オンプレミス Cisco Collaboration 導入のための TLS 1.2

初版：2017 年 10 月 5 日
最終更新日：2018 年 4 月 20 日

はじめに

Transport Layer Security (TLS) およびその前身である Secure Socket Layer (SSL) は、ネットワーク上で通信のセキュリティを提供する暗号プロトコルです。 ただし、SSL、TLS 1.0、および場合によっては TLS 1.1 は、組織が要求するレベルのセキュリティを提供できない場合があります。 多くの組織では TLS 1.2 が必要となる場合があります。

このホワイトペーパーでは、TLS 1.2 のサポートおよびオンプレミスの Cisco Collaboration 展開において、低いバージョンの TLS を無効化する機能について説明しています。 また、TLS 1.0 および 1.1 を無効にした場合の影響についても論じています。 ただし、TLS 1.2 における暗号スイートのサポートについては扱っていません。

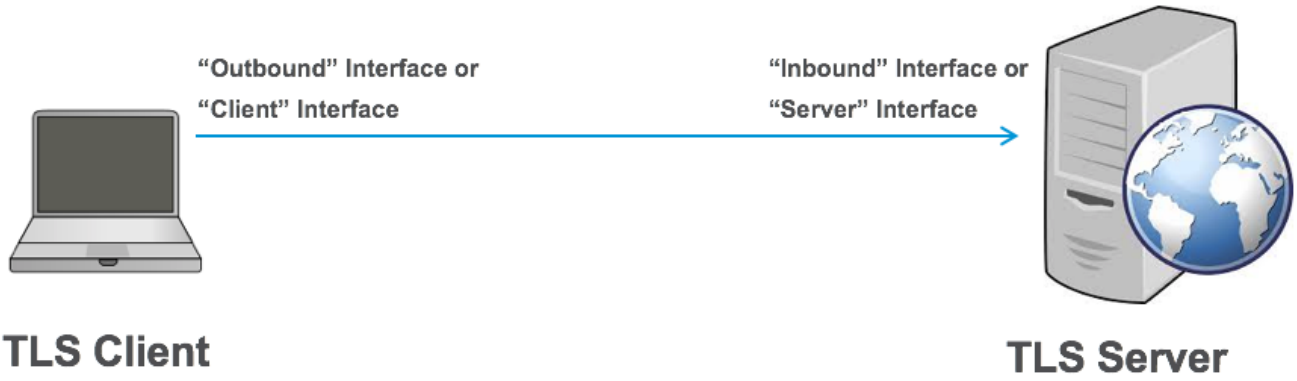
この文書は、以下の文書を補完するものです。

- *Cisco Collaboration 製品の TLS 1.2 互換性マトリックス*: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/unified/communications/system/Compatibility/TLS/TLS1-2-Compatibility-Matrix.html
- *TLS 1.2 設定概要ガイド*: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/TLS/TLS-1-2-Configuration-Overview-Guide.html

用語 – TLS クライアントおよびサーバーインターフェイス

TLS 接続では、TLS リクエストを開始するデバイスは TLS **クライアント**と呼ばれ、そのインターフェイスは**アウトバウンドインターフェイス**または**クライアントインターフェイス**と呼ばれます。 一方、接続のもう一端で TLS リクエストを受信するデバイスは TLS **サーバー**と呼ばれ、そのインターフェイスは**インバウンドインターフェイス**または**サーバーインターフェイス**と呼ばれます。 図 1 は、この用語の関係を示す図です。

図 1: TLS クライアントと TLS サーバー



コラボレーションソリューションにおいて、エンドポイントまたは電話機はクライアントとみなされます。 Cisco Unified Communications Manager（Unified CM）のようなアプリケーションは、Cisco Collaboration 展開における主要な機能に基づき、サーバーとして扱われます。 しかし、TLS 接続の観点から見ると、クライアントとサーバーの定義は異なります。 1 つのデバイスは、クライアントインターフェイスとサーバーインターフェイスの両方を持つことがあります。 たとえば、エンドポイントは、コールシグナリング（SIP または SCCP）のためのインターフェイスを持ち、これが暗号化される場合、Unified CM に対して TLS クライアントとして動作します。一方で、エンドポイントは内部 Web サーバーへの Web インターフェイスも持っており、これが HTTPS により暗号化される場合、そのエンドポイントは TLS サーバーとして動作します。 図 2 は、エンドポイント上の TLS サーバーインターフェイスと TLS クライアントインターフェイスの例を示しています。 同様に、Unified CM はセキュア LDAP インターフェイスなどの TLS クライアントインターフェイスを持つ一方で、Web インターフェイスのような TLS サーバーインターフェイスも備えています。 また、Unified CM の SIP インターフェイスは、TLS クライアントおよび TLS サーバーインターフェイスの両方として機能します。 図 3 には、Unified CM のいくつかのインターフェイスが示されています。

図 2: エンドポイントにおける TLS サーバーおよび TLS クライアントインターフェイスの例

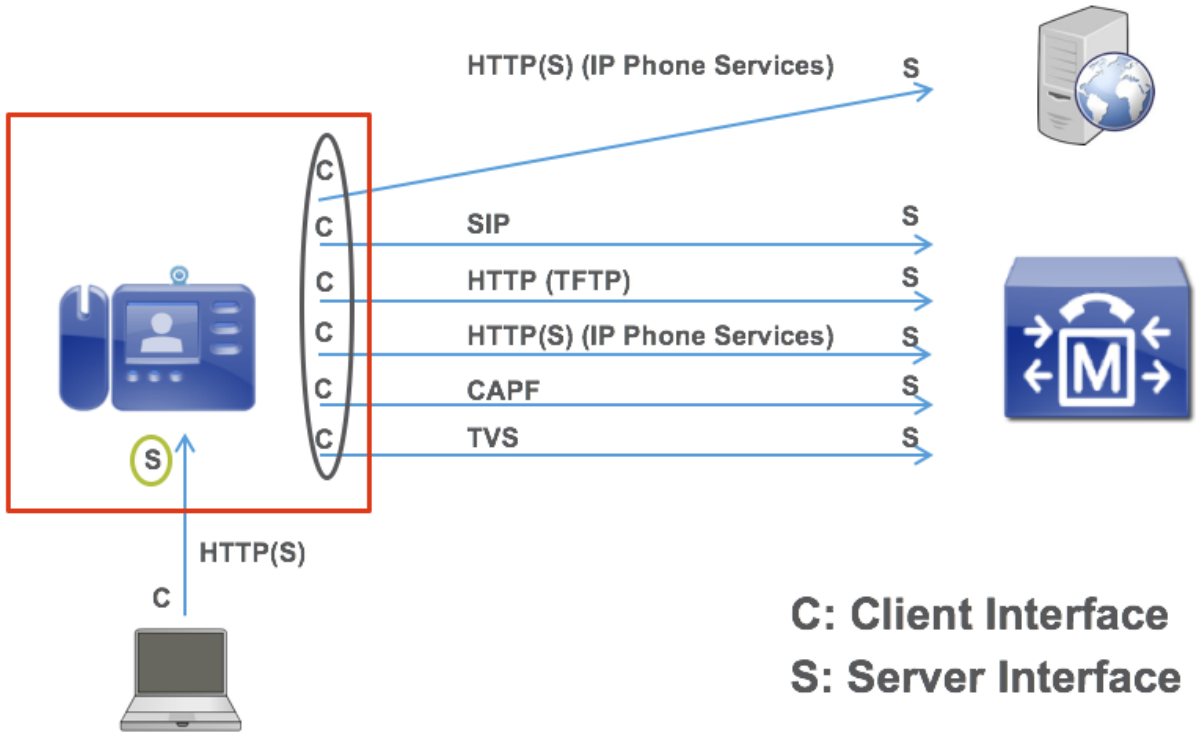
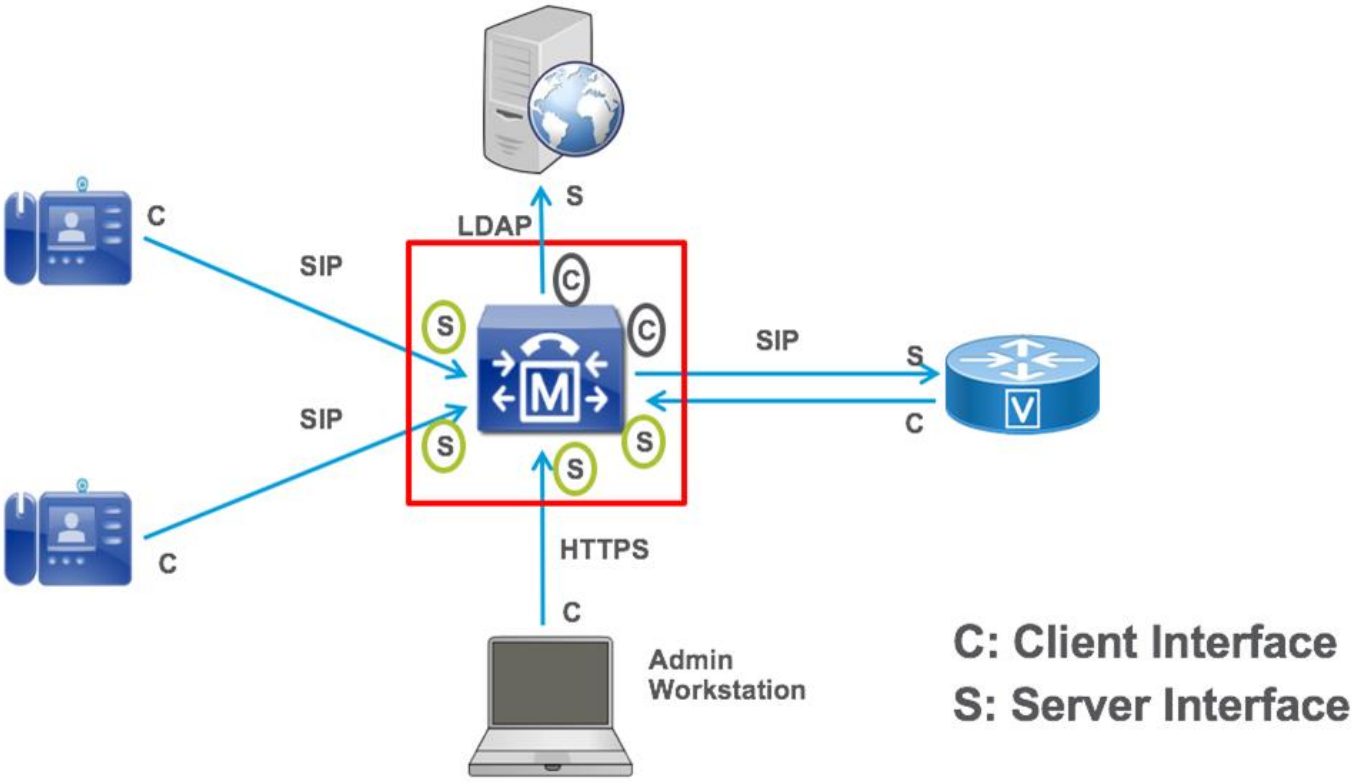


図3: Unified CM における TLS サーバーおよび TLS クライアントインターフェイスの例



TLS バージョンネゴシエーションのデフォルトは TLS 1.2 です

TLS クライアントと TLS サーバーの両方が TLS 1.2 をサポートしている場合、TLS 1.0 および TLS 1.1 もサポートしていたとしても、デフォルトでは TLS バージョン 1.2 がネゴシエートされます。

TLS ハンドシェイクは、TLS 接続を開始します。 TLS ハンドシェイクの開始時に、TLS クライアントは TLS バージョンを含む ClientHello を送信します。 TLS クライアントが TLS 1.0、1.1、および 1.2 をサポートしている場合、デフォルトでは最初に TLS バージョンを 1.2 に設定した ClientHello を送信します。 TLS サーバーが TLS 1.2 もサポートしている場合、TLS バージョンを 1.2 に設定した ServerHello で応答します。 クライアントまたはサーバーが TLS 1.0/1.1 もサポートしている場合でも、この時点で TLS バージョンのネゴシエーションは完了しています。

しかし、最初の TLS 1.2 ハンドシェイクに問題があった場合、TLS クライアントは後続の ClientHello メッセージで TLS 1.0 または 1.1 を示します。 通常の TLS ネゴシエーションは図 3 に示されています。

図 3: TLS クライアントとサーバーが TLS 1.2 およびそれ以前の TLS バージョンをサポートしている場合にネゴシエートされる TLS 1.2

Cisco Collaboration Systems Release 12.0 のほとんどのコンポーネントは、TLS 1.2 をサポートしています。
TLS 1.2 をサポートする Cisco Collaboration 製品の一覧については、
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/unified/communications/system/Compatibility/TLS/TLS1-2-Compatibility-Matrix.html にある *「Cisco Collaboration 製品の TLS 1.2 互換性マトリクス」*を参照してください。

注: SSL は、Cisco コラボレーション製品のほとんど、および *Cisco コラボレーション製品の TLS 1.2 互換性マトリックスに記載されているすべての製品から削除されました。*

TLS 1.0/1.1 の無効化

TLS 1.2 をサポートするデバイス間では、TLS 1.0 および TLS 1.1 もサポートしている場合であっても、常に TLS バージョン 1.2 がネゴシエートされる必要があります。 しかし、TLS ハンドシェイクを改ざんし、TLS の低バージョン、あるいは SSL をネゴシエートしようとする中間者攻撃（MitM 攻撃）が存在する可能性がある。 これを防ぐには、TLS 1.0（および TLS 1.1）を無効にして、すべての TLS 通信を TLS 1.2（および TLS 1.1）のみに制限します。 *「Cisco コラボレーション製品の TLS 1.2 互換性マトリクス」*は、TLS バージョン 1.0 および 1.1 を無効化できる Cisco Collaboration 製品の最小バージョンを示しています。

TLS 接続における TLS 1.0/1.1 の無効化は、理論的にはクライアントインターフェイスまたはサーバーインターフェイスのいずれかで実行可能であり、両方のインターフェイスタイプで実行する必要はありません。 Cisco Collaboration 製品では、これはサーバーインターフェイス上で行われます。 管理者が TLS 1.0/1.1 を無効にすると、TLS サーバーインターフェイスは TLS 1.0/1.1 を許可しなくなります。 場合によっては、TLS サーバーインターフェイスに加えて、TLS 1.0/1.1 の無効化は TLS クライアントインターフェイスにも適用されることがあります。たとえば、Unified CM における LDAP クライアントインターフェイスや SIP クライアントインターフェイスがこれに該当します。

図 4 は、TLS 1.0 および 1.1 を無効にする設定がサーバーインターフェイスに適用され、TLS 接続のバージョンが 1.2 に制限される典型的な実装を示しています。 これは *「Cisco Collaboration 製品の TLS 1.2 互換性マトリクス」*に記載されています。 製品のすべての TLS サーバーインターフェイスが TLS バージョン 1.0 および 1.1 を無効にできる場合、その製品は TLS バージョン 1.0/1.1 を無効にできるとみなされます。 クライアントインターフェイスでは、TLS 1.0 および TLS 1.1 が引き続き許可されている場合があります。 このマトリックスは、クライアントインターフェイスで TLS 1.0/1.1 を無効にする機能を追跡していません。

図 4：TLS 1.0/1.1 を無効にするための設定（サーバーインターフェイスに適用）

TLS 1.0/1.1 を無効にすると、一部のコンポーネントが TLS 1.2 をサポートしていない場合、互換性の問題が発生する可能性があります。 TLS 1.0/1.1 を無効にする前に、展開環境内のすべての製品が TLS 1.2 をサポートしていることを確認し、次のセクションで説明する制限事項を考慮してください。

TLS 1.0/1.1 を無効にする際の制限事項

製品上で TLS のバージョンを無効にする場合は、その製品に接続している他の製品とネゴシエート可能な共通の TLS バージョンが引き続き存在することを確認してください。 例えば、Unified CM で TLS 1.0 と TLS 1.1 を無効にする場合は、TLS 接続を介して Unified CM に接続するすべての製品が TLS 1.2 をサポートしていることを確認してください。 そうでない場合、相互運用性の問題が発生する可能性があります。

TLS 1.2 をサポートする製品の一覧については、 *「Cisco Collaboration 製品の TLS 1.2 互換性マトリクス」*を参照してください。

以下のセクションでは、TLS 1.0/1.1 を無効にすることによる主な制限事項について説明します。

Unified CM で TLS 1.0/1.1 を無効にする際の制限事項

Unified CM ノードで TLS 1.0/1.1 を無効にすると、TLS の最小バージョンが設定され、そのバージョンが Unified CM ノード内のすべてのサーバーインターフェイス（HTTPS Web サーバーインターフェイス、SIP サーバーインターフェイス、Certificate Trust List（CTL）プロバイダーサーバーインターフェイスなど）に適用されます。 また、SIP クライアントインターフェイスや LDAP クライアントインターフェイスなど、一部のクライアントインターフェイスにもこのバージョンが適用されます。 Unified CM の最小 TLS バージョンを TLS 1.1 または 1.2 に設定すると、以下の制限事項が適用されます。

- **証明書信頼リストクライアント**
  Unified CM における主な制約は、証明書信頼リスト（CTL）クライアントに関するものです。 Unified CM の混合モードを有効にするために USB eToken で使用される CTL クライアントは、Unified CM 12.0 でも TLS 1.2 をサポートしていません。
  - **回避策**: 混合モードを有効にする場合、または CTL ファイルを更新する場合は、Unified CM で一時的に TLS 1.0 を有効にします。
  - **回避策**: トークンレス CTL (CLI ベース) に移行します。

- Cisco IP 電話 Address Book Synchronizer
  Cisco IP 電話 Address Book Synchronizer は、ユーザーが Microsoft Windows Address Book を Cisco 個人用アドレス帳と同期できるようにします。 このクライアントは TLS 1.0 のみをサポートしています。
    - **回避策**: 回避策はありません。
- **古いリリースを実行している Unified CM クラスタとの相互接続**
  Unified CM 10.5(2) より前のリリースは TLS 1.2 をサポートしていません。 したがって、ローカルの Unified CM クラスタで TLS バージョンを制限すると、古いクラスタとの相互接続が制限される可能性があります。 たとえば、セキュア SIP トランク、セキュアロケーション帯域幅管理情報（LBM）、クラスタ間検索サービス（ILS）、および Extension Mobility Cross Cluster（EMCC）で使用されるリモートクラスタ検出サービスなどが機能しない可能性があります。
    - **回避策** : Unified CM 10.5(2) では、SIP など多くのインターフェイスで TLS 1.2 のサポートが導入されましたが、すべての Unified CM インターフェイスで TLS 1.2 をサポートするには、Unified CM 11.5(1)SU3 以降を導入する必要があります。
- **SIP トランクを介した旧製品との相互接続**
  TLS 1.0/1.1 の無効化は、SIP サーバーインターフェイスと SIP クライアントインターフェイスに適用されます。
    - **回避策**: Unified CM ノードが SIP トランク経由で接続する製品も TLS 1.2 をサポートしていることを確認してください。 たとえば、Cisco Unified Border Element（CUBE）を導入している場合は、TLS 1.2 をサポートするリリースで動作していることを確認してください。
- **古い電話機との相互運用性**
    - この制約については、次のセクションで説明します。

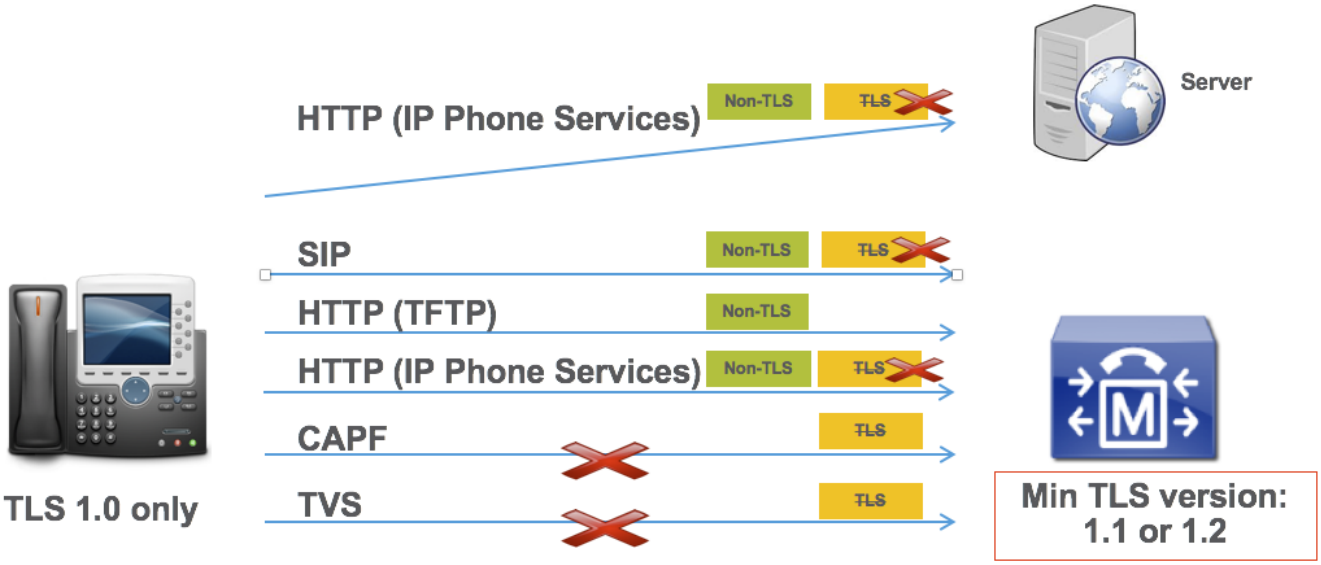
古い電話機の制限

Unified CM で TLS 1.0/1.1 を無効化すると、Cisco Unified IP Phone 8961、Cisco Unified IP Phone 9900、7900、6900、3900 シリーズ、および Cisco IP Communicator などの古い電話機に大きな影響を及ぼす可能性があります。

これらの古い電話機は TLS 1.1 および TLS 1.2 をサポートしていません。 したがって、Unified CM で最小 TLS バージョンが 1.1 または 1.2 に設定されている場合、TLS 接続を確立することはできません。 IP Phone サービスで使用される SIP および HTTP については、回避策として暗号化されていない接続を使用することができますが、これはセキュリティ上の問題となる可能性があります。 一信頼検証サービス（TVS）や認証局プロキシ機能（CAPF）などの他の Unified CM インターフェイスは TLS のみを許可しており、暗号化されていない接続は利用できません。そのため、これらのサービスは古い電話機では利用できなくなります。

Unified CM で最小 TLS バージョンを 1.1 または 1.2 に設定した場合の接続例については、図 5 を参照してください。 暗号化されていない接続であれば、一部の接続は依然として可能な場合があります。 TLS のみをサポートする他の接続は動作しなくなります。

図 5: TLS 1.1 または 1.2 が Unified CM の最小バージョンとして設定されている場合の古い電話機との接続



以下のセクションでは、これらの制限事項と可能な回避策についてさらに詳しく説明します。

SIP インターフェイス

電話機が認証モードまたは暗号化モードで構成されている場合、TLS 接続（暗号化された SIP または暗号化された SCCP）を介して Unified CM に登録されます。 電話機の SIP インターフェイスが TLS 1.2 をサポートしておらず、Unified CM が最小 TLS バージョンを 1.2 に設定して構成されている場合、この接続は確立できません。 さらに、このモードで構成されている場合、セキュリティ上の理由により、電話機は非 TLS 接続を使用して登録を試行しません。 そのため、エンドポイントは登録できず、通話の発信や受信もできなくなります。

回避策: 電話機を非セキュアモードで設定します。

IP Phone サービス用 HTTPS Web サーバーインターフェイス

IP 電話サービス用の Unified CM ウェブサービスに接続する電話クライアントインターフェイスは、古い電話機では TLS 1.2 をサポートしていません。 したがって、電話機が HTTPS を使用して IP 電話サービスに接続しようとすると、IP 電話サービスは動作しません。 電話機が IP Phone サービスインターフェイスで HTTPS をサポートしていない場合（例：7940/7960）、設定されているセキュア URL は無視され、HTTPS は使用されず、非セキュア URL が使用されます。 この場合、IP Phone サービスは動作します。 ただし、電話機が HTTPS をサポートしている場合は、セキュリティ上の理由により、セキュア URL が設定されている場合、またはデフォルト設定で組み込みの Cisco IP Phone Service（例：Application:Cisco/CorporateDirectory）が使用されている場合には、HTTPS のみを使用し、HTTP へのフォールバックは行われません。 古い電話機では TLS 1.2 がサポートされていないため、IP Phone サービスは完全に利用できなくなります。 この制限は、ここで扱っている多くの古い電話機のほとんど（例：7941/7961、または新しい 7900 モデル、6900、9900、8961 モデルなど）にも適用されます。

回避策：導入環境内のすべての電話機で、非セキュア URL（HTTPS ではなく HTTP）を使用してください。 ただし、HTTP は安全ではないため推奨されず、特に Extension Mobility のユーザー ID や PIN などの機密データが送信される場合には懸念があります。 また、デフォルトの Cisco IP Phone Service（例：Application:Cisco/CorporateDirectory）では、特定の URL を使用することには欠点があります。 これらのデフォルトの Cisco IP Phone Service がデフォルト設定されている場合、電話機は CM グループに設定された Unified CM ノードを使用し、呼処理と同じ優先順に従います。 プライマリの Unified CM コール処理サブスクライバに障害が発生した場合でも、電話機はセカンダリのコール処理サブスクライバにフェールオーバーします。 ただし、URL を個別に設定すると単一のサーバーが指定されるため、IP Phone サービスの冗長性が失われます。 も

う一つの欠点は、URL を設定する際に負荷が適切に分散されない可能性があることです。 すべての IP Phone サービスに同じサーバーが設定されている場合、そのサーバーのパフォーマンスに影響が出る可能性があります。

これらの問題を軽減するために、古い電話機には非セキュア URL（HTTP）を設定し、TLS 1.2 をサポートする新しい電話機には通常の構成（セキュア URL およびデフォルトの Cisco IP Phone Service）を使用することができます。 ただし、古い電話機に HTTP、新しい電話機に HTTPS を設定する場合、プロビジョニングの面で課題が生じます。 そのためには、HTTP ベースの IP Phone サービスと HTTPS ベースの IP Phone サービスをそれぞれ個別に追加し、各電話機を適切な IP Phone サービスに関連付ける必要があります。 また、Unified CM のエンタープライズパラメータページから一部のセキュア URL を削除し、その後、新しい電話機のみに対して再設定する必要が生じる場合もあります。

信頼検証サービスインターフェイス

信頼検証サービス（TVS）は、Unified CM のデフォルトのセキュリティアーキテクチャの主要コンポーネントです。 TVS は、電話機に代わって証明書を検証したり、電話機に証明書を提供したりすることができます。 たとえば、TVS はエンドポイントが IP Phone サービスに安全に接続できるようにします（HTTPS 経由）。 Unified CM 12.0 より前のリリースでは、エンドポイントが CallManager 証明書を更新したり、Unified CM クラスタ間を移行したりする際に、Unified CM を信頼するために TVS も使用されていました。 Unified CM 12.0 以降では、トークンレス CTL および ITL ファイルが ITLrecovery キーによって署名されるため、これらのシナリオでは通常 TVS は使用されません。

古いエンドポイントは、このインターフェイスで TLS 1.2 をサポートしていません。 TVS では TLS のみが利用可能なオプションであるため（暗号化されていない接続は許可されていない）、Unified CM が最小 TLS バージョンを 1.1 または 1.2 に設定して構成されている場合、古いエンドポイントは Unified CM TVS サービスに接続できません。 その影響は以下のとおりです。

- 古いエンドポイントは、外部の IP Phone サービス（Unified CM でホストされていないものを含む）であっても、IP Phone サービスに対してセキュア URL（HTTPS）を使用できません。
    - **回避策**: 安全でない URL (HTTP) を使用しますが、セキュリティ上の問題が発生する可能性があるため、推奨されません。 プロビジョニングに関する課題が発生する可能性もあります。
- Unified CM 11.5(1)SU3 およびそれ以降の SU では、CallManager 証明書を更新すると、古い電話機は Unified CM を信頼できなくなる場合があります。これは、電話機が新しい CallManager キーで署名された CTL および ITL ファイルを検証できないためです。 Unified CM リリース 12.0 以降では、トークンレス CTL および ITL ファイルは ITLrecovery キーで署名されているため、この問題は発生しません。
    - **回避策**：一時的にエンタープライズパラメータ Prepare Cluster for Rollback to pre 8.0 を True に設定します。
    - **回避策**: Unified CM で一時的に TLS 1.0 を許可します。
    - **回避策**: Unified CM 12.0 以降にアップグレードしてください。
- Unified CM 11.5(1)SU3 以降では、混合モードが有効になっていない場合、または CLI（トークンレス CTL）で有効になっている場合、古い電話機では Extension Mobility Cross Cluster（EMCC）は動作しません。 さらに、ある Unified CM クラスタから別の Unified CM クラスタへ電話機を移行するには、各電話機上の CTL/ITL ファイルを削除する必要があります。
    - **回避策**：USB eToken を使用して Unified CM 混合モードを有効にし、すべての Unified CM クラスタで同一の eToken を使用してください。
    - **回避策**: Unified CM 12.0 以降にアップグレードしてください。
- Unified CM 11.5(1)SU3 およびそれ以降の SU で、Proxy TFTP サーバーが導入されている場合、古い電話機はプロキシ TFTP サーバーによって署名された静的ファイル（着信音リストファイル、背景画像、ロケールなど）を検証できません。
    - **回避策**: Unified CM ホーム クラスタを Unified CM 12.0 以降にアップグレードします。

認証局プロキシ機能インターフェイス

Unified CM の認証局プロキシ機能（CAPF）サービスを使用すると、エンドポイント上でローカルに重要な証明書（LSC）を発行または更新したり、暗号化された TFTP 構成ファイルをサポートするために必要なエンドポイント証明書と公開鍵を取得したりするなど、証明書関連の操作を実行できます。

古いエンドポイントは、このインターフェイスで TLS 1.2 をサポートしていません。 CAPF では TLS のみが利用可能であり（非暗号化接続は許可されていないため）、Unified CM の最小 TLS バージョンが 1.2 に設定されている場合、古いエンドポイントは Unified CM の CAPF サービスに接続できなくなります。 その意味するところは以下のとおりです。

- LSC 証明書は古い電話機にはインストールできません。 したがって、LSC 証明書に基づくサービスは利用できません。 たとえば、802.1x 認証および Phone VPN は LSC 証明書に基づくことができません。
    - **回避策**: LSC 証明書に基づくサービスは、MIC 証明書やエンドユーザーの認証情報などの他の認証メカニズムに基づく必要があります。
- MIC 証明書を使用しても、暗号化された TFTP 設定ファイルは利用できません。
    - **回避策**：暗号化されていない TFTP 設定ファイルを使用してください。ただし、Unified CM Administration の電話ページで資格情報が設定されている場合など、セキュリティ上の懸念が生じる可能性があります。

古い電話機の制約と回避策のまとめ

Unified CM の最小 TLS バージョンが 1.1 または 1.2 に設定されている場合、Cisco Unified IP Phone 8961、Cisco Unified IP Phone 9900、7900、6900、3900 シリーズ、および Cisco IP Communicator などの古い電話機は完全には動作せず、重要な制限が発生します。 以下の表は、主な制限事項をまとめ、いくつかの回避策を示しています。 推奨される対応としては、これらの古い電話機を Cisco IP Phone 7800 や 8800 などの新しい電話機へアップグレードすることです。

表 1：Unified CM の最小 TLS バージョンが 1.1 または 1.2 の場合における古い電話機の制限と回避策の概要

機能	制限	回避策
SIP インターフェイス		
暗号化モードまたは認証モード	暗号化モードまたは認証モードの古い電話機は動作せず、Unified CM に登録できません。	それらの電話機を非セキュアモードで設定してください。
IP Phone サービス用 HTTPS Web サーバーインターフェイス		
セキュア URL（HTTPS）を使用する IP Phone サービス	古い電話機は、セキュア URL（HTTPS）を使用した IP Phone サービスに接続できません。	安全でない URL（HTTP）を使用することもできますが、セキュリティ上の問題が発生する可能性があるため、推奨されません。 プロビジョニングに関する課題が発生する可能性もあります。
信頼検証サービスインターフェイス		

CallManager 証明書の更新	Unified CM リリース 11.5(1)SU3 およびそれ以降の SU では、CallManager 証明書が更新されると、古い電話機は信頼を失います。 これは Unified CM 12.0 以降では発生しない問題です。	一時的にエンタープライズパラメータ Prepare Cluster for Rollback to pre 8.0 を True に設定します。 または Unified CM で TLS 1.0 を一時的に許可します。 または Unified CM 12.0 以降のバージョンにアップグレードしてください。
クラスタ間のエクステンションモビリティ（EMCC）	EMCC は、古い電話機および Unified CM 11.5(1)SU3 以降の SU において、混合モードが有効になっていない場合や CLI（トークンレス CTL）で有効になっている場合にはサポートされません。	USB eToken を使用して Unified CM 混合モードを有効にし、すべての Unified CM クラスタで同一の eToken を使用してください。 または Unified CM 12.0 以降のバージョンにアップグレードしてください。
プロキシ TFTP サーバー	Unified CM 11.5(1)SU3 およびそれ以降の SU で、Proxy TFTP サーバーが導入されている場合、古い電話機はプロキシ TFTP サーバーによって署名された静的ファイル（着信音リストファイル、背景画像、ロケールなど）を検証できません。	Unified CM のホームクラスタを Unified CM 12.0 以降のリリースへアップグレードしてください。
認証局プロキシ機能インターフェイス		
ローカルで有効な証明書 (LSC)	古い電話機では LSC をインストールまたは更新することができません。 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。	MIC 証明書やエンドユーザー資格情報など、他の認証メカニズムを使用してください。
暗号化された Trivial File Transfer Protocol (TFTP) 構成ファイル	古い機種では TFTP 設定ファイルを暗号化することはできません。	暗号化されていない TFTP 設定ファイルを使用し、Unified CM Administration の電話ページに資格情報を設定しないようにしてください。

TLS 1.0/1.1 無効化設定例

TLS 1.0 および TLS 1.1 を無効にするための設定方法は、製品によって異なります。 この例では、Unified CM の IM and Presence Service に加え、同じプラットフォームをベースとする製品（Cisco Unity Connection、Cisco Emergency Responder（Emergency Responder）、Cisco Prime Collaboration Deployment など）で TLS バージョンを無効にする方法を示しています。

注： 他の製品の構成情報については、関連する製品のドキュメントを参照してください。

デフォルトでは、Unified CM with IM and Presence Service、Cisco Unity Connection、Emergency Responder、または Cisco Prime Collaboration Deployment の場合、TLS の最小バージョンは 1.0 に設定されています。 TLS の最小バージョンを 1.1 に設定すると、TLS 1.0 が無効になります。 TLS の最小バージョンを 1.2 に設定すると、TLS 1.0 と TLS 1.1 が無効になります。

TLS 1.0 と TLS 1.1 を無効にするには、コマンドラインインターフェイスにログインし、 set tls min-version 1.2 CLI コマンドを実行します。

図 6 は、Unified CM（IM and Presence Service を含む）ノードで TLS の最小バージョンを設定する方法の例を示しています。 設定後、ノードは再起動します。 この設定はローカルノードにのみ適用されるため、クラスタ内のすべてのノードで TLS 1.0/1.1 を無効にする場合は、クラスタ内のすべてのノードにこの設定を適用してください。

図 6：Unified CM（IM and Presence Service を含む）で TLS 1.2 を最小バージョンとして設定する

```
admin:set tls min-version 1.2

This command will result in setting minimum TLS version to 1.2 on all the secure interfaces.
If you have custom applications that makes secure connection to the system, please ensure they support the TLS version you have chosen to configure.
Also, please refer to the Cisco Unified Reporting Administration Guide to ensure all the endpoints in your deployment supports this feature

********************************************************************************

Warning: This will set the minimum TLS to 1.2 and the server will reboot.

********************************************************************************

Do you want to continue (yes/no) ? yes

Successfully set minimum TLS version to 1.2

The system will reboot in a few minutes.
```

Unified CM および IM and Presence Service、Cisco Unity Connection、Emergency Responder、または Cisco Prime Collaboration Deployment で現在構成されている最小 TLS 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。

図 7：Unified CM（IM and Presence Service を含む）で設定された最小 TLS バージョンの確認

```
admin:show tls min-version
Configured TLS minimum version: 1.2
```

概要

現行の Cisco コラボレーション製品および現行リリースでは、SSL は無効になっており、TLS 1.2 がデフォルトでネゴシエートされるはずです。 TLS バージョンのダウングレード攻撃を防ぐため、TLS 1.0 と TLS 1.1 を無効にしてください。 TLS 1.0 および TLS 1.1 を無効にする前に、関連する TLS 接続に関与する他の製品が TLS 1.2 をサポートしていることを確認してください。 古い電話機を使用している場合、完全には動作せず、重要な制限が生じる可能性があります。 Cisco IP Phone 7800 シリーズや 8800 シリーズなどの最新機種へのアップグレードをお勧めします。

関連資料

- TLS 1.2 をサポートし、TLS 1.0 および TLS 1.1 を無効にできる Cisco Collaboration 製品の一覧については、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/unified/communications/system/Compatibility/TLS/TLS1-2-Compatibility-Matrix.html にある *「Cisco コラボレーション製品の TLS 1.2 互換性マトリクス」* を参照してください。 このマトリクスは、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-system/products-device-support-tables-list.html にある互換性情報ページからも参照できます。

- Cisco Collaboration 製品で TLS 1.2 を有効にし、TLS 1.0 および 1.1 を無効にする方法の概要については、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/TLS/TLS-1-2-Configuration-Overview-Guide.html にある『*TLS 1.2 Configuration Overview Guide*』を参照してください。
- TLS 1.0/1.1 の無効化、またはサーバーインターフェイスでの TLS 最小バージョンの設定については、https://www.cisco.com/ にある製品のサポートドキュメントを参照してください。
- Unified CM のセキュリティ情報については、https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html にある『*Cisco Unified Communications Manager セキュリティガイド*』を参照してください。
- Cisco Unity Connection のセキュリティ情報については、https://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html にある『*Cisco Unity Connection のセキュリティ ガイド*』を参照してください。
- Cisco Collaboration Systems リリースと互換性のある製品ソフトウェアのリリースバージョンについては、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/uc_system/unified/communications/system/Compatibility/CSR-Compatibility-Matrix.html にある『*Cisco Collaboration Systems リリース互換性マトリックス*』を参照してください。

ドキュメントの変更点

表 2. ドキュメントの変更

日付（Date）	変更内容（Change）
2018 年 4 月 20 日	TLS 1.2 Configuration Overview Guide へのリンクを追加しました。

マニュアルの入手方法およびサービスリクエストの送信方法

ドキュメントの入手方法、Cisco Bug Search Tool（BST）の使用方法、サービスリクエストの送信方法、追加情報の収集方法については、*「Cisco 製品の新機能に関するドキュメント」*を参照してください。

新規および改訂された Cisco の技術コンテンツをデスクトップで直接受け取るには、「Cisco 製品の新機能ドキュメント RSS フィード」を購読してください。 RSS フィードは無料のサービスです。

いかなる場合においても、シスコシステムズおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコシステムズまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

★定型★このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。 ★定型★マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。 説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

すべての印刷されたコピーおよび複製されたソフトコピーは管理外のコピーと見なされ、元のオンラインバージョンを参照して最新版を確認する必要があります。

シスコは世界各国 200 箇所にオフィスを開設しています。 住所、電話番号、FAX 番号は、Cisco の Web サイト www.cisco.com/go/officesに掲載されています。

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。