CHAPTER 5

Cisco Unity Connection での FIPS 準拠

Cisco Unity Connection 9.x は、FIPS モードをサポートしています。FIPS モードは、連邦情報処理標準 140-2（FIPS）要件に準拠しています。

Cisco Unified Communications Manager Business Edition（CMBE）では、FIPS モードはサポートされていません。管理者に対して **utils fips <option>** コマンドライン インターフェイス（CLI）コマンドが表示されますが、これは機能しません。

次の場合に、Connection の FIPS モードをイネーブルにすることを推奨します。

- Cisco Unity Connection 9.x の新規インストールを実行し、FIPS モードを使用する場合は、Connection サーバの設定とテレフォニー統合の追加を行う前に FIPS をイネーブルにする必要があります。
- Cisco Unity Connection 9.x へのアップグレードを実行する場合は、既存のテレフォニー統合を使用する前に、証明書を手順に従って再生成してください。証明書を再生成する方法については、「FIPS の証明書の再生成」の項を参照してください。

次の項を参照してください。

FIPS の CLI コマンドの実行

Cisco Unity Connection で FIPS 機能をイネーブルにするには、**utils fips enable** CLI コマンドを使用します。また、次の CLI コマンドも使用できます。

- **utils fips disable**：FIPS 機能をディセーブルにします。

- **utils fips status**：FIPS コンプライアンスのステータスをチェックします。

utils fips <option> CLI コマンドの詳細については、該当する『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』を参照してください。このガイドは、http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html から入手可能です。

注意　FIPS モードをイネーブル化またはディセーブル化した後、Cisco Unity Connection サーバが自動的に再起動します。

注意　Cisco Unity Connection サーバがクラスタ内にある場合は、現在のノード上で FIPS の操作が完了し、システムが再起動して稼働するまで、他のすべてのノード上の FIPS 設定を変更しないでください。

FIPS の証明書の再生成

既存のテレフォニー統合を備えた Cisco Unity Connection サーバの場合は、FIPS モードをイネーブル化またはディセーブル化した後に手動で再生成されたルート証明書を持っている必要があります。テレフォニー統合が Authenticated モードまたは Encrypted Security モードを使用する場合は、対応するすべての Cisco Unified Communications Manager サーバに、再生成されたルート証明書を再アップロードする必要があります。新規インストールの場合は、テレフォニー統合を追加する前に FIPS モードをイネーブルにすると、ルート証明書の再生成を回避できます。

FIPS モードをイネーブルまたはディセーブルにするたびに、次の手順を実行します。

（注）　クラスタの場合は、すべてのノード上で次の手順を実行します。

1. Cisco Unity Connection の管理にログインします。
2. [テレフォニー統合（Telephony Integrations）] > [セキュリティ（Security）] > [ルート証明書（Root Certificate）] を選択します。
3. [ルート証明書の表示（View Root Certificate）] ページで [新規作成（Generate New）] をクリックします。
4. テレフォニー統合が Authenticated モードまたは Encrypted Security モードを使用する場合は、ステップ 5 ～ 10 を実行してください。そうでない場合は、ステップ 12 へ進んでください。
5. [ルート証明書の表示（View Root Certificate）] ページで [右クリックして証明書をファイルとして保存（Right-Click to Save the Certificate as a File）] リンクを右クリックします。
6. [名前を付けて保存（Save As）] を選択して Cisco Unity Connection ルート証明書を保存する場所を参照し、.pem ファイルとして保存します。

注意　証明書は、拡張子 .pem（.htm ではなく）のファイルとして保存する必要があります。そうしないと、Cisco Unified CM で証明書が認識されません。

7. 次のサブステップを実行して、Cisco Unity Connection ルート証明書をすべての Cisco Unified CM サーバにコピーします。
   a. Cisco Unified CM サーバで Cisco Unified オペレーティング システムの管理にサインインします。

b. [セキュリティ（Security）] メニューから [証明書の管理（Certificate Management）] オプションを選択します。

c. [証明書の一覧（Certificate List）] ページで [証明書/証明書チェーンのアップロード（Upload Certificate/Certificate Chain）] を選択します。

d. [証明書/証明書チェーンのアップロード（Upload Certificate/Certificate Chain）] ページで、[証明書の名前（Certificate Name）] ドロップダウンから [CallManager-trust] を選択します。

e. [ルート証明書（Root Certificate）] フィールドに Cisco Unity Connection ルート証明書を入力します。

f. [ファイルのアップロード（Upload File）] フィールドで [参照（Browse）] をクリックし、ステップ 5 で保存した Cisco Unity Connection ルート証明書を見つけて選択します。

g. [ファイルのアップロード（Upload File）] をクリックします。

h. [閉じる（Close）] をクリックします。

8. Cisco Unified CM サーバで Cisco Unified Serviceability にサインインします。
9. [ツール（Tools）] メニューから [サービス管理（Service Management）] を選択します。
10. [コントロール センター - 機能サービス（Control Center - Feature Services）] ページで、Cisco CallManager サービスを再起動します。
11. Cisco Unified CM クラスタ内にある残りのすべての Cisco Unified CM サーバ上で、ステップ 5 ～ 10 を繰り返します。
12. 次の手順に従って、Connection Conversation Manager Service を再起動します。

a. Cisco Unity Connection Serviceability にログインします。

b. [ツール（Tools）] メニューから [サービス管理（Service Management）] を選択します。

c. [重要なサービス（Critical Services）] セクションで [停止（Stop）] を選択して Connection Conversation Manager サービスを停止します。

d. [ステータス（Status）] エリアに、Connection Conversation Manager サービスが正常に停止されたというメッセージが表示されたら、そのサービスの [スタート（Start）] を選択します。

13. 新規および既存のテレフォニー統合のポートが Cisco Unified CM に正常に登録されます。

FIPS は、Cisco Unified Communications Manager と Cisco Unity Connection の間の SCCP 統合および SIP 統合の両方でサポートされています。

証明書の管理の詳細については、『*Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection*』の「Security」の章の「Manage Certificates and Certificate Trust Lists」の項を参照してください。このガイドは、http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/os_administration/guide/9xcucosag060.html#wp1053189 から入手可能です。

FIPS モード使用時の追加設定

FIPS コンプライアンスを維持するためには、次の機能への追加設定が必須です。

- ネットワーキング：サイト内、サイト間、VPIM
- ユニファイド メッセージング：ユニファイド メッセージング サービス

次の項を参照してください。

- 「FIPS モード使用時のネットワーキングの設定」（P.5-4）
- 「FIPS モード使用時のユニファイド メッセージングの設定」（P.5-4）

FIPS モード使用時のネットワーキングの設定

Cisco Unity Connection から別のサーバへのネットワーキングは、IPsec ポリシーによって保護される必要があります。これには、サイト間リンク、サイト内リンク、および VPIM ロケーションが含まれます。リモート サーバには、独自の FIPS コンプライアンスを保証する責任があります。

（注） セキュア メッセージは、IPsec ポリシーが設定されない限り FIPS 準拠の方法では送信されません。

FIPS モード使用時のユニファイド メッセージングの設定

ユニファイド メッセージング サービスには、次の設定が必要です。

- Cisco Unity Connection と Microsoft Exchange または Cisco Unified MeetingPlace の間に IPsec ポリシーを設定します
- [Connection 管理（Connection Administration）] の [ユニファイド メッセージング サービスの編集（Edit Unified Messaging Service）] ページにある [Web ベース認証モード（Web-Based Authentication Mode）] を [基本認証（Basic）] に設定します。

注意 サーバ間の IPsec ポリシーは、基本 Web 認証のプレーン テキストの形式を保護するために必要です。

FIPS モード使用時の IPsec ポリシーの設定

IPsec ポリシーの設定については、『*Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection*』の「Security」の章の「IPSEC Management」の項を参照してください。このガイドは、http://www.cisco.com/en/US/docs/voice_ip_comm/connection/9x/os_administration/guide/9xcucosagx.html から入手可能です。

Microsoft Exchange サーバの IPsec ポリシーの設定については、Microsoft の IPsec 関連のマニュアルを参照してください。

FIPS モード使用時にサポートされない機能

FIPS モードがイネーブルの場合、次の Cisco Unity Connection の機能はサポートされません。

- SpeechView 文字変換サービス
- SIP ダイジェスト認証（SIP テレフォニー統合用の設定）

サインインするタッチトーン カンバセーション ユーザのボイスメール PIN の設定

Cisco Unity Connection 9.x の FIPS をイネーブルにすると、次の 2 つのオプションの両方に該当する場合、タッチトーン カンバセーションのユーザがサインインして音声メッセージを再生または送信したり、ユーザ設定を変更したりするのを防ぎます。

- Cisco Unity 5.x またはそれ以前のバージョンでユーザが作成され、その後 Connection に移行した場合。
- Connection ユーザが、Cisco Unity 5.x またはそれ以前のバージョンで割り当てられたボイスメール PIN を保持している場合。

タッチトーン カンバセーションのユーザは、ID（通常はユーザの内線番号）とボイスメール PIN を入力してサインインします。ID および PIN は、ユーザの作成時に割り当てられます。管理者またはユーザのいずれかが PIN を変更できます。Connection Administration では、管理者が PIN にアクセスできないように、PIN がハッシュされます。Cisco Unity 5.x 以前のバージョンでは、Cisco Unity が MD5 ハッシュ アルゴリズム（FIPS 非準拠）を使用して PIN をハッシュします。Cisco Unity 7.x 以降、および Connection では、復号化がより困難な SHA-1 アルゴリズム（FIPS 準拠）を使用して PIN をハッシュします。

次の項では、FIPS がイネーブルの場合に Connection でボイスメール PIN を設定する方法について説明します。

- 「Cisco Unity Connection 9.x でのすべてのボイス メール PIN の SHA-1 アルゴリズム使用ハッシュ」（P.5-5）
- 「Cisco Unity 5.x またはそれ以前のバージョンでの、MD5 によってハッシュされたボイスメール PIN と SHA-1 アルゴリズムとの置き換え」（P.5-5）

Cisco Unity Connection 9.x でのすべてのボイス メール PIN の SHA-1 アルゴリズム使用ハッシュ

バージョン 9.x では、FIPS がイネーブルの場合、Cisco Unity Connection はデータベースのチェックを行わず、ユーザのボイスメール PIN が MD5 と SHA-1 アルゴリズムのどちらでハッシュされたのかを判別しません。Connection はすべてのボイスメール PIN を SHA-1 でハッシュし、その PIN を Connection データベース内でハッシュされた PIN と比較します。ユーザが入力して MD5 によってハッシュされたボイスメール PIN が、データベース内で SHA-1 によってハッシュされたボイスメール PIN と一致しない場合、ユーザはサインインを許可されません。

Cisco Unity 5.x またはそれ以前のバージョンでの、MD5 によってハッシュされたボイスメール PIN と SHA-1 アルゴリズムとの置き換え

Cisco Unity 5.x またはそれ以前のバージョンで作成された Connection ユーザ アカウントでは、MD5 アルゴリズムによってハッシュされたボイスメール PIN が SHA-1 アルゴリズムに置き換えられる必要があります。MD5 によってハッシュされたパスワードを SHA-1 によってハッシュされたパスワードに置き換える際には、次の点を考慮します。

- User Data Dump ユーティリティの最新バージョンを使用して、MD5 によってハッシュされた PIN を持っているユーザの数を判別します。各ユーザの [Pin_Hash_Type] カラムに MD5 または SHA-1 のいずれかが表示されます。このユーティリティの最新バージョンをダウンロードして [ヘ

ルプ（Help）] を表示する方法については、次の URL にある Cisco Unity Tools Web サイトの [User Data Dump] ページを参照してください。
http://ciscounitytools.com/Applications/CxN/UserDataDump/UserDataDump.html

（注） User Data Dump ユーティリティの古いバージョンには、[Pin_Hash_Type] カラムは含まれていません。

- FIPS をイネーブルにする前に、[Connection 管理（Connection Administration）] の [パスワードの設定（Password Settings）] ページで、[次回サインイン時に、ユーザによる変更が必要（User Must Change at Next Sign-In）] チェックボックスをオンにしてください。これにより、ユーザは Connection にサインインして自分のボイスメール PIN を変更できるようになります。
- ボイスメール PIN を変更していないユーザがいる場合は、Bulk Password Edit ユーティリティを実行します。Bulk Password Edit ユーティリティを使用すると、PIN をランダムな値に選択的に変更し、そのデータを .csv ファイルとしてエクスポートできます。エクスポートされるファイルには、PIN が変更された各ユーザの名前、エイリアス、電子メール アドレス、および新しい PIN が含まれます。この .csv ファイルを使用して、新しい PIN を持つ各ユーザに電子メールを送信することができます。このユーティリティは、次の URL にある Cisco Unity Tools Web サイトから入手できます。
http://www.ciscounitytools.com/Applications/CxN/BulkPasswordEdit/BulkPasswordEdit.html