TLS セットアップ

- TLS の概要 （1 ページ）
- TLS 前提条件 （1 ページ）
- TLS 設定タスク フロー （2 ページ）
- TLS の連携動作および制限 （7 ページ）

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やデータ転送を実現します。 TLS は、Unified Communications Manager が制御するシステム、デバイス、プロセス間の接続を保護および制御し、音声ドメインへのアクセスを防止します。

TLS 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、メディアの終了点（MTP）、Xcoder、Prime Collaboration Assurance、Prime Collaboration Provisioning、Cisco Unity Connection、Cisco Meeting Server、Cisco IP 電話、Cisco Room Devices、Fusion Onboarding Service（FOS）などのクラウドサービス、Common Identity Service、Smart License Manager（SLM）、プッシュ REST サービス、Cisco Jabber および Webex アプリクライアントと他のサードパーティ アプリケーション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

以下のタスクを完了して、TLS 接続用に Unified Communications Manager 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	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。 セキュリティがより高いバージョンの TLS を必要とする場合、システムは TLS 1.1 または1.2を使用するように再設定する必要があります。
ステップ 2	（任意） TLS 暗号化の設定 （3 ページ）.	Unified Communications Manager がサポートする TLS 暗号オプションを設定します。
ステップ 3	SIP トランク セキュリティ プロファイルでの TLS の設定 （4 ページ）.	TLS 接続を SIP トランクに割り当てます。 このプロファイルを使用するトランクは、シグナリングに TLS を使用します。 セキュアなトランクを使用して、会議ブリッジなどのデバイスに TLS 接続を追加することもできます。
ステップ 4	SIP トランクへのセキュア プロファイルの追加 （4 ページ）.	TLS が有効な 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、トランクが TLS をサポートできるようにします。 セキュアなトランク

	コマンドまたはアクション	目的
		を使用して、電話会議ブリッジなどのリソースに接続できます。
ステップ 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）.	TLS 接続を電話セキュリティプロファイルに割り当てます。 このプロファイルを使用する電話は、シグナリングに TLS を使用します。
ステップ 6	セキュアフォンプロファイルを電話に追加する （6 ページ）.	作成した TLS が有効なプロファイルを電話に割り当てます。
ステップ 7	セキュア電話プロファイルをユニバーサルデバイステンプレートに追加する （7 ページ）.	TLS が有効な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ます。 このテンプレートで LDAP ディレクトリ同期を設定すると、LDAP 同期で電話に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 前提条件 （1 ページ）を参照してください。

ステップ 1 **コマンドライン インターフェイス**にログインします。

ステップ 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。

ステップ 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。

（注） リリース 15SU1 までは、すべての Unified Communications Manager および IM and Presence Service のサービスクラスタノードで、**ステップ 3** を実行します。

TLS 暗号化の設定

SIP インターフェイスの使用可能な最も強力な暗号化を選択することによって、弱い暗号化を無効にできます。 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。

ステップ 1 Cisco Unified CM Administrationから、**[システム]** > **[企業パラメータ]** を選択します。

ステップ 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。

ステップ 3 **[保存]** をクリックします。

（注） すべての TLS 暗号は、クライアント暗号の設定に基づいてネゴシエートされます。

SIP トランク セキュリティ プロファイルでの TLS の設定

この手順を使用して、TLS接続をSIPトランクセキュリティプロファイルに指定します。 このプロファイルを使用するトランクは、シグナリングに TLS を使用します。

ステップ 1 Cisco Unified CM Administration から、**[システム（System）]** > **[セキュリティ（Security）]** > **[SIPトランクのセキュリティプロファイル（SIP Trunk Security Profile）]** を選択します。

ステップ 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、既存のテンプレートを選択します。

ステップ 3 [**名前**] フィールドにプロファイルの名前を入力します。

ステップ 4 **端末セキュリティモード** フィールドの値を **暗号化** または **認証済み**に設定します.

ステップ 5 **[着信トランスポートタイプ（Incoming Transport Type）]** と **[発信トランスポートタイプ（Outgoing Transport Type）]** の両方のフィールド値を **[TLS]** に設定します。

ステップ 6 [**SIP トランクセキュリティプロファイル**] 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。

ステップ 7 **[保存（Save）]** をクリックします。

（注） この注意事項は、リリース 15SU2 以降に適用されます。 Unified CM でサポートされている最小の TLS バージョンが 1.3 に設定されている場合、端末セキュリティモード **[認証済み]（Authenticated）]** のトランクは宛先との接続に失敗します。

SIP トランクへのセキュア プロファイルの追加

この手順を使用して、TLS が有効な SIP トランクセキュリティプロファイルを SIP トランクに指定します。 このトランクを使用して、会議ブリッジなどのリソースへの安全な接続を作成できます。

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[トランク（Trunk）]** を選択します。

ステップ 2 **[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。

ステップ 3 [**端末名**] フィールドにトランクの端末名を入力します。

ステップ 4 [**端末プール**] ドロップダウンリストから端末プールを選択します。

ステップ 5 [**SIP プロファイル**] ドロップダウンリストから、SIP プロファイルを選択します。

ステップ 6 [**SIP トランクセキュリティプロファイル**] ドロップダウンリストから、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。

ステップ 7 **宛先** エリアに宛先 IP アドレスを入力します。 最大 16 件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。

ステップ 8 **トランク設定**ウィンドウの残りのフィールドをすべて入力します。 フィールドとその設定に関するヘルプは、オンラインヘルプを参照してください。

ステップ 9 **[保存（Save）]** をクリックします。

（注） トランクをセキュア デバイスに接続している場合、セキュア デバイスの証明書を Unified Communications Manager に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** の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

この手順を使用して、TLS 接続を電話セキュリティ プロファイルに指定します。 このプロファイルを使用する電話は、シグナリングに TLS を使用します。

ステップ 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。

ステップ 2 次のいずれかの手順を実行します。

- 新しいプロファイルを作成するには、[新規追加（Add New）]をクリックします。
- **[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。

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

（注） ユニバーサル端末テンプレートと LDAP 同期を使用して、LDAP 同期によるセキュリティのプロビジョニングを行う場合は、[**電話セキュリティプロファイルタイプ**] で [**Universal Device Template] を選択します**。

ステップ 4 プロファイルの名前を入力します。

ステップ 5 [デバイスのセキュリティモード（Device Security Mode）]ドロップダウンリストから、[暗号化（Encrypted）] または [認証済み（Authenticated）]を選択します。

ステップ 6 (SIP 電話のみ) 転送タイプから、 **TLS** を選択します。

ステップ 7 [電話のセキュリティプロファイルの設定（Phone Security Profile Configuration）]ウィンドウで、残りのフィールドを設定します。 フィールドとその設定に関するヘルプは、オンラインヘルプを参照してください。

ステップ 8 **[保存（Save）]** をクリックします。

（注） この注意事項は、リリース 15SU2 以降に適用されます。 端末セキュリティ モードを **認証済み** に設定すると、電話は登録用に 1.3 以前の TLS バージョンに切り替わります。

Unified CM でサポートされる最小の TLS バージョンが 1.3 に設定されている場合、 **認証済み** 端末セキュリティモードの電話は登録されません。

セキュアフォンプロファイルを電話に追加する

この手順を使用して、TLS が有効な電話セキュリティプロファイルを電話に指定します。

（注） 一度に多数の電話にセキュリティプロファイルを割り当てるには、一括管理ツールを使用して、それらの電話にセキュリティ プロファイルを再割り当てします。

ステップ 1 Cisco Unified CM 管理から、**[デバイス]** > **[電話機]** を選択します。

ステップ 2 次のいずれかの手順を実行します。

- 新しい電話機を作成するには、[新規追加] をクリックします。
- **[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。

ステップ 3 電話のタイプとプロトコルを選択し、**[次へ（Next）]** をクリックします。

ステップ 4 [**端末セキュリティプロファイル**] ドロップダウンリストから、作成したセキュリティプロファイルを電話に指定します。

ステップ 5 次の必須フィールドに値を指定します:

- 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)]

ステップ 6 [電話の設定（Phone Configuration）]ウィンドウで、残りのフィールドを入力します。 フィールドとその設定に関するヘルプは、オンラインヘルプを参照してください。

ステップ 7 **[保存（Save）]** をクリックします。

セキュア電話プロファイルをユニバーサル デバイス テンプレートに追加する

この手順を使用して、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 テンプレートに指定します。 LDAP ディレクトリ同期を構成している場合、機能グループ テンプレートとユーザ プロファイルを通じて、このユニバーサル デバイス テンプレートを LDAP 同期に含めることができます。 同期が行われると、セキュアプロファイルが電話にプロビジョニングされます。

ステップ 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** > **ユーザ/電話追加** > **ユニバーサル端末テンプレート**。

ステップ 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。

ステップ 3 [**名前**] フィールドにテンプレートの名前を入力します。

ステップ 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。

ステップ 5 **[端末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 対応のセキュリティプロファイルを選択します。

（注） 電話セキュリティ プロファイルは、 **Universal Device Template** を端末タイプとして使用して作成されている必要があります。

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

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

ステップ 8 **[ユニバーサルデバイステンプレートの設定（Universal Device Template Configuration）]** ウィンドウで、残りのフィールドを入力します。 フィールドとその設定に関するヘルプは、オンラインヘルプを参照してください。

ステップ 9 **[保存（Save）]** をクリックします。
LDAP ディレクトリ同期にユニバーサル 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セットアップ方法については、『Cisco Unified Communications Manager システム設定ガイド』の「「エンドユーザーの設定」」の部分を参照してください。

TLS の連携動作および制限

この章では、TLS 相互作用と制限に関する情報を提供します。

TLS の連携動作

表 *1 : TLS* の連携動作

機能	データのやり取り
共通基準モード	最小 TLS バージョンの構成と共に、Common Criteria モードを有効にできます。 有効にする場合、アプリケーションは引き続き共通基準の要件に準拠し、TLS 1.0 セキュア接続をアプリケーション レベルで無効にします。 共通基準モードが有効な場合、アプリケーションの最小 TLS バージョンを 1.1 または 1.2 のいずれかとして設定できます。 コモンクライテリアモードの詳細については、『 *Cisco Unified Communications Solutions* コマンドラインインターフェイスリファレンスガイド』の「コモンクライテリアへの準拠」を参照してください。

TLS の制限

次の表では、79xx、69xx、89xx、99xx、39xx、IP Communicator などのレガシー電話に 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がある問題を示します。 お使いの電話がこのリリースでセキュア モードをサポートしているかどうかを確認するには、Cisco Unified Reporting の電話機能リスト レポートを参照してください。 レガシー電話の機能制限とこの機能を実装するための回避策を次の表に示します。

（注） 回避策は、影響を受ける機能がシステムで機能するように設計されています。 ただし、その機能の TLS 1.2 準拠は保証されません。

表 *2 : Transport Layer Security* バージョン *1.2* の制限

機能	制約事項
暗号化モードの旧型の電話	暗号化モードの旧型の電話は機能しません。 回避策はありません。
認証モードの旧型の電話	認証モードのレガシー電話は機能しません。 回避策はありません。

機能	制約事項
HTTPSに基づくセキュアな 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 電話サービスは機能しません。 IP 電話サービスを使用するための回避策: 基礎とな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、企業ディレクトリとパーソナル ディレクトリです。 ただし、Extension Mobilityなどの機能のために機密データを入力する必要がある場合、HTTPは安全性が低いため、推奨されません、特に機密データを入力する必要がある場合。 HTTP の使用には、次のような欠点があります。 • レガシー電話に HTTP を設定し、サポートされている電話に HTTPS を設定する際のプロビジョニングの課題。 • IP 電話サービスにはレジリエンスがありません。 • IP電話サービスを処理するサーバのパフォーマンスが影響を受ける場合があります。
レガシー電話の Extension Mobility Cross Cluster (EMCC)	EMCC は、TLS 1.2 を使用した従来の電話ではサポートされていません。 回避策: 以下のタスクを完了して EMCC を有効にします。 1. HTTPS の代わりに HTTP 上の EMCC を有効にします。 2. すべての Unified Communications Manager クラスタで混合モードをオンにしてください。 3. すべての Unified Communications Manager クラスタに同じ USB eToken を使用してください。
レガシー電話でのローカルに重要な証明書 (LSC)	LSC は従来の電話の TLS 1.2 では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 認証は利用できません。 802.1x の回避策: 古い電話の EAP-MD5 を使用した MIC またはパスワードに基づく認証。 ただし、これらはお勧めできません。 VPN 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 認証を使用します。
暗号化された Trivial File Transfer Protocol (TFTP) 構成ファイル	暗号化されたトリビアル ファイル転送プロトコル (TFTP) 構成ファイルは、製造元がインストールした証明書 (MIC) があっても、従来の電話の TLS 1.2 ではサポートされていません。 回避策はありません。

機能	制約事項
CallManager 証明書の更新により、レガシー電話の信頼が失われます。	レガシー電話は、CallManager証明書が更新されると信頼を失います。たとえば、証明書を更新した後は、電話は新しい設定を取得できません。 これは Unified Communications Manager 11.5.1 にのみ適用されます。 回避策: 従来の電話の信頼性が失われるのを防ぐには、次の手順を実行します。 1. CallManager証明書を有効にする前に、**[8.0 以前にロールバックするためのクラスタ（Cluster For Roll Back to Pre 8.0）]** エンタープライズパラメータを **[はい（True）]** に設定します。 既定では、この設定によりセキュリティが無効になります。 2. 一時的に TLS 1.0 を許可します (複数の Unified Communications Manager のリブート)。
サポートされていないバージョンの Cisco Unified Communications Manager に接続する	上位の TLS バージョンをサポートしていない古いバージョン Unified Communications Manager への TLS 1.2 接続は機能しません。 たとえば、 Unified Communications Manager リリース 9.x への TLS 1.2 SIP トランク接続は機能しません。このリリースは TLS 1.2 をサポートしていないためです。 以下のいずれかの回避策を使用できます。 • 接続を有効にするための回避策: 推奨されるオプションではありませんが、セキュアではないトランクを使用することができます。 • TLS 1.2 使用中に接続を有効にする回避策: サポートされていないバージョンを TLS 1.2 をサポートするリリースにアップグレードすることができます。
証明書信頼リスト (CTL) クライアント	CTL クライアントは TLS 1.2 をサポートしません。 以下のいずれかの回避策を使用できます。 • CTL クライアントの使用時に TLS 1.0 を一時的に許可し、その後クラスタを Common Criteria モードに移動することができます。最小 TLS を 1.1 または 1.2 に設定する • トークンレス CTL に移行するには、CLI コマンド **utils ctl set-cluster 混合モード** を共通基準モードで使用します。 最小TLS を 1.1 または 1.2 に設定する
アドレス帳シンクロナイザー	回避策はありません。

Transport Layer Security バージョン 1.2 の影響を受ける Cisco Unified Communications Manager ポート

Unified Communications Manager TLS バージョン 1.2 の影響を受けるポートを次の表に示します:

表 *3 : Transport Layer Security* バージョン *1.2* の影響を受ける *Cisco Unified Communications Manager* ポート

アプリケーション (Application)	プロトコル	宛先/リスナー	通常モードで動作している Cisco Unified Communications Manager			共通基準モードで動作する Cisco Unified Communications Manager		
			最小 TLS バージョン 1.0	最小 TLS バージョン 1.1	最小 TLS バージョン 1.2	最小 TLS バージョン 1.0	最小 TLS バージョン 1.1	最小 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 - SEC - SIG	シグナリング接続コントロール部 (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
コンピュータテレフォニー インテグレーション（CTI）	クイックバッファエンコーディング (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
クラスター間検索サービス (ILS)	なし	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

アプリケーション (Application)	プロトコル	宛先/リスナー	通常モードで動作している Cisco Unified Communications Manager			共通基準モードで動作する Cisco Unified Communications Manager		
			最小 TLS バージョン 1.0	最小 TLS バージョン 1.1	最小 TLS バージョン 1.2	最小 TLS バージョン 1.0	最小 TLS バージョン 1.1	最小 TLS バージョン 1.2
管理 XML (AXL)	シンプルオブジェクトアクセスプロトコル (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 (HA プロキシ)	[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 (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
HA プロキシ	[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
Trust Verification Service (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プレゼンスサービスのポートに Transport Layer Security バージョン 1.3 が適用される

次の表は、Transport Layer Security バージョン 1.2 が適用される IM and Presence Service ポートの一覧です:

表 *4 : TLS* バージョン *1.2* の影響を受けるインスタントメッセージ *&* プレゼンス ポート

宛先/リスナ	インスタントメッセージおよびプレゼンスは通常モードで動作しています			インスタントメッセージおよびプレゼンスは共通基準モードで動作しています		
	最小 **TLS** バージョン **1.0**	最小 **TLS** バージョン **1.1**	最小 **TLS** バージョン **1.2**	最小 **TLS** バージョン **1.0**	最小 **TLS** バージョン **1.1**	最小 **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
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

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。