Cisco 電話プロキシの設定

この章では、Cisco 電話プロキシ機能向けに ASA を設定する方法について説明します。

この章の内容は、次のとおりです。

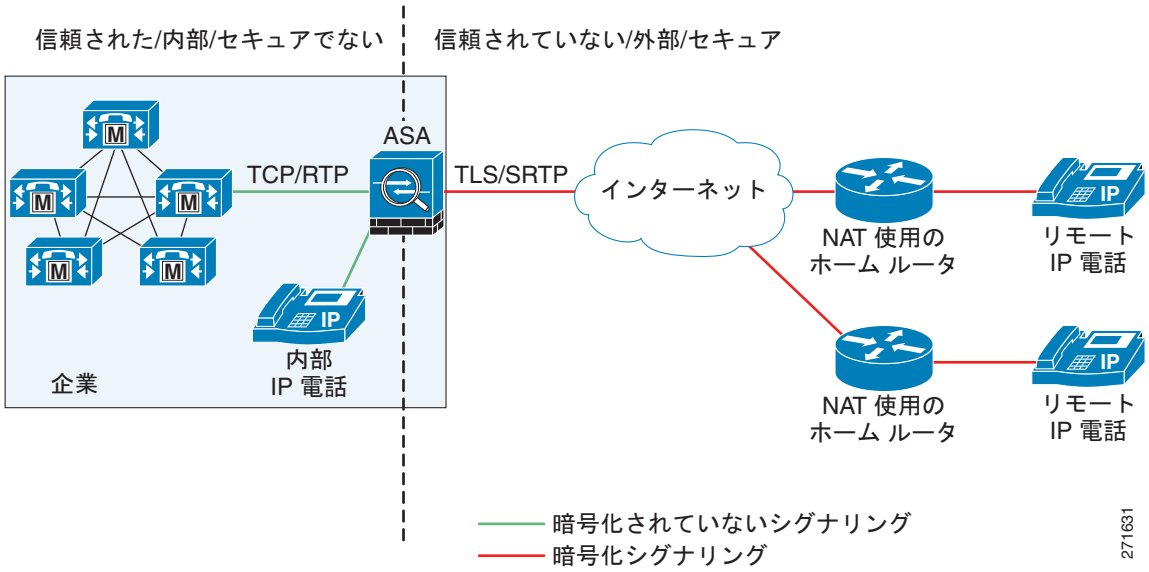
Cisco 電話プロキシに関する情報

ASA の Cisco 電話プロキシは、非信頼ネットワーク上のリモート電話から伝送されるデータを強制的に暗号化することにより、企業 IP テレフォニー ネットワークとインターネットの間の IP テレフォニーを安全にブリッジします。

電話プロキシ機能

電話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 IP 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。図 16-1 を参照してください。

図 16-1　電話プロキシの安全な構成



電話プロキシでは、混合モードまたはノンセキュア モードの Cisco Unified Communications Manager（UCM）クラスタがサポートされています。クラスタ モードにかかわらず、暗号化機能を持つリモート電話は常に暗号化モードになります。Transport Layer Security（TLS）（シグナリング）および Secure Real-time Transport Protocol（SRTP）（メディア）は、常に ASA で終端します。また、ASA 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、SCCP や SIP などのプロトコルのインスペクション ポリシーを適用したりできます。ノンセキュア クラスタ モードや、電話がノンセキュア モードに設定された混合モードの場合、電話プロキシは次のように動作します。

- 電話からの TLS 接続は ASA で終端され、Cisco UCM への TCP 接続が開始されます。
- 外部の IP 電話から内部ネットワークの IP 電話に ASA 経由で送信される SRTP は、Real-time Transport Protocol（RTP）に変換されます。

内部の IP 電話が認証モードに設定された混合モード クラスタの場合、TLS 接続は Cisco UCM への TCP に変換されませんが、SRTP は RTP に変換されます。

内部の IP 電話が暗号化モードに設定された混合モード クラスタの場合、TLS 接続は TLS のまま Cisco UCM に接続され、リモート電話からの SRTP は SRTP のまま内部の IP 電話に伝送されます。

電話プロキシでは、ノンセキュア クラスタへの通話時に電話の動作を安全に保つことが主な目的のため、次の機能が実行されます。

- 証明書ベースのリモート電話の認証に使用する、Certificate Trust List（CTL; 証明書信頼リスト）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。これらの変更によって、リモート電話で暗号化シグナリングとメディアが強制的に実行されるようになり、安全性が確保されます。
- 電話からの TLS シグナリングを終端し、Cisco UCM への TCP または TLS を開始します。
- Skinny および SIP のシグナリング メッセージを変更することによって、メディア パスに入ります。
- SRTP を終端し、受信側への RTP/SRTP を開始します。

（注）　TLS ハンドシェイクによるリモート IP 電話の認証の代わりに、LSC プロビジョニングによる認証を設定できます。LSC プロビジョニングでは、リモート IP 電話ユーザごとにパスワードを作成し、各ユーザはリモート IP 電話でパスワードを入力して LSC を取得します。

リモート IP 電話の認証に LSC プロビジョニングを使用するには、IP 電話をまずノンセキュア モードで登録する必要があります。このため、IP 電話をエンドユーザに渡す前に、企業ネットワーク内で LSC プロビジョニングを実行することを推奨します。そうしない場合、IP 電話をノンセキュア モードで登録するには、SIP および SCCP 用のノンセキュア シグナリング ポートを ASA 上で管理者が開く必要があります。

CAPF（Certificate Authority Proxy Function; 認証局プロキシ関数）を使用した、ローカルで有効な証明書（LSC）のインストールについては、『Cisco Unified Communications Manager Security Guide』も参照してください。

電話プロキシでサポートされる Cisco UCM および IP Phone

Cisco Unified Communications Manager

次のリリースの Cisco Unified Communications Manager が電話プロキシでサポートされています。

- Cisco Unified CallManager バージョン 4.*x*
- Cisco Unified CallManager バージョン 5.0
- Cisco Unified CallManager バージョン 5.1
- Cisco Unified Communications Manager 6.1
- Cisco Unified Communications Manager 7.0
- Cisco Unified Communications Manager 8.0

Cisco Unified IP Phone

電話プロキシでは、次の IP 電話機能がサポートされます。

- 電話プロキシを介して接続されたリモート電話上での電話会議などのエンタープライズ機能
- XML サービス

Cisco Unified IP Phones 7900 シリーズの次の IP Phone が電話プロキシでサポートされています。

- Cisco Unified IP Phone 7975
- Cisco Unified IP Phone 7971
- Cisco Unified IP Phone 7970
- Cisco Unified IP Phone 7965
- Cisco Unified IP Phone 7962
- Cisco Unified IP Phone 7961
- Cisco Unified IP Phone 7961G-GE
- Cisco Unified IP Phone 7960（SCCP プロトコルのサポートに限る）
- Cisco Unified IP Phone 7945
- Cisco Unified IP Phone 7942
- Cisco Unified IP Phone 7941

- Cisco Unified IP Phone 7941G-GE
- Cisco Unified IP Phone 7940（SCCP プロトコルのサポートに限る）
- Cisco Unified Wireless IP Phone 7921
- Cisco Unified Wireless IP Phone 7925

（注） Cisco Unified Wireless IP Phone 7925 をサポートするには、電話プロキシと適切に連携できるように、IP 電話上で MIC または LSC を設定する必要もあります。

- ソフトウェア電話対応の CIPC（認証モードの CIPC バージョンに限る）

（注） Cisco IP Communicator は、電話プロキシ VLAN トラバーサルの認証 TLS モードでサポートされています。Cisco IP Communicator では SRTP および TLS が現在サポートされていないため、リモート アクセスに使用することはお勧めしません。

（注） ASA は、SCCP プロトコル バージョン 19 以前が稼働している Cisco IP Phone からのトラフィックのインスペクションをサポートします。

電話プロキシのライセンス要件

ASA でサポートされる Cisco 電話プロキシ機能には、Unified Communications Proxy ライセンスが必要です。

次の表に、Unified Communications Proxy ライセンスの詳細をプラットフォーム別に示します。

（注） この機能は、ペイロード暗号化機能のないモデルでは使用できません。

モデル	ライセンス要件[1]
ASA 5505	基本ライセンスと Security Plus ライセンス：2 セッション。 *オプション ライセンス：24 セッション。*
ASA 5510	基本ライセンスと Security Plus ライセンス：2 セッション。 *オプション ライセンス：24、50、または 100 セッション。*
ASA 5520	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、または 1000 セッション。*
ASA 5540	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、または 2000 セッション。*
ASA 5550	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、2000、または 3000 セッション。*
ASA 5580	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、2000、3000、5000、または 10,000 セッション。*[2]

モデル	ライセンス要件[1]
ASA 5512-X	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、または 500 セッション。*
ASA 5515-X	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、または 500 セッション。*
ASA 5525-X	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、または 1000 セッション。*
ASA 5545-X	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、または 2000 セッション。*
ASA 5555-X	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、2000、または 3000 セッション。*
ASA 5585-X（SSP-10）	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、2000、または 3000 セッション。*
ASA 5585-X（SSP-20、-40、または -60）	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、2000、3000、5000、または 10,000 セッション。*[2]
ASASM	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、2000、3000、5000、または 10,000 セッション。*[2]

1. 次のアプリケーションでは、接続時に TLS プロキシ セッションを使用します。これらのアプリケーションで使用される各 TLS プロキシ セッション（およびこれらのアプリケーションのみ）は UC ライセンスの制限に対してカウントされます。
   - 電話プロキシ
   - プレゼンス フェデレーション プロキシ
   - 暗号化音声インスペクション

   TLS プロキシ セッションを使用するその他のアプリケーション（ライセンスが不要な Mobility Advantage Proxy、個別の IME ライセンスが必要な IME など）では、UC 制限に対してカウントしません。

   UC アプリケーションによっては、1 つの接続に複数のセッションを使用する場合があります。たとえば、プライマリとバックアップの Cisco Unified Communications Manager を電話に設定した場合は、TLS プロキシ接続が 2 つあるため、UC Proxy セッションも 2 つ使用されます。

   [Configuration] > [Firewall] > [Unified Communications] > [TLS Proxy] ペインを使用して個別に TLS プロキシの制限を設定します。デフォルトの TLS プロキシ制限よりも高い UC ライセンスを適用する場合、ASA では、その UC 制限に一致するように TLS プロキシの制限が自動的に設定されます。UC ライセンスの制限よりも TLS プロキシ制限が優先されます。TLS プロキシ制限を UC ライセンスよりも少なく設定すると、UC ライセンスですべてのセッションを使用できません。

   注：「K8」で終わるライセンス製品番号（たとえばユーザ数が 250 未満のライセンス）では、TLS プロキシ セッション数は 1000 までに制限されます。「K9」で終わるライセンス製品番号（たとえばユーザ数が 250 以上のライセンス）では、TLS プロキシの制限はコンフィギュレーションに依存し、モデルの制限が最大数になります。K8 と K9 は、エクスポートについてそのライセンスが制限されるかどうかを示します。K8 は制限されず、K9 は制限されます。

   注：設定をクリアすると、TLS プロキシ制限がモデルのデフォルトに設定されます。このデフォルトが UC ライセンスの制限よりも低い場合、制限を再度引き上げるようにエラー メッセージが表示されます（ASDM の [TLS Proxy] ペインを使用します）。フェールオーバーを使用して、プライマリ ユニットで [File] > [Save Running Configuration to Standby Unit] を使用して設定の同期を強制する場合、**clear configure all** コマンドがセカンダリ ユニットに自動的に生成されるので、セカンダリ ユニットに警告メッセージが表示されることがあります。コンフィギュレーションの同期によりプライマリ装置の TLS プロキシ制限の設定が復元されるため、この警告は無視できます。

   接続には、SRTP 暗号化セッションを使用する場合もあります。
   - K8 ライセンスでは、SRTP セッション数は 250 までに制限されます。
   - K9 ライセンスに制限はありません。

   （注） メディアの暗号化/復号化を必要とするコールだけが、SRTP 制限に対してカウントされます。コールに対してパススルーが設定されている場合は、両方のレッグが SRTP であっても、SRTP 制限に対してカウントされません。
2. 10,000 セッション UC ライセンスの場合、組み合わせたセッション数は合計 10,000 までですが、電話プロキシ セッションの最大数は 5000 です。

ライセンスの詳細については、一般的な操作のコンフィギュレーション ガイドの Chapter 3, “Managing Feature Licenses for Cisco ASA Version 9.1.” を参照してください。

電話プロキシの前提条件

ここでは、次の内容について説明します。

メディア ターミネーション インスタンスの前提条件

ASA には、次の基準を満たすメディア ターミネーション インスタンスが必要です。

- ASA 上の電話プロキシごとに、メディアの停止を 1 つ設定する必要があります。ASA では、複数のメディア ターミネーション インスタンスはサポートされていません。
- メディア ターミネーション インスタンスでは、すべてのインターフェイスに対してグローバルなメディア ターミネーション アドレスを設定することも、インターフェイスごとにメディア ターミネーション アドレスを設定することもできます。しかし、グローバルなメディア ターミネーション アドレスと、インターフェイスごとに設定するメディア ターミネーション アドレスは同時に使用できません。
- 複数のインターフェイスに対してメディア ターミネーション アドレスを設定する場合、IP 電話との通信時に ASA で使用するアドレスを、インターフェイスごとに設定する必要があります。

  たとえば、ASA 上に 3 つのインターフェイス（1 つの内部インターフェイスと 2 つの外部インターフェイス）があって、いずれかの外部インターフェイスだけを IP 電話との通信に使用する場合、メディア ターミネーション アドレスを 2 つ（内部インターフェイスに 1 つ、IP 電話と通信する外部インターフェイスに 1 つ）設定します。
- 1 つのインターフェイスに設定できるメディア ターミネーション アドレスは 1 つだけです。
- IP アドレスは、そのインターフェイスのアドレス範囲内で使用されていない、パブリックにルーティング可能な IP アドレスです。
- インターフェイスの IP アドレスを、ASA 上のインターフェイスと同じアドレスにはできません。
- IP アドレスを、既存のスタティック NAT プールまたは NAT ルールとオーバーラップさせることはできません。
- IP アドレスを、Cisco UCM や TFTP サーバと同じ IP アドレスにはできません。
- ルータやゲートウェイの背後の IP 電話についても、この前提条件を満たす必要があります。ルータまたはゲートウェイで、IP 電話と通信する ASA インターフェイス上のメディア ターミネーション アドレスにルートを追加して、電話からそのアドレスに到達できるようにします。

Cisco UCM の証明書

Cisco UCM に保存されている次の証明書をインポートします。ASA で電話プロキシを使用するには、これらの証明書が必要です。

- Cisco_Manufacturing_CA
- CAP-RTP-001
- CAP-RTP-002
- CAPF 証明書（任意）

LSC プロビジョニングが必要な場合や、IP 電話の LSC がイネーブルになっている場合は、Cisco UCM から CAPF 証明書をインポートする必要があります。Cisco UCM に CAPF 証明書が複数ある場合は、それらのすべてを ASA にインポートする必要があります。

（注）　LSC プロビジョニングを設定すると、エンドユーザ認証を追加できます。詳細については、Cisco Unified Communications Manager のコンフィギュレーション ガイドを参照してください。

たとえば、電話プロキシで IP 電話の証明書を検証するには、CA 製造業者証明書が必要です。

DNS lookup の前提条件

- Cisco UCM に IP アドレスではなく Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）を設定した場合は、ASA で DNS lookup を設定してイネーブルにする必要があります。
- DNS lookup の設定後、ASA から、設定した FQDN で Cisco UCM を ping できることを確認します。
- CAPF サービスがイネーブルになっており、Cisco UCM がパブリッシャ上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 で設定されている場合は、DNS lookup を設定する必要があります。

Cisco Unified Communications Manager の前提条件

- TFTP サーバは、Cisco UCM と同じインターフェイス上に置く必要があります。
- Cisco UCM は内部のプライベート ネットワーク上に置くことができますが、ASA 上の Cisco UCM には、ルーティング可能なパブリック アドレスに対するスタティック マッピングが必要です。
- Cisco UCM に NAT が必要な場合は、既存のファイアウォール上ではなく、ASA 上に設定する必要があります。

ACL ルール

既存のファイアウォールの背後に電話プロキシが構成されている場合は、シグナリングを許可するアクセス リストのルール、TFTP 要求、および電話プロキシへのメディア トラフィックを設定する必要があります。

TFTP サーバまたは Cisco UCM 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 ACL で使用する必要があります。

表 16-1 に、既存のファイアウォールに設定する必要があるポートを示します。

表 16-1　ポート設定要件

アドレス	ポート	プロトコル	説明
メディアの停止	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

表 16-1　ポート設定要件 （続き）

アドレス	ポート	プロトコル	説明
Cisco UCM	2443	TCP	セキュア SCCP の着信を許可する
Cisco UCM	5061	TCP	セキュア SIP の着信を許可する
（Cisco UCM 上の）CAPF サービス	3804	TCP	LSC プロビジョニングに対する CAPF サービスを許可する

（注）　これらすべてのポートは、TFTP を除き、Cisco UCM に設定可能です。これらはデフォルト値であり、Cisco UCM 上で変更した場合は、変更する必要があります。たとえば、CAPF サービスのデフォルト ポートは 3804 です。Cisco UCM 上でこのデフォルト値を変更した場合は、変更する必要があります。

NAT と PAT の前提条件

NAT の前提条件

- TFTP サーバに対して NAT を設定する場合は、TFTP サーバで電話プロキシの設定を行う前に NAT 設定を行う必要があります。
- TFTP サーバまたは Cisco UCM 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 ACL で使用する必要があります。

PAT の前提条件

- Skinny インスペクション グローバル ポートにデフォルト以外のポートを使用するように設定する場合は、このノンセキュア ポートを `global_sccp_port+443` として設定する必要があります。

  したがって、*global_sccp_port* が 7000 の場合、グローバル セキュア SCCP ポートは 7443 です。電話プロキシ構成に複数の Cisco UCM が含まれていて、インターフェイスの IP アドレスまたはグローバル IP アドレスを共有する必要があるときは、ポートの再設定が必要な場合があります。

（注）　ノンセキュア ポートとセキュア ポートの両方に PAT の設定を行う必要があります。

- IP 電話から Cisco UCM 上の CAPF に接続する必要があって、Cisco UCM にスタティック PAT（LCS プロビジョニングが必要）が設定されている場合は、デフォルト CAPF ポート 3804 にスタティック PAT を設定する必要があります。

複数インターフェイス上にある IP 電話の前提条件

IP 電話が複数インターフェイス上にある場合は、電話プロキシ設定で、Cisco UCM の正しい IP アドレスを CTL ファイルに設定する必要があります。

IP アドレスの正しい設定方法については、次のトポロジ例を参照してください。

```
phones --- (dmz)-----|
                     |----- ASA PP --- (outside Internet) --- phones
phones --- (inside)--|
```

このトポロジ例では、次の IP アドレスを設定します。

- 内部インターフェイス上の Cisco UCM は 10.0.0.5
- DMZ ネットワークは 192.168.1.0/24
- 内部ネットワークは 10.0.0.0/24

Cisco UCM は、DMZ から、外部インターフェイスと内部インターフェイス、外部インターフェイスへ、複数のグローバル IP アドレスでマッピングされます。

IP アドレスが 2 つあるため、CTL ファイル内には Cisco UCM のエントリが 2 つ必要です。たとえば、Cisco UCM の static 文が次のようであったとします。

```
object network obj-10.0.0.5-01
    host 10.0.0.5
    nat (inside,outside) static 209.165.202.129
object network obj-10.0.0.5-02
    host 10.0.0.5
    nat (inside,dmz) static 198.168.1.2
```

この Cisco UCM の場合、CTL ファイルに次の 2 つのレコード エントリが必要です。

```
record-entry cucm trustpoint cucm_in_to_out address 209.165.202.129
record-entry cucm trustpoint cucm_in_to_dmz address 192.168.1.2
```

7960 および 7940 IP Phone のサポート

- これらの IP Phone には MIC が事前インストールされていないため、LSC をインストールする必要があります。電話プロキシで使用する前に、各電話機に LSC をインストールします。そうすれば、ノンセキュア モードで Cisco UCM に IP Phone を登録するためにノンセキュア SCCP ポートを開かずに済みます。

  IP Phone に LSC をインストールする手順については、次のマニュアルを参照してください。

  http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/security/7_0_1/secugd/secucapf.html#wp1093518

（注） 別の Cisco UCM クラスタの LSC が IP Phone にすでにインストールされている場合は、その LSC を削除して、現在の Cisco UCM クラスタから LSC をインストールしてください。

（注） LSC プロビジョニングを設定すると、エンドユーザ認証を追加できます。詳細については、Cisco Unified Communications Manager のコンフィギュレーション ガイドを参照してください。

- CAPF 証明書を ASA にインポートする必要があります。
- ASA 上に作成する CTL ファイルは、CAPF レコード エントリで作成する必要があります。
- SIP プロトコルではこれらの IP Phone の暗号化がサポートされないため、SCCP プロトコルだけを使用するように電話を設定する必要があります。
- 電話プロキシ経由で LSC プロビジョニングを行う場合は、ACL を追加して、IP Phone がノンセキュア ポート 2000 で Cisco UCM に登録できるようにする必要があります。

Cisco IP Communicator の前提条件

Cisco IP Communicator（CIPC）に電話プロキシを設定するには、次の前提条件を満たす必要があります。

- [Configuration] > [Firewall] > [Unified Communications] > [Phone Proxy] の順に選択し、[Call Manager and Phone Settings] 領域の [Enable CICP security mode authentication] チェックボックスをオンにします。
- ACL を作成し、CIPC がノンセキュア モードで Cisco UCM に登録できるようにします。
- SSL 暗号化サイファの 1 つとして null-sha1 を設定します。

現在のバージョンの Cisco IP Communicator（CIPC）は認証モードをサポートしており、TLS シグナリングを実行しますが、音声の暗号化は行いません。

CIPC は、TLS ハンドシェイクの実行に LSC を必要とするため、ノンセキュア モードでクリアテキスト シグナリングを使用して Cisco UCM に登録する必要があります。CIPC が登録できるようにするには、ノンセキュア SIP/SCCP シグナリング ポート（5060/2000）での Cisco UCM への接続を CIPC に許可する ACL を作成します。

（注） LSC プロビジョニングを設定すると、エンドユーザ認証を追加できます。詳細については、Cisco Unified Communications Manager のコンフィギュレーション ガイドを参照してください。

CIPC は TLS ハンドシェイクの実行時に別のサイファを使用するため、null-sha1 サイファと SSL 暗号化の設定が必要です。null-shal 暗号を追加するには、show run all ssl コマンドを使用して ssl encryption コマンドの出力を表示し、null-shal を SSL 暗号化リストの最後に追加します。

（注） CIPC で電話プロキシを使用する際は、エンドユーザが CIPC でデバイス名をリセット（[Preferences] > [Network] タブ > [Use this Device Name] フィールド）することも、管理者が Cisco Unified CM Administration Console でデバイス名をリセット（[Device] メニュー > [Phone Configuration] > [Device Name] フィールド）することもできません。電話プロキシを使用するには、CIPC コンフィギュレーション ファイルの形式を SEP<mac_address>.cnf.xml とする必要があります。デバイス名がこの形式（SEP<mac_address>）でない場合、電話プロキシ経由で Cisco UMC からコンフィギュレーション ファイルを取得できないため、CIPC は機能しません。

レート制限 TFTP 要求の前提条件

リモート アクセスのシナリオにおいては、インターネット経由で接続するすべての IP 電話に、TFTP サーバに対する TFTP 要求の送信が許可されるため、TFTP 要求にレート制限を設定することをお勧めします。

TFTP 要求にレート制限を設定するには、モジュラ ポリシー フレームワークで **police** コマンドを設定します。**police** コマンドの使用方法については、コマンド リファレンスを参照してください。

ポリシングは、設定した最大レート（ビット/秒単位）を超えるトラフィックが発生しないようにして、1 つのトラフィック フローが全体のリソースを占有しないようにする方法です。トラフィックが最大レートを超えると、ASA は超過した分のトラフィックをドロップします。また、ポリシングでは、許可されるトラフィックの最大単一バーストも設定されます。

レート制限の設定例

次の例では、**police** コマンドとモジュラ ポリシー フレームワークを使用して、TFTP 要求にレート制限を設定する方法について説明します。

最初に、電話プロキシに必要な準拠レートを算出します。準拠レートを算出するには、次の数式を使用します。

```
X * Y * 8
```

ここで、

X = 秒あたりの要求数

Y = 各パケットのサイズ（L2、L3、L4、およびペイロードを含む）

したがって、秒あたり 300 の TFTP 要求レートが必要な場合、準拠レートは次のように計算します。

```
300 requests/second * 80 bytes * 8 = 192000
```

どのホストからメディア ターミネーション アドレスに ping できるかを制御するには、ICMP ルールを作成します。[Configuration] > [Device Management] > [Management Access] > [ICMP] の順に選択し、[Add] ボタンをクリックします。

エンドユーザの電話のプロビジョニング

電話プロキシは、TFTP とシグナリングのトランザクションに関して透過的なプロキシです。Cisco UCM TFTP サーバに NAT が設定されていない場合は、Cisco UCM クラスタの TFTP サーバ アドレスを IP 電話に設定する必要があります。

Cisco UCM TFTP サーバに NAT が設定されている場合は、Cisco UCM TFTP サーバのグローバル アドレスが TFTP サーバ アドレスとして IP 電話に設定されます。

エンド ユーザに対する IP 電話の導入方法

どちらのオプションでも、NAT 機能を持つ商用ケーブル/DSL ルータの背後にリモート IP 電話を導入できます。

オプション 1（推奨）

IP 電話をエンド ユーザに配布する前に本社で準備します。

- ネットワーク内部で電話を登録します。電話の設定、イメージのダウンロード、および登録に問題がないことを、IT 部門が確認します。
- Cisco UCM クラスタが混合モードであった場合は、電話機をエンド ユーザに配布する前に CTL ファイルを削除する必要があります。

このオプションの利点は次のとおりです。

- 電話が Cisco UCM に登録され機能しているかどうかがわかっているため、ネットワークや電話プロキシのトラブルシューティングや問題の分離が容易。
- ユーザが低速で時間を要する場合のあるブロードバンド接続経由で電話機にファームウェアをダウンロードする必要がないため、ユーザ エクスペリエンスが向上。

オプション 2

IP 電話をエンド ユーザに配布します。オプション 2 を使用する場合は、適切な Cisco UCM および TFTP サーバの IP アドレスを使用して電話機の設定を変更するように、ユーザに指示する必要があります。

（注）　TLS ハンドシェイクによるリモート IP 電話の認証の代わりに、LSC プロビジョニングによる認証を設定できます。LSC プロビジョニングでは、リモート IP 電話ユーザごとにパスワードを作成し、各ユーザはリモート IP 電話でパスワードを入力して LSC を取得します。

リモート IP 電話の認証に LSC プロビジョニングを使用するには、IP 電話をまずノンセキュア モードで登録する必要があります。このため、IP 電話をエンドユーザに渡す前に、企業ネットワーク内で LSC プロビジョニングを実行することを推奨します。そうしない場合、IP 電話をノンセキュア モードで登録するには、SIP および SCCP 用のノンセキュア シグナリング ポートを ASA 上で管理者が開く必要があります。

CAPF（Certificate Authority Proxy Function; 認証局プロキシ関数）を使用した、ローカルで有効な証明書（LSC）のインストールについては、『Cisco Unified Communications Manager Security Guide』も参照してください。

電話プロキシのガイドラインと制限事項

この項では、次のトピックについて取り上げます。

- 「一般的なガイドラインと制限事項」（P.16-13）
- 「メディア ターミネーション アドレスのガイドラインと制限事項」（P.16-14）

一般的なガイドラインと制限事項

電話プロキシの一般的な制限事項は次のとおりです。

- 電話プロキシ インスタンスは、**phone-proxy** コマンドを使用して ASA 上に 1 つだけ設定できます。**phone-proxy** コマンドの詳細については、コマンド リファレンスを参照してください。「電話プロキシ インスタンスの作成」（P.16-19）も参照してください。
- 電話プロキシは、Cisco UCM クラスタを 1 つだけサポートします。電話プロキシ用に Cisco UCM クラスタを設定する手順については、「CTL ファイルの作成」（P.16-16）を参照してください。
- ASA がトランスペアレント モードまたはマルチ コンテキスト モードで実行されている場合、電話プロキシはサポートされません。
- リモート IP 電話から無効な内線または外線が呼び出された場合、電話プロキシは、Cisco UCM からのアナンシエータ メッセージを再生できません。そのリモート IP 電話には、アナンシエータ メッセージ「Your call cannot be completed ...」の代わりに、高速のビジー信号が再生されます。一方、内部の IP 電話から無効な内線に電話をかけた場合は、アナンシエータ メッセージによって「Your call cannot be completed ...」が再生されます。
- VPN トンネルを介して電話プロキシに接続する電話のパケットは、ASA インスペクション エンジンの検査対象となりません。

- 電話プロキシでは、IP 電話で ASA を通して Real-Time Control Protocol（RTCP; リアルタイム制御プロトコル）パケットを送信することができません。Cisco Unified CM Administration Console の [Phone Configuration] ページで、RTCP パケットをディセーブルにしてください。このオプションの設定方法については、Cisco Unified Communications Manager（CallManager）のマニュアルを参照してください。
- CIPC で電話プロキシを使用する際は、エンドユーザが CIPC でデバイス名をリセット（[Preferences] > [Network] タブ > [Use this Device Name] フィールド）することも、管理者が Cisco Unified CM Administration Console でデバイス名をリセット（[Device] メニュー > [Phone Configuration] > [Device Name] フィールド）することもできません。電話プロキシを使用するには、CIPC コンフィギュレーション ファイルの形式を SEP<mac_address>.cnf.xml とする必要があります。デバイス名がこの形式（SEP<mac_address>）でない場合、電話プロキシ経由で Cisco UMC からコンフィギュレーション ファイルを取得できないため、CIPC は機能しません。
- SCCP ビデオ メッセージでは SRTP キーがサポートされないため、電話プロキシでは、IP 電話で Cisco VT Advantage を使用して SCCP ビデオ メッセージを送信することができません。
- 混合モード クラスタで電話プロキシを使用する場合、ASA を通して、暗号化されたコンフィギュレーション ファイルを Cisco Unified Call Manager で TFTP を使用して IP 電話に送信できません。
- 1 つの NAT デバイスの背後にある複数の IP 電話では、同一のセキュリティ モードを使用するように設定する必要があります。

  電話プロキシを混合モード クラスタ用に設定し、1 つの NAT デバイスの背後にある複数の IP 電話を電話プロキシで登録する場合は、Unified Call Manager で、SIP および SCCP のすべての IP 電話を認証モードまたは暗号化モードに設定するか、すべてをノンセキュア モードに設定する必要があります。

  たとえば、1 つの NAT デバイスの背後に 4 つの IP 電話があり、そのうちの 2 つは SIP で、残りの 2 つは SCCP で設定されている場合、Unified Call Manager で可能な設定は次のとおりです。

  - 2 つの SIP IP 電話：1 つが認証モードで 1 つが暗号化モード、両方が認証モード、または両方が暗号化モード

    2 つの SCCP IP 電話：1 つが認証モードで 1 つが暗号化モード、両方が認証モード、または両方が暗号化モード
  - 2 つの SIP IP 電話：両方がノンセキュア モード

    2 つの SCCP IP 電話：1 つが認証モードで 1 つが暗号化モード、両方が認証モード、両方が暗号化モード
  - 2 つの SIP IP 電話：1 つが認証モードで 1 つが暗号化モード、両方が認証モード、両方が暗号化モード

    2 つの SCCP IP 電話：両方がノンセキュア モード

  この制限事項は、IP 電話用のアプリケーション リダイレクト ルール（TLS から TCP への変換ルール）に起因しています。

メディア ターミネーション アドレスのガイドラインと制限事項

電話プロキシでは、メディア ターミネーション アドレスの設定に関して、次の制限事項があります。

- 電話プロキシでは、強制的にノンセキュア セキュリティ モードを使用しない限り、メディア ターミネーション アドレスの設定時に内部 IP 電話（内部ネットワーク上の IP 電話）を Cisco UCM 以外のネットワーク インターフェイス上に配置できません。

内部 IP 電話が Cisco UCM 以外のネットワーク インターフェイス上にある場合でも、IP 電話のシグナリング セッションはASA を通過しますが、IP 電話トラフィックは電話プロキシを通過しません。このため、内部 IP 電話は Cisco UMC と同じネットワーク インターフェイス上に配置することをお勧めします。

Cisco UMC と内部 IP 電話を異なるネットワーク インターフェイス上に配置する必要がある場合は、Cisco UMC があるメディア ターミネーション アドレスのネットワーク インターフェイスにアクセスするルートを、内部 IP 電話に追加する必要があります。

グローバルなメディア ターミネーション アドレスを使用するように電話プロキシを設定した場合は、すべての IP 電話に同じグローバル アドレスが表示されます。これはルーティング可能なパブリック アドレスです。

- メディア ターミネーション アドレスを（グローバル インターフェイスを使用せずに）複数インターフェイスに設定する場合は、電話プロキシ サービス ポリシーの適用前に、少なくとも 2 つのインターフェイス（内部インターフェイスと外部インターフェイス）上にメディア ターミネーション アドレスを設定する必要があります。そうしないと、SIP インスペクションと Skinny インスペクションで電話プロキシをイネーブルにした際に、エラー メッセージが表示されます。
- 電話プロキシで一度に使用できるメディア ターミネーション インスタンスは 1 つのタイプだけです。たとえば、すべてのインターフェイスに対してグローバルなメディア ターミネーション アドレスを設定することも、インターフェイスごとにメディア ターミネーション アドレスを設定することもできます。しかし、グローバルなメディア ターミネーション アドレスと、インターフェイスごとに設定するメディア ターミネーション アドレスは同時に使用できません。

電話プロキシの設定

この項では、次のトピックについて取り上げます。

電話プロキシの設定のタスク フロー

（注）　この機能は、適応型セキュリティ アプライアンスのバージョン 8.1.2 に対してはサポートされていません。

Phone Proxy を設定するには、次の手順に従います。

ステップ 1：CTL ファイルを作成します。「CTL ファイルの作成」（P.16-16）を参照してください。

ステップ 2：暗号化シグナリングを処理する TLS Proxy インスタンスを作成します。「TLS Proxy インスタンスの追加」（P.17-9）を参照してください。

ステップ 3：Phone Proxy インスタンスを作成します。「電話プロキシ インスタンスの作成」（P.16-19）を参照してください。

ステップ 4：Phone Proxy のメディア停止アドレスを設定します。「メディア ターミネーション インスタンスの作成」（P.16-18）を参照してください。

（注）　Phone Proxy の SIP および Skinny インスペクションをイネーブルにする（Phone Proxy をサービス ポリシー ルールに適用することによって行います）前に、Phone Proxy に、MTA インスタンス、TLS Proxy、および CTL ファイルが割り当てられていないと、Phone Proxy をサービス ポリシーに適用できません。さらに、Phone Proxy をサービス ポリシー ルールに適用すると、Phone Proxy を変更または削除できなくなります。

Step 5：Phone Proxy の SIP および Skinny インスペクションをイネーブルにします。「SIP インスペクション」（P.11-21）および「Skinny（SCCP）インスペクション」（P.11-33）を参照してください。

CTL ファイルの作成

Phone Proxy によって要求される証明書信頼リスト（CTL）ファイルを作成します。新しい CTL ファイルを作成、または、フラッシュ メモリから解析するための既存の CTL ファイルのパスを指定することによって、必要な証明書を指定します。

トラストポイントを作成し、IP 電話にとって信頼できるものでなければならない、ネットワーク内の各エンティティ（CUCM、CUCM と TFTP、TFTP サーバ、CAPF）の証明書を生成します。証明書は、CTL ファイルの作成に使用されます。ネットワーク内の各 CUCM（セカンダリ CUCM が使用されている場合は、プライマリとセカンダリ）と TFTP サーバのトラストポイントを作成する必要があります。トラストポイントは、CUCM を信頼する電話の CTL ファイル内にある必要があります。

TFTP 中に IP 電話に対して示される CTL ファイルを作成します。NAT が設定されている場合、アドレスは、TFTP サーバまたは CUCM の、変換済みまたはグローバル アドレスである必要があります。

ファイルを作成すると、TFTP ファイルに署名するために Phone Proxy によって使用される内部トランスポイントが作成されます。トラストポイントには **_internal_PP_***ctl-instance_filename* という名前が付けられます。

（注）　CTL ファイル インスタンスが Phone Proxy に割り当てられると、そのインスタンスは [CTL File] ペインで修正できなくなり、ペインがディセーブルになります。電話プロキシに割り当てられている CTL ファイルを修正するには、[Phone Proxy] ペイン（[Configuration] > [Firewall] > [Unified Communications] > [Phone Proxy]）に移動し、[Use the Certificate Trust List File generated by the CTL instance] チェックボックスをオフにします。

[Create a Certificate Trust List (CTL) File] ペインを使用して、Phone Proxy の CTL ファイルを作成します。このペインによって、ASA との TFTP ハンドシェイク中に IP 電話に提示される CTL ファイルが作成されます。電話プロキシによって使用される CTL ファイルの詳細な概要については、「CTL ファイルの作成」（P.16-16）を参照してください。

[Create a Certificate Trust List (CTL) File] ペインは、CTL ファイルを生成するための属性を設定するために使用されます。CTL ファイル インスタンスの名前は、ASDM によって生成されます。ユーザが CTL ファイル インスタンス コンフィギュレーションを編集しようとすると、ASDM によって、最初に **shutdown** CLI コマンドが、そして最後のコマンドとして **no shutdown** CLI コマンドが自動的に生成されます。

このペインにアクセスするには、[Configuration] > [Firewall] > [Unified Communications] > [CTL File] ペインの順に選択します。

ステップ 1　[Configuration] > [Firewall] > [Unified Communications] > [CTL File] ペインを開きます。

ステップ 2　[Enable Certificate Trust List File] チェックボックスをオンにして、機能をイネーブルにします。

ステップ 3　Phone Proxy に対して使用する CTL ファイルを指定するには、次のいずれかを実行します。

- 既存の CTL ファイルが利用できる場合は、ASDM の [Tools] メニューにあるファイル管理ツールを使用して、その CTL ファイルをフラッシュ メモリにダウンロードします。[Use certificates present in the CTL stored in flash] オプション ボタンをオンにして、テキスト ボックスに CTL ファイルの名前とパスを指定します。

  既存の CTL ファイルを使用して、IP 電話にとって信頼できるものでなければならない、ネットワーク内の各エンティティ（CUCM、CUCM と TFTP、TFTP サーバ、CAPF）のトラストポイントをインストールします。各エンティティの正しい IP アドレス（つまり、CUCM または TFTP サーバに対して IP 電話が使用する IP アドレス）が格納されている既存の CTL ファイルがある場合、そのファイルを使用して、新しい CTL ファイルを作成できます。既存の CTL ファイルのコピーをフラッシュ メモリに保存し、そのコピーを `CTLFile.tlv` とは異なる名前に変更します。
- 既存の CTL ファイルが使用できない場合、[Create new CTL file] オプション ボタンをオンにします。

  ネットワーク内の各エンティティ（CUCM、TFTP、CUCM-TFTP オプションなど）に対する Record エントリを追加するには、[Add] をクリックします。[Add Record Entry] ダイアログボックスが開きます。「CTL ファイル内の Record エントリの追加または編集」（P.16-17）を参照してください。

ステップ 4　必要な番号 SAST 証明書トークンを指定します。デフォルトは 2 です。指定できる最大数は 5 です。

PhoneProxy によって CTL ファイルが生成されるので、CTL ファイル自体に署名するための System Administrator Security Token（SAST）キーを作成する必要があります。このキーは、ASA で生成できます。SAST は、自己署名証明書として作成されます。通常、CTL ファイルには複数の SAST が含まれています。ある SAST が回復可能でない場合は、後でもう 1 つの SAST を使用してファイルを署名できます。

ステップ 5　[Apply] をクリックして CTL ファイル コンフィギュレーション設定内容を保存します。

CTL ファイル内の Record エントリの追加または編集

（注）　この機能は、適応型セキュリティ アプライアンスのバージョン 8.1.2 に対してはサポートされていません。

[Add/Edit Record Entry] ダイアログボックスを使用して、CTL ファイルの作成に使用されるトラストポイントを指定します。

（注）　CTL ファイル内のエントリを編集するには、[Edit Record Entry] ダイアログボックスを使用しますが、このダイアログボックスで設定を変更しても、電話プロキシの関連設定は変更されません。たとえば、CUCM または TFTP サーバの IP アドレスをこのダイアログボックスで編集すると、変更されるのは CTL ファイル内のみであり、これらのサーバの実際のアドレスが変更されることも、電話プロキシに必要なアドレス変換が更新されることもありません。
CTL ファイルの設定を修正するには、Unified Communications Wizard をもう一度実行して CTL ファイル設定を編集して、すべての電話プロキシ設定を確実に正しく同期させることを推奨します。

CTL ファイルで必要な各エントリに対して、さらに record-entry コンフィギュレーションを追加します。

ステップ 1　[Configuration] > [Firewall] > [Unified Communications] > [CTL File] ペインを開きます。

ステップ 2　[Enable Certificate Trust List File] チェックボックスをオンにして、機能をイネーブルにします。

ステップ 3　[Type] フィールドで、作成するトラストポイントのタイプを指定します。

- [cucm]：このトラストポイントの役割を CCM に指定します。複数の CCM トラストポイントを設定できます。
- [cucm-tftp]：このトラストポイントの役割を CCM+TFTP に指定します。複数の CCM+TFTP トラストポイントを設定できます。
- [tftp]：このトラストポイントの役割を TFTP に指定します。複数の TFTP トラストポイントを設定できます。
- [capf]：このトラストポイントの役割を CAPF に指定します。1 つの CAPF トラストポイントのみを設定できます。

ステップ 4　[Host] フィールドで、トラストポイントの IP アドレスを指定します。NAT が設定されている場合、指定する IP アドレスは、TFTP サーバまたは CUCM のグローバル アドレスである必要があります。グローバル IP アドレスは IP 電話によって検出される IP アドレスです。これは、グローバル IP アドレスは、トラストポイントの CTL レコードに対して使用される IP アドレスになるからです。

ステップ 5　[Certificate] フィールドで、CTL ファイル内のレコード エントリに対する ID 証明書を指定します。新しい ID 証明書を作成するには、[Manage] をクリックします。[Manage Identify Certificates] ダイアログボックスが開きます。一般的な操作のコンフィギュレーション ガイドの“Configuring Identity Certificates Authentication” section on page 38-55 を参照してください。

自己署名証明書を生成するか、SCEP 登録によって証明書を取得するか、PKCS-12 フォーマットで証明書をインポートすることによって、ID 証明書を追加できます。CTL ファイルの設定に関する要件に基づいて、最適なオプションを選択してください。

ステップ 6　（任意）[Domain Name] フィールドで、トラストポイントの DNS フィールドの作成に使用される、トラストポイントのドメイン名を指定します。この名前は、サブジェクト DN の一般名フィールドに追加されて、DNS 名が作成されます。トラストポイントに FQDN が設定されていない場合は、ドメイン名を設定する必要があります。domain-name は、1 つのみ指定できます。

（注）　CUCM および TFTP サーバのドメイン名を使用している場合、ASA 上で DNS 検索を設定する必要があります。ASA の各外部インターフェイスのエントリを DNS サーバに追加します（これらのエントリがすでに存在しない場合）。ASA の各外部 IP アドレスには、ルックアップ用に関連付けられている DNS エントリが含まれている必要があります。これらの DNS エントリに対しては、逆ルックアップもイネーブルにする必要があります。さらに、ASA 上の DNS サーバ IP アドレスを定義します。たとえば、`dns name-server 10.2.3.4`（DNS サーバの IP アドレス）。

メディア ターミネーション インスタンスの作成

電話プロキシで使用する、メディア ターミネーション インスタンスを作成します。

設定するメディア ターミネーション アドレスは、「メディア ターミネーション インスタンスの前提条件」（P.16-7）の説明に従って要件を満たす必要があります。

（注）　8.2（1）以前のバージョンでは、リモート Cisco IP 電話がある適応型セキュリティ アプライアンスの外部インターフェイス上に、1 つのメディア停止アドレス（MTA）を設定していました。バージョン 8.2(1) 以降では、すべてのインターフェイスのためのグローバルなメディア ターミネーション アドレスを設定することも、インターフェイスごとに別のメディア ターミネーション アドレスを設定するこ

ともできます。

この機能拡張の結果、以前のコンフィギュレーションは非推奨となりました。必要な場合は、引き続き古いコンフィギュレーションを使用できます。ただし、コンフィギュレーションを変更する必要がある場合、新しいコンフィギュレーション方式だけが受け付けられます。古いコンフィギュレーションは復元できません。下位互換性を維持する必要がある場合は、古いコンフィギュレーションをそのままの形で維持する必要があります。

ステップ 1　[Configuration] > [Firewall] > [Unified Communications] > [Media Termination Address] ペインを開きます。

ステップ 2　[Enable Media Termination Address] チェックボックスをオンにしてこの機能をイネーブルにします。

ステップ 3　[Media Termination Address Settings] 領域で、メディア ターミネーション アドレス（MTA）をインターフェイスごとに設定するか、グローバル MTA を設定するかを指定します。すべてのインターフェイスに対してグローバル メディア停止アドレスを設定したり、各インターフェイスに対して 1 つのメディア停止アドレスを設定したりできます。

- インターフェイスごとに MTA を設定するには、[Configure MTA per Interface] オプション ボタンをクリックし、[Add] ボタンをクリックします。表示されるダイアログボックスで、インターフェイス名を指定し、IP アドレスまたはホスト名を入力します。

  複数のインターフェイスに対してメディア ターミネーション アドレスを設定する場合、IP 電話との通信時に ASA で使用するアドレスを、インターフェイスごとに設定する必要があります。IP アドレスは、そのインターフェイスのアドレス範囲内で使用されていない、パブリックにルーティング可能な IP アドレスです。

  メディア停止インスタンスの作成時およびメディア停止アドレスの設定時に従う必要があるすべての要件の一覧については、「メディア ターミネーション インスタンスの前提条件」（P.16-7）を参照してください。

- グローバル MTA を設定するには、[Configure global MTA on interface] オプション ボタンをクリックし、テキスト ボックスに IP アドレスを入力します。グローバル メディア停止アドレスの設定時に従う必要があるすべての要件の一覧については、「メディア ターミネーション インスタンスの前提条件」（P.16-7）を参照してください。

ステップ 4　メディア停止インスタンスの RTP ポート範囲の最小および最大値を指定します。最小ポートと最大ポートに指定できる値の範囲は 1024 ～ 65535 です。

ステップ 5　[Apply] をクリックして、メディア ターミネーション アドレスのコンフィギュレーション設定内容を保存します。

電話プロキシ インスタンスの作成

電話プロキシ インスタンスを作成します。電話プロキシのすべての機能を使用するには、この他にも必要なタスクがあります。たとえば、MTA の作成と SIP および SCCP（Skinny）インスペクションのイネーブル化です。すべてのタスクの一覧については、「電話プロキシの設定のタスク フロー」（P.16-15）を参照してください。

前提条件

電話プロキシ用の CTL ファイルおよび TLS プロキシ インスタンスの作成が完了している必要があります。

「CTL ファイルの作成」（P.16-16）および「TLS Proxy インスタンスの追加」（P.17-9）を参照してください。

（注）　この機能は、適応型セキュリティ アプライアンスのバージョン 8.1.2 に対してはサポートされていません。

[Configure Phone Proxy] ペインを使用して、Phone Proxy を追加します。

このペインにアクセスするには、[Configuration] > [Firewall] > [Unified Communications] > [Phone Proxy] ペインの順に選択します。

ステップ 1　[Configuration] > [Firewall] > [Unified Communications] > [Phone Proxy] ペインを開きます。

ステップ 2　[Enable Phone Proxy] チェックボックスをオンにして、機能をイネーブルにします。

ステップ 3　メディア ターミネーション アドレスを電話プロキシ インスタンスに追加するには、[Apply MTA instance to Phone Proxy] チェックボックスをオンにします。メディア停止アドレスが設定されている必要があります。設定済みアドレスは、Phone Proxy インスタンスに追加されます。

（注）　メディア停止アドレスを設定するには、[Configure MTA] ボタンをクリックします。[Media Termination Address] ダイアログボックスが表示されます。[Add MTA instance to Phone Proxy] チェックボックスをオンにすると、メディア停止アドレス インスタンスが変更できなくなり、ボタンが [View MTA Configuration] に変わります。メディア停止アドレスを変更するには、[Add MTA instance to Phone Proxy] チェックボックスをオフにします。

ステップ 4　必要に応じて、電話プロキシの TFTP サーバを追加します。電話プロキシのための新しい TFTP サーバを追加するには、[Add] をクリックします。[Add TFTP Server] ダイアログボックスが開きます。「電話プロキシの TFTP サーバの追加または編集」（P.16-22）を参照してください。

（注）　TFTP サーバは、Cisco Unified Call 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。さらに、NAT が TFTP サーバに対して設定してある場合、Phone Proxy インスタンスの作成中に TFTP サーバの指定を設定する前に、NAT コンフィギュレーションを設定する必要があります。

ステップ 5　次のいずれかを実行して、Phone Proxy に対して使用する CTL ファイルを指定します。

- 既存の CTL ファイルを使用するには、[Use the Certificate Trust List File generated by the CTL instance] チェックボックスをオンにします。
- 新しい Phone Proxy の CTL ファイルを作成するには、リンク [Generate Certificate Trust List File] をクリックします。[Create a Certificate Trust List (CTL) File] ペインが開きます。「CTL ファイルの作成」（P.16-16）を参照してください。

ステップ 6　CUCM クラスタのセキュリティ モードを指定するには、[CUCM Cluster Mode] フィールドで、次のオプションのいずれかをクリックします。

- [Non-secure] : Phone Proxy 機能の設定時にノンセキュア モードになるクラスタ モードを指定します。
- [Mixed] : Phone Proxy 機能の設定時に混合モードになるクラスタ モードを指定します。

ステップ 7　セキュア電話機エントリが Phone Proxy データベースから削除されるまでのアイドル時間（デフォルトは 5 分）を設定するには、*hh*:*mm*:*ss* のフォーマットで値を入力します。

セキュア フォンによって起動時に必ず CTL ファイルが要求されるため、電話プロキシは、電話をセキュアとしてマークするデータベースを作成します。セキュア電話機データベース内のエントリは、指定された設定済みタイムアウト後に削除されます。エントリのタイムスタンプは、Phone Proxy が、SIP 電話機、および SCCP 電話機のキープアライブの登録リフレッシュを受信するたびに更新されます。

SCCP キープアライブおよび SIP レジスタ更新の最大タイムアウト値より大きい値を指定します。たとえば、SCCP キープアライブが 1 分間隔で設定されており、SIP 登録リフレッシュが 3 分に設定されている場合、このタイムアウト値は 3 分を超える値に設定します。

ステップ 8　IP 電話上の Call Manager コンフィギュレーションを保持するには、[Preserve the Call Manager's configuration on the phone...] チェックボックスをオンにします。このチェックボックスをオフにすると、次のサービス設定が IP 電話でディセーブルになります。

- PC Port
- Gratuitous ARP
- Voice VLAN Access
- Web Access
- Span to PC Port

ステップ 9　CIPC ソフトフォンが音声およびデータ VLAN シナリオで採用されている場合に、強制的に Cisco IP Communicator（CIPC）ソフトフォンを認証モード内で動作させるには、[Enable CIPC security mode authentication] チェックボックスをオンにします。

CIPC は、LSC が TLS ハンドシェイクを実行することを要求するので、クリアテキスト シグナリングを使用して、CIPC をノンセキュア モードの CUCM に登録する必要があります。CIPC の登録を可能にするには、CIPC がノンセキュア SIP/SCCP シグナリング ポート（5060/2000）上の CUCM に接続することを許可する ACL を作成します。

CIPC は TLS ハンドシェイクの実行時に別のサイファを使用するため、null-sha1 サイファと SSL 暗号化の設定が必要です。null-shal 暗号化を追加するには、[Configuration] > [Device Management] > [Advanced] > [SSL Settings] > [Encryption] セクションに移動します。null-shal SSL 暗号化タイプを選択し、それを [Available Algorithms] に追加します。

現在のバージョンの Cisco IP Communicator（CIPC）は認証モードをサポートしており、TLS シグナリングを実行しますが、音声の暗号化は行いません。

ステップ 10　<proxyServerURL> タグの下の IP フォンのコンフィグレーション ファイルに書き込まれる Phone Proxy 機能の HTTP プロキシを設定するには、以下を実行します。

a. [Configure a http-proxy which would be written into the phone's config file...] チェックボックスをオンにします。

b. [IP Address] フィールドで、HTTP プロキシの IP アドレスと、HTTP プロキシのリスニング ポートを入力します。

入力する IP アドレスは､IP フォンと HTTP プロキシが存在している場所に基づいたグローバル IP アドレスにします。[IP Address] フィールドにホスト名を入力できるのは、ASA によってホスト名が IP アドレスに解決できるとき（DNS 検索が設定されている場合など）です。ASA によって、ホスト名が IP アドレスに解決されるからです。ポートが指定されていない場合、デフォルトで 8080 になります。

c. [Interface] フィールドで、ASA 上の、HTTP プロキシが常駐しているインターフェイスを選択します。

電話プロキシのプロキシ サーバ コンフィギュレーション オプションを設定すると、DMZ または外部ネットワークで HTTP プロキシを使用できます。これらのネットワークでは、電話機上のサービスについてすべての IP フォンの URL がこのプロキシ サーバに誘導されます。この設定では、非セキュアな HTTP トラフィックに対応します。このようなトラフィックは社内ネットワークに入ることはできません。

ステップ 11　[Apply] をクリックして電話プロキシ コンフィギュレーション設定内容を保存します。

（注）　Phone Proxy インスタンスを作成したら、そのインスタンスの SIP および Skinny インスペクションをイネーブルにします。「SIP インスペクション」（P.11-21）および「Skinny（SCCP）インスペクション」（P.11-33）を参照してください。

ただし、Phone Proxy の SIP および Skinny インスペクションをイネーブルにする（Phone Proxy をサービス ポリシー ルールに適用することによって行います）前に、Phone Proxy に、MTA インスタンス、TLS Proxy および CTL ファイルが割り当てられていないと、Phone Proxy をサービス ポリシーに適用できません。さらに、Phone Proxy をサービス ポリシー ルールに適用すると、Phone Proxy を変更または削除できなくなります。

電話プロキシの TFTP サーバの追加または編集

（注）　この機能は、適応型セキュリティ アプライアンスのバージョン 8.1.2 に対してはサポートされていません。

（注）　TFTP サーバ設定を編集するには、[Edit TFTP Server] ダイアログボックスを使用しますが、このダイアログボックスで設定を変更しても電話プロキシのための関連設定は変更されません。たとえば、TFTP サーバの IP アドレスをこのダイアログボックスで編集しても、CTL ファイル内の設定は変更されず、電話プロキシに必要なアドレス変換が更新されることもありません。
TFTP サーバ設定を修正するには、Unified Communications Wizard をもう一度実行して、すべての電話プロキシ設定を確実に正しく同期させることを推奨します。

ステップ 1　[Configuration] > [Firewall] > [Unified Communications] > [Phone Proxy] ペインを開きます。

ステップ 2　[Enable Phone Proxy] チェックボックスをオンにして、機能をイネーブルにします。

ステップ 3　電話プロキシの TFTP サーバ情報を追加または編集するには、[Add] ボタンまたは [Edit] ボタンをクリックします。[Add/Edit TFTP Server] ダイアログボックスが表示されます。

[Add/Edit TFTP Server] ダイアログボックスを使用して、TFTP サーバと、TFTP サーバが常駐するインターフェイスの IP アドレスを指定します。

電話プロキシには、少なくとも 1 つの CUCM TFTP サーバを設定する必要があります。電話プロキシに対して TFTP サーバを 5 つまで設定できます。

TFTP サーバは、信頼ネットワーク上のファイアウォールの背後に存在すると想定されます。そのため、電話プロキシは IP 電話と TFTP サーバの間の要求を代行受信します。

（注）　NAT が TFTP サーバに対して設定してある場合、Phone Proxy インスタンスの作成中に TFTP サーバを指定する前に、NAT コンフィギュレーションを設定する必要があります。

ステップ 4　[TFTP Server IP Address] フィールドで、TFTP サーバの IP アドレスを指定します。実際の内部 IP アドレスを使用して、TFTP サーバを作成します。

ステップ 5　（任意）[Port] フィールドで、TFTP リクエストをリッスンするための TFTP サーバのポートを指定します。デフォルトの TFTP ポート 69 でない場合に、設定する必要があります。

ステップ 6　[Interface] フィールドで、TFTP サーバが存在するインターフェイスを指定します。TFTP サーバは、Cisco Unified Call Manager（CUCM）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。

ステップ 7　[OK] をクリックして設定を適用します。

電話プロキシの UDP ポート転送用 Linksys ルータの設定

IP 電話が NAT 機能を持つルータの背後にある場合は、UDP ポートを IP 電話の IP アドレスに転送するようにルータを設定できます。具体的には、ルータによる着信 TFTP データ パケットのドロップが原因で、TFTP 要求時に IP 電話のエラーが発生する場合に、ルータに UDP ポート転送を設定します。ポート 69 で IP 電話に対する UDP ポート転送をイネーブルにするように、ルータを設定します。

一部のケーブル/DSL ルータでは、明示的な UDP 転送の代わりに、IP 電話を DMZ ホストとして指定する必要があります。ケーブル/DSL ルータの場合、この特別なホストは、パブリック ネットワークからの着信接続をすべて受信します。

電話プロキシを設定する際、明示的な UDP ポート転送を指定される IP 電話と、DMZ ホストとして指定される IP 電話の間に、機能的な違いはありません。エンド ユーザの能力と好みに応じて選択してください。

ルータの設定

一連の UDP ポートを IP 電話に転送するように、ファイアウォールとルータを設定する必要があります。それにより、コールの受発信時に IP 電話で音声を受信できるようになります。

（注）　この設定の方法は、ケーブル/DSL ルータによって異なります。また、NAT 機能を持つほとんどのルータでは、1 つの IP アドレスに転送可能なポート範囲が限られています。

ファイアウォールとルータのブランドやモデルごとに設定は異なりますが、タスクは同じです。使用するルータのブランドやモデルに固有の手順については、製造業者の Web サイトを参照してください。

Linksys ルータ

ステップ 1　Web ブラウザでルータ管理の Web ページにアクセスします。Linksys の場合、通常は `http://192.168.1.1` です。

ステップ 2　[Applications & Gaming] タブまたは [Port Forwarding] タブ（使用するルータに表示されるタブ）をクリックします。

ステップ 3　ポート転送データのテーブルを見つけて、次の値を含むエントリを追加します。

表 16-2　ルータに追加するポート転送値

アプリケーション	開始	完了	プロトコル	IP アドレス	イネーブル
IP 電話	1024	65535	UDP	*電話の IP アドレス*	オン
TFTP	69	69	UDP	*電話の IP アドレス*	オン

ステップ 4　[Save Settings] をクリックします。ポート転送の設定が完了しました。

電話プロキシの機能履歴

表 16-3 に、この機能のリリース履歴を示します。

表 16-3　Cisco 電話プロキシの機能履歴

機能名	リリース	機能情報
Cisco 電話プロキシ	8.0(4)	電話プロキシ機能が導入されました。電話プロキシ機能に ASDM でアクセスするには、次のオプションを選択します。 [Configuration] > [Firewall] > [Advanced] > [Encrypted Traffic Inspection] > [Phone Proxy] ペイン
メディア ターミネーション アドレスに対する NAT	8.1(2)	メディア ターミネーションのフィールドが [Phone Proxy] ペインから削除され、[Media Termination] ペインに追加されました。 [Configuration] > [Firewall] > [Advanced] > [Encrypted Traffic Inspection] > [Media Termination Address] ペイン