CHAPTER 39

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。

この章は、次の項で構成されています。

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、ENTERPRISE_PKG ライセンスが必要です（第 3 章「ライセンスの入手とインストール」を参照）。

この項では、次のトピックについて取り上げます。

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 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 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。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。

- 自動学習も自動的にイネーブルになります。つまり、
  - 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かぎり、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、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。

ヒント　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。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 セキュリティ設定の注意事項

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、自動学習の動作が異なります。

この項では、次のトピックについて取り上げます。

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

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.39-5）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.39-13）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.39-6）を参照してください。

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。「変更のコミット」（P.39-13）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。「自動学習のディセーブル化」（P.39-8）を参照してください。

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。「変更のコミット」（P.39-13）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　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。「ポート セキュリティ データベースのコピー」（P.39-17）を参照してください。

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。「変更のコミット」（P.39-13）を参照してください。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。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.39-5）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.39-6）を参照してください。

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。「自動学習のディセーブル化」（P.39-8）を参照してください。

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。「ポート セキュリティ データベースのコピー」（P.39-17）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.39-5）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.39-10）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.39-6）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.39-8）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。

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。

ポート セキュリティをイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t`	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。
	`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ベーション

この項では、次のトピックについて取り上げます。

- 「ポート セキュリティのアクティブ化」（P.39-6）
- 「データベースのアクティブ化の拒否」（P.39-6）

ポート セキュリティのアクティブ化

ポート セキュリティ機能をアクティブにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t` `switch(config)#`	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 1`	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。
	`switch(config)# port-security activate vsan 1 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。
	`switch(config)# no port-security activate vsan 1`	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。

（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.39-8）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 PortChannel 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）　**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。

存在しないエントリや矛盾するエントリを表示するには、EXEC モードで **port-security database diff active vsan** コマンドを使用します。

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には、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t` `switch(config)#`	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 1 force`	競合にかかわらず VSAN 1 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 データベースを再アクティブ化するには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t` `switch(config)#`	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 1`	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` `switch# port-security database copy vsan 1`	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。
ステップ 4	`switch# config t` `switch(config)# port-security activate vsan 1`	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

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

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には、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t` `switch(config)#`	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 1`	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には、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t` `switch(config)#`	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 1`	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

表 39-1 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 39-1　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	自動学習がイネーブルの場合は許可
4			自動学習がディセーブルの場合は拒否
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	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ことが前提です。

- 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 39-2 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まとめます。ここに示す条件は、表 39-1 の条件を参照しています。

表 39-2　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。

表 39-2　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
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。
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。

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。

この項では、次のトピックについて取り上げます。

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かぎ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 PortChannel 内のすべての PortChannel 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。

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には、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t` `switch(config)#`	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 1` `switch(config-port-security)#`	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。
	`switch(config)# no port-security database vsan 1` `switch(config)#`	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。

	コマンド	目的
ステップ 3	switch(config-port-security)# **swwn 20:01:33:11:00:2a:4a:66 interface port-channel 5**	PortChannel 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。
	switch(config-port-security)# **any-wwn interface fc1/1 - fc1/8**	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。
	switch(config-port-security)# **pwwn 20:11:00:33:11:00:2a:4a fwwn 20:81:00:44:22:00:4a:9e**	指定された fWWN を介した場合だけログインするように、指定された pWWN を設定します。
	switch(config-port-security)# **no pwwn 20:11:00:33:11:00:2a:4a fwwn 20:81:00:44:22:00:4a:9e**	前のステップで設定した指定 pWWN を削除します。
	switch(config-port-security)# **nwwn 26:33:22:00:55:05:3d:4c fwwn 20:81:00:44:22:00:4a:9e**	指定された fWWN を介してログインするように、指定された nWWN を設定します。
	switch(config-port-security)# **pwwn 20:11:33:11:00:2a:4a:66**	ファブリック内のポートを介してログインするように、指定された pWWN を設定します。
	switch(config-port-security)# **pwwn 20:11:33:11:00:2a:4a:66 swwn 20:00:00:0c:85:90:3e:80**	指定されたスイッチの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 fc3/1**	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 を設定します。
	switch(config-port-security)# **any-wwn interface fc3/1**	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 を設定します。
	switch(config-port-security)# **no any-wwn interface fc2/1**	前のステップで設定したワイルドカードを削除します。

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現し、VSAN 内のファブリック全体にシングル ポイント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（第 7 章「CFS インフラストラクチャの使用」を参照）。

この項では、次のトピックについて取り上げます。

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。「アクティブ化および自動学習の設定の配信」（P.39-14）を参照してください。

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** コマンドを発行した場合と同じ結果になります。

ヒント この場合、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。

ポート セキュリティ配信をイネーブルにするには、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t` `switch(config)#`	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。
	`switch(config)# no port-security distribute`	配信をディセーブルにします。

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には、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t` `switch(config)#`	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 3`	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には、次の手順を実行します。

	コマンド	目的
ステップ 1	`switch# config t` `switch(config)#`	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 abort vsan 5`	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。

アクティブ化および自動学習の設定の配信

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るだけです。

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。

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 39-3 を参照）。

表 39-3　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

表 39-3　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	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。

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）エントリの統合を指します。詳細については、「CFS マージのサポート」（P.7-9）を参照してください。

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てください。

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。

データベースの相互作用

表 39-4 に、アクティブ データベースとコンフィギュレーション データベース間の相違、および相互作用を示します。

表 39-4　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。

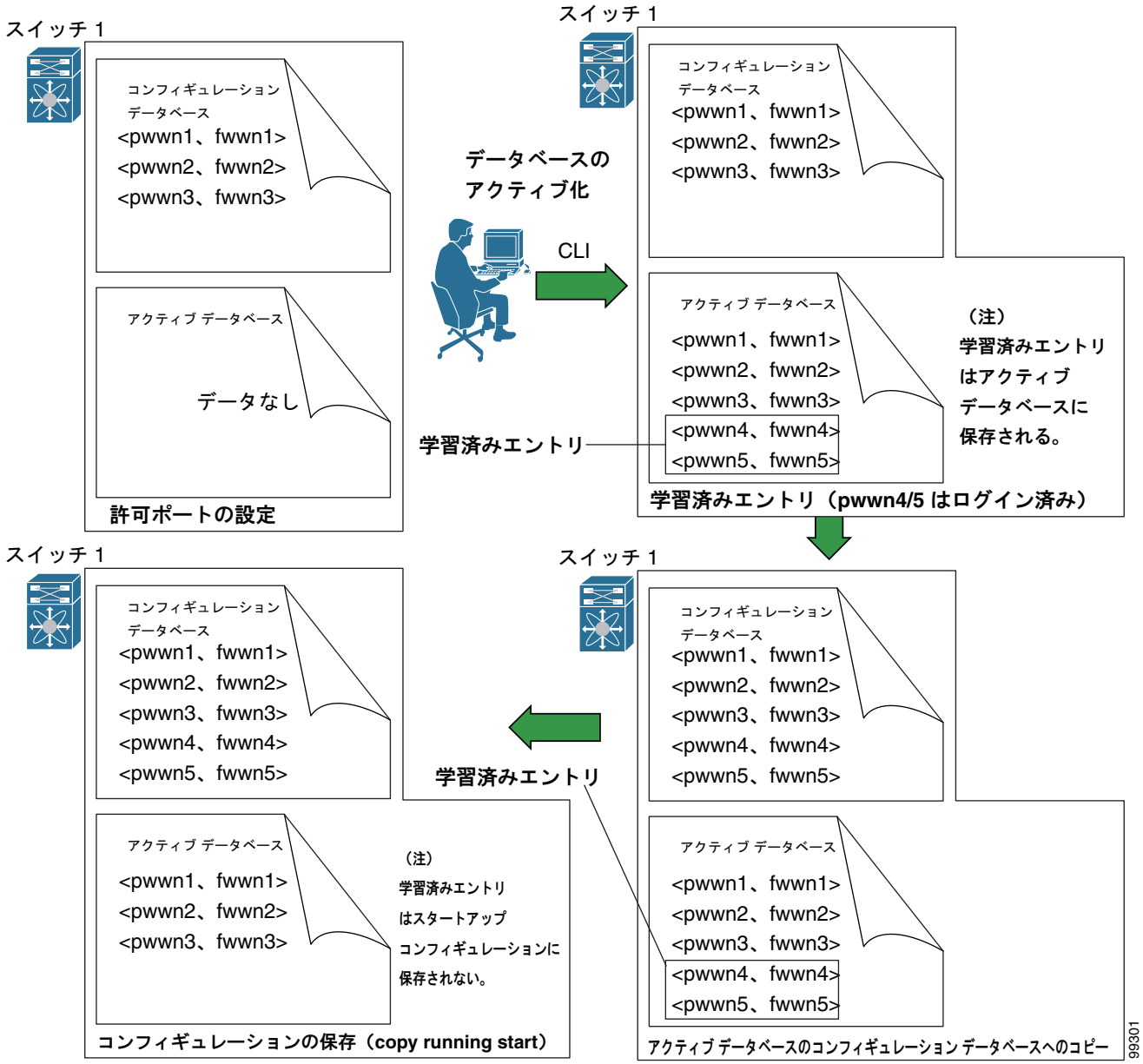
（注）　**port-security database copy vsan** コマンドを使用すると、コンフィギュレーション データベースをアクティブ データベースで上書きできます。アクティブ データベースとコンフィギュレーション データベースとの相違を表示するには、EXEC モードで **port-security database diff active vsan** コマンドを使用します。

この項では、次のトピックについて取り上げます。

データベースのシナリオ

図 39-1 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 39-1　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、**port-security database copy vsan** コマンドを発行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 データベースを確実に同期化できます。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表示するには、**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ーンアップ

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 fc1/1 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 スイッチだけに関連するので、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 コマンドを使用すると、設定されたポート セキュリティ情報が表示されます（例 39-1 ～ 39-11 を参照）。

例 39-1　　ポート セキュリティ コンフィギュレーション データベースの内容の表示

```
switch# show port-security database
---------------------------------------------------------------------------------------
VSAN    Logging-in Entity               Logging-in Point       (Interface)
---------------------------------------------------------------------------------------
1       21:00:00:e0:8b:06:d9:1d(pwwn)  20:0d:00:05:30:00:95:de(fc1/13)
1       50:06:04:82:bc:01:c3:84(pwwn)  20:0c:00:05:30:00:95:de(fc1/12)
2       20:00:00:05:30:00:95:df(swwn)  20:0c:00:05:30:00:95:de(port-channel 128)
3       20:00:00:05:30:00:95:de(swwn)  20:01:00:05:30:00:95:de(fc1/1)
[Total 4 entries]
```

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（例 39-2 を参照）。

例 39-2　　VSAN 1 のポート セキュリティ コンフィギュレーション データベースの表示

```
switch# show port-security database vsan 1
---------------------------------------------------------------------------------
Vsan   Logging-in Entity              Logging-in Point        (Interface)
---------------------------------------------------------------------------------
1                  *                  20:85:00:44:22:00:4a:9e (fc3/5)
1      20:11:00:33:11:00:2a:4a(pwwn)  20:81:00:44:22:00:4a:9e (fc3/1)
[Total 2 entries]
```

例 39-3　　アクティブなデータベースの表示

```
switch# show port-security database active
-------------------------------------------------------------------------------------------
VSAN    Logging-in Entity               Logging-in Point     (Interface)          Learnt
-------------------------------------------------------------------------------------------
1       21:00:00:e0:8b:06:d9:1d(pwwn)   20:0d:00:05:30:00:95:de(fc1/13)            Yes
1       50:06:04:82:bc:01:c3:84(pwwn)   20:0c:00:05:30:00:95:de(fc1/12)            Yes
2       20:00:00:05:30:00:95:df(swwn)   20:0c:00:05:30:00:95:de(port-channel 128) Yes
3       20:00:00:05:30:00:95:de(swwn)   20:01:00:05:30:00:95:de(fc1/1)
[Total 4 entries]
```

例 39-4　　一時的なコンフィギュレーション データベースの内容の表示

```
switch# show port-security pending vsan 1
Session Context for VSAN 1
--------------------------
Activation Status: Active
Auto Learn Status: On
Force activate: No
Config db modified: Yes
Activation done: Yes
Session owner: admin(2)
Session database:
```

```
--------------------------------------------------------------------------------
VSAN Logging-in Entity Logging-in Point (Interface)
--------------------------------------------------------------------------------
1 20:11:00:33:22:00:2a:4a(pwwn) 20:41:00:05:30:00:4a:1e(fc2/1)
[Total 1 entries]
```

例 39-5　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 データベースの差異の表示

```
switch# show port-security pending-diff vsan 1
Session Diff for VSAN: 1
------------------------
Database will be activated
Learning will be turned ON
Database Diff:
+pwwn 20:11:00:33:22:00:2a:4a fwwn 20:41:00:05:30:00:4a:1e
```

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（例 39-6 ～ 39-8 を参照）。

例 39-6　VSAN 1 のワイルドカード fWWN ポート セキュリティの表示

```
switch# show port-security database fwwn 20:85:00:44:22:00:4a:9e vsan 1
Any port can login thru' this fwwn
```

例 39-7　VSAN 1 の設定済み fWWN ポート セキュリティの表示

```
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)
```

例 39-8　VSAN 2 のインターフェイス ポート情報の表示

```
switch# show port-security database interface fc 1/1 vsan 2
20:00:00:0c:88:00:4a:e2(swwn)
```

ポート セキュリティの統計情報は、常に更新され、いつでも利用可能です（例 39-9 を参照）。

例 39-9　ポート セキュリティの統計情報の表示

```
switch# show port-security statistics
Statistics For VSAN: 1
------------------------
Number of pWWN permit: 2
Number of nWWN permit: 2
Number of sWWN permit: 2
Number of pWWN deny  : 0
Number of nWWN deny  : 0
Number of sWWN deny  : 0

Total Logins permitted  : 4
Total Logins denied     : 0
Statistics For VSAN: 2
------------------------
Number of pWWN permit: 0
Number of nWWN permit: 0
```

```
Number of sWWN permit: 2
Number of pWWN deny  : 0
Number of nWWN deny  : 0
Number of sWWN deny  : 0
...
```

アクティブ データベースと自動学習コンフィギュレーションのステータスを確認するには、**show port-security status** コマンドを使用します（例 39-10 を参照）。

例 39-10　　ポート セキュリティのステータスの表示

```
switch# show port-security status
Fabric Distribution Enabled
VSAN 1 :No Active database, learning is disabled, Session Lock Taken
VSAN 2 :No Active database, learning is disabled, Session Lock Taken
...
```

show port-security コマンドでは、過去 100 回の違反をデフォルトで表示します（例 39-11 を参照）。

例 39-11　　ポート セキュリティ データベースでの違反の表示

```
switch# show port-security violations

-------------------------------------------------------------------------------------------
VSAN    Interface       Logging-in Entity               Last-Time          [Repeat count]
-------------------------------------------------------------------------------------------
1       fc1/13          21:00:00:e0:8b:06:d9:1d(pwwn)   Jul  9 08:32:20 2003    [20]
                        20:00:00:e0:8b:06:d9:1d(nwwn)
1       fc1/12          50:06:04:82:bc:01:c3:84(pwwn)   Jul  9 08:32:20 2003    [1]
                        50:06:04:82:bc:01:c3:84(nwwn)
2       port-channel 1  20:00:00:05:30:00:95:de(swwn)   Jul  9 08:32:40 2003    [1]
[Total 2 entries]
```

last *number* オプションを指定した **show port-security** コマンドでは、最初に表示されるエントリの指定数だけを表示します。

デフォルト設定

表 39-5 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 39-5　　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
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、スイッチ上のすべての VSAN の配信がイネーブルになります。