ポート セキュリティの設定

この章の内容は、次のとおりです。

ポート セキュリティの設定

Cisco SAN スイッチには、侵入の試みを拒否して管理者に報告するポート セキュリティ機能が組み込まれています。

（注） ポート セキュリティは、仮想ファイバ チャネル ポートと物理ファイバ チャネル ポートでサポートされます。

ポート セキュリティについて

通常、SAN 内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、次の方法を使用して、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（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。配信はデフォルトでディセーブルになっています。
- 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。

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、デバイスおよびスイッチ ポート インターフェイス（これらを通じて各デバイスまたはスイッチが接続される）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 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たび、およびポートを起動しようとした場合に実行されます。

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、設定の変更を受け入れ、実装します。

- コンフィギュレーションデータベース：すべての設定の変更が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：ファブリックが現在実行しているデータベース。 ポート セキュリティ機能を実行するには、スイッチに接続されているすべてのデバイスがポート セキュリティ アクティブ データベースに格納されている必要があります。 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

指定期間内にポートセキュリティ設定を自動的に学習するように、スイッチを設定できます。この機能を使用すると、任意の Cisco SAN 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初めてアクティブにするときに、この機能を使用してください。ポートごとに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。

自動学習がイネーブルのときは、まだ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実行されます。 自動学習がまだイネーブルなときにポートをシャットダウンすると、そのポートに関する学習エントリが消去されます。

学習は、既存の設定済みのポートセキュリティ ポリシーを上書きしません。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、自動学習がエントリを追加して、そのインターフェイス上の他の pWWN を許可することはありません。 他のすべての pWWN は、自動学習モードであってもブロックされます。

シャットダウン状態のポートについては、学習エントリは作成されません。

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する場合、自動学習をディセーブルにするまでポート 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、ポート セキュリティ機能はアクティブにされていません。

ポート セキュリティ機能をアクティブにすると、次のようになります。

- 自動学習も自動的にイネーブルになります。つまり、
  - この時点から、まだ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対してだけ自動学習が行われます。
  - 自動学習をディセーブルにするまで、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は学習され、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がアクティブになる前に、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、自動学習をディセーブルにすることもできます。

ポートがログインを拒否されて停止している場合、その後でログインを許可するようにデータベースを設定しても、ポートは自動的に起動しません。 明示的に **no shutdown** CLI コマンドを入力して、そのポートをオンラインに戻す必要があります。

ポート セキュリティの設定

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

自動学習とCFS配信を使用する場合にポート セキュリティを設定するには、次の手順に従ってください。

手順の概要

1. ポート セキュリティをイネーブルにします。
2. CFS 配信をイネーブルにします。
3. 各 VSAN で、ポート セキュリティをアクティブにします。
4. CFS コミットを発行して、ファブリック内のすべてのスイッチにこの設定をコピーします。
5. すべてのスイッチとすべてのホストが自動的に学習されるまで待ちます。
6. 各 VSAN で、自動学習をディセーブルにします。
7. CFS コミットを発行して、ファブリック内のすべてのスイッチにこの設定をコピーします。
8. 各VSANの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。
9. CFS コミットを発行して、ファブリック内のすべてのスイッチにこの設定をコピーします。
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。

手順の詳細

ステップ 1 ポート セキュリティをイネーブルにします。

ステップ 2 CFS 配信をイネーブルにします。

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。

ステップ 4 CFS コミットを発行して、ファブリック内のすべてのスイッチにこの設定をコピーします。
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、自動学習がイネーブルになります。

ステップ 5 すべてのスイッチとすべてのホストが自動的に学習されるまで待ちます。

ステップ 6 各 VSAN で、自動学習をディセーブルにします。

ステップ 7 CFS コミットを発行して、ファブリック内のすべてのスイッチにこの設定をコピーします。
すべてのスイッチから自動学習されたエントリが、すべてのスイッチへ配信されるスタティックなアクティブ データベースに集約されます。

ステップ 8 各 VSAN の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。

ステップ 9 CFS コミットを発行して、ファブリック内のすべてのスイッチにこの設定をコピーします。
これで、ファブリック内の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。

関連トピック

ポート セキュリティのアクティブ化, （7 ページ）
変更のコミット, （18 ページ）

ポート セキュリティ データベースのコピー, （25 ページ）
自動学習のディセーブル化, （11 ページ）
ポート セキュリティのイネーブル化, （6 ページ）
ポート セキュリティの配信のイネーブル化, （16 ページ）

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 を使用しない場合にポート セキュリティを設定するには、次の手順に従ってください。

手順の概要

1. ポート セキュリティをイネーブルにします。
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。
3. すべてのスイッチとすべてのホストが自動的に学習されるまで待ちます。
4. 各 VSAN で、自動学習をディセーブルにします。
5. 各VSANの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。
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。
7. ファブリック内のすべてのスイッチに対して上記の手順を繰り返します。

手順の詳細

ステップ 1 ポート セキュリティをイネーブルにします。

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。

ステップ 3 すべてのスイッチとすべてのホストが自動的に学習されるまで待ちます。

ステップ 4 各 VSAN で、自動学習をディセーブルにします。

ステップ 5 各 VSAN の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。

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対して上記の手順を繰り返します。

関連トピック

ポート セキュリティのアクティブ化, （7 ページ）
ポート セキュリティ データベースのコピー, （25 ページ）

自動学習のディセーブル化, （11 ページ）
ポート セキュリティのイネーブル化, （6 ページ）

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

手動でポート セキュリティ データベースを設定する場合にポート セキュリティを設定するには、次の手順に従ってください。

手順の概要

1. ポート セキュリティをイネーブルにします。
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。
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。
4. 各 VSAN で、自動学習をディセーブルにします。
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。
6. ファブリック内のすべてのスイッチに対して上記の手順を繰り返します。

手順の詳細

ステップ 1 ポート セキュリティをイネーブルにします。

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。

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。

ステップ 4 各 VSAN で、自動学習をディセーブルにします。

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対して上記の手順を繰り返します。

ポート セキュリティのイネーブル化

デフォルトでは、ポート セキュリティ機能はディセーブルです。

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。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **port-security enable**
3. switch(config)# **no port-security enable**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **port-security enable**	スイッチ上でポート セキュリティをイネーブルにします。
ステップ 3	switch(config)# **no port-security enable**	スイッチ上でポート セキュリティをディセーブル（デフォルト）にします。

ポート セキュリティのアクティブ化

ポート セキュリティのアクティブ化

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。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **port-security activate vsan** *vsan-id*
3. switch(config)# **port-security activate vsan** *vsan-id* **no-auto-learn**
4. switch(config)# **no port-security activate vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **port-security activate vsan** *vsan-id*	指定された VSAN のポート セキュリティ データベースをアクティブにし、自動的に自動学習をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 3	switch(config)# **port-security activate vsan** *vsan-id* **no-auto-learn**	指定された VSAN のポート セキュリティ データベースをアクティブにし、自動学習をディセーブルにします。
ステップ 4	switch(config)# **no port-security activate vsan** *vsan-id*	指定された VSAN のポート セキュリティ データベースを無効にし、自動的に自動学習をディセーブルにします。

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あるが、アクティブ データベースにはない場合。
- アクティベーションの前に、自動学習機能がイネーブルに設定されていた場合。 この状態の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あり、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 つ以上発生したためにデータベース アクティベーションが拒否された場合は、ポート セキュリティ アクティベーションを強制して継続することができます。

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アクティベーション要求が拒否された場合は、アクティベーションを強制できます。

（注） アクティベーションを強制すると、既存のデバイスがアクティブ データベースに違反したときに既存のデバイスがログアウトされます。

port-security database diff active vsan コマンドを使用して、欠落しているか矛盾するエントリを表示できます。

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にする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **port-security activate vsan** *vsan-id* **force**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **port-security activate vsan** *vsan-id* **force**	矛盾がある場合でも、指定された VSAN のポート セキュリティ データベースを強制的にアクティブにします。

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の場合、force オプションを使用しないと、自動学習をディセーブルにするまでデータベースをアクティブにできません。

ポート セキュリティ データベースを再度アクティブにする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **no no port-security auto-learn vsan** *vsan-id*
3. switch(config)# **exit**
4. switch# **port-security database copy vsan** *vsan-id*
5. switch# **configuration terminal**
6. switch(config)# **port-security activate vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **no no port-security auto-learn vsan** *vsan-id*	自動学習をディセーブルにし、スイッチにアクセスする新規デバイスをスイッチが学習しないように設定します。 この時点までに学習されたデバイスに基づいて、データベースの内容を処理します。
ステップ 3	switch(config)# **exit**	
ステップ 4	switch# **port-security database copy vsan** *vsan-id*	アクティブ データベースから設定済みデータベースにコピーします。

	コマンドまたはアクション	目的
ステップ 5	switch# **configuration terminal**	再びコンフィギュレーション モードを開始します。
ステップ 6	switch(config)# **port-security activate vsan** *vsan-id*	指定された VSAN のポート セキュリティ データベースをアクティブにし、自動的に自動学習をイネーブルにします。

自動学習

自動学習のイネーブル化について

自動学習設定の状態は、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アクティブでない場合、自動学習はデフォルトでディセーブルです。
- 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です（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 上で自動学習がイネーブルの場合、force オプションを使用して、この VSAN のデータベースだけをアクティブにできます。

自動学習のイネーブル化

自動学習をイネーブルにする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **port-security auto-learn vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **port-security auto-learn vsan** *vsan-id*	自動学習をイネーブルにして、VSAN 1 へのアクセスが許可されたすべてのデバイスについて、スイッチが学習できるよ

	コマンドまたはアクション	目的
		うにします。 これらのデバイスは、ポート セキュリティ アクティブ データベースに記録されます。

自動学習のディセーブル化

自動学習をディセーブルにする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **no port-security auto-learn vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **no port-security auto-learn vsan** *vsan-id*	自動学習をディセーブルにし、スイッチにアクセスする新規デバイスをスイッチが学習しないように設定します。 この時点までに学習されたデバイスに基づいて、データベースの内容を処理します。

自動学習デバイスの許可

次の表に、デバイス要求に対して接続が許可される条件をまとめます。

表 *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	認証
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

条件	デバイス（pWWN、nWWN、sWWN）	接続先	認証
3	未設定	設定されていないスイッチ ポート	自動学習がイネーブルの場合は許可
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許可するスイッチ 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	未設定	その他のデバイスが設定されたポート	拒否

許可される場合

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ことが前提です。

- pWWN（P1）には、インターフェイス fc2/1（F1）からアクセスできます。
- pWWN（P2）には、インターフェイス fc2/2（F1）からアクセスできます。
- nWWN（N1）には、インターフェイス fc2/2（F2）からアクセスできます。
- インターフェイス vfc3/1（F3）からは、任意の WWN にアクセスできます。
- 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）からアクセスできます。
- sWWN（S1）には、インターフェイス fc3/1 ～ 3（F10 ～ F13）からアクセスできます。
- pWWN（P10）には、インターフェイス vfc4/1（F11）からアクセスできます。

次の表に、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要約します。

表 *2*：各シナリオの許可結果

デバイス接続要求	認証	条件	理由
P1、N2、F1	許可	1	競合しません。

デバイス接続要求	認証	条件	理由
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 でだけ許可されます。
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 と 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。

デバイス接続要求	認証	条件	理由
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（*）が一致しています。

関連トピック

自動学習デバイスの許可, （11 ページ）

ポート セキュリティの手動設定

ポート セキュリティを手動で設定するには、次の作業を行います。

手順の概要

1. 保護する必要があるポートの WWN を識別します。
2. 許可された nWWN または pWWN に対して fWWN を保護します。
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。
4. 設定を確認します。

手順の詳細

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。

WWN の識別に関する注意事項

ポート セキュリティを手動で設定する場合は、次に従い行ってください。

- 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。
- 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 ポートを介してだけログインできます。
- 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ことにより、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を保存します。 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 ペアを識別したら、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。

ポート セキュリティに関して許可済みのポート ペアを追加する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **port-security database vsan** *vsan-id*
3. switch(config)# **no port-security database vsan** *vsan-id*
4. switch(config-port-security)# **swwn** *swwn-id* **interface san-port-channel 5**
5. switch(config-port-security)# **any-wwn interface fc** *slot*/*port* - **fc** *slot*/*port*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **port-security database vsan** *vsan-id*	指定された VSAN に対してポート セキュリティ データベース モードを開始します。
ステップ 3	switch(config)# **no port-security database vsan** *vsan-id*	指定された VSAN からポート セキュリティ コンフィギュレーション データベースを削除します。
ステップ 4	switch(config-port-security)# **swwn** *swwn-id* **interface san-port-channel 5**	SAN ポート チャネル 5 を介した場合だけログインするように、指定された sWWN を設定します。
ステップ 5	switch(config-port-security)# **any-wwn interface fc** *slot*/*port* - **fc** *slot*/*port*	指定されたインターフェイスを介してログインするようにすべての WWN を設定します。

次に、VSAN 2 に対してポート セキュリティ データベース モードを開始する例を示します。

```
switch(config)# port-security database vsan 2
```

次に、SAN ポート チャネル 5 を介した場合だけログインするように、指定された sWWN を設定する例を示します。

```
switch(config-port-security)# swwn 20:01:33:11:00:2a:4a:66 interface san-port-channel 5
```

次に、指定されたスイッチの指定されたインターフェイスを介してログインするように、指定された pWWN を設定する例を示します。

```
switch(config-port-security)# pwwn 20:11:33:11:00:2a:4a:66 swwn 20:00:00:0c:85:90:3e:80
interface fc 3/2
```

次に、任意のスイッチの指定されたインターフェイスを介してログインするようにすべての WWN を設定する例を示します。

```
switch(config-port-security)# any-wwn interface fc 3/2
```

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現し、VSAN 内のファブリック全体に 1 つの設定を提供します。また、ファブリック全体でポート セキュリティ ポリシーを実行します。

追加情報については、『*Cisco Nexus 5000 Series System Management Configuration Guide*』の「Using Cisco Fabric Services」を参照してください。

ポート セキュリティの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）データベースに保存されます。 設定を変更する場合、設定に対して保留中のデータベースの変更をコミットまたは廃棄する必要が

あります。その間、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への変更は、変更をコミットするまで設定に反映されません。

（注） CFS配信がイネーブルの場合、ポートのアクティベーションまたは非アクティベーション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、CFSコミットを発行するまで有効になりません。 常に CFS コミットとこれらの処理のいずれかを使用して、正しい設定を確認してください。

たとえば、ポート セキュリティをアクティブにし、自動学習をディセーブルにし、最後に保留状態のデータベースに変更をコミットすると、**port-security activate vsan** *vsan-id* no-auto-learn コマンドを入力した場合と同じ結果になります。

ヒント ポート セキュリティをアクティブにし、自動学習をイネーブルにしたあとに、コミットを実行することを推奨します。

ポート セキュリティ データベースを再度アクティブにする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **port-security distribute**
3. switch(config)# **no port-security distribute**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# **port-security distribute**	配信をイネーブルにします。
ステップ 3	switch(config)# **no port-security distribute**	配信をディセーブルにします。

関連トピック

アクティベーション設定と自動学習設定の配信, （19 ページ）

ファブリックのロック

既存の設定を変更するときの最初のアクションが実行されると、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。

- 他のユーザがこの機能の設定に変更を加えることができなくなります。
- 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

設定に加えられた変更をコミットする場合、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。 コミットが正常に行われると、設定の変更がファブリック全体に適用され、ロックが解除されます。

指定された VSAN のポート セキュリティ設定の変更をコミットする手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **port-security commit vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# **port-security commit vsan** *vsan-id*	指定された VSAN のポート セキュリティの変更をコミットします。

変更の廃棄

保留中のデータベースに加えられた変更を廃棄（中断）する場合、設定は影響されないまま、ロックが解除されます。

指定された VSAN のポート セキュリティ設定の変更を廃棄する手順は、次のとおりです。

手順の概要

1. switch# **configuration terminal**
2. switch(config)# **port-security abort vsan** *vsan-id*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configuration terminal**	コンフィギュレーション モードに入ります。

	コマンドまたはアクション	目的
ステップ 2	switch(config)# **port-security abort vsan** *vsan-id*	指定された VSAN のポート セキュリティの変更を廃棄し、保留中のコンフィギュレーション データベースをクリアします。

アクティベーション設定と自動学習設定の配信

配信モードのアクティベーション設定および自動学習設定は、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する処理として記憶されます。

学習済みエントリは一時的なもので、ログインを許可するか否かを決定するロールを持ちません。そのため、学習済みエントリは配信に参加しません。 学習をディセーブルにし、保留中のデータベースの変更をコミットする場合、学習済みエントリはアクティブ データベース内のスタティック 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。 コミット後、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り、学習をディセーブルにできます。

保留中のデータベースに複数のアクティベーションおよび自動学習設定が含まれる場合、変更をコミットすると、アクティベーションおよび自動学習の変更が統合され、動作が変化する場合があります（次の表を参照）。

表 *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	アクション	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およびBが存在し、アクティベーションが行われておらず、デバイスCおよびDがログインされています。	1. ポートセキュリティデータベースをアクティブにし、自動学習をイネーブルにします。	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 + アクティベーション（イネーブル）}
	2. 新規のエントリEがコンフィギュレーションデータベースに追加されました。	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+アクティベーション（イネーブル）}
	3. コミットを行います。	N/A	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 = 空の状態

シナリオ	アクション	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およびBが存在し、アクティベーションが行われておらず、デバイスCおよびDがログインされています。	1. ポートセキュリティデータベースをアクティブにし、自動学習をイネーブルにします。	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＋アクティベーション（イネーブル）}
	2. 学習をディセーブルにします。	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＋アクティベーション（イネーブル）＋学習（ディセーブル）}
	3. コミットを行います。	N/A	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およびDがログアウトされます。これは、自動学習をディセーブルにした場合のアクティベーションと同じです。 保留中のデータベース=空の状態

[1] *（アスタリスク）は学習されたエントリを意味します。

ポート セキュリティ データベース結合の注意事項

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）エントリの統合を指します。

2 つのファブリック間のデータベースをマージする場合は、次のことに気をつけて行ってください。

- アクティベーション ステータスと自動学習ステータスが両方のファブリックで同じであることを確認します。
- 両方のデータベースの各 VSAN の設定を合わせた数が 2000 を超えていないことを確認します。

注意 この 2 つの条件に従わない場合は、マージに失敗します。 次の配信がデータベースとファブリック内のアクティベーション ステートを強制的に同期化します。

追加情報については、『*Cisco Nexus 5000 Series System Management Configuration Guide*』の「CFS Merge Support」を参照してください。

データベースの相互作用

次の表に、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差異および相互作用を示します。

表 *4*: アクティブおよびコンフィギュレーション ポート セキュリティ データベース

アクティブ データベース	コンフィギュレーション データベース
読み取り専用。	読み取りと書き込み。
設定を保存すると、アクティブなエントリだけが保存されます。 学習済みエントリは保存されません。	設定を保存すると、コンフィギュレーション データベース内のすべてのエントリが保存されます。
アクティブ化すると、VSAN にログイン済みのすべてのデバイスも学習され、アクティブ データベースに追加されます。	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。

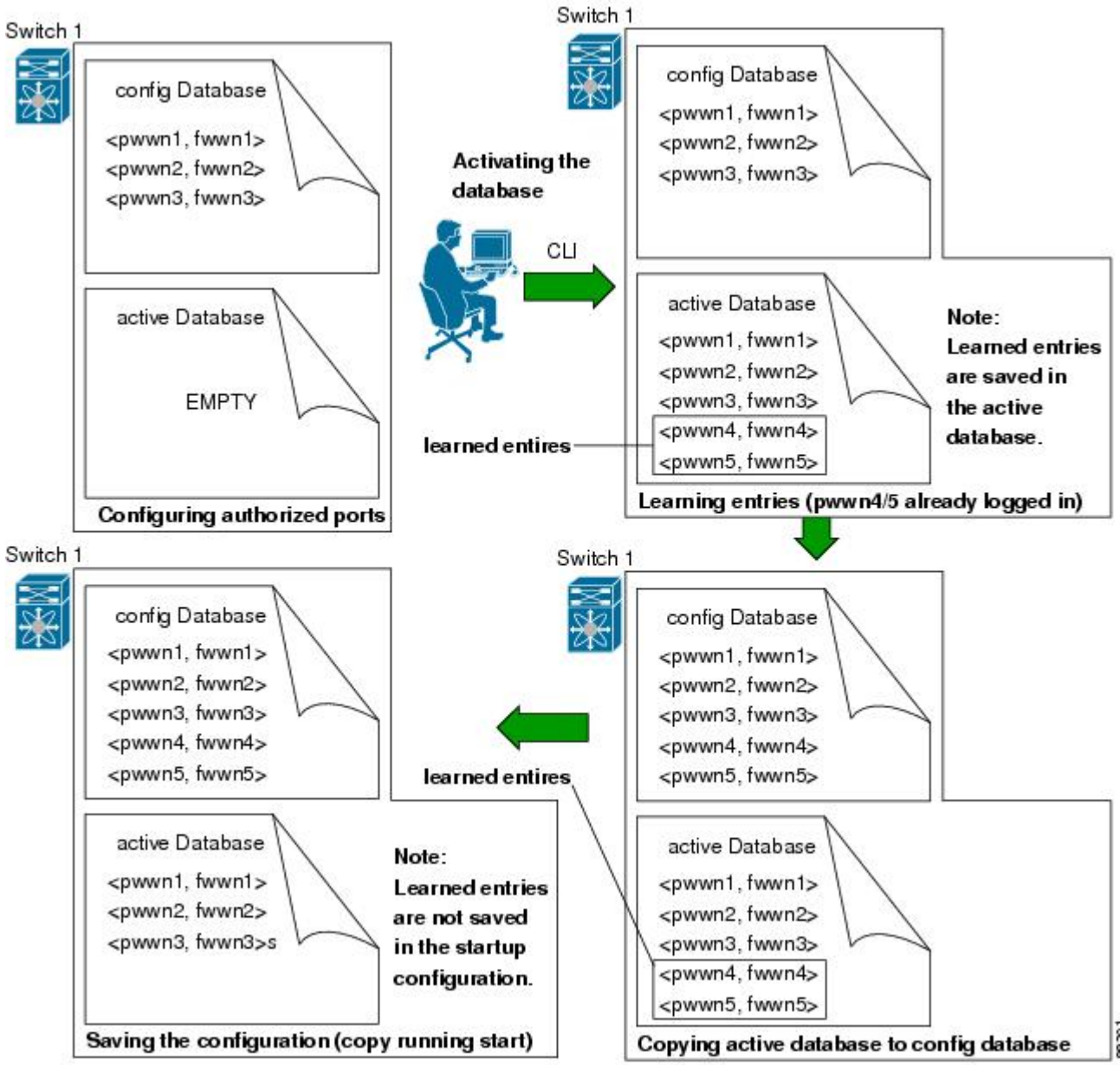
アクティブ データベース	コンフィギュレーション データベース
アクティブデータベースを設定済みデータベースで上書きするには、ポートセキュリティデータベースをアクティブ化します。 強制的にアクティブにすると、アクティブデータベースの設定済みエントリに違反が生じることがあります。	コンフィギュレーション データベースをアクティブ データベースで上書きできます。

（注） **port-security database copy vsan** コマンドを使用すると、コンフィギュレーション データベースをアクティブ データベースで上書きできます。 **port-security database diff active vsan** コマンドは、アクティブ データベースとコンフィギュレーション データベースの差異を示します。

データベースのシナリオ

次の図は、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すさまざまなシナリオを示します。

図 *1*：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。 このアクションにより、コンフィギュレーションデータベースがアクティブデータベースと確実に同期化されます。配信がイネーブルの場合、このコマンドによって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、結果として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。

アクティブ データベースから設定済みデータベースにコピーするには、 **port-security database copy vsan** コマンドを使用します。 アクティブ データベースが空の場合、このコマンドは受け付けられません。

```
switch# port-security database copy vsan 1
```

アクティブ データベースとコンフィギュレーション データベースとの相違を表示するには、**port-security database diff active vsan** コマンドを使用します。 このコマンドは、矛盾を解決する場合に使用できます。

```
switch# port-security database diff active vsan 1
```

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との違いに関する情報を取得するには、**port-security database diff config vsan** コマンドを使用します。

```
switch# port-security database diff config vsan 1
```

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、削除によってデータベースのコピーが作成されます。 実際にデータベースを削除するには、明示的に **port-security commit** コマンドを入力する必要があります。

指定された VSAN の設定済みデータベースを削除するには、コンフィギュレーション モードで **no port-security database vsan** コマンドを使用します。

```
switch(config)# no port-security database vsan 1
```

ポート セキュリティ データベースのクリア

指定された VSAN のポート セキュリティ データベースから既存の統計情報をすべてクリアするには、**clear port-security statistics vsan** コマンドを使用します。

```
switch# clear port-security statistics vsan 1
```

VSAN 内の指定されたインターフェイスに関するアクティブ データベース内の学習済みエントリをすべてクリアするには、**clear port-security database auto-learn interface** コマンドを使用します。

```
switch# clear port-security database auto-learn interface fc2/1 vsan 1
```

VSAN 全体に関するアクティブ データベース内の学習済みエントリをすべてクリアするには、**clear port-security database auto-learn vsan** コマンドを使用します。

```
switch# clear port-security database auto-learn vsan 1
```

（注） **clear port-security database auto-learn** および **clear port-security statistics** コマンドはローカル スイッチのみに関連するため、ロックを取得しません。 また、学習済みエントリはスイッチにだけローカルで、配信に参加しません。

VSAN 内で、任意のスイッチから VSAN の保留中のセッションをクリアするには、**port-security clear vsan** コマンドを使用します。

```
switch# clear port-security session vsan 5
```

ポート セキュリティ設定の表示

show port-security database コマンドを実行すると、設定されたポート セキュリティ情報が表示されます。 **show port-security** コマンドで fWWN や VSAN、またはインターフェイスや VSAN を指定すると、アクティブなポート セキュリティの出力を表示することもできます。

各ポートのアクセス情報は個別に表示されます。 fWWN または interface オプションを指定すると、（その時点で）アクティブ データベース内で指定された fWWN またはインターフェイスとペアになっているすべてのデバイスが表示されます。

次に、ポート セキュリティ コンフィギュレーション データベースを表示する例を示します。

```
switch# show port-security database
```

次に、VSAN 1 のポート セキュリティ コンフィギュレーション データベースを表示する例を示します。

```
switch# show port-security database vsan 1
```

次に、アクティブなデータベースを表示する例を示します。

```
switch# show port-security database active
```

次に、一時的なコンフィギュレーション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相違を表示する例を示します。

```
switch# show port-security pending-diff vsan 1
```

次に、VSAN 1 内の設定済み fWWN ポート セキュリティを表示する例を示します。

```
switch# show port-security database fwwn 20:01:00:05:30:00:95:de vsan 1
20:00:00:0c:88:00:4a:e2(swwn)
```

次に、ポート セキュリティ統計情報を表示する例を示します。

```
switch# show port-security statistics
```

次に、アクティブ データベースのステータスおよび自動学習設定を確認する例を示します。

```
switch# show port-security status
```

ポート セキュリティのデフォルト設定

次の表に、任意のスイッチにおけるすべてのポート セキュリティ機能のデフォルト設定を示します。

表 *5*：セキュリティのデフォルト設定値

パラメータ	デフォルト
Auto-learn	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、スイッチ上のすべてのVSANの配信がイネーブルになります。