

Firepower 1010 スイッチポートの基本インターフェイス構成

Firepower 1010220/ の各インターフェイスは、通常のファイアウォール インターフェイスとしてまたはレイヤ2ハードウェアスイッチポートとして実行するように構成できます。この章では、スイッチモードの有効化と無効化、VLANインターフェイスの作成、そのインターフェイスのスイッチポートへの割り当てなど、スイッチポート設定を開始するためのタスクについて説明します。また、サポート対象のインターフェイスで Power on Ethernet（PoE）をカスタマイズする方法についても説明します。

- スイッチポートについて （1 ページ）
- スイッチポートの前提条件 （3 ページ）
- スイッチポートのガイドライン （3 ページ）
- スイッチポートと Power over Ethernet の設定 （5 ページ）
- スイッチポートのモニタリング （10 ページ）
- スイッチポートの履歴 （11 ページ）

スイッチポートについて

この項では、レイヤ 2 スイッチを搭載したモデルのスイッチポートについて説明します。

スイッチポートおよびインターフェイス

スイッチポートとファイアウォールは異なるOSI レイヤで動作して、通信転送を処理します。

ポートおよびインターフェイスのタイプ

物理インターフェイスごとに、その動作をファイアウォールインターフェイスまたはスイッチポートとして設定できます。次の情報は、物理インターフェイスとポートタイプ、およびスイッチポートを割り当てる論理 VLAN インターフェイスについて説明するものです。

- 物理ファイアウォールインターフェイス：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インターフェイス間でトラフィックを転送するブリッジグループメンバーです。ルーテッドモードでは、一部のインターフェイスでブリッジグループメンバーとして、その他のインターフェイスでレイヤ3インターフェイスとして、統合ルーティングおよびブリッジングを使用することもできます。デフォルトでは、イーサネット 1/1 インターフェイスはファイアウォール インターフェイスとして設定されます。

- 物理スイッチポート：スイッチポートは、ハードウェアのスイッチ機能を使用して、レイヤ 2 でトラフィックを転送します。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。トラフィックには、ASA セキュリティポリシーは適用されません。アクセスポートはタグなしトラフィックのみを受け入れ、単一のVLANに割り当てることができます。トランクポートはタグなしおよびタグ付きトラフィックを受け入れ、複数の VLAN に属することができます。デフォルトでは、イーサネット 1/2 以降のポートは VLAN 1 のアクセススイッチポートとして構成されています。Management インターフェイスをスイッチポートとして設定することはできません。
- 論理 VLAN インターフェイス：これらのインターフェイスは物理ファイアウォール インターフェイスと同じように動作しますが、サブインターフェイス、またはEtherChannelインターフェイスを作成できないという例外があります。スイッチポートが別のネットワークと通信する必要がある場合、ASA デバイスは VLAN インターフェイスにセキュリティポリシーを適用し、別の論理 VLAN インターフェイスまたはファイアウォール インターフェイスにルーティングします。ブリッジグループメンバーとして VLAN インターフェイスで統合ルーティングおよびブリッジングを使用することもできます。同じ VLAN 上のスイッチポート間のトラフィックに ASA セキュリティポリシーは適用されませんが、ブリッジグループ内の VLAN 間のトラフィックにはセキュリティポリシーが適用されるため、ブリッジグループとスイッチポートを階層化して特定のセグメント間にセキュリティポリシーを適用できます。

Power Over Ethernet

PoE は、IEEE 802.3af（PoE）および 802.3at（PoE+）を使用する Ethernet 1/7 および Ethernet 1/8 で、ポートあたり最大 30 ワットまで使用できます。

PoE + では、Link Layer Discovery Protocol（LLDP）を使用して、電力レベルをネゴシエートします。電力は必要なときのみ供給されます。

インターフェイスをシャットダウンすると、デバイスへの給電が無効になります。

Auto-MDI/MDIX 機能

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。

Auto-MDI/MDIX 設定の詳細

すべてのスイッチポートで、デフォルトの自動ネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。速度またはデュプレックスがオートネゴシエーションに設定されている場合、インターフェイスで Auto-MDI/MDIX が有効になります。速度とデュプレックスの両方に固定値を指定すると、オートネゴシエーションが無効にされ、Auto-MDI/MDIX も無効になります。速度とデュプレックスを 1000 およびフルに設定すると、インターフェイスは常にオートネゴシエーションを行います。この状態では Auto-MDI/MDIX が有効になり、無効にすることはできません。

スイッチポートの前提条件

このリファレンスは、スイッチポートのモデルサポートおよびその他の前提条件を示します。

モデルのサポート

- Firepower 1010

スイッチポートのガイドライン

コンテキストモードの制限事項

マルチコンテキストモードは、Secure Firewall 1210/1220 という特定の例外を除き、複数のファイアウォールモデルではサポートされていません。

- Firepower 1010 はマルチ コンテキスト モードをサポートしません。
- Cisco Secure Firewall 1210/1220 はマルチコンテキストモードをサポートしません。

フェイルオーバー およびクラスタリングの制限事項

スイッチポートはハードウェアで動作し、アクティブユニットとスタンバイユニットの両方で通信を渡し続けるため、フェイルオーバーを使用している場合はスイッチポート機能を使用しないでください。

- クラスタはサポートされません。
- アクティブ/スタンバイのフェールオーバーのみサポートされます。
- スイッチポートはハードウェアで動作するため、アクティブユニットとスタンバイユニットの両方でトラフィックを通過させ続けます。フェイルオーバーは、トラフィックがスタンバイユニットを通過するのを防ぐように設計されていますが、この機能はスイッチポートには拡張されていません。通常の フェイルオーバー のネットワーク設定では、両方のユニットのアクティブなスイッチ ポートがネットワーク ループにつながります。スイッチング機能には外部スイッチを使用することをお勧めします。VLANインターフェイスはフェールオーバーによってモニターできますが、スイッチポートはモニターできません。

理論的には、1 つのスイッチ ポートを VLAN に配置して、フェイルオーバー を正常に使用することができますが、代わりに物理ファイアウォールインターフェイスを使用する設定の方が簡単です。

- ファイアウォールインターフェイスはフェールオーバーリンクとしてのみ使用できます。

論理 VLAN インターフェイス（SVI）の設定要件

競合を防ぐため、ファイアウォールインターフェイスの論理VLANインターフェイスとVLANサブインターフェイスとの間に一意の VLAN ID を設定してください。

- また、ファイアウォール インターフェイスで VLAN サブインターフェイスを使用する場合、論理 VLAN インターフェイスと同じ VLAN ID は使用できません。
- MAC アドレス：
  - ルーテッド ファイアウォール モード：すべての VLAN インターフェイスが 1 つの MAC アドレスを共有します。接続スイッチがどれもこのシナリオをサポートできるようにします。接続スイッチに固有の MAC アドレスが必要な場合、手動で MAC アドレスを割り当てることができます。手動 MAC アドレス、MTU、および TCP MSS の設定 を参照してください。
  - トランスペアレント ファイアウォール モード：各 VLAN インターフェイスに固有の MAC アドレスがあります。必要に応じて、手動で MAC アドレスを割り当てて、生成された MAC アドレスを上書きできます。手動 MAC アドレス、MTU、および TCP MSS の設定を参照してください。

ブリッジグループの制限事項

同じブリッジ グループ内に論理 VLAN インターフェイスと物理ファイアウォール インターフェイスを混在させることはできません。

VLANインターフェイスおよびスイッチポートでサポートされていない機能

VLAN インターフェイスおよびスイッチポートは、次の機能をサポートしていません。

- ダイナミック ルーティング
- マルチキャスト ルーティング
- ポリシーベース ルーティング
- 等コストマルチパス（ECMP）ルーティング
- VXLAN
- EtherChannel：スイッチのポートを EtherChannel の一部にはできません。PoE も、EtherChannel のポートではサポートされません。
- フェールオーバーおよびステートリンク

- トラフィック ゾーン
- セキュリティグループタグ（SGT）

その他のガイドラインと制限事項

最大 60 個の名前付きインターフェイスを設定し、Management インターフェイスがスイッチポートとして設定されていないことを確認します。

デフォルト設定

各ファイアウォールモデルのデフォルトのインターフェイス割り当てを把握して、設定を適切に計画してください。

- イーサネット 1/1 はファイアウォール インターフェイスです。
- イーサネット 1/2 ～ 1/8 が、VLAN 1 に割り当てられたスイッチポートです。
- デフォルトの速度とデュプレックス：デフォルトでは、速度とデュプレックスは自動ネゴシエーションに設定されます。

スイッチポートと Power over Ethernet の設定

スイッチ ポートおよび PoE を設定するには、次のタスクを実行します。

VLAN インターフェイスの設定

ここでは、関連付けられたスイッチポートで使用するための VLAN インターフェイス（SVI）の構成方法について説明します。スイッチポートを関連付けられた最大 60 個の VLAN インターフェイスを作成できます。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** を選択し、**[Add]** > **[VLAN Interface]** を選択します。

ステップ 2 [VLAN ID] フィールドに、このインターフェイスの VLAN ID を 1 ー 4070 の範囲で入力します。ただし、内部使用のために予約されている 3968 ー 4047 の範囲の ID は除きます。

ステップ 3 （任意） [Block Traffic From this Interface to] ドロップダウンリストで、この VLAN インターフェイスがトラフィックを開始できない VLAN を選択します。

たとえば、1 つの VLAN をインターネット アクセスの外部に、もう 1 つを内部ビジネス ネットワーク内に、そして 3 つ目をホーム ネットワークにそれぞれ割り当てます。ホームネットワークはビジネスネットワークにアクセスする必要がないので、ホーム VLAN で [Block Traffic From this Interface to] オプションを使用できます。ビジネスネットワークはホームネットワークにアクセスできますが、その反対はできません。

ステップ 4 [OK] をクリックします。

ステップ 5 [Apply] をクリックします。

スイッチポートのアクセスポートとしての構成

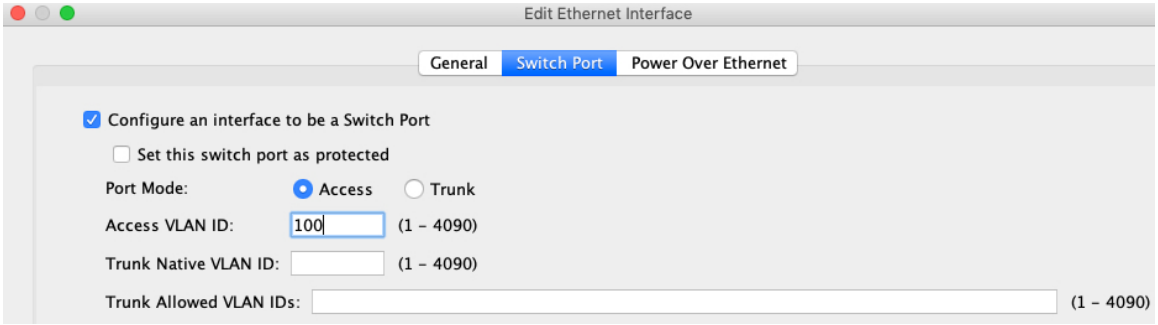
1 つの VLAN にスイッチ ポートを割り当てるには、アクセス ポートとして設定します。アクセスポートは、タグなしのトラフィックのみを受け入れます。デフォルトでは、イーサネット 1/2 ～ イーサネット 1/8 スイッチポートが有効になっており、VLAN 1 に割り当てられています。

（注） デバイスは、ネットワーク内のループ検出に使用されるスパニングツリープロトコルをサポートしていません。したがって、ASA との接続はいずれもネットワークループ内で終わらないようにする必要があります。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** を選択し、編集するインターフェイスを選択して [Edit] をクリックします。

ステップ 2 [Switch Port] をクリックします。



ステップ 3 [Configure an interface to be a Switch Port] チェックボックスをオンにします。

ステップ 4 （任意） [Set this switch port as protected] チェックボックスをオンにして、スイッチポートが同じ VLAN 上の他の保護されたスイッチポートと通信するのを防ぎます。

スイッチ ポート上のデバイスが主に他の VLAN からアクセスされる場合、VLAN 内アクセスを許可する必要がない場合、および感染やその他のセキュリティ侵害に備えてデバイスを相互に分離する場合に、スイッチ ポートが相互に通信しないようにします。たとえば、3 つの Web サーバーをホストする DMZ がある場合、各スイッチポートに [Set this switch port as protected] オプションを適用すると、Web サーバーを相互に分離できます。内部ネットワークと外部ネットワークはいずれも 3 つの Web サーバーすべてと通信でき、その逆も可能ですが、Web サーバーは相互に通信できません。

ステップ 5 [Port Mode] の場合は、[Access] オプションボタンをクリックします。

ステップ 6 このスイッチポートに関連付けられている [Access VLAN ID] を 1 ～ 4070 の範囲で入力します。

デフォルトは VLAN 1 です。

ステップ 7 [General] をクリックします。

ステップ 8 [Enable Interface] をオンにします。

（注） [General] ページのその他のフィールド（[Interface Name] など）は、スイッチポートには適用されません。

ステップ 9 （任意） ハードウェアのプロパティを設定します。

a) [Configure Hardware Properties] をクリックします。

b) [Duplex] を選択します。

デフォルトは [自動（Auto）] です。

c) [Speed] を選択します。

デフォルトは [自動（Auto）] です。

d) [OK] をクリックします。

ステップ 10 [OK] をクリックします。

ステップ 11 [Apply] をクリックします。

スイッチポートのトランクポートとしての設定

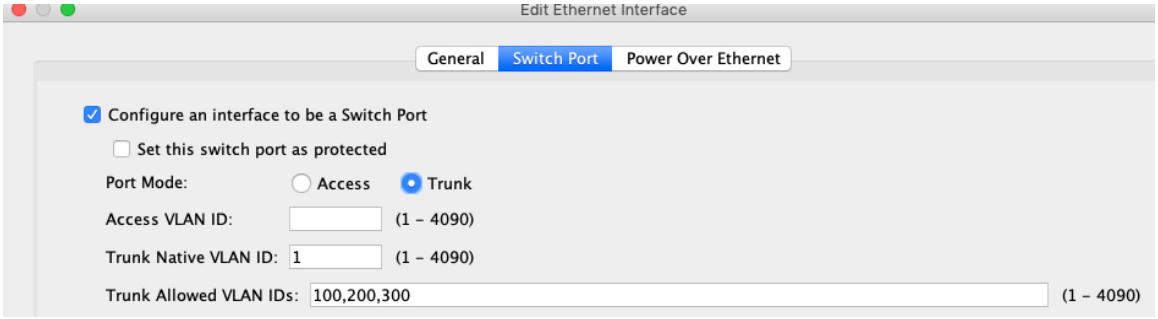
この手順では、802.1Q タグ付けを使用して複数の VLAN を伝送するトランク ポートの作成方法について説明します。トランクポートは、タグなしトラフィックとタグ付きトラフィックを受け入れます。許可された VLAN のトラフィックは、トランクポートを変更せずに通過します。

トランクは、タグなしトラフィックを受信すると、そのトラフィックをネイティブ VLAN ID にタグ付けして、ASA が正しいスイッチポートにトラフィックを転送したり、別のファイアウォールインターフェイスにルーティングしたりできるようにします。ASA は、トランクポートからネイティブ VLAN ID トラフィックを送信する際に VLAN タグを削除します。タグなしトラフィックが同じ VLAN にタグ付けされるように、他のスイッチのトランク ポートに同じネイティブ VLAN を設定してください。

手順

ステップ 1 **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** を選択し、編集するインターフェイスを選択して [Edit] をクリックします。

ステップ 2 [Switch Port] をクリックします。



ステップ 3 [Configure an interface to be a Switch Port] チェックボックスをオンにします。

ステップ 4 （任意） [Set this switch port as protected] チェックボックスをオンにして、スイッチポートが同じ VLAN 上の他の保護されたスイッチポートと通信するのを防ぎます。

スイッチ ポート上のデバイスが主に他の VLAN からアクセスされる場合、VLAN 内アクセスを許可する必要がない場合、および感染やその他のセキュリティ侵害に備えてデバイスを相互に分離する場合に、スイッチ ポートが相互に通信しないようにします。たとえば、3 つの Web サーバーをホストする DMZ がある場合、各スイッチポートに [Set this switch port as protected] オプションを適用すると、Web サーバーを相互に分離できます。内部ネットワークと外部ネットワークはいずれも 3 つの Web サーバーすべてと通信でき、その逆も可能ですが、Web サーバーは相互に通信できません。

ステップ 5 [Port Mode] の場合は、[Trunk] オプションボタンをクリックします。

ステップ 6 [Trunk Native VLAN ID] を 1 ～ 4070 の範囲で入力します。デフォルトは VLAN 1 です。

各ポートのネイティブ VLAN は 1 つのみですが、すべてのポートに同じネイティブ VLAN または異なるネイティブ VLAN を使用できます。

ステップ 7 このスイッチポートに関連付けられている [Trunk Allowed VLAN IDs] を 1 ～ 4070 の範囲で入力します。

このフィールドにネイティブ VLAN を含めても無視されます。トランク ポートは、ネイティブ VLAN トラフィックをポートから送信するときに、常に VLAN タグを削除します。また、まだネイティブ VLAN タグが付いているトラフィックを受信しません。

ステップ 8 [General] をクリックします。

ステップ 9 [Enable Interface] をオンにします。

（注） [General] ページのその他のフィールド（[Interface Name] など）は、スイッチポートには適用されません。

ステップ 10 （任意） ハードウェアのプロパティを設定します。

a) [Configure Hardware Properties] をクリックします。
b) [Duplex] を選択します。

デフォルトは [自動（Auto）] です。

c) [Speed] を選択します。

デフォルトは [自動（Auto）] です。

d) [OK] をクリックします。

ステップ 11 [OK] をクリックします。

ステップ 12 [Apply] をクリックします。

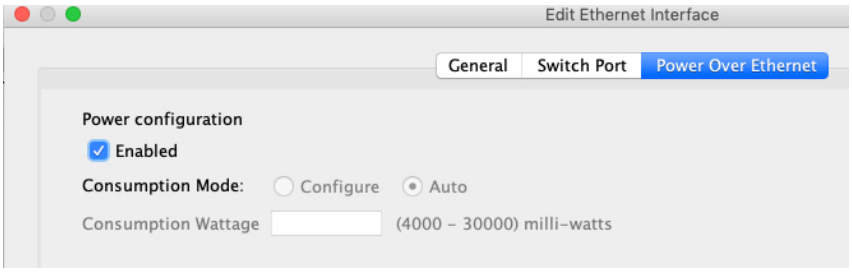
Power over Ethernet の設定

Power over Ethernet（PoE）ポートは、IP 電話や無線アクセスポイントなどのデバイスに電力を供給します。PoE はデフォルトでイネーブルです。この手順では、PoE を無効および有効にする方法と、オプションパラメータを設定する方法について説明します。

手順

ステップ 1 **[設定（Configuration）]>[デバイス設定（Device Setup）]>[インターフェイス設定（Interface Settings）]>[インターフェイス（Interfaces）]** を選択し、編集するインターフェイスを選択して [編集（Edit）] をクリックします。

ステップ 2 [Power Over Ethernet] をクリックします。



ステップ 3 [Enabled] をオンにします。

ステップ 4 [Consumption Mode] で、[Configure] または [Auto] オプションボタンをクリックします。

- [Auto]：給電先デバイスのクラスに適したワット数を使用して、給電先デバイスに自動的に電力を供給します。ファイアウォールはLLDPを使用して、さらに適切なワット数をネゴシエートします。
- [設定（Configure）]：[消費ワット数（Consumption Wattage）] フィールドに、ミリワット単位でワット数を手動で入力します（4,000 ～ 30,000の範囲で指定可能）。ワット数を手動で設定し、LLDP ネゴシエーションを無効にする場合は、このコマンドを使用します。

ステップ 5 [OK] をクリックします。

ステップ 6 [Apply] をクリックします。

ステップ 7 **[モニター（Monitor）]** > **[インターフェイス（Interfaces）]** > **[Power Over Ethernet]** を選択して、現在の PoE ステータスを表示します。

スイッチポートのモニタリング

- **[Monitoring]** > **[Interfaces]** > **[ARP Table]**

  スタティック エントリやダイナミック エントリを含む ARP テーブルを表示します。ARP テーブルには、MAC アドレスを所定のインターフェイスの IP アドレスにマッピングするエントリが含まれます。

- **[Monitoring]** > **[Interfaces]** > **[MAC Address Table]**

  スタティックおよびダイナミック MAC アドレス エントリを表示します。

- **[Monitoring]** > **[Interfaces]** > **[Interface Graphs]**

  インターフェイスの統計情報をグラフ形式またはテーブル形式で表示できます。

- **[Monitoring]** > **[Interfaces]** > **[L2 Switching]**

  VLAN とスイッチポートの関連付けおよびスタティックおよびダイナミック MAC アドレスエントリを表示します。

- **[Monitoring]** > **[Interfaces]** > **[Power Over Ethernet]**

  PoE+ ステータスを表示します。

スイッチポートの履歴

表 *1:* スイッチポートの履歴

機能名	バージョン	機能情報
Firepower 1010 ハードウェア スイッチのサポート	9.13(1)	Firepower 1010 では、各イーサネット インターフェイスをスイッチ ポートまたはファイアウォール インターフェイスとして設定できます。 新しい/変更された画面： • **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** > **[Edit]** > **[Switch Port]** • **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** > **[Add VLAN Interface]** • **[Monitoring]** > **[Interfaces]** > **[L2 Switching]**
イーサネット 1/7 およびイーサネット 1/8 での Firepower 1010 PoE+ のサポート	9.13(1)	Firepower 1010 は、イーサネット 1/7 およびイーサネット 1/8 での Power over Ethernet+（PoE+） をサポートしています。 新しい/変更された画面： • **[Configuration]** > **[Device Setup]** > **[Interface Settings]** > **[Interfaces]** > **[Edit]** > **[Power Over Ethernet]** • **[Monitoring]** > **[Interfaces]** > **[Power Over Ethernet]**

スイッチポートの履歴

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。

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。

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。