



## 基本的なインターフェイス設定

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的な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。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。。



- (注) プラットフォームモードの Firepower 2100 および 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。

- [基本的なインターフェイス設定について \(1 ページ\)](#)
- [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 \(ASA モデルと ASA v および ISA 3000\) \(10 ページ\)](#)
- [モニタリングインターフェイス \(11 ページ\)](#)
- [基本インターフェイスの例 \(11 ページ\)](#)
- [基本インターフェイスの設定の履歴 \(12 ページ\)](#)

## 基本的なインターフェイス設定について

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 を有効にするには、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無効にされ、Auto-MDI/MDIX も無効になります。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 は常に有効になり、無効にできません。

## 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 1000	—	—	—	対応	対応	対応

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 2100	—	—	—	対応	— 注：技術的には、通過トラフィックを有効にすることはできませんが、このインターフェイスのスループットはデータ操作には適していません。	○
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。	—	—	—	—	対応
ASA 5506-X	—	—	—	対応	—	—
ASA 5508-X	—	—	—	対応	—	—
ASA 5516-X	—	—	—	対応	—	—
ASA 5525-X	対応	—	—	—	—	—
ASA 5545-X	対応	—	—	—	—	—
ASA 5555-X	対応	—	—	—	—	—
ISA 3000	—	—	—	対応	—	—
ASAv	対応	—	—	—	対応	—



- (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せん。

## 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 (**management-only** コマンドを参照)。

## 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）のいずれか）を個別の管理専用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。Firepower デバイスモデルで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。ただし、ASA モデルでは、管理インターフェイスのサブインターフェイスが許可されないため、それらのモデルでコンテキスト単位の管理を行うには、データインターフェイスに接続する必要があります。Firepower 4100/9300 シャーシでは、管理インターフェイスとそのサブインターフェイスは、コンテキスト内で特別に許可された管理インターフェイスとして認識されません。この場合、管理サブインターフェイスをデータインターフェイスとして扱い、BVI に追加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

Asaasa 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、ISA 3000）：有効。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（その他のモデル）：無効。



(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。

#### 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。
- (ASA ハードウェア) 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。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

#### 手順

**ステップ 1** 設定するインターフェイスを指定します。

**interface** *physical\_interface*

例：

```
ciscoasa(config)# interface gigabitethernet 0/0
```

*physical\_interface* ID には、タイプ、スロット、およびポート番号 (type[slot/]port) が含まれます。

物理インターフェイスのタイプには、次のものがあります。

- **ethernet**
- **gigabitethernet**
- **tengigabitethernet**
- **management**

タイプに続けてスロット/ポートを入力します。たとえば、**gigabitethernet0/1** というようになります。タイプとスロット/ポートの間のスペースは任意です。

**ステップ 2** (任意) 速度を選択します (モデルによって異なります)。

**speed** {*auto* | *speed* | **nonegotiate**}

例：

```
ciscoasa(config-if)# speed 100
```

SFP インターフェイスの場合、**no speed nonegotiate** を指定すると速度が 1,000 Mbps に設定され、フロー制御パラメータとリモート障害情報のリンクネゴシエーションがイネーブルになります。10 Gbps インターフェイスの場合、このオプションを指定すると速度が 1,000 Mbps に設定されます。**nonegotiate** キーワードは、SFP インターフェイスで使用できる唯一のキーワードです。**speed nonegotiate** コマンドは、リンクネゴシエーションをディセーブルにします。

**ステップ 3** (任意) RJ-45 インターフェイスのデュプレックスを設定します。

**duplex** {*auto* | **full** | **half**}

SFP インターフェイスは全二重のみをサポートします。

例：

```
ciscoasa(config-if)# duplex full
```

**ステップ 4** (任意) (ASA ハードウェア) 1 ギガビット以上の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します。

**flowcontrol send on** [*low\_water high\_water pause\_time*] [**noconfirm**]

例：

```
ciscoasa(config-if)# flowcontrol send on 95 200 10000
```



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。

このコマンドを使用すると、次の警告が表示されます。

```
Changing flow-control parameters will reset the interface. Packets may be lost during the reset.  
Proceed with flow-control changes?
```

プロンプトを表示しないでパラメータを変更するには、**noconfirm** キーワードを使用します。

(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。

## ステップ5 インターフェイスをイネーブルにします。

### no shutdown

例：

```
ciscoasa(config-if)# no shutdown
```

インターフェイスをディセーブルにするには、**shutdown** コマンドを入力します。**shutdown** コマンドを入力すると、すべてのサブインターフェイスもシャットダウンします。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します。

# ジャンボフレームサポートの有効化 (ASA モデルと ASAv および ISA 3000)

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。

この手順は、ASA ハードウェアモデル、ISA 3000 および ASAv にのみ適用されます。その他のモデルは、デフォルトでジャンボフレームをサポートしています。

ジャンボフレームは、8GB RAM 未満の ASAv5 と ASAv10 ではサポートされません。

## 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、`mtu` コマンドを使用して値を 9198 に設定します。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。
- Be sure to adjust the TCP MSS, either to disable it for non-IPsec traffic (use the `sysopt connection tcpmss 0` command), or to increase it in accord with the MTU.

## 手順

---

ジャンボフレームサポートをイネーブルにします。

### **jumbo-frame reservation**

---

## 例

次に、ジャンボフレームの予約をイネーブルにし、コンフィギュレーションを保存して ASA をリロードする例を示します。

```
ciscoasa(config)# jumbo-frame reservation
WARNING: this command will take effect after the running-config is saved
and the system has been rebooted. Command accepted.

ciscoasa(config)# write memory
```

```
Building configuration...
Cryptochecksum: 718e3706 4edb11ea 69af58d0 0a6b7cb5

70291 bytes copied in 3.710 secs (23430 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm] Y
```

## モニタリングインターフェイス

次のコマンドを参照してください。



- (注) プラットフォームモードの Firepower 2100 および Firepower 4100/9300 の場合、一部の統計情報は ASA コマンドを使用して表示されません。FXOS コマンドを使用して、より詳細なインターフェイス統計情報を表示する必要があります。これらのコマンドは、アプライアンスモードの Firepower 1000 および 2100 にも役立ちます。

- /eth-uplink/fabric# **show interface**
- /eth-uplink/fabric# **show port-channel**
- /eth-uplink/fabric/interface# **show stats**

プラットフォームモードの Firepower 2100 の場合は、次の FXOS connect local-mgmt コマンドも参照してください。

- (local-mgmt)# **show portmanager counters**
- (local-mgmt)# **show lacp**
- (local-mgmt)# **show portchannel**

詳細については、『[FXOS troubleshooting guide](#)』を参照してください。

---

### • **show interface**

インターフェイス統計情報を表示します。

### • **show interface ip brief**

インターフェイスの IP アドレスとステータスを表示します。

## 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、GigabitEthernet0/1.1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
Firepower 1000 および 2100 の SFP インターフェイスでの速度の自動ネゴシエーションの無効化	9.14(1)	自動ネゴシエーションを無効にするように Firepower 1100 または 2100 SFP インターフェイスを設定できるようになりました。10GB インターフェイスの場合、自動ネゴシエーションなしで速度を 1GB に設定できます。速度が 10 GB に設定されているインターフェイスの自動ネゴシエーションは無効にできません。  新規/変更されたコマンド: <b>speed nonegotiate</b>
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)	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るようになりました。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。  次のコマンドが変更されました。 <b>management-only</b>

機能名	リリース	機能情報
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)	すべての ASA モデルでギガビットイーサネ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。  <b>flowcontrol</b> コマンドが変更されました。
ASA 5580 10 ギガビットイーサネットインターフェイスでのフロー制御のポーズフレームのサポート	8.2(2)	フロー制御のポーズ (XOFF) フレームをイネーブルにできるようになりました。  この機能は、ASA 5585-X でもサポートされます。  <b>flowcontrol</b> コマンドが導入されました。
ASA 5580 に対するジャンボ パケットサポート	8.1(1)	ASA 5580 はジャンボフレームをサポートします。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。  この機能は、ASA 5585-X でもサポートされます。  <b>jumbo-frame reservation</b> コマンドが導入されました。
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。 <b>speed</b> コマンドを使用してインターフェイスの速度を変更します。また、 <b>show interface</b> コマンドを使用して各インターフェイスの現在の設定速度を確認します。
ASA 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。



## 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。