FIPS の設定

この章では、Cisco NX-OS デバイスで連邦情報処理標準（FIPS）モードを設定する方法について説明します。

この章は、次の項で構成されています。

- FIPS について （1 ページ）
- FIPS の前提条件 （3 ページ）
- FIPS の注意事項と制約事項 （3 ページ）
- FIPS のデフォルト設定 （3 ページ）
- FIPS の設定 （4 ページ）
- FIPS 設定の確認 （6 ページ）
- 2048ビットRSAキーの作成 （6 ページ）
- FIPS の設定例 （7 ページ）
- FIPS に関する追加情報 （7 ページ）

FIPS について

FIPS 140-2 の刊行物『*Security Requirements for Cryptographic Modules*』には、暗号モジュールに対する米国政府の要件が詳細に記載されています。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、暗号化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 は特定の暗号化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を指定しています。

FIPS のセルフテスト

暗号モジュールは、自身の正常な動作を保証するために、電源投入時セルフテストと条件付きセルフテストを実行する必要があります。

電源投入時セルフテストは、デバイスの電源が投入された後に自動的に実行されます。デバイスが FIPS モードになるのは、すべてのセルフテストが正常に完了した後だけです。いずれか

のセルフテストが失敗すると、デバイスはシステムメッセージをログに記録し、エラー状態に移行します。

最小モジュラス サイズが 2048 の「crypto key generate rsa label test exportable modulus」を生成します。キーサイズが 2048 未満の場合は、「FIPS セルフテストまたは FIPS エラー状態」に分類されます。

デバイスは、既知解テスト（KAT）という暗号化アルゴリズムを使用して、デバイス上に実装されている FIPS 140-2 で承認された暗号機能（暗号化、復号化、認証、および乱数生成）ごとに FIPS モードをテストします。デバイスは、このアルゴリズムを、すでに正しい出力がわかっているデータに対して適用します。次に、計算された出力を、以前に生成された出力と比較します。計算された出力が既知解に等しくない場合は、KAT が失敗します。

適用可能なセキュリティ機能または操作が呼び出された場合は、条件付きセルフテストが自動的に実行されます。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。

ペアワイズ一貫性テスト

このテストは、公開キーまたは秘密キーのペアが生成されたときに実行されます。

連続乱数ジェネレータ 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。

また、Cisco TrustSec マネージャは、暗号化されたテキストが決してプレーン テキストとして送信されないようにするためにバイパス テストを実行します。

（注） CTS に対応したポート上でバイパス テストが失敗すると、それらの対応するポートのみがシャットダウンされます。バイパス テストは、データ パスの輻輳によって発生したパケットドロップのために失敗することがあります。このような場合は、そのポートを再び立ち上げてみることを推奨します。

FIPS エラー状態

システムが FIPS モードで起動されると、スーパーバイザおよびラインカード モジュール上で FIPS 電源投入時セルフテストが実行されます。これらの起動テストのいずれかが失敗すると、システム全体が FIPS エラー状態に移行されます。この状態では、FIPS の要件に従って、すべての暗号キーが削除され、すべてのラインカードがシャットダウンされます。このモードは、デバッグのみを目的にしています。

スイッチが FIPS エラー状態になった後、ラインカードをリロードすると常に、そのラインカードが障害状態に移行されます。スイッチを FIPS モードに戻すには、再起動する必要があります。ただし、スイッチが FIPS モードになった後、ラインカードのそれ以降のリロードまたは挿入で電源投入時セルフテストが失敗すると常に、そのラインカードにのみ影響を与え、対応するラインカードのみが障害状態に移行されます。

FIPS の前提条件

FIPS には、次の前提条件があります。

- Telnet をディセーブルにする。ユーザのログインはセキュア シェル（SSH）だけで行ってください。
- SNMP v3 に対して設定された、デバイス上の既存ユーザ 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。
- SSH サーバの RSA1 キー ペアすべてを削除してください。
- Cisco TrustSec セキュリティ アソシエーション プロトコル（SAP）ネゴシエーション中に使用する HMAC-SHA1 メッセージ整合性チェック（MIC）をイネーブルにします。そのためには、cts-manual または cts-dot1x モードで **sap hash-algorithm HMAC-SHA-1** コマンドを入力します。

FIPS の注意事項と制約事項

FIPS 設定時の注意事項と制約事項は次のとおりです。

- SSH でサポートされているユーザ認証メカニズムは、ユーザ名とパスワード、公開キー、および X.509 証明書です。
- パスワードは、最小 8 文字の英数字である必要があります。
- FIPS モードがオンの場合は、Radius と TACACS を無効にします。これは、FIPS モードの OpenSSL により適用されます。
- ASCII リロード後に **fips mode enable** コマンドを実行する場合は、**copy running-config startup-config** コマンドの実行後に Cisco NX-OS スイッチをリロードする必要があります。

FIPS のデフォルト設定

次の表に、FIPS パラメータのデフォルト設定を示します。

表 *1 :* デフォルトの *FIPS* パラメータ

パラメータ	デフォルト
FIPS モード	無効化

FIPS の設定

ここでは、Cisco NX-OS デバイスで FIPS モードを設定する方法について説明します。

FIPS モードの有効化

Cisco NX-OS リリース 7.0(3)I5(1) 以降では、デバイスの FIPS モードを有効にできます。

始める前に

デフォルト VDC にいることを確認します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル 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	**fips mode enable** 例： `switch(config)# fips mode enable`	FIPS モードを有効にします。 （注） **fips mode enable** はすべての LC がオンラインのときにのみ入力できます。LC がオンラインでないときに入力すると、LC で障害が発生します。

ステップ 3	**exit**
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	（任意） **show fips status**
	例：
	`switch# show fips status`
	`FIPS mode is enabled`
		FIPSモードのステータスを表示します。

ステップ 5	必須: **copy running-config startup-config** 例： `switch# copy running-config startup-config`	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。

	コマンドまたはアクション	目的
ステップ 6	必須: **reload** 例： `switch# reload`	Cisco NX-OS デバイスをリロードします。 （注） FIPS をイネーブルにすると、システムが FIPS モードで動作するためにリブートが必要です。

FIPS の無効化

デバイスの FIPS モードを無効にできます。

始める前に

デフォルト VDC にいることを確認します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル 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	**no fips mode enable** 例： `switch(config)# no fips mode enable`	FIPS モードを無効にします。

ステップ 3	**exit**
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	（任意） **show fips status**
	例：
	`switch# show fips status`
	`FIPS mode is disabled`
		FIPS モードのステータスを表示します。

ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	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。

	コマンドまたはアクション	目的
ステップ 6	**reload** 例： `switch# reload`	Cisco NX-OS デバイスをリロードします。

FIPS 設定の確認

FIPS 設定情報を表示するには、次のいずれかの作業を実行します。

コマンド	目的
show fips status	FIPS機能のステータスを表示します。

このコマンドの出力フィールドの詳細については、『*Cisco Nexus 9000* シリーズ *NX-OS* セキュリティ コマンド リファレンス』を参照してください。

2048ビットRSAキーの作成

2048ビットRSAキーを作成する手順：

- `N9k-Switch# conf t`

  `Enter configuration commands, one per line. End with CNTL/Z.`
- `N9k-Switch(config)# no feature ssh`

  `XML interface to system may become unavailable since ssh is disabled`
- `N9k-Switch(config)# no ssh key rsa`
- `N9k-Switch(config)# ssh key rsa 2048`
- `New SSH Key has a bitcount of 2048:`

  `N9k-Switch(config)# show ssh key`

  `**********`

  `rsa Keys generated:Wed Apr 28 13:05:18 2021`

  `ssh-rsa  AAAAB3NzaC1yc2EAAAADAQABAAABAQDHpxEgZ9LwmbOEpJeJtLwqedmTLkZV7Setxb9D4xgO`

  `p2o2f6wt/48bPp/vLDGsxTF2PtLRtRSSDFNSQmkw9bg+MXvTpgNivdxWLjxtwo3YpYwPkBiReVmyrFgE`

  `UuBmV/sDfhJpHXLoH9lR2+y0L5w1OG3cJxMe30TI37O3M8fZPjrAtHgkUubfEpiTbcyEw+aIHf+chyoR`

  `eDJxcEdnlboiTDFR0/+jMUUM/vMtxd5x5DH3AO7htA/i8lvskrReR1CpX1sOOdcshmS57EEuEzR9cs+w`

  `KSftQh6vLD802207T6+J7/+cXMVNQEbq0mCSzeTmOsuIQe8u9ZC24pgYzZ19`

  `bitcount：2048`

  `fingerprint:`

```
SHA256:Am9861AIq5MzfSPQr4ZXGe0f5M9crnhk7HVZBXhMVBo
************************************
could not retrieve dsa key information
************************************
could not retrieve ecdsa key information
************************************
```

FIPS の設定例

FIPS モードをイネーブルにする例を示します。

```
config terminal
fips mode enable
show fips status
exit
copy running-config startup-config
reload
```

FIPS に関する追加情報

ここでは、FIPS の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS のライセンス	『*Cisco NX-OS* ライセンス ガイド』
コマンド リファレンス	『*Cisco Nexus 9000* シリーズ *NX-OS* セキュリティ コマンド リファレンス』

標準

標準	タイトル
FIPS 140-2	暗号モジュールのセキュリティ要件

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。