Cisco Unified Communications Manager の回線側サポート

Cisco Unified Communications Manager は、エンタープライズ クラス IP 通信処理システムです。これは、IP Phone、メディア処理デバイス、VoIP ゲートウェイ、モバイル デバイスおよびマルチメディア アプリケーションにエンタープライズ テレフォニー機能を拡張します。Cisco Unified Border Element（SP Edition）は、Cisco Unified Communications Manager の回線側のサポートを提供します。このサポートにより、リモート ユーザが使用する電話が、組織のネットワーク上の電話と通信できるようになります。

Cisco Unified Border Element（SP Edition）は、以前は Integrated Session Border Controller と呼ばれており、このマニュアルでは通常 Session Border Controller（SBC; セッション ボーダー コントローラ）と呼びます。

本章で使用されているコマンドの詳細な説明については、次の場所にある『*Cisco Unified Border Element (SP Edition) Command Reference: Unified Model*』を参照してください。

http://www.cisco.com/en/US/docs/ios/sbc/command/reference/sbcu_book.html

すべての Cisco IOS コマンドの詳細については、http://tools.cisco.com/Support/CLILookup にある Command Lookup Tool を使用するか、Cisco IOS マスター コマンド リストを参照してください。

（注） Cisco Unified Communications Manager の回線側のサポート機能は、Cisco IOS XE Release 3.5S 以降の統合モデルでサポートされます。

Cisco Unified Communications Manager の回線側サポートの機能履歴

リリース	変更内容
Cisco IOS XE Release 3.5S	Cisco Unified Communications Manager の回線側サポート機能が追加されました。

内容

この章の内容は、次のとおりです。

Cisco Unified Communications Manager の回線側サポート機能について

Cisco Unified Communications Manager は組織のネットワーク上の IP 電話のまとまりの管理に使用されます。次のいずれかのモードで動作します。

- ノンセキュア モード：このモードでは、非セキュア プロファイルと Real-Time Transport Protocol（RTP）メディアを使用するデバイスが Cisco Unified Communications Manager に接続できます。
- 混合モード：このモードでは、非セキュアまたはセキュア プロファイルと RTP または Secure Real-Time Transport Protocol（SRTP）メディアを使用するデバイスが Cisco Unified Communications Manager に接続できます。

Cisco Unified Communications Manager の詳細については、次の URL にある、この製品のマニュアルを参照してください。

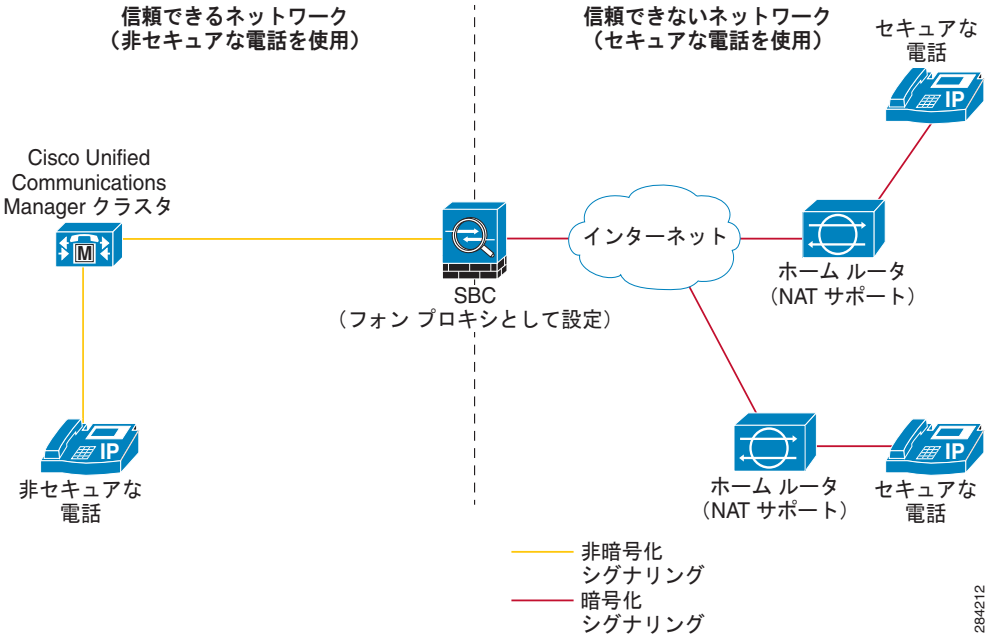
http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_documentation_roadmaps_list.html

（注） この章では、組織のネットワークは、信頼ネットワークと呼ばれます。インターネットを含むその他のネットワークはすべて信頼できないネットワークと呼ばれます。暗号化によってセキュリティ保護された通信はセキュア通信と呼ばれ、暗号化されていない通信は非セキュアな通信と呼ばれます。

信頼ネットワーク上の電話間の通信は、信頼ネットワーク上にあるため、暗号化されません。組織でリモート コンピュータのユーザが使用する VPN は信頼ネットワークの拡張です。リリース 3.5.0 以前のリリースでは、VPN のサポートが IP Phone を対象にしていいないため、リモート ユーザが自身の電話機を使用して信頼ネットワーク上の電話にコールできませんでした。リリース 3.5.0 から、Cisco Unified Border Element（SP Edition）は、Cisco Unified Communications Manager の回線側のサポートを提供します。このサポートにより、SBC 上フォン プロキシの設定が可能になります。リモート ユーザが使用する電話機は、フォン プロキシを通じて組織のネットワーク上の電話機と通信できます。

SBC 上のフォン プロキシは、社内の IP テレフォニー ネットワークとインターネット間の IP テレフォニーをブリッジします。信頼できないネットワークの電話機からのデータの暗号化を強制するようにフォン プロキシを設定して、このブリッジを保護できます。また、フォン プロキシは信頼できないネットワーク上の電話機からの TCP および RTP をサポートするように設定できます。フォン プロキシを使用すると、VPN トンネルを経由しなくても、在宅勤務者の電話から企業 IP テレフォニー ネットワークにインターネット経由で安全に接続できます。これを図 1 に示します。

図 1　フォン プロキシとして設定された SBC



証明書信頼リスト（CTL）は、Cisco Unified Communications Manager サーバ認証プロセスの中心となります。CTL ファイルは、電話機登録プロセス中に電話機でダウンロードするファイルの 1 つです。このファイルには、セキュリティ トークンを使用してシステム管理者によって照明されている ID のリストが含まれます。この場合、ID は Cisco Unified Communications Manager によって管理される電話機です。セキュリティ トークンには、認証局をルートとする証明書が含まれています。この CA は、電話機のトラスト アンカー リストに含まれています。CTL の署名を検証するため、電話機はシステム管理者のセキュリティ トークンの証明書を検証し、証明書に含まれている公開キーを使用してファイル シグニチャを検証します。電話機は CTL ファイルのシグニチャを検証した後、CTL ファイルにリストされているすべての ID を信頼できるシステム エレメントとしてインストールします。

SBC 上で設定されたフォン プロキシは、混合モードとノンセキュア モードの Cisco Unified Communications Manager クラスタをサポートできます。セキュアな通信のためにフォン プロキシを設定する場合、暗号化対応のリモート電話機はクラスタ モードにかかわらず暗号化モードに強制的に設定されます。また、Transport Layer Security（TLS）、つまりシグナリングと SRTP（メディア）は、常に SBC 上で終端します。また、SBC では、NAT を実行したり、メディア用にピンホールを開いたり、受信 SIP ストリームに対してインスペクション ポリシーを適用したりできます。

隣接で設定されているフォン プロキシは、TFTP プロキシとして機能し、隣接のシグナリング アドレスでリッスンします。したがって、Cisco ASR 1000 シリーズ ルータで動作する Cisco IOS XE が提供するネイティブ TFTP サービスは、同じ IP アドレスを使用できません。

フォン プロキシがセキュアな通信用に設定されている場合、フォン プロキシが、SBC 上で外部の電話機からの TLS 接続を終端し、SBC から Cisco Unified Communications Manager への TCP 接続を開きます。フォン プロキシが非セキュアな通信用に設定されている場合、フォン プロキシが、SBC 上で外部の電話機からの TCP 接続を終端し、SBC から Cisco Unified Communications Manager への新しい TCP 接続を開きます。

フォン プロキシは次の追加機能を実行します。

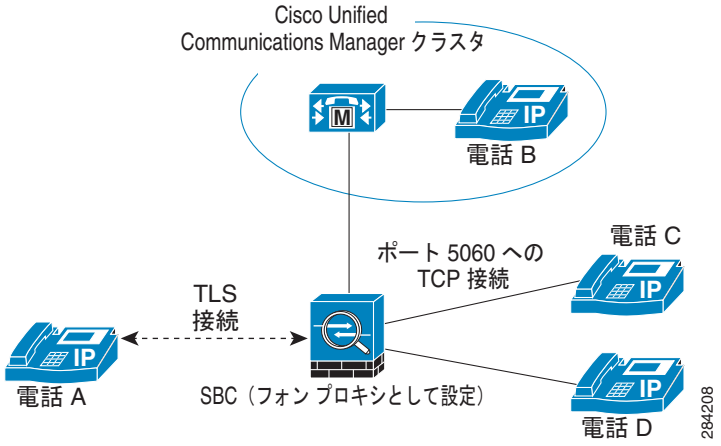
- 証明書ベースの信頼できないネットワーク上の電話機の認証に使用する、CTL ファイルを作成します。

- TFTP 経由で要求された場合に IP 電話のコンフィギュレーション ファイルを変更し、セキュリティ フィールドをノンセキュアからセキュアに変更し、電話に送信されるすべてのファイルに署名します。これらの変更は、暗号化されたシグナリングとメディアを実行することを電話機に強制することで、信頼できないネットワーク上の電話機を保護します。

コール中のシグナリングおよびメディア フロー

コール中にフォン プロキシでサポートされるシグナリング プロトコルおよびメディア フロー プロトコルは、コールに参加する発信側電話機と着信側電話機のタイプに依存します。図 2 に、フォン プロキシ経由で Cisco Unified Communications Manager と通信できる電話機のタイプを示します。

図 2　　コール中のシグナリングおよびメディア フローを示すサンプル シナリオ



この図では次のようになっています。

- 電話機 A は信頼できないネットワークにあります。SBC と電話機 A の間の通信は TLS で暗号化されます。
- 電話機 B は、信頼ネットワーク内の Cisco Unified Communications Manager によって管理されるクラスタにあります。
- 電話機 C と電話機 D は信頼できないネットワークにあります。これらの 2 つの電話機は、NAT デバイスの背後に配置されていない場合とそうでない場合があります。これら 2 つの電話機と SBC 間の通信は暗号化されません。電話機 C と電話機 D の間の通信はこの章で説明していませんが、フォン プロキシにより電話機 C と電話機 D 間の通信も可能であることに注意してください。

次のシナリオでは、図 2 に示す要素を使用し、さまざまなシナリオでコール中のシグナリングとメディアのフローについて説明します。

- 「シナリオ 1：信頼できないネットワークのセキュアな電話機が信頼できないネットワークの非セキュアな電話機にコール」（P.651）
- 「シナリオ 2：信頼できないネットワークのセキュアな電話機が信頼ネットワークの非セキュアな電話機にコール」（P.651）
- 「シナリオ 3：信頼できないネットワークの非セキュアな電話機が信頼ネットワークの非セキュアな電話機にコール」（P.652）

シナリオ 1：信頼できないネットワークのセキュアな電話機が信頼できないネットワークの非セキュアな電話機にコール

図 2 で、電話機 A は信頼できないネットワーク上のセキュアな電話機であり、電話機 C は信頼できないネットワークの非セキュアな電話機です。表 1 に、電話機 A から電話機 C へのコール中のシグナリングとメディア フローで使用されるプロトコルの一覧を示します。

表 1　電話機 A と電話機 C の間のシグナリングおよびメディア フロー

フローの方向	シグナリング プロトコル	メディア プロトコル
電話機 A から SBC へ	SIP over TLS	SRTP
SBC から Cisco Unified Communications Manager へ	SIP over TCP	RTP
Cisco Unified Communications Manager から SBC へ	SIP over TCP	RTP
SBC から電話機 C へ	SIP	RTP
電話機 C から SBC へ	SIP	RTP
SBC から Cisco Unified Communications Manager へ	SIP over TCP	RTP
Cisco Unified Communications Manager から SBC へ	SIP over TCP	RTP
SBC から電話機 A へ	SIP over TLS	SRTP

シナリオ 2：信頼できないネットワークのセキュアな電話機が信頼ネットワークの非セキュアな電話機にコール

図 2 で、電話機 A は信頼できないネットワーク上のセキュアな電話機であり、電話機 B は信頼ネットワークの非セキュアな電話機です。表 2 に、電話機 A から電話機 B へのコール中のシグナリングとメディア フローで使用されるプロトコルの一覧を示します。

表 2　電話機 A と電話機 B の間のシグナリングおよびメディア フロー

フローの方向	シグナリング プロトコル	メディア プロトコル
電話機 A から SBC へ	SIP over TLS	SRTP
SBC から Cisco Unified Communications Manager へ	SIP over TCP	RTP
Cisco Unified Communications Manager から電話機 B へ	SIP	RTP
電話機 B から Cisco Unified Communications Manager へ	SIP	RTP
Cisco Unified Communications Manager から SBC へ	SIP over TCP	RTP
SBC から電話機 A へ	SIP over TLS	SRTP

シナリオ 3：信頼できないネットワークの非セキュアな電話機が信頼ネットワークの非セキュアな電話機にコール

図 2 で、電話機 C は信頼できないネットワーク上の非セキュアな電話機であり、電話機 B は信頼ネットワークの非セキュアな電話機です。表 3 に、電話機 C から電話機 B へのコール中のシグナリングとメディア フローで使用されるプロトコルの一覧を示します。

表 3　電話機 C と電話機 B の間のシグナリングおよびメディア フロー

フローの方向	シグナリング プロトコル	メディア プロトコル
電話機 C から SBC へ	SIP	RTP
SBC から Cisco Unified Communications Manager へ	SIP over TCP	RTP
Cisco Unified Communications Manager から電話機 B へ	SIP	RTP
電話機 B から Cisco Unified Communications Manager へ	SIP	RTP
Cisco Unified Communications Manager から SBC へ	SIP over TCP	RTP
SBC から電話機 C へ	SIP	RTP

Cisco Unified Communications Manager の回線側サポート機能の制約事項

次に、Cisco Unified Communications Manager の回線側サポート機能に関する制約事項を示します。

- 隣接で設定されているフォン プロキシは、TFTP プロキシとして機能し、隣接のシグナリング アドレスでリッスンします。したがって、Cisco ASR 1000 シリーズ ルータで動作する Cisco IOS XE が提供するネイティブ TFTP サービスは、同じ IP アドレスを使用できません。
- Cisco Unified Communications Manager TFTP サーバが IP アドレスではなくドメイン名で設定されている場合、DNS 応答の最初の IP アドレスだけが使用されます。つまり、最初の IP アドレスが何らかの理由で到達可能である場合、代替 IP アドレスは試行されず、接続は失敗します。
- 設定ハイ アベイラビリティ機能だけがサポートされます。TFTP セッションのハイ アベイラビリティ機能はサポートされません。したがって、スイッチオーバー後、すべての TFTP 接続が失われ、IP 電話はこれらの接続を再確立する必要があります。
- シャーシ内ハイ アベイラビリティ機能だけがサポートされます。Cisco Unified Communications Manager の回線側サポート機能は、シャーシ間ハイ アベイラビリティ機能をサポートしない暗号化公開キー インフラストラクチャ（PKI）を使用するため、シャーシ間ハイ アベイラビリティ機能はサポートされません。
- TLS 双方向認証はサポートされていません。
- IPv4 だけがサポートされます。IPv6 はサポートされていません。
- Cisco Unified Communications Manager 上の Key Press Markup Language（KPML）はサポートされません。Cisco Unified Communications Manager を設定する際、KPML の代わりにダイヤル プランを選択する必要があります。

- オーバーラップ ダイヤリング、アドホック会議、コール ピックアップ、コール パーク、共用回線、リセットおよびリスタートなどのサービスはサポートされません。

フォン プロキシの設定

ここでは、フォン プロキシの設定について説明します。

設定の要件

フォン プロキシを設定する前に、SBC が次の設定要件を満たしていることを確認してください。

- SBC には、次の基準を満たすメディア終端の IP アドレスが必要です。
  - IP アドレスは、SBC の外部ネットワーク インターフェイスに関連付けられたアドレス範囲内の未使用の IP アドレスである、パブリックにルーティング可能なアドレスです。
  - IP アドレスは、SBC 上のインターフェイスと同一アドレスにはできません。これには、リモート IP 電話の接続先である SBC 上の外部インターフェイスの IP アドレスが含まれます。
  - IP アドレスは、既存のスタティック NAT プールまたは NAT 規則と重複できません。
  - IP アドレスは、Cisco Unified Communications Manager サーバまたは TFTP サーバの IP アドレスと同じにはできません。
- ルータまたはゲートウェイの背後にある IP 電話の場合は、電話がメディア終端アドレスに到達できるように、ルータまたはゲートウェイでメディア終端アドレスにルートを追加する必要があります。

（注） 組織のセキュリティ ポリシーで、内部ネットワーク上の IP 電話に外部ネットワークへのルートを指定できないことが義務付けられている場合は、内部ネットワーク上で Cisco Unified Communications Manager と互換性がある NAT デバイスを使用することを推奨します。内部ネットワーク アドレスの範囲内にあるアドレスでメディア終端アドレスを表すことによって、内部 IP 電話を外部ルートに公開する必要がなくなります。

- TFTP サーバは、Cisco Unified Communications Manager と同じインターフェイス上に常駐している必要があります。
- Cisco Unified Communications Manager を設定する際、KPML の代わりにダイヤル プランを選択する必要があります。これは、Cisco Unified Communications Manager 上の KPML がフォン プロキシでサポートされないためです。手順については、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

- Cisco Unified Communications Manager に設定されている IP アドレスではなく、完全修飾ドメイン名（FQDN）がある場合、SBC で DNS ルックアップを設定しイネーブルにする必要があります。DNS ルックアップの設定後、SBC から、設定した FQDN で Cisco Unified Communications Manager に ping できることを確認します。
- Certificate Authority Proxy Function（CAPF）サービスをイネーブルにし、Cisco Unified Communications Manager がパブリッシャで実行されておらず、パブリッシャが IP アドレスではなく FQDN を使用して設定されている場合、DNS ルックアップを設定する必要があります。
- TFTP 要求を許可するように SBC で次のアクセスリスト ルールを設定する必要があります。
  - アドレス：TFTP サーバ
  - ポート：69
  - プロトコル：UDP
  - 説明：TFTP の着信を許可する
- フォン プロキシが、既存のファイアウォールの背後に導入されている場合は、フォン プロキシへのシグナリング、TFTP、およびメディア トラフィックを許可するアクセス リスト規則を設定する必要があります。ただし、NAT が Cisco Unified Communications Manager 用に必要な場合、既存のファイアウォール上ではなく、SBC 上で NAT を設定する必要があります。

  表 4 にポートの設定要件をリストします。

表 4　ポート設定要件

アドレス	ポート	プロトコル	説明
メディアの終端	1024-65535	UDP	SRTP の着信を許可する
TFTP サーバ	69	UDP	TFTP の着信を許可する
Cisco Unified Communications Manager	5061	TCP	セキュア SIP の着信を許可する

（注） これらすべてのポートは、TFTP を除き、Cisco Unified Communications Manager に設定可能です。この表に示されているデフォルト値は、Cisco Unified Communications Manager で設定された値と一致するように変更する必要があります。TFTP サーバまたは Cisco Unified Communications Manager に NAT が設定されている場合は、変換後のグローバル アドレスをアクセス リストで使用する必要があります。

プロキシでサポートされている Cisco Unified Communications Manager と IP Phone のバージョン

Cisco Unified Communications Manager の回線側サポート機能は、Cisco Unified Communications Manager Release 7.0 以降でサポートされます。これは、Cisco Unified Communications Manager の以前のリリースが、1 つの IP アドレスで登録された複数の電話機をサポートしないためです。

Cisco Unified Communications Manager は、電話機が SIP over TCP を使用する場合だけ、1 つの IP アドレスで登録されている複数の電話機をサポートします。したがって、UDP ベースの電話機はサポートされません。電話機が UDP ベースかどうかを判別するには、電話機に付属のユーザ マニュアルを参照してください。

エンドユーザの電話機のプロビジョニング

電話機を登録するには、フォン プロキシと Cisco Unified Communications Manager を介して認証し他の電話機と通信するために必要な情報を電話機に設定することが必要です。登録は、電話機を信頼ネットワークに接続するときに実行される、自動化されたプロセスです。次に、登録プロセスの要約を示します。

1. 電話機は、認証用に製造元がインストールした証明書（MIC）を Cisco Unified Call Manager パブリッシャ上の CAPF サービスに提示します。

   デフォルトでは、MIC は電話機にあります。

2. CAPF は、MIC を認証した後、電話機にローカルで有効な証明書（LSC）を配置します。

   LSC は、各コール中に Cisco Unified Communications Manager と電話機間の TLS 接続を確立するために使用されます。

3. 電話機が CTL ファイルをダウンロードします。

   電話機は、SBC に CTL ファイルの TFTP 要求を送信します。設定手順の一部として、SBC は、CTL ファイルを生成します。SBC は、電話機からの TFTP 要求にこのファイルを送信することで応答します。

4. 電話機は Initial Trust List（ITL）ファイルをダウンロードします。

   電話機は、SBC に ITL ファイルの TFTP 要求を送信します。SBC は、Cisco Unified Communications Manager にこの要求を転送し、Cisco Unified Communications Manager が SBC にこのファイルを送信することによって応答します。SBC は、電話機にファイルを転送します。

5. 電話機は、SEP ファイルをダウンロードします。

   電話機は、SBC に Selsius Ethernet Phone（SEP）ファイル（つまり、SEP<mac>.cnf.xml ファイル）の TFTP 要求を送信します。SBC は、Cisco Unified Communications Manager にこの要求を転送し、Cisco Unified Communications Manager が SBC にこのファイルを送信することによって応答します。SBC は、Cisco Unified Communications Manager でサポートされるサービスに対して定義されたアクセス権を反映させてファイルを更新します。これらのアクセス権は、フォン プロキシを設定する際に設定することに注意してください。SBC は、ファイルに署名し、電話機に転送します。

6. 他のいくつかのファイル（ロケール固有のファイルなど）は、Cisco Unified Communications Manager から SBC によってダウンロードされます。SBC はこれらのファイルに署名してから電話機に転送します。

フォン プロキシを設定する手順の概要

次に、フォン プロキシを設定するための手順の概要を示します。

1. PKI トラスト ポイントを作成します。
2. CTL ファイルを作成します。
3. フォン プロキシを作成します。
4. 隣接にフォン プロキシを接続します。

PKI トラスト ポイントの作成

フォン プロキシが使用する TLS プロキシが TLS ハンドシェイクを完了するためには、TLS プロキシが IP Phone からの証明書を確認する必要があります。TLS プロキシは、TLS ハンドシェイクが Cisco Unified Communications Manager との間で実行される場合、Cisco Unified Communications Manager からの証明書も確認する必要があります。TLS プロキシは、IP Phone の証明書を検証するために、CA 製造業者証明書を必要とします。CA 製造業者証明書を Cisco Unified Communications Manager から SBC にインポートするには次の手順を実行します。

ステップ 1 SBC 上でキーペアと自己署名トラストポイントを作成するには、次のコマンドを実行します。

```
Router(config)# crypto key generate rsa label pp_rsa modulus 1024 general-keys
Router(config)# crypto pki trustpoint self_trustpoint
Router(config-ca-trustpoint)# enrollment selfsigned
Router(config-ca-trustpoint)# subject-name CN=SBC-Phone-Proxy,OU=my_BU,O=my_company
Router(config-ca-trustpoint)# crypto pki enroll self_trustpoint
Router(config-ca-trustpoint)# rsakeypair pp_rsa
```

ステップ 2 Cisco Unified Communications Manager のオペレーティング システム管理 Web ページを開きます。

ステップ 3 [Security] > [Certificate Management] の順に選択します。

（注） Cisco Unified Communications Manager の一部のリリースには別の UI があり、証明書を見つけるために異なる手順の実行が必要な場合があります。

ステップ 4 [Find] をクリックします。証明書のリストが表示されます。

ステップ 5 **Cisco_Manufacturing_CA.pem** ファイルをダブルクリックします。証明書をダウンロードすることも可能なダイアログ ボックスに認証情報が表示されます。

（注） 認証リストに、ファイル名が Cisco_Manufacturing_CA の証明書が複数含まれている場合は、Cisco_Manufacturing_CA.pem（つまり拡張子 .pem が付いたファイル）を選択してください。

ステップ 6 [Download] をクリックし、ファイルをテキスト ファイルとして保存します。

ステップ 7 SBC で、Cisco Manufacturing CA にトラストポイントを作成し、次のコマンドを入力して端末経由で登録します。ステップ 6 でダウンロードする証明書をコピーするため、端末で登録する必要があります。

```
Router(config)# crypto ca trustpoint trustpoint_name
Router(config-ca-trustpoint)# enrollment terminal
```

ステップ 8 次のコマンドを実行して、トラストポイントを認証します。

```
Router(config)# crypto ca authenticate trustpoint
```

ステップ 9 Base-64 で符号化された CA 証明書を入力するプロンプトで、ステップ 6 でダウンロードするファイルの内容をコピーし、プロンプトで貼り付けます。ファイルはすでに Base-64 で符号化されているため、変換は不要です。ファイルを受け入れるプロンプトで **yes** と入力します。

（注） 証明書をコピーする場合は、BEGIN および END の行もコピーしてください。

ステップ 10 次の認証についてステップ 2 ～ 9 を繰り返します。表 5 に、SBC で必要な証明書を示します。

表 5　SBC でフォン プロキシに必要な証明書

証明書名	目的
Cisco_Manufacturing_CA	MIC で IP Phone を認証します。
CAP-RTP-001	MIC で IP Phone を認証します。
CAP-RTP-002	MIC で IP Phone を認証します。
CAPF	LSC で IP 電話を認証します。

CTL ファイルの作成

この作業では、CTL ファイルを作成する方法を示します。

手順の概要

1. **configure terminal**
2. **sbc ctl-file** *ctl-file-name*
3. **description** *description*
4. **record-entry [capf | selfsigned] trustpoint** *trustpoint-name*
5. **complete**
6. **end**
7. **show sbc ctl-file [***ctl-file-name***]**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードをイネーブルにします。
ステップ 2	**sbc ctl-file** *ctl-file-name* **例：** `Router(config)# sbc ctl-file ctl-1`	CTL ファイルを作成します。 • *ctl-file-name*：CTL ファイルの名前。
ステップ 3	**description** *description* **例：** `Router(config-ctl-file)# description ctl_101`	CTL ファイルの説明を設定します。 • *description*：CTL ファイルの説明。

	コマンドまたはアクション	目的
ステップ 4	**record-entry [capf | selfsigned] trustpoint** *trustpoint-name* **例：** `Router(config-ctl-file)# record-entry capf trustpoint trustpoint_1`	CTL ファイルの作成に使用するトラストポイントを指定します。 • **capf**：トラストポイントが Cisco Unified Communications Manager からルータにインポートされた CAPF 証明書を使用して作成されることを指定します。 • **selfsigned**：トラストポイントがルータで自己署名されていることを指定します。 • **trustpoint** *trustpoint-name*：トラスト ポイントの名前を指定します。
ステップ 5	**complete** **例：** `Router(config-ctl-file)# complete`	CTL ファイルの作成を完了します。
ステップ 6	**end** **例：** `Router(config-ctl-file)# end`	CTL ファイル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 7	**show sbc ctl-file** [*ctl-file-name*] **例：** `Router# show sbc ctl-file ctl-1`	すべての CTL ファイルまたは指定した CTL ファイルの詳細を表示します。

SBC でのフォン プロキシの設定

この作業では、SBC でフォン プロキシを設定する方法を示します。

手順の概要

1. **configure terminal**
2. **sbc phone-proxy** *phone-proxy-name*
3. **description** *description*
4. **tftp-server address [ipv4** *server-ip-address* **|** *domain-name***] local-address ipv4** *local-ip-address* **vrf** *vrf-name*
5. **ctl-file** *ctl-file-name*
6. **access-secure**
7. **disable service-settings**
8. **capf-address ipv4** *ip-address*
9. **session-timeout** *timeout-interval*
10. **max-concurrent-sessions** *number-of-sessions*
11. **complete**
12. **end**

13. **show sbc phone-proxy** [*phone-proxy-name* **[sessions]** | **sessions]**
14. **show sbc** *sbc-name* **sbe adjacencies pp-sip detail**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードをイネーブルにします。
ステップ 2	**sbc phone-proxy** *phone-proxy-name* **例：** `Router(config)# sbc phone-proxy phone-proxy-1`	フォン プロキシを設定します。 • *phone-proxy-name*：フォン プロキシの名前。
ステップ 3	**description** *description* **例：** `Router(config-phone-proxy)# description cluster-test`	フォン プロキシの説明を設定します。 • *description*：フォン プロキシの説明。
ステップ 4	**tftp-server address [ipv4** *server-ip-address*| **domain-name] local-address ipv4** *local-ip-address* **vrf** *vrf-name* **例：** `Router(config-phone-proxy)# tftp-server address ipv4 198.51.100.101 local-address ipv4 192.168.0.109 vrf vrf1`	TFTP サーバのアドレスを指定します。
ステップ 5	**ctl-file** *ctl-file-name* **例：** `Router(config-phone-proxy)# ctl-file myctl`	CTL ファイルの名前を指定します。 • *ctl-file-name*：CTL ファイルの名前。
ステップ 6	**access-secure** **例：** `Router(config-phone-proxy)# access-secure`	セキュア（暗号化）モードを SBC へのアクセスに使用することを指定します。デフォルトでは、非セキュア モードが SBC との通信に使用されます。
ステップ 7	**disable service-settings** **例：** `Router(config-phone-proxy)# disable-service-settings`	Cisco Unified Communications Manager で設定されたサービス設定をディセーブルにします。PC ポート、Gratuitous ARP、音声 VLAN アクセス、Web アクセス、および Span to PC Port は、Cisco Unified Communications Manager でデフォルトで有効になっているサービスの例です。
ステップ 8	**capf-address ipv4** *ip-address* **例：** `Router(config-phone-proxy)# capf-address ipv4 198.51.100.102`	CAPF サービスのローカル アドレスとしてダミー IP アドレスを設定します。このアドレスは LSC の更新に使用されます。 • *ip-address*：CAPF サービスのダミー IP アドレス。 **（注）** 指定するダミーの IP アドレスは他のサービスで使用することはできません。

	コマンドまたはアクション	目的
ステップ 9	**session-timeout** *timeout-interval* **例：** `Router(config-phone-proxy)# session-timer 200`	TFTP セッションを開いたままにしておくことができる最大時間（秒単位）を指定します。範囲は 60 ～ 6000 です。デフォルト値は 180 です。 • *timeout-interval*：セッションの最大長。
ステップ 10	**max-concurrent-sessions** *number-of-sessions* **例：** `Router(config-phone-proxy)# max-concurrent-sessions 4`	同時セッションの最大数を指定します。 • *number-of-sessions*：同時セッションの最大数。 デフォルトは 30 セッションです。
ステップ 11	**complete** **例：** `Router(config-phone-proxy)# complete`	フォン プロキシの設定を完了します。
ステップ 12	**end** **例：** `Router(config-phone-proxy)# end`	フォン プロキシ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 13	**show sbc phone-proxy** [*phone-proxy-name* **[sessions] | sessions]** **例：** `Router# show sbc phone-proxy phone-proxy-1`	指定しフォン プロキシまたはすべてのフォン プロキシで実行中のセッションの詳細を表示します。 • *phone-proxy-name*：フォン プロキシの名前。
ステップ 14	**show sbc** *sbc-name* **sbe adjacencies pp-sip detail** **例：** `Router# show sbc mysbc sbe adjacencies pp-sip detail`	指定した隣接の設定の詳細を表示します。

フォン プロキシの TFTP ポート範囲の設定

この作業では、フォン プロキシの TFTP ポート範囲を設定する方法を示します。

手順の概要

1. **configure terminal**
2. **sbc phone-proxy tftp-address ipv4** *ip-address* **[vrf** *vrf-name***]**
3. **port-range** *min-port max-port*
4. **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	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードをイネーブルにします。
ステップ 2	**sbc phone-proxy tftp-address ipv4** *ip-address* **[vrf** *vrf-name***]** **例：** `Router(config)# sbc phone-proxy tftp-address ipv4 192.168.0.109 vrf vrf1`	TFTP サーバの IP アドレスと VRF 名を指定します。 • *ip-address*：TFTP サーバの IP アドレス。 • *vrf-name*：TFTP サーバの VRF 名。
ステップ 3	**port-range** *min-port max-port* **例：** `Router(config-pp-pr)# port-range 30000 40000`	TFTP サーバのポート範囲を指定します。 • *min-port*：ポート範囲の開始ポート番号。 • *max-port*：ポート範囲の終了ポート番号。
ステップ 4	**end** **例：** `Router(config-pp-pr)# end`	フォン プロキシ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

隣接へのフォン プロキシの関連付け

この作業では、隣接にフォン プロキシを関連付ける方法を示します。

手順の概要

1. **configure terminal**
2. **sbc** *sbc-name*
3. **sbe**
4. **adjacency sip** *adjacency-name*
5. **phone-proxy** *phone-proxy-name*
6. **attach**
7. **end**
8. **show sbc** *sbc-name* **sbe adjacencies** *adjacency-name* **detail**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードをイネーブルにします。
ステップ 2	**sbc** *sbc-name* **例：** `Router(config)# sbc mysbc`	SBC サービス モードを開始します。 • *sbc-name*：SBC の名前。
ステップ 3	**sbe** **例：** `Router(config)# sbe`	SBC サービス内で SBE エンティティ モードを開始します。
ステップ 4	**adjacency sip** *adjacency-name* **例：** `Router(config-sbc-sbe)# adjacency sip pp-adj`	SBE SIP 隣接のモードを開始します。 • *adjacency-name*：隣接名。
ステップ 5	**phone-proxy** *phone-proxy-name* **例：** `Router(config-sbc-sbe-adj-sip)# phone-proxy phone-proxy-1`	隣接に関連付けるフォン プロキシの名前を指定します。 • *phone-proxy-name*：フォン プロキシの名前。
ステップ 6	**attach** **例：** `Router(config-sbc-sbe-adj-sip)# attach`	隣接にフォン プロキシを関連付けます。
ステップ 7	**end** **例：** `Router(config-sbc-sbe-adj-sip)# end`	SBE SIP 隣接モードを終了し、特権 EXEC モードを開始します。
ステップ 8	**show sbc** *sbc-name* **sbe adjacencies** *adjacency-name* **detail** **例：** `Router# show sbc mysbc sbe adjacencies pp-adj detail`	指定した隣接の設定の詳細を表示します。

フォン プロキシに関する情報の表示

フォン プロキシに関する情報を表示し、問題をトラブルシューティングするには、次のコマンドを使用します。

- フォン プロキシの接続に関するデータのデバッグ ロギングをイネーブルにするには、次のコマンドを使用します。

debug sbc phone-proxy [all | cli| | detail | error | event]

- フォン プロキシのハイ アベイラビリティ機能に関するデータのデバッグ ロギングをイネーブルにするには、次のコマンドを使用します。

  debug sbc *sbc-name* **high-availability phone-proxy**

設定例

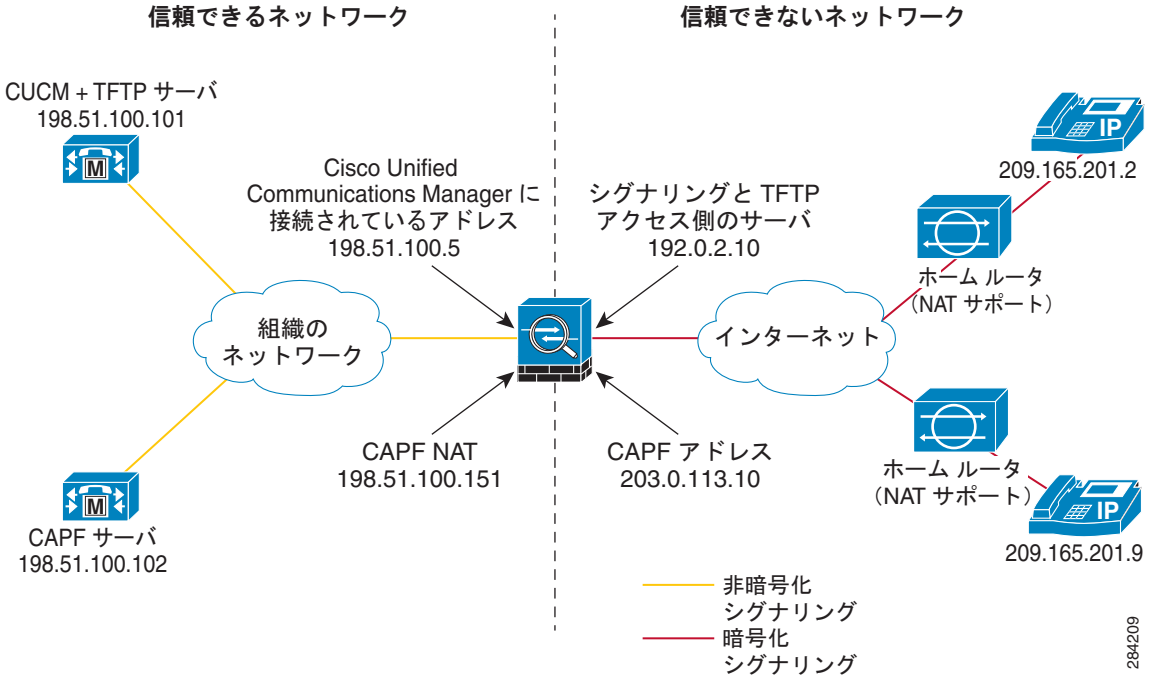
以降の項で説明する例は、フォン プロキシをさまざまなシナリオで設定する例を示します。

- 「単一クラスタの LSC がインストールされたセキュア アクセスのためのフォン プロキシの設定」（P.663）
- 「単一クラスタの LSC がインストールされていないセキュア アクセスのためのフォン プロキシの設定」（P.665）
- 「単一クラスタの非セキュア アクセスのためのフォン プロキシの設定」（P.668）
- 「フォン プロキシの削除」（P.669）

単一クラスタの LSC がインストールされたセキュア アクセスのためのフォン プロキシの設定

図 3 に、信頼できないネットワーク上のセキュアな電話機が信頼ネットワークの電話機にアクセスする動作環境を示します。このサンプル シナリオでは、LSC がインストールされ CAPF サーバが設定されます。

図 3　信頼できないネットワーク上のセキュアな電話機が、LSC がインストールされている信頼ネットワーク上の電話機にアクセス



この動作環境でフォン プロキシおよび他のエンティティを設定するには、次の手順を実行します。いくつかのコマンドが簡潔さのためにこれらの手順から除外されていることに注意してください。

ステップ 1 既存の自己署名トラストポイントおよび証明書が存在する場合、この手順をスキップして次の手順に直接進みます。そうでない場合は、次のコマンドを実行して、RSA キーペアおよび自己署名トラストポイントを作成し、証明書を生成します。

```
Router(config)# crypto key generate rsa label pp_rsa modulus 1024 general-keys
Router(config)# crypto pki trustpoint self_trustpoint
Router(config-ca-trustpoint)# enrollment selfsigned
Router(config-ca-trustpoint)# subject-name CN=SBC-Phone-Proxy,OU=my_BU,O=my_company
Router(config-ca-trustpoint)# crypto pki enroll self_trustpoint
Router(config-ca-trustpoint)# rsakeypair pp_rsa
```

ステップ 2 次のコマンドを実行して、CAPF 証明書を Cisco Unified Communications Manager からインポートし、トラスト ポイントを作成します。

```
Router(config)# crypto pki trustpoint capf_trustpoint
Router(config-ca-trustpoint)# enrollment terminal
Router(config-ca-trustpoint)# crypto pki authenticate capf_trustpoint
```

ステップ 3 次のコマンドを実行して、CTL ファイルを作成します。

```
Router(config)# sbc ctl-file myctl
Router(config-ctl-file)# record-entry capf trustpoint capf_trustpoint
Router(config-ctl-file)# record-entry selfsigned trustpoint self_trustpoint
Router(config-ctl-file)# complete
```

ステップ 4 次のコマンドを実行して、フォン プロキシを作成します。

```
Router(config)# sbc phone-proxy mypp_1
Router(config-phone-proxy)# tftp-server address ipv4 198.51.100.101 local-address ipv4
192.0.2.10 vrf vrf1
Router(config-phone-proxy)# ctl-file myctl
Router(config-phone-proxy)# access-secure
Router(config-phone-proxy)# capf-address ipv4 203.0.113.10
Router(config-phone-proxy)# complete
```

（注） capf-address の値は、未使用の任意の IP アドレスにすることができます。

ステップ 5 次のコマンドを実行して、TFTP ポート範囲を定義します。

```
Router(config)# sbc phone-proxy tftp-address ipv4 192.0.2.10 vrf vrf1
Router(config-pp-pr)# port-range 8192 30000
  .
  .
  .
Router(config)# sbc phone-proxy tftp-address ipv4 192.0.2.10
```

（注） 使用中の各 TFTP クライアント アドレスとローカル TFTP サーバ アドレス（アクセス側隣接のシグナリング アドレスと同じ）の TFTP アドレス エントリを作成します。各 TFTP アドレスのポート範囲の指定は任意です。ポート範囲を指定しない場合は、32768 ～ 65535 がデフォルトのポート範囲として使用されます。

ステップ 6 次のコマンドを実行して、SIP 隣接を設定します。

```
Router(config)# sbc sbc1
Router(config-sbc)# sbe
```

```
.
.
.
Router(config-sbc-sbe)# adjacency sip access-1
.
.
.
Router(config-sbc-sbe-adj-sip)# fast-register disable
Router(config-sbe-adj-sip)# inherit profile preset-access
Router(config-sbc-sbe-adj-sip)# security untrusted-encrypted
Router(config-sbc-sbe-adj-sip)# signaling-address ipv4 192.0.2.10
Router(config-sbc-sbe-adj-sip)# remote-address ipv4 209.165.201.2 255.255.255.0
Router(config-sbc-sbe-adj-sip)# signaling-peer 209.165.201.2
Router(config-sbc-sbe-adj-sip)# phone-proxy mypp_1
Router(config-sbc-sbe-adj-sip)# registration rewrite-register
Router(config-sbc-sbe-adj-sip)# attach
.
.
.
Router(config-sbc-sbe)# adjacency sip core-1
Router(config-sbc-sbe-adj-sip)# vrf vrf1
Router(config-sbc-sbe-adj-sip)# force-signaling-peer
.
.
.
Router(config-sbc-sbe-adj-sip)# inherit profile preset-core
Router(config-sbc-sbe-adj-sip)# signaling-address ipv4 198.51.100.5
Router(config-sbc-sbe-adj-sip)# remote-address ipv4 198.51.100.101 255.255.255.255
Router(config-sbc-sbe-adj-sip)# signaling-peer 198.51.100.101
Router(config-sbc-sbe-adj-sip)# registration target address 198.51.100.101
Router(config-sbc-sbe-adj-sip)# registration contact username passthrough
Router(config-sbc-sbe-adj-sip)# attach
```

（注） registration target address は Cisco Unified Communications Manager の IP アドレスです。

ステップ 7 次のコマンドを実行して、CAPF の NAT を設定します。

（注） 指定したアドレス範囲は隣接のリモート アドレス範囲である必要があります。

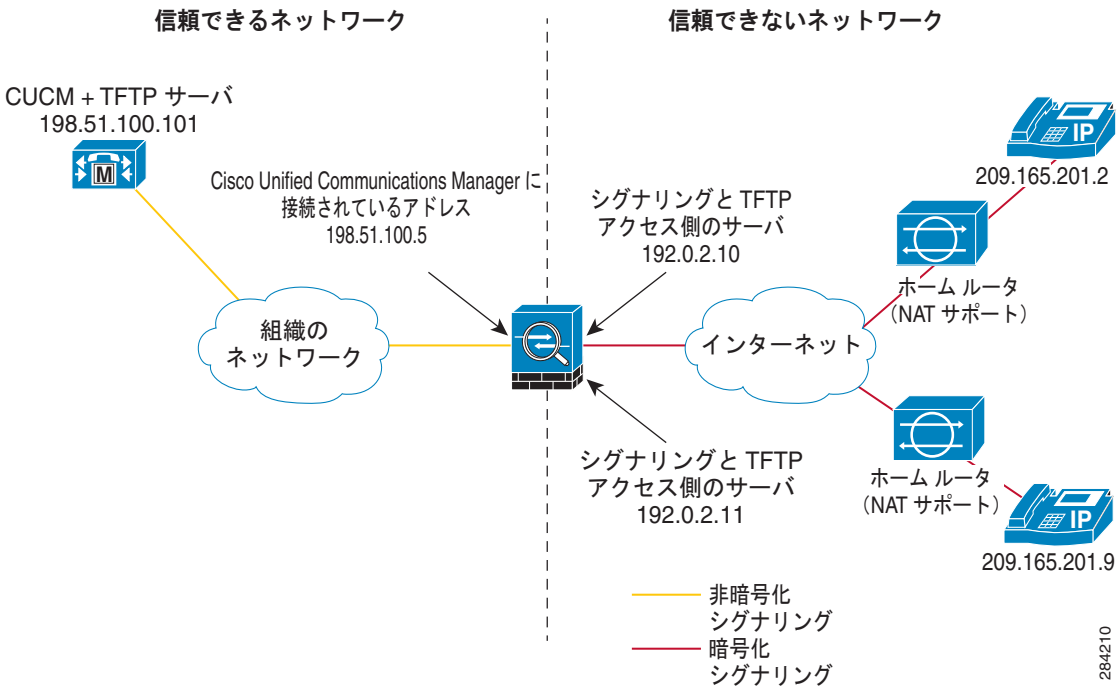
```
Router(config)# access-list 1 permit 209.165.201.2 0.0.0.255
Router(config)# ip nat pool CAPF_NAT 198.51.100.151 198.51.100.151 netmask 255.255.255.0
Router(config)# ip nat inside source list 1 pool CAPF_NAT overload
Router(config)# ip nat outside source static 198.51.100.102 203.0.113.10 add-route
```

（注） 203.0.113.10 はフォン プロキシで設定したダミー CAPF IP アドレスです。ダミー IP アドレスは、他のサービスには使用できません。

単一クラスタの LSC がインストールされていないセキュア アクセスのためのフォン プロキシの設定

図 4 に、信頼できないネットワーク上のセキュアな電話機が信頼ネットワークの電話機にアクセスする動作環境を示します。LSC はこのサンプル シナリオでインストールされていません。

図 4　信頼できないネットワーク上のセキュアな電話機が、LSC がない信頼ネットワーク上の電話機にアクセス



この動作環境でフォン プロキシおよび他のエンティティを設定するには、次の手順を実行します。いくつかのコマンドが簡潔さのためにこれらの手順から除外されていることに注意してください。

ステップ 1　既存の自己署名トラストポイントおよび証明書が存在する場合、この手順をスキップして次の手順に直接進みます。そうでない場合は、次のコマンドを実行して、RSA キーペアおよび自己署名トラストポイントを作成し、証明書を生成します。

```
Router(config)# crypto key generate rsa label pp_rsa modulus 1024 general-keys
Router(config)# crypto pki trustpoint self_trustpoint
Router(config-ca-trustpoint)# enrollment selfsigned
Router(config-ca-trustpoint)# subject-name CN=SBC-Phone-Proxy,OU=my_BU,O=my_company
Router(config-ca-trustpoint)# crypto pki enroll self_trustpoint
Router(config-ca-trustpoint)# rsakeypair pp_rsa
```

ステップ 2　次のコマンドを実行して、CAPF 証明書を Cisco Unified Communications Manager からインポートし、トラスト ポイントを作成します。

```
Router(config)# crypto pki trustpoint CAP-RTP-001_trustpoint
Router(config-ca-trustpoint)# enrollment terminal
Router(config)# crypto pki authenticate CAP-RTP-001_trustpoint
Router(config)# crypto pki trustpoint CAP-RTP-002_trustpoint
Router(config-ca-trustpoint)# enrollment terminal
Router(config)# crypto pki authenticate CAP-RTP-002_trustpoint
Router(config)# crypto pki trustpoint Cisco_Manufacturing_CA_trustpoint
Router(config-ca-trustpoint)# enrollment terminal
Router(config)# crypto pki authenticate Cisco_Manufacturing_CA_trustpoint
```

ステップ 3　次のコマンドを実行して、CTL ファイルを作成します。

```
Router(config)# sbc ctl-file myctl
Router(config-ctl-file)# record-entry selfsigned trustpoint self_trustpoint
Router(config-ctl-file)# complete
```

ステップ 4 次のコマンドを実行して、フォン プロキシを作成します。

```
Router(config)# sbc phone-proxy mypp_1
Router(config-phone-proxy)# tftp-server address ipv4 198.51.100.101 local-address ipv4
192.0.2.10 vrf vrf1
Router(config-phone-proxy)# ctl-file myctl
Router(config-phone-proxy)# access-secure
Router(config-phone-proxy)# disable-service-settings
Router(config-phone-proxy)# complete
```

ステップ 5 次のコマンドを実行して、TFTP ポート範囲を定義します。

```
Router(config)# sbc phone-proxy tftp-address ipv4 192.0.2.10 vrf vrf1
Router(config-pp-pr)# port-range 30000-60000
.
.
.
Router(config)# sbc phone-proxy tftp-address ipv4 192.0.2.10
Router(config)# sbc phone-proxy tftp-address ipv4 10.10.2.6
Router(config-pp-pr)# port-range 35000 55000
```

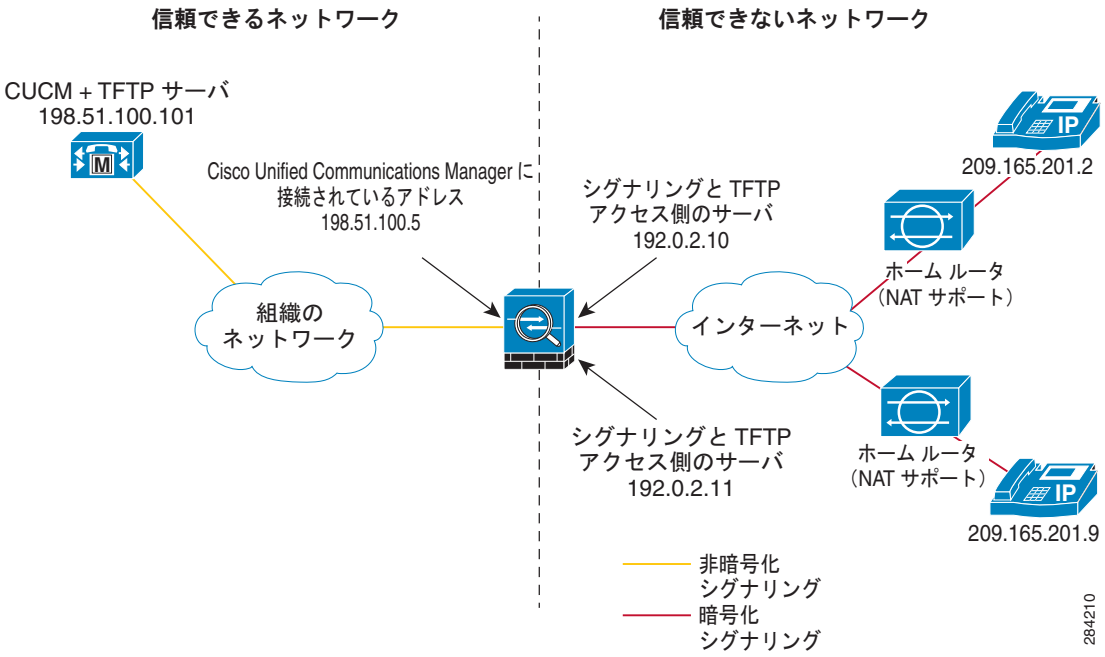
ステップ 6 次のコマンドを実行して、SIP 隣接を設定します。

```
Router(config)# sbc sbc1
Router(config-sbc)# sbe
.
.
.
Router(config-sbc-sbe)# adjacency sip access-1
.
.
.
Router(config-sbe-adj-sip)# inherit profile preset-access
Router(config-sbc-sbe-adj-sip)# security untrusted-encrypted
Router(config-sbc-sbe-adj-sip)# signaling-address ipv4 192.0.2.10
Router(config-sbc-sbe-adj-sip)# remote-address ipv4 209.165.201.2 255.255.255.0
Router(config-sbc-sbe-adj-sip)# signaling-peer 209.165.201.2
Router(config-sbc-sbe-adj-sip)# phone-proxy mypp_1
Router(config-sbc-sbe-adj-sip)# registration rewrite-register
Router(config-sbc-sbe-adj-sip)# attach
Router(config-sbc-sbe)# adjacency sip access-2
.
.
.
Router(config-sbc-sbe-adj-sip)# security untrusted-encrypted
Router(config-sbc-sbe-adj-sip)# signaling-address ipv4 10.10.2.6
Router(config-sbc-sbe-adj-sip)# remote-address 69.118.130.9 255.255.255.5
Router(config-sbc-sbe-adj-sip)# signaling-peer 69.118.122.6
Router(config-sbc-sbe-adj-sip)# phone-proxy mypp_1
Router(config-sbc-sbe-adj-sip)# registration rewrite-register
Router(config-sbc-sbe-adj-sip)# attach
Router(config-sbc-sbe)# adjacency sip core-1
Router(config-sbc-sbe-adj-sip)# vrf vrf1
Router(config-sbc-sbe-adj-sip)# force-signaling-peer
.
.
.
Router(config-sbc-sbe-adj-sip)# inherit profile preset-core
Router(config-sbc-sbe-adj-sip)# signaling-address ipv4 198.51.100.5
Router(config-sbc-sbe-adj-sip)# remote-address ipv4 198.51.100.101 255.255.255.255
Router(config-sbc-sbe-adj-sip)# signaling-peer 198.51.100.101
Router(config-sbc-sbe-adj-sip)# registration target address 198.51.100.101
Router(config-sbc-sbe-adj-sip)# attach
```

単一クラスタの非セキュア アクセスのためのフォン プロキシの設定

図 5 に、クラスタ外かつ信頼ネットワーク内の電話機がクラスタ内の電話機にアクセスする設定を示します。

図 5　　非クラスタの電話機がクラスタ内の電話機にアクセス



この動作環境でフォン プロキシおよび他のエンティティを設定するには、次の手順を実行します。いくつかのコマンドが簡潔さのためにこれらの手順から除外されていることに注意してください。

ステップ 1　既存の自己署名トラストポイントおよび証明書が存在する場合、この手順をスキップして次の手順に直接進みます。そうでない場合は、次のコマンドを実行して、RSA キーペアおよび自己署名トラストポイントを作成し、証明書を生成します。

```
Router(config)# crypto key generate rsa label pp_rsa modulus 1024 general-keys
Router(config)# crypto pki trustpoint self_trustpoint
Router(config-ca-trustpoint)# enrollment selfsigned
Router(config-ca-trustpoint)# crypto pki enroll self_trustpoint
```

ステップ 2　次のコマンドを実行して、CTL ファイルを作成します。

```
Router(config)# sbc ctl-file myctl
Router(config-ctl-file)# record-entry selfsigned trustpoint self_trustpoint
Router(config-ctl-file)# complete
```

ステップ 3　次のコマンドを実行して、フォン プロキシを作成します。

```
Router(config)# sbc phone-proxy mypp_1
Router(config-phone-proxy)# tftp-server address ipv4 198.51.100.101 local-address ipv4
192.168.0.109 vrf vrf1
Router(config-phone-proxy)# ctl-file myctl
Router(config-phone-proxy)# no access-secure
Router(config-phone-proxy)# complete
```

ステップ 4　次のコマンドを実行して、TFTP ポート範囲を定義します。

```
Router(config)# sbc phone-proxy tftp-address ipv4 192.0.2.10 vrf vrf1
Router(config-pp-pr)# port-range 30000 60000
Router(config)# sbc phone-proxy tftp-address ipv4 192.0.2.10
Router(config)# sbc phone-proxy tftp-address ipv4 10.10.2.6
Router(config-pp-pr)# port-range 35000 55000
```

ステップ 5 次のコマンドを実行して、SIP 隣接を設定します。

```
Router(config)# sbc sbc-name
Router(config-sbc)# sbe
.
.
.
Router(config-sbc-sbe)# adjacency sip access-1
.
.
.
Router(config-sbc-sbe-adj-sip)# inherit profile preset-access
Router(config-sbc-sbe-adj-sip)# signaling-address ipv4 192.0.2.10
Router(config-sbc-sbe-adj-sip)# remote-address 69.118.122.5 255.255.255.5
Router(config-sbc-sbe-adj-sip)# signaling-peer 69.118.122.5
Router(config-sbc-sbe-adj-sip)# phone-proxy mypp_1
Router(config-sbc-sbe-adj-sip)# registration rewrite-register
Router(config-sbc-sbe-adj-sip)# attach
Router(config-sbc-sbe)# adjacency sip access-2
.
.
.
Router(config-sbc-sbe-adj-sip)# inherit profile preset-access
Router(config-sbc-sbe-adj-sip)# signaling-address ipv4 10.10.2.6
Router(config-sbc-sbe-adj-sip)# remote-address 69.118.130.9 255.255.255.5
Router(config-sbc-sbe-adj-sip)# signaling-peer 209.165.201.9
Router(config-sbc-sbe-adj-sip)# phone-proxy mypp_1
Router(config-sbc-sbe-adj-sip)# registration rewrite-register
Router(config-sbc-sbe-adj-sip)# attach
Router(config-sbc-sbe)# adjacency sip core-1
Router(config-sbc-sbe-adj-sip)# vrf vrf1
Router(config-sbc-sbe-adj-sip)# force-signaling-peer
.
.
.
Router(config-sbc-sbe-adj-sip)# inherit profile preset-core
Router(config-sbc-sbe-adj-sip)# signaling-address ipv4 198.51.100.5
Router(config-sbc-sbe-adj-sip)# remote-address ipv4 198.51.100.101 255.255.255.255
Router(config-sbc-sbe-adj-sip)# signaling-peer 198.51.100.101
Router(config-sbc-sbe-adj-sip)# registration target address 198.51.100.101
Router(config-sbc-sbe-adj-sip)# attach
```

フォン プロキシの削除

次に、フォン プロキシを削除する方法を示します。

```
Router# configure terminal
Router(config)# sbc mysbc
Router(config)# sbe
Router(config-sbc-sbe)# adjacency sip pp-adj
Router(config-sbc-sbe-adj-sip)# no attach
Router(config-sbc-sbe-adj-sip)# no phone-proxy pp
Router(config-sbc-sbe-adj-sip)# exit
Router(config-sbc-sbe)# exit
Router(config-sbc)# exit
Router(config)# sbc phone-proxy pp
```

```
Router(config-phone-proxy)# no complete
Router(config-phone-proxy)# exit
Router(config)# no sbc phone-proxy pp
Router(config)# sbc ctl-file ctl-1
Router(config-ctl-file)# no complete
Router(config-ctl-file)# exit
Router(config)# no sbc ctl-file ctl-1
```