セキュリティの設定

この章では、Cisco Unified Communications Manager Express（Cisco Unified CME）の電話機認証サポート、Cisco Unified IP Phone に対する Hypertext Transfer Protocol Secure（HTTPS）のプロビジョニング、および次のセキュア音声コール機能を提供する Cisco Unified CME のメディア暗号化（SRTP）機能について説明します。

- Secure Real-Time Transport Protocol（SRTP）および H.323 プロトコルを使用した、Cisco Unified CME ネットワークでのセキュア コール制御シグナリングおよびメディア ストリーム。
- H.323 トランクを使用した Cisco Unified CME ネットワークのセキュア補足サービス。
- セキュアな Cisco VG224 Analog Phone Gateway エンドポイント。

このモジュールで紹介する機能情報の入手方法

お使いの Cisco Unified CME のバージョンが、このモジュールで説明されている機能の一部をサポートしていないことがあります。各機能がサポートされているバージョンのリストについては、「セキュリティの機能情報」（P.665）を参照してください。

内容

- 「セキュリティの前提条件」（P.590）
- 「セキュリティの制約事項」（P.590）
- 「セキュリティについて」（P.591）
- 「セキュリティの設定方法」（P.603）
- 「セキュリティの設定例」（P.649）
- 「次の作業」（P.663）
- 「その他の参考資料」（P.664）
- 「セキュリティの機能情報」（P.665）

セキュリティの前提条件

- 電話機認証用に Cisco Unified CME 4.0 以降のバージョン。
- Cisco Unified CME でのメディア暗号化（SRTP）用に Cisco Unified CME 4.2 以降のバージョン。
- サポートされるプラットフォームでの Cisco IOS フィーチャ セットの Advanced Enterprise Services（adventerprisek9）または Advanced IP Services（advipservicesk9）。
- Firmware 9.0(4) 以降のバージョンが、HTTPS プロビジョニング用に IP Phone にインストールされていること。
- 次のいずれかの方法を使用して、システム クロックが設定されていること。
  - ネットワーク タイム プロトコル（NTP）を設定する。設定については、「Cisco Unified CME ルータでのネットワーク タイム プロトコルのイネーブル化」（P.100）を参照してください。
  - **clock set** コマンドを使用して、ソフトウェア クロックを手動で設定する。このコマンドの詳細については、『*Cisco IOS Network Management Command Reference*』を参照してください。

セキュリティの制約事項

電話機認証

- Cisco Unified CME の電話機認証は、Cisco IAD 2400 シリーズまたは Cisco 1700 シリーズでサポートされていません。

メディア暗号化

- セキュアな 3 者間ソフトウェア会議はサポートされていません。SRTP で開始したセキュア コールで会議に参加すると、必ず非セキュアなリアルタイム転送プロトコル（RTP）に戻ります。
- 1 人の参加者が 3 者間会議から退出すると、残りの 2 人の参加者が単一の Cisco Unified CME への SRTP 対応ローカル Skinny Client Control Protocol（SCCP）エンドポイントであり、残りの参加者のどちらかが会議の作成者である場合、その 2 人の参加者間コールがセキュアに戻ります。残り 2 人の参加者の一方だけが RTP に対応している場合、コールは非セキュアなままになります。残りの 2 人の参加者が FXS、PSTN、または VoIP を介して接続されている場合、コールは非セキュアのままになります。
- Cisco Unity Express へのコールはセキュアではありません。
- 保留音（MOH）はセキュアではありません。
- ビデオ コールはセキュアではありません。
- モデム リレーおよび T.3 Fax リレーのコールはセキュアではありません。
- メディアのフローアラウンドは、コール転送およびコール自動転送に対応していません。
- インバンド トーンと RFC 2833 DTMF の間の変換はサポートされていません。RFC 2833 DTMF の処理は、暗号キーがセキュア DSP Farm デバイスに送信される場合はサポートされますが、コーデック パススルーに対してはサポートされません。
- セキュアな Cisco Unified CME は SIP トランクをサポートしていません。H.323 トランクのみサポートされています。
- セキュア コールは、デフォルトのセッション アプリケーションのみでサポートされています。

セキュリティについて

セキュリティをイネーブルにするには、次の概念について理解しておく必要があります。

電話機認証

- 「電話機認証の概要」（P.591）
- 「公開キー インフラストラクチャ」（P.592）
- 「電話機認証のコンポーネント」（P.593）
- 「電話機の認証プロセス」（P.596）
- 「スタートアップ メッセージ」（P.597）
- 「コンフィギュレーション ファイルのメンテナンス」（P.597）
- 「CTL ファイルのメンテナンス」（P.597）
- 「CTL クライアントとプロバイダー」（P.598）
- 「MIC ルート証明書の手動インポート」（P.598）

メディア暗号化

- 「メディア暗号化の機能設計」（P.598）
- 「セキュアな Cisco Unified CME」（P.599）
- 「セキュアな補足サービス」（P.600）
- 「DSP Farm トランスコーディングが設定された状態のリモート電話機に対するセキュアなトランスコーディング」（P.602）
- 「セキュア Cisco Unified CME と Cisco Unity Express」（P.602）
- 「セキュア Cisco Unified CME と Cisco Unity」（P.603）

HTTPS プロビジョニング

- 「Cisco Unified IP Phone 用の HTTPS プロビジョニング」（P.603）

電話機認証の概要

電話機認証は、Cisco Unified CME と IP Phone の間にセキュアな SCCP シグナリングを提供するためのセキュリティ インフラストラクチャです。Cisco Unified CME 電話機認証の目的は、Cisco Unified CME IP テレフォニー システムにセキュアな環境を作成することです。

電話機認証は、セキュリティに関する次のニーズに対処します。

- システム内の各エンドポイントのアイデンティティを確立する
- デバイスを認証する
- シグナリング セッションのプライバシーを提供する
- コンフィギュレーション ファイルを保護する

Cisco Unified CME 電話機認証は、認証と暗号化を実装して、電話機または Cisco Unified CME システムの ID 盗用、データ改ざん、コール シグナリングの改ざん、またはメディア ストリームの改ざんを防止します。これらの脅威を防止するために、Cisco Unified IP テレフォニー ネットワークは認証済みの通信ストリームを確立および管理し、ファイルが電話機に転送される前にファイルにデジタル署名を行って、Cisco Unified IP Phone 間のコール シグナリングを暗号化します。

Cisco Unified CME 電話機認証は、次のプロセスを使用します。

- 「電話機認証」（P.592）
- 「ファイル認証」（P.592）
- 「シグナリング認証」（P.592）

電話機認証

電話機認証プロセスは、Cisco Unified CME ルータとサポートされるデバイスとの間で、各エンティティが他のエンティティの証明書を受け取ると行われます。その場合のみ、エンティティ間でセキュアな接続が行われます。電話機認証は、既知の信頼できる証明書およびトークンである証明書信頼リスト（CTL）ファイルを使用します。電話機はトランスポート層セキュリティ（TLS）セッション接続を使用して Cisco Unified CME と通信します。これを行うには、次の基準を満たす必要があります。

- 証明書が電話機に存在していること。
- 電話機のコンフィギュレーション ファイルが電話機に存在し、そのファイルに Cisco Unified CME エントリと証明書が存在していること。

ファイル認証

ファイル認証プロセスは、電話機が Trivial File Transfer Protocol（TFTP）サーバからダウンロードしたデジタル署名されたファイル（たとえば、コンフィギュレーション ファイル、リング リスト ファイル、ロケール ファイル、および CTL ファイル）を検証します。電話機がこれらのタイプのファイルを TFTP サーバから受け取ると、電話機はそのファイルの署名を検証して、ファイルが作成された後にファイルの改ざんが行われていないことを確認します。

シグナリング認証

シグナリング完全性とも呼ばれるシグナリング認証プロセスは、TLS プロトコルを使用して、伝送中にシグナリング パケットが改ざんされていないことを検証します。シグナリング認証は、CTL ファイルの作成に依存します。

公開キー インフラストラクチャ

Cisco Unified CME の電話機認証では、IP Phone の証明書ベースの認証に、Cisco IOS ソフトウェアの公開キー インフラストラクチャ（PKI）機能が使用されます。PKI を使用すると、セキュアなデータ ネットワークで暗号化情報と ID 情報を配信、管理、失効するためのスケーラブルでセキュアなメカニズムを実現できます。セキュア通信に参加しているすべてのエンティティ（人またはデバイス）は、エンティティが Rivest-Shamir-Adleman（RSA）キー ペア（秘密キーと公開キー）を生成し、信頼できるエンティティ（認証局（CA）またはトラストポイントとも呼ばれます）によって ID を検証するというプロセスを使用して、PKI に登録します。

各エンティティが PKI に登録されると、PKI のすべてのピア（エンド ホストともいいます）は、CA が発行したデジタル証明書を付与されます。

セキュアな通信セッションをネゴシエーションする必要があるときは、ピアはデジタル証明書を交換します。ピアは証明書内の情報を基に他のピアの ID を確認し、証明書内の公開キーを使って、暗号化されたセッションを確立します。

PKI の詳細については、ご使用の Cisco IOS リリースの『*Cisco IOS Security Configuration Guide*』にある「*Implementing and Managing a PKI Features Roadmap*」の項を参照してください。

電話機認証のコンポーネント

さまざまなコンポーネントが連携して、Cisco Unified CME システムでのセキュアな通信が確保されます。表 52 に、Cisco Unified CME 電話認証コンポーネントを示します。

表 52　Cisco Unified CME の電話認証コンポーネント

コンポーネント	定義
証明書	ユーザ名またはデバイス名をその公開キーにバインドする電子文書。通常、証明書はデジタル署名を検証するために使用されます。セキュアな通信中は、認証に証明書が必要です。エンティティは CA に登録することで証明書を取得します。
シグニチャ	エンティティに関連するトランザクションが真性であることの、エンティティからの保証。エンティティの秘密キーを使用して、トランザクションに署名を行い、対応する公開キーを使用して復号化を行います。
RSA キー ペア	RSA は公開キー暗号化システムで、Ron Rivest、Adi Shamir、Leonard Adleman の 3 名によって開発されました。 RSA キー ペアは、公開キーと秘密キーで構成されます。公開キーは証明書に含まれているため、ピアはそれを使用してルータに送信されるデータを暗号化できます。秘密キーはルータに保持され、ピアによって送信されたデータの復号化と、ピアとネゴシエーションするときの、トランザクションのデジタル署名に使用されます。 複数の RSA キー ペアを使用して、さまざまな認証局またはさまざまな証明書に対して、キーの長さ、キーのライフタイム、およびキーのタイプなどのポリシー要件を照合できます。
証明書サーバ トラストポイント	証明書サーバは、正当な要求の受信に対して、証明書を生成および発行します。証明書サーバと同じ名前を持つトラストポイントが証明書を保存します。各トラストポイントには 1 つの証明書と、CA 証明書のコピーがあります。
認証局（CA）	ルート証明書サーバ。証明書要求の管理と、関係するネットワークデバイスへの証明書の発行を担当します。このサービスは、参加デバイスを一元的に管理します。またこれらのサービスによって受信者は、明示的に信頼してアイデンティティを確認し、デジタル証明書を作成できます。CA は、Cisco Unified CME ルータ上の Cisco IOS CA、別のルータ上の Cisco IOS CA、またはサードパーティの CA にすることができます。
Registration Authority（RA）	CA に必要なデータの一部またはすべてを記録または確認して、証明書を発行します。CA がサードパーティ CA である場合や、Cisco IOS CA が Cisco Unified CME ルータにない場合に、これが必要になります。

表 52　Cisco Unified CME の電話認証コンポーネント （続き）

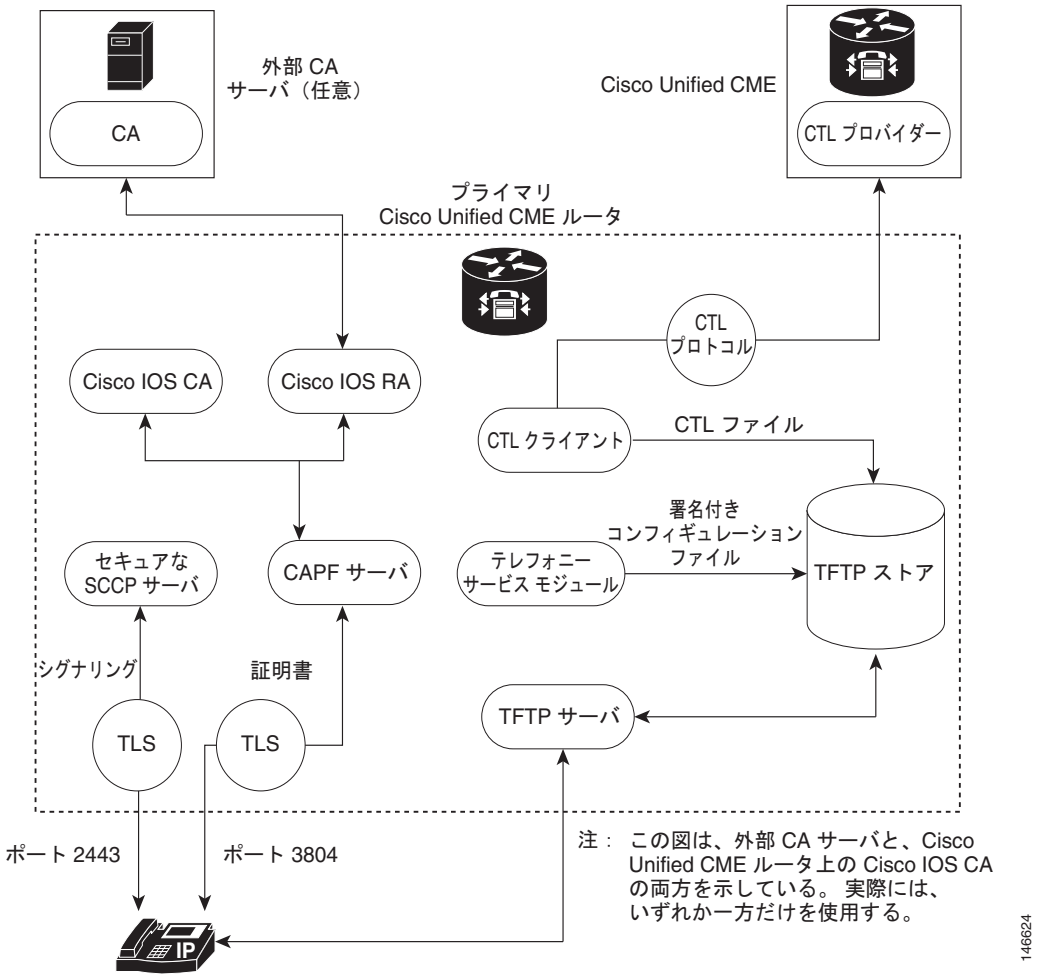
コンポーネント	定義
証明書信頼リスト（CTL）ファイル CTL クライアント CTL プロバイダー	IP Phone が対話する必要のあるすべてのサーバ（たとえば、Cisco Unified CME サーバ、TFTP サーバ、および CAPF サーバ）の公開キー情報（サーバ ID）を含む必須構造。CTL ファイルは、SAST によってデジタル署名されます。 CTL クライアントを設定した後、CTL ファイルを作成して、それを TFTP ディレクトリで使用できるようにします。CTL ファイルは、SAST 証明書の対応する秘密キーを使用して署名されます。これで、IP Phone はこの CTL ファイルを TFTP ディレクトリからダウンロードできるようになります。各電話機の CTL ファイルのファイル名形式は CTLSEP<mac-addr>.tlv です。 CTL クライアントが、Cisco Unified CME ルータではないネットワーク上のルータで実行されている場合、ネットワーク上の各 Cisco Unified CME ルータに CTL プロバイダーを設定する必要があります。同様に、CTL クライアントがネットワーク上の 2 台の Cisco Unified CME ルータの一方で実行されている場合、CTL プロバイダーをもう一方の Cisco Unified CME ルータに設定する必要があります。CTL プロトコルは、2 番めの Cisco Unified CME ルータが電話機によって信頼され、その逆の方向にも信頼されるようにできる CTL プロバイダーとの間で情報を転送します。
証明書失効リスト（CRL）	証明書の失効日を含み、示されている証明書が有効か失効しているかを判別するために使用されるファイル。
システム管理者のセキュリティ トークン（SAST）	CTL ファイルの署名を担当する CTL クライアントの部分。Cisco Unified CME の証明書と、それに関連するキー ペアが、SAST 機能に使用されます。セキュリティ上の理由で、CTL ファイルには 2 つの異なる証明書に関連する 2 つの SAST レコードが実際にあります。これらは、SAST1 および SAST2 と呼ばれます。証明書の 1 つが失われるか、破損すると、CTL クライアントはもう 1 つの証明書を使用して CTL ファイルを再生成します。電話機が新しい CTL ファイルをダウンロードすると、以前にインストールされていた元の 2 つの公開キーの 1 つだけを使用して検証します。このメカニズムにより、IP Phone は不明なソースから CTL ファイルを受け取らないようになります。
Certificate Authority Proxy Function（CAPF）	要求元の電話機に証明書（LSC）を発行するエンティティ。CAPF は電話機のプロキシであり、CA と直接通信することはできません。CAPF は、次の証明書管理タスクを実行することもできます。 • ローカルで有効な既存の証明書を電話機でアップグレードする。 • 電話機の証明書を取得して、表示およびトラブルシューティングに使用する。 • 電話機の LSC を削除する。

表 52　Cisco Unified CME の電話認証コンポーネント （続き）

コンポーネント	定義
製造元でインストールされる証明書（MIC） ローカルで有効な証明書（LSC）	電話機でセキュアな通信を行うには、証明書が必要です。多くの電話機は MIC 付きで工場から出荷されますが、MIC は期限切れになったり、紛失や破損が生じたりすることがあります。MIC 付きで出荷されない電話機もあります。LSC は、CAPF サーバを使用してローカルで電話機に発行される証明書です。
トランスポート層セキュリティ（TLS）プロトコル	Netscape Secure Socket Layer（SSL）プロトコルに基づいた IETF 標準（RFC 2246）プロトコル。TLS セッションは、ハンドシェイク プロトコルを使用してプライバシーとデータ整合性を提供することで確立されます。 TLS レコード層フラグメントは、ハンドシェイク メッセージを含むアプリケーション データや他の TLS 情報のフラグメント化とデフラグメント化、圧縮と復元、および暗号化と復号化を行います。

図 21 に、Cisco Unified CME 電話機の認証環境における構成要素を示します。

図 21　Cisco Unified CME 電話機の認証



電話機の認証プロセス

次に、電話機の認証プロセスについて概要を説明します。

Cisco Unified CME 電話機の認証は、次のよう行われます。

1. 証明書が発行されます。

   CA が、Cisco Unified CME、SAST、CAPF、および TFTP の各機能に証明書を発行します。

2. CTL ファイルが作成されて、署名および公開されます。

   a. CTL ファイルは、コンフィギュレーション駆動型の CTL クライアントによって作成されます。その目的は、各電話機に CTLfile.tlv を作成し、それを TFTP ディレクトリに保存することです。このタスクを完了するには、CTL クライアントに CAPF サーバ、Cisco Unified CME サーバ、TFTP サーバ、および SAST の証明書と公開キー情報が必要です。

   b. CTL ファイルは SAST クレデンシャルによって署名されます。セキュリティ上の理由で、CTL ファイルには 2 つの異なる証明書に関連する 2 つの SAST レコードがあります。証明書の 1 つが失われるか、破損すると、CTL クライアントはもう 1 つの証明書を使用して CTL ファイルを再生成します。電話機が新しい CTL ファイルをダウンロードすると、以前にインストールされていた元の 2 つの公開キーの中の 1 つだけを使用してダウンロードを検証します。このメカニズムにより、IP Phone は不明なソースから CTL ファイルを受け取らないようになります。

   c. CTL ファイルは TFTP サーバで公開されます。外部 TFTP サーバはセキュア モードでサポートされていないため、コンフィギュレーション ファイルは Cisco Unified CME システム自体で生成され、TFTP サーバのクレデンシャルによって署名されます。TFTP サーバのクレデンシャルは、Cisco Unified CME のクレデンシャルと同じにすることができます。必要であれば、CTL クライアント インターフェイスで適切なトラストポイントが設定されている場合、TFTP 機能用に別個の証明書を生成できます。

3. テレフォニー サービス モジュールは、電話機のコンフィギュレーション ファイルに署名し、各電話機はそのファイルを要求します。

4. IP Phone が起動すると、TFTP サーバから CTL ファイル（CTLfile.tlv）を要求し、デジタル署名されたそのコンフィギュレーション ファイルをダウンロードします。ファイル名の形式は SEP<mac-address>.cnf.xml.sgn です。

5. 次に、電話機はコンフィギュレーション ファイルから CAPF コンフィギュレーション ステータスを読み取ります。証明動作が必要な場合、電話機は TCP ポート 3804 で CAPF サーバを使用して TLS セッションを開始し、CAPF プロトコル ダイアログを開始します。証明動作には、アップグレード、削除、またはフェッチの各動作があります。アップグレード動作が必要な場合、CAPF サーバは電話機に代わって CA から証明書を要求します。CAPF サーバは CAPF プロトコルを使用して、公開キーや電話機 ID など、電話機から必要な情報を取得します。電話機がサーバから証明書を正常に受け取ると、電話機はそれをフラッシュ メモリに保存します。

6. .cnf.xml ファイルのデバイス セキュリティ モード設定が認証済みまたは暗号化済みに設定されている場合、電話機は証明書をフラッシュに保存し、既知の TCP ポート（2443）でセキュアな Cisco Unified CME サーバとの TLS 接続を開始します。この TLS セッションは、両者から相互に認証されます。IP Phone は、TFTP サーバから最初にダウンロードした CTL ファイルからの Cisco Unified CME サーバの証明書を認識します。発行元の CA 証明書がルータに存在するため、電話機の LSC は Cisco Unified CME サーバに対して信頼できる相手になります。

スタートアップ メッセージ

証明書サーバがスタートアップ コンフィギュレーションの一部である場合、起動プロシージャの間に次のメッセージが表示される場合があります。

```
% Failed to find Certificate Server's trustpoint at startup
% Failed to find Certificate Server's cert.
```

これらのメッセージは、スタートアップ コンフィギュレーションがまだ完全に解析されていないため、証明書サーバを設定するために一時的に使用できなくなることを示す情報メッセージです。スタートアップ コンフィギュレーションが破損した場合、これらのメッセージはデバッグに役立ちます。

コンフィギュレーション ファイルのメンテナンス

セキュアな環境では、複数タイプのコンフィギュレーション ファイルをホストして使用するには、事前にデジタル署名する必要があります。署名されたすべてのファイルのファイル名には .sgn サフィックスが付けられます。

Cisco Unified CME テレフォニー サービス モジュールは電話機のコンフィギュレーション ファイル（.cnf.xml suffix）を作成し、それらを Cisco IOS TFTP サーバに収容します。これらのファイルは TFTP サーバのクレデンシャルによって署名されます。

電話機のコンフィギュレーション ファイル以外に、ネットワーク ファイルやユーザのローカル ファイルなど、他の Cisco Unified CME コンフィギュレーション ファイルにも署名が必要です。これらのファイルは Cisco Unified CME によって内部生成され、署名されていないバージョンが更新または作成されると必ず、署名されたバージョンが現在のコード パスに自動的に作成されます。

ringlist.xml、distinctiveringlist.xml、オーディオ ファイルなど、Cisco Unified CME で生成されない他のコンフィギュレーション ファイルは、Cisco Unified CME の機能に使用されることがよくあります。これらのコンフィギュレーション ファイルの署名されたバージョンは、自動的には作成されません。Cisco Unified CME で生成されていない新しいコンフィギュレーション ファイルが Cisco Unified CME にインポートされた場合は必ず、**load-cfg-file** コマンドを使用してください。このコマンドによって、次の処理がすべて実行されます。

- 署名されていないバージョンのファイルを TFTP サーバに収容する。
- 署名されたバージョンのファイルを作成する。
- 署名されたバージョンのファイルを TFTP サーバに収容する。

署名されていないバージョンのファイルのみを TFTP サーバに収容する必要がある場合は、**tftp-server** コマンドの代わりに **load-cfg-file** コマンドを使用する方法もあります。

CTL ファイルのメンテナンス

CTL ファイルには SAST レコードとその他のレコードが含まれています。(最大 2 つの SAST レコードが存在する可能性があります)。CTL ファイルにリストされている SAST クレデンシャルの 1 つによって CTL ファイルがデジタル署名された後、CTL ファイルは電話機にダウンロードされ、フラッシュに保存されます。CTL ファイルを受信すると、電話機は、元の CTL ファイルに存在する SAST クレデンシャルの 1 つによって署名されている場合にのみ、新しい CTL ファイルまたは変更された CTL ファイルを信頼します。

このため、元の SAST クレデンシャルの 1 つだけを含んだ CTL ファイルが再生成されるよう注意する必要があります。両方の SAST クレデンシャルが破損し、新しいクレデンシャルを使用して CTL ファイルを生成する必要がある場合は、電話機を出荷時の初期状態にリセットする必要があります。

CTL クライアントとプロバイダー

CTL クライアントは CTL ファイルを生成します。CTL クライアントは、CTL ファイルに必要なトラストポイントの名前を入手する必要があります。これは Cisco Unified CME と同じルータ、または別のスタンドアロン ルータで実行できます。CTL クライアントがスタンドアロン ルータ（Cisco Unified CME ルータ以外のルータ）で実行されている場合、各 Cisco Unified CME ルータに CTL プロバイダーを設定する必要があります。CTL プロバイダーは、Cisco Unified CME サーバ機能のクレデンシャルを、別のルータで実行している CTL クライアントにセキュアに伝達します。

CTL クライアントがプライマリまたはセカンダリのいずれかの Cisco Unified CME ルータで実行している場合、CTL クライアントが実行していない各 Cisco Unified CME ルータ上に CTL プロバイダーを設定する必要があります。

CTL クライアントと CTL プロバイダーとの間の通信には、CTL プロトコルが使用されます。CTL プロトコルを使用することで、すべての Cisco Unified CME ルータのクレデンシャルが CTL ファイルに存在するようになり、すべての Cisco Unified CME ルータが、CA によって発行された電話機証明書へのアクセス権を持つことができます。両方の要素が、セキュアな通信の前提条件になります。

CTL クライアントとプロバイダーをイネーブルにするには、「CTL クライアントの設定」（P.614）および「CTL プロバイダーの設定」（P.626）を参照してください。

MIC ルート証明書の手動インポート

CAPF サーバとの TLS ハンドシェイク中に電話機が MIC を使用する場合、CAPF サーバはそれを確認するための MIC のコピーを持っている必要があります。IP Phone のタイプごとに、異なる証明書が使用されます。

電話機が MIC は持っているが、LSC は持っていない場合、電話機は認証に MIC を使用します。たとえば、デフォルトで MIC は持っているが、LSC は持っていない Unified IP Phone 7970 を使用するとします。この電話機の MIC に設定された認証モードを使用して証明書のアップグレードをスケジュールすると、電話機は認証用として、その MIC を Cisco Unified CME CAPF サーバに提示します。CAPF サーバが電話機の MIC を検証するには、MIC のルート証明書のコピーを持っている必要があります。このコピーがない場合、CAPF のアップグレード オプションは失敗します。

CAPF サーバが、必要な MIC のコピーを確実に入手できるようにするには、証明書を CAPF サーバに手動でインポートする必要があります。インポートする必要のある証明書の数は、ネットワーク コンフィギュレーションによって異なります。手動登録の場合は、コピー アンド ペーストまたは TFTP 転送メソッドを使用します。

証明書の登録の詳細については、ご使用の Cisco IOS リリースの『*Cisco IOS Security Configuration Guide*』の「*Configuring Certificate Enrollment for a PKI*」の章にある「*Configuring Cut-and-Paste Certificate Enrollment*」の項を参照してください。

MIC ルート証明書を手動でインポートするには、「MIC ルート証明書の手動インポート」（P.633）を参照してください。

メディア暗号化の機能設計

付属する音声セキュリティ Cisco IOS 機能によって、以下を実行できるサポート対象ネットワーク デバイス上で、セキュアなエンドツーエンドの IP テレフォニー コールを対象とした全体的なアーキテクチャが提供されます。

- セキュアな相互運用性を持つ SRTP 対応 Cisco Unified CME ネットワーク
- セキュアな Cisco IP Phone コール

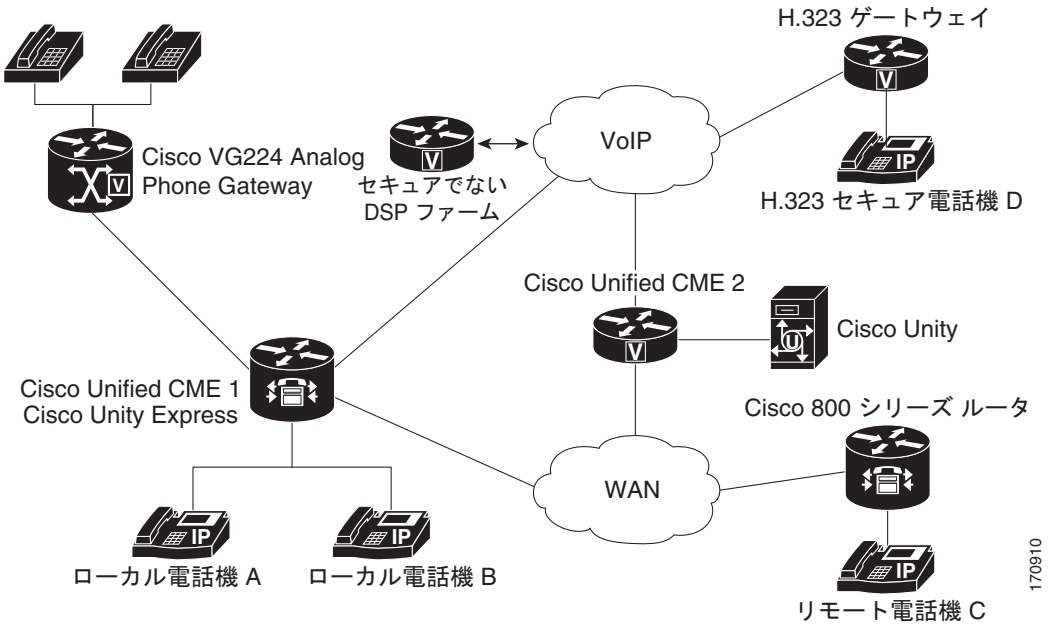
- セキュアな Cisco VG224 Analog Phone Gateway エンドポイント
- セキュアな補足サービス

これらの機能は、Cisco IOS H.323 ネットワークでメディアおよびシグナリング認証と暗号化を使用することで実装されます。H.323 は、パケット ベースのビデオ会議、音声会議、およびデータ会議を記述する ITU-T 標準であり、H.450 を含む他の標準のセットを参照して、実際のプロトコルを記述します。H.323 は、標準通信プロトコルを使用することで、異なる通信デバイスがお互いに通信できるようにし、コードの共通セット、コール セットアップおよびネゴシエーション プロシージャ、基本データ転送メソッドを定義します。H.450 は H.323 標準のコンポーネントの 1 つであり、テレフォニーのような補足サービスの提供に使用されるシグナリングとプロシージャを定義します。H.450 メッセージは H.323 ネットワークに使用され、セキュアな補足サービスのサポートが実装されます。また、メディア機能をネゴシエーションするための、空の機能セット（ECS）メッセージングも実装されます。

セキュアな Cisco Unified CME

セキュアな Cisco Unified CME ソリューションには、音声メディアに対応した、Cisco Unified CME と Cisco Unified Communications Manager の間のセキュア対応音声ポート、SCCP エンドポイント、およびセキュア H.323 トランクなどが含まれます。SIP トランクはサポートされていません。図 22 に、セキュア Cisco Unified CME システムの構成要素を示します。

図 22　　セキュア Cisco Unified CME システム



セキュア Cisco Unified CME は、セキュア チャネル用にトランスポート層セキュリティ（TLS）または IPsec（IP セキュリティ）を実装し、メディア暗号化に SRTP を使用します。セキュア Cisco Unified CME は、エンドポイントおよびゲートウェイに対する SRTP キーを管理します。

Cisco Unified CME 機能のメディア暗号化（SRTP）は、次の機能をサポートします。

- SCCP エンドポイント用の SRTP を使用するセキュア音声コール。
- 混在共有回線環境のセキュア音声コールにより、RTP と SRTP の両方でエンドポイントを使用できます。共有回線のメディア セキュリティは、エンドポイント設定に応じて異なります。

- H.450 を使用するセキュア補足サービスは次のとおりです。
  - コール自動転送
  - コール転送
  - コールの保留と復帰
  - コール パークとコール ピックアップ
  - 非セキュアなソフトウェア会議

（注） H.323 を介した STRP 電話会議では、コールが会議に参加すると、0 秒から 2 秒の間隔でノイズが発生する場合があります。

- 非 H.450 環境でのセキュアなコール。
- セキュア Cisco Unity とセキュア Cisco Unified CME の対話。
- Cisco Unity Express とセキュア Cisco Unified CME との対話（対話がサポートされ、コールは非セキュア モードにダウングレードされます）。
- DSP Farm トランスコーディングが設定された状態のリモート電話機に対するセキュアなトランスコーディング

これらの機能については、次の項で説明します。

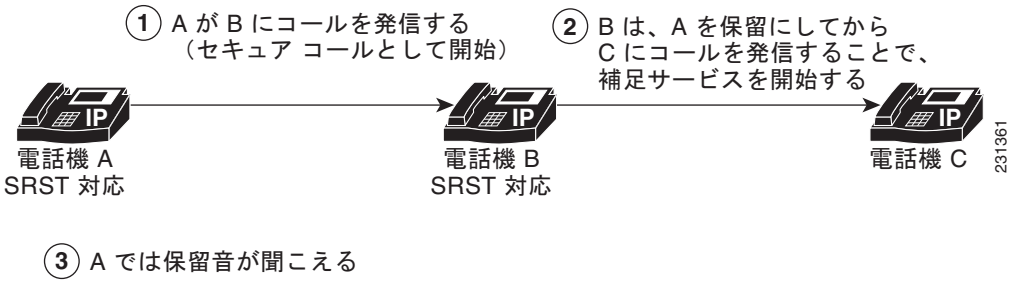
セキュアな補足サービス

メディア暗号化（SRTP）機能は、H.450 と非 H.450 の両方の Cisco Unified CME ネットワークで、セキュアな補足サービスをサポートします。セキュア Cisco Unified CME ネットワークは、H.450 または非 H.450 にする必要があり、ハイブリッドにはできません。

H.450 環境でのセキュア Cisco Unified CME

セキュアなエンドポイント間のシグナリングとメディア暗号化がサポートされており、セキュアなエンドポイント間でのコール転送（H.450.2）とコール自動転送（H.450.3）などの補足サービスが可能です。コール パークとピック アップには、H.450 メッセージが使用されます。セキュア Cisco Unified CME では、デフォルトで H.450 がイネーブルになっていますが、セキュアな保留音（MOH）とセキュアな会議（3 者間コール）はサポートされていません。たとえば、図 23 に示すように補足サービスが開始された場合、A と B との間の当初はセキュアであったコールが、ECS と端末機能セット（TCS）を使用したネゴシエーションで RTP になり、A には保留音が聞こえます。B が A へのコールを再開すると、コールは SRTP に戻ります。同様に、転送が開始されると、転送される通話者は保留状態になり、コールはネゴシエーションによって RTP になります。コールが転送されると、もう一方で SRTP を使用できる場合、コールは SRTP に戻ります。

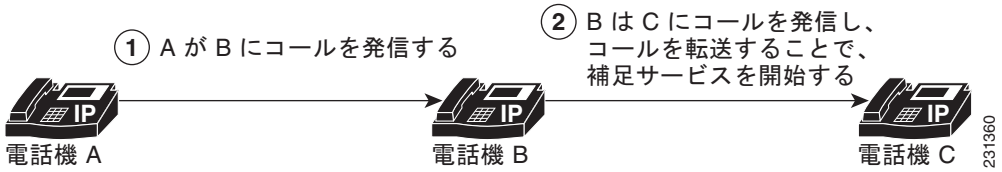
図 23　H.450 環境での保留音



非 H.450 環境でのセキュア Cisco Unified CME

補足サービスのセキュリティでは、コール中キー ネゴシエーションまたはコール中メディア再ネゴシエーションを行う必要があります。H.450 メッセージがない H.323 ネットワークでは、コーデック不一致やセキュア コールなどのシナリオでは、ECS を使用してメディア再ネゴシエーションが実装されます。ルータでグローバルに H.450 をディセーブルにすると、設定は RTP コールと SRTP コールに適用されます。シグナリング パスは、Cisco Unified CME と Cisco Unified Communications Manager の XOR によるヘアピンになります。たとえば図 24 では、シグナリング パスは A から B（補足サービスの発信者）を通って C に到達します。このシナリオで音声セキュリティを採用する場合は、メディア セキュリティ キーが XOR を通過する（転送要求を発行したエンドポイントである B を通過する）ことを考慮してください。中間者攻撃を防止するには、XOR が信頼できるエンティティになっている必要があります。

図 24　非 H.450 環境での転送



メディア パスはオプションです。Cisco Unified CME のデフォルトのメディア パスはヘアピンになっています。ただし、可能であればいつでもメディア フロー アラウンドを Cisco Unified CME に設定できます。メディア フロー スルー（デフォルト）を設定するときは、複数の XOR ゲートウェイをメディア パスでチェーン化すると、遅延が大きくなり、音声品質が低下することに注意してください。ルータ リソースと音声の品質により、チェーン化できる XOR ゲートウェイの数は制限されます。要件はプラットフォームによって異なり、シグナリングとメディアの間で変わる可能性があります。実用的なチェーン化レベルは 3 です。

コーデックの不一致があり、ECS と TCS のネゴシエーションが失敗すると、トランスコーダが挿入されます。たとえば、電話機 A と電話機 B で SRTP が使用可能であるが、電話機 A が G.711 コーデックを使用し、電話機 B が G.729 コーデックを使用している場合、電話機 B にトランスコーダがあればそれが挿入されます。ただし、コーデック要件を満たすために、コールは RTP にネゴシエーションされるため、コールは非セキュアになります。

DSP Farm トランスコーディングが設定された状態のリモート電話機に対するセキュアなトランスコーディング

dspfarm-assist キーワードを指定して **codec** コマンドが設定されたリモート電話機では、トランスコーディングがサポートされています。リモート電話機とは、Cisco Unified CME に登録され、WAN を介してリモート ロケーションに存在する電話機のことです。WAN 接続全体の帯域幅を節約するために、そのような電話機へのコールは、ephone の **codec g729r8 dspfarm assist** コマンドを設定することで、G.729r8 コーデックを使用して行うことができます。**g729r8** キーワードによって、そのような電話機へのコールは強制的に G.729 コーデックを使用するようになります。電話機への H.323 コールをトランスコードする必要がある場合、**dspfarm-assist** キーワードを使用すると、利用可能な DSP リソースを使用できるようになります。

（注） トランスコーディングは、リモートの電話機からの異なるコーデックを持つ H.323 コールが、リモートの電話機へのコールを行おうとする場合にのみイネーブルになります。リモートの電話機と同じ Cisco Unified CME 上にあるローカルの電話機がリモートの電話機にコールを行うと、ローカルの電話機はトランスコーディングを使用する代わりに、強制的にコーデックが G.729 に変更されます。

ポイント ツー ポイント SRTP コールのセキュアなトランスコーディングは、Cisco Unified CME トランスコーディングと、コールのそのピアによってサービスが提供される両方の SCCP 電話機で SRTP が使用可能であり、SRTP キーが正常にネゴシエーションされた場合にのみ行われます。ポイントツーポイント SRTP コールのセキュアなトランスコーディングは、コール内のピアの 1 つだけが SRTP に対応している場合には行えません。

Cisco Unified CME トランスコーディングをセキュアなコールで実行する場合、Cisco Unified CME 機能のメディア暗号化（SRTP）によって、Cisco Unified CME は DSP Farm に追加パラメータとしてセキュア コールの暗号キーを提供できるため、Cisco Unified CME トランスコーディングを正常に実行できます。暗号キーがないと、DSP Farm は暗号化された音声データを読み取って、それをトランスコードすることができません。

（注） ここで説明されているセキュアなトランスコーディングは、IP-IP ゲートウェイ トランスコーディングには適用されません。

Cisco Unified CME トランスコーディングは VoIP コール レッグをブリッジするためではなく、SCCP エンドポイントに対してのみ呼び出されるため、IP-to-IP ゲートウェイ トランスコーディングとは異なります。Cisco Unified CME トランスコーディングと IP-to-IP ゲートウェイ トランスコーディングは相互に排他的です。コールに対して呼び出せるのは、1 つのタイプのトランスコーディングのみです。SRTP トランスコーディングの DSP Farm 機能を使用できない場合、Cisco Unified CME のセキュアなトランスコーディングは実行されず、コールは G.711 を使用して通過します。

設定については、「セキュア モードでの Cisco Unified CME 4.2 以降のバージョンへの DSP ファームの登録」（P.480）を参照してください。

セキュア Cisco Unified CME と Cisco Unity Express

Cisco Unity Express は、セキュアなシグナリング、およびメディア暗号化をサポートしていません。セキュア Cisco Unified CME は Cisco Unity Express と相互運用できますが、Cisco Unified CME と Cisco Unity Express との間のコールはセキュアではありません。

セキュアな H.323 ネットワークでの Cisco Unified CME を使用した一般的な Cisco Unity Express 導入では、セッション開始プロトコル（SIP）がシグナリングに使用され、メディア パスは RTP による G.711 になります。応答なしのコール転送（CFNA）とすべてのコールの転送（CFA）の場合、メディア パスが確立される前に、シグナリング メッセージが送信されて、RTP メディア パスがネゴシエーションされます。コーデックのネゴシエーションが失敗すると、トランスコーダが挿入されます。Cisco Unified CME 機能の H.323 サービス プロバイダー インターフェイス（SPI）のメディア暗号化（SRTP）は、ファスト スタート コールをサポートします。通常、Cisco Unity Express から Cisco Unified CME に転送または戻されたコールは、既存のコール フローに入れられ、通常の SIP コールや RTP コールとして処理されます。

Cisco Unified CME 機能のメディア暗号化（SRTP）は、Cisco Unified CME に戻されるブラインド転送のみをサポートしています。コール中のメディア再ネゴシエーションが設定されると、H.450.2 または Empty Capability Set（ECS）のどの転送メカニズムが使用されるかに関係なく、エンドポイントのセキュア機能が再ネゴシエーションされます。

セキュア Cisco Unified CME と Cisco Unity

Cisco Unified CME 機能のメディア暗号化（SRTP）は、SCCP を使用する Cisco Unity 4.2 以降のバージョンと Cisco Unity Connection 1.1 以降のバージョンをサポートします。Cisco Unified CME のセキュア Cisco Unity は、セキュアな SCCP 電話機のように機能します。セキュアなシグナリングを確立するには、ある程度のプロビジョニングが必要です。Cisco Unity は Cisco Unified CME デバイス証明書を証明書信頼リスト（CTL）から受け取り、Cisco Unity 証明書は Cisco Unified CME に手動で挿入されます。SIP を使用した Cisco Unity はサポートされていません。

Cisco Unity Connection の証明書は、「ポート グループ設定」の下の Cisco Unity 管理 Web アプリケーションにあります。

Cisco Unified IP Phone 用の HTTPS プロビジョニング

HTTPS を使用して、Cisco Unified IP Phone で Web コンテンツに安全にアクセスする必要性が高まっています。サードパーティ Web サーバの X.509 証明書を IP Phone の CTL ファイルに保存して Web サーバを認証する必要がありますが、トラストポイント情報を入力するために使用した **server** コマンドを使用して CTL ファイルを証明書にインポートすることはできません。**server** コマンドでは、証明書チェーンの検証にサードパーティの Web サーバからの秘密キーが必要ですが、ユーザは Web サーバからその秘密キーを取得することはできないため、**import certificate** コマンドが追加されて、信頼できる証明書が CTL ファイルに追加されます。

HTTPS プロビジョニング用に、信頼できる証明書を IP Phone の CTL ファイルにインポートする方法の詳細については、「Cisco Unified IP Phone 用の HTTPS プロビジョニング」（P.644）を参照してください。

Cisco Unified CME での電話機の認証サポートについては、「電話機認証の概要」（P.591）を参照してください。

セキュリティの設定方法

ここでは、次の作業について説明します。

電話機認証

- 「Cisco IOS 認証局の設定」（P.604）（必須）

- 「サーバ機能の証明書の取得」（P.608）（必須）
- 「Telephony-Service セキュリティ パラメータの設定」（P.611）（必須）
- 「CTL クライアントの設定」（P.614）（必須）
- 「CAPF サーバの設定」（P.619）（必須）
- 「ephone のセキュリティ パラメータの設定」（P.623）（必須）
- 「CTL プロバイダーの設定」（P.626）（任意）
- 「登録局の設定」（P.629）（任意）
- 「電話機での認証文字列の入力」（P.632）（任意）
- 「MIC ルート証明書の手動インポート」（P.633）（任意）

メディア暗号化

- 「Cisco Unified CME でのメディア暗号化（SRTP）の設定」（P.636）（必須）
- 「H.323 ダイヤルピア用の Cisco Unified CME SRTP フォールバックの設定」（P.639）（任意）
- 「セキュア Cisco Unified CME 動作用の Cisco Unity の設定」（P.640）（任意）

HTTPS プロビジョニング

- 「Cisco Unified IP Phone 用の HTTPS プロビジョニング」（P.644）（任意）

Cisco IOS 認証局の設定

ローカル ルータまたは外部ルータに Cisco IOS 証明局（CA）を設定するには、次の手順を実行します。

ヒント 詳細については、『*Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment*』を参照してください。

（注） サードパーティの CA を使用している場合は、これらの手順を実行するのではなく、プロバイダーの指示に従ってください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **crypto pki server** *label*
5. **database level** {**minimal** | **names** | **complete**}
6. **database url** *root-url*
7. **lifetime certificate** *time*
8. **issuer-name CN=***label*
9. **exit**

10. **crypto pki trustpoint** *label*
11. **enrollment url** *ca-url*
12. **exit**
13. **crypto pki server** *label*
14. **grant auto**
15. **no shutdown**
16. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip http server** **例：** `Router(config)# ip http server`	ローカル Cisco Unified CME ルータで Cisco We ブラウザのユーザ インターフェイスをイネーブルにします。
ステップ 4	**crypto pki server** *label* **例：** `Router(config)# crypto pki server sanjose1`	Cisco IOS CA のラベルを定義し、証明書サーバ コンフィギュレーション モードを開始します。
ステップ 5	**database level** {**minimal** | **names** | **complete**} **例：** `Router(config-cs-server)# database level complete`	（任意）証明書登録データベースに保管されるデータのタイプを制御します。 • **minimal**：新しい証明書を、継続して問題なく発行できる程度の情報が保管されます。これがデフォルト値です。 • **names**：指定された最低限の情報以外に、各証明書のシリアル番号と件名も提供されます。 • **complete**：minimal レベルおよび names レベルで提供される情報以外に、発行済みの各証明書がデータベースに書き込まれます。このキーワードを使用する場合、**database url** コマンドを使用して、データの保存先にする外部 TFTP サーバも指定する必要があります。

	コマンドまたはアクション	目的
ステップ 6	**database url** *root-url* **例：** `Router(config-cs-server)# database url nvram:`	（任意）証明書サーバのすべてのデータベース エントリが書き出される、NVRAM 以外の場所を指定します。 • 前のステップで、**complete** キーワードを設定して **database level** コマンドを設定した場合に必要です。 • *root-url* : Cisco IOS ファイル システムでサポートされている URL。ここに、データベース エントリが書き込まれます。CA が大量の証明書を発行しようとしている場合、証明書を保存するためのフラッシュやその他のストレージ デバイスなどの適切な保存場所を選択します。 • 保存場所としてフラッシュを選択し、このデバイス上のファイル システム タイプがクラス B（LEFS）の場合は、デバイス上の空き領域を定期的にチェックし、**squeeze** コマンドを使用して、削除されたファイルが使用していた領域を解放します。このプロセスには数分かかることがあるため、このプロセスは、スケジュールされたメンテナンス期間中、またはオフピーク時に実行する必要があります。
ステップ 7	**lifetime certificate** *time* **例：** `Router(config-cs-server) lifetime certificate 888`	（任意）この Cisco IOS CA によって発行される証明書のライフタイムを日数で指定します。 • *time* : 証明書が期限切れになるまでの日数。範囲は 1 ～ 1825 日です。デフォルトは 365 です。証明書の最大のライフタイムは、CA 証明書のライフタイムよりも 1 ヵ月短い日数です。 • このコマンドは、**no shutdown** コマンドを使用して Cisco IOS CA がイネーブルになる前に設定します。
ステップ 8	**issuer-name CN=***label* **例：** `Router(config-cs-server)# issuer-name CN=sanjose1`	（任意）Cisco IOS CA の発行者名として識別名（DN）を指定します。 • デフォルトは、Cisco IOS CA に対して設定済みのラベルです。ステップ 4 を参照してください。
ステップ 9	**exit** **例：** `Router(config-cs-server)# exit`	証明書サーバ コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 10	**crypto pki trustpoint** *label* **例：** `Router(config)# crypto pki trustpoint sanjose1`	（任意）トラストポイントを宣言し、CA トラストポイント コンフィギュレーション モードを開始します。 • ローカル CA のみ。このコマンドは、外部ルータ上の Cisco IOS CA には必要ありません。 • Cisco IOS CA に特定の RSA キーを使用する必要がある場合、このコマンドを使用し、**crypto pki server** コマンドで使用するものと同じラベルを使用して独自のトラストポイントを作成します。ルータが crypto pki サーバと同じラベルを持つ設定済みのトラストポイントを認識すると、トラストポイントは自動的には作成されず、そのトラストポイントが使用されるようになります。
ステップ 11	**enrollment url** *ca-url* **例：** `Router(config-ca-trustpoint)# enrollment url http://ca-server.company.com`	発行元の Cisco IOS CA の登録 URL を指定します。 • ローカルの Cisco IOS CA に対してのみ。このコマンドは、外部ルータ上の Cisco IOS CA には必要ありません。 • *ca-url* : Cisco IOS CA がインストールされているルータの URL。
ステップ 12	**exit** **例：** `Router(config-ca-trustpoint)# exit`	CA 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 13	**crypto pki server** *label* **例：** `Router(config)# crypto pki server sanjose1`	証明書サーバ コンフィギュレーション モードを開始します。 • *label* : 設定される Cisco IOS CA の名前。
ステップ 14	**grant auto** **例：** `Router(config-cs-server)# grant auto`	（任意）すべての要求者に対して証明書が自動的に発行されるようにします。 • デフォルトで推奨される方法は、手動登録です。 • このコマンドは、簡易ネットワークのテストおよび構築中にのみ使用してください。設定の後に **no grant auto** コマンドを使用すると、証明書が自動的に付与されないように設定されます。
ステップ 15	**no shutdown** **例：** `Router(config-cs-server)# no shutdown`	（任意）Cisco IOS CA をイネーブルにします。 • このコマンドは、Cisco IOS CA の設定を完了した後にのみ使用してください。
ステップ 16	**end** **例：** `Router(config-cs-server)# end`	特権 EXEC モードに戻ります。

例

次の **show running-config** コマンドからの部分出力は、ローカルの Cisco Unified CME ルータで実行している「sanjose1」という名前の Cisco IOS CA に対する設定を示しています。

```
ip http server

crypto pki server sanjose1
 database level complete
 database url nvram:

crypto pki trustpoint sanjose1
 enrollment url http://ca-server.company.com

crypto pki server authority1
 no grant auto
 no shutdown
```

サーバ機能の証明書の取得

CA は、次のサーバ機能の証明書を発行します。

- Cisco Unified CME：電話機を含む TLS セッションに証明書が必要です。
- TFTP：コンフィギュレーション ファイルの署名にキー ペアと証明書が必要です。
- HTFTP：コンフィギュレーション ファイルの署名にキー ペアと証明書が必要です。
- CAPF：電話機を含む TLS セッションに証明書が必要です。
- SAST：CTL ファイルの署名に必要です。2 つの SAST 証明書を作成して、1 つはプライマリとして使用し、もう 1 つはバックアップ用にすることを推奨します。

サーバ機能の証明書を入手するには、サーバ機能ごとに次の手順を実行します。

（注） サーバ機能ごとに異なるトラストポイントを設定できます（「例」（P.610）を参照）。または、「セキュリティの設定例」（P.649）と、このモジュールの最後に記載されているように、複数のサーバ機能に対して同じトラストポイントを設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *trustpoint-label*
4. **enrollment url** *url*
5. **revocation-check** *method1* [*method2* [*method3*]]
6. **rsakeypair** *key-label* [*key-size* [*encryption-key-size*]]
7. **exit**
8. **crypto pki authenticate** *trustpoint-label*
9. **crypto pki enroll** *trustpoint-label*
10. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki trustpoint** *trustpoint-label* **例：** `Router(config)# crypto pki trustpoint capf`	CA で使用する必要のあるトラストポイントを宣言し、CA トラストポイント コンフィギュレーション モードを開始します。 • *trustpoint-label*: 設定されるサーバ機能のラベル。
ステップ 4	**enrollment url** *url* **例：** `Router(config-ca-trustpoint)# enrollment url http://ca-server.company.com`	発行元の CA の登録 URL を指定します。 • *url*：発行元の CA がインストールされたルータの URL。
ステップ 5	**revocation-check** *method1* [*method2* [*method3*]] **例：** `Router(config-ca-trustpoint)# revocation-check none`	（任意）証明書の失効ステータスを確認するために使用する方法を指定します。 • *method*：2 番めと 3 番めの方法を指定した場合、これに続く方法はその直前の方法でエラーが返された場合（サーバがダウンしている場合など）にだけ使用されます。 – **crl**：証明書のチェックは、証明書失効リスト（CRL）によって実行されます。これはデフォルトの動作です。 – **none**：証明書のチェックは不要です。 – **ocsp**：証明書のチェックは、Online Certificate Status Protocol（OCSP）サーバによって実行されます。
ステップ 6	**rsakeypair** *key-label* [*key-size* [*encryption-key-size*]] **例：** `Router(config-ca-trustpoint)# rsakeypair capf 1024 1024`	（任意）証明書で使用するキー ペアを指定します。 • *key-label*：キー ペアの名前がまだ存在しない場合、または **auto-enroll regenerate** コマンドが設定されている場合、登録時に生成されるキー ペアの名前。 • *key-size*：目的の RSA キーのサイズ。指定されなかった場合は、既存のキー サイズが使用されます。 • *encryption-key-size*：個別の暗号化、署名キー、および証明書を要求するために使用される 2 番めのキーのサイズ。 • 複数のトラストポイントで同じキーを共有できます。

	コマンドまたはアクション	目的
ステップ 7	**exit** **例：** `Router(config-ca-trustpoint)# exit`	CA 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 8	**crypto pki authenticate** *trustpoint-label* **例：** `Router(config)# crypto pki authenticate capf`	CA 証明書を取得して認証し、プロンプトが表示された場合は、証明書のフィンガープリントを確認します。 • CA 証明書がコンフィギュレーションにすでにロードされている場合、このコマンドはオプションです • *trustpoint-label*：設定されるサーバ機能にすでに設定されているラベル。
ステップ 9	**crypto pki enroll** trustpoint-label **例：** `Router(config)# crypto pki enroll capf`	CA に登録し、このトランスポイントの証明書を取得します。 • *trustpoint-label*：設定されるサーバ機能にすでに設定されているラベル。
ステップ 10	**exit** **例：** `Router(config)# exit`	特権 EXEC モードに戻ります。

例

次の **show running-config** コマンドの出力の一部は、さまざまなサーバ機能の証明書を取得する方法を示しています。

CAPF サーバ機能の証明書の取得

```
!configuring a trust point
 crypto pki trustpoint capf-server
 enrollment url http://192.168.1.1:80
 revocation-check none
!authenticate w/ the CA and download its certificate
crypto pki authenticate capf-server
! enroll with the CA and obtain this trustpoint's certificate
 crypto pki enroll capf-server
```

Cisco Unified CME サーバ機能の証明書の取得：

```
crypto pki trustpoint cme-server
 enrollment url http://192.168.1.1:80
 revocation-check none

crypto pki authenticate cme-server
crypto pki enroll cme-server
```

TFTP サーバ機能の証明書の取得：

```
crypto pki trustpoint tftp-server
 enrollment url http://192.168.1.1:80
 revocation-check none

crypto pki authenticate tftp-server
crypto pki enroll tftp-server
```

最初の SAST サーバ機能（sast1）の証明書の取得：

```
crypto pki trustpoint sast1
 enrollment url http://192.168.1.1:80
 revocation-check none

crypto pki authenticate sast1
crypto pki enroll sast1
```

2 番めの SAST サーバ機能（sast2）の証明書の取得：

```
crypto pki trustpoint sast2
 enrollment url http://192.168.1.1:80
 revocation-check none

crypto pki authenticate sast2
crypto pki enroll sast2
```

Telephony-Service セキュリティ パラメータの設定

テレフォニー サービスのセキュリティ パラメータを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **secure-signaling trustpoint** *label*
5. **tftp-server-credentials trustpoint** *label*
6. **device-security-mode** {**authenticated** | **none** | **encrypted**}
7. **cnf-file perphone**
8. **load-cfg-file** *file-url* **alias** *file-alias* [**sign**] [**create**]
9. **server-security-mode** {**erase** | **non-secure** | **secure**}
10. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**telephony-service** **例：** `Router(config)# telephony-service`	telephony-service コンフィギュレーション モードを開始します。
ステップ 4	**secure-signaling trustpoint** *label* **例：** `Router(config-telephony)# secure-signaling trustpoint cme-sccp`	セキュリティ シグナリングに使用するトラストポイントを設定します。 • *label* : TCP ポート 2443 で IP Phone との TLS ハンドシェイクに使用される有効な証明書を持つ、設定済みの PKI トラストポイントの名前。
ステップ 5	**tftp-server-credentials trustpoint** *label* **例：** `Router(config-telephony)# tftp-server-credentials trustpoint cme-tftp`	コンフィギュレーション ファイルの署名に使用する TFTP サーバ クレデンシャル（トラストポイント）を設定します。 • *label* : 電話機のコンフィギュレーション ファイルの署名に使用される有効な証明書を持つ、設定済みの PKI トラストポイントの名前。これは、前のステップで使用した CAPF トラストポイントにすることも、有効な証明書を持ついずれかのトラストポイントにすることもできます。
ステップ 6	**device-security-mode** {**authenticated** | **none** | **encrypted**} **例：** `Router(config-telephony)# device-security-mode authenticated`	エンドポイントのセキュリティ モードをイネーブルにします。 • **authenticated** : 暗号化なしで TLS 接続を確立するようにデバイスに指示します。メディア パスにセキュアな Real-Time Transport Protocol（SRTP）がありません。 • **none** : SCCP シグナリングはセキュアではありません。これがデフォルトです。 • **encrypted** : デバイスに、SRTP を使用してセキュアなメディア パスへの暗号化された TLS 接続を確立するように指示します。 • このコマンドは、ephone コンフィギュレーション モードでも設定できます。ephone コンフィギュレーション モードで設定された値は、telephony-service コンフィギュレーション モードで設定された値よりも優先されます。

	コマンドまたはアクション	目的
ステップ 7	**cnf-file perphone** **例：** `Router(config-telephony)# cnf-file perphone`	システムで各 IP 電話に個別の設定 XML ファイルを生成することを指定します。 • セキュリティのために、各エンドポイントに個別のコンフィギュレーション ファイルが必要です。
ステップ 8	**load-cfg-file** *file-url* **alias** *file-alias* [**sign**] [**create**] **例：** `Router(config-telephony)# load-cfg-file slot0:Ringlist.xml alias Ringlist.xml sign create`	（任意）Cisco Unified CME で作成されたものではないコンフィギュレーション ファイルに署名します。また、ファイルの署名付きバージョンと、署名なしバージョンを TFTP サーバにロードします。 • *file-url*：ローカル ディレクトリでコンフィギュレーション ファイルのパスを完成させます。 • **alias** *file-alias*：TFTP サーバに保存されるファイルのエイリアス。 • **sign**：（任意）ファイルはデジタル署名されて、TFTP サーバに保存される必要があります。 • **create**：（任意）ローカル ディレクトリに署名済みファイルを作成します。 • 各ファイルに対してこのコマンドを最初に使用する場合は、**create** キーワードと **sign** キーワードを使用します。キーワードは、署名済みのファイルがリロードのたびに再作成されないように、**create** キーワードは実行中の設定には保持されません。 • すでに署名されているファイルを TFTP サーバに保存するには、**create** キーワードと **sign** キーワードなしでこのコマンドを使用します。
ステップ 9	**server-security-mode** {**erase** | **non-secure** | **secure**} **例：** `Router(config-telephony)# server-security-mode non-secure`	（任意）サーバのセキュリティ モードを変更します。 • **erase**：CTL ファイルを削除します。 • **non-secure**：非セキュア モード。 • **secure**：セキュア モード。 • CTL ファイルが CTL クライアントによって最初に生成されるまで、このコマンドは効果がありません。CTL ファイルが生成されると、CTL クライアントは自動的にサーバのセキュリティ モードをセキュアに設定します。
ステップ 10	**end** **例：** `Router(config-ephone)# end`	特権 EXEC モードに戻ります。

Telephony-Service セキュリティ パラメータの確認

ステップ 1 **show telephony-service security-info**

このコマンドを使用して、telephony-service コンフィギュレーション モードに設定されているセキュリティ関連情報を表示します。

```
Router# show telephony-service security-info

Skinny Server Trustpoint for TLS: cme-sccp
TFTP Credentials Trustpoint: cme-tftp
Server Security Mode: Secure
Global Device Security Mode: Authenticated
```

ステップ 2 **show running-config**

このコマンドを使用して、実行コンフィギュレーションを表示し、テレフォニーおよび電話機ごとのセキュリティ設定を確認します。

```
Router# show running-config

telephony-service
 secure-signaling trustpoint cme-sccp
 server-security-mode secure
 device-security-mode authenticated
 tftp-server-credentials trustpoint cme-tftp
.
.
.
```

CTL クライアントの設定

実際のネットワーク コンフィギュレーションに応じて、次のタスクのいずれかを実行します。

- 「Cisco Unified CME ルータでの CTL クライアントの設定」（P.614）
- 「Cisco Unified CME ルータ以外のルータでの CTL クライアントの設定」（P.617）

Cisco Unified CME ルータでの CTL クライアントの設定

ローカルの Cisco Unified CME ルータ上に既知の信頼できる証明書とトークンのリストが作成されるように CTL クライアントを設定するには、次の手順を実行します。

（注） プライマリとセカンダリの Cisco Unified CME ルータがある場合は、そのどちらかに CTL クライアントを設定できます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ctl-client**
4. **sast1 trustpoint** *label*
5. **sast2 trustpoint** *label*

6. **server** {**capf** | **cme** | **cme-tftp** | **tftp**} *ip-address* **trustpoint** *trustpoint-label*
7. **server cme** *ip-address* **username** *name-string* **password** {**0** | **1**} *password-string*
8. **regenerate**
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ctl-client** **例：** `Router(config)# ctl-client`	CTL-client コンフィギュレーション モードを開始します。
ステップ 4	**sast1 trustpoint** *label* **例：** `Router(config-ctl-client)# sast1 trustpoint sast1tp`	プライマリ SAST のクレデンシャルを設定します。 • *label* : SAST1 トラストポイントの名前。 **（注）** SAST1 証明書と SAST2 証明書は、互いに異なるものにする必要があります。CTL ファイルは常に SAST1 によって署名されます。SAST2 証明書は CTL ファイルに含まれるため、SAST1 証明書が破損した場合、SAST2 でファイルを署名することで、電話機が工場出荷時のデフォルト設定にリセットされることを防止できます。
ステップ 5	**sast2 trustpoint** *label* **例：** `Router(config-ctl-client)# sast2 trustpoint`	セカンダリ SAST のクレデンシャルを設定します。 • *label* : SAST2 トラストポイントの名前。 **（注）** SAST1 証明書と SAST2 証明書は、互いに異なるものにする必要があります。CTL ファイルは常に SAST1 によって署名されます。SAST2 証明書は CTL ファイルに含まれるため、SAST1 証明書が破損した場合、SAST2 でファイルを署名することで、電話機が工場出荷時のデフォルト設定にリセットされることを防止できます。

	コマンドまたはアクション	目的
ステップ 6	**server** {**capf** | **cme** | **cme-tftp** | **tftp**} *ip-address* **trustpoint** *trustpoint-label* **例：** `Router(config-ctl-client)# server capf 10.2.2.2 trustpoint capftp`	Cisco Unified CME ルータでローカルに実行しているサーバ機能ごとにトラストポイントを設定します。 • *ip-address*：Cisco Unified CME ルータの IP アドレス。複数のネットワーク インターフェイスがある場合、電話機が接続されているローカル LAN のインターフェイス アドレスを使用します。 • **trustpoint** *trustpoint-label*：設定されるサーバ機能の PKI トラストポイントの名前。 • Cisco Unified CME ルータでローカルに実行しているサーバ機能ごとに、このコマンドを繰り返します。
ステップ 7	**server cme** *ip-address* **username** *name-string* **password** {**0** | **1**} *password-string* **例：** `Router(config-ctl-client)# server cme 10.2.2.2 username user3 password 0 38h2KL`	（任意）ネットワーク上の別の Cisco Unified CME ルータ（プライマリまたはセカンダリ）についての情報を提供します。 • *ip-address*：他の Cisco Unified CME ルータの IP アドレス。 • **username** *name-string*：CTL プロバイダーに設定されるユーザ名。 • **password**：ユーザがパスワードを入力する方法ではなく、**show** コマンド出力でパスワードが表示される方法を定義します。 – **0**：暗号化なし。 – **1**：メッセージ ダイジェスト 5（MD5）を使用した暗号化。 • *password-string*：リモートの Cisco Unified CME ルータで実行している CTL プロバイダーの管理パスワード。
ステップ 8	**regenerate** **例：** `Router(config-ctl-client)# regenerate`	CTL クライアント コンフィギュレーションに変更を行った後に、新しい CTLFile.tlv を作成します。
ステップ 9	**end** **例：** `Router(config-ctl-client)# end`	特権 EXEC モードに戻ります。

例

次の **show ctl-client** コマンドの出力例は、システムのトラストポイントを示しています。

```
Router# show ctl-client

CTL Client Information
------------------------------
        SAST 1 Certificate Trustpoint: cmeserver
        SAST 1 Certificate Trustpoint: sast2
        List of Trusted Servers in the CTL
                CME     10.1.1.1        cmeserver
                TFTP    10.1.1.1        cmeserver
```

```
CAPF    10.1.1.1        cmeserver
```

次の作業

これで、CTL クライアントの設定は終わりました。「CAPF サーバの設定」（P.619）を参照してください。

Cisco Unified CME ルータ以外のルータでの CTL クライアントの設定

Cisco Unified CME ルータ以外のスタンドアロン ルータで CTL クライアントを設定するには、以下の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ctl-client**
4. **sast1 trustpoint** *label*
5. **sast2 trustpoint** *label*
6. **server cme** *ip-address* **username** *name-string* **password** {**0** | **1**} *password-string*
7. **regenerate**
8. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ctl-client** **例：** `Router(config)# ctl-client`	CTL-client コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**sast1 trustpoint** *label* **例：** `Router(config-ctl-client)# sast1 trustpoint sast1tp`	プライマリ SAST のクレデンシャルを設定します。 • *label*：SAST1 トラストポイントの名前。 **（注）** SAST1 証明書と SAST2 証明書は互いに異なっている必要がありますが、どちらかに Cisco Unified CME ルータと同じ証明書を使用すると、メモリを節約できます。CTL ファイルは常に SAST1 によって署名されます。SAST2 証明書は CTL ファイルに含まれるため、SAST1 証明書が破損した場合、SAST2 でファイルを署名することで、電話機が工場出荷時のデフォルト設定にリセットされることを防止できます。
ステップ 5	**sast2 trustpoint** *label* **例：** `Router(config-ctl-client)# sast2 trustpoint`	セカンダリ SAST のクレデンシャルを設定します。 • *label*：SAST2 トラストポイントの名前。 **（注）** SAST1 証明書と SAST2 証明書は互いに異なっている必要がありますが、どちらかに Cisco Unified CME ルータと同じ証明書を使用すると、メモリを節約できます。CTL ファイルは常に SAST1 によって署名されます。SAST2 証明書は CTL ファイルに含まれるため、SAST1 証明書が破損した場合、SAST2 でファイルを署名することで、電話機が工場出荷時のデフォルト設定にリセットされることを防止できます。
ステップ 6	**server cme** *ip-address* **username** *name-string* **password** {**0** | **1**} *password-string* **例：** `Router(config-ctl-client)# server cme 10.2.2.2 username user3 password 0 38h2KL`	（任意）存在する場合は、ネットワーク上の別の Cisco Unified CME ルータ（プライマリまたはセカンダリ）に関する情報を提供します。 • *ip-address*：他の Cisco Unified CME ルータの IP アドレス。 • **username** *name-string*：CTL プロバイダーに設定されるユーザ名。 • **password**：パスワード文字列の暗号化ステータス。 – **0**：暗号化なし。 – **1**：メッセージ ダイジェスト 5（MD5）を使用した暗号化。 **（注）** このオプションは、show コマンド出力でパスワードが表示される方法に関するものであり、このコマンドにパスワードを入力する方法に関するものではありません。 • *password-string*：リモートの Cisco Unified CME ルータで実行している CTL プロバイダーの管理パスワード。

	コマンドまたはアクション	目的
ステップ 7	**regenerate** **例：** `Router(config-ctl-client)# regenerate`	CTL クライアント コンフィギュレーションに変更を行った後に、新しい CTLFile.tlv を作成します。
ステップ 8	**end** **例：** `Router(config-ctl-client)# end`	特権 EXEC モードに戻ります。

例

次の **show ctl-client** コマンドの出力例は、システムのトラストポイントを示しています。

```
Router# show ctl-client

CTL Client Information
---------------------------
        SAST 1 Certificate Trustpoint: cmeserver
        SAST 1 Certificate Trustpoint: sast2
        List of Trusted Servers in the CTL
                CME     10.1.1.1        cmeserver
                TFTP    10.1.1.1        cmeserver
                CAPF    10.1.1.1        cmeserver
```

CAPF サーバの設定

証明書動作中に電話機と TLS セッションを確立できるように、CAPF サーバ用に証明書を入手する必要があります。CAPF サーバは、セキュリティがイネーブルになっている電話機で、ローカルで有効な証明書（LSC）をインストール、フェッチ、または削除できます。Cisco Unified CME ルータで CAPF をイネーブルにするには、次の手順を実行します。

ヒント 電話機の証明書をインストールするために CAPF サーバを使用する場合、メンテナンスのスケジュールされた期間内にそれを行うように準備します。同時に多数の証明書を生成すると、コール処理が中断される場合があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **capf-server**
4. **trustpoint-label** *label*
5. **cert-enroll-trustpoint** *label* **password** {**0** | **1**} *password-string*
6. **source-addr** *ip-address*
7. **auth-mode** {**auth-string** | **LSC** | **MIC** | **none** | **null-string**}
8. **auth-string** {**delete** | **generate**} {**all** | *ephone-tag*} [*digit-string*]
9. **phone-key-size** {**512** | **1024** | **2048**}

10. **port** *tcp-port*
11. **keygen-retry** *number*
12. **keygen-timeout** *minutes*
13. **cert-oper** {**delete all** | **fetch all** | **upgrade all**}
14. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**capf-server** **例：** `Router(config)# capf-server`	capf-server コンフィギュレーション モードを開始します。
ステップ 4	**trustpoint-label** *label* **例：** `Router(config-capf-server)# trustpoint-label tp1`	トラストポイントのラベルを指定します。 • *label*：CAPF サーバと電話機の間の TLS 接続に証明書が使用されるトラストポイントの名前。
ステップ 5	**cert-enroll-trustpoint** *label* **password** {**0** | **1**} *password-string* **例：** `Router(config-capf-server)# cert-enroll-trustpoint ra1 password 0 x8oWiet`	CA を使用して CAPF を登録します（CA が Cisco Unified CME ルータに対してローカルではない場合は RA）。 • *label*：グローバル コンフィギュレーション モードで **crypto pki trustpoint** コマンドを使用して、以前に設定された CA と RA の PKI トラストポイント ラベル。 • **password**：パスワード文字列の暗号化ステータス。 • *password-string*：証明書の登録に使用するパスワード。このパスワードは、CA への証明書要求とともに送信される失効パスワードです。
ステップ 6	**source-addr** *ip-address* **例：** `Router(config-capf-server)# source addr 10.10.10.1`	Cisco Unified CME ルータで、CAPF サーバの IP アドレスを定義します。

	コマンドまたはアクション	目的
ステップ 7	**auth-mode** {**auth-string** | **LSC** | **MIC** | **none** | **null-string**} **例：** `Router(config-capf-server)# auth-mode auth-string`	証明書を要求するエンドポイントを確認するための、CAPF セッションの認証モードのタイプを指定します。 • **auth-string**：電話機ユーザは、電話機で特別な認証文字列を入力します。この文字列は、システム管理者によってユーザに提供され、**auth-string generate** コマンドを使用して設定されます。 • **LSC**：存在する場合、電話機は認証用の LSC を提供します。 • **MIC**：存在する場合、電話機は認証用の MIC を提供します。このオプションを選択した場合、MIC のユーザ証明書を PKI トラストポイントにインポートする必要があります。 • **none**：証明書のアップグレードは開始されません。これがデフォルトです。 • **null-string**：認証は行われません。
ステップ 8	**auth-string** {**delete** | **generate**} {**all** | *ephone-tag*} [*digit-string*] **例：** `Router(config-capf-server)# auth-string generate all`	（任意）1 台またはすべてのセキュアな電話機用の認証文字列を作成または削除します。 • 前のステップで **auth-string** キーワードが指定されている場合は、このコマンドを使用します。文字列は ephone コンフィギュレーションの一部になります。 • **delete**：指定したセキュアなデバイスの認証文字列を削除します。 • **generate**：指定したセキュアなデバイスの認証文字列を作成します。 • **all**：すべての電話機。 • *ephone-tag*：認証文字列を受け取るための ephone の ID。 • *digit-string*：CAPF 認証を行うために電話機ユーザがダイヤルする必要のある番号。文字列の長さは、キーパッドで押すことができる 4 ～ 10 桁です。この値を指定しなかった場合は、電話機ごとにランダムな文字列が生成されます。 • ephone コンフィギュレーション モードで **capf-auth-str** コマンドを使用して、個々の SCCP IP Phone の認証文字列を定義することもできます。
ステップ 9	**phone-key-size** {**512** | **1024** | **2048**} **例：** `Router(config-capf-server)# phone-key-size 2048`	（任意）電話機の証明書用に電話機に生成される RSA キーペアのサイズをバイト単位で指定します。 • **512**：512。 • **1024**：1024。これがデフォルトです。 • **2048**：2048。
ステップ 10	**port** *tcp-port* **例：** `Router(config-capf-server)# port 3804`	（任意）CAPF サーバが電話機からのソケット接続をリッスンする対象となる TCP ポート番号を定義します。 • *tcp-port*：TCP ポート番号。範囲は 2000 ～ 9999 です。デフォルトは 3804 です。

	コマンドまたはアクション	目的
ステップ 11	**keygen-retry** *number* **例：** `Router(config-capf-server)# keygen-retry 5`	（任意）サーバがキー生成要求を送信する回数を指定します。 • *number*：再試行回数。範囲は 0 ～ 100 です。デフォルトは 3 です。
ステップ 12	**keygen-timeout** *minutes* **例：** `Router(config-capf-server)# keygen-timeout 45`	（任意）サーバが電話機からのキー生成応答を待機する時間を指定します。 • *minutes*：生成プロセスがタイムアウトになるまでの時間（分単位）。範囲は 1 ～ 120 です。デフォルトは 30 です。
ステップ 13	**cert-oper** {**delete all** | **fetch all** | **upgrade all**} **例：** `Router(config-capf-server)# cert-oper upgrade all`	（任意）システム上のすべての設定済みエンドポイントで、示されている証明書の操作を開始します。 • **delete all**：すべての電話機証明書を削除します。 • **fetch all**：トラブルシューティング用にすべての電話機証明書を取得します。 • **upgrade all**：すべての電話機証明書をアップグレードします。 • このコマンドを ephone コンフィギュレーション モードで設定して、個々の電話機で証明書の操作を開始することもできます。ephone コンフィギュレーション モードでのこのコマンドは、CAPF サーバ コンフィギュレーション モードでのこのコマンドよりも優先されます。
ステップ 14	**end** **例：** `Router(config-capf-server)# end`	特権 EXEC モードに戻ります。

CAPF サーバの確認

show capf-server summary コマンドを使用して、CAPF サーバのコンフィギュレーション情報を表示します。

```
Router# show capf-server summary

CAPF Server Configuration Details
        Trustpoint for TLS With Phone: tp1
        Trustpoint for CA operation: ra1
        Source Address: 10.10.10.1
        Listening Port: 3804
        Phone Key Size: 1024
        Phone KeyGen Retries: 3
        Phone KeyGen Timeout: 30 minutes
```

ephone のセキュリティ パラメータの設定

個々の電話機にセキュリティ パラメータを設定するには、次の手順を実行します。

前提条件

- セキュリティ用に設定する電話機が、Cisco Unified CME で基本コール用に設定されていること。設定については、「基本的なコール発信のための電話機の設定」（P.191）を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **ephone** *phone-tag*
4. **device-security-mode** {**authenticated** | **none** | **encrypted**}
5. **codec** {**g711ulaw** | **g722r64** | **g729r8** [**dspfarm-assist**]}
6. **capf-auth-str** *digit-string*
7. **cert-oper** {**delete** | **fetch** | **upgrade**} **auth-mode** {**auth-string** | **LSC** | **MIC** | **null-string**}
8. **reset**
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ephone** *phone-tag* **例：** `Router(config)# ephone 24`	ephone コンフィギュレーション モードを開始します。 • *phone-tag*：設定する電話機の固有識別子。

	コマンドまたはアクション	目的
ステップ 4	**device-security-mode** {**authenticated** | **none** | **encrypted**} **例：** `Router(config-ephone)# device-security-mode authenticated`	（任意）個々の SCCP IP 電話機のセキュリティ モードをイネーブルにします。 • **authenticated**：暗号化なしで TLS 接続を確立するようにデバイスに指示します。メディア パスにセキュアな Real-Time Transport Protocol（SRTP）がありません。 • **none**：SCCP シグナリングはセキュアではありません。これがデフォルトです。 • **encrypted**：デバイスに、SRTP を使用してセキュアなメディア パスへの暗号化された TLS 接続を確立するように指示します。 • このコマンドは、telephony-service コンフィギュレーション モードでも設定できます。ephone コンフィギュレーション モードで設定された値は、telephony-service コンフィギュレーション モードで設定された値よりも優先されます。
ステップ 5	**codec** {**g711ulaw** | **g722r64** | **g729r8** [**dspfarm-assist**]} **例：** `Router(config-ephone)# codec g711ulaw dspfarm-assist`	（任意）Cisco Unified CME ルータと通信している電話機の SCCP シグナリングにセキュリティ モードを設定します。 • **dspfarm-assist**：Cisco Unified CME を使用したセキュアなトランスコーディングに必要です。コールに対して G.711 がネゴシエーションされた場合、電話機と Cisco Unified CME ルータの間のセグメントをトランスコードするために、システムが DSP ファーム リソースを使用しようとします。SCCP エンドポイント タイプが ATA、VG224、または VG248 の場合、キーワードは無視されます。
ステップ 6	**capf-auth-str** *digit-string* **例：** `Router(config-ephone)# capf-auth-str 2734`	（任意）CAPF 認証の Personal Identification Number（PIN）として使用する文字列を定義します。 **（注）** 電話機に文字列を入力する方法の詳細については、「電話機での認証文字列の入力」（P.632）を参照してください。 • *digit-string*：CAPF 認証を行うために電話機ユーザがダイヤルする必要のある番号。文字列の長さは 4 ～ 10 桁です。 • このコマンドは、telephony-service コンフィギュレーション モードでも設定できます。ephone コンフィギュレーション モードで設定された値は、telephony-service コンフィギュレーション モードで設定された値よりも優先されます。 • CAPF サーバ コンフィギュレーション モードで **auth-string** コマンドを使用して、CAPF 認証用の PIN を定義することもできます。

	コマンドまたはアクション	目的
ステップ 7	**cert-oper** {**delete** | **fetch** | **upgrade**} **auth-mode** {**auth-string** | **LSC** | **MIC** | **null-string**} **例：** `Router(config-ephone)# cert-oper upgrade auth-mode auth-string`	（任意）設定する ephone で、示された証明書の操作を開始します。 • **delete**：電話機の証明書を削除します。 • **fetch**：トラブルシューティング用に、電話機の証明書を取得します。 • **upgrade**：電話機の証明書をアップグレードします。 • **auth-mode**：証明書を要求するエンドポイントを確認するために CAPF セッション中に使用する認証のタイプ。 • **auth-string**：電話機ユーザが電話機に入力する認証文字列。auth-string は、**capf-auth-str** コマンドを使用して設定します。設定については、「電話機での認証文字列の入力」（P.632）を参照してください。 • **LSC**：認証用の電話機証明書をその電話機が提供します。LSC が存在する場合は、LSC が優先されます。 • **MIC**：認証用の電話機証明書をその電話機が提供します。MIC が存在する場合は、MIC が優先されます。MIC のユーザ証明書を PKI トラストポイントにインポートする必要があります。詳細については、「MIC ルート証明書の手動インポート」（P.633）を参照してください。 • **null-string**：認証は行われません。 • このコマンドを CAPF サーバ コンフィギュレーション モードで設定して、グローバル レベルで認証動作を開始することもできます。ephone コンフィギュレーション モードでのこのコマンドは、CAPF サーバ コンフィギュレーション モードでのこのコマンドよりも優先されます。 • CAPF サーバ コンフィギュレーション モードで **auth-mode** コマンドを使用して、グローバル レベルで認証を設定することもできます。
ステップ 8	**reset** **例：** `Router(config-ephone)# reset`	電話機の完全なリブートを実行します。
ステップ 9	**end** **例：** `Router(config-ephone)# end`	特権 EXEC モードに戻ります。

ephone のセキュリティ パラメータの確認

show capf-server auth-string コマンドを使用して、CAPF 認証を確立するためにユーザが電話機に入力する設定済みの認証文字列（PIN）を表示します。

```
Router# show capf-server auth-string

Authentication Strings for configured Ephones
Mac-Addr        Auth-String
--------        -----------
000CCE3A817C    2734
001121116BDD    922
000D299D50DF    9182
000ED7B10DAC    3114
000F90485077    3328
0013C352E7F1    0678
```

次の作業

- ネットワーク上に複数の Cisco Unified CME ルータがある場合、CTL クライアントを実行していない各 Cisco Unified CME ルータに CTL プロバイダーを設定する必要があります。CTL クライアントが実行していない各 Cisco Unified CME ルータに CTL プロバイダーを設定するには、「CTL プロバイダーの設定」（P.626）を参照してください。
- CA がサードパーティ CA であるか、Cisco IOS CA が Cisco Unified CME ルータの外部にある Cisco IOS ルータにある場合、RA を設定して電話機に証明書を発行する必要があります。詳細については、「登録局の設定」（P.629）を参照してください
- CAPF セッションに指定した認証モードが認証文字列である場合、更新された LSC を受け取る各電話機に認証文字列を入力する必要があります。詳細については、「電話機での認証文字列の入力」（P.632）を参照してください。
- CAPF セッションに指定した認証モードが MIC である場合、MIC の発行者証明書が PKI トラストポイントにインポートされる必要があります。詳細については、「MIC ルート証明書の手動インポート」（P.633）を参照してください。
- メディア暗号化の設定方法については、「Cisco Unified CME でのメディア暗号化（SRTP）の設定」（P.636）を参照してください。

CTL プロバイダーの設定

ネットワーク上に複数の Cisco Unified CME ルータがある場合、CTL クライアントを実行していない各 Cisco Unified CME ルータに CTL プロバイダーを設定する必要があります。CTL クライアントが実行していない各 Cisco Unified CME ルータに CTL プロバイダーを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **credentials**
4. **ip source-address** *ip-address* **port** *port-number*
5. **trustpoint** *trustpoint-label*
6. **ctl-service admin** *username* **secret** {**0** | **1**} *password-string*
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**credentials** **例：** `Router(config)# credentials`	クレデンシャル インターフェイス モードを開始して、CTL プロバイダーを設定します。
ステップ 4	**ip source-address** [*ip-address* [**port** [*port-number*]]] **例：** `Router(config-credentials)# ip source-address 172.19.245.1 port 2444`	この CTL プロバイダーが設定されるローカル ルータを識別します。 • *ip-address*：通常は、ルータのイーサネット ポートのアドレスの 1 つ。 • **port** *port-number*：クレデンシャル サービス通信用の TCP ポート。デフォルトは 2444 です。デフォルト値を使用することを推奨します。
ステップ 5	**trustpoint** *trustpoint-label* **例：** `Router(config-credentials)# trustpoint ctlpv`	トラストポイントを設定します。 • *trustpoint-label*：CTL クライアントで TLS セッションに使用される CTL プロバイダー トラストポイントの名前。

	コマンドまたはアクション	目的
ステップ 6	**ctl-service admin** *username* **secret** {**0** | **1**} *password-string* **例：** `Router(config-credentials)# ctl-service admin user4 secret 0 c89L8o`	CTL プロトコルの間にクレデンシャルを取得するために接続する場合に、CTL クライアントを認証するユーザ名とパスワードを指定します。 • *username*：クライアントの認証に使用される名前。 • **secret**：ログイン認証用の文字列と、文字列が実行中の設定に保存される場合に文字列を暗号化すべきかどうかを指定します。 – **0**：暗号化なし。 – **1**：メッセージ ダイジェスト 5（MD5）を使用した暗号化。 • *password-string*：ログイン認証用の文字列。
ステップ 7	**end** **例：** `Router(config-credentials)# end`	特権 EXEC モードに戻ります。

CTL プロバイダーの確認

show credentials コマンドを使用して、クレデンシャル設定を表示します。

```
Router# show credentials

Credentials IP: 172.19.245.1
Credentials PORT: 2444
Trustpoint: ctlpv
```

次の作業

- CA がサードパーティ CA であるか、Cisco IOS CA が Cisco Unified CME ルータの外部にある Cisco IOS ルータにある場合、RA を設定して電話機に証明書を発行する必要があります。詳細については、「登録局の設定」（P.629）を参照してください
- CAPF セッションに指定した認証モードが認証文字列である場合、更新された LSC を受け取る各電話機に認証文字列を入力する必要があります。詳細については、「電話機での認証文字列の入力」（P.632）を参照してください。
- CAPF セッションに指定した認証モードが MIC である場合、MIC の発行者証明書が PKI トラストポイントにインポートされる必要があります。詳細については、「MIC ルート証明書の手動インポート」（P.633）を参照してください。
- メディア暗号化の設定方法については、「Cisco Unified CME でのメディア暗号化（SRTP）の設定」（P.636）を参照してください。

登録局の設定

登録局（RA）とは、CA が証明書を発行するために必要なデータの一部またはすべてを記録あるいは検証する役割を担う機関です。多くの場合、CA は RA 機能自体をすべて処理しますが、CA が広範囲にわたる地理的な場所を処理するか、ネットワークのエッジに CA を公開することにセキュリティ上の問題がある場合は、タスクの一部を RA に委任して、CA が証明書の署名という最も重要なタスクに集中できるようにすることを推奨します。

RA モードで実行するように CA を設定できます。RA が手動または Simple Certificate Enrollment Protocol（SCEP）登録要求を受け取ると、管理者はローカル ポリシーに基づいて、それを拒否または許可することができます。要求が許可されると、その要求は発行元 CA に転送され、CA は自動的に証明書を生成して RA に返します。クライアントは、許可された証明書を RA から後で取得できます。

RA を設定するには、Cisco Unified CME ルータで次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *label*
4. **enrollment url** *ca-url*
5. **revocation-check** *method1* [*method2* [*method3*]]
6. **serial-number** [**none**]
7. **rsakeypair** *key-label* [*key-size* [*encryption-key-size*]]
8. **exit**
9. **crypto pki server** *label*
10. **mode ra**
11. **lifetime certificate** *time*
12. **grant auto**
13. **no shutdown**
14. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**crypto pki trustpoint** *label* **例：** `Router(config)# crypto pki trustpoint ra12`	RA モード証明書サーバが使用するトラストポイントを宣言し、CA トラストポイント コンフィギュレーション モードを開始します。 • *label*：トランスポイントおよび RA の名前。 **ヒント** このラベルは、CA プロキシを設定するときに、**cert-enroll-trustpoint** コマンドにも必要です。「CAPF サーバの設定」（P.619）を参照してください。
ステップ 4	**enrollment url** *ca-url* **例：** `Router(config-ca-trustpoint)# enrollment url http://ca-server.company.com`	発行元の CA（ルート CA）の登録 URL を指定します。 • *ca-url*：ルート CA がインストールされたルータの URL。
ステップ 5	**revocation-check** *method1* [*method2* [*method3*]] **例：** `Router(config-ca-trustpoint)# revocation-check none`	（任意）証明書の失効ステータスをチェックし、ステータスをチェックするための 1 つまたは複数の方法を指定します。2 番めと 3 番めの方法を指定した場合、各方法はその直前の方法でエラーが返された場合（サーバがダウンしている場合など）にだけ使用されます。 *methodn* の有効な値は、次のとおりです。 • **crl**：証明書のチェックは、証明書失効リスト（CRL）によって実行されます。これはデフォルトの動作です。 • **none**：証明書のチェックは不要です。 • **ocsp**：証明書のチェックは、Online Certificate Status Protocol（OCSP）サーバによって実行されます。
ステップ 6	**serial-number** [**none**] **例：** `Router(config-ca-trustpoint)# serial-number`	（任意）証明書要求にルータのシリアル番号を含める必要があるかどうかを指定します。このコマンドを使用しなかった場合は、証明書の登録時にシリアル番号の入力を求められます。 • **none**：（任意）証明書要求にシリアル番号が含まれません。
ステップ 7	**rsakeypair** *key-label* [*key-size* [*encryption-key-size*]] **例：** `Router(config-ca-trustpoint)# rsakeypair exampleCAkeys 1024 1024`	（任意）証明書で使用する RSA キー ペアを指定します。 • *key-label*：キー ペアが存在していない場合、または **auto-enroll regenerate** コマンドが使用される場合に、登録中に生成されるキー ペアの名前。 • *key-size*：（任意）目的の RSA キーのサイズ。指定されなかった場合は、既存のキー サイズが使用されます。 • *encryption-key-size*：（任意）個別の暗号化、署名キー、および証明書を要求するために使用される 2 番めのキーのサイズ。 • 複数のトラストポイントで同じキーを共有できます。

	コマンドまたはアクション	目的
ステップ 8	**exit** **例：** `Router(config-ca-trustpoint)# exit`	CA 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 9	**crypto pki server** *label* **例：** `Router(config)# crypto pki server ra12`	証明書サーバのラベルを定義し、証明書サーバ コンフィギュレーション モードを開始します。 • *label*：トランスポイントおよび RA の名前。ステップ 3 で、トラストポイントおよび RA として以前に作成したものと同じラベルを使用します。
ステップ 10	**mode ra** **例：** `Router(config-cs-server)# mode ra`	PKI サーバを RA の証明書サーバ モードにします。
ステップ 11	**lifetime certificate** *time* **例：** `Router(config-cs-server)# lifetime certificate 1800`	（任意）証明書のライフタイムを日数で指定します。 • *time*：証明書が期限切れになるまでの日数。範囲は 1 ～ 1825 です。デフォルトは 365 です。証明書の最大のライフタイムは、CA 証明書のライフタイムよりも 1 ヵ月短い日数です。 • このコマンドは、**no shutdown** コマンドでサーバがイネーブルになる前に使用する必要があります。
ステップ 12	**grant auto** **例：** `Router(config-cs-server)# grant auto`	すべての要求者に対して証明書が自動的に発行されるようにします。 • このコマンドは、簡易ネットワークのテストおよび構築中に登録する場合のみ設定してください。 • セキュリティ上のベスト プラクティスとして、**no grant auto** コマンドを使用して設定後にこの機能をディセーブルにすることで、証明書が継続的に付与されないようにします。
ステップ 13	**no shutdown** **例：** `Router(config-cs-server)# no shutdown`	（任意）証明書サーバをイネーブルにします。 • プロンプトが表示されたら、CA 証明書、ルータ証明書、チャレンジ パスワード、および秘密キーを保護するためのパスワードの承認に関して入力します。 • 証明書サーバの設定が完了した後にのみ、このコマンドを使用します。
ステップ 14	**end** **例：** `Router(config-cs-server)# end`	特権 EXEC モードに戻ります。

次の作業

- ネットワーク上に複数の Cisco Unified CME ルータがある場合、CTL クライアントを実行していない各 Cisco Unified CME ルータに CTL プロバイダーを設定する必要があります。CTL クライアントが実行していない各 Cisco Unified CME ルータに CTL プロバイダーを設定するには、「CTL プロバイダーの設定」（P.626）を参照してください。

- CAPF セッションに指定した認証モードが認証文字列である場合、更新された LSC を受け取る各電話機に認証文字列を入力する必要があります。詳細については、「電話機での認証文字列の入力」（P.632）を参照してください。
- CAPF セッションに指定した認証モードが MIC である場合、MIC の発行者証明書が PKI トラストポイントにインポートされる必要があります。詳細については、「MIC ルート証明書の手動インポート」（P.633）を参照してください。
- メディア暗号化の設定方法については、「Cisco Unified CME でのメディア暗号化（SRTP）の設定」（P.636）を参照してください。

電話機での認証文字列の入力

この手順は、電話機に LSC の 1 回限りのインストールを行う場合と、CAPF セッションの認証モードを認証文字列に設定した場合にのみ必要です。認証文字列は、電話機ユーザが電話機に入力できるよう、LSC をインストールする前に電話機ユーザに知らせておく必要があります。

証明書をインストールするには、次の手順を実行します。

（注） **show capf-server auth-string** コマンドを使用すると、電話機の認証文字列をリストできます。

前提条件

- 署名されたイメージが IP Phone に存在すること。ご使用の電話機のモデルをサポートする Cisco Unified IP Phone の管理マニュアルを参照してください。
- IP Phone が Cisco Unified CME に登録されていること。
- CTL ファイルに CAPF 証明書が存在すること。詳細については、「CTL クライアントの設定」（P.614）を参照してください。
- 入力する認証文字列が、CAPF サーバ コンフィギュレーション モードで **auth-string** コマンドを使用して設定されているか、ephone コンフィギュレーション モードで **capf-auth-str** コマンドを使用して設定されていること。詳細については、「Telephony-Service セキュリティ パラメータの設定」（P.611）を参照してください。
- **device-security-mode** コマンドが **none** キーワードを使用して設定されていること。詳細については、「Telephony-Service セキュリティ パラメータの設定」（P.611）を参照してください。

制約事項

- 認証文字列は 1 回だけ使用できます。

手順の詳細

ステップ 1 **設定**ボタンを押します。Cisco Unified IP Phone 7921 では、**下矢印**を押して [設定（Settings）] メニューにアクセスします。

ステップ 2 設定がロックされている場合は、[**#]（アスタリスク、アスタリスク、ポンド記号）を押してロック解除します。

ステップ 3 [設定（Settings）] メニューまでスクロールダウンします。セキュリティ設定を強調表示して、[選択（Select）] ソフトキーを押します。

ステップ 4 [セキュリティ設定（Security Configuration）] メニューまでスクロールダウンします。LSC を強調表示して、[更新（Update）] ソフトキーを押します。Cisco Unified IP Phone 7921 では、[**#] を押すと、[セキュリティ設定（Security Configuration）] メニューがロック解除されます。

ステップ 5 認証文字列の入力を求められたら、システム管理者から提供された文字列を入力して、[送信（Submit）] ソフトキーを押します。

CAPF コンフィギュレーションに応じて、電話機は証明書をインストール、更新、削除、またはフェッチします。

電話機に表示されるメッセージを確認して、証明書動作の進捗をモニタできます。[送信（Submit）] を押すと、「処理中（Pending）」というメッセージが LSC オプションの下に表示されます。電話機によって公開キーと秘密キーのペアが生成され、電話機の情報が表示されます。電話機でプロセスが正常に完了すると、電話機に成功のメッセージが表示されます。電話機に失敗のメッセージが表示された場合は、間違った認証文字列を入力したか、電話機が更新できるように設定されていません。

[停止（Stop）] を選択すると、プロセスをいつでも停止できます。

ステップ 6 証明書が電話機にインストールされたことを確認します。電話機画面の [設定（Settings）] メニューから、[モデル情報（Model Information）] を選択した後、[選択（Select）] ソフトキーを押して、[モデル情報（Model Information）] を表示します。

ステップ 7 ナビゲーション ボタンを押して、LSC までスクロールします。この項目の値は、LSC が [インストール済み（Installed）] または [未インストール（Not Installed）] のどちらであるかを示します。

次の作業

- ネットワーク上に複数の Cisco Unified CME ルータがある場合、CTL クライアントを実行していない各 Cisco Unified CME ルータに CTL プロバイダーを設定する必要があります。CTL クライアントが実行していない各 Cisco Unified CME ルータに CTL プロバイダーを設定するには、「CTL プロバイダーの設定」（P.626）を参照してください。
- CA がサードパーティ CA であるか、Cisco IOS CA が Cisco Unified CME ルータの外部にある Cisco IOS ルータにある場合、RA を設定して電話機に証明書を発行する必要があります。詳細については、「登録局の設定」（P.629）を参照してください
- CAPF セッションに指定した認証モードが MIC である場合、MIC の発行者証明書が PKI トラストポイントにインポートされる必要があります。詳細については、「MIC ルート証明書の手動インポート」（P.633）を参照してください。
- メディア暗号化の設定方法については、「Cisco Unified CME でのメディア暗号化（SRTP）の設定」（P.636）を参照してください。

MIC ルート証明書の手動インポート

Cisco Unified CME が提示された MIC を認証できるようにするには、MIC ルート証明書が Cisco Unified CME ルータに存在している必要があります。MIC ルート証明書を Cisco Unified CME ルータに手動でインポートするには、認証に MIC が必要な電話機のタイプごとに、次の手順を実行します。

前提条件

この作業を実行するには、次のいずれかに該当する必要があります。

- **device-security-mode** コマンドが **none** キーワードを使用して設定されていること。詳細については、「Telephony-Service セキュリティ パラメータの設定」（P.611）を参照してください。
- MIC が、CAPF セッションで電話機認証用に指定された認証モードになっていること。
- 電話機の LSC ではなく、MIC が使用されて、SCCP シグナリング用の TLS セッションが確立されている。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **revocation-check none**
5. **enrollment terminal**
6. **exit**
7. **crypto pki authenticate** *name*
8. 4 つの MIC ルート ファイルをダウンロードします。証明書の該当するテキストをカット アンド ペーストします。証明書を受け入れます。
9. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki trustpoint** *name* **例：** `Router(config)# crypto pki trustpoint sanjose1`	ルータが使用する CA を宣言し、CA トラストポイント コンフィギュレーション モードを開始します。 • *name*：すでに設定済みの CA のラベル。
ステップ 4	**revocation-check none** **例：** `Router(ca-trustpoint)# revocation-check none`	失効チェックが実行されず、証明書が常に受け入れられることを指定します。
ステップ 5	**enrollment terminal** **例：** `Router(ca-trustpoint)# enrollment terminal`	手動（コピー アンド ペースト）での証明書登録を指定します。

	コマンドまたはアクション	目的
ステップ 6	**exit** **例：** `Router(ca-trustpoint)# exit`	CA 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 7	**crypto pki authenticate** *name* **例：** `Router(config)# crypto pki authenticate sanjose1`	CA から証明書を取得することにより、CA を認証します。 • *name*：すでに設定済みの CA のラベル。
ステップ 8	4 つの MIC ルート証明書ファイルをダウンロードします。証明書ごとに、該当するテキストをカット アンド ペーストします。証明書を受け入れます。	
	a. 証明書のリンクをクリックします。	証明書は、次のリンクで入手できます。 • CAP-RTP-001： http://www.cisco.com/security/pki/certs/CAP-RTP-001.cer • CAP-RTP-002： http://www.cisco.com/security/pki/certs/CAP-RTP-002.cer • CMCA： http://www.cisco.com/security/pki/certs/cmca.cer • CiscoRootCA2048： http://www.cisco.com/security/pki/certs/crca2048.cer
	b. [証明書のダウンロード中（Downloading Certificate）] ダイアログ ウィンドウが開いたら、証明書を「表示」するオプションを選択します。証明書はインストールしないでください。	
	c. 上部にある [詳細（Detail）] タブを選択します。	
	d. 下部にある [エクスポート（Export）] をクリックして、証明書をファイルに保存します。	
	e. ワードパッドでファイルを開きます。	
	f. 「-----BEGIN CERTIFICATE-----」と「-----END CERTIFICATE-----」の間のテキストを IOS コンソールにカット アンド ペーストします。	
	g. プロンプトが表示されたら、Enter を押して、**quit** と入力します。	証明書を貼り付けたら、Enter を押して、**quit** と 1 行で入力します。
	h. **y** と入力して、証明書を受け入れます。	システムは貼り付けられた証明書テキストに対して、MD5 および SHA1 フィンガープリントを提示し、証明書を受け入れるかどうかを問い合わせます。 証明書を受け入れるには **y** と入力し、拒否するには **n** と入力します。

	コマンドまたはアクション	目的
	i. 証明書ごとに、ステップ a から h を繰り返します。	
ステップ 9	**exit** **例：** `Router(config)# exit`	特権 EXEC モードに戻ります。

次の作業

- ネットワーク上に複数の Cisco Unified CME ルータがある場合、CTL クライアントを実行していない各 Cisco Unified CME ルータに CTL プロバイダーを設定する必要があります。CTL クライアントが実行していない各 Cisco Unified CME ルータに CTL プロバイダーを設定するには、「CTL プロバイダーの設定」（P.626）を参照してください。
- CA がサードパーティ CA であるか、Cisco IOS CA が Cisco Unified CME ルータの外部にある Cisco IOS ルータにある場合、RA を設定して電話機に証明書を発行する必要があります。詳細については、「登録局の設定」（P.629）を参照してください
- CAPF セッションに指定した認証モードが認証文字列である場合、更新された LSC を受け取る各電話機に認証文字列を入力する必要があります。詳細については、「電話機での認証文字列の入力」（P.632）を参照してください。
- メディア暗号化の設定方法については、「Cisco Unified CME でのメディア暗号化（SRTP）の設定」（P.636）を参照してください。

Cisco Unified CME でのメディア暗号化（SRTP）の設定

H.323 トランクを経由した Cisco Unified CME システム間のセキュア コールのネットワークを設定するには、Cisco Unified CME ルータで次の手順を実行します。

前提条件

- Cisco Unified CME 4.2 以降のバージョン。
- H.323 コールを保護するには、telephony-service のセキュリティ パラメータが設定されていること。「Telephony-Service セキュリティ パラメータの設定」（P.611）を参照してください。
- Cisco VG224 Analog Phone Gateway に互換性のある Cisco IOS リリースが存在すること。詳細については、『Cisco Unified CME and Cisco IOS Release Compatibility Matrix』を参照してください。

制約事項

- セキュアな 3 者間ソフトウェア会議はサポートされていません。SRTP で開始されたセキュアなコールは、会議に参加すると必ず、非セキュアなリアルタイム転送プロトコル（RTP）に戻ります。
- 1 人の参加者が 3 者間会議から退出すると、残りの 2 人の参加者が単一の Cisco Unified CME への SRTP 対応ローカル Skinny Client Control Protocol（SCCP）エンドポイントであり、残りの参加者のどちらかが会議の作成者である場合、その 2 人の参加者間コールがセキュアに戻ります。残り

2 人の参加者の一方だけが RTP に対応している場合、コールは非セキュアなままになります。残りの 2 人の参加者が FXS、PSTN、または VoIP を介して接続されている場合、コールは非セキュアのままになります。

- Cisco Unity Express へのコールはセキュアではありません。
- 保留音（MOH）はセキュアではありません。
- ビデオ コールはセキュアではありません。
- モデム リレーおよび T.3 Fax リレーのコールはセキュアではありません。
- メディアのフローアラウンドは、コール転送およびコール自動転送に対応していません。
- インバンド トーンと RFC 2833 DTMF の間の変換はサポートされていません。RFC 2833 DTMF の処理は、暗号キーがセキュア DSP Farm デバイスに送信される場合はサポートされますが、コーデック パススルーに対してはサポートされません。
- セキュアな Cisco Unified CME は SIP トランクをサポートしていません。H.323 トランクのみサポートされています。
- メディア暗号化（SRTP）は、H.450 と非 H.450 の両方の Cisco Unified CME ネットワークで、セキュアな補足サービスをサポートします。セキュア Cisco Unified CME ネットワークは、H.450 または非 H.450 にする必要があり、ハイブリッドにはできません。
- セキュア コールは、デフォルトのセッション アプリケーションのみでサポートされています。

手順の概要

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **supplementary-service media-renegotiate**
5. **srtp fallback**
6. **h323**
7. **emptycapability**
8. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**voice service voip** **例：** `Router(config)# voice service voip`	音声サービス コンフィギュレーション モードを開始します。 • **voip** キーワードによって、VoIP のカプセル化が指定されます。

	コマンドまたはアクション	目的
ステップ 4	**supplementary-service media-renegotiate** **例：** `Router(conf-voi-serv)# supplementary-service media-renegotiate`	SRTP 暗号化キーのコール中再ネゴシエーションをイネーブルにします。
ステップ 5	**srtp fallback** **例：** `Router(conf-voi-serv)# srtp fallback`	メディア暗号化と認証用に SRTP を使用してセキュア コールをグローバルにイネーブルにし、SRTP-to-RTP フォールバックをイネーブルにして、リングバック音や MOH などの補足サービスをサポートします。 • 個々のダイヤルピアでフォールバックを設定する場合は、このステップをスキップします。 • このコマンドは、ダイヤルピア コンフィギュレーション モードでも設定できます。ダイヤルピア コンフィギュレーション コマンドでのこのコマンドは、音声サービス VoIP コンフィギュレーション モードでのこのコマンドよりも優先されます。
ステップ 6	**h323** **例：** `Router(conf-voi-serv)# h323`	H.323 音声サービス コンフィギュレーション モードを開始します。
ステップ 7	**emptycapability** **例：** `Router(conf-serv-h323)# emptycapability`	ロータリー グループのすべてのダイヤルピアでの、同一のコーデック機能の必要性を排除します。
ステップ 8	**exit** **例：** `Router(conf-serv-h323)# exit`	H.323 音声サービス コンフィギュレーション モードを終了します。

次の作業

Cisco Unified CME にメディア暗号化（SRTP）を設定するために必要な作業が完了しました。これで、次のオプション タスクを実行できます。

- 「H.323 ダイヤルピア用の Cisco Unified CME SRTP フォールバックの設定」（P.639）（任意）
- 「セキュア Cisco Unified CME 動作用の Cisco Unity の設定」（P.640）（任意）

H.323 ダイヤルピア用の Cisco Unified CME SRTP フォールバックの設定

個々のダイヤルピア用に SRTP フォールバックを設定するには、Cisco Unified CME ルータで次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **voice class codec** *tag*
4. **codec preference** *value codec-type*
5. **exit**
6. **dial-peer voice** *tag* **voip**
7. **srtp fallback**
8. **voice-class codec** *tag*
9. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**voice class codec** *tag* **例：** `Router(config)# voice class codec 1`	音声クラス コンフィギュレーション モードを開始し、コーデック音声クラスに識別タグ番号を割り当てます。
ステップ 4	**codec preference** *value codec-type* **例：** `Router(config-voice-class)# codec preference 1 g711alaw`	ダイヤルピアで使用するコーデックのリストを優先順位を付けて指定します。 • このステップを繰り返して、優先されるコーデックのリストを作成します。 • H.323 トランクのどちら側でも、両方の Cisco Unified CME でコーデック リストに同じ優先順位を使用します。
ステップ 5	**exit** **例：** `Router(config-voice-class)# exit`	voice-class コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 6	**dial-peer voice** *tag* **voip** **例：** `Router(config)# dial-peer voice 101 voip`	ダイヤルピア音声コンフィギュレーション モードを開始します。
ステップ 7	**srtp fallback** **例：** `Router(config-dial-peer)# srtp fallback`	メディア暗号化と認証に SRTP を使用するセキュア コールをイネーブルにして、フォールバック機能を指定します。 • **no srtp** コマンドを使用して SRTP をディセーブルにし、ダイヤルピアを RTP モードに戻します。 • **fallback**：個々のダイヤルピアで非セキュア モード（RTP）へのフォールバックをイネーブルにします。**no srtp fallback** コマンドは、フォールバックと SRTP をディセーブルにします。 • このコマンドは、音声サービス VoIP コンフィギュレーション モードでも設定できます。ダイヤルピア コンフィギュレーション コマンドでのこのコマンドは、音声サービス VoIP コンフィギュレーション モードでのこのコマンドよりも優先されます。
ステップ 8	**voice-class codec** *tag* **例：** `Router(config-dial-peer)# voice-class codec 1`	以前に設定したコーデックの選択優先リスト（コーデック音声クラス）を Voice over IP（VoIP）ダイヤルピアに割り当てます。 • このステップの *tag* 引数は、ステップ 3 の *tag* と同じにします。
ステップ 9	**exit** **例：** `Router(config-dial-peer)# exit`	ダイヤルピア音声コンフィギュレーション モードを終了します。

セキュア Cisco Unified CME 動作用の Cisco Unity の設定

ここでは、次の作業について説明します。

- 「前提条件」（P.640）
- 「Cisco Unified CME と Cisco Unity との連動の設定」（P.640）
- 「Cisco Unified CME への Cisco Unity ルート証明書のインポート」（P.641）
- 「セキュアな登録のための Cisco Unity ポートの設定」（P.644）
- 「Cisco Unity がセキュアに登録されたことの確認」（P.644）

前提条件

- Cisco Unity 4.2 以降のバージョン。

Cisco Unified CME と Cisco Unity との連動の設定

Cisco Unified CME と Cisco Unity との連動の設定を変更するには、Cisco Unity サーバで次の手順を実行します。

ステップ 1 Cisco Unity Telephony Integration Manager（UTIM）が Cisco Unity サーバでまだ開いていない場合は、Windows の [スタート（Start）] メニューから、[プログラム（Program）] > [Cisco Unity] > [連動の管理（Manage Integrations）] を選択します。UTIM ウィンドウが表示されます。

ステップ 2 左ペインで、[Cisco Unity サーバ（Cisco Unity Server）] をダブルクリックします。既存の連動が表示されます。

ステップ 3 [Cisco Unified Communications Manager] 連動をクリックします。

ステップ 4 右ペインで、連動のためのクラスタをクリックします。

ステップ 5 [サーバ（Servers）] タブをクリックします。

ステップ 6 [Cisco Unified Communications Manager クラスタ セキュリティ モード（Cisco Unified Communications Manager Cluster Security Mode）] フィールドで、適切な設定をクリックします。

ステップ 7 [保証なし（Non-secure）] をクリックした場合、[保存（Save）] をクリックしてこの残りの手順を省略します。

[認証済（Authenticated）] 設定または [暗号化済（Encrypted）] をクリックした場合、[セキュリティ（Security）] タブと [Tftp サーバ追加（Add TFTP Server）] ダイアログボックスが表示されます。[Tftp サーバ追加（Add TFTP Server）] ダイアログボックスの [IP アドレス/ホスト名（IP Address or Host Name）] フィールドに、Cisco Unified Communications Manager クラスタのプライマリ TFTP サーバの IP アドレス（または DNS 名）を入力して、[OK] をクリックします。

ステップ 8 Cisco Unity で Cisco Unified Communications Manager 証明書のダウンロードに使用する TFTP サーバがさらにある場合は、[追加（Add）] をクリックします。[Tftp サーバ追加（Add TFTP Server）] ダイアログボックスが表示されます。

ステップ 9 [IP アドレス/ホスト名（IP Address or Host Name）] フィールドで、Cisco Unified Communications Manager クラスタのためのセカンダリ TFTP サーバの IP アドレス（または DNS 名）を入力し、[OK] をクリックします。

ステップ 10 [保存（Save）] をクリックします。

Cisco Unity によってボイスメッセージング ポート デバイス証明書が作成され、Cisco Unity サーバ ルート証明書がエクスポートされて、[Cisco Unity ルート証明書のエクスポート（Export Cisco Unity Root Certificate）] ダイアログボックスが表示されます。

ステップ 11 エクスポートされた Cisco Unity サーバ ルート証明書のファイル名をメモし、[OK] をクリックします。

ステップ 12 Cisco Unity サーバで、CommServer\SkinnyCerts ディレクトリに移動します。

ステップ 13 ステップ 11 でエクスポートした、Cisco Unity サーバ ルート証明書を見つけます。

ステップ 14 そのファイルを右クリックし、[名前の変更（Rename）] をクリックします。

ステップ 15 ファイル拡張子を .0 から .pem に変更します。たとえば、エクスポートされた Cisco Unity サーバ ルート証明書ファイルの場合、ファイル名「12345.0」を「12345.pem」に変えます。

ステップ 16 このファイルを、Cisco Unified CME ルータにアクセスできる PC にコピーします。

Cisco Unified CME への Cisco Unity ルート証明書のインポート

Cisco Unity ルート証明書を Cisco Unified CME にインポートするには、Cisco Unified CME ルータで次の手順を実行します。

手順の概要

1. **enable**

2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **revocation-check none**
5. **enrollment terminal**
6. **exit**
7. **crypto pki authenticate** *trustpoint-label*
8. ステップ 16 で、Cisco Unity サーバからコピーしたルート証明書ファイルを開きます。
9. CA 証明書を入力するよう求められます。コマンド ラインで「BEGIN CERTIFICATE」と「END CERTIFICATE」の間の Base64 エンコードされた証明書のすべての内容をカット アンド ペーストします。Enter を押して、「quit」と入力します。ルータから、証明書を受け入れるよう求められます。「yes」と入力して証明書を受け入れます。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki trustpoint** *name* **例：** `Router(config)# crypto pki trustpoint PEM`	RA モード証明書サーバが使用するトラストポイントを宣言し、CA トラストポイント コンフィギュレーション モードを開始します。 • *label*：トランスポイントおよび RA の名前。
ステップ 4	**revocation-check none** **例：** `Router(ca-trustpoint)# revocation-check none`	（任意）証明書の確認が必要ないことを指定します。
ステップ 5	**enrollment terminal** **例：** `Router(ca-trustpoint)# enrollment terminal`	カット アンド ペーストによる手動での証明書登録を指定します。
ステップ 6	**exit** **例：** `Router(ca-trustpoint)# exit`	CA 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 7	**crypto pki authenticate** *trustpoint-label* **例：** `Router(config)# crypto pki authenticate pem`	CA 証明書を取得して、認証します。証明書のフィンガープリントをチェックするよう求められた場合、証明書フィンガープリントをチェックします。 • *trustpoint-label*：すでに設定済みのトラストポイントと RA の名前。ステップ 3 を参照してください。

	コマンドまたはアクション	目的
ステップ 8	ステップ 16 で、Cisco Unity サーバからコピーしたルート証明書ファイルを開きます。	
ステップ 9	CA 証明書を入力するよう求められます。コマンド ラインで「BEGIN CERTIFICATE」と「END CERTIFICATE」の間の Base64 エンコードされた証明書のすべての内容をカット アンド ペーストします。Enter を押して、「quit」と入力します。ルータから、証明書を受け入れるよう求められます。「yes」と入力して証明書を受け入れます。	Cisco Unified CME ルータへの Cisco Unity ルート証明書のコピーが完了します。

セキュアな登録のための Cisco Unity ポートの設定

セキュア モードでの登録用に Cisco Unity のポートを設定するには、次の手順を実行します。

ステップ 1 更新する Cisco ボイスメール ポートを選択します。

ステップ 2 [デバイス セキュリティ モード（Device Security Mode）] ドロップダウン リストから、[暗号化済（Encrypted）] を選択します。

ステップ 3 [更新（Update）] をクリックします。

Cisco Unity がセキュアに登録されたことの確認

show sccp connections コマンドを使用して、Cisco Unity ポートが Cisco Unified CME にセキュアに登録されていることを確認します。

show sccp connection：例

次の例では、タイプ フィールドのセキュアな値によって、接続がセキュアであることが示されています。

```
Router# show sccp connections

sess_id    conn_id    stype        mode     codec   ripaddr       rport sport

16777222   16777409   secure-xcode sendrecv g729b   10.3.56.120   16772 19534
16777222   16777393   secure-xcode sendrecv g711u   10.3.56.50    17030 18464

Total number of active session(s) 1, and connection(s) 2
```

Cisco Unified IP Phone 用の HTTPS プロビジョニング

HTTPS を使用して Web コンテンツにセキュアにアクセスするために Cisco Unified IP Phone をプロビジョニングするには、次の手順を実行します。

前提条件

- 登録の無限ループを防止するため、Firmware 9.0(4) 以降のバージョンが IP Phone にインストールされていること。
- フラッシュ メモリから IP Phone にインポートする証明書ファイルが、プライバシーが強化されたメール形式になっていること。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **crypto pki server** *cs-label*
5. **database level** {**minimum** | **names** | **complete**}
6. **database url** *root url*

7. **grant auto**
8. **exit**
9. **crypto pki trustpoint** *name*
10. **enrollment url** *url*
11. **exit**
12. **crypto pki server** *cs-label*
13. **no shutdown**
14. **exit**
15. **crypto pki trustpoint** *name*
16. **enrollment url** *url*
17. **revocation-check** *method1* [*method2*[*method3*]]
18. **rsakeypair** *key-label*
19. **exit**
20. **crypto pki authenticate** *name*
21. **crypto pki enroll** *name*
22. **crypto pki trustpoint** *name*
23. **enrollment url** *url*
24. **revocation-check** *method1* [*method2*[*method3*]]
25. **rsakeypair** *key-label*
26. **exit**
27. **crypto pki authenticate** *name*
28. **crypto pki enroll** *name*
29. **ctl-client**
30. **sast1 trustpoint** *label*
31. **sast2 trustpoint** *label*
32. **import certificate** *tag description* **flash:***cert_name*
33. **regenerate**
34. **end**

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 3	**ip http server** **例：** `Router(config)# ip http server`	Cisco Unified CME ルータで HTTP サーバをイネーブルにします。
ステップ 4	**crypto pki server** *cs-label* **例：** `Router(config)# crypto pki server IOS-CA`	Cisco IOS 証明書サーバをイネーブルにし、証明書サーバ コンフィギュレーション モードを開始します。 • *cs-label*：証明書サーバの名前。 **（注）** 証明書サーバの名前は 13 文字までです。
ステップ 5	**database level** {**minimum** | **names** | **complete**} **例：** `Router(cs-server)# database level complete`	証明書登録データベースに保管されるデータのタイプを制御します。 • **complete**：発行された各証明書はデータベースに書き込まれます。このキーワードを使用する場合は、**database url** コマンドをイネーブルにする必要があります。
ステップ 6	**database url** *root url* **例：** `Router(cs-server)# database url flash:`	証明書サーバのデータベース エントリが保存または公開される場所を指定します。 • *root url*：データベース エントリが書き込まれる場所。
ステップ 7	**grant auto** **例：** `Router(cs-server)# grant auto`	（任意）あらゆる要求者に対して証明書が自動的に発行されるようにします。推奨される方法、およびこのコマンドを使用しなかった場合のデフォルトは手動登録です。
ステップ 8	**exit** **例：** `Router(cs-server)# exit`	証明書サーバ コンフィギュレーション モードを終了します。
ステップ 9	**crypto pki trustpoint** *name* **例：** `Router(config)# crypto pki trustpoint IOS-CA`	トラストポイントを宣言し、CA トラストポイント コンフィギュレーション モードを開始します。 • *name*：トラストポイントの名前。
ステップ 10	**enrollment url** *url* **例：** `Router(ca-trustpoint)# enrollment url http://10.1.1.1:80`	認証局の登録パラメータを指定します。 • *url*：ルータが証明書要求を送信するファイル システムの URL を指定します。
ステップ 11	**exit** **例：** `Router(ca-trustpoint)# exit`	CA 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 12	**crypto pki server** *cs-label* **例：** `Router(config)# crypto pki server IOS-CA`	Cisco IOS 証明書サーバをイネーブルにし、証明書サーバ コンフィギュレーション モードを開始します。 • *cs-label*：証明書サーバの名前。 **（注）** 証明書サーバの名前は 13 文字までです。

	コマンドまたはアクション	目的
ステップ 13	**no shutdown** **例：** `Router(cs-server)# no shutdown`	Cisco IOS 認証局をイネーブルにします。
ステップ 14	**exit** **例：** `Router(cs-server)# exit`	証明書サーバ コンフィギュレーション モードを終了します。
ステップ 15	**crypto pki trustpoint** *name* **例：** `Router(config)# crypto pki trustpoint primary-cme`	トラストポイントを宣言し、CA トラストポイント コンフィギュレーション モードを開始します。 • *name*：トラストポイントの名前。
ステップ 16	**enrollment url** *url* **例：** `Router(ca-trustpoint)# enrollment url http://10.1.1.1:80`	認証局の登録パラメータを指定します。 • *url*：ルータが証明書要求を送信するファイル システムの URL を指定します。
ステップ 17	**revocation-check** *method1* [*method2*[*method3*]] **例：** `Router(ca-trustpoint)# revocation-check none`	証明書の失効ステータスをチェックします。 • **none**：証明書のチェックは不要です。
ステップ 18	**rsakeypair** *key-label* **例：** `Router(ca-trustpoint)# rsakeypair primary-cme`	証明書に関連付ける RSA キー ペアを指定します。 • *key-label*：キー ペアの名前がまだ存在しない場合、または **auto-enroll regenerate** コマンドが設定されている場合、登録時に生成されるキー ペアの名前。
ステップ 19	**exit** **例：** `Router(ca-trustpoint)# exit`	CA 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 20	**crypto pki authenticate** *name* **例：** `Router(config)# crypto pki authenticate primary-cme`	認証局の証明書を取得して、認証局を認証します。 • *name*：認証局の名前。
ステップ 21	**crypto pki enroll** *name* **例：** `Router(config)# crypto pki enroll primary-cme`	認証局からルータの証明書を取得します。 • *name*：認証局の名前。**crypto pki trustpoint** コマンドを使用して認証局を宣言したときと同じ名前を使用します。
ステップ 22	**crypto pki trustpoint** *name* **例：** `Router(config)# crypto pki trustpoint sast-secondary`	トラストポイントを宣言し、CA トラストポイント コンフィギュレーション モードを開始します。 • *name*：トラストポイントの名前。

	コマンドまたはアクション	目的
ステップ 23	**enrollment url** *url* **例：** `Router(ca-trustpoint)# enrollment url http://10.1.1.1:80`	認証局の登録パラメータを指定します。 • *url*：ルータが証明書要求を送信するファイル システムの URL を指定します。
ステップ 24	**revocation-check** *method1* [*method2*[*method3*]] **例：** `Router(ca-trustpoint)# revocation-check none`	証明書の失効ステータスをチェックします。 • **none**：証明書のチェックは不要です。
ステップ 25	**rsakeypair** *key-label* **例：** `Router(ca-trustpoint)# rsakeypair sast-secondary`	証明書に関連付ける RSA キー ペアを指定します。 • *key-label*：キー ペアの名前がまだ存在しない場合、または **auto-enroll regenerate** コマンドが設定されている場合、登録時に生成されるキー ペアの名前。
ステップ 26	**exit** **例：** `Router(ca-trustpoint)# exit`	CA 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 27	**crypto pki authenticate** *name* **例：** `Router(config)# crypto pki authenticate sast-secondary`	認証局の証明書を取得して、認証局を認証します。 • *name*：認証局の名前。
ステップ 28	**crypto pki enroll** *name* **例：** `Router(config)# crypto pki enroll sast-secondary`	認証局からルータの証明書を取得します。 • *name*：認証局の名前。**crypto pki trustpoint** コマンドを使用して認証局を宣言したときと同じ名前を使用します。
ステップ 29	**ctl-client** **例：** `Router(config)# ctl-client`	CTL クライアント コンフィギュレーション モードを開始して、CTL クライアントのパラメータを設定します。
ステップ 30	**sastl trustpoint** *label* **例：** `Router(config-ctl-client)# sast1 trustpoint first-sast`	プライマリ SAST のクレデンシャルを設定します。 • *label*：SAST1 トラストポイントの名前。 **（注）** SAST1 証明書と SAST2 証明書は、互いに異なるものにする必要があります。CTL ファイルは常に SAST1 によって署名されます。SAST2 証明書は CTL ファイルに含まれるため、SAST1 証明書が破損した場合、SAST2 でファイルを署名することで、電話機が工場出荷時のデフォルト設定にリセットされることを防止できます。

	コマンドまたはアクション	目的
ステップ 31	**sast2 trustpoint** *label* **例：** `Router(config-ctl-client)# sast2 trustpoint second-sast`	セカンダリ SAST のクレデンシャルを設定します。 • *label*：SAST2 トラストポイントの名前。 **（注）** SAST1 証明書と SAST2 証明書は、互いに異なるものにする必要があります。CTL ファイルは常に SAST1 によって署名されます。SAST2 証明書は CTL ファイルに含まれるため、SAST1 証明書が破損した場合、SAST2 でファイルを署名することで、電話機が工場出荷時のデフォルト設定にリセットされることを防止できます。
ステップ 32	**import certificate** *tag description* **flash:***cert_name* **例：** `Router(config-ctl-client)# import certificate 5 FlashCert flash:flash_cert.cer`	フラッシュ メモリから IP Phone の CTL ファイルに、信頼できる証明書を PEM 形式でインポートします。 • *tag*：信頼できる証明書の ID。 • *description*：信頼できる証明書のわかりやすい名前。 • **flash:***cert_cert*：フラッシュ メモリに保存された、信頼できる証明書のファイル名を指定します。
ステップ 33	**regenerate** **例：** `Router(config-ctl-client)# regenerate`	CTL クライアント コンフィギュレーションに変更を行った後に、新しい CTLFile.tlv を作成します。
ステップ 34	**end** **例：** `Router(config-ctl-client)# end`	特権 EXEC モードに戻ります。

セキュリティの設定例

この項では、次の例について説明します。

電話機認証

- 「Cisco IOS CA：例」（P.650）
- 「Cisco Unified CME ルータへの MIC ルート証明書の手動インポート：例」（P.650）
- 「Telephony-Service のセキュリティ パラメータ：例」（P.653）
- 「Cisco Unified CME ルータで実行される CTL クライアント：例」（P.653）

メディア暗号化

- 「セキュア Cisco Unified CME：例」（P.656）

Cisco IOS CA：例

```
crypto pki server iosca
 grant auto
 database url flash:
!
crypto pki trustpoint iosca
 revocation-check none
 rsakeypair iosca
!
crypto pki certificate chain iosca
 certificate ca 01
  308201F9 30820162 ...
```

Cisco Unified CME ルータへの MIC ルート証明書の手動インポート：例

次の例は、ルータにインポートされる 3 つの証明書（7970、7960、PEM）の例を示しています。

```
Router(config)# crypto pki trustpoint 7970
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate 7970

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDqDCCApCgAwIBAgIQNT+yS9cPFKNGwfOprHJWdTANBgkqhkiG9w0BAQUFADAu
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRQwEgYDVQQDEwtDQVAtUlRQLTAwMjAe
Fw0wMzEwMTAyMDE4NDlaFw0yMzEwMTAyMDI3MzdaMC4xFjAUBgNVBAoTDUNpc2Nv
IFN5c3RlbXMxFDASBgNVBAMTC0NBUC1SVFAtMDAyMIIBIDANBgkqhkiG9w0BAQEF
AAOCAQ0AMIIBCAKCAQEAxCZlBK19w/2NZVVvpjCPrpW1cCY7V1q9lhzI85RZZdnQ
2M4CufgIzNa3zYxGJIAYeFfcRECnMB3f5A+x7xNiEuzE87UPvK+7S80uWCY0Uhtl
AVVf5NQgZ3YDNoNXg5MmONb8lT86F55EZyVac0XGne77TSIbIdejrTgYQXGP2MJx
Qhg+ZQlGFDRzbHfM84Duv2Msez+l+SqmqO80kIckqE9Nr3/XCSj1hXZNNVg8D+mv
Hth2P6KZqAKXAAStGRLSZX3jNbS8tveJ3Gi5+sj9+F6KKK2PD0iDwHcRKkcUHb7g
lI++U/5nswjUDIAph715Ds2rn9ehkMGipGLF8kpuCwIBA6OBwzCBwDALBgNVHQ8E
BAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUUpIr4ojuLgmKTn5wLFal
mrTUm5YwbwYDVR0fBGgwZjBkoGKgYIYtaHR0cDovL2NhcC1ydHAtMDAyL0NlcnRF
bnJvbGwvQ0FQLVJUUC0wMDIuY3Jshi9maWxlOi8vXFxjYXAtcnRwLTAwMlxDZXJ0
RW5yb2xsXENBUC1SVFAtMDAyLmNybDAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG
9w0BAQUFAAOCAQEAVoOM78TaOtHqj7sVL/5u5VChlyvU168f0piJLNWip2vDRihm
E+DlXdwMS5JaqUtuaSd/m/xzxpcRJm4ZRRwPq6VeaiiQGkjFuZEe5jSKiSAK7eHg
tup4HP/ZfKSwPA40DlsGSYsKNMm3OmVOCQUMH02lPkS/eEQ9sIw6QS7uuHN4y4CJ
NPnRbpFRLw06hnStCZHtGpKEHnY213QOy3h/EWhbnp0MZ+hdr20FujSI6G1+L39l
aRjeD708f2fYoz9wnEpZbtn2Kzse3uhU1Ygq1D1x9yuPq388C18HWdmCj4OVTXux
V6Y47H1yv/GJM8FvdgvKlExbGTFnlHpPiaG9tQ==
quit
Certificate has the following attributes:
Fingerprint MD5: F7E150EA 5E6E3AC5 615FC696 66415C9F
Fingerprint SHA1: 1BE2B503 DC72EE28 0C0F6B18 798236D8 D3B18BE6
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported
Router(config)# crypto pki trustpoint 7960
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate 7960

Enter the base 64 encoded CA certificate.
```

```
End with a blank line or the word "quit" on a line by itself
MIICKDCCAZGgAwIBAgIC8wEwDQYJKoZIhvcNAQEFBQAwQDELMAkGA1UEBhMCVVMx
GjAYBgNVBAoTEUNpc2NvIFN5c3RlbXMgSW5jMRUwEwYDVQQDEwxDQVBGLTdEN0Qw
QzAwHhcNMDQwNzE1MjIzODMyWhcNMTkwNzEyMjIzODMxWjBAMQswCQYDVQQGEwJV
UzEaMBgGA1UEChMRQ2lzY28gU3lzdGVtcyBJbmMxFTATBgNVBAMTDENBUEYtN0Q3
RDBDMDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA0hvMOZZ9ENYWme11YGY1
it2rvE3Nk/eqhnv8P9eqB1iqt+fFBeAG0WZ5bO5FetdU+BCmPnddvAeSpsfr3Z+h
x+r58fOEIBRHQLgnDZ+nwYH39uwXcRWWqWwlW147YHjV7M5c/R8T6daCx4B5NBo6
kdQdQNOrV3IP7kQaCShdM/kCAwEAAaMxMC8wDgYDVR0PAQH/BAQDAgKEMB0GA1Ud
JQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDBTANBgkqhkiG9w0BAQUFAAOBgQCaNi6x
sL6M5NlDezpSBO3QmUVyXMfrONV2ysrSwcXzHu0gJ9MSJ8TwiQmVaJ47hSTlF5a8
YVYJ0IdifXbXRo+/EEO7kkmFE8MZta5rM7UWj8bAeR42iqA3RzQaDwuJgNWT9Fhh
GgfuNAlo5h1Aikxsvxi vmDlLdZyCMoqJJd7B2Q==
quit
Certificate has the following attributes:
Fingerprint MD5: 4B9636DF 0F3BA6B7 5F54BE72 24762DBC
Fingerprint SHA1: A9917775 F86BB37A 5C130ED2 3E528BB8 286E8C2D
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported


Router(config)# crypto pki trustpoint PEM
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate PEM

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDqDCCApCgAwIBAgIQdhL5YBU9b59OQiAgMrcjVjANBgkqhkiG9w0BAQUFADAu
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRQwEgYDVQQDEwtDQVAtUlRQLTAwMTAe
Fw0wMzAyMDYyMzI3MTNaFw0yMzAyMDYyMzM2MzRaMC4xFjAUBgNVBAoTDUNpc2Nv
IFN5c3RlbXMxFDASBgNVBAMTC0NBUC1SVFAtMDAxMIIBIDANBgkqhkiG9w0BAQEF
AAOCAQ0AMIIBCAKCAQEArFW77Rjem4cJ/7yPLVCauDohwZZ/3qf0sJaWlLeAzBlq
Rj2lFlSij0ddkDtfEEo9VKmBOJsvx6xJlWJiuBwUMDhTRbsuJz+npkaGBXPOXJmN
Vd54qlpc/hQDfWlbrIFkCcYhHws7vwnPsLuy1Kw2L2cP0UXxYghSsx8H4vGqdPFQ
NnYy7aKJ43SvDFt4zn37n8jrvlRuz0x3mdbcBEdHbA825Yo7a8sk12tshMJ/YdMm
vny0pmDNZXmeHjqEgVO3UFUn6GVCO+K1y1dUU1qpYJNYtqLkqj7wgccGjsHdHr3a
U+bw1uLgSGsQnxMWeMaWo8+6hMxwlANPweufgZMaywIBA6OBwzCBwDALBgNVHQ8E
BAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQU6Rexgscfz6ypG270qSac
cK4FoJowbwYDVR0fBGgwZjBkoGKgYIYtaHR0cDovL2NhcC1ydHAtMDAxL0NlcnRF
bnJvbGwvQ0FQLVJUUC0wMDEuY3Jshi9maWxlOi8vXFxjYXAtcnRwLTAwMVxDZXJ0
RW5yb2xsXENBUC1SVFAtMDAxLmNybDAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG
9w0BAQUFAAOCAQEAq2T96/YMMtw2Dw4QX+F1+g1XSrUCrNyjx7vtFaRDHyB+kobw
dwkpohfkzfTyYpJELzV1r+kMRoyuZ7oIqqccEroMDnnmeApc+BRGbDJqS1Zzk4OA
c6Ea7fm53nQRlcSPmUVLjDBzKYDNbnEjizptaIC5fgB/S9S6C1q0YpTZFn5tjUjy
WXzeYSXPrcxb0UH7IQJ1ogpONAAUKLoPaZU7tVDSH3hD4+VjmLyysaLUhksGFrrN
phzZrsVVilK17qpqCPllKLGAS4fSbkruq3r/6S/SpXS6/gAoljBKixP7ZW2PxgCU
1aU9cURLPO95NDOFN3jBk3Sips7cVidcogowPQ==
quit

Certificate has the following attributes:
Fingerprint MD5: 233C8E33 8632EA4E 76D79FEB FFB061C6
Fingerprint SHA1: F7B40B94 5831D2AB 447AB8F2 25990732 227631BE
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

show crypto pki trustpoint status コマンドを使用すると、登録が成功し、5 つの CA 証明書が付与されたことが表示されます。5 つの証明書には、入力されたばかりの 3 つの証明書と、CA サーバ証明書、およびルータ証明書が含まれています。

```
Router# show crypto pki trustpoint status
```

```
Trustpoint 7970:
Issuing CA certificate configured:
Subject Name:
cn=CAP-RTP-002,o=Cisco Systems
Fingerprint MD5: F7E150EA 5E6E3AC5 615FC696 66415C9F
Fingerprint SHA1: 1BE2B503 DC72EE28 0C0F6B18 798236D8 D3B18BE6
State:
Keys generated ..... Yes (General Purpose)
Issuing CA authenticated ..... Yes
Certificate request(s) ..... None
Trustpoint 7960:
Issuing CA certificate configured:
Subject Name:
cn=CAPF-508A3754,o=Cisco Systems Inc,c=US
Fingerprint MD5: 6BAE18C2 0BCE391E DAE2FE4C 5810F576
Fingerprint SHA1: B7735A2E 3A5C274F C311D7F1 3BE89942 355102DE
State:
Keys generated ..... Yes (General Purpose)
Issuing CA authenticated ..... Yes
Certificate request(s) ..... None
Trustpoint PEM:
Issuing CA certificate configured:
Subject Name:
cn=CAP-RTP-001,o=Cisco Systems
Fingerprint MD5: 233C8E33 8632EA4E 76D79FEB FFB061C6
Fingerprint SHA1: F7B40B94 5831D2AB 447AB8F2 25990732 227631BE
State:
Keys generated ..... Yes (General Purpose)
Issuing CA authenticated ..... Yes
Certificate request(s) ..... None
Trustpoint srstcaserver:
Issuing CA certificate configured:
Subject Name:
cn=srstcaserver
Fingerprint MD5: 6AF5B084 79C93F2B 76CC8FE6 8781AF5E
Fingerprint SHA1: 47D30503 38FF1524 711448B4 9763FAF6 3A8E7DCF
State:
Keys generated ..... Yes (General Purpose)
Issuing CA authenticated ..... Yes
Certificate request(s) ..... None

Trustpoint srstca:
Issuing CA certificate configured:
Subject Name:
cn=srstcaserver
Fingerprint MD5: 6AF5B084 79C93F2B 76CC8FE6 8781AF5E
Fingerprint SHA1: 47D30503 38FF1524 711448B4 9763FAF6 3A8E7DCF
Router General Purpose certificate configured:
Subject Name:
serialNumber=F3246544+hostname=c2611XM-sSRST.cisco.com
Fingerprint: 35471295 1C907EC1 45B347BC 7A9C4B86
State:
Keys generated ..... Yes (General Purpose)
Issuing CA authenticated ..... Yes
Certificate request(s) ..... Yes
```

Telephony-Service のセキュリティ パラメータ：例

次の例は、Cisco Unified CME のセキュリティ パラメータを示しています。

```
telephony-service
 device-security-mode authenticated
 secure-signaling trustpoint cme-sccp
 tftp-server-credentials trustpoint cme-tftp
 load-cfg-file slot0:Ringlist.xml alias Ringlist.xml sign create

ephone 24
 device-security-mode authenticated
 capf-auth-str 2734
 cert-oper upgrade auth-mode auth-string
```

Cisco Unified CME ルータで実行される CTL クライアント：例

```
ctl-client
 server capf 10.1.1.1 trustpoint cmeserver
 server cme 10.1.1.1 trustpoint cmeserver
 server tftp 10.1.1.1 trustpoint cmeserver
 sast1 trustpoint cmeserver
 sast2 trustpoint sast2CTL Client Running on Another Router: Example
ctl-client
 server cme 10.1.1.100 trustpoint cmeserver
 server cme 10.1.1.1 username cisco password 1 0822455D0A16544541
 sast1 trustpoint cmeserver
 sast2 trustpoint sast1CAPF Server: Example
!
ip dhcp pool cme-pool
   network 10.1.1.0 255.255.255.0
   option 150 ip 10.1.1.1
   default-router 10.1.1.1
!
capf-server
 port 3804
 auth-mode null-string
 cert-enroll-trustpoint iosra password 1 00071A1507545A545C
 trustpoint-label cmeserver
 source-addr 10.1.1.1
!
crypto pki server iosra
 grant auto
 mode ra
 database url slot0:
!
crypto pki trustpoint cmeserver
 enrollment url http://10.1.1.100:80
 serial-number
 revocation-check none
 rsakeypair cmeserver
!
crypto pki trustpoint sast2
 enrollment url http://10.1.1.100:80
 serial-number
 revocation-check none
 rsakeypair sast2
!
```

```
!
crypto pki trustpoint iosra
 enrollment url http://10.1.1.200:80
 revocation-check none
 rsakeypair iosra
!
!
crypto pki certificate chain cmeserver
 certificate 1B
  30820207 30820170 A0030201 0202011B 300D0609 2A864886 F70D0101 04050030
  ....
  quit
 certificate ca 01
  3082026B 308201D4 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  ...
  quit
crypto pki certificate chain sast2
 certificate 1C
  30820207 30820170 A0030201 0202011C 300D0609 2A864886 F70D0101 04050030
  ....
  quit
 certificate ca 01
  3082026B 308201D4 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  .....
  quit
crypto pki certificate chain capf-tp
crypto pki certificate chain iosra
 certificate 04
  30820201 3082016A A0030201 02020104 300D0609 2A864886 F70D0101 04050030
  ......
 certificate ca 01
  308201F9 30820162 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  ....
  quit
!
!
credentials
 ctl-service admin cisco secret 1 094F471A1A0A464058
 ip source-address 10.1.1.1 port 2444
 trustpoint cmeserver
!
!
telephony-service
 no auto-reg-ephone
 load 7960-7940 P00307010200
 load 7914 S00104000100
 load 7941GE TERM41.7-0-0-129DEV
 load 7970 TERM70.7-0-0-77DEV
 max-ephones 20
 max-dn 10
 ip source-address 10.1.1.1 port 2000 secondary 10.1.1.100
 secure-signaling trustpoint cmeserver
 cnf-file location flash:
 cnf-file perphone
 dialplan-pattern 1 2... extension-length 4
 max-conferences 8 gain -6
 transfer-pattern ....
 tftp-server-credentials trustpoint cmeserver
 server-security-mode secure
 device-security-mode encrypted
 load-cfg-file slot0:Ringlist.xml alias Ringlist.xml sign
 load-cfg-file slot0:P00307010200.bin alias P00307010200.bin
 load-cfg-file slot0:P00307010200.loads alias P00307010200.loads
 load-cfg-file slot0:P00307010200.sb2 alias P00307010200.sb2
```

```
 load-cfg-file slot0:P00307010200.sbn alias P00307010200.sbn
 load-cfg-file slot0:cnu41.2-7-4-116dev.sbn alias cnu41.2-7-4-116dev.sbn
 load-cfg-file slot0:Jar41.2-9-0-101dev.sbn alias Jar41.2-9-0-101dev.sbn
 load-cfg-file slot0:CVM41.2-0-0-96dev.sbn alias CVM41.2-0-0-96dev.sbn
 load-cfg-file slot0:TERM41.DEFAULT.loads alias TERM41.DEFAULT.loads
 load-cfg-file slot0:TERM70.DEFAULT.loads alias TERM70.DEFAULT.loads
 load-cfg-file slot0:Jar70.2-9-0-54dev.sbn alias Jar70.2-9-0-54dev.sbn
 load-cfg-file slot0:cnu70.2-7-4-58dev.sbn alias cnu70.2-7-4-58dev.sbn
 load-cfg-file slot0:CVM70.2-0-0-49dev.sbn alias CVM70.2-0-0-49dev.sbn
 load-cfg-file slot0:DistinctiveRingList.xml alias DistinctiveRingList.xml sign
 load-cfg-file slot0:Piano1.raw alias Piano1.raw sign
 load-cfg-file slot0:S00104000100.sbn alias S00104000100.sbn
 create cnf-files version-stamp 7960 Aug 13 2005 12:39:24
!
!
ephone  1
 device-security-mode encrypted
 cert-oper upgrade auth-mode null-string
 mac-address 000C.CE3A.817C
 type 7960 addon 1 7914
 button  1:2 8:8
!
!
ephone  2
 device-security-mode encrypted
 capf-auth-str 2476
 cert-oper upgrade auth-mode null-string
 mac-address 0011.2111.6BDD
 type 7970
 button  1:1
!
!
ephone  3
 device-security-mode encrypted
 capf-auth-str 5425
 cert-oper upgrade auth-mode null-string
 mac-address 000D.299D.50DF
 type 7970
 button  1:3
!
!
ephone  4
 device-security-mode encrypted
 capf-auth-str 7176
 cert-oper upgrade auth-mode null-string
 mac-address 000E.D7B1.0DAC
 type 7960
 button  1:4
!
!
ephone  5
 device-security-mode encrypted
 mac-address 000F.9048.5077
 type 7960
 button  1:5
!
!
ephone  6
 device-security-mode encrypted
 mac-address 0013.C352.E7F1
 type 7941GE
 button  1:6
!
```

セキュア Cisco Unified CME：例

```
Router# show running-config

Building configuration...

Current configuration : 12735 bytes
!
! No configuration change since last restart
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname Router
!
boot-start-marker
boot-end-marker
!
card type e1 1 1
logging queue-limit 10000
logging buffered 9999999 debugging
logging rate-limit 10000
no logging console
!
aaa new-model
!
!
aaa accounting connection h323 start-stop group radius
!
aaa session-id common
!
resource policy
!
clock timezone IST 5
no network-clock-participate slot 1
!
!
ip cef
!
!
isdn switch-type primary-net5
!
voice-card 0
 no dspfarm
!
voice-card 1
 no dspfarm
!
!
ctl-client
 server capf 10.13.32.11 trustpoint mytrustpoint1
 server tftp 10.13.32.11 trustpoint mytrustpoint1
 server cme 10.13.32.11 trustpoint mytrustpoint1
 sast1 trustpoint mytrustpoint1
 sast2 trustpoint sast2
!
capf-server
 port 3084
 auth-mode null-string
 cert-enroll-trustpoint iosra password 1 mypassword
```

```
 trustpoint-label mytrustpoint1
 source-addr 10.13.32.11
 phone-key-size 512
!
voice call debug full-guid
!
voice service voip
 srtp fallback
 allow-connections h323 to h323
 no supplementary-service h450.2
 no supplementary-service h450.3
 no supplementary-service h450.7
 supplementary-service media-renegotiate
 h323
  emptycapability
  ras rrq ttl 4000
!
!
voice class codec 2
 codec preference 1 g711alaw
 codec preference 2 g711ulaw
!
voice class codec 3
 codec preference 1 g729r8
 codec preference 8 g711alaw
 codec preference 9 g711ulaw
!
voice class codec 1
 codec preference 1 g729r8
 codec preference 2 g728
 codec preference 3 g723ar63
 codec preference 4 g711ulaw
!
!
voice iec syslog
voice statistics type iec
voice statistics time-range since-reset
!
!
!
crypto pki server myra
 database level complete
 grant auto
 lifetime certificate 1800
!
crypto pki trustpoint myra
 enrollment url http://10.13.32.11:80
 revocation-check none
 rsakeypair iosra
!
crypto pki trustpoint mytrustpoint1
 enrollment url http://10.13.32.11:80
 revocation-check none
 rsakeypair mytrustpoint1
!
crypto pki trustpoint sast2
 enrollment url http://10.13.32.11:80
 revocation-check none
 rsakeypair sast2
!
!
crypto pki certificate chain myra
 certificate ca 01
  308201F9 30820162 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
```

```
  10310E30 0C060355 04031305 696F7372 61301E17 0D303630 37303730 35343031
  375A170D 30393037 30363035 34303137 5A301031 0E300C06 03550403 1305696F
  73726130 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100
  D8CE29F9 C9FDB1DD 0E1517E3 6CB4AAF7 52B83DE2 1C017ACA DFC4AF42 F9D10D08
  E74BF95B 29378902 B49E32C4 85907384 84CAE4B2 7759BB84 8AB1F578 580793C4
  B11A2DBE B2ED02CC DA0C3824 A5FCC377 18CE87EA C0C297BA BE54530F E62247D8
  1483CD14 9FD89EFE 05DFBB37 E03FD3F8 B2B1C0B8 A1931BCC B1174A9E 6566F8F5
  02030100 01A36330 61300F06 03551D13 0101FF04 05300301 01FF300E 0603551D
  0F0101FF 04040302 0186301F 0603551D 23041830 168014B7 16F6FD67 29666C90
  D0C62515 E14265A9 EB256230 1D060355 1D0E0416 0414B716 F6FD6729 666C90D0
  C62515E1 4265A9EB 2562300D 06092A86 4886F70D 01010405 00038181 002B7F41
  64535A66 D20D888E 661B9584 5E3A28DF 4E5A95B9 97E57CAE B07A7C38 7F3B60EE
  75C7E5DE 6DF19B06 5F755FB5 190BABFC EF272CEF 865FE01B 1CE80F98 F320A569
  CAFFA5D9 3DB3E7D8 8A86C66C F227FF81 6C4449F2 AF8015D9 8129C909 81AFDC01
  180B61E8 85E19873 96DB3AE3 E6B70726 9BF93521 CA2FA906 99194ECA 8F
  quit
crypto pki certificate chain mytrustpoint1
 certificate 02
  308201AB 30820114 A0030201 02020102 300D0609 2A864886 F70D0101 04050030
  10310E30 0C060355 04031305 696F7372 61301E17 0D303630 37303730 35343233
  385A170D 30393037 30363035 34303137 5A301A31 18301606 092A8648 86F70D01
  09021609 32383531 2D434D45 32305C30 0D06092A 864886F7 0D010101 0500034B
  00304802 4100B3ED A902646C 3851B7F6 CF94887F 0EC437E3 3B6FEDB2 2B4B45A6
  3611C243 5A0759EA 1E8D96D1 60ABE028 ED6A3F2A E95DCE45 BE0921AF 82E53E57
  17CC12F0 C1270203 010001A3 4F304D30 0B060355 1D0F0404 030205A0 301F0603
  551D2304 18301680 14B716F6 FD672966 6C90D0C6 2515E142 65A9EB25 62301D06
  03551D0E 04160414 4EE1943C EA817A9E 7010D5B8 0467E9B0 6BA76746 300D0609
  2A864886 F70D0101 04050003 81810003 564A6DA1 868B2669 7C096F9A 41173CFC
  E49246EE C645E30B A0753E3B E1A265D1 6EA5A829 F10CD0E8 3F2E3AD4 39D8DFE8
  83525F2B D19F5E15 F27D6262 62852D1F 43629B68 86D91B5F 7B2E2C25 3BD2CCC3
  00EF4028 714339B2 6A7E0B2F 131D2D9E 0BE08853 5CCAE47C 4F74953C 19305A20
  B2C97808 D6E01351 48366421 A1D407
  quit
 certificate ca 01
  308201F9 30820162 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  10310E30 0C060355 04031305 696F7372 61301E17 0D303630 37303730 35343031
  375A170D 30393037 30363035 34303137 5A301031 0E300C06 03550403 1305696F
  73726130 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100
  D8CE29F9 C9FDB1DD 0E1517E3 6CB4AAF7 52B83DE2 1C017ACA DFC4AF42 F9D10D08
  E74BF95B 29378902 B49E32C4 85907384 84CAE4B2 7759BB84 8AB1F578 580793C4
  B11A2DBE B2ED02CC DA0C3824 A5FCC377 18CE87EA C0C297BA BE54530F E62247D8
  1483CD14 9FD89EFE 05DFBB37 E03FD3F8 B2B1C0B8 A1931BCC B1174A9E 6566F8F5
  02030100 01A36330 61300F06 03551D13 0101FF04 05300301 01FF300E 0603551D
  0F0101FF 04040302 0186301F 0603551D 23041830 168014B7 16F6FD67 29666C90
  D0C62515 E14265A9 EB256230 1D060355 1D0E0416 0414B716 F6FD6729 666C90D0
  C62515E1 4265A9EB 2562300D 06092A86 4886F70D 01010405 00038181 002B7F41
  64535A66 D20D888E 661B9584 5E3A28DF 4E5A95B9 97E57CAE B07A7C38 7F3B60EE
  75C7E5DE 6DF19B06 5F755FB5 190BABFC EF272CEF 865FE01B 1CE80F98 F320A569
  CAFFA5D9 3DB3E7D8 8A86C66C F227FF81 6C4449F2 AF8015D9 8129C909 81AFDC01
  180B61E8 85E19873 96DB3AE3 E6B70726 9BF93521 CA2FA906 99194ECA 8F
  quit
crypto pki certificate chain sast2
 certificate 03
  308201AB 30820114 A0030201 02020103 300D0609 2A864886 F70D0101 04050030
  10310E30 0C060355 04031305 696F7372 61301E17 0D303630 37303730 35343331
  375A170D 30393037 30363035 34303137 5A301A31 18301606 092A8648 86F70D01
  09021609 32383531 2D434D45 32305C30 0D06092A 864886F7 0D010101 0500034B
  00304802 4100C703 840B11A7 81FCE5AE A14FE593 5114D3C2 5473F488 B8FB4CC5
  41EAFA3A D99381D8 21AE6AA9 BA83A84E 9DF3E8C6 54978787 5EF6CC35 C334D55E
  A3051372 17D30203 010001A3 4F304D30 0B060355 1D0F0404 030205A0 301F0603
  551D2304 18301680 14B716F6 FD672966 6C90D0C6 2515E142 65A9EB25 62301D06
  03551D0E 04160414 EB2146B4 EE24AA61 8B5D2F8D 2AD3B786 CBADC8F2 300D0609
  2A864886 F70D0101 04050003 81810057 BA0053E9 8FD54B25 72D85A4C CAB47F26
  8316F494 E94DFFB9 8E9D065C 9748465C F54719CA C7724F50 67FBCAFF BC332109
```

```
  DC2FB93D 5AD86583 EDC3E648 39274CE8 D4A5F002 5F21ED3C 6D524AB7 7F5B1876
  51867027 9BD2FFED 06984558 C903064E 5552015F 289BA9BB 308D327A DFE0A3B9
  78CF2B02 2DD4C208 80CDC0A8 43A26A
  quit
 certificate ca 01
  308201F9 30820162 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  10310E30 0C060355 04031305 696F7372 61301E17 0D303630 37303730 35343031
  375A170D 30393037 30363035 34303137 5A301031 0E300C06 03550403 1305696F
  73726130 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100
  D8CE29F9 C9FDB1DD 0E1517E3 6CB4AAF7 52B83DE2 1C017ACA DFC4AF42 F9D10D08
  E74BF95B 29378902 B49E32C4 85907384 84CAE4B2 7759BB84 8AB1F578 580793C4
  B11A2DBE B2ED02CC DA0C3824 A5FCC377 18CE87EA C0C297BA BE54530F E62247D8
  1483CD14 9FD89EFE 05DFBB37 E03FD3F8 B2B1C0B8 A1931BCC B1174A9E 6566F8F5
  02030100 01A36330 61300F06 03551D13 0101FF04 05300301 01FF300E 0603551D
  0F0101FF 04040302 0186301F 0603551D 23041830 168014B7 16F6FD67 29666C90
  D0C62515 E14265A9 EB256230 1D060355 1D0E0416 0414B716 F6FD6729 666C90D0
  C62515E1 4265A9EB 2562300D 06092A86 4886F70D 01010405 00038181 002B7F41
  64535A66 D20D888E 661B9584 5E3A28DF 4E5A95B9 97E57CAE B07A7C38 7F3B60EE
  75C7E5DE 6DF19B06 5F755FB5 190BABFC EF272CEF 865FE01B 1CE80F98 F320A569
  CAFFA5D9 3DB3E7D8 8A86C66C F227FF81 6C4449F2 AF8015D9 8129C909 81AFDC01
  180B61E8 85E19873 96DB3AE3 E6B70726 9BF93521 CA2FA906 99194ECA 8F
  quit
!
!
username admin password 0 mypassword2
username cisco password 0 mypassword2
!
!
controller E1 1/0
 pri-group timeslots 1-31
!
controller E1 1/1
 pri-group timeslots 1-31
gw-accounting aaa
!
!
!
!
!
interface GigabitEthernet0/0
 ip address 10.13.32.11 255.255.255.0
 duplex auto
 speed auto
 fair-queue 64 256 32
 h323-gateway voip interface
 h323-gateway voip id GK1 ipaddr 10.13.32.13 1719
 h323-gateway voip id GK2 ipaddr 10.13.32.16 1719
 h323-gateway voip h323-id 2851-CiscoUnifiedCME
 h323-gateway voip tech-prefix 1#
 ip rsvp bandwidth 1000 100
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial1/0:15
 no ip address
 encapsulation hdlc
 isdn switch-type primary-net5
 isdn protocol-emulate network
 isdn incoming-voice voice
 no cdp enable
```

```
!
interface Serial1/1:15
 no ip address
 encapsulation hdlc
 isdn switch-type primary-net5
 isdn protocol-emulate network
 isdn incoming-voice voice
 no cdp enable
!
ip route 0.0.0.0 0.0.0.0 10.13.32.1
!
!
ip http server
ip http authentication local
no ip http secure-server
ip http path flash:
!
!
!
!
!
!
tftp-server flash:music-on-hold.au
tftp-server flash:TERM70.DEFAULT.loads
tftp-server flash:TERM71.DEFAULT.loads
tftp-server flash:P00308000300.bin
tftp-server flash:P00308000300.loads
tftp-server flash:P00308000300.sb2
tftp-server flash:P00308000300.sbn
tftp-server flash:SCCP70.8-0-3S.loads
tftp-server flash:cvm70sccp.8-0-2-25.sbn
tftp-server flash:apps70.1-1-2-26.sbn
tftp-server flash:dsp70.1-1-2-26.sbn
tftp-server flash:cnu70.3-1-2-26.sbn
tftp-server flash:jar70sccp.8-0-2-25.sbn
radius-server host 10.13.32.241 auth-port 1645 acct-port 1646
radius-server timeout 40
radius-server deadtime 2
radius-server key cisco
radius-server vsa send accounting
!
control-plane
!
no call rsvp-sync
!
!
voice-port 1/0/0
!
voice-port 1/0/1
!
voice-port 1/0:15
!
voice-port 1/1:15
!
!
!
!
!
dial-peer voice 1 voip
 destination-pattern ........
 voice-class codec 2
 session target ras
 incoming called-number 9362....
 dtmf-relay h245-alphanumeric
```

```
 req-qos controlled-load audio
!
dial-peer voice 2 pots
 destination-pattern 93621101
!
dial-peer voice 3 pots
 destination-pattern 93621102
!
dial-peer voice 10 voip
 destination-pattern 2668....
 voice-class codec 1
 session target ipv4:10.13.46.200
!
dial-peer voice 101 voip
 shutdown
 destination-pattern 5694....
 voice-class codec 1
 session target ipv4:10.13.32.10
 incoming called-number 9362....
!
dial-peer voice 102 voip
 shutdown
 destination-pattern 2558....
 voice-class codec 1
 session target ipv4:10.13.32.12
 incoming called-number 9362....
!
dial-peer voice 103 voip
 shutdown
 destination-pattern 9845....
 voice-class codec 1
 session target ipv4:10.13.32.14
 incoming called-number 9362....
!
dial-peer voice 104 voip
 shutdown
 destination-pattern 9844....
 voice-class codec 1
 session target ipv4:10.13.32.15
 incoming called-number 9362....
!
dial-peer voice 201 pots
 destination-pattern 93625...
 no digit-strip
 direct-inward-dial
 port 1/0:15
!
dial-peer voice 202 pots
 destination-pattern 93625...
 no digit-strip
 direct-inward-dial
 port 1/1:15
!
!
gateway
 timer receive-rtp 1200
!
!
!
telephony-service
 load 7960-7940 P00308000300
 max-ephones 4
 max-dn 4
 ip source-address 10.13.32.11 port 2000
```

```
 auto assign 1 to 4
 secure-signaling trustpoint mytrustpoint1
 cnf-file location flash:
 cnf-file perphone
 voicemail 25589000
 max-conferences 4 gain -6
 call-forward pattern .T
 moh flash:music-on-hold.au
 web admin system name admin password mypassword2
 dn-webedit
 time-webedit
 transfer-system full-consult
 transfer-pattern ........
 tftp-server-credentials trustpoint mytrustpoint1
 server-security-mode secure
 device-security-mode encrypted
 create cnf-files version-stamp 7960 Oct 25 2006 07:19:39
!
!
ephone-dn  1
 number 93621000
 name 2851-PH1
 call-forward noan 25581101 timeout 10
!
!
ephone-dn  2
 number 93621001
 name 2851-PH2
 call-forward noan 98441000 timeout 10
!
!
ephone-dn  3
 number 93621002
 name 2851-PH3
!
!
ephone-dn  4
 number 93621003
 name 2851-PH4
!
!
ephone  1
 no multicast-moh
 device-security-mode encrypted
 mac-address 0012.4302.A7CC
 type 7970
 button  1:1
!
!
!
ephone  2
 no multicast-moh
 device-security-mode encrypted
 mac-address 0017.94CA.9CCD
 type 7960
 button  1:2
!
!
!
ephone  3
 no multicast-moh
 device-security-mode encrypted
 mac-address 0017.94CA.9833
 type 7960
```

```
 button  1:3
!
!
!
ephone  4
 no multicast-moh
 device-security-mode none
 mac-address 0017.94CA.A141
 type 7960
 button  1:4
!
!
!
line con 0
 logging synchronous level all limit 20480000
line aux 0
line vty 0 4
!
scheduler allocate 20000 1000
ntp clock-period 17179791
ntp server 10.13.32.12
!
webvpn context Default_context
 ssl authenticate verify all
 !
 no inservice
!
!
end
```

次の作業

PKI 管理

Cisco IOS 公開キー インフラストラクチャ（PKI）を使用すると、IP セキュリティ（IPsec）、セキュアシェル（SSH）、Secure Socket Layer（SSL）などのセキュリティ プロトコルをサポートする証明書管理を実現できます。詳細については、次のマニュアルを参照してください。

- 『*Cisco IOS Security Configuration Guide*』の「*Implementing and Managing a PKI Features Roadmap*」
- *『Cisco IOS Security Command Reference』*

Cisco VG224 Analog Phone Gateway

- Cisco VG224 Analog Phone Gateway にセキュアなエンドポイントを設定するには、『*Supplementary Services Features for FXS Ports on Cisco IOS Voice Gateways Configuration Guide, Release 12.4T*』の「Configuring Secure Signalling and Media Encryption on the Cisco VG224」の項を参照してください。

その他の参考資料

次の各項では、Cisco Unified CME 機能に関連するその他の資料について説明します。

関連資料

関連項目	参照先
Cisco Unified CME の設定	• *『Cisco Unified CME Command Reference』* • 『Cisco Unified CME Documentation Roadmap』
Cisco IOS コマンド	• *『Cisco IOS Voice Command Reference』* • 『Cisco IOS Software Releases 12.4T Command References』
Cisco IOS の設定	• *『Cisco IOS Voice Configuration Library』* • 『Cisco IOS Software Releases 12.4T Configuration Guides』
Cisco VG224 Analog Phone Gateway	• *『Supplementary Services Features for FXS Ports on Cisco IOS Voice Gateways Configuration Guide, Cisco IOS Release 15.1M&T』* • *『Cisco VG224 Voice Gateway Software Configuration Guide』*
Cisco Unified CME 用の電話機のマニュアル	• 『User Documentation for Cisco Unified IP Phones』

シスコのテクニカル サポート

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

セキュリティの機能情報

表 53 に、このモジュールで説明した機能、およびバージョンごとの拡張機能を示します。

特定の Cisco Unified CME バージョンをサポートするための適切な Cisco IOS リリースを判断するには、http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/requirements/guide/33matrix.htm にある『*Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix*』を参照してください

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator では、特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートしている Cisco IOS ソフトウェア イメージを確認できます。Cisco Feature Navigator にアクセスするには、http://www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

（注） 表 53 には、特定の機能に対するサポートを導入した Cisco Unified CME のバージョンが示されています。特に明記されていない限り、Cisco Unified CME ソフトウェアの後続のバージョンでもこの機能をサポートします。

表 53　セキュリティの機能情報

機能名	Cisco Unified CME バージョン	機能情報
Cisco Unified IP Phone 用の HTTPS プロビジョニング	8.8	**import certificate** コマンドを使用して、IP Phone の信頼できる証明書を IP Phone の CTL ファイルにインポートできます。
Cisco Unified CME でのメディア暗号化（SRTP）	4.2	Cisco Unified CME でのメディア暗号化が導入されました。
電話機認証	4.0	Cisco Unified CME の電話機に電話機認証が導入されました。