



CHAPTER 12

インターフェイス コンフィギュレーションの開始 (ASA 5505)

この章では、VLAN インターフェイスを作成してスイッチ ポートに割り当てる方法など、ASA 5505 のインターフェイス コンフィギュレーションを開始するためのタスクについて説明します。

ASA 5510 以降のコンフィギュレーションについては、「[ASA 5505 インターフェイスの機能履歴](#) (P.12-14) を参照してください。

この章の内容は、次のとおりです。

- 「[ASA 5505 インターフェイスについて](#)」 (P.12-1)
- 「[ASA 5505 インターフェイスのライセンス要件](#)」 (P.12-5)
- 「[注意事項と制限事項](#)」 (P.12-5)
- 「[デフォルト設定](#)」 (P.12-5)
- 「[ASA 5505 インターフェイス コンフィギュレーションの開始](#)」 (P.12-6)
- 「[インターフェイスのモニタリング](#)」 (P.12-11)
- 「[ASA 5505 インターフェイスの設定例](#)」 (P.12-11)
- 「[次の作業](#)」 (P.12-13)
- 「[ASA 5505 インターフェイスの機能履歴](#)」 (P.12-14)

ASA 5505 インターフェイスについて

この項では、ASA 5505 のポートおよびインターフェイスについて説明します。次の項目を取り上げます。

- 「[ASA 5505 のポートおよびインターフェイスについて](#)」 (P.12-2)
- 「[ライセンスで使用できる最大アクティブ VLAN インターフェイス数](#)」 (P.12-2)
- 「[VLAN MAC アドレス](#)」 (P.12-4)
- 「[Power Over Ethernet](#)」 (P.12-4)
- 「[SPAN を使用したトラフィックのモニタリング](#)」 (P.12-4)
- 「[Auto-MDI/MDIX 機能](#)」 (P.12-4)

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サポートしています。次の 2 種類のポートおよびインターフェイスを設定する必要があります。

- 物理スイッチ ポート：ASA には 8 個のファストイーサネット スイッチ ポートがあり、これら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。これらのポートのうちの 2 つは PoE ポートです。詳細については、「[Power Over Ethernet](#)」(P.12-4) を参照してください。これらのインターフェイスを、PC、IP 電話、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。最大 VLAN インターフェイス数の詳細については、「[ライセンスで使用できる最大アクティブ VLAN インターフェイス数](#)」を参照してください。VLAN インターフェイスを使用することにより、別々の VLAN、たとえばホーム VLAN、ビジネス VLAN、インターネット VLAN などに装置を分けることができます。

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、VLAN 1 のスイッチ ポートが VLAN 2 のスイッチ ポートと通信する場合、ASA は、セキュリティ ポリシーを 2 つの VLAN 間のトラフィックとルートまたはブリッジに適用します。

ライセンスで使用できる最大アクティブ VLAN インターフェイス数

ルーテッド モードでは、ライセンスに応じて次の VLAN を設定できます。

- 基本ライセンス：3 つのアクティブ VLAN。3 つ目の VLAN は、別の VLAN へのトラフィックを開始する目的に限り設定できます。詳細については、[図 12-1](#) を参照してください。
- Security Plus ライセンス：20 個のアクティブ VLAN。

トランスペアレント ファイアウォール モードでは、ライセンスに応じて次の VLAN を設定できます。

- 基本ライセンス：1 つのブリッジ グループ内の 2 つのアクティブ VLAN。
- Security Plus ライセンス：3 つのアクティブ VLAN、1 つのブリッジ グループ内の 2 つのアクティブ VLAN、およびフェールオーバー リンクの 1 つのアクティブ VLAN。

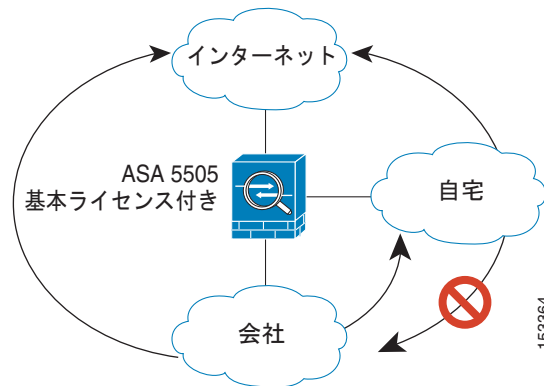


(注)

アクティブ VLAN とは、`nameif` コマンドが設定された VLAN のことです。

ルーテッドモードの基本ライセンスの場合、3 つ目の VLAN は、別の VLAN へのトラフィックを開始する目的に限り設定できます。図 12-1 のネットワークの例では、ホーム VLAN はインターネットと通信できますが、ビジネス VLAN とは接続を開始できません。

図 12-1 基本ライセンスでの ASA 5505



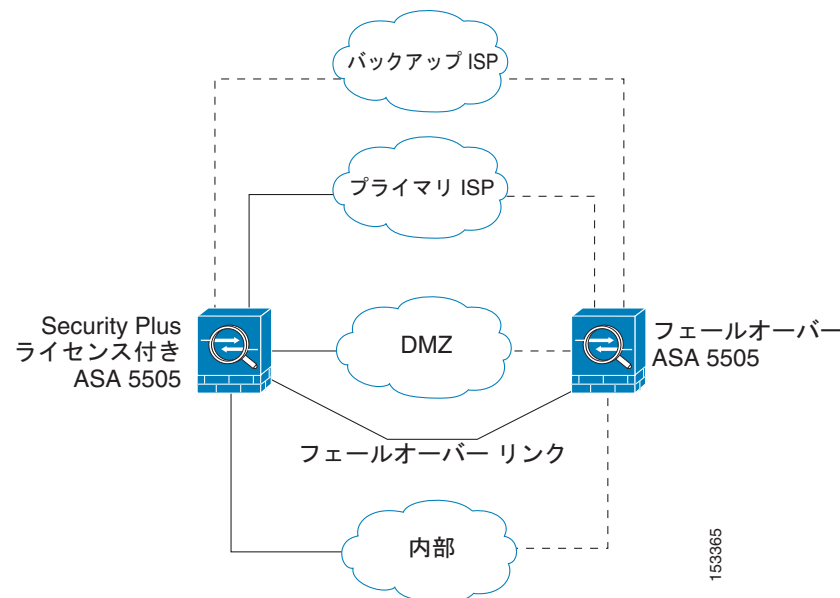
Security Plus ライセンスでは、ルーテッドモードの 20 個の VLAN インターフェイスを設定できます。これには、フェールオーバー用の VLAN インターフェイスと、ISP へのバックアップリンクとしての VLAN インターフェイスも含まれます。バックアップ インターフェイスは、プライマリ インターフェイス経由のルートで障害が発生しない限り、トラフィックを通過させないように設定できます。トランクポートを設定して、1 つのポートで複数の VLAN を使用できます。



(注) ASA 5505 は、アクティブ/スタンバイ フェールオーバーをサポートしていますが、ステートフル フェールオーバーはサポートしていません。

ネットワークの例については、図 12-2 を参照してください。

図 12-2 Security Plus ライセンスでの ASA 5505



VLAN 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 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。「[MAC アドレスおよび MTU の設定](#)」(P.13-10) 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 に固有の MAC アドレスが割り当てられます。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。「[MAC アドレスおよび MTU の設定](#)」(P.14-14) を参照してください。

Power Over Ethernet

Ethernet 0/6 および Ethernet 0/7 は、IP 電話や無線アクセス ポイントなどのデバイス用に PoE をサポートしています。非 PoE デバイスをインストールした場合やこれらのスイッチ ポートに接続しない場合、ASA はスイッチ ポートに電源を供給しません。

shutdown コマンドを使用してスイッチ ポートをシャットダウンすると、デバイスへの電源がディセーブルになります。**no shutdown** コマンドを使用してポートをイネーブルにすると、電源が復元します。スイッチ ポートのシャットダウンの詳細については、「[スイッチ ポートのアクセス ポートとしての設定とイネーブル化](#)」(P.12-7) を参照してください。

接続されているデバイスのタイプ (Cisco または IEEE 802.3af) など、PoE スイッチ ポートのステータスを確認するには、**show power inline** コマンドを使用します。

SPAN を使用したトラフィックのモニタリング

1 つまたは複数のスイッチ ポートを出入りするトラフィックをモニタするには、スイッチ ポートモニタリングとも呼ばれる SPAN をイネーブルにします。SPAN をイネーブルにしたポート (宛先ポートと呼ばれる) は、特定の送信元ポートで送受信するすべてのパケットのコピーを受信します。SPAN 機能を使用すれば、スニファを宛先ポートに添付して、すべてのトラフィックをモニタできます。SPAN を使用しないと、モニタするポートごとにスニファを添付しなければなりません。SPAN をイネーブルにすることができるのは、1 つの宛先ポートのみです。

詳細については、コマンドリファレンスの **switchport monitor** コマンドを参照してください。

Auto-MDI/MDIX 機能

すべての ASA 5505 インターフェイスには、Auto-MDI/MDIX 機能が含まれています。

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。Auto-MDI/MDIX はディセーブルにできません。

ASA 5505 インターフェイスのライセンス要件

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

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

注意事項と制限事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

ASA 5505 はマルチ コンテキスト モードをサポートしません。

ファイアウォール モードのガイドライン

- トランスペアレント モードでは、最大 8 個のブリッジグループを設定できます。少なくとも 1 つのブリッジグループを使用しなければならないことに注意してください。データ インターフェイスはブリッジグループに属している必要があります。
- 各ブリッジグループには、最大 4 個の VLAN インターフェイスをライセンス制限まで含めることができます。

デフォルト設定

この項では、工場出荷時のデフォルト コンフィギュレーションが設定されていない場合のインターフェイスのデフォルト設定を示します。工場出荷時のデフォルト コンフィギュレーションについては、「[工場出荷時のデフォルト コンフィギュレーション](#)」(P.3-18) を参照してください。

インターフェイスのデフォルトの状態

インターフェイスには、次のデフォルト状態があります。

- スイッチ ポート : ディセーブル。
- VLAN : イネーブル。ただし、トラフィックが VLAN を通過するためには、スイッチ ポートもイネーブルになっている必要があります。

デフォルトの速度および二重通信

デフォルトでは、速度と二重通信はオートネゴシエーションに設定されています。

ASA 5505 インターフェイス コンフィギュレーションの開始

この項では、次のトピックについて取り上げます。

- 「[インターフェイス コンフィギュレーションを開始するためのタスク フロー](#)」 (P.12-6)
- 「[VLAN インターフェイスの設定](#)」 (P.12-6)
- 「[スイッチ ポートのアクセス ポートとしての設定とイネーブル化](#)」 (P.12-7)
- 「[スイッチ ポートのトランク ポートとしての設定とイネーブル化](#)」 (P.12-9)

インターフェイス コンフィギュレーションを開始するためのタスク フロー

シングル モードでインターフェイスを設定するには、次の手順を実行します。

-
- ステップ 1** VLAN インターフェイスを設定します。「[VLAN インターフェイスの設定](#)」 (P.12-6) を参照してください。
 - ステップ 2** スイッチ ポートをアクセス ポートとして設定し、イネーブルにします。「[スイッチ ポートのアクセス ポートとしての設定とイネーブル化](#)」 (P.12-7) を参照してください。
 - ステップ 3** (Security Plus ライセンスのオプション) スイッチ ポートをトランク ポートとして設定し、イネーブルにします。「[スイッチ ポートのトランク ポートとしての設定とイネーブル化](#)」 (P.12-9) を参照してください。
 - ステップ 4** 第 13 章「[インターフェイス コンフィギュレーションの実行 \(ルーテッド モード\)](#)」または第 14 章「[インターフェイス コンフィギュレーションの実行 \(トランスペアレント モード\)](#)」に従って、インターフェイス コンフィギュレーションを実行します。
-

VLAN インターフェイスの設定

この項では、VLAN インターフェイスを設定する方法について説明します。ASA 5505 のインターフェイスの詳細については、「[ASA 5505 インターフェイスについて](#)」 (P.12-1) を参照してください。

ガイドライン

インターフェイスをすべて設定してから Easy VPN をイネーブルにすることをお勧めします。

手順の詳細

コマンド	目的
<p>ステップ1 <code>interface vlan number</code></p> <p>例: hostname(config)# interface vlan 100</p>	<p>VLAN インターフェイスを追加します。<i>number</i> の範囲は 1 ~ 4090 です。</p> <p>この VLAN インターフェイスとすべての関連コンフィギュレーションを削除するには、no interface vlan コマンドを入力します。このインターフェイスには、インターフェイス名コンフィギュレーションも含まれており、名前は他のコマンドでも使用されているため、それらのコマンドも削除されます。</p>
<p>ステップ2 (基本ライセンスの場合は任意)</p> <p><code>no forward interface vlan number</code></p> <p>例: hostname(config-if)# no forward interface vlan 101</p>	<p>このインターフェイスを 3 つ目の VLAN とするために、このインターフェイスから別の VLAN への接続開始を制限します。</p> <p><i>number</i> には、VLAN ID を指定します。この VLAN インターフェイスからこの VLAN へのトラフィック開始はできなくなります。</p> <p>基本ライセンスでは、このコマンドを使用して制限した場合だけ、3 つ目の VLAN を設定できます。</p> <p>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 no forward interface コマンドを使用できます。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。</p> <p>すでに 2 つの VLAN インターフェイスを nameif コマンドで設定している場合は、3 つ目のインターフェイスに対して nameif コマンドを使用する前に no forward interface コマンドを入力してください。ASA では、ASA 5505 の基本ライセンスで 3 つのフル機能 VLAN インターフェイスを持つことは許可されていません。</p> <p>(注) Security Plus ライセンスにアップグレードすれば、このコマンドを削除して、このインターフェイスのフル機能を取得することができます。このコマンドを設定したままにすると、アップグレード後もインターフェイスの制限はそのまま残ります。</p>

次の作業

スイッチ ポートを設定します。「[スイッチ ポートのアクセス ポートとしての設定とイネーブル化](#) (P.12-7) および「[スイッチ ポートのトランク ポートとしての設定とイネーブル化](#) (P.12-9) を参照してください。

スイッチ ポートのアクセス ポートとしての設定とイネーブル化

デフォルト (コンフィギュレーションなし) では、すべてのスイッチ ポートがシャットダウンされ、VLAN 1 に割り当てられます。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。複数の VLAN を伝送するトランク ポートを作成するには、「[スイッチ ポートのトラ](#)

「リンク ポートとしての設定とイネーブル化」(P.12-9) を参照してください。工場出荷時のデフォルト コンフィギュレーションが設定されている場合に、次の手順に従ってデフォルトのインターフェイス設定を変更する必要があるかどうかを確認するには、「ASA 5505 のデフォルト コンフィギュレーション」(P.3-19) を参照してください。

ASA 5505 のインターフェイスの詳細については、「ASA 5505 インターフェイスについて」(P.12-1) を参照してください。


注意

ASA 5505 は、ネットワーク内のループ検出用のスパニングツリー プロトコルをサポートしていません。したがって、ASA とのすべての接続は、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。

手順の詳細

	コマンド	目的
ステップ 1	<code>interface ethernet0/port</code> 例: <code>hostname(config)# interface ethernet0/1</code>	設定するスイッチ ポートを指定します。port は 0 ~ 7 です。
ステップ 2	<code>switchport access vlan number</code> 例: <code>hostname(config-if)# switchport access vlan 100</code>	このスイッチ ポートを VLAN に割り当てます。number は VLAN ID で、範囲は 1 ~ 4090 です。スイッチ ポートに割り当てる VLAN インターフェイスを設定するには、「VLAN インターフェイスの設定」(P.12-6) を参照してください。設定済みの VLAN を表示するには、 show interface コマンドを入力します。 (注) インターネット アクセス デバイスにレイヤ 2 冗長性が含まれている場合は、複数のスイッチ ポートをプライマリ VLAN またはバックアップ VLAN に割り当てることができます。
ステップ 3	(任意) <code>switchport protected</code> 例: <code>hostname(config-if)# switchport protected</code>	このスイッチ ポートと、同じ VLAN 上の他の保護されたスイッチ ポートとの通信を禁止します。 スイッチ ポート間で相互通信するのを防ぐのは、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 内のアクセスを許可する必要がなく、感染やセキュリティ違反が発生した際に、個々のデバイスを相互に孤立させる場合です。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 switchport protected コマンドを適用すると、Web サーバ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 サーバすべてと通信でき、その逆も可能ですが、Web サーバは相互に通信できません。
ステップ 4	(任意) <code>speed {auto 10 100}</code> 例: <code>hostname(config-if)# speed 100</code>	速度を設定します。auto 設定がデフォルトです。PoE ポート Ethernet 0/6 または 0/7 で速度を auto 以外に設定すると、IEEE 802.3af をサポートしていない Cisco IP Phone およびシスコの無線アクセス ポイントは検出されず、電源も供給されません。

	コマンド	目的
ステップ5	(任意) <code>duplex {auto full half}</code> 例: <code>hostname(config-if)# duplex full</code>	二重通信を設定します。 auto 設定がデフォルトです。PoE ポート Ethernet 0/6 または 0/7 で二重通信を auto 以外に設定すると、IEEE 802.3af をサポートしていない Cisco IP Phone およびシスコの無線アクセス ポイントは検出されず、電源も供給されません。
ステップ6	<code>no shutdown</code> 例: <code>hostname(config-if)# no shutdown</code>	スイッチ ポートをイネーブルにします。スイッチ ポートをディセーブルにするには、 shutdown コマンドを入力します。

次の作業

- スイッチ ポートをトランク ポートとして設定する場合は、「[スイッチ ポートのトランク ポートとしての設定とイネーブル化](#)」(P.12-9) を参照してください。
- インターフェイス コンフィギュレーションを実行する場合は、[第 13 章「インターフェイス コンフィギュレーションの実行 \(ルーテッド モード\)」](#)または[第 14 章「インターフェイス コンフィギュレーションの実行 \(トランスペアレント モード\)」](#)を参照してください。

スイッチ ポートのトランク ポートとしての設定とイネーブル化

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 モードが使用できるのは Security Plus ライセンスだけです。

インターフェイスが 1 つの VLAN にだけ割り当てられるアクセス ポートを作成するには、「[スイッチ ポートのアクセス ポートとしての設定とイネーブル化](#)」(P.12-7) を参照してください。

ガイドライン

ネイティブまたは非ネイティブにかかわらず、少なくとも 1 つの VLAN が割り当てられないと、このスイッチ ポートはトラフィックを通過させることができません。

手順の詳細

	コマンド	目的
ステップ1	<code>interface ethernet0/port</code> 例: <code>hostname(config)# interface ethernet0/1</code>	設定するスイッチ ポートを指定します。 <i>port</i> は 0 ~ 7 です。
ステップ2	このトランクに VLAN を割り当てるには、次の 1 つ以上を実行します。	

コマンド	目的
<pre>switchport trunk allowed vlan <i>vlan_range</i></pre> <p>例 : hostname(config)# switchport trunk allowed vlan 100-200</p>	<p>トランク ポートに割り当てることができる 1 つ以上の VLAN を特定します。<i>vlan_range</i> (1 ~ 4090 の範囲の VLAN) は、次のいずれかの方法で特定します。</p> <ul style="list-style-type: none"> • 単一の番号 (n) • 範囲 (n-x) • 番号および範囲は、カンマで区切ります。たとえば、次のように指定します。 5,7-10,13,45-100 <p>カンマの代わりにスペースを入力できますが、コマンドはカンマ付きでコンフィギュレーションに保存されます。</p> <p>このコマンドにネイティブ VLAN を含めることができますが、必須ではありません。ネイティブ VLAN は、このコマンドに含まれているかどうかに関係なく渡されます。</p>
<pre>switchport trunk native vlan <i>vlan_id</i></pre> <p>例 : hostname(config-if)# switchport trunk native vlan 100</p>	<p>ネイティブ VLAN をトランクに割り当てます。<i>vlan_id</i> は単一の VLAN ID で、範囲は 1 ~ 4090 です。</p> <p>ネイティブ VLAN 上のパケットは、トランク経由で送信されるときに変更されません。たとえば、ポートに VLAN 2、3、および 4 が割り当てられており、VLAN 2 がネイティブ VLAN である場合、ポートを出る VLAN 2 上のパケットは 802.1Q ヘッダーによって変更されません。このポートに入ってくるフレームは、802.1Q ヘッダーが付いていない場合は VLAN 2 に割り当てられます。</p> <p>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。</p>
<p>ステップ 3</p> <pre>switchport mode trunk</pre> <p>例 : hostname(config-if)# switchport mode trunk</p>	<p>このスイッチ ポートをトランク ポートにします。このポートをアクセス モードに復元するには、switchport mode access コマンドを入力します。</p>
<p>ステップ 4</p> <p>(任意)</p> <pre>switchport protected</pre> <p>例 : hostname(config-if)# switchport protected</p>	<p>このスイッチ ポートと、同じ VLAN 上の他の保護されたスイッチ ポートとの通信を禁止します。</p> <p>スイッチ ポート間で相互通信するのを防ぐのは、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 内のアクセスを許可する必要がなく、感染やセキュリティ違反が発生した際に、個々のデバイスを相互に孤立させる場合です。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 switchport protected コマンドを適用すると、Web サーバ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 サーバすべてと通信でき、その逆も可能ですが、Web サーバは相互に通信できません。</p>
<p>ステップ 5</p> <p>(任意)</p> <pre>speed {auto 10 100}</pre> <p>例 : hostname(config-if)# speed 100</p>	<p>速度を設定します。auto 設定がデフォルトです。PoE ポート Ethernet 0/6 または 0/7 で速度を auto 以外に設定すると、IEEE 802.3af をサポートしていない Cisco IP Phone およびシスコの無線アクセス ポイントは検出されず、電源も供給されません。</p>

	コマンド	目的
ステップ6	(任意) <code>duplex {auto full half}</code> 例: <code>hostname(config-if)# duplex full</code>	二重通信を設定します。 auto 設定がデフォルトです。PoE ポート Ethernet 0/6 または 0/7 で二重通信を auto 以外に設定すると、IEEE 802.3af をサポートしていない Cisco IP Phone およびシスコの無線アクセス ポイントは検出されず、電源も供給されません。
ステップ7	<code>no shutdown</code> 例: <code>hostname(config-if)# no shutdown</code>	スイッチ ポートをイネーブルにします。スイッチ ポートをディセーブルにするには、 shutdown コマンドを入力します。

インターフェイスのモニタリング

インターフェイスをモニタするには、次のいずれかのコマンドを入力します。

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

ASA 5505 インターフェイスの設定例

この項では、次のトピックについて取り上げます。

- 「アクセス ポートの例」(P.12-11)
- 「トランク ポートの例」(P.12-12)

アクセス ポートの例

次の例では 5 つの VLAN インターフェイスを設定しています。これには、**failover lan** コマンドを使用して設定されるフェールオーバー インターフェイスも含まれます。

```
hostname(config)# interface vlan 100
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 300
hostname(config-if)# nameif dmz
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.3.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

```

hostname(config-if)# interface vlan 400
hostname(config-if)# nameif backup-isp
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.1.2.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# failover lan faillink vlan500
hostname(config)# failover interface ip faillink 10.4.1.1 255.255.255.0 standby 10.4.1.2
255.255.255.0

hostname(config)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 400
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 500
hostname(config-if)# no shutdown

```

トランク ポートの例

次の例では 7 つの VLAN インターフェイスを設定しています。これには、**failover lan** コマンドを使用して設定されるフェールオーバー インターフェイスも含まれます。VLAN 200、201、および 202 は、イーサネット 0/1 でトランキングされています。

```

hostname(config)# interface vlan 100
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 201
hostname(config-if)# nameif dept1
hostname(config-if)# security-level 90
hostname(config-if)# ip address 10.2.2.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 202
hostname(config-if)# nameif dept2
hostname(config-if)# security-level 90
hostname(config-if)# ip address 10.2.3.1 255.255.255.0
hostname(config-if)# no shutdown

```

```
hostname(config-if)# interface vlan 300
hostname(config-if)# nameif dmz
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.3.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 400
hostname(config-if)# nameif backup-isp
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.1.2.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# failover lan faillink vlan500
hostname(config)# failover interface ip faillink 10.4.1.1 255.255.255.0 standby 10.4.1.2
255.255.255.0

hostname(config)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport mode trunk
hostname(config-if)# switchport trunk allowed vlan 200-202
hostname(config-if)# switchport trunk native vlan 5
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 400
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 500
hostname(config-if)# no shutdown
```

次の作業

第 13 章「インターフェイス コンフィギュレーションの実行 (ルーテッド モード)」または第 14 章「インターフェイス コンフィギュレーションの実行 (トランスペアレント モード)」に従って、インターフェイス コンフィギュレーションを実行します。

ASA 5505 インターフェイスの機能履歴

表 12-1 に、この機能のリリース履歴を示します。

表 12-1 インターフェイスの機能履歴

機能名	リリース	機能情報
VLAN 数の増加	7.2(2)	ASA 5505 上の Security Plus ライセンスに対する VLAN 最大数が、5 (3 つのフル機能インターフェイス、1 つのフェールオーバー インターフェイス、1 つのバックアップ インターフェイスに制限されるインターフェイス) から 20 のフル機能インターフェイスに増加されました。また、トランク ポート数も 1 から 8 に増加されました。フル機能のインターフェイスの数が 20 になり、バックアップ ISP インターフェイスを停止するために <code>backup interface</code> コマンドを使用する必要がなくなりました。つまり、バックアップ ISP インターフェイス用にフル機能のインターフェイスを使用できるようになりました。 <code>backup interface</code> コマンドは、これまでどおり Easy VPN 設定用に使用できます。
ASA 5505 に対するネイティブ VLAN サポート	7.2(4)/8.0(4)	ネイティブ VLAN を ASA 5505 トランク ポートに割り当てることができるようになりました。 <code>switchport trunk native vlan</code> コマンドが導入されました。