



ポート セキュリティの設定

Nexus 5000 シリーズ スイッチは、侵入に関する試みを拒否し、管理者にこれらの侵入を報告するポート セキュリティを提供します。



(注)

ポート セキュリティは、仮想ファイバ チャンネル ポートおよび物理ファイバ チャンネル ポートでサポートされています。

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 \(p.24-2\)](#)
- [ポート セキュリティの設定 \(p.24-4\)](#)
- [ポート セキュリティのイネーブル化 \(p.24-7\)](#)
- [ポート セキュリティのアクティブ化 \(p.24-9\)](#)
- [自動学習 \(p.24-13\)](#)
- [ポート セキュリティの手動設定 \(p.24-17\)](#)
- [ポート セキュリティ設定の配信 \(p.24-20\)](#)
- [データベース マージの注意事項 \(p.24-22\)](#)
- [データベースの相互作用 \(p.24-23\)](#)
- [デフォルト設定 \(p.24-26\)](#)

ポートセキュリティの概要

通常、SAN 内のすべてのファイバ チャンネル 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、次の方式を使用して Nexus 5000 シリーズ スイッチのスイッチ ポートへの不正アクセスを防止します。

- 不正なファイバ チャンネル デバイス (N 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。
- 設定配信は 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ています。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 ポリシーを設定するには、ストレージプロトコル サービス ライセンスが必要です。

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 \(p.24-2\)](#)
- [自動学習の概要 \(p.24-3\)](#)
- [ポートセキュリティのアクティブ化 \(p.24-3\)](#)

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 N 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。

N ポートおよび 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 Nexus 5000 シリーズ 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、VSAN 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、Nexus 5000 シリーズ 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、次の処理が行われます。

- 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、以降で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入力する必要があります。

ポートセキュリティの設定

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 \(p.24-4\)](#)
- [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 \(p.24-5\)](#)
- [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 \(p.24-6\)](#)

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」 \(p.24-7\)](#) 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」 \(p.24-20\)](#) 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。

この操作によって、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」 \(p.24-9\)](#) を参照してください。

ステップ 4 CFS 確定を発行して、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」 \(p.24-21\)](#) を参照してください。すべてのスイッチでポートセキュリティ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」 \(p.24-14\)](#) を参照してください。

ステップ 7 CFS 確定を発行して、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」 \(p.24-21\)](#) を参照してください。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」 \(p.24-24\)](#) を参照してください。

ステップ 9 CFS 確定を発行して、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.24-21) 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。

このステップにより、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.24-7) を参照してください。

ステップ 2 各 VSAN のポートセキュリティをアクティブにし、デフォルトで自動学習を有効にします。

「[ポートセキュリティのアクティブ化](#)」(p.24-9) 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.24-14) 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.24-24) 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.24-7) 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。

「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.24-6) 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。

「自動学習のディセーブル化」(p.24-14) 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.24-14) 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](#) ~ [5](#) を繰り返します。

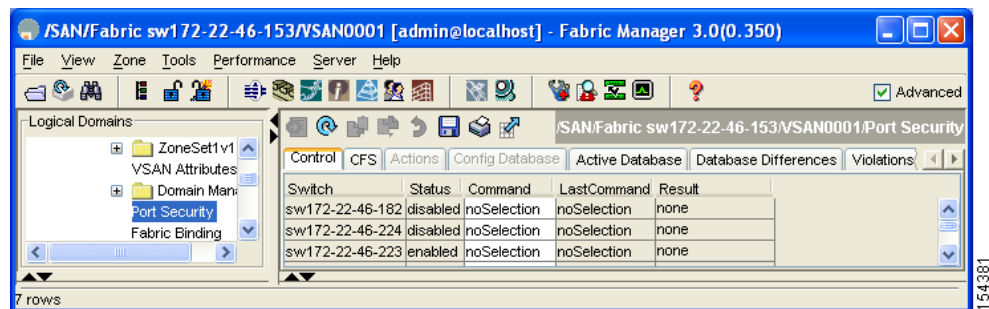
ポートセキュリティのイネーブル化

デフォルトでは、Nexus 5000 シリーズ 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 VSAN を展開し、Logical Domains ペインで **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 24-1 を参照）。

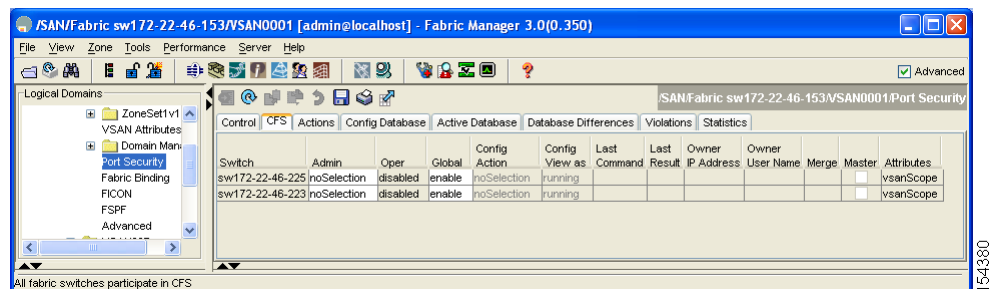
図 24-1 ポートセキュリティ設定



ステップ 2 CFS タブをクリックします。

図 24-2 のような情報が表示されます。

図 24-2 ポートセキュリティ CFS



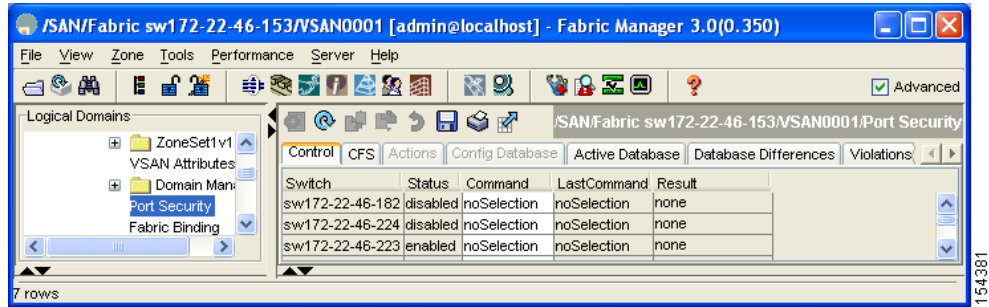
ステップ 3 Global カラムの各エントリをクリックし、**enable** を選択して、VSAN 内のすべての参加スイッチ上の CFS をイネーブルにします。

ステップ 4 **Apply Changes** 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タスが表示されます (図 24-3 を参照)。

図 24-3 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、**Status** カラムで **enable** を選択します。

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** カラムで **commit** を選択します。

ステップ 8 **Apply Changes** 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 \(p.24-9\)](#)
- [データベースのアクティブ化の拒否 \(p.24-10\)](#)
- [ポートセキュリティの強制的なアクティブ化 \(p.24-10\)](#)
- [データベースの再アクティブ化 \(p.24-11\)](#)
- [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 \(p.24-11\)](#)
- [アクティブなポートセキュリティ設定の表示 \(p.24-12\)](#)
- [ポートセキュリティ統計情報の表示 \(p.24-12\)](#)
- [ポートセキュリティ違反の表示 \(p.24-12\)](#)

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 VSAN を展開し、Logical Domains ペインで **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 Activation の下の Action カラムで、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 を選択します。ドロップダウンリストに、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 の **Apply Changes** をクリックして、変更を保存します。

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 チャンネル 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)

アクティブ化を強制すると、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がログアウトします。

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** VSAN を展開し、Logical Domains ペインで **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** Activation の下の **Action** カラムで、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 を選択し、**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 フィールドを選択します。
 - 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 カラムで **commit** を選択します。
 - ステップ 6** Fabric Manager の **Apply Changes** をクリックして、変更を保存します。
-

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、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 VSAN を展開し、Logical Domains ペインで **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には、**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 カラムで **commit** を選択します。

ステップ 6 これらの変更を保存する場合は **Apply Changes** をクリックします。保存されていない変更を廃棄する場合は **Undo Changes** 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 VSAN を展開し、Logical Domains ペインで **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 VSAN を展開し、Logical Domains ペインで **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 VSAN を展開し、Logical Domains ペインで **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

ここで説明する内容は、次のとおりです。

- 自動学習のイネーブル化の概要 (p.24-13)
- 自動学習のイネーブル化 (p.24-13)
- 自動学習のディセーブル化 (p.24-14)
- 自動学習デバイスの許可 (p.24-15)
- 許可の例 (p.24-15)

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 VSAN を展開し、Logical Domains ペインで **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 24-4](#) を参照）。

図 24-4 ポートセキュリティ設定

Master	Action	Enabled	Result	LastChange	CopyActive ToConfig	AutoLearn	Clear Autolearned	AutoLearned Inter
sw172-22-46-220	NoSelection	False	success	n/a	<input type="checkbox"/>	<input checked="" type="checkbox"/>	NoSelection	

ステップ 2 **Actions** タブをクリックします。

ステップ 3 Activation の下の Action カラムで、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 を選択します。ドロップダウンリストに、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、これらの変更を保存します。

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 VSAN を展開し、Logical Domains ペインで **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 24-4 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、これらの変更を保存します。

自動学習デバイスの許可

表 24-1 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 24-1 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)
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

許可の例

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て示します。

- pWWN (P1) には、インターフェイス fc2/1 (F1) からアクセスできる
- pWWN (P2) には、インターフェイス fc2/2 (F1) からアクセスできる
- nWWN (N1) には、インターフェイス fc2/2 (F2) からアクセスできる
- インターフェイス vfc3/1 (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 fc2/4 (F4) からアクセスできる
- sWWN (S1) には、インターフェイス fc3/1 ~ 3 (F10 ~ F13) からアクセスできる
- pWWN (P10) には、インターフェイス vfc4/1 (F11) からアクセスできる

表 24-2 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 24-1 の条件に基づいています。

表 24-2 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。

表 24-2 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
P5、N1、F5	拒否	2	N1 は F2 でのみ許可されます。
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。
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

Nexus 5000 シリーズ 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。
- 「許可済みのポート ペアの追加」(p.24-18) を参照してください。
- 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 の識別の注意事項](#) (p.24-17)
- [許可済みのポート ペアの追加](#) (p.24-18)
- [ポートセキュリティ設定の削除](#) (p.24-19)

WWN の識別の注意事項

ポートセキュリティを手動で設定する場合は、次の点に注意してください。

- 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。
- N ポートが SAN スイッチ ポート F にログインできる場合、その N ポートは指定された F ポートを通してのみログインできます。
- N ポートの nWWN が F ポート WWN にバインドされている場合、N ポートのすべての pWWN は暗黙的に F ポートとペアになります。
- TE ポート チェックは、VSAN 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 SAN ポート チャンネル内のすべてのポート チャンネル 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。

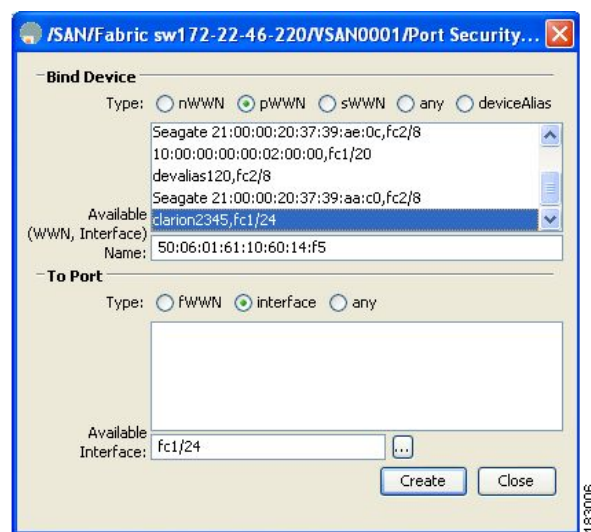
ステップ 1 VSAN を展開し、Logical Domains ペインで **Port Security** を選択します。

ステップ 2 **Config Database** タブをクリックします。

ステップ 3 **Create Row** 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 24-5 を参照)。

図 24-5 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** 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、これらの変更を保存します。

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 VSAN を展開し、Logical Domains ペインで **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** を選択します。

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** 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** 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、これらの変更を保存します。

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 の使用」を参照)。

ここでは、次の内容について説明します。

- 配信のイネーブル化 (p.24-20)
- ファブリックのロック (p.24-21)
- 変更のコミット (p.24-21)
- アクティブ化および自動学習の設定の配信 (p.24-21)

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、(一時的な) 保留データベースに保管されます。設定を変更するには、保留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.24-21) を参照してください。



ヒント

ポートセキュリティのアクティブ化後、および自動学習のイネーブル化後に、コミットを実行することを推奨します。

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 VSAN を展開し、Logical Domains ペインで **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 24-4 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** カラムで、ドロップダウンリストから **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、保留データベースの変更をコミットするときに行わ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、処理結果が変更されることがあります (表 24-3 を参照)。

表 24-3 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*} 保留データベース = 空

表 24-3 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 (続き)

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*、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あと、および自動学習のイネーブル化のあとです。

データベース マージの注意事項

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。詳細については、「[CFS マージのサポート](#)」(p.7-7) を参照してください。

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てください。
- 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、2000 を超えていないことを確認してください。



注意

これらの 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

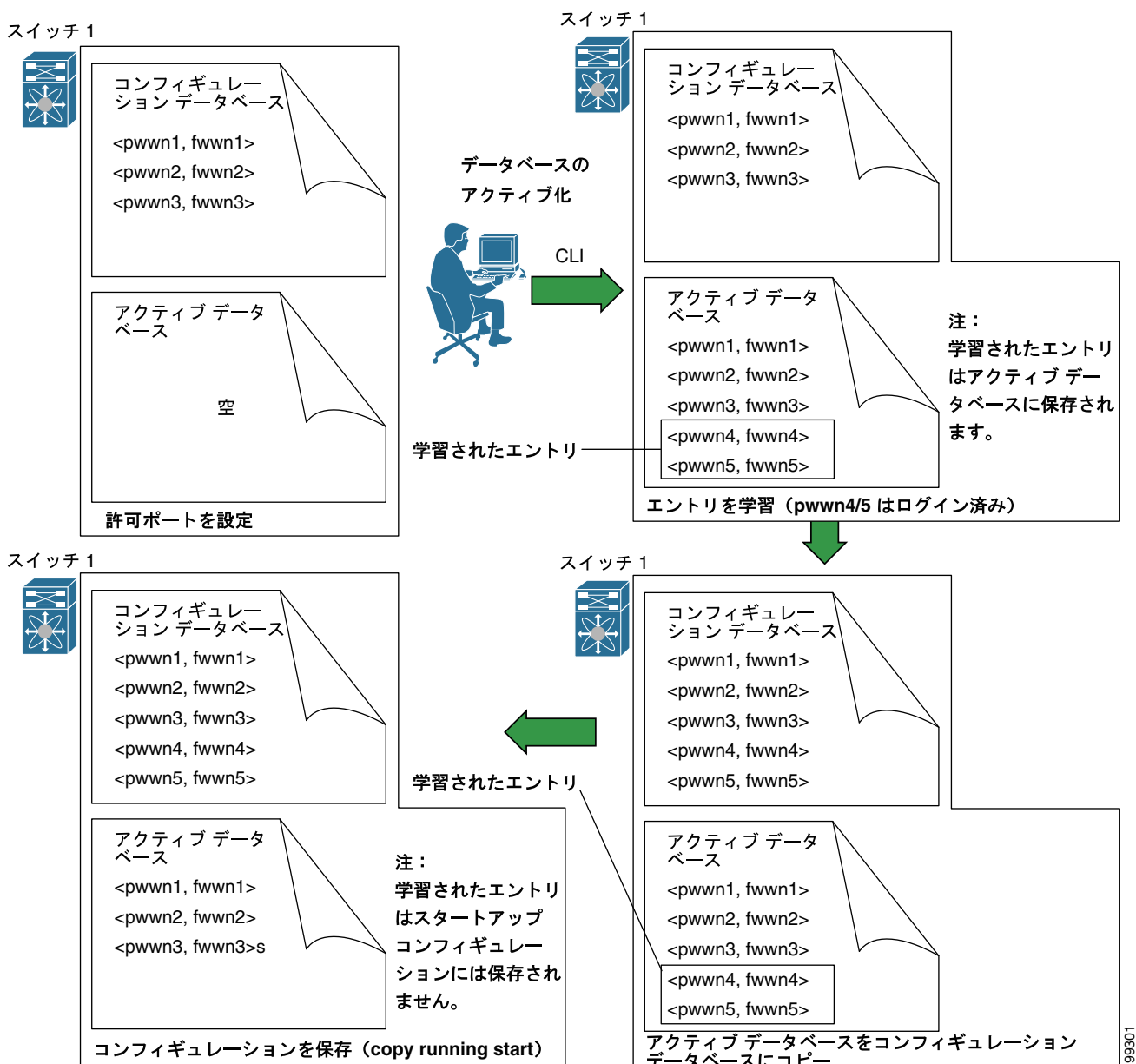
ここで説明する内容は、次のとおりです。

- データベースのシナリオ (p.24-23)
- ポートセキュリティ データベースのコピー (p.24-24)
- ポートセキュリティ データベースの削除 (p.24-25)
- ポートセキュリティ データベースのクリア (p.24-25)

データベースのシナリオ

図 24-6 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。

図 24-6 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 *Fabric* を展開し、**VSAN** を展開して、Logical Domains ペインで **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 *Fabric* を展開し、**VSAN** を展開して、Logical Domains ペインで **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 *Fabric* を展開し、**VSAN** を展開して、Logical Domains ペインで **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** 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ア

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 *Fabric* を展開し、**VSAN** を展開して、Logical Domains ペインで **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 24-4 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 *Fabric* を展開し、**VSAN** を展開して、Logical Domains ペインで **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、**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

表 24-4 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 24-4 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。