



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

Release 6.0(1)

**【注意】この文書はお客様の便宜のために作成された参考和訳であり、お客様とシスコシステムズとの間の契約を構成するものではありません。正式な契約条件は、弊社担当者、または弊社販売パートナーにご確認ください。**

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。見当たらない場合には、代理店にご連絡ください。

シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB (University of California, Berkeley) パブリック ドメイン パーミッションとして、UCB が開発したプログラムを最適化したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、すべてのマニュアルおよび上記各社のソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記各社は、商品性や特定の目的への適合性、権利を侵害しないことに関する、または取り扱い、使用、または取り引きによって発生する、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその代理店は、このマニュアルの使用またはこのマニュアルを使用できないことによって起こる制約、利益の損失、データの損傷など間接的で偶発的に起こる特殊な損害のあらゆる可能性がシスコまたは代理店に知られていても、それらに対する責任を一切負いかねます。

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0612R)

*Cisco Unified Communications Manager* **トラブルシューティングガイド**  
Copyright © 2002-2006 Cisco Systems, Inc.  
All rights reserved.



## CONTENTS

<b>このマニュアルについて</b>	<b>xi</b>
目的	xii
対象読者	xii
マニュアルの構成	xiii
関連マニュアル	xiv
表記法	xiv
技術情報の入手方法、サポートの利用方法、およびセキュリティ ガイドライン	xvi
シスコ製品のセキュリティの概要	xvi

---

### CHAPTER 1

<b>トラブルシューティングの概要</b>	<b>1-1</b>
Cisco Unified Serviceability	1-2
Cisco Unified Communications オペレーティング システムの管理ページ	1-2
一般的な問題解決モデル	1-3
ネットワーク障害への事前準備	1-4
その他の情報	1-4

---

### CHAPTER 2

<b>トラブルシューティング ツール</b>	<b>2-1</b>
Cisco Unified Serviceability トラブルシューティング ツール	2-2
コマンドライン インターフェイス	2-3
CiscoWorks2000	2-3
システム ログの管理	2-3
シスコ検出プロトコル (CDP) のサポート	2-4
簡易ネットワーク管理プロトコルのサポート	2-4
スニファ トレース	2-5
デバッグ	2-5
Cisco Secure Telnet	2-6
パケット キャプチャ	2-6
パケット キャプチャの概要	2-6
パケット キャプチャ設定のチェックリスト	2-7
Standard Packet Sniffer Users グループへのエンド ユーザの追加	2-7
パケット キャプチャのサービス パラメータの設定	2-8
電話の設定 (Phone Configuration) ウィンドウでのパケット キャプチャの設定	2-9

ゲートウェイの設定 ( Gateway Configuration ) ウィンドウおよびトランクの設定 ( Trunk Configuration ) ウィンドウでのパケット キャプチャの設定 2-10

パケット キャプチャの設定値 2-11

キャプチャしたパケットの分析 2-12

一般的なトラブルシューティングの作業、ツール、およびコマンド 2-13

トラブルシューティングのヒント 2-16

Cisco Unified Communications Manager サービスが動作していることの確認 2-18

CHAPTER 3

**Cisco Unified Communications Manager システムの問題 3-1**

応答しない Cisco Unified Communications Manager システム 3-2

    Cisco Unified Communications Manager システムが応答を停止する 3-2

    Cisco Unified Communications Manager の管理ページが表示されない 3-3

    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 3-3

    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 3-4

    表示する権限がない 3-4

    Cisco Unified Communications Manager でのユーザの表示または追加に関する問題 3-4

    名前からアドレスへの解決の失敗 3-5

    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 3-6

    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 3-6

パブリッシャとサブスクリバの間で複製が失敗する 3-8

サーバの応答が遅い 3-9

JTAPI サブシステムの起動に関する問題 3-9

    JTAPI サブシステムが OUT\_OF\_SERVICE である 3-9

        MIVR-SS\_TEL-4-ModuleRunTimeFailure 3-10

        MIVR-SS\_TEL-1-ModuleRunTimeFailure 3-12

    JTAPI サブシステムが PARTIAL\_SERVICE である 3-13

セキュリティの問題 3-14

    セキュリティ アラーム 3-14

    セキュリティ パフォーマンス モニタ カウンタ 3-14

    セキュリティ ログおよびトレース ファイルの確認 3-16

    証明書の問題 3-16

    CTL セキュリティ トークンのトラブルシューティング 3-16

        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 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	3-17
CAPF のトラブルシューティング	3-17
電話機での認証文字列のトラブルシューティング	3-17
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	3-18
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	3-18
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	3-18
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	3-18
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	3-18
パケット キャプチャの使用方法	3-18
CAPF エラー コード	3-19

## CHAPTER 4

**デバイスの問題** 4-1

音声品質	4-2
音声の損失または歪み	4-2
Cisco Unified IP Phone による音声問題の解決	4-4
エコー	4-5
単方向音声または無音声	4-6
コーデックとリージョンの不一致	4-11
ロケーションと帯域幅	4-12
電話機の問題	4-13
電話機のリセット	4-13
ドロップされたコール	4-14
電話機が登録されない	4-14
ゲートウェイの問題	4-15
ゲートウェイのリオーダー音	4-15
ゲートウェイの登録障害	4-15
ゲートキーパーの問題	4-21
アドミッション拒否	4-21
登録拒否	4-21
Restart_Ack に Channel IE が含まれていない場合に B チャンネルがロックされたままになる	4-22

## CHAPTER 5

**ダイヤル プランとルーティングの問題** 5-1

ルート パーティションとコーリング サーチ スペース	5-1
グループ ピックアップ設定	5-4
ダイヤル プランの問題	5-5

番号をダイヤルするときの問題 5-5  
 安全なダイヤル プラン 5-6

CHAPTER 6

**Cisco Unified Communications Manager サービスの問題 6-1**

使用可能な会議ブリッジがない 6-1  
 ハードウェア トランスコーダが期待どおりに機能しない 6-3  
 確立されたコールで補助的なサービスが使用できない 6-5

CHAPTER 7

**ボイス メッセージの問題 7-1**

30 秒経過するとボイス メッセージが停止する 7-2  
 Cisco Unity がロール オーバーせずにビジー音が聞こえる 7-2  
 ボイス メッセージ システムに転送されたコールが Cisco Unity に対する直接コールとして処理される 7-3  
 管理者アカウントが Cisco Unity サブスクライバに関連付けられていない 7-4

CHAPTER 8

**機能およびサービスのトラブルシューティング 8-1**

割り込みのトラブルシューティング 8-2  
 コール パークのトラブルシューティング 8-3  
 Cisco Call Back のトラブルシューティング 8-3  
     Cisco Call Back の使用方法に関する問題 8-3  
         呼び出し音が鳴る前にユーザが折返しソフトキーを押した 8-3  
         折返しソフトキーを押してから、コール バックが発生する前に、ユーザが電話機のケーブルを抜くか、電話機をリセットした 8-4  
         発信者が、電話機がリセットされる前の使用可能通知を見逃した。置換 / 保持画面に、使用可能通知が発生したことが明示されない 8-4  
     Cisco Call Back のエラー メッセージ 8-5  
     Cisco Call Back のログ ファイルの場所 8-5  
 Cisco エクステンション モビリティのトラブルシューティング 8-6  
     Cisco エクステンション モビリティの一般的な問題のトラブルシューティング 8-6  
     Cisco エクステンション モビリティのエラー メッセージのトラブルシューティング 8-7  
 Cisco Unified Communications Manager Assistant のトラブルシューティング 8-9  
     IPMAConsoleInstall.jsp で「HTTP Status 503—This Application is Not Currently Available」エラーが表示される 8-10  
     IPMAConsoleInstall.jsp で「No Page Found Error」エラーが表示される 8-10  
     Exception: java.lang.ClassNotFoundException: InstallerApplet.class 8-11  
     ダウンロードによる Microsoft 仮想マシンの自動インストールが利用できなくなった 8-11  
     ユーザ認証が失敗する 8-12

アシスタント コンソールで「システムエラーが発生しました。システム管理者にお問い合わせください」エラーが表示される	8-12
アシスタント コンソールで「Cisco Unified Communications Manager Assistant サービスにアクセスできません。しばらくしてから再試行してください」エラーが表示される	8-13
フィルタリングをオンまたはオフにするとコールがルーティングされない	8-14
Cisco IP Manager Assistant サービスが初期化できない	8-15
発信側にリオーダー音が聞こえる	8-16
マネージャがログアウトしてもサービスが動作している	8-16
アシスタントのプロキシ回線上で鳴っているコールをマネージャが代行受信できない	8-17
Cisco IP Manager Assistant サービスがダウンしているときにマネージャの電話にコールできない	8-17
Cisco Unified Communications Manager Attendant Console のトラブルシューティング	8-19
テレフォニーの初期化のエラー	8-19
テレフォニーの初期化の失敗	8-19
コール制御の初期化の失敗	8-20
アテンダントがサーバにアクセスできないというエラー メッセージの表示	8-21
コールの発信と受信に関する問題	8-22
パイロット ポイントにコールを発信できない	8-22
アップグレード後にファースト ビジー シグナルを受信する	8-22
回線が使用できない	8-23
電話機の回線が使用不可になる	8-24
ディレクトリの問題	8-24
ボイス メッセージの問題	8-25
Cisco Unified Communications Manager Attendant Console インターフェイスを使用する際の問題	8-26
Cisco Unified Communications Manager Attendant Console インターフェイスにアクセスできない	8-26
Cisco Unified Communications Manager Attendant Console サーバと通信できない	8-26
テキストが不適切な言語で表示される	8-27
Unicode 言語で検索できない	8-27
短縮ダイヤル ウィンドウとディレクトリ ウィンドウで回線状態が正しく表示されない	8-28
電話番号の回線状態が不明と表示される	8-28
Cisco Unified Communications Manager Serviceability が JTAPI ログを生成しない	8-28
サーバ ログの収集	8-29

Cisco Unified Communications Manager Attendant Console のパフォーマンス モニタ カウンタ	8-29
Cisco Web Dialer のトラブルシューティング	8-30
認証エラー	8-30
サービスが一時的に使用できない	8-30
ディレクトリサービスがダウンしている	8-31
Cisco CTIManager がダウンしている	8-31
セッションの期限切れ、再ログイン	8-31
ユーザがログインしているデバイスがない	8-32
デバイス / 回線が開けない	8-32
転送先に到達できない	8-32
ダイレクト コール パークのトラブルシューティング	8-33
即時転送のトラブルシューティング	8-35
キーがアクティブではありません	8-35
一時エラー発生	8-35
話中	8-35

APPENDIX A

**TAC への問い合わせ** A-1

必要な情報	A-2
必要な予備情報	A-2
ネットワーク レイアウト	A-2
問題の説明	A-3
一般的な情報	A-3
オンラインの利用	A-4
Cisco Live!	A-4
リモート アクセス	A-4
Cisco Secure Telnet	A-5
ファイアウォール保護	A-5
Cisco Secure Telnet の設計	A-5
Cisco Secure Telnet の構造	A-6

APPENDIX B

**ケース スタディ : Cisco Unified IP Phone コールのトラブルシューティング** B-1

クラスタ内 Cisco Unified IP Phone コールのトラブルシューティング	B-2
トポロジの例	B-2
Cisco Unified IP Phone の初期化プロセス	B-3
Cisco Unified Communications Manager の初期化プロセス	B-3
自己起動プロセス	B-4
Cisco Unified Communications Manager の登録プロセス	B-6
Cisco Unified Communications Manager の KeepAlive プロセス	B-6

Cisco Unified Communications Manager のクラスタ内コール フローのトレース	B-7
クラスタ間 Cisco Unified IP Phone コールのトラブルシューティング	B-11
トポロジの例	B-11
クラスタ間 H.323 通信	B-11
コール フローのトレース	B-11
コール フローの失敗	B-12

## APPENDIX C

**ケース スタディ : Cisco Unified IP Phone と Cisco IOS Gateway 間のコールの  
トラブルシューティング** C-1

コール フローのトレース	C-2
Cisco IOS Gatekeeper のデバッグ メッセージと表示コマンド	C-5
Cisco IOS Gateway のデバッグ メッセージと表示コマンド	C-6
T1/PRI インターフェイスを使用する Cisco IOS Gateway	C-10
T1/CAS インターフェイスを使用する Cisco IOS Gateway	C-11

## INDEX

**索引**





## このマニュアルについて

---

ここでは、このマニュアルの目的、対象読者、構成、および表記法、そして関連資料の入手方法について説明します。

次のトピックについて取り上げます。

- [目的 \(P.xii\)](#)
- [対象読者 \(P.xii\)](#)
- [マニュアルの構成 \(P.xiii\)](#)
- [関連マニュアル \(P.xiv\)](#)
- [表記法 \(P.xiv\)](#)
- [技術情報の入手方法、サポートの利用方法、およびセキュリティ ガイドライン \(P.xvi\)](#)
- [シスコ製品のセキュリティの概要 \(P.xvi\)](#)

## 目的

『Cisco Unified Communications Manager トラブルシューティング ガイド』では、Cisco Unified Communications Manager のトラブルシューティングの手順について説明しています。



(注) このバージョンの『Cisco Unified Communications Manager トラブルシューティング ガイド』の情報は、Cisco Unified Communications Manager ソフトウェアの以前のリリースに適用されない場合があります。

このマニュアルは、Cisco Unified Communications Manager システムで発生する可能性のあるすべてのトラブル事象を網羅しているわけではなく、Cisco Technical Assistance Center (TAC) で頻繁に扱っているトラブル事象やニュースグループから頻繁に問い合わせのある質問を重点的に取り上げています。

## 対象読者

『Cisco Unified Communications Manager トラブルシューティング ガイド』は、企業の管理者および従業員のために Cisco Unified Communications Manager システムの管理を担当するネットワーク管理者を対象としています。テレフォニーおよび IP ネットワーキング テクノロジーに関する知識が必要です。

## マニュアルの構成

表 1 は、このマニュアルの構成を示しています。

表 1 このマニュアルの構成

章とタイトル	説明
第 1 章「トラブルシューティングの概要」	Cisco Unified Communications Manager のトラブルシューティングに利用できるツールとリソースの概要を説明します。
第 2 章「トラブルシューティングツール」	Cisco Unified Communications Manager の設定、監視、およびトラブルシューティングに使用できるツールとユーティリティについて説明し、同じデータを何度もテストしたり再収集したりするのを避けるために情報収集に関する一般的なガイドラインを示します。
第 3 章「Cisco Unified Communications Manager システムの問題」	Cisco Unified Communications Manager システムに関連する最も一般的な問題の解決方法について説明します。
第 4 章「デバイスの問題」	IP Phone とゲートウェイに関連する最も一般的な問題の解決方法について説明します。
第 5 章「ダイヤルプランとルーティングの問題」	ダイヤルプラン、ルートパーティション、およびコーリングサーチスペースに関連する最も一般的な問題の解決方法について説明します。
第 6 章「Cisco Unified Communications Manager サービスの問題」	会議ブリッジやメディアターミネーションポイントなどのサービスに関連する最も一般的な問題の解決方法について説明します。
第 7 章「ボイスメッセージの問題」	ボイスメッセージに関連する最も一般的な問題の解決方法について説明します。
第 8 章「機能およびサービスのトラブルシューティング」	Cisco Unified Communications Manager の機能およびサービスに関する一般的な問題の解決方法について説明します。
付録 A「TAC への問い合わせ」	TAC に問い合わせを行う際に必要となる情報について説明します。
付録 B「ケーススタディ：Cisco Unified IP Phone コールのトラブルシューティング」	同一クラスタ内にある 2 台の Cisco Unified IP Phone 間のコールフローについて詳細に説明します。
付録 C「ケーススタディ：Cisco Unified IP Phone と Cisco IOS Gateway 間のコールのトラブルシューティング」	ローカル PBX または Public Switched Telephone Network (PSTN; 公衆電話交換網) に接続された電話機に Cisco IOS Gateway を介してコールを発信する Cisco Unified IP Phone について説明します。

## 関連マニュアル

Cisco IP Telephony 関連のアプリケーションと製品の詳細については、『*Cisco Unified Communications Manager Documentation Guide*』を参照してください。次の URL はドキュメント ガイドへのパスの例を示しています。

[http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_callmg/<リリース番号>/doc\\_gd/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/<リリース番号>/doc_gd/index.htm)

Cisco Unity に関連するマニュアルについては、次の URL を参照してください。

[http://www.cisco.com/en/US/products/sw/voicesw/ps2237/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/voicesw/ps2237/tsd_products_support_series_home.html)

日本語版マニュアルを参照する場合は、次の URL にアクセスしてください。

[http://www.cisco.com/japanese/warp/public/3/jp/service/manual\\_j/index\\_ipt.shtml](http://www.cisco.com/japanese/warp/public/3/jp/service/manual_j/index_ipt.shtml)

## 表記法

このマニュアルは、次の表記法を使用しています。

表記法	説明
太字	コマンドおよびキーワードは、太字で示しています。
イタリック体	ユーザが値を指定する引数は、イタリック体で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{ x y z }	必ずどれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[ x y z ]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
ストリング	引用符を付けない一組の文字。ストリングの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてストリングとみなされます。
screen フォント	システムが表示する端末セッションおよび情報は、screen フォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
イタリック体の screen フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
< >	パスワードのように出力されない文字は、かぎカッコで囲んで示しています。

(注)は、次のように表しています。



(注)

「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

ワンポイントアドバイスは、次のように表しています。



ワンポイント・アドバイス

時間を節約する方法です。ここに紹介している方法で作業を行うと、時間を短縮できます。

ヒントは、次のように表しています。



ヒント

便利なヒントです。

注意は、次のように表しています。



注意

「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

警告は、次のように表しています。



警告

「危険」の意味です。人身事故を予防するための注意事項が記述されています。機器の作業を行うときは、電気回路の危険性および一般的な事故防止対策に十分注意してください。

## 技術情報の入手方法、サポートの利用方法、およびセキュリティ ガイドライン

技術情報の入手、サポートの利用、技術情報に関するフィードバックの提供、セキュリティ ガイドライン、推奨するエイリアスおよび一般的なシスコのマニュアルに関する情報は、月刊の『*What's New in Cisco Product Documentation*』を参照してください。ここでは、新規および改訂版のシスコの技術マニュアルもすべて記載されています。次の URL からアクセスできます。

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

## シスコ製品のセキュリティの概要

本製品には暗号化機能が備わっており、輸入、輸出、配布および使用に適用される米国および他の国での法律を順守するものとします。シスコの暗号化製品を譲渡された第三者は、その暗号化技術の輸入、輸出、配布、および使用を許可されたわけではありません。輸入業者、輸出業者、販売業者、およびユーザは、米国および他の国での法律を順守する責任があります。本製品を使用するにあたっては、関係法令の順守に同意する必要があります。米国および他の国の法律を順守できない場合は、本製品を至急送り返してください。

シスコの暗号化製品に適用される米国の法律の概要については、次の URL で参照できます。

<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

何かご不明な点があれば、[export@cisco.com](mailto:export@cisco.com) まで電子メールを送信してください。



# トラブルシューティングの概要

---

この章では、Cisco Unified Communications Manager のトラブルシューティングで必要となる背景情報や使用できるリソースについて説明します。

この章では、次のトピックについて取り上げます。

- [Cisco Unified Serviceability \(P.1-2\)](#)
- [Cisco Unified Communications オペレーティング システムの管理ページ \(P.1-2\)](#)
- [一般的な問題解決モデル \(P.1-3\)](#)
- [ネットワーク障害への事前準備 \(P.1-4\)](#)
- [その他の情報 \(P.1-4\)](#)

## Cisco Unified Serviceability

Cisco Unified Communications Manager の Web ベースのトラブルシューティング ツールである Cisco Unified Serviceability は、管理者がシステムの問題をトラブルシューティングできるように次の機能を提供します。

- トラブルシューティングに備えて、Cisco Unified Communications Manager サービスのアラームとイベントを保存し、アラーム メッセージの定義を提供します。
- トラブルシューティングに備えて、Cisco Unified Communications Manager サービスのトレース情報を各種ログ ファイルに保存します。管理者は、トレース情報の設定、収集、および表示を行うことができます。
- Real-Time Monitoring Tool (RTMT) によって、Cisco Unified Communications Manager クラスタ内のコンポーネントの動作をリアルタイムで監視します。
- Cisco Unified Communications Manager CDR Analysis and Reporting (CAR) によって、Quality of Service (QoS; サービス品質)、トラフィック、および課金情報に関するレポートを生成します。
- [Service Activation] ウィンドウでアクティブ化、非アクティブ化、および表示できる機能サービスを提供します。
- 機能サービスとネットワーク サービスを起動および停止するインターフェイスを提供します。
- Cisco Unified Serviceability ツールに関連付けられたレポートをアーカイブします。
- Cisco Unified Communications Manager が SNMP リモート管理およびトラブルシューティングのために管理対象デバイスとして機能できるようにします。
- 1 つのサーバ (またはクラスタ内のすべてのサーバ) 上のログパーティションのディスク使用状況を監視します。

Cisco Unified Serviceability にアクセスするには、Cisco Unified Communications Manager の管理ページで、[ナビゲーション] ドロップダウン リスト ボックスから [Cisco Unified サービスアビリティ] を選択します。Cisco Unified Communications Manager ソフトウェアをインストールすると、Cisco Unified Serviceability が自動的にインストールされて使用できるようになります。

サービスアビリティ ツールの詳細および設定手順については、『Cisco Unified Serviceability アドミニストレーションガイド』を参照してください。

## Cisco Unified Communications オペレーティング システムの管理 ページ

Cisco Unified Communications オペレーティング システムの管理ページでは、Cisco Unified Communications オペレーティング システムを設定および管理するために次の作業を行うことができます。

- ソフトウェアとハードウェアのステータス チェック
- IP アドレスのチェックと更新
- 他のネットワーク デバイスへの ping
- ネットワーク タイム プロトコル サーバの管理
- システム ソフトウェアとオプションのアップグレード
- システムの再起動

サービスアビリティ ツールの詳細および設定手順については、『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。

## 一般的な問題解決モデル

テレフォニーまたは IP ネットワーク環境でトラブルシューティングを行う場合は、症状を見極め、その症状を引き起こしていると考えられるすべての問題を洗い出し、症状がなくなるまで、考えられるそれぞれの問題を体系的に（可能性の高いものから順番に）排除していきます。

次の手順は、問題解決プロセス用のガイドラインを示しています。

- 
- ステップ 1** ネットワークの問題を分析し、問題点を明確に記述します。症状および考えられる原因を明らかにします。
  - ステップ 2** 問題の原因を特定するために役立つファクト（事実）を収集します。
  - ステップ 3** 収集したファクトに基づいて、考えられる原因を検討します。
  - ステップ 4** その原因に基づいて、アクション プランを作成します。最も可能性の高い問題から着手し、1 つの変数だけを操作するプランになるようにします。
  - ステップ 5** アクション プランを実施します。テストして症状が消えたかどうかを確認しながら、各手順を慎重に実行します。
  - ステップ 6** 結果を分析し、問題が解決したかどうかを確認します。問題が解決した場合、プロセスは完了したと見なします。
  - ステップ 7** 問題が解決していない場合は、上記のリストで次に可能性の高い原因に基づいてアクション プランを作成します。[ステップ 4](#) に戻り、問題が解決するまでプロセスを繰り返します。

アクション プランの実施中に何かを変更した場合は、必ずその変更を取り消してください。一度に 1 つの変数だけを変更してください。



- (注)** 一般的な対策（本書で説明しているもの、または環境に応じて独自に考案したもの）をすべて実施しても問題が解決しない場合は、Cisco TAC に連絡してください。

## ネットワーク障害への事前準備

ネットワーク障害が発生したときにその回復を容易にするには、事前準備が重要です。ネットワーク障害への事前準備ができていないかどうかを判断するには、次の質問に教えてください。

- ネットワーク上のすべてのデバイスの物理的な位置および接続方法を示した、インターネットワークの正確な物理および論理マップがありますか。また、ネットワークアドレス、ネットワーク番号、およびサブネットワークを記述した論理マップがありますか。
- ネットワークに実装されているすべてのネットワーク プロトコルのリストと、各プロトコルに関連付けられているネットワーク番号、サブネットワーク、ゾーン、およびエリアのリストがありますか。
- どのプロトコルがルーティングされているか、および各プロトコルについての正確かつ最新の設定情報を知っていますか。
- どのプロトコルがブリッジされているかを知っていますか。そのブリッジにはフィルタが設定されていますか。その設定のコピーはありますか。そのコピーは Cisco Unified Communications Manager に適用できますか。
- インターネットへの接続も含めて、外部ネットワークへのすべての接点を知っていますか。各外部ネットワーク接続について、使用されているルーティング プロトコルを知っていますか。
- 現在の問題とベースラインを比較できるように、通常のネットワーク動作およびパフォーマンスについて組織で文書化されていますか。

これらの質問に対して「はい」と答えることができる場合は、障害から迅速に回復できます。

## その他の情報

IP テレフォニーの各種トピックについては、次のリンクを参照してください。

- Cisco IP Telephony 関連のアプリケーションと製品の詳細については、『Cisco Unified Communications Manager Documentation Guide』を参照してください。次の URL はドキュメント ガイドへのパスの例を示しています。  
[http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_callmg/<リリース番号>/doc\\_gd/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/<リリース番号>/doc_gd/index.htm)
- Cisco Unity に関連するマニュアルについては、次の URL を参照してください。  
[http://www.cisco.com/en/US/products/sw/voicesw/ps2237/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/voicesw/ps2237/tsd_products_support_series_home.html)
- Cisco Emergency Responder に関連するマニュアルについては、次の URL を参照してください。  
<http://www.cisco.com/univercd/cc/td/doc/product/voice/respond/index.htm>
- Cisco Unified IP Phone に関連するマニュアルについては、次の URL を参照してください。  
[http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_ipphon/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/index.htm)
- IP テレフォニー ネットワークの設計とトラブルシューティングについては、  
[www.cisco.com/go/srnd](http://www.cisco.com/go/srnd) から入手できる『Cisco IP テレフォニー ソリューション リファレンス ネットワーク デザイン ガイド』を参照してください。



## トラブルシューティング ツール

---

この章では、Cisco Unified Communications Manager の設定、監視、およびトラブルシューティングに使用するツールとユーティリティについて説明し、同じデータを何度もテストしたり再収集したりすることを避けるために、情報収集に関する一般的なガイドラインを示します。



**(注)** 本書に示す URL サイトの中には、登録ユーザとしてログインしないとアクセスできないものもあります。

---

この章では、次のトピックについて取り上げます。

- [Cisco Unified Serviceability](#) [トラブルシューティング ツール](#) (P.2-2)
- [コマンドライン インターフェイス](#) (P.2-3)
- [CiscoWorks2000](#) (P.2-3)
- [スニファ トレース](#) (P.2-5)
- [デバッグ](#) (P.2-5)
- [Cisco Secure Telnet](#) (P.2-6)
- [パケット キャプチャ](#) (P.2-6)
- [一般的なトラブルシューティングの作業、ツール、およびコマンド](#) (P.2-13)
- [トラブルシューティングのヒント](#) (P.2-16)
- [Cisco Unified Communications Manager サービスが動作していることの確認](#) (P.2-18)

## Cisco Unified Serviceability トラブルシューティングツール

次に示す各種ツールの詳細については、『Cisco Unified Serviceability アドミニストレーション ガイド』を参照してください。これらのツールは、多様な Cisco Unified Communications Manager システムを監視および分析するために、Cisco Unified Serviceability により提供されます。

表 2-1 サービスアビリティ ツール

用語	定義
Real-Time Monitoring Tool (RTMT)	<p>この用語は、Cisco Unified Communications Manager のデバイスおよびパフォーマンスカウンタに関するリアルタイム情報を提供し、管理者がトレースを収集できる、サービスアビリティのプログラムを示します。</p> <p>パフォーマンスカウンタは、システム固有のものも Cisco Unified Communications Manager 固有のものもあります。オブジェクトは、Cisco Unified IP Phone や Cisco Unified Communications Manager System Performance など、特定のデバイスまたは機能に関する同様のカウンタを論理グループにまとめたもので構成されます。カウンタは、システムパフォーマンスのさまざまな側面を測定します。カウンタは、登録されている電話機の数、試行されたコール、進行中のコールなど、統計情報を測定します。</p>
アラーム	<p>管理者は、アラームを使用して、Cisco Unified Communications Manager システムの実行時のステータスや状態を確認します。アラームには、説明や推奨処置など、システムの問題に関する情報が含まれています。</p> <p>管理者は、アラーム定義データベースを検索して、アラーム情報を見つけます。アラーム定義には、アラームの説明および推奨処置が含まれています。</p>
トレース	<p>管理者およびシスコのエンジニアは、トレース ファイルを使用して、Cisco Unified Communications Manager サービスの問題に関する特定の情報を取得します。Cisco Unified Serviceability は、設定されているトレース情報をトレース ログ ファイルに送信します。SDI と SDL という2つのタイプのトレース ログ ファイルがあります。</p> <p>すべてのサービスには、デフォルトのトレース ログ ファイルが含まれています。システムは、サービスからの system diagnostic interface (SDI) 情報をトレースし、実行時のイベントおよびトレースをログ ファイルに記録します。</p> <p>SDL トレース ログ ファイルには、Cisco CallManager や Cisco CTIManager などのサービスからのコール処理情報が含まれています。システムは、コールの signal distribution layer (SDL) をトレースし、状態遷移をログ ファイルに記録します。</p> <p> <b>(注)</b> ほとんどの場合は、Cisco Technical Assistance Center (TAC) から要求された場合にだけ、SDL トレースを収集します。</p>
品質レポート ツール	<p>この用語は、Cisco Unified Serviceability に含まれる、音声品質および一般的な問題を報告するユーティリティを示します。</p>

## コマンドライン インターフェイス

基本的なメンテナンスおよび障害からの回復を目的として、Cisco Unified Communications Manager システムにアクセスするには、Command Line Interface (CLI; コマンドライン インターフェイス) を使用します。システムには、物理的に接続された端末 (システム モニタおよびキーボード) を使用してアクセスすることも、SSH セッションを実行してアクセスすることもできます。

インストール中に、アカウント名とパスワードが作成されます。パスワードはインストール後に変更できますが、アカウント名は一切変更できません。

コマンドは、システムで何らかの機能を実行するための、テキストによる命令文です。コマンドは、スタンドアロンで実行することも、必須または省略可能な引数やオプションを指定して実行することもできます。

レベルは、コマンドの集合で構成されます。たとえば、*show* はレベルを表し、*show status* はコマンドを表します。レベルおよびコマンドには、それぞれ特権レベルも関連付けられています。ユーザがコマンドを実行できるのは、十分な特権レベルを持っている場合に限られます。

Cisco Unified Communications Manager の CLI コマンド セットの詳細については、『*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。

## CiscoWorks2000

CiscoWorks2000 は、Cisco Unified Communications Manager を含め、すべてのシスコ デバイスに最適なネットワーク管理システムとして機能します。CiscoWorks2000 は Cisco Unified Communications Manager にバンドルされていないため、別途購入する必要があります。次のツールを CiscoWorks2000 と併用すると、リモート サービスアビリティが得られます。

- システム ログの管理
- シスコ検出プロトコル (CDP) のサポート
- 簡易ネットワーク管理プロトコルのサポート

CiscoWorks2000 の詳細については、次の URL にある CiscoWorks2000 のマニュアルを参照してください。

<http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/index.htm>

## システム ログの管理

システム ログ管理プロセスは他のネットワーク管理システムに適合させることもできますが、シスコ デバイスからの Syslog メッセージの管理には、CiscoWorks2000 Resource Manager Essentials に付属の Cisco Syslog Analysis が最適です。

Cisco Syslog Analyzer は、Cisco Syslog Analysis のコンポーネントとして機能し、複数のアプリケーションのシステム ログの共通ストレージおよび分析を提供します。もう 1 つの主要コンポーネントである Syslog Analyzer Collector は、Cisco Unified Communications Manager サーバからログメッセージを収集します。

これら 2 つのシスコ アプリケーションは連動し、シスコ ユニファイド コミュニケーション ソリューション用の集中システム ログGING サービスを提供します。

## シスコ検出プロトコル (CDP) のサポート

シスコ検出プロトコル(CDP)のサポートにより、CiscoWorks2000 で、Cisco Unified Communications Manager サーバを検出および管理できます。

## 簡易ネットワーク管理プロトコルのサポート

Network Management System (NMS; ネットワーク管理システム) は、業界標準のインターフェイスである SNMP を使用して、ネットワーク デバイス間で管理情報を交換します。TCP/IP プロトコルスイートの一部である SNMP を使用すると、管理者はリモートでネットワーク パフォーマンスを管理し、ネットワークの問題を検出して解決し、ネットワークの拡張を計画できます。

SNMP で管理されるネットワークは、管理対象デバイス、エージェント、およびネットワーク管理システムという 3 つの主要コンポーネントで構成されます。

- 管理対象デバイスとは、SNMP エージェントを含み、管理対象ネットワークに常駐するネットワーク ノードです。管理対象デバイスは、管理情報を収集して格納し、SNMP を使用してその情報を使用できるようにします。
- エージェントは、ネットワーク管理ソフトウェアとして、管理対象デバイスに常駐します。エージェントは、管理情報をローカルで認識し、その情報を SNMP と互換性のある形式に変換します。
- ネットワーク管理システムは、SNMP 管理アプリケーションと、そのアプリケーションを実行するコンピュータで構成されます。NMS は、管理対象デバイスを監視および制御するアプリケーションを実行します。NMS は、ネットワーク管理に必要な処理リソースおよびメモリ リソースの大部分を提供します。次の NMS は Cisco Unified Communications Manager と互換性があります。
  - CiscoWorks2000
  - HP OpenView
  - SNMP および Cisco Unified Communications Manager SNMP インターフェイスをサポートするサードパーティ製アプリケーション

## スニファトレース

通常は、VLAN をスパンするように設定された Catalyst ポートまたはトラブル情報を含むポート (CatOS、Cat6K-IOS、XL-IOS) 上で、ラップトップ、またはスニファを装備した他のデバイスを接続することにより、スニファトレースを収集します。ポートが空いていない場合は、スイッチとデバイス間に挿入されているハブ上で、スニファを装備したデバイスを接続します。



### ヒント

TAC では Sniffer Pro ソフトウェアが広く使用されているため、TAC エンジニアがトレースを簡単に読み取って解釈できるように、このソフトウェアを使用することをお勧めします。

関係するすべての機器 (IP Phone、ゲートウェイ、Cisco Unified Communications Manager など) の IP アドレスと MAC アドレスを用意しておいてください。

## デバッグ

`debug` 特権 EXEC コマンドからの出力には、プロトコルステータスやネットワークアクティビティ全般に関連するさまざまなインターネットワーキングイベントについての診断情報が記載されています。

デバッグ出力をファイルに取り込むことができるように、ターミナルエミュレータソフトウェア (ハイパーターミナルなど) を設定します。ハイパーターミナルでは、[転送] をクリックし、[テキストのキャプチャ] をクリックして、適切なオプションを選択します。

IOS 音声ゲートウェイのデバッグを実行する前に、ゲートウェイ上で `service timestamps debug datetime msec` がグローバルに設定されていることを確認します。



### (注)

営業時間中にライブ環境でデバッグを収集しないでください。

営業時間外にデバッグを収集することをお勧めします。ライブ環境でデバッグを収集する必要がある場合は、`no logging console` および `logging buffered` を設定します。デバッグを収集するには、`show log` を使用します。

デバッグは長くなることがあるため、コンソールポート (デフォルト `logging console`) またはバッファ (`logging buffer`) でデバッグを直接収集します。Telnet セッションを介してデバッグを収集すると、デバイスのパフォーマンスが低下して、デバッグが不完全となり、デバッグを再収集する必要が生じることがあります。

デバッグを停止するには、`no debug all` または `undebug all` コマンドを使用します。`show debug` コマンドを使用して、デバッグがオフになっていることを確認してください。

## Cisco Secure Telnet

Cisco Secure Telnet を使用すると、Cisco Service Engineer (CSE; シスコ サービス エンジニア) は、ファイアウォールを介してお客様のサイトの Cisco Unified Communications Manager ノードに透過的にアクセスできます。Cisco Secure Telnet は、強力な暗号化を使用して、シスコシステムズ内の特別な Telnet クライアントを、お客様のファイアウォールの内側にある Telnet デーモンに接続できます。このセキュアな接続により、ファイアウォールを変更せずに、お客様の Cisco Unified Communications Manager ノードの監視およびトラブルシューティングをリモートで行うことができます。



(注)

シスコでは、お客様の承諾を得た場合にだけこのサービスを提供します。作業を開始する場合は、お客様のサイトでネットワーク管理者のご協力をお願いしています。

## パケット キャプチャ

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 \(P.2-6\)](#)
- [パケット キャプチャ設定のチェックリスト \(P.2-7\)](#)
- [Standard Packet Sniffer Users グループへのエンド ユーザの追加 \(P.2-7\)](#)
- [パケット キャプチャのサービス パラメータの設定 \(P.2-8\)](#)
- [電話の設定 \(Phone Configuration\) ウィンドウでのパケット キャプチャの設定 \(P.2-9\)](#)
- [ゲートウェイの設定 \(Gateway Configuration\) ウィンドウおよびトランクの設定 \(Trunk Configuration\) ウィンドウでのパケット キャプチャの設定 \(P.2-10\)](#)
- [パケット キャプチャの設定値 \(P.2-11\)](#)
- [キャプチャしたパケットの分析 \(P.2-12\)](#)

## パケット キャプチャの概要

メディアや TCP パケットをスニフリ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、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 Unified 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。
- デバイス間で交換される Secure Real Time Protocol (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。



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。

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。

## パケットキャプチャ設定のチェックリスト

必要なデータを抽出し、分析するには、表 2-2 に示す作業を行います。

表 2-2 パケットキャプチャ設定のチェックリスト

設定のステップ	手順およびトピック
<b>ステップ 1</b>	エンド ユーザを Standard Packet Sniffer Users グループに追加します。
<b>ステップ 2</b>	Cisco Unified Communications Manager の管理ページの[ サービスパラメータ設定 ( Service Parameter Configuration ) ]ウィンドウで、パケットキャプチャのサービスパラメータを設定します。たとえば、Packet Capture Enable サービスパラメータを設定します。
<b>ステップ 3</b>	[ 電話の設定 ( Phone Configuration ) ] [ ゲートウェイの設定 ( Gateway Configuration ) ]、または [ トランクの設定 ( Trunk Configuration ) ] のウィンドウで、デバイスごとのパケットキャプチャの設定を行います。   <b>(注)</b> パケットキャプチャは、複数のデバイスで同時には有効にしないことを強くお勧めします。この作業によって、ネットワークに含まれている CPU の使用率が上昇する可能性があるためです。
<b>ステップ 4</b>	該当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。
<b>ステップ 5</b>	パケットをキャプチャしたら、Packet Capture Enable サービスパラメータを False に設定します。
<b>ステップ 6</b>	パケットの分析に必要なファイルを収集します。
<b>ステップ 7</b>	Cisco Technical Assistance Center ( TAC ) がパケットを分析します。この作業については、TAC に直接ご依頼ください。

## Standard Packet Sniffer Users グループへのエンドユーザの追加

Standard Packet Sniffer Users グループに所属するユーザは、パケットキャプチャをサポートしているデバイスについて、[ パケットキャプチャモード ( Packet Capture Mode ) ] と [ パケットキャプチャ時間 ( Packet Capture Duration ) ] を設定できます。ユーザが Standard Packet Sniffer Users グループに含まれていない場合、そのユーザはパケットキャプチャを開始できません。

次の手順では、エンドユーザを Standard Packet Sniffer Users グループに追加する方法について説明します。この手順では、『Cisco Unified Communications Manager アドミニストレーションガイド』の説明に従って、Cisco Unified Communications Manager の管理ページでエンドユーザを設定したことを前提としています。

### 手順

- ステップ 1** 『Cisco Unified Communications Manager アドミニストレーションガイド』の説明に従って、ユーザグループを検索します。

## ■ パケットキャプチャ

- ステップ2** [ ユーザグループの検索と一覧表示 (Find and List User Groups) ] ウィンドウが表示されたら、[ Standard Packet Sniffer Users ]リンクをクリックします。
- ステップ3** [ グループにエンドユーザを追加 ]ボタンをクリックします。
- ステップ4** 『Cisco Unified Communications Manager アドミニストレーション ガイド』の説明に従って、エンドユーザを追加します。

## パケットキャプチャの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 Unified Communications Manager の管理ページで、[ システム ]>[ サービスパラメータ ]を選択します。
- ステップ2** [ サーバ ( Server ) ]ドロップダウン リスト ボックスから、Cisco Unified CallManager サービスをアクティブにした Active サーバを選択します。
- ステップ3** [ サービス ( Service ) ]ドロップダウン リスト ボックスから、Cisco CallManager ( Active ) サービスを選択します。
- ステップ4** TLS Packet Capture Configurations ペインまでスクロールして、パケットキャプチャを設定します。



### ヒント

サービスパラメータについては、ウィンドウに表示されているパラメータ名または疑問符をクリックしてください。



### (注)

パケットキャプチャを実行するには、Packet Capture Enable サービスパラメータを True に設定する必要があります。

- ステップ5** 変更内容を有効にするには、[ 保存 ]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行する場合は、次のいずれかの項を参照してください。
- [電話の設定 \( Phone Configuration \) ウィンドウでのパケットキャプチャの設定 \( P.2-9 \)](#)
  - [ゲートウェイの設定 \( Gateway Configuration \) ウィンドウおよびトランクの設定 \( Trunk Configuration \) ウィンドウでのパケットキャプチャの設定 \( P.2-10 \)](#)

## 電話の設定 ( Phone Configuration ) ウィンドウでのパケット キャプチャの設定

[ サービスパラメータ設定 ( Service Parameter Configuration ) ] ウィンドウでパケット キャプチャを有効にしたら、Cisco Unified Communications Manager の管理ページの [ 電話の設定 ( 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ことができます。

電話機ごとに、パケット キャプチャを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 キャプチャは、複数の電話機で同時には有効にしないことを強くお勧めします。この作業によって、ネットワークに含まれている CPU の使用率が上昇する可能性があるためです。

パケットをキャプチャしない場合、または作業が完了した場合は、Packet Capture Enable サービスパラメータを False に設定します。

電話機のパケット キャプチャを設定するには、次の手順を実行します。

### 手順

- ステップ 1** パケット キャプチャを設定する前に、[P.2-7 の「パケット キャプチャ設定のチェックリスト」](#)を参照してください。
- ステップ 2** 『Cisco Unified Communications Manager アドミニストレーションガイド』の説明に従って、SIP 電話機または SCCP 電話機を検索します。
- ステップ 3** [ 電話の設定 ( Phone Configuration ) ] ウィンドウが表示されたら、[表 2-3](#) の説明に従って、トラブルシューティングの設定を行います。
- ステップ 4** 設定が完了したら、[ 保存 ] をクリックします。
- ステップ 5** [ デバイスリセット ( Device Reset ) ] ダイアログボックスで、[ リスタート ] をクリックします。



### ヒント

Cisco Unified Communications Manager の管理ページからデバイスをリセットするように求められますが、パケットをキャプチャするためにデバイスをリセットする必要はありません。

### この他の手順

該当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。

パケットをキャプチャしたら、Packet Capture Enable サービスパラメータを False に設定します。

[P.2-12 の「キャプチャしたパケットの分析」](#)を参照してください。

## ゲートウェイの設定 (Gateway Configuration) ウィンドウおよびトランクの設定 (Trunk Configuration) ウィンドウでのパケットキャプチャの設定

次のゲートウェイおよびトランクは、Cisco Unified Communications Manager の管理ページでパケットキャプチャをサポートしています。

- Cisco IOS MGCP ゲートウェイ
- H.323 ゲートウェイ
- H.323 トランク、H.245 トランク、H.225 トランク
- SIP トランク



### ヒント

パケットキャプチャは、複数のデバイスで同時には有効にしないことを強くお勧めします。この作業によって、ネットワークに含まれている CPU の使用率が上昇する可能性があります。

パケットをキャプチャしない場合、または作業が完了した場合は、Packet Capture Enable サービスパラメータを False に設定します。

[ゲートウェイの設定 (Gateway Configuration) ] ウィンドウまたは [トランクの設定 (Trunk Configuration) ] ウィンドウでパケットキャプチャの設定を行うには、次の手順を実行します。

### 手順

**ステップ 1** パケットキャプチャを設定する前に、[P.2-7](#) の「[パケットキャプチャ設定のチェックリスト](#)」を参照してください。

**ステップ 2** 次のいずれかの作業を行います。

- 『Cisco Unified Communications Manager アドミニストレーションガイド』の説明に従って、Cisco IOS MGCP ゲートウェイを検索します。
- 『Cisco Unified Communications Manager アドミニストレーションガイド』の説明に従って、H.323 ゲートウェイを検索します。
- 『Cisco Unified Communications Manager アドミニストレーションガイド』の説明に従って、H.323、H.245、または H.225 トランクを検索します。
- 『Cisco Unified Communications Manager アドミニストレーションガイド』の説明に従って、SIP トランクを検索します。

**ステップ 3** 設定ウィンドウが表示されたら、[パケットキャプチャモード (Packet Capture Mode) ]設定値と [パケットキャプチャ時間 (Packet Capture Duration) ]設定値を確認します。



### ヒント

Cisco IOS MGCP ゲートウェイを見つけたら、Cisco IOS MGCP ゲートウェイ用のポートを『Cisco Unified Communications Manager 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あることを確認します。Cisco IOS MGCP ゲートウェイのパケットキャプチャ設定値は、エンドポイント識別子の [ゲートウェイの設定 (Gateway Configuration) ] ウィンドウに表示されます。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識別子をクリックします。

**ステップ 4** [表 2-3](#) の説明に従って、トラブルシューティングの設定を行います。

**ステップ5** パケットキャプチャを設定したら、[保存]をクリックします。

**ステップ6** [デバイスリセット (Device Reset)]ダイアログボックスで、[リスタート]をクリックします。

**ヒント**

Cisco Unified Communications Manager の管理ページからデバイスをリセットするように求められますが、パケットをキャプチャするためにデバイスをリセットする必要はありません。

**この他の手順**

該当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。

パケットをキャプチャしたら、Packet Capture Enable サービスパラメータを False に設定します。

P.2-12 の「キャプチャしたパケットの分析」を参照してください。

## パケットキャプチャの設定値

[パケットキャプチャモード (Packet Capture Mode)]設定値および[パケットキャプチャ時間 (Packet Capture Duration)]設定値について説明した表 2-3 とともに、次の項も参照してください。

- [電話の設定 \(Phone Configuration\) ウィンドウでのパケットキャプチャの設定 \(P.2-9\)](#)
- [ゲートウェイの設定 \(Gateway Configuration\) ウィンドウおよびトランクの設定 \(Trunk Configuration\) ウィンドウでのパケットキャプチャの設定 \(P.2-10\)](#)

## ■ パケットキャプチャ

表 2-3 パケットキャプチャの設定値

設定値	説明
[パケットキャプチャモード (Packet Capture Mode)]	<p>この設定値は、暗号化のトラブルシューティングを行う場合のみ使用します。パケットキャプチャを実行すると、CPUの使用率が上昇して、コール処理が妨げられる可能性があります。ドロップダウンリストボックスから、次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> <li>• <b>None</b> : このオプションは、パケットキャプチャが発生しないことを示します(デフォルト設定)。パケットキャプチャが完了すると、Cisco Unified Communications Manager は [パケットキャプチャモード (Packet Capture Mode)] を None に設定します。</li> <li>• <b>Batch Processing Mode</b> : Cisco Unified Communications Manager は、復号化された(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、毎日新しい暗号鍵を使用して、新しいファイルを作成します。Cisco Unified Communications Manager はファイルを 7 日間保管し、ファイルを暗号化する鍵も安全な場所に格納します。ファイルの保管先は、PktCap 仮想ディレクトリです。1つのファイルの中に、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、パケットのプロトコル、メッセージの長さ、およびメッセージが保持されます。TAC のデバッグツールでは、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保持している暗号化済みファイルを 1 つのみ要求します。同様に、暗号化されているファイルを復号化するための鍵情報も要求します。</li> </ul> <p> <b>ヒント</b> TAC にお問い合わせいただく前に、該当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。</p>
[パケットキャプチャ時間 (Packet Capture Duration)]	<p>この設定値は、暗号化のトラブルシューティングを行う場合のみ使用します。パケットキャプチャを実行すると、CPUの使用率が上昇して、コール処理が妨げられる可能性があります。</p> <p>このフィールドには、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上限を分単位で指定します。デフォルト設定は 0 で、範囲は 0 ~ 300 分です。</p> <p>パケットキャプチャを開始するには、このフィールドに 0 以外の値を入力します。パケットキャプチャが完了すると、値 0 が表示されます。</p>

## キャプチャしたパケットの分析

Cisco Technical Assistance Center (TAC) は、デバッグツールを使用してパケットを分析します。TAC にお問い合わせいただく前に、該当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てください。次の情報を収集したら、TAC まで直接お問い合わせください。

- パケットキャプチャファイル : <https://<IP アドレスまたはサーバ名>/pktCap/pktCap.jsp?file=mm-dd-yyyy.pkt>。サーバを参照し、西暦年と日付 (mm-dd-yyyy) 別のパケットキャプチャファイルを見つけます。
- ファイルの鍵 : <https://<IP アドレスまたはサーバ名>/pktCap/pktCap.jsp?key=mm-dd-yyyy.pkt>。サーバを参照し、西暦年と日付 (mm-dd-yyyy) 別の鍵を見つけます。
- Standard Packet Sniffer Users グループに所属しているエンドユーザのユーザ名とパスワード。

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。

## 一般的なトラブルシューティングの作業、ツール、およびコマンド

この項は、ルートアクセスが無効になっている Cisco Unified Communications Manager サーバをトラブルシューティングするためのコマンドおよびユーティリティのクイック リファレンスです。表 2-4 に、システムのさまざまな問題をトラブルシューティングするための情報収集に使用できる CLI コマンドおよび GUI 選択オプションの要約を示します。

表 2-4 CLI コマンドおよび GUI 選択オプションの要約

情報	Linux コマンド	サービスアビリティの GUI ツール	CLI コマンド
CPU 使用率	top	RTMT [ View ] タブに移動し、[ Server ]> [ CPU and Memory ] を選択	プロセッサの CPU 使用率： show perf query class Processor プロセスの CPU 使用率(すべてのプロセス): show perf query counter Process "% CPU Time" 個々のプロセスのカウンタの詳細 (CPU 使用率含む): show perf query instance <プロセスのタスク名>
プロセスの状態	ps	RTMT [ View ] タブに移動し、[ Server ]> [ Process ] を選択	show perf query counter Process "Process Status"
ディスクの使用状況	df/du	RTMT [ View ] タブに移動し、[ Server ]> [ Disk Usage ] を選択	show perf query counter Partition "% Used" または show perf query class Partition
メモリ	free	RTMT [ View ] タブに移動し、[ Server ]> [ CPU and Memory ] を選択	show perf query class Memory
ネットワークのステータス	netstats		show network status
サーバのリブート	reboot	サーバのプラットフォームの管理 Web ページにログイン [ Restart ]>[ Current Version ]に移動	utils system restart
トレースとログの収集	Sftp, ftp	RTMT [ Tools ] タブに移動し、[ Trace ]> [ Trace & Log Central ] を選択	ファイル一覧の表示 : file list ファイルのダウンロード : file get ファイル内容の表示 : file view

## ■ 一般的なトラブルシューティングの作業、ツール、およびコマンド

表 2-5 に、一般的な問題と、そのトラブルシューティングに使用するツールのリストを示します。

表 2-5 CLI コマンドおよび GUI 選択オプションによる一般的な問題のトラブルシューティング

作業	GUI ツール	CLI コマンド
データベースにアクセスする。	なし	admin としてログインし、次のいずれかの show コマンドを使用します。 <ul style="list-style-type: none"> <li>show tech database</li> <li>show tech dbinuse</li> <li>show tech dbschema</li> <li>show tech devdefaults</li> <li>show tech gateway</li> <li>show tech locales</li> <li>show tech notify</li> <li>show tech procedures</li> <li>show tech routepatterns</li> <li>show tech routeplan</li> <li>show tech systables</li> <li>show tech table</li> <li>show tech triggers</li> <li>show tech version</li> <li>show tech params*</li> </ul> SQL コマンドを実行するには、run コマンドを使用します。 <ul style="list-style-type: none"> <li>run &lt;SQL コマンド&gt;</li> </ul>
 <p>(注) Log パーティションにあるファイルのみ、削除することができます。</p>	RTMT クライアント アプリケーションを使用して、[ Tools ] タブに移動し、[ Trace & Log Central ]>[ Collect Files ] を選択します。 収集するファイルの選択基準を選択し、[ Delete Files ] オプションのチェックボックスをオンにします。この操作を実行すると、ファイルが PC にダウンロードされ、Cisco Unified Communications Manager サーバ上のファイルは削除されます。	file delete
コア ファイルを表示する。	コア ファイルは表示できませんが、RTMT アプリケーションを使用して [ Trace & Log Central ]>[ Collect Crash Dump ] を選択すると、コア ファイルをダウンロードできます。	Core [ options.. ]
Cisco Unified Communications Manager サーバをリブートする。	サーバ上でプラットフォームの管理ページにログインし、[ Restart ] > [ Current Version ] に移動します。	utils system restart

表 2-5 CLI コマンドおよび GUI 選択オプションによる一般的な問題のトラブルシューティング (続き)

作業	GUI ツール	CLI コマンド
トレースのデバッグ レベルを変更する。	Cisco Unified Serviceability( <a href="https://&lt;サーバの IP アドレス &gt;:8443/ccmservice/">https://&lt;サーバの IP アドレス &gt;:8443/ccmservice/</a> )にログインし、[ Trace ]>[ Configuration ] を選択します。	set trace enable [ Detailed, Significant, Error, Arbitrary, Entry_exit, State_Transition, Special ][ syslogmib, cdpmib, dbl, dbnotify ]
ネットワークのステータスを表示する。	なし	show network status

## トラブルシューティングのヒント

次の各ヒントは、Cisco Unified Communications Manager のトラブルシューティングに役立ちます。



ヒント

Cisco Unified Communications Manager のリリース ノートで既知の問題を確認します。リリース ノートには、既知の問題の説明と対応策が記載されています。



ヒント

デバイスの登録先を確認します。

各 Cisco Unified Communications Manager ログはファイルをローカルでトレースします。電話機またはゲートウェイが特定の Cisco Unified Communications Manager に登録されている場合、その Cisco Unified Communications Manager でコールが開始されると、コール処理はそこで実行されます。問題をデバッグするには、その Cisco Unified Communications Manager 上のトレースを取り込む必要があります。

デバイスがサブスクリバ サーバに登録されているにも関わらず、パブリッシャ サーバ上のトレースを取り込むという間違いがよくあります。そのトレース ファイルはほとんど空です（そのファイルには目的のコールがまったく含まれていません）。

デバイス 1 を CM1 に登録し、デバイス 2 を CM2 に登録しているために問題が生じることも多くあります。デバイス 1 がデバイス 2 をコールすると CM1 でコールトレースが実行され、デバイス 2 がデバイス 1 をコールすると CM2 でトレースが実行されます。双方向のコール問題のトラブルシューティングを行う場合は、トラブルシューティングに必要なすべての情報を得るために、両方の Cisco Unified Communications Manager からの両方のトレースが必要となります。



ヒント

問題のおおよその時刻を認識します。

複数のコールが発信された可能性があるため、コールのおおよその時刻を認識していると、TAC が問題を迅速に特定するのに役立ちます。

アクティブなコール中に [i] または [?] ボタンを 2 回押すと、Cisco Unified IP Phone 79xx 上で統計情報を取得できます。

テストを実行して問題を再現し、情報を生成する場合は、問題を理解するために不可欠な次のデータを確認してください。

- 発信側の番号または着信側の番号
- 特定のシナリオに関係する他の番号
- コールの時刻



(注) トラブルシューティングには、すべての機器の時刻が同期化されていることが重要であることに注意してください。

問題を再現している場合は、ファイルの変更日付とタイムスタンプを調べて、その時間枠のファイルを選択します。適切なトレースを収集する最良の方法は、問題を再現してからすぐに最新のファイルを見つけ、そのファイルを Cisco Unified Communications Manager サーバからコピーすることです。



---

**ヒント**

ログ ファイルを保存して、上書きされないようにします。

---

ファイルは、時間が経つと上書きされます。ログが記録されているファイルを調べる唯一の方法は、メニューバーで [表示]>[最新の情報に更新]を選択し、ファイルの日付と時刻を確認することです。

## Cisco Unified Communications Manager サービスが動作していることの確認

サーバ上で Cisco CallManager サービスがアクティブであ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** Cisco Unified Communications Manager の管理ページから、[ ナビゲーション ] > [ Cisco Unified サービスアビリティ ] を選択します。

**ステップ 2** [ Tools ] > [ Service Activation ] を選択します。

**ステップ 3** [ Server ] カラムから、サーバを選択します。

選択したサーバが Current Server というタイトルの隣に表示され、設定済みのサービスを示す一連のボックスが表示されます。

Cisco CallManager 行の [ Activation Status ] カラムに、[ Activated ] または [ Deactivated ] と表示されます。

[ Activated ] というステータスが表示されている場合、選択したサーバ上で、指定した Cisco CallManager サービスがアクティブのままになっています。

[ Deactivated ] というステータスが表示されている場合は、引き続き次のステップを実行します。

**ステップ 4** 目的の Cisco CallManager サービスのチェックボックスをオンにします。

**ステップ 5** [ Update ] ボタンをクリックします。

指定した Cisco CallManager サービス行の [ Activation Status ] カラムに [ Activated ] と表示されます。

これで、選択したサーバ上の指定したサービスがアクティブになりました。

Cisco CallManager サービスがアクティブであるかどうか、およびサービスが現在動作しているかどうかを確認するには、次の手順を実行します。

### 手順

**ステップ 1** Cisco Unified Communications Manager の管理ページから、[ ナビゲーション ] > [ Cisco Unified サービスアビリティ ] を選択します。

[ Cisco Unified Communications Manager Serviceability ] ウィンドウが表示されます。

**ステップ 2** [ Tools ] > [ Control Center – Feature Services ] を選択します。

**ステップ 3** [ Server ] カラムから、サーバを選択します。

選択したサーバが Current Server というタイトルの隣に表示され、設定済みのサービスを示すボックスが表示されます。

[ Status ] カラムに、選択したサーバでどのサービスが動作しているかが表示されます。



# 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 \(P.3-2\)](#)
- [パブリッシャとサブスクリバの間で複製が失敗する \(P.3-8\)](#)
- [サーバの応答が遅い \(P.3-9\)](#)
- [JTAPI サブシステムの起動に関する問題 \(P.3-9\)](#)
- [セキュリティの問題 \(P.3-14\)](#)

## 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 (P.3-2)
- Cisco Unified Communications Manager の管理ページが表示されない (P.3-3)
- Cisco Unified Communications Manager の管理ページにアクセスしようとするエラーが発生する (P.3-3)
- 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エラーが発生する (P.3-4)
- 表示する権限がない (P.3-4)
- Cisco Unified Communications Manager でのユーザの表示または追加に関する問題 (P.3-4)
- 名前からアドレスへの解決の失敗 (P.3-5)
- 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 (P.3-6)
- 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 (P.3-6)
- サーバの応答が遅い (P.3-9)

### 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、perfmom 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、perfmom 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、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 に問い合わせてください。

**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、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リ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リバと呼ばれます。

### 症状

パブリッシャ上で行われた変更が、サブスクリ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リ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 Performance 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 - 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 - 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 - 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。

- [セキュリティ アラーム \(P.3-14\)](#)
- [セキュリティ パフォーマンス モニタ カウンタ \(P.3-14\)](#)
- [セキュリティ ログおよびトレース ファイルの確認 \(P.3-16\)](#)
- [証明書のトラブルシューティング \(P.3-16\)](#)
- [CTL セキュリティ トークンのトラブルシューティング \(P.3-16\)](#)
- [CAPF のトラブルシューティング \(P.3-17\)](#)
- [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 \(P.3-18\)](#)



(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せん。

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
<i>Cisco Unified Communications Manager</i>	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 \(P.3-17\)](#)
- [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 \(P.3-18\)](#)
- [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 \(P.3-18\)](#)
- [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 \(P.3-18\)](#)
- [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 \(P.3-18\)](#)
- [CAPF エラー コード \(P.3-19\)](#)

## 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 パケットをスニフリ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_CREDENTIALS, /* 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。



## デバイスの問題

---

この章では、Cisco Unified IP Phone、ゲートウェイ、および関連デバイスで発生する可能性のある、次のような一般的な問題について説明します。

- [音声品質 \(P.4-2\)](#)
- [コーデックとリージョンの不一致 \(P.4-11\)](#)
- [ロケーションと帯域幅 \(P.4-12\)](#)
- [電話機の問題 \(P.4-13\)](#)
- [ゲートウェイの問題 \(P.4-15\)](#)
- [ゲートキーパーの問題 \(P.4-21\)](#)
- [Restart\\_Ack に Channel IE が含まれていない場合に B チャネルがロックされたままになる \(P.4-22\)](#)

## 音声品質

通話中に、音声信号の損失や歪みなど、音声品質の問題が発生することがあります。

一般的な問題としては、音声途切れ（言葉が聞き取れないなど）、異常なノイズが入る、音声が歪む（エコーが聞こえるなど）、音声がこもったり合成音のようになっていたりする、といった問題があります。単方向音声（二者間でどちらか一方だけに音声が聞こえる会話）は、本来は音声品質の問題ではありませんが、この問題についてもこの章で取り上げます。

音声問題は、次のアイテムのいずれか1つまたは複数で発生する可能性があります。

- ゲートウェイ
- 電話機
- ネットワーク

この項では、次の一般的な音声品質問題について説明します。

- [音声の損失または歪み \(P.4-2\)](#)
- [Cisco Unified IP Phone による音声問題の解決 \(P.4-4\)](#)
- [エコー \(P.4-5\)](#)
- [単方向音声または無音声 \(P.4-6\)](#)

## 音声の損失または歪み

### 症状

発生する可能性のある最も一般的な問題の1つに、音声信号の途切れがあります（これは、「音声が聞き取りにくい」、「単語や文の中の音節が脱落する」などによく言われる問題です）。この問題の一般的な原因は、パケット損失とジッタの2つです。どちらか1つまたは両方が原因になる場合があります。パケット損失とは、音声パケットがドロップされたため、または到達が遅すぎて無効になったために、音声パケットが宛先に到達しないことを意味します。ジッタは、パケットの到達時間のばらつきを示します。最適な状況では、すべての Voice over IP (VoIP) パケットが正確に 20 ミリ秒 (ms) に 1 個の割合で到達します。ジッタは、パケットがポイント A からポイント B に到達する所要時間ではなく、単に、パケット到達時間のばらつきであることに注意してください。

### 考えられる原因

ネットワークには、遅延のばらつきの原因が数多く存在します。それらの原因の中は、制御できるものとできないものがあります。パケット音声ネットワークにおける遅延のばらつきを完全になくすことはできません。電話機などの音声対応デバイス上の Digital Signal Processors (DSP; デジタル信号プロセッサ) は、遅延のばらつきを想定して音声の一部を計画的にバッファリングします。このデジタリングは、音声パケットが宛先に到達し、通常の音声ストリームに使用される準備が整った場合に限り実行されます。

Cisco Unified IP Phone 7960 モデルは、1 秒間の音声サンプルをバッファリングできます。ジッタ バッファは状況に応じて使用されるので、一度に大量のパケットが受信された場合、Cisco Unified IP Phone 7960 モデルはジッタを制御するためにそれらのパケットを再生することができます。ネットワーク管理者は、quality of service (QoS; サービス品質) などの手段をあらかじめ適用することで、パケット到達時間のばらつきを最小化する必要があります（この作業は、コールが WAN を経由する場合は特に重要です）。

ビデオ エンドポイントの中には、G.728 をサポートしていないものもあります。そのため、G.728 を使用するとノイズが発生することがあります。そのような場合には、G.729 など、別のコーデックを使用してください。

## 推奨処置

1. 音声の損失または歪みの問題が発生した場合は、最初に、その音声のパスを割り出す必要があります。そのコールの音声ストリームのパスにある各ネットワーク デバイス（スイッチおよびルータ）を特定します。音声は、2 台の電話機間、電話機とゲートウェイ間、または複数の区間（電話機からトランスコーディング デバイスまでの区間、およびそのトランスコーディング デバイスから別の電話機までの区間）に存在する場合がありますことに留意してください。問題が発生しているのは、2 つのサイト間だけか、特定のゲートウェイを介した場合だけか、特定のサブネット上か、などを特定します。このような作業によって、さらに詳しく調べる必要があるデバイスの範囲を絞り込むことができます。
2. 次に、無音抑止（Voice Activation Detection または VAD とも呼ばれます）を無効にします。このメカニズムは、無音が発生する場合に音声を送信しないようにすることで帯域幅を節約しますが、単語の最初の部分で顕著な（容認できない）音飛びが発生する原因となる場合があります。

Cisco Unified Communications Manager の管理ページで、このサービスを無効にし、[システム] > [サービスパラメータ] を選択します。表示されたメニューで、サーバと Cisco CallManager サービスを選択します。

3. Cisco Communications Manager クラスタ内のすべてのデバイスに対して無音抑止を無効にするには、SilenceSuppression を **False** に設定します。または、SilenceSuppressionForGateways を **False** に設定する方法もあります。判断に迷う場合は、それぞれ **False** を選択して、両方ともオフにします。
4. ネットワーク アナライザが使用可能な場合には、ネットワーク アナライザを使用して、無音抑止が無効の状態では 2 台の電話機間の監視対象コールに 1 秒あたり 50 パケット（20 ミリ秒あたり 1 パケット）が存在するかどうかを確認します。適切なフィルタリングを行うことで、極端に多くのパケットが失われていないか、または遅延していないかを確認できます。

音飛びの原因となるのは遅延そのものではなく、遅延のばらつきだけです。次の表に注目してください。この表は、20 ミリ秒の音声パケット（RTP ヘッダーを含む）間の到達時間に関する完全なトレースを表しています。低品質のコール（多くのジッタが含まれるコールなど）の場合、到達時間は大きく変動します。

次の表は、完全なトレースを示しています。

パケット番号	時間 - 絶対値（秒）	時間 - 増分値（ミリ秒）
1	0	
2	0.02	20
3	0.04	20
4	0.06	20
5	0.08	20

パケット アナライザをネットワーク内のさまざまなポイントに配置すると、遅延が発生する場所の数を絞り込むのに役立ちます。使用可能なアナライザがない場合は、他の方法を使用する必要があります。音声のパスにある各デバイスのインターフェイス統計情報を調べてください。

診断に使用する Call Detail Record (CDR; コール詳細レコード) には、低音質のコールの追跡に役立つ別のツールが指定されています。CDR の詳細については、『Cisco Unified Communications Manager CDR Analysis and Reporting アドミニストレーションガイド』を参照してください。

## Cisco Unified IP Phone による音声問題の解決

### 症状

音声問題はコールの進行中に発生します。

### 考えられる原因

デバイスでは高速インターフェイスが低速インターフェイスに送り込まれるため、デバイスが遅延とパケット損失の最も一般的な原因になります。たとえば、ルータによっては、LAN に接続された 100 メガバイト (MB) のファーストイーサネットインターフェイスと WAN に接続された低速フレームリレー インターフェイスを持っている場合があります。リモートサイトに通信しているときにだけ音声品質が低下する場合は、その問題の最も可能性の高い原因としては、次のようなことが挙げられます。

- データ トラフィックより音声トラフィックが優先されるようにルータが正しく設定されていない。
- アクティブ コールが多すぎて WAN がサポートできない (つまり、発信可能なコール数を制限するコール アドミッション制御がない)。
- 物理ポートのエラーが発生している。
- WAN 自体で輻輳が発生している。

LAN 上の最も一般的な問題は、物理レベルのエラー (CRC エラーなど) です。これらのエラーは、ケーブルやインターフェイスの障害、またはデバイスの誤った設定 (ポートの速度やデュプレックスの不一致など) が原因で発生します。トラフィックがハブなどのシェアドメディア デバイスを通過していないことを確認してください。

### 推奨処置

Cisco Unified IP Phone 7960 モデルには、発生する可能性のある音声問題を診断するためのツールが別途用意されています。

- アクティブ コールに対して、[i] または [?] ボタンをすばやく 2 回押すと、電話機の情報画面に、送受信したパケットの統計情報、平均ジッタ カウンタ、および最大ジッタ カウンタが表示されます。



(注)

このウィンドウで、ジッタは最後に到達した 5 パケットの平均値を表し、最大ジッタは平均ジッタの最大値を表します。

- トラフィックが予想よりも遅いパスでネットワークを通過するという状況が発生することもあります。QoS が正しく設定されている場合は、コール アドミッション制御が実行されていない可能性があります。アドミッション制御を実行するには、トポロジに応じて、Cisco Unified Communications Manager の管理ページでロケーションの設定を使用するか、または Cisco IOS ルータをゲートキーパーとして使用します。いずれの場合も、WAN 全体でサポートされる最大コール数を常に認識しておく必要があります。
- クラックル ノイズ (パチパチという音) も音声品質の低下を示す症状の 1 つです。これは、電源装置の欠陥や電話機周辺の何らかの強い電氣的干渉が原因になる場合があります。電源装置を交換し、電話機を移動してください。
- ゲートウェイと電話機のロードを確認します。www.cisco.com で、最新のソフトウェアのロード、新しいパッチ、または問題に関連するリリース ノートがあるかどうかを確認します。

適切なフィックスを適用した後に、次の手順を実行して音声品質を確認します。

1. P.4-2 の「**音声の損失または歪み**」の説明に従って無音抑止を無効にしてテストを行います。次に、2 つのサイト間で通話します。パケットが送信されなくなるので、コールを保留または消音にしないでください。
2. WAN を経由するコールの最大数が設定されていれば、すべてのコールは許容できる品質になります。
3. コールをもう 1 件発信しようとしたときに、速いビジー音が返ってくることを確認するテストを行います。

## エコー

### 症状

エコーが発生するのは、生成された音声エネルギーがプライマリ信号パスに伝送され、遠端の受信パスに連結されたときです。このとき、送話者には、エコーパスの合計遅延時間の分だけ遅れて自分の声が聞こえます。

音声は反響することがあります。従来の音声ネットワークでは、反響しても遅延が小さいので認識されません。ユーザにとっては、エコーというよりも側音のように聞こえます。VoIP ネットワークでは、パケット化と圧縮により遅延が大きくなるため、常にエコーは明確に認識されます。

### 考えられる原因

エコーの原因は必ずアナログ コンポーネントと配線にあります。たとえば、IP パケットは、低い音声レベルのソースまたはデジタル T1/E1 回線上のソースに方向を変えて戻ることができません。例外となる可能性があるのは、一方がスピーカフォンを使用して音量を極端に高く設定している場合など、音声ループが生成されるような状況が発生している場合だけです。

### 推奨処置

1. 問題の電話機でスピーカフォンが使用されていないこと、およびヘッドセットの音量が適切なレベル（最大音声レベルの 50 パーセントから開始する）に設定されていることを確認します。ほとんどの場合、この問題は、デジタル ゲートウェイまたはアナログ ゲートウェイを経由して PSTN に接続しているときに発生します。

#### ゲートウェイのテスト

2. 使用されているゲートウェイを判別します。デジタル ゲートウェイが使用されている場合、送信方向に（PSTN に向かって）パディングを追加できます。信号の強度を低下させると反響するエネルギーが減少するので、この方法で問題を解決できます。

これに加えて、受信レベルを調整することで、反響音をさらに小さくすることもできます。1 回の調整は微量にすることが重要です。信号の減衰量が大きすぎると、コールの両側で音声聞こえなくなります。

3. 通信事業者に連絡して、回線の確認を依頼する方法もあります。北米で一般的な T1/PRI 回線の場合、入力信号は -15 dB である必要があります。信号レベルがそれよりも大幅に高い（たとえば -5 dB）場合は、エコーが発生する可能性があります。

#### エコー ログの記録

4. エコーが発生したすべてのコールのログを記録する必要があります。

問題が発生した時刻、発信側の電話番号、および着信側の電話番号を記録します。ゲートウェイのエコー キャンセレーションは固定で 16 ミリ秒に設定されています。

反響音の遅延がこれよりも大きい場合、エコー キャンセラは正常に動作できません。正常に動作できなくても、市内電話については問題ありませんが、長距離電話の場合は、セントラル オフィスでネットワークに組み込まれた外部エコー キャンセラを使用する必要があります。この事実、エコーが発生するコールの外部電話番号を記録することが必要である理由の 1 つです。

### ロードの確認

5. ゲートウェイと電話機のロードを確認します。www.cisco.com で、最新のソフトウェアのロード、新しいパッチ、または問題に関連するリリース ノートがあるかどうかを確認します。

## 単方向音声または無音声

### 症状

IP ステーションから Cisco IOS 音声ゲートウェイまたはルータを介してコールを確立すると、一方の側しか音声を受信しません（単方向通信）。

2つの Cisco ゲートウェイ間でトールバイパス コールを確立すると、一方の側しか音声を受信しません（単方向通信）。

### 考えられる原因

この問題が発生する可能性があるのは、特に、Cisco IOS ゲートウェイ、ファイアウォール、またはルーティングの設定が正しくない場合、またはデフォルト ゲートウェイに問題がある場合です。

### 推奨処置

**Cisco IOS ゲートウェイまたはルータで IP ルーティングが有効になっていることを確認する**

VG200 など、Cisco IOS ゲートウェイの中には、IP ルーティングがデフォルトで無効になっているものがあります。これが原因で単方向音声の問題が発生します。



(注)

作業を進める前に、ルータの IP ルーティングが有効になっている（つまり、ルータにグローバル設定コマンド `no ip routing` が設定されていない）ことを確認してください。

IP ルーティングを有効にするには、Cisco IOS ゲートウェイで次のグローバル設定コマンドを入力するだけです。

```
voice-ios-gwy(config)#ip routing
```

基本 IP ルーティングを確認する

基本 IP の到達可能性は、必ず最初に確認する必要があります。RTP ストリームは UDP で転送されるコネクションレス型なので、トラフィックは一方方向には正常に進みますが、反対方向には正常に進みません。

次の条件を確認してください。

- エンドステーションにデフォルト ゲートウェイが設定されている。
- そのデフォルト ゲートウェイの IP ルートが宛先ネットワークに通じている。



(注)

各種 Cisco Unified IP Phone のデフォルト ルータまたはゲートウェイの設定を検証する方法を次に示します。

- Cisco Unified IP Phone 7910 モデル : [ 設定 ] ボタンを押し、オプション 6 を選択してから、[ デフォルト ルータ ] フィールドが表示されるまで下向きの音量キーを押します。

- Cisco Unified IP Phone 7960/40 モデル : [ 設定 ] ボタンを押し、オプション 3 を選択してから、[ デフォルト ルータ ] フィールドが表示されるまで下方向にスクロールします。
- Cisco Unified IP Phone 2SP+/30VIP モデル : **\*\*\*#** を押してから、**gtwy=** が表示されるまで **#** を押します。



(注)

Cisco DT24+ Gateway の場合は、DHCP Scope を確認し、スコープ内に Default Gateway (003 router) オプションがあることを確認してください。003 router パラメータは、デバイスと PC の Default Gateway フィールドに読み込まれます。スコープ オプション 3 には、ゲートウェイ用のルーティングを実行するルータ インターフェイスの IP アドレスが指定されている必要があります。

### H.323 シグナリングを Cisco IOS ゲートウェイまたはルータ上の特定の IP アドレスにバインドする

Cisco IOS ゲートウェイにアクティブな IP インターフェイスが複数ある場合、H.323 シグナリングの一部は送信元の 1 つの IP アドレスを使用し、その他の部分は別の送信元アドレスを参照することがあります。この結果、さまざまな問題が発生します。その 1 つが単方向音声です。

この問題を回避するには、H.323 シグナリングを特定の送信元アドレスにバインドします。この送信元アドレスは、物理インターフェイスまたは仮想インターフェイスに属することができます ( ループバック )。インターフェイス設定モードで使用するコマンド構文は、**h323-gateway voip bind srcaddr<IP アドレス>** です。Cisco Unified Communications Manager が指す IP アドレスを持つインターフェイスで、このコマンドを設定します。

このコマンドは『*Configuring H.323 Support for Virtual Interfaces*』で文書化され、Cisco IOS Release 12.1.2T で導入されました。



(注)

バージョン 12.2(6) にはバグが存在するため、このソリューションでは単方向音声の問題が発生する可能性があります。詳細については、Cisco Software Bug Toolkit (登録済みのお客様専用) でバグ ID CSCdw69681 (登録済みのお客様専用) を参照してください。

### Telco または交換機から応答監視が正しく送受信されていることを確認する

Telco または交換機に接続された Cisco IOS ゲートウェイが含まれる実装では、Telco または交換機の内側にある着信側デバイスがコールに応答するときに、応答監視が正しく送信されることを確認します。応答監視の受信に失敗すると、Cisco IOS ゲートウェイは順方向の音声パスをカットスルー (オープン) できず、単方向音声となります。これを回避するには、**voice rtp send-recv on** を設定する必要があります。

### Cisco IOS ゲートウェイまたはルータで **voice rtp send-recv** を使用し、双方向音声を早期にカットスルーする

RTP ストリームが開始されるとすぐに、逆方向の音声パスが確立されます。順方向の音声パスは、Cisco IOS ゲートウェイが Connect メッセージをリモート エンドから受信するまでカットスルーされません。

場合によっては、RTP チャンネルが開いたらすぐに (Connect メッセージが受信される前に) 双方向の音声パスを確立する必要があります。これを実現するには、**voice rtp send-recv** グローバル設定コマンドを使用します。

### Cisco IOS ゲートウェイまたはルータのリンクバイリンク ベースの cRTP 設定を確認する

この問題は、複数の Cisco IOS ルータまたはゲートウェイが音声パスに関与していて、Compressed RTP (cRTP; 圧縮 RTP) が使用されている、ツールバイパスなどのシナリオに該当します。cRTP、つまり RTP ヘッダー圧縮機能は、VoIP パケットのヘッダーを小さくして帯域幅を取り戻すための方法です。cRTP では、VoIP パケット上に 40 バイトの IP/UDP/RTP ヘッダーを設定し、それを 1 パケットにつき 2 ~ 4 バイトに圧縮するので、G.729 で符号化されたコールの場合、cRTP 使用時に約 12 KB の帯域幅が得られます。

cRTP はホップバイホップ ベースで実行され、すべてのホップで圧縮解除と再圧縮が行われます。ルーティングするには各パケットヘッダーを検査する必要があるため、IP リンクの両端で cRTP を有効にします。

リンクの両端で cRTP が期待どおりに機能していることも確認します。各 Cisco IOS レベルは、スイッチングパスと同時 cRTP サポートによって異なります。

履歴の要約を次に示します。

- Cisco IOS Software Release 12.0.5T まで、cRTP はプロセス交換されます。
- Cisco IOS Software Release 12.0.7T では、cRTP に対するファーストスイッチングと Cisco Express Forwarding (CEF; Cisco エクスプレス転送) スwitching のサポートが導入され、12.1.1T でも引き続きサポートされています。
- Cisco IOS Software Release 12.1.2T では、アルゴリズムのパフォーマンスが向上しています。

Cisco IOS プラットフォーム (IOS Release 12.1) 上で cRTP を実行している場合は、バグ CSCds08210 (登録済みのお客様専用) (VoIP and FAX not working with RTP header compression ON) がご使用の IOS バージョンに影響しないことを確認します。

### Cisco IOS ゲートウェイまたはルータ上の NAT に必要な最低限のソフトウェア レベルを確認する

Network Address Translation (NAT; ネットワーク アドレス変換) を使用している場合は、最低限のソフトウェア レベルを満たす必要があります。以前のバージョンの NAT は Skinny プロトコル変換をサポートしないので、単方向音声の問題が発生します。

NAT と Skinny を同時に使用するために必要な最低限のソフトウェア レベルは、Cisco IOS® Software 12.1(5)T と定められています。IOS ゲートウェイが NAT を使用して Skinny と H.323v2 をサポートするには、このレベルのソフトウェアが必要です。



(注) Cisco Unified Communications Manager が Skinny シグナリング用にデフォルトの 2000 と異なる TCP ポートを使用している場合は、`ip nat service skinny tcp port<番号>` グローバル設定コマンドを使用して NAT ルータを調整する必要があります。

PIX ファイアウォール上で NAT と Skinny を同時に使用するために必要な最低限のソフトウェア レベルは 6.0 と定められています。



(注) これらのレベルのソフトウェアが、ゲートキーパーのフル サポートに必要なすべての RAS メッセージをサポートするわけではありません。ゲートキーパーのサポートについては、本書では取り上げません。

### AS5350 および AS5400 の voice-fastpath を無効にする

Cisco IOS コマンド `voice-fastpath enable` は、AS5350 および AS5400 用の非表示のグローバル設定コマンドを取得します。これは、デフォルトで有効になっています。これを無効にするには、`no voice-fastpath enable` グローバル設定コマンドを使用します。

有効になっていると、このコマンドは特定のコール用に開いている論理チャンネルの IP アドレスと UDP ポート番号の情報をキャッシュします。それによって RTP ストリームはアプリケーション層に到達できなくなり、それより下位の層にパケットが転送されます。そのため、大量のコールがあるシナリオでは CPU 使用率がわずかに抑えられます。

保留や転送などの補助的なサービスを使用している場合、`voice-fastpath` コマンドを使用すると、ルータは保留されたコールの再開後または転送の完了後に収集された新しい論理チャンネルの情報を無視して、キャッシュされている IP アドレスと UDP ポートに音声を送信します。この問題を回避するには、論理チャンネルの再定義を考慮して、音声 新しい IP アドレスと UDP ポートのペアに送信されるように、トラフィックを常にアプリケーション層に到達させる必要があります。そのため、補助的なサービスをサポートするには `voice-fastpath` を無効にする必要があります。

### VPN IP アドレスを SoftPhone に設定する

Cisco IP SoftPhone を使用すると、PC を Cisco Unified IP Phone 7900 モデルシリーズの電話機のように使用できます。リモート ユーザが VPN を経由して自社のネットワークに接続し直す場合は、単方向音声の問題を回避するために、いくつかの追加設定を行う必要があります。

これを解決策するには、Network Audio Settings でネットワーク アダプタの IP アドレスの代わりに VPN IP アドレスを設定する必要があります。



## コーデックとリージョンの不一致

オフフックしたときにリオーダー音（話し中の音）が聞こえる場合は、リージョン間でコーデックが一致していないことが原因である可能性があります。コールの両端で少なくとも1つの共通のコーデック（たとえば、G.711）がサポートされていることを確認してください。共通のコーデックがサポートされていない場合は、トランスコードを使用する必要があります。

リージョンには、他の各リージョンとともに使用できる、サポートされているコーデックの種類が特定されています。すべてのデバイスはリージョンに属します。



---

**(注)** Cisco IOS ルータとのコーデック ネゴシエーションはサポートされていません。

---

たとえば、Region1<->Region2 = G.711 は、Region1 のデバイスと Region2 のデバイス間のコールで G.711 またはその他のサポートされている任意のコーデック（G.711、G.729、G.723 など、G.711 と同じかそれより小さい帯域幅を必要とするコーデック）を使用できることを意味しています。



---

**(注)** 各デバイス用にサポートされているコーデックを次に示します。  
Cisco Unified IP Phone 7960 モデル : G.711A-law/mu-law、G.729、G.729A、G.729Annex-B  
Cisco Unified IP Phone SP12 シリーズおよび VIP 30 : G.711a-law/mu-law、G.723.1  
Cisco Access Gateway DE30 および DT-24+ : G.711a-law/mu-law、G.723.1

---

## ロケーションと帯域幅

番号をダイヤルした後にリオーダー音が聞こえる場合は、いずれかのコール終端デバイスのロケーションに対する Cisco Unified Communications Manager の帯域割り当てを超過したことが原因である可能性を示しています。Cisco Unified Communications Manager は、コールを発信する前に、各デバイスで使用できる帯域幅があるかどうかを確認します。使用可能な帯域幅がない場合、Cisco Unified Communications Manager はコールを発信しないので、ユーザにはリオーダー音が聞こえます。

```
12:42:09.017 Cisco Communications Manager|Locations:Orig=1 BW=12Dest=0 BW=-1(-1
implies infinite bw available)
12:42:09.017 Cisco Communications Manager|StationD - stationOutputCallState
tcpHandle=0x4f1ad98
12:42:09.017 Cisco Communications Manager|StationD - stationOutputCallInfo
CallingPartyName=, CallingParty=5003, CalledPartyName=, CalledParty=5005,
tcpHandle=0x4f1ad98
12:42:09.017 Cisco Communications Manager|StationD - stationOutputStartTone:
37=ReorderTone tcpHandle=0x4f1ad98
```

コールが確立されると、Cisco Unified Communications Manager は、そのコールで使用されるコーデックに応じてロケーションから帯域幅を差し引きます。

- コールで G.711 が使用されている場合、Cisco Unified Communications Manager は 80k を差し引きます。
- コールで G.723 が使用されている場合、Cisco Unified Communications Manager は 24k を差し引きます。
- コールで G.729 が使用されている場合、Cisco Unified Communications Manager は 24k を差し引きます。

## 電話機の問題

この項では、次の電話機の問題について説明します。

- [電話機のリセット \(P.4-13\)](#)
- [ドロップされたコール \(P.4-14\)](#)
- [電話機が登録されない \(P.4-14\)](#)

## 電話機のリセット

### 症状

電話機がリセットされます。

### 考えられる原因

電話機の電源が切れて再投入されたり、電話機がリセットされたりする理由には、次の2つがあります。

- Cisco Unified Communications Manager に接続する際に TCP エラーが発生した。
- 電話機の KeepAlive メッセージに対する確認応答を受信する際にエラーが発生した。

### 推奨処置

1. 電話機とゲートウェイを調べて、最新のソフトウェア ロードを使用していることを確認します。
2. [www.cisco.com](http://www.cisco.com) で、最新のソフトウェアのロード、新しいパッチ、または問題に関連するリリース ノートがあるかどうかを確認します。
3. 電話機のリセットに関するインスタンスがあるかどうかを Cisco Real-Time Monitoring Tool の Syslog Viewer で確認します。電話機のリセットは情報イベントに相当します。
4. 電話機がリセットされた時刻の前後に発生した可能性のあるエラーを探します。
5. SDI トレースを開始し、リセットが発生している電話機に共通する特徴を見極めて、問題を特定します。たとえば、それらの電話機がすべて同じサブネットに配置されているかどうか、あるいは、同じ VLAN に配置されているかどうかなどを確認します。トレースを調べて次の点を確認します。

リセットは通話中に発生するか、それとも断続的に発生するか。

電話機モデル (Cisco Unified IP Phone 7960 モデルまたは Cisco Unified IP Phone 30VIP モデルなど) に類似性があるかどうか。

6. 頻繁にリセットが発生する電話機上でスニファ トレースを開始します。電話機がリセットされた後にトレースを調べて、TCP リトライが行われているかどうかを確認します。行われている場合は、ネットワークに問題があることを示しています。トレースを実行すると、たとえば、電話機のリセットが7日に1回発生しているなど、リセットの規則性が見いだされる場合があります。このことから、DHCP リースの有効期限が7日に1回の周期に設定されている可能性があります (この値はユーザが設定できます。たとえば、2分に1回にすることもできます)。

## ドロップされたコール

### 症状

ドロップされたコールが早期異常終了します。

### 考えられる原因

ドロップされたコールが早期異常終了する場合は、電話機またはゲートウェイのリセットが原因である可能性があります (P.4-13 の「電話機のリセット」を参照)。または、PRI 設定の誤りなど、回線の問題が原因である可能性もあります。

### 推奨処置

1. この問題を 1 台の電話機または 1 つの電話機グループに特定できるかどうかを確認します。影響を受けている電話機はすべて特定のサブネットまたはロケーションに配置されていることもあります。
2. 電話機またはゲートウェイのリセットを Cisco Real-Time Monitoring Tool の Syslog Viewer で確認します。

リセットが発生する電話機ごとに、警告メッセージとエラーメッセージが 1 つずつ表示されます。これは、その電話機が Cisco Unified Communications Manager への TCP 接続を維持できないために、Cisco Unified Communications Manager が接続をリセットすることを示しています。このリセットは、電話機の電源をオフにしたため、またはネットワークに問題があるために発生することがあります。この問題が断続的に発生しているときは、RTMT のパフォーマンスモニタリングを使用すると役立つ場合があります。

3. 特定のゲートウェイ (Cisco Access DT-24+ など) を経由した場合にだけ問題が発生していると考えられる場合は、トレースを有効にするか、CDR を確認するか、あるいはその両方を行います。CDR ファイルには、問題の原因を判別するのに役立つ Cause of Termination (CoT) が含まれています。CDR の詳細については、『Cisco Unified Communications Manager CDR Analysis and Reporting アドミニストレーションガイド』を参照してください。
4. 接続解除の理由種別 (コールを接続解除した側に応じて origCause\_value および destCause\_value) を見つけます。接続解除の理由種別は、次の場所にある Q.931 接続解除理由コード (10 進表記) に対応しています。

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/dbook/disdn.htm>

5. コールがゲートウェイから出て PSTN に向かう場合は、CDR を使用して、どちらの側がコールを切断したかを判別できます。Cisco Unified Communications Manager でトレースを有効にすることにより、ほぼ同じ情報を入手できます。トレース ツールは Cisco Unified Communications Manager のパフォーマンスに影響を与える可能性があるため、最後の手段として使用するか、またはネットワークが稼働していないときに使用してください。

## 電話機が登録されない

### 症状

5000 台を超える電話機を登録できません。

### 考えられる原因

Maximum Number of Registered Devices サービス パラメータによってデフォルト値が指定されています。

### 推奨処置

各ノードの Maximum Number of Registered Devices サービス パラメータの値を適切な値に変更します。

## ゲートウェイの問題

この項では、次のゲートウェイの問題について説明します。

- [ゲートウェイのリオーダー音](#)
- [ゲートウェイの登録障害](#)

### ゲートウェイのリオーダー音

#### 症状

リオーダー音が発生します。

#### 考えられる原因

ゲートウェイを経由するコールを発信する場合、制限されているコールを発信したり、ブロックされている番号にダイヤルしたりすると、リオーダー音が聞こえることがあります。リオーダー音は、ダイヤルした番号が使用不可になっている場合、または PSTN の機器やサービスに問題がある場合に発生することがあります。

リオーダー音を発しているデバイスが登録されていることを確認してください。また、ダイヤルプラン設定を調べて、コールが正常にルーティングされることも確認してください。

#### 推奨処置

ゲートウェイを経由する場合のリオーダー音のトラブルシューティングを行う手順を次に示します。

1. ゲートウェイを調べて、最新のソフトウェア ロードを使用していることを確認します。
2. [www.cisco.com](http://www.cisco.com) で、最新のソフトウェアのロード、新しいパッチ、または問題に関連するリリース ノートがあるかどうかを確認します。
3. SDI トレースを開始し、問題を再現します。リオーダー音は、Cisco Unified Communications Manager が許容可能なコール数を制限する、ロケーション ベースのアドミッション制御またはゲートキーパー ベースのアドミッション制御に関する設定の問題が原因です。SDI トレースでコールを特定して、ルート パターンやコーリング サーチ スペースなどの構成設定によってそのコールが意図的にブロックされたかどうかを判別します。
4. PSTN を経由する場合もリオーダー音が発生することがあります。SDI トレースで Q.931 メッセージがないかどうか確認します。特に接続解除メッセージに注意します。Q.931 の接続解除メッセージがある場合、接続解除の原因は相手側にあり、こちら側でそれを解決することはできません。

### ゲートウェイの登録障害

この項では、ゲートウェイの2つのカテゴリについて説明します。これらのカテゴリは類似していますが、同一ではありません。Cisco Access AS-X、AT-X、Cisco Access DT-24+、および DE-30+ は同じカテゴリに属します。これらのゲートウェイは、Network Management Processor (NMP; ネットワーク管理プロセッサ) に直接接続されていないスタンドアロン ユニットです。もう1つのカテゴリには、Analog Access WS-X6624 および Digital Access WS-X6608 が含まれます。これらのゲートウェイは、Catalyst 6000 のシャーシに取り付けられたブレードとして、制御とステータス管理のために NMP に直接接続できます。

#### 症状

登録の問題は、Cisco Unified Communications Manager に設定されたゲートウェイで発生する最も一般的な問題の1つです。

### 考えられる原因

登録が失敗するのは、さまざまな理由が考えられます。

### 推奨処置

1. まず、ゲートウェイが稼働していることを確認します。すべてのゲートウェイにはハートビート LED が付属しており、ゲートウェイ ソフトウェアが正常に稼働している場合は 1 秒間隔で点滅します。

この LED がまったく点滅しない場合、または非常に速く点滅する場合、ゲートウェイ ソフトウェアが稼働していないことを示します。その結果、通常、ゲートウェイは自動的にリセットされます。また、約 2 ~ 3 分経過して登録プロセスを完了できない場合にも、通常、ゲートウェイは自動的にリセットされるものと見なします。したがって、確認したときデバイスがたまたまりセット中である場合もありますが、10 ~ 15 秒後に通常の点滅パターンが示されない場合は、ゲートウェイに重大な障害があります。

Cisco Access Analog ゲートウェイでは、前面パネルの右端に緑色ハートビート LED があります。Cisco Access Digital ゲートウェイでは、カード上部の左端に赤色 LED があります。Cisco Analog Access WS-X6624 では、前面に近いカード右端にあるブレードの内部に緑色 LED があります（前面パネルからは見えません）。Digital Access WS-X6608 では、ブレード上の 8 スパンそれぞれに別個のハートビート LED があります。8 個の赤色 LED はカード上に並んでいます（前面パネルからは見えません）。これらの LED は、背面に向かって約 3 分の 2 進んだ位置にあります。

2. ゲートウェイが自分の IP アドレスを受信したことを確認します。スタンドアロン ゲートウェイは、自分の IP アドレスを DHCP または BOOTP を介して受信する必要があります。Catalyst ゲートウェイは、DHCP または BOOTP によって、あるいは NMP を介した手動設定によって自分の IP アドレスを受信できます。
3. DHCP サーバに対するアクセス権を持っている場合、スタンドアロン ゲートウェイを調べる最善の方法は、デバイスに未解決の IP アドレス リースがあるかどうかを確認することです。ゲートウェイがサーバ上に表示される場合、そのことは良い目安になりますが、決定的なものではありません。DHCP サーバで、そのリースを削除します。
4. ゲートウェイをリセットします。
5. 数分以内にゲートウェイがリースとともにサーバ上に再び表示される場合、この領域の動作はすべて正常です。表示されない場合は、ゲートウェイが DHCP サーバに接続できない（ルータの設定が誤っていないか、そのために DHCP ブロードキャストが転送されていないか、また、サーバが稼働しているかを確認してください）か、または、肯定応答を取得できない（IP アドレス プールがいっぱいになっていないかを確認してください）かのいずれかです。
6. これらのことを確認しても答えが得られない場合は、スニファ ツールを使用して問題点を特定します。
7. Catalyst 6000 ゲートウェイの場合、NMP がゲートウェイと通信できることを確認する必要があります。これは、NMP からゲートウェイの内部 IP アドレスに対して ping を実行することで確認できます。

IP アドレスには次の形式が使用されます。

```
127.1.module.port
```

```
For example, for port 1 on module 7, you would enter
Console (enable) ping 127.1.7.1
127.1.7.1 is alive
```

8. ping が正常に実行された場合、show port コマンドを使用すると IP アドレス情報が表示されます。IP アドレス情報と TFTP IP アドレスが正しいことも確認してください。
9. ゲートウェイが有効な DHCP 情報の取得に失敗する場合は、Cisco TAC によって提供される Tracy ユーティリティを使用して問題を特定します。
10. このユーティリティを TAC から入手したら、Cat6000 Command Line Interface (CLI; コマンドライン インターフェイス) から次のコマンドを発行します。



16. ヘルパー アプリケーションとして tracy ユーティリティを使用するには、割り当てられている IP アドレスを使用してゲートウェイに接続します。この tracy アプリケーションはすべてのゲートウェイ上で動作し、ゲートウェイごとに別個のトレース ウィンドウを表示します（一度にトレースできるのは最大 8 個）。トレースは指定したファイルに直接記録できます。
17. TFTP サーバの IP アドレスがゲートウェイに正しく指定されたことを確認します。DHCP は通常、Option 66（名前または IP アドレス）、Option 150（IP アドレスのみ）、または si\_addr（IP アドレスのみ）で DHCP を提供します。サーバに複数の Option が設定されている場合、si\_addr が Option 150 より優先され、Option 150 は Option 66 より優先されます。

Option 66 が TFTP サーバの DNS\_NAME を提供する場合、DNS サーバの IP アドレスは DHCP によって指定されている必要があります。また、Option 66 に入力された名前は正しい TFTP サーバの IP アドレスに解決される必要があります。NMP を使用して DHCP が無効になるように Catalyst ゲートウェイを設定できます。その場合、NMP オペレータは、TFTP サーバのアドレスを含むすべての設定パラメータをコンソールから手動で入力する必要があります。

また、ゲートウェイは、常に DNS を介して名前 CiscoCM1 の解決を試行します。解決に成功すると、CiscoCM1 の IP アドレスは、DHCP サーバまたは NMP が TFTP サーバのアドレスとして示すどの情報よりも優先されます。これは、NMP が DHCP を無効にしている場合も同じです。

18. ゲートウェイにある現在の TFTP サーバの IP アドレスは、tracy ユーティリティを使用して確認できます。次のコマンドを入力して、設定タスク番号を取得します。

```
TaskID: 0
Cmd:    show tl
```

config または CFG が含まれる行を探し、対応する番号を次の行（Cisco Access Digital gateway など）の taskID として使用します。この後の例では、説明対象のメッセージを判別しやすいように太字のテキスト行で示しています。実際の画面出力では、テキストは太字で表示されません。これらの例は WS-X6624 モデルの出力です。DHCP 情報をダンプするコマンドは次のとおりです。

```
TaskID: 6
Cmd:    show dhcp
```

19. このコマンドによって、TFTP サーバの IP アドレスが表示されます。その IP アドレスが正しくない場合は、DHCP オプションと表示されたその他の情報が正しいことを確認します。
20. TFTP アドレスが正しい場合は、ゲートウェイが自分の設定ファイルを TFTP サーバから取得していることを確認します。tracy 出力で次の情報が表示される場合は、TFTP サービスが正常に機能していないか、ゲートウェイが Cisco Unified Communications Manager に設定されていない可能性があります。

```
00:09:05.620 (CFG) Requesting SAA00107B0013DE.cnf File From TFTP Server
00:09:18.620 (CFG) TFTP Error: Timeout Awaiting Server Response for .cnf File!
```

ゲートウェイは設定ファイルを取得しない場合、TFTP サーバと同じ IP アドレスに対する接続を試行します。クラスタ化された環境でなければ、これで接続できます。クラスタ化された環境では、ゲートウェイは冗長 Cisco Unified Communications Manager のリストを受信する必要があります。

21. カードが自分の TFTP 情報を正常に取得していない場合は、Cisco Unified Communications Manager の TFTP サービスを調べて、サービスが動作していることを確認してください。
22. Cisco Unified Communications Manager の TFTP トレースを確認します。

ゲートウェイが Cisco Unified Communications Manager に正しく設定されていない場合は、別の一般的な問題が発生します。典型的なエラーは、ゲートウェイ用に誤った MAC アドレスを入力したことで発生します。その場合、Catalyst 6000 ゲートウェイでは、次のメッセージが 2 分間隔で NMP コンソールに表示されることがあります。

```
2000 Apr 14 19:24:08 %SYS-4-MODHPRESET:Host process (860) 7/1 got reset
asynchronously
2000 Apr 14 19:26:05 %SYS-4-MODHPRESET:Host process (860) 7/1 got reset
asynchronously
2000 Apr 14 19:28:02 %SYS-4-MODHPRESET:Host process (860) 7/1 got reset
asynchronously
```

The following example shows what the Tracy output would look like if the gateway is not in the Cisco CallManager database:

```
00:00:01.670 (CFG) Booting DHCP for dynamic configuration.
00:00:05.370 (CFG) DHCP Request or Discovery Sent, DHCPState = INIT_REBOOT
00:00:05.370 (CFG) DHCP Server Response Processed, DHCPState = BOUND
00:00:05.370 (CFG) Requesting DNS Resolution of CiscoCM1
00:00:05.370 (CFG) DNS Error on Resolving TFTP Server Name.
00:00:05.370 (CFG) TFTP Server IP Set by DHCP Option 150 = 10.123.9.2
00:00:05.370 (CFG) Requesting SAA00107B0013DE.cnf File From TFTP Server
00:00:05.370 (CFG) TFTP Error: .cnf File Not Found!
00:00:05.370 (CFG) Requesting SAADefault.cnf File From TFTP Server
00:00:05.380 (CFG) .cnf File Received and Parsed Successfully.
00:00:05.380 (CFG) Updating Configuration ROM...
00:00:05.610 MSG: GWEvent = CFG_DONE --> GWState = SrchActive
00:00:05.610 MSG: CCM#0 CPEvent = CONNECT_REQ --> CPState = AttemptingSocket
00:00:05.610 MSG: Attempting TCP socket with CM 10.123.9.2
00:00:05.610 MSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = BackupUnified CM
00:00:05.610 MSG: GWEvent = SOCKET_ACK --> GWState = RegActive
00:00:05.610 MSG: CCM#0 CPEvent = REGISTER_REQ --> CPState = SentRegister
00:00:05.680 MSG: CCM#0 CPEvent = CLOSED --> CPState = NoTCPsocket
00:00:05.680 MSG: GWEvent = DISCONNECT --> GWState = Rollover
00:00:20.600 MSG: GWEvent = TIMEOUT --> GWState = SrchActive
00:00:20.600 MSG: CCM#0 CPEvent = CONNECT_REQ --> CPState = AttemptingSocket
00:00:20.600 MSG: Attempting TCP socket with CM 10.123.9.2
00:00:20.600 MSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = Backup CCM
```

登録に関する別の問題としては、ロード情報が正しくないこと、またはロードファイルが破損していることが考えられます。この問題は、TFTP サーバが稼働していない場合にも発生する可能性があります。この場合、ファイルが見つからないという TFTP サーバからの報告が Tracy によって次のように表示されます。

```
00:00:07.390 MSG: CCM#0 CPEvent = REGISTER_REQ --> CPState = SentRegister
00:00:08.010 MSG: TFTP Request for application load A0021300
00:00:08.010 MSG: CCM#0 CPEvent = LOADID --> CPState = AppLoadRequest
00:00:08.010 MSG: ***TFTP Error: File Not Found***
00:00:08.010 MSG: CCM#0 CPEvent = LOAD_UPDATE --> CPState = LoadResponse
```

この場合、正しいアプリケーションロード名がA0020300であるにもかかわらず、ゲートウェイはアプリケーションロードA0021300を要求しています。Catalyst 6000ゲートウェイでは、新しいアプリケーションロードがそれに対応するDSPロードも取得する必要がある場合、同じ問題が発生する可能性があります。新しいDSPロードが見つからない場合、類似のメッセージが表示されます。

```

ELVIS>> 00:00:00.020 (XA) MAC Addr : 00-10-7B-00-13-DE
00:00:00.050 NMPTask:got message from XA Task
00:00:00.050 (NMP) Open TCP Connection ip:7f010101
00:00:00.050 NMPTask:Send Module Slot Info
00:00:00.060 NMPTask:get DIAGCMD
00:00:00.160 (DSP) Test Begin -> Mask<0x00FFFFFF>
00:00:01.260 (DSP) Test Complete -> Results<0x00FFFFFF/0x00FFFFFF>
00:00:01.260 NMPTask:get VLANCONFIG
00:00:02.030 (CFG) Starting DHCP
00:00:02.030 (CFG) Booting DHCP for dynamic configuration.
00:00:05.730 (CFG) DHCP Request or Discovery Sent, DHCPState = INIT_REBOOT
00:00:05.730 (CFG) DHCP Server Response Processed, DHCPState = BOUND
00:00:05.730 (CFG) Requesting DNS Resolution of CiscoCM1
00:00:05.730 (CFG) DNS Error on Resolving TFTP Server Name.
00:00:05.730 (CFG) TFTP Server IP Set by DHCP Option 150 = 10.123.9.2
00:00:05.730 (CFG) Requesting SAA00107B0013DE.cnf File From TFTP Server
00:00:05.730 (CFG) .cnf File Received and Parsed Successfully.
00:00:05.730 MSG: GWEvent = CFG_DONE --> GWState = SrchActive
00:00:05.730 MSG: CCM#0 CPEvent = CONNECT_REQ --> CPState = AttemptingSocket
00:00:05.730 MSG: Attempting TCP socket with CM 10.123.9.2
00:00:05.730 MSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = Backup CCM
00:00:05.730 MSG: GWEvent = SOCKET_ACK --> GWState = RegActive
00:00:05.730 MSG: CCM#0 CPEvent = REGISTER_REQ --> CPState = SentRegister
00:00:06.320 MSG: CCM#0 CPEvent = LOADID --> CPState = LoadResponse
00:01:36.300 MSG: CCM#0 CPEvent = TIMEOUT --> CPState = BadUnified CM
00:01:36.300 MSG: GWEvent = DISCONNECT --> GWState = Rollover
00:01:46.870 MSG: CCM#0 CPEvent = CLOSED --> CPState = NoTCPSToken
00:01:51.300 MSG: GWEvent = TIMEOUT --> GWState = SrchActive
00:01:51.300 MSG: CCM#0 CPEvent = CONNECT_REQ --> CPState = AttemptingSocket
00:01:51.300 MSG: Attempting TCP socket with CM 10.123.9.2
00:01:51.300 MSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = Backup CCM
00:01:51.300 MSG: GWEvent = SOCKET_ACK --> GWState = RegActive
00:01:51.300 MSG: CCM#0 CPEvent = REGISTER_REQ --> CPState = SentRegister
00:01:51.890 MSG: Unified CM#0 CPEvent = LOADID --> CPState = LoadResponse

```

ここでの相違点は、ゲートウェイが **LoadResponse** の段階に留まっているために、最終的にはタイムアウトすることです。この問題は、Cisco Unified Communications Manager の管理ページの [ デバイスのデフォルト設定 ( Device Defaults Configuration ) ] ウィンドウでロードファイル名を修正することで解決できます。

## ゲートキーパーの問題

ゲートキーパーのトラブルシューティングを開始する前に、ネットワーク内に IP 接続が存在することを確認してください。IP 接続が存在する場合は、この項にある次の情報を参照してゲートキーパー コールのトラブルシューティングを行ってください。

- [アドミッション拒否 \(P.4-21\)](#)
- [登録拒否 \(P.4-21\)](#)

### アドミッション拒否

#### 症状

Cisco Unified Communications Manager がゲートキーパーに登録されていてもコールを送信できない場合に、Admission Reject (ARJ; アドミッション拒否) が発行されます。

#### 考えられる原因

ゲートキーパーが ARJ を発行している場合は、特にゲートキーパーの設定の問題に注目する必要があります。

#### 推奨処置

1. Cisco Unified Communications Manager からゲートキーパーへの IP 接続を確認します。
2. ゲートキーパーのステータスを表示し、ゲートキーパーが動作していることを確認します。
3. ゲートキーパーにゾーン サブネットが定義されていることを確認します。定義されている場合は、許可されたサブネットに Cisco Unified Communications Manager のサブネットが含まれていることを確認します。
4. Cisco Unified Communications Manager とゲートキーパー設定との間でテクノロジー プレフィックスが一致していることを確認します。
5. 帯域幅の設定を確認します。

### 登録拒否

#### 症状

Cisco Unified Communications Manager がゲートキーパーに登録できない場合に、Registration Reject (RRJ; 登録拒否) が発行されます。

#### 考えられる原因

ゲートキーパーが RRJ を発行している場合は、特にゲートキーパーの設定の問題に注目する必要があります。

#### 推奨処置

1. Cisco Unified Communications Manager からゲートキーパーへの IP 接続を確認します。
2. ゲートキーパーのステータスを表示し、ゲートキーパーが動作していることを確認します。
3. ゲートキーパーにゾーン サブネットが定義されていることを確認します。定義されている場合は、許可されたサブネットにゲートウェイのサブネットが含まれていることを確認します。

## Restart\_Ack に Channel IE が含まれていない場合に B チャンネルがロックされたままになる

### 症状

Cisco Unified Communications Manager システムは、ie=channel not available という理由付きの Release Complete を受信すると、Restart を送信してこのチャンネルをアイドル状態に戻します。

### 考えられる原因

Restart 内で、Channel IE を使用して、再起動する必要があるチャンネルを指定しています。ネットワークが Channel IE を含めずに Restart\_Ack で応答した場合、システムはこのチャンネルがロックされた状態を維持します。ネットワーク側では、この同じチャンネルがアイドル状態に戻ります。

その結果、ネットワークは着信コール用にこのチャンネルを要求することになります。

チャンネルは Cisco Unified Communications Manager サーバ上でロックされているので、Cisco Unified Communications Manager はこのチャンネルに対するコール要求をすべて解放します。

この動作は、ゲートウェイが E1 ブレードの場合、イギリスの多数のサイトで発生します (MGCP バックホールを 2600/3600 上で使用している場合も同じ動作が発生する可能性があります)。

グレア状態は、Release Complete が送信される理由であると考えられます。

これは大量のコールがあるサイトで頻繁に発生します。

ネットワークでの B チャンネルの選択がトップダウンまたはボトムアップの場合、すべての着信コールは、上位または下位の B チャンネルが解放されるまで成功しません (アクティブ コールがクリアされた場合)。

B チャンネルの選択が一定時間のラウンドロビンの場合、E1 ブレードのすべての B チャンネルがロックされる結果になります。

### 推奨処置

E1 ポートをリセットします。

### 確認

B チャンネルはアイドル状態に戻ります。



## ダイヤルプランとルーティングの問題

この章では、ダイヤルプラン、ルートパーティション、およびコーリングサーチスペースで発生する可能性のある、次のような一般的な問題について説明します。

- ルートパーティションとコーリングサーチスペース
- グループピックアップ設定
- ダイヤルプランの問題

### ルートパーティションとコーリングサーチスペース

ルートパーティションは、Cisco Unified Communications Manager ソフトウェアのエラー処理機能を継承します。つまり、情報メッセージとエラーメッセージをログに記録するために、コンソールおよびSDI ファイルトレースが提供されます。これらのメッセージは、トレースの番号分析コンポーネントの一部となります。問題の原因を特定するには、パーティションとコーリングサーチスペースがどのように設定されているか、各パーティションおよびそのパーティションに関連付けられているコーリングサーチスペースにどのようなデバイスがあるかを把握しておく必要があります。コーリングサーチスペースにより、コールの発信にどの番号を使用できるかが決まります。パーティションにより、デバイスまたはルートリストへの許可されるコールが決まります。

詳細については、『Cisco Unified Communications Manager アドミニストレーションガイド』および『Cisco Unified Communications Manager システムガイド』のルートプランに関する章を参照してください。

次のトレースは、デバイスのコーリングサーチスペース内にある番号がダイヤルされる例を示しています。SDIトレースの詳細については、本書のケーススタディを参照してください。

```
08:38:54.968 CCM Communications Manager|StationInit - InboundStim - OffHookMessageID
tcpHandle=0x6b88028
08:38:54.968 CCM CallManager|StationD - stationOutputDisplayText tcpHandle=0x6b88028,
Display= 5000
08:38:54.968 CCM CallManager|StationD - stationOutputSetLamp stim: 9=Line instance=1
lampMode=LampOn tcpHandle=0x6b88028
08:38:54.968 CCM CallManager|StationD - stationOutputCallState tcpHandle=0x6b88028
08:38:54.968 CCM CallManager|StationD - stationOutputDisplayPromptStatus
tcpHandle=0x6b88028
08:38:54.968 CCM CallManager|StationD - stationOutputSelectSoftKeys
tcpHandle=0x6b88028
08:38:54.968 CCM CallManager|StationD - stationOutputActivateCallPlane
tcpHandle=0x6b88028
08:38:54.968 CCM CallManager|Digit analysis: match(fqcn="5000", cn="5000",
pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="")
```

上記のトレースの番号分析コンポーネントでは、コールを発信するデバイスの pss (パーティション検索スペース。コーリングサーチスペースとも呼ばれる) が表示されています。

次のトレースにおいて、RTP\_NC\_Hardwood;RTP\_NC\_Woodland;Local\_RTP は、このデバイスがコールできるパーティションを示しています。

```
08:38:54.968 CCM CallManager|Digit analysis: potentialMatches=PotentialMatchesExist
08:38:54.968 CCM CallManager|StationD - stationOutputStartTone: 33=InsideDialTone
tcpHandle=0x6b88028
08:38:55.671 CCM CallManager|StationInit - InboundStim - KeypadButtonMessageID
kpButton: 5 tcpHandle=0x6b88028
08:38:55.671 CCM CallManager|StationD - stationOutputStopTone tcpHandle=0x6b88028
08:38:55.671 CCM CallManager|StationD - stationOutputSelectSoftKeys
tcpHandle=0x6b88028
08:38:55.671 CCM CallManager|Digit analysis: match(fqcn="5000", cn="5000",
pss="RTP_NC_Hardwood;RTP_NC_Woodland;Local RTP", dd="5")
08:38:55.671 CCM CallManager|Digit analysis: potentialMatches=PotentialMatchesExist
08:38:56.015 CCM CallManager|StationInit - InboundStim - KeypadButtonMessageID
kpButton: 0 tcpHandle=0x6b88028
08:38:56.015 CCM CallManager|Digit analysis: match(fqcn="5000", cn="5000",
pss="RTP_NC_Hardwood;RTP_NC_Woodland;Local RTP", dd="50")
08:38:56.015 CCM CallManager|Digit analysis: potentialMatches=PotentialMatchesExist
08:38:56.187 CCM CallManager|StationInit - InboundStim - KeypadButtonMessageID
kpButton: 0 tcpHandle=0x6b88028
08:38:56.187 CCM CallManager|Digit analysis: match(fqcn="5000", cn="5000",
pss="RTP_NC_Hardwood;RTP_NC_Woodland;Local RTP", dd="500")
08:38:56.187 CCM CallManager|Digit analysis: potentialMatches=PotentialMatchesExist
08:38:56.515 CCM CallManager|StationInit - InboundStim - KeypadButtonMessageID
kpButton: 3 tcpHandle=0x6b88028
08:38:56.515 CCM CallManager|Digit analysis: match(fqcn="5000", cn="5000",
pss="RTP_NC_Hardwood;RTP_NC_Woodland;Local RTP", dd="5003")
08:38:56.515 CCM CallManager|Digit analysis: analysis results
08:38:56.515 CCM CallManager||PretransformCallingPartyNumber=5000
```

PotentialMatchesExist は、完全な一致が見つかり、それに従ってコールがルーティングされるまでの間にダイヤルされた番号に関する番号分析の結果であることに注意してください。

次のトレースは、Cisco Unified Communications Manager が電話番号 1001 をダイヤルしようとしているときに、その番号がそのデバイスのコーリングサーチスペースにない場合の処理を示しています。この場合も、最初の番号がダイヤルされるまでの間に番号分析ルーチンが一致の候補を処理していることに注意してください。番号 1 に関連付けられているルートパターンは、デバイスのコーリングサーチスペース RTP\_NC\_Hardwood;RTP\_NC\_Woodland;Local\_RTP 以外のパーティションに存在します。したがって、電話機はリオーダー音（話し中の音）を受信します。

```
08:38:58.734 CCM CallManager|StationInit - InboundStim - OffHookMessageID
tcpHandle=0x6b88028
08:38:58.734 CCM CallManager|StationD - stationOutputDisplayText tcpHandle=0x6b88028,
Display= 5000
08:38:58.734 CCM CallManager|StationD - stationOutputSetLamp stim: 9=Line instance=1
lampMode=LampOn tcpHandle=0x6b88028
08:38:58.734 CCM CallManager|StationD - stationOutputCallState tcpHandle=0x6b88028
08:38:58.734 CCM CallManager|StationD - stationOutputDisplayPromptStatus
tcpHandle=0x6b88028
08:38:58.734 CCM CallManager|StationD - stationOutputSelectSoftKeys
tcpHandle=0x6b88028
08:38:58.734 CCM CallManager|StationD - stationOutputActivateCallPlane
tcpHandle=0x6b88028
08:38:58.734 CCM CallManager|Digit analysis: match(fqcn="5000", cn="5000",
pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="")
08:38:58.734 CCM CallManager|Digit analysis: potentialMatches=PotentialMatchesExist
08:38:58.734 CCM CallManager|StationD - stationOutputStartTone: 33=InsideDialTone
tcpHandle=0x6b88028
08:38:59.703 CCM CallManager|StationInit - InboundStim - KeypadButtonMessageID
kpButton: 1 tcpHandle=0x6b88028
08:38:59.703 CCM CallManager|StationD - stationOutputStopTone tcpHandle=0x6b88028
08:38:59.703 CCM CallManager|StationD - stationOutputSelectSoftKeys
tcpHandle=0x6b88028
08:38:59.703 CCM CallManager|Digit analysis: match(fqcn="5000", cn="5000",
pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="1")
08:38:59.703 CCM CallManager|Digit analysis: potentialMatches=NoPotentialMatchesExist
08:38:59.703 CCM CallManager|StationD - stationOutputStartTone: 37=ReorderTone
tcpHandle=0x6b88028
```

ルートパーティションは、パーティション名をシステム内の各電話番号に関連付けることによって機能します。その電話番号をコールできるのは、コールの発信先として許可されているパーティションのリスト（パーティション検索スペース）内のパーティションが発信側のデバイスに含まれている場合だけです。この動作によって、きわめて強力的にルーティングを制御できます。

コールが発信されると、番号分析により、パーティション検索スペースで指定されているパーティションだけで、ダイヤルされたアドレスの解決が試行されます。各パーティション名は、ダイヤル可能なグローバルアドレススペースの個々のサブセットで構成されています。番号分析では、一覧表示されている各パーティションから、ダイヤルされた一連の番号と一致するパターンが取得されます。その後、番号分析では、一致するパターンの中から、一致度の最も高いものが選択されます。2つのパターンで、ダイヤルされた一連の番号に対する一致度が等しい場合、番号分析では、パーティション検索スペースに最初に記載されているパーティションに関連付けられているパターンが選択されます。

## グループピックアップ設定

### 症状

パーティションを設定されているグループで、グループピックアップ機能が動作しません。

### 考えられる原因

グループ内の各 Directory Number (DN; 電話番号) の Calling Search Space (CSS; コーリングサーチスペース) が、正しく設定されていない可能性があります。

### 例

次の手順は、パーティショニングがある場合の正しいグループピックアップ設定の例を示しています。

1. Marketing/5656 という名前のグループを設定します。ここで *Marketing* はパーティションで、*5656* はピックアップ番号です。
2. DN 6000 および 7000 の設定で、これらの DN をそれぞれ *Marketing/5656* という名前のピックアップグループに追加します。

### 推奨処置

グループピックアップが失敗する場合は、各ドメイン名(この例では DN 6000 および 7000)の CSS を確認します。この例で、*Marketing* という名前のパーティションがそれぞれの CSS に含まれていない場合は、設定が誤っているためにピックアップが失敗した可能性があります。

## ダイヤルプランの問題

この項では、次のようなダイヤルプランの問題について説明します。

- [番号をダイヤルするときの問題](#)
- [安全なダイヤルプラン](#)

### 番号をダイヤルするときの問題

#### 症状

番号をダイヤルするときに問題が発生します。

#### 考えられる原因

ダイヤルプランは、番号および番号グループのリストで構成されます。このリストは、特定の番号列が収集されるときに、コールの送信先となるデバイス（電話機やゲートウェイなど）を Cisco Unified Communications Manager に知らせます。このステップはルータのスタティックルーティングテーブルに類似していると考えてください。

ダイヤルプランに関連すると思われる問題のトラブルシューティングを行う前に、ダイヤルプランの概念、基本的なコールルーティング、およびプランニングが入念に検討され正しく設定されていることを確認してください。多くの場合、プランニングと設定に問題があります。詳細については、『Cisco Unified Communications Manager アドミニストレーションガイド』のルートプランの設定に関する章を参照してください。

#### 推奨処置

1. コールを発信している Directory Number (DN; 電話番号) を識別します。
2. その DN のコーリングサーチスペースを識別します。



**ヒント** コーリングサーチスペースにより、コールの発信にどの番号を使用できるかが決まります。

3. 該当する場合、コーリングサーチスペースでこの DN に関連付けられているデバイスを識別します。必ず正しいデバイスを識別してください。複数ラインアピアランスがサポートされているため、複数のデバイスに同じ DN が設定されている場合があります。デバイスのコーリングサーチスペースを把握します。

コールの発信元が Cisco Unified IP Phone である場合は、特定の回線 (DN) およびその回線が関連付けられているデバイスがコーリングサーチスペースを持つことに注意してください。コールの発信時に、コーリングサーチスペースが結合されます。たとえば、回線インスタンス 1000 がコーリングサーチスペース AccessLevelX を持ち、内線番号が 1000 に設定されている Cisco Unified IP Phone がコーリングサーチスペース AccessLevelY を持つ場合、そのラインアピアランスからコールを発信すると、Cisco Unified Communications Manager はコーリングサーチスペース AccessLevelX と AccessLevelY に含まれるパーティションを検索します。

4. コーリングサーチスペースに関連付けられているパーティションを識別します。



**ヒント** パーティションにより、デバイスまたはルートリストへの許可されるコールが決まります。

5. デバイスのどのパーティションにコールが発信されるか（または発信されないか）を識別します。
6. ダイアルされている番号を識別します。ユーザが2つ目の発信音を聞いたかどうか、聞いた場合はいつ聞いたかを把握します。すべての番号を入力した後にユーザには何が聞こえるか（リオーダー、速いビジー音）にも注意します。その前に、ユーザにプログレス トーンが聞こえるかどうかを確認します。発信者は、番号間タイマーが切れるのを待たなければならないことがあるため、最後の番号を入力してから少なくとも 10 秒間待つ必要があります。
7. Cisco Unified Communications Manager の管理ページでルート プラン レポートを生成し、そのレポートを使用して、問題のコールのコーリング サーチ スペース内にあるパーティションのすべてのルート パターンを調べます。
8. 必要に応じて、ルート パターンまたはルート フィルタを追加または変更します。
9. コールの送信先のルート パターンを検出できる場合は、そのパターンが指すルート リストまたはゲートウェイを把握します。
10. それがルート リストである場合、どのルート グループがそのリストに含まれているか、およびどのゲートウェイがそのルート グループに含まれているかを確認します。
11. 適切なデバイスが Cisco Unified Communications Manager に登録されていることを確認します。
12. ゲートウェイが Cisco Unified Communications Manager にアクセスできない場合は、show tech コマンドを使用して、その情報を取り込んで確認します。
13. @ 記号に注意します。このマクロは、多くの異なる機能を含むように展開できます。これは、多くの場合、フィルタリング オプションと組み合わせて使用されます。
14. デバイスがパーティションに含まれていない場合、そのデバイスはヌル パーティションまたはデフォルト パーティションに含まれていると見なします。すべてのユーザが、そのデバイスにコールできます。システムは、常に、ヌル パーティションを最後に検索します。
15. 9.@ パターンに一致する外線番号にダイヤルし、コールが通じるまでに 10 秒かかる場合は、フィルタリング オプションを確認します。デフォルトでは、9.@ パターンを使用する場合、7桁の番号がダイヤルされると、Cisco Unified IP Phone は 10 秒待ってからコールを発信します。LOCAL-AREA-CODE DOES-NOT- EXIST および END-OF-DIALING DOES-NOT-EXIST と表示されるパターンにルート フィルタを適用する必要があります。

## 安全なダイヤルプラン

ユーザ向けに安全なダイヤルプランを作成するように Cisco Unified Communications Manager を設定するには、パーティションとコーリング サーチ スペースに加え、ルート パターン内の @ マクロ (North American Numbering Plan を意味する) のセクションに基づく一般的なフィルタリングを使用します。パーティションとコーリング サーチ スペースはセキュリティに不可欠であり、特に、マルチテナント環境や、個々のユーザ レベルの作成に役立ちます。コーリング サーチ スペースおよびパーティションの概念のサブセットであるフィルタリングにより、セキュリティ プランをさらに綿密にすることができます。

通常は、フィルタリングの問題を解決する手段として SDI トレースを実行することはお勧めできません。このトレースでは、十分な情報が得られないうえ、問題が悪化する可能性が非常に高くなります。



# Cisco Unified Communications Manager サービスの問題

この項では、Cisco Unified Communications Manager サービスに関連する、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。

- 使用可能な会議ブリッジがない (P.6-1)
- ハードウェア トランスコーダが期待どおりに機能しない (P.6-3)
- 確立されたコールで補助的なサービスが使用できない (P.6-5)

## 使用可能な会議ブリッジがない

### 症状

「会議ブリッジがありません」というメッセージが表示されます。

### 考えられる原因

これは、ソフトウェアまたはハードウェアのいずれかに問題があることを示している可能性があります。

### 推奨処置

1. Cisco Unified Communications Manager に登録されている使用可能なソフトウェアまたはハードウェアの会議ブリッジ リソースがあるかどうかを確認します。
2. Cisco Unified Communications Manager Real-Time Monitoring Tool を使用して、Unicast AvailableConferences の数を確認します。

Cisco IP Voice Media Streaming アプリケーションは、会議ブリッジ機能を実行します。次のトレースに示されているように、Cisco IP Voice Media Streaming の 1 つのソフトウェア インストールは、16 個の Unicast Available Conferences (3 人 / 会議) をサポートします。



(注) サポートされるデバイスの数は、Cisco Unified Communications Manager のリリースによって異なる場合があります。

[http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_callmg/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm) で、該当するバージョンの Cisco Unified Communications Manager のマニュアルを参照してください。

## ■ 使用可能な会議ブリッジがない

```
10:59:29.951 CCM CallManager|UnicastBridgeControl - wait_capabilities_StationCapRes
- Device= CFB_kirribilli - Registered - ConfBridges= 16, Streams= 48,
tcpHandle=4f12738
10:59:29.951 CCM CallManager|UnicastBridgeManager - UnicastBridgeRegistrationReq -
Device Registration Complete for Name= Xoð ô%ð - DeviceType= 50,
ResourcesAvailable= 16, deviceTblIndex= 0
```

次のトレースに示されているように、1 個の E1 ポート ( WS-X6608-E1 カードには 8 個の E1 ポートがあります ) は、5 個の Unicast Available Conferences( 最大会議サイズ = 6 ) を提供します。

```
11:14:05.390 CCM CallManager|UnicastBridgeControl - wait_capabilities_StationCapRes
- Device= CFB00107B000FB0 - Registered - ConfBridges= 5, Streams= 16,
tcpHandle=4f19d64
11:14:05.480 CCM CallManager|UnicastBridgeManager - UnicastBridgeRegistrationReq -
Device Registration Complete for Name= Xoð ô%ð - DeviceType= 51,
ResourcesAvailable= 5, deviceTblIndex= 0
```

次の Cisco Catalyst 6000 8 Port Voice T1/E1 および Services Module のハードウェア トレースは、カードの E1 ポート 4/1 が会議ブリッジとして Cisco Unified Communications Manager に登録されていることを示しています。

```
greece-sup (enable) sh port 4/1
Port Name Status Vlan Duplex Speed Type
-----
4/1 enabled 1 full -Conf Bridge

Port DHCP MAC-Address IP-Address Subnet-Mask
-----
4/1 disable 00-10-7b-00-0f-b0 10.200.72.31 255.255.255.0

Port Call-Manager(s) DHCP-Server TFTP-Server Gateway
-----
4/1 10.200.72.25 - 10.200.72.25 -

Port DNS-Server(s) Domain
-----
4/1 - 0.0.0.0

Port CallManagerState DSP-Type
-----
4/1 registered C549

Port NoiseRegen NonLinearProcessing
-----
4/1 disabled disabled
```

- Ad Hoc 会議または Meet-Me 会議に設定されている最大ユーザ数を調べて、この数を超過したために問題が発生したかどうかを確認します。
- [ ロケーションの設定 ( Location Configuration ) ] ウィンドウの [ オーディオ帯域幅 ( Audio Bandwidth ) ] フィールドの設定を確認します。コールの帯域幅がこの設定済みの制限値を超えると、会議は失敗します。この問題を解決するには、[ 無制限 ( Unlimited ) ] オプション ボタンを選択します。[ ロケーションの設定 ( Location Configuration ) ] ウィンドウの詳細については、『Cisco Unified Communications Manager アドミニストレーション ガイド』を参照してください。

## ハードウェア トランスコーダが期待どおりに機能しない

### 症状

Cisco Catalyst 6000 8 Port Voice T1/E1 および Services Module にインストールしたハードウェア トランスコーダが期待どおりに機能しません (共通のコーデックを持たない2人のユーザ間でコールを発信できません)。

### 考えられる原因

Cisco Unified Communications Manager に登録された使用可能なトランスコーダ リソース (ハードウェア) がない可能性があります。

### 推奨処置

Cisco Unified Communications Manager Real-Time Monitoring Tool を使用し、Cisco MTP Device オブジェクト内の ResourceAvailable カウンタを表示して、使用可能なリソースの数を確認します。

次のトレースに示されているように、1 個の E1 ポート (WS-X6608-E1 カードには 8 個の E1 ポートがあります) は、16 件のコールに対応するトランスコーダ /MTP リソースを提供します。



(注) サポートされるデバイスの数は、Cisco Unified Communications Manager のリリースによって異なる場合があります。  
[http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_callmg/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm) で、該当するバージョンの Cisco Unified Communications Manager のマニュアルを参照してください。

```
11:51:09.939 CCM CallManager|MediaTerminationPointControl - Capabilities Received -
Device= MTP00107B000FB1 - Registered - Supports 16 calls
```

次の Cisco Catalyst 6000 8 Port Voice T1/E1 および Services Module のハードウェア トレースは、カードの E1 ポート 4/2 が MTP/ トランスコーダとして Cisco Unified Communications Manager に登録されていることを示しています。

```
greece-sup (enable) sh port 4/2
Port Name Status Vlan Duplex Speed Type
-----
4/2 enabled 1 full - MTP

Port DHCP MAC-Address IP-Address Subnet-Mask
-----
4/2 disable 00-10-7b-00-0f-b1 10.200.72.32 255.255.255.0

Port Call-Manager(s) DHCP-Server TFTP-Server Gateway
-----
4/2 10.200.72.25 - 10.200.72.25 -

Port DNS-Server(s) Domain
-----
4/2 - 0.0.0.0

Port CallManagerState DSP-Type
-----
4/2 registered C549

Port NoiseRegen NonLinearProcessing
-----
4/2 disabled disabled
```



(注) 会議ブリッジとトランスコーダ /MTP の両方に同一の E1 ポートを設定することはできません。

ビットレートの低いコード (G.729 や G.723 など) を使用していて、同一のコーデックをサポートしていない 2 つのデバイス間でコールを発信するには、トランスコーダ リソースが必要です。

Region1 と Region2 間のコーデックが G.729 になるように Cisco Unified Communications Manager が設定されていると仮定します。この場合、次のシナリオが該当します。

- 発信者が Phone A でコールを開始した場合、Cisco Unified Communications Manager は G.729 をサポートする Cisco Unified IP Phone 7960 モデルであると認識します。番号が収集された後に、Cisco Unified Communications Manager は、コールの宛先が Region2 にいる User D であると判別します。宛先デバイスも G.729 をサポートしているため、コールが確立され、音声は Phone A と Phone D 間を直接流れます。
- Cisco Unified IP Phone 12SP+ モデルの Phone B で発信者が Phone D に対するコールを開始した場合、Cisco Unified Communications Manager は、発信側の電話機が G.723 または G.711 だけをサポートすると認識します。Phone B とトランスコーダ間は G.711 として、Phone D とトランスコーダ間は G.729 として、それぞれ音声が行くように、Cisco Unified Communications Manager はトランスコーディング リソースを割り当てる必要があります。使用可能なトランスコーダがない場合、Phone D では呼び出し音が鳴りますが、そこで応答すると、そのコールはすぐに接続解除されます。
- Phone B で Cisco Unified IP Phone 12SP+ モデルの Phone F にコールを発信した場合は、そのリージョン間で使用されるコーデックとして G.729 が設定されていても、この 2 台の電話機は G.723 を使用します。G.723 が使用されるのは、両方のエンドポイントで G.723 がサポートされており、G.729 よりも小さい帯域幅を使用するためです。

## 確立されたコールで補助的なサービスが使用できない

### 症状

コールは確立されますが、補助的なサービスが使用できません。

### 考えられる原因

コールが確立されていても、H323v2 をサポートしない H.323 デバイスで補助的なサービスが使用できない場合は、MTP リソースの問題がトランスコーディングの問題の原因になっている可能性があります。

### 推奨処置

1. Cisco Unified Communications Manager に登録されている使用可能なソフトウェアまたはハードウェアの MTP リソースがあるかどうかを確認します。
2. Cisco Unified Communications Manager Real-Time Monitoring Tool のパフォーマンス モニタリングを使用して、使用可能な MTP デバイスの数を確認します。

次のトレースに示されているように、H.323v2 をサポートしない H.323 デバイスで MTP を使用して補助的なサービスをサポートすると、1 つの MTP ソフトウェア アプリケーションが 24 件のコールをサポートできます。



**(注)** サポートされるデバイスの数は、Cisco Unified Communications Manager のリリースによって異なる場合があります。

[http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_callmg/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm) で、該当するバージョンの Cisco Unified Communications Manager のマニュアルを参照してください。

```
10:12:19.161 CCM CallManager|MediaTerminationPointControl - Capabilities Received -  
Device= MTP_kirribilli. - Registered - Supports 24 calls
```

次のトレースに示されているように、1 個の E1 ポート (WS-X6608-E1 カードには 8 個の E1 ポートがあります) は、16 件のコールに対応する MTP リソースを提供します。

```
11:51:09.939 CCM CallManager|MediaTerminationPointControl - Capabilities Received -  
Device= MTP00107B000FB1 - Registered - Supports 16 calls
```

## ■ 確立されたコールで補助的なサービスが使用できない

次の Cisco Catalyst 6000 8 Port Voice T1/E1 および Services Module のハードウェア トレースは、カードの E1 ポート 4/2 が MTP/ トランスコーダとして Cisco Unified Communications Manager に登録されていることを示しています。

```
greece-sup (enable) sh port 4/2
Port Name Status Vlan Duplex Speed Type
-----
4/2 enabled 1 full - MTP

Port DHCP MAC-Address IP-Address Subnet-Mask
-----
4/2 disable 00-10-7b-00-0f-b1 10.200.72.32 255.255.255.0

Port Call-Manager(s) DHCP-Server TFTP-Server Gateway
-----
4/2 10.200.72.25 - 10.200.72.25 -

Port DNS-Server(s) Domain
-----
4/2 - 0.0.0.0

Port CallManagerState DSP-Type
-----
4/2 registered C549

Port NoiseRegen NonLinearProcessing
-----
4/2 disabled disabled
```

3. Cisco Unified Communications Manager の管理ページの[ ゲートウェイの設定( Gateway Configuration ) ] ウィンドウで、[ **メディアターミネーションポイントが必須 (Media Termination Point Required)** ] チェックボックスがオンになっているかどうかを確認します。
4. Cisco Unified Communications Manager が必要な数の MTP デバイスを割り当てていることを確認します。



## ボイス メッセージの問題

---

この章では、ボイス メッセージに関連する、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。

- 30 秒経過するとボイス メッセージが停止する (P.7-2)
- Cisco Unity がロール オーバーせずにビジー音が聞こえる (P.7-2)
- ボイス メッセージ システムに転送されたコールが Cisco Unity に対する直接コールとして処理される (P.7-3)
- 管理者アカウントが Cisco Unity サブスクリバに関連付けられていない (P.7-4)

Cisco Unity ボイス メッセージに関する広範なトラブルシューティング情報については、次の URL で『Cisco Unity トラブルシューティング ガイド』を参照してください。

[http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod\\_troubleshooting\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_troubleshooting_guides_list.html)

Cisco Unity に関連するすべてのマニュアルについては、次の URL を参照してください。

[http://www.cisco.com/en/US/products/sw/voicesw/ps2237/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/sw/voicesw/ps2237/tsd_products_support_series_home.html)

## 30 秒経過するとボイスメッセージが停止する

### 症状

Cisco Unified Communications Manager と連動して Cisco Unity を実行している場合に、ボイスメールメッセージを残すための時間が発信者に 30 秒しか与えられていません。

### 考えられる原因

この問題は、発信者がボイスメッセージを残そうとしているときに発生し、メッセージ開始から 30 秒でコールが強制終了されます。有効な内線番号または電話番号をダイヤルし、30 秒より長いボイスメッセージを残そうとすることで、これは簡単に再現できます。

### 推奨処置

1. この問題を解決するには、Media Gateway Control Protocol (MGCP; メディアゲートウェイコントロールプロトコル) が音声ゲートウェイで使用されていることを確認します。
2. MGCP が使用されている場合は、`no mgcp timer receive-rtcp` コマンドを追加します。
3. MGCP が音声ゲートウェイで使用されていない場合は、Cisco Unity サーバに対する Skinny トレースと Cisco Communications Manager トレースを有効にします。

Cisco Unity 診断トレースの設定については、次の URL で、該当する『Cisco Unity トラブルシューティングガイド』の「診断トレースユーティリティとログ」の項を参照してください。  
[http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod\\_troubleshooting\\_guides\\_list.html#3](http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_troubleshooting_guides_list.html#3)

## Cisco Unity がロールオーバーせずにビジー音が聞こえる

### 症状

Cisco Unity が最初の回線を通過せず、2 番目のポートにロールオーバーしません。

### 例

```
Call 5000 from 1001
Get Unity
Place the call on Hold
Press New Call
Dial 5000
Get Busy tone
Press End Call
Press Resume Call
Press End Call
```

### 考えられる原因

Cisco Messaging Interface (CMI) サービスが Cisco Unity と同じ番号 (5000) で設定されており、代行受信を登録中であるため、コールが CMI にヒットしています。

### 推奨処置

CMI サービスのパラメータを調べて、`voicemaildn` パラメータが設定されていないことを確認します。

## ボイスメッセージシステムに転送されたコールが Cisco Unity に対する直接コールとして処理される

### 症状

ある Cisco Unified IP Phone から別の IP Phone へのコールがボイスメッセージシステムに転送されると、そのコールは発信側の電話機から Cisco Unity への直接コールとして処理されます。ただし、これは番号がダイヤルされた場合に発生しますが、[リダイヤル]ソフトキーが押された場合には正しく機能しません（着信側電話機のグリーティングを受信します）。

### 考えられる原因

TSP のロジックでは、転送されたコールの場合、originalCalledPartyName が「Voicemail」のときは、そのコールは直接コールと見なされます。これは、Cisco Unified Communications Manager を使用しているフェールオーバー Cisco Unity システムのための動作です。

### 推奨処置

1. Cisco Unified Communications Manager サーバで、Cisco Voice Mail ポートの表示に関するフィールドの名前を「VoiceMail」以外のものに変更します。
2. Unity サーバで、HKLM\Software\ActiveVoice\AvSkinny\voiceMail display Name= *anything other than VoiceMail* という新しい Registry 文字列値を追加します。

## 管理者アカウントが Cisco Unity サブスクリバに関連付けられていない

### 症状

System Administrator ( SA ) ページにアクセスしようとしているとき、管理者アカウントが Unity サブスクリバに関連付けられていないというメッセージが表示されます。

### 考えられる原因

ユーザにアクセス権が設定されていません。

### 推奨処置

1. SA ページに対する適切なアクセス権を取得するには、GrantUnityAccess ユーティリティを実行する必要があります。このツールは C:\commsserver\grantunityaccess.exe にあります。



(注) GrantUnityAccess ユーティリティの詳細については、[http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod\\_troubleshooting\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_troubleshooting_guides_list.html) で、該当する『Cisco Unity システム アドミニストレーションガイド』にある「Cisco Unity システム管理のアカウントの管理」の章の「別の Cisco Unity サーバに対する管理者権限の付与」の項を参照してください。

2. オプションを選択せずにこのユーティリティを実行すると、使用説明が表示されます。このツールを通常の使用方法で実行すると、SA に対するアクセス権が付与されるアカウントのドメインまたはエイリアスが表示され、次に、それらのアクセス権のコピー元となるアカウントに関する情報が表示されます。

たとえば、管理者アクセス権を付与する対象のユーザのエイリアスが TempAdministrator で、自分のドメイン名が MyDOMAIN の場合、DOS プロンプトで次のコマンドを使用します。  
`GrantUnityAccess -u MyDOMAIN\TempAdministrator -s Installer -f`

インストール担当者のアカウントには、常に管理者アクセス権を持つ特別なアカウントが指定されます。ただし、そのアカウントはディレクトリ自体には作成されず、SQL データベース専用のローカルなアカウントになります。



# 機能およびサービスのトラブルシューティング

---

この章では、Cisco Unified Communications Manager の機能およびサービスに関する一般的な問題の解決に役立つ情報を提供します。

- [割り込みのトラブルシューティング \(P.8-2\)](#)
- [コールパークのトラブルシューティング \(P.8-3\)](#)
- [Cisco Call Back のトラブルシューティング \(P.8-3\)](#)
- [Cisco エクステンション モビリティのトラブルシューティング \(P.8-6\)](#)
- [Cisco Unified Communications Manager Assistant のトラブルシューティング \(P.8-9\)](#)
- [Cisco Unified Communications Manager Attendant Console のトラブルシューティング \(P.8-19\)](#)
- [Cisco Web Dialer のトラブルシューティング \(P.8-30\)](#)
- [ダイレクト コールパークのトラブルシューティング \(P.8-33\)](#)
- [即時転送のトラブルシューティング \(P.8-35\)](#)

## 割り込みのトラブルシューティング

この項では、割り込み機能に関連する一般的な問題の解決方法について説明します。

### 症状

[ 割り込み ] ソフトキーを押すと、IP Phone に「会議ブリッジがありません」というメッセージが表示されます。

### 考えられる原因

該当する電話機の [ 電話の設定 ( Phone Configuration ) ] で、[ ビルトインブリッジ ( Built In Bridge ) ] 設定値が正しく設定されていません。

### 対応策

この問題を解決するには、次の手順を実行します。

### 手順

- 
- ステップ 1** Cisco Unified Communications Manager の管理ページで、[ デバイス ] > [ 電話 ] に移動し、問題が発生している電話機の電話設定を見つけます。
  - ステップ 2** [ ビルトインブリッジ ( Built In Bridge ) ] パラメータを On に設定します。
  - ステップ 3** [ 保存 ] をクリックします。
  - ステップ 4** 電話機をリセットします。
-

## コールパークのトラブルシューティング

表 8-1 に、コールパークに関連する一般的な問題のトラブルシューティングリカバリのヒントを示します。

表 8-1 コールパークのトラブルシューティングのヒント

問題の説明	推奨処置
ユーザがコールをパークできない。ユーザが [パーク] ソフトキーまたは機能ボタンを押しても、コールがパークされない。	<p>クラスタ内の各 Cisco Unified Communications Manager に固有のコールパーク番号が割り当てられていることを確認します。『Cisco Unified Communications Manager アドミニストレーションガイド』を参照してください。</p> <p>コールパーク番号に割り当てられたパーティションが、電話機の電話番号に割り当てられたパーティションと一致していません。『Cisco Unified Communications Manager アドミニストレーションガイド』を参照してください。</p>
コールパーク番号の表示時間が短すぎる。	Call Park Display Timer の設定時間を長くします。コールパークのパラメータの設定については、『Cisco Unified Communications Manager 機能およびサービスガイド』を参照してください。

## Cisco Call Back のトラブルシューティング

この項では、Cisco Call Back が期待どおりに機能しない場合の症状、考えられる原因、推奨処置、およびエラーメッセージを示します。この項では、次のトピックについて取り上げます。

- [Cisco Call Back の使用方法に関する問題 \(P.8-3\)](#)
- [Cisco Call Back のエラーメッセージ \(P.8-5\)](#)
- [Cisco Call Back のログファイルの場所 \(P.8-5\)](#)

### Cisco Call Back の使用方法に関する問題

この項では、問題、考えられる原因、推奨処置、およびエラーメッセージ(それぞれの問題に該当するものがある場合)について説明します。

#### 呼び出し音が鳴る前にユーザが折返しソフトキーを押した

##### 症状

コールの最中に、電話機の呼び出し音がまだ鳴っていないにもかかわらず、[折返し] ソフトキーが電話機に表示されることがあります。

##### 考えられる原因

ユーザが適切なタイミングで [折返し] ソフトキーを押していない可能性があります。

##### 対応策

ユーザは、呼び出し音が鳴るか、話し中の音が聞こえてから [折返し] ソフトキーを押す必要があります。このソフトキーを不適切なタイミングで押すと、電話機にエラーメッセージが表示されることがあります。

## 折返しソフトキーを押してから、コールバックが発生する前に、ユーザが電話機のケーブルを抜くか、電話機をリセットした

### 症状 (その 1)

[折返し]ソフトキーが押されてから、Cisco Call Back がアクティブになる前に発信者の電話機のリセットが発生します。

### 考えられる原因

ユーザが電話機をリセットしました。

### 対応策 (その 1)

リセット後に、発信者の電話機にはコールバックがアクティブになったことを示すウィンドウが表示されません。アクティブな Cisco Call Back サービスを発信者が表示するには、[折返し]ソフトキーを押す必要があります。コールバック通知は電話機に表示されます。

### 症状 (その 2)

コールバックがアクティブになった後、着信側が使用可能になる前に発信者の電話機のリセットが発生します。

### 考えられる原因

ユーザが電話機をリセットしました。

### 対応策 (その 2)

対応策を実施する必要はありません。着信側が使用可能になる前にリセットが発生した場合、Cisco Call Back は期待どおりに発生します。

### 症状 (その 3)

コールバックがアクティブになった後に発信者の電話機のリセットが発生しましたが、リセットが発信者の電話機で完了する前に、着信側が使用可能になります。

### 考えられる原因

ユーザが電話機をリセットしました。

### 対応策 (その 3)

コールバック通知は、自動的には発生しません。このため、アクティブな Call Back サービスを発信者が表示するには、[折返し]ソフトキーを押す必要があります。

## 発信者が、電話機がリセットされる前の使用可能通知を見逃した。置換 / 保持画面に、使用可能通知が発生したことが明示されない

### 症状

クラスタ内またはクラスタ間のコールバックシナリオで、発信者がユーザ (たとえば、使用不可になっているユーザ B) に対するコールバックを開始します。ユーザ B が使用可能になると、発信者の電話機に使用可能通知画面が表示され、トーンが再生されます。発信者が何らかの理由で使用可能通知を見逃して、電話機がリセットされます。

発信者が別のユーザ（ユーザ C など）にコールし、ユーザ C が話し中であったため、[折返し] ソフトキーを押します。発信者の電話機に置換 / 保持画面が表示されますが、この画面には、ユーザ B の使用可能通知がすでに発生したことが示されません。

#### 考えられる原因

ユーザが電話機をリセットしました。

#### 対応策

電話機がリセットされた後、アクティブなコールがないときに、電話機のコールバック通知を確認します。[折返し] ソフトキーを押します。

## Cisco Call Back のエラー メッセージ

この項では、電話機に表示されるエラー メッセージのリストを示します。

**エラー メッセージ** 有効なコールバックはありません。終了するには、[終了] を押してください。

**説明** アイドル状態のときに、ユーザが [折返し] ソフトキーを押しています。

**推奨処置** エラー メッセージに推奨処置が示されています。

**エラー メッセージ** コールバックは xxxxx で有効になっています。yyyy で有効にするには、[OK] を押してください。終了するには、[終了] を押してください。

**説明** ユーザがコールバックをアクティブにしようとしたますが、すでにアクティブになっています。

**推奨処置** エラー メッセージに推奨処置が示されています。

**エラー メッセージ** コールバックを xxxxx で有効にすることはできません。

**説明** ユーザがコールバックをアクティブにしようとしたますが、データベース内に内線番号が見つかりません。

**推奨処置** ユーザは、操作をもう一度実行する必要があります。または、管理者が電話番号を Cisco Unified Communications Manager の管理ページに追加する必要があります。

**エラー メッセージ** サービスがアクティブではありません。

**説明** Call Back Enabled Flag サービス パラメータを False に設定しているため、機能が無効のままになっています。

**推奨処置** コールバック機能を使用するには、Cisco CallManager のサービス パラメータ Call Back Enabled Flag を True に設定します。

## Cisco Call Back のログ ファイルの場所

Cisco Call Back 機能のトレースは、Cisco Communications Manager および CTIManager の SDL レコードおよび SDI レコードとして存在しています。このトレースにアクセスするには、『Cisco Unified Communications Manager Serviceability アドミニストレーションガイド』を参照してください。

## Cisco エクステンション モビリティのトラブルシューティング

Cisco エクステンション モビリティでは、管理者用のトラブルシューティング ツールを提供しています。これらのツールには、Cisco Unified Communications Manager Serviceability の一部であるパフォーマンス カウンタとアラームが含まれます。パフォーマンス カウンタおよびアラームについては、『Cisco Unified Communications Manager Serviceability システム ガイド』および『Cisco Unified Communications Manager Serviceability アドミニストレーション ガイド』を参照してください。

この項では、Cisco Communications Manager エクステンション モビリティに関連する問題のトラブルシューティングを支援するために、次の情報を提供します。

- [Cisco エクステンション モビリティの一般的な問題のトラブルシューティング \(P.8-6\)](#)
- [Cisco エクステンション モビリティのエラー メッセージのトラブルシューティング \(P.8-7\)](#)

### Cisco エクステンション モビリティの一般的な問題のトラブルシューティング

Cisco エクステンション モビリティで問題が発生した場合は、まずトラブルシューティングに関する次のヒントを参考にしてください。

- 次の手順を実行して、Cisco エクステンション モビリティのトレース ディレクトリを設定し、デバッグのトレースを有効にします。
  - Cisco Unified Communications Manager Serviceability ページで、[ Trace ] > [ Configuration ] を選択します。
  - [ Server ] ドロップダウン リスト ボックスから、サーバを選択します。
  - [ Service ] ドロップダウン メニューから、[ Cisco Extension Mobility ] を選択します。
- Cisco Extension Mobility サービスの URL を正しく入力したことを確認します。この URL では、大文字と小文字が区別されることに注意してください。
- すべての設定プロセスをひととおり正しく実行したことを確認します。
- Cisco エクステンション モビリティ ユーザの認証で問題が発生する場合は、ユーザのページに移動して PIN を確認します。

それでも問題が解決しない場合は、[表 8-2](#) のトラブルシューティング手段を使用します。

**表 8-2 Cisco Unified Communications Manager エクステンション モビリティのトラブルシューティング**

問題の説明	推奨処置
ユーザがログアウトして電話機がデフォルトのデバイス プロファイルに戻った後に、ユーザが電話サービスを使用できなくなる。	<ol style="list-style-type: none"> <li>1. [ エンタープライズパラメータ設定 (Enterprise Parameters Configuration) ] ウィンドウを参照して、Synchronization Between Auto Device Profile and Phone Configuration が True に設定されていることを確認します。</li> <li>2. 電話機を Cisco Extension Mobility サービスにサブスクライブします。</li> </ol>
ログイン後に、ユーザが電話サービスを使用できない。	<p>この問題が発生するのは、ユーザ プロファイルが電話機にロードされたときに、そのプロファイルにサービスが関連付けられていなかったためです。</p> <p>次の手順を実行します。</p> <ol style="list-style-type: none"> <li>1. ユーザ プロファイルに変更を加えて、Cisco Extension Mobility サービスが含まれるようにします。</li> <li>2. ユーザがログインする電話機の設定を変更して、Cisco エクステンション モビリティが含まれるようにします。電話機が更新されると、ユーザは電話サービスにアクセスできるようになります。</li> </ol>

表 8-2 Cisco Unified Communications Manager エクステンション モビリティのトラブルシューティング (続き)

問題の説明	推奨処置
ログインまたはログアウトを実行した後に、電話機が再起動される代わりにリセットされる。	<p>ロケールの変更によってリセットが発生している可能性があります。</p> <p>ログイン ユーザまたはプロファイルに関連付けられているユーザ ロケールが、デバイスのロケールと同じものでない場合、ログインが正常に完了すると、電話機は再起動を実行し、次にリセットを実行します。この動作が発生するのは、電話機の設定ファイルが再構築中であるためです。</p>

## Cisco エクステンション モビリティのエラー メッセージのトラブルシューティング

Cisco エクステンション モビリティを使用しているときに電話機に表示されるエラー コードおよびエラー メッセージをトラブルシューティングするには、表 8-3 の情報を使用します。

表 8-3 電話機に表示されるエラー メッセージのトラブルシューティング

エラー コード	電話機のメッセージ	推奨処置
201	[ 201 ] - 認証エラー	ユーザ ID と PIN を正しく入力したことをユーザが確認します。また、ユーザ ID と PIN が正しいものかどうかをユーザがシステム管理者に確認します。
22	[ 22 ]- デバイスのログインが無効	[ 電話の設定 ( Phone Configuration ) ] ウィンドウで、[ エクステンションモビリティの有効化 ( Enable ExtensionMobility ) ] が選択されていることを確認します。『Cisco Unified Communications Manager 機能およびサービス ガイド』を参照してください。
205	[ 205 ] - ユーザプロファイルなし	デバイス プロファイルがユーザに関連付けられていることを確認します。『Cisco Unified Communications Manager 機能およびサービス ガイド』を参照してください。
208	[ 208 ] -EMService 接続エラー	[ Cisco Unified Serviceability ] > Tools > [ Control Center—Feature Services ] を選択して、Cisco エクステンション モビリティ サービスが実行されていることを確認します。
25	[ 25 ]- ユーザは既にログイン済み	ユーザが別の電話機にログインしているかどうかを確認します。複数のログインを許可する必要がある場合は、Multiple Login Behavior サービス パラメータが Multiple Logins Allowed に設定されていることを確認します。
	ホストを検出できません	[ Cisco Unified Serviceability ] > Tools > [ Control Center—Feature Services ] を選択して、Cisco Tomcat サービスが実行されていることを確認します。
	HTTP エラー [ 503 ]	<p>[ サービス ] ボタンを押したときに、このエラーが表示される場合は、[ Cisco Unified Serviceability ] &gt; [ Tools ] &gt; [ Control Center—Feature Services ] を選択して、Cisco Communications Manager Cisco IP Phone Services サービスが実行されていることを確認します。</p> <p>エクステンション モビリティ サービスを選択したときに、このエラーが表示される場合は、[ Cisco Unified Serviceability ] &gt; [ Tools ] [ Control Center—Network Services ] を選択して、Cisco エクステンション モビリティ アプリケーション サービスが実行されていることを確認します。</p>
202	[ 202 ] ユーザ ID または PIN が空です	有効なユーザ ID および PIN を入力します。

表 8-3 電話機に表示されるエラー メッセージのトラブルシューティング (続き)

エラー コード	電話機のメッセージ	推奨処置
26	[ 26 ]- ビジー。再実行してください。	<p>同時ログイン要求および同時ログアウト要求の数が Maximum Concurrent requests サービス パラメータより大きいかどうかを確認します。大きい場合、同時要求の数を減らします。</p> <p>同時ログイン要求および同時ログアウト要求の数を確認するには、Cisco Unified Communications Manager Real-Time Monitoring Tool を使用して、エクステンション モビリティ オブジェクト内の Requests In Progress カウンタを表示します。</p>
6	[ 6 ]- データベースエラー	<p>要求が大量にあるかどうかを確認します。</p> <p>要求が大量にある場合、エクステンション モビリティ オブジェクト内の Requests In Progress カウンタに高い値が指定されています。大量の同時要求が原因で要求が拒否される場合は、Requests Throttled カウンタにも高い値が指定されています。</p> <p>詳細なデータベース ログを収集します。</p>
207	[ 207 ]- デバイス名が空白です	Cisco エクステンション モビリティ用に設定された URL が正しいことを確認します。

## Cisco Unified Communications Manager Assistant のトラブルシューティング

この項では、Cisco Unified Communications Manager Assistant に関する一般的な問題の解決方法について説明します。表 8-4 に、Cisco Unified Communications Manager Assistant のトラブルシューティングツールとクライアントデスクトップの説明を示します。

表 8-4 Cisco Unified Communications Manager Assistant のトラブルシューティングツールとクライアントデスクトップ

ツールの説明	場所
Cisco Unified CM Assistant サーバのトレースファイル	<p>ログファイルは、Cisco IP Manager Assistant サービスを実行するサーバ上にあります。</p> <p>これらのファイルは、次のいずれかの方法を使用して、サーバからダウンロードできます。</p> <ul style="list-style-type: none"> <li>CLI コマンド <code>file get activelog tomcat/logs/ipma/log4j</code> を使用する。</li> <li>Cisco Unified Communications Manager Real-Time Monitoring Tool (RTMT) のトレース収集機能を使用する。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。</li> </ul> <p>デバッグトレースを有効にするには、[ Cisco Unified Serviceability ] &gt; [ Trace ] &gt; [ Configuration ] を選択します。</p>
Cisco IPMA クライアントのトレースファイル	<p>クライアントのデスクトップで、Cisco Unified Communications Manager Assistant のアシスタント コンソールと同じ位置にある <code>\$INSTALL_DIR\logs\ACLog*.txt</code> です。</p> <p>デバッグトレースを有効にするには、アシスタント コンソールの設定ダイアログボックスに移動します。詳細設定のパネルで、[ トレースを有効にする ] チェックボックスをオンにします。</p> <p> (注) この操作で有効になるのは、デバッグ トレースのみです。エラートレースは常にオンになっています。</p>
Cisco IPMA クライアントのインストールトレースファイル	<p>クライアントのデスクトップで、Cisco Unified Communications Manager Assistant のアシスタント コンソールと同じ位置にある <code>\$INSTALL_DIR\InstallLog.txt</code> です。</p>
Cisco IPMA クライアントの AutoUpdater トレースファイル	<p>クライアントのデスクトップで、Cisco Unified Communications Manager Assistant のアシスタント コンソールと同じ位置にある <code>\$INSTALL_DIR\UpdatedLog.txt</code> です。</p>
インストール ディレクトリ	<p>デフォルトでは、<code>C:\Program Files\Cisco\Unified Communications Manager Assistant Console\</code> です。</p>

次の各項では、Cisco Unified Communications Manager Assistant のエラーおよび回復手順について説明します。

- IPMAConsoleInstall.jsp で「HTTP Status 503—This Application is Not Currently Available」エラーが表示される (P.8-10)
- IPMAConsoleInstall.jsp で「No Page Found Error」エラーが表示される (P.8-10)

- Exception: java.lang.ClassNotFoundException: InstallerApplet.class ( P.8-11 )
- ダウンロードによる Microsoft 仮想マシンの自動インストールが利用できなくなった ( P.8-11 )
- ユーザ認証が失敗する ( P.8-12 )
- アシスタント コンソールで「システムエラーが発生しました。システム管理者にお問い合わせください」エラーが表示される ( P.8-12 )
- アシスタント コンソールで「Cisco Unified Communications Manager Assistant サービスにアクセスできません。しばらくしてから再試行してください」エラーが表示される ( P.8-13 )
- フィルタリングをオンまたはオフにするとコールがルーティングされない ( P.8-14 )
- Cisco IP Manager Assistant サービスが初期化できない ( P.8-15 )
- 発信側にリオーダー音が聞こえる ( P.8-16 )
- マネージャがログアウトしてもサービスが動作している ( P.8-16 )
- アシスタントのプロキシ回線上で鳴っているコールをマネージャが代行受信できない ( P.8-17 )
- Cisco IP Manager Assistant サービスがダウンしているときにマネージャの電話にコールできない ( P.8-17 )

## IPMAConsoleInstall.jsp で「HTTP Status 503—This Application is Not Currently Available」エラーが表示される

### 症状

http://<サーバ名>:8443/ma/Install/IPMAConsoleInstall.jsp を参照すると、次のエラーが表示されます。

HTTP Status 503—This application is not currently available

### 考えられる原因

Cisco IP Manager Assistant サービスがアクティブになっていないか、実行されていません。

### 対応策

[ Cisco Unified Serviceability ] > [ Tools ] > [ Service Activation ] で、サービスのアクティベーションステータスを調べて、Cisco IP Manager Assistant サービスがアクティブになっていることを確認します。

Cisco IP Manager Assistant サービスがアクティブになっている場合は、[ Cisco Unified Communications Manager Serviceability ] > [ Tools ] > [ Control Center—Feature Services ] を選択して、Cisco Unified Communications Manager Assistant を再起動します。

## IPMAConsoleInstall.jsp で「No Page Found Error」エラーが表示される

### 症状

http://<サーバ名>:8443/ma/Install/IPMAConsoleInstall.jsp を参照すると、次のエラーが表示されます。

No Page Found Error

### 考えられる原因 (その1)

ネットワークに問題があります。システムの問題の詳細については、P.3-1 の「Cisco Unified Communications Manager システムの問題」を参照してください。

**対応策 (その 1)**

クライアントからサーバへの接続が存在することを確認します。URL の中で指定したサーバ名を ping して、到達できることを確認します。

**考えられる原因 (その 2)**

URL のつづりを間違えています。

**対応策 (その 2)**

URL では大文字と小文字が区別されるため、URL が指示と完全に一致していることを確認してください。

**Exception: java.lang.ClassNotFoundException: InstallerApplet.class****症状**

アシスタント コンソールを Web からインストールできません。次のエラー メッセージが表示されます。

```
Exception: java.lang.ClassNotFoundException: InstallerApplet.class
```

**考えられる原因**

Cisco Unified Communications Manager Assistant Console の標準インストールで、Microsoft Java 仮想マシン (JVM) の代わりに Sun Java プラグインの仮想マシンを使用すると、処理が失敗します。

**対応策**

Sun Java プラグインをサポートしている JSP ページの URL ( `https://<サーバ名>:8443/ma/Install/IPMAConsoleInstallJar.jsp` ) を、管理者がユーザに通知します。

**ダウンロードによる Microsoft 仮想マシンの自動インストールが利用できなくなった****症状**

Microsoft Windows XP を実行しているコンピュータ上で、アシスタント コンソールを Web からインストールしようとする失敗します。このプログラム用のすべてのコンポーネントを使用できない、というメッセージが表示されます。ユーザがダウンロードを選択すると、次のメッセージが表示されます。

```
Automatic installation of MS Virtual Machine is no longer available for download
```

**考えられる原因**

Microsoft は、Windows XP の Internet Explorer Version 6 では Microsoft JVM をサポートしていません。

**(注)**

このエラーは、システムに Windows XP Service Pack 1 とともに Microsoft JVM がインストールされている場合には発生しません。

### 対応策

次のいずれかの対応策に従います。

- Netscape ブラウザ (バージョン 7.x) をインストールし、Netscape を使用してアシスタント コンソールをインストールします。
- 次の URL から、IE 用の Sun Java 仮想マシン プラグインをインストールします。  
<http://java.sun.com/getjava/download.html>  
 Sun Java プラグインのインストールが完了したら、ブラウザで次の URL を参照します。  
<https://<サーバ名>:8443/ma/Install/IPMAInstallJar.jsp>
- Microsoft Java 仮想マシン (JVM) を Windows XP Service Pack 1 とともにインストールし、次にアシスタント コンソールをインストールします。

## ユーザ認証が失敗する

### 症状

ログイン画面にアシスタント コンソールからサインインすると、ユーザ認証が失敗します。

### 考えられる原因

次のような原因が挙げられます。

- データベース内で、ユーザの管理が不適切である。
- ユーザをアシスタントまたはマネージャとして誤って管理している。

### 対応策

Cisco Unified Communications Manager の管理ページで、ユーザ ID とパスワードが Cisco Unified Communications Manager ユーザとして管理されていることを確認します。

管理者は、ユーザを Cisco Unified Communications Manager Assistant ユーザ情報と関連付けて、アシスタントまたはマネージャとして管理する必要があります。このためには、[ Cisco Unified CM の管理 ] > [ ユーザ管理 ] > [ エンドユーザ ] にアクセスします。

## アシスタント コンソールで「システムエラーが発生しました。システム管理者にお問い合わせください」エラーが表示される

### 症状

アシスタント コンソールを起動すると、次のメッセージが表示されます。

システムエラーが発生しました。システム管理者にお問い合わせください。

### 考えられる原因 (その1)

Cisco Unified Communications Manager を Release 4.x から Release 5.x にアップグレードした可能性があります。アシスタント コンソールは Release 4.x から Release 5.x に自動的にアップグレードできません。

### 対応策 (その1)

[ スタート ] [ プログラム ] [ Cisco Unified Communications Manager Assistant ] [ Uninstall Assistant Console ] を選択して、コンソールをアンインストールします。次に、URL <https://<サーバ名>:8443/ma/Install/IPMAConsoleInstall.jsp> からコンソールを再インストールします。

**考えられる原因 (その 2)**

ユーザがデータベース内で正しく設定されていません。

**対応策 (その 2)**

Cisco Unified Communications Manager の管理ページで、ユーザ ID とパスワードが Cisco Unified Communications Manager ユーザとして管理されていることを確認します。

管理者は、ユーザを Cisco Unified Communications Manager Assistant ユーザ情報と関連付けて、アシスタントまたはマネージャとして管理する必要があります。このためには、[ Cisco Unified CM の管理 ] > [ ユーザ管理 ] > [ エンドユーザ ] にアクセスします。詳細については、『Cisco Unified Communications Manager 機能およびサービス ガイド』を参照してください。

**考えられる原因 (その 3)**

マネージャをアシスタントから削除すると、Cisco Unified Communications Manager の管理ページでアシスタントの回線はブランクのままになります。

**対応策 (その 3)**

[ Cisco IPMA Assistant の設定 ( Cisco IPMA Assistant Configuration ) ] ウィンドウで、プロキシ回線をもう一度割り当てます。詳細については、『Cisco Unified Communications Manager 機能およびサービス ガイド』を参照してください。

## アシスタント コンソールで「Cisco Unified Communications Manager Assistant サービスにアクセスできません。しばらくしてから再試行してください」エラーが表示される

**症状**

アシスタント コンソールを起動すると、次のメッセージが表示されます。

Cisco Unified Communications Manager Assistant サービスにアクセスできません。しばらくしてから再試行してください。

**考えられる原因 (その 1)**

Cisco IP Manager Assistant サービスが停止している可能性があります。

**対応策 (その 1)**

[ Cisco Unified Serviceability ] > [ Tools ] > [ Control Center—Feature Services ] を選択して、Cisco Unified Communications Manager Assistant を再起動します。

**考えられる原因 (その 2)**

プライマリとセカンダリの Cisco Unified Communications Manager Assistant サーバのアドレスが、DNS 名を使用して設定されていますが、その DNS 名が、DNS サーバ内に設定されていません。

**対応策 (その 2)**

次の手順を実行して、DNS 名を置き換えます。

**手順**

---

**ステップ 1** [ Cisco Unified CM の管理 ] > [ システム ] > [ サーバ ] を選択します。

**ステップ 2** サーバの DNS 名を、対応する IP アドレスで置き換えます。

**ステップ 3** [ Cisco Unified Serviceability ] > [ Tools ] > [ Control Center—Feature Services ] を選択して、Cisco Unified Communications Manager Assistant を再起動します。

#### 考えられる原因 (その 3)

Cisco CTI Manager サービスが停止している可能性があります。

#### 対応策 (その 3)

[ Cisco Unified Serviceability ] > [ Tools ] > [ Control Center—Feature Services ] を選択して、Cisco CTI Manager サービスと Cisco IP Manager Assistant サービスを再起動します。

#### 考えられる原因 (その 4)

Cisco Unified Communications Manager Assistant サービスは CTI 接続をセキュア モードで開くように設定されていても、セキュリティ設定がまだ完了していない可能性があります。

この場合、次のエラー メッセージがアラーム ビューアまたは Cisco Unified Communications Manager Assistant サービス ログに表示されます。

IPMA Service cannot initialize - Could not get Provider.

#### 対応策 (その 4)

Cisco IP Manager Assistant サービスのサービス パラメータでセキュリティ設定を確認します。詳細については、『Cisco Unified Communications Manager 機能およびサービス ガイド』を参照してください。

[ Cisco Unified Serviceability ] > [ Tools ] > [ Control Center—Feature Services ] を選択して、Cisco Unified Communications Manager Assistant を再起動します。

## フィルタリングをオンまたはオフにするとコールがルーティングされない

#### 症状

コールが正しくルーティングされません。

#### 考えられる原因 (その 1)

Cisco CTI Manager サービスが停止している可能性があります。

#### 対応策 (その 1)

[ Cisco Unified Serviceability ] > [ Tools ] > [ Control Center—Feature Services ] を選択して、Cisco CTI Manager サービスと Cisco IP Manager Assistant サービスを再起動します。

#### 考えられる原因 (その 2)

Cisco Unified Communications Manager Assistant ルート ポイントが正しく設定されていません。

### 対応策（その 2）

ワイルドカードを使用して、Cisco Unified Communications Manager Assistant CTI ルート ポイントの電話番号と、Cisco Unified Communications Manager Assistant に設定されたすべてのマネージャのプライマリ電話番号を対応付けます。

### 考えられる原因（その 3）

マネージャの電話機のステータス ウィンドウには、「Filtering Down」というメッセージが表示されます。Cisco Unified Communications Manager Assistant CTI ルート ポイントが削除されたか、使用されていない可能性があります。

### 対応策（その 3）

次の手順を実行して、CTI ルート ポイントを設定し、Cisco IP Manager Assistant サービスを再起動します。

#### 手順

- 
- ステップ 1** Cisco Unified Communications Manager の管理ページから、[ デバイス ] > [ CTI ルートポイント ] を選択します。
  - ステップ 2** ルート ポイントを検索するか、新しいルート ポイントを追加します。設定の詳細については、『*Cisco Unified Communications Manager アドミニストレーションガイド*』を参照してください。
  - ステップ 3** [ Cisco Unified Serviceability ] > [ Tools ] > [ Control Center—Feature Services ] を選択して、Cisco IP Manager Assistant サービスを再起動します。
- 

## Cisco IP Manager Assistant サービスが初期化できない

### 症状

Cisco IP Manager Assistant サービスが CTI Manager への接続を開くことができません。次のメッセージが表示されます。

```
IPMA Service cannot initialize - Could not get Provider.
```

### 考えられる原因

Cisco IP Manager Assistant サービスが CTI Manager への接続を開くことができません。エラーメッセージがアラーム ビューアまたは Cisco Unified CM Assistant サービス ログに表示されます。

### 対応策

[ Cisco Unified Serviceability ] > [ Tools ] > [ Control Center—Feature Services ] を選択して、Cisco CTI Manager サービスと Cisco IP Manager Assistant サービスを再起動します。

## 発信側にリオーダー音が聞こえる

### 症状

発信側にリオーダー音または「おかけになった電話番号では、正しくおつなぎできません」というメッセージが聞こえます。

### 考えられる原因

発信側回線のコーリングサーチスペースが正しく設定されていない可能性があります。

### 対応策

回線のコーリングサーチスペースを確認します。詳細については、『Cisco Unified Communications Manager アドミニストレーションガイド』を参照してください。

また、Cisco Dialed Number Analyzer サービスを使用して、コーリングサーチスペースに不備がないかどうかを確認できます。詳細については、『Cisco Unified Communications Manager Dialed Number Analyzer ガイド』を参照してください。

## マネージャがログアウトしてもサービスが動作している

### 症状

マネージャが Cisco Unified Communications Manager Assistant からログアウトしても、サービスがまだ動作しています。マネージャの IP Phone の表示は消えています。フィルタリングがオンになっているにもかかわらず、コールがルーティングされません。マネージャがログアウトしたことを確認するには、Cisco Unified Real-Time Monitoring Tool を使用してアプリケーションログを表示します。Cisco IP Manager Assistant サービスがログアウトしたことを示す、Cisco Java アプリケーションからの警告がないかどうかを調べます。

### 考えられる原因

マネージャが、ソフトキーを 1 秒間に 5 回（許容回数）以上押しました。

### 対応策

Cisco Unified Communications Manager 管理者が、マネージャの設定を更新する必要があります。次の手順を実行して、問題点を修正します。

### 手順

---

**ステップ 1** Cisco Unified Communications Manager の管理ページから、[ ユーザ管理 ] > [ エンドユーザ ] を選択します。

[ ユーザの検索と一覧表示 ( Find and List Users ) ] ウィンドウが表示されます。

**ステップ 2** マネージャ名を検索フィールドに入力し、[ 検索 ] ボタンをクリックします。

**ステップ 3** 更新するマネージャを結果リストから選択します。

[ エンドユーザの設定 ( End User Configuration ) ] ウィンドウが表示されます。

**ステップ 4** [ 関連リンク ] ドロップダウン リスト ボックスから [ マネージャの設定 ] を選択し、[ 移動 ] をクリックします。

**ステップ 5** マネージャの設定に必要な変更を加え、[保存] をクリックします。

---

## アシスタントのプロキシ回線上で鳴っているコールをマネージャが代行受信できない

### 症状

アシスタントのプロキシ回線上で呼び出し音が鳴っているコールを、マネージャが代行受信できません。

### 考えられる原因

プロキシ回線のコーリング サーチ スペースが正しく設定されていません。

### 対応策

アシスタントの電話機について、プロキシ回線のコーリング サーチ スペースを確認します。次の手順を実行して、問題点を修正します。

### 手順

**ステップ 1** Cisco Unified Communications Manager の管理ページから、[デバイス] > [電話] を選択します。

[電話の検索と一覧表示 (Find and List Phones)] ウィンドウが表示されます。

**ステップ 2** アシスタントの電話機をクリックします。

[電話の設定 (Phone Configuration)] ウィンドウが表示されます。

**ステップ 3** 電話機および電話番号 (回線) のコーリング サーチ スペースの設定を確認し、必要に応じて更新します。

---

## Cisco IP Manager Assistant サービスがダウンしているときにマネージャの電話にコールできない

### 症状

Cisco IP Manager Assistant サービスがダウンしたときに、コールがマネージャに正しくルーティングされません。

### 考えられる原因

Cisco Unified Communications Manager Assistant CTI ルート ポイントで、無応答時自動転送が有効になっていません。

### 対応策

次の手順を実行して、Cisco Unified Communications Manager Assistant ルート ポイントを正しく設定します。

---

## 手順

**ステップ 1** Cisco Unified Communications Manager の管理ページから、[ デバイス ] > [ CTI ルートポイント ] を選択します。

[ CTI ルートポイントの検索と一覧表示 ( Find and List CTI Route Points ) ] 検索ウィンドウが表示されます。

**ステップ 2** [ 検索 ] ボタンをクリックします。

設定済み CTI ルート ポイントのリストが表示されます。

**ステップ 3** 更新する Cisco Unified Communications Manager Assistant CTI ルート ポイントを選択します。

**ステップ 4** [ CTI ルートポイントの設定 ( CTI Route Point Configuration ) ] ウィンドウで、更新する回線を [ 割り当て情報 ( Association Information ) ] 領域から選択します。

[ 電話番号の設定 ( Directory Number Configuration ) ] ウィンドウが表示されます。

**ステップ 5** [ コール転送とコールピックアップの設定 ( Call Forward and Call Pickup Settings ) ] セクションで、[ 無応答時転送 ( Forward No Answer Internal、内部 ) ] チェックボックスと [ 無応答時転送 ( Forward No Answer External、外部 ) ] チェックボックスの両方または一方をオンにし、CTI ルートポイントの DN を [ 着信先別 ( Destination ) ] フィールドに入力します (たとえば、ルートポイント DN 1xxx の CFNA を設定する場合は 1xxx )。

**ステップ 6** [ コーリングサーチスペース ( Calling Search Space ) ] ドロップダウン リスト ボックスで、CSS-M-E (または適切なコーリングサーチスペース) を選択します。

**ステップ 7** [ 保存 ] ボタンをクリックします。

---

## Cisco Unified Communications Manager Attendant Console の トラブルシューティング

Cisco Unified Communications Manager Attendant Console では、管理者用のトラブルシューティングツールを提供しています。これらのツールには、Cisco Unified Communications Manager Serviceability の一部であるパフォーマンス カウンタとアラームが含まれます。パフォーマンス カウンタおよびアラームの詳細については、『Cisco Unified Communications Manager Serviceability システム ガイド』および『Cisco Unified Communications Manager Serviceability アドミニストレーション ガイド』を参照してください。

この項では、Cisco Unified Communications Manager Attendant Console に関連する問題のトラブルシューティングを支援するために、次の情報を提供します。

- [テレフォニーの初期化のエラー \(P.8-19\)](#)
- [コールの発信と受信に関する問題 \(P.8-22\)](#)
- [ディレクトリの問題 \(P.8-24\)](#)
- [ボイス メッセージの問題 \(P.8-25\)](#)
- [Cisco Unified Communications Manager Attendant Console インターフェイスを使用する際の問題 \(P.8-26\)](#)
- [Cisco Unified Communications Manager Serviceability が JTAPI ログを生成しない \(P.8-28\)](#)
- [サーバ ログの収集 \(P.8-29\)](#)
- [Cisco Unified Communications Manager Attendant Console のパフォーマンス モニタ カウンタ \(P.8-29\)](#)

### テレフォニーの初期化のエラー

この項では、次に示す Cisco Unified Communications Manager Attendant Console の電話初期化エラーメッセージの表示について説明します。

- [テレフォニーの初期化の失敗 \(P.8-19\)](#)
- [コール制御の初期化の失敗 \(P.8-20\)](#)
- [アテンダントがサーバにアクセスできないというエラー メッセージの表示 \(P.8-21\)](#)

### テレフォニーの初期化の失敗

#### 症状

テレフォニーの初期化に失敗したというメッセージをアテンダントが受信しました。

#### 考えられる原因

考えられる原因は次のとおりです。

- Attendant Console アプリケーション ユーザと認証ユーザのいずれか一方または両方が存在しません。
- 制御されている電話機が、Attendant Console 認証ユーザの制御デバイス リストに含まれていません。
- [ アプリケーションユーザの設定 (Application User Configuration) ] ウィンドウで Attendant Console アプリケーション ユーザと認証ユーザに設定したユーザ名が、Cisco CallManager Attendant Console Server サービス パラメータでこれらのユーザに設定したユーザ名と一致していません。

- Cisco Unified Communications Manager の管理ページで、Standard CTI Enabled ユーザ グループ、Standard CTI Allow Call Park Monitoring ユーザ グループ、および Standard Allow Control of All Devices ユーザ グループ(あるいは、これらのユーザ グループのいずれか)に Attendant Console アプリケーション ユーザが関連付けられていません。

### 推奨処置

次の作業は必ず実行してください。

- 『Cisco Unified Communications Manager 機能およびサービス ガイド』の説明に従って、Attendant Console アプリケーション ユーザと認証ユーザを作成します。
- [ アプリケーションユーザの設定 (Application User Configuration) ] ウィンドウで、Attendant Console アプリケーション ユーザと認証ユーザのユーザ名を入力します (Cisco CallManager Attendant Console Server サービス パラメータに入力するユーザ名と同じにします)。
- Attendant Console アプリケーション ユーザに使用するユーザ ID は、[ サービスパラメータ設定 (Service Parameter Configuration) ] ウィンドウの Cisco CallManager Attendant Console Server サービスの [ JTAPI Username ] フィールドと同じ値にしてください。
- Attendant Console 認証ユーザに使用するユーザ ID は、[ サービスパラメータ設定 (Service Parameter Configuration) ] ウィンドウの Cisco CallManager Attendant Console Server サービスの [ Device Authentication Application Username ] フィールドと同じ値にしてください。
- 『Cisco Unified Communications Manager 機能およびサービス ガイド』の説明に従って、Cisco Unified Communications Manager の管理ページで Standard CTI Enabled ユーザ グループ、Standard CTI Allow Call Park Monitoring ユーザ グループ、および Standard Allow Control of All Devices ユーザ グループに Attendant Console アプリケーション ユーザを関連付けます。

## コール制御の初期化の失敗

### 症状

Cisco Unified Communications Manager Attendant Console が、コール制御の初期化に失敗しました。

### 考えられる原因

次のいずれかの理由で、コール制御が発生しません。

- Windows XP SP2 をアテンダントの PC にインストールして、ファイアウォールを解除しませんでした。
- アテンダントの電話機の [ 電話の設定 (Phone Configuration) ] ウィンドウで、[ CTI からデバイスを制御可能 (Allow Control of Device from CTI) ] チェックボックスをオフにしました。

### 推奨処置

次のいずれかの処理を実行します。

- 各アテンダントの電話機の [ 電話の設定 (Phone Configuration) ] ウィンドウで、[ CTI からデバイスを制御可能 (Allow Control of Device from CTI) ] チェックボックスがオンになっていることを確認します。このフィールドは、システムのデフォルトではオンになっています。アテンダントの電話機についてこのチェックボックスがオンになっていない場合、その Attendant Console ではコール制御が発生しません。
- Windows XP SP2 のインストール後に Cisco Unified Communications Manager Attendant Console を初めて起動すると、ダイアログボックスが表示され、ACClient アプリケーションの機能の一部が Windows ファイアウォールによってブロックされたことが示されます。Windows ファイアウォールでの例外を作成するには、そのまま Cisco Unified Communications Manager Attendant Console の使用を続けて、[ ブロックを解除する ] をクリックします。動作の例外が自動的に設定されます。

Windows XP SP2 のインストール後に Cisco Unified Communications Manager Attendant Console を初めて起動したとき、[ ブロックを解除する ] をクリックしなかった場合は、次の手順に従って例外を作成し、Cisco Unified Communications Manager Attendant Console をそのまま使用できるようにします。

### 手順

- 
- ステップ 1** [ スタート ] > [ 設定 ] > [ コントロール パネル ] > [ Windows ファイアウォール ] を選択します。  
[ Windows ファイアウォール ] ダイアログボックスが表示されます。
- ステップ 2** [ 例外 ] タブを選択します。
- ステップ 3** [ プログラムの追加 ] ボタンをクリックします。  
[ プログラムの追加 ] ダイアログボックスが表示されます。
- ステップ 4** [ 参照 ] をクリックします。ACClient.exe ファイルを参照し、[ 開く ] をクリックします。  
[ Windows ファイアウォール ] ダイアログボックスの [ 例外 ] タブで、アプリケーションのリストに ACClient が表示されます。
- ステップ 5** [ 編集 ] をクリックします。  
[ プログラムの編集 ] ダイアログボックスが表示されます。
- ステップ 6** [ スコープの変更 ] をクリックします。  
[ スコープの変更 ] ダイアログボックスが表示されます。
- ステップ 7** [ 任意のコンピュータ(インターネット上のコンピュータを含む) ] オプション ボタンが選択されていることを確認します。
- ステップ 8** [ OK ] を 2 回クリックします。
- 

## アテンダントがサーバにアクセスできないというエラー メッセージの表示

### 症状

アテンダントがサーバにログインしようとする時、アテンダントがサーバにアクセスできないことを示すダイアログボックスが表示されます。

### 考えられる原因

アテンダントの PC にある Attendant Console のバージョンが、Cisco Unified Communications Manager の管理ページから使用できる Attendant Console のバージョンと一致していません。

### 推奨処置

アテンダントの PC で動作している Attendant Console のバージョンをアップグレードします。Cisco Unified Communications Manager の管理ページからプラグインにアクセスするには、[ アプリケーション ] > [ プラグイン ] を選択します。Attendant Console をインストールした後に、インストールプロセスで設定しなかった Attendant Console 設定値を設定したり更新したりすることができます。

## コールの発信と受信に関する問題

この項では、次に示す、コールの発信と受信に関する Cisco Unified Communications Manager Attendant Console の問題について説明します。

- [パイロットポイントにコールを発信できない \(P.8-22\)](#)
- [アップグレード後にファースト ビジー シグナルを受信する \(P.8-22\)](#)
- [回線が使用できない \(P.8-23\)](#)
- [電話機の回線が使用不可になる \(P.8-24\)](#)

### パイロットポイントにコールを発信できない

#### 症状

ユーザがパイロットポイントにコールすると、リオーダー音が再生されます。

#### 考えられる原因

制御されている電話機が、Attendant Console 認証ユーザの制御デバイス リストに含まれていません。

#### 推奨処置

Cisco Unified Communications Manager の管理ページで、Attendant Console 認証ユーザを 1 人設定し、そのユーザにアテンダントの電話機を関連付ける必要があります。このユーザを設定していない場合、Attendant Console は CTIManager と情報を交換できず、アテンダントがコールを受信できません。ユーザを設定した後は、必ず Cisco CTI Manager サービスと Cisco Unified CallManager Attendant Console Server サービスを再起動してください。認証ユーザの作成の詳細については、『*Cisco Unified Communications Manager 機能およびサービス ガイド*』を参照してください。サービスの再起動の詳細については、『*Cisco Unified Serviceability アドミニストレーション ガイド*』を参照してください。

### アップグレード後にファースト ビジー シグナルを受信する

#### 症状

Cisco Unified Communications Manager Attendant Console のアップグレード後に、ハントグループおよび CTI ルートポイントで速いビジー音が聞こえます。

#### 考えられる原因

Cisco Unified Communications Manager Attendant Console を正しく設定していないか、またはサービスを再起動していません。

#### 推奨処置

Cisco Unified Communications Manager の管理ページで、Attendant Console 認証ユーザを 1 人設定し、そのユーザにアテンダントの電話機を関連付ける必要があります。このユーザを設定していない場合、Attendant Console は CTIManager と情報を交換できず、アテンダントがコールを受信できません。ユーザを設定した後は、必ず Cisco CTI Manager サービスと Cisco Unified CallManager Attendant Console Server サービスを再起動してください。認証ユーザの作成の詳細については、『*Cisco Unified Communications Manager 機能およびサービス ガイド*』を参照してください。サービスの再起動の詳細については、『*Cisco Unified Serviceability アドミニストレーション ガイド*』を参照してください。

## 回線が使用できない

### 症状

選択した回線が使用できないというメッセージをアテンダントが受信しました。

### 考えられる原因

回線で同時にサポートできるのは、設定可能な一定数のコールです。アテンダントの回線が 2 つのコールをサポートしていて、回線 1 をコールの転送に使用している場合、同じ回線上でアテンダントが別のコールを保留状態にすると、アテンダントの選択した回線は使用できなくなります。この回線は、アテンダントが次のいずれかの作業を行うまでは使用不可のままになります。

### 推奨処置

回線がサポートするコール数を増やすには、次の手順を実行します。

### 手順

---

**ステップ 1** [ デバイス ] > [ 電話 ] を選択します。

[ 電話の検索と一覧表示 ( Find and List Phones ) ] ウィンドウが表示されます。

**ステップ 2** 特定の電話機を見つけるための検索条件を入力します。

検索条件に一致した電話機のリストが表示されます。

**ステップ 3** 更新する電話機の名前をクリックします。

[ 電話の設定 ( Phone Configuration ) ] ウィンドウが表示されます。

**ステップ 4** [ 割り当て情報 ( Association Information ) ] にある電話番号のリストで、更新する回線をクリックします。

[ 電話番号の設定 ( Directory Number Configuration ) ] ウィンドウが表示されます。

**ステップ 5** [ コール最大数 ( Maximum Number of Calls ) ] フィールドに、回線でサポートするコールの数を入力します。

**ステップ 6** [ 保存 ] をクリックします。

**ステップ 7** 変更内容を有効にするには、[ リセット ] をクリックします。

再起動の対象となるデバイス数を示すメッセージが表示されます。

**ステップ 8** デバイスを再起動するには、[ リセット ] をクリックします。

---

## 電話機の回線が使用不可になる

### 症状

アテンダントの電話機の回線が、Cisco Unified Communications Manager Attendant Console で使用不可になっています。

### 考えられる原因

制御されている電話機が、Attendant Console 認証ユーザの制御デバイス リストに含まれていません。

### 推奨処置

『Cisco Unified Communications Manager 機能およびサービス ガイド』の説明に従って、Attendant Console 認証ユーザを作成し、そのユーザにアテンダントの電話機を関連付けます。

## ディレクトリの問題

この項では、[ディレクトリ] ウィンドウにユーザが表示されない問題について説明し、考えられるいくつかの原因と対応策を示します。

### 症状

Cisco Unified Communications Manager の管理ページで追加したユーザが、Cisco Unified Communications Manager Attendant Console の [ディレクトリ] ウィンドウに表示されません。

### 考えられる原因

サーバがユーザ リストをディレクトリから抽出するのは、次のいずれかの状況が発生した場合のみです。

- Cisco CallManager Attendant Console Server サービスが開始され、Directory Sync Period サービスパラメータには 0 以外の間隔が指定されている。
- Directory Sync Period サービスパラメータに指定された間隔が経過している。
- Cisco Unified Communications Manager の管理ページの Directory Sync Period サービスパラメータの値が変更されている。

Cisco Unified Communications Manager Attendant Console がユーザ リストをロードするのは、ログイン時のみです。

### 推奨処置

上記のいずれかの状況が発生した場合は、アテンダントがもう一度ログインする必要があります。

### 考えられる原因

Cisco Unified Communications Manager Attendant Console では、電話番号を持たないユーザは表示されません。

### 推奨処置

関係するすべてのユーザについて、それぞれの電話番号がディレクトリ内にリストされていることを確認します。

## 手順

---

**ステップ 1** Cisco Unified Communications Manager の管理ページから、[ ユーザ管理 ] > [ エンドユーザ ] を選択します。

[ ユーザの検索と一覧表示 ( Find and List Users ) ] ウィンドウが表示されます。

**ステップ 2** [ 検索対象 : ユーザ、検索条件 : ] フィールドに適切な検索条件を入力し、[ 検索 ] をクリックします。

**ステップ 3** [ 検索結果 ( Search Results ) ] リストで、電話番号を追加するユーザの名前をクリックします。

**ステップ 4** [ 電話番号 ( Telephone Number ) ] フィールドに、ユーザの電話番号を入力します。

**ステップ 5** [ 保存 ] をクリックします。

---

## ボイス メッセージの問題

この項では、不適切なボイス メッセージ グリーティングが再生される問題について説明します。

### 症状

コールがアテンダントによって応答されずにボイス メッセージに転送されたとき、ボイス メッセージ システムが、パイロット ポイントのグリーティングではなくアテンダントのグリーティングを再生します。

### 考えられる原因

Reset Original Called Party on Redirect サービス パラメータに True が指定されています。

### 推奨処置

次の手順を実行して、サービス パラメータを適切な値に設定します。

## 手順

---

**ステップ 1** [ システム ] > [ サービスパラメータ ] を選択します。

**ステップ 2** [ サーバ ( Server ) ] ドロップダウン リスト ボックスから、Attendant Console のサーバを選択します。

**ステップ 3** [ サービス ( Service ) ] ドロップダウン リスト ボックスから、Cisco CallManager Attendant Console Server サービスを選択します。

**ステップ 4** Reset Original Called Party on Redirect ドロップダウン リスト ボックスから、False を選択します。

---

## Cisco Unified Communications Manager Attendant Console インターフェイスを使用する際の問題

この項では、次に示す Cisco Unified Communications Manager Attendant Console インターフェイスの問題について説明します。

- Cisco Unified Communications Manager Attendant Console インターフェイスにアクセスできない (P.8-26)
- Cisco Unified Communications Manager Attendant Console サーバと通信できない (P.8-26)
- テキストが不適切な言語で表示される (P.8-27)
- Unicode 言語で検索できない (P.8-27)
- 短縮ダイヤル ウィンドウとディレクトリ ウィンドウで回線状態が正しく表示されない (P.8-28)
- 電話番号の回線状態が不明と表示される (P.8-28)

### Cisco Unified Communications Manager Attendant Console インターフェイスにアクセスできない

#### 症状

アテンダントが Cisco Unified Communications Manager Attendant Console にアクセスできません。

#### 考えられる原因

アテンダントが PC 上のローカル管理者アクセス権を持っていません。

#### 対応策

適切なディレクトリに対する権限を変更しない限り、Cisco Unified Communications Manager Attendant Console はローカル管理者アクセス権がない PC 上で実行されません。Windows NT を実行する PC では、KEY\_LOCAL\_MACHINE\Software\Cisco Systems, Inc. レジストリ キーのセキュリティを変更して、このキーおよびすべてのサブキーに対するフルアクセス権をアテンダントに付与します。Windows 2000 または Windows XP を実行する PC では、NTFS 権限を変更して c:\program files\cisco\call manager attendant console\ とすべてのサブディレクトリおよびファイルに対するフルアクセスを許可し、さらに、KEY\_LOCAL\_MACHINE\Software\Cisco Systems, Inc. レジストリ キーのセキュリティを変更して、このキーおよびすべてのサブキーに対するフルアクセス権をアテンダントに付与します。

### Cisco Unified Communications Manager Attendant Console サーバと通信できない

#### 症状

アテンダントが Attendant Console にログインしようとする、Attendant Console がサーバと通信できないことを示すダイアログボックスが表示されます。

#### 考えられる原因

Attendant Console クライアントと Attendant Console サーバが、同じドメイン内にありません。

#### 推奨処置

Attendant Console クライアントの hosts ファイルに、サーバの IP アドレスと完全修飾ドメイン名とのマッピングを入力します。

## 手順

**ステップ 1** Cisco Unified Communications Manager Attendant Console の PC で、次の位置にある hosts ファイルを開きます。  
c:\program files\winnt\system32\drivers\etc\hosts

**ステップ 2** サーバの IP アドレスと完全修飾ホスト名のエントリを作成します。

IP アドレスが 10.104.1.4 で、ドメイン名が tbd2-pub-7835.cluster1.com であるサーバのエントリを作成するには、次のエントリを作成します。

```
10.104.1.4 tbd2-pub-7835.cluster1.com
```

## テキストが不適切な言語で表示される

### 症状

一部のテキストが英語で表示されます。その他のテキストは、アテンダントが Cisco Unified Communications Manager Attendant Console のダイアログボックスで選択した言語で表示されます。

### 考えられる原因

選択した言語で利用できる、最新のロケール インストーラがインストールされていません。

### 対応策

選択した言語で利用できる最新のロケール インストーラをインストールする必要があります。Web で入手可能な『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。

## Unicode 言語で検索できない

### 症状

Cisco Unified IP Phone のディレクトリおよび Cisco Unified Communications Manager Attendant Console などのアプリケーションで、日本語などの Unicode 言語で検索ができません。

### 考えられる原因

Cisco Unified IP Phone および特定のアプリケーションでは、Unicode 言語をサポートしていません。

### 推奨処置

ディレクトリ検索機能を有効にするには、Cisco Unified Communications Manager の管理ページの[ エンドユーザの設定 (End User Configuration)] ウィンドウにある姓と名のフィールドで、Unicode 名の前に、ASCII テキストで名前の読み方と省略記号 (...) を入力しておきます。電話機およびアプリケーションでは、名前の ASCII テキストバージョンを対象として検索できます。Cisco Unified Communications Manager Attendant Console の詳細検索機能を使用する場合は、ASCII 名と Unicode 名のどちらでも検索できます。

## 短縮ダイヤル ウィンドウとディレクトリ ウィンドウで回線状態が正しく表示されない

### 症状

[短縮ダイヤル]ウィンドウと[ディレクトリ]ウィンドウで、回線の状態が正しく表示されません。

### 考えられる原因

回線状態の更新情報は、サーバからクライアントに UDP パケットを使用して送信されます。NAT デバイスまたはファイアウォールによってクライアントとサーバが分離されている場合は、クライアントがサーバから回線状態の更新情報を受信できないことがあります。

### 推奨処置

クライアントとサーバの両方を、NAT デバイスまたはファイアウォールから見て同じ側に配置します。

## 電話番号の回線状態が不明と表示される

### 症状

一部の電話番号の回線状態が、不明な状態と表示されます。

### 考えられる原因

電話機がコール処理サービスを受けるすべての Cisco Unified Communications Manager サーバ上で、Cisco CallManager Attendant Console Server サービスが開始されていません。

### 推奨処置

電話機がコール処理サービスを受けるすべての Cisco Unified Communications Manager サーバ上で、Cisco CallManager Attendant Console Server サービスをアクティブにして開始します。サービスをアクティブにする方法については、『Cisco Unified Communications Manager Serviceability アドミニストレーション ガイド』を参照してください。

## Cisco Unified Communications Manager Serviceability が JTAPI ログを生成しない

この項では、JTAPI ログが生成されない問題について説明します。

### 症状

トレース レベルを Error から Detailed に変更しましたが、JTAPI ログが生成されません。

### 考えられる原因

JTAPI トレース レベルが JTAPI の初期化中に設定され、以降に変更されていません。

### 推奨処置

Cisco CallManager Attendant Console Server サービスを再起動します。サービスの再起動については、『Cisco Unified Serviceability アドミニストレーション ガイド』を参照してください。

## サーバ ログの収集

この項では、サーバ ログの収集方法について説明します。

### 症状

すべてのサーバ側ログを収集する手段が必要です。

### 考えられる原因

サーバの問題をデバッグするには、次のトレースを収集します。

- CCM
- CTI
- SDL CCM
- SDL CTI
- Cisco Communications Manager Attendant Console Server
- JTAPI

### 推奨処置

Cisco Unified Real-Time Monitoring Tool (RTMT) または CLI を使用して、適切なログ ファイルを収集します。RTMT については、『*Cisco Unified Serviceability 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。

## Cisco Unified Communications Manager Attendant Console のパフォーマンス モニタ カウンタ

Real-Time Monitoring Tool (RTMT) で Cisco Unified Communications Manager Attendant Console のパフォーマンス モニタ カウンタを使用すると、Cisco CallManager Attendant Console Server サービスが実行されている時間、Cisco CallManager Attendant Console Server サービスが起動してからの時間、発生したコールの数、リダイレクトされたコールの数、登録されているアテンダントの数、パイロットポイントの数、および登録されたクライアントの数を監視できます。

Attendant Console の CcmLineLinkState パフォーマンス モニタでは、Attendant Console が正しく機能しているかどうかを簡単に確認できます。

- CcmLineLinkState カウンタが 11 の場合、Cisco CallManager Attendant Console Server サービスが正常に機能していることを示します。
- CcmLineLinkState の左端の数字は、Cisco CallManager Attendant Console Server サービスが Cisco Unified Communications Manager CTI に接続および登録されているかどうかを示します。この数字が 0 の場合、CTI またはディレクトリに問題が存在する可能性があります。
- CcmLineLinkState の右端の数字は、Cisco CallManager Attendant Console Server サービスが Cisco Unified Communications Manager を通じて回線状態情報を認識できるかどうかを示します。この数字が 0 の場合、Cisco Unified Communications Manager に問題が存在する可能性があります。



### (注)

Attendant Console ユーザが Attendant Console にログインできず、回線状態情報が入手できない場合は、CcmLineLinkState パフォーマンス モニタを表示して、Attendant Console のすべてのコンポーネントが正しく機能していることを確認してください。

パフォーマンス モニタ カウンタおよびアラームの詳細については、『*Cisco Unified Communications Manager Serviceability アドミニストレーション ガイド*』を参照してください。

## Cisco Web Dialer のトラブルシューティング

この項では、Cisco Web Dialer に関連する一般的な問題のエラー メッセージについて説明します。

- 認証エラー (P.8-30)
- サービスが一時的に使用できない (P.8-30)
- ディレクトリサービスがダウンしている (P.8-31)
- Cisco CTIManager がダウンしている (P.8-31)
- セッションの期限切れ、再ログイン (P.8-31)
- ユーザがログインしているデバイスがない (P.8-32)
- デバイス / 回線が開けない (P.8-32)
- 転送先に到達できない (P.8-32)

### 認証エラー

#### 症状

Cisco Web Dialer で、次のメッセージが表示されます。

認証に失敗しました。もう一度入力してください。

#### 考えられる原因

ユーザが、間違ったユーザ ID またはパスワードを入力しました。

#### 対応策

ユーザ ID とパスワードを確認します。Cisco Unified Communications Manager のユーザ ID とパスワードを使用してログインする必要があります。

### サービスが一時的に使用できない

#### 症状

Cisco Web Dialer で、次のメッセージが表示されます。

サービスは一時的に使用できない状態です。あとでもう一度実行してください。

#### 考えられる原因

同時 CTI セッションのロットリング上限値(3 セッション)に達したため、Cisco CallManager サービスが過負荷になっています。

#### 対応策

しばらくしてから、接続を再試行します。

## ディレクトリサービスがダウンしている

### 症状

Cisco Web Dialer で、次のメッセージが表示されます。

サービスは一時的に使用できない状態です。あとでもう一度実行してください: ディレクトリサービスがダウンしています。

### 考えられる原因

Cisco Communications Manager のディレクトリ サービスがダウンしている可能性があります。

### 対応策

しばらくしてから、接続を再試行します。

## Cisco CTIManager がダウンしている

### 症状

Cisco Web Dialer で、次のメッセージが表示されます。

サービスは一時的に使用できない状態です。あとでもう一度実行してください: Cisco CTIManager がダウンしています。

### 考えられる原因

Cisco Web Dialer 用に設定されている Cisco CTIManager サービスがダウンしました。

### 対応策

しばらくしてから、接続を再試行します。

## セッションの期限切れ、再ログイン

### 症状

Cisco Web Dialer で、次のメッセージが表示されます。

セッションの期限が切れました。もう一度ログインしてください。

### 考えられる原因

次の場合には、Cisco Web Dialer セッションの有効期限が切れます。

- Web Dialer サブレットが設定された後
- Cisco Tomcat サービスが再起動された場合

### 対応策

Cisco Unified Communications Manager のユーザ ID とパスワードを使用してログインします。

## ユーザがログインしているデバイスがない

### 症状

Cisco Web Dialer で、次のメッセージが表示されます。

ユーザがログインしているデバイスがありません。

### 考えられる原因

ユーザが、Cisco Web Dialer のプリファレンス ページで Cisco エクステンション モビリティを使用するように選択しましたが、どの IP Phone にもログインしていません。

### 対応策

- 電話機にログインしてから Cisco Web Dialer を使用します。
- [ **エクステンションモビリティを使用する** ] オプションを選択するのではなく、デバイスをダイヤログボックスの Cisco Web Dialer プリファレンス リストから選択します。

## デバイス / 回線が開けない

### 症状

ユーザがコールを発信しようとする、Cisco Web Dialer で、次のメッセージが表示されます。

デバイス / 回線が開けませんでした。

### 考えられる原因

- ユーザが、Cisco Unified Communications Manager に登録されていない Cisco Unified IP Phone を選択しました。たとえば、アプリケーションを起動する前に、ユーザが Cisco IP SoftPhone を優先デバイスとして選択しています。
- 新しい電話機を持っているユーザが、使用されなくなった古い電話機を選択しています。

### 対応策

Cisco Unified Communications Manager に登録され、使用されている電話機を選択します。

## 転送先に到達できない

### 症状

Cisco Web Dialer で、コールの終了ウィンドウに次のメッセージが表示されます。

転送先に到達できません。

### 考えられる原因

- ユーザが、間違った番号をダイヤルしました。
- 正しいダイヤル規則が適用されませんでした。たとえば、ユーザが 95550100 ではなく 5550100 をダイヤルしています。

### 対応策

ダイヤル規則を確認します。

## ダイレクト コール パークのトラブルシューティング

表 8-5 に、ダイレクト コール パークに関連する一般的な問題のトラブルシューティング リカバリのヒントを示します。

表 8-5 ダイレクト コール パークのトラブルシューティングのヒント

問題の説明	推奨処置
ユーザがコールをパークできない。[ 転送 ] ソフトキー（または使用できる場合は [ 転送 ] ボタン）を押して、ダイレクト コール パーク番号をダイヤルした後、コールがパークされない。	<p>コール パーク番号に割り当てられたパーティションが、電話機の電話番号に割り当てられたパーティションと一致することを確認します。『Cisco Unified Communications Manager アドミニストレーション ガイド』を参照してください。</p> <p>パーティションとコーリング サーチ スペースがデバイスに対して正しく設定されていることを確認します。『Cisco Unified Communications Manager アドミニストレーション ガイド』を参照してください。</p>
ユーザがコールをパークできない。[ 転送 ] ソフトキー（または使用できる場合は [ 転送 ] ボタン）を押して、ダイレクト コール パーク番号をダイヤルした後、ビジー音が聞こえ、IP Phone に「パークスロットが利用できません」というメッセージが表示される。	ダイヤルしたダイレクト コール パーク番号が、パークされたコールによってまだ使用されていないことを確認します。または、別のダイレクト コール パーク番号にコールをパークします。
ユーザがコールをパークできない。[ 転送 ] ソフトキー（または使用できる場合は [ 転送 ] ボタン）を押して、ダイレクト コール パーク番号をダイヤルした後、リオーダー音またはアナウンスが聞こえる。	ダイヤルした番号がダイレクト コール パーク番号として設定されていることを確認します。『Cisco Unified Communications Manager 機能およびサービス ガイド』を参照してください。
パークされたコールの復元が早すぎる。	Call Park Reversion Timer の設定時間を長くします。『Cisco Unified Communications Manager 機能およびサービス ガイド』を参照してください。
ユーザがコールをパークできない。復元タイマーの期限が切れた後、リオーダー音が聞こえる。	<p>ユーザがダイレクト コール パーク番号をダイヤルする前に、[ 転送 ] ソフトキー（または使用できる場合は [ 転送 ] ボタン）を押し、ダイレクト コール パーク番号をダイヤルした後もう一度 [ 転送 ] ソフトキー（または [ 転送 ] ボタン）を押すか、オンフックにしていることを確認します。ダイレクト コール パークは転送機能であるため、ダイレクト コール パーク番号を単独でダイヤルすることはできません。『Cisco Unified Communications Manager 機能およびサービス ガイド』を参照してください。</p> <p> (注) Transfer On-hook Enabled サービス パラメータが True に設定されている場合は、2 度目の [ 転送 ] ソフトキー（または [ 転送 ] ボタン）を押す代わりに、オンフックにするだけで転送を完了できます。『Cisco Unified Communications Manager システム ガイド』を参照してください。</p>

表 8-5 ダイレクトコールパークのトラブルシューティングのヒント (続き)

問題の説明	推奨処置
ユーザが、パークされたコールを取得できない。パークされたコールを取得するためにダイレクトコールパーク番号をダイヤルした後、ビジー音が聞こえ、IP Phone に「パークスロットが利用できません」というメッセージが表示される。	取得用プレフィックス、ダイレクトコールパーク番号の順にダイヤルしていることを確認します。『Cisco Unified Communications Manager 機能およびサービス ガイド』を参照してください。
パークされたコールが、コールをパークした番号に復元されない。	ダイレクトコールパーク番号の復元先が、別の電話番号ではなく、コールをパークした番号に設定されていることを確認します。『Cisco Unified Communications Manager 機能およびサービス ガイド』を参照してください。
ダイレクトコールパーク番号または番号の範囲を削除しようとする、番号または範囲は使用中のため削除できないというメッセージが表示される。	ダイレクトコールパーク番号を (BLF ボタンで) 監視するようにデバイスが設定されている場合、ダイレクトコールパーク番号は削除できません。番号を使用しているデバイスを確認するには、[ダイレクトコールパークの設定 (Directed Call Park Configuration)] ウィンドウで [依存関係レコード] リンクをクリックします。
ダイレクトコールパーク番号の範囲を設定した後、範囲内の番号にコールをパークできない。	ダイレクトコールパーク番号の範囲を入力する構文を確認します。使用している構文に誤りがある場合、実際には範囲が設定されていないのに、設定されているように見えます。『Cisco Unified Communications Manager 機能およびサービス ガイド』を参照してください。

## 即時転送のトラブルシューティング

この項では、即時転送機能に関連する、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。

- キーがアクティブではありません (P.8-35)
- 一時エラー発生 (P.8-35)
- 話中 (P.8-35)

### キーがアクティブではありません

#### 症状

ユーザが [ 即転送 ] を押すと、電話機にこのメッセージが表示されます。

#### 考えられる原因

[ 即転送 ] を押したユーザのボイス メッセージ プロファイルに、ボイス メッセージ パイロットが設定されていません。

#### 対応策

ユーザのボイス メッセージ プロファイルに、ボイス メッセージ パイロットを設定します。

### 一時エラー発生

#### 症状

ユーザが [ 即転送 ] を押すと、電話機にこのメッセージが表示されます。

#### 考えられる原因

ボイス メッセージ システムが機能していないか、ネットワークに問題があります。

#### 対応策

ボイス メッセージ システムをトラブルシューティングします。トラブルシューティングまたはボイス メッセージのドキュメントを参照してください。

### 話中

#### 症状

ユーザが [ 即転送 ] を押すと、電話機にこのメッセージが表示されます。

#### 考えられる原因

このメッセージは、ボイス メッセージ システムがビジーになっていることを意味します。

#### 対応策

追加のボイス メッセージ ポートを設定するか、操作をもう一度実行します。

■ 即時転送のトラブルシューティング



## TAC への問い合わせ

---

シスコと正式なサービス契約を交わしているすべてのお客様、パートナー、および代理店は、Cisco Technical Support で 24 時間テクニカル サポートを利用することができます。Cisco Technical Support Web サイトでは、シスコ製品やシスコの技術に関するトラブルシューティングにお役立ていただけるように、オンラインでマニュアルやツールを提供しています。この Web サイトは、24 時間 365 日、いつでも利用可能です。URL は次のとおりです。

<http://www.cisco.com/techsupport>

オンラインの TAC Service Request Tool を使用すると、S3 と S4 のサービス リクエストを短時間でオープンできます (S3 : ネットワークに軽微な障害が発生した、S4 : 製品情報が必要である)。状況を入力すると、その状況を解決するための推奨手段が自動的に検索されます。これらの推奨手段で問題を解決できない場合は、Cisco TAC のエンジニアが対応します。TAC Service Request Tool には、次の URL からアクセスできます。

<http://www.cisco.com/techsupport/servicerequest>

S1 または S2 のサービス リクエストの場合、またはインターネットにアクセスできない場合は、Cisco TAC に電話でお問い合わせください (S1 : ネットワークがダウンした、S2 : ネットワークの機能が著しく低下した)。S1 および S2 のサービス リクエストには、Cisco TAC のエンジニアがすぐに割り当てられ、業務を円滑に継続できるようサポートします。

Cisco TAC の連絡先については、次の URL を参照してください。

<http://www.cisco.com/techsupport/contacts>

この項では、TAC にお問い合わせいただく際に必要な情報の種類、および TAC の担当者と情報を共有する方法について説明します。

- [必要な情報 \(P.A-2\)](#)
- [必要な予備情報 \(P.A-2\)](#)
- [オンラインの利用 \(P.A-4\)](#)
- [Cisco Live! \(P.A-4\)](#)
- [リモート アクセス \(P.A-4\)](#)
- [Cisco Secure Telnet \(P.A-5\)](#)

## 必要な情報

Cisco TAC へのお問い合わせに際しては、問題点を識別して限定しやすくするために、予備情報をご提供いただく必要があります。問題の性質によっては、追加情報をご提供いただく場合もあります。お問い合わせをした後に、エンジニアが求める次の情報を収集した場合には、必然的に解決が遅れます。

- [必要な予備情報](#)
  - [ネットワーク レイアウト](#)
  - [問題の説明](#)
  - [一般的な情報](#)
- [オンラインの利用](#)
- [Cisco Live!](#)
- [リモート アクセス](#)
- [Cisco Secure Telnet](#)

## 必要な予備情報

すべての問題について、次の情報は必ず TAC に提供してください。TAC に問い合わせを行う際に使用できるように、これらの情報を収集および保存しておき、変更については定期的に更新してください。

- [ネットワーク レイアウト](#)
- [問題の説明](#)
- [一般的な情報](#)

## ネットワーク レイアウト

物理的な構成と論理的な構成に関する詳細な説明、および音声ネットワークに關与する次のネットワーク要素（該当する場合）に関する詳細な説明です。

- Cisco Unified Communications Manager
  - バージョン（Cisco Unified Communications Manager の管理ページで [バージョン情報] を選択して確認します）
  - Cisco Unified Communications Manager の数
  - 構成（スタンドアロン、クラスタ）
- Unity
  - バージョン（Cisco Unified Communications Manager の管理ページで確認します）
  - 統合タイプ
- アプリケーション
  - インストールされているアプリケーションのリスト
  - 各アプリケーションのバージョン番号
- IP/ 音声ゲートウェイ
  - OS バージョン
  - Show tech（IOS ゲートウェイ）
  - Cisco Unified Communications Manager ロード（Skinny ゲートウェイ）
- スイッチ
  - OS バージョン

- VLAN 設定
- ダイアル プラン : 番号付け方式、コール ルーティング

可能な場合は、Visio またはその他の詳細な図 (JPG など) を提出してください。Cisco Live! セッションで、ホワイトボードを使用して図を用意することもできます。

## 問題の説明

問題発生時にユーザが実行した操作を順序どおりに説明した詳細な情報を用意してください。その中には次の項目を含めてください。

- 予想した動作
- 実際の動作の詳細

## 一般的な情報

次の情報をすぐに提示できるようにしておいてください。

- 新しいバージョンをインストールしているか。
- 古いバージョンの Cisco Unified Communications Manager をインストールしている場合、この問題は当初から発生していたか (当初は発生していなかった場合、システムに対して最近どのような変更を行ったか)。
- この問題は再現可能か。
  - 再現可能な場合、それは通常の場合か、それとも特殊な状況か。
  - 再現不能な場合、問題が実際に発生した状況に関して何か特別な情報はあるか。
  - 問題が発生する頻度はどのくらいか。
- 影響を受けるデバイスは何か。
  - 特定の複数デバイスが影響を受ける場合 (影響を受けるデバイスがいつも決まっている場合) それらのデバイスに共通することは何か。
  - 問題に関与するすべてのデバイスの DN または IP アドレス (ゲートウェイの場合)。
- Call-Path 上にあるデバイスは何か (該当する場合)。

## オンラインの利用

Cisco.com を利用したオンラインの問い合わせは、その他のすべての方法に優先して取り扱われます。優先度の高い問い合わせ (P1 および P2) は、この規則の例外となります。

CCO を利用して問い合わせを行う際は、問題を正確に記述する必要があります。その記述により、それに応じた解決方法を提供すると考えられる URL リンクが返されます。

問題の解決方法が見つからない場合は、その問い合わせ内容を TAC エンジニアに送信するプロセスに進みます。

## Cisco Live!

暗号化されたセキュアな Java アプレットである Cisco Live! では、Collaborative Web Browsing および URL 共有、ホワイトボード、Telnet、およびクリップボードの各ツールを利用することによって、Cisco TAC エンジニアと協力して、より効果的に作業を進めることができます。

Cisco Live! には、次の URL でアクセスします。

<http://c3.cisco.com/>

## リモート アクセス

リモート アクセスにより、必要なすべての機器に対して、Terminal Services( リモート ポート 3389 )、HTTP( リモート ポート 80 )、および Telnet( リモート ポート 23 )の各セッションを確立できます。



### 注意

ダイヤルインを設定するときは、**login:cisco** および **password:cisco** を使用しないでください。これらは、システムに脆弱性をもたらす要因となります。

次のいずれかの方法により、デバイスに対するリモート アクセスを TAC エンジニアに許可することで、多くの問題を非常に迅速に解決できます。

- パブリック IP アドレスを持つ機器
- ダイヤルイン アクセス:( 優先順位の高いものから )アナログ モデム、Integrated Services Digital Network ( ISDN; サービス総合デジタルネットワーク ) モデム、Virtual Private Network ( VPN; バーチャルプライベートネットワーク )
- Network Address Translation ( NAT; ネットワーク アドレス変換 ): プライベート IP アドレスを持つ機器に対するアクセスを許可する IOS および Private Internet Exchange ( PIX )

エンジニアの介入時にファイアウォールが IOS トラフィックおよび PIX トラフィックを遮断しないこと、および Terminal Services などの必要なすべてのサービスがサーバ上で起動していることを確認してください。



### (注)

TAC は、すべてのアクセス情報の取り扱いに最大限の注意を払います。また、お客様の同意なしにシステムに変更を加えることはありません。

## Cisco Secure Telnet

Cisco Secure Telnet を使用すると、Cisco Service Engineer (CSE; シスコ サービス エンジニア) は、ファイアウォールを介してお客様のサイトの Cisco Unified Communications Manager サーバに透過的にアクセスできます。

Cisco Secure Telnet が機能するためには、シスコシステムズのファイアウォールの内側にある Telnet クライアントが、お客様のファイアウォールの内側にある Telnet デーモンに接続できるようにする必要があります。このセキュアな接続により、ファイアウォールを変更せずに、お客様の Cisco Unified Communications Manager サーバの監視およびメンテナンスをリモートで行うことができます。



(注)

シスコは、必ずお客様の許可を得た上で、お客様のネットワークにアクセスします。作業を開始する場合は、お客様のサイトでネットワーク管理者のご協力をお願いしています。

## ファイアウォール保護

ほぼすべての内部ネットワークでは、ファイアウォールアプリケーションを使用して、内部ホストシステムに対する外部アクセスを制限しています。これらのアプリケーションは、ネットワークとパブリック インターネット間の IP 接続を制限することで、ネットワークを保護しています。

ファイアウォールの機能は、外部で開始された TCP/IP 接続を許可するように設定が変更されない限り、そのような接続を自動的にブロックすることです。

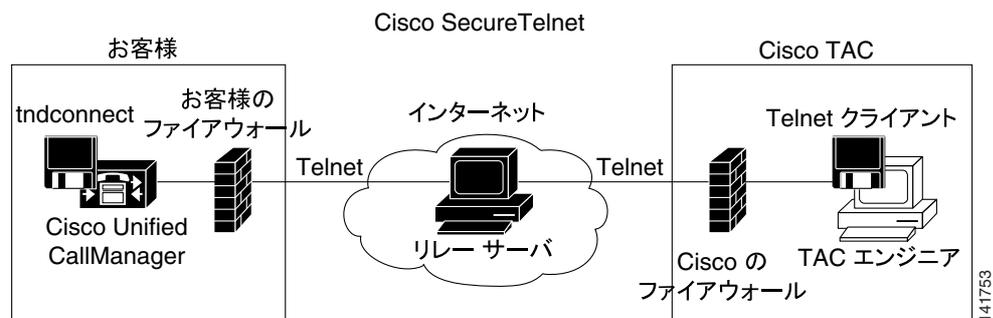
通常、企業ネットワークはパブリック インターネットとの通信を許可します。ただし、外部ホストへの接続がファイアウォールの内側で開始された場合に限りです。

## Cisco Secure Telnet の設計

Cisco Secure Telnet では、Telnet 接続がファイアウォールの内側から簡単に開始できるという点を利用しています。外部のプロキシ マシンを使用して、システムはファイアウォールの内側から Cisco Technical Assistance Center (TAC) にある別のファイアウォールの内側のホストへ TCP/IP 通信をリレーします。

このリレー サーバを使用することで、保護されたりリモート システム間のセキュアな通信がサポートされるとともに、両方のファイアウォールの整合性が維持されます。

図 A-1 Cisco Secure Telnet システム



## Cisco Secure Telnet の構造

外部リレー サーバは Telnet トンネルを構築することにより、お客様のネットワークとシスコシステムズ間の接続を確立します。この処理によって、Cisco Unified Communications Manager サーバの IP アドレスとパスワード識別情報を CSE に送信できるようになります。



(注) パスワードは、お客様側の管理者と CSE が相互に同意したテキスト文字列で構成されます。

管理者は Telnet トンネルを起動してプロセスを開始します。この操作により、お客様側のファイアウォールの内側からパブリック インターネット上のリレー サーバへの TCP 接続が確立されます。その後、Telnet トンネルによって、お客様のローカル Telnet サーバへの別の接続が確立され、エンティティ間に双方向のリンクが作成されます。



(注) Cisco TAC の Telnet クライアントは、Windows NT および Windows 2000 上のシステムまたは UNIX オペレーティングシステムのもとで動作します。

お客様のサイトの Cisco Communications Manager がパスワードを受け入れた後、Cisco TAC で動作している Telnet クライアントは、お客様側のファイアウォールの内側で実行されている Telnet デモンに接続します。その結果、透過的な接続が実現するので、ローカルでマシンを使用している場合と同様のアクセスが可能になります。

Telnet 接続が安定した後に、CSE はすべてのリモート サービスアビリティ機能を使用して、Cisco Unified Communications Manager サーバに対してメンテナンス、診断、およびトラブルシューティングの各作業を実行できます。

CSE によって送信されたコマンドおよび Cisco Unified Communications Manager サーバからの応答を表示することができますが、これらのコマンドおよび応答は必ずしも完全にフォーマットされているとは限りません。



A P P E N D I X

**B**

## ケーススタディ: Cisco Unified IP Phone コールのトラブルシューティング

---

この付録では、次の2つのケーススタディを取り上げます。

- [クラスタ内 Cisco Unified IP Phone コールのトラブルシューティング](#)
- [クラスタ間 Cisco Unified IP Phone コールのトラブルシューティング](#)

## クラスタ内 Cisco Unified IP Phone コールのトラブルシューティング

この項のケーススタディでは、クラスタ内コールと呼ばれる、1つのクラスタ内にある2台の Cisco Unified IP Phone 間のコールフローについて詳細に説明します。また、このケーススタディでは、Cisco Unified Communications Manager と Cisco Unified IP Phone の初期化、登録、およびキープアライブの各プロセスについても取り上げます。クラスタ内コールフローに関する詳細な説明はその後続きます。各プロセスの説明では、第2章「トラブルシューティングツール」で取り上げているトレースユーティリティおよびツールを使用します。

この章では、次のトピックについて取り上げます。

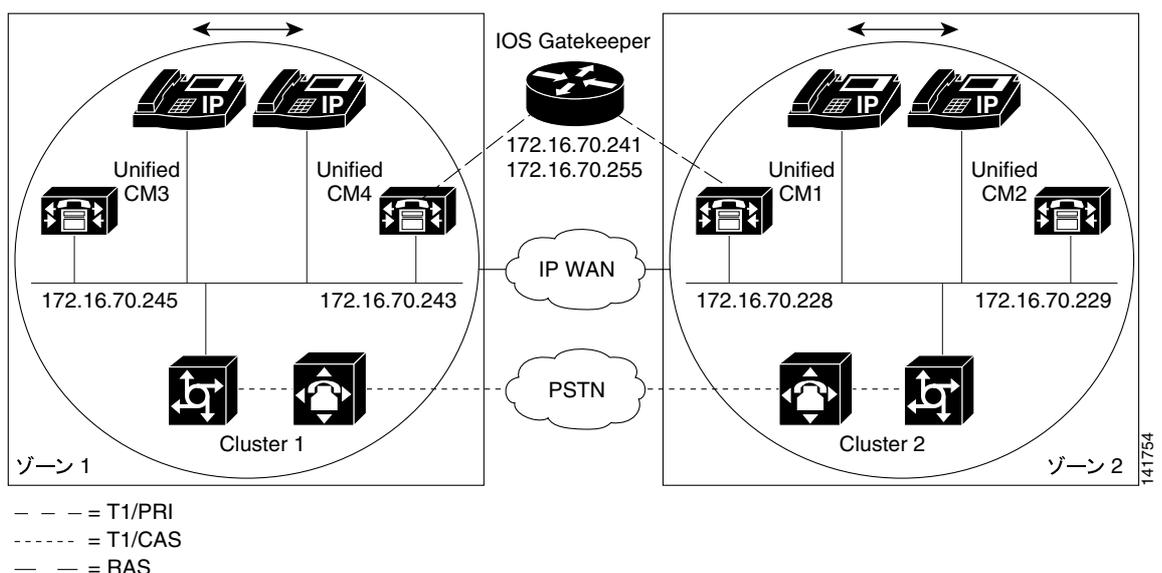
- [トポロジの例](#)
- [Cisco Unified IP Phone の初期化プロセス](#)
- [Cisco Unified Communications Manager の初期化プロセス](#)
- [自己起動プロセス](#)
- [Cisco Unified Communications Manager の登録プロセス](#)
- [Cisco Unified Communications Manager の KeepAlive プロセス](#)
- [Cisco Unified Communications Manager のクラスタ内コールフローのトレース](#)

### トポロジの例

Cluster 1 および Cluster 2 という2つのクラスタがあります。Cluster 1 には Unified CM3 および Unified CM4 という2つの Cisco Unified Communications Manager があり、Cluster 2 には Unified CM1 および Unified CM2 という2つの Cisco Unified Communications Manager があります。

このケーススタディのトレースは、Cluster 2 にある Unified CM1 から収集されたものです ( [図 B-1](#) を参照 )。Cluster 2 にある2台の Cisco Unified IP Phone がコールフローのベースです。これら2台の Cisco Unified IP Phone の IP アドレスは、それぞれ 172.16.70.230 ( 電話番号 1000 ) と 172.16.70.231 ( 電話番号 1001 ) です。

図 B-1 Cisco IP Phone と Cisco IP Phone 間のクラスタ内コールのトポロジの例



## Cisco Unified IP Phone の初期化プロセス

Cisco Unified IP Phone の初期化（ブートアップ）プロセスの詳細な手順を次に示します。

### 手順

- 
- ステップ 1** DHCP サーバで適切なオプション（Option 066、Option 150 など）が設定されていれば、Cisco Unified IP Phone は初期化時に DHCP サーバに対して要求を送信し、IP アドレス、Domain Name System（DNS; ドメイン ネーム システム）サーバのアドレス、および TFTP サーバの名前またはアドレスを取得します。また、DHCP サーバで該当するオプション（Option 003）が設定されている場合は、デフォルトゲートウェイのアドレスも取得します。
- ステップ 2** DHCP が TFTP サーバの DNS 名を送信する場合は、その名前を IP アドレスにマッピングするために DNS サーバの IP アドレスが必要になります。DHCP サーバが TFTP サーバの IP アドレスを送信する場合は、この手順を省略します。このケーススタディでは、DNS は設定されていないので、DHCP サーバは TFTP の IP アドレスを送信しました。
- ステップ 3** DHCP 応答に TFTP サーバ名が含まれていない場合、Cisco IP Phone はデフォルトのサーバ名を使用します。
- ステップ 4** 設定ファイル（.cnf）は TFTP サーバから取得されます。すべての .cnf ファイルには、SEP<MAC アドレス>.cnf という名前が付いています。この電話機を初めて Cisco Unified Communications Manager に登録する場合は、デフォルトファイルの SEPdefault.cnf が Cisco Unified IP Phone にダウンロードされます。このケーススタディでは、1 台目の Cisco Unified IP Phone は IP アドレス 172.16.70.230（MAC アドレスは SEP0010EB001720）、2 台目の Cisco Unified IP Phone は IP アドレス 172.16.70.231（MAC アドレスは SEP003094C26105）をそれぞれ使用します。
- ステップ 5** すべての .cnf ファイルには、プライマリおよびセカンダリの Cisco Unified Communications Manager の IP アドレスが含まれています。Cisco Unified IP Phone は、この IP アドレスを使用してプライマリ Cisco Unified Communications Manager に接続して登録します。
- ステップ 6** Cisco Unified IP Phone が Cisco Unified Communications Manager に接続して登録すると、Cisco Unified Communications Manager は、使用する実行ファイルのバージョン（ロード ID と呼ばれる）をその Cisco Unified IP Phone に通知します。指定されたバージョンが Cisco Unified IP Phone 上の実行ファイルのバージョンと一致しない場合、Cisco Unified IP Phone は新しい実行ファイルのバージョンを TFTP サーバに要求し、自動的にリセットします。
- 

## Cisco Unified Communications Manager の初期化プロセス

この項では、Unified CM1（IP アドレス 172.16.70.228 で識別される）から取り込んだトレースを使用して、Cisco Unified Communications Manager の初期化プロセスについて説明します。前述のように、SDI トレースは、エンドポイント間で送信されたすべてのパケットに関する詳細情報を提供するもので、非常に効果的なトラブルシューティングツールです。

この項では、Cisco Unified Communications Manager の初期化時に発生するイベントについて説明します。トレースの見方を理解していれば、Cisco Unified Communications Manager の各プロセスのトラブルシューティング、およびそれらのプロセスがサービス（会議、転送など）に及ぼす影響のトラブルシューティングを適切に行うことができます。

次のメッセージは、Cisco Unified Communications Manager SDI トレースユーティリティから出力され、Cisco Unified Communications Manager の 1 つ (このケーススタディでは Unified CM1) に対する初期化プロセスを示しています。

- 最初のメッセージは、Cisco Unified Communications Manager が自分の初期化プロセスを開始したことを示しています。
- 2 番目のメッセージは、Cisco Unified Communications Manager がデフォルト データベース (このケーススタディではプライマリ データベースまたはパブリッシュ データベース) の値を読み取ったことを示しています。
- 3 番目のメッセージは、Cisco Unified Communications Manager が TCP ポート 8002 で各種メッセージを受信したことを示しています。
- 4 番目のメッセージは、それらのメッセージを受信した後に、Cisco Unified Communications Manager が 2 つ目の Cisco Unified Communications Manager (Unified CM2 (172.16.70.229)) を自分のリストに加えたことを示しています。
- 5 番目のメッセージは、Cisco Unified Communications Manager が起動し、Cisco Unified Communications Manager バージョン 3.1(1) を実行していることを示しています。

```
16:02:47.765 CCM|CMProcMon - Communications ManagerState Changed - Initialization
Started.
16:02:47.796 CCM|NodeId: 0, EventId: 107 EventClass: 3 EventInfo: Cisco CCMDatabase
Defaults Read
16:02:49.937 CCM| SDL Info - NodeId: [1], Listen IP/Hostname: [172.16.70.228], Listen
Port: [8002]
16:02:49.984 CCM|dBProcs - Adding SdlLink to NodeId: [2], IP/Hostname: [172.16.70.229]
16:02:51.031 CCM|NodeId: 1, EventId: 1 EventClass: 3 EventInfo: Cisco CallManager
Version=<3.1(1)> started
```

## 自己起動プロセス

Cisco Unified Communications Manager は、稼働状態になると、その内部で他のプロセスをいくつか起動します。それらのプロセスには、MulticastPoint Manager、UnicastBridge Manager、番号分析、ルートリストなどがあります。これらのプロセスの実行中に出力されるメッセージは、Cisco Unified Communications Manager の機能に関連する問題のトラブルシューティングに非常に役立ちます。

たとえば、ルートリストが機能を停止して使用不可になっているとします。この問題のトラブルシューティングを行うには、これらのトレースを監視して、Cisco Unified Communications Manager が RoutePlanManager をすでに起動したか、および RouteLists のロードを試行しているかを確認します。次に示す設定の例は、RouteListName="ipwan" および RouteGroupName="ipwan" がロードおよび起動していることを示しています。

```

16:02:51.031 CCM|MulicastPointManager - Started
16:02:51.031 CCM|UnicastBridgeManager - Started
16:02:51.031 CCM|MediaTerminationPointManager - Started
16:02:51.125 CCM|MediaCoordinator(1) - started
16:02:51.125 CCM|NodeId: 1, EventId: 1543 EventClass: 2 EventInfo: Database
manager started
16:02:51.234 CCM|NodeId: 1, EventId: 1542 EventClass: 2 EventInfo: Link manager
started
16:02:51.390 CCM|NodeId: 1, EventId: 1541 EventClass: 2 EventInfo: Digit analysis
started
16:02:51.406 CCM|RoutePlanManager - Started, loading RouteLists
16:02:51.562 CCM|RoutePlanManager - finished loading RouteLists
16:02:51.671 CCM|RoutePlanManager - finished loading RouteGroups
16:02:51.671 CCM|RoutePlanManager - Displaying Resulting RoutePlan
16:02:51.671 CCM|RoutePlanServer - RouteList Info, by RouteList and RouteGroup
Selection Order
16:02:51.671 CCM|RouteList - RouteListName='ipwan'
16:02:51.671 CCM|RouteList - RouteGroupName='ipwan'
16:02:51.671 CCM|RoutePlanServer - RouteGroup Info, by RouteGroup and Device Selection
Order
16:02:51.671 CCM|RouteGroup - RouteGroupName='ipwan'

```

次のトレースは、RouteGroup がデバイス 172.16.70.245 を追加していることを示しています。このデバイスは Cluster 1 に配置された Unified CM3 で、H.323 デバイスであると見なされます。このケーススタディでは、RouteGroup は、Cisco IOS Gatekeeper の許可を得てコールを Cluster 1 の Unified CM3 にルーティングするために作成されています。Cluster 1 に配置された Cisco Unified IP Phone へのコールのルーティング中に問題が発生した場合、その原因を特定するには次のメッセージが役立ちます。

```

16:02:51.671 CCM|RouteGroup - DeviceName='172.16.70.245'
16:02:51.671 CCM|RouteGroup -AllPorts

```

一部の初期化プロセスは、Cisco Unified Communications Manager が「Dn」（電話番号）を追加していることを示しています。これらのメッセージを確認することで、Cisco Unified Communications Manager がデータベースから電話番号を読み取ったかどうかを判別できます。

```

16:02:51.671 CCM|NodeId: 1, EventId: 1540 EventClass: 2 EventInfo: Call control
started
16:02:51.843 CCM|ProcessDb - Dn = 2XXX, Line = 0, Display = ,
RouteThisPattern, NetworkLocation = OffNet, DigitDiscardingInstruction = 1,
WhereClause =
16:02:51.859 CCM|Digit analysis: Add local pattern 2XXX , PID: 1,80,1
16:02:51.859 CCM|ForwardManager - Started
16:02:51.984 CCM|CallParkManager - Started
16:02:52.046 CCM|ConferenceManager - Started

```

次のトレースでは、Cisco Unified Communications Manager の Device Manager が 2 つのデバイスを静的に初期化しています。IP アドレス 172.17.70.226 のデバイスはゲートキーパーを表し、IP アドレス 172.17.70.245 のデバイスは異なるクラスタにある別の Cisco Unified Communications Manager を取得します。その Cisco Unified Communications Manager は、H.323 ゲートウェイとしてこの Cisco Unified Communications Manager に登録されます。

```

16:02:52.250 CCM|DeviceManager: Statically Initializing Device;
DeviceName=172.16.70.226
16:02:52.250 CCM|DeviceManager: Statically Initializing Device;
DeviceName=172.16.70.245

```

## Cisco Unified Communications Manager の登録プロセス

SDI トレースでは、登録プロセスも重要な要素です。デバイスは電源がオンになると、DHCP を介して情報を取得し、TFTP サーバに接続して自分の .cnf ファイルを取得し、その .cnf ファイルで指定されている Cisco Unified Communications Manager に接続します。そのデバイスは、MGCP ゲートウェイ、Skinny ゲートウェイ、または Cisco Unified IP Phone である可能性があります。したがって、Cisco ネットワークでデバイスが正常に登録されたかどうかを検出できることが重要になります。

次のトレースでは、Cisco Unified Communications Manager が登録のための新しい接続を受信しています。登録するデバイスは、MTP\_nsa-cm1 (Unified CM1 上の MTP サービス) および CFB\_nsa-cm1 (Unified CM1 上の会議ブリッジ サービス) で構成されます。これらは Cisco Unified Communications Manager で動作しているソフトウェア サービスですが、内部的には異なる外部サービスとして扱われるため、TCPHandle、ソケット番号、ポート番号、およびデバイス名が割り当てられます。

```
16:02:52.750 CCM|StationInit - New connection accepted. DeviceName=,
TCPHandle=0x4fbba00, Socket=0x594, IPAddr=172.16.70.228, Port=3279, StationD=[0,0,0]
16:02:52.750 CCM|StationInit - New connection accepted. DeviceName=,
TCPHandle=0x4fe05e8, Socket=0x59c, IPAddr=172.16.70.228, Port=3280, StationD=[0,0,0]
16:02:52.781 CCM|StationInit - Processing StationReg. regCount: 1
DeviceName=MTP_nsa-cm1, TCPHandle=0x4fbba00, Socket=0x594, IPAddr=172.16.70.228,
Port=3279, StationD=[1,45,2]
16:02:52.781 CCM|StationInit - Processing StationReg. regCount: 1
DeviceName=CFB_nsa-cm1, TCPHandle=0x4fe05e8, Socket=0x59c, IPAddr=172.16.70.228,
Port=3280, StationD=[1,96,2]
```

## Cisco Unified Communications Manager の KeepAlive プロセス

ステーション、デバイス、またはサービスと Cisco Unified Communications Manager は、相互間の通信チャンネルに関する情報を保持するために次のメッセージを使用します。このメッセージは、Cisco Unified Communications Manager とステーション間の通信リンクがアクティブ状態を維持するためのキープアライブシーケンスを開始します。次のメッセージは、Cisco Unified Communications Manager とステーションのどちらからでも発信できます。

```
16:03:02.328 CCM|StationInit - InboundStim - KeepAliveMessage - Forward KeepAlive to
StationD. DeviceName=MTP_nsa-cm2, TCPHandle=0x4fa7dc0, Socket=0x568,
IPAddr=172.16.70.229, Port=1556, StationD=[1,45,1]
16:03:02.328 CCM|StationInit - InboundStim - KeepAliveMessage - Forward KeepAlive to
StationD. DeviceName=CFB_nsa-cm2, TCPHandle=0x4bf8a70, Socket=0x57c,
IPAddr=172.16.70.229, Port=1557, StationD=[1,96,1]
16:03:06.640 CCM|StationInit - InboundStim - KeepAliveMessage - Forward KeepAlive to
StationD. DeviceName=SEP0010EB001720, TCPHandle=0x4fbb150, Socket=0x600,
IPAddr=172.16.70.230, Port=49211, StationD=[1,85,2]
16:03:06.703 CCM|StationInit - InboundStim - KeepAliveMessage - Forward KeepAlive to
StationD. DeviceName=SEP003094C26105, TCPHandle=0x4fbbc30, Socket=0x5a4,
IPAddr=172.16.70.231, Port=52095, StationD=[1,85,1]
```

次のトレースに含まれるメッセージは、Cisco Unified Communications Manager とステーション間の通信リンクがアクティブであることを示すキープアライブシーケンスを表しています。これらのメッセージも、Cisco Unified Communications Manager とステーションのどちらからでも発信できます。

```
16:03:02.328 CCM|MediaTerminationPointControl - stationOutputKeepAliveAck
tcpHandle=4fa7dc0
16:03:02.328 CCM|UnicastBridgeControl - stationOutputKeepAliveAck tcpHandle=4bf8a70
16:03:06.703 CCM|StationInit - InboundStim - IpPortMessageID: 32715(0x7fcb)
tcpHandle=0x4fbbc30
16:03:06.703 CCM|StationD - stationOutputKeepAliveAck tcpHandle=0x4fbbc30
```

## Cisco Unified Communications Manager のクラスタ内コールフローのトレース

この項の SDI トレースは、クラスタ内コールフローの詳細を示しています。コールフローの Cisco Unified IP Phone は、電話番号 (dn)、tcpHandle、および IP アドレスで識別できます。Cluster 2 に配置された Cisco Unified IP Phone (dn: 1001、tcpHandle: 0x4fbbc30、IP アドレス: 172.16.70.231) は、同一クラスタ内の別の Cisco Unified IP Phone (dn: 1000、tcpHandle: 0x4fbb150、IP アドレス: 172.16.70.230) にコールを発信します。TCP ハンドル値、タイムスタンプ、またはデバイスの名前を調べることで、デバイスをトレース上で追跡できます。デバイスをリポートするかオフラインにするまで、デバイスの TCP ハンドル値は変わりません。

次のトレースは、Cisco Unified IP Phone (1001) がオフフックになっていることを示しています。下記のトレースは、一意のメッセージ、TCP ハンドル、および着信側の番号を示しています。これらは Cisco Unified IP Phone に表示されます。この時点では、まだユーザが番号をダイヤルしていないので、発信側の番号は表示されていません。次の情報は、Cisco Unified IP Phone と Cisco Unified Communications Manager 間の Skinny Station メッセージの形式で表示されます。

```
16:05:41.625 CCM|StationInit - InboundStim - OffHookMessageID tcpHandle=0x4fbbc30
16:05:41.625 CCM|StationD - stationOutputDisplayText tcpHandle=0x4fbbc30, Display=
1001
```

次のトレースは、Cisco Unified Communications Manager から Cisco Unified IP Phone に発信された Skinny Station メッセージを示しています。最初のメッセージは、発信側の Cisco Unified IP Phone のランプをオンにします。

```
16:05:41.625 CCM|StationD - stationOutputSetLamp stim: 9=Line instance=1
lampMode=LampOn tcpHandle=0x4fbbc30
```

Cisco Unified Communications Manager は、stationOutputCallState メッセージを使用して、特定のコールに関する情報をステーションに通知します。

```
16:05:41.625 CCM|StationD - stationOutputCallState tcpHandle=0x4fbbc30
```

Cisco Unified Communications Manager は、stationOutputDisplayPromptStatus メッセージを使用して、コールに関するプロンプトメッセージを Cisco Unified IP Phone に表示します。

```
16:05:41.625 CCM|StationD - stationOutputDisplayPromptStatus tcpHandle=0x4fbbc30
```

Cisco Unified Communications Manager は、stationOutputSelectSoftKey メッセージを使用して、Skinny Station で特定のソフトキーのセットを選択します。

```
16:05:41.625 CCM|StationD - stationOutputSelectSoftKeys tcpHandle=0x4fbbc30
```

Cisco Unified Communications Manager は、次のメッセージを使用して、表示用の正確な回線コンテキストについて Skinny Station に指示します。

```
16:05:41.625 CCM|StationD - stationOutputActivateCallPlane tcpHandle=0x4fbbc30
```

次のメッセージは、番号分析プロセスによって、着信番号の識別、およびデータベース内にルーティングの一致があるかどうかの確認ができる状態になっていることを示します。エントリ cn=1001 は発信側の番号を表しています。dd="" はダイヤルされた番号であり、着信側の番号を示しています。電話機が StationInit メッセージを送信し、Cisco Unified Communications Manager が StationD メッセージを送信した後に、Cisco Unified Communications Manager は番号分析を実行します。

```
16:05:41.625 CCM|Digit analysis: match(fqcn="", cn="1001", pss="", dd="")
16:05:41.625 CCM|Digit analysis: potentialMatches=PotentialMatchesExist
```

次のデバッグメッセージは、Cisco Unified Communications Manager が発信側の Cisco Unified IP Phone に内部発信音を鳴らしていることを示しています。

```
16:05:41.625 CCM|StationD - stationOutputStartTone: 33=InsideDialTone
tcpHandle=0x4fbbc30
```

Cisco Unified Communications Manager は着信メッセージを検出し、Cisco Unified IP Phone のキーパッド ボタン 1 が押されたことを認識すると、ただちに出力トーンを停止します。

```
16:05:42.890 CCM|StationInit - InboundStim - KeypadButtonMessageID kpButton: 1
tcpHandle=0x4fbbc30
16:05:42.890 CCM|StationD - stationOutputStopTone tcpHandle=0x4fbbc30
16:05:42.890 CCM|StationD - stationOutputSelectSoftKeys tcpHandle=0x4fbbc30
16:05:42.890 CCM|Digit analysis: match(fqcn="", cn="1001", pss="", dd="1")
16:05:42.890 CCM|Digit analysis: potentialMatches=PotentialMatchesExist
16:05:43.203 CCM|StationInit - InboundStim - KeypadButtonMessageID kpButton: 0
tcpHandle=0x4fbbc30
16:05:43.203 CCM|Digit analysis: match(fqcn="", cn="1001", pss="", dd="10")
16:05:43.203 CCM|Digit analysis: potentialMatches=PotentialMatchesExist
16:05:43.406 CCM|StationInit - InboundStim - KeypadButtonMessageID kpButton: 0
tcpHandle=0x4fbbc30
16:05:43.406 CCM|Digit analysis: match(fqcn="", cn="1001", pss="", dd="100")
16:05:43.406 CCM|Digit analysis: potentialMatches=PotentialMatchesExist
16:05:43.562 CCM|StationInit - InboundStim - KeypadButtonMessageID kpButton: 0
tcpHandle=0x4fbbc30
16:05:43.562 CCM|Digit analysis: match(fqcn="", cn="1001", pss="", dd="1000")
```

Cisco Unified Communications Manager は、一致していると判別できるだけの番号を受信すると、番号分析の結果をテーブル形式で表示します。一致するものがすでに見つかっているので、Cisco Unified Communications Manager は、それ以降に電話機で押された番号をすべて無視します。

```
16:05:43.562 CCM|Digit analysis: analysis results
16:05:43.562 CCM||PretransformCallingPartyNumber=1001
|CallingPartyNumber=1001
|DialingPattern=1000
|DialingRoutePatternRegularExpression=(1000)
|PotentialMatches=PotentialMatchesExist
|DialingSdlProcessId=(1,38,2)
|PretransformDigitString=1000
|PretransformPositionalMatchList=1000
|CollectedDigits=1000
|PositionalMatchList=1000
|RouteBlockFlag=RouteThisPattern
```

次のトレースは、Cisco Unified Communications Manager がこの情報を着信側の電話機に送信していることを示しています（電話機は tcpHandle 番号で識別されます）。

```
16:05:43.578 CCM|StationD - stationOutputCallInfo CallingPartyName=1001,
CallingParty=1001, CalledPartyName=1000, CalledParty=1000, tcpHandle=0x4fbb150
```

次のトレースは、Cisco Unified Communications Manager が、着信側の Cisco Unified IP Phone にある着信コール用ランプを点滅するように指示していることを示しています。

```
16:05:43.578 CCM|StationD - stationOutputSetLamp stim: 9=Line instance=1
lampMode=LampBlink tcpHandle=0x4fbb150
```

次のトレースでは、Cisco Unified Communications Manager が、呼び出し音や表示通知などのコール関連の情報を着信側の Cisco Unified IP Phone に提供しています。ここでも、トレース全体を通して同じ tcpHandle が使用されているので、すべてのメッセージが同じ Cisco Unified IP Phone に送信されていることを確認できます。

```
16:05:43.578 CCM|StationD - stationOutputSetRinger: 2=InsideRing tcpHandle=0x4fbb150
16:05:43.578 CCM|StationD - stationOutputDisplayNotify tcpHandle=0x4fbb150
16:05:43.578 CCM|StationD - stationOutputDisplayPromptStatus tcpHandle=0x4fbb150
16:05:43.578 CCM|StationD - stationOutputSelectSoftKeys tcpHandle=0x4fbb150
```

Cisco Unified Communications Manager が発信側の Cisco Unified IP Phone にも同様の情報を提供していることに注意してください。ここでも、Cisco Unified IP Phone は tcpHandle によって識別されます。

```
16:05:43.578 CCM|StationD - stationOutputCallInfo CallingPartyName=1001,
CallingParty=1001, CalledPartyName=, CalledParty=1000, tcpHandle=0x4fbbc30
16:05:43.578 CCM|StationD - stationOutputCallInfo CallingPartyName=1001,
CallingParty=1001, CalledPartyName=1000, CalledParty=1000, tcpHandle=0x4fbbc30
```

次のトレースでは、Cisco Unified Communications Manager がアラート音または呼び出し音を発信側の Cisco Unified IP Phone で鳴らし、接続が確立されたことを通知しています。

```
16:05:43.578 CCM|StationD - stationOutputStartTone: 36=AlertingTone
tcpHandle=0x4fbbc30
16:05:43.578 CCM|StationD - stationOutputCallState tcpHandle=0x4fbbc30
16:05:43.578 CCM|StationD - stationOutputSelectSoftKeys tcpHandle=0x4fbbc30
16:05:43.578 CCM|StationD - stationOutputDisplayPromptStatus tcpHandle=0x4fbbc30
```

この時点で、着信側の Cisco Unified IP Phone はオフフックになるので、Cisco Unified Communications Manager は発信側での呼び出し音を停止します。

```
16:05:45.140 CCM|StationD - stationOutputStopTone tcpHandle=0x4fbbc30
```

次のメッセージでは、Cisco Unified Communications Manager が Skinny Station に Unicast RTP ストリームの受信を開始するように指示しています。そのために、Cisco Unified Communications Manager は着信側の IP アドレス、コーデック情報、およびパケットサイズ(ミリ秒)を提供します。PacketSize は、RTP パケットの作成に使用されるサンプリング時間(ミリ秒)の整数です。



**(注)** 通常、この値は 30 ミリ秒に設定されます。このケーススタディでは、20 ミリ秒に設定されます。

```
16:05:45.140 CCM|StationD - stationOutputOpenReceiveChannel tcpHandle=0x4fbbc30 myIP:
e74610ac (172.16.70.231)
16:05:45.140 CCM|StationD - ConferenceID: 0 msecPacketSize: 20
compressionType: (4)Media_Payload_G711Ulaw64k
```

同様に、Cisco Unified Communications Manager は着信側(1000)に情報を提供します。

```
16:05:45.140 CCM|StationD - stationOutputOpenReceiveChannel tcpHandle=0x4fbb150 myIP:
e64610ac (172.16.70.230)
16:05:45.140 CCM|StationD - ConferenceID: 0 msecPacketSize: 20
compressionType: (4)Media_Payload_G711Ulaw64k
```

Cisco Unified Communications Manager は、RTP ストリーム用のオープンチャネルを確立するために、着信側から確認応答メッセージを受信しました。また、着信側の IP アドレスも受信しました。このメッセージにより、Skinny Station に関する 2 種類の情報が Cisco Unified Communications Manager に通知されます。1 つは、オープンアクションのステータスです。もう 1 つは、リモートエンドへ

の伝送に使用する受信ポートのアドレスと番号です。RTP ストリームのトランスミッタ（発信側）の IP アドレスは ipAddr で、PortNumber は RTP ストリーム トランスミッタ（発信側）の IP ポート番号です。

```
16:05:45.265 CCM|StationInit - InboundStim - StationOpenReceiveChannelAckID
tcpHandle=0x4fbb150, Status=0, IpAddr=0xe64610ac, Port=17054, PartyID=2
```

Cisco Unified Communications Manager は、次のメッセージを使用して、指定のリモート Cisco Unified IP Phone の IP アドレスとポート番号に音声およびビデオ ストリームの伝送を開始するようにステーションに指示しています。

```
16:05:45.265 CCM|StationD - stationOutputStartMediaTransmission tcpHandle=0x4fbbc30
myIP: e74610ac (172.16.70.231)
16:05:45.265 CCM|StationD - RemoteIpAddr: e64610ac (172.16.70.230)
RemoteRtpPortNumber: 17054 msecPacketSize: 20
compressionType: (4)Media_Payload_G711Ulaw64k
```

```
16:03:25.328 CCM|StationD(1): TCPPIid=[1.100.117.1] OpenMultiReceiveChannel
conferenceID=16777217 passThruPartyID=1000011 compressionType=101(Media_Payload_H263)
qualifierIn=?. myIP: e98e6b80 (128.107.142.233) |<CT::1,100,11,1.1><IP::><DEV::>
```

```
16:03:25.375 CCM|StationInit: TCPPIid=[1.100.117.1]
StationOpenMultiMediaReceiveChannelAck Status=0, IpAddr=0xe98e6b80, Port=65346,
PartyID=16777233 |<CT::1,100,105,1.215><IP::128.107.142.233>
```

```
16:03:25.375 CCM|StationD(2): TCPPIid = [1.100.117.2]
star_StationOutputStartMultiMediaTransmission conferenceID=16777218
passThruPartyID=16777250 remoteIpAddress=e98e6b80(66.255.0.0)
remotePortNumber=65346 compressType=101(Media_Payload_H263) qualifierOut=?. myIP:
e98e6b80 (128.107.142.233) |<CT::1,100,105,1.215><IP::128.107.142.233>
```

次のトレースでは、前述のメッセージが着信側に送信されます。RTP メディア ストリームが着信側と発信側の間で開始されたことを示すメッセージが、これらのメッセージの後に続きます。

```
16:05:45.312 CCM|StationD - stationOutputStartMediaTransmission tcpHandle=0x4fbb150
myIP: e64610ac (172.16.70.230)
16:05:45.328 CCM|StationD - RemoteIpAddr: e74610ac (172.16.70.231)
RemoteRtpPortNumber: 18448 msecPacketSize: 20
compressionType: (4)Media_Payload_G711Ulaw64k
16:05:46.203 CCM|StationInit - InboundStim - OnHookMessageID tcpHandle=0x4fbbc30
```

最後に、発信側の Cisco IP Phone がオンフックになります。そのため、Skinny Station と Cisco Unified Communications Manager 間のすべての制御メッセージ、および Skinny Station 間の RTP ストリームが終了します。

```
16:05:46.203 CCM|StationInit - InboundStim - OnHookMessageID tcpHandle=0x4fbbc30
```

## クラスタ間 Cisco Unified IP Phone コールのトラブルシューティング

この項のケーススタディでは、異なるクラスタに配置された別の Cisco Unified IP Phone にコールを発信する Cisco Unified IP Phone について説明します。このタイプのコールをクラスタ間 Cisco Unified IP Phone コールであると見なします。

この章では、次のトピックについて取り上げます。

- [トポロジの例](#)
- [クラスタ間 H.323 通信](#)
- [コールフローのトレース](#)
- [コールフローの失敗](#)

### トポロジの例

このケーススタディでは、次に示すトポロジの例を使用します。2つのクラスタがあり、各クラスタには2つの Cisco Unified Communications Manager があります。また、Cisco IOS Gateway と Cisco IOS Gatekeeper も配置されています。

### クラスタ間 H.323 通信

Cluster 1 の Cisco IP Phone が Cluster 2 の Cisco Unified IP Phone にコールを発信します。クラスタ間 Cisco Unified Communications Manager 通信は、H.323 バージョン 2 プロトコルを使用して行われます。Cisco IOS Gatekeeper もアドミッション制御に使用されます。

Cisco Unified IP Phone は Skinny Station プロトコルを使用して Cisco Unified Communications Manager に接続でき、Cisco Unified Communications Manager は H.323 Registration, Admission, and Status (RAS) プロトコルを使用して Cisco IOS Gatekeeper に接続できます。admission request (ARQ; アドミッション要求) メッセージが Cisco IOS Gatekeeper に送信され、この Gatekeeper は H.323 バージョン 2 プロトコルを使用してクラスタ間コールが発信できることを確認した後、admission confirmed (ACF; アドミッション確認) メッセージを送信します。この処理が実行された後、RTP プロトコルを使用して、異なるクラスタにある Cisco Unified IP Phone 間に音声パスが作成されます。

### コールフローのトレース

この項では、CCM000000000 ファイルに取り込んだ SDI トレースの例を使用して、コールフローについて説明します。このケーススタディで取り上げるトレースでは、コールフロー自体に焦点を絞っています。

このコールフローでは、Cluster 2 に配置された Cisco Unified IP Phone (2002) が、Cluster 1 に配置された Cisco Unified IP Phone (1001) にコールを発信します。TCP ハンドル値、タイムスタンプ、またはデバイスの名前を調べることで、デバイスをトレース上で追跡できます。デバイスをリポートするかオフラインにするまで、デバイスの TCP ハンドル値は変わりません。

次のトレースでは、Cisco Unified IP Phone ( 2002 ) がオフフックになりました。このトレースは、一意のメッセージ、TCP ハンドル、および発信側の番号を示しています。これらは Cisco Unified IP Phone に表示されます。次のデバッグ出力は、着信側の番号 ( 1001 )、H.225 接続、および H.245 確認メッセージを示しています。コーデックタイプは G.711 mu-law です。

```
16:06:13.921 CCM|StationInit - InboundStim - OffHookMessageID tcpHandle=0x1c64310
16:06:13.953 CCM|Out Message -- H225ConnectMsg -- Protocol= H225Protocol
16:06:13.953 CCM|Ie - H225UserUserIe IEData= 7E 00 37 05 02 C0 06
16:06:13.953 CCM|StationD - stationOutputCallInfo CallingPartyName=,
CallingParty=2002, CalledPartyName=1001, CalledParty=1001, tcpHandle=0x1c64310
16:06:14.015 CCM|H245Interface(2) OLC indication chan number = 2
16:06:14.015 CCM|StationD - stationOutputOpenReceiveChannel tcpHandle=0x1c64310 myIP:
e74610ac (172.16.70.231)
16:06:14.015 CCM|StationD - ConferenceID: 0 msecPacketSize: 20
compressionType: (4)Media_Payload_G711Ulaw64k
16:06:14.062 CCM|StationInit - InboundStim - StationOpenReceiveChannelAckID
tcpHandle=0x1c64310, Status=0, IpAddr=0xe74610ac, Port=20444, PartyID=2
16:06:14.062 CCM|H245Interface(2) paths established ip = e74610ac, port = 20444
16:06:14.187 CCM|H245Interface(2) OLC outgoing confirm ip = fc4610ac, port = 29626
```

次のトレースは、発信側と着信側の番号を示しています。これらの番号は IP アドレスおよび 16 進数値に関連付けられています。

```
16:06:14.187 CCM|StationD - stationOutputStartMediaTransmission tcpHandle=0x1c64310
myIP: e74610ac (172.16.70.231)
16:06:14.187 CCM|StationD - RemoteIpAddr: fc4610ac (172.16.70.252)
```

次のトレースは、Cisco IP Phone ( 2002 ) のパケット サイズと MAC アドレスを示しています。このトレースの後に接続解除メッセージが続き、その後にオンフックメッセージが続きます。

```
RemoteRtpPortNumber: 29626 msecPacketSize: 20
compressionType: (4)Media_Payload_G711Ulaw64k
16:06:16.515 CCM| Device SEP003094C26105 , UnRegisters with SDL Link to monitor
NodeID= 1
16:06:16.515 CCM|StationD - stationOutputCloseReceiveChannel tcpHandle=0x1c64310 myIP:
e74610ac (172.16.70.231)
16:06:16.515 CCM|StationD - stationOutputStopMediaTransmission tcpHandle=0x1c64310
myIP: e74610ac (172.16.70.231)
16:06:16.531 CCM|In Message -- H225ReleaseCompleteMsg -- Protocol= H225Protocol
16:06:16.531 CCM|Ie - Q931CauseIe -- IEData= 08 02 80 90
16:06:16.531 CCM|Ie - H225UserUserIe -- IEData= 7E 00 1D 05 05 80 06
16:06:16.531 CCM|Locations:Orig=1 BW=64Dest=0 BW=-1 (-1 implies infinite bw available)
16:06:16.531 CCM|MediaManager - wait_AuDisconnectRequest - StopSession sending
disconnect to (64,2) and remove connection from list
16:06:16.531 CCM|MediaManager - wait_AuDisconnectReply - received all disconnect
replies, forwarding a reply for party1(16777219) and party2(16777220)
16:06:16.531 CCM|MediaCoordinator - wait_AuDisconnectReply - removing MediaManager(2)
from connection list
16:06:16.734 CCM|StationInit - InboundStim - OnHookMessageID tcpHandle=0x1c64310
```

## コールフローの失敗

この項では、SDI トレースを確認しながら、クラスタ間コールフローの失敗について説明します。次のトレースでは、Cisco Unified IP Phone ( 1001 ) はオフフックになります。TCP ハンドルが Cisco Unified IP Phone に割り当てられます。

```
16:05:33.468 CCM|StationInit - InboundStim - OffHookMessageID tcpHandle=0x4fbbc30
16:05:33.468 CCM|StationD - stationOutputDisplayText tcpHandle=0x4fbbc30, Display=
1001
16:05:33.484 CCM|StationD - stationOutputSetLamp stim: 9=Line instance=1
lampMode=LampOn tcpHandle=0x4fbbc30
```

次のトレースでは、ユーザが着信側の Cisco Unified IP Phone の番号 (2000) をダイヤルし、番号分析プロセスが番号を照合しようとしています。

```
16:05:33.484 CCM|Digit analysis: match(fqcn="", cn="1001", pss="", dd="")
16:05:33.484 CCM|Digit analysis: potentialMatches=PotentialMatchesExist
16:05:35.921 CCM|Digit analysis: match(fqcn="", cn="1001", pss="", dd="2")
16:05:35.921 CCM|Digit
analysis:potentialMatches=ExclusivelyOffnetPotentialMatchesExist
16:05:36.437 CCM|Digit analysis: match(fqcn="", cn="1001", pss="", dd="20")
16:05:36.437 CCM|Digit
analysis:potentialMatches=ExclusivelyOffnetPotentialMatchesExist
16:05:36.656 CCM|Digit analysis: match(fqcn="", cn="1001", pss="", dd="200")
16:05:36.656 CCM|Digit
analysis:potentialMatches=ExclusivelyOffnetPotentialMatchesExist
16:05:36.812 CCM|Digit analysis: match(fqcn="", cn="1001", pss="", dd="2000")
```

これで番号分析が完了しました。次のトレースは、その結果を示しています。次の PotentialMatches=NoPotentialMatchesExist 参照は、Cisco Unified Communications Manager がこの電話番号を照合できないことを示しています。この点に注意してください。最後に、リオーダー音が発信側 (1001) に送信され、その後にオンフックメッセージが続きます。

```
16:05:36.812 CCM|Digit analysis: analysis results
16:05:36.812 CCM||PretransformCallingPartyNumber=1001
|CallingPartyNumber=1001
|DialingPattern=2XXX
|DialingRoutePatternRegularExpression=(2XXX)
|PotentialMatches=NoPotentialMatchesExist
|CollectedDigits=2000
16:05:36.828 CCM|StationD - stationOutputCallInfo CallingPartyName=1001,
CallingParty=1001, CalledPartyName=, CalledParty=2000, tcpHandle=0x4fbbc30
16:05:36.828 CCM|StationD - stationOutputStartTone: 37=ReorderTone tcpHandle=0x4fbbc30
16:05:37.953 CCM|StationInit - InboundStim - OnHookMessageID tcpHandle=0x4fbbc30
```

■ クラスタ間 Cisco Unified IP Phone コールのトラブルシューティング



## ケーススタディ : Cisco Unified IP Phone と Cisco IOS Gateway 間のコールの トラブルシューティング

付録 B「ケーススタディ : Cisco Unified IP Phone コールのトラブルシューティング」のケーススタディでは、クラスタ内コールのコールフローについて説明しました。この付録のケーススタディでは、ローカル PBX または Public Switched Telephone Network (PSTN; 公衆電話交換網) に接続された電話機に Cisco IOS Gateway を介してコールを発信する Cisco Unified IP Phone について説明します。概念的には、コールが Cisco IOS Gateway に到達すると、ゲートウェイはそのコールを FXS ポートまたは PBX に接続された電話機のどちらかに転送します。コールが PBX に転送された場合、そのコールはローカル PBX に接続された電話機で終端するか、PBX によって PSTN に転送されて PSTN 上のどこかで終端します。

この章では、次のトピックについて取り上げます。

- [コールフローのトレース](#)
- [Cisco IOS Gatekeeper のデバッグメッセージと表示コマンド](#)
- [Cisco IOS Gateway のデバッグメッセージと表示コマンド](#)
- [T1/PRI インターフェイスを使用する Cisco IOS Gateway](#)
- [T1/CAS インターフェイスを使用する Cisco IOS Gateway](#)

## コールフローのトレース

この項では、Cisco Communications Manager トレース ファイル CCM000000000 の例を使用して、コールフローについて説明します。付録 B「ケーススタディ : Cisco Unified IP Phone コールのトラブルシューティング」で詳細なトレース情報（初期化、登録、キープアライブメカニズムなど）についてはすでに説明したので、このケーススタディのトレースでは、コールフロー自体に焦点を絞っています。

このコールフローでは、Cluster 2 に配置された Cisco Unified IP Phone（電話番号 1001）が、PSTN に配置された電話機（電話番号 3333）にコールを発信します。TCP ハンドル値、タイムスタンプ、またはデバイスの名前を調べることで、デバイスをトレース上で追跡できます。デバイスをリポートするかオフラインにするまで、デバイスの TCP ハンドル値は変わりません。

次のトレースでは、Cisco Unified IP Phone（1001）がオフフックになりました。このトレースは、一意のメッセージ、TCP ハンドル、および発信側の番号を示しています。これらは Cisco Unified IP Phone に表示されます。この時点では、まだユーザが番号をダイヤルしていないので、着信側の番号は表示されていません。

```
16:05:46.37515:20:18.390 CCM|StationInit - InboundStim - OffHookMessageID
tcpHandle=0x5138d98
```

```
15:20:18.390 CCM|StationD - stationOutputDisplayText tcpHandle=0x5138d98, Display=1001
```

次のトレースでは、ユーザが DN 3333 をダイヤルします（数字を 1 つずつダイヤルします）。3333 という番号は電話機の宛先番号であり、この電話機は PSTN ネットワークに配置されています。Cisco Unified Communications Manager の番号分析プロセスは現在アクティブになっていて、コールのルーティング先を検出するために番号を分析します。番号分析については、付録 B「ケーススタディ : Cisco Unified IP Phone コールのトラブルシューティング」で詳細に説明しています。

```
15:20:18.390 CCM|Digit analysis: match(fqcn="", cn="1001", pss="", dd="")
15:20:19.703 CCM|Digit analysis: match(fqcn="", cn="1001", pss="", dd="3")
15:20:20.078 CCM|Digit analysis: match(fqcn="", cn="1001", pss="", dd="33")
15:20:20.718 CCM|Digit analysis: match(fqcn="", cn="1001", pss="", dd="333")
15:20:21.421 CCM|Digit analysis: match(fqcn="", cn="1001", pss="", dd="3333")
15:20:21.421 CCM|Digit analysis: analysis results
```

次のトレースでは、番号分析が完了して発信側と着信側が一致し、情報の解析が完了しました。

```
|CallingPartyNumber=1001
|DialingPattern=3333
|DialingRoutePatternRegularExpression=(3333)
|PretransformDigitString=3333
|PretransformPositionalMatchList=3333
|CollectedDigits=3333
|PositionalMatchList=3333
```

次のトレースでは、番号 0 は発信元のロケーションを示し、番号 1 は宛先のロケーションを示しています。BW = -1 によって発信元のロケーションの帯域幅が決定されています。値 -1 は、帯域幅が無限であることを意味します。LAN 環境に配置されている Cisco Unified IP Phone からコールが発信されたため、帯域幅は無限であると見なされます。BW = 64 によって宛先のロケーションの帯域幅が決定されています。コールの宛先には PSTN に配置されている電話機が指定されていて、使用されるコーデックタイプは G.711（64 Kbps）です。

```
15:20:21.421 CCM|Locations:Orig=0 BW=-1 Dest=1 BW=64 (-1 implies infinite bw
available)
```

次のトレースは、発信側と着信側の情報を示しています。この例では、管理者が John Smith などの表示名を設定しなかったため、発信側の名前と番号は同じままです。

```
15:20:21.421 CCM|StationD - stationOutputCallInfo CallingPartyName=1001,
CallingParty=1001, CalledPartyName=, CalledParty=3333, tcpHandle=0x5138d98
```

次のトレースは、H.323 コードが初期化されて H.225 セットアップ メッセージを送信していることを示しています。従来の HDLC SAPI メッセージ、着信側の 16 進表記の IP アドレス、およびポート番号も確認できます。

```
15:20:21.421 CCM|Out Message -- H225SetupMsg -- Protocol= H225Protocol
15:20:21.421 CCM|MMan_Id= 1. (iep= 0 dsl= 0 sapi= 0 ces= 0 IpAddr=e24610ac
IpPort=47110)
```

次のトレースは、発信側と着信側の情報および H.225 アラート メッセージを示しています。また、Cisco Unified IP Phone の 16 進数値と IP アドレスのマッピングも示しています。Cisco Unified IP Phone (1001) の IP アドレスには 172.16.70.231 が指定されています。

```
15:20:21.437 CCM|StationD - stationOutputCallInfo CallingPartyName=1001,
CallingParty=1001, CalledPartyName=, CalledParty=3333, tcpHandle=0x5138d98
15:20:21.453 CCM|In Message -- H225AlertMsg -- Protocol= H225Protocol
15:20:21.953 CCM|StationD - stationOutputOpenReceiveChannel tcpHandle=0x5138d98 myIP:
e74610ac (172.16.70.231)
```

次のトレースは、このコールに使用される圧縮タイプ (G.711 mu-law) を示しています。

```
15:20:21.953 CCM|StationD - ConferenceID: 0 msecPacketSize: 20
compressionType: (4)Media_Payload_G711Ulaw64k
```

H.225 アラート メッセージが送信された後、H.323 は H.245 を初期化します。次のトレースは、発信側と着信側の情報および H.245 メッセージを示しています。TCP ハンドル値はこれまでと変わらず、同一コールが継続していることを示しています。

```
ONE FOR EACH Channel- 16:53:36.855 CCM|H245Interface(3) paths established ip =
e98e6b80, port = 1304|<CT::1,100,105,1.1682><IP::128.107.142.233>
ONE FOR EACH Channel- 16:53:37.199 CCM|H245Interface(3) OLC outgoing confirm ip =
b870701, port = 49252|<CT::1,100,128,3.9><IP::1.7.135.11>
```

```
H323 EP has answered the call and H245 channel setup in progress:
16:53:13.479 CCM|In Message -- H225ConnectMsg -- Protocol= H225Protocol|
```

```
16:03:25.359 CCM|StationD(1): TCPPid = [1.100.117.1] CallInfo callingPartyName='
callingParty=13001 cgpnVoiceMailbox= calledPartyName=' calledParty=11002
cdpnVoiceMailbox= originalCalledPartyName=' originalCalledParty=11002
originalCdpnVoiceMailbox= originalCdpnRedirectReason=0 lastRedirectingPartyName='
lastRedirectingParty=11002 lastRedirectingVoiceMailbox= lastRedirectingReason=0
callType=2(OutBound) lineInstance=1 callReference=16777217. version:
0|<CT::1,100,11,2.1><IP::><DEV::>
```

```
16:03:25.328 CCM|StationD(1): TCPPid = [1.100.117.1] OpenReceiveChannel
conferenceID=16777217 passThruPartyID=16777233 millisecondPacketSize=20
compressionType=4(Media_Payload_G711Ulaw64k) qualifierIn=?. myIP: e98e6b80
(128.107.142.233)|<CT::1,100,11,1.1><IP::><DEV::>
16:03:25.359 CCM|StationD(2): TCPPid = [1.100.117.2] StartMediaTransmission
conferenceID=16777218 passThruPartyID=16777249 remoteIpAddress=e98e6b80(64.255.0.0)
remotePortNumber=65344 milliSecondPacketSize=20
compressType=4(Media_Payload_G711Ulaw64k) qualifierOut=?. myIP: e98e6b80
(128.107.142.233)|<CT::1,100,105,1.213><IP::128.107.142.233>
16:03:25.375 CCM|StationD(2): TCPPid = [1.100.117.2]
star_StationOutputStartMultiMediaTransmission conferenceID=16777218
passThruPartyID=16777250 remoteIpAddress=e98e6b80(66.255.0.0)
remotePortNumber=65346 compressType=101(Media_Payload_H263) qualifierOut=?. myIP:
e98e6b80 (128.107.142.233)|<CT::1,100,105,1.215><IP::128.107.142.233>
```

## ■ コールフローのトレース

```
16:03:25.328 CCM|StationD(1): TCPPid=[1.100.117.1] OpenMultiReceiveChannel
conferenceID=16777217 passThruPartyID=1000011 compressionType=101(Media_Payload_H263)
qualifierIn=?. myIP: e98e6b80 (128.107.142.233) |<CT::1,100,11,1.1><IP::><DEV::>
```

次のトレースは、H.225 接続メッセージおよびその他の情報を示しています。H.225 接続メッセージが受信されると、コールが接続されます。

```
15:20:22.968 CCM|In Message -- H225ConnectMsg -- Protocol= H225Protocol
15:20:22.968 CCM|StationD - stationOutputCallInfo CallingPartyName=1001,
CallingParty=1001, CalledPartyName=, CalledParty=3333, tcpHandle=0x5138d98
15:20:22.062 CCM|MediaCoordinator - wait_AuConnectInfoInd
15:20:22.062 CCM|StationD - stationOutputStartMediaTransmission tcpHandle=0x5138d98
myIP: e74610ac (172.16.70.231)
15:20:22.062 CCM|StationD - RemoteIpAddr: e24610ac (172.16.70.226)
RemoteRtpPortNumber: 16758 msecPacketSize: 20
compressionType: (4)Media_Payload_G711Ulaw64k
15:20:22.062 CCM|Locations:Orig=0 BW=-1Dest=1 BW=6(-1 implies infinite bw available)
16:03:25.359 CCM|MediaManager(1) - wait_AuConnectInfo - recieved response, fowarding,
CI(16777217,16777218) |<CT::1,100,105,1.213><IP::128.107.142.233>
16:03:25.359 CCM|MediaCoordinator -
wait_AuConnectInfoInd |<CT::1,100,105,1.213><IP::128.107.142.233>
16:03:25.359 CCM|ConnectionManager - wait_AuConnectInfoInd,
CI(16777217,16777218) |<CT::1,100,105,1.213><IP::128.107.142.233>
```

次のメッセージは、Cisco Unified IP Phone (1001) からのオンフックメッセージが受信されていることを示しています。オンフックメッセージが受信されるとすぐに、H.225 メッセージと Skinny Station デバイス接続解除メッセージが送信され、H.225 メッセージ全体が表示されます。最後のメッセージは、コールが終了したことを示しています。

```
15:20:27.296 CCM|StationInit - InboundStim - OnHookMessageID tcpHandle=0x5138d98
15:20:27.296 CCM|ConnectionManager -wait_AuDisconnectRequest (16777247,16777248): STOP
SESSION
15:20:27.296 CCM|MediaManager - wait_AuDisconnectRequest - StopSession sending
disconnect to (64,5) and remove connection from list
15:20:27.296 CCM| Device SEP003094C26105 , UnRegisters with SDL Link to monitor
NodeID= 1
15:20:27.296 CCM|StationD - stationOutputCloseReceiveChannel tcpHandle=0x5138d98 myIP:
e74610ac (172.16.70.231)
15:20:27.296 CCM|StationD - stationOutputStopMediaTransmission tcpHandle=0x5138d98
myIP: e74610ac (172.16.70.231)
15:20:28.328 CCM|In Message -- H225ReleaseCompleteMsg -- Protocol= H225Protocol
16:03:33.344 CCM|StationInit - InboundStim - StationOnHookMessageID: Msg
Size(received, defined) = 4, 12 |<CT::1,100,105,1.219><IP::128.107.142.233>
16:03:33.359 CCM|ConnectionManager - wait_AuDisconnectRequest(16777217,16777218): STOP
SESSION |<CT::1,100,105,1.219><IP::128.107.142.233>
16:03:33.359 CCM|StationD(2): TCPPid = [1.100.117.2] CloseReceiveChannel
conferenceID=16777218 passThruPartyID=16777249. myIP: e98e6b80
(128.107.142.233) |<CT::1,100,105,1.219><IP::128.107.142.233>
16:03:33.359 CCM|StationD(2): TCPPid = [1.100.117.2] StopMediaTransmission
conferenceID=16777218 passThruPartyID=16777249. myIP: e98e6b80
(128.107.142.233) |<CT::1,100,105,1.219><IP::128.107.142.233>
16:03:33.359 CCM|StationD(2): TCPPid = [1.100.117.2]
star_StationOutputCloseMultiMediaReceiveChannel conferenceID=16777218
passThruPartyID=16777249. myIP: e98e6b80
(128.107.142.233) |<CT::1,100,105,1.219><IP::128.107.142.233>
16:03:33.359 CCM|StationD(2): TCPPid = [1.100.117.2]
star_StationOutputStopMultiMediaTransmission conferenceID=16777218
passThruPartyID=16777250. myIP: e98e6b80
(128.107.142.233) |<CT::1,100,105,1.219><IP::128.107.142.233>
```

## Cisco IOS Gatekeeper のデバッグメッセージと表示コマンド

P.C-2の「コールフローのトレース」では、Cisco Unified Communications Manager SDI トレースについて詳細に説明しました。このケーススタディのトポロジでは、debug ras コマンドが Cisco IOS Gatekeeper でオンになりました。

次のデバッグメッセージは、Cisco IOS Gatekeeper が Cisco Unified Communications Manager (172.16.70.228) に対する admission request (ARQ; アドミッション要求) を受信し、その他の正常な Remote Access Server (RAS) メッセージがその後に続いていることを示しています。最後に、Cisco IOS Gatekeeper が admission confirmed (ACF; アドミッション確認) メッセージを Cisco Unified Communications Manager に送信します。

```
*Mar 12 04:03:57.181: RASLibRASRecvData ARQ (seq# 3365) rcvd from [172.16.70.228883]
on sock [0x60AF038C]
*Mar 12 04:03:57.181: RASLibRAS_WK_TInit ipsock [0x60A7A68C] setup successful
*Mar 12 04:03:57.181: RASLibras_sendto msg length 16 from 172.16.70.2251719 to
172.16.70.228883
*Mar 12 04:03:57.181: RASLibRASSendACF ACF (seq# 3365) sent to 172.16.70.228
```

次のデバッグメッセージは、コールが進行中であることを示しています。

```
*Mar 12 04:03:57.181: RASLibRASRecvData successfully rcvd message of length 55 from
172.16.70.228883
```

次のデバッグメッセージは、Cisco IOS Gatekeeper が Cisco Unified Communications Manager (172.16.70.228) から disengage request (DRQ; 解除要求) を受信し、Cisco IOS Gatekeeper が disengage confirmed (DCF; 解除確認) を Cisco Unified Communications Manager に送信したことを示しています。

```
*Mar 12 04:03:57.181: RASLibRASRecvData DRQ (seq# 3366) rcvd from [172.16.70.228883]
on sock [0x60AF038C]
*Mar 12 04:03:57.181: RASLibras_sendto msg length 3 from 172.16.70.2251719 to
172.16.70.228883
*Mar 12 04:03:57.181: RASLibRASSendDCF DCF (seq# 3366) sent to 172.16.70.228
*Mar 12 04:03:57.181: RASLibRASRecvData successfully rcvd message of length 124 from
172.16.70.228883
```

Cisco IOS Gatekeeper に対するコマンド show gatekeeper endpoints は、4 つの Cisco Unified Communications Manager がすべて Cisco IOS Gatekeeper に登録されていることを示します。このケーススタディのトポロジでは、各クラスタに 2 つずつ、計 4 つの Cisco Unified Communications Manager が存在します。この Cisco IOS Gatekeeper には 2 つのゾーンがあり、各ゾーンに 2 つの Cisco Unified Communications Manager があります。

R2514-1#show gatekeeper endpoints

```

                                GATEKEEPER ENDPOINT REGISTRATION
                                =====
CallSignalAddr  Port  RASSignalAddr  Port  Zone Name          Type
-----
172.16.70.228   2    172.16.70.228   1493  gka.cisco.com      VOIP-GW
H323-ID: ac1046e4->ac1046f5
172.16.70.229   2    172.16.70.229   3923  gka.cisco.com      VOIP-GW
H323-ID: ac1046e5->ac1046f5
172.16.70.245   1    172.16.70.245   1041  gkb.cisco.com      VOIP-GW
H323-ID: ac1046f5->ac1046e4
172.16.70.243   1    172.16.70.243   2043  gkb.cisco.com      VOIP-GW
H323-ID: ac1046f5->ac1046e4
Total number of active registrations = 4
```

## Cisco IOS Gateway のデバッグメッセージと表示コマンド

P.C-5 の「Cisco IOS Gatekeeper のデバッグメッセージと表示コマンド」では、Cisco IOS Gatekeeper の表示コマンドとデバッグ出力について詳細に説明しました。この項では、Cisco IOS Gateway のデバッグ出力と表示コマンドについて取り上げます。このケーススタディのトポロジでは、コールは Cisco IOS Gateway を経由します。Cisco IOS Gateway は、T1/CAS または T1/PRI のいずれかのインターフェイスで PSTN または PBX に接続しています。次の例は、debug voip ccapi inout、debug H225 events、debug H225 asn1 などのコマンドのデバッグ出力を示しています。

次のデバッグ出力では、Cisco IOS Gateway が Cisco Unified Communications Manager ( 172.16.70.228 ) からの TCP 接続要求を H.225 用のポート 2328 で受け入れます。

```
*Mar 12 04:03:57.169: H225Lib::h225TAccept: TCP connection accepted from
172.16.70.228:2328 on socket [1]
*Mar 12 04:03:57.169: H225Lib::h225TAccept: Q.931 Call State is initialized to be
[Null].
*Mar 12 04:03:57.177: Hex representation of the received TPKT03000065080000100
```

次のデバッグ出力は、この TCP セッションで Cisco Unified Communications Manager から H.225 データが到達していることを示しています。このデバッグ出力には、使用されている H.323 バージョンを指定する protocolIdentifier が表示されます。次のデバッグは、H.323 バージョン 2 が使用されていることを示しています。この例は、着信側と発信側の番号も示しています。

```
- Source Address H323-ID
- Destination Address e164
*Mar 12 04:03:57.177: H225Lib::h225RecvData: Q.931 SETUP received from socket
[1]value H323-UserInformation ::=
*Mar 12 04:03:57.181: {
*Mar 12 04:03:57.181: h323-uu-pdu
*Mar 12 04:03:57.181: {
*Mar 12 04:03:57.181: h323-message-body setup :
*Mar 12 04:03:57.181: {
*Mar 12 04:03:57.181: protocolIdentifier { 0 0 8 2250 0 2 },
*Mar 12 04:03:57.181: sourceAddress
*Mar 12 04:03:57.181: {
*Mar 12 04:03:57.181: h323-ID : "1001"
*Mar 12 04:03:57.181: },
*Mar 12 04:03:57.185: destinationAddress
*Mar 12 04:03:57.185: {
*Mar 12 04:03:57.185: e164 : "3333"
*Mar 12 04:03:57.185: },
*Mar 12 04:03:57.189: H225Lib::h225RecvData: State changed to [Call Present].
```

次のデバッグ出力は、Call Control Application Programming Interface (CCAPi) を示しています。Call Control API は着信コールを指定します。次の出力では、着信側と発信側の情報も確認できます。CCAPi はダイヤルピア 0 と一致します。0 はデフォルトのダイヤルピアです。CCAPi がダイヤルピア 0 と一致するのは、発信側の番号について他のダイヤルピアが見つからなかったため、デフォルトのダイヤルピアを使用しているためです。

```
*Mar 12 04:03:57.189: cc_api_call_setup_ind (vdbPtr=0x616C9F54, callInfo={called=3333,
calling=1001, fdest=1 peer_tag=0}, callID=0x616C4838)
*Mar 12 04:03:57.193: cc_process_call_setup_ind (event=0x617A2B18) handed call to app
"SESSION"
*Mar 12 04:03:57.193: sess_appl: ev(19=CC_EV_CALL_SETUP_IND), cid(17), disp(0)
*Mar 12 04:03:57.193: ccCallSetContext (callID=0x11, context=0x61782BBC)
Mar 12 04:03:57.193: ssaCallSetupInd finalDest cllng(1001), cllid(3333)
*Mar 12 04:03:57.193: ssaSetupPeer cid(17) peer list: tag(1)
*Mar 12 04:03:57.193: ssaSetupPeer cid(17), destPat(3333), matched(4), prefix(),
peer(6179E63C)
*Mar 12 04:03:57.193: ccCallSetupRequest (peer=0x6179E63C, dest=, params=0x61782BD0
mode=0, *callID=0x617A87C0)
*Mar 12 04:03:57.193: callingNumber=1001, calledNumber=3333, redirectNumber=
*Mar 12 04:03:57.193: accountNumber=, finalDestFlag=1,
guid=0098.89c8.9233.511d.0300.cddd.ac10.46e6
```

CCAPi は、ダイヤルピア 1 と宛先パターン (着信側の番号 3333) を一致させます。peer\_tag はダイヤルピアを意味します。要求パケット内の発信側と着信側の番号が表示されます。

```
*Mar 12 04:03:57.193: peer_tag=1
*Mar 12 04:03:57.197: ccIFCallSetupRequest: (vdbPtr=0x617BE064, dest=,
callParams={called=3333, calling=1001, fdest=1, voice_peer_tag=1}, mode=0x0)
```

次のデバッグ出力は、H.225 アラートメッセージが Cisco Unified Communications Manager に返されていることを示しています。

```
*Mar 12 04:03:57.197: ccCallSetContext (callID=0x12, context=0x61466B30)
*Mar 12 04:03:57.197: ccCallProceeding (callID=0x11, prog_ind=0x0)
*Mar 12 04:03:57.197: cc_api_call_proceeding(vdbPtr=0x617BE064, callID=0x12,
prog_ind=0x0)
*Mar 12 04:03:57.197: cc_api_call_alert(vdbPtr=0x617BE064, callID=0x12, prog_ind=0x8,
sig_ind=0x1)
*Mar 12 04:03:57.201: sess_appl: ev(17=CC_EV_CALL_PROCEEDING), cid(18), disp(0)
*Mar 12 04:03:57.201: ssa:
cid(18)st(1)oldst(0)cfid(-1)csize(0)in(0)fDest(0)-cid2(17)st2(1)oldst2(0)
*Mar 12 04:03:57.201: ssaIgnore cid(18), st(1),oldst(1), ev(17)
*Mar 12 04:03:57.201: sess_appl: ev(7=CC_EV_CALL_ALERT), cid(18), disp(0)
*Mar 12 04:03:57.201: ssa:
cid(18)st(1)oldst(1)cfid(-1)csize(0)in(0)fDest(0)-cid2(17)st2(1)oldst2(0)
*Mar 12 04:03:57.201: ssaFlushPeerTagQueue cid(17) peer list: (empty)
*Mar 12 04:03:57.201: ccCallAlert (callID=0x11, prog_ind=0x8, sig_ind=0x1)
*Mar 12 04:03:57.201: ccConferenceCreate (confID=0x617A8808, callID1=0x11,
callID2=0x12, tag=0x0)
*Mar 12 04:03:57.201: cc_api_bridge_done (confID=0x7, srcIF=0x616C9F54,
srcCallID=0x11, dstCallID=0x12, disposition=0, tag=0x0)value H323-UserInformation
*Mar 12 04:03:57.201: {
*Mar 12 04:03:57.201:   h323-uu-pdu
*Mar 12 04:03:57.201:   {
*Mar 12 04:03:57.201:     h323-message-body alerting :
*Mar 12 04:03:57.201:     {
*Mar 12 04:03:57.201:       protocolIdentifier { 0 0 8 2250 0 2 },
*Mar 12 04:03:57.205:       destinationInfo
*Mar 12 04:03:57.205:       {
*Mar 12 04:03:57.205:         mc FALSE,
*Mar 12 04:03:57.205:         undefinedNode FALSE
*Mar 12 04:03:57.205:       },
```

このパケットでは、Cisco IOS が H.245 アドレスとポート番号も Cisco Unified Communications Manager に送信します。Cisco IOS Gateway は到達不能なアドレスを送信する必要があるため、無音声または単方向音声になることがあります。

```
*Mar 12 04:03:57.205:          h245Address ipAddress :
*Mar 12 04:03:57.205:          {
*Mar 12 04:03:57.205:          ip 'AC1046E2'H,
*Mar 12 04:03:57.205:          port 011008
*Mar 12 04:03:57.205:          },
*Mar 12 04:03:57.213: Hex representation of the ALERTING TPKT to send.0300003D0100
*Mar 12 04:03:57.213:
*Mar 12 04:03:57.213:          H225Lib::h225AlertRequest: Q.931 ALERTING sent from socket
[1]. Call state changed to [Call Received].
*Mar 12 04:03:57.213: cc_api_bridge_done (confID=0x7, srcIF=0x617BE064,
srcCallID=0x12, dstCallID=0x11, disposition=0, tag=0x0)
```

次のデバッグ出力は、H.245 セッションが開始していることを示しています。コーデック ネゴシエーションの機能表示および各音声パケットに含まれるバイト数を確認できます。

```
*Mar 12 04:03:57.217: cc_api_caps_ind (dstVdbPtr=0x616C9F54, dstCallId=0x11,
srcCallId=0x12, caps={codec=0xEBFB, fax_rate=0x7F, vad=0x3, modem=0x617C5720
codec_bytes=0, signal_type=3})
*Mar 12 04:03:57.217: sess_appl: ev(23=CC_EV_CONF_CREATE_DONE), cid(17), disp(0)
*Mar 12 04:03:57.217: ssa:
cid(17)st(3)oldst(0)cfid(7)csz(0)in(1)fDest(1)-cid2(18)st2(3)oldst(1)
*Mar 12 04:03:57.653: cc_api_caps_ind (dstVdbPtr=0x617BE064, dstCallId=0x12,
srcCallId=0x11, caps={codec=0x1, fax_rate=0x2, vad=0x2, modem=0x1, codec_bytes=160,
signal_type=0})
```

次のデバッグ出力は、両方の側が正常にネゴシエートし、160 バイトのデータを持つ G.711 コーデックで合意したことを示しています。

```
*Mar 12 04:03:57.653: cc_api_caps_ack (dstVdbPtr=0x617BE064, dstCallId=0x12,
srcCallId=0x11, caps={codec=0x1, fax_rate=0x2, vad=0x2, modem=0x1, codec_bytes=160,
signal_type=0})
*Mar 12 04:03:57.653: cc_api_caps_ind (dstVdbPtr=0x617BE064, dstCallId=0x12,
srcCallId=0x11, caps={codec=0x1, fax_rate=0x2, vad=0x2, modem=0x1, codec_bytes=160,
signal_type=0})
*Mar 12 04:03:57.653: cc_api_caps_ack (dstVdbPtr=0x617BE064, dstCallId=0x12,
srcCallId=0x11, caps={codec=0x1, fax_rate=0x2, vad=0x2, modem=0x1, codec_bytes=160,
signal_type=0})
*Mar 12 04:03:57.657: cc_api_caps_ack (dstVdbPtr=0x616C9F54, dstCallId=0x11,
srcCallId=0x12, caps={codec=0x1, fax_rate=0x2, vad=0x2, modem=0x1, codec_bytes=160,
signal_type=0})
*Mar 12 04:03:57.657: cc_api_caps_ack (dstVdbPtr=0x616C9F54, dstCallId=0x11,
srcCallId=0x12, caps={codec=0x1, fax_rate=0x2, vad=0x2, modem=0x1, codec_bytes=160,
signal_type=0})
```

H.323 接続および接続解除のメッセージがこの後に続きます。

```
*Mar 12 04:03:59.373: cc_api_call_connected(vdbPtr=0x617BE064, callID=0x12)
*Mar 12 04:03:59.373: sess_appl: ev(8=CC_EV_CALL_CONNECTED), cid(18), disp(0)
*Mar 12 04:03:59.373: ssa:
cid(18)st(4)oldst(1)cfid(7)csize(0)in(0)fDest(0)-cid2(17)st2(4)oldst2(3)
*Mar 12 04:03:59.373: ccCallConnect (callID=0x11)
*Mar 12 04:03:59.373: {
*Mar 12 04:03:59.373:   h323-uu-pdu
*Mar 12 04:03:59.373:   {
*Mar 12 04:03:59.373:     h323-message-body connect :
*Mar 12 04:03:59.373:     {
*Mar 12 04:03:59.373:       protocolIdentifier { 0 0 8 2250 0 2 },
*Mar 12 04:03:59.373:       h245Address ipAddress :
*Mar 12 04:03:59.373:       {
*Mar 12 04:03:59.377:         ip 'AC1046E2'H,
*Mar 12 04:03:59.377:         port 011008
*Mar 12 04:03:59.377:       },
*Mar 12 04:03:59.389: Hex representation of the CONNECT TPKT to send.03000052080
*Mar 12 04:03:59.393: H225Lib::h225SetupResponse: Q.931 CONNECT sent from socket [1]
*Mar 12 04:03:59.393: H225Lib::h225SetupResponse: Q.931 Call State changed to
[Active].
*Mar 12 04:04:08.769: cc_api_call_disconnected(vdbPtr=0x617BE064, callID=0x12,
cause=0x10)
*Mar 12 04:04:08.769: sess_appl: ev(12=CC_EV_CALL_DISCONNECTED), cid(18), disp(0)
```

## T1/PRI インターフェイスを使用する Cisco IOS Gateway

前述したように、2つのタイプのコールが Cisco IOS Gateway を経由し、Cisco IOS Gateway は、T1/CAS または T1/PRI のいずれかのインターフェイスで PSTN または PBX に接続しています。次の例は、Cisco IOS Gateway が T1/PRI インターフェイスを使用する場合のデバッグ出力を示しています。

Cisco IOS Gateway で `debug isdn q931` コマンドがオンになり、ISDN 環境にある D チャネル用のレイヤ 3 シグナリング プロトコルである Q.931 が有効になります。T1/PRI インターフェイスからコールが発信されるたびに、セットアップ パケットが送信される必要があります。セットアップ パケットには必ずプロトコル記述子 `pd = 8` が含まれており、`callref` 用にランダムな 16 進数値が生成されます。`callref` はコールを追跡します。たとえば、2つのコールが発信された場合、`callref` の値によって、RX (受信済み) メッセージの対象になっているコールを判別できます。ベアラ機能 `0x8890` は 64 Kbps データ コールを意味します。これが `0x8890218F` だった場合は、56 Kbps データ コールになり、音声コールでは `0x8090A3` になります。次のデバッグ出力では、ベアラ機能は `0x8090A3` (音声用) です。この例は、着信側と発信側の番号を示しています。

`callref` では、最初の数字に異なる値が使用され (TX と RX を区別するため) 2 番目の値は同じです (SETUP には最後の数字に 0 が設定され、CONNECT\_ACK にも 0 が設定されています)。ルータは PSTN または PBX に完全に依存して Bearer チャネル (B チャネル) を割り当てます。PSTN または PBX がルータにチャネルを割り当てない場合、コールはルーティングされません。このケーススタディでは、交換機から受信される CONNECT メッセージに、ALERTING 用に受信されたものと同じ参照番号 (`0x800B`) が含まれます。最後に、コールが接続解除される時、DISCONNECT メッセージの交換の後に、RELEASE メッセージおよび RELEASE\_COMP メッセージが続きます。RELEASE\_COMP メッセージの後には、コール拒否の理由 ID が続きます。理由 ID は 16 進数値です。理由の内容は、16 進数値のデコードとプロバイダーのフォローアップによって確認します。

```
*Mar 1 225209.694 ISDN Se115 TX -> SETUP pd = 8 callref = 0x000B
*Mar 1 225209.694 Bearer Capability i = 0x8090A3
*Mar 1 225209.694 Channel ID i = 0xA98381
*Mar 1 225209.694 Calling Party Number i = 0x2183, '1001'
*Mar 1 225209.694 Called Party Number i = 0x80, '3333'
*Mar 1 225209.982 ISDN Se115 RX <- ALERTING pd = 8 callref = 0x800B
*Mar 1 225209.982 Channel ID i = 0xA98381
*Mar 1 225210.674 ISDN Se115 RX <- CONNECT pd = 8 callref = 0x800B
*Mar 1 225210.678 ISDN Se115 TX -> CONNECT_ACK pd = 8 callref = 0x000B
*Mar 1 225215.058 ISDN Se115 RX <- DISCONNECT pd = 8 callref = 0x800B
*Mar 1 225215.058 Cause i = 0x8090 - Normal call clearing 225217 %ISDN-6
DISCONNECT Int S10 disconnected from unknown , call lasted 4 sec
*Mar 1 225215.058 ISDN Se115 TX -> RELEASE pd = 8 callref = 0x000B
*Mar 1 225215.082 ISDN Se115 RX <- RELEASE_COMP pd = 8 callref = 0x800B
*Mar 1 225215.082 Cause i = 0x829F - Normal, unspecified or Special intercept, call
blocked group restriction
```

## T1/CAS インターフェイスを使用する Cisco IOS Gateway

2つのタイプのコールが Cisco IOS Gateway を経由し、Cisco IOS Gateway は、T1/CAS または T1/PRI のいずれかのインターフェイスで PSTN または PBX に接続しています。次の例は、Cisco IOS Gateway が T1/CAS インターフェイスを使用する場合のデバッグ出力を示しています。Cisco IOS Gateway で debug cas はオンになりました。

次のデバッグメッセージは、Cisco IOS Gateway がオフフック信号を交換機に送信していることを示しています。

```
Apr  5 17:58:21.727: from NEAT(0): (0/15): Tx LOOP_CLOSURE (ABCD=1111)
```

次のデバッグメッセージは、交換機が Cisco IOS Gateway から閉ループ信号を受信した後にウィンクを送信していることを示しています。

```
Apr  5 17:58:21.859: from NEAT(0): (0/15): Rx LOOP_CLOSURE (ABCD=1111)
Apr  5 17:58:22.083: from NEAT(0): (0/15): Rx LOOP_OPEN (ABCD=0000)
```

次のデバッグメッセージは、Cisco IOS Gateway がオフフックしようとしていることを示しています。

```
Apr  5 17:58:23.499: from NEAT(0): (0/15): Rx LOOP_CLOSURE (ABCD=1111)
```

次の出力は、コール進行中の Cisco IOS Gateway での show call active voice brief を示しています。この出力は、着信側と発信側の番号およびその他の有用な情報も示しています。

```
R5300-5#show call active voice brief
<ID>: <start>hs.<index> +<connect> pid:<peer_id> <dir> <addr> <state>
tx:<packets>/<bytes> rx:<packets>/<bytes> <state>
  IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
delay:<last>/<min>/<max>ms <codec>
  FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n> sig:<on/off> <codec>
(payload size)
  Tele <int>: tx:<tot>/<v>/<fax>ms <codec> noise:<l> acom:<l> i/o:<l>/<l> dBm
511D : 156043737hs.1 +645 pid:0 Answer 1001 active
tx:1752/280320 rx:988/158080
  IP172.16.70.228:18888 rtt:0ms pl:15750/80ms lost:0/0/0 delay:25/25/65ms g711ulaw
511D : 156043738hs.1 +644 pid:1 Originate 3333 active
tx:988/136972 rx:1759/302548
  Tele 1/0/0 (30): tx:39090/35195/0ms g711ulaw noise:-43 acom:0 i/o:-36/-42 dBm
```

■ T1/CAS インターフェイスを使用する Cisco IOS Gateway



## INDEX

### Numerics

- 30 秒経過するとボイス メッセージが停止する 7-2
- 30 秒経過するとボイス メールが停止する、トラブルシューティング 7-2

### A

- Attendant Console サーバと通信できない 8-26

### C

- CCO の利用、問い合わせ A-4
- CCO を利用した問い合わせ、URL ロケーション A-4
- Certificate Authority Proxy Function ( CAPF )
  - CAPF 証明書のインストールの確認 3-18
  - LSC 検証の失敗 3-18
  - MIC の存在の確認 3-18
  - トラブルシューティング 3-17
- Cisco Call Back のエラー メッセージ 8-5
- Cisco Call Back のログ ファイルの場所 8-5
- Cisco CTIManager がダウンしている 8-31
- Cisco CTL クライアント、トラブルシューティング 3-16
- Cisco IOS Gateway
  - T1/CAS インターフェイス C-11
  - T1/PRI インターフェイス C-10
- Cisco IP Phone と Cisco IP Phone 間のクラスタ内コールのトポロジの例 B-2
- Cisco IP Phone による音声問題の解決 4-4
- Cisco Live!、問い合わせ内容の報告 A-4
- Cisco Secure Telnet
  - 概要 2-6
  - 構造 A-6
  - サーバ アクセス A-5
  - システム A-5
  - 設計 A-5
- Cisco Syslog Analysis
  - Cisco Syslog Analyzer 2-3
  - Cisco Syslog Analyzer Collector 2-3

### Cisco Unified Communications Manager

- Assistant、トラブルシューティング 8-9
- Assistant のトラブルシューティング ツールとクライアント デスクトップ 8-9
- Attendant Console の問題
  - インターフェイスの問題 8-26
  - 収集、サーバ ログ 8-29
  - ディレクトリの問題 8-24
  - テレフォニーの初期化のエラー 8-19
  - ボイスメールの問題 8-25
  - 問題、コールの発信と受信に関する 8-22
- Attendant Console の問題、Serviceability が JTAPI ログを生成しない 8-28
- KeepAlive プロセス B-6
- Serviceability が JTAPI ログを生成しない 8-28
- エクステンション モビリティ、一般的な問題の解決 8-6
- 応答しないシステム 3-2
- 管理ページが表示されない 3-3
- クラスタ内コール フローのトレース B-7
- サービスの問題 6-1
- システムが応答を停止する 3-2
- システムの問題 3-1
- 初期化プロセス B-3
- 登録プロセス B-6
- トラブルシューティング ツール 2-6
- Cisco Unified Communications Manager サービスが動作していることの確認 2-18
- Cisco Unified IP Phone
  - 音声問題のトラブルシューティング 4-4
  - 初期化プロセス B-3
  - トラブルシューティング
    - LSC の確認 3-18
    - 認証文字列 3-17
- Cisco Unity がロールオーバーしない、トラブルシューティング 7-2
- Cisco エクステンション モビリティ
  - エラーの解決 8-7
  - トラブルシューティング 8-6
- CiscoWorks2000 2-3

- CLI コマンドおよび GUI 選択オプションの要約  
2-13, 2-14
- CTL クライアント、トラブルシューティング 3-16
- ## E
- etoken、トラブルシューティング 3-16
- Exception、java.lang.ClassNotFoundException 8-11
- ## I
- IP Phone、トラブルシューティング
- LSC の確認 3-18
  - 認証文字列 3-17
- IPMAConsoleInstall.jsp でエラーが表示される、No Page Found 8-10
- ## J
- JTAPI サブシステム
- OUT\_OF\_SERVICE 3-9
  - PARTIAL\_SERVICE の状態 3-13
  - 起動に関する問題 3-9
- ## M
- MIVR-SS\_TEL-1-ModuleRunTimeFailure 3-12
- MIVR-SS\_TEL-4-ModuleRunTimeFailure 3-10
- ## R
- Restart\_Ack に Channel IE が含まれていない場合に B チャンネルがロックされたままになる、トラブルシューティング 4-22
- ## S
- SNMP
- サポート 2-4
  - 定義 2-4
  - ~でのリモート モニタリング 2-4
- syslog 分析、説明 2-3
- ## T
- TAC
- Cisco Live! A-4
  - 必要な情報 A-2
  - リモート アクセスの許可 A-4
- TAC への問い合わせ、必要な情報 A-2
- Telnet、Cisco Secure
- 構造 A-5
  - 設計 A-5
  - 説明 2-6
- ## U
- Unicode 言語で検索できない 8-27
- Unity がロール オーバーせずにビジー音が聞こえる 7-2
- ## W
- Web Dialer、トラブルシューティング 8-30
- ## あ
- アシスタント コンソールでエラーが表示される、Cisco Unified Communications Manager Assistant サービスにアクセスできません。しばらくしてから再試行してください 8-13
- アシスタントのプロキシ回線上で鳴っているコールをマネージャが代行受信できない 8-17
- アテンダントがサーバにアクセスできないというエラー メッセージの表示 8-21
- アドミSSION拒否 4-21
- 暗号化
- トラブルシューティング、SRTP/SCCP 2-6
  - パケット キャプチャによるトラブルシューティング 3-18
- 安全なダイヤル プラン 5-6
- ## い
- 一時エラー発生 8-35
- 一般的な問題解決モデル 1-3

- え
- エコー 4-5
- お
- 応答しないシステム  
     トラブルシューティング 3-2  
     トラブルシューティングの概要 3-2
- 折返しソフトキーを押してから、コールバックが発生する前に、ユーザが電話機のケーブルを抜くか、電話機をリセットした 8-4
- 音声の損失または歪み 4-2
- 音声品質 4-2
- か
- 回線が使用できない 8-23
- 概要 2-3  
     Cisco Secure Telnet 2-6  
     CiscoWorks2000 2-3  
     サービスアビリティ 1-2  
     トラブルシューティング 1-1
- 確立されたコールで補助的なサービスが使用できない 6-5
- 管理者アカウントが Cisco Unity サブスクライバに関連付けられていない 7-4
- 管理ページが表示されない、トラブルシューティング 3-3
- き
- キーがアクティブではありません 8-35
- 機能、トラブルシューティング 7-1
- キャプチャしたパケット、分析 2-12
- く
- クラスタ間 H.323 通信 B-11
- グループ ピックアップ設定 5-4
- け
- ケース スタディ  
     Cisco Unified IP Phone コールのトラブルシューティング B-1
- Cisco Unified IP Phone と Cisco IOS Gateway 間の  
     コールのトラブルシューティング C-1
- ゲートウェイのテスト 4-5
- ゲートウェイの登録障害 4-15
- ゲートウェイの問題 4-15
- ゲートウェイのリオーダー音 4-15
- ゲートキーパーの問題 4-21
- こ
- コーデックとリージョンの不一致 4-11
- コーリング サーチ スペース 5-4
- コールパーク  
     トラブルシューティング 8-3
- コールフローの失敗 B-12
- コールフローのトレース B-11, C-2
- コール制御の初期化の失敗 8-20
- コマンドライン インターフェイス 2-3
- さ
- サーバの応答が遅い 3-9
- サービス、トラブルシューティング 6-1
- サービスアビリティ  
     概要 1-2  
     ツール 2-2
- サービスが一時的に使用できない 8-30
- し
- 自己起動プロセス B-4
- シスコ検出プロトコル (CDP) のサポート 2-4
- システム ロギング、説明 2-3
- システム ログの管理 2-3
- システムの問題、トラブルシューティング 3-1
- 収集  
     スニファトレース 2-5  
     デバッグ 2-5
- 収集、サーバ ログ 8-29
- 使用可能な会議ブリッジがない 6-1
- 証明書、トラブルシューティング 3-16
- 診断、サーバの応答が遅い 3-9

- す
- スニファトレース、収集 2-5
- せ
- 製造元でインストールされる証明書 (MIC) の確認 3-18
- セキュリティ
- トークン 3-16
  - トラブルシューティング、パケットキャプチャ 2-6
- セキュリティ、ファイアウォールの整合性 A-5
- セッションの期限切れ、再ログイン 8-31
- 接続性がない、リモートサーバ 3-6
- そ
- 即時転送、トラブルシューティング 8-35
- た
- ダイヤルプランとルーティングの問題 5-1
- ダイヤルプランの問題 5-5
- ダイレクトコールパーク、トラブルシューティング 8-33
- ダウンロードによる Microsoft 仮想マシンの自動インストールが利用できなくなった 8-11
- 短縮ダイヤルウィンドウとディレクトリウィンドウで回線状態が正しく表示されない 8-28
- 単方向音声または無音声 4-6
- て
- ディレクトリサービスがダウンしている 8-31
- ディレクトリの問題 8-24
- テキストが不適切な言語で表示される 8-27
- デバイス / 回線が開けない 8-32
- デバイスの問題
- 概要 4-1
  - トラブルシューティング 4-1
- デバッグ、収集 2-5
- デバッグメッセージと表示コマンド
- Cisco IOS Gatekeeper C-5
  - Cisco IOS Gateway C-6
- テレフォニーの初期化のエラー 8-19
- テレフォニーの初期化の失敗 8-19
- 転送先に到達できない 8-32
- 電話機の回線が使用不可になる 8-24
- 電話機の問題 4-13
- 電話機のリセット 4-13
- 電話番号の回線状態が不明と表示される 8-28
- と
- 登録拒否 4-21
- ドメイン名 5-4
- トラブルシューティング
- 30 秒経過するとボイスメールが停止する 7-2
  - ARJ 4-21
  - CAPF 3-17
  - CAPF 証明書のインストールの確認 3-18
  - Cisco Call Back 8-3
  - Cisco CTL クライアント 3-16
  - Cisco Live! の使用 A-4
  - Cisco Unified Communications Manager Assistant 8-9
  - Cisco Unified IP Phone コール
    - クラスタ間 B-11
    - クラスタ内 B-2
  - Cisco Unified IP Phone による音声問題 4-4
  - Cisco Web Dialer 8-30
  - Cisco エクステンション モビリティ
    - エラーメッセージ 8-7
    - 概要 8-6
  - CTL セキュリティ トークン 3-16
  - LSC 検証の失敗 3-18
  - LSC のインストールの確認 3-18
  - MIC の存在の確認 3-18
  - Restart\_Ack に Channel IE が含まれていない場合に B チャンネルがロックされたままになる 4-22
  - RRJ 4-21
  - TAC のリモートアクセス A-4
  - TAC への問い合わせ A-1
  - Unity がロールオーバーしない 7-2
  - アドミッション拒否 4-21
  - アラーム 3-14
  - 暗号化を使用するパケットキャプチャ 3-18
  - 安全なダイヤルプラン 5-6
  - エコー 4-5
  - 応答しない Cisco Unified Communications Manager システム 3-2

- 音声の損失または歪みの問題 4-2
  - 音声品質の問題 4-2
  - 概要 1-1
  - 管理者アカウントが CiscoUnity サブスクリバに  
関連付けられていない 7-4
  - 管理ページが表示されない 3-3
  - 機能 7-1
  - 機能およびサービス 8-1
  - ゲートウェイの登録障害 4-15
  - ゲートウェイのリオーダー音の問題 4-15
  - ゲートキーパーの問題 4-21
  - コーデックとリージョンの不一致 4-11
  - コーリング サーチ スペース 5-1
  - サービス 6-1
  - システムが応答を停止する 3-2
  - システムの問題 3-1
  - 証明書 3-16
  - セキュリティ
    - SRTP/SCCP の概要 2-6
    - パケット キャプチャ設定のチェックリスト  
(表) 2-7
    - パケット キャプチャのサービス パラメータ  
2-8
    - パケット キャプチャの設定値 2-11
    - 分析、キャプチャしたパケット 2-12
  - 即時転送 8-35
  - ダイヤル プランの問題 5-5
  - 単方向音声または無音声 4-6
  - ツール 2-1, 2-2
  - デバイスの問題 4-1
  - 電話機で入力された不適切な認証文字列 3-17
  - 電話機のリセット 4-13
  - 問い合わせ A-4
  - 登録拒否 4-21
  - トレース ファイル 3-16
  - ドロップされたコール 4-14
  - 名前からアドレスへの解決の失敗 3-5
  - パケット キャプチャ 3-18
  - パフォーマンス モニタ カウンタ 3-14
  - パフォーマンス モニタ カウンタの説明 (表)  
3-15
  - 必要な予備情報 A-2
  - ヒント 2-16
  - ブロックされたポート 80 3-6
  - ページを表示する権限がない 3-4
  - 他のデバイスへの接続性がない 3-6
  - ルートパーティションの問題 5-1
  - ログ ファイル 3-16
  - ロケーションと帯域幅の問題 4-12
  - 割り込み 8-2
  - トラブルシューティング ツール 2-1
  - ドロップされたコール 4-14
- な
- 名前からアドレスへの解決の失敗、トラブルシュー  
ティング 3-5
- に
- 認証エラー 8-30
- ね
- ネットワーク レイアウト A-2
  - ネットワーク障害への事前準備 1-4
- は
- パーティショニング 5-4
  - ハードウェア トランスコーダが期待どおりに機能し  
ない 6-3
  - パイロット ポイントにコールを発信できない 8-22
  - パケット キャプチャ
    - 概要 2-6
    - サービス パラメータ 2-8
    - 設定値 2-11
    - 設定のチェックリスト (表) 2-7
    - 分析 2-12
  - パケット キャプチャ設定のチェックリスト 2-7
  - パケット キャプチャの設定
    - ゲートウェイとトランクの設定ウィンドウ  
2-10
    - サービス パラメータ 2-8
    - 電話の設定 (Phone Configuration) ウィンドウ  
2-9
  - 発信者が、電話機がリセットされる前の使用可能通知  
を見逃した 8-4
- ふ
- ファイアウォール保護 A-5

フィルタリングをオンまたはオフにするとコールがルーティングされない 8-14

複製、再確立 3-8

ブロックされたポート 80、トラブルシューティング 3-6

分析、キャプチャしたパケット 2-12

## ほ

ボイス メッセージの問題 7-1

ボイスメールに転送されたコールが直接コールとして処理される、トラブルシューティング 7-3

ボイスメールの問題 8-25

## ま

マネージャがログアウトしてもサービスが動作している 8-16

## も

### 問題

Attendant Console インターフェイスの使用 8-26

Cisco Call Back の使用 8-3

コールの発信と受信 8-22

番号をダイヤルするときの 5-5

ユーザの表示または追加 3-4

問題解決のガイドライン 1-3

## ゆ

ユーザがログインしているデバイスがない 8-32

ユーザ認証が失敗する 8-12

## よ

呼び出し音が鳴る前にユーザが折返しソフトキーを押した 8-3

## り

リモート アクセス A-4

リモート アクセスの許可、方法 A-4

リモート サーバ、接続性がない 3-6

## る

ルート アクセスを使用しないサーバのトラブルシューティング 2-13

ルート パーティションとコーリング サーチ スペース 5-1

## ろ

ローカルで有効な証明書 (LSC)、トラブルシューティング

インストールの確認 3-18

検証の失敗 3-18

ログ、エコー ログ 4-5

ログ ファイル、トラブルシューティング 3-16

ロケーションと帯域幅 4-12

## わ

割り込み、トラブルシューティング 8-2