# TLS セットアップ



## TLS の概要

Transport Layer Security（TLS）はセキュア ポートと証明書交換を使用して、2 つのシステム間またはデバイス間でセキュアで信頼できるシグナリングとデータ転送を実現します。TLS は音声ドメインへのアクセスを防ぐために、ユニファイドコミュニケーションマネージャ 制御システム、デバイス およびプロセス間の接続を保護および制御します。

## TLS の前提条件

最低 TLS バージョンを設定する前に、ネットワーク デバイスとアプリケーションの両方でその TLS バージョンがサポートされていることを確認します。また、それらが、ユニファイドコミュニケーション マネージャIM およびプレゼンスサービス で設定する TLS で有効になっていることを確認します。次の製品のいずれかが展開されているなら、最低限の TLS 要件を満たしていることを確認します。この要件を満たしていない場合は、それらの製品をアップグレードします。

- Skinny Client Control Protocol（SCCP）Conference Bridge
- トランスコーダ（Transcoder）
- ハードウェア メディア ターミネーション ポイント（MTP）
- SIP ゲートウェイ
- Cisco Prime Collaboration Assurance
- Cisco Prime Collaboration Provisioning
- Cisco Prime Collaboration Deployment

- Cisco Unified Border Element（CUBE）
- Cisco Expressway
- Cisco TelePresence Conductor

会議ブリッジ、メディア ターミネーション ポイント（MTP）、Xcoder、Prime Collaboration Assurance および Prime Collaboration Provisioning をアップグレードすることはできません。

（注） ユニファイドコミュニケーションマネージャの旧リリースからアップグレードする場合は、上位のバージョンの TLS を設定する前に、すべてのデバイスとアプリケーションでそのバージョンがサポートされていることを確認します。たとえば、ユニファイドコミュニケーションマネージャ IM およびプレゼンスサービス のリリース 9.x でサポートされるのは、TLS 1.0 のみです。

# TLS 設定タスク フロー

TLS 接続の Unified Communications Manager を構成するには、次の作業を実行します。

手順

| | コマンドまたはアクション | 目的 |
|---|---|---|
| **Step 1** | 最小 TLS バージョンの設定 （3 ページ）. | デフォルトでは、Unified Communications Manager において、最小 TLS バージョンとして 1.0 がサポートされています。上位のバージョンの TLS がセキュリティ要件で求められる場合は、TLS 1.1 または 1.2 を使用するようにシステムを再設定します。 |
| **Step 2** | （任意） TLS 暗号化の設定 （4 ページ）。 | Unified Communications Manager でサポートされる TLS 暗号オプションを構成します。 |
| **Step 3** | SIP トランクのセキュリティ プロファイルでの TLS の設定 （4 ページ）。 | SIP トランクに TLS 接続を割り当てます。このプロファイルを使用するトランクでは、シグナリングのために TLS を使用します。また、セキュア トランクを使用することにより、会議ブリッジなどのデバイスに TLS 接続を追加することができます。 |
| **Step 4** | SIP トランクへのセキュア プロファイルの追加 （5 ページ）。 | トランクの TLS サポートを可能にするため、TLS 対応 SIP トランク セキュリティ プロファイルを SIP トランクに割り当てます。また、セキュア トランクを使用する |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | ことにより、会議ブリッジなどのリソースに接続することができます。 |
| **Step 5** | 電話セキュリティ プロファイルでの TLS の設定 （5 ページ）。 | 電話セキュリティ プロファイルに TLS 接続を割り当てます。このプロファイルを使用する電話では、シグナリングのために TLS を使用します。 |
| **Step 6** | 電話へのセキュア電話プロファイルの追加 （6 ページ）。 | 作成した TLS 対応プロファイルを電話に割り当てます。 |
| **Step 7** | ユニバーサル デバイス テンプレートへのセキュア電話プロファイルの追加 （7 ページ）. | TLS 対応の電話のセキュリティ プロファイルをユニバーサル デバイス テンプレートに割り当てます。LDAP ディレクトリ同期がこのテンプレートで設定されている場合は、LDAP 同期化を通じて電話のセキュリティをプロビジョニングできます。 |

# 最小 TLS バージョンの設定

デフォルトでは、Unified Communications Manager において、最小 TLS バージョンとして 1.0 がサポートされています。Unified Communications Manager および IM and Presence Service の最低サポート TLS バージョンを 1.1 または 1.2 などの上位バージョンにリセットするには、次の手順を使用します。

設定対象の TLS バージョンが、ネットワーク内のデバイスとアプリケーションでサポートされていることを確認します。詳細については、「TLS の前提条件 （1 ページ）」を参照してください。

### 手順

**Step 1** コマンド ライン インターフェイスにログインします。

**Step 2** 既存の TLS のバージョンを確認するには、**show tls min-version** CLI コマンドを実行します。

**Step 3** **set tls min-version** <*minimum*> CLI コマンドを実行します。ここで、<*minimum*> は TLS のバージョンを示します。

たとえば、最低 TLS バージョンを 1.2 に設定するには、**set tls min-version 1.2** を実行します。

**Step 4** すべての Unified Communications Manager と IM and Presence Service クラスタノードで、手順 3 を実行します。

# TLS 暗号化の設定

SIP インターフェイスで使用可能な最強の暗号方式を選択することで、弱い暗号を無効にすることができます。TLS 接続を確立するために Unified Communications Manager でサポートされる暗号化を設定するには、この手順を使用します。

### 手順

**Step 1** Cisco Unified CM の管理から、**[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。

**Step 2** [セキュリティ パラメータ（Security Parameters）] で、[TLS 暗号化（TLS Ciphers）] エンタープライズ パラメータの値を設定します。使用可能なオプションについては、エンタープライズ パラメータのオンラインヘルプを参照してください。

**Step 3** [保存（Save）] をクリックします。

# SIP トランクのセキュリティ プロファイルでの TLS の設定

SIP トランク セキュリティ プロファイルに TLS 接続を割り当てるには、次の手順を実行します。このプロファイルを使用するトランクでは、シグナリングのために TLS を使用します。

### 手順

**Step 1** Cisco Unified CM の管理から、**[システム（System）] > [セキュリティ（Security）] > [SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）]** を選択します。

**Step 2** 次のいずれかの手順を実行します。

- [新規追加（Add New）] をクリックして、新しい SIP トランク セキュリティ プロファイルを作成します。
- **[検索（Find）]** をクリックして検索し、既存のプロファイルを選択します。

**Step 3** [名前（Name）] フィールドに、プロファイルの名前を入力します。

**Step 4** [デバイス セキュリティ モード（Device Security Mode）] フィールドの値を、[暗号化（Encrypted）] または [認証（Authenticated）] に設定します。

**Step 5** [受信転送タイプ（Incoming Transport Type）] フィールドと [送信転送タイプ（Outgoing Transport Type）] フィールドの両方の値を、TLS に設定します。

**Step 6** **[SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）]** ウィンドウの残りのフィールドにデータを入力します。フィールドとその設定のヘルプについては、オンライン ヘルプを参照してください。

**Step 7** [保存（Save）] をクリックします。

# SIP トランクへのセキュア プロファイルの追加

TLS 対応の SIP トランク セキュリティ プロファイルを SIP トランクに割り当てるには、次の手順を使用します。このトランクを使用することにより、会議ブリッジなどのリソースとのセキュア接続を作成できます。

### 手順

**Step 1** Cisco Unified CM の管理から、**[デバイス（Device）] > [トランク（Trunk）]** を選択します。

**Step 2** **[検索（Find）]** をクリックして検索し、既存のトランクを選択します。

**Step 3** [デバイス名（Device Name）] フィールドに、トランクのデバイス名を入力します。

**Step 4** **[デバイス プール（Device Pool）]** ドロップダウン リストから、デバイス プールを選択します。

**Step 5** **[SIP プロファイル（SIP Profile）]** ドロップダウン リストで、SIP プロファイルを選択します。

**Step 6** **[SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）]** ドロップダウン リスト ボックスから、前のタスクで作成した TLS 対応の SIP トランク プロファイルを選択します。

**Step 7** [宛先（Destination）] 領域に、宛先 IP アドレスを入力します。最大 16 の宛先アドレスを入力できます。追加の宛先を入力するには、[+] ボタンをクリックします。

**Step 8** [トランクの設定（Trunk Configuration）] ウィンドウのその他のフィールドを設定します。フィールドとその設定のヘルプについては、オンライン ヘルプを参照してください。

**Step 9** [保存（Save）] をクリックします。

（注） トランクをセキュア デバイスに接続する場合、Unified Communications Manager にセキュア デバイスの証明書をアップロードする必要があります。証明書の詳細については、「証明書」セクションを参照してください。

# 電話セキュリティ プロファイルでの TLS の設定

電話セキュリティ プロファイルに TLS 接続を割り当てるには、次の手順を実行します。このプロファイルを使用する電話では、シグナリングのために TLS を使用します。

### 手順

**Step 1** Cisco Unified CM Administration から、**[システム（System）] > [セキュリティ（Security）] > [電話セキュリティ プロファイル（Phone Security Profile）]** の順に選択します。

**Step 2** 次のいずれかの手順を実行します。

- [新規追加（Add New）] をクリックして新しいプロファイルを作成します。
- **[検索（Find）]** をクリックして検索し、既存のプロファイルを選択します。

**Step 3** 新しいプロファイルを作成する場合は、電話モデルとプロトコルを選択し、[次へ（Next）] をクリックします。

（注） ユニバーサル デバイス テンプレートと LDAP 同期を使用して LDAP 同期を通じてセキュリティをプロビジョニングする場合は、[電話セキュリティ プロファイル タイプ（Phone Security Profile Type）] に [ユニバーサル デバイス テンプレート（Universal Device Template）] を選択します。

**Step 4** プロファイル名を入力します

**Step 5** **[デバイス セキュリティ モード（Device Security Mode）]** ドロップダウン リスト ボックスで、**[暗号化（Encrypted）]** または **[認証（Authenticated）]** を選択します。

**Step 6** （SIP 電話のみ）転送タイプには、**TLS** を選択します。

**Step 7** [電話セキュリティ プロファイルの設定（Phone Security Profile Configuration）] ウィンドウの残りのフィールドを入力します。フィールドとその設定のヘルプについては、オンライン ヘルプを参照してください。

**Step 8** [保存（Save）] をクリックします。

# 電話へのセキュア電話プロファイルの追加

TLS 対応の電話セキュリティ プロファイルを電話に割り当てるには、次の手順を使用します。

（注） 一度に多数の電話にセキュア プロファイルを割り当てるには、一括管理ツールを使用することにより、それらのセキュリティ プロファイルの再割り当てを行います。

## 手順

**Step 1** Cisco Unified CM の管理から、**[デバイス（Device）]** > **[電話（Phone）]** を選択します。

**Step 2** 次のいずれかの手順を実行します。

- [新規追加（Add New）] をクリックして新しい電話機を作成します。
- **[検索（Find）]** をクリックして検索し、既存の電話機を選択します。

**Step 3** 電話の種類とプロトコルを選択し、[次（Next）] をクリックします。

**Step 4** [デバイス セキュリティ プロファイル（Device Security Profile）] ドロップダウン リストから、作成したセキュア プロファイルを電話に割り当てます。

**Step 5** 次の必須フィールドに値を割り当てます。

- MAC アドレス
- [デバイスプール（Device Pool）]
- [SIPプロファイル（SIP Profile）]

- [オーナーのユーザID（Owner User ID）]
- 電話ボタンテンプレート（Phone Button Template）

**Step 6** [電話の設定（Phone Configuration）] ウィンドウの残りのフィールドを入力します。フィールドとその設定のヘルプについては、オンライン ヘルプを参照してください。

**Step 7** [保存（Save）] をクリックします。

# ユニバーサル デバイス テンプレートへのセキュア電話プロファイルの追加

TLS 対応の電話セキュリティ プロファイルをユニバーサル デバイス テンプレートに割り当てるには、次の手順を使用します。LDAP ディレクトリ同期が設定されている場合は、機能グループテンプレートとユーザ プロファイルにより LDAP 同期にこのユニバーサル デバイス テンプレートを含めることができます。同期処理が発生すると、電話に対してセキュア プロファイルがプロビジョニングされます。

### 手順

**Step 1** [Cisco Unified CM 管理（Cisco Unified CM Administration）] から、以下を選択します。**[ユーザ管理（User Management）] > [ユーザ/電話の追加（User/Phone Add）] > [ユニバーサルデバイステンプレート（Universal Device Template）]**

**Step 2** 次のいずれかの手順を実行します。

- [新規追加（Add New）] をクリックして新しいテンプレートを作成します。
- **[検索（Find）]** をクリックして検索し、既存のテンプレートを選択します。

**Step 3** [名前（Name）] フィールドに、テンプレートの名前を入力します。

**Step 4** **[デバイス プール（Device Pool）]** ドロップダウン リストから、デバイス プールを選択します。

**Step 5** **[デバイス セキュリティ プロファイル（Device Security Profile）]** ドロップダウンリストから、作成した TLS 対応セキュリティプロファイルを選択します。

（注） [ユニバーサル デバイス テンプレート（Universal Device Template）] をデバイス タイプとする電話セキュリティ プロファイルが作成されていなければなりません。

**Step 6** **[SIP プロファイル（SIP Profile）]** を選択します。

**Step 7** **[電話ボタン テンプレート（Phone Button Template）]** を選択します。

**Step 8** [ユニバーサル デバイス テンプレートの設定（Universal Device Template Configuration）] ウィンドウの残りのフィールドに入力します。フィールドとその設定のヘルプについては、オンライン ヘルプを参照してください。

**Step 9** [保存（Save）] をクリックします。

LDAP ディレクトリ同期処理に、ユニバーサル デバイス テンプレートを含めます。LDAP ディレクトリ同期の設定方法の詳細については、Cisco Unified Communications Manager システム設定ガイド の「「エンドユーザの設定」」部分を参照してください。

# TLS の連携動作と制約事項

この章では、TLS のインタラクションと制限事項について説明します。

## TLS の相互作用

表 *1 : TLS* の相互作用

| 機能 | 連携動作 |
|---|---|
| コモン クライテリア モード | コモン クライテリア モードは、最低限の TLS バージョンの設定と共に有効にすることができます。そのようにする場合、アプリケーションは、引き続きコモン クライテリアの要件に準拠し、アプリケーション レベルで TLS 1.0 セキュア接続を無効にすることになります。コモン クライテリア モードが有効な場合、アプリケーションで最低限の TLS バージョンを 1.1 または 1.2 のいずれかとして設定することができます。コモン クライテリア モードの詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』の中のコモン クライテリアへの準拠のトピックを参照してください。 |

## TLS の制限

79xx、69xx、89xx、99xx、39xx、IP Communicator など、従来型の電話に Transport Layer Security（TLS）バージョン 1.2 を実装する際に発生する可能性のある問題を、次の表に示します。使用している電話で、このリリースのセキュア モードがサポートされているかどうかを確認するには、Cisco Unified Reporting の Phone Feature List Report を参照してください。従来型の電話の機能制限および機能を実装するための回避策の一覧を、次の表に示します。

（注） 回避策は、影響を受ける機能が、実際のシステムで動作するように設計されています。しかし、その機能の TLS 1.2 コンプライアンスについては保証できません。

表 *2 : Transport Layer Security*（*TLS*）バージョン *1.2* の制約事項

| 機能 | 制限事項 |
|---|---|
| 暗号化モードの従来型の電話 | 暗号化モードの従来型の電話は動作しません。回避策はありません。 |
| 認証モードの従来型の電話 | 認証モードの従来型の電話は動作しません。回避策はありません。 |
| HTTPS に基づくセキュア URL を使用する IP 電話サービス。 | HTTPS に基づくセキュア URL を使用する IP 電話サービスは動作しません。<br>IP 電話サービスを使用するための回避策：基盤になっているすべてのサービス オプションに HTTP を使用します。たとえば、社内ディレクトリと個人用ディレクトリ。しかし、エクステンション モビリティなどの機能で、機密データを入力することが必要な場合、HTTP では安全ではないため、HTTP はお勧めしません。HTTP 使用には、次の欠点があります。<br>• 従来型の電話に HTTP、サポート対象の電話に HTTPS を設定する場合のプロビジョニングに関する課題。<br>• IP 電話サービスの復元力の欠如。<br>• IP 電話サービスを処理するサーバのパフォーマンスが低下する可能性。 |
| 従来型の電話でのエクステンション モビリティ クロス クラスタ（EMCC） | EMCC は、従来型の電話の TLS 1.2 でサポートされていません。<br>回避策：EMCC を有効にするため、次の作業を実行します。<br>**1.** HTTPS ではなく HTTP により EMCC を有効にします。<br>**2.** すべての Unified Communications Manager クラスタで混合モードをオンにします。<br>**3.** すべての Unified Communications Manager クラスタに同じ USB eToken を使用します。 |
| 従来型の電話でのローカルで有効な証明書（LSC） | LSC は、従来型の電話の TLS 1.2 でサポートされていません。結果として、LSC に基づく 802.1x および電話 VPN 認証はご利用いただけません。<br>802.1x のための回避策：古い電話では、MIC または EAP-MD5 によるパスワードに基づく認証。ただし、これらは推奨されません。<br>VPN のための回避策：エンドユーザのユーザ名とパスワードに基づく電話 VPN 認証を使用。 |

| 機能 | 制限事項 |
| --- | --- |
| 暗号化 Trivial File Transfer Protocol（TFTP）構成ファイル | 暗号化 Trivial File Transfer Protocol（TFTP）構成ファイルは、メーカーのインストールした証明書（MIC）がある場合でも、従来型の電話の TLS 1.2 でサポートされません。<br>回避策はありません。 |
| CallManager 証明書を更新すると、従来型の電話は信頼を失う | 従来型の電話は、CallManager 証明書が更新された時点で信頼を失います。たとえば、証明書更新後、電話は新しい構成を取得できなくなります。これは、ユニファイドコミュニケーション マネージャ11.5.1 だけで適用されます。<br>回避策：従来型の電話が信頼を失わないようにするため、次の手順を実行します。<br>**1.** CallManager 証明書を有効にする前に、[8.0 より前のリリースへロールバックするクラスタ（Cluster For Roll Back to Pre 8.0）] エンタープライズパラメータを True に設定します。デフォルトでは、この設定により、セキュリティが無効になります。<br>**2.** 一時的に TLS 1.0 を許可します（ユニファイド コミュニケーション マネージャを複数回リブート）。 |
| サポートされていないバージョンの Cisco Unified Communications Manager への接続 | より高い TLS バージョンをサポートしていない Unified Communications Manager の古いバージョンへの TLS 1.2 接続は動作しません。たとえば、Unified Communications Manager リリース 9.x への TLS 1.2 SIP トランク接続は動作しません。このリリースでは TLS 1.2 がサポートされていないためです。<br>次の回避策のいずれかを使用できます。<br>• 接続を有効にするための回避策：非セキュア トランクを使用。ただし、推奨されるオプションではありません。<br>• TLS 1.2 を使用しつつ接続を有効にするための回避策：TLS 1.2 をサポートしていないバージョンから、サポートするリリースにアップグレードします。 |
| Certificate Trust List（CTL）クライアント | CTL クライアントでは、TLS 1.2 がサポートされません。<br>次の回避策のいずれかを使用できます。<br>• CTL クライアントを使用する際に一時的に TLS 1.0 を許可し、クラスタをコモン クライテリア モードに移します。最小 TLS を 1.1 または 1.2 に設定します<br>• コモン クライテリア モードで CLI コマンド **utils ctl set-cluster mixed-mode** を使用することにより、Tokenless CTL に移行します。最小 TLS を 1.1 または 1.2 に設定します |

| 機能 | 制限事項 |
|---|---|
| Address Book Synchronizer | 回避策はありません。 |

### Cisco Unified Communications ManagerIM およびプレゼンスサービス のポートのうち Transport Layer Security Version 1.2 によって影響を受けるもの

次の表に、TLS バージョン 1.2 の影響を受ける Unified Communications Manager ポートを示します。

表 *3 : Cisco Unified Communications Manager* のポートのうち *Transport Layer Security Version 1.2* によって影響を受けるもの

| アプリケーション | プロトコル | 宛先/リスナー | 通常モードで動作する **Cisco Unified Communications Manager** | | | コモン クライテリア モードで動作する **Cisco Unified Communications Manager** | | |
|---|---|---|---|---|---|---|---|---|
| | | | 最低 **TLS** バージョン **1.0** | 最低 **TLS** バージョン **1.1** | 最低 **TLS** バージョン **1.2** | 最低 **TLS** バージョン **1.0** | 最低 **TLS** バージョン **1.1** | 最低 **TLS** バージョン **1.2** |
| Tomcat | HTTPS | 443 | TLS 1.0、TLS 1.1、TLS 1.2 | TLS 1.1、TLS v1.2 | TLS 1.2 | TLS 1.1 | TLS 1.1、TLS 1.2 | TLS 1.2 |
| SCCP-秒-SIG | Signalling Connection Control Part（SCCP） | 2443 | TLS 1.0、TLS 1.1、TLS 1.2 | TLS 1.1、TLS 1.2 | TLS 1.2 | TLS 1.1 | TLS 1.1、TLS 1.2 | TLS 1.2 |
| CTL-SERV | 専用 | 2444 | TLS 1.0、TLS 1.1、TLS 1.2 | TLS 1.1、TLS 1.2 | TLS 1.2 | TLS 1.1 | TLS 1.1、TLS 1.2 | TLS 1.2 |

| アプリケーション | プロトコル | 宛先/リスナー | 通常モードで動作する Cisco Unified Communications Manager | | | コモン クライテリア モードで動作する Cisco Unified Communications Manager | | |
|---|---|---|---|---|---|---|---|---|
| | | | 最低 TLS バージョン 1.0 | 最低 TLS バージョン 1.1 | 最低 TLS バージョン 1.2 | 最低 TLS バージョン 1.0 | 最低 TLS バージョン 1.1 | 最低 TLS バージョン 1.2 |
| コンピュータテレフォニーインテグレーション（CTI）[こんぴゅーたてれふぉにーいんてぐれーしょんCTI] | Quick Buffer Encoding（QBE）[QuickBufferEncoding QBE] | 2749 | TLS 1.0、TLS 1.1、TLS 1.2 | TLS 1.1、TLS 1.2 | TLS 1.2 | TLS 1.1 | TLS 1.1、TLS 1.2 | TLS 1.2 |
| CAPF-SERV | Transmission Control Protocol（TCP） | 3804 | TLS 1.0、TLS 1.1、TLS 1.2 | TLS 1.1、TLS 1.2 | TLS 1.2 | TLS 1.1 | TLS 1.1、TLS 1.2 | TLS 1.2 |
| クラスタ間検索サービス（ILS） | N/A | 7501 | TLS 1.0、TLS 1.1、TLS 1.2 | TLS 1.1、TLS 1.2 | TLS 1.2 | TLS 1.1 | TLS 1.1、TLS 1.2 | TLS 1.2 |
| Administrative XML（AXL） | Simple Object Access Protocol（SOAP） | 8443 | TLS 1.0、TLS 1.1、TLS 1.2 | TLS 1.1、TLS 1.2 | TLS 1.2 | TLS 1.1 | TLS 1.1、TLS 1.2 | TLS 1.2 |
| 高可用性プロキシ（HAProxy） | TCP | 9443 | TLS 1.2 | TLS 1.2 | TLS 1.2 | TLS 1.1 | TLS 1.2 | TLS 1.2 |
| SIP-SIG | Session Initiation Protocol（SIP） | 5061（トランクで設定可能） | TLS 1.0、TLS 1.1、TLS 1.2 | TLS 1.1、TLS 1.2 | TLS 1.2 | TLS 1.1 | TLS 1.1、TLS 1.2 | TLS 1.2 |

| アプリケーション | プロトコル | 宛先/リスナー | 通常モードで動作する Cisco Unified Communications Manager | | | コモン クライテリア モードで動作する Cisco Unified Communications Manager | | |
|---|---|---|---|---|---|---|---|---|
| | | | 最低 TLS バージョン 1.0 | 最低 TLS バージョン 1.1 | 最低 TLS バージョン 1.2 | 最低 TLS バージョン 1.0 | 最低 TLS バージョン 1.1 | 最低 TLS バージョン 1.2 |
| HA Proxy | [TCP] | 6971、6972 | TLS 1.2 | TLS 1.2 | TLS 1.2 | TLS 1.1 | TLS 1.1、TLS 1.2 | TLS 1.2 |
| Cisco Tomcat | HTTPS | 8080、8443 | 8443：TLS 1.0、TLS 1.1、TLS 1.2 | 8443：TLS 1.1、TLS 1.2 | 8443：TLS 1.2 | TLS 1.1 | 8443：TLS 1.1、TLS 1.2 | 8443：TLS 1.2 |
| 信頼検証サービス（TVS） | 専用 | 2445 | TLS 1.0、TLS 1.1、TLS 1.2 | TLS 1.1、TLS 1.2 | TLS 1.2 | TLS 1.1 | TLS 1.1、TLS 1.2 | TLS 1.2 |

### インスタント メッセージングと Presence のポートのうち Transport Layer Security バージョン 1.2 による影響を受けるもの

次の表は、Transport Layer Security バージョン 1.2 の影響を受ける IM and Presence Service ポートを示します。

表 *4 :* インスタント メッセージングと *Presence* のポートのうち *Transport Layer Security* バージョン *1.2* による影響を受けるもの

| 宛先/リスナー | 通常モードで動作するインスタント メッセージングと Presence | | | コモン クライテリア モードで動作するインスタント メッセージングと Presence | | |
|---|---|---|---|---|---|---|
| | 最低 TLS バージョン 1.0 | 最低 TLS バージョン 1.1 | 最低 TLS バージョン 1.2 | 最低 TLS バージョン 1.0 | 最低 TLS バージョン 1.1 | 最低 TLS バージョン 1.2 |
| 443 | TLS 1.0、TLS 1.1、TLS 1.2 | TLS 1.1、TLS 1.2 | TLS 1.2 | TLS 1.1 | TLS 1.1、TLS 1.2 | TLS 1.2 |
| 5061 | TLS 1.0、TLS 1.1、TLS 1.2 | TLS 1.1、TLS 1.2 | TLS 1.2 | TLS 1.1 | TLS 1.1、TLS 1.2 | TLS 1.2 |
| 5062 | TLS 1.0、TLS 1.1、TLS 1.2 | TLS 1.1、TLS 1.2 | TLS 1.2 | TLS 1.1 | TLS 1.1、TLS 1.2 | TLS 1.2 |

| 宛先/リスナー | 通常モードで動作するインスタントメッセージングと Presence | | | コモン クライテリア モードで動作するインスタント メッセージングと Presence | | |
|---|---|---|---|---|---|---|
| | 最低 TLS バージョン 1.0 | 最低 TLS バージョン 1.1 | 最低 TLS バージョン 1.2 | 最低 TLS バージョン 1.0 | 最低 TLS バージョン 1.1 | 最低 TLS バージョン 1.2 |
| 7335 | TLS 1.0、TLS 1.1、TLS 1.2 | TLS 1.1、TLS 1.2 | TLS 1.2 | TLS 1.1 | TLS 1.1、TLS 1.2 | TLS 1.2 |
| 8083 | TLS 1.0、TLS 1.1、TLS 1.2 | TLS 1.1、TLS 1.2 | TLS 1.2 | TLS 1.1 | TLS 1.1、TLS 1.2 | TLS 1.2 |
| 8443 | TLS 1.0、TLS 1.1、TLS 1.2 | TLS 1.1、TLS 1.2 | TLS 1.2 | TLS 1.1 | TLS 1.1、TLS 1.2 | TLS 1.2 |