セキュリティ設定の構成

セキュリティの概要

この章では、IM and Presence Service のセキュリティ設定の設定手順について説明します。IM and Presence Service では、セキュア TLS 接続を設定し、FIPS モードなどの拡張セキュリティ設定を有効にすることができます。

IM and Presence Service が、Cisco Unified Communications Manager とプラットフォームを共有します。Cisco Unified Communications Managerのセキュリティ設定の方法の詳細は、*Cisco Unified Communications Manager* システム設定ガイド を参照してください。

セキュリティ設定のタスク フロー

このタスクを実行して、IM and Presence Service のセキュリティを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	ログイン バナーの作成 （2 ページ）	ユーザが IM and Presence Service インターフェイスでのログインの際に確認できるバナーを作成できます。
ステップ 2	セキュアな XMPP 接続の設定 （2 ページ）	このタスクを完了して、XMPPセキュリティ設定を行います。
ステップ 3	TLS ピア サブジェクトの設定 （4 ページ）	TLS ピアを設定する場合は、これらのタスクを設定します。
ステップ 4	TLS コンテキストの設定 （4 ページ）	TLS ピアの TLS コンテキストと TLS 暗号を設定します。

	コマンドまたはアクション	目的
ステップ 5	FIPS Mode （5 ページ）	FIPS 準拠の展開にする場合は、FIPS モードを有効にすることが可能です。セキュリティを強化するために、拡張セキュリティ モードおよび共通の準拠モードを有効にすることもできます。

ログイン バナーの作成

ユーザが IM and Presence サービス インターフェイスへのログインの一部として確認するバナーを作成できます。任意のテキスト エディタを使用して .txt ファイルを作成し、ユーザに対する重要な通知を含め、そのファイルを Cisco Unified IM and Presence OS の管理ページにアップロードします。

このバナーはすべての IM and Presence サービス インターフェイスに表示され、法的な警告や義務などの重要な情報をログインする前にユーザに通知します。Cisco Unified CM IM and Presence の管理、Cisco Unified IM and Presence オペレーティング システムの管理、Cisco Unified IM and Presence のサービスアビリティ、Cisco Unified IM and Presence のレポート、および IM and Presence のディザスタ リカバリ システム のインターフェースでは、このバナーがユーザがログインする前後に表示されます。

手順

ステップ 1 バナーに表示する内容を含む .txt ファイルを作成します。

ステップ 2 Cisco Unified IM and Presence オペレーティング システムの管理にサインインします。

ステップ 3 **[ソフトウェア アップグレード（Software Upgrades）]** > **[ログイン メッセージのカスタマイズ（Customized Logon Message）]** を選択します。

ステップ 4 **[参照（Browse）]** を選択し .txt ファイルを検索します。

ステップ 5 [ファイルのアップロード] をクリックします。

バナーは、ほとんどの IM and Presence サービス インターフェイスでログインの前後に表示されます。

（注） 「.txt」ファイルは、各 IM and Presence Service ノードに個別にアップロードする必要があります。

セキュアな XMPP 接続の設定

TLS を使用したセキュアな XMPP 接続を有効にするには、次の手順を使用します。

手順

ステップ 1 Cisco Unified CM IM and Presence 管理で、**システム** > **セキュリティ** > **設定**を選択します。

ステップ 2 適切なチェック ボックスをオンにして、以下の XMPP セキュリティ設定を有効にします。

表 *1 : IM and Presence Service* の *XMPP* セキュリティの設定

設定	説明
Enable XMPP Client To IM/P Service Secure Mode（XMPP クライアントと IM/P サービス間のセキュア モードの有効化）	有効にすると、IM and Presence Service が、クラスタの XMPP クライアント アプリケーションで、セキュアな TLS 接続を確立します。 この設定はデフォルトでイネーブルになっています。このセキュア モードをオフにしないことを推奨します。ただし、XMPP クライアント アプリケーションが非セキュア モードでクライアント ログイン クレデンシャルを保護できる場合を除きます。セキュア モードをオフにする場合は、他の方法で XMPP のクライアント ツー ノード通信を保護できることを確認してください。
Enable XMPP Router-to-Router Secure Mode（XMPP ルータ ツールータ セキュア モードの有効化）	この設定をオンにすると、IM and Presence サービスは同じクラスタ内または別のクラスタ内の XMPP ルータ間にセキュアな TLS 接続を確立します。IM and Presence サービスは XMPP 証明書を XMPP 信頼証明書として自動的にクラスタ内またはクラスタ間で複製します。XMPP ルータは、同じクラスタ内または別のクラスタ内にある他の XMPP ルータとの TLS 接続を確立しようとし、TLS 接続の確立に使用できます。
Enable Web Client to IM/P Service Secure Mode（Web クライアントと IM/P サービス間のセキュア モードの有効化）	この設定をオンにすると、IM and Presence サービスは、IM and Presence サービス ノードと XMPP ベースの API クライアント アプリケーション間のセキュアな TLS 接続を確立します。この設定をオンにした場合は、IM and Presence サービスの cup-xmpp-trust リポジトリに Web クライアントの証明書または署名付き証明書をアップロードします。

ステップ 3 **[保存（Save）]** をクリックします。

次のタスク

XMPP クライアントと IM/P サービス間のセキュア モードの有効化 設定を更新した場合、Cisco XCP Connection Manager を再起動します。

IM and Presence Service の SIP セキュリティの設定

TLS ピア サブジェクトの設定

IM and Presence サービス証明書をインポートすると、IM and Presence サービスは自動的に TLS ピア サブジェクトを TLS ピア サブジェクト リストおよび TLS コンテキスト リストに追加しようとします。要件に合わせて TLS ピア サブジェクトおよび TLS コンテキストが設定されていることを確認します。

手順

ステップ 1 **Cisco Unified CM IM and Presence 管理** で、**システム** > **セキュリティ** > **TLS ピア サブジェクト** を選択します。

ステップ 2 **[新規追加]** をクリックします。

ステップ 3 ピア サブジェクト名に対して次の手順のいずれかを実行します。

a) ノードが提示する証明書のサブジェクト CN を入力します。

b) 証明書を開き、CN を探してここに貼り付けます。

ステップ 4 [説明（Description）] フィールドにノードの名前を入力します。

ステップ 5 [保存（Save）] をクリックします。

次のタスク

TLS コンテキストを設定します。

TLS コンテキストの設定

TLS ピア サブジェクトに TLS コンテキストおよび TLS 暗号を割り当てるには、次の手順を使用します。

（注） IM and Presence Service証明書をインポートする際、IM and Presence Service は自動的に TLS ピア サブジェクトの TLS ピア サブジェクト リストおよび TLS コンテキスト リストへの追加を試みます。

始める前に

TLS ピア サブジェクトの設定 （4 ページ）

手順

ステップ 1 **Cisco Unified CM IM and Presence Administration**で、**システム** > **セキュリティ** > **TLS コンテキスト設定**を選択します。

ステップ 2 [検索（Find）] をクリックします。

ステップ 3 **[Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context]** を選択します。

ステップ 4 使用可能な TLS ピア サブジェクトのリストから、設定した TLS ピア サブジェクトを選択します。

ステップ 5 > の矢印を利用して、TLS ピア サブジェクトを**選択した TLS ピア サブジェクト**に移動します。

ステップ 6 **TLS 暗号のマッピング**の設定

a) **利用可能な TLS 暗号**および **選択した TLS 暗号** ボックスで利用できる TLS 暗号の一覧を確認します。

b) 現在選択されていない TLS 暗号を有効にするには、> 矢印を利用して、暗号を**選択した TLS 暗号**に移動します。

ステップ 7 **[保存（Save）]** をクリックします。

ステップ 8 Cisco SIP Proxy サービスを再起動します。

a) [Cisco Unified IM and Presenceのサービスアビリティ（Cisco Unified IM and Presence Serviceability）] から、**[ツール（Tools）]** > **[コントロールセンター-機能サービス（Control Center - Feature Services）]** を選択します。

b) **サーバ** ドロップダウン リスト ボックスで、IM and Presence Service クラスタ ノードを選択し、**移動**をクリックします。

c) **Cisco SIP プロキシ** サービスを選択し、**再起動**をクリックします。

FIPS Mode

IM and Presence Serviceには、一連の拡張システム セキュリティ モードが含まれています。この機能を使用すると、暗号化、データとシグナリング、および監査ログなどのアイテムを対象とした、より厳格なセキュリティ ガイドラインおよびリスク管理制御下でシステムが動作します。

- FIPS モード：IM and Presence Service を FIPS モードで動作するように設定することが可能です。これによりシステムは FIPS または連邦情報処理規格、米国およびカナダ政府の標準に準拠し、暗号化モジュールを使用することができます。
- 拡張セキュリティ モード：セキュリティ強化モードが FIPS 対応のシステム上で実行され、データ暗号化要件、より厳密な資格情報ポリシー、連絡先検索のためのユーザ認証、およびより厳密な監査のためのログ要件などの追加のリスク管理制御が提供されます。
- 共通基準モード：共通基準モードは、FIPS 対応システム上でも、システムを TLS や x.509 v3 証明書の使用などの一般的な基準ガイドラインに準拠するための追加制御機能を提供します。

（注） 外部データベースが MSSQL の場合、メッセージアーカイバ、テキスト会議マネージャ、ファイル転送マネージャなどのサービスを共通基準モードで動作させるには、次の手順を実行する必要があります。

1. TLS 1.1 以降をサポートするために、MSSQL データベースをホストするサーバを設定します。
2. IM and プレゼンスサービスにデータベース証明書を再アップロードします。
3. [**External Database Configuration**] ページの [**Enable SSL**] チェックボックスをオンにします。[Cisco Unified CM IM and Presenceの管理（Cisco Unified CM IM and Presence Administration）] > [メッセージ（Messaging）] > [外部サーバの設定（External Server Setup）] > [外部データベース（External Databases）] を選択して、外部データベースを設定します。

重要 この注記は、リリース 12.5(1)SU7 にのみ適用されます。

クラスタにマルチサーバーの SAN 証明書構成があり、クラスタを FIPS およびコモンクライテリアモードに移行している場合。マルチサーバー SAN 証明書が自己署名証明書に変換されます。

FIPS およびコモンクライテリアモードの Unified Communications Manager サーバーに古いマルチサーバー SAN 証明書が残っている場合は、手動で削除する必要があります。

FIPS モード、拡張セキュリティ モード、共通基準モードを Cisco Unified Communications Manager および IM and Presence Service で有効にする方法は、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html の *Cisco Unified Communications Manager* セキュリティ ガイドの,「FIPS モードの設定」の章を参照してください。

FIPS の Microsoft Outlook カレンダー統合

IM and Cisco Presence サービスサーバで FIPS モードが有効になっている場合、Exchange Web サービス情報の取得には NTLMv2 だけがサポートされます。FIPS モードが無効になっている場合、既存の動作に従って NTLMv1 と NTLMv2 の両方がサポートされます。基本認証は、FIPS モードの有効化または無効化に関係なく、両方のケースでサポートされます。

Presence Engine サービスには、[FIPSモードのExchange Server認証（FIPS Mode Exchange Server Authentication）] という新しいサービスパラメータが導入されています。これにより、Microsoft Outlook カレンダー統合機能を通じて Exchange Server との接続を確立するときに Presence Engine で使用される認証の種類を確認できます。

[**FIPS Mode Exchange Server Authentication**] サービスパラメータは、[**Auto**] または [**Basic Only**] のいずれかに設定できます。

サービスパラメータが [**自動 (Auto**)] に設定されている場合: プレゼンスエンジンは、最初に ntlmv2 をネゴシエートし、ntlmv2 ネゴシエーションが失敗した場合にのみ「基本認証」にフォールバックします。NTLMv1 は FIPS モードではネゴシエートされません。

サービスパラメータが**基本のみ**に設定されている: プレゼンスエンジンは、Exchange サーバが NTLM と基本認証の両方を許可するように設定されている場合でも、「基本認証」を使用するように強制されます。

（注） サービスパラメータ設定を変更する場合は、Cisco Presence エンジンを再起動する必要があります。

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。