FIPS の設定

連邦情報処理標準規格（FIPS）140-2、*暗号モジュール セキュリティ要件*は、暗号モジュールに対する米国政府の要求条件を定義しています。FIPS 140-2 では、暗号モジュールがハードウェア、ソフトウェア、ファームウェア、または何らかの組み合わせのセットで、暗号機能またはプロセスを実装し、暗号アルゴリズムおよび任意のキー生成機能を含み、明確に定義された暗号境界の内部に位置しなければならないと定義しています。

FIPS は特定の暗号アルゴリズムがセキュアであることを条件とするほか、ある暗号モジュールが FIPS 準拠であると称する場合は、どのアルゴリズムを使用すべきかも指定しています。

（注） Cisco MDS SAN-OS Release 3.1(1) および NX-OS Release 4.1(1b) 以降は FIPS に準拠して実装しており、現在のところ米国政府による認定途中にありますが、現時点では FIPS 準拠ではありません。

この章は、次の項で構成されています。

設定時の注意事項

FIPS モードをイネーブルにする前に次の注意事項を守ってください。

- パスワードは最小限 8 文字の長さで作成してください。
- Telnet をディセーブルにします。ユーザのログインは SSH だけで行ってください。
- RADIUS/TACACS+ によるリモート認証をディセーブルにしてください。スイッチに対してローカルのユーザだけが認証可能です。
- SNMP v1 および v2 をディセーブルにしてください。SNMP v3 に対して設定された、スイッチ上の既存ユーザ アカウントのいずれについても、認証およびプライバシー用 AES/3DES は SHA で設定されていなければなりません。
- VRRP をディセーブルにしてください。
- 認証用 MD5 または暗号用 DES のいずれかを含む、すべての IKE ポリシーを削除してください。認証に SHA、暗号用に 3DES/AES を使用するようにポリシーを修正してください。
- SSH サーバの RSA1 キー ペアすべてを削除してください。

FIPS モードのイネーブル化

FIPS モードを有効にするには、次の手順に従ってください。

	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)# fips mode enable`	FIPS モードをイネーブルにします。
	`switch(config)# no fips mode enable`	FIPS モードをディセーブルにします。

FIPS ステータスの表示

FIPS のステータスを表示するには **show fips status** コマンドを入力します。

FIPS セルフテスト

暗号モジュールは、適正に動作していることを確認するために、電源投入時のセルフテストと条件付きセルフテストを実行しなければなりません。

（注）　FIPS の電源投入時セルフテストは、**fips mode enable** コマンドを入力して FIPS モードがイネーブルにされていると自動的に実行されます。スイッチが FIPS モードに入るのは、すべてのセルフテストが正しく完了したときだけです。セルフテストのいずれかが失敗すると、スイッチは再起動します。

電源投入時セルフテストは、FIPS モードのイネーブル後、即時に実行されます。既知の解を使用する暗号アルゴリズム テストは、Cisco MDS 9000 ファミリ製品に実装されている FIPS 140-2 認定暗号アルゴリズムのそれぞれに対して、すべての暗号機能で実行されなければなりません。

既知解テスト（KAT）を利用すると、暗号アルゴリズムは正しい出力があらかじめわかってるデータに対して実行され、その計算出力は前回生成された出力と比較されます。計算出力が既知解と等しくない場合は、既知解テストに失敗したことになります。

何かに対応してセキュリティ機能または操作が始動された場合は、条件付きセルフテストが実行されなければなりません。電源投入時セルフテストとは異なって、条件付きセルフテストはそれぞれに関連する機能がアクセスされるたびに実行されます。

条件付きセルフテストでは次を含むテストが行われます。

- ペア整合性テスト: このテストは公開キー/秘密キー ペアが生成されたときに実行されます。
- 乱数連続生成テスト: このテストは乱数が生成されたときに実行されます。

以上の両方はスイッチが FIPS モードに入っていると自動的に実行されます。