CHAPTER 3

Cisco Unified Communications Manager システムの問題

この章では、Cisco Unified Communications Manager システムに関連する、次のような一般的な問題の解決方法について説明します。

応答しない Cisco Unified Communications Manager システム

この項では、応答しない Cisco Unified Communications Manager システムに関する次の問題について説明します。

Cisco Unified Communications Manager システムが応答を停止する

症状

Cisco Unified Communications Manager システムが応答しません。

Cisco CallManager サービスがクラッシュすると、システム イベント ログに次のメッセージが表示されます。

```
The Cisco CallManager service terminated unexpectedly.
It has done this 1 time. The following corrective action
will be taken in 60000 ms. Restart the service.
```

クラッシュの場合、次のようなメッセージが表示されることもあります。

```
Timeout 3000 milliseconds waiting for
Cisco CallManager service to connect.
```

Cisco Communications Manager は、次のエラーのために起動できませんでした。

```
The service did not respond to the start or control request in a timely fashion.
```

この時点で、Cisco Unified IP Phone やゲートウェイなどのデバイスが Cisco Unified Communications Manager から登録解除されると、ユーザに発信音の遅延が発生したり、CPU の使用率が高いために Cisco Unified Communications Manager サーバがフリーズしたりします。ここに記載されていないイベント ログ メッセージについては、Cisco Unified Communications Manager のイベント ログを参照してください。

考えられる原因

Cisco CallManager サービスがクラッシュする可能性があるのは、サービスが機能するための十分なリソース（CPU やメモリ）がない場合です。通常、サーバの CPU 使用率はその時点で 100 % です。

推奨処置

発生するクラッシュのタイプに応じて、クラッシュの根本原因を特定するために役立つデータを収集する必要があります。

リソース不足によるクラッシュが発生している場合は、次の手順を実行します。

手順

ステップ 1　クラッシュの前後 15 分の Cisco CallManager トレースを収集します。

ステップ 2　クラッシュの前後 15 分の SDL トレースを収集します。

ステップ 3　使用可能になっている場合は、perfmon トレースを収集します。

ステップ 4　このトレースが使用可能になっていない場合は、perfmon トレースの収集を開始して、サーバ上で動作しているプロセスごとにメモリと CPU の使用状況を追跡します。このトレースは、次にリソース不足によるクラッシュが発生した場合に役立ちます。

Cisco Unified Communications Manager の管理ページが表示されない

症状

Cisco Unified Communications Manager の管理ページが表示されません。

考えられる原因

Cisco CallManager サービスが停止しています。

推奨処置

P.2-18 の「Cisco Unified Communications Manager サービスが動作していることの確認」または『*Cisco Unified Serviceability アドミニストレーション ガイド*』の説明に従って、サーバ上で Cisco CallManager サービスがアクティブであること、および動作していることを確認します。

Cisco Unified Communications Manager の管理ページにアクセスしようとするとエラーが発生する

症状

Cisco Unified Communications Manager の管理ページにアクセスしようとすると、次のいずれかのメッセージが表示されます。

- Internet Explorer：The page cannot be displayed.
- Netscape（警告ボックスが表示されます）：There was no response.The server could be down or is not responding.

考えられる原因

サービスは、期待どおりには自動開始されませんでした。Cisco Unified Communications Manager の管理ページが表示されない原因で最も多いのは、サービスのいずれかが停止していることです。

推奨処置

他のサービスを開始してみます。

後続ノードで Cisco Unified Communications Manager の管理ページにアクセスしようとするとエラーが発生する

症状

Cisco Unified Communications Manager の管理ページにアクセスしようとすると、次のいずれかのエラー メッセージが表示されます。

考えられる原因

最初の Cisco Unified Communications Manager ノードの IP アドレスが変更されたときに、後続ノードがオフラインになっていた場合、後続ノードで Cisco Unified Communications Manager の管理ページにログインできないことがあります。

推奨処置

このエラーが発生した場合は、後続の Cisco Unified Communications Manager ノードで IP アドレスを変更する手順を実行します。この手順は、『*Cisco Unified Communications Operating System アドミニストレーション ガイド*』に記載されています。

表示する権限がない

症状

Cisco Unified Communications Manager の管理ページにアクセスすると、次のいずれかのメッセージが表示されます。

- You Are Not Authorized to View This Page
- You do not have permission to view this directory or page using the credentials you supplied.
- Server Application Error.The server has encountered an error while loading an application during the processing of your request.Please refer to the event log for more detailed information.Please contact the server administrator for assistance.
- Error: Access is Denied.

考えられる原因

不明

推奨処置

TAC に問い合せてください。

Cisco Unified Communications Manager でのユーザの表示または追加に関する問題

症状

Cisco Unified Communications Manager の管理ページで、ユーザを追加することも、検索することもできません。

考えられる原因

ホスト名に特殊文字（アンダースコアなど）が含まれるサーバにインストールされた Cisco Unified Communications Manager で作業している場合、または SP2 および Q313675 パッチ以降が適用された Microsoft Internet Explorer 5.5 で作業している場合、次の問題が発生することがあります。

- 基本的な検索を行うときに［検索］をクリックすると、同じページが再表示される。
- 新しいユーザを追加しようとすると、次のメッセージが表示される。

```
The following error occurred while trying to execute the command.
Sorry, your session object has timed out.
Click here to Begin a New Search
```

推奨処置

Cisco Unified Communications Manager のホスト名にアンダースコアやピリオドなどの特殊文字が含まれている場合（たとえば、Call_Manager）は、Cisco Unified Communications Manager の管理ページでユーザを追加することも、検索することもできません。Domain Name System（DNS; ドメイン ネーム システム）でサポートされている文字は、すべての英字（A ～ Z、a ～ z）、数字（0 ～ 9）、およびハイフン（-）であり、特殊文字は使用できません。ブラウザに Q313675 パッチがインストールされている場合は、URL に DNS でサポートされていない文字が含まれていないことを確認してください。

Q313675 パッチの詳細については、「MS01-058: File Vulnerability Patch for Internet Explorer 5.5 and Internet Explorer 6.」を参照してください。

この問題を解決するには、次の方法があります。

- サーバの IP アドレスを使用して Cisco Unified Communications Manager の管理ページにアクセスする。
- サーバ名に DNS でサポートされていない文字を使用しない。
- URL に localhost または IP アドレスを使用する。

名前からアドレスへの解決の失敗

症状

次の URL にアクセスしようとすると、次のいずれかのメッセージが表示されます。

http://your-cm-server-name/ccmadmin

- Internet Explorer：This page cannot be displayed
- Netscape：Not Found.The requested URL / ccmadmin was not found on this server.

名前ではなく Cisco Communications Manager の IP アドレス（http://10.48.23.2/ccmadmin）を使用して同じ URL にアクセスすると、ウィンドウが表示されます。

考えられる原因

「your-cm-server-name」に入力した名前が、DNS または hosts ファイルで間違った IP アドレスにマッピングされています。

推奨処置

DNS を使用するように設定した場合は、DNS を調べて、*your-cm-server-name* のエントリに Cisco Unified Communications Manager サーバの正しい IP アドレスが関連付けられているかどうかを確認します。IP アドレスが正しくない場合は、変更します。

DNS を使用していない場合は、ローカル マシンで「hosts」ファイルを調べて、*your-cm-server-name* およびそれに関連付けられている IP アドレスのエントリがあるかどうかを確認します。このファイルを開き、Cisco Unified Communications Manager のサーバ名と IP アドレスを追加します。hosts ファイルは、**C:\WINNT\system32\drivers\etc\hosts** にあります。

ブラウザと Cisco Unified Communications Manager サーバ間でポート 80 がブロックされる

症状

ファイアウォールが Web サーバまたは http トラフィックによって使用されるポートをブロックすると、次のいずれかのメッセージが表示されます。

- Internet Explorer：This page cannot be displayed
- Netscape：There was no response.The server could be down or is not responding

考えられる原因

セキュリティ上の理由から、システムが、ローカル ネットワークからサーバ ネットワークへの http アクセスをブロックしました。

推奨処置

1. Cisco Unified Communications Manager サーバへの他のタイプのトラフィック（ping や Telnet など）が許可されるかどうかを確認します。許可されるトラフィックがある場合は、リモート ネットワークから Cisco Unified Communications Manager Web サーバへの http アクセスがブロックされていると考えられます。
2. ネットワーク管理者に連絡して、セキュリティ ポリシーを確認します。
3. サーバが配置されているそのネットワークから、再試行します。

リモート マシンに不適切なネットワーク設定が存在する

症状

接続性がありません。または、Cisco Unified Communications Manager と同じネットワーク内の他のデバイスへの接続性がありません。

他のリモート マシンから同じアクションを試行すると、Cisco Unified Communications Manager の管理ページが表示されます。

考えられる原因

ステーションまたはデフォルト ゲートウェイのネットワーク設定が正しくないと、そのネットワークへの接続性が一部または完全になくなるため、Web ページが表示されないことがあります。

推奨処置

1. Cisco Unified Communications Manager サーバおよび他のデバイスの IP アドレスに ping を試行し、接続できないことを確認します。
2. ローカル ネットワークから他のどのデバイスへの接続も失敗する場合は、自分のステーションでネットワーク設定を確認します。また、ケーブルとコネクタの整合性を確認します。詳細については、該当するハードウェアのマニュアルを参照してください。

   LAN で TCP-IP を使用して接続している場合は、引き続き次のステップを実行して、リモート ステーションのネットワーク設定を確認します。

3. ［スタート］>［設定］>［ネットワークとダイヤルアップ接続］を選択します。
4. ［ローカル エリア接続］を選択し、［プロパティ］を選択します。

   チェックボックスがオンになった状態で、通信プロトコルのリストが表示されます。
5. ［インターネット プロトコル （TCP/IP）］を選択し、［プロパティ］を再度クリックします。
6. ネットワークに応じて、［IP アドレスを自動的に取得する］または［次の IP アドレスを使う］のどちらかを選択します。

   ブラウザ固有の設定が正しくない可能性もあります。
7. Internet Explorer ブラウザで、［ツール］>［インターネット オプション］を選択します。
8. ［接続］タブを選択し、LAN 設定またはダイヤルアップ設定を確認します。

   デフォルトでは、LAN 設定およびダイヤルアップ設定は行われていません。Windows からの一般的なネットワーク設定が使用されます。
9. Cisco Unified Communications Manager ネットワークへの接続だけが失敗する場合は、ネットワークにルーティングの問題が存在する可能性があります。ネットワーク管理者に連絡して、デフォルト ゲートウェイに設定されているルーティングを確認します。

（注）　この手順を実行してもリモート サーバからブラウズできない場合は、TAC に連絡し、問題の詳しい調査を依頼してください。

パブリッシャとサブスクライバの間で複製が失敗する

データベースの複製は、Cisco Communications Manager クラスタの中核機能です。データベースのマスター コピーを持つサーバはパブリッシャと呼ばれ、そのデータベースを複製するサーバはサブスクライバと呼ばれます。

症状

パブリッシャ上で行われた変更が、サブスクライバに登録されている電話機に反映されません。

考えられる原因

パブリッシャとサブスクライバの間で複製が失敗しています。

推奨処置

次の手順を実行して、2 つのシステム間の関係を再確立します。

1. 複製を確認します。
   a. Cisco Unified Communications Manager Real-Time Monitoring Tool（RTMT）を開きます。
   b. ［System］>［Performance］>［Open Peformance Monitoring］を選択します。
   c. パブリッシャ ノードをダブルクリックしてパフォーマンス モニタを展開します。
   d. ［Replication Counters］をダブルクリックします。
   e. ［Number of Replicates Created］をダブルクリックします。
   f. ［Object Instances］ダイアログボックスで［ReplicateCount］を選択し、［Add］をクリックします。
   g. ［Replication Status］をダブルクリックします。
   h. ［Object Instances］ダイアログボックスで［ReplicateCount］を選択し、［Add］をクリックします。

（注）　カウンタの定義を表示するには、カウンタ名を右クリックして［Counter Description］を選択します。

2. CLI を使用して、複製の状態を確認します。
   a. プラットフォームの CLI にアクセスし、次のコマンドを使用して複製を確認します。

      ```
      utils dbreplication status file view activelog <filename_output_above>
      ```

   b. 各ノードの要約情報およびカウントを参照して、複製を確認します。
3. 複製を修復するには、次の手順を実行します。
   a. プラットフォームの CLI にアクセスします。
   b. 次のコマンドを使用して、複製を修復します。

      ```
      utils dbreplication repair usage:utils dbreplicatoin repair [nodename]|all
      ```

サーバの応答が遅い

この項では、デュプレックス ポート設定の不一致が原因で、サーバからの応答が遅いことに関連する問題について説明します。

症状

サーバからの応答が遅くなっています。

考えられる原因

スイッチのデュプレックス設定が Cisco Unified Communications Manager サーバ上のデュプレックス ポート設定と一致しない場合、応答が遅くなることがあります。

推奨処置

1. 最適なパフォーマンスを得るには、スイッチとサーバの両方を **100/Full** に設定します。

   スイッチでもサーバでも Auto 設定を使用することはお勧めしません。
2. Cisco Unified Communications Manager サーバを再起動して、この変更を有効にする必要があります。

JTAPI サブシステムの起動に関する問題

Java Telephony API（JTAPI）サブシステムは、Cisco Customer Response Solutions（CRS）プラットフォームの非常に重要なコンポーネントです。JTAPI は Cisco Unified Communications Manager と通信し、テレフォニー　コール制御を担当します。CRS　プラットフォームは、Cisco　Unified Auto-Attendant、Cisco IP ICD、Cisco Unified IP-IVR などのテレフォニー アプリケーションをホストします。この項は、これらのうち特定のアプリケーションを対象としているわけではありませんが、JTAPI サブシステムは、これらすべてのアプリケーションによって使用される基本コンポーネントであることに留意してください。

トラブルシューティング プロセスを開始する前に、使用しているソフトウェア バージョンの互換性を確認してください。互換性を確認するには、使用している Cisco Unified Communications Manager のバージョンの『Cisco Unified Communications Manager Release Notes』をお読みください。

CRS のバージョンを確認するには、http://servername/appadmin（*servername* は、CRS がインストールされているサーバの名前）と入力して AppAdmin ページにログインします。メイン メニューの右下隅に、現在のバージョンが表示されます。

JTAPI サブシステムが OUT_OF_SERVICE である

症状

JTAPI サブシステムが起動しません。

考えられる原因

トレース ファイルに次のいずれかの例外が表示されます。

- MIVR-SS_TEL-4-ModuleRunTimeFailure
- MIVR-SS_TEL-1-ModuleRunTimeFailure

MIVR-SS_TEL-4-ModuleRunTimeFailure

トレース ファイルで **MIVR-SS_TEL-1-ModuleRunTimeFailure** という文字列を検索します。その行の末尾に、例外の原因が表示されています。

一般的なエラーは、次のとおりです。

- Unable to create provider － bad login or password
- Unable to create provider － Connection refused
- Unable to create provider － login=
- Unable to create provider － hostname
- Unable to create provider － Operation timed out
- Unable to create provider － null

Unable to create provider － bad login or password

考えられる原因

管理者が誤ったユーザ名またはパスワードを JTAPI 設定に入力しました。

エラー メッセージの全テキスト

```
%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-time
failure in JTAPI subsystem: Module=JTAPI
Subsystem,Failure Cause=7,Failure
Module=JTAPI_PROVIDER_INIT,
Exception=com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- bad login or password.
%MIVR-SS_TEL-7-
EXCEPTION:com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- bad login or password.
```

推奨処置

ユーザ名とパスワードが正しいことを確認します。［Cisco Unified CM ユーザオプション］ページ（http://servername/ccmuser）にログインし、Cisco Unified Communications Manager が正しく認証できることを確認します。

Unable to create provider － Connection refused

考えられる原因

Cisco Unified Communications Manager への JTAPI 接続が、Cisco Unified Communications Manager によって拒否されました。

エラー メッセージの全テキスト

```
%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-time
failure in JTAPI subsystem: Module=JTAPI Subsystem,
Failure Cause=7,Failure Module=JTAPI_PROVIDER_INIT,
Exception=com.cisco.jtapi.PlatformExceptionImpl: Unable
to create provider -- Connection refused
%MIVR-SS_TEL-7-EXCEPTION:com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- Connection refused
```

推奨処置

Cisco Unified Serviceability のコントロールセンタで、CTI Manager サービスが実行されていることを確認します。

Unable to create provider ー login=

考えられる原因

［JTAPI configuration］ウィンドウで、設定が行われていません。

エラー メッセージの全テキスト

```
%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-time
failure in JTAPI subsystem: Module=JTAPI Subsystem,
Failure Cause=7,Failure Module=JTAPI_PROVIDER_INIT,
Exception=com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- login=
%MIVR-SS_TEL-7-EXCEPTION:com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- login=
```

推奨処置

CRS サーバの［JTAPI configuration］ウィンドウで、JTAPI プロバイダーを設定します。

Unable to create provider ー hostname

考えられる原因

CRS エンジンが Cisco Unified Communications Manager のホスト名を解決できません。

エラー メッセージの全テキスト

```
%M%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-time
failure in JTAPI subsystem: Module=JTAPI Subsystem,
Failure Cause=7,Failure Module=JTAPI_PROVIDER_INIT,
Exception=com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- dgrant-mcs7835.cisco.com
%MIVR-SS_TEL-7-EXCEPTION:com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- dgrant-mcs7835.cisco.com
```

推奨処置

CRS エンジンから、DNS 解決が正しく機能していることを確認します。DNS 名ではなく、IP アドレスを使用してみます。

Unable to create provider ー Operation timed out

考えられる原因

CRS エンジンに、Cisco Unified Communications Manager との IP 接続性がありません。

エラー メッセージの全テキスト

```
101: Mar 24 11:37:42.153 PST
%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-time
failure in JTAPI subsystem: Module=JTAPI Subsystem,
Failure Cause=7,Failure Module=JTAPI_PROVIDER_INIT,
Exception=com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- Operation timed out
102: Mar 24 11:37:42.168 PST %MIVR-SS_TEL-7-EXCEPTION:
com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- Operation timed out
```

推奨処置

CRS サーバで、JTAPI プロバイダーに設定されている IP アドレスを確認します。CRS サーバと Cisco Unified Communications Manager で、デフォルト ゲートウェイの設定を確認します。IP ルーティングの問題が存在しないことを確認します。CRS サーバから Cisco Unified Communications Manager に ping を実行して、接続性をテストします。

Unable to create provider — null

考えられる原因

JTAPI プロバイダーの IP アドレスまたはホスト名が設定されていません。または、JTAPI クライアントが正しいバージョンを使用していません。

エラー メッセージの全テキスト

```
%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-time
failure in JTAPI subsystem: Module=JTAPI Subsystem,
Failure Cause=7,Failure Module=JTAPI_PROVIDER_INIT,
Exception=com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- null
```

推奨処置

JTAPI 設定で、ホスト名または IP アドレスが設定されていることを確認します。JTAPI のバージョンが正しくない場合は、Cisco Unified Communications Manager の［プラグインの検索と一覧表示（Find and List Plugins）］ウィンドウから JTAPI クライアントをダウンロードし、CRS サーバにインストールします。

MIVR-SS_TEL-1-ModuleRunTimeFailure

症状

この例外は、通常、JTAPI サブシステムがポートを初期化できない場合に発生します。

考えられる原因

CRS サーバは Cisco Unified Communications Manager と通信できますが、JTAPI を介して CTI ポートまたは CTI ルート ポイントを初期化できません。このエラーは、CTI ポートおよび CTI ルート ポイントが JTAPI ユーザに関連付けられていない場合に発生します。

エラー メッセージの全テキスト

```
255: Mar 23 10:05:35.271 PST %MIVR-SS_TEL-1-ModuleRunTimeFailure:
Real-time failure in JTAPI subsystem: Module=JTAPI Subsystem,
Failure Cause=7,Failure Module=JTAPI_SS,Exception=null
```

推奨処置

Cisco Unified Communications Manager で JTAPI ユーザをチェックし、CRS サーバに設定されている CTI ポートおよび CTI ルート ポイントがユーザに関連付けられていることを確認します。

JTAPI サブシステムが PARTIAL_SERVICE である

症状

トレース ファイルに次の例外が表示されます。

MIVR-SS_TEL-3-UNABLE_REGISTER_CTIPORT

考えられる原因

JTAPI サブシステムが、1 つまたは複数の CTI ポートまたはルート ポイントを初期化できません。

エラー メッセージの全テキスト

```
1683: Mar 24 11:27:51.716 PST
%MIVR-SS_TEL-3-UNABLE_REGISTER_CTIPORT:
Unable to register CTI Port: CTI Port=4503,
Exception=com.cisco.jtapi.InvalidArgumentExceptionImpl:
Address 4503 is not in provider's domain.
1684: Mar 24 11:27:51.716 PST %MIVR-SS_TEL-7-EXCEPTION:
com.cisco.jtapi.InvalidArgumentExceptionImpl:
Address 4503 is not in provider's domain.
```

推奨処置

トレース内のメッセージには、どの CTI ポートまたはルート ポイントを初期化できないかが記載されています。このデバイスが Cisco Unified Communications Manager 設定に存在すること、および Cisco Unified Communications Manager でこのデバイスが JTAPI ユーザに関連付けられていることを確認します。

セキュリティの問題

この項では、セキュリティ関連の測定について説明し、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際の一般的なガイドラインを示します。この項では、次のトピックについて取り上げます。

（注）　この項では、Cisco Unified 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。電話機のリセットについては、電話機のモデルに対応した『*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。

CTL ファイルを Cisco Unified IP Phone（7970 モデル、7960 モデル、および 7940 モデルのみ）から削除する方法については、『*Cisco Unified Communications Manager セキュリティ ガイド*』または電話機のモデルに対応した『*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。

セキュリティ アラーム

Cisco Unified Serviceability は、X.509 名の不一致、認証エラー、および暗号化エラーに対して、セキュリティ関連のアラームを生成します。サービスアビリティの GUI にはアラーム定義があります。

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場合に電話機で生成されます。電話機で生成されるアラームについては、電話機のモデルとタイプ（SCCP または SIP）に対応した『*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。

セキュリティ パフォーマンス モニタ カウンタ

パフォーマンス モニタ カウンタは、Cisco Unified Communications Manager 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 3-1 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 3-1　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 Unified Communications Manager	AuthenticatedCallsActive AuthenticatedCallsCompleted AuthenticatedPartiallyRegisteredPhone AuthenticatedRegisteredPhones EncryptedCallsActive EncryptedCallsCompleted EncryptedPartiallyRegisteredPhones EncryptedRegisteredPhones SIPLineServerAuthorizationChallenges SIPLineServerAuthorizationFailures SIPTrunkServerAuthenticationChallenges SIPTrunkServerAuthenticationFailures SIPTrunkApplicationAuthorization SIPTrunkApplicationAuthorizationFailures TLSConnectedSIPTrunk
SIP スタック	StatusCodes4xxIns StatusCodes4xxOuts 次の例を参考にしてください。 401 未認証（HTTP 認証が必要） 403 禁止 405 メソッドが許可されない 407 プロキシ認証が必要
TFTP サーバ	BuildSignCount EncryptCount

RTMT でパフォーマンス モニ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、『*Cisco Unified Communications Manager Real-Time Monitoring Tool アドミニストレーション 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 Unified Communications Operating System アドミニストレーション ガイド*』を参照してください。

セキュリティ ログおよびトレース ファイルの確認

Cisco Unified Communications Manager 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（cm/log、cm/trace、tomcat/logs、tomcat/logs/security など）に格納します。

（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。

Real-Time Monitoring Tool のトレース収集機能または CLI コマンドを使用して、ログ ファイルとトレース ファイルの検索、表示、および操作を行うことができます。

証明書のトラブルシューティング

Cisco Unified Communications プラットフォームの管理ページ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** のように使用します）。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 Unified Communications Operating System アドミニストレーション ガイド*』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

この項では、次のトピックについて取り上げます。

- 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.3-16）
- 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.3-17）

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、再試行カウンタが含まれています。このカウンタは、［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 トークンの再試行カウンタ値は 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。

『*Cisco Unified Communications Manager セキュリティ ガイド*』の説明に従って、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。必要に応じて、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、『*Cisco Unified Communications Manager セキュリティ ガイド*』を参照してください。

ステップ 3　『*Cisco Unified Communications Manager セキュリティ ガイド*』の説明に従って、電話機をすべてリセットします。

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。

電話機での認証文字列のトラブルシューティング

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

ヒント　電話機が Cisco Unified Communications Manager に登録されていることを確認してください。電話機が Cisco Unified Communications Manager に登録されていない場合、電話機で認証文字列を入力することはできません。

電話機のデバイス セキュリティ モードが非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［認証ストリング］に設定されていることを確認します。

CAPF では、電話機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

電話機では、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はない場合、証明書の有効期限が切れている場合、CAPF 証明書がクラスタ内のすべて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、電話機が Cisco Unified Communications Manager に登録されていない場合などに、失敗することがあります。ローカルで有効な証明書の検証が失敗したときは、SDL トレース ファイルと CAPF トレース ファイルでエラーを確認します。

CAPF 証明書がクラスタ内のすべてのサーバ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 Unified Communications プラットフォーム GUI または CLI を使用して、次の 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電話機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、**[モデル情報]** または［セキュリティ設定］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、電話機のモデルとタイプ（SCCP または SIP）に対応した『*Cisco Unified 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）が電話機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、**[モデル情報]** または［セキュリティ設定］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、電話機のモデルとタイプ（SCCP または SIP）に対応した『*Cisco Unified 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（P.3-18）

パケット キャプチャの使用方法

メディアや TCP パケットをスニフィングするサードパーティ製トラブルシューティング ツールは、SRTP 暗号化を有効にした後は機能しません。このため、問題が発生した場合は、Cisco Unified Communications Manager の管理ページを使用して次の作業を行う必要があります。

- Cisco Unified Communications Manager とデバイス（Cisco Unified IP Phone、Cisco SIP IP Phone、Cisco IOS MGCP ゲートウェイ、H.323 ゲートウェイ、H.323/H.245/H.225 トランク、または SIP トランク）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。

- デバイス間で交換される SRTP パケットをキャプチャする。
- メディア暗号鍵関連情報をメッセージから抽出し、デバイス間で交換されるメディアを復号化する。

パケット キャプチャを使用または設定する方法、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）のパケットを分析する方法については、P.2-6 の「パケット キャプチャ」を参照してください。

ヒント　この作業を複数のデバイスに対して同時に行うと、CPU の使用率が上昇し、コールの処理が妨げられる可能性があります。この作業を行うのは、コール処理への影響が最小限で済む時間帯にすることを強くお勧めします。

この Cisco Unified Communications Manager リリースと互換性のある一括管理ツールを使用すると、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 Unified Communications Manager Bulk Administration ガイド*』を参照してください。

ヒント　この作業を Cisco Unified Communications Manager 一括管理で行うと、CPU の使用率が上昇し、コールの処理が妨げられる可能性があります。この作業を行うのは、コール処理への影響が最小限で済む時間帯にすることを強くお勧めします。

CAPF エラー コード

次の表は、CAPF ログ ファイルに含まれる可能性のある CAPF エラー コードと、その対応策を示しています。

表 3-2　CAPF エラー コード

エラー コード	説明	対応策
0	CAPF_OP_SUCCESS /*Success */	対応策は必要ありません。
1	CAPF_FETCH_SUCCESS_BUT_NO_CERT /* Fetch is successful; however there is no cert */	電話機に証明書をインストールします。詳細については、『*Cisco Unified Communications Manager セキュリティ ガイド*』を参照してください。
2	CAPF_OP_FAIL /* Fail */	実施できる対応策はありません。
3	CAPF_OP_FAIL_INVALID_AUTH_STR /* Invalid Authentication string */	電話機に正しい認証文字列を入力します。詳細については、『*Cisco Unified Communications Manager セキュリティ ガイド*』を参照してください。
4	CAPF_OP_FAIL_INVALID_LSC /* Invalid LSC */	電話機のローカルで有効な証明書（LSC）を更新します。詳細については、『*Cisco Unified Communications Manager セキュリティ ガイド*』を参照してください。

表 3-2　CAPF エラー コード（続き）

エラー コード	説明	対応策
5	CAPF_OP_FAIL_INVALID_MIC, /* Invalid MIC */	製造元でインストールされる証明書（MIC）が無効になっています。LSC をインストールする必要があります。詳細については、『*Cisco Unified Communications Manager セキュリティ ガイド*』を参照してください。
6	CAPF_OP_FAIL_INVALID_CRENDENTIALS, /* Invalid credential */	正しいクレデンシャルを入力します。
7	CAPF_OP_FAIL_PHONE_COMM_ERROR, /* Phone Communication Failure*/	実施できる対応策はありません。
8	CAPF_OP_FAIL_OP_TIMED_OUT, /* Operation timeout */	操作のスケジュールを再設定します。
11	CAPF_OP_FAIL_LATE_REQUEST /* User Initiated Request Late */	CAPF 操作のスケジュールを再設定します。