# Cisco Unified Communications Manager によるセキュアな SCCP Analog Endpoints over TLS の設定

このモジュールでは、Transport Layer Security（TLS）を使用したセキュア シグナリングおよびメディアの暗号化によって、SCCP Telephony Control（STC）Application（STCAPP）の Foreign Exchange Station（FXS）セキュリティ アナログ エンドポイントを、Secure Skinny Client Control Protocol（SCCP）で拡張する方法について説明します。この機能は Cisco Unified Communications Manager（Cisco Unified CM）で制御されるアナログ SCCP エンドポイントのみでサポートされます。

**このモジュール内の機能情報の検索**

ご使用の Cisco IOS ソフトウェア リリースが、このモジュールで説明している機能の一部をサポートしていない場合があります。このモジュール内に記載されている特定の機能のリンクにアクセスする場合、および各機能がサポートされているリリースのリストを参照する場合は、「Cisco Unified CM によるセキュアな SCCP Analog Endpoints over TLS の機能情報」（P.234）を参照してください。

**プラットフォーム、および Cisco IOS ソフトウェア イメージの各サポート情報を検索するには**

プラットフォームのサポートと、Cisco IOS および Catalyst OS ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

## 目次

# Cisco Unified CM によるセキュアな SCCP Analog Endpoints over TLS の前提条件

**Cisco Unified CM によるセキュアな SCCP Analog Endpoints over TLS には、次のソフトウェア コンポーネントが必要です。**

- Cisco Unified CM 8.5 以降

**Cisco IOS 音声ゲートウェイ**

- Cisco IOS Release 15.1(3)T 以降のバージョン
- Cisco 音声ゲートウェイの動作がセットアップおよび設定されていること。詳細については、シスコの該当する設定マニュアルを参照してください。
- アナログ FXS 音声ポートの動作がセットアップおよび設定されていること。詳細については、『*Cisco IOS Voice Port Configuration Guide*』を参照してください。
- Cisco 音声ゲートウェイで SCCP と STCAPP がイネーブルになっていること。詳細については、「*Configuring FXS Ports for Basic Calls*」を参照してください。

# Cisco Unified CM によるセキュアな SCCP Analog Endpoints over TLS の制約事項

- この機能では、次の Cisco IOS プラットフォームのみがサポートされます。
  - Cisco ISR 1861/2801/2811/2821/2851/3825/3845
  - Cisco ISR G2 2901/2911/2921/2951/3925/3945/3925E/3945E
  - Cisco VG202/VG204/VG224

# Cisco Unified CM によるセキュアな SCCP Analog Endpoints over TLS の利点

Secure SCCP では、Cisco Unified CM で TLS および Secured Real-time Transport Protocol（SRTP）を使用するシグナリング完全性およびメディアの暗号化によって、STCAPP FXS アナログ エンドポイントが拡張されます。

この機能では、現行の時分割多重システムにパリティが提供されます。

# Cisco Unified CM によるセキュアな SCCP Analog Endpoints over TLS について

Cisco 音声ゲートウェイの FXS ポートに接続されたアナログ電話機で SCCP 補足機能をイネーブルにするには、次の概念を理解しておく必要があります。

- 「Cisco Unified CM によるセキュアな SCCP Analog Endpoints over TLS」（P.225）

# Cisco Unified CM によるセキュアな SCCP Analog Endpoints over TLS

非セキュア Cisco Unified CM ゲートウェイ環境では、ポート 2000 の TCP 接続を介して Cisco Unified CM と Cisco IOS 音声ゲートウェイの間の SCCP 接続が確立され、ゲートウェイと Cisco Unified CM の間のメディアは RTP になります。これらの接続は暗号化されていないため、ハッカーによるシグナリングの妨害やメディア接続の盗聴によってダメージを受けます。

Secure SCCP over TLS 機能では、既存の Cisco IOS Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）を使用して Cisco IOS 音声ゲートウェイ上のセキュリティ証明書を管理し、Cisco Unified CM に接続することによって、STCAPP セキュリティ エンドポイントを拡張します。

この機能の目的は、次の方法によって、IP テレフォニー環境におけるコール シグナリングの完全性およびメディアの暗号化を実現することです。

- 「TLS を使用した SCCP シグナリング認証、完全性、および暗号化」（P.225）
- 「SRTP によるメディア保護」（P.226）

### TLS を使用した SCCP シグナリング認証、完全性、および暗号化

大規模な展開ではコンフィギュレーションが複雑となる、IPSEC トンネル経由のセキュアなシグナリングではなく、メディア チャネルごとの動的でセキュアな SCCP シグナリングを使用すると、SRTP によってセキュアなメディアが補完され、静的な IPSEC トンネルのセットアップに必要な複雑さを排除できます。

次の手順を使用すると、複数の IOS SCCP アナログ音声ゲートウェイと Cisco Unified CM の間のセキュアな TLS 接続を実装することによって、シグナリングのセキュリティを強化できます。

- Cisco Unified CM と STCAPP の両方で使用されるデジタル セキュリティ証明書（暗号化およびデジタル署名に使用される公開キーが含まれる）を Certificate Authority（CA; 認証局）サーバから取得することによって、STCAPP の ID を確立します。

  **（注）** ゲートウェイは PKI サブシステムで Cisco IOS を実行しているため、証明書を発行するための Certificate Authority Proxy Function（CAPF）と呼ばれるプロキシ機能は不要です。Cisco Unified CM では、Simple Certificate Exchange Protocol（SCEP）に基づく標準をサポートしているサードパーティ CA または専用 Cisco IOS ルータが、CA サーバの役割を果たします。また、Cisco Unified CM では組み込みのサポートを使用して手動で外部 CA からの証明書を要求してインポートし、Cisco IOS CA サーバから証明書を取得することもできます。各 Cisco IOS 音声ゲートウェイは、PKI 自動プロビジョニングによって Cisco IOS CA サーバから独自のセキュリティ証明書を受け取り、大規模な展開を実現できます。

- 同じルート CA から証明書を取得することによって、ゲートウェイと Cisco Unified CM の ID を確立します。TLS では相互認証による標準ハンドシェイクが使用されます。ゲートウェイと Cisco Unified CM は、TLS ハンドシェイクの実行中に証明書を交換して検証することによって、互いを認証します。標準 TLS ハンドシェイクとは別に、Cisco Unified CM ではゲートウェイの証明書の Subject フィールドでデバイス名と MAC アドレスが検証されます。

  **（注）** セキュア ゲートウェイが非セキュア Cisco Unified CM に登録しようとするか、非セキュア ゲートウェイがセキュア Cisco Unified CM に登録しようとすると、登録が拒否され、コンフィギュレーションの不一致を示すエラー メッセージを受け取ります。

理論上は、Cisco VG224 音声ゲートウェイ上の 24 台のアナログ電話機のそれぞれに対して、最大 24 の証明書を発行できます。ただし、1 つの VG224 ボックスに対して 1 つの証明書だけが発行され、Cisco Unified CM への TLS 接続が確立されている間は、すべての電話機でこの証明書が共有されます。その理由は次のとおりです。

- 独自の証明書を持つ各アナログ ポートは大量の NVRAM メモリを消費するが、Cisco IOS プラットフォームの NVRAM メモリ容量には制限がある。
- Cisco Unified CM とゲートウェイの間のデータ パスが 1 つであるため、アナログ ポートごとに証明書を持ってもセキュリティはそれほど向上しない。

### SRTP によるメディア保護

SRTP は、コール制御シグナリングおよび IP エンドポイントの一方から他方へのメディア ストリームを暗号化するために使用されます。メディアの暗号化では、Cisco Unified CM で制御される 2 つのアナログ エンドポイントが、コール制御シグナリング パケットの暗号化と復号化に使用されるキーを交換します。送信側にはパケットを暗号化するために使用されるキー（tx キー）があり、受信側にはパケットを復号化するための同様のキー（rx キー）があります。パケットを正常に復号化するには、受信側の「rx キー」が送信側の「tx キー」と似ている必要があります。

メディア保護では、次のことが行われます。

- 「セキュリティ キーの生成と配布」（P.226）
- 「セキュリティ キーを使用した Digital Signal Processor（DSP; デジタル シグナル プロセッサ）プログラミングによるメディアのセキュリティ」（P.226）

#### セキュリティ キーの生成と配布

セキュリティ キーは Cisco Unified CM で TLS プロトコルを介した SCCP シグナリング メッセージの一部として生成され、SCCP アナログ エンドポイントに配布されます。

#### セキュリティ キーを使用した Digital Signal Processor（DSP; デジタル シグナル プロセッサ）プログラミングによるメディアのセキュリティ

PVDM2 および PVDM3 パケット音声 DSP モジュールを使用する SCCP FXS アナログ エンドポイントがサポートされます。

セキュリティ機能が有効なエンドポイントで SRTP を介してメディアのセキュリティを実現するには、メディアを実際に起動する前に SRTP キーを交換するか、またはエンドポイントにコマンドを送信します。

Cisco IOS によって、DSP が音声モードになった後で SRTP を使用する DSP プログラミングされます。補足サービスが使用される場合、DSP チャネル（コール レッグに関連付けられたもの）をセキュア モードから非セキュア モードへ、またはその逆に切り替えます。DSP はアプリケーションからの命令に基づいて再プログラミングされます。DSP の再プログラミングは、DSP がリセットされ、音声モードになった後で行われます。

# Cisco Unified CM によるセキュアな SCCP Analog Endpoints over TLS の設定方法

（注） 本書では、Cisco Unified CM または IOS CA の詳しい設定方法は説明しません。インストールおよび設定手順については、該当する製品のマニュアルを参照してください。

動的でセキュアな SCCP シグナリングをイネーブルにして、Cisco Unified CM に接続された Cisco 音声ゲートウェイ上の SRTP を介してセキュアなメディアを補完するには、次の作業を実行します。

- 「Cisco IOS 音声ゲートウェイ上のトラストポイントの作成」（P.227）
- 「Cisco Unified CM によるセキュアな SCCP Analog Endpoints over TLS の設定」（P.229）

## Cisco IOS 音声ゲートウェイ上のトラストポイントの作成

Cisco IOS ゲートウェイ上にセキュリティ トラストポイントを作成するには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *label*
4. **enrollment url** *ca-url*
5. **serial-number** [**none**]
6. **fqdn** [***name*** | **none**]
7. **ip-address none**
8. **mac-address** *mac-address*
9. **revocation-check** [**none**]
10. **exit**

### 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br><br>**例：**<br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br>• プロンプトが表示されたら、パスワードを入力します。 |
| ステップ 2 | **configure terminal**<br><br>**例：**<br>`Router# configure terminal` | グローバル コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 3 | **crypto pki trustpoint** *label*<br><br>**例：**<br>`Router(config)# crypto pki trustpoint VG224` | 登録局モード証明書サーバが使用するトラストポイントを指定し、CA-trustpoint コンフィギュレーション モードを開始します。<br>• *label*：トラストポイントと登録局の名前。 |
| ステップ 4 | **enrollment url** *ca-url*<br><br>**例：**<br>`Router(ca-trustpoint)# enrollment url http://1.4.32.7:80` | 発行元 CA 証明書サーバ（ルート証明書サーバ）の登録 URL を指定します。<br>• *ca-url*：ルート CA がインストールされたルータの URL。 |
| ステップ 5 | **serial-number** [**none**]<br><br>**例：**<br>`Router(ca-trustpoint)# serial-number none` | 証明書要求にルータのシリアル番号を含める必要があるかどうかを指定します。<br>• **none**：（任意）証明書要求にシリアル番号が含まれないことを指定します。 |
| ステップ 6 | **fqdn** [*name* \| **none**}<br><br>**例：**<br>`Router(ca-trustpoint)# fqdn none` | 証明書要求に含まれる完全修飾ドメイン名を指定します。<br>• ***name***：証明書要求に「unstructured Name」として含まれる FQDN。<br>• **none**：証明書要求にルータの FQDN が含まれません。 |
| ステップ 7 | **ip-address none**<br><br>**例：**<br>`Router(ca-trustpoint)# ip-address none` | 証明書要求の「unstructuredAddress」として含まれるドット付きの IP アドレスまたはインターフェイスを指定します。<br>• **none**：証明書要求に IP アドレスが含まれないことを指定します。 |
| ステップ 8 | **mac-address** *mac-address*<br><br>**例：**<br>`Router(ca-trustpoint)# mac-address FastEthernet0/0` | Cisco Unified CM によってセキュリティの追加層として要求されるゲートウェイ MAC アドレスを指定します。<br>• *mac-address*：音声ゲートウェイの MAC アドレス。 |
| ステップ 9 | **revocation-check** [**none**]<br><br>**例：**<br>`Router(ca-trustpoint)# revocation-check none` | 証明書の失効ステータスをチェックし、ステータスをチェックする方法を指定します。<br>• **none**：（任意）証明書のチェックは不要です。 |
| ステップ 10 | **exit**<br><br>**例：**<br>`Router(config)# exit` | CA-trustpoint コンフィギュレーション モードを終了します。 |

# Cisco Unified CM によるセキュアな SCCP Analog Endpoints over TLS の設定

（注） 本書では、STCAPP の詳しい設定方法は説明しません。詳細については、「音声ゲートウェイでの SCCP のイネーブル化」（P.33）を参照してください。

セキュアな SCCP アナログ エンドポイントを設定するには、Cisco IOS 音声ゲートウェイで次の手順を実行します。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **stcapp security trustpoint** *line*
4. **stcapp security** *mode* {**authenticated** | **encrypted** | **none**}
5. **stcapp**
6. **dial-peer voice** *tag* **pots**
7. **security mode** [**authenticated** | **encrypted** | **none**]
8. **end**

## 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br><br>**例：**<br>`Router> enable` | 特権 EXEC モードをイネーブルにします。<br>• プロンプトが表示されたら、パスワードを入力します。 |
| ステップ 2 | **configure terminal**<br><br>**例：**<br>`Router# configure terminal` | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **stcapp security trustpoint** *line*<br><br>**例：**<br>`Router(config)# stcapp security trustpoint VG204` | STCAPP エンドポイントのセキュリティをイネーブルにして、TLS 接続の設定に使用するトラストポイントを指定します。<br>• *line*：STCAPP エンドポイントのセキュリティ トラストポイント。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 4 | **stcapp security** *mode* {**authenticat4ed** \| **encrypted** \| **none**}<br><br>**例：**<br>`Router(config)# stcapp security mode encrypted` | STCAPP エンドポイントをイネーブルにして、TLS 接続の設定に使用するグローバル セキュリティ モードを指定します。<br>• **authenticated**：セキュリティ モードが認証され、セキュアな TLS 接続を介して音声ゲートウェイと Cisco Unified CM の間の SCCP シグナリングがイネーブルになります。<br>• **encrypted**：セキュリティ モードが暗号化されます。STCAPP エンドポイントは SRTP を介したデータの暗号化を使用して暗号化されます。<br>• **none**：セキュリティ モードがディセーブルになります。グローバル コンフィギュレーション モードをデフォルトにします。 |
| ステップ 5 | **stcapp**<br><br>**例：**<br>`Router(config)# stcapp` | STCAPP 機能をイネーブルにします。<br>**（注）** stcapp セキュリティ トラストポイントと stcapp セキュリティ モードの両方を開始し、STCAPP エンドポイントのセキュリティをイネーブルにする必要があります。 |
| ステップ 6 | **dial-peer voice** *tag* **pots**<br><br>**例：**<br>`Router(config)# dial-peer voice 1 pots` | （任意）ダイヤルピア音声コンフィギュレーション モードを開始します。<br>• *tag*：特定のダイヤル ピアを定義する番号。範囲は 1 ～ 2147483647 です。<br>• **pots**：IP バックボーンで VoIP カプセル化を使用する POTS ピアであることを示します。 |
| ステップ 7 | **security mode** [**authenticated** \|**encrypted** \| **none**]<br><br>**例：**<br>`Router(config-dialpeer)# security mode encrypted` | （任意）ダイヤルピア レベルの STCAPP エンドポイント セキュリティをイネーブルにして、グローバル コンフィギュレーションを上書きします。<br>• **authenticated**：シグナリング認証を使用して、STCAPP エンドポイントをイネーブルにします。<br>• **encrypted**：データの暗号化を使用して、STCAPP エンドポイントをイネーブルにします。<br>• **none**：ダイヤルピア レベルの STCAPP エンドポイント セキュリティ コンフィギュレーションをディセーブルにして、グローバル レベルのコンフィギュレーションをデフォルトにします。 |
| ステップ 8 | **end**<br><br>**例：**<br>`Router(config-dialpeer)# end` | ダイヤルピア コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |

# Cisco Unified CM によるセキュアな SCCP Analog Endpoints over TLS の設定例

ここでは、次の設定例について説明します。



## 例：Cisco IOS CA サーバの設定

次に、CA サーバの IP アドレスが登録 URL として入力される Cisco IOS CA サーバの設定方法の例を示します。

```
Router# show run
.
.
.
crypto pki server cserver1
 grant auto
!
crypto pki trustpoint cserver1
 enrollment url http://1.4.32.7:80
 revocation-check crl
 rsakeypair cserver1
```

## 例：Cisco IOS VG224 音声ゲートウェイの設定

次に、CA サーバの IP アドレスが登録 URL として入力される Cisco IOS VG224 音声ゲートウェイの設定方法の例を示します。

```
Router# show run
.
.
.
crypto pki trustpoint VG224
 enrollment url http://1.4.32.7:80
 serial-number none
 fqdn none
 ip-address none
 mac-address FastEthernet0/0
 revocation-check none
!
stcapp security trustpoint VG224
stcapp security mode encrypted
stcapp
```

# 参考資料

ここでは、Cisco 音声ゲートウェイの FXS ポート用の SCCP アナログ電話機サポートに関連する資料を示します。

## 関連資料

| 関連項目 | 参照先 |
|---|---|
| Cisco Unified Communications Manager | 『*Cisco Unified Communications Manager*』 |
| Cisco Unified Communications Manager Express | 『*Cisco Unified Communications Manager Express*』 |
| Cisco IOS のデバッグ | 『*Cisco IOS Debug Command Reference*』 |
| Cisco IOS の音声コマンド | 『*Cisco IOS Voice Command Reference*』 |
| Cisco IOS の音声設定 | 『*Cisco IOS Voice Configuration Library*』 |
| Cisco 音声ゲートウェイ | • 『*Cisco VG200 Series Gateway*』<br>• 『*Cisco 1800 Series Integrated Services Routers*』<br>• 『*Cisco 2800 Series Integrated Services Routers*』<br>• 『*Cisco 3800 Series Integrated services Routers*』<br>• 『*Cisco Unified 500 Series*』 |
| 会議およびコード変換リソース | • 『*Cisco Unified CallManager and Cisco IOS Interoperability Guide*』の「Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers」の章<br>• 『*Cisco CallManager and IOS Gateway DSP Farm Configuration Example*』 |

## RFC

| RFC | タイトル |
|---|---|
| RFC 2246 | 『The TLS Protocol Version 1.0』 |

# シスコのテクニカル サポート

| 説明 | リンク |
|---|---|
| 右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。<br><br>以下を含むさまざまな作業にこの Web サイトが役立ちます。<br>・テクニカル サポートを受ける<br>・ソフトウェアをダウンロードする<br>・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける<br>・ツールおよびリソースへアクセスする<br>- Product Alert の受信登録<br>- Field Notice の受信登録<br>- Bug Toolkit を使用した既知の問題の検索<br>・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する<br>・トレーニング リソースへアクセスする<br>・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する<br><br>この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。 | http://www.cisco.com/en/US/support/index.html |

# Cisco Unified CM によるセキュアな SCCP Analog Endpoints over TLS の機能情報

表 28 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。この表には、Cisco IOS Release 15.1(3)T 以降のリリースで導入または変更された機能だけを示します。

このテクノロジーの機能でここに記載されていない情報については、「補足サービスの機能ロードマップ」（P.13）を参照してください。

ご使用の Cisco IOS ソフトウェア リリースでは、一部のコマンドが使用できない場合があります。特定のコマンドのリリース情報については、コマンド リファレンス マニュアルを参照してください。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS と Catalyst OS のソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 28 に、特定の Cisco IOS ソフトウェア リリース群で特定の機能をサポートする Cisco IOS ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

**表 28　Cisco Unified CM によるセキュアな SCCP Analog Endpoints over TLS の機能情報**

| 機能名 | リリース | 機能情報 |
|---|---|---|
| Cisco Unified CM によるセキュアな SCCP Analog Endpoints over TLS | 15.1(3)T | TLS を使用したセキュア シグナリングおよびメディアの暗号化によって、STCAPP FXS セキュリティ アナログ エンドポイントを拡張します。この機能は、Cisco Unified CM で制御されるアナログ SCCP エンドポイントのみでサポートされます。<br>次の項で、この機能に関する情報を参照できます。<br>• 「Cisco Unified CM によるセキュアな SCCP Analog Endpoints over TLS について」（P.224）<br>• 「Cisco Unified CM によるセキュアな SCCP Analog Endpoints over TLS の設定方法」（P.227）<br>この機能によって導入された新しいコマンドはありません。 |