セキュリティモード

セキュリティモードの概要

データや情報の改ざんを防ぐためのセキュリティメカニズムを実装するために、Unified Communications Manager は、次のセキュリティモードを提供します。

- 非セキュアモード：デフォルトモード
- セキュアモードまたは混合モード：セキュアエンドポイントと非セキュアエンドポイントをサポートします。
- SIP Auth モード：セキュアな環境での Cisco Jabber 認証に OAuth 更新トークンを使用します。

非セキュアモード（デフォルトモード）

非セキュアモードは、Unified Communications Manager を初めてインストールする場合のデフォルトのセキュリティモードです。このモードでは、Unified Communications Manager はセキュアなシグナリングやメディアサービスを提供しません。

セキュアモードの設定

セキュリティを適用するには、導入に適用するセキュリティモードを設定します。

手順

	コマンドまたはアクション	目的
Step 1	混合モード	混合モードを有効にして、Cisco IP 電話および Webex デバイスのセキュリティを強化します。混合モードの有効化と確認の方法について説明します。
Step 2	SIP OAuth モード	Cisco Jabber クライアントおよびその他デバイスのセキュリティを強化するには、SIP OAuth モードを設定します。

混合モード

混合モードまたはセキュアモードは、セキュアエンドポイントと非セキュアエンドポイントをサポートします。クラスタまたはサーバに Unified Communications Manager を新しくインストールすると、デフォルトでは非セキュアモードになります。ただし、セキュリティモードは非セキュアモードからセキュアモードまたは混合モードに変換できます。

クラスタを非セキュアモードから混合モード（セキュアモード）に変更するには、次の手順を実行します。

- パブリッシャ上で認証局プロキシ機能（CAPF）サービスを有効にします。
- パブリッシャ上で証明書信頼リスト（CTL）サービスを有効にします。

Call Manager 証明書が電子署名されている場合、CTL ファイルには、サーバーごとのサーバー証明書、公開キー、シリアル番号、署名、発行者名、サブジェクト名、サーバー機能、DNS 名、および IP アドレスが含まれています。

Multi-SAN Call Manager 証明書の場合、CTL ファイルにはパブリッシャーの Call Manager 証明書が含まれています。

電話が次回初期化されたときに、その電話ではこの CTL ファイルを TFTP サーバからダウンロードします。CTL ファイルに自己署名証明書が含まれた TFTP サーバのエントリがある場合、電話では .sgn 形式の署名付き設定ファイルを要求します。TFTP サーバに証明書が含まれていない場合、電話では署名なしのファイルを要求します。

次のコマンドを実行して CTL ファイルを更新できます。

- **utils ctl set-cluster mixed-mode**

  CTL ファイルを更新し、クラスタを混合モードに設定します。

- **utils ctl set-cluster non-secure-mode**

  CTL ファイルを更新し、クラスタを非セキュア モードに設定します。

- **utils ctl update CTLFile**

  クラスタ内の各ノードの CTL ファイルを更新します。

（注） エンドポイントのセキュリティのためには、シグナリングに Transport Layer Security（TLS）を使用し、メディアに Secure RTP（SRTP）を使用します。

混合モードを有効にするには、発行元ノードのコマンドライン インターフェイスにログインし、CLI コマンド `utils ctl set-cluster mixed-mode` を実行します。

（注） Unified Communications Manager が Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに登録されていることを確認してください。スマートアカウントまたはバーチャルアカウントから受信した登録トークンには、このクラスタへの登録中に [エクスポート制御機能を許可する（Allow Export-Controlled）] 機能が有効になっています。

Tokenless CTL ファイルについては、ユニファイド コミュニケーション マネージャ リリース 12.0(1) で USB トークンを使用して生成されたアップロード済み CTL ファイルのダウンロードをエンドポイントで実行するよう、管理者が確認する必要があります。ダウンロード後、管理者は Tokenless CTL ファイルに切り替えることができます。次に、utils ctl upgrade CLI コマンドを実行することができます。

セキュリティモードを非セキュアモードからセキュアモードまたは混合モードに変更した場合は、そのモードを確認できます。モードを確認するには、**[エンタープライズパラメータの設定（Enterprise Parameters Configuration）]** ページに移動して、クラスタまたはサーバが混合モードであるかどうか確認します。詳細については、「セキュリティモードの確認」トピックを参照してください。

セキュリティモードの確認

セキュリティモードを非セキュアモードからセキュアモードまたは混合モードに変更した場合は、そのモードを確認できます。モードを確認するには、**[エンタープライズパラメータの設定（Enterprise Parameters Configuration）]** ページに移動して、クラスタまたはサーバが混合モードであるかどうか確認します。

セキュリティモードを確認するには、次の手順を実行します。

手順

Step 1 [Unified Communications Manager Administration] で、**[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）]** を選択します。
[エンタープライズパラメータの設定（Enterprise Parameters Configuration）] ページが表示されます。

Step 2 [セキュリティパラメータ（Security Parameters）] ペインに移動します。
適切な値の [クラスタセキュリティモード（Cluster Security Mode）] フィールドがあります。値に 1 が表示されている場合、Unified Communications Manager は混合モードに正常に設定されていま

す。Cisco Unified CM Administration ページでは、この値を設定できません。この値は、CLI コマンド `set utils cli` を入力した後に表示されます。

（注） クラスタセキュリティモードでは、スタンドアロンサーバまたはクラスタのセキュリティ機能を設定します。

CTL ファイルの SAST 役割

（注） CTL ファイルに署名するには、次の表に記載されている*署名者が使用されます。

表 *1 : CTL* ファイルのシステム管理者セキュリティ トークン（*SAST*）役割

Cisco Unified Communications Manager のバージョン	トークンベースの CTL ファイルでの SAST 役割	Tokenless CTL ファイルでの SAST 役割
12.0(1)	トークン 1（署名者*） トークン 2 ITLRecovery CallManager	ITLRecovery（署名者） CallManager
11.5(x)	トークン 1（署名者） トークン 2 ITLRecovery CallManager	CallManager（署名者） ITLRecovery
10.5(2)	トークン 1（署名者） トークン 2	CallManager（署名者） ITLRecovery
10.5(1) （サポート外）	トークン 1（署名者） トークン 2	CallManager（署名者）
10.0(1) （サポート外）	トークン 1（署名者） トークン 2	CallManager（署名者）
9.1(2)	トークン 1（署名者） トークン 2	N/A

SIP OAuth モード

SIP OAuth モードでは、セキュアな環境での Cisco Jabber 認証に OAuth 更新トークンを使用できます。Unified Communications Manager の SIP 回線で OAuth をサポートすることで、CAPF なしでセキュア シグナリングとセキュア メディアが可能になります。Unified Communication Manager クラスタおよびCisco Jabberエンドポイントで OAuthベースの認証を有効にすると、SIP 登録中の OAuth トークン検証が完了します。

SIP登録の OAuth サポートは、Cisco Jabber デバイスおよび特定の電話機モデルで使用できます。SIP OAuth の詳細については、Cisco Unified Communications Manager 機能設定ガイドを参照してください。

CLI を使用した SIP OAuth 設定

CLI を使用して、クラスタ SIP OAuth モードを設定することができます。

（注） Cisco Unified Communications Manager での SIP OAuth モードの設定方法の詳細については、『*Feature Configuration Guide for Cisco Unified Communications Manager*、リリース *14*』を参照してください。

次の点を考慮してください。

- クラスタ SIP OAuth モードが有効になっている場合、Cisco ユニファイドコミュニケーション マネージャーは、セキュアデバイスから OAuth トークンを受信した SIP 登録を受け入れることができます。

  有効にすると、Cisco Unified Communications Managerのユーザインターフェイスを使用して設定可能な次の TLS ポートが開かれます。

  - **SIP OAuth ポート**
  - **SIP OAuth MRA ポート**

  [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、**[システム（System）]** > **[Cisco Unified CM]** > **Call Manager** ページを選択します。

- パラメータ変更を反映するには、すべてのノードで Cisco CallManager サービスを再起動してください。

この暗号化方法では次の CLI コマンドを使用します。

管理者: ユーティリティ sipOAuth モード
クラスタ内の SIP OAuth モードのステータスを確認します。

ユーティリティ sipOAuth モードの有効化
クラスタ内の SIP OAuth モードを有効にします。

ユーティリティ sipOAuth モードの無効化
クラスタ内の SIP OAuth モードを無効にします。

（注） パブリッシャ ノードでのみ CLI コマンドを実行すします。

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。