



## インターフェイス管理

---

- [インターフェイスについて \(1 ページ\)](#)
- [インターフェイスに関する注意事項と制約事項 \(21 ページ\)](#)
- [インターフェイスの設定 \(24 ページ\)](#)
- [モニタリング インターフェイス \(35 ページ\)](#)
- [インターフェイスのトラブルシューティング \(38 ページ\)](#)
- [インターフェイスの履歴 \(44 ページ\)](#)

## インターフェイスについて

Firepower 4100/9300 シャーシは、物理インターフェイス、コンテナインスタンス用の VLAN サブインターフェイス、および EtherChannel (ポートチャネル) インターフェイスをサポートします。EtherChannel のインターフェイスには、同じタイプのメンバインターフェイスを最大で 16 個含めることができます。

## シャーシ管理インターフェイス

シャーシ管理インターフェイスは、SSH または シャーシマネージャ によって、FXOS シャーシの管理に使用されます。このインターフェイスは、アプリケーション管理の論理デバイスに割り当てる管理タイプのインターフェイスから分離されています。

このインターフェイスのパラメータを設定するには、CLI から設定にする必要があります。[管理 IP アドレスの変更](#)も参照してください。このインターフェイスについての情報を FXOS CLI で表示するには、ローカル管理に接続し、管理ポートを表示します。

**FirePOWER connect local-mgmt**

```
firepower(local-mgmt) # show mgmt-port
```

物理ケーブルまたは SFP モジュールが取り外されている場合や **mgmt-port shut** コマンドが実行されている場合でも、シャーシ管理インターフェイスは稼働状態のままである点に注意してください。



(注) シャーシ管理インターフェイスはジャンボフレームをサポートしていません。

## インターフェイスタイプ

物理インターフェイス、コンテナインスタンスの VLAN サブインターフェイス、および EtherChannel (ポートチャネル) インターフェイスは、次のいずれかのタイプになります。

- **Data** : 通常のデータに使用します。データインターフェイスを論理デバイス間で共有することはできません。また、論理デバイスからバックプレーンを介して他の論理デバイスに通信することはできません。データインターフェイスのトラフィックの場合、すべてのトラフィックは別の論理デバイスに到達するために、あるインターフェイスでシャーシを抜け出し、別のインターフェイスで戻る必要があります。
- **Data-sharing** : 通常のデータに使用します。コンテナインスタンスでのみサポートされ、これらのデータインターフェイスは1つまたは複数の論理デバイス/コンテナインスタンス (脅威に対する防御 **Management Center** 専用) で共有できます。各コンテナインスタンスは、このインターフェイスを共有する他のすべてのインスタンスと、バックプレーン経由で通信できます。共有インターフェイスは、展開可能なコンテナインスタンスの数に影響することがあります。共有インターフェイスは、ブリッジグループメンバーインターフェイス (トランスペアレントモードまたはルーテッドモード)、インラインセット、パッシブインターフェイス、クラスタ、またはフェールオーバーリンクではサポートされません。
- **Mgmt** : アプリケーションインスタンスの管理に使用します。これらのインターフェイスは、外部ホストにアクセスするために1つまたは複数の論理デバイスで共有できます。論理デバイスが、このインターフェイスを介して、インターフェイスを共有する他の論理デバイスと通信することはできません。各論理デバイスには、管理インターフェイスを1つだけ割り当てることができます。アプリケーションと管理によっては、後でデータインターフェイスから管理を有効にできます。ただし、データ管理を有効にした後で使用する予定がない場合でも、管理インターフェイスを論理デバイスに割り当てる必要があります。



(注) 管理インターフェイスを変更すると、論理デバイスが再起動します。たとえば、e1/1 から e1/2 に1回変更すると、論理デバイスが再起動して新しい管理が適用されます。

- **Eventing** : **Management Center** デバイスを使用した 脅威に対する防御 のセカンダリ管理インターフェイスとして使用します。このインターフェイスを使用するには、脅威に対する防御 CLI で IP アドレスなどのパラメータを設定する必要があります。たとえば、イベント (Web イベントなど) から管理トラフィックを分類できます。詳細については、[管理センター構成ガイド](#)を参照してください。Eventing インターフェイスは、外部ホストにアクセスするために1つまたは複数の論理デバイスで共有できます。論理デバイスはこのイン

ターフェイスを介してインターフェイスを共有する他の論理デバイスと通信することはできません。後で管理用のデータインターフェイスを設定する場合は、別のイベントインターフェイスを使用できません。



- (注) 各アプリケーションインスタンスのインストール時に、仮想イーサネットインターフェイスが割り当てられます。アプリケーションがイベントインターフェイスを使用しない場合、仮想インターフェイスは管理上ダウンの状態になります。

```
Firepower # show interface Vethernet775
Firepower # Vethernet775 is down (Administratively down)
Bound Interface is Ethernet1/10
Port description is server 1/1, VNIC ext-mgmt-nic5
```

- **Cluster** : クラスタ化された論理デバイスのクラスタ制御リンクとして使用します。デフォルトでは、クラスタ制御リンクは 48 番のポートチャンネル上に自動的に作成されます。クラスタタイプは、**EtherChannel** インターフェイスのみでサポートされます。マルチインスタンスクラスタリングの場合、デバイス間でクラスタタイプのインターフェイスを共有することはできません。各クラスタが別個のクラスタ制御リンクを使用できるように、クラスタ **EtherChannel** に VLAN サブインターフェイスを追加できます。クラスタインターフェイスにサブインターフェイスを追加した場合、そのインターフェイスをネイティブクラスタには使用できません。Device Manager および CDO はクラスタリングをサポートしていません。



- (注) この章では、**FXOS VLAN** サブインターフェイスについてのみ説明します。Threat Defense アプリケーション内でサブインターフェイスを個別に作成できます。詳細については、[FXOS インターフェイスとアプリケーションインターフェイス \(5 ページ\)](#) を参照してください。

スタンドアロン展開とクラスタ展開での Threat Defense および ASA アプリケーションのインターフェイスタイプのサポートについては、次の表を参照してください。

表 1: インターフェイスタイプのサポート

アプリケーション		データ	データ： サブインターフェイス	データ共有	データ共有： サブインターフェイス	管理	イベント (Eventing)	クラスタ (EthaChannelのみ)	クラスタ： サブインターフェイス
<b>Threat Defense</b>	スタンドアロンネイティブインスタンス	対応	—	—	—	対応	対応	—	—
	スタンドアロンコンテナインスタンス	対応	対応	対応	対応	対応	対応	—	—
	クラスタネイティブインスタンス	対応 (シャresh間クラスタ専用のEthaChannel)	—	—	—	対応	対応	対応	—
	クラスタコンテナインスタンス	対応 (シャresh間クラスタ専用のEthaChannel)	—	—	—	対応	対応	対応	対応
<b>ASA</b>	スタンドアロンネイティブインスタンス	対応	—	—	—	対応	—	対応	—
	クラスタネイティブインスタンス	対応 (シャresh間クラスタ専用のEthaChannel)	—	—	—	対応	—	対応	—

## FXOS インターフェイスとアプリケーションインターフェイス

Firepower 4100/9300 は、物理インターフェイス、コンテナインスタンスの VLAN サブインターフェイス、および EtherChannel（ポートチャネル）インターフェイスの基本的なイーサネット設定を管理します。アプリケーション内で、より高いレベルの設定を行います。たとえば、FXOS では Etherchannel のみを作成できます。ただし、アプリケーション内の EtherChannel に IP アドレスを割り当てることができます。

続くセクションでは、インターフェイスの FXOS とアプリケーション間の連携について説明します。

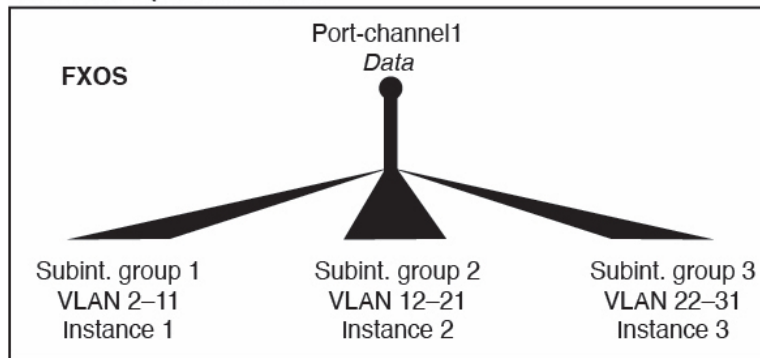
### VLAN サブインターフェイス

すべての論理デバイスで、アプリケーション内に VLAN サブインターフェイスを作成できます。

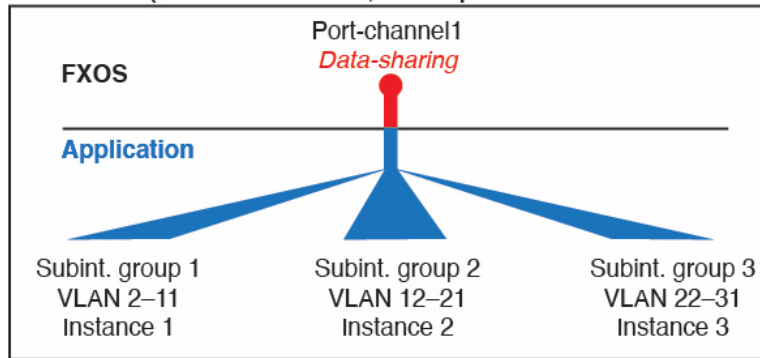
スタンドアロンモードのコンテナインスタンスの場合のみ、FXOS で VLAN サブインターフェイスを作成することもできます。マルチインスタンスクラスタは、クラスタタイプのインターフェイスを除いて、FXOS のサブインターフェイスをサポートしません。アプリケーション定義のサブインターフェイスは、FXOS 制限の対象にはなりません。サブインターフェイスを作成するオペレーティングシステムの選択は、ネットワーク導入および個人設定によって異なります。たとえば、サブインターフェイスを共有するには、FXOS でサブインターフェイスを作成する必要があります。FXOS サブインターフェイスを優先するもう 1 つのシナリオでは、1 つのインターフェイス上の別のサブインターフェイスグループを複数のインスタンスに割り当てます。たとえば、インスタンス A で VLAN 2-11 を、インスタンス B で VLAN 12-21 を、インスタンス C で VLAN 22-31 を使用して Port-Channel1 を使うとします。アプリケーション内でこれらのサブインターフェイスを作成する場合、FXOS 内で親インターフェイスを共有しますが、これはお勧めしません。このシナリオを実現する 3 つの方法については、次の図を参照してください。

図 1: FXOS の VLAN とコンテナインスタンスのアプリケーション

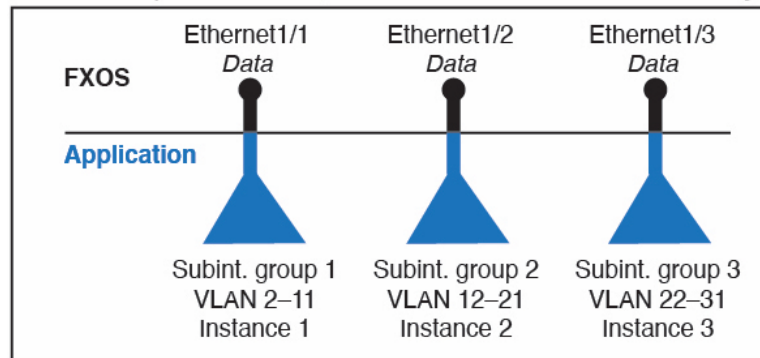
Scenario 1 (recommended)



Scenario 2 (not recommended, worse performance)



Scenario 3 (recommended, but lacks EtherChannel redundancy)



シャーシとアプリケーションの独立したインターフェイスの状態

管理上、シャーシとアプリケーションの両方で、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ため、シャーシとアプリケーションの間で不一致が発生することがあります。

アプリケーション内のインターフェイスのデフォルトの状態は、インターフェイスのタイプによって異なります。たとえば、物理インターフェイスまたは EtherChannel は、アプリケーショ

ン内ではデフォルトで無効になっていますが、サブインターフェイスはデフォルトで有効になっています。

## ハードウェアバイパス ペア

脅威に対する防御 では、Firepower 9300 および 4100 シリーズの特定のインターフェイス モジュールを使用することで、ハードウェアバイパス 機能を有効にできます。ハードウェアバイパス は、停電時にトラフィックがインライン インターフェイス ペア間で流れ続けることを確認します。この機能は、ソフトウェアまたはハードウェア障害の発生時にネットワーク接続を維持するために使用できます。

ハードウェアバイパス 機能は、脅威に対する防御 アプリケーション内で設定されます。これらのインターフェイスをハードウェアバイパス ペアとして使用する必要はありません。これらは、ASA と脅威に対する防御 アプリケーションの両方について通常のインターフェイスとして使用できます。ハードウェアバイパス 対応のインターフェイスをブレイクアウト ポート用に設定することはできないため注意してください。ハードウェアバイパス 機能を使用するには、ポートをEtherChannelとして設定しないでください。そうでない場合は、これらのインターフェイスを通常のインターフェイスモードのEtherChannelメンバとして含めることができます。

ハードウェアバイパス がインラインペアで有効になっている場合、スイッチのバイパスが最初に試行されます。スイッチのエラーが原因でバイパス設定が失敗した場合は、物理バイパスが有効になります。



- (注) ハードウェアバイパス (FTW) は、VDP/Radwareなどのサードパーティ製アプリケーションを使用したサービスチェイニングにインストールされた脅威に対する防御 ではサポートされません。



- (注) 同じインラインセットに対してハードウェアバイパス およびリンクステートの伝達を有効にしないでください。

脅威に対する防御 は、以下のモデルの特定のネットワーク モジュールのインターフェイス ペアでハードウェアバイパス をサポートします。

- Firepower 9300
- Firepower 4100 シリーズ

これらのモデルでサポートされているハードウェアバイパス ネットワーク モジュールは以下のとおりです。

- Firepower 6 ポート 1G SX FTW ネットワーク モジュール シングルワイド (FPR-NM-6X1SX-F)

- Firepower 6 ポート 10G SR FTW ネットワーク モジュール シングルワイド (FPR-NM-6X10SR-F)
- Firepower 6 ポート 10G LR FTW ネットワーク モジュール シングルワイド (FPR-NM-6X10LR-F)
- Firepower 2 ポート 40G SR FTW ネットワーク モジュール シングルワイド (FPR-NM-2X40G-F)
- Firepower 8 ポート 1G Copper FTW ネットワーク モジュール シングルワイド (FPR-NM-8X1G-F)

ハードウェア バイパス では以下のポート ペアのみ使用できます。

- 1 および 2
- 3 および 4
- 5 および 6
- 7 および 8

## ジャンボ フレーム サポート

Firepower 4100/9300 シャーシは、デフォルトで有効になっているジャンボフレームをサポートします。Firepower 4100/9300 シャーシにインストールされた特定の論理デバイスのジャンボフレームサポートを有効にするには、論理デバイスのインターフェイスに適切な MTU の設定を構成する必要があります。

Firepower 4100/9300 シャーシのアプリケーションでサポートされている最大 MTU は、9184 です。



---

(注) シャーシ管理インターフェイスはジャンボフレームをサポートしていません。

---

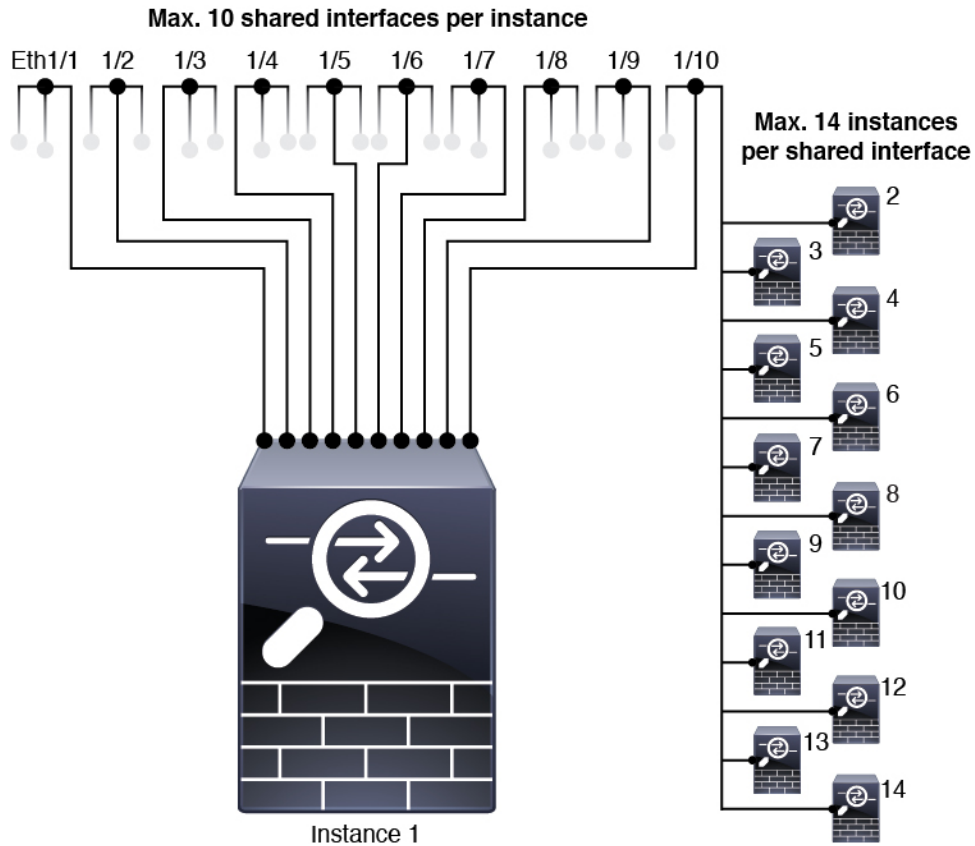
## 共有インターフェイスの拡張性

インスタンスは、データ共有タイプのインターフェイスを共有できます。この機能を使用して、物理インターフェイスの使用率を節約し、柔軟なネットワークの導入をサポートできます。インターフェイスを共有すると、シャーシは一意の MAC アドレスを使用して、正しいインスタンスにトラフィックを転送します。ただし、共有インターフェイスでは、シャーシ内にフルメッシュトポロジが必要になるため、転送テーブルが大きくなることがあります（すべてのインスタンスが、同じインターフェイスを共有するその他すべてのインスタンスと通信できる必要があります）。そのため、共有できるインターフェイスの数には制限があります。

転送テーブルに加えて、シャーシは VLAN サブインターフェイスの転送用に VLAN グループテーブルも保持します。最大 500 個の VLAN サブインターフェイスを作成できます。



共有インターフェイスの割り当てに次の制限を参照してください。



## 共有インターフェイスのベストプラクティス

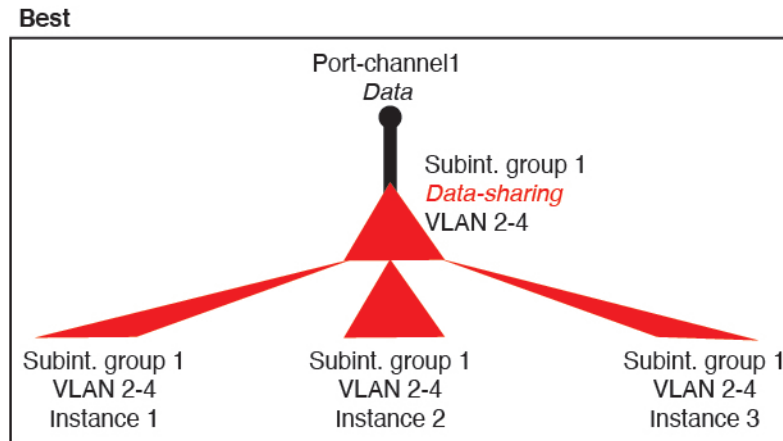
転送テーブルの拡張性を最適にするには、共有するインターフェイスの数をできる限り少なくします。代わりに、1つまたは複数の物理インターフェイスに最大 500 個の VLAN サブインターフェイスを作成し、コンテナインスタンスで VLAN を分割できます。

インターフェイスを共有する場合は、拡張性の高いものから低いものの順に次の手順を実行します。

1. 最適：単一の親の下のサブインターフェイスを共有し、インスタンスグループと同じサブインターフェイスのセットを使用します。

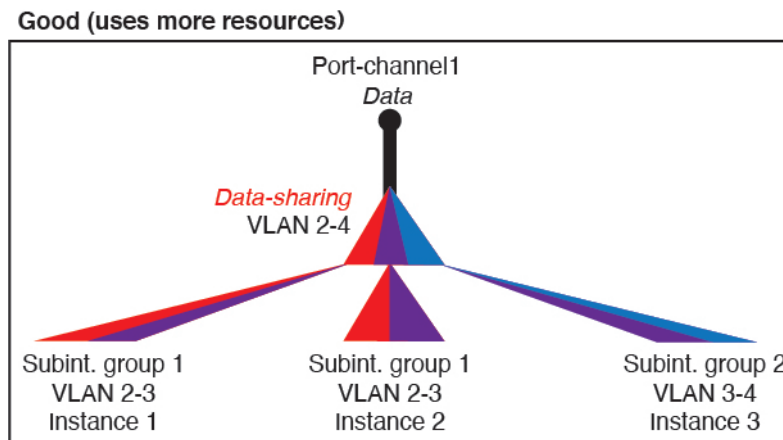
たとえば、同じ種類のインターフェイスをすべてバンドルするための大規模な EtherChannel を作成し、Port-Channel2、Port-Channel3、Port-Channel4 の代わりに、その EtherChannel のサブインターフェイス (Port-Channel1.2、3、4) を共有します。単一の親のサブインターフェイスを共有する場合、物理/EtherChannel インターフェイスまたは複数の親にわたるサブインターフェイスを共有するときの VLAN グループ テーブルの拡張性は転送テーブルよりも優れています。

図 2:最適 : 単一の親のサブインターフェイスグループを共有



インスタンスグループと同じサブインターフェイスのセットを共有しない場合は、(VLAN グループよりも) より多くのリソースを設定で使用する可能性があります。たとえば、Port-Channel1.2 および 3 をインスタンス 1 および 2 と共有するとともに Port-Channel1.3 および 4 をインスタンス 3 と共有する (2つの VLAN グループ) のではなく、Port-Channel1.2、3、および 4 をインスタンス 1、2、および 3 と共有 (1つの VLAN グループ) します。

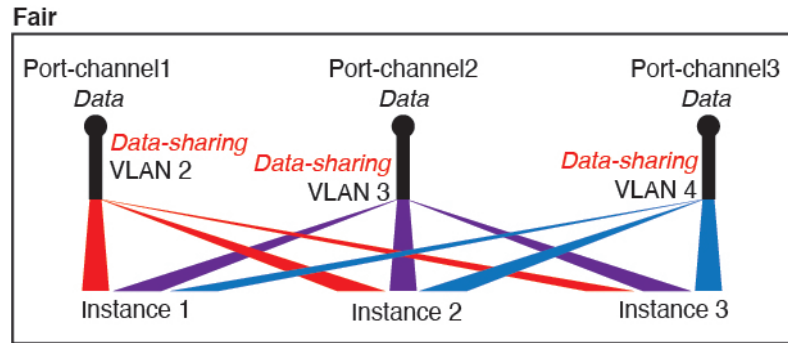
図 3:良好 : 単一の親の複数のサブインターフェイスグループを共有



2. 普通 : 親の間でサブインターフェイスを共有します。

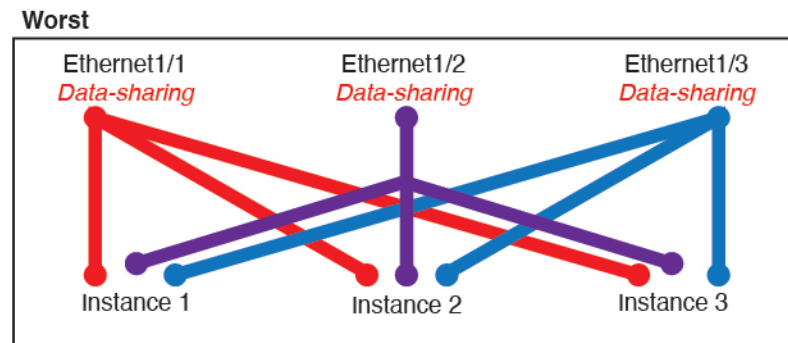
たとえば、Port-Channel2、Port-Channel4、およびPort-Channel4ではなく、Port-Channel1.2、Port-Channel2.3、およびPort-Channel3.4を共有します。この使用法は同じ親のサブインターフェイスのみを共有するよりも効率は劣りますが、VLAN グループを利用しています。

図 4: 普通 : 個別の親のサブインターフェイスを共有



3. 最悪 : 個々の親インターフェイス (物理または EtherChannel) を共有します。この方法は、最も多くの転送テーブル エントリを使用します。

図 5: 最悪 : 親インターフェイスを共有



## 共有インターフェイスの使用状況の例

インターフェイスの共有と拡張性の例について、以下の表を参照してください。以下のシナリオは、すべてのインスタンス間で共有されている管理用の 1 つの物理/EtherChannel インターフェイスと、ハイアベイラビリティで使用する専用のサブインターフェイスを含むもう 1 つの物理/EtherChannel インターフェイスを使用していることを前提としています。

- 表 2 : 3 つの SM-44 を備えた Firepower 9300 の物理/EtherChannel インターフェイスとインスタンス (12 ページ)
- 表 3 : 3 つの SM-44 を備えた Firepower 9300 上の 1 つの親のサブインターフェイスとインスタンス (14 ページ)
- 表 4 : 1 つの SM-44 を備えた Firepower 9300 の物理/EtherChannel インターフェイスとインスタンス (16 ページ)
- 表 5 : 1 つの SM-44 を備えた Firepower 9300 上の 1 つの親のサブインターフェイスとインスタンス (18 ページ)

### 3つの SM-44 と firepower 9300

次の表は、物理インターフェイスまたはEtherchannelのみを使用している 9300 の SM-44 セキュリティモジュールに適用されます。サブインターフェイスがなければ、インターフェイスの最大数が制限されます。さらに、複数の物理インターフェイスを共有するには、複数のサブインターフェイスを使用するよりも多くの転送テーブルリソースを使用します。

各 SM-44 モジュールは、最大 14 のインスタンスをサポートできます。インスタンスは、制限内に収める必要に応じてモジュール間で分割されます。

表 2: 3つの SM-44 を備えた Firepower 9300 の物理/EtherChannel インターフェイスとインスタンス

専用インターフェイス	共有インターフェイス	インスタンス数	転送テーブルの使用率 (%)
<b>32 :</b> <ul style="list-style-type: none"> <li>• 8</li> <li>• 8</li> <li>• 8</li> <li>• 8</li> </ul>	<b>0</b>	<b>4 :</b> <ul style="list-style-type: none"> <li>• インスタンス 1</li> <li>• インスタンス 2</li> <li>• インスタンス 3</li> <li>• インスタンス 4</li> </ul>	16 %
<b>30 :</b> <ul style="list-style-type: none"> <li>• 15</li> <li>• 15</li> </ul>	<b>0</b>	<b>2:</b> <ul style="list-style-type: none"> <li>• インスタンス 1</li> <li>• インスタンス 2</li> </ul>	14%
<b>14 :</b> <ul style="list-style-type: none"> <li>• 14 (各 1)</li> </ul>	<b>1</b>	<b>14 :</b> <ul style="list-style-type: none"> <li>• インスタンス 1-インスタンス 14</li> </ul>	46 %
<b>33 :</b> <ul style="list-style-type: none"> <li>• 11 (各 1)</li> <li>• 11 (各 1)</li> <li>• 11 (各 1)</li> </ul>	<b>3 :</b> <ul style="list-style-type: none"> <li>• 1</li> <li>• 1</li> <li>• 1</li> </ul>	<b>33 :</b> <ul style="list-style-type: none"> <li>• インスタンス 1-インスタンス 11</li> <li>• インスタンス 12 - インスタンス 22</li> <li>• インスタンス 23 - インスタンス 33</li> </ul>	98%

専用インターフェイス	共有インターフェイス	インスタンス数	転送テーブルの使用率 (%)
<b>33 :</b> <ul style="list-style-type: none"> <li>• 11 (各 1)</li> <li>• 11 (各 1)</li> <li>• 12 (各 1)</li> </ul>	<b>3 :</b> <ul style="list-style-type: none"> <li>• 1</li> <li>• 1</li> <li>• 1</li> </ul>	<b>34 :</b> <ul style="list-style-type: none"> <li>• インスタンス 1 - インスタンス 11</li> <li>• インスタンス 12 - インスタンス 22</li> <li>• インスタンス 23 - インスタンス 34</li> </ul>	102 % 許可しない
<b>30 :</b> <ul style="list-style-type: none"> <li>• 30 (各 1)</li> </ul>	<b>1</b>	<b>6 :</b> <ul style="list-style-type: none"> <li>• インスタンス 1 - インスタンス 6</li> </ul>	25 %
<b>30 :</b> <ul style="list-style-type: none"> <li>• 10 (各 5)</li> <li>• 10 (各 5)</li> <li>• 10 (各 5)</li> </ul>	<b>3 :</b> <ul style="list-style-type: none"> <li>• 1</li> <li>• 1</li> <li>• 1</li> </ul>	<b>6 :</b> <ul style="list-style-type: none"> <li>• インスタンス 1 - インスタンス 2</li> <li>• インスタンス 2 - インスタンス 4</li> <li>• インスタンス 5 - インスタンス 6</li> </ul>	23 %
<b>30 :</b> <ul style="list-style-type: none"> <li>• 30 (各 6)</li> </ul>	<b>2</b>	<b>5 :</b> <ul style="list-style-type: none"> <li>• インスタンス 1 - インスタンス 5</li> </ul>	28%
<b>30 :</b> <ul style="list-style-type: none"> <li>• 12 (各 6)</li> <li>• 18 (各 6)</li> </ul>	<b>4 :</b> <ul style="list-style-type: none"> <li>• 2</li> <li>• 2</li> </ul>	<b>5 :</b> <ul style="list-style-type: none"> <li>• インスタンス 1 - インスタンス 2</li> <li>• インスタンス 2 - インスタンス 5</li> </ul>	26 %

専用インターフェイス	共有インターフェイス	インスタンス数	転送テーブルの使用率 (%)
<b>24 :</b> <ul style="list-style-type: none"> <li>• 6</li> <li>• 6</li> <li>• 6</li> <li>• 6</li> </ul>	<b>7</b>	<b>4 :</b> <ul style="list-style-type: none"> <li>• インスタンス 1</li> <li>• インスタンス 2</li> <li>• インスタンス 3</li> <li>• インスタンス 4</li> </ul>	44 %
<b>24 :</b> <ul style="list-style-type: none"> <li>• 12 (各 6)</li> <li>• 12 (各 6)</li> </ul>	<b>14 :</b> <ul style="list-style-type: none"> <li>• 7</li> <li>• 7</li> </ul>	<b>4 :</b> <ul style="list-style-type: none"> <li>• インスタンス 1-インスタンス 2</li> <li>• インスタンス 2-インスタンス 4</li> </ul>	41%

次の表は、単一の親物理インターフェイス上でサブインターフェイスを使用している 9300 上の3つの SM-44 セキュリティモジュールに適用されます。たとえば、同じ種類のインターフェイスをすべてバンドルするための大規模な EtherChannel を作成し、EtherChannel のサブインターフェイスを共有します。複数の物理インターフェイスを共有するには、複数のサブインターフェイスを使用するよりも多くの転送テーブルリソースを使用します。

各 SM-44 モジュールは、最大 14 のインスタンスをサポートできます。インスタンスは、制限内に収める必要に応じてモジュール間で分割されます。

表 3: 3つの SM-44 を備えた Firepower 9300 上の 1 つの親のサブインターフェイスとインスタンス

専用サブインターフェイス	共有サブインターフェイス	インスタンス数	転送テーブルの使用率 (%)
<b>168 :</b> <ul style="list-style-type: none"> <li>• 168 (4 ea.)</li> </ul>	<b>0</b>	<b>42 :</b> <ul style="list-style-type: none"> <li>• インスタンス 1-インスタンス 42</li> </ul>	33%
<b>224 :</b> <ul style="list-style-type: none"> <li>• 224 (16 ea.)</li> </ul>	<b>0</b>	<b>14 :</b> <ul style="list-style-type: none"> <li>• インスタンス 1-インスタンス 14</li> </ul>	27 %
<b>14 :</b> <ul style="list-style-type: none"> <li>• 14 (各 1)</li> </ul>	<b>1</b>	<b>14 :</b> <ul style="list-style-type: none"> <li>• インスタンス 1-インスタンス 14</li> </ul>	46 %

専用サブインターフェイス	共有サブインターフェイス	インスタンス数	転送テーブルの使用率 (%)
<b>33 :</b> <ul style="list-style-type: none"> <li>• 11 (各 1)</li> <li>• 11 (各 1)</li> <li>• 11 (各 1)</li> </ul>	<b>3 :</b> <ul style="list-style-type: none"> <li>• 1</li> <li>• 1</li> <li>• 1</li> </ul>	<b>33 :</b> <ul style="list-style-type: none"> <li>• インスタンス 1 - インスタンス 11</li> <li>• インスタンス 12 - インスタンス 22</li> <li>• インスタンス 23 - インスタンス 33</li> </ul>	98%
<b>70 :</b> <ul style="list-style-type: none"> <li>• 70 (5 ea.)</li> </ul>	<b>1</b>	<b>14 :</b> <ul style="list-style-type: none"> <li>• インスタンス 1 - インスタンス 14</li> </ul>	46 %
<b>165 :</b> <ul style="list-style-type: none"> <li>• 55 (5 ea.)</li> <li>• 55 (5 ea.)</li> <li>• 55 (5 ea.)</li> </ul>	<b>3 :</b> <ul style="list-style-type: none"> <li>• 1</li> <li>• 1</li> <li>• 1</li> </ul>	<b>33 :</b> <ul style="list-style-type: none"> <li>• インスタンス 1 - インスタンス 11</li> <li>• インスタンス 12 - インスタンス 22</li> <li>• インスタンス 23 - インスタンス 33</li> </ul>	98%
<b>70 :</b> <ul style="list-style-type: none"> <li>• 70 (5 ea.)</li> </ul>	<b>2</b>	<b>14 :</b> <ul style="list-style-type: none"> <li>• インスタンス 1 - インスタンス 14</li> </ul>	46 %
<b>165 :</b> <ul style="list-style-type: none"> <li>• 55 (5 ea.)</li> <li>• 55 (5 ea.)</li> <li>• 55 (5 ea.)</li> </ul>	<b>6 :</b> <ul style="list-style-type: none"> <li>• 2</li> <li>• 2</li> <li>• 2</li> </ul>	<b>33 :</b> <ul style="list-style-type: none"> <li>• インスタンス 1 - インスタンス 11</li> <li>• インスタンス 12 - インスタンス 22</li> <li>• インスタンス 23 - インスタンス 33</li> </ul>	98%
<b>70 :</b> <ul style="list-style-type: none"> <li>• 70 (5 ea.)</li> </ul>	<b>10</b>	<b>14 :</b> <ul style="list-style-type: none"> <li>• インスタンス 1 - インスタンス 14</li> </ul>	46 %

専用サブインターフェイス	共有サブインターフェイス	インスタンス数	転送テーブルの使用率 (%)
<b>165 :</b> <ul style="list-style-type: none"> <li>• 55 (5 ea.)</li> <li>• 55 (5 ea.)</li> <li>• 55 (5 ea.)</li> </ul>	<b>30 :</b> <ul style="list-style-type: none"> <li>• 10</li> <li>• 10</li> <li>• 10</li> </ul>	<b>33 :</b> <ul style="list-style-type: none"> <li>• インスタンス 1 - インスタンス 11</li> <li>• インスタンス 12 - インスタンス 22</li> <li>• インスタンス 23 - インスタンス 33</li> </ul>	<b>102 %</b> 許可しない

### 1つの SM 44 を備えた Firepower 9300

次の表は、物理インターフェイスまたは Etherchannel のみを使用している 1 つの SM-44 を備えた Firepower 9300 に適用されます。サブインターフェイスがなければ、インターフェイスの最大数が制限されます。さらに、複数の物理インターフェイスを共有するには、複数のサブインターフェイスを使用するよりも多くの転送テーブルリソースを使用します。

1 つの SM-44 を備えた Firepower 9300 は、最大 14 のインスタンスをサポートできます。

表 4: 1 つの SM-44 を備えた Firepower 9300 の物理/EtherChannel インターフェイスとインスタンス

専用インターフェイス	共有インターフェイス	インスタンス数	転送テーブルの使用率 (%)
<b>32 :</b> <ul style="list-style-type: none"> <li>• 8</li> <li>• 8</li> <li>• 8</li> <li>• 8</li> </ul>	<b>0</b>	<b>4 :</b> <ul style="list-style-type: none"> <li>• インスタンス 1</li> <li>• インスタンス 2</li> <li>• インスタンス 3</li> <li>• インスタンス 4</li> </ul>	<b>16 %</b>
<b>30 :</b> <ul style="list-style-type: none"> <li>• 15</li> <li>• 15</li> </ul>	<b>0</b>	<b>2:</b> <ul style="list-style-type: none"> <li>• インスタンス 1</li> <li>• インスタンス 2</li> </ul>	<b>14%</b>
<b>14 :</b> <ul style="list-style-type: none"> <li>• 14 (各 1)</li> </ul>	<b>1</b>	<b>14 :</b> <ul style="list-style-type: none"> <li>• インスタンス 1 - インスタンス 14</li> </ul>	<b>46 %</b>



専用インターフェイス	共有インターフェイス	インスタンス数	転送テーブルの使用率 (%)
<b>14 :</b> <ul style="list-style-type: none"> <li>• 7 (各 1)</li> <li>• 7 (各 1)</li> </ul>	<b>2:</b> <ul style="list-style-type: none"> <li>• 1</li> <li>• 1</li> </ul>	<b>14 :</b> <ul style="list-style-type: none"> <li>• インスタンス 1-インスタンス 7</li> <li>• インスタンス 8-インスタンス 14</li> </ul>	37 %
<b>32 :</b> <ul style="list-style-type: none"> <li>• 8</li> <li>• 8</li> <li>• 8</li> <li>• 8</li> </ul>	<b>1</b>	<b>4 :</b> <ul style="list-style-type: none"> <li>• インスタンス 1</li> <li>• インスタンス 2</li> <li>• インスタンス 3</li> <li>• インスタンス 4</li> </ul>	21 %
<b>32 :</b> <ul style="list-style-type: none"> <li>• 16 (各 8)</li> <li>• 16 (各 8)</li> </ul>	<b>2</b>	<b>4 :</b> <ul style="list-style-type: none"> <li>• インスタンス 1-インスタンス 2</li> <li>• インスタンス 3-インスタンス 4</li> </ul>	20 %
<b>32 :</b> <ul style="list-style-type: none"> <li>• 8</li> <li>• 8</li> <li>• 8</li> <li>• 8</li> </ul>	<b>2</b>	<b>4 :</b> <ul style="list-style-type: none"> <li>• インスタンス 1</li> <li>• インスタンス 2</li> <li>• インスタンス 3</li> <li>• インスタンス 4</li> </ul>	25 %
<b>32 :</b> <ul style="list-style-type: none"> <li>• 16 (各 8)</li> <li>• 16 (各 8)</li> </ul>	<b>4 :</b> <ul style="list-style-type: none"> <li>• 2</li> <li>• 2</li> </ul>	<b>4 :</b> <ul style="list-style-type: none"> <li>• インスタンス 1-インスタンス 2</li> <li>• インスタンス 3-インスタンス 4</li> </ul>	24 %

専用インターフェイス	共有インターフェイス	インスタンス数	転送テーブルの使用率 (%)
24 : • 8 • 8 • 8	8	3 : • インスタンス 1 • インスタンス 2 • インスタンス 3	37 %
10 : • 10 (各 2)	10	5 : • インスタンス 1-イン タンス 5	69%
10 : • 6 (各 2) • 4 (各 2)	20 : • 10 • 10	5 : • インスタンス 1-イン タンス 3 • インスタンス 4-イン タンス 5	59%
14 : • 12 (2 ea.)	10	7 : • インスタンス 1-イン タンス 7	109% 許可しない

次の表は、単一の親物理インターフェイス上でサブインターフェイスを使用している 1 つの SM-44 を備えた Firepower 4150 に適用されます。たとえば、同じ種類のインターフェイスをすべてバンドルするための大規模な EtherChannel を作成し、EtherChannel のサブインターフェイスを共有します。複数の物理インターフェイスを共有するには、複数のサブインターフェイスを使用するよりも多くの転送テーブルリソースを使用します。

1 つの SM-44 を備えた Firepower 9300 は、最大 14 のインスタンスをサポートできます。

表 5: 1 つの SM-44 を備えた Firepower 9300 上の 1 つの親のサブインターフェイスとインスタンス

専用サブインターフェイス	共有サブインターフェイス	インスタンス数	転送テーブルの使用率 (%)
112 : • 112 (各 8)	0	14 : • インスタンス 1-イン タンス 14	17%

専用サブインターフェイス	共有サブインターフェイス	インスタンス数	転送テーブルの使用率 (%)
224 : • 224 (16 ea.)	0	14 : • インスタンス 1-インスタンス 14	17%
14 : • 14 (各 1)	1	14 : • インスタンス 1-インスタンス 14	46 %
14 : • 7 (各 1) • 7 (各 1)	2: • 1 • 1	14 : • インスタンス 1-インスタンス 7 • インスタンス 8-インスタンス 14	37 %
112 : • 112 (各 8)	1	14 : • インスタンス 1-インスタンス 14	46 %
112 : • 56 (各 8) • 56 (各 8)	2: • 1 • 1	14 : • インスタンス 1-インスタンス 7 • インスタンス 8-インスタンス 14	37 %
112 : • 112 (各 8)	2	14 : • インスタンス 1-インスタンス 14	46 %
112 : • 56 (各 8) • 56 (各 8)	4 : • 2 • 2	14 : • インスタンス 1-インスタンス 7 • インスタンス 8-インスタンス 14	37 %

専用サブインターフェイス	共有サブインターフェイス	インスタンス数	転送テーブルの使用率 (%)
<b>140 :</b> <ul style="list-style-type: none"> <li>• 140 (各 10)</li> </ul>	<b>10</b>	<b>14 :</b> <ul style="list-style-type: none"> <li>• インスタンス 1-インスタンス 14</li> </ul>	46 %
<b>140 :</b> <ul style="list-style-type: none"> <li>• 70 (各 10)</li> <li>• 70 (各 10)</li> </ul>	<b>20 :</b> <ul style="list-style-type: none"> <li>• 10</li> <li>• 10</li> </ul>	<b>14 :</b> <ul style="list-style-type: none"> <li>• インスタンス 1-インスタンス 7</li> <li>• インスタンス 8-インスタンス 14</li> </ul>	37 %

## 共有インターフェイス リソースの表示

転送テーブルと VLAN グループの使用状況を表示するには、`show detail` コマンドを入力し **scope fabric-interconnect** ます。次に例を示します。

```
Firepower# scope fabric-interconnect
Firepower /fabric-interconnect # show detail

Fabric Interconnect:
  ID: A
  Product Name: Cisco FPR9K-SUP
  PID: FPR9K-SUP
  VID: V02
  Vendor: Cisco Systems, Inc.
  Serial (SN): JAD104807YN
  HW Revision: 0
  Total Memory (MB): 16185
  OOB IP Addr: 10.10.5.14
  OOB Gateway: 10.10.5.1
  OOB Netmask: 255.255.255.0
  OOB IPv6 Address: ::
  OOB IPv6 Gateway: ::
  Prefix: 64
  Operability: Operable
  Thermal Status: Ok
  Ingress VLAN Group Entry Count (Current/Max): 0/500
  Switch Forwarding Path Entry Count (Current/Max): 16/1021
  Current Task 1:
  Current Task 2:
  Current Task 3:
```

## Threat Defense のインラインセット リンク ステート伝達サポート

インラインセットはワイヤ上のバンプのように動作し、2つのインターフェイスを一緒にバインドし、既存のネットワークに組み込みます。この機能によって、隣接するネットワークデバイスの設定がなくても、任意のネットワーク環境にシステムをインストールすることができま

す。インラインインターフェイスはすべてのトラフィックを無条件に受信しますが、これらのインターフェイスで受信されたすべてのトラフィックは、明示的にドロップされない限り、インラインセットの外部に再送信されます。

脅威に対する防御 アプリケーションでインラインセットを設定し、リンクステート伝達を有効にすると、脅威に対する防御はインラインセットメンバーシップをFXOSシャーシに送信します。リンクステート伝達により、インラインセットのインターフェイスの1つが停止した場合、シャーシは、インラインインターフェイスペアの2番目のインターフェイスも自動的に停止します。停止したインターフェイスが再び起動すると、2番目のインターフェイスも自動的に起動します。つまり、1つのインターフェイスのリンクステートが変化すると、シャーシはその変化を検知し、その変化に合わせて他のインターフェイスのリンクステートを更新します。ただし、シャーシからリンクステートの変更が伝達されるまで最大4秒かかります。障害状態のネットワークデバイスを避けてトラフィックを自動的に再ルーティングするようルータが設定された復元力の高いネットワーク環境では、リンクステート伝播が特に有効です。



- 
- (注) 同じインラインセットに対してハードウェアバイパスおよびリンクステートの伝達を有効にしないでください。
- 

## インターフェイスに関する注意事項と制約事項

### VLAN サブインターフェイス

- 本書では、FXOS VLAN サブインターフェイスについてのみ説明します。Threat Defense アプリケーション内でサブインターフェイスを個別に作成できます。詳細については、[FXOS インターフェイスとアプリケーションインターフェイス \(5 ページ\)](#) を参照してください。
- サブインターフェイス（および親インターフェイス）はコンテナインスタンスにのみ割り当てることができます。



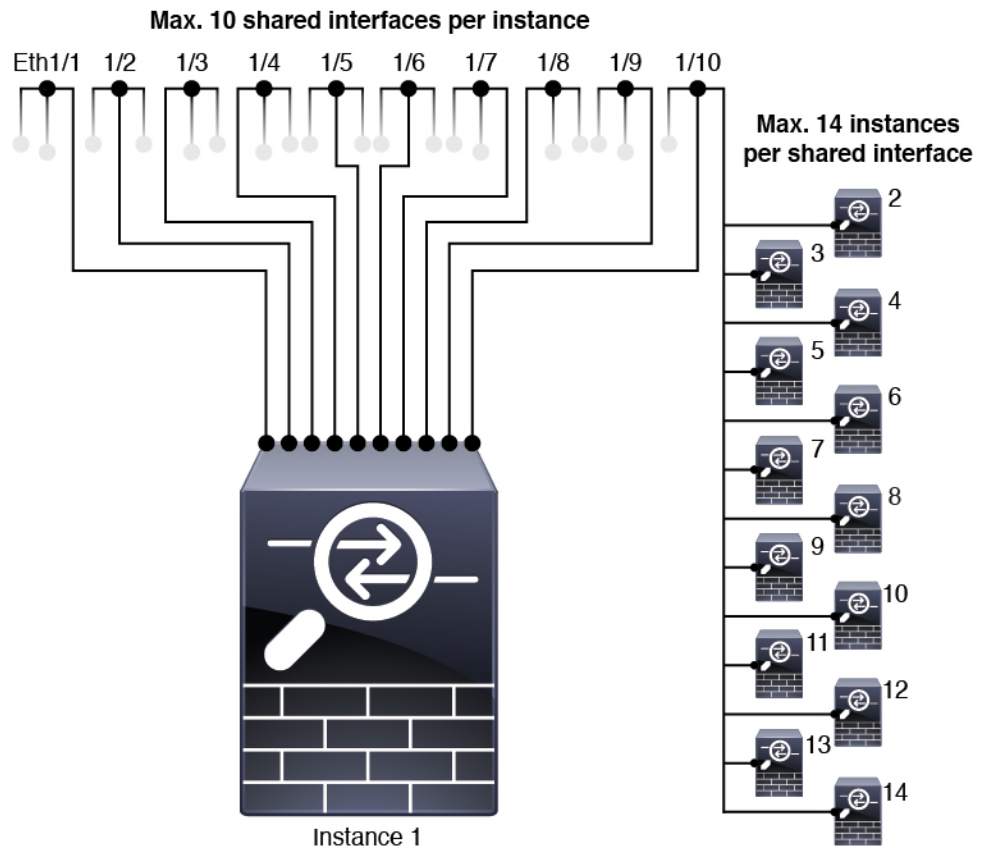
- 
- (注) コンテナインスタンスに親インターフェイスを割り当てる場合、タグなし（非VLAN）トラフィックのみを渡します。タグなしトラフィックを渡す必要がない限り、親インターフェイスを割り当てないでください。クラスタタイプのインターフェイスの場合、親インターフェイスを使用することはできません。
- 

- サブインターフェイスはデータまたはデータ共有タイプのインターフェイス、およびクラスタタイプのインターフェイスでサポートされます。クラスタインターフェイスにサブインターフェイスを追加した場合、そのインターフェイスをネイティブクラスタには使用できません。

- マルチインスタンス クラスタリングの場合、データインターフェイス上の FXOS サブインターフェイスはサポートされません。ただし、クラスタ制御リンクではサブインターフェイスがサポートされているため、クラスタ制御リンクには専用の EtherChannel または EtherChannel のサブインターフェイスを使用できます。アプリケーション定義のサブインターフェイスは、データインターフェイスでサポートされていることに注意してください。
- 最大 500 個の VLAN ID を作成できます。
- 論理デバイスアプリケーション内での次の制限事項を確認し、インターフェイスの割り当てを計画する際には留意してください。
  - 脅威に対する防御 インラインセットに、またはパッシブインターフェイスとしてサブインターフェイスを使用することはできません。
  - フェールオーバーリンクに対してサブインターフェイスを使用する場合、その親にあるすべてのサブインターフェイスと親自体のフェールオーバーリンクとしての使用が制限されます。一部のサブインターフェイスをフェールオーバーリンクとして、一部を通常のデータインターフェイスとして使用することはできません。

#### データ共有インターフェイス

- ネイティブインスタンスではデータ共有インターフェイスを使用することはできません。
- 共有インターフェイスごとの最大インスタンス数：14。たとえば、Instance1 ～ Instance14 に Ethernet1/1 を割り当てることができます。  
インスタンスごとの最大共有インターフェイス数：10 たとえば、Ethernet1/1.10 を介して Instance1 に Ethernet1/1.1 を割り当てることができます。



- クラスタではデータ共有インターフェイスを使用することはできません。
- 論理デバイスアプリケーション内での次の制限事項を確認し、インターフェイスの割り当てを計画する際には留意してください。
  - トランスペアレントファイアウォールモードデバイスでデータ共有インターフェイスを使用することはできません。
  - 脅威に対する防御 インラインセットでまたはパッシブインターフェイスとしてデータ共有インターフェイスを使用することはできません。
  - フェールオーバーリンクに対してデータ共有インターフェイスを使用することはできません。

#### 次に対するインラインセット Threat Defense

- 物理インターフェイス（通常かつブレイクアウトポート）と Etherchannel のサポート。サブインターフェイスはサポートされません。
- リンクステートの伝達はサポートされます。
- 同じインラインセットに対してハードウェアバイパスおよびリンクステートの伝達を有効にしないでください。

### ハードウェアバイパス

- 脅威に対する防御 をサポート。ASA の通常のインターフェイスとして使用できます。
- 脅威に対する防御 はインラインセットでのみハードウェアバイパスをサポートします。
- ハードウェア バイパス 対応のインターフェイスをブレイクアウト ポート用に設定することはできません。
- ハードウェア バイパス インターフェイスを EtherChannel に含めたり、ハードウェア バイパス用に使用することはできません。EtherChannel で通常のインターフェイスとして使用できます。
- ハードウェア バイパス は高可用性ではサポートされません。
- 同じインラインセットに対して ハードウェア バイパス およびリンクステートの伝達を有効にしないでください。

### デフォルトの MAC アドレス

#### ネイティブインスタンス向け：

デフォルトの MAC アドレスの割り当ては、インターフェイスのタイプによって異なります。

- 物理インターフェイス：物理インターフェイスは Burned-In MAC Address を使用します。
- EtherChannel：EtherChannel の場合は、そのチャネルグループに含まれるすべてのインターフェイスが同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワークアプリケーションとユーザに対してトランスペアレントになります。ネットワークアプリケーションやユーザから見えるのは1つの論理接続のみであり、個々のリンクのことは認識しないためです。ポート チャネルインターフェイスは、プールからの一意の MAC アドレスを使用します。インターフェイスのメンバーシップは、MAC アドレスには影響しません。

#### コンテナインスタンス向け：

- すべてのインターフェイスの MAC アドレスは MAC アドレス プールから取得されます。サブインターフェイスでは、MAC アドレスを手動で設定する場合、分類が正しく行われるように、同じ親インターフェイス上のすべてのサブインターフェイスで一意の MAC アドレスを使用します。[コンテナ インスタンス インターフェイスの自動 MAC アドレス](#) を参照してください。

## インターフェイスの設定

デフォルトでは、物理インターフェイスは無効になっています。インターフェイスを有効にし、EtherChannels を追加して、VLAN サブインターフェイスを追加し、インターフェイスプロパティを編集、ブレイクアウト ポートを設定できます。





(注)

## 物理インターフェイスの設定

インターフェイスを物理的に有効および無効にすること、およびインターフェイスの速度とデュプレックスを設定することができます。インターフェイスを使用するには、インターフェイスをFXOSで物理的に有効にし、アプリケーションで論理的に有効にする必要があります。



(注) QSFPH40G-CUxMの場合、自動ネゴシエーションはデフォルトで常に有効になっており、無効にすることはできません。

### 始める前に

- すでに EtherChannel のメンバーであるインターフェイスは個別に変更できません。EtherChannel に追加する前に、設定を行ってください。

### 手順

**ステップ 1** インターフェイスモードに入ります。

```
scope eth-uplink
```

```
scope fabric a
```

**ステップ 2** インターフェイスを有効にします。

```
enter interface interface_id
```

```
enable
```

例 :

```
Firepower /eth-uplink/fabric # enter interface Ethernet1/8  
Firepower /eth-uplink/fabric/interface # enable
```

(注) すでにポートチャネルのメンバであるインターフェイスは個別に変更できません。ポートチャネルのメンバーであるインターフェイスで **enter interface** コマンドまたは **scope interface** コマンドを使用すると、オブジェクトが存在しないことを示すエラーを受け取ります。ポートチャネルに追加する前に、**enter interface** コマンドを使用してインターフェイスを編集する必要があります。

**ステップ 3** (任意) デバウンス時間を設定します。

```
set debounce-time 5000 {Enter a value between 0-15000 milli-seconds}
```

例：

```
Firepower /eth-uplink/fabric/interface # set debounce-time 5000
```

**ステップ 4** (オプション) インターフェイスタイプを設定します。

```
set port-type {data | data-sharing | mgmt | firepower-eventing | cluster}
```

例：

```
Firepower /eth-uplink/fabric/interface # set port-type mgmt
```

**data** キーワードがデフォルトのタイプです。**data-sharing** タイプは、コンテナインスタンスでのみサポートされます。**cluster** キーワードは選択しないでください。デフォルトでは、クラスター制御リンクはポートチャネル 48 に自動的に作成されます。

**ステップ 5** インターフェイスでサポートされている場合、自動ネゴシエーションを有効化または無効化します。

```
set auto-negotiation {on | off}
```

例：

```
Firepower /eth-uplink/fabric/interface* # set auto-negotiation off
```

**ステップ 6** インターフェイスの速度を設定します。

```
set admin-speed {10mbps | 100mbps | 1gbps | 10gbps | 40gbps | 100gbps}
```

例：

```
Firepower /eth-uplink/fabric/interface* # set admin-speed 1gbps
```

**ステップ 7** インターフェイスのデュプレックスモードを設定します。

```
set admin-duplex {fullduplex | halfduplex}
```

例：

```
Firepower /eth-uplink/fabric/interface* # set admin-duplex halfduplex
```

**ステップ 8** デフォルトのフロー制御ポリシーを編集した場合は、インターフェイスにすでに適用されています。新しいポリシーを作成した場合は、そのポリシーをインターフェイスに適用します。[フロー制御ポリシーの設定 \(33 ページ\)](#) を参照してください。

```
set flow-control-policy name
```

例：

```
Firepower /eth-uplink/fabric/interface* # set flow-control-policy flow1
```

**ステップ 9** 設定を保存します。

### commit-buffer

例：

```
Firepower /eth-uplink/fabric/interface* # commit-buffer
Firepower /eth-uplink/fabric/interface #
```

## EtherChannel (ポートチャネル) の追加

EtherChannel (ポートチャネルとも呼ばれる) は、同じメディアタイプと容量の最大16個のメンバーインターフェイスを含むことができ、同じ速度とデュプレックスに設定する必要があります。メディアタイプはRJ-45またはSFPのいずれかです。異なるタイプ (銅と光ファイバ) のSFPを混在させることができます。容量の大きいインターフェイスで速度を低く設定することによってインターフェイスの容量 (1GBインターフェイスと10GBインターフェイスなど) を混在させることはできません。リンク集約制御プロトコル (LACP) では、2つのネットワークデバイス間でリンク集約制御プロトコルデータユニット (LACPDU) を交換することによって、インターフェイスが集約されます。

EtherChannel内の各物理データまたはデータ共有インターフェイスを次のように設定できます。

- アクティブ：LACP アップデートを送信および受信します。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。
- オン：EtherChannel は常にオンであり、LACP は使用されません。「オン」の EtherChannel は、別の「オン」の EtherChannel のみと接続を確立できます。



(注) モードを [On] から [Active] に変更するか、[Active] から [On] に変更すると、EtherChannel が動作状態になるまで最大3分かかることがあります。

非データ インターフェイスのみがアクティブ モードをサポートしています。

LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバーインターフェイスの両端が正しいチャネルグループに接続されていることがチェックされます。「オン」モードではインターフェイスがダウンしたときにチャネルグループ内のスタンバイ インターフェイスを使用できず、接続とコンフィギュレーションはチェックされません。

Firepower 4100/9300 シャーシが EtherChannel を作成すると、EtherChannel は [一時停止 (Suspended)] 状態 (Active LACP モードの場合) または [ダウン (Down)] 状態 (On LACP モードの場合) になり、物理リンクがアップしても論理デバイスに割り当てられるまでそのままになります。EtherChannel は次のような状況でこの [一時停止 (Suspended)] 状態になります。

- EtherChannel がスタンドアロン論理デバイスのデータまたは管理インターフェイスとして追加された

- EtherChannel がクラスタの一部である論理デバイスの管理インターフェイスまたは Cluster Control Link として追加された
- EtherChannel がクラスタの一部である論理デバイスのデータインターフェイスとして追加され、少なくとも 1 つのユニットがクラスタに参加している

EtherChannel は論理デバイスに割り当てるまで動作しないことに注意してください。EtherChannel が論理デバイスから削除された場合や論理デバイスが削除された場合は、EtherChannel が [一時停止 (Suspended) ] または [ダウン (Down) ] 状態に戻ります。

## 手順

**ステップ 1** インターフェイス モードを開始します。

```
scope eth-uplink
```

```
scope fabric a
```

**ステップ 2** ポートチャネルを作成します。

```
create port-channel ID
```

```
enable
```

**ステップ 3** メンバインターフェイスを割り当てます。

```
create member-port interface_id
```

同じメディアタイプとキャパシティで最大 16 のインターフェイスを追加できます。メンバーインターフェイスは、同じ速度とデュプレックスに設定する必要があります。このポートチャネルに設定した速度とデュプレックスと一致させる必要があります。メディアタイプは RJ-45 または SFP のいずれかです。異なるタイプ (銅と光ファイバ) の SFP を混在させることができます。容量の大きいインターフェイスで速度を低く設定することによってインターフェイスの容量 (1GB インターフェイスと 10GB インターフェイスなど) を混在させることはできません。

例 :

```
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
```

**ステップ 4** (任意) インターフェイス タイプを設定します。

```
set port-type {data | data-sharing | mgmt | firepower-eventing | cluster}
```

例 :

```
Firepower /eth-uplink/fabric/port-channel # set port-type data
```

**data** キーワードがデフォルトのタイプです。**data-sharing** タイプは、コンテナインスタンスでのみサポートされます。デフォルトの代わりにこのポートチャネルをクラスター制御リンクとして使用する場合以外は、**cluster** キーワードを選択しないでください。

**ステップ 5** ポートチャネルのメンバーに適したインターフェイス速度を設定します。

```
set speed {10mbps | 100mbps | 1gbps | 10gbps | 40gbps | 100gbps}
```

指定した速度ではないメンバーインターフェイスを追加すると、ポートチャネルに正常に参加できません。デフォルトは **10gbps** です。

例：

```
Firepower /eth-uplink/fabric/port-channel* # set speed 1gbps
```

**ステップ 6** (任意) ポートチャネルのメンバーに適したデュプレックスを設定します。

```
set duplex {fullduplex | halfduplex}
```

指定したデュプレックスのメンバーインターフェイスを追加すると、ポートチャネルに正常に参加されます。デフォルトは **fullduplex** です。

例：

```
Firepower /eth-uplink/fabric/port-channel* # set duplex fullduplex
```

**ステップ 7** インターフェイスでサポートされている場合、自動ネゴシエーションを有効化または無効化します。

```
set auto-negotiation {on | off}
```

例：

```
Firepower /eth-uplink/fabric/interface* # set auto-negotiation off
```

**ステップ 8** データとデータ共有インターフェイスの LACP ポートチャネルモードを設定します。非データおよび非データ共有インターフェイスの場合、モードは常にアクティブです。

```
set port-channel-mode {active | on}
```

例：

```
Firepower /eth-uplink/fabric/port-channel* # set port-channel-mode on
```

**ステップ 9** デフォルトのフロー制御ポリシーを編集した場合は、インターフェイスにすでに適用されています。新しいポリシーを作成した場合は、そのポリシーをインターフェイスに適用します。[フロー制御ポリシーの設定 \(33 ページ\)](#) を参照してください。

```
set flow-control-policy name
```

例：

```
Firepower /eth-uplink/fabric/interface* # set flow-control-policy flow1
```

**ステップ 10** 設定をコミットします。

**commit-buffer**

## コンテナ インスタンスの VLAN サブインターフェイスの追加

シャーシには最大 500 個のサブインターフェイスを追加できます。

マルチインスタンス クラスターリングの場合、クラスタタイプのインターフェイスにサブインターフェイスを追加するだけです。データインターフェイス上のサブインターフェイスはサポートされません。

インターフェイスごとの VLAN ID は一意である必要があります。コンテナインスタンス内では、VLAN ID は割り当てられたすべてのインターフェイス全体で一意である必要があります。異なるコンテナ インターフェイスに割り当てられている限り、VLAN ID を別のインターフェイス上で再利用できます。ただし、同じ ID を使用していても、各サブインターフェイスが制限のカウント対象になります。

本書では、FXOS VLAN サブインターフェイスについてのみ説明します。Threat Defense アプリケーション内でサブインターフェイスを個別に作成できます。

手順

**ステップ 1** fabric a モードを開始します。

**scope eth-uplink**

**scope fabric a**

例：

```
Firepower# scope eth-uplink
Firepower /eth-uplink # scope fabric a
Firepower /eth-uplink/fabric #
```

**ステップ 2** サブインターフェイスに追加するインターフェイスを入力します。

**enter {interface | port-channel} interface\_id**

現在論理デバイスに割り当てられている物理インターフェイスにサブインターフェイスを追加することはできません。親の他のサブインターフェイスが割り当てられている場合、その親インターフェイス自体が割り当てられていない限り、新しいサブインターフェイスを追加できます。

サブインターフェイスはデータまたはデータ共有タイプのインターフェイス、およびクラスタータイプのインターフェイスでサポートされます。

例：

```
Firepower /eth-uplink/fabric # enter interface Ethernet1/8
Firepower /eth-uplink/fabric/interface #
```

**ステップ 3** サブインターフェイスを作成します。

**enter subinterface *id***

- *id* : 1 ~ 4294967295 で ID を設定します。この ID は、*interface\_id.subinterface\_id* のように親インターフェイスの ID に追加されます。たとえば、サブインターフェイスを ID 100 でイーサネット 1/1 に追加する場合、そのサブインターフェイス ID はイーサネット 1/1.100 になります。利便性を考慮して一致するように設定することができますが、この ID は VLAN ID と同じではありません。

例：

```
Firepower /eth-uplink/fabric/interface # enter subinterface 100
Firepower /eth-uplink/fabric/interface/subinterface* #
```

**ステップ 4** [VLAN] を設定します。

**set vlan *id***

- [*id*] : 1 ~ 4095 の間で VLAN ID を設定します。

例：

```
Firepower /eth-uplink/fabric/interface/subinterface* # set vlan 100
```

**ステップ 5** インターフェイス タイプを設定します。

**set port-type {*data* | *data-sharing* | *cluster*}**

例：

```
Firepower /eth-uplink/fabric/interface/subinterface* # set port-type data
```

データインターフェイスおよびデータ共有インターフェイスの場合：タイプは、親インターフェイスのタイプに依存しません。たとえば、データ共有の親とデータサブインターフェイスを設定できます。デフォルトのタイプは *Dtata* です。

**ステップ 6** 設定を保存します。

**commit-buffer**

例：

```
Firepower /eth-uplink/fabric/interface/subinterface* # commit-buffer
```

```
Firepower /eth-uplink/fabric/interface/subinterface #
```

### 例

次に、イーサネット 1/1 上の 3 つのサブインターフェイスを作成し、データ共有インターフェイスに設定する例を示します。

```
Firepower# scope eth-uplink
Firepower /eth-uplink # scope fabric a
Firepower /eth-uplink/fabric # enter interface Ethernet1/1
Firepower /eth-uplink/fabric/interface # enter subinterface 10
Firepower /eth-uplink/fabric/interface/subinterface* # set vlan 10
Firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
Firepower /eth-uplink/fabric/interface/subinterface* # exit
Firepower /eth-uplink/fabric/interface # enter subinterface 11
Firepower /eth-uplink/fabric/interface/subinterface* # set vlan 11
Firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
Firepower /eth-uplink/fabric/interface/subinterface* # exit
Firepower /eth-uplink/fabric/interface # enter subinterface 12
Firepower /eth-uplink/fabric/interface/subinterface* # set vlan 12
Firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
Firepower /eth-uplink/fabric/interface/subinterface* # commit-buffer
Firepower /eth-uplink/fabric/interface/subinterface #
```

## ブレイクアウト ケーブルの設定

Firepower 4100/9300 シャーシで使用するブレイクアウトケーブルを設定するには、次の手順に従います。ブレイクアウトケーブルを使用すると、1 つの 40 Gbps ポートの代わりに 4 つの 10 Gbps ポートを実装できます。

### 始める前に

ハードウェア バイパス 対応のインターフェイスをブレイクアウト ポート用に設定することはできません。

### 手順

**ステップ 1** 新しいブレイクアウトを作成するには、次のコマンドを使用します。

- a) ケーブル接続モードを開始します。

```
scope cabling
```

```
scope fabric a
```

- b) ブレイクアウトを作成します。

```
create breakout network_module_slot port
```



例：

```
Firepower /cabling/fabric/ # create breakout 2 1
```

- c) 設定をコミットします。

#### **commit-buffer**

これにより自動リブートが実行されます。複数のブレイクアウトを設定する場合、**commit-buffer** コマンドを発行する前にそれらすべてを作成する必要があります。

**ステップ 2** ブレイクアウト ポートを有効化または設定するには、次のコマンドを使用します。

- a) インターフェイス モードを開始します。

#### **scope eth-uplink**

#### **scope fabric a**

#### **scope aggr-interface network\_module\_slot port**

(注) すでにポートチャネルのメンバであるインターフェイスは個別に変更できません。ポートチャネルのメンバーであるインターフェイスで **enter interface** コマンドまたは **scope interface** コマンドを使用すると、オブジェクトが存在しないことを示すエラーを受け取ります。ポートチャネルに追加する前に、**enter interface** コマンドを使用してインターフェイスを編集する必要があります。

- b) インターフェイス速度およびポート タイプを設定するには、**set** コマンドを使用します。インターフェイスの管理状態を設定するには、**enable** または **disable** コマンドを使用します。
- c) 設定をコミットします。

#### **commit-buffer**

## フロー制御ポリシーの設定

フロー制御ポリシーは、ポートの受信バッファがいっぱいになったときに、イーサネットポートが IEEE 802.3x ポーズフレームを送受信するかどうかを決定します。これらのポーズフレームは、バッファがクリアされるまでの数ミリ秒間、送信側ポートからのデータの送信を停止するように要求します。フロー制御をデバイス間で稼働状態にするには、対応する送受信フロー制御パラメータを両方のデバイスで有効にする必要があります。

デフォルトポリシーは、送受信の制御を無効にし、自動ネゴシエーションに優先順位を設定します。

## 手順

**ステップ1** イーサネットアップリンクを入力してから、フロー制御モードを入力します。

**scope eth-uplink**

**scope flow-control**

例：

```
firepower-4110# scope eth-uplink
firepower-4110 /eth-uplink # scope flow-control
firepower-4110 /eth-uplink/flow-control #
```

**ステップ2** フロー制御ポリシーを編集または作成します。

**enter policy name**

デフォルトポリシーを編集する場合、名前に **default** と入力します。

例：

```
firepower-4110 /eth-uplink/flow-control # enter policy default
firepower-4110 /eth-uplink/flow-control/policy* #
```

**ステップ3** 優先順位を設定します。

**set prio {auto | on}**

優先順位は、ネゴシエートするかどうか、またはこのリンクのPPPを有効にするかどうかを設定します。

例：

```
firepower-4110 /eth-uplink/flow-control/policy* # set prio on
```

**ステップ4** フロー制御受信ポーズを有効または無効にします。

**set receive {on | off}**

- **on** : ポーズ要求に従います。ネットワークでポーズ要求が取り消されるまで、そのアップリンクポート上のすべてのトラフィックが停止されます。
- **off** : ネットワークからのポーズ要求が無視され、トラフィックフローは正常に続行されます。

例：

```
firepower-4110 /eth-uplink/flow-control/policy* # set receive on
```

**ステップ5** フロー制御送信ポーズを有効または無効にします。

**set send {on | off}**

- [on] : 着信パケットレートが高くなり過ぎると、Firepower 4100/9300 からポーズ要求がネットワークに送信されます。ポーズは数ミリ秒有効になった後、通常のレベルにリセットされます。
- [off] : パケット負荷に関係なくポート上のトラフィックが通常どおり流れます。

例 :

```
firepower-4110 /eth-uplink/flow-control/policy* # set send on
```

**ステップ 6** 設定を保存します。

**commit-buffer**

例 :

```
firepower-4110 /eth-uplink/flow-control/policy* # commit-buffer
firepower-4110 /eth-uplink/flow-control/policy #
```

例

次の例では、フロー制御ポリシーを設定します。

```
firepower-4110# scope eth-uplink
firepower-4110 /eth-uplink # scope flow-control
firepower-4110 /eth-uplink/flow-control # enter policy FlowControlPolicy23
firepower-4110 /eth-uplink/flow-control/policy* # set prio auto
firepower-4110 /eth-uplink/flow-control/policy* # set receive on
firepower-4110 /eth-uplink/flow-control/policy* # set send on
firepower-4110 /eth-uplink/flow-control/policy* # commit-buffer
firepower-4110 /eth-uplink/flow-control/policy #
```

## モニタリング インターフェイス



(注) 脅威に対する防御/ASAでのフラグメンテーションドロップにより、FXOSと脅威に対する防御/ASAのインターフェイス使用率に違いが生じることがあります。フラグメンテーションドロップを表示するには、脅威に対する防御/ASAの **show asp drop** コマンドと **show fragment** コマンドを参照してください。

• **show interface**

インターフェイス ステータスを表示します。



(注) ポートチャネルのポートとして機能するインターフェイスは、このリストに表示されません。

```
Firepower# scope eth-uplink
Firepower /eth-uplink # scope fabric a
Firepower /eth-uplink/fabric # show interface
```

Interface:

Port Name	Port Type	Admin State	Oper State
Allowed Vlan	State Reason		
Ethernet1/2	Data	Enabled	Up
All			
Ethernet1/4	Mgmt	Enabled	Up
All			
Ethernet1/5	Data	Enabled	Up
Untagged			
Ethernet1/7	Firepower Eventing	Enabled	Up
All			
Ethernet1/8	Data	Disabled	Sfp Not
Present All	Unknown		
Ethernet2/1	Data	Disabled	Sfp Not
Present All	Unknown		
Ethernet2/2	Data	Disabled	Sfp Not
Present All	Unknown		
Ethernet2/3	Data	Disabled	Sfp Not
Present All	Unknown		
Ethernet2/4	Data	Disabled	Sfp Not
Present All	Unknown		
Ethernet2/5	Data	Disabled	Sfp Not
Present All	Unknown		
Ethernet2/6	Data	Disabled	Sfp Not
Present All	Unknown		
Ethernet2/7	Data	Disabled	Sfp Not
Present All	Unknown		
Ethernet2/8	Data	Disabled	Sfp Not
Present All	Unknown		

• show port-channel

ポートチャネルのステータスを表示します。

```
Firepower# scope eth-uplink
Firepower /eth-uplink # scope fabric a
Firepower /eth-uplink/fabric # show port-channel
```

Port Channel:

Port Channel Id	Name	Port Type	Admin State	Oper State
Port Channel Mode	Allowed Vlan	State Reason		
1	Port-channel1	Data	Enabled	Up
Active	Untagged			
2	Port-channel2	Data	Enabled	Failed
Active	All	No operational members		
48	Port-channel48	Cluster	Enabled	Up

Active All

• **show detail**

共有インターフェイスの転送テーブルおよび VLAN グループの使用状況を表示します。

```
Firepower# scope fabric-interconnect
DFirepower /fabric-interconnect # show detail

Fabric Interconnect:
  ID: A
  Product Name: Cisco FPR9K-SUP
  PID: FPR9K-SUP
  VID: V02
  Vendor: Cisco Systems, Inc.
  Serial (SN): JAD104807YN
  HW Revision: 0
  Total Memory (MB): 16185
  OOB IP Addr: 10.10.5.14
  OOB Gateway: 10.10.5.1
  OOB Netmask: 255.255.255.0
  OOB IPv6 Address: ::
  OOB IPv6 Gateway: ::
  Prefix: 64
  Operability: Operable
  Thermal Status: Ok
  Ingress VLAN Group Entry Count (Current/Max): 0/500
  Switch Forwarding Path Entry Count (Current/Max): 16/1021
  Current Task 1:
  Current Task 2:
  Current Task 3:
```

• **show subinterface**

特定のインターフェイスのサブインターフェイスを表示します。

```
Firepower# scope eth-uplink
Firepower /eth-uplink # scope fabric a
Firepower /eth-uplink/fabric # enter interface ethernet1/8
Firepower /eth-uplink/fabric/interface # show subinterface
Sub Interface:
  Sub-If Id  Sub-Interface Name  VLAN      Port Type
  -----  -
           10 Ethernet1/8.10          11        Data
           11 Ethernet1/8.11          12        Data
```

• **show mac-address**

コンテナ インスタンス インターフェイスの MAC アドレスの割り当てを表示します。

```
Firepower# scope ssa
Firepower /ssa # scope auto-macpool
Firepower /ssa/auto-macpool # show mac-address
Mac Address Item:
  Mac Address      Owner Profile      Owner Name
  -----
  A2:46:C4:00:00:1E  ftd13              Port-channel14
  A2:46:C4:00:00:20  ftd14              Port-channel15
  A2:46:C4:00:01:7B  ftd1                Ethernet1/3
```

A2:46:C4:00:01:7C	ftd12	Port-channel11
A2:46:C4:00:01:7D	ftd13	Port-channel14
A2:46:C4:00:01:7E	ftd14	Port-channel15
A2:46:C4:00:01:7F	ftd1	Ethernet1/2
A2:46:C4:00:01:80	ftd12	Ethernet1/2
A2:46:C4:00:01:81	ftd13	Ethernet1/2
A2:46:C4:00:01:82	ftd14	Ethernet1/2
A2:46:C4:00:01:83	ftd2	Ethernet3/1/4
A2:46:C4:00:01:84	ftd2	Ethernet3/1/1
A2:46:C4:00:01:85	ftd2	Ethernet3/1/3
A2:46:C4:00:01:86	ftd2	Ethernet3/1/2
A2:46:C4:00:01:87	ftd2	Ethernet1/2
A2:46:C4:00:01:88	ftd1	Port-channel21
A2:46:C4:00:01:89	ftd1	Ethernet1/8

## インターフェイスのトラブルシューティング

エラー：スイッチの転送パスに**1076**のエントリがあり、**1024**の制限を超えています。インターフェイスを追加する場合は、論理デバイスに割り当てられている共有インターフェイスの数を減らすか、論理デバイス共有インターフェイスの数を減らすか、または共有されていないサブインターフェイスを使用します。サブインターフェイスを削除すると、このメッセージが表示されます。これは、残りの設定が **[Switch Forwarding Path]** テーブル内に収まるように最適化されなくなったためです。削除の使用例に関するトラブルシューティング情報については、**FXOS** コンフィギュレーションガイドを参照してください。'scope fabric-interconnect' の 'show detail' を使用して、現在の **[Switch Forwarding Path Entry Count]** を表示します。

論理デバイスから共有サブインターフェイスを削除しようとしたときにこのエラーが表示される場合は、新しい設定が共有サブインターフェイス向けのこのガイドラインに従っていないためです。同じ論理デバイスのグループと同じサブインターフェイスのセットを使用します。1つの論理デバイスから共有サブインターフェイスを削除すると、さらに多くの VLAN グループを作成できるため、転送テーブルの使用効率が低くなります。この状況に対処するには、CLIを使用して共有サブインターフェイスを同時に追加および削除し、同じ論理デバイスのグループに対して同じサブインターフェイスのセットを維持する必要があります。

詳細については、次のシナリオを参照してください。これらのシナリオは、次のインターフェイスと論理デバイスから始まります。

- 同じ親で設定された共有サブインターフェイス：Port-Channel1.100 (VLAN 100)、Port-Channel1.200 (VLAN 200)、Port-Channel1.300 (VLAN 300)
- 論理デバイス グループ：LD1、LD2、LD3、LD4

**シナリオ 1**：あるサブインターフェイスを1つの論理デバイスから削除するが、他の論理デバイスに割り当てられたままにする

サブインターフェイスは削除しないでください。アプリケーション設定で無効にするだけでください。サブインターフェイスを削除する必要がある場合は、一般に共有インターフェイスの数を減らして、転送テーブルに収まるようにする必要があります。

**シナリオ 2**：1つの論理デバイスからセット内のすべてのサブインターフェイスを削除する

CLIで論理デバイスからセット内のすべてのサブインターフェイスを削除した後、設定を保存して、削除が同時に実行されるようにします。

1. 参照用の VLAN グループを表示します。次の出力では、グループ 1 には、3 つの共有サブインターフェイスを表す VLAN 100、200、300 が含まれています。

```
firepower# connect fxos
[...]
firepower(fxos)# show ingress-vlan-groups
ID   Class ID  Status      INTF      Vlan Status
1    1          configured
                                100 present
                                200 present
                                300 present

2048 512      configured
                                0   present

2049 511      configured
                                0   present

firepower(fxos)# exit
firepower#
```

2. 変更する論理デバイスに割り当てられている共有サブインターフェイスを表示します。

```
firepower# scope ssa
firepower /ssa # scope logical-device LD1
firepower /ssa/logical-device # show external-port-link

External-Port Link:
  Name          Port or Port Channel Name Port Type      App
  Name          Description
  -----
  Ethernet14_ftd      Ethernet1/4          Mgmt          ftd
  PC1.100_ftd         Port-channel1.100   Data Sharing  ftd
  PC1.200_ftd         Port-channel1.200   Data Sharing  ftd
  PC1.300_ftd         Port-channel1.300   Data Sharing  ftd
```

3. 論理デバイスからサブインターフェイスを削除した後、設定を保存します。

```
firepower /ssa/logical-device # delete external-port-link PC1.100_ftd
firepower /ssa/logical-device* # delete external-port-link PC1.200_ftd
firepower /ssa/logical-device* # delete external-port-link PC1.300_ftd
firepower /ssa/logical-device* # commit-buffer
firepower /ssa/logical-device #
```

途中で設定を確定すると、2 つの VLAN グループが存在する結果になります。これにより、スイッチ転送パス エラーが発生し、設定を保存できなくなる場合があります。

### シナリオ 3 : グループ内のすべての論理デバイスから 1 つのサブインターフェイスを削除する

CLIでグループ内のすべての論理デバイスからサブインターフェイスを削除した後、設定を保存して、削除が同時に実行されるようにします。次に例を示します。

1. 参照用の VLAN グループを表示します。次の出力では、グループ 1 には、3 つの共有サブインターフェイスを表す VLAN 100、200、300 が含まれています。

```
firepower# connect fxos
[...]
firepower(fxos)# show ingress-vlan-groups
ID   Class ID   Status          INTF          Vlan Status
---  ---  ---  ---  ---
1    1          configured
                                100 present
                                200 present
                                300 present
2048 512       configured
                                0   present
2049 511       configured
                                0   present
```

2. 各論理デバイスに割り当てられているインターフェイスを表示し、共通の共有サブインターフェイスに注目してください。同じ親インターフェイス上に存在する場合、それらは1つのVLANグループに属し、**show ingress-vlan-groups** リストと一致しているはずです。シャーシマネージャでは、各共有サブインターフェイスにカーソルを合わせて、割り当てられているインスタンスを確認できます。

図 6: 共有インターフェイスごとのインスタンス

Interface	Type	Admin Speed	Operational Speed	Instances	VLAN
MGMT	Management				
Port-channel1	data	1gbps	1gbps		
Port-channel1.100	data-sharing			LD4...	100
Port-channel1.200	data-sharing			LD4...	
Port-channel1.300	data-sharing			LD4...	300
Ethernet1/3					
Port-channel2	data	1gbps	1gbps		

CLI では、割り当てられたインターフェイスを含むすべての論理デバイスの特性を表示できます。

```
firepower# scope ssa
firepower /ssa # show logical-device expand

Logical Device:
  Name: LD1
  Description:
  Slot ID: 1
  Mode: Standalone
  Oper State: Ok
  Template Name: ftd

External-Port Link:
  Name: Ethernet14_ftd
  Port or Port Channel Name: Ethernet1/4
  Port Type: Mgmt
  App Name: ftd
  Description:

  Name: PC1.100_ftd
  Port or Port Channel Name: Port-channel1.100
  Port Type: Data Sharing
```



```
App Name: ftd
Description:

Name: PC1.200_ftd
Port or Port Channel Name: Port-channel1.200
Port Type: Data Sharing
App Name: ftd
Description:

System MAC address:
  Mac Address
  -----
  A2:F0:B0:00:00:25

Name: PC1.300_ftd
Port or Port Channel Name: Port-channel1.300
Port Type: Data Sharing
App Name: ftd
Description:
```

[...]

```
Name: LD2
Description:
Slot ID: 1
Mode: Standalone
Oper State: Ok
Template Name: ftd

External-Port Link:
  Name: Ethernet14_ftd
  Port or Port Channel Name: Ethernet1/4
  Port Type: Mgmt
  App Name: ftd
  Description:

  Name: PC1.100_ftd
  Port or Port Channel Name: Port-channel1.100
  Port Type: Data Sharing
  App Name: ftd
  Description:

  Name: PC1.200_ftd
  Port or Port Channel Name: Port-channel1.200
  Port Type: Data Sharing
  App Name: ftd
  Description:

System MAC address:
  Mac Address
  -----
  A2:F0:B0:00:00:28

Name: PC1.300_ftd
Port or Port Channel Name: Port-channel1.300
Port Type: Data Sharing
App Name: ftd
Description:
```

[...]

```
Name: LD3
Description:
Slot ID: 1
```

```
Mode: Standalone
Oper State: Ok
Template Name: ftd

External-Port Link:
  Name: Ethernet14_ftd
  Port or Port Channel Name: Ethernet1/4
  Port Type: Mgmt
  App Name: ftd
  Description:

  Name: PC1.100_ftd
  Port or Port Channel Name: Port-channel1.100
  Port Type: Data Sharing
  App Name: ftd
  Description:

  Name: PC1.200_ftd
  Port or Port Channel Name: Port-channel1.200
  Port Type: Data Sharing
  App Name: ftd
  Description:

System MAC address:
  Mac Address
  -----
  A2:F0:B0:00:00:2B

  Name: PC1.300_ftd
  Port or Port Channel Name: Port-channel1.300
  Port Type: Data Sharing
  App Name: ftd
  Description:

[...]

Name: LD4
Description:
Slot ID: 1
Mode: Standalone
Oper State: Ok
Template Name: ftd

External-Port Link:
  Name: Ethernet14_ftd
  Port or Port Channel Name: Ethernet1/4
  Port Type: Mgmt
  App Name: ftd
  Description:

  Name: PC1.100_ftd
  Port or Port Channel Name: Port-channel1.100
  Port Type: Data Sharing
  App Name: ftd
  Description:

  Name: PC1.200_ftd
  Port or Port Channel Name: Port-channel1.200
  Port Type: Data Sharing
  App Name: ftd
  Description:

System MAC address:
  Mac Address
```

```

-----
A2:F0:B0:00:00:2E

Name: PC1.300_ftd
Port or Port Channel Name: Port-channel1.300
Port Type: Data Sharing
App Name: ftd
Description:

[...]

```

3. 各論理デバイスからサブインターフェイスを削除した後、設定を保存します。

```

firepower /ssa # scope logical device LD1
firepower /ssa/logical-device # delete external-port-link PC1.300_ftd
firepower /ssa/logical-device* # exit
firepower /ssa* # scope logical-device LD2
firepower /ssa/logical-device* # delete external-port-link PC1.300_ftd
firepower /ssa/logical-device* # exit
firepower /ssa* # scope logical-device LD3
firepower /ssa/logical-device* # delete external-port-link PC1.300_ftd
firepower /ssa/logical-device* # exit
firepower /ssa* # scope logical-device LD4
firepower /ssa/logical-device* # delete external-port-link PC1.300_ftd
firepower /ssa/logical-device* # commit-buffer
firepower /ssa/logical-device #

```

途中で設定を確定すると、2つのVLANグループが存在する結果になります。これにより、スイッチ転送パスエラーが発生し、設定を保存できなくなる場合があります。

#### シナリオ 4 : 1つまたは複数の論理デバイスにサブインターフェイスを追加する

CLIでグループ内のすべての論理デバイスにサブインターフェイスを追加し、その後、その追加が同時になるように設定を保存します。

1. 各論理デバイスにサブインターフェイスを追加してから、設定を保存します。

```

firepower# scope ssa
firepower /ssa # scope logical-device LD1
firepower /ssa/logical-device # create external-port-link PC1.400_ftd Port-channel1.400
ftd
firepower /ssa/logical-device/external-port-link* # exit
firepower /ssa/logical-device* # exit
firepower /ssa # scope logical-device LD2
firepower /ssa/logical-device # create external-port-link PC1.400_ftd Port-channel1.400
ftd
firepower /ssa/logical-device/external-port-link* # exit
firepower /ssa/logical-device* # exit
firepower /ssa # scope logical-device LD3
firepower /ssa/logical-device # create external-port-link PC1.400_ftd Port-channel1.400
ftd
firepower /ssa/logical-device/external-port-link* # exit
firepower /ssa/logical-device* # exit
firepower /ssa # scope logical-device LD4
firepower /ssa/logical-device # create external-port-link PC1.400_ftd Port-channel1.400
ftd
firepower /ssa/logical-device/external-port-link* # commit-buffer
firepower /ssa/logical-device/external-port-link #

```

途中で設定を確定すると、2つの VLAN グループが存在する結果になります。これにより、スイッチ転送パス エラーが発生し、設定を保存できなくなる場合があります。

2. Port-Channel1.400 VLAN ID が VLAN グループ 1 に追加されたことを確認できます。

```
firepower /ssa/logical-device/external-port-link # connect fxos
[...]
firepower(fxos)# show ingress-vlan-groups
ID   Class ID  Status          INTF          Vlan Status
1    1          configured
                                     200 present
                                     100 present
                                     300 present
                                     400 present
2048 512       configured
                                     0   present
2049 511       configured
                                     0   present

firepower(fxos)# exit
firepower /ssa/logical-device/external-port-link #
```

## インターフェイスの履歴

機能名	プラットフォームリリース	機能情報
脅威に対する防御 動作リンク状態と物理リンク状態の同期	2.9.1	<p>シャーシでは、脅威に対する防御 動作リンク状態をデータインターフェイスの物理リンク状態と同期できるようになりました。現在、FXOS管理状態がアップで、物理リンク状態がアップである限り、インターフェイスはアップ状態になります。脅威に対する防御 アプリケーションインターフェイスの管理状態は考慮されません。脅威に対する防御 からの同期がない場合は、たとえば、脅威に対する防御 アプリケーションが完全にオンラインになる前に、データインターフェイスが物理的にアップ状態になったり、脅威に対する防御 のシャットダウン開始後からしばらくの間はアップ状態のままになる可能性があります。インラインセットの場合、この状態の不一致によりパケットがドロップされることがあります。これは、脅威に対する防御 が処理できるようになる前に外部ルータが脅威に対する防御 へのトラフィックの送信を開始することがあるためです。この機能はデフォルトで無効になっており、FXOS の論理デバイスごとに有効にできます。</p> <p>(注) この機能は、クラスタリング、コンテナインスタンス、またはRadware vDP デコレータを使用する脅威に対する防御 ではサポートされません。ASA ではサポートされていません。</p> <p>新規/変更された シャーシマネージャ 画面 : [Logical Devices] &gt; [Enable Link State]</p> <p>新規/変更された FXOS コマンド : <b>set link-state-sync enabled</b>、<b>show interface expand detail</b></p>

機能名	プラットフォームリリース	機能情報
クラスタタイプインターフェイスでの VLAN サブインターフェイスのサポート (マルチインスタンス使用のみ)	2.8.1	マルチインスタンスクラスタで使用するために、クラスタタイプのインターフェイスで VLAN サブインターフェイスを作成できるようになりました。各クラスタには一意のクラスタ制御リンクが必要であるため、VLAN サブインターフェイスはこの要件を満たすための簡単な方法を提供します。または、クラスタごとに専用の EtherChannel を割り当てることもできます。複数のクラスタタイプのインターフェイスが許可されるようになりました。  新規/変更されたコマンド： <b>set port type cluster</b>
500 Vlan のサポート (不測事態がない場合)	2.7.1	以前は、親インターフェイスの数とその他の導入の決定事項に応じて、250 から 500 の VLAN がサポートされていました。すべてのケースで 500 の VLAN を使用できるようになりました。
コンテナインスタンスで使用される VLAN サブインターフェイス	2.4.1	柔軟な物理インターフェイスの使用を可能にするため、FXOS で VLAN サブインターフェイスを作成し、複数のインスタンス間でインターフェイスを共有することができます。  (注) 脅威に対する防御 バージョン 6.3 以降が必要です。  新規/変更されたコマンド： <b>create subinterface、set vlan、show interface、show subinterface</b>  新規/変更された Management Center 画面： [デバイス (Devices) ]>[デバイス管理 (Device Management) ]>[編集 (Edit) ]アイコン>[インターフェイス (Interfaces) ]タブ
コンテナインスタンスのデータ共有インターフェイス	2.4.1	柔軟な物理インターフェイスの使用を可能にするため、複数のインスタンス間でインターフェイスを共有することができます。  (注) 脅威に対する防御 バージョン 6.3 以降が必要です。  新規/変更されたコマンド： <b>set port-type data-sharing、show interface</b>
オンモードでのデータ EtherChannel のサポート	2.4.1	データおよびデータ共有 EtherChannel をアクティブ LACP モードまたはオンモードに設定できるようになりました。Etherchannel の他のタイプはアクティブモードのみをサポートします。  新規/変更されたコマンド： <b>set port-channel-mode</b>
脅威に対する防御 インラインセットでの EtherChannel のサポート	2.1(1)	脅威に対する防御 インラインセットで EtherChannel を使用できるようになりました。

機能名	プラットフォームリリース	機能情報
脅威に対する防御 のインラインセットリンクステート伝達サポート	2.0(1)	<p>脅威に対する防御 アプリケーションでインラインセットを設定し、リンクステート伝達を有効にすると、脅威に対する防御 はインラインセットメンバーシップをFXOSシャーシに送信します。リンクステート伝達により、インラインセットのインターフェイスの1つが停止した場合、シャーシは、インラインインターフェイス ペアの2番目のインターフェイスも自動的に停止します。</p> <p>新規/変更されたコマンド：<b>show fault  grep link-down、 show interface detail</b></p>
ハードウェア バイパスネットワーク モジュールのサポート 脅威に対する防御	2.0(1)	<p>ハードウェアバイパスは、停電時にトラフィックがインラインインターフェイス ペア間で流れ続けることを確認します。この機能は、ソフトウェアまたはハードウェア障害の発生時にネットワーク接続を維持するために使用できます。</p> <p>新規/変更された Management Center 画面：  <b>[デバイス (Devices) ]&gt;[デバイス管理 (Device Management) ]&gt;[インターフェイス (Interfaces) ]&gt;[物理インターフェイスの編集 (Edit Physical Interface) ]</b></p>
脅威に対する防御 の Firepower イベント タイプ インターフェイス	1.1.4	<p>脅威に対する防御 で使用するために、Firepower イベントとしてインターフェイスを指定できます。このインターフェイスは、脅威に対する防御 デバイスのセカンダリ管理インターフェイスです。このインターフェイスを使用するには、脅威に対する防御 CLI で IP アドレスなどのパラメータを設定する必要があります。たとえば、イベント (Web イベントなど) から管理トラフィックを分類できます。Management Center 構成ガイドのシステム設定の章にある「管理インターフェイス」のセクションを参照してください。</p> <p>新規/変更された FXOS コマンド：<b>set port-type firepower-eventing、 show interface</b></p>

## 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。