Cisco Intercompany Media Engine
インストレーション / コンフィグレーション ガイド

Cisco Intercompany Media Engine Installation and Configuration Guide

リリース 8.6(1)

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco Intercompany Media Engine インストレーション / コンフィグレーション ガイド

CONTENTS

はじめに

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

（注） マニュアル全体の PDF 版には、マニュアルが最初に発行された時点での情報が含まれています。マニュアルの PDF 版には、内容に対する以後の更新が反映されていない場合があります。

更新が含まれる章には、章のタイトルの後に目印（改定日 mm/dd/yyyy）があります。最新の内容については、これらの章の HTML 版および PDF 版を参照してください。

このマニュアルの最新版は、次の URL から入手できます：

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/ime/8_0_2/ime802.html または
http://www.cisco.com/en/US/docs/voice_ip_comm/cucmbe/ime/8_0_2/ime802.html

この項の構成は、次のとおりです。

目的

このマニュアルでは、Cisco Intercompany Media Engine（Cisco IME）のインストールと管理について説明します。このマニュアルには、Cisco Unified Communications Manager の管理 および Cisco IME のコマンド ライン インターフェイスを使用して行う作業手順の説明があります。

対象読者

このマニュアルは、Cisco Unified Communications Manager システムの管理を担当するネットワーク管理者を対象としています。このマニュアルを使用するには、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

次の表に、このマニュアルの構成を示します。

章	説明
第 1 章	「概要」 Cisco Intercompany Media Engine の機能に関する一般的な情報を提供し、その機能により企業間で直接 IP 接続を確立する方法を説明します。
第 2 章	「インストールと Cisco IME サーバの設定」 Cisco Intercompany Media Engine サーバのインストールおよび設定について説明します。
第 3 章	「Cisco Unified Communications Manager の管理での Cisco IME の設定」 Cisco Unified Communications Manager の管理 で Cisco Intercompany Media Engine 機能を設定する方法について説明します。
第 4 章	「Cisco ASA 設定」 コマンド ライン インターフェイスおよび ASDM（Web ベースの GUI アプリケーション）を使用した ASA の設定について説明します。
第 5 章	「Cisco IME サーバのバックアップと復元」 Cisco Intercompany Media Engine サーバでのバックアップ関連および復元関連の作業の実行について説明します。
第 6 章	「Cisco Intercompany Media Engine サーバ上のサービスの管理」 Cisco Intercompany Media Engine サーバで使用できるサービスについて説明します。
第 7 章	「Cisco Intercompany Media Engine での RTMT の使用」 Real-Time Monitoring Tool のインストールおよび使用に関する説明および手順が記載されています。
第 8 章	「Cisco IME クライアント コール アクティビティ レポートの生成」 Cisco Unified サービスアビリティ で Cisco IME クライアント コール アクティビティ レポートを生成する方法について説明します。
第 9 章	「Cisco IME での SNMP の設定」 SNMP バージョン 3 の設定、SNMP トラップおよびインフォーム パラメータの設定、MIB-II システム グループのシステム接点およびシステム ロケーション オブジェクトの設定に関する手順について説明します。管理者は、トラブルシューティング、診断、およびネットワーク管理作業を実行するために SNMP を使用します。

章	説明
第 10 章	「トラブルシューティング」 Cisco Intercompany Media Engine サーバのトラブルシューティングを支援するツールについて説明します。
第 11 章	「Cisco Intercompany Media Engine のパフォーマンス オブジェクトおよびカウンタ」 Cisco Intercompany Media Engine のパフォーマンス オブジェクトとそれらの関連するカウンタのリストが記載されています。
第 12 章	「Cisco Intercompany Media Engine アラートの説明およびデフォルト設定」 Cisco Intercompany Media Engine アラートの説明とデフォルト設定が記載されています。

関連資料

Cisco IP テレフォニー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。

- 『*Cisco Unified Communications Manager Documentation Guide*』
- 『*Release Notes for Cisco Unified Communications Manager*』
- 『*Release Notes for Cisco Intercompany Media Engine*』
- 『*Cisco Intercompany Media Engine Release 8.5(1) TCP and UDP Port Usage*』
- 『*Cisco Intercompany Media Engine Command Line Interface Reference Guide*』
- 『*Cisco Unified Communications Manager システム ガイド*』
- 『*Cisco Unified Communications Manager 機能およびサービス ガイド*』
- 『*Cisco Unified Communications Manager アドミニストレーション ガイド*』
- 『*Cisco Unified Serviceability Administration Guide*』
- 『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』
- 『*Cisco Unified Communications Manager Bulk Administration ガイド*』
- 『*Cisco Unified Communications Solution Reference Network Design (SRND)*』

表記法

このマニュアルでは、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 }	必ずいずれか 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]	いずれか 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。

表記法	説明
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見なされます。
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。
——→	例の中で重要な文字を強調しています。
^	^ 記号は、Ctrl キーを表します。たとえば、画面に表示される ^D というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します。
< >	パスワードのように出力されない文字は、かぎカッコ（<>）で囲んで示しています。

注は、次のように表しています。

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

ワンポイント アドバイスは、次のように表しています。

ワンポイントアドバイス *時間を節約する方法*です。ここに紹介している方法で作業を行うと、時間を短縮できます。

ヒントは、次のように表しています。

ヒント *役立つヒント*です。

注意は、次のように表しています。

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

警告は、次のように表しています。

警告 **「危険」の意味です。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。**

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

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

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

CHAPTER 1

概要

Cisco Intercompany Media Engine（Cisco IME）は、ピアツーピア技術を既存の Public Switched Telephone Network（PSTN; 公衆電話交換網）インフラストラクチャと結合することで、企業間に直接 IP 接続を確立できる技術です。Cisco IME を使用すると、Cisco Unified Communications Manager をすでに導入している企業は、エンタープライズ間にダイナミックな Session Initiation Protocol（SIP; セッション開始プロトコル）トランクを作成し、PSTN ではなくインターネット経由でセキュアに通信を行うことができるようになります。インターネットを経由するエンタープライズ外のトラフィックを有効にすることで、Cisco IME はビデオ可能なコール、ワイドバンド オーディオのサポート、リッチ発信者 ID、プレゼンスといった、これまではエンタープライズ内でだけ動作していた機能を外部コールにも拡張します。

Cisco IME によって、コンサルタント、製造業者、供給業者、外部委託業者、販売業者、サプライチェーン パートナーといったビジネスに欠かせない外部パートナーとの、もっと効果的な通信が実現します。

この項の内容は次のとおりです。

機能と利点

Cisco Intercompany Media Engine（Cisco IME）は、事業者間に順次ダイナミック SIP トランクを作成して、協働する一群のエンタープライズを、エンタープライズ間にクラスタ間トランクを持つ 1 つの大きな事業者と見なせるようにします。Cisco IME によって、必要に応じて会社間でインターネットを介して相互接続できるようになります。この機能は、お客様にとって重要な特徴を数多く有しています。

- 電話番号で使用可能：Cisco IME は、お客様がお持ちの電話番号で使用できます。Cisco IME では、お客様が新しい番号を覚える必要も、プロバイダーを変更する必要もありません。
- 既存の電話機と使用可能：Cisco IME は、エンタープライズ内の既存の電話機とともに使用できます。さらに機能が豊富な電話機を必要としないのであれば、電話機の変更は必要ありません。
- 新規サービスの購入が不要：Cisco IME なら、サービス プロバイダーから新しいサービスを購入する必要は何もありません。現在の PSTN とインターネット接続を継続使用できます。Cisco IME は、コールを順次 PSTN からインターネットに移していきます。
- ユニファイド コミュニケーションを全面体験：Cisco IME は事業者間にクラスタ間 SIP トランクを作成するため、SIP トランク経由で動作し SIP トランクだけを必要とする機能であれば、すべて事業者間でも動作するようになります。

- インターネットで動作：Cisco IME では、インターネットや管理対象外部ネットを介してコールを送信できます。
- 世界中に到達可能：Cisco IME なら、Cisco IME テクノロジーが運用されているエンタープライズであれば、世界のどのエンタープライズにも接続できます。
- 高い拡張性：Cisco IME では、連繋できるエンタープライズの数に制限がありません。
- 自己学習性：ご自分のネットワークの情報を設定した後は、他の事業者への IP ルートを Cisco IME が自動的に学習します。他の事業者の電話プレフィックス、IP アドレス、ポート、ドメイン名、証明書といった情報を入力する必要はまったくありません。
- QoS 管理：Cisco IME には、インターネット接続の Quality of Service（QoS; サービス品質）管理に役立つ機能が準備されています。Cisco IME は Real-Time Transport Protocol（RTP; リアルタイム転送プロトコル）トラフィックの QoS をリアルタイムに監視し、問題が発生すると自動的に PSTN にフォールバックします。

動作

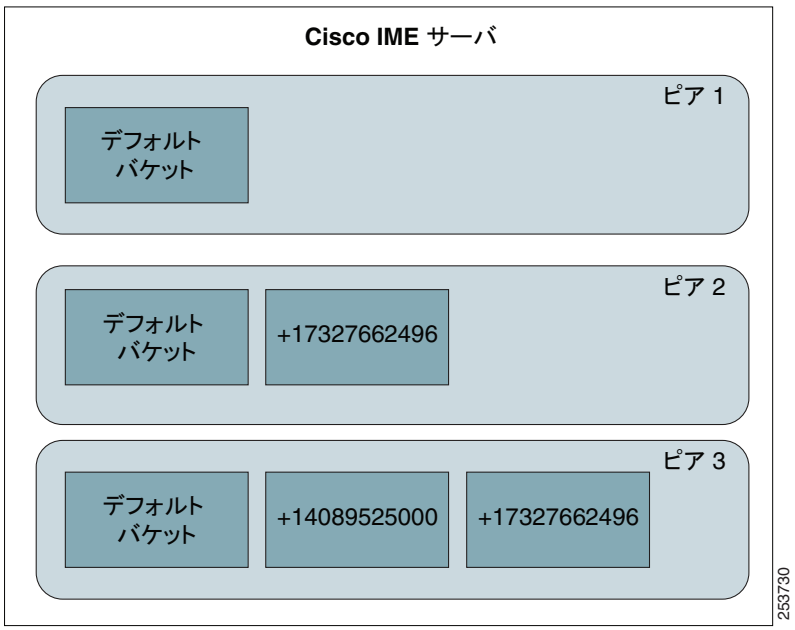
Cisco Intercompany Media Engine（Cisco IME）を使用すると、Cisco Unified Communications Manager をすでに配置している企業は、エンタープライズ間にダイナミック SIP トランクを作成し、PSTN ではなくインターネット経由で通信を行えるようになります。

Cisco IME を使用するには、Cisco IME ソリューションを導入する必要があります。これには、Cisco IME に参加させる Cisco Unified Communications Manager で Direct Inward Dialing number（DID; ダイヤル イン）を設定することが含まれます。Cisco Unified Communications Manager はこれらの番号を、今度は IME 分散キャッシュ リング内のサーバに番号を発行する Cisco IME サーバに発行します。Cisco IME（ピア）サーバはすべて、暗号化形式で IME 分散キャッシュ リングに参加し、データを保存します。

（注）　Cisco IME では、ユーザのダイヤルする番号を、システムが国際番号「+」プレフィックスを含む E.164 形式の番号（「+14085551212」など）に変更することが要求されています。この形式のことを、本マニュアル中では「+E.164」形式と呼びます。

図 1-1 に IME 分散キャッシュ リングの例を示します。

図 1-1　IME 分散キャッシュ リング



IME 分散キャッシュ リングに格納された番号を持つ別のエンタープライズとインターネットを介して通信するには、最初に Public Switched Telephone Network（PSTN; 公衆電話交換網）コールの設定可能な番号を、そのエンタープライズ内の番号として完成させる必要があります。PSTN コールの終了後、コール当事者のエンタープライズは、コールについての情報を Voice Call Record（VCR; 音声コール レコード）で Cisco IME サーバに送ります。VCR では、コールについて、開始時間、停止時間、着信者番号、発信者番号といった情報が示されます。検証プロセスが始まります。発信側の Cisco IME サーバは、ダイヤルされた番号の所有者とされるエンタープライズの特定を試み、着信側エンタープライズが実際にその電話番号を所有しているどうかを検証するプロセスを開始します。着信側では、このドメイン名がブラックリスト ドメインのセットに含まれていないことを検証します。

検証が完了すると、発信者側 Cisco IME サーバは Cisco Unified Communications Manager サーバにメッセージを送信し、この番号の VoIP ルートを提供します。発信者側 Cisco Unified Communications Manager はルートを学習し、今後の使用のためデータベース内にルートと検証チケットを保存します。このチケットは、宛先エンタープライズの特定の電話番号へのコールの権限がエンタープライズに与えられていることを示します。ルートとチケットの有効期限は 1 年間です。ユーザが次に発信側エンタープライズのいずれかの番号から同じ番号へコールが発信するときには、コールはダイナミック SIP トランクにより Internet を介して送信されます。このコールが着信側で Cisco Intercompany Media Engine 有効 ASA に到達すると、Cisco Intercompany Media Engine 有効 ASA は SIP メッセージに含まれるチケットを検証します。チケット内のドメインは発信エンタープライズのドメインと、着信者番号はチケットが許可した番号とそれぞれ一致している必要があります。

Cisco IME では、有効なルートだけが Cisco Unified Communications Manager に送られるようにするためのセキュリティと、インターネット接続品質低下時に QoS を維持するための方法とが準備されています。これらの機能の詳細については、次の項を参照してください。

- 「検証ルール」（P.1-4）
- 「PSTN フォールバック」（P.1-5）

検証ルール

Cisco Unified Communications Manager サーバのセキュリティを確保するため、Cisco Intercompany Media Engine（Cisco IME）機能は検証ルールのセットを適用し、有効なルートだけが Cisco Unified Communications Manager に送られるようにします。

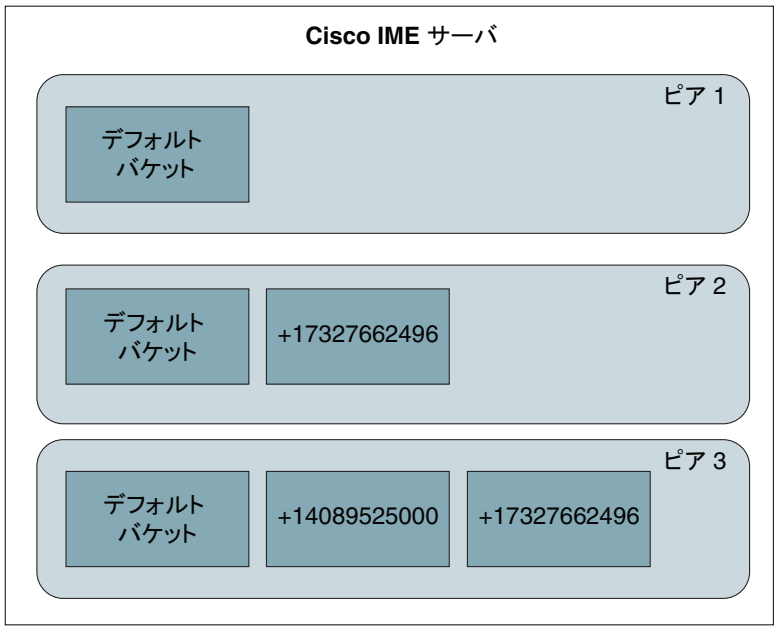
次のリストに、検証基準の要約を示します。

- Cisco Unified Communications Manager が Cisco IME サーバからの学習したルートを受信する前に満たす必要がある、指定のエンタープライズ（または Cisco IME サーバ）の所有する DID に対する検証の連続成功回数。デフォルトでは、Cisco Intercompany Media Engine は 3 回の検証を要求します。検証は、異なる接続先番号に対するものでもかまいません。検証に 3 回連続して成功すると、Cisco IME サーバは学習した 3 ルートすべてを Cisco Unified Communications Manager に送ります。セキュリティ要求事項に応じて、Cisco Unified Communications Manager がルートを学習するまでに必要な検証成功回数を増減できます。
- 特定の番号に対する検証が失敗した場合、システムは、Cisco IME が学習したルートを Cisco Unified Communications Manager に送る前に、当該番号に対する検証が連続して成功することを要求します。
- Voice Call Record（VCR; 音声コール レコード）が相関しないようにするため、Cisco Unified Communications Manager が 1 時間以内に発生した 2 つの同一番号の VCR を検証することはありません。セキュリティ要求事項に応じ、同一番号への検証試行の最小間隔を設定できます。

検証結果を追跡するために、Cisco IME サーバはプールを使用します。プールは特定の Cisco IME（またはピア）と関連付けられたバケットの集合です。デフォルト バケットは Cisco IME サーバに対する検証成功を追跡し、番号バケツは同一 DID に対する検証成功を追跡します。

図 1-2 に、3 つの異なるピアのプールを持つ Cisco IME サーバの例を示します。

図 1-2　プールとバケット



この例では、各プールにデフォルト バケットが含まれています。Peer 2 は、+17327662496 の番号特定バケットも含んでいます。Peer 3 には、+1408952500 および +17327662496 という 2 つの番号特定バケットが含まれています。番号 +17327662496 が 2 つの異なる Cisco IME サーバ（またはピア）に存在するため、この番号の番号特定バケットが 2 つの異なるプールに存在しますが、これらのバケットは相関していません。

それぞれのバケットに、検証成功の結果が保持されています。特定のピアに対する検証が成功すると、Cisco IME は、検証された番号に一致する番号特定バケットが存在する場合そのバケットに、存在しない場合はデフォルト バケットに検証結果を置きます。各検証結果はまた、Cisco IME サーバがコールの検証に使用した方法に応じて、特定の値と関連付けられます。検証結果がバケットに入れられると、バケットの値が検証結果の値（8 または 12）だけ増加します。

各バケットにはしきい値が設定されています。設定されたしきい値は、デフォルト バケットと番号特定バケットの両方に適用されます。バケットの検証結果の値がしきい値を超えると、バケット内の検証結果は削除され（空にされ）、結果は Cisco Unified Communications Manager に送られます。

（注）　Cisco IME サーバ上のバケットのしきい値は、set ime validator local bucketentropy CLI コマンドで変更できます。

あるピアへの検証が失敗すると、Cisco IME はそのピアに対応するプール内のバケットすべてを空にし、プールに宛先番号の番号特定バケットを作成します（存在しない場合）。検証失敗後にピアがルート学習を行うためには、同一番号への検証実行が連続して成功する必要があります。

番号特定バケットは、ペナルティ ボックスを表します。いつでも検証結果が成功するピアには番号特定バケットが作成されず、ピアは異なる番号に対する検証が設定した回数連続して成功した後にルートを学習します。検証に失敗したピアは番号特定バケットを持つようになり、同一番号に対する検証が設定した回数連続して成功する必要があります。

PSTN フォールバック

Cisco IME 機能は、許容レベルを下回るほど Quality of Service（QoS; サービス品質）が低下した場合に、コールを PSTN にフォールバックするメカニズムを提供します。発信側と着信側の Cisco Intercompany Media Engine 有効 ASA は、トラフィックの品質を監視します。見つかったロスとジッターのプロパティをもとに、Cisco Intercompany Media Engine 有効 ASA はコールを PSTN にフォールバックさせる必要があるかを判定します。音声コールは PSTN 上で継続され、コールへの影響やユーザへのアラートは発生しません。

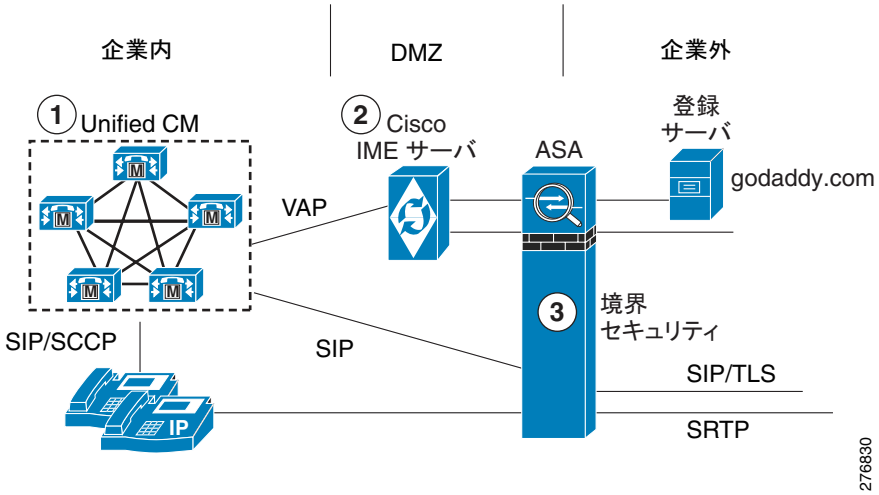
PSTN にフォールバックが必要なコールについては、発信側 Cisco Unified Communications Manager が Cisco IME コールが有効なうちに PSTN コールをセットアップします。Cisco Unified Communications Manager が PSTN コールを確立すると、Cisco Unified Communications Manager は Internet/RTP ストリームをインターネットから PSTN にシームレスにスイッチします。ビデオなどの拡張機能はすべて失われますが、コールの音声部分はそのまま残ります。

コンポーネント

Cisco Intercompany Media Engine（Cisco IME）ソリューションは、ルートのダイナミックな学習、および組織間のセキュアに暗号化されたコール シグナリングとメディアを実現する、いくつかのコンポーネントで構成されています。コンポーネントには Cisco IME サーバ、Cisco Unified Communications Manager サーバ、Cisco Intercompany Media Engine 有効 ASA、GoDaddy.com Web サイトからの証明書などがあります。Cisco IME サーバは加入者宅内の Demilitarized Zone（DMZ; 非武装地帯）に存在し、自動化されたプロビジョニング サービスとして機能します。サーバは特定の電話番号への VoIP（または Cisco IME）ルートを学習し、ルートを Cisco Unified Communications Manager にプッシュします。Cisco Unified Communications Manager サーバは Validation Access Protocol（VAP; 検証アクセス プロトコル）という標準プロトコルによって Cisco IME サーバに接続します。標準 Cisco Unified Communications Manager 導入としては、Cisco Unified Communications Manager がコール処理機能すべてを実行します。Cisco Intercompany Media Engine 有効 ASA は、Cisco Intercompany Media Engine ソリューションに周辺のセキュリティを提供します。GoDaddy.com Web サイトでは、Cisco IME サーバのリングが作成するピアツーピア ネットワークへの参加に必要な証明書を取得できます。

図 1-3 に、Cisco Intercompany Media Engine ネットワークのコンポーネントを示します。

図 1-3　Cisco Intercompany Media Engine コンポーネント



次のセクションで、Cisco IME コンポーネントについて詳しく説明します。

Cisco Intercompany Media Engine（ピア）サーバ

DMZ 内に位置する Cisco IME サーバは、Validation Access Protocol（VAP; 検証アクセス プロトコル）によって Cisco Unified Communications Manager サーバと通信し、他の Cisco IME サーバとはインターネットを介して通信します。Cisco IME サーバは協働して、公衆インターネット経由の IME 分散キャッシュリングを作成するピアツーピア ネットワークを形成します。

IME 分散キャッシュ リング内の各 Cisco IME サーバは、リングが所有するデータの一部を格納します。データは暗号化され、データを格納する Cisco IME サーバが内容を読み取れないようになっています。リング上の各 Cisco IME が、データをリングに格納し、リングからデータを取得することが可能です。リングに格納される Direct Inward Dialing（DID; ダイヤル イン）番号は、DHT に格納される前に一方向ハッシュされます。Cisco IME サーバはコール制御を行いません。Cisco IME サーバは Direct Inward Dialing numbers（DID; ダイヤル イン）を IME 分散キャッシュ リングに格納し、リングから Cisco Unified Communications Manager に提供されるリモート DID へのルートを学習します。

Cisco IME のローカル管理とメンテナンスは、Command Line Interface（CLI; コマンド ライン インターフェイス）を通じて行います。

Cisco Intercompany Media Engine（ブートストラップ）サーバ

Cisco IME の動作は、Cisco Systems が管理する一群のブートストラップ サーバに依存します。ブートストラップ サーバは、どのピア サーバが IME 分散キャッシュ リングに加われるかを決定します。ブートストラップ サーバは設定情報を配布します。Cisco がブートストラップ サーバ上で設定変更を行うと、変更はリング全体に伝搬され、他のすべてのノードの設定が更新されます。

Cisco Unified Communications Manager

Cisco Unified Communications Manager は Cisco IME サーバから学習した VoIP ルートを格納し、Cisco IME ソリューションのコール処理機能すべてを提供します。Cisco Unified Communications Manager の管理 は、Cisco Unified Communications Manager で Cisco IME 機能を使用するためのプロビジョニングを助けます。Cisco Unified Communications Manager の管理 では、Cisco IME サーバ、Cisco IME の使用を許可する電話番号、信頼するドメインなどを指定します。パラメータを指定して、コール品質が許容レベル以下になった場合に Cisco IME コールを Public Switched Telephone Network（PSTN; 公衆電話交換網）フォールバックさせることも可能です。

ASA

Cisco Intercompany Media Engine 有効 Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）は、Cisco IME ソリューションのセキュリティの中核を担います。Cisco Intercompany Media Engine 有効 ASA は、コール制御とメディアのインターフェイスをセキュアにします。Cisco Intercompany Media Engine プロキシと同時に使用することで、ASA は周辺のセキュリティ機能を提供し、SIP トランク間の SIP シグナリングを検査します。Cisco Intercompany Media Engine 有効 ASA は、具体的には次の機能を実行します。

- SIP Application Level Gateway（ALG; アプリケーション レベル ゲートウェイ）: Cisco Intercompany Media Engine 有効 ASA を通過する SIP シグナリング メッセージを検査します。Cisco Intercompany Media Engine 有効 ASA は、SDP とさまざまな SIP ヘッダー フィールドを適用して、Network Address Translation（NAT; ネットワーク アドレス変換）が有効なケースを扱います。SIP ALG はまた、メディア ストリームのためのピンホールを空けて（またはバインドを作成して）、メディアのフローの Cisco Intercompany Media Engine 有効 ASA への出入りを可能にします。
- SIP メッセージ検証：SIP メッセージが Cisco Unified Communications Manager やネットワーク内の他のコンポーネントをクラッシュさせないようにします。Cisco Intercompany Media Engine 有効 ASA は、Uniform Resource Identifiers（URI; ユニフォーム リソース識別子）を許可するキー ヘッダー フィールドを解析し、検証します。Cisco Intercompany Media Engine 有効 ASA は、SIP ステート ダイアグラムに準拠していないメッセージをブロックします。
- SIP から SIP/TLS へ：Cisco Unified Communications Manager がセキュア モードでない場合に、インターネットへの SIP/TLS 接続を終了し、Cisco Unified Communications Manager への TCP だけの接続を再度開始します。Cisco Unified Communications Manager がセキュア モードの場合、Cisco Intercompany Media Engine 有効 ASA は Cisco Unified Communications Manager への TLS 接続を開始します。Cisco Intercompany Media Engine 有効 ASA は TLS プロキシとして動作するようになり、Cisco Unified Communications Manager は SIP メッセージの参照や処理が行えるようになります。Cisco Intercompany Media Engine 有効 ASA は、既知の Certificate Authority（CA; 認証局）に対する遠端側エンタープライズが発行した証明書を検証します。
- NAT：ASA は、インターネットとの使用でしばしば必要となる NAT と SIP ALG の機能を提供します。
- RTP/SRTP：SRTP キーを作成し、コールの他端に送られる暗号化シグナリングを含めることで、Cisco Intercompany Media Engine 有効 ASA の内側の RTP を、Cisco Intercompany Media Engine 有効 ASA のインターネット側 SRTP に変換します。

- チケットの検証：Cisco IME チケットのヘッダーを検査し、Cisco Unified Communications Manager へのシグナリングすべてがチケット内の情報に基づいて許可されていることを確認します。Cisco Intercompany Media Engine 有効 ASA は、有効なチケットのない要求すべてを拒否します。
- RTP のモニタリング：RTP ストリームで Quality of Service（QoS; サービス品質）を監視します。

システムを設定することで、Cisco IME トラフィックは Cisco Intercompany Media Engine 有効 ASA を経由して送信し、他の企業トラフィックは既存の ASA を経由して送信するようにできます。詳細については、「配置モデル」（P.1-8）を参照してください。

登録サーバ（GoDaddy.com）

GoDaddy.com は、Cisco Intercompany Media Engine（Cisco IME）サーバが Cisco IME ピアツーピア ネットワークに参加できるようにするための証明書を提供します。ライセンスを購入して Cisco IME サーバにインストールした後、GoDaddy.com の Web サイトで Cisco IME 証明書を購入します。証明書購入プロセスでは、GoDaddy で Cisco IME を一意で識別するために Cisco IME サーバ ID を提供する必要があります。GoDaddy がサーバを有効と判定した場合、GoDaddy は Cisco IME サーバの証明書を返します。証明書によって、分散キャッシュ リングを形成する Cisco IME サーバ間の TLS 接続が可能になります。

配置モデル

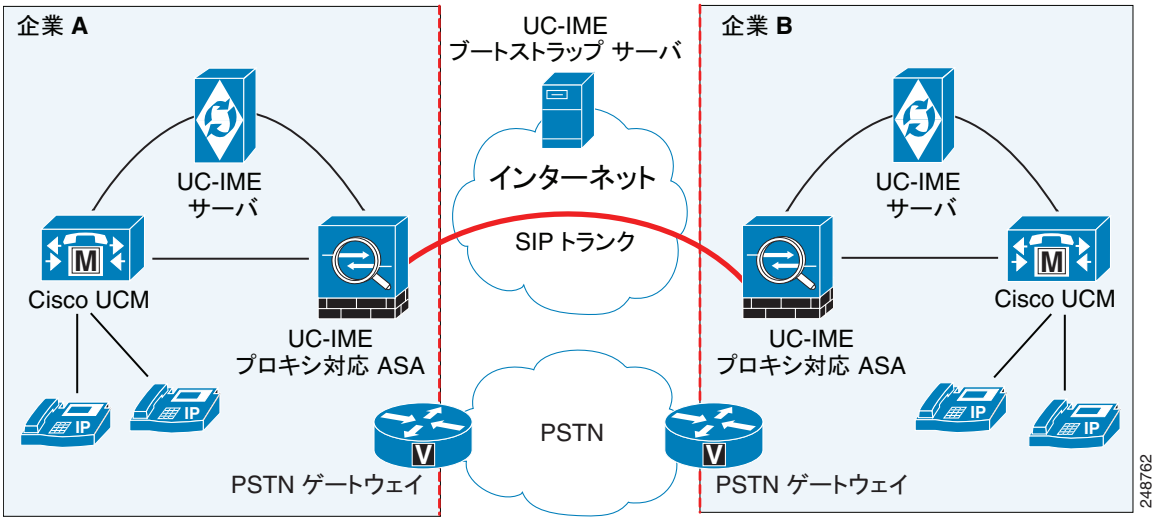
このセクションでは、Cisco Intercompany Media Engine で利用可能な配置モデルについて説明します。

基本配置

基本配置では、Cisco Intercompany Media Engine プロキシはインターネット ファイアウォールとインラインに存在するため、すべてのインターネット トラフィックが Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）を通過します。この配置では、Cisco Intercompany Media Engine（Cisco IME）サーバとともに、単一の Cisco Unified Communications Manager または Cisco Unified Communications Manager クラスタが、エンタープライズ内部で中心的に配置されます。単一のインターネット接続が、Cisco Intercompany Media Engine プロキシが有効な ASA を通過します。

図 1-4 に示すとおり、ASA はエンタープライズのエッジに位置し、エンタープライズ間にダイナミック SIP トランクを作成することで SIP シグナリングを検査します。

図 1-4　基本配置モデル



オフパス配置

企業ネットワーク間で 2 層のファイアウォールを使用する典型的な大規模ネットワークでは、既存のインターネット ファイアウォールを Cisco Intercompany Media Engine 有効 ASA に置き換える（またはアップグレードする）ことや、既存のセキュリティ アーキテクチャを Cisco Intercompany Media Engine 有効 ASA をインターネット ファイアウォールとインラインに追加するよう変更することが難しい場合があります。この問題を解決するため、Cisco では Cisco Intercompany Media Engine のオフパス ASA モデルを許容しています。

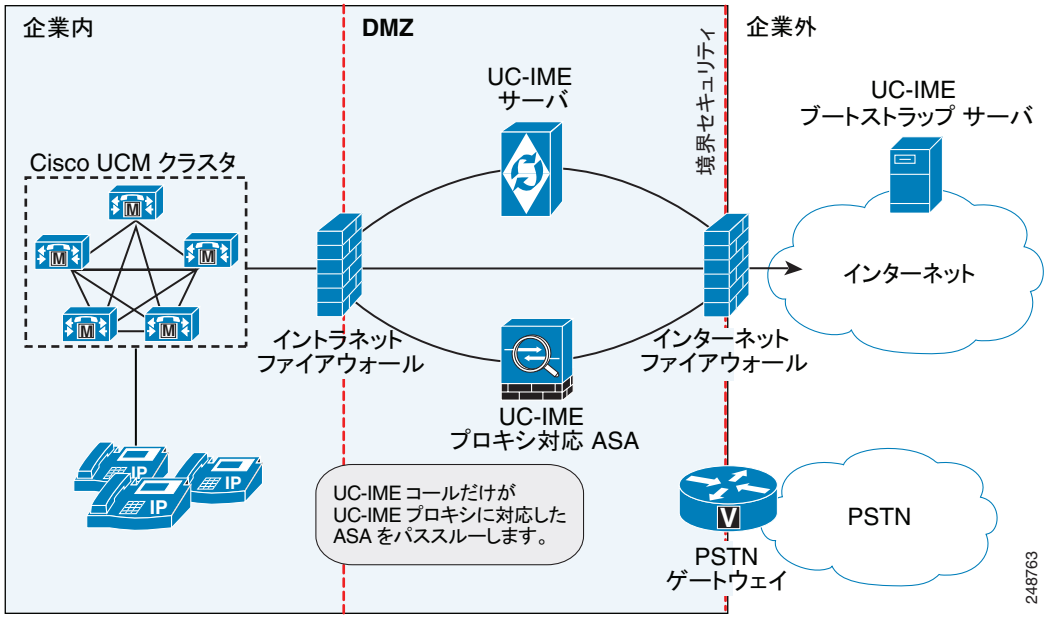
オフパス配置では、Cisco Intercompany Media Engine コールの発着信は Cisco Intercompany Media Engine プロキシが有効な Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）をパススルーします。DMZ 内の ASA は、主に Cisco Intercompany Media Engine のサポート提供用として設定します。通常のインターネット向けトラフィックがこの ASA を流れることはありません。

着信コールはすべて、シグナリングが直接 ASA に転送されます。宛先 Cisco Unified Communications Manager が ASA 上のグローバル IP アドレスに設定されているからです。発信コールでは、着信側にインターネット上のどの IP アドレスでも指定できます。このため、ASA は、インターネット上の着信側の各グローバル IP アドレスに対し、ダイナミックに ASA 上の内部 IP アドレスを提供するマッピング サービスによって設定されます。

Cisco Unified Communications Manager は、発信コールすべてを、インターネット上の着信側のグローバル IP アドレスではなく、マッピングされた ASA 上の内部 IP アドレスに直接送ります。その後、ASA がコールを着信側のグローバル IP アドレスに転送します。

図 1-5 に、オフパス配置の Cisco Intercompany Media Engine のアーキテクチャを示します。

図 1-5　オフパス配置モデル



オフパス配置では、Cisco IME トランクを持つ Cisco Unified Communications Manager サーバのために、Cisco IME 配置をサポートする ASA への TCP 接続を開くことが必要です。この接続は、1024 ～ 65535 からランダムに選択されるポートに存在します。Cisco Unified Communications Manager サーバと ASA をサポートする Cisco IME との間に何らかのファイアウォールが存在する場合、ファイアウォールでこのポート範囲を開いておくことが必要です。

次の例に、サンプル ACL エントリを示します。

access-list SAMPLE extended permit tcp object-group CUCM object-group IME-ASA range 1024 65535

関連項目

- 「機能と利点」（P.1-1）
- 「動作」（P.1-2）
- 「配置モデル」（P.1-8）
- 「関連項目」（P.1-10）

CHAPTER 2

インストールと Cisco IME サーバの設定

この章では、Cisco Intercompany Media Engine サーバのインストールと設定について説明します。インストール手順を開始する前に、インストールについての指示すべてをよく確認してください。この章の構成は、次のとおりです。

重要な考慮事項

インストールを進める前に、次の要求事項と推奨事項について考慮してください。

- Cisco Unified Communications Manager サーバで、Cisco Unified Communications Manager ソフトウェアの互換性のあるバージョンが実行されていることを確認します。次の URL で、『*Cisco Unified Communications Manager Software Compatibility Matrix*』を参照してください。

  http://www.cisco.com/en/US/partner/docs/voice_ip_comm/cucm/compat/ccmcompmatr.html

- Cisco Unified Communications Manager サーバで NTP が有効になっていることを確認します。NTP ステータスを確認するには、Cisco Unified Communications Manager コマンド ライン インターフェイスにログインし、**utils ntp status** と入力します。

- 既存のサーバにインストールする場合、ハード ドライブはフォーマットされ、ドライブ上に存在するデータすべてが上書きされることに注意します。

- バックアップ電源によってシステムを保護できるよう、サーバが Uninterruptible Power Supply（UPS; 無停電電源装置）に接続されていることを確認します。このようにしなかった場合、物理メディアに損傷が生じて Cisco Intercompany Media Engine（Cisco IME）の新規インストールが必要となる可能性があります。

  Cisco IME ノードで UPS シグナリングを自動的に監視し、電源喪失時にグレースフル シャットダウンを自動で開始させるには、特定の UPS とサーバ モデルの使用が必要です。サポートされているモデルと設定についての詳細は、『*Release Notes for Cisco Intercompany Media Engine*』を参照してください。

- スタティック IP アドレスを使用してサーバを設定し、サーバが固定された IP アドレスを得られるようにします。
- インストール中、このサーバで DNS を有効にし、NTP を設定する必要があります。
- インストール中は、設定作業を実行しないでください。
- インストールが完了するまで、シスコで検証済みのアプリケーションはインストールしないでください。
- サーバ モデル 7825 I3（160 GB SATA ディスク ドライブ）のディスク ミラーリングには、約 3 時間かかります。
- インストールを進める前に、次の情報を注意深く読んでください。

インストールに関する FAQ

次の項では、一般的な質問と回答について取り上げます。インストールを始める前に、この項を注意深く読んでください。この項は、次の内容で構成されています。

インストールにはどれくらいの時間がかかりますか。

サーバ タイプによりますが、インストール前後の作業を除いたインストール プロセス全体で 20 ～ 30 分必要です。

どのようなユーザ名とパスワードを指定する必要がありますか。

（注）　システムはパスワードの強度をチェックします。強度の高いパスワード作成のガイドラインについては、「強度の高いパスワードとはどのようなパスワードですか。」（P.2-3）を参照してください。

インストール中、次のユーザ名とパスワードを指定する必要があります。

- 管理者アカウントのユーザ名とパスワード
- セキュリティ パスワード

管理者アカウントのユーザ名とパスワード

次の領域へのログインには、管理者アカウントのユーザ名とパスワードを使用します。

- ディザスタ リカバリ システム
- コマンド ライン インターフェイス

管理者アカウントのユーザ名とパスワードを指定するには、次のガイドラインに従います。

- 管理者アカウント ユーザ名：管理者アカウントのユーザ名には、英数字、ハイフン、アンダースコアを使用できますが、先頭は英字にします。
- 管理者アカウント パスワード：管理者アカウントのパスワードは、最低 6 文字とし、英数字、ハイフン、アンダースコアを使用できます。

コマンド ライン インターフェイスを使用して、管理者アカウント パスワードの変更や新規管理者アカウントの追加が行えます。詳しくは、『*Cisco Intercompany Media Engine Command Line Interface Reference Guide*』を参照してください。

セキュリティ パスワード

セキュリティ パスワードは最低 6 文字とします。英数字、ハイフン、アンダースコアを使用できます。

強度の高いパスワードとはどのようなパスワードですか。

インストール ウィザードは、入力されたパスワードの強度をチェックします。強度の高いパスワードを作成するには、次の推奨事項に従います。

- 大文字と小文字を混在させる。
- 英字と数字を混在させる。
- ハイフンやアンダースコアを含める。
- 長いパスワードは短いパスワードより強度が高く、セキュアになることに留意してください。

次のタイプのパスワードの使用は避けます。

- 固有名詞や辞書にある単語など、認識可能な単語は使用しない（数字と組み合わせた場合も含む）。
- 認識可能な単語を反転させたものは使用しない。
- aaabbb、qwerty、zyxwvuts、123321 のようにパターン化された単語や数字は使用しない。
- 他の言語で認識可能な単語は使用しない。
- いかなるものにしろ、誕生日、郵便番号、子供やペットの名前のような個人情報は使用しない。

Cisco Unified Communications アンサー ファイル ジェネレータとは何ですか。

Cisco Unified Communications アンサー ファイル ジェネレータは、Cisco Intercompany Media Engine の無人インストールのアンサー ファイルを生成するウェブ アプリケーションです。個別のアンサー ファイルは USB キーまたはフロッピーディスクのルート ディレクトリにコピーされ、インストール プロセスで Cisco Intercompany Media Engine DVD に加えて使用されます。

このウェブ アプリケーションには、次のような機能があります。

- データ エントリの構文検証
- オンライン ヘルプと資料
- 新規インストールのサポート（アップグレードはサポートしません）

Cisco Unified Communications アンサー ファイル ジェネレータは、次の URL でアクセスできます。

http://www.cisco.com/web/cuc_afg/index.html

Cisco Unified Communications アンサー ファイル ジェネレータは、Internet Explorer バージョン 6.0 以降および Mozilla バージョン 1.5 以降をサポートしています。

USB キーは、Linux 2.4 互換である必要があります。Cisco では、コンフィギュレーション ファイル用として、Linux 2.4 互換で事前にフォーマットされた USB キーを使用することを推奨します。これらのキーは W95 FAT32 フォーマットを使用します。

このインストールで、Cisco はどのようなサーバをサポートしていますか。

サポートされているサーバ モデルについては、ご使用の製品リリースのリリース ノートを参照してください。

Cisco はどのような SFTP サーバをサポートしていますか。

どのような SFTP サーバ製品でも使用できますが、Cisco では Cisco Technology Developer Partner（CTDP）プログラムで Cisco が認定した SFTP 製品を推奨します。GlobalSCAPE などの CTDP パートナーは、自社製品での特定のバージョンの Cisco Unified Communications Manager の使用を保証しています。ご使用のバージョンの Cisco Unified Communications Manager の自社製品での動作を保証しているベンダーについては、次の URL を参照してください。

http://www.cisco.com/pcgi-bin/ctdp/Search.pl

サポートされている Cisco Unified Communications バージョンの GlobalSCAPE での使用については、次の URL を参照してください。

http://www.globalscape.com/gsftps/cisco.aspx

シスコでは、次のサーバを内部テストに使用しています。これらのサーバのいずれかを使用できますが、サポートについてはベンダーにお問い合わせください。

- Open SSH（http://sshwindows.sourceforge.net/ を参照）
- Cygwin（http://www.cygwin.com/ を参照）
- Titan（http://www.titanftp.com/ を参照）

（注）　CTDP プロセスによる認証を受けていないサードパーティ製品との問題のサポートについては、サードパーティ ベンダーにお問い合わせください。

サーバに他のソフトウェアをインストールできますか。

ソフトウェアのインストールとアップグレードは、すべて Command Line Interface（CLI; コマンド ライン インターフェイス）で行う必要があります。システムがアップロードして処理できるのは、Cisco Systems 承認済みソフトウェアだけです。

未承認のサードパーティ ソフトウェア アプリケーションのインストールや実行はできません。

インストール前の作業

表 2-1 に、Cisco Intercompany Media Engine を確実にインストールするために必要なインストール前の作業のリストを示します。

表 2-1　インストール前の作業

	タスク	特記事項
ステップ 1	このマニュアル全体をよく読み、インストール手順についてよく理解してください。	
ステップ 2	Cisco は、Cisco IME のサイト分析と計画のセッションを完了しておくことを推奨します。これには、オフパス Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）の設定、IP アドレッシング、ピン ホール、スタティック Network Address Translation（NAT; ネットワーク アドレス変換）、Demilitarized Zone（DMZ; 非武装地帯）設定が含まれます。現在のネットワーク設定に適用される Cisco IME 要求事項について理解しておく必要があります。	*Cisco Unified Communications Manager:SRND*
ステップ 3	企業のファイアウォールで、必要なトラフィックを有効にします。 Cisco Intercompany Media Engine の設計と導入の早い段階で、企業のファイアウォールや DMZ の管理チーム（IT チームや情報セキュリティ チームなど）に参加しておく必要があります。Cisco IME コールの開始前に、企業のファイアウォールに必要な Access Control List（ACL; アクセス コントロール リスト）がすべて承認され、実装されているようにします。	「ネットワーク トラフィックの許可」（P.2-6）
ステップ 4	製造元が提供するユーティリティを実行して、すべての新規サーバ ハードウェアの整合性を検証します（ハードドライブやメモリなど）。	
ステップ 5	新規サーバを接続するスイッチ ポートの Network Interface Card（NIC; ネットワーク インターフェイス カード）の速度とデュプレックス設定を記録します。 サーバとスイッチ ポートの NIC 設定を同じにする必要があります。GigE（1000/FULL）の場合、NIC とスイッチ ポート設定は Auto/Auto にする必要があり、固定値は設定しません。	Cisco サーバに接続するスイッチポートすべてで PortFast を有効にします。PortFast を有効にすると、転送遅延をなくすことによりスイッチはポートをブロック状態から転送状態へすぐに変更します（転送遅延は、Spanning Tree Protocol（STP; スパニング ツリー プロトコル）ラーニングおよびリスニング ステートから転送ステートに変わるまでポートが待つ時間の長さを指します）。
ステップ 6	Cisco IME をインストール予定のサーバすべてが正しく DNS に登録されていることを確認します。	GoDaddy.com サーバと intercompanymedianetwork.com ブートストラップ サーバの解決と ping が実行できる必要があります。
ステップ 7	Cisco IME ライセンス ファイルを取得します。	「ライセンス ファイルの取得」（P.2-8）を参照してください。
ステップ 8	インストール予定の各サーバの設定値を記録します。	設定値の記録については、表 2-4 を参照してください。

追加情報

「関連項目」（P.2-29）

ネットワーク トラフィックの許可

この項では、IME トラフィックをサポートするために設定する必要がある、必要最低限のポートについて説明します。表 2-2 に、企業のファイアウォールに設定する必要があるポートの概要を示します。表 2-3 にオフパス ASA に設定する必要があるポートの概要を示します。これらの表中のポート設定は、デフォルト設定に基づいています。デフォルト設定を変更した場合、これらの設定を更新する必要があります。

ご使用のネットワークに他のサーバ/ポートが必要な場合、そのトラフィックの許可も必要です。

表 2-2　企業のファイアウォール設定

インターフェイス	方向	ソース	宛先	プロトコル	ポート	説明
内側	インバウンド	Cisco Unified CM IP アドレス	オフパス ASA 内部シグナリング アドレス（物理アドレスと同じ）	TCP	8060	Cisco Unified CM と ASA シグナリング アドレスとのオフパス マッピング。クラスタ内の各 Cisco Unified CM にエントリが必要。
内側	インバウンド	Cisco Unified CM IP アドレス	オフパス ASA 内部シグナリング アドレス（物理アドレスと同じ）	TCP	1024 ～ 65535	Cisco Unified CM と ASA シグナリング アドレスとのオフパス マッピング。クラスタ内の各 Cisco Unified CM にエントリが必要。
DMZ	インバウンド	オフパス ASA 内部シグナリング アドレス（物理アドレスと同じ）	Cisco Unified CM IP アドレス	TCP	5060	ASA シグナリング アドレスと Cisco Unified CM との間の SIP シグナリング。クラスタ内の各 Cisco Unified CM にエントリが必要。ポート番号設定可能。
内側	インバウンド	Cisco Unified CM IP アドレス	Cisco IME サーバ DMZ IP アドレス	TCP	5620	Cisco IME と Cisco Unified Communications Manager との間の VAP 通信
内側	インバウンド	ユニファイド コミュニケーション デバイスすべて（MeetingPlace、ボイスメール、ソフトクライアント IP 範囲、音声ゲートウェイ、ASA 経由の通信が必要なすべてのメディア デバイスを含む）	オフパス ASA 内部メディアの終端 IP	UDP	16384 ～ 32767	UDP ポートは、Cisco IME が有効な ASA メディアの終端アドレス設定および同時コール数に基づいて制限可能です。

表 2-2　企業のファイアウォール設定 （続き）

インターフェイス	方向	ソース	宛先	プロトコル	ポート	説明
DMZ	インバウンド	オフパス ASA 内部メディアの終端 IP （送信元ポート範囲は Cisco IME 設定に基づいて制限可能です）	ユニファイドコミュニケーション デバイスすべて（MeetingPlace、ボイスメール、ソフトクライアント IP 範囲、音声ゲートウェイ、ASA 経由の通信が必要なすべてのメディア デバイスを含む）	UDP	16384 ～ 32767	メディア トラフィックの UDP ポート。
内側	インバウンド	内部ネットワークまたはいずれかの管理ワークステーション	Cisco IME サーバ DMZ IP アドレス	TCP	22	ライセンス / ソフトウェアのアップロード、アップグレード、CLI アクセスのための Cisco IME サーバへの SFTP アクセス。
内側	インバウンド	内部ネットワークまたはいずれかの管理ワークステーション	Cisco IME サーバ DMZ IP アドレス	HTTPS	443	Cisco IME サーバからの RTMT ダウンロード。
DMZ	インバウンド	Cisco IME サーバ DMZ IP アドレス	GoDaddy Web サイト	HTTPS	443	GoDaddy からの証明書ダウンロード。
DMZ	インバウンド	Cisco IME サーバ DMZ IP アドレス	任意	TLS	6084	Cisco IME サーバからインターネットへのアウトバウンド IME 分散キャッシュ通信。
外側	インバウンド	任意	Cisco IME サーバ DMZ IP アドレス	TLS	6084	インターネットから Cisco IME サーバへのインバウンド IME 分散キャッシュ通信。
DMZ	インバウンド	Cisco IME サーバ DMZ IP アドレス	任意	TLS	8470	Cisco IME サーバからインターネットへのアウトバウンド IME 分散キャッシュ通信。
外側	インバウンド	任意	Cisco IME サーバ DMZ IP アドレス	TLS	8470	インターネットから Cisco IME サーバへのインバウンド IME 分散キャッシュ通信。

表 2-3　外部 Cisco IME ASA ファイアウォール（オフパス ASA）

インターフェイス	方向	ソースの説明	宛先の説明	プロトコル	ポート	説明
DMZ	インバウンド	Cisco Unified CM IP アドレス	リモート Cisco Unified CM	TCP	5560 ～ 5590	リモート Cisco Unified CM への内部 Cisco Unified CM シグナリング（リモート PAT 設定）。
DMZ	インバウンド	Cisco Unified CM IP アドレス	リモート Cisco Unified CM	TCP	5060	リモート Cisco Unified CM への内部 Cisco Unified CM シグナリング（リモート PAT 設定）。
外側	インバウンド	任意	Cisco Unified CM IP アドレス	TCP	5060	内部 Cisco Unified CM へのリモート Cisco Unified CM シグナリング。

追加情報

「インストール前の作業」（P.2-5）

ライセンス ファイルの取得

製品付属の Product Authorization Key（PAK; 製品認可キー）を使用して、Cisco IME サーバに必要なライセンスを取得できます。ライセンス ファイルには、Cisco IME のサポートされているバージョン、Cisco IME サーバの MAC アドレス、ライセンスされれた Cisco IME アプリケーション数（ピアカウント）、GoDaddy からの証明書取得に必要な情報（タグと署名）が含まれます。証明書によって、Cisco IME サーバが IME 分散キャッシュ リング上にある他の Cisco IME サーバへの TLS 接続を確立できるようになります。

例 2-1 に、Cisco IME ライセンス ファイルの例を示します。

例 2-1　ライセンス ファイルの例

```
INCREMENT IME_SERVICE cisco 8.0 permanent uncounted ¥
    VENDOR_STRING=<ime><peercount>5</peercount><tag>163d18ab727c0fa14fce75c6651b1362</tag>
    <signature>154fe09fdbb012407cbfac8c74c55cb6be460199c813b0af29b83bc3b10824519bef7427f7a
    be7a7b9e6692e9b905e73fa9a1199c90ef7fd269c89f0a9179677bbee34cb1eeb915f03e2372cb1e9d272d
    af907be0077c7fd128ecc0216f036bb9447f06857cdcb4b066e746dc80ebe33fc212117b5c6c95aa404751
    6120e403c320f703a9a94ac7c177a07963dd83aa79b75c1c585250481bce340ef3bf02f86633f245cbfaef
    c2a1851b29c6cf48f580655c8a983b65d5584e316f350a15ff90478cbcb8e39128049edbb6972b33203130
    00f28db28cc51a8eb7666a40184cb5389e216cdfeac7c1d42b0e4fdf2c608bea28faeff807fcc0862497dd
    59ca676</signature></ime><LicFileVersion>1.0</LicFileVersion> ¥
    HOSTID=00163569b2e0 ¥
    NOTICE="<LicFileID>20090730162506350</LicFileID><LicLineID>1</LicLineID> ¥
    <PAK></PAK>" SIGN="0288 1F4A 07D6 0C34 F35B D4D5 0339 C538 ¥
    AC1E BC65 8697 9D5F 18D3 A57D 27DD 18D2 8C3B 14BA E72F 4932 ¥
    E27D 7BE9 C410 5477 9B85 AAF7 2F42 8C44 0985 CFF1"
```

Cisco IME サーバのライセンス ファイルを取得するには、次の手順に従います。

手順

ステップ 1　Cisco Intercompany Media Engine に付属の Product Authorization Key（PAK; 製品認可キー）を、http://www.cisco.com/go/license にある License Registration Web ツールに入力します。

ステップ 2　[Submit] をクリックします。

ステップ 3　システム プロンプトの指示に従います。Cisco Intercompany Media Engine をインストール予定のサーバの Network Interface Card（NIC; ネットワーク インターフェイス カード）の MAC アドレスと、有効な電子メール アドレスを入力する必要があります。MAC アドレスを知るには、Cisco IME Command Line Interface（CLI; コマンド ライン インターフェイス）にログインし、**show status** と入力します。[License MAC] フィールドに MAC アドレスが表示されます。

システムは、入力された電子メール アドレス宛てに電子メールでライセンス ファイルを送信します。

ライセンス ファイルの形式は、IME<timestamp>.lic です。.lic 拡張子を保持していれば、ライセンス ファイルの名前を変更することもできます。ファイルの内容に何らかの編集を加えると、ライセンスは使用できなくなります。

ステップ 4　ライセンス ファイルは、ステップ 3 で入力した MAC アドレスに一致するサーバにアップロードする必要があります。「ライセンス ファイルのアップロード」（P.2-23）を参照してください。

追加情報

「インストール前の作業」（P.2-5）

インストールのための情報収集

表 2-4 を使用して、サーバについての情報を記録します。すべての情報を取得する必要はありません。ご使用のシステムとネットワーク設定に関連する情報だけを収集します。

（注）　一部のフィールドはオプションであり、ご使用の設定には適用されない場合があります。

注意　一部のフィールドは、いったんインストールすると、ソフトウェアを再インストールしない限り変更できません。入力する値はよく確認してください。

表の最後の列に、インストール後にフィールドを変更できるかが示されています。変更できる場合、そのための適切な Command Line Interface（CLI; コマンド ライン インターフェイス）コマンドも示されています。

表 2-4　サーバ設定データ

パラメータ	説明	インストール後の変更の可否
[管理者 ID(Administrator ID)] 入力内容：	このフィールドは、Cisco Intercompany Media Engine サーバ上の CLI へのセキュア シェル アクセスに使用する管理者アカウントのユーザ ID を指定します。	インストール後はエントリを変更できません。 **（注）**　インストール後に追加の管理者アカウントを作成することはできますが、元の管理者アカウントのユーザ ID は変更できません。

表 2-4　サーバ設定データ （続き）

パラメータ	説明	インストール後の変更の可否
[管理者パスワード (Administrator Password)] 入力内容：	このフィールドは、CLI へのセキュア シェル アクセスに使用する管理者アカウントのパスワードを指定します。 このパスワードは、adminsftp ユーザでも使用します。adminsftp ユーザは、ローカル バックアップ ファイルへのアクセスやサーバライセンスのアップロードなどに使用します。 パスワードは最低 6 文字とし、英数字、ハイフン、アンダースコアを使用するようにします。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set password admin**
[国 (Country)] 入力内容：	リストから、インストールに応じて適切な国を選択します。 **（注）** 入力した値は、Certificate Signing Request（CSR; 証明書署名要求）の生成に使用されます。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set web-security**
[DHCP] 入力内容：	Cisco は、[DHCP] オプションに [いいえ (No)] を選択するよう要求します。[いいえ (No)] を選択した後、ホスト名、IP アドレス、IP マスク、ゲートウェイを入力します。	インストール後にエントリを変更しないでください。
[DNS 有効 (DNS Enable)] 入力内容：	DNS サーバは、ホスト名を IP アドレスに、IP アドレスをホスト名に解決します。 Cisco IME では DNS サーバの使用が必須です。[はい (Yes)] を選択して、DNS を有効にします。	インストール後にエントリを変更しないでください。
[DNS プライマリ (DNS Primary)] 入力内容：	プライマリ DNS サーバとして指定する DNS サーバの IP アドレスを入力します。IP アドレスは、ドット付き 10 進表記形式（ddd.ddd.ddd.ddd）で入力します。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set network dns** DNS とネットワークの情報を参照するには、次の CLI コマンドを使用します。 CLI > **network eth0 detail**
[DNS セカンダリ (DNS Secondary)]（オプション） 入力内容：	セカンダリ DNS サーバ（オプション）として指定する DNS サーバの IP アドレスを入力します。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set network dns**
[ゲートウェイアドレス (Gateway Address)] 入力内容：	ネットワーク ゲートウェイの IP アドレスを入力します。 ゲートウェイがない場合でも、このフィールドには 255.255.255.255 を設定する必要があります。ゲートウェイがない場合、通信はご使用のサブネット上のデバイスだけに制限されます。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set network gateway**

表 2-4　サーバ設定データ （続き）

パラメータ	説明	インストール後の変更の可否
[ホスト名 (Hostname)] 入力内容：	サーバの一意なホスト名を入力します。 ホスト名は最大 64 文字で、英数字とハイフンを使用できます。ハイフンは先頭に使用できません。	インストール後にエントリを変更できます。 CLI > **set network hostname**
[IP アドレス (IP Address)] 入力内容：	ご使用のサーバの IP アドレスを入力します。	インストール後にエントリを変更できます。 CLI > **set network ip eth0** （注）　ネットワーク耐障害性が有効になっている場合、IP アドレスの変更前に set network failover dis と入力して無効にする必要があります。IP アドレス変更後、set network failover ena と入力してネットワーク耐障害性を再度有効にします。
[IP マスク (IP Mask)] 入力内容：	このマシンの IP サブネット マスクを入力します。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set network ip eth0**
[ロケーション (Location)] 入力内容：	サーバの場所を入力します。 システムは、サードパーティの証明書取得に使用する Certificate Signing Requests（CSR; 証明書署名要求）の生成にこの情報を使用します。 組織にとって意味のある任意の場所を入力できます。例ではサーバの所在する都道府県や都市を含めています。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set web-security**
[MTU サイズ (MTU Size)] 入力内容：	Maximum Transmission Unit（MTU; 最大伝送ユニット）は、ホストがネットワーク上で送信する最大のパケットをバイト単位で表します。 ご使用のネットワークの MTU サイズをバイト単位で入力します。ネットワークの MTU 設定がよくわからない場合、デフォルト値を使用します。 デフォルトでは 1500 バイトが指定されます。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set network mtu**
[NIC デュプレックス (NIC Duplex)] 入力内容：	Network Interface Card（NIC; ネットワーク インターフェイス カード）のデュプレックス モードを Full と Half から選択します。 （注）　このパラメータは、自動ネゴシエーションを使用しないよう選択した場合にだけ表示されます。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set network nic**

表 2-4　サーバ設定データ （続き）

パラメータ	説明	インストール後の変更の可否
[NIC スピード(NIC Speed)] 入力内容：	NIC のスピードを、10 メガビット毎秒と 100 メガビット毎秒から選択します。 **（注）** このパラメータは、自動ネゴシエーションを使用しないよう選択した場合にだけ表示されます。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set network nic**
[NTP サーバ(NTP Server)] 入力内容：	同期に使用する 1 つ以上の Network Time Protocol（NTP; ネットワーク タイム プロトコル）サーバのホスト名または IP アドレスを入力します。 NTP サーバは 5 つまで入力できます。 **（注）** 互換性、精度、およびネットワークジッタに関する潜在的な問題を回避するには、プライマリ ノードに指定した外部 NTP サーバが NTP v4（バージョン 4）である必要があります。IPv6 アドレッシングを使用している場合、外部 NTP サーバは NTP v4 である必要があります。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **utils ntp server**
[組織(Organization)] 入力内容：	組織の名前を入力します。 **ヒント** このフィールドを使用して、複数の組織ユニットを入力できます。複数の組織ユニット名を入力するには、エントリをカンマで区切ります。カンマを含むエントリの場合、エントリの一部に含まれるカンマの前にバックスラッシュを入力します。 **（注）** 入力した値は、Certificate Signing Request（CSR; 証明書署名要求）の生成に使用されます。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set web-security**
[セキュリティパスワード(Security Password)] 入力内容：	パスワードは、最低 6 文字の英数字である必要があります。パスワードにはハイフンとアンダースコアを使用できますが、先頭に使用できるのは英数字だけです。 **（注）** このパスワードを保存します。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set password security**
[都道府県(State)] 入力内容：	サーバの所在する都道府県を入力します。 **（注）** 入力した値は、Certificate Signing Request（CSR; 証明書署名要求）の生成に使用されます。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set web-security**

表 2-4　サーバ設定データ （続き）

パラメータ	説明	インストール後の変更の可否
[タイムゾーン (Time Zone)] 入力内容：	このフィールドは、現地タイム ゾーンと Greenwich Mean Time（GMT; グリニッジ標準時）からの差を指定します。 マシンの所在地に適したタイム ゾーンを選択します。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set timezone** 現在のタイム ゾーン設定を参照するには、次の CLI コマンドを入力します。 CLI > **show timezone config**
[ユニット (Unit)] 入力内容：	ユニットを入力します。 **（注）** 入力した値は、Certificate Signing Request（CSR; 証明書署名要求）の生成に使用されます。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set password admin**

追加情報

「インストール前の作業」（P.2-5）

インストールの開始

このセクションでは、オペレーティング システムと Cisco Intercompany Media Engine アプリケーションのインストール方法について説明します。オペレーティング システムとアプリケーションのインストールは、1 つのインストール プログラムを実行して行います。

インストール ウィザード内での移動方法については、表 2-5 を参照してください。

表 2-5　インストール ウィザードのナビゲーション

機能	キー
次のフィールドへ移動	**Tab**
前のフィールドへ移動	**Alt-Tab**
オプションの選択	Space または Enter
リスト内のスクロール	↑または↓
前のウィンドウに戻る	Space または Enter で [戻る (Back)] を選択（使用可能時）
ウィンドウについてのヘルプ表示	Space または Enter で [ヘルプ (Help)] を選択（使用可能時）

インストールを開始するには、次の手順に従います。

手順

ステップ 1　アンサー ファイル ジェネレータが生成した設定情報が入った USB キーがある場合、ここで USB キーを挿入します。

（注）　ソフトウェアがプレインストールされた新規サーバの場合、より新しい製品リリースでサーバの再イメージ化を行うのでない限り、DVD からインストールする必要はありません。直接 ステップ 9 に進めます。

ステップ 2　インストール DVD をトレイに入れてサーバを再起動し、DVD からサーバを起動します。サーバの起動シーケンス完了後、[DVD が見つかりました (DVD Found)] ウィンドウが表示されます。

ステップ 3　メディア チェックを実行する場合、[はい (Yes)] を選択します。メディア チェックをスキップする場合、[いいえ (No)] を選択します。

メディア チェックは DVD の整合性をチェックします。すでにメディア チェックに合格している DVD の場合、メディア チェックのスキップを選択できます。

ステップ 4　[はい (Yes)] を選択してメディア チェックを実行した場合、[メディアチェックの結果 (Media Check Result)] ウィンドウが表示されます。次の作業のいずれかを実行します。

a. [メディアチェックの結果 (Media Check Result)] に [合格 (Pass)] と表示された場合、[OK] を選択してインストールを継続します。

b. メディアがメディア チェックに不合格だった場合、Cisco.com から改めてダウンロードするか、別の DVD を Cisco から直接入手します。

ステップ 5　システム インストーラは次のハードウェア チェックを実行して、システムが正しく設定されていることを確認します。インストーラがハードウェア設定に何らかの変更を加える場合、システムの再起動を求めるプロンプトが表示されます。再起動中、DVD はドライブに入れたままにしておきます。

- 最初に、インストール プロセスは正しいドライバかどうかをチェックします。次の警告が表示される場合があります。

  ```
  No hard drives have been found.You probably need to manually choose device drivers for
  install to succeed.Would you like to select drivers now?
  ```

  インストールを継続するには、[はい (Yes)] を選択します。

- インストールでは次に、サポートされているハードウェア プラットフォームかどうかをチェックします。サーバがハードウェア要件を厳密に満たしていない場合、インストール プロセスに重大なエラーが発生して失敗します。この失敗が正常なものでないと思われる場合、エラーをキャプチャして Cisco サポートに報告します。
- インストール プロセスは次に、RAID 設定と BIOS 設定を確認します。

（注）　このステップが反復される場合、もう一度 [はい (Yes)] を選択します。

- インストール プログラムで BIOS 更新が必要な場合、システムの再起動が必要なことが通知されます。何かキーを押してインストールを継続します。

ハードウェアのチェックが完了すると、[製品配置の選択 (Product Deployment Selection)] ウィンドウが表示されます。

ステップ 6　[製品配置の選択 (Product Deployment Selection)] ウィンドウで、[OK] を選択します。

ステップ 7　ソフトウェアが現在サーバにインストールされている場合、[ハードドライブの上書き (Overwrite Hard Drive)] ウィンドウが表示され、ハード ドライブ上の現在のソフトウェアのバージョンと DVD 上のバージョンとが表示されます。インストールを継続する場合 [はい (Yes)] を、キャンセルする場合 [いいえ (No)] を選択します。

注意　[ハードドライブの上書き (Overwrite Hard Drive)] ウィンドウで [はい (Yes)] を選択した場合、ハード ドライブ上の既存のデータはすべて上書きされて消去されます。

[プラットフォームインストールウィザード (Platform Installation Wizard)] ウィンドウが表示されます。

ステップ 8　次のいずれかのオプションを選択します。

- 設定情報を手動入力し、インストール プログラムが設定されたソフトウェアをサーバへインストールするようにする場合、[続行 (Proceed)] を選択し、ステップ 12 に進みます。
- 次の作業のいずれかを行う場合、[スキップ (Skip)] を選択し、ステップ 9 に進みます。
  - サーバにプリインストールされたソフトウェアを手動で設定する：この場合、ソフトウェアのインストールは必要ありませんが、プリインストールされたソフトウェアの設定が必要です。
  - 無人インストールの実行：この場合、USB キーかフロッピーディスク上の既存の設定情報を準備します。
  - ソフトウェアをインストールしてから手動で設定する：この場合、インストール プログラムがソフトウェアをインストールし、手動設定を求めるプロンプトが表示されます。サーバにまずアプリケーションをプリインストールしておき、設定情報は後で入力する場合、[スキップ (Skip)] を選択します。この方法は、他の方法より時間がかかる場合があります。

ステップ 9　システムの再起動後、[既存のインストール設定 (Preexisting Installation Configuration)] ウィンドウが表示されます。

ステップ 10　アンサー ファイル ジェネレータで作成された既存の設定情報がある場合、情報はフロッピーディスクまたは USB キーに格納されます。ディスクまたは USB キーを挿入して、[続行 (Continue)] を選択します。インストール ウィザードは、インストール プロセスで設定情報を読み取ります。

（注）　システムが新しいハードウェアを検出したことを示すポップアップ ウィンドウが表示された場合、何かキーを押し、次のウィンドウで [インストール (Install)] を選択します。

[プラットフォームインストールウィザード (Platform Installation Wizard)] ウィンドウが表示されます。

ステップ 11　[プラットフォームインストールウィザード (Platform Installation Wizard)] を継続する場合、[続行 (Proceed)] を選択します。

ステップ 12　[基本インストール (Basic Install)] ウィンドウで、[続行 (Continue)] を選択し、DVD 上のソフトウェア バージョンをインストールするか、プリインストールされたソフトウェアを設定します。

ステップ 13　[タイムゾーン設定 (Timezone Configuration)] が表示されたら、サーバに適したタイム ゾーンを選択し、[OK] を選択します。

[自動ネゴシエーション設定 (Auto Negotiation Configuration)] ウィンドウが表示されます。

ステップ 14　インストール プロセスでは、イーサネット Network Interface Card（NIC; ネットワーク インターフェイス カード）の速度とデュプレックスの設定を自動ネゴシエーションによって自動設定するよう設定できます。この設定はインストール後に変更できます。

- 自動ネゴシエーションを有効にするには、[はい (Yes)] を選択し、ステップ 17 に進みます。

  [MTU 設定 (MTU Configuration)] ウィンドウが表示されます。

（注）　このオプションを使用する場合、ハブまたはイーサネット スイッチが自動ネゴシエーションに対応している必要があります。

- 自動ネゴシエーションを無効にする場合、[いいえ (No)] を選択し、ステップ 15 に進みます。

  [NIC スピードとデュプレックス設定 (NIC Speed and Duplex Configuration)] ウィンドウが表示されます。

ステップ 15　自動ネゴシエーション無効を選択した場合、ここで NIC の適切な速度とデュプレックス設定を選択し、[OK] を選択して継続します。

[MTU 設定 (MTU Configuration)] ウィンドウが表示されます。

ステップ 16　[MTU 設定 (MTU Configuration)] ウィンドウでは、MTU サイズをオペレーティング システムのデフォルトから変更できます。

Maximum Transmission Unit（MTU; 最大伝送ユニット）は、ホストがネットワーク上で送信する最大のパケットをバイト単位で表します。ネットワークの MTU 設定がよくわからない場合、デフォルト値として指定されている 1500 バイトを使用します。

注意　MTU サイズの設定が不適切な場合、ネットワークのパフォーマンスが低下する場合があります。

- デフォルト値（1500 バイト）を受け入れる場合、[いいえ (No)] を選択します。
- MTU サイズをオペレーティング システムのデフォルトから変更する場合、[はい (Yes)] を選択します。新しい MTU サイズを入力し、[OK] を選択します。

[DHCP 設定 (DHCP Configuration)] ウィンドウが表示されます。

ステップ 17　ネットワーク設定として、Cisco では Dynamic Host Configuration Protocol（DHCP; ダイナミック ホスト設定プロトコル）ではなく、サーバにスタティックなネットワーク IP アドレスを設定することを要求しています。DHCP を選択するかどうか尋ねられたときは、[いいえ (No)] を選択します。[スタティックネットワーク設定 (Static Network Configuration)] ウィンドウが表示されます。

ステップ 18　スタティックなネットワーク設定値を設定し、[OK] を選択します。フィールドの説明については、表 2-4 を参照してください。

[DNS クライアント設定 (DNS Client Configuration)] ウィンドウが表示されます。

ステップ 19　Cisco は、DNS を有効にすることを要求します。[はい (Yes)] を選択します。DNS クライアント情報を入力し、[OK] を選択します。フィールドの説明については、表 2-4 を参照してください。

新しい設定情報を使用してネットワークが再起動します。[管理者ログイン設定 (Administrator Login Configuration)] ウィンドウが表示されます。

ステップ 20　表 2-4 の管理者ログインとパスワードを入力します。

（注）　管理者ログインは先頭がアルファベットの 6 文字以上の文字列とし、英数字、ハイフン、アンダースコアを使用できます。コマンド ライン インターフェイスへのログインでは、管理者ログインが必要です。

[証明書情報 (Certificate Information)] ウィンドウが表示されます。

ステップ 21　証明書署名要求情報を入力し、[OK] を選択します。

[NTP クライアント設定 (Network Time Protocol Client Configuration)] ウィンドウが開きます。

ステップ 22　Cisco Systems では、正確なシステム時刻のため、外部 NTP サーバの使用を推奨します。外部 NTP サーバがストラタム 9 以上まで識別できる（つまり、ストラタム 1 ～ 9 を含む）ことを確認します。

外部 NTP サーバを設定するか、システム時刻を手動設定するかを選択します。

- 外部 NTP サーバをセットアップする場合、[はい (Yes)] を選択します。最低 1 つの NTP サーバの IP アドレス、NTP サーバ名または NTP サーバ プール名を入力します。NTP サーバは 5 つまで設定できます。Cisco Systems では、最低 3 つの NTP サーバを設定することを推奨します。[続行 (Proceed)] を選択してインストールを継続します。

システムは NTP サーバと接続し、自動でハードウェア クロックに時刻を設定します。

（注）　[テスト (Test)] ボタンが表示された場合、[テスト (Test)] を選択して NTP サーバにアクセスできるかどうかを確認できます。

- システム時刻を手動設定する場合、[いいえ (No)] を選択します。ハードウェア クロックに設定する適切な日付と時刻を入力します。[OK] を選択してインストールを継続します。

[セキュリティ設定 (Security Configuration)] ウィンドウが開きます。

ステップ 23　表 2-4 のセキュリティ パスワードを入力します。

（注）　セキュリティ パスワードは先頭が英数字の 6 文字以上の文字列とし、英数字、ハイフン、アンダースコアを使用できます。

[プラットフォーム設定の確認 (Platform Configuration Confirmation)] ウィンドウが開きます。

ステップ 24　インストールを継続する場合、[OK] を選択します。プラットフォーム設定を変更する場合、[戻る (Back)] を選択します。

システムがソフトウェアのインストールと設定を行います。DVD ドライブがイジェクトされ、サーバが再起動します。DVD を再挿入しないでください。

ステップ 25　インストール プロセスが完了すると、管理者アカウントとパスワードでログインするようプロンプトが表示されます。

ステップ 26　「インストール後の作業」（P.2-18）に記載されている、インストール後の作業を実行します。

追加情報

「関連項目」（P.2-29）

インストール後の作業

サーバにソフトウェアをインストールした後、表 2-6 にリストしたインストール後の作業を完了する必要があります。

表 2-6　インストール後の作業

設定手順		関連する手順と項目
ステップ 1	Real-Time Monitoring Tool をクライアント マシンにインストールします。	Real-Time Monitoring Tool を使用して、システムの稼動状態の監視や、ログの参照と収集が行えます。 Real-Time Monitoring Tool のインストール手順と詳しい情報については、「RTMT のインストール」（P.7-1）を参照してください。
ステップ 2	サーバに Cisco Intercompany Media Engine ライセンス ファイルをアップロードします。	「ライセンス ファイルのアップロード」（P.2-23）を参照してください。
ステップ 3	GoDaddy.com から Cisco Intercompany Media Engine 証明書を取得します。	「証明書の購入と登録」（P.2-23）および 「Cisco Intercompany Media Engine 証明書の手動更新」（P.2-25）を参照してください。

表 2-6　インストール後の作業 （続き）

設定手順		関連する手順と項目
ステップ 4	Cisco Unified Communications Manager と Cisco Intercompany Media Engine との間のセキュアな通信のために、自己署名またはサードパーティ製証明書にアクセスし、インストールします。	次のトピックを参照してください。 • 「Cisco Intercompany Media Engine サーバ上での自己署名証明書の生成とアップロード」（P.3-18） • 「Cisco Intercompany Media Engine 用のサードパーティ証明書の生成およびアップロード」（P.3-19）
ステップ 5	バックアップ設定を行います。 Cisco Intercompany Media Engine データは毎日バックアップするようにします。	「Cisco IME サーバのバックアップと復元」（P.5-1）を参照してください。
ステップ 6	Cisco IME サーバに、Cisco Unified Communications Manager と Cisco IME サーバとを接続して VAP シグナリングを交換可能な設定を作成する必要があります。 最初に、vapserver の名前とポートをセットアップします。	Cisco IME CLI にログインし、次のコマンドを入力します。 add ime vapserver vapserver の名前、ポート、認証モードの指定を求められます。ここで入力する名前が、このインスタンスの固有識別子となります。Cisco Unified Communications Manager の名前と一致させる必要はありません。選択する認証モードは、Cisco Unified Communications Manager と一致させる必要があります（暗号化済または認証済）。 **（注）** 同じ Cisco IME サーバを使用する複数の Cisco Unified Communications Manager がある場合、各クラスタに vapserver エントリを追加する必要があります。 各 vapserver 名につき、一意のポート番号を指定してください。 1 つのインスタンスを認証済モード用、もう 1 つを暗号化済および認証済モード用にした、複数の vapserver インスタンスを持つことができます。これらのインスタンスは、異なるポートを使用する必要があります。 コマンド オプションの詳細については、『*Cisco Intercompany Media Engine Command Line Interface Reference Guide*』を参照してください。
ステップ 7	管理する vapserver をすべて表示します。	Cisco IME CLI にログインし、次のコマンドを入力します。 show ime vapserver all

表 2-6　インストール後の作業 （続き）

設定手順		関連する手順と項目
ステップ 8	（オプション）設定した各 vapserver インスタンスについて、必要に応じてオプションを設定します。	Cisco IME CLI にログインし、次のコマンドを入力します。 • set ime vapserver authenticationmode • set ime vapserver enabled • set ime vapserver keepaliveinterval • set ime vapserver maxconnectionsallowed • set ime vapserver port **（注）** Cisco では、認証モードを*暗号化済*に設定することを強く推奨します。 コマンド オプションの詳細については、『*Cisco Intercompany Media Engine Command Line Interface Reference Guide*』を参照してください。
ステップ 9	VAP ユーザ クレデンシャルを Cisco IME サーバに設定します。	Cisco IME CLI にログインし、次のコマンドを入力します。 add ime vapusercredentials コマンド プロンプトがユーザ名とパスワードを尋ねます。 **（注）** 入力するアプリケーションのユーザ名とパスワードは、表 3-1 の ステップ 3 の Cisco Unified Communications Manager の管理 のアプリケーション ユーザに入力したものと一致している必要があります。 **（注）** チケットのパスワードと Epoch は、Cisco IME ASA で設定されたものと一致している必要があります。Cisco では、最低 20 文字のパスワードを作成することを推奨します。 コマンド オプションの詳細については、『*Cisco Intercompany Media Engine Command Line Interface Reference Guide*』を参照してください。

表 2-6　インストール後の作業 （続き）

設定手順		関連する手順と項目

ステップ 10	Cisco IME サーバがファイアウォール内にあり、公衆インターネットからサーバに到達するために Network Address Translation（NAT; ネットワークアドレス変換）が必要な場合、サーバが IME 分散キャッシュに参加可能になる前に Cisco IME サーバに外部アドレスを設定しておく必要があります。	1. Cisco IME CLI にログインし、次のコマンドを入力します。
		set ime addressing publicipaddrv4 *external ip addr*
		たとえば、Cisco IME のパブリック IP アドレスが 65.65.65.65 となる場合、次のように入力します。
		set ime addressing publicipaddrv4 65.65.65.65
		2. その後、次のコマンドを入力して設定を検証します。
		show ime addressing
		次の例では、Cisco IME サーバのパブリック IP アドレスとプライベート アドレスが表示されています。
		`admin: show ime addressing`
		`====================================`
		`Public IP Address = 65.65.65.65`
		`Private IP Address = 10.10.10.10`
		`DHT Port = 6084`
		`Validator Port = 8470`
		`====================================`

ステップ 11	Cisco IME サーバのピア ID のリストとブートストラップ サーバの IP アドレスが表示できることを確認します。	Cisco IME CLI にログインし、次のコマンドを入力します。 • show ime peerid ピア ID が表示されない場合、Cisco IME 証明書に問題がある可能性があります。設定を継続する前に、この問題を修正する必要があります。 • show ime bootstrap ip 最低 1 つの IP アドレスが表示されることを確認します。IP アドレスがまったく表示されない場合、Cisco IME が DNS 経由でブートストラップ サーバに接続できないことを意味します。

表 2-6　インストール後の作業 （続き）

設定手順		関連する手順と項目

ステップ 12	IME 分散キャッシュ上の Cisco IME サーバの状態を確認します。
	（注） サーバがリングに参加し、ステータスがグリーンに変わるまでに 20 分かかる場合があります。
		Cisco IME CLI にログインし、次のコマンドを入力します。
		show ime dht summary
		[DHT Health] フィールドに、[Peer ID] フィールドのサーバのステータスが表示されます。グリーンは正常動作状態を示します。
		`Peer ID = 514dd001c7553593ebefee2b076ad9d4`
		`DHT Health.....= GREEN`
		`BootStrap: 5619e12c7a647e1d3364c8a46c9e58f7`
		`Last Contact (sec)..... = 48`
		`Current Sequence.....= 1250036323`
		`Num.Tokens Received.....= 3`
		`Delay from BootStrap.....= 1`
		`Peer Count Distance.....= 5`
		ピア ID のステータスがグリーンで表示されない場合、Cisco IME 証明書が正しくインストールされていることを確認し、Cisco IME ポートと Cisco IME が有効な ASA をチェックします。
		show ime addressing コマンドを使用して、パブリック IP アドレスが正しく設定されたことを確認する必要がある場合もあります。

ステップ 13	Cisco では、お客様連絡先情報を設定しておくことを強く推奨します。この情報はご使用の Cisco IME サーバ上に保存され、Cisco テクニカル サポートが Cisco IME サーバの設定ミスを検出した場合に使用されます。	Cisco IME CLI にログインし、次のコマンドを入力します。 set ime customerinfo 次の情報を尋ねるプロンプトがシステムに表示されます。 • [会社名 (Company Name)] : Cisco IME サーバを使用する企業の名前 • [ユニット名 (Unit Name)] : 企業内のユニット（都市名や部門） • [都道府県 (State)] : サーバの位置する都道府県 • [国 (Country)] : サーバの位置する国 • [サポート担当者名 (Support Contact Name)] : ご使用の Cisco IME サーバで Cisco が設定ミスを検出した場合に連絡する担当者 • [サポート電子メール (Support Contact Email)] : 会社のサポート連絡先電子メール • [サポート電話番号 (Support Contact Phone)] : サポート連絡先電話番号 お客様情報の設定後、show ime customerinfo コマンドで情報を表示できます。

追加情報

「関連項目」（P.2-29）

ライセンス ファイルのアップロード

ライセンス ファイル要求時に入力した MAC アドレスと一致する Cisco IME サーバに対して、ライセンス ファイルをアップロードする手順は、次のとおりです。ライセンス ファイルの取得については、「ライセンス ファイルの取得」（P.2-8）を参照してください。

始める前に

サーバに Cisco IME サーバ ソフトウェアがインストールされていることを確認します。

手順

ステップ 1　Cisco IME ライセンス ファイル（.lic）を、ローカル ハード ドライブ上の一時ディレクトリに保存します。

ステップ 2　SFTP クライアントを開き、インストール中にセットアップした adminsftp ユーザと管理者パスワードを使用して Cisco IME サーバに接続します。

ステップ 3　**cd license** と入力してライセンス ディレクトリに移動し、このディレクトリにライセンス ファイルをコピーします。

ステップ 4　**put** <*license filename*> と入力します。ここで、<*license filename*> には電子メールで受け取ったライセンス ファイルの名前を指定します。

ステップ 5　Cisco IME Command Line Interface（CLI; コマンド ライン インターフェイス）にログインして **utils ime license file install <license filename>** と入力し、Cisco IME ライセンスをアップロードします。

（注）　受信するライセンス ファイルの形式は、IME<タイムスタンプ>.lic です。.lic 拡張子を保持していれば、ライセンス ファイルの名前を変更することもできます。ファイルの内容に何らかの編集を加えると、ライセンスは使用できなくなります。

インストール後、サーバはライセンス ファイルを /usr/local/ime/conf/licfiles に保存します。サーバはライセンス ログを /active/cm/trace/ime/licensing/log4j に保存します。

追加情報

「インストール後の作業」（P.2-18）

証明書の購入と登録

Cisco IME はサーバ間の通信を暗号化します。同一グループによって信頼された各サーバに証明書が必要となります。証明書への自己署名はできません。証明書により、Cisco IME サーバは IME 分散キャッシュ リング上の他の Cisco IME サーバと TLS 接続を確立できるようになります。

IME 分散キャッシュ リングの証明書は、GoDaddy が提供します。GoDaddy は、タグ、peerIDCount、署名など Cisco IME ライセンス内の情報を使用して各サーバを一意に識別し、証明書を生成します。

Cisco IME サーバ用の証明書は、GoDaddy の Web サイトで購入します。証明書購入後、GoDaddy に証明書を登録します。登録プロセスでは、証明書を取得可能な、有効なサーバがあることを示す情報を提供します。証明書は購入日から 1 年間有効です。

Cisco IME サーバは、有効期限日付の前に証明書の更新を試みます。自動登録に失敗した場合、サーバは EnrollFailure アラームを生成します。この場合、証明書の手動更新が必要です。証明書の更新の詳細については、「Cisco Intercompany Media Engine 証明書の手動更新」（P.2-25）を参照してください。

新規証明書の購入と登録は、次の手順に従います。

始める前に

ライセンスを Cisco IME サーバにインストールします。手順は 「ライセンス ファイルのアップロード」（P.2-23）に説明されています。

手順

ステップ 1　http://www.godaddy.com に移動します。

ステップ 2　アカウント マネージャにログインします。

ステップ 3　[使用している製品(My Products)] セクションで、[SSL 証明書(SSL Certificates)] を選択します。

ステップ 4　Cisco IME サーバ用のライセンスを購入します。

（注）　証明書購入について詳しくは、GoDaddy の Web サイト上にある Cisco Intercompany Media Engine 証明書の要求とインストールについてのサポート トピック（http://help.godaddy.com/article/5414）を参照してください。

購入プロセスでは、ご使用のサーバのサーバ ID の入力が必要です。この ID を入手するには、Cisco IME サーバの CLI にログインし、**show ime certenrollment server ID** と入力します。

ステップ 5　プロンプトが表示されたら、Cisco IME サーバ CLI に **utils ime certenrollment enroll** と入力して Cisco IME サーバに証明書をインストールします。

ステップ 6　登録に成功した場合、Cisco IME サーバは SuccessfulEnrollment アラートを生成します。失敗した場合、EnrollFailure アラートを生成します。

ステップ 7　Cisco IME サーバ上の証明書を表示するには、CLI に移動して **show cert own intercompanymedianetwork** と入力します。

（注）　システムは、手動登録と自動登録のログ ファイルを、ディレクトリ /active/platform/log/cli*.log と /active/platform/log/certm.log にそれぞれ保存します。

追加情報

「インストール後の作業」（P.2-18）

Cisco Intercompany Media Engine 証明書の手動更新

Cisco IME サーバを最初にインストールする場合、GoDaddy で証明書の購入と登録が必要です。「証明書の購入と登録」（P.2-23）に説明されています。証明書は購入日から 1 年間有効です。Cisco IME サーバは、有効期限日付の前に証明書の更新を試みます。自動登録に失敗した場合、サーバは EnrollFailure アラートを生成します。次の手順で証明書を手動更新する必要があります。

手順

ステップ 1　http://www.godaddy.com に移動します。

ステップ 2　アカウント マネージャにログインします。

ステップ 3　[使用している製品 (My Products)] セクションで、[SSL 証明書 (SSL Certificates)] を選択し、更新する証明書を探します。

（注）　証明書更新について詳しくは、GoDaddy の Web サイト上にある Cisco Intercompany Media Engine 証明書の更新についてのサポート トピック（http://help.godaddy.com/article/5415）を参照してください。

ステップ 4　GoDaddy が支払を受領すると、次のいずれかのイベントが発生します。

- GoDaddy が以前の証明書の期限前に支払を受領した場合、証明書が更新され、それ以上の作業は必要ありません。
- GoDaddy が以前の証明書の期限後に支払を受領した場合、Cisco IME サーバ CLI で **utils ime certenrollment enroll** と入力します。

ステップ 5　登録に成功した場合、Cisco IME サーバは SuccessfulEnrollment アラートを生成します。失敗した場合、EnrollFailure アラートを生成します。

ステップ 6　Cisco IME サーバ上の証明書を表示するには、CLI に移動して **show cert own intercompanymedianetwork** と入力します。

（注）　システムは、手動登録と自動登録のログ ファイルを、ディレクトリ /active/platform/log/cli*.log と /active/platform/log/certm.log にそれぞれ保存します。

追加情報

「インストール後の作業」（P.2-18）

管理者パスワードとセキュリティ パスワードのリセット

管理者パスワードやセキュリティ パスワードを紛失した場合、次の手順でこれらのパスワードをリセットします。

パスワードのリセット プロセス実行では、システム コンソールを介してシステムに接続している必要があります。つまり、サーバにキーボードとモニタを接続する必要があります。セキュア シェル セッションを介してシステムに接続している場合、パスワードはリセットできません。

（注）　この手順の間、システムに物理的にアクセスできることを証明するため、有効な CD または DVD をディスクドライブから取り出し、挿入することが必要になります。

手順

ステップ 1　次のユーザ名とパスワードでシステムにログインします。

- ユーザ名：pwrecovery
- パスワード：pwreset

[プラットフォームパスワードのリセットへようこそ (Welcome to platform password reset)] ウィンドウが表示されます。

ステップ 2　何かキーを押して継続します。

ステップ 3　ディスク ドライブに CD や DVD が入っている場合、ここで取り出します。

ステップ 4　何かキーを押して継続します。

システムは、CD や DVD をディスク ドライブから取り出したことをテストで確認します。

ステップ 5　ディスク ドライブに有効な CD または DVD を挿入します。

（注）　このテストでは、音楽 CD ではなくデータ CD を使用します。

システムはディスクが挿入されたことをテストで確認します。

ステップ 6　システムは、ディスクが挿入されたことを確認した後、次のオプションのいずれかを選択して継続するようプロンプトを表示します。

- 管理者パスワードを変更するには、a を入力します。
- セキュリティ パスワードを変更するには、s を入力します。
- 終了するには、q を入力します。

ステップ 7　選択したタイプの新しいパスワードを入力します。

ステップ 8　新しいパスワードを再入力します。

パスワードは、最低 6 文字ある必要があります。システムは新規パスワードの強度をチェックします。パスワードが強度チェックに合格しなかった場合、新しいパスワードを入力するよう求められます。

ステップ 9　システムが新しいパスワードの強度を確認すると、パスワードがリセットされます。何かキーを押してパスワード リセット ユーティリティを終了するようプロンプトが表示されます。

追加情報

「関連項目」（P.2-29）

Cisco Intercompany Media Engine ソフトウェアのアップグレード

アップグレード プロセスを開始する前に、Cisco.com から適切なアップグレード ファイルを入手しておく必要があります。

次の手順で、Cisco Intercompany Media Engine（Cisco IME）サーバ ソフトウェアをアップグレードします。

（注） Cisco IME をアップグレードする場合、Cisco Unified Communications Manager 上で Cisco IME サービスと通信するサービスは停止します。この停止により、Cisco Unified Communications Manager はアップグレードが完了し Cisco IME サーバが新しいリリースにスイッチされるまで一時的にルートの学習を停止します。この期間中、Cisco IME サービスがダウンしていることを示すアラートが Cisco Unified Communications Manager サーバに表示されます。Cisco Unified Communications Manager への影響を最小限にするため、Cisco では Cisco IME サーバのアップグレードをアクティブでない時間帯に行うことを強く推奨します。アップグレード手順には、約 20 ～ 30 分かかります。

手順

ステップ 1　Cisco Intercompany Media Engine サーバをアップグレードするためのアップグレード メディアを取得します。

Cisco.com からソフトウェア実行ファイルをダウンロードした場合、次のいずれかを実行します。

- 次のステップを実行して、ローカル ディレクトリからのアップグレードを準備します。
  - Cisco IME アップグレード ファイルをローカル ハード ドライブの一時ディレクトリにコピーします。
  - ダウンロードしたアップグレード ファイルを ISO イメージとして DVD に焼き付け、アップグレード ディスクを作成します。

    （注） .iso ファイルを DVD にコピーしても ISO イメージが作成されない場合、ご使用のサーバをその DVD でアップグレードすることはできません。ほとんどの商用ディスク作成アプリケーションは、ISO イメージ ディスクを作成できます。

  - SFTP クライアントを開き、インストール中にセットアップした adminsftp ユーザと管理者パスワードを使用して Cisco IME サーバに接続します。
  - **cd upgrade** と入力してアップグレード ディレクトリに移動し、ライセンス ファイルをそのディレクトリにコピーします。
  - **put** <*upgrade filename*> と入力します。ここで、<*upgrade filename*> には Cisco.com からダウンロードした、または DVD で入手したアップグレード ファイルの名前を指定します。
- アップグレード ファイルをアップグレード中のサーバからアクセス可能な FTP または SFTP サーバ上に置きます。

  シスコが準備したアップグレード ディスクがある場合、ディスクの内容をリモート サーバにコピーします。

  アップグレード ファイルをダウンロードした場合、ダウンロードしたファイルをリモート サーバにコピーします。

ステップ 2　DVD をサーバに挿入した後、もしくはアップグレード ファイルをリモート サーバやローカル ディレクトリにアップロードした後、Cisco IME CLI にログインし、**utils system upgrade initiate** と入力します。

ステップ 3　アップグレードするときのソースを次の中から選択します。

- 1：リモート ファイルシステム、SFTP 経由
- 2：リモート ファイルシステム、FTP 経由
- 3：ローカル DVD/CD
- 4：ローカル アップロード ディレクトリ

ステップ 4　選択したアップグレード オプションのシステム プロンプトに従います。

ステップ 5　システムは、アップグレード プロセス完了時にプロンプトを表示します。バージョンの自動切り替えオプションを選択しなかった場合、**utils system switch-version** と入力し、さらに **yes** と入力してサーバの再起動と新しいソフトウェア バージョンへの切り替えを承認します。

ステップ 6　インストールが完了したら、Cisco IME CLI にログインし、次の内容を確認します。

- Cisco IME CLI にログインし、**show ime dht summary** と入力して DHT がグリーンのヘルス ステータスを表示していることを確認します。サーバがリングに参加し、ステータスがグリーンに変わるまでに 20 分かかる場合があります。
- **show ime vapstatus summary** と入力して、[登録ステータス (Registration Status)] が [登録済み (Registered)] になり、[クライアント IP ADDR(Client IP ADDR)] が Cisco Unified Communications Manager サーバの IP アドレスと同じになっていることを確認します。

追加情報

「関連項目」（P.2-29）

インストールのトラブルシューティング

次のセクションを使用して、Cisco Intercompany Media Engine ソフトウェアのインストール中に発生する問題のトラブルシューティングを行います。

- 「インストール中のネットワーク エラーの処理」（P.2-28）
- 「ログ ファイルの調査」（P.2-29）

インストール中のネットワーク エラーの処理

インストール プロセスの間、インストール プログラムは入力されたネットワーク設定を使用してサーバがネットワーク接続に成功するかどうかを検証します。サーバに接続できない場合、メッセージが表示され、次のオプションのいずれかを選択するよう促されます。

- [RETRY]：インストール プログラムは再度ネットワーキングを検証します。検証に失敗すると、エラー ダイアログボックスが再度表示されます。
- [REVIEW (Check Install)]：このオプションでは、ネットワーキング設定の確認と変更が行えます。検出された場合、インストール プログラムはネットワーク設定のウィンドウに戻ります。

  ネットワーキングは各ネットワーキング ウィンドウの完了後に検証されるため、メッセージが複数回表示される場合があります。

- [停止 (HALT)]：インストールを停止します。ネットワーク設定のトラブルシューティングに役立てるため、インストール ログ ファイルを USB ディスクにコピーできます。
- [無視 (IGNORE)]：インストールを継続します。ネットワーキングのエラーのログが記録されます。場合によっては、インストール プログラムがネットワーキングを複数回検証することがあり、このエラー ダイアログボックスも複数回表示されます。ネットワーク エラーを無視して継続すると、インストールが失敗する場合があります。

追加情報

「関連項目」（P.2-29）

ログ ファイルの調査

インストールの問題が発生した場合、コマンド ライン インターフェイスで次のコマンドを入力してインストール ログ ファイルを調査できます。

コマンド ラインからインストール ログ ファイルのリストを取得するには、次のように入力します。

```
CLI>file list install *
```

コマンド ラインからログ ファイルを表示するには、次のように入力します。

```
CLI>file view install log_file
```

log_file にはログ ファイル名を指定します。

Real-Time Monitoring Tool を使用してログを表示することもできます。Real-Time Monitoring Tool の使用とインストールについて詳しくは、『*Cisco Unified Real Time Monitoring Tool Administration Guide*』を参照してください。

システム履歴ログを表示またはダウンロードすることで、インストール イベントの詳細情報を知ることができます。詳細については、次の資料を参照してください。

- 「システム履歴ログ」（P.10-1）
- 『*Cisco Unified Real Time Monitoring Tool Administration Guide*』の「Working with Trace and Log Central」の章

追加情報

「関連項目」（P.2-29）

関連項目

- 「重要な考慮事項」（P.2-1）
- 「インストールに関する FAQ」（P.2-2）
- 「インストール前の作業」（P.2-5）
- 「インストールの開始」（P.2-13）
- 「インストール後の作業」（P.2-18）
- 「管理者パスワードとセキュリティ パスワードのリセット」（P.2-26）
- 「インストールのトラブルシューティング」（P.2-28）

関連項目

CHAPTER 3

Cisco Unified Communications Manager の管理での Cisco IME の設定

Cisco Intercompany Media Engine（Cisco IME）を使用すると、お客様は、企業間直接 IP 接続を確立できます。Cisco IME サーバにソフトウェアをインストールしてインストール後の作業を実施した後で、Cisco Unified Communications Manager サーバを設定して Cisco Intercompany Media Engine 機能を使用可能にする必要があります。

ここでは、Cisco Unified Communications Manager の管理ページのユーザ インターフェイスの使用方法について説明し、Cisco Intercompany Media Engine 機能を使用するように Cisco Unified Communications Manager サーバを設定する詳細な手順を示します。この章は、次の内容で構成されています。

Cisco Unified Communications Manager の管理の基礎

Web ベースのアプリケーションである Cisco Unified Communications Manager の管理を使用して、Cisco Unified Communications Manager サーバの設定作業を実行します。ここでは、ナビゲーション メニュー、Cisco.com で Cisco Unified Communications Manager のドキュメントを検索するためのドキュメント検索機能など、グラフィカル ユーザ インターフェイスの基本要素について説明します。

詳細については、次のトピックを参照してください。

Cisco Unified Communications Manager の管理のグラフィカル ユーザ インターフェイスの使用

Cisco Unified Communications Manager の管理ページのインターフェイスには次のオプションがあります。

（注）　Cisco Unified Communications Manager の管理ページへのログインの詳細については、『*Cisco Unified Communications Manager アドミニストレーション ガイド*』を参照してください。

- [ナビゲーション (Navigation)] : ログインすると、Cisco Unified Communications Manager の管理ページのメイン ウィンドウが再表示されます。このウィンドウの右上には、[ナビゲーション (Navigation)] と呼ばれるドロップダウン リスト ボックスがあります。このドロップダウン リスト ボックスにあるアプリケーションにアクセスするには、必要なプログラムを選択し、[移動 (Go)] をクリックします。ドロップダウン リスト ボックスに表示されるオプションには、次の Cisco Unified Communications Manager アプリケーションが含まれます。
  - [Cisco Unified Communications Manager の管理 (Cisco Unified Communications Manager Administration)] : Cisco Unified Communications Manager にアクセスしたときに、デフォルトとして表示されます。システム パラメータ、ルート プラン、デバイスなどを設定するには、Cisco Unified Communications Manager の管理ページを使用します。
  - [Cisco Unified OS の管理 (Cisco Unified サービスアビリティ)] : Cisco Unified サービスアビリティのメイン ウィンドウが表示されます。Cisco Unified サービスアビリティ は、トレース ファイルおよびアラームを設定する場合や、サービスをアクティブ化および非アクティブ化する場合に使用します。
  - [Cisco Unified OS の管理 (Cisco Unified OS Administration)] : Cisco Unified オペレーティング システムの管理のメイン ウィンドウが表示され、Cisco Unified Communications Manager プラットフォームの設定と管理を行うことができます。このアプリケーションにログインするには、その前に他のすべてのアプリケーションからログオフする必要があります。

  - [ディザスタ リカバリ システム (Disaster Recovery System)] : Cisco ディザスタ リカバリ システムが表示されます。このプログラムは、Cisco Unified Communications Manager クラスタ内のすべてのサーバに対して、フル データ バックアップ機能および復元機能を提供します。このアプリケーションにログインするには、その前に他のすべてのアプリケーションからログオフする必要があります。

- [ドキュメントの検索 (Search Documentation)] : Cisco.com で現行のリリースの Cisco Unified Communications Manager のドキュメントを検索するには、このリンクをクリックします。[Cisco Unified CM のドキュメントの検索 (Cisco Unified CM Documentation Search)] ウィンドウが表示されます。検索する語句を入力し、[検索 (Search)] ボタンをクリックします。検索結果が表示されます。検索結果の上に表示される、ドキュメント タイプ変更ボタンを選択して、検索結果を絞り込むことができます (Unified CM のインストール/アップグレード、Unified CM Business Edition リリース ノートなど)。
- [バージョン情報 (About)] : Cisco Unified Communications Manager の管理ページのメイン ウィンドウが表示されて、システム ソフトウェア バージョンを確認できます。
- [ログアウト (Logout)] : Cisco Unified Communications Manager の管理アプリケーションからログアウトできます。ログイン フィールドのあるウィンドウが再表示されます。
- メニュー バー : インターフェイスの最上部にある水平バーには、メニューの名前が表示されます。メニュー オプションをクリックして、Cisco Unified Communications Manager の管理ページの各ウィンドウを表示します。このマニュアルでは、メニュー項目は [ ] で囲んで示しています。メニュー項目の選択の流れは、>（より大きい）記号を使用して示しています。たとえば、「[拡張機能 (Advanced Features)] > [Intercompany Media Service] > [サービス (Service)] を選択します」のように記述しています。

追加情報

「Cisco Unified Communications Manager の管理の基礎」（P.3-2）

Cisco Unified Communications Manager の管理のヘルプの使用方法

ヘルプにアクセスするには、Cisco Unified Communications Manager の管理ページのナビゲーション バーで [ヘルプ (Help)] メニューをクリックし、次のいずれかのオプションを選択します。

- [目次 (Contents)] : 新しいブラウザ ウィンドウが開き、Cisco Unified Communications Manager の管理のヘルプ システムのホーム ページが表示されます。[ヘルプ (Help)] ウィンドウの左側のペインにあるリンクを使用して、ヘルプ システムのすべてのトピックにアクセスできます。
- [このページ (This Page)] : Cisco Unified Communications Manager の管理のヘルプ システムの新しいブラウザ ウィンドウが開きます。ウィンドウの右側のペインには、Cisco Unified Communications Manager の管理ページの現在のウィンドウにある各フィールドの定義が表示されます。ほとんどの場合、現在のウィンドウに関連するその他のトピックが相互参照によって示されます。
- [バージョン情報 (About)] : Cisco Unified Communications Manager の管理ページのメイン ウィンドウが表示されて、システム ソフトウェア バージョンを確認できます。

ヘルプ システムの左側のペインには、ヘルプ システムに含まれるすべての製品ガイドの目次が表示されます。目次を展開すると、右側に表示されているヘルプ トピックの階層内での場所が示されます。

ヘルプの検索方法など、Cisco Unified Communications Manager の管理システムについての詳細は、[ヘルプ (Help)] ウィンドウの上部にある [ヘルプの使用方法 (Using Help)] リンクをクリックしてください。

追加情報

「Cisco Unified Communications Manager の管理の基礎」（P.3-2）

レコードの検索および削除

Cisco Unified Communications Manager を検索し、Cisco Unified Communications Manager の管理ページのウィンドウを使用してデータベースに追加したレコード、またはデフォルトのエントリとして存在するレコードを見つけることができます。レコードを検索するには、[電話の検索と一覧表示 (Find and List Phones)]（[デバイス (Device)] > [電話 (Phone)]）など、対象のレコードの検索と一覧表示ウィンドウに移動します。すべてのレコードを検索するか、検索条件を入力して検索結果を絞り込むことができます。検索パラメータは、検索するレコードによって異なります。たとえば、電話を検索する場合は、電話番号に特定の番号が含まれる電話やデバイス名に特定の文字が含まれる電話を検索できます。エンド ユーザを検索する場合は、特定の文字が含まれる姓または名を検索できます。

見つかったレコードは、そのレコードが表示されている検索と一覧表示ウィンドウから削除できます。個々のレコードを削除することも、ウィンドウ内の全レコードを削除することもできます。

Cisco Unified Communications Manager の管理ページからレコードを検索および削除する手順は、次のとおりです。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで、対象のコンポーネントの検索と一覧表示ウィンドウに移動します。たとえば、電話を検索する場合は、[デバイス (Device)] > [電話 (Phone)] を選択して、[電話の検索と一覧表示 (Find and List Phones)] ウィンドウを表示します。

ステップ 2　データベース内のすべてのレコードを検索するには、ダイアログボックスが空になっていることを確認し、ステップ 3 に進みます。

ステップ 3　レコードをフィルタリングまたは検索するには、次の手順を実行します。

- 最初のドロップダウン リスト ボックスで、検索パラメータを選択します。検索パラメータは、検索の実行対象となるフィールドを表します。検索パラメータは、レコードのタイプによって異なります。
- 2 番目のドロップダウン リスト ボックスで、検索パターンを選択します。検索パターンによって、レコードの検索方法が定義されます。たとえば、検索テキスト フィールドで指定する特定の値を含むレコード（検索パラメータ）を検索できます。
- 必要に応じて、適切な検索テキストを指定します。検索テキストによって、検索する値を指定できます。このフィールドは、検索パラメータ フィールドおよび検索パターン フィールドとあわせて使用します。たとえば、検索パラメータ ドロップダウン リスト ボックスから [電話番号 (Directory Number)] を選択し、検索パターン ドロップダウン リスト ボックスから [が次の文字列を含む (contains)] を選択し、検索テキストとして 5551212 を入力した場合、5551212 という番号を含む電話番号が検索されます。

（注）　別の検索条件を追加するには、[+] ボタンをクリックします。条件を追加した場合は、指定したすべての条件に一致するレコードが検索されます。条件を削除するには、[–] ボタンをクリックして最後に追加した条件を削除するか、[フィルタのクリア (Clear Filter)] ボタンをクリックして追加したすべての検索条件を削除します。

ステップ 4　[検索 (Find)] をクリックします。

一致するすべてのレコードが表示されます。

[ページあたりの行数 (Rows per Page)] ドロップダウン リスト ボックスから異なる値を選択すると各ページに表示される項目数を変更できます。

リストの見出しに上矢印または下矢印がある場合は、その矢印をクリックして、ソート順序を逆にすることができます。

（注）　該当するレコードの横にあるチェックボックスをオンにして [選択項目の削除 (Delete Selected)] をクリックすると、複数のレコードをデータベースから削除できます。この選択方法ですべての設定可能なレコードを削除するには、チェックボックスの列の一番上にあるチェックボックスをクリックしてから [選択項目の削除 (Delete Selected)] をクリックします。

ステップ 5　表示されたレコード リストから、目的のレコードのリンクをクリックします。

選択した項目がウィンドウに表示されます。

追加情報

「Cisco Unified Communications Manager の管理の基礎」（P.3-2）

レコードの追加およびコピー

Cisco Unified Communications Manager の管理ページで新しいレコードを作成したり、既存のレコードをコピーしたりすることによって、Cisco Unified Communications Manager に項目を追加できます。データベースにレコードを追加またはコピーする手順は、次のとおりです。

手順

ステップ 1　Cisco Unified Communications Manager の管理ページで、追加（またはコピー）するコンポーネントの検索と一覧表示ウィンドウに移動します。たとえば、信頼要素を追加するには、[拡張機能 (Advanced Features)] > [Intercompany Media Services] > [信頼要素 (Trust Element)] を選択して、[Intercompany Media Service の信頼要素の検索と一覧表示 (Find and List Intercompany Media Services Trust Elements)] ウィンドウを表示します。

ステップ 2　新しいレコードを追加する場合は、[新規追加 (Add New)] ボタンをクリックします。

ウィンドウが更新され、新しいレコードが表示されます。必要な変更を行い、[保存 (Save)] をクリックします。

ステップ 3　既存のレコードをコピーするには、次のいずれかを行います。

- [検索と一覧表示 (Find and List)] ウィンドウで、使用可能であれば、[コピー (Copy)] ボタンをクリックします。
- 「レコードの検索および削除」（P.3-4）の説明に従って、コピーするレコードを検索します。レコードを選択し、設定ウィンドウの [コピー (Copy)] ボタンをクリックします。たとえば、コピーする信頼要素レコードを検索し、[信頼要素の設定 (Trust Element Configuration)] ウィンドウの [コピー (Copy)] ボタンをクリックします。

ウィンドウが更新され、新しいレコードが表示されます。必要な変更を行い、[保存 (Save)] をクリックします。

ステップ 4　既存のレコードをコピーし、既存のレコードから関連するすべての情報を新しいレコードに入力するには、次の手順を実行します。

- [検索と一覧表示 (Find and List)] ウィンドウで、使用可能であれば、[スーパーコピー (Super Copy)] ボタンをクリックします。
- 「レコードの検索および削除」（P.3-4）の説明に従って、コピーするレコードを検索します。レコードを選択し、設定ウィンドウの [スーパーコピー (Super Copy)] ボタンをクリックします。たとえば、コピーする電話レコードを検索し、[電話の設定 (Phone Configuration)] ウィンドウの [スーパーコピー (Super Copy)] ボタンをクリックします。

ウィンドウが更新され、新しい [デバイス名 (Device Name)] フィールドが表示されます。必要な変更を行い、[保存 (Save)] をクリックします。

追加情報

「Cisco Unified Communications Manager の管理の基礎」（P.3-2）

Cisco IME の設定チェックリスト

表 3-1 は、Cisco Unified Communications Manager の管理で、Cisco Intercompany Media Engine（Cisco IME）機能を設定する手順の概要を示しています。

（注）　始める前に、Cisco Intercompany Media Engine ソフトウェアをサーバにインストールして、ライセンス ファイルのアップロードや証明書の登録などのインストール後の作業を実行したことを確認してください。「インストールと Cisco IME サーバの設定」（P.2-1）を参照してください。

表 3-1　Cisco IME の設定チェックリスト

設定手順		関連する手順と項目
ステップ 1	適切な Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）ライセンスがあることを確認します。	詳しくは、『*Cisco Unified Communications Manager Software Compatibility Matrix*』（http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/compat/ccmcompmatr.html）を参照してください。

表 3-1　Cisco IME の設定チェックリスト（続き）

設定手順		関連する手順と項目
ステップ 2	Cisco IME トランクが何らかの原因で故障した場合に、コールが入力ゲートウェイ デバイスにすぐに再ルーティングされるようにするには、[SIP INVITE の再試行数 (Retry Count for SIP Invite)] サービス パラメータに小さい値を設定します。原因としては、TCP 接続のタイムアウトや、オフパス ASA のオフライン化などが考えられます。 このパラメータの値は、2 に設定することをお勧めします。 **ヒント** UDP トランクがあるかどうかを確認するには、SIP セキュリティ プロファイルのトランスポート タイプを調べます（[システム (System)] > [セキュリティ (Security)] > [SIP トランクセキュリティプロファイル (SIP Trunk Security Profile)]）。 デフォルト値の 6 のままにしたときに ASA で障害が発生すると、Cisco Unified Communications Manager で Cisco IME コールを PSTN に戻すまで、最大 1 分かかります。 **（注）** [SIP INVITE の再試行数 (Retry Count for SIP Invite)] サービス パラメータは、Cisco Unified Communications Manager サーバに設定するすべての SIP トランクに適用されます。	1. [システム (System)] > [サービスパラメータ (Service Parameters)] を選択します。 2. [Server] ドロップダウン リスト ボックスから、適切なサーバを選択します。 3. [サービス (Service)] ドロップダウン リスト ボックスから Cisco CallManager サービスを選択します。 4. [SIP INVITE の再試行数 (Retry Count for SIP Invite)] サービス パラメータの値に、適切な値を設定します。 5. [保存 (Save)] をクリックします。

表 3-1　Cisco IME の設定チェックリスト（続き）

設定手順		関連する手順と項目
ステップ 3	Cisco Unified Communications Manager の管理でアプリケーション ユーザを作成します。 Cisco Unified Communications Manager では、Cisco Unified Communications Manager で Cisco IME サービスをアクティブ化するときに、アプリケーション ユーザ名およびパスワードの設定を使用します。 Cisco Unified Communications Manager は、Cisco IME サーバの IP アドレスおよびポートを取得して、そのサーバのアプリケーション ユーザ名およびパスワードの設定を検査します。Cisco Unified Communications Manager は、セキュリティ設定および Cisco IME サービスのアプリケーション ユーザ情報も検査します。 Cisco Unified Communications Manager は、TCP を使用して、Cisco IME サーバへの接続を開始します。セキュリティ モードで暗号化が指定されている場合は、TLS 接続が確立されます。この TLS 接続では、インストール時に Cisco Unified Communications Manager 用に作成される自己署名証明書が使用されます。 Cisco IME サーバ用の証明書は、Cisco Unified Communications Manager サーバ上の信頼ストアに存在する必要があります。 Cisco Unified Communications Manager ノードは、信頼ストアにある Cisco IME サーバからのすべての証明書を受け入れます。接続が確立されると、Cisco Unified Communications Manager は、Cisco IME サービス用のアプリケーション ユーザのユーザ ID およびパスワードを含む REGISTER メッセージを送信します。Cisco IME サーバは、設定されているユーザ名およびパスワードに対して、このクレデンシャルを検査します。	Cisco Unified Communications Manager の管理ページで、[ユーザ管理(User Management)] > [アプリケーションユーザ(Application User)] を選択して、[新規追加(Add New)] をクリックします。add vapusercredentials CLI コマンドを使用して Cisco IME サーバに設定した VAP ユーザ名とパスワードを、[アプリケーションユーザの設定(Application User Configuration)] ウィンドウの [ユーザ ID(User ID)] フィールドと [パスワード(Password)] フィールドに入力します（表 2-6 のステップ 9 を参照）。 [アプリケーションユーザの設定(Application User Configuration)] ウィンドウの他のフィールドは、デフォルト値に設定されたままにします。 [アプリケーションユーザ(Application User)] ウィンドウで入力するユーザ名とパスワードの値が Cisco IME サーバ上の VAP ユーザ名およびパスワードの値と一致しない場合は、Cisco Unified Communications Manager サーバを Cisco IME サーバに登録できません。 **（注）** アプリケーション ユーザとサーバの関連付けは、このチェックリストで後述するように、[Intercompany Media Engine サーバ接続の設定(Intercompany Media Engine Server Connection Configuration)] ウィンドウで行います。

表 3-1　Cisco IME の設定チェックリスト（続き）

設定手順		関連する手順と項目
ステップ 4	Cisco Intercompany Media Engine 対応の ASA に接続するための正しい SIP リスニング ポートおよびセキュリティ モードが SIP セキュリティ プロファイルに指定されていることを確認します。[Out-of-Dialog REFER の許可 (Accept Out-of-Dialog REFER)] チェックボックスをオンにします。 （注）　[Out-of-Dialog REFER の許可 (Accept Out-of-Dialog REFER)] チェックボックスをオンにして、PSTN への通話中のフォールバックを許可する必要があります。	1. [システム (System)] > [セキュリティ (Security)] > [SIP トランクセキュリティプロファイル (SIP Trunk Security Profile)] の順に選択します。 2. [デバイスセキュリティモード (Device Security Mode)] ドロップダウン リスト ボックスから選択する値によって、ASA に接続できることを確認します。この値は、ASA 上に設定した値と一致する必要があります。 3. Cisco Unified Communications Manager で ASA と通信するために使用するポートの正しい値が [着信ポート (Incoming Port)] フィールドに入力されていることを確認します。デフォルトでは、Cisco Unified Communications Manager は、ポート 5060 を使用します。デフォルト以外のポートを使用している場合は、そのポートをここに入力する必要があります。 4. [Out-of-Dialog REFER の許可 (Accept Out-of-Dialog REFER)] チェックボックスをオンにします。 5. Unsolicited NOTIFY、Replaces ヘッダー、プレゼンスの SUBSCRIBE を Cisco IME トランクに許可し、セキュリティステータスを送信できるようにするには、[SIP トランクセキュリティプロファイルの設定 (SIP Trunk Security Profile Configuration)] ウィンドウの対応するチェックボックスをオンにします。

表 3-1　Cisco IME の設定チェックリスト（続き）

設定手順		関連する手順と項目
ステップ 5	Cisco Intercompany Media Engine と組み合わせて使用する SIP トランクを設定します。 IME SIP トランクは、固定の宛先 IP アドレスおよびポートを持ちません。トランクでは、代わりに、Cisco IME ネットワークを介して Cisco Unified Communications Manager が学習するルーティング情報から、リモート IP アドレスおよびポートを取得します。 IME SIP トランクでは IPv6 をサポートしていないため、IME トランクでは IPv4 のみが指定されていることを確認してください。IPv6 が有効化されていないシステムの場合は、この問題に該当しません。 **（注）** このチェックリストの後述の手順で、このトランクを IME サービスと関連付けます。	1. [デバイス (Device)] > [トランク (Trunk)] の順に選択し、[新規追加 (Add New)] をクリックします。 2. [トランクタイプ (Trunk Type)] ドロップダウン リスト ボックスで [SIP トランク (SIP Trunk)] を選択します。 3. [トランクサービスタイプ (Trunk Service Type)] ドロップダウン リスト ボックスで [Cisco Intercompany Media Engine] を選択します。 4. [次へ (Next)] ボタンをクリックします。 5. 次の考慮事項に従ってトランクを設定します。 Cisco IME コールの場合、着信の発信者番号および着信者番号では、常に +E.164 番号形式、つまり、「+」から始まるグローバル化された番号を指定します。Cisco Unified Communications Manager ダイヤル プランおよびルーティング アーキテクチャによっては、Cisco Unified Communications Manager 内で着信番号をルーティングできるように、発信者番号および着信者番号のトランスフォーメーションまたはトランスレーション パターンを定義する必要があることがあります。そうしない場合、着信 Cisco IME コールは、番号分析エラーによって失敗します。 たとえば、ゲートウェイ レベルで先行「+」を発信者番号から削除して、コールを Cisco Unified Communications Manager 内でルーティングできるようにする必要があることがあります。 必要なトランスフォーメーションを設定するには、[インバウンドコール (Inbound Calls)] グループ ボックス内のフィールドを設定します。 6. トランクを再起動します。 トランクの設定の詳細については、『*Cisco Unified Communications Manager アドミニストレーション ガイド*』を参照してください。
ステップ 6	Cisco IME コールで保留音を使用可能にするには、Cisco CallManager の Duplex Streaming Enabled サービス パラメータを True に設定する必要があります。このパラメータによって、保留音およびアナンシエータでデュプレックス ストリーミングを使用するかどうかが決まります。	1. [システム (System)] > [サービスパラメータ (Service Parameters)] を選択します。 2. [サーバ (Server)] ドロップダウン リスト ボックスで、サーバを選択します。 3. [サービス (Service)] ドロップダウン リスト ボックスで、Cisco CallManager サービスを選択します。 4. Duplex Streaming Enabled パラメータを [はい (True)] に設定します。

表 3-1　Cisco IME の設定チェックリスト（続き）

設定手順		関連する手順と項目
ステップ 7	VAP 通信で使用する IP アドレスとポートなど、Cisco Unified Communications Manager が接続する Cisco IME サーバに関する情報を指定します。	「Cisco IME サーバ接続の設定」（P.3-15）。
ステップ 8	ステップ 7 で、Cisco IME サーバについて [暗号化済および認証済 (Encrypted and Authenticated)] セキュリティ モードを選択した場合は、サードパーティの証明書または自己署名証明書を使用して、Cisco Intercompany Media Engine サーバと Cisco IME サーバの間に TLS 接続を設定する必要があります。	「Cisco Unified Communications Manager と Cisco Intercompany Media Engine サーバの間の TLS 接続の設定」（P.3-17）
ステップ 9	登録済みパターンの割り当て先として使用できる登録済みグループを作成します。登録済みパターンは、Cisco IME コールに加わることができる番号を指定します。登録済みグループは、登録済みパターンの集合を指定します。 登録済みグループを作成した後で登録済みパターンを作成して、パターンをグループに割り当てます（ステップ 10 を参照）。 **ヒント** 登録済みグループを一括で設定する方法の詳細については、『*Cisco Unified Communications Manager Bulk Administration ガイド*』を参照してください。	「Cisco IME 登録済みグループの設定」（P.3-21）
ステップ 10	登録済みパターンを作成して、Cisco IME コールの送信および受信を許可する、一連の +E.164 番号を指定します。	「Cisco IME 登録済みパターンの設定」（P.3-22）
ステップ 11	Cisco IME を使用させない番号と関連付ける除外グループを作成します （オプション）。 **ヒント** 除外済みグループを一括で設定する方法の詳細については、『*Cisco Unified Communications Manager Bulk Administration ガイド*』を参照してください。	「Cisco IME 除外グループの設定」（P.3-24）
ステップ 12	アナログ デバイスの番号やファクス機の番号など、Cisco IME を使用させない番号を指定します。ステップ 11 で作成した除外グループと除外番号を関連付けます。	「Cisco IME 除外番号の設定」（P.3-24）
ステップ 13	Cisco IME で信頼する信頼要素（ドメインおよびプレフィックス）または信頼しない信頼要素を割り当てることができる、信頼グループを作成します （オプション）。 **（注）** 信頼グループを設定していない場合、Cisco IME では、すべてのプレフィックスおよびドメインを信頼します。 **ヒント** 信頼グループを一括で設定する方法の詳細については、『*Cisco Unified Communications Manager Bulk Administration ガイド*』を参照してください。	「Cisco IME 信頼グループの設定」（P.3-25）

表 3-1　Cisco IME の設定チェックリスト（続き）

設定手順		関連する手順と項目
ステップ 14	信頼するプレフィックスまたはドメインか、信頼しないプレフィックスまたはドメインを指定して、この信頼要素を信頼グループと関連付けます。Cisco IME コールは、信頼要素に対してのみ行うことができます。 **ヒント** 信頼要素を一括で設定する方法の詳細については、『*Cisco Unified Communications Manager Bulk Administration ガイド*』を参照してください。	「Cisco IME 信頼要素の設定」（P.3-26）
ステップ 15	Cisco IME サービスを設定します。このサービスは、SIP トランク、信頼グループ、除外グループ、および登録済みグループなど、この Cisco IME インスタンスで使用する要素を定義します。	「Cisco IME サービスの設定」（P.3-27）
ステップ 16	クラスタ内の各 Cisco Unified Communications Manager 用の外部 IP アドレスおよびポートを定義し、このアドレスを Cisco IME サービスと関連付けます。	「外部 IP アドレスおよびポート情報の設定」（P.3-30）
ステップ 17	発信側および着信側のトランスフォーメーション パターンを設定します。 **（注）** トランスフォーメーションの適用とトランクのリセットは、必ず、メンテナンス期間中に行ってください。	「Cisco IME 用トランスフォーメーション パターンの設定」（P.3-31）
ステップ 18	着信発信者番号に 1 つと、着信着信者番号に 1 つの、2 つのトランスフォーメーション プロファイルを設定します。 システムでは、トランスフォーメーション プロファイルを使用して、着信コールの発信者番号および着信者番号を完全修飾 +E.164 番号形式に変換できます。 プロファイルは、ステップ 19 で説明されている Cisco IME トランスフォーメーションと関連付けます。 変換された番号は、Cisco IME で PSTN コールを検証するために使用する、Voice Call Records（VCRs; 音声コール レコード）に格納されます。	「Cisco IME トランスフォーメーション プロファイルの設定」（P.3-31）
ステップ 19	Cisco IME +E.164 トランスフォーメーションを設定します。トランスフォーメーションでは、PSTN コールの終了後に発呼側と終端側（着信側と発信側）の両方で、発信者番号および着信者番号を +E.164 形式に変換します。 ステップ 20 では、このトランスフォーメーションをシステム内のすべての PSTN アクセス トランクと関連付けます。	「Cisco IME E.164 トランスフォーメーションの設定」（P.3-37）
ステップ 20	VCR を Cisco IME サーバに送信できるように、トランクを設定します。PSTN に到達する可能性のあるコールを処理するすべてのトランクを設定する必要があります。	「PSTN アクセス トランクの設定」（P.3-39）

表 3-1　Cisco IME の設定チェックリスト（続き）

設定手順		関連する手順と項目
ステップ 21	Cisco IME に適用される機能パラメータを確認し、必要に応じて変更を加えます。たとえば、[ドメイン内 IME の有効化 (Enable Intradomain IME)] 機能パラメータのデフォルト値を変更する必要があることがあります。他の機能パラメータのデフォルト値は、大部分の設定について実用的です。	「Cisco IME 機能設定の入力」（P.3-39）
ステップ 22	（オプション）特定のデバイスまたはトランクで Cisco IME コールを発信できないようにする場合は、発信コールに対して Cisco IME をオフにした共通デバイス設定を作成し、この共通デバイス設定をデバイスと関連付けます。 **（注）** [Intercompany Media Service 機能設定 (Intercompany Media Services Feature Configuration)] ウィンドウ（[拡張機能 (Advanced Features)] > [Intercompany Media Services] > [機能設定 (Feature Configuration)]）で Cisco Intercompany Media Engine を使用不可にしたうえで、関連付けられたデバイスに対して Cisco IME を使用可能にする共通デバイス設定を作成することもできます。	1. [デバイス (Device)] > [デバイスの設定 (Device Settings)] > [共通デバイス設定 (Common Device Configuration)] の順に選択します。 2. 共通デバイス設定を作成します。この共通デバイス設定と関連付けられたデバイスに対して Cisco IME を使用不可にするには、[アウトバウンドコールに Intercompany Media Engine(IME) を使用 (Use Intercompany Media Engine (IME) for Outbound Calls)] ドロップダウン リスト ボックスで [オフ (Off)] を選択します。Cisco IME を使用可能にするには、ドロップダウン リスト ボックスで [オン (On)] を選択します。 デフォルト値は、[Intercompany Media Service 機能設定 (Intercompany Media Services Feature Configuration)] ウィンドウ（[拡張機能 (Advanced Features)] > [Intercompany Media Services] > [機能設定 (Feature Configuration)]）で、[アウトバウンドコールに IME を使用 (Use IME for Outbound Calls)] フィールドに設定した値と同じです。 3. 適切なデバイスをこの共通デバイス設定と関連付けます。デバイスと共通デバイス設定の関連付けの詳細については、『*Cisco Unified Communications Manager アドミニストレーション ガイド*』を参照してください。
ステップ 23	Cisco IME サーバと Cisco Unified Communications Manager サーバの間の VAP 接続を確認します。	「接続の確認」（P.3-43）
フォールバック情報の設定（オプション） 通話中のフォールバック情報を設定してある場合は、設定したしきい値に基づいて音声品質の問題が検出され、オーディオ パスのみが別のベアラ チャネル、通常は PSTN に切り替えられます。フォールバックを機能させるには、コールの発信側と終端側の両方でフォールバックを設定する必要があります。		
ステップ 24	必ず、[SIP トランクセキュリティプロファイル (SIP Trunk Security Profile)] ウィンドウの [Out-of-Dialog REFER の許可 (Accept Out-of-Dialog REFER)] チェックボックスをオンにして、PSTN への通話中のフォールバックを許可してください（ステップ 4 を参照）。	

表 3-1　Cisco IME の設定チェックリスト（続き）

設定手順		関連する手順と項目
ステップ 25	PSTN フォールバック中のタイムアウトを防ぐために、Media Exchange Stop Streaming Timer を 12 秒に上げることをお勧めします。 このパラメータは、StopStreaming 要求に対する応答を受信するまで Cisco Unified Communications Manager が待機する最大秒数を指定します。指定した時間内に Cisco Unified Communications Manager が受信しなかった場合、Cisco Unified Communications Manager は、コールを終了します。	1. [システム (System)] > [サービスパラメータ (Service Parameters)] を選択します。 2. [サーバ (Server)] ドロップダウン リスト ボックスで、サーバを選択します。 3. [サービス (Service)] ドロップダウン リスト ボックスで、Cisco CallManager サービスを選択します。 4. Media Exchange Stop Streaming Timer パラメータに 12 秒を設定します。
ステップ 26	Cisco IME コールを PSTN にフォールバックするために Cisco Unified Communications Manager で使用する複数の値を定義する、フォールバック プロファイルを設定します （オプション）。 **ヒント** フォールバック設定の間に、デバイスがデバイス プールと関連付けられます。デバイス プールは登録済みグループと関連付けできます。登録済みグループは、フォールバックを設定するために必要な情報を含むフォールバック プロファイルを指定できます。	「フォールバック プロファイルの設定」（P.3-46）
ステップ 27	フォールバック プロファイルを登録済みグループと関連付けます。	1. [拡張機能 (Advanced Features)] > [Intercompany Media Service] > [登録済みグループ (Enrolled Group)] の順に選択します。作成したフォールバック プロファイルと関連付ける登録済みグループを検索します。 2. [フォールバックプロファイル (Fallback Profile)] ドロップダウン リスト ボックスから、選択した登録済みグループに関連付けるプロファイルを選択します。 3. [保存 (Save)] をクリックします。
ステップ 28	フォールバック プロファイルと関連付けた登録済みグループをデバイス プールと関連付けます。 **ヒント** このデバイス プールと関連付けられたデバイスは、デバイス プール内の登録済みグループから取得したパターンを使用して、PSTN フォールバック用の発信者 ID を使用します。	1. [システム (System)] > [デバイスプール (Device Pool)] の順に選択します。 2. ステップ 27 で設定したフォールバック プロファイルを関連付けるデバイス プールを検索します。 3. [Intercompany Media Service の登録済みグループ (Intercompany Media Services Enrolled Group)] ドロップダウン リスト ボックスから登録済みグループを選択します。 4. [保存 (Save)] をクリックします。
ステップ 29	Cisco Unified Communications Manager で通話中の Cisco IME コールを PSTN にフォールバックするときに使用する、フォールバック機能パラメータを確認します。デフォルト設定は、大部分の設定で適切です。	「フォールバック機能パラメータの設定」（P.3-50）

表 3-1　Cisco IME の設定チェックリスト（続き）

設定手順		関連する手順と項目
オフパス設定の入力（オプション） 着信と発信の Cisco IME コールが Cisco Intercompany Media Engine プロキシを有効化した Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）を通過する一方で、インターネットに接している通常のトラフィックがこの ASA を通過しないオフパス配置を設定する場合は、この項の説明を参照して、Cisco Intercompany Media Engine プロキシを有効化した ASA を設定する必要があります。		
ステップ 30	ASA マッピング サービスの IP アドレスおよびポートを設定します。	「Intercompany Media Service のファイアウォール情報の設定」（P.3-52）
ステップ 31	ファイアウォール設定に適用される次の機能パラメータを設定します。 • [IME コールのファイアウォール接続要求タイマー(Firewall Connection Request Timer for IME Calls)] • [IME コールのファイアウォールマッピング応答タイマー (Firewall Mapping Response Timer for IME Calls)] • [IME コールのファイアウォールマッピング接続アイドルタイマー (Firewall Mapping Connection Idle Timer for IME Calls)]	「Cisco IME 機能設定の入力」（P.3-39）
全般情報		
ステップ 32	Cisco Intercompany Media Engine の学習済みルートを表示できる他、学習ルートを使用可能にしたり使用不可にしたりできます。	「Cisco Intercompany Media Engine 学習ルート」（P.3-53）

Cisco IME サーバ接続の設定

[Intercompany Media Engine サーバ接続の設定 (Intercompany Media Engine Server Connection Configuration)] ウィンドウを使用して、Cisco Unified Communications Manager で接続する Cisco Intercompany Media Engine（Cisco IME）サーバに関する情報を指定します。Cisco Unified Communications Manager では、指定された情報を使用して Cisco IME サーバに接続し、VAP メッセージングを開始できます。サーバ間のこのインターフェイスにより、Cisco Unified Communications Manager では、設定された Direct Inward Dialing（DID; ダイヤル イン）パターンをパブリッシュしたり、新しいルートを学習したりできます。

Cisco Unified Communications Manager は接続を確立します。次に Cisco Unified Communications Manager は、VAP REGISTER メッセージを Cisco IME サーバに送信します。このメッセージは、[アプリケーションユーザ (Application User)] フィールドで指定するアプリケーション ユーザと関連付けられたユーザ名を含んでいます。Cisco IME サーバは、設定されている VAP ユーザ名とパスワード（「インストール後の作業」（P.2-18）のステップ 9 で設定）と照合して、このクレデンシャルを検査します。値が一致しない場合、検証は失敗し、Cisco IME サーバは Cisco Unified Communications Manager サーバと通信できません。

（注）　Cisco Unified Communications Manager の管理 で Cisco IME サーバを設定する前に、Cisco IME サーバをインストールしておくことと、サーバの動作を確認しておくことをお勧めします。

Cisco Unified Communications Manager の管理 で Cisco IME サーバを設定するときは、Cisco Intercompany Media Engine サーバが使用可能になるまで、[Intercompany Media Service の設定 (Intercompany Media Service Configuration)] ウィンドウ（**[拡張機能 (Advanced Features)] >**

[Intercompany Media Services] > [サービス (Service)]）で、Cisco Intercompany Media Engine サービスを必ず非アクティブ化してください。

Cisco Unified Communications Manager の管理 を設定するときに Cisco IME サーバを使用できない場合、Cisco Unified Communications Manager では、Cisco Intercompany Media Engine サービスに対して設定する再接続間隔に基づいて、引き続き Cisco Intercompany Media Engine サーバへの接続を試行します。

[Intercompany Media Engine サーバ接続の設定 (Intercompany Media Engine Server Connection Configuration)] ウィンドウにアクセスするには、[拡張機能 (Advanced Features)] > [Intercompany Media Services] > [サーバ接続 (Server Connections)] を選択します。

GUI の使用方法

Cisco Unified Communications Manager の管理の Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）を使用してレコードを検索、削除、設定、またはコピーする方法については、「Cisco Unified Communications Manager の管理の基礎」（P.3-2）およびそのサブセクションを参照してください。GUI の使用方法とボタンおよびアイコンの機能の詳細が説明されています。

設定項目の表

表 3-2 では、Cisco IME サーバの設定値について説明します。

関連する手順については、「Cisco IME の設定チェックリスト」（P.3-6）を参照してください。

表 3-2　Cisco IME サーバの設定値

フィールド	説明
[サーバ情報 (Server Information)]	
[名前 (Name)]	50 文字までの Cisco IME サーバの名前。クラスタ内で一意の名前を指定します。 有効な値は、英数字（a ～ z、A ～ Z、0 ～ 9）、ピリオド（.）、ダッシュ（-）、アンダースコア（_）、スペース（ ）です。
[説明 (Description)]	Cisco IME サーバの内容を表す名前を入力します。128 文字まで入力できます （オプション）。
[IP アドレス (IP Address)]	Cisco Unified Communications Manager が接続する Cisco IME サーバの IP アドレスを入力します。IPv4 アドレスを入力する必要があります。
[ポート (Port)]	Cisco Unified Communications Manager サーバで Cisco IME サーバへの Validation Access Protocol（VAP）通信に使用するポートを指定します。デフォルトは 5620 です。有効な値の範囲は、0 ～ 65535 です。 入力するポート番号は、Cisco IME サーバで設定したポート番号と一致している必要があります（表 2-6 の ステップ 6 を参照）。
[認証情報 (Authentication Information)]	
[アプリケーションユーザ (Application User)]	表 3-1 のステップ 3 で設定したアプリケーション ユーザを選択します。このアプリケーション ユーザ ID は、表 2-6 の ステップ 6 で設定した vapusername と一致している必要があります。

表 3-2　Cisco IME サーバの設定値（続き）

フィールド	説明
[サーバセキュリティモード (Server Security Mode)]	Cisco Unified Communications Manager サーバと Cisco IME サーバの間の適切なセキュリティ モードを選択します。これは、[認証済 (Authenticated)] または [暗号化済および認証済 (Encrypted and Authenticated)] のいずれかです。選択するセキュリティ モードは、Cisco Intercompany Media Engine サーバで設定したセキュリティ モードと一致している必要があります（表 2-6 の ステップ 6 を参照）。 [認証済 (Authenticated)] モードでは、サーバ間でダイジェスト ベースの認証を使用しますが、データは暗号化されません。[暗号化済および認証済 (Encrypted and Authenticated)] モードでは、Cisco Unified Communications Manager サーバと Cisco IME サーバの間の TLS 接続を介して実行する必要のあるダイジェスト認証を使用します。[暗号化済および認証済 (Encrypted and Authenticated)] を選択する場合は、Cisco Unified Communications オペレーティング システム（[セキュリティ (Security)] > [証明書の管理 (Certificate Management)]）を使用して、Cisco Intercompany Media Engine 証明書を Cisco Unified Communications Manager の信頼ストアにアップロードする必要があります。デフォルトは [認証済 (Authenticated)] です。 [暗号化済および認証済 (Encrypted and Authenticated)] モードを選択することを強くお勧めします。 **（注）** サーバ セキュリティ モードを変更すると、Cisco Unified Communications Manager は Cisco IME サーバへの接続を閉じます。
[サーバの再接続/VAP 再試行間隔 (Server Reconnect/VAP Retry Interval)]	接続が中断された後で Cisco Unified Communications Manager サーバで Cisco IME サーバへの接続を試行する頻度（秒数）を指定します。Cisco Unified Communications Manager サーバは、この間隔で、Cisco IME サーバへの接続を無期限で試行します。 有効な値は 60 ～ 600 秒です。デフォルトは 120 秒です。

追加情報

「Cisco IME の設定チェックリスト」（P.3-6）

Cisco Unified Communications Manager と Cisco Intercompany Media Engine サーバの間の TLS 接続の設定

自己署名証明書またはサードパーティの証明書を使用して、Cisco Unified Communications Manager と Cisco Intercompany Media Engine（Cisco IME）サーバの間の TLS 接続を設定できます。次の手順を参照してください。

- 「Cisco Intercompany Media Engine サーバ上での自己署名証明書の生成とアップロード」（P.3-18）
- 「Cisco Intercompany Media Engine 用のサードパーティ証明書の生成およびアップロード」（P.3-19）

Cisco Intercompany Media Engine サーバ上での自己署名証明書の生成とアップロード

自己署名証明書を使用して Cisco Unified Communications Manager と Cisco Intercompany Media Engine（Cisco IME）サーバの間に TLS 接続を設定する場合は、自己署名証明書を生成して、適切な信頼ストアにこの証明書をアップロードする必要があります。

自己署名証明書を使用する場合は、次の手順を使用します。

手順

ステップ 1　Cisco IME サーバで Cisco IME Command Line Interface（CLI; コマンド ライン インターフェイス）にログインし、**show cert own IME** コマンドを入力します。

Cisco IME 証明書が表示されます。

ステップ 2　「-----BEGIN CERTIFICATE-----」から「-----END CERTIFICATE-----」までの証明書の内容をコピーし、PC に保管した IME_Cert.pem というファイルに貼り付けます。

ステップ 3　Cisco IME サーバに接続する Cisco Unified Communications Manager サーバで、Cisco Unified Communications オペレーティング システムにログインし、[セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択します。

ステップ 4　[証明書のアップロード (Upload Certificate)] をクリックします。

[証明書のアップロード (Upload Certificate)] ダイアログボックスが表示されます。

ステップ 5　[証明書の名前 (Certificate Name)] ドロップダウン リストから [CallManager の信頼性 (CallManager-trust)] を選択します。

ステップ 6　次のいずれかの手順を実行して、アップロードするファイルを選択します。

- [ファイルのアップロード (Upload File)] テキストボックスに、ファイルのパスを入力します。
- [参照 (Browse)] ボタンをクリックし、このファイルまで移動してから [オープン (Open)] をクリックします。

ステップ 7　[ファイルのアップロード (Upload File)] ボタンをクリックして、Cisco Unified Communications Manager サーバにファイルをアップロードします。

Cisco IME サーバへの Cisco Unified Communications Manager 署名証明書のアップロード

ステップ 8　Cisco Unified Communications Manager サーバで、証明書を表示します。これを行うには、Cisco Unified Communications オペレーティング システムで [セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択し、[検索 (Find)] をクリックします。

ステップ 9　CallManager.pem 証明書を選択します。この証明書の説明には、システムで生成した自己署名証明書であることが示されています。

ステップ 10　[ダウンロード (Download)] ボタンを選択して、PC にファイルを保存します。

ステップ 11　テキスト エディタを使用して PC 上のファイルを開き、「-----BEGIN CERTIFICATE-----」から「-----END CERTIFICATE-----」までのファイルの内容をコピーします。

ステップ 12　Cisco IME CLI にログインし、**set cert import trust IME** コマンドを入力します。

ステップ 13　コピーしておいた証明書を貼り付けます。

ステップ 14　CLI コマンド **show ime vapserver** *vapservername* を入力して、Cisco IME で認証モードに「encrypted」が指定されていることを確認します。ここで、*vapservername* は、Cisco IME サーバ上に作成した VAP サーバ インスタンスの名前です。

ステップ 15　Cisco Unified Communications Manager サーバで、認証モードに [暗号化済および認証済 (Encrypted and Authenticated)] を設定していることを確認します。これを行うには、Cisco Unified Communications Manager の管理にログインし、[Intercompany Media Engine サーバ接続の設定 (Intercompany Media Engine Server Connection Configuration)] ウィンドウ（[拡張機能 (Advanced Features)] > [Intercompany Media Services] > [サーバ接続 (Server Connections)]）を表示します。対応する Cisco IME サーバの [サーバセキュリティモード (Server Security Mode)] が [暗号化済および認証済 (Encrypted and Authenticated)] であることを確認します。

Cisco IME サーバにアップロードした Cisco Unified Communications Manager 署名証明書の確認

ステップ 16　Cisco Unified Communications Manager サーバで、Cisco Unified Communications オペレーティングシステムにログインし、[セキュリティ (Security)] > [証明書の管理 (Certificate Management)] を選択して CallManager.pem 自己署名証明書を表示します。[検索 (Find)] ボタンをクリックし、証明書のリストから CallManager.pem 自己署名証明書を選択します。証明書の内容が表示されます。

ステップ 17　Cisco IME サーバで Cisco IME CLI にログインし、**show cert list trust** コマンドを入力してから **show cert trust** *trust name* コマンドを入力して、Cisco IME 信頼名を見つけます。

ステップ 18　Cisco Unified Communications Manager サーバからの証明書と Cisco IME サーバからの証明書の内容を比較して、一致していることを確認します。

（注）　この手順は、Cisco IME サーバに接続する Cisco Unified Communications Manager サーバごとに繰り返す必要があります。

追加情報

「Cisco IME の設定チェックリスト」（P.3-6）

Cisco Intercompany Media Engine 用のサードパーティ証明書の生成およびアップロード

サードパーティの証明書を使用して Cisco Unified Communications Manager サーバと Cisco IME サーバの間に TLS 接続を設定する場合は、Certificate Signing Request（CSR; 証明書署名要求）を生成し、Cisco IME サーバに証明書をアップロードする必要があります。次に、CSR を生成して、サードパーティの証明書を Cisco Unified Communications Manager サーバにアップロードする必要があります。

この手順は、サードパーティの証明書用の Certificate Signing Request（CSR; 証明書署名要求）を生成して、Cisco Unified Communications Manager サーバおよび Cisco IME サーバに証明書をアップロードする場合に使用します。

手順

ステップ 1　Cisco IME Command Line Interface（CLI; コマンド ライン インターフェイス）にログインし、**set csr gen IME** コマンドを入力してから **show csr own IME** コマンドを入力して、Cisco IME 用の CSR を生成します。

ステップ 2　サードパーティの Certificate Agent（CA; 証明書エージェント）に CSR をコピーします。

ステップ 3　Cisco IME 用の署名アプリケーション証明書およびルート証明書を CA から入手してダウンロードします。

ステップ 4　Cisco IME CLI にログインし、**set cert import trust IME** コマンドを入力して、ルート証明書を Cisco IME サーバにインポートします。新しく生成した Cisco IME 信頼要素をメモします。

ステップ 5　**set cert import own IME *IME CA Cert*** コマンドを入力して、署名アプリケーション証明書を Cisco IME サーバにインポートします。

ステップ 6　**show ime vapserver** *vapservername* コマンドを入力して、Cisco IME で認証モードに「encrypted」が指定されていることを確認します。ここで、*vapservername* は、Cisco IME サーバ上に作成した VAP サーバ インスタンスの名前です。

認証モードを変更する必要がある場合は、**set ime vapserver authenticationmode** *vapservername* **encrypted** コマンドを入力します。

Cisco Unified Communications Manager サーバ上でのサードパーティ証明書の生成とアップロード

ステップ 7　Cisco Unified Communications オペレーティング システムにログインし、[セキュリティ (Security)] > [証明書の管理 (Certificate Management)] の順に選択します。

ステップ 8　CallManager CSR を生成してダウンロードします（『*Cisco Unified Communications Operating System Administration Guide*』を参照）。[証明書の名前 (Certificate Name)] ドロップダウン リストでは、必ず [CallManager の信頼性 (CallManager)] を選択します。

ステップ 9　生成された CSR を使用して、サードパーティの署名アプリケーション証明書およびルート証明書を Certificate Agent（CA; 証明書エージェント）から入手してダウンロードします。

ステップ 10　Cisco Unified Communications オペレーティング システム（[セキュリティ (Security)] > [証明書の管理 (Certificate Management)]）から CallManager-Trust ルート証明書および CallManager 署名証明書をアップロードします。

ステップ 11　Cisco Unified Communications Manager の管理の [Intercompany Media Engine サーバ接続の設定 (Intercompany Media Engine Server Connection Configuration)] ウィンドウ（[拡張機能 (Advanced Features)] > [Intercompany Media Services] > [サーバ接続 (Server Connections)]）で、認証モードに [暗号化済および認証済 (Encrypted and Authenticated)] を設定したことを確認します。

Cisco IME と Cisco Unified Communications Manager の間の証明書の確認

ステップ 12　Cisco Unified Communications オペレーティング システムで、[セキュリティ (Security)] > [証明書の管理 (Certificate Management)] の順に選択します。

ステップ 13　ステップ 10 でアップロードした、CallManager ルート証明書を検索して表示します。

ステップ 14　Cisco IME サーバ CLI にログインし、**show cert trust list** コマンドを使用して、ルート証明書の名前を取得します。

ステップ 15　**show cert trust** *filename* コマンドを入力します。ここで、filename は、ステップ 14 で取得した証明書の名前です。

ステップ 16　Cisco Unified Communications Manager サーバ上のルート証明書と Cisco IME サーバ上のルート証明書が一致することを確認します。

（注）　この手順のステップ 7 とステップ 16 は、Cisco IME サーバに接続する Cisco Unified Communications Manager サーバごとに繰り返す必要があります。

追加情報

「Cisco IME の設定チェックリスト」（P.3-6）

Cisco IME 登録済みグループの設定

Cisco Intercompany Media Engine（Cisco IME）に参加させる番号を指定するには、登録済みグループと登録済みパターンを作成します。登録済みグループは、登録済みパターンの集合です。これらのパターンは、Cisco IME コールの発信と受信を行う、一連の +E.164 番号を定義します。Cisco IME は、これらの番号を IME 分散キャッシュにパブリッシュします。これにより、Cisco IME では、他の企業が Cisco IME を介してこれらの番号を学習できるようにします。Cisco IME コールを発信するには、自社内の番号も登録済みグループ内のパターンと一致している必要があります。キャンパスまたはサイトごとに登録済みグループを作成すると、特定のサイトまたはキャンパスから始めて、使用の拡大に連れて導入を広げることにより、Cisco IME を漸進的に導入しやすくなります。

登録済みグループを作成した後で登録済みパターンを作成し、パターンをグループに割り当て、グループを Cisco IME サービスと関連付けます。企業内の特定の電話に対して Cisco IME を使用不可にするには、該当する電話に対して、登録済みグループの Cisco IME サービスからの割り当てを解除できます。

[Intercompany Media Service の登録済みグループの設定 (Intercompany Media Services Enrolled Group Configuration)] ウィンドウにアクセスするには、[拡張機能 (Advanced Features)] > [Intercompany Media Services] > [登録済みグループ (Enrolled Group)] を選択します。

GUI の使用方法

Cisco Unified Communications Manager の管理の Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）を使用してレコードを検索、削除、設定、またはコピーする方法については、「Cisco Unified Communications Manager の管理の基礎」（P.3-2）およびそのサブセクションを参照してください。GUI の使用方法とボタンおよびアイコンの機能の詳細が説明されています。

設定項目の表

表 3-3 に、Cisco IME 登録済みグループの設定項目を示します。

関連する手順については、「Cisco IME の設定チェックリスト」（P.3-6）を参照してください。

表 3-3　Cisco Intercompany Media Engine 登録済みグループの設定値

フィールド	説明
[グループ名 (Group Name)]	登録済みグループの一意の名前を入力します。名前は、1 文字以上である必要があり、32 文字まで使用できます。
[説明 (Description)]	登録済みグループの説明を入力します。128 文字まで入力できます（オプション）。

表 3-3　Cisco Intercompany Media Engine 登録済みグループの設定値（続き）

フィールド	説明
[フォールバックプロファイル (Fallback Profile)]	この登録済みグループに関連付けるフォールバック プロファイルを選択します。 フォールバック プロファイルは、この登録済みグループと関連付けられている番号が PSTN にフォールバックされるときに、Cisco Unified Communications Manager で処理する方法を定義します。 [なし(None)] を選択した場合、このパターン グループに含まれている Direct Inward Dialing（DID; ダイヤル イン）番号へのコールは、PSTN にフォールバックされません。 フォールバック プロファイルは、[フォールバックプロファイルの設定 (Fallback Profile Configuration)] ウィンドウで設定します。詳細については、「フォールバック プロファイルの設定」（P.3-46）を参照してください。 （注）　Cisco IME を初めて設定するときは、このフィールドでフォールバック プロファイルを選択する前に、Cisco Unified Communications Manager の管理の設定のこれ以外の部分を完了することをお勧めします。
[グループ内のすべてのパターンがエイリアス (All Patterns in Group Are Aliases)]	グループ内のすべてのパターンで、互いにエイリアスを設定する必要がある場合に、このチェックボックスをオンにします。たとえば、+E.164 番号を登録した 18xx の番号があるときに、サービス プロバイダーが 18xx の番号からのマッピングを実行して、この 18xx 番号の着信者番号として代わりに DID を示す場合に、このチェックボックスをオンにします。 このチェックボックスは、同じグループ内の他のパターンへの正確なエイリアスを指定するパターンの場合のみオンにしてください。エイリアスに使用できるのは、正確なパターンのみです。ワイルドカードは使用できません。

追加情報

「Cisco IME の設定チェックリスト」（P.3-6）

Cisco IME 登録済みパターンの設定

Cisco Intercompany Media Engine（Cisco IME）登録済みパターンは、Cisco IME コールを発信および受信する一連の +E.164 番号を定義します。Cisco IME は、これらの番号を IME 分散キャッシュにパブリッシュします。これにより、Cisco IME では、他の企業が Cisco IME を介してこれらの番号を学習できるようにします。パターンでは、企業が所有している有効な Direct Inward Dialing（DID; ダイヤル イン）番号を指定する必要があります。Cisco IME コールを発信するには、自社内の番号が登録済みグループ内にあるパターンと一致している必要があります。

個々の電話機がシステムに追加されたり、システムから削除されたりすることによって、個別の番号を毎日プロビジョニングしなくてもよくするために、特定のサイトの番号を広く含むグループを表すパターンを追加できます。登録済みパターンは、電話機に割り当てられていない番号を含むことができます。電話機に割り当てられていない番号は、検証されません。

登録済みパターンを作成してから、登録済みパターンを登録済みグループに関連付け、登録済みグループを Cisco Intercompany Media Engine サービスに割り当てます。登録済みグループと Cisco IME サービスの関連付けを解除したり、関連付けたりすることにより、Cisco IME で企業内の特定の電話機をコールできるようにしたり、できないようにしたりすることができます。

（注）　除外グループおよび除外番号を設定すると、登録済みパターンの範囲内にある特定の番号を、Cisco IME に加わる対象から除外できます。詳細については「Cisco IME 除外グループの設定」（P.3-24）、および「Cisco IME 除外番号の設定」（P.3-24）を参照してください。

[IME 登録済みパターンのサーバ設定 (IME Enrolled Pattern Server Configuration)] ウィンドウにアクセスするには、[拡張機能 (Advanced Features) > [Intercompany Media Services] > [登録済みパターン (Enrolled Pattern)] を選択します。

GUI の使用方法

Cisco Unified Communications Manager の管理の Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）を使用してレコードを検索、削除、設定、またはコピーする方法については、「Cisco Unified Communications Manager の管理の基礎」（P.3-2）およびそのサブセクションを参照してください。GUI の使用方法とボタンおよびアイコンの機能の詳細が説明されています。

設定項目の表

表 3-4 に、Cisco IME 登録済みパターンの設定項目を示します。

関連する手順については、「Cisco IME の設定チェックリスト」（P.3-6）を参照してください。

表 3-4　Cisco Intercompany Media Engine 登録済みパターンの設定値

フィールド	説明
[パターン (Pattern)]	次の特徴を持つ一意のパターンを作成してください。 • プラス記号（+）で開始されている。 • 0 ～ 9 の数字と、パターンの末尾 3 桁までのワイルドカード（X）文字を含む、最大 15 桁を含んでいる。 • ワイルドカード文字は、0 ～ 9 の数字を表します。 次のパターンは、有効な登録済みパターンを表します。 • +14089021xxx • +191937611xx • +14089523513
[説明 (Description)]	登録済みパターンの内容を表す名前を入力します。128 文字まで入力できます （オプション）。
[登録済みグループ (Enrolled Group)]	この登録済みパターンと関連付ける Cisco IME 登録済みグループを選択します。 （注）　登録済みグループをさらに設定する場合は、「Cisco IME 登録済みグループの設定」（P.3-21）を参照してください。

追加情報

「Cisco IME の設定チェックリスト」（P.3-6）

Cisco IME 除外グループの設定

除外グループは、アナログ デバイスやファクス機の番号など、Cisco Intercompany Media Engine（Cisco IME）を使用させない番号のリストを含みます。まず、除外グループを作成してから、特定の除外グループと関連付ける除外番号を作成します。次に、除外グループを Cisco IME サービスと関連付けます。

除外グループを作成する手順は、次のとおりです。

[拡張機能 (Advanced Features)] > [Intercompany Media Services] > [除外グループ (Exclusion Group)] を選択して [Intercompany Media Service の除外グループの設定 (Intercompany Media Services Exclusion Group Configuration)] ウィンドウにアクセスします。

GUI の使用方法

Cisco Unified Communications Manager の管理の Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）を使用してレコードを検索、削除、設定、またはコピーする方法については、「Cisco Unified Communications Manager の管理の基礎」（P.3-2）およびそのサブセクションを参照してください。GUI の使用方法とボタンおよびアイコンの機能の詳細が説明されています。

設定項目の表

表 3-5 に、Cisco IME 除外グループの設定項目を示します。

関連する手順については、「Cisco IME の設定チェックリスト」（P.3-6）を参照してください。

表 3-5　Cisco Intercompany Media Engine 除外グループの設定値

フィールド	説明
[名前 (Name)]	除外グループの一意の名前を入力します。この名前には、最長 32 文字まで指定できます。
[説明 (Description)]	除外グループの内容を表す名前を入力します。128 文字まで入力できます （オプション）。

追加情報

「Cisco IME の設定チェックリスト」（P.3-6）

Cisco IME 除外番号の設定

Cisco IME 登録済みパターンに含まれている番号のリストにある番号であっても、Cisco Intercompany Media Engine（Cisco IME）を使用しない番号、一連の番号、プレフィックス、または一連のプレフィックスを定義するには、[Intercompany Media Service 除外番号の設定 (Intercompany Media Services Exclusion Number Configuration)] ウィンドウを使用します。

[Intercompany Media Service 除外番号の設定 (Intercompany Media Services Exclusion Number Configuration)] ウィンドウにアクセスするには、[拡張機能 (Advanced Features)] > [Intercompany Media Services] > [除外番号 (Exclusion Number)] を選択します。

GUI の使用方法

Cisco Unified Communications Manager の管理の Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）を使用してレコードを検索、削除、設定、またはコピーする方法については、「Cisco Unified Communications Manager の管理の基礎」（P.3-2）およびそのサブセクションを参照してください。GUI の使用方法とボタンおよびアイコンの機能の詳細が説明されています。

設定項目の表

表 3-6 に、Cisco IME 除外番号の設定項目を示します。

関連する手順については、「Cisco IME の設定チェックリスト」（P.3-6）を参照してください。

表 3-6　Cisco Intercompany Media Engine 除外番号の設定値

フィールド	説明
[パターン (Pattern)]	Cisco IME から除外する +E.164 番号を指定します。番号の前にプラス記号（+）を付ける必要があります。番号は 15 桁まで入力できます。 ワイルドカードを使用せずに、+E.164 番号を正確に入力する必要があります。
[説明 (Description)]	除外番号の内容を表す名前を入力します。128 文字まで入力できます （オプション）。
[除外グループ (Exclusion Group)]	ドロップダウン リスト ボックスから、この除外番号に関連付ける Cisco IME グループを選択します。 除外グループをさらに設定する場合は、「Cisco IME 除外グループの設定」（P.3-24）を参照してください。

追加情報

「Cisco IME の設定チェックリスト」（P.3-6）

Cisco IME 信頼グループの設定

Cisco Intercompany Media Engine（Cisco IME）信頼グループは、その信頼グループと関連付けられている Cisco IME サービスによって信頼されている（または信頼されていない）ドメインとプレフィックスのリストを含みます。Cisco Unified Communications Manager では、信頼されているドメインまたはプレフィックスに対してのみ Cisco IME コールを発信します。

信頼グループの設定はオプションです。信頼グループを作成していない場合、Cisco IME では、デフォルトですべてのコールを信頼します。

信頼グループを削除する手順は、次のとおりです。信頼グループに含めるドメインおよびプレフィックスの作成については、「Cisco IME 信頼要素の設定」（P.3-26）を参照してください。

[Intercompany Media Service の信頼グループの設定 (Intercompany Media Services Trust Group Configuration)] ウィンドウにアクセスするには、[拡張機能 (Advanced Features)] > [Intercompany Media Services] > [信頼グループ (Trust Group)] を選択します。

GUI の使用方法

Cisco Unified Communications Manager の管理の Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）を使用してレコードを検索、削除、設定、またはコピーする方法については、「Cisco Unified Communications Manager の管理の基礎」（P.3-2）およびそのサブセクションを参照してください。GUI の使用方法とボタンおよびアイコンの機能の詳細が説明されています。

設定項目の表

表 3-7 では、Intercompany Media Service の信頼グループの設定値について説明します。

関連する手順については、「Cisco IME の設定チェックリスト」（P.3-6）を参照してください。

表 3-7　Intercompany Media Service の信頼グループの設定値

フィールド	説明
[名前 (Name)]	信頼グループの一意の名前を入力します。この名前には、最長 32 文字まで指定できます。
[説明 (Description)]	信頼グループの内容を表す名前を入力します。128 文字まで入力できます （オプション）。
[信頼済み (Trusted)]	ドロップダウン リスト ボックスから、信頼の値として、[はい (Yes)]（信頼されている）または [いいえ (No)]（信頼されていない）を選択します。 この信頼グループを使用している信頼要素がある場合は、この値を変更できません。これは、1 つの値を変更することによって、信頼されていないグループ（ブラックリスト）を信頼グループ（ホワイトリスト）に誤って変更しないための制限です。 デフォルト値はありません。値を 1 つ選択する必要があります。

追加情報

「Cisco IME の設定チェックリスト」（P.3-6）

Cisco IME 信頼要素の設定

Cisco Intercompany Media Engine（Cisco IME）信頼要素は、信頼するプレフィックスまたはドメインか、信頼しないプレフィックスまたはドメインを指定します。信頼要素は、信頼グループに含めます。Cisco Unified Communications Manager では、信頼されているドメインまたはプレフィックスに対してのみ Cisco IME コールを発信します。信頼されていない要素にプレフィックスまたはドメインが含まれている番号からは、Cisco IME コールを受けることができません。

信頼要素を作成し、この信頼要素を信頼グループと関連付ける手順は、次のとおりです。信頼要素を作成してから信頼グループを Cisco IME サービスと関連付けて、信頼グループで指定しているプレフィックスまたはドメインを信頼するまたは信頼しないようにします。

[Intercompany Media Service の信頼要素の設定 (Intercompany Media Services Trust Element Configuration)] ウィンドウにアクセスするには、[拡張機能 (Advanced Features)] > [Intercompany Media Services] > [信頼要素 (Trust Element)] を選択します。

GUI の使用方法

Cisco Unified Communications Manager の管理の Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）を使用してレコードを検索、削除、設定、またはコピーする方法については、「Cisco Unified Communications Manager の管理の基礎」（P.3-2）およびそのサブセクションを参照してください。GUI の使用方法とボタンおよびアイコンの機能の詳細が説明されています。

設定項目の表

表 3-8 では、Intercompany Media Service の信頼要素の設定値について説明します。

関連する手順については、「Cisco IME の設定チェックリスト」（P.3-6）を参照してください。

表 3-8　Intercompany Media Service の信頼要素の設定値

フィールド	説明
[名前 (Name)]	ドメイン名またはプレフィックスを入力します。 ドメイン名には、最長 128 文字を指定できます。有効なドメイン名を指定する必要があります。 プレフィックスは「+」記号で始まり、15 文字までか 14 文字と 1 文字のワイルドカード「!」である必要があります。
[説明 (Description)]	エンジン信頼要素の内容を表す名前を入力します。128 文字まで入力できます （オプション）。
[要素タイプ (Element Type)]	[ドメイン (Domain)] または [プレフィックス (Prefix)] から適切な要素タイプを選択します。
[信頼グループ (Trust Group)]	適切な信頼グループを選択します。この要素をホワイトリスト（信頼グループ）に含めるには、ドロップダウン リスト ボックスから信頼グループを選択します。この要素をブラックリスト（信頼されていないグループ）に含めるには、ドロップダウン リスト ボックスから信頼されていないグループを選択します。 信頼グループを設定する方法の詳細については、「Cisco IME 信頼グループの設定」（P.3-25）を参照してください。

追加情報

「Cisco IME の設定チェックリスト」（P.3-6）

Cisco IME サービスの設定

Cisco Intercompany Media Engine（Cisco IME）サービスの設定とアクティブ化には、[Intercompany Media Service の設定 (Intercompany Media Service Configuration)] ウィンドウを使用します。Cisco Unified Communications Manager の管理 で Cisco IME サービスを設定するには、信頼グループ、登録済みグループ、除外グループなど、すでに設定したさまざまなコンポーネントを関連付けます。Cisco Unified Communications Manager と通信する Cisco IME サーバを指定します。Cisco Unified Communications Manager サーバと Cisco IME サーバの間の通信は、Cisco IME サービスを設定してアクティブ化した後で開始されます。

システムの作業を複数の Cisco Intercompany Media Engine サーバに分散させるロード バランシングを開始するには、異なる Cisco Intercompany Media Engine サーバを使用する 1 つ以上の Cisco Intercompany Media Engine サービスを作成し、登録済みグループの一部を元の Cisco Intercompany Media Engine サービスから新規サービスに移動します。

[Intercompany Media Service の設定 (Intercompany Media Service Configuration)] ウィンドウにアクセスするには、[拡張機能 (Advanced Features)] > [Intercompany Media Services] > [サービス (Service)] を選択します。

[CUCM 外部アドレスリスト (CUCM External Address List)] ポップアップ ウィンドウについては、「外部 IP アドレスおよびポート情報の設定」（P.3-30）を参照してください。

GUI の使用方法

Cisco Unified Communications Manager の管理の Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）を使用してレコードを検索、削除、設定、またはコピーする方法については、「Cisco Unified Communications Manager の管理の基礎」（P.3-2）およびそのサブセクションを参照してください。GUI の使用方法とボタンおよびアイコンの機能の詳細が説明されています。

設定項目の表

表 3-9 では、Intercompany Media Services の設定値について説明します。

関連する手順については、「Cisco IME の設定チェックリスト」（P.3-6）を参照してください。

表 3-9　Intercompany Media Service の設定値

フィールド	説明
[Intercompany Media Service の情報 (Intercompany Media Service Information)]	
[名前 (Name)]	Cisco IME サービスの一意の名前を入力します。この名前には、最長 50 文字まで指定できます。
[説明 (Description)]	Cisco IME サービスの内容を表す名前を入力します。説明には、最長 128 文字まで指定できます （オプション）。
[ドメイン (Domain)]	Cisco IME で使用するドメイン名を入力します。通常は、会社のドメイン名（cisco.com など）を指定します。 このドメイン名は、ASA の GoDaddy.com から受け取る SSL 証明書内のドメイン名と一致している必要があります。
[SIP トランク (SIP Trunk)]	このサービスで使用する SIP トランクを選択します。 ドロップダウン リスト ボックスには、Cisco Intercompany Media Engine トランク サービス タイプを指定するトランクが読み込まれています。 選択したトランクは、トランクと関連付けられている Cisco Unified Communications Manager グループの定義に従って、クラスタ内にある一連の特定のノードで実行されます。Cisco IME サービスも、同じ一連のノードで実行されます。 **ヒント** Cisco Intercompany Media Engine トランクは、「Cisco IME の設定チェックリスト」（P.3-6）のステップ 5 で設定しています。
[信頼グループ (Trust Group)]	必要に応じて、信頼グループを選択します。信頼グループは、そのグループと関連付けられている Cisco IME サービスによって信頼されている（または信頼されていない）ドメインとプレフィックスのリストを含みます。Cisco Unified Communications Manager では、信頼されているドメインまたはプレフィックスに対してのみ Cisco IME コールを発信します。 ドロップダウン リスト ボックスには、[Intercompany Media Service の信頼グループの設定 (Intercompany Media Services Trust Group Configuration)] ウィンドウ（[拡張機能 (Advanced Features)] > [Intercompany Media Services] > [信頼グループ (Trusted Group)]）で設定したサーバが読み込まれています。 信頼グループを選択していない場合、Cisco IME では、すべてのプレフィックスおよびドメインを信頼します。

表 3-9　Intercompany Media Service の設定値（続き）

フィールド	説明
[除外グループ(Exclusion Group)]	必要に応じて、除外グループを選択します。除外グループは、Cisco Intercompany Media Engine を使用しない番号を含みます。 ドロップダウン リスト ボックスには、[Intercompany Media Service の除外グループの設定(Intercompany Media Services Exclusion Group Configuration)] ウィンドウ（[拡張機能(Advanced Features)] > [Intercompany Media Services] > [除外グループ(Exclusion Group)]）で設定したサーバが読み込まれています。
[ファイアウォール(Firewall)]	オフパス ASA 配置モデルを使用している場合は、このサービスと関連付けるファイアウォールを選択します。
[使用可能な登録済みグループ(Available Enrolled Groups)]	このリスト ボックスには、この Cisco IME サービスとの関連付けに使用できる登録済みグループが表示されます。登録済みグループは、Cisco IME コールの発信と受信を行う、一連の +E.164 番号を指定します。 登録済みグループをこの Cisco IME サービスに関連付けるには、登録済みグループを選択し、このリスト ボックスの下にある下矢印をクリックします。
[選択された登録済みグループ(Selected Enrolled Groups)]	このリスト ボックスには、この Cisco IME サービスとの関連付けられている登録済みグループが表示されます。登録済みグループを削除するには、登録済みグループ名を選択し、このリスト ボックスの上にある上矢印をクリックします。登録済みグループを追加するには、[使用可能な登録済みグループ(Available Enrolled Groups)] リストボックスで登録済みグループを選択し、リスト グループ ボックスの間にある下矢印をクリックします。登録済みグループの順序は、リスト ボックスの右側にある上矢印および下矢印をクリックして変更できます。
[アクティブ化(Activated)]	Cisco IME サービスをアクティブ化するには、[アクティブ化(Activated)] チェックボックスをオンにします。サービスをアクティブ化していない場合は、Cisco IME コールを発信することも受信することもできません。
[サーバ情報(Server Information)]	
[プライマリ IME サーバ(Primary IME Server)]	プライマリ Cisco IME サーバを選択します。 ドロップダウン リスト ボックスには、[Intercompany Media Engine サーバ接続の設定(Intercompany Media Engine Server Connection Configuration)] ウィンドウ（[拡張機能(Advanced Features)] > [Intercompany Media Services] > [サーバ接続(Server Connections)]）で設定したサーバが読み込まれています。 選択したサーバは、複数のサービスで使用できます。 Cisco IME サービスを複数定義する一方で、Cisco IME サーバが 1 台のみの場合は、複数の Cisco IME サービスを単一のサーバと関連付けできます。

表 3-9　Intercompany Media Service の設定値（続き）

フィールド	説明
[セカンダリ IME サーバ (Secondary IME Server)]	（オプション）セカンダリ Cisco IME サーバを選択します。 ドロップダウン リスト ボックスには、[Intercompany Media Engine サーバ接続の設定 (Intercompany Media Engine Server Connection Configuration)] ウィンドウ（[拡張機能 (Advanced Features)] > [Intercompany Media Services] > [サーバ接続 (Server Connections)]）で設定したサーバが読み込まれています。 プライマリとセカンダリの Cisco IME サーバには、別々のサーバを選択する必要があります。 選択したサーバは、複数のサービスで使用できます。

追加情報

「Cisco IME の設定チェックリスト」（P.3-6）

外部 IP アドレスおよびポート情報の設定

クラスタ内の各 Cisco Unified Communications Manager の外部 IP アドレスおよびポートを定義するには、[CUCM 外部アドレスリスト (CUCM External Address List)] ポップアップ ウィンドウを使用します。この IP アドレスおよびポートは、Cisco Unified Communications Manager で Cisco Intercompany Media Engine（Cisco IME）サービスに通知するグローバル アドレス（実アドレス）を表します。他の企業は、このアドレスを学習して、Cisco IME コールをルーティングするために使用します。設定する IP アドレスまたはホスト名は、Cisco IME を使用するすべての企業で、解決できることを確認してください。

インバウンド コールの場合、Cisco Intercompany Media Engine 対応の ASA では、Network Address Translation（NAT; ネットワーク アドレス変換）を利用します。ASA インターフェイスの 1 つに設定されている特定の IP/ ポートは、内部の各 Cisco Unified Communications Manager ノードへのスタティック マッピングを持ちます。Cisco Unified Communications Manager では、既存の設定経由で、代わりに ASA 上の IP/ ポートをアドバタイズします。この結果、インバウンド コールは、Cisco Intercompany Media Engine 対応の ASA に到達します。

Cisco Unified Communications Manager サーバがファイアウォールまたは NAT の背後にある場合は、外部 IP アドレスまたはホスト名を設定する必要があります。

[CUCM 外部アドレスリスト (CUCM External Address List)] ポップアップ ウィンドウにアクセスするには、[拡張機能 (Advanced Features)] > [Intercompany Media Services] > [サービス (Service)] を選択して、IP アドレスとポートを関連付ける Cisco IME サービスを検索します。[Intercompany Media Service の設定 (Intercompany Media Service Configuration)] ウィンドウの [関連リンク (Related Links)] ドロップダウン リスト ボックスで、[CUCM 外部アドレスリストの追加 / 更新 (Add/Update CUCM External Address List)] オプションを選択し、[移動 (Go)] をクリックします。

表 3-10 では、アドレス リストの設定値について説明します。

関連する手順については、「Cisco IME の設定チェックリスト」（P.3-6）を参照してください。

表 3-10　CUCM 外部アドレス リストの設定値

フィールド	説明
[CUCM 外部アドレスリスト (CUCM External Address List)]	
[Cisco Unified CM]	システムに含まれている Cisco Unified Communications Manager サーバが表示されます。
[IP アドレス / ホスト (IP Address/Host)]	自社へのコールをルーティングするために、他の企業で使用する IP アドレスまたはホスト名を入力します。Cisco IME を使用するすべての企業で解決できる IP アドレスまたはホスト名を入力する必要があります。
[ポート (Port)]	外部 Cisco IME トラフィックで使用するポートを入力します。

追加情報

「Cisco IME の設定チェックリスト」（P.3-6）

Cisco IME 用トランスフォーメーション パターンの設定

トランスフォーメーションで +E.164 番号を準備できるように、着信者番号および発信者番号のトランスフォーメーション パターンを設定します。+E.164 形式の番号にするために、桁を追加または削除したり、「+」記号を含むプレフィックス桁を追加または削除したりする必要があることがあります。

[発呼側トランスフォーメーションパターンの設定 (Calling Party Transformation Pattern Configuration)] ウィンドウにアクセスするには、[コールルーティング (Call Routing)] > [トランスフォーメーション (Transformation)] > [トランスフォーメーションパターン (Transformation Pattern)] > [発呼側トランスフォーメーションパターン (Calling Party Transformation Pattern)] を選択します。

[着信側トランスフォーメーションパターンの設定 (Called Party Transformation Pattern Configuration)] ウィンドウにアクセスするには、[コールルーティング (Call Routing)] > [トランスフォーメーション (Transformation)] > [トランスフォーメーションパターン (Transformation Pattern)] > [着信側トランスフォーメーションパターン (Called Party Transformation Pattern)] を選択します。

発信側および着信側のトランスフォーメーション パターンの設定値については、『*Cisco Unified Communications Manager アドミニストレーション ガイド*』を参照するか、Cisco Unified Communications Manager の管理の対応するウィンドウで [ヘルプ (Help)] > [このページ (This Page)] を選択してください。

関連する手順については、「Cisco IME の設定チェックリスト」（P.3-6）を参照してください。

追加情報

「Cisco IME の設定チェックリスト」（P.3-6）

Cisco IME トランスフォーメーション プロファイルの設定

システムでは、トランスフォーメーション プロファイルを使用して、発信コールの発信者番号および着信者番号を完全修飾 +E.164 番号形式に変換できます。変換された番号は、Cisco Intercompany Media Engine（Cisco IME）で PSTN コールを検証するために使用する、Voice Call Records（VCRs;

音声コール レコード）に格納されます。番号トランスフォーメーションは、通常のコール ルーティング処理の後で行われます。Cisco Unified Communications Manager では、コール ルーティングにトランスフォーメーション プロファイルを使用しません。

着信の着信番号用に 1 つと、着信の発信者番号用に 1 つプロファイルを作成する必要があります。トランスフォーメーション プロファイルは、「Cisco IME E.164 トランスフォーメーションの設定」（P.3-37）で説明した Cisco IME トランスフォーメーションと関連付けます。

（注）　Cisco IME では、+E.164 形式の番号を含まない VCR をアップロードしません。

[トランスフォーメーションプロファイルの設定 (Transformation Profile Configuration)] ウィンドウにアクセスするには、[コールルーティング (Call Routing)] > [トランスフォーメーション (Transformation)] > [トランスフォーメーションプロファイル (Transformation Profile)] を選択します。

GUI の使用方法

Cisco Unified Communications Manager の管理の Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）を使用してレコードを検索、削除、設定、またはコピーする方法については、「Cisco Unified Communications Manager の管理の基礎」（P.3-2）およびそのサブセクションを参照してください。GUI の使用方法とボタンおよびアイコンの機能の詳細が説明されています。

設定項目の表

表 3-11 では、トランスフォーメーション プロファイルの設定値について説明します。

関連する手順については、「Cisco IME の設定チェックリスト」（P.3-6）を参照してください。

表 3-11　Cisco Intercompany Media Engine のトランスフォーメーション プロファイルの設定値

フィールド	説明
[トランスフォーメーションプロファイルの情報 (Transformation Profile Information)]	
[名前 (Name)]	トランスフォーメーション プロファイルの一意の名前を入力します。この名前には、最長 50 文字まで指定できます。
[説明 (Description)]	トランスフォーメーション プロファイルの内容を表す名前を入力します。説明には、最長 128 文字まで指定できます （オプション）。
[着信側の設定 (Incoming Party Setting)]	
[プレフィックス設定のクリア (Clear Prefix Settings)]	すべての発信者番号タイプのプレフィックスを削除するには、[プレフィックス設定のクリア (Clear Prefix Settings)] ボタンをクリックします。
[デフォルトプレフィックス設定 (Default Prefix Settings)]	すべての発信者番号タイプのプレフィックスをデフォルト値にリセットするには、[デフォルトプレフィックス設定 (Default Prefix Settings)] ボタンをクリックします。

表 3-11　Cisco Intercompany Media Engine のトランスフォーメーション プロファイルの設定値（続き）

フィールド	説明
[国内番号(National Number)]	番号タイプとして [国内(National)] を使用する発信側番号をグローバル化するには、次の項目を設定します。[国内(National)] 番号タイプは、国内のコールで使用されます。 • [プレフィックス(Prefix)]：Cisco Unified Communications Manager は、発信者番号タイプとして [国内(National)] を使用する発信側番号に、このフィールドに入力されたプレフィックスを適用します。8 文字まで入力でき、数字、国際的なエスケープ文字（+）、アスタリスク（*）、またはシャープ（#）を含めることができます。プレフィックスを入力する代わりに Default と入力できます。 **ヒント** [ゲートウェイの設定(Gateway Configuration)] または [トランクの設定(Trunk Configuration)] ウィンドウの [プレフィックス(Prefix)] フィールドに [デフォルト(Default)] と表示されている場合、[ゲートウェイの設定(Gateway Configuration)] または [トランクの設定(Trunk Configuration)] ウィンドウの [削除桁数(Strip Digits)] フィールドは設定できません。この場合、Cisco Unified Communications Manager は、デバイスに適用されているデバイス プールの [プレフィックス(Prefix)] フィールドと [削除桁数(Strip Digits)] フィールドの設定を使用します。[デバイスプール設定(Device Pool Configuration)] ウィンドウの [プレフィックス(Prefix)] フィールドに [デフォルト(Default)] と表示されている場合、Cisco Unified Communications Manager は、着信コール発信側プレフィックスのサービス パラメータ設定を適用します。この設定は、プレフィックスと桁除去の両方の機能をサポートしています。 **ヒント** [デバイスプール設定(Device Pool Configuration)]、[ゲートウェイの設定(Gateway Configuration)]、または [トランクの設定(Trunk Configuration)] ウィンドウで [削除桁数(Strip Digits)] フィールドを設定するには、[プレフィックス(Prefix)] フィールドを空白のままにするか、[プレフィックス(Prefix)] フィールドに有効な設定値を入力する必要があります。これらのウィンドウで [削除桁数(Strip Digits)] フィールドを設定する場合は、[プレフィックス(Prefix)] フィールドに Default と入力しないでください。 • [削除桁数(Strip Digits)]：Cisco Unified Communications Manager でプレフィックスを適用する前に、国内タイプの発信側番号から Cisco Unified Communications Manager に除去させる桁数を入力します。 • [コーリングサーチスペース(Calling Search Space)]：この設定を使用すると、デバイスで [国内(National)] 発信者番号タイプの発信者番号をグローバル化できます。選択するコーリング サーチ スペースに、このデバイスに割り当てる発信側トランスフォーメーション パターンが含まれていることを確認してください。

表 3-11　Cisco Intercompany Media Engine のトランスフォーメーション プロファイルの設定値（続き）

フィールド	説明
[国際番号 (International Number)]	番号タイプとして [国際 (International)] を使用する発信側番号をグローバル化するには、次の項目を設定します。[国際 (International)] 番号タイプは、国内のダイヤル プラン外のコールで使用されます。 • [プレフィックス (Prefix)] : Cisco Unified Communications Manager は、発信者番号タイプとして [国際 (International)] を使用する発信側番号に、このフィールドに入力されたプレフィックスを適用します。8 文字まで入力でき、数字、国際的なエスケープ文字（+）、アスタリスク（*）、またはシャープ（#）を含めることができます。プレフィックスを入力する代わりに Default と入力できます。 **ヒント** [ゲートウェイの設定 (Gateway Configuration)] または [トランクの設定 (Trunk Configuration)] ウィンドウの [プレフィックス (Prefix)] フィールドに [デフォルト (Default)] と表示されている場合、[ゲートウェイの設定 (Gateway Configuration)] または [トランクの設定 (Trunk Configuration)] ウィンドウの [削除桁数 (Strip Digits)] フィールドは設定できません。この場合、Cisco Unified Communications Manager は、デバイスに適用されているデバイス プールの [プレフィックス (Prefix)] フィールドと [削除桁数 (Strip Digits)] フィールドの設定を使用します。[デバイスプール設定 (Device Pool Configuration)] ウィンドウの [プレフィックス (Prefix)] フィールドに [デフォルト (Default)] と表示されている場合、Cisco Unified Communications Manager は、着信コール発信側プレフィックスのサービス パラメータ設定を適用します。この設定は、プレフィックスと桁除去の両方の機能をサポートしています。 **ヒント** [デバイスプール設定 (Device Pool Configuration)]、[ゲートウェイの設定 (Gateway Configuration)]、または [トランクの設定 (Trunk Configuration)] ウィンドウで [削除桁数 (Strip Digits)] フィールドを設定するには、[プレフィックス (Prefix)] フィールドを空白のままにするか、[プレフィックス (Prefix)] フィールドに有効な設定値を入力する必要があります。これらのウィンドウで [削除桁数 (Strip Digits)] フィールドを設定する場合は、[プレフィックス (Prefix)] フィールドに Default と入力しないでください。 • [削除桁数 (Strip Digits)] : Cisco Unified Communications Manager でプレフィックスを適用する前に、国際タイプの発信側番号から Cisco Unified Communications Manager に除去させる桁数を入力します。 • [コーリングサーチスペース (Calling Search Space)] : この設定を使用すると、デバイスで [国際 (International)] 発信者番号タイプの発信者番号をグローバル化できます。選択する発信側トランスフォーメーション CSS に、このデバイスに割り当てる発信側トランスフォーメーション パターンが含まれていることを確認してください。 **ヒント** デバイスは、コールが発生する前に、番号分析を使用してトランスフォーメーションを適用する必要があります。CSS を [なし (None)] に設定すると、トランスフォーメーションは一致せず、適用されません。発信側トランスフォーメーション パターンは、必ず、ルーティングに使用されない非ヌル パーティションに設定してください。

表 3-11　Cisco Intercompany Media Engine のトランスフォーメーション プロファイルの設定値（続き）

フィールド	説明
[不明な番号(Unknown Number)]	番号タイプとして [不明(Unknown)] を使用する発信側番号をグローバル化するには、次の項目を設定します。[不明(Unknown)] 番号タイプは、ダイヤル プランが不明な場合に使用されます。 • [プレフィックス(Prefix)]：Cisco Unified Communications Manager は、このフィールドに入力されたプレフィックスを、発信者番号タイプとして [不明(Unknown)] を使用する発信側番号に適用します。8 文字まで入力でき、数字、国際的なエスケープ文字（+）、アスタリスク（*）、またはシャープ（#）を含めることができます。プレフィックスを入力する代わりに Default と入力できます。 **ヒント** [ゲートウェイの設定(Gateway Configuration)] または [トランクの設定(Trunk Configuration)] ウィンドウの [プレフィックス(Prefix)] フィールドに [デフォルト(Default)] と表示されている場合、[ゲートウェイの設定(Gateway Configuration)] または [トランクの設定(Trunk Configuration)] ウィンドウの [削除桁数(Strip Digits)] フィールドは設定できません。この場合、Cisco Unified Communications Manager は、デバイスに適用されているデバイス プールの [プレフィックス(Prefix)] フィールドと [削除桁数(Strip Digits)] フィールドの設定を使用します。[デバイスプール設定(Device Pool Configuration)] ウィンドウの [プレフィックス(Prefix)] フィールドに [デフォルト(Default)] と表示されている場合、Cisco Unified Communications Manager は、着信コール発信側プレフィックスのサービス パラメータ設定を適用します。この設定は、プレフィックスと桁除去の両方の機能をサポートしています。 **ヒント** [デバイスプール設定(Device Pool Configuration)]、[ゲートウェイの設定(Gateway Configuration)]、または [トランクの設定(Trunk Configuration)] ウィンドウで [削除桁数(Strip Digits)] フィールドを設定するには、[プレフィックス(Prefix)] フィールドを空白のままにするか、[プレフィックス(Prefix)] フィールドに有効な設定値を入力する必要があります。これらのウィンドウで [削除桁数(Strip Digits)] フィールドを設定する場合は、[プレフィックス(Prefix)] フィールドに Default と入力しないでください。 • [削除桁数(Strip Digits)]：Cisco Unified Communications Manager でプレフィックスを適用する前に、不明タイプの発信側番号から Cisco Unified Communications Manager に除去させる桁数を入力します。 • [コーリングサーチスペース(Calling Search Space)]：この設定を使用すると、デバイスで [不明(Unknown)] 発信者番号タイプの発信者番号をグローバル化できます。選択する発信側トランスフォーメーション CSS に、このデバイスに割り当てる発信側トランスフォーメーション パターンが含まれていることを確認してください。 **ヒント** デバイスは、コールが発生する前に、番号分析を使用してトランスフォーメーションを適用する必要があります。CSS を [なし(None)] に設定すると、トランスフォーメーションは一致せず、適用されません。発信側トランスフォーメーション パターンは、必ず、ルーティングに使用されない非ヌル パーティションに設定してください。

表 3-11　Cisco Intercompany Media Engine のトランスフォーメーション プロファイルの設定値（続き）

フィールド	説明
[加入者番号(Subscriber Number)]	番号タイプとして [加入者(Subscriber)] を使用する発信側番号をグローバル化するには、次の項目を設定します。[加入者(Subscriber)] 番号タイプは、短縮された加入者番号を使用して電話加入者にダイヤルする場合に使用されます。 • [プレフィックス(Prefix)]：Cisco Unified Communications Manager は、このフィールドに入力されたプレフィックスを、発信者番号タイプとして [加入者(Subscriber)] を使用する発信側番号に適用します。8 文字まで入力でき、数字、国際的なエスケープ文字（+)、アスタリスク（*)、またはシャープ（#) を含めることができます。プレフィックスを入力する代わりに Default と入力できます。 **ヒント** [ゲートウェイの設定(Gateway Configuration)] または [トランクの設定(Trunk Configuration)] ウィンドウの [プレフィックス(Prefix)] フィールドに [デフォルト(Default)] と表示されている場合、[ゲートウェイの設定(Gateway Configuration)] または [トランクの設定(Trunk Configuration)] ウィンドウの [削除桁数(Strip Digits)] フィールドは設定できません。この場合、Cisco Unified Communications Manager は、デバイスに適用されているデバイス プールの [プレフィックス(Prefix)] フィールドと [削除桁数(Strip Digits)] フィールドの設定を使用します。[デバイスプール設定(Device Pool Configuration)] ウィンドウの [プレフィックス(Prefix)] フィールドに [デフォルト(Default)] と表示されている場合、Cisco Unified Communications Manager は、着信コール発信側プレフィックスのサービス パラメータ設定を適用します。この設定は、プレフィックスと桁除去の両方の機能をサポートしています。 **ヒント** [デバイスプール設定(Device Pool Configuration)]、[ゲートウェイの設定(Gateway Configuration)]、または [トランクの設定(Trunk Configuration)] ウィンドウで [削除桁数(Strip Digits)] フィールドを設定するには、[プレフィックス(Prefix)] フィールドを空白のままにするか、[プレフィックス(Prefix)] フィールドに有効な設定値を入力する必要があります。これらのウィンドウで [削除桁数(Strip Digits)] フィールドを設定する場合は、[プレフィックス(Prefix)] フィールドに Default と入力しないでください。 • [削除桁数(Strip Digits)]：Cisco Unified Communications Manager でプレフィックスを適用する前に、加入者タイプの発信側番号から Cisco Unified Communications Manager に除去させる桁数を入力します。 • [コーリングサーチスペース(Calling Search Space)]：この設定を使用すると、デバイスで [加入者(Subscriber)] 発信者番号タイプの発信者番号をグローバル化できます。選択する CSS に、このデバイスに割り当てる発信側トランスフォーメーション パターンが含まれていることを確認してください。 **ヒント** デバイスは、コールが発生する前に、番号分析を使用してトランスフォーメーションを適用する必要があります。CSS を [なし(None)] に設定すると、トランスフォーメーションは一致せず、適用されません。発信側トランスフォーメーション パターンは、必ず、ルーティングに使用されない非ヌル パーティションに設定してください。

追加情報

「Cisco IME の設定チェックリスト」（P.3-6）

Cisco IME E.164 トランスフォーメーションの設定

Cisco Intercompany Media Engine（Cisco IME）E.164 トランスフォーメーションでは、PSTN コールの終了後に、発呼側と終端側（着信側と発信側）の両方で、発信者番号および着信者番号を +E.164 形式に変換します。Cisco IME E.164 トランスフォーメーションは、Cisco Unified Communications Manager でのコール ルーティングおよび番号分析に影響しません。トランスフォーメーションによって、次の操作が可能になります。

- 学習されていない Direct Inward Dialing（DID; ダイヤル イン）番号の UploadVCR を Cisco Intercompany Media Engine サーバに送信する。
- 学習した表に DID が存在している場合に、Cisco IME トランクにコールを再ルーティングする。

Cisco IME E.164 トランスフォーメーションは、PSTN アクセス トランクと関連付けます。トランスフォーメーションによって、コールの着信側または発信側で有効な発信者番号または着信者番号が生成されない場合は、VCR アップロードは行われず、このコールの Cisco IME 処理は停止されます。

[Intercompany Media Service E.164 トランスフォーメーションの設定 (Intercompany Media Services E.164 Transformation Configuration)] ウィンドウにアクセスするには、[拡張機能 (Advanced Features) > [Intercompany Media Services] > [E.164 トランスフォーメーション (E.164 Transformation)] を選択します。

GUI の使用方法

Cisco Unified Communications Manager の管理の Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）を使用してレコードを検索、削除、設定、またはコピーする方法については、「Cisco Unified Communications Manager の管理の基礎」（P.3-2）およびそのサブセクションを参照してください。GUI の使用方法とボタンおよびアイコンの機能の詳細が説明されています。

設定項目の表

表 3-12 では、トランスフォーメーションの設定値について説明します。

関連する手順については、「Cisco IME の設定チェックリスト」（P.3-6）を参照してください。

表 3-12　Cisco Intercompany Media Engine E.164 トランスフォーメーションの設定値

フィールド	説明
[E.164 トランスフォーメーション (E.164 Transformation)]	
[名前 (Name)]	トランスフォーメーション プロファイルの一意の名前を入力します。この名前には、最長 50 文字まで指定できます。
[説明 (Description)]	トランスフォーメーション プロファイルの内容を表す名前を入力します。説明には、最長 128 文字まで指定できます （オプション）。

表 3-12　Cisco Intercompany Media Engine E.164 トランスフォーメーションの設定値（続き）

フィールド	説明
[発信の発呼側設定 (Outgoing Calling Party Settings)]	
[発信側 E.164 トランスフォーメーション CSS(Outgoing Party E.164 Transformation CSS)]	ドロップダウン リスト ボックスから、発信の発信側の適切なコーリング サーチ スペースを選択します。 [発呼側トランスフォーメーション (Calling Party Transformations)] ウィンドウ（[コールルーティング (Call Routing)] > [トランスフォーメーション (Transformation)] > [トランスフォーメーションパターン (Transformation Pattern)] > [発呼側トランスフォーメーションパターン (Calling Party Transformation Pattern)]）で設定した発信側トランスフォーメーション パターンで使用するパーティションを含むコーリング サーチ スペースを選択します。
[適用オン (Apply On)]	コーリング サーチ スペースを元の番号に適用するのか、ルーティング トランスフォーメーション番号に適用するのかを選択します。
[発信の発呼側設定 (Outgoing Called Party Settings)]	
[発信側 E.164 トランスフォーメーション CSS(Outgoing Party E.164 Transformation CSS)]	ドロップダウン リスト ボックスから、発信の着信側の適切なコーリング サーチ スペースを選択します。 [着信側トランスフォーメーション (Called Party Transformations)] ウィンドウ（[コールルーティング (Call Routing)] > [トランスフォーメーション (Transformation)] > [トランスフォーメーションパターン (Transformation Pattern)] > [着信側トランスフォーメーションパターン (Called Party Transformation Pattern)]）で設定した着信側トランスフォーメーション パターンで使用するパーティションを含むコーリング サーチ スペースを選択します。
[適用オン (Apply On)]	コーリング サーチ スペースを元の番号に適用するのか、ルーティング トランスフォーメーション番号に適用するのかを選択します。
[着信トランスフォーメーションプロファイルの設定 (Incoming Transformation Profile Settings)]	
[着信の発呼側トランスフォーメーションプロファイル (Incoming Calling Party Transformation Profile)]	[トランスフォーメーションプロファイルの設定 (Transformation Profile Configuration)] ウィンドウ（[コールルーティング (Call Routing)] > [トランスフォーメーション (Transformation)] > [トランスフォーメーションプロファイル (Transformation Profile)]）で設定した適切な着信の発信側トランスフォーメーション プロファイルを選択します（「Cisco IME トランスフォーメーション プロファイルの設定」（P.3-31）を参照）。
[着信の着呼側トランスフォーメーションプロファイル (Incoming Called Party Transformation Profile)]	[トランスフォーメーションプロファイルの設定 (Transformation Profile Configuration)] ウィンドウ（[コールルーティング (Call Routing)] > [トランスフォーメーション (Transformation)] > [トランスフォーメーションプロファイル (Transformation Profile)]）で設定した適切な着信の着信側トランスフォーメーション プロファイルを選択します（「Cisco IME トランスフォーメーション プロファイルの設定」（P.3-31）を参照）。

追加情報

「Cisco IME の設定チェックリスト」（P.3-6）

PSTN アクセス トランクの設定

PSTN に到達する可能性のあるコールを処理するすべての SIP、MGCP、または H.323 トランクを PSTN トランクとして設定します。PSTN アクセス トランクがあると、システムでは、Voice Call Records（VCRs; 音声コール レコード）を Cisco Intercompany Media Engine（Cisco IME）サーバに送信できます。PSTN アクセス トランクを設定するには、[トランクの設定 (Trunk Configuration)] ウィンドウの [PSTN アクセス (PSTN Access)] チェックボックスをオンにし、適切な E.164 トランスフォーメーションを選択します。PSTN アクセス トランクを設定していない場合、Cisco Unified Communications Manager では、コールの終了後に VCR をアップロードしません。

ネットワーク内の SIP トランクが PSTN に接続している SIP ゲートウェイに接続している場合は、この SIP トランクを PSTN アクセス トランクとして設定できます。クラスタ間トランクの別の SIP トランクがネットワーク内の別のクラスタに接続している場合は、このトランクからのコールが PSTN にルーティングされることがないため、この SIP トランクを PSTN アクセス トランクとして設定する必要はありません。

手順

ステップ 1　[デバイス (Device)] > [トランク (Trunk)] を選択し、PSTN アクセス トランクとして設定するトランクを検索します。

ステップ 2　[PSTN アクセス (PSTN Access)] チェックボックスをオンにします。

ステップ 3　[E.164 トランスフォーメーションプロファイル (E.164 Transformation Profile)] ドロップダウン リスト ボックスで、[E.164 トランスフォーメーションの設定 (E.164 Transformation Configuration)] ウィンドウ（[拡張機能 (Advanced Features)] > [Intercompany Media Services] > [E.164 トランスフォーメーション (E.164 Transformation)]）で作成した適切な E.164 トランスフォーメーションを選択します。このプロファイルにより、着信者番号および発信者番号が +E.164 形式に変換されます。コール検証のために、+E.164 形式の番号である必要があります。

このドロップダウン リスト ボックスでプロファイルを選択しなかった場合、Cisco Unified Communications Manager では、VCR を Cisco Intercompany Media Engine サーバにアップロードしません。

追加情報

「Cisco IME の設定チェックリスト」（P.3-6）

Cisco IME 機能設定の入力

Cisco Intercompany Media Engine（Cisco IME）に適用する機能パラメータを設定するには、[Intercompany Media Service 機能設定 (Intercompany Media Services Feature Configuration)] ウィンドウを使用します。

[Intercompany Media Service 機能設定 (Intercompany Media Services Feature Configuration)] ウィンドウにアクセスするには、[拡張機能 (Advanced Features)] > [Intercompany Media Services] > [機能設定 (Feature Configuration)] を選択します。

設定項目の表

表 3-13 では、Intercompany Media Services 機能の設定値について説明します。

関連する手順については、「Cisco IME の設定チェックリスト」（P.3-6）を参照してください。

表 3-13　Intercompany Media Service 機能の設定値

フィールド	説明
Intercompany Media Services パラメータ	
[MGCP FXS/FXO を使用する IME コールの許可 (Allow IME Calls through MGCP FXS/FXO)]	Cisco IME で、ファクス機への接続に使用される MGCP FXS/FXO アナログ ゲートウェイ デバイスを使用した Cisco IME コールの発信を許可するかどうかを指定します。MGCP FXO/FXS ゲートウェイで Cisco IME コールを発信できるようにするには、[はい (True)] を選択します。MGCP FXO/FXS ゲートウェイで Cisco IME コールを発信できるようにしない場合は、[いいえ (False)] を選択します。 デフォルト値は [いいえ (False)] です。
[ドメイン内 IME の有効化 (Enable Intradomain IME)]	企業内の別のクラスタへのコールに対して Cisco IME を使用可能にするかどうかを指定します。通常は、クラスタ間トランクでクラスタ間のコールを管理しますが、同じドメイン内のクラスタ間で PSTN を使用している場合は、このフィールドを使用可能にすることにより、Cisco IME を使用して、このクラスタ間のパターンを学習できます。 Cisco IME を使用可能にするには [はい (True)] を選択します。Cisco IME を使用不可にするには [いいえ (False)] を選択します。 デフォルト値は [いいえ (False)] です。
[IME 学習ルートを使用する MWI の許可 (Allow MWI via IME Learned Routes)]	Cisco Unified Communications Manager で、Message Waiting Indicator（MWI; メッセージ受信インジケータ）通知に Cisco IME 学習ルートを使用できるかどうかを指定します。Cisco Unified Communications Manager で MWI メッセージに Cisco IME 学習ルートを使用できるようにするには、[はい (True)] を選択します。Cisco Unified Communications Manager で MWI メッセージに Cisco IME 学習ルートを使用できないようにするには、[いいえ (False)] を選択します。 デフォルト値は [はい (True)] です。
[接続先企業の SIP トランク IME 接続タイマー (SIP Trunk IME Connection Timer for Destination Enterprise)]	Cisco IME SIP トランクが接続先企業への学習ルート用に存在している SIP Uniform Resource Identifier（URI; ユニフォーム リソース識別子）への接続の確立を試行する時間を秒数で指定します。このタイマーが期限切れになったとき、この接続先企業へのこの学習ルートで使用可能な次の URI があれば、SIP トランクは、その URI への接続を確立しようとします。 デフォルト値は 2 秒です。有効な値の範囲は 1 ～ 5 です。

表 3-13　Intercompany Media Service 機能の設定値（続き）

フィールド	説明
[IME コールのファイアウォール接続要求タイマー (Firewall Connection Request Timer for IME Calls)]	Cisco Unified Communications Manager で Cisco IME ファイアウォールとの TCP 接続の確立を待機する時間を、秒数で指定します。タイマーが期限切れになる前に Cisco Unified Communications Manager 接続要求に対する接続応答がファイアウォールから送信されない場合、Cisco Unified Communications Manager では、Cisco IME ファイアウォールを経由せずにコールを続行します。つまり、Cisco Unified Communications Manager は PSTN コールを発信します。 デフォルト値は 2 秒です。有効な値の範囲は 1 ～ 5 です。
[IME コールのファイアウォールマッピング応答タイマー (Firewall Mapping Response Timer for IME Calls)]	Cisco Unified Communications Manager で Cisco IME ファイアウォールとのマッピング トランザクション（要求と応答）の完了を待機する時間を、秒数で指定します。タイマーが期限切れになる前に Cisco Unified Communications Manager マップ アドレス要求に対するマップ アドレス応答がファイアウォールから送信されない場合、Cisco Unified Communications Manager では、Cisco IME ファイアウォールを経由せずにコールを続行します。つまり、Cisco Unified Communications Manager は PSTN コールを発信します。 デフォルト値は 2 秒です。有効な値の範囲は 1 ～ 5 です。
[IME コールのファイアウォールマッピング接続アイドルタイマー (Firewall Mapping Connection Idle Timer for IME Calls)]	Cisco IME ファイアウォールが Cisco Unified Communications Manager との接続を切断せずに、Cisco Unified Communications Manager と Cisco IME ファイアウォールの間の接続をアイドルのままにすることができる時間を分単位で指定します。 このタイマーは、Cisco Unified Communications Manager が Cisco IME ファイアウォールに新しいコール要求を送信しなくなると開始されます。 このフィールドで大きい値を選択すると、Cisco IME ファイアウォールを経由する新しいコールを接続するときの遅延を短縮でき、小さい値を選択すると、接続をすみやかに閉じることができます。値を小さくするとセキュリティが向上しますが、新しいコールを確立するときに、わずかに遅延することがあります。 デフォルト値は 10 です。有効な値の範囲は、5 ～ 60 です。

表 3-13　Intercompany Media Service 機能の設定値（続き）

フィールド	説明
[IME 失敗コール試行しきい値 (IME Failed Call Attempt Threshold)]	超過した場合に、Cisco Unified Communications Manager で IMEQualityAlertEntry アラームを生成する、失敗 Cisco IME コール試行の割合を指定します。 失敗 Cisco IME コール設定試行の割合がこのフィールドで定義したしきい値未満であり、[IME コールのフォールバック試行しきい値 (IME Call Fallback Attempt Threshold)] フィールドで指定しているフォールバックしきい値を超えていない場合、Cisco Unified Communications Manager は IMEQualityAlertExit アラームをトリガーします。この結果、IMEQualityAlertEntry アラームがクリアされます。 大きいしきい値を入力すると、システムは失敗 Cisco IME コール試行に対して寛容になるため、Cisco Unified Communications Manager がアラームをトリガーするまでのコールの失敗数が増えます。値を大きくすると、軽微なネットワーク障害がある場合に有用です。 小さいしきい値を入力すると、システムは Cisco IME コール設定の失敗に対して寛容でなくなるため、Cisco Unified Communications Manager が IMEQualityAlertEntry アラームをトリガーするまでのコールの失敗数が少なくなります。 デフォルト値は 50 % です。有効な値の範囲は、10 ～ 100 です。
[IME コールのフォールバック試行しきい値 (IME Call Fallback Attempt Threshold)]	これを超過した場合に Cisco Unified Communications Manager で IMEQualityAlertEntry アラームを生成する、PSTN にフォールバックされるアクティブ Cisco IME コールの割合を指定します。 通話中に PSTN にフォールバックされた Cisco IME コールの割合がこのフィールドに定義したしきい値を下回っており、失敗 Cisco IME コール設定試行の割合が [IME 失敗コール試行しきい値 (IME Failed Call Attempt Threshold)] フィールドに指定した値よりも小さい場合、Cisco Unified Communications Manager は IMEQualityAlertExit アラームを生成します。この結果、IMEQualityAlertEntry アラームがクリアされます。 大きいしきい値を入力すると、システムは、通話中に PSTN にフォールバックされる Cisco IME コールに対して寛容になるため、Cisco Unified Communications Manager がアラームをトリガーするまでに PSTN にフォールバックされるコールの数が多くなります。値を大きくすると、軽微なネットワーク障害がある場合に有用です。 小さいしきい値を入力すると、システムは通話中に PSTN にフォールバックされる Cisco IME コールに対して寛容でなくなるため、Cisco Unified Communications Manager が IMEQualityAlertEntry アラームをトリガーするまでのフォールバックされるコールの数が少なくなります。 デフォルト値は 50 です。有効な値の範囲は、10 ～ 100 です。

表 3-13　Intercompany Media Service 機能の設定値（続き）

フィールド	説明
[IME 品質アラート評価間隔 (IME Quality Alert Evaluation Interval)]	Cisco Unified Communications Manager で [IME 失敗コール試行しきい値 (IME Failed Call Attempt Threshold)] パラメータおよび [IME コールのフォールバック試行しきい値 (IME Call Fallback Attempt Threshold)] パラメータのステータスを検査して、IMEQualityAlertEntry アラームの生成を続行するかどうかを判定するために使用する、時間間隔を秒数で指定します。 デフォルト値は 120 です。有効な値の範囲は、30 ～ 1800 です。
[アウトバウンドコールに Intercompany Media Engine(IME) を使用 (Use Intercompany Media Engine (IME) for Outbound Calls)]	デバイスで Cisco Intercompany Media Engine 機能を使用してコールを発信できるようにするかどうかを指定します。デバイスで Cisco IME コールを発信できるようにするには、[はい (True)] を選択します。デバイスで Cisco IME コールを発信できるようにしない場合は、[いいえ (False)] を選択します。 デフォルト値は [はい (True)] です。

追加情報

「Cisco IME の設定チェックリスト」（P.3-6）

接続の確認

Cisco Unified Communications Manager サーバと Cisco Intercompany Media Engine（Cisco IME）サーバは、Validation Access Protocol（VAP）を使用して通信します。このサーバ間の通信がないと、Cisco Unified Communications Manager は Cisco IME ルートを学習できず、ユーザは Cisco IME コールを発信できません。VAP 接続が存在するかどうかを判断するには、Cisco Unified Communications Manager サーバが Cisco IME サーバに登録されていることおよび Cisco Unified Communications Manager サーバが Vservice を Cisco IME サーバにパブリッシュしていることを確認する必要があります。

次の項を参照してください。

- 「登録ステータス」（P.3-43）
- 「Vservice のパブリッシュ」（P.3-44）
- 「DID のパブリッシュ」（P.3-45）

追加情報

「Cisco IME の設定チェックリスト」（P.3-6）

登録ステータス

Cisco Unified Communications Manager サーバと Cisco Intercompany Media Engine（Cisco IME）サーバの間の接続のステータスは、次のいずれかの方法を使用してモニタできます。

（注）　登録ステータスの確認を終えれば、Cisco Unified Communications Manager サーバは Cisco IME サービス（Vservice）を Cisco IME サーバにパブリッシュしたことを確認することにより、引き続き Cisco Unified Communications Manager サーバと Cisco IME サーバの間の接続を確認できます（「Vservice のパブリッシュ」（P.3-44）を参照）。

CLI を使用する場合

Cisco Intercompany Media Engine CLI で次のコマンドを入力します。

show ime vapstatus summary

このコマンドは、ポート番号の示すクライアントの登録ステータスを表示します。Registration Status が *Registered* になっており、Client IP ADDR が Cisco Unified Communications Manager サーバの IP アドレスになっていることを確認してください。

次の例は、Cisco Unified Communications Manager が Cisco IME サーバに登録されている show ime vapstatus summary コマンドの出力を示します。

```
admin:show ime vapstatus summary
    VAP Client Connection Details
        Registration Status ...... Registered
        Client IP ADDR............ 10.94.150.96
        Client Handle ............ 1
        Packets Sent ............106
        Packets Rcvd ............106
        VAPServer Name ..........vapuser
        Missed Keep Alive Count ..0
        Connection Up Time .......3 hours 7 min 0 sec
```

RTMT を使用する場合

RTMT を使用して Cisco Unified Communications Manager サーバにアクセスし、次のメニューおよびカウンタを選択します。

[システム(System)] > [パフォーマンス(Performance)] > [パフォーマンス モニタリングを開く(Open Performance Monitoring)] > [IME クライアントインスタンス(IME Client Instance)] > [VAPStatus]

Cisco IME サーバと Cisco Unified Communications Manager サーバの間に接続が存在する場合、カウンタは 1（正常）です。有効な値は、0（不明）、1（正常）、2（正常でない）です。

（注）　このカウンタは、プライマリとセカンダリの Cisco IME サーバ間の接続をモニタします。

追加情報

「Cisco IME の設定チェックリスト」（P.3-6）

Vservice のパブリッシュ

Cisco Intercompany Media Engine（Cisco IME）サーバに対する Cisco Unified Communications Manager サーバの登録ステータスの確認を終えれば、Cisco Unified Communications Manager サーバが Cisco IME サービス（Vservice）を Cisco IME サーバにパブリッシュしたことを確認することにより、引き続きサーバ間の接続を確認できます。

Cisco Unified Communications Manager は、[Intercompany Media Service の設定(Intercompany Media Service Configuration)] ウィンドウ（[拡張機能(Advanced Features)] > [Intercompany Media Services] > [サービス(Service)]）の [アクティブ化(Activated)] チェックボックスをオンにした後で、Vservice をパブリッシュします。

パブリッシュされた Vservice は、アクティブなサービスが Cisco Unified Communications Manager 上に存在しており、このサービスが Cisco IME サーバに接続していることを示します。

Vservice のパブリッシュを確認するには、Cisco IME コマンド ラインで **show ime vservice details** コマンドを入力します。

次の例は、Cisco Unified Communications Manager が Vservice をパブリッシュしているコマンドの出力を示します。VServiceProfiles フィールドは、[Intercompany Media Service の設定 (Intercompany Media Service Configuration)] ウィンドウで入力した Cisco IME サービス名と一致しています。

```
admin: show ime vservice details
    VServiceProfiles: Vservice12-ccm18
    VServiceId = 3834353762636435
    overlay = intercompanymedianetwork
    domain  = cisco.com
    DiDCount (max) = 100
    SIPURI =
    sip:d954c46b-51b4-ea2d-cda4-8a20134279f6@cisco.com:5082;maddr=10.94.150.96;transport=t
    cp
```

（注）　Vservice のパブリッシュの確認を終えれば、Cisco Unified Communications Manager サーバが DID を IME 分散キャッシュにパブリッシュしたことを確認することにより、引き続き Cisco Unified Communications Manager サーバと Cisco IME サーバの接続を確認できます（「DID のパブリッシュ」（P.3-45）を参照）。

追加情報

「Cisco IME の設定チェックリスト」（P.3-6）

DID のパブリッシュ

Cisco Unified Communications Manager サーバと Cisco Intercompany Media Engine（Cisco IME）サーバの間の接続を確認した後で、Cisco IME サーバが IME 分散キャッシュに登録済みパターン（DID）をパブリッシュしたことを確認できます。DID のパブリッシュを確認するには、次の方法を使用します。

CLI を使用する場合

Cisco Intercompany Media Engine CLI で次のコマンドを入力します。

utils ime fetch did *E.164 number*

このコマンドの出力は、Cisco IME サーバが IME 分散キャッシュに DID をパブリッシュしたかどうかおよびその番号を所有しているノードを示します。

Cisco IME RTMT

RTMT を使用して Cisco Unified Communications Manager サーバにアクセスし、次のメニューおよびカウンタを選択します。

[システム (System)] > [パフォーマンス (Performance)] > [パフォーマンス モニタリングを開く (Open Performance Monitoring)] > [IME クライアントインスタンス (IME Client Instance)] > [PublishedRoutes]

このカウンタは、すべての Cisco IME クライアント インスタンスにわたって、IME 分散キャッシュに正常にパブリッシュされた DID の合計数を示します。

フォールバック プロファイルの設定

フォールバック プロファイルは、Cisco Intercompany Media Engine（Cisco IME）コールを PSTN にフォールバックするために Cisco Unified Communications Manager で使用する複数の値を定義します。フォールバック プロファイルは、Cisco Unified Communications Manager が通話中のフォールバックを試行するときの Quality of Service のレベルおよび Cisco Unified Communications Manager で PSTN コールを呼び出すために使用するフォールバック番号を定義します。

フォールバック プロファイルとリンクされている番号にユーザがコールを発信した場合、発信側の Cisco Unified Communications Manager は、着信側の Cisco Unified Communications Manager に設定されているフォールバック電話番号を受信します。ASA が PSTN へのフォールバックをトリガーした場合、Cisco Unified Communications Manager は PSTN コール用のフォールバック番号を使用します。

フォールバック プロファイルの設定とフォールバック機能パラメータの設定を終えたら、フォールバック プロファイルを IME 登録済みグループと関連付けます（**[拡張機能 (Advanced Features)] > [Intercompany Media Services] > [登録済みグループ (Enrolled Group)]**）。

（注）　コールを PSTN にフォールバックする場合は、[フォールバック機能設定 (Fallback Feature Configuration)] ウィンドウ（[拡張機能 (Advanced Features)] > [フォールバック (Fallback)] > [フォールバック機能設定 (Fallback Feature Configuration)]）の [IME コールのフォールバックの有効化 (Enable Fallback for IME Calls)] パラメータを必ず設定してください。

[フォールバックプロファイルの設定 (Fallback Profile Configuration)] ウィンドウにアクセスするには、[拡張機能 (Advanced Features)] > [フォールバック (Fallback)] > [フォールバックプロファイル (Fallback Profile)] を選択します。

GUI の使用方法

Cisco Unified Communications Manager の管理の Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）を使用してレコードを検索、削除、設定、またはコピーする方法については、「Cisco Unified Communications Manager の管理の基礎」（P.3-2）およびそのサブセクションを参照してください。GUI の使用方法とボタンおよびアイコンの機能の詳細が説明されています。

設定項目の表

表 3-14 では、フォールバック プロファイルの設定値について説明します。

関連する手順については、「Cisco IME の設定チェックリスト」（P.3-6）を参照してください。

表 3-14　フォールバック プロファイルの設定値

フィールド	説明
[フォールバックプロファイル情報 (Fallback Profile Information)]	
[名前 (Name)]	フォールバック プロファイルの一意の名前を入力します。この名前には、最長 32 文字まで指定できます。
[説明 (Description)]	フォールバック プロファイルの内容を表す名前を入力します。説明には、最長 128 文字まで指定できます （オプション）。

表 3-14　フォールバック プロファイルの設定値（続き）

フィールド	説明
[コールセットアップフォールバックの設定(Call Setup Fallback Settings)]	
[アドバタイズされたフォールバックのE.164番号(Advertised Fallback Directory E.164 Number)]	Cisco Unified Communications Manager で Cisco IME コールを PSTN にフォールバックするときに使用する +E.164 DID 番号を指定します。入力する番号は + で始まる必要があり、15 桁まで入力できます。 コールの受信側からの Cisco Unified Communications Manager はコールの発信側の Cisco Unified Communications Manager にこの番号を渡して、このフォールバック プロファイルで指定しているレベルを下回るサービスの品質になったときに、発信側の Cisco Unified Communications Manager で PSTN へのフォールバックを開始できるようにします。 たとえば、発信側の企業がフォールバック DID として +14089023232 を受信した場合、発信側の企業は、PSTN 経由でこの番号をこのフォールバック DID を送信した受信側の企業にルーティングする、ルート パターンまたはトランスレーション パターンを持つ必要があります。いずれのデバイスにも割り当てられていない専用の +E.164 番号を使用する必要があります。

表 3-14　フォールバック プロファイルの設定値（続き）

フィールド	説明
[コールフォールバックのトリガー設定(Call Fallback Trigger Settings)]	
[フォールバックのQOSの重要度レベル(Fallback QOS Sensitivity Level)]	PSTN にコールをフォールバックする条件を判定するために IME 対応の ASA で使用する、RTP オーディオ ストリームの重要度レベルを指定します。Cisco Unified Communications Manager は、ASA ファイアウォールに、この値を送信します。次のいずれかのオプションを選択します。 • [フォールバックの無効化(Disable Fallback)]：このオプションは、通話中のフォールバック機能を使用不可にします。このオプションをオンにした場合は、Cisco IME VoIP コールの PSTN へのフォールバックは行われません。 • [ユーティリティ(Utility)]：このオプションでは、最低品質の Cisco IME コールが保持されます。このオプションでは、一定品質の VoIP は実現されませんが、最もコストの高い PSTN 経由で再ルーティングするのではなく、VoIP ネットワーク上で保持されるコールの数を最大にすることができます。接続時間の長いコールにこのオプションを使用することはお勧めしません。このオプションは、コールの品質を問わずに、IP ネットワーク経由でできるだけ多数のコールを保持する場合に、推奨されます。 • [適応可能(Accommodative)]：Cisco IME VoIP コール上のオーディオについて、基本レベルまたは低レベルの品質を受け入れる場合に、このオプションを選択します。このレベルの場合、IME 対応の ASA では、コールのオーディオ品質が望ましい品質を下回る場合でも、PSTN にフォールバックするのではなく、IP ネットワーク経由のコールを保持しようとします。 • [基準(Nominal)]：優良または PSTN コールより優れた品質を持つ Cisco IME VoIP コールを保持する場合に、このオプションを選択します。相当に高品質で高速なインターネット接続に基づく、大部分の企業に導入される品質です（デフォルト）。 • [中レベル(Moderate)]：このオプションでは、最良の QoS を持つ Cisco IME VoIP コールのみが保持されます。QoS 統計値の低いコールは、PSTN にフォールバックされます。このオプションの場合、コールの両端の企業は、ティア 1 またはティア 2 のネットワークを持つ必要があります。企業がこのネットワーク要件を満たしていない場合、コールは PSTN 経由でルーティングされます。 • [アグレッシブ(Aggressive)]：このオプションでは、優れた QoS 品質を持つ Cisco IME VoIP コール、つまり、QoS プロビジョニング VoIP と実質的に等しいコールのみが保持されます。このレベルのコールに対する QoS 統計値を満たさないすべてのコールは、PSTN にフォールバックされます。このオプションの場合、コールの両端の企業は、ティア 1 またはティア 2 のネットワークを持つ必要があります。企業がこのネットワーク要件を満たしていない場合、コールは PSTN 経由でルーティングされます。 デフォルトは、[フォールバック機能設定(Fallback Feature Configuration)] ウィンドウ（[拡張機能(Advanced Features)] > [フォールバック(Fallback)] > [フォールバック機能設定(Fallback Feature Configuration)]）の [フォールバックのQOSの重要度レベル(Fallback QOS Sensitivity Level)] パラメータの値です。

表 3-14　フォールバック プロファイルの設定値（続き）

フィールド	説明
[フォールバックのコール設定 (Fallback Call Settings)]	
[フォールバックのコール CSS(Fallback Call CSS)]	フォールバック コールを発信側 Cisco Unified Communications Manager クラスタ上の PSTN にルーティングするために使用するコーリング サーチ スペースを選択します。デフォルトは [コーリングデバイス AAR のコーリングサーチスペース (Calling device AAR Calling Search Space)] です。 AAR コーリング サーチ スペースを定義していない場合、システム設定によっては、再ルーティング CSS を使用できます。
[フォールバックのコール応答タイマー (Fallback Call Answer Timer)]	Cisco TAC エンジニアから指示される場合を除いて、この値を変更しないでください。 このフィールドは、発信側 Cisco Unified Communications Manager で、通話中のフォールバック PSTN コールへの応答を待機する時間を秒数で指定します（1 ～ 10）。 デフォルト値は、[フォールバック機能設定 (Fallback Feature Configuration)] ウィンドウ（**[拡張機能 (Advanced Features)] > [フォールバック (Fallback)] > [フォールバック機能設定 (Fallback Feature Configuration)]**）の [フォールバックのコール応答タイマー (Fallback Call Answer Timer)] の値です。 **（注）** [フォールバック機能設定 (Fallback Feature Configuration)] ウィンドウの [フォールバックのコール応答タイマー (Fallback Call Answer Timer)] フィールドの値がここで設定する値より大きい場合に通話中のフォールバックが起きると、フォールバック コールでは、[フォールバック機能設定 (Fallback Feature Configuration)] ウィンドウの値を使用します。
[フォールバックのコール処理設定 (Fallback Call Handling Settings)]	
[フォールバックの電話番号パーティション (Fallback Directory Number Partition)]	フォールバック コールをルーティングするときに Cisco Unified Communications Manager が使用するパーティションを選択します。 このパーティションは、フォールバック番号のコールを受信するゲートウェイ デバイスで使用する、コーリング サーチ スペースに含まれている必要があります。 デフォルトは、デフォルト パーティションです。 パーティションおよびコーリング サーチ スペースの設定の詳細については、『*Cisco Unified Communications Manager アドミニストレーション ガイド*』を参照してください。

表 3-14　フォールバック プロファイルの設定値（続き）

フィールド	説明
[フォールバックの電話番号 (Fallback Directory Number)]	（オプション）このフィールドは、フォールバック電話番号の非 E.164 バージョンを指定するために使用します。 たとえば、アドバタイズされた +E.164 フォールバック番号が +14089023092 で、着信番号をルーティングする前に 7 桁に正規化する場合、フォールバック電話番号は 9023092 です。 このフィールドに値を指定していない場合は、+E.164 番号が番号分析の対象になります。 **ヒント** +E.164 バックプレーンをサポートするダイヤル プランを使用する場合は、このフィールドをブランクのままにすることができます。
[発信者 ID の部分一致の桁数 (Number of Digits for Caller ID Partial Match)]	このフィールドには、着信フォールバック コールと特定の Cisco IME コールを一致していると見なすために一致する必要のある最小桁数を指定します。 フォールバック コールを受信した場合、Cisco Unified Communications Manager では、フォールバック対象の特定の Cisco IME コールと着信コールを照合するためのキーとして、着信コールの発信者 ID を使用します。発信者 ID 番号は PSTN 内で変換できるため、Cisco Unified Communications Manager では、一部の桁が一致すれば一致する発信者 ID と見なすことができる、部分照合アルゴリズムを使用します。 デフォルトは 5 桁です。

追加情報

「Cisco IME の設定チェックリスト」（P.3-6）

フォールバック機能パラメータの設定

通話中の Cisco Intercompany Media Engine（Cisco IME）コールを PSTN にフォールバックするときに適用される機能パラメータを設定するには、[フォールバック機能設定 (Fallback Feature Configuration)] ウィンドウを使用します。

[フォールバックプロファイルの設定 (Fallback Profile Configuration)] ウィンドウにアクセスするには、[拡張機能 (Advanced Features)] > [フォールバック (Fallback)] > [フォールバック機能設定 (Fallback Feature Configuration)] を選択します。

設定項目の表

表 3-15 では、フォールバックの設定値について説明します。

関連する手順については、「Cisco IME の設定チェックリスト」（P.3-6）を参照してください。

表 3-15　フォールバック機能の設定値

フィールド	説明
[IME コールのフォールバックの有効化 (Enable Fallback for IME Calls)]	Cisco Unified Communications Manager で PSTN フォールバックを使用するかどうかを指定します。フォールバックに関する他のすべての設定は、この値で上書きされます。 PSTN フォールバックが行われるには、コールの発信側と受信側でこのパラメータをオンにする必要があります。 デフォルトは [はい (True)] です。
[フォールバックの QOS の重要度レベル (Fallback QOS Sensitivity Level)]	ASA ファイアウォールでコールを PSTN にフォールバックする条件を判別するために使用する重要度レベルを指定します。Cisco Unified Communications Manager は、ASA ファイアウォールに、この値を送信します。 このパラメータは、[フォールバックプロファイルの設定 (Fallback Profile Configuration)] ウィンドウ（[拡張機能 (Advanced Features)] > [フォールバック (Fallback)] > [フォールバックプロファイル (Fallback Profile)]）の [フォールバックの QOS の重要度レベル (Fallback QOS Sensitivity Level)] に読み込まれるデフォルト値になり、フォールバック プロファイルを定義していない場合のデフォルトの重要度レベルにもなります。 このパラメータは、PSTN フォールバックのときに、受信側に適用されます。 デフォルト値は [基準 (Nominal)] 重要度です。
[DTMF 相関番号のフォールバック番号 (Fallback Number of DTMF Correlation Digits)]	Cisco Unified Communications Manager で通話中のフォールバック PSTN コールに使用する DTMF の桁数を指定します。 このパラメータは、PSTN フォールバックのときに、受信側に適用されます。 デフォルト値は 4 です。有効な値の範囲は、4 ～ 20 です。
[フォールバック DTMF 収集タイマー (Fallback DTMF Collection Timer)]	Cisco Unified Communications Manager で、通話中のフォールバック PSTN コールの間に DTMF 桁の収集を待機する時間（秒数）を指定します。 このパラメータは、PSTN フォールバックのときに、受信側に適用されます。 デフォルト値は 3 です。有効な値の範囲は 1 ～ 10 です。

表 3-15　フォールバック機能の設定値（続き）

フィールド	説明
[フォールバックのコール応答タイマー (Fallback Call Answer Timer)]	アラート通知を受け取った後に、Cisco Unified Communications Manager で、通話中のフォールバック PSTN コールに対する応答の待機を続行する時間（秒数）を指定します。 このパラメータは、PSTN フォールバックのときに、発信側に適用されます。 このパラメータは、フォールバック プロファイルに取り込まれるデフォルト値になり、プロファイルが定義されていない場合のデフォルト値にもなります。 デフォルト値は 3 です。有効な値の範囲は 1 ～ 10 です。 （注）　このウィンドウの [フォールバックのコール応答タイマー (Fallback Call Answer Timer)] フィールドに入力する値が、[フォールバックプロファイルの設定 (Fallback Profile Configuration)] ウィンドウ（[拡張機能 (Advanced Features)] > [フォールバック (Fallback)] > [フォールバックプロファイル (Fallback Profile)]）の [フォールバックのコール応答タイマー (Fallback Call Answer Timer)] フィールドに設定する値より大きい場合、通話中のフォールバックが発生したときのフォールバック コールでは、[フォールバック機能設定 (Fallback Feature Configuration)] ウィンドウの値が使用されます。
[フォールバックのコール CSS(Fallback Call CSS)]	フォールバック コールのルーティングで使用するコーリング サーチ スペースを指定します。 このパラメータは、PSTN フォールバックのときに、発信側に適用されます。 デフォルト値は [AAR コーリングサーチスペース (AAR Calling Search Space)] です。

追加情報

「Cisco IME の設定チェックリスト」（P.3-6）

Intercompany Media Service のファイアウォール情報の設定

ASA マッピング サービスの IP アドレスおよびポートを設定するには、[Intercompany Media Service のファイアウォールの設定 (Intercompany Media Services Firewall Configuration)] ウィンドウを使用します。この情報は、インターネットに接している通常のトラフィックが Cisco Intercompany Media Engine（Cisco IME）トラフィックと同じ Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）を経由しないオフパス配置モデルを実装した場合に設定する必要があります。

発信コールの試行中、SIP INVITE メッセージは、オフパス Cisco IME 対応の ASA にルーティングされる必要があります。Cisco Unified Communications Manager は、リモート エンタープライズ（Cisco IME 学習ルートで検出）のグローバル IP/ポートを Cisco IME 対応の ASA 上の内部 IP/ポートにマッピングする要求を ASA に送信します。Cisco Unified Communications Manager は、次に、この内部 IP/ポートをルーティングする SIP INVITE を開始します。Cisco IME 対応の ASA は、IME 学習ルー

トから入手したリモート エンタープライズのグローバル IP/ポートにマッピングして、NAT を実行します。オフパス Cisco IME 対応の ASA は、このシグナリング セッションをプロキシ処理し、このグローバル IP/ポート（リモート エンタープライズの Cisco IME 対応の ASA）への TLS セッションを開始します。

[Intercompany Media Service のファイアウォールの設定 (Intercompany Media Services Firewall Configuration)] ウィンドウにアクセスするには、[拡張機能 (Advanced Features)] > [Intercompany Media Services] > [ファイアウォール (Firewall)] を選択します。

GUI の使用方法

Cisco Unified Communications Manager の管理の Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）を使用してレコードを検索、削除、設定、またはコピーする方法については、「Cisco Unified Communications Manager の管理の基礎」（P.3-2）およびそのサブセクションを参照してください。GUI の使用方法とボタンおよびアイコンの機能の詳細が説明されています。

設定項目の表

表 3-16 では、Intercompany Media Services のファイアウォールの設定値について説明します。

関連する手順については、「Cisco IME の設定チェックリスト」（P.3-6）を参照してください。

表 3-16　Intercompany Media Service のファイアウォールの設定値

フィールド	説明
[名前 (Name)]	ASA マッピング サービスの一意の名前を指定します。
[説明 (Description)]	ASA マッピング サービスの説明を指定します （オプション）。
[IP アドレス (IP Address)]	ASA マッピング サービスの IP アドレスを入力します。
[ポート (Port)]	ASA マッピング サービスのポートを入力します。

Cisco Intercompany Media Engine 学習ルート

学習ルートには、システムが Cisco Intercompany Media Engine（Cisco IME）を介して学習したすべての +E.164 番号のリストが示されます。特定のルートを使用可能にしたり、使用不可にしたりすることができます。特定のルートに問題があり、トラブルシューティングのために使用不可にする必要がある場合に、使用不可にすることができます。

[IME 学習ルート (IME Learned Routes)] ウィンドウにアクセスするには、[拡張機能 (Advanced Features)] > [Intercompany Media Services] > [学習ルート (Learned Route)] を選択します。

GUI の使用方法

Cisco Unified Communications Manager の管理の Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）を使用してレコードを検索、削除、設定、またはコピーする方法については、「Cisco Unified Communications Manager の管理の基礎」（P.3-2）およびそのサブセクションを参照してください。GUI の使用方法とボタンおよびアイコンの機能の詳細が説明されています。

設定項目の表

表 3-17 では、Intercompany Media Services 学習ルートの設定値について説明します。

関連する手順については、「Cisco IME の設定チェックリスト」（P.3-6）を参照してください。

表 3-17　Cisco Intercompany Media Engine 学習ルートの設定値

フィールド	説明
[E.164]	このフィールドには、Cisco Unified Communications Manager が学習した +E.164 番号が示されます。
[ドメイン (Domain)]	このフィールドには、+E.164 番号のドメインが示されます。
[シグナリング (Signaling)]	このフィールドには、あて先 DID に到達するために使用されるダイナミック SIP トランクのあて先リモート IP アドレスとポートが示されます。
[学習 (Learned-On)]	このフィールドには、Cisco Unified Communications Manager がこのルートを学習した日付が示されます。
[有効期限 (Expires-On)]	このフィールドには、このルートの有効期限が切れる日付が示されます。ルートは、学習日付の 1 年後に期限切れになります。
[管理者対応 (Admin Enabled)]	このフィールドは、学習ルートが使用中かどうかを示します。データベースから削除せずにルートを使用不可にするには、[管理者対応 (Admin Enabled)] チェックボックスをオフにします。ルートを使用可能にして Cisco Intercompany Media Engine でそのルートを使用できるようにするには、このチェックボックスをオンにします。

追加情報

「Cisco IME の設定チェックリスト」（P.3-6）

関連項目

- 「Cisco Unified Communications Manager の管理の基礎」（P.3-2）
- 「Cisco IME の設定チェックリスト」（P.3-6）
- 「Cisco IME サーバ接続の設定」（P.3-15）
- 「Cisco Unified Communications Manager と Cisco Intercompany Media Engine サーバの間の TLS 接続の設定」（P.3-17）
- 「Cisco IME 登録済みグループの設定」（P.3-21）
- 「Cisco IME 登録済みパターンの設定」（P.3-22）
- 「Cisco IME 除外グループの設定」（P.3-24）
- 「Cisco IME 除外番号の設定」（P.3-24）
- 「Cisco IME 信頼グループの設定」（P.3-25）
- 「Cisco IME 信頼要素の設定」（P.3-26）
- 「Cisco IME サービスの設定」（P.3-27）
- 「外部 IP アドレスおよびポート情報の設定」（P.3-30）
- 「Cisco IME 用トランスフォーメーション パターンの設定」（P.3-31）

- 「Cisco IME トランスフォーメーション プロファイルの設定」（P.3-31）
- 「Cisco IME E.164 トランスフォーメーションの設定」（P.3-37）
- 「PSTN アクセス トランクの設定」（P.3-39）
- 「Cisco IME 機能設定の入力」（P.3-39）
- 「接続の確認」（P.3-43）
- 「フォールバック プロファイルの設定」（P.3-46）
- 「フォールバック機能パラメータの設定」（P.3-50）
- 「Intercompany Media Service のファイアウォール情報の設定」（P.3-52）
- 「Cisco Intercompany Media Engine 学習ルート」（P.3-53）

関連項目

CHAPTER 4

Cisco ASA 設定

Cisco Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）ファイアウォールは、Cisco Intercompany Media Engine ソリューションのセキュリティにおいて、重要な役割を果たします。この項では、コマンド ライン インターフェイスを使用した ASA の設定についてと、Web ベースの GUI アプリケーションの ASDM について説明します。

プロキシ設定のガイドラインと制限事項

コンテキスト モード ガイドライン

シングル コンテキスト モードのみがサポートされています。

ファイアウォール モード ガイドライン

ルーティング ファイアウォール モードのみがサポートされています。

IPv6 ガイドライン

IPv6 アドレスはサポートされていません。

その他のガイドラインおよび制限事項

Cisco Intercompany Media Engine には、以下の制限があります。

- ファクスはサポートされていません。ファクス機能を SIP トランクで無効にする必要があります。
- Cisco Unified Intercompany Media Engine のステートフル フェールオーバーはサポートされていません。フェールオーバーの間は、Cisco Intercompany Media Engine プロキシを通過中の既存のコールは切断されますが、フェールオーバーが終了した後、新規のコールはこのプロキシを正常に通過します。
- Cisco Intercompany Media Engine プロキシでは、複数の適応型セキュリティ アプライアンスのインターフェイス上での Cisco UCM の使用はサポートされていません。適応型セキュリティ アプライアンスで、マッピング サービスのリスニング インターフェイスを指定し、Cisco UCM を 1 つの信頼できるインターフェイスに接続する必要があるため、特に、オフパス配置では、1 つの信頼できるインターフェイスで Cisco UCM を使用する必要があります。
- 複数 MIME はサポートされていません。
- 既存の SIP の機能およびメッセージのみがサポートされています。

- H.264 はサポートされていません。
- RTCP はサポートされていません。適応型セキュリティ アプライアンスは、内部インターフェイスから外部インターフェイスに送信されるすべての RTCP トラフィックをドロップします。適応型セキュリティ アプライアンスは、内部インターフェイスからの RTCP トラフィックを SRTP トラフィックに変換しません。
- 適応型セキュリティ アプライアンスで設定された Cisco Intercompany Media Engine プロキシは、リモート環境への各接続のダイナミック SIP トランクを作成します。ただし、SIP トランクごとに一意な件名を設定できません。Cisco Intercompany Media Engine プロキシは、プロキシに設定された件名を 1 つだけ設定できます。

  また、Cisco Intercompany Media Engine プロキシに設定した件名 DN は、ローカル Cisco UCM に設定したドメイン名と一致します。
- Cisco Intercompany Media Engine プロキシのサービス ポリシー ルールが（サービス ポリシー コマンドを使用せずに）削除されたり、再設定されたりした場合、適応型セキュリティ アプライアンスを通過する最初のコールは失敗します。Cisco UCM は接続がクリアされたことを認識せず、シグナリングのためにそのクリアされた IME SIP トランクの使用を試行するため、コールは PSTN にフェールオーバーします。

  この問題を解決するには、**clear connection all** コマンドを追加で入力し、適応型セキュリティ アプライアンスを再起動する必要があります。フェールオーバーのために失敗する場合、プライマリ適応型セキュリティ アプライアンスからの接続はスタンバイ適応型セキュリティ アプライアンスに同期されません。
- UC-IME プロキシが有効な適応型セキュリティ アプライアンスで **clear connection all** コマンドが発行されます。IME コールが PSTN にフェールオーバーされた後、SCCP IP Phone の発信側と着信側の間の次の IME コールは完了しますが、音声がなく、シグナリング セッションが確立するとドロップされます。

  SCCP IP Phone 間の IME コールは、両方向の IME SIP トランクを使用します。つまり、発信側から着信側へのシグナリングは IME SIP トランクを使用します。次に着信側は、リターン シグナリングおよびメディア変換のためにリバース IME SIP トランクを使用します。ただし、この接続が適応型セキュリティ アプライアンスですでにクリアされている場合、IME コールが失敗する原因となります。

  次の IME コール（**clear connection all** コマンドが発行されてから 3 番目のコール）は正常に完了します。

  （注） この制限は、発信側および着信側の IP Phone が SIP で設定されている場合、適用されません。

- 適応型セキュリティ アプライアンスでは、ライセンスが取得されている必要があります。また、IME コール ボリュームを処理するために十分な TLS プロキシ セッションが設定されている必要もあります。TLS プロキシ セッションに関するライセンス要件については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

  この制限は、IME コールを完了するために必要な TLS プロキシ セッションが十分に残されていないと、IME コールが PSTN にフォールバックできないために発生します。2 つの SCCP IP Phone 間の IME コールでは、適応型セキュリティ アプライアンスが 2 つの TLS プロキシ セッションを使用して TLS ハンドシェイクを正常に完了する必要があります。

  たとえば、適応型セキュリティ アプライアンスが最大 100 の TLS プロキシ セッションを使用できるように設定されていて、SCCP IP Phone 間の IME コールがすでに 101 TLS プロキシ セッションを確立しているとします。この例では、次の IME コールは発信側の SCCP IP Phone によって正常

に開始されますが、着信側 SCCP IP Phone によって受け取られると失敗します。着信側 IP Phone の呼び出し音は鳴りますが、コールに応答すると、TLS ハンドシェイクが完了していないために、そのコールは切断します。コールは PSTN にフォールバックされません。

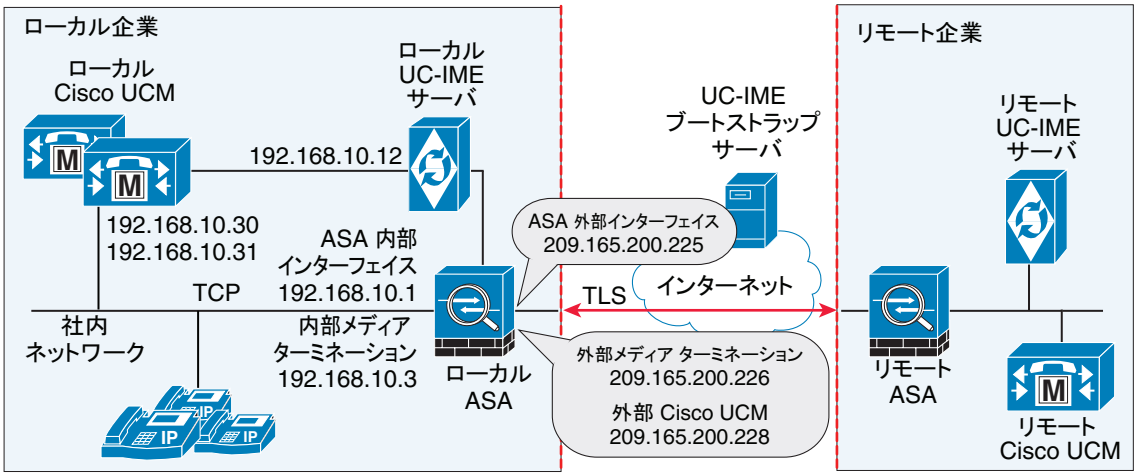
プロキシ CLI 設定

この項では、次のトピックについて取り上げます。

Cisco Intercompany Media Engine の設定のタスク フロー

図 4-1 では、Cisco Intercompany Media Engine の基本配置の例が示されています。以下のタスクには、図 4-1 に基づくコマンド ラインの例が含まれています。

図 4-1　基本（インライン）配置タスクの例



（注）　ステップ 1 からステップ 8 は、基本（インライン）配置およびオフパス配置の両方に適用され、ステップ 9 は、オフパス配置にのみ適用されます。

基本配置で Cisco Intercompany Media Engine を構成する場合、以下のタスクを実行します。

ステップ 1　Cisco UCM のスタティック NAT を設定します。「Cisco Intercompany Media Engine プロキシの NAT 設定」（P.4-4）を参照してください。

または

UCM サーバの PAT を設定します。「Cisco UCM サーバの PAT 設定」（P.4-6）を参照してください。

ステップ 2　Cisco Intercompany Media Engine プロキシのアクセス リストを作成します。「Cisco Intercompany Media Engine プロキシのアクセス リストの作成」（P.4-8）を参照してください。

ステップ 3　Cisco Intercompany Media Engine プロキシのメディア ターミネーション アドレス インスタンスを作成します。「メディア ターミネーション インスタンスの作成」（P.4-9）を参照してください。

ステップ 4　Cisco Intercompany Media Engine プロキシを作成します。「Cisco Intercompany Media Engine プロキシの作成」（P.4-11）を参照してください。

ステップ 5　トラストポイントを作成し、Cisco Intercompany Media Engine プロキシの証明書を生成します。「トラストポイントの作成および証明書の生成」（P.4-14）を参照してください。

ステップ 6　TLS プロキシを作成します。「TLS プロキシの作成」（P.4-17）を参照してください。

ステップ 7　Cisco Intercompany Media Engine プロキシの SIP インスペクションを設定します。「Cisco Intercompany Media Engine プロキシの SIP インスペクションの有効化」（P.4-18）を参照してください。

ステップ 8　（オプション）環境内の TLS を設定します。「（オプション）ローカル環境内での TLS の設定」（P.4-20）を参照してください。

ステップ 9　（オプション）オフパス シグナリングを設定します。「（オプション）オフパス シグナリングの設定」（P.4-24）を参照してください。

（注）　オフパス配置で Cisco Intercompany Media Engine プロキシを設定しているときのみ、ステップ 9 を実行できます。

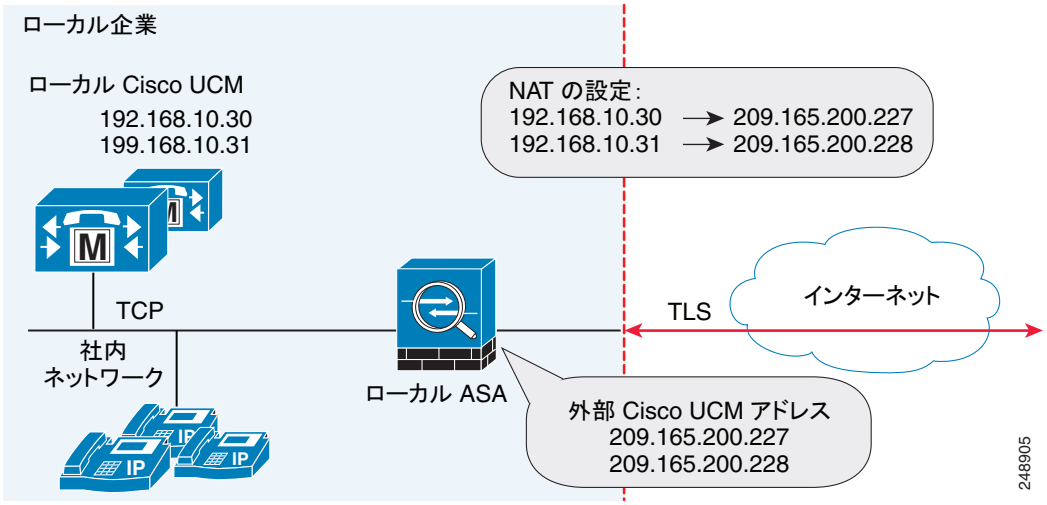
Cisco Intercompany Media Engine プロキシの NAT 設定

自動 NAT を設定するには、まずオブジェクトを設定し、そのオブジェクト コンフィギュレーション モードで **nat** コマンドを使用します。

このタスクのコマンド ラインの例は、基本（インライン）配置に基づいています。このタスクのコマンド ラインの例を説明する図については、図 4-1（P.4-3）を参照してください。

また、Cisco Intercompany Media Engine プロキシの PAT を設定することもできます。「Cisco UCM サーバの PAT 設定」（P.4-6）を参照してください。

図 4-2　配置に関する NAT の設定例



Cisco UCM サーバの自動 NAT ルールを設定するには、以下の手順を実行します。

	コマンド	目的

ステップ 1	`hostname(config)# object network name`
	例：
	`hostname(config)# object network ucm_real_192.168.10.30`
	`hostname(config)# object network ucm_real_192.168.10.31`
		変換する Cisco UCM の実際のアドレスのネットワーク オブジェクトを設定します。

ステップ 2	`hostname(config-network-object)# host ip_address`
	例：
	`hostname(config-network-object)# host 192.168.10.30`
	`hostname(config-network-object)# host 192.168.10.31`
		ネットワーク オブジェクトの Cisco UCM ホストの実際の IP アドレスを指定します。

ステップ 3	（オプション）
	`hostname(config-network-object)# description string`
	例：
	`hostname(config-network-object)# description "Cisco UCM Real Address"`
		ネットワーク オブジェクトの説明を示します。

ステップ 4	`hostname(config-network-object)# exit`	オブジェクト コンフィギュレーション モードを終了します。

ステップ 5	`hostname(config)# object network name`
	例：
	`hostname(config)# object network ucm_map_209.165.200.228`
		Cisco UCM のマップされたアドレスのネットワーク オブジェクトを設定します。

ステップ 6	`hostname(config-network-object)# host ip_address`
	例：
	`hostname(config-network-object)# host 209.165.200.228`
		ネットワーク オブジェクトの Cisco UCM ホストのマップされた IP アドレスを指定します。

ステップ 7	（オプション）
	`hostname(config-network-object)# description string`
	例：
	`hostname(config-network-object)# description "Cisco UCM Mapped Address"`
		ネットワーク オブジェクトの説明を示します。

	コマンド	目的
ステップ 8	`hostname(config-network-object)# exit`	オブジェクト コンフィギュレーション モードを終了します。

ステップ 9	`hostname(config)# nat (inside,outside) source static real_obj mapped_obj`
	例：
	`hostname(config)# nat (inside,outside) source static ucm_real_192.168.10.30 ucm_209.165.200.228`
	`hostname(config)# nat (inside,outside) source static ucm_real_192.168.10.31 ucm_209.165.200.228`
		この手順で作成されたネットワーク オブジェクトでのアドレス変換を指定します。
		ここで、*real_obj* は、このタスクのステップ 1 で作成した *name* です。
		ここで、*mapped_obj* は、このタスクのステップ 5 で作成した *name* です。

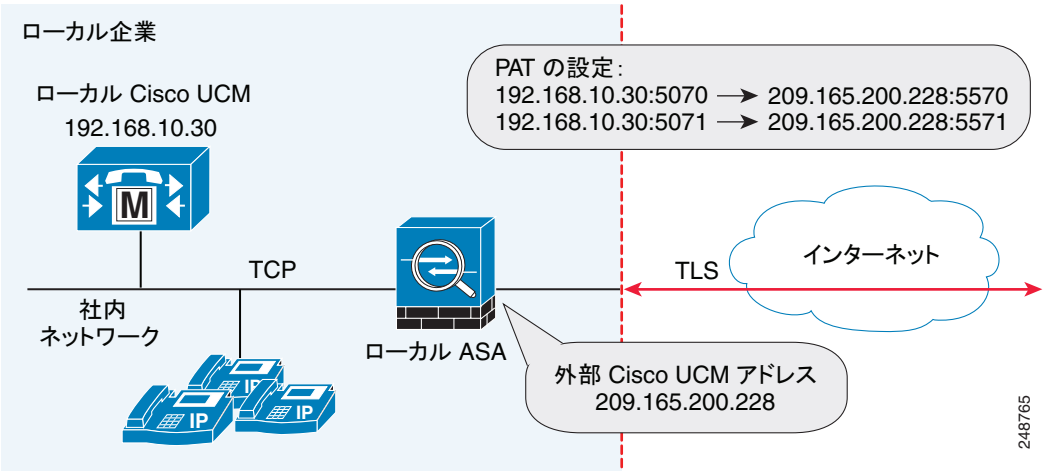
次のタスクの内容

Cisco Intercompany Media Engine プロキシのアクセス リストを作成します。「Cisco Intercompany Media Engine プロキシのアクセス リストの作成」（P.4-8）を参照してください。

Cisco UCM サーバの PAT 設定

Cisco Intercompany Media Engine プロキシの NAT を設定する別の方法としてこのタスクを実行します。

図 4-3　　配置に関する PAT の設定例



（注）　Cisco UCM サーバに対して NAT を設定していないときのみ、この手順を実行できます。

Cisco UCM サーバの PAT を設定するには、以下の手順を実行します。

	コマンド	目的
ステップ 1	hostname(config)# **object network** *name* 例： hostname(config)# object network ucm-pat-209.165.200.228	変換する Cisco UCM の外部 IP アドレスについてネットワーク オブジェクトを設定します。
ステップ 2	hostname(config-network-object)# **host** *ip_address* 例： hostname(config-network-object)# host 209.165.200.228	ネットワーク オブジェクトの Cisco UCM ホストの実際の IP アドレスを指定します。
ステップ 3	hostname(config-network-object)# **exit**	オブジェクト コンフィギュレーション モードを終了します。
ステップ 4	hostname(config)# **object service** *name* 例： hostname(config)# object service tcp_5070 hostname(config)# object service tcp_5071	外部 Cisco Intercompany Media Engine ポートのサービス オブジェクトを作成します。
ステップ 5	hostname(config-service-object)# **tcp source eq** *port* 例： hostname(config-service-object)# tcp source eq 5070 hostname(config-service-object)# tcp source eq 5071	ポート番号を指定します。
ステップ 6	hostname(config-service-object)# **exit**	オブジェクト コンフィギュレーション モードを終了します。
ステップ 7	hostname(config)# **object network** *name* 例： hostname(config)# object network ucm-real-192.168.10.30 hostname(config)# object network ucm-real-192.168.10.31	Cisco UCM の実際の IP アドレスを表すネットワーク オブジェクトを設定します。
ステップ 8	hostname(config-network-object)# **host** *ip_address* 例： hostname(config-network-object)# host 192.168.10.30 hostname(config-network-object)# host 192.168.10.31	ネットワーク オブジェクトの Cisco UCM ホストの実際の IP アドレスを指定します。
ステップ 9	hostname(config-network-object)# **exit**	オブジェクト コンフィギュレーション モードを終了します。
ステップ 10	hostname(config)# **object service** *name* 例： hostname(config)# object service tcp_5570 hostname(config)# object service tcp_5571	Cisco UCM SIP ポートのサービス オブジェクトを作成します。
ステップ 11	hostname(config-service-object)# **tcp source eq** *port* 例： hostname(config-service-object)# tcp source eq 5570 hostname(config-service-object)# tcp source eq 5571	ポート番号を指定します。

	コマンド	目的
ステップ 12	hostname(config-service-object)# **exit**	オブジェクト コンフィギュレーション モードを終了します。
ステップ 13	hostname(config)# **nat (inside,outside) source static** *real_obj mapped_obj* **service** *real_port mapped_port* **例：** hostname(config)# nat (inside,outside) source static ucm-real-192.168.10.30 ucm-pat-209.165.200.228 service tcp_5070 tcp_5570 hostname(config)# nat (inside,outside) source static ucm-real-192.168.10.31 ucm-pat-128.106.254.5 service tcp_5071 tcp_5571	Cisco UCM のスタティック マッピングを作成します。 *ここで、real_obj は、このタスクのステップ 1 で作成した名前です。* *ここで、mapped_obj は、このタスクのステップ 7 で作成した名前です。* *ここで、real_port は、このタスクのステップ 4 で作成した名前です。* *ここで、mapped_obj は、このタスクのステップ 10 で作成した名前です。*

Cisco Intercompany Media Engine プロキシのアクセス リストの作成

Cisco UCM サーバに到達するように Cisco Intercompany Media Engine プロキシのアクセス リストを設定するには、以下の手順を実行します。

このタスクのコマンド ラインの例は、基本（インライン）配置に基づいています。このタスクのコマンド ラインの例を説明する図については、図 4-1（P.4-3）を参照してください。

	コマンド	目的
ステップ 1	hostname(config)# **access-list** *id* **extended permit tcp any host** *ip_address* **eq** *port* **例：** hostname(config)# access-list incoming extended permit tcp any host 192.168.10.30 eq 5070	Access Control Entry（ACE; アクセス コントロール エントリ）を追加します。アクセス リストは、同じアクセス リスト ID を使用する 1 つ以上の ACE によって構成されます。この ACE は、指定されたポートでの Cisco Intercompany Media Engine 接続の着信アクセスを許可して、アクセス コントロールを提供します。 *ip_address* 引数に、Cisco UCM の実際の IP アドレスを指定します。
ステップ 2	hostname(config)# **access-group** *access-list* **in interface** *interface_name* **例：** hostname(config)# access-group incoming in interface outside	アクセス リストをインターフェイスにバインドします。
ステップ 3	hostname(config)# **access-list** *id* **extended permit tcp any host** *ip_address* **eq** *port* **例：** hostname(config)# access-list ime-inbound-sip extended permit tcp any host 192.168.10.30 eq 5070	ACE を追加します。この ACE によって、適応型セキュリティ アプライアンスは Cisco Intercompany Media Engine のインバウンド SIP トラフィックを許可できます。このエントリは、クラス マップおよびポリシー マップのトラフィックを分類するために使用されます。 **（注）**　ここで設定するポートは、Cisco UCM で設定されるトランクの設定に一致します。この設定に関する詳細については、Cisco Unified Communications Manager の関連資料を参照してください。

	コマンド	目的
ステップ 4	hostname(config)# **access-list** *id* **extended permit tcp** *ip_address mask* **any range** *range* **例：** hostname(config)# access-list ime-outbound-sip extended permit tcp 192.168.10.30 255.255.255.255 any range 5000 6000	ACE を追加します。この ACE によって、適応型セキュリティ アプライアンスは Cisco Intercompany Media Engine のアウトバウンド SIP トラフィックを許可できます（例では、ソースが 192.168.10.30 で、宛先ポートの範囲が 5000 ～ 6000 のすべての TCP トラフィックが許可されます）。このエントリは、クラス マップおよびポリシー マップのトラフィックを分類するために使用されます。 **（注）** Cisco UCM と Cisco Intercompany Media Engine サーバとの間の TCP トラフィックには、このポート範囲を使用しないでください（その接続が適応型セキュリティ アプライアンスを経由する場合）。
ステップ 5	hostname(config)# **access-list** *id* **permit tcp any host** *ip_address* **eq 6084** **例：** hostname(config)# access-list ime-traffic permit tcp any host 192.168.10.12 eq 6084	ACE を追加します。この ACE によって、適応型セキュリティ アプライアンスは Cisco Intercompany Media Engine サーバからリモート Cisco Intercompany Media Engine サーバへのトラフィックを許可できます。
ステップ 6	hostname(config)# **access-list** *id* **permit tcp any host** *ip_address* **eq 8470** **例：** hostname(config)# access-list ime-bootserver-traffic permit tcp any host 192.168.10.12 eq 8470	ACE を追加します。この ACE によって、適応型セキュリティ アプライアンスは Cisco Intercompany Media Engine サーバから Cisco Intercompany Media Engine のブートストラップ サーバへのトラフィックを許可できます。

次のタスクの内容

Cisco Intercompany Media Engine プロキシの適応型セキュリティ アプライアンス上にメディア ターミネーション インスタンスを作成します。「メディア ターミネーション インスタンスの作成」（P.4-9）を参照してください。

メディア ターミネーション インスタンスの作成

ガイドライン

設定するメディア ターミネーション アドレスは、以下の要件を満たしている必要があります。

- グローバル インターフェイスを使用せずに、インターフェイスで、メディア ターミネーション アドレスを設定する場合、Cisco Intercompany Media Engine プロキシのサービス ポリシーを適用する前に、少なくとも 2 つのインターフェイス（内部インターフェイスと外部インターフェイス）に 1 つのメディア ターミネーション アドレスを設定する必要があります。設定しない場合、プロキシで SIP インスペクションを有効にしていると、エラー メッセージを受け取ります。

（注） Cisco は、グローバル メディア ターミネーション アドレスを設定せずに、インターフェイスで Cisco Intercompany Media Engine プロキシのメディア ターミネーション アドレスを設定することをお勧めします。

- Cisco Intercompany Media Engine プロキシは、一度に 1 つのタイプのメディア ターミネーション インスタンスを使用できます。たとえば、すべてのインターフェイス用の 1 つのグローバル メディア ターミネーション アドレスを設定するか、または異なるインターフェイス用の 1 つのメ

ディア ターミネーション アドレスを設定できます。しかし、同時にグローバル メディア ターミネーション アドレスとインターフェイスごとに設定されたメディア ターミネーション アドレスを使用できません。

（注）　プロキシのメディア ターミネーション アドレスを作成した後に、Cisco Intercompany Media Engine プロキシ設定に何らかの変更を加えた場合、**no media-termination** コマンドを使用してメディア ターミネーション アドレスを再設定する必要があります。その際、以下の手順のように再設定します。

手順

Cisco Intercompany Media Engine プロキシとともに使用するメディア ターミネーション インスタンスを作成します。

このタスクのコマンド ラインの例は、基本（インライン）配置に基づいています。このタスクのコマンド ラインの例を説明する図については、図 4-1（P.4-3）を参照してください。

Cisco Intercompany Media Engine プロキシ用にメディア ターミネーション インスタンスを作成するには、以下の手順を実行します。

	コマンド	目的

ステップ 1	`hostname(config)# media-termination instance_name`
	例：
	`hostname(config)# media-termination uc-ime-media-term`
		Cisco Intercompany Media Engine プロキシに接続するメディア ターミネーション インスタンスを作成します。

ステップ 2	`hostname(config-media-termination)# address ip_address interface intf_name`
	例：
	`hostname(config-media-termination)# address 209.165.200.228 interface outside`
		適応型セキュリティ アプライアンスの外部インターフェイスによって使用されるメディア ターミネーション アドレスを設定します。
		外部 IP アドレスは、パブリックにルーティング可能なアドレスで、そのインターフェイスのアドレス範囲内で未使用の IP アドレスである必要があります。
		UC-IME プロキシ設定については、「Cisco Intercompany Media Engine プロキシの作成」（P.4-11）を参照してください。**no service-policy** コマンドについては、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

	コマンド	目的
ステップ 3	hostname(config-media-termination)# **address** *ip_address* **interface** *intf_name* **例：** hostname(config-media-termination)# address 192.168.10.3 interface inside	適応型セキュリティ アプライアンスの内部インターフェイスによって使用されるメディア ターミネーション アドレスを設定します。 **（注）** この IP アドレスは、そのインターフェイスの同じサブネット内で未使用の IP アドレスである必要があります。
ステップ 4	（オプション） hostname(config-media-termination)# ***rtp-min-port*** *port1* **rtp-maxport** *port2* **例：** hostname(config-media-termination)# rtp-min-port 1000 rtp-maxport 2000	Cisco Intercompany Media Engine プロキシの RTP 最小ポートおよび RTP 最大ポート制限を設定します。Cisco Intercompany Media Engine をサポートするコール数を増やす必要があるときに、メディア ターミネーション ポイントの RTP ポート範囲を設定します。 ここで、*port1* には、メディア ターミネーション ポイントの RTP ポート範囲の最小値を指定します。port1 には、1024 ～ 65535 までの値を指定できます。デフォルトでは、*port1* の値は 16384 です。 ここで、*port2* には、メディア ターミネーション ポイントの RTP ポート範囲の最大値を指定します。port2 には、1024 ～ 65535 までの値を指定できます。デフォルトでは、*port2* の値は 32767 です。

次のタスクの内容

メディア ターミネーション インスタンスを作成したら、Cisco Intercompany Media Engine プロキシを作成します。「Cisco Intercompany Media Engine プロキシの作成」（P.4-11）を参照してください。

Cisco Intercompany Media Engine プロキシの作成

Cisco Intercompany Media Engine プロキシを作成するには、以下の手順を実行します。

このタスクのコマンド ラインの例は、基本（インライン）配置に基づいています。このタスクのコマンド ラインの例を説明する図については、図 4-1（P.4-3）を参照してください。

（注） プロキシが SIP インスペクションに対して有効なときに、以下の手順で示されている Cisco Intercompany Media Engine プロキシのいかなる設定も変更できません。この手順で説明されている設定のいずれかを変更するには、SIP インスペクションから Cisco Intercompany Media Engine プロキシを削除します。

	コマンド	目的
ステップ 1	hostname(config)# **uc-ime** *uc_ime_name* **例：** hostname(config)# uc-ime local-ent-ime	Cisco Intercompany Media Engine プロキシを設定します。 ここで、*uc_ime_name* は、Cisco Intercompany Media Engine プロキシの名前です。この名前は、64 文字までに制限されています。 適応型セキュリティ アプライアンスでは、Cisco Intercompany Media Engine プロキシを 1 つだけ設定できます。
ステップ 2	hostname(config-uc-ime)# **media-termination** *mta_instance_name* **例：** hostname(config-uc-ime)# media-termination ime-media-term	Cisco Intercompany Media Engine プロキシによって使用されるメディア ターミネーション インスタンスを指定します。 **（注）** Cisco Intercompany Media Engine プロキシでメディア ターミネーション インスタンスを指定する前に、このインスタンスを作成する必要があります。 ここで、*mta_instance_name* は、メディア ターミネーション インスタンスの作成のステップ 1 で作成した *instance_name* です。 メディア ターミネーション インスタンスを作成する手順については、「メディア ターミネーション インスタンスの作成」（P.4-9）を参照してください。
ステップ 3	hostname(config-uc-ime)# **ucm address** *ip_address* **trunk-security-mode** [**nonsecure** | **secure**] **例：** hostname(config-uc-ime)# ucm address 192.168.10.30 trunk-security-mode non-secure	環境内の Cisco UCM サーバを指定します。Cisco UCM サーバの実際の IP アドレスを指定する必要があります。サーバのマップされた IP アドレスを指定しないでください。 **（注）** SIP トランクが有効な Cisco Intercompany Media Engine を使用するクラスタ内の各 Cisco UCM にエントリを含める必要があります。 ここで、**nonsecure** および **secure** オプションは、Cisco UCM または Cisco UCM のクラスタのセキュリティ モードを指定します。 **（注）** Cisco UCM または Cisco UCM クラスタに対して **secure** を指定すると、Cisco UCM または Cisco UCM クラスタは TLS を開始します。そのため、コンポーネントの TLS を設定する必要があります。「（オプション）ローカル環境内での TLS の設定」（P.4-20）を参照してください。 このタスクで **secure** オプションを指定できます。または、後で環境の TLS を設定する際に、このオプションを更新できます。「（オプション）ローカル環境内での TLS の設定」（P.4-20）のステップ 11 を参照してください。

	コマンド	目的

ステップ 4	`hostname(config-uc-ime)# ticket epoch n password password`
	例：
	`hostname(config-uc-ime)# ticket epoch 1 password password1234`
		Cisco Intercompany Media Engine のチケット エポックおよびパスワードを設定します。
		ここで、*n* は 1 ～ 255 までの整数です。エポックには、パスワードが変更されるたびに更新される整数が入ります。プロキシを初めて設定し、パスワードを初めて入力するときに、エポックの整数として 1 を入力します。パスワードを変更するたびに、新しいパスワードを示すためにエポックを増やします。ユーザはパスワードを変更するたびにエポックの値を増やす必要があります。
		通常は、順番にエポックを増やしますが、適応型セキュリティ アプライアンスを使用すると、エポックを更新する際に任意の値を選択できます。
		エポック値を変更する場合、現在のパスワードは無効となり、新規パスワードを入力する必要があります。
		ここで、*password* には、US-ASCII 文字セットから印刷可能な 10 ～ 64 文字が入ります。使用可能な文字には、0x21 ～ 0x73 までが含まれ、スペース文字は除外されます。
		少なくとも 20 文字以上のパスワードが推奨されています。同時に設定できるパスワードは 1 つだけです。
		チケット パスワードは、フラッシュに格納されます。**show running-config uc-ime** コマンドの出力には、パスワード文字列の代わりに「*****」が表示されます。
		（注） 適応型セキュリティ アプライアンスで設定するエポックおよびパスワードは、Cisco Intercompany Media Engine サーバで設定するエポックおよびパスワードと一致する必要があります。詳細については、Cisco Intercompany Media Engine サーバの関連資料を参照してください。

	コマンド	目的

ステップ 5	（オプション）
	`hostname(config-uc-ime)# fallback monitoring timer timer_millisec | hold-down timer timer_sec`
	例：
	`hostname(config-uc-ime)# fallback monitoring timer 120`
	`hostname(config-uc-ime)# fallback hold-down timer 30`
		Cisco Intercompany Media Engine のフォールバック タイマーを指定します。
		monitoring timer を指定すると、適応型セキュリティ アプライアンスがインターネットから受信する RTP パケットをサンプリングする時間間隔が設定されます。適応型セキュリティ アプライアンスは、このデータ サンプルを使用して、コールに対して PSTN へのフォールバックが必要であるかを判別します。
		ここで、*timer_millisec* には、モニタリング タイマーの長さを指定します。デフォルトでは、モニタリング タイマーの長さは 100 ミリ秒です。使用可能な範囲は、10 ～ 600 ミリ秒です。
		hold-down timer を指定すると、PSTN にフォールバックするかどうかを Cisco UCM に通知するまで適応型セキュリティ アプライアンスが待機する時間が設定されます。
		ここで、*timer_sec* には、ホールドダウン タイマーの長さを指定します。デフォルトでは、ホールドダウン タイマーの長さは 20 秒です。使用可能な範囲は、10 ～ 360 秒です。
		このコマンドを使用してフォールバック タイマーを指定しない場合、適応型セキュリティ アプライアンスはフォールバック タイマーのデフォルト設定を使用します。

ステップ 6	（オプション）
	`hostname(config-uc-ime)# fallback sensitivity-file file_name`
	例：
	`hostname(config-uc-ime)# fallback sensitivity-file ime-fallback-sensitvity.fbs`
		通話中 PSTN フォールバックに使用するファイルを指定します。
		ここで、*file_name* は、.fbs ファイル拡張子を含むディスク上のファイルの名前である必要があります。
		フォールバック ファイルは、Cisco Intercompany Media Engine がコールを PSTN に転送するほどコールの QoS が低下しているかを識別するために使用されます。

次のタスクの内容

ローカル エンティティ信頼ストアに証明書をインストールします。ローカル エンティティによって信頼されたローカル CA で証明書を登録することもできます。

トラストポイントの作成および証明書の生成

適応型セキュリティ アプライアンスによって使用される証明書のキー ペアを生成する必要があります。また、TLS ハンドシェイクで適応型セキュリティ アプライアンスによって送信される証明書を識別するようにトラストポイントを設定する必要があります。

このタスクのコマンド ラインの例は、基本（インライン）配置に基づいています。このタスクのコマンド ラインの例を説明する図については、図 4-1（P.4-3）を参照してください。

（注）　このタスクは、ローカル環境とリモート環境のトラストポイントを作成する方法、およびこれらの環境の間での証明書の交換方法を説明します。このタスクでは、ローカル Cisco UCM とローカル適応型セキュリティ アプライアンスとの間でのトラストポイントの作成および証明書の交換に関する手順は扱われません。ただし、ローカル環境内での追加のセキュリティが必要な場合、「（オプション）ローカル環境内での TLS の設定」（P.4-20）で示されるオプションのタスクを実行する必要があります。そのタスクを実行することにより、ローカル Cisco UCM とローカル適応型セキュリティ アプライアンスとの間でのセキュア TLS 接続が可能となります。そのタスクでは、ローカル Cisco UCM とローカル適応型セキュリティ アプライアンスとの間のトラストポイントを作成する方法が説明されます。

証明書のインストールに関する前提条件

リモート エンティティによって信頼された適応型セキュリティ アプライアンスでプロキシ証明書を作成するには、信頼できる CA から証明書を取得する、またはリモート環境の適応型セキュリティ アプライアンスから証明書をエクスポートします。

リモート環境から証明書をエクスポートするには、リモートの適応型セキュリティ アプライアンスで以下のコマンドを入力します。

hostname(config)# **crypto ca export trustpoint identity-certificate**

適応型セキュリティ アプライアンスは、ターミナルの画面に証明書を表示します。ターミナルの画面から証明書をコピーします。このタスクのステップ 5 で、この証明書のテキストが必要になります。

手順

トラストポイントを作成し、証明書を生成するには、以下の手順を実行します。

	コマンド	目的
ステップ 1	hostname(config)# **crypto key generate rsa label** *key-pair-label* **modulus** *size* **例：** hostname(config)# crypto key generate rsa label local-ent-key modulus 2048	ローカルの適応型セキュリティ アプライアンスで、トラストポイントで使用される RSA キー ペアを作成します。これは、ローカル エンティティの署名付き証明書に関するキー ペアおよびトラストポイントです。 選択するモジュール キー サイズは、設定するセキュリティのレベル、および証明書を取得する CA によって課される制約によって異なります。選択する数が増えれば増えるほど、証明書のセキュリティ レベルは高くなります。ほとんどの CA では、キー モジュール サイズとして 2048 が推奨されています。ただし、 （注）　GoDaddy では、キー モジュール サイズは 2048 である必要があります。
ステップ 2	hostname(config)# **crypto ca trustpoint** *trustpoint_name* **例：** hostname(config)# crypto ca trustpoint local_ent	ローカル エンティティのトラストポイントが作成できるように、指定したトラストポイントのトラストポイント コンフィギュレーション モードを入力します。 トラストポイントは、CA によって発行された証明書に基づく CA ID、場合によってはデバイス ID を表します。名前の最大長は、128 文字です。

	コマンド	目的
ステップ 3	hostname(config-ca-trustpoint)# **subject-name** *X.500_name* **例：** hostname(config-ca-trustpoint)# subject-name cn=Ent-local-domain-name**	登録時に、証明書に示された件名 DN を指定します。 **（注）** ここで入力するドメイン名は、ローカル Cisco UCM で設定したドメイン名と一致する必要があります。Cisco UCM のドメイン名の設定方法については、Cisco Unified Communications Manager の関連資料を参照してください。
ステップ 4	hostname(config-ca-trustpoint)# **keypair** *keyname* **例：** hostname(config-ca-trustpoint)# keypair local-ent-key	認証される公開鍵のキー ペアを指定します。
ステップ 5	hostname(config-ca-trustpoint)# **enroll terminal**	このトラストポイントを登録する方法として、「コピー アンド ペースト」（手動登録）の使用を指定します。
ステップ 6	hostname(config-ca-trustpoint)# **exit**	CA トラストポイント コンフィギュレーション モードを終了します。
ステップ 7	hostname(config)# **crypto ca enroll** *trustpoint* **例：** hostname(config)# crypto ca enroll remote-ent % % Start certificate enrollment ... % The subject name in the certificate will be: % cn=enterpriseA % The fully-qualified domain name in the certificate will @ be: ciscoasa % Include the device serial number in the subject name?[yes/no]: no Display Certificate Request to terminal?[yes/no]: yes	CA での登録プロセスを開始します。 ここで、*trustpoint* は、ステップ 2 で入力した *trustpoint_name* と同じ値です。 手動登録（**enroll terminal** コマンド）でトラストポイントを設定していると、適応型セキュリティ アプライアンスは Base 64 エンコード PKCS10 の証明書要求をコンソールに書き込み、CLI プロンプトを表示します。プロンプトからテキストをコピーします。 証明書要求を CA に送信します。たとえば、プロンプトに表示されたテキストを CA Web サイトの証明書署名要求登録ページに貼り付けます。 CA から署名付き ID 証明書が送られてきたら、この手順のステップ 8 に進みます。
ステップ 8	hostname(config)# **crypto ca import** *trustpoint* **certificate** **例：** hostname(config)# crypto ca import remote-ent certificate	手動登録要求の返信として CA から受け取った署名付き証明書をインポートします。 ここで、*trustpoint* には、ステップ 2 で作成したトラストポイントを指定します。 適応型セキュリティ アプライアンスは、Base 64 形式の署名付き証明書をターミナルに貼り付けるよう求めるプロンプトを表示します。
ステップ 9	hostname(config)# **crypto ca authenticate** *trustpoint* **例：** hostname(config)# crypto ca authenticate remote-ent	CA から受け取ったサードパーティ ID 証明書を認証します。この ID 証明書は、リモート環境用に作成したトラストポイントに関連付けられます。 適応型セキュリティ アプライアンスは、CA からの Base 64 形式の ID 証明書をターミナルに貼り付けるよう求めるプロンプトを表示します。

次のタスクの内容

Cisco Intercompany Media Engine の TLS プロキシを作成します。「TLS プロキシの作成」（P.4-17）を参照してください。

TLS プロキシの作成

ローカル Cisco UCM サーバ、リモート Cisco UCM サーバのどちらの環境でも、TLS ハンドシェイクを開始できるので（クライアントのみが TLS ハンドシェイクを開始できる IP テレフォニーまたは Cisco Mobility Advantage とは異なります）、双方向 TLS プロキシのルールを設定する必要があります。各環境で、TLS プロキシとして適応型セキュリティ アプライアンスを使用できます。

個別に接続が開始されたローカルおよびリモート エンティティの TLS プロキシ インスタンスを作成します。TLS 接続を開始するエンティティは、「TLS クライアント」のロールになります。TLS プロキシには、「クライアント」と「サーバ」の厳密な定義があるため、2 つの TLS プロキシ インスタンスは、いずれのエンティティで接続を開始できるか定義する必要があります。

このタスクのコマンド ラインの例は、基本（インライン）配置に基づいています。このタスクのコマンド ラインの例を説明する図については、図 4-1（P.4-3）を参照してください。

TLS プロキシを作成するには、次の手順を実行します。

	コマンド	目的

ステップ 1	`hostname(config)# tls-proxy proxy_name`
	例：
	`hostname(config)# tls-proxy local_to_remote-ent`
		アウトバウンド接続用の TLS プロキシを作成します。

ステップ 2	`hostname(config-tlsp)# client trust-point proxy_trustpoint`
	例：
	`hostname(config-tlsp)# client trust-point local-ent`
		アウトバウンド接続では、適応型セキュリティ アプライアンスが TLS クライアントのロールを担っているときに、TLS ハンドシェイクで使用するトラストポイントおよび関連する証明書を指定します。適応型セキュリティ アプライアンスが証明書（ID 証明書）を所有する必要があります。
		ここで、*proxy_trustpoint* には、「トラストポイントの作成および証明書の生成」（P.4-14）のステップ 2で **crypto ca trustpoint** コマンドによって定義されたトラストポイントを指定します。

ステップ 3	`hostname(config-tlsp)# client cipher-suite cipher_suite`
	例：
	`hostname(config-tlsp)# client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1`
		アウトバウンド接続に対して、暗号スイートの TLS ハンドシェイク パラメータを制御します。
		ここで、*cipher_suite* には、des-sha1、3des-sha1、aes128-sha1、aes256-sha1、または null-sha1 が入ります。
		クライアント プロキシ（このプロキシはサーバに対して TLS クライアントとして機能します）では、ユーザ定義の暗号スイートによって、デフォルトの暗号スイートまたは **ssl encryption** コマンドによって定義された暗号スイートが置き換えられます。このコマンドを使用して、2 つの TLS セッション間で異なる暗号化を実現します。AES 暗号を Cisco UCM サーバで使用する必要があります。

ステップ 4	`hostname(config-tlsp)# exit`	TLS プロキシ コンフィギュレーション モードを終了します。

	コマンド	目的
ステップ 5	hostname(config)# **tls-proxy** *proxy_name* **例：** hostname(config)# tls-proxy remote_to_local-ent	インバウンド接続用の TLS プロキシを作成します。
ステップ 6	hostname(config-tlsp)# **server trust-point** *proxy_trustpoint* **例：** hostname(config-tlsp)# server trust-point local-ent	**インバウンド**接続では、TLS ハンドシェイク時に提示するプロキシ トラストポイント証明書を指定します。適応型セキュリティ アプライアンスが証明書（ID 証明書）を所有する必要があります。 ここで、*proxy_trustpoint* には、「トラストポイントの作成および証明書の生成」（P.4-14）のステップ 2 で **crypto ca trustpoint** コマンドによって定義されたトラストポイントを指定します。 TLS プロキシには、クライアント プロキシとサーバ プロキシの厳密な定義があるため、2 つの TLS プロキシ インスタンスは、いずれのエンティティで接続を開始できるか定義する必要があります。
ステップ 7	hostname(config-tlsp)# **client cipher-suite** *cipher_suite* **例：** hostname(config-tlsp)# client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1	インバウンド接続に対して、暗号スイートの TLS ハンドシェイク パラメータを制御します。 ここで、*cipher_suite* には、des-sha1、3des-sha1、aes128-sha1、aes256-sha1、または null-sha1 が入ります。
ステップ 8	hostname(config-tlsp)# **exit**	TSL プロキシ コンフィギュレーション モードを終了します。
ステップ 9	hostname(config)# **ssl encryption 3des-sha1 aes128-sha1** [*algorithms*]	SSL/TLS プロトコルが使用する暗号化アルゴリズムを指定します。3des-sha1 と aes128-sha1 を指定する必要があります。その他のアルゴリズムの指定は、オプションです。 **（注）** Cisco Intercompany Media Engine プロキシでは、強度の高い暗号化を使用する必要があります。プロキシに K9 ライセンスを使用するライセンスがあるときは、このコマンドを指定する必要があります。

次のタスクの内容

TLS プロキシを作成したら、そのプロキシを SIP インスペクションに対して有効にします。

Cisco Intercompany Media Engine プロキシの SIP インスペクションの有効化

TLS プロキシを SIP インスペクションに対して有効にし、接続を開始できる両方のエンティティのポリシーを定義します。

このタスクのコマンド ラインの例は、基本（インライン）配置に基づいています。このタスクのコマンド ラインの例を説明する図については、図 4-1（P.4-3）を参照してください。

（注）　SIP インスペクションを有効にした後、Cisco Intercompany Media Engine プロキシの設定を変更する場合、**no service-policy** コマンドを入力し、以下の手順で示されているようにサービス ポリシーを再設定する必要があります。サービス ポリシーの削除および再設定は、既存のコールに影響しませんが、Cisco Intercompany Media Engine プロキシを通過する最初のコールは失敗します。**clear connection** コマンドを入力し、適応型セキュリティ アプライアンスを再起動します。

Cisco Intercompany Media Engine プロキシの SIP インスペクションを有効にするには、以下の手順を実行します。

	コマンド	目的

ステップ 1	`hostname(config)# class-map class_map_name`
	例：
	`hostname(config)# class-map ime-inbound-sip`
		インバウンド Cisco Intercompany Media Engine SIP トラフィックのクラスを定義します。

ステップ 2	`hostname(config-cmap)# match access-list access_list_name`
	例：
	`hostname(config-cmap)# match access-list ime-inbound-sip`
		検査する SIP トラフィックを指定します。
		ここで、*access_list_name* は、タスク Cisco Intercompany Media Engine プロキシのアクセス リストの作成の「ステップ 3」（P.4-8）で作成したアクセス リストです。

ステップ 3	`hostname(config-cmap)# exit`	クラス マップ コンフィギュレーション モードを終了します。

ステップ 4	`hostname(config)# class-map class_map_name`
	例：
	`hostname(config)# class-map ime-outbound-sip`
		Cisco Intercompany Media Engine からのアウトバウンド SIP トラフィックのクラスを定義します。

ステップ 5	`hostname(config)# match access-list access_list_name`
	例：
	`hostname(config-cmap)# match access-list ime-outbound-sip`
		検査するアウトバウンド SIP トラフィックを指定します。
		ここで、*access_list_name* は、タスク Cisco Intercompany Media Engine プロキシのアクセス リストの作成の「ステップ 4」（P.4-9）で作成したアクセス リストです。

ステップ 6	`hostname(config-cmap)# exit`	クラス マップ コンフィギュレーション モードを終了します。

ステップ 7	`hostname(config)# policy-map name`
	例：
	`hostname(config)# policy-map ime-policy`
		トラフィックのクラスのアクションに関連するポリシー マップを定義します。

ステップ 8	`hostname(config-pmap)# class classmap_name`
	例：
	`hostname(config-pmap)# class ime-outbound-sip`
		アクションをクラス マップ トラフィックに割り当てることができるように、クラス マップをポリシー マップに割り当てます。
		ここで、*classmap_name* は、このタスクのステップ 1 で作成した SIP クラス マップの名前です。

ステップ 9	`hostname(config-pmap-c)# inspect sip [sip_map] tls-proxy proxy_name uc-ime uc_ime_map`
	例：
	`hostname(config-pmap-c)# inspect sip tls-proxy local_to_remote-ent uc-ime local-ent-ime`
		TLS プロキシおよび Cisco Intercompany Media Engine プロキシを指定した SIP インスペクション セッションに対して有効にします。

ステップ 10	`hostname(config-cmap-c)# exit`	ポリシー マップ クラス コンフィギュレーション モードを終了します。

	コマンド	目的
ステップ 11	hostname(config-pmap)# **class** *class_map_name* **例：** hostname(config-pmap)# class ime-inbound-sip	アクションをクラス マップ トラフィックに割り当てることができるように、クラス マップをポリシー マップに割り当てます。 ここで、*classmap_name* は、このタスクのステップ 4 で作成した SIP クラス マップの名前です。
ステップ 12	hostname(config-pmap-c)# **inspect sip** [*sip_map*] **tls-proxy** *proxy_name* **uc-ime** *uc_ime_map* **例：** hostname(config-pmap-c)# inspect sip tls-proxy remote-to-local-ent uc-ime local-ent-ime	TLS プロキシおよび Cisco Intercompany Media Engine プロキシを指定した SIP インスペクション セッションに対して有効にします。
ステップ 13	hostname(config-pmap-c)# **exit**	ポリシー マップ クラス コンフィギュレーション モードを終了します。
ステップ 14	hostname(config-pmap)# **exit**	ポリシー マップ コンフィギュレーション モードを終了します。
ステップ 15	hostname(config)# **service-policy** *policymap_name* **global** **例：** hostname(config)# service-policy ime-policy global	すべてのインターフェイスの SIP インスペクションのサービス ポリシーを有効にします。 ここで、*policymap_name* は、このタスクのステップ 7 で作成したポリシー マップの名前です。 UC-IME プロキシ設定については、「Cisco Intercompany Media Engine プロキシの作成」（P.4-11）を参照してください。**no service-policy** コマンドについては、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

次のタスクの内容

TLS プロキシを SIP インスペクションに対して有効にしたら、必要に応じて、環境内の TLS を設定します。「（オプション）ローカル環境内での TLS の設定」（P.4-20）を参照してください。

（オプション）ローカル環境内での TLS の設定

内部ネットワーク内で TCP が使用可能な場合、このタスクは必要ありません。

適応型セキュリティ アプライアンスが参照するように、環境内の TLS は Cisco Intercompany Media Engine トランクのセキュリティ ステータスを参照します。

（注） Cisco UCM で Cisco Intercompany Media Engine トランクの転送セキュリティを変更した場合、同様に、適応型セキュリティ アプライアンスでも変更セキュリティを変更する必要があります。一致していないと、コール失敗が発生します。適応型セキュリティ アプライアンスは、SRTP を非セキュア IME トランクではサポートしません。適応型セキュリティ アプライアンスでは、SRTP がセキュア トランクで許可されていることが想定されています。そのため、TLS を使用する場合、IME トランクの [SRTP を許可 (SRTP Allowed)] をオンにする必要があります。適応型セキュリティ アプライアンスは、セキュア IME トランク コールの RTP への SRTP フォールバックをサポートします。

前提条件

ローカル Cisco UCM で、Cisco UCM 証明書をダウンロードします。詳細については、Cisco Unified Communications Manager の関連資料を参照してください。以下の手順のステップ 6 を実行するときに、この証明書が必要になります。

手順

ローカル環境内で TLS を設定するには、ローカルの適応型セキュリティ アプライアンスで以下の手順を実行します。

	コマンド	目的
ステップ 1	hostname(config)# **crypto key generate rsa label** *key-pair-label* hostname(config)# **crypto ca trustpoint** *trustpoint_name* hostname(config-ca-trustpoint)# **enroll self** hostname(config-ca-trustpoint)# **keypair** *keyname* hostname(config-ca-trustpoint)# **subject-name** *x.500_name* **例：** hostname(config)# crypto key generate rsa label local-ent-key hostname(config)# crypto ca trustpoint local-asa hostname(config-ca-trustpoint)# enroll self hostname(config-ca-trustpoint)# keypair key-local-asa hostname(config-ca-trustpoint)# subject-name *cn=Ent-local-domain-name****., o="Example Corp"	自己署名証明書の RSA キーおよびトラストポイントを作成します。 ここで、*key-pair-label* は、ローカル適応型セキュリティ アプライアンスの RSA キーです。 ここで、*trustpoint_name* は、ローカル適応型セキュリティ アプライアンスのトラストポイントです。 ここで、*keyname* は、ローカル適応型セキュリティ アプライアンスのキー ペアです。 ここで、*x.500_name* には、ローカル適応型セキュリティ アプライアンスの X.500 識別名が入ります。たとえば、*cn=Ent-local-domain-name**** となります。 **（注）** ここで入力するドメイン名は、ローカル Cisco UCM で設定したドメイン名と一致する必要があります。Cisco UCM のドメイン名の設定方法については、Cisco Unified Communications Manager の関連資料を参照してください。
ステップ 2	hostname(config-ca-trustpoint)# **exit**	トラストポイント コンフィギュレーション モードを終了します。

	コマンド	目的
ステップ 3	hostname(config)# **crypto ca export** *trustpoint* **identity-certificate** **例：** hostname(config)# crypto ca export local-asa identity-certificate	ステップ 1 で作成した証明書をエクスポートします。証明書の内容は、ターミナルの画面に表示されます。 ターミナルの画面から証明書をコピーします。この証明書によって、Cisco UCM は、TLS ハンドシェイクで適応型セキュリティ アプライアンスが送信する証明書を検証できます。 ローカル Cisco UCM で、証明書を Cisco UCM トラスト ストアにアップロードします。詳細については、Cisco Unified Communications Manager の関連資料を参照してください。 **（注）** ローカル Cisco UCM に証明書をアップロードする際に入力した件名は、Cisco UCM 上の SIP トランク セキュリティ プロファイルで入力された [X.509 件名 (X.509 Subject Name)] フィールドと比較されます。たとえば、このタスクのステップ 1 で、「Ent-local-domain-name」と入力した場合、Cisco UCM 設定でも「Ent-local-domain-name」と入力する必要があります。
ステップ 4	hostname(config)# **crypto ca trustpoint** *trustpoint_name* hostname(config-ca-trustpoint)# **enroll terminal** **例：** hostname(config)# crypto ca trustpoint local-ent-ucm hostname(config-ca-trustpoint)# enroll terminal	ローカル Cisco UCM のトラストポイントを作成します。 ここで、*trustpoint_name* は、ローカル Cisco UCM のトラストポイントです。
ステップ 5	hostname(config-ca-trustpoint)# **exit**	トラストポイント コンフィギュレーション モードを終了します。
ステップ 6	hostname(config)# **crypto ca authenticate** *trustpoint* **例：** hostname(config)# crypto ca authenticate local-ent-ucm	ローカル Cisco UCM から証明書をインポートします。 ここで、*trustpoint* は、ローカル Cisco UCM のトラストポイントです。 ローカル Cisco UCM からダウンロードした証明書を貼り付けます。この証明書によって、適応型セキュリティ アプライアンスは、TLS ハンドシェイクで Cisco UCM が送信する証明書を検証できます。

	コマンド	目的
ステップ 7	hostname(config)# **tls-proxy** *proxy_name* hostname(config-tlsp)# **server trust-point** *proxy_trustpoint* hostname(config-tlsp)# **client trust-point** *proxy_trustpoint* hostname(config-tlsp)# **client cipher-suite** aes128-sha1 aes256-sha1 3des-sha1 null-sha1 **例：** hostname(config)# tls-proxy local_to_remote-ent hostname(config-tlsp)# server trust-point local-ent-ucm hostname(config-tlsp)# client trust-point local-ent hostname(config-tlsp)# client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1	**outbound** 接続の TLS プロキシを更新します。 ここで、*proxy_name* は、タスク TLS プロキシの作成のステップ 1 で入力した名前です。 ここで、**server trust-point** コマンドの *proxy_trustpoint* は、この手順のステップ 4 で入力した名前です。 ここで、**client trust-point** コマンドの *proxy_trustpoint* は、タスクトラストポイントの作成および証明書の生成のステップ 2で入力した名前です。 **（注）** この手順では、クライアントとサーバの異なるトラストポイントを作成しています。
ステップ 8	hostname(config-tlsp)# **exit**	TLS プロキシ コンフィギュレーション モードを終了します。
ステップ 9	hostname(config)# **tls-proxy** proxy_name hostname(config-tlsp)# **server trust-point** *proxy_trustpoint* hostname(config-tlsp)# **client trust-point** *proxy_trustpoint* hostname(config-tlsp)# **client cipher-suite** aes128-sha1 aes256-sha1 3des-sha1 null-sha1 **例：** hostname(config)# tls-proxy remote_to_local-ent hostname(config-tlsp)# server trust-point local-ent hostname(config-tlsp)# client trust-point local-ent-ucm hostname(config-tlsp)# client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1	**インバウンド**接続用の TLS プロキシを更新します。 ここで、*proxy_name* は、タスク TLS プロキシの作成のステップ 5 で入力した名前です。 ここで、**server trust-point** コマンドの *proxy_trustpoint* は、タスクトラストポイントの作成および証明書の生成のステップ 2で入力した名前です。 ここで、**client trust-point** コマンドの *proxy_trustpoint* は、この手順のステップ 4 で入力した名前です。
ステップ 10	hostname(config-tlsp)# **exit**	TLS プロキシ コンフィギュレーション モードを終了します。
ステップ 11	hostname(config)# **uc-ime** *uc_ime_name* hostname(config-uc-ime)# **ucm address** *ip_address* **trunk-security-mode secure** **例：** hostname(config)# uc-ime local-ent-ime hostname(config-uc-ime)# ucm address 192.168.10.30 trunk-security-mode secure	トランク セキュリティ モードの Cisco Intercompany Media Engine プロキシを更新します。 ここで、*uc_ime_name* は、タスク Cisco Intercompany Media Engine プロキシの作成のステップ 1 で入力した名前です。 タスク Cisco Intercompany Media Engine プロキシの作成のステップ 3 で非セキュアを入力した場合、この手順のみを実行します。

次のタスクの内容

環境内の TLS を設定したので、必要に応じて、オフパス配置のオフパス シグナリングを設定します。「（オプション）オフパス シグナリングの設定」（P.4-24）を参照してください。

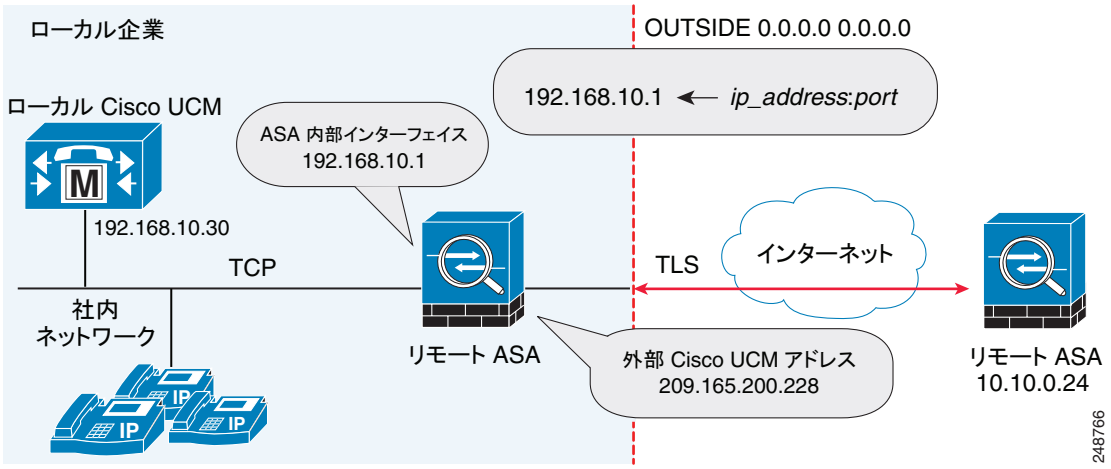
（オプション）オフパス シグナリングの設定

オフパス配置の一部として、Cisco Intercompany Media Engine プロキシを設定しているときのみ、このタスクを実行します。Cisco Intercompany Media Engine を使用したいものの、既存のインターネット ファイアウォールを Cisco Intercompany Media プロキシで有効化された適応型セキュリティ アプライアンス で置き換えたくないときに、オフパス配置を選択できます。

オフパス配置でご使用の環境に配置している既存のファイアウォールは、Cisco Intercompany Media Engine トラフィックを送信できません。

オフパス シグナリングでは、外部 IP アドレスを内部 IP アドレスに変換する必要があります。内部インターフェイス アドレスは、このマッピング サービス設定に使用されます。Cisco Intercompany Media Engine プロキシでは、適応型セキュリティ アプライアンスが、外部アドレスの内部 IP アドレスへのダイナミック マッピングを作成します。そのため、アウトバウンド コールでダイナミック NAT 設定を使用する際、Cisco UCM は SIP トラフィックをこの内部 IP アドレスに送信し、適応型セキュリティ アプライアンスがこのマッピングを使用して、インバウンド コールでの実際の宛先を識別します。オフパス設定のインバウンド コールでは、スタティック NAT または PAT マッピングが使用されます。

図 4-4　　オフパス配置でのオフパス シグナリングの設定例



オフパス シグナリングを設定した後、適応型セキュリティ アプライアンス マッピング サービスはインターフェイス「inside」で要求を受信します。このサービスが要求を受信すると、宛先インターフェイスとして「outside」のダイナミック マッピングを作成します。

Cisco Intercompany Media Engine プロキシのオフパス シグナリングを設定するには、以下の手順を実行します。

	コマンド	目的

ステップ 1	`hostname(config)# object network name`
	例：
	`hostname(config)# object network outside-any`
		オフパス適応型セキュリティ アプライアンスでは、すべての外部アドレスを表すネットワーク オブジェクトを作成します。

ステップ 2	`hostname(config-network-object)# subnet ip_address`
	例：
	`hostname(config-network-object)# subnet 0.0.0.0 0.0.0.0`
		サブネットの IP アドレスを指定します。

ステップ 3	`hostname(config-network-object)# nat (outside,inside) dynamic interface inside`	リモート環境の Cisco UCM のマッピングを作成します。

	コマンド	目的
ステップ 4	hostname(config-network-object)# **exit**	オブジェクト コンフィギュレーション モードを終了します。
ステップ 5	hostname(config)# **uc-ime** *uc_ime_name* **例：** hostname(config)# uc-ime local-ent-ime	タスク「Cisco Intercompany Media Engine プロキシの作成」（P.4-11）で作成した Cisco Intercompany Media Engine プロキシを指定します。 ここで、*uc_ime_name* は、「Cisco Intercompany Media Engine プロキシの作成」（P.4-11）のステップ 1 で指定した名前です。
ステップ 6	hostname(config)# **mapping-service listening-interface** *interface_name* [**listening-port** *port*] **uc-ime-interface** *uc-ime-interface_name* **例：** hostname(config-uc-ime)# mapping-service listening-interface inside listening-port 8060 uc-ime-interface outside	オフパス適応型セキュリティ アプライアンスの場合、マッピング サービスを Cisco Intercompany Media Engine プロキシに追加します。 適応型セキュリティ アプライアンス マッピング サービスのインターフェイスおよびリスニング ポートを指定します。 Cisco Intercompany Media Engine プロキシのために設定できるマッピング サーバは 1 つだけです。 ここで、*interface_name* は、適応型セキュリティ アプライアンスがマッピング要求を受信するインターフェイスの名前です。 ここで、port は、適応型セキュリティ アプライアンスがマッピング要求を受信する TCP ポートです。デバイス上のその他のサービス（Telnet または SSH など）との競合を避けるため、1024 ～ 65535 の間のポート番号を指定する必要があります。デフォルトでは、ポート番号は TCP 8060 です。 ここで、*uc-ime-interface_name* は、リモート Cisco UCM に接続するインターフェイスの名前です。

ASDM を使用したプロキシ設定

この項では、次の内容で構成されています。

- 「UC-IME プロキシ ペインを使用した Cisco UC-IMC プロキシの設定」（P.4-25）
- 「ユニファイド コミュニケーション ウィザードを使用した Cisco UC-IMC プロキシの設定」（P.4-28）

UC-IME プロキシ ペインを使用した Cisco UC-IMC プロキシの設定

[Cisco Intercompany Media Engine(UC-IME) プロキシの設定 (Configure Cisco Intercompany Media Engine(UC-IME)proxy)] ペインを使用して、Cisco Intercompany Media Engine プロキシ インスタンスを追加または編集します。

（注）　Cisco Intercompany Media Engine プロキシは、このプロキシに必要なライセンスが適応型セキュリティ アプライアンスにインストールされていない場合、[ナビゲーション(Navigation)] ペインの [ユニファイドコミュニケーション(Unified Communications)] セクションの下にオプションとして表示されません。

このペインを使用してプロキシ インスタンスを作成しますが、UC-IME プロキシをフル機能で使用する場合、NAT ステートメント、アクセス リスト、および MTA の作成、証明書の設定、TLS プロキシの作成、SIP インスペクションの有効化など追加のタスクを完了する必要があります。

UC-IME プロキシがインターネット トラフィックのオフパスまたはインラインのどちらで配置されているかに応じて、Cisco UCM の組み込み NAT ステートメント、または PAT ステートメントを使用し、適切なネットワーク オブジェクトを作成する必要があります。

このペインは、[設定(Configuration)] > [ファイアウォール(Firewall)] > [ユニファイドコミュニケーション(Unified Communications)] > [UC-IME プロキシ(UC-IME Proxy)] から使用できます。

ステップ 1　[設定(Configuration)] > [ファイアウォール(Firewall)] > [ユニファイドコミュニケーション(Unified Communications)] > [UC-IME プロキシ(UC-IME Proxy)] からペインを開きます。

ステップ 2　[Cisco UC-IME プロキシの有効化(Enable Cisco UC-IME proxy)] チェックボックスをオンにして、機能を有効にします。

ステップ 3　[Unified CM サーバ(Unified CM Servers)] 領域で、Cisco Unified Communications Manager（Cisco UCM）の IP アドレスまたはホスト名を入力するか、省略記号をクリックしてダイアログを開き、IP アドレスまたはホスト名を参照します。

ステップ 4　[トランクセキュリティモード(Trunk Security Mode)] フィールドで、セキュリティ オプションをクリックします。Cisco UCM または Cisco UCM クラスタに [secure] を指定すると、Cisco UCM または Cisco UCM クラスタは TLS を開始します。

ステップ 5　[追加(Add)] をクリックして、Cisco Intercompany Media Engine プロキシの Cisco UCM を追加します。SIP トランクが有効な Cisco Intercompany Media Engine を使用するクラスタ内の各 Cisco UCM にエントリを含める必要があります。

ステップ 6　[チケットエポック(Ticket Epoch)] フィールドに、1 ～ 255 の整数を入力します。

エポックには、パスワードが変更されるたびに更新される整数が入ります。プロキシを初めて設定し、パスワードを初めて入力するときに、エポックの整数として 1 を入力します。パスワードを変更するたびに、新しいパスワードを示すためにエポックを増やします。ユーザはパスワードを変更するたびにエポックの値を増やす必要があります。

通常は、順番にエポックを増やしますが、適応型セキュリティ アプライアンスを使用すると、エポックを更新する際に任意の値を選択できます。

エポック値を変更する場合、現在のパスワードは無効となり、新規パスワードを入力する必要があります。

（注）　適応型セキュリティ アプライアンスのこのステップで設定するエポックおよびパスワードは、Cisco Intercompany Media Engine サーバで設定するエポックおよびパスワードと一致する必要があります。詳細については、Cisco Intercompany Media Engine サーバの関連資料を参照してください。

ステップ 7　[チケットパスワード(Ticket Password)] フィールドに、US-ASCII 文字セットから印刷可能な少なくとも 10 文字を入力します。使用可能な文字には、0x21 ～ 0x73 までが含まれ、スペース文字は除外されます。チケット パスワードには、最長 64 文字まで指定できます。入力したパスワードを確認します。同時に設定できるパスワードは 1 つだけです。

ステップ 8　[MTA を UC-IME Link プロキシに適用する (Apply MTA to UC-IME Link proxy)] チェックボックスをオンにし、メディア ターミネーション アドレスを Cisco Intercompany Media Engine プロキシと関連付けます。

（注）　このアドレスを Cisco Intercompany Media Engine プロキシと関連付ける前に、メディア ターミネーション インスタンスを作成する必要があります。必要に応じて、[MTA の構成 (Configure MTA)] ボタンをクリックして、メディア ターミネーション アドレス インスタンスを設定します。

ステップ 9　Cisco Intercompany Media Engine プロキシがオフパス配置の一部として設定されている場合、[オフパスアドレスマッピングサービスの有効化 (Enable off path address mapping service)] チェックボックスをオンにして、オフパス配置設定を行います。

a. [リスニングインターフェイス (Listening Interface)] フィールドから適応型セキュリティ アプライアンスのインターフェイスを選択します。これは、適応型セキュリティ アプライアンスがマッピング要求を受信するインターフェイスです。

b. [ポート (Port)] フィールドに、適応型セキュリティ アプライアンスがマッピング要求を受信する TCP ポートとして 1024 ～ 65535 までの間の数字を入力します。デバイス上のその他のサービス（Telnet または SSH など）との競合を避けるため、1024 以上のポート番号を指定する必要があります。デフォルトでは、ポート番号は TCP 8060 です。

c. [UC-IME インターフェイス (UC-IME Interface)] フィールドで、リストからインターフェイスを選択します。これは、適応型セキュリティ アプライアンスがリモート Cisco UCM と接続するために使用するインターフェイスです。

（注）　オフパス配置で環境に配置している既存の適応型セキュリティ アプライアンスは、Cisco Intercompany Media Engine トラフィックを送信できません。オフパス シグナリングでは、外部アドレスを（NAT を使用して）内部 IP アドレスに変換する必要があります。内部インターフェイス アドレスは、このマッピング サービス設定に使用されます。Cisco Intercompany Media Engine プロキシでは、適応型セキュリティ アプライアンスが外部アドレスの内部 IP アドレスへのダイナミック マッピングを作成します。

ステップ 10　[フォールバック (Fallback)] 領域で、以下の設定を指定して、Cisco Intercompany Media Engine のフォールバック タイマーを設定します。

a. [フォールバック重要度ファイル (Fallback Sensitivity File)] フィールドに、適応型セキュリティ アプライアンスが通話中 PSTN フォールバックに使用するフラッシュ メモリにあるファイルへのパスを入力します。入力するファイル名は .fbs ファイル拡張子を含むディスク上のファイルの名前である必要があります。または、[フラッシュの参照 (Browse Flash)] ボタンをクリックして、フラッシュ メモリからファイルを見つけて選択します。

b. [コール音声品質評価の間隔 (Call Quality Evaluation Interval)] フィールドに、10 ～ 600 の間の数字（ミリ秒単位）を入力します。この数字は、適応型セキュリティ アプライアンスがインターネットから受信する RTP パケットをサンプリングする頻度を制御します。適応型セキュリティ アプライアンスは、このデータ サンプルを使用して、コールに対して PSTN へのフォールバックが必要であるかを判別します。デフォルトでは、タイマーの間隔は 100 ミリ秒です。

c. [通知間隔 (Notification Interval)] フィールドに、10 ～ 360 の間の数字（秒単位）を入力します。この数字は、PSTN にフォールバックするかどうかを Cisco UCM に通知するまで、適応型セキュリティ アプライアンスが待機する時間を制御します。デフォルトでは、このタイマーの間隔は 20 秒です。

（注）　Cisco Intercompany Media Engine プロキシのフォールバック タイマーを変更すると、ASDM が自動で SIP インスペクションからプロキシを削除します。また、プロキシが再度有効化されるときに、SIP インスペクションが再適用されます。

ステップ 11　[適用(Apply)] をクリックして、Cisco Intercompany Media Engine プロキシの設定変更を保存します。

ユニファイド コミュニケーション ウィザードを使用した Cisco UC-IMC プロキシの設定

ASDM を使用して Cisco Intercompany Media Engine プロキシを設定するには、メニューから [ウィザード(Wizards)] > [ユニファイドコミュニケーションウィザード(Unified Communications Wizard)] を選択します。[ユニファイドコミュニケーションウィザード(Unified Communications Wizard)] が開きます。最初のページで、[企業間(Business-to-Business)] セクションの下の [Cisco Intercompany Media Engine プロキシ(Cisco Intercompany Media Engine Proxy)] オプションを選択します。

ウィザードにより必要な TLS プロキシが自動で作成されます。その後ウィザードに従って、Intercompany Media Engine プロキシを作成し、必要な証明書のインポートおよびインストールを行うと、Intercompany Media Engine トラフィックの SIP インスペクションが自動で有効になります。

ウィザードに従って以下のステップを実行し、Cisco Intercompany Media Engine プロキシを作成します。

ステップ 1　[Intercompany Media Engineプロキシ(Intercompany Media Engine Proxy)] オプションを選択します。

ステップ 2　Cisco Intercompany Media Engine プロキシのトポロジを選択します。つまり、適応型セキュリティ アプライアンスはエッジ ファイアウォールとなり、すべてのインターネット トラフィックを通過させるか、または適応型セキュリティ アプライアンスは主なインターネット トラフィックのオフパス（オフパス配置とも呼ばれます）となるかを選択します。

ステップ 3　Cisco UCM IP アドレスやチケット設定などプライベート ネットワーク設定を指定します。

ステップ 4　パブリック ネットワーク設定を指定します。

ステップ 5　Cisco UCM のメディア ターミネーション アドレスを指定します。

ステップ 6　ローカル側の証明書（つまり、ローカル Cisco Unified Communications Manager サーバと適応型セキュリティ アプライアンスとの間で交換される証明書）の管理を設定します。ウィザードがこのステップで生成する ID 証明書は、このプロキシを使用するクラスタ内の各 Cisco Unified Communications Manager（UCM）サーバにインストールする必要があります。また、Cisco UCM からの各 ID 証明書を適応型セキュリティ アプライアンスにインストールする必要があります。適応型セキュリティ アプライアンスおよび Cisco UCM は、TLS ハンドシェイク中にそれぞれが互いを認証するために、これらの証明書を使用します。ウィザードでは、このステップの自己署名証明書のみがサポートされています。

ステップ 7　リモート側の証明書（つまり、リモート サーバと適応型セキュリティ アプライアンスとの間で交換される証明書）の管理を設定します。このステップでは、ウィザードは Certificate Signing Request（CSR; 証明書署名要求）を生成します。プロキシの ID 証明書要求が正常に生成された後、ウィザードはファイルを保存するか確認するプロンプトを表示します。

CSR テキスト ファイルを Certificate Authority（CA; 認証局）に送信する（たとえば、テキスト ファイルを CA Web サイトの CSR 登録ページに貼り付ける）必要があります。CA から ID 証明書が送られてきたら、その証明書を適応型セキュリティ アプライアンスにインストールする必要があります。この証明書は、リモート サーバが適応型セキュリティ アプライアンスを信頼できるサーバとして認証できるように、リモート サーバに提示されます。

最後に、ウィザードのこのステップに従って、適応型セキュリティ アプライアンスが、信頼できるリモート サーバであると判別できるように、リモート サーバからの CA のルート証明書をインストールします。

ウィザードは、Cisco Intercompany Media Engine 用に作成された設定の概要を表示して完了します。詳細については、このマニュアルのユニファイド コミュニケーション ウィザードに関するセクションを参照してください。

CHAPTER 5

Cisco IME サーバのバックアップと復元

Cisco IME サーバの Command Line Interface（CLI; コマンド ライン インターフェイス）から起動できる ディザスタ リカバリ システム（DRS; ディザスタ リカバリ システム）には、Cisco IME サーバ用のフル データのバックアップ機能と復元機能が備わっています。ディザスタ リカバリ システム を使用すると、スケジュールされた定期的な自動データ バックアップおよびユーザが起動するデータ バックアップを実行できます。

DRS は、バックアップ / 復元プロセスの一部として、独自の設定（バックアップ デバイス設定およびスケジュール設定）を復元します。DRS は、drfDevice.xml ファイルおよび drfSchedule.xml ファイルをバックアップおよび復元します。これらのファイルを含めてサーバが復元されれば、DRS バックアップ デバイスとスケジュールを再設定する必要はありません。

バックアップ ファイルは、ローカル デバイスにもネットワーク デバイスにも保存できます。Cisco IME サーバへの SFTP アクセスがない場合は、ローカル デバイスを選択する必要があります。ローカル デバイスにバックアップ ファイルを保存する場合、DRS は、/common/adminsftp/backup ディレクトリにバックアップ ファイルを保存します。SFTP クライアントを開き、インストール時に設定した adminsftp ユーザと管理者パスワードを使用して Cisco IME サーバに接続することにより、Cisco IME サーバからローカル バックアップ ファイルを手動で移動する必要があります。

注意 Cisco IME を復元する前に、サーバにインストールされている Cisco IME のバージョンが、復元するバックアップ ファイルのバージョンと一致していることを確認してください。ディザスタ リカバリ システム による復元では、一致するバージョンの Cisco IME のみをサポートしています。たとえば、ディザスタ リカバリ システム バージョン 8.0.(**1**).1000-1 からバージョン 8.0(**2**).1000-1 への復元や、バージョン 8.0.(1).1000-**1** からバージョン 8.0(1).1000-**2** への復元は許可されません。

ディザスタ リカバリ システム には、次の機能があります。

- バックアップ タスクおよび復元タスクを実行するためのコマンド ライン インターフェイス。
- バックアップ機能および復元機能を実行するための分散システム アーキテクチャ。
- スケジュールされたバックアップ。
- ローカル ドライブまたはリモート SFTP サーバへのバックアップのアーカイブ。ディザスタ リカバリ システム では、Cisco IME サーバ上のバックアップおよび復元で、テープ ドライブをサポートしていません。

（注） 1 週間前よりも古いローカル バックアップ ファイルは自動的に削除されます。1 週間後にローカル バックアップ ファイルが削除されることになるバックアップを実行すると、警告メッセージが表示されます。

ディザスタ リカバリ システム には、Master Agent（MA; マスター エージェント）と Local Agent（LA; ローカル エージェント）という 2 つの主要機能があります。マスター エージェントは、バックアップおよび復元操作をローカル エージェントと調整します。

注意　コール処理の中断やサービスへの影響を避けるために、オフピーク時にバックアップするようスケジュールしてください。

バックアップ手順および復元手順のクイック リファレンス表

次の表は、バックアップ手順および復元手順のクイック リファレンスになっています。

（注）　DRS は、drfDevice.xml ファイルおよび drfSchedule.xml ファイルをバックアップおよび復元します。これらのバックアップ デバイス設定およびスケジュール設定は、バックアップ/復元プロセスの一部として復元されます。これらのファイルを含めてサーバが復元された後に DRS バックアップ デバイスとスケジュールを再設定する必要はありません。

バックアップのクイック リファレンス

表 1 は、ディザスタ リカバリ システム を使用してバックアップ手順を実行するために必要な主な高位ステップのクイック リファレンスを、時系列順に示しています。

表 1　バックアップ手順を実行する場合の主要ステップ

アクション	参照先
データのバックアップ先にするバックアップ デバイスを作成します。	「バックアップ デバイスの管理」（P.5-4）
スケジュールに従ってデータをバックアップするためのバックアップ スケジュールを作成します。	「バックアップ スケジュールの作成」（P.5-6）
データをバックアップするバックアップ スケジュールを使用可能または使用不可にします。	「スケジュールの使用可能化、使用不能化、および削除」（P.5-7）
オプションで、手動バックアップを実行します。	「手動バックアップの開始」（P.5-7）
バックアップのステータスの確認：バックアップの実行中に、現在のバックアップ ジョブのステータスを確認できます。	「バックアップ ステータスの確認」（P.5-8）

復元のクイック リファレンス

表 2 は、ディザスタ リカバリ システム を使用して復元手順を実行するために必要な主な高位ステップのクイック リファレンスを、時系列順に示しています。

表 2　復元手順を実行する場合の主要ステップ

アクション	参照先
ローカル ディレクトリまたはネットワーク ディレクトリからバックアップ ファイルを復元します。	「サーバの復元」（P.5-9）
復元のステータスの確認：復元プロセスの実行中に、現在の復元ジョブのステータスを確認できます。	「復元ステータスの表示」（P.5-10）

システム要件

ネットワーク上のリモート デバイスにデータをバックアップするか、ローカル バックアップを別の場所に移動する場合は、設定済みの SFTP サーバが必要です。どのような SFTP サーバ製品でも使用できますが、Cisco では Cisco Technology Developer Partner（CTDP）プログラムで Cisco が認定した SFTP 製品を推奨します。GlobalSCAPE などの CTDP パートナーは、自社製品での特定のバージョンの Cisco Unified Communications Manager の使用を保証しています。ご使用のバージョンの Cisco Unified Communications Manager の自社製品での動作を保証しているベンダーについては、次の URL を参照してください。

http://www.cisco.com/pcgi-bin/ctdp/Search.pl

サポートされている Cisco Unified Communications バージョンの GlobalSCAPE での使用については、次の URL を参照してください。

http://www.globalscape.com/gsftps/cisco.aspx

シスコでは、次のサーバを内部テストに使用しています。これらのサーバのいずれかを使用できますが、サポートについてはベンダーにお問い合わせください。

- Open SSH（http://sshwindows.sourceforge.net/ を参照）
- Cygwin（http://www.cygwin.com/ を参照）
- Titan（http://www.titanftp.com/ を参照）

（注）　注：CTDP プロセスによって認定されていないサードパーティ製品に関連する問題については、サードパーティのベンダーにサポートを依頼してください。

（注）　バックアップまたは復元の実行中は、ディザスタ リカバリ システム がプラットフォーム API をロックしてすべての OS 管理要求をブロックするため、いずれの OS 管理タスクも実行できません。ただし、プラットフォーム API ロック パッケージを使用するのは、CLI ベースのアップグレード コマンドのみであるため、大部分の CLI コマンドはブロックされません。

ヒント　バックアップは、ネットワーク トラフィックが少ないと思われる期間にスケジュールしてください。

ディザスタ リカバリ システム へのアクセス方法

ディザスタ リカバリ システム にアクセスするには、インストール時に作成したものと同じ管理者ユーザ名とパスワードを使用して、Cisco IME CLI にリモートまたはローカルでログインします。

- SSH を使用すると、クライアント ワークステーションから CLI に安全に接続できます。
- インストール時に使用したモニタとキーボードを使用して Cisco IME CLI に直接アクセスすることも、シリアル ポートに接続されているターミナル サーバを使用することもできます。IP アドレスに関する問題がある場合は、この方法を使用してください。

（注） 管理者ユーザ名とパスワードは、Cisco IME のインストール時に設定するもので、CLI を使用して管理者パスワードを変更したり、新規管理者アカウントを設定したりできます。『*Cisco Intercompany Media Engine Command Line Interface Reference Guide*』を参照してください。

マスター エージェントの役割およびアクティブ化

サーバ上の Master Agent（MA; マスター エージェント）は自動的にアクティブ化されます。Master Agent（MA; マスター エージェント）は、次の機能を実行します。

- システム全体のコンポーネント登録情報を保存します。
- スケジュールされたタスクの完全なセットを単一の XML ファイルに保持します。スケジュールの更新をユーザ インターフェイスから受け取ったときに、このファイルを更新します。スケジュールに従って、実行可能なタスクを該当するローカル エージェントに送信します（ローカル エージェントは、遅延なしで即時にバックアップ タスクを実行します）。
- ディザスタ リカバリ システム ユーザ インターフェイスから MA にアクセスして、バックアップ デバイスの設定、新規バックアップ スケジュールの追加によるバックアップのスケジューリング、既存スケジュールの表示または更新、実行されたスケジュールのステータスの表示、システム復旧の実行などの操作を実行します。
- ローカル ディレクトリまたはリモート ネットワーク ロケーションにバックアップ データを保存します。

ローカル エージェント

サーバは、バックアップ機能および復元機能を実行するためにローカル エージェントを持ちます。ローカル エージェントは、サーバ上でバックアップ スクリプトおよび復元スクリプトを実行します。

バックアップ デバイスの管理

ディザスタ リカバリ システム を使用する前に、バックアップ ファイルを保存する場所を設定する必要があります。ローカル バックアップ デバイスまたはネットワーク バックアップ デバイスを作成できます。ローカル バックアップ デバイスを作成した場合、ディザスタ リカバリ システム は、Cisco IME サーバ上の設定済みのディレクトリにバックアップ ファイルを保存します。SFTP クライアントを開き、インストール時に設定した adminsftp ユーザと管理者パスワードを使用して Cisco IME サーバに接続することにより、Cisco IME サーバからローカル バックアップ ファイルを手動で移動する必要があります。

バックアップ デバイスは 10 個まで設定できます。バックアップ デバイスを設定する手順は、次のとおりです。

手順

ステップ 1　ディザスタ リカバリ システム にアクセスするには、Cisco IME CLI にログインします（「ディザスタ リカバリ システム へのアクセス方法」（P.5-4）を参照）。

CLI の管理プロンプトが表示されます。

ステップ 2　ローカル デバイスを作成するには、**utils disaster_recovery device local** *device_name number of backups* を入力します。

変数の意味は、次のとおりです。

device_name は、バックアップ デバイスの名前です。バックアップ デバイス名には、英数字、スペース（ ）、ダッシュ（-）、およびアンダースコア（_）だけを含めることができます。他の文字は使用しないでください。DRS は、デフォルトでは、ローカル デバイスの場合のバックアップ ファイルを /common/adminsftp/backup ディレクトリに保存します。

number of backups は、このデバイスで許可されるバックアップの数です。

ステップ 3　SFTP 接続を介してアクセスするネットワーク ドライブにバックアップ ファイルを保存できるようにネットワーク デバイスを作成するには、**utils disaster_recovery device network** *device_name path server_name* ***username number of backups*** を入力します。

変数の意味は、次のとおりです。

device_name は、バックアップ デバイスの名前です。バックアップ デバイス名には、英数字、スペース（ ）、ダッシュ（-）、およびアンダースコア（_）だけを含めることができます。他の文字は使用しないでください。

path は、バックアップ ファイルの保存先にするディレクトリのパス名です。

server_name は、ネットワーク サーバの名前または IP アドレスです。

username は、リモート システム上のアカウントの有効なユーザ名です。

number of backups は、このデバイスで許可されるバックアップの数です。

（注）　ネットワーク ストレージ ロケーションを設定するには、SFTP サーバにアクセスできる必要があります。SFTP パスは、バックアップの前に存在している必要があります。SFTP サーバへのアクセスに使用するアカウントは、選択したパスへの書き込み権限を持つ必要があります。

（注）　DRS マスター エージェントは、選択されたバックアップ デバイスを検証します。ユーザ名、パスワード、サーバ名、またはディレクトリ パスが無効な場合、コマンドは失敗します。

ステップ 4　バックアップ デバイスのリストを表示するには、**utils disaster_recovery *device list*** を入力します。

デバイス名、デバイス タイプ、および各バックアップ デバイスのデバイス パスが表示されます。

ステップ 5　バックアップ デバイスを削除するには、**utils disaster_recovery device delete** *device_name* を入力します。ここで、*device_name* は、削除するデバイスの名前です。

（注）　バックアップ スケジュールでバックアップ デバイスとして設定されているバックアップ デバイスは削除できません。まず、このデバイス名を使用しているスケジュールを削除してから、このデバイスを削除する必要があります。

バックアップ スケジュールの作成

バックアップ スケジュールは 10 個まで作成できます。各バックアップ スケジュールは、自動バックアップのスケジュール、バックアップする一連の機能、ストレージ ロケーションなどの一連の独自のプロパティを持ちます。

注意　コール処理の中断やサービスへの影響を避けるために、オフピーク時にバックアップするようスケジュールしてください。

バックアップ スケジュールを作成する手順は、次のとおりです。

手順

ステップ 1　ディザスタ リカバリ システム にアクセスするには、Cisco IME CLI にログインします（「ディザスタ リカバリ システム へのアクセス方法」（P.5-4）を参照）。

CLI の管理プロンプトが表示されます。

ステップ 2　**utils disaster_recovery schedule add** *schedulename devicename featurelist datetime frequency* を入力します。

変数の意味は、次のとおりです。

schedulename は、スケジュールの名前です。

devicename は、ディザスタ リカバリ システム でバックアップ ファイルを保存する場所です。

featurelist は IME です。

datetime は、ディザスタ リカバリ システム でバックアップを実行する日時を指定します。フォーマットは、*yyyy/mm/dd-hh:mm* です。24 時間制の時間を入力してください。

frequency は、ディザスタ リカバリ システム でバックアップを実行する頻度です。オプションは、[一度 (once)]、[毎日 (daily)]、[毎週 (weekly)]、および [毎月 (monthly)] です。

ステップ 3　スケジュールを使用可能にするには、**utils disaster_recovery schedule enable *schedulename*** を入力します。

次回のバックアップは、設定した時間に実行されます。

（注）　スケジュールを使用不可にしたり削除したりする場合は、「スケジュールの使用可能化、使用不能化、および削除」（P.5-7）を参照してください。

スケジュールの使用可能化、使用不能化、および削除

バックアップ スケジュールを使用可能化、使用不能化、または削除するには、次の手順に従います。

手順

ステップ 1　ディザスタ リカバリ システム にアクセスするには、Cisco IME CLI にログインします（「ディザスタ リカバリ システム へのアクセス方法」（P.5-4）を参照）。

CLI の管理プロンプトが表示されます。

ステップ 2　バックアップ スケジュールのリストを表示するには、**utils disaster_recovery schedule list** を入力します。

各スケジュールのデバイス名およびステータスが CLI に表示されます。デバイス名は、ディザスタ リカバリ システム で、バックアップ ファイルを保存する場所を指定します。

ステップ 3　次の作業のいずれかを実行します。

- スケジュールを使用可能にするには、**utils disaster_recovery schedule enable *schedulename*** を入力します。
- スケジュールを使用不可にするには、**utils disaster_recovery schedule disable *schedulename*** を入力します。
- スケジュールを削除するには、**utils disaster_recovery schedule delete *schedulename*** を入力します。

スケジュールは、1 度に 1 つだけ、使用可能化、使用不能化、または削除できます。

手動バックアップの開始

手動バックアップを開始するには、次の手順に従います。

手順

ステップ 1　ディザスタ リカバリ システム にアクセスするには、Cisco IME CLI にログインします（「ディザスタ リカバリ システム へのアクセス方法」（P.5-4）を参照）。

CLI の管理プロンプトが表示されます。

ステップ 2　**utils disaster_recovery backup *type featurelist device_name*** を入力します。

変数の意味は、次のとおりです。

type は、バックアップの場所で、local または network のいずれかです。

featurelist は IME です。

device_name は、バックアップ デバイスの名前です。

ステップ 3　現在のバックアップのステータスを表示するには、**utils disaster_recovery status backup** を入力します。

ステップ 4　現在のバックアップをキャンセルするには、**utils disaster_recovery cancel_backup yes** を入力します。

バックアップ ステータスの確認

現在のバックアップ ジョブのステータスの確認と現在のバックアップ ジョブのキャンセルを行うことができます。バックアップ ファイルのリストを表示するには、「復元ステータスの表示」（P.5-10）を参照してください。

注意　リモート サーバへのバックアップが 20 時間以内に完了しない場合、バックアップ セッションは時間切れになります。この場合は、新規バックアップを開始する必要があります。

現在のバックアップ ジョブのステータスを確認する手順は、次のとおりです。

手順

ステップ 1　ディザスタ リカバリ システム にアクセスするには、Cisco IME CLI にログインします（「ディザスタ リカバリ システム へのアクセス方法」（P.5-4）を参照）。

CLI の管理プロンプトが表示されます。

ステップ 2　現在のバックアップのステータスを表示するには、**utils disaster_recovery status backup** を入力します。

ステップ 3　現在のバックアップをキャンセルするには、**utils disaster_recovery cancel_backup yes** を入力します。

（注）　バックアップは、現在のコンポーネントがバックアップ操作を完了してからキャンセルされます。

バックアップ ファイルの表示

次の手順を使用すると、ローカル ドライブまたはネットワーク ドライブに保存されているバックアップ ファイルのリストを参照できます。

手順

ステップ 1　ディザスタ リカバリ システム にアクセスするには、Cisco IME CLI にログインします（「ディザスタ リカバリ システム へのアクセス方法」（P.5-4）を参照）。

CLI の管理プロンプトが表示されます。

ステップ 2　バックアップ ファイルを表示するには、次のいずれかを行います。

- ローカル ディレクトリ（/common/adminsftp/backup）にあるバックアップ ファイルのリストを表示するには、**utils disaster_recovery show_backupfiles local backup** を入力します。
- ローカル復元ディレクトリ（/common/adminsftp/restore）にあるバックアップ ファイルのリストを表示するには、**utils disaster_recovery show_backupfiles local restore** を入力します。
- ネットワーク ドライブ上のバックアップ ファイルのリストを表示するには、**utils disaster_recovery show_backupfiles network** *path servername userid* を入力します。

変数の意味は、次のとおりです。

path は、バックアップ ファイルが保存されているディレクトリのパス名です。

servername は、ネットワーク サーバの名前または IP アドレスです。

userid は、リモート システム上のアカウントの有効なユーザ ID です。

サーバの復元

ネットワーク ディレクトリまたはローカル ディレクトリにあるバックアップ ファイルから Cisco IME サーバを復元できます。Cisco IME サーバを復元するには、次のいずれかの手順を実行します。

注意　Cisco IME を復元する前に、サーバにインストールされている Cisco IME のバージョンが、復元するバックアップ ファイルのバージョンと一致していることを確認してください。ディザスタ リカバリ システム による復元では、一致するバージョンの Cisco IME のみをサポートしています。たとえば、ディザスタ リカバリ システム バージョン 8.0.(**1**).1000-1 からバージョン 8.0.(**2**).1000-1 への復元や、バージョン 8.0.(1).1000-**1** からバージョン 8.0.(1).1000-**2** への復元は許可されません。基本的には、ディザスタ リカバリ システム で Cisco IME の復元を正常に実行するには、製品バージョンが完全に一致している必要があります。ディザスタ リカバリ システム は、厳密なバージョン検査に準拠しており、一致するバージョンの Cisco IME 間の復元のみを許可します。

注意　データの復元先のサーバを選択すると、このサーバにある既存のデータは、すべて上書きされます。

手順 1：ローカル ディレクトリからの復元

ステップ 1　SFTP クライアントを開き、インストール時に設定した adminsftp ユーザと管理者パスワードを使用して Cisco IME サーバに接続することにより、Cisco IME サーバにバックアップ ファイルをコピーします。これを行うには、**cd backup** を入力してバックアップ ディレクトリに移動し、/common/adminsftp/restore ディレクトリにバックアップ ファイルをコピーします。

ステップ 2　Cisco IME CLI にログインして ディザスタ リカバリ システム にアクセスします（「ディザスタ リカバリ システム へのアクセス方法」（P.5-4）を参照）。

CLI の管理プロンプトが表示されます。

ステップ 3　**utils disaster_recovery restore local *restore_server tarfilename device_name*** を入力します。

変数の意味は、次のとおりです。

restore_server は、復元するサーバのホスト名です。

tarfilename は復元するバックアップ ファイルの名前（拡張子を除く）で、たとえば、2008-01-21-18-25-03 です。

device_name は、バックアップ デバイスの名前です。

ステップ 4　データは、選択したサーバ上に復元されます。現在の復元のステータスを表示するには、**utils disaster_recovery status restore** を入力します。

ステップ 5　サーバを再起動します。

手順 2：ネットワーク ディレクトリからの復元

ステップ 1　ディザスタ リカバリ システム にアクセスするには、Cisco IME CLI にログインします（「ディザスタ リカバリ システム へのアクセス方法」（P.5-4）を参照）。

CLI の管理プロンプトが表示されます。

ステップ 2　**utils disaster_recovery restore network** ***restore_server tarfilename device_name*** を入力します。

変数の意味は、次のとおりです。

restore_server は、復元するサーバのホスト名です。

tarfilename は、復元するファイルの名前（拡張子を除く）で、たとえば、2008-01-21-18-25-03 です。

device_name は、バックアップ デバイスの名前です。

注意　データの復元先のサーバを選択すると、このサーバにある既存のデータは、すべて上書きされます。

ステップ 3　データは、選択したサーバ上に復元されます。現在の復元のステータスを表示するには、**utils disaster_recovery status restore** を入力します。

ステップ 4　サーバを再起動します。

復元ステータスの表示

現在の復元ジョブのステータスを確認する手順は、次のとおりです。

手順

ステップ 1　ディザスタ リカバリ システム にアクセスするには、Cisco IME CLI にログインします（「ディザスタ リカバリ システム へのアクセス方法」（P.5-4）を参照）。

CLI の管理プロンプトが表示されます。

ステップ 2　現在の復元ジョブのステータスを表示するには、**utils disaster_recovery status restore** を入力します。ステータスには、復元の割合、ログ ファイルの場所、タイムスタンプ、機能名、サーバ名、コンポーネント名、およびコンポーネントのステータスが表示されます。

トレース ファイル

ViPR の場合は、次のトレース ファイルがあります。

このリリースの ディザスタ リカバリ システム では、マスター エージェント、GUI、および各ローカル エージェントのトレース ファイルが次の場所に書き込まれます。

- マスター エージェントの場合は、*platform/drf/trace/drfMA0** にあるトレース ファイルを検索してください。
- 各ローカル エージェントの場合は、*platform/drf/trace/drfLA0** にあるトレース ファイルを検索してください。

エラー メッセージ

ディザスタ リカバリ システム（DRS; ディザスタ リカバリ システム）は、バックアップ手順または復元手順の際に発生することがあるさまざまなエラーのアラームを出します。表 3 に、Cisco DRS アラームのリストを示します。

表 3　ディザスタ リカバリ システム アラーム

アラーム名	説明	意味
DRFBackupDeviceError	DRF バックアップ プロセスで、デバイスへのアクセスに問題があります。	DRS バックアップ プロセスでデバイスにアクセスしているときにエラーが発生しました。
DRFBackupFailure	Cisco DRF バックアップ プロセスが失敗しました。	DRS バックアップ プロセスでエラーが発生しました。
DRFBackupInProgress	別のバックアップがまだ実行されているときは、新規バックアップを開始できません。	別のバックアップがまだ実行されている場合、DRS は、新規バックアップを開始できません。
DRFInternalProcessFailure	DRF の内部プロセスでエラーが発生しました。	DRS の内部プロセスでエラーが発生しました。
DRFLA2MAFailure	DRF ローカル エージェントがマスター エージェントに接続できません。	DRS ローカル エージェントがマスター エージェントに接続できません。
DRFLocalAgentStartFailure	DRF ローカル エージェントが開始されません。	DRS ローカル エージェントが停止している可能性があります。
DRFLocalDeviceError	DRF で、ローカル デバイスへのアクセスに問題があります。	DRS でローカル デバイスにアクセスしているときにエラーが発生しました。
DRFMA2LAFailure	DRF マスター エージェントがローカル エージェントに接続しません。	DRS マスター エージェントがローカル エージェントに接続できません。
DRFMABackupComponent Failure	DRF で、バックアップできないコンポーネントが 1 つ以上あります。	DRS は、コンポーネントにコンポーネントのデータのバックアップを要求しましたが、バックアップ プロセスの実行中にエラーが発生し、コンポーネントはバックアップされませんでした。
DRFMABackupNodeDisconnect	バックアップ中のノードが、完全にバックアップされる前にマスター エージェントから接続されました。	DRS マスター エージェントが Cisco Unified Communications Manager ノードでバックアップ操作を実行していたときに、バックアップ操作が完了する前にノードが切断されました。
DRFMARestoreComponent Failure	DRF で復元できないコンポーネントが 1 つ以上あります。	DRS は、コンポーネントにコンポーネントのデータの復元を要求しましたが、復元プロセスの実行中にエラーが発生し、コンポーネントは復元されませんでした。
DRFMARestoreNodeDisconnect	復元中のノードが、完全に復元される前にマスター エージェントから接続されました。	DRS マスター エージェントが Cisco Unified Communications Manager ノードで復元操作を実行していたときに、復元操作が完了する前にノードが切断されました。

表 3　ディザスタ リカバリ システム アラーム （続き）

アラーム名	説明	意味
DRFMasterAgentStartFailure	DRF マスター エージェントが開始されませんでした。	DRS マスター エージェントが停止している可能性があります。
DRFNoRegisteredComponent	使用可能な登録済みのコンポーネントがないためバックアップは失敗しました。	使用可能な登録済みのコンポーネントがないため DRS バックアップは失敗しました。
DRFNoRegisteredFeature	バックアップ対象として選択された機能はありません。	バックアップ対象として選択された機能はありません。
DRFRestoreDeviceError	DRF 復元プロセスで、デバイスへのアクセスに問題があります。	DRS 復元プロセスで、デバイスから読み取ることができません。
DRFRestoreFailure	DRF 復元プロセスが失敗しました。	DRS 復元プロセスでエラーが発生しました。
DRFSftpFailure	DRF SFTP 操作にエラーがあります。	DRS SFTP 操作にエラーがあります。
DRFSecurityViolation	DRF システムは、セキュリティ違反になるおそれのある迷惑パターンを検出しました。	コード挿入やディレクトリ トラバーサルなど、セキュリティ違反になるおそれのある迷惑パターンが DRF ネットワーク メッセージに含まれています。DRF ネットワーク メッセージはブロックされました。
DRFTruststoreMissing	IPsec 信頼ストアがノード上にありません。	IPsec 信頼ストアがノード上にありません。DRF ローカル エージェントがマスター エージェントに接続できません。
DRFUnknownClient	pub 上の DRF マスター エージェントは、クラスタ外の不明なサーバからのクライアント接続要求を受信しました。要求は拒否されました。	パブリック上の DRF マスター エージェントは、クラスタ外の不明なサーバからのクライアント接続要求を受信しました。要求は拒否されました。

CHAPTER 6

Cisco Intercompany Media Engine サーバ上のサービスの管理

Cisco IME サーバには、システムが機能するために必要なネットワーク サービスおよびサーブレットが含まれます。これらのサービスは基本機能のために必須であるため、アクティブ化は必要ありません。ただし、トラブルシューティングの目的で、これらのサービスを停止し、開始する（再起動する）必要がある場合があります。

サービスまたはサーブレットに関して何か異常がある場合、RTMT で CriticalServiceDown アラートが発行されます。アラームは、実行時のステータスおよびシステムの状態に関する情報を提供するため、システムに関連する問題をトラブルシューティングできます。アラーム情報を確認した後、サービスのトレースを実行できます。トレース ファイルは、システムの問題を細かくトラブルシューティングする場合に役立ちます。

この項では、サービスについて説明し、またアラームおよびトレースを使用して問題をトラブルシューティングする方法について説明します。

サービス

Cisco IME アプリケーションのインストール後、サーバでネットワーク サービスが自動的に開始されます。ネットワーク サービスには、たとえば、データベース サービスやプラットフォーム サービスなど、システムが機能するために必要なサービスが含まれます。各サービスのサービス パラメータを設定することで、これらのサービスを設定できます。たとえば、トラブルシューティングなどの目的で、ネットワーク サービスを停止し、開始する（再起動する）必要がある場合があります。これらの作業は、Cisco IME サーバで Command Line Interface（CLI; コマンド ライン インターフェイス）を使用して実行できます。

この項では、サービスおよびサーブレットについて説明し、また、CLI からサービスを開始および停止する方法、およびサービス パラメータを設定する方法について説明します。

サービスの説明

この項では、Cisco IME サーバに存在し、次の機能領域に分類されるネットワーク サービスについて説明します。

- 「パフォーマンス サービスおよびモニタリング サービス」（P.6-2）
- 「バックアップ サービスおよび復元サービス」（P.6-3）
- 「システム サービス」（P.6-3）
- 「プラットフォーム サービス」（P.6-3）

サービスの操作の詳細については、「サービス設定チェックリスト」（P.6-5）を参照してください。

パフォーマンス サービスおよびモニタリング サービス

この項では、パフォーマンス サービスおよびモニタリング サービスについて説明します。

Cisco CallManager Serviceability RTMT

Cisco CallManager Serviceability RTMT サーブレットは Real-Time Monitoring Tool（RTMT）をサポートします。これを使用すると、トレースを収集および表示すること、パフォーマンス モニタリング オブジェクトを表示すること、アラートを操作すること、およびデバイスとシステムのパフォーマンスを監視することなどができます。

Cisco Log Partition Monitoring Tool

Cisco Log Partition Monitoring Tool サービスは Log Partition Monitoring 機能をサポートします。この機能は、設定済みのしきい値およびポーリング間隔を使用して、サーバ上のログ パーティションのディスク使用状況を監視します。

Cisco RIS Data Collector

Real-time Information Server（RIS）は、デバイス登録ステータス、パフォーマンス カウンタ統計、生成される重要アラームなど、リアルタイム情報を保持します。Cisco RIS Data Collector サービスは、RIS サーバに保持されている情報を取得するために、Real-Time Monitoring Tool（RTMT）などのアプリケーションのインターフェイスを提供します。

Cisco AMC Service

Real-Time Monitoring Tool（RTMT）に対し使用されます。このサービス、Alert Manager、および Collector サービスにより、RTMT は、サーバに存在するリアルタイム情報を取得できます。

Cisco Audit Event Service

Cisco Audit Event Service は、ユーザによる Cisco IME システムの設定変更、またはユーザ操作の結果としてのこれらの設定変更を監視し、ログに記録します。

バックアップ サービスおよび復元サービス

この項では、バックアップ サービスおよび復元サービスについて説明します。

Cisco DRF Master

CiscoDRF Master Agent サービスは DRF Master Agent をサポートします。これは、必要に応じてバックアップのスケジュール、復元の実行、依存関係の表示、ジョブのステータスの確認、およびジョブのキャンセルを実行するための ディザスタ リカバリ システム Command Line Interface（CLI; コマンド ライン インターフェイス）を処理します。Cisco DRF Master Agent は、バックアップおよび復元プロセス用のストレージ メディアも用意します。

Cisco DRF Local

Cisco DRF Local サービスは、DRF Master Agent のワークホースとして動作する Cisco DRF Local Agent をサポートします。コンポーネントは、ディザスタ リカバリ フレームワークを使用するために Cisco DRF Local Agent に登録します。Cisco DRF Local Agent は、Cisco DRF Master Agent から受信したコマンドを実行します。Cisco DRF Local Agent は Cisco DRF Master Agent に対してステータス、ログ、およびコマンドの結果を送信します。

システム サービス

この項では、システム サービスについて説明します。

Cisco CDP

Cisco CDP は、音声アプリケーションを他のネットワーク管理アプリケーションに通知します。これにより、ネットワーク管理アプリケーション（たとえば、SNMP や CiscoWorks Lan Management Solution）は、音声アプリケーションのネットワーク管理タスクを実行できます。

Cisco Trace Collection Servlet

Cisco Trace Collection Servlet は Cisco Trace Collection Service とともにトレース収集をサポートします。これにより、ユーザは RTMT を使用してトレースを表示できます。サーバでこのサービスを停止すると、そのサーバでトレースを収集することや確認することができなくなります。

SysLog Viewer および Trace & Log Central を RTMT で動作させるには、Cisco Trace Collection Servlet および Cisco Trace Collection Service がサーバで実行されている必要があります。

Cisco Trace Collection Service

Cisco Trace Collection Service は Cisco Trace Collection Servlet とともにトレース収集をサポートします。これにより、ユーザは RTMT クライアントを使用してトレースを確認できます。サーバでこのサービスを停止すると、そのサーバでトレースを収集することや確認することができなくなります。

SysLog Viewer および Trace & Log Central を RTMT で動作させるには、Cisco Trace Collection Servlet および Cisco Trace Collection Service がサーバで実行されている必要があります。

ヒント　初期化時間を削減するために、必要に応じて、Cisco Trace Collection Servlet を再起動する前に Cisco Trace Collection Service を再起動することをお勧めします。

プラットフォーム サービス

この項では、プラットフォーム サービスについて説明します。

Cisco Tomcat

Cisco Tomcat サービスは Web サーバをサポートします。

SNMP Master Agent

このサービスは、エージェント プロトコル エンジンとして動作し、SNMP 要求に関連する認証、許可、アクセス制御、およびプライバシー機能を提供します。

ヒント　CLI で SNMP 設定を完了した後、[Control Center - Network Features] ウィンドウで SNMP Master Agent サービスを再起動する必要があります。

MIB2 Agent

このサービスは、RFC 1213 で定義されている変数への SNMP アクセスを提供します。たとえば、システム、インターフェイス、IP などの変数を読み取ること、および書きこむことができます。

Host Resources Agent

このサービスは、ストレージ リソース、プロセス テーブル、インストール済みのソフトウェア ベースなど、ホスト情報への SNMP アクセスを提供します。このサービスは HOST-RESOURCES-MIB を実装しています。

Native Agent Adaptor

このサービスはベンダー MIB をサポートします。これを使用すると、システムで実行されている別の SNMP エージェントに SNMP 要求を転送できます。

System Application Agent

このサービスは、システムにインストールされ、実行されているアプリケーションへの SNMP アクセスを提供します。このサービスは SYSAPPL-MIB を実装しています。

Cisco CDP Agent

このサービスは、Cisco Discovery Protocol を使用して、Cisco IME サーバ上のネットワーク接続情報への SNMP アクセスを提供します。このサービスは CISCO-CDP-MIB を実装しています。

Cisco Syslog Agent

このサービスは、各種のコンポーネントが生成する syslog メッセージの収集をサポートします。このサービスは CISCO-SYSLOG-MIB を実装しています。

Cisco Certificate Expiry Monitor

このサービスは、システムが生成する証明書の有効期限ステータスを定期的にチェックし、証明書の期限切れ日に近くなった時点で通知を送信します。

Cisco IME サービス

このサービスは、IME サーバの主要機能を提供します。このサービスは、ピアツーピア ネットワークのデータ、ピアツーピア ネットワークでの他のノードとの通信、および Cisco Unified Communication Manager との通信を管理します。

Cisco IME Configuration Manager

このサービスは、他のサービスが使用する管理設定および構成設定を管理します。

サービス設定チェックリスト

表 6-1 に、サービスを設定する手順の概要を示します。

表 6-1　アラーム設定チェックリスト

設定手順		関連する手順と項目
ステップ 1	適切なサービス パラメータを設定します。	「サービスの操作」（P.6-5）
ステップ 2	CLI で、収集するアプリケーション（サービス）アラーム情報について、1 つ以上のサーバ、サービス、宛先、およびイベント レベルを設定します。 • すべてのサービスを SDI ログに送ることができます（ただし、これは **set alarm** CLI コマンドを使用して設定する必要があります）。 • すべてアラームを SysLog Viewer に送ることができます。 • Event Log アラーム監視が目的の重大度を使用して有効になっていることを確認します。このために **set alarm** CLI コマンドを使用します。 • リモート Syslog サーバに syslog メッセージを送信するには、リモート Syslog 宛先を有効にし、ホスト名を指定します。この設定のために **set alarm** CLI コマンドを使用します。リモート サーバ名を設定していない場合、システムは syslog メッセージをリモート Syslog サーバに送信しません。 **ヒント** Cisco Unified Communications Manager サーバはリモート Syslog サーバとして設定しないでください。	• 「アラーム」（P.6-6）
ステップ 3	アラーム宛先として SDI トレース ファイルを選択した場合、RTMT の Trace & Log Central オプションを使用してトレースを収集し、情報を表示します。	• 「トレース」（P.6-8） • 『*Cisco Unified Real Time Monitoring Tool Administration Guide*』
ステップ 4	アラーム宛先としてローカル syslog を選択した場合、RTMT の SysLog Viewer でアラーム情報を表示します。	• 「トレース」（P.6-8） • 『*Cisco Unified Real Time Monitoring Tool Administration Guide*』
ステップ 5	RTMT の SysLog Viewer で、対応するアラーム定義を参照し、説明および推奨処置を確認します。	• 『*Cisco Unified Real Time Monitoring Tool Administration Guide*』

サービスの操作

Cisco IME サーバ上のサービスを開始、停止、または再起動するには、あるいはこのサーバ上のサービスのサービス パラメータを設定するには、Command Line Interface（CLI; コマンド ライン インターフェイス）を使用する必要があります。一度に 1 つのサービスのみ開始、停止、またはリフレッシュできます。サービスが停止処理中の場合、そのサービスが完全に停止するまで、そのサービスを開始できませんので注意してください。同様に、サービスが開始処理中の場合、そのサービスが完全に開始するまで、そのサービスは停止できません。

注意　サービス パラメータに変更を加えると、システム障害が発生する場合があります。変更する機能を熟知している場合、または Cisco Technical Assistance Center（TAC）から特別の指示がある場合を除いて、サービス パラメータを変更しないことをお勧めします。

表 6-2 に、Cisco IME サーバ上のサービスを操作するために必要なコマンドを示します。

表 6-2　サービスの CLI コマンド

タスク	コマンド
サービスとサービスのステータスのリストを表示する。	utils service list
サービスを停止する。	utils service stop *servicename*
サービスを開始する。	utils service start *servicename*
サービスを再起動する。	utils service restart *servicename*
サービス パラメータを表示する。	show *servicename* serviceparam *serviceparametername* 変数の意味は、次のとおりです。 *servicename* には ime、amc、risdc、または enterprise を指定できます。 *serviceparametername* は、そのサービスに対し定義されているサービス パラメータのいずれかです。 サービスに対し定義されているサービス パラメータのリストを表示するには、次のコマンドを使用します。 show *servicename* serviceparam ?
サービス パラメータを設定する。	set *servicename* serviceparam *service parameter name* *servicename* は <ime | amc | risdc | enterprise> であり、*service parameter name* はそのサービスに対し定義されているサービス パラメータのいずれかです。

追加情報

「関連項目」（P.6-11）

アラーム

アラームは、システムの実行時ステータスおよび状態に関する情報を提供します。これにより、システムに関連する問題をトラブルシューティングできます。たとえば、ディザスタ リカバリ システム に関する問題を特定できます。アラーム情報には、説明および推奨処置が含まれ、またアプリケーション名、マシン名なども含まれるため、トラブルシューティングの実行に役立ちます。

複数のロケーションにアラーム情報を送信するには、アラーム インターフェイスを設定します。各ロケーションで、任意のアラーム イベント レベル（デバックから緊急まで）を設定できます。Syslog Viewer（ローカル syslog）、Syslog ファイル（リモート syslog）、SDI トレース ログ ファイル、またはすべての宛先にアラームを送信できます。

サービスがアラームを発行すると、アラーム インターフェイスはそのアラーム情報を、ユーザが設定し、かつアラーム定義のルーティング リストで指定されているロケーション（たとえば SDI トレース）に送信します。システムは、SNMP トラップと同様に、アラーム情報を転送することもできますし、またはその最終宛先（ログ ファイルなど）に書き込むこともできます。

SDI トレース ログ ファイルに送信されるアラームを収集するには、Real-Time Monitoring Tool（RTMT）の Trace & Log Central オプションを使用します。ローカル syslog に送信されるアラーム情報を表示するには、RTMT の SysLog Viewer を使用します。

CLI コマンドを入力すると、ただちにシステムは必要なパラメータを要求するプロンプトを表示します。出力を表示するには、値を入力します。

表 6-3 に、Cisco IME サーバでアラームを操作するために必要なコマンドを示します。

表 6-3　アラームの CLI コマンド

タスク	コマンド
特定のサービスまたは一連のすべてのサービスのアラーム設定を表示する。	show alarm 必須パラメータ： *servicename*：サービスの名前。複数の語を含めることができます。 例： すべてのサービスのアラーム設定を表示するには、servicename として *all* を入力します。 Cisco Tomcat サービスのアラーム設定を表示するには、servicename として *Cisco Tomcat* を入力します。
特定の宛先に対しアラームを有効または無効にする。	set alarm *status* 必須パラメータ： *status*：enable または disable。 *servicename*：サービスの名前。複数の語を含めることができます。 *monitorname*：SDI、SDL、Event_Log、または Sys_Log。
リモート Syslog サーバに対しアラームを有効にする。	set alarm remotesyslogserver 必須パラメータ： *servicename*：サービスの名前。複数の語を含めることができます。 *servername*：リモート syslog サーバの名前。

表 6-3　アラームの CLI コマンド （続き）

タスク	コマンド
アラームのイベント レベルを設定する。	set alarm *severity* 必須パラメータ： *servicename*：サービスの名前。複数の語を含めることができます。 *monitorname*：SDI、SDL、Event_Log、または Sys_Log。 *severity* は次のいずれかです。 – [緊急 (Emergency)]：このレベルは、システムが使用不可であることを示します。 – [アラート (Alert)]：このレベルは、ただちに処置が必要であることを示します。 – [重要 (Critical)]：システムが重要な状態を検出したことを示します。 – [エラー (Error)]：このレベルは、エラー状態が存在することを示します。 – [警告 (Warning)]：このレベルは、警告状態が検出されたことを示します。 – [通知 (Notice)]：このレベルは、正常であるけれども重要な状態であることを示します。 – [情報 (Informational)]：このレベルは、単なる情報メッセージであることを示します。 – [デバッグ (Debug)]：このレベルは、Cisco TAC エンジニアがデバッグのために使用する詳細なイベント情報であることを示します。
アラーム設定をデフォルト値に設定する。 **ヒント** このオプションは、名前が Cisco で始まるサービスに対してのみ使用できます。	set alarm default 必須パラメータ： *servicename*：サービスの名前。複数の語を含めることができます。

追加情報

「関連項目」（P.6-11）

トレース

トレースは、アプリケーションの問題をトラブルシューティングする場合に役立ちます。トレースする情報のレベルを指定するには、および各トレース ファイルに書き込む情報のタイプを指定するには、CLI を使用します。Cisco IME サーバ上のサービスに対しトレース パラメータを設定できます。

SDI トレース ログ ファイルなど、各種のロケーションにアラームを送信できます。これを行う場合、Real-Time Monitoring Tool（RTMT）でアラートのトレースを設定できます。

トレース ファイルに書き込む、各種サービスの情報を設定した後、Real-Time Monitoring Tool（RTMT）の Trace & Log Central オプションを使用してトレース ファイルを収集し、表示できます。これを行うには、**set alarm** CLI コマンドを使用してアラームを設定します。

トレースする情報のレベル（デバッグ レベル）、トレースする情報内容（トレース フィールド）、およびトレース ファイルに関する情報（サービスあたりのファイルの数、ファイルのサイズ、トレース ファイルにデータを保存する時間など）を設定できます。

トレース ファイルに書き込む、各種サービスの情報を設定した後、RTMT の Trace & Log Central オプションを使用してトレース ファイルを収集できます。トレース収集の詳細については、『*Cisco Unified Real Time Monitoring Tool Administration Guide*』を参照してください。

トレースの設定

Cisco IME サーバ上の特定サービスのトレースを有効または無効にするには、およびそれらのサービスのトレースの設定を行うには、Command Line Interface（CLI; コマンド ライン インターフェイス）を使用します。CLI コマンドを入力すると、ただちにシステムは必要なパラメータを要求するプロンプトを表示します。システムがトレース ファイルを生成した後、RTMT を使用してそれらのファイルを収集します。トレース収集の詳細については、「トレースの収集」（P.6-10）および『*Cisco Unified Real Time Monitoring Tool Administration Guide*』を参照してください。

表 6-4 に、Cisco IME サーバでトレースを操作するために必要なコマンドを示します。

表 6-4　トレースの CLI コマンド

タスク	コマンド
指定したサービスのトレース設定を表示する。	show trace 必須パラメータ： *servicename*：サービスの名前。複数の語を含めることができます。 例： すべてのサービスのトレース設定を表示するには、servicename として *all* を入力します。 Cisco AMC サービスのトレース設定を表示するには、servicename として *Cisco AMC Service* を入力します。
指定したサービスに対し使用できるトレース レベルを表示する。	show tracelevels 必須パラメータ： *servicename*：サービスの名前。複数の語を含めることができます。
指定したサービスのトレースを有効または無効にする。	set trace *status* 必須パラメータ： *status*：enable または disable。 *servicename*：サービスの名前。複数の語を含めることができます。

表 6-4　トレースの CLI コマンド （続き）

タスク	コマンド
指定したサービスのデバッグ トレース レベル設定を指定する。	set trace *tracelevel* 必須パラメータ： *tracelevel*：指定した servicename のトレース レベルを確認するには、show tracelevels CLI コマンドを使用します。 *servicename*：サービスの名前。複数の語を含めることができます。
特定サービスのトレース ファイルの最大サイズ（1 ～ 10 MB）を指定する。	set trace maxfilesize 必須パラメータ： *servicename*：サービスの名前。複数の語を含めることができます。 *size*：トレース ファイルの最大サイズ（1 ～ 10 MB）。
サービスあたりのトレース ファイルの最大数を指定する。 ファイルを識別できるように、システムにより、ファイル名にシーケンス番号が自動的に付加されます（たとえば、cus299.txt）。一連のファイルのうちの最後のファイルの容量がフルになった場合、最初のファイルに戻り、そのファイルからトレース データの書き込みが再開されます。	set trace maxnumfiles 必須パラメータ： *servicename*：サービスの名前。複数の語を含めることができます。 *filecount*：トレース ファイルの数（1 ～ 10000）。
指定したサービスについて、usercategories フラグを決められた値に設定する。 **ヒント** このオプションは、名前が Cisco で始まるサービスに対してのみ使用できます。	set trace usercategories 必須パラメータ： *flagnumber*：16 進数値（0 ～ 7FFF）。7FFF は、すべてのフラグを有効にすることを意味します。 *servicename*：サービスの名前。複数の語を含めることができます。
指定したサービスについて、トレース設定をデフォルト値に設定する。 **ヒント** このオプションは、名前が Cisco で始まるサービスに対してのみ使用できます。	set trace default 必須パラメータ： *servicename*：サービスの名前。複数の語を含めることができます。

追加情報

「関連項目」（P.6-11）

トレースの収集

Cisco Unified Real-Time Monitoring Tool（RTMT; リアルタイム監視ツール）の Trace & Log Central 機能を使用すると、特定の日付範囲または絶対時間におけるオンデマンド トレース収集を設定できます。指定した検索条件を含むトレース ファイルを収集し、そのトレース収集条件を後で使用するため

に保存できます。また、1 つのトレース収集を反復するようにスケジューリングすること、ネットワーク上の SFTP サーバまたは FTP サーバ、あるいはローカルホストにトレース ファイルをダウンロードすること、クラッシュ ダンプ ファイルを収集することができます。

ファイルを収集した後、リアルタイム監視ツール内の適切なビューアでそれらを表示できます。また、リモート ブラウズ機能を使用することで、トレース ファイルをダウンロードせずに、サーバ上でトレースを表示できます。RTMT に備わっている内部ビューアを選択することで、または外部ビューアとして適切なプログラムを選択することで、トレース ファイルを開くことができます。

（注）　RTMT から、指定したサーバでのトレースのトレース設定を編集することもできます。トレース設定を有効にするとシステムのパフォーマンスが低下するため、トレースはトラブルシューティングを行う場合に限り有効にしてください。

（注）　RTMT の Trace & Log Central 機能を使用するには、RTMT が、Network Address Translation（NAT; ネットワーク アドレス変換）なしでサーバに直接アクセスできる必要があります。デバイスにアクセスするために NAT を設定している場合、IP アドレスの代わりとなるホスト名をサーバに設定し、ホスト名とそれらのルーティング可能な IP アドレスを DNS サーバまたはホスト ファイルに追加する必要があります。

追加情報

「関連項目」（P.6-11）

関連項目

- 「サービス」（P.6-1）
- 「サービスの説明」（P.6-2）
- 「サービス設定チェックリスト」（P.6-5）
- 「サービスの操作」（P.6-5）
- 「アラーム」（P.6-6）
- 「トレース」（P.6-8）
- 「トレースの設定」（P.6-9）
- 「トレースの収集」（P.6-10）

関連項目

CHAPTER 7

Cisco Intercompany Media Engine での RTMT の使用

RTMT は、Cisco Intercompany Media Engine 製品の健康状態の監視を支援する、一連のデフォルト モニタリング オブジェクトを提供しています。Cisco IME サーバ上および Cisco Unified Communications Manager サーバ上の Cisco Intercompany Media Engine 製品を監視します。Cisco Unified Communications Manager 上のオブジェクトには、学習ルートおよびコール アクティビティに関する情報が格納されます。Cisco IME 上のオブジェクトには、ネットワークおよびサーバ アクティビティに関する情報が格納されます。

システムは、事前定義済みのカウンタのために、5 分おきにデータをログに記録します。

この章は、次の内容で構成されています。

RTMT のインストール

コンピュータにインストールされた RTMT の単一コピーを使用すると、一度に 1 つのサーバまたは 1 つのクラスタのみ監視できます。たとえば、次のエンティティのいずれかを監視できます。

- 1 つのサーバ上の Cisco Unified Communications Manager 製品
- クラスタ上のサーバ（クラスタの健康状態を監視するため）

Cisco IME サーバ上の Cisco Intercompany Media Engine 製品など、異なるサーバ上の製品を監視するには、最初にサーバからログオフする必要があります。ログオフ後、他のサーバにログインできます。

RTMT をインストールする前に、以下を考慮します。

- クライアント マシンには、Cisco Unified Communications Manager や Cisco Intercompany Media Engine など、1 つの製品タイプからダウンロードした RTMT クライアントのみインストールできます。異なる製品タイプの RTMT クライアントを同じクライアント マシンにインストールすることはサポートされていません。

- 現在の RTMT ダウンロードは、Cisco Unified Communications Manager の以前のリリースをサポートしていない場合があります。Cisco Unified Communications Manager の一部のリリースでは、場合により、RTMT の異なるバージョンをご使用のコンピュータにインストールする必要があります（Cisco Unified Communications Manager リリースごとに 1 つのバージョン）。インストールする RTMT バージョンが、監視する Cisco Unified Communications Manager に対応していることを確認してください。使用する RTMT バージョンが、監視するサーバに対応していない場合、対応するバージョンをダウンロードするよう要求するプロンプトがシステムにより表示されます。
- ご使用のコンピュータには、IP アドレス、RTMT フレーム サイズなど、最後に終了した RTMT クライアントのユーザ プリファレンスが保存されます。

Cisco IME サーバから RTMT をインストールするには、次の手順を実行します。

（注） Windows Vista プラットフォームに RTMT をインストールする場合、ユーザ アカウント制御に関するポップアップ メッセージ「認識できないプログラムがこのコンピュータへのアクセスを要求しています(An unidentified program wants to access your computer)」が表示されます。[許可(Allow)] をクリックして、RTMT の処理を続行します。

（注） RTMT を起動する場合、RTMT クライアント アプリケーションをダウンロードした元の製品タイプと同じ製品タイプにログインします。異なる製品タイプにログインした場合、RTMT は起動しないか、正常に動作しません。

手順

ステップ 1　任意のオペレーティング システム ブラウザを起動します。

（注） Microsoft Internet Explorer には既知のバグがあり、IME サーバから IME RTMT をダウンロードできません。FireFox、Safari など、その他のブラウザは使用できます。

ステップ 2　Web ブラウザのアドレスバーに次の URL を入力します。大文字と小文字は区別してください。

https://<Cisco IME-server-name>:{8443}/ast/rtmtinstaller.jsp

<Cisco IME-server-name> は、Cisco IME サーバの名前または IP アドレスです。

（注） ポート番号を指定することもできます。

ステップ 3　[セキュリティの警告(Security Alert)] ダイアログボックスが表示されます。適切なボタンをクリックします。

ステップ 4　インストール時に指定した管理者のユーザ名およびパスワードを入力します。

ステップ 5　次のいずれかを実行します。

- Microsoft Windows オペレーティング システムを実行しているコンピュータに RTMT ツールをインストールする場合、RTMT Windows インストーラ リンクをクリックします。
- Linux オペレーティング システムを実行しているコンピュータに RTMT ツールをインストールする場合、RTMT Linux インストーラ リンクをクリックします。

ステップ 6　実行可能ファイルをクライアント上の任意の場所にダウンロードします。

ステップ 7　Windows バージョンをインストールするには、デスクトップ上に表示される RTMT アイコンをダブルクリックするか、ファイルをダウンロードした先のディレクトリに移動し、RTMT インストール ファイルを実行します。

展開プロセスが開始されます。

ステップ 8　Linux バージョンをインストールするには、ファイルに実行特権を設定する必要があります。たとえば、次のコマンドを大文字と小文字を区別して入力します：**chmod +x CcmServRtmtPlugin.bin**

ステップ 9　RTMT の [ようこそ (welcome)] ウィンドウが表示された後、[次へ (Next)] をクリックします。

ステップ 10　ライセンス契約書を受諾するには、[ライセンス契約書の条項に同意する (I accept the terms of the License Agreement)] をクリックし、[次へ (Next)] をクリックします。

ステップ 11　RTMT をインストールする先の場所を選択します。デフォルトの場所を使用しない場合、[参照 (Browse)] をクリックし、別の場所を指定します。[次へ (Next)] をクリックします。

デフォルトのインストール パスでは、以下が指定されます。

- Windows：C:¥Program Files¥Cisco¥Unified-Communications-Manager Serviceability¥JRtmt
- Linux：/opt/Cisco/Unified-Communications-Manager_Serviceability/JRtmt

ステップ 12　インストールを開始するには、[次へ (Next)] をクリックします。

[キャンセル (Cancel)] はクリックしないでください。

ステップ 13　インストールを完了するには、[終了 (Finish)] をクリックします。

RTMT のアンインストール

ヒント　RTMT を使用すると、ローカル クライアント マシンにユーザ プリファレンスとモジュール jar ファイル（キャッシュ）が保存されます。RTMT をアンインストールする場合、このキャッシュを削除するか、または保存するか選択します。

Windows クライアントでは、[コントロールパネル (Control Panel)] の [プログラムの追加と削除 (Add/Remove Programs)] を使用して RTMT をアンインストールします （[スタート (Start)] > [設定 (Settings)] > [コントロールパネル (Control Panel)] > [プログラムの追加と削除 (Add Remove Programs)] の順に選択します）。

KDE クライアント、Gnome クライアント、またはその両方を備えた Hat Linux で RTMT をアンインストールするには、タスクバーから [スタート (Start)] > [アクセサリ (Accessories)] > [リアルタイム監視ツールのアンインストール (Uninstall Real-time Monitoring tool)] の順に選択します。

（注）　Windows Vista マシンで RTMT をアンインストールする場合、ユーザ アカウント制御に関するポップアップ メッセージ「認識できないプログラムがこのコンピュータへのアクセスを要求しています (An unidentified program wants to access your computer)」が表示されます。[許可 (Allow)] をクリックして、RTMT の処理を続行します。

RTMT の起動

（注）　Windows Vista マシンで RTMT を使用する場合、ユーザ アカウント制御に関するポップアップ メッセージ「認識できないプログラムがこのコンピュータへのアクセスを要求しています (An unidentified program wants to access your computer)」が表示されます。[許可 (Allow)] をクリックして、RTMT の処理を続行します。

手順

ステップ 1　プラグインをインストールした後、次のいずれかのタスクを実行します。

- Windows デスクトップで [リアルタイム監視ツール (Real-Time Monitoring Tool)] アイコンをダブルクリックします。
- [スタート (Start)] > [すべてのプログラム (Programs)] > [Cisco] > [Unified Serviceability] > [リアルタイム監視ツール (Real-Time Monitoring Tool)] > [リアルタイム監視ツール (Real-Time Monitoring Tool)] の順に選択します。

[リアルタイム監視ツールのログイン (Real-Time Monitoring Tool Login)] ウィンドウが表示されます。

ステップ 2　[ホストの IP アドレス (Host IP Address)] フィールドに、サーバまたはクラスタ内の第 1 サーバ（該当する場合）の IP アドレスまたはホスト名を入力します。

ステップ 3　[ユーザ名 (User Name)] フィールドに、アプリケーションの管理者のユーザ名を入力します。

ステップ 4　[パスワード (Password)] フィールドに、ユーザ名に対し設定した、管理者のユーザ パスワードを入力します。

（注）　認証が失敗した場合、またはサーバにアクセスできない場合、サーバおよび認証の詳細を再入力するよう要求するプロンプトがツールで表示されます。[キャンセル (Cancel)] ボタンをクリックしてアプリケーションを終了することもできます。認証が成功した後、RTMT により、ローカル キャッシュから、またはリモート サーバからモニタリング モジュールが起動されます。バックエンド バージョンに一致するモニタリング モジュールがローカル キャッシュに含まれていない場合、リモート サーバからモニタリング モジュールが起動されます。

ステップ 5　アプリケーションがサーバをリッスンするために使用するポートを入力します。デフォルト設定では 8443 が指定されています。

（注）　RTMT の Trace & Log Central ツールは、指定したポート番号を使用して、クラスタ内のすべてのノードと通信します。システムでポート マッピングを使用し、すべての Cisco Intercompany Media Engine ノードが同じポート番号にマップされていない場合、一部の RTMT ツールはそれらのノードに接続できません。接続できないツールは、Trace & Log Central、Job Status、SyslogViewer、Perfmon Log Viewer、FTP/SFTP Configuration などです。

ステップ 6　[セキュア接続 (Secure Connection)] チェックボックスをオンにします。

ステップ 7　[OK] をクリックします。

ステップ 8　プロンプトが表示されたら、[はい (Yes)] をクリックして証明書ストアを追加します。

Real-Time Monitoring Tool（RTMT; リアルタイム監視ツール）が起動します。

RTMT の操作

RTMT ウィンドウは、次のメイン コンポーネントで構成されます。

- メニュー バー：ご使用の設定に基づき、次のメニュー オプションの一部またはすべてが含まれます。
  - [ファイル (File)] : 既存の RTMT プロファイルを保存、復元、および削除すること、Java ヒープ メモリ使用量を監視すること、Cisco Unified サービスアビリティ の [サービスアビリティ レポートのアーカイブ (Serviceability Report Archive)] ウィンドウに移動すること、RTMT からログオフすること、および RTMT を終了することができます。

  （注）　RTMT メニュー オプションの [ファイル (File)] > [Cisco Unified Reporting] により RTMT から Cisco Unified Reporting にアクセスできます。インスペクションまたはトラブル シューティングのために、Cisco Unified Reporting アプリケーションを使用して Cisco Unified Communications Manager クラスタ データのスナップショットを作成できます。詳細については、『*Cisco Unified Reporting Administration Guide*』を参照してください。

  - [システム (System)] : システムの概要およびサーバ リソースを監視すること、パフォーマンス カウンタおよびアラートを操作すること、トレースを収集すること、および syslog メッセージを表示することができます。
  - [Communications Manager] : サーバ上の Cisco Unified Communications Manager の概要情報を表示すること、コール処理情報を監視すること、およびデバイス、モニタ サービス、および CTI を表示および検索することができます。
  - [Unity Connection] : ポート監視ツールを表示できます。
  - [IME サービス (IME Service)] : Cisco Intercompany Media Engine サーバのサーバ アクティビティおよびネットワーク アクティビティを監視できます。
  - [編集 (Edit)] :（テーブル形式のビューの）カテゴリを設定すること、デバイスのポーリング レートおよびパフォーマンス モニタリング カウンタを設定すること、クイック起動チャネルを非表示にすること、および RTMT のトレース設定を編集することができます。
  - [ウィンドウ (Window)] : 1 つの RTMT ウィンドウまたはすべての RTMT ウィンドウを閉じることができます。
  - [アプリケーション (Application)] : ご使用の設定に基づき、Cisco Unified Communications Manager の管理、Cisco Unified サービスアビリティ、Cisco Unity Connection の管理、および Cisco Unity Connection のサービスアビリティのアプリケーション Web ページをブラウズできます。
  - [ヘルプ (Help)] : RTMT のドキュメント オンライン ヘルプにアクセスすることや、RTMT のバージョンを表示することができます。
- [クイック起動チャネル (Quick Launch Channel)] : RTMT ウィンドウの左側にある、タブを備えたこのペインをクリックすると、サーバまたはアプリケーションに関する情報を表示できます。タブにはアイコンのグループが含まれており、それらのアイコンをクリックすると、各種オブジェクトを監視できます。
- [モニタ (Monitor)] ペイン：モニタリング結果が表示されるペイン。

RTMT の事前定義済み Cisco Intercompany Media Engine モニタリング オブジェクト

RTMT は、Cisco Intercompany Media Engine 機能の健康状態の監視を支援する、一連の事前定義済みモニタリング オブジェクトを提供しています。Cisco Unified Communications Manager サーバで、Cisco IME コールのコール処理アクティビティおよびルーティング アクティビティを監視できます。Cisco Intercompany Media Engine サーバで、インターネットの帯域幅、および IME 分散キャッシュのステータスに関連する各種統計を監視できます。Cisco Intercompany Media Engine 製品のパフォーマンスを監視するには、両方のサーバのオブジェクトが必要です。

この項の内容は次のとおりです。

Cisco Unified Communications Manager サーバの Intercompany Media Services 事前定義済みオブジェクトの監視

ヒント　準備済みの各モニタリング ウィンドウのポーリング レートは固定されており、デフォルト値として 30 秒が指定されています。Alert Manager and Collector（AMC）サービス パラメータの収集レートが変更されると、準備済みウィンドウのポーリング レートも更新されます。また、バックエンド サーバの時間ではなく、RTMT クライアント アプリケーションのローカル時間が、各グラフのタイム スタンプの基礎となります。

ヒント　事前定義済みオブジェクトのモニタにズームインするには、目的のグラフの領域の上で左マウス ボタンをクリックし、ドラッグします。領域を選択したら左マウス ボタンを離します。RTMT によりモニタ ビューが更新されます。ズームアウトして、モニタを初期デフォルト ビューにリセットするには、R キーを押します。

Intercompany Media Services モニタリング カテゴリでは、次の項目が監視されます。

- [ルーティング (Routing)] : Cisco Unified Communications Manager が保持する Cisco Intercompany Media Engine ルートの合計数が表示されます。この合計数には、次のルートが含まれます。
  - Cisco Intercompany Media Engine クライアントが学習し、Cisco Unified Communications Manager ルーティング テーブルに存在する電話番号を表す学習ルート
  - Cisco Intercompany Media Engine ルートが存在する対象のピア企業の固有ドメイン
  - すべての Cisco Intercompany Media Engine サービス間の IME 分散ハッシュ テーブルに正常に発行された Direct Inward Dialing（DID; ダイヤル イン）の番号を表す発行済みルート
  - 管理者がブロックしたために拒否される学習ルートの番号を表す拒否ルート

  これらのグラフは、Cisco IME Client パフォーマンス オブジェクトの次のパフォーマンス カウンタを表します : RoutesLearned、DomainsUnique、RoutesPublished、および RoutesRejected。

  ルーティングに関する情報を表示するには、[CallManager] > [Cisco IME クライアント (Cisco IME Client)] > [ルーティング (Routing)] の順に選択します。

- [コールアクティビティ (Call Activities)] : Cisco Intercompany Media Engine コールの合計数を監視できます。この合計数には、次のタイプのコールが含まれます。
  - 試行されたコール（受け入れられたコール、話し中のコール、応答のないコール、および失敗したコールが含まれます）
  - 受信されたコール
  - 確立されたコール（つまり、Cisco Unified Communications Manager が実行し、リモート パーティが受け入れたコール）
  - 受け入れられたコール（つまり、Cisco Unified Communications Manager が受信し、着信側として応答したコール）
  - PSTN へのフォールバックが完了したコール
  - PSTN に正常にフォールバックされなかったコール

  これらのグラフは、Cisco IME Client パフォーマンス オブジェクトの次のパフォーマンス カウンタを表します : CallsAttempted、CallAccepted、CallsReceived、CallsSetup、IMESetupsFailed、および FallbackCallsFailed。

  コール アクティビティに関する情報を表示するには、[CallManager] > [Cisco IME クライアント (Cisco IME Client)] > [コールアクティビティ (Call Activities)] の順に選択します。

使用できるオブジェクトおよびカウンタの詳細については、「Cisco Intercompany Media Engine のパフォーマンス オブジェクトおよびカウンタ」（P.11-1）を参照してください。

Cisco IME サーバのオブジェクトの監視

Cisco IME サーバには、次のオブジェクトがあります。

- 「IME サービスの監視」（P.7-7）
- 「IME システムのパフォーマンスの監視」（P.7-8）

IME サービスの監視

IME サービス カテゴリでは、次の項目が監視されます。

- [ネットワークアクティビティ (Network Activity)] : Cisco Intercompany Media Engine に関連する、Cisco Unified Communications Manager 上のアクティビティが表示されます。Network Activity オブジェクトにより、次のグラフが表示されます。
  - [IME 分散キャッシュの健康状態 (IME Distributed Cache Health)] : IME サーバ パフォーマンス オブジェクトの IMEDistributedCacheHealth カウンタに基づき、IME 分散キャッシュの正常性が表示されます。
  - [IME 分散ノードの数 (IME Distributed Node Count)] : IME サーバ パフォーマンス オブジェクトの IMEDistributedCacheNodeCount カウンタの値に基づき、IME 分散キャッシュ内のノードの概数が表示されます。各物理 Cisco Intercompany Media Engine サーバには複数のノードが含まれるため、グラフに表示される数は、IME 分散キャッシュに参加している物理 Cisco Intercompany Media Engine サーバの数を示しません。
  - [受信用インターネット BW(Internet BW Received)] : Cisco IME サービスが着信インターネット トラフィックのために使用する帯域幅量がキロビット / 秒単位で表示されます。IME サーバ パフォーマンス オブジェクトの InternetBandwidthRecv カウンタを表します。
  - [送信用インターネット BW(Internet BW Send)] : Cisco IME サービスが発信インターネット トラフィックのために使用する帯域幅量がキロビット / 秒単位で表示されます。IME サーバ パフォーマンス オブジェクトの InternetBandwidthSend カウンタを表します。

  - [IME 分散キャッシュに保存されたデータレコード (IME Distributed Cache Stored Data Records)]：Cisco Intercompany Media Engine サーバが保存した IME 分散キャッシュ レコードの数が表示されます。IME サーバ パフォーマンス オブジェクトの IMEDistributedCacheStoredData カウンタを表します。

  ネットワーク アクティビティに関する情報を表示するには、[Cisco IME サービス (Cisco IME Service)] > [ネットワークアクティビティ (Network Activity)] の順に選択します。

- [サーバアクティビティ (Server Activity)] : Cisco Intercompany Media Engine サーバ上のアクティビティを監視できます。Server Activity オブジェクトにより、次のグラフが表示されます。
  - [登録済みクライアントの数 (Number of Registered Clients)] : Cisco IME サービスに接続しているクライアントの現在の数が表示されます。IME サーバ パフォーマンス オブジェクトの ClientsRegistered カウンタの値を表します。
  - [IME 分散キャッシュクォータ (IME Distributed Cache Quota)] : この IME サーバに接続している Cisco Unified CM が IME 分散キャッシュに書き込むことのできる個々の DID の数を示します。この数は、IME 分散キャッシュのすべての設定、および IME サーバにインストールされている IME ライセンスにより決まります。
  - [IME 分散キャッシュクォータの使用 (IME Distributed Cache Quota Used)] : Intercompany Media Service の登録済みパターンを通じて発行される、この IME サーバに現在接続している Cisco Unified CM が設定した、固有 DID 番号の合計数を示します。
  - [受信 VCR(Terminating VCRs)] : コールの受信側のために Cisco IME サーバに保存されている IME 音声コール レコードの合計数を示します。これらのレコードは、学習ルートの検証のために使用できます。
  - [保留中の検証 (Validations Pending)] : Cisco IME サービスの保留中の検証の数および検証のしきい値が表示されます。このグラフは、Cisco IME サーバ パフォーマンス オブジェクトの ValidationsPending カウンタを表します。

  サーバ アクティビティに関する情報を表示するには、[Cisco IME サービス (Cisco IME Service)] > [サーバアクティビティ (Server Activity)] の順に選択します。

使用できるオブジェクトおよびカウンタの詳細については、「Cisco Intercompany Media Engine のパフォーマンス オブジェクトおよびカウンタ」（P.11-1）を参照してください。

IME システムのパフォーマンスの監視

IME システム パフォーマンス モニタリング カテゴリは SDL キュー オブジェクトを提供しています。このオブジェクトでは、SDL キュー内の信号の数、および特定の Signal Distribution Layer（SDL）キュー タイプとして処理された信号の数が監視されます。SDL キュー タイプには、高、通常、低、および最低キューがあります。特定のサーバまたはクラスタ全体（該当する場合）の SDL キューを監視できます。

SDL キューに関する情報を表示するには、[Cisco IME サービス (Cisco IME Service)] > [SDL キュー (SDL Queue)] の順に選択します。[SDL キュータイプ (SDL Queue Type)] ドロップダウン リスト ボックスからタイプを選択します。

使用できるオブジェクトおよびカウンタの詳細については、「Cisco Intercompany Media Engine のパフォーマンス オブジェクトおよびカウンタ」（P.11-1）を参照してください。

Trace & Log Central の操作

Cisco Unified Real-Time Monitoring Tool（RTMT）の Trace & Log Central 機能を使用すると、特定の日付範囲または絶対時間におけるオンデマンド トレース収集を設定できます。指定した検索条件を含むトレース ファイルを収集し、そのトレース収集条件を後で使用するために保存できます。また、1 つのトレース収集を反復するようにスケジューリングすること、ネットワーク上の FTP サーバまたは SFTP サーバ、あるいは Cisco IME 上のローカル（ローカルホスト）ファイルにトレース ファイルをダウンロードすること、クラッシュ ダンプ ファイルを収集することができます。

Cisco IME 上のローカルホスト ディレクトリにトレース ファイルをダウンロードする場合、SFTP クライアントを開くことでファイルにアクセスできます。インストール時に設定した adminsftp を使用することで Cisco IME サーバに接続します。

RTMT を使用したトレース収集の詳細については、『*Cisco Unified Real Time Monitoring Tool Administration Guide*』を参照してください。

関連項目

- 「RTMT のインストール」（P.7-1）
- 「RTMT のアンインストール」（P.7-3）
- 「RTMT の起動」（P.7-4）
- 「RTMT の操作」（P.7-5）
- 「RTMT の事前定義済み Cisco Intercompany Media Engine モニタリング オブジェクト」（P.7-6）
- 「Trace & Log Central の操作」（P.7-9）
- 「Cisco Unified Communications Manager の管理での Cisco IME の設定」（P.3-1）
- 「Cisco Intercompany Media Engine のパフォーマンス オブジェクトおよびカウンタ」（P.11-1）
- 「Cisco Intercompany Media Engine アラートの説明およびデフォルト設定」（P.12-1）
- 『*Cisco Unified Real Time Monitoring Tool Administration Guide*』

関連項目

CHAPTER 8

Cisco IME クライアント コール アクティビティ レポートの生成

Cisco Serviceability Reporter サービスは、Performance Protection Report など、Cisco Unified サービスアビリティ で日次レポートを生成します。各レポートは概要情報を提供し、その概要情報はその特定レポート用の統計を表示する各種グラフで構成されます。Reporter は、ログに記録された情報に基づき、1 日に 1 回レポートを生成します。Cisco Unified サービスアビリティ で [ツール(Tools)] メニューから、Reporter が生成するレポートにアクセスできます。各概要レポートは、その特定レポート用の統計を表示する各種グラフにより構成されます。サービスをアクティブ化した後、レポートが生成されるまで最大で 24 時間かかる場合があります。Cisco Unified Communications Manager クラスタ構成の場合、Reporter でクラスタ内の各サーバのデータが個別に表示されます。

Performance Protection Report は、最近 1 週間のデフォルト モニタリング オブジェクトの傾向分析情報を提供し、これにより、Cisco Intercompany Media Engine に関する情報を追跡できます。Performance Protection Report には、Cisco IME クライアントの合計コール数とフォールバック コール数の比率を示す Cisco IME Client Call Activity グラフが含まれます。このグラフは 2 つの線で構成され、一方の線が、試行された Cisco IME コールと最近 1 時間以内に完了した 1 時間あたりのコールの数を示し、もう一方の線が、現在の時間中および前の時間中に PSTN にフォールバックされた Cisco IME コールの比率を示します。データが存在しない場合、Reporter ではグラフの下部に水平な線が生成されます。

表 8-1 は、Cisco Unified Communications Manager サーバで Cisco Serviceability Reporter サービスを設定するための 設定チェックリストです。

（注） Cisco Serviceability Reporter の詳細については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。

表 8-1　サービスアビリティ レポートのアーカイブの設定チェックリスト

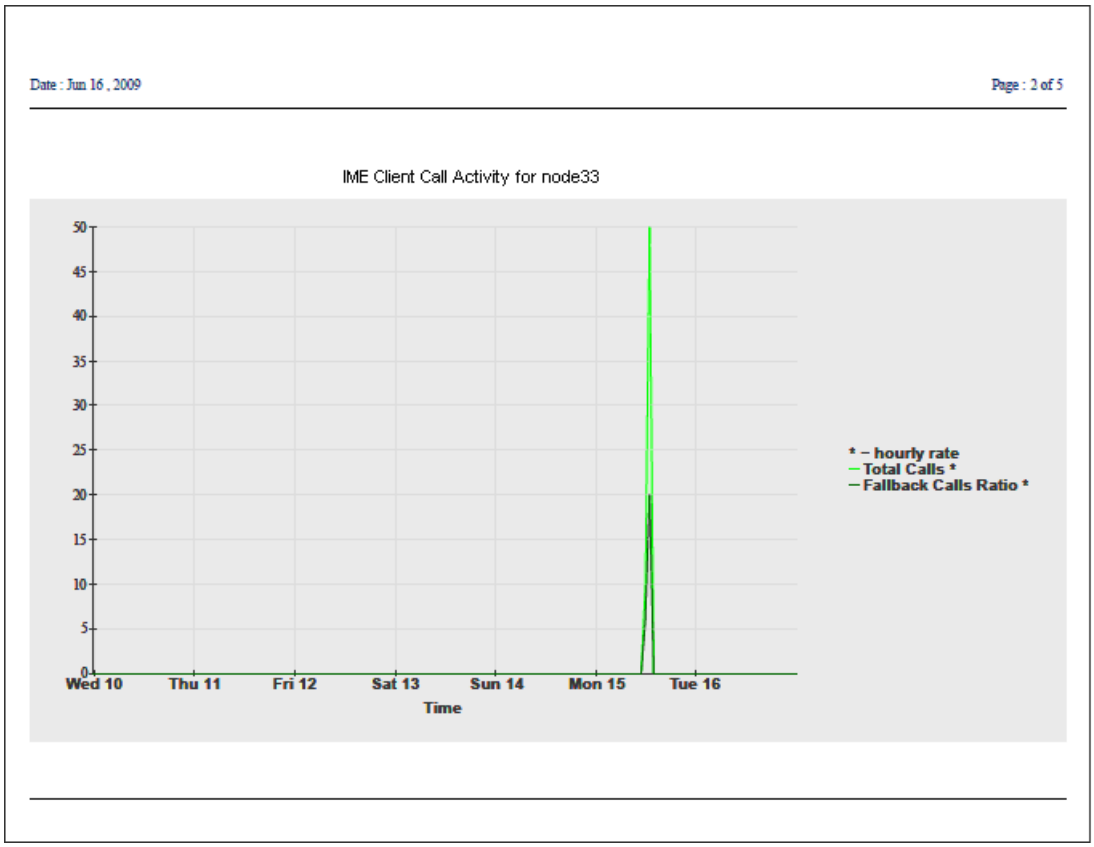
設定手順		関連する手順と項目
ステップ 1	Cisco Serviceability Reporter サービスをアクティブ化します。	1. [ツール(Tools)] > [サービスのアクティブ化(Service Activation)] の順に選択します。 [サービスのアクティブ化(Service Activation)] ウィンドウが表示されます。 2. [サーバ(Server)] ドロップダウン リスト ボックスから、サービスをアクティブ化する対象のサーバを選択し、[移動(Go)] をクリックします。Cisco Unified Communications Manager クラスタ構成の場合、1 番目のノードを選択します。 3. [Cisco Serviceability Reporter] チェックボックスをオンにし、[保存(Save)] をクリックします。
ステップ 2	Cisco Serviceability Reporter サービスのパラメータを設定します。	1. [システム(System)] > [サービスパラメータ(Service Parameters)] を選択します。 2. [サーバ(Server)] ドロップダウン リスト ボックスで、サーバを選択します。Cisco Unified Communications Manager クラスタ構成の場合、1 番目のノードを選択します。 3. [サービス(Service)] ドロップダウン リスト ボックスから、[Cisco Serviceability Reporter] サービスを選択します。 4. パラメータのリストと説明を表示するには、疑問符ボタンをクリックします。特定のパラメータをリストの上部に表示するには、[サービスパラメータ設定(Service Parameter Configuration)] ウィンドウでそのパラメータをクリックします。 5. 該当するパラメータ値を更新します。サービスのこのインスタンスのサービス パラメータをすべてデフォルト値に設定するには、[デフォルトに設定(Set to Default)] ボタンをクリックします。 6. [保存(Save)] をクリックします。

表 8-1　サービスアビリティ レポートのアーカイブの設定チェックリスト （続き）

設定手順		関連する手順と項目
ステップ 3	Cisco Serviceability Reporter サービスが生成したレポートを表示します。	1. [ツール (Tools)] > [サービスアビリティレポートのアーカイブ (Serviceability Reports Archive)] の順に選択します。 [サービスアビリティレポートのアーカイブ (Serviceability Reports Archive)] ウィンドウに、レポートを使用できる対象の月と年が表示されます。 2. [月 - 年 (Month-Year)] ペインで、レポートを表示する対象の月と年を選択します。 月に対応する日のリストが表示されます。 3. レポートを表示するには、レポートが生成された対象の日に対応するリンクをクリックします。 選択した日のレポート ファイルが表示されます。 4. 特定の PDF レポートを表示するには、表示するレポートのリンクをクリックします。 サーバ名を使用して Cisco Unified サービスアビリティを参照する場合、レポートを表示する前に、Cisco Unified サービスアビリティ にログインする必要があります。 ご使用のネットワークで Network Address Translation（NAT; ネットワーク アドレス変換）を使用していて、NAT 内のサービスアビリティ レポートにアクセスする場合、NAT に関連付けられているプライベート ネットワークの IP アドレスを、ブラウザの URL フィールドに入力します。NAT 外のレポートにアクセスする場合、パブリック IP アドレスを入力します。この場合、NAT により対応するプライベート IP アドレスに変換またはマップされます。 PDF レポートを表示するには、ご使用のマシンに Acrobat ® Reader をインストールする必要があります。Acrobat Reader をダウンロードするには、[サービスアビリティレポートのアーカイブ (Serviceability Reports Archive)] ウィンドウの下部にあるリンクをクリックします。ウィンドウが開き、選択したレポートの PDF ファイルが表示されます。

図 8-1 に、Cisco IME クライアント コール アクティビティ レポートの例を示します。

図 8-1　Cisco IME クライアント コール アクティビティ レポート



CHAPTER 9

Cisco IME での SNMP の設定

SNMP バージョン 3 には、認証（要求が本物の送信元から送られていることの確認）、プライバシー（データの暗号化）、許可（ユーザが要求した操作を許可されていることの確認）、アクセス制御（ユーザが要求したオブジェクトへのアクセス権を所持していることの確認）などのセキュリティ機能が備わっています。ネットワークで SNMP パケットが漏えいしないようにするために、SNMPv3 では暗号化を設定できます。

この章では、ネットワーク管理システムで Cisco IME を監視できるようにするために、SNMP v3 を設定する方法を説明します。この章は、次の内容で構成されています。

SNMP 設定チェックリスト

表 9-1 に、SNMP を設定するための手順の概要を示します。

表 9-1　SNMP 設定チェックリスト

設定手順		関連する手順と項目
ステップ 1	SNMP NMS をインストールおよび設定します。	NMS をサポートする SNMP 製品ドキュメント
ステップ 2	CLI で、次の SNMP サービスがシステムで開始されたことを確認します。 • SNMP Master Agent • Native Agent • System Application Agent • Cisco Syslog Agent • MIB2 Agent • Host Resources Agent	Cisco IME コマンド ラインで、次のコマンドを入力します。 utils service list
ステップ 3	SNMP ユーザを設定します。	「SNMP ユーザ」（P.9-3）
ステップ 4	トラップまたはインフォームの通知先を設定します。	• 「SNMP トラップ通知の宛先」（P.9-4） • 「SNMP インフォーム通知の宛先」（P.9-5）

表 9-1　SNMP 設定チェックリスト （続き）

設定手順		関連する手順と項目
ステップ 5	システム接点および MIB2 システム グループのロケーションを設定します。	「MIB2 システム グループ」（P.9-7）
ステップ 6	CISCO-SYSLOG-MIB のトラップ設定を設定します。	次のガイドラインを使用して、システムで CISCO-SYSLOG-MIB トラップ設定を設定します。 • SNMP Set 操作を使用して clogsNotificationEnabled（1.3.6.1.4.1.9.9.41.1.1.2）を true に設定します。たとえば、linux コマンド ラインから net-snmp set ユーティリティを使用して、この OID を true に設定します。以下を使用します：snmpset -c <*community string*> -v2c <*transmitter ipaddress*> 1.3.6.1.4.1.9.9.41.1.1.2.0 i 1 SNMP Set 操作に対し、その他の SNMP 管理アプリケーションも使用できます。 • SNMP Set 操作を使用して clogMaxSeverity（1.3.6.1.4.1.9.9.41.1.1.3）値を設定します。たとえば、linux コマンド ラインから net-snmp set ユーティリティを使用して、この OID 値を設定します。以下を使用します：snmpset -c public -v2c 1<*transmitter ipaddress*> 1.3.6.1.4.1.9.9.41.1.1.3.0 i <*value*> <value> 設定に対し重大度を示す数値を入力します。重大度値が大きいほど、重大度がより低いことを示します。値 1（緊急）は最も高い重大度を示し、値 8（デバッグ）は最も低い重大度を示します。Syslog Agent は、指定した重大度値よりも大きい重大度値のメッセージを無視します。たとえば、すべての syslog メッセージをトラップするには、値 8 を使用します。
ステップ 7	SNMP Master Agent サービスを再起動します （オプション）。 **ヒント** utils snmp config コマンドを実行した後、システムにより SNMP Master Agent エージェントが自動的に再起動されます。	Cisco IME コマンド ラインで、次のコマンドを入力します。 utils service start SNMP Master Agent
ステップ 8	NMS で、Cisco IME トラップ パラメータを設定します。	• 「SNMP Managed Information Base（MIB; 管理情報ベース）」（P.9-9） • NMS をサポートする SNMP 製品ドキュメント

追加情報

「関連項目」（P.9-12）を参照してください。

SNMP ユーザ

表 9-2 に、Cisco IME サーバで SNMP ユーザを操作するために必要なコマンドを示します。

表 9-2　トレースの CLI コマンド

タスク	コマンド
SNMP ユーザをリストする。	utils snmp config user 3 list
SNMP ユーザを追加する。	utils snmp config user 3 add システムにより、パラメータを要求するプロンプトが表示されます。パラメータの名前と説明については、表 9-3 を参照してください。
SNMP ユーザを更新する。	utils snmp config user 3 update システムにより、パラメータを要求するプロンプトが表示されます。パラメータの名前と説明については、表 9-3 を参照してください。
SNMP ユーザを削除する。	utils snmp config user 3 delete システムにより、パラメータを要求するプロンプトが表示されます。パラメータの名前と説明については、表 9-3 を参照してください。

SNMP ユーザの CLI パラメータ

表 9-3 で、V3 の SNMP ユーザ パラメータの設定について説明します。

表 9-3　V3 の SNMP ユーザ パラメータの設定

フィールド	説明
username	アクセス権を付与するユーザの名前。名前には、最大 32 の文字を指定でき、英数字、ハイフン（-）、およびアンダースコア（_）を任意に組み合わせて指定できます。 **ヒント** ネットワーク管理システム（NMS）に対して設定したユーザを入力します。
authprotocol	認証プロトコル。HMAC-SHA を指定するには、SHA と入力します。
authpassphrase	認証プロトコルのパスワードを指定します。パスワードは 8 文字以上指定する必要があります。
privprotocol	プライバシー プロトコル（AES128、AES192、または AES256）を指定します。
privpassphrase	プライバシー プロトコルのパスワードを指定します。パスワードは 8 文字以上指定する必要があります。

表 9-3　V3 の SNMP ユーザ パラメータの設定 （続き）

フィールド	説明
accessprivilege	アクセス レベルに関する次のオプションのいずれかを入力します。 • **ReadOnly**：ユーザは MIB オブジェクトの値を読み取ることのみできます。 • **ReadWrite**：ユーザは MIB オブジェクトの値を読み取ること、および書き込むことができます。 • **ReadWriteNotify**：ユーザは、MIB オブジェクトの値を読み取ること、および書き込むことができ、さらにトラップ メッセージおよびインフォーム メッセージに関する MIB オブジェクト値を送信できます。 • **NotifyOnly**：ユーザは、トラップ メッセージおよびインフォーム メッセージに関する MIB オブジェクト値を送信することのみできます。 • **ReadNotifyOnly**：ユーザは、MIB オブジェクトの値を読み取ることができ、さらにトラップ メッセージおよびインフォーム メッセージに関する値を送信できます。 • **None**：ユーザは、トラップ情報を読み取ること、書き込むこと、および送信することができません。 **ヒント** トラップ設定パラメータを変更するには、ユーザに NotifyOnly、ReadNotifyOnly、または ReadWriteNotify 特権を設定する必要があります。
ipaddress1	パケットを受け取る送信元の IP アドレスを指定します。デフォルトでは、すべてのホストからのパケットを受け取るように指定されます。
ipaddress2	パケットを受け取る送信元の IP アドレスを指定します。デフォルトでは、すべてのホストからのパケットを受け取るように指定されます。

追加情報

「関連項目」（P.9-12）を参照してください。

SNMP トラップ通知の宛先

SNMP エージェントは、重要なシステム イベントを示すために、トラップまたはインフォームの形式で NMS に通知を送信します。トラップでは宛先からの確認応答を受信しますが、インフォームでは確認応答は受信しません。

次の項は、SNMP V3 通知宛先設定に適用されます。

表 9-4 に、Cisco IME サーバで SNMP トラップ通知宛先を操作するために必要なコマンドを示します。

表 9-4　SNMP トラップ通知宛先の CLI コマンド

タスク	コマンド
トラップ通知の宛先をリストする。	utils snmp config trap 3 list
設定済みの v3 ユーザ名に関連する v3 トラップ通知宛先を追加する。	utils snmp config trap 3 add システムにより、パラメータを要求するプロンプトが表示されます。パラメータの名前と説明については、表 9-5 を参照してください。
トラップ通知宛先を更新する。	utils snmp config trap 3 update システムにより、パラメータを要求するプロンプトが表示されます。パラメータの名前と説明については、表 9-5 を参照してください。
トラップ通知宛先を削除する。	utils snmp config trap 3 delete システムにより、パラメータを要求するプロンプトが表示されます。パラメータの名前と説明については、表 9-5 を参照してください。

トラップ通知宛先のパラメータの設定

表 9-5 で、V3 のトラップ通知宛先パラメータの設定について説明します。

表 9-5　V3 のトラップ通知宛先パラメータの設定

フィールド	説明
ipaddress	通知宛先のホスト IP アドレス。
portno	宛先サーバの通知受信ポート番号。
oldportno	現在設定されている宛先サーバの通知受信ポート番号。
newportno	トラップ通知宛先の更新時に使用する宛先サーバの通知受信ポート番号。
username	通知宛先に関連する SNMP ユーザを指定します。

追加情報

「関連項目」（P.9-12）を参照してください。

SNMP インフォーム通知の宛先

SNMP エージェントは、重要なシステム イベントを示すために、トラップまたはインフォームの形式で NMS に通知を送信します。トラップでは宛先からの確認応答を受信しますが、インフォームでは確認応答は受信しません。

表 9-6 で、V3 のインフォーム通知宛先の設定について説明します。

表 9-6　SNMP インフォーム通知宛先の CLI コマンド

タスク	コマンド
インフォーム通知の宛先をリストする。	utils snmp config inform 3 list
v3 インフォーム通知の宛先を追加する。	utils snmp config inform 3 add システムにより、パラメータを要求するプロンプトが表示されます。パラメータの名前と説明については、表 9-7 を参照してください。
インフォーム通知の宛先を更新する。	utils snmp config inform 3 update システムにより、パラメータを要求するプロンプトが表示されます。パラメータの名前と説明については、表 9-7 を参照してください。
インフォーム通知の宛先を削除する。	utils snmp config inform 3 delete システムにより、パラメータを要求するプロンプトが表示されます。パラメータの名前と説明については、表 9-7 を参照してください。

インフォーム通知宛先のパラメータの設定

表 9-7　V3 のインフォーム通知宛先パラメータの設定

フィールド	説明
ipaddress	通知宛先のホスト IP アドレス。
portno	宛先サーバの通知受信ポート番号。
oldportno	現在設定されている宛先サーバの通知受信ポート番号。
newportno	インフォーム通知宛先の更新時に使用する宛先サーバの通知受信ポート番号。
username	通知宛先に関連する SNMP ユーザを指定します。
oldusername	インフォームに現在関連付けられている v3 ユーザ名を指定します。
newusername	インフォームに関連付ける v3 ユーザ名を指定します。
deleteuserconf	Y または N を使用して、古いユーザの削除を確定するかどうか指定します。
authprotocol	認証プロトコル。HMAC-SHA を指定するには、SHA と入力します。
authpassphrase	認証プロトコルのパスワードを指定します。パスワードは 8 文字以上指定する必要があります。
privprotocol	プライバシー プロトコル（AES128、AES192、または AES256）を指定します。
privpassphrase	プライバシー プロトコルのパスワードを指定します。パスワードは 8 文字以上指定する必要があります。

表 9-7　V3 のインフォーム通知宛先パラメータの設定 （続き）

フィールド	説明
accessprivilege	アクセス レベルに関する次のオプションのいずれかを入力します。 • **ReadWriteNotify**：ユーザは、MIB オブジェクトの値を読み取ること、および書き込むことができ、さらにトラップ メッセージおよびインフォーム メッセージに関する MIB オブジェクト値を送信できます。 • **NotifyOnly**：ユーザは、トラップ メッセージおよびインフォーム メッセージに関する MIB オブジェクト値を送信することのみできます。 • **ReadNotifyOnly**：ユーザは、MIB オブジェクトの値を読み取ることができ、さらにトラップ メッセージおよびインフォーム メッセージに関する値を送信できます。
engineId	インフォーム メッセージを送信する先のサーバのリモート エンジン ID を指定します。

追加情報

「関連項目」（P.9-12）を参照してください。

MIB2 システム グループ

CLI を使用して、MIB-II システム グループのシステム接点およびシステム ロケーション オブジェクトを設定できます。たとえば、システム接点として Administrator, 555-121-6633 と入力すること、およびシステム ロケーションとして San Jose, Bldg 23, 2nd floor と入力することができます。

表 9-8 に、Cisco IME サーバで MIB2 システム グループを操作するために必要なコマンドを示します。

表 9-8　MIB2 の CLI コマンド

タスク	コマンド
MIB2 システム グループ設定をリストする。	utils snmp config mib2 list
MIB2 システム グループを追加する。	utils snmp config mib2 add システムにより、パラメータを要求するプロンプトが表示されます。パラメータの名前と説明については、表 9-9 を参照してください。
MIB2 システム グループを更新する。	utils snmp config mib2 update システムにより、パラメータを要求するプロンプトが表示されます。パラメータの名前と説明については、表 9-9 を参照してください。
MIB2 システム グループを削除する。	utils snmp config mib2 delete システムにより、パラメータを要求するプロンプトが表示されます。パラメータの名前と説明については、表 9-9 を参照してください。

MIB2 システム グループの CLI パラメータ

表 9-9 で、MIB2 システム グループのパラメータの設定について説明します。

表 9-9　MIB2 システム グループのパラメータの設定

フィールド	説明
Server	接点を設定する対象のサーバ。
SysContact	問題発生時に通知するユーザを指定します。
SysLocation	システム接点として指定するユーザのロケーションを指定します。

追加情報

「関連項目」（P.9-12）を参照してください。

SNMP Managed Information Base（MIB; 管理情報ベース）

SNMP では、Managed Information Base（MIB; 管理情報ベース）にアクセスできます。MIB は、階層的に編成された情報の集合です。MIB は、オブジェクト ID で識別される管理対象オブジェクトにより構成されます。管理対象デバイスの特定の特性が格納される MIB オブジェクトは、1 つ以上のオブジェクト インスタンス（変数）で構成されます。

SNMP インターフェイスは、次の Cisco 標準 MIB を提供しています。

- CISCO-CDP-MIB
- CISCO-SYSLOG-MIB

Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）拡張エージェントは、サーバに常駐し、CISCO-CCM-MIB を公開します。CISCO-CCM-MIB は、サーバが認識しているデバイスに関する詳細情報を提供します。クラスタ構成の場合、SNMP 拡張エージェントはクラスタ内の各サーバに常駐します。CISCO-CCM-MIB は、サーバのデバイス登録ステータス、IP アドレス、説明、モデル タイプなど、デバイス情報を提供します（クラスタをサポートする構成でも、クラスタではなくサーバの情報が提供されます）。

SNMP インターフェイスは、次の業界標準 MIB も提供しています。

- SYSAPPL-MIB
- MIB-II (RFC 1213)
- HOST-RESOURCES-MIB

ベンダーが固有にサポートしているハードウェア MIB については、「ベンダー固有の MIB」項を参照してください。

Cisco IME SNMP インターフェイスは、次の MIB をサポートしています。

CISCO-CDP-MIB

Cisco Discovery Protocol MIB、CISCO-CDP-MIB を読み取るには、Cisco Unified Communications Manager CDP サブエージェントを使用します。この MIB により、Cisco IME はそれ自体をネットワーク上の他のシスコ デバイスにアドバタイズできます。

CDP サブエージェントは CDP-MIB を実装しています。CDP-MIB には、次のオブジェクトが含まれます。

- cdpInterfaceIfIndex
- cdpInterfaceMessageInterval
- cdpInterfaceEnable
- cdpInterfaceGroup
- cdpInterfacePort
- cdpGlobalRun
- cdpGlobalMessageInterval
- cdpGlobalHoldTime
- cdpGlobalLastChange
- cdpGobalDeviceId
- cdpGlobalDeviceIdFormat
- cdpGlobalDeviceIdFormatCpd

SYSAPPL-MIB

インストールされているアプリケーション、アプリケーション コンポーネント、システムで実行されているプロセスなどの情報を SYSAPPL-MIB から取得するには、System Application Agent を使用します。

System Application Agent は、SYSAPPL-MIB の次のオブジェクト グループをサポートしています。

- sysApplInstallPkg
- sysApplRun
- sysApplMap
- sysApplInstallElmt
- sysApplElmtRun

MIB-II

MIB-II から情報を取得するには、MIB2 エージェントを使用します。MIB2 エージェントは、インターフェイス、IP など、RFC 1213 で定義されている変数へのアクセスを提供します。MIB2 エージェントは、次のオブジェクト グループをサポートしています。

- system
- interfaces
- at
- ip
- icmp
- tcp
- udp
- snmp

HOST-RESOURCES MIB

HOST-RESOURCES-MIB から値を取得するには、Host Resources Agent を使用します。Host Resources Agent は、ストレージ リソース、プロセス テーブル、デバイス情報、インストールされているソフトウェア ベースなど、ホスト情報への SNMP アクセスを提供します。Host Resources Agent は、次のオブジェクト グループをサポートしています。

- hrSystem
- hrStorage
- hrDevice
- hrSWRun
- hrSWRunPerf
- hrSWInstalled

CISCO-SYSLOG-MIB

Syslog は、情報メッセージから重要メッセージまで、すべてのシステム メッセージを追跡し、ログに記録します。この MIB を使用すると、ネットワーク管理アプリケーションで SNMP トラップとして syslog メッセージを受信できます。

Cisco Syslog Agent は、次の MIB オブジェクトについてトラップ機能をサポートしています。

- clogNotificationsSent

- clogNotificationsEnabled
- clogMaxSeverity
- clogMsgIgnores
- clogMsgDrops

ベンダー固有の MIB

各種の Cisco MCS には、ベンダーおよびモデル番号に基づき、次の MIB が含まれます。これらの MIB を照会するために、HP Systems Insight Manager（SIM）、IBM Director Server+Console など、ハードウェア ベンダーが開発した標準 MIB ブラウザを使用できます。MIB ブラウザの使用の詳細については、ハードウェア ベンダーが提供するドキュメントを参照してください。

ベンダー固有の MIB の情報については、次の表を参照してください。

- 表 9-10：サポートされている IBM MIB について説明しています。
- 表 9-11：サポートされている HP MIB について説明しています。

表 9-10　IBM MIB

MIB	OID	説明
参照専用としてサポート		
IBM-SYSTEM-HEALTH-MIB	1.3.6.1.4.1.2.6.159.1.1.30	温度、電圧、およびファンのステータスを提供します。
IBM-SYSTEM-ASSETID-MIB	1.3.6.1.4.1.2.6.159.1.1.60	ハードウェア コンポーネントのアセット データを提供します。
IBM-SYSTEM-LMSENSOR-MIB	1.3.6.1.4.1.2.6.159.1.1.80	温度、電圧、およびファンの詳細情報を提供します。
IBM-SYSTEM-NETWORK-MIB	1.3.6.1.4.1.2.6.159.1.1.110	Network Interface Card（NIC; ネットワーク インターフェイス カード）のステータスを提供します。
IBM-SYSTEM-MEMORY-MIB	1.3.6.1.4.1.2.6.159.1.1.120	物理メモリの詳細情報を提供します。
IBM-SYSTEM-POWER-MIB	1.3.6.1.4.1.2.6.159.1.1.130	電源の詳細情報を提供します。
IBM-SYSTEM-PROCESSOR-MIB	1.3.6.1.4.1.2.6.159.1.1.140	CPU アセットまたはステータスのデータを提供します。
システム トラップ用としてサポート		
IBM-SYSTEM-TRAP	1.3.6.1.4.1.2.6.159.1.1.0	温度、電圧、ファン、ディスク、NIC、メモリ、電源、および CPU の詳細情報を提供します。
IBM-SYSTEM-RAID-MIB	1.3.6.1.4.1.2.6.167.2	RAID のステータスを提供します。

表 9-11　HP MIB

MIB	OID	説明
参照およびシステム トラップ用としてサポート		
CPQSTDEQ-MIB	1.3.6.1.4.1.232.1	ハードウェア コンポーネントの設定データを提供します。
CPQSINFO-MIB	1.3.6.1.4.1.232.2	ハードウェア コンポーネントのアセット データを提供します。
CPQIDA-MIB	1.3.6.1.4.1.232.3	RAID のステータスおよびイベントを提供します。
CPQHLTH-MIB	1.3.6.1.4.1.232.6	ハードウェア コンポーネントのステータスおよびイベントを提供します。
CPQSTSYS-MIB	1.3.6.1.4.1.232.8	ストレージ（ディスク）システムのステータスおよびイベントを提供します。
CPQSM2-MIB	1.3.6.1.4.1.232.9	iLO のステータスおよびイベントを提供します。
CPQTHRSH-MIB	1.3.6.1.4.1.232.10	アラームしきい値の管理を提供します。
CPQHOST-MIB	1.3.6.1.4.1.232.11	オペレーティング システム情報を提供します。
CPQIDE-MIB	1.3.6.1.4.1.232.14	IDE（CD-ROM）ドライブのステータスおよびイベントを提供します。
CPQNIC-MIB	1.3.6.1.4.1.232.18	Network Interface Card（NIC; ネットワーク インターフェイス カード）のステータスおよびイベントを提供します。

関連項目

- 「SNMP 設定チェックリスト」（P.9-1）
- 「SNMP ユーザ」（P.9-3）
- 「SNMP トラップ通知の宛先」（P.9-4）
- 「SNMP インフォーム通知の宛先」（P.9-5）
- 「MIB2 システム グループ」（P.9-7）
- 「SNMP Managed Information Base（MIB; 管理情報ベース）」（P.9-9）

CHAPTER 10

トラブルシューティング

この項では、Cisco Intercompany Media Engine サーバをトラブルシューティングする際に役立つツールについて説明します。Cisco Intercompany Media Engine 機能のトラブルシューティングに関する詳細については、以下の URL を参照してください。

http://docwiki.cisco.com/wiki/Cisco_Intercompany_Media_Engine

この項では、次のトピックについて取り上げます。

システム履歴ログ

このシステム履歴ログにより、初期システム インストール、システム アップグレード、Cisco オプション インストール、DRS バックアップと DRS 復元、バージョンの切り替え、リブート履歴などの情報が一元的に管理され、これらの概要をすばやく取得できます。

この項では、次のトピックについて取り上げます。

システム履歴ログの概要

システム履歴ログはシンプルな ASCII ファイル（**system-history.log**）で、データはデータベースでは管理されません。このログは過度にサイズが大きくなることがないため、システム履歴ファイルのローテーションは行われません。

システム履歴ログは、以下の機能を提供します。

- サーバ上の初期ソフトウェア インストールをログに記録します。
- すべてのソフトウェア アップグレード（Cisco オプション ファイルおよびパッチ）の成功、失敗、またはキャンセルをログに記録します。
- 実行されたすべての DRS のバックアップおよび復元をログに記録します。
- CLI または GUI によって発行されるバージョンの切り替えの呼び出しをすべてログに記録します。

- CLI または GUI によって発行される再起動とシャットダウンの呼び出しをすべてログに記録します。
- システムのすべてのブートをログに記録します。ブートは、再起動エントリまたはシャットダウン エントリと関連しない場合、手動によるリブート、電源の再投入、またはカーネル パニックの結果として生じます。
- 初期インストールから、または機能が使用可能になってからのシステム履歴を収めた単一ファイルを管理します。
- インストール フォルダに存在します。**file** コマンドを使用して CLI から、または Real Time Monitoring Tool（RTMT; リアルタイム監視ツール）からログにアクセスできます。

システム履歴ログのフィールド

ログには、製品名、製品バージョン、カーネル イメージなどの情報を格納する一般的なヘッダーが表示されます。以下に例を示します。

```
======================================
Product Name - Cisco Intercompany Media Engine
Product Version - 8.0.0.30671-1
Kernel Image - 2.6.9-78.EL
======================================
```

各システム履歴ログ エントリには、以下のフィールドが含まれます。

timestamp userid action description start/result

システム履歴ログ フィールドには、以下の値が含まれます。

- *timestamp*：サーバ上のローカル時刻と日付を *mm/dd/yyyy hh:mm:ss* という形式で表示します。
- *userid*：アクションを起動したユーザのユーザ名を表示します。
- *action*：以下のアクションのいずれか 1 つを表示します。
  - インストール
  - アップグレード
  - Cisco オプション インストール
  - バージョンの切り替え
  - システム再起動
  - シャットダウン
  - ブート
  - DRS バックアップ
  - DRS 復元
- *description*：以下のメッセージのいずれか 1 つを表示します。
  - *Version*：基本インストール アクションおよびアップグレード アクションに関する表示です。
  - *Cisco Option file name*：Cisco オプション インストール アクションに関する表示です。
  - *Timestamp*：DRS バックアップ アクションおよび DRS 復元アクションに関する表示です。
  - *Active version to inactive version*：バージョンの切り替えアクションに関する表示です。
  - *Active version*：システム再起動アクション、シャットダウン アクション、およびブート アクションに関する表示です。

- *result*：以下の結果を表示します。
  - 開始
  - 成功または失敗
  - キャンセル

例

例 1 にシステム履歴ログのサンプルを示します。

例 1　　システム履歴ログ

```
======================================
Product Name -    Cisco Intercompany Media Engine
Product Version - 8.0.0.30671-1
Kernel Image -    2.6.9-78.EL
======================================
08/28/2009 10:40:34 | root: Install 8.0.0.30671-1 Start
08/28/2009 10:58:03 | root: Boot 8.0.0.30671-1 Start
08/28/2009 11:02:47 | root: Install 8.0.0.30671-1 Success
08/28/2009 11:02:47 | root: Boot 8.0.0.30671-1 Start
08/28/2009 13:33:48 | root: Cisco Option Install ciscoime.proxy_commands.cop Start
08/28/2009 13:34:18 | root: Cisco Option Install ciscoime.proxy_commands.cop Success
09/07/2009 23:44:43 | root: Upgrade 8.0.0.30600-103 Start
09/07/2009 23:56:48 | root: Upgrade 8.0.0.30600-103 Success
09/07/2009 23:57:06 | root: Switch Version 8.0.0.30671-1 to 8.0.0.30600-103 Start
09/07/2009 23:57:52 | root: Switch Version 8.0.0.30671-1 to 8.0.0.30600-103 Success
09/07/2009 23:57:52 | root: Restart 8.0.0.30600-103 Start
09/08/2009 00:00:36 | root: Boot 8.0.0.30600-103 Start
09/17/2009 12:40:38 | root: Upgrade 8.0.0.96000-2 Start
09/17/2009 12:52:54 | root: Upgrade 8.0.0.96000-2 Success
09/17/2009 12:53:11 | root: Switch Version 8.0.0.30600-103 to 8.0.0.96000-2 Start
09/17/2009 12:53:55 | root: Switch Version 8.0.0.30600-103 to 8.0.0.96000-2 Success
09/17/2009 12:53:55 | root: Restart 8.0.0.96000-2 Start
09/17/2009 12:56:27 | root: Boot 8.0.0.96000-2 Start
09/17/2009 13:29:47 | root: Switch Version 8.0.0.96000-2 to 8.0.0.30600-103 Start
09/17/2009 13:30:34 | root: Switch Version 8.0.0.96000-2 to 8.0.0.30600-103 Success
09/17/2009 13:30:34 | root: Restart 8.0.0.30600-103 Start
09/17/2009 13:33:06 | root: Boot 8.0.0.30600-103 Start
09/17/2009 14:22:20 | root: Upgrade 8.0.0.30600-9003 Start
09/17/2009 14:33:30 | root: Upgrade 8.0.0.30600-9003 Success
09/17/2009 14:33:48 | root: Switch Version 8.0.0.30600-103 to 8.0.0.30600-9003 Start
09/17/2009 14:34:33 | root: Switch Version 8.0.0.30600-103 to 8.0.0.30600-9003 Success
09/17/2009 14:34:33 | root: Restart 8.0.0.30600-9003 Start
09/17/2009 14:37:03 | root: Boot 8.0.0.30600-9003 Start
```

システム履歴ログへのアクセス

CLI または RTMT のいずれかを使用して、システム履歴ログにアクセスできます。

CLI の使用

CLI **file** コマンドを使用して、システム履歴ログにアクセスできます。以下に例を示します。

- **file view install system-history.log**
- **file get install system-history.log**

CLI **file** コマンドの詳細については、『*Cisco Intercompany Media Engine Command Line Interface Reference Guide*』を参照してください。

RTMT の使用

RTMT を使用して、システム履歴ログにアクセスできます。[Trace & Log Central] タブから [インストールログの収集 (Collect Install Logs)] を選択します。

RTMT の使用方法の詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。

監査ロギング

一元化された監査ロギングにより、Cisco Intercompany Media Engine システムへの設定変更を監査用の別のログ ファイルに記録できます。監査イベントとは、ログの記録が必要なすべてのイベントを表します。以下の Cisco Intercompany Media Engine システム コンポーネントは監査イベントを生成します。

- Real-Time Monitoring Tool
- Cisco Unified Communications オペレーティング システム
- コマンド ライン インターフェイス
- リモート サポート アカウント有効化 (テクニカル サポート チームによって発行される CLI コマンド)

以下に、監査イベントの例を示します。

```
10:39:28.787| UserID:Administrator  ClientAddress:10.194.109.32  Severity:6  EventType:
CLICommand  ResourceAccessed: GenericCLI  EventStatus: Success  CompulsoryEvent: No
AuditCategory: AdministrativeEvent  ComponentID: CLI  AuditDetails: CLI Command-> utils
ime license file install IME20091020095547801_node32.lic App ID:Command Line Cluster ID:
Node ID: node32
```

監査イベントに関する情報が記録される監査ログは、共通パーティションで書き込まれます。Log Partition Monitor（LPM）を使用して、トレース ファイルと同様、必要に応じてこれらの監査ログの消去を管理します。デフォルトでは、LPM は監査ログを消去しますが、監査ユーザは Cisco Intercompany Media Engine Command Line Interface（CLI; コマンド ライン インターフェイス）からこの設定を変更できます。LPM は、共通パーティションのディスク使用量がしきい値を超えたときにアラートを送信します。ただし、このアラートには、監査ログまたはトレース ファイルのどちらのためにディスクがいっぱいになったかを示す情報は含まれていません。

ヒント　Cisco Audit Event Service は、監査ロギングをサポートしています。監査ログが記録されていない場合、CLI（utils service stop **Cisco Audit Event Service** および utils service start **Cisco Audit Event Service**）を使用してこのサービスを停止および開始します。

Real-Time Monitoring Tool の [Trace & Log Central] から、すべての監査ログの収集、表示、および削除が行えます。RTMT の [Trace & Log Central] で監査ログにアクセスします。[システム (System)] > [リアルタイムトレース (Real Time trace)] > [監査ログ (Audit Logs)] > [ノード (Nodes)] と進みます。ノードを選択した後、別ウィンドウが表示されたら、[システム (System)] > [Cisco 監査ログ (Cisco Audit Logs)] を選択します。

以下のタイプの監査ログが RTMT に表示されます。

- 「アプリケーション ログ」(P.10-5)
- 「オペレーティング システム ログ」(P.10-5)
- 「リモート サポート アカウント有効化のログ」(P.10-6)

アプリケーション ログ

RTMT の AuditApp フォルダに表示されるアプリケーション監査ログは、Cisco Unified Communications Manager の管理、Cisco Unified サービスアビリティ、CLI、および Real-Time Monitoring Tool（RTMT; リアルタイム監視ツール）の設定変更を行います。

デフォルトでは、アプリケーション ログは有効ですが、CLI **set auditlog status** コマンドを使用して監査ロギングを無効にできます。監査ログが無効になると、監査ログ ファイルは新規で作成されなくなります。

Cisco Unified Communications Manager は、設定された最大ファイル サイズに達するまで、1 つのアプリケーション監査ログ ファイルを使用します。最大ファイル サイズに達すると、そのファイルを閉じ、新規アプリケーション監査ログ ファイルを作成します。システムでログ ファイルのローテーションが指定されている場合、Cisco Unified Communications Manager は設定されている数のファイルを保存します。ロギング イベントの一部は、RTMT SyslogViewer を使用して表示できます。

以下の Cisco Unified サービスアビリティのイベントは、ログに記録されます。

- [サービスアビリティ (Serviceability)] ウィンドウからのサービスのアクティブ化、非アクティブ化、開始、または停止。
- トレース設定およびアラーム設定での変更。
- SNMP 設定での変更。

RTMT は、監査イベント アラームを使用する以下のイベントをログに記録します。

- アラート設定。
- アラート一時停止。
- 電子メール設定。
- ノード アラート ステータスの設定。
- アラート追加。
- アラート アクションの追加。
- アラートのクリア。
- アラートの有効化。
- アラート アクションの削除。
- アラートの削除。

（注） 監査ログは、コマンドの実行が許可されていない場合でも、CLI コマンドを正常にログに記録します。たとえば、次の操作は、ブートストラップ サーバでのみ許可されています。

```
admin:set ime dht global storagequota 1
```

上記のコマンドが他のサーバで実行されると、ユーザは「このコマンドの実行はブートストラップサーバでのみ許可されています(This command is only allowed to be run on a bootstrap server)」というメッセージを受け取りますが、監査ログは CLI コマンドを status=Success でログに記録します。

オペレーティング システム ログ

RTMT の vos フォルダに表示されるオペレーティング システム監査ログは、オペレーティング システムによってトリガーされるイベントを記録します。デフォルトでは、有効ではありません。**utils auditd** CLI コマンドによって、このイベントに関するステータスの有効化、無効化、または付与が行われます。

CLI で監査が有効になるまで、RTMT の vos フォルダには表示されません。

リモート サポート アカウント有効化のログ

RTMT の vos フォルダに表示されるリモート サポート アカウント有効化の監査ログは、テクニカル サポート チームによって発行される CLI コマンドを記録します。ユーザはこのログを設定できません。このログは、テクニカル サポート チームによってリモート サポート アカウントが有効なときのみ、作成されます。

監査ロギングの設定

表 10-1 に、Cisco Intercompany Media Engine サーバで SNMP ユーザを操作するために必要なコマンドを示します。

表 10-1　監査ロギング設定チェックリスト

設定手順		関連する手順と項目
ステップ 1	オペレーティング システム監査ログを有効にします。RTMT からシステムの監査ログ ファイルを取得できます。 **ヒント** オペレーティング システム監査ログのステータスを確認するには、**utils auditd status** CLI コマンドを入力します。	utils auditd *status* ここで、 *status* は enable または disable です。
ステップ 2	監査ロギングを有効にします。RTMT からシステムの監査ログ ファイルを取得できます。 **ヒント** 監査ログのステータスを確認するには、**show auditlog** CLI コマンドを入力します。	set auditlog status *status* パラメータを入力するよう求めるプロンプトが表示されます。ここで、 *status* は enable または disable です。
ステップ 3	ステータスの消去を設定します。 Log Partition Monitor（LPM）は、[消去の有効化 (Enable Purging)] オプションを確認し、監査ログを消去するかどうかを識別します。消去が有効な場合、共通パーティションのディスク使用量が最高水準値を超えると、LPM は RTMT 内のすべての監査ログ ファイルを消去します。ただし、チェックボックスをオフにすることで、消去を無効にできます。 消去が無効な場合、ディスクがいっぱいになるまで、監査ログの数は増加します。このアクションは、システムに障害が発生する原因になる可能性があります。 この消去オプションは、監査ログがあるパーティションがアクティブかどうかに応じて指定できます。監査ログが非アクティブなパーティションにある場合、ディスク使用量が最高水準値を超えたときに、それらの監査ログを消去します。 RTMT の [Trace & Log Central] > [監査ログ (Audit Logs)] を選択して、監査ログにアクセスできます。	set auditlog purging *status* パラメータを入力するよう求めるプロンプトが表示されます。ここで、 *status* は enable または disable です。

表 10-1　監査ロギング設定チェックリスト （続き）

設定手順		関連する手順と項目
ステップ 4	ログ ローテーション ステータスを設定します。 システムは、このオプションを読み込み、監査ログ ファイルをローテーションする必要があるか、または新規ファイルを作成し続ける必要があるかを識別します。ファイルの最大数は、5000 を超えて指定できません。[ローテーションの有効化 (Enable Rotation)] オプションが有効な場合、ファイルの最大数に達すると、システムは最も古い監査ログ ファイルから上書きを開始します。 **ヒント** ローテーションが無効な場合、監査ログは [ファイルの最大数 (Maximum No. of Files)] 設定 を無視します。	set auditlogrotation *status* パラメータを入力するよう求めるプロンプトが表示されます。ここで、 *status* は enable または disable です。
ステップ 5	ファイルの最大数を設定します。 ログに含めるファイルの最大数を入力します。[ファイルの最大数 (Maximum No. of Files)] 設定に入力した値が、[ログローテーション時に削除されるファイル数 (No. of Files Deleted on Log Rotation)] 設定に入力した値より 大きいことを確認してください。	set auditlog maxnumfiles *filecount* パラメータを入力するよう求めるプロンプトが表示されます。ここで、 *filecount* は 1 ～ 10000 の範囲です。
ステップ 6	最大ファイル サイズを設定します。	set auditlog maxfilesize *size* パラメータを入力するよう求めるプロンプトが表示されます。ここで、 *size* は 1 ～ 10 の範囲です。
ステップ 7	監査ログ リモート Syslog 重大度レベルを設定します。	set auditlog remotesyslogseverity *severity* パラメータを入力するよう求めるプロンプトが表示されます。ここで、 *severity* は 「緊急 (Emergency)」、「アラート (Alert)」、「重要 (Critical)」、「エラー (Error)」、「警告 (Warning)」、「通知 (Notice)」、「情報 (Informational)」、または「デバッグ (Debug)」 のいずれかです。
ステップ 8	リモート Syslog サーバ名を入力します。	set auditlog remotesyslogserver *servername* パラメータを入力するよう求めるプロンプトが表示されます。ここで、 *servername* は、リモート Syslog サーバの有効なホスト名です。

netdump ユーティリティ

netdump ユーティリティを使用して、データおよびメモリ クラッシュ ダンプ ログをネットワーク上の 1 台のサーバから別のサーバに送信できます。netdump クライアントとして設定されたサーバは、クラッシュ ログを netdump サーバとして設定されたサーバに送信します。ログ ファイルは、netdump サーバのクラッシュ ディレクトリに送信されます。

Cisco Unified Communications Manager クラスタでは、少なくとも 2 つのノードを netdump サーバとして設定する必要があります。そうすることで、最初のノードも後続のノードも、相互にクラッシュ ダンプ ログを送信できます。

たとえば、クラスタに 3 台のサーバ（1 台のプライマリ（最初の）ノードと 2 台の後続ノード）がある場合、最初のノードと後続ノード #1 を netdump サーバとして設定できます。また、最初のノードを後続ノード #1 の netdump クライアントとして設定し、後続のすべてのノードを最初のノードの netdump クライアントとして設定できます。最初のノードがクラッシュした場合、最初のノードは netdump を後続ノード #1 に送信します。後続ノードのいずれかがクラッシュした場合、そのノードは netdump を最初のノードに送信します。

Cisco Unified Communications Manager サーバを netdump サーバとして設定する代わりに、外部の netdump サーバを使用することもできます。外部 netdump サーバの設定の詳細については、TAC にお問い合わせください。

（注） Cisco は、Cisco Unified Communications Manager をインストールした後に netdump ユーティリティを設定して、トラブルシューティングに役立てることをお勧めします。設定をまだ行っていない場合、サポートされているアプライアンス リリースから Cisco Unified Communications Manager をアップグレードする前に、この netdump ユーティリティを設定してください。

netdump のサーバおよびクライアントを設定するには、次のセクションで説明されるように、Cisco Unified Communications オペレーティング システムを使用可能にする Command Line Interface（CLI; コマンド ライン インターフェイス）を使用します。

- 「netdump サーバの設定」（P.10-9）
- 「netdump クライアントの設定」（P.10-10）
- 「netdump サーバが収集するファイルでの作業」（P.10-10）
- 「netdump ステータスの監視」（P.10-10）

netdump サーバの設定

netdump サーバとしてノードを設定するには、以下の手順を使用します。

手順

ステップ 1　『*Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*』で説明されているように、netdump サーバとして設定するノード上で、CLI セッションを開始します。

ステップ 2　**utils netdump server start** コマンドを実行します。

ステップ 3　netdump サーバのステータスを表示するには、**utils netdump server status** コマンドを実行します。

ステップ 4　「netdump クライアントの設定」（P.10-10）で説明されるように、netdump クライアントを設定します。

netdump クライアントの設定

netdump クライアントとしてノードを設定するには、以下の手順を使用します。

手順

ステップ 1　『*Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*』で説明されているように、netdump クライアントとして設定するノード上で、CLI セッションを開始します。

ステップ 2　**utils netdump client start** *ip-address-of-netdump-server* コマンドを実行します。

ステップ 3　**utils netdump server add-client** *ip-address-of-netdump-client* を実行します。netdump クライアントとして設定する各ノードに対して、このコマンドを繰り返し実行します。

（注）　正しい IP アドレスが入力されているか確認してください。CLI は IP アドレスを検証しません。

ステップ 4　netdump クライアントのステータスを表示するには、**utils netdump client status** コマンドを実行します。

netdump サーバが収集するファイルでの作業

netdump サーバからクラッシュ情報を表示するには、Real-Time Monitoring Tool または Command Line Interface（CLI; コマンド ライン インターフェイス）を使用します。Real-Time Monitoring Tool を使用して netdump ログを収集するには、[Trace & Log Central] で [ファイルの収集 (Collect Files)] オプションを選択します。[システムサービス / アプリケーションの選択 (Select System Services/Applications)] タブで、[Netdump ログ (Netdump logs)] チェックボックスを選択します。Real-Time Monitoring Tool を使用するファイルの収集の詳細については、『*Cisco Unified Real Time Monitoring Tool Administration Guide*』を参照してください。

CLI を使用して netdump ログを収集するには、クラッシュ ディレクトリにあるファイルに「file」CLI コマンドを実行します。ログのファイル名は、netdump クライアントの IP アドレスで始まり、末尾にファイルの作成日が付きます。file コマンドの詳細については、『*Command Line Interface Reference Guide for Cisco Unifed Communications Solutions*』を参照してください。

netdump ステータスの監視

Real-Time Monitoring Tool の SyslogSearchStringFound アラートを設定して、netdump ステータスを監視できます。以下の手順を使用して、適切なアラートを設定してください。

手順

ステップ 1　Real-Time Monitoring Tool のクイック起動チャネルから、[ツール (Tools)] > [Alert Central] を選択します。

ステップ 2　[SyslogStringMatchFound] アラートを右クリックし、[アラート / プロパティの設定 (Set Alert/Properties)] を選択します。

ステップ 3　[次へ (Next)] を 3 回クリックします。

ステップ 4　[SysLog アラート (SysLog Alert)] ウィンドウで、[追加 (Add)] ボタンをクリックします。[検索文字列の追加 (Add Search String)] ダイアログボックスが表示されたら、「**netdump: failed**」を入力し、[追加 (Add)] をクリックします。次に、[次へ (Next)] をクリックします。

（注）　大文字 / 小文字および構文が完全に一致していることを確認してください。

ステップ 5　[電子メール通知 (Email Notification)] ウィンドウで、適切なトリガー アラート アクションを選択して、任意のユーザ定義の電子メール テキストを入力し、[保存 (Save)] をクリックします。

CHAPTER 11

Cisco Intercompany Media Engine のパフォーマンス オブジェクトおよびカウンタ

この項では、Cisco Intercompany Media Engine のオブジェクトおよびカウンタについて説明します。Cisco Unified Communications Manager サーバと Cisco Intercompany Media Engine サーバには、どちらにもオブジェクトとカウンタの固有セットが含まれます。Cisco Intercompany Media Engine 製品のパフォーマンスを監視するために、両方のサーバのカウンタが必要な場合があります。

パフォーマンス オブジェクトおよびカウンタにアクセスするには、該当するサーバの RTMT にログインし、[システム (System)] > [パフォーマンス (Performance)] > [パフォーマンスモニタリングを開く (Open Performance Monitoring)] の順に選択します。パフォーマンス カウンタおよびオブジェクトの操作の詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。

この項の内容は次のとおりです。

Cisco Intercompany Media Engine サーバ オブジェクト

Cisco Unified Communications Manager サーバ オブジェクト

追加情報

IME Configuration Manager

IME Configuration Manager オブジェクトは、IME 分散キャッシュ証明書に関する情報を提供します。表 11-1 で、Cisco IME 設定カウンタについて説明します。

表 11-1　IME Configuration Manager

カウンタ	カウンタの説明
DaysUntilCertExpiry	このカウンタは、IME 分散キャッシュ証明書が期限切れになるまでの残りの日数を示します。証明書が期限切れになる前に、代わりの証明書を用意する必要があります。 このカウンタの値が 14 未満の場合、値が 14 を上回るまで毎日 1 回アラートが生成されます。

IME Server

IME Server オブジェクトは、Cisco IME サーバに関する情報を提供します。表 11-2 で、Cisco IME Server カウンタについて説明します。

表 11-2　IME Server

カウンタ	カウンタの説明
BlockedValidationOrigTLSLimit	このカウンタは、TLSValidationThreshold に達したことが原因でブロックされた検証の合計数を示します。
BlockedValidationTermTLSLimit	このカウンタは、TLSValidationThreshold に達したことが原因でブロックされた検証の合計数を示します。
ClientsRegistered	このカウンタは、Cisco IME サーバに現在接続されている Cisco IME クライアントの数を示します。
IMEDistributedCacheHealth	このカウンタは、IME 分散キャッシュの健康状態を示します。場合により、次の値が表示されます。 • 0（赤）：IME 分散キャッシュが正常に機能していないことを警告として示します。たとえば、ネットワークが分割された後、Cisco IME は問題を解決できません。この場合、検証試行は失敗することがあります。たとえば、ネットワークに接続されていない Cisco IME サービスは、ブートストラップ サーバにアクセスできません。 値が赤のステータス以外に変更されるまで、1 時間おきにアラートが生成されます。 • 1（黄）：ブートストラップ サーバ間の接続、Cisco IME ネットワークのその他の問題など、Cisco IME ネットワークで深刻ではない問題が発生したことを示します（ネットワークの問題を特定するには、Cisco IME アラームを確認します）。 • 2（緑）：Cisco IME が正常に機能しており、健康と見なされることを示します。

表 11-2　IME Server （続き）

カウンタ	カウンタの説明
IMEDistributedCacheNodeCount	このカウンタは、IME 分散キャッシュ内のノードのおおよその合計数を示す整数です。各物理 Cisco IME サーバは複数のノードをホストするため、このカウンタは IME 分散キャッシュに参加する物理 Cisco IME サーバの数を直接的には示しません。このカウンタは、IME 分散キャッシュの健康状態の指標となります。たとえば、ある日に予想通りの値が表示され（たとえば 300）、次の日に値が大幅に減少した場合（たとえば 10 や 2）、IME 分散キャッシュで問題が発生している可能性があります。
IMEDistributedCacheQuota	この IME サーバに接続している Cisco Unified CM が IME 分散キャッシュに書き込むことができる個々の DID の数を示します。この数は、IME 分散キャッシュのすべての設定、および IME サーバにインストールされている IME ライセンスにより決まります。
IMEDistributedCacheQuotaUsed	Intercompany Media Service の登録済みパターンを通じて発行される、この IME サーバに現在接続している Cisco Unified CM が設定した、固有 DID 番号の合計数を示します。
IMEDistributedCacheReads	このカウンタは、IME 分散キャッシュに対して Cisco IME サーバが試行した読み取りの合計数を示します。この数は、Cisco IME サーバが機能しているかどうか、つまりサーバが他のノードと対話しているかどうかを示す指標となります。
IMEDistributedCacheStoredData	このカウンタは、この Cisco IME サーバが提供している IME 分散キャッシュ ストレージの容量をバイト単位で示します。
IMEDistributedCacheStores	このカウンタは、Cisco IME サーバが IME 分散キャッシュに対して試行した保存の合計数（発行数）を示します。この数は、Cisco IME サーバが機能しているかどうかの指標となります。
InternetBandwidthRecv	このカウンタは、Cisco IME サーバが消費しているインターネットのダウンリンクの帯域幅量をキロビット/秒単位で示します。
InternetBandwidthSend	このカウンタは、Cisco IME サーバが消費しているインターネットのアップリンクの帯域幅量をキロビット/秒単位で示します。
TerminatingVCRs	このカウンタは、コールの受信後、Cisco IME サーバに保存された Cisco IME Voice Call Records（VCRs; 音声コール レコード）の合計数を示します。学習ルートを検証するために、これらのレコードを使用できます。
ValidationAttempts	このカウンタは、Cisco IME ネットワークでダイヤル番号が見つかったために、Cisco IME サーバが検証実行時に行った試行の合計数を示します。このカウンタは、システム使用の全体的な指標となります。
ValidationsAwaitingConfirmation	このカウンタは、検証された一方で、システムのセキュリティを改善するために、以降のコールを待機している接続先電話番号の合計数を示します。新しいルートを学習するために、より高いレベルのセキュリティを使用する場合、Cisco IME サーバでは、ルートを IP コールで使用できるようにする前に、そのルートの検証が複数回成功する必要があります。このカウンタは、使用可能な IP ルートという結果に至らなかった成功検証の数を追跡します。

表 11-2　IME Server （続き）

カウンタ	カウンタの説明
ValidationsPending	このカウンタは、学習ルートを取得するためのスケジュール済み検証試行の数（整数）を示します。この値は、Cisco IME サーバ上の Cisco IME サービスの未処理の作業を示します。 値が上限を上回ると、または下限を下回ると、アラートが生成されます。上限に達すると、直後にアラートが送信され、さらに値が上限を下回るまで 1 時間に 1 回アラートが送信されます。上限に達した場合、Cisco IME サービスは、データの期限切れ前に未処理の作業をクリアできません。この状況が原因でレコードが欠落し、検証が実行されない場合があります。負荷を軽減するには、負荷を分担できる Cisco IME サーバを追加します。
ValidationsBlocked	このカウンタは、発信側が信頼済みでないため、つまり、発信側がブラックリストに含まれているため、またはホワイトリストに含まれていないために、Cisco IME サービスが検証試行を拒否した回数を示します。この値は、検証のブロックが原因で、今後 VoIP コールが実行されない回数の指標となります。

IME サーバ システムのパフォーマンス

Cisco IME System Performance オブジェクトは、Cisco IME サーバのパフォーマンスに関する情報を提供します。表 11-3 で、Cisco IME サーバ システムのパフォーマンス カウンタについて説明します。

表 11-3　IME サーバ システムのパフォーマンス

カウンタ	カウンタの説明
QueueSignalsPresent 1-High	このカウンタは、Cisco IME サーバ上のキュー内の高優先順位信号の数を示します。高優先順位信号には、タイムアウト イベント、内部キープアライブ メッセージ、内部プロセス作成などがあります。高優先順位信号イベントが多数あると、Cisco IME サービスのパフォーマンスが低下し、結果として検証が低速になるか、失敗します。このカウンタと QueueSignalsProcessed 1-High カウンタを併用して、Cisco IME サーバでの処理の遅延を確認します。
QueueSignalsPresent 2-Normal	このカウンタは、Cisco IME サーバ上のキュー内の通常優先順位信号の数を示します。通常優先順位信号には、コールの検証、IME 分散キャッシュ操作（保存、読み取りなど）などがあります。通常優先順位イベントが多数あると、Cisco IME サービスのパフォーマンスが低下し、結果として検証が低速になるか、失敗する場合があります。また IME 分散キャッシュに接続できなくなる場合があります。このカウンタと QueueSignalsProcessed 2-Normal カウンタを併用して、Cisco IME サーバでの処理の遅延を確認します。 高優先順位信号の処理は、通常優先順位信号の処理が開始される前に完了するため、遅延が発生した原因を正確に理解するには、高優先順位カウンタを確認します。
QueueSignalsPresent 3-Low	このカウンタは、Cisco IME サーバ上のキュー内の低優先順位信号の数を示します。低優先順位信号には、IME 分散キャッシュ信号、その他のイベントなどがあります。このキュー内の信号の数が多いと、IME 分散キャッシュに接続できない場合、または他のイベントが実行できない場合があります。
QueueSignalsPresent 4-Lowest	このカウンタは、Cisco IME サーバ上のキュー内の最低優先順位信号の数を示します。このキュー内の信号の数が多いと、IME 分散キャッシュに接続できない場合、および他のイベントが実行できない場合があります。

表 11-3　IME サーバ システムのパフォーマンス （続き）

カウンタ	カウンタの説明
QueueSignalsProcessed 1-High	このカウンタは、Cisco IME サービスが 1 秒間に処理する高優先順位信号の数を示します。このカウンタと QueueSignalsPresent 1-High カウンタを併用して、このキューの処理の遅延を確認します。
QueueSignalsProcessed 2-Normal	このカウンタは、Cisco IME サービスが 1 秒間に処理する通常優先順位信号の数を示します。このカウンタと QueueSignalsPresent 1-High カウンタを併用して、このキューの処理の遅延を確認します。通常優先順位信号の前に高優先順位信号が処理されます。
QueueSignalsProcessed 3-Low	このカウンタは、Cisco IME サービスが 1 秒間に処理する低優先順位信号の数を示します。このカウンタと QueueSignalsPresent 3-Low カウンタを併用して、このキューの処理の遅延を確認します。
QueueSignalsProcessed 4-Lowest	このカウンタは、Cisco IME サービスが 1 秒間に処理する最低優先順位信号の数を示します。このカウンタと QueueSignalsPresent 4-Lowest カウンタを併用して、このキューの処理の遅延を確認します。
QueueSignalsProcessed Total	このカウンタは、Cisco IME サービスが 1 秒間に処理する、すべてのキュー レベル（高、通常、低、および最低）のすべてのキュー信号の合計数を示します。

IME クライアント

IME クライアント オブジェクトは、Cisco Unified Communications Manager サーバ上の Cisco IME クライアントに関する情報を提供します。表 11-4 で、Cisco IME クライアント カウンタについて説明します。

表 11-4　Cisco IME クライアント

カウンタ	カウンタの説明
CallsAccepted	このカウンタは、Cisco Unified Communications Manager が正常に受信し、着信側として応答し、結果として IP コールとなった Cisco IME コールの数を示します。
CallsAttempted	このカウンタは、Cisco IME を通じて Cisco Unified Communications Manager が受信したコールの数を示します。この数には、承認されたコール、失敗したコール、および通話中で応答なしのコールが含まれます。このカウンタは、Cisco Unified Communications Manager が Cisco IME を通じてコールを受信するたびに 1 増えます。
CallsReceived	このカウンタは、Cisco Unified Communications Manager が Cisco IME を通じて受信するコールの数を示します。この数には、承認されたコール、失敗したコール、および通話中で応答なしのコールが含まれます。このカウンタは、コール開始時に 1 増えます。
CallsSetup	このカウンタは、Cisco Unified Communications Manager が正常に送信し、リモート側が応答し、結果として IP コールとなった Cisco IME コールの数を示します。
DomainsUnique	このカウンタは、Cisco IME クライアントが検出したピア企業の固有ドメイン名の数を示します。このカウンタは、システムの全体的な使用状況の指標となります。
FallbackCallsFailed	このカウンタは、失敗したフォールバック試行の合計数を示します。

表 11-4　Cisco IME クライアント （続き）

カウンタ	カウンタの説明
FallbackCallsSuccessful	このカウンタは、品質の問題が原因で通話中に PSTN にフォールバックされた Cisco IME コールの合計数を示します。このカウンタには、この Cisco Unified Communications Manager が開始したコールおよび受信したコールが含まれます。
IMESetupsFailed	このカウンタは、Cisco IME ルートが使用できた一方で、IP ネットワークを通じてターゲットに接続できなかったことが原因で、PSTN を通じて確立されたコール試行の合計数を示します。
RoutesLearned	このカウンタは、Cisco IME が学習し、Cisco Unified Communications Manager ルーティング テーブル内にルートとして存在する個別の電話番号の合計数を示します。この数が大きくなりすぎると、サーバがクラスタあたりの制限を超過する場合があり、場合によりサーバをクラスタに追加する必要があります。
RoutesPublished	このカウンタは、すべての Cisco IME クライアント インスタンス間の IME 分散キャッシュに正常に発行された DID の合計数を示します。このカウンタが示す動的測定値は、任意のプロビジョニングの使用の指標となります。またこの動的測定値により、ネットワークでシステムによる DID の保存がどの程度成功したか判断できます。
RoutesRejected	このカウンタは、管理者が番号またはドメインをブラックリストに追加したために拒否された学習ルートの数を示します。このカウンタは、検証がブロックされたことが原因で、今後実行できない VoIP コールの数の指標となります。
VCRUploadRequests	このカウンタは、Cisco Unified Communications Manager が Cisco IME サーバに送信した、IME 分散キャッシュに保存する Voice Call Records（VCRs; 音声コール レコード）のアップロード要求の数を示します。

IME クライアント インスタンス

IME クライアント インスタンス オブジェクトは、Cisco Unified Communications Manager サーバ上の Cisco IME クライアント インスタンスに関する情報を提供します。表 11-5 で、Cisco IME クライアント インスタンス カウンタについて説明します。

表 11-5　IME クライアント

カウンタ	カウンタの説明
IMEServiceStatus	このカウンタは、特定の Cisco IME クライアント インスタンス（Cisco Unified Communications Manager）用の Cisco IME サービスへの接続について全体的な正常性を示します。このカウンタは、場合により次の値を示します。 • 0：不明の状態を示します（Cisco IME サービスがアクティブでないことを示す場合があります）。 値が 0 の場合、接続が不明の状態の間、1 時間に 1 回アラートが生成されます。 • 1：健康な状態を示します。つまり、Cisco IME サービスがアクティブであり、Cisco Unified Communications Manager が、Cisco IME クライアント インスタンス用のプライマリ サーバおよびバックアップ サーバ（設定されている場合）への接続を正常に確立したことを示します。 • 2：不健康な状態を示します。つまり、Cisco IME サービスがアクティブである一方で、Cisco Unified Communications Manager が、Cisco IME クライアント インスタンス用のプライマリ サーバおよびバックアップ サーバ（設定されている場合）への接続を正常に確立できなかったことを示します。

関連項目

- 「Cisco Unified Communications Manager の管理での Cisco IME の設定」（P.3-1）
- 「Cisco Intercompany Media Engine での RTMT の使用」（P.7-1）
- 『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』

関連項目

CHAPTER 12

Cisco Intercompany Media Engine アラートの説明およびデフォルト設定

この項では、Cisco Intercompany Media Engine アラートについて説明しています。事前に定義された条件になった場合、Cisco Unified Communications Manager サーバと Cisco Intercompany Media Engine サーバのいずれもが、一意の一連のアラートを生成します。両方のサーバからのアラートを監視して、Cisco Intercompany Media Engine 製品の状態を判別する必要があります。

アラートにアクセスするには、適切なサーバ上の RTMT にログインし、[システム (System)] > [ツール (Tools)] > [アラート (Alert)] > [Alert Central] を選択します。アラートの処理の詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。

次のリストには、Cisco Intercompany Media Engine アラート、アラートの定義、およびデフォルト設定を示してあります。

Cisco Intercompany Media Engine サーバのアラート

Cisco Unified Communications Manager サーバのアラート

- 「TCPSetupToIMEFailed」（P.12-16）
- 「TLSConnectionToIMEFailed」（P.12-17）

追加情報

「関連項目」（P.12-19）

BannedFromNetwork

このアラートは、ネットワーク管理者がネットワーク（IME 分散キャッシュ リング）でこの Cisco IME サーバを禁止して、この Cisco IME サービスを全体的または部分的に操作不能にしたことを示します。ネットワーク管理者がサーバの操作を禁止することはまれですが、ネットワークへの悪質な攻撃でそのサーバが使用されていることを検出した場合などが該当します。エラーに含まれたこのアラートを受け取った場合は、すぐに TAC に問い合わせてください。

デフォルトの設定

表 12-1　BannedFromNetwork アラートのデフォルトの設定

値	デフォルトの設定
[アラートの有効化 (Enable Alert)]	選択済み
[重大度 (Severity)]	[アラート (Alert)]
[次のサーバでのこのアラートの有効/無効 :(Enable/Disable this alert on the following server(s))]	リストされたサーバで有効化
[しきい値 (Threshold)]	次の条件が満たされた場合にアラートをトリガーする。 Cisco IME サービスがネットワークで禁止されている。
[接続時間 (Duration)]	アラートをただちにトリガーする。
[頻度 (Frequency)]	すべてのポーリングでアラートをトリガーする。
[スケジュール (Schedule)]	毎日 24 時間
[電子メールの有効化 (Enable Email)]	選択済み
[アラートのトリガーアクション :(Trigger Alert Action:)]	[デフォルト (Default)]

IMEDistributedCacheCertificateExpiring

このアラートは、IME 分散キャッシュ用に使用されている証明書の有効期限が切れるまでの残日数を示します。有効期限が切れる前に証明書を交換する必要があります。

デフォルトの設定

表 12-2　IMEDistributedCacheCertificateExpiring アラートのデフォルトの設定

値	デフォルトの設定
[アラートの有効化 (Enable Alert)]	選択済み
[重大度 (Severity)]	[警告 (Warning)]
[次のサーバでのこのアラートの有効/無効 :(Enable/Disable this alert on the following server(s))]	リストされたサーバで有効化
[しきい値 (Threshold)]	次の条件が満たされた場合にアラートをトリガーする。 Cisco IME 分散キャッシュ証明書の有効期限が切れそうになっている。14 日間。
[接続時間 (Duration)]	アラートをただちにトリガーする。
[頻度 (Frequency)]	1440 分以内に最大 1 個のアラートをトリガーする
[スケジュール (Schedule)]	毎日 24 時間
[電子メールの有効化 (Enable Email)]	選択済み
[アラートのトリガーアクション :(Trigger Alert Action:)]	[デフォルト (Default)]

IMEDistributedCacheFailure

このアラートは、IME 分散キャッシュの正常性を示します。値ゼロ（赤）は、IME 分散キャッシュに次のような重大な問題が発生していることを示します。

- ネットワークが分割された後で、Cisco IME が問題を解決できない。この場合、試行した検証は失敗します。
- Cisco IME サービスがネットワークにまったく接続されておらず、ブートストラップ サーバに到達できない。

値 1（黄色）は、Cisco IME ネットワークで、ブートストラップ サーバとの接続の問題などの軽微な問題や、その他の Cisco IME ネットワークの問題が発生していることを示します。このカウンタが 1 になった原因を示す可能性のある、すべてのアラームを調べてください。値 2 は、IME 分散キャッシュが正常に機能しており、システムは正常であると見なされることを示します。

デフォルトの設定

表 12-3　IMEDistributedCacheFailure アラートのデフォルトの設定

値	デフォルトの設定
[アラートの有効化 (Enable Alert)]	選択済み
[重大度 (Severity)]	[アラート (Alert)]
[次のサーバでのこのアラートの有効/無効 :(Enable/Disable this alert on the following server(s))]	リストされたサーバで有効化
[しきい値 (Threshold)]	次の条件が満たされた場合にアラートをトリガーする。 IME 分散キャッシュの状態が正常でない 1：ネットワークで軽微な問題が発生 0：ネットワークに問題あり
[接続時間 (Duration)]	アラートをただちにトリガーする。
[頻度 (Frequency)]	60 分以内にアラートを 1 個トリガー
[スケジュール (Schedule)]	毎日 24 時間
[電子メールの有効化 (Enable Email)]	選択済み
[アラートのトリガーアクション :(Trigger Alert Action:)]	[デフォルト (Default)]

IMESdlLinkOutOfService

このアラートは、Cisco IME サービスと、Cisco AMC サービスや Cisco CallManager サービスなどの Cisco IME Config Manager サービスとの通信が切断されたことを示します。

通常、このアラートは、メンテナンスのために意図的に、または接続の障害が原因で意図せずに、このいずれかのサービスが停止したことを示します。

デフォルトの設定

表 12-4　IMESdlLinkOutOfService アラートのデフォルトの設定

値	デフォルトの設定
[アラートの有効化 (Enable Alert)]	選択済み
[重大度 (Severity)]	[重要 (Critical)]

表 12-4　IMESdlLinkOutOfService アラートのデフォルトの設定 （続き）

値	デフォルトの設定
[次のサーバでのこのアラートの有効/無効 :(Enable/Disable this alert on the following server(s))]	リストされたサーバで有効化
[しきい値 (Threshold)]	次の条件が満たされた場合にアラートをトリガーする。 SDLLinkOOS イベントが生成された
[接続時間 (Duration)]	アラートをただちにトリガーする。
[頻度 (Frequency)]	すべてのポーリングでアラートをトリガーする。
[スケジュール (Schedule)]	毎日 24 時間
[電子メールの有効化 (Enable Email)]	選択済み
[アラートのトリガーアクション :(Trigger Alert Action:)]	[デフォルト (Default)]

InvalidCertificate

このアラートは、管理者が Cisco IME サーバ上で IME 分散キャッシュを使用可能にした一方で、有効な証明書を設定していないか、正しくない証明書を設定していることを示します。

デフォルトの設定

表 12-5　InvalidCertificate アラートのデフォルトの設定

値	デフォルトの設定
[アラートの有効化 (Enable Alert)]	選択済み
[重大度 (Severity)]	[アラート (Alert)]
[次のサーバでのこのアラートの有効/無効 :(Enable/Disable this alert on the following server(s))]	リストされたサーバで有効化
[しきい値 (Threshold)]	次の条件が満たされた場合にアラートをトリガーする。 無効な証明書が設定された。
[接続時間 (Duration)]	アラートをただちにトリガーする。
[頻度 (Frequency)]	すべてのポーリングでアラートをトリガーする。
[スケジュール (Schedule)]	毎日 24 時間
[電子メールの有効化 (Enable Email)]	選択済み
[アラートのトリガーアクション :(Trigger Alert Action:)]	[デフォルト (Default)]

InvalidCredentials

このアラートは、Cisco Unified Communications Manager 上に設定されているユーザ名およびパスワードが、Cisco IME サーバ上に設定されているユーザ名およびパスワードと一致していないために、Cisco Unified Communications Manager が Cisco IME サーバに接続できないことを示します。

このアラートには、Cisco IME サーバに接続するために使用されたユーザ名とパスワードが含まれ、さらにターゲット Cisco IME サーバの IP アドレスと名前も含まれます。このアラートを解決するには、Cisco IME サーバにログインし、設定されているユーザ名およびパスワードが、Cisco Unified Communications Manager に設定されているユーザ名およびパスワードと一致していることを確認します。

デフォルトの設定

表 12-6　InvalidCredentials アラートのデフォルト設定

値	デフォルトの設定
[アラートの有効化 (Enable Alert)]	選択済み
[重大度 (Severity)]	[エラー (Error)]
[次のサーバでのこのアラートの有効/無効 :(Enable/Disable this alert on the following server(s))]	リストされたサーバで有効化
[しきい値 (Threshold)]	次の条件が満たされた場合にアラートをトリガーする。 信用証明書が無効か、一致していない。
[接続時間 (Duration)]	アラートをただちにトリガーする。
[頻度 (Frequency)]	すべてのポーリングでアラートをトリガーする。
[スケジュール (Schedule)]	毎日 24 時間
[電子メールの有効化 (Enable Email)]	選択済み
[アラートのトリガーアクション :(Trigger Alert Action:)]	[デフォルト (Default)]

MessageOfTheDay

Cisco IME サービスは、Cisco IME ネットワークの管理者からのメッセージがある場合に、このアラートを生成します。

デフォルトの設定

表 12-7　MessageOfTheDay アラートのデフォルトの設定

値	デフォルトの設定
[アラートの有効化 (Enable Alert)]	選択済み
[重大度 (Severity)]	[通知 (Notice)]
[次のサーバでのこのアラートの有効/無効 :(Enable/Disable this alert on the following server(s))]	リストされたサーバで有効化

表 12-7　MessageOfTheDay アラートのデフォルトの設定 （続き）

値	デフォルトの設定
[しきい値 (Threshold)]	次の条件が満たされた場合にアラートをトリガーする。 ネットワーク管理者からのメッセージ
[接続時間 (Duration)]	アラートをただちにトリガーする。
[頻度 (Frequency)]	1440 分以内に最大 1 個のアラートをトリガーする
[スケジュール (Schedule)]	毎日 24 時間
[電子メールの有効化 (Enable Email)]	選択済み
[アラートのトリガーアクション :(Trigger Alert Action:)]	[デフォルト (Default)]

SWUpdateRequired

Cisco IME サーバは、Cisco IME サーバ ソフトウェアの新バージョンが必要な場合に、このアラートを生成します。このアラートは、アップグレードを実行するまで繰り返されます。ソフトウェア アップデートの詳細については、Cisco Web サイトを参照してください。このアラートを受け取ってから数日以内に重要なアップデートをインストールする必要があります。

このアップグレードは、セキュリティ上の脆弱性や重要な機能の障害に対処するものです。重要なアップグレードをすぐに適用しないと、Cisco IME サーバがネットワークに接続できなくなることがあります。

デフォルトの設定

表 12-8　SWUpdateRequired アラートのデフォルト設定

値	デフォルトの設定
[アラートの有効化 (Enable Alert)]	選択済み
[重大度 (Severity)]	[警告 (Warning)]
[次のサーバでのこのアラートの有効/無効 :(Enable/Disable this alert on the following server(s))]	リストされたサーバで有効化
[しきい値 (Threshold)]	次の条件が満たされた場合にアラートをトリガーする。 ソフトウェアのアップデートが必要
[接続時間 (Duration)]	アラートをただちにトリガーする。
[頻度 (Frequency)]	60 分以内に最大 1 個のアラートをトリガーする

表 12-8　SWUpdateRequired アラートのデフォルト設定 （続き）

値	デフォルトの設定
[スケジュール (Schedule)]	毎日 24 時間
[電子メールの有効化 (Enable Email)]	選択済み
[アラートのトリガーアクション :(Trigger Alert Action:)]	[デフォルト (Default)]

TicketPasswordChanged

Cisco IME サーバは、認証チケットの生成に使用されるパスワードを管理者が変更する場合に、このアラートを生成します。

権限のある管理者によるパスワードの変更であることを確認してください。無許可で変更されている場合は、Cisco IME サービス上の管理インターフェイスのセキュリティが破られていることを示している場合があります。無許可で変更されたと判断した場合は、Cisco IME サーバ上の管理パスワードをすぐに変更して、さらなる不正アクセスを防ぐ必要があります。管理パスワードを変更するには、Cisco IME サーバ CLI で **set password admin** と入力します。

デフォルトの設定

表 12-9　TicketPasswordChanged アラートのデフォルトの設定

値	デフォルトの設定
[アラートの有効化 (Enable Alert)]	選択済み
[重大度 (Severity)]	[通知 (Notice)]
[次のサーバでのこのアラートの有効/無効 :(Enable/Disable this alert on the following server(s))]	リストされたサーバで有効化
[しきい値 (Threshold)]	次の条件が満たされた場合にアラートをトリガーする。 チケットのパスワードが変更された。
[接続時間 (Duration)]	アラートをただちにトリガーする。
[頻度 (Frequency)]	ポーリングごとにトリガーする。
[スケジュール (Schedule)]	毎日 24 時間

表 12-9　TicketPasswordChanged アラートのデフォルトの設定 （続き）

値	デフォルトの設定
[電子メールの有効化 (Enable Email)]	選択済み
[アラートのトリガーアクション :(Trigger Alert Action:)]	[デフォルト (Default)]

ValidationsPendingExceeded

このアラートは、Cisco IME サーバ上の保留中の検証の数を示します。この数は、Cisco IME サーバ上の未処理作業のインジケータになります。

デフォルトの設定

表 12-10　ValidationsPendingExceeded アラートのデフォルトの設定

値	デフォルトの設定
[アラートの有効化 (Enable Alert)]	選択済み
[重大度 (Severity)]	[重要 (Critical)]
[次のサーバでのこのアラートの有効/無効 :(Enable/Disable this alert on the following server(s))]	リストされたサーバで有効化
[しきい値 (Threshold)]	次の条件が満たされた場合にアラートをトリガーする。 Cisco IME の保留中の検証が 100 件を超えている。
[接続時間 (Duration)]	アラートをただちにトリガーする。
[頻度 (Frequency)]	60 分以内に最大 1 個のアラートをトリガーする
[スケジュール (Schedule)]	毎日 24 時間
[電子メールの有効化 (Enable Email)]	選択済み
[アラートのトリガーアクション :(Trigger Alert Action:)]	[デフォルト (Default)]

IMEDistributedCacheInactive

Cisco Unified Communications Manager が Cisco IME サーバに接続試行した一方で、IME 分散キャッシュが現在アクティブでない場合、このアラームが生成されます。

CLI を使用して、Cisco IME サーバの証明書がプロビジョニングされていること、および IME 分散キャッシュがアクティブ化されていることを確認してください。

デフォルトの設定

表 12-11　IMEDistributedCacheInactive アラートのデフォルト設定

値	デフォルトの設定
[アラートの有効化 (Enable Alert)]	選択済み
[重大度 (Severity)]	[エラー (Error)]
[次のサーバでのこのアラートの有効/無効 :(Enable/Disable this alert on the following server(s))]	リストされたサーバで有効化
[しきい値 (Threshold)]	次の条件が満たされた場合にアラートをトリガーする。 IME 分散キャッシュが非アクティブ
[接続時間 (Duration)]	アラートをただちにトリガーする。
[頻度 (Frequency)]	すべてのポーリングでアラートをトリガーする。
[スケジュール (Schedule)]	毎日 24 時間
[電子メールの有効化 (Enable Email)]	選択済み
[アラートのトリガーアクション :(Trigger Alert Action:)]	[デフォルト (Default)]

IMEOverQuota

このアラートは、この Cisco IME サービスを使用する Cisco Unified Communications Manager サーバが、IME 分散キャッシュに発行された Direct Inward Dialing（DID; ダイヤル イン）番号のクォータを超過したことを示します。このアラートには、Cisco IME サーバの名前と、現在のクォータ値およびターゲット クォータ値が含まれます。

この Cisco IME サービスを使用するすべての Cisco Unified Communications Manager サーバに DID プレフィックスを正しくプロビジョニングしたことを確認します。

プレフィックスを正しくプロビジョニングし、Cisco IME サービスのキャパシティを超過した場合、別のサービスを設定し、各 Cisco IME サービスの Cisco IME クライアント インスタンス（Cisco Unified Communications Manager）間で DID プレフィックスを分け合う必要があります。

デフォルトの設定

表 12-12　IMEOverQuota アラートのデフォルト設定

値	デフォルトの設定
[アラートの有効化 (Enable Alert)]	選択済み
[重大度 (Severity)]	[アラート (Alert)]
[次のサーバでのこのアラートの有効/無効 :(Enable/Disable this alert on the following server(s))]	リストされたサーバで有効化
[しきい値 (Threshold)]	次の条件が満たされた場合にアラートをトリガーする。 VAP over クォータ
[接続時間 (Duration)]	アラートをただちにトリガーする。
[頻度 (Frequency)]	すべてのポーリングでアラートをトリガーする。
[スケジュール (Schedule)]	毎日 24 時間
[電子メールの有効化 (Enable Email)]	選択済み
[アラートのトリガーアクション :(Trigger Alert Action:)]	[デフォルト (Default)]

IMEQualityAlert

IP ネットワークの品質の問題により、相当数の Cisco IME コールが PSTN にフォールバックしたこと、または確立されなかったことを Cisco Unified Communications Manager が検出した場合、このアラートが生成されます。次の 2 つのタイプのイベントがこのアラートをトリガーします。

- 現在アクティブな多数の Cisco IME コールが、すべて PSTN へのフォールバックを要求した、または PSTN にフォールバックした。
- 最近のコール試行の多くが PSTN に移行し、IP で行われなかった。

このアラートを受信した場合、IP 接続を確認します。IP 接続に問題がない場合、コールが PSTN にフォールバックした原因、またはコールが IP を介して実行されなかった原因を特定するために、場合により、ファイアウォールの CDR、CMR、およびログを確認する必要があります。

デフォルトの設定

表 12-13　IMEQualityAlert アラートのデフォルト設定

値	デフォルトの設定
[アラートの有効化 (Enable Alert)]	選択済み
[重大度 (Severity)]	[エラー (Error)]
[次のサーバでのこのアラートの有効/無効 :(Enable/Disable this alert on the following server(s))]	リストされたサーバで有効化
[しきい値 (Threshold)]	次の条件が満たされた場合にアラートをトリガーする。 Cisco IME のリンク品質に問題がある。
[接続時間 (Duration)]	アラートをただちにトリガーする。
[頻度 (Frequency)]	すべてのポーリングでアラートをトリガーする。
[スケジュール (Schedule)]	毎日 24 時間
[電子メールの有効化 (Enable Email)]	選択済み
[アラートのトリガーアクション :(Trigger Alert Action:)]	[デフォルト (Default)]

InsufficientFallbackIdentifiers

現在進行中の多数の Cisco IME コールが同じフォールバック DID を使用していて、Cisco Unified Communications Manager が処理する新しい Cisco IME コールに割り当てる DTMF ディジット シーケンスがこれ以上存在しない場合、このアラートが生成されます。新しいコールは続行されますが、音声品質が悪化しても、コールは PSTN にフォールバックできません。

このアラートが生成された場合、このコールに関連するフォールバック プロファイルを確認します。Cisco Unified Communications Manager の管理 でこのプロファイルを確認し、[関連 DTFM ディジットのフォールバック数 (Fallback Number Of DTMF Correlation Digits)] フィールドの現在の設定を調べます。このフィールドの値を 1 増やし、その新しい値で、これらのアラートが生成されなくなるかどうか確認します。10 をこのパラメータ値で累乗した数が、このプロファイルに関連する登録番号に対して行われる同時 Cisco IME コールの数よりも常に大幅に大きくなるように、通常、このパラメータには十分大きい値を設定する必要があります。たとえば、このフォールバック プロファイルに関連するパターンに対し 10,000 未満の同時 Cisco IME コールが常にある場合、この値を 5 に設定すると（10 の 5 乗で 100,000）、Cisco Unified Communications Manager はこのアラートを生成しなくなります。

ただし、この値を増やすと、フォールバックの実行にかかる時間がわずかに増えます。したがって、このアラートが生成されないようにするために、[関連 DTFM ディジットのフォールバック数 (Fallback Number Of DTMF Correlation Digits)] フィールドは十分大きい値に設定する必要があります。

DTMF ディジット フィールドの値を増やす代わりに、異なるフォールバック DID を使用する別のフォールバック プロファイルを追加し、そのフォールバック プロファイルをより少数の登録パターンに関連付けることもできます。この方法を使用する場合、より少数のディジットを使用できます。

デフォルトの設定

表 12-14　InsufficientFallbackIdentifiers アラートのデフォルト設定

値	デフォルトの設定
[アラートの有効化 (Enable Alert)]	選択済み
[重大度 (Severity)]	[エラー (Error)]
[次のサーバでのこのアラートの有効/無効 :(Enable/Disable this alert on the following server(s))]	リストされたサーバで有効化
[しきい値 (Threshold)]	次の条件が満たされた場合にアラートをトリガーする。 フォールバック ID を割り当てることができない。
[接続時間 (Duration)]	アラートをただちにトリガーする。
[頻度 (Frequency)]	1 分内に最大 1 つのアラートをトリガーする。
[スケジュール (Schedule)]	毎日 24 時間
[電子メールの有効化 (Enable Email)]	選択済み
[アラートのトリガーアクション :(Trigger Alert Action:)]	[デフォルト (Default)]

IMEServiceStatus

このアラートは、特定の Cisco IME クライアント インスタンス（Cisco Unified Communications Manager）に対する Cisco IME サービスへの接続の全般的な正常性を示します。このアラートは次の状態を示します。

- 0：不明。多くの場合、Cisco IME サービスがアクティブでないことを示します。
- 1：正常。Cisco Unified Communications Manager が、Cisco IME クライアント インスタンス用のプライマリ サーバおよびバックアップ サーバ（設定されている場合）への接続を正常に確立したことを示します。
- 2：正常でない。Cisco IME はアクティブですが、Cisco IME サーバとのハンドシェイク手順は正常に完了していません。このカウンタは、プライマリおよびセカンダリの両方の IME サーバのハンドシェイク ステータスを反映していることに注意してください。

デフォルトの設定

表 12-15　IMEServiceStatus アラートのデフォルト設定

値	デフォルトの設定
[アラートの有効化 (Enable Alert)]	選択済み
[重大度 (Severity)]	[重要 (Critical)]
[次のサーバでのこのアラートの有効/無効 :(Enable/Disable this alert on the following server(s))]	リストされたサーバで有効化
[しきい値 (Threshold)]	次の条件が満たされた場合にアラートをトリガーする。 VAP 接続の問題
[接続時間 (Duration)]	アラートをただちにトリガーする。
[頻度 (Frequency)]	60 分ごとに最大 1 つのアラートをトリガーする。
[スケジュール (Schedule)]	毎日 24 時間
[電子メールの有効化 (Enable Email)]	選択済み
[アラートのトリガーアクション :(Trigger Alert Action:)]	[デフォルト (Default)]

InvalidCredentials

このアラートは、Cisco Unified Communications Manager で設定されているユーザ名、パスワード、またはその両方が、Cisco IME サーバで設定されているユーザ名、パスワード、またはその両方に一致しないために、Cisco Unified Communications Manager が Cisco IME サーバに接続できないことを示します。

このアラートには、Cisco IME サーバに接続するために使用されたユーザ名とパスワードが含まれ、さらにターゲット Cisco IME サーバの IP アドレスと名前も含まれます。このアラートを解決するには、Cisco IME サーバにログインし、設定済みのユーザ名およびパスワードが、Cisco Unified Communications Manager で設定されているユーザ名およびパスワードと一致しているか確認します。

デフォルトの設定

表 12-16　InvalidCredentials アラートのデフォルト設定

値	デフォルトの設定
[アラートの有効化 (Enable Alert)]	選択済み
[重大度 (Severity)]	[アラート (Alert)]
[次のサーバでのこのアラートの有効/無効 :(Enable/Disable this alert on the following server(s))]	リストされたサーバで有効化
[しきい値 (Threshold)]	次の条件が満たされた場合にアラートをトリガーする。 Cisco IME サーバに対するクレデンシャルの失敗
[接続時間 (Duration)]	アラートをただちにトリガーする。
[頻度 (Frequency)]	すべてのポーリングでアラートをトリガーする。
[スケジュール (Schedule)]	毎日 24 時間
[電子メールの有効化 (Enable Email)]	選択済み
[アラートのトリガーアクション :(Trigger Alert Action:)]	[デフォルト (Default)]

TCPSetupToIMEFailed

このアラートは、Cisco Unified Communications Manager が Cisco IME サーバとの TCP 接続を確立できない場合に生成されます。このアラートは、Cisco IME サーバの IP アドレスおよびポートが Cisco Unified Communications Manager の管理 で誤って設定されている場合、またはイントラネットの接続の問題が存在し、それにより接続が確立できない場合に通常生成されます。

アラート内の Cisco IME サーバの IP アドレスとポートが有効であることを確認します。問題が引き続き発生する場合、Cisco Unified Communications Manager サーバと Cisco IME サーバの間の接続をテストします。

デフォルトの設定

表 12-17　TCPSetupToIMEFailed アラートのデフォルト設定

値	デフォルトの設定
[アラートの有効化 (Enable Alert)]	選択済み
[重大度 (Severity)]	[重要 (Critical)]
[次のサーバでのこのアラートの有効/無効 :(Enable/Disable this alert on the following server(s))]	リストされたサーバで有効化
[しきい値 (Threshold)]	次の条件が満たされた場合にアラートをトリガーする。 Cisco IME サーバへの接続の失敗
[接続時間 (Duration)]	アラートをただちにトリガーする。
[頻度 (Frequency)]	すべてのポーリングでアラートをトリガーする。
[スケジュール (Schedule)]	毎日 24 時間
[電子メールの有効化 (Enable Email)]	選択済み
[アラートのトリガーアクション :(Trigger Alert Action:)]	[デフォルト (Default)]

TLSConnectionToIMEFailed

このアラートは、Cisco IME サービスが提示した証明書の有効期限が切れたか、Cisco Unified Communications Manager CTL に存在しないために、Cisco IME サービスへの TLS 接続を確立できなかった場合に出されます。

Cisco IME サービスの証明書が Cisco Unified Communications Manager に設定されていることを確認してください。

デフォルトの設定

表 12-18　TLSConnectionToIMEFailed アラートのデフォルト設定

値	デフォルトの設定
[アラートの有効化 (Enable Alert)]	選択済み
[重大度 (Severity)]	[アラート (Alert)]
[次のサーバでのこのアラートの有効/無効 :(Enable/Disable this alert on the following server(s))]	リストされたサーバで有効化
[しきい値 (Threshold)]	次の条件が満たされた場合にアラートをトリガーする。 Cisco IME サービスへの TLS の失敗
[接続時間 (Duration)]	アラートをただちにトリガーする。
[頻度 (Frequency)]	すべてのポーリングでアラートをトリガーする。
[スケジュール (Schedule)]	毎日 24 時間
[電子メールの有効化 (Enable Email)]	選択済み
[アラートのトリガーアクション :(Trigger Alert Action:)]	[デフォルト (Default)]

関連項目

- 「Cisco Unified Communications Manager の管理での Cisco IME の設定」（P.3-1）
- 「Cisco Intercompany Media Engine での RTMT の使用」（P.7-1）
- 『*Cisco Unified Real Time Monitoring Tool Administration Guide*』

関連項目

INDEX

M

N

P

S

V

あ

い

お

か

き

さ

し

つ

と

ね

は

ふ

ほ

ら

り