CHAPTER 3

Cisco Unified Communications Manager システムの問題

この項では、Cisco Unified Communications Manager システムに関連する次のような最も一般的な問題の解決策について説明します。

Cisco Unified Communications Manager システムが応答しない

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。

- 「サーバの応答が遅い」（P.3-15）

Cisco Unified Communications Manager システムが応答を停止した

症状

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

Cisco CallManager サービスが応答しなくなった場合は、次のメッセージがシステム イベント ログに表示されます。

```
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.
```

この場合では、その他にも次のメッセージが表示されることがあります。

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

Cisco Communications Manager が、次のエラーにより起動しませんでした。

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

この状態で 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、ユーザが受信するダイヤル トーンが遅延したり、高い CPU 使用率が原因で 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

サービスが機能するために十分なリソース（CPU やメモリなど）がない場合には、Cisco CallManager サービスは応答を停止できます。一般に、その時点でサーバの CPU 使用率は 100% になります。

推奨処置

発生している中断のタイプに応じて、その中断の根本原因の確認に役立つさまざまなデータを収集する必要があります。

リソースの不足による中断が発生した場合は、次の手順を使用します。

手順

ステップ 1　中断の前後 15 分間の Cisco CallManager トレースを収集します。

ステップ 2　中断の前後 15 分間の Specification and Description Language（SDL）トレースを収集します。

ステップ 3　ある場合は、perfmon トレースを収集します。

ステップ 4　トレースがない場合は、perfmon トレースの収集を開始し、サーバ上で実行されている各プロセスのメモリと CPU の使用率をトラッキングします。これらは、リソースの不足による中断が再度発生した場合に役立ちます。

Cisco Unified Communications Manager の管理が表示されない

症状

Cisco Unified CM の管理が表示されません。

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

「Cisco Unified Communications Manager サービスが動作していることの確認」（P.2-24）または『*Cisco Unified Serviceability Administration Guide*』を参照して、Cisco CallManager サービスがサーバ上でアクティブであり、実行されていることを確認します。

Cisco Unified Communications Manager の管理へのアクセス時にエラーが発生する

症状

Cisco Unified Communications Manager の管理へのアクセスを試みたときに、エラー メッセージが表示されます。

考えられる原因

必要なサービスが自動的に開始されていません。Cisco Unified CM の管理が表示されない最も一般的な理由は、必要なサービスのいずれかが停止していることです。

推奨処置

停止しているサービスを開始します。

後続のノードで Cisco Unified Communications Manager の管理へのアクセス時にエラーが発生する

症状

Cisco Unified Communications Manager の管理へのアクセスを試みたときに、エラー メッセージが表示されます。

考えられる原因

後続ノードがオフラインである場合に Cisco Unified Communications Manager の第 1 ノードの IP アドレスが変更されると、後続ノードで Cisco Unified Communications Manager の管理にログインできない場合があります。

推奨処置

このエラーが発生した場合は、『*Changing the IP Address and Host Name for Cisco Unified Communications Manager*』の説明に従って、Cisco Unified Communications Manager の後続ノードの IP アドレスを変更します。

表示権限がない

症状

Cisco Unified Communications Manager の管理にアクセスしたときに、次のいずれかのメッセージが表示されます。

- このページを表示する権限がありません（You Are Not Authorized to View This Page）
- 指定したクレデンシャルを使用してこのディレクトリまたはページを表示する権限がありません。（You do not have permission to view this directory or page using the credentials you supplied.）
- サーバ アプリケーション エラー。（Server Application Error.）要求の処理時におけるアプリケーションのロード中に、サーバでエラーが発生しました。（The server has encountered an error while loading an application during the processing of your request.）詳細については、イベント ログを参照してください。（Please refer to the event log for more detailed information.）サーバ管理者にお問い合わせください。（Please contact the server administrator for assistance.）
- エラー：アクセスが拒否されました。（Error: Access is Denied.）

考えられる原因

不明

推奨処置

TAC にお問い合わせください。

Cisco Unified Communications Manager でのユーザの表示または追加における問題

症状

Cisco Unified Communications Manager の管理で、ユーザを追加したり、検索を行ったりできません。

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）を含むサーバ上にインストールされた Cisco Unified Communications Manager を使用する場合、または Microsoft Internet Explorer 5.5 SP2 および Q313675 パッチ以上を使用している場合には、次の問題が発生する可能性があります。

- 基本検索を実行して [送信（Submit）] をクリックしても、同じページが再表示されます。
- 新規ユーザの挿入を試みると、次のメッセージが表示されます。

```
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（Call_Manager など）は、Cisco Unified Communications Manager の管理でユーザを追加したり、検索を実行したりできない場合があります。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、アルファベット（A ～ Z、a ～ z）、数字（0 ～ 9）、およびハイフン（-）です。特殊文字は許可されていません。ブラウザに Q313675 パッチがインストールされている場合は、DNS でサポートされていない文字が URL に含まれないようにしてください。

Q313675 パッチの詳細については、「[MS01-058] Internet Explorer 5.5 と Internet Explorer 6 のファイルの脆弱性に対する対策」を参照してください。

次のいずれかの方法を使用して、この問題を解決できます。

- サーバの IP アドレスを使用して Cisco Unified Communications Manager の管理にアクセスする
- DNS でサポートされていない文字をサーバ名で使用しない
- URL で 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が失敗する

症状

次の URL へのアクセスを試みたときに、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：ページを表示できません（This page cannot be displayed）
- Netscape：見つかりません。（Not Found.）要求された URL/ccmadmin がこのサーバ上に見つかりませんでした。（The requested URL /ccmadmin was not found on this server.）

Cisco Unified Communications Manager の名前の代わりに IP アドレスを使用して同じ URL にアクセスすると（http://10.48.23.2/ccmadmin）、ウィンドウが表示されます。

考えられる原因

「your-cm-server-name」として入力した名前が、DNS または hosts ファイルで誤った 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ている場合は、DNS を確認して、*your-cm-server-name* のエントリに Cisco Unified Communications Manager サーバの正しい IP アドレスが設定されていることを確認します。正しくない場合は変更します。

DNS を使用していない場合、ローカル マシンでは、hosts ファイルを確認することによって、*your-cm-server-name* のエントリが存在するかどうか、およびサーバ名に関連付けられている IP アドレスが確認されます。hosts ファイルを開いて、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 サーバとの間でポート 80 がブロックされる

症状

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がファイアウォールによってブロックされている場合は、次のメッセージが表示されます。

- Internet Explorer：ページを表示できません（This page cannot be displayed）
- Netscape：応答がありません。（There was no response.）サーバがダウンしているか、応答していない可能性があります（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により、ローカル ネットワークからサーバ ネットワークへの HTTP アクセスがブロックされています。

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）が許可されているかどうかを確認します。いずれかのタイプのアクセスに成功した場合は、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ます。
2. ネットワーク管理者にセキュリティ ポリシーを確認してください。
3. サーバが配置されているネットワークと同じネットワークから再試行します。

リモート マシンのネットワーク設定が正しくない

症状

Cisco Unified Communications Manager に接続できないか、または Cisco Unified Communications Manager と同じネットワーク内の他のデバイスに接続できません。

他のリモート マシンから同じ処理を試みると、Cisco Unified Communications Manager の管理が表示されます。

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値が正しくない場合は、Web サーバのネットワークに対して接続できないか、または部分的にしか接続できないため、Web ページが表示されない場合があります。

推奨処置

1. 接続できないことを確認するために、Cisco Unified Communications Manager サーバおよびその他のデバイスの IP アドレスに対して ping を実行します。
2. ローカル ネットワークの外部にあるすべてのデバイスに対する接続に失敗する場合は、ステーションのネットワーク設定、およびケーブルとコネクタの整合性を確認してください。詳細については、該当するハードウェア マニュアルを参照してください。

   接続に LAN 経由で TCP/IP を使用している場合は、次の手順を実行して、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（Start）] > [設定（Setting）] > [ネットワークとダイヤルアップ接続（Network and Dial-up connections）] を選択します。
4. [ローカル エリア接続（Local Area Connection）]、[プロパティ（Properties）] の順に選択します。

   通信プロトコルのリストがチェックボックスとともに表示されます。
5. [インターネット プロトコル（TCP/IP）（Internet Protocol (TCP/IP)）] を選択して、再度 [プロパティ（Properties）] をクリックします。
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（Obtain an ip address automatically）] または**アドレス、マスク、およびデフォルト ゲートウェイの手動設定**を選択します。

   また、ブラウザ固有の設定が誤っている可能性もあります。
7. Internet Explorer ブラウザで、[ツール（Tools）] > [インターネット オプション（Internet Options）] を選択します。
8. [接続（Connections）] タブを選択して、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設定されていません。Windows 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には、ネットワークにルーティングの問題があ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てください。

（注）　この手順を実行してもリモート サーバからのブラウジングができない場合は、TAC に連絡して、問題の詳細な調査を依頼してください。

データベース複製

この項では、Cisco Unified Communications Manager システムにおけるデータベース複製に関する次の問題について説明します。

- 「パブリッシャ サーバとサブスクライバ サーバとの間の複製に失敗する」（P.3-7）
- 「接続が失われたノードで接続が復元された場合にデータベース複製が行われない」（P.3-10）
- 「データベース テーブルで同期が外れてもアラートがトリガーされない」（P.3-11）
- 「古い製品リリースに戻す場合のデータベース複製のリセット」（P.3-12）

パブリッシャ サーバとサブスクライバ サーバとの間の複製に失敗する

データベースの複製は、Cisco Unified Communications Manager クラスタのコア機能です。データベースのマスター コピーを備えたサーバはパブリッシャ（最初のノード）として機能し、データベースを複製するサーバはサブスクライバ（以降のノード）を構成します。

ヒント　サブスクライバ サーバに Cisco Unified Communications Manager をインストールする前に、パブリッシャ データベース サーバ上のデータベースをサブスクライバが確実に複製できるように、Cisco Unified CM の管理の [サーバの設定（Server Configuration）] ウィンドウにサブスクライバを追加する必要があります。サブスクライバ サーバを [サーバの設定（Server Configuration）] ウィンドウに追加し、Cisco Unified Communications Manager をサブスクライバにインストールしたら、サブスクライバはパブリッシャ サーバ上のデータベースのコピーを受け取ります。

症状

パブリッシャ サーバ上の変更が、サブスクライバ サー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 サーバとサブスクライバ サーバの間の複製に失敗する。

推奨処置

データベースの複製を確認し、必要に応じて、次の手順に従って修正します。

手順

ステップ 1　データベースの複製を確認します。データベースの複製は、CLI、Cisco Unified Reporting、または RTMT を使用して確認できます。

- CLI を使用した確認については、ステップ 2 を参照してください。

- Cisco Unified Reporting を使用した確認については、ステップ 3 を参照してください。
- RTMT を使用した確認については、ステップ 4 を参照してください。

ステップ 2　CLI を使用してデータベース複製を確認するには、CLI にアクセスし、次のコマンドを発行して、各ノードにおける複製を確認します。各ノードでこの CLI コマンドを実行し、その複製のステータスを確認する必要があります。また、サブスクライバをインストールしたあと、サブスクライバの数によっては、2 のステータスになるまでにかなりの時間がかかる場合があります。

```
admin: show perf query class "Number of Replicates Created and State of Replication"
==>query class:

        - Perf class (Number of Replicates Created and State of Replication)
    has instances and values:
        ReplicateCount  -> Number of Replicates Created   = 344
        ReplicateCount  -> Replicate_State                = 2
```

この場合に Replicate_State オブジェクトが 2 の値を示すことに注意してください。次に、Replicate_State が取ることのできる値を示します。

- 0：この値は、複製が開始されていないことを示します。後続のノード（サブスクライバ）がありません。または、Cisco Database Layer Monitor サービスが、サブスクライバのインストール後から実行されていません。
- 1：この値は、複製が作成されているにもかかわらず、カウントが間違っていることを示します。
- 2：この値は、複製の状態が良好であることを示します。
- 3：この値は、クラスタで複製に問題があることを示します。
- 4：この値は、複製の設定に失敗したことを示します。

ステップ 3　Cisco Unified Reporting を使用してデータベース複製を確認するには、次のタスクを実行します。

a. Cisco Unified CM の管理の右上隅にある [ナビゲーション（Navigation）] ドロップダウン リスト ボックスから、[Cisco Unified Reporting] を選択します。

b. Cisco Unified Reporting が表示されたら、[System Reports] をクリックします。

c. データベース複製のデバッグ情報を示す [Unified CM Database Status] レポートを生成および表示します。

レポートを生成したあと、レポートを開いて、[Unified CM Database Status] を確認します。ここには、クラスタ内の全サーバの RTMT レプリケーション カウンタが含まれます。すべてのサーバの複製状態は 2 になっていなければならず、すべてのサーバで同じ数の複製が作成されている必要があります。

前述のステータスの確認で複製の状態が 2 になっていない場合は、このレポートの「Replication Server List」を参照してください。ここには、接続され、各ノードとやり取りしているサーバが表示されます。リストにおいて、各サーバは、自身をローカルとして示し、その他のサーバをアクティブに接続されているサーバとして示します。いずれかのサーバの接続が切断されていると表示されている場合は、通常、ノード間に通信上の問題が発生しています。

d. このためには、Cisco Unified Communications Manager データベースの健全性のスナップショットを提供する [Unified CM Database Status] レポートを生成および表示します。

ステップ 4　RTMT を使用してデータベース複製を確認するには、次のタスクを実行します。

a. Cisco Unified Real-Time Monitoring Tool（RTMT）を開きます。

b. [CallManager] タブをクリックします。

c. [Database Summary] をクリックします。[Replication Status] ペインが表示されます。

[Replication Status] ペインに表示される値を次に示します。

- 0：この値は、複製が開始されていないことを示します。後続のノード（サブスクライバ）がありません。または、Cisco Database Layer Monitor サービスが、サブスクライバのインストール後から実行されていません。
- 1：この値は、複製が作成されているにもかかわらず、カウントが間違っていることを示します。
- 2：この値は、複製の状態が良好であることを示します。
- 3：この値は、クラスタで複製に問題があることを示します。
- 4：この値は、複製の設定に失敗したことを示します。

d. Replicate_State パフォーマンス モニタリング カウンタを表示するには、[System] > [Performance] > [Open Performance Monitoring] を選択します。パブリッシャ データベース サーバ（最初のノード）をダブルクリックし、パフォーマンス モニタを拡張します。[Number of Replicates Created and State of Replication] をクリックします。[Replicate_State] をダブルクリックします。[Object Instances] ウィンドウの [ReplicateCount] をクリックし、[Add] をクリックします。

ヒント 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、[Counter Description] を選択します。

ステップ 5　すべてのサーバで RTMT のステータスが良好であるにもかかわらず、データベースが同期していないことが疑われる場合は、CLI コマンド **utils dbreplication status** を実行します（いずれかのサーバで RTMT ステータスが 4 と表示される場合は、ステップ 6 に進みます）。

このステータス コマンドは、**utils dbreplication status all** を使用してすべてのサーバで、または **utils dbreplication status** <*hostname*> を使用して 1 つのサブスクライバで実行できます。

ステータス レポートは、疑わしいテーブルがあるかどうかを示します。疑わしいテーブルがある場合は、複製修正 CLI コマンドを使用し、パブリッシャ サーバからサブスクライバ サーバにデータを同期します。

複製の修正は、次のコマンドを使用して、すべてのサブスクライバ サーバで実行することも（**all** パラメータを使用）、1 つのサブスクライバ サーバだけで実行することもできます。

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

複製の修正を実行した後（数分間かかることがある）、別のステータス コマンドを実行して、すべてのテーブルが同期されたことを確認できます。

修正後にテーブルが同期されていれば、複製の修正は成功です。

（注） サーバの 1 つで RTMT のステータスが 4 の場合、またはステータス 0 の状態が 4 時間を超えた場合に限り、ステップ 6 を実行します。

ステップ 6　データベース複製のデバッグ情報を示す [Unified CM Database Status] レポートを生成および表示します。RTMT のステータスが不良と表示される各サブスクライバで、hosts、rhosts、sqlhosts、およびサービス ファイルに適切な情報が含まれることを確認します。

[Cisco Unified CM Cluster Overview] レポートを生成し、表示します。サブスクライバ サーバのバージョンが同一であること、接続が正常であること、時間遅延が許容値内であることを確認します。

前述の条件が許容できるものである場合、次の手順を実行して、そのサブスクライバ サーバ上でレプリケーションをリセットします。

a. サブスクライバ サーバで、CLI コマンド **utils dbreplication stop** を実行します。これを、RTMT の値が 4 のすべてのサブスクライバ サーバで実行します。

b. パブリッシャ サーバで、CLI コマンド **utils dbreplication stop** を実行します。

c. パブリッシャ サーバで、CLI コマンド **utils dbreplication reset** <*hostname*> を実行します。ここで、<*hostname*> はリセットする必要のあるサブスクライバ サーバのホスト名です。すべてのサブスクライバ サーバをリセットする必要がある場合は、コマンド **utils dbreplication reset all** を使用します。

参照先

- 『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』
- 『*Cisco Unified Reporting Administration Guide*』
- 『*Command Line Interface Reference Guide for Cisco Unified Solutions*』

接続が失われたノードで接続が復元された場合にデータベース複製が行われない

症状

失われたノードの回復時に接続が復元されても、データベースの複製が行われません。トピック「パブリッシャ サーバとサブスクライバ サーバとの間の複製に失敗する」（P.3-7）で説明する方法を使用して、複製の状態を確認できます。ノードですでに複製のリセットを試み、その操作に失敗している場合に限り、次の手順を使用します。

考えられる原因

デバイス テーブルでの削除により、CDR チェックがループに入っている。

推奨処置

ステップ 1　影響を受けているサブスクライバで **utils dbreplication stop** を実行します。これはすべて同時に実行できます。

ステップ 2　ステップ 1 が完了するまで待ち、次に、影響を受けているパブリッシャ サーバで **utils dbreplication stop** を実行します。

ステップ 3　影響を受けているパブリッシャ サーバから **utils dbreplication clusterreset** を実行します。このコマンドを実行すると、ログ名がログ ファイルにリストされます。このファイルを確認し、プロセスのステータスをモニタします。パスは次のとおりです。
/var/log/active/cm/trace/dbl/sdi

ステップ 4　影響を受けているパブリッシャから **utils dbreplication reset all** を実行します。

ステップ 5　クラスタ内のすべてのサブスクライバ サーバですべてのサービスを停止し、再起動して（または、すべてのシステム（サブスクライバ サーバ）を再起動/リブートして）、サービスを変更します。この操作は必ず、**utils dbreplication status** で 2 のステータスが表示されてから実行します。

データベース テーブルで同期が外れてもアラートがトリガーされない

（注）　「同期されていない」とは、クラスタ内の 2 つのサーバで、特定のデータベース テーブルに同じ情報が含まれていない状態を指します。

症状

Cisco Unified Communications Manager バージョン 6.x 以降では、この症状には予期しないコール処理の動作が含まれます。コールが、予期したようにルーティングまたは処理されません。この症状は、パブリッシャ サーバとサブスクライバ サーバのいずれかで発生することがあります。

Cisco Unified Communications Manager バージョン 5.x では、この症状には予期しないコール処理の動作が含まれます。コールのルーティングと処理は予想どおりに実行されませんが、これは、パブリッシャ サーバがオフラインになっているときに限ります。

この症状が発生したときに CLI で **utils dbrepication status** を実行すると、`Out of sync` とレポートされます。
`Out of sync` と表示されない場合、問題はありません。

考えられる原因

ノード間でデータベース テーブルの同期が外れたままになっています。複製アラートは、複製プロセスの障害だけを示し、データベース テーブルの同期が外れた時期は示しません。通常、複製が正しく行われている場合は、テーブルの同期は維持されているはずです。場合によっては、複製が正しく行われているように見えるにもかかわらず、データベース テーブルが「同期されていない」状況が発生することがあります。

推奨処置

ステップ 1　CLI コマンドを使用してクラスタの複製をリセットします。この処置を実行するためには、クラスタ内のサーバがオンラインで、IP 接続が完全に確立されていることが必要です。クラスタ内のすべてのサーバがオンラインであるかどうかは、プラットフォームの CLI および Cisco Unified Reporting を使用して確認します。

ステップ 2　サーバの複製の状態が 2 の場合は、パブリッシャ サーバで次のコマンドを実行します。
utils dbreplication repair *server name*

サーバの複製の状態が 2 ではない場合は、
すべてのサブスクライバ サーバで次のコマンドを実行します。
utils dbreplication stop

次に、すべてのパブリッシャ サーバで次のコマンドを実行します。
utils dbreplication stop
次に以下のコマンドを実行します。
utils dbreplication reset all

古い製品リリースに戻す場合のデータベース複製のリセット

古い製品リリースを実行できるようにクラスタ内のサーバを元に戻す場合は、クラスタ内部でデータベースの複製を手動でリセットする必要があります。すべてのクラスタ サーバを古い製品リリースに戻したあとにデータベース複製をリセットするには、パブリッシャ サーバで CLI コマンド **utils dbreplication reset all** を入力します。

Cisco Unified Communications Operating System Administration または CLI を使用してバージョンを切り替えると、古い製品バージョンに戻すときに、データベース複製のリセット要件に関するメッセージが表示されます。

utils dbreplication clusterreset

このコマンドを使用すると、クラスタ全体でデータベース複製がリセットされます。

コマンド構文

utils dbreplication clusterreset

使用上のガイドライン

このコマンドを実行する前に、utils dbreplication stop コマンドをすべてのサブスクライバ サーバで実行し、その後、パブリッシャ サーバでも実行します。

要件

コマンド特権レベル：0

アップグレード時の使用：可能

utils dbreplication dropadmindb

このコマンドは、クラスタ内のすべてのサーバにある Informix の syscdr データベースをドロップします。

コマンド構文

utils dbreplication dropadmindb

使用上のガイドライン

このコマンドは、データベース複製のリセットまたはクラスタのリセットが失敗し、複製を再起動できない場合にのみ使用します。

要件

コマンド特権レベル：0

アップグレード時の使用：可能

LDAP 認証の失敗

この項では、LDAP 認証に失敗した場合の一般的な問題について説明します。

症状

エンド ユーザのログインに失敗します。ユーザがログインする前に、認証タイムアウトが発生します。

考えられる原因

Cisco Unified CM の管理の [LDAP 認証（LDAP Authentication）] ウィンドウにおける [LDAP ポート（LDAP Port）] の設定が誤っています。

推奨処置

社内ディレクトリの設定に応じて、[LDAP ポート（LDAP Port）] フィールドに入力するポート番号が決まります。たとえば、[LDAP ポート（LDAP Port）] フィールドを設定する前に、LDAP サーバがグローバル カタログ サーバとして動作するかどうかや、設定に LDAP over SSL が必要であるかどうかを確認します。たとえば、次のようなポート番号を入力します。

例：LDAP サーバがグローバル カタログ サーバではない場合の LDAP ポート

- 389：SSL が必要でない場合。（このポート番号は、[LDAP ポート（LDAP Port）] フィールドに表示されるデフォルトです）。
- 636：SSL が必要な場合。（このポート番号を入力する場合は、[SSL を使用（Use SSL）] チェックボックスがオンであることを確認します）。

例：LDAP サーバがグローバル カタログ サーバである場合の LDAP ポート

- 3268：SSL が必要でない場合。
- 3269：SSL が必要な場合。（このポート番号を入力する場合は、[SSL を使用（Use SSL）] チェックボックスがオンであることを確認します）。

ヒント 設定によっては、上記の例に示した番号以外のポート番号を入力する必要がある場合があります。[LDAP ポート（LDAP Port）] フィールドを設定する前に、ディレクトリ サーバの管理者に問い合わせて、入力する正しいポート番号を確認してください。

LDAP over SSL の問題

この項では、LDAP over SSL を使用する場合の一般的な問題について説明します。

症状

LDAP over SSL が動作しません。

考えられる原因

ほとんどの場合、LDAP over SSL の問題の原因は、Cisco Unified Communications Manager サーバ上の証明書（チェーン）が無効であるか、誤っているか、または不完全であることです。

説明

SSL には、複数の証明書を使用する場合があります。ほとんどの場合、LDAP over SSL を動作させるには、ディレクトリ信頼証明書として AD ルート証明書をアップロードするだけで済みます。ただし、異なるディレクトリ信頼証明書がアップロードされた場合、つまりルート証明書以外の証明書がアップロードされた場合は、その証明書をルート証明書などの上位レベルの証明書によって確認する必要があります。この場合、複数の証明書が関係するため、証明書チェーンが作成されます。たとえば、証明書チェーンには、次の証明書が含まれている場合があります。

- ルート証明書：信頼チェーンにおける最上位の CA 証明書です。この証明書の発行者と被認証者は同じです。
- 中間証明書：信頼チェーンの一部を構成する CA 証明書です（最上位以外）。中間証明書によって、階層のルートから最下位の中間証明書までがつながります。

- リーフ証明書：1 つ上の階層の中間証明書によって署名された、サービスやサーバに発行される証明書です。

企業における証明書チェーンには、たとえば 2 つの証明書および 1 つのルート証明書があります。次に、証明書の内容を示します。

Data:

Version: 3 (0x2)

Serial Number:

77:a2:0f:36:7c:07:12:9c:41:a0:84:5f:c3:0c:64:64

Signature Algorithm: sha1WithRSAEncryption

Issuer: DC=com, DC=DOMAIN3, CN=jim

Validity

Not Before: Apr 13 14:17:51 2009 GMT

Not After: Apr 13 14:26:17 2014 GMT

Subject: DC=com, DC=DOMAIN3, CN=jim

推奨処置

2 ノードのチェーンの場合、チェーンにはルート証明書とリーフ証明書が含まれています。この場合は、ディレクトリ信頼ストアにルート証明書をアップロードするだけで済みます。

3 つ以上のノードのチェーンの場合、チェーンには、ルート証明書、リーフ証明書、および中間証明書が含まれています。この場合は、ルート証明書、およびリーフ証明書を除くすべての中間証明書をディレクトリ信頼ストアにアップロードする必要があります。

証明書チェーンの最上位（ルート証明書）の Issuer（発行者）フィールドと Subject（被認証者）フィールドが同じであることを確認します。Issuer フィールドと Subject フィールドが同じでない場合、証明書はルート証明書ではなく中間証明書となります。この場合は、ルートから最下位中間証明書までのチェーン全体を特定して、チェーン全体をディレクトリ信頼ストアにアップロードします。

また、Validity フィールドを確認して、証明書の有効期限が切れていないことを確認します。中間証明書の有効期限が切れている場合は、新しいチェーン、および新しいチェーンを使用して署名された新しいリーフ証明書を認証機関から取得します。リーフ証明書の有効期限だけが切れている場合は、署名された新しいリーフ証明書を取得します。

OpenLDAP で LDAP サーバに接続するための証明書を確認できない

症状

CTI クライアントまたは JTAPI クライアント経由でのエンド ユーザ認証に失敗しますが、Unified CM へのユーザ認証は動作します。

考えられる原因

OpenLDAP では、LDAP サーバに接続するための証明書を確認できません。

説明

証明書は、完全修飾ドメイン名（FQDN）を使用して発行されます。OpenLDAP の検証プロセスでは、FQDN がアクセス先のサーバと照合されます。アップロードされている証明書では FQDN が使用され、Web フォームでは IP アドレスが使用されているため、OpenLDAP はサーバに接続できません。

推奨処置

- 可能な場合には、DNS を使用します。

  証明書署名要求（CSR）プロセス時に、被認証者 CN の一部として FQDN を指定します。この CSR を使用して自己署名証明書または CA 証明書を取得すると、通常名には同じ FQDN が含まれます。したがって、CTI や CTL などのアプリケーションで LDAP 認証がイネーブル化された場合でも、信頼証明書がディレクトリ信頼ストアにインポートされていれば、問題は発生しません。

- DNS を使用していない場合は、Cisco Unified CM の管理の [LDAP 認証設定（LDAP Authentication Configuration）] ウィンドウに IP アドレスを入力します。その後、/etc/openldap/ldap.conf に次の 1 行を追加します。

  TLS_REQCERT never

  このファイルを更新するには、リモート アカウントが必要です。このように設定すると、OpenLDAP ライブラリで、サーバの証明書が確認されません。ただし、後続の通信は引き続き SSL を使用して行われます。

サーバの応答が遅い

この項では、全二重ポートの設定が一致しないためにサーバからの応答が遅くなることに関連した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ります。

考えられる原因

スイッチの全二重ポート設定が Cisco Unified Communications Manager サーバの全二重ポート設定と一致しない場合、応答が遅くなる可能性があります。

推奨処置

1. 最適なパフォーマンスを得るために、スイッチおよびサーバの両方を **100/Full** に設定します。

   スイッチまたはサーバで Auto 設定を使用することは推奨しません。

2. この変更を有効にするには、Cisco Unified Communications Manager サーバを再起動する必要があります。

JTAPI サブシステム起動の問題

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 プラットフォームには、Cisco Unified Auto-Attendant、Cisco IP ICD、Cisco Unified IP-IVR などのテレフォニー アプリケーションがホストされます。この項ではこれらのアプリケーションに固有の内容については説明しませんが、JTAPI サブシステムはこれらすべてのアプリケーションで使用される基本的なコンポーネントであることに注意する必要があります。

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 バージョンが互換性のあるものであることを確認します。互換性を確認するには、使用しているバージョンの Cisco Unified Communications Manager の『Cisco Unified Communications Manager Release Notes』を参照してください。

CRS のバージョンを確認するには、http://servername/appadmin と入力して AppAdmin にログインします。ここで、*servername* には、CRS がインストールされているサーバの名前を指定します。メイン メニューの右下隅で現在のバージョンを確認します。

JTAPI サブシステムが OUT_OF_SERVICE になる

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** ストリングを検索します。行の末尾に、例外の理由が表示されます。

次に、最も一般的なエラーを示します。

- 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、JTAPI 設定に誤ったユーザ名またはパスワードを入力しました。

エラー メッセージの全文

```
%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

ユーザ名およびパスワードが正しいかどうかを確認します。Cisco Unified Communications Manager の [Cisco Unified CM ユーザ（Cisco Unified CM User）] ウィンドウ（http://servername/ccmuser）にログインして、Cisco Unified Communications Manager が正しく認証できないことを確認します。

Unable to create provider—Connection refused

考えられる原因

Cisco Unified Communications Manager で、JTAPI から Cisco Unified Communications Manager への接続が拒否されました。

エラー メッセージの全文

```
%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 コントロール センターで、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—login=

考えられる原因

JTAPI 設定ウィンドウで何も設定されていません。

エラー メッセージの全文

```
%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 設定ウィンドウで、JTAPI プロバイダーを設定します。

Unable to create provider—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 メッセージの全文

```
%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 エンジンからの DNS 名前解決が正しく動作しているかどうかを確認します。DNS 名の代わりに IP アドレスを使用します。

Unable to create provider—Operation timed out

考えられる原因

CRS エンジンから Cisco Unified Communications Manager に IP 接続できません。

エラー メッセージの全文

```
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 サーバの 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 サーバおよび Cisco Unified Communications Manager のデフォルト ゲートウェイ設定を確認します。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 アドレスやホスト名が設定されていないか、または正しいバージョンの JTAPI クライアントを使用していません。

エラー メッセージの全文

```
%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 バージョンが正しくない場合は、Cisco Unified Communications Manager の [プラグイン（Plugins）] ウィンドウから JTAPI クライアントをダウンロードして、CRS サーバにインストールします。

MIVR-SS_TEL-1-ModuleRunTimeFailure

症状

通常、この例外は、JTAPI サブシステムでどのポートも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 を通して 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 メッセージの全文

```
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 の JTAPI ユーザを確認して、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 になる

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 サブシステムで、1 つ以上の 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 メッセージの全文

```
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

トレースのメッセージには、どの CTI ポートまたはルート ポイントが初期化できないかが示されます。このデバイスが Cisco Unified Communications Manager の設定に存在すること、および Cisco Unified Communications Manager の 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の情報、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ための一般的なガイドラインについて説明します。この項では、次のトピックについて説明します。

- 「証明書のトラブルシューティング」（P.3-22）
- 「CTL セキュリティ トークンのトラブルシューティング」（P.3-22）
- 「CAPF のトラブルシューティング」（P.3-23）
- 「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.3-24）

（注）　この項では、Cisco Unified IP Phone が不適切な負荷やセキュリティに関するバグなどによって機能しなくなった場合のリセット方法については説明していません。電話機のリセットの詳細については、電話機のモデルに応じた『*Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager*』を参照してください。

Cisco Unified IP Phone models 7970、7960、および 7940 のみから CTL ファイルを削除する方法については、電話機のモデルに応じた『*Cisco Unified Communications Manager Security Guide*』または『*Cisco Unified IP Phone Administration Guide 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 では、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、セキュリティ関連アラームが生成されます。Cisco Unified Serviceability によってアラーム定義が提供されます。

TFTP サーバ エラーおよび CTL ファイル エラーが発生した場合は、電話機でアラームが生成される可能性があります。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）に応じた『*Cisco Unified IP Phone Administration Guide 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 カウンタでは、Cisco Unified Communications Manager に登録された認証済み電話機の数、完了した認証済みコールの数、および現時点でアクティブな認証済みコールの数が監視されます。表 3-1 に、セキュリティ機能に該当するパフォーマンス 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
	例：
	401 権限なし（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 でのパフォーマンス モニタへのアクセス、perfmon ログの設定、およびカウンタの詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。

CLI コマンド **show perf** を使用すると、パフォーマンス監視情報が表示されます。CLI インターフェイスの使用方法の詳細については、『*Command Line Interface Reference Guide for Cisco Unified Solutions*』を参照してください。

セキュリティ ログ ファイルおよびトレース ファイルの確認

Cisco Unified Communications Manager では、複数のディレクトリ（cm/log、cm/trace、tomcat/logs、tomcat/logs/security など）にログ ファイルおよびトレース ファイルが保存されます。

（注）　暗号化をサポートするデバイスでは、SRTP キー情報はトレース ファイルに出力されません。

Cisco Unified Real-Time Monitoring Tool または CLI コマンドのトレース収集機能を使用すると、ログ ファイルおよびトレース ファイルを検索、表示、および操作できます。

証明書のトラブルシューティング

Cisco Unified Communications Platform Administration の証明書管理ツールを使用すると、証明書の表示、証明書の削除、証明書の再生成、証明書の有効期限の監視、証明書と CTL ファイルのダウンロードやアップロードを行うことができます。たとえば、更新した CTL ファイルを Unity にアップロードできます。CLI を使用すると、自己署名証明書および信頼証明書を一覧表示または表示したり、自己署名証明書を再生成したりできます。

CLI コマンド **show cert**、**show web-security**、**set cert regen**、および **set web-security** を使用すると、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 を使用した証明書の管理方法の詳細については、『*Cisco Unified Communications Operating System Administration Guide*』および『*Command Line Interface Reference Guide for Cisco Unified Solutions*』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、次のトピックで構成されています。

- 「連続して誤ったセキュリティ トークン パスワードを入力したあとに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.3-22）
- 「1 つのセキュリティ トークン（eToken）が失われた場合のトラブルシューティング」（P.3-22）

すべてのセキュリティ トークン（eToken）が失われた場合は、Cisco TAC に問い合わせてください。

連続して誤ったセキュリティ トークン パスワードを入力したあとに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。このカウンタには、eToken の [パスワード（Password）] ウィンドウでログインを連続して試行できる回数が指定されています。セキュリティ トークンの再試行カウンタ値は 15 です。カウンタ値を超える回数のログインが連続して試みられた場合、つまり 16 回連続してログインに失敗した場合は、セキュリティ トークンがロックされて使用できなく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 トークンは、再度イネーブル化することができません。

『*Cisco Unified Communications Manager Security Guide*』の説明に従って、追加のセキュリティ トークンを入手して 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 トークンを購入して、ファイルを設定します。

ヒント　パスワードの入力に成功すると、カウンタはゼロにリセットされます。

1 つのセキュリティ トークン（eToken）が失われた場合のトラブルシューティング

1 つのセキュリティ トークンが失われた場合は、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 ファイルを署名したトークンを使用し、次のタスクを実行することによって 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. 失われたトークンを CTL ファイルから削除します。

これらのタスクの実行方法の詳細については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。

ステップ 3　『*Cisco Unified Communications Manager Security Guide*』の説明に従って、すべての電話機をリセットします。

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説明します。

- 「電話機の認証文字列のトラブルシューティング」（P.3-23）
- 「ローカルで有効な証明書の確認に失敗した場合のトラブルシューティング」（P.3-24）
- 「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」（P.3-24）
- 「電話機にローカルで有効な証明書が存在することの確認」（P.3-24）
- 「電話機に Manufacture-Installed Certificate（MIC; 製造元でインストールされる証明書）が存在することの確認」（P.3-24）
- 「CAPF エラー コード」（P.3-25）

電話機の認証文字列のトラブルシューティング

電話機に誤った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てください。

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ます。電話機が Cisco Unified Communications Manager に登録されていない場合は、電話機に認証文字列を入力できません。

電話機のデバイス セキュリティ モードが非セキュアであることを確認します。

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

CAPF では、電話機に認証文字列を連続して入力できる回数が制限されています。10 回連続して誤った認証文字列を入力した場合は、10 分間以上待機してから再度正しい認証文字列を入力します。

ローカルで有効な証明書の確認に失敗した場合のトラブルシューティング

電話機では、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に存在しない場合、CAPF 証明書が CAPF ディレクトリに存在しない場合、電話機が Cisco Unified Communications Manager に登録されていない場合などに、ローカルで有効な証明書の確認が失敗します。ローカルで有効な証明書の確認に失敗した場合は、SDL トレース ファイルおよび 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 固有のキー ペアおよび証明書が CAPF によって自動的に生成されます。Cisco CTL クライアントがクラスタ内のすべてのサーバにコピーする CAPF 証明書の拡張子は .0 です。CAPF 証明書が存在することを確認するには、Cisco Unified Communications プラットフォームの GUI で CAPF 証明書を表示するか、または CLI を使用します。

- DER 符号化形式：CAPF.cer
- PEM 符号化形式：CAPF.cer と同じ通常名ストリングを含む拡張子が .0 のファイル

電話機にローカルで有効な証明書が存在することの確認

[モデル情報（Model Information）] または [セキュリティ設定（Security Configuration）] 電話機メニューで LSC 設定を表示することによって、電話機にローカルで有効な証明書がインストールされていることを確認できます。詳細については、電話機のモデルとタイプ（SCCP または SIP）に応じた『*Cisco Unified IP Phone Administration Guide*』を参照してください。

電話機に Manufacture-Installed Certificate（MIC; 製造元でインストールされる証明書）が存在することの確認

[モデル情報（Model Information）] または [セキュリティ設定（Security Configuration）] 電話機メニューで MIC 設定を表示することによって、電話機に MIC が存在することを確認できます。詳細については、電話機のモデルとタイプ（SCCP または SIP）に応じた『*Cisco Unified IP Phone Administration Guide*』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説明します。

- 「パケット キャプチャの使用」（P.3-24）

パケット キャプチャの使用

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 暗号化をイネーブルにしたあとは機能しません。このため、問題が発生した場合は、Cisco Unified Communications Manager の管理を使用して次のタスクを行う必要があります。

- Cisco Unified Communications Manager とデバイスとの間で交換されるメッセージのパケットの分析（Cisco Unified IP Phone [SCCP および SIP]、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）。

（注）　SIP トランクでは、SRTP はサポートされていません。

- デバイス間の SRTP パケットのキャプチャ。
- メッセージからのメディア暗号キー情報の抽出、およびデバイス間のメディアの復号化。

パケット キャプチャの使用または設定、および SRTP を使用して暗号化されたコール（およびその他すべてのコール タイプ）のキャプチャしたパケットの分析に関する詳細については、「パケット キャプチャ」（P.2-8）を参照してください。

ヒント　このタスクを複数のデバイスに対して同時に実行すると、CPU 使用率が高くなり、コール処理が中断される可能性があります。このタスクは、コール処理が中断される危険性が最も少ないときに実行することを強く推奨します。

Cisco Unified Communications Manager のこのリリースと互換性がある Bulk Administration Tool を使用することによって、電話機のパケット キャプチャ モードを設定できます。このタスクの実行方法の詳細については、『*Cisco Unified Communications Manager Bulk Administration Guide*』を参照してください。

ヒント　Cisco Unified Communications Manager Bulk Administration でこのタスクを実行すると、CPU 使用率が高くなり、コール処理が中断される可能性があります。このタスクは、コール処理が中断される危険性が最も少ないときに実行することを強く推奨します。

CAPF エラー コード

次の表に、CAPF ログ ファイルに出力される可能性がある CAPF エラー コード、および各コードに対応する修正処置を示します。

表 3-2　CAPF エラー コード

エラー コード	説明	対処方法
0	CAPF_OP_SUCCESS /*Success */	修正処置は必要ありません。
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 Security Guide*』を参照してください。
2	CAPF_OP_FAIL /* Fail */	修正処置はありません。
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てください。詳細については、『*Cisco Unified Communications Manager Security Guide*』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	対処方法
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 Security Guide*』を参照してください。
5	CAPF_OP_FAIL_INVALID_MIC, /* Invalid MIC */	このコードは、製造元でインストールされる証明書（MIC）が無効になったことを示しています。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 Security Guide*』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*/	修正処置はありません。
8	CAPF_OP_FAIL_OP_TIMED_OUT, /* Operation timeout */	操作を再スケジュールします。
11	CAPF_OP_FAIL_LATE_REQUEST /* User Initiated Request Late */	CAPF 操作を再スケジュールします。

障害が発生した RAID ディスクの交換の実行

ここでは、障害が発生したディスクの交換についての情報と、Redundant Array of Inexpensive Disks（RAID）の再構築機能のトラブルシューティングについての一般的なガイドラインを説明します。ここでは、次の内容について説明します。

- 再起動を 1 回行って、障害が発生した RAID ディスクを交換する
- Linux ソフトウェア RAID で再起動を 1 回行って、障害が発生した RAID ディスクを交換する
- 再起動を行わないで、障害が発生した RAID ディスクを交換する

MCS サーバでは、ハードディスクで障害またはその他の問題が発生した場合にデータが失われないようにするために、RAID ドライブが使用されています。

RAID 再構築手順を実行して障害が発生したディスクを交換するには、システムが 2 台以上のハードディスクを使用して動作している必要があります。

1 台のハードディスクだけで動作するシステムでは、RAID のミラーは適用されず、ディスクで障害が発生するとデータがすべて失われます。このようなサーバを回復するには、障害が発生した単一のディスクを代わりの新しいディスクに交換して、DRS 回復を実行する必要があります。このようなサーバでは、事前に DRS を設定して、日次バックアップをスケジュールすることを強く推奨します。これにより、このような致命的な障害が発生した場合でも、可能なかぎり多くのデータを回復できます。

DRS の詳細については、『*Disaster Recovery Administration Guide*』を参照してください。

制限事項

最初に、RAID 再構築に関する次の制限事項について理解する必要があります。

- これらの手順は、Cisco Unified Communications Manager 7.1(2) リリース以降に適用されます。
- これらの RAID 再構築手順は、物理ディスクを 1 台だけ備える次のサーバ モデルには適用されません。
  - MCS-7815-I3
  - MCS-7816-H3
  - MCS-7816-I3
  - MCS-7816-I4
- RAID の再構築を行うと、入出力（I/O）のパフォーマンスに影響があるため、障害が発生したディスクの交換作業および再構築作業は、オフピーク時またはメンテナンス時間帯にスケジュールしてください。
- 障害が発生したディスクの交換についての説明は、各項で説明されているように RAID が設定されているサーバでだけサポートされ、RAID ディスクのうちの 1 つに障害が発生した場合にだけ適用されます。

  通常、ディスクの障害は、SNMP トラップ、RTMT トラップ、またはディスクの LED ステータス（サポートされているサーバだけ）によって検出されます。次の手順で説明するように、CLI コマンド **show hardware** を使用して、手動で RAID ドライブのステータスを確認できます。

警告　**次の手順で障害が発生していると検出されないディスクのディスク交換を行う場合、次の手順は適用されず、サポートもされません。**

わかりやすくするために、RAID 再構築手順は、サーバのモデル番号に基づいてさまざまなサーバ タイプに分類されています。サーバのモデル番号に応じて、対応する手順を選択し、障害が発生したディスクを交換できます。

次の表では、各手順において必要なシステム再起動の回数に応じて各サーバ タイプに分類されています。

表 3-3　再起動回数に応じたサーバの分類

必要な再起動回数	サーバ モデル	手順
1 回	MCS-7825-H4	再起動を 1 回行って、障害が発生した RAID ディスクを交換する
	MCS-7825-I3	
	MCS-7825-I4	
	MCS-7828-I3	
	MCS-7825-H3	Linux ソフトウェア RAID で再起動を 1 回行って、障害が発生した RAID ディスクを交換する
	MCS-7828-H3	

表 3-3　再起動回数に応じたサーバの分類（続き）

必要な再起動回数	サーバ モデル	手順
再起動なし	MCS-7835-H2	再起動を行わないで、障害が発生した RAID ディスクを交換する
	MCS-7835-I2	
	MCS-7845-H2	
	MCS-7845-I2	
	MCS-7835-I3	
	MCS-7845-I3	
	DL-380-G6	

再起動を 1 回行って、障害が発生した RAID ディスクを交換する

次の特定のサーバにおいて障害が発生した RAID ディスクを交換するには、次の手順を実行します。

- MCS-7825-H4
- MCS-7825-I3
- MCS-7825-I4
- MCS-7828-I3

ステップ 1　管理者としてコンソールにログインし、CLI コマンド **show hardware** を入力します。

ステップ 2　論理ドライブのステータスを確認します。次のいずれかを実行します。

- 論理ドライブのステータスが OK または Optimal である場合は、これ以上の処理は必要ありません。
- 論理ドライブのステータスが OK ではない場合は、ステップ 3 で説明されているように物理ディスクのステータスを確認します。

ステップ 3　CLI コマンド **show hardware** を再度入力して、次のいずれかを実行します。

- 「Failed」というステータスの物理ディスクがない場合、これ以上の処理は必要ありません。
- 論理ドライブのステータスが OK または Optimal ではなく、「Failed」と表示された物理ディスクがある場合は、次のようにサーバ上の物理ディスクを特定します。

障害が発生したディスクの LED の色がオレンジ色または赤色になります。

（注）　ステップ 2 を実行して論理 RAID ドライブのステータスを確認してから、ステップ 3 を実行して物理ディスクのステータスを確認する必要があります。

障害が発生したドライブを交換して RAID を再構築するには、ステップ 4 に進みます。

ステップ 4　CLI コマンド **utils system shutdown** を使用して、サーバを正常にシャットダウンします。

ステップ 5　システムをシャットダウンしたあと、障害が発生したディスクが設置されていた空きスロットに、元のディスクと同じタイプ、同じ製造業者、同じサイズの新しいディスクを装着します。たとえば、Western Digital 社のディスクを装着します。

ステップ 6　新しい交換用ディスクがしっかりと挿入されていることを確認します。

ステップ 7　システムを起動します。

ステップ 8　システムの起動時に RAID についてのメッセージが表示された場合は、デフォルトのオプションを受け入れて、システムの起動を続行します。

ステップ 9　システムが起動したあと、CLI にログインして、CLI コマンド **show hardware** を入力します。

show hardware コマンド出力の「Logical Drive」セクションで、「Current Operation」フィールドに「Rebuild」が、「Percentage Complete」フィールドに RAID 再構築の完了割合が表示されます。

再構築中は、新しい交換用ハードディスクのステータスが「Rebuilding」と表示されます。

再構築が完了するまでに 1 ～ 2 時間かかります。必要な時間は、ディスクのサイズに応じて異なります。

障害が発生した RAID ディスクの交換が完了すると、論理ドライブおよび新しい物理ディスクのステータスが両方とも「OK」かつ「Online」と表示されます。

Linux ソフトウェア RAID で再起動を 1 回行って、障害が発生した RAID ディスクを交換する

次の特定のサーバにおいて障害が発生した RAID ディスクを交換するには、次の手順を実行します。

- MCS-7825-H3
- MCS-7828-H3

ステップ 1　管理者としてコンソールにログインし、CLI コマンド **show hardware** を入力します。

ステップ 2　論理ドライブのステータスを確認します。

- 論理ドライブの状態が Active または Clean の場合、これ以上の処理は必要ありません。
- 論理ドライブの状態が低下している場合は、ステップ 3 で説明されているように物理ディスクのステータスを確認します。

ステップ 3　CLI コマンド **show hardware** を再度入力して、物理ディスク ステータスを確認します。

- 「Removed」という状態の物理ディスクがない場合、これ以上の処理は必要ありません。
- 論理ドライブの状態が低下し、いずれかの物理ディスクに「Removed」という状態が表示されるときは、障害が発生したディスクの LED の色はオレンジか赤になるため、これを手がかりにサーバ上の物理ディスクを特定します。

ステップ 2 を実行して論理 RAID ドライブのステータスを確認してから、ステップ 3 を実行して物理ディスクのステータスを確認する必要があります。

障害が発生したドライブを交換して RAID を再構築するには、ステップ 4 に進みます。

ステップ 4　**utils system shutdown** CLI コマンドを使用して、サーバをシャットダウンします。

ステップ 5　システムをシャットダウンしたあと、障害が発生したディスクを、元のディスクとタイプ、サイズ、および製造元（たとえば、Western Digital）が同じ新しいディスクに置き換えます。

ステップ 6　新しい交換用ディスクがしっかりと挿入されていることを確認します。

ステップ 7　システムを起動します。

ステップ 8　システムの電源を投入したあと、CLI にログインして、CLI コマンド **show hardware** を入力します。

show hardware コマンド出力の Logical Drive セクションで、Current Operation フィールドに Rebuild と表示されます。

再構築中は、新しい交換用ハードディスクのステータスが Spare Rebuilding と表示されます。

再構築が完了するまでに 8 ～ 10 時間かかります。この時間は、ディスクのサイズと I/O 動作によって異なります。

障害が発生した RAID ディスクの交換が完了すると、論理ドライブおよび新しい物理ディスクのステータスが両方とも Clean かつ Active と表示されます。

警告　**障害が発生したディスクが配列内の最初のディスクである場合、パーティションがない空の新しいディスクに交換します。ただし、障害が発生したディスクを、HP RAID を使用して以前に設定したディスクに置き換えると、システムは起動できなくなり、カーネル パニックが発生します。**

再起動を行わないで、障害が発生した RAID ディスクを交換する

次の特定のサーバにおいて障害が発生した RAID ディスクを交換するには、次の手順を実行します。

- MCS-7835-H2
- MCS-7835-I2
- MCS-7845-H2
- MCS-7845-I2
- MCS-7835-I3
- MCS-7845-I3
- DL-380-G6

ステップ 1　管理者としてコンソールにログインし、CLI コマンド **show hardware** を入力します。

ステップ 2　論理ドライブのステータスを確認します。次のいずれかを実行します。

- 論理ドライブのステータスが OK または Optimal である場合は、これ以上の処理は必要ありません。
- 論理ドライブのステータスが OK ではない場合は、ステップ 3 で説明されているように物理ディスクのステータスを確認します。

ステップ 3　CLI コマンド **show hardware** を再度入力して、次のいずれかを実行します。

- 「Failed」というステータスの物理ディスクがない場合、これ以上の処理は必要ありません。
- 論理ドライブのステータスが OK または Optimal ではなく、「Failed」と表示された物理ディスクがある場合は、次のようにサーバ上の物理ディスクを特定します。

障害が発生したディスクの LED の色がオレンジ色または赤色になります。

（注）　ステップ 2 を実行して論理 RAID ドライブのステータスを確認してから、ステップ 3 を実行して物理ディスクのステータスを確認する必要があります。

障害が発生したドライブを交換して RAID を再構築するには、ステップ 4 に進みます。

ステップ 4　障害が発生したディスクをスロットから取り外します。

ステップ 5　**show hardware** CLI コマンドを入力して、現在の物理ディスク数が報告されることを確認します。

報告される内容は、次のとおりです。

- 7835 クラスのサーバでは、**show hardware** CLI コマンド出力に 1 つの物理ディスクだけが報告されます。
- 7845 クラスのサーバでは、**show hardware** CLI コマンド出力に 3 つの物理ディスクだけが報告されます。

ステップ 6　障害が発生したディスクが設置されていた空きスロットに、元のディスクと同じタイプ、同じ製造業者、同じサイズの新しいディスクを装着します。たとえば、Western Digital 社のディスクを装着します。

ステップ 7　新しい交換用ディスクがしっかりと挿入されていることを確認します。

ステップ 8　**show hardware** CLI コマンドを実行して、新しく挿入された物理ディスクが検出されることを確認します。

報告される内容は、次のとおりです。

- 7835 クラスのサーバでは、**show hardware** CLI コマンド出力に 2 つの物理ディスクだけが報告されます。
- 7845 クラスのサーバでは、**show hardware** CLI コマンド出力に 4 つの物理ディスクだけが報告されます。

ステップ 9　報告されるディスク数が正しくない場合は、新しいディスクを取り外し、ステップ 5 からやり直してください。

ステップ 10　CLI コマンド **show hardware** を入力して、RAID ステータスを確認します。再構築の完了割合が表示されます。

再構築が完了するまでに 1 ～ 2 時間かかります。必要な時間は、ディスクのサイズに応じて異なります。

障害が発生した RAID ディスクの交換が完了すると、論理ドライブおよび新しい物理ディスクのステータスが両方とも「OK」かつ「Online」と表示されます。