CHAPTER 21

ポート セキュリティの設定

すべての Cisco MDS 9000 ファミリー スイッチには、侵入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 セキュリティがサポートされるのは、ファイバ チャネル ポートのみです。

この章の内容は、次のとおりです。

- ポート セキュリティ機能（p.21-2）
- ポート セキュリティの開始（p.21-3）
- ポート セキュリティの手動設定（p.21-3）
- ポート セキュリティのアクティブ化（p.21-5）
- 自動学習について（p.21-8）
- ポート セキュリティ設定の配布（p.21-11）
- データベース結合に関する注意事項（p.21-14）
- データベースの相互作用（p.21-14）
- ポート セキュリティ データベースのコピー（p.21-16）
- ポート セキュリティ データベースの削除（p.21-16）
- ポート セキュリティ データベースのクリア（p.21-17）
- ポート セキュリティ設定の表示（p.21-18）
- デフォルト設定値（p.21-21）

ポート セキュリティ機能

通常、SAN 内の任意のファイバ チャネル デバイスを任意の SAN スイッチ ポートに接続し、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することができます。ポート セキュリティ機能により、Cisco MDS 9000 ファミリー内のスイッチ ポートへの不正アクセスが禁止されます。

- 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。
- Cisco SAN OS Release 2.0(1b) 以降では、Cisco Fabric Services（CFS）インフラストラクチャを使用して設定が配布されます。設定は、CFS に対応しているスイッチだけに配布されます。配布はデフォルトでディセーブルにされています。
- 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）。

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。

- 各デバイスに 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。
- 各スイッチに 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 ポートを設定すると、接続先を単一ポートまたはポート範囲に制限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なければなりません。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、許可を行います。

ポート セキュリティの開始

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

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。

	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 モードを開始します。
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 セキュリティの手動設定

Cisco MDS 9000 ファミリー 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。

WWN の識別

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 ポートの場合：
  - SAN スイッチ ポート Fx にログインできる場合、Nx ポートは指定された Fx ポートを通してのみログインできます。
  - nWWN が Fx ポート WWN にバインドしている場合、Nx ポートのすべての pWWN は Fx ポートと暗黙的にペアになります。
- TE ポートのチェックは、トランク ポートの許可 VSAN（仮想 SAN）リスト内の VSAN ごとに実行されます。
- すべてのポート チャネル xE ポートには、同じポート チャネル内の同じ WWN セットを設定する必要があります。
- E ポート セキュリティは E ポートのポート VSAN 内で実装されます。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 データベースを変更しても、アクティブ データベースには影響が及びません。

- 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。

許可されたポート 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　Cisco SAN OS Release 2.0(1b) 以降では、ローカル スイッチでリモート スイッチのバインドを指定できます。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 セキュリティを設定する手順は、次のとおりです。

	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 モードを開始します。
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。
ステップ 3	`switch(config-port-security)# swwn 20:01:33:11:00:2a:4a:66 interface port-channel 5`	ポート チャネル 5 を介した場合のみ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を介した場合のみ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`	上記ステップで設定した指定の 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`	ファブリック内の任意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任意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`	上記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すべての Cisco MDS 9000 ファミリー スイッチで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場合、次のようになります。

- 自動学習も自動的にイネーブルにされます。自動学習がイネーブルにされると、次のようになります。
  - この時点から、アクティブ化されていないデバイスまたはインターフェイスに対してのみ学習が行われます。
  - 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することはできません。
- ログインされた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、アクティブ化されたポートによってバインドされた WWN ペアの影響を受けます。

ポート セキュリティ機能をアクティブにすると、**auto-learn** オプション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、**auto-learn** をディセーブルにすることもできます。それには、**port-security activate vsan** *number* **no-auto-learn** コマンドを使用します。

ポート セキュリティ機能をアクティブにする手順は、次のとおりです。

	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 モードを開始します。
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)# no port-security activate vsan 1`	指定された VSAN のポート セキュリティ データベースを非アクティブにし、自動的に自動学習をディセーブルにします。

（注）　必要な場合は、自動学習をディセーブルにすることができます（「自動学習のディセーブル化」[p.21-9] 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。
- アクティブ化の前に、自動学習機能がイネーブルになっていた場合。この状態においてデータベースを再アクティブにする場合。
- 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 つまたは複数発生したためにデータベースのアクティブ化が拒否された場合は、ポート セキュリティのアクティブ化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

（注）　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、**force** オプションを使用してアクティブ化している場合は、既存のデバイスをログアウトできます。

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、**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手順は、次のとおりです。

	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 モードを開始します。
ステップ 2	`switch(config)# port-security activate vsan 1 force`	矛盾がある場合でも、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　**auto-learn** オプションがイネーブルの場合は、データベースをアクティブにしても、処理を継続できません。

データベースを再アクティブにする手順は、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　設定済み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は、この手順を実行できません。

ステップ 3　コンフィギュレーション データベースに必要な変更を加えます。

ステップ 4　データベースをアクティブにします。

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

	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 モードを開始します。
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。

自動学習について

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、スイッチに指示することができます。この機能を使用すると、任意の Cisco MDS 9000 ファミリー 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することができます。最初に、この機能を使用してポート セキュリティ機能をアクティブにしてください。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。**auto-learn** オプションは VSAN 単位で設定する必要があります。自動学習がイネーブルの場合は、ポート アクセスを設定していない場合でも、スイッチへの接続が許可されたデバイスおよびスイッチが自動学習されます。ポート上の学習されたエントリは、そのポートがシャットダウンされたあとに削除されます。学習は、強制されたポート セキュリティ ポリシーを上書きしません。

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。自動学習をイネーブルにした場合、次のようになります。

- アクティブ化されていないデバイスまたはインターフェイスに対してのみ学習が行われます。
- データベースをアクティブにすることはできません。

自動学習の設定

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、**auto-learn** オプション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、**auto-learn** オプション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 **auto-learn** オプション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。

自動学習をイネーブルにする手順は、次のとおりです。

	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 モードを開始します。
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 へのアクセスを許可されたすべてのデバイスを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手順は、次のとおりです。

	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 モードを開始します。
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 21-1 に、デバイス要求に対して接続が許可される場合をまとめます。

表 21-1　自動学習デバイスの許可

デバイス（pWWN、nWWN、sWWN）	接続先	許可	状態
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	設定されたポート上のスイッチ	許可	1
	他のポート上のスイッチ	拒否	2
設定されていない場合	設定されていないポート	許可（自動学習がイネーブルの場合）	3
		拒否（自動学習がディセーブルの場合）	4
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	5
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	6
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	7

許可シナリオ

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ことが前提です。

- pWWN（P1）にインターフェイス fc1/1（F1）を介してアクセス可能
- pWWN（P2）にインターフェイス fc1/1（F1）を介してアクセス可能
- nWWN（N1）にインターフェイス fc1/2（F2）を介してアクセス可能
- 任意の WWN にインターフェイス fc1/3（F3）を介してアクセス可能
- nWWN（N3）に任意のインターフェイスを介してアクセス可能
- pWWN（P3）にインターフェイス fc1/4（F4）を介してアクセス可能
- sWWN（S1）にインターフェイス fc1/10 ～ 13（F10 ～ 13）を介してアクセス可能
- pWWN（P10）にインターフェイス fc1/11（F11）を介してアクセス可能

表 21-2 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。

表 21-2　各シナリオの許可結果

シナリオ	デバイス接続要求	許可	状態	理由
1	P1、N2、F1	許可	1	競合なし。
2	P2、N2、F1	許可	1	競合なし。
3	P3、N2、F1	拒否	2	F1 が P1/P2 にバインドされています。
4	P1、N3、F1	許可	6	N3 に関するワイルドカードが一致しています。
5	P1、N1、F3	許可	5	F3 に関するワイルドカードが一致しています。
6	P1、N4、F5	拒否	2	P1 が F1 にバインドされています。
7	P5、N1、F5	拒否	2	N1 は F2 でのみ許可されます。
8	P3、N3、F4	許可	1	競合なし。
9	S1、F10	許可	1	競合なし。
10	S2、F11	拒否	7	P10 が F11 にバインドされています。
11	P4、N4、F5 （自動学習が有効）	許可	3	競合なし。
12	P4、N4、F5 （自動学習が無効）	拒否	4	一致なし。
13	S3、F5 （自動学習が有効）	許可	3	競合なし。
14	S3、F5 （自動学習が無効）	拒否	4	一致なし。
15	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。
16	P5、N5、F1 （自動学習が有効）	拒否	7	P3 が F1 にバインドされています。
17	S3、F4 （自動学習が有効）	拒否	7	P3 と F4 がペアになります。
18	S1、F3 （自動学習が有効）	許可	5	競合なし。
19	P5、N3、F3	許可	6	F3 および N3 に関するワイルドカード（*）が一致しています。
20	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 セキュリティ設定の配布

ポート セキュリティ機能は 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（第 9 章「CFS インフラストラクチャの使用」を参照）。

配布のイネーブル化

配布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。

ポート セキュリティの配布をイネーブルにする手順は、次のとおりです。

	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 モードを開始します。
ステップ 2	`switch(config)# port-security distribute`	配布をイネーブルにします。
	`switch(config)# no port-security distribute`	配布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布されます。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。

	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 モードを開始します。
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手順は、次のとおりです。

	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 モードを開始します。
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。

アクティブ化設定および自動学習設定の配布

配布モードのアクティブ化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だけに実行するアクションです。

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役割を持ちません。そのため、学習済みエントリは配布に参加しません。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、学習済みの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布されます。コミットのあと、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することができます。

保留中のデータベースに複数のアクティブ化設定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、アクティブ化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（表 21-3 を参照）。

ポート セキュリティをアクティブ化（**port-security activate** コマンド）し、次に自動学習をディセーブル（**no port-security auto-learn** コマンド）にし、最後に保留中のデータベースの変更をコミットする場合、**port-security activate no-auto-learn** コマンドを入力した場合と同じ結果が得られます。

表 21-3　配布モードのアクティブ化設定および自動学習設定のシナリオ

シナリオ	アクション	配布がオフの場合	配布がオンの場合
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、アクティブ化が行われておらず、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化し、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 + アクティブ化（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 + アクティブ化（イネーブル）}
	3. コミットを行います。	該当なし	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 21-3　配布モードのアクティブ化設定および自動学習設定のシナリオ（続き）

シナリオ	アクション	配布がオフの場合	配布がオンの場合
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、アクティブ化が行われておらず、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 + アクティブ化（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 + アクティブ化（イネーブル）+ 学習（ディセーブル）}
	3. コミットを行います。	該当なし	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ブ化と同じです。 保留中のデータベース = 空の状態

1. *（アスタリスク）は学習済みエントリを示します。

ヒント　この場合、各操作の最後（ポート セキュリティをアクティブ化し、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。

データベース結合に関する注意事項

データベース結合とは、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）エントリの合体を指しています。詳しい概念については、「CFS 結合のサポート」（p.9-7）を参照してください。

2 つのファブリックのデータベースを結合する場合は、次の注意事項に従ってください。

- アクティブ化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 2K 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、結合に失敗します。次の配布がファブリック内のデータベースとアクティブ化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 21-4 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 21-4　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

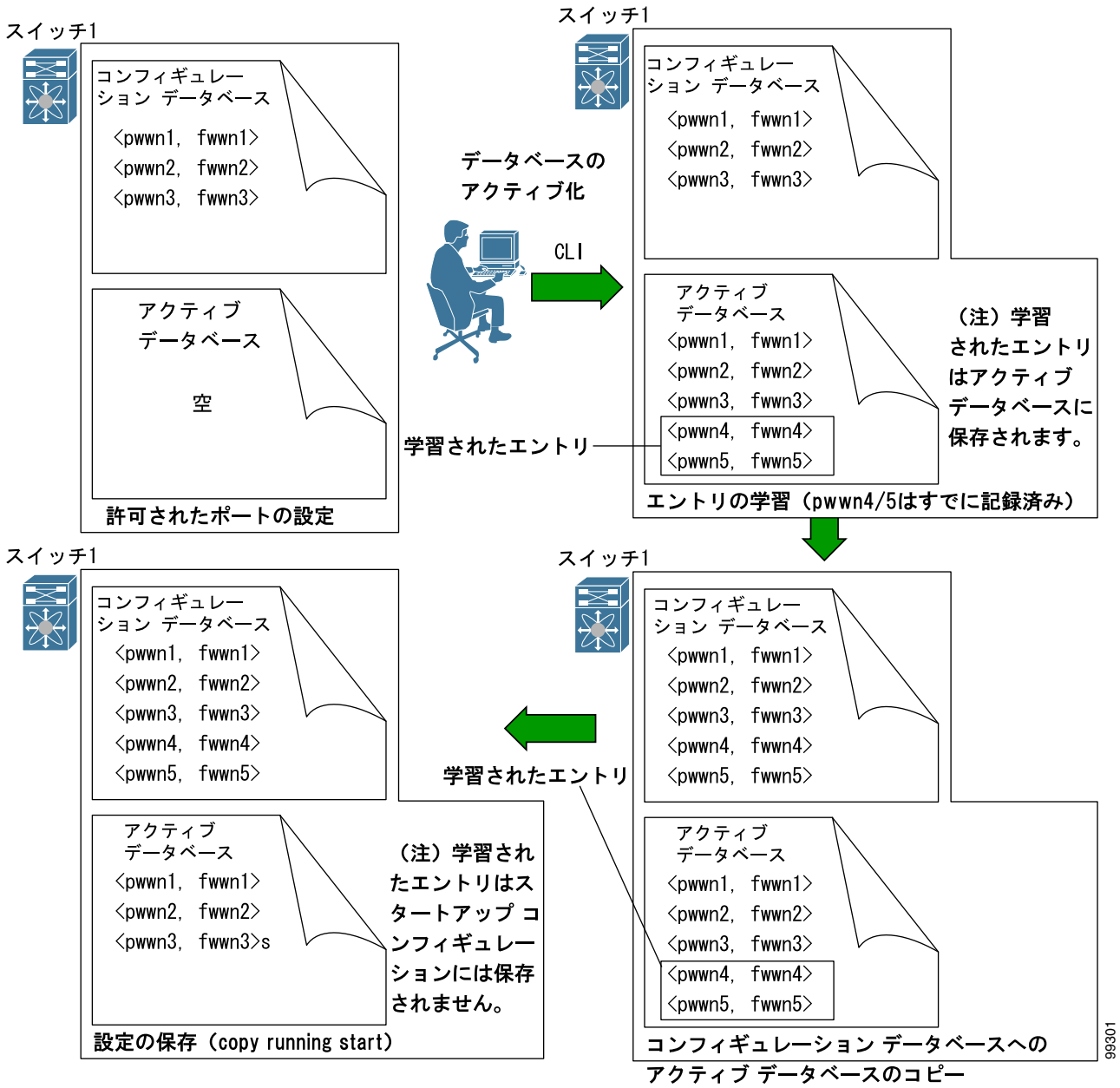
コンフィギュレーション データベース	アクティブ データベース
読み取り / 書き込み	読み取り専用
設定を保存すると、コンフィギュレーション データベース内のすべてのエントリが保存されます。	設定を保存すると、アクティブなエントリのみが保存されます。学習されたエントリは保存されません。
アクティブ化されたコンフィギュレーション データベースを変更しても、アクティブ データベースには反映されません。	アクティブ化すると、VSAN にログイン済みのすべてのデバイスも学習され、アクティブ データベースに追加されます。
コンフィギュレーション データベースをアクティブ データベースで上書きすることができます。	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。アクティブ化を強制すると、アクティブ データベース内に設定されているエントリに違反することがあります。

（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することができます。アクティブ データベースとコンフィギュレーション データベース間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。

データベースのシナリオ

図 21-1 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ます。

図 21-1　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たあと、**port-security database copy vsan** コマンドを入力することを推奨します。このアクションは、コンフィギュレーション データベースを確実にアクティブ データベースと同期化させます。配布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（および必然的にファブリック ロック）を取得できます。ファブリックをロックする場合、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
switch#
```

アクティブ データベースとコンフィギュレーション データベース間の違いを表示するには、**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 データベース間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　配布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 **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** 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** 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** 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のみにローカルで、配布に参加しません。

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 コマンドは、設定されたポート セキュリティ情報を表示します（例 21-1 ～ 21-11 を参照）。

例 21-1　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 21-2 を参照）。

例 21-2　VSAN 1 内のポート 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 21-3　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 21-4　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 21-5　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 データベースの相違の表示

```
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を個別に表示できます。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 21-6 ～ 21-8 を参照）。

例 21-6　VSAN 1 内のワイルドカード 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 21-7　VSAN 1 内の設定済み 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 21-8　VSAN 2 内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 セキュリティ統計情報は継続的に更新され、いつでも使用できます（例 21-9 を参照）。

例 21-9　ポート セキュリティ統計情報の表示

```
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 データベースのステータスおよび自動学習設定を確認するには、**show port-security status** コマンドを使用します（例 21-10 を参照）。

例 21-10　ポート セキュリティ 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 コマンドは、デフォルトで、直前の 100 個の違反を表示します（例 21-11 を参照）。

例 21-11　ポート セキュリティ データベースの違反の表示

```
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て **show port-security** コマンドを使用すると、指定された個数のエントリが先頭から表示されます。

デフォルト設定値

表 21-5 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値を示します。

表 21-5　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
配布	ディセーブル （注）　配布のイネーブル化は、スイッチ上のすべての VSAN の配布をイネーブルにします。