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 - セキュアおよび非セキュア エンドポイントをサポートします。
- SIP 認証モード — 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)

初めてインストールするときの既定のセキュリティモードは、非セキュアモードです。 Unified Communications Manager このモードでは、 Unified Communications Manager はセキュアなシグナリングまたは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、展開に適用されるセキュリティモードを構成します。

手順

	コマンドまたはアクション	目的
ステップ 1	混合モード	混合モードを有効にすると、Cisco IP 電話と Webex デバイスのセキュリティが強化されます。 混合モードを有効にして確認する方法に関する情報を提供します。
ステップ 2	SIP OAuth モード	SIP OAuth モードを設定して、Cisco Jabber クライアントとその他のデバイスのセキュリティを強化します。

混合モード

混合モードまたはセキュア モードは、セキュアおよび非セキュア 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新たに Unified Communications Manager インストールすると、デフォルトで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を非セキュアからセキュアまたは混合モードに変換することはできます。

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、以下を実行します:

- 発行元で認証局プロキシ機能 (CAPF) サービスを有効にします。
- 発行元で証明書信頼リスト (CTL) サービスを有効にします。

Call Manager 証明書が自己署名の場合、CTL ファイルには各サーバのサーバ証明書、公開キー、シリアル番号、署名、発行者名、サブジェクト名、サーバ機能、DNS 名、および IP アドレスが含まれます。

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。

次に電話が初期化されるときに、TFTP サーバから CTL ファイルがダウンロードされます。 CTL ファイルに、自己署名証明書を持つ TFTP サーバエントリが含まれている場合、電話機は .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、電話機は署名されていない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 混合モード**

  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 ノンセキュア モード**

  CTL ファイルを更新し、クラスタをノンセキュア モードに設定します。

- **utils ctl update CTLFile**

  クラスターの各ノードで CTL ファイルを更新します。

（注） エンドポイントセキュリティでは、Transport Layer Security (TLS) がシグナリングに使用され、セキュアな RTP (SRTP) がメディアに使用されます。

混合モードを有効にするには、パブリッシャノードのコマンドラインインターフェースにログインし、CLI コマンド `utils ctl set-cluster 混合-モード`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け取った登録トークンは、このクラスターに登録する際に、輸出規制対象の許可機能が有効になっています。

トークンレス CTL ファイルの場合、管理者は、Unified Communications Manager リリース 12.0 (1) 以降で、USB トークンを使用して生成され、アップロードされた CTL ファイルをエンドポイントがダウンロードするようにする必要があります。 ダウンロード後、トークンレス CTL ファイルに切り替えることができます。 その後、util ctl update CLI コマンドを実行できます。

セキュリティモードを非セキュアからセキュアまたは混合モードに変更した場合、セキュリティ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設定**] ページに移動して、クラスタまたはサーバが混在モードになっていないことを確認してください。 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からセキュアまたは混合モードに変更した場合、セキュリティ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設定**] ページに移動して、クラスタまたはサーバが混在モードかどうかを確認してください。

セキュリティモードを確認するには、以下の手順を実行します。

ステップ 1 Unified Communications Manager の管理から **[システム]** > **エンタープライズパラメータ**を選択します。
[**エンタープライズパラメータの設定**] ページが表示されます。

ステップ 2 [**セキュリティパラメータ**] ペインに移動します。
[クラスターセキュリティモード（Cluster Security Mode）] フィールドが適切な値で見つかります。 値が 1 と表示されたら、Unified Communications Manager を混合モードに設定することに成功しています。 この値は Cisco Unified CM Administration の管理ページでは設定できません。 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。

SASTのCTLファイルの役割

（注） *次の表に記載されている署名者は、CTL ファイルへの署名に使用されます。

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

[Cisco Unified Communications Managerのバージョン（Cisco Unified Communications Manager Version）]	トークンベースのCTLファイルのシステム管理者セキュリティ トークン（SAST）の役割	トークンレスのCTLファイルのシステム管理者セキュリティ トークン（SAST）の役割
12.0(1)	トークン 1 (署名者*) トークン 2 ITL リカバリ CallManager	ITLRecovery (署名者) CallManager
11.5(x)	トークン 1 (署名者) トークン 2 ITL リカバリ CallManager	CallManager (署名者) ITL リカバリ
10.5(2)	トークン 1 (署名者) トークン 2	CallManager (署名者) ITL リカバリ
10.5(1) (サポートされていません)	トークン 1 (署名者) トークン 2	CallManager (署名者)
10.0(1) (サポートされていません)	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	なし

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。

以降の Cisco Jabber デバイスでのみ拡張されています。SIP 登録に対する OAuth サポートは、Cisco Jabber デバイスと特定の電話機で利用できます。SIP OAuth の詳細は、『Feature Configuration Guide for Cisco Unified Communications Manager』を参照してください。

CLI による SIP Oauth の構成

CLI を通じて、クラスター SIP Oauth モードを設定できます。

（注） Cisco Unified Communications Manager で SIP OAuth モードを設定する方法の詳細は、『*Cisco Unified Communications Manager* 機能設定ガイド、リリース *14*』を参照してください。

以下の点を考慮してください。

- クラスター SIP OAuth モードが有効な場合、Cisco Unified Communications Manager はセキュアなデバイスからの OAuth トークンによる SIP 登録を受け付けます。

  有効にすると、次の TLS ポートが開きます。これらは Cisco Unified Communications Manager ユーザインターフェイスから設定できます。

  - **SIP Oauth ポート**
  - **SIP Oauth MRA ポート**

  Cisco Unified CM Administration でポートを設定できます。**[システム（System）] > [Cisco Unified CM] > [CallManager]** ページを選択します。

- パラメータの変更を有効にするために、すべてのノードで Cisco CallManager サービスを再起動します。

暗号化オプションは以下の CLI コマンドで構成されています。

admin:utils sipOAuth-mode
クラスターの SIP OAuth モードの状況を確認します。
utils sipOAuth-mode enable
クラスターで SIP Oauth モードを有効にします。
utils sipOAuth-mode disable
クラスターで 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。