ファブリック セキュリティ

この章は、次の項で構成されています。

- 連邦情報処理標準（FIPS）について （1 ページ）
- FIPS の注意事項と制約事項 （1 ページ）
- GUI を使用した Cisco APIC の FIPS の設定 （2 ページ）
- NX-OS Style CLI を使用した Cisco APIC 向けの FIPS を設定する （3 ページ）
- REST API を使用した Cisco APIC の FIPS の設定 （3 ページ）

連邦情報処理標準（FIPS）について

連邦情報処理標準（FIPS）発行 140-2、暗号化モジュールのセキュリティ要件では、暗号化モジュールの米国政府要件が詳述されています。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。

FIPS の注意事項と制約事項

FIPS には、次の注意事項および制約事項が適用されます。

- FIPS が有効になっている場合、FIPS はCisco Application Policy Infrastructure Controller（APIC）全体に適用されます。
- FIPS が有効の場合は、Cisco APIC を FIPS がサポートされていないリリースにダウングレードする前に、FIPS を無効にする必要があります。
- 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。SSH のみを使用してログインします。Telnet は 5.3(1) 以降のリリースではサポートされていません。

- SSH サーバーの RSA1 キー ペアすべてを削除してください。
- セキュア シェル（SSH） および SNMP がサポートされます。
- SNMP v1 および v2 をディセーブルにしてください。SNMPv3 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 AES3 は SHA でのみ設定されていなければなりません。
- 2.3(1) 以降のリリースでは、FIPS はスイッチレベルで構成できます。
- 3.1(1) 以降のリリースでは、FIP が有効になっている場合、NTP は FIPS モードで動作します。FIPS モードでは、NTP は HMAC-SHA1 による認証ありと認証なしをサポートしています。
- 5.2(3) 以前のリリースでは、Cisco APIC で FIPS を有効にした後、デュアルスーパーバイザスパインスイッチを 2 回再読み込みして FIPS を有効にします。
- 5.2(4) 以降のリリースでは、Cisco APIC で FIPS を有効にした後、デュアルスーパーバイザスパインスイッチを再読み込みしてから電源を入れ直し、FIPS を有効にします。
- 5.2(3) 以前のリリースでは、FIPS が有効になっているデュアルスーパーバイザ スパインスイッチで、すべてのスーパーバイザを交換した場合、FIPS を有効にするためにスパインスイッチを 2 回再読み込みする必要があります。
- 5.2(4) 以降のリリースでは、FIPS が有効になっているデュアルスーパーバイザ スパインスイッチで、すべてのスーパーバイザを交換した場合、スパインスイッチを再読み込みしてから、FIPS を有効にするために電源を再投入する必要があります。
- 5.2(3) 以前のリリースでは、RADIUS および TACACS+ リモート認証方式を無効にします。FIPS モードでは、ローカルおよび LDAP 認証方法のみがサポートされています。
- 5.2(4) 以降のリリースでは、RADIUS、TACACS+、および RSA リモート認証方式を無効にしてください。FIPS モードでは、ローカル、LDAP、OAuth2、および SAML 認証方法のみがサポートされています。

GUI を使用した Cisco APIC の FIPS の設定

FIPS が有効になっている場合、Cisco Application Policy Infrastructure Controller(APIC) 全体に適用されます。

手順

ステップ 1 メニュー バーで、**[システム（System）]** > **[システム設定（System Settings）]** の順に選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ファブリック セキュリティ（Fabric Security）]** を選択します。

ステップ 3 **[作業]** ペインの **[プロパティ]** 領域で、目的の FIPSモードを選択します。

FIPSモードのオプションは、**[無効化]** と **[有効化]** です。デフォルト値は **[無効（Disable）]** です。

（注）
設定を完了するには再起動する必要があります。モードを変更すると、設定を完了するため必ず再起動する必要があります。

NX-OS Style CLI を使用した Cisco APIC 向けの FIPS を設定する

FIPS を有効にすると、Cisco Application Policy Infrastructure Controller(APIC) 全体に適用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	コンフィギュレーション モードを開始します。 **例**： `apic1# configure`	
ステップ 2	FIPS を有効にします。 **例**： `apic1(config)# fips mode enable`	設定を完了するには再起動する必要があります。モードを変更すると、設定を完了するため必ず再起動する必要があります。 **no fips mode enable** コマンドにより FIPS が無効になります。

REST API を使用した Cisco APIC の FIPS の設定

FIPS を有効にすると、Cisco APIC 全体に適用されます。

手順

すべてのテナントの FIPS を設定します。

例：

```
https://apic1.cisco.com/api/node/mo/uni/userext.xml
<aaaFabricSec fipsMode="enable" />
```

（注）

設定を完了するには再起動する必要があります。モードを変更すると、設定を完了するため必ず再起動する必要があります。

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。