CHAPTER 3

Cisco CTL クライアントの設定

この章は、次の内容で構成されています。

- Cisco CTL クライアントの概要（P.3-2）
- Cisco CTL クライアントの設定のヒント（P.3-3）
- Cisco CTL クライアントの設定用チェックリスト（P.3-4）
- Cisco CTL Provider サービスのアクティブ化（P.3-5）
- Cisco CAPF サービスのアクティブ化（P.3-6）
- TLS 接続用ポートの設定（P.3-6）
- Cisco CTL クライアントのインストール（P.3-8）
- Cisco CTL クライアントのアップグレードおよび Cisco CTL ファイルの移行（P.3-10）
- Cisco CTL クライアントの設定（P.3-11）
- CTL ファイルの更新（P.3-15）
- CTL ファイル エントリの削除（P.3-17）
- Cisco Unified Communications Manager セキュリティ モードの更新（P.3-17）
- Cisco CTL クライアントの設定内容（P.3-18）
- Cisco Unified Communications Manager のセキュリティ モードの確認（P.3-21）
- Smart Card サービスの開始および自動の設定（P.3-22）
- セキュリティ トークン パスワード（etoken）の変更（P.3-23）
- Cisco Unified IP Phone 上の CTL ファイルの削除（P.3-24）
- Cisco CTL クライアントのバージョンの特定（P.3-25）
- Cisco CTL クライアントの確認とアンインストール（P.3-25）
- その他の情報（P.3-26）

Cisco CTL クライアントの概要

デバイス認証、ファイル認証、およびシグナリング認証は、Certificate Trust List（CTL; 証明書信頼リスト）ファイルの作成に依存します。このファイルは、USB ポートのある単一の Windows ワークステーションまたはサーバに Cisco Certificate Trust List（CTL）クライアントをインストールおよび設定したときに作成されます。

（注）　Cisco CTL クライアント用としてサポートされる Windows のバージョンは、Windows 2000 と Windows XP です。Terminal Services は、Cisco CTL クライアントのインストールに使用しないでください。シスコは、Cisco Technical Assistance Center（TAC）がリモートでトラブルシューティングおよび設定作業を行えるように Terminal Services をインストールしています。

CTL ファイルには、次のサーバまたはセキュリティ トークンのためのエントリが含まれています。

- Site Administrator Security Token（SAST）
- 同一のサーバで実行される Cisco CallManager および Cisco Tftp
- Certificate Authority Proxy Function（CAPF）
- PIX Firewall

CTL ファイルには、各サーバのサーバ証明書、公開鍵、シリアル番号、シグニチャ、発行者名、件名、サーバ機能、DNS 名、および IP アドレスが含まれます。

CTL ファイルを作成したら、Cisco Unified Serviceability で Cisco CallManager および Cisco Tftp サービスを再起動する必要があります。次回、電話機を初期化するときには、CTL ファイルが TFTP サーバからダウンロードされます。CTL ファイルに自己署名証明書を持つ TFTP サーバ エントリが含まれている場合、電話機は .sgn 形式の署名付き設定ファイルを要求します。どの TFTP サーバにも証明書がない場合、電話機は署名なしファイルを要求します。

Cisco CTL クライアントが CTL ファイルにサーバ証明書を追加すると、CTL クライアントの GUI にこの証明書を表示できます。

ファイアウォールを CTL ファイルに設定すると、セキュアな Cisco Unified Communications Manager システムの一部として Cisco PIX Firewall を保護できます。Cisco CTL クライアントは、ファイアウォール証明書を「CCM」証明書として表示します。

Cisco Unified Communications Manager の管理ページは、etoken を使用して、CTL クライアントとプロバイダーとの間の TLS 接続を認証します。

Cisco CTL クライアントの設定のヒント

Cisco Unified Communications Manager の管理ページで Cisco CTL クライアントを設定する場合は、次の点を考慮してください。

- Cisco Unified Communications Manager ノードのホスト名が、Cisco CTL クライアントがインストールされているリモート PC で解決可能であることを確認します。解決可能でない場合、Cisco CTL クライアントは正しく動作しません。
- Cisco CTL Provider サービスをアクティブにする必要があります。クラスタ環境がある場合は、クラスタ内のすべてのサーバで Cisco CTL Provider サービスをアクティブにする必要があります。
- CTL ファイルを作成または更新したら、これらのサービスを実行するすべての Cisco Unified Communications Manager サーバおよびクラスタ内のすべての TFTP サーバで Cisco Unified Serviceability を使用して、Cisco CallManager サービスおよび Cisco Tftp サービスを再起動する必要があります。
- Cisco CTL クライアントに、代替 TFTP サーバまたは集中 TFTP サーバなどのクラスタ外サーバのエントリが含まれている場合、これらのサーバでも Cisco CTL Provider サービスを実行する必要があります。
- CTL クライアント GUI の 代替 TFTP サーバのセクションで、別のクラスタに存在する Cisco TFTP サーバを指定します。［Alternate TFTP Server］タブの設定値を使用して、代替 TFTP サーバおよび集中 TFTP サーバを CTL クライアントに設定します。

（注）　クラスタ外の（代替および集中）TFTP サーバの設定方法の詳細については、『*Cisco Unified Communications Manager システム ガイド*』の「Cisco TFTP」を参照してください。

- 集中 TFTP 設定では、混合モードで動作するすべてのクラスタ外 TFTP サーバで、マスター TFTP サーバまたはマスター TFTP サーバの IP アドレスをクラスタ外 CTL ファイルに追加する必要があります。マスター TFTP サーバで、マスター TFTP サーバ用に設定された代替ファイル リスト内のすべての代替 TFTP サーバの設定ファイルを処理します。集中 TFTP 設定のクラスタすべてで同じセキュリティ モードを使用する必要はありません。各クラスタで独自のモードを選択できます。

Cisco CTL クライアントの設定用チェックリスト

表 3-1 に、初めて Cisco CTL クライアントをインストールおよび設定する場合に実行する設定作業のリストを示します。Cisco Unified Communications Manager をアップグレードするときの CTL ファイル設定の詳細については、P.3-10 の「Cisco CTL クライアントのアップグレードおよび Cisco CTL ファイルの移行」を参照してください。

表 3-1　Cisco CTL クライアントの設定用チェックリスト

設定手順		関連手順および関連項目
ステップ 1	Cisco Unified Serviceability で Cisco CTL Provider サービスをアクティブにします。 クラスタ内の各 Cisco Unified Communications Manager サーバで Cisco CTL Provider サービスをアクティブにします。 **ヒント**　Cisco Unified Communications Manager のアップグレード前にこのサービスをアクティブにした場合は、サービスを再度アクティブにする必要はありません。アップグレード後にサービスは自動的にアクティブになります。	Cisco CTL Provider サービスのアクティブ化（P.3-5）
ステップ 2	Cisco Unified Serviceability で Cisco Certificate Authority Proxy サービスをアクティブにします。 **ヒント**　クラスタ内の最初のノードでのみ Cisco Certificate Authority Proxy サービスをアクティブにします。 **ワンポイント・アドバイス**　Cisco CTL クライアントをインストールして設定する前にこの作業を実行すれば、CAPF を使用するために CTL ファイルを更新する必要がなくなります。	Certificate Authority Proxy Function サービスのアクティブ化（P.6-6）
ステップ 3	デフォルト設定を使用しない場合は、TLS 接続用のポートを設定します。 **ヒント**　これらの設定を Cisco Unified Communications Manager のアップグレード前に設定した場合、設定は自動的に移行されます。	TLS 接続用ポートの設定（P.3-6）
ステップ 4	Cisco CTL クライアント用に設定するサーバについて、少なくとも 2 つのセキュリティ トークンとパスワード、ホスト名または IP アドレス、およびポート番号を入手します。	Cisco CTL クライアントの設定（P.3-11）
ステップ 5	Cisco CTL クライアントをインストールします。	• システム要件（P.1-5） • インストール（P.1-15） • Cisco CTL クライアントのインストール（P.3-8）
ステップ 6	Cisco CTL クライアントを設定します。	Cisco CTL クライアントの設定（P.3-11）

Cisco CTL Provider サービスのアクティブ化

Cisco CTL クライアントの設定後、Cisco CTL Provider サービスによってセキュリティ モードが非セキュア モードから混合モードに変更され、サーバ証明書が CTL ファイルに転送されます。その後、このサービスによって、CTL ファイルがすべての Cisco Unified Communications Manager および Cisco TFTP サーバに転送されます。

サービスをアクティブにしてから Cisco Unified Communications Manager をアップグレードした場合、Cisco Unified Communications Manager によってサービスはアップグレード後に自動的に再度アクティブになります。

ヒント　クラスタ内のすべてのサーバで Cisco CTL Provider サービスをアクティブにする必要があります。

サービスをアクティブにするには、次の手順を実行します。

手順

ステップ 1　Cisco Unified Serviceability で、［**Tools**］>［**Service Activation**］の順に選択します。

ステップ 2　［Server］ドロップダウン リスト ボックスで、Cisco Unified Communications Manager サービスまたは Cisco TFTP サービスをアクティブにしたサーバを選択します。

ステップ 3　［**Cisco CTL Provider**］サービス オプション ボタンをクリックします。

ステップ 4　［**Save**］をクリックします。

ヒント　クラスタ内のすべてのサーバで、この手順を実行します。

（注）　Cisco CTL Provider サービスをアクティブにする前に、CTL ポートを入力できます。デフォルトのポート番号を変更する場合は、P.3-6 の「TLS 接続用ポートの設定」を参照してください。

ステップ 5　サービスがサーバで実行されていることを確認します。サービスの状態を確認するには、Cisco Unified Serviceability で［**Tools**］>［**Control Center - Feature Services**］の順に選択します。

追加情報

詳細については、P.3-26 の「関連項目」を参照してください。

Cisco CAPF サービスのアクティブ化

このサービスのアクティブ化については、P.6-6 の「Certificate Authority Proxy Function サービスのアクティブ化」を参照してください。

ワンポイント・アドバイス　Cisco CTL クライアントをインストールして設定する前にこの作業を実行すれば、CAPF を使用するために CTL ファイルを更新する必要がなくなります。

TLS 接続用ポートの設定

デフォルトのポートが現在使用中の場合や、ファイアウォールを使用していてファイアウォール内のポートを使用できない場合には、異なる TLS ポート番号の設定が必要になることもあります。

- Cisco CTL Provider の TLS 接続用デフォルト ポートは 2444 です。Cisco CTL Provider ポートでは Cisco CTL クライアントからの要求を監視します。このポートでは、CTL ファイルの取得、セキュリティ モードの設定、CTL ファイルの TFTP サーバへの保存など、Cisco CTL クライアントの要求を処理します。
- Ethernet Phone ポートは、SCCP 電話機からの登録要求を監視します。非セキュア モードの場合、電話機はポート 2000 を介して接続されます。混合モードの場合、Cisco Unified Communications Manager の TLS 接続用ポートは Cisco Unified Communications Manager ポート番号に 443 を加算（+）した番号になるため、Cisco Unified Communications Manager のデフォルトの TLS 接続は 2443 になります。ポートが現在使用中の場合や、ファイアウォールを使用していてファイアウォール内のポートを使用できない場合にのみ、この設定を更新します。
- SIP セキュア ポートを使用すると、Cisco Unified Communications Manager は SIP 電話機からの SIP メッセージを傍受できます。デフォルト値は 5061 です。このポートを変更した場合は、Cisco Unified Serviceability で Cisco CallManager サービスを再起動し、SIP 電話機をリセットする必要があります。

ヒント　ポートを更新した後は、Cisco Unified Serviceability で Cisco CTL Provider サービスを再起動する必要があります。

CTL ポートは、CTL クライアントが実行されているデータ VLAN に対して開いている必要があります。Cisco Unified Communications Manager にシグナルを戻すために TLS を実行している電話機も CTL クライアントが使用するポートを使用します。これらのポートは、電話機が認証済みステータスまたは暗号化済みステータスに設定されているすべての VLAN に対して必ず開いてください。

デフォルト設定を変更するには、次の手順を実行します。

手順

ステップ 1　変更するポートに応じて、次の作業を実行します。

- Cisco CTL Provider サービスの Port Number パラメータを変更するには、ステップ 2 ～ステップ 6 を実行します。
- ［イーサネット電話ポート（Ethernet Phone Port）］または［SIP 電話セキュアポート（SIP Phone Secure Port）］の設定を変更するには、ステップ 7 ～ステップ 11 を実行します。

ステップ 2　Cisco CTL Provider ポートを変更するには、Cisco Unified Communications Manager の管理ページで［システム］>［サービスパラメータ］の順に選択します。

ステップ 3　［サーバ（Server）］ドロップダウン リスト ボックスで、Cisco CTL Provider サービスを実行しているサーバを選択します。

ステップ 4　［サービス（Service）］ドロップダウン リスト ボックスで、**Cisco CTL Provider** サービスを選択します。

ヒント　サービス パラメータの詳細については、疑問符またはリンク名をクリックしてください。

ステップ 5　Port Number パラメータの値を変更するには、［パラメータ値（Parameter Value）］フィールドに新しいポート番号を入力します。

ステップ 6　［保存］をクリックします。

ステップ 7　［イーサネット電話ポート（Ethernet Phone Port）］または［SIP 電話セキュアポート（SIP Phone Secure Port）］の設定を変更するには、Cisco Unified Communications Manager の管理ページで［システム］>［Cisco Unified CM］の順に選択します。

ステップ 8　『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の説明に従い、Cisco CallManager サービスを実行しているサーバを検索します。結果が表示されたら、サーバの［名前（Name）］リンクをクリックします。

ステップ 9　［Cisco Unified Communications Manager の設定（Cisco Unified CallManager Configuration）］ウィンドウが表示されたら、［イーサネット電話ポート（Ethernet Phone Port）］フィールドまたは［SIP 電話セキュアポート（SIP Phone Secure Port）］フィールドに新しいポート番号を入力します。

ステップ 10　電話機をリセットし、Cisco Unified Serviceability で Cisco CallManager サービスを再起動します。

ステップ 11　［保存］をクリックします。

追加情報

詳細については、P.3-26 の「関連項目」を参照してください。

Cisco CTL クライアントのインストール

次のイベントが発生するときには、クライアントを使用して CTL ファイルを更新する必要があります。

- セキュリティ モードの最初の設定時
- CTL ファイルの最初の作成時
- Cisco Unified Communications Manager のインストール後
- Cisco Unified Communications Manager サーバまたは Cisco Unified Communications Manager データの復元後
- Cisco Unified Communications Manager サーバの IP アドレスまたはホスト名の変更後
- セキュリティ トークンの追加後または削除後
- PIX Firewall の追加後または削除後
- TFTP サーバの追加後または削除後
- Cisco Unified Communications Manager サーバの追加後または削除後
- サードパーティ CA 署名証明書のプラットフォームへのアップロード後

ヒント　クライアントをインストールしようとしているサーバまたはワークステーションで、Smart Card サービスが「開始」および「自動」に設定されていない場合、インストールは失敗します。

Cisco CTL クライアントをインストールするには、次の手順を実行します。

手順

ステップ 1　『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の説明に従い、クライアントをインストールしようとする Windows ワークステーションまたはサーバから Cisco Unified Communications Manager の管理ページに移動します。

ステップ 2　Cisco Unified Communications Manager の管理ページで、**［アプリケーション］** > **［プラグイン］** の順に選択します。

［プラグインの検索と一覧表示（Find and List Plugins）］ウィンドウが表示されます。

ステップ 3　［かつプラグインタイプが次に等しい］ドロップダウン リスト ボックスから **［インストール］** を選択し、**［検索］** をクリックします。

ステップ 4　［Cisco CTL Client］を見つけます。

ステップ 5　ファイルをダウンロードするには、ウィンドウの右側の、Cisco CTL クライアント プラグイン名のちょうど反対側にある **［ダウンロード］** をクリックします。

ステップ 6　**［保存］** をクリックして、ファイルを任意の場所に保存します。

ステップ 7　インストールを開始するには、**［Cisco CTL Client］**（ファイルを保存した場所によってアイコンまたは実行ファイルになります）をダブルクリックします。

（注）　［ダウンロードの完了］ボックスで［**ファイルを開く**］をクリックすることもできます。

ステップ 8　Cisco CTL クライアントのバージョンが表示されるので、［**Next**］をクリックします。

ステップ 9　インストール ウィザードが表示されます。［**Next**］をクリックします。

ステップ 10　使用許諾契約に同意して［**Next**］をクリックします。

ステップ 11　クライアントをインストールするフォルダを選択します。必要な場合は、［Browse］をクリックしてデフォルトの場所を変更することができます。場所を選択したら、［**Next**］をクリックします。

ステップ 12　インストールを開始するには、［**Next**］をクリックします。

ステップ 13　インストールが完了したら、［**Finish**］をクリックします。

追加情報

詳細については、P.3-26 の「関連項目」を参照してください。

Cisco CTL クライアントのアップグレードおよび Cisco CTL ファイルの移行

Cisco Unified Communications Manager Release 5.x から 6.x にアップグレードした後で CTL ファイルを変更するには、アップグレード前にインストールしていた Cisco CTL クライアントをアンインストールし、最新の Cisco CTL クライアントをインストールし（P.3-8 の「Cisco CTL クライアントのインストール」を参照）、CTL ファイルを再生成する必要があります。アップグレード前にサーバの削除や追加を実行しなかった場合は、アップグレード後に Cisco CTL クライアントを再設定する必要はありません。Cisco Unified Communications Manager のアップグレードにより、CTL ファイル内のデータは自動的に移行されます。

Cisco Unified Communications Manager 4.x からリリース 6.x にアップグレードし、セキュリティがクラスタ上で有効になっている場合は、アップグレード前にインストールしていた Cisco CTL クライアントをアンインストールし､最新の Cisco CTL クライアントをインストールして CTL ファイルを再生成する必要があります。アップグレードされたクラスタのセキュリティを有効にするには、次の手順に従います。

手順

ステップ 1　既存の Cisco CTL クライアントをアンインストールします。

ステップ 2　新しい Cisco CTL クライアントをインストールします（P.3-8 の「Cisco CTL クライアントのインストール」を参照）。

ステップ 3　以前に使用した USB キーのうち少なくとも 1 つを使用して Cisco CTL クライアントを実行します（P.3-11 の「Cisco CTL クライアントの設定」を参照）。

ステップ 4　これらのサービスを実行するすべての Cisco Unified Communications Manager サーバおよびクラスタ内のすべての TFTP サーバで Cisco Unified Serviceability を使用して、Cisco CallManager サービスおよび Cisco Tftp サービスを再起動する必要があります。

追加情報

詳細については、P.3-26 の「関連項目」を参照してください。

Cisco CTL クライアントの設定

ヒント　Cisco CTL クライアントは、スケジューリングされたメンテナンス画面で設定します。これは、Cisco CallManager サービスおよび Cisco Tftp サービスを再起動する必要があるためです。

Cisco CTL クライアントは、次のタスクを実行します。

- Cisco Unified Communications Manager クラスタのセキュリティ モードを設定する。

（注）　クラスタ セキュリティ モードは、スタンドアロン サーバまたはクラスタのセキュリティ機能を設定します。

ヒント　Cisco Unified Communications Manager の管理ページの［エンタープライズパラメータ設定（Enterprise Parameters Configuration）］ウィンドウで Cisco Unified Communications Manager クラスタのセキュリティ パラメータを混合モードに設定することはできません。クラスタ セキュリティ モードを設定するには、CTL クライアントを設定する必要があります。詳細については、P.3-18 の「Cisco CTL クライアントの設定内容」を参照してください。

- Certificate Trust List（CTL; 証明書信頼リスト）を作成する。これは、セキュリティ トークン、Cisco Unified Communications Manager、PIX Firewall および CAPF サーバ用の証明書エントリが含まれたファイルです。

  CTL ファイルによって、電話接続用の TLS をサポートするサーバが示されます。クライアントは自動的に Cisco Unified Communications Manager、Cisco CAPF、および PIX Firewall を検出して、これらのサーバの証明書エントリを追加します。

  設定時に挿入したセキュリティ トークンによって CTL ファイルが署名されます。

（注）　CTL クライアントは、Cisco Unified Communications Manager スーパークラスタ サポートも提供します。スーパークラスタには、最大 16 のコールを処理するサーバ、1 つのパブリッシャ、2 つの TFTP サーバ、および最大 9 つのメディア リソース サーバが含まれます。

始める前に

ヒント　Cisco Unified Communications Manager をアップグレードするときの CTL ファイル設定の詳細については、P.3-10 の「Cisco CTL クライアントのアップグレードおよび Cisco CTL ファイルの移行」を参照してください。

Cisco CTL クライアントを設定する前に、Cisco CTL Provider サービスおよび Cisco Certificate Authority Proxy Function サービスを Cisco Unified Serviceability でアクティブにしたことを確認します。少なくとも 2 つのセキュリティ トークンを入手します。これらのセキュリティ トークンは、

Cisco certificate authority が発行します。シスコから取得したセキュリティ トークンを使用する必要があります。トークンを一度に 1 つずつサーバまたはワークステーションの USB ポートに挿入します。サーバに USB ポートがない場合、USB PCI カードを使用することができます。

次のパスワード、ホスト名または IP アドレス、ポート番号を取得します。

- Cisco Unified Communications Manager の管理ユーザ名とパスワード

ヒント　管理ユーザ名は、エンドユーザではなく、アプリケーション ユーザである必要があり、また、スーパーユーザ権限を持つスーパーユーザ グループのメンバーでなければなりません。

- セキュリティ トークンの管理者パスワード
- PIX Firewall の管理ユーザ名とパスワード

これらの説明については、P.3-18 の表 3-2 を参照してください。

ヒント　Cisco CTL クライアントをインストールする前に、サーバへのネットワーク接続を確認します。ネットワーク接続したことを確認するには、『*Cisco Unified Communications Operating System アドミニストレーション ガイド*』の説明に従って ping コマンドを実行します。クラスタ環境では、クラスタ内のすべてのサーバにネットワーク接続できることを確認してください。

複数の Cisco CTL クライアントをインストールした場合、Cisco Unified Communications Manager では一度に 1 台のクライアントの CTL 設定情報しか受け入れません。ただし、設定作業は同時に 5 台までの Cisco CTL クライアントで実行できます。あるクライアントで設定作業を実行している間、その他のクライアントで入力した情報は Cisco Unified Communications Manager によって自動的に保存されます。

Cisco CTL クライアントの設定が完了すると、CTL クライアントは次のタスクを実行します。

- CTL ファイルをすべての Cisco Unified Communications Manager サーバに書き込む。
- CAPF capf.cer をクラスタ内のすべての Cisco Unified Communications Manager 後続ノード（最初のノード以外）に書き込む。
- PEM 形式の CAPF 証明書ファイルをクラスタ内のすべての Cisco Unified Communications Manager 後続ノード（最初のノード以外）に書き込む。
- すべての設定済み TFTP サーバにこのファイルを書き込む。
- すべての設定済み PIX Firewall にこのファイルを書き込む。
- CTL ファイルを作成した時点で USB ポートに存在するセキュリティ トークンの秘密鍵を使用して、CTL ファイルに署名する。

クライアントを設定するには、次の手順を実行します。

手順

ステップ 1　購入したセキュリティ トークンを少なくとも 2 つ入手します。

ステップ 2　次の作業のどちらかを実行します。

- インストールしたワークステーションまたはサーバのデスクトップにある［**Cisco CTL Client**］アイコンをダブルクリックします。

- ［スタート］>［プログラム］>［**Cisco CTL Client**］の順に選択します。

ステップ 3　表 3-2 の説明に従って Cisco Unified Communications Manager サーバの設定内容を入力し、［**Next**］をクリックします。

ステップ 4　表 3-2 の説明に従って、［**Set Cisco Unified Communications Manager Cluster to Mixed Mode**］をクリックし、［**Next**］をクリックします。

ステップ 5　設定する内容に応じて、次の作業を実行します。

- セキュリティ トークンを追加するには、ステップ 6 ～ステップ 12 を参照します。
- Cisco CTL クライアント設定を完了するには、ステップ 17 ～ステップ 21 を参照します。

注意　クライアントを初めて設定する場合、少なくとも 2 つのセキュリティ トークンが必要です。アプリケーションが要求しない限り、トークンを挿入しないでください。ワークステーションまたはサーバに USB ポートが 2 つある場合は、2 つのセキュリティ トークンを同時に挿入しないでください。

ステップ 6　アプリケーションが要求したら、現在 Cisco CTL クライアントを設定しているワークステーションまたはサーバで使用可能な USB ポートにセキュリティ トークンを 1 つ挿入して、［**OK**］をクリックします。

ステップ 7　挿入したセキュリティ トークンについての情報が表示されます。［**Add**］をクリックします。

ステップ 8　検出された証明書エントリがペインに表示されます。

ステップ 9　他のセキュリティ トークン（複数も可能）を証明書信頼リストに追加するには、［**Add Tokens**］をクリックします。

ステップ 10　サーバまたはワークステーションに挿入したトークンを取り外していない場合は、取り外します。アプリケーションが要求したら、次のトークンを挿入して［**OK**］をクリックします。

ステップ 11　2 番目のセキュリティ トークンについての情報が表示されます。［**Add**］をクリックします。

ステップ 12　すべてのセキュリティ トークンについて、ステップ 9 ～ステップ 11 を繰り返します。

ステップ 13　証明書エントリがペインに表示されます。

ステップ 14　P.3-18 の表 3-2 の説明に従って、設定内容を入力します。

ステップ 15　［**Next**］をクリックします。

ステップ 16　表 3-2 の説明に従って設定内容を入力し、［**Next**］をクリックします。

ステップ 17　すべてのセキュリティ トークンおよびサーバを追加したら、［**Finish**］をクリックします。

ステップ 18　表 3-2 の説明に従ってセキュリティ トークンのユーザ パスワードを入力し、［**OK**］をクリックします。

ステップ 19　クライアントによって CTL ファイルが作成されると、各サーバのウィンドウに、サーバ、ファイル ロケーション、および CTL ファイルのステータスが表示されます。［**Finish**］をクリックします。

ステップ 20　すべてのデバイスをリセットします。詳細については、P.1-13 の「デバイスのリセット、サービスの再起動またはリブート」を参照してください。

ステップ 21　Cisco Unified Serviceability で、Cisco CallManager サービスおよび Cisco Tftp サービスを再起動します。

ヒント　これらのサービスを実行するすべての Cisco Unified Communications Manager サーバとクラスタ内のすべての TFTP サーバで、これらのサービスを再起動します。

ステップ 22　CTL ファイルを作成したら、USB ポートからセキュリティ トークンを取り外します。すべてのセキュリティ トークンを安全な任意の場所に格納します。

追加情報

詳細については、P.3-26 の「関連項目」を参照してください。

CTL ファイルの更新

次のシナリオが発生した場合、CTL ファイルを更新する必要があります。

- 新しい Cisco Unified Communications Manager サーバをクラスタに追加した場合
- Cisco Unified Communications Manager サーバの名前または IP アドレスを変更した場合
- いずれかの設定済み TFTP サーバの IP アドレスまたはホスト名を変更した場合
- いずれかの設定済み PIX Firewall の IP アドレスまたはホスト名を変更した場合
- Cisco Unified Serviceability で Cisco Certificate Authority Function サービスを有効にした場合
- セキュリティ トークンを追加または削除する必要がある場合
- TFTP サーバを追加または削除する必要がある場合
- Cisco Unified Communications Manager サーバを追加または削除する必要がある場合
- PIX Firewall を追加または削除する必要がある場合
- Cisco Unified Communications Manager サーバまたは Cisco Unified Communications Manager データを復元した場合
- サードパーティの CA 署名証明書をプラットフォームにアップロードした後

ヒント　ファイルの更新は、コール処理がほとんど中断されないときに実行することを強く推奨します。

CTL ファイルにある情報を更新するには、次の手順を実行します。

手順

ステップ 1　最新の CTL ファイルを設定するために挿入したセキュリティ トークンを 1 つ入手します。

ステップ 2　インストールしたワークステーションまたはサーバのデスクトップにある［**Cisco CTL Client**］アイコンをダブルクリックします。

ステップ 3　表 3-2 の説明に従って Cisco Unified Communications Manager サーバの設定内容を入力し、［**Next**］をクリックします。

ヒント　このウィンドウでは、Cisco Unified Communications Manager サーバについて更新します。

ステップ 4　CTL ファイルを更新するには、表 3-2 の説明にあるように［**Update CTL File**］をクリックし、［**Next**］をクリックします。

注意　すべての CTL ファイルを更新するには、すでに CTL ファイルに存在するセキュリティ トークンを（1 つ）USB ポートに挿入する必要があります。クライアントでは、このトークンを使用して CTL ファイルのシグニチャを検証します。CTL クライアントによってシグニチャが検証されるまで、新しいトークンは追加できません。ワークステーションまたはサーバに USB ポートが 2 つある場合は、両方のセキュリティ トークンを同時に挿入しないでください。

ステップ 5　現在 CTL ファイルを更新しているワークステーションまたはサーバで使用可能な USB ポートにまだセキュリティ トークンを挿入していない場合は、いずれかのセキュリティ トークンを挿入してから［**OK**］をクリックします。

ステップ 6　挿入したセキュリティ トークンについての情報が表示されます。［**Next**］をクリックします。

検出された証明書エントリがペインに表示されます。

ヒント　このペインでは、Cisco Unified Communications Manager、Cisco TFTP、または PIX Firewall のエントリを更新できません。Cisco Unified Communications Manager エントリを更新するには、［**Cancel**］をクリックし、ステップ 2 ～ ステップ 6 をもう一度実行します。

ステップ 7　既存の Cisco CTL エントリを更新するか、あるいはセキュリティ トークンを追加または削除する際は、次の点を考慮してください。

- サーバ設定の更新手順または新しいセキュリティ　トークンの追加手順については、P.3-11 の「Cisco CTL クライアントの設定」を参照してください。
- セキュリティ トークンを削除するには、P.3-17 の「CTL ファイル エントリの削除」を参照してください。

ステップ 8　CTL　ファイルの更新が終了したら、Cisco　Unified　Serviceability　で、Cisco CallManager　および Cisco Tftp サービスを再起動します。

ヒント　これらのサービスを実行するすべてのクラスタ内のすべてのノードで　Tftp　サービスおよび　Cisco CallManager サービスを再起動してください。

追加情報

詳細については、P.3-26 の「関連項目」を参照してください。

CTL ファイル エントリの削除

Cisco CTL クライアントの［CTL Entries］ウィンドウに表示される一部の CTL エントリは、いつでも削除することができます。クライアントを開いて、［CTL Entries］ウィンドウを表示するプロンプトに従い、削除する項目を強調表示してから［**Delete Selected**］をクリックしてエントリを削除します。

Cisco Unified Communications Manager、Cisco TFTP、PIX Firewall、または Cisco CAPF を実行するサーバを、CTL ファイルから削除することはできません。

CTL ファイルには常に 2 つのセキュリティ トークン エントリが存在している必要があります。ファイルからセキュリティ トークンをすべて削除することはできません。

追加情報

詳細については、P.3-26 の「関連項目」を参照してください。

Cisco Unified Communications Manager セキュリティ モードの更新

クラスタのセキュリティ モードを設定するには、Cisco CTL クライアントを使用する必要があります。Cisco Unified Communications Manager セキュリティ モードは、Cisco Unified Communications Manager の管理ページの［エンタープライズパラメータ設定（Enterprise Parameters Configuration）］ウィンドウで変更することはできません。

（注）　クラスタ セキュリティ モードは、スタンドアロン サーバまたはクラスタのセキュリティ機能を設定します。

Cisco CTL クライアントの初期設定後にクラスタ セキュリティ モードを変更するには、CTL ファイルを更新する必要があります。［Cluster Security Mode］ウィンドウに移動して、モードの設定を変更し、**［Next］**、**［Finish］**の順にクリックします（P.3-15 の「CTL ファイルの更新」および表 3-2 を参照）。

セキュリティ モードを混合モードから非セキュア モードに変更した場合、CTL ファイルはサーバに存在したままですが、CTL ファイルに証明書は含まれません。CTL ファイルに証明書が存在しないため、電話機は署名なし設定ファイルを要求し、非セキュアとして Cisco Unified Communications Manager に登録されます。

Cisco CTL クライアントの設定内容

クラスタのセキュリティ モードは、表 3-2 の説明にあるように、非セキュア モードまたは混合モードのいずれかに設定できます。混合モードだけが認証、シグナリング暗号化、およびメディア暗号化をサポートしています。

（注）　クラスタ セキュリティ モードは、スタンドアロン サーバまたはクラスタのセキュリティ機能を設定します。

表 3-2 を使用して、初めての Cisco CTL クライアント設定、CTL ファイルの更新、または混合モードから非セキュア モードへの変更を行うことができます。

- 設定のヒントについては、P.3-3 の「Cisco CTL クライアントの設定のヒント」を参照してください。
- 関連する情報および手順については、P.3-26 の「関連項目」を参照してください。

表 3-2　CTL クライアントの設定内容

設定	説明
Cisco Unified Communications Manager Server	
Hostname or IP Address	最初のノードのホスト名または IP アドレスを入力します。
Port	この Cisco Unified Communications Manager サーバで実行されている Cisco CTL Provider サービスの CTL ポート番号を入力します。デフォルトのポート番号は 2444 です。
Username and Password	最初のノードでスーパーユーザの管理者権限を持つアプリケーション ユーザのユーザ名とパスワードと同じものを入力します。
Security Mode	
Set Cisco Unified Communications Manager Cluster to Mixed Mode	混合モードでは、認証済みで暗号化済み、および非セキュアの Cisco Unified IP Phone を Cisco Unified Communications Manager に登録することができます。このモードでは、認証済みまたは暗号化済みのデバイスでセキュア ポートが使用されることを Cisco Unified Communications Manager が保証します。 （注）　混合モードに設定すると、Cisco Unified Communications Manager によって自動登録は無効になります。

表 3-2　CTL クライアントの設定内容（続き）

設定	説明
Set Cisco Unified Communications Manager Cluster to Non-Secure Mode	非セキュア モードに設定すると、すべてのデバイスは非認証として登録され、Cisco Unified Communications Manager はイメージ認証のみサポートします。 このモードを選択すると、CTL クライアントは CTL ファイルにあるすべてのエントリの証明書を削除しますが、CTL ファイルは引き続き指定したディレクトリに存在します。電話機は署名なし設定ファイルを要求し、非セキュアとして Cisco Unified Communications Manager に登録されます。 **ヒント**　電話機をデフォルトの非セキュア　モードに戻すには、電話機およびすべての Cisco Unified Communications Manager サーバから CTL ファイルを削除する必要があります。 このモードでは自動登録を使用できます。
Update CTL File	CTL ファイルの作成後にこのファイルを変更するには、このオプションを選択する必要があります。このオプションを選択すると、Cisco Unified Communications Manager のセキュリティ モードは変更されません。
CTL Entries	
Add Tokens	証明書信頼リスト（CTL）にセキュリティ トークンを追加するには、このボタンをクリックします。 サーバまたはワークステーションに最初に挿入したトークンを取り外していない場合は、取り外します。アプリケーションが要求したら、次のトークンを挿入して［**OK**］をクリックします。追加したセキュリティ トークンについての情報が表示されたら、［**Add**］をクリックします。すべてのセキュリティ トークンについて、これらの作業を繰り返します。
Add TFTP Server	CTL に代替 TFTP サーバを追加するには、このボタンをクリックします。設定の詳細については、［Alternate TFTP Server］タブの設定値が表示された後で［**Help**］ボタンをクリックします。設定を入力したら、［**Next**］をクリックします。
Add Firewall	CTL に PIX Firewall を追加するには、このボタンをクリックします。設定の詳細については、［Firewall］タブの設定値が表示された後で［**Help**］ボタンをクリックします。設定を入力したら、［**Next**］をクリックします。

表 3-2　CTL クライアントの設定内容（続き）

設定	説明
Alternate TFTP Server	
Hostname or IP Address	TFTP サーバのホスト名または IP アドレスを入力します。 代替 TFTP サーバには、別のクラスタに存在する Cisco TFTP サーバを指定します。代替 TFTP サーバの設定に 2 つの異なるクラスタを使用する場合は、両クラスタが使用するクラスタ セキュリティ モードが同じであることが必要です。これは、Cisco CTL クライアントを両方のクラスタにインストールして設定する必要があることを意味します。さらに、同じバージョンの Cisco Unified Communications Manager が両方のクラスタで動作している必要があります。 TFTP サービス パラメータ FileLocation 内のパスが、クラスタ内のすべてのサーバで同じであることを確認してください。 詳細については、P.3-3 の「Cisco CTL クライアントの設定のヒント」を参照してください。
Port	今回のリリースの Cisco Unified Communications Manager では不要です。
Username and Password	今回のリリースの Cisco Unified Communications Manager では不要です。
Firewall	
Hostname or IP Address	ファイアウォールのホスト名または IP アドレスを入力します。
Port	設定できません。デフォルトのポートである 2444 番の Cisco Unified Communications Manager ポートを使用します。
Username and Password	設定できません。Cisco Unified Communications Manager のインストール時に設定した管理者名とパスワードがシステムによって使用されます。
Security Token	
User Password	Cisco CTL クライアントを初めて設定するときは、デフォルト パスワードの **Cisco123** を大文字と小文字を区別して入力し、証明書の秘密鍵を取得して CTL ファイルが署名済みであることを確認します。

Cisco Unified Communications Manager のセキュリティ モードの確認

クラスタのセキュリティ モードを確認するには、次の手順を実行します。

（注）　クラスタ セキュリティ モードは、スタンドアロン サーバまたはクラスタのセキュリティ機能を設定します。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで［**システム**］>［**エンタープライズパラメータ**］の順に選択します。

ステップ 2　［**Cluster Security Mode**］フィールドを見つけます。フィールド内の値が **1** と表示される場合、Cisco Unified Communications Manager は混合モードに正しく設定されています。（詳細については、フィールド名をクリックしてください）。

ヒント　この値は Cisco Unified Communications Manager の管理ページで設定することができません。この値が表示されるのは、Cisco CTL クライアントの設定後です。

追加情報

詳細については、P.3-26 の「関連項目」を参照してください。

Smart Card サービスの開始および自動の設定

Cisco CTL クライアント インストールにより、Smart Card サービスが無効であると検出された場合は、Cisco CTL プラグインをインストールするサーバまたはワークステーションで、Smart Card サービスを「自動」および「開始」に設定する必要があります。

ヒント　サービスが「開始」および「自動」に設定されていない場合は、セキュリティ トークンを CTL ファイルに追加できません。

オペレーティング　システムのアップグレード、サービス　リリースの適用、Cisco　Unified Communications Manager のアップグレードなどを行ったら、Smart Card サービスが「開始」および「自動」になっていることを確認します。

サービスを「開始」および「自動」に設定するには、次の手順を実行します。

手順

ステップ 1　Cisco CTL クライアントをインストールしたサーバまたはワークステーションで、**[スタート]** > **[プログラム]** > **[管理ツール]** > **[サービス]** または **[スタート]** > **[コントロール パネル]** > **[管理ツール]** > **[サービス]** の順に選択します。

ステップ 2　[サービス] ウィンドウで、**Smart Card** サービスを右クリックし、**[プロパティ]** を選択します。

ステップ 3　[プロパティ] ウィンドウに [全般] タブが表示されていることを確認します。

ステップ 4　[スタートアップの種類] ドロップダウン リスト ボックスから、**[自動]** を選択します。

ステップ 5　**[適用]** をクリックします。

ステップ 6　[サービスの状態] 領域で、**[開始]** をクリックします。

ステップ 7　**[OK]** をクリックします。

ステップ 8　サーバまたはワークステーションをリブートし、サービスが動作していることを確認します。

追加情報

詳細については、P.3-26 の「関連項目」を参照してください。

セキュリティ トークン パスワード（etoken）の変更

この管理パスワードは、証明書の秘密鍵を取得し、CTL ファイルが署名されることを保証します。各セキュリティ トークンには、デフォルト パスワードが付属されています。セキュリティ トークン パスワードはいつでも変更できます。Cisco CTL クライアントによりパスワードの変更を求めるプロンプトが表示されたら、設定を続行する前にパスワードを変更する必要があります。

パスワード設定の関連情報を検討するには、［**Show Tips**］ボタンをクリックします。何らかの理由でパスワードを設定できない場合は、表示されるヒントを検討してください。

セキュリティ トークン パスワードを変更するには、次の手順を実行します。

手順

ステップ 1　Cisco CTL クライアントを Windows サーバまたはワークステーションにインストールしたことを確認します。

ステップ 2　Cisco CTL クライアントをインストールした Windows サーバまたはワークステーションの USB ポートにセキュリティ トークンが挿入されていなければ挿入します。

ステップ 3　［スタート］> ［プログラム］> ［**etoken**］> ［**Etoken Properties**］の順に選択します。次に、［**etoken**］を右クリックし、［**Change etoken password**］を選択します。

ステップ 4　［Current Password］フィールドに、最初に作成したトークン パスワードを入力します。

ステップ 5　新しいパスワードを入力します。

ステップ 6　確認のため、新しいパスワードを再入力します。

ステップ 7　［**OK**］をクリックします。

追加情報

詳細については、P.3-26 の「関連項目」を参照してください。

Cisco Unified IP Phone 上の CTL ファイルの削除

注意　セキュアな実験室環境でこの作業を実行することをお勧めします。特に、クラスタ内のCisco Unified Communications Manager サーバから CTL ファイルを削除する予定がない場合にお勧めします。

次の状況が発生した場合は、Cisco Unified IP Phone 上の CTL ファイルを削除してください。

- CTL ファイルに署名したセキュリティ トークンをすべて紛失した。
- CTL ファイルに署名したセキュリティ トークンが漏洩した。
- 電話機をセキュア環境からストレージ領域などに移動する。
- 電話機を、非セキュア クラスタ、または異なるドメインの別のセキュア クラスタへと移動する。
- 電話機を、未知のセキュリティ ポリシーを持つ領域からセキュアな Cisco Unified Communications Manager へと移動する。
- 代替 TFTP サーバ アドレスを、CTL ファイル内に存在しないサーバへと変更する。

Cisco Unified IP Phone 上の CTL ファイルを削除するには、表 3-3 の作業を実行します。

表 3-3　Cisco Unified IP Phone 上の CTL ファイルの削除

Cisco Unified IP Phone モデル	作業
Cisco Unified IP Phone 7960 および 7940	IP Phone 上の［セキュリティ設定］メニューにある、**［CTL ファイル］**、**［解除］**または **#、および **［削除］**を押します。
Cisco Unified IP Phone 7970 および同等モデル	次の方法のどちらかを実行します。 • ［セキュリティ設定］メニューのロックを解除します（『*Cisco Unified IP Phone アドミニストレーション ガイド for Cisco Unified Communications Manager*』を参照）。CTL オプションの下にある**［削除］**ソフトキーを押します。 • ［設定］メニューにある**［削除］**ソフトキーを押します。 **（注）**　［設定］メニューにある［削除］ソフトキーを押すと、CTL ファイル以外の情報も削除されます。詳細については、『*Cisco Unified IP Phone アドミニストレーション ガイド for Cisco Unified Communications Manager*』を参照してください。

追加情報

詳細については、P.3-26 の「関連項目」を参照してください。

Cisco CTL クライアントのバージョンの特定

使用している Cisco CTL クライアントのバージョンを特定するには、次の手順を実行します。

手順

ステップ 1　次の作業のどちらかを実行します。

- デスクトップ上の［**Cisco CTL Client**］アイコンをダブルクリックします。
- ［**スタート**］>［**プログラム**］>［**Cisco CTL Client**］の順に選択します。

ステップ 2　Cisco CTL クライアント ウィンドウの左上隅にあるアイコンをクリックします。

ステップ 3　［**About Cisco CTL Client**］を選択します。クライアントのバージョンが表示されます。

追加情報

詳細については、P.3-26 の「関連項目」を参照してください。

Cisco CTL クライアントの確認とアンインストール

Cisco CTL クライアントをアンインストールしても、CTL ファイルは削除されません。同様に、クライアントをアンインストールしても、Cisco Unified Communications Manager のセキュリティ モードと CTL ファイルは変更されません。必要であれば、CTL クライアントをアンインストールし、クライアントを別の Windows ワークステーションまたはサーバにインストールして、同じ CTL ファイルを引き続き使用することができます。

Cisco CTL クライアントがインストールされていることを確認するには、次の手順を実行します。

手順

ステップ 1　［**スタート**］>［**コントロール パネル**］>［**アプリケーションの追加と削除**］の順に選択します。

ステップ 2　［**アプリケーションの追加と削除**］をダブルクリックします。

ステップ 3　クライアントがインストールされていることを確認するには、［**Cisco CTL Client**］を見つけます。

ステップ 4　クライアントをアンインストールするには、［**削除**］をクリックします。

追加情報

詳細については、P.3-26 の「関連項目」を参照してください。

その他の情報

関連項目

- システム要件（P.1-5）
- Cisco CTL クライアントの概要（P.3-2）
- Cisco CTL クライアントの設定用チェックリスト（P.3-4）
- Cisco CTL Provider サービスのアクティブ化（P.3-5）
- Cisco CAPF サービスのアクティブ化（P.3-6）
- TLS 接続用ポートの設定（P.3-6）
- Cisco CTL クライアントのインストール（P.3-8）
- Cisco CTL クライアントのアップグレードおよび Cisco CTL ファイルの移行（P.3-10）
- Cisco CTL クライアントの設定（P.3-11）
- CTL ファイルの更新（P.3-15）
- CTL ファイル エントリの削除（P.3-17）
- Cisco Unified Communications Manager セキュリティ モードの更新（P.3-17）
- Cisco CTL クライアントの設定内容（P.3-18）
- Cisco Unified Communications Manager のセキュリティ モードの確認（P.3-21）
- Smart Card サービスの開始および自動の設定（P.3-22）
- Cisco Unified IP Phone 上の CTL ファイルの削除（P.3-24）
- Cisco CTL クライアントのバージョンの特定（P.3-25）
- Cisco CTL クライアントの確認とアンインストール（P.3-25）
- Certificate Authority Proxy Function の使用方法（P.6-1）

シスコの関連マニュアル

Cisco Unified IP Phone アドミニストレーション ガイド for Cisco Unified Communications Manager

Cisco Unified Communications Manager トラブルシューティング ガイド