Cisco Unity Connection における FIPS コンプライアンス

Cisco Unity Connection における FIPS コンプライアンス

はじめに

連邦情報処理標準（FIPS）は、暗号モジュールにおいて遵守が必要な要件が定義された、米国およびカナダ政府の認証規格です。

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。Cisco Unity Connection 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、認定を確認するには、 次のリンクの FIPS 140 のドキュメントを参照してください。https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html

FIPS の CLI コマンドの実行

Cisco Unity Connection で FIPS 機能を有効にするには、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 機能を無効にします。
- 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 の <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*』を参照ください。このガイドは、http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html でご利用いただけます。

注意 FIPS モードを有効または無効にした後、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。

（注） Unity Connection サーバで FIPS モードを有効にする前に、セキュリティ パスワードの長さが 14 文字以上であることを確認してください。Unity Connection をアップグレードする場合は、以前のバージョンで FIPS が有効だった場合、パスワードを更新する必要があります。

すべての新しい証明書は、FIPS モードで SHA-256 ハッシュ アルゴリズムを使用して署名されます。自己署名証明書または証明書署名要求を生成する場合、ハッシュ アルゴリズムとして SHA-256 のみ選択することができます。

FIPS の証明書の再生成

ルート証明書の再生成

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 モードを有効化または無効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 モードを有効化すると、ルート証明書の再生成を回避できます。

（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 Administration にサインインします。
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、Cisco Unity Connection ルート証明書を .pem ファイルとして保存する場所を参照します。

   （注） 証明書は、拡張子を（.htm ではなく）.pem 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. Cisco Unity Connection ルート証明書をすべての Cisco Unified CM サーバにコピーするため、次のサブ手順を実行します。
   1. Cisco Unified CM サーバで、[Cisco Unified オペレーティング システムの管理（Cisco Unified Operating System Administration）] にサインインします。
   2. [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。
   3. [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。
   4. [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。
   5. [ルート証明書（Root Certificate）] フィールドに「Cisco Unity Connection Root Certificate」と入力します。
   6. [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。
   7. [Upload File] をクリックします。
   8. [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、Unity Connection Conversation Manager Service を再起動します。
    1. Cisco Unity Connection Serviceability にサインインします。
    2. [ツール（Tools）] メニューから [サービス管理（Service Management）] を選択します。
    3. [重要なサービス（Critical Services）] セクションで [停止（Stop）] を選択して Unity Connection Conversation Manager サービスを停止します。
    4. [ステータス（Status）] エリアに、Unity 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 の間での SCCP 統合と 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」の章にある「Manage Certificates and Certificate Trust Lists」の項を参照してください。このガイドは、以下のリンクからご利用いただけます。https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/os_administration/guide/b_14cucosagx.html

Tomcat 証明書の再生成

Unity Connection は、SIP 統合を使用してセキュアなコールを設定するために RSA キー ベースの Tomcat 証明書のみをサポートしています。これにより、SIP のセキュアなコール用に自己署名証明書およびサードパーティ CA 署名付き証明書を使用できるようになっています。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 モードを有効化または無効化した後に手動で再生成された Tomcat 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 tomcat 証明書を再アップロードする必要があります。羽化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 モードを有効化すると、ルート証明書の再生成を回避できます。

証明書を再生成する方法については、『*Cisco Unified Communications Manager SIP Integration Guide for Cisco Unity Connection Release 14*』の「Setting Up a Cisco Unified Communications Manager SIP Trunk Integration」の章にある「Settings for RSA Key Based certificates」の項を参照してください。このガイドは、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/integration/cucm_sip/b_14cucintcucmsip.html からご利用いただけます。

（注） Cisco Unified Communications Manager の [SIP トランク セキュリティ プロファイルの設定（SIP Trunk Security Profile Configuration）] ページの **[X.509 Subject Name]** フィールドに入力された値が、Unity Connection サーバの FQDN であることを確認してください。

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。

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 間で IPsec ポリシーを設定します。
- [Unity Connection 管理（Unity 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。NTLM Web 認証モードは FIPS モードではサポートされていません。

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 ポリシーの設定の詳細については、『*Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 14*』の「Security」の章の「IPSec Management」の項を参照してください。このガイドは、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/os_administration/guide/b_14cucosagx.html からご利用いただけます。

Unity Connection を使用した場合の IPsec ポリシーの影響については、『*Install, Upgrade, and Maintenance Guide for Cisco Unity Connection Release 14*』の「Upgrading Cisco Unity Connection」の章を参照してください。このガイドは、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/14/install_upgrade/guide/b_14cuciumg.html からご利用いただけます。

FIPS モード使用時にサポートされない機能

FIPS モードが有効な場合、次の Cisco Unity Connection の機能はサポートされません。

- SpeechView 音声テキスト変換サービス。
- SIP ダイジェスト認証（SIP テレフォニー統合用の設定）。
- SIP NTLM 認証（SIP テレフォニー統合用の設定）。
- ビデオ メッセージング。

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 で FIPS を有効にすると、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。
- Unity 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 Unity 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。

Unity Connection でのすべての SHA-1 アルゴリズムによるボイス メール PIN のハッシュ

FIPS が有効な場合、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。Unity 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 Unity 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 Unity 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 の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 を有効にする前に、[Unity Connection の管理（Unity Connection Administration）] の [パスワードの設定（Password Settings）] ページで、[ユーザは次回サインイン時に変更する必要あり（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 Unity 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