CHAPTER 16

トラブルシューティング

この章では、セキュリティ関連の測定、およびセキュリティ関連の問題をトラブルシューティングするときの一般的なガイドラインについて説明します。この章は、次の内容で構成されています。

Cisco CallManager のアラーム、パフォーマンス モニタ、ログ、およびトレースまたはエラー メッセージと修正処置の詳細については、次のマニュアル（またはオンライン ヘルプ）を参照してください。

- Real-Time Monitoring Tool（RTMT）の GUI およびパフォーマンス モニタのアラームの詳細については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』および『*Cisco CallManager Serviceability システム ガイド*』を参照してください。
- エラー メッセージの詳細については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』を参照してください。
- RTMT でのログおよびトレースの表示の詳細については、『*Cisco CallManager Serviceability システム ガイド*』を参照してください。
- パケット キャプチャの使用または設定、およびキャプチャしたパケットの分析の詳細については、『*Cisco CallManager トラブルシューティング ガイド Release 5.0(1)*』を参照してください。
- トラブルシューティングの手順および修正処置の詳細については、『*Cisco CallManager トラブルシューティング ガイド Release5.0(1)*』を参照してください。

（注）　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。

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は、表 3-3、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。

CLI の使用方法

Cisco IPT Platform Administration GUI の使用中に問題が発生した場合、管理者はコマンドライン インターフェイス（CLI）を使用して、トラブルシューティングの目的でシステム機能にアクセスできます。

CLI インターフェイスを使用するには、SSH アクセスができる環境とログイン ID およびパスワードが必要です。CLI を使用してログ、トレース、およびパフォーマンス モニタを表示する方法については、『*Cisco IP Telephony Platform Administration Guide*』を参照してください。

アラームの使用方法

Cisco CallManager Serviceability は、X.509 名不一致、認証エラー、暗号化エラーに対して、セキュリティ関連アラームを生成します。Serviceability GUI を使用して、アラームを定義できます。

アラームは、TFTP サーバおよび CTL ファイルのエラーが発生したときに、IP Phone で生成されます。IP Phone で生成されるアラームについては、IP Phone のモデルとタイプ（SCCP または SIP）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.3-18 の「Cisco IP Phone 上の CTL ファイルの削除」を参照してください。

パフォーマンス モニタ カウンタの使用方法

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します。表 16-1 に、セキュリティ機能に適用されるパフォーマンス カウンタを示します。

表 16-1　セキュリティ パフォーマンス カウンタ

オブジェクト	カウンタ
Cisco CallManager	AuthenticatedCallsActive
	AuthenticatedCallsCompleted
	AuthenticatedPartiallyRegisteredPhone
	AuthenticatedRegisteredPhones
	EncryptedCallsActive
	EncryptedCallsCompleted
	EncryptedPartiallyRegisteredPhone
	EncryptedRegisteredPhones
	CCMSIPLineServerAuthChallenges
	CCMSIPLineServerAuthFailures
	CCMSIPTrunkServerAuthChallenges
	CCMSIPTrunkServerAuthFailures
	CCMSIPTrunkClientAuthResponses
	CCMSIPTrunkClientAuthRejects
	CCMSIPPresenceAuthorizations
	CCMSIPPresenceAuthorizationsFailure
	CCMSIPTrunkMethodAuthorization
	CCMSIPTrunkMethodAuthorizationFailure
	TLSConnectedSIPTrunk
SIP スタック	StatusCodes4xxIns（405 Method Not Allowed など）
	StatusCodes4xxOuts（405 Method Not Allowed など）
TFTP サーバ	BuildSigCount
	EncryptCount

RTMT でパフォーマンス カウンタにアクセスする方法、perfmon ログの設定、およびカウンタの詳細については、『*CallManager Serviceability システム ガイド*』、を参照してください。

CLI コマンドの **show perf** は、パフォーマンス モニタ情報を表示します。CLI インターフェイスの使用方法については、『*Cisco IP Telephony Platform Administration Guide*』を参照してください。

ログおよびトレース ファイルの確認

Cisco 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、RTMT でノードのログ ファイルおよびトレース ファイルを確認してください。

管理者は、Serviceability Real-Time Monitoring Tool（RTMT）の Trace Collection Tool を使用して、ログ ファイルおよびトレース ファイルをサーバからダウンロードできます。ファイルを収集した後、RTMT の適切なビューアで表示できます。

（注） 暗号化をサポートするデバイスの場合、SRTP 鍵関連情報はトレース ファイルに表示されません。

トレース収集ツールの使用方法およびフィルタリングを使用してログ ファイル レコードを確認する方法については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』および『*Cisco CallManager Serviceability システム ガイド*』を参照してください。

Cisco CallManager は、ログ ファイルおよびトレース ファイルを複数のディレクトリに格納します（cm/log、cm/trace、tomcat/logs、tomcat/logs/security など）。CLI コマンドの **activelog** および **inactivelog** を使用して、ログ ファイルおよびトレース ファイルの検索、表示、および操作ができます。

CLI インターフェイスの使用方法の詳細については、『*Cisco IP Telephony Platform Administration Guide*』を参照してください。

ヒント ログ ファイルまたはトレース ファイルのディレクトリおよびファイル名がわからない場合は、TAC に問い合せてください。

セキュリティ ファイルのバックアップと復元

CAPF データなど、セキュリティ ファイルのバックアップおよび復元の手順については、『*Cisco IP Telephone Disaster Recovery Framework Administration Guide*』を参照してください。

証明書のトラブルシューティング

Cisco IPT Platform Administration の証明書管理ツールを使用すると、証明書の表示、削除と再生成、証明書の有効期限の監視、証明書および CTL ファイルのダウンロードとアップロード（更新した CTL ファイルを Unity にアップロードするなど）ができます。CLI を使用すると、自己署名証明書および信頼された証明書の一覧および表示、自己署名証明書の再生成ができます。

CLI コマンドの **show cert**、**show web-security**、**set cert regen**、および **set web-security** を使用して、CLI インターフェイスで証明書を管理できます（たとえば、**set cert regen tomcat** と使用します）。GUI または CLI を使用して証明書を管理する方法については、『*Cisco IP Telephony Platform Administration Guide*』を参照してください。

CTL セキュリティ トークン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。

すべてのセキュリティ トークン（etoken）を紛失した場合は、Cisco TAC に問い合せてください。

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.3-9 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。

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.3-12 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.1-10 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）。

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。

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。

電話機に適用されるセキュリティ プロファイルの認証モードが By Authentication String に設定されていることを確認します。

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。

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。

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 に固有な鍵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、Cisco IPT Platform GUI または CLI で、CAPF 証明書を表示します。

- 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

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電話機にインストールされていることを確認するには、Model Information または Security Configuration 電話機メニューを使用して、LSC 設定を表示します。詳細については、IP Phone のモデルとタイプ（SCCP または SIP）に対応した『*Cisco IP Phone アドミニストレーション ガイド*』を参照してください。

製造元でインストールされる証明書（MIC）が IP Phone 内に存在することの確認

MIC が電話機に存在することを確認するには、Model Information または Security Configuration 電話機メニューを使用して、MIC 設定を表示します。詳細については、IP Phone のモデルとタイプ（SCCP または SIP）に対応した『*Cisco IP Phone アドミニストレーション ガイド*』を参照してください。

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 キャプチャの使用方法

SRTP 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（Cisco IP Phone、Cisco SIP IP Phone、Cisco IOS MGCP ゲートウェイ、H.323 ゲートウェイ、または H.323/H.245/H.225 トランク）との間で交換されるメッセージのパケットを分析する。

（注）　SIP トランクは SRTP をサポートしません。

- 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鍵関連情報を抽出し、デバイス間のメディアを復号化する。

パケット キャプチャの使用または設定、およびキャプチャした SRTP 暗号化コール（および、その他のすべてのコール タイプ）のパケットの分析の詳細については、『*Cisco CallManager トラブルシューティング ガイド Release 5.0(1)*』を参照してください。

ヒント　この作業を同時に複数のデバイスで実行すると、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。

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、電話機でパケット キャプチャ モードを設定できます。この作業を実行する方法については、『*Cisco CallManager Bulk Administration Guide*』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。

その他の情報

関連項目

- 対話および制限（P.1-6）
- 証明書の種類（P.1-13）
- メディア暗号化の設定と割り込み（P.1-11）
- CLI の使用方法（P.16-2）
- アラームの使用方法（P.16-2）
- パフォーマンス モニタ カウンタの使用方法（P.16-3）
- ログおよびトレース ファイルの確認（P.16-4）
- セキュリティ ファイルのバックアップと復元（P.16-4）
- 証明書のトラブルシューティング（P.16-4）
- CTL セキュリティ トークンのトラブルシューティング（P.16-5）
- CAPF のトラブルシューティング（P.16-6）
- 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.16-8）

シスコの関連マニュアル

- *Cisco IP Telephone Disaster Recovery Framework Administration Guide*
- *Cisco CallManager Bulk Administration Guide*
- *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 CallManager トラブルシューティング ガイド Release5.0(1)*
- *Cisco IP Telephony Platform Administration Guide*
- 電話機のモデルおよびプロトコルに対応した Cisco IP Phone アドミニストレーション ガイド