FIPS 140-2 モードの設定

この章では、FIPS 140-2 モードの設定について説明します。

FIPS 140-2 の設定

⚠

注意 FIPS モードは、FIPS 準拠のリリースだけでサポートされます。Unified Communications Managerの FIPS 非準拠のバージョンにアップグレードする前に、必ず FIPS モードを無効にしてください。

FIPS 準拠のリリースと、そのリリースの証明書を確認するには、https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html の *FIPS 140* のドキュメントを参照してください。

連邦情報処理標準（FIPS）は、米国およびカナダ政府の認証規格です。暗号化モジュールで順守する必要がある要件が規定されています。

Unified Communications Manager の特定のバージョンは、米国の National Institute of Standards（NIST）に従って FIPS 140-2 に準拠しています。これらは FIPS モード、レベル 1 に準拠して動作できます。

Unified Communications Manager

- 再起動
- スタートアップ時に認定のセルフテストを実行する
- 暗号モジュールの整合性チェックを実行する
- キー情報を再生成する

FIPS 140-2 モードを有効にすると、この時点で、Unified Communications Manager は FIPS 140-2 モードで動作しています。

FIPS の要件には、次のものが含まれます。

- スタートアップ時のセルフテストの実行
- 一連の承認済み暗号機能に対する制限

FIPS モードでは、次の FIPS 140-2 レベル 1 検証済み暗号化モジュールが使用されます。

- CiscoSSL 1.0.2n.6.2.194 with FIPS Module CiscoSSL FOM 6_2_0
- CiscoJ 5.2.1
- RSA CryptoJ 6_2_3
- Openssh 7.5.9
- Libreswan
- NSS

次の FIPS 関連作業を実行できます。

- FIPS 140-2 モードの有効化
- FIPS 140-2 モードの無効化
- FIPS 140-2 モードのステータスの確認

（注）
- デフォルトでは、システムは非FIPSモードになっているため、有効にする必要があります。
- クラスタ上で FIPS、コモンクライテリア、または強化されたセキュリティモードにアップグレードする前に、セキュリティパスワードの長さが最小 14 文字である必要があります。旧バージョンが FIPS を有効にしていた場合でもパスワードを更新します。

FIPSモードで自己署名証明書または証明書署名要求（CSR）を生成する場合は、SHA256ハッシュアルゴリズムを使用して証明書を暗号化する必要があり、SHA1 を選択できません。

IPsec の要件

このリリースでは、Libreswan ライブラリサポートは、IPsec の Openswan ライブラリのサポートに置き換えられています。このサポートには、既存の機能に対する変更はありません。

証明書ベースの認証を Libreswan ライブラリで機能させるには、送信元と宛先の両方の証明書が CA 署名付き証明書である必要があります。さらに、同じ認証局 (CA) がこれらの証明書に署名する必要があります。Libreswan ライブラリへの移行には、次の制限事項があります。

- 自己署名証明書を使用した証明書ベースの認証を使用してIPsecが設定されているユニファイドコミュニケーションマネージャをアップグレードすると、アップグレードは失敗します。アップグレードを正常に実行するには、CA 署名付き証明書を使用して IPsec ポリシーを再設定します。

- 証明書ベースの認証を使用しており、IPsecを設定するために自己署名証明書を使用している場合、IPsec は動作を停止します。
- 証明書ベースの認証を使用しており、IPsec を設定するための送信元と宛先に対して異なる CA で署名された CA 署名付き証明書を使用している場合、IPsec は動作を停止します。
- Unified Communications Manager では、DH グループ キー値が 1、2、または 5 の IPsec ポリシーは無効になっています。ただし、DH グループキー値 1、2、または 5 を使用して IPSec ポリシーを設定し、FIPS モードが有効になっている場合は、ユニファイド コミュニケーション マネージャへのアップグレードがブロックされます。

FIPS 140-2 モードの有効化

Unified Communications Managerで FIPS 140-2 モードを有効にする前に、次の点を検討してください。

- 非 FIPS モードから FIPS モードに切り替えた場合は、MD5 および DES プロトコルは機能しません。
- 単一サーバクラスタでは、証明書が再生成されるため、FIPS モードを有効にする前に、CTL クライアントを実行するか、または [Prepare Cluster for Rollback to pre-8.0] エンタープライズ パラメータを適用する必要があります。これらの手順のいずれかを実行しない場合は、FIPS モードを有効にした後に手動で ITL ファイルを削除する必要があります。
- クラスタでは、すべてのノードが FIPS モードまたは非 FIPS モードである必要があります。異なるモードの各ノードは許可されません。たとえば、FIPS モードのノード A と非 FIPS モードのノード B は許可されません。
- FIPS モードをサーバで有効にした後は、サーバがリブートし、電話が正常に再登録されるまで待機してから、次のサーバで FIPS を有効にしてください。

注意 FIPS モードを有効にする前に、システム バックアップを実行することを強く推奨します。FIPS のチェックが起動時に失敗した場合は、システムが停止し、復元するにはリカバリ CD が必要になります。

手順

Step 1 CLI セッションを開始します。

詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』の「「CLI セッションの開始」」セクションを参照してください。

Step 2 CLI で **utils fips enable** を入力します。

14 文字未満のパスワードを入力すると、次のプロンプトが表示されます。

```
FIPS、コモンクライテリア、強化されたセキュリティモードなどのセキュリティモードを有効にするには、クラスタセキュリティパスワードは 14 文字以上使用する必要があります。すべてのノードで「set password user security」CLI コマンドを使用してクラスタ セキュリティ パスワードを更新し、このコマンドを再試行します。
**************************************************************************
 コマンドの実行に失敗しました（Executed command unsuccessfully）
```

14 文字を超えるパスワードを入力すると、次のプロンプトが表示されます。

```
セキュリティ警告：この操作により、1)CallManager 2)Tomcat 3)IPsec 4)TVS 5)CAPF 6)SSH 7)ITLRecovery の証明書が再生成されます。上記のコンポーネント用にアップロードされたサードパーティの CA 署名付き証明書を再アップロードする必要があります。（The operation will regenerate certificates for 1)CallManager 2)Tomcat 3)IPsec 4)TVS 5)CAPF 6)SSH 7)ITLRecovery Any third party CA signed certificates that have been uploaded for the above components will need to be re-uploaded.）システムが混合モードで動作している場合は、ctl ファイルを更新するために CTL クライアントを再実行する必要があります。クラスタ内に他のサーバがある場合は、このノードの FIPS 操作が完了してシステムがバックアップおよび実行されるまで待機して、他のノードの FIPS 設定を変更しないでください。エンタープライズパラメータの [TFTP ファイル署名アルゴリズム（TFTP File Signature Algorithm）] に Unified Communications Manager の現行バージョンの FIPS 準拠ではない値 [SHA-1] が設定されている場合は、完全に FIPS にするために、パラメータ値を SHA-512 に変更することを推奨します。SHA-512 を署名アルゴリズムとして設定するには、クラスタにプロビジョニングされているすべての電話機が SHA-512 署名付き設定ファイルを検証できる必要がある場合があります。そうでない場合、電話機の登録が失敗する可能性があります。詳細については、『Cisco Unified Communications Manager Security Guide』を参照してください。これにより、システムが FIPS モードに変更され、再起動します。
********************************************************************************
警告：続行したら、Ctrl+C キーを押さないでください。開始後にこの操作をキャンセルすると、システムは一貫性のない状態になります。リカバリするには、システムをリーブートし、「utils fips status」を実行する必要があります。（Once you continue do not press Ctrl+C. Canceling this operation after it starts will leave the system in an inconsistent state; rebooting the system and running "utils fips status" will be required to recover.）
********************************************************************************
Do you want to continue (yes/no)?
```

Step 3 **Yes** と入力します。

次のメッセージが表示されます。

```
証明書を生成しています...オペレーティングシステムで FIPS モードを設定しています。FIPS mode enabled successfully. システムのバックアップが実行されると、システムを再起動した後に、これを強くお勧めします。システムは数分で再起動します。
```

Unified Communications Manager が自動的にリブートされます。

（注）
- 証明書および SSH キーは、FIPS 要件に応じて、自動的に再生成されます。
- 単一のサーバ クラスタを使用しており、[Prepare Cluster for Rolback to pre 8.0] エンタープライズ パラメータを適用してから FIPS 140-2 モードを有効にした場合は、すべての電話がサーバに正常に登録されたことを確認してから、このエンタープライズ パラメータを無効にする必要があります。

（注） FIPS モードでは、Unified Communications Manager は Racoon 検証済み（非 FIPS 検証）の代わりに、Libreswan（FIPS 検証済）を使用します。Raccoon のセキュリティポリシーに、FIPS で承認されていない機能が含まれている場合、CLI コマンドは、FIPS で承認された機能を使用してセキュリティポリシーを定義し直すよう表示して中止されます。詳細については、Cisco Unified Communications Manager アドミニストレーション ガイドの「IPsec の管理」に関連するトピックを参照してください。

FIPS 140-2 モードの無効化

FIPS 140-2 モードを Unified Communications Manager で無効にする前に、次の点を考慮してください。

- 単一または複数のサーバクラスタでは、CTL クライアントを実行することを推奨します。CTL クライアントが単一のサーバクラスタで実行されていない場合は、FIPS モードを無効にした後で、手動で ITL ファイルを削除する必要があります。
- 複数サーバのクラスタでは、各サーバを個別に無効にする必要があります。これは、FIPS モードはクラスタ全体ではなくサーバごとに無効になるためです。

FIPS 140-2 モードを無効にするには、次の手順を実行します。

手順

Step 1 CLI セッションを開始します。

詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』の「Starting a CLI Session」の項を参照してください。

Step 2 CLI で、**utils fips disable** と入力します。

Unified Communications Manager がリブートされ、非 FIPS モードに戻ります。

（注） 証明書と SSH キーは自動的に再生成されます。

FIPS 140-2 モードのステータス確認

FIPS 140-2 モードが有効になっているかどうかを確認するには、CLI からモードステータスを確認します。

FIPS 140-2 モードのステータスを確認するには、次の手順を実行します。

手順

Step 1 CLI セッションを開始します。

詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』の「Starting a CLI Session」の項を参照してください。

Step 2 CLI に **utils fips status** と入力します。

FIPS 140-2 モードが有効になっていることを確認するために、次のメッセージが表示されます。

```
admin: システムが FIPS モードで動作している状態の fips ステータス。自己診断テストのステータス:-S T A R T----------------------FIPS selftests ランの実行時間が N 3 の開始時刻: Thu Apr 28 15:59:24 PDT 2011 NSS の自己診断テストが成功しました。カーネル暗号テストに合格しました。オペレーティングシステムの OpenSSL 自己診断テストに合格しました。Libreswan 自己診断テストに合格しました。OpenSSL の自己診断テストに合格しました。CryptoJ 自己診断テストに合格しました...
```

FIPS 140-2 モードサーバのリブート

FIPS 140-2 モードで Unified Communications Manager サーバがリブートすると、リブート後に各 FIPS 140-2 モジュールで FIPS のスタートアップ時のセルフテストがトリガーされます。

注意 これらのセルフテストのいずれかが失敗すると、Unified Communications Managerサーバが停止します。

（注） 対応する CLI コマンドを使用して FIPS を有効または無効にすると、Unified Communications Manager サーバが自動的に再起動されます。リブートを開始することもできます。

注意 一時的なエラーによってスタートアップセルフテストに失敗した場合は、 Unified Communications Managerサーバの再起動によって問題が修正されます。ただし、起動時のセルフテスト エラーが解消されない場合は、FIPS モジュールに重大な問題があるため、リカバリ CD の使用が唯一の選択肢となります。

強化されたセキュリティ モード

強化されたセキュリティモードはFIPS対応システムで稼働します。強化されたセキュリティモードで動作するために、Unified Communications Manager と IM and Presence Service の両方を有効にすることで、次のセキュリティとリスク管理制御を備えるシステムを有効にすることができます。

- ユーザのパスワードとパスワードの変更に関して厳格化されたクレデンシャル ポリシーが適用されます。
- デフォルトでは、連絡先検索の認証機能が有効です。
- リモート監査ログ用のプロトコルが TCP または UDP に設定されている場合は、デフォルトのプロトコルがTCPに変更されます。リモート監査ログのプロトコルがTLSに設定されている場合、デフォルトのプロトコルは TLS のままです。コモン クライテリア モードでは、厳密なホスト名検証が使用されます。そのため、サーバには、証明書と一致する完全修飾ドメイン名（FQDN）を設定する必要があります。

Unified Communications Managerが FIPS モードの場合、バックアップデバイスとして設定するデバイスはFIPS 準拠である必要があります。キー交換アルゴリズム**diffie-hellman-group1-sha1**はFIPSモードではサポートされていません。非 FIPS モードのUnified Communications Manager で **diffie-hellman-group1-sha1** アルゴリズムを設定すると、FIPS モードを有効にすると、このアルゴリズムは SSH キー交換から自動的に削除されます。

クレデンシャル ポリシーの更新

強化されたセキュリティモードを有効にすると、新しいユーザパスワードとパスワード変更に関してより厳格なクレデンシャルポリシーが有効になります。強化されたセキュリティモードを有効にした後で、管理者は一連の CLI コマンド **set password ***** を使用して、次の要件のいずれかを変更できます。

- パスワードの長さは 14 ～ 127 文字です。
- パスワードには少なくとも 1 つの小文字、1 つの大文字、1 つの数字 および 1 つの特殊文字が含まれている必要があります。
- 過去 24 回以内に使用したパスワードを再使用することはできません。
- パスワードの最短有効期間は 1 日、最長有効期間は 60 日です。
- 新たに生成されるパスワードの文字列では、古いパスワードの文字列と少なくとも 4 文字が異なる必要があります。

強化されたセキュリティ モードの設定

強化されたセキュリティ モードを有効にする前に、FIPS を有効にしてください。

すべての Unified Communications Manager または IM and Presence Service クラスタノードでこの手順を使用して、強化されたセキュリティモードを設定します。

（注） 拡張セキュリティモードを有効にした後で、Unified Communications Manager パブリッシャのパスワードを変更する場合は、IM and Presence Service パブリッシャのサービスが「STARTED」状態（「Cisco IM and Presence Data Monitor」サービスおよび SyncAgent）であることを確認する必要があります。

手順

Step 1 コマンドライン インターフェイスにログインします。

Step 2 **utils EnhancedSecurityMode status** コマンドを実行し、強化されたセキュリティモードが有効であるかどうかを確認します。

Step 3 Unified Communications Manager クラスタノードで次のいずれかのコマンドを実行します。

- 強化されたセキュリティ モードを有効にするには、**utils EnhancedSecurityMode enable** コマンドを実行します。
- 強化されたセキュリティ モードを無効にするには、**utils EnhancedSecurityMode disable** コマンドを実行します。

Step 4 拡張セキュリティモードを有効にした後、Cisco Unified CM の管理ユーザインターフェイスで、14 文字を含む新しいパスワードに変更します。

Unified Communications Manager パブリッシャで拡張セキュリティモードを有効にした後、次の手順を実行します。

1. Unified Communications Manager サブスクライバで拡張セキュリティモードを有効にします。
2. IM and Presence Service パブリッシャで拡張セキュリティモードを有効にします。
3. IM and Presence Service サブスクライバで拡張セキュリティモードを有効にします。

（注） **utils EnhancedSecurityMode enable** CLI コマンドまたは **utils EnhancedSecurityMode disable** CLI コマンドをすべてのノードで同時に実行しないでください。

コモン クライテリア モード

コモンクライテリアモードでは、Unified Communications Manager と IM and Presence Service サービスの両方がコモンクライテリアのガイドラインに準拠できます。コモンクライテリアモードは、各クラスタ ノードで次に示す CLI コマンドを使用して設定できます。

- ユーティリティ `fips_common_criteria` 有効
- ユーティリティ `fips_common_criteria disable`
- ユーティリティ `fips_common_criteria` ステータス

コモン クライテリア構成のタスク フロー

- 一般的な基準モードを有効にするには、FIPS モードが実行されている必要があります。FIPS がまだ有効になっていない場合、コモンクライテリアモードを有効にしようとすると FIPS を有効にするよう求められます。FIPS を有効にすると、証明書を再生成する必要があります。詳細については、FIPS 140-2 モードの有効化 （3 ページ）を参照してください。
- コモンクライテリアモードでは、証明書ベースの IPSec ポリシーの IPSec ポリシーを設定する前に、クラスタおよびノード間で証明書交換操作が必須です。
- X.509 v3 証明書は、共通基準モードで必要です。X.509 v3 証明書は、次の通信プロトコルとして TLS 1.2 を使用する場合にセキュアな接続を有効にします。
  - リモート監査ログ
  - FileBeat クライアントと logstash サーバ間の接続を確立しています。

Unified Communications Manager と IM and Presence Service をコモンクライテリアモードに設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
Step 1	TLSの有効化 （9 ページ）	TLS は、共通基準モードを設定するための前提条件です。
Step 2	コモン クライテリア モードの構成 （10 ページ）	Unified Communications Manager と IM and Presence Service のすべてのクラスタノードでコモンクライテリアモードを設定します。

TLSの有効化

TLS 1.2 バージョンまたは TLS バージョン1.1 は、共通基準モードの要件です。TLS バージョン1.0 を使用したセキュア接続は、共通基準モードを有効にした後は許可されません。

- TLS 接続の確立中に、ピア証明書の`Extendedkeyusage`拡張機能が適切な値についてチェックされます。
  - ピアがサーバの場合、ピア証明書には、 `Extendedkeyusage`拡張機能として`serverauth`が必要です。
  - ピアがクライアントである場合、ピア証明書には、 `Extendedkeyusage`拡張として`clientauth`が必要です。

`Extendedkeyusage`拡張がピア証明書に存在しない場合、または正しく設定されていない場合は、接続が閉じられます。

TLS バージョン 1.2 をサポートするには、次の手順を実行します。

手順

Step 1 Soap UI バージョン5.2.1 をインストールします。

Step 2 Microsoft Windows プラットフォームで実行している場合は、次のようにします。

a) `C:\Program Files\SmartBear\SoapUI-5.2.1\bin`に移動します。

b) `] Vmoptions]`ファイルを編集して、追加`-dsoapui. https. プロトコル = tlsv 1.2、TLSv1、SSLv3`を編集し、ファイルを保存します。

Step 3 Linux で実行している場合は、`bin/soaup. sh`ファイルを編集して`JAVA_OPTS = "$JAVA _OPTS-dsoapui. https. プロトコル = SSLv3, tlsv 1.2"`を追加し、ファイルを保存します。

Step 4 OSX を実行している場合は、次のようになります。

a) [アプリケーション (applications)]/[コンテンツ `(Contents)`] に移動します。

b) `] Vmoptions]`を編集して、追加`-dsoapui. https. プロトコル = tlsv 1.2、TLSv1、SSLv3`を編集し、ファイルを保存します。

Step 5 SoapUI ツールを再起動し、AXL テストを続行します。

コモン クライテリア モードの構成

Unified Communications Manager と IM and Presence Service サービスのコモンクライテリアモードを設定するには、次の手順を使用します。

手順

Step 1 コマンドライン インターフェイス プロンプトにログインします。

Step 2 `utils fips_common_criteria status` コマンドを実行し、システムがコモンクライテリアモードで実行されているかどうかを確認します。

Step 3 クラスタ ノードで次のいずれかのコマンドを実行します。

- 共通基準モードを有効にするには、[コマンドユーティリティ `(enable)`] fips_common_criteria 実行します。
- 共通基準モードを無効にするには、[コマンドユーティリティ `(disable)`] fips_common_criteria 実行します。

  共通基準モードが無効になっている場合は、最小 TLS バージョンを設定するためのプロンプトが表示されます。

（注） これらのコマンドをすべてのノードで同時に実行しないでください。

Step 4 単一のクラスタ全体でコモンクライテリアモードを有効にするには、すべてのUnified Communications Manager および IM and Presence Service クラスタノードでこの手順を繰り返します。

（注）
- CTL クライアントは TLS 1.1 プロトコルと TLS 1.2 プロトコルをサポートしていないので、サーバがコモンクライテリアモードである場合、CTL クライアントはUnified Communications Managerノードに接続しません。
- 一般的な基準モードでは、TLS 1.1 または TLS 1.2 (DX シリーズおよび 88 XX シリーズの電話機など) をサポートする電話機モデルのみがサポートされています。7975や9971などの TLSv 1.0 のみをサポートする電話機モデルは、共通基準モードではサポートされていません。
- CTL クライアントを使用する際に一時的に TLS 1.0 を許可し、クラスタをコモン クライテリア モードに移します。最小 TLS を 1.1 または 1.2 に設定します。
- コモン クライテリア モードで CLI コマンド **utils ctl set-cluster mixed-mode** を使用することにより、Tokenless CTL に移行します。最小 TLS を 1.1 または 1.2 に設定します。

Step 5 ノード間で ICSA がすでに設定されているマルチクラスタ設定で共通基準モードを有効にするには、次の順序で各ノードの共通基準モードを有効にします。

1. Unified Communications Manager - クラスタ 1（パブリッシャ）
2. IM and Presence Service - クラスタ 1（パブリッシャ）
3. IM and Presence Service - クラスタ 1（1 つ以上のサブスクライバ）
4. Unified Communications Manager - クラスタ 2（パブリッシャ）
5. IM and Presence Service - クラスタ 2（パブリッシャ）
6. IM and Presence Service - クラスタ 2（1 つ以上のサブスクライバ）

Step 6 証明書の同期に失敗した場合は、次を参照してください。

CiscoSSH サポート

Unified Communications Manager は CiscoSSH をサポートします。システムで FIPS モードを有効にすると、CiscoSSH は自動的に有効になります。追加設定は不要です。

CiscoSSH サポート

CiscoSSH は、次のキー交換アルゴリズムをサポートします。

- **Diffie-Hellman-Group14-SHA1**
- **Diffie-Hellman-Group-Exchange-SHA256**

- **Diffie-Hellman-Group-Exchange-SHA1**

CiscoSSH は、Unified Communications Manager サーバで次の暗号をサポートしています。

- **AES-128-CTR**
- **AES-192-CTR**
- **AES-256-CTR**
- **AES-128-GCM@openssh.com**
- **AES-256-GCM@openssh.com**
- **AES-128-CBC**（リリース 12.0(1) 以降をサポート）
- **AES-192-CBC**（リリース 12.0(1) 以降をサポート）
- **AES-256-CBC**（リリース 12.0(1) 以降をサポート）

CiscoSSH は、クライアントの次の暗号方式をサポートします。

- **AES-128-CTR**
- **AES-192-CTR**
- **AES-256-CTR**
- **AES-128-GCM@openssh.com**
- **AES-256-GCM@openssh.com**
- **AES-128-CBC**
- **AES-192-CBC**
- **AES-256-CBC**

FIPS モードの制約事項

機能	機能制限
SNMP v3	FIPS モードでは、MD5 または DES を使用した SNMP v3 はサポートされていません。FIPS モードが有効になっているときに SNMP v3 が設定されている場合は、認証プロトコルとして**SHA**を設定し、プライバシープロトコルとして**AES128**を設定する必要があります。
証明書のリモート登録	FIPS モードでは、証明書のリモート登録はサポートされていません。

機能	機能制限
SFTP サーバ	デフォルトでは、JSCH ライブラリは SFIPS 接続に ssh-rsa を使用していましたが、FIPS モードは ssh-rsa をサポートしません。CentOS の最近の更新により、JSCH ライブラリは、変更後の FIPS 値に応じて 、**ssh-rsa**（SHA1withRSA）または **rsa-sha2-256**（SHA256withRSA）の両方をサポートします。具体的には、次の選択を行います。 （注） • FIPS モードは **rsa-sha2-256** のみをサポートします。 • 非 FIPS モードは、ssh-rsa と **rsa-sha2-256** の両方をサポートします。 **rsa-sha2-256**（SHA256WithRSA）のサポートは OpenSSH 6.8 バージョン以降でのみ利用可能です。FIPS モードでは、OpenSSH 6.8 バージョン以降で実行されている SFIPS サーバだけが **rsa-sha2-256**（SHA256WithRSA）をサポートします。