

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。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） 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 （4 ページ）
- 基本インターフェイスのデフォルト設定 （5 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 （6 ページ）
- ジャンボフレームサポートの有効化（ASA 仮想、ISA 3000） （10 ページ）
- Cisco Secure Firewall 3100 のネットワークモジュールの管理 （11 ページ）
- 基本インターフェイスの例 （16 ページ）
- 基本インターフェイスの設定の履歴 （17 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

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する機能です。この機能は、RJ-45インターフェイスで自動ネゴシエーションする場合にデフォルトで有効になり、速度またはデュプレックスのいずれかを自動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
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すが、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。	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
Cisco Secure Firewall 3100	—	—	—	対応	対応	対応
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
ISA 3000	—	—	—	対応	—	—
ASAv	対応	—	—	—	対応	—

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）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。

（注） 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。

管理専用トラフィック

管理インターフェイスは、To-the-Box および From-the-Box トラフィック専用で、トラフィックを通過することができません。いずれの場合も、ブリッジグループは他のブリッジグループと

通信できないため、トラフィックによるサポートがあった場合でも、管理インターフェイスからブリッジグループに、またはその逆にルーティングすることはできません。

共有 MAC アドレステーブルおよびスイッチ接続

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 Cisco ASA の 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、Cisco 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。

マルチ コンテキスト モード

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。サポートされるモデルの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。一部の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。

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.
```

- 10/100-Mbps イーサネットリンクの両側で自動ネゴシエーションを使用するように設定するか、両側を同じ固定速度およびデュプレックス設定で設定します。一端が固定速度および全二重に設定され、もう一方の端が自動ネゴシエーションを使用している場合、自動ネゴシエーション側では速度は判別されますが、デュプレックス設定は判別できず、デフォルトで半二重になります。これにより、ネットワークのパフォーマンスに影響を与える可能性のあるデュプレックスの不一致が発生します。

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。
- 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（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。
- フロー制御のポーズ フレームをイネーブルにする。
- 前方誤り訂正を設定する

この手順は、インターフェイス設定のごく一部にすぎません。この時点では、他のパラメータを設定しないようにします。たとえば、EtherChannel インターフェイスの一部として使用するインターフェイスには名前を付けることはできません。正確なインターフェイスオプションは、モデルおよびインターフェイスのタイプによって異なります。

（注） Firepower 4100/9300 の場合、FXOS の基本インターフェイスの設定を行います。

（注） / 1010/ スイッチポートについては、「Firepower 1010 スイッチポートの基本インターフェイス構成」を参照してください。

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 フロー制御に対してポーズ（XOFF）フレームを有効にするには、[フロー制御（Flow-Control）] チェックボックスをオンにします。

フロー制御により、接続しているイーサネットポートは、輻輳しているノードがリンク動作をもう一方の端で一時停止できるようにすることによって、輻輳時のトラフィック レートを制御できます。ASA ポートで輻輳が生じ（内部スイッチでキューイングリソースが枯渇）、それ以上はトラフィックを受信できなくなった場合、ポーズフレームを送信することによって、その状態が解消されるまで送信を中止するように、そのポートから相手ポートに通知します。ポーズ フレームを受信すると、送信側デバイスはデータ パケットの送信を中止するので、輻輳時のデータ パケット損失が防止されます。

（注） ASA は、リモートピアがトラフィックをレート制御できるように、ポーズ フレームの送信をサポートしています。

ただし、ポーズフレームの受信はサポートされていません。

内部スイッチには、それぞれ 250 バイトの 8000 バッファのグローバルプールがあり、スイッチはバッファを各ポートに動的に割り当てます。バッファ使用量がグローバルハイ ウォーターマーク（2 MB（8000 バッファ））を超えると、フロー制御が有効になっているすべてのインターフェイスからポーズフレームが送信されます。また、バッファがポートのハイ ウォーターマーク（.3125 MB（1250 バッファ））を超えると、特定のインターフェイスからポーズフレームが送信されます。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（グローバルでは 1.25MB（5000 バッファ）、ポートごとに 25 MB（1000 バッファ））リンク パートナーは、XON フレームを受信するとトラフィックを再開できます。

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 6 （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) [デュプレックス（Duplex）] を設定するには、ドロップダウンリストで、インターフェイスの種類に応じて、[全二重（Full）]、[半二重（Half）]、[自動（Auto）] のいずれかを選択します。

（注） SFP インターフェイスは全二重のみをサポートします。

b) **速度**を設定するには、ドロップダウンリストから値を選択します（モデルによって異なります）。

Firepower 1000 および 2100 SFP インターフェイスの場合、**Negotiate** 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** オプションを指定するとリンクネゴシエーションがディセーブルになります。その他のモデル自動ネゴシエーションオプションについては、[詳細設定（Advanced）] の [自動ネゴシエーション（Auto-negotiate）]

チェックボックスを確認します。このチェックボックスにより、1,000 Mbps 以上のインターフェイスの自動ネゴシエーションをオン/オフに切り替えることができます。

[SFPを検出（Detect SFP）] を選択してインストールされている SFP モジュールの速度を検出し、適切な速度を使用します。デュプレックスは常に全二重であり、自動ネゴシエーションは有効になっていて、FEC は自動に設定されています。デュアルスピード トランシーバの場合、低い方の速度が使用されます。このオプションは、後でネットワークモジュールを別のモデルに変更し、速度を自動的に更新する場合に便利です。一部のスイッチおよびトランシーバは、特に高速のインターフェイスの場合、自動ネゴシエーションをサポートしていません。この場合は、Cisco ASA のインターフェイスを手動速度に設定し、**自動ネゴシエーション**も無効にして、リンクがアップ状態になるようにします。

（注） 10/100 Mbps イーサネットリンクの場合、速度、デュプレックス、および自動ネゴシエーションの設定が接続されたピアと一致していることを確認します。一端が固定速度で全二重に設定され、もう一方の端が自動ネゴシエーションを使用する場合、自動ネゴシエーション側では速度は決定できますが、デュプレックス設定は特定できず、デフォルトで半二重になります。これにより、ネットワークのパフォーマンスに影響を与える可能性のあるデュプレックスの不一致が発生します。

c) 25 Gbps 以上のインターフェイスに対して [FECモード（FEC Mode）] を設定するには、ドロップダウンリストで値を選択します。

EtherChannel メンバーインターフェイスの場合は、EtherChannel に追加する前に FEC を設定する必要があります。EtherChannel からインターフェイスを削除する場合は、再起動後にインターフェイスの FEC を再設定する必要があります。

一部のスイッチは、特に大規模なインターフェイスの場合、FEC の auto モードをサポートしていません。スイッチのサポートに応じて、FEC を無効にするか、手動で設定してください。

自動を使用する場合に選択する設定は、トランシーバのタイプと、インターフェイスが固定（内蔵）かネットワークモジュールかによって異なります。

表 *2*：自動設定のデフォルト *FEC*

トランシーバ タイプ	固定ポートのデフォルト FEC	ネットワークモジュールのデフォルト FEC
25G-SR	cl108-rs	cl108-rs
25G-LR	cl108-rs	cl108-rs
10/25G-CSR	cl108-rs	cl74-fc
25G-AOC*x*M	cl74-fc	cl74-fc
25G-CU2.5/3M	自動ネゴシエーション	自動ネゴシエーション

トランシーバ タイプ	固定ポートのデフォルト FEC	ネットワークモジュールのデフォルト FEC
25G-CU4/5M	自動ネゴシエーション	自動ネゴシエーション

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

ステップ 7 [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（ASA 仮想、ISA 3000）

ジャンボフレームとは、標準的な最大値 1,518 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、9,216 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、ISA 3000、および ASA 仮想 にのみ適用できます。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 および 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、Cisco 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。
- Be sure to adjust the TCP MSS, either to disable it for non-IPsec traffic, or to increase it in accord with the MTU.

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有効にするには、[設定（Configuration）] > [コンテキスト管理（Context Management）]>[インターフェイス（Interfaces）] を選択し、

[ジャンボフレームサポートの有効化（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：1,500 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有効になります。この設定を手動で有効または無効にするには、[設定（Configuration）] > [デバイスの設定（Device Setup）] > [インターフェイスの設定（Interface Settings）] > [インターフェイス（Interfaces）] を選択し、[ジャンボフレームサポートの有効化（Enable jumbo frame support）] チェックボックスをクリックします。

Cisco Secure Firewall 3100 のネットワークモジュールの管理

最初にファイアウォールの電源をオンにする前にネットワークモジュールをインストールした場合、アクションは不要です。ネットワークモジュールは有効になり、使用できる状態になっています。

初回ブートアップ後にネットワークモジュールのインストールを変更する必要がある場合は、次の手順を参照してください。

ブレークアウトポートの設定

40 GB 以上のインターフェイスごとに小さいブレークアウトポートを構成できます。この手順では、ポートのブレークアウトと再参加の方法について説明します。ブレークアウトポートは、EtherChannel への追加を含め、他の物理イーサネットポートと同じように使用できます。たとえば、40 GB インターフェイスから 4 つの 10 GB ポートにブレークアウトできます。ポートの正確なサイズと数はモデルによって異なります。

設定でインターフェイスがすでに使用されている場合は、存在しなくなるインターフェイスに関連する設定を手動で削除する必要があります。

始める前に

- サポートされているブレークアウトケーブルを使用する必要があります。詳細については、ハードウェア設置ガイドを参照してください。
- クラスタリングまたはフェールオーバーの場合、クラスタ/フェールオーバーリンクで（分割用の）親インターフェイスか（再結合用の）子インターフェイスが使用されていないことを確認してください。クラスタ/フェールオーバーリンクに使用されている場合、インターフェイスを変更することはできません。

手順

ステップ 1 **[構成（Configuration）]、** > **[デバイス管理（Device Management）]、** > **[詳細設定（Advanced）]、** > **[EPM]** の順に選択し、1 つ以上の 40GB 以上のインターフェイスからポートを分割するか、分割する 1 つ以上の [ポート番号（Port Numbers）] をカンマ区切りでスペースなしで入力します。

スロットは常に **2** です。

たとえば、Ethernet2/1 インターフェイスと Ethernet2/2 インターフェイスを分割するには、[ポート番号（Port Number）] フィールドで **1,2** と指定します。分割後の子インターフェイスは、Ethernet2/1/1、Ethernet2/1/2、Ethernet2/1/3、Ethernet2/1/4、Ethernet2/2/1、Ethernet2/2/2、Ethernet2/2/3、Ethernet2/2/4 として識別されます。

クラスタリングまたはフェールオーバーの場合は、制御ノード/アクティブユニットでこの手順を実行します。インターフェイスの変更は他のノードに複製されます。

ステップ 2 [設定（Configuration）] > [デバイス管理（Device Management）] > [詳細（Advanced）] > [EPM] の順に選択し、1 つ以上の**ポート番号**を削除することにより、ブレークアウトポートを再結合してインターフェイスを復元します。

クラスタリングまたはフェールオーバーの場合は、制御ノード/アクティブユニットでこの手順を実行します。モジュールの状態は他のノードに複製されます。

指定されたインターフェイスのすべての子ポートを再結合する必要があります。

ステップ 3 [Apply] をクリックします。

ファイアウォールに設定が適用されます。

ネットワークモジュールの追加

初回起動後にファイアウォールにネットワークモジュールを追加するには、次の手順を実行します。新しいモジュールを追加するには、リロードが必要です。クラスタリングまたはフェールオーバーの場合、ゼロダウンタイムはサポートされないため、この手順は必ずメンテナンスウィンドウ中に実行してください。

手順

ステップ 1 ハードウェア設置ガイドに従ってネットワークモジュールをインストールします。ファイアウォールの電源がオンの状態でネットワークモジュールをインストールできます。

クラスタリングまたはフェールオーバーの場合は、すべてのノードにネットワークモジュールをインストールします。

ステップ 2 ファイアウォールをリロードします。[ツール（Tools）]>[システムのリロード（System Reload）] を参照してください。

クラスタリングまたはフェールオーバーの場合は、すべてのノードをリロードします。ネットワークモジュールが異なるノードはクラスタ/フェールオーバーペアに参加できないため、クラスタ/フェールオーバーペアを再作成する前に、新しいモジュールですべてのノードをリロードする必要があります。

ステップ 3 [設定（Configuration）] > [デバイス管理（Device Management）] > [詳細（Advanced）] > [EPM] の順に選択し、[NetModの無効化（Disable Netmod）] をオフにしてネットワークモジュールを有効化します。 > > >

クラスタリングまたはフェールオーバーの場合は、制御ノード/アクティブユニットでこの手順を実行します。モジュールの状態は他のノードに複製されます。

ステップ 4 [Apply] をクリックします。

ファイアウォールに設定が適用されます。

ネットワークモジュールの交換方法

リロードすることなく、同じタイプの新しいモジュールのネットワークモジュールをホットスワップできます。ただし、現在のモジュールを安全に取り外すには、シャットダウンする必要があります。この手順では、古いモジュールをシャットダウンし、新しいモジュールをインストールして有効にする方法について説明します。

クラスタリングまたはフェールオーバーの場合、クラスタ制御リンク/フェールオーバーリンクがモジュール上にあると、ネットワークモジュールを無効化できません。

手順

ステップ 1 クラスタリングまたはフェールオーバーの場合は、次の手順を実行します。

- **クラスタリング**：ホットスワップを実行するユニットがデータノードであることを確認します（「制御ノードの変更」を参照）。次に、そのノードでクラスタリングを無効化します。非アクティブノードになるまたは制御ノードからのデータノードの非アクティブ化を参照してください。

  クラスタ制御リンクがネットワークモジュール上にある場合は、クラスタから脱退する必要があります。クラスタからの脱退を参照してください。アクティブなクラスタ制御リンクがあるネットワークモジュールを無効化することはできません。

- **フェールオーバー**：ホットスワップを実行するユニットがスタンバイノードであることを確認します。フェールオーバーの強制実行 を参照してください。

  フェールオーバーリンクがネットワークモジュール上にある場合は、フェールオーバーを無効化する必要があります。フェールオーバーのディセーブル化を参照してください。ア

クティブなフェールオーバーリンクがあるネットワークモジュールを無効化することはできません。

ステップ 2 [設定（Configuration）] > [デバイス管理（Device Management）] > [詳細（Advanced）] > [EPM] の順に選択し、[NetModの無効化（Disable Netmod）] をオンにしてネットワークモジュールを無効化します。

ステップ 3 [Apply] をクリックします。

ファイアウォールに設定が適用されます。

ステップ 4 ハードウェア設置ガイドに従ってネットワークモジュールを交換します。ファイアウォールの電源がオンの状態でネットワークモジュールを交換できます。

ステップ 5 [設定（Configuration）] > [デバイス管理（Device Management）] > [詳細（Advanced）] > [EPM] の順に選択し、[NetModの無効化（Disable Netmod）] をオフにしてネットワークモジュールを有効化します。 > > >

ステップ 6 [Apply] をクリックします。

ファイアウォールに設定が適用されます。

ステップ 7 クラスタリングまたはフェールオーバーの場合は、次の手順を実行します。

- **クラスタリング**：ノードをクラスタに追加して戻します。クラスタへの再参加または制御ノードからの新しいデータノードの追加を参照してください。
- **フェールオーバー**：フェールオーバーを無効化した場合は、もう一度フェールオーバーを実行します。

ネットワークモジュールを別のタイプに交換する

ネットワークモジュールを別のタイプに交換する場合は、リロードが必要です。新しいモジュールのインターフェイス数が古いモジュールよりも少ない場合は、存在しなくなるインターフェイスに関連する構成を手動で削除する必要があります。クラスタリングまたはフェールオーバーの場合、ゼロダウンタイムはサポートされないため、この手順は必ずメンテナンスウィンドウ中に実行してください。

手順

ステップ 1 [設定（Configuration）] > [デバイス管理（Device Management）] > [詳細（Advanced）] > [EPM] の順に選択し、[NetModの無効化（Disable Netmod）] をオンにしてネットワークモジュールを無効化します。

クラスタリングまたはフェールオーバーの場合は、制御ノード/アクティブユニットでこの手順を実行します。モジュールの状態は他のノードに複製されます。

ステップ 2 [Apply] をクリックします。

ファイアウォールに設定が適用されます。設定を保存しないでください。リロードすると、保存された設定でモジュールが有効になります。

ステップ 3 ハードウェア設置ガイドに従ってネットワークモジュールを交換します。ファイアウォールの電源がオンの状態でネットワークモジュールを交換できます。

クラスタリングまたはフェールオーバーの場合は、すべてのノードにネットワークモジュールをインストールします。

ステップ 4 ファイアウォールをリロードします。[ツール（Tools）]>[システムのリロード（System Reload）] を参照してください。

クラスタリングまたはフェールオーバーの場合は、すべてのノードをリロードします。ネットワークモジュールが異なるノードはクラスタ/フェールオーバーペアに参加できないため、クラスタ/フェールオーバーペアを再作成する前に、新しいモジュールですべてのノードをリロードする必要があります。

ステップ 5 再ロードの前に設定を保存した場合は、モジュールを再有効化する必要があります。

ネットワーク モジュールの取り外し

ネットワークモジュールを完全に削除する場合は、次の手順に従います。ネットワークモジュールを削除するには、リロードが必要です。クラスタリングまたはフェールオーバーの場合、ゼロダウンタイムはサポートされないため、この手順は必ずメンテナンスウィンドウ中に実行してください。

始める前に

クラスタリングまたはフェールオーバーの場合、クラスタ/フェールオーバーリンクがネットワークモジュール上にないことを確認してください。この場合、モジュールを削除することはできません。

手順

ステップ 1 [設定（Configuration）] > [デバイス管理（Device Management）] > [詳細（Advanced）] > [EPM] の順に選択し、[NetModの無効化（Disable Netmod）] をオンにしてネットワークモジュールを無効化します。

クラスタリングまたはフェールオーバーの場合は、制御ノード/アクティブユニットでこの手順を実行します。モジュールの状態は他のノードに複製されます。

ステップ 2 [適用（Apply）]、[保存（Save）] の順にクリックします。

ファイアウォールに設定が保存されます。

ステップ 3 ハードウェア設置ガイドに従ってネットワークモジュールを削除します。ファイアウォールの電源がオンの状態でネットワークモジュールを削除できます。

クラスタリングまたはフェールオーバーの場合は、すべてのノードのネットワークモジュールを削除します。

ステップ 4 ファイアウォールをリロードします。[ツール（Tools）]>[システムのリロード（System Reload）]を参照してください。

クラスタリングまたはフェールオーバーの場合は、すべてのノードをリロードします。ネットワークモジュールが異なるノードはクラスタ/フェールオーバーペアに参加できないため、クラスタ/フェールオーバーペアを再作成する前に、モジュールのないすべてのノードをリロードする必要があります。

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 *3:* インターフェイスの履歴

機能名	リリース	機能情報
Secure Firewall 3100 固定ポートのデフォルトの前方誤り訂正（FEC）が、25 GB+ SR、CSR、および LR トランシーバの cl74-fc から cl108-rs に変更されました	9.18(3)/9.19(1)	Secure Firewall 3100 の固定ポートで FEC を Auto に設定すると、25 GB SR、CSR、および LR トランシーバのデフォルトのタイプが cl74-fc ではなく cl108-rs に設定されるようになりました。 新規/変更された画面：**[設定（Configuration）]** > **[デバイスのセットアップ（Device Setup）]** > **[インターフェイスの設定（Interface Settings）]** > **[インターフェイス（Interfaces）]** > **[インターフェイスの編集（Edit Interface）]** > **[ハードウェアプロパティの構成（Configure Hardware Properties）]** > **[FECモード（FEC Mode）]**
Cisco Secure Firewall 3100 のフロー制御に対応するためのフレームの一時停止	9.18(1)	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。 新規/変更された画面：**[設定（Configuration）]** > **[デバイス設定（Device Setup）]** > **[インターフェイス（Interface）]** > **[全般（General）]**
Secure Firewall 3130 および 3140 のブレークアウトポート	9.18(1)	Cisco Secure Firewall 3130 および 3140 の 40 GB インターフェースごとに 4 つの 10 GB ブレークアウトポートを構成できるようになりました。 新規/変更された画面：**[設定（Configuration）]** > **[デバイス管理（Device Management）]** > **[詳細（Advanced）]** > **[EPM]**
Cisco Secure Firewall 3100 におけるネットワークモジュールのホットスワップのサポート	9.17(1)	Cisco Secure Firewall 3100 では、ファイアウォールの電源がオンの状態でネットワークモジュールを追加または削除できます。モジュールを同じタイプの別のモジュールに交換する場合、再起動は必要ありません。最初の起動の後にモジュールを追加するか、モジュールを完全に削除するか、モジュールを新しいタイプのモジュールに交換する場合は、再起動が必要です。 新しい/変更された画面： **[Configuration]** > **[Device Management]** > **[Advanced]** > **[EPM]**

機能名	リリース	機能情報
Cisco Secure Firewall 3100 における前方誤り訂正のサポート	9.17(1)	Cisco Secure Firewall 3100 25 Gbps インターフェイスは、前方誤り訂正（FEC）をサポートします。FEC はデフォルトで有効になっており、[自動（Auto）] に設定されています。 新しい/変更された画面： **[Configuration] > [Device Settings] > [Interfaces] > [Edit Interface] > [Configure Hardware Properties]**
Cisco Secure Firewall 3100 における SFP に基づく速度設定のサポート	9.17(1)	Cisco Secure Firewall 3100 は、インストールされている SFP に基づくインターフェイスの速度検出をサポートします。SFP の検出はデフォルトで有効になっています。このオプションは、後でネットワークモジュールを別のモデルに変更し、速度を自動的に更新する場合に便利です。 新しい/変更された画面： **[Configuration] > [Device Settings] > [Interfaces] > [Edit Interface] > [Configure Hardware Properties]**
Secure Firewall 3100 の自動ネゴシエーションは、1 ギガビット以上のインターフェイスで有効または無効にすることができます。	9.17(1)	Secure Firewall 3100 の自動ネゴシエーションは、1 ギガビット以上のインターフェイスについて、速度とは別に有効または無効にすることができます。 新規/変更された画面： **[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Advanced]**
Firepower 1100 および 2100 の光ファイバ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 光ファイバ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/変更された画面：**[構成（Configuration）] > [デバイスの設定（Device Settings）] > [インターフェイス（Interfaces）] > [インターフェイスの編集（Edit Interface）] > [ハードウェアプロパティの構成（Configure Hardware Properties）] > [速度（Speed）]**
ASA 仮想 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)	ASA 仮想 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 ASA 仮想 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 ASA 仮想 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に設定できますが、デフォルトでは管理専用に設定されていません。

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。 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)] [Configuration] > [Interfaces] > [Add/Edit Interface]
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。 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)] [Configuration] > [Interfaces] > [Add/Edit Interface]
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。 次の画面が変更されました。[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add/Edit Interface] > [Advanced]。
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 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。

基本インターフェイスの設定の履歴

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。