



仮想スイッチのセットアップ

複数ネットワーク間のパケットスイッチングを提供できるように、レイヤ 2 展開で管理対象デバイスを設定することができます。レイヤ 2 展開では、ネットワークをいくつかの論理セグメントに分割して、スタンドアロン型ブロードキャストドメインとして機能するよう、管理対象デバイス上の仮想スイッチを設定できます。仮想スイッチは、ホストからの Media Access Control (MAC) アドレスを使用して、パケットの送信先を判別します。

仮想スイッチを設定すると、スイッチはまず、スイッチ上の使用可能なすべてのポートからパケットをブロードキャストします。その後は、タグ付きのリターントラフィックを使用して、各ポートに接続されたネットワーク上にどのホストが存在するのかを学習していきます。

仮想スイッチがトラフィックを処理するには、仮想スイッチに複数のスイッチドインターフェイスがなければなりません。仮想スイッチごとに、トラフィックは、スイッチドインターフェイスとして設定されたいくつかのポートに限定されます。たとえば、4 つのスイッチドインターフェイスのある仮想スイッチを設定した場合、ブロードキャスト用に 1 つのポートを介して送入されるパケットは、そのスイッチ上の残る 3 つのポートからのみ送出可能です。

物理スイッチドインターフェイスを設定するときには、仮想スイッチにそれを割り当てる必要があります。また、必要に応じて、物理ポート上に追加の論理スイッチドインターフェイスを定義することもできます。シリーズ 3 管理対象デバイスでは、複数の物理インターフェイスを Link Aggregation Group (LAG) と呼ばれる単一の論理スイッチドインターフェイスにグループ化できます。このように 1 つに集約された論理リンクは、帯域幅と冗長性の向上および、2 つのエンドポイント間でのロードバランシングを実現します。



注意

何らかの理由でレイヤ 2 展開に障害が発生した場合、デバイスはトラフィックを通過させなくなります。

レイヤ 2 展開の設定についての詳細情報は、次の項を参照してください。

- [スイッチドインターフェイスの設定 \(6-2 ページ\)](#)
- [仮想スイッチの設定 \(6-6 ページ\)](#)
- [LAG の設定 \(8-2 ページ\)](#)

スイッチドインターフェイスの設定

ライセンス:Control

サポートされるデバイス:シリーズ 3

物理設定または論理設定を備えるよう、スイッチドインターフェイスをセットアップできます。タグなし VLAN トラフィックを処理するよう物理スイッチドインターフェイスを設定できます。また、VLAN タグが指定されたトラフィックを処理するよう論理スイッチドインターフェイスを作成することもできます。

レイヤ 2 展開では、外部の物理インターフェイス上でトラフィックを受信した場合、それを待機しているスイッチドインターフェイスがなければ、システムはそのトラフィックをドロップします。システムが VLAN タグなしの packets を受信した場合、該当するポートに物理スイッチドインターフェイスがまだ設定されていなければ、パケットはドロップされます。システムが VLAN タグ付きの packets を受信した場合、論理スイッチドインターフェイスがまだ設定されていなければ、同じくパケットはドロップされます。

スイッチドインターフェイスで VLAN タグ付きで受信されたトラフィックをシステムが処理するときには、ルールの評価や転送の決定を行う前に、入力における最も外側の VLAN タグを取り除きます。VLAN タグ付き論理スイッチドインターフェイスを介してデバイスから出るパケットは、出力において関連する VLAN タグ付きでカプセル化されます。

親の物理インターフェイスをインラインまたはパッシブに変更すると、システムは関連するすべての論理インターフェイスを削除することに注意してください。

詳細については、次の各項を参照してください。

- [物理スイッチドインターフェイスの設定 \(6-2 ページ\)](#)
- [論理スイッチドインターフェイスの追加 \(6-4 ページ\)](#)
- [論理スイッチドインターフェイスの削除 \(6-5 ページ\)](#)

物理スイッチドインターフェイスの設定

ライセンス:Control

サポートされるデバイス:シリーズ 3

管理対象デバイス上の 1 つ以上の物理ポートをスイッチドインターフェイスとして設定できます。トラフィックを処理できるようにするには、その前に、物理スイッチドインターフェイスを仮想スイッチに割り当てる必要があります。



注意

センシング インターフェイスまたはインラインセットの MTU の任意の値(シリーズ 2)または最高値(シリーズ 3)を変更すると、変更を適用する際、変更したインターフェイスだけではなく、デバイス上のすべてのセンシング インターフェイスに対するトラフィック インспекションが一時的に中断されます。この中断中にトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。[Snort の再開によるトラフィックへの影響 \(1-9 ページ\)](#)を参照してください。

物理スイッチドインターフェイスを設定する方法:

アクセス: Admin/Network Admin

-
- 手順 1** [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
[デバイス管理 (Device Management)] ページが表示されます。
- 手順 2** スwitchドインターフェイスを設定するデバイスの横にある編集アイコン(✎)をクリックします。
[インターフェイス (Interfaces)] タブが表示されます。
- 手順 3** スwitchドインターフェイスとして設定するインターフェイスの横にある編集アイコン(✎)をクリックします。
[インターフェイスの編集 (Edit Interface)] ポップアップ ウィンドウが表示されます。
- 手順 4** [スイッチド (Switched)] をクリックして、スイッチドインターフェイスのオプションを表示させます。
- 手順 5** オプションで、[セキュリティ ゾーン (Security Zone)] ドロップダウン リストから既存のセキュリティ ゾーンを選択するか、または [新規 (New)] を選択して新しいセキュリティ ゾーンを追加します。
- 手順 6** オプションで、[仮想スイッチ (Virtual Switch)] ドロップダウン リストから既存の仮想スイッチを選択するか、[新規 (New)] を選択して新しい仮想スイッチを追加します。
新しい仮想スイッチを追加する場合は、スイッチドインターフェイスのセットアップ後に、[デバイス管理 (Device Management)] ページの [仮想スイッチ (Virtual Switches)] タブ ([デバイス (Devices)] > [デバイス管理 (Device Management)] > [仮想スイッチ (Virtual Switches)]) でそのスイッチを設定する必要があることに注意してください。[仮想スイッチの追加 \(6-7 ページ\)](#) を参照してください。
- 手順 7** [有効化 (Enabled)] チェック ボックスを選択して、スイッチドインターフェイスがトラフィックを処理できるようにします。
このチェック ボックスをオフにすると、インターフェイスは無効になり、ユーザはセキュリティ上の理由によりアクセスできなくなります。
- 手順 8** [モード (Mode)] ドロップダウン リストからリンク モードを指定するオプションを選択するか、または [自動ネゴシエーション (Autonegotiation)] を選択して、速度とデュプレックス設定を自動的にネゴシエートするようインターフェイスを設定します。モード設定は銅インターフェイスでのみ使用可能であることに注意してください。



(注) 8000 シリーズ アプライアンスのインターフェイスは、半二重オプションをサポートしません。

- 手順 9** [MDI/MDIX] ドロップダウン リストから、インターフェイスの設定対象として MDI (メディア依存型インターフェイス)、MDIX (メディア依存型インターフェイス クロスオーバー)、または Auto-MDIX のいずれかを指定するオプションを選択します。MDI/MDIX 設定は銅線インターフェイス専用であることに注意してください。
デフォルトでは、MDI/MDIX は Auto-MDIX に設定され、MDI と MDIX の間のスイッチングを自動的に処理してリンクを確立します。
- 手順 10** [MTU] フィールドに最大伝送ユニット (MTU) を入力して、パケットの最大許容サイズを指定します。
設定可能な MTU の範囲は、FireSIGHT システムのデバイス モデルおよびインターフェイスのタイプによって異なる場合があります。詳細については、[管理対象デバイスの MTU の範囲 \(4-70 ページ\)](#) を参照してください。

手順 11 [保存(Save)] をクリックします。

物理スイッチドインターフェイスが設定されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください(詳しくは[デバイスへの変更の適用\(4-27 ページ\)](#)を参照してください)。

論理スイッチドインターフェイスの追加

ライセンス:Control


サポートされるデバイス:シリーズ 3

物理スイッチドインターフェイスごとに、複数の論理スイッチドインターフェイスを追加できます。物理インターフェイスで受信した VLAN タグ付きのトラフィックは、各論理インターフェイスにその特定のタグが関連付けられていなければ処理されません。トラフィックを処理するには、論理スイッチドインターフェイスを仮想スイッチに割り当てる必要があります。




注意

センシング インターフェイスまたはインライン セットの MTU の任意の値(シリーズ 2)または最高値(シリーズ 3)を変更すると、変更を適用する際、変更したインターフェイスだけでなく、デバイス上のすべてのセンシング インターフェイスに対するトラフィック インспекションが一時的に中断されます。この中断中にトラフィックがドロップされるか、それ以上インспекションが行われずに受け渡されるかは、管理対象デバイスのモデルおよびインターフェイスのタイプに応じて異なります。[Snort の再開によるトラフィックへの影響\(1-9 ページ\)](#)を参照してください。

既存の論理スイッチドインターフェイスを編集するには、インターフェイスの横にある編集アイコン()をクリックします。

論理スイッチドインターフェイスを追加する方法:

アクセス:Admin/Network Admin

- 手順 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
[デバイス管理 (Device Management)] ページが表示されます。
- 手順 2 スイッチドインターフェイスを追加するデバイスの横にある編集アイコン()をクリックします。
[インターフェイス (Interfaces)] タブが表示されます。
- 手順 3 [インターフェイスの追加 (Add Interface)] をクリックします。
[インターフェイスの追加 (Add Interface)] ポップアップ ウィンドウが表示されます。
- 手順 4 [スイッチド (Switched)] をクリックして、スイッチドインターフェイスのオプションを表示させます。
- 手順 5 [インターフェイス (Interface)] ドロップダウン リストから、VLAN タグ付きトラフィックを受信する物理インターフェイスを選択します。
- 手順 6 [VLAN タグ (VLAN Tag)] フィールドで、このインターフェイス上のインバウンド/アウトバウンドトラフィックに割り当てるタグ値を入力します。この値には、1 ~ 4094 の任意の整数を指定できます。

- 手順 7 オプションで、[セキュリティゾーン (Security Zone)] ドロップダウン リストから既存のセキュリティゾーンを選択するか、または [新規 (New)] を選択して新しいセキュリティゾーンを追加します。
- 手順 8 オプションで、[仮想スイッチ (Virtual Switch)] ドロップダウン リストから既存の仮想スイッチを選択するか、[新規 (New)] を選択して新しい仮想スイッチを追加します。
新しい仮想スイッチを追加する場合は、スイッチドインターフェイスのセットアップ後に、[デバイス管理 (Device Management)] ページ ([デバイス (Devices)] > [デバイス管理 (Device Management)] > [仮想スイッチ (Virtual Switches)]) でそのスイッチを設定する必要があることに注意してください。[仮想スイッチの追加 \(6-7 ページ\)](#) を参照してください。
- 手順 9 [有効化 (Enabled)] チェック ボックスを選択して、スイッチドインターフェイスがトラフィックを処理できるようにします。
このチェック ボックスをオフにすると、インターフェイスは無効になり、管理上はダウンした状態になります。物理インターフェイスを無効にする場合、それに関連付けられているすべての論理インターフェイスも無効にします。
- 手順 10 [MTU] フィールドに最大伝送ユニット (MTU) を入力して、パケットの最大許容サイズを指定します。
設定可能な MTU の範囲は、FireSIGHT システムのデバイス モデルおよびインターフェイスのタイプによって異なる場合があります。詳細については、[管理対象デバイスの MTU の範囲 \(4-70 ページ\)](#) を参照してください。
- 手順 11 [保存 (Save)] をクリックします。
論理スイッチドインターフェイスが追加されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください (詳しくは [デバイスへの変更の適用 \(4-27 ページ\)](#) を参照してください)。



- (注) 1 つの物理インターフェイスを無効化すると、その物理インターフェイスに関連付けられた論理インターフェイスも無効化されます。

論理スイッチドインターフェイスの削除


ライセンス: Control

サポートされるデバイス: シリーズ 3

論理スイッチドインターフェイスを削除すると、それが存在する物理インターフェイスから、および関連付けられている仮想スイッチとセキュリティゾーンからそれが削除されます。

スイッチドインターフェイスを削除する方法:

アクセス: Admin/Network Admin

- 手順 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
[デバイス管理 (Device Management)] ページが表示されます。
- 手順 2 削除するスイッチドインターフェイスが含まれる管理対象デバイスを選択し、そのデバイスの編集アイコン () をクリックします。
デバイスの [インターフェイス (Interfaces)] タブが表示されます。

- 手順 3 削除する論理スイッチド インターフェイスの横にある削除アイコン(🗑️)をクリックします。
- 手順 4 入力を求められた場合、インターフェイスを削除することを確認します。
インターフェイスが削除されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください(詳しくは[デバイスへの変更の適用 \(4-27 ページ\)](#)を参照してください)。

仮想スイッチの設定

ライセンス:Control

サポートされるデバイス:シリーズ 3

レイヤ 2 展開でスイッチド インターフェイスを使用できるようにするには、その前に仮想スイッチを設定して、スイッチド インターフェイスを割り当てます。仮想スイッチは、ネットワーク経由のインバウンド/アウトバウンド トラフィックを処理する複数のスイッチド インターフェイスからなるグループです。

仮想スイッチの設定についての詳細情報は、次の項を参照してください。

- [仮想スイッチの表示 \(6-6 ページ\)](#)
- [仮想スイッチの追加 \(6-7 ページ\)](#)
- [仮想スイッチの詳細設定 \(6-8 ページ\)](#)
- [仮想スイッチの削除 \(6-10 ページ\)](#)

仮想スイッチの表示

ライセンス:Control

サポートされるデバイス:シリーズ 3

[デバイス管理 (Device Management)] ページの [仮想スイッチ (Virtual Switches)] タブには、デバイス上で設定済みのすべての仮想スイッチのリストが表示されます。このページには、次の表に示すように、各スイッチに関する要約情報が含まれます。

表 6-1 仮想スイッチの表形式ビューのフィールド

フィールド	説明
[名前 (Name)]	仮想スイッチの名前。
インターフェイス	仮想スイッチに割り当てられたすべてのスイッチド インターフェイス。[インターフェイス (Interfaces)] タブで無効にしたインターフェイスは表示されません。
ハイブリッド インターフェイス (Hybrid Interface)	仮想スイッチを仮想ルータに結合する、オプション設定のハイブリッド インターフェイス。

表 6-1 仮想スイッチの表形式ビューのフィールド(続き)

フィールド	説明
ユニキャスト パケット (Unicast Packets)	次の項目を含む、仮想スイッチのユニキャスト パケット統計: <ul style="list-style-type: none"> 受信されたユニキャスト パケット 転送されたユニキャスト パケット (ホストによるドロップを除く) 誤ってドロップされたユニキャスト パケット
ブロードキャスト パケット (Broadcast Packets)	次の項目を含む、仮想スイッチのブロードキャスト パケット統計: <ul style="list-style-type: none"> 受信されたブロードキャスト パケット 転送されたブロードキャスト パケット 誤ってドロップされたブロードキャスト パケット

仮想スイッチの追加

ライセンス: Control

サポートされるデバイス: シリーズ 3

[デバイス管理 (Device Management)] ページの [仮想スイッチ (Virtual Switches)] タブから仮想スイッチを追加できます。また、スイッチド インターフェイスを設定するときにスイッチを追加することもできます。

仮想スイッチには、スイッチド インターフェイスだけ割り当てることができます。管理対象デバイス上でスイッチド インターフェイスを設定する前に仮想スイッチを作成する必要がある場合は、空の仮想スイッチを作成し、あとでそれにインターフェイスを追加できます。



ヒント

既存の仮想スイッチを編集するには、スイッチの横にある編集アイコン(✎)をクリックします。

仮想スイッチを追加する方法:

アクセス: Admin/Network Admin

- 手順 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
[デバイス管理 (Device Management)] ページが表示されます。
- 手順 2 仮想スイッチを追加するデバイスの横にある編集アイコン(✎)をクリックします。
[インターフェイス (Interfaces)] タブが表示されます。
- 手順 3 [仮想スイッチ (Virtual Switches)] をクリックします。
[仮想スイッチ (Virtual Switches)] タブが表示されます。
- 手順 4 [仮想スイッチの追加 (Add Virtual Switch)] をクリックします。
[仮想スイッチの追加 (Add Virtual Switch)] ポップアップ ウィンドウが表示されます。
- 手順 5 [名前 (Name)] フィールドに、仮想スイッチの名前を入力します。英数字とスペースを使用できます。
- 手順 6 [利用可能 (Available)] で、仮想スイッチに追加される 1 つ以上のスイッチド インターフェイスを選択します。



ヒント

[インターフェイス(Interfaces)] タブですでに無効にしたインターフェイスは使用できません。インターフェイスを追加した後で無効にすると、設定からそれが削除されます。

手順 7 [追加(Add)] をクリックします。

手順 8 オプションで、[ハイブリッドインターフェイス(Hybrid Interface)] ドロップダウン リストから、仮想スイッチを仮想ルータに結合するハイブリッドインターフェイスを選択します。詳細については、[ハイブリッドインターフェイスの設定\(9-1 ページ\)](#)を参照してください。

手順 9 [保存(Save)] をクリックします。

仮想スイッチが追加されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください(詳しくは[デバイスへの変更の適用\(4-27 ページ\)](#)を参照してください)。



ヒント

スタティック MAC エントリやスパニング ツリー プロトコルなどの詳細なスイッチ設定を構成するには、[仮想スイッチの詳細設定\(6-8 ページ\)](#)を参照してください。

仮想スイッチの詳細設定

ライセンス:Control

サポートされるデバイス:シリーズ 3

仮想スイッチを追加したり編集したりするときには、スタティック MAC エントリの追加、スパニング ツリー プロトコル(STP)の有効化、ブリッジプロトコルデータ ユニット(BPDU)のドロップ、厳密な TCP 適用(強制)の有効化を行うことができます。

時間の経過とともに、仮想スイッチは、ネットワークからのリターン トラフィックにタグを付けることで MAC アドレスを学習します。オプションで、手動でスタティック MAC エントリを追加できます。これにより、MAC アドレスが特定のポート上にあることを指定します。そのポートからトラフィックを受信するかどうかにかかわらず、MAC アドレスはテーブル内で静的な状態を保ちます。仮想スイッチごとに 1 つ以上のスタティック MAC アドレスを指定できます。

STP は、ネットワーク ループを防止するために使われるネットワーク プロトコルです。BPDU は、ネットワーク ブリッジに関する情報を伝送し、ネットワークを介して交換されます。ネットワーク内に冗長リンクがある場合、プロトコルは BPDU を使用して最も高速なネットワーク リンクを識別し、選択します。ネットワーク リンクに障害が発生した場合、スパニング ツリーは既存の代替リンクにフェールオーバーします。

仮想スイッチが複数 VLAN 間でトラフィックをルーティングする場合、ルータ オンア スティックと同様に、BPDU はさまざまな論理スイッチド インターフェイスを介してデバイスを出入りしますが、物理スイッチド インターフェイスは同一です。その結果、STP はデバイスを冗長ネットワーク ループとして識別します。特定のレイヤ 2 展開ではこれにより問題が生じる場合があります。それを防ぐには、トラフィックのモニタリング時にデバイスが BPDU をドロップするよう、ドメイン レベルで仮想スイッチを設定できます。



(注)

デバイス クラスタに展開される予定の仮想スイッチを設定する際には、STP を有効にするよう、Cisco は強く推奨します。

最大の TCP セキュリティを実現するには、厳密な適用 (強制) を有効にできます。この機能は、3 ウェイ ハンドシェイクが完了していない接続をブロックします。厳密な適用では次のパケットもブロックされます。

- 3 ウェイ ハンドシェイクが完了していない接続の非 SYN TCP パケット
- レスポンダが SYN-ACK を送信する前に TCP 接続のイニシエータから送信された非 SYN/RST パケット
- SYN の後、セッションの確立前に TCP 接続のレスポンダから送信された非 SYN-ACK/RST パケット
- イニシエータまたはレスポンダから確立された TCP 接続の SYN パケット

仮想スイッチを論理ハイブリッドインターフェイスに関連付けると、そのスイッチでは、論理ハイブリッドインターフェイスに関連付けられた仮想ルータと同じ厳密な TCP 強制設定が使用されることに注意してください。この場合、スイッチで厳密な TCP 強制を指定することはできません。

仮想スイッチの詳細設定を構成する方法:

アクセス: Admin/Network Admin

-
- 手順 1 [デバイス (Devices)] > [デバイス管理 (Device Management)] を選択します。
[デバイス管理 (Device Management)] ページが表示されます。
- 手順 2 編集する仮想スイッチが含まれるデバイスの横にある編集アイコン(✎)をクリックします。
[インターフェイス (Interfaces)] タブが表示されます。
- 手順 3 [仮想スイッチ (Virtual Switches)] をクリックします。
[仮想スイッチ (Virtual Switches)] タブが表示されます。
- 手順 4 編集する仮想スイッチの横にある編集アイコン(✎)をクリックします。
[仮想スイッチの編集 (Edit Virtual Switch)] ポップアップ ウィンドウが表示されます。
- 手順 5 [詳細設定 (Advanced)] をクリックします。
[詳細設定 (Advanced)] タブが表示されます。
- 手順 6 スタティック MAC エントリを追加するには、[追加 (Add)] をクリックします。
[スタティック MAC アドレスを追加 (Add Static MAC Address)] ポップアップ ウィンドウが表示されます。
- 手順 7 [MAC アドレス (MAC Address)] フィールドで、2 桁の 16 進数 6 組をコロンで区切った標準形式を使用して、アドレスを入力します (たとえば 01:23:45:67:89:AB)。



(注) ブロードキャスト アドレス (00:00:00:00:00:00 と FF:FF:FF:FF:FF:FF) をスタティック MAC アドレスとして追加することはできません。

- 手順 8 [インターフェイス (Interface)] ドロップダウン リストから、MAC アドレスを割り当てるインターフェイスを選択します。
- 手順 9 [追加 (Add)] をクリックします。
MAC アドレスが Static MAC Entries テーブルに追加されます。
MAC アドレスを編集するには、編集アイコン(✎)をクリックします。MAC アドレスを削除するには、削除アイコン(🗑)をクリックします。

- 手順 10** オプションで、スパニング ツリー プロトコルを有効にするには、[スパニング ツリー プロトコルを有効化(Enable Spanning Tree Protocol)] を選択します。仮想スイッチが複数のネットワーク インターフェイス間でトラフィックを切り替える場合にのみ、[スパニング ツリー プロトコルを有効化(Enable Spanning Tree Protocol)] を選択してください。
- [スパニング ツリー プロトコルを有効化(Enable Spanning Tree Protocol)] をクリアしない限り、[BPDU をドロップする(Drop BPDUs)] を選択することはできません。
- 手順 11** オプションで、[厳密な TCP 強制(Strict TCP Enforcement)] を選択して、厳密な TCP 強制を有効にします。
- 仮想スイッチを論理ハイブリッド インターフェイスに関連付けると、このオプションは表示されず、論理ハイブリッド インターフェイスに関連付けられた仮想ルータと同じ設定がスイッチで使用されます。
- 手順 12** オプションで、[BPDU をドロップする(Drop BPDUs)] を選択して、ドメイン レベルで BPDU をドロップします。仮想スイッチが 1 つの物理インターフェイス上の VLAN 間でトラフィックをルーティングする場合にのみ、[BPDU をドロップする(Drop BPDUs)] を選択してください。
- [BPDU をドロップする(Drop BPDUs)] をクリアしない限り、[スパニング ツリー プロトコルを有効化(Enable Spanning Tree Protocol)] を選択することはできません。
- 手順 13** [保存(Save)] をクリックします。
- 変更が保存されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください(詳しくは[デバイスへの変更の適用\(4-27 ページ\)](#)を参照してください)。

仮想スイッチの削除

ライセンス:Control

サポートされるデバイス:シリーズ 3

仮想スイッチを削除すると、そのスイッチに割り当てられたスイッチド インターフェイスを別のスイッチに含めることができるようになります。

仮想スイッチを削除する方法:

アクセス:Admin/Network Admin

- 手順 1** [デバイス(Devices)] > [デバイス管理(Device Management)] を選択します。
- [デバイス管理(Device Management)] ページが表示されます。
- 手順 2** 削除する仮想スイッチが含まれる管理対象デバイスを選択し、そのデバイスの編集アイコン(✎)をクリックします。
- デバイスの [インターフェイス(Interfaces)] タブが表示されます。
- 手順 3** [仮想スイッチ(Virtual Switches)] をクリックします。
- [仮想スイッチ(Virtual Switches)] タブが表示されます。
- 手順 4** 削除する仮想スイッチの横にある削除アイコン(🗑️)をクリックします。
- 手順 5** プロンプトに応じて、仮想スイッチを削除することを確認します。
- 仮想スイッチが削除されます。デバイス設定を適用するまでは、変更内容が有効にならないことに注意してください(詳しくは[デバイスへの変更の適用\(4-27 ページ\)](#)を参照してください)。