CHAPTER 52

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適応型セキュリティ アプライアンス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。

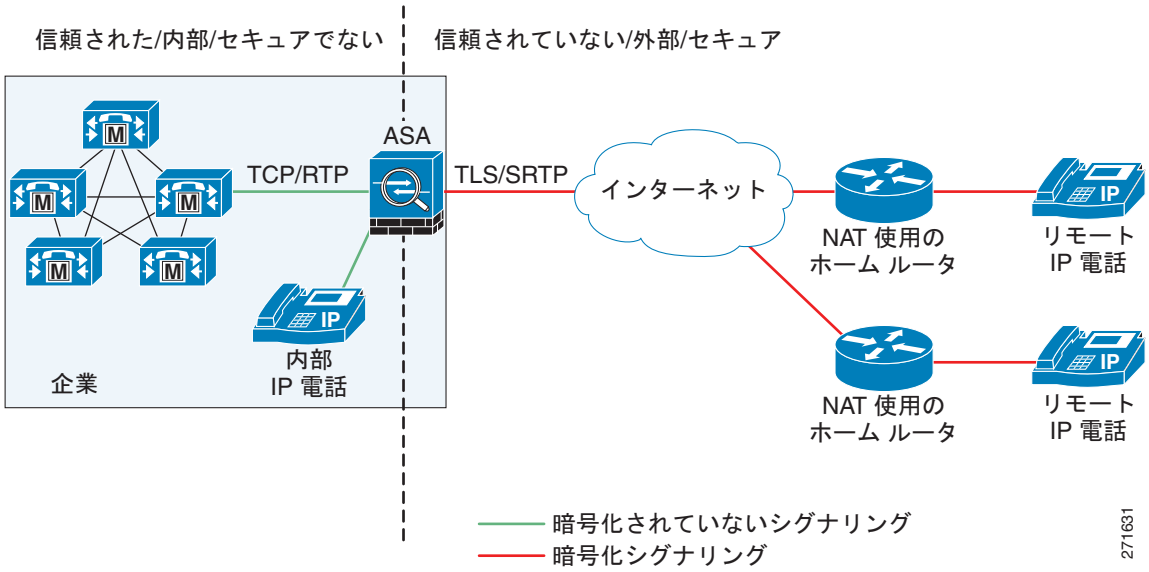
Cisco 電話プロキシに関する情報

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 52-1 を参照してください。

図 52-1　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。

「例 5：混合モードの Cisco UCM クラスタにおける LSC プロビジョニング、パブリッシャ上の Cisco UCM および TFTP サーバ」（P.52-52）を参照してください。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 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。

   tls-proxy maximum-sessions コマンドを使用して TLS プロキシの制限を独立して設定できます。モデルの制限を表示するには、**tls-proxy maximum-sessions ?** コマンドを入力します。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：（たとえば **clear configure all** コマンドを使用して）コンフィギュレーションをクリアすると、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小さいと、tls-proxy maximum-sessions コマンドを使用したときに、再び制限を高めるようにエラー メッセージが表示されます。プライマリ装置でフェールオーバーを使用して、**write standby** コマンドを入力して強制的にコンフィギュレーションの同期を行うと、セカンダリ装置で **clear configure all** コマンドが自動的に生成され、セカンダリ装置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、第 4 章「機能のライセンスの管理」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。

「Cisco UCM からの証明書のインポート」（P.52-17）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 domain-lookup** コマンドと、このコマンドで DNS lookup を設定する方法については、コマンド リファレンスを参照してください。
- 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。

アクセス リストのルール

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」アドレスをアクセス リストで使用する必要があります。

表 52-1 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 52-1　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
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 NAT を設定する場合は、電話プロキシの下で **tftp-server** コマンドを設定する前に 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」アドレスをアクセス リスト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。

```
/* use the default ports for the first CUCM */
object network obj-10.0.0.1-01
    host 10.0.0.1
    nat (inside,outside) static interface service tcp 2000 2000
object network obj-10.0.0.1-02
    host 10.0.0.1
    nat (inside,outside) static interface service tcp 2443 2443
/* use non-default ports for the 2nd CUCM */
object network obj-10.0.0.2-01
    host 10.0.0.2
    nat (inside,outside) static interface service tcp 2000 7000
object network obj-10.0.0.2-02
    host 10.0.0.2
    nat (inside,outside) static interface service tcp 2443 7443
```

（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。

- 電話プロキシ インスタンスの設定時に、**phone-proxy** コマンドの下に **cipc security-mode authenticated** コマンドを含めます。
- 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。したがって、電話プロキシ インスタンスの設定時には次のコマンドを含める必要があります。

cipc security-mode authenticated

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
```

次の設定例では、計算した準拠レートを **police** コマンドで使用する方法を示します。

```
access-list tftp extended permit udp any host 192.168.0.1 eq tftp

class-map tftpclass
    match access-list tftp

policy-map tftpmap
    class tftpclass
    police output 192000

service-policy tftpmap interface inside
```

メディア ターミネーション アドレスを宛先とする ICMP トラフィックについて

メディア ターミネーション アドレスを ping できるホストを管理するには、ASA で **icmp** コマンドを使用して、外部インターフェイスにアクセス ルールを適用します。

外部インターフェイスに適用した ICMP アクセス ルールは、メディア ターミネーション アドレスを宛先とするトラフィックに適用されます。

たとえば、すべてのホストからの、メディア ターミネーション アドレスを宛先とする ICMP ping を拒否するには、次のコマンドを使用します。

icmp deny any outside

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。

「例 5：混合モードの Cisco UCM クラスタにおける LSC プロビジョニング、パブリッシャ上の Cisco UCM および TFTP サーバ」（P.52-52）を参照してください。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.52-14）
- 「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.52-15）

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.52-26）」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.52-20）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。

ノンセキュア Cisco UCM クラスタにおける電話プロキシ設定のタスク フロー

ノンセキュア Cisco UCM クラスタで電話プロキシを設定するには、次のタスクを実行します。

ステップ 1　IP 電話で信頼する必要があるネットワーク内のエンティティ（Cisco UCM、Cisco UCM および TFTP、TFTP サーバ、CAPF）に対して、トラストポイントを作成し、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。「トラストポイントの作成と証明書の生成」（P.52-19）を参照してください。

（注）　トラストポイントの作成と証明書の生成を実行する前に、Cisco UCM に保存されている証明書をインポートする必要があります。「Cisco UCM の証明書」（P.52-7）および「Cisco UCM からの証明書のインポート」（P.52-17）を参照してください。

ステップ 2　電話プロキシ用の CTL ファイルを作成します。「CTL ファイルの作成」（P.52-20）を参照してください。

ステップ 3　TLS プロキシ インスタンスを作成します。「ノンセキュア Cisco UCM クラスタ用の TLS プロキシ インスタンスの作成」（P.52-22）を参照してください。

ステップ 4　電話プロキシ用のメディア ターミネーション インスタンスを作成します。「メディア ターミネーション インスタンスの作成」（P.52-25）を参照してください。

ステップ 5　電話プロキシ 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.52-26）を参照してください。

ステップ 6　電話プロキシを SIP インスペクションと Skinny インスペクションでイネーブルにします。「SIP インスペクションおよび Skinny インスペクションにおける電話プロキシのイネーブル化」（P.52-28）を参照してください。

Cisco UCM からの証明書のインポート

電話プロキシで使用される TLS プロキシが TLS ハンドシェイクを正常に実行するためには、IP 電話の証明書を（Cisco UCM で TLS を実行する場合は、Cisco UCM の証明書も）確認する必要があります。IP 電話の証明書を検証するには、Cisco UCM に保存されている CA 製造業者証明書が必要です。次の手順に従って、CA 製造業者証明書を ASA にインポートします。

ステップ 1　Cisco UCM Operating System Administration の Web ページにアクセスします。

ステップ 2　[Security] > [Certificate Management] の順に選択します。

（注）　以前のバージョンの Cisco UCM では UI と証明書の場所が異なります。たとえば、Cisco UCM バージョン 4.x では、証明書が `C:\Program Files\Cisco\Certificates` ディレクトリにあります。証明書の場所については、Cisco Unified Communications Manager（CallManager）のマニュアルを参照してください。

ステップ 3　[Find] をクリックすると、すべての証明書が表示されます。

ステップ 4　`Cisco_Manufacturing_CA` というファイル名を探します。これが、IP 電話の証明書の確認に必要な証明書です。`Cisco_Manufacturing_CA.pem` という .PEM ファイルをクリックします。証明書情報と、証明書をダウンロードするオプションがあるダイアログボックスが表示されます。

（注）　証明書リストに `Cisco_Manufacturing_CA` というファイル名の証明書が複数含まれている場合は、.pem ファイル拡張子を持つ証明書 `Cisco_Manufacturing_CA.pem` を選択します。

ステップ 5　[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 6　ASA 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。端末経由で登録するのは、ステップ 4 でダウンロードした証明書を貼り付けるためです。

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

ステップ 7　次のコマンドを入力して、トラストポイントを認証します。

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

ステップ 8　「Enter the base 64 encoded CA Certificate.」というメッセージが表示されます。ステップ 4 でダウンロードした .PEM ファイルをコピーし、コマンドラインに貼り付けます。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。証明書に問題がなければ、確認を求める「Do you accept this certificate?[yes/no].」というメッセージが表示されます。**yes** と入力します。

（注） 証明書をコピーする際は、BEGIN および END の列もコピーしてください。

ヒント 証明書に問題がある場合は、**debug crypto ca** コマンドを使用して、PKI アクティビティ（CA で使用）のデバッグ メッセージを表示します。

ステップ 9　次の証明書について、ステップ 1 からステップ 8 を繰り返します。表 52-2 に、ASA で必要な証明書を示します。

表 52-2　セキュリティ アプライアンスで電話プロキシに必要な証明書

証明書名	目的
CallManager	TLS ハンドシェイク時に Cisco UCM を認証します。混合モード クラスタだけに必要です。
Cisco_Manufacturing_CA	Manufacturer Installed Certificate（MIC; 製造元でインストールされる証明書）で IP 電話を認証します。
CAP-RTP-001	MIC で IP 電話を認証します。
CAP-RTP-002	MIC で IP 電話を認証します。
CAPF	LSC で IP 電話を認証します。

混合モードの Cisco UCM クラスタにおける電話プロキシ設定のタスク フロー

（注） 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。

ノンセキュア Cisco UCM クラスタで電話プロキシを設定するには、次のタスクを実行します。

ステップ 1　IP 電話で信頼する必要があるネットワーク内のエンティティ（Cisco UCM、Cisco UCM および TFTP、TFTP サーバ、CAPF）に対して、トラストポイントを作成し、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。「トラストポイントの作成と証明書の生成」（P.52-19）を参照してください。

（注） トラストポイントの作成と証明書の生成を実行する前に、Cisco UCM に保存されている証明書をインポートする必要があります。「Cisco UCM の証明書」（P.52-7）および「Cisco UCM からの証明書のインポート」（P.52-17）を参照してください。

ステップ 2　電話プロキシ用の CTL ファイルを作成します。「CTL ファイルの作成」（P.52-20）を参照してください。

（注）　混合モード クラスタで実行されるように電話プロキシを設定する際は、トラストポイントのインストールに既存の CTL ファイルを使用することもできます。「既存の CTL ファイルの使用」（P.52-22）を参照してください。

ステップ 3　TLS プロキシ インスタンスを作成します。「混合モード Cisco UCM クラスタ用の TLS プロキシの作成」（P.52-23）を参照してください。

ステップ 4　電話プロキシ用のメディア ターミネーション インスタンスを作成します。「メディア ターミネーション インスタンスの作成」（P.52-25）を参照してください。

ステップ 5　電話プロキシ 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.52-26）を参照してください。

ステップ 6　電話プロキシ インスタンスの設定時に（電話プロキシ コンフィギュレーション モードで）次のコマンドを入力して、クラスタのモード（デフォルトはノンセキュア）を混合モードに設定します。

```
hostname(config-phone-proxy)# cluster-mode mixed
```

ステップ 7　電話プロキシを SIP インスペクションと Skinny インスペクションでイネーブルにします。「SIP インスペクションおよび Skinny インスペクションにおける電話プロキシのイネーブル化」（P.52-28）を参照してください。

トラストポイントの作成と証明書の生成

IP 電話で信頼する必要があるネットワーク内のエンティティ（Cisco UCM、Cisco UCM および TFTP、TFTP サーバ、CAPF）に対して、トラストポイントを作成し、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 Cisco UCM（セカンダリ Cisco UCM を使用する場合はプライマリとセカンダリ）および TFTP サーバごとに、トラストポイントを作成する必要があります。電話機で Cisco UCM を信頼するには、これらのトラストポイントが CTL ファイルに必要です。

前提条件

Cisco UCM に保存されている、必要な証明書をインポートします。「Cisco UCM の証明書」（P.52-7）および「Cisco UCM からの証明書のインポート」（P.52-17）を参照してください。

	コマンド	目的
ステップ 1	hostname(config)# **crypto key generate rsa label** *key-pair-label* **modulus** *size* **Example:** crypto key generate rsa label cucmtftp_kp modulus 1024	トラストポイントに使用できるキー ペアを作成します。
ステップ 2	hostname(config)# **crypto ca trustpoint** *trustpoint_name* **Example:** crypto ca trustpoint cucm_tftp_server	ネットワーク内のエンティティ（プライマリ Cisco UCM、セカンダリ Cisco UCM、および TFTP サーバ）ごとにトラストポイントを作成します。 **（注）** TFTP サーバに別個のトラストポイントを作成する必要があるのは、TFTP サーバが Cisco UCM とは異なるサーバ上にある場合だけです。この設定の例については、「例 3：混合モードの Cisco UCM クラスタ、異なるサーバ上の Cisco UCM および TFTP サーバ」（P.52-49）を参照してください。
ステップ 3	hostname(config-ca-trustpoint)# **enrollment self**	自己署名した証明書を生成します。
ステップ 4	hostname(config-ca-trustpoint)# **keypair** *keyname* **Example:** keypair cucmtftp_kp	公開キーが認証の対象となるキー ペアを指定します。
ステップ 5	hostname(config-ca-trustpoint)# **exit**	トラストポイント コンフィギュレーション モードを終了します。
ステップ 6	hostname(config)# **crypto ca enroll** *trustpoint* **Example:** crypto ca enroll cucm_tftp_server	CA サーバの証明書を要求し、ASA で証明書を生成します。 デバイスのシリアル番号をサブジェクト名に含めるかどうかを確認するメッセージが表示されたら、シリアル番号を含める場合は **Y**、含めない場合は **N** と入力します。 自己署名した証明書の生成を求められたら、**Y** と入力します。

次の作業

トラストポイントの作成と証明書の生成が完了したら、電話プロキシ用の CTL ファイルを作成します。「CTL ファイルの作成」（P.52-20）を参照してください。

混合モード クラスタで電話プロキシを設定する場合は、既存の CTL ファイルを使用できます。「既存の CTL ファイルの使用」（P.52-22）を参照してください。

CTL ファイルの作成

TFTP 要求時に IP 電話に提示される CTL ファイルを作成します。

前提条件

Cisco UCM および TFTP サーバのドメイン名を使用する場合は、ASA に DNS lookup 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。

dns domain-lookup *interface_name* コマンド（*interface_name* は DNS サーバへのルートを持つインターフェイス）を使用して、ASA で DNS lookup をイネーブルにします。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）。

（注） **dns domain-lookup** コマンドを複数回入力すると、複数のインターフェイス上で DNS lookup をイネーブルにできます。ASA で複数のコマンドを入力した場合、コンフィギュレーション内の順序で、応答が受信されるまで各インターフェイスが試されます。

dns domain-lookup コマンドについては、コマンド リファレンスを参照してください。

	コマンド	目的

ステップ 1	`hostname(config)# ctl-file ctl_name`
	Example:
	`ctl-file myctl`
		CTL ファイル インスタンスを作成します。

ステップ 2	`hostname(config-ctl-file)# record-entry tftp trustpoint trustpoint_name address TFTP_IP_address`
	Example:
	`record-entry cucm-tftp trustpoint cucm_tftp_server address 10.10.0.26`
		TFTP サーバのレコード エントリを作成します。
		（注） NAT が設定されている場合は、TFTP サーバまたは Cisco UCM のグローバル IP アドレスまたはマッピング IP アドレスを使用します。

ステップ 3	`hostname(config-ctl-file)# record-entry cucm trustpoint trustpoint_name address IP_address`
	Example:
	`record-entry cucm trustpoint cucm_server address 10.10.0.26`
		Cisco UCM（プライマリおよびセカンダリ）ごとにレコード エントリを作成します。
		（注） Cisco UCM のグローバル IP アドレスまたはマッピング IP アドレスを使用します。

ステップ 4	`hostname(config-ctl-file)# record-entry capf trustpoint trust_point address`
	Example:
	`record-entry capf trustpoint capf address 10.10.0.26`
		CAPF のレコード エントリを作成します。
		（注） LSC プロビジョニングが必要な場合か、IP 電話の LSC がイネーブルになっている場合に限り、このコマンドを入力します。

ステップ 5	`hostname(config-ctl-file)# no shutdown`	CTL ファイルを作成します。 ファイルの作成時に、電話プロキシで TFTP ファイルの署名に使用される内部トラスト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。
ステップ 6	`hostname(config)# copy running-configuration startup-configuration`	証明書の設定をフラッシュ メモリに保存します。

次の作業

電話プロキシ用の CTL ファイルの設定が完了したら、TLS プロキシ インスタンスを作成します。ノンセキュア モードにおける電話プロキシ設定時に TLS プロキシを追加するには、「ノンセキュア Cisco UCM クラスタ用の TLS プロキシ インスタンスの作成」（P.52-22）を参照してください。混合モード クラスタで電話プロキシが実行されている場合は、「混合モード Cisco UCM クラスタ用の TLS プロキシの作成」（P.52-23）を参照してください。

既存の CTL ファイルの使用

（注）　電話プロキシが混合モード クラスタで実行されている場合に限り、トラストポイントのインストールに既存の CTL ファイルを使用できます。

エンティティの正しい IP アドレス（IP 電話で Cisco UCM または TFTP サーバ用に使用する IP アドレス）を含む CTL ファイルがすでにある場合は、その CTL ファイルから新しい CTL ファイルを作成できます。これによって、既存の CTL ファイルを利用して、IP 電話で信頼する必要があるネットワーク内の各エンティティ（Cisco UCM、Cisco UCM および TFTP、TFTP サーバ、CAPF）にトラストポイントをインストールできます。

前提条件

クラスタ用の CTL ファイルがある場合は、その CTL ファイルをフラッシュ メモリにコピーします。CTL ファイルをフラッシュ メモリにコピーするときに、ファイルの名前を変更します。`CTLFile.tlv` という名前は使用しないでください。

Cisco UCM および TFTP サーバのドメイン名を使用する場合は、ASA に DNS lookup を設定する必要があります。「CTL ファイルの作成」（P.52-20）の前提条件を参照してください。

	コマンド	目的

ステップ 1	`hostname(config)# ctl-file ctl_name`
	Example:
	`ctl-file myctl`
		CTL ファイル インスタンスを作成します。

ステップ 2	`hostname(config-ctl-file)# cluster-ctl-file filename_path`
	Example:
	`hostname(config-ctl-file)# cluster-ctl-file disk0:/old_ctlfile.tlv`
		フラッシュ メモリに保存した既存の CTL ファイルにあるトラストポイントを使用します。
		既存の CTL ファイルは、`CTLFile.tlv` 以外のファイル名（`old_ctlfile.tlv` など）でフラッシュ メモリに保存されています。

次の作業

既存の CTL ファイルを使用して電話プロキシを設定する際は、必要に応じてファイルにエントリを追加できます。「CTL ファイルの作成」（P.52-20）を参照してください。

電話プロキシ用の CTL ファイルの設定が完了したら、TLS プロキシ インスタンスを作成します。ノンセキュア モードにおける電話プロキシ設定時に TLS プロキシを追加するには、「ノンセキュア Cisco UCM クラスタ用の TLS プロキシ インスタンスの作成」（P.52-22）を参照してください。混合モード クラスタで電話プロキシが実行されている場合は、「混合モード Cisco UCM クラスタ用の TLS プロキシの作成」（P.52-23）を参照してください。

ノンセキュア Cisco UCM クラスタ用の TLS プロキシ インスタンスの作成

暗号化されたシグナリングを処理するための TLS プロキシ インスタンスを作成します。

	コマンド	目的
ステップ 1	hostname(config)# **tls-proxy** *proxy_name* **Example:** tls-proxy mytls	TLS プロキシ インスタンスを作成します。
ステップ 2	hostname(config-tlsp)# **server trust-point** **_internal_PP_***ctl-instance_filename* **Example:** server trust-point _internal_PP_myctl	サーバ トラストポイントを設定し、**_internal_PP_***ctl-instance_filename* という名前の内部トラストポイントを参照します。

次の作業

TLS プロキシ インスタンスの作成が完了したら、電話プロキシ 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.52-26）を参照してください。

混合モード Cisco UCM クラスタ用の TLS プロキシの作成

混合モード クラスタでは、IP 電話がすでに暗号化モードに設定されている場合があるため、Cisco UCM に TLS が必要です。TLS プロキシの LDC 発行元を設定する必要があります。

	コマンド	目的
ステップ 1	hostname(config)# **crypto key generate rsa label** *key-pair-label* **modulus** *size* **Examples:** hostname(config)# crypto key generate rsa label ldc_signer_key modulus 1024 hostname(config)# crypto key generate rsa label phone_common modulus 1024	必要な RSA キー ペアを作成します。 *key-pair-label* は、LDC 署名者キーおよび IP 電話用キーです。
ステップ 2	hostname(config)# **crypto ca trustpoint** *trustpoint_name* **Example:** hostname(config)# crypto ca trustpoint ldc_server	Cisco IP Phone の LDC に署名する内部ローカル CA を作成します。 *trustpoint_name* は LDC 用です。
ステップ 3	hostname(config-ca-trustpoint)# **enrollment self**	自己署名した証明書を生成します。
ステップ 4	hostname(config-ca-trustpoint)# **proxy-ldc-issuer**	TLS プロキシのダイナミック証明書を発行するトラストポイントに、ローカル CA の役割を定義します。
ステップ 5	hostname(config-ca-trustpoint)# **fqdn** *fqdn* **Example:** hostname(config-ca-trustpoint)# fqdn my_ldc_ca.example.com	登録時に、指定した FQDN を証明書の Subject Alternative Name 拡張子に含めます。 *fqdn* は LDC 用です。
ステップ 6	hostname(config-ca-trustpoint)# **subject-name** *X.500_name* **Example:** hostname(config-ca-trustpoint)# subject-name cn=FW_LDC_SIGNER_172_23_45_200	登録時に、指定したサブジェクト DN を証明書に含めます。 *X.500_name* は LDC 用です。 属性と値のペアを区切るには、カンマを使用します。カンマやスペースを含む値は、引用符で囲みます。 たとえば、次のように入力します。 cn=crl,ou=certs,o="cisco systems, inc.",c=US 最大長は 500 文字です。

	コマンド	目的
ステップ 7	hostname(config-ca-trustpoint)# **keypair** *keypair* **Example:** hostname(config-ca-trustpoint)# keypair ldc_signer_key	公開キーが認証の対象となるキー ペアを指定します。 *keypair* は LDC 用です。
ステップ 8	hostname(config)# **crypto ca enroll** *ldc_server* **Example:** hostname(config)# crypto ca enroll ldc_server	CA で登録プロセスを開始します。
ステップ 9	hostname(config)# **tls-proxy** *proxy_name* **Example:** tls-proxy mytls	TLS プロキシ インスタンスを作成します。
ステップ 10	hostname(config-tlsp)# **server trust-point _internal_PP_***ctl-instance_filename* **Example:** hostname(config-tlsp)# server trust-point _internal_PP_myctl	サーバ トラストポイントを設定し、**_internal_PP_***ctl-instance_filename* という名前の内部トラストポイントを参照します。
ステップ 11	hostname(config-tlsp)# **client ldc issuer** *ca_tp_name* **Example:** client ldc issuer ldc_server	クライアントのダイナミック証明書を発行するローカル CA トラストポイントを指定します。
ステップ 12	hostname(config-tlsp)# **client ldc keypair** *key_label* **Example:** hostname(config-tlsp)# client ldc keypair phone_common	クライアントのダイナミック証明書で使用する RSA キー ペアを指定します。
ステップ 13	hostname(config-tlsp)# **client cipher-suite** *cipher-suite* **Example:** hostname(config-tlsp)# client cipher-suite aes128-sha1 aes256-sha1	暗号スイートを指定します。 オプションには、des-sha1、3des-sha1、aes128-sha1、aes256-sha1、および null-sha1 が含まれます。
ステップ 14		次のいずれかを実行して、ローカル CA 証明書をエクスポートし、信頼できる証明書として Cisco Unified Communications Manager サーバにインストールします。
•	hostname(config)# **crypto ca export** *trustpoint* **identity-certificate** **Example:** hostname(config)# crypto ca export ldc_server identity-certificate	ダイナミック証明書の署名者として proxy-ldc-issuer のトラストポイントを使用する場合に、証明書をエクスポートします。
•	hostname(config)# **show crypto ca server certificates**	埋め込みローカル CA サーバ LOCAL-CA-SERVER の場合に、証明書をエクスポートします。 証明書をエクスポートしたら、出力をファイルに保存し、Cisco Unified Communications Manager にインポートする必要があります。Cisco Unified Communications Manager ソフトウェアの Display Certificates 機能を使用すると、インストールされた証明書を確認できます。 これらの手順の実行については、次の URL を参照してください。 http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/cucos/5_0_4/iptpch6.html#wp1040848 http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/cucos/5_0_4/iptpch6.html#wp1040354

次の作業

TLS プロキシ インスタンスの作成と、Cisco Unified Communications Manager への証明書のインストールが完了したら、電話プロキシ 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.52-26）を参照してください。

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.52-7）の説明に従って要件を満たす必要があります。

	コマンド	目的
ステップ 1	hostname(config)# **media-termination** *instance_name* **Example:** hostname(config)# **media-termination** *mediaterm1*	電話プロキシに関連付ける、メディア ターミネーション インスタンスを作成します。
ステップ 2	hostname(config-media-termination)# **address** *ip_address* [**interface** *intf_name*] **Examples:** hostname(config-media-termination)# address 192.0.2.25 interface inside hostname(config-media-termination)# address 10.10.0.25 interface outside	メディア ターミネーション インスタンスで使用されるメディア ターミネーション アドレスを設定します。電話プロキシでは、SRTP と RTP にこのアドレスが使用されます。 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。 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 ターミネーション インスタンスの作成時およびメディア ターミネーション アドレスの設定時に満たす必要がある前提条件の完全なリストについては、「メディア ターミネーション インスタンスの前提条件」（P.52-7）を参照してください。
ステップ 3	（任意） hostname(config-media-termination)# **rtp-min-port** *port1* **rtp-max-port** *port2* **Example:** hostname(config-media-termination)# rtp-min-port 2001 rtp-maxport 32770	メディア ターミネーション インスタンスの RTP ポート範囲の最小値と最大値を指定します。 *port1* と *port2* には 1024 から 65535 までの値を指定できます。

次の作業

メディア ターミネーション インスタンスの作成が完了したら、電話プロキシ 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.52-26）を参照してください。

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。

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.52-20）および「ノンセキュア Cisco UCM クラスタ用の TLS プロキシ インスタンスの作成」（P.52-22）を参照してください。

	コマンド	目的
ステップ 1	hostname(config)# **phone-proxy** *phone_proxy_name* **Example:** hostname(config)# phone-proxy myphoneproxy	電話プロキシ インスタンスを作成します。 セキュリティ アプライアンス上に設定できる電話プロキシ インスタンスは 1 つだけです。
ステップ 2	hostname(config-phone-proxy)# **media-termination** *instance_name* **Examples:** hostname(config-phone-proxy)# media-termination my_mt	電話プロキシで SRTP と RTP に使用されるメディア ターミネーション インスタンスを指定します。 **（注）** メディア ターミネーション インスタンスは、電話プロキシ インスタンスに指定する前に作成しておく必要があります。 メディア ターミネーション インスタンスの作成手順については、「メディア ターミネーション インスタンスの作成」（P.52-25）を参照してください。
ステップ 3	hostname(config-phone-proxy)# **tftp-server address** *ip_address* **interface** *interface* **Example:** hostname(config-phone-proxy)# tftp-server address 192.0.2.101 interface inside	実際の内部アドレスを使用して TFTP サーバを作成し、TFTP サーバを置くインターフェイスを指定します。
ステップ 4	hostame(config-phone-proxy)# **tls-proxy** *proxy_name* **Example:** hostame(config-phone-proxy)# tls-proxy mytls	すでに作成した TLS プロキシ インスタンスを設定します。
ステップ 5	hostname(config-phone-proxy)# **ctl-file** *ctl_name* **Example:** hostame(config-phone-proxy)# ctl-file myctl	すでに作成した CTL ファイル インスタンスを設定します。

	コマンド	目的
ステップ 6	hostname(config-phone-proxy)# **proxy-server address** *ip_address* [*listen_port*] **interface** *ifc* **Example:** hostname(config-phone-proxy)# proxy-server 192.168.1.2 interface inside	（任意）IP 電話からのすべての HTTP 要求が送信される外部 HTTP プロキシが実行環境にある場合は、プロキシ サーバを設定します。 電話プロキシの使用中に設定できるプロキシ サーバは 1 つだけです。 デフォルトでは、エンタープライズ パラメータの下に設定された電話の URL パラメータは、URL 内で FQDN を使用しています。HTTP プロキシ用の DNS lookup で FQDN が解決されない場合は、IP アドレスを使用するようにこれらのパラメータを変更する必要があります。 **（注）** プロキシ サーバの設定後に IP 電話ですでにコンフィギュレーション ファイルがダウンロードされている場合は、IP 電話を再起動して、プロキシ サーバ アドレスの含まれたコンフィギュレーション ファイルを取得する必要があります。
ステップ 7	hostname(config-phone-proxy)# **cipc security-mode authenticated**	（任意）音声 VLAN およびデータ VLAN のシナリオで Cisco IP Communicator（CIPC）ソフトウェア電話を構成する場合に、強制的に認証モードで実行します。 CIPC で電話プロキシを使用するための要件については、「Cisco IP Communicator の前提条件」（P.52-11）を参照してください。
ステップ 8	hostname(config-phone-proxy)# **no disable service-settings**	（任意）設定する各 IP 電話に対して、Cisco UCM での設定内容を維持します。 デフォルトでは、次の設定内容が IP 電話ではディセーブルになります。 • PC Port • Gratuitous ARP • Voice VLAN Access • Web Access • Span to PC Port

次の作業

電話プロキシ インスタンスの作成が完了したら、電話プロキシ用の SIP および Skinny を設定します。「SIP インスペクションおよび Skinny インスペクションにおける電話プロキシのイネーブル化」（P.52-28）を参照してください。

SIP インスペクションおよび Skinny インスペクションにおける電話プロキシのイネーブル化

SIP および Skinny のプロトコル トラフィックを検査するように、作成した電話プロキシ インスタンスをイネーブルにします。

前提条件

電話プロキシ インスタンスの作成が完了している必要があります。「電話プロキシ インスタンスの作成」（P.52-26）を参照してください。

	コマンド	目的
ステップ 1	hostname(config)# **class-map** *class_map_name* **Example:** class-map sec_sccp	検査するセキュア Skinny クラスのトラフィックを設定します。Cisco Unified Communications Manager と Cisco IP Phone の間のトラフィックは SCCP を使用しており、SCCP インスペクションによって処理されます。 *class_map_name* には、Skinny クラス マップの名前を指定します。
ステップ 2	hostname(config-cmap)# **match port tcp eq 2443**	セキュア Skinny インスペクションのアクションを適用する TCP ポート 2443 に照合します。
ステップ 3	hostname(config-cmap)# **exit**	クラス マップ コンフィギュレーション モードを終了します。
ステップ 4	hostname(config)# **class-map** *class_map_name* **Example:** class-map sec_sip	検査するセキュア SIP クラスのトラフィックを設定します。 *class_map_name* には、SIP クラス マップの名前を指定します。
ステップ 5	hostname(config-cmap)# **match port tcp eq 5061**	セキュア SIP インスペクションのアクションを適用する TCP ポート 5061 に照合します。
ステップ 6	hostname(config-cmap)# **exit**	クラス マップ コンフィギュレーション モードを終了します。
ステップ 7	hostname(config)# **policy-map** *name* **Example:** policy-map pp_policy	ポリシー マップを設定し、アクションをトラフィック クラスに関連付けます。
ステップ 8	hostname(config-pmap)# **class** *classmap-name* **Example:** class sec_sccp	クラス マップ トラフィックにアクションを割り当てることができるように、クラス マップをポリシー マップに割り当てます。 *classmap_name* には、Skinny クラス マップの名前を指定します。
ステップ 9	hostname(config-pmap-c)# **inspect skinny phone-proxy** *pp_name* **Example:** inspect skinny phone-proxy mypp	SCCP（Skinny）アプリケーション インスペクションをイネーブルにし、指定したインスペクション セッションに対して電話プロキシをイネーブルにします。

	コマンド	目的
ステップ 10	hostnae(config-pmap)# **class** *classmap-name* **Example:** class sec_sip	クラス マップ トラフィックにアクションを割り当てることができるように、クラス マップをポリシー マップに割り当てます。 *classmap_name* には、SIP クラス マップの名前を指定します。
ステップ 11	hostname(config-pmap-c)# **inspect sip phone-proxy** *pp_name* **Example:** inspect sip phone-proxy mypp	SIP アプリケーション インスペクションをイネーブルにし、指定したインスペクション セッションに対して電話プロキシをイネーブルにします。
ステップ 12	hostname(config-pmap-c)# **exit**	ポリシー マップ コンフィギュレーション モードを終了します。
ステップ 13	hostname(config)# **service-policy** *policymap_name* **interface** *intf* **Example:** service-policy pp_policy interface outside	外部インターフェイスでサービス ポリシーをイネーブルにします。

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 52-3　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。

電話プロキシのトラブルシューティング

この項では、次のトピックについて取り上げます。

- 「セキュリティ アプライアンスによるデバッグ情報」（P.52-30）
- 「IP 電話によるデバッグ情報」（P.52-34）
- 「IP 電話の登録エラー」（P.52-35）
- 「メディア ターミネーション アドレスのエラー」（P.52-43）
- 「IP 電話の音声に関する問題」（P.52-44）
- 「SAST キーの保存」（P.52-45）

セキュリティ アプライアンスによるデバッグ情報

この項では、**debug**、**capture**、**show** の各コマンドを使用して電話プロキシのデバッグ情報を取得する方法について説明します。これらのコマンドの構文の詳細については、コマンド リファレンスを参照してください。

表 52-4 に、電話プロキシで使用する **debug** コマンドの一覧を示します。

表 52-4　電話プロキシで使用するセキュリティ アプライアンスの debug コマンド

目的	使用するコマンド	コメント
TLS プロキシインスペクションのエラー メッセージとイベント メッセージを表示する。	**debug inspect tls-proxy** [**events** | **errors**]	IP 電話で TFTP ファイルはすべて正常にダウンロードできたが、電話プロキシ用に設定された TLS プロキシで TLS ハンドシェイクを完了できない場合に、このコマンドを使用します。
SIP インスペクションおよび Skinny インスペクションのメディア セッションの、電話プロキシに関するエラー メッセージとイベント メッセージを表示する。	**debug phone-proxy media** [**events** | **errors**]	IP 電話でのコールや音声に問題がある場合に、**debug sip** コマンドや **debug skinny** コマンドと合わせて、このコマンドを使用します。

表 52-4　電話プロキシで使用するセキュリティ アプライアンスの debug コマンド（続き）

目的	使用するコマンド	コメント
SIP インスペクションおよび Skinny インスペクションのシグナリング セッションの、電話プロキシに関するエラー メッセージとイベント メッセージを表示する。	**debug phone-proxy signaling** [**events** | **errors**]	IP 電話を Cisco UCM に登録できない場合やコールに問題がある場合に、**debug sip** コマンドや **debug skinny** コマンドと合わせて、このコマンドを使用します。
CTL ファイルの作成およびコンフィギュレーション ファイルの解析を含めた、TFTP インスペクションのエラー メッセージとイベント メッセージを表示する。	**debug phone-proxy tftp** [**events** | **errors**]	
SIP アプリケーション インスペクションのデバッグ メッセージを表示する。	**debug sip**	ネットワーク内部には接続できるがネットワーク外部とは通話できないなど、IP 電話の接続に問題がある場合に、このコマンドを使用します。出力内の 4XX または 5XX のメッセージを確認してください。
SCCP（Skinny）アプリケーション インスペクションのデバッグ メッセージを表示する。	**debug skinny**	ネットワーク内部には接続できるがネットワーク外部とは通話できないなど、IP 電話の接続に問題がある場合に、このコマンドを使用します。出力内の 4XX または 5XX のメッセージを確認してください。

表 52-5 に、電話プロキシで使用する capture コマンドの一覧を示します。パケット スニフィングとネットワーク障害箇所特定のパケット取得機能をイネーブルにするには、適切なインターフェイス（IP 電話および Cisco UCM）に対して **capture** コマンドを使用します。

表 52-5　電話プロキシで使用するセキュリティ アプライアンスの capture コマンド

目的	使用するコマンド	コメント
ASA インターフェイス上のパケットをキャプチャする。	**capture** *capture_name* **interface** *interface_name*	問題があってパケットを調べる場合に、このコマンドを使用します。 たとえば、TFTP に問題があっても、**debug** コマンドの出力で詳細が判明しない場合は、IP 電話のあるインターフェイスと TFTP サーバのあるインターフェイスに対して **capture** コマンドを実行し、トランザクションと問題箇所を確認します。
内部インターフェイス上で電話プロキシに接続するノンセキュア IP 電話がある場合に、TLS プロキシからデータをキャプチャする。	**capture** *capture_name* **packet-length** *bytes* **interface inside buffer** *buf_size*	

表 52-5　電話プロキシで使用するセキュリティ アプライアンスの capture コマンド（続き）

目的	使用するコマンド	コメント
内部インターフェイス上で電話プロキシに接続するセキュア IP 電話がある場合に、TLS プロキシから暗号化されたデータをキャプチャする。	**capture** *capture_name* **type tls-proxy buffer** *buf_size* **packet-length** *bytes* **interface inside**	
1 つ以上のインターフェイスで、暗号化された着信データと発信データを TLS プロキシからキャプチャする。	**capture** *capture_name* **type tls-proxy buffer** *buf_size* **packet-length** *bytes* **interface** *interface_name*	シグナリングに失敗する場合は、復号化されたパケットをキャプチャして、SIP および SCCP のシグナリング メッセージの内容を確認することをお勧めします。**capture** コマンドに **type tls-proxy** オプションを使用してください。

表 52-6 に、電話プロキシで使用する **show** コマンドの一覧を示します。

表 52-6　電話プロキシで使用するセキュリティ アプライアンスの show コマンド

目的	使用するコマンド	コメント
高速セキュリティ パスによってドロップされたパケットまたは接続を表示する。	**show asp drop**	IP 電話の音質に関する問題や、電話プロキシのトラフィックに関するその他の問題をトラブルシューティングする場合に、このコマンドを使用します。このコマンドの実行に加えて、電話機からコール状態を取得し、ドロップされたパケットやジッタがないかどうかを確認してください。「IP 電話によるデバッグ情報」（P.52-34）を参照してください。
特定の分類子ドメインについて、高速セキュリティ パスの分類子の内容を表示する。	**show asp table classify domain** *domain_name*	IP 電話で TFTP ファイルがダウンロードされない場合は、このコマンドを使用して、ドメイン `inspect-phone-proxy` の分類ルールで、電話プロキシ インスタンス下の設定された TFTP サーバにホストが分類されるように設定されていることを確認します。 IP 電話で登録に失敗する場合は、このコマンドを使用して、登録できない IP 電話にドメイン `app-redirect` の分類ルールが設定されていることを確認します。

表 52-6　電話プロキシで使用するセキュリティ アプライアンスの show コマンド（続き）

目的	使用するコマンド	コメント
ASA に対する接続、ASA からの接続、および通過トラフィック接続を表示する。	**show conn all**	音声に問題がある場合は、このコマンドを使用して、IP 電話からメディア ターミネーション アドレスまでの接続が開かれていることを確認します。 **（注）** （使用されていない）接続を複製した TFTP 接続を表示するには、**show conn** コマンドに次のオプションを使用します。 `hostname# show conn	include p` TFTP 接続に関する出力の末尾には「p」フラグが付きます。 `UDP out 64.169.58.181:9014 in 192.168.200.101:39420 idle 0:01:51 bytes 522 flags p` このコマンドを使用すると、TFTP 接続を検査する inspect-phone-proxy を通過する接続が電話プロキシにあることがわかります。このコマンドを使用すると、p フラグがあるため、TFTP 要求が検査されていることが確認されます。
バッファ内のログとロギング設定を表示する。	**show logging**	**show logging** コマンドを入力する前に **logging buffered** コマンドをイネーブルにして、**show logging** コマンドで現在のメッセージ バッファと現在の設定内容が表示されるようにします。 電話プロキシと IP 電話で TLS ハンドシェイクが正常に実行されるかどうかを調べる場合に、このコマンドを使用します。 **（注）** **show logging** コマンドを使用すると、パケット拒否や変換エラーの発生などの多くの問題のトラブルシューティングに役立ちます。
電話プロキシによって保存されている、対応するメッセージ セッションを表示する。	**show phone-proxy media-sessions**	正常なコールからの出力を表示するには、このコマンドを使用します。さらに、片通話など、IP 電話の音声に関する問題をトラブルシューティングする場合にも、このコマンドを使用します。

表 52-6　電話プロキシで使用するセキュリティ アプライアンスの show コマンド （続き）

目的	使用するコマンド	コメント
データベースに保存されている、セキュア モード機能を持つ IP 電話を表示する。	**show phone-proxy secure-phones**	どのような問題の場合でも、この出力内に IP 電話のエントリがあることと、この IP 電話用のポートがゼロ以外であることを確認します。それによって、Cisco UCM に正常に登録されていることがわかります。
電話プロキシによって保存されている、対応するシグナリング セッションを表示する。	**show phone-proxy signaling-sessions**	メディアまたはシグナリングのエラーをトラブルシューティングする場合に、このコマンドを使用します。
設定されたサービス ポリシーを表示する。	**show service-policy**	サービス ポリシーの統計情報を表示する場合に、このコマンドを使用します。
電話プロキシ関連の、アクティブな TLS プロキシ セッションを表示する。	**show tls-proxy sessions**	IP 電話の登録に失敗した場合は、このコマンドを使用して、電話プロキシ用に設定された TLS プロキシと IP 電話のハンドシェイクが正常に実行されているかどうかを確認します。

IP 電話によるデバッグ情報

IP 電話で次のアクションを実行します。

- [Settings] ボタン > [Status] > [Status Messages] の順に選択し、表示する状態項目を選択して、IP 電話の状態メッセージを確認します。
- [Settings] ボタン > [Status] > [Call Statistic] の順に選択して、IP 電話からコール統計情報データを取得します。次のようなデータが表示されます。

```
RxType: G.729              TxType: G.729
RxSize:   20 ms            TxSize:  20 ms
RxCnt: 0                   TxCnt: 014174
AvgJtr:   10               MaxJtr:  59
RxDisc: 0000               RxLost: 014001
```

- [Settings] ボタン > [Security Configuration] の順に選択して、IP 電話のセキュリティ設定を確認します。Web アクセス、セキュリティ モード、MIC、LSC、CTL ファイル、信頼リスト、および CAPF の設定が表示されます。セキュリティ モードの項目で、IP 電話が暗号化モードに設定されていることを確認します。
- [Settings] ボタン > [Security Configuration] > [Trust List] の順に選択して、IP 電話にインストールされている証明書を確認します。信頼リストで次の点を確認します。
  - IP 電話から到達する必要があるエンティティごとにエントリがあることを確認します。プライマリ Cisco UCM とバックアップ Cisco UCM がある場合は、それぞれの Cisco UCM に対するエントリが信頼リストに含まれている必要があります。
  - IP 電話に LSC が必要な場合は、レコード エントリに CAPF エントリが含まれている必要があります。
  - 各エントリに表示される IP アドレスが、IP 電話から到達できるエンティティのマッピング IP アドレスであることを確認します。

- Web ブラウザを開いて、URL `http://IP_phone_IP address` にある IP 電話のコンソール ログにアクセスします。ページにデバイス情報が表示されます。左ペインにある [Device Logs] セクションの [Console Logs] をクリックします。

IP 電話の登録エラー

IP 電話を電話プロキシに登録できない場合は、次のエラーが考えられます。

IP 電話のコンソールに TFTP Auth Error と表示される

問題　IP 電話に次の状態メッセージが表示されます。

```
TFTP Auth Error
```

ソリューション　この状態メッセージが表示される場合は、IP 電話の CTL ファイルに問題がある可能性があります。

IP 電話の CTL ファイルの問題を修正するには、次の手順を実行します。

ステップ 1　IP 電話で、[Setting] ボタン > [Security Configuration] > [Trust List] の順に選択します。ネットワーク内のエンティティ（プライマリ Cisco UCM、セカンダリ Cisco UCM、TFTP サーバ）ごとに個別のエントリが信頼リストにあることと、各エンティティの IP アドレスに IP 電話から到達可能であることを確認します。

ステップ 2　ASA で、電話プロキシ用の CTL ファイルに、ネットワーク内のエンティティ（プライマリ Cisco UCM、セカンダリ Cisco UCM、TFTP サーバ）ごとに 1 つずつのレコード エントリが含まれていることを確認します。

```
hostname# show running-config all ctl-file [ctl_name]
```

これらのレコード エントリから、それぞれ 1 つのエントリが IP 電話の信頼リストに作成されます。電話プロキシによって、CUCM と TFTP の機能を持つ 1 つのエントリが内部的に作成されます。

ステップ 3　CTL ファイルの各 IP アドレスが、エンティティのグローバル IP アドレスまたはマッピング IP アドレスであることを確認します。IP 電話が複数のインターフェイス上にある場合は、追加のアドレッシング要件が適用されます。「複数インターフェイス上にある IP 電話の前提条件」（P.52-10）を参照してください。

コンフィギュレーション ファイルの解析エラー

問題　ASA で Cisco UCM から受信したコンフィギュレーション ファイルの解析を試みると、デバッグ出力（**debug phone-proxy tftp errors**）に次のエラーが表示されます。

```
PP: 192.168.10.5/49357 requesting SEP00010002003.cnf.xml.sgn
PP: opened 0x193166
.......
PP: Beginning of element tag is missing, got !
PP: error parsing config file
PP: Error modifying config file, dropping packet
```

ソリューション　この問題をトラブルシューティングするには、次の手順を実行します。

ステップ 1　Web ブラウザに次の URL を入力して、Cisco Unified CM Administration Console から IP 電話のコンフィギュレーション ファイルを取得します。

```
http://<cucm_ip>:6970/<config_file_name>
```

たとえば、Cisco UCM の IP アドレスが 128.106.254.2 で、IP 電話のコンフィギュレーション ファイルの名前が SEP000100020003.cnf.xml である場合、次のように入力します。

```
http://128.106.254.2:6970/SEP000100020003.cnf.xml
```

ステップ 2　このファイルを保存し、TAC にケースを開いて、このファイルと、ASA で **debug phone-proxy tftp** コマンドを実行した出力結果を送信します。

コンフィギュレーション ファイルの解析エラー：DNS 応答を受信できない

問題　ASA で Cisco UCM から受信したコンフィギュレーション ファイルの解析を試みると、デバッグ出力（**debug phone-proxy tftp errors**）に次のエラーが表示されます。

```
PP: 192.168.10.5/49357 requesting SEP00010002003.cnf.xml.sgn
PP: opened 0x193166
.......
PP: Callback required for parsing config file
PP: Unable to get dns response for id 7
PP: Callback, error modifying config file
```

このエラーは、Cisco UCM が FQDN として設定されており、電話プロキシが DNS lookup を試みているが応答を得られないことを示しています。

ソリューション

ステップ 1　ASA に DNS lookup が設定されていることを確認します。

ステップ 2　DNS lookup が設定されている場合は、ASA から Cisco UCM の FQDN を ping できるかどうかを調べます。

ステップ 3　ASA で Cisco UCM の FQDN を ping できない場合は、DNS サーバに問題がないかどうか確認します。

ステップ 4　さらに、**name** コマンドを使用して、名前と IP アドレスを FQDN に関連付けます。**name** 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。

コンフィギュレーション ファイル以外のファイルの解析エラー

問題　ASA で Cisco UCM から IP 電話のコンフィギュレーション ファイル以外のファイルを受信し、解析を試みます。デバッグ出力（**debug phone-proxy tftp**）に次のエラーが表示されます。

```
PP: 192.168.10.5/49357 requesting SK72f64050-7ad5-4b47-9bfa-5e9ad9cd4aa9.xml.sgn
PP: opened 0x193166
.......
PP: Beginning of element tag is missing, got !
PP: error parsing config file
PP: Error modifying config file, dropping packet
```

ソリューション　電話プロキシで解析されるのは、IP 電話のコンフィギュレーション ファイルだけです。電話プロキシの TFTP の状態が out of state の場合は、電話プロキシで IP 電話のコンフィギュレーション ファイル以外のファイルの解析を試みても検出できず、ASA の **debug phone-proxy tftp** コマンド出力に上記のエラーが表示されます。

この問題をトラブルシューティングするには、次の手順を実行します。

ステップ 1　IP 電話をリブートします。

ステップ 2　ASA で次のコマンドを入力して、最初の TFTP 要求から最初のエラー発生時点までのエラー情報を取得します。

```
hostname# debug phone-proxy tftp
```

ステップ 3　IP 電話から ASA へのパケットをキャプチャします。IP 電話に接するインターフェイス上と、Cisco UCM に接するインターフェイス上で、パケットをキャプチャしてください。「セキュリティ アプライアンスによるデバッグ情報」（P.52-30）を参照してください。

ステップ 4　このトラブルシューティング データを保存し、TAC にケースを開いて、この情報を送信します。

コンフィギュレーション ファイルを求める TFTP 要求に Cisco UCM が応答しない

問題　ASA で IP 電話のコンフィギュレーション ファイルを求める TFTP 要求を Cisco UCM に転送した際に、Cisco UCM から応答がなく、デバッグ出力（**debug phone-proxy tftp**）に次のエラーが表示されます。

```
PP: 192.168.10.5/49355 requesting SEP001562106AF3.cnf.xml.sgn
PP: opened 0x17ccde
PP: 192.168.10.5/49355 requesting SEP001562106AF3.cnf.xml.sgn
PP: Client outside:192.168.10.5/49355 retransmitting request for Config file
SEP001562106AF3.cnf.xml.sgn
PP: opened 0x17ccde
PP: 192.168.10.5/49355 requesting SEP001562106AF3.cnf.xml.sgn
PP: Client outside:192.168.10.5/49355 retransmitting request for Config file
SEP001562106AF3.cnf.xml.sgn
PP: opened 0x17ccde
PP: 192.168.10.5/49355 requesting SEP001562106AF3.cnf.xml.sgn
PP: Client outside:192.168.10.5/49355 retransmitting request for Config file
SEP001562106AF3.cnf.xml.sgn
PP: opened 0x17ccde
```

ソリューション　この問題をトラブルシューティングするには、次の手順を実行します。

ステップ 1　次のトラブルシューティング アクションを実行して、Cisco UCM が TFTP 要求に応答しない原因を調べます。

- ASA の外部インターフェイスに PAT が設定されているときに、Cisco UCM を使用して内部インターフェイスを ping し、IP 電話の IP アドレスが ASA の内部インターフェイスの IP アドレスに NAT を使用するようにします。
- NAT と PAT が設定されていないときに、Cisco UCM を使用して IP 電話の IP アドレスを ping します。

ステップ 2　ASA で TFTP 要求が転送されていることを確認します。ASA と Cisco UCM の間のインターフェイス上でパケットをキャプチャします。「セキュリティ アプライアンスによるデバッグ情報」（P.52-30）を参照してください。

セキュリティ アプライアンスによる TFTP データの送信後に IP 電話が応答しない

問題　IP 電話からの CTL ファイルを求める TFTP 要求を ASA で受信し、データを IP 電話に転送したとき、電話がデータを認識しない場合があり、TFTP トランザクションが失敗します。

デバッグ出力（**debug phone-proxy tftp**）に次のエラーが表示されます。

```
PP: Client outside:68.207.118.9/33606 retransmitting request for CTL file
CTLSEP001DA2B78E91.tlv
PP: opened 0x214b27a
PP: Data Block 1 forwarded from 168.215.146.220/20168 to 68.207.118.9/33606 ingress ifc
outside
PP: 68.207.118.9/33606 requesting CTLSEP001DA2B78E91.tlv
PP: Client outside:68.207.118.9/33606 retransmitting request for CTL file
CTLSEP001DA2B78E91.tlv
PP: 68.207.118.9/33606 requesting CTLSEP001DA2B78E91.tlv
PP: Client outside:68.207.118.9/33606 retransmitting request for CTL file
CTLSEP001DA2B78E91.tlv
```

ソリューション　IP 電話が応答しない原因を調べ、問題をトラブルシューティングするには、次の手順を実行します。

ステップ 1　次のコマンドを入力し、ASA と IP 電話の間のインターフェイス上でパケットをキャプチャすることによって、ASA で TFTP 要求が転送されていることを確認します。

```
hostname# capture out interface outside
```

capture コマンドの使用方法の詳細については、コマンド リファレンスを参照してください。

ステップ 2　IP 電話がルータの背後にある場合は、ルータでデータがドロップされている可能性があります。ルータで UDP ポート転送がイネーブルになっていることを確認します。

ステップ 3　ルータが Linksys ルータの場合は、設定要件について 「電話プロキシの UDP ポート転送用 Linksys ルータの設定」（P.52-29）を参照してください。

IP 電話が無署名ファイルを要求するエラー

問題　IP 電話では、常に、署名されたファイルを要求する必要があります。したがって、要求される TFTP ファイルの拡張子は常に .SGN です。

IP 電話が署名されたファイルを要求しない場合は、デバッグ出力（**debug phone-proxy tftp errors**）に次のエラーが表示されます。

```
Error: phone requesting for unsigned config file
```

ソリューション　ほとんどの場合、このエラーは、IP 電話が ASA から CTL ファイルを正常にインストールしていないために発生します。

IP 電話の状態メッセージを確認して、IP 電話が ASA から CTL ファイルを正常にダウンロードおよびインストールしたかどうかを調べます。詳細については、「IP 電話によるデバッグ情報」（P.52-34）を参照してください。

IP 電話で CTL ファイルをダウンロードできない

問題　IP 電話の状態メッセージに、CTL ファイルをダウンロードできないと表示され、IP 電話をセキュア（暗号化）モードに変換できません。

ソリューション　IP 電話に既存の CTL ファイルがない場合は、[Settings] ボタン > [Status] > [Status Messages] の順に選択して、状態メッセージを確認します。IP 電話に CTL File Auth エラーが発生したことを示す状態メッセージがリストに含まれている場合は、IP 電話のコンソール ログを取得し、TAC にケースを開いてログを送信します。

ソリューション　IP 電話に既存の CTL ファイルがある場合に、IP 電話の状態メッセージにこのエラーが表示される可能性があります。

ステップ 1　IP 電話にすでに CTL ファイルがあるかどうかを確認します。以前に混合モードの Cisco UCM クラスタに登録した IP 電話には、ファイルが存在する可能性があります。IP 電話で、[Settings] ボタン > [Security Configuration] > [CTL file] の順に選択します。

ステップ 2　[Settings] ボタン > [Security Configuration] > [CTL file] > [Select] の順に選択して、既存の CTL ファイルを削除します。キーパッドで **# と入力し、[Erase] を選択します。

ソリューション　メディアの停止に関する問題が原因で、CTL ファイルをダウンロードできない場合があります。次のコマンドを入力して、電話プロキシにメディア ターミネーション アドレスが正しく設定されているかどうかを調べます。

```
hostname(config)# show running-config all phone-proxy
!
phone-proxy mypp
    media-termination address 10.10.0.25
    cipc security-mode authenticated
    cluster-mode mixed
    disable service-settings
    timeout secure-phones 0:05:00
hostname(config)#
```

それぞれのメディア ターミネーション インスタンスが正しく作成されていることと、アドレスが正しく設定されていることを確認します。ASA は、メディアの停止に関する特定基準を満たしている必要があります。メディア ターミネーション インスタンスの作成時およびメディア ターミネーション アドレスの設定時に満たす必要がある前提条件の完全なリストについては、「メディア ターミネーション インスタンスの前提条件」（P.52-7）を参照してください。

シグナリング接続からの IP 電話の登録エラー

問題　IP 電話で、電話プロキシとの TLS ハンドシェイクと、TFTP を使用したファイルのダウンロードを実行できません。

ソリューション

ステップ 1　次の手順を実行して、電話プロキシと IP 電話の間で TLS ハンドシェイクが行われているかどうかを調べます。

a. 次のコマンドを実行して、ロギングをイネーブルにします。

```
hostname(config)# logging buffered debugging
```

b. 次のコマンドを入力して、**logging buffered** コマンドで取得した syslog の出力を確認します。

```
hostname# show logging
```

syslog に含まれている情報で、IP 電話で TLS ハンドシェイクを試みた時間がわかります。この時間は、IP 電話でコンフィギュレーション ファイルのダウンロードが実行された後です。

ステップ 2　TLS プロキシが電話プロキシ用に正しく設定されているかどうかを調べます。

a. 次のコマンドを入力して、現在実行されている TLS プロキシ設定をすべて表示します。

```
hostname# show running-config tls-proxy
    tls-proxy proxy
    server trust-point _internal_PP_<ctl_file_instance_name>
    client ldc issuer ldc_signer
    client ldc key-pair phone_common
    no client cipher-suite
hostname#
```

b. 出力の **tls-proxy** コマンド（ステップ a. を参照）の下に **server trust-point** コマンドが含まれていることを確認します。

server trust-point コマンドが含まれていない場合は、電話プロキシ設定の TLS プロキシを修正します。

「ノンセキュア Cisco UCM クラスタにおける電話プロキシ設定のタスク フロー」（P.52-16）のステップ 3 または 「混合モードの Cisco UCM クラスタにおける電話プロキシ設定のタスク フロー」（P.52-18）のステップ 3 を参照してください。

電話プロキシ用の TLS プロキシ設定にこのコマンドがないと、TLS ハンドシェイクに失敗します。

ステップ 3　TLS ハンドシェイクが成功するために必要な証明書がすべて ASA にインポートされていることを確認します。

a. 次のコマンドを入力して、ASA にインストールされている証明書を調べます。

```
hostname# show running-config crypto
```

さらに、IP 電話にインストールされている証明書も調べます。IP 電話に MIC がインストールされているかどうかの確認方法については、「IP 電話によるデバッグ情報」（P.52-34）を参照してください。

b. インストール済み証明書のリストに、電話プロキシに必要な証明書がすべて含まれているかどうかを確認します。

詳細については、表 52-2、「セキュリティ アプライアンスで電話プロキシに必要な証明書」を参照してください。

c. 不足している証明書を ASA にインポートします。「「Cisco UCM からの証明書のインポート」（P.52-17）」も参照してください。

ステップ 4　上記の手順で問題が解決しない場合は、次の手順を実行して、シスコ サポートのために追加のトラブルシューティング情報を取得します。

a. 次のコマンドを入力して、電話プロキシのデバッグ情報をさらに取得します。

```
hostname# debug inspect tls-proxy error
hostname# show running-config ssl
hostname(config) show tls-proxy tls_name session host host_addr detail
```

b. パケット スニッフィングとネットワーク障害箇所特定のパケット取得機能をイネーブルにするには、内部インターフェイスおよび外部インターフェイス（IP 電話および Cisco UCM）に対して **capture** コマンドをイネーブルにします。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。

問題　TLS ハンドシェイクは成功するが、シグナリング接続に失敗します。

ソリューション　次のアクションを実行します。

- 次のコマンドを使用して、SIP および Skinny のシグナリングが成功しているかどうかを確認します。
  - **debug sip**
  - **debug skinny**
- TLS ハンドシェイクに失敗して次の syslog を受信する場合は、SSL 暗号化方式の設定が正しくない可能性があります。

```
%ASA-6-725001: Starting SSL handshake with client dmz:171.169.0.2/53097 for TLSv1
session.
%ASA-7-725010: Device supports the following 1 cipher(s).
%ASA-7-725011: Cipher[1] : RC4-SHA
%ASA-7-725008: SSL client dmz:171.169.0.2/53097 proposes the following 2 cipher(s).
%ASA-7-725011: Cipher[1] : AES256-SHA
%ASA-7-725011: Cipher[2] : AES128-SHA
%ASA-7-725014: SSL lib error.Function: SSL3_GET_CLIENT_HELLO Reason: no shared cipher
%ASA-6-725006: Device failed SSL handshake with dmz client:171.169.0.2/53097
```

次の手順を実行して、正しいサイファを設定します。

ステップ 1　電話プロキシで使用されているサイファを確認するには、次のコマンドを入力します。

```
hostname# show run all ssl
```

ステップ 2　必要なサイファを追加するには、次のコマンドを入力します。

```
hostname(config)# ssl encryption
```

デフォルトでは、すべてのアルゴリズムを次の順序で使用できます。

[3des-sha1] [des-sha1] [rc4-md5] [possibly others]

ssl encryption コマンドによるサイファ設定の詳細については、コマンド リファレンスを参照してください。

SSL ハンドシェイク エラー

問題　電話プロキシが機能しません。初期トラブルシューティングで、ASA の syslog に次のエラーが見つかりました。

```
%ASA-7-725014: SSL lib error.Function: SSL3_READ_BYTES Reason: ssl handshake failure
%ASA-7-725014: SSL lib error.Function: SSL3_GET_CLIENT_CERTIFICATE Reason: no certificate
returned
%ASA-6-725006: Device failed SSL handshake with outside client:72.146.123.158/30519
%ASA-3-717009: Certificate validation failed.No suitable trustpoints found to validate
certificate serial number: 62D06172000000143FCC, subject name:
cn=CP-7962G-SEP002155554502,ou=EVVBU,o=Cisco Systems Inc.
%ASA-3-717027: Certificate chain failed validation.No suitable trustpoint was found to
validate chain.
```

ソリューション

TLS ハンドシェイクが成功するために必要な証明書がすべて ASA にインポートされていることを確認します。

ステップ 1　次のコマンドを入力して、ASA にインストールされている証明書を調べます。

```
hostname# show running-config crypto
```

さらに、IP 電話にインストールされている証明書も調べます。IP 電話に MIC がインストールされているかどうかの確認方法については、「IP 電話によるデバッグ情報」（P.52-34）を参照してください。

ステップ 2　インストール済み証明書のリストに、電話プロキシに必要な証明書がすべて含まれているかどうかを確認します。

詳細については、表 52-2、「セキュリティ アプライアンスで電話プロキシに必要な証明書」を参照してください。

ステップ 3　不足している証明書を ASA にインポートします。「「Cisco UCM からの証明書のインポート」（P.52-17）」も参照してください。

問題　電話プロキシが機能しません。初期トラブルシューティングで、ASA の syslog に次のエラーが見つかりました。

```
%ASA-6-725001: Starting SSL handshake with client dmz:171.169.0.2/53097 for TLSv1
session.
%ASA-7-725010: Device supports the following 1 cipher(s).
%ASA-7-725011: Cipher[1] : RC4-SHA
%ASA-7-725008: SSL client dmz:171.169.0.2/53097 proposes the following 2 cipher(s).
%ASA-7-725011: Cipher[1] : AES256-SHA
%ASA-7-725011: Cipher[2] : AES128-SHA
%ASA-7-725014: SSL lib error.Function: SSL3_GET_CLIENT_HELLO Reason: no shared cipher
%ASA-6-725006: Device failed SSL handshake with dmz client:171.169.0.2/53097
```

ソリューション　SSL 暗号化方式の設定が正しくない可能性があります。次の手順を実行して、正しいサイファを設定します。

ステップ 1　電話プロキシで使用されているサイファを確認するには、次のコマンドを入力します。

```
hostname# show run all ssl
```

ステップ 2　必要なサイファを追加するには、次のコマンドを入力します。

```
hostname(config)# ssl encryption
```

デフォルトでは、すべてのアルゴリズムを次の順序で使用できます。

[3des-sha1] [des-sha1] [rc4-md5] [possibly others]

ssl encryption コマンドによるサイファ設定の詳細については、コマンド リファレンスを参照してください。

証明書の検証エラー

問題　ASA のログに、証明書の検証エラーが発生したと表示されます。

show logging asdm コマンドを入力すると、次のエラーが表示されました。

```
3|Jun 19 2008 17:23:54|717009: Certificate validation failed.No suitable trustpoints found
to validate
certificate serial number: 348FD2760000000E6E27, subject name:
cn=CP-7961G-SEP001819A89CC3,ou=EVVBU,o=Cisco Systems Inc.
```

ソリューション

IP 電話から提供される MIC を電話プロキシで認証するには、Cisco Manufacturing CA（MIC）証明書が ASA にインポートされている必要があります。

TLS ハンドシェイクが成功するために必要な証明書がすべて ASA にインポートされていることを確認します。

ステップ 1　次のコマンドを入力して、ASA にインストールされている証明書を調べます。

```
hostname# show running-config crypto
```

さらに、IP 電話にインストールされている証明書も調べます。証明書情報は、[Security Configuration] メニューの下に表示されます。IP 電話に MIC がインストールされているかどうかの確認方法については、「IP 電話によるデバッグ情報」（P.52-34）を参照してください。

ステップ 2　インストール済み証明書のリストに、電話プロキシに必要な証明書がすべて含まれているかどうかを確認します。

詳細については、表 52-2、「セキュリティ アプライアンスで電話プロキシに必要な証明書」を参照してください。

ステップ 3　不足している証明書を ASA にインポートします。「「Cisco UCM からの証明書のインポート」（P.52-17）」も参照してください。

メディア ターミネーション アドレスのエラー

問題　**media-termination address** コマンドを入力すると、次のエラーが表示されます。

```
hostname(config-phone-proxy)# media-termination address ip_address
ERROR: Failed to apply IP address to interface Virtual254, as the network overlaps with
interface GigabitEthernet0/0.Two interfaces cannot be in the same subnet.
ERROR: Failed to set IP address for the Virtual interface
ERROR: Could not bring up Phone proxy media termination interface
ERROR: Failed to find the HWIDB for the Virtual interface
```

ソリューション　次のコマンドを入力して、電話プロキシにメディア ターミネーション アドレスが正しく設定されているかどうかを調べます。

```
hostname(config)# show running-config all phone-proxy
asa2(config)# show running-config all phone-proxy
!
phone-proxy mypp
    media-termination address 10.10.0.25
    cipc security-mode authenticated
    cluster-mode mixed
    disable service-settings
    timeout secure-phones 0:05:00
hostname(config)#
```

それぞれのメディア ターミネーション インスタンスが正しく作成されていることと、アドレスが正しく設定されていることを確認します。ASA は、メディアの停止に関する特定基準を満たしている必要があります。メディア ターミネーション インスタンスの作成時およびメディア ターミネーション アドレスの設定時に満たす必要がある前提条件の完全なリストについては、「メディア ターミネーション インスタンスの前提条件」（P.52-7）を参照してください。

IP 電話の音声に関する問題

電話プロキシ経由の IP 電話接続時には、次の音声エラーが発生する可能性があります。

音声通話のメディア エラー

問題　コール シグナリングが完了しても、片通話になるか、まったく音声が聞こえません。

ソリューション

- メディアの停止に関する問題が原因で、片通話になったり音声が聞こえなかったりする場合があります。次のコマンドを入力して、電話プロキシにメディア ターミネーション アドレスが正しく設定されているかどうかを調べます。

  ```
  hostname(config)# show running-config all phone-proxy
  asa2(config)# show running-config all phone-proxy
  !
  phone-proxy mypp
      media-termination address 10.10.0.25
      cipc security-mode authenticated
      cluster-mode mixed
      disable service-settings
      timeout secure-phones 0:05:00
  hostname(config)#
  ```

- それぞれのメディア ターミネーション インスタンスが正しく作成されていることと、アドレスが正しく設定されていることを確認します。ASA は、メディアの停止に関する特定基準を満たしている必要があります。メディア ターミネーション インスタンスの作成時およびメディア ターミネーション アドレスの設定時に満たす必要がある前提条件の完全なリストについては、「メディア ターミネーション インスタンスの前提条件」（P.52-7）を参照してください。
- メディア ターミネーション アドレスが要件を満たしている場合は、それらの IP アドレスにすべての IP 電話から到達可能かどうかを調べます。
- 各 IP アドレスが正しく設定されていて、すべての IP 電話から到達可能である場合は、IP 電話のコール統計情報を確認して（「IP 電話によるデバッグ情報」（P.52-34）を参照）、IP 電話に Rcvr パケットと Sender パケットがあるかどうか、また、Rcvr Lost パケットまたは Discarded パケットがあるかどうかを調べます。

SAST キーの保存

ハードウェア障害のために回復が必要な場合や、交換が必要な場合に備えて、ASA の Site Administrator Security Token（SAST）キーを保存できます。次の手順では、SAST キーを回復して新しいハードウェアに使用する方法を示します。

SAST キーは、**show crypto key mypubkey rsa** コマンドで表示できます。SAST キーは、**_internal_***ctl-file_name*_**SAST_***X* というトラストポイントに関連付けられています。*ctl-file-name* は、設定された CTL ファイル インスタンスの名前です。*X* は 0 から N-1 までの整数で、N は CTL ファイルに対して設定された SAST の数（デフォルトは 2）です。

ステップ 1　ASA で **crypto ca export** コマンドを使用して、すべての SAST キーを PKCS-12 形式でエクスポートします。

```
hostname(config)# crypto ca export _internal_ctl-file_name_SAST_X pkcs12 passphrase

hostname(config)# Exported pkcs12 follows:
MIIGZwIBAzCCBiEGCSqGSIb3DQEHAaCCBhIEggYOMIIGCjCCBgYGCSqGSIb3DQEH

[snip]

MIIGZwIBAzCCBiEGCSqGSIb3DQEHAaCCBhIEggYOMIIGCjCCBgYGCSqGSIb3DQEH
---End - This line not part of the pkcs12---

hostname(config)# crypto ca export _internal_ctl-file_name_SAST_X pkcs12 passphrase

hostname(config)# Exported pkcs12 follows:
MIIGZwIBAzCCBiEGCSqGSIb3DQEHAaCCBhIEggYOMIIGCjCCBgYGCSqGSIb3DQEH

[snip]

mGF/hfDDNAICBAA=

---End - This line not part of the pkcs12---
hostname(config)#
```

（注）　この出力を安全な場所に保存します。

ステップ 2　新しい ASA に SAST キーをインポートします。

a.　SAST キーをインポートするには、次のコマンドを入力します。

```
hostname(config)# crypto ca import trustpoint pkcs12 passphrase
```

trustpoint は **_internal_***ctl-file_name*_**SAST_***X* です。*ctl-file-name* は設定された CTL ファイル インスタンスの名前で、*X* は 0 ～ 4 の整数です。この整数は、ASA からのエクスポート結果によって異なります。

b.　次のコマンドを入力し、プロンプトが表示されたら、ステップ 1 で保存した PKCS-12 出力を貼り付けます。

```
hostname(config)# crypto ca import _internal_ctl-file_name_SAST_X pkcs12 passphrase

hostname(config)# Enter the base 64 encoded pkcs12.
hostname(config)# End with the word "quit" on a line by itself:
MIIGZwIBAzCCBiEGCSqGSIb3DQEHAaCCBhIEggYOMIIGCjCCBgYGCSqGSIb3DQEH

[snip]

muMiZ6eClQICBAA=
```

```
hostname(config)# quit
INFO: Import PKCS12 operation completed successfully
hostname(config)# crypto ca import _internal_ctl-file_name_SAST_X pkcs12 passphrase

hostname(config)# Enter the base 64 encoded pkcs12.
hostname(config)# End with the word "quit" on a line by itself:
MIIGZwIBAzCCBiEGCSqGSIb3DQEHAaCCBhIEggYOMIIGCjCCBgYGCSqGSIb3DQEH

[snip]

mGF/hfDDNAICBAA=
hostname(config)# quit
INFO: Import PKCS12 operation completed successfully
hostname(config)#
```

ステップ 3　次のコマンドを入力して、新しい ASA に CTL ファイル インスタンスを作成します。このとき、ステップ 2 で作成した SAST トラストポイントで使用した名前を使用します。各 Cisco UMC（プライマリおよびセカンダリ）にトラストポイントを作成します。

```
hostname(config)# ctl-file ctl_name
hostname(config-ctl-file)# record-entry cucm trustpoint trust_point address address
hostname(config-ctl-file)# record-entry capf trustpoint trust_point address address
hostname(config-ctl-file)# no shutdown
```

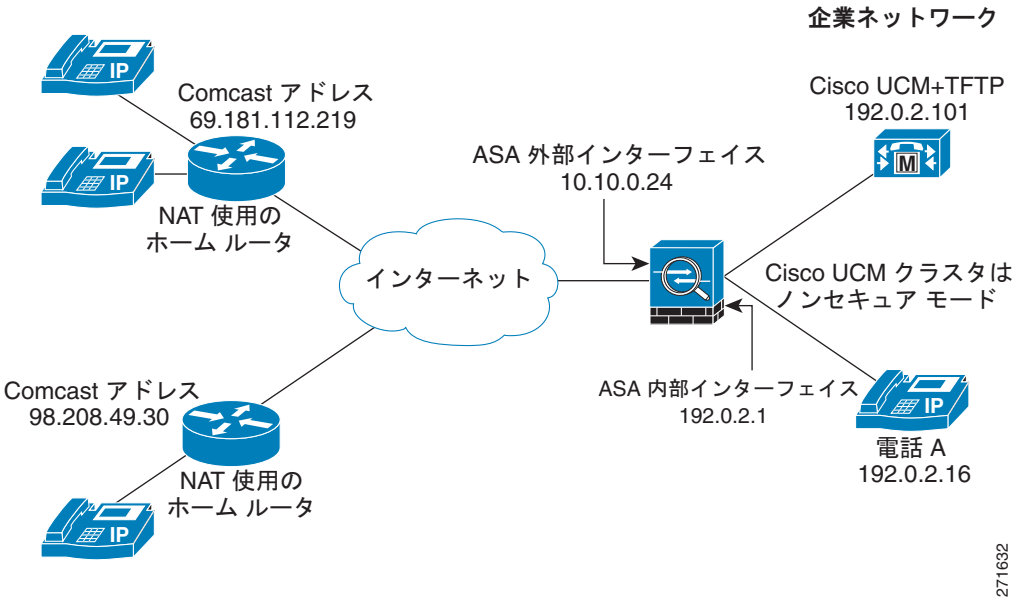
電話プロキシの設定例

この項では、次のトピックについて取り上げます。

例 1：ノンセキュア Cisco UCM クラスタ、パブリッシャ上の Cisco UCM および TFTP サーバ

図 52-2 に、次のトポロジを使用したノンセキュア Cisco UCM クラスタの設定例を示します。

図 52-2　ノンセキュア Cisco UCM クラスタ、パブリッシャ上の Cisco UCM および TFTP サーバ

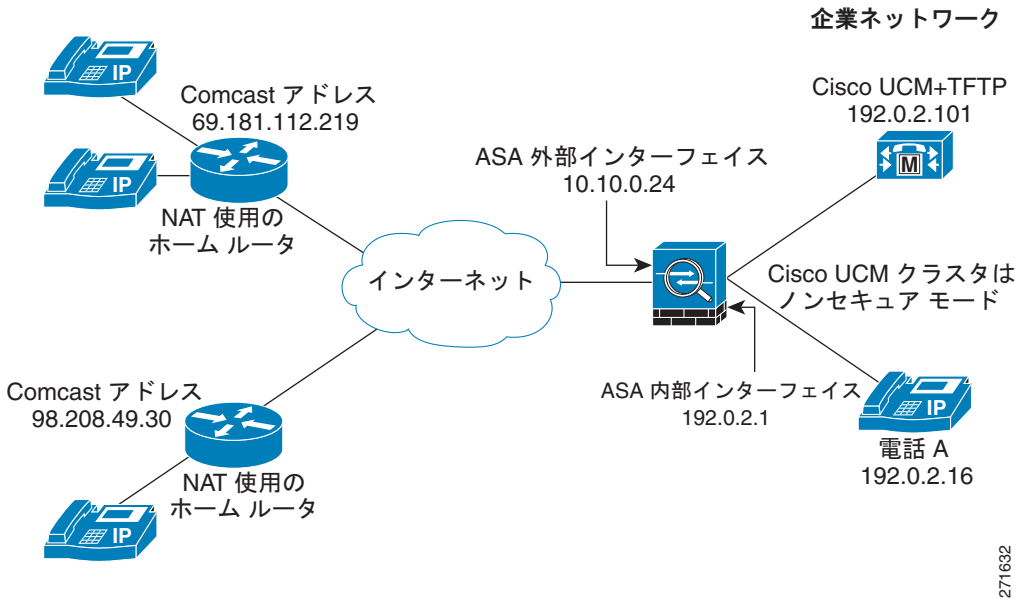



```
object network obj-192.0.2.101
    host 192.0.2.101
    nat (inside,outside) static 10.10.0.26
access-list pp extended permit udp any host 10.10.0.26 eq 69
access-group pp in interface outside
crypto key generate rsa label cucmtftp_kp modulus 1024
crypto ca trustpoint cucm_tftp_server
    enrollment self
    keypair cucmtftp_kp
crypto ca enroll cucm_tftp_server
ctl-file myctl
    record-entry cucm-tftp trustpoint cucm_tftp_server address 10.10.0.26
    no shutdown
tls-proxy mytls
    server trust-point _internal_PP_myctl
media-termination my_mediaterm
    address 192.0.2.25 interface inside
    address 10.10.0.25 interface outside
phone-proxy mypp
    media-termination my_mediaterm
    tftp-server address 192.0.2.101 interface inside
    tls-proxy mytls
    ctl-file myctl
class-map sec_sccp
    match port tcp 2443
class-map sec_sip
    match port tcp eq 5061
policy-map pp_policy
    class sec_sccp
        inspect skinny phone-proxy mypp
    class sec_sip
        inspect sip phone-proxy mypp
service-policy pp_policy interface outside
```

例 2 : 混合モードの Cisco UCM クラスタ、パブリッシャ上の Cisco UCM および TFTP サーバ

図 52-3 に、次のトポロジを使用した混合モードの Cisco UCM クラスタの設定例を示します。

図 52-3　混合モードの Cisco UCM クラスタ、パブリッシャ上の Cisco UCM および TFTP サーバ




```
object network obj-192.0.2.101
    host 192.0.2.101
    nat (inside,outside) static 10.10.0.26
access-list pp extended permit udp any host 10.10.0.26 eq 69
access-group pp in interface outside
crypto key generate rsa label cucmtftp_kp modulus 1024
crypto ca trustpoint cucm_tftp_server
    enrollment self
    keypair cucmtftp_kp
crypto ca enroll cucm_tftp_server
ctl-file myctl
    record-entry cucm-tftp trustpoint cucm_tftp_server address 10.10.0.26
    no shutdown
crypto key generate rsa label ldc_signer_key modulus 1024
crypto key generate rsa label phone_common modulus 1024
crypto ca trustpoint ldc_server
    enrollment self
    proxy_ldc_issuer
    fqdn my-ldc-ca.exmaple.com
    subject-name cn=FW_LDC_SIGNER_172_23_45_200
    keypair ldc_signer_key
    crypto ca enroll ldc_server
tls-proxy my_proxy
    server trust-point _internal_PP_myctl
    client ldc issuer ldc_server
    client ldc keypair phone_common
    client cipher-suite aes128-sha1 aes256-sha1
media-termination my_mediaterm
    address 192.0.2.25 interface inside
    address 10.10.0.25 interface outside
```

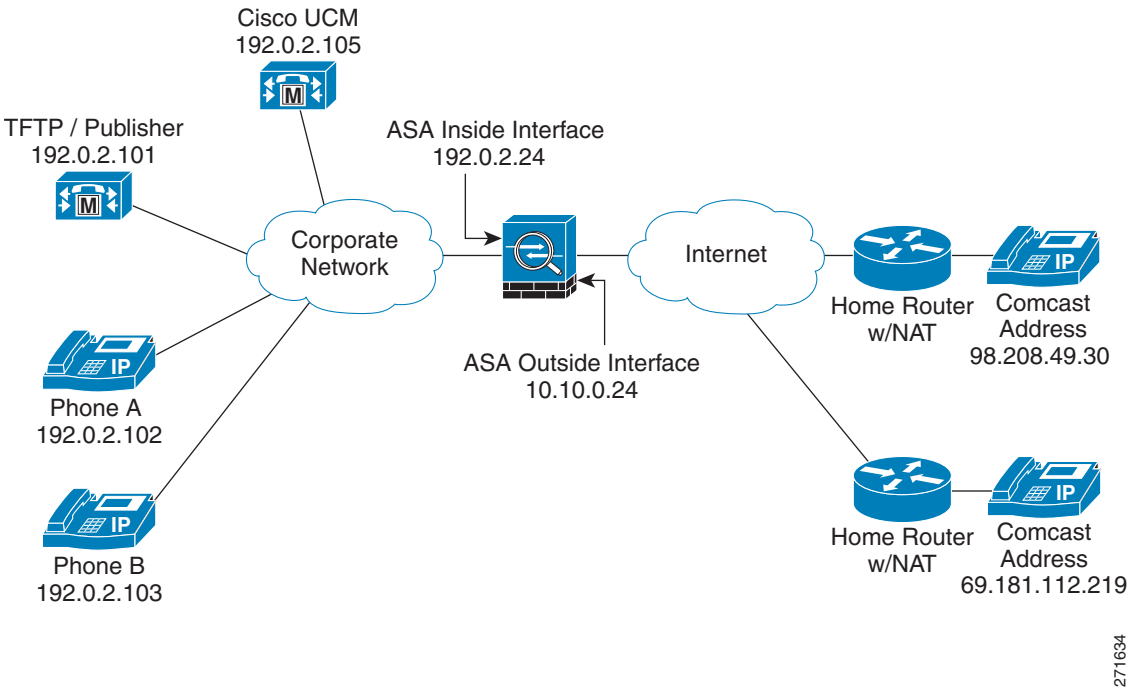
```
phone-proxy mypp
    media-termination my_mediaterm
    tftp-server address 192.0.2.101 interface inside
    tls-proxy mytls
    ctl-file myctl
    cluster-mode mixed
class-map sec_sccp
    match port tcp 2443
class-map sec_sip
    match port tcp eq 5061
policy-map pp_policy
    class sec_sccp
        inspect skinny phone-proxy mypp
    class sec_sip
        inspect sip phone-proxy mypp
service-policy pp_policy interface outside
```

例 3：混合モードの Cisco UCM クラスタ、異なるサーバ上の Cisco UCM および TFTP サーバ

図 52-4 に、次のトポロジを使用した混合モードの Cisco UCM クラスタの設定例を示します。このトポロジでは、TFTP サーバが Cisco UCM とは異なるサーバ上に置かれています。

この例では、TFTP サーバのスタティック インターフェイス PAT が、ASA の outside インターフェイスの IP アドレスであるかのように設定されています。

図 52-4　混合モードの Cisco UCM クラスタ、異なるサーバ上の Cisco UCM および TFTP サーバ




```
object network obj-192.0.2.105
    host 192.0.2.105
    nat (inside,outside) static 10.10.0.26
object network obj-192.0.2.101
    host 192.0.2.101
```

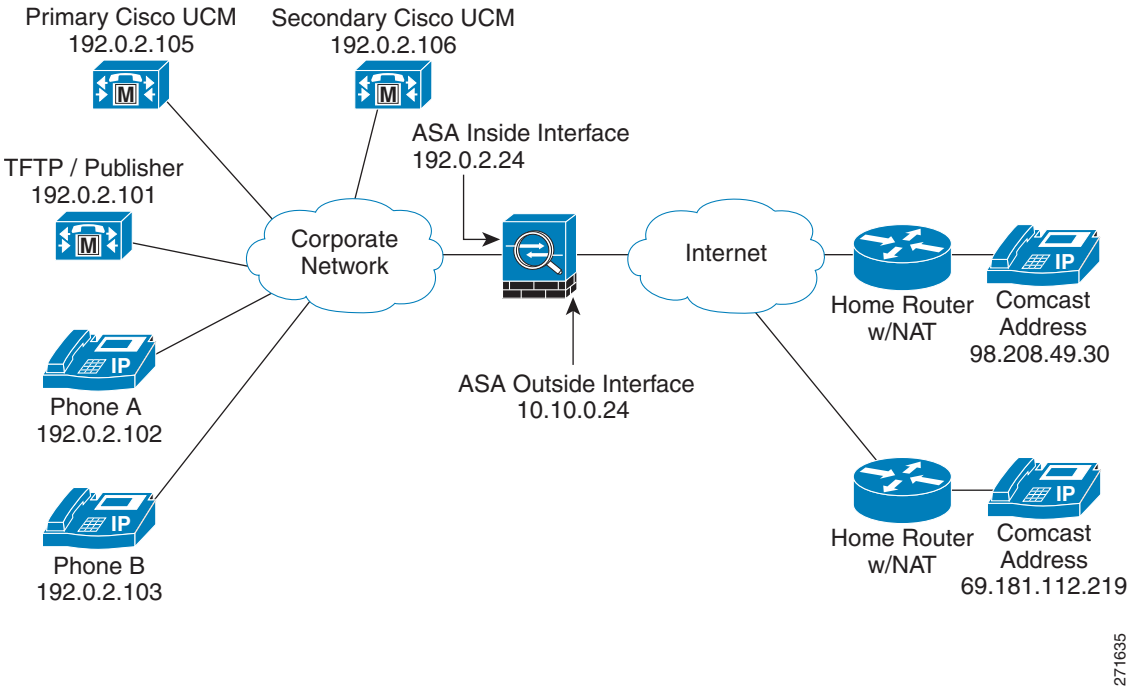
```
    nat (inside,outside) static interface udp 69 69
access-list pp extended permit udp any host 10.10.0.24 eq 69
access-group pp in interface outside
crypto key generate rsa label cucm_kp modulus 1024
crypto ca trustpoint cucm
    enrollment self
    keypair cucm_kp
crypto ca enroll cucm
crypto key generate rsa label tftp_kp modulus 1024
crypto ca trustpoint tftp_server
    enrollment self
    keypair tftp_kp
crypto ca enroll tftp_server
ctl-file myctl
    record-entry cucm trustpoint cucm_server address 10.10.0.26
    no shutdown
crypto key generate rsa label ldc_signer_key modulus 1024
crypto key generate rsa label phone_common modulus 1024
crypto ca trustpoint ldc_server
    enrollment self
    proxy_ldc_issuer
    fqdn my-ldc-ca.exmaple.com
    subject-name cn=FW_LDC_SIGNER_172_23_45_200
    keypair ldc_signer_key
    crypto ca enroll ldc_server
tls-proxy my_proxy
    server trust-point _internal_PP_myctl
    client ldc issuer ldc_server
    client ldc keypair phone_common
    client cipher-suite aes128-sha1 aes256-sha1
media-termination my_mediaterm
    address 192.0.2.25 interface inside
    address 10.10.0.25 interface outside
phone-proxy mypp
    media-termination my_mediaterm
    tftp-server address 192.0.2.101 interface inside
    tls-proxy mytls
    ctl-file myctl
    cluster-mode mixed
class-map sec_sccp
    match port tcp 2443
class-map sec_sip
    match port tcp eq 5061
policy-map pp_policy
    class sec_sccp
        inspect skinny phone-proxy mypp
    class sec_sip
        inspect sip phone-proxy mypp
service-policy pp_policy interface outside
```

例 4：混合モードの Cisco UCM クラスタ、異なるサーバ上のプライマリ Cisco UCM、セカンダリ Cisco UCM、および TFTP サーバ

図 52-5 に、次のトポロジを使用した混合モードの Cisco UCM クラスタの設定例を示します。このトポロジでは、TFTP サーバが、プライマリ Cisco UCM ともセカンダリ Cisco UCM とも異なるサーバ上に置かれています。

この例では、TFTP サーバのスタティック インターフェイス PAT が、ASA の outside インターフェイスの IP アドレスであるかのように設定されています。

図 52-5　混合モードの Cisco UCM クラスタ、異なるサーバ上のプライマリ Cisco UCM、セカンダリ Cisco UCM、および TFTP サーバ




```
object network obj-192.0.2.105
    host 192.0.2.105
    nat (inside,outside) static 10.10.0.27
object network obj-192.0.2.101
    host 192.0.2.101
    nat (inside,outside) static interface udp 69 69
object network obj-192.0.2.106
    host 192.0.2.106
    nat (inside,outside) static 10.10.0.26
access-list pp extended permit udp any host 10.10.0.24 eq 69
access-group pp in interface outside
crypto key generate rsa label cluster_kp modulus 1024
crypto ca trustpoint pri_cucm
    enrollment self
    keypair cluster_kp
crypto ca enroll pri_cucm
crypto ca trustpoint sec_cucm
    enrollment self
    serial-number
    keypair cluster_kp
crypto ca enroll sec_cucm
crypto ca trustpoint tftp_server
    enrollment self
    fqdn my_tftp.example.com
    keypair cluster_kp
crypto ca enroll tftp_server
ctl-file myctl
    record-entry tftp trustpoint tftp_server address 10.10.0.24
    record-entry cucm trustpoint pri_cucm_server address 10.10.0.27
    record-entry cucm trustpoint sec_cucm_server address 10.10.0.2
    no shutdown
crypto key generate rsa label ldc_signer_key modulus 1024
crypto key generate rsa label phone_common modulus 1024
```

```
crypto ca trustpoint ldc_server
    enrollment self
    proxy_ldc_issuer
    fqdn my-ldc-ca.exmaple.com
    subject-name cn=FW_LDC_SIGNER_172_23_45_200
    keypair ldc_signer_key
    crypto ca enroll ldc_server
tls-proxy my_proxy
    server trust-point _internal_PP_myctl
    client ldc issuer ldc_server
    client ldc keypair phone_common
    client cipher-suite aes128-sha1 aes256-sha1
media-termination my_mediaterm
    address 192.0.2.25 interface inside
    address 10.10.0.25 interface outside
phone-proxy mypp
    media-termination my_mediaterm
    tftp-server address 192.0.2.101 interface inside
    tls-proxy mytls
    ctl-file myctl
    cluster-mode mixed
class-map sec_sccp
    match port tcp 2443
class-map sec_sip
    match port tcp eq 5061
policy-map pp_policy
    class sec_sccp
        inspect skinny phone-proxy mypp
    class sec_sip
        inspect sip phone-proxy mypp
service-policy pp_policy interface outside
```

例 5：混合モードの Cisco UCM クラスタにおける LSC プロビジョニング、パブリッシャ上の Cisco UCM および TFTP サーバ

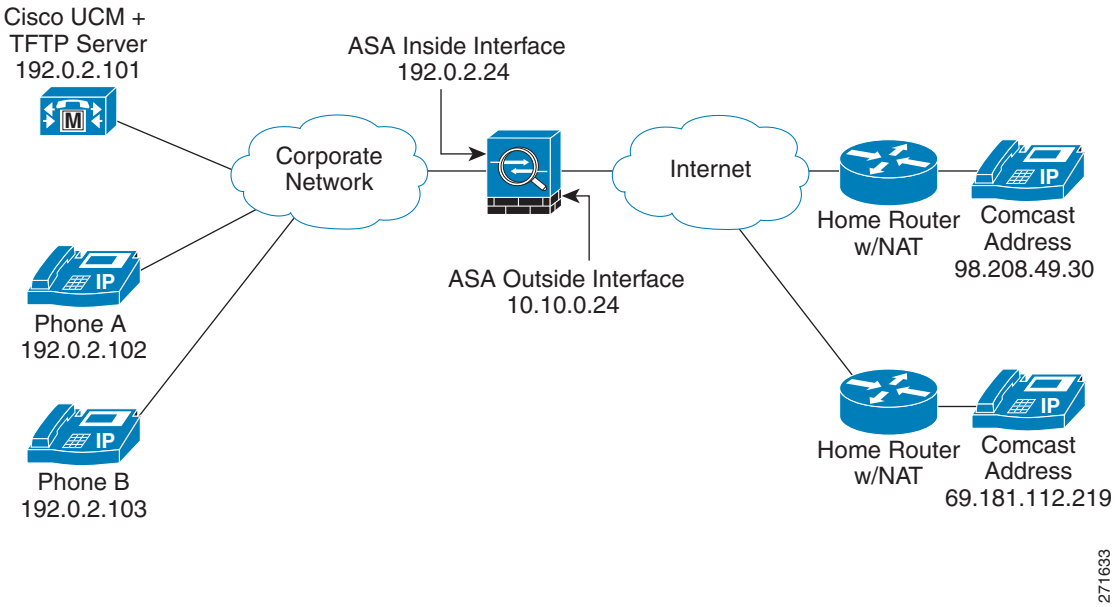
図 52-6 に、次のトポロジを使用した混合モードの Cisco UCM クラスタの設定例を示します。このクラスタでは、LSC プロビジョニングが必要です。

（注） リモート IP 電話に LSC プロビジョニングを行うことはお勧めしません。LSC プロビジョニングを実行するには、最初に IP 電話をノンセキュア モードで登録する必要があるためです。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。可能であれば、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してください。

この例では、アクセス リストを作成して、IP 電話から TFTP サーバに到達できるようにし、IP 電話で SIP および SCCP 用のノンセキュア ポートと LSC プロビジョニング用の CAPF ポートを開くことによって、ノンセキュア モードで登録できるようにします。

さらに、Cisco UCM Certificate Management ソフトウェアから CAPF 証明書をコピーして貼り付けることによって、CAPF トラストポイントを作成します。

図 52-6　混合モードの Cisco UCM クラスタにおける LSC プロビジョニング、パブリッシャ上の Cisco UCM および TFTP サーバ




```
object network obj-192.0.2.105
    host 192.0.2.105
    nat (inside,outside) static 10.10.0.26
object network obj-192.0.2.101
    host 192.0.2.101
    nat (inside,outside) static interface udp 69 69
access-list pp extended permit udp any host 10.10.0.24 eq 69
access-list pp extended permit tcp any host 10.10.0.26 eq 2000
access-list pp extended permit tcp any host 10.10.0.26 eq 5060
access-list pp extended permit tcp any host 10.10.0.26 eq 3804
access-group pp in interface outside
crypto key generate rsa label cluster_kp modulus 1024
crypto ca trustpoint cucm
    enrollment self
    keypair cluster_kp
crypto ca enroll cucm
crypto ca trustpoint tftp_server
    enrollment self
    serial-number
    keypair cluster_kp
crypto ca enroll tftp_server
crypto ca trustpoint capf
    enroll terminal
crypto ca authenticate capf
ctl-file myctl
    record-entry cucm trustpoint cucm_server address 10.10.0.26
    record-entry capf trustpoint capf address 10.10.0.26
    no shutdown
crypto key generate rsa label ldc_signer_key modulus 1024
crypto key generate rsa label phone_common modulus 1024
crypto ca trustpoint ldc_server
    enrollment self
    proxy_ldc_issuer
    fqdn my-ldc-ca.exmaple.com
    subject-name cn=FW_LDC_SIGNER_172_23_45_200
    keypair ldc_signer_key
    crypto ca enroll ldc_server
tls-proxy my_proxy
```

```
    server trust-point _internal_PP_myctl
    client ldc issuer ldc_server
    client ldc keypair phone_common
    client cipher-suite aes128-sha1 aes256-sha1
media-termination my_mediaterm
    address 192.0.2.25 interface inside
    address 10.10.0.25 interface outside
phone-proxy mypp
    media-termination my_mediaterm
    tftp-server address 192.0.2.101 interface inside
    tls-proxy mytls
    ctl-file myctl
    cluster-mode mixed
class-map sec_sccp
    match port tcp 2443
class-map sec_sip
    match port tcp eq 5061
policy-map pp_policy
    class sec_sccp
        inspect skinny phone-proxy mypp
    class sec_sip
        inspect sip phone-proxy mypp
service-policy pp_policy interface outside
```

例 6：VLAN トランスバーサル

図 52-7 に、音声およびデータの VLAN シナリオで Cisco IP Communicator（CIPC）ソフトウェア電話を構成する場合に、強制的に認証モードで実行する設定例を示します。データ VLAN 上の CIPC ソフトウェア電話と音声 VLAN 上のハードウェア電話との間には、VLAN トランスバーサルが必要です。

この例の Cisco UCM クラスタ モードはノンセキュアです。

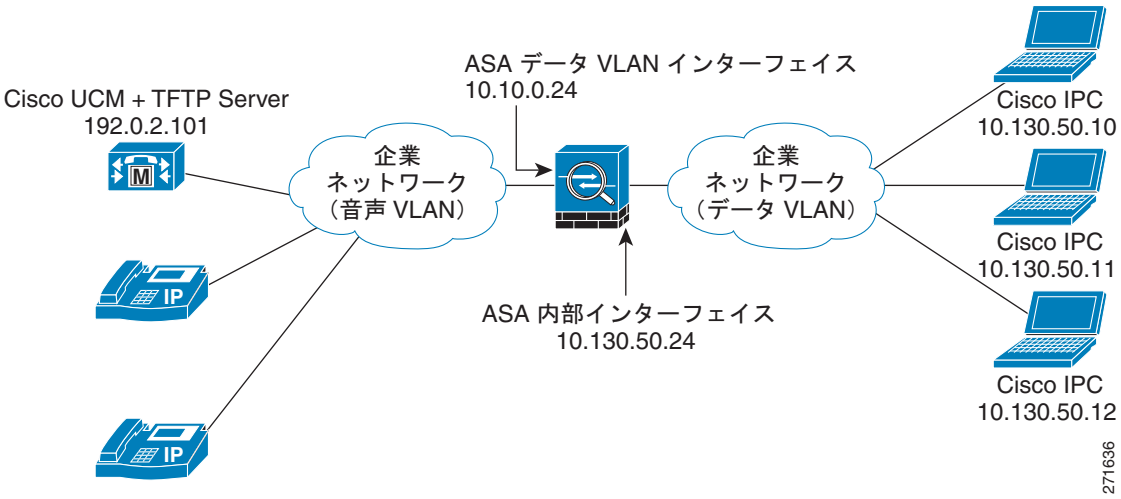
この例では、アクセス リストを作成して、IP 電話から TFTP サーバに到達できるようにし、IP 電話で SIP および SCCP 用のノンセキュア ポートと LSC プロビジョニング用の CAPF ポートを開くことによって、ノンセキュア モードで登録できるようにします。

この例では、各 CIPC が音声 VLAN の IP アドレス空間にマッピングされるように、PAT を使用して CIPC に NAT を設定します。

さらに、Cisco UCM Certificate Management ソフトウェアから CAPF 証明書をコピーして貼り付けることによって、CAPF トラストポイントを作成します。

（注） Cisco IP Communicator では認証モードだけがサポートされ、暗号化モードはサポートされません。したがって、暗号化された音声トラフィック（SRTP）が CIPC ソフトウェア電話から流れることはありません。

図 52-7　データ VLAN 上の CIPC ソフトウェア電話と音声 VLAN 上のハードウェア電話との間の VLAN トランスバーサル




```
object network obj-10.130.50.0
    subnet 10.130.50.0 255.255.255.0
    nat (data,voice) dynamic 192.0.2.10
object network obj-10.130.50.5
    host 10.130.50.5
    nat (data,voice) static 192.0.2.101
access-list pp extended permit udp any host 10.130.50.5 eq 69
access-list pp extended permit tcp any host 10.130.50.5 eq 2000
access-list pp extended permit tcp any host 10.130.50.5 eq 5060
access-list pp extended permit tcp any host 10.130.50.5 eq 3804
access-group pp in interface data
crypto ca generate rsa label cucmtftp_kp modulus 1024
crypto ca trustpoint cucm_tftp_server
    enrollment self
    keypair cucmtftp_kp
crypto ca enroll cucm_tftp_server
crypto ca trustpoint capf
    enrollment terminal
crypto ca authenticate capf
ctl-file myctl
    record-entry cucm-tftp trustpoint cucm_tftp_server address 10.130.50.5
    record-entry capf trustpoint capf address 10.130.50.5
    no shutdown
tls-proxy mytls
    server trust-point _internal_PP_myctl
media-termination my_mediaterm
    address 10.130.50.2
phone-proxy mypp
    media-termination my_mediaterm
    tftp-server address 10.10.0.20 interface inside
    tls-proxy mytls
    ctl-file myctl
    cipc security-mode authenticated
class-map sec_sccp
    match port tcp eq 2443
class-map sec_sip
    match port tcp eq 5061
policy-map pp_policy
    class sec_sccp
        inspect skinny phone-proxy mypp
```

```
    class sec_sip
        inspect sip phone-proxy mypp
service-policy pp_policy interface data
```

電話プロキシの機能履歴

表 52-7 に、この機能のリリース履歴を示します。

表 52-7　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。次の新しいコマンドが導入されました。 **cipc security-mode authenticated**、**clear configure ctl**、**clear configure phone-proxy**、**cluster-ctl-file**、**cluster-mode nonsecure**、**ctl-file**（グローバル）、**ctl-file**（電話プロキシ）、**debug phone proxy**、**disable service-settings**、**media-termination address**、**phone-proxy**、**proxy-server**、**record-entry**、**sast**、**show phone-proxy**、**show running-config ctl**、**show running-config phone-proxy**、**timeout secure-phones**、**tftp-server address**。
メディア ターミネーション アドレスに対する NAT	8.1(2)	**media-termination address** コマンドが NAT に対応するように以下のように変更されました。 [**no**] **media-termination address** *ip_address* **interface** *intf_name* **interface** *inft_name* キーワードが追加されました。 **rtp-min-port** キーワードと **rtp-max-ports** キーワードがコマンド構文から除外され、次のような別個のコマンドになりました。 **rtp-min-port** *port1* **rtp-max-port** *port2*