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 サービスでセキュリティ設定を行う手順について説明します。IM and Presence サービスでは、安全な 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できます。

IM and Presence サービスは Cisco Unified Communications Manager とプラットフォームを共有します。Cisco Unified Communications Manager でのセキュリティの設定手順については、*Security Guide for Cisco Unified Communications Manager*を参照してください。

セキュリティ設定構成のタスク フロー

これらのオプションのタスクを完了して、IM and Presence サービス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 サービス インターフェイスへのログイン時に確認する必要があるログインバナーを作成します。
ステップ 2	安全な XMPP 接続の設定 （3 ページ）	XMPP セキュリティを設定するためにこれらのタスクを完了して下さい。
ステップ 3	TLS ピア サブジェクトの設定 （4 ページ）	TLS ピアを設定したい場合は、これらのタスクを設定してください。

	コマンドまたはアクション	目的
ステップ 4	TLS コンテキストの設定 （4 ページ）	TLS ピアに TLS コンテキストと TLS 暗号を設定します。
ステップ 5	FIPSモード （5 ページ）	展開を FIPS 準拠にしたい場合は、FIPS モードを有効にできます。セキュリティを強化するために、拡張セキュリティ モードと共通コンプライアンス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（Upload File）] 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 サービス ノードに個別にアップロードする必要があります。

安全な XMPP 接続の設定

TLS を使用して安全な XMPP 接続を有効にするには、この手順を使用してください。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）]から、**[システム（System）] > [セキュリティ（Security）] > [設定（Settings）]** 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、次の XMPP セキュリティ設定を有効にします。

表 *1 : IM and Presence Service* での *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）	有効な場合は、IM and Presence サービスはクラスタ内の XMPP クライアント アプリケーションにセキュアな TLS 接続を確立します。 この設定はデフォルトでは有効になっています。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 ツー IM/P サービスのセキュア モードを有効にする（Enable XMPP Client To IM/P Service Secure Mode）]設定を更新した場合は、Cisco XCP Connection Manager を再起動します。

IM and Presence Service での 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 Administration**で、**[システム（System）] > [セキュリティ（Security）] > [TLSピアサブジェクト（TLS Peer Subjects）]**を選択します。

ステップ 2 [新規追加（Add New）] 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

この手順を使用して、TLS コンテキストと TLS 暗号を TLS ピアサブジェクトに割り当てます。

（注） 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。

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（System）] > [セキュリティ（Security）] > [TLS コンテキスト設定（TLS Context Configuration）]**に移動します。

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 >をクリックして、この TLS ピア サブジェクトを**[選択された TLS ピア サブジェクト（Selected TLS Peer Subjects）]**に移動します。

ステップ 6 **TLS 暗号のマッピング**オプションの設定：

a) **利用可能な TLS 暗号**そして**選択された TLS 暗号**ボックスで利用可能な TLS 暗号のリストを確認します。

b) 現在選択されていない TLS 暗号を有効にしたい場合は、> 矢印を使用して暗号を**選択された 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 プロキシ 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（Server）]** ドロップダウンリストから [IM and Presence Service] ノードを選択し、**[移動（Go）]** をクリックします。

c) **Cisco SIP Proxy** サービスを選択して**[再起動（Restart）]**をクリックします。

FIPSモード

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 サービスは FIPS モードで動作するように設定できます。これにより、システムは FIPS または米国およびカナダの政府標準の暗号化モジュール規格に準拠できます。
- 拡張セキュリティモード-拡張セキュリティモードはFIPS対応システム上で動作し、データ暗号化要件、厳格な認証情報ポリシー、連絡先検索のためのユーザー認証、厳格な監査ログ要件などの追加のリスク管理制御を提供します。

- 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コモン クライテリア 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. MSSQL データベースをホストしているサーバで、TLS 1.1 以降をサポートするように設定します。
2. IM and Presence Service にデータベース証明書を再アップロードします。
3. [外部データベースの設定（Enable SSL）] ページの [SSLの有効化（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。

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 Service サーバで FIPS モードを有効にすると、Exchange Web サービス情報を取得するためにサポートされるのは NTLMv2 だけになります。FIPS モードが無効の場合は、既存の動作と同様に NTLMv1 と NTLMv2 の両方がサポートされます。基本認証は、FIPS モードが有効か無効かにかかわらず、どちらの場合にもサポートされます。

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モードのExchange Server認証（FIPS Mode Exchange Server Authentication）] サービス パラメータは、[自動（Auto）] または [基本のみ（Basic Only）] に設定できます。

サービス パラメータを [自動（Auto）] に設定した場合： Presence Engine 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。FIPS モードでは NTLMv1 はネゴシエートされません。

サービス パラメータを [基本のみ（Basic Only）] に設定した場合：Exchange Server 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、Presence Engine は「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した場合は、Cisco Presence Engine を再起動する必要があります。