Cisco CallManager
トラブルシューティング ガイド Release 5.0(1)

Text Part Number: OL-8764-01-J

CONTENTS

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、および表記法について説明します。また、関連マニュアルを入手する方法についても説明します。

次のトピックについて取り上げます。

目的

『*Cisco CallManager トラブルシューティング ガイド Release 5.0(1)*』では、Cisco CallManager 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 CallManager トラブルシューティング ガイド*』の情報は、Cisco CallManager 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 CallManager 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せのある質問を重点的に取り上げています。

対象読者

『*Cisco CallManager トラブルシューティング ガイド Release 5.0(1)*』は、企業の管理者および従業員のために Cisco CallManager 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 CallManager 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 CallManager 5.0(1)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 CallManager Attendant Console」	Cisco CallManager Attendant Console が提供する、管理者用のトラブルシューティング ツールについて説明します。これらのツールには、Cisco CallManager 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。
第 4 章「Cisco CallManager システムの問題」	Cisco CallManager 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 5 章「ディレクトリの問題」	ディレクトリのインストールと設定に関する情報を参照する方法について説明します。
第 6 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 7 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 8 章「Cisco CallManager サービスの問題」	会議ブリッジやメディア終端点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 9 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。
付録 A「TAC への問い合せ」	TAC に問い合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 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 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 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 IP Phone について説明します。
付録 D「機能およびサービスのトラブルシューティング」	Cisco CallManager 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。

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は、次の資料を参照してください。

- *Release Notes for Cisco CallManager*
- *Cisco CallManager Documentation Guide*
- *Cisco CallManager アドミニストレーション ガイド*
- *Cisco CallManager システム ガイド*
- *Cisco CallManager Serviceability アドミニストレーション ガイド*
- *Cisco CallManager 機能およびサービス ガイド*
- *Cisco CallManager Attendant Console ユーザ ガイド*
- *Cisco CallManager インストレーション ガイド*
- *Cisco IP Phone アドミニストレーション ガイド for Cisco CallManager*
- *Cisco CallManager Bulk Administration Tool ユーザ ガイド*
- *Cisco Technical Solution Series: IP Telephony Solution Guide*
- *Guide to Cisco Systems VOIP Infrastructure Solution for SIP*

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 アドバイスでは、次の表記法を使用しています。

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。

ヒントでは、次の表記法を使用しています。

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、次の表記法を使用しています。

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

シスコの製品マニュアルやその他の資料は、Cisco.com でご利用いただけます。また、テクニカルサポートおよびその他のリソースを、さまざまな方法で入手することができます。ここでは、シスコ製品に関する技術情報を入手する方法について説明します。

Cisco.com

マニュアルの最新版は、次の URL で参照できます。

http://www.cisco.com/univercd/home/home.htm

シスコの Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com

また、シスコの Web サイトの各国語版へは、次の URL からアクセスできます。

http://www.cisco.com/public/countries_languages.shtml

シスコ製品の最新資料の日本語版は、次の URL からアクセスしてください。

http://www.cisco.com/jp

マニュアルの発注方法（英語版）

英文マニュアルの発注方法については、次の URL にアクセスしてください。

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

シスコ製品の英文マニュアルは、次の方法で発注できます。

- Cisco.com 登録ユーザ（Cisco Direct Customers）の場合、Ordering ツールからシスコ製品の英文マニュアルを発注できます。次の URL にアクセスしてください。

  http://www.cisco.com/en/US/partner/ordering/index.shtml
- Cisco.com に登録されていない場合、製品を購入された代理店へお問い合せください。

シスコシステムズマニュアルセンター

シスコシステムズマニュアルセンターでは、シスコ製品の日本語マニュアルの最新版を PDF 形式で公開しています。また、日本語マニュアル、および日本語マニュアル CD-ROM もオンラインで発注可能です。ご希望の方は、次の URL にアクセスしてください。

http://www2.hipri.com/cisco/

また、シスコシステムズマニュアルセンターでは、日本語マニュアル中の誤記、誤植に関するコメントをお受けしています。次の URL の「製品マニュアル内容不良報告」をクリックすると、コメント入力画面が表示されます。

http://www2.hipri.com/cisco/

なお、技術内容に関するお問い合せは、この Web サイトではお受けできませんので、製品を購入された各代理店へお問い合せください。

シスコ製品のセキュリティの概要

シスコでは、オンラインの Security Vulnerability Policy ポータル（英文のみ）を無料で提供しています。URL は次のとおりです。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このサイトは、次の目的に利用できます。

- シスコ製品のセキュリティ脆弱性を報告する。
- シスコ製品に伴うセキュリティ事象についてサポートを受ける。
- シスコからセキュリティ情報を受け取るための登録をする。

シスコ製品に関するセキュリティ勧告および注意事項の最新のリストには、次の URL からアクセスできます。

http://www.cisco.com/go/psirt

勧告および注意事項がアップデートされた時点でリアルタイムに確認する場合は、次の URL から Product Security Incident Response Team Really Simple Syndication（PSIRT RSS）フィードにアクセスしてください。

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

この製品は暗号機能を含みます。また、この製品の輸出、輸入、譲渡および使用に関しては、米国およびその他の国の法律に従います。シスコの暗号化製品の販売は、第三者権限への暗号化の輸入、輸出、配布および使用を意味するものではありません。輸出入業者、代理店およびユーザは、米国およびその他の国の法律を順守する責任があります。この製品を使用すると、適用される法律および規則を順守することに同意したことになります。米国およびその他の国の法律を順守できない場合、直ちに製品を返却してください。

シスコの暗号化製品に関する米国の法律の概要については、次の URL を参照してください。

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

さらに詳しい情報が必要な場合は、export@cisco.com まで電子メールでご連絡ください。

シスコ製品のセキュリティ問題の報告

シスコでは、セキュアな製品を提供すべく全力を尽くしています。製品のリリース前には内部でテストを行い、すべての脆弱性を早急に修正するよう努力しています。万一、シスコ製品に脆弱性が見つかった場合は、PSIRT にご連絡ください。

- 緊急の場合：security-alert@cisco.com（英語のみ）
- 緊急でない場合：psirt@cisco.com（英語のみ）

ヒント シスコに機密情報をお送りいただく際には、PGP（Pretty Good Privacy）または互換製品を使用して、暗号化することをお勧めします。PSIRT は、PGP バージョン 2.*x* から 8.*x* と互換性のある暗号化情報に対応しています。

無効になった、または有効期限が切れた暗号鍵は、絶対に使用しないでください。PSIRT に連絡する際に使用する正しい公開鍵は、次の公開鍵サーバのリストで作成日が最新の鍵です。

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

緊急の場合は、電話で PSIRT に連絡することもできます。

- 1 877 228-7302（英語のみ）
- 1 408 525-6532（英語のみ）

テクニカル サポート

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.com の Cisco Technical Support Web サイトでは、多数のサポート リソースをオンラインで提供しています。また、Cisco Technical Assistance Center（TAC）のエンジニアが電話でのサポートにも対応します。シスコと正式なサービス契約を交わしていない場合は、代理店にお問い合せください。

Cisco Technical Support Web サイト

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

Cisco Technical Support Web サイトのツールにアクセスするには、Cisco.com のユーザ ID とパスワードが必要です。サービス契約が有効で、ユーザ ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://tools.cisco.com/RPF/register/register.do

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト（http://www.cisco.com/tac）のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://www.cisco.com/jp/register

サービス リクエストの発行

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

サービス リクエストのシビラティの定義

シスコでは、報告されるサービス リクエストを標準化するために、シビラティを定義しています。

シビラティ 1（S1）：ネットワークが「ダウン」した状態か、業務に致命的な損害が発生した場合。お客様およびシスコが、24 時間体制でこの問題を解決する必要があると判断した場合。

シビラティ 2（S2）：既存のネットワーク動作が著しく低下したか、シスコ製品が十分に機能しないため、業務に重大な影響を及ぼした場合。お客様およびシスコが、通常の業務中の全時間を費やして、この問題を解決する必要があると判断した場合。

シビラティ 3（S3）：ネットワークの動作パフォーマンスが低下しているが、ほとんどの業務運用は継続できる場合。お客様およびシスコが、業務時間中にサービスを十分なレベルにまで復旧させる必要があると判断した場合。

シビラティ 4（S4）：シスコ製品の機能、インストレーション、コンフィギュレーションについて、情報または支援が必要な場合。業務の運用には、ほとんど影響がありません。

その他の資料および情報の入手方法

シスコの製品、テクノロジー、およびネットワーク ソリューションに関する情報について、さまざまな資料をオンラインおよび印刷物で入手できます。

- Cisco Marketplace では、シスコの書籍やリファレンス ガイド、ロゴ製品を数多く提供しています。購入を希望される場合は、次の URL にアクセスしてください。

  http://www.cisco.com/go/marketplace/

- 『*Cisco Product Catalog*』には、シスコシステムズが提供するネットワーキング製品のほか、発注方法やカスタマー サポート サービスについての情報が記載されています。『Cisco Product Catalog』には、次の URL からアクセスしてください。

  http://cisco.com/univercd/cc/td/doc/pcat/

- Cisco Press では、ネットワーク全般、トレーニング、および認定資格に関する出版物を幅広く発行しています。これらの出版物は、初級者にも上級者にも役立ちます。Cisco Press の最新の出版物やその他の情報を調べるには、次の URL から Cisco Press にアクセスしてください。

  http://www.ciscopress.com

- 『*Packet*』はシスコシステムズが発行する技術者向けの雑誌で、インターネットやネットワークへの投資を最大限に活用するために役立ちます。本誌は季刊誌として発行され、業界の最先端トレンド、最新テクノロジー、シスコ製品やソリューション情報が記載されています。また、ネットワーク構成およびトラブルシューティングに関するヒント、コンフィギュレーション例、カスタマー ケース スタディ、認定情報とトレーニング情報、および充実したオンライン サービスへのリンクの内容が含まれます。『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/packet

  日本語版『*Packet*』は、米国版『*Packet*』と日本版のオリジナル記事で構成されています。日本語版『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/japanese/warp/public/3/jp/news/packet/

- 『*iQ Magazine*』はシスコシステムズの季刊誌で、成長企業が収益を上げ、業務を効率化し、サービスを拡大するためには技術をどのように利用したらよいかを学べるように構成されています。本誌では、実例とビジネス戦略を挙げて、成長企業が直面する問題とそれを解決するための技術を紹介し、読者が技術への投資に関して適切な決定を下せるよう配慮しています。『*iQ Magazine*』には、次の URL からアクセスしてください。

  http://www.cisco.com/go/iqmagazine

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『*Internet Protocol Journal*』には、次の URL からアクセスしてください。

  http://www.cisco.com/ipj

- シスコは、国際的なレベルのネットワーク関連トレーニングを実施しています。最新情報については、次の URL からアクセスしてください。

  http://www.cisco.com/en/US/learning/index.html

トラブルシューティングの概要

この章では、Cisco CallManager 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 CallManager

Cisco CallManager は、Cisco IP Telephony Solution のソフトウェア ベース コール処理コンポーネントとして機能します。Cisco IP Telephony Applications Server は、Cisco CallManager のコール処理、サービス、およびアプリケーションで使用するための可用性の高いサーバ プラットフォームを提供します。Cisco CallManager はソフトウェア アプリケーションであるため、サーバ プラットフォームでソフトウェアをアップグレードするだけで、実稼働環境で機能を拡張できます。

Cisco CallManager システムは、企業のテレフォニー機能を、IP Phone、メディア処理デバイス、voice-over-IP（VoIP）ゲートウェイ、マルチメディア アプリケーションなど、パケット テレフォニー デバイスにまで拡張します。Cisco CallManager システムには、音声会議や手動コンソール機能を実行するための統合音声アプリケーション群が組み込まれています。この音声アプリケーション群があるので、音声処理用の特別なハードウェアが不要となります。

保留、任意転送、自動転送、会議、複数回線の着信表示、自動ルート選択、短縮ダイヤル、最後にダイヤルした番号のリダイヤルなど、補助的な拡張サービスが IP Phone とゲートウェイに付加されます。その他にも、統合メッセージング、マルチメディア会議、コラボラティブなコンタクト センター、対話型マルチメディア応答システムなど、データ、音声、ビデオの各サービスは、Cisco CallManager オープン テレフォニー アプリケーション プログラミング インターフェイス（API）を介して情報を交換します。

IP ネットワークを介して Cisco CallManager とすべての Cisco IP Phone、ゲートウェイ、およびアプリケーションを分散させることにより、分散型の仮想テレフォニー ネットワークが構築されます。このアーキテクチャにより、システムのアベイラビリティとスケーラビリティが向上します。コール アドミッション制御により、帯域幅に制約のある WAN リンク全体で音声の quality of service（QoS; サービス品質）が保証され、WAN 帯域幅が使用できない場合は代わりの public switched telephone network（PSTN; 公衆電話交換網）のルートにコールが転送されます。

データベースへの Web ベースのインターフェイスである Cisco CallManager Administration により、リモート デバイスとリモート システムの設定機能およびサービサビリティが提供されます。また、このインターフェイスを使用して、ユーザおよび管理者が HTML ベースのオンライン ヘルプにアクセスすることもできます。

Cisco CallManager は、シスコの統合テレフォニー アプリケーションに加えて、サードパーティ製アプリケーションに対してもシグナリングおよびコール制御のサービスを提供します。Cisco CallManager が実行する主な機能は、次のとおりです。

- コール処理
- シグナリングおよびデバイス制御
- ダイヤル プランの管理
- 電話機能の管理
- ディレクトリ サービス
- Operations, administration, management, and provisioning（OAM&P; 運用管理と保守およびプロビジョニング）
- 外部の音声処理アプリケーション（Cisco SoftPhone、Cisco IP Interactive Voice Response、Cisco Personal Assistant、Cisco CallManager Attendant Console など）に対するプログラミング インターフェイス

サービサビリティ

管理者は、Cisco CallManager Administration サービス ツールを使用して、システム問題のトラブルシューティングを行うことができます。この Web ベースのツール Serviceability は、次のサービスを提供します。

- アラーム：トラブルシューティングに備えて、Cisco CallManager サービスによって生成されたアラームとイベントを保存し、アラーム メッセージ定義を提供します。
- トレース：トラブルシューティングに備えて、Cisco CallManager サービスによって生成されたトレース情報をさまざまなログ ファイルに保存します。管理者は、トレース情報を設定および収集できます。
- Real-Time Monitoring Tool：Cisco CallManager 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。
- Service Activation：Cisco CallManager 機能のサービスのアクティベーション ステータスを表示します。管理者は、Service Activation を使用して、機能のサービスをアクティブおよび非アクティブにします。
- Control Center：Cisco CallManager サービスのステータスを表示します。管理者は、Control Center を使用して、サービスを開始および停止します。

Cisco CallManager Serviceability にアクセスするには、Cisco CallManager Administration ウィンドウで、Navigation ドロップダウン リスト ボックスから Cisco CallManager Serviceability を選択します。Cisco CallManager ソフトウェアをインストールすると、Cisco CallManager 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。

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

ハードウェアおよびソフトウェアの互換性

すべての Cisco CallManager コンポーネントの互換バージョンについては、『*Cisco CallManager Compatibility Matrix*』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、プロセスは完了です。

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るかどうかを判断するには、次の質問に答えてください。

- 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ングされているかを知っていますか。そのブリッジに設定されているフィルタはありますか。その設定のコピーはありますか。そのコピーは Cisco CallManager 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。

IP テレフォニー ネットワーク

IP テレフォニー ネットワークのトラブルシューティングについては、『*Cisco Technical Solution Series: IP Telephony Solution Guide*』を参照してください。

その他の情報

Cisco IP Telephony 関連のアプリケーションと製品の詳細は、次の資料を参照してください。

- *Release Notes for Cisco CallManager Release 5.0(1)*
- *Cisco CallManager Release 5.0(1) インストレーション ガイド*
- *Cisco CallManager Release 5.0(1) アップグレード手順*
- *Cisco CallManager システム ガイド*
- *Cisco CallManager セキュリティ ガイド*
- *Cisco CallManager アドミニストレーション ガイド*
- *Cisco CallManager Serviceability アドミニストレーション ガイド*
- *CiscoCallManager Serviceability システム ガイド*
- *Cisco CallManager 機能およびサービス ガイド*
- *Cisco CallManager Bulk Administration Tool ユーザ ガイド*
- *Cisco IP Phone アドミニストレーション ガイド for Cisco CallManager*

CHAPTER 2

トラブルシューティング ツール

この章では、Cisco CallManager 5.0(1) 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。

(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。

Sniffer 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 sniffer を装備した他のデバイスを接続することにより、sniffer 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の間に挿入されているハブ上で、sniffer 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 CallManager 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。

トレースの収集

CallManager クラスタから Call Connection Manager（CCM）と Signal Distribution Layer（SDL）の基本的なトレースを収集する方法については、ここで説明するビデオで示しています。収集した情報は、TAC Service Request Tool で使用することができます。

このビデオを観た後は、次の作業ができるようになります。

- 問題を文書化する。
- 問題を再現し、必要な情報を収集する。
- 収集した情報を TAC エンジニアに提出する。

この Flash による説明ビデオは、次の Web サイトで閲覧できます。

www.cisco.com/warp/public/788/video_64826/callmanager-tool.html
（未登録のユーザ用）

www.cisco.com/warp/customer/788/video_64826/callmanager-tool.html
（登録済みユーザ用）

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（HyperTerminal など）を設定します。HyperTerminal では、**Transfer** をクリックし、**Capture Text** 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。

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

メディアや TCP パケットをスニフィングするサードパーティ製トラブルシューティング ツールは、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 CallManager Administration を使用して次の作業を行う必要があります。

- Cisco CallManager とデバイス（Cisco IP Phone、Cisco SIP IP Phone、Cisco IOS MGCP ゲートウェイ、H.323 ゲートウェイ、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 RealTime Protocol（SRTP）パケットをキャプチャする。
- メディア暗号鍵の材料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 CallManager 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 2-1 に示す作業を行います。

表 2-1　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
ステップ 1	エンド ユーザを Standard Packet Sniffer Users グループに追加します。	Standard Packet Sniffer Users グループへのエンド ユーザの追加（P.2-5）
ステップ 2	Cisco CallManager Administration の 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。	パケット キャプチャのサービス パラメータの設定（P.2-6）

表 2-1　パケット キャプチャ設定のチェックリスト（続き）

設定のステップ		手順およびトピック
ステップ 3	Phone Configuration、Gateway Configuration、または Trunk Configuration 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。 （注）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。	• Phone Configuration ウィンドウでのパケット キャプチャの設定（P.2-6） • Gateway Configuration ウィンドウおよび Trunk Configuration ウィンドウでのパケット キャプチャの設定（P.2-7） • パケット キャプチャの設定値（P.2-9）
ステップ 4	該当するデバイス間で 、Sniffer トレースを使用して、SRTP パケットをキャプチャします。	使用している Sniffer トレース ツールに対応したマニュアルを参照
ステップ 5	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。	• パケット キャプチャのサービス パラメータの設定（P.2-6） • パケット キャプチャの設定値（P.2-9）
ステップ 6	パケットの分析に必要なファイルを収集します。	キャプチャしたパケットの分析（P.2-10）
ステップ 7	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。	キャプチャしたパケットの分析（P.2-10）

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、Packet Capture Mode 設定と Packet Capture Duration 設定を行うことができます。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 CallManager Administration でエンド ユーザを『*Cisco CallManager アドミニストレーション ガイド*』の説明に従って設定したことを前提としています。

手順

ステップ 1　『*Cisco CallManager 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。

ステップ 2　Find/List 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　**Add Users to Group** ボタンをクリックします。

ステップ 4　『*Cisco CallManager 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。

ステップ 5　ユーザを追加したら、**Save** をクリックします。

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 CallManager Administration で、**System > Service Parameters** を選択します。

ステップ 2　Server ドロップダウン リスト ボックスから、Cisco CallManager サービスをアクティブにした Active サーバを選択します。

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

ステップ 4　TLS Packet Capturing Configuration 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、**Save** 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。

- Phone Configuration ウィンドウでのパケット キャプチャの設定（P.2-6）
- Gateway Configuration ウィンドウおよび Trunk Configuration ウィンドウでのパケット キャプチャの設定（P.2-7）

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

パケット キャプチャを Service Parameter ウィンドウで有効にしたら、Cisco CallManager Administration の Phone Configuration ウィンドウで、デバイスごとにパケット キャプチャを設定することができます。

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.2-4 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 CallManager 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　Phone Configuration ウィンドウが表示されたら、表 2-2 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、**Save** をクリックします。

ステップ 5　Reset ダイアログボックスで、**OK** をクリックします。

ヒント　Cisco CallManager Administration 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 Sniffer 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.2-10 の「キャプチャしたパケットの分析」を参照してください。

Gateway Configuration ウィンドウおよび 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 CallManager Administration でのパケット 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。

Gateway Configuration ウィンドウまたは 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.2-4 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 CallManager 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 CallManager 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 CallManager 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 CallManager 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、Packet Capture Mode 設定値と 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 CallManager アドミニストレーション ガイド*』の説明に従って設定して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 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 2-2 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、**Save** をクリックします。

ステップ 6　Reset ダイアログボックスで、**OK** をクリックします。

ヒント　Cisco CallManager Administration 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 Sniffer 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.2-10 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

Packet Capture Mode 設定値および Packet Capture Duration 設定値について説明した表 2-2 とともに、次の項も参照してください。

- Phone Configuration ウィンドウでのパケット キャプチャの設定（P.2-6）
- Gateway Configuration ウィンドウおよび Trunk Configuration ウィンドウでのパケット キャプチャの設定（P.2-7）

表 2-2　パケット キャプチャの設定値

設定値	説明
Packet Capture Mode	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。 • **None**：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 CallManager は Packet Capture Mode を None に設定します。 • **Batch Processing Mode**：Cisco CallManager 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 CallManager 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。ファイルの格納先は、/var/pktCap 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。 **ヒント**　TAC にお問い合せいただく前に、該当するデバイス間で Sniffer トレースを使用して、SRTP パケットをキャプチャする必要があります。
Packet Capture Duration	この設定値は、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。 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。 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。

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 にお問い合せいただく前に、該当するデバイス間で Sniffer 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 CallManager セキュリティ ガイド*』を参照してください。

Cisco CallManager トラブルシューティング ツール

さまざまな Cisco CallManager システムを監視および分析するために Cisco CallManager Serviceability が提供する、次のようなタイプのツールの詳細については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』および『*Cisco CallManager Serviceability システム ガイド*』を参照してください。

表 2-3　Serviceability ツール

用語	定義
Real-Time Monitoring Tool（RTMT）	この用語は、Cisco CallManager 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する、Serviceability 内のプログラムを示します。
アラーム	管理者は、アラームを使用して、Cisco CallManager 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、説明や推奨される処置など、システムの問題に関する情報が含まれています。
アラーム カタログ	この用語は、Cisco CallManager サービスのすべてのアラーム定義を含むファイルを示します。Serviceability は、アラーム タイプに固有の複数のアラーム カタログをサポートしています。
アラーム定義	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される処置が含まれています。
アラーム イベント レベル	管理者は、アラームに含まれる情報のレベルを決定します。レベルの範囲は、システムに関する一般的な情報から、デバッグだけを目的とした情報にまで及びます。
アラーム フィルタ	管理者は、アラームに含まれる情報のレベル、およびアラーム 情報が保存される場所を決定します。
アラーム モニタ	Cisco CallManager Serviceability では、モニタと呼ばれるさまざまな宛先（ローカルの syslog、リモートの syslog、SDI トレース、および SDL トレース）にアラームを送信できます。
アラート通知	管理者は、Real-Time Monitoring Tool を使用して、パフォーマンス カウンタおよびゲートウェイ ポート（チャネル）のアラート通知を設定します。リアルタイム モニタリングでは、電子メールまたはシステム通知（ポップアップ）ウィンドウで管理者にアラートが送信されます。
カテゴリ タブ	管理者は、トラブルシューティングの目的で、リアルタイム モニタリングに特定のモニタリング ウィンドウを設定します。管理者は、カテゴリ タブを使用して、その特定のウィンドウを作成します。
チャート ビュー	Performance Monitoring ウィンドウでは、デフォルトで、チャート ビューにパフォーマンス カウンタが表示されます。チャート ビューでは、カウンタ情報がグラフィカルに表示されます。
Cisco CallManager サービス	Cisco CallManager は、TFTP、CTI、Music On Hold（MOH; 保留音）など、特定の機能を実行するソフトウェアの形で、多くのサービスをサポートしています。
Control Center	Serviceability の Control Center ツールを使用すると、管理者は、Cisco CallManager サービスのステータスを表示したり、Cisco Callmanager サービスを開始および停止できます。
デバッグ トレース レベル	管理者は、トレースに含まれる情報のレベルを決定します。レベルの範囲は、一般的なエラーから、デバッグを目的とした詳細なエラーにまで及びます。

表 2-3　Serviceability ツール（続き）

用語	定義
デバイス モニタリング	リアルタイム モニタリングでは、電話機やゲートウェイなど、Cisco CallManager デバイスに関するリアルタイム情報が表示されます。
Device Monitoring ウィンドウ	Real-Time Monitoring Tool がデバイスのパフォーマンスを監視しているときに、Real-Time Monitoring Tool ウィンドウの右側にデバイスのパフォーマンス情報が表示されます。
デバイス名に基づくトレース モニタリング	管理者は、Cisco CallManager および Cisco CTIManager サービスのトレース パラメータを設定することにより、選択したデバイスに関するトレース情報を取得します。
Monitoring Objects ウィンドウ	Real-Time Monitoring Tool ウィンドウの左側には、クラスタに対応する、Cisco CallManager 関連のオブジェクトおよびカウンタまたはデバイスが表示されます。表示される情報は、ウィンドウでアクティブになっているタブによって異なります。
オブジェクトとカウンタ	システムは、さまざまなオブジェクトおよびカウンタに関する情報を含むパフォーマンス データを提供します。オブジェクトとは、Cisco IP Phone や Cisco CallManager 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。Real-Time Monitoring Tool は、これらのカウンタによって生成されるリアルタイムの統計情報を監視します。
パフォーマンス モニタリング	Real-Time Monitoring Tool には、パフォーマンス カウンタに関するリアルタイム情報が表示されます。パフォーマンス カウンタは、システム固有のものも Cisco CallManager 固有のものもあります。
Performance Monitoring ウィンドウ	Real-Time Monitoring Tool がカウンタを監視しているときに、Real-Time Monitoring Tool ウィンドウの右側にカウンタの統計情報が表示されます。
CCM トレース ログ ファイル（以前は SDI トレース）	すべての Cisco CallManager 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。
Quality Report Tool	この用語は、Cisco CallManager 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。
SDL トレース ログ ファイル	このファイルには、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。 **（注）** 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。
サービスのステータス	Control Center には、サーバ上のサービスのステータスが表示されます。
トレース	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 CallManager サービスの問題に関する特定の情報を取得します。

表 2-3　Serviceability ツール（続き）

用語	定義
トレース ログ ファイル	Cisco CallManager Serviceability は、設定されているトレース情報をこのファイルに送信します。CCM 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。
ウィンドウ ステータス バー	Real-Time Monitoring Tool ウィンドウの右下隅には、ウィンドウ ステータス バーが表示されます。このステータス バーには、Preferences、Cluster Information、Resource Usage、About、および Help という 5 つのアイコンが表示されます。

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 CallManager 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 CallManager 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。

コマンドライン インターフェイス

コマンドライン インターフェイス（CLI）は、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 CallManager システムにアクセスするために使用します。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、コマンドの集合です。たとえば、***show*** はレベルであり、***show status*** はコマンドです。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 CallManager の CLI コマンド セットの詳細については、『*Cisco IP Telephony Platform Administration Guide Release 5.0(1)*』の「Appendix A」を参照してください。

トラブルシューティング用 perfmon データのロギング

注意　トラブルシューティング用 perfmon データのロギング機能を有効にすると、有効にしたノード上ではシステムのパフォーマンスが低下します。このパラメータは、Cisco Technical Assistance Center（TAC）からの指示がない限り有効にしないでください。

トラブルシューティング用 perfmon データのロギング機能は、システムの問題点を特定する際に、Cisco TAC が利用します。トラブルシューティング用 perfmon データのロギングを有効にすると、有効にしたノード上では、Cisco CallManager およびオペレーティング システムのパフォーマンスに関する、一連の統計情報の収集が開始されます。収集される統計情報には、システムの診断に利用できる包括的な情報、および現在の事前設定済みカウンタ セットに含まれていない、一連のカウンタからの情報が含まれています。

大量の情報が短時間で収集されるため、トラブルシューティング用 perfmon データのロギングは、長時間にわたって有効にしないことを強くお勧めします。また、有効にしている間は、Log Partitioning Monitor を有効にしてディスクの使用状況を監視してください。

トラブルシューティング用 perfmon データのロギング機能をアクティブな電話コールが発生しないシステム上で有効にし、このロギングのパラメータをデフォルト設定のまま使用した場合、シスコによる見積りでは、システムでの CPU 使用率の上昇は 5 % 未満であり、使用メモリ量の増加はわずかなもので、ログ ファイルには 1 日あたり約 50 MB の情報が書き込まれます。

トラブルシューティング用 perfmon データのロギング機能については、次の管理タスクを実行できます。

- トラブルシューティング用 perfmon データのロギングのトレース フィルタを有効または無効にする。
- 各サーバ上で、事前定義済みの一連の System パフォーマンス オブジェクトおよび Cisco CallManager パフォーマンス オブジェクト、およびカウンタを監視する。
- ローカル サーバ上のアクティブなログ パーティションと cm/log/ris/csv ディレクトリに、監視対象のパフォーマンス データを CSV ファイル形式で記録する。ログ ファイルの命名規則は、PerfMon_<node>_<month>_<day>_<year>_<hour>_<minute>.csv です。たとえば、PerfMon_172.19.240.80_06_15_2005_11_25.csv のようになります。
- ポーリングのレートを指定する。このレートは、パフォーマンス データを収集し、ログに記録するレートです。設定できるポーリング レートは、最短で 5 秒です。デフォルトのポーリング レートは 15 秒です。
- ディスクに格納するログ ファイルの最大数を指定する。この制限値を超えると、ログ ファイルが自動的に消去されます（最も古いログ ファイルが削除されます）。
- ファイルの最大サイズ（MB 単位）に基づいて、ログ ファイルのロールオーバー基準を指定する。デフォルト値は 2 MB です。
- TCT/SOAP トレース収集ツール（TCT）またはコマンドライン インターフェイスを使用して、ログ ファイルを収集する。
- Microsoft Windows の Performance ツールを使用して、ログ ファイルをグラフ形式で表示する。

トラブルシューティング用 perfmon データのロギング機能では、次の perfmon オブジェクトに含まれている次のカウンタから情報を収集します。各カウンタについては、『*Cisco CallManager Serviceability システム ガイド*』の「Performance Objects and Counters」の章を参照してください。

- Cisco CallManager オブジェクト：
  - CallManagerHeartBeat
  - CallsActive

  - CallsAttempted
  - CallsCompleted
  - InitializationState
  - RegisteredHardwarePhones
  - RegisteredMGCPGateway
- Cisco CallManager System パフォーマンス オブジェクト：
  - QueueSignalsPresent 1-High
  - QueueSignalsPresent 2-Normal
  - QueueSignalsPresent 3-Low
  - QueueSignalsPresent 4-Lowest
  - QueueSignalsProcessed 1-High
  - QueueSignalsProcessed 2-Normal
  - QueueSignalsProcessed 3-Low
  - QueueSignalsProcessed 4-Lowest
  - QueueSignalsProcessed Total
- Cisco TFTP：
  - BuildAbortCount
  - BuildCount
  - BuildDeviceCount
  - BuildDialruleCount
  - BuildDuration
  - BuildSignCount
  - BuildSoftkeyCount
  - BuildUnitCount
  - ChangeNotifications
  - DeviceChangeNotifications
  - DialruleChangeNotifications
  - EncryptCount
  - GKFoundCount
  - GKNotFoundCount
  - HeartBeat
  - HttpConnectRequests
  - HttpRequests
  - HttpRequestsAborted
  - HttpRequestsNotFound
  - HttpRequestsOverflow
  - HttpRequestsProcessed
  - HttpServedFromDisk
  - LDFoundCount
  - LDNotFoundCount
  - MaxServingCount
  - Requests
  - RequestsAborted

  - RequestsInProgress
  - RequestsNotFound
  - RequestsOverflow
  - RequestsProcessed
  - SegmentsAcknowledged
  - SegmentsFromDisk
  - SegmentsSent
  - SEPFoundCount
  - SEPNotFoundCount
  - SIPFoundCount
  - SIPNotFoundCount
  - SoftkeyChangeNotifications
  - UnitChangeNotifications
- Process オブジェクト：
  - PID
  - STime
  - % CPU Time
  - Page Fault Count
  - VmData
  - VmSize
  - Thread Count
- Memory オブジェクト：
  - Used Kbytes
  - Free Kbytes
  - Total Kbytes
  - Shared Kbytes
  - Buffers Kbytes
  - Cached Kbytes
  - Free Swap Kbytes
  - Total Swap Kbytes
  - Used Swap Kbytes
  - Pages Input
  - Pages Output
  - Pages
  - % Page Usage
  - % VM Used
  - % Mem Used
- Processor オブジェクト：
  - Irq Percentage
  - Softirq Percentage
  - IOwait Percentage
  - User Percentage
  - Nice Percentage

  - System Percentage
  - Idle Percentage
  - %CPU Time
- Thread オブジェクト（トラブルシューティング用 perfmon データのロギング機能で記録されるのは、CCM スレッドのみ）：
  - PID
  - %CPU Time
- Partition オブジェクト：
  - Used Mbytes
  - Total Mbytes
  - %Used
  - % Wait in Read Time
  - % Wait in Write Time
  - % CPU Time
  - Read Bytes Per Sec
  - Write Bytes Per Sec
  - Queue Length
- IP オブジェクト：
  - In Receives
  - InHdr Errors
  - In Unknown Protos
  - In Discards
  - In Delivers
  - Out Requests
  - Out Discards
  - Reasm Reqds
  - Reasm Oks
  - Reasm Fails
  - Frag OKs
  - Frag Fails
  - Frag Creates
  - InOut Requests
- TCP オブジェクト：
  - Active Opens
  - Passive Opens
  - Attempt Fails
  - Estab Resets
  - Curr Estab
  - In Segs
  - Out Segs
  - Retrans Segs
  - InOut Segs

- Network Interface オブジェクト：
  - Rx Bytes
  - Rx Packets
  - Rx Errors
  - Rx Dropped
  - Rx Multicast
  - Tx Bytes
  - Tx Packets
  - Tx Errors
  - Tx Dropped
  - Total Bytes
  - Total Packets
  - Tx QueueLen
- System オブジェクト：
  - Allocated FDs
  - Freed FDs
  - Being Used FDs
  - Max FDs
  - Total Processes
  - Total Threads
  - Total CPU Time

次に、トラブルシューティング用 perfmon データのロギング機能を使用する手順を示します。

手順

ステップ 1　Cisco RIS Data Collector サービスの Troubleshooting Perfmon Data Logging パラメータを設定します。

P.2-19 の「トラブルシューティング用 perfmon データのロギングの設定」を参照してください。

ステップ 2　ログ パーティションの監視が有効になっていることを確認します。

『*Cisco CallManager アドミニストレーション ガイド*』を参照してください。

ステップ 3　トラブルシューティング用 perfmon データのロギングを有効にしたサーバ上で、Cisco RIS Data Collector サービスのログ ファイルを収集します。

- ログ ファイルを RTMT を使用してダウンロードする場合は、『*Cisco CallManager アドミニストレーション ガイド*』を参照してください。
- ログ ファイルを CLI を使用してダウンロードする場合は、『*Cisco IP Telephony Platform Administration Guide*』を参照してください。

ステップ 4　Microsoft Windows の Performance ツールを使用して、ログ ファイルを表示します。

P.2-20 の「Microsoft Performance ツールでの perfmon ログ ファイルの表示」を参照してください。

ステップ 5　必要なファイルをすべて収集したら、Enable Logging パラメータを False に設定して、トラブルシューティング用 perfmon データのロギングを無効にします。

トラブルシューティング用 perfmon データのロギングの設定

ここでは、トラブルシューティング用 pefmon データのロギング機能を設定する手順について説明します。

手順

ステップ 1　Cisco CallManager Administration で、**System > Service Parameters** を選択します。

Service Parameter Configuration ウィンドウが表示されます。

ステップ 2　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。

ステップ 3　Service ドロップダウン リスト ボックスから、Cisco RIS Data Collector を選択します。

ステップ 4　表 2-4 の説明に従って、適切な設定値を入力します。

ステップ 5　**Save** をクリックします。

表 2-4　トラブルシューティング用 perfmon データのロギングのパラメータ

フィールド	説明
Enable Logging	ドロップダウン リスト ボックスから、**True** を選択してトラブルシューティング用 perfmon データのロギングを有効にします。または、**False** を選択して無効にします。
Polling Rate	ポーリング レート（間隔）を秒単位で入力します。5（最短）～ 300（最長）の値を入力できます。デフォルト値は 15 です。
Maximum No. of Files	ディスクに格納するトラブルシューティング用 perfmon データのロギング ファイル数の上限を入力します。1（最少）～ 100（最大）の値を入力できます。デフォルト値は 50 です。 Maximum No. of Files パラメータおよび Maximum File Size パラメータを設定するときは、ストレージ容量を考慮に入れてください。Maximum No. of Files 値に Maximum File Size 値を掛けたときに、値が 100 MB を超えないようにすることをお勧めします。 ファイル数がこのフィールドで指定したファイル数上限値を超えると、タイムスタンプの最も古いログ ファイルが削除されます。 **注意**　このパラメータを変更する場合は、事前にログ ファイルを別のマシンに保存しておかないと、ログ ファイルが失われる恐れがあります。

表 2-4　トラブルシューティング用 perfmon データのロギングのパラメータ（続き）

フィールド	説明
Maximum File Size	perfmon ログ ファイルに格納するときの最大ファイル サイズを MB 単位で入力します。このサイズに達すると、新しいファイルが作成されます。1（最小）～ 500（最大）の値を入力できます。デフォルト値は 2 です。 Maximum No. of Files パラメータおよび Maximum File Size パラメータを設定するときは、ストレージ容量を考慮に入れてください。Maximum No. of Files 値に Maximum File Size 値を掛けたときに、値が 100 MB を超えないようにすることをお勧めします。

Microsoft Performance ツールでの perfmon ログ ファイルの表示

Microsoft の Performance ツールを使用してログ ファイルを表示するには、次の手順に従います。

手順

ステップ 1　**Start > Settings > Control Panel > Administrative Tools > Performance** を選択します。

ステップ 2　アプリケーションのウィンドウで、マウスの右ボタンをクリックし、**Properties** を選択します。

ステップ 3　System Monitor Properties ダイアログボックスで、Source タブをクリックします。

ステップ 4　perfmon ログ ファイルをダウンロードしたディレクトリを参照し、perfmon の csv ファイルを選択します。ログ ファイルの命名規則は、PerfMon_<node>_<month>_<day>_<year>_<hour>_<minute>.csv です。たとえば、PerfMon_172.19.240.80_06_15_2005_11_25.csv のようになります。

ステップ 5　**Apply** をクリックします。

ステップ 6　**Time Range** ボタンをクリックします。表示する perfmon ログ ファイルについて期間を指定するには、バーを適切な開始時刻および終了時刻にドラッグします。

ステップ 7　Add Counters ダイアログボックスを開くには、Data タブをクリックし、**Add** をクリックします。

ステップ 8　Performance Object ドロップダウン リスト ボックスから、perfmon オブジェクトを選択します。オブジェクトに複数のインスタンスがある場合は、**All instances** を選択するか、表示するインスタンスのみ選択します。

ステップ 9　**All Counters** を選択するか、表示するカウンタのみ選択します。

ステップ 10　選択したカウンタを追加するには、**Add** をクリックします。

ステップ 11　カウンタの選択が終了したら、**Close** をクリックします。

CiscoWorks2000

CiscoWorks2000 は、Cisco CallManager 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 CallManager 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 サービサ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、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』、および次の 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 CallManager 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、Cisco IP テレフォニー ソリューション用の集中システム ロギング サービスを提供します。

詳細については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』を参照してください。

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 CallManager サーバを検出および管理できます。

CiscoWorks2000 の詳細については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』、および次の 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

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 CallManager と互換性があります。
  - CiscoWorks2000
  - HP OpenView
  - SNMP および Cisco CallManager 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

詳細については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』および『*Cisco CallManager Serviceability システム ガイド*』を参照してください。

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

この項は、ルート アクセスが無効になっている Cisco CallManager 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。この項では、次のトピックについて取り上げます。

- よく使用される Linux コマンドに対応する Serviceability の GUI および CLI コマンド
- 一般的なトラブルシューティング作業
  - ログおよびトレース ファイルを収集する方法
  - ログおよびトレース ファイルの収集スケジュールを設定する方法
  - データベースにアクセスする方法
  - ハードディスクの空き容量を増やす方法
  - コア ファイルを表示する方法
  - Cisco CallManager サーバをリブートする方法
  - トレースのデバッグ レベルを変更する方法
  - ネットワークのステータスを表示する方法

よく使用される Linux コマンドに対応する Serviceability の GUI および CLI コマンド

Real Time Monitoring Tool（RTMT）は、管理者の PC にインストールできるクライアント アプリケーションです。インストールするには、RTMT クライアントを次の URL でサーバからダウンロードします。

https://<server_ipaddress>:8443/ccmadmin/pluginsFindList.do

手順

ステップ 1　Cisco CallManager にログインします。

ステップ 2　**Applications > Plugins** を選択します。

図 2-1 に示す Find and List Plugins 画面が表示されます。

図 2-1　Cisco CallManager の Find and List Plugins 画面

ステップ 3　選択ボックスを **Name contains** に設定し、**tool** と入力します。

ステップ 4　**Plugin Type** 選択ボックスを **Installation** に設定します。

ステップ 5　**Find** をクリックします。

Search Results ボックスに、Cisco CallManager Real-Time Monitoring Tool の Windows バージョンおよび Linux バージョンへのリンクが表示されます。

ステップ 6　適切な RTMT インストール プラグイン（Windows バージョンまたは Linux バージョン）をダウンロードします。

ステップ 7　RTMT クライアント アプリケーションを PC またはワークステーションにインストールします。

表 2-5 に、以降の各項で説明する 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 2-5　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	Serviceability の GUI ツール	CLI コマンド
CPU 使用率	top	RTMT View > Server CPU and Memory に移動	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 <Process task_name>
プロセスの状態	ps	RTMT View > Server Process に移動	show perf query counter Process "Process Status"
ディスクの使用状況	df/du	RTMT View > Server Disk Usage に移動	show perf query counter Partition "% Used" または show perf query class Partition
メモリ	free	RTMT View > Server CPU and Memory に移動	show perf query class Memory
ネットワークのステータス	netstats		show network status

表 2-5　CLI コマンドおよび GUI 選択オプションの要約（続き）

情報	Linux コマンド	Serviceability の GUI ツール	CLI コマンド
サーバのリブート	reboot	サーバの Platform 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 > Trace > Trace & Log Central > Collect Files に移動	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

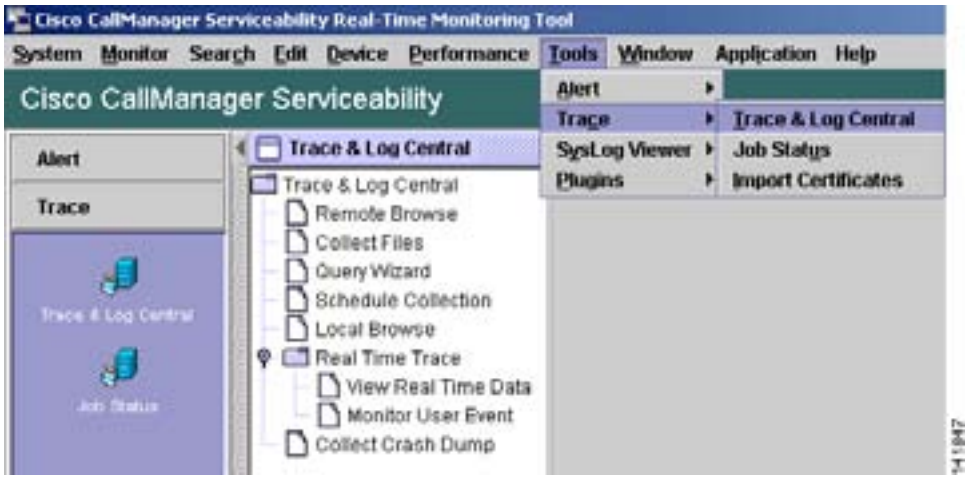
一般的なトラブルシューティング作業

ログおよびトレース ファイルを収集する方法

GUI

RTMT クライアント アプリケーションを使用して、**Tools** メニューに移動し、**Trace > Trace & Log Central** を選択して、各種のトレース ユーティリティを表示します。

図 2-2　Cisco CallManager RTMT の Trace & Log Central



CLI

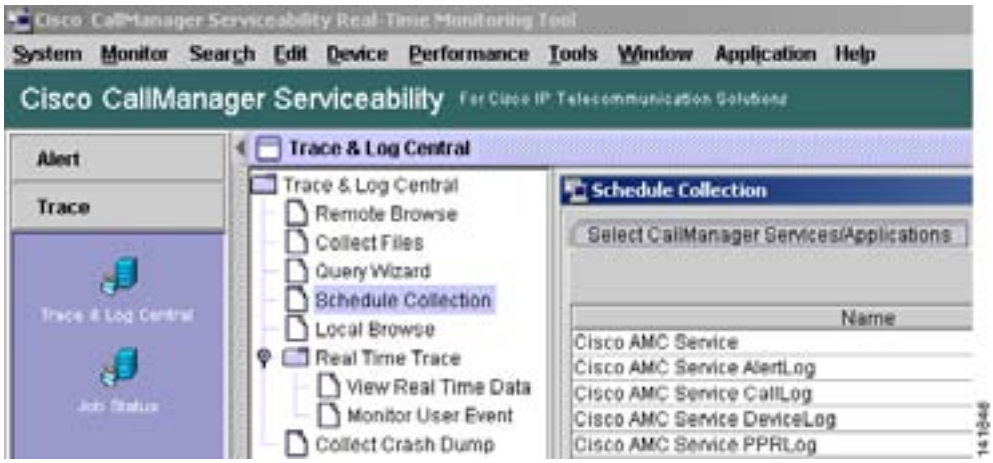
- file list
- file get
- file view

ログおよびトレース ファイルの収集スケジュールを設定する方法

GUI

RTMT クライアント アプリケーションを使用して、**Tools** メニューに移動し、**Trace & Log Central > Schedule Collection** を選択します。

図 2-3　Cisco CallManager RTMT の Schedule Collection



データベースにアクセスする方法

CLI

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。

- show tech database
- show tech dbinuse
- show tech dbschema
- show tech devdefaults
- show tech gateway
- show tech locales
- show tech notify
- show tech procedures
- show tech routepatterns
- show tech routeplan
- show tech systables
- show tech table
- show tech triggers
- show tech version
- show tech params*

SQL コマンドを実行するには、**run** コマンドを使用します。

- run <sql command>

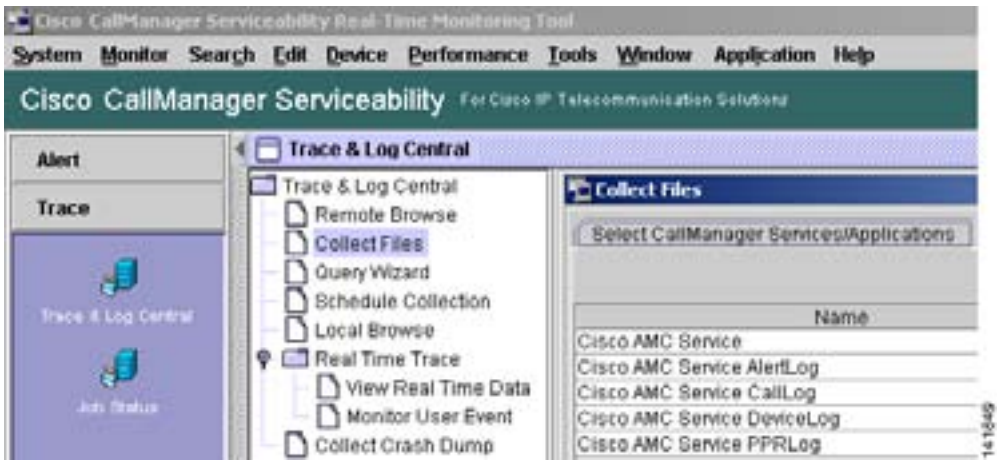
ハードディスクの空き容量を増やす方法

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。

GUI

RTMT クライアントを使用して、**Tools** メニューに移動し、**Trace & Log Central > Collect Files** を選択します。

図 2-4　Cisco CallManager RTMT の Collect Files



収集するファイルの選択基準を選択し、**Delete Files** オプションをチェックします。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 CallManager サーバ上のファイルは削除されます。

CLI

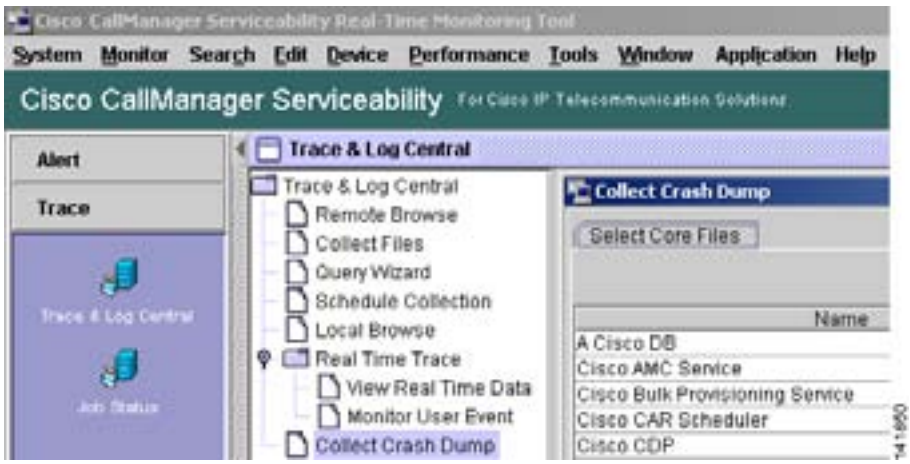
- file delete

コア ファイルを表示する方法

GUI

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 **Tools > Trace 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。

図 2-5　Cisco CallManager RTMT の Collect Crash Dump



CLI

- Core [options..]

Cisco CallManager サーバをリブートする方法

GUI

サーバ上で Platform Web ページにログインし、**Restart > Current Version** に移動します。

CLI

- utils system restart

トレースのデバッグ レベルを変更する方法

GUI

Serviceability の Web ページ（https://<server_ipaddress>:8443/ccmservice/）にログインし、**Trace > Configuration** に移動します。

CLI

- 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方法

GUI

なし

CLI

- show network status

トラブルシューティングのヒント

次のヒントは、Cisco CallManager のトラブルシューティングに役立ちます。

ヒント　Cisco CallManager 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 CallManager 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 CallManager に登録されている場合、コールがそこで開始されると、コール処理がその Cisco CallManager で実行されます。問題をデバッグするには、その Cisco CallManager 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ライバ 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 CallManager 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** ボタンを 2 回押すと、Cisco 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 CallManager 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 **View** > **Refresh** を選択し、ファイルの日付と時刻を確認することです。

Cisco CallManager 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。

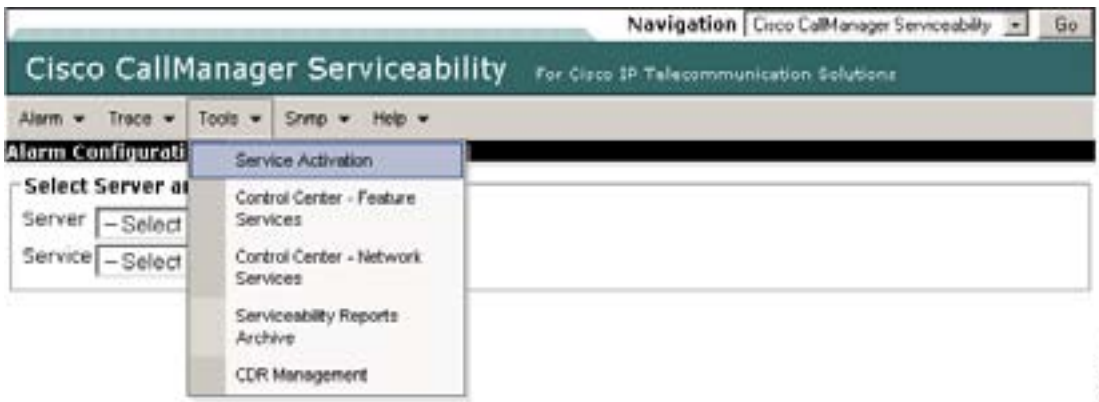
手順

ステップ 1　Cisco CallManager Administration から、**Navigation** > **Cisco CallManager Serviceability** を選択します。

Cisco CallManager Serviceability ウィンドウが表示されます。

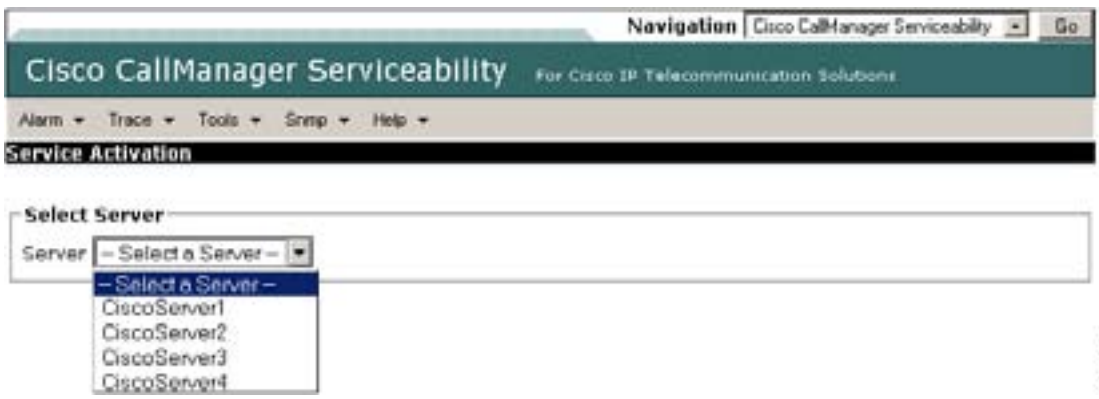
ステップ 2　図 2-6 のように、**Tools** > **Service Activation** を選択します。

図 2-6　Cisco CallManager Serviceability ウィンドウの Tools メニュー



ステップ 3　Servers カラムから、目的のサーバを選択します（図 2-7 を参照）。

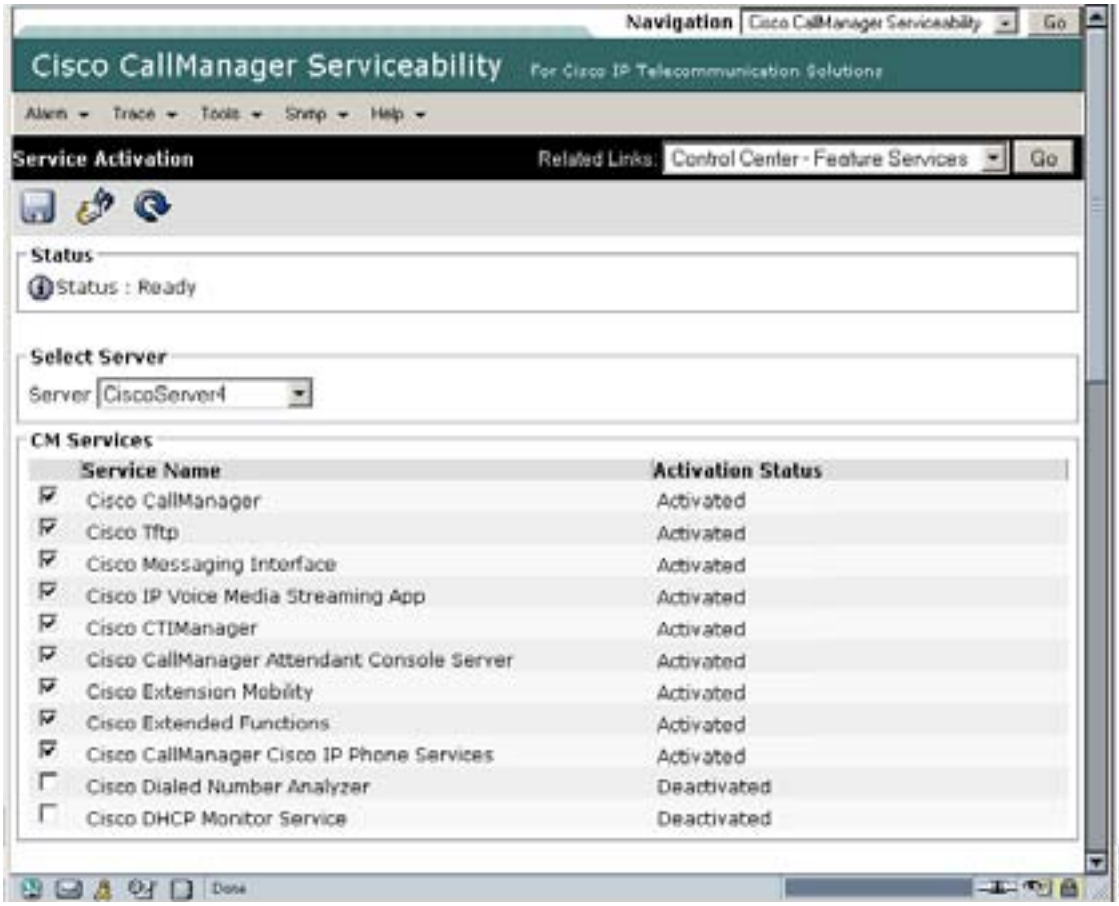
図 2-7　Cisco CallManager Serviceability ウィンドウの Service Activation



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。

図 2-8 のように、Cisco CallManager 行の Activated Status カラムに Activated または Deactivated と表示されます。

図 2-8　Service Activation ウィンドウ



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です。

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 Cisco CallManager サービスがアクティブになりました。

Cisco CallManager が使用されているかどうか、および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 CallManager Administration から、**Navigation > Cisco CallManager Serviceability** を選択します。

Cisco CallManager 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　Servers 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、選択したサーバ上でどのサービスが動作しているかが表示されます。

その他の情報

参考資料

- *Cisco CallManager Serviceability アドミニストレーション ガイド*
- *CiscoCallManager Serviceability システム ガイド*
- *Cisco CallManager アドミニストレーション ガイド*
- *Cisco CallManager セキュリティ ガイド*
- *Cisco CallManager インストレーション ガイド*

■ その他の情報

CHAPTER 3

Cisco CallManager Attendant Console

Cisco CallManager 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 CallManager 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 CallManager Serviceability システム ガイド*』および『*Cisco CallManager Serviceability アドミニストレーション ガイド*』を参照してください。

この章では、Cisco CallManager Attendant Console で発生する次の問題をトラブルシューティングするための情報を示します。

テレフォニー初期化エラー

この項では、Cisco CallManager Attendant Console の次の電話初期化エラー メッセージ表示について説明します。

テレフォニー初期化の失敗

症状　アテンダントが、テレフォニーの初期化が失敗したことを示すエラー メッセージを受信しました。

考えられる原因　Cisco CallManager Administration で、「ac」ユーザを Standard CTI Allow Park Monitoring ユーザ グループに関連付ける必要があります。

この他の原因としては、次のものが挙げられます。

- パイロット　ポイントおよび制御されている電話機のいずれかまたは両方が、「ac」ユーザの制御デバイス リストに含まれていません。
- 「ac」ユーザが存在していません。
- 「ac」ユーザのパスワードが一致していません。
- Cisco CallManager Administration で、「ac」ユーザが Standard CTI Enabled ユーザ グループに関連付けられていません。

推奨処置　次の手順を実行します。

手順

ステップ 1　Cisco CallManager Administration から、**User Management > User Groups** を選択します。

Find and List User Groups ウィンドウが表示されます。

ステップ 2　**Standard CTI Allow Park Monitoring** ユーザ グループのリンクをクリックします。

User Group Configuration ウィンドウが表示されます。

ステップ 3　**Add Application Users to Group** ボタンをクリックします。

Find and List Application Users ウィンドウが表示されます。

ステップ 4　ユーザ名「ac」を検索ボックスに入力し、**Find** をクリックします。

ステップ 5　「ac」ユーザの隣にあるチェックボックスをオンにし、**Add Selected** をクリックします。

コール制御の初期化の失敗

☑ Allow Control of Device from CTI

各アテンダントの電話機の Phone Configuration ウィンドウで、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、そのアテンダントのコンソールでは、コール制御が発生しません。

症状　Cisco CallManager 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　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。

推奨処置　Windows XP SP2 のインストール後に Cisco CallManager 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 CallManager Attendant Console の使用を続けて、**Unblock** 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 CallManager Attendant Console を初めて起動したとき、Unblock 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 CallManager 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　**Start > Settings > Control Panel > Windows Firewall** を選択します。

Windows Firewall ダイアログボックスが表示されます。

ステップ 2　Exception タブを選択します。

ステップ 3　**All Program** ボタンをクリックします。

Add a Program ダイアログボックスが表示されます。

ステップ 4　**Browse** をクリックします。ACClient.exe ファイルを参照し、**Open** をクリックします。

Windows Firewall ダイアログボックスの Exceptions 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　**Edit** をクリックします。

Edit a Program ダイアログボックスが表示されます。

ステップ 6　**Change Scope** をクリックします。

Change Scope ダイアログボックスが表示されます。

ステップ 7　**Any computer (including those on the internet)** 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 メッセージが表示される

症状

アテンダントがサーバにログインしようとすると、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 にあるコンソールのバージョンが、Cisco CallManager Administration から使用できるコンソールのバージョンと一致していません。

対応策

アテンダントの PC で動作しているコンソールのバージョンをアップグレードします。

手順

ステップ 1　Cisco CallManager Attendant Console のある各 PC から、Cisco CallManager Administration が動作しているサーバを参照し、管理特権を持つアカウントでログインします。

ステップ 2　Cisco CallManager Administration から、**Application** > **Plugins** を選択します。

ステップ 3　**Find** をクリックします。

ステップ 4　Cisco CallManager Attendant Console の隣にある **Download** リンクをクリックします。

ステップ 5　**Open** をクリックします。

Cisco CallManager Attendant Console のインストール ウィザードが起動します。

ステップ 6　インストール ウィザードの最初のウィンドウで、**Next** をクリックします。

ステップ 7　License Agreement ウィンドウで、**I accept the license agreement** オプション ボタンをクリックし、**Next** をクリックします。

ステップ 8　コンソールは、デフォルトの位置にインストールすることも、Browse ボタンを使用して指定する新しい位置にインストールすることもできます。位置を指定したら、**Next** をクリックします。

ステップ 9　Ready to Install ウィンドウで、**Next** をクリックします。

ステップ 10　ファイルのインストールが完了したら、コンピュータをすぐに再起動するか、後で再起動するかを選択し、**Finish** をクリックします。

ステップ 11　コンピュータを再起動するように求められた場合は、再起動します。

コンソール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コンソール設定をしたり更新したりできます。

コールの発信と受信に関する問題

この項では、コールの発信と受信に関する Cisco CallManager Attendant Console の次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

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

パイロット ポイントおよび制御されている電話機のいずれかまたは両方が、「ac」ユーザの制御デバイス リストに含まれていません。

対応策

Cisco CallManager Administration で、「ac」という名前のユーザを設定し、アテンダントの電話機とパイロット ポイントをそのユーザに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、コンソールは 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。

手順

ステップ 1　**User Management > Application User** を選択します。

Find and List Application Users ウィンドウが表示されます。

ステップ 2　**Add New** をクリックします。

Application User Configuration ウィンドウが表示されます。

ステップ 3　User ID フィールドに、**ac** と入力します。

ステップ 4　Password フィールドに、**12345** と入力します。

ステップ 5　Confirm Password フィールドに、**12345** と入力します。

ステップ 6　**Save** をクリックします。

ステップ 7　**User Management > User Groups** を選択します。

Find and List User Groups ウィンドウが表示されます。

ステップ 8　**Standard CTI Allow Park Monitoring** ユーザ グループのリンクをクリックします。

User Group Configuration ウィンドウが表示されます。

ステップ 9　**Add Application Users to Group** ボタンをクリックします。

Find and List Application Users ウィンドウが表示されます。

ステップ 10　ユーザ名「ac」を検索ボックスに入力し、**Find** をクリックします。

ステップ 11　「ac」ユーザの隣にあるチェックボックスをオンにし、**Add Selected** をクリックします。

ステップ 12　Related Topics ドロップ リスト ボックスの隣にある **Go** ボタンをクリックします。

ステップ 13　**Standard CTI Enabled** ユーザ グループのリンクをクリックします。

ステップ 14　**Add Application Users to Group** ボタンをクリックします。

ステップ 15　ユーザ名「ac」を検索ボックスに入力し、**Find** をクリックします。

ステップ 16　「ac」ユーザの隣にあるチェックボックスをオンにし、**Add Selected** をクリックします。

ステップ 17　Application End User Configuration ウィンドウで、デバイスとパイロット ポイントが ac ユーザに関連付けられていることを確認します。

回線が使用できない

症状

アテンダントが、選択した回線が使用できないことを示すエラー メッセージを受信しました。

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。

対応策

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　**Device > Phone** を選択します。

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基準を入力します。

検索基準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。

Phone Configuration ウィンドウが表示されます。

ステップ 4　Directory Numbers リストで、更新する回線をクリックします。

Directory Number Configuration ウィンドウが表示されます。

ステップ 5　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　**Update** 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、**Reset Devices** 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　**OK** をクリックして、デバイスを再起動します。

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 CallManager Attendant Console で使用不可になっています。

考えられる原因

パイロット ポイントおよび制御されている電話機のいずれかまたは両方が、ac ユーザの制御デバイス リストに含まれていません。

対応策

次の手順を実行し、ac ユーザを作成して、このユーザをパイロット ポイントおよびアテンダントの電話機に関連付けます。

手順

ステップ 1　**User Management > Application User** を選択します。

Find and List Application Users ウィンドウが表示されます。

ステップ 2　**Add New** をクリックします。

Application User Configuration ウィンドウが表示されます。

ステップ 3　User ID フィールドに、**ac** と入力します。

ステップ 4　Password フィールドに、**12345** と入力します。

ステップ 5　Confirm Password フィールドに、**12345** と入力します。

ステップ 6　**Save** をクリックします。

ステップ 7　**User Management > User Groups** を選択します。

Find and List User Groups ウィンドウが表示されます。

ステップ 8　**Standard CTI Allow Park Monitoring** ユーザ グループのリンクをクリックします。

User Group Configuration ウィンドウが表示されます。

ステップ 9　**Add Application Users to Group** ボタンをクリックします。

Find and List Application Users ウィンドウが表示されます。

ステップ 10　ユーザ名「ac」を検索ボックスに入力し、**Find** をクリックします。

ステップ 11　「ac」ユーザの隣にあるチェックボックスをオンにし、**Add Selected** をクリックします。

ステップ 12　Related Topics ドロップ リスト ボックスの隣にある **Go** ボタンをクリックします。

ステップ 13　**Standard CTI Enabled** ユーザ グループのリンクをクリックします。

ステップ 14　**Add Application Users to Group** ボタンをクリックします。

ステップ 15　ユーザ名「ac」を検索ボックスに入力し、**Find** をクリックします。

ステップ 16　「ac」ユーザの隣にあるチェックボックスをオンにし、**Add Selected** をクリックします。

ステップ 17　デバイスを ac ユーザに関連付けるには、**User Managerment > Application User** を選択し、ac ユーザを見つけます。

ステップ 18　Application User Configuration ウィンドウで、**Find more Phones** ボタンをクリックします。

ステップ 19　ac ユーザに関連付ける電話機を見つけます。

ステップ 20　関連付ける電話機の隣にあるチェックボックスをオンにし、**Add Selected** をクリックします。

ステップ 21　**Find more Pilot Points** ボタンをクリックします。

ステップ 22　ac ユーザに関連付けるパイロット ポイントを見つけます。

ステップ 23　関連付けるパイロット ポイントの隣にあるチェックボックスをオンにし、**Add Selected** をクリックします。

ステップ 24　**Save** をクリックします。

ディレクトリの問題

この項では、Cisco CallManager Attendant Console の次の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。

Directory ウィンドウにユーザが表示されない（P.3-9）

Directory ウィンドウにユーザが表示されない

症状

Cisco CallManager Administration で追加したユーザが、Cisco CallManager Attendant Console の Directory ウィンドウに表示されません。

考えられる原因（その 1）

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。
- Directory Sync Period サービス パラメータの値を Cisco CallManager Administration で変更する。

Cisco CallManager 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。

対応策（その 1）

上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（その 2）

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

対応策（その 2）

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 CallManager Administration から、**User Management > End User** を選択します。

Find and List Users ウィンドウが表示されます。

ステップ 2　User Search フィールドに適切な検索基準を入力し、**Find** をクリックします。

ステップ 3　名前検索の結果リストで、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　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　**Save** をクリックします。

ボイスメールの問題

この項では、Cisco CallManager Attendant Console ボイスメールの次の問題について説明します。

不適切なボイスメール グリーティングが再生される（P.3-10）

不適切なボイスメール グリーティングが再生される

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ールに転送されたとき、ボイスメール 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 サービス パラメータに True が指定されています。

対応策

手順

ステップ 1　**System > Service Parameters** を選択します。

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

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

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

Cisco CallManager Attendant Console インターフェイスを使用する際の問題

この項では、Cisco CallManager Attendant Console インターフェイスの次の問題について説明します。

Cisco CallManager Attendant Console サーバと通信できない

症状　アテンダントがコンソールにログインしようとすると、コンソール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　コンソールのクライアントとコンソールのサーバが、同じドメイン内にありません。

推奨処置　コンソールのクライアントの 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 CallManager 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 CallManager 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 IP Telephony Platform Administration のマニュアルを参照してください。

Unicode 言語で検索できない

症状　Cisco IP Phone のディレクトリおよび Cisco CallManager 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 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 CallManager Administration の 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 CallManager 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。

Speed Dial ウィンドウと Directory ウィンドウで回線状態が正しく表示されない

症状

Speed Dial ウィンドウと Directory 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。

対応策

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 CallManager サーバ上で、Cisco CallManager Attendant Console Server サービスが開始されていません。

対応策

電話機がコール処理サービスを受けるすべての Cisco CallManager サーバ上で、Cisco CallManager Attendant Console Server サービスをアクティブにします。

手順

ステップ 1　Cisco CallManager Serviceability で、**Tools > Service Activation** を選択します。

ステップ 2　Servers ドロップダウン リスト ボックスから、Cisco CallManager Attendant Console Server サービスを開始するサーバを選択します。

選択したサーバのサービス、およびそのサービスのアクティベーション ステータスがウィンドウに表示されます。

ステップ 3　Cisco CallManager Attendant Console Server サービスの隣にあるオプション ボタンをクリックします。

ステップ 4　**Start** ボタンをクリックします。

Service Status のシンボルが、四角形から矢印に変化します。

Cisco CallManager Serviceability が JTAPI ログを生成しない

この項では、Cisco CallManager Attendant Console の次の問題について説明します。

JTAPI ログが生成されない（P.3-13）

JTAPI ログが生成されない

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。

対応策

次の手順を実行し、Cisco CallManager Attendant Console Server サービスを再起動します。

手順

ステップ 1　Cisco CallManager Serviceability で、**Tools > Control Center - Feature Services** を選択します。

ステップ 2　Server ドロップダウン リスト ボックスから、Cisco CallManager Attendant Console Server サービスを再起動するサーバを選択します。

選択したサーバのサービス、およびそのサービスのステータスとアクティベーション ステータスがウィンドウに表示されます。

ステップ 3　Cisco CallManager Attendant Console Server サービスの隣にあるオプション ボタンをクリックします。

ステップ 4　**Restart** ボタンをクリックします。

サーバ ログの収集

この項では、サーバ ログの収集に関する Cisco CallManager Attendant Console の次の問題について説明します。

すべてのサーバ ログを収集する方法（P.3-14）

すべてのサーバ ログを収集する方法

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 CallManager Attendant Console Server
- JTAPI

対応策

次のディレクトリにある **accollectlogs.bat** を実行します。
C:\Program Files\Cisco\CallManagerAttendant\bin ディレクトリ

必須となるオプション パラメータが 3 つあります。

- **-directory <directory_name>**：Cisco CallManager のトレースが存在するディレクトリ
- **-time <n_minutes>**：最近 <n_minutes> 分間のログを収集することを指定
- **-output <zip_file_name>**：出力される ZIP ファイルの名前

CHAPTER 4

Cisco CallManager システムの問題

この章では、Cisco CallManager 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 CallManager システム

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

Cisco CallManager システムが応答を停止する

症状

Cisco CallManager システムが応答しません。

考えられる原因

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 CallManager 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 IP Phone やゲートウェイなどのデバイスが Cisco CallManager 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 CallManager 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 CallManager Event Logs』を参照してください。

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。P.4-3 の「リソース不足」を参照してください。

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

リソース不足によるクラッシュが発生している場合は、次の手順を実行します。

手順

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

ステップ 2　クラッシュの前後 15 分の SDL トレースを収集します。

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

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

Cisco CallManager Administration ページが表示されない

症状

Administration Web 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

次の手順を実行し、ローカル サーバまたはリモート 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します。

1. Cisco CallManager Serviceability で、**Tools > Service Activation** を選択します。
2. Servers 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。

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

   Activated と表示された場合は、選択したサーバ上で Cisco CallManager がアクティブであるため、TAC に問い合せる必要があります。

   Deactivated と表示された場合は、引き続き次のステップを実行します。
3. **Cisco CallManager** チェックボックスをオンにします。
4. **Update** ボタンをクリックします。

   Cisco CallManager 行の Activation Status カラムに **Activated** と表示されます。

   これで、選択したサーバの Cisco CallManager がアクティブになりました。

Cisco CallManager がアクティブであるかどうか、および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。

1. Cisco CallManager Serviceability で、**Tools** > **Control Center - Feature Services** を選択します。
2. Servers 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 CallManager Administration 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 CallManager Administration ページにアクセスしようとすると、次のいずれかのエラー メッセージが表示されます。

- 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。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。

ページを表示する権限がない

症状

Cisco CallManager Administration ページにアクセスすると、次のエラー メッセージが表示されます。

エラー メッセージ `You Are Not Authorized to View This Page`

また、次のようなエラー メッセージが表示されることもあります。

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

考えられる原因

不明

推奨処置

TAC に問い合せてください。

Cisco CallManager Administration ページへのアクセスでエラーが発生する

Cisco CallManager サーバ上で Administration Web ページにローカルではアクセスできても、リモート サーバからはこのページを参照できない場合は、次のいずれかの状況が該当するかどうかを確認してください。最も可能性の高い原因から順に記載しています。

Cisco CallManager でのユーザの表示または追加に関する問題

症状

Cisco CallManager Administration ユーザ 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 CallManager 5.x 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 MS 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 submit をクリックすると、同じページに戻る。
- 新しいユーザを追加しようとすると、次のエラー 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 CallManager 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）、Cisco CallManager Admin ユーザ 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 CallManager Admin ページにアクセスする。
- サーバ名に DNS でサポートされていない文字を使用しない。
- URL に localhost または IP アドレスを使用する。

名前からアドレスへの解決の失敗

症状

次の URL にアクセスしようとすると、次のいずれかのエラー 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 CallManager 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、ページが表示されます。

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

1. 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 CallManager 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。
2. DNS を使用していない場合は、ローカル マシンで「hosts」ファイルを調べて、*your-cm-server-name* のエントリおよびそれに関連付けられている IP アドレスがあるかどうかを確認します。このファイルを開き、Cisco CallManager 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 CallManager 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、次のいずれかのエラー 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 CallManager 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 CallManager 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。

アクセスが明示的に拒否されているマシンにアクセスしようとする

症状

次のいずれかのエラー メッセージが表示されます。

- Internet Explorer：`This page cannot be displayed`
- Netscape：`Not Found.The requested URL / ccmadmin was not found on this server.`
- **show friendly http error messages** 詳細設定が行われていない両方のブラウザから：`Access to this server is forbidden.`

考えられる原因

ネットワーク管理者によって適用されているセキュリティ ポリシーが原因と考えられます。

推奨処置

1. 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。別のマシンから再試行します。
2. 自分がネットワーク管理者である場合は、Cisco CallManager サーバの Internet Service Manager で、**Default Web Site** の **Directory Security** タブを確認します。
3. この設定を確認するには、次のように選択します。
   Start > Programs > Administrative tools/Internet Service Manager
4. サーバ名を示すアイコンを展開します。
5. **Default Web Site** を右クリックします。選択する必要のあるオプションのプロパティが用意されています。
6. **Directory Security** タブを探し、設定を確認します。

リモート マシンに不適切なネットワーク設定が存在する

症状

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

他のリモート マシンから同じアクションを試行すると、Cisco CallManager Administration 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 CallManager 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。
3. 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。
4. **Start > Setting > Network and Dial-up connections** を選択します。
5. **Local Area Connection** を選択し、**Properties** 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。
6. **Internet Protocol (TCP-IP)** を選択し、**Properties** を再度クリックします。
7. ネットワークに応じて、**Obtain an ip address automatically** または **set manually your address, mask and default Gateway** 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。
8. Internet Explorer ブラウザで、**Tools > Internet Options** を選択します。
9. **Connections** 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。

10. Cisco CallManager　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。

設定の詳細については、次の URL を参照してください。

http://www.cisco.com/warp/public/63/initial_config.shtml

パブリッシャとサブスクライバの間で複製が失敗する

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

サブスクライバがパブリッシャからのデータ複製を停止する

症状

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

考えられる原因

パブリッシャとサブスクライバの間で複製が失敗しています。

推奨処置

次の手順を実行し、2 つのシステム間の関係を再確立します。まず、パブリッシャ上でサブスクライバのサブスクリプションを再作成する必要があります。次に、サブスクリプションを削除し、サブスクライバ システム上で再作成します。

1. パブリッシャ上で、サブスクリプションを再作成します。
2. 障害の発生している Cisco CallManager サブスクリプションを選択し、そのエントリを削除します。

   パブリッシャでサブスクリプションが削除されたが、サブスクライバでは削除されていないことを示す警告が表示され、サブスクライバに接続してサブスクリプションを削除するかどうかの確認を求められます。
3. **Yes** をクリックします。

   次に、サブスクリプションは削除されたが、データは削除されていないことを示すメッセージが表示されます。
4. **OK** をクリックします。
5. サブスクライバ上で、サブスクリプションを再作成します。

   サブスクリプションは実行状態で、パブリッシャと再び同期化されています。更新内容は、ローカルのサブスクライバ データベースに記録されます。

サーバの応答が遅い

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

デュプレックス ポート設定の不一致

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が Cisco CallManager 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 CallManager 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 CallManager と通信するコンポーネントで、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 AutoAttendant、Cisco IP ICD、Cisco 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。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す。

トラブルシューティング プロセスを開始する前に、使用しているソフトウェア バージョン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 CallManager のバージョンの Cisco CallManager Release Notes を読んでください。

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、例外の原因が記載されています。

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 ー bad login or password

考えられる原因

JTAPI 設定に入力されているユーザ名またはパスワードが正しくありません。

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 -- 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 CallManager で CCMuser ページ（http://servername/ccmuser）にログインし、Cisco CallManager 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 CallManager への JTAPI 接続が、Cisco CallManager 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 CallManager Control Center 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 ページで、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 ページで、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 CallManager 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 CallManager 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 CallManager 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 CallManager 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 CallManager Plugins ページから 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 CallManager 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 CallManager 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

トレース内のエラー 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かったかが記載されています。このデバイスが Cisco CallManager 設定に存在すること、および Cisco CallManager 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

この項では、次のセキュリティ問題について説明し、セキュリティ プロセスに関する詳細なマニュアルを参照できる場所を示します。

短期的なセキュリティ ソリューション

次のドキュメントを参照して、ネットワーク全体で quality of service（QoS; サービス品質）が正しく設定されていることを確認し、残りのクリーンアップ操作中に音声品質への影響ができるだけ小さくなるようにします。

- *Cisco IP Telephony QoS Design Guide*
- *Cisco IP Telephony Network Design Guide*
- *IP Telephony Solutions Guide*

個別の Voice/Data VLAN を確立する方法については、『*Cisco IP Telephony Network Design Guide*』を参照してください。

（注） 関連するネットワークのサイズや複雑さによっては、短期的なソリューションが長期的なソリューションになることもあります。

関連情報

次の URL では、『*Cisco CallManager Security Patch Process*』が提供されています。

http://www.cisco.com/warp/public/cc/pd/nemnsw/callmn/prodlit/cmspp_qa.pdf

IP テレフォニー ネットワークのセキュリティの考慮事項については、次の URL を参照してください。

http://www.cisco.com/warp/public/779/largeent/it/ese/srnd.html

CHAPTER 5

ディレクトリの問題

Cisco CallManager のこのリリースには、次の特徴があります。

- 組み込み型の DC Directory はありません。
- Active Directory（AD）および Netscape Directory（ND）用のプラグインはありません。
- AD または ND との統合では、お客様のディレクトリに対するスキーマ拡張はありません。
- ユーザ情報は、常に Informix データベースに格納されます。
- シスコの製品は、お客様のディレクトリにはデータを一切格納しません。
- シスコの製品は、お客様のディレクトリに到達不能な場合でも完全に機能します。
- ユーザ情報は、標準の LDAP コネクタ（Cisco DirSync）を使用してデータベースに入力されます。
- 製品は常にユーザ情報のデータベースにアクセスし、お客様のディレクトリには一切アクセスしません。

アラームは、イベント ログ（Syslog）および SNMP トラップに配信されます。ログ ファイルを表示および収集するには、RTMT を使用します。

関連情報

ディレクトリのインストールと設定については、次の URL にアクセスしてください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/5_0/sys_ad/5_0_1/ccmsys/a04direc.htm

関連情報

CHAPTER 6

デバイスの問題

この章では、Cisco 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

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、音声が途切れる（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」
- 「Cisco IP Phone による音声問題の解決」
- 「エコー」
- 「単方向音声または無音声」

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」などと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。最適的な状況では、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。このデジッタリングは、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 IP Phone 7960 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ます。つまり、一度に大量のパケットが受信された場合、Cisco IP Phone 7960 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る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、無音があ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 CallManager Administration でこのサービスを無効にし、**Service > Service Parameters** 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 CallManager　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 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。下記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）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 CallManager Serviceability アドミニストレーション ガイド*』を参照してください。

Cisco 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 コールの数が多すぎて 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 IP Phone 7960 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。

1. アクティブ コールに対して、*i* ボタンをすばやく 2 回押すと、電話機の情報画面に、パケットの送受信に関する統計情報、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） この画面で、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。

2. 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のであれば、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 CallManager Administration 設定の **Locations** 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 ノイズの診断

3. 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気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。

ロードの確認

4. ゲートウェイと電話機のロードを確認します。www.cisco.com の Cisco Connection Online（CCO）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。

確認

1. 「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が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。この事実は、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重要である理由の 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 の Cisco Connection Online 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 Gateway、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 ルーティングの確認

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。

次の点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 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 IP Phone 7910：**Settings** を押し、オプション 6 を選択してから、Default Router 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 IP Phone 7960/40：**Settings** を押し、オプション 3 を選択してから、Default Router 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 IP Phone 2sp+/30vip：****#** を押してから、gtwy= が表示されるまで **#** を押します。

（注） Cisco IP SoftPhone アプリケーションを使用していて、複数の Network Interface Card（NIC; ネットワーク インターフェイス カード）がボックスにインストールされている場合は、ボックスに正しい NIC が設定されていることを確認してください。この問題は、Cisco IP SoftPhone ソフトウェア バージョン 1.1.x に共通する問題です（バージョン 1.2 では解決します）。

（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るものです。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 1 つの IP アドレスから調達され、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 address>** です。Cisco CallManager 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 Cisco IOS Release 12.1.2T で導入され、『*Configuring H.323 Support for Virtual Interfaces*』で文書化されています。

（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てい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。回避方法は、**voice rtp send-recv on** を設定することです。

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、ト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ので、IP リンクの両端で cRTP を有効にする必要があります。

リンクの両端で cRTP が期待どおりに機能していることを確認することも重要です。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）スイッチング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 です。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 CallManager 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<number>** 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 です。

（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、この文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、論理チャネルの再定義を考慮して、音声が新しい 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 IP Phone 7900 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。

解決策は、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ことです。

確認

パケット フローを確認するには、コマンド **debug cch323 rtp** が便利です。このコマンドは、ルータが送信したパケット（X）と受信したパケット（R）を表示します。大文字は正常な送信または受信を示し、小文字はドロップされたパケットを示します。次の例を参照してください。

```
voice-ios-gwy#debug cch323 rtp
RTP packet tracing is enabled
voice-ios-gwy#
voice-ios-gwy#
voice-ios-gwy#
voice-ios-gwy#
voice-ios-gwy#

!--- This is an unanswered outgoing call.
!--- Notice that voice path only cuts through in forward
!--- direction and that packets are dropped. Indeed,
!--- received packets are traffic from the IP phone to the PSTN
!--- phone. These will be dropped until the call is answered.

Mar 3 23:46:23.690: ****** cut through in FORWARD direction *****
XXXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr
XrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr
XrXrXXrrrrrrrrrrrrrrrr
voice-ios-gwy#
voice-ios-gwy#

!--- This is an example of an answered call:

voice-ios-gwy#
voice-ios-gwy#
*Mar 3 23:53:26.570: ****** cut through in FORWARD direction *****
XXXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr
XrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr
XXrrrrrXrXrXrXrXrXrXrXrXrXrXrXrrXXrrXrXrXrXrXrXXXXXXXXXXXXXXXXXrXXXXXXXXrXrXrXXrrXr
XrXrXrXrXrXrXrXrXXrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr

!-- At this point the remote end picks up the phone.

*Mar 3 23:53:30.378: ****** cut through in BOTH direction *****
```

```
XRXRXRXRXRXRXRXRXXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRXRXRXRXRXR
XXRRRXRXRXXRRXRXRXRXRXXRXRXRXRXRXRRXRXXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRRRRRRRRRRRRRRRRRRRRRRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXXRRRRRRRRRRRRRRRRRRRRRRRRRRXRXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
R
RRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXXRXRXRXRXRXRRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXXRRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XXRRRRRRRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXXRRRRXR

!-- End of conversation.
```

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、トランスコーダー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 IP Phone 7960：G.711A-law/μ-law、G.729、G729A、G.729Annex-B
Cisco 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 CallManager の帯域割り当てが超過していることが原因である可能性があります。Cisco CallManager 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 CallManager 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 CallManager|Locations:Orig=1 BW=12Dest=0 BW=-1(-1 implies infinite
bw available)
12:42:09.017 Cisco CallManager|StationD - stationOutputCallState tcpHandle=0x4f1ad98
12:42:09.017 Cisco CallManager|StationD - stationOutputCallInfo CallingPartyName=,
CallingParty=5003, CalledPartyName=, CalledParty=5005, tcpHandle=0x4f1ad98
12:42:09.017 Cisco CallManager|StationD - stationOutputStartTone: 37=ReorderTone
tcpHandle=0x4f1ad98
```

コールが確立されると、Cisco CallManager 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 CallManager 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 CallManager は 24k を差し引きます。
- コールで G0.729 が使用されている場合、Cisco CallManager 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

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 CallManager 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 の Cisco Connection Online 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 Event Viewer で確認します。電話機のリセットは Information 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 IP Phone 7960 または Cisco IP Phone 30VIP 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 Sniffer 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（「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 Event Viewer で確認します。

   リセットが発生する電話機ごとに、Warning メッセージと Error 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 CallManager への TCP 接続を維持できないために、Cisco CallManager 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、Microsoft Performance を使用して電話機登録を記録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、Call Detail Record（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 CallManager Serviceability アドミニストレーション ガイド*』を参照してください。
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 CallManager 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 CallManager のパフォーマンスに影響を与える可能性があるので、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。

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 の Cisco Connection Online 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 CallManager 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ある可能性があります。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 CallManager 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 ソフトウェアは稼働していません。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ます。したがって、確認したときデバイスがたまたまリ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、Sniffer トレース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。

    tracy_start *mod port*

この例では、WS-X6624 はモジュール 7 に相当し、1 個の 860 プロセッサしか持っていないのでポート 1 です。コマンド **tracy_start 7 1** を発行します。

ゲートウェイ ボード自体の 860 コンソール ポートから実際に出力される結果を次に示します。ただし、tracy コマンドの出力は、860 コンソール ポートの単なるリモート コピーです。

```
      |             |
      |             |
    | | |         | | |
   | | | | |     | | | | |
| | | | | |:.:| | | | | |:..
C i s c o   S y s t e m s
CAT6K Analog Gateway (ELVIS)
APP Version : A0020300, DSP Version : A0030300, Built Jun  1 2000 16:33:01

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
00:00:02.870 (CFG) Starting DHCP
00:00:02.870 (CFG) Booting DHCP for dynamic configuration.
00:00:06.570 (CFG) DHCP Request or Discovery Sent, DHCPState = INIT_REBOOT
00:00:06.570 (CFG) DHCP Server Response Processed, DHCPState = INIT_REBOOT
00:00:06.780 (CFG) IP Configuration Change!  Restarting now...
00:00:10.480 (CFG) DHCP Request or Discovery Sent, DHCPState = INIT
00:00:14:480 (CFG) DHCP Timeout Waiting on Server, DHCPState = INIT
00:00:22:480 (CFG) DHCP Timeout Waiting on Server, DHCPState = INIT
00:00:38:480 (CFG) DHCP Timeout Waiting on Server, DHCPState = INIT
```

このタイムアウト メッセージがスクロールし続ける場合は、DHCP サーバへの接続に問題があります。

11. まず、Catalyst 6000 ゲートウェイ ポートが正しい VLAN 上にあることを確認します。

    この情報は、**show port** コマンドを使用して取得した情報に含まれています。

12. DHCP サーバが Catalyst 6000 ゲートウェイと同じ VLAN 上にない場合は、DHCP 要求を DHCP サーバに転送するように適切な IP ヘルパー アドレスが設定されていることを確認します。VLAN 番号が変わった後に、ゲートウェイは、リセットされるまで INIT 状態のままになっていることがあります。

13. INIT 状態になっている場合は、ゲートウェイをリセットします。860 をリセットするたびに tracy セッションは失われるので、次のコマンドを発行して既存のセッションを閉じ、新しいセッションを再度確立する必要があります。

    tracy_close *mod port*

    tracy_start *mod port*

14. それでも `DHCPState = INIT` メッセージが表示される場合は、DHCP サーバが正常に機能しているかどうかを確認します。

15. 正常に機能している場合は、Sniffer トレースを開始して、要求が送信されているかどうか、およびサーバが応答しているかどうかを確認します。

    DHCP が正常に機能している場合、tracy デバッグ ユーティリティの使用を可能にする IP アドレスがゲートウェイに設定されています。このユーティリティには、Catalyst ゲートウェイ用の NMP コマンド セットの組み込み機能が含まれており、Windows 98/NT/2000 上でスタンドアロン ゲートウェイ用のヘルパー アプリケーションとして使用可能です。

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 CallManager 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 CallManager 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 CallManager 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 CallManager の TFTP トレースを確認します。

ゲートウェイが Cisco CallManager 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 GMSG: GWEvent = CFG_DONE --> GWState = SrchActive
00:00:05.610 GMSG: CCM#0 CPEvent = CONNECT_REQ --> CPState = AttemptingSocket
00:00:05.610 GMSG: Attempting TCP socket with CCM 10.123.9.2
00:00:05.610 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = BackupCCM
00:00:05.610 GMSG: GWEvent = SOCKET_ACK --> GWState = RegActive
00:00:05.610 GMSG: CCM#0 CPEvent = REGISTER_REQ --> CPState = SentRegister
00:00:05.680 GMSG: CCM#0 CPEvent = CLOSED --> CPState = NoTCPSocket
00:00:05.680 GMSG: GWEvent = DISCONNECT --> GWState = Rollover
00:00:20.600 GMSG: GWEvent = TIMEOUT --> GWState = SrchActive
00:00:20.600 GMSG: CCM#0 CPEvent = CONNECT_REQ --> CPState = AttemptingSocket
00:00:20.600 GMSG: Attempting TCP socket with CCM 10.123.9.2
00:00:20.600 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = BackupCCM
```

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 GMSG: CCM#0 CPEvent = REGISTER_REQ --> CPState = SentRegister
00:00:08.010 GMSG: TFTP Request for application load A0021300
00:00:08.010 GMSG: CCM#0 CPEvent = LOADID --> CPState = AppLoadRequest
00:00:08.010 GMSG: ***TFTP Error: File Not Found***
00:00:08.010 GMSG: 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 GMSG: GWEvent = CFG_DONE --> GWState = SrchActive
00:00:05.730 GMSG: CCM#0 CPEvent = CONNECT_REQ --> CPState = AttemptingSocket
00:00:05.730 GMSG: Attempting TCP socket with CCM 10.123.9.2
00:00:05.730 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = BackupCCM
00:00:05.730 GMSG: GWEvent = SOCKET_ACK --> GWState = RegActive
00:00:05.730 GMSG: CCM#0 CPEvent = REGISTER_REQ --> CPState = SentRegister
00:00:06.320 GMSG: CCM#0 CPEvent = LOADID --> CPState = LoadResponse
00:01:36.300 GMSG: CCM#0 CPEvent = TIMEOUT --> CPState = BadCCM
00:01:36.300 GMSG: GWEvent = DISCONNECT --> GWState = Rollover
00:01:46.870 GMSG: CCM#0 CPEvent = CLOSED --> CPState = NoTCPSocket
00:01:51.300 GMSG: GWEvent = TIMEOUT --> GWState = SrchActive
00:01:51.300 GMSG: CCM#0 CPEvent = CONNECT_REQ --> CPState = AttemptingSocket
00:01:51.300 GMSG: Attempting TCP socket with CCM 10.123.9.2
00:01:51.300 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = BackupCCM
00:01:51.300 GMSG: GWEvent = SOCKET_ACK --> GWState = RegActive
00:01:51.300 GMSG: CCM#0 CPEvent = REGISTER_REQ --> CPState = SentRegister
00:01:51.890 GMSG: CCM#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 CallManager Administration の Device Defaults エリアでロード 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。

- 「クラスタ間トランクまたは H.225 トランク」
- 「アドミッション拒否」
- 「登録拒否」

クラスタ間トランクまたは H.225 トランク

次の場所で、『*Cisco CallManager アドミニストレーション ガイド*』および『*Cisco CallManager システム ガイド*』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/index.htm

アドミッション拒否

症状

Admission Reject（ARJ; アドミッション拒否）が発行されるのは、Cisco CallManager 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です。

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 CallManager 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 CallManager のサブネットが含まれていることを確認します。
4. Cisco CallManager 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

Registration Reject（RRJ; 登録拒否）が発行されるのは、Cisco CallManager がゲートキーパーに登録できない場合です。

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 CallManager 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 チャネルがロックされたままになる

症状

Cisco CallManager 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、再起動する必要のあるチャ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ネルを要求することになります。

チャネルは Cisco CallManager サーバ上でロックされているので、Cisco CallManager はこのチャ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

ルート パーティションは、Cisco CallManager 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 CallManager アドミニストレーション ガイド*』および『*Cisco CallManager 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 Cisco CallManager|StationInit - InboundStim - OffHookMessageID
tcpHandle=0x6b88028
08:38:54.968 Cisco CallManager|StationD - stationOutputDisplayText
tcpHandle=0x6b88028, Display= 5000
08:38:54.968 Cisco CallManager|StationD - stationOutputSetLamp stim: 9=Line instance=1
lampMode=LampOn tcpHandle=0x6b88028
08:38:54.968 Cisco CallManager|StationD - stationOutputCallState tcpHandle=0x6b88028
08:38:54.968 Cisco CallManager|StationD - stationOutputDisplayPromptStatus
tcpHandle=0x6b88028
08:38:54.968 Cisco CallManager|StationD - stationOutputSelectSoftKeys
tcpHandle=0x6b88028
08:38:54.968 Cisco CallManager|StationD - stationOutputActivateCallPlane
tcpHandle=0x6b88028
08:38:54.968 Cisco 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 Cisco CallManager|Digit analysis: potentialMatches=PotentialMatchesExist
08:38:54.968 Cisco CallManager|StationD - stationOutputStartTone: 33=InsideDialTone
tcpHandle=0x6b88028
08:38:55.671 Cisco CallManager|StationInit - InboundStim - KeypadButtonMessageID
kpButton: 5 tcpHandle=0x6b88028
08:38:55.671 Cisco CallManager|StationD - stationOutputStopTone tcpHandle=0x6b88028
08:38:55.671 Cisco CallManager|StationD - stationOutputSelectSoftKeys
tcpHandle=0x6b88028
08:38:55.671 Cisco CallManager|Digit analysis: match(fqcn="5000", cn="5000",
pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="5")
08:38:55.671 Cisco CallManager|Digit analysis: potentialMatches=PotentialMatchesExist
08:38:56.015 Cisco CallManager|StationInit - InboundStim - KeypadButtonMessageID
kpButton: 0 tcpHandle=0x6b88028
08:38:56.015 Cisco CallManager|Digit analysis: match(fqcn="5000", cn="5000",
pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="50")
08:38:56.015 Cisco CallManager|Digit analysis: potentialMatches=PotentialMatchesExist
08:38:56.187 Cisco CallManager|StationInit - InboundStim - KeypadButtonMessageID
kpButton: 0 tcpHandle=0x6b88028
08:38:56.187 Cisco CallManager|Digit analysis: match(fqcn="5000", cn="5000",
pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="500")
08:38:56.187 Cisco CallManager|Digit analysis: potentialMatches=PotentialMatchesExist
08:38:56.515 Cisco CallManager|StationInit - InboundStim - KeypadButtonMessageID
kpButton: 3 tcpHandle=0x6b88028
08:38:56.515 Cisco CallManager|Digit analysis: match(fqcn="5000", cn="5000",
pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="5003")
08:38:56.515 Cisco CallManager|Digit analysis: analysis results
08:38:56.515 Cisco 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特に注意してください。

次のトレースは、Cisco CallManager 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特に

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 Cisco CallManager|StationInit - InboundStim - OffHookMessageID
tcpHandle=0x6b88028
08:38:58.734 Cisco CallManager|StationD - stationOutputDisplayText
tcpHandle=0x6b88028, Display= 5000
08:38:58.734 Cisco CallManager|StationD - stationOutputSetLamp stim: 9=Line instance=1
lampMode=LampOn tcpHandle=0x6b88028
08:38:58.734 Cisco CallManager|StationD - stationOutputCallState tcpHandle=0x6b88028
08:38:58.734 Cisco CallManager|StationD - stationOutputDisplayPromptStatus
tcpHandle=0x6b88028
08:38:58.734 Cisco CallManager|StationD - stationOutputSelectSoftKeys
tcpHandle=0x6b88028
08:38:58.734 Cisco CallManager|StationD - stationOutputActivateCallPlane
tcpHandle=0x6b88028
08:38:58.734 Cisco CallManager|Digit analysis: match(fqcn="5000", cn="5000",
pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="")
08:38:58.734 Cisco CallManager|Digit analysis: potentialMatches=PotentialMatchesExist
08:38:58.734 Cisco CallManager|StationD - stationOutputStartTone: 33=InsideDialTone
tcpHandle=0x6b88028
08:38:59.703 Cisco CallManager|StationInit - InboundStim - KeypadButtonMessageID
kpButton: 1 tcpHandle=0x6b88028
08:38:59.703 Cisco CallManager|StationD - stationOutputStopTone tcpHandle=0x6b88028
08:38:59.703 Cisco CallManager|StationD - stationOutputSelectSoftKeys
tcpHandle=0x6b88028
08:38:59.703 Cisco CallManager|Digit analysis: match(fqcn="5000", cn="5000",
pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="1")
08:38:59.703 Cisco CallManager|Digit analysis:
potentialMatches=NoPotentialMatchesExist
08:38:59.703 Cisco 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 Domain Name（DN; ドメイン名）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。

a. 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。

b. DN 6000 および 7000 の設定ページで、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

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 CallManager に知らせます。ダイヤル プランは、ルータのスタティック ルーティング テーブルに似ています。

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 CallManager 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、どのデバイスでコーリング サーチ スペースがこの DN に関連付けられているかを識別します。必ず正しいデバイスを識別してください。複数回線の着信表示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 スペースに注意してください。

   コールの発信元が Cisco 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 IP Phone がコーリング サーチ スペース AccessLevelY を持つ場合、その回線からコールを発信すると、Cisco CallManager 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. ダイヤ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に注意します。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 CallManager Administration で Route Plan Report 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に注意します。
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 CallManager 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 CallManager 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考えられます。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 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 CallManager 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でけではなく、問題が悪化する可能性が非常に高くなります。

CHAPTER 8

Cisco CallManager サービスの問題

この章では、Cisco CallManager 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 Conference Bridge がない

エラー メッセージ `No Conference Bridge Available`

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 CallManager 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 Conference Bridge リソースがあるかどうかを確認します。
2. Microsoft Performance または Admin Serviceability Tool のいずれかを使用して、Unicast AvailableConferences の数を確認します。

（注） Cisco CallManager Release 3.1 では、カウンタとオブジェクトに対して異なる名前が使用されています。詳細については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』を参照してください。

Cisco IP Voice Media Streaming アプリケーションは、Conference Bridge 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 CallManager 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/3_1/index.htm で、Release 3.1 のマニュアルを参照してください。

```
10:59:29.951 Cisco CallManager|UnicastBridgeControl -
wait_capabilities_StationCapRes - Device= CFB_kirribilli - Registered -
ConfBridges= 16, Streams= 48, tcpHandle=4f12738
10:59:29.951 Cisco 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 Cisco CallManager|UnicastBridgeControl -
wait_capabilities_StationCapRes - Device= CFB00107B000FB0 - Registered -
ConfBridges= 5, Streams= 16, tcpHandle=4f19d64
11:14:05.480 Cisco CallManager|UnicastBridgeManager -
UnicastBridgeRegistrationReq - Device Registration Complete for Name= Xoð ô%ð
- DeviceType= 51, ResourcesAvailable= 5, deviceTblIndex= 0
```

Cisco Catalyst 6000 8 Port Voice T1/E1 および Services Module の次のハードウェア トレースは、カードの E1 ポート 4/1 が Conference Bridge として Cisco CallManager 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
```

3. 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。

ハードウェア トランスコーダー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 トランスコーダー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 CallManager に登録された使用可能なトランスコーダー 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

Microsoft Performance または Admin Serviceability Tool のいずれかを使用して、使用可能な MediaTermPointsAvailable の数を確認します。

（注） Cisco CallManager Release 3.1 では、カウンタとオブジェクトに対して異なる名前が使用されています。詳細については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』を参照してください。

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ー /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 CallManager 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/3_1/index.htm で、Release 3.1 のマニュアルを参照してください。

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

Cisco Catalyst 6000 8 Port Voice T1/E1 および Services Module の次のハードウェア トレースは、カードの E1 ポート 4/2 が MTP/ トランスコーダーとして Cisco CallManager 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)　Conference Bridge と Transcoder/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、トランスコーダー 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 CallManager 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。

- Phone A で発信者がコールを開始すると、Cisco CallManager はその電話機が Cisco IP Phone 7960 であり、G.729 をサポートしていると認識します。番号が収集された後に、Cisco CallManager 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ので、コールが確立され、音声が Phone A と Phone D 間を直接流れます。
- Cisco IP Phone 12SP+ 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 CallManager 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 とトランスコーダー間は G.711 として、Phone D とトランスコーダー間は G.729 として、それぞれ音声が流れるように、Cisco CallManager 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ーがない場合、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 IP Phone 12SP+ 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 CallManager 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. Microsoft Performance または Admin Serviceability Tool のいずれかを使用して、MediaTermPointsAvailable の数を確認します。

（注） Cisco CallManager Release 3.1 では、カウンタとオブジェクトに対して異なる名前が使用されています。詳細については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』を参照してください。

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 CallManager 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/3_1/index.htm で、Release 3.1 のマニュアルを参照してください。

```
10:12:19.161 Cisco 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 Cisco CallManager|MediaTerminationPointControl - Capabilities
Received - Device= MTP00107B000FB1 - Registered - Supports 16 calls
```

Cisco Catalyst 6000 8 Port Voice T1/E1 および Services Module の次のハードウェア トレースは、カードの E1 ポート 4/2 が MTP/ トランスコーダーとして Cisco CallManager 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 CallManager Administration の Gateway Configuration 画面で、**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 CallManager 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。

■ 確立されたコールで補助的なサービスが使用できない

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。

ボイス メッセージ

Cisco Unity ボイス メッセージに関する広範なトラブルユ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/univercd/cc/td/doc/product/voice/c_unity/unity31/tsg/tsg314/index.htm

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/univercd/cc/td/doc/product/voice/index.htm

Cisco Unity の日本語版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/japanese/warp/public/3/jp/service/manual_j/index_uc_cu_shtml

30 秒経過するとボイス メッセージが停止する

症状

Cisco CallManager と連動して Cisco Unity 3.x 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 CallManager トレースを有効にします。

Cisco Unity 3.x 以降で Skinny トレースを設定する方法の詳細については、次の URL で『*Configuring Unity Traces with MaestroTools.exe*』を参照してください。
http://www.cisco.com/warp/public/788/AVVID/unity_trace_maestrotools.html

Cisco Unity 3.1 以降は、MaestroTools に代わって Cisco Unity Diagnostic Tool が採用されています。このツールの使用方法の詳細については、次の URL で「Cisco Unity Diagnostic Tool」を参照してください。
http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity31/tsg/tsg31/tsg_0900.htm#xtocid13

Unity の問題

この項では、次のトピックについて取り上げます。

Unity がロール オーバーせずにビジー音が聞こえる

症状

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

Messaging Interface が 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 が設定されていないことを確認します。

ボイス メッセージに転送されたコールが Unity に対する直接コールとして処理される

症状

Unity のバージョンは 2.4.5.135、TSP は 6.0(1)、Cisco CallManager は 3.1(31)spD です。

ある IP Phone から別の IP Phone へのコールがボイス メッセージに転送されると、そのコールは発信側の電話機から 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、Redial ソフトキーが押された場合には正しく機能します（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 CallManager を使用するフェールオーバー Unity システムのための動作です。

推奨処置

1. Cisco CallManager サーバで、Cisco Voice Mail ポートの Display 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 サブスクライ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 サブスクライバに関連付けられていないというエラーが表示されます。

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:\commserver\grantunityaccess.exe** にあります。

   （注） GrantUnityAccess ユーティリティの詳細については、次の URL で、「*Granting Administrative Rights to Other Cisco Unity Servers*」を参照してください。
   http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity31/sag/sag312/sag_0255.htm#xtocid8

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。

Cisco Unity 3.1.2 または 3.1.3 の録音メッセージにノイズがある

症状

この問題が発生するのは、Automatic Gain Control（AGC）のレジストリ設定値が誤っている場合だけです。一般に、誤った値には次のものがあります。

- AGCsamplesize が 16 進数 4e20（10 進数 20000）になっている。16 進数 1f40（10 進数 8000）にする必要があります。
- AGCgainthreshold が 16 進数 28（10 進数 40）になっている。16 進数 5（10 進数 5）にする必要があります。

考えられる原因

Cisco Unity 3.1.2 サーバの場合、AGC レジストリ設定が誤った値に設定されていることがあります。また、Cisco Unity 3.1.3 にアップグレードされたサーバの場合も、その可能性があります。これらの誤った設定が原因で、大きなホワイト ノイズが次の位置で発生する可能性があります。

- メッセージの冒頭
- メッセージの途中（メッセージの録音中にユーザが話すのを中断したとき）
- メッセージの末尾

推奨処置　対応策

レジストリ設定を正しい値に変更することで問題は解消します。詳細については、次の URL で Cisco Unity 製品のマニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/index.htm

TAC への問い合せ

Cisco Technical Assistance Center（TAC）は、シスコのお客様、パートナー、および代理店に対してテクニカル サポート サービスを提供します。お客様のニーズに十分にお応えするために、TAC では次の 2 タイプのサポートを用意しています。

- Cisco TAC Web サイト（www.cisco.com/tac）でのオンライン サポート
- TAC Escalation Center による電子メールおよび電話でのサポート

TAC からの支援が必要になった場合は、次の 3 つの方法で TAC にお問い合せいただけます。

1. **Web による連絡**

   TAC Service Request Tool を使用すると、TAC へのお問い合せプロセスが自動化されます。Service Request Tool は、http://tools.cisco.com/ServiceRequestTool/create/launch.do でいつでも入手することができます。

   TAC Service Request Tool は、お問い合せプロセスの中で、解決方法を自動的に提案します。このため、実際にお問い合せいただく前に問題を解決できることがあります。お問い合せが必要となる場合、TAC Service Request Tool は自身のステータスをチェックし、アップデートを追加することができます。

   Technical Documentation & Support Web サイト（各種ツールや TAC エンジニアが作成した技術文書を豊富に収集したサイト）を使用して、一般的な問題を分析し、解決方法を見つけることもできます。次の URL からアクセスできます。http://www.cisco.com/en/US/support/index.html

2. **電子メールによる連絡**

   お問い合せは、電子メールで行っていただくこともできます。メッセージの送付先は tac@cisco.com です。

3. **電話による連絡**

   TAC にご連絡いただく場合の電話番号は、お客様の所在地に応じて異なります。現在の番号を次に示します。

地域	電話番号
アジア太平洋	+61 2 8448 7107
北米	1 800 553 2447
ヨーロッパ、中東、アフリカ	+32 2 704 5555

最寄り地域の電話番号があるかどうかについては、TAC の Web サイトもご確認ください。

（注） Web および電子メールでのお問い合せは、デフォルトでは自動的にプライオリティ 3 または 4 の案件になります。
プライオリティ 1 または 2 の案件については、GCC に電話でお問い合せください。

必要な情報

Cisco TAC へのお問い合せに際しては、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
- TAC Web
- CCO の利用
- 添付ファイル
- Cisco Live!
- リモート アクセス

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

物理的な構成と論理な構成に関する詳細な説明、および音声ネットワークに関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 CallManager
  - バージョン（Cisco CallManager Administration で **Details** を選択して確認します）
  - Cisco CallManager の数
  - 構成（スタンドアロン、クラスタ）
- Unity
  - バージョン（Cisco CallManager Administration 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 CallManager ロード（Skinny ゲートウェイ）
- スイッチ
  - OS バージョン
  - VLAN 設定
- ダイヤル 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レールしているか。
- 古いバージョンの Cisco CallManager 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、それは通常の状況か、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）。

TAC Web

TAC Web（各種ツールや TAC エンジニアが作成した技術文書を豊富に収集したサイト）は、一般的な問題を分析し、解決方法を見いだすために使用します。TAC Web ツールとその使用方法を説明するコンテンツについては、次の URL を参照してください。

http://www.cisco.com/public/support/tac/home.shtml

CCO の利用

CCO を利用した問い合せは、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、その問い合せ内容を TAC エンジニアに送信するプロセスに進みます。

添付ファイル

問い合せ内容に添付するレポートは、電子メールでエンジニアに送信します。100 KB よりも大きい文書の場合は zip ファイルを添付します。

次の URL で、*Manage a TAC Case* セクションを使用してください。*please login* リンクを使用して、登録ユーザとしてログインします。

http://www.cisco.com/public/support/tac/contact.shtml

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 CallManager 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 CallManager 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。

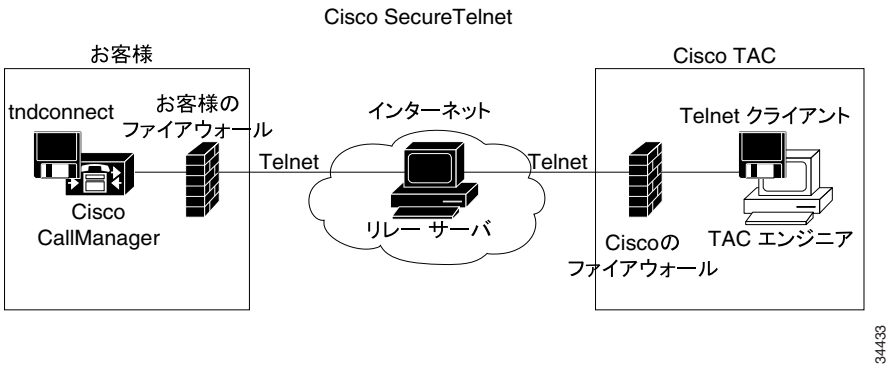
通常、企業ネットワークはパブリック インターネットとの通信を許可します。ただし、外部ホストへの接続がファイアウォールの内側で開始された場合に限ります。

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 CallManager 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 CallManager 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 デーモンに接続します。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　接続が安定すると、CSE　はすべてのリモート　サービサビリティ機能を使用して、Cisco CallManager 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 CallManager 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。

その他の情報

詳細については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』を参照してください。

ケース スタディ：Cisco 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 IP Phone コールのトラブルシューティング
- クラスタ間 Cisco IP Phone コールのトラブルシューティング

クラスタ内 Cisco IP Phone コールのトラブルシューティング

この付録のケース 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 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 CallManager と Cisco 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に続きます。各プロセスの説明は、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て行われています。

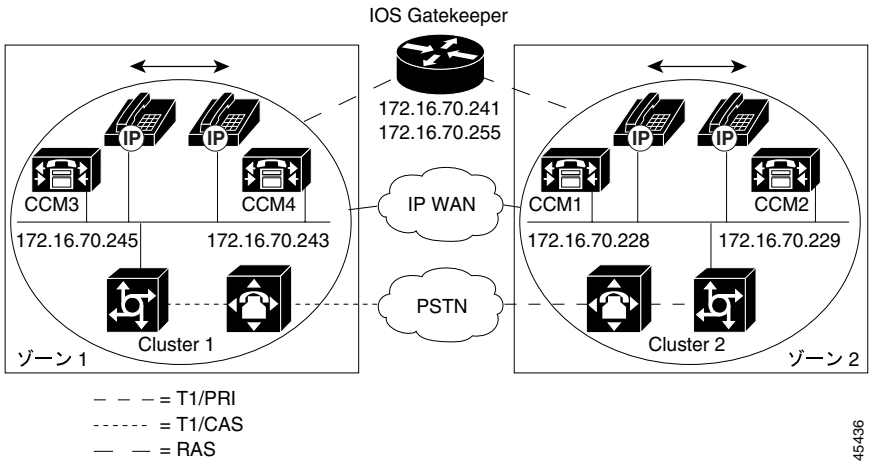
この章では、次のトピックについて取り上げます。

トポロジの例

Cluster 1 および Cluster 2 という 2 つのクラスタがあり、Cluster 1 には CCM3 および CCM4 という 2 つの Cisco CallManager 、Cluster 2 には CCM1 および CCM2 という 2 つの Cisco CallManager があると仮定します。

このケース スタディのトレースは、Cluster 2 にある CCM1 から収集されたものです（図 B-1 を参照）。コール フローのベースは、Cluster 2 にある 2 台の Cisco IP Phone です。これら 2 台の Cisco IP Phone の IP アドレスは、それぞれ、172.16.70.230（電話番号 1000）、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 IP Phone の初期化プロセス

Cisco 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 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　TFTP サーバ名が DHCP 応答に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_address>.cnf という名前が付いています。この電話機を初めて Cisco CallManager に登録する場合は、デフォルト ファイルの SEPdefault.cnf が Cisco 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 IP Phone は IP アドレス 172.16.70.230（MAC アドレスは SEP0010EB001720）、2 台目の Cisco 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 CallManager の IP アドレスが含まれています。Cisco IP Phone は、この IP アドレスを使用してプライマリ Cisco CallManager に接続して登録します。

ステップ 6　Cisco IP Phone が Cisco CallManager に接続して登録すると、Cisco CallManager は、使用する実行ファイルのバージョン（ロード ID と呼ばれます）をその Cisco IP Phone に通知します。指定されたバージョンが Cisco 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 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 CallManager の初期化プロセス

この項では、CCM1（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 CallManager 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 CallManager 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 CallManager 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 CallManager SDI トレース ユーティリティから出力され、Cisco CallManager の 1 つ（このケース スタディでは CCM1）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 CallManager 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 CallManager 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ャ 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 CallManager 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 CallManager が 2 つ目の Cisco CallManager（CCM2（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 CallManager が起動し、Cisco CallManager 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 - CallManagerState Changed - Initialization Started.
16:02:47.796 CCM|NodeId:  0, EventId: 107 EventClass: 3 EventInfo: Cisco CM Database
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 CallManager 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 CallManager 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 CallManager 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 CCM3 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 CCM3 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 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 CallManager 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 CallManager 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 CallManager 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 CallManager を取得します。その Cisco CallManager は、H.323 Gateway としてこの Cisco CallManager 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 CallManager 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 CallManager 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 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 CallManager 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（CCM1 上の MTP サービス）および CFB_nsa-cm1（CCM1 上の Conference Bridge サービス）です。これらは Cisco CallManager 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=0x4fbaa00, 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=0x4fbaa00, 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 CallManager 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 CallManager は、それらの相互間の通信チャ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 CallManager 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 KeepAlive シーケンスを開始します。次のメッセージは、Cisco CallManager 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 CallManager 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 KeepAlive シーケンスを表しています。これらのメッセージも、Cisco CallManager 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 CallManager 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 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 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 IP Phone（dn：1000、tcpHandle：0x4fbb150、IP アドレス：172.16.70.230）にコールを発信しています。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。デバイスをリブ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 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 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。下記の情報は、Cisco IP Phone と Cisco CallManager 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 CallManager から Cisco 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 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 CallManager 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 CallManager 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 IP Phone に表示します。

```
16:05:41.625 CCM|StationD - stationOutputDisplayPromptStatus tcpHandle=0x4fbbc30
```

Cisco CallManager 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 CallManager 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
```

次のメッセージでは、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 CallManager が StationD メッセージを送信した後に、Cisco CallManager 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 CallManager が発信側の Cisco 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 CallManager は着信メッセージを検出し、Cisco 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 CallManager 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 CallManager 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 CallManager 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 CallManager が、着信側の Cisco 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
```

次のトレースは、Cisco CallManager 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 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 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 CallManager が発信側の Cisco 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 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 CallManager がアラート音または呼び出し音を発信側の Cisco 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 IP Phone はオフフックになるので、Cisco CallManager は発信側で呼び出し音を鳴らすのを停止します。

```
16:05:45.140 CCM|StationD - stationOutputStopTone tcpHandle=0x4fbbc30
```

次のメッセージでは、Cisco CallManager 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 CallManager 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 ミリ秒に設定されています。

```
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 CallManager 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 CallManager 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す。また、着信側の IP アドレスも受信します。このメッセージにより、Skinny Station に関する 2 種類の情報が Cisco CallManager 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 CallManager は、次のメッセージを使用して、指定のリモート Cisco 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):   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::>

16:03:25.375 CCM|StationInit: TCPPid=[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):   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>
```

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ています。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 CallManager 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 IP Phone コールのトラブルシューティング

この付録のケース スタディでは、異なるクラスタに配置された別の Cisco IP Phone にコールを発信する Cisco IP Phone について説明します。このタイプのコールは、クラスタ間 Cisco IP Phone コールとも呼ばれます。

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

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 CallManager があります。また、Cisco IOS Gateways 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 IP Phone にコールを発信します。クラスタ間 Cisco CallManager 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 IP Phone は Skinny Station プロトコルを使用して Cisco CallManager に接続でき、Cisco CallManager 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ると、RTP プロトコルを使用して、異なるクラスタにある Cisco IP Phone 間に音声パスが作成されます。

コール フロー 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 IP Phone（2002）が Cluster 1 に配置された Cisco IP Phone（1001）にコールを発信しています。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。デバイスをリブ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 IP Phone（2002）はオフフックになっています。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 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 IP Phone（1001）はオフフックになります。TCP ハンドルが Cisco 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 IP Phone の番号（2000）をダイヤルし、番号分析プロセスが番号を一致させようとしています。

```
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 CallManager がこの電話番号と一致しないことを示しています。この点に注意することが重要です。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 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 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 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 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 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 トレース

この項では、Cisco CallManager 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 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、KeepAlive のメカニズムなど）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 IP Phone（電話番号 1001）が、PSTN に配置された電話機（電話番号 3333）にコールを発信しています。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。デバイスをリブ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 IP Phone（1001）はオフフックになっています。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 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 をダイヤルしています（数字を 1 つずつダイヤルしています）。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 CallManager 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ています。番号分析については、付録 B「ケース スタディ：Cisco 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ています。

```
|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。帯域幅が無限であるのは、LAN 環境に配置された Cisco IP Phone からコールが発信されたためです。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 に配置された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ていないので、発信側の名前と番号は同じです。

```
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 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 IP Phone（1001）の IP アドレスは 172.16.70.231 です。

```
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>
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 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

「コール フロー トレース」では、Cisco CallManager 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 でオンになっています。

次のデバッグ メッセージは、Cisco IOS Gatekeeper が Cisco CallManager（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 CallManager 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 CallManager（172.16.70.228）から disengaged request (DRQ; 解除要求）を受信し、Cisco IOS Gatekeeper が disengage confirmed（DCF; 解除確認）を Cisco CallManager 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 CallManager がすべて Cisco IOS Gatekeeper に登録されていることを表示します。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 CallManager が存在することに注意してください。この Cisco IOS Gatekeeper には 2 つのゾーンがあり、各ゾーンには 2 つの Cisco CallManager 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

「Cisco IOS Gatekeeper のデバッグ メッセージと表示コマンド」の項では、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 CallManager（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 CallManager から H.225 データが到達していることを示しています。このデバッグ出力では、使用されている H.323 バージョンを指定する protocolIdentifier に注意してください。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ので、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), clled(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することに留意してください。要求パケット内の発信側と着信側の番号に注目してください。

```
*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 CallManager 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 CallManager に送信していることに注意してください。Cisco IOS Gateway は到達不能なアドレスを送信する場合があるため、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)csize(0)in(1)fDest(1)-cid2(18)st2(3)oldst2(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=0x, 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っていて、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 が有効になっています。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。下記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、ALERTING 用に受信されたものと同じ参照番号（0x800B）を使用して、CONNECT メッセージが交換機から受信されます。最後に、コールが接続解除されるとき、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できます。

```
 *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 はオンになっています。

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/0:-36/-42 dBm
```

機能およびサービスのトラブルシューティング

この付録では、Cisco CallManager 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。

Cisco CallManager 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 CallManager 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 CallManager 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 CallManager Serviceability システム ガイド*』および『*Cisco CallManager Serviceability アドミニストレーション ガイド*』を参照してください。

この項では、Cisco CallManager エクステンション モビリティで発生する次の問題のトラブルシューティングに役立つ情報を提供します。

Cisco CallManager 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 CallManager 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 CallManager 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 CallManager Administration で、画面右上の **Navigation** ウィンドウにある **Cisco CallManager Serviceability** リンクを選択し、**Go** をクリックします。

    Cisco CallManager Serviceability ウィンドウが表示されます。
  - **Trace** メニューから、**Trace Configuration** を選択します。
  - Servers 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。
  - Configured Services のドロップダウン 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 CallManager 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。

これでも問題が解決しない場合は、表 D-1 のトラブルシューティング手段を使用します。

表 D-1　Cisco CallManager 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	推奨される処置
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。	1. Enterprise Parameters 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。 2. 電話機で Cisco Extension Mobility サービスをサブスクライブします。
ログイン後に、ユーザが電話サービスを使用できない。	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。 次の手順を実行します。 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。 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。
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。	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。 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。

Cisco CallManager 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 CallManager 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 D-2 の情報を使用します。

表 D-2　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 コードまたは エラー メッセージ	推奨される処置
0	Cisco CallManager エクステンション モビリティが設定されている電話機にユーザがログインして UserID と PIN を入力しようとすると、電話機に「0」が表示される。 すべての Cisco CallManager サービスが実行されていることを確認します。
2, 3	ユーザが Services ボタンを押すと、電話機に「2」または「3」が表示される。 Cisco CallManager エクステンション モビリティの次のレジストリ エントリを確認します。 HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems Inc.\Directory Configuration\AppUsers\EMApp 「Password」のエントリが存在していること、および「UserID」が「EMApp」であることを確認します。これらのエントリが存在しない場合は、インストールに問題があります。
6	Cisco CallManager エクステンション モビリティが設定されている電話機にユーザがログインして UserID と PIN を入力しようとすると、電話機に「6」が表示される。 このエラーが発生するのは、サービスがユーザを認証していない場合です。 Virtual Directory に問題がある可能性があります。Virtual Directory Login Password が正しいことを確認してください。
9	Cisco CallManager エクステンション モビリティが設定されている電話機にユーザがログインして UserID と PIN を入力しようとすると、電話機に「9」が表示される。 LDAP ディレクトリに問題があります。DirUser.jar ファイルが存在していることを確認してください。
6, 12	Cisco CallManager エクステンション モビリティが設定されている電話機にユーザがログインして UserID と PIN を入力しようとすると、電話機に「6」または「12」が表示される。 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。

表 D-2　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 コードまたは エラー メッセージ	推奨される処置
100	ユーザが Services ボタンを押すと、電話機に「100」が表示される。 Cisco Extension Mobility サービスの URL に、最後のパラメータ（下に**太字**で示した部分）が含まれていません。 http://<IPAddressofCallManager>/emapp/EMAppServlet **?device=#DEVICENAME#** <IPAddressofCallManager> は、Cisco CallManager エクステンション モビリティがインストールされている Cisco CallManager サーバの IP アドレスです。 URL が正しく、完全なものであることを確認してください。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。
101	Cisco CallManager エクステンション モビリティが設定されている電話機にユーザがログインして UserID と PIN を入力しようとすると、電話機に「101」が表示される。 Cisco CallManager パブリッシャの IP アドレスが変更されている可能性があります。次の手順を実行します。 1. DC Directory (DCD) Administration で、Cisco.com > CCN > systemProfiles に移動します。 2. **Hoteling Profile** を選択します。 3. URL フィールドにある IP アドレスが、Cisco CallManager パブリッシャの IP アドレスであることを確認します。
HTTP error	ユーザが Services ボタンを押した後にこのエラー メッセージが表示される場合は、電話機ロードにエラーがあります。 この問題を解決するには、Cisco.com にある最新の電話機ロードを適用し、電話機をリセットします。
Invalid host	ユーザが Services ボタンを押すと、電話機に「Invalid host」メッセージまたはブランク画面が表示される。 1. Enterprise Parameters にある Services URL エントリが正しいことを確認します。 2. 問題が解決しない場合は、電話機をリセットします。
No services configured	ユーザが Services ボタンを押すと、電話機に「No services configured」と表示される。 Cisco Extension Mobility サービスが電話機にサブスクライブされ、ユーザのデバイス プロファイルが選択されていることを確認します。
Requesting...	ユーザが Services ボタンを押して Cisco Extension Mobility Service を選択すると、電話機に「Requesting...」と表示される。 Cisco CallManager　エクステンション モビリティが配置されている Cisco CallManager サーバ上で、Cisco Tomcat Service が開始され、動作していることを確認します。

表 D-2　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 コードまたは エラー メッセージ	推奨される処置
Authentication error	ユーザが UserID と PIN を入力すると、電話機に「Authentication error」と表示される。 UserID と PIN を正しく入力したことをユーザが確認します。また、UserID 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。 Active Directory プラグインを使用している場合は、そのユーザが User Base の下位 OU ではなく、User Base の直下に表示されていることを確認します。
Device does not allow logon	Cisco CallManager エクステンション モビリティが設定されている電話機にユーザがログインして UserID と PIN を入力しようとすると、電話機に「Device does not allow logon」と表示される。 Phone Configuration ウィンドウで、Enable Extension Mobility Feature が選択されていることを確認します。
Device profile unavailable	Cisco CallManager Directory がダウンしている可能性があります。
User logged in elsewhere	このエラーは、複数ログインを制御するサービス パラメータで、1 台のデバイスにしかログインできないように設定されている場合に、ユーザが 2 台目のデバイスにログインしようとしていることを意味します。 次のいずれかの手順を実行します。 • 設定が正しい場合は、ユーザを 1 台目のデバイスからログアウトさせて、2 台目のデバイスにログインするように依頼します。また、この問題が再発しないようにするため、ユーザにシングル ログイン ポリシーについて説明しておきます。 • 複数のデバイスにログインすることをユーザに許可するには、Service Parameters Configuration ウィンドウで、Multiple Login Behavior フィールドを Multiple Logins Allowed に設定します。

Cisco IP Manager Assistant のトラブルシューティング

この項では、Cisco IP Manager Assistant（Cisco IPMA）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 D-3 に、Cisco IPMA 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 D-3　Cisco IPMA のトラブルシューティング ツールとクライアントのデスクトップ

ツールの説明	場所
Cisco IPMA　サーバのトレース ファイル	Cisco CallManager Administration > Application > Serviceability > Trace > Configuration を選択して、IPMA トレース ディレクトリを設定し、デバッグ トレースを有効にします。
Cisco IPMA　クライアントのトレース ファイル	クライアントのデスクトップで、Cisco IPMA アシスタント コンソールと同じ位置にある $INSTALL_DIR\logs\ACLog*.txt です。 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、Enable Trace チェックボックスをオンにします。 **（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。 ダイアログボックスには、現在のトレース ファイルの位置と名前が表示されます。
Cisco IPMA　クライアントのインストール トレース ファイル	クライアントのデスクトップで、Cisco IPMA アシスタント コンソールと同じ位置にある $INSTALL_DIR\InstallLog.txt です。
Cisco IPMA　クライアントの AutoUpdater トレース ファイル	クライアントのデスクトップで、Cisco IPMA アシスタント コンソールと同じ位置にある $INSTALL_DIR\UpdatedLog.txt です。
インストール ディレクトリ	デフォルトでは、C:\Program Files\Cisco\IPMA Assistant Console です。

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

- 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（P.D-20）
- IPMA 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.D-20）

IPMAConsoleInstall.jsp で「Exception While Getting Service Parameters」エラーが表示される

症状

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

エラー メッセージ　`Exception While Getting Service Parameters`

考えられる原因

Cisco IPMA のサービス パラメータの設定で、エラーが発生しました。

対応策

次の手順を使用して、Cisco IPMA のサービス パラメータを設定します。

Cisco CallManager Administration > **Service** > **Service Parameters** を選択します。Cisco IPMA サービスが配置されているサーバを選択し、Cisco IP Manager Assistant サービスを選択します。

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

症状

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

エラー メッセージ　`No Page Found Error`

考えられる原因

Cisco IPMA サービスが動作していません。

対応策

次の手順を使用して、Cisco IP Manager Assistant を起動します。

手順

ステップ 1　管理特権を持つアカウントを使用して、次のアドレスにある Cisco Tomcat マネージャ アプリケーションにログインし、IPMA サービスを再起動します。

http://<ipaddress>/manager/list

ステップ 2　Cisco IP Manager Assistant サービスの隣にある **Reload** リンクをクリックします。

ステップ 3　サービスが開始されます。

症状

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

エラー メッセージ　`No Page Found Error`

考えられる原因

ネットワークに問題があります。システムに関する問題の詳細については、『*Cisco CallManager トラブルシューティング ガイド*』を参照してください。

対応策

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。

症状

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

エラー メッセージ　`No Page Found Error`

考えられる原因

URL のつづりを間違えています。

対応策

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。

エラー メッセージ　`Exception: java.lang.ClassNotFoundException: InstallerApplet.class`

考えられる原因

IPMA コンソール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（http://<servername>/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と失敗します。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 Download Now を選択すると、次のメッセージが表示されます。

エラー メッセージ　`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 Exploler 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。

  http://<servername>/ma/Install/IPMAConsoleInstallJar.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。

- ディレクトリ内で、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 CallManager Administration で、ユーザ ID とパスワードが Cisco CallManager 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 IPMA 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 CallManager Administration > User** にアクセスします。

アシスタント コンソールで「Cisco IPMA Service Unreachable」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。

エラー メッセージ　`Cisco IPMA Service Unreachable`

考えられる原因

Cisco IPMA サービスが停止している可能性があります。

対応策

次の手順を使用して、Cisco IP Manager Assistant を起動します。

手順

ステップ 1　管理特権を持つアカウントを使用して、次のアドレスにある Cisco Tomcat マネージャ アプリケーションにログインし、IPMA サービスを再起動します。

http://<ipaddress>/manager/list

ステップ 2　Cisco IP Manager Assistant サービスの隣にある **Reload** リンクをクリックします。

ステップ 3　サービスが開始されます。

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。

エラー メッセージ　Cisco IPMA Service Unreachable

考えられる原因

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

対応策

次の手順を実行し、DNS 名を置き換えます。

手順

ステップ 1　**Cisco CallManager Administration > System > Server** 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　管理特権を持つアカウントを使用して、次のアドレスにある Cisco Tomcat マネージャ アプリケーションにログインし、IPMA サービスを再起動します。

http://<ipaddress>/manager/list

ステップ 4　Cisco IP Manager Assistant サービスの隣にある **Reload** リンクをクリックします。

ステップ 5　サービスが開始されます。

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。

エラー メッセージ　Cisco IPMA Service Unreachable

考えられる原因

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

次の手順を実行し、Cisco CTI Manager サービスと Cisco IPMA サービスを開始します。

手順

ステップ 1　Start メニューから、**Start > Programs > Administration Tools > Services** を選択します。

ステップ 2　CTI Manager サービスを右クリックします。

ステップ 3　**Start** をクリックします。

ステップ 4　**Yes** をクリックします。

ステップ 5　管理特権を持つアカウントを使用して、次のアドレスにある Cisco Tomcat マネージャ アプリケーションにログインし、IPMA サービスを再起動します。

http://<ipaddress>/manager/list

ステップ 6　Cisco IP Manager Assistant サービスの隣にある **Reload** リンクをクリックします。

ステップ 7　サービスが開始されます。

新しいマネージャが期待どおりに作成されない

症状

新しいマネージャが Cisco IPMA で作成されませんでした。

考えられる原因

Cisco CallManager Administration の Manager Configuration ウィンドウで、**Insert** をクリックしませんでした。

対応策

次の手順を実行し、Cisco IPMA のマネージャを正しく設定します。

手順

ステップ 1　**User > Global Directory** を選択します。

ステップ 2　マネージャを検索する場合は、**Search** をクリックします。

ステップ 3　マネージャ名をクリックします。

ステップ 4　**Cisco IPMA** リンクをクリックします。

ステップ 5　**Add/Delete Assistants** リンクから、アシスタントを割り当てます。

ステップ 6　**Update and Close** をクリックします。

ステップ 7　Manager Configuration で、デバイスと IPMA 制御の回線を入力します。

ステップ 8　**Insert** をクリックします。

アシスタントの割り当てが期待どおりに変更されない

症状

割り当てを別のアシスタントに変更しても、変更内容が有効になりません。

考えられる原因

Add/Delete Assistant ウィンドウで、**Update** または **Update and Close** をクリックしませんでした。

対応策

次の手順を実行し、Cisco IPMA のアシスタントを正しく設定します。

手順

ステップ 1　**User > Global Directory** を選択します。

ステップ 2　マネージャを検索する場合は、**Search** をクリックします。

ステップ 3　マネージャ名をクリックします。

ステップ 4　**Cisco IPMA** リンクをクリックします。

ステップ 5　**Add/Delete Assistant** リンクをクリックします。

ステップ 6　Add/Delete Assistant ウィンドウで、マネージャのアシスタントを選択します。

ステップ 7　**Update** または **Update and Close** をクリックします。

アシスタントのプロキシ回線でマネージャのフィールドがブランクになる

症状

アシスタントのプロキシ回線に、ブランク フィールドが含まれています。

考えられる原因

マネージャをアシスタントから削除すると、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

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。

マネージャまたはアシスタントの検索が遅い

症状

検索を実行しようとしましたが、システムが結果を返すのに時間がかかります。

考えられる原因

すべてのマネージャ、すべてのアシスタント、または多数のマネージャやアシスタントを検索しようとしました。

対応策

検索対象を小さな範囲に絞ることで、パフォーマンスが向上します。

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

フィルタリングがオンになっていると、コールがルーティングされません。

考えられる原因

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

次の手順を実行し、(Cisco Tomcat マネージャを使用して)Cisco CTI Manager サービスと Cisco IPMA を開始します。

手順

ステップ 1　Start メニューから、**Start > Programs > Administration Tools > Services** を選択します。

ステップ 2　CTI Manager サービスを右クリックします。

ステップ 3　**Start** をクリックします。

ステップ 4　**Yes** をクリックします。

ステップ 5　管理特権を持つアカウントを使用して、次のアドレスにある Cisco Tomcat マネージャ アプリケーションにログインし、IPMA サービスを再起動します。

http://<ipaddress>/manager/list

ステップ 6　Cisco IP Manager Assistant サービスの隣にある **Reload** リンクをクリックします。

ステップ 7　サービスが開始されます。

症状

CTI Provider Object を取得できず、次のメッセージが表示されます。

エラー メッセージ　`TimeoutException - Could not get Provider.`

考えられる原因

このエラーは、次の位置にあるログに記録されます。

C:\Program Files\Cisco\Trace\IPMA\IPMA*.txt

または、Cisco CallManager Serviceability の Trace Configuration を使用して作成したディレクトリに記録されます。

対応策

次の手順を実行し、Cisco CTI Manager サービスと Cisco IPMA サービスを開始します。

手順

ステップ 1　Start メニューから、**Start > Programs > Administration Tools > Services** を選択します。

ステップ 2　CTI Manager サービスを右クリックします。

ステップ 3　**Start** をクリックします。

ステップ 4　**Yes** をクリックします。

ステップ 5　管理特権を持つアカウントを使用して、次のアドレスにある Cisco Tomcat マネージャ アプリケーションにログインし、IPMA サービスを再起動します。

http://<ipaddress>/manager/list

ステップ 6　Cisco IP Manager Assistant サービスの隣にある **Reload** リンクをクリックします。

ステップ 7　サービスが開始されます。

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

IPMA ルート ポイントが正しく設定されていません。

対応策

ワイルドカードを使用して、IPMA ルート ポイントの電話番号と、すべての Cisco IPMA マネージャのプライマリ電話番号を対応付けます。

症状

コールが正しくルーティングされません。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。

考えられる原因

IPMA 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

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

手順

ステップ 1　Cisco CallManager Administration から、**Device > CTI Route Point** 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 CallManager 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　管理特権を持つアカウントを使用して、次のアドレスにある Cisco Tomcat マネージャ アプリケーションにログインし、IPMA サービスを再起動します。

http://<ipaddress>/manager/list

ステップ 4　Cisco IP Manager Assistant サービスの隣にある **Reload** リンクをクリックします。

ステップ 5　サービスが開始されます。

更新したユーザ情報が失われる

症状

サービスを再起動すると、更新したユーザ情報が失われます。

考えられる原因

不正な CMDBUtilJNI.dll ファイルが存在しています。

対応策

次の手順を実行し、CMDBUtilJNI.dll ファイルを置き換えます。

手順

ステップ 1　C:\Program files\Cisco\Trace\MA\initTrace**.txt ファイルの内容を表示します。

このファイルには、次の行が含まれています。

```
java.lang.UnsatisfiedLinkError: method name
```

これは、CMDBUtilJNI.dll がメソッドを含んでいないことを意味します。

ステップ 2　CMDBUtilJNI.dll を必要な CMDBUtilJNI.dll に置き換えます。

症状

サービスを再起動すると、更新したユーザ情報が失われます。

考えられる原因

パブリッシャ データベースが動作していません。

対応策

パブリッシャ データベースを起動します。

症状

サービスを再起動すると、更新したユーザ情報が失われます。

考えられる原因

パブリッシャ ディレクトリが動作していません。

対応策

パブリッシャ ディレクトリを起動します。ディレクトリの詳細については、『*Cisco CallManager トラブルシューティング 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

Cisco IPMA のマネージャが IPMA 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 IPMA サーバ上で、イベント ビューアのアプリケーション ログを表示します。IPMA 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 CallManager の管理者が、User Configuration を使用して IPMA 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、問題点を修正します。

手順

ステップ 1　Cisco CallManager Administration から、**User > Global Directory** を選択します。

User Information 検索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、**Search** ボタンをクリックします。

ステップ 3　User Information ウィンドウで、更新するマネージャを選択します。

ステップ 4　User Configuration ウィンドウで、**Cisco IPMA** リンクをクリックします。

ステップ 5　マネージャの User Configuration ウィンドウが表示されます。**Update** ボタンをクリックします。

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、問題点を修正します。

手順

ステップ 1　Cisco CallManager Administration から、**Device > Phone** を選択します。

Find and List Phones 検索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。

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。

IPMA 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

IPMA サービスがダウンしたときに、コールが Cisco IPMA マネージャへ正しくルーティングされません。

考えられる原因

IPMA ルート ポイントで、無応答時自動転送（Call Forward No Answer）が有効になっていません。

対応策

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

手順

ステップ 1　Cisco CallManager Administration から、**Device > CTI Route Point** を選択します。

Find and List CTI Route Point 検索ウィンドウが表示されます。

ステップ 2　**Find** 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 IPMA ルート ポイントを選択します。

ステップ 4　CTI Route Point Configuration ウィンドウで、更新する回線を Directory Numbers ボックスから選択します。

Directory Number Configuration ウィンドウが表示されます。

ステップ 5　Call Forward and Pickup Settings セクションで、Forward No Answer Internal チェックボックスと Forward No Answer External 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 Coverage/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　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　**Update** ボタンをクリックします。

Cisco CallManager AutoAttendant のトラブルシューティング

この項では、Cisco CallManager AutoAttendant に関連する一般的な問題およびその解決方法について説明します。

Cisco CallManager のアップグレード後に IP IVR サーバが起動しない

症状

Cisco CallManager サーバをアップグレードした後に、IP-IVR サーバが起動しません。

考えられる原因

Java Telephony API（JTAPI）クライアントは、Cisco CallManager の既存バージョンと互換性があるものにする必要があります。

対応策

Cisco CallManager のプラグイン ウィンドウで、JTAPI プラグインを再インストールします。Cisco CallManager Administration に移動し、**Application > Install Plugins** を選択します。Cisco JTAPI をダウンロードし、IP-IVR サーバにインストールします。

JTAPI サブシステムが一部しか使用されない

症状

Engine ウィンドウの Engine Status 領域で、JTAPI サブシステムが一部しか使用されていないと表示されます。

考えられる原因

JTAPI クライアントが正しく設定されていません。少なくとも 1 つの（ただし、すべてではない）CTI ポート、ルート ポイント、またはダイアログ チャネル（CMT または Nuance）を初期化できませんでした。

対応策

次の手順を実行します。

手順

ステップ 1　Cisco CRA のトレース ファイルを参照して、初期化されなかった部分を特定します。

ステップ 2　Cisco CallManager で、すべての CTI ポートと CTI ルート ポイントが JTAPI ユーザに関連付けられていることを確認します。

ステップ 3　Cisco CallManager の IP アドレスと JTAPI 設定の IP アドレスが一致していることを確認します。

ステップ 4　Cisco CallManager の JTAPI ユーザが、すべての CTI ポートと CTI ルート ポイントを制御していることを確認します。

ステップ 5　Directory Setup ウィンドウの Configuration Setup 領域にある Directory Host Name フィールドに指定したコンピュータ上で、LDAP ディレクトリが動作していることを確認します。

ステップ 6　アプリケーション ファイルが、Repository Manager を使用しているリポジトリにアップロードされたことを確認します。

Cisco CallManager 自動応答機能のプロンプトが再生されない

症状

Cisco CallManager 自動応答機能のプロンプトが再生されません。

考えられる原因

Cisco Script Application ウィンドウの welcomePrompt フィールドで、誤った初期プロンプトが指定されています。

対応策

Cisco CRA Administration で、System > System Parameters を選択します。User Prompt Directory フィールドに、次の情報が表示されていることを確認します。

```
C:\program files\cisco\wfavvid\Prompts\User
```

名前でのダイヤルで所定のユーザが見つからない

症状

Cisco CallManager 自動応答機能で名前を指定してダイヤルするときに、発信者の指定したユーザが見つかりません。

考えられる原因

要求されたユーザが Cisco CallManager で割り当てられるプライマリ内線番号を持っていないか、ccndir.ini ファイルの情報が欠損しています。したがって、このユーザの内線番号は有効ではありません。

対応策

次の手順を実行します。

手順

ステップ 1　Cisco CallManager Administration の User Information ウィンドウで、AutoAttendant Dialing フィールドにユーザのエントリがあること、User レコードに電話機が関連付けられていること、および Primary Extension 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 2　Cisco CRA サーバ上で、ユーザベースとプロファイルベースの正しい情報が ccndir.ini ファイルに含まれていることを確認します。たとえば、次のようなエントリが含まれています。

```
USERBASE "ou=Users, o=cisco.com"
PROFILEBASE "ou=profiles, ou=CCN, o=cisco.com"
```

名前の録音をアップロードしても使用されない

症状

名前の録音をアップロードした後に、名前の録音が使用されません。

考えられる原因

このファイルは、CCITT μ 法コーデックのモノラル形式（8.000 KHz、8 ビット）にする必要があります。

対応策

詳細については、サーバ上のドキュメント http://<server_name>/appadmin/PromptInstruct.htm を参照してください。

IOS 音声ゲートウェイからコールすると、電話番号を入力してもアナウンスが流れ続ける

症状

IOS 音声ゲートウェイからコールすると、電話番号を入力した後もアナウンスが流れ続けます。

考えられる原因

IOS ゲートウェイ上で DTMF リレーが設定されていません。

対応策

Cisco CallManager を指している VoIP ピア上で、dtmf-relay h245-alphanumeric を設定します。

```
dial-peer voice 7000 voip
destination-pattern 2...
session target ipv4:10.200.72.36
dtmf-relay h245-alphanumeric
```

スクリプトをルート ポイントに割り当てて言語を設定しても、発信者にプロンプトが再生されない

症状

ルート ポイントに割り当てられ、言語が設定されているスクリプトにコールしたときに、発信者にプロンプトが再生されません。

考えられる原因

スクリプトが無効であるか、スクリプトに対して設定されている言語が正常にインストールされていません。

対応策

次の手順を実行します。

ステップ 1　スクリプトを確認します。

ステップ 2　ルート ポイント上で、言語を en_US に設定し、スクリプトが正しく動作することを確認します。正常に動作しない場合は、次の手順に従います。

a. Cisco CRA Administration で、**System > System Engine** を選択します。

b. Trace Configuration ハイパーリンクをクリックし、LIB_MEDIA サブファシリティと SS_TEL サブファシリティの Debugging チェックボックスをオンにします。

c. スクリプトをもう一度実行し、Cisco CRA のトレース ファイルを参照します。Cisco CRA のトレース ファイルにプロンプト例外が記録されている場合は、該当する言語を再インストールします。

発信側と Cisco CRA でコーデックが共通していない

症状

発信側が Cisco CRA アプリケーションにコールすると、ファースト ビジー シグナルが再生されます。Cisco CRS のログには、次のように記録されます。

```
CTIERR_REDIRECT_CALL_PROTOCOL_ERROR
```

考えられる原因

Cisco Customer Response Solution 3.5 は、G.729 または G.711 のいずれかを指定してインストールできます。同時にサポートされるコーデックは 1 つのみです。発信側デバイスのコーデックが、Cisco CRA と互換性がない可能性があります。

対応策

Cisco CallManager 上でトランスコーディング サービスを使用するか、Cisco CRA サーバ上に設定されているコーデックに応じて、発信側デバイスで G.711 または G.729 を使用するようにします。

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、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。P.D-27 の「使用可能な Conference Bridge がない」を参照してください。

使用可能な Conference Bridge がない

症状

Barge（割り込み）ソフトキーを押すと、IP Phone に No Conference Bridge Available 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 Phone Configuration で、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。

1. Cisco CallManager Administration で、**Device > Phone** に移動し、**Find the phone** をクリックして、問題が発生している電話機の電話設定を見つけます。
2. Built In Bridge パラメータを On に設定します。
3. Update をクリックします。
4. 電話機をリセットします。

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ない

症状

ユーザが iDivert を押すと、電話機に Key is not active というメッセージが表示されます。

考えられる原因

iDivert 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。

一時的な障害

症状

ユーザが iDivert を押すと、電話機に Temporary Failure という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。

ビジー

症状

ユーザが iDivert を押すと、電話機に Busy という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。

Cisco WebDialer のトラブルシューティング

この項では、Cisco WebDialer 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。

Authentication Error

考えられる原因

ユーザが、間違った userID またはパスワードを入力しました。

対応策

userID とパスワードを確認します。Cisco CallManager の userID とパスワードを使用してログインする必要があります。

Service Temporarily Unavailable

考えられる原因

同時 CTI セッションのスロットリング上限値（2 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。

Directory Service Down

考えられる原因

Cisco CallManager 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 Down

考えられる原因

Cisco WebDialer 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。

Session Expired, Please Login Again

考えられる原因

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

- WebDialer サーブレットが設定された
- Cisco Tomcat サービスが再起動された

対応策

Cisco CallManager の userID とパスワードを使用してログインします。

User Not Logged in on Any Device

考えられる原因

ユーザが、Cisco WebDialer のプリファレンス ページで Cisco CallManager 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 WebDialer を使用します。
- **Use Extension Mobility** オプションを選択するのではなく、デバイスをダイアログボックスの Cisco WebDialer プリファレンス リストから選択します。

Failed to Open Device/Line

考えられる原因

- ユーザが、Cisco CallManager に登録されていない Cisco 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 CallManager に登録され、使用されている電話機を選択します。

Destination Not Reachable

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。

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、推奨される処置、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

この項では、問題、考えられる原因、推奨される処置、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 Callback 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、**Callback** ソフトキーが電話機に表示されることがあります。

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 **CallBack** 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。

CallBack 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）

CallBack 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。

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、**CallBack** 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。

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。

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、**CallBack** 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、**CallBack** 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。

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。**CallBack** 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　`Call Back is not active. Press Exit to quit this screen.`

説明　アイドル状態のときに、ユーザが **CallBack** 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　`CallBack is already active on xxxx. Press OK to activate on yyyy. Press Exit to quit this screen.`

説明　ユーザがコール バックをアクティブにしようとしましたが、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　`CallBack cannot be activated for xxxx.`

説明　ユーザがコール バックをアクティブにしようとしましたが、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 CallManager Administration に追加する必要があります。

エラー メッセージ　`Service is not active.`

説明　Callback 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 Callback 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 CallManager 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 CallManager Serviceability アドミニストレーション ガイド*』を参照してください。

Numerics

A

C

I

R

S

せ

そ

た

つ

て

と

り

ろ

わ