ファイアウォール デバイスの管理

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き Cisco Catalyst スイッチ、PIX、FWSM、IOS デバイス、および IPS をサポートしていますが、バグ修正や拡張機能はサポートしていません。

ここでは、Cisco セキュリティ デバイス上のセキュリティ サービスおよびポリシーの設定と管理について説明します。Cisco セキュリティ デバイスとは、Adaptive Security Appliances（ASA; 適応型セキュリティ アプライアンス）、PIX ファイアウォール、および Catalyst 6500 シリーズ スイッチ サービス モジュール（Firewall Services Module（FWSM; ファイアウォール サービス モジュール）および ASA-SM）を指しています。

この章は次のトピックで構成されています。

ファイアウォールデバイスのタイプ

Security Manager は、さまざまな Cisco セキュリティ アプライアンスやファイアウォール デバイスを検出および管理できます。その中には、特に次のものが含まれます。

- PIX 500 シリーズ ファイアウォール デバイス
- Cisco Virtual Security Appliance（ASAv）を含む ASA 5500 シリーズ セキュリティ アプライアンス
- Firepower 3100 シリーズ ファイアウォール デバイス
- セキュリティ固有の Catalyst サービスモジュール

PIX 500 シリーズ

Private Internet eXchange（PIX）500 シリーズ ファイアウォール アプライアンスは販売終了となっていますが、現在でもサポートされており、世界中で多数が使用されています。

ASA 5500 シリーズ

適応型セキュリティアプライアンス（ASA）5500 シリーズデバイスは、コンテキスト認識型ファイアウォール機能やリアルタイム脅威防御など、包括的なセキュリティサービスを提供します。ASA 5500 は、シスコのプライマリ セキュリティ アプライアンスとして PIX 500 に代わるものです。詳細については、cisco.com の「Cisco ASA 5500 Series Adaptive Security Appliance」のページを参照してください。

Cisco ASAv 仮想アプライアンスは、ASA 9.2(1) で導入され、仮想環境に包括的なファイアウォール機能を提供し、データセンタートラフィックとマルチテナント環境のセキュリティを強化します。ASAv は、VMware vSphere 上で稼働します。ASAv は仮想デバイスですが、Security Manager で他の ASA デバイスと同様に管理されます。ASAv の詳細については、「http://www.cisco.com/c/en/us/support/security/virtual-adaptive-security-appliance-firewall/tsd-products-support-series-home.html」を参照してください。

（注） ASAv は、次の ASA 機能をサポートしていません：クラスタリング、マルチコンテキストモード、アクティブ/アクティブフェールオーバー、イーサチャネル、共有 AnyConnect プレミアムライセンス。

Firepower 3100 シリーズ

Firepower 3100 シリーズ ファイアウォール デバイスのサポートは、CSM 4.24 の ASA 9.17(1) デバイスに導入されました。

Catalyst サービス モジュール

Catalyst 6500 スイッチには、ファイアウォールサービスとセキュリティサービスを提供する 2 つを含む、さまざまなサービスモジュール（SM）が用意されています。これは、スイッチシャーシに直接インストールするブレード タイプのモジュールです。

ファイアウォール サービス モジュール（FWSM）を使用すると、スイッチ上の任意のポートをファイアウォールポートとして動作させることができ、ネットワーク構造の内部のファイアウォールセキュリティを統合できます。

Adaptive Security Appliance Service Module（ASA-SM; 適応型セキュリティ アプライアンス サービス モジュール）は、レイヤ 2 から 7 で高速のセキュリティ サービスを提供し、1 台のスイッチに 4 台の ASA-SM ブレードをインストール可能にすることで、64 Gbps のスケーラビリティを提供します。

（注） ASA-SM は、物理的に FWSM と同じように、Catalyst 6500 スイッチにインストールされたブレードですが、ASA デバイスであり、そのように文書化されています。ASA-SM に関する情報については、ASA 関連のトピックを参照してください。必要な場合には、サービス モジュールと ASA アプライアンスに関する注意点および相違点が記載されています。

ファイアウォールのデフォルト設定

ファイアウォールデバイスは、すでにある程度設定された状態で出荷されています。新規で設置したファイアウォール デバイスを手動で Cisco Security Manager に追加する場合は、そのデバイスのプリセットまたはデフォルト ポリシーを見つける（インポートする）必要があります。これらのポリシーを Security Manager にインポートすることによって、そのデバイスに最初に設定を展開したときに、これらのポリシーを意図せずに削除してしまわずにすみます。ポリシーをインポートする方法の詳細については、ポリシーの検出を参照してください。

Cisco Security Manager には、多数のデバイス タイプやバージョンのデフォルト ポリシーを含む設定ファイルのセットが用意されています。これらの設定ファイルは、<install_dir>\CSCOpx\MDC\fwtools\pixplatform\ ディレクトリ（たとえば、C:\Program Files\CSCOpx\MDC\fwtools\pixplatform\）に格納されています。

ファイル名は、デバイス タイプ、オペレーティング システムのバージョン、コンテキストのサポート、および動作タイプを表しています。たとえば、「FactoryDefault_FWSM2_2_MR.cfg」は、FWSM、バージョン 2.2 で、マルチコンテキストをサポートし、ルーテッドモードで動作する場合の設定ファイルです。同様に、「FactoryDefault_ASA7_0_1_ST.cfg」は、ASA、バージョン 7.0.1、シングルコンテキストのトランスペアレントモードの設定ファイルです。

セキュリティ コンテキストの詳細については、シングルおよびマルチ コンテキストのインターフェイス （7 ページ）を、ルーテッドおよびトランスペアレント動作の詳細については、ルーテッド モードおよびトランスペアレント モードのインターフェイス （6 ページ）を参照してください。

提供されている設定ファイルから新しいデバイスを追加する方法については、設定ファイルからのデバイスの追加を参照してください。

ファイアウォール デバイスのインターフェイスの設定

[Interfaces] ページには、設定されている物理インターフェイス、論理インターフェイス、および冗長インターフェイスが表示されます。また、選択したデバイスのハードウェア ポートとブリッジ グループも表示されます。このページでは、インターフェイスを追加、編集、および削除できます。また、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可能にしたり、VPDN グループおよび PPPoE ユーザを管理したりできます。

（注） ASA 5505 デバイスに表示される [Interfaces] ページには、[Hardware Ports] および [Interfaces] の 2 つのタブ付きパネルが表示されます。同様に、トランスペアレントモードで動作している Catalyst 6500 サービス（ASA-SM および FWSM）に表示される [インターフェイス（Interfaces）] ページにも、[インターフェイス（Interfaces）] と [ブリッジグループ（Bridge Groups）] の 2 つのタブ付きパネルが表示されます。

ナビゲーション パス

[インターフェイス（Interfaces）] ページにアクセスするには、デバイスビューでセキュリティ デバイスを選択し、デバイスポリシーセレクタから [インターフェイス（Interfaces）] を選択します。

ここでは、次の内容について説明します。

- デバイス インターフェイスについて （4 ページ）
- デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （43 ページ）
- 高度なインターフェイス設定（PIX/ASA/FWSM） （110 ページ）

デバイス インターフェイスについて

インターフェイスは、セキュリティ デバイスと他のネットワーク デバイスとの間の接続ポイントです。インターフェイスは、最初はディセーブルになっています。そのため、ファイアウォール設定に不可欠な作業として、インターフェイスをイネーブルにし、適切なパケット インスペクションおよび転送を許可するように設定する必要があります。

インターフェイスには、物理インターフェイスと論理インターフェイスの2つのタイプがあります。物理インターフェイスは、ネットワーク ケーブルが差し込まれるデバイス上の実際のスロットであり、論理インターフェイスは、特定の物理ポートに割り当てられる仮想ポートです。一般的に、物理ポートはインターフェイスと呼ばれます。また、論理ポートは機能に応じて、サブインターフェイス、仮想インターフェイス、VLAN、または EtherChannel と呼ばれます。定義できるインターフェイスの数とタイプは、アプライアンス モデルおよび購入したライセンスのタイプによって異なります。

（注） PIX オペレーティングシステムのバージョン 6.3 を実行しているデバイスでは、「インターフェイス」および「サブインターフェイス」ではなく、「物理」および「論理」というラベルが使用されます。また、トランスペアレントモードとマルチコンテキストは、これらのデバイスではサポートされていません。

サブインターフェイスを使用すると、物理インターフェイスを異なる VLAN ID がタグ付けされた複数の論理インターフェイスに分割できます。VLANにより、特定の物理インターフェイ

ス上でトラフィックを分離しておくことができるため、物理インターフェイスやセキュリティアプライアンスを追加しなくても、ネットワークで使用できるインターフェイスの数を増やすことができます。この機能は、マルチ コンテキスト モードで特に役立ち、これにより、各コンテキストに一意のインターフェイスを割り当てることができます。

原則として、インターフェイスはルータベースのネットワークに接続し、サブインターフェイスはスイッチベースのネットワークに接続します。すべてのサブインターフェイスが、許可トラフィックを正しくルーティングする物理インターフェイスに関連付けられている必要があります。

物理インターフェイスはタグの付いていないパケットを通過させるため、サブインターフェイスを使用する場合、通常は物理インターフェイスでトラフィックを通過させないようにします。サブインターフェイスでトラフィックを通過させるために、物理インターフェイスはイネーブルにしておく必要がありますが、物理インターフェイスではトラフィックを通過させないように、物理インターフェイスには名前を付けないでください。ただし、物理インターフェイスでタグの付いていないパケットを通過させる場合には、通常のようにインターフェイスに名前を付けることができます（インターフェイスの命名の詳細については、デバイスインターフェイス、ハードウェア ポート、ブリッジ グループの管理 （43 ページ）を参照してください）。

（注） スイッチ機能とセキュリティ アプライアンス機能を組み合わせた ASA 5505 は、物理スイッチ ポートと論理 VLAN インターフェイスの両方を設定する特殊な事例です。詳細については、 ASA 5505 のポートおよびインターフェイスについて （8 ページ）を参照してください。

Catalyst 6500 サービスモジュール（ASA-SM および FWSM）には外部物理インターフェイスは含まれません。代わりに、内部 VLAN インターフェイスを使用します。たとえば、VLAN 201 を FWSM 内部インターフェイスに割り当てて、VLAN 200 を外部インターフェイスに割り当てるとします。これらの VLAN を物理スイッチ ポートに割り当てると、ホストがこれらのポートに接続します。VLAN 201 と 200 間で通信が行われる場合は、FWSM が VLAN 間で唯一使用可能なパスであり、トラフィックはステートフルに検査されるように強制されます。

デバイス インターフェイスの追加情報については、次の項を参照してください。

- ルーテッド モードおよびトランスペアレント モードのインターフェイス （6 ページ）
- シングルおよびマルチ コンテキストのインターフェイス （7 ページ）
- ASA 5505 のポートおよびインターフェイスについて （8 ページ）
- サブインターフェイスの設定（PIX/ASA） （9 ページ）
- 冗長インターフェイスの設定 （11 ページ）
- EtherChannel の設定 （13 ページ）
- VNI インターフェイスの設定 （20 ページ）
- トンネルインターフェイスの設定 （30 ページ）

セキュリティ アプライアンスの設定

ファイアウォールデバイスではさまざまな設定が可能であり、設定によって、特定のデバイスに関連付けられるインターフェイスの定義方法が決まります。次の表に、さまざまな設定の概要を示します。

表 *1:* セキュリティ アプライアンスの設定

デバイスタイプ	動作モード（ルータまたはトランスペアレント）	コンテキストのサポート（シングルまたはマルチ）
PIX 6.3.x	該当なし	該当なし
PIX 7.0 以降/ASA	ルータまたはトランスペアレント	シングル
PIX 7.0 以降/ASA、または管理対象外の PIX 7.0 以降/ASA のセキュリティ コンテキスト	ルータまたはトランスペアレント	マルチ（マルチ セキュリティ コンテキストを設定するためのチェックリストを参照）
FWSM、または管理対象外スイッチのセキュリティ コンテキスト（マルチ モード）	ルータまたはトランスペアレント	シングルまたはマルチ

ルーテッド モードおよびトランスペアレント モードのインターフェイス

ASA/PIX 7.0 および FWSM 2.2.1 以降、2 つのモード（ルーテッドまたはトランスペアレント）のどちらかで動作するように、セキュリティデバイスを設定できるようになりました。（PIX 6.3 はルーテッド モードでだけ動作します）。

ルーテッドモードの場合、セキュリティアプライアンスは接続されているネットワークのゲートウェイまたはルータとして機能します。つまり、そのインターフェイスの IP アドレスを保持し、IP アドレス（レイヤ 3）情報に基づいて、これらのインターフェイスを通過するトラフィックを検査およびフィルタリングします。このモードでは、各デバイスインターフェイスが別の IP サブネットに接続され、そのサブネット上で専用の IP アドレスを持ちます。ルーテッドモードは、シングルモードで、またはコンテキストごとに、最大256個のインターフェイスをサポートし、最大で 1000 個のインターフェイスがすべてのコンテキスト間で分配されます。

トランスペアレントモードの場合、セキュリティアプライアンスはレイヤ 2（データリンク）デバイス、またはトランスペアレントブリッジとして動作し、多くの場合、「Bump In The Wire」または「ステルスファイアウォール」と呼ばれます。このモードでは、内部と外部の 2 つのインターフェイスのみを定義できます。これらのインターフェイスには IP アドレスは必要ありません。VLAN ID を使用して検査済みのトラフィックを転送します。ただし、デバイスに専用の管理インターフェイスが含まれている場合は、これ（物理インターフェイスまたはサブインターフェイスのどちらか）をデバイス管理トラフィック用の3番めのインターフェイスとして使用できます。

（注） Cisco Security Manager は、検出中に FWSM 2.x デバイスのインターフェイス情報を読み込みません。

ブリッジ グループ

ASA 8.4.1 および FWSM 3.1 から、トランスペアレント モードでブリッジ グループを使用して、デバイスやコンテキストで使用可能なインターフェイスの数を増やすことができるようになりました。ブリッジグループは 8 個まで設定できます。FWSM では各グループに 2 つのインターフェイスを含めることができ、ASA 9.7.1（Cisco Security Manager 4.13）では各グループに最大 64 のインターフェイスを含めることができます。詳細については、[Add Bridge Group]/[Edit Bridge Group] ダイアログボックス （102 ページ）を参照してください。

シングルおよびマルチ コンテキストのインターフェイス

セキュリティの「コンテキスト」によって、単一の物理デバイスが複数の独立したファイアウォールとして動作できます。マルチ コンテキスト モードの場合、個々のコンテキストは独自の設定を備えた単一の仮想ファイアウォールを定義します。各コンテキストは一意の仮想ファイアウォールとして機能して、そのコンテキストに割り当てられたインターフェイスを通過するトラフィックを検査およびフィルタリングします。コンテキストはそれぞれ、同じセキュリティアプライアンスに定義されている他のコンテキストを「認識しません」。

シングル コンテキストのルーテッド モード デバイスの場合、マルチ コンテキスト デバイス上のインターフェイスはルータベースのネットワークに接続し、サブインターフェイスはスイッチベースのネットワークに接続します。さらに、各サブインターフェイスは、許可トラフィックを正しくルーティングするインターフェイスに関連付けられている必要があります。

ただし、コンテキストを定義して展開するまで、設定のルーテッド モード部分である IP アドレスは定義できず、管理インターフェイスも指定できません。しかし、必要なインターフェイスおよびサブインターフェイスを定義するまで、セキュリティ コンテキストは定義できません。

つまり、セキュリティ コンテキスト自体を定義および設定する前に、（ルーテッド モードまたはトランスペアレント モードのどちらの場合でも）複数のセキュリティ コンテキストを提供するデバイス上でインターフェイスおよびサブインターフェイスをイネーブルにして設定する必要があります。

非対称ルーティング グループについて

場合によっては、セッションのリターン トラフィックは、そのセッションが送信されたインターフェイスとは別のインターフェイスでルーティングされることがあります。同様に、フェールオーバー設定では、ある装置から発信された接続のリターン トラフィックが、ピア装置を経由して返送されることがあります。これは一般に、1 つの FWSM 上の 2 つのインターフェイス、またはフェールオーバー ペアの 2 つの FWSM が別々のサービス プロバイダーに接続され、発信接続で NAT アドレスを使用しない場合に起こります。デフォルトでは、リターン トラフィックには接続情報がないため、FWSM はそのトラフィックをドロップします。

ドロップが発生する可能性のある VLAN インターフェイスに、Asymmetric Routing（ASR; 非対称ルーティング）グループを割り当てることで、リターン トラフィックのドロップを防止できます。メンバインターフェイスがセッション情報のないパケットを受信すると、そのインターフェイスは同じグループのメンバである他のインターフェイスのセッション情報を確認します。

一致が検出されない場合は、パケットはドロップされます。一致が検出された場合は、次のいずれかのアクションが実行されます。

- 着信トラフィックが同一 FWSM 上の異なるインターフェイスで発信された場合、レイヤ 2 ヘッダーの一部または全部が書き換えられ、パケットは再度ストリームに入れられます。
- 着信トラフィックがフェールオーバー設定のピア装置で発信された場合、レイヤ 2 ヘッダーの一部または全部が書き換えられ、パケットはもう一方の装置にリダイレクトされます。このリダイレクトは、セッションがアクティブである限り続行されます。

（注） フェールオーバー設定では、スタンバイ ユニットやフェールオーバー グループからアクティブ ユニットやフェールオーバー グループに転送されるセッション情報について、ステートフル フェールオーバーをイネーブルにする必要があります。

FWSM 仮想インターフェイスを非対称ルーティング グループに割り当てるには、単に ASR Group ID を [Add Interface]/[Edit Interface] ダイアログボックス - [Advanced] タブ（ASA/PIX 7.0 以降） （66 ページ）に指定します。グループが存在しない場合はグループが作成され、インターフェイスがそのグループに割り当てられます。

この ASR グループに参加するインターフェイスごとに、この割り当てを繰り返す必要があります。最大 32 個の ASR グループを作成して、各グループに最大 8 個のインターフェイスを割り当てることができます。

（注） フェールオーバー設定のスタンバイ ユニットからアクティブ ユニットにパケットをリダイレクトできるようにするには、アップストリーム ルータとダウンストリーム ルータは、VLAN ごとに 1 つの MAC アドレスを使用し、異なる VLAN には異なる MAC アドレスを使用する必要があります。

ASA 5505 のポートおよびインターフェイスについて

ASA 5505 は組み込みスイッチを含んでいるという点で独特であり、また、設定に必要なポートおよびインターフェイスが 2 種類存在します。

- 物理スイッチ ポート：ASA 5505 には、ハードウェアのスイッチング機能を使用して、レイヤ 2 でトラフィックを転送するファストイーサネット スイッチ ポートが 8 個あります。これらのポートのうちの 2 つは、Power-over-Ethernet（PoE）ポートです。これらのポートは、PC、IP Phone、または DSL モデムなどのユーザ機器に直接接続できます。または、別のスイッチに接続できます。

- 論理 VLAN インターフェイス：ルーテッド モードでは、これらのインターフェイスは、設定済みのセキュリティ ポリシーを使用してファイアウォールと VPN サービスを適用することによって、レイヤ 3 の VLAN ネットワーク間でトラフィックを転送します。トランスペアレント モードでは、これらのインターフェイスは、設定済みのセキュリティ ポリシーを使用してファイアウォール サービスを適用することによって、レイヤ 2 の同じネットワーク上の VLAN 間でトラフィックを転送します。

スイッチ ポートを別々の VLAN に分離するには、各スイッチ ポートを VLAN インターフェイスに割り当てます。同じ VLAN 上のスイッチ ポートは、ハードウェア スイッチングを使用して相互に通信できます。ただし、1 つの VLAN 上のスイッチ ポートが別の VLAN 上のスイッチ ポートとの通信を試行した場合は、ASA 5505 によって、トラフィックおよび 2 つの VLAN 間のルートまたはブリッジにセキュリティ ポリシーが適用されます。

（注） サブインターフェイスと冗長インターフェイスは、ASA 5505 では使用できません。

ナビゲーション パス

ASA 5505 デバイスに表示される [インターフェイス（Interfaces）] ページには、[ハードウェア ポート（Hardware Ports）] および [インターフェイス（Interfaces）] の 2 つのタブ付きパネルが表示されます。これらのパネルにアクセスするには、[デバイスビュー（Device View）] で ASA 5505 を選択し、デバイスポリシーセレクタから [インターフェイス（Interfaces）] を選択します。

ASA 5505 スイッチのポートとインターフェイスの設定

スイッチ ポートの設定については、ASA 5505 でのハードウェア ポートの設定 （99 ページ）を参照してください。

インターフェイスの設定については、[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM） （50 ページ）を参照してください。

関連項目

- デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （43 ページ）

サブインターフェイスの設定（PIX/ASA）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしますが、バグ修正や拡張機能はサポートしていません。

サブインターフェイスを使用すると、物理インターフェイスを異なる VLAN ID がタグ付けされた複数の論理インターフェイスに分割できます。VLAN により、特定の物理インターフェイ

ス上でトラフィックを分離しておくことができるため、物理インターフェイスやセキュリティアプライアンスを追加しなくても、ネットワークで使用できるインターフェイスの数を増やすことができます。この機能はマルチ コンテキスト モードで特に役立ち、これにより、各コンテキストに一意のインターフェイスを割り当てることができます。

（注） 物理インターフェイスはタグの付いていないパケットを通過させるため、サブインターフェイスを使用する場合、通常は物理インターフェイスでトラフィックを通過させないようにします。サブインターフェイスでトラフィックを通過させるために、物理インターフェイスはイネーブルにしておく必要がありますが、物理インターフェイスではトラフィックを通過させないように、物理インターフェイスには名前を付けないでください。ただし、物理インターフェイスでタグの付いていないパケットを通過させる場合には、通常のようにインターフェイスに名前を付けることができます

（注） このオプションは PIX 7.0 以降のデバイスと 5505 ASA 以外のデバイスでのみ使用できます。

サブインターフェイスの定義

サブインターフェイスを [Add Interface] または [Edit Interface]（ASA/PIX 7.0 以降）ダイアログボックスで設定するには、次の手順を行います。このダイアログボックスには、デバイスの [Interfaces] ページからアクセスできます（デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （43 ページ）を参照）。

1. [インターフェイスの追加（Add Interface）] または [インターフェイスの編集（Edit Interface）] ダイアログボックスで、インターフェイスの [タイプ（Type）] として [サブインターフェイス（Subinterface）] を選択します。

[VLAN ID] と [サブインターフェイスID（Subinterface ID）] のフィールドが [ハードウェアポート（Hardware Port）]、[名前（Name）]、[セキュリティレベル（Security Level）] のフィールドの下に表示されます。

1. 以前に定義したインターフェイスポートのリストから、目的の [ハードウェアポート（Hardware Port）] を選択します。目的のインターフェイス ID が表示されない場合は、インターフェイスが定義済みで、イネーブルにされていることを確認してください。

2. [VLAN ID]：このサブインターフェイスの VLAN ID を指定します。1 ～ 4094 の値を入力します。指定した VLAN ID は、どの接続デバイスでも使用されていない必要があります。

一部の VLAN ID は接続されているスイッチで予約されている場合があります。詳細については、スイッチのマニュアルを確認してください。マルチコンテキスト モードでは、VLAN ID はシステム設定でのみ設定できます。

1. [セカンダリ VLAN ID（Secondary VLAN ID）]：このサブインターフェイスのセカンダリ VLAN ID 値を指定します。これにより、ASA は、セカンダリ VLAN 上の ASA に到着する

パケットをプライマリ VLAN にマッピングできます。設定：1 ～ 4090 の値を入力します。セカンダリ VLAN ID は一意である必要があり、VLAN ID と同じであってはなりません。セカンダリ VLAN は、シングルコンテキストのルーテッドモードまたはファイアウォールモードで、または L2 クラスタとして、ASA 9.5.2 以降を実行しているデバイスでサポートされます。

（注） 複数の VLAN ID はスペースまたはコンマで区切って追加できます。56 ～ 78 などの VLAN ID の範囲を指定することもできます。

1. [サブインターフェイスID（Subinterface ID）]：サブインターフェイス ID として 1 ～ 4294967293 の整数を指定します。許可されるサブインターフェイスの番号は、プラットフォームによって異なります。

サブインターフェイスのポート ID の場合、この ID は選択したハードウェア ポートに付加されます。たとえば、*GigabitEthernet0.4* は、GigabitEthernet0 ポートで動作する、4 の ID を割り当てられたサブインターフェイスを示します。

（注） 設定後は ID を変更できません。

1. [インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM） （50 ページ）の説明に従って、このインターフェイスの設定を続けます。

冗長インターフェイスの設定

Security Manager 3.2.2 から、論理的な「冗長」インターフェイスを定義して、セキュリティアプライアンスの信頼性を向上させることができるようになりました。冗長インターフェイスは物理インターフェイスの特定のペアであり、1 つをアクティブ（またはプライマリ）として指定し、もう 1 つをスタンバイ（またはセカンダリ）として指定します。アクティブ インターフェイスで障害が発生すると、スタンバイ インターフェイスがアクティブになり、トラフィックの送信を開始します。この機能はデバイス レベルのフェールオーバーとは別のものですが、必要な場合には、フェールオーバーと同様に冗長インターフェイスを設定できます。最大 8 個の冗長インターフェイス ペアを設定できます。

冗長インターフェイスは、常にメンバペアの 1 つだけがアクティブになる単一のインターフェイス（内部、外部など）として機能します。この冗長インターフェイスは、一意のインターフェイス名、セキュリティ レベル、および IP アドレスを使用して通常どおりに設定します。各メンバインターフェイスは同じタイプ（ギガビットイーサネットなど）である必要があり、名前、セキュリティ レベル、または IP アドレスを割り当てられないことに注意してください。実際には、メンバー インターフェイスに対して [Duplex] および [Speed] 以外のオプションを設定しないでください。

冗長インターフェイスは、指定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。または、冗長インターフェイスに明示的に MAC アドレスを割り当てることもできます。この場合、メンバインターフェイスの MAC アドレスに関係なく、このアドレスが使用されます。どちらの場合にも、アクティブインターフェイスがスタンバイにフェールオーバーしたときには、トラフィックが中断されないように同じ MAC アドレスが保持されます。

（注） このオプションは PIX 8.0 以降のデバイスと 5505 ASA 以外のデバイスでのみ使用できます。

冗長インターフェイスの定義

2 つの物理インターフェイスを単一の論理的な「冗長インターフェイス」として [インターフェイスの追加（Add Interface）] または [インターフェイスの編集（Edit Interface）]（ASA/PIX 7.0 以降）ダイアログボックスで設定するには、次の手順を行います。このダイアログボックスには、デバイスの [インターフェイス（Interfaces）] ページからアクセスできます（デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （43 ページ）を参照）。

1. [インターフェイスの追加（Add Interface）] または [インターフェイスの編集（Edit Interface）] ダイアログボックスで、インターフェイスの [タイプ（Type）] として [冗長（Redundant）] を選択します。

[Redundant ID]、[Primary Interface]、および [Secondary Interface] オプションが表示されます。

1. この冗長インターフェイスの ID を [冗長ID（Redundant ID）] フィールドに指定します。有効な ID は、1 ～ 8 の整数です。
2. [プライマリインターフェイス（Primary Interface）]：この使用可能なインターフェイスのリストから、冗長インターフェイスペアのプライマリメンバーを選択します。名前付きインターフェイスは冗長インターフェイス ペアでは指定できないため、使用可能なインターフェイスが [Hardware Port ID] に表示されます。
3. [セカンダリインターフェイス（Secondary Interface）]：この使用可能なインターフェイスのリストから、冗長インターフェイスペアのセカンダリメンバーを選択します。名前付きインターフェイスは冗長インターフェイス ペアでは指定できないため、使用可能なインターフェイスが [Hardware Port ID] に表示されます。

（注） メンバ インターフェイスはイネーブルである必要があります。また、メンバ インターフェイスは同じタイプ（GigabitEthernet など）である必要があります。[Name]、[IP Address]、または [Security Level] を割り当てることはできません。実際には、メンバー インターフェイスに対して [Duplex] および [Speed] 以外のオプションを設定しないでください。

1. [インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM） （50 ページ）の説明に従って、このインターフェイスの設定を続けます。

EtherChannel の設定

ASA 8.4.1 から、論理 EtherChannel インターフェイスを定義できるようになりました。ポートチャネル インターフェイスとも呼ばれる EtherChannel は、個別のイーサネット リンクのバンドル（チャネル グループ）で構成される論理インターフェイスです。EtherChannel を使用すると、個別のリンクと比較して帯域幅と耐障害性を強化できます。

EtherChannel インターフェイスは、単一の物理インターフェイスと同様の方法で設定および使用されます。最大 48 個の EtherChannel を設定できます。各 EtherChannel は 1 ～ 8 個のアクティブなファスト イーサネット ポート、ギガビット イーサネット ポート、または Ten-Gigabit イーサネット ポートで構成されます。ASA 9.2(1) では、アクティブインターフェイスの数が 16 に増加しました。

（注） EtherChannel の一部として冗長インターフェイスを使用することはできません。また、冗長インターフェイスの一部として EtherChannel を使用することはできません。冗長インターフェイスと EtherChannel インターフェイスでは同じ物理インターフェイスを使用できません。ただし、冗長インターフェイスと EtherChannel インターフェイスが同じ物理インターフェイスを使用しない場合は、両方のタイプを ASA に設定できます。

EtherChannel MAC アドレス指定

1 つのチャネル グループに含まれるすべてのインターフェイスは、同じ MAC アドレスを共有します。これにより、ネットワーク アプリケーションとユーザに対して EtherChannel がトランスペアレントになります。これは、ネットワーク アプリケーションとユーザは 1 つの論理接続のみを認識し、個別のリンクは認識しないためです。デフォルトでは、EtherChannel は最も番号の小さいメンバ インターフェイスの MAC アドレスをその EtherChannel の 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。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、MAC アドレスを手動で設定することを推奨します。たとえば、ポートチャネル MAC アドレスを提供するインターフェイスを削除する場合、そのポートチャネルには次に番号の小さいインターフェイスの MAC アドレスが割り当てられるため、トラフィックが分断されます。手動で一意の MAC アドレスを EtherChannel インターフェイスに割り当てることにより、この分断を防止できます（マルチコンテキスト モードでは、EtherChannel インターフェイスを含め、個別のコンテキストに割り当てられているインターフェイスに一意の MAC アドレスを割り当てることができます）。

管理専用 EtherChannel インターフェイスについて

EtherChannel グループは管理専用インターフェイスとして指定できますが、次の点に注意してください。

- ルーテッド モード：EtherChannel を管理専用として明示的に [インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM） （50 ページ）で設定する必要があります。管理専用ポートチャネルに追加された管理用ではないすべてのインターフェイスは、管理ポートとして扱われます。すでに管理専用として定義されているインターフェイスを管理専用グループに追加する場合、物理インターフェイスではその属性は無視されます。同様に、インターフェイスがすでに管理専用ポートチャネルのメンバである場合は、そのインターフェイスを管理専用として指定できません。
- トランスペアレント モード：このモードでは、管理専用 EtherChannel のメンバ自体は管理専用ポートにしかなれません。そのため、管理専用メンバをトランスペアレント モードの EtherChannel に追加する場合、チャネルは管理専用の指定を継承する一方、その指定はメンバ インターフェイスから削除されます。反対に、そのようなインターフェイスが EtherChannel から削除されると、その指定は個別のインターフェイス上で復元されます。

EtherChannel インターフェイスのフェールオーバーリンクとしての使用

EtherChannel インターフェイスがフェールオーバー リンクとして指定されている場合、そのリンクのすべての状態同期トラフィックは単一の物理インターフェイスで送信されます。その物理インターフェイスに障害が発生すると、状態同期トラフィックは EtherChannel 集約リンクに含まれる別の物理インターフェイスを通過します。フェールオーバー用に指定された EtherChannel リンクに使用可能な物理インターフェイスが残っていない場合、冗長インターフェイスが指定されていれば、ASA は冗長インターフェイスに切り替えます。

EtherChannel インターフェイスはアクティブなフェールオーバー リンクとして使用されますが、その EtherChannel 設定を変更することはできません。そのリンクの EtherChannel 設定を変更するには、次のようにして、リンクまたはフェールオーバーのいずれかをディセーブルにする必要があります。

- 設定を変更している間は EtherChannel リンクをディセーブルにし、その後リンクを再アクティブ化します（リンクがディセーブルになっている間はフェールオーバーは発生しません）。
- 設定を変更している間はフェールオーバーをディセーブルにし、その後フェールオーバーをイネーブルにします（その間フェールオーバーは発生しません）。

（注） フェールオーバー リンクとして割り当てられている他のタイプのインターフェイスと同様、EtherChannel インターフェイスに名前を付けることはできません。さらに、EtherChannel のメンバ インターフェイスに名前を付けることもできません。

ASA での EtherChannel の定義

複数の物理インターフェイスを単一の論理 EtherChannel インターフェイスとして ASA の [Add Interface] または [Edit Interface] ダイアログボックスで設定するには、次の手順を行います。このダイアログボックスには、デバイスの [Interfaces] ページからアクセスできます（デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （43 ページ）を参照）。

ステップ 1 インターフェイスの [タイプ（Type）] として [EtherChannel] を選択します。

[EtherChannel ID] およびインターフェイスの選択オプション（[ロードバランシング（Load Balancing）]、[LACP モード（LACP Mode）]、および [アクティブ物理インターフェイス（Active Physical Interfaces）]）がダイアログボックスの [全般（General）] パネルに表示されます。[最小（Minimum）] と [最大（Maximum）] フィールドが [詳細設定（Advanced）] パネルに表示されます。

ステップ 2 この EtherChannel の ID を [EtherChannel ID] フィールドに指定します。有効な ID は、1 ～ 48 の整数です。この数字は「Port-channel」に追加され、デバイスの [インターフェイス（Interfaces）] ページにあるテーブルの [インターフェイス（Interface）] 列で、EtherChannel を識別します。

ステップ 3 [使用可能なインターフェイス（Available Interfaces）]：この使用可能なインターフェイスのリストで 1 つ以上のインターフェイスを選択して、[>>] ボタンをクリックして右のメンバリストに追加して、このポートチャネルグループのメンバを指定します。

（注） チャネル グループのすべてのインターフェイスは、同じタイプと速度である必要があります。チャネル グループに追加された最初のインターフェイスによって、正しいタイプと速度が決まります。

最大 16 個のインターフェイスをチャネル グループに割り当てられます。ASA 9.2(1) 以降の場合、各チャネルグループに、最大 16 個のアクティブインターフェイスを設定できます。8 個のアクティブインターフェイスだけをサポートするスイッチを使用していて、ASA のバージョンが 9.2(1) より前の場合、8 個のインターフェイスのみアクティブにできるため、残りのインターフェイスは、インターフェイス障害発生時のスタンバイリンクとして動作できます。または、[LACP Mode] を [On] に設定すると、スタティックな EtherChannel を作成できます（次に説明されているとおり、[Advanced] パネルで設定）。これにより、グループ内のすべてのインターフェイスでトラフィックを通過させることができます。

（注） この EtherChannel グループにインターフェイスを割り当てたら、EtherChannel に割り当てられているインターフェイスの LACP パラメータの編集 （16 ページ）の説明に従って、各メンバ インターフェイスの [LACP Port] パラメータを編集できます。

ステップ 4 [詳細設定（Advanced）] タブをクリックして、そのパネルを表示します。

ステップ 5 EtherChannel のセクションで、[ロードバランシング（Load Balancing）] オプションを選択します。このオプションの詳細については、EtherChannel のロード バランシングについて （18 ページ）を参照してください。

ステップ 6 目的の [LACP モード（LACP Mode）] を選択します。デフォルトの [アクティブ（Active）] を選択すると、[アクティブ物理インターフェイス（Active Physical Interfaces）] の [最小（Minimum）] 値と [最大（Maximum）] 値で指定されているとおり、最大 8 個のインターフェイスをアクティブにして、最大 8 個のインターフェイスをスタンバイモードにできます。

[オン（On）] を選択すると、すべてのメンバインターフェイスが「オン」になっているスタティックポートチャネルが作成されます。つまり、トラフィックを通過する最大16個のポートを設定できます。この場合、スタンバイポートはありません。このオプションを選択すると、この EtherChannel グループに割り当てられているすべてのインターフェイスの [Mode] は [On] に切り替わります（それぞれの [Mode] が [On] ではない場合）。このモードの詳細については、EtherChannel に割り当てられているインターフェイスの LACP パラメータの編集 （16 ページ）を参照してください。

ステップ 7 この EtherChannel のアクティブな物理インターフェイスの最小数と最大数を [Minimum] と [Maximum] に指定します。

前述のように、EtherChannel は、9.2(1) より前の ASA デバイスの場合は 1 ～ 8 個のアクティブリンク、ASA 9.2(1) 以降の場合は 1 ～ 16 個のアクティブリンクで構成できます。これらのフィールドを使用して、特定の時点でこのチャネル グループでアクティブにできるインターフェイスの最小値と最大値を指定します。スイッチが 16 個のアクティブインターフェイスをサポートしていない場合、最大数は必ず 8 以下に設定する必要があります。

ステップ 8 [インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM）（50 ページ）の説明に従って、このインターフェイスの設定を続けます。

（注） このデバイスの EtherChannel の [LACP システム優先順位（LACP System Priority）] は、高度なインターフェイス設定（PIX/ASA/FWSM） （110 ページ）ダイアログボックスで指定します。

EtherChannel に割り当てられているインターフェイスの LACP パラメータの編集

インターフェイスを EtherChannel（ポートチャネル）グループに割り当てたら、ここでの説明に従って、各メンバ インターフェイスの [LACP Port] パラメータを編集できます。

（注） この機能は ASA 8.4.1 以降のデバイスでのみ使用できます。

Link Aggregation Control Protocol（LACP; リンク集約制御プロトコル）は、物理的なファストイーサネット、ギガビットイーサネット、または Ten-Gigabit イーサネットのインターフェイスを集約して 1 つの EtherChannel グループに転送します。また、互換性のあるポートセットが見つかった場合に、リモートパートナーデバイスを現在の情報に更新し、「操作キー」と呼ばれる一意の値をグループに割り当てます。操作キーは自動で割り当てられます。設定することはできません。

注意 EtherChannel がフェールオーバーリンクとして割り当てられている場合、これらの LACP パラメータは使用できません。

LACP システムプライオリティ

各 LACP 対応デバイスには一意のシステム ID があります。この ID は、システムプライオリティ ID とシステムの MAC アドレスの組み合わせによって構成されます。特定の状況では、EtherChannel でリンクされている 2 つのシステムのポート セットに割り当てられている操作キーを変更して、集約を最適化する必要がある場合があります。そのような場合、プライオリティの高いシステムのポートに割り当てられている操作キーの値を動的に変更して、集約を向上させることができます。プライオリティの低いシステムでは、操作キーの値を変更することはできません。システム プライオリティ ID は、高度なインターフェイス設定（PIX/ASA/FWSM） （110 ページ）の説明に従って、ユーザが設定できます。

LACP ポートパラメータ

ポート ID は、各グループ インターフェイスに割り当てられている一意の数字で指定されます。この ID は設定可能な [Port Priority] の数字と、インターフェイスに割り当てられているポート番号の組み合わせで構成されます。

ポート ID はポート集約のプライオリティを指定します。集約では、システム内で最も集約プライオリティの高いポートからアクティブ ポートとして使われ始め、ポート ID のリストに従って上から順番に使用されていきます。このポート集約プライオリティを使用すると、すべてのリンクで LACP を同時に実行している場合と同様の方法で集約のリンクが選択されるため、集約を予測したり再現したりできるようになります。

さらに、各ポートのプライオリティを設定して、スタンバイ ポートのセットを管理制御できます。たとえば、プライオリティの最も低いポートは、グループの集約で最後に使用されるため、スタンバイ ポートになります（スタンバイ ポートを用意するために十分なメンバがグループに割り当てられていることが前提です）。

関連項目

- EtherChannel の設定 （13 ページ）

既存の EtherChannel インターフェイスの LACP ポートパラメータの編集

既存の EtherChannel が割り当てられているインターフェイスを編集するには、次の手順を行います。

ステップ 1 デバイスの [インターフェイス（Interfaces）] ページにあるテーブルで、ポートチャネルグループのメンバであるインターフェイスを選択します。（このテーブルのアクセスと使用については、デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （43 ページ）を参照してください）。

ステップ 2 [行の編集（Edit Row）] をクリックして、そのインターフェイスで [インターフェイスの編集（Edit Interface）] ダイアログボックスを開きます。

[Enable Interface] チェックボックス、[LACP Port] パラメータ、および [Description] フィールドのみを変更できます。

ステップ 3 必要に応じて、[LACPポート（LACP Port）] パラメータを編集します。

- [優先順位（Priority）]：この数字とインターフェイスに割り当てられているポート番号が組み合わさって、一意のポート ID 番号が生成されます。この値には 1 ～ 65535 を指定できます。数字が大きいほど、プライオリティは低くなります。デフォルトは32768 です。このパラメータは、ポートが [Active] モードまたは [Passive] モードの場合にのみ適用されます。
- [モード（Mode）]：これらの LACP モードの 1 つを選択します。
  - [アクティブ（Active）]：アクティブモードでは、ポートはパートナーデバイスとの LACP の交換を開始して、定期的にパートナーに更新を送信します。アクティブな LACP は、パートナーの制御モードに関係なく、プロトコルに参加するポートの優先度を反映します。
  - [パッシブ（Passive）]：パッシブモードのポートは LACP の交換を開始しませんが、パートナーからの要求を受信すると、ポートはそのパートナーと LACP 情報の交換を開始します。パッシブモードは、リモート ポートが LACP をサポートしているかどうかがわからない場合に便利です。

一部のデバイスは、LACP がイネーブルになっていない場合に定期的な LACP 更新を受信すると、正常に動作しないことがあります。ただし、正常に動作するようにチャネルを設定するには、少なくとも 1 つのポートがアクティブ モードに設定されている必要があります。

- • [オン（On]）：このモードは、すべてのメンバーのインターフェイスがオンになっているスタティックポートチャネルを、スタンバイ ポートなしで設定するために使用します。ネゴシエーションは行われず、他の 2 つのモードに関連するほとんどの制約も適用されません。たとえば、すべてのメンバーポートの速度設定とデュプレックス設定を同じにする必要はありません。また、すべてのメンバーポートはアクティブのままになります。リモート ポートもオンにする必要があります。「オン」の EtherChannel は、別の「オン」の EtherChannel のみと接続を確立できます。

- [VSSまたはvPCスイッチID（VSS or vPC Switch ID）]：インターフェイスが接続されている仮想スイッチングシステム（VSS）または仮想ポート チャネル（vPC）スイッチ ID を識別します。

ステップ 4 [インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM）（50 ページ）の説明に従って、このインターフェイスの編集を続けます。

EtherChannel のロード バランシングについて

EtherChannel のトラフィックは、バンドルされている個別のリンク間で決定論的手法により分散されます。ただし、すべてのリンクで負荷が均等に分配されるわけではありません。代わりに、ハッシュ アルゴリズムの結果として、フレームは特定のリンクに転送されます。このアルゴリズムでは、特定のフィールドまたはフィールドの組み合わせをパケット ヘッダーで使用して、使用するリンクを示す固定の Result Bundle Hash（RBH）値を生成します。

アルゴリズムは、パケット ヘッダー フィールド（送信元 IP アドレス、宛先 IP アドレス、送信元 MAC アドレス、宛先 MAC アドレス、TCP/UDP ポート番号、VLAN ID）の 1 つまたはそれらのフィールドの組み合わせを使用して、リンクの割り当てを決定します。このアルゴリズムで使用するフィールドの組み合わせは、[ロードバランシング（Load Balancing）] リストから選択されます（ASA の [インターフェイスの追加（Add Interface）] および [インターフェイスの編集（Edit Interface）] ダイアログボックスの [詳細設定（Advanced）] タブ）。これらのオプションは、後続の項で説明されています。詳細については、 EtherChannel の設定 （13 ページ）を参照してください。

たとえば、フィールドに送信元 MAC アドレス（src-mac）を選択した場合、パケットが EtherChannel に転送されると、それらのパケットは各着信パケットの送信元 MAC アドレスに基づいて、チャネル内のポート間で分散されます。そのため、ロード バランシングを行うには、異なるホストからのパケットはチャネル内の異なるポートを使用しますが、同じホストからのパケットはチャネル内の同じポートを使用します（また、デバイスが学習した MAC アドレスは変更されません）。

同様に、宛先 MAC アドレス転送では、パケットが EtherChannel に転送されると、各パケットはパケットの宛先ホスト MAC アドレスに基づいて、チャネル内のポート間で分散されます。したがって、宛先が同じパケットは同じポートに転送され、宛先の異なるパケットはそれぞれ異なるチャネル ポートに転送されます。

そのため、ロード バランシング オプションを選択するときには、柔軟に設定できるオプションを使用します。たとえば、チャネル上のほとんどのトラフィックが 1 つの MAC アドレスにのみ送信される場合、宛先 MAC アドレスを選択すると、ほとんどのトラフィックが常にチャネル内の同じリンクを使用するようになります。別の方法として、送信元アドレスや IP アドレスを使用すると、ロード バランシングが向上する場合があります。また、UDP ポート番号や TCP ポート番号とともに送信元アドレスと宛先アドレスを使用すると、まったく異なる方式でトラフィックを分配できます。

（注） このオプションは ASA 8.4.1 以降のデバイスでのみ使用できます。

ロード バランシング オプション

単一の論理 EtherChannel インターフェイスを ASA の [インターフェイスの追加（Add Interface）] または [インターフェイスの編集（Edit Interface）] ダイアログボックスで定義する場合、次のいずれかの [ロードバランシング（Load Balancing）] のオプションを選択し（[Add Interface]/[Edit Interface] ダイアログボックス - [Advanced] タブ（ASA/PIX 7.0 以降） （66 ページ）で設定）、負荷分散の基本を指定します。

- [dst-ip]：宛先ホストの IP アドレスにのみ基づいて負荷分散が行われます。パケットの送信元は考慮されません。同じ宛先 IP アドレスを持つ各パケットは、同じリンクで転送されます。
- [dst-ip-port]：宛先ホストの IP アドレスと TCP/UDP ポートに基づいて負荷分散が行われます。このオプションを使用すると、宛先 IP アドレスだけの場合より、よりきめ細かく多少複雑な負荷分散を実行できます。
- [dst-mac]：着信パケットの宛先ホストの MAC アドレスに基づいて負荷分散が行われます。
- [dst-port]：宛先ポートに基づいて負荷分散が行われます。つまり、物理インターフェイスではなく、TCP ポートまたは UDP ポートに基づいて行われます。
- [src-dst-ip]：送信元 IP アドレスと宛先 IP アドレスに基づいて負荷分散が行われます。ハッシュ計算では、送信元 IP アドレスと宛先 IP アドレスがペアで使用されます。この方式を使用すると、宛先 IP アドレスよりもきめ細かい負荷分散を実行できます。たとえば、同じ宛先へのパケットが異なる IP 送信元から送信されている場合、ポートチャネル内の異なるリンクからそのパケットを転送できます。
- [src-dst-ip-port]：分散の計算では、送信元 IP アドレスと宛先 IP アドレス、および TCP/UDP ポートが考慮されます。さらにきめ細かい負荷分散を実行できます。
- [src-dst-mac]：送信元 MAC アドレスと宛先 MAC アドレスのペアに基づいて計算が行われます。
- [src-dst-port]：送信元と宛先の TCP/UDP ポートに基づいて負荷分散が行われます。
- [src-ip]：送信元のホスト IP アドレスのみに基づきます。
- [src-ip-port]：送信元 IP アドレスおよび TCP/UDP ポート。

- [src-mac]：送信元 MAC アドレスのみ。
- [src-port]：送信元 TCP/UDP ポートのみ。
- [vlan-dst-ip]：宛先 IP アドレスと VLAN ID のペア。
- [vlan-dst-ip-port]：宛先 IP アドレス、TCP/UDP ポート、および VLAN ID の組み合わせ。
- [vlan-only]：VLAN ID のみ。
- [vlan-src-dst-ip]：送信元 IP アドレスと宛先 IP アドレス、および VLAN ID。
- [vlan-src-dst-ip-port]：送信元 IP アドレスと宛先 IP アドレス、TCP/UDP ポート、および VLAN ID。
- [vlan-src-ip]：送信元 IP アドレスと VLAN ID。
- [vlan-src-ip-port]：送信元 IP アドレス、TCP/UDP ポート、および VLAN ID。

VNI インターフェイスの設定

VNI インターフェイスは VLAN インターフェイスに似ています。VNI インターフェイスは、タギングを使用して特定の物理インターフェイスでのネットワーク トラフィックの分割を維持する仮想インターフェイスです。各VNI インターフェイスにセキュリティ ポリシーを直接適用します。すべての VNI インターフェイスは、同じ VTEP インターフェイスに関連付けられます。

VXLAN を設定するには、最初に VXLAN ポリシーの設定 （116 ページ）の手順を実行してから VNI インターフェイスを作成し、設定された VXLAN ポリシーを VNI インターフェイスに関連付ける必要があります。

[インターフェイスの追加（Add Interface）] または [インターフェイスの編集（Edit Interface）] ダイアログボックスの [タイプ（Type）] で [VNIインターフェイス（VNI Interface）] を選択した場合、オプションとして [全般（General）]、[詳細設定（Advanced）]、[IPv6] の 3 つタブ付きパネルが表示されます。以下の各項では、3 つのタブ付きパネルを使用した VNI インターフェイスの設定方法について説明します。

- VXLAN （116 ページ）
- VNI インターフェイス：[全般（General）] タブ （20 ページ）
- VNI インターフェイス：[詳細（Advanced）] タブ （24 ページ）
- VNI インターフェイス：[IPv6] タブ （25 ページ）

VNI インターフェイス：[全般（General）] タブ

[インターフェイスの追加（Add Interface）] または [インターフェイスの編集（Edit Interface）] ダイアログボックスの [タイプ（Type）] で [VNIインターフェイス（VNI Interface）] を選択した場合、このダイアログボックスには、[全般（General）]、[詳細設定（Advanced）]、[IPv6] の3つオプションのタブ付きパネルが表示されます。ここでは、[全般（General）]パネルに表示される各オプションについて説明します。

ナビゲーション パス

[全般（General）] パネルには [インターフェイスの追加（Add Interface）] および [インターフェイスの編集（Edit Interface）] ダイアログボックスからアクセスできます。各ダイアログボックスには、デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （43 ページ）の説明に従って、ASA の [インターフェイス（Interfaces）] ページからアクセスできます。

関連項目

- VNI インターフェイスの設定 （20 ページ）
- VNI インターフェイス：[詳細（Advanced）] タブ （24 ページ）
- VNI インターフェイス：[IPv6] タブ （25 ページ）

フィールド リファレンス

表 *2 : [全般（General）] タブ：[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（ASA）*

要素	説明
[Enable Interface]	VNI インターフェイスがまだ有効になっていない場合は、このボックスをオンにして有効にします。
名前	[Interface Name] を入力します。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。
セキュリティ レベル（Security Level）	[Security Level] に 0（最低）～100（最高）を入力します。
VXLAN	
VNI ID	[VNI ID] は 1 ～ 10000 の間で入力します。この ID は内部インターフェイス識別子です。
VNIセグメントID（VNI Segment ID）	[VNI Segment ID] は 1 ～ 16777215 の間で入力します。セグメント ID は VXLAN タギングに使用されます。
Multicast Group IP Address	（シングル モード）[Multicast Group IP Address] を入力します。 VNI インターフェイスに対してマルチキャスト グループを設定しない場合は、VTEP 送信元インターフェイス設定のデフォルト グループが使用されます（使用可能な場合）。VTEP 送信元インターフェイスに対して手動でVTEP ピア IP を設定した場合、VNI インターフェイスに対してマルチキャスト グループを指定することはできません。マルチキャストは、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。

要素	説明
VTEPインターフェイスにマッピングされているNVE（NVE Mapped to VTEP Interface）	[NVE Mapped to VTEP Interface] チェック ボックスをオンにします。この設定により、VNI インターフェイスが VTEP 送信元インターフェイスに関連付けられます。
IP タイプ（IP Type）	利用可能なオプションから [IPタイプ（IP Type）] を選択します。
スタティック IP（Static IP）	[IPアドレス（IP Address）]：（ルーテッドモード）[IPアドレス（IP Address）] 領域で、IPv4 アドレスを設定します。IPv6 を設定するには、[IPv6] タブをクリックします。 [サブネットマスク（Subnet Mask）]：サブネットマスクを指定します。
DHCP を使用する	[DHCP学習済みルートメトリック（DHCP Learned Route Metric）]：（必須）学習したルートにアドミニストレーティブディスタンスを割り当てるには、[DHCP学習済みルートメトリック（DHCP Learned Route Metric）] フィールドに 1 ～ 255 の値を入力します。このフィールドを空白のままにすると、既知のルートのアドミニストレーティブディスタンスは 1 になります。 [DHCPを使用したデフォルトルートの取得（Obtain Default Route using DHCP）]：（任意）デフォルトのスタティックルートを設定する必要がないようにDHCPサーバーからデフォルトルートを取得するには、このオプションを選択します。 [DHCP学習済みルートのトラッキングの有効化（Enable Tracking for DHCP Learned Route）]：（任意）[DHCPを使用したデフォルトルートの取得（Obtain Default Route using DHCP）] を選択した場合、このオプションを選択し、特定のサービスレベル契約（SLA）モニターによるルートトラッキングを有効にできます。次のオプションが使用可能になります。 [トラッキング済みSLAモニター（Tracked SLA Monitor）]：[DHCP学習済みルートのトラッキングの有効化（Enable Tracking for DHCP Learned Route）] を選択した場合は必須です。このインターフェイスに適用されるルートトラッキング（接続性のモニタリング）を定義している SLA モニタ オブジェクトの名前を入力または選択します。
説明	（任意）インターフェイスの説明を指定します。

表 *3 : [*全般（*General*）*]* タブ：*[*インターフェイスの追加*/*編集（*Add/Edit Interface*）*]* ダイアログボックス（*ASAv*）

要素	説明
[Enable Interface]	VNIインターフェイスがまだ有効になっていない場合は、このボックスをオンにして有効にします。
名前	[Interface Name] を入力します。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。
セキュリティ レベル（Security Level）	[Security Level] に 0（最低）～100（最高）を入力します。
VXLAN	
Proxy Single-Arm	ASAv デバイスの AWS GWLB をサポートする Proxy Single-Arm を選択します。 **重要** CSM UI で Proxy Single-Arm を表示および設定するには、ハイパーバイザ XENAWS または KVMAWS を備えた ASAv デバイスで AWS を有効にする必要があります。ASAv30 は、Proxy Single-Arm 構成でサポートされる最小のプラットフォームです。
VNI ID	[VNI ID] は 1 ～ 10000 の間で入力します。この ID は内部インターフェイス識別子です。
VNIセグメントID（VNI Segment ID）	[VNI Segment ID] は 1 ～ 16777215 の間で入力します。セグメント ID は VXLAN タギングに使用されます。
Multicast Group IP Address	（シングル モード）[Multicast Group IP Address] を入力します。 VNI インターフェイスに対してマルチキャスト グループを設定しない場合は、VTEP 送信元インターフェイス設定のデフォルト グループが使用されます（使用可能な場合）。VTEP送信元インターフェイスに対して手動でVTEP ピア IP を設定した場合、VNI インターフェイスに対してマルチキャスト グループを指定することはできません。マルチキャストは、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。
VTEPインターフェイスにマッピングされている NVE（NVE Mapped to VTEP Interface）	[NVE Mapped to VTEP Interface] チェック ボックスをオンにします。この設定により、VNI インターフェイスが VTEP 送信元インターフェイスに関連付けられます。
IP タイプ（IP Type）	利用可能なオプションから [IPタイプ（IP Type）] を選択します。

要素	説明
スタティック IP（Static IP）	[IPアドレス（IP Address）]：（ルーテッドモード）[IPアドレス（IP Address）] 領域で、IPv4 アドレスを設定します。IPv6 を設定するには、[IPv6] タブをクリックします。 [サブネットマスク（Subnet Mask）]：サブネットマスクを指定します。

VNI インターフェイス：[詳細（Advanced）] タブ

[インターフェイスの追加（Add Interface）] または [インターフェイスの編集（Edit Interface）] ダイアログボックスの [タイプ（Type）] で [VNIインターフェイス（VNI Interface）] を選択した場合、このダイアログボックスには、[全般（General）]、[詳細（Advanced）]、[IPv6] の 3 つオプションのタブ付きパネルが表示されます。ここでは、[詳細（Advanced）] パネルに表示されるこれらのオプションについて説明します。

ナビゲーション パス

[詳細（Advanced）] タブには [インターフェイスの追加（Add Interface）] および [インターフェイスの編集（Edit Interface）] ダイアログボックスからアクセスできます。各ダイアログボックスには、デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （43 ページ）の説明に従って、ASA の [インターフェイス（Interfaces）] ページからアクセスできます。

関連項目

- VNI インターフェイスの設定 （20 ページ）
- VNI インターフェイス：[全般（General）] タブ （20 ページ）
- VNI インターフェイス：[IPv6] タブ （25 ページ）

フィールド リファレンス

表 *4: [詳細（Advanced）] タブ：[インターフェイスの追加（Add Interface）]/[インターフェイスの編集（Edit Interface）] ダイアログボックス（ASA）*

要素	説明
Active MAC Address	[アクティブMACアドレス（Active MAC Address）] フィールドを使用して、プライベート MAC アドレスをインターフェイスに手動で割り当てます。
Standby MAC Address	[スタンバイ MAC アドレス（Standby MAC Address）] フィールドを使用して、デバイス レベルのフェールオーバーで使用するスタンバイ MAC アドレスを設定できます。

要素	説明
ロール（Roles）	このインターフェイスに割り当てられているすべてのインターフェイス ロールが、このフィールドに一覧表示されます。ロールの割り当ては、このインターフェイスに指定されている名前と、Cisco Security Manager に現在定義されているインターフェイス ロール オブジェクト間のパターン マッチングに基づきます。インターフェイス ロール オブジェクトは、各デバイスの設定が生成されるときに、実際のインターフェイスの IP アドレスで置き換えられます。インターフェイス ロールを使用すると、複数のインターフェイスに適用可能な汎用ルールを定義できます。
DHCP リレーサーバー	IP アドレスを入力するか、またはこのインターフェイスの DHCP 要求をリレーする先のインターフェイス固有の DHCP サーバーを示すネットワーク/ホスト オブジェクトを選択します。複数の値はカンマで区切ります。最大4台のインターフェイス固有の DHCP リレーサーバーと、最大 10 台のグローバルおよびインターフェイス固有の DHCP リレーサーバーを設定できます。
DHCP リレー信頼情報（オプション82）	信頼するこの DHCP クライアント インターフェイスを指定します。DHCP Option 82 を維持するために、インターフェイスを信頼できるインターフェイスとして設定できます。

VNI インターフェイス：[IPv6] タブ

[インターフェイスの追加（Add Interface）] または [インターフェイスの編集（Edit Interface）] ダイアログボックスの [タイプ（Type）] で [VNIインターフェイス（VNI Interface）] を選択した場合、このダイアログボックスには、[全般（General）]、[詳細設定（Advanced）]、[IPv6] の 3 つオプションのタブ付きパネルが表示されます。ここでは、[IPv6] パネルに表示されるこれらのオプションについて説明します。

ナビゲーション パス

IPv6 パネルには [インターフェイスの追加（Add Interface）] と [インターフェイスの編集（Edit Interface）] のダイアログボックスでアクセスできます。これらのダイアログボックスには、デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （43 ページ）の説明に従って、ASA の [インターフェイス（Interfaces）] ページからアクセスできます。

関連項目

- VNI インターフェイスの設定 （20 ページ）
- VNI インターフェイス：[全般（General）] タブ （20 ページ）
- VNI インターフェイス：[詳細（Advanced）] タブ （24 ページ）

フィールド リファレンス

表 *5 : [IPv6]* タブ：*[インターフェイスの追加（Add Interface）]/[インターフェイスの編集（Edit Interface）]* ダイアログ ボックス（*ASA/FWSM*）

要素	説明
IPv6を有効化（Enable IPv6）	IPv6 をイネーブルにして、このインターフェイスで IPv6 アドレスを設定するには、このチェックボックスをオンにします。このオプションをオフにすると、このインターフェイスで IPv6 をディセーブルにできますが、設定情報は保持されます。
Enforce EUI-64	オンにすると、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 ID の使用を適用します。 このオプションがインターフェイスでイネーブルにされると、その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 アドレスに対して検証され、インターフェイス ID が Modified EUI-64 形式を使用していることが確認されます。IPv6 パケットのインターフェイス ID が Modified EUI-64 形式でない場合、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。 「%PIX|ASA-3-325003: EUI-64 source address check failed.」 アドレス形式の検証は、フローが作成された場合にのみ行われます。既存のフローからのパケットは確認されません。さらに、アドレス検証はローカル 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。 Modified EUI-64 形式のインターフェイス ID は、リンク層アドレスの上位 3 バイト（OUI フィールド）と下位 3 バイト（シリアル番号）の間に 16 進数の FFFE を挿入することで、48 ビット リンク層（MAC）アドレスから導出されます。選択されたアドレスが一意のイーサネット MAC アドレスから生成されることを保証するため、上位バイトの下位から 2 番めのビット（ユニバーサル/ローカル ビット）が反転され、48 ビット アドレスの一意性が示されます。たとえば、MAC アドレス 00E0.B601.3B7A のインターフェイスには、02E0:B6FF:FE01:3B7A の 64 ビット インターフェイス ID が指定されます。

要素	説明
DAD Attempts	Duplicate Address Detection（DAD; 重複アドレス検出）の実行中にインターフェイスで送信される連続ネイバー送信要求メッセージの数を指定するには、このフィールドに 0 ～ 600 の数を入力します。0 を入力すると、インターフェイス上で重複アドレス検出がディセーブルになります。1 を入力すると、フォローアップ送信のない一度の送信を設定します。これはデフォルトです。 アドレスがインターフェイスに割り当てられる前に、重複アドレス検出によって、新しいユニキャスト IPv6 アドレスの一意性が確認されます（重複アドレス検出の実行中、新しいアドレスは一時的な状態になります）。重複アドレス検出では、ネイバー送信要求メッセージを使用して、ユニキャスト IPv6 アドレスの一意性を確認します。 重複アドレス検出によって重複アドレスが特定された場合、そのアドレスの状態は DUPLICATE に設定され、アドレスは使用されなくなります。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の場合は、そのインターフェイス上で IPv6 パケットの処理がディセーブルになり、次のようなエラー メッセージが発行されます。 %PIX-4-DUPLICATE: Duplicate address FE80::1 on outside 重複アドレスがインターフェイスのグローバルアドレスの場合は、そのアドレスは使用されず、前述のリンクローカル アドレスと同様のエラー メッセージが発行されます。 重複アドレスに関連付けられているコンフィギュレーション コマンドはすべて設定済みのままになりますが、アドレスの状態は DUPLICATE に設定されます。インターフェイスのリンクローカルアドレスに変更があると、新しいリンクローカルアドレスに対して重複アドレス検出が行われ、そのインターフェイスに関連付けられている他のすべての IPv6 アドレスが再生成されます（つまり、重複アドレス検出は、新しいリンクローカル アドレスでのみ行われます）。
NS Interval	IPv6 ネイバー送信要求メッセージの再送信間隔（ミリ秒単位）。有効な値の範囲は 1000 ～ 3600000 ミリ秒で、デフォルト値は 1000 ミリ秒です。 （注） この値は、このインターフェイスで送信されるすべての IPv6 ルータ アドバタイズメントに含まれます。
Reachable Time	リモート IPv6 ノードが到達可能であることが最初に確認されてから、このノードが到達可能であると見なされ続ける時間（ミリ秒単位）。有効な値の範囲は 0 ～ 3600000 ミリ秒で、デフォルト値は 0 です。この値に 0 を使用する場合、到達可能時間は未定に設定されます。つまり、到達可能時間の設定および追跡は受信デバイス次第です。 設定時間によって、使用不可のネイバーを検知できます。時間を短く設定すると、使用できないネイバーをより早く検出できます。ただし、時間を短くするほど、IPv6 ネットワーク帯域幅とすべての IPv6 ネットワーク デバイスの処理リソースの消費量が増えます。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。

要素	説明
管理対象設定フラグ	IPv6 ルータ アドバタイズメント パケットの「managed-config-flag」フラグを設定するかどうか。
その他の設定フラグ	IPv6 ルータ アドバタイズメント パケットの「other-config-flag」フラグを設定するかどうか。
Enable RA	オンにすると、インターフェイスで IPv6 ルータ アドバタイズメントの送信がイネーブルになります。次のオプションを使用できます。 • [RA Lifetime]：「ルータライフタイム」値は、ローカルリンク上のノードがセキュリティアプライアンスをリンク上のデフォルトルータと見なし続ける期間を指定します。有効な値の範囲は 0 ～ 9000 秒で、デフォルトは 1800 秒です。0 を入力すると、セキュリティ アプライアンスは選択したインターフェイスのデフォルト ルータとは見なされません。 0 以外の任意の値は、次の [RA Interval] 値より小さい値にはできません。 （注） この値は、このインターフェイスで送信されるすべての IPv6 ルータ アドバタイズメントに含まれます。 • [RA Interval]：このインターフェイスでの IPv6 ルータアドバタイズメントの送信間隔。有効な値の範囲は 3 ～ 1800 秒です（次の [RA Interval in Milliseconds] オプションがオンの場合は 500 ～ 1800000 ミリ秒）。デフォルトは 200 秒です。 [RA Lifetime] が 0 以外の場合、送信の間隔は [RA Lifetime] の値以下にする必要があります。他の IPv6 ノードと同期しないようにするには、使用する実際値を必要値の 20 % 以内にランダムに調整します。 • [RA Interval in Milliseconds]：このオプションをオンにすると、指定した [RA Interval] の値が秒ではなくミリ秒になります。

要素	説明
Interface IPv6 Addresses	ダイアログボックスのこのセクションで、インターフェイスに割り当てられている IPv6 アドレスを指定します。 • [Link-Local Address]：インターフェイスに自動的に生成されたリンクローカルアドレスを上書きするには、このフィールドに目的の IPv6 リンクローカルアドレスを入力します。 リンクローカル アドレスは、リンクローカル プレフィックス FE80::/64 と修正 EUI-64 形式のインターフェイス ID で形成されます。たとえば、MAC アドレス 00E0.B601.3B7A のインターフェイスには、リンクローカル アドレス FE80::2E0:B6FF:FE01:3B7A が指定されます。指定されたアドレスを別のホストが使用している場合は、エラーが表示されます。 • [Enable Address Auto-Configuration]：ステートレス自動設定を使用して、インターフェイスで IPv6 アドレスの自動設定をイネーブルにするには、このオプションをオンにします。アドレスは、Router Advertisement（RA; ルータ アドバタイズメント）メッセージで受信されたプレフィックスに基づいて設定されます。リンクローカルアドレスが設定されていなければ、アドレスはこのインターフェイス用に自動的に生成されます。生成されたリンクローカルアドレスを別のホストが使用している場合は、エラーが発生されます。 • [Trust the DHCP Servers for default gateway]：このラジオボタンを選択して、信頼できる送信元（直接接続されたネットワーク）からのルータアドバタイズメントから、デフォルトのルートをインストールします。 • [Ignore trust and accept router advertisements]：このラジオボタンを選択して、別のネットワークからのルータアドバタイズメントから、デフォルトのルートをインストールします。 • このセクションのテーブルには、このインターフェイスに割り当てられている IPv6 アドレスが表示されます。このテーブルの下の [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します（テーブルの使用に説明されているとおり、これらは標準のボタンです）。 [Add Row] および [Edit Row] を使用すると、[IPv6 Address for Interface] ダイアログボックス （87 ページ）が開きます。
Interface IPv6 Prefixes	このセクションのテーブルを使用して、IPv6 ルータ アドバタイズメントに含まれる IPv6 プレフィックス（つまり、IPv6 アドレスのネットワーク部分）を設定します。このテーブルの下の [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します（テーブルの使用に説明されているとおり、これらは標準のボタンです）。 [Add Row] および [Edit Row] を使用すると、[IPv6 Prefix Editor] ダイアログボックス （89 ページ）が開きます。

トンネルインターフェイスの設定

Cisco Security Manager 4.13 は、サイト間 VPN でルートベースの VPN 方式をサポートしています。このサポートには、スタティック クリプト マップ アクセス リストの設定とインターフェイスへのマッピングが必要です。この要件により、大企業および仮想プライベートクラウドは、すべてのリモートサブネットを追跡し、それらをクリプト マップ アクセス リストに含める必要があります。この課題を克服するために、ASA 9.7.1 は、VTI（仮想トンネルインターフェイス）を使用したルートベースの VPN 方式をサポートするよう強化されています。したがって、Cisco Security Manager 4.13 以降では、VPN とそれに関連付けられた IPSec ポリシーのトンネルインターフェイスを定義できます。

VTI は、ハブアンドスポークを使用した通常の IPsec、およびポイントツーポイント VPN トポロジでのみサポートされます。VTI は、フルメッシュトポロジ、エクストラネット VPN トポロジ、および RAVPN ポリシーなどの他のトポロジではサポートされていません。

マルチハブおよびマルチスポークのシナリオでは、トンネルインターフェイスが 1 つのピアから別のピアへの接続を確立するために、インターフェイスロールがハブアンドスポークに適用されていることを確認します。

（注） BGPv6 アドレスは、ASA 9.16(1) 以降のバージョンのデバイスで、ポイントツーポイントおよびハブアンドスポークトポロジのもと、通常の IPSec VTI の IPv6 ファミリでサポートされています。設定した BGPv6 アドレスは、トンネルの IP アドレスと一致する必要があります。一致しない場合、検証エラーがトリガーされます。

（注） [詳細（Advanced ）] タブと [IPv6] タブのオプションは、VTI には適用されません。

ここでは、トンネルインターフェイスの設定方法について説明します。

- [トンネル（Tunnel）] : [全般（General）] タブ （30 ページ）
- トンネルインターフェイス向け IPSec ポリシーの設定 （34 ページ）

[トンネル（Tunnel）] : [全般（General）] タブ

[インターフェイスの追加（Add Interface）] または [インターフェイスの編集（Edit Interface）] ダイアログボックスで、[タイプ（Type）] ドロップダウンから [トンネル（Tunnel）] を選択すると、ダイアログボックスに [全般（General）]、[詳細（Advanced）]、および [IPv6] の 3 つのタブが表示されます。ここでは、[全般（General）] パネルに表示されるオプションについて説明します。

ナビゲーション パス

デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （43 ページ）で説明されているように、[ASAインターフェイス（ASA Interfaces）] ページから [全般（General）] パネルにアクセスできます。

関連項目

- トンネルインターフェイスの設定 （30 ページ）
- トンネルインターフェイス向け IPSec ポリシーの設定 （34 ページ）

フィールド リファレンス

表 *6 : [*全般（*General***）*]* タブ：*[*インターフェイスの追加/編集（***Add/Edit Interface***）*]* ダイアログボックス（***ASA***）**

要素	説明
[Enable Interface]	トンネルインターフェイスがまだ有効になっていない場合は、このボックスをオンにして有効にします。
名前	[Interface Name] を入力します。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。
トンネル インターフェイス	
Tunnel ID	0 ～ 10413 の範囲で一意のトンネル ID を入力します。この ID は内部インターフェイス識別子です。指定し ID はインターフェイス名にマッピングされます。名前と ID のペアは一意である必要があります。 通常の IPSEC VTI VPN では、このフィールドは必須です。
送信元インターフェイス（Source Interface）	VTI の作成に使用する送信元インターフェイスを入力します。IP アドレスはこのインターフェイスから取得されます。 [選択（Select）] ボタンをクリックして、使用可能なインターフェイスから送信元インターフェイスを選択します。詳細については、ポリシーのオブジェクトの選択を参照してください。 • IPv6：このボックスをオンにして、IPv6 アドレスを入力します。 • 送信元IPv6アドレス：送信元 IPv6 アドレスを入力します。 （注） トンネルの送信元と宛先のペアは一意である必要があります。
宛先 IP/ホスト名	VTI に使用されるトンネルの宛先 IP アドレス。4.14 以降、Cisco Security Manager では、宛先 IP としてホスト名を指定できます。 （注） トンネルの送信元と宛先のペアは一意である必要があります。

要素	説明
IPSec トンネルモードを有効にする	IPv4 または IPv6 トンネル保護モードをパスするには、このボックスをオンにします。 次に、2 つの IPSec トンネルモードを示します。 • IPv4：IPv4 を選択して、トンネル保護モードとして IPv4 をパスします。現在、IPSec のみがサポートされています。IPv4 ネットワークはトンネル内にカプセル化されます。 • IPv6：IPv6 を選択して、トンネル保護モードとして IPv6 をパスします。現在、IPSec のみがサポートされています。IPv6 ネットワークはトンネル内にカプセル化されます。
IPv4 モード	チェックボックスをオンにして、IPv4 をトンネル保護モードとしてパスします。現在、IPSec のみがサポートされています。IPv4 ネットワークはトンネル内にカプセル化されます。
IPSec プロファイル	トンネルインターフェイスに添付される IPSec プロファイルを入力します。 ポリシーオブジェクトが Policy Object Manager で作成されている必要があります。ポリシーオブジェクトの作成については、トンネルインターフェイス向け IPSec ポリシーの設定 （34 ページ）を参照してください。 （注） ピアに対して異なる IKEV1 トランスフォームセットを持つ IPSec プロファイルを選択すると、Cisco Security Manager はトンネルインターフェイスを作成しますが、2 つのピア間の接続は確立されません。 [IPSecオブジェクトセレクタ（IPSec Object Selector）] ダイアログからプロファイルを選択するには、[選択（Select）] ボタンをクリックします。詳細については、ポリシーのオブジェクトの選択を参照してください。 （注） ポリシーを指定する場合、トンネル名が入力されていることを確認してください。[名前（Name）] フィールドが空白の場合、Cisco Security Manager はエラーメッセージを表示します。

要素	説明
Profile	トンネルインターフェイスに添付されるIPSecプロファイルを入力します。 ポリシーオブジェクトがPolicy Object Managerで作成されている必要があります。ポリシーオブジェクトの作成については、トンネルインターフェイス向け IPSec ポリシーの設定 （34 ページ）を参照してください。 （注） ピアに対して異なる IKEV1 トランスフォームセットを持つ IPSec プロファイルを選択すると、Cisco Security Manager はトンネルインターフェイスを作成しますが、2 つのピア間の接続は確立されません。 [IPSecオブジェクトセレクタ（IPSec Object Selector）] ダイアログからプロファイルを選択するには、[選択（Select）] ボタンをクリックします。詳細については、ポリシーのオブジェクトの選択を参照してください。 （注） ポリシーを指定する場合、トンネル名が入力されていることを確認してください。[名前（Name）] フィールドが空白の場合、Cisco Security Manager はエラーメッセージを表示します。
IP タイプ（IP Type）	ドロップダウンから、[スタティック IP（ Static IP）] を選択します。 • [IP アドレス（IP Address）] :（ルーテッドモード）[IP アドレス（IP Address）] 領域で、IPv4 アドレスを設定します。IPv6 を設定するには、[IPv6] タブをクリックします。 • [サブネットマスク（Subnet Mask）] : サブネットマスクを指定します。
説明	（任意）インターフェイスの説明を指定します。

通常の IPSec VPN トンネルの確立

以下のチェックポイント（トンネルの設定中： トンネルインターフェイスの設定 （30 ページ））は、通常の IPSec VPN トンネル接続を正常に確立するのに役立ちます。

1. トンネル ID 値を入力する必要があります。
2. 送信元インターフェイスが設定されている必要があり、ISP またはルーティングを介してピアに到達できる必要があります。
3. [宛先IP（Destination IP）] フィールドにピア送信元インターフェイスの IP アドレスを入力する必要があります。
4. [IPSecプロファイル（IPSec Profile）] フィールドの場合：
    1. 両方のピアデバイスに同じ IKEV1 トランスフォームセットを選択します。
    2. ポイントツーポイントトポロジでは、いずれかのピアがレスポンダである必要があります。

3. ハブアンドスポークトポロジでは、ハブをレスポンダとして選択し、すべてのスポークをイニシエータとして選択します。

5. 対象トラフィックを有効にするには、IPV4 モードを設定する必要があります。
6. VPN を確立するには IP アドレスを入力する必要があります。ダイナミック IP アドレスはサポートされていません。
7. 対象トラフィックを有効にするには、スタティックまたは BGP ルーティングを選択します。ファイアウォールポリシーの場合、VTI はスタティックルーティングでのみサポートされます。

（注） ポイントツーポイント トポロジ、および 1 つのハブと 1 つのスポークを持つハブアンドスポークトポロジに対して BGP/スタティックルートが正しく設定されていない場合、Cisco Security Manager からエラーメッセージが表示されます。マルチハブ/スポークシナリオの場合、エラーメッセージは表示されません。

トンネルインターフェイス向け IPSec ポリシーの設定

[IPsecポリシー（IPsec Policy）]ページを使用して、ハブアンドスポークおよびポイントツーポイント VPN トポロジによる通常の IPsec の IKE フェーズ 1 および IKE フェーズ 2 ネゴシエーション中に使用される IPsec ポリシーを設定します。

ポイントツーポイントおよびハブアンドスポークトポロジで、通常の IPSec VTI に対して BGPv6 を有効にできるようになりました。[BGP] ページの [ファミリ（Family）] タブで IPv6 IP アドレスを設定することもできます。

ナビゲーション パス

- [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して [Policy Object Manager] を開きます。[すべてのオブジェクトタイプ（All Object Types）] で、[IPSecプロファイル（IPSec Profile）]をクリックします。プロファイルを追加するには、[追加（Add）] ボタンをクリックします。

フィールド リファレンス

表 *7: IPsec* プロファイル

要素	説明
名前	IPSec ポリシーの名前。
説明	ポリシーの説明。

要素	説明
IKE Version	関連する IKE バージョン（IKEv1 または IKEv2）を選択します。 （注） 4.14 以降、Cisco Security Manager は IKEv2 をサポートしています。ただし、一度に選択できる IKE のバージョンは 1 つだけです。
IKEv1 トランスフォーム セット	トンネルポリシーに使用される IKEv1 トランスフォームセット。トランスフォーム セットは、トンネル内のトラフィックを保護するために使用される認証および暗号化アルゴリズムを指定します。最大 11 個のトランスフォーム セットを選択できます。詳細については、トランスフォーム セットの概要を参照してください。 トランスフォーム セットでは、トンネル モードの IPsec 動作だけを使用できます。 複数の IKEv1 トランスフォームセットを関連付けることができます。選択したトランスフォーム セットの 2 つ以上が両方のピアでサポートされている場合は、最も高いセキュリティを提供するトランスフォームセットが使用されます。 （注） トンネルが機能するには、両方のピアの IKEv1 トランスフォームセットが同じである必要があります。 [選択（Select）] をクリックして、トポロジで使用する IPSec トランスフォーム セット ポリシー オブジェクトを選択します。必要なオブジェクトがまだ定義されていない場合、選択ダイアログボックスの使用可能なオブジェクトリストの下にある [作成（Create）]（+）ボタンをクリックして、新しいオブジェクトを作成できます。詳細については、IPSec IKEv1 または IKEv2 トランスフォーム セット ポリシー オブジェクトの設定を参照してください。 このフィールドは IKEv2 では使用できません。
[IKEv2 IPSecプロポーザル（IKEv2 IPSec Proposal）]（ASA 9.8(1) 以降）	[選択（Select）] をクリックして、トンネルポリシーに使用する IPSec プロポーザルを選択します。Cisco Security Manager では、複数のプロポーザルを選択できます。必要なオブジェクトがまだ定義されていない場合、選択ダイアログボックスの使用可能なオブジェクトリストの下にある [作成（Create）]（+）ボタンをクリックして、新しいオブジェクトを作成できます。詳細については、IPSec IKEv1 または IKEv2 トランスフォーム セット ポリシー オブジェクトの設定を参照してください。 このフィールドは IKEv1 では使用できません。

要素	説明
[トラストポイント（Trustpoint）]（ASA 9.8(1) 以降）	[選択（Select）] をクリックして、参加している IPSec ネットワークデバイスに証明書を発行する CA サーバーを選択します。このポリシーで設定されたピアは、選択した CA サーバーからデジタル証明書を取得します。指定できるトラストポイントは 1 つのみです。 IKEv1 の場合、認証にトラストポイントが使用されるときに、イニシエータは IPSec プロファイルのトラストポイント設定で指定されたトラストポイントを持っている必要があります。レスポンダの場合、トラストポイントはトンネルグループ CLI で指定する必要があります（非 VTI 設定と同様）。 （注） サイト間 VPN でトラストポイント設定が認証として使用される場合、IKE プロファイルが証明書に含まれている必要があります。トンネルを稼働させるには、VTI VPN のサイト間 VPN マネージャで、IKE プロファイル CLI とトンネルグループ CLI の間におけるアクティビティの検証が必要です。 IKEv2 の場合、認証にトラストポイントが使用されるときに、トラストポイント CLI は、イニシエータとレスポンダ両方のトンネルグループ CLI で指定されます。
[証明書チェーン（Certificate Chain）]（ASA 9.8(1) 以降）	許可のための証明書チェーン送信を有効にするには、このチェックボックスを選択します。 証明書チェーンには、ルート CA 証明書、ID 証明書、およびキー ペアが含まれます。
[レスポンダのみ（Responder Only）]	このポリシーに関連付けられたピアがレスポンダとして機能するように設定するには、このチェックボックスをオンにします。ピアの一方だけがレスポンダのみの設定になっていることを確認します。

要素	説明
Enable Perfect Forward Secrecy (PFS) 係数グループ（Modulus Group）	暗号化された各交換で一意のセッション キーを生成および使用するために、Perfect Forward Secrecy（PFS; 完全転送秘密）の使用をイネーブルにするかどうかを指定します。IPsec ネゴシエーションでは、PFS によって、新しい各暗号キーが以前のいずれのキーとも関連しないことが保証されます。 このオプションを選択する場合は、[係数グループ（Modulus Group）] リストで、PFS セッションキーの生成時に使用する Diffie-Hellman キー導出アルゴリズムも選択します。オプションの説明については、使用する Diffie-Hellman 係数グループの決定を参照してください。 次の係数グループは、IKEv1 ではサポートされていません。IKEv1 ではこれらを選択しないでください。 • group19 • group20 • group21 • group24 • group1 （注） Cisco Security Manager 4.19 以降、DH グループ 1 オプションは、ASA 9.12(1) 以降のデバイスではサポートされません。
[ライフタイム（秒）（Lifetime (Seconds)）] [ライフタイム（KB）（Lifetime (Kilobytes)）]	暗号化 IPsec セキュリティ アソシエーション（SA）のグローバルなライフタイム設定。IPSec ライフタイムは、秒、KB、またはその両方で指定できます。 • [秒（Seconds）]：SA が期限切れになるまでに存続できる秒数。120 ～ 2147483647 秒の範囲内の値を入力します。 • [KB（Kilobytes）]：特定の SA が期限切れになる前にその SA を使用して IPSec ピア間を通過できるトラフィック量（KB 単位）。有効な値は、デバイス タイプに応じて異なります。10 ～ 2147483647 の範囲内の値を入力します。 無制限に許可するには、[無制限のライフタイムを有効にする（KB）（Enable Unlimited Lifetime (Kilobytes)）] チェックボックスをオンにします。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。

要素	説明
デバイスごとに値のオーバーライドを許可	このオブジェクトのプロパティを個々のデバイスで再定義できるようする場合に選択します。 デバイスのオーバーライドを許可した場合は、[Edit] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[Overrides] フィールドは、このオブジェクトに対するオーバーライドを持つデバイスの数を示します。

（注） DH グループ 2、5、および 24 は、ASA 9.14(1) 以降のデバイスではサポートされません。

VLAN インターフェイスの設定

バージョン 4.20 以降、Cisco Security Manager は、Cisco FPR-1010 適応型セキュリティアプライアンスでの L2 ハードウェアスイッチングをサポートしています。L2 スイッチングのサポートを利用するには、それぞれの VLAN インターフェイスを設定する必要があります。

[VLANインターフェイス（VLAN Interface）]：[全般（General）] タブ

[インターフェイスの追加（Add Interface）] または [インターフェイスの編集（Edit Interface）] ダイアログボックスで、[タイプ（Type）] ドロップダウンリストから [VLANインターフェイス（VLAN Interface）] を選択すると、ダイアログボックスに [全般（General）]、[詳細（Advanced）]、[IPv6]、[スイッチポート（Switch Port）]、および [Power over Ethernet] の 5 つのタブが表示されます。

（注） VLAN インターフェイスに [スイッチポート（Switch Port）] と [Power over Ethernet] を設定することはできません。

ナビゲーション パス

デバイスポリシーセレクタから [インターフェイス（Interfaces）] > [インターフェイスの追加（Add Interface）] を選択し、[タイプ（Type）] ドロップダウンリストから [VALNインターフェイス（VLAN Interface）] を選択します。

フィールド リファレンス

表 8 : [General] タブ：[Add Interface]/[Edit Interface] ダイアログボックス

要素	説明
インターフェイスの有効化	VLAN インターフェイスがまだ有効になっていない場合は、このボックスをオンにして有効にします。

要素	説明
管理専用	[管理専用（Management Only）] 機能を有効にするには、このチェックボックスをオンにします。オンにすると、このデバイスへのトラフィックのみを許可するデバイス管理用にインターフェイスが予約されます。他のインターフェイスおよびデバイスへのパススルートラフィックは拒否されます。
名前	[Interface Name] を入力します。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。
セキュリティレベル	[Security Level] に 0（最低）～100（最高）を入力します。
L2 VLAN ID	0（最低）～ 4090（最高）の L2 VLAN ID を入力します。これは必須フィールドです。
非転送インターフェイス VLAN ID	0（最低）～ 4090（最高）の非転送インターフェイス VLAN ID を入力します。
ルート マップ	[ルートマップオブジェクトセレクタ（Route Map Object Selector）] ダイアログボックスから [ルートマップ（Route Map）] を選択します。[フィルタ（Filter）] ドロップダウンリストから適用するフィルタを選択するか、[フィルタの作成（Create Filter）] オプションを使用して新しいフィルタを作成します。
IP タイプ	使用可能な次のオプションから IP タイプを選択します。[スタティックIP（Static IP）]、[DHCPを使用（Use DHCP）]、および [PPPoE（PIXおよびASA 7.2+）（PPPoE (PIX and ASA 7.2+)）]
スタティック IP	[IPアドレス（IP Address）]：（ルーテッドモード）[IPアドレス（IP Address）] 領域で、IPv4 アドレスを設定します。IPv6 を設定するには、[IPv6] タブをクリックします。 [サブネットマスク（Subnet Mask）]：サブネットマスクを指定します。

要素	説明
DHCP を使用する	[DHCP学習済みルートメトリック（DHCP Learned Route Metric）]：（必須）アドミニストレーティブ ディスタンスを学習したルートに割り当てるには、[DHCP学習済みルートメトリック（DHCP Learned Route Metric）] フィールドに 1 ～ 255 の値を入力します。このフィールドを空白のままにすると、既知のルートのアドミニストレーティブ ディスタンスは 1 になります。 [DHCPを使用したデフォルトルートの取得（Obtain Default Route using DHCP）]：デフォルト スタティック ルートを設定する必要がないように DHCP サーバーからデフォルトルートを取得するには、このオプションを選択します。 [DHCP学習済みルートのトラッキングの有効化（Enable Tracking for DHCP Learned Route）]：（任意）[DHCPを使用したデフォルトルートの取得（Obtain Default Route using DHCP）] を選択した場合、このオプションを選択し、特定のサービスレベル契約（SLA）モニターによるルートトラッキングを有効にできます。次のオプションが使用可能になります。 [トラッキング済みSLAモニター（Tracked SLA Monitor）]：[DHCP学習済みルートのトラッキングの有効化（Enable Tracking for DHCP Learned Route）] を選択した場合は必須です。このインターフェイスに適用されるルート トラッキング（接続性のモニタリング）を定義している SLA モニタ オブジェクトの名前を入力または選択します。

要素	説明
PPPoE（PIXおよびASA 7.2+）	

要素	説明
	Point-to-Point Protocol over Ethernet（PPPoE）を有効にして、接続ネットワーク上のPPPoEサーバーからIPアドレスが自動的に割り当てられるようにします。このオプションは、フェールオーバーではサポートされません。[IPタイプ（IP Type）] ドロップダウンから [PPPoE（PIXおよびASA 7.2+）（PPPoE (PIX and ASA 7.2+)）] を選択すると、次のオプションが使用可能になります。 [VPDNグループ名（VPDN Group Name）]（必須）：ネットワーク接続、ネゴシエーション、および認証に使用する認証方式とユーザー名/パスワードが含まれるバーチャル プライベート ダイヤルアップ ネットワーク（VPDN）グループを選択します。詳細については、VPDNグループの管理 （114 ページ）を参照してください。 [IPアドレス（IP Address）]：指定した場合、ネゴシエートされたアドレスではなく、このスタティック IP アドレスが接続および認証に使用されます。 [サブネットマスク（Subnet Mask）]：指定した IP アドレスとともに使用されるサブネットマスク。 [PPPoE学習済みルートメトリック（PPPoE Learned Route Metric）]（必須）：学習したルートにアドミニストレーティブ ディスタンスを割り当てます。有効な値は 1 ～ 255 です。デフォルトは 1 です。 すべてのルートに、その使用プライオリティを示す値または「メトリック」があります。（このメトリックは「アドミニストレーティブ ディスタンス」とも呼ばれます）同じ接続先に対して 2 つ以上のルートが使用可能な場合、デバイスはアドミニストレーティブ ディスタンスを使って使用するルートを決定します。 [PPPoEを使用したデフォルトルーティングの取得（Obtain Default Routing Using PPPoE）]：このオプションを選択して、PPPoE サーバーからデフォルトルートを取得します。このオ

要素	説明
	プションを選択すると、PPPoE クライアントが接続をまだ確立していない場合に、デフォルトルートが設定されます。このオプションを使用する場合は、スタティックに定義されたルートを設定に含めることができません。 [PPPoE学習ルートのトラッキングの有効化（Enable Tracking for PPPoE Learned Route）]：[PPPoEを使用したデフォルトルーティングの取得（Obtain Default Routing Using PPPoE）] を選択した場合、このオプションを選択して、PPPoE が学習したルートのルートトラッキングを有効化できます。選択すると、次のオプションが使用可能になります。 [デュアルISPインターフェイス（Dual ISP Interface）]：デュアル ISP サポート用のインターフェイスを定義する場合、設定中の接続を示す [プライマリ（Primary）] または [セカンダリ（Secondary）] を選択します。 [トラッキング済みSLAモニター（Tracked SLA Monitor）]：[DHCP学習済みルートのトラッキングの有効化（Enable Tracking for DHCP Learned Route）] を選択した場合は必須です。このインターフェイスに適用されるルート トラッキング（接続性のモニタリング）を定義している SLA モニタ オブジェクトの名前を入力または選択します。
説明	（任意）インターフェイスの説明を指定します。

デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理

[Interfaces] ページには、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、仮想インターフェイス（VLAN）、および EtherChannel インターフェイスが表示されます。また、選択したデバイスに設定されているハードウェア ポートとブリッジ グループが表示され、それらを追加、編集、および削除できます。

使用可能なインターフェイスのタイプは、デバイス タイプ、オペレーティング システムのバージョン、およびモード（ルーテッドまたはトランスペアレント）によって異なります。たとえば、EtherChannel インターフェイスは、ルーテッドとトランスペアレントの両方のモードにあ

る ASA 8.4.1 以降のデバイスでのみ使用できます。詳細については、デバイス インターフェイスについて （4 ページ）を参照してください。

（注） ASA 5505 デバイスに表示される [インターフェイス（Interfaces）] ページには、[インターフェイス（Interfaces）] および [ハードウェアポート（Hardware Ports）] の 2 つのタブ付きパネルが表示されます。同様に、トランスペアレントモードで動作している Firewall Services Module（FWSM; ファイアウォール サービス モジュール）バージョン 3.1 以降と ASA バージョン 8.4.1 以降の両方に表示される [インターフェイス（Interfaces）] ページにも、[インターフェイス（Interfaces）] および [ブリッジグループ（Bridge Groups）] の 2 つのタブ付きパネルが表示されます。これらの機能の設定については、次の手順にあるリンクを参照してください。

各セキュリティ デバイスが設定され、各アクティブ インターフェイスがイネーブルになっている必要があります。非アクティブインターフェイスをディセーブルにすることができます。ディセーブルにした場合、インターフェイスでデータの送受信は行われませんが、その設定情報は保持されます。

新しいセキュリティ デバイスをブートストラップした場合、設定機能で設定されるのは、内部インターフェイスに関連付けられたアドレスおよび名前だけです。そのセキュリティ デバイスを通過するトラフィックのアクセス ルールおよび変換ルールを指定する前に、そのデバイス上の残りのインターフェイスを定義する必要があります。

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渡すことができます。ただし、専用の管理インターフェイスがプラットフォームに含まれている場合は、そのインターフェイス（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の第 3 のインターフェイスとして使用できます。

セキュリティ デバイスのインターフェイスと関連オプションを管理するには、次の手順を行います。選択したデバイスのタイプに応じて、設定されているインターフェイス、サブインターフェイス、冗長インターフェイス、仮想インターフェイス（VLAN）、EtherChannel インターフェイス、ハードウェア ポート、およびブリッジ グループを追加、編集、および削除できます。

ステップ 1 デバイスビューが現在のアプリケーションビューであることを確認します。必要に応じて、ツールバーの [デバイスビュー（Device View）] ボタンをクリックします。

（注） デバイス ビューを使用したデバイス ポリシーの設定の詳細については、デバイス ビューおよび Site-to-Site VPN Manager におけるポリシーの管理を参照してください。

ステップ 2 設定するセキュリティ デバイスを選択します。

ステップ 3 デバイスポリシーセレクタで [インターフェイス（Interfaces）] を選択します。

[Interfaces] ページが表示されます。表示される情報およびページは、選択したデバイス タイプおよびバージョン、動作モード（ルーテッドまたはトランスペアレント）、およびデバイスでホストするコンテキスト（シングルコンテキストまたはマルチコンテキスト）によって異なります。

ASA 5505 デバイスの [Interfaces] ページには、[Hardware Ports] および [Interfaces] の 2 つのタブ付きパネルが表示されます。同様に、トランスペアレント モードで動作している FWSM（バージョン 3.1 以降）および ASA（バージョン 8.4.1 以降）の両方に表示される [Interfaces] ページにも、[Interfaces] および [Bridge Groups] の 2 つのタブ付きパネルが表示されます。

ステップ 4 必要に応じて、インターフェイスと関連オプションを追加、編集、および削除します。

[Interfaces] ページまたはパネルと [Bridge Groups] および [Hardware Ports] パネルには、Security Manager の標準のテーブルが表示されます。テーブルの使用で説明されているとおり、このテーブルには [Add Row]、[Edit Row]、[Delete Row] ボタンがあります。

[行の追加（Add Row）] または [行の編集（Edit Row）] ボタンをクリックして表示される実際のダイアログボックスは、選択したデバイス（およびパネル）のタイプによって異なります。デバイス固有のダイアログボックスについては、次のトピックを参照してください。

- [Add Interface]/[Edit Interface] ダイアログボックス（PIX 6.3） （45 ページ）
- [インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM） （50 ページ）
- ASA 5505 でのハードウェア ポートの設定 （99 ページ）
- [Add Bridge Group]/[Edit Bridge Group] ダイアログボックス （102 ページ）

ステップ 5 同じセキュリティ レベルが設定されているインターフェイス間の通信のイネーブル化などを設定する [Advanced Interface Settings] を管理するには、[Interfaces] ページの下部にある [Add Row] ボタンをクリックして、[Advanced Interface Settings] ダイアログボックスを開きます。詳細については、高度なインターフェイス設定（PIX/ASA/FWSM） （110 ページ）を参照してください。

ステップ 6 インターフェイスの追加、編集、削除が終わったら、ウィンドウの下部にある [保存（Save）] をクリックして、インターフェイス定義を Cisco Security Manager サーバーに保存します。

[Add Interface]/[Edit Interface] ダイアログボックス（PIX 6.3）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしますが、バグ修正や拡張機能はサポートしていません。

表 *9 : [Add Interface]/[Edit Interface] ダイアログボックス（PIX 6.3）*

要素	説明
[Enable Interface]	このインターフェイスでトラフィックを渡せるようにします。セキュリティ ポリシーに応じてトラフィックが通過できるようにするには、この設定に加えて、[IP Type] と [Name] を指定する必要があります。 イネーブルにした任意の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イネーブルにする必要があります。

要素	説明
タイプ（Type）	インターフェイスのタイプを選択します。 • [物理（Physical）]：VLANは、その基礎となるハードウェアインターフェイスと同じネットワーク上にあります。 • [論理（Logical）]：VLANは論理インターフェイスに関連付けられます。
名前	最大48文字のインターフェイス名を指定します。[Name]には、インターフェイスの用途に関係する覚えやすい名前を付けます。サポートされるインターフェイス名は、次のとおりです。 • [Inside]：内部ネットワークに接続します。最もセキュアなインターフェイスにする必要があります。 • [DMZ]：非武装地帯（中間インターフェイス）。境界ネットワークとも呼ばれます。 • [Outside]：外部ネットワークまたはインターネットに接続します。セキュア度の最も低いインターフェイスにする必要があります。
Hardware Port	物理ネットワーク インターフェイスを定義する場合、この値は、デバイスでのインターフェイス タイプとそのスロットまたはポートを識別する名前を表します。 論理ネットワーク インターフェイスを追加する場合、論理インターフェイスを追加する、イネーブル化された任意の物理インターフェイスを選択できます。目的のハードウェア ポートが表示されない場合は、インターフェイスがイネーブルであることを確認してください。 有効な値は次のとおりです。 • ethernet0 ～ ethernet*n*。 • gb-ethernet*n* 。 *n* は、デバイスでのネットワーク インターフェイスの番号を表します。
IP タイプ（IP Type）	[IPタイプ（IP Type）] では、インターフェイスに使用する IP アドレス指定のタイプを定義します。[スタティックiP（Static IP）]または[DHCPの使用（Use DHCP）] を選択します（デバイス インターフェイス：IP タイプ（PIX 6.3）（48 ページ）を参照）。（PPPoE オプションは PIX 6.3 デバイスには適用できません）。 （注） DHCP は、セキュリティアプライアンスの外部インターフェイスにのみ設定できます。

要素	説明
Speed and Duplex	物理インターフェイスの速度オプションが表示されます。論理インターフェイスには適用されません。次のいずれかのオプションを選択します。 • [auto]：イーサネットの速度を自動的に設定します。[auto] キーワードは、Intel 10/100 自動速度検出ネットワーク インターフェイス カードでのみ使用できます。 • [10baset]：10 Mbps イーサネット半二重。 • [10full]：10 Mbps イーサネット全二重。 • [100basetx]：100 Mbps イーサネット半二重。 • [100full]：100-Mbps イーサネット全二重。 • [1000auto]：1000 Mbps イーサネット（全二重または半二重をオートネゴシエーション）。 ヒント　ネットワーク内のスイッチなどのデバイスとの互換性を維持するために、このオプションを使用しないことを推奨します。 • [1000full]：オートネゴシエーション、アドバタイジング 1000 Mbps イーサネット全二重。 • [1000full nonnegotiate]：1000 Mbps イーサネット全二重。 • [aui]：AUI ケーブルインターフェイスとの 10 Mbps イーサネット半二重通信。 • [bnc]：BNC ケーブルインターフェイスとの 10 Mbps イーサネット半二重通信。 （注）　自動検知を正しく処理しないスイッチなどのデバイスがネットワーク環境に含まれている場合に、ネットワーク インターフェイスの速度を指定することを推奨します。
MTU	最大パケット サイズ、つまり最大伝送単位（MTU）をバイト数で指定します。この値は、インターフェイスに接続されているネットワークのタイプによって異なります。有効な値は 300 ～ 65535 バイトです。デフォルトは 1500 です。
Physical VLAN ID	物理インターフェイスでは、VLAN ID を 1 ～ 4094 の範囲で入力します。この VLAN ID は、接続されているデバイスで使用中であってはなりません。
Logical VLAN ID	この論理インターフェイスに関連付けられた VLAN のエイリアスを 1 ～ 4094 の値で指定します。この値は、論理インターフェイスのタイプが選択されている場合に必要です。

要素	説明
セキュリティ レベル（Security Level）	インターフェイスのセキュリティ レベルを指定します。0（最もセキュア度の低い）～ 100（最もセキュア度の高い）の値を入力します。セキュリティ アプライアンスにより、トラフィックは、内部ネットワークから外部ネットワーク（セキュリティ レベルがより低い）まで自由に通過できます。他の多くのセキュリティ機能が、2 つのインターフェイスの相対的なセキュリティ レベルによる影響を受けます。 • 外部インターフェイスは、常に 0 です。 • 内部インターフェイスは、常に 100 です。 • DMZ インターフェイスの値の範囲は 1 ～ 99 です。
ロール（Roles）	ロールの詳細とその定義方法および使用方法については、インターフェイス ロール オブジェクトについてを参照してください。 このインターフェイスに割り当てられているすべてのインターフェイス ロールが、このフィールドに一覧表示されます。ロールの割り当ては、このインターフェイスに指定されている名前と、Cisco Security Manager に現在定義されているインターフェイス ロール オブジェクト間のパターン マッチングに基づきます。 インターフェイス ロール オブジェクトは、各デバイスの設定が生成されるときに、実際のインターフェイスの IP アドレスで置き換えられます。インターフェイス ロールを使用すると、複数のインターフェイスに適用可能な汎用ルールを定義できます。 ロールの詳細とその定義方法および使用方法については、インターフェイス ロール オブジェクトについてを参照してください。

デバイス インターフェイス：IP タイプ（PIX 6.3）

PIX 6.3 のセキュリティ デバイスには、そのインターフェイスの IP アドレス指定が必要です。ただし、ファイアウォール インターフェイスには、割り当てられるまで IP アドレスがありません。

PIX 6.3 セキュリティ デバイスで表示される [インターフェイスの追加（Add Interface）] または [インターフェイスの編集（Edit Interface）] ダイアログボックスには、[IP タイプ（IP Type）] セクションがあります。次の説明に従って、インターフェイスの IP アドレス指定のタイプをここに指定して、関連するパラメータを入力します。ダイアログボックスの他のセクションについては、[Add Interface]/[Edit Interface] ダイアログボックス（PIX 6.3） （45 ページ）を参照してください。

（注） その他のセキュリティ アプライアンス用に表示される [IP Type] オプションについては、デバイス インターフェイス：IP タイプ（PIX/ASA 7.0 以降） （94 ページ）を参照してください。

[インターフェイスの追加（Add Interface）] または [インターフェイスの編集（Edit Interface）] ダイアログボックスで、次のように、[IPタイプ（IP Type）] リストからアドレス割り当て方式を選択し、関連パラメータを指定します。

- [スタティック IP（Static IP）]：このインターフェイスが接続するネットワーク上のセキュリティデバイスを示すスタティック IP アドレスおよびサブネットマスクを指定します。IP アドレスは、インターフェイスごとに一意でなければなりません。

サブネット マスクは、ドット区切り 10 進表記（255.255.255.0 など）で表すか、またはネットワーク マスクのビット数（24 など）を入力して表すことができます。バージョン 4.13 以降、Cisco Security Manager では、ポイント ツー ポイント インターフェイスに 255.255.255.254 を使用できます。ネットワークに接続するインターフェイスには 255.255.255.255 を使用しないでください。使用すると、トラフィックがこのインターフェイスで停止します。サブネット マスク値を指定しない場合は、次に示すように「クラスフル」ネットワークが使用されます。

-
  - IP アドレスの最初のオクテットが 1 ～ 126 の場合（つまり、アドレスが 1.0.0.0 ～ 126.255.255.255 の場合）、クラス A ネットマスク（255.0.0.0）が使用されます。
  - IP アドレスの最初のオクテットが 128 ～ 191 の場合（つまり、アドレスが 128.0.0.0 ～ 191.255.255.255 の場合）、クラス B ネットマスク（255.255.0.0）が使用されます。
  - IP アドレスの最初のオクテットが 192 ～ 223 の場合（つまり、アドレスが 192.0.0.0 ～ 223.255.255.255 の場合）、クラス C ネットマスク（255.255.255.0）が使用されます。

（注） グローバル プールやスタティック NAT エントリの IP アドレスなど、以前にルータ、ホスト、または他のファイアウォール デバイス コマンドに使用したアドレスは使用しないでください。

- [Use DHCP]：Dynamic Host Configuration Protocol（DHCP）をイネーブルにして、接続ネットワーク上の DHCP サーバから IP アドレスが自動的に割り当てられるようにします。次のオプションを使用できます。
  - [DHCPを使用したデフォルトルートの取得（Obtain Default Route using DHCP）]：デフォルトのスタティックルートを設定する必要がないように DHCP サーバーからデフォルトルートを取得するには、このチェックボックスをオンにします。
  - [再試行回数（Retry Count）]：PIX が DHCP 要求を再送信する回数。有効な値は 4 ～ 16 です。デフォルトは 2 です。
- [PPPoE（PIX および ASA 7.2 以降）（PPPoE (PIX and ASA 7.2+)）]：このオプションは PIX 6.3 デバイスには適用されません。

（注） DHCP は、ファイアウォール デバイスの外部インターフェイスにのみ設定できます。

[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしていますが、バグ修正や拡張機能はサポートしていません。

これらの [インターフェイスの追加（Add Interface）] と [インターフェイスの編集（Edit Interface）] ダイアログボックスは、PIX 7.0 以降、ASA、FPR、および FWSM デバイスでインターフェイス、サブインターフェイス、冗長インターフェイス、および EtherChannel インターフェイスを定義および設定するために使用します。[Add Interface] と [Edit Interface] ダイアログボックスには、[Interfaces] ページからアクセスできます。詳細については、デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （43 ページ）を参照してください。

（注） バージョン 4.24 以降、Cisco Security Manager は、ASA 9.17(1) 以降のデバイスの FPR-3100 シリーズのデバイスをサポートします。

（注） スイッチ機能とセキュリティ アプライアンス機能を組み合わせた ASA 5505 は、物理スイッチ ポートと論理 VLAN インターフェイスの両方を設定する特殊な事例です。したがって、ASA 5505 デバイスに表示される [インターフェイス（Interfaces）] ページには、[ハードウェアポート（Hardware Ports）] および [インターフェイス（Interfaces）] の 2 つのタブ付きパネルが表示されます。詳細については、ASA 5505 のポートおよびインターフェイスについて （8 ページ）を参照してください。トランスペアレントモードで動作している ASA 8.4.1 以降および FWSM 3.1 以降のデバイスにも、[インターフェイス（Interfaces）] および [ブリッジグループ（Bridge Groups）] の 2 つのタブ付きパネルが表示されます。ブリッジ グループの設定については、[Add Bridge Group]/[Edit Bridge Group] ダイアログボックス （102 ページ）を参照してください。

これらのダイアログボックスに表示されるパラメータの多くは、デバイス タイプとバージョン、動作モード（ルーテッドまたはトランスペアレント）、およびデバイスでホストするコンテキスト（シングルコンテキストまたはマルチコンテキスト）によって異なります。

（注） フェールオーバーにインターフェイスを使用する場合は、[インターフェイスの追加（Add Interface）] ダイアログボックスでそのインターフェイスを定義できますが、ここでは設定せずに、代わりに [フェールオーバー（Failover）] ページを使用してください。特に、インターフェイス名は指定しないでください。このパラメータを指定すると、インターフェイスをフェールオーバー リンクとして使用できなくなります。

[Add Interface] と [Edit Interface] ダイアログボックスの使用

次の手順では、これらのダイアログボックスの一般的な使用方法を説明します。

1. [Add Interface] と [Edit Interface] ダイアログボックスの上部に、インターフェイスの [Type] ドロップダウン リストが表示されます

（注） Catalyst 6500 サービスモジュール（ASA-SM および FWSM）および ASA 5505 では、[タイプ（Type）] リストは表示されません。

デバイスタイプ、オペレーティングシステムのバージョン、動作モード（ルータまたはトランスペアレント）に応じて、[タイプ（Type）] には次のうちの 2 ～ 3 個のオプション、またはすべてのオプションが表示されます。

- • [物理インターフェイス（Physical Interface）]：デバイスに物理インターフェイスを設定するには、このオプションを選択します。
  - [サブインターフェイス（Sub-Interface）]：以前に定義した物理インターフェイスに関連付けられる論理インターフェイス（またはVLAN接続）を設定するには、このオプションを選択します。詳細については、サブインターフェイスの設定（PIX/ASA）（9 ページ）を参照してください。
  - [冗長（Redundant）]：2 つの物理インターフェイスを単一の論理的な「冗長インターフェイス」として設定するには、このオプションを選択します。詳細については、冗長インターフェイスの設定 （11 ページ）を参照してください。
  - [EtherChannel]：最大 8 つの個別のイーサネットリンクのバンドルで構成されている論理インターフェイスを設定するには、このオプションを選択します。このバンドルは EtherChannel またはポートチャネル インターフェイスと呼ばれます（このオプションは ASA 8.4 以降のデバイスでのみ使用できます）。詳細については、EtherChannel の設定 （13 ページ）を参照してください。
  - [VNIインターフェイス（VNI Interface）]：VNI インターフェイスを設定するには、このオプションを選択します。VNI インターフェイスは、タギングを使用して特定の物理インターフェイスでのネットワークトラフィックの分割を維持する仮想インターフェイスです。各VNIインターフェイスにセキュリティ ポリシーを直接適用します。すべての VNI インターフェイスは、同じ VTEP インターフェイスに関連付けられま

す。詳細については、VNI インターフェイスの設定 （20 ページ）を参照してください。

- [トンネル（Tunnel）]：このオプションを選択して論理インターフェイス（VTI）を構成し、サイト間 VPN トポロジのルートベースの VPN 方式をサポートします。詳細については、トンネルインターフェイスの設定 （30 ページ）を参照してください。

- [Type] オプションの下部のダイアログボックスには、最大 3 つのタブ付きパネルが表示されます。このパネルもデバイス タイプ、オペレーティング システムのバージョン、および動作モードによって異なります。

PIX 7.0 以降の [Add Interface] と [Edit Interface] ダイアログボックスには、[General] と [Advanced] の 2 つのタブ付きパネルが表示されます。ASA 7.0 以降の [Add Interface] と [Edit Interface] ダイアログボックスには、[General]、[Advanced]、[IPv6] の 3 つのタブ付きパネルが表示されます。

FPR-3100 の [インターフェイスの追加（Add Interface）] と [インターフェイスの編集（Edit Interface）] ダイアログボックスには、[一般（General）]、[詳細（Advanced）]、[IPv6] の 3 つのタブ付きパネルが表示されます。

- - [General] オプションを必要に応じて設定します。このパネルについては、[Add Interface]/[Edit Interface] ダイアログボックス - [General] タブ（PIX 7.0 以降/ASA/FWSM）（52 ページ）を参照してください。

  - [Advanced] パネル オプションを必要に応じて設定します。このパネルについては、[Add Interface]/[Edit Interface] ダイアログボックス - [Advanced] タブ（ASA/PIX 7.0 以降） （66 ページ）を参照してください。

  - [IPv6] オプションを必要に応じて設定します。このパネルについては、IPv6 インターフェイスの設定（ASA/FWSM） （79 ページ）を参照してください。

  - 必要に応じて、[スイッチ ポート（Switch Port）] のオプションを設定します。このオプションの詳細については、[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス：[スイッチポート（Switch Port）] タブ （98 ページ）を参照してください。

  - 必要に応じて [Power Over Ethernet] のオプションを設定します。このオプションの詳細については、[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス：[Power Over Ethernet] タブ （99 ページ）を参照してください。

- このインターフェイスの設定が終了したら、[OK] をクリックしてダイアログボックスを閉じ、デバイスの [インターフェイス（Interfaces）] ページに戻ります。

[Add Interface]/[Edit Interface] ダイアログボックス - [General] タブ（PIX 7.0 以降/ASA/FWSM）

[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM） （50 ページ）は、ファイアウォール デバイスでインターフェイス、サブインターフェイス、VLAN インターフェイス、冗長インターフェイスおよび EtherChannel インターフェイスを定義および設定するために使用します。[Add Interface] と [Edit Interface] ダイアログボックスには、[Interfaces] ページからアクセスできます。詳細については、デバイス

インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （43 ページ）を参照してください。

（注） 以下の説明では、「インターフェイス」という用語はインターフェイスのタイプを表す一般的な用語として使用されます。

このダイアログボックスの [General] パネルは、[Name]、[Security Level]、[IP Type] パラメータなどの一般的なインターフェイスの値を設定するために使用します。このパネルに表示されるパラメータの多くは、デバイスタイプとバージョン、動作モード（ルーテッドまたはトランスペアレント）、およびデバイスでホストするコンテキスト（シングルコンテキストまたはマルチコンテキスト）によって異なります。そのため、次の表のオプションによっては、設定しているデバイスに表示されないものもあります。

関連項目

- サブインターフェイスの設定（PIX/ASA） （9 ページ）
- 冗長インターフェイスの設定 （11 ページ）
- EtherChannel の設定 （13 ページ）
- [Add Interface]/[Edit Interface] ダイアログボックス - [Advanced] タブ（ASA/PIX 7.0 以降）（66 ページ）
- IPv6 インターフェイスの設定（ASA/FWSM） （79 ページ）
- ASA 5505 のポートおよびインターフェイスについて （8 ページ）
- ASA 5505 でのハードウェア ポートの設定 （99 ページ）

表 *10 : [General]* タブ：*[Add Interface]/[Edit Interface]* ダイアログボックス

要素	説明
[Enable Interface]	このインターフェイスでトラフィックを渡せるようにします。 デフォルトでは、すべての物理インターフェイスがシャットダウンされています。インターフェイスがイネーブルでない場合、トラフィックはあらゆるタイプのインターフェイスを通過できません。サブインターフェイスなどの論理インターフェイスを定義する場合は、サブインターフェイスを定義する前に、関連付ける物理インターフェイスをイネーブルにします。冗長インターフェイスまたは EtherChannel インターフェイスを定義する場合は、グループインターフェイスを定義する前に、メンバインターフェイスをイネーブルにします。 このオプションをオンにする場合、セキュリティ ポリシーに従ってトラフィックが通過できるようにするためには [Name] も指定し、ルーテッドモードでは [IP Type] も指定します（または FWSM または ASA-SM では [IP Address] および [Subnet Mask] を指定します）。 マルチコンテキスト モードでは、物理インターフェイスまたは論理インターフェイスを 1 つのコンテキストに割り当てると、そのコンテキスト内のインターフェイスがデフォルトでは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シャットダウンされます。
Management Only	このインターフェイスをデバイス管理用に予約します。このデバイスの管理用トラフィックだけが受け入れられます。他のインターフェイスおよびデバイスのパススルー トラフィックは拒否されます。 プライマリまたはセカンダリの ISP インターフェイスは管理専用に設定できません。 管理専用 EtherChannel インターフェイスの定義には、特定のメンバ インターフェイスの制限があります。詳細については、EtherChannel の設定（13 ページ）を参照してください。 （注） これは、トランスペアレントモードのデバイスでは使用できません。インターフェイスが [管理専用（Management Only）] として割り当てられている場合、[ルートマップ（Route Map）] をそのインターフェイスに割り当てることはできません。つまり、インターフェイスには [管理専用（Management Only）] または [ルートマップ（Route Map）] のいずれかのみ割り当てることができます。

要素	説明
インターフェイス	

要素	説明
	ASA 5505 では、[Hardware Port] は [Hardware Ports] パネルで指定します（ASA 5505 でのハードウェア ポートの設定 （99 ページ）を参照）。また、このオプションは、Catalyst 6500 サービス モジュール（ASA-SM と FWSM）設定の一部ではありません。 物理インターフェイスの場合、ネットワークタイプ、スロット、およびポート番号を含む物理ポート ID を type[slot/]port の形式で入力して、インターフェイスに割り当てる固有のハードウェアポートを指定します。これは、サブインターフェイスをインターフェイスに関連付ける名前でもあります。 物理インターフェイスのネットワーク タイプには、Ethernet または GigabitEthernet のいずれかを指定できます。ASA 5580 の場合は、TenGigabitEthernet も使用できます。このフィールドでは自動パターンマッチングが行われます。たとえば、e という文字を最初に入力すると、「Ethernet」がこのフィールドに挿入されます。同様に、g という文字を入力すると、「GigabitEthernet」が挿入されます。したがって、有効な値は次のとおりです。 • Ethernet0 ～ Ethernetn • GigabitEthernet0 ～ GigabitEthernetn • GigabitEthernets /n • TenGigabitEthernets/n（ASA 5580 のみ） s はスロット番号、n はポート番号を表し、スロットまたはデバイスのネットワークポートの最大数が上限です。 ASA 5500 シリーズ アプライアンスの場合は、タイプとスロット/ポートのペアを入力します（gigabitethernet0/1 など）。シャーシに組み込まれているポートはスロット 0 に割り当てられ、4-Port Gigabit Ethernet Security Services Module（4 GE SSM; 4 ポート ギガビット イーサネット セキュリティ サービス モジュール）のポートはスロット 1 に割り当てられます。スロットとポートのペアを入力すると、[Media Type] オプションがイネーブルになります。 ASA 5500 シリーズ アプライアンスには、**管理**インターフェイスタイプも含まれています。管理インターフェイスは、デバイス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、必要な場合には、この物理インターフェイスを通過トラフィックに使用できます（[Management Only] オプションは選択しないでください）。そのため、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使用できる 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も使用できます。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 コンテキストにおける管理を提供することもできます。

要素	説明
	サブインターフェイスを定義する場合は、定義済みのポートのリストから簡単に目的のハードウェア ポートを選択できます（VLAN ID も指定する必要があります）。目的のインターフェイス ID が表示されない場合は、インターフェイスが定義済みで、イネーブルにされていることを確認してください。
名前	このインターフェイスに最大 48 文字の ID を指定します。名前には、インターフェイスの用途に関係する覚えやすい名前を付けます。ただし、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用に予約しているインターフェイスに名前を付けないでください。これには、フェールオーバー用に使用する EtherChannel およびそのメンバ インターフェイスも含まれます。また、冗長インターフェイス ペアのメンバとして使用するインターフェイスに名前を付けないでください。 セキュリティ アプライアンスのインターフェイス命名ルールに従って、いくつかの名前が特定のインターフェイス用に予約されています。そのため、これらの予約名を使用すると、次のように、デフォルトの予約済みセキュリティ レベルが適用されます。 • [Inside]：内部ネットワークに接続します。最もセキュアなインターフェイスにする必要があります。 • [DMZ]：中間インターフェイスに接続された「緩衝地帯」。DMZ は境界ネットワークとも呼ばれます。DMZ インターフェイスに任意の名前を付けることができます。一般的に、DMZ インターフェイスには、インターフェイスタイプを識別するために「DMZ」というプレフィックスを付けます。 • [Outside]：外部ネットワークまたはインターネットに接続します。セキュア度の最も低いインターフェイスにする必要があります。 同様に、一般的にサブインターフェイス名には、一意の ID に加えて、関連付けられているインターフェイスも示されます。たとえば、DMZoobmgmt で、DMZ インターフェイスに接続されているアウトオブバンド管理ネットワークを示すことができます。 （注） この場合でも、**インターフェイスをフェールオーバー用または冗長インターフェイスのメンバーとして使用する場合は、そのインターフェイスの名前を付けないでください**。詳細については、冗長インターフェイスの設定 （11 ページ）を参照してください。

要素	説明
セキュリティ レベル（Security Level）	インターフェイスのセキュリティ レベルを指定します。0（最もセキュア度の低い）～ 100（最もセキュア度の高い）の値を入力します。セキュリティ アプライアンスにより、トラフィックは、内部ネットワークから外部ネットワーク（セキュリティ レベルがより低い）まで自由に通過できます。他の多くのセキュリティ機能が、2 つのインターフェイスの相対的なセキュリティ レベルによる影響を受けます。 • 外部インターフェイスは、常に 0 です。 • 内部インターフェイスは、常に 100 です。 • DMZ インターフェイスの値の範囲は 1 ～ 99 です。
メディア タイプ（Media Type）	[Interface] が [Type] で選択されているタイプである場合に、[Hardware Port] フィールドにハードウェア ポート ID とスロット番号またはポート番号を入力すると、これらのオプションがイネーブルになります（これらのオプションはASAのスロットまたはポートのインターフェイスにのみ適用されます）。 ASA 5505 を除くすべての 5500 シリーズのアプライアンスでは、シャーシに組み込まれているポートはスロット 0 に割り当てられ、4GE SSM のポートはスロット 1 に割り当てられます。デフォルトでは、ASA で使用されるコネクタはすべて RJ-45 コネクタです。ただし、4GE SSM のポートには、ファイバ SFP コネクタを含めることができます。これらのファイバベースの接続のインターフェイス設定の一環として、[Media Type] の設定をデフォルト（RJ45）からファイバコネクタ設定（SFP）に変更する必要があります。 ファイバベースのインターフェイスではデュプレックス設定はサポートされず、また固定速度もありません。そのため、[Duplex] オプションはディセーブルになり、[Speed] オプションは [auto] および [nonegotiate] のみを選択できます。 このスロット 1 インターフェイスで使用するコネクタ タイプを選択します。 • [RJ45]：ポートは RJ-45（銅線）コネクタを使用します。 • [SFP]：ポートはファイバ SFP コネクタを使用します。10 ギガビット イーサネット カードの場合に必要です。

要素	説明
VLAN ID（Admin. VLAN ID）	インターフェイスの [タイプ（Type）] として [サブインターフェイス（Subinterface）] を選択した場合や、トランスペアレントモードで動作しているデバイス、ASA 5505、または Catalyst 6500 サービスモジュール上で論理インターフェイスを定義している場合は、このインターフェイスの VLAN ID を指定します。 7.2(2)18 以前のオペレーティング システムを PIX/ASA デバイスで実行している場合、有効な VLAN ID は 1 ～ 1001 です。バージョン 7.2(2)19 以降での有効な ID は 1 ～ 4090 です。Catalyst 6500 サービス モジュールでは、有効な ID は 1 ～ 4096 です。指定した VLAN ID は、どの接続デバイスでも使用されていない必要があります。 一部の VLAN ID は接続されているスイッチで予約されている場合があります。詳細については、スイッチのマニュアルを確認してください。マルチコンテキストモードでは、VLAN ID はシステム設定でのみ設定できます。 詳細については、サブインターフェイスの設定（PIX/ASA） （9 ページ）を参照してください。
Subinterface ID	インターフェイスの [Type] として [Subinterface] を選択した場合や、トランスペアレント モードで動作しているデバイス上でインターフェイスを定義している場合、サブインターフェイス ID として 1 ～ 4294967293 の整数を指定します。 サブインターフェイスのポート ID の場合、この ID は選択したハードウェア ポートに付加されます。たとえば、*GigabitEthernet0.4* は、GigabitEthernet0 ポートで動作する、4 の ID を割り当てられたサブインターフェイスを示します。 （注） 設定後は ID を変更できません。
ルート マップ	[ルートマップオブジェクトセレクタ（Route Map Object Selector）] ダイアログボックスから [ルートマップ（Route Map）] を選択します。 （注） VNI インターフェイスを除き、他のすべてのインターフェイスタイプでは、ソフトウェアバージョン 9.4(1) 以降を実行している ASA デバイスのポリシーベースルーティングがサポートされています。VNI インターフェイスでは、ソフトウェアバージョン 9.5(1) 以降を実行している ASA デバイスのポリシーベースルーティングがサポートされています。

要素	説明
IP タイプ（IP Type）	**PIX 7.0 以降と ASA（トランスペアレント モードの 5505 を除く）のみ。** [IPタイプ（IP Type）] では、インターフェイスに使用する IP アドレス指定のタイプを定義します。[スタティックiP（Static IP）]、[DHCPの使用（Use DHCP）]、または [PPPoE] を選択します（デバイス インターフェイス：IP タイプ（PIX/ASA 7.0 以降） （94 ページ）を参照）。 （注） DHCP および PPPoE は、セキュリティ アプライアンスの外部インターフェイスにかぎり設定できます。

要素	説明
IPアドレス サブネットマスク	**ルーテッドモードの Catalyst 6500 サービスモジュール（ASA-SM および FWSM）のみ。** これらの 2 つのフィールドを使用して、IP アドレスとサブネット マスクを VLAN インターフェイスに割り当てます。IP アドレスは、インターフェイスごとに一意でなければなりません。 サブネット マスクは、ドット区切り 10 進表記（255.255.255.0 など）で表すか、またはネットワーク マスクのビット数（24 など）を入力して表すことができます。 バージョン 4.12、255.255.255.254 および 255.255.255.255 までは、ネットワークに接続するインターフェイスに使用しないでください。使用すると、トラフィックがインターフェイス上で停止します。 バージョン 4.13 以降、/31 サブネットマスク（または 2555.2555.255.254）は、ネットワークに接続されたポイントツーポイント インターフェイスでサポートされています。Cisco Security Manager では、インターフェイス レコードの保存時に警告メッセージが表示されます。 サブネット マスク値を指定しない場合は、次に示すように「クラスフル」ネットワークが使用されます。 • IP アドレスの最初のオクテットが 1 ～ 126 の場合（つまり、アドレスが 1.0.0.0 ～ 126.255.255.255 の場合）、クラス A ネットマスク（255.0.0.0）が使用されます。 • サブネットマスク IP アドレスの最初のオクテットが 128 ～ 191 の場合（つまり、アドレスが 128.0.0.0 ～ 191.255.255.255 の場合）、クラス B ネットマスク（255.255.0.0）が使用されます。 • IP アドレスの最初のオクテットが 192 ～ 223 の場合（つまり、アドレスが 192.0.0.0 ～ 223.255.255.255 の場合）、クラス C ネットマスク（255.255.255.0）が使用されます。 （注） グローバル プールやスタティック NAT エントリの IP アドレスなど、以前にルータ、ホスト、または他のファイアウォール デバイス コマンドに使用したアドレスは使用しないでください。

要素	説明
説明	復帰を使用しないで 1 行に最大 240 文字の任意の説明を入力できます。マルチコンテキスト モードでは、システムの説明とコンテキストの説明に関係はありません。 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」、または「LAN/STATE Failover Interface」などに固定されます。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。
冗長インターフェイス。以下のオプションは、ASA 5505 デバイス上または Catalyst 6500 サービス モジュール（ASA-SM と FWSM）上では使用できません。	
Redundant ID	インターフェイスの [Type] に [Redundant Interface] が選択されている場合、この冗長インターフェイスの ID を指定します。有効な ID は 1 ～ 8 の整数です。 詳細については、冗長インターフェイスの設定 （11 ページ）を参照してください。
プライマリ インターフェイス（Primary Interface） Secondary Interface	インターフェイスの [Type] に [Redundant Interface] が選択されている場合、使用可能なインターフェイスの [Primary Interface] リストから、冗長インターフェイス ペアのプライマリ メンバを選択します。名前付きインターフェイスは冗長インターフェイス ペアでは指定できないため、使用可能なインターフェイスが [Hardware Port ID] に表示されます。 同様に、使用可能なインターフェイスの [Secondary Interface] リストから、冗長インターフェイス ペアのセカンダリ メンバを選択します。 （注） メンバインターフェイスはイネーブルである必要があります。また、メンバ インターフェイスは同じタイプ（GigabitEthernet など）である必要があります。[Name]、[IP Address]、または [Security Level] を割り当てることはできません。実際には、メンバーインターフェイスに対して [Duplex] および [Speed] 以外のオプションを設定しないでください。
これらのオプションは ASA 5505 デバイスでのみ使用できます。	
Block Traffic To	この VLAN インターフェイスが、ここで選択された VLAN との接続を開始するのを制限します。

要素	説明
バックアップ インターフェイス	たとえば、ISP へのバックアップ インターフェイスとして VLAN インターフェイスを選択します。プライマリ インターフェイスによるデフォルト ルートに障害が発生しないかぎり、バックアップ インターフェイスはトラフィックを通過させません。トラフィックがバックアップ インターフェイスを必ず通過できるようにするには、プライマリ インターフェイスに障害が発生したときにバックアップ インターフェイスを使用できるように、プライマリ インターフェイスとバックアップ インターフェイスの両方でデフォルト ルートを設定します。
Active MAC Address Standby MAC Address	プライベート MAC アドレスを手動でインターフェイスに割り当てるには、[Active MAC Address] フィールドを使用します。[Standby MAC Address] フィールドを使用すると、デバイス レベルのフェールオーバーで使用するスタンバイ MAC アドレスを設定できます。 これらのフィールドの詳細については、デバイス インターフェイス：MAC アドレス （97 ページ）を参照してください。
[EtherChannel Interface] オプションは、ASA 8.4.1 以降のデバイスでのみ使用できます。	
EtherChannel:ID	インターフェイスの [Type（タイプ）] に EtherChannel が選択されている場合、その EtherChannel（別名「ポートチャネル」）の ID を入力します。有効な値は 1 ～ 48 です。最大 48 個のポートチャネル グループを定義できます。詳細については、EtherChannel の設定 （13 ページ）を参照してください。

要素	説明
Available Interfaces/Members in Group	インターフェイスの [Type] に EtherChannel が選択されている場合、[Available Interfaces] リストからインターフェイスを選択して、[>>] ボタンをクリックして右のメンバ リストに追加すると、この EtherChannel グループにインターフェイスを割り当てることができます。 最大 16 個のインターフェイスをチャネル グループに割り当てられます。ASA 9.2(1) 以降の場合、各チャネルグループに、最大 16 個のアクティブインターフェイスを設定できます。8 個のアクティブインターフェイスのみサポートするスイッチを使用していて、ASA のバージョンが 9.2(1) より前の場合、8 個のインターフェイスのみアクティブにできるため、残りのインターフェイスは、インターフェイス障害発生時のスタンバイリンクとして動作できます。または、[LACPモード（LACP Mode）] を [オン（On）] に設定すると、スタティック EtherChannel を作成できます（[詳細設定（Advanced）] タブで設定、 [Add Interface]/[Edit Interface] ダイアログボックス - [Advanced] タブ（ASA/PIX 7.0 以降） （66 ページ）を参照）。作成すると、グループ内のすべてのインターフェイスでトラフィックを通過させることができます。 （注） チャネル グループのすべてのインターフェイスは、同じタイプと速度である必要があります。チャネル グループに追加された最初のインターフェイスによって、グループのタイプと速度が決まります。 詳細については、EtherChannel の設定 （13 ページ）を参照してください。

[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス：Cisco Firepower 9000（[全般（General）] タブと [詳細（Advanced）] タブ）

Cisco Firepower 9000 デバイスの [全般（General）] タブと [詳細（Advanced）] タブでサポートされる要素については、[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM） （50 ページ）を参照してください。さらに、次の変更は Cisco Firepower 9000 デバイスにのみ適用されます。

表 *11 : [インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス：Cisco Firepower 9000*

要素	説明
タイプ	インターフェイスのタイプを選択します。冗長インターフェイスは、Cisco Firepower 9000 デバイスではサポートされていません。

要素	説明
[管理専用個別（Management Only Individual）]	Cisco Firepower 9000 デバイスでのみ、デバイスがクラスタモードの場合にのみ適用されます。 （注） [管理専用（Management Only）] チェックボックスと [管理専用個別（Management Only Individual）] チェックボックスの両方を同時に有効にすることはできません。[管理専用個別（Management Only Individual）] チェックボックスがオンになっている場合にのみ、クラスタプールを設定できます。
名前	最大48文字のインターフェイス名を指定します。[Name] には、インターフェイスの用途に関係する覚えやすい名前を付けます。 インターフェイス名は「Ethernet」で始めて、次の形式にする必要があります。 Ethernet[スロット]/[ポート]/サブポート。ここで、 • スロットは 1 ～ 3 で指定します。 • ポートは 1 ～ 8 で指定します。 • サブポートは 1 ～ 4 で指定します。 • サブポートはスロット 1 には適用されません。
次の要素は、Cisco Firepower 9000 デバイスではサポートされていません。	
[メディアタイプ（Media Type）]（[全般（General）] タブ）	
[デュプレックス（Duplex）]（[詳細（Advanced）] タブ）	
[速度（Speed）]（[詳細（Advanced）] タブ）	
[使用可能なインターフェイス（Available Interfaces）]/[グループ内のメンバー（Members In Group）]（[全般（General）] タブ）	
[ロードバランシング（Load Balancing）]（[詳細（Advanced）] タブ）	
[LACPモード（LACP Mode）]（[詳細（Advanced）] タブ）	
[VSSスイッチID（VSS Switch ID）]/[vPCスイッチID（vPC Switch ID）]（[詳細（Advanced）] タブ）	
[アクティブな物理インターフェイス（Active Physical Interfaces）]（[詳細（Advanced）] タブ）	
[ASAクラスタでのEtherChannelのスパン（Span EtherChannel across the ASA Cluster）]（[詳細（Advanced）] タブ）	

要素	説明
[VSSまたはvPCモードでスイッチペア間のロードバランシングを有効にする（Enable load balancing between switch pairs in VSS or vPC mode）]（[詳細（Advanced）] タブ）	
[メンバーインターフェイスの設定（Member Interface Configuration）]（[詳細（Advanced）] タブ）	

[Add Interface]/[Edit Interface] ダイアログボックス - [Advanced] タブ（ASA/PIX 7.0 以降）

[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM） （50 ページ）は、ASA および PIX 7.0 以降のデバイスでインターフェイス、サブインターフェイス、冗長インターフェイスおよびEtherChannel インターフェイスを定義および設定するために使用します。[Add Interface] と [Edit Interface] ダイアログボックスには、[Interfaces] ページからアクセスできます。詳細については、デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （43 ページ）を参照してください。

このダイアログボックスの [Advanced] パネルは、[Duplex]、[Speed]、最大伝送単位（MTU）パラメータなど、基本のインターフェイス設定を設定するために使用します。次の表ではこれらの設定の詳細を説明します。

関連項目

- [Add Interface]/[Edit Interface] ダイアログボックス - [General] タブ（PIX 7.0 以降/ASA/FWSM）（52 ページ）
- IPv6 インターフェイスの設定（ASA/FWSM） （79 ページ）

表 *12 : [Advanced]* タブ：*[Add Interface]/[Edit Interface]* ダイアログボックス（*ASA/PIX 7.0* 以降）

要素	説明
デュプレックス	インターフェイスのデュプレックス オプションが一覧表示されます。インターフェイス タイプに応じて、[Full]、[Half]、または [N/A] があります。 [TenGigabitEthernet (ASA 5580 only)] の場合、[Duplex] は自動的に [Full] に設定されます。 （注） [Interface] のタイプとして [Subinterface] または [Redundant] が選択されている場合、このオプションは使用できません。

要素	説明
速度	

要素	説明
	物理インターフェイスの速度オプションがビット/秒で表示されます。論理インターフェイスには適用されません。使用できる速度は、インターフェイス タイプによって異なります。 • auto • 10 • 100 • 1000 • 10000（TenGigabitEthernet インターフェイスに自動的に設定されます。ASA 5580 でのみ使用できます） • nonegotiate （注） [Interface] のタイプとして [Subinterface] または [Redundant] が選択されている場合、このオプションは使用できません。 管理インターフェイスのポート PID は、パス C:\Program Files (x86)\CSCOpx\MDC\athena\config\csm.properties で指定する必要があります。管理対象インターフェイスでサポートされる速度オプションは次のとおりです。 • 1000 • 10000 • Detect SFP FPR-3100 デバイスの Ethernet1/1 から Ethernet1/8 までででサポートされる RJ 45 インターフェイスの設定可能な速度オプションは次のとおりです。 • 10 • 100 • 1000 RJ45 インターフェイスでは、次の速度オプションの組み合わせはサポートされていません。 • 1000 およびデュプレックスハーフ • 自動およびデュプレックスハーフ SFP ポート（Ethernet1/9 から Ethernet1/16）で設定可能な速度オプションは、CSM.properties で設定できる SFP ポート PID に基づいて識別されます。SFP ポートのポート PID は、パス C:\Program Files (x86)\CSCOpx\MDC\athena\config\csm.properties

要素	説明
	で指定する必要があります。 （注） SFP ポートに半二重の値を設定することはできません。全二重のみが許可されます。 • FPR-3110 および FPR-3120 でサポートされる速度オプションは次のとおりです。 • 1000 • 10000 • no-negotiate • sfp-detect • FPR-3130 および FPR-3140 でサポートされる速度オプションは次のとおりです。 • 1000 • 10000 • 25000 • no-negotiate • sfp-detect EPM ポート（Ethernet2/1 から Ethernet2/8）の FPR-3100 シリーズ デバイスで設定可能な速度オプションは、デバイスショーインベントリからのモジュールタイプに基づいて識別されます。EPM ポートは、パス C:\Program Files (x86)\CSCOpx\MDC\athena\config\csm.properties で指定する必要があります。サポートされている速度オプションは次のとおりです。

要素	説明
	• FPR-X-NM-8X10G モジュール： • 1000 • 10000 • no-negotiate • sfp-detect • FPR-X-NM-8X25G モジュール： • 1000 • 10000 • 25000 • no-negotiate • sfp-detect • FPR-X-NM-4X40G モジュール： • 40000 • sfp-detect • no-negotiate

要素	説明
FEC モード（FEC Mode）	**物理インターフェイス**を選択した場合、ノイズの多いチャネルを介したデータ送信のエラーを減らすように **FEC モード**を設定できます。 **FEC モード**は、Ethernet1/9 から Ethernet1/16 までの**物理インターフェイス** ハードウェア ポートをサポートします。デフォルト値は auto です。**FEC モード**設定は、次の Firepower デバイスでサポートされています。 • FPR-3130 • FPR-3140 使用可能な FEC モードの値は次のとおりです。 • auto • cl108-rs • cl74-fc • disable （注） FEC モードの設定は、ASA 9.17(1) 以降のデバイスにのみ適用されます。FECモードは管理インターフェイスには適用されません。
Negotiate-Auto	**物理インターフェイス**を選択した場合、ピアとの相互運用性の問題がある場合はいつでも **Negotiate-Auto** を設定できます。 **Negotiate-Auto** 設定は、次の Firepowerデバイスでサポートされています。 • FPR-3110 • FPR-3120 • FPR-3130 • FPR-3140 （注） **Negotiate-Auto** 設定は、ASA 9.17(1) 以降のデバイスにのみ適用されます。Negotiate-Auto（AP-port）は管理インターフェイスには適用されず、インターフェイスがポート チャネル インターフェイスのメンバーである場合はサポートされません。

要素	説明
MTU	最大パケット サイズ、つまり最大伝送単位（MTU）をバイト数で指定します。この値は、インターフェイスに接続されているネットワークのタイプによって異なります。有効な値は 300 ～ 65535 バイトです。PPPoE を除くすべてのタイプのデフォルトは 1500 で、PPPoE のデフォルトは 1492 です。マルチコンテキスト モードでは、コンテキスト設定で MTU を設定します。
Active MAC Address Standby MAC Address	**PIX 7.2 以降および ASA 7.2 以降のデバイスでのみ使用できます。** プライベート MAC アドレスを手動でインターフェイスに割り当てるには、[Active MAC Address] フィールドを使用します。[Standby MAC Address] フィールドを使用すると、デバイス レベルのフェールオーバーで使用するスタンバイ MAC アドレスを設定できます。 これらのフィールドの詳細については、デバイス インターフェイス：MAC アドレス （97 ページ）を参照してください。
ロール（Roles）	このインターフェイスに割り当てられているすべてのインターフェイス ロールが、このフィールドに一覧表示されます。ロールの割り当ては、このインターフェイスに指定されている名前と、Cisco Security Manager に現在定義されているインターフェイス ロール オブジェクト間のパターン マッチングに基づきます。 インターフェイス ロール オブジェクトは、各デバイスの設定が生成されるときに、実際のインターフェイスの IP アドレスで置き換えられます。インターフェイス ロールを使用すると、複数のインターフェイスに適用可能な汎用ルールを定義できます。 ロールの詳細とその定義方法および使用方法については、インターフェイス ロール オブジェクトについてを参照してください。
MAC アドレス	サイト固有の MAC アドレス。
サイト ID（Site ID）	現在のユニットが属するサイトを指定するサイト ID。
ソフトウェアバージョン 9.5(1) 以降を実行している ASA デバイスの Security Manager バージョン 4.9 以降、ルーテッドモードのスパンド EtherChannel にサイト間クラスタリングを使用できます。MAC アドレスのフラッピングを防ぐには、各インターフェイスのサイト別の MAC アドレスがサイトのユニット上で共有できるように、各クラスタ メンバーのサイト ID を設定します。	
[EtherChannel Interface] オプションは、ASA 8.4.1 以降のデバイスでのみ使用できます。	
ロード バランシング	（[General] パネルで）インターフェイスの [Type] に EtherChannel が選択されている場合、チャネル リンクのロード バランシング方式を設定します。このオプションの詳細については、EtherChannel のロード バランシングについて （18 ページ）を参照してください。

要素	説明
LACP Mode	目的の [LACP モード（LACP Mode）] を選択します。デフォルトの [アクティブ（Active）] を選択すると、[アクティブ物理インターフェイス（Active Physical Interfaces）] の [最小（Minimum）] 値と [最大（Maximum）] 値で指定されているとおり、最大 8 個のインターフェイスをアクティブにして、最大 8 個のインターフェイスをスタンバイモードにできます。 [オン（On）] を選択すると、すべてのメンバーインターフェイスが「オン」になっているスタティックポートチャネルが作成されます。つまり、スタンバイポートなしで、最大 16 個のポートにトラフィックを通過させることができます。このオプションを選択すると、この EtherChannel グループに割り当てられているすべてのインターフェイスの [Mode] は [On] に切り替わります（それぞれの [Mode] が [On] ではない場合）。このモードの詳細については、EtherChannel に割り当てられているインターフェイスの LACP パラメータの編集 （16 ページ）を参照してください。

要素	説明
Active Physical Interfaces	（[General] パネルで）インターフェイスの [Type] に EtherChannel が選択されている場合、この EtherChannel グループでアクティブにできるインターフェイスの最小数と最大数を [Minimum] と [Maximum] に指定します。 • [最少（Minimum）]：このグループでアクティブなインターフェイスの最小数を指定します。ASA 9.2(1)+ の場合、1 ～ 16 の値を指定できます。これより以前のバージョンでは、1 ～ 8 の値を入力します。 チャネル グループ内のアクティブ インターフェイス数がこの値よりも小さい場合、ポートチャネル インターフェイスがダウンし、デバイスレベル フェールオーバーが開始されます。 • [最大（Maximum）]：アクティブにできるインターフェイスの最大数を指定します。ASA 9.2(1)+ の場合、1 ～ 16 の値を指定できます。これより以前のバージョンでは、1 ～ 8 の値を入力します。 16 個のアクティブ インターフェイスの場合、スイッチがこの機能をサポートしている必要があります（たとえば、Cisco Nexus 7000 と F2 シリーズ 10 ギガビット イーサネット モジュール）。スイッチが 16 個のアクティブ インターフェイスをサポートしていない場合、このコマンドは必ず 8 以下に設定する必要があります。 チャネルに使用できるインターフェイスは、このダイアログボックスの [General] タブで選択されます（[Add Interface]/[Edit Interface] ダイアログボックス - [General] タブ（PIX 7.0 以降/ASA/FWSM）（52 ページ））。 EtherChannel バンドルに 3、5、6、7 個のアクティブ ポートを指定すると、一部のポートが他の最大 2 倍の負荷を処理するため、ロード バランシングの効率が低下します。EtherChannel ごとに 2、4、8 個のアクティブ ポートを指定して、効率的なロードバランシングを実行することを推奨します（1 の値を指定すると、ロード バランシングはまったく実行されません）。
DHCP リレーオプション。 ASA-SM 9.1.2+ デバイスでのみ使用可能。	

要素	説明
DHCP リレーサーバー	IP アドレスを入力するか、またはこのインターフェイスの DHCP 要求をリレーする先のインターフェイス固有の DHCP サーバーを示すネットワーク/ホスト オブジェクトを選択します。複数の値はカンマで区切ります。最大4台のインターフェイス固有の DHCP リレーサーバーと、最大 10 台のグローバルおよびインターフェイス固有の DHCP リレーサーバーを設定できます。 （注） インターフェイス固有のサーバーでは、IPv6 はサポートされていません。 インターフェイスに DHCP 要求が届くと、ユーザーの設定に基づいて、ASA からその要求がリレーされる DHCP サーバーが決定されます。設定できるサーバのタイプは次のとおりです。 • インターフェイス固有の DHCP サーバー：特定のインターフェイスに DHCP 要求が届くと、ASA はその要求をインターフェイス固有のサーバーにだけリレーします。 • グローバル DHCP サーバー：インターフェイス固有のサーバーが設定されていないインターフェイスに DHCP 要求が届くと、ASA はその要求をすべてのグローバル サーバーにリレーします。インターフェイスにインターフェイス固有のサーバーが設定されている場合、グローバル サーバーは使用されません。詳細については、[DHCP Relay] ページを参照してください。
DHCP リレー信頼情報（オプション 82）	信頼するこの DHCP クライアント インターフェイスを指定します。DHCP Option 82 を維持するために、インターフェイスを信頼できるインターフェイスとして設定できます。 （注） すべての DHCP クライアント インターフェイスを信頼することもできます。詳細については、[DHCP Relay] ページを参照してください。 DHCP Option 82 は、DHCP スヌーピングおよび IP ソース ガードのために、ダウンストリームのスイッチおよびルータによって使用されます。通常、ASA DHCP リレーエージェントが Option 82 をすでに設定した DHCP パケットを受信しても、giaddr フィールド（サーバーにパケットを転送する前に、リレーエージェントによって設定された DHCP リレーエージェントアドレスを指定するフィールド）が 0 に設定されている場合は、ASA はそのパケットをデフォルトで削除します。インターフェイスを信頼できるインターフェイスとして指定することで、Option 82 を維持したままパケットを転送できます。

要素	説明
セキュアグループのタギングオプション。 ASA 9.3.1 以降のデバイスでのみ使用できます。 SGT とイーサネット タギング（レイヤ 2 SGT インポジションとも呼ばれる）を利用すると、ASA でシスコ独自のイーサネット フレーミング（EtherType 0x8909）を使用して、イーサネット インターフェイスでセキュリティ グループ タグを送受信できます。これにより、送信元のセキュリティ グループ タグをプレーンテキストのイーサネット フレームに挿入できます。ASA は、インターフェイスごとの手動設定に基づいて、発信パケットにセキュリティ グループ タグを挿入し、着信パケットのセキュリティ グループ タグを処理します。この機能を使用することで、ネットワーク デバイス間におけるエンドポイント ID の伝搬をインラインかつホップバイホップで実行できます。また、各ホップ間でシームレスなレイヤ 2 SGT インポジションを実現できます。 （注） 物理インターフェイス、VLAN インターフェイス、ポート チャネル インターフェイスおよび冗長インターフェイスでのみサポートされます。BVI、TVI、VNI などの論理インターフェイスや仮想インターフェイスではサポートされません。フェールオーバーリンクまたはクラスタ制御リンクはサポートしません。	
Cisco TrustSec のセキュアグループタギングの有効化	SGT とイーサネットタギングを有効にします（レイヤ 2 SGT インポジションとも呼ばれます）。
セキュアグループタグで出力パケットにタグ付け	インターフェイスでのセキュリティ グループ タグ（sgt と呼ばれる）の伝播をイネーブルにします。
すべての入力パケットにスタティック セキュア グループ タグを割り当て	ピアからの着信トラフィックにスタティック セキュリティ グループ タグを適用します。有効になっている場合、使用する SGT 番号を [セキュアグループタグ（Secure Group Tag）] フィールドで指定する必要があります。
セキュリティ グループ タグ（SGT）	ピアからの着信トラフィックに適用する SGT 番号を指定します。有効な値の範囲は 2 ～ 65519 です。
信頼できるインターフェイス	インターフェイス上の入力トラフィックにより、既存の SGT を、指定したスタティック SGT で上書きしてはならないことを示します。
ASA クラスタ（レイヤ 3）。クラスタモードの ASA 5580 および 5585 デバイスでのみ使用可能。 ASA クラスタがルータモードの場合はすべてのインターフェイスでサポートされ、ASA クラスタがトランスペアレントモードの場合は管理インターフェイスでサポートされます。	
IPv4 アドレスプール	使用するアドレスのプールを表す IPv4 プールオブジェクトを入力または選択します。
MAC アドレス プール	使用する MAC アドレスのプールを表す MAC プールオブジェクトを入力または選択します。

要素	説明
ASA クラスタ（レイヤ 2）。クラスタモードの ASA 5580 および 5585 デバイスでのみ使用可能。 ASA クラスタの EtherChannel インターフェイスでのみサポートされます。ASA クラスタがトランスペアレントモードの場合、管理インターフェイスではサポートされません。	
ASA クラスタに広がるスパン EtherChannel	選択して、クラスタ内のすべての ASA に広がる EtherChannel を設定し、EtherChannel の動作の一部としてロードバランシングを提供します。
VSS または vPC モードのスイッチペア間のロードバランシングを有効にする	（任意）仮想スイッチングシステム（VSS）または仮想ポートチャネル（vPC）の 2 台のスイッチに ASA を接続する場合は、[VSSまたはvPCモードのスイッチペア間のロードバランシングを有効にする（Enable load balancing between switch pairs in VSS or vPC mode）] チェックボックスをオンにして、ロードバランシングを有効にする必要があります。この機能を使用すると、ASA と VSS（または vPC）ペアとの間の物理リンク接続の負荷が確実に分散されます。
メンバー インターフェイスの設定	インターフェイスの LACP モード、および指定したインターフェイスが接続されている仮想スイッチングシステム（VSS）または仮想ポート チャネル（vPC）のスイッチ（1 または 2）を識別します。
ASA 5505 デバイス固有の [Advanced] タブ オプション（ルーテッド モードのみ）	
Block Traffic To	この VLAN インターフェイスが、ここで選択された VLAN との接続を開始するのを制限します。
バックアップ インターフェイス	たとえば、ISP へのバックアップ インターフェイスとして VLAN インターフェイスを選択します。プライマリ インターフェイスによるデフォルト ルートに障害が発生しないかぎり、バックアップ インターフェイスはトラフィックを通過させません。トラフィックがバックアップ インターフェイスを必ず通過できるようにするには、プライマリ インターフェイスに障害が発生したときにバックアップ インターフェイスを使用できるように、プライマリ インターフェイスとバックアップ インターフェイスの両方でデフォルト ルートを設定します。
FWSM 3.1 以降のデバイス固有の [Advanced] タブ オプション	
ブリッジ グループ	トランスペアレント モードで動作している FWSM 3.1 以降では、この読み取り専用フィールドで、このインターフェイスが割り当てられるブリッジ グループを指定します。詳細については、[Add Bridge Group]/[Edit Bridge Group] ダイアログボックス （102 ページ）を参照してください。

要素	説明
ASR Group	このインターフェイスを非対称ルーティング グループに追加するには、このフィールドにASR グループ番号を入力します。フェールオーバー設定の装置間で非対象ルーティング サポートを適切に機能させるためには、ステートフル フェールオーバーをイネーブルにする必要があります。ASR グループの有効な値の範囲は 1 ～ 32 です。詳細については、非対称ルーティング グループについて （7 ページ）を参照してください。
フロー制御のポーズフレームオプション ネットワーク インターフェイスが過負荷になると、フロー制御が、データを送信するデバイスに一次停止要求を送信することをネットワーク インターフェイスに許可し、過負荷状態を解消します。フロー制御が有効になっていないときに過負荷状態が発生すると、デバイスはパケットをドロップします。 インターフェイスの受信側が高ウォーターマークに達すると、インターフェイスの送信側はポーズフレームの生成を開始します。リモートデバイスは、ポーズフレームで指定された一次停止時間、パケットの送信を停止または削減することが期待されます。インターフェイスの受信側がそのキューをクリアできるか、一時停止時間内に低ウォーターマークに達した場合、インターフェイスの送信側は、一時停止時間を 0 とする特別なポーズフレームを送信します。これにより、リモートデバイスはパケットの送信を開始できます。インターフェイスの受信側がまだキューで動作している場合、一時停止時間が経過すると、インターフェイスの送信側は、新しい一時停止時間を持つ新しいポーズフレームを再度送信します。 （注） フロー制御のポーズフレームは、シングルコンテキストモードおよびマルチコンテキストモードの ASA 8.2 以降の物理インターフェイスでのみサポートされます。BVI、TVI、VNI などの論理インターフェイスや仮想インターフェイスではサポートされません。	
Enable Pause Frame	（任意）フロー制御用のポーズフレームの送信を有効にします。
デフォルト値を使用する	（任意）デバイスに基づいて、低ウォーターマーク、高ウォーターマーク、および一次停止時間のデフォルト値を使用します。 これがオンになっていない場合は、デバイス固有のポーズフレームのフロー制御値の参照表に従って値を指定します。
低ウォーターマーク（キロバイト）	低ウォーターマークの値を入力します。インターフェイスからポーズフレームが送信された後、バッファの使用率が低ウォーターマークを下回ると、インターフェイスから「送信オン」フレームが送信されます。リモートデバイスはデータの送信を再開できます。
高ウォーターマーク（キロバイト）	高ウォーターマークの値を入力します。バッファの使用率が高ウォーターマークを超えると、インターフェイスからポーズフレームが送信されます。

要素	説明
一時停止時間	一次停止のリフレッシュのしきい値を 0 ～ 65535 スロットの範囲で設定します。各スロットは 64 バイトを転送するために必要な時間なので、ユニットあたりの時間はリンク速度によって異なります。リモートデバイスは、ポーズフレーム内のタイマー値による制御に従い、送信オンフレームを受信した後、または送信オフフレームの期限が切れた後、トラフィックを再開できます。バッファの使用量が継続的に高基準値を超えている場合は、ポーズリフレッシュのしきい値に指定された間隔でポーズフレームが繰り返し送信されます。

表 *13 :* デバイス固有のポーズフレームフロー制御値

デバイスタイプ	低ウォーターマーク範囲（Kb）	デフォルト低ウォーターマーク範囲（Kb）	高ウォーターマーク範囲（Kb）	デフォルト高ウォーターマーク範囲（Kb）	一次停止時間の範囲	デフォルトの一時停止時間
ASA 5515	0 ～ 20	8	0 ～ 20	16	0 ～ 65535	26624
ASA 5525	0 ～ 20	8	0 ～ 20	16	0 ～ 65535	26624
ASA 5545	0 ～ 20	8	0 ～ 20	16	0 ～ 65535	26624
ASA 5510	0 ～ 48	16	0 ～ 48	24	0 ～ 65535	26624
ASA 5585	値はサポートされていません。「フロー制御送信オン」のみがサポートされています。					
ASA 5506	1 ～ 25	3	1 ～ 25	8	1 ～ 65535	18432
ISA-3000-2C2F	0-64	27	0-64	34	0 ～ 65535	26624
ISA-3000-4C	0-64	27	0-64	34	0 ～ 65535	26624
1783-SAD4T0S	0-64	27	0-64	34	0 ～ 65535	26624

IPv6 インターフェイスの設定（ASA/FWSM）

[Add Interface] または [Edit Interface] ダイアログボックスの [Type] で [Interface]、[Subinterface]、[Redundant]、[EtherChannel] を選択した場合、このダイアログボックスには、[General]、[Advanced]、[IPv6] の 3 つオプションのタブ付きパネルが表示されます。ここでは、[IPv6] パネルに表示されるこれらのオプションについて説明します。

（注） これらのオプションは、ルーテッドモードの ASA 7.0 以降のデバイス、トランスペアレントモードの ASA 8.2 以降のデバイス、ルーテッドモードの FWSM 3.1 以降のデバイスでのみ使用できます。

ナビゲーション パス

IPv6 パネルには [Add Interface] と [Edit Interface] のダイアログボックスでアクセスできます。これらのダイアログボックスには、デバイスインターフェイス、ハードウェア ポート、ブリッジ グループの管理 （43 ページ）の説明に従って、ASA または FWSM の [Interfaces] ページからアクセスできます。

関連項目

- Security Manager での IPv6 サポート
- [Add Interface]/[Edit Interface] ダイアログボックス - [General] タブ（PIX 7.0 以降/ASA/FWSM）（52 ページ）
- [Add Interface]/[Edit Interface] ダイアログボックス - [Advanced] タブ（ASA/PIX 7.0 以降）（66 ページ）

フィールド リファレンス

表 *14 : IPv6* タブ：*[Add Interface]/[Edit Interface]* ダイアログボックス（*ASA/FWSM*）

要素	説明
IPv6を有効化（Enable IPv6）	IPv6 をイネーブルにして、このインターフェイスで IPv6 アドレスを設定するには、このチェックボックスをオンにします。このオプションをオフにすると、このインターフェイスで IPv6 をディセーブルにできますが、設定情報は保持されます。

要素	説明
Enforce EUI-64	オンにすると、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 ID の使用を適用します。 このオプションがインターフェイスでイネーブルにされると、その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 アドレスに対して検証され、インターフェイス ID が Modified EUI-64 形式を使用していることが確認されます。IPv6 パケットのインターフェイス ID が Modified EUI-64 形式でない場合、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。 「%PIX|ASA-3-325003: EUI-64 source address check failed.」 アドレス形式の検証は、フローが作成された場合にのみ行われます。既存のフローからのパケットは確認されません。さらに、アドレス検証はローカル 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。 Modified EUI-64 形式のインターフェイス ID は、リンク層アドレスの上位 3 バイト（OUI フィールド）と下位 3 バイト（シリアル番号）の間に 16 進数の FFFE を挿入することで、48 ビット リンク層（MAC）アドレスから導出されます。選択されたアドレスが一意のイーサネット MAC アドレスから生成されることを保証するため、上位バイトの下位から 2 番めのビット（ユニバーサル/ローカル ビット）が反転され、48 ビット アドレスの一意性が示されます。たとえば、MAC アドレス 00E0.B601.3B7A のインターフェイスには、02E0:B6FF:FE01:3B7A の 64 ビット インターフェイス ID が指定されます。

要素	説明
DAD Attempts	Duplicate Address Detection（DAD; 重複アドレス検出）の実行中にインターフェイスで送信される連続ネイバー送信要求メッセージの数を指定するには、このフィールドに 0 ～ 600 の数を入力します。0 を入力すると、インターフェイス上で重複アドレス検出がディセーブルになります。1 を入力すると、フォローアップ送信のない一度の送信を設定します。これはデフォルトです。 アドレスがインターフェイスに割り当てられる前に、重複アドレス検出によって、新しいユニキャスト IPv6 アドレスの一意性が確認されます（重複アドレス検出の実行中、新しいアドレスは一時的な状態になります）。重複アドレス検出では、ネイバー送信要求メッセージを使用して、ユニキャスト IPv6 アドレスの一意性を確認します。 重複アドレス検出によって重複アドレスが特定された場合、そのアドレスの状態は DUPLICATE に設定され、アドレスは使用されなくなります。重複アドレスがインターフェイスのリンクローカル アドレスの場合は、そのインターフェイス上で IPv6 パケットの処理がディセーブルになり、次のようなエラー メッセージが発行されます。 %PIX-4-DUPLICATE: Duplicate address FE80::1 on outside 重複アドレスがインターフェイスのグローバル アドレスの場合は、そのアドレスは使用されず、前述のリンクローカル アドレスと同様のエラー メッセージが発行されます。 重複アドレスに関連付けられているコンフィギュレーション コマンドはすべて設定済みのままになりますが、アドレスの状態は DUPLICATE に設定されます。インターフェイスのリンクローカル アドレスに変更があると、新しいリンクローカル アドレスに対して重複アドレス検出が行われ、そのインターフェイスに関連付けられている他のすべての IPv6 アドレスが再生成されます（つまり、重複アドレス検出は、新しいリンクローカル アドレスでのみ行われます）。
NS Interval	IPv6 ネイバー送信要求メッセージの再送信間隔（ミリ秒単位）。有効な値の範囲は 1000 ～ 3600000 ミリ秒で、デフォルト値は 1000 ミリ秒です。 （注） この値は、このインターフェイスで送信されるすべての IPv6 ルータ アドバタイズメントに含まれます。
Reachable Time	リモート IPv6 ノードが到達可能であることが最初に確認されてから、このノードが到達可能であると見なされ続ける時間（ミリ秒単位）。有効な値の範囲は 0 ～ 3600000 ミリ秒で、デフォルト値は 0 です。この値に 0 を使用する場合、到達可能時間は未定に設定されます。つまり、到達可能時間の設定および追跡は受信デバイス次第です。 設定時間によって、使用不可のネイバーを検知できます。時間を短く設定すると、使用できないネイバーをより早く検出できます。ただし、時間を短くするほど、IPv6 ネットワーク帯域幅とすべての IPv6 ネットワーク デバイスの処理リソースの消費量が増えます。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。

要素	説明
管理対象設定フラグ	IPv6 ルータ アドバタイズメント パケットの「managed-config-flag」フラグを設定するかどうか。
その他の設定フラグ	IPv6 ルータ アドバタイズメント パケットの「other-config-flag」フラグを設定するかどうか。
Enable RA	オンにすると、インターフェイスで IPv6 ルータ アドバタイズメントの送信がイネーブルになります。次のオプションを使用できます。 • [RA Lifetime]：「ルータライフタイム」値は、ローカルリンク上のノードがセキュリティアプライアンスをリンク上のデフォルトルータと見なし続ける期間を指定します。有効な値の範囲は 0 ～ 9000 秒で、デフォルトは 1800 秒です。0 を入力すると、セキュリティ アプライアンスは選択したインターフェイスのデフォルト ルータとは見なされません。 0 以外の任意の値は、次の [RA Interval] 値より小さい値にはできません。 （注） この値は、このインターフェイスで送信されるすべての IPv6 ルータ アドバタイズメントに含まれます。 • [RA Interval]：このインターフェイスでの IPv6 ルータアドバタイズメントの送信間隔。有効な値の範囲は 3 ～ 1800 秒です（次の [RA Interval in Milliseconds] オプションがオンの場合は 500 ～ 1800000 ミリ秒）。デフォルトは 200 秒です。 [RA Lifetime] が 0 以外の場合、送信の間隔は [RA Lifetime] の値以下にする必要があります。他の IPv6 ノードと同期しないようにするには、使用する実際値を必要値の 20 % 以内にランダムに調整します。 • [RA Interval in Milliseconds]：このオプションをオンにすると、指定した [RA Interval] の値が秒ではなくミリ秒になります。

要素	説明
Interface IPv6 Addresses	ダイアログボックスのこのセクションで、インターフェイスに割り当てられている IPv6 アドレスを指定します。 • [Link-Local Address]：インターフェイスに自動的に生成されたリンクローカルアドレスを上書きするには、このフィールドに目的の IPv6 リンクローカルアドレスを入力します。 リンクローカル アドレスは、リンクローカル プレフィックス FE80::/64 と修正 EUI-64 形式のインターフェイス ID で形成されます。たとえば、MAC アドレス 00E0.B601.3B7A のインターフェイスには、リンクローカル アドレス FE80::2E0:B6FF:FE01:3B7A が指定されます。指定されたアドレスを別のホストが使用している場合は、エラーが表示されます。 • [Enable Address Auto-Configuration]：ステートレス自動設定を使用して、インターフェイスで IPv6 アドレスの自動設定をイネーブルにするには、このオプションをオンにします。アドレスは、Router Advertisement（RA; ルータアドバタイズメント）メッセージで受信されたプレフィックスに基づいて設定されます。リンクローカル アドレスが設定されていなければ、アドレスはこのインターフェイス用に自動的に生成されます。生成されたリンクローカル アドレスを別のホストが使用している場合は、エラーが発生されます。 • [Trust the DHCP Servers for default gateway]：このラジオボタンを選択して、信頼できる送信元（直接接続されたネットワーク）からのルータアドバタイズメントから、デフォルトのルートをインストールします。 • [Ignore trust and accept router advertisements]：このラジオボタンを選択して、別のネットワークからのルータアドバタイズメントから、デフォルトのルートをインストールします。 • このセクションのテーブルには、このインターフェイスに割り当てられている IPv6 アドレスが表示されます。このテーブルの下の [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します（テーブルの使用に説明されているとおり、これらは標準のボタンです）。 [Add Row] および [Edit Row] を使用すると、 [IPv6 Address for Interface] ダイアログボックス （87 ページ）が開きます。

要素	説明
Interface IPv6 Prefixes	このセクションのテーブルを使用して、IPv6 ルータ アドバタイズメントに含まれる IPv6 プレフィックス（つまり、IPv6 アドレスのネットワーク部分）を設定します。このテーブルの下の [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します（テーブルの使用に説明されているとおり、これらは標準のボタンです）。 [Add Row] および [Edit Row] を使用すると、 [IPv6 Prefix Editor] ダイアログボックス （89 ページ）が開きます。

要素	説明
Interface IPv6 DHCP	このセクションを使用して、1 つ以上のインターフェイスで DHCPv6 プレフィクス委任クライアントをイネーブルにします。ASA は、サブネット化して内部ネットワークに割り当てることができる 1 つ以上の IPv6 プレフィックスを取得します。通常、プレフィックス委任クライアントをイネーブルにしたインターフェイスは DHCPv6 アドレス クライアントを使用して IP アドレスを取得し、その他の ASA インターフェイスだけが、委任されたプレフィックスから取得されるアドレスを使用します。 次のいずれかを選択します。 • [Server Pool]：これを選択して、DHCPv6 サーバーに提供させる情報が含まれる IPv6 DHCP プールを設定します。必要に応じてインターフェイスごとに個別のプールを設定できます。また、複数のインターフェイスで同じプールを使用することもできます。[DHCPプールセレクタ（DHCP Pool Selector）] ダイアログの [行の追加（Add Row）] ボタンと [行の編集（Edit Row）] ボタンを使用して、これらのエントリを管理します。（これらはテーブルの使用で説明されている標準ボタンです。）[行の追加（Add Row）] と [行の編集（Edit Row）] で [DHCPv6 プールの追加または編集（Add or Edit DHCPv6 Pool）] ダイアログボックス （92 ページ）が開きます。 または • [Client Prefix Delegation Name]：このインターフェイスで取得したプレフィックスに名前を入力して、DHCPv6 プレフィックス委任クライアントを有効にします。有効な値は、200 文字を超えない文字列です。 • [DHCPv6 Prefix Hint]：[行の追加（Add Row）] ボタンを使用して、受信したい委任されたプレフィックスに関する 1 つ以上のヒントを提供します。通常、特定のプレフィクス長（::/60 など）を要求しますが、以前に特定のプレフィックスを受信しており、リースの期限が切れるときにそれを確実に再取得したい場合は、そのプレフィックスの全体をヒントとして入力できます。複数のヒント（異なるプレフィックスまたはプレフィックス長）を入力すると、どのヒントに従うのか、またはそもそもヒントに従うのかどうかが DHCP サーバーによって決定されます。 （注） ヒントとして提案されたプレフィックスが関連付けられたローカルプレフィックスプールの有効なプレフィックスで、いずれにも割り当てられていない場合、サーバーはクライアントが提案したプレフィックスを委任します。それ以外の場合、ヒントは無視され、プレフィックスはプールのフリー リストから委任されます。 • • [Enable DHCP]：DHCPv6 を使用してアドレスを取得するには、これを選択します。オプションとして、ルータアドバタイズメントからデフォルトルートを取得するには、[デフォルトルートを有効にする（Enable Default Route）] を選択します。

要素	説明
（注）	DHCPv6 クライアントまたはサーバープールが IPv6 インターフェイスで設定されている場合、同じインターフェイスを使用して DHCPv6 リレーを設定することはできません。

[IPv6 Address for Interface] ダイアログボックス

このダイアログボックスは、ASA または FWSM のインターフェイスに割り当てられている IPv6 アドレスを追加または編集するために使用します。[Add Interface] または [Edit Interface] ダイアログボックスの [IPv6] パネルでは、インターフェイスに複数の IPv6 アドレスを割り当てることができます。

（注） このダイアログボックスは、ルーテッド モードの ASA 7.0 以降のデバイス、トランスペアレント モードの ASA 8.2 以降のデバイス、ルーテッド モードの FWSM 3.1 以降のデバイスでのみ使用できます。

ナビゲーション パス

[IPv6 Address for Interface] ダイアログボックスには、次の場所からアクセスできます。

- ASA または FWSM の [Add Interface] と [Edit Interface] ダイアログボックスの [IPv6 パネル]。
- トランスペアレント ファイアウォール モードの ASA 5505（バージョン 8.2 と 8.3 のデバイスのみ）の [Management IPv6] ページ。

[Interfaces IPv6 Addresses] セクションのテーブルの下にある [Add Row] または [Edit Row] ボタンをクリックすると、ダイアログボックスが開きます。

関連項目

- [IPv6 Prefix Editor] ダイアログボックス （89 ページ）
- [インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM） （50 ページ）
- デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （43 ページ）
- [Management IPv6] ページ（ASA 5505）

フィールド リファレンス

表 *15 : [IPv6 Address for Interface]* ダイアログボックス

要素	説明
プレフィックス名（Prefix Name）	（任意）委任されたプレフィックスを使用するプレフィックス名を入力します。有効な値は、200 文字を超えない文字列です。 **ヒント** 「DHCP」は予約語なので、Cisco Security Manager では [プレフィックス名（Prefix Name）] として使用できません。 **（注）** ASA インターフェイスで DHCPv6 プレフィックス委任クライアントが有効になっていることを確認します。詳細については、表 14 : IPv6 タブ : [Add Interface]/[Edit Interface] ダイアログボックス（ASA/FWSM） （80 ページ）のインターフェイス IPv6 DHCP 要素を参照してください。
Address/Prefix Length	インターフェイスに割り当てられる IPv6 ネットワーク アドレスを入力し、プレフィックス長を [Prefix Length] に追加します。[Prefix Length] の整数は、アドレスのネットワーク部分を構成するアドレスの上位ビット秒の数を示します。プレフィックス長の前にスラッシュ（/）を付ける必要があります。たとえば、3FFE:C00:0:1::/64 です。 通常、委任されたプレフィクスは /60 以下であるため、複数 /64 ネットワークにサブネット化できます。接続されるクライアント用に SLAAC をサポートする必要がある場合は、/64 がサポートされるサブネット長です。/60 サブネットを補完するアドレス（::1:0:0:0:1 など）を指定する必要があります。 プレフィックスが /60 未満の場合は、アドレスの前に :: を入力します。たとえば、委任されたプレフィクスが 2001:DB8:1234:5670::/60 である場合、このインターフェイスに割り当てられるグローバル IP アドレスは 2001:DB8:1234:5671::1/64 です。ルータ アドバタイズメントでアドバタイズされるプレフィクスは 2001:DB8:1234:5671::/64 です。この例では、プレフィクスが /60 未満である場合、プレフィックスの残りのビットは、前に配置される :: によって示されるように、0 になります。たとえば、プレフィクスが 2001:DB8:1234::/48 である場合、IPv6 アドレスは 2001:DB8:1234::1:0:0:0:1/64 になります。

要素	説明
EUI-64	このチェックボックスをオンにすると、IPv6 アドレスの低位の 64 ビットに EUI-64 インターフェイス ID が使用されます。[Prefix Length] に指定される値が 64 ビットを超える場合、プレフィックス ビットはインターフェイス ID より優先されます。指定されたアドレスを別のホストが使用している場合は、エラーが発生します。 Modified EUI-64 形式のインターフェイス ID は、リンク層アドレスの上位 3 バイト（OUI フィールド）と下位 3 バイト（シリアル番号）の間に 16 進数の FFFE を挿入することで、48 ビット リンク層（MAC）アドレスから導出されます。選択されたアドレスが一意のイーサネット MAC アドレスから生成されることを保証するため、上位バイトの下位から 2 番めのビット（ユニバーサル/ローカル ビット）が反転され、48 ビット アドレスの一意性が示されます。たとえば、MAC アドレス 00E0.B601.3B7A のインターフェイスには、02E0:B6FF:FE01:3B7A の 64 ビット インターフェイス ID が指定されます。
IPv6アドレス プール（IPv6 Address Pool）	使用するアドレスのプールを表す IPv6 プールオブジェクトを入力または選択します。

[IPv6 Prefix Editor] ダイアログボックス

このダイアログボックスは、プレフィックスを IPv6 ルータ アドバタイズメントに含めるかどうかなどの個別のパラメータを制御して、IPv6プレフィックス（つまり、IPv6アドレスのネットワーク部分）を追加または編集するために使用します。ASA または FWSM の [Add Interface] または [Edit Interface] ダイアログボックスの [IPv6] パネルでは、複数のプレフィックスを設定できます。

（注） このダイアログボックスは、ルーテッド モードの ASA 7.0 以降のデバイス、トランスペアレント モードの ASA 8.2 以降のデバイス、ルーテッド モードの FWSM 3.1 以降のデバイスでのみ使用できます。

デフォルトでは、アドレスとしてインターフェイスに設定されているプレフィックスがルータ アドバタイズメントでアドバタイズされます。アドバタイズメントに特定のプレフィックスを設定する場合、これらのプレフィックスだけがアドバタイズされます。有効な推奨ライフタイムは、リアルタイムでカウントダウンされます。または、日付を設定して、プレフィックスの有効期限を指定できます。期限に達すると、プレフィックスはアドバタイズされなくなります。

ナビゲーション パス

[IPv6 Prefix Editor] ダイアログボックスには、[Add Interface] と [Edit Interface] ダイアログボックスの [IPv6] パネルからアクセスできます。これらのダイアログボックスの [Interfaces IPv6

Prefixes] セクションにあるテーブルの下にある [Add Row] または [Edit Row] ボタンをクリックします。

関連項目

- [IPv6 Address for Interface] ダイアログボックス （87 ページ）
- [インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM） （50 ページ）
- デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （43 ページ）

フィールド リファレンス

表 *16 : [IPv6 Prefix Editor]* ダイアログボックス

要素	説明
Address/Prefix Length	IPv6 ネットワーク アドレスを入力し、プレフィックス長を [Prefix Length] に追加します。[Prefix Length] の整数は、アドレスのネットワーク部分を構成するアドレスの上位ビット秒の数を示します。プレフィックス長の前にスラッシュ（/）を付ける必要があります。たとえば、3FFE:C00:0:1::/64 です。
デフォルト	このチェックボックスをオンにすると、このダイアログボックスの設定は 1 つのアドレスではなく、すべてのプレフィックスに適用されます（オンにすると、[Address/Prefix Length] フィールドはディセーブルになります）。
No Advertisements	オンにすると、ローカルリンクのホストでは、指定したプレフィックスをアドバタイズメントで使用できません。
Off Link	オンにすると、指定したプレフィックスは「オフリンク」になります。つまり、リンクにはローカルから到達できなくなります。 オンリンク（デフォルト）の場合、指定したプレフィックスがリンクに割り当てられます。指定したプレフィックスを含むアドレスにトラフィックを送信するノードは、宛先がリンク上でローカルに到達可能であると見なします。
No Auto-Configuration	オンにすると、ローカル リンクのホストでは、IPv6 自動設定に指定したプレフィックスを使用できません。 自動設定がオンの場合（デフォルト）、ローカル リンク上のホストは IPv6 自動設定に指定したプレフィックスを使用します。

要素	説明
Prefix Lifetime	ダイアログボックスのこのセクションを展開すると、次の期限オプションを表示できます。 • [ライフタイム期間（Lifetime Duration）]：このオプションを選択して、プレフィックスの期限を時間の長さとして定義します。次のオプションがイネーブルになります。 • [有効期間（Valid Lifetime）]：指定された IPv6 プレフィックスが有効なものとしてアドバタイズされる時間（秒）。値を 0 ～ 4294967295 秒の範囲で入力します。最大値は無限を示します（つまり、ライフタイムの期限は切れません）。これは、[無限（Infinite）] ボックスをオンにしても指定できます。デフォルトは 2592000（30 日間）です。 • [優先ライフタイム（Preferred Lifetime）]：指定された IPv6 プレフィックスが優先プレフィックスとしてアドバタイズされる期間（秒単位）。値を 0 ～ 4294967295 秒の範囲で入力します。最大値は無限を示します（つまり、ライフタイムの期限は切れません）。これは、[無限（Infinite）] ボックスをオンにしても指定できます。デフォルトは 604800（7 日間）です。[優先ライフタイム（Preferred Lifetime）] は、[有効期間（Valid Lifetime）] の値以下である必要があります。 • [ライフタイムの有効期限（Lifetime Expiration Date）]：このオプションをオンにて、プレフィックスの期限を特定の日付として定義します。この日付には、今日から 1 年後までの日付の値を指定できます。次のオプションを使用できます。 • [有効（Valid）]：この日時まで、プレフィックスは有効としてアドバタイズされます。 Mmm dd yyyy の形式で日付を入力します（つまり、3 文字の月の短縮形、2 桁の日、4 桁の年）。またはカレンダー アイコンをクリックして、カレンダーをスクロールして日付を選択します。また、指定した日付に期限が切れる時間を入力します。形式は 24 時間形式で hh:mm です。 • [優先（Preferred）]：この日時まで、プレフィックスは優先としてアドバタイズされます。 Mmm dd yyyy の形式で日付を入力します（つまり、3 文字の月の短縮形、2 桁の日、4 桁の年）。またはカレンダー アイコンをクリックして、カレンダーをスクロールして日付を選択します。また、指定した日付に期限が切れる時間を入力します。形式は 24 時間形式で hh:mm です。[Preferred] の日時は [Valid] の日時以前である必要があります。

[DHCPv6 プールの追加または編集（Add or Edit DHCPv6 Pool）] ダイアログボックス

このダイアログボックスを使用して、DHCPv6 サーバープールを追加または編集します。ステートレスアドレス自動設定（SLAAC）をプレフィックス委任機能と併用するクライアントについては、クライアントが情報要求（IR）パケットを ASA に送信する際に情報（DNS サーバー、ドメイン名など）を提供するように ASA を設定できます。ASA は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。

ナビゲーション パス

- [管理（Manage）] メニューから [ポリシーオブジェクト（Policy Objects）] を選択するか、ボタンバーの [Policy Object Manager] ボタンをクリックして、[Configuration Manager] ウィンドウの下部にある [Policy Object Manager] ペインを開きます。オブジェクトタイプセレクタから **[プールオブジェクト（Pool Objects）]>[DHCPv6 プールオブジェクト（DHCPv6 Pool Object）]** を選択します。作業領域内で右クリックして [新規オブジェクト（New Object）] を選択し、オブジェクトタイプを選択するか、または行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。ペインの下部にある関連するボタンを使用して、いずれかのダイアログボックスを開くこともできます。

または

- [DHCPv6 プールの追加（Add DHCPv6 Pool）] ダイアログボックスには、[DHCPv6 プールセレクタ（DHCPv6 Pool Selector）] ダイアログボックスからアクセスできます。[使用可能な DHCPv6 プール（Available DHCPv6 Pool）] テーブルの下にある [行の追加（Add Row）] または [行の編集（Edit Row）] ボタンをクリックします。[DHCPv6 プールセレクタ（DHCPv6 Pool Selector）] ダイアログボックスには、[インターフェイスの追加（Add Interface）] および [インターフェイスの編集（Edit Interface）] ダイアログボックスの [IPv6] パネルの [インターフェイス IPv6 DHCP（Interface IPv6 DHCP）] セクションにある [サーバープール（Server Pool）] オプションボタンからアクセスできます。

関連項目

- [IPv6 Address for Interface] ダイアログボックス （87 ページ）
- [インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM） （50 ページ）
- デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （43 ページ）

フィールド リファレンス

表 *17 : [DHCPv6 プールの追加（Add DHCPv6 Pool）] ダイアログボックス*

要素	説明
名前	DHCPv6 プール名は 200 文字までです。オブジェクト名では、大文字と小文字が区別されません。

要素	説明
• 1 つ以上のタブでパラメータを設定し、IR メッセージに対する応答をクライアントに提供します。 • タブごとに、必要に応じて次の内容を指定します。 • DNS/SIP/NIS/NISP/SNTP サーバー：サーバー名を入力します。IPv6 アドレスが正しい形式であることを確認してください。IPv6 アドレス形式の詳細については、http://www.ietf.org/rfc/rfc2373.txt を参照してください。 • DNS/SIP/NIS/NISP ドメイン名：ドメイン名を入力します。ドメイン名の先頭と末尾は数字または文字にする必要があります。内部文字として使用できるのは文字、数字、ハイフンのみです。ラベルはドットで区切ります。各ラベルは最大 63 文字で、ホスト名全体は最大 255 文字です。ドメイン名形式の詳細については、http://www.ietf.org/rfc/rfc1123.txt を参照してください。 （注） import コマンドは、プレフィックス委任クライアント インターフェイスで ASA が DHCPv6 サーバから取得した 1 つ以上のパラメータを使用します。手動で設定されたパラメータとインポートされたパラメータを組み合わせて使用できますが、同じコマンドを手動と import コマンドで設定することはできません。	
[サーバ（Server）] タブ	（任意）DNS サーバー名とドメイン名を指定します。
[SIP] タブ	（任意）SIP サーバー名と SIP ドメイン名を指定します。
[NIS] タブ	（任意）NIS サーバー名と NIS ドメイン名を指定します。
[NISP] タブ	（任意）NISP サーバー名と NISP ドメイン名を指定します。
[SNTP] タブ	（任意）SNTP サーバー名を指定します。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

デバイス インターフェイス：IP タイプ（PIX/ASA 7.0 以降）

シングルコンテキストのルーテッド モードで動作しているセキュリティ デバイスには、そのインターフェイスの IP アドレス指定が必要です。ただし、ファイアウォール インターフェイスには、割り当てられるまで IP アドレスがありませんトランスペアレントモードでは、デバイスはアクセス制御ブリッジ（「Bump In The Wire」）として機能することに注意してください。つまり、インターフェイスにそれぞれ異なる VLAN を割り当てますが、IP アドレス指定は必要ありません。

シングルコンテキスト、ルーテッドモードの独立した ASA または PIX 7.0 以降のデバイスに表示される [インターフェイスの追加（Add Interface）] または [インターフェイスの編集（Edit Interface）] ダイアログボックスには、[IP タイプ（IP Type）] セクションがあります。次の説明に従って、ここにインターフェイスの IP アドレス指定のタイプを指定し、関連するパラメータを入力します。（PIX 6.3 デバイス用の [Add Interface] または [Edit Interface] ダイアログボックスの [IP Type] セクションについては、デバイス インターフェイス：IP タイプ（PIX 6.3）（48 ページ）を参照してください）。

マルチコンテキスト モードでは、インターフェイス IP アドレスはコンテキスト設定で設定されます。

（注） グローバルプールやスタティック NAT エントリの IP アドレスなど、以前にルータ、ホスト、または他のファイアウォール デバイス コマンドに使用したアドレスは使用しないでください。また、冗長インターフェイスとして使用するインターフェイスには、IP タイプの情報を指定しないでください。

ステップ 1 [インターフェイスの追加（Add Interface）] または [インターフェイスの編集（Edit Interface）] ダイアログボックスで、次のように、[IP タイプ（IP Type）] リストからアドレス割り当て方式（[スタティック IP（Static IP）]、[DHCP の使用（Use DHCP）]、または [PPPoE]（PIX および ASA 7.2 以降））を選択し、関連パラメータを指定します。

- [スタティック IP（Static IP）]：このインターフェイスが接続するネットワーク上のセキュリティデバイスを示すスタティック IP アドレスおよびサブネットマスクを指定します。IP アドレスは、インターフェイスごとに一意でなければなりません。

サブネット マスクは、ドット区切り 10 進表記（255.255.255.0 など）で表すか、またはネットワーク マスクのビット数（24 など）を入力して表すことができます。バージョン 4.13 以降、Cisco Security Manager では、ポイント ツー ポイント インターフェイスに 255.255.255.254 を使用できます。ネットワークに接続するインターフェイスには 255.255.255.255 を使用しないでください。使用すると、トラフィックがこのインターフェイスで停止します。サブネット マスク値を指定しない場合は、次に示すように「クラスフル」ネットワークが使用されます。

- IP アドレスの最初のオクテットが 1 ～ 126 の場合（つまり、アドレスが 1.0.0.0 ～ 126.255.255.255 の場合）、クラス A ネットマスク（255.0.0.0）が使用されます。
- IP アドレスの最初のオクテットが 128 ～ 191 の場合（つまり、アドレスが 128.0.0.0 ～ 191.255.255.255 の場合）、クラス B ネットマスク（255.255.0.0）が使用されます。
- IP アドレスの最初のオクテットが 192 ～ 223 の場合（つまり、アドレスが 192.0.0.0 ～ 223.255.255.255 の場合）、クラス C ネットマスク（255.255.255.0）が使用されます。

（注） グローバル プールやスタティック NAT エントリの IP アドレスなど、以前にルータ、ホスト、または他のファイアウォール デバイス コマンドに使用したアドレスは使用しないでください。

- [Use DHCP]：Dynamic Host Configuration Protocol（DHCP）をイネーブルにして、接続ネットワーク上の DHCP サーバから IP アドレスが自動的に割り当てられるようにします。次のオプションを使用できます。
  - [DHCP 学習済みルートメトリック（DHCP Learned Route Metric）]（必須）：学習したルートにアドミニストレーティブ ディスタンスを割り当てます。有効な値は 1 ～ 255 です。学習されたルートのアドミニストレーティブ ディスタンスはデフォルトで 1 になります。

すべてのルートに、その使用プライオリティを示す値または「メトリック」があります。（このメトリックは「アドミニストレーティブ ディスタンス」とも呼ばれます）。同じ接続先に対して 2 つ以上のルートが使用可能な場合、デバイスはアドミニストレーティブ ディスタンスを使って使用するルートを決定します。

- [DHCP を使用したデフォルトルートの取得（Obtain Default Route using DHCP）]：デフォルトのスタティックルートを設定する必要がないように DHCP サーバーからデフォルトルートを取得するには、このオプションを選択します。スタティック ルートの設定も参照してください。
  - [DHCP 学習済みルートのトラッキングの有効化（Enable Tracking for DHCP Learned Route）]：[DHCP を使用したデフォルトルートの取得（Obtain Default Route using DHCP）] を選択した場合、このオプションを選択し、特定のサービスレベル契約（SLA）モニターによるルートトラッキングを有効にできます。次のオプションが使用可能になります。
  - [トラッキング済み SLA モニター（Tracked SLA Monitor）]：[DHCP 学習済みルートのトラッキングの有効化（Enable Tracking for DHCP Learned Route）] を選択した場合は必須です。このインターフェイスに適用されるルート トラッキング（接続性のモニタリング）を定義している SLA モニタ

オブジェクトの名前を入力または選択します。詳細については、接続を維持するためのサービス レベル契約（SLA）のモニタリングを参照してください。

- [PPPoE]（PIX および ASA 7.2 以降）：Point-to-Point Protocol over Ethernet（PPPoE）をイネーブルにして、接続ネットワーク上の PPPoE サーバーから IP アドレスが自動的に割り当てられるようにします。このオプションは、フェールオーバーではサポートされません。次のオプションを使用できます。
  - [VPDN グループ名（VPDN Group Name）]（必須）：ネットワーク接続、ネゴシエーション、および認証に使用する認証方式とユーザー名/パスワードが含まれるバーチャル プライベート ダイヤルアップ ネットワーク（VPDN）グループを選択します。詳細については、接続を維持するためのサービス レベル契約（SLA）のモニタリングを参照してください。
  - [IP アドレス（IP Address）]：指定した場合、ネゴシエートされたアドレスではなく、このスタティック IP アドレスが接続および認証に使用されます。
  - [サブネットマスク（Subnet Mask）]：指定した IP アドレスとともに使用されるサブネットマスク。
  - [PPPoE 学習済みルートメトリック（PPPoE Learned Route Metric）]（必須）：学習したルートにアドミニストレーティブ ディスタンスを割り当てます。有効な値は 1 ～ 255 です。デフォルトは 1 です。

すべてのルートに、その使用プライオリティを示す値または「メトリック」があります。（このメトリックは「アドミニストレーティブ ディスタンス」とも呼ばれます）。同じ接続先に対して 2 つ以上のルートが使用可能な場合、デバイスはアドミニストレーティブ ディスタンスを使って使用するルートを決定します。

-
  - [PPPoE を使用してデフォルトルートを取得（Obtain Default Route using PPPoE）]：PPPoE サーバーからデフォルトルートを取得するには、このオプションをオンにします。PPPoE クライアントでまだ接続が確立されていない場合には、デフォルトルートを設定します。このオプションを使用する場合は、スタティックに定義されたルートを設定に含めることができません。
  - [PPPoE 学習ルートのトラッキングの有効化（Enable Tracking for PPPoE Learned Route）]：[PPPoE を使用したデフォルトルーティングの取得（Obtain Default Routing Using PPPoE）] を選択した場合、このオプションを選択して、PPPoE が学習したルートのルートトラッキングを有効化できます。次のオプションを使用できます。
  - [デュアル ISP インターフェイス（Dual ISP Interface）]：デュアル ISP サポート用のインターフェイスを定義する場合、設定中の接続を示す [プライマリ（Primary）] または [セカンダリ（Secondary）] を選択します。
  - [トラッキング済み SLA モニター（Tracked SLA Monitor）]：[DHCP 学習済みルートのトラッキングの有効化（Enable Tracking for DHCP Learned Route）] を選択した場合は必須です。このインターフェイスに適用されるルートトラッキング（接続性のモニタリング）を定義している SLA モニタオブジェクトの名前を入力または選択します。詳細については、接続を維持するためのサービス レベル契約（SLA）のモニタリングを参照してください。

（注） DHCP および PPPoE は、ファイアウォール デバイスの外部インターフェイスでだけ設定できます。外部インターフェイスで PPPoE がすでに設定されている場合は、オプションとして使用できません。

ステップ 2 [インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM）（50 ページ）に従ってデバイス インターフェイスの設定を続けます。

デバイス インターフェイス：MAC アドレス

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では、最初に追加された物理インターフェイスの MAC アドレスが使用されます。構成でメンバーインターフェイスの順序を変更すると、MAC アドレスがリストの先頭にある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。手動で冗長インターフェイスに MAC アドレスを割り当てた場合、物理インターフェイスの MAC アドレスに関係なく、このアドレスが使用されます。

同様に、EtherChannel グループに割り当てられているすべてのインターフェイスは、同じ MAC アドレスを共有します。デフォルトでは、EtherChannel は最も番号の小さいメンバ インターフェイスの MAC アドレスを使用します。ただし、最も小さい番号のインターフェイスがグループから削除された場合にトラフィックの分断を防止するため、EtherChannel の MAC アドレスを手動で設定できます。

サブインターフェイスに一意の MAC アドレスを割り当てることが必要になる場合もあります。たとえば、サービス プロバイダーが MAC アドレスに基づいてアクセスを制御している場合などです。

さらに、フェールオーバーを使用する場合は、スタンバイ MAC アドレスを指定できます。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。

（注） 次のオプションは、PIX 7.2 以降と ASA 7.2 以降のデバイスの [Add Interface] と [Edit Interface] ダイアログボックスの [Advanced] タブにのみ表示されます。

（任意）プライベート MAC アドレスを現在のインターフェイスに手動で割り当てるには、次の手順を実行します。

ステップ 1 [インターフェイスの追加（Add Interface）] または [インターフェイスの編集（Edit Interface）] ダイアログボックスで、[アクティブなMACアドレス（Active MAC Address）] フィールドに目的の MAC アドレスを入力します。

MAC アドレスは、H.H.H の形式で指定します。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 の場合、000C.F142.4CDE と入力します。

（注） 場合によっては、[Standby MAC Address] フィールドをアクティブにするためには、[Active MAC Address] に入力したあとに、Tab キーを押す必要がある場合があります。

ステップ 2 必要に応じて、デバイスレベルのフェールオーバーで使用する**スタンバイ MAC アドレス**を指定します。

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 [インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM）（50 ページ）に従ってデバイス インターフェイスの設定を続けます。

[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス：[スイッチポート（Switch Port）] タブ

[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックスの [スイッチポート（Switch Port）] パネルを使用して、Firepower 1010 デバイスのモード、アクセス VLAN ID、トランクタイプ、VLAN ID などを設定します。

ナビゲーション パス

[Add Interface] と [Edit Interface] ダイアログボックスには、[Interfaces] ページからアクセスできます。[スイッチポートの有効化（Enable Switchport）] チェックボックスをオンにして、これらを設定します。

フィールド リファレンス

表 *18 : [スイッチポート（Switch Port）] タブ：[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス*

要素	説明
[スイッチポートの有効化（Enable Switchport）]	選択したインターフェイスでスイッチポートを有効にするには、このボックスをオンにします。このオプションをオフにすると、インターフェイスのスイッチポートが無効になりますが、設定情報はそのまま保持されます。
[モード（Mode）]	利用可能な 2 つのモードであるアクセスまたはトランクのいずれかを選択します。
アクセス VLAN ID	このダイアログボックスは、アクセスモードが選択されている場合にのみ有効になります。0 ～ 4190 の範囲内で値を入力します。インターフェイスに設定されている VLAN ID がここに入力されます。
トランク タイプ	使用可能な 2 つのトランクタイプである許可またはネイティブのいずれかを選択します。

要素	説明
VLAN ID（Admin. VLAN ID）	選択したモードに従って、このポートの VLAN ID を入力します。
[保護の有効化（Enable Protected）]	このオプションは、このポートが同じ VLAN 上の他のスイッチポートと通信できないようにする場合に選択します。

[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス：[Power Over Ethernet] タブ

[インターフェイスの追加（Add Interface）]/[インターフェイスの編集（Edit Interface）] ダイアログボックスの [Power Over Ethernet (POE)] は、電力消費モードとワット数を設定するために使用されます。ASA 9.13(1) 以降、この機能は Firepower 1010 デバイスでサポートされ、ポート Ethernet1/7 および Ethernet1/8 の物理インターフェイスの一部です。

POE機能を使用すると、物理インターフェイスを構成して、クラス制限ワット数に従って、接続されたデバイスに電力が自動的に供給されるようにできます。指定されたポート（Ethernet1/7 または Ethernet1/8）から電源が遮断されます。指定されたポートに必要なワット数は、LLDP ネゴシエーションなしでミリワット単位で事前に設定されています。

フィールド リファレンス

表 *19 : [*スイッチポート（*Switch Port***）*]* タブ：*[*インターフェイスの追加/編集（***Add/Edit Interface***）*]* ダイアログボックス**

要素	説明
POEを無効にする（Disable POE）	指定したポート（Ethernet 1/7 または Ethernet 1/9）への電源を遮断するには、このチェックボックスをオンにします。
消費モード（Consumption Mode）	電力消費モードを選択します。 • [自動（Auto）]（デフォルト）：これを選択すると、クラス制限ワット数に従って、接続されたデバイスに自動的に電力が供給されます。 • [設定（Configure）]：これを選択して、選択したポートに必要な消費ワット数を手動で指定します。
消費ワット数（Consumption Wattage）	選択したポートに必要な消費ワット数（ミリワット）を指定します。

ASA 5505 でのハードウェア ポートの設定

ASA 5505 デバイスに表示される [インターフェイス（Interfaces）] ページには、[ハードウェアポート（Hardware Ports）] および [インターフェイス（Interfaces）] の 2 つのタブ付きパネルが表示されます。[Hardware Ports] パネルのテーブルには、選択した ASA 5505 に現在設定されているスイッチ ポートが表示されます。

[Configure Hardware Ports] ダイアログボックスを使用して、ASA 5505 のスイッチ ポートを設定します。モードの設定、スイッチ ポートの VLAN への割り当て、[Protected] オプションの設定などが含まれます。（次のダイアログボックス パラメータの説明では、[Hardware Ports] テーブルのフィールドも説明します）。

注意 ASA 5505 では、ネットワーク内のループ検出のためのスパニングツリー プロトコルはサポートされません。そのため、アプライアンスとの接続がネットワーク ループにならないようにする必要があります。

ナビゲーション パス

[Configure Hardware Ports] ダイアログボックスには、ASA 5505 の [Interfaces] ページにある [Hardware Ports] パネルの [Add Row] または [Edit Row] をクリックするとアクセスできます。詳細については、デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理（43 ページ）を参照してください。

関連項目

- ASA 5505 のポートおよびインターフェイスについて （8 ページ）
- [インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM） （50 ページ）

フィールド リファレンス

表 20 : [Configure Hardware Ports] ダイアログボックス

要素	説明
[Enable Interface]	このオプションを選択すると、このスイッチ ポートがイネーブルになります。このオプションをオフにすると、このポートをディセーブルにできますが、設定情報は保持されます。
隔離（Isolated）	このオプションは、このポートが同じ VLAN 上の他の隔離されたスイッチポートまたは「保護された」スイッチポートと通信できないようにする場合に選択します。 スイッチ ポート上のデバイスが主に他の VLAN からアクセスされ、VLAN 内アクセスを許可する必要がなく、感染などのセキュリティ違反があったときにデバイスを相互に分離する必要がある場合、それらのポートが相互に通信できないようにすることがあります。たとえば、3 つの Web サーバをホストする DMZ がある場合、各スイッチ ポートに [Protected] オプションを適用すると、Web サーバを相互に分離できます。内部および外部ネットワークはいずれも 3 つすべての Web サーバと通信でき、またその逆も可能ですが、Web サーバどうしは通信できません。

要素	説明
Hardware Port	設定しているスイッチ ポートを選択します。すべてのデバイス ポートが一覧表示されます。
[モード（Mode）]	このポートのモードを選択します。 • [アクセスポート（Access Port）]：ポートをアクセスモードに設定します。各アクセス ポートは 1 つの VLAN に割り当てることができます。 • [トランクポート（Trunk Port）]：ポートを 802.1Q タギングを使用するトランクモードに設定します。トランク ポートは、802.1Q タギングを使用して複数の VLAN を伝送できます。 トランク モードが使用できるのは Security Plus ライセンスだけです。トランク ポートでは、タグが付いていないパケットはサポートされません。ネイティブ VLAN サポートはなく、すべてアプライアンスはタグが含まれていないパケットをドロップします。
VLAN ID（Admin. VLAN ID）	選択した [Mode] に従って、このポートの VLAN ID を入力します。 • [Access Port] モードでは、このスイッチ ポートが割り当てられる VLAN ID を入力します。 • [Trunk Port] モードでは、複数の VLAN ID および複数の ID 範囲（4-8 など）をカンマで区切って入力できます。 （注） 7.2(2)18 以前のオペレーティング システムをデバイスで実行している場合、有効な VLAN ID は 1 ～ 1001 です。バージョン 7.2(2)19 以降での有効な ID は 1 ～ 4090 です。
デュプレックス	ポートのデュプレックスオプションを [フル（Full）]、[ハーフ（Half）]、[自動（Auto）] から選択します。デフォルトである [Auto] 設定を推奨します。 PoE ポート Ethernet 0/6 または 0/7 のデュプレックスを [Auto] 以外に設定した場合、IEEE 802.3af をサポートしない Cisco IP Phone および Cisco ワイヤレス アクセス ポイントは検出されず、電力は供給されません。

要素	説明
速度	ポートの速度を [10]、[100]、[自動（Auto）] から選択します。デフォルトである [Auto] 設定を推奨します。 PoE ポート Ethernet 0/6 または 0/7 の速度を [Auto] 以外に設定した場合、IEEE 802.3af をサポートしない Cisco IP Phone および Cisco ワイヤレス アクセス ポイントは検出されず、電力は供給されません。 デフォルトの [Auto] 設定には、Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスで Auto-MDI/MDIX をイネーブルにするには、[Speed] または [Duplex] のいずれかを [Auto] に設定する必要があります。[Speed] と [Duplex] の両方を明示的に固定値に設定し、したがって両方の設定のオートネゴシエーションをディセーブルにした場合、Auto-MDI/MDIX もディセーブルになります。

[Add Bridge Group]/[Edit Bridge Group] ダイアログボックス

トランスペアレント ファイアウォールは、その内部インターフェイスと外部インターフェイスで同じネットワークを接続し、コンテキストにつき 2 つのインターフェイスだけをサポートします。ただし、ブリッジ グループを使用すると、コンテキストに使用できるインターフェイスの数を増やすことができます。ブリッジ グループは 8 個まで設定できます。FWSM では各グループに 2 つのインターフェイスを含めることができ、ASA 9.6.1 では各グループに 64 のインターフェイスを含めることができます。

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、トラフィックはセキュリティ アプライアンス内の別のブリッジ 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セキュリティ アプライアンス内の別のブリッジ グループにルーティングされる前に、セキュリティ アプライアンス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防ぐ場合、またはセキュリティ コンテキストの使用を最小限に抑える場合、複数のブリッジ グループを使用することがあります。ブリッジング機能はブリッジ グループごとに分かれていますが、その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、syslog サーバーまたは AAA サーバーの設定は、すべてのブリッジ グループで共有されます。セキュリティ ポリシーを完全に分離するには、各コンテキスト内に 1 つのブリッジ グループにして、セキュリティ コンテキストを使用します。

Cisco Security Manager 4.13 以降、ブリッジグループ仮想インターフェイス（BV） 機能がルーテッドファイアウォールモードに拡張されています。ルーテッドファイアウォールは、ブリッジグループを設定することによって実装されます。ユーザは、最大 8 つのブリッジグループを設定でき、ASA 9.7.1（Cisco Security Manager 4.13）では、各グループに最大 64 のインターフェイスを含めることができます。Cisco Security Manager 4.13 以前のバージョンでは、ユーザは最大 2 つのブリッジグループを設定できます。各グループには、最大 4 つのインターフェイスが含まれます。トランスペアレントモードでサポートされる BVI 機能に加えて、ルーテッド ファイアウォール モードには、次の追加の通信モードのサポートが含まれます。

- BVI 間通信
- BVI からデータポートへの通信（レイヤ 2 からレイヤ 3）およびその逆

トランスペアレント モードの FWSM 3.1 以降および ASA 8.4.1 以降のデバイスでは、[Interfaces] ページには [Interfaces] および [Bridge Groups] の 2 つのタブ付きパネルが表示されます。次の情報は [Bridge Groups] パネルと [Add Bridge Group] または [Edit Bridge Group] ダイアログボックスに適用されます。[Interfaces] パネルについては、[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM） （50 ページ）を参照してください。

ナビゲーション パス

[ブリッジグループの追加（Add Bridge Group）] または [ブリッジグループの編集（Edit Bridge Group）] ダイアログボックスには、[インターフェイス（Interfaces）] ページの [ブリッジグループ（Bridge Groups）] パネルからアクセスできます。

関連項目

- ルーテッド モードおよびトランスペアレント モードのインターフェイス （6 ページ）
- FWSM 3.1 のブリッジング サポート
- デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （43 ページ）

フィールド リファレンス

表 21 : [Add Bridge Group]/[Edit Bridge Group] ダイアログボックス

要素	説明
[General] タブ	
ブリッジ グループ	このブリッジ グループの名前を入力します。

要素	説明
名前	このインターフェイスに最大 48 文字の ID を指定します。名前には、インターフェイスの用途に関係する覚えやすい名前を付けます。ただし、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用に予約しているインターフェイスに名前を付けないでください。これには、フェールオーバー用に使用する EtherChannel およびそのメンバインターフェイスも含まれます。また、冗長インターフェイスペアのメンバとして使用するインターフェイスに名前を付けないでください。 セキュリティアプライアンスのインターフェイス命名ルールに従って、いくつかの名前が特定のインターフェイス用に予約されています。そのため、これらの予約名を使用すると、次のように、デフォルトの予約済みセキュリティ レベルが適用されます。 • [Inside]：内部ネットワークに接続します。最もセキュアなインターフェイスにする必要があります。 • [DMZ]：中間インターフェイスに接続された「緩衝地帯」。DMZ は境界ネットワークとも呼ばれます。DMZ インターフェイスに任意の名前を付けることができます。一般的に、DMZ インターフェイスには、インターフェイスタイプを識別するために「*DMZ*」というプレフィックスを付けます。 • [Outside]：外部ネットワークまたはインターネットに接続します。セキュア度の最も低いインターフェイスにする必要があります。 同様に、一般的にサブインターフェイス名には、一意の ID に加えて、関連付けられているインターフェイスも示されます。たとえば、*DMZoobmgmt* は、DMZ インターフェイスに接続されている Out of Band Management Network を示すことができます。 （注） この場合でも、**インターフェイスをフェールオーバー用または冗長インターフェイスのメンバーとして使用する場合は、そのインターフェイスに名前を付けないでください**。詳細については、冗長インターフェイスの設定 （11 ページ）を参照してください。
ID	1 ～ 100 の整数でこのブリッジ グループの ID を入力します。
セキュリティ レベル（Security Level）	VLAN インターフェイスにセキュリティレベルを割り当てます。有効な値は 0 ～ 100 で、100 が最も安全です。

要素	説明
Available Interfaces	使用可能なインターフェイスまたはVLANのリストから選択して、このブリッジグループに割り当てます。使用可能なすべてのインターフェイスが一覧表示されます。 （注） ASA 9.7.1（Cisco Security Manager 4.13）以降、ブリッジグループごとに最大 64 のインターフェイスがサポートされます。
グループ内のメンバー（Members In Group）	現在のブリッジグループのインターフェイスの数を表示します
IP タイプ（IP Type）	インターフェイスの IP タイプを選択します。 • [スタティック IP（Static IP）]：ブリッジグループのインターフェイスに IP アドレスとサブネットマスクを割り当てます。 • [DHCP]： DHCP を使用して インターフェイスの IP アドレスを取得します。 • [DHCPを使用してデフォルトルートを取得する（Obtain Default Route using DHCP）]：選択すると、Cisco Security Manager は DHCP サーバーによって提供されるデフォルトルートを使用します。
IPアドレス	ブリッジ グループの管理 IP アドレスを入力または選択します。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。したがって、ブリッジ グループに必要な IP 設定は、この管理 IP アドレスだけです。このアドレスは、システム メッセージや AAA サーバとの通信など、セキュリティ アプライアンスで発信されるトラフィックの送信元アドレスです。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。 （注） IPv6 アドレスはブリッジ グループではサポートされていません。
ネットマスク	指定した IP アドレスのネットワーク マスク。値は、ドット区切り 10 進表記（255.255.255.0 など）で表すか、またはネットワーク マスクのビット数（24 など）を入力して表すことができます。 （注） ネットワークに接続するインターフェイスには 255.255.255.255 を使用しないでください。使用すると、トラフィックがこのインターフェイスで停止します。
説明	このブリッジ グループの説明（任意）を入力できます。
[IPv6] タブ	
IPv6を有効化（Enable IPv6）	IPv6 を有効化して、このブリッジグループで IPv6 アドレスを設定するには、このチェックボックスをオンにします。このオプションをオフにすると、このブリッジグループで IPv6 を無効化できますが、設定情報は保持されます。

要素	説明
Enforce EUI-64	オンにすると、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 ID の使用を適用します。 このオプションがブリッジグループで有効化されていると、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、ブリッジ グループ 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検査されます。IPv6 パケットのインターフェイス ID が Modified EUI-64 形式でない場合、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。 「%PIX|ASA-3-325003: EUI-64 source address check failed.」 アドレス形式の検証は、フローが作成された場合にのみ行われます。既存のフローからのパケットは確認されません。さらに、アドレス検証はローカル 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。 Modified EUI-64 形式のインターフェイス ID は、リンク層アドレスの上位 3 バイト（OUI フィールド）と下位 3 バイト（シリアル番号）の間に 16 進数の FFFE を挿入することで、48 ビット リンク層（MAC）アドレスから導出されます。選択されたアドレスが一意のイーサネット MAC アドレスから生成されることを保証するため、上位バイトの下位から 2 番めのビット（ユニバーサル/ローカル ビット）が反転され、48 ビット アドレスの一意性が示されます。たとえば、MAC アドレス 00E0.B601.3B7A のインターフェイスには、02E0:B6FF:FE01:3B7A の 64 ビット インターフェイス ID が指定されます。

要素	説明
DAD Attempts	Duplicate Address Detection（DAD; 重複アドレス検出）の実行中にブリッジ グループインターフェイスで送信される連続ネイバー送信要求メッセージの数を指定するには、このフィールドに0～600の数を入力します。0を入力すると、インターフェイス上で重複アドレス検出がディセーブルになります。1 を入力すると、フォローアップ送信のない一度の送信を設定します。これはデフォルトです。 アドレスがインターフェイスに割り当てられる前に、重複アドレス検出によって、新しいユニキャスト IPv6 アドレスの一意性が確認されます（重複アドレス検出の実行中、新しいアドレスは一時的な状態になります）。重複アドレス検出では、ネイバー送信要求メッセージを使用して、ユニキャスト IPv6 アドレスの一意性を確認します。 重複アドレス検出によって重複アドレスが特定された場合、そのアドレスの状態は DUPLICATE に設定され、アドレスは使用されなくなります。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の場合は、そのインターフェイス上で IPv6 パケットの処理がディセーブルになり、次のようなエラー メッセージが発行されます。 %PIX-4-DUPLICATE: Duplicate address FE80::1 on outside 重複アドレスがインターフェイスのグローバルアドレスの場合は、そのアドレスは使用されず、前述のリンクローカル アドレスと同様のエラー メッセージが発行されます。 重複アドレスに関連付けられているコンフィギュレーション コマンドはすべて設定済みのままになりますが、アドレスの状態は DUPLICATE に設定されます。インターフェイスのリンクローカルアドレスに変更があると、新しいリンクローカルアドレスに対して重複アドレス検出が行われ、そのインターフェイスに関連付けられている他のすべての IPv6 アドレスが再生成されます（つまり、重複アドレス検出は、新しいリンクローカルアドレスでのみ行われます）。
NS Interval	IPv6 ネイバー送信要求メッセージの再送信間隔（ミリ秒単位）。有効な値の範囲は 1000 ～ 3600000 ミリ秒で、デフォルト値は 1000 ミリ秒です。 （注） この値は、このインターフェイスで送信されるすべての IPv6 ルータ アドバタイズメントに含まれます。

要素	説明
Reachable Time	リモートIPv6ノードが到達可能であることが最初に確認されてから、このノードが到達可能であると見なされ続ける時間（ミリ秒単位）。有効な値の範囲は0 ～ 3600000 ミリ秒で、デフォルト値は 0 です。この値に 0 を使用する場合、到達可能時間は未定に設定されます。つまり、到達可能時間の設定および追跡は受信デバイス次第です。 設定時間によって、使用不可のネイバーを検知できます。時間を短く設定すると、使用できないネイバーをより早く検出できます。ただし、時間を短くするほど、IPv6 ネットワーク帯域幅とすべての IPv6 ネットワーク デバイスの処理リソースの消費量が増えます。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。
管理対象設定フラグ	IPv6 ルータ アドバタイズメント パケットの「managed-config-flag」フラグを設定するかどうか。
その他の設定フラグ	IPv6 ルータ アドバタイズメント パケットの「other-config-flag」フラグを設定するかどうか。
Enable RA	オンにすると、インターフェイスで IPv6 ルータ アドバタイズメントの送信がイネーブルになります。次のオプションを使用できます。 • [RA Lifetime]：「ルータライフタイム」値は、ローカルリンク上のノードがセキュリティアプライアンスをリンク上のデフォルトルータと見なし続ける期間を指定します。有効な値の範囲は 0 ～ 9000 秒で、デフォルトは1800秒です。0を入力すると、セキュリティアプライアンスは選択したインターフェイスのデフォルト ルータとは見なされません。 0 以外の任意の値は、次の [RA Interval] 値より小さい値にはできません。 （注） この値は、このインターフェイスで送信されるすべての IPv6 ルータ アドバタイズメントに含まれます。 • [RA Interval]：このインターフェイスでの IPv6 ルータアドバタイズメントの送信間隔。有効な値の範囲は 3 ～ 1800 秒です（次の [RA Interval in Milliseconds] オプションがオンの場合は 500 ～ 1800000 ミリ秒）。デフォルトは 200 秒です。 [RA Lifetime] が 0 以外の場合、送信の間隔は [RA Lifetime] の値以下にする必要があります。他の IPv6 ノードと同期しないようにするには、使用する実際値を必要値の 20 % 以内にランダムに調整します。 • [RA Interval in Milliseconds]：このオプションをオンにすると、指定した [RA Interval] の値が秒ではなくミリ秒になります。

要素	説明
Interface IPv6 Addresses	ダイアログボックスのこのセクションで、ブリッジ グループ インターフェイスに割り当てられている IPv6 アドレスを指定します。 • [Link-Local Address]：インターフェイスに自動的に生成されたリンクローカルアドレスを上書きするには、このフィールドに目的の IPv6 リンクローカルアドレスを入力します。 リンクローカル アドレスは、リンクローカル プレフィックス FE80::/64 と修正 EUI-64 形式のインターフェイス ID で形成されます。たとえば、MAC アドレス 00E0.B601.3B7A のインターフェイスには、リンクローカル アドレス FE80::2E0:B6FF:FE01:3B7A が指定されます。指定されたアドレスを別のホストが使用している場合は、エラーが表示されます。 • [Enable Address Auto-Configuration]：ステートレス自動設定を使用して、インターフェイスで IPv6 アドレスの自動設定をイネーブルにするには、このオプションをオンにします。アドレスは、Router Advertisement（RA; ルータアドバタイズメント）メッセージで受信されたプレフィックスに基づいて設定されます。リンクローカルアドレスが設定されていなければ、アドレスはこのインターフェイス用に自動的に生成されます。生成されたリンクローカルアドレスを別のホストが使用している場合は、エラーが発生されます。 • [Trust the DHCP Servers for default gateway]：このラジオボタンを選択して、信頼できる送信元（直接接続されたネットワーク）からのルータアドバタイズメントから、デフォルトのルートをインストールします。 • [Ignore trust and accept router advertisements]：このラジオボタンを選択して、別のネットワークからのルータアドバタイズメントから、デフォルトのルートをインストールします。 • このセクションのテーブルには、このインターフェイスに割り当てられている IPv6 アドレスが表示されます。このテーブルの下の [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します（テーブルの使用に説明されているとおり、これらは標準のボタンです）。 [Add Row] および [Edit Row] を使用すると、 [IPv6 Address for Interface] ダイアログボックス （87 ページ）が開きます。

要素	説明
Interface IPv6 Prefixes	このセクションのテーブルを使用して、IPv6 ルータ アドバタイズメントに含まれる IPv6 プレフィックス（つまり、IPv6 アドレスのネットワーク部分）を設定します。このテーブルの下の [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します（テーブルの使用に説明されているとおり、これらは標準のボタンです）。 [Add Row] および [Edit Row] を使用すると、[IPv6 Prefix Editor] ダイアログボックス （89 ページ）が開きます。

高度なインターフェイス設定（PIX/ASA/FWSM）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしますが、バグ修正や拡張機能はサポートしていません。

高度な設定オプションは、シングルコンテキストモードで動作している FWSM および ASA/PIX 7.0 以降のデバイスと、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動作している ASA 9.0 以降のデバイス上のインターフェイスに使用可能です。

これらは全般的なデバイス関連設定です。つまり、個別のインターフェイスには適用されません。

（注） この項の情報は、PIX 6.3 デバイスにも、マルチコンテキスト モードのセキュリティ デバイスにも適用されません。

[Advanced Interface Settings] ダイアログボックスには、次の要素があります。

- [MACアドレス自動（MAC Address Auto）]：各共有コンテキスト インターフェイスにプライベート MAC アドレスを自動的に割り当てることができます。オプションで、MAC アドレスの一部として使用するユーザー定義のプレフィックスを設定できます。prefix は、0 ～ 65535 の 10 進数です。プレフィックスを入力しない場合、ASA によりデフォルトのプレフィックスが生成されます。このプレフィックスは、4 桁の 16 進数値に変換されます。プレフィックスにより、各 ASA は固有の MAC アドレスを使用（異なるプレフィックスの値を使用）することになるため、たとえば 1 つのネットワークセグメントに複数の ASA を配置できます。
- [同じセキュリティレベルのインターフェイス間でのトラフィック（Traffic between interfaces with same security levels）]：このパラメータでは、同じセキュリティレベルのインターフェイスとサブインターフェイス間の通信を制御します。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。詳細については、同じセキュリティ レベルを持つインターフェイス間のトラフィックのイネーブル化 （112 ページ）を参照してください。

- [PPPoEユーザー（PPPoE Users）] ボタン：このボタンをクリックして、[PPPoEユーザー（PPPoE Users）] ダイアログボックスを開きます。このダイアログボックスでは、PPPoE ユーザ リストの管理 （113 ページ）で説明されているとおり、PPPoE ユーザーを追加、編集、および削除できます。このオプションは、ASA および PIX 7.0 以降のデバイスでのみ使用できます。
- [VPDNグループ（VPDN Groups）]（PIX および ASA 7.2 以降）：このテーブルには、現在定義されている VPDN グループが一覧表示されます。テーブルの下にあるボタンは、VPDN グループの管理 （114 ページ）の説明に従って、VPDN グループのエントリを追加、編集、および削除するために使用します。
- [LACPシステムプライオリティ（LACP System Priority）]（ASA 8.4.1 以降）：EtherChannel リンク集約に参加するすべてのシステムには、Link Aggregation Control Protocol（LACP）システムプライオリティが必要です。この値には 1 ～ 65535 を指定できます。数字が大きいほど、プライオリティは低くなります。デフォルトは 32768 です。

この値とシステムの MAC アドレスが組み合わされて、システムの LACP 識別子が形成されます。したがって、EtherChannel インターフェイスにのみ適用されます。詳細については、EtherChannel の設定 （13 ページ）を参照してください。

（注） EtherChannel に割り当てられている個別のインターフェイスの [Edit Interface] ダイアログボックスでは、追加の LACP パラメータを使用できます。詳細については、EtherChannel に割り当てられているインターフェイスの LACP パラメータの編集 （16 ページ）を参照してください。

（注） LACP システムプライオリティは、Cisco Firepower 9000 デバイスではサポートされていません。

- [スタティックポートプライオリティ（Static Port Priority）]（スパンドモードの ASA 9.2.1 以降のクラスタ）：LACP のダイナミック ポート プライオリティを無効にします。一部のスイッチはダイナミック ポート プライオリティをサポートしていないので、このパラメータによりスイッチの互換性が向上します。スタティック ポート プライオリティを有効にすると、16 のアクティブなスパンド EtherChannel メンバーのサポートが有効になります。このパラメータを使用しないと、サポートされるのは 8 個のアクティブ メンバと 8 個のスタンバイ メンバのみです。このパラメータをイネーブルにした場合、スタンバイ メンバは使用できません。すべてのメンバがアクティブです。このパラメータは、ブートストラップ設定には含まれておらず、制御ユニットからメンバーユニットに複製されます。

（注） スタティック ポート プライオリティを有効にすると、8 ノードではなく 16 ノードをクラスタに含めることができます。

- [ディレクタのローカリゼーション（Director-Localization）]：複数のデータセンターサイトがサポートされている Geo クラスタリングでは、クラスタ間のラウンドトリップ時間（RTT）の待機時間が DC 内よりも長くなります。この遅延は、VoIP メディアストリームなどのアプリケーションのパフォーマンスに影響します。4.13 以降、ディレクタのローカリゼーションを使用して、RTT 遅延とパフォーマンス ルックアップ メッセージの遅延を最小限に抑えます。このオプションを有効にすると、フローの所有者とディレクタが同じ DC サイトに配置されるため、フローの所有者のルックアップはローカル DC サイトで実行され、トラフィックが同じサイト内で競合します。

（注） ディレクタのローカリゼーションは、Cisco Firepower 2100 シリーズ、Firepower 4000 シリーズ、および Firepower 9000 シリーズ デバイスではサポートされていません。

- [サイト冗長性の有効化（Enable Site Redundancy）]：4.16 以降、サイトの障害からフローを保護するために、サイトの冗長性を有効にできます。サイトの冗長性は、制御ユニットでのみ有効にすることができ、クラスタグループのメンバーユニットに複製されます。接続バックアップオーナーがオーナーと同じサイトにある場合は、障害の発生しているサイトからフローを保護するために、追加のバックアップオーナーが別のサイトから選択されます。ディレクタ ローカリゼーションとサイトの冗長性は別々の機能です。そのうちの 1 つまたは両方を設定することができます。

（注） サイトの冗長性は、Cisco Firepower 2100 シリーズ、Firepower 4000 シリーズ、および Firepower 9000 シリーズ デバイスではサポートされていません。

ナビゲーション パス

[Advanced Interface Settings] ダイアログボックスは、[Interfaces] ページの下部にある [Advanced] ボタンをクリックすると開きます（5505 ASA 以外のデバイス、PIX 7.0 以降のデバイス、および FWSM）。また、ASA 5505 の [Ports] および [Interfaces] ページの [Interfaces] タブの下部にある [Advanced] ボタンをクリックすると開きます。

関連項目

- デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （43 ページ）

同じセキュリティ レベルを持つインターフェイス間のトラフィックのイネーブル化

この項で説明するように、シングルコンテキストのセキュリティデバイスに表示される高度なインターフェイス設定（PIX/ASA/FWSM） （110 ページ）ダイアログボックスには、[同じセキュリティレベルのインターフェイス間のトラフィック（Traffic between interfaces with the same security level）] ドロップダウンリストがあります。

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またはサブインターフェイスは、相互に通信できません。同じセキュリティ レベルのインターフェイス間で通信できるようにすると、次の利点が得られます。

- 101 より多い数の通信インターフェイスを設定できます。

インターフェイスごとに異なるレベルを使用し、同じセキュリティ レベルにインターフェイスを割り当てないようにすると、1 レベルにつき 1 つのインターフェイスしか設定できません（0 ～ 100）。

- アクセス リストを使用しないで、同じセキュリティ レベルのすべてのインターフェイス間でトラフィックを自由に通過させることができます。

（注） NAT 制御をイネーブルにしている場合、同じセキュリティ レベルのインターフェイス間で NAT を設定する必要はありません。

ステップ 1 [高度なインターフェイスの設定（Advanced Interface Settings）] ダイアログボックスで、このデバイスに [同じセキュリティ レベルのインターフェイス間のトラフィック（Traffic between interfaces with the same security level）] を処理させる方法を示すオプションを選択します。

- [無効（Disabled）]：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許可しません。
- [インターフェイス間（Inter-interface）]：同じセキュリティ レベルが設定されているインターフェイス間のトラフィック フローをイネーブルにします。このオプションをイネーブルにした場合、ファイアウォール デバイス内のインターフェイス間のトラフィック フローをイネーブルにするために変換ルールを定義する必要はありません。
- [インターフェイス内（Intra-interface）]：同じセキュリティ レベルが設定されているサブインターフェイス間のトラフィック フローをイネーブルにします。このオプションをイネーブルにした場合、インターフェイスに割り当てられているサブインターフェイス間のトラフィック フローをイネーブルにするために変換ルールを定義する必要はありません。
- [両方（Both）]：同じセキュリティ レベルのインターフェイスおよびサブインターフェイスで、インターフェイス内およびインターフェイス間の両方の通信を許可します。

ステップ 2 高度なインターフェイス設定（PIX/ASA/FWSM） （110 ページ）の設定に進むか、または [OK] をクリックして [Advanced Interface Settings] ダイアログボックスを閉じます。

PPPoE ユーザ リストの管理

Point-to-Point Protocol over Ethernet（PPPoE）では、デバイス上のイーサネット インターフェイスを介して、セキュリティ デバイスと外部 ISP 間で標準の PPP 通信を実行できます。通信リンクを確立するには、デバイスで認証クレデンシャルを提供して、ネットワーク パラメータを取得する必要があります。これは、Virtual Private Dialup Network（VPDN; バーチャル プライ

ベート ダイヤルアップ ネットワーク）グループを使用することで実行されます。VPDN グループは、基本的には既定の PPPoE ユーザ クレデンシャル（ユーザ名およびパスワードなど）と認証プロトコルで構成されます。VPDN グループの詳細については、VPDN グループの管理（114 ページ）を参照してください。

VPDN グループで使用できる PPPoE ユーザのクレデンシャルは、[PPPoE Users] ダイアログボックスに保持されます。このダイアログボックスには、高度なインターフェイス設定（PIX/ASA/FWSM）（110 ページ）ダイアログボックスおよび [Add VPND Group] または [Edit VPND Group] ダイアログボックスからアクセスできます。

PPPoE ユーザの追加と編集

[PPPoE Users] ダイアログボックスには、標準の [Add Row]、[Edit Row]、および [Delete Row] ボタンとともに、現在定義されている PPPoE ユーザのテーブルが表示されます。[Add Row] ボタンをクリックすると [Add PPPoE User] ダイアログボックスが開き、[Edit Row] ボタンをクリックすると、実質的に同一の [Edit PPPoE User] ダイアログボックスが開きます。

次の PPPoE ユーザ パラメータを入力または編集してから、[OK] をクリックして [Add PPPoE User] または [Edit PPPoE User] ダイアログボックスを閉じ、[AdvancedInterface Settings] ダイアログボックスに戻ります。

（注） PPPoE ユーザ オプションは、Firewall Service Modules（FWSM; ファイアウォール サービス モジュール）では使用できません。

フィールド リファレンス

表 *22 : [Add PPPoE User]/[Edit PPPoE User]* ダイアログボックス

要素	説明
[ユーザー名（Username）]	このユーザーアカウントに割り当てられる名前。通常、外部 ISP によって提供されます。
パスワード	このユーザアカウントに割り当てられるパスワード。通常、外部 ISP によって提供されます。
確認（Confirm）	パスワードを再入力します。
Store Username and Password in Local Flash	オンにすると、この PPPoE ユーザ情報は、間違って上書きされないように、デバイスのローカルフラッシュメモリに保存されます。

VPDN グループの管理

Virtual Private Dialup Network（VPDN; バーチャル プライベート ダイヤルアップ ネットワーク）グループ（基本的には、既定の PPPoE ユーザと認証プロトコル）は、PPPoE 通信リンクを確

立してネットワーク パラメータを取得することを目的として、セキュリティ デバイスが外部 ISP にアクセスし、自分自身を認証するために使用します（PPPoE ユーザを確立する方法の詳細については、 PPPoE ユーザ リストの管理 （113 ページ）を参照してください）。

使用可能な VPDN グループが [Advanced Interface Settings] ダイアログボックスに保持されます。このダイアログボックスは、高度なインターフェイス設定（PIX/ASA/FWSM） （110 ページ）の説明に従って、[Interfaces] ページの下部にある [Advanced] ボタンをクリックすると開きます。

VPND グループの追加または編集

[Advanced Interface Settings] ダイアログボックスには、現在定義されている VPDN グループのテーブルと、標準の [Add Row]、[Edit Row]、および [Delete Row] ボタンがあります。[Add Row] ボタンをクリックすると [Add VPDN Group] ダイアログボックスが開き、[Edit Row] ボタンをクリックすると、実質的に同一の [Edit VPDN Group] ダイアログボックスが開きます。

次の PPPoE グループ パラメータを入力または編集してから、[OK] をクリックして [Add VPDN Group] または [Edit VPDN Group] ダイアログボックスを閉じ、[AdvancedInterface Settings] ダイアログボックスに戻ります。

（注） VPDN グループ オプションは、Firewall Service Modules（FWSM; ファイアウォール サービス モジュール）では使用できません。

フィールド リファレンス

表 *23 : [Add VPND Group]/[Edit VPND Group]* ダイアログボックス

要素	説明
グループ名（Group Name）	このグループを Security Manager 内で識別する最大 63 文字の名前。
PPPoE Username	このグループが ISP との認証に使用する PPPoE クレデンシャルを識別する名前。使用可能な PPPoE ユーザのリストから選択します。 このリストから [ユーザの編集（Edit User）] を選択して、[PPPoEユーザ（PPPoE Users）] ダイアログボックスを開きます。このダイアログボックスでは、このオプションのユーザを追加または編集できます。ユーザの作成および編集の詳細については、PPPoE ユーザ リストの管理 （113 ページ）を参照してください。

要素	説明
PPP Authentication	PPP 認証方式を選択します。 • [PAP]：パスワード認証プロトコル。クリアテキストでクレデンシャルを交換します。 • [CHAP]：チャレンジ ハンドシェイク認証プロトコル。暗号化されたクレデンシャルを交換します。 • [MSCHAP]：Microsoft 社の CHAP。バージョン 1 だけです。

VXLAN

仮想拡張 LAN（VXLAN）は、レイヤ 3 物理ネットワークの上のレイヤ 2 仮想ネットワークとして機能し、レイヤ 2 ネットワークを拡張します。VXLAN は、VLAN の場合と同じイーサネットレイヤ2ネットワークサービスを提供しますが、より優れた拡張性と柔軟性を備えています。VLAN と比較して、VXLAN には次の利点があります。

- データセンター全体でのマルチテナントセグメントの柔軟な配置。
- より多くのレイヤ 2 セグメント（最大 1,600 万の VXLAN セグメント）に対応するための高度なスケーラビリティ。

バージョン 4.9 以降、Security Manager は、バージョン 9.4(1) 以降の ASA、ASAv、および ASASM デバイスの VXLAN をサポートします。

（注） VxLAN は FWSM デバイスではサポートされていません。

VXLAN を設定するには、次の手順を実行します。

1. VXLAN ポリシーの設定 （116 ページ）
2. VNI インターフェイスの設定 （20 ページ）を作成し、設定された VXLAN ポリシーを VNI インターフェイスに関連付けます。

VXLAN ポリシーの設定

VXLAN を構成するには、最初に VXLAN ポリシーを設定してから VNI インターフェイスを作成し、設定された VXLAN ポリシーを VNI インターフェイスに関連付ける必要があります。ここでは、VXLAN ポリシーの設定方法について説明します。

ナビゲーション パス

VXLANページにアクセスするには、[デバイスビュー（Device View）]に移動し、ASA、ASAv、またはASASMデバイスを選択して、[ポリシー（Policies）]から[VxLAN]をクリックします。

関連項目

- VXLAN （116 ページ）
- VNI インターフェイスの設定 （20 ページ）

フィールド リファレンス

表 *24 : VxLAN*

要素	説明
VXLAN ポート番号の有効化 VxLAN 宛先ポート	[VXLAN宛先ポート（VXLAN Destination Port）] の値をデフォルト 4789 から変更する場合は、このチェックボックスをオンにします。オンにした場合、1024 ～ 65535 の範囲の数値を入力します。
ネットワーク仮想化エンドポイント（NVE）	
NVE の有効化	選択すると、VTEP トンネルインターフェイスを選択できます。
VXLAN NVE 番号	VXLAN NVE 番号の値は「1」です。この値は編集できません。
VxLan NVE または GENEVE カプセル化の有効化	[NVEカプセル化の有効化（Enable NVE Encapsulation）]：VXLANを使用してNVEカプセル化を有効にするには、このチェックボックスをオンにします。 [Geneveカプセル化の有効化（Enable Geneve Encapsulation）]：VXLANを使用してGeneveカプセル化を有効にするには、このオプションを選択します。
VTEP トンネルインターフェイス	[選択（Select）]をクリックして、VTEP トンネルインターフェイスを選択します。

要素	説明
VTEP IP アドレスまたはマルチキャスト トラフィック アドレスの有効化	次のいずれかを選択します。 • [ピアVTEP IPアドレス（Peer VTEP IP Address）]：ピア VTEP IP アドレスを手動で指定します。ピア IP アドレスを指定した場合、マルチキャスト グループ ディスカバリは使用できません。マルチキャストは、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。VTEPには1つのピアのみを指定できます。ピア VTEP IP アドレスは VTEP トンネルインターフェイスから到達可能である必要があることに注意してください。そうでない場合、展開は失敗します。VXLAN ポリシーでピア IP アドレスを使用した場合、VNIインターフェイスを含む[インターフェイス（Interface）] ページでマルチキャスト IP アドレスを設定することはできません。 • [デフォルトマルチキャストIPアドレス（Default Multicast IP Address）]：関連するすべての VNI インターフェイスのデフォルト マルチキャスト グループを指定します。IP アドレスの有効な範囲は 224.0.0.0 ～ 239.255.255.255 です。VNI インターフェイスごとにマルチキャスト グループを設定していない場合は、このグループが使用されます。その VNI インターフェイス レベルでグループを設定している場合は、そのグループがこの設定よりも優先されます。 • [Geneveポート番号の有効化（Enable Geneve Port Number）]：Geneve 宛先ポートの値を変更するには、このチェックボックスをオンにします。デフォルト値は 6081 です。1024 ～ 65535 の数値を入力します。 （注） デフォルトのポート番号 6081 の場合、CSM はデルタ設定を構築しません。
保存	[保存（Save）]をクリックして、VXLAN 設定を保存します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。