FIPS 管理

この章は、次の項で構成されています。

FIPS 管理の概要

Federal Information Processing Standard（FIPS；連邦情報処理標準）140 は、米国およびカナダ連邦政府が共同で策定して公式に発表した標準規格です。これは、慎重な扱いを要するにもかかわらず機密扱いでない情報を保護するために、政府機関によって使用される暗号化モジュールの要件を規定しています。Cisco Secure Email and Web Manager は、FIPS 140-2 Level 1 コンプライアンスの達成に Cisco SSL 暗号化ツールキットを使用します。

Cisco SSL 暗号化ツール キットは、OpenSSL の FIS サポートの拡張バージョンと、FIPS 準拠のシスコの共通の暗号化モジュールである Cisco SSL を含む GGSG 承認された暗号化スイートです。シスコの共通の暗号化モジュールは、Cisco Secure Email and Web Manager が SSH などのプロトコルに対する FIPS 検証済み暗号化アルゴリズムに使用するソフトウェアライブラリです。

（注） Cisco Secure Email and Web Manager の FIPS 認定は、電子メールゲートウェイの統合にのみ適用され、Cisco Secure Web Appliance の統合には適用されません。

FIPS モードでの設定変更

Cisco Secure Email and Web Manager は、アプライアンスが FIPS モードの場合、Cisco SSL と FIPS 準拠の証明書を通信に使用します。詳細については、アプライアンスの FIPS モードへの切り替え （2 ページ）を参照してください。

FIPS レベル 1 に準拠するため、Cisco Secure Email and Web Manager はお使いの設定に次の変更を行います。

- **SMTP の受信および配信**：Cisco Secure Email and Web Manager のパブリックリスナーとリモートホスト間の TLS での着信および発信 SMTP カンバセーションは、TLS バージョン 1.1 または 1.2 および FIPS 暗号スイートを使用します。TLS v 1.1 および 1.2 は、FIPS モードでサポートされる TLS のバージョンです。
- **Web インターフェイス**：Cisco Secure Email and Web Manager の Web インターフェイスへの HTTPS セッションに、TLS バージョン 1.1 または 1.2 および FIPS 暗号スイートを使用します。これには、スパム隔離への HTTPS セッションなど、他の IP インターフェイスが含まれます。
- **LDAPS**：外部認証用の LDAP サーバーを使用するなど、Cisco Secure Email and Web Manager と LDAP サーバー間の TLS トランザクションは、TLS バージョン 1.1 または 1.2 および FIPS 暗号スイートを使用します。LDAP サーバーが MD5 ハッシュを使用してパスワードを保存する場合、SMTP 認証クエリーは MD5 が FIPS 準拠でないため、失敗します。
- **ログ**：SSH2 は、SCP 経由のログのプッシュに許可された唯一のプロトコルです。FIPS 管理に関するエラーメッセージについては、INFO レベルの FIPS ログを確認してください。
- **SSL 暗号**：FIPS 準拠の SSL 暗号のみがサポートされます。

アプライアンスの FIPS モードへの切り替え

`fipsconfig` CLI コマンドを使用して、アプライアンスを FIPS モードに切り替えます。

（注） 管理者だけがこのコマンドを使用できます。アプライアンスを非 FIPS モードから FIPS モードに切り替えた後は、再起動が必要になります。

はじめる前に

アプライアンスに FIPS に準拠していないオブジェクトがないことを確認します。FIPS モードを有効にするには、すべての FIPS 非準拠オブジェクトを FIPS 要件を満たすように変更する必要があります。FIPS モードでの設定変更 （1 ページ）を参照してください。アプライアンスに FIPS 非準拠オブジェクトが含まれるかどうかを確認する手順については、FIPS モードのコンプライアンスの確認 （3 ページ）を参照してください。

手順

```
mail.example.com> fipsconfig
FIPS mode is currently disabled.
Choose the operation you want to perform:
- SETUP - Configure FIPS mode.
- FIPSCHECK - Check for FIPS mode compliance.
[]> setup

In FIPS mode, the RSA certificates must have 2048 bits or more key length, and the MD5
algorithm is deprecated.
It is not recommended to add WSA (in FIPS or non-FIPS mode) to an SMA in FIPS Mode.
```

```
It is not recommended to add ESA in non-FIPS mode to an SMA in FIPS Mode.
It is not recommended to move SMA to FIPS Mode when the connected ESA or WSA is in
non-FIPS mode.

To finalize FIPS mode, the appliance will reboot immediately. No commit will be required.
Are you sure you want to enable FIPS mode and reboot now ? [N]> y
Enter the number of seconds to wait before forcibly closing connections.
[30]>
System rebooting.  Please wait while the queue is being closed...
Closing CLI connection.
Rebooting the system...
```

FIPS モードのコンプライアンスの確認

`fipsconfig` コマンドを使用して、Cisco Secure Email and Web Manager に FIPS 非準拠オブジェクトが含まれているかどうかを確認します。

手順

```
mail.example.com> fipsconfig
FIPS mode is currently disabled.
Choose the operation you want to perform:
- SETUP - Configure FIPS mode.
- FIPSCHECK - Check for FIPS mode compliance.
[]> fipscheck
All objects in the current configuration are FIPS compliant.
FIPS mode is currently disabled.
```

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。