



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 \(1 ページ\)](#)
- [FIPS モードでの設定変更 \(1 ページ\)](#)
- [アプライアンスの FIPS モードへの切り替え \(2 ページ\)](#)
- [FIPS モードでの機密データの暗号化 \(3 ページ\)](#)
- [FIPS モードのコンプライアンスの確認 \(4 ページ\)](#)
- [証明書およびキーの管理 \(5 ページ\)](#)
- [DKIM 署名と検証のキーの管理 \(5 ページ\)](#)

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 E メールセキュリティアプライアンスは 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、E メールセキュリティアプライアンスが 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。

FIPS モードでの設定変更

E メールセキュリティアプライアンスは、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、E メールセキュリティアプライアンスはお使いの設定に次の変更を行いません。

- **SMTP の受信および配信。** E メールセキュリティ アプライアンス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。FIPS モードでは、`sslconfig` を使用して暗号スイートを変更できます。TLS v1 は FIPS モードでサポートされる TLS の唯一のバージョンです。
- **Web インターフェイス。** E メールセキュリティ アプライアンスの 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。FIPS モードでは、`sslconfig` を使用して暗号スイートを変更できます。
- **証明書。** FIPS モードは、アプライアンスに使用される証明書のタイプを制限します。証明書には、SHA-224、SHA-256、SHA-384、および SHA-512 のいずれかの署名アルゴリズム、ならびにサイズが 1,024、2,048、またはそれ以上のビットの RSA キーを使用する必要があります。アプライアンスは、これらのアルゴリズムのいずれも使用しない証明書はインポートしません。アプライアンスは非準拠の証明書を使用中の場合は FIPS モードにスイッチすることはできません。代わりにエラーメッセージ代わりに表示されます。詳細については、[証明書およびキーの管理 \(5 ページ\)](#) を参照してください。
- **DKIM 署名および検証。** DKIM 署名に使用される RSA キーの長さは 2,048 ビット、および検証に使用される RSA キーの長さは 1,024、1,536、2,048 ビットである必要があります。アプライアンスは非準拠の RSA キーを使用中の場合は FIPS モードにスイッチすることはできません。代わりにエラーメッセージ代わりに表示されます。DKIM 署名を検証する場合に署名が FIPS 準拠のキーを使用しないと、アプライアンスは永続的な障害を返します。[DKIM 署名と検証のキーの管理 \(5 ページ\)](#) を参照してください
- **LDAPS。** 外部認証用の LDAP サーバーを使用するなど、E メールセキュリティ アプライアンスと LDAP サーバー間の TLS トランザクションは TLS バージョン 1 および FIPS の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。
- **一元管理。** クラスタ化されたアプライアンスについては、FIPS モードはクラスタ レベルでしか有効にできません。
- **SSL 暗号化。** FIPS モードでは、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、キー サイズが 512 ビットの DKIM 検証プロファイルなど、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 \(4 ページ\)](#) 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.
- ENCRYPTCONFIG - Configure encryption of sensitive data in the appliance.
[ ]> setup

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]> yes

Do you want to minimize FIPS restriction on SMTP DANE in the email gateway ? [N]> no

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 モードでの機密データの暗号化

fipsconfig > encryptconfig サブコマンドを使用して、パスワードやキーなど、アプライアンスの機密データを暗号化します。このオプションを有効にすると、

- アプライアンスの次の重要なセキュリティパラメータが暗号化されて保存されます。
 - 証明書の秘密キー
 - RADIUS パスワード
 - LDAP バインドのパスワード
 - ローカル ユーザのパスワードのハッシュ
 - SNMP パスワード
 - DK/DKIM 署名キー
 - 発信 SMTP 認証パスワード
 - PostX 暗号化キー
 - PostX 暗号化プロキシパスワード
 - FTP プッシュ ログ サブスクリプションのパスワード
 - IPMI LAN パスワード

- アップデータ サーバの URL



(注) 管理者を含むすべてのユーザーは、設定ファイルの機密情報を表示できません。

- アプライアンスのスワップ領域は、アプライアンスの物理的なセキュリティが侵害された場合の不正アクセスや調査攻撃を防ぐために暗号化されます。

手順

```
mail1.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.
- ENCRYPTCONFIG - Configure encryption of sensitive data in the appliance.
[]> encryptconfig

Do you want to enable encryption of sensitive data in the appliance? [Y]> yes

Encryption is in enable state.
mail1.example.com>
```

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、アプライアンスに 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.
- ENCRYPTCONFIG - Configure encryption of sensitive data in the appliance
[]> fipscheck

Currently, there are non-FIPS-compliant objects configured.

List of non FIPS compliant DKIM Verification Profiles:
-----
Profile Name          Key Size
-----
1.          DEFAULT          512

To be FIPS compliant, you must modify the above listed objects to meet FIPS requirements.
For more information, see the
FIPS Management chapter in the Cisco AsyncOS Email User Guide.

FIPS mode is currently disabled.
```

証明書およびキーの管理

AsyncOS では、証明書と秘密キーのペアを使用してアプライアンスと外部のマシン間の通信を暗号化することができます。既存の証明書とキーのペアをアップロードしたり、自己署名証明書を生成したり、または Certificate Signing Request (CSR; 証明書署名要求) を生成して認証局に送信し、公開証明書を取得したりできます。認証局は秘密キーによって署名された信頼できる公開証明書を戻し、それをアプライアンスにアップロードできます。

アプライアンスが FIPS モードの場合は、次に進むことができます。

アプライアンス側 FIPS モードは、アプライアンスが FIPS に準拠するためにアプライアンスが使用する証明書に一定の制限を追加します。証明書は、次のいずれかのシグニチャアルゴリズムを使用する必要があります: SHA-1、SHA-224、SHA-256、SHA-384、および SHA-512。

アプライアンスは、これらのアルゴリズムのいずれも使用しない証明書はインポートしません。また、リスナーで使用中の非準拠の証明書が存在する場合、FIPS モードにスイッチすることもできません。代わりにエラーメッセージ代わりに表示されます。

証明書の非 FIPS 状態はアプライアンスが FIPS モードであるときに CLI と GUI の両方に表示されます。リスナーまたは送信先コントロールなどの機能に対して使用する証明書を選択するときに、アプライアンスはオプションとして非準拠の証明書を表示しません。

アプライアンスにおける証明書の使用の詳細については、[証明書の使用](#)を参照してください。

次のいずれかのサービスで FIPS 準拠の証明書を使用できます。

- **SMTPの受信および配信。** TLS を使用して暗号化を必要とするすべてのリスナーに証明書を割り当てるには、[ネットワーク (Network)] > [リスナー (Listeners)] ページ (または listenerconfig -> edit -> certificate CLI コマンド) を使用します。インターネットに対するリスナーの TLS のみをイネーブルにするか (公開リスナー)、または内部システムを含むすべてのリスナーの暗号化をイネーブルにする (プライベートリスナー) ことができます。
- **宛先制御。** 電子メール配信のすべての発信 TLS 接続にグローバル設定として証明書を割り当てるには、[メールポリシー (Mail Policies)] > [送信先コントロール (Destination Controls)] ページ (または destconfig CLI コマンド) を使用します。
- **インターフェイス。** 管理インターフェイスが含まれるインターフェイスで HTTPS サービスの証明書をイネーブルにするには、[ネットワーク (Network)] > [IP インターフェイス (IP Interfaces)] ページ (または interfaceconfig CLI コマンド) を使用します。
- **LDAP。** TLS 接続が必要なすべての LDAP トラフィックに証明書を割り当てるには、[システム管理 (System Administration)] > [LDAP] ページを使用します。このアプライアンスでは、ユーザーの外部認証の LDAP を使用することもできます。

DKIM 署名と検証のキーの管理

E メールセキュリティアプライアンスでの DomainKeys および DKIM の動作の概要については、[電子メール認証](#)を参照してください。

関連項目

- [DKIM 署名 \(6 ページ\)](#)
- [DKIM 検証 \(6 ページ\)](#)

DKIM 署名

DKIM 署名キーの作成時に、キー サイズを指定します。FIPS モードの E メールセキュリティ アプライアンスでは、2,048 ビットのキーサイズのみがサポートされます。キーサイズが大きいほどセキュリティが向上しますが、パフォーマンスに影響する可能性があります。

アプライアンスは非準拠の RSA キーを使用中の場合は FIPS モードにスイッチすることはできません。代わりにエラー メッセージ代わりに表示されます。

FIPS 準拠の署名キーはドメインプロファイルで利用可能です。これは [メールポリシー (Mail Policies)] > [ドメインプロファイル (Domain Profiles)] ページを使用してドメインプロファイルを作成または編集するときに、[署名キー (Signing Key)] のリストに表示されます。署名キーをドメインプロファイルに関連付けると、公開キーが含まれる DNS テキストレコードを作成できます。これは、ドメインプロファイルのリストの [DNS テキストレコード (DNS Text Record)] カラムの [生成 (Generate)] リンクから (または CLI の `domainkeysconfig -> profiles -> dnstxt` から) 実行します。

DKIM 検証

アプライアンスは、メッセージが DKIM 署名を検証する際に FIPS 準拠キーを使用する必要があります。シグニチャが FIPS 準拠のキーを使用しない場合、アプライアンスは永続的な障害を返します。

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。