トラブルシューティング

この章は、次の内容で構成されています。

- アラームの使用方法（P.9-2）
- Microsoft パフォーマンス モニタ カウンタの使用方法（P.9-3）
- ログ ファイルの検討（P.9-4）
- HTTPS のトラブルシューティング（P.9-6）
- Cisco CTL クライアントのトラブルシューティング（P.9-11）
- CAPF のトラブルシューティング（P.9-42）
- 電話機および Cisco IOS MGCP ゲートウェイの暗号化のトラブルシューティング（P.9-48）
- セキュア SRST リファレンスのトラブルシューティング（P.9-60）

ヒント この章では、Cisco IP Phone がロード エラーやセキュリティのバグなどによって障害を起こした場合に IP Phone をリセットする方法は説明していません。IP Phone のリセットについては、IP Phone のモデルに対応した『*Cisco IP Phone アドミニストレーション ガイド for Cisco CallManager*』を参照してください。

ここでは、Cisco IP Phone 7970 モデル、7960 モデル、および 7940 モデルだけから CTL ファイルを削除する方法について説明します。この作業の実行方法については、表 9-4、または IP Phone のモデルに対応した『*Cisco IP Phone アドミニストレーション ガイド for Cisco CallManager*』を参照してください。

アラームの使用方法

Cisco CallManager Serviceability は、次の場合にアラームを生成します。

- 認証済みデバイスが非 TLS SCCP 接続を使用して登録する場合や、認証されていない IP Phone が TLS SCCP 接続を使用して登録する場合。
- ピア証明書のタイトルに含まれているデバイス名が、デバイス登録に使用されるデバイス名と一致しない場合。
- デバイスが Cisco CallManager 設定と互換性のない TLS 接続を使用して、Cisco CallManager に登録する場合。

次の状況では、IP Phone でアラームが生成される場合があります。

- TFTP Not Authorized: <IP address>

  IP Phone がこのアラームを生成するのは、TFTP サーバ情報（代替またはそれ以外）が CTL ファイル内に存在しない場合です。DHCP がプライマリとバックアップのサーバ アドレスを提供した状況で、どちらのアドレスも CTL ファイルに存在しない場合は、IP Phone がアラームを 2 回発行することがあります。CTL ファイル情報を正しく入力したこと、および DHCP サーバに正しいアドレスを設定したことを確認してください。

- File Auth Failed

  IP Phone がこのアラームを生成する理由には、CTL ファイルの破損など、さまざまなものがあります。CTL ファイルが破損した場合は、sniffer トレースを使用して、ネットワークのトラブルシューティングを行う必要があります。問題を特定できない場合は、コンソール ケーブルを使用してデバッグする必要があります。詳細については、『*Cisco IP Phone アドミニストレーション ガイド for Cisco CallManager*』を参照してください（ただし、Cisco IP Phone 7970 モデル、7960 モデル、および 7940 モデルの場合で、IP Phone モデルに対応した管理マニュアルに詳細が記載されていないとき）。

ヒント　IP Phone で生成されるその他のアラームについては、IP Phone のモデルに対応した『*Cisco IP Phone アドミニストレーション ガイド for Cisco CallManager* 』と、P.9-30 の「CTL ファイルに問題がある場合の IP Phone のトラブルシューティング」を参照してください。

関連項目

- *Cisco CallManager Serviceability アドミニストレーション ガイド*
- *Cisco CallManager Serviceability システム ガイド*
- *Cisco IP Phone アドミニストレーション ガイドfor Cisco CallManager*

Microsoft パフォーマンス モニタ カウンタの使用方法

Microsoft パフォーマンス モニタ カウンタは、Cisco CallManager に登録する認証済み IP Phone の数、完了した認証済みコールの数、および任意の時点でアクティブになっている認証済みコールの数を監視するために用意されています。

関連項目

- *Cisco CallManager Serviceability アドミニストレーション ガイド*
- *Cisco CallManager Serviceability システム ガイド*

ログ ファイルの検討

Cisco AVVID Partner や Cisco Technical Assistance Center（TAC）など、この製品のテクニカル サポートに連絡する場合は、事前に次のログ ファイルを取得して検討します。

- Cisco CallManager：C:\Program Files\Cisco\Trace\CCM
- TFTP：C:\Program Files\Cisco\Trace\TFTP
- DBL：C:\Program Files\Cisco\Trace\DBL
  - C:\Program Files\Cisco\Trace\DBL\DBLR*
  - C:\Program Files\Cisco\Trace\DBL\DBLRT*
  - C:\Program Files\Cisco\Trace\DBL\DBL_CCM*
  - C:\Program Files\Cisco\Trace\DBL\DBL_TFTP*
  - C:\Program Files\Cisco\Trace\DBL\DBL_CTLPROVIDER*
- Cisco CallManager SDL Traces：C:\Program Files\Cisco\Trace\SDL\CCM

ヒント　ローカルで有効な証明書の検証が失敗する場合は、SDL トレース ファイルを検討します。

- HTTPS：C:\program files\common files\cisco\logs\HTTPSCertInstall.log
- CTL Provider Service：C:\Program Files\Cisco\Trace\CTLProvider
- Cisco CTL クライアント：C:\Program Files\Cisco\CTL Client\Trace

  デフォルトでは、Cisco CTL クライアントのインストール先は、CTL クライアントが存在するサーバまたはワークステーション上の C:\Program Files\Cisco\CTL File になります（C:\ctlinstall.log を参照）。
- Cisco Certificate Authority Proxy Function（CAPF）サービス：C:\Program Files\Cisco\Trace\CAPF
- SRST リファレンス：winnt\system32\Trace

関連項目

- Cisco CTL クライアントの設定（P.3-1）
- Certificate Authority Proxy Function の使用方法（P.4-1）
- HTTP over SSL（HTTPS）の使用方法（P.2-1）
- Survivable Remote Site Telephony（SRST）リファレンスのセキュリティ設定（P.7-1）

HTTPS のトラブルシューティング

この項は、次の内容で構成されています。

- HTTPS の設定時に表示されるメッセージ（P.9-6）
- HTTPS の有効化（P.9-8）
- 仮想ディレクトリの HTTPS の無効化（P.9-9）

HTTPS の設定時に表示されるメッセージ

表 9-1 は、HTTPS の設定時に問題が発生した場合に表示されるメッセージ、その問題への修正処置、および理由を説明しています。

表 9-1　HTTPS の設定時に表示されるメッセージ

メッセージ	修正処置または理由
The security library has encountered an improperly formatted DER-encoded message.	このエラーが発生するのは、HTTPS サービスを有効にする証明書が、証明書のサブジェクト名としてホスト名を使用するためです。Netscape 4.79 はサブジェクト名に含まれているアンダースコアを無効な文字と見なすため、HTTPS は動作しません。 メッセージが表示された場合は、**OK** をクリックします。 HTTPS をサポートするには、Internet Explorer を使用します。Netscape 4.79 とホスト名を使用してアプリケーションにアクセスするには、HTTPS を無効にします（P.9-9 の「仮想ディレクトリの HTTPS の無効化」を参照）。

表 9-1　HTTPS の設定時に表示されるメッセージ（続き）

メッセージ	修正処置または理由
A network error occurred while Netscape was receiving data. (Network Error: Connection refused) Try connecting again.	HTTPS 用の Cisco CallManager 証明書が、ローカルの Netscape 4.79 ブラウザに存在しますが、Cisco CallManager HTTPS 証明書が表示されました。ユーザは、Netscape 4.79 ブラウザを使用して接続することはできません。 次の方法のいずれかを使用して接続します。 • Internet Explorer を使用して、アプリケーションにアクセスします。 • Netscape 4.79 を使用して、**Communicator -> Tools -> Security Info -> Certificates -> Web sites** の順に選択し、Cisco CallManager サーバ用の HTTPS 証明書を強調表示させます。Web Sites Certificates ウィンドウで **Delete** をクリックします。確認プロンプトで **OK** をクリックして確定します。次に **OK** をクリックします。

関連項目

- HTTPS の有効化（P.9-8）
- HTTPS 証明書の削除（P.9-10）
- HTTP over SSL（HTTPS）の使用方法（P.2-1）

HTTPS の有効化

仮想ディレクトリの HTTPS を有効にするには、次の手順を実行します。

手順

ステップ 1　**Start > Programs > Administrative Tools > Internet Services Manager** の順に選択します。

ステップ 2　HTTPS 証明書が存在するサーバの名前をクリックします。

ステップ 3　**Default Web Site** をクリックします。

ステップ 4　仮想ディレクトリをクリックします。

ステップ 5　**Properties** を右クリックします。

ステップ 6　**Directory Security** タブをクリックします。

ステップ 7　Secure Communications の下にある **Edit** ボタンをクリックします。

ステップ 8　**SSL Required** チェックボックスをオンにします。

ステップ 9　HTTPS を有効にするすべての仮想ディレクトリについて、この手順を実行します。

関連項目

- HTTPS の有効化（P.9-8）
- HTTPS の設定時に表示されるメッセージ（P.9-6）
- HTTP over SSL（HTTPS）の使用方法（P.2-1）

仮想ディレクトリの HTTPS の無効化

仮想ディレクトリの HTTPS を無効にするには、次の手順を実行します。

手順

ステップ 1　**Start > Programs > Administrative Tools > Internet Services Manager** の順に選択します。

ステップ 2　HTTPS 証明書が存在するサーバの名前をクリックします。

ステップ 3　**Default Web Site** をクリックします。

ステップ 4　仮想ディレクトリ（たとえば、CCMAdmin）をクリックします。

ステップ 5　**Properties** を右クリックします。

ステップ 6　**Directory Security** タブをクリックします。

ステップ 7　Secure Communications の下にある **Edit** をクリックします。

ステップ 8　**SSL Required** チェックボックスをオフにします。

ステップ 9　この作業を、CCMAdmin、CCMService、CCMUser、AST、BAT、RTMTReports、CCMTraceAnalysis、CCMServiceTraceCollectionTool、PktCap、および ART の各仮想ディレクトリについて実行します。

関連項目

- HTTP over SSL（HTTPS）の使用方法（P.2-1）
- HTTPS 証明書の削除（P.9-10）
- HTTPS の有効化（P.9-8）

HTTPS 証明書の削除

HTTPS 証明書を削除するには、次の手順を実行します。

手順

ステップ 1　**Start > Programs > Administrative Tools > Internet Services Manager** の順に選択します。

ステップ 2　HTTPS 証明書が存在するサーバの名前をクリックします。

ステップ 3　**Directory Security** タブをクリックします。

ステップ 4　Secure Communications で **Server Certificate** ボタンをクリックします。

ステップ 5　**Next** をクリックします。

ステップ 6　**Remove the Current Certificate** を選択します。

ステップ 7　**Next** をクリックします。

ステップ 8　**Finish** をクリックします。

関連項目

- HTTPS の有効化（P.9-8）
- HTTPS の設定時に表示されるメッセージ（P.9-6）
- HTTP over SSL（HTTPS）の使用方法（P.2-1）

Cisco CTL クライアントのトラブルシューティング

この項は、次の内容で構成されています。

- セキュリティ トークン パスワード（Etoken）の変更（P.9-11）
- 不適切なセキュリティ トークン パスワードを続けて入力した場合のロックされたセキュリティ トークンのトラブルシューティング（P.9-13）
- Smart Card サービスの Started および Automatic への設定（P.9-14）
- Cisco CTL クライアントに関するメッセージ（P.9-15）
- CTL ファイルに問題がある場合の IP Phone のトラブルシューティング（P.9-30）
- Cisco IP Phone およびサーバ上の CTL ファイルの比較（P.9-32）
- Cisco IP Phone 上の CTL ファイルの削除（P.9-33）
- サーバ上の CTL ファイルの削除（P.9-35）
- セキュリティ トークン（Etoken）を 1 つ紛失した場合のトラブルシューティング（P.9-36）
- セキュリティ トークン（Etoken）をすべて紛失した場合のトラブルシューティング（P.9-37）
- Cisco CTL クライアントの確認とアンインストール（P.9-40）
- Cisco CallManager クラスタのセキュリティ モードの確認（P.9-39）

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、証明書の秘密キーを取得し、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 2000 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 2000 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　**Start > Programs > 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。

関連項目

- Cisco CTL クライアントのインストール（P.3-10）
- Cisco CTL クライアントの設定（P.3-14）
- CTL ファイルの更新（P.3-20）
- Cisco CTL クライアント設定（P.3-24）

不適切なセキュリティ トークン パスワードを続けて入力した場合のロックされたセキュリティ トークンのトラブルシューティング

各セキュリティ トークンには、リトライ カウンタが含まれています。リトライ カウンタは、etoken Password ウィンドウへのログインの連続試行回数を指定します。セキュリティ トークンのリトライ カウンタ値は 15 です。連続試行回数がカウンタ値を超えた場合、つまり、16 回連続で試行が失敗した場合は、セキュリティ トークンがロックされ、使用不能になったことを示すメッセージが表示されます。ロックされたセキュリティ トークンを再び有効にすることはできません。

追加のセキュリティ トークン（複数可）を取得し、CTL ファイルを設定します（P.3-14 の「Cisco CTL クライアントの設定」を参照）。必要であれば、新しいセキュリティ トークン（複数可）を購入し、ファイルを設定します。

ヒント　パスワードを正しく入力すると、カウンタがゼロにリセットされます。

関連項目

- Cisco CTL クライアントのインストール（P.3-10）
- Cisco CTL クライアントの設定（P.3-14）
- CTL ファイルの更新（P.3-20）
- Cisco CTL クライアント設定（P.3-24）

Smart Card サービスの Started および Automatic への設定

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 automatic および started に設定する必要があります。

ヒント　サービスが started および automatic 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 CallManager のアップグレードなどを行ったら、Smart Card サービスが started および automatic になっていることを確認します。

サービスを started および automatic 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、**Start > Programs > Administrative Tools > Services** の順に選択します。

ステップ 2　Services ウィンドウで、**Smart Card** サービスを右クリックし、**Properties** を選択します。

ステップ 3　Properties ウィンドウに General タブが表示されていることを確認します。

ステップ 4　Startup type ドロップダウン リスト ボックスから、**Automatic** を選択します。

ステップ 5　**Apply** をクリックします。

ステップ 6　Service Status 領域で、**Start** 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。

関連項目

- システム要件（P.1-5）
- 対話および制限（P.1-6）
- Cisco CTL Provider サービスのアクティブ化（P.3-5）
- Cisco CTL Provider サービスのアクティブ化（P.3-5）
- Cisco CTL クライアントの設定（P.3-14）
- CTL ファイルの更新（P.3-20）
- デバイス セキュリティ モードの設定（P.5-7）

Cisco CTL クライアントに関するメッセージ

表 9-2 は、Cisco CTL クライアントに関して表示される可能性のあるメッセージと、対応する修正処置または理由を示しています。

表 9-2　Cisco CTL クライアントに関するメッセージ

メッセージ	修正処置または理由
Unknown CTL Error	内部 CTL エラーが発生しました。CTL ログでエラーを検討してください。
Invalid Port number	有効なポート番号（数字のみ）を入力します。
Invalid Range for port numbers	正しい範囲を指定します。有効なポート番号範囲は、1026 ～ 32767 です。
Could not write information to the local Windows Registry	CTL クライアントにレジストリへのアクセス権がありません。ローカル管理者アカウントまたはローカル パワー ユーザ アカウントを使用してログインしたことを確認してください。Cisco CTL クライアントでは、サーバ名、ポート、および管理者名は以後のログイン用に保存されません。

表 9-2　Cisco CTL クライアントに関するメッセージ（続き）

メッセージ	修正処置または理由
Invalid Group Name	CTL Provider サービスで、ユーザの属する Windows 2000 ユーザ グループを取得できません。ローカル管理者アカウントまたはローカル パワー ユーザ アカウントを使用してログインしたことを確認してください。
Invalid User Name	有効なユーザ名を入力しませんでした。user name フィールドがブランクであるか、名前が最大文字数を超えています。有効なユーザ名を入力します。
Invalid IP Address	有効な IP アドレスを入力しませんでした。アドレスが X.X.X.X 形式になっており、有効な IP 範囲を含んでいることを確認してください。有効な IP アドレスを入力します。
Invalid Hostname	有効なホスト名を入力しませんでした。server name フィールドがブランクであるか、フィールド内の文字数が最大許容文字数を超えています。有効なホスト名を入力します。
User could not be authenticated	指定されたユーザ名に対して、誤ったパスワードを入力しました。正しいパスワードを入力します。
Invalid Password	無効なパスワードを入力しました。パスワードがブランクであるか、パスワードが最大許容文字数を超えています。正しいパスワードを入力します。
Cannot run CTL Client from Terminal Services	CTL クライアントが Terminal Services と連動しません。アプリケーションをインストールしたマシン上でクライアントを設定する必要があります。
Failed to create CTL File	エラー発生後、CTL client ウィンドウ内に、サーバと障害理由のリストを示すダイアログボックスが表示されます。
Please insert a Security Token.Click Ok when done	セキュリティ トークンを挿入し、**OK** をクリックします。メッセージが引き続き表示される場合は、クライアント マシン上の Etoken Notification サービスを再起動します。

表 9-2　Cisco CTL クライアントに関するメッセージ（続き）

メッセージ	修正処置または理由
Cannot create CTL Entries.Total number of CTL Records has exceeded the Maximum	CTL ファイルに含まれている証明書またはエントリの数が、ファイルで許容された最大数を超えています。不要なサーバまたは etoken を削除します。最大限度は 100 です。
Unable to create CTL Entry	CTL ファイルが、最大ファイル サイズの限度を越えています。最大ファイル サイズは 75K です。不要なセキュリティ トークンまたは代替 TFTP サーバ エントリの削除を検討します。
Unable to parse CTL File	システムで CTL ファイルを分析できませんでした。CTL ファイルが破損しています。クラスタ内のすべてのサーバ上で、CTL ファイルが他のユーザによって改ざんまたは置換されていないかどうかを調べます。 ヒント　CTL クライアントからサブスクライバ サーバに接続し、サブスクライバ サーバから CTL ファイルを取得することができます。サブスクライバ サーバ上のファイルが破損している場合は、既存の CTL ファイルを削除し、新しいファイルを作成します。サブスクライバ サーバ上の CTL ファイルが破損していなければ、ファイルをパブリッシャに手動でコピーします。ただし、ファイルをコピーする前に、CTL ファイルが最新のものであることを確認してください。
CTL Client version is not compatible with the CTL Provider	CTL クライアントのバージョンと Cisco CallManager のバージョンを比較します。Cisco CallManager Administration 4.1 に表示される Cisco CTL クライアントを実行します。
Please select an item to delete	CTL Entries ウィンドウで、エントリを選択してから Delete をクリックします。

表 9-2　Cisco CTL クライアントに関するメッセージ（続き）

メッセージ	修正処置または理由
Error occurred when creating Dialog	システム メモリが不足しています。メモリ リソースを開放してから、CTL クライアントを再実行します。
--- No Issuer Name---	ノンセキュア モードでは、CTL Entries ウィンドウで発行者が No Issuer Name と表示されます。このメッセージは、ノンセキュア モードになっているためにアプリケーションが CTL ファイルにヌルの発行者名を書き込むことを示しています。
--- No Subject Name---	ノンセキュア モードでは、CTL Entries ウィンドウでサブジェクト名が No Subject Name と表示されます。このメッセージは、ノンセキュア モードになっているためにアプリケーションが CTL ファイルにヌルの発行者名を書き込むことを示しています。
You cannot delete this item.You can only delete Security Tokens and multi-cluster TFTP	CTL Entries ウィンドウで削除できるのは、セキュリティ トークンと代替 TFTP サーバだけです。
Are you sure you want to delete this item?	このメッセージは、CTL Entries ウィンドウからエントリを削除する前に表示されます。
You have selected to exit the CTL Client application.Are you sure you want to exit?	このメッセージは、Cisco CTL クライアント ウィンドウで Cancel をクリックしたとき、またはウィンドウを終了するときに表示されます。
You must have at least 2 security tokens in the CTL File	Finish をクリックして CTL ファイルに署名する前に、CTL Entries ペインに 2 つ以上のセキュリティ トークンが存在することを確認してください。
You must have at least one CallManager server in the cluster	Finish をクリックして CTL ファイルに署名する前に、CTL Entries ペインに 1 つの Cisco CallManager サーバ（CCM+TFTP 機能を含む）が存在することを確認してください。

表 9-2　Cisco CTL クライアントに関するメッセージ（続き）

メッセージ	修正処置または理由
Could not get CallManager Certificate from server <server name>	次の作業を実行してください。 1. Cisco CallManager サーバにネットワーク接続できることを確認します。 2. Cisco CTL Provider サービスが設定されているポートに、Cisco CTL クライアントが接続されていることを確認します。 3. Cisco CallManager の自己署名証明書が c:\program files\cisco\certificates\ccmserver.cer に存在することを確認します。 4. Cisco CallManager Serviceability で、Cisco CTL Provider サービスの詳細なトレースを有効にし、そのサービスのトレースを検討します。
Entry for Server already exists.	サーバのエントリがすでに CTL ファイル内に存在します。
No Help available.	このウィンドウのオンライン ヘルプは存在しません。
No CTL File exists on the server but the CallManager Cluster Security Mode is in Mixed Mode. You must create the CTL File and set Call Manager Cluster to Mixed Mode.	このメッセージが表示されるのは、CTL ファイルが他のユーザによって手動で削除または改ざんされている場合です。CTL ファイルから、証明書やセキュリティ トークンの情報を含むデータがすべて削除されています。CTL ファイルを再作成します。
The CTL File signature is invalid or the CTL File is corrupt.	CTL ファイルが破損しています。CTL ファイルから、証明書やセキュリティ トークンの情報を含むデータがすべて削除されています。CTL ファイルを再作成します。
You must recreate the CTL File.All existing certificate information in the CTL file will be lost.	Cisco CTL を実行して、CTL ファイルを再作成します。

表 9-2　Cisco CTL クライアントに関するメッセージ（続き）

メッセージ	修正処置または理由
There are no Security Tokens in CTL File.You must have at least 2 security tokens.Select Update CTL File to add security Tokens.	このメッセージが表示されるのは、CTL ファイルが破損している場合、無効の場合、または CTL クライアントでセキュリティ トークン情報を読み取ることができない場合です。CTL ファイルには、2 つ以上のセキュリティ トークンのエントリが含まれている必要があります。**Update CTL File** オプションを選択し、CTL ファイルを再作成します。
Please insert a Security Token.Click Ok when done.	USB ポートに Cisco セキュリティ トークンを挿入します。**OK** をクリックします。このメッセージが引き続き表示される場合は、セキュリティ トークンがシスコから発行されていること、および Etoken Notification サービスと Smart Card サービスが動作していることを確認してください。
Please insert another Security Token.Click Ok when done.	CTL ファイルに新しいトークンを追加するには、USB ポートに Cisco セキュリティ トークンを挿入します。**OK** をクリックします。このメッセージが引き続き表示される場合は、セキュリティ トークンがシスコから発行されていること、および Etoken Notification サービスと Smart Card サービスが動作していることを確認してください。
The Security Token you have inserted already exists in the CTL File.	セキュリティ トークン情報がすでに CTL ファイル内に存在します。ファイル内に存在しないトークンを挿入します。
The Security Token cannot be used to sign the CTL File.The token must already exist in the CTL file.	ファイル内に存在するトークンを挿入して、CTL ファイルに署名する必要があります。
No CTL File.	CTLFile.tlv が存在しません。
Error opening CTL File.	アプリケーションで CTLFile.tlv を開くことができません。Cisco CTL Provider サービスのトレースを検討してください。

表 9-2　Cisco CTL クライアントに関するメッセージ（続き）

メッセージ	修正処置または理由
Error reading CTL File.	システムで CTLFile.tlv を読み取ることができませんでした。Cisco CTL Provider サービスのトレースを検討してください。
CTL Filename or contents are invalid.	CTL ファイル名が無効であるか、CTL ファイルの内容が無効です。CTLFile.tlv が TFTP サービス パラメータの FileLocation パスに存在することを確認し、Cisco CTL Provider サービスのトレースを検討してください。
CTL File is not valid.	CTL ファイルが破損しているか、無効です。Cisco CTL Provider サービスのトレースを検討してください。
CTL File created successfully.	CTL ファイルは TFTPPath ロケーションに存在します。
CTL File operation was not successful on one or all the servers.Please correct the error and run the CTL Client again.	このエラーが表示された CTL クライアント ウィンドウで、サーバ名、パス、およびエラーの理由を確認してください。
You must restart all the CallManager and TFTP nodes in the Cluster.	CTL ファイルを作成したら、サービスを実行するクラスタ内のすべてのサーバ上で Cisco CallManager と TFTP サービスを再起動します。同様に、デバイスもリセットします。
No Valid Server Certificate found.	アプリケーションでセキュリティ トークン証明書を読み取ることができません。セキュリティ トークンがシスコから発行されていること、およびトークンが有効であることを確認してください。
No Server Certificate File found.	アプリケーションで Cisco CallManager サーバから証明書ファイルを読み取ることができません。c:\program files\cisco\certificiates\ccmserver.cer が存在することを確認してください。

表 9-2　Cisco CTL クライアントに関するメッセージ（続き）

メッセージ	修正処置または理由
Server Certificate is Invalid.	アプリケーションが無効な Cisco CallManager 証明書を検出しました。c:\program files\cisco\certificiates\ccmserver.cer が存在することを確認してください。Cisco CTL Provider サービスのトレースを検討してください。
Certificate Date Invalid.	アプリケーションが、証明書に無効なデータが含まれていることを検出しました。Cisco CTL Provider サービスのトレースを検討してください。 Cisco CTL クライアントの Security Token Information ウィンドウで、セキュリティ トークン証明書の発行日と有効期限を確認してください。
Certificate expired.	証明書の期限が切れました。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
Certificate is not of type RSA.	Cisco CallManager 証明書が RSA タイプを使用していません。**ccmserver.cer** をダブルクリックします。Certificate Details ウィンドウで、公開キーに RSA が指定されていることを確認してください。指定されていない場合、Cisco CallManager サーバ証明書は無効です。
No Issuer Name in Certificate.	証明書に発行者名が含まれていません。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
Issuer name is not valid.	証明書の発行者名が無効です。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
Invalid Issuer Name length.	証明書の発行者名の長さが、256 文字を超えています。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。

表 9-2　Cisco CTL クライアントに関するメッセージ（続き）

メッセージ	修正処置または理由
No Subject Name in Certificate.	証明書にサブジェクト名が含まれていません。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
Subject name is not valid.	証明書のサブジェクト名が無効です。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
Invalid Subject Name length.	証明書のサブジェクト名が、256 文字を超えています。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
No Public Key in Certificate.	証明書に公開キーが含まれていません。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
Public Key is not valid.	証明書の公開キーが無効です。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
Invalid Public Key length.	証明書の公開キーの長さが、512 文字を超えています。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
No Private Key File.	証明書に秘密キーが含まれていません。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
Private Key File is not valid.	証明書の秘密キーが無効です。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。

表 9-2　Cisco CTL クライアントに関するメッセージ（続き）

メッセージ	修正処置または理由
Invalid Cipher for Private key.	証明書の秘密キー暗号が無効です。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
Invalid Signature length.	証明書のシグニチャの長さが、1024 文字を超えています。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
Invalid Signature Algorithm.	証明書のシグニチャ アルゴリズムが無効です。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
No Signature.	証明書にシグニチャが含まれていません。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
Invalid Thumbprint.	証明書の指紋が無効です。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
Invalid Serial Number.	証明書のシリアル番号が無効です。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
Invalid Serial Number length.	証明書のシリアル番号が、256 文字を超えています。Cisco CTL Provider サービスのトレースを検討してください。セキュリティ トークンの証明書を検討してください。
Error Opening Security Token Store.	アプリケーションでセキュリティ トークン証明書を読み取ることができません。Etoken Notification サービスと Smart Card サービスが動作していることを確認してください。

表 9-2　Cisco CTL クライアントに関するメッセージ（続き）

メッセージ	修正処置または理由
No Certificate in Security Token.	セキュリティ トークンに証明書が含まれていません。セキュリティ トークンがシスコから発行されていることを確認してください。
Could not Sign Message.	Cisco CTL クライアントで CTL ファイルの内容に署名できません。Cisco CTL クライアントのトレースを検討してから、Cisco CTL クライアントを再度実行します。
Could not verify Message.	Cisco CTL クライアントで、CTL ファイルの内容への署名後にシグニチャを確認できません。Cisco CTL クライアントのトレースを検討してから、Cisco CTL クライアントを再度実行します。
Could not sign CTL File.	Cisco CTL クライアントのトレースを検討してから、Cisco CTL クライアントを再度実行します。
For the security of the phones, tokens inserted during update cannot be used to sign the CTL File.You must use one of the tokens that already existed in the CTL file to sign.Once this token has been inserted and the phones have been restarted, you may use the new tokens to sign the CTL File.	このメッセージは、修正処置を示しています。
Error Initializing SDI Control.	CTL Provider のトレースの初期化時に重大エラーが発生しました。Cisco CallManager Serviceability でトレースを設定します。
DBL Exception occurred.	CTL Provider の Database 層の初期化時に重大エラーが発生しました。DBL ログで例外を検討してください。

表 9-2　Cisco CTL クライアントに関するメッセージ（続き）

メッセージ	修正処置または理由
CM Name is too long.	入力した Cisco CallManager ホスト名が、256 文字を超えています。ホスト名を再度入力します。
Init TLS Failed.	アプリケーションで、Cisco CTL クライアントと Cisco CTL Provider サービスの間の SSL を初期化できません。Cisco CTL クライアントのトレースを検討してから、Cisco CTL クライアントを再度実行します。
TLS Connect Error when Opening Sockets.	Cisco CTL クライアントのトレースを検討してから、Cisco CTL クライアントを再度実行します。
Error occurred during SSL Handshake.	Cisco CTL クライアントのトレースを検討してから、Cisco CTL クライアントを再度実行します。
Could not connect to CTL provider Service.	クライアントの接続する Cisco CTL Provider ホスト名が、有効およびアクセス可能であることを確認してください。CTL Provider が、クライアントの接続するポートを傍受していることを確認してください。
Parsing data from CTLProvider failed.	内部エラーが発生しました。Cisco CTL クライアントが、Cisco CTL Provider サービスから無効なデータを受信しました。
Error occurred during Post CTL File operation.	Cisco CTL クライアントがクラスタ内のサーバに CTL ファイルをコピーしようとしたときに、内部エラーが発生しました。
Error occurred during Get CAPF File operation.	Cisco CTL クライアントが certificate trust list フォルダからファイルを取得しようとしたときに、内部エラーが発生しました。
Error occurred during Get CCM Certificate operation.	Cisco CTL クライアントが Cisco CallManager 証明書を取得しようとしたときに、内部エラーが発生しました。
Error occurred during Get CAPF Certificate operation.	Cisco CTL クライアントが CAPF 証明書を取得しようとしたときに、内部エラーが発生しました。

表 9-2　Cisco CTL クライアントに関するメッセージ（続き）

メッセージ	修正処置または理由
Error occurred during Authenticate User operation.	Cisco CTL クライアントがユーザを認証しようとしたときに、内部エラーが発生しました。
Invalid Response for Authenticate User operation.	Cisco CTL クライアントのバージョンが、Cisco CTL Provider サービスと互換性がありません。Cisco CallManager Administration 4.1 に表示される Cisco CTL クライアント プラグインをインストールおよび設定します。
Invalid Response for Get CCM List operation.	Cisco CTL クライアントのバージョンが、Cisco CTL Provider サービスと互換性がありません。Cisco CallManager Administration 4.1 に表示される Cisco CTL クライアント プラグインをインストールおよび設定します。
Invalid Response for Get CCM Certificate operation.	Cisco CTL クライアントのバージョンが、Cisco CTL Provider サービスと互換性がありません。Cisco CallManager Administration 4.1 に表示される Cisco CTL クライアント プラグインをインストールおよび設定します。
Invalid Response for Get CAPF Certificate operation.	Cisco CTL クライアントのバージョンが、Cisco CTL Provider サービスと互換性がありません。Cisco CallManager Administration 4.1 に表示される Cisco CTL クライアント プラグインをインストールおよび設定します。
Invalid Response for get CTL File operation.	Cisco CTL クライアントのバージョンが、Cisco CTL Provider サービスと互換性がありません。Cisco CallManager Administration 4.1 に表示される Cisco CTL クライアント プラグインをインストールおよび設定します。
Invalid Response for Get CAPF File operation.	Cisco CTL クライアントのバージョンが、Cisco CTL Provider サービスと互換性がありません。Cisco CallManager Administration 4.1 に表示される Cisco CTL クライアント プラグインをインストールおよび設定します。

表 9-2　Cisco CTL クライアントに関するメッセージ（続き）

メッセージ	修正処置または理由
Invalid Response for Get Cluster Security Mode operation.	Cisco CTL クライアントのバージョンが、Cisco CTL Provider サービスと互換性がありません。Cisco CallManager Administration 4.1 に表示される Cisco CTL クライアント プラグインをインストールおよび設定します。
Invalid Response for Get CTL Version operation.	Cisco CTL クライアントのバージョンが、Cisco CTL Provider サービスと互換性がありません。Cisco CallManager Administration 4.1 に表示される Cisco CTL クライアント プラグインをインストールおよび設定します。
Invalid Response for Get Alternate Paths operation.	Cisco CTL クライアントのバージョンが、Cisco CTL Provider サービスと互換性がありません。Cisco CallManager Administration 4.1 に表示される Cisco CTL クライアント プラグインをインストールおよび設定します。
Invalid Response for Authenticate User operation.	Cisco CTL クライアントのバージョンが、Cisco CTL Provider サービスと互換性がありません。Cisco CallManager Administration 4.1 に表示される Cisco CTL クライアント プラグインをインストールおよび設定します。
Not enough Memory to run Application.	システム メモリが不足しているため、Cisco CTL クライアントを実行できません。メモリ リソースを開放してから、Cisco CTL クライアントを再実行します。
Could not get CAPF Certificate(s).CAPF Service seems to be running on the CCM Publisher but the certificate file(s) do not exist in the Certificates trust path.Please check if the following certificates exist.	パブリッシャ データベース サーバ上で CAPF Service をアクティブにした場合は、capf.cer ファイルおよび対応する capf (.0) ファイルが certificates trust フォルダに存在することを確認してください。

表 9-2　Cisco CTL クライアントに関するメッセージ（続き）

メッセージ	修正処置または理由
Entry for this certificate already exists.	代替 TFTP サーバが CTL ファイル内に存在しないことを確認してください。
Failed to set Cluster Security Mode on the CallManager publisher.You must run the CTL Client again to set the correct value for the Cluster Security Mode.	CTL クライアントで Cluster Security Mode を正しい値に設定できません。このメッセージは、修正処置を示しています。
The Alternate TFTP Server entry is invalid.You must delete the entry for the Alternate TFTP Server and add it again	Cisco CTL Entries ペインから代替 TFTP サーバのエントリを削除し、エントリを再度追加します。このタスクを実行しないと、IP Phone が登録に失敗する場合があります。

関連項目

- システム要件（P.1-5）
- 対話および制限（P.1-6）
- Cisco CTL クライアントのインストール（P.3-10）
- Cisco CTL クライアントの設定（P.3-14）
- CTL ファイルの更新（P.3-20）
- ログ ファイルの検討（P.9-4）

CTL ファイルに問題がある場合の IP Phone のトラブルシューティング

表 9-3 は、IP Phone 上の CTL ファイルに関して発生する可能性のある問題を説明しています。

表 9-3 の修正処置を実行するには、CTL ファイル内に存在するセキュリティ トークンを 1 つ取得します。CTL ファイルを更新するには、P.3-20 の「CTL ファイルの更新」を参照してください。

表 9-3　IP Phone に関連する CTL ファイルの問題

問題	考えられる原因	修正処置
IP Phone が CTL ファイルを認証できない。	次の原因を検討してください。 • 最新の CTL ファイルに署名したセキュリティ トークンが、IP Phone 上の CTL ファイル内に存在しない。 • 既存の CTL ファイルに新しいセキュリティ トークンを追加しようとした。ファイルに追加された最後のトークンを使用して CTL ファイルに署名しようとした。IP Phone 上の既存の CTL ファイルに、新しいセキュリティ トークンのレコードが含まれていない可能性がある。	CTL ファイルを更新し、ファイル内に存在するセキュリティ トークンを使用して CTL ファイルに署名します。 問題が引き続き発生する場合は、IP Phone から CTL ファイルを削除し、Cisco CTL クライアントを再度実行します。
IP Phone が、CTL ファイル以外の設定ファイルを認証できない。	CTL ファイル内に不適切な TFTP エントリが存在する。	CTL ファイルを更新します。
IP Phone が TFTP 認証エラーを報告する。	次の原因を検討してください。 • IP Phone の代替 TFTP アドレスが CTL ファイル内に存在しない。 • 新しい TFTP レコードを含む新しい CTL ファイルを作成した場合、IP Phone 上の既存の CTL ファイルに新しい TFTP サーバのレコードが含まれていない可能性がある。	CTL ファイルを更新します。 新しい CTL ファイルに含まれている TFTP 情報が、IP Phone 上の既存の CTL ファイル内の情報と異なる場合は、IP Phone から既存の CTL ファイルを削除します。P.9-33 の「Cisco IP Phone 上の CTL ファイルの削除」を参照してください。

表 9-3　IP Phone に関連する CTL ファイルの問題（続き）

問題	考えられる原因	修正処置
IP Phone が Cisco CallManager に登録されない。	CTL ファイルに、Cisco CallManager サーバに関する正しい情報が含まれていない。 自動登録が有効になっている可能性がある。	自動登録が無効になっていることを確認してください。 CTL ファイルを更新します。
IP Phone が、ローカルで有効な証明書を取得するための正しい CAPF サーバと相互対話しない。 TLS ハンドシェイク エラーが発生する。	CTL ファイルが最後に更新された後で、CAPF 証明書が変更されている。	CTL ファイルを更新します。
IP Phone が署名付きの設定ファイルを要求しない。	CTL ファイルに含まれている TFTP エントリに、証明書が関連付けられていない。	CTL ファイルを更新します。 CTL ファイルを更新したら、Cisco CallManager クラスタ全体のセキュリティ モードを混合モードに設定したことを確認してください。

関連項目

- システム要件（P.1-5）
- Cisco CTL Provider サービスのアクティブ化（P.3-5）
- Cisco CTL クライアントのインストール（P.3-10）
- Cisco CTL クライアントの設定（P.3-14）
- CTL ファイルの更新（P.3-20）
- ログ ファイルの検討（P.9-4）

Cisco IP Phone およびサーバ上の CTL ファイルの比較

IP Phone 上の CTL ファイルのバージョンを特定するには、MD5 ハッシュを計算します。MD5 ハッシュとは、ファイルの内容に基づいて計算される暗号ハッシュです。

IP Phone には、MD5 ハッシュ値を計算するための、CTL ファイル用のオプションがあります。MD5 アプリケーションを使用すると、ディスク上でファイルの MD5 ハッシュを計算できます。ディスク上に保存されている CTL ファイルのハッシュ値を電話機に表示されている値と比較すると、電話機にどのバージョンがインストールされているかがわかります。

IP Phone 上の CTL ファイルのバージョンを特定したら、サーバの CTL ファイルに対して MD5 チェックを実行すると、IP Phone が正しい CTL ファイルを使用していることを確認できます。

MD5 値を計算するには、次の手順を実行します。

手順

ステップ 1　CTL ファイルが存在するサーバ上で、コマンド ウィンドウを開き、**cd c:\program files\cisco\bin** と入力します。

ステップ 2　ファイルの MD5 値を計算するには、**MD5UTIL.EXE <drive:><path><filename>** と入力します。

ヒント　<drive:><path> <filename> という変数は、MD5 値の計算対象となるドライブ、ディレクトリ、またはその両方を指定します。この説明を CLI に表示するには、**md5util -?** と入力します。

たとえば、CTL ファイルの MD5 値を計算するには、
MD5UTIL.exe c:\program files\cisco\tftppath\ctlfile.tlv と入力します。

関連項目

- Cisco CTL Provider サービスのアクティブ化（P.3-5）
- Cisco CTL クライアントの設定（P.3-14）
- CTL ファイルの更新（P.3-20）
- Cisco CTL クライアント設定（P.3-24）

Cisco 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 CallManager 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 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。
- IP Phone をセキュア クラスタから、ストレージ領域、ノンセキュア 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。
- IP Phone 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 クラスタへと移動する。
- 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 IP Phone 上の CTL ファイルを削除するには、表 9-4 の作業を実行します。

表 9-4　Cisco IP Phone 上の CTL ファイルの削除

Cisco IP Phone モデル	作業
Cisco IP Phone 7960 および 7940	IP Phone 上の Security Configuration メニューにある、**CTL file**、**unlock** または ****#**、および **erase** を押します。
Cisco IP Phone 7970	次の方法のどちらかを実行します。 • Security Configuration メニューのロックを解除します（『*Cisco IP Phone アドミニストレーション ガイド for Cisco CallManager*』を参照）。CTL オプションの下にある **Erase** ソフトキーを押します。 • Settings メニューにある **Erase** ソフトキーを押します。 （注）　Settings メニューにある Erase 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 IP Phone アドミニストレーション ガイド for Cisco CallManager*』を参照してください。

関連項目

- システム要件（P.1-5）
- Cisco CTL Provider サービスのアクティブ化（P.3-5）
- Cisco CTL クライアントのインストール（P.3-10）
- Cisco CTL クライアントの設定（P.3-14）
- CTL ファイルの更新（P.3-20）
- ログ ファイルの検討（P.9-4）

サーバ上の CTL ファイルの削除

次の状況が発生した場合は、サーバ上の 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。

ヒント　Cisco CallManager または Cisco TFTP サービスが動作するクラスタ内のサーバすべてからファイルを必ず削除してください。

CTL ファイルを削除するには、次の手順を実行します。

手順

ステップ 1　**C:\Program Files\Cisco\tftppath**（デフォルトの場所）または CTLFile.tlv が保存されている場所を参照します。

ステップ 2　**CTLFile.tlv** を右クリックし、**Delete** を選択します。

ステップ 3　Cisco CallManager または Cisco TFTP サービスが動作するクラスタ内のサーバすべてについて、この手順を実行します。

関連項目

- システム要件（P.1-5）
- Cisco CTL Provider サービスのアクティブ化（P.3-5）
- Cisco CTL クライアントのインストール（P.3-10）
- Cisco CTL クライアントの設定（P.3-14）
- CTL ファイルの更新（P.3-20）
- ログ ファイルの検討（P.9-4）

セキュリティ トークン（Etoken）を 1 つ紛失した場合のトラブルシューティング

セキュリティ トークンを 1 つ紛失した場合は、次の手順を実行します。

手順

ステップ 1　新しいセキュリティ トークンを購入します。

ステップ 2　CTL ファイルに署名したトークンを使用し、次の作業を実行して CTL ファイルを更新します。

a. 新しいトークンを CTL ファイルに追加します。
b. 紛失したトークンを CTL ファイルから削除します。

各作業の実行方法の詳細については、P.3-20 の「CTL ファイルの更新」を参照してください。

ステップ 3　IP Phone をすべてリセットします（P.1-11 の「デバイスのリセット、サービスの再起動、またはサーバおよびクラスタのリブート」を参照）。

関連項目

- システム要件（P.1-5）
- Cisco CTL Provider サービスのアクティブ化（P.3-5）
- Cisco CTL クライアントのインストール（P.3-10）
- Cisco CTL クライアントの設定（P.3-14）
- CTL ファイルの更新（P.3-20）
- ログ ファイルの検討（P.9-4）

セキュリティ トークン（Etoken）をすべて紛失した場合のトラブルシューティング

ヒント　次の手順は、定期のメンテナンス期間に実行してください。これは、変更内容を有効にするために、クラスタ内のサーバすべてをリブートする必要があるためです。

セキュリティ トークンを紛失した場合、CTL ファイルを更新する必要がある場合は、次の手順を実行します。

手順

ステップ 1　各 Cisco CallManager、Cisco TFTP、または代替 TFTP サーバ上で、CTLFile.tlv ファイルが存在するディレクトリを参照します。

デフォルト ディレクトリは、C:\program files\cisco\tftppath です。CTL ファイルが保存されている場所を特定するには、Cisco CallManager Administration の Service Parameters ウィンドウで、TFTP サービスの File Location サービス パラメータを見つけます。

ステップ 2　**CTLFile.tlv** を削除します。

ステップ 3　ステップ 1 とステップ 2 を、すべての Cisco CallManager、Cisco TFTP、および代替 TFTP サーバについて繰り返します。

ステップ 4　新しいセキュリティ トークンを 2 つ以上取得します。

ステップ 5　Cisco CTL クライアントを使用して、CTL ファイルを作成します（P.3-10 の「Cisco CTL クライアントのインストール」と P.3-14 の「Cisco CTL クライアントの設定」を参照）。

ヒント　クラスタ全体のセキュリティ モードが混合モードの場合は、Cisco CTL クライアントにより、「No CTL File exists on the server but the CallManager Cluster Security Mode is in Mixed Mode.For the system to function, you must create the CTL File and set CallManager Cluster to Mixed Mode.」というメッセージが表示されます。**OK** をクリックします。次に、**Set Call Manager Cluster to Mixed Mode** を選択して、CTL ファイルの設定を完了します。

ステップ 6　すべてのサーバ上に CTL ファイルを作成したら、IP Phone から CTL ファイルを削除します（P.9-33 の「Cisco IP Phone 上の CTL ファイルの削除」を参照）。

ステップ 7　クラスタ内のサーバをすべてリブートします。

関連項目

- システム要件（P.1-5）
- Cisco CTL Provider サービスのアクティブ化（P.3-5）
- Cisco CTL クライアントのインストール（P.3-10）
- Cisco CTL クライアントの設定（P.3-14）
- CTL ファイルの更新（P.3-20）
- ログ ファイルの検討（P.9-4）

Cisco CallManager クラスタのセキュリティ モードの確認

Cisco CallManager 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。

手順

ステップ 1　Cisco CallManager Administration で、**System > Enterprise Parameters** 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 CallManager クラスタは混合モードに正しく設定されています。

ヒント　この値は、Cisco CallManager Administration では変更できません。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。

関連項目

- システム要件（P.1-5）
- Cisco CTL Provider サービスのアクティブ化（P.3-5）
- Cisco CTL クライアントのインストール（P.3-10）
- Cisco CTL クライアントの設定（P.3-14）
- CTL ファイルの更新（P.3-20）
- ログ ファイルの検討（P.9-4）

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、クラスタ全体のセキュリティ 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 2000 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　**Start > Control Panel > Add Remove Programs** の順に選択します。

ステップ 2　**Add Remove Programs** 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　クライアントを削除するには、**Remove** をクリックします。

関連項目

- システム要件（P.1-5）
- Cisco CTL Provider サービスのアクティブ化（P.3-5）
- Cisco CTL クライアントのインストール（P.3-10）
- Cisco CTL クライアントの設定（P.3-14）
- CTL ファイルの更新（P.3-20）
- ログ ファイルの検討（P.9-4）

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。
- **Start > Programs > 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。

関連項目

- Cisco CTL Provider サービスのアクティブ化（P.3-5）
- Cisco CTL クライアントのインストール（P.3-10）
- Cisco CTL クライアントの設定（P.3-14）

CAPF のトラブルシューティング

この項では、次のトピックについて取り上げます。

- CAPF に関するメッセージ（P.9-42）
- IP Phone での認証文字列のトラブルシューティング（P.9-44）
- ローカルで有効な証明書の検証が失敗する場合のトラブルシューティング（P.9-45）
- CAPF 証明書がクラスタ内のサーバすべてにインストールされていることの確認（P.9-45）
- ローカルで有効な証明書が IP Phone 上に存在することの確認（P.9-46）
- Manufacture-Installed Certificate（MIC）が IP Phone 内に存在することの確認（P.9-46）

CAPF に関するメッセージ

表 9-5 は、CAPF に関するメッセージと修正処置を示しています。

表 9-5　CAPF に関するメッセージ

メッセージ	修正処置
Authentication String contains one or more invalid characters.Valid characters for Authentication String are numbers.	メッセージで指摘されたように、適切な情報を入力します。
CAPF Authentication String length should be between 4 and 10.	4 桁以上 10 桁未満を入力します。
Operation Completes By contains one or more invalid characters.Valid characters for Operation Completes By are numbers.	メッセージで指摘されたように、適切な情報を入力します。
Invalid Year.Please enter a value equal to or greater than the current year.	このメッセージは、修正処置を示しています。
Invalid Month.Please adjust your entry to continue.	このメッセージは、修正処置を示しています。

表 9-5　CAPF に関するメッセージ（続き）

メッセージ	修正処置
Invalid Date.Please enter a value equal to or greater than the current date.	過去の日付を入力しました。適切な日付を入力します。
Invalid Date.Please adjust your entry to continue.	その月に対して無効な日付を入力しました。適切な日付を入力します。
Invalid Time.Please enter a value equal to or greater than current time (hours).	過去の時間を入力しました。適切な時間を入力します。
Invalid Time.Please adjust your entry to continue.	このメッセージは、修正処置を示しています。

関連項目

- システム要件（P.1-5）
- 対話および制限（P.1-6）
- Certificate Authority Proxy Function の概要（P.4-2）
- CAPF の設定用チェックリスト（P.4-10）
- Phone Configuration ウィンドウの CAPF 設定（P.4-21）
- 電話機での認証文字列の入力（P.4-26）

IP Phone での認証文字列のトラブルシューティング

IP Phone で不適切な認証文字列を入力すると、IP Phone 上にメッセージが表示されます。IP Phone に正しい認証文字列を入力します。

ヒント　IP Phone が Cisco CallManager に登録されていることを確認してください。IP Phone が Cisco CallManager に登録されていない場合、IP Phone で認証文字列を入力することはできません。

IP Phone のデバイス セキュリティ モードがノンセキュアになっていることを確認してください。

CAPF では、IP Phone で認証文字列を入力できる連続試行回数が制限されています。10 回連続で正しい認証文字列が入力されなかった場合は、正しい文字列の入力を再試行できる状態になるまでに、10 分以上かかります。

関連項目

- 電話機での認証文字列の入力（P.4-26）
- CAPF の設定用チェックリスト（P.4-10）
- Phone Configuration ウィンドウの CAPF 設定（P.4-21）

ローカルで有効な証明書の検証が失敗する場合のトラブルシューティング

IP Phone では、次のような場合に、ローカルで有効な証明書の検証が失敗することがあります。たとえば、証明書が CAPF によって発行されたバージョンでない場合、CAPF 証明書がクラスタ内の一部のサーバ上に存在しない場合、CAPF 証明書が CAPF ディレクトリ内に存在しない場合、IP Phone が Cisco CallManager に登録されていない場合などです。ローカルで有効な証明書の検証が失敗する場合は、SDL トレース ファイルと CAPF トレース ファイルでエラーを検討します。

関連項目

- 電話機での認証文字列の入力（P.4-26）
- CAPF の設定用チェックリスト（P.4-10）
- Phone Configuration ウィンドウの CAPF 設定（P.4-21）
- ログ ファイルの検討（P.9-4）
- Certificate Authority Proxy Function の概要（P.4-2）

CAPF 証明書がクラスタ内のサーバすべてにインストールされていることの確認

Cisco Certificate Authority Proxy Function サービスをアクティブにすると、CAPF に固有なキー ペアおよび証明書が CAPF によって自動生成されます。CAPF 証明書は Cisco CTL クライアントによってクラスタ内のすべてのサーバにコピーされ、拡張子 .0 を使用します。CAPF 証明書が存在することを確認するには、クラスタ内の各サーバで C:\Program Files\Cisco\Certificates を参照し、次のファイルを見つけます。

- DER 符号化形式の場合：CAPF.cer
- PEM 符号化形式の場合：CAPF.cer と同じ通常名文字列が含まれる .0 拡張子ファイル

関連項目

- 電話機での認証文字列の入力（P.4-26）
- CAPF の設定用チェックリスト（P.4-10）
- Phone Configuration ウィンドウの CAPF 設定（P.4-21）

ローカルで有効な証明書が IP Phone 上に存在することの確認

ローカルで有効な証明書が IP Phone にインストールされていることを確認するには、**Settings > Model Information** の順に選択し、LSC 設定を表示します。LSC 設定では、環境に応じて、**Installed** または **Not Installed** と表示されます。

関連項目

- 電話機での認証文字列の入力（P.4-26）
- CAPF の設定用チェックリスト（P.4-10）
- Phone Configuration ウィンドウの CAPF 設定（P.4-21）

Manufacture-Installed Certificate（MIC）が IP Phone 内に存在することの確認

MIC が IP Phone 内に存在することを確認するには、IP Phone の Security Configuration メニューで MIC option を選択します。この設定では、環境に応じて、**Installed** または **Not Installed** と表示されます。

関連項目

- CAPF の設定用チェックリスト（P.4-10）
- Phone Configuration ウィンドウの CAPF 設定（P.4-21）
- ログ ファイルの検討（P.9-4）
- Certificate Authority Proxy Function の概要（P.4-2）

CAPF 1.0(1) ユーティリティのアンインストール

CAPF 1.0(1) ユーティリティをアンインストールするには、**Add/Remove Programs** に移動してアプリケーションを削除します。ユーティリティの削除後、P.9-47 の「新規 CAPF 証明書の生成」を参照してください。

新規 CAPF 証明書の生成

Certificate Authority Proxy Function には、独自の証明書と、認証に使用される秘密キーが含まれています。たとえば CAPF 1.0(1) ユーティリティの削除後など、CAPF 証明書または秘密キーが存在しない場合は、次の手順を実行します。

手順

ステップ 1　C:\Program Files\Cisco\Certificates にある CAPF.cer ファイルの最新のコピーを、覚えやすい場所に保存します。

ステップ 2　C:\Program Files\Cisco\Certificates にある CAPF.cer ファイルを削除します。

ステップ 3　Cisco CallManager Serviceability で、Cisco Certificate Authority Proxy Function（CAPF）サービスを停止して起動します。

ステップ 4　CTL ファイルを更新します。

ステップ 5　更新された CTL ファイルを電話機がダウンロードしたことを確認します。

電話機および Cisco IOS MGCP ゲートウェイの暗号化のトラブルシューティング

この項では、次のトピックについて取り上げます。

- パケット キャプチャの概要（P.9-48）
- パケット キャプチャの設定チェックリスト（P.9-49）
- パケット キャプチャ サービス パラメータの設定（P.9-50）
- パケット キャプチャ サービス パラメータ（P.9-51）
- BAT に対する IP Phone のパケット キャプチャの設定（P.9-52）
- Phone Configuration ウィンドウでのパケット キャプチャの設定（P.9-53）
- エンドポイント ID の MGCP Gateway Configuration ウィンドウでのパケット キャプチャの設定（P.9-54）
- IP Phone のパケット キャプチャおよび MGCP ゲートウェイ設定の設定値（P.9-56）
- キャプチャされたパケットの解析（P.9-57）
- Cisco CallManager Administration でのパケット キャプチャに関するメッセージ（P.9-58）
- 暗号化および割り込みの設定に関するメッセージ（P.9-59）

パケット キャプチャの概要

暗号化を有効にした後は、メディア パケットと TCP パケットのスニファを実行するサードパーティ製のトラブルシューティング ツールが連動しないため、問題が発生する場合は、Cisco CallManager Administration を使用して次の作業を実行する必要があります。

- Cisco CallManager とデバイス（電話機または Cisco IOS MGCP ゲートウェイ）の間で交換されるメッセージのパケットを分析する。
- デバイス間の SRTP パケットをキャプチャする。
- メッセージからメディアの暗号化キー関連情報を抽出し、デバイス間のメディアを復号化する。

関連項目

- パケット キャプチャの設定チェックリスト（P.9-49）

- パケット キャプチャ サービス パラメータ（P.9-51）
- IP Phone のパケット キャプチャおよび MGCP ゲートウェイ設定の設定値（P.9-56）
- キャプチャされたパケットの解析（P.9-57）
- Cisco CallManager Administration でのパケット キャプチャに関するメッセージ（P.9-58）

パケット キャプチャの設定チェックリスト

該当するデータを抽出および解析するには、次に示す表 9-6 の作業を実行します。

表 9-6　パケット キャプチャの設定チェックリスト

設定手順		関連手順および関連項目
ステップ 1	Cisco CallManager Administration の Service Parameter ウィンドウでパケット キャプチャを有効にします。	• パケット キャプチャ サービス パラメータの設定（P.9-50） • パケット キャプチャ サービス パラメータ（P.9-51）
ステップ 2	サービス パラメータのデフォルト設定を使用しない場合は、Service Parameter ウィンドウで別の適用可能なサービス パラメータに更新します。	• パケット キャプチャ サービス パラメータの設定（P.9-50） • パケット キャプチャ サービス パラメータ（P.9-51）
ステップ 3	Phone or MGCP Gateway Configuration ウィンドウで、デバイスごとにパケット キャプチャを設定します。 **（注）** パケット キャプチャを一度に多くのデバイスに対して有効にしないことを強くお勧めします。これは、そのように設定すると、ネットワークにおける CPU 消費量が高くなる場合があるためです。	• Phone Configuration ウィンドウでのパケット キャプチャの設定（P.9-53） • IP Phone のパケット キャプチャおよび MGCP ゲートウェイ設定の設定値（P.9-56）
ステップ 4	関係するデバイス間でスニファ トレースを使用して、SRTP パケットをキャプチャします。	ご使用のスニファ トレース ツールをサポートするマニュアルを参照してください。

表 9-6　パケット キャプチャの設定チェックリスト（続き）

設定手順		関連手順および関連項目
ステップ 5	パケットをキャプチャしたら、Signal Packet Capture Mode を **None** に設定し、Packet Capture Enable サービス パラメータを **False** に設定します。	• パケット キャプチャ サービス パラメータの設定（P.9-50） • パケット キャプチャ サービス パラメータ（P.9-51）
ステップ 6	パケットの解析に必要なファイルを収集します。	キャプチャされたパケットの解析（P.9-57）
ステップ 7	Cisco Technical Assistance Center（TAC）がパケットを解析します。この作業を実行するには、TAC に直接連絡してください。	キャプチャされたパケットの解析（P.9-57）

パケット キャプチャ サービス パラメータの設定

パケット キャプチャのパラメータを設定するには、次の手順を実行します。

手順

ステップ 1　Cisco CallManager Administration で、**Service > Service Parameters** の順に選択します。

ステップ 2　Server ドロップダウン リスト ボックスから、Cisco CallManager 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　Service ドロップダウン リスト ボックスから、**Cisco CallManager** サービスを選択します。

ステップ 4　Packet Capture パラメータまでスクロールし、設定値を設定します（表 9-7 を参照）。

ステップ 5　変更内容を有効にするには、**Update** をクリックします。

ステップ 6　パケット　キャプチャの設定を続けるには、次の項のいずれかを参照してください。

- Phone Configuration ウィンドウでのパケット キャプチャの設定（P.9-53）
- エンドポイント ID の MGCP Gateway Configuration ウィンドウでのパケット キャプチャの設定（P.9-54）

関連項目

- パケット キャプチャの設定チェックリスト（P.9-49）
- パケット キャプチャ サービス パラメータ（P.9-51）

パケット キャプチャ サービス パラメータ

P.9-50 の「パケット キャプチャ サービス パラメータの設定」および表 9-7 を参照してください。

表 9-7　パケット キャプチャ サービス パラメータ

パラメータ	説明
Packet Capture Enable	このパラメータは、TLS 接続でのパケット キャプチャを有効にします。デフォルト値については、Service Parameter ウィンドウに表示される i ボタンをクリックしてください。
Packet Capture Service Listen TLS Port	このポートは、TLS 接続でのパケットをキャプチャするためのリアルタイム デバッグ ツールからの要求を受け付けます。デフォルト値については、Service Parameter ウィンドウに表示される i ボタンをクリックしてください。
Packet capture Max real time Client Connections	このパラメータは、パケット キャプチャに使用可能なリアルタイム デバッグ ツールからの接続の最大数を指定します。デフォルト値については、Service Parameter ウィンドウに表示される i ボタンをクリックしてください。

表 9-7　パケット キャプチャ サービス パラメータ

パラメータ	説明
Packet Capture Max File	このパラメータは、バッチ モードのデバッグ時に Cisco CallManager で作成されるパケット キャプチャ ファイルの最大サイズを指定します。最大値に達すると、Cisco CallManager はファイルへの書き込みを停止します。デフォルト値と最大値については、Service Parameter ウィンドウに表示される i ボタンをクリックしてください。

関連項目

- パケット キャプチャの設定チェックリスト（P.9-49）
- パケット キャプチャ サービス パラメータの設定（P.9-50）
- IP Phone のパケット キャプチャおよび MGCP ゲートウェイ設定の設定値（P.9-56）

BAT に対する IP Phone のパケット キャプチャの設定

この Cisco CallManager リリースと互換性のある Bulk Administration Tool を使用すると、電話機で Packet Capture モードを設定できます。この作業の実行方法については、『*Bulk Administration Tool ユーザ ガイド*』を参照してください。

ヒント　BAT でこの作業を実行すると、CPU 消費量が高くなり、コール処理が中断される場合があります。この作業は、コール処理の中断を最小限に抑えられるときに実行することを強くお勧めします。

関連項目

- *Bulk Administration Tool ユーザ ガイド*
- パケット キャプチャの概要（P.9-48）
- パケット キャプチャの設定チェックリスト（P.9-49）

Phone Configuration ウィンドウでのパケット キャプチャの設定

Service Parameter ウィンドウでパケット キャプチャを有効にしたら、Cisco CallManager Administration の Phone Configuration ウィンドウで、デバイスごとにパケット キャプチャを設定する必要があります。

パケット キャプチャを電話機ごとに有効または無効にします。パケット キャプチャのデフォルト設定は、None です。

ヒント　パケット　キャプチャを一度に多くの電話機に対して有効にしないことを強くお勧めします。これは、そのように設定すると、Cisco CallManager ネットワークにおける CPU 消費量が高くなる場合があるためです。

パケットをキャプチャしない場合や、作業が完了した場合は、Signal Packet Capture Mode を None に設定し、Packet Capture Enable サービス パラメータを False に設定します。

保護された電話機でパケット キャプチャを設定する場合は、次のガイドラインを考慮してください。

1. パケット キャプチャを設定する前に、P.9-49 の「パケット キャプチャの設定チェックリスト」を参照してください。
2. Cisco CallManager Administration のデバイスにアクセスするには、**Device > Phone** を選択します。
3. IP Phone の検索対象を指定してから **Find** をクリックするか、**Find** をクリックして IP Phone すべてのリストを表示します。データベースに電話機を追加していない場合、電話機はリストに表示されません。IP Phone の追加については、『*Cisco CallManager アドミニストレーション ガイド*』を参照してください。
4. デバイス名をクリックして、デバイスの Phone Configuration ウィンドウを開きます。
5. トラブルシューティングの設定値を設定します（P.9-56 の「IP Phone のパケット キャプチャおよび MGCP ゲートウェイ設定の設定値」を参照）。
6. 設定の完了後、**Update** をクリックしてから **Reset Phone** をクリックします。

ヒント　IP Phone をリセットすると、ゲートウェイ上のアクティブ コールは終了します。

7. 関係するデバイス間でスニファ トレースを使用して、SRTP パケットをキャプチャします。
8. パケットをキャプチャしたら、Signal Packet Capture Mode を **None** に設定し、Packet Capture Enable サービス パラメータを **False** に設定します。
9. 詳細については、P.9-57 の「キャプチャされたパケットの解析」を参照してください。

関連項目

- IP Phone のパケット キャプチャおよび MGCP ゲートウェイ設定の設定値（P.9-56）
- パケット キャプチャの設定チェックリスト（P.9-49）

エンドポイント ID の MGCP Gateway Configuration ウィンドウでのパケット キャプチャの設定

ヒント　Cisco IOS MGCP ゲートウェイが『*Cisco CallManager セキュリティ ガイド*』で説明されている音声セキュリティ機能をサポートしているかどうかについては、『*Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*』を参照してください。ご使用の Cisco IOS MGCP ゲートウェイが SRTP をサポートしている場合は、Cisco CallManager Administration を使用してパケットをキャプチャできます。

Cisco IOS MGCP ゲートウェイが Cisco CallManager に登録すると、システムはゲートウェイ上のすべてのデバイスに対してデータベースから設定済みの Signal Packet Capture Mode と Packet Capture Duration を取得します。

ヒント　パケット キャプチャを一度に多くのデバイスに対して有効にしないことを強くお勧めします。これは、そのように設定すると、Cisco CallManager ネットワークにおける CPU 消費量が高くなる場合があるためです。

パケットをキャプチャしない場合や、作業が完了した場合は、Signal Packet Capture Mode を None に設定し、Packet Capture Enable サービス パラメータを False に設定します。

パケット キャプチャを設定する場合は、次のガイドラインを考慮してください。

1. パケット キャプチャを設定する前に、P.9-49 の「パケット キャプチャの設定チェックリスト」を参照してください。
2. Cisco CallManager Administration のゲートウェイにアクセスするには、**Device > Gateway** の順に選択します。
3. パケット キャプチャを設定する Cisco IOS MGCP ゲートウェイを検索します。この作業を実行する方法については、『*Cisco CallManager アドミニストレーション ガイド*』を参照してください。
4. Cisco IOS MGCP ゲートウェイのポートをまだ設定していない場合は、『*Cisco CallManager アドミニストレーション ガイド*』の説明に従って設定してください。
5. エンドポイント ID の Gateway Configuration ウィンドウにパケット キャプチャ設定が表示されます。このウィンドウにアクセスするには、音声インターフェイス カードのエンドポイント ID をクリックします。
6. トラブルシューティングを設定する場合は、P.9-56 の「IP Phone のパケット キャプチャおよび MGCP ゲートウェイ設定の設定値」を参照してください。
7. パケット キャプチャを設定したら、**Update** および **Reset Gateway** をクリックします。
8. 関係するデバイス間でスニファ トレースを使用して、SRTP パケットをキャプチャします。
9. パケットをキャプチャしたら、Signal Packet Capture Mode を **None** に設定し、Packet Capture Enable サービス パラメータを **False** に設定します。
10. 詳細については、P.9-57 の「キャプチャされたパケットの解析」を参照してください。

IP Phone のパケット キャプチャおよび MGCP ゲートウェイ設定の設定値

Signal Packet Capture Mode 設定と Packet Capture Duration 設定について説明している次の情報を、次の各項とともに参照してください。

- Phone Configuration ウィンドウでのパケット キャプチャの設定（P.9-53）
- エンドポイント ID の MGCP Gateway Configuration ウィンドウでのパケット キャプチャの設定（P.9-54）

Signal Packet Capture Mode

Signal Packet Capture Mode ドロップダウン ボックスから、次のオプションのいずれかを選択します。

- **None**：このオプションはデフォルト設定であり、パケット キャプチャが実行されないことを示します。パケット キャプチャの実行後、この設定値を設定します。
- **Real-Time Mode**：Cisco CallManager が、復号化されたメッセージまたは暗号化されていないメッセージを、セキュアなチャネルを通じて解析デバイスに送信します。Cisco CallManager と TAC デバッグ ツールの間に、TLS 接続が確立されます。Cisco CallManager とデバッグ ツールの間で認証が行われた後、Cisco CallManager は SCCP メッセージ（電話機）または UDP および TCP バックホール メッセージ（ゲートウェイ）を、接続されているすべてのリアルタイム デバッグ ツールに送信します。このアクションの対象は、パケット キャプチャを設定した選択済みのデバイスだけです。

  このモードの場合、ネットワーク上でスニファは使用できません。

  TAC デバッグ ツール（IREC）は、SRTP パケットをキャプチャし、復号化された SCCP か、UDP または TCP バックホール メッセージから抽出されたキー関連情報を使用して、パケットを復号化します。

  デバッグ サイトにあるデバッグ ツールを実行する必要があります。
- **Batch Processing Mode**：Cisco CallManager が、復号化されたメッセージまたは暗号化されていないメッセージをファイルに書き込み、システムが各ファイルを暗号化します。システムは、毎日、新しい暗号化キーを使用して新しいファイルを作成します。また、Cisco CallManager は 7 日ごとにファイルを格納する際に、ファイルを暗号化するキーをセキュアな場所に格納します。Cisco CallManager はファイルを C:\Program Files\Cisco\PktCap に格納します。単一のファイルに含まれるのは、タイム スタンプ、送信元 IP アドレス、送信元 IP ポート、宛先 IP アドレス、パケット プロトコル、メッセージ長、およびメッセージです。TAC デバッグ ツールは、HTTPS、管理者のユーザ名

とパスワード、および指定された日付を使用して、キャプチャされたパケットを含む単一の暗号化ファイルを要求します。同様に、ツールは暗号化されたファイルを復号化するキー情報を要求します。

TAC に連絡する前に、関係するデバイス間でスニファ トレースを使用して、SRTP パケットをキャプチャする必要があります。

Packet Capture Duration

このフィールドは、1 つのパケット キャプチャ セッションに割り当てる時間の最大値（分単位）を指定します。デフォルト設定値は 60 ですが、範囲は 0 ～ 300 分です。

関連項目

- パケット キャプチャの設定チェックリスト（P.9-49）
- キャプチャされたパケットの解析（P.9-57）
- Phone Configuration ウィンドウでのパケット キャプチャの設定（P.9-53）
- Cisco CallManager Administration でのパケット キャプチャに関するメッセージ（P.9-58）

キャプチャされたパケットの解析

Cisco Technical Assistance Center（TAC）は、デバッグ ツールを使用してパケットを解析します。TAC に連絡する前に、関係するデバイス間でスニファ トレースを使用して、SRTP パケットをキャプチャします。次の情報を収集したら、TAC に直接連絡してください。

- パケット キャプチャ ファイル：
  https://<server name or IP address>/pktcap/pktcap.asp?file=mm-dd-yyyy.pkt。ここで、サーバを参照し、月、日、年（mm-dd-yyyy）に基づいてパケット キャプチャ ファイルを見つけます。
- ファイルのキー：
  https://<server name or IP address>pktcap/pktcap.asp?key=mm-dd-yyyy.pkt。ここで、サーバを参照し、月、日、年（mm-dd-yyyy）に基づいてキーを見つけます。
- Cisco CallManager サーバの管理ユーザ名とパスワード。

関連項目

- パケット キャプチャの設定チェックリスト（P.9-49）
- IP Phone のパケット キャプチャおよび MGCP ゲートウェイ設定の設定値（P.9-56）
- Cisco CallManager Administration でのパケット キャプチャに関するメッセージ（P.9-58）

Cisco CallManager Administration でのパケット キャプチャに関するメッセージ

表 9-8 は、Cisco CallManager Administration でパケット キャプチャを設定するときに表示される可能性のあるメッセージのリストを示しています。

表 9-8　パケット キャプチャに関するメッセージ

メッセージ	修正処置
Packet Capture Duration contains one or more invalid characters.Valid characters for Packet Capture Duration are numbers.	このメッセージは、修正処置を示しています。
Invalid Packet Capture Duration.Packet Capture Duration should be between 0 and 300.	メッセージで指摘されたように、適切な情報を入力します。

関連項目

- IP Phone のパケット キャプチャおよび MGCP ゲートウェイ設定の設定値（P.9-56）
- パケット キャプチャの設定チェックリスト（P.9-49）

暗号化および割り込みの設定に関するメッセージ

P.1-6 の「対話および制限」に加えて、次の情報も参照してください。

暗号化が設定されている Cisco IP Phone 7960 モデルおよび 7940 モデルに対して割り込みを設定しようとすると、次のメッセージが表示されます。

If you configure encryption for Cisco IP Phone models 7960 and 7940, those encrypted devices cannot accept a barge request when they are participating in an encrypted call.When the call is encrypted, the barge attempt fails.

メッセージが表示されるのは、Cisco CallManager Administration で次の作業を実行したときです。

- Phone Configuration ウィンドウで、Device Security Mode に **Encrypted** を選択し（システム デフォルトは Encrypted）、Built In Bridge 設定に **On** を選択し（デフォルト設定は On）、さらにこの特定の設定の作成後に **Insert** または **Update** をクリックする。
- Enterprise Parameter ウィンドウで、Device Security Mode パラメータを更新する。
- Service Parameter ウィンドウで、Built In Bridge Enable パラメータを更新する。

ヒント　変更内容を有効にするには、従属する Cisco IP デバイスをリセットする必要があります。

関連項目

- 対話および制限（P.1-6）
- 暗号化の概要（P.1-27）
- その他の情報（P.1-35）

セキュア SRST リファレンスのトラブルシューティング

この項では、次のトピックについて取り上げます。

- SRST リファレンスの設定時に表示されるセキュリティ メッセージ（P.9-60）
- SRST 証明書がゲートウェイから削除された場合のトラブルシューティング（P.9-61）

SRST リファレンスからのセキュリティの削除

セキュリティの設定後に SRST リファレンスをノンセキュアにするには、Cisco CallManager Administration の SRST Configuration ウィンドウで、**Is the SRTS Secure?** チェックボックスをオフにします。ゲートウェイ上のクレデンシャル サービスを無効にする必要がある旨のメッセージが表示されます。

関連項目

- Survivable Remote Site Telephony（SRST）リファレンスのセキュリティ設定（P.7-1）
- *Cisco CallManager アドミニストレーション ガイド*
- SRST 対応のゲートウェイおよびこのバージョンの Cisco CallManager に対応したシステム管理マニュアル

SRST リファレンスの設定時に表示されるセキュリティ メッセージ

Cisco CallManager Administration でセキュア SRST リファレンスを設定するときに、次のメッセージが表示される場合があります。

「Port Numbers can only contain digits.」というメッセージです。このメッセージが表示されるのは、SRST Certificate Provider Port の設定時に無効なポート番号を入力した場合です。ポート番号は、1024 ～ 49151 の範囲に存在する必要があります。

関連項目

- Survivable Remote Site Telephony（SRST）リファレンスのセキュリティ設定（P.7-1）
- *Cisco CallManager アドミニストレーション ガイド*
- SRST 対応のゲートウェイおよびこのバージョンの Cisco CallManager に対応したシステム管理マニュアル

SRST 証明書がゲートウェイから削除された場合のトラブルシューティング

SRST 証明書が SRST 対応のゲートウェイから削除されている場合は、その SRST 証明書を Cisco CallManager データベースと IP Phone から削除する必要があります。

この作業を実行するには、SRST Configuration ウィンドウで、**Is the SRST Secure?** チェックボックスをオフにして **Update** をクリックし、**Reset Devices** をクリックします。

関連項目

- Survivable Remote Site Telephony（SRST）リファレンスのセキュリティ設定（P.7-1）
- *Cisco CallManager アドミニストレーション ガイド*
- SRST 対応のゲートウェイおよびこのバージョンの Cisco CallManager に対応したシステム管理マニュアル