）」を参照してください。

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 リンクおよびステート リンクの設定については、「アクティブ/スタンバイ フェールオーバーの設定」（P.9-8）または「アクティブ/アクティブ フェールオーバーの設定」（P.10-9）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。

ASASM の 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 ASA に割り当てられた VLAN だけです。ASA に割り当てられたすべての VLAN を表示するには、**show vlan** コマンドを使用します。

スイッチによって ASA 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。ASA 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。

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.3-18）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。

ASASM のインターフェイスのデフォルトの状態

- シングル モードまたはシステム実行スペースでは、VLAN インターフェイスがデフォルトでイネーブルになります。
- 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。

ジャンボ フレーム サポート

デフォルトでは、ASASM はジャンボ フレームをサポートしています。「MAC アドレスおよび MTU の設定」（P.13-10）に従って、目的のパケット サイズの MTU を設定します。

ルーテッド 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

この項は、次の内容で構成されています。

- 「IPv6 アドレッシングの設定」（P.13-14）
- 「同じセキュリティ レベルの通信の許可」（P.13-17）

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　モデルに応じてインターフェイスを設定します。

- ASA 5510 以降：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）」
- ASA 5505：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）」
- ASASM：第 2 章「ASA サービス モジュール を使用するためのスイッチの設定」

ステップ 2　（マルチ コンテキスト モード）「マルチ コンテキストの設定」（P.6-15）に従って、コンテキストにインターフェイスを割り当てます。

ステップ 3　（マルチ コンテキスト モード）設定するコンテキストに切り替えるには、**changeto context** *name* コマンドを入力します。インターフェイス名、セキュリティ レベル、IPv4 アドレス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.13-7）を参照してください。

ステップ 4　（任意）MAC アドレスと MTU を設定します。「MAC アドレスおよび MTU の設定」（P.13-10）を参照してください。

ステップ 5　（任意）IPv6 アドレッシングを設定します。「IPv6 アドレッシングの設定」（P.13-14）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、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.13-17）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

この手順では、名前、セキュリティ レベル、IPv4 アドレス、およびその他のオプションを設定する方法について説明します。

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
- EtherChannel インターフェイス

ASA 5505 および ASASM 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

ガイドラインと制限事項

- ASA 5550 では、スループットを最大にするために、トラフィックを 2 つのインターフェイス スロットに分散してください。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。

- 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、「アクティブ/スタンバイ フェールオーバーの設定」（P.9-8）または「アクティブ/アクティブ フェールオーバーの設定」（P.10-9）を参照してください。

制限事項

- PPPoE は、マルチ コンテキスト モードではサポートされていません。
- ASASM では、PPPoE および DHCP はサポートされません。

前提条件

- モデルに応じてインターフェイスを設定します。
  - ASA 5510 以降：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）」
  - ASA 5505：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）」
  - ASASM：第 2 章「ASA サービス モジュール を使用するためのスイッチの設定」
- マルチ コンテキスト モードで設定できるのは、「マルチ コンテキストの設定」（P.6-15）に従ってシステム 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。
- 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 コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、**changeto context** *name* コマンドを入力します。

手順の詳細

	コマンド	目的
ステップ 1	ASA 5510 以降の場合： **interface** {{**redundant** *number* | **port-channel** *number* | *physical_interface*}[.*subinterface*] | *mapped_name*} ASA 5505 または ASASM の場合： hostname(config)# **interface** {**vlan** *number* | *mapped_name*} **例：** hostname(config)# interface gigabithethernet 0/0	まだインターフェイス コンフィギュレーション モードを開始していない場合は、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。 **redundant** *number* 引数には、冗長インターフェイス ID（**redundant 1** など）を指定します。 **port-channel** *number* 引数は、**port-channel 1** などの EtherChannel インターフェイス ID です。 物理インターフェイス ID 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」の説明を参照してください。 *subinterface* ID は、物理インターフェイス ID または冗長インターフェイス 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 **mapped_name** に入力します。
ステップ 2	**nameif** *name* **例：** hostname(config-if)# nameif inside	インターフェイスに名前を付けます。 *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	次のいずれかを実行します。	
	ip address *ip_address* [*mask*] [**standby** *ip_address*] **例：** hostname(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2	IP アドレスを手動で設定します。 **（注）**　フェールオーバーで使用する場合、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_address* 引数および *mask* 引数には、インターフェイスの IP アドレスとサブネット マスクを設定します。 **standby** *ip_address* 引数は、フェールオーバーで使用します。詳細については、「アクティブ/スタンバイ フェールオーバーの設定」（P.9-8）または「アクティブ/アクティブ フェールオーバーの設定」（P.10-9）を参照してください。
	ip address dhcp [**setroute**] **例：** hostname(config-if)# ip address dhcp	DHCP サーバから IP アドレスを取得します。 **setroute** キーワードを指定すると、ASA が DHCP サーバから渡されたデフォルト ルートを使用できるようになります。 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。

	コマンド	目的
	PPPoE サーバからの IP アドレスの取得については、第 76 章「PPPoE クライアントの設定」を参照してください。	PPPoE は、マルチ コンテキスト モードではサポートされていません。
ステップ 4	**security-level** *number* **例：** `hostname(config-if)# security-level 50`	セキュリティ レベルを設定します。*number* には、0（最下位）～ 100（最上位）の整数を指定します。「セキュリティ レベル」（P.13-1）を参照してください。
ステップ 5	（任意） **management-only** **例：** `hostname(config-if)# management-only`	インターフェイスを管理専用モードに設定してトラフィックが通過しないようにします。 デフォルトでは、管理インターフェイスは管理専用として設定されます。この設定をディセーブルにするには、**no management-only** コマンドを入力します。 （ASA 5512-X ～ ASA 5555-X）管理 0/0 インターフェイスの **management-only** をディセーブルにすることはできません。 **management-only** コマンドは、冗長インターフェイスではサポートされません。

例

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、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。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
```

次の作業

- （任意）MAC アドレスと MTU を設定します。「MAC アドレスおよび MTU の設定」（P.13-10）を参照してください。
- （任意）IPv6 アドレッシングを設定します。「IPv6 アドレッシングの設定」（P.13-14）を参照してください。

MAC アドレスおよび MTU の設定

この項では、インターフェイスに MAC アドレスおよび MTU を設定する方法について説明します。

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。

ASASM では、すべての VLAN がバックプレーンから提供される同じ 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.6-3）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.6-24）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 に関する情報

MTU は接続で送信される最大データグラム サイズです。MTU 値よりも大きいデータは、送信前にフラグメント化されます。

ASA は、IP パス MTU ディスカバリを（RFC 1191 での規定に従って）サポートします。これにより、ホストはパスに沿ったさまざまなリンクで許容される最大 MTU サイズをダイナミックに検出し、各サイズの差に対処できます。パケットがインターフェイスに対して設定されている MTU よりも大きくなっているものの、「Don't Fragment」（DF）ビットが設定されているために、ASA がデータグラムを転送できないことがあります。ネットワーク ソフトウェアは、メッセージを送信ホストに送信して、問題を警告します。送信ホストは、パスに沿ったすべてのリンクのうち最小のパケット サイズに適合するように、宛先へのパケットをフラグメント化する必要があります。

デフォルトの MTU は、イーサネット インターフェイスのブロックでは 1500 バイトです。ほとんどのアプリケーションではこの値で十分ですが、ネットワーク状況によってはこれよりも小さい値にすることもできます。

ジャンボ フレームはデフォルトで ASASM でサポートされます。ジャンボ フレームをイネーブルにするには、「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.11-35）を参照してください。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。ジャンボ フレームを使用するには、値を大きくします（たとえば 9000 バイト）。

前提条件

- モデルに応じてインターフェイスを設定します。
  - ASA 5510 以降：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）」
  - ASA 5505：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）」
  - ASASM：第 2 章「ASA サービス モジュール を使用するためのスイッチの設定」
- マルチ コンテキスト モードで設定できるのは、「マルチ コンテキストの設定」（P.6-15）に従ってシステム 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。
- 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 コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、**changeto context** *name* コマンドを入力します。

手順の詳細

	コマンド	目的
ステップ 1	ASA 5510 以降の場合： **interface** {{**redundant** *number* | **port-channel** *number* | *physical_interface*}[*.subinterface*] | *mapped_name*} ASA 5505 または ASASM の場合： hostname(config)# **interface** {**vlan** *number* | *mapped_name*} **例：** hostname(config)# interface vlan 100	まだインターフェイス コンフィギュレーション モードを開始していない場合は、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。 **redundant** *number* 引数には、冗長インターフェイス ID（**redundant 1** など）を指定します。 **port-channel** *number* 引数は、**port-channel 1** などの EtherChannel インターフェイス ID です。 物理インターフェイス ID 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」の説明を参照してください。 *subinterface* ID は、物理インターフェイス ID または冗長インターフェイス 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 **mapped_name** に入力します。
ステップ 2	**mac-address** *mac_address* [**standby** *mac_address*] **例：** hostname(config-if)# mac-address 000C.F142.4CDE	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ます。*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 00-0C-F1-42-4C-DE は、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。 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。
ステップ 3	**mtu** *interface_name bytes* **例：** hostname(config)# mtu inside 9200	MTU を 300 ～ 65,535 バイトの間で設定します。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モデルでは、インターフェイスに 1500 よりも大きな値を入力する場合、ジャンボ フレームのサポートをイネーブルにする必要があります。「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.11-35）を参照してください。

次の作業

（任意）IPv6 アドレッシングを設定します。「IPv6 アドレッシングの設定」（P.13-14）を参照してください。

IPv6 アドレッシングの設定

この項では、IPv6 アドレッシングを設定する方法について説明します。IPv6 の詳細については、「IPv6 アドレス」（P.B-5）を参照してください。

この項は、次の内容で構成されています。

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。
- 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。

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と、リンクローカル アドレスがインターフェイスに自動的に設定されるため、リンクローカル アドレスを個別に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。

（注）　リンクローカル アドレスの設定だけを行う場合は、コマンド リファレンスの **ipv6 enable** コマンド（自動設定）または **ipv6 address link-local** コマンド（手動設定）を参照してください。

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。

グローバル IPv6 アドレスの設定

グローバル IPv6 アドレスを設定するには、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。

制限事項

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

- モデルに応じてインターフェイスを設定します。
  - ASA 5510 以降：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）」
  - ASA 5505：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）」
  - ASASM：第 2 章「ASA サービス モジュール を使用するためのスイッチの設定」
- マルチ コンテキスト モードで設定できるのは、「マルチ コンテキストの設定」（P.6-15）に従ってシステム 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。
- 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 コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、**changeto context** *name* コマンドを入力します。

手順の詳細

	コマンド	目的
ステップ 1	ASA 5510 以降の場合： **interface** {{**redundant** *number* | **port-channel** *number* | *physical_interface*}[.*subinterface*] | *mapped_name*} ASA 5505 または ASASM の場合： hostname(config)# **interface** {**vlan** *number* | *mapped_name*} **例：** hostname(config)# interface gigabithethernet 0/0	まだインターフェイス コンフィギュレーション モードを開始していない場合は、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。 **redundant** *number* 引数には、冗長インターフェイス ID（**redundant 1** など）を指定します。 **port-channel** *number* 引数は、**port-channel 1** などの EtherChannel インターフェイス ID です。 物理インターフェイス ID 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」の説明を参照してください。 *subinterface* ID は、物理インターフェイス ID または冗長インターフェイス 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 **mapped_name** に入力します。
ステップ 2	次のいずれかを実行します。	
	ipv6 address autoconfig **例：** hostname(config-if)# ipv6 address autoconfig	インターフェイスでステートレスな自動設定をイネーブルにします。インターフェイスでステートレスな自動設定をイネーブルにすると、ルータ アドバタイズメント メッセージで受信したプレフィックスに基づいて IPv6 アドレスが設定されます。ステートレスな自動設定がイネーブルになっている場合、インターフェイスのリンクローカル アドレスは、Modified EUI-64 インターフェイス ID に基づいて自動的に生成されます。 **（注）** RFC 4862 では、ステートレス自動設定に設定されたホストは、ルータ アドバタイズメント メッセージを送信しないと規定されていますが、この場合、ASA はルータ アドバタイズメント メッセージを送信します。メッセージを抑制するには、**ipv6 nd suppress-ra** コマンドを参照してください。
	ipv6 address *ipv6-address/prefix-length* [**standby** *ipv6-address*] **例：** hostname(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48	インターフェイスにグローバル アドレスを割り当てます。グローバル アドレスを割り当てると、インターフェイスのリンクローカル アドレスが自動的に作成されます。 **standby** は、フェールオーバー ペアのセカンダリ ユニットまたはフェールオーバー グループで使用されるインターフェイス アドレスを指定します。 IPv6 アドレッシングの詳細については、「IPv6 アドレス」（P.B-5）を参照してください。

	コマンド	目的
	ipv6 address *ipv6-prefix/prefix-length* **eui-64** **例：** hostname(config-if)# ipv6 address 2001:0DB8::BA98::/48 eui-64	Modified EUI-64 形式を使用してインターフェイスの MAC アドレスから生成されたインターフェイス ID と、指定されたプレフィックスを結合することによって、インターフェイスにグローバル アドレスを割り当てます。グローバル アドレスを割り当てると、インターフェイスのリンクローカル アドレスが自動的に作成されます。 スタンバイ アドレスを指定する必要はありません。インターフェイス ID が自動的に生成されます。 IPv6 アドレッシングの詳細については、「IPv6 アドレス」（P.B-5）を参照してください。
ステップ 3	（任意） **ipv6 enforce-eui64** *if_name* **例：** hostname(config)# ipv6 enforce-eui64 inside	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します。 *if_name* 引数には、**nameif** コマンドで指定したインターフェイスの名前を指定します。このインターフェイスに対してアドレス形式を適用できます。 詳細については、「Modified EUI-64 インターフェイス ID」（P.13-14）を参照してください。

IPv6 ネイバー探索の設定

IPv6 ネイバー探索を設定するには、第 32 章「IPv6 ネイバー探索の設定」を参照してください。

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。この項では、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と、インターフェイス内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で相互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。

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。

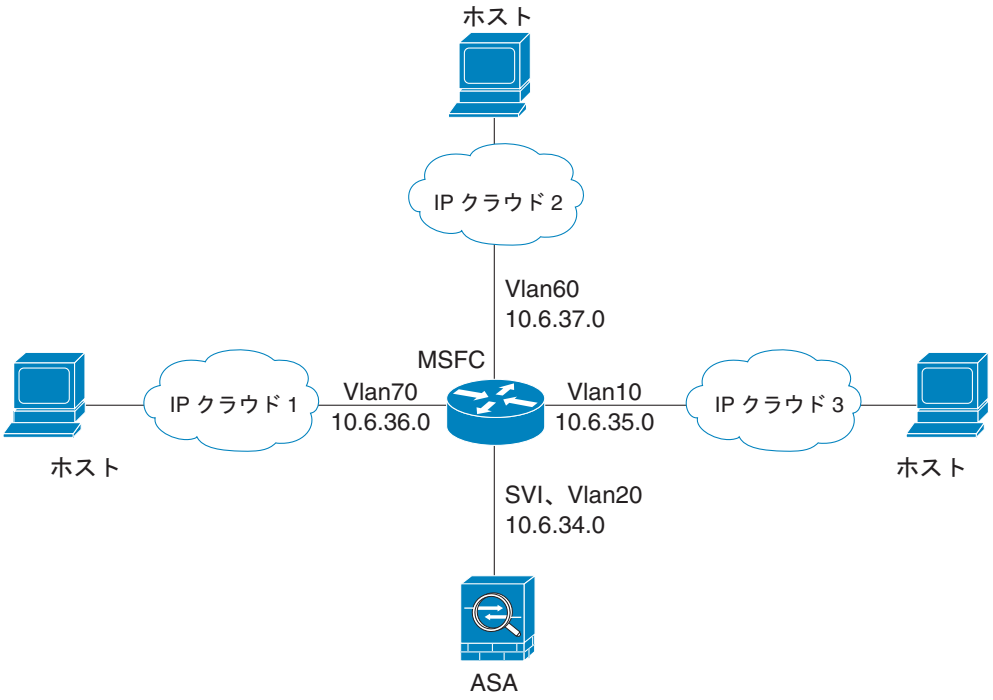
インターフェイス内通信に関する情報

インターフェイス内通信は、インターフェイスに入ってくる VPN トラフィックに対して使用できますが、その場合は同じインターフェイスのルートから外されます。この場合、VPN トラフィックは暗号化解除されたり、別の VPN 接続のために再度暗号化されたりする場合があります。たとえば、ハブ アンド スポーク VPN ネットワークがあり、ASA がハブ、リモート VPN ネットワークがスポークの場合、あるスポークが別のスポークと通信するためには、トラフィックは ASA に入ってから他のスポークに再度ルーティングされる必要があります。

（注） この機能で許可されたすべてのトラフィックは、引き続きファイアウォール規則に従います。リターン トラフィックが ASA を通過できない原因となるため、非対称なルーティング状態にしないよう注意してください。

ASASM の場合、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、ASA 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 13-1 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。

図 13-1　同一インターフェイス上のホスト間の通信



次の設定例では、図 13-1 に示すネットワークのポリシー ルーティングをイネーブルにするために使用される Cisco IOS **route-map** コマンドを示します。

```
route-map intra-inter3 permit 0
    match ip address 103
    set interface Vlan20
    set ip next-hop 10.6.34.7
!
route-map intra-inter2 permit 20
    match ip address 102
    set interface Vlan20
```

```
    set ip next-hop 10.6.34.7
!
route-map intra-inter1 permit 10
    match ip address 101
    set interface Vlan20
    set ip next-hop 10.6.34.7
```

手順の詳細

コマンド	目的
same-security-traffic permit inter-interface	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します。
same-security-traffic permit intra-interface	同じインターフェイスに接続されたホスト間の通信をイネーブルにします。

インターフェイスのオン/オフ

ここでは、インターフェイスのオン/オフの方法について説明します。

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。マルチ コンテキスト モードでは、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は、そのコンテキスト インターフェイスだけが影響を受けます。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インターフェイスに影響します。

手順の詳細

	コマンド	目的
ステップ 1	hostname(config)# **interface** {**vlan** *number* | *mapped_name*} **例：** hostname(config)# interface vlan 100	まだインターフェイス コンフィギュレーション モードを開始していない場合は、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。 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 **mapped_name** に入力します。
ステップ 2	**shutdown** **例：** hostname(config-if)# shutdown	インターフェイスをディセーブルにします。
ステップ 3	**no shutdown** **例：** hostname(config-if)# no shutdown	インターフェイスを再びイネーブルにします。

インターフェイスのモニタリング

インターフェイスをモニタするには、次のいずれかのコマンドを入力します。

コマンド	目的
show interface	インターフェイス統計情報を表示します。
show interface ip brief	インターフェイスの IP アドレスとステータスを表示します。

ルーテッド モードのインターフェイス コンフィギュレーション例

この項では、次のトピックについて取り上げます。

- 「ASA 5505 の例」（P.13-20）

ASA 5505 の例

次の例では、基本ライセンスの 3 つの VLAN インターフェイスを設定しています。3 つ目の home インターフェイスは、トラフィックを business インターフェイスに転送できません。

```
hostname(config)# interface vlan 100
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address dhcp
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif business
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 300
hostname(config-if)# no forward interface vlan 200
hostname(config-if)# nameif home
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

ルーテッド モードのインターフェイスの機能履歴

表 13-1 に、この機能のリリース履歴の一覧を示します。

表 13-1　インターフェイスの機能履歴

機能名	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 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 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 では 100 から 150 に、ASA 5550 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 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 Fast Ethernet（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。**speed** コマンドを使用してインターフェイスの速度を変更します。また、**show interface** コマンドを使用して各インターフェイスの現在の設定速度を確認します。
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。 **switchport trunk native vlan** コマンドが導入されました。

表 13-1　インターフェイスの機能履歴 （続き）

機能名	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。 **jumbo-frame reservation** コマンドが導入されました。
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。 **flowcontrol** コマンドが導入されました。