CHAPTER 2

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。

この章では、次の事項について説明します。

FIPS セルフテストの概要

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。

注意事項と制限

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。

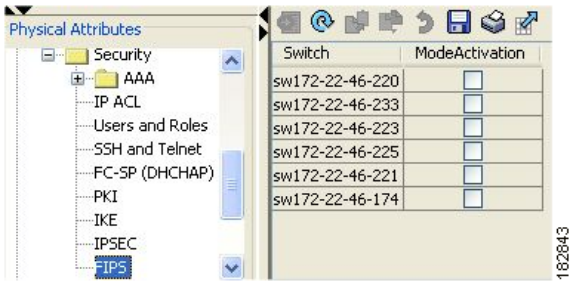
FIPS モードのイネーブル

手順の詳細

DCNM-SAN を使用して FIPS モードをイネーブルにする手順は、次のとおりです。

ステップ 1　[Physical Attributes] ペインで [Switches] を開きます。[Security] を開いてから [FIPS] を選択します。[Information] ペインに FIPS 有効設定の詳細が表示されます（図 2-1 を参照）。

図 2-1　DCNM-SAN での FIPS 有効設定



ステップ 2　FIPS モードをイネーブルにするスイッチの [ModeActivation] チェックボックスにチェックを入れます。

ステップ 3　[Apply Changes] をクリックして、その変更をコミットして割り当てます。

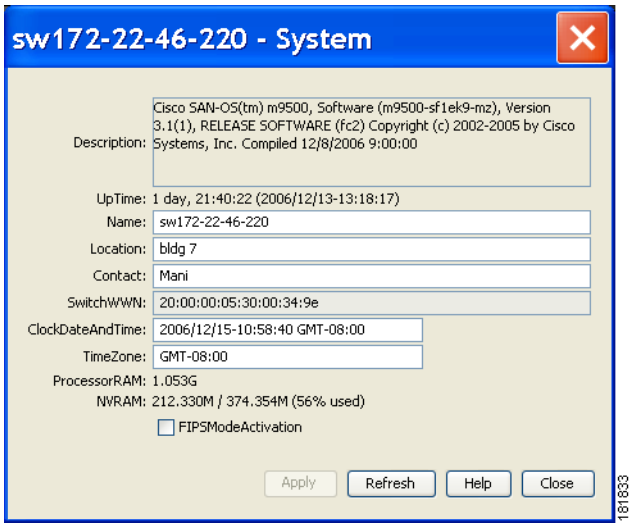
ステップ 4　保存していない変更を廃棄するために [Undo Changes] をクリックします。

Device Manager を使用して FIPS モードをイネーブルにする手順は、次のとおりです。

ステップ 1　[Physical] > [System] を選択するか、[Configure] を右クリックして選択します。

図 2-2 に示す [System] ダイアログボックスが表示されます。

図 2-2　[System] ダイアログボックス



ステップ 2　[FIPSModeActivation] チェックボックスにチェックを入れて、選択したスイッチの FIPS モードをイネーブルにします。

ステップ 3　[Apply] をクリックして、変更内容を保存します。

ステップ 4　[Close] をクリックして、ダイアログボックスを閉じます。

FIPS のフィールドの説明

FIPS

フィールド	説明
ModeActivation	デバイスの FIPS モードをイネーブルまたはディセーブルにします。FIPS 140-2 は暗号モジュールに関する一連のセキュリティ要件であり、暗号モジュールに対する米国政府の要求条件を詳細に記述しています。モジュールは、ハードウェアとソフトウェアの両方で構成されます（たとえば、データセンターのスイッチングまたはルーティング モジュール）。 FIPS モードをイネーブルにするための要求が受信され、その要求に応じて一連のセルフテストが正常に実行される場合、モジュールは FIPS 対応モードにあると言われます。セルフテストが失敗した場合は、適切なエラーが返されます。