CHAPTER 9

ポート セキュリティの設定

Cisco MDS 9000 ファミリのスイッチにはすべて、侵入の試みを拒否し、管理者に侵入を報告するポート セキュリティ機能があります。

（注） ポート セキュリティがサポートされるのは、ファイバ チャネル ポートだけです。

この章の内容は、次のとおりです。

- 「ポート セキュリティの概要」（P.9-1）
- 「ポート セキュリティ設定」（P.9-3）
- 「ポート セキュリティのイネーブル化」（P.9-9）
- 「ポート セキュリティのアクティブ化」（P.9-10）
- 「自動学習のイネーブル化の概要」（P.9-14）
- 「ポート セキュリティの手動設定」（P.9-17）
- 「ポート セキュリティ設定の配信」（P.9-19）
- 「データベース マージに関する注意事項」（P.9-22）
- 「ポート セキュリティのアクティブ化」（P.9-10）
- 「自動学習」（P.9-14）
- 「ポート セキュリティの手動設定」（P.9-17）
- 「ポート セキュリティ設定の配信」（P.9-19）
- 「データベース マージに関する注意事項」（P.9-22）
- 「データベースの相互作用」（P.9-22）
- 「データベース マージに関する注意事項」（P.9-22）

ポート セキュリティの概要

通常、Storage Area Network（SAN; ストレージ エリア ネットワーク）のすべてのファイバ チャネル デバイスを任意の SAN スイッチ ポートに接続して、ゾーン メンバーシップに基づいて SAN サービスにアクセスできます。ポート セキュリティ機能は、次の方法で、Cisco MDS 9000 ファミリのスイッチ ポートへの不正アクセスを防止します。

- 不正なファイバ チャネル デバイス（Nx ポート）およびスイッチ（xE ポート）からのログイン要求は拒否されます。

- 侵入に関するすべての試みは、システム メッセージを通して SAN 管理者に報告されます。
- 設定の配布は Cisco Fabric Services（CFS）インフラストラクチャを使用し、CFS 対応スイッチに制限されます。配布はデフォルトでディセーブルです。
- ポート セキュリティ ポリシーの設定には、ENTERPRISE_PKG ライセンスが必要です（『*Cisco MDS 9000 Family NX-OS Licensing Guide*』を参照）。

ここで説明する内容は、次のとおりです。

- 「ポート セキュリティの実行」（P.9-2）
- 「自動学習の概要」（P.9-2）
- 「ポート セキュリティのアクティブ化」（P.9-3）

ポート セキュリティの実行

ポート セキュリティを実行するには、デバイスまたはスイッチに、それぞれを接続するポート インターフェイスを設定し、設定をアクティブにします。

- デバイスごとに Nx ポート接続を指定するには、Port World Wide Name（pWWN）または Node World Wide Name（nWWN）を使用します。
- スイッチごとに xE ポート接続を指定するには、Switch World Wide Name（sWWN）を使用します。

Nx および xE ポートをそれぞれ設定して、単一ポートまたはポート範囲に限定することができます。

ポート セキュリティ ポリシーは、ポートがアクティブになるごとに、およびポートの起動時に適用されます。

ポート セキュリティ機能は 2 つのデータベースを使用して、設定変更を受け入れて、実装します。

- コンフィギュレーション データベース：設定の変更はすべて、コンフィギュレーション データベースに保存されます。
- アクティブ データベース：ファブリックで現在実行されているデータベースです。ポート セキュリティ機能を実行するには、スイッチに接続しているすべてのデバイスを、ポート セキュリティ アクティブ データベースに登録する必要があります。ソフトウェアはこのアクティブ データベースを使用して、認証を行います。

自動学習の概要

指定した期間にわたって、スイッチがポート セキュリティ設定を自動学習（auto-learn）するように設定できます。この機能を使用すると、任意の Cisco MDS 9000 ファミリ スイッチで、接続先のデバイスおよびスイッチについて自動的に学習できます。ポート セキュリティ機能を最初にアクティブにするときに、この機能を使用すると、各ポートを手動で設定する面倒な作業が軽減されます。自動学習は、Virtual SAN（VSAN; 仮想 SAN）単位で設定する必要があります。この機能をイネーブルにすると、ポート アクセスを設定していない場合でも、スイッチに接続可能なデバイスおよびスイッチが自動学習されます。

自動学習をイネーブルにすると、スイッチにログインしていないデバイスまたはインターフェイスに関する学習だけが実行されます。自動学習がイネーブルのときにポートをシャットダウンすると、そのポート上で学習されたエントリは消去されます。

学習によって、設定済みのポート セキュリティ ポリシーが上書きされることはありません。たとえば、インターフェイスが特定の pWWN を許可するように設定されている場合、自動学習によって、そのインターフェイスに他の pWWN を許可する新しいエントリが追加されることはありません。自動学習モードであっても、他のすべての pWWN はブロックされます。

シャットダウン状態のポートについては、エントリは学習されません。

ポート セキュリティ機能をアクティブにすると、自動学習も自動的にイネーブルになります。

（注）　ポート セキュリティをアクティブにする前に自動学習をイネーブルにした場合、自動学習をディセーブルにしないと、ポート セキュリティをアクティブにできません。

ポート セキュリティのアクティブ化

デフォルトでは、すべての Cisco MDS 9000 ファミリ スイッチで、ポート セキュリティ機能は非アクティブです。

ポート セキュリティ機能をアクティブにすると、次の処理が適用されます。

- 自動学習が自動的にイネーブルになります。
  - この時点から、スイッチにログインしていないデバイスまたはインターフェイスに限り、自動学習が実行されます。
  - 自動学習をディセーブルにするまでは、データベースをアクティブにできません。
- すでにログインしているすべてのデバイスが学習され、アクティブ データベースに追加されます。
- 設定済みデータベースのすべてのエントリが、アクティブ データベースにコピーされます。

データベースをアクティブにすると、以降のデバイスのログインは、自動学習されたエントリを除き、アクティブ化されたポートによってバインドされた WWN ペアの対象になります。自動学習されたエントリをアクティブにするには、自動学習をディセーブルにする必要があります。

ポート セキュリティ機能をアクティブにすると、自動学習も自動的にイネーブルになります。ポート セキュリティ機能をアクティブにして、自動学習をディセーブルにすることもできます。

ヒント　ログインが拒否されてシャットダウンしたポートは、その後ログインが許可されるようにデータベースを設定しても、自動的には起動しません。そのポートをオンラインに戻すには、**no shutdown** CLI コマンドを明示的に発行する必要があります。

ポート セキュリティ設定

ポート セキュリティを設定する手順は、使用する機能によって異なります。CFS 配信を使用している場合には、自動学習の動作が異なります。

ここで説明する内容は、次のとおりです。

- 「自動学習と CFS 配信を使用するポート セキュリティの設定」（P.9-4）
- 「自動学習を使用し、CFS 配信を使用しないポート セキュリティの設定」（P.9-4）
- 「手動データベース設定によるポート セキュリティの設定」（P.9-5）

自動学習と CFS 配信を使用するポート セキュリティの設定

自動学習および CFS 配信を使用してポート セキュリティを設定する手順は、次のとおりです。

ステップ 1　ポート セキュリティをイネーブルにします。「ポート セキュリティのイネーブル化」（P.9-9）を参照してください。

ステップ 2　CFS 配信をイネーブルにします。「配信のイネーブル化」（P.9-19）を参照してください。

ステップ 3　各 VSAN でポート セキュリティをアクティブにします。デフォルトで、自動学習が有効になります。「ポート セキュリティのアクティブ化」（P.9-10）を参照してください。

ステップ 4　CFS コミットを発行して、この設定をファブリック内のすべてのスイッチにコピーします。「変更のコミット」（P.9-20）を参照してください。この時点で、すべてのスイッチがアクティブになり、自動学習が有効になります。

ステップ 5　すべてのスイッチおよびホストが自動学習されるまで待機します。

ステップ 6　各 VSAN で自動学習をディセーブルにします。「自動学習のディセーブル化」（P.9-15）を参照してください。

ステップ 7　CFS コミットを発行して、この設定をファブリック内のすべてのスイッチにコピーします。「変更のコミット」（P.9-20）を参照してください。この時点で、すべてのスイッチから自動学習されたエントリが、すべてのスイッチに配信されるスタティックなアクティブ データベースに組み込まれます。

ステップ 8　アクティブ データベースを、各 VSAN のコンフィギュレーション データベースにコピーします。「ポート セキュリティ データベースのコピー」（P.9-23）を参照してください。

ステップ 9　CFS コミットを発行して、この設定をファブリック内のすべてのスイッチにコピーします。「変更のコミット」（P.9-20）を参照してください。これにより、ファブリック内のすべてのスイッチで、コンフィギュレーション データベースが同一になります。

ステップ 10　ファブリック オプションを使用して、実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。これにより、ポート セキュリティ コンフィギュレーション データベースが、ファブリック内のすべてのスイッチのスタートアップ コンフィギュレーションに保存されます。

自動学習を使用し、CFS 配信を使用しないポート セキュリティの設定

自動学習を使用し、CFS 配信を使用しないポート セキュリティを設定する手順は、次のとおりです。

ステップ 1　ポート セキュリティをイネーブルにします。「ポート セキュリティのイネーブル化」（P.9-9）を参照してください。

ステップ 2　各 VSAN でポート セキュリティをアクティブにします。デフォルトで、自動学習が有効になります。「ポート セキュリティのアクティブ化」（P.9-10）を参照してください。

ステップ 3　すべてのスイッチおよびホストが自動学習されるまで待機します。

ステップ 4　各 VSAN で自動学習をディセーブルにします。「自動学習のディセーブル化」（P.9-15）を参照してください。

ステップ 5　アクティブ データベースを、各 VSAN のコンフィギュレーション データベースにコピーします。「ポート セキュリティ データベースのコピー」（P.9-23）を参照してください。

ステップ 6　実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。これにより、ポート セキュリティ コンフィギュレーション データベースがスタートアップ コンフィギュレーションに保存されます。

ステップ 7　ファブリック内のすべてのスイッチについて、ステップ 1 ～ステップ 6 を繰り返します。

手動データベース設定によるポート セキュリティの設定

ポート セキュリティを設定し、ポート セキュリティ データベースを手動設定する手順は、次のとおりです。

ステップ 1　ポート セキュリティをイネーブルにします。「ポート セキュリティのイネーブル化」（P.9-9）を参照してください。

ステップ 2　各 VSAN のコンフィギュレーション データベースに、すべてのポート セキュリティ エントリを手動で設定します。「ポート セキュリティの手動設定」（P.9-17）を参照してください。

ステップ 3　各 VSAN でポート セキュリティをアクティブにします。デフォルトで、自動学習が有効になります。「ポート セキュリティのアクティブ化」（P.9-10）を参照してください。

ステップ 4　各 VSAN で自動学習をディセーブルにします。「自動学習のディセーブル化」（P.9-15）を参照してください。

ステップ 5　実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。これにより、ポート セキュリティ コンフィギュレーション データベースがスタートアップ コンフィギュレーションに保存されます。

ステップ 6　ファブリック内のすべてのスイッチについて、ステップ 1 ～ステップ 5 を繰り返します。

設定ウィザードを使用したポート セキュリティの設定

ポート セキュリティの設定ウィザードを使用すると、選択した VSAN のポート セキュリティ ポリシーの設定をステップバイステップ方式で実行できます。ポート セキュリティの設定ウィザードでは、設定全体の一元的な管理を可能にする、CFS を使用した中央管理をサポートしています。

ウィザードでは自動的に、いくつかの必須操作が行われます。たとえば、中央管理が必要な場合は、ウィザードが CFS 機能をチェックし、CFS をイネーブルにして、CFS コミットを発行する操作を適切な段階で実行します。

特定のポートでセキュリティを管理する場合は、このウィザードを使って VSAN 全体のポート セキュリティ ポリシーを設定する必要はなく、そのポート自体でアクセスを直接編集できます。この操作は、[Port Binding] ダイアログボックスで実行できます。ポートが付属するスイッチでポート セキュリティをまだイネーブルにしていない場合、ダイアログボックスではまずセキュリティをイネーブルにします。ポート セキュリティがイネーブルになると、ダイアログボックスではユーザの操作に基づいてポリシー データベースが編集されます。

前提条件

ポート セキュリティを設定するための前提条件は、次のとおりです。

- スイッチでポート セキュリティがイネーブルである。
- ポート セキュリティ ポリシーが、バインドされたデバイス、スイッチ、またはポートを編集することによって手動で、または自動学習機能を使用して定義されている。
- ポート セキュリティ ポリシーがアクティブである。

- アクティブ化されたデータベースと設定済みデータベースがコピーによって同期化されている。
- アクティブ化されたデータベースが、スタートアップ コンフィギュレーションにするためにコピーされいる。
- CFS が VSAN 内のすべてのスイッチでイネーブルである。すべての設定の実行に CFS マスタースイッチが選択されている。すべての変更は、CFS **commit** コマンドを使って VSAN に配布されます。

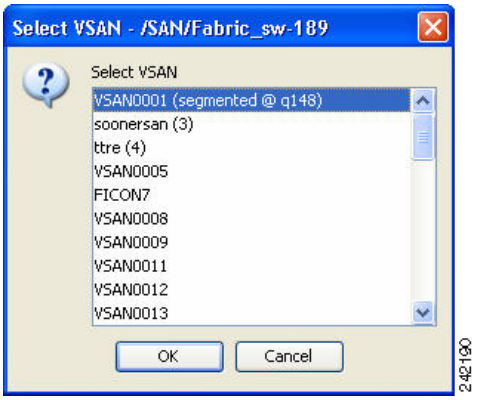
ポート セキュリティを設定する手順は、次のとおりです。

ステップ 1　ツールバーの [Port Security]  ボタンをクリックします。

[Port Security Setup Wizard] を起動する前に、Fabric Manager によって VSAN 内のスイッチの CFS 機能がチェックされます。

VSAN コンテキストを使用できない場合、VSAN を選択するプロンプトが表示されます（図 9-1 を参照）。

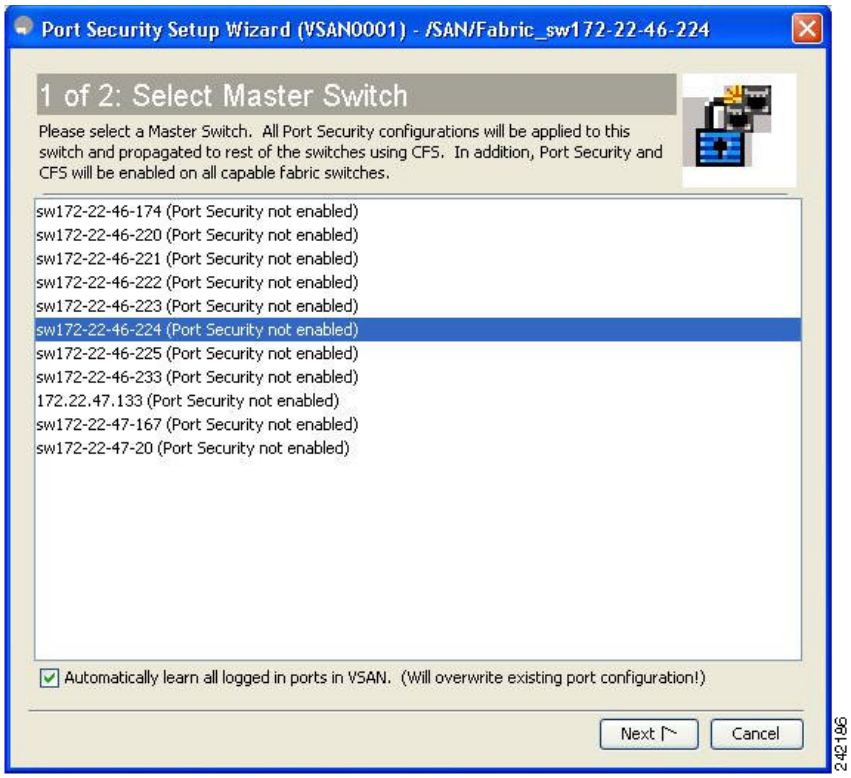
図 9-1　[Select VSAN] ウィンドウ



ステップ 2　リストから VSAN を選択し、[OK] ボタンをクリックします。

[Port Security Setup Wizard] の最初のページが表示されます（図 9-2 を参照）。

図 9-2　[Select Master Switch] ページ



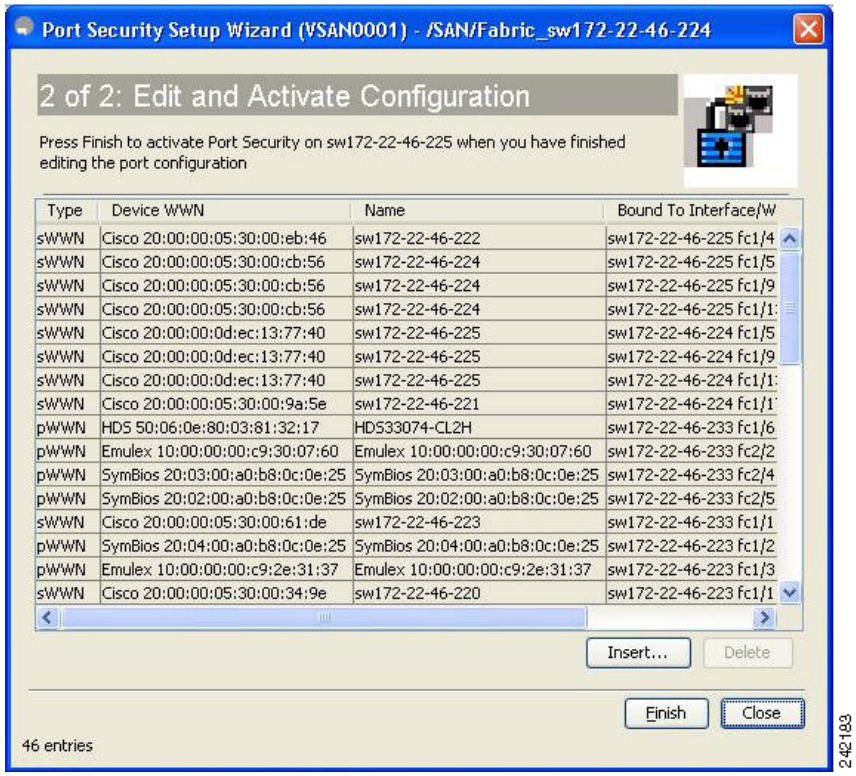
ステップ 3　[Select Master Switch] ページで次の操作を行います。

- 必要なマスター スイッチを選択します。
- ポート設定を自動学習させるには、[Automatically learn all logged in ports in VSAN] チェックボックスをオンにします。

ステップ 4　[Next] ボタンをクリックして先に進みます。

[Edit and Activate Configuration] ページが表示されます（図 9-3 を参照）。

図 9-3　[Edit and Activate Configuration] ページ



ステップ 5　[Insert] ボタンをクリックして、ポート バインディングを作成します。

[Insert Port Security Devices] ダイアログボックスが表示されます（図 9-4 を参照）。

図 9-4　*[Insert Port Security Devices] ダイアログボックス*

ステップ 6　[Insert Port Security Devices] ダイアログボックスでは、次の 2 つのタイプのポート バインディングを作成できます。

- [Port WWN]：インターフェイス WWN にバインドされる pWWN
- [Switch]：インターフェイスにバインドされるスイッチ WWN （主に ISL バインディングに有効）

ステップ 7　オプション ボタンをクリックしてポート バインディングのタイプを選択し、サポートする値を入力します。

ステップ 8　[OK] ボタンをクリックします。

ステップ 9　[Close] ボタンをクリックして [Insert Port Security] ウィンドウを終了します。

（注）　ウィザードの [Edit and Activate Configuration] ページのエントリを削除するには、[Delete] ボタンをクリックします。

ステップ 10　[Finish] をクリックして、選択したスイッチのポート セキュリティの設定を完了します。

ポート セキュリティのイネーブル化

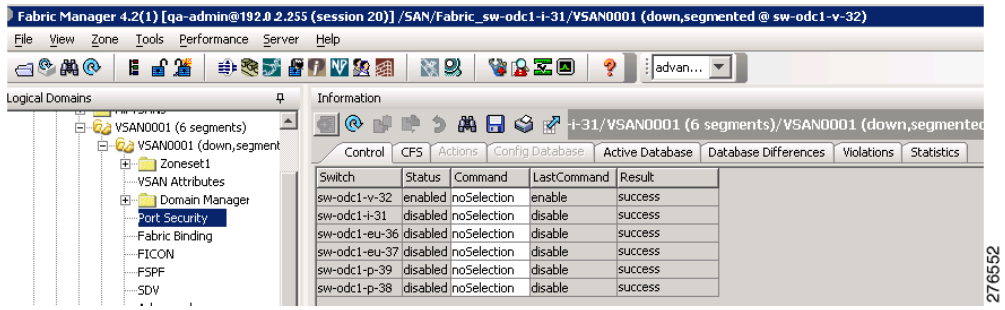
デフォルトでは、すべての Cisco MDS 9000 ファミリ スイッチで、ポート セキュリティ機能はディセーブルです。

Fabric Manager を使用してポート セキュリティをイネーブルにする手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [VSAN] を展開し、[Port Security] を選択します。

[Information] ペインに、その VSAN のポート セキュリティ設定が表示されます（図 9-5 を参照）。

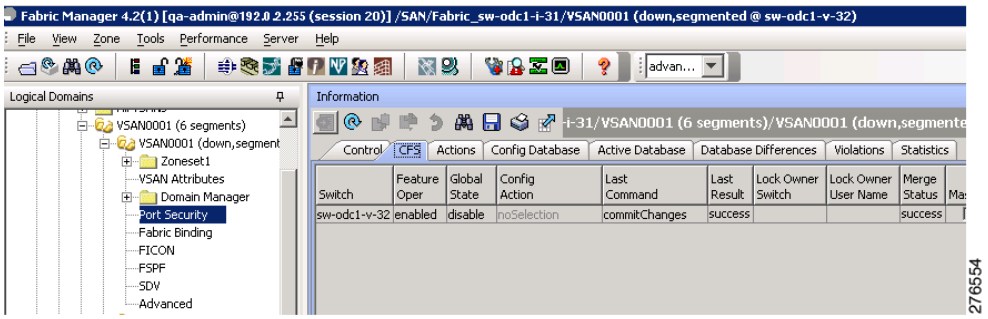
図 9-5　ポート セキュリティ設定



ステップ 2　[CFS] タブをクリックします。

図 9-6 のような情報が表示されます。

図 9-6　ポート セキュリティ CFS



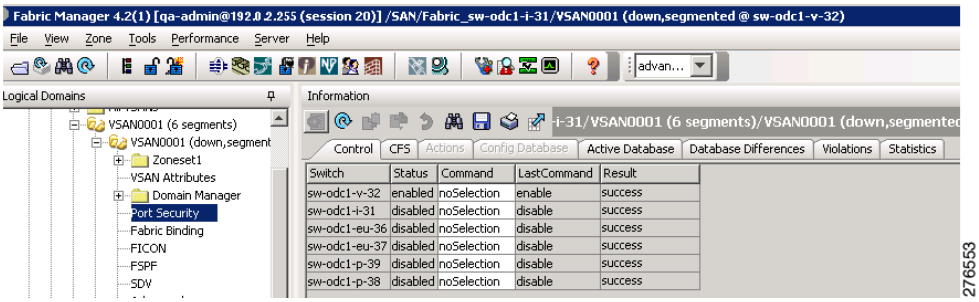
ステップ 3　[Global] カラムの各エントリをクリックし、[enable] を選択して、VSAN 内のすべての参加スイッチ上の CFS をイネーブルにします。

ステップ 4　[Apply Changes] アイコンをクリックし、ポート セキュリティ機能の CFS 配布をイネーブルにします。

ステップ 5　[Control] タブをクリックします。

選択した VSAN 内の全スイッチのポート セキュリティ イネーブル ステートが表示されます（図 9-7 を参照）。

図 9-7　　ポート セキュリティ設定



ステップ 6　VSAN 内の各スイッチについて、[Command] カラムを [enable] に設定します。

ステップ 7　[CFS] タブをクリックし、VSAN 内のすべての参加スイッチについて、[Command] カラムを [commit] に設定します。

ステップ 8　[Apply Changes] アイコンをクリックして、VSAN 内の全スイッチに、イネーブルにしたポート セキュリティを配信します。

ポート セキュリティのアクティブ化

ここで説明する内容は、次のとおりです。

- 「ポート セキュリティのアクティブ化」（P.9-10）
- 「データベースのアクティブ化の拒否」（P.9-11）
- 「ポート セキュリティの強制的なアクティブ化」（P.9-11）
- 「」（P.9-12）
- 「コンフィギュレーション データベースへのアクティブ データベースのコピー」（P.9-12）
- 「アクティブなポート セキュリティ設定の表示」（P.9-13）
- 「ポート セキュリティ統計情報の表示」（P.9-13）
- 「ポート セキュリティ違反の表示」（P.9-13）

ポート セキュリティのアクティブ化

Fabric Manager を使用してポート セキュリティをアクティブにする手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [VSAN] を展開し、[Port Security] を選択します。

[Information] ペインに、その VSAN のポート セキュリティ設定が表示されます。

ステップ 2　[Actions] タブをクリックします。

ステップ 3　ポート セキュリティをアクティブにするスイッチまたは VSAN の横にある、[Activation] の下の [Action] カラムをクリックします。ドロップダウン メニューに、次のオプションが表示されます。

- [activate]：有効なポート セキュリティ設定をアクティブにします。
- [activate (TurnLearningOff)]：有効なポート セキュリティ設定をアクティブにし、自動学習をオフにします。
- [forceActivate]：強制的にアクティブにします。
- [forceActivate (TurnLearningOff)]：強制的にアクティブにし、自動学習をオフにします。
- [deactivate]：現在アクティブであるすべてのポート セキュリティ設定を非アクティブにします。
- [NoSelection]：何も実行しません。

ステップ 4　スイッチに適用する [Action] フィールドを設定します。

ステップ 5　自動学習をディセーブルにするには、VSAN の各スイッチの [AutoLearn] チェックボックスをオフにします。

ステップ 6　[CFS] タブをクリックし、VSAN 内のすべての参加スイッチについて、[Command] カラムを [commit] に設定します。

ステップ 7　Fabric Manager で [Apply Changes] アイコンをクリックするか、Device Manager で [Apply] ボタンをクリックし、変更内容を保存します。

（注）　必要に応じて、自動学習をディセーブルに設定できます（「自動学習のディセーブル化」（P.9-15）を参照）。

データベースのアクティブ化の拒否

次の場合は、データベースをアクティブ化しようとしても、拒否されます。

- 存在しないエントリや矛盾するエントリがコンフィギュレーション データベースに存在するが、アクティブ データベースにはない場合。
- アクティブ化する前に、自動学習機能がイネーブルに設定されていた場合。この状態でデータベースを再アクティブ化するには、自動学習をディセーブルにします。
- 各ポート チャネル メンバーに正確なセキュリティが設定されていない場合。
- 設定済みデータベースが空で、アクティブ データベースが空でない場合。

上記のような矛盾が 1 つまたは複数発生し、データベースのアクティブ化が拒否された場合でも、ポート セキュリティを強制的にアクティブ化すれば、処理を続行できます。

ポート セキュリティの強制的なアクティブ化

ポート セキュリティのアクティブ化要求が拒否された場合、アクティブ化を強制的に実行できます。

（注）　**force** オプションを使用してアクティブ化すると、アクティブ データベースに違反している既存のデバイスをログアウトさせることができます。

Fabric Manager を使用してポート セキュリティ データベースを強制的にアクティブ化する手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [VSAN] を展開し、[Port Security] を選択します。

[Information] ペインに、その VSAN のポート セキュリティ設定が表示されます。

ステップ 2　[Actions] タブをクリックします。

ステップ 3　ポート セキュリティをアクティブにするスイッチまたは VSAN の横にある、[Activation] の下の [Action] カラムをクリックし、[forceactivate] オプションを選択します。

ステップ 4　スイッチに適用する [Action] フィールドを設定します。

ステップ 5　[CFS] タブをクリックし、VSAN 内のすべての参加スイッチについて、[Command] カラムを [commit] に設定します。

ステップ 6　Fabric Manager で [Apply Changes] アイコンをクリックするか、Device Manager で [Apply] ボタンをクリックし、変更内容を保存します。

データベースの再アクティブ化

ヒント　自動学習がイネーブルで、データベースをアクティブ化できない場合、処理を継続できません。

Fabric Manager を使用してポート セキュリティ データベースを再アクティブ化する手順は、次のとおりです。

ステップ 1　自動学習をディセーブルにします。

ステップ 2　コンフィギュレーション データベースにアクティブ データベースをコピーします。

ヒント　アクティブ データベースが空の場合には、この手順を実行できません。

ステップ 3　必要に応じて、コンフィギュレーション データベースを変更します。

ステップ 4　データベースをアクティブにします

コンフィギュレーション データベースへのアクティブ データベースのコピー

Fabric Manager を使用して、コンフィギュレーション データベースにアクティブ データベースをコピーする手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [VSAN] を展開し、[Port Security] を選択します。

[Information] ペインに、その VSAN のポート セキュリティ設定が表示されます。

ステップ 2　[Actions] タブをクリックします。

その VSAN のスイッチが表示されます。

ステップ 3　データベースをコピーするスイッチの横にある、[CopyActive ToConfig] チェックボックスをオンにします。

セキュリティ設定がアクティブになると、アクティブ データベースがコンフィギュレーション データベースにコピーされます。

ステップ 4　セキュリティ設定をアクティブにしたときにデータベースをコピーしない場合は、[CopyActive ToConfig] チェックボックスをオフにします。

ステップ 5　[CFS] タブをクリックし、VSAN 内のすべての参加スイッチについて、[Command] カラムを [commit] に設定します。

ステップ 6　変更内容を保存するには、[Apply Changes] アイコンをクリックします。変更内容を取り消すには、[Undo Changes] アイコンをクリックします。

アクティブなポート セキュリティ設定の表示

Fabric Manager を使用してアクティブなポート セキュリティ設定を表示する手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [VSAN] を展開し、[Port Security] を選択します。

[Information] ペインに、その VSAN のポート セキュリティ設定が表示されます。

ステップ 2　[Active Database] タブをクリックします。

その VSAN のアクティブなポート セキュリティ設定が表示されます。

ポート セキュリティ統計情報の表示

Fabric Manager を使用してポート セキュリティ統計情報を表示する手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [VSAN] を展開し、[Port Security] を選択します。

[Information] ペインに、その VSAN のポート セキュリティ設定が表示されます。

ステップ 2　[Statistics] タブをクリックします。

その VSAN のポート セキュリティ統計情報が表示されます。

ポート セキュリティ違反の表示

ポート違反とは、不正なログイン試行のことです（たとえば、不正なファイバ チャネル デバイスからログイン要求があった場合）。Fabric Manager を使用すると、これらの試行に関するリストを VSAN 単位で表示できます。

ポート セキュリティ違反を表示する手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [VSAN] を展開し、[Port Security] を選択します。

[Information] ペインに、その VSAN のポート セキュリティ設定が表示されます。

ステップ 2　[Violations] タブをクリックします。その VSAN のポート セキュリティ違反が表示されます。

自動学習

ここでは、次の内容について説明します。

- 「自動学習のイネーブル化の概要」（P.9-14）
- 「自動学習のイネーブル化」（P.9-14）
- 「自動学習のディセーブル化」（P.9-15）
- 「自動学習デバイスの許可」（P.9-15）
- 「許可のシナリオ」（P.9-16）

自動学習のイネーブル化の概要

自動学習の設定の状態は、ポート セキュリティ機能の状態によって異なります。

- ポート セキュリティ機能が非アクティブである場合、自動学習はデフォルトでディセーブルになります。
- ポート セキュリティ機能がアクティブである場合、自動学習はデフォルトでイネーブルになります（このオプションを明示的にディセーブルにしていない場合）。

ヒント　VSAN 上の自動学習がイネーブルである場合、**force** オプションを使用しないと、その VSAN のデータベースをアクティブ化できません。

自動学習のイネーブル化

Fabric Manager を使用して自動学習をイネーブルにする手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [VSAN] を展開し、[Port Security] を選択します。

[Information] ペインに、その VSAN のポート セキュリティ設定が表示されます（図 9-8 を参照）。

図 9-8　ポート セキュリティ設定

ステップ 2　[Actions] タブをクリックします。

ステップ 3　ポート セキュリティをアクティブにするスイッチまたは VSAN の横にある、[Activation] の下の [Action] カラムをクリックします。ドロップダウン メニューに、次のオプションが表示されます。

- [activate]：有効なポート セキュリティ設定をアクティブにします。

- [activate (TurnLearningOff)]：有効なポート セキュリティ設定をアクティブにし、自動学習をオフにします。
- [forceActivate]：強制的にアクティブにします。
- [forceActivate (TurnLearningOff)]：強制的にアクティブにし、自動学習をオフにします。
- [deactivate]：現在アクティブであるすべてのポート セキュリティ設定を非アクティブにします。
- [NoSelection]：何も実行しません。

ステップ 4　そのスイッチに適用する、いずれかのポート セキュリティ オプションを選択します。

ステップ 5　自動学習をイネーブルにするには、VSAN の各スイッチの [AutoLearn] チェックボックスをオンにします。

ステップ 6　[Apply Changes] アイコンをクリックして変更内容を保存します。

自動学習のディセーブル化

Fabric Manager を使用して自動学習をディセーブルにする手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [VSAN] を展開し、[Port Security] を選択します。

[Information] ペインに、その VSAN のポート セキュリティ設定が表示されます（図 9-8 を参照）。

ステップ 2　[Actions] タブをクリックします。

その VSAN のスイッチが表示されます。

ステップ 3　自動学習をディセーブルにするには、スイッチの横にある [AutoLearn] チェックボックスをオフにします。

ステップ 4　[Apply Changes] アイコンをクリックして変更内容を保存します。

自動学習デバイスの許可

表 9-1 に、デバイス要求に対して接続が許可される条件を示します。

表 9-1　許可される自動学習デバイス要求

条件	デバイス（pWWN、nWWN、sWWN）	接続先	許可
1	1 つまたは複数のスイッチ ポートに設定されている場合	設定済みスイッチ ポート	許可
2		他のすべてのスイッチ ポート	拒否
3	設定されていない場合	設定されていないスイッチ ポート	許可（自動学習がイネーブルの場合）
4			拒否（自動学習がディセーブルの場合）

表 9-1　許可される自動学習デバイス要求 （続き）

条件	デバイス（pWWN、nWWN、sWWN）	接続先	許可
5	設定されている場合、または設定されていない場合	任意のデバイスを接続できるスイッチ ポート	許可
6	任意のスイッチ ポートにログインするように設定されている場合	スイッチ上の任意のポート	許可
7	設定されていない場合	その他のデバイスが設定されたポート	拒否

許可のシナリオ

ポート セキュリティ機能がアクティブで、アクティブ データベースに次の条件が指定されているものとします。

- pWWN（P1）には、インターフェイス fc1/1（F1）からアクセスできる
- pWWN（P2）には、インターフェイス fc1/1（F1）からアクセスできる
- nWWN（N1）には、インターフェイス fc1/2（F2）からアクセスできる
- インターフェイス fc1/3（F3）からは、任意の WWN にアクセスできる
- nWWN（N3）には、任意のインターフェイスからアクセスできる
- pWWN（P3）には、インターフェイス fc1/4（F4）からアクセスできる
- sWWN（S1）には、インターフェイス fc1/10 ～ 13（F10 ～ F13）からアクセスできる
- pWWN（P10）には、インターフェイス fc1/11（F11）からアクセスできる

表 9-2 に、このアクティブ データベースに対するポート セキュリティ許可の結果を示します。ここに示す条件は、表 9-1 の条件に基づいています。

表 9-2　各シナリオの許可結果

デバイス接続要求	許可	条件	理由
P1、N2、F1	許可	1	競合しません。
P2、N2、F1	許可	1	競合しません。
P3、N2、F1	拒否	2	F1 が P1/P2 にバインドされています。
P1、N3、F1	許可	6	N3 に関するワイルドカード一致です。
P1、N1、F3	許可	5	F3 に関するワイルドカード一致です。
P1、N4、F5	拒否	2	P1 が F1 にバインドされています。
P5、N1、F5	拒否	2	N1 は F2 だけで許可されます。
P3、N3、F4	許可	1	競合しません。
S1、F10	許可	1	競合しません。
S2、F11	拒否	7	P10 が F11 にバインドされています。
P4、N4、F5（自動学習が有効）	許可	3	競合しません。

表 9-2　各シナリオの許可結果 （続き）

デバイス接続要求	許可	条件	理由
P4、N4、F5（自動学習が無効）	拒否	4	一致しません。
S3、F5（自動学習が有効）	許可	3	競合しません。
S3、F5（自動学習が無効）	拒否	4	一致しません。
P1、N1、F6（自動学習が有効）	拒否	2	P1 が F1 にバインドされています。
P5、N5、F1（自動学習が有効）	拒否	7	P1 および P2 だけが F1 にバインドされています。
S3、F4（自動学習が有効）	拒否	7	P3 と F4 がペアになります。
S1、F3（自動学習が有効）	許可	5	競合しません。
P5、N3、F3	許可	6	F3 および N3 に関するワイルドカード（*）一致です。
P7、N3、F9	許可	6	N3 に関するワイルドカード（*）一致です。

ポート セキュリティの手動設定

Cisco MDS 9000 ファミリの任意のスイッチにポート セキュリティを設定する手順は、次のとおりです。

ステップ 1　保護する必要があるポートの WWN を識別します。

ステップ 2　許可された nWWN または pWWN に対して fWWN を保護します。

ステップ 3　ポート セキュリティ データベースをアクティブにします。

ステップ 4　設定を確認します。

ここで説明する内容は、次のとおりです。

- 「WWN の識別の概要」（P.9-17）
- 「許可済みのポート ペアの追加」（P.9-18）
- 「ポート セキュリティ設定の削除」（P.9-19）

WWN の識別の概要

ポート セキュリティを手動で設定する場合は、次の注意事項に従ってください。

- インターフェイスまたは fWWN でスイッチ ポートを識別します。
- pWWN または nWWN でデバイスを識別します。
- Nx ポートが SAN スイッチ ポート Fx にログインできる場合、その Nx ポートは指定された Fx ポートを通した場合に限りログインできます。
- Nx ポートの nWWN が Fx ポート WWN にバインドされている場合、Nx ポートのすべての pWWN は暗黙的に Fx ポートとペアになります。
- TE ポート チェックは、トランク ポートの許可 VSAN リスト内の VSAN ごとに実行されます。

- 同じポートチャネル内のすべてのポートチャネル xE ポートに、同じ WWN セットを設定する必要があります。
- E ポートのセキュリティは、E ポートのポート VSAN に実装されます。この場合、sWWN を使用して許可チェックを保護します。
- アクティブ化されたコンフィギュレーション データベースは、アクティブ データベースに影響を与えることなく変更できます。
- 実行コンフィギュレーションを保存すると、コンフィギュレーション データベース、およびアクティブ データベース内のアクティブ化されたエントリが保存されます。アクティブ データベース内の学習済みエントリは保存されません。

許可済みのポート ペアの追加

バインドする必要がある WWN を識別したら、これらのペアをポート セキュリティ データベースに追加します。

ヒント　リモート スイッチのバインドは、ローカル スイッチで指定できます。リモート インターフェイスを指定する場合、fWWN または sWWN インターフェイスの組み合わせを使用できます。

Fabric Manager を使用して、許可済みのポート ペアをポート セキュリティに追加する手順は、次のとおりです。

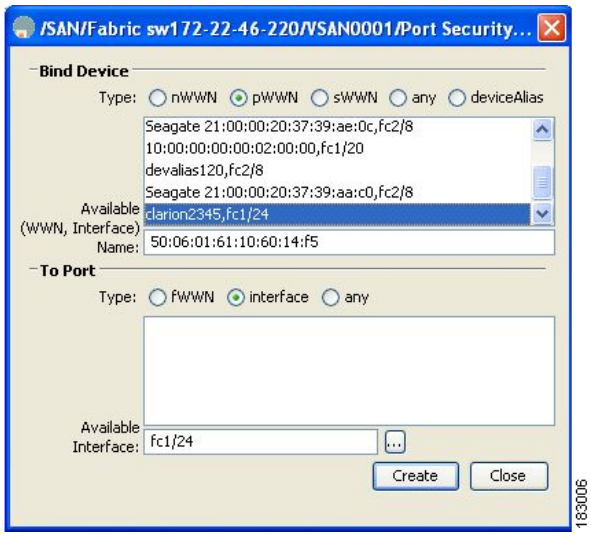
ステップ 1　[Logical Domains] ペインで [VSAN] を展開し、[Port Security] を選択します。

ステップ 2　[Config Database] タブをクリックします。

ステップ 3　[Create Row] アイコンをクリックして、許可済みのポート ペアを追加します。

[Create Port Security] ダイアログボックスが表示されます（図 9-9 を参照）。

図 9-9　[Create Port Security] ダイアログボックス



ステップ 4　リストから、ポート セキュリティ設定を作成するデバイスをダブルクリックします。

ステップ 5　リストから、デバイスをバインドするポートをダブルクリックします。

ステップ 6　[Create] ボタンをクリックして、ポート セキュリティ設定を作成します。

ステップ 7　[Apply Changes] アイコンをクリックして変更内容を保存します。

ポート セキュリティ設定の削除

スイッチ上の既存のデータベースからポート セキュリティ設定を削除する手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [VSAN] を展開し、[Port Security] を選択します。

ステップ 2　[Config Database] タブをクリックします。

VSAN の既存のポート セキュリティ設定が表示されます。

ステップ 3　削除する行をクリックします。

ステップ 4　[Delete Row] をクリックします。

確認ダイアログボックスが表示されます。

ステップ 5　行を削除するには、[Yes] ボタンをクリックします。行を削除しないで確認ダイアログボックスを閉じるには、[No] ボタンをクリックします。

ステップ 6　[Apply Changes] アイコンをクリックして変更内容を保存します。

ポート セキュリティ設定の配信

ポート セキュリティ機能は、Cisco Fabric Services（CFS）インフラストラクチャを使用して効率的なデータベース管理を実行し、VSAN 内のファブリック全体に単一の設定を提供して、ファブリック全体でポート セキュリティ ポリシーを施行します（第 7 章「CFS インフラストラクチャの使用」を参照）。

ここで説明する内容は、次のとおりです。

- 「配信のイネーブル化」（P.9-19）
- 「ファブリックのロック」（P.9-20）
- 「変更のコミット」（P.9-20）
- 「アクティブ化および自動学習の設定の配信」（P.9-20）

配信のイネーブル化

配信モードで実行されたすべての設定は、保留中の（一時的な）データベースに保管されます。設定を変更するには、保留中のデータベースの変更を設定にコミットするか、廃棄する必要があります。この処理の実行中は、ファブリックはロックされた状態になります。保留中のデータベースの変更は、変更をコミットするまでは、設定に反映されません。

（注） CFS 配信がイネーブルの場合、CFS コミットが実行されるまでは、ポートのアクティブ化または非アクティブ化および自動学習のイネーブル化またはディセーブル化は有効になりません。適正な設定を保持するには、必ず、CFS コミットに関するいずれかの処理を行ってください。「アクティブ化および自動学習の設定の配信」（P.9-20）を参照してください。

ヒント 各処理の最後にコミットを実行することを推奨します。つまり、ポート セキュリティのアクティブ化の後、および自動学習のイネーブル化の後です。

Fabric Manager を使用して配信をイネーブルにする手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [VSAN] を展開し、[Port Security] を選択します。

[Information] ペインに、その VSAN のポート セキュリティ設定が表示されます（図 9-8 を参照）。

ステップ 2　[Control] タブをクリックします。

その VSAN のスイッチが表示されます。

ステップ 3　[Command] カラムをクリックして、ドロップダウン メニューから [enable] または [disable] を選択します。

ステップ 4　[Apply Changes] アイコンをクリックして、変更内容を保存します。

ファブリックのロック

既存設定の変更を開始すると、保留中のデータベースが作成され、VSAN 内の機能がロックされます。ファブリックがロックされると、次のような状況になります。

- 他のユーザは、この機能の設定を変更できなくなります。
- コンフィギュレーション データベースのコピーが、保留中のデータベースになります。

変更のコミット

設定に変更をコミットすると、保留中のデータベースの設定が、他のスイッチに配信されます。コミットが正常に実行されると、ファブリック全体に設定の変更が適用され、ロックが解除されます。

アクティブ化および自動学習の設定の配信

配信モードでのアクティブ化および自動学習の設定は、保留中のデータベースの変更をコミットするときに実行される動作として認識されます。

学習されたエントリは一時的なもので、ログインが許可されるかどうかには影響しません。したがって、学習されたエントリは配信には含まれません。学習をディセーブルにして保留中のデータベースの変更をコミットすると、学習されたエントリがアクティブ データベース内のスタティックなエントリになり、ファブリック内のすべてのスイッチに配信されます。コミット実行後は、すべてのスイッチのアクティブ データベースが同一になるので、学習をディセーブルにできます。

変更をコミットする場合、保留中のデータベースに複数のアクティブ化および自動学習の設定が含まれていると、アクティブ化と自動学習の変更が統合され、処理が変更されることがあります（表 9-3 を参照）。

表 9-3　配信モードでのアクティブ化および自動学習の設定シナリオ

シナリオ	操作	配信がオフの場合	配信がオンの場合
コンフィギュレーション データベースに A と B が存在し、アクティブ化は実行されていない状態で、デバイス C と D がログインしている。	**1.** ポート セキュリティ データベースをアクティブ化し、自動学習をイネーブルに設定	コンフィギュレーション データベース = {A、B} アクティブ データベース = {A、B、C[1]、D*}	コンフィギュレーション データベース = {A、B} アクティブ データベース = {ヌル} 保留中のデータベース = {A、B + アクティブ化がイネーブル}
	2. 新規エントリ E をコンフィギュレーション データベースに追加	コンフィギュレーション データベース = {A、B、E} アクティブ データベース = {A、B、C*、D*}	コンフィギュレーション データベース = {A、B} アクティブ データベース = {ヌル} 保留中のデータベース = {A、B、E + アクティブ化がイネーブル}
	3. コミットを発行	適用外	コンフィギュレーション データベース = {A、B、E} アクティブ データベース = {A、B、E、C*、D*} 保留中のデータベース = 空
コンフィギュレーション データベースに A と B が存在し、アクティブ化は実行されていない状態で、デバイス C と D がログインしている。	**1.** ポート セキュリティ データベースをアクティブ化し、自動学習をイネーブルに設定	コンフィギュレーション データベース = {A、B} アクティブ データベース = {A、B、C*、D*}	コンフィギュレーション データベース = {A、B} アクティブ データベース = {ヌル} 保留中のデータベース = {A、B + アクティブ化がイネーブル}
	2. 学習をディセーブルにする	コンフィギュレーション データベース = {A、B} アクティブ データベース = {A、B、C、D}	コンフィギュレーション データベース = {A、B} アクティブ データベース = {ヌル} 保留中のデータベース = {A、B + アクティブ化がイネーブル + 学習がディセーブル}
	3. コミットを発行	適用外	コンフィギュレーション データベース = {A、B} アクティブ データベース = {A、B}、デバイス C と D がログアウト。自動学習をディセーブルにしたアクティブ化と同等。 保留中のデータベース = 空

1. *（アスタリスク）は学習されたエントリを意味します。

ヒント　各処理の最後にコミットを実行することを推奨します。つまり、ポート セキュリティのアクティブ化の後、および自動学習のイネーブル化の後です。

データベース マージに関する注意事項

データベースのマージとは、コンフィギュレーション データベースと、アクティブ データベース内のスタティック（学習されていない）エントリの統合を意味します。

2 つのファブリック間でデータベースをマージする場合には、次の事項に注意してください。

- 両方のファブリックのアクティブ化および自動学習が同じ状態であることを確認します。
- 両方のデータベースの、各 VSAN のコンフィギュレーションの合計数が、2 K を超えていないことを確認します。

注意　この 2 つの条件が満たされていない場合、マージは失敗します。次の配信によって、ファブリックのデータベースおよびアクティブ化の状態が強制的に同期化されます。

データベースの相互作用

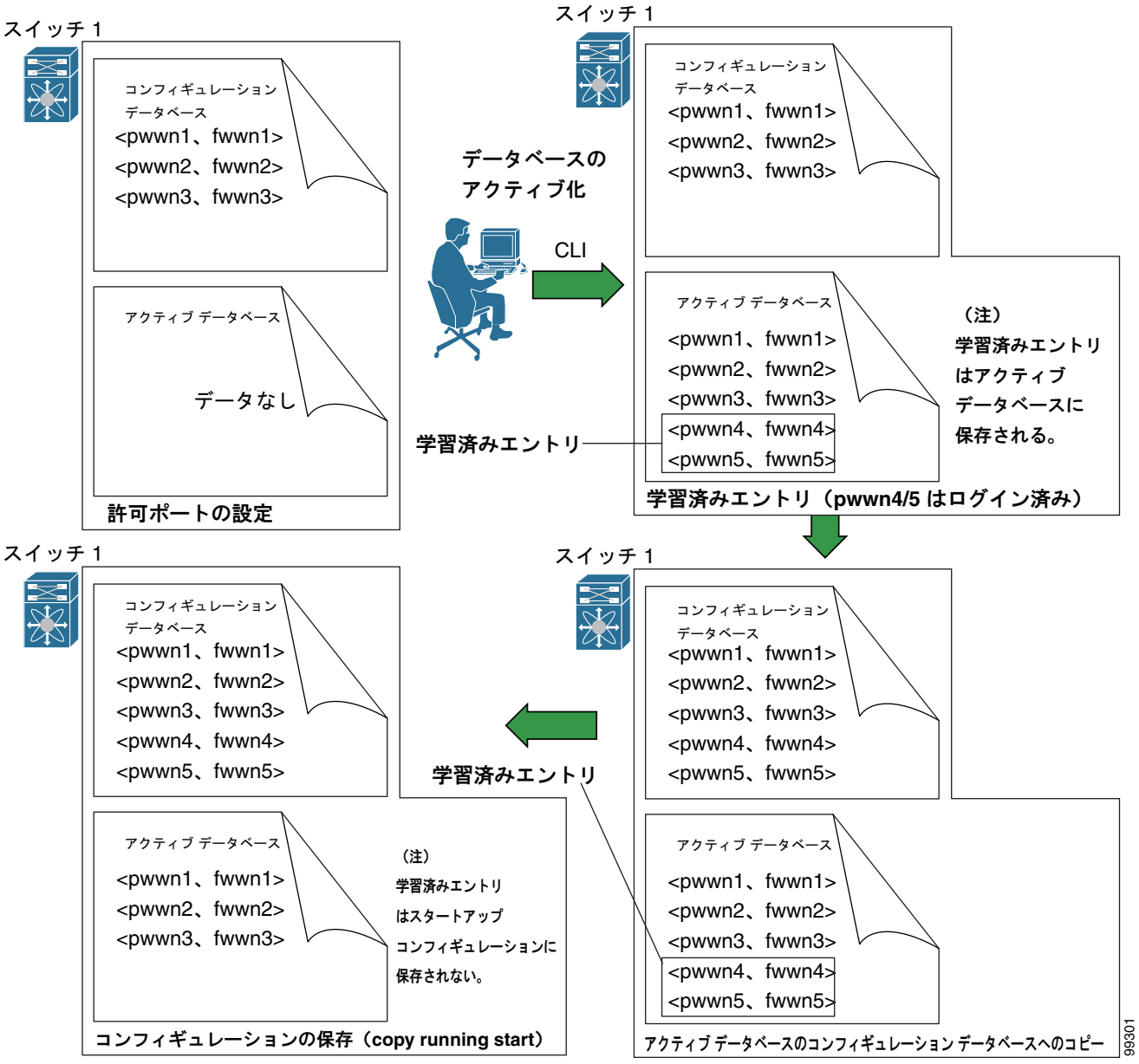
ここで説明する内容は、次のとおりです。

- 「データベースのシナリオ」（P.9-22）
- 「ポート セキュリティ データベースのコピー」（P.9-23）
- 「ポート セキュリティ データベースの削除」（P.9-24）
- 「ポート セキュリティ データベースのクリーニング」（P.9-25）

データベースのシナリオ

図 9-9 の各シナリオは、ポート セキュリティ設定に基づくアクティブ データベースとコンフィギュレーション データベースのステータスを示しています。

ポート セキュリティ データベースのシナリオ



ポート セキュリティ データベースのコピー

ヒント　自動学習をディセーブルにしてから、アクティブ データベースをコンフィギュレーション データベースにコピー することを推奨します。これにより、コンフィギュレーション データベースとアクティブ データベースを完全に同期化できます。配信がイネーブルの場合には、このコマンドにより、コンフィギュレーション データベースの一時的なコピーが作成されます（同時にファブリックがロックされます）。ファブリックがロックされた場合、すべてのスイッチのコンフィギュレーション データベースに変更をコミットする必要があります。

Fabric Manager を使用して、アクティブ データベースをコンフィギュレーション データベースにコピーする手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [Fabric]、[VSAN] の順に展開して、[Port Security] を選択します。

ステップ 2　[Actions] タブをクリックします。すべてのコンフィギュレーション データベースが表示されます。

ステップ 3　適切なコンフィギュレーション データベースを選択し、[Copy Active to Config] チェックボックスをオンにします。

ステップ 4　[Apply Changes] アイコンをクリックして変更内容を保存します。

Fabric Manager を使用して、アクティブ データベースとコンフィギュレーション データベース間の差分を表示する手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [Fabric]、[VSAN] の順に展開して、[Port Security] を選択します。

[Information] ペインに、ポート セキュリティ情報が表示されます。

ステップ 2　[Database Differences] タブをクリックします。すべてのコンフィギュレーション データベースが表示されます。

ステップ 3　適切なコンフィギュレーション データベースを選択します。[Active] または [Config] オプションを選択して、選択したデータベースとアクティブ / コンフィギュレーション データベース間の差分を比較します。

ステップ 4　[Apply Changes] アイコンをクリックして変更内容を保存します。

ポート セキュリティ データベースの削除

ヒント　配信がイネーブルの場合、削除を実行すると、データベースのコピーが作成されます。データベースを実際に削除するには、明示的な削除が必要です。

Fabric Manager を使用してポート セキュリティ データベースを削除する手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [Fabric]、[VSAN] の順に展開して、[Port Security] を選択します。

[Information] ペインに、ポート セキュリティ情報が表示されます。

ステップ 2　[Config Database] タブをクリックします。すべてのコンフィギュレーション データベースが表示されます。

ステップ 3　適切なコンフィギュレーション データベースを選択し、[Delete Row] ボタンをクリックします。

ステップ 4　コンフィギュレーション データベースを削除する場合は、[Yes] ボタンをクリックします。

ポート セキュリティ データベースのクリーニング

Fabric Manager を使用して、指定した VSAN に関するすべての既存の統計情報をポート セキュリティ データベースからクリアする手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [Fabric]、[VSAN] の順に展開して、[Port Security] を選択します。

[Information] ペインに、ポート セキュリティ情報が表示されます（図 9-8 を参照）。

ステップ 2　[Statistics] タブをクリックします。

すべてのコンフィギュレーション データベースが表示されます。

ステップ 3　適切なコンフィギュレーション データベースを選択し、[Clear] オプションを選択します。

ステップ 4　[Apply Changes] アイコンをクリックして変更内容を保存します。

Fabric Manager を使用して、VSAN 内の指定したインターフェイスについて、すべての学習済みエントリをアクティブ データベースからクリアする手順は、次のとおりです。

ステップ 1　[Logical Domains] ペインで [Fabric]、[VSAN] の順に展開して、[Port Security] を選択します。

[Information] ペインに、ポート セキュリティ情報が表示されます。

ステップ 2　[Actions] タブを選択します。すべてのコンフィギュレーション データベースが表示されます。

ステップ 3　適切なコンフィギュレーション データベースを選択し、[AutoLearn] オプションを選択します。

ステップ 4　[Apply Changes] アイコンをクリックして変更内容を保存します。

（注）　[Statistics] タブおよび [AutoLearn] オプションで情報をクリアできるのは、ロックが適用されないローカル スイッチだけです。また、学習済みエントリはスイッチのローカル情報になるだけで、配信には含まれません。

デフォルト設定値

表 9-5 に、スイッチのすべてのポート セキュリティ機能のデフォルト設定を示します。

表 9-5　セキュリティのデフォルト設定

パラメータ	デフォルト
自動学習	ポート セキュリティがイネーブルの場合はイネーブル
ポート セキュリティ	ディセーブル
配信	ディセーブル **（注）**　配信をイネーブルにすると、スイッチのすべての VSAN 上でイネーブルになります。