



# Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータの管理



(注) バージョン 4.17 以降、Cisco Security Manager は引き続き Cisco Catalyst スイッチの機能をサポートしますが、バグ修正や拡張機能はサポートしていません。

Cisco Security Manager は、Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータにおけるセキュリティ サービスやその他のプラットフォーム固有サービスの管理と設定をサポートします。

VTP トランスペアレント モードまたは VTP クライアント/サーバ モードで設定された Catalyst スイッチおよび 7600 デバイスを管理できます。Security Manager は、デバイスにおける VLAN データベース管理 (VLAN の作成、削除、スイッチ上の VLAN データベース内の VLAN のモニタリングなど) をバイパスすることによって、クライアント/サーバ モードで設定されたスイッチを管理します。

この章は次のトピックで構成されています。

- [Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータにおけるポリシーの検出](#) (2 ページ)
- [Catalyst サマリー情報の表示](#) (3 ページ)
- [Catalyst インターフェイス、VLAN、および VLAN グループの概要の表示](#) (4 ページ)
- [インターフェイス](#) (6 ページ)
- [VLANs](#) (36 ページ)
- [VLAN グループ](#) (44 ページ)
- [VLAN ACL \(VACL\)](#) (50 ページ)
- [IDS/IPS 設定](#) (59 ページ)

# Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータにおけるポリシーの検出



(注) バージョン 4.17 以降、Cisco Security Manager は引き続き Cisco Catalyst スイッチの機能をサポートしますが、バグ修正や拡張機能はサポートしていません。

Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータの設定（およびそれらに関連付けられているサービス モジュールやセキュリティ コンテキストの設定）を検出したり、設定をポリシーとして Security Manager にインポートしたりできます。これにより、既存のデバイスを追加し、それらを Security Manager で管理できるようになり、各デバイスをポリシーごとに手動で設定する必要がなくなります。詳細については、[デバイスインベントリへのデバイスの追加](#)を参照してください。

Security Manager で設定できるコマンドを検出できます。サポートされていないコマンドは検出されません。つまり、これらのコマンドは、次に展開が行われたあともデバイスにそのまま残されています。さらに、Security Manager で検出できるコマンドの場合でも、そのコマンドに関連するサブコマンドとキーワードがすべて検出されるわけではなく、サポートされていない要素は、検出されずにデバイスにそのまま残されます。

また、Security Manager ですでに管理されているデバイスの設定をいつでも再検出できます。ただし、再検出を実行すると Security Manager で定義したポリシーが上書きされるため、通常は再検出を実行することは推奨しません。詳細については、[Security Manager にすでに存在するデバイス上のポリシーの検出](#)を参照してください。



(注) ポリシーの検出後すぐに（ポリシーに変更を加えたり、デバイスからポリシーの割り当てを解除したりする前に）展開を実行することを推奨します（この推奨事項は、デバイスによってホストされるサービスモジュールまたはセキュリティコンテキストにも適用されます）。このようにしないと、Security Manager で設定した変更内容がデバイスに展開されない可能性があります。[展開および Configuration Archive の使用](#)を参照してください。

## 関連項目

- [ポリシーについて](#)
- [ポリシーの検出](#)
- [Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータの管理](#) (1 ページ)
- [展開および Configuration Archive の使用](#)

## Catalyst サマリー情報の表示

[Catalyst Summary Info] ページを使用して、Security Manager によって検出されたサービス モジュール、ポート、VLAN などのシステム情報の概要を表示します。

Catalyst 概要情報を表示するには、デバイスビューで Catalyst スイッチまたは Cisco 7600 シリーズ ルータを右クリックし、[Catalyst サマリー情報 (Catalyst Summary Info)] を選択するか、または [ツール (Tools)] > [Catalyst サマリー情報 (Catalyst Summary Info)] を選択します。



- (注) Security Manager が特定の Cisco Catalyst スイッチまたは Cisco 7600 シリーズ ルータの検出を完了していない場合、そのデバイスの [Catalyst サマリー情報 (Catalyst Summary Info)] ページに「No information is available. This information is acquired during device discovery.」（利用できる情報がありません。この情報は、デバイス検出時に取得されます）というメッセージが表示されます。

### 関連項目

- [IDSM 設定 \(59 ページ\)](#)
- [\[VLAN Access Lists\] ページ \(54 ページ\)](#)
- [テーブルのフィルタリング](#)

### フィールドリファレンス

表 1: [Catalyst Summary Info] ページ

要素	説明
ホスト名 (Hostname)	デバイスの設定済みホスト名が表示されます。
Device Type	デバイス タイプを表示します。
シリアル番号	デバイスのシリアル番号を表示します。
OS Version	デバイスで実行されている Cisco IOS イメージのバージョンが表示されます。
イメージ (Image)	デバイスで実行されているイメージの名前が表示されます。
Last Update	最新の検出のタイムスタンプを表示します。
合計ポート数	アクセスポート、ルーテッドポート、およびトランクポートを合わせた設定済みポートの合計数が表示されます。
アクセスポート	シャーシの設定済みアクセスポートの数が表示されます。

要素	説明
トランク ポート	シャーシの設定済みトランク ポートの数が表示されます。
ルーテッド ポート	シャーシの設定済みルーテッド ポートの数が表示されます。
Total VLANs	シャーシおよびそのすべてのサービス モジュールの設定済み VLAN の合計数が表示されます。
Layer 2 VLANs	レイヤ 2 で稼働している VLAN の数が表示されます。
Layer 3 VLANs	レイヤ 3 で稼働している VLAN の数が表示されます。
[Service Module] テーブル	
スロット	サービス モジュールが接続されているスロットが表示されます。
デバイスタイプ	サービスモジュールの簡単な説明を表示します。
シリアル番号	サービス モジュールのシリアル番号が表示されます。
モデル	サービス モジュールのモデル タイプが表示されます。
OS Version	インストールされ、サービス モジュールで稼働している OS バージョンが表示されます。
Assigned VLANs	FWSM が割り当てられている VLAN の合計数が表示されます。  ヒント [Interfaces/VLANs] ポリシーの [Summary] タブをクリックすると、IDSM または VPNSM に割り当てられている VLAN を確認できます。
コンテキスト	マルチコンテキストモードで動作する FWSM に設定されているセキュリティコンテキストの総数を表示します。  ヒント [インターフェイス/VLAN (Interfaces/VLANs)] ポリシーの [サマリー (Summary)] タブをクリックすると、IDSM に設定されている仮想センサーの数を確認できます。

## Catalyst インターフェイス、VLAN、および VLAN グループの概要の表示

[インターフェイス/VLAN (Interfaces/VLAN)] ポリシーの [サマリー (Summary)] タブには、サポートされている Catalyst 6500 シリーズおよび 7600 シリーズ シャーシとそれらに関連付けられたサービスモジュールに設定されているすべての VLAN、VLAN グループ、インターフェイス、およびサブインターフェイスの属性が表示されます。

インターフェイスサマリー情報を表示するには、デバイスビューでポリシーセクタから [インターフェイス/VLAN (Interfaces/VLANs)] を選択し、[サマリー (Summary)] タブをクリックします。



(注) [Summary] タブは、Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータの場合だけ使用できます。

#### 関連項目

- [\[Interfaces/VLANs\] ページ - \[VLANs\] タブ \(38 ページ\)](#)
- [\[Interfaces/VLANs\] ページ - \[VLAN Groups\] タブ \(46 ページ\)](#)
- [\[Interfaces/VLANs\] ページ - \[Interfaces\] タブ \(10 ページ\)](#)
- [Catalyst サマリー情報の表示 \(3 ページ\)](#)
- [テーブルのフィルタリング](#)

#### フィールド リファレンス

表 2: [Interfaces/VLANs] ページ - [Summary] タブ

要素	説明
VLAN ID (Admin. VLAN ID)	インターフェイスまたはサブインターフェイスに関連付けられた VLAN ID。VLAN ID は、指定されたインターフェイスまたはサブインターフェイスで 802.1Q タグ付きパケットを送受信する場所を示します。VLAN ID が指定されていない場合は、インターフェイスまたはサブインターフェイスでトラフィックを送受信できません。  (注) 同じ物理インターフェイスに設定されたすべてのサブインターフェイスでは、VLAN ID がすべて一意である必要があります。
[VLAN 名(VLAN Name)]	インターフェイスまたはサブインターフェイスに対応する VLAN の名前。VLAN003、Trunk1 などです。
VLAN Group	テーブルの行が示す VLAN に設定されている VLAN グループの数値 ID。
VLAN タイプ	VLAN が Layer 2 または Layer 3 にアクセスできるかどうかを指定します。
IP アドレス/マスク (IP Address/Mask)	インターフェイスまたはサブインターフェイスに設定されている VLAN の IP アドレスおよび対応するサブネットマスク。

要素	説明
アクセス ポート	VLANが使用するアクセスポートに割り当てられている名前が表示されます（名前が割り当てられている場合）。
トランク ポート	トランクを介したトラフィックの伝送が許可される VLAN を示します。
Slot (-Port)	シャーシスロット番号（関連サービスモジュールの取り付け先）を、ハイフンで結び付けられた x-y の形式でポート番号に関連付けます（3-1 など）。
[ブレードタイプ (Blade Type) ]	特定の VLAN が設定されているサービス モジュールの種類（FWSM、VPNSM など）を示します。
セキュリティコンテキスト	インターフェイスに関連付けられたセキュリティコンテキストを示します。ただし、取り付けられたモジュールでマルチモードがアクティブであり、そのモジュールに管理コンテキストが設定されている場合にかぎります。
[セキュリティコンテキスト インターフェイス (Security Context Interface) ]	セキュリティコンテキストがトラフィックを検査する物理インターフェイスおよびサブインターフェイス ID を表示します。表示される ID は、物理インターフェイス、単一のサブインターフェイス（範囲を 1 と定義）、またはサブインターフェイスの範囲を表します。
セキュリティ レベル (Security Level)	<p>インターフェイスのセキュリティレベルが表示されます。値の範囲は 0（最低のセキュリティ）～ 100（最高のセキュリティ）です。</p> <ul style="list-style-type: none"> <li>外部インターフェイスの場合、デフォルトは 0 です。</li> <li>内部インターフェイスの場合、デフォルトは 100 です。</li> <li>DMZ のインターフェイスの場合、デフォルトは通常 1 ～ 99 です。</li> </ul>

## インターフェイス

[Interfaces/VLANs] ページの [Interfaces] タブを使用して、次のタイプのポートを表示および管理します。

- アクセスポート：ホストマシンまたはサービスの接続に使用されるスイッチングポート。アクセスポートは、1つのVLANだけに属し、1つのVLANだけのトラフィックを伝送します。トラフィックは、VLANタグが付いていないネイティブ形式で送受信されます。
- トランクポート：レイヤ2で操作され、複数のVLANのトラフィックを送信するスイッチングポート。トラフィックには、各VLANからのトラフィックを区別するVLAN番号

がタグ付けされます。トランクポートは、スイッチ間の接続またはスイッチとルータ間の接続に使用されます。

- ルーテッドポート：ルータ上のポートのように機能する物理ポート。ルーテッドポートは特定の VLAN に関連付けられず、通常のルータインターフェイスのように動作します。ルーテッドポートにはレイヤ 3 ルーティングプロトコルを設定できます。
- ダイナミックポート：ネイバーポートがトランクポートとして設定されている場合に、トランクポートに動的に変更できるポート。
- サポートされないポート：Security Manager によってサポートされない Catalyst デバイス上のポート。

[インターフェイス (Interfaces)] タブを表示するには、デバイスビューで Catalyst デバイスを選択し、ポリシーセレクタから [インターフェイス/VLAN (Interfaces/VLANs)] を選択して作業領域で [インターフェイス (Interfaces)] タブをクリックします。

次の項では、Catalyst デバイスのインターフェイスを定義するときに行えるアクションについて説明します。

- [Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータでのポートの作成または編集 \(7 ページ\)](#)
- [Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータでのポートの削除 \(9 ページ\)](#)
- [\[Interfaces/VLANs\] ページ - \[Interfaces\] タブ \(10 ページ\)](#)

#### 関連項目

- [VLANs \(36 ページ\)](#)
- [VLAN グループ \(44 ページ\)](#)
- [VLAN ACL \(VACL\) \(50 ページ\)](#)

## Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータでのポートの作成または編集



- (注) バージョン 4.17 以降、Cisco Security Manager は引き続き Cisco Catalyst スイッチの機能をサポートしていますが、バグ修正や拡張機能はサポートしていません。

Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータのアクセスポート、ルーテッドポート、またはトランクポートを作成できますが、次の制限事項があります。

- 各インターフェイスに名前が必要です。
- アクセスポートは 1 つの VLAN だけに関連付けることができます。

- トランク ポートは 1 つ以上の VLAN に関連付けることができます。

#### 関連項目

- [Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータでのポートの削除](#) (9 ページ)
- [VLAN の作成または編集](#) (36 ページ)
- [VLAN グループの作成または編集](#) (44 ページ)
- [\[Interfaces/VLANs\] ページ - \[Interfaces\] タブ](#) (10 ページ)
- [インターフェイス](#) (6 ページ)

- 
- ステップ 1** (デバイスビュー) Catalyst デバイスを選択し、ポリシーセレクトタから [インターフェイス/VLAN (Interfaces/VLANs)] を選択して作業領域で [インターフェイス (Interfaces)] タブをクリックします。
- [Interfaces] タブが表示されます。このタブの各フィールドの説明については、[\[Interfaces/VLANs\] ページ - \[Interfaces\] タブ](#) (10 ページ) を参照してください。
- ステップ 2** 次のいずれかを実行します。
- 新しいインターフェイスの属性を定義するには、[行の追加 (Add Row)] をクリックします。
  - インターフェイスの属性を編集するには、リストで選択して [行の編集 (Edit Row)] をクリックします。
- ステップ 3** (任意) このインターフェイスをシャットダウンモードにする場合は、[インターフェイスの有効化 (Enable Interface)] チェックボックスをオフにします。
- ステップ 4** [タイプ (Type)] リストから [インターフェイス (Interface)] または [サブインターフェイス (Subinterface)] を選択します。
- ステップ 5** (インターフェイスだけ) インターフェイスの名前を入力します。[選択 (Select)] をクリックするとダイアログボックスが開き、インターフェイスタイプ、およびインターフェイスの位置情報 (カード、スロット、サブインターフェイスなど) に基づいて、標準の名前を生成できます。ダイアログボックスを使用してインターフェイス名を生成する方法については、[\[Interface Auto Name Generator\] ダイアログボックス](#) を参照してください。
- ステップ 6** (インターフェイスのみ) [モード (Mode)] リストからオプションを選択して、ポート設定タイプを指定します。ダイアログボックスのフィールドは、選択に応じて変わります。
- ステップ 7** (サブインターフェイスだけ) サブインターフェイスの親インターフェイスを選択し、ID 番号を入力します。
- ステップ 8** 選択したタイプの設定を定義または指定します。
- [Access Port] : フィールドの説明については、[\[Create Interface\]/\[Edit Interface\] ダイアログボックス - アクセスポートモード](#) (12 ページ) を参照してください。
  - [Routed Port] : フィールドの説明については、[\[Create Interface\]/\[Edit Interface\] ダイアログボックス - ルーテッドポートモード](#) (17 ページ) を参照してください。



- [Trunk Port] : フィールドの説明については、[\[Create Interface\]/\[Edit Interface\] ダイアログボックス - トランク ポート モード \(20 ページ\)](#) を参照してください。
- [Dynamic Port] : フィールドの説明については、[\[Create Interface\]/\[Edit Interface\] ダイアログボックス - ダイナミック モード \(26 ページ\)](#) を参照してください。
- [Subinterface] : フィールドの説明については、[\[Create Interface\]/\[Edit Interface\] ダイアログボックス - サブインターフェイス \(31 ページ\)](#) を参照してください。
- [Unsupported] : フィールドの説明については、[\[Create Interface\]/\[Edit Interface\] ダイアログボックス - サポートされていないモード \(33 ページ\)](#) を参照してください。

**ステップ 9** [速度 (Speed) ] リストから、インターフェイスの速度を定義するオプションを選択します。

**ステップ 10** インターフェイスに特定の速度を定義した結果、[デュプレックス (Duplex) ] リストが有効になっている場合は、デュプレックスオプションを選択します。

**ステップ 11** [MTU] フィールドに、最大伝送単位値を入力します。

**ステップ 12** インバウンド (受信) トラフィックとアウトバウンド (送信) トラフィックに対してフロー制御を使用するかどうかを設定します。

**ステップ 13** (任意) [説明 (Description) ] フィールドにインターフェイスの説明を入力します。

**ステップ 14** [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。

## Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータでのポートの削除



- (注) バージョン 4.17 以降、Cisco Security Manager は引き続き Cisco Catalyst スイッチの機能をサポートしていますが、バグ修正や拡張機能はサポートしていません。

インターフェイスの定義はいつでも削除できますが、このオプションは慎重に使用してください。関連デバイスでポリシー定義にインターフェイス定義が含まれている場合は、インターフェイスを削除すると、これらのポリシー定義をデバイスに展開できなくなります。

### 関連項目

- [Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータでのポートの作成または編集 \(7 ページ\)](#)
- [インターフェイス \(6 ページ\)](#)

**ステップ 1** (デバイス ビュー) デバイス セレクタから Cisco Catalyst スイッチまたは Cisco 7600 シリーズ ルータを選択します。

**ステップ 2** ポリシーセレクタから [インターフェイス/VLAN (Interfaces/VLANs) ] を選択します。

ステップ 3 作業領域で [Interfaces] タブをクリックします。

[Interfaces] タブが表示されます。このタブの各フィールドの説明については、[\[Interfaces/VLANs\] ページ - \[Interfaces\] タブ \(10 ページ\)](#) を参照してください。

ステップ 4 テーブルからインターフェイスを選択し、[行の削除 (Delete Row)] をクリックします。インターフェイスが削除されます。

## [Interfaces/VLANs] ページ - [Interfaces] タブ

[Interfaces] タブを使用して、サポートされている Cisco Catalyst スイッチと Cisco 7600 シリーズ ルータおよびそれらに関連付けられたサービスモジュール (ブレード) のインターフェイスやサブインターフェイスを表示および設定します。

### ナビゲーションパス

(デバイスビュー) デバイスセレクトから [インターフェイス/VLAN (Interfaces/VLANs)] を選択し、[インターフェイス (Interfaces)] タブをクリックします。

### 関連項目

- [\[Interfaces/VLANs\] ページ - \[VLANs\] タブ \(38 ページ\)](#)
- [\[Interfaces/VLANs\] ページ - \[VLAN Groups\] タブ \(46 ページ\)](#)
- [Catalyst インターフェイス、VLAN、および VLAN グループの概要の表示 \(4 ページ\)](#)
- [テーブルのフィルタリング](#)

### フィールド リファレンス

表 3: [Interfaces/VLANs] ページ - [Interfaces] タブ

要素	説明
名前	インターフェイスタイプ、シャーシスロット、およびインターフェイスカードの番号。たとえば、 <i>FastEthernet 2/7</i> は、ファストイーサネット、スロット 2、インターフェイス 7 を意味します。

要素	説明
[モード (Mode) ]	物理ポートのコンフィギュレーション モード : <ul style="list-style-type: none"> <li>• アクセス (Access)</li> <li>• ルーテッド</li> <li>• トランク</li> <li>• Dynamic Auto</li> <li>• Dynamic Desirable</li> <li>• 非サポート対象</li> </ul>
VLAN ID (Admin. VLAN ID)	説明されたサブインターフェイスに関連付けられた VLAN ID。イーサネットインターフェイスおよび VLAN インターフェイスについてのみ表示されます。
IP Address	インターフェイスの IP アドレス。
[有効 (Enabled) ]	インターフェイスがイネーブルになっているかディセーブル (シャットダウン状態) になっているかを示します。
Interface Roles	命名パターンがこのインターフェイスと一致するインターフェイス ロール。 <a href="#">インターフェイス ロール オブジェクトについて</a> を参照してください。
説明	(任意) インターフェイスの説明。
[Add Row] ボタン	新しいインターフェイスを定義できる [Create Interface] ダイアログボックスを開きます。詳細については、関連するモードの説明を参照してください。 <ul style="list-style-type: none"> <li>• アクセス ポート モード : <a href="#">[Create Interface]/[Edit Interface] ダイアログボックス - アクセス ポート モード (12 ページ)</a>。</li> <li>• ルーテッド ポート モード : <a href="#">[Create Interface]/[Edit Interface] ダイアログボックス - ルーテッド ポート モード (17 ページ)</a></li> <li>• トランク ポート モード : <a href="#">[Create Interface]/[Edit Interface] ダイアログボックス - トランク ポート モード (20 ページ)</a></li> <li>• ダイナミック モード : <a href="#">[Create Interface]/[Edit Interface] ダイアログボックス - ダイナミック モード (26 ページ)</a></li> </ul>

要素	説明
[Edit Row] ボタン	<p>[インターフェイスの編集 (Edit Interface) ] ダイアログボックスを開きます。ここで、選択したインターフェイスを編集できます。詳細については、関連するモードの説明を参照してください。</p> <ul style="list-style-type: none"> <li>• アクセス ポート モード : <a href="#">[Create Interface]/[Edit Interface] ダイアログボックス - アクセス ポート モード (12 ページ)</a>。</li> <li>• ルーテッド ポート モード : <a href="#">[Create Interface]/[Edit Interface] ダイアログボックス - ルーテッド ポート モード (17 ページ)</a></li> <li>• トランク ポート モード : <a href="#">[Create Interface]/[Edit Interface] ダイアログボックス - トランク ポート モード (20 ページ)</a></li> <li>• ダイナミック モード : <a href="#">[Create Interface]/[Edit Interface] ダイアログボックス - ダイナミック モード (26 ページ)</a></li> <li>• サポートなし : <a href="#">[Create Interface]/[Edit Interface] ダイアログボックス - サポートされていないモード (33 ページ)</a></li> </ul>
[Delete Row] ボタン	選択したインターフェイスを削除します。

## [Create Interface]/[Edit Interface] ダイアログボックス - アクセス ポート モード

[Create Interface] ダイアログボックス (または [Edit Interface] ダイアログボックス) を使用して、アクセス ポート モードで稼働する物理インターフェイスや仮想インターフェイスの属性を設定します。

### ナビゲーションパス

[\[Interfaces/VLANs\] ページ - \[Interfaces\] タブ \(10 ページ\)](#) に移動し、[追加 (Add) ] または [編集 (Edit) ] をクリックして [インターフェイスの作成 (Create Interface) ]/[インターフェイスの編集 (Edit Interface) ] ダイアログボックスを開き、[モード (Mode) ] リストから [アクセス ポート (Access Port) ] を選択します。

### 関連項目

- [\[Create Interface\]/\[Edit Interface\] ダイアログボックス - ルーテッド ポート モード \(17 ページ\)](#)
- [\[Create Interface\]/\[Edit Interface\] ダイアログボックス - トランク ポート モード \(20 ページ\)](#)
- [\[Create Interface\]/\[Edit Interface\] ダイアログボックス - ダイナミック モード \(26 ページ\)](#)
- [\[Interface Auto Name Generator\] ダイアログボックス](#)
- [FlexConfig ポリシーとポリシー オブジェクトについて](#)

- [インターフェイス ロール オブジェクトについて](#)

## フィールド リファレンス

表 4: [Create Interface]/[Edit Interface] ダイアログボックス - アクセス ポート モード

要素	説明
[Enable Interface]	このチェックボックスをオンにすると、インターフェイスがイネーブルになります。  オフにすると、shutdown コマンドを使用してインターフェイスがディセーブルになります。
タイプ (Type)	定義をインターフェイスに適用するか、サブインターフェイスに適用するかを指定します。  サブインターフェイスを定義する方法の詳細については、 <a href="#">[Create Interface]/[Edit Interface] ダイアログボックス - サブインターフェイス (31 ページ)</a> を参照してください。
Name ([Select] ボタン)	名前が設定されている場合は、生成されたインターフェイスの名前を表示します。  <a href="#">[Interface Auto Name Generator] ダイアログボックス</a> を開くには、[選択 (Select)] をクリックします。このダイアログボックスで、Security Manager がインターフェイス名の生成に使用する詳細情報を入力または編集できます。
[モード (Mode)]	このインターフェイスのポート設定タイプ。  [アクセスポート (Access Port)] を選択すると、アクセスポートに関連する設定オプションが表示されます。
アクセス ポート設定	

要素	説明
VLAN ID (選択ボタン)	<p>VLAN を選択した場合、アクセスポートモードで使用する VLAN のインターフェイス固有の ID が表示されます。それ以外の場合は、[選択 (Select)] をクリックすると <a href="#">[VLAN Selector] ダイアログボックス (49 ページ)</a> が開きます。</p> <p>VLAN ID は、サブインターフェイスで 802.1Q タグ付きパケットを送受信する場所を示します。VLAN ID が指定されていない場合は、サブインターフェイスでトラフィックを送受信できません。有効値の範囲は 1 ~ 4094 です。接続されているデバイスで VLAN ID が予約されている場合があります。詳細については、デバイスのマニュアルを参照してください。マルチコンテキスト モードの場合、VLAN はシステム設定でしか設定できません。</p> <p>(注) 同じ物理インターフェイスに設定されたすべてのサブインターフェイスでは、VLAN ID がすべて一意である必要があります。</p> <p>ヒント VLAN をサブインターフェイスに関連付けずに、イーサネットインターフェイスで DOT1Q カプセル化を設定するには、CLI コマンドまたは FlexConfig を使用して <b>vlan-id dot1q</b> コマンドを使用します。メインインターフェイスに VLAN を設定すると、デバイスに設定できる VLAN の数が多くなります。</p>
Enable Port Security	<p>このチェックボックスをオンにすると、ポートへのアクセスを許可される MAC アドレスを限定して、インターフェイスへの入力を制限できます。オフにすると、ポートセキュリティがディセーブルになります。</p>
最大MACアドレス (Max. MAC Addresses)	<p>[Enable Port Security] がオンの場合にだけ適用されます。</p> <p>インターフェイスのセキュア MAC アドレスの最大数。有効な値の範囲は 1 ~ 4097 です。</p> <p>(注) セキュア MAC アドレスは、接続されたデバイスの MAC アドレスを使用して動的に設定されます。</p>

要素	説明
Violation Policy	<p>セキュリティ違反が発生した場合に実行されるアクション。</p> <ul style="list-style-type: none"> <li>• [Port Security Protect] : セキュア MAC アドレスを必要な数だけ削除してカウントが最大値を下回るまで、送信元アドレスが不明なパケットをドロップします。</li> <li>• [ポートセキュリティ制限 (Port Security Restrict) ] : セキュア MAC アドレスを必要な数だけ削除してカウントが最大値を下回るまで、送信元アドレスが不明なパケットをドロップします。さらに、SecurityViolation カウンタを 1 増やします。</li> <li>• [Port Security Shutdown] : インターフェイスをただちに error-disabled 状態とし、SNMP トラップ通知を送信します。</li> </ul> <p>セキュリティ違反は、セキュア MAC アドレスが最大数まで設定されたあと、アドレス テーブルに MAC アドレスが登録されていないワークステーションがインターフェイスにアクセスしようとした場合に発生します。</p>
Enable VACL Capture	<p>このチェックボックスをオンにすると、VACL キャプチャがイネーブルになります。キャプチャビットが設定されると、キャプチャ機能がイネーブルなポートで、転送されたパケットを受信できます。</p> <p>オフにすると、VACL キャプチャがディセーブルになります。</p>
Capture VLANs ([Select] ボタン)	<p>転送された VLAN パケットを VACL で受信する必要がある VLAN を識別できます。このオプションは、[Enable VACL Capture] チェックボックスをオンにした場合にだけ使用できます。</p> <p>カンマで区切られた VLAN ID のリストを入力するか、[選択 (Select) ] をクリックして <a href="#">[VLAN Selector] ダイアログボックス (49 ページ)</a> を開きます。</p> <p>VACL は、VLAN パケットが VLAN に最初にルーティングまたはブリッジングされた場合だけ、このパケットをキャプチャできます。キャプチャできるのは、転送されたパケットだけです。</p>
共通インターフェイス設定	

要素	説明
速度	<p>物理インターフェイスの速度。</p> <ul style="list-style-type: none"> <li>• [10] : 10 Mbps で送信します。</li> <li>• [100] : 100 Mbps で送信します。</li> <li>• [1000] : 1,000 Mbps で送信します。</li> <li>• [10000] : 10,000 Mbps で送信します。</li> <li>• [Auto] : [Speed] を [Auto] に設定すると、[Speed] および [Duplex] がどちらもオートネゴシエーションされます。</li> <li>• [Non-Negotiate] : リンクのネゴシエーションをディセーブルにします。</li> </ul>
デュプレックス	<p>インターフェイスのデュプレックス設定 :</p> <ul style="list-style-type: none"> <li>• [Auto] : デュプレックス設定をオートネゴシエーションします。</li> <li>• [Half] : データの送受信を同時には行いません。</li> <li>• [Full] : データの送受信を同時に行います。</li> </ul> <p>[Speed] が [Auto] に設定されている場合は、デュプレックス設定も [Auto] に設定する必要があります。</p>
[ MTU]	<p>最大伝送単位。これは、インターフェイスで処理できる最大パケットサイズ (バイト単位) です。有効な値の範囲は、インターフェイス タイプによって異なります。</p>
説明	<p>インターフェイスを説明するテキスト。復帰を使用しないで1行に最大240文字を入力します。</p> <p>(注) マルチ コンテキスト モードの場合、システムの説明とコンテキストの説明に関係はありません。</p>
Flow Control Receive	<p>受信フレームのフロー制御設定。</p> <ul style="list-style-type: none"> <li>• [Off] : ネイバーポートがフロー制御を要求しても、ポートではフロー制御を使用しません。</li> <li>• [On] : ネイバーポートの要求に従って、ポートでフロー制御を使用します。</li> <li>• [Desired] : ポートでフロー制御フレームは許可されますが、必須ではありません。</li> </ul> <p>フロー制御フレーム (別名ポーズフレーム) は、バッファが一杯になったときに、指定した間隔だけフレームの送信を停止するよう送信元にシグナリングする特別なパケットです。</p>



要素	説明
Flow Control Send	送信フレームのフロー制御設定。 <ul style="list-style-type: none"> <li>• [Off] : ポートはネイバー ポートにフロー制御フレームを送信しません。</li> <li>• [On] : ポートはネイバー ポートにフロー制御フレームを送信します。</li> <li>• [Desired] : ポートでフロー制御フレームは許可されますが、必須ではありません。</li> </ul>
ロール (Roles)	インターフェイスに関連付けられたインターフェイス ロールを表示します。インターフェイス ロールとは、各デバイスの設定が生成されるときに、実際のインターフェイス IP アドレスで置き換えられるオブジェクトです。インターフェイス ロールを使用すると、複数のインターフェイスに適用可能な汎用ルールを定義できます。 <a href="#">インターフェイスロールオブジェクトについて</a> を参照してください。

## [Create Interface]/[Edit Interface] ダイアログボックス - ルーテッド ポート モード

[Create Interface] ダイアログボックス (または [Edit Interface] ダイアログボックス) を使用して、レイヤ 3 においてルーテッド ポート モードで稼働する物理インターフェイスの属性を設定します。

### ナビゲーションパス

[\[Interfaces/VLANs\] ページ - \[Interfaces\] タブ \(10 ページ\)](#) に移動し、[追加 (Add)] または [編集 (Edit)] をクリックして [インターフェイスの作成 (Create Interface)]/[インターフェイスの編集 (Edit Interface)] ダイアログボックスを開き、[モード (Mode)] リストから [ルーテッド ポート (Routed Port)] を選択します。

### 関連項目

- [\[Create Interface\]/\[Edit Interface\] ダイアログボックス - アクセス ポート モード \(12 ページ\)](#)
- [\[Create Interface\]/\[Edit Interface\] ダイアログボックス - トランク ポート モード \(20 ページ\)](#)
- [\[Create Interface\]/\[Edit Interface\] ダイアログボックス - ダイナミック モード \(26 ページ\)](#)
- [インターフェイス ロール オブジェクトについて](#)
- [ネットワーク/ホストオブジェクトについて](#)
- [ポリシーのオブジェクトの選択](#)

## フィールド リファレンス

表 5: [Create Interface]/[Edit Interface] ダイアログボックス - ルーテッドポートモード

要素	説明
[Enable Interface]	このチェックボックスをオンにすると、インターフェイスがイネーブルになります。  オフにすると、shutdown コマンドを使用してインターフェイスがディセーブルになります。
タイプ (Type)	定義をインターフェイスに適用するか、サブインターフェイスに適用するかを指定します。  サブインターフェイスを定義する方法の詳細については、 <a href="#">[Create Interface]/[Edit Interface] ダイアログボックス - サブインターフェイス (31 ページ)</a> を参照してください。
Name ([Select] ボタン)	名前が設定されている場合は、生成されたインターフェイスの名前を表示します。  <a href="#">[Interface Auto Name Generator] ダイアログボックス</a> を開くには、[選択 (Select)] をクリックします。このダイアログボックスで、Security Manager がインターフェイス名の生成に使用する詳細情報を入力または編集できます。
[モード (Mode) ]	このインターフェイスのポート設定タイプ。  [ルーテッドポート (Routed Port) ]を選択すると、ルーテッドポートに関連する設定オプションが表示されます。
ルーテッドポートの設定	
IP タイプ (IP Type)	ポートで使用する IP アドレスのタイプ。  • [Static IP] : インターフェイスで永続的な IP アドレスを使用することを指定し、関連する GUI 要素をアクティブにします。
IP Address ([Select] ボタン)	IP アドレスを入力するか、または [選択 (Select) ] をクリックして、IP アドレスを選択できる [ネットワーク/ホストセレクタ (Networks/Hosts Selector) ] を開くことができます。
Helper IP Addresses ([Select] ボタン)	インターフェイスにヘルパー IP アドレスを割り当てることができます。ヘルパー IP アドレスによって、ブロードキャストの DHCP 要求が、DHCP サーバだけに送信されるユニキャストの要求に変換されます。

要素	説明
Mask	<p>サブネット マスクを指定できます。ネットマスク値を入力するか、またはリストからネットマスクを選択できます。ネットマスクを入力する場合は、その値をドット付き 10 進表記 (255.255.255.0 など) で指定するか、またはビット数 (24 など) を入力します。</p> <p>(注) ネットワークに接続されたインターフェイスに対して、255.255.255.254 または 255.255.255.255 を使用しないでください。これらのネットマスクを使用すると、インターフェイス上のすべてのトラフィックが停止します。</p>
共通インターフェイス設定	
速度	<p>物理インターフェイスの速度。</p> <ul style="list-style-type: none"> <li>• [10] : 10 Mbps で送信します。</li> <li>• [100] : 100 Mbps で送信します。</li> <li>• [1000] : 1,000 Mbps で送信します。</li> <li>• [10000] : 10,000 Mbps で送信します。</li> <li>• [Auto] : [Speed] を [Auto] に設定すると、[Speed] および [Duplex] がどちらもオートネゴシエーションされます。</li> <li>• [Non-Negotiate] : リンクのネゴシエーションをディセーブルにします。</li> </ul>
デュプレックス	<p>インターフェイスのデュプレックス設定 :</p> <ul style="list-style-type: none"> <li>• [Auto] : デュプレックス設定をオートネゴシエーションします。</li> <li>• [Half] : データの送受信を同時には行いません。</li> <li>• [Full] : データの送受信を同時に行います。</li> </ul> <p>[Speed] が [Auto] に設定されている場合は、デュプレックス設定も [Auto] に設定する必要があります。</p>
[ MTU]	<p>最大伝送単位。これは、インターフェイスで処理できる最大パケットサイズ (バイト単位) です。有効な値の範囲は、インターフェイスタイプによって異なります。</p>
説明	<p>インターフェイスを説明するテキスト。復帰を使用しないで 1 行に最大 240 文字を入力します。</p> <p>(注) マルチコンテキストモードの場合、システムの説明とコンテキストの説明に関係はありません。</p>

要素	説明
Flow Control Receive	<p>受信フレームのフロー制御設定。</p> <ul style="list-style-type: none"> <li>• [Off] : ネイバー ポートがフロー制御を要求しても、ポートではフロー制御を使用しません。</li> <li>• [On] : ネイバー ポートの要求に従って、ポートでフロー制御を使用します。</li> <li>• [Desired] : ポートでフロー制御フレームは許可されますが、必須ではありません。</li> </ul> <p>フロー制御フレーム（別名ポーズフレーム）は、バッファが一杯になったときに、指定した間隔だけフレームの送信を停止するよう送信元にシグナリングする特別なパケットです。</p>
Flow Control Send	<p>送信フレームのフロー制御設定。</p> <ul style="list-style-type: none"> <li>• [Off] : ポートはネイバー ポートにフロー制御フレームを送信しません。</li> <li>• [On] : ポートはネイバー ポートにフロー制御フレームを送信します。</li> <li>• [Desired] : ポートでフロー制御フレームは許可されますが、必須ではありません。</li> </ul>
ロール (Roles)	<p>インターフェイスに関連付けられたインターフェイス ロールを表示します。インターフェイス ロールとは、各デバイスの設定が生成されるときに、実際のインターフェイス IP アドレスで置き換えられるオブジェクトです。インターフェイス ロールを使用すると、複数のインターフェイスに適用可能な汎用ルールを定義できます。 <a href="#">インターフェイス ロール オブジェクトについて</a> を参照してください。</p>

## [Create Interface]/[Edit Interface] ダイアログボックス - トランク ポート モード

[Create Interface] ダイアログボックス（または [Edit Interface] ダイアログボックス）を使用して、トランク ポート モードで稼働する物理インターフェイスや仮想インターフェイスの属性を設定します。

### ナビゲーションパス

[\[Interfaces/VLANs\] ページ - \[Interfaces\] タブ \(10 ページ\)](#) に移動し、[追加 (Add)] または [編集 (Edit)] をクリックして [インターフェイスの作成 (Create Interface)]/[インターフェイスの編集 (Edit Interface)] ダイアログボックスを開き、[モード (Mode)] リストから [トランク ポート (Trunk Port)] を選択します。

## 関連項目

- [\[Create Interface\]/\[Edit Interface\] ダイアログボックス - アクセス ポート モード](#) (12 ページ)
- [\[Create Interface\]/\[Edit Interface\] ダイアログボックス - ルーテッド ポート モード](#) (17 ページ)
- [\[Create Interface\]/\[Edit Interface\] ダイアログボックス - ダイナミック モード](#) (26 ページ)
- [FlexConfig ポリシーとポリシー オブジェクトについて](#)
- [インターフェイス ロール オブジェクトについて](#)

## フィールド リファレンス

表 6: [Create Interface]/[Edit Interface] ダイアログボックス - トランク ポート モード

要素	説明
[Enable Interface]	このチェックボックスをオンにすると、インターフェイスがイネーブルになります。  オフにすると、shutdown コマンドを使用してインターフェイスがディセーブルになります。
タイプ (Type)	定義をインターフェイスに適用するか、サブインターフェイスに適用するかを指定します。  サブインターフェイスを定義する方法の詳細については、 <a href="#">[Create Interface]/[Edit Interface] ダイアログボックス - サブインターフェイス</a> (31 ページ) を参照してください。
Name ([Select] ボタン)	名前が設定されている場合は、生成されたインターフェイスの名前を表示します。  <a href="#">[Interface Auto Name Generator] ダイアログボックス</a> を開くには、[選択 (Select)] をクリックします。このダイアログボックスで、Security Manager がインターフェイス名の生成に使用する詳細情報を入力または編集できます。
[モード (Mode) ]	このインターフェイスのポート設定タイプ。  [トランクポート (Trunk Port) ]を選択すると、トランクポートに関連する設定オプションが表示されます。
トランク ポート設定	

要素	説明
カプセル化	<p>次のいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• [DOT1Q] : トランク リンクでの VLAN カプセル化を、IEEE 802.1Q 規格で定義されたカプセル化に指定します。イーサネット サブインターフェイスだけに適用されます。</li> <li>• [ISL] : トランク リンクでの ISL カプセル化を指定します。10 ギガビットイーサネット ポートは ISL カプセル化をサポートしていません。</li> </ul> <p><b>ヒント</b> VLAN をサブインターフェイスに関連付けずに、イーサネット インターフェイスで DOT1Q カプセル化を設定するには、CLI コマンドまたは FlexConfig を使用して <b>vlan-id dot1q</b> コマンドを使用します。メインインターフェイスに VLAN を設定すると、ルータに設定できる VLAN の数が多くなります。</p>
Native VLAN ([Select] ボタン)	<p>[VLAN ID] フィールドで指定された ID を使用して、このインターフェイスに関連付けるネイティブ VLAN を選択できます (ネイティブ VLAN に VLAN ID が指定されていない場合、デフォルト値は 1 です)。このオプションは、802.1Q トランクインターフェイスとして機能する物理インターフェイスを設定する場合にだけ適用されます。</p> <p>カプセル化タイプとして DOT1Q を先に指定しておく必要があります。</p> <p>トランクインターフェイスのネイティブ VLAN は、タグ付けされていないすべての VLAN パケットが論理的に割り当てられる VLAN です。これには、VLAN に関連付けられた管理トラフィックが含まれます。</p> <p>オフにすると、ネイティブ VLAN はこのインターフェイスに関連付けられません。</p> <p>(注) トランク インターフェイスのサブインターフェイスには、ネイティブ VLAN を設定できません。リンクの両端には必ず同じ [Native VLAN] 値を設定してください。同じ値を設定しないと、トラフィックが失われたり、間違った VLAN に送信される場合があります。</p> <p>[VLAN Selector] ダイアログボックス (49 ページ) を開くには、[選択 (Select)] をクリックします。このダイアログボックスで、指定したインターフェイスにネイティブ VLAN を関連付けることができます。</p>
Enable DTP negotiation	<p>このチェックボックスをオンにすると、ダイナミック トランッキングプロトコル (DTP) ネゴシエーションがイネーブルになります。DTP は、デバイス間のトランク オートネゴシエーション (ISL および 802.1Q) を管理します。</p> <p>オフにすると、DTP ネゴシエーションがディセーブルになります。</p>

要素	説明
Allowed VLANs ([Select] ボタン)	<p>トランクで許可される VLAN を指定できます。VLANID を入力してください。カンマを使用して複数の VLAN を区切るか、またはハイフンを使用して VLAN の範囲を指定します (12,17,22 または 2-200 など)。有効な ID の範囲は 1 ~ 4094 です。</p> <p>あるいは、[選択 (Select)] をクリックして <a href="#">[VLAN Selector] ダイアログボックス (49 ページ)</a> を開きます。このダイアログボックスで、トランクに含める VLAN を選択できます。</p>
Prune VLANs ([Select] ボタン)	<p>プルーニング可能な VLAN を指定できます。VLAN ID を入力してください。カンマを使用して複数の VLAN を区切るか、またはハイフンを使用して VLAN の範囲を指定します (12,17,22 または 2-200 など)。</p> <p>あるいは、[選択 (Select)] をクリックして <a href="#">[VLAN Selector] ダイアログボックス (49 ページ)</a> を開きます。このダイアログボックスで、プルーニング可能な VLAN を選択できます。</p>
Enable VACL Capture	<p>このチェックボックスをオンにすると、VACL キャプチャがイネーブルになります。キャプチャビットが設定されると、キャプチャ機能がイネーブルなポートで、転送されたパケットを受信できます。</p> <p>オフにすると、VACL キャプチャがディセーブルになります。</p>
Capture VLANs ([Select] ボタン)	<p>転送された VLAN パケットを VACL で受信する必要がある VLAN を識別できます。このオプションは、[Enable VACL Capture] チェックボックスをオンにした場合にだけ使用できます。</p> <p>カンマで区切られた VLAN ID のリストを入力するか、[選択 (Select)] をクリックして <a href="#">[VLAN Selector] ダイアログボックス (49 ページ)</a> を開きます。</p> <p>VACL は、VLAN パケットが VLAN に最初にルーティングまたはブリッジングされた場合だけ、このパケットをキャプチャできます。キャプチャできるのは、転送されたパケットだけです。</p>
Enable Port Security	<p>IOS ソフトウェアバージョン 12.2(18)SXE2 以降を実行しているデバイスにだけ適用されます。</p> <p>このチェックボックスをオンにすると、ポートへのアクセスを許可される MAC アドレスを限定して、インターフェイスへの入力を制限できます。</p> <p>オフにすると、ポートセキュリティがディセーブルになります。</p> <p>(注) このオプションを選択した場合、[Enable DTP Negotiation] オプションは自動的にオフになります。</p>

要素	説明
[最大 MAC アドレス (Max. MAC Addresses) ]	<p>[Enable Port Security] がオンの場合にだけ適用されます。</p> <p>インターフェイスのセキュア MAC アドレスの最大数。有効な値の範囲は 1 ~ 4097 です。</p> <p>(注) セキュア MAC アドレスは、接続されたデバイスの MAC アドレスを使用して動的に設定されます。</p>
Violation Policy	<p>セキュリティ違反が発生した場合に実行されるアクション。</p> <ul style="list-style-type: none"> <li>• [Port Security Protect] : セキュア MAC アドレスを必要な数だけ削除してカウントが最大値を下回るまで、送信元アドレスが不明なパケットをドロップします。</li> <li>• [ポートセキュリティ制限 (Port Security Restrict) ] : セキュア MAC アドレスを必要な数だけ削除してカウントが最大値を下回るまで、送信元アドレスが不明なパケットをドロップします。さらに、SecurityViolation カウンタを 1 増やします。</li> <li>• [Port Security Shutdown] : インターフェイスをただちに error-disabled 状態とし、SNMP トラップ通知を送信します。</li> </ul> <p>セキュリティ違反は、セキュア MAC アドレスが最大数まで設定されたあと、アドレス テーブルに MAC アドレスが登録されていないワークステーションがインターフェイスにアクセスしようとした場合に発生します。</p>
共通インターフェイス設定	
速度	<p>物理インターフェイスの速度。</p> <ul style="list-style-type: none"> <li>• [10] : 10 Mbps で送信します。</li> <li>• [100] : 100 Mbps で送信します。</li> <li>• [1000] : 1,000 Mbps で送信します。</li> <li>• [10000] : 10,000 Mbps で送信します。</li> <li>• [Auto] : [Speed] を [Auto] に設定すると、[Speed] および [Duplex] がどちらもオートネゴシエーションされます。</li> <li>• [Non-Negotiate] : リンクのネゴシエーションをディセーブルにします。</li> </ul>



要素	説明
デュプレックス	<p>インターフェイスのデュプレックス設定：</p> <ul style="list-style-type: none"> <li>• [Auto]：デュプレックス設定をオートネゴシエーションします。</li> <li>• [Half]：データの送受信を同時には行いません。</li> <li>• [Full]：データの送受信を同時に行います。</li> </ul> <p>[Speed] が [Auto] に設定されている場合は、デュプレックス設定も [Auto] に設定する必要があります。</p>
[ MTU ]	<p>最大伝送単位。これは、インターフェイスで処理できる最大パケットサイズ (バイト単位) です。有効な値の範囲は、インターフェイスタイプによって異なります。</p>
説明	<p>インターフェイスを説明するテキスト。復帰を使用しないで1行に最大240文字を入力します。</p> <p>(注) マルチ コンテキスト モードの場合、システムの説明とコンテキストの説明に関係はありません。</p>
Flow Control Receive	<p>受信フレームのフロー制御設定。</p> <ul style="list-style-type: none"> <li>• [Off]：ネイバー ポートがフロー制御を要求しても、ポートではフロー制御を使用しません。</li> <li>• [On]：ネイバー ポートの要求に従って、ポートでフロー制御を使用します。</li> <li>• [Desired]：ポートでフロー制御フレームは許可されますが、必須ではありません。</li> </ul> <p>フロー制御フレーム (別名ポーズフレーム) は、バッファが一杯になったときに、指定した間隔だけフレームの送信を停止するよう送信元にシグナリングする特別なパケットです。</p>
Flow Control Send	<p>送信フレームのフロー制御設定。</p> <ul style="list-style-type: none"> <li>• [Off]：ポートはネイバー ポートにフロー制御フレームを送信しません。</li> <li>• [On]：ポートはネイバー ポートにフロー制御フレームを送信します。</li> <li>• [Desired]：ポートでフロー制御フレームは許可されますが、必須ではありません。</li> </ul>

要素	説明
ロール (Roles)	インターフェイスに関連付けられたインターフェイス ロールを表示します。インターフェイス ロールとは、各デバイスの設定が生成されるときに、実際のインターフェイス IP アドレスで置き換えられるオブジェクトです。インターフェイス ロールを使用すると、複数のインターフェイスに適用可能な汎用ルールを定義できます。 <a href="#">インターフェイスロールオブジェクトについて</a> を参照してください。

## [Create Interface]/[Edit Interface] ダイアログボックス - ダイナミック モード

[Create Interface] ダイアログボックス (または [Edit Interface] ダイアログボックス) を使用して、ダイナミック モードで稼働する物理インターフェイスや仮想インターフェイスの属性を設定します。ダイナミック ポートは、ネイバー ポートの設定に基づいてリンクをトランク リンクに変換できます。

### ナビゲーションパス

[\[Interfaces/VLANs\] ページ](#) - [\[Interfaces\] タブ \(10 ページ\)](#) に移動し、[追加 (Add)] または [編集 (Edit)] をクリックして [インターフェイスの作成 (Create Interface)]/[インターフェイスの編集 (Edit Interface)] ダイアログボックスを開き、[モード (Mode)] リストから [ダイナミック (Dynamic)] を選択します。

### 関連項目

- [\[Create Interface\]/\[Edit Interface\] ダイアログボックス - アクセス ポート モード \(12 ページ\)](#)
- [\[Create Interface\]/\[Edit Interface\] ダイアログボックス - ルーテッド ポート モード \(17 ページ\)](#)
- [\[Create Interface\]/\[Edit Interface\] ダイアログボックス - トランク ポート モード \(20 ページ\)](#)
- [\[Interface Auto Name Generator\] ダイアログボックス](#)
- [FlexConfig ポリシーとポリシー オブジェクトについて](#)
- [インターフェイス ロール オブジェクトについて](#)

## フィールドリファレンス

表 7: [Create Interface]/[Edit Interface] ダイアログボックス - ダイナミック モード

要素	説明
[Enable Interface]	このチェックボックスをオンにすると、インターフェイスがイネーブルになります。 オフにすると、shutdown コマンドを使用してインターフェイスがディセーブルになります。
タイプ (Type)	定義をインターフェイスに適用するか、サブインターフェイスに適用するかを指定します。 サブインターフェイスを定義する方法の詳細については、 <a href="#">[Create Interface]/[Edit Interface] ダイアログボックス - サブインターフェイス (31 ページ)</a> を参照してください。
Name ([Select] ボタン)	名前が設定されている場合は、生成されたインターフェイスの名前を表示します。 <a href="#">[Interface Auto Name Generator] ダイアログボックス</a> を開くには、[選択 (Select)] をクリックします。このダイアログボックスで、Security Manager がインターフェイス名の生成に使用する詳細情報を入力または編集できます。
[モード (Mode) ]	このインターフェイスのポート設定タイプ。 [Dynamic] を選択すると、ダイナミックポートに関連する設定オプションが表示されます。
ダイナミック ポート設定	
Dynamic Mode	ダイナミック トランク モード : <ul style="list-style-type: none"> <li>• [Auto] : ポートはリンクをトランク リンクに変換できます。ポートが トランク ポートになるのは、ネイバー ポートが [Trunk] または [Desirable] モードに設定されている場合です。</li> <li>• [Desirable] : ポートはアクティブにリンクをトランク リンクに変換しようとします。</li> </ul>
アクセス VLAN ID	ポートがトランクリンクとして機能しない場合に使用するアクセス VLAN ID。ネイバー リンクが [Trunk]、[Auto]、または [Desirable] モードに設定されている場合に、このような状況になる可能性があります。 有効値の範囲は 1 ~ 4094 です。

要素	説明
カプセル化	<p>次のいずれかを選択します。</p> <ul style="list-style-type: none"> <li>• [DOT1Q] : トランク リンクでの VLAN カプセル化を、IEEE 802.1Q 規格で定義されたカプセル化に指定します。イーサネット サブインターフェイスだけに適用されます。</li> <li>• [ISL] : トランク リンクでの ISL カプセル化を指定します。10 ギガビットイーサネット ポートは ISL カプセル化をサポートしていません。</li> <li>• [Negotiate] : インターフェイスがネイバー インターフェイスの設定と機能に基づいて ISL または 802.1Q トランクになるように、ネイバー インターフェイスとネゴシエートすることを指定します。</li> </ul> <p><b>ヒント</b> VLAN をサブインターフェイスに関連付けずに、イーサネット インターフェイスで DOT1Q カプセル化を設定するには、CLI コマンドまたは FlexConfig を使用して <b>vlan-id dot1q</b> コマンドを使用します。メインインターフェイスに VLAN を設定すると、ルータに設定できる VLAN の数が多くなります。</p>
Native VLAN ([Select] ボタン)	<p>[VLAN ID] フィールドで指定された ID を使用して、このインターフェイスに関連付けるネイティブ VLAN を選択できます (ネイティブ VLAN に VLAN ID が指定されていない場合、デフォルト値は 1 です)。このオプションは、802.1Q トランクインターフェイスとして機能する物理インターフェイスを設定する場合にだけ適用されます。</p> <p>カプセル化タイプとして DOT1Q を先に指定しておく必要があります。</p> <p>トランク インターフェイスのネイティブ VLAN は、タグ付けされていないすべての VLAN パケットが論理的に割り当てられる VLAN です。これには、VLAN に関連付けられた管理トラフィックが含まれます。</p> <p>オフにすると、ネイティブ VLAN はこのインターフェイスに関連付けられません。</p> <p>(注) トランク インターフェイスのサブインターフェイスには、ネイティブ VLAN を設定できません。リンクの両端には必ず同じ [Native VLAN] 値を設定してください。同じ値を設定しないと、トラフィックが失われたり、間違った VLAN に送信される場合があります。</p> <p>[VLAN Selector] ダイアログボックス (49 ページ) を開くには、[選択 (Select)] をクリックします。このダイアログボックスで、指定したインターフェイスにネイティブ VLAN を関連付けることができます。</p>

要素	説明
Allowed VLANs ([Select] ボタン)	<p>トランクで許可される VLAN を指定できます。VLAN ID を入力してください。カンマを使用して複数の VLAN を区切るか、またはハイフンを使用して VLAN の範囲を指定します (12,17,22 または 2-200 など)。有効な ID の範囲は 1 ~ 4094 です。</p> <p>あるいは、[選択 (Select)] をクリックして <a href="#">[VLAN Selector] ダイアログボックス (49 ページ)</a> を開きます。このダイアログボックスで、トランクに含める VLAN を選択できます。</p>
Prune VLANs ([Select] ボタン)	<p>プルーニング可能な VLAN を指定できます。VLAN ID を入力してください。カンマを使用して複数の VLAN を区切るか、またはハイフンを使用して VLAN の範囲を指定します (12,17,22 または 2-200 など)。</p> <p>あるいは、[選択 (Select)] をクリックして <a href="#">[VLAN Selector] ダイアログボックス (49 ページ)</a> を開きます。このダイアログボックスで、プルーニング可能な VLAN を選択できます。</p>
Enable VACL Capture	<p>このチェックボックスをオンにすると、VACL キャプチャがイネーブルになります。キャプチャ ビットが設定されると、キャプチャ機能がイネーブルなポートで、転送されたパケットを受信できます。</p> <p>オフにすると、VACL キャプチャがディセーブルになります。</p>
Capture VLANs ([Select] ボタン)	<p>転送された VLAN パケットを VACL で受信する必要がある VLAN を識別できます。このオプションは、[Enable VACL Capture] チェックボックスをオンにした場合にだけ使用できます。</p> <p>カンマで区切られた VLAN ID のリストを入力するか、[選択 (Select)] をクリックして <a href="#">[VLAN Selector] ダイアログボックス (49 ページ)</a> を開きます。</p> <p>VACL は、VLAN パケットが VLAN に最初にルーティングまたはブリッジングされた場合だけ、このパケットをキャプチャできます。キャプチャできるのは、転送されたパケットだけです。</p>
共通インターフェイス設定	

要素	説明
速度	<p>物理インターフェイスの速度。</p> <ul style="list-style-type: none"> <li>• [10] : 10 Mbps で送信します。</li> <li>• [100] : 100 Mbps で送信します。</li> <li>• [1000] : 1,000 Mbps で送信します。</li> <li>• [10000] : 10,000 Mbps で送信します。</li> <li>• [Auto] : [Speed] を [Auto] に設定すると、[Speed] および [Duplex] がどちらもオートネゴシエーションされます。</li> <li>• [Non-Negotiate] : リンクのネゴシエーションをディセーブルにします。</li> </ul>
デュプレックス	<p>インターフェイスのデュプレックス設定 :</p> <ul style="list-style-type: none"> <li>• [Auto] : デュプレックス設定をオートネゴシエーションします。</li> <li>• [Half] : データの送受信を同時には行いません。</li> <li>• [Full] : データの送受信を同時に行います。</li> </ul> <p>[Speed] が [Auto] に設定されている場合は、デュプレックス設定も [Auto] に設定する必要があります。</p>
[ MTU]	<p>最大伝送単位。これは、インターフェイスで処理できる最大パケットサイズ (バイト単位) です。有効な値の範囲は、インターフェイスタイプによって異なります。</p>
説明	<p>インターフェイスを説明するテキスト。復帰を使用しないで1行に最大240文字を入力します。</p> <p>(注) マルチ コンテキスト モードの場合、システムの説明とコンテキストの説明の関係はありません。</p>
Flow Control Receive	<p>受信フレームのフロー制御設定。</p> <ul style="list-style-type: none"> <li>• [Off] : ネイバー ポートがフロー制御を要求しても、ポートではフロー制御を使用しません。</li> <li>• [On] : ネイバー ポートの要求に従って、ポートでフロー制御を使用します。</li> <li>• [Desired] : ポートでフロー制御フレームは許可されますが、必須ではありません。</li> </ul> <p>フロー制御フレーム (別名 ポーズ フレーム) は、バッファが一杯になったときに、指定した間隔だけフレームの送信を停止するよう送信元にシグナリングする特別なパケットです。</p>

要素	説明
Flow Control Send	送信フレームのフロー制御設定。 <ul style="list-style-type: none"> <li>• [Off] : ポートはネイバー ポートにフロー制御フレームを送信しません。</li> <li>• [On] : ポートはネイバー ポートにフロー制御フレームを送信します。</li> <li>• [Desired] : ポートでフロー制御フレームは許可されますが、必須ではありません。</li> </ul>
ロール (Roles)	インターフェイスに関連付けられたインターフェイス ロールを表示します。インターフェイス ロールとは、各デバイスの設定が生成されるときに、実際のインターフェイス IP アドレスで置き換えられるオブジェクトです。インターフェイス ロールを使用すると、複数のインターフェイスに適用可能な汎用ルールを定義できます。 <a href="#">インターフェイスロールオブジェクトについて</a> を参照してください。

## [Create Interface]/[Edit Interface] ダイアログボックス - サブインターフェイス

[Create Interface] ダイアログボックス（または [Edit Interface] ダイアログボックス）を使用して、Catalyst 6500/7600 デバイスに定義されているサブインターフェイスの属性を設定します。

### ナビゲーションパス

[\[Interfaces/VLANs\] ページ - \[Interfaces\] タブ \(10 ページ\)](#) に移動し、[追加 (Add)] または [編集 (Edit)] をクリックして [インターフェイスの作成 (Create Interface)]/[インターフェイスの編集 (Edit Interface)] ダイアログボックスを開き、[タイプ (Type)] リストから [サブインターフェイス (Subinterface)] を選択します。

### 関連項目

- [\[Create Interface\]/\[Edit Interface\] ダイアログボックス - アクセス ポート モード \(12 ページ\)](#)
- [\[Create Interface\]/\[Edit Interface\] ダイアログボックス - ルーテッド ポート モード \(17 ページ\)](#)
- [\[Create Interface\]/\[Edit Interface\] ダイアログボックス - トランク ポート モード \(20 ページ\)](#)
- [\[Create Interface\]/\[Edit Interface\] ダイアログボックス - ダイナミック モード \(26 ページ\)](#)
- [インターフェイス ロール オブジェクトについて](#)

## フィールド リファレンス

表 8 : [Create Interface]/[Edit Interface] ダイアログボックス - サブインターフェイス

要素	説明
[Enable Interface]	このチェックボックスをオンにすると、サブインターフェイスがイネーブルになります。  オフにすると、shutdown コマンドを使用してサブインターフェイスがディセーブルになります。
タイプ (Type)	定義をインターフェイスに適用するか、サブインターフェイスに適用するかを指定します。[サブインターフェイス (Subinterface)] を選択します。
親	サブインターフェイスの親インターフェイスを識別します。
サブインターフェイスID (Subint. ID) ID	サブインターフェイスの ID アドレスを指定します。数値 ID 文字列は 10 文字を超えることはできません。
IP タイプ (IP Type)	サブインターフェイスで使用される IP アドレスのタイプ:  • [Static IP] : サブインターフェイスで永続的な IP アドレスを使用することを指定し、関連する GUI 要素をアクティブにします。
IP アドレス	IP アドレスを入力できます。
Helper IP Addresses	サブインターフェイスにヘルパー IP アドレスを割り当てることができます。ヘルパー IP アドレスによって、ブロードキャストの DHCP 要求が、DHCP サーバだけに送信されるユニキャストの要求に変換されます。
Mask	サブネットマスクを指定できます。ネットマスク値を入力するか、またはリストからネットマスクを選択できます。ネットマスクを入力する場合は、その値をドット付き 10 進表記 (255.255.255.0 など) で指定するか、またはビット数 (24 など) を入力します。  (注) ネットワークに接続されたインターフェイスに対して、255.255.255.254 または 255.255.255.255 を使用しないでください。これらのネットマスクを使用すると、インターフェイス上のすべてのトラフィックが停止します。



要素	説明
カプセル化	<p>サブインターフェイスに定義するカプセル化タイプ :</p> <ul style="list-style-type: none"> <li>• [blank] : カプセル化は定義されません。</li> <li>• [DOT1Q] : トランク リンクでの VLAN カプセル化を、IEEE 802.1Q 規格で定義されたカプセル化に指定します。イーサネットサブインターフェイスだけに適用されます。</li> <li>• [ISL] : トランク リンクでの ISL カプセル化を指定します。10 ギガビットイーサネットポートは ISL カプセル化をサポートしていません。</li> </ul> <p>ヒント VLAN をサブインターフェイスに関連付けずに、イーサネットインターフェイスで DOT1Q カプセル化を設定するには、CLI コマンドまたは FlexConfig を使用して <b>vlan-id dot1q</b> コマンドを使用します。メインインターフェイスに VLAN を設定すると、ルータに設定できる VLAN の数が多くなります。</p>
VLAN ID (Admin. VLAN ID)	<p>サブインターフェイスにカプセル化が定義されている場合にだけ適用されます。</p> <p>サブインターフェイスに関連付ける VLAN ID。</p>
説明	<p>インターフェイスを説明するテキスト。復帰を使用しないで 1 行に最大 240 文字を入力します。</p> <p>(注) マルチ コンテキスト モードの場合、システムの説明とコンテキストの説明に関係はありません。</p>

## [Create Interface]/[Edit Interface] ダイアログボックス - サポートされていないモード

Security Manager でサポートされていないモードが設定されたインターフェイスが検出された場合 (dot1q-tunnel、private-vlan など)、そのインターフェイスは [Unsupported] モードで表示されます。このインターフェイスの属性を表示できますが、設定を変更する場合は、まずモードを変更する必要があります。[Mode] を除くすべての定義フィールドは読み取り専用です。

### ナビゲーションパス

[Interfaces/VLANs] ページ - [Interfaces] タブ (10 ページ) に移動し、モードが [サポート対象外 (Unsupported)] として定義されているインターフェイスを選択します。次に、[追加 (Add)] または [編集 (Edit)] をクリックして [インターフェイスの作成/編集 (Create/Edit Interface)] ダイアログボックスを開きます。

### 関連項目

- [\[Create Interface\]/\[Edit Interface\] ダイアログボックス - アクセス ポート モード \(12 ページ\)](#)

- [Create Interface]/[Edit Interface] ダイアログボックス - ルーテッドポートモード (17 ページ)
- [Create Interface]/[Edit Interface] ダイアログボックス - トランクポートモード (20 ページ)
- [Create Interface]/[Edit Interface] ダイアログボックス - ダイナミックモード (26 ページ)

## フィールドリファレンス

表 9: [Create Interface]/[Edit Interface] ダイアログボックス - サポートされていないモード

要素	説明
[Enable Interface]	このチェックボックスがオンになっている場合、インターフェイスはイネーブルになっています。  オフになっている場合、インターフェイスは shutdown コマンドを使用してディセーブルになっています。
タイプ (Type)	定義をインターフェイスに適用するか、サブインターフェイスに適用するかを指定します。
Name ([Select] ボタン)	インターフェイスの名前が表示されます。
[モード (Mode) ]	[Unsupported] が表示されます。これは、モードが Security Manager によってサポートされないインターフェイスを示します。  インターフェイスモードを変更するには、別のオプションを選択します。  (注) インターフェイスモードを変更すると、このダイアログボックスの他の設定を変更できるようになります。
速度	物理インターフェイスの速度を表示します。 <ul style="list-style-type: none"> <li>• [10] : 10 Mbps で送信します。</li> <li>• [100] : 100 Mbps で送信します。</li> <li>• [1000] : 1,000 Mbps で送信します。</li> <li>• [10000] : 10,000 Mbps で送信します。</li> <li>• [Auto] : [Speed] を [Auto] に設定すると、[Speed] および [Duplex] がどちらもオートネゴシエーションされます。</li> <li>• [Non-Negotiate] : リンクのネゴシエーションをディセーブルにします。</li> </ul>

要素	説明
デュプレックス	<p>インターフェイスのデュプレックス設定が表示されます。</p> <ul style="list-style-type: none"> <li>• [Auto] : デュプレックス設定をオートネゴシエーションします。</li> <li>• [Half] : データの送受信を同時には行いません。</li> <li>• [Full] : データの送受信を同時に行います。</li> </ul> <p>[Speed] が [Auto] に設定されている場合は、デュプレックス設定も [Auto] に設定する必要があります。</p>
[ MTU]	<p>最大伝送単位が表示されます。これは、インターフェイスで処理できる最大パケットサイズ (バイト単位) です。有効な値の範囲は、インターフェイス タイプによって異なります。</p>
説明	<p>インターフェイスを説明するテキストが表示されます。マルチコンテキストモードの場合、システムの説明とコンテキストの説明に関係はありません。</p>
Flow Control Receive	<p>受信フレームのフロー制御設定が表示されます。</p> <ul style="list-style-type: none"> <li>• [Off] : ネイバーポートがフロー制御を要求しても、ポートではフロー制御を使用しません。</li> <li>• [On] : ネイバーポートの要求に従って、ポートでフロー制御を使用します。</li> <li>• [Desired] : ポートでフロー制御フレームは許可されますが、必須ではありません。</li> </ul> <p>フロー制御フレーム (別名ポーズフレーム) は、バッファが一杯になったときに、指定した間隔だけフレームの送信を停止するよう送信元にシグナリングする特別なパケットです。</p>
Flow Control Send	<p>送信フレームのフロー制御設定が表示されます。</p> <ul style="list-style-type: none"> <li>• [Off] : ポートはネイバーポートにフロー制御フレームを送信しません。</li> <li>• [On] : ポートはネイバーポートにフロー制御フレームを送信します。</li> <li>• [Desired] : ポートでフロー制御フレームは許可されますが、必須ではありません。</li> </ul>

要素	説明
ロール (Roles)	インターフェイスに関連付けられたインターフェイス ロールを表示します。インターフェイス ロールとは、各デバイスの設定が生成されるときに、実際のインターフェイス IP アドレスで置き換えられるオブジェクトです。インターフェイスロールを使用すると、複数のインターフェイスに適用可能な汎用ルールを定義できます。 <a href="#">インターフェイス ロール オブジェクトについて</a> を参照してください。

## VLANs

VLAN は、物理的な場所には基づかずに、論理的にセグメント化されたスイッチドネットワークです。たとえば、VLAN は地理的に分散したワークグループのメンバーを相互接続する場合があります。VLAN は、人員、機器、およびネットワーク インフラストラクチャの物理的な配置を変更する必要性を減らすことで、多くの組織にとって実用的な利便性を提供します。正しく設定された VLAN はスケーラブルかつ安全であり、ネットワーク管理タスクを簡素化できます。

VLAN は、単一のブリッジングドメインで接続されたホストとネットワーク デバイス（ブリッジやルータなど）で構成されます。VLAN 間のトラフィックは、ルーティングする必要があります。

Security Manager を使用すると、VLAN を作成して、Cisco Catalyst スイッチと Cisco 7600 シリーズ ルータ、およびそれらをサポートするサービス モジュールやセキュリティ コンテキストに対して定義されたインターフェイスに対する VLAN 設定を定義できます。

次の項では、Catalyst デバイスの VLAN を定義するときに実行できるアクションについて説明します。

- [VLAN の作成または編集](#) (36 ページ)
- [VLAN の削除](#) (38 ページ)
- [\[Interfaces/VLANs\] ページ - \[VLANs\] タブ](#) (38 ページ)

### 関連項目

- [VLAN グループ](#) (44 ページ)
- [VLAN ACL \(VACL\)](#) (50 ページ)

## VLAN の作成または編集

VLAN を作成、または VLAN の属性を再設定できます。

### 関連項目

- [VLAN の削除](#) (38 ページ)

- [VLAN グループの作成または編集 \(44 ページ\)](#)
- [VACL の作成または編集 \(51 ページ\)](#)
- [\[Create VLAN\]/\[Edit VLAN\] ダイアログボックス \(40 ページ\)](#)
- [VLANs \(36 ページ\)](#)

**ステップ 1** (デバイス ビュー) Catalyst デバイスを選択し、ポリシーセクタから [Interfaces/VLANs] を選択して作業領域で [VLANs] タブをクリックします。

[VLANs] タブが表示されます。このタブの各フィールドの説明については、[\[Interfaces/VLANs\] ページ - \[VLANs\] タブ \(38 ページ\)](#) を参照してください。

**ステップ 2** 次のいずれかを実行します。

- 新しい VLAN の属性を定義するには、[行の追加 (Add Row)] をクリックします。
- VLAN の属性を編集するには、リストで選択して [行の編集 (Edit Row)] をクリックします。

ダイアログボックスにあるフィールドの説明については、[\[Create VLAN\]/\[Edit VLAN\] ダイアログボックス \(40 ページ\)](#) を参照してください。

**ステップ 3** [VLAN ID] フィールドに、VLAN の一意の ID 番号を入力します。ブリッジグループ内の他の VLAN に割り当てられていない番号を入力する必要があります。

**ステップ 4** (任意) VLAN の名前を入力します。

**ステップ 5** (任意) VLAN が VLAN グループの一部である場合は、グループ ID を選択するか、または [グループの追加 (Add Group)] を選択して [VLAN グループの作成 (Create VLAN Group)] ダイアログボックスを開きます。詳細については、[VLAN グループの作成または編集 \(44 ページ\)](#) を参照してください。

**ステップ 6** [Status] リストから、VLAN のステータスを指定します ([Active] または [Suspended])。

**ステップ 7** [タイプ (Type)] リストから [レイヤ 2 (Layer 2)] または [レイヤ 3 (Layer 3)] を選択します。

**ステップ 8** (任意) レイヤ 3 VLAN の場合、Switched Virtual Interface (SVI; スイッチ仮想インターフェイス) を定義します。

- a) SVI をアクティブにするには、[インターフェイスの有効化 (Enable Interface)] チェックボックスをオンにします。SVI を使用すると、VLAN 間のルーティングが可能になり、スイッチへの IP ホスト接続が提供されます。このチェックボックスをオフにすると、SVI はシャットダウンモードで作成されます。
- b) SVI の IP アドレスを入力します。
- c) SVI サブネットマスクを入力するか、または [Subnet Mask] リストからネットマスクの値を選択します。
- d) (任意) 必要に応じて説明を入力します。

**ステップ 9** 次のいずれかまたは両方を実行します。

- アクセスポートを VLAN に関連付けるには、[アクセスポート (Access Ports)] テキストボックスにポート名を入力するか、または [選択 (Select)] をクリックしてインターフェイスセクタを開きます。

- トランクポートを VLAN に関連付けるには、[トランクポート (Trunk Ports)] テキストボックスにポート名を入力するか、または[選択 (Select)] をクリックしてインターフェイスセレクトを開きます。

このダイアログボックスのフィールドの説明については、[\[Interface Selector\] ダイアログボックス - VLAN ACL の内容 \(59 ページ\)](#) を参照してください。ポートの定義の詳細については、[Cisco Catalyst スイッチおよび Cisco 7600 シリーズルータでのポートの作成または編集 \(7 ページ\)](#) を参照してください。

**ステップ 10** [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。

## VLAN の削除

VLAN を削除できます。ただし、VLAN を削除しても、その VLAN を参照する可能性があるポリシーからは削除されません。VLAN を削除する前に、他のポリシーでその VLAN が使用されていないことを確認してください。変更をデータベースに送信するときに、他のポリシーで参照されている未定義の VLAN が示されます。

### 関連項目

- [VLAN の作成または編集 \(36 ページ\)](#)
- [VLANs \(36 ページ\)](#)

**ステップ 1** (デバイス ビュー) デバイス セレクトから Cisco Catalyst スイッチまたは Cisco 7600 シリーズ ルータを選択します。

**ステップ 2** ポリシーセレクトから [インターフェイス/VLAN (Interfaces/VLANs)] を選択します。

**ステップ 3** 作業領域で [VLANs] タブをクリックします。

[VLANs] タブが表示されます。このタブの各フィールドの説明については、[\[Interfaces/VLANs\] ページ - \[VLANs\] タブ \(38 ページ\)](#) を参照してください。

**ステップ 4** テーブルから VLAN を選択し、[行の削除 (Delete Row)] をクリックします。

VLAN が削除されます。

## [Interfaces/VLANs] ページ - [VLANs] タブ

[VLANs] タブを使用して、サポートされている Cisco Catalyst スイッチと Cisco 7600 シリーズルータの VLAN を表示および設定します。

### ナビゲーションパス

- (デバイスビュー) デバイスセレクトから [インターフェイス/VLAN (Interfaces/VLANs)] を選択し、[VLANs] タブをクリックします。

## 関連項目

- [\[Interfaces/VLANs\] ページ - \[VLAN Groups\] タブ](#) (46 ページ)
- [\[Interfaces/VLANs\] ページ - \[Interfaces\] タブ](#) (10 ページ)
- [Catalyst インターフェイス、VLAN、および VLAN グループの概要の表示](#) (4 ページ)
- [FlexConfig ポリシーとポリシー オブジェクトについて](#)
- [\[Create VLAN\]/\[Edit VLAN\] ダイアログボックス](#) (40 ページ)
- [テーブルのフィルタリング](#)

## フィールド リファレンス

表 10: [Interfaces/VLANs] ページ - [VLANs] タブ

要素	説明
VLAN ID (Admin. VLAN ID)	<p>テーブルの行が示す VLAN のインターフェイス固有の ID。VLAN ID は、サブインターフェイスで 802.1Q タグ付きパケットを送受信する場所を示します。VLANID が指定されていない場合は、サブインターフェイスでトラフィックを送受信できません。有効な値の範囲は 2 ~ 4094 です (VLAN ID 1 は予約されています)。</p> <p>(注) 同じ物理インターフェイスに設定されたすべてのサブインターフェイスでは、VLAN ID がすべて一意である必要があります。</p> <p>ヒント VLAN をサブインターフェイスに関連付けずに、イーサネットインターフェイスで DOT1Q カプセル化を設定するには、CLI コマンドまたは FlexConfig を使用して <code>vlan-id dot1q</code> コマンドを使用します。メインインターフェイスに VLAN を設定すると、デバイスに設定できる VLAN の数が多くなります。</p>
名前	インターフェイスまたはサブインターフェイスの対応する VLAN の名前。
インターフェイス	インターフェイス (インターフェイスのロール) または物理的なインターフェイスの論理名を示します。
タイプ (Type)	VLAN が Layer 2 または Layer 3 にアクセスできるかどうかを指定します。
ステータス	VLAN がアクティブになっているか一時停止状態になっているかを示します。
[Add Row] ボタン	新しい VLAN を定義する [Create VLAN] ダイアログボックスを開きます。

要素	説明
[Edit Row] ボタン	選択した VLAN を編集する [Edit VLAN] ダイアログボックスを開きます。
[Delete Row] ボタン	選択した VLAN を削除します。

## [Create VLAN]/[Edit VLAN] ダイアログボックス

[Create VLAN] ダイアログボックス（または [Edit VLAN] ダイアログボックス）を使用して、VLAN 設定および属性を設定または再設定します。

### ナビゲーションパス

[Interfaces/VLANs] ページ - [VLANs] タブ (38 ページ) に移動してから、テーブルの下にある [追加 (Add)] または [編集 (Edit)] ボタンをクリックします。

### 関連項目

- [FlexConfig ポリシーとポリシー オブジェクトについて](#)
- [\[Create VLAN Group\]/\[Edit VLAN Group\] ダイアログボックス \(47 ページ\)](#)
- [\[Interface Selector\] ダイアログボックス - VLAN ACL の内容 \(59 ページ\)](#)

### フィールド リファレンス

表 11: [VLAN] の作成 (*Create VLAN*) / [VLAN] の編集 (*Edit VLAN*) ダイアログボックス

要素	説明
VLAN ID (Admin. VLAN ID)	<p>設定されている VLAN ID が表示されます。設定されていない場合は、ID を手動で入力します。VLAN ID は、インターフェイスまたはサブインターフェイスで 802.1Q タグ付きパケットを送受信する場所を示します。VLAN ID が指定されていない場合は、インターフェイスまたはサブインターフェイスでトラフィックを送受信できません。各 VLAN には ID が必要です。有効値の範囲は 1 ~ 4094 です。</p> <p>(注) 同じ物理インターフェイスに設定されたすべてのサブインターフェイスでは、VLAN ID がすべて一意である必要があります。</p> <p>ヒント VLAN をサブインターフェイスに関連付けずに、イーサネットインターフェイスで DOT1Q カプセル化を設定するには、CLI コマンドまたは FlexConfig を使用して <b>vlan-id dot1q</b> コマンドを使用します。メインインターフェイスに VLAN を設定すると、デバイスに設定できる VLAN の数が多くなります。</p>



要素	説明
名前	VLAN の名前を入力します。VLAN 名を以前に入力した場合は、その名前が表示されます。各 VLAN に ID が必要であり、名前は任意で指定できます。最大長は 32 文字です。
グループ	VLAN が属している VLAN グループ。VLAN は 1 つのグループだけに関連付けることができます。  VLAN を既存のグループに関連付けるか、または [グループの追加 (Add Group)] を選択して [VLAN グループの作成 (Create VLAN Group)] ダイアログボックスを開きます。
ステータス	VLAN の現在のステータス :  <ul style="list-style-type: none"> <li>• [Active] : VLAN はトラフィックを伝送します。</li> <li>• [Suspended] : VLAN はパケットを通過させません。</li> </ul>
タイプ (Type)	指定された VLAN がレイヤ 2 とレイヤ 3 のどちらに設定されているかを示し、使用する VLAN の種類を選択できます。  レイヤ 3 VLAN の場合、IP アドレスが必要であり、VLAN インターフェイスが作成されます。
Switch Virtual Interface	レイヤ 3 VLAN を定義する場合にだけ適用されます。  <ul style="list-style-type: none"> <li>• [Enable Interface] : このチェックボックスをオンにすると、任意の VLAN に接続可能な仮想インターフェイスである <b>Switched Virtual Interface (SVI; スイッチ仮想インターフェイス)</b> がイネーブルになります。SVI を使用すると、VLAN 間のルーティングが可能になり、スイッチへの IP ホスト接続が提供されます。オフにすると、SVI がディセーブルになります。</li> <li>• [IP Address] : SVI の IP アドレス。IP アドレスは管理アクセスに必要です。</li> <li>• [Subnet Mask] : SVI のサブネット マスク。有効なサブネット マスク エントリのリストからオプションを選択します。</li> <li>• [Description] : 復帰を使用しないで 1 行に最大 240 文字の説明を入力できます。マルチ コンテキスト モードの場合、システムの説明とコンテキストの説明に関係はありません。</li> </ul>

要素	説明
Access Ports ([Select] ボタン)	指定した VLAN に関連付けられているアクセス ポートが表示され、指定した VLAN のアクセス ポートの関連付けを追加または削除できます。任意の数のアクセス ポートを VLAN に関連付けることができます。  [Access Port Selector] ダイアログボックス (42 ページ) を開くには、[選択 (Select)] をクリックします。このダイアログボックスで、指定した VLAN にアクセス ポートを関連付けたり、VLAN からアクセス ポートの関連付けを削除したりできます。
Trunk Ports ([Select] ボタン)	指定した VLAN に関連付けられているトランク ポートが表示され、指定した VLAN のトランク ポートの関連付けを追加または削除できます。VLAN は、許可された 1 つ以上のトランク ポートに属することができます。トランク ポート グループに VLAN を含めることができます。  [Trunk Port Selector] ダイアログボックス (43 ページ) を開くには、[選択 (Select)] をクリックします。このダイアログボックスで、指定した VLAN にトランク ポートを関連付けたり、VLAN からトランク ポートの関連付けを削除したりできます。

## [Access Port Selector] ダイアログボックス

[Access Port Selector] ダイアログボックスを使用して、選択した VLAN に関連付けられているアクセス ポートを定義します。

### ナビゲーションパス

[Create VLAN]/[Edit VLAN] ダイアログボックス (40 ページ) を開き、[アクセスポート (Access Ports)] フィールドの [選択 (Select)] をクリックします。

### 関連項目

- [Create Interface]/[Edit Interface] ダイアログボックス - アクセス ポート モード (12 ページ)
- [Trunk Port Selector] ダイアログボックス (43 ページ)
- テーブルのフィルタリング

### フィールド リファレンス

表 12: [Access Port Selector] ダイアログボックス

要素	説明
Available Access Ports	特定の VLAN に割り当てられていないアクセス ポートが表示されます。

要素	説明
[Add >>] ボタン	[Available Access Ports] リストで選択したインターフェイスを [Selected Access Ports] リストに追加します。
[Remove <<] ボタン	選択したインターフェイスを [Selected Access Ports] リストから削除します。
Selected Access Ports	選択されたインターフェイス オブジェクトを表示します。
[Add Row] ボタン	新しいインターフェイスを定義する [Create Interface] ダイアログボックスを開きます。
[Edit Row] ボタン	選択したインターフェイスを編集する [Edit Interface] ダイアログボックスを開きます。

## [Trunk Port Selector] ダイアログボックス

[Trunk Port Selector] ダイアログボックスを使用して、選択した VLAN に関連付けるトランクポートを定義します。

### ナビゲーションパス

[Create VLAN]/[Edit VLAN] ダイアログボックス (40 ページ) を開き、[トランクポート (Trunk Ports) ] フィールドの [選択 (Select) ] をクリックします。

### 関連項目

- [Create Interface]/[Edit Interface] ダイアログボックス - トランク ポート モード (20 ページ)
- [Access Port Selector] ダイアログボックス (42 ページ)
- テーブルのフィルタリング

### フィールド リファレンス

表 13: [Trunk Port Selector] ダイアログボックス

要素	説明
Available Trunk Ports	使用可能なすべてのトランク ポートが表示されます。
[Add >>] ボタン	[Available Trunk Ports] リストで選択したインターフェイスを [Selected Trunk Ports] リストに追加します。
[Remove <<] ボタン	選択したインターフェイスを [Selected Trunk Ports] リストから削除します。

要素	説明
Selected Trunk Ports	選択されたインターフェイス オブジェクトを表示します。
[Add Row] ボタン	新しいインターフェイスを定義する [Create Interface] ダイアログボックスを開きます。
[Edit Row] ボタン	選択したインターフェイスを編集する [Edit Interface] ダイアログボックスを開きます。

## VLAN グループ

VLAN グループは、VLAN の論理集合を定義します。[Interfaces/VLANs] ページの [VLAN Groups] タブに、次の情報が表示されます。

- 選択したデバイスに定義されているすべての VLAN グループ。
- VLAN グループがバインドされているサービス モジュール スロット。
- 各 VLAN グループに属している VLAN。

VLAN グループは、VLAN を FWSM セキュリティ コンテキストに割り当てる場合に使用できます。VLAN グループを複数の FWSM に割り当てたり、各 FWSM に複数の VLAN グループを割り当てたりすることができます。この割り当てを実行するには、[Add Security Context]/[Edit Security Context] ダイアログボックス (FWSM) を参照してください。

次の項では、Catalyst デバイスの VLAN グループを定義するときに行うことができるアクションについて説明します。

- [Create VLAN]/[Edit VLAN] ダイアログボックス (40 ページ)
- VLAN グループの削除 (46 ページ)
- [Interfaces/VLANs] ページ - [VLAN Groups] タブ (46 ページ)

### 関連項目

- インターフェイス (6 ページ)
- VLANs (36 ページ)
- VLAN ACL (VACL) (50 ページ)

## VLAN グループの作成または編集

VLAN グループを作成できます。VLAN グループを作成する場合は、次の点に留意してください。

- 各グループに ID が必要です。

- VLAN グループは 1 つ以上の FWSM モジュールに関連付けることができます。
- 各 VLAN を複数の VLAN グループのメンバーにすることはできません。

#### 関連項目

- [VLAN グループの削除](#) (46 ページ)
- [VLAN の作成または編集](#) (36 ページ)
- [VACL の作成または編集](#) (51 ページ)
- [\[Interfaces/VLANs\] ページ - \[VLAN Groups\] タブ](#) (46 ページ)
- [VLAN グループ](#) (44 ページ)

- 
- ステップ 1** (デバイスビュー) Catalyst デバイスを選択し、ポリシーセクタから [インターフェイス/VLAN (Interfaces/VLANs)] を選択して、作業領域で [VLAN グループ (VLAN Groups)] タブをクリックします。 [VLAN Groups] タブが表示されます。このタブの各フィールドの説明については、 [\[Interfaces/VLANs\] ページ - \[VLAN Groups\] タブ](#) (46 ページ) を参照してください。
- ステップ 2** 次のいずれかを実行します。
- 新しい VLAN グループの属性を定義するには、[行の追加 (Add Row)] をクリックします。
  - VLAN グループの属性を編集するには、リストでグループを選択して [行の編集 (Edit Row)] をクリックします。
- このダイアログボックスのフィールドの説明については、 [\[Create VLAN Group\]/\[Edit VLAN Group\] ダイアログボックス](#) (47 ページ) を参照してください。
- ステップ 3** [VLAN Group ID] フィールドに、VLAN グループの一意的 ID 番号を入力します。他の VLAN グループに割り当てられていない番号を入力する必要があります。
- ステップ 4** VLAN グループを特定のサービスモジュールスロットに関連付けるには ([\[Add Security Context\]/\[Edit Security Context\] ダイアログボックス \(FWSM\)](#))、[サービスモジュールスロット (Service Module Slots)] テキストボックスにスロット番号を入力するか、[選択 (Select)] をクリックしてセクタを開きます。
- (注) この関連付けを定義すると、あとでこの VLAN グループを FWSM のセキュリティ コンテキストに割り当てることができます。 [\[Add Security Context\]/\[Edit Security Context\] ダイアログボックス \(FWSM\)](#) を参照してください。
- ステップ 5** VLAN グループに追加する VLAN を入力するか、[選択 (Select)] をクリックしてセクタを開きます。
- ステップ 6** [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。
-

## VLAN グループの削除

VLAN グループを削除できます。VLAN グループを削除しても、グループ内の VLAN には影響しません。

### 関連項目

- [VLAN グループの作成または編集 \(44 ページ\)](#)
- [VLAN グループ \(44 ページ\)](#)

---

**ステップ 1** (デバイスビュー) デバイスセレクトタから Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータを選択します。

**ステップ 2** ポリシーセレクトタから [インターフェイス/VLAN (Interfaces/VLANs)] を選択します。

**ステップ 3** 作業領域で [VLAN Groups] タブをクリックします。

[VLANs] タブが表示されます。このタブの各フィールドの説明については、[\[Interfaces/VLANs\] ページ - \[VLAN Groups\] タブ \(46 ページ\)](#) を参照してください。

**ステップ 4** テーブルから VLAN グループを選択し、[行の削除 (Delete Row)] をクリックします。VLAN グループが削除されます。

---

## [Interfaces/VLANs] ページ - [VLAN Groups] タブ

[VLAN Groups] タブを使用して、サポートされている 6500 シリーズ スイッチおよび 7600 シリーズ ルータの VLAN グループを表示および設定します。



---

(注) [VLAN Groups] タブは、Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータの場合だけ使用できます。

---

### ナビゲーションパス

- (デバイスビュー) デバイスセレクトタから [インターフェイス/VLAN (Interfaces/VLANs)] を選択し、[VLANグループ (VLAN Groups)] タブをクリックします。

### 関連項目

- [\[Interfaces/VLANs\] ページ - \[VLANs\] タブ \(38 ページ\)](#)
- [\[Interfaces/VLANs\] ページ - \[Interfaces\] タブ \(10 ページ\)](#)
- [Catalyst インターフェイス、VLAN、および VLAN グループの概要の表示 \(4 ページ\)](#)
- [\[Create VLAN Group\]/\[Edit VLAN Group\] ダイアログボックス \(47 ページ\)](#)

- [テーブルのフィルタリング](#)

## フィールド リファレンス

表 14: [Interfaces/VLANs] ページ - [VLAN Groups] タブ

要素	説明
VLAN Group	選択したデバイスに設定されている VLAN グループの数値 ID。
Service Module Slots	シャーシスロット番号（関連サービスモジュールの取り付け先）を、特定の VLAN が VLAN グループへの参加に使用するインターフェイスに関連付けます。
VLAN IDs	このグループに関連付けられている VLAN ID。有効値の範囲は 1 ~ 65535 です。
[Add Row] ボタン	新しい VLAN グループを定義する [Create VLAN Group] ダイアログボックスを開きます。
[Edit Row] ボタン	選択した VLAN グループを編集する [Edit VLAN Group] ダイアログボックスを開きます。
[Delete Row] ボタン	選択した VLAN グループを削除します。

## [Create VLAN Group]/[Edit VLAN Group] ダイアログボックス

[Create VLAN Group]/[Edit VLAN Group] ダイアログボックスを使用して、VLAN グループの属性を設定または再設定します。VLAN グループは、VLAN ポート ポリシーを定義するときに相互に関連付ける VLAN の論理グループです。

### ナビゲーションパス

次のいずれかを実行します。

- [\[Interfaces/VLANs\] ページ - \[VLAN Groups\] タブ \(46 ページ\)](#) に移動してから、テーブルの下にある [追加 (Add)] または [編集 (Edit)] ボタンをクリックします。
- [\[Interfaces/VLANs\] ページ - \[VLANs\] タブ \(38 ページ\)](#) に移動し、テーブルの下にある [追加 (Add)] ボタンまたは [編集 (Edit)] ボタンをクリックして [グループ (Group)] リストから [グループの追加 (Add Group)] を選択します。

### 関連項目

- [\[Service Module Slot Selector\] ダイアログボックス \(48 ページ\)](#)

## フィールド リファレンス

表 15: [Create VLAN Group]/[Edit VLAN Group] ダイアログボックス

要素	説明
VLAN Group ID	802.1q VLAN グループ名。有効値の範囲は 1 ~ 65535 です。
Service Module Slots ([Select] ボタン)	<p>特定の VLAN が VLAN グループへの参加に使用するインターフェイスに関連付けられる、シャーシスロット番号（関連サービスモジュールの取り付け先）。</p> <p>スロット番号を入力するか、または [選択 (Select)] をクリックして <a href="#">[Service Module Slot Selector] ダイアログボックス (48 ページ)</a> を開きます。</p> <p>(注) VLAN グループを FWSM などのサービスモジュールに関連付けたあとで、VLAN グループを FWSM のセキュリティコンテキストに割り当てることができます。 <a href="#">[Add Security Context]/[Edit Security Context] ダイアログボックス (FWSM)</a> を参照してください。</p>
VLAN IDs ([Select] ボタン)	<p>グループに含まれるすべての VLAN のカンマで区切られた ID。各 VLAN を複数のグループのメンバーにすることはできません。</p> <p><a href="#">[Service Module Slot Selector] ダイアログボックス (48 ページ)</a> を開くには、[選択 (Select)] をクリックします。このダイアログボックスで、VLAN グループに含める VLAN を選択できます。</p>

## [Service Module Slot Selector] ダイアログボックス

[Service Module Slot Selector] ダイアログボックスを使用して、サービスモジュールを VLAN に関連付けます。

## ナビゲーションパス

[\[Create VLAN Group\]/\[Edit VLAN Group\] ダイアログボックス \(47 ページ\)](#) に移動し、[サービスモジュールスロット (Service Module Slots)] フィールドの [選択 (Select)] をクリックします。

## 関連項目

- [\[VLAN Selector\] ダイアログボックス \(49 ページ\)](#)
- テーブルのフィルタリング



## フィールド リファレンス

表 16: [Service Module Selector] ダイアログボックス

要素	説明
Available Service Module Slots	定義されているサービス モジュール スロットが表示されます。
[Add >>] ボタン	選択したサービス モジュール スロットを [Available Service Module Slots] リストから [Selected Service Module Slots] リストに移動します。
[Remove <<] ボタン	選択したサービス モジュール スロットを [選択したサービス モジュール (Selected Service Module) ] リストから削除します。
選択したサービス モジュール スロット (Selected Service Module Slots)	選択したサービス モジュール スロットが表示されます。

## [VLAN Selector] ダイアログボックス

[VLAN Selector] ダイアログボックスを使用して、VLAN をインターフェイス、VLAN グループ、セキュリティ コンテキスト、および VACL に関連付けます。

## ナビゲーションパス

インターフェイス、VLAN グループ、IDSM 設定、または VACL を定義するときこのダイアログボックスにアクセスするには、VLAN の定義に使用するフィールドの [選択 (Select) ] ボタンをクリックします。

## 関連項目

- [\[Service Module Slot Selector\] ダイアログボックス \(48 ページ\)](#)
- [テーブルのフィルタリング](#)

## フィールド リファレンス

表 17: [VLAN Selector] ダイアログボックス

要素	説明
Available VLANs	設定するオブジェクトに関連付けることができる定義済みの VLAN が表示されます。  (注) 使用可能な VLAN は、設定するオブジェクトのタイプおよびデバイスに定義されているその他の設定によって異なります。たとえば、VLAN グループに割り当てる VLAN を選択する場合、[Available VLANs] リストには、別の VLAN グループに割り当てられていない VLAN だけが含まれます。セキュリティ コンテキストに割り当てる VLAN を選択する場合、[Available VLANs] リストには、設定するサービスモジュールに割り当てられている VLAN グループ内の VLAN だけが含まれます。
[Add >>] ボタン	選択した VLAN を [Available VLANs] リストから [Selected VLANs] リストに移動します。
[Remove <<] ボタン	選択した VLAN を [Selected VLANs] リストから削除します。
Selected VLANs	選択した VLAN が表示されます。
VLAN の範囲	セレクタを開く前に手動で入力された VLAN 範囲 (ある場合)。

## VLAN ACL (VACL)

Cisco IOS の標準 ACL と拡張 ACL は、ルータ インターフェイスに対してだけ設定し、ルーティングされるパケットにだけ適用されます。一方、Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータでは、VLAN ACL (VACL) を使用して、VLAN 内でブリッジングされるすべてのパケット、または WAN インターフェイスを介した VACL キャプチャのために VLAN との間でルーティングされるすべてのパケットのアクセスを制御できます。VACL の特徴は次のとおりです。

- ハードウェアで処理されます。
- Cisco IOS ACL を使用します。
- ハードウェアでサポートされていない Cisco IOS ACL フィールドを無視します。



(注) Security Manager では、MAC ACL (MACL) の作成または設定はサポートされません。MACL は、MAC アドレスに基づいて IPX、DECnet、AppleTalk、VINES、または XNS トラフィックをフィルタリングするために、VACL とともに使用されることがある名前付き ACL です。

VACL を設定して VLAN に適用すると、VLAN に着信するすべてのパケットは VACL に基づいてチェックされます。

VACL を VLAN に適用し、その同じ VLAN 内のルーテッドインターフェイスに ACL を適用すると、VLAN に着信するパケットは、まず VACL に基づいてチェックされます。次に、許可されたパケットは、ルーテッドインターフェイスに到達する前に入力 ACL に基づいてチェックされます。

パケットは、ある VLAN から別の VLAN にルーティングされる場合、まずルーテッドインターフェイスに適用される出力 ACL に基づいてチェックされます。次に、許可されたパケットは、宛先 VLAN に設定された VACL に基づいてチェックされます。

パケットタイプに VACL が設定され、そのタイプのパケットが VACL と一致しない場合のデフォルトアクションは拒否です。

#### VLAN アクセスマップ (VLAN Access Maps)

Security Manager では、VLAN アクセスマップを使用して VACL を設定します。VLAN アクセスマップは概念的にはルートマップと似ており、1 つ以上のステートメント (アクションと一致する条件) を配置したり、重要度に基づいて番号を付けたりするコンテナです。VLAN アクセスマップでは、マップが適用される VLAN を指定したり、マップ名を含めたり、少なくとも 1 つの VACL シーケンスを指定したりする必要があります。

VACL シーケンスにはシーケンス番号と少なくとも 1 つのアクションが必要であり、VACL シーケンスは少なくとも 1 つの ACL と一致する必要があります。

デバイスはシーケンス内のマップ ステートメントを評価します。複数の VLAN アクセスマップを任意のデバイス シャーシに関連付けることができます。

VACL を管理するには、デバイスビューで Catalyst デバイスを選択し、[プラットフォーム (Platform)] > [VLAN アクセスリスト (VLAN Access Lists)] を選択します。VLAN アクセスマップを使用して IP トラフィックの VACL を設定します。

次の項では、Catalyst デバイスの VACL を定義するときに実行できるアクションについて説明します。

- [VACL の作成または編集 \(51 ページ\)](#)
- [VACL の削除 \(53 ページ\)](#)
- [\[VLAN Access Lists\] ページ \(54 ページ\)](#)

#### 関連項目

- [VLANs \(36 ページ\)](#)
- [VLAN グループ \(44 ページ\)](#)

## VACL の作成または編集

VACL を作成または編集できる場合は、次の操作を実行する必要があります。

- VACL に名前を付けます。
- VACL が適用される VLAN を定義します。
- 少なくとも 1 つの VACL シーケンスが含まれるシーケンス マップを定義します。

#### 関連項目

- [VACL の削除 \(53 ページ\)](#)
- [VLAN の作成または編集 \(36 ページ\)](#)
- [VLAN グループの作成または編集 \(44 ページ\)](#)
- [\[Create VLAN ACL\]/\[Edit VLAN ACL\] ダイアログボックス \(56 ページ\)](#)
- [\[VLAN Access Lists\] ページ \(54 ページ\)](#)

**ステップ 1** 次のいずれかを実行します。

- (デバイスビュー) Catalyst デバイスを選択してから、ポリシーセクタで **[プラットフォーム (Platform)]** > **[VLAN アクセスリスト (VLAN Access Lists)]** の順に選択します。
- (ポリシービュー) **[Catalyst プラットフォーム (Catalyst Platform)]** > **[VLAN アクセスリスト (VLAN Access Lists)]** の順に選択します。

[VLAN Access Lists] ページが表示されます。このページにあるフィールドの説明については、[\[VLAN Access Lists\] ページ \(54 ページ\)](#) を参照してください。

**ステップ 2** 次のいずれかを実行します。

- 新しい VACL の属性を定義するには、[行の追加 (Add Row)] をクリックします。
- VACL の属性を編集するには、リストで選択して [行の編集 (Edit Row)] をクリックします。

ダイアログボックスが表示されます。ダイアログボックスにあるフィールドの説明については、[\[Create VLAN ACL\]/\[Edit VLAN ACL\] ダイアログボックス \(56 ページ\)](#) を参照してください。

**ステップ 3** [VLAN ACL 名 (VLAN ACL Name)] フィールドに VACL の名前を入力します。

**ステップ 4** [VLANs] フィールドで、VACL を適用する VLAN を指定するか、または [選択 (Select)] をクリックして VLAN セクタを開きます。

**ステップ 5** シーケンス マップを定義します。

- [シーケンスマップ (Sequence Map)] テーブルの下にある [行の追加 (Add Row)] または [行の編集 (Edit Row)] をクリックします。ダイアログボックスが表示されます。[\[Create VLAN ACL Content\]/\[Edit VLAN ACL Content\] ダイアログボックス \(57 ページ\)](#) を参照してください。
- シーケンスを識別する番号を入力します。
- シーケンスに割り当てる標準 ACL または拡張 ACL を指定します。または、[選択 (Select)] をクリックしてリストから ACL オブジェクトを選択するか、新しい ACL オブジェクトを作成します。ACL オ

プロジェクトの詳細については、[アクセス コントロール リスト オブジェクトの作成](#)を参照してください。

- d) このシーケンスで定義されている ACL と一致するトラフィックに対して実行するアクションを指定します (アクションとして [リダイレクト (Redirect)] を選択した場合は、物理的な宛先インターフェイスを指定するか、または [選択 (Select)] をクリックしてセレクタを表示します。[ポリシー定義中のインターフェイスの指定](#) を参照してください)。
- e) [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。シーケンスが [Sequence Map] テーブルに表示されます。
- f) プロセスを繰り返して、シーケンスをシーケンス マップに追加します。
- g) 上向きおよび下向き矢印を使用して、必要に応じてシーケンスを並べ替えます。

(注) シーケンスを配置する順序が重要です。フローが許可 ACL エントリと一致する場合、関連付けられたアクションが実行され、残りのシーケンスはチェックされません。フローが拒否 ACL エントリと一致する場合、フローは同じシーケンス内の次の ACL または次のシーケンスに基づいてチェックされます。フローがどの ACL エントリとも一致せず、1 つまたは複数の ACL がそのパケット タイプ用に設定されている場合、パケットは拒否されます。

## VACL の削除

デバイス、ポリシー、またはオブジェクトで使用されていない VACL は削除できます。

### はじめる前に

データベースから VACL を削除する前に、VACL へのすべての参照を削除する必要があります。VACL へのすべての参照を確認するには、その VACL のオブジェクト使用状況レポートを実行します。[オブジェクト使用状況レポートの生成](#) を参照してください。

### 関連項目

- [VACL の作成または編集](#) (51 ページ)
- [\[Interfaces/VLANs\] ページ - \[VLANs\] タブ](#) (38 ページ)
- [VLAN ACL \(VACL\)](#) (50 ページ)

**ステップ 1** 次のいずれかを実行します。

- (デバイスビュー) Catalyst デバイスを選択してから、ポリシーセレクタで [プラットフォーム (Platform)] > [VLAN アクセスリスト (VLAN Access Lists)] の順に選択します。
- (ポリシービュー) [Catalyst プラットフォーム (Catalyst Platform)] > [VLAN アクセスリスト (VLAN Access Lists)] の順に選択します。

[VLAN Access Lists] ページが表示されます。このページにあるフィールドの説明については、[を参照してください](#)。

ステップ2 行をクリックして VACL を選択し、[削除 (Delete)] をクリックします。

ステップ3 [OK] をクリックして変更を保存します。 [\[VLAN Access Lists\] ページ \(54 ページ\)](#)

## [VLAN Access Lists] ページ

[VLAN Access Lists] ページを使用して、Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータの VLAN アクセス リストを表示および設定します。

### ナビゲーションパス

このページには次の手順でアクセスできます。

- (デバイスビュー) デバイスポリシーセレクトタから [\[プラットフォーム \(Platform\)\] > \[VLANアクセスリスト \(VLAN Access Lists\)\]](#) の順に選択します。
- (デバイスビュー) ポリシータイプセレクトタから [\[プラットフォーム \(Platform\)\] > \[VLANアクセスリスト \(VLAN Access Lists\)\]](#) の順に選択します。

### 関連項目

- [アクセス コントロール リスト オブジェクトの作成](#)
- [\[Create VLAN ACL\]/\[Edit VLAN ACL\] ダイアログボックス \(56 ページ\)](#)
- [\[Create VLAN ACL Content\]/\[Edit VLAN ACL Content\] ダイアログボックス \(57 ページ\)](#)
- [テーブルのフィルタリング](#)

### フィールド リファレンス

表 18: [\[VLAN Access Lists\] ページ](#)

要素	説明
[VLAN Access Lists] テーブル	
VLAN ACL	VLAN ACL 名が表示されます。
シーケンス	マップシーケンス番号を指定します。VACL シーケンスは、小さい番号から大きい番号の順に適用されます。
マッチング	一致 ACL が表示されます (定義されている場合)。VACL のマッチングは、ACL 許可が見つかった場合にだけ実行されます。ACL 拒否は無視されます。

要素	説明
操作	<p>アクションとして、パケットのドロップ、ドロップと記録、転送、転送とキャプチャ、またはリダイレクトのいずれかを指定します。</p> <p>(注) リダイレクトアクションを使用すると、最大5つのインターフェイス（物理インターフェイスまたはEtherChannel）を指定できます。EtherChannel メンバまたはVLAN インターフェイスにはパケットをリダイレクトできません。</p>
VLAN IDs	<p>テーブルの行が示す VLAN のインターフェイス固有の ID。VLAN ID は、サブインターフェイスで 802.1Q タグ付きパケットを送受信する場所を示します。VLAN ID が指定されていない場合は、サブインターフェイスでトラフィックを送受信できません。</p>
[Add Row] ボタン	<p>新しい VACL を定義できる [Create VLAN ACL] ダイアログボックスを開きます。</p>
[Edit Row] ボタン	<p>選択した VACL を編集できる [Edit VLAN ACL] ダイアログボックスを開きます。</p>
[Delete Row] ボタン	<p>選択したアクセス リストを削除します。</p>
その他のフィールド	
Log Table Size	<p>ログ テーブルのサイズが表示されます。</p> <p>有効なサイズの範囲は 0 ～ 2048 で、デフォルトは 500 です。新しいフローからの記録済みパケットは、テーブルが一杯になるとドロップされます。</p>
最大パケットレート	<p>秒あたりの最大リダイレクト VACL ロギング パケット レートが表示されます。</p> <p>有効なレートの範囲は秒あたり 10 ～ 5000 パケットで、デフォルトレートは 2000 です。制限を超えるパケットはドロップされます。</p>
Logging Threshold	<p>ロギングしきい値が表示されます（設定されている場合）。デフォルトでは、しきい値は設定されません。</p> <p>VACL ロギングを設定した場合、フローのしきい値に達すると、拒否された IP パケットにより、5 分未満の間隔でフローごとにログ メッセージが生成されます。記録できるのは、ドロップされた IP パケットだけです。</p>

要素	説明
Capture Interfaces	<p>キャプチャビットが設定された転送されるパケットをキャプチャするインターフェイスを示します。任意のインターフェイスをキャプチャインターフェイスとして設定できます。</p> <p>capture アクションを指定すると、転送されたパケットのキャプチャビットが設定されて、キャプチャ機能がイネーブルであるポートがパケットを受信できるようになります。キャプチャできるのは、転送されたパケットだけです。</p> <p>(注) ここに表示される情報は読み取り専用です。キャプチャインターフェイスを定義するには、[Create Interface]/[Edit Interface] ダイアログボックスを使用します。 <a href="#">[Interfaces/VLANs] ページ - [Interfaces] タブ (10 ページ)</a> を参照してください。</p>

## [Create VLAN ACL]/[Edit VLAN ACL] ダイアログボックス

[Create VLAN ACL] ダイアログボックス（または [Edit VLAN ACL] ダイアログボックス）を使用して、VACL 属性を設定または再設定します。

### ナビゲーションパス

[\[VLAN Access Lists\] ページ \(54 ページ\)](#) に移動してから、テーブルの下にある [追加 (Add)] または [編集 (Edit)] ボタンをクリックします。

### 関連項目

- [\[Create VLAN\]/\[Edit VLAN\] ダイアログボックス \(40 ページ\)](#)
- [\[Create VLAN Group\]/\[Edit VLAN Group\] ダイアログボックス \(47 ページ\)](#)
- [テーブルのフィルタリング](#)

### フィールド リファレンス

表 19: [Create VLAN ACL]/[Edit VLAN ACL] ダイアログボックス

要素	説明
VLAN ACL Name	VACL のユーザ定義名。



要素	説明
VLANs ([Select] ボタン)	<p>VACL を適用する VLAN を指定できます。次のいずれかを実行します。</p> <ul style="list-style-type: none"> <li>• VLAN ID を入力します。カンマを使用して複数の VLAN を区切るか、またはハイフンを使用して VLAN の範囲を指定できます。たとえば、12,17,22、2-200 など。有効な ID の範囲は 1 ~ 4094 です。</li> <li>• <a href="#">[VLAN Selector] ダイアログボックス (49 ページ)</a> を開くには、[選択 (Select) ] をクリックします。</li> </ul>
[Sequence Map] テーブル	<p>VLAN アクセス マップに含まれるシーケンス マップ。</p> <p>VLAN アクセスマップは、1つ以上のマップシーケンスで構成される場合があります。各シーケンスでは、トラックフィルタリング用の ACL オブジェクトを指定する match 句および一致 ACL で定義されている基準を満たすパケットに対して実行するアクションを指定する action 句がペアになっています。</p> <ul style="list-style-type: none"> <li>• シーケンス マップを追加するには、[Add Row] (+) ボタンをクリックし、<a href="#">[Create VLAN ACL Content] ダイアログボックス</a>に入力します（<a href="#">[Create VLAN ACL Content]/[Edit VLAN ACL Content] ダイアログボックス (57 ページ)</a> を参照）。</li> <li>• シーケンス マップを編集するには、そのマップを選択して [Edit Row] ボタンをクリックします。</li> <li>• シーケンス マップを削除するには、そのマップを選択して [Delete Row] ボタンをクリックします。</li> <li>• マップの順序を変更するには、マップを選択し、マップが目的の位置に配置されるまで上矢印ボタンまたは下矢印ボタンをクリックします。シーケンス番号は、移動すると変わります。</li> </ul>

## [Create VLAN ACL Content]/[Edit VLAN ACL Content] ダイアログボックス

[Create VLAN ACL Content] ダイアログボックス（または [Edit VLAN ACL Content] ダイアログボックス）を使用して、VACL シーケンスを設定または再設定します。

### ナビゲーションパス

[\[Create VLAN ACL\]/\[Edit VLAN ACL\] ダイアログボックス \(56 ページ\)](#) に移動してから、[シーケンスマップ (Sequence Map) ] テーブルの下にある [追加 (Add) ] ボタンまたは [編集 (Edit) ] ボタンをクリックします。

### 関連項目

- [\[Create VLAN\]/\[Edit VLAN\] ダイアログボックス \(40 ページ\)](#)

- [\[Create VLAN Group\]/\[Edit VLAN Group\] ダイアログボックス](#) (47 ページ)

## フィールド リファレンス

表 20: [Create VLAN ACL Content]/[Edit VLAN ACL Content] ダイアログボックス

要素	説明
シーケンス	VLAN アクセス マップのマップ シーケンス番号を指定します。有効値の範囲は 1 ~ 65535 です。
Match ACLs	シーケンスの match 句に含める ACL を指定します。  シーケンスに含める標準 ACL オブジェクトまたは拡張 ACL オブジェクトの名前を入力します。または、[選択 (Select)] をクリックしてリストから ACL を選択するか、または新しい ACL を作成します。  MAC レイヤ ACL は使用できません。
操作	一致 ACL で定義されている基準を満たすパケットに対して実行するオプション。  <ul style="list-style-type: none"> <li>• [Drop] : パケットをドロップします。</li> <li>• [Drop/Log] : ドロップされたパケットをログに記録します。</li> <li>• [Forward] : ハードウェア スイッチングを使用してパケットを宛先に転送します。</li> <li>• [Forward/Capture] : 転送されるパケットにキャプチャビットを設定して、キャプチャ機能が有効なポートでこのパケットも受信するようにします。</li> <li>• [Redirect] : [Interfaces] フィールドで定義されているイーサネットインターフェイスにパケットをリダイレクトします。</li> </ul>
Interfaces ([Select] ボタン)	指定したアクションが [Redirect] の場合にだけ適用されます。  リダイレクト パケットの宛先インターフェイス。最大 5 つの物理インターフェイスの名前を入力するか、または [選択 (Select)] をクリックして <a href="#">[Interface Selector] ダイアログボックス - VLAN ACL の内容</a> (59 ページ) を開きます。リダイレクトインターフェイスは、VACL アクセスマップが設定されている VLAN 内にある必要があります。  (注) EtherChannel メンバまたは VLAN インターフェイスにはパケットをリダイレクトできません。サブインターフェイスにもパケットをリダイレクトできません。

## [Interface Selector] ダイアログボックス - VLAN ACL の内容

VACL シーケンス マップのエントリを作成するときに、[Interface Selector] ダイアログボックスを使用して、リダイレクト インターフェイスを定義します。

### ナビゲーションパス

- [\[Create VLAN ACL\]/\[Edit VLAN ACL\] ダイアログボックス](#) (56 ページ)
- [\[VLAN Access Lists\] ページ](#) (54 ページ)
- [テーブルのフィルタリング](#)

### フィールド リファレンス

表 21 : [Interface Selector] ダイアログボックス

要素	説明
Available Interfaces	[Interfaces/VLANs] ポリシーで定義されている物理インターフェイスが表示されます。
[Add >>] ボタン	[Available Interfaces] リストで選択されているインターフェイスを [Selected Interfaces] リストに追加します。
[Remove <<] ボタン	選択したインターフェイスを [Selected Interfaces] リストから削除します。
選択されたインターフェイス	選択したインターフェイスが表示されます。

## IDSМ 設定

デバイスビューで Catalyst デバイスを選択し、ポリシーセクタから [プラットフォーム (Platform) ] > [IDSМ設定 (IDSМ Settings) ] を選択すると、次のリストが表示されます。

- Intrusion Detection System Service Module (IDSМ) のデータ ポートの設定が表示されます。
- このリストは、IDSМ データ ポートをチャンネル グループに整理するのに役立ちます。

IDSМ カードは、ネットワーク接続上のセキュリティ脅威を検出し、阻止します。2 つのデータポートに着信したトラフィックを検査し、セキュリティ脅威が検出された場合はパケットをドロップします。データ ポート設定では、次の定義を行います。

- VLAN ID で定義されたデータ ポートで受信するトラフィック
- データ ポートで使用する検知モード :
  - [Trunk (IPS)] : IDSМ は 802.1q トランクとして動作し、同じデータ ポート内にある VLAN ペア間で VLAN ブリッジングを実行します。IDSМ は、VLAN ペアの各 VLAN

上で受信するトラフィックを検査し、そのパケットをペアのもう一方の VLAN に転送するか、または侵入の試行が検出された場合はそのパケットをドロップできます。

- **[Capture (IDS)]** : IDSM は、VACL キャプチャまたは SPAN を使用して、Catalyst スイッチがデータ ポートにコピーしたネットワーク トラフィックをパッシブにモニタします。データ ポートは、別の VLAN をトランキングするように設定できる 802.1q トランクとして動作します。このパッシブ モードで動作している場合、IDSM はネットワーク侵入の試行が検出されてもパケットをドロップできませんが、侵入をブロックする目的でデータ ポートを介して TCP リセットを送信できます。



- (注) Security Manager は、IOS 12.2(18)SXF4 以降が実行されているシャーシにおける一部の IDSM 設定がサポートされます。トランク (IPS) モードとキャプチャ (IDS) モードはサポートされますが、インラインモードはサポートされません。Security Manager では、スパニングツリーまたはアクセス VLAN の一部である IDSM データ ポートを管理できません。

トラフィックの多いネットワークでは、EtherChannel を使用して複数のデータ ポート間でロード バランシングを実行します。これらのデータ ポートは、同じ Catalyst デバイス内の異なる IDSM カードに配置できます。

EtherChannel を使用して、ポート障害時にトラフィックがチャネルグループ内の残りのポートにリダイレクトされることもあります。このような復元力により、ユーザによる介入なしに最小限のパケット損失で侵入の検出や防御を維持できます。

次の項では、IDSM 設定を定義するときに実行できるアクションについて説明します。

- [EtherChannel VLAN 定義の作成または編集 \(60 ページ\)](#)
- [EtherChannel VLAN 定義の削除 \(62 ページ\)](#)
- [データ ポート VLAN 定義の作成または編集 \(63 ページ\)](#)
- [データ ポート VLAN 定義の削除 \(64 ページ\)](#)
- [\[IDSM Settings\] ページ \(65 ページ\)](#)

#### 関連項目

- [VLANs \(36 ページ\)](#)
- [Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータでのポートの作成または編集 \(7 ページ\)](#)

## EtherChannel VLAN 定義の作成または編集

EtherChannel VLAN 定義を行う場合は、次の操作を実行する必要があります。

- チャンネル グループに追加するデータ ポートを含む、スロットとポートの組み合わせを定義します。
- データ ポートで使用する検知モードを選択します。
- データ ポートに転送する VLAN を定義します。

次の制約事項が適用されます。

- チャンネル グループごとに 1 つの定義しか保持できません。
- スロットとデータ ポートの組み合わせごとに 1 つの定義しか保持できません。つまり、このスロットとデータ ポートに対してすでにデータ ポート定義が存在する場合は、EtherChannel VLAN 定義を作成できません。

#### 関連項目

- [EtherChannel VLAN 定義の削除 \(62 ページ\)](#)
- [データ ポート VLAN 定義の作成または編集 \(63 ページ\)](#)
- [IDSM 設定 \(59 ページ\)](#)

**ステップ 1** 次のいずれかを実行します。

- (デバイスビュー) Catalyst デバイスを選択してから、ポリシーセクタで [プラットフォーム (Platform) ] > [IDSM設定 (IDSM Settings) ] の順に選択します。
- (ポリシービュー) [Catalystプラットフォーム (Catalyst Platform) ] > [IDSM設定 (IDSM Settings) ] の順に選択します。

[IDSM Settings] ページが表示されます。このページにあるフィールドの説明については、[\[IDSM Settings\] ページ \(65 ページ\)](#) を参照してください。

**ステップ 2** 次のいずれかを実行します。

- IDSM EtherChannel VLAN 定義を作成するには、[EtherChannel VLANs] テーブルの下にある [行の追加 (Add Row) ] をクリックします。
- IDSM EtherChannel VLAN 定義を編集するには、リストで定義を選択し、テーブルの下にある [行の編集 (Edit Row) ] をクリックします。

[IDSM EtherChannel VLAN] ダイアログボックスが表示されます。このダイアログボックスにあるフィールドの説明については、[\[Create IDSM EtherChannel VLANs\]/\[Edit IDSM EtherChannel VLANs\] ダイアログボックス \(67 ページ\)](#) を参照してください。

**ステップ 3** VLAN のイーサネットインターフェイスにチャンネルグループ番号を割り当てたり、チャンネルグループ番号を変更したりするには、[チャンネルグループ (Channel Group) ] テキストボックスに番号を入力します。

**ステップ 4** IDSM サービス モジュールを取り付けた番号付きシャーシスロットに VLAN を関連付け、その VLAN に 1 つのモジュール データ ポートを関連付けるには、次のいずれかを実行します。

- [スロット/ポート (Slot-Ports)] テキストボックスにスロット/ポート番号を入力します。
- [選択 (Select)] をクリックして、[IDSMスロット/ポートセレクタ (IDSM Slot-Port Selector)] ダイアログボックスを開きます。

(注) 1つのモジュールデータポートを VLAN に関連付けると、データポートを手動で設定する代わりに、グループレベルでポートを設定できます。

**ステップ 5** [Mode] リストから、EtherChannel VLAN の動作モードを選択します。[Capture] を選択する場合は、チェックボックスをオンにして、指定したチャンネルグループをキャプチャ先として設定します。

(注) このチェックボックスをオンにしなかった場合、キャプチャポートはシャットダウンモードで作成されます。

**ステップ 6** 指定したチャンネルグループに VLAN を含めるには、次のいずれかを実行します。

- [VLAN IDs] テキストボックスで数値 ID を入力します。
- [選択 (Select)] をクリックして、[VLANセレクタ (VLAN Selector)] ダイアログボックスを開きます。

複数の VLAN ID を入力または選択できます。

**ステップ 7** [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。

---

## EtherChannel VLAN 定義の削除

IDSM の EtherChannel VLAN 定義を削除できます。

### 関連項目

- [EtherChannel VLAN 定義の作成または編集 \(60 ページ\)](#)
- [データポート VLAN 定義の削除 \(64 ページ\)](#)
- [IDSM 設定 \(59 ページ\)](#)

---

**ステップ 1** 次のいずれかを実行します。

- (デバイスビュー) Catalyst デバイスを選択してから、ポリシーセレクタで [プラットフォーム (Platform)] > [IDSM設定 (IDSM Settings)] の順に選択します。
- (ポリシービュー) [Catalystプラットフォーム (Catalyst Platform)] > [IDSM設定 (IDSM Settings)] の順に選択します。

[IDSM Settings] ページが表示されます。このページにあるフィールドの説明については、[\[IDSM Settings\] ページ \(65 ページ\)](#) を参照してください。

**ステップ 2** テーブル内の行をクリックして、削除する VLAN 定義を選択します。

ステップ 3 [Delete Row] をクリックします。

## データ ポート VLAN 定義の作成または編集

データ ポート VLAN 定義を行う場合は、次の操作を実行する必要があります。

- データ ポートを配置するスロットとポートの組み合わせを定義します。
- データ ポートで使用する検知モードを選択します。
- データ ポートに転送する VLAN を定義します。

次の制約事項が適用されます。

- データ ポートごとに 1 つの定義しか保持できません。
- データ ポートがチャンネルグループの一部としてすでに定義されている場合は、データ ポート定義を作成できません。

### 関連項目

- [データ ポート VLAN 定義の削除 \(64 ページ\)](#)
- [EtherChannel VLAN 定義の作成または編集 \(60 ページ\)](#)
- [IDSM 設定 \(59 ページ\)](#)

ステップ 1 次のいずれかを実行します。

- (デバイスビュー) Catalyst デバイスを選択してから、ポリシーセクタで [プラットフォーム (Platform) ] > [IDSM設定 (IDSM Settings) ] の順に選択します。
- (デバイスビュー) [Catalystプラットフォーム (Catalyst Platform) ] > [IDSM設定 (IDSM Settings) ] の順に選択します。

[IDSM Settings] ページが表示されます。このページにあるフィールドの説明については、[\[IDSM Settings\] ページ \(65 ページ\)](#) を参照してください。

ステップ 2 次のいずれかを実行します。

- IDSM データポート VLAN 定義を作成するには、[データポートVLAN (Data Port VLANs) ] テーブルの下にある [行の追加 (Add Row) ] をクリックします。
- IDSM データポート VLAN 定義を編集するには、リストで定義を選択し、テーブルの下にある [行の編集 (Edit Row) ] をクリックします。

[IDSM Data Port VLAN] ダイアログボックスが表示されます。このダイアログボックスにあるフィールドの説明については、[\[Create IDSM Data Port VLANs\]/\[Edit IDSM Data Port VLANs\] ダイアログボックス \(68 ページ\)](#) を参照してください。

**ステップ 3** IDSM サービス モジュールを取り付けた番号付きシャーシ スロットに VLAN を関連付け、その VLAN に 1 つのモジュール データ ポートを関連付けるには、次のいずれかを実行します。

- [スロット/ポート (Slot-Ports) ] テキストボックスにスロット/ポート番号を入力します。
- [選択 (Select) ] をクリックして、[IDSMスロット/ポートセレクタ (IDSM Slot-Port Selector) ] ダイアログボックスを開きます。

(注) 1 つのモジュール データ ポートを VLAN に関連付けると、データ ポートを手動で設定する代わりに、グループ レベルでポートを設定できます。

**ステップ 4** [Mode] リストから、データ ポート VLAN の動作モードを選択します。[Capture] を選択する場合は、チェックボックスをオンにして、指定したデータ ポートをキャプチャ先として設定します。

(注) このチェックボックスをオンにしなかった場合、キャプチャポートはシャットダウンモードで作成されます。

**ステップ 5** 指定したデータ ポートに VLAN を割り当てるには、次のいずれかを実行します。

- [VLAN IDs] テキスト ボックスで数値 ID を入力します。
- [選択 (Select) ] をクリックして、[VLANセレクタ (VLAN Selector) ] ダイアログボックスを開きます。

複数の VLAN ID を入力または選択できます。

**ステップ 6** [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。

---

## データ ポート VLAN 定義の削除

IDSM のデータ ポート VLAN 定義を削除できます。

### 関連項目

- [データ ポート VLAN 定義の作成または編集 \(63 ページ\)](#)
- [EtherChannel VLAN 定義の削除 \(62 ページ\)](#)
- [IDSM 設定 \(59 ページ\)](#)

---

**ステップ 1** 次のいずれかを実行します。

- (デバイスビュー) Catalyst デバイスを選択してから、ポリシーセレクタで [プラットフォーム (Platform) ] > [IDSM設定 (IDSM Settings) ] の順に選択します。
- (ポリシービュー) [Catalystプラットフォーム (Catalyst Platform) ] > [IDSM設定 (IDSM Settings) ] の順に選択します。



[IDS Settings] ページが表示されます。このページにあるフィールドの説明については、[\[IDS Settings\] ページ \(65 ページ\)](#) を参照してください。

**ステップ 2** テーブル内の行をクリックして、削除する VLAN 定義を選択します。

**ステップ 3** [Delete Row] をクリックします。

## [IDS Settings] ページ

[IDS Settings] ページを使用して、Intrusion Detection System Service Module (IDS) のデータポートとチャンネルグループの VLAN 設定を表示および設定します。

### ナビゲーションパス

このページには次の手順でアクセスできます。

- (デバイスビュー) デバイスポリシーセクタから [プラットフォーム (Platform) ] > [IDS設定 (IDS Settings) ] を選択します。
- (ポリシービュー) ポリシータイプセクタから [Catalystプラットフォーム (Catalyst Platform) ] > [IDS設定 (IDS Settings) ] を選択します。

### 関連項目

- [\[Create IDS EtherChannel VLANs\]/\[Edit IDS EtherChannel VLANs\] ダイアログボックス \(67 ページ\)](#)
- [\[Create IDS Data Port VLANs\]/\[Edit IDS Data Port VLANs\] ダイアログボックス \(68 ページ\)](#)
- [テーブルのフィルタリング](#)
- [ファイアウォール デバイスの管理](#)

### フィールドリファレンス

表 22: [IDS Settings] ページ

要素	説明
[EtherChannel VLANs] テーブル	
チャンネルグループ	イーサネットインターフェイスが割り当てられる EtherChannel グループを示します。

要素	説明
Module Slot-Data Port	2つのポートを区別する番号（1または2）で IDSM サービス モジュールのデータ ポートを示します。  各 IDSM サービス モジュール（ブレード）に2つのデータポートがあります。データポートを個々に設定したり、EtherChannel グループに割り当てたりできます。チャンネルグループ内のすべてのデータポートは、グループ レベルで設定されます。
[モード (Mode) ]	動作モードがトランク (IPS) かキャプチャ (IDS) かを示します。
Capture Enabled	指定したチャンネルグループがキャプチャ先として設定されているかどうかを示します。
Allowed VLANs	指定したチャンネル グループで許可される VLAN を示します。
[Add Row] ボタン	[Create IDSM EtherChannel VLANs] ダイアログボックスを開きます。このダイアログボックスで、EtherChannel グループ内のデータポートに送信するトラフィックと使用する検知モードを定義できます。
[Edit Row] ボタン	[Edit IDSM EtherChannel VLANs] ダイアログボックスを開きます。このダイアログボックスで、EtherChannel VLAN 定義の属性を変更できます。
[Delete Row] ボタン	選択した VLAN を IDSM から削除します。
[Data Port VLANs] テーブル	
Module Slot-Data Port	2つのポートを区別する番号（1または2）で IDSM サービス モジュールのデータ ポートを示します。
[モード (Mode) ]	動作モードがトランク (IPS) かキャプチャ (IDS) かを示します。モードを変更するには、関連するテーブル行を選択して編集します。
Capture Enabled	指定したデータポートがキャプチャ先として設定されているかどうかを示します。
Allowed VLANs	指定したデータ ポートで許可される VLAN を示します。
[Add Row] ボタン	[Create IDSM Data Port VLANs] ダイアログボックスを開きます。このダイアログボックスで、特定のデータポートに送信するトラフィックと使用する検知モードを定義できます。
[Edit Row] ボタン	[Edit IDSM Data Port VLANs] ダイアログボックスを開きます。このダイアログボックスで、データポート VLAN 定義の属性を変更できます。
[Delete Row] ボタン	選択した VLAN を IDSM から削除します。

## [Create IDSM EtherChannel VLANs]/[Edit IDSM EtherChannel VLANs] ダイアログボックス

[Create IDSM EtherChannel VLANs] ダイアログボックス（または [Edit IDSM EtherChannel VLANs] ダイアログボックス）を使用して、IDSM EtherChannel VLAN の属性を設定または再設定します。

### ナビゲーションパス

[IDSM Settings] ページ（65 ページ）に移動してから、[EtherChannel VLAN（EtherChannel VLANs）] テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

### 関連項目

- [Create IDSM Data Port VLANs]/[Edit IDSM Data Port VLANs] ダイアログボックス（68 ページ）
- [IDSM Slot-Port Selector] ダイアログボックス（69 ページ）
- [Service Module Slot Selector] ダイアログボックス（48 ページ）

### フィールドリファレンス

表 23 : [Create IDSM EtherChannel VLANs]/[Edit IDSM EtherChannel VLANs] ダイアログボックス

要素	説明
Channel Group	イーサネット インターフェイスが割り当てられる EtherChannel グループ。
Slot-Ports ([Select] ボタン)	シャーシスロット番号（関連サービスモジュールの取り付け先）を $x-y$ の形式でデータポートに関連付けます。ここで、 $x$ はスロット番号、 $y$ はポート番号です。たとえば、2-1 はスロット 2 のデータポート 1 を表します。  [IDSM Slot-Port Selector] ダイアログボックス（69 ページ）を開くには、[選択（Select）] をクリックします。このダイアログボックスで、EtherChannel グループに含める IDSM のスロットとポートの組み合わせを選択できます。
[モード（Mode）]	EtherChannel グループの動作モード： <ul style="list-style-type: none"> <li>• [Capture (IDS)] : IDSM2 は、VACL キャプチャまたは SPAN を使用して、Catalyst スイッチがデータポートにコピーしたネットワークトラフィックをパッシブにモニタします。</li> <li>• [Trunk (IPS)] : IDSM2 は 802.1Q トランクとして動作し、同じデータポート内にある VLAN ペア間で VLAN ブリッジングを実行します。</li> </ul>

要素	説明
Capture Enabled	動作モードが [Capture (IDS)] の場合にだけ適用されます。 このチェックボックスをオンにすると、指定したチャンネルグループがキャプチャ先として設定されます。オフにすると、チャンネルグループはキャプチャ先として機能しません。
VLAN IDs ([Select] ボタン)	指定したチャンネルグループで許可される VLAN を示します。 <a href="#">[VLAN Selector] ダイアログボックス (49 ページ)</a> を開くには、[選択 (Select)] をクリックします。このダイアログボックスで、追加または除外する VLAN を選択できます。

## [Create IDSM Data Port VLANs]/[Edit IDSM Data Port VLANs] ダイアログボックス

[Create IDSM Data Port VLANs] ダイアログボックス（または [Edit IDSM Data Port VLANs] ダイアログボックス）を使用して、IDSM データポートに送信するトラフィックとそのトラフィックに対して使用する検知モードを定義します。

### ナビゲーションパス

[\[IDSM Settings\] ページ \(65 ページ\)](#) に移動してから、データポート VLAN テーブルの下にある [追加 (Add)] または [編集 (Edit)] ボタンをクリックします。

### 関連項目

- [\[Create IDSM EtherChannel VLANs\]/\[Edit IDSM EtherChannel VLANs\] ダイアログボックス \(67 ページ\)](#)
- [\[IDSM Slot-Port Selector\] ダイアログボックス \(69 ページ\)](#)
- [\[Service Module Slot Selector\] ダイアログボックス \(48 ページ\)](#)

### フィールドリファレンス

表 24: [Create IDSM Data Port VLANs]/[Edit IDSM Data Port VLANs] ダイアログボックス

要素	説明
Slot-Port	シャーシスロット番号（関連サービスモジュールの取り付け先）を $x-y$ の形式でデータポートに関連付けます。ここで、 $x$ はスロット番号、 $y$ はポート番号です。たとえば、2-1 はスロット 2 のデータポート 1 を表します。  <a href="#">[IDSM Slot-Port Selector] ダイアログボックス (69 ページ)</a> を開くには、[選択 (Select)] をクリックします。このダイアログボックスで、データポート VLAN 定義に含める IDSM のスロットとポートの組み合わせを選択できます。

要素	説明
[モード (Mode) ]	データ ポートの動作モード : <ul style="list-style-type: none"> <li>• [Capture (IDS)] : IDSM2 は、VACL キャプチャまたは SPAN を使用して、Catalyst スイッチがデータ ポートにコピーしたネットワーク トラフィックをパッシブにモニタします。</li> <li>• [Trunk (IPS)] : IDSM2 は 802.1Q トランクとして動作し、同じデータ ポート内にある VLAN ペア間で VLAN ブリッジングを実行します。</li> </ul>
Capture Enabled	動作モードが [Capture (IDS)] の場合にだけ適用されます。 このチェックボックスをオンにすると、指定したチャンネルグループがキャプチャ先として設定されます。オフにすると、チャンネルグループはキャプチャ先として機能しません。
VLAN IDs ([Select] ボタン)	指定したデータ ポートで許可される VLAN を示します。 <a href="#">[VLAN Selector] ダイアログボックス (49 ページ)</a> を開くには、[選択 (Select) ] をクリックします。このダイアログボックスで、追加または除外する VLAN を選択できます。

### [IDSM Slot-Port Selector] ダイアログボックス

[IDSM Slot-Port Selector] ダイアログボックスを使用して、スロットポート オブジェクトを EtherChannel グループに関連付けます。

#### ナビゲーションパス

[\[Create IDSM EtherChannel VLANs\]/\[Edit IDSM EtherChannel VLANs\] ダイアログボックス \(67 ページ\)](#) または [\[Create IDSM Data Port VLANs\]/\[Edit IDSM Data Port VLANs\] ダイアログボックス \(68 ページ\)](#) に移動し、[スロットポート (Slot-Port) ] フィールドの [選択 (Select) ] をクリックします。

#### 関連項目

- [\[VLAN Selector\] ダイアログボックス \(49 ページ\)](#)
- [テーブルのフィルタリング](#)

#### フィールド リファレンス

表 25: [IDSM Slot-Port Selector] ダイアログボックス

要素	説明
[Available IDSM Slot-Ports] リスト	使用可能なスロットポート定義が表示されます。

要素	説明
[Add >>] ボタン	EtherChannel VLAN のスロットポートを選択する場合にだけ適用されます。  [Available IDSM Slot-Ports] リストで選択した IDSM スロットポートオブジェクトを [Selected IDSM Slot-Ports] リストに追加します。
[Remove <<] ボタン	EtherChannel VLAN のスロットポートを選択する場合にだけ適用されます。  選択した IDSM スロットポートオブジェクトを [Selected IDSM Slot-Ports] リストから削除します。
[Selected IDSM Slot-Ports] リスト	データポートまたは EtherChannel グループに関連付けるために選択された IDSM スロットポートオブジェクトが表示されます。

## 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。