



基本インターフェイスの設定

この章では、イーサネット設定、ジャンボフレーム設定などの基本インターフェイス設定について説明します。



(注) マルチコンテキストモードでは、この項のすべてのタスクをシステム実行スペースで実行してください。まだシステム実行スペースに入っていない場合は、[Configuration] > [Device List] ペイン内で、アクティブなデバイスのIPアドレスの下にある[System]をダブルクリックします。



(注) ASA サービス モジュール インターフェイスについては、[『ASA Services Module quick start guide』](#)を参照してください。

Firepower 4100/9300 シャーシでは、FXOS オペレーティング システムで基本的なインターフェイス設定を行います。詳細については、お使いのシャーシの設定または導入ガイドを参照してください。

- [基本インターフェイスの設定について \(1 ページ\)](#)
- [基本インターフェイスの設定のライセンス \(5 ページ\)](#)
- [基本インターフェイスの設定のガイドライン \(5 ページ\)](#)
- [基本インターフェイスのデフォルト設定 \(6 ページ\)](#)
- [物理インターフェイスのイネーブル化およびイーサネットパラメータの設定 \(7 ページ\)](#)
- [ジャンボ フレーム サポートの有効化 \(9 ページ\)](#)
- [基本インターフェイスの例 \(10 ページ\)](#)
- [基本インターフェイスの設定の履歴 \(11 ページ\)](#)

基本インターフェイスの設定について

この項では、インターフェイスの機能と特殊なインターフェイスについて説明します。

Auto-MDI/MDIX 機能

RJ-45 インターフェイスでは、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。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。インターフェイスの Auto-MDI/MDIX をイネーブルにするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、Auto-MDI/MDIX もディセーブルになります。ギガビットイーサネットの速度と二重通信をそれぞれ 1000 と全二重に設定すると、インターフェイスでは常にオートネゴシエーションが実行されるため、Auto-MDI/MDIX は常にイネーブルになり、ディセーブルにできません。

管理インターフェイス

管理インターフェイスは、使用しているモデルに応じて、管理トラフィック専用の個別インターフェイスとなります。

管理インターフェイスの概要

次のインターフェイスに接続して ASA を管理できます。

- 任意の通過トラフィック インターフェイス
- 専用の管理スロット/ポート インターフェイス（使用しているモデルで使用できる場合）

管理アクセスの説明に従って、管理アクセスへのインターフェイスを設定する必要がある場合があります。

管理スロット/ポート インターフェイス

次の表に、モデルごとの管理インターフェイスを示します。

表 1: モデルごとの管理インターフェイス

モデル	管理 0/0	管理 0/1	管理 1/0	管理 1/1	通過トラフィックに対して設定可能	サブインターフェイスを使用可能
Firepower 4100/9300	該当なし インターフェイス ID は ASA 論理デバイスに割り当てた物理 mgmt タイプ インターフェイスに基づいています。	—	—	—	—	○

モデル	管理 0/0	管理 0/1	管理 1/0	管理 1/1	通過トラフィックに対して設定可能	サブインターフェイスを使用可能
ASA 5506-X	—	—	—	○	—	—
ASA 5508-X	—	—	—	○	—	—
ASA 5512-X	○	—	—	—	—	—
ASA 5515-X	○	—	—	—	—	—
ASA 5516-X	—	—	—	○	—	—
ASA 5525-X	○	—	—	—	—	—
ASA 5545-X	○	—	—	—	—	—
ASA 5555-X	○	—	—	—	—	—
ASA 5585-X	○	○	○ SSP をスロット 1 に設置した場合は、 Management 1/0 および 1/1 ではスロット 1 の SSP への管理アクセスのみが提供されます。	○	○	○
ISA 3000	—	—	—	○	—	—
ASASM	—	—	—	—	—	—
ASAv	○	—	—	—	○	—



(注) モジュールをインストールした場合は、モジュール管理インターフェイスでは、モジュールの管理アクセスのみが提供されます。ソフトウェア モジュールを搭載したモデルでは、ソフトウェア モジュールによって ASA と同じ物理管理インターフェイスが使用されます。

管理専用トラフィックに対する任意のインターフェイスの使用

任意のインターフェイスを、管理トラフィック用として設定することによって管理専用インターフェイスとして使用できます。これには、EtherChannel インターフェイスも含まれます。

トランスペアレントモードの管理インターフェイス

トランスペアレントファイアウォールモードでは、許可される最大通過トラフィックインターフェイスに加えて、管理インターフェイス（物理インターフェイス、サブインターフェイス（使用しているモデルでサポートされている場合）、管理インターフェイスからなるEtherChannelインターフェイス（複数の管理インターフェイスがある場合）のいずれか）を個別の管理インターフェイスとして使用できます。他のインターフェイスタイプは管理インターフェイスとして使用できません。Firepower 4100/9300 シャーシでは、管理インターフェイス ID は ASA 論理デバイスに割り当てた `mgmt-type` インターフェイスに基づいています。

マルチ コンテキスト モードでは、どのインターフェイスも（これには管理インターフェイスも含まれます）、コンテキスト間で共有させることはできません。コンテキスト単位で管理を行うには、管理インターフェイスのサブインターフェイスを作成し、管理サブインターフェイスを各コンテキストに割り当てます。ASA 5555-X 以前では、管理インターフェイスのサブインターフェイスは許可されないため、コンテキスト単位で管理を行うには、データインターフェイスに接続する必要があります。

管理インターフェイスは、通常のブリッジグループの一部ではありません。動作上の目的から、設定できないブリッジグループの一部です。



- (注) トランスペアレントファイアウォールモードでは、管理インターフェイスによってデータインターフェイスと同じ方法でMACアドレステーブルがアップデートされます。したがって、いずれかのスイッチポートをルーテッドポートとして設定しない限り、管理インターフェイスおよびデータインターフェイスを同じスイッチに接続しないでください（デフォルトでは、Catalyst スイッチがすべてのVLANスイッチポートのMACアドレスを共有します）。そうしないと、物理的に接続されたスイッチから管理インターフェイスにトラフィックが到着すると、ASAによって、データインターフェイスではなく、管理インターフェイスを使用してスイッチにアクセスするようにMACアドレステーブルがアップデートされます。この処理が原因で、一時的にトラフィックが中断します。セキュリティ上の理由から、少なくとも30秒間は、スイッチからデータインターフェイスへのパケットのためにMACアドレステーブルがASAによって再アップデートされることはありません。

冗長管理インターフェイスの非サポート

冗長インターフェイスは、`Management slot/port` インターフェイスをメンバとしてサポートしません。ただし、管理インターフェイス以外の複数インターフェイスからなる冗長インターフェイスを、管理専用として設定できます。

ASA モデルの管理インターフェイスの特性

ASA 5585-X を除く ASA 5500-X モデルの管理インターフェイスには、次の特性があります。

- 通過トラフィックはサポートされません。
- サブインターフェイスはサポートされません
- プライオリティ キューはサポートされません

- マルチキャスト MAC はサポートされません
- ソフトウェア モジュールは、管理インターフェイスを共有します。ASA とモジュールに対して、別の MAC アドレスと IP アドレスがサポートされます。モジュールのオペレーティング システムでモジュールの IP アドレスのコンフィギュレーションを実行する必要があります。ただし、物理特性（インターフェイスの有効化など）は、ASA 上で設定されます。

基本インターフェイスの設定のライセンス

モデル	ライセンス要件
ASA 5585-X	SSP-10 および SSP-20 のインターフェイス速度： <ul style="list-style-type: none"> • 基本ライセンス：ファイバインターフェイスの場合 1 ギガビットイーサネット • 10 GE I/O ライセンス（Security Plus）：ファイバインターフェイスの場合 10 ギガビットイーサネット • （SSP-40 および SSP-60 は 10 ギガビットイーサネットをデフォルトでサポートします）。

基本インターフェイスの設定のガイドライン

トランスペアレント ファイアウォール モード

マルチコンテキストのトランスペアレントモードでは、各コンテキストが別個のインターフェイスを使用する必要があります。コンテキスト間でインターフェイスを共有することはできません。

フェールオーバー

データインターフェイスと、フェールオーバーまたはステートのインターフェイスを共有することはできません。

その他のガイドライン

一部の管理関連のサービスは、管理対象外のインターフェイスが有効になり、ASA が「システム レディ」状態になるまで使用できません。ASA が「System Ready」状態になると、次の syslog メッセージを生成します。

```
%ASA-6-199002: Startup completed. Beginning operation.
```

基本インターフェイスのデフォルト設定

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。

インターフェイスのデフォルトの状態

インターフェイスのデフォルトの状態は、そのタイプおよびコンテキストモードによって異なります。

マルチ コンテキスト モードでは、システム実行スペース内でのインターフェイスの状態にかかわらず、すべての割り当て済みのインターフェイスがデフォルトでイネーブルになっています。ただし、トラフィックがインターフェイスを通過するためには、そのインターフェイスもシステム実行スペース内でイネーブルになっている必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。

シングルモードまたはシステム実行スペースでは、インターフェイスのデフォルトの状態は次のとおりです。

- 物理インターフェイス：ディセーブル。
- 冗長インターフェイス：イネーブル。ただし、トラフィックが冗長インターフェイスを通過するためには、メンバ物理インターフェイスもイネーブルになっている必要があります。
- VLAN サブインターフェイス：イネーブル。ただし、トラフィックがサブインターフェイスを通過するためには、物理インターフェイスもイネーブルになっている必要があります。
- VXLAN VNI インターフェイス：イネーブル。
- EtherChannel ポートチャネルインターフェイス（ASA モデル）：イネーブル。ただし、トラフィックが EtherChannel を通過するためには、チャネルグループ物理インターフェイスもイネーブルになっている必要があります。
- EtherChannel ポートチャネルインターフェイス（Firepower モデル）：ディセーブル。



(注) Firepower 4100/9300 の場合、管理上、シャーシおよび ASA の両方で、インターフェイスを有効および無効にできます。インターフェイスを動作させるには、両方のオペレーティングシステムで、インターフェイスを有効にする必要があります。インターフェイスの状態は個別に制御されるので、シャーシと ASA の間の不一致が生じることがあります。

デフォルトの速度および二重通信

- デフォルトでは、銅線（RJ-45）インターフェイスの速度とデュプレックスは、オートネゴシエーションに設定されます。
- 5585-X のファイバインターフェイスでは、自動リンク ネゴシエーションの速度が設定されます。

デフォルトのコネクタタイプ

2つのコネクタタイプ（copper RJ-45 と fiber SFP）を持つモデルもあります。RJ-45 がデフォルトです。ASA にファイバ SFP コネクタを使用するように設定できます。

デフォルトの 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。

物理インターフェイスのイネーブル化およびイーサネットパラメータの設定

ここでは、次の方法について説明します。

- 物理インターフェイスをイネーブルにする。
- 特定の速度と二重通信（使用できる場合）を設定する。
- フロー制御のポーズフレームをイネーブルにする。

始める前に

マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。まだシステム コンフィギュレーション モードに入っていない場合、**[Configuration] > [Device List]** ペインで、アクティブなデバイスの IP アドレスの下にある **[System]** をダブルクリックします。

手順

ステップ 1 コンテキスト モードによって次のように異なります。

- シングル モードの場合、**[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces]** ペインを選択します。
- マルチ モードの場合、システム実行スペースで、**[Configuration] > [Context Management] > [Interfaces]** ペインを選択します。

デフォルトでは、すべての物理インターフェイスが一覧表示されます。

ステップ 2 設定する物理インターフェイスをクリックし、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが表示されます。

(注) シングルモードでは、この手順では [Edit Interface] ダイアログボックスでのパラメータのサブセットのみを対象としています。マルチコンテキストモードでは、インターフェイスの設定を完了する前に、コンテキストにインターフェイスを割り当てる必要があります。

ステップ 3 インターフェイスをイネーブルにするには、[Enable Interface] チェックボックスをオンにします。

ステップ 4 説明を追加するには、[Description] フィールドにテキストを入力します。

説明は 240 文字以内で入力できます。改行を入れずに 1 行で入力します。フェールオーバーまたはステートリンクの場合、説明は「LAN Failover Interface」、「STATE Failover Interface」、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。

ステップ 5 (任意) メディア タイプ、二重通信、速度を設定し、フロー制御のポーズフレームをイネーブルにするには、[Configure Hardware Properties] をクリックします。

a) インターフェイス タイプに応じて、[Media Type] ドロップダウンリストから [RJ-45] または [SFP] のいずれかを選択できます。

RJ-45 がデフォルトです。

b) RJ-45 インターフェイスにデュプレックスを設定するには、[Duplex] ドロップダウンリストからインターフェイス タイプに応じて [Full]、[Half]、または [Auto] を選択します。

(注) EtherChannel インターフェイスのデュプレックスの設定は [Full] または [Auto] である必要があります。

c) 速度を設定するには、[Speed] ドロップダウンリストから値を選択します。

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。SFP インターフェイスでは、速度を [Negotiate] または [Nonegotiate] に設定できます。[Negotiate] (デフォルト) ではリンクネゴシエーションをイネーブルにして、フロー制御パラメータとリモート障害情報を交換します。[Nonegotiate] では、リンクパラメータのネゴシエーションを行いません。RJ-45 インターフェイスでは、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。

d) 1 ギガビットイーサネットインターフェイスおよび 10 ギガビットイーサネットインターフェイスでフロー制御のポーズ (XOFF) フレームをイネーブルにするには、[Enable Pause Frame] チェックボックスをオンにします。

トラフィックバーストが発生している場合、バーストが NIC の FIFO バッファまたは受信リングバッファのバッファリング容量を超えると、パケットがドロップされる可能性があります。フロー制御用のポーズフレームをイネーブルにすると、このような問題の発生を

抑制できます。ポーズ (XOFF) および XON フレームは、FIFO バッファ使用量に基づいて、NIC ハードウェアによって自動的に生成されます。バッファ使用量が高ウォーターマークを超えると、ポーズ フレームが送信されます。デフォルトの *high_water* 値は 128 KB (10 ギガビット イーサネット) および 24 KB (1 ギガビット イーサネット) です。0 ~ 511 (10 ギガビット イーサネット) または 0 ~ 47 KB (1 ギガビット イーサネット) に設定できます。ポーズの送信後、バッファ使用量が低ウォーターマークよりも下回ると、XON フレームを送信できます。デフォルトでは、*low_water* 値は 64 KB (10 ギガビット イーサネット) および 16 KB (1 ギガビット イーサネット) です。0 ~ 511 (10 ギガビット イーサネット) または 0 ~ 47 KB (1 ギガビット イーサネット) に設定できます。リンク パートナーは、XON を受信した後、または XOFF の期限が切れた後、トラフィックを再開できます。XOFF の期限は、ポーズ フレーム内のタイマー値によって制御されます。デフォルトの *pause_time* 値は 26624 です。この値は 0 ~ 65535 に設定できます。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。

[Low Watermark]、[High Watermark]、[Pause Time] のデフォルト値を変更するには、[Use Default Values] チェックボックスをオフにします。

(注) 802.3x に定義されているフロー制御フレームのみがサポートされています。プライオリティベースのフロー制御はサポートされていません。

e) [OK] をクリックして [Hardware Properties] の変更を受け入れます。

ステップ 6 [OK] をクリックして [Interface] の変更を受け入れます。

ジャンボ フレーム サポートの有効化

ジャンボ フレームとは、標準的な最大値 1518 バイト (レイヤ 2 ヘッダーおよび VLAN ヘッダーを含む) より大きく、9216 バイトまでのイーサネット パケットのことです。イーサネット フレームを処理するためのメモリ容量を増やすことにより、すべてのインターフェイスに対してジャンボ フレームのサポートをイネーブルにできます。ジャンボ フレームに割り当てるメモリを増やすと、他の機能 (ACL など) の最大使用量が制限される場合があります。ASA MTU はレイヤ 2 (14 バイト) および VLAN ヘッダー (4 バイト) を含まずにペイロードサイズを設定するので、モデルによっては MTU 最大値が 9198 になることに注意してください。

始める前に

- マルチコンテキストモードでは、システム実行スペースでこのオプションを設定します。
- この設定を変更した場合は、ASA のリロードが必要です。
- ジャンボフレームを送信する必要のある各インターフェイスの MTU を、デフォルト値の 1500 より大きい値に設定してください。たとえば、マルチコンテキストモードでは、各コンテキスト内で MTU を設定します。

- TCP MSS は必ず調整してください。非 IPsec トラフィックについては、無効にするか、または MTU に応じて増やします。

手順

コンテキスト モードによって次のように異なります。

- マルチ モード：ジャンボ フレーム サポートをイネーブルにするには、[Configuration] > [Context Management] > [Interfaces] を選択し、[Enable jumbo frame support] チェックボックスをオンにします。
- シングル モード：1500 バイトを超える MTU を設定すると、ジャンボ フレームが自動的にイネーブルになります。この設定を手動でイネーブルまたはディセーブルにするには、[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] を選択し、[Enable jumbo frame support] チェック ボックスをオンにします。

基本インターフェイスの例

次の設定例を参照してください。

物理インターフェイス パラメータの例

次に、シングル モードで物理インターフェイスのパラメータを設定する例を示します。

```
interface gigabitethernet 0/1
speed 1000
duplex full
no shutdown
```

マルチ コンテキスト モードの例

次に、システム コンフィギュレーション用にマルチ コンテキスト モードでインターフェイス パラメータを設定し、GigabitEthernet 0/1.1 サブインターフェイスをコンテキスト A に割り当てる例を示します。

```
interface gigabitethernet 0/1
speed 1000
duplex full
no shutdown
interface gigabitethernet 0/1.1
vlan 101
context contextA
allocate-interface gigabitethernet 0/1.1
```

基本インターフェイスの設定の履歴

表 2: インターフェイスの履歴

機能名	リリース	機能情報
ASA 5510 上の基本ライセンスに対する増加したインターフェイス	7.2(2)	ASA 5510 上の基本ライセンスについて、最大インターフェイス数が 3 プラス管理インターフェイスから無制限のインターフェイスに増加しました。
ASA 5510 Security Plus ライセンスに対するギガビットイーサネットサポート	7.2(3)	ASA 5510 は、GE（ギガビットイーサネット）を Security Plus ライセンスのあるポート 0 および 1 でサポートするようになりました。ライセンスを Base から Security Plus にアップグレードした場合、外部 Ethernet 0/0 および Ethernet 0/1 ポートの容量は、元の FE（ファストイーサネット）の 100 Mbps から GE の 1000 Mbps に増加します。インターフェイス名は Ethernet 0/0 および Ethernet 0/1 のままです。
ASA 5580 に対するジャンボ パケットサポート	8.1(1)	<p>Cisco ASA 5580 はジャンボフレームをサポートしています。ジャンボフレームとは、標準的な最大値 1518 バイト（レイヤ 2 ヘッダーおよび FCS を含む）より大きく、9216 バイトまでのイーサネットパケットのことです。イーサネットフレームを処理するためのメモリ容量を増やすことにより、すべてのインターフェイスに対してジャンボフレームのサポートをイネーブルにできます。ジャンボフレームに割り当てるメモリを増やすと、他の機能（ACL など）の最大使用量が制限される場合があります。</p> <p>この機能は、ASA 5585-X でもサポートされます。</p> <p>次の画面が変更されました。 [Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Interface] > [Advanced]。</p>

機能名	リリース	機能情報
ASA 5580 10 ギガビットイーサネット インターフェイスでのフロー制御の ポーズ フレームのサポート	8.2(2)	<p>フロー制御のポーズ (XOFF) フレームをイネーブルにできるようになりました。</p> <p>この機能は、ASA 5585-X でもサポートされます。</p> <p>次の画面が変更されました。[(Single Mode) Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Interface] > [General (Multiple Mode, System)]</p> <p>[Configuration] > [Interfaces] > [Add/Edit Interface]</p>
ギガビットイーサネットインターフェイスでのフロー制御のポーズフレームのサポート	8.2(5)/8.4(2)	<p>すべてのモデルでギガビットインターフェイスのフロー制御のポーズ (XOFF) フレームをイネーブルにできるようになりました。</p> <p>次の画面が変更されました。[(Single Mode) Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Interface] > [General (Multiple Mode, System)]</p> <p>[Configuration] > [Interfaces] > [Add/Edit Interface]</p>
ASAv の管理 0/0 インターフェイスでの通過トラフィック サポート	9.6(2)	<p>ASAv の管理 0/0 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した。以前は、Microsoft Azure 上の ASAv のみで通過トラフィックをサポートしていました。今後は、すべての ASAv で通過トラフィックがサポートされます。任意で、このインターフェイスを管理専用を設定できますが、デフォルトでは管理専用には設定されていません。</p>