Cisco Video/TelePresence アーキテクチャ デザイン ガイド

2012 年 3 月 30 日

Text Part Number: OL-27011-01-J

【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 Video/TelePresence アーキテクチャ デザイン ガイド

CONTENTS

はじめに

このマニュアルは、ビデオ コミュニケーションに関連するいくつかの概念について説明したものです。ビデオ対応ネットワークの設計に関する考慮事項やガイドラインについても記載されています。

このマニュアルは、次の Web サイトから入手できる他のマニュアルとあわせてお読みください。

- シスコのコラボレーションおよびユニファイド コミュニケーションのシステム設計マニュアル：
  http://www.cisco.com/go/ucsrnd
- その他のシスコ設計ガイド：
  http://www.cisco.com/go/designzone
- シスコのテレプレゼンスおよびビデオの製品マニュアル：
  http://www.cisco.com

マニュアルの変更履歴

このマニュアルは、予告なしに更新されることがあります。このマニュアルの最新バージョンは、次の URL から入手できます。

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

この Cisco.com の Web サイトを定期的に参照し、お手元のマニュアルの改訂日と Web サイトにあるマニュアルの改訂日とを比較して、内容が更新されていないかどうかを確認してください。

次の表は、このマニュアルの改訂履歴を示したものです。

改訂日	マニュアル部品番号	コメント
2012 年 3 月 30 日	OL-27011-01-J	このマニュアルの最初のバージョン。

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記載されています。

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。

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	用途
太字フォント	コマンド、キーワード、およびユーザが入力したテキストは、**太字**フォントで示しています。
*イタリック体*フォント	ドキュメント名、新規用語または強調する用語、値を指定するための引数は、*イタリック体*フォントで示しています。
[ ]	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。
string	引用符を付けない一組の文字。string 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 string とみなされます。
`courier` フォント	システムが表示するターミナル セッションおよび情報は、`courier` フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注） 「*注釈*」です。

ヒント 「*問題解決に役立つ情報*」です。

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。

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。

警告 **「*警告*」の意味です。人為ミスを予防するための注意事項が記述されています。**

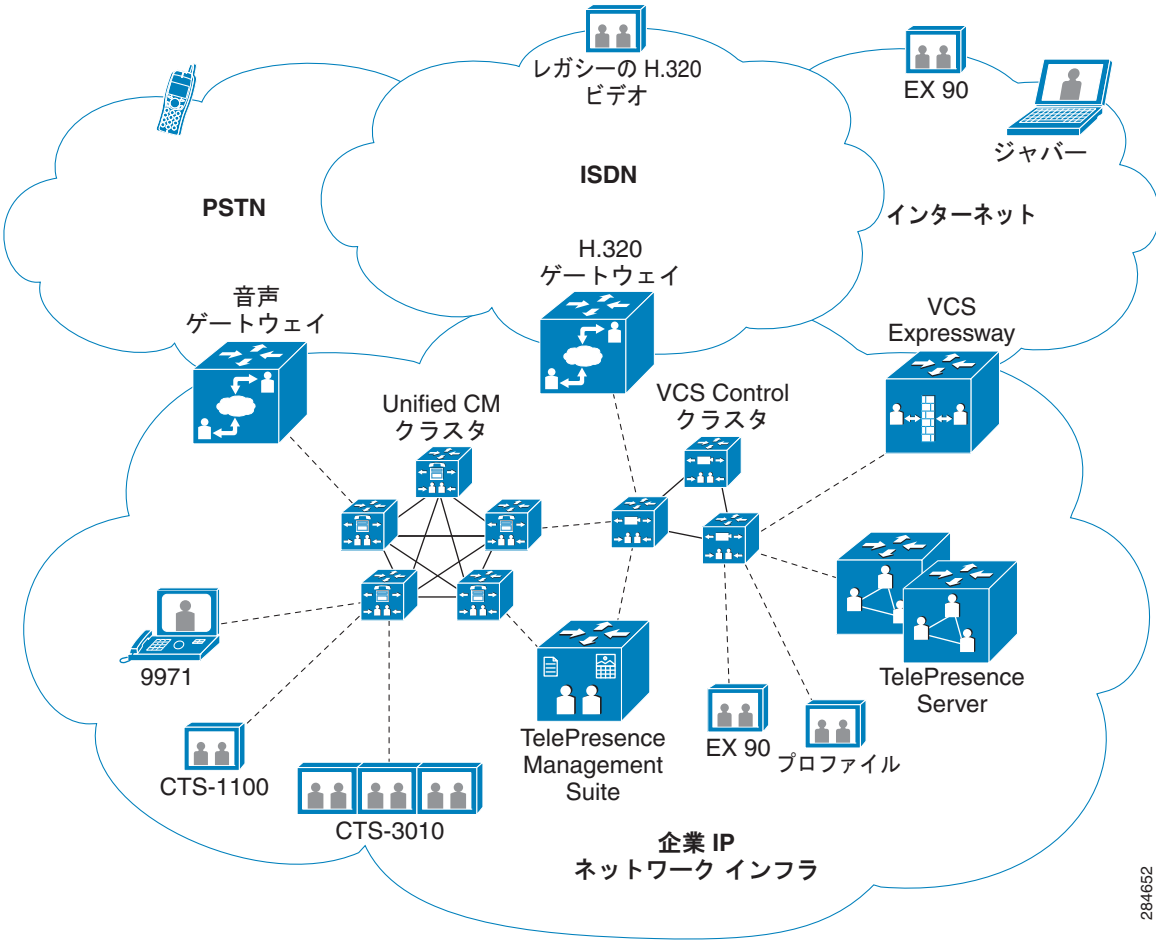
CHAPTER 1

概要

このマニュアルは、Cisco TelePresence や Cisco Unified Communications など、シスコが提供する双方向のインタラクティブ ビデオ ソリューションを中心に解説したものです。ソリューション全体の概要やテクノロジー コンポーネント、導入に際しての考慮事項などについて説明します。シスコは、TelePresence および Unified Communications の製品群を通じて、大会議場用のインタラクティブ ビデオ アプリケーションからモバイル ユーザ用のインタラクティブ ビデオ アプリケーションまで、多岐に渡るビデオ ソリューションを提供しています。またこのマニュアルでは扱いませんが、ストリーミング ビデオ、デジタル サイネージ、メディア変換などの単方向ビデオ アプリケーションについても幅広く用意しています。

Cisco TelePresence および Cisco Unified Communications のソリューションは、それぞれをスタンドアロン ソリューションとして導入することができるほか、複数を統合ソリューションとして導入することもできます。図 1-1 は、TelePresence および Unified Communications のビデオ エンドポイントを共にサポートしたビデオ アーキテクチャの例を図示したものです。この例では、ボイスコール用の PSTN、レガシー ビデオ用の ISDN、およびインターネットベースのビデオ デバイスにアクセスする経路も示されています。

図 1-1　Cisco TelePresence および Cisco Unified Communications のビデオ アーキテクチャ



このアーキテクチャには、表 1-1 に記載されているエンドポイント、および表 1-2 に記載されているインフラストラクチャ コンポーネントが組み込まれます。

表 1-1　現在の Cisco TelePresence および Cisco Unified Communications のビデオ エンドポイント

カテゴリ	エンドポイント
TelePresence：イマーシブ	TX9000 シリーズ CTS 3000 シリーズ CTS T シリーズ TX1300 シリーズ
TelePresence：多目的	CTS MX シリーズ CTS Profile MXP シリーズ CTS Profile シリーズ
TelePresence：デスクトップ	CTS EX シリーズ CTS MXP シリーズ
TelePresence：オフィス	CTS 1100 CTS 500
TelePresence：パーソナル	Cisco Jabber Video for TelePresence（Movi）
TelePresence：ビデオ電話	CTS E20
Unified Communications：ビデオ電話	Cisco Unified IP Phones 9900 シリーズ
Unified Communications：デスクトップ	Cisco Unified Personal Communicator Cisco Jabber
Unified Communications：タブレット	Cius

表 1-2　シスコのビデオ インフラストラクチャ製品

目的	製品名	製品カテゴリ	説明
コール制御	Cisco Unified Communications Manager	テレプレゼンスおよびユニファイド コミュニケーション	ユニファイド コミュニケーション デバイスおよびテレプレゼンス デバイスのコール制御
	Cisco TelePresence Video Communications Server	制御	テレプレゼンス デバイスおよびビデオ会議デバイスのコール制御
会議	Cisco Integrated Services Router G2 Conferencing Services	ユニファイド コミュニケーション	3 スクリーン イマーシブを除くすべてのビデオ エンドポイントに対応したマルチポイント会議
	Cisco TelePresence Server	テレプレゼンス	3 スクリーン イマーシブを含むすべてのビデオ エンドポイントに対応したマルチポイント コントロール ユニット
	Cisco TelePresence Conductor	テレプレゼンス	マルチポイント デバイス管理用のポリシー サーバ
	Cisco TelePresence Multipoint Control Unit	テレプレゼンス	3 スクリーン イマーシブを除くすべてのビデオ エンドポイントに対応したマルチポイント コントロール ユニット
	Cisco TelePresence Multipoint Switch	テレプレゼンス	CTS シリーズ、EX シリーズ、および Profile シリーズのビデオ エンドポイントに対応したマルチポイント スイッチ
ゲートウェイ	ISDN Gateway	テレプレゼンス	H.323 ビデオ エンドポイントおよび SIP ビデオ エンドポイントから ISDN H.320 エンドポイントへの接続を可能にするビデオ ゲートウェイ
	Advanced Media Gateway	テレプレゼンス	標準の H.323 ビデオ エンドポイントおよび SIP ビデオ エンドポイントから Microsoft Lync デバイスおよび Microsoft Office Communicator デバイスへの接続を可能にするゲートウェイ
	Cisco Telepresence Video Communications Server Expressway	テレプレゼンス	SIP および H.323 のビデオ エンドポイント間におけるセキュアな通信をインターネット経由で実現するためのゲートウェイ
	Cisco Unified Border Element	テレプレゼンス	IP ネットワーク間のセキュアな境界を実現するためのゲートウェイ
	Cisco Intercompany Media Engine	ユニファイド コミュニケーション	Unified CM および ASA ファイアウォールの併用時に企業間接続を実現するためのゲートウェイ
録画とストリーミング	Cisco TelePresence コンテンツ サーバ	テレプレゼンス	すべてのビデオ エンドポイントに対応した録画とストリーミング
	Cisco TelePresence Recording Server	テレプレゼンス	CTS シリーズのビデオ エンドポイントに対応した録画サーバ
管理	Cisco TelePresence Manager	テレプレゼンス	シスコおよびサードパーティのビデオ エンドポイントに対応したスケジューリング/管理プラットフォーム
	Cisco TelePresence Management Suite	テレプレゼンス	シスコおよびサードパーティのビデオ エンドポイントに対応したスケジューリング/管理プラットフォーム
	Cisco Prime Collaboration Manager	テレプレゼンス	メディア フロー用のネットワークおよびエンドポイントの管理

Cisco TelePresence および Cisco Unified Communications には、お客様の複雑な要件に可能な限り対応できるよう、多種多様なビデオ エンドポイントやインフラストラクチャ コンポーネントが用意されています。ただ、多種多様であるがゆえに、どのソリューションが適切なのか選択に苦慮することも考えられます。

このマニュアル全体を通して言及されているように、Cisco TelePresence および Cisco Unified Communications のエンドポイントおよびインフラストラクチャ コンポーネントは、使用されるプロトコル、音声コーデック、およびビデオ コーデックが共通しており、導入に際しての考慮事項もほぼ同じです。このマニュアルでは、Cisco TelePresence および Cisco Unified Communications に関連のある次の各項目について詳しく解説します。

- ビデオ コンポーネント

  ビデオ コンポーネントは、ビデオ エンドポイント、コール制御、会議、ゲートウェイ、および管理プラットフォームで構成されます。

- ビデオ ソリューションの基本的な概念と用語

  一般にテレプレゼンスおよびビデオに関しては、他のテクノロジーには見られない目新しい用語や概念が多数登場します。わずかここ数年の間に、ビデオ エンドポイントや会議デバイス、エラー隠蔽技術の進歩に伴って、新しい製品や機能が数多く開発されています。

- コール制御プロトコル

  コール制御プロトコルは、ネットワーク上のメディア フローに関する設定や処理を行うためのものです。さまざまなネットワーク メディアを介してインタラクティブ ビデオを転送する際には、数多くのビデオ コール制御プロトコルが使用されます。

- QoS（Quality of Service）とコール アドミッション制御

  インタラクティブ ビデオは、遅延、損失、およびジッターの影響を大きく受けます。ビデオを適正に導入するうえで重要なポイントは、帯域幅が利用可能な場合に限ってネットワークに対するアドミッションを許可すること、およびサービス内容合意書（SLA）の内容に適合するメディア フローを保証することにあります。

- ダイヤル プラン

  ダイヤル プランは、インターネットおよび PSTN を経由した企業間ビデオ コールや、PSTN 音声専用コールなど、ビデオ デバイスと企業の外部にあるデバイスとの間のコール ルーティングを実現するためのものです。高度な機能群のサポートやエンドポイントのアドレス指定をどのような方法で行うかによっては、ダイヤル プランに十分な配慮が必要です。

- 導入シナリオ

  インタラクティブ ビデオの導入に関しては豊富な導入シナリオが用意されています。導入シナリオは、エンド ポイントの数やタイプなどさまざまな要素に基づいており、コール制御、ビデオ サービス、およびネットワーク設計のあらゆる面が考慮されています。

- Business-to-Business（B2B）

  ビデオを導入し使用する企業が増加しているのに伴って、Business-to-Business（B2B）ビデオ コミュニケーションの重要性はますます高まっています。Business-to-Business（B2B）ビデオ コミュニケーションを実現する方法は、各企業で使用するコール制御プラットフォームやエンドポイントによってさまざまです。

- 会議

  会議システムでは、1 件の会議につき 2 つ以上のデバイス間で通信を行うことができます。会議を開始する際にはさまざまなオプションを使用することが可能で、会議ビデオ ポイントに利用できるプラットフォームも幅広く用意されています。

- セキュリティ

  ビデオ コールのセキュリティは、Business-to-Business（B2B）コミュニケーションにビデオを使用している企業をはじめ多くの企業にとって必須事項です。シグナリング トラフィックやメディアを暗号化する方法にはさまざまな種類があり、セキュアなビデオ コミュニケーションを導入する際に考慮すべき要素も多岐に渡ります。

このマニュアルのほかにも、設計および導入に関するガイドが数多く用意されているため、それらを参考にすれば適切なアーキテクチャを選択することができます。これらのガイドには、ビデオ アーキテクチャに関する情報だけでなく、ネットワーク上のビデオ コールを適切に処理できるようにネットワーク要件についても記載されています。次の設計ガイドおよび導入ガイドには、Cisco TelePresence および Cisco Unified Communications のビデオの導入に関する情報が記載されています。

- 『Cisco Unified Communications System SRND』

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

- 『Cisco TelePresence Network Systems Design Guide』

  http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns819/landing_vid_tPresence.html

CHAPTER 2

ビデオ インフラストラクチャ コンポーネント

企業の間で、出張の削減や生産性の向上、ユニファイド コミュニケーション プラットフォームによるビデオの拡張が重要視されるのに伴い、ビデオを導入する動きはさらに広がりを見せています。ユニファイド コミュニケーションの市場とテレプレゼンスの市場は、成長し成熟するにつれて、その境界線が曖昧になってきています。テレプレゼンスのビデオ デバイスとユニファイド コミュニケーションのビデオ デバイスは、互いに共通のプロトコルやコーデックが数多く採用されているため、完全な統合が可能であり、どちらのソリューションのインフラストラクチャ デバイスでも利用することができます。

Cisco TelePresence ソリューションおよび Cisco Unified Communications ソリューションはどちらも、シスコの自社開発と戦略的買収によって劇的に拡大しました。

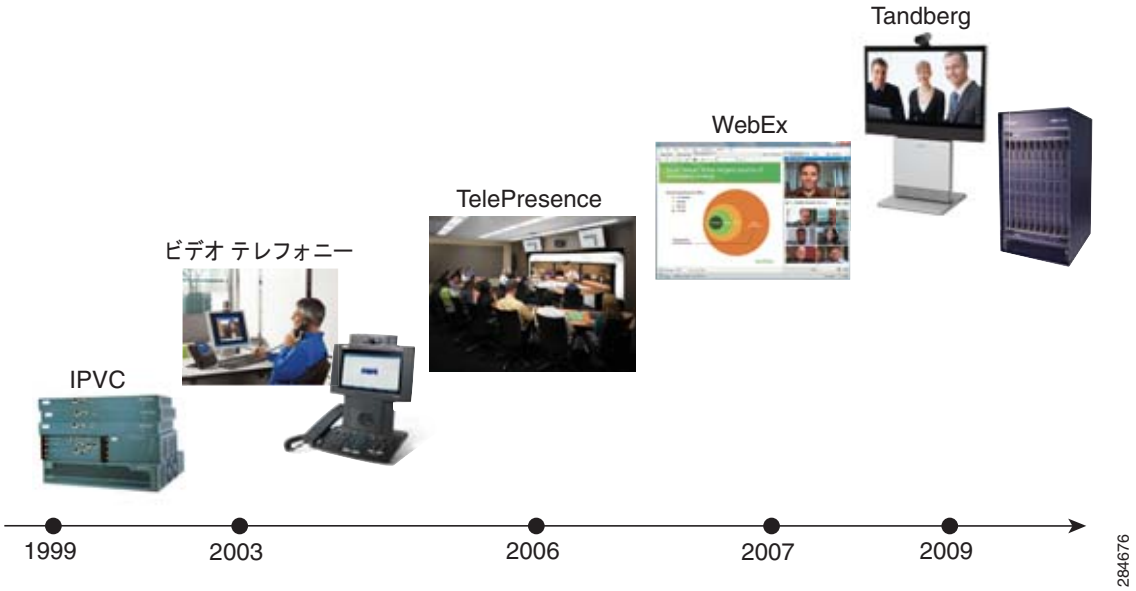
Cisco TelePresence および Cisco Unified Communications

シスコは 1999 年の暮れ、OEM 関係を結ぶ Radvision 社を介して、双方向インタラクティブ ビデオの分野に初めて参入しました。Radvision 社との OEM 関係を通じて市場に投入されたシスコ名義のビデオ会議インフラストラクチャ製品は、Cisco IPVC マルチポイント コントロール ユニット（MCU）や Cisco IPVC ゲートウェイなど、多数に上ります。その数年後、シスコは自社の音声コール制御エージェントである Cisco Unified Communications Manager（Unified CM）に対するサポートを開始するとともに、ビデオの応用範囲を PC ベースのソフト クライアントやビデオ電話にまで広げたビデオ テレフォニー製品を数多く発売しました。

2006 年暮れには、Cisco TelePresence が初めて発表され、エンドポイント、マルチポイント スイッチ、TelePresence 管理、録画サーバなど一連の高品位（HD）会議製品が登場します。Cisco TelePresence の発表とともにビデオ会議システムの市場は活気を取り戻し、HD がその標準となりました。

シスコは 2007 年、WebEx 社を買収したことで、新しいビデオ ソフト クライアントなど、さらなるユニファイド コミュニケーション製品をポートフォリオに追加しました。シスコは、2009 年になってようやく Tandberg 社を買収します。買収当時 Tandberg 社は、業界屈指の充実度を誇る製品ラインを武器に、ビデオ会議システム市場の先頭に立っていました。その Tandberg 社の製品と Cisco TelePresence とを組み合わせることで、シスコは短期間のうちにデスクトップ用から会議室用まで最高のテレプレゼンス製品を提供できるようになりました。図 2-1 は、シスコの製品ポートフォリオにおけるインタラクティブ ビデオの変遷を示したものです。

図 2-1　シスコの双方向インタラクティブ ビデオ製品の変遷



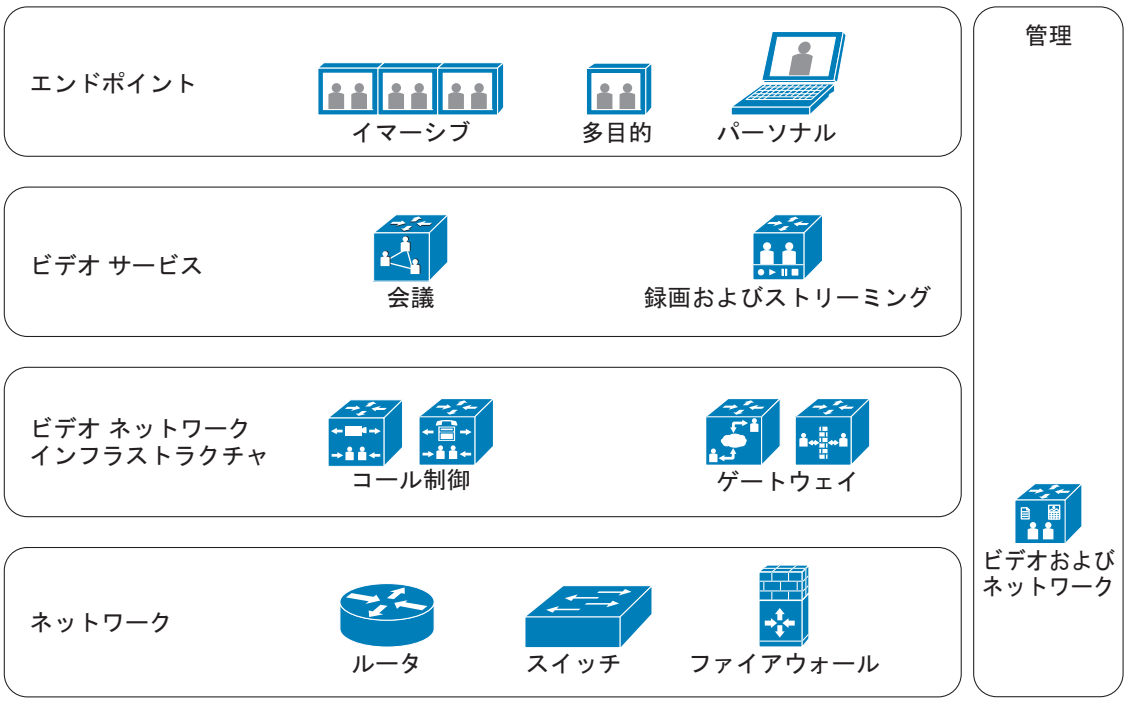
ビデオ アーキテクチャ

インタラクティブ ビデオ アーキテクチャはいずれも、図 2-2 に示した 5 つのカテゴリで構成されています。

- 「エンドポイント」（P.2-3）
- 「ビデオ サービス」（P.2-4）
- 「ビデオ ネットワーク サービス」（P.2-6）
- 「管理」（P.2-8）
- 「ネットワーク」（P.2-9）

各カテゴリには、ビデオの導入にあたって特定の機能を担うデバイスが含まれますが、ビデオを導入する際は常にすべてのカテゴリのデバイスが必要となるわけではなく、使用されるわけでもありません。

図 2-2　ビデオ アーキテクチャ



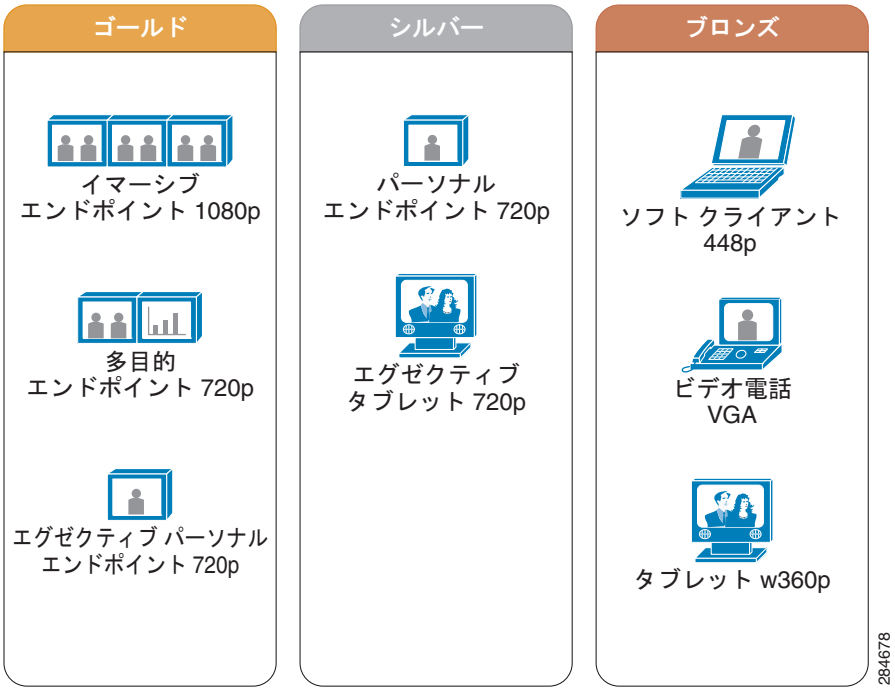
エンドポイント

各エンドポイントは、スクリーン、マイク、スピーカー、およびコーデックというビデオと音声を処理するデバイスで構成されます。通常これらの構成要素は、スクリーン付き電話（基本的なエンドポイント）、大型テレビまたはそれに準ずるデバイス、テーブル/座席一体型のイマーシブ マルチスクリーン システムなど、1 つのユニットにまとめて組み込まれます。シスコは、ビデオ対応タブレットからマルチスクリーン イマーシブ エンドポイントまで、多種多様なビデオ エンドポイントを用意しています。

そのユーザ エクスペリエンスはビデオ エンドポイントのタイプによってさまざまであり、多くの場合機能群もビデオ エンドポイントのタイプによって異なります。個々のビデオ エンドポイントは複数の解像度をサポートしていますが、すべてのビデオ エンドポイントが同じ範囲の解像度をサポートしているわけではありません。たとえば、マルチスクリーン イマーシブ エンドポイントであれば 30 フレーム/秒（fps）で最大 1080 p の高解像度をサポートしているのに対し、ビデオ対応タブレットがサポートしている解像度は 30 fps で最大 720 p です。各ビデオ エンドポイントは共通のコア機能群を備えています。通常このコア機能群は、ライブ音声およびライブ ビデオの送受信機能と共有コンテンツの送受信機能で構成されます。エンドポイントのタイプによっては、統合型会議機能や追加のビデオ ソースおよび音声ソースのサポート機能など、高度な機能を利用することができます。

ただし、解像度を高くすると、より大きなネットワーク帯域幅が必要になるため注意が必要です。導入に際しては、エンドポイントのタイプやユーザのタイプに基づいて解像度に上限を設定するよう選択するお客様がほとんどです。通常、ビデオを導入する場合は、導入するビデオ エンドポイントのタイプおよびサポートする解像度を最初に決定します。サポートされている解像度やユーザのタイプと密接に関連するビデオ クラスが複数作成されるケースもよくあります。クラスは通常、各エンドポイントまたは各タイプのユーザに対して提供される最低限度のサービスを基にしたものです。これらのクラスには、同一タイプのエンドポイントで使用されるユーザ別の最大解像度を設定することができます。
図 2-3 は、企業に導入されるビデオ クラスの一例を示したものです。

図 2-3　ビデオ クラスの一例



ビデオ サービス

ビデオ サービスには、次の 2 つのサブカテゴリがあります。

- 「会議」（P.2-4）
- 「ストリーミングと録画」（P.2-5）

ビデオ サービスは必須ではありませんが、ビデオの導入に当たっては重要な要素となります。これらのサービスのうち少なくとも一方は、ビデオを導入する際にほぼ例外なく使用されます。

会議

会議デバイスを使用すると、1 件の会議につき同時に 3 つ以上のビデオ デバイスが参加できます。一部の会議デバイスは、会議リソースの管理機能を備えています。これにより、会議ポートをより効率的に使用できるようになります。シスコでは、スイッチングおよびトランスコーディングをサポートした会議デバイスを用意しています。

スイッチングとは、ビデオ メディアそのものを操作することなく、着信音声および着信ビデオを転送することです。スイッチング プラットフォームでは、基本的にエンドポイント間でのビデオのスイッチングが行われますが、そのためには同じ会議内で使用されるすべてのビデオ ポイントで同じ解像度のビデオが送受信されることが必要です。ビデオを導入するにあたって、各ビデオ エンドポイントで同じ範囲の解像度をサポートしつつも、継続的なプレゼンスやアクティブ プレゼンスなど高度なビデオ機能を必要としない場合は、スイッチング デバイスがコスト効率の良いスケーラブルなソリューションとなります。

トランスコーディングとは、エンドポイント間のビデオ メディア ストリームをエンコードおよびデコードすることです。トランスコーディング デバイスを使用すると、サポートする解像度が互いに異なる複数のビデオ エンドポイントを同一の会議に参加させることができるほか、継続的なプレゼンスやアクティブ プレゼンスなど高度なビデオ機能をサポートすることができます。これより、会議が持つ柔軟性や機能群を最大限利用することが可能です。

シスコでは、スイッチングおよびトランスコーディングをサポートするビデオ会議プラットフォームを複数用意しています。表 2-1 は、スイッチングをサポートするデバイスおよびトランスコーディングをサポートするデバイスを示したものです。

表 2-1　スイッチングおよびトランスコーディングに使用する会議プラットフォーム

会議プラットフォーム	スイッチング	トランスコーディング
Cisco TelePresence Multipoint Switch	Yes	No
Cisco TelePresence Server	No	Yes
Cisco TelePresence MCU 4000 シリーズおよび MSE 8000 シリーズ	No	Yes
Cisco Integrated Services Router（ISR）G2	No	Yes

Cisco TelePresence Conductor は、会議ポートを自動で管理できる新しいタイプの会議デバイスです。Cisco TelePresence Conductor は、会議デバイスすべてのフロントエンドとして機能し、会議要求の配信の管理を行います。Cisco TelePresence Conductor を使用すると、分散している膨大な会議リソースを、静的設定によって会議デバイスに限定することなく、動的に割り当てることができます。

ストリーミングと録画

ストリーミング デバイスおよび録画デバイスを使用すると、重要性の高い会議やメッセージ、更新情報の記録、リプレイ、およびストリーミングを行うことができます。また、多数のユーザが観覧者として会議に参加できるように会議をストリーミングすることもできます。シスコでは次のような、TelePresence ビデオ エンドポイントおよび Unified Communications ビデオ エンドポイント用の録画/ストリーミング サーバと、TelePresence エンドポイント専用の録画サーバをそれぞれ 1 つずつ用意しています。

- Cisco TelePresence Content Server（TCS）

  Cisco TCS は、Cisco TelePresence Media Services Engine（MSE）シャーシ用のアプライアンスまたはブレードとして提供されます。Cisco TCS を使用すると、TelePresence ビデオ エンドポイントまたは Unified Communications ビデオ エンドポイントから、ビデオ会議のライブ録画、ライブ ストリーミング、およびライブ再生を実行することができます。ライブ ストリームおよびライブ録画は、標準的な QuickTime、RealPlayer、および Windows Media Players で視聴できます。

- Cisco TelePresence Recording Server（CTRS）

  CTRS は、Cisco TelePresence System 3*x*10、1300、1100、および 500 のエンドポイントに対応したサーバベースのプラットフォームで、スタジオ モードの運用やイベントの録画および再生が可能です。録画した内容は、ネイティブの解像度 1080 p または 720 p で、Cisco TelePresence System 3*x*10、1300、1100、および 500 のエンドポイントから視聴できます。また、QuickTime、RealPlayer、または Windows Media Player から CIF 形式で視聴することもできます。

ビデオ ネットワーク サービス

ビデオ ネットワーク サービスにも、次の 2 つのサブカテゴリがあります。

- 「コール制御」（P.2-6）
- 「ゲートウェイ」（P.2-7）

ビデオ ネットワーク サービスは、外部ビデオ ネットワークへのコール ルーティングやアクセスなどを行う重要なサービスです。

コール制御

コール制御の主な機能は、エンドポイントの登録、コール ルーティング、モニタリング、接続の維持などです。またコール制御プラットフォームは、ネットワーク ダイヤル プランや、コール アドミッション制御のオプションにとっての基盤でもあります。シスコは、Cisco Unified Communications Manager（Unified CM）および Cisco TelePresence Video Communication Server（VCS）という 2 つの主要なインタラクティブ ビデオ用コール制御プラットフォームを用意しています。世界最大規模の IP 音声システムの中には、コール制御およびプロビジョニングに Unified CM を使用しているものがいくつかあります。ただし本来 Unified CM は、Cisco TelePresence デバイスおよび Cisco Unified Communications デバイスに対応したコール制御/プロビジョニング用のプラットフォームです。

Cisco VCS は、大規模環境への導入をサポートするための高度なビデオ機能を備えた H.323 ビデオ環境および Session Initiation Protocol（SIP）ビデオ環境のコール制御を目的とした設計されたものです。VCS は、次のいずれかとして導入できます。

- VCS Control：企業に導入されたビデオ環境のコール制御を行います。
- VCS Expressway：ネットワーク アドレス変換（NAT）およびファイアウォール トラバーサルをサポートします。これにより、社外のビデオも使用できるようになるため、Business-to-Business（B2B）コミュニケーションが可能になるほか、遠隔地の社員もインターネットを介して利用することができるようになります。

コール制御プラットフォームは、導入済みか新規に導入するかを問わず、それぞれを個別に導入することも、統合されたソリューションとしてまとめて導入することも可能です。Unified CM では、Unified Communications ビデオ エンドポイントはすべてサポートされているほか、TelePresence エンドポイントもその大半がサポートされています。一方 VCS の場合、TelePresence エンドポイントについては大半がサポートされていますが、Unified Communications エンドポイントはサポートされていません。表 2-2 は、コール制御のサポート状況をビデオ エンドポイントのタイプまたはシリーズごとにまとめたものです。

表 2-2　各ビデオ エンドポイントでのコール制御のサポート状況

エンドポイント	Unified CM	VCS
TX9000 シリーズ	Yes	No
CTS 3000 シリーズ	Yes	No
CTS T シリーズ	No	Yes
TX1300 シリーズ	Yes	No
CTS MX シリーズ	Yes	Yes
CTS Profile MXP シリーズ	Yes	Yes
CTS Profile シリーズ	Yes	Yes
CTS EX シリーズ	Yes	Yes
CTS MXP シリーズ	No	Yes

表 2-2　各ビデオ エンドポイントでのコール制御のサポート状況 （続き）

エンドポイント	Unified CM	VCS
CTS 1100	Yes	No
CTS 500	Yes	No
Cisco Jabber Video for TelePresence（Movi）	No	Yes
CTS E20	Yes	Yes
9900 シリーズ	Yes	No
Cisco Unified Personal Communicator	Yes	No
Cisco Jabber	Yes	No
Cius	Yes	No

ゲートウェイ

ビデオ ゲートウェイは、ネットワーク間のアクセスを実現するためのものです。シスコでは、次のビデオ ゲートウェイを用意しています。

- ISDN ゲートウェイ

  ISDN ゲートウェイを使用すると、TelePresence ビデオ エンドポイントおよび Unified Communications ビデオ エンドポイントからレガシーな H.320 ビデオ エンドポイントへの接続が可能になります ISDN ゲートウェイは H.320 ゲートウェイとも呼ばれます。

- 拡張メディア ゲートウェイ

  拡張メディア ゲートウェイを使用すると、Microsoft Office Communications Server 2007 R2 または Microsoft Lync Server のユーザと、標準ベースの TelePresence デバイスおよびビデオ会議デバイスとの通信が可能になります。

- IP-to-IP ゲートウェイ

  シスコでは、次の IP-to-IP ゲートウェイを用意しています。これらのゲートウェイにより、Business-to-Business（B2B）接続が可能になるほか、ビデオ エンドポイントのインターネット接続もサポートされます。

  - Cisco VCS Expressway

    VCS Expressway は、VCS Control と連動して、H.460.18 プロトコル、Assent プロトコル、または SIP プロトコルを使用したファイアウォール トラバーサルを可能にするアプライアンスです。Traversal Using Relay NAT（TURN）サーバがサポートされています。さらに VCS Expressway では、SIP ビデオ デバイスおよび H.323 ビデオ デバイスを対象としたエンドポイントの登録および信号とメディアのインターワーキングを公衆インターネット経由で行うことができます。

  - Cisco Unified Border Element

    Cisco Unified Border Element は、シスコのさまざまなルータ プラットフォーム上で使用することができます。信号のインターワーキング、メディアのインターワーキング、アドレスおよびポートの変換、課金、セキュリティ、QoS（Quality of Service）、および帯域幅管理のネットワーク間境界ポイントとして機能します。サービス プロバイダーの TelePresence Exchange では通常、IP-to-IP ゲートウェイとして実装されます。これは、Cisco Unified Border Element をお客様のネットワーク間の境界ポイントにすることでセキュリティを実現できるためです。

– Cisco Intercompany Media Engine（IME）

Cisco IME は、Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスおよび Cisco Unified CM 8.*x* 以降のリリースと連動して Business-to-Business（B2B）接続を可能にするサーバベースのプラットフォームです。

管理

ビデオ管理プラットフォームでは、スケジューリングや、ビデオ エンドポイントおよびインフラストラクチャのモニタリングのほか、場合によってはプロビジョニングや、ネットワーク上のメディア フローのトレースなど、さまざまな機能が実行されます。シスコでは、TelePresence および Unified Communications のビデオ用として次の 3 つの主要な管理プラットフォームを用意しています。

- 「Cisco TelePresence Management Suite」（P.2-8）
- 「Cisco TelePresence Manager」（P.2-8）
- 「Cisco Prime Collaboration Manager」（P.2-8）

Cisco TelePresence Management Suite

Cisco TelePresence Management Suite（TMS）は、管理アプライアンス、またはサーバ上にロード可能なソフトウェアとして提供されています。Cisco TMS では、VCS に登録された TelePresence エンドポイントを対象に、One-Button-To-Push（OBTP）コールの始動、スケジューリング、モニタリング、およびプロビジョニングを行うことができます。また TMS では、Unified CM に登録された TelePresence エンドポイントを対象に OBTP、スケジューリング、および統計情報の収集を行うこともできます。さらに TMS では、Polycom や LifeSize など、サードパーティのテレプレゼンス エンドポイントおよびビデオ エンドポイントに対しても、スケジューリング機能や一部のモニタリング機能を実行できます。

TMS は、企業の予定表管理システム（Microsoft Exchange など）と統合することができます。これにより、Microsoft Outlook などのツールを使用してスケジューリングを行えるようになります。また TMS は、組み込み Web スケジューリング インターフェイスを備えています。これを使用すればユーザは TMS から直接、会議のスケジューリングを行うことができます。

Cisco TelePresence Manager

Cisco TelePresence Manager は、元々 Cisco TelePresence エンドポイントを対象とした OBTP コールの始動、スケジューリング、および管理を行うことを目的に開発されたサーバベースのプラットフォームです。また Cisco TelePresence Manager では、Unified CM に登録されていないサードパーティのエンドポイントを含むテレプレゼンス エンドポイントのスケジューリングも実行されます。

Cisco TelePresence Manager は、企業の予定表管理システム（Microsoft Exchange など）と統合することができます。これにより、Microsoft Outlook などのツールを使用してスケジューリングを行えるようになります。TMS とは異なり、Cisco TelePresence Manager では組み込み Web ベース スケジューリングは使用できません。

Cisco Prime Collaboration Manager

Cisco Prime Collaboration Manager はサーバベースのネットワーク管理プラットフォームです。これを使用すると、メディア フローのモニタリングおよび分析を Cisco メディアネット対応デバイスからリアルタイムに行うことができます。Cisco Medianet デバイスとは、Cisco Mediatrace をサポートしているルータおよびスイッチのことです。Cisco Mediatrace は、ネットワーク上をメディアが転送される際の経路をマッピングするためのもので、Cisco メディア サービス インターフェイス（MSI）を備えた

エンドポイントとのみ使用することができます。MSI は、ビデオ エンドポイントおよびコラボレーション アプリケーションに組み込まれたソフトウェア コンポーネントで、ネットワーク ポートの自動設定や Mediatrace の開始などの高度な機能を備えています。また Cisco Prime Collaboration Manager では、履歴情報のレポートを表示できるほか、使用状況や問題発生の傾向、重大な機能障害などを確認することができます。

ネットワーク

ネットワークを適切に設計することは、ビデオ設計における重要事項です。既存のネットワーク プロトコル、機能、およびツールを使用すると、ビデオの導入が容易になるだけでなく、目的通りの環境が実現しやすくなります。インタラクティブ ビデオ デバイスは損失の影響を受けやすいため、損失は最小限に留めることが必要です。ネットワーク上のビデオ トラフィックを把握しエンドツーエンドの QoS（Quality of Service）を保証することによって、期待通りのビデオ エクスペリエンスを実現することができます。

ネットワーク デバイス間での情報共有に使用されるシスコ独自のデータリンク層プロトコルである Cisco Discovery Protocol（CDP）などを使用すれば、ビデオ エンドポイントを自動的に識別することができるため、それらの QoS マーキングを信頼し、適切な仮想ローカル エリア ネットワーク（VLAN）にトラフィックを送出して、パケットを適切にキューイングすることができるようになります。さらに VLAN を使用すると、ビデオ トラフィックを他のネットワーク トラフィックから隔離することができるため、セキュリティの強化にもつながります。

ビデオ対応ネットワークではリアルタイムのトラフィック分析を実行できるため、ネットワークの問題に関するトラブルシューティングもリアルタイムに行うことができます。現在のようなネットワークでは、2 つのエンドポイント間のビデオ フローがネットワーク上の複数の経路をたどる可能性があるため、その状況によっては、ネットワーク上のビデオ フローをトラッキングし、ネットワーク内で損失が発生している場所を正確に特定することが不可欠です。Cisco メディアネット対応デバイスでは、リアルタイムのトラフィック分析を実行できるだけでなく、ネットワークのオーバーサブスクリプションを回避できるよう使用率データを確認することもできます。

CHAPTER 3

ビデオに関する基本的な概念

この章では、ビデオ ソリューションに関連するいくつかの基本的な概念や用語について説明します。

IP ビデオ ソリューションの基本用語

IP ビデオ ソリューションに関連する概念や用語にはさまざまなものがあり、その範囲はビデオ ストリームの構成から、ビデオ ストリームをネットワーク上へ送出するためのデバイスやその方式にまでおよびます。ここでは、最も基本的な概念および用語を取り上げます。IP ビデオ テクノロジーとどのような関連があるのかなど、その内容をできるだけわかりやすく解説します。

ビデオ フレーム

ビデオとは、連続する複数の画像によって一連の動きを構成したものです。連続する各画像を時間の経過と共に順次表示することで、一連の動きが表現されます。これらの各静止画像をビデオ フレームと言います。各ビデオ フレーム間の時間差が小さいほどリフレシュ レートは高くなるため、ビデオの動きはより自然なものになります。一連の動きを表現するために表示される 1 秒あたりのビデオ フレーム数が多ければ、フレーム間の画像の変化は小さく、動きがより滑らかになるからです。

IP ビデオ ソリューションでの圧縮

IP ビデオの圧縮とはその名のとおり、ビデオ情報全体のサイズを小さくするプロセスです。サイズが非常に小さい IP テレフォニー ストリームの音声データとは異なり、ビデオ データは元々サイズが大きいうえ、そのストリーム フローも大きく変動します。フローが変動する原因は、ビデオが静止部分（背景など）の情報と動きがある部分（人物など）の情報で構成されている点にあります。また動きは常に一定というわけではなく、その対象の大きさも同じではありません。そのため、リアルタイム ビデオを転送する際には、そのサイズやフローの変動を小さくするための複雑なメカニズムが必要となります。ビデオを圧縮すると、そのサイズが軽減されるため転送が容易になります。IP ビデオの主な圧縮方法は次のとおりです。

- 「ロスレス圧縮」（P.3-2）
- 「ロッシー圧縮」（P.3-2）

いずれの圧縮方法でも、次のような方式を使用できます。

- 「イントラフレーム」（P.3-2）
- 「インターフレーム」（P.3-2）

ロスレス圧縮

ロスレス IP ビデオ圧縮では、圧縮を解除すると圧縮前の元の画像とまったく同じ状態の画像が復元されます。ロスレス圧縮の場合、統計に基づいて冗長な情報のみ削除されるため、受け取る側はビデオ信号を完全に再現することができます。つまり、圧縮プロセスの中で何らかビデオ情報が意図的に破棄されることはありません。ロスレス圧縮は、元の画像についての情報をすべて保持できることから、主にデータを保管する際に使用されます。ただしビデオをロスレス圧縮しても、生成される情報量は膨大であり、ストリーミングにも支障が出ることになります。そのため、IP ビデオ ソリューションでロスレス ビデオ圧縮が使用されることはほとんどありません。

ロッシー圧縮

IP ビデオでは、ロスレス圧縮よりもロッシー ビデオ圧縮を使用するのが一般的です。ロッシー ビデオ圧縮では、ビデオの中に視聴者にとって不要な情報や認識できない情報が含まれていることを前提として、圧縮プロセスの際にビデオ情報の一部が意図的に破棄されます。たとえば、アナログからデジタルに変換した場合のノイズなどは、この「不要な」ビデオ情報に当たります。ロッシー ビデオ圧縮では、非常に高い画質を維持しながらペイロード サイズを大幅に縮小することができます。この圧縮手法が IP ビデオ ソリューションで多用される理由はここにあります。ビデオ圧縮では常に、ビデオのサイズと画質とがトレードオフの関係にあることに留意する必要があります。この他、フレームの持続時間や、1 秒当たりのフレーム数を表すフレーム レート（単位は fps）にも、他の要素との間にトレードオフの関係があります。たとえば、30 fps で 1080 p の解像度を持つ画像よりも、60 fps で 720 p の解像度を持つ画像の方が、動きが見やすいうえ帯域幅も約 10 % 節約できるため、メリットは大きいと言えます。

イントラフレーム

イントラフレーム方式は、1 回につき 1 つのビデオ フレームを対象にその内容を圧縮するもので、その前後のビデオ フレームは考慮されません。すべてのビデオ フレームが個別に圧縮されるため、特定の圧縮ビデオ フレームを圧縮解除する場合、前後の圧縮ビデオ フレームは必要ありません。つまり、すべての圧縮ビデオ フレームをキー フレームと見なすことができます。

イントラフレーム圧縮は圧縮率がインターフレーム方式ほど高くないため、ビデオ ストリーミングやビデオ会議に単独で使用しても、あまりメリットはありません。そのためビデオ会議では、イントラフレーム圧縮は常にインターフレーム方式と併用されます。

インターフレーム

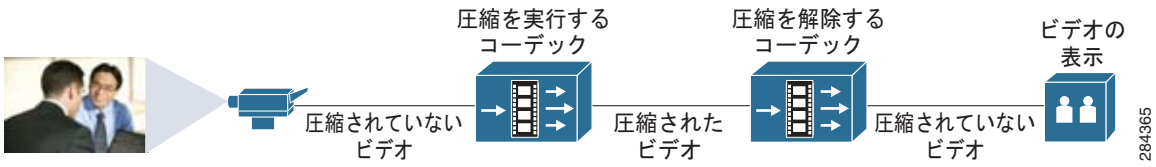
イントラフレーム方式とは異なり、インターフレーム方式では、先行するビデオ フレームについての情報を基にして圧縮が実行されます。インターフレーム方式を実装した一部のビデオ形式（たとえば H.264 などの Advanced Video Coding 形式）では、圧縮を実行する際、後続のビデオ フレームに関する情報も考慮されます。

インターフレーム方式では、ビデオの中で圧縮を行う画像の各部分には常に動きがあるわけではないという事実を基に、コンプレッサから、ビデオ フレームに関するすべての情報ではなく差分（動きのあった部分）のみが転送されます。重要な点は、この方式がキー フレームという考え方を基盤としていることです。キー フレームとは、圧縮処理の基準として使用される初期ビデオ フレームです。したがって、キー フレームがデコーダに到達しなければ、圧縮解除の処理は適正に行われません。このため、インターフレーム方式を採用しているビデオ形式では通常、リカバリのメカニズムが実装されています。インターフレーム圧縮方式では、キー フレームは基準として使用されるため、それを圧縮した内容が前後のフレームに依存することはありません。

IP ビデオ ソリューションのコーデック

コーデック（CODEC）とは、コンプレッサ/デコンプレッサ（COmpressor-DECompressor）またはコーダ/デコーダ（COder-DECoder）を表す用語です。ビデオ コーデック（Cisco TelePresence System または C シリーズのコーデックなど）は、ビデオをエンコードおよびデコードするためのハードウェアまたはソフトウェアです。また、コーデックという用語は通常、ビデオ形式を表す場合にも使用されます。各ビデオ コーデックは、少なくとも 1 つのビデオ形式を実装することができます。またこれらの形式では、イントラフレーム圧縮方式またはインターフレーム圧縮方式のいずれかを使用したロスレス圧縮またはロッシー圧縮を実装できます。IP ビデオ ソリューションでは、ほとんどすべての IP ビデオ エンドポイントが基本機能としてコーデックを搭載しています。「IP ビデオ ソリューションでの圧縮」（P.3-1）で述べられているように、圧縮が必要となる理由は、セッション内で転送するビデオ データのサイズが大きいことにあります。図 3-1 には、圧縮を実行するコーデックが示されています。このコーデックでビデオ ストリームの圧縮処理が行われることにより、そのサイズと変動が軽減されます。

図 3-1　　ビデオ圧縮を実行するコーデック



ビデオの圧縮形式

「IP ビデオ ソリューションのコーデック」（P.3-3）で述べられているように、ビデオ形式はコーデックと呼ばれることも多く、この 2 つの用語は混用されています。ビデオ形式は、特定の技術に基づいてビデオの圧縮またはエンコードをどのように行うかについての仕様です。たとえば、広く使用されている H.264 は、ロッシー圧縮を採用したビデオ形式です。ビデオ形式は、ビデオをエンコードするビデオ エンドポイントに搭載されたコーデックにより実装されます。IP ビデオ エンドポイントでは、使用するビデオ形式について、コール時にネゴシエーションを行ったうえで同意する必要があります。方法や方式が同じビデオ形式であっても、その特性は必ずしも同じではありません。それぞれのビデオ形式が持つ強みやメリットは、その方法や方式がどのように実装されているのかによって決まります。

一般にビデオ形式は、国際電気通信連合（ITU）電気通信標準化部門（ITU-T）、または国際標準化機構（ISO）と国際電気標準会議（IEC）が共同で策定しています。IP ビデオ ソリューションでの利用頻度が最も高い 3 つのビデオ形式のうち、H.261 と H.263 の 2 つは ITU-T が策定したものであり、H.264（Moving Picture Experts Group（MPEG））は ITU-T、ISO、および IEC が共同で策定したものです。表 3-1 は、これらの形式が持つ機能と特性を比較したものです。

表 3-1　　ビデオの圧縮形式の比較

機能	H.261	H.263	H.264
帯域幅効率	低	中	高
HD サポート	No	No	Yes
サポートされている圧縮ビデオ フレーム	I フレーム、P フレーム	I フレーム、B フレーム、P フレーム	I フレーム、B フレーム、P フレーム

表 3-1　ビデオの圧縮形式の比較 （続き）

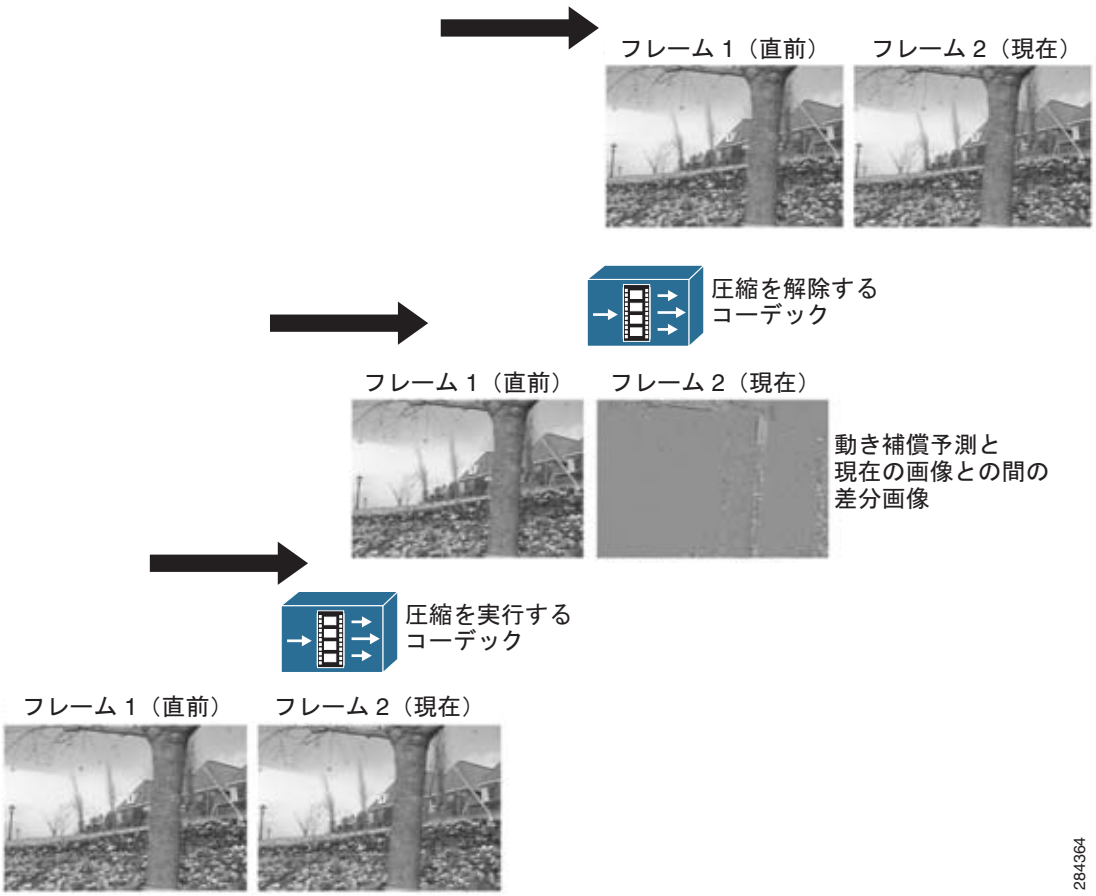
機能	H.261	H.263	H.264
圧縮およびメディアの復元機能	エラー フィードバック メカニズム	エラー フィードバック メカニズム 最適化された仮想チャネル リンク（VLC）テーブル オプションのネゴシエーション モード（Annex D、E、F、および G）	エラー フィードバック メカニズム 高度な動き推定 拡張エントロピー コーディング I フレーム用のイントラ予測コーディング 4x4 Display Channel Table（DCT） ネットワーク抽象化層 Gradual Decoder Refresh（GDR）フレーム Long-Term Reference Picture（LTRP）フレーム

現在、ほとんどの Cisco IP Video エンドポイントでは、H.264 がデフォルトのビデオ圧縮形式として利用されています。

圧縮ビデオ フレーム

圧縮ビデオ フレームとは、（イントラフレーム方式またはインターフレーム方式、およびロッシー圧縮またはロスレス圧縮を使用した）圧縮処理による生成物のことです。通常の（圧縮されていない）ビデオ フレームの代わりに使用することで、転送するビデオ情報全体のサイズを軽減することができます。図 3-2 は、ビデオ フレームがコーデックで圧縮される過程を示したものです。この例で生成される圧縮ビデオ フレームは I フレームです。

図 3-2　圧縮の処理過程



IP ビデオ ソリューションでは、さまざまなタイプの圧縮ビデオ フレームが使用されます。このうち主なタイプは次のとおりです。

- 「I フレーム」（P.3-5）
- 「P フレーム」（P.3-6）
- 「B フレーム」（P.3-6）

I フレーム

I フレームは、その内部データのみに基づくもので、シーケンスの開始時に圧縮解除（またはデコード）を行うことができます。I フレームの圧縮には、イントラフレーム方式が使用されます。I フレームは、その内容が他のいずれのフレームに依存せず、かつ他のフレームの基準として使用されることから、別名キーフレームと呼ばれることもあります。インターフレーム圧縮の項で説明したように、キーフレーム（初期フレーム）は、圧縮対象である画像シーケンスの先頭に使用されます。Instant Decoder Refresh（IDR）フレーム、Gradual Decoder Refresh（GDR）フレーム、Long-Term Reference Picture（LTRP）フレームは代表的な I フレームです。GDR フレームは、複数のフレームに細分することで送信間隔を短くすることができるのに対し、IDR フレームは 1 つのパケットで送信されます。これが、IDR フレームと GDR フレームとの主な違いです。GDR フレームを使用する目的は、IDR フレームを使用した場合に生じるデータ レートの大幅な上昇を回避し、エンド ユーザにとってより質の高いビデオ再生を実現することにあります。GDR を実装すると、たとえば全体として 1 つのフレームを構成す

る 10 個の IDR エンコード ビデオ画像を個別に送信することができます。この場合、10 フレームのウィンドウ上で徐々に変化するのは元のフレームのわずか 1/10 であるため、ユーザが知覚するビデオの品質は一般にかなり高くなります。

一方 LTRP フレームは、一部のコーデックに実装されているメディアの復元機能に使用されます。ネットワーク上では避けることが難しい圧縮ビデオの損失やエラーは、デコーダで表示エラーが生じる原因になります。こうしたエラーは、後続の P フレームにも影響を与えます。この問題を回避するには、デコーダからエンコーダへ I フレームを要求してエラーを解消する（エラー フィードバック メカニズム）のが自然な方法です。ただし、別のフレーム（より以前の長時間フレーム）を基準として使用するほうが、対処方法としては適切です。フィードバック メカニズムと、エラーのない LTRP フレームとを併用することにより、消失したビデオ データ（スライスなど）を回復し、エラーのある LTRP フレームを破棄することができます。コーデックにこのような仕組みが実装されている場合、（IDR と GDR のいずれを使用している場合でも）LTRP フレームとなるのは、コーデックに到達する最後の I フレームです。受信側のコーデックでは、この最後の I フレームが LTRP フレームとして保存されますが、その後新たに I フレームが到達した場合は、それが LTRP フレームになります。I フレームが転送中に消失した場合、受信側のコーデックでは LTRP フレームを使用してその回復が試みられます。

I フレームは、イントラフレーム方式を使用して圧縮されます。これは、ビデオ ストリームの帯域幅使用量に直接的な影響を与えます。I フレームの使用頻度が高いほど、より多くの帯域幅が必要となります。

P フレーム

予測フレーム（P フレーム）は、I フレームよりも圧縮率が高いフレームです。P フレームは、インターフレーム エンコード方式を使用して圧縮されます。P フレームは、ビデオ ストリームの中で I フレームに後続するフレームであり、先行する I フレームから変更されたビデオ情報のみ保持します。インターフレーム圧縮の項で説明したように、P フレームを正しくデコードするためには、直近の I フレーム（キー フレーム）を組み合わせて使用する必要があります。

B フレーム

P フレームを使用すると圧縮率は大幅に高くなりますが、双方向予測フレーム（B フレーム）を使用すれば全体の圧縮率はさらに高まります。B フレームは、直前の I フレームおよび後続の P フレームを参照し、それらの画像間の差分のみを保持します。ただし 2 つのアンカー フレームの間に十分なバッファを確保するためにはコーデックのメモリを 2 倍にする必要があるため、一部のコーデックでは（コールで使用されるビデオ形式が B フレームをサポートしている場合でも）B フレームを実装できません。また B フレームを使用した場合は、いくらかの遅延が新たに発生します。この遅延は B フレームの実装ロジックに起因するものです。

図 3-3 は、ビデオ ストリーム内の圧縮ビデオ フレームの順序を図示したものです。この例の場合、コーデックは I フレーム、P フレーム、および B フレームを実装できるものとします。

図 3-3　　ビデオを表示する順序

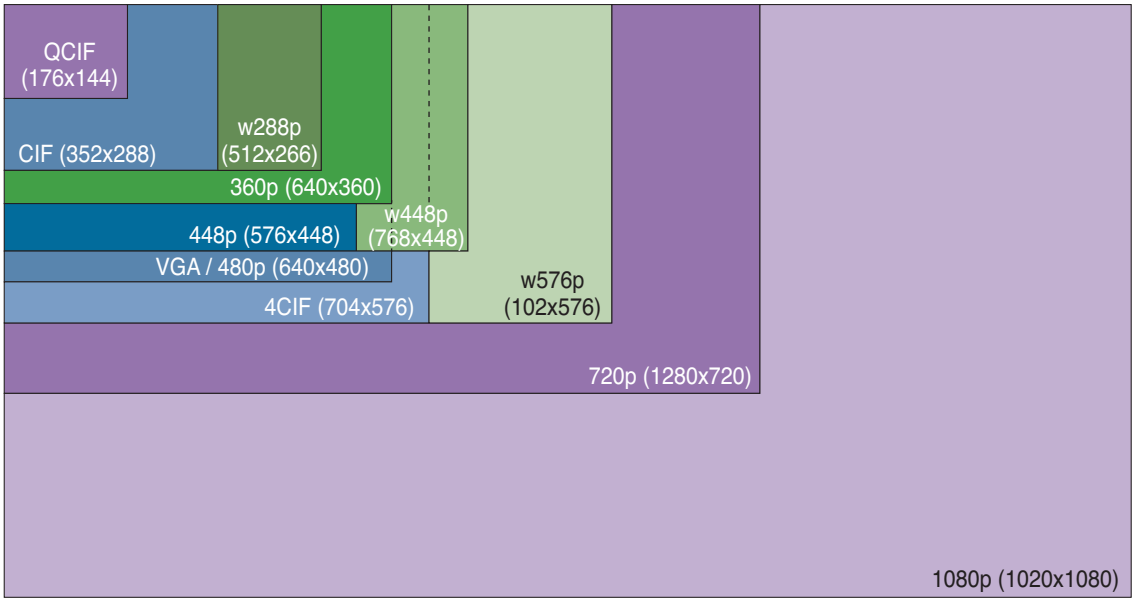
IP ビデオ ソリューションの解像度形式

簡単に言えば、解像度形式とは画像サイズのことです。現在は多くのビデオ エンドポイントが、ビデオを表示するスクリーンに合わせて画像を拡大または縮小する機能を備えています。遠くからでもビデオを見られるようにするにはこうした機能が必要ですが、その場合画像の鮮明度は低下します。

ビデオ解像度形式は正式には、表示の際に使用される特定のピクセル数とスキャン方式との組み合わせとして定義されます。次のリストおよび図 3-4 は、IP ビデオ ソリューションで使用される主なビデオ解像度形式を列記および図示したものです。

- CIF：Common Intermediate Format（共通中間フォーマット）
- QCIF：Quarter CIF
- 360 p：垂直 360、プログレッシブ スキャン
- 480 p：垂直 480、プログレッシブ スキャン
- 720 p：垂直 720、プログレッシブ スキャン
- 1080 i：垂直 1080、インターレース ビデオ
- 1080 p：垂直 1080、プログレッシブ スキャン

図 3-4　主なビデオ解像度



シスコの IP ビデオ ソリューションの変遷

IP ビデオは、他のビデオ会議方式に代わって利用されることが多くなっています。ただし、場合によっては方式間の相互接続が必要となるため、他の方式についても基本的な知識を習得しておくことは有用です。ここでは、ISDN メディア経由でのビデオから比較的新しいクラウドホスト型ビデオ ソリューションに至るビデオ会議ソリューションの変遷と、それらのソリューション間の相互運用性について概説します。取り上げるのは次のようなビデオ ソリューションで、それらの相互運用性についても説明します。

これらのソリューションの説明は、必ずしも年代順には記述されていません。ソリューションの中には互いに重複した部分を持つものや同時期に開発されたものもあります。

ISDN 経由でのビデオ

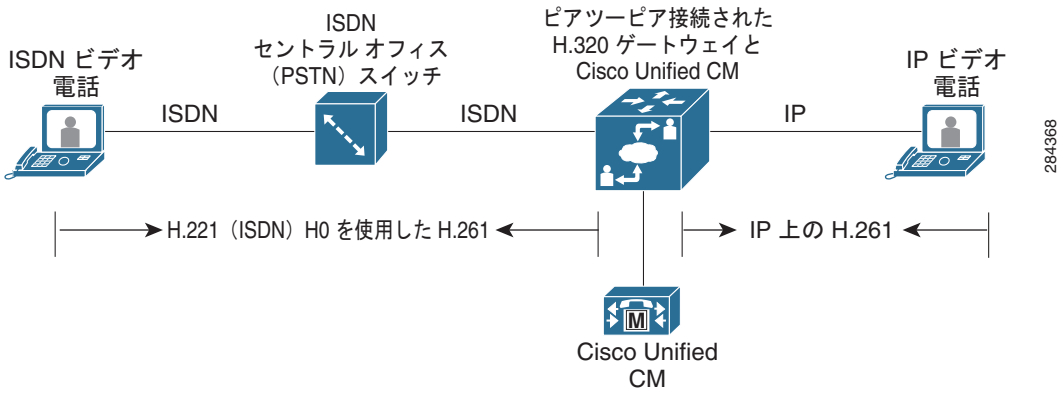
ビデオ会議が広く利用されるようになったのは、Integrated Services Digital Network（ISDN）規格が登場して以降です。そのため ISDN は、ビデオ会議が普及するきっかけとなった最初のテクノロジーであると目されています。その後ビデオ会議の普及が進むにつれて、より優れた相互運用性や復元機能、ビデオ品質を実現する新しいソリューションが次々と登場しました。そしてシスコがビデオ会議の市場に参入する頃になると、ISDN ビデオ端末に最先端の技術を取り入れる必要があるということが強く認識されるようになります。シスコは、既存の ISDN ビデオ端末から新しい IP ビデオ ネットワークに接続できるよう、H.320 ゲートウェイとして Cisco Unified Videoconferencing 3500 シリーズ製品を IP ビデオ ソリューションに組み入れました。それ以降シスコは、ISDN ビデオをサポートするため、さまざまな H.320 デバイスをポートフォリオに組み入れています。これらの H.320 デバイスを Cisco Unified Communications Manager（Unified CM）や Cisco TelePresence Video Communication Server（VCS）などのゲートキーパーに接続することで、IP ビデオ エンドポイントから、PSTN クラウドの反対側に位置する ISDN ビデオ エンドポイントへのアクセスが実現されます。

H.320 規格には、ISDN でのマルチメディア（ここでの内容に関係があるのはビデオ用の H.221）が規定されています。H.320 では元々、ISDN でビデオを使用する際のビデオ形式として H.261 または H.263 が規定されており、前回の更新時に H.264 が追加されました。H.221 には、Px64 kbps、H0（384 kbps）、H11（1536 kbps）、および H12（1920 kbps）という 4 つの転送モードが定義されています。ビデオがエンコードされると、選択したビデオ形式（H.261 など）は H.221 規格に基づいて多重化されます。

ISDN は、サポートしているビデオ解像度形式の画像サイズが大きく制限されていることから、ナローバンド テレビ電話システムと呼ばれます。ISDN は、ビデオ解像度形式として QCIF、CIF、4CIF、および 16CIF をサポートしています。

この種のソリューションは、サポートしている ISDN サービス プロバイダーに依存するという点に大きな特徴があります。この ISDN サービス プロバイダーが常時関与することにより、異なる ISDN 端末間でコールを行うことができます（図 3-5 を参照）。

図 3-5　画像 4。ISDN 経由でのビデオと使用されるプロトコル



IP ビデオ テレフォニー

実際に導入された初めてのビデオ会議テクノロジーが ISDN 経由でのビデオだとすれば、ビデオ会議をはるかに大きな規模で企業に導入できるようにしたのが IP ビデオ テレフォニーです。IP ビデオ テレフォニーを使用すると、さまざまな方法で企業にビデオを導入することができます。PC 上で稼動するソフトウェア クライアントを介することによりユーザの IP 電話でビデオを使用できるほか、専用のビデオ エンドポイントやビデオ会議ブリッジを組み込むことで、充実したメディア利用を実現することができます。ISDN 経由でのビデオとは異なり、IP ビデオ テレフォニーはビデオ解像度、復元機能、および相互運用性に優れています。

いずれの IP ビデオ テレフォニー ソリューションにとっても欠かせないものがコール制御要素です。この要素ではコール ルーティングが行われるほか、多くの場合、相互運用性や特殊機能に関わる処理も行われます。シスコが初めて提供した IP ビデオ テレフォニー関連の製品は、コール制御を行うための Cisco Unified Communications Manager（Unified CM）です。図 3-6 は、シスコの IP ビデオ テレフォニーにおけるトポロジーの一例です。

図 3-6　IP ビデオ テレフォニー

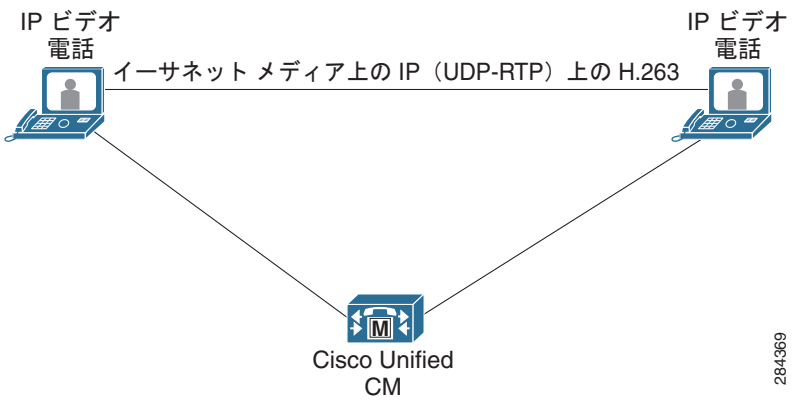
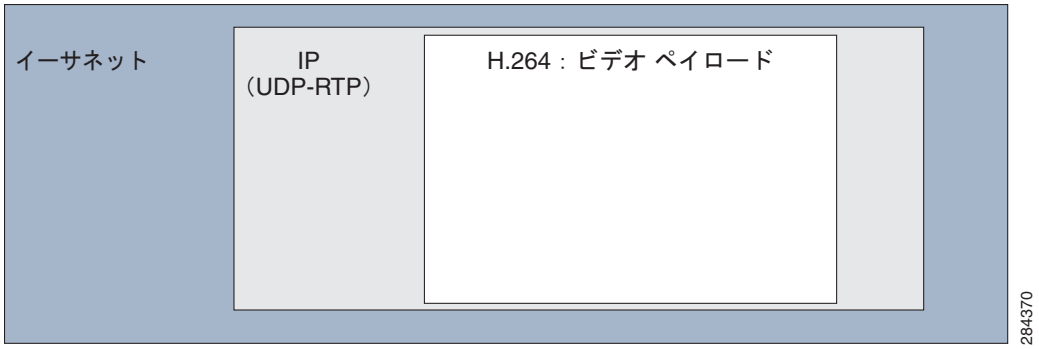


図 3-7 に示したように、IP ビデオ テレフォニーでは、ISDN 経由でのビデオ（米国の場合は 1.54 Mbps）のように 2 Mbps に制限されないさまざまな物理転送メディアにより柔軟な転送を行うことで、より優れたビデオ解像度が実現しています。また、IP（ビデオ用のユーザ データグラム プロト

コル）でカプセル化されたパケットを、イーサネット、ワイヤレス通信、マルチプロトコル ラベル スイッチング（MPLS）などを経由して伝送することが可能です。新しい転送メディア（MPLS、イーサネット、光通信など）と IP との相乗効果により、高解像度に伴う大量の圧縮ビデオ フレームでも転送することができます。新しいコーデックにより実装された新たなエラー回復技術により復元機能も強化されていますが、下位互換性は維持されています。

図 3-7　　IP による圧縮ビデオ フレームのカプセル化

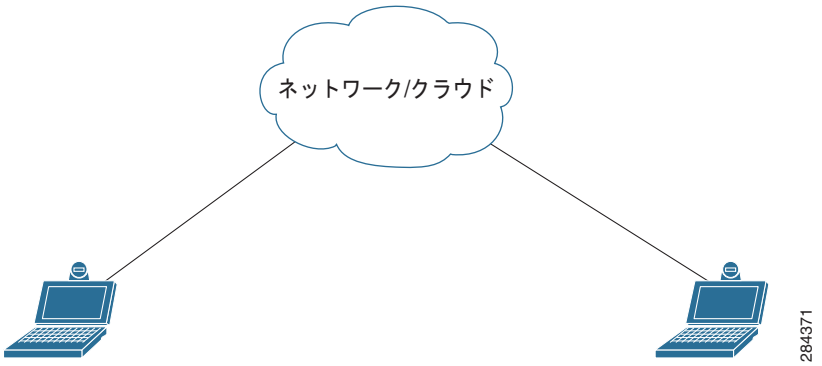


デスクトップ ビデオ会議

デスクトップ ビデオ会議は、次世代コミュニケーションとして IP ビデオが強化されています。デスクトップ ビデオ会議は、インスタント メッセージ プログラムに対するオドオンとして導入されました。同時に IP ビデオ テレフォニー技術関連の企業はその長所を認識し、従来の IP テレフォニー環境に接続できるソフトウェア ビデオ クライアントを開発しました。技術によっては、現在のようなハードウェア IP 電話が利用されるものもあれば、ソフトウェア IP 電話が利用されるものもあります。シスコが初めて提供したデスクトップ会議は、Cisco Unified Video Advantage（VT Advantage）でした。これは、ハードウェア IP 電話とソフトウェア IP 電話のどちらでもビデオ機能を利用できるようにしたソフトウェア ビデオ クライアントです。

デスクトップ ビデオ会議クライアントでは、コンピュータのリソースを使用してソフトウェアによるビデオのエンコードおよびデコードが実行されます。ビデオ解像度形式が高度になり、ビデオ形式が複雑になるほど、必要となるコンピュータのリソースは増加します。コンピュータの性能が向上すると同時に、より効率的なエンコードおよびデコードのメカニズムが開発されることで、エンド ユーザの間でも高度なデスクトップ ビデオ会議クライアントが普及するようになりました。図 3-8 は、セッション中のビデオ ソフトウェア クライアントの一般的な使用方法と基本的なトポロジーを図示したものです。

図 3-8　　ソフトウェア ビデオ会議



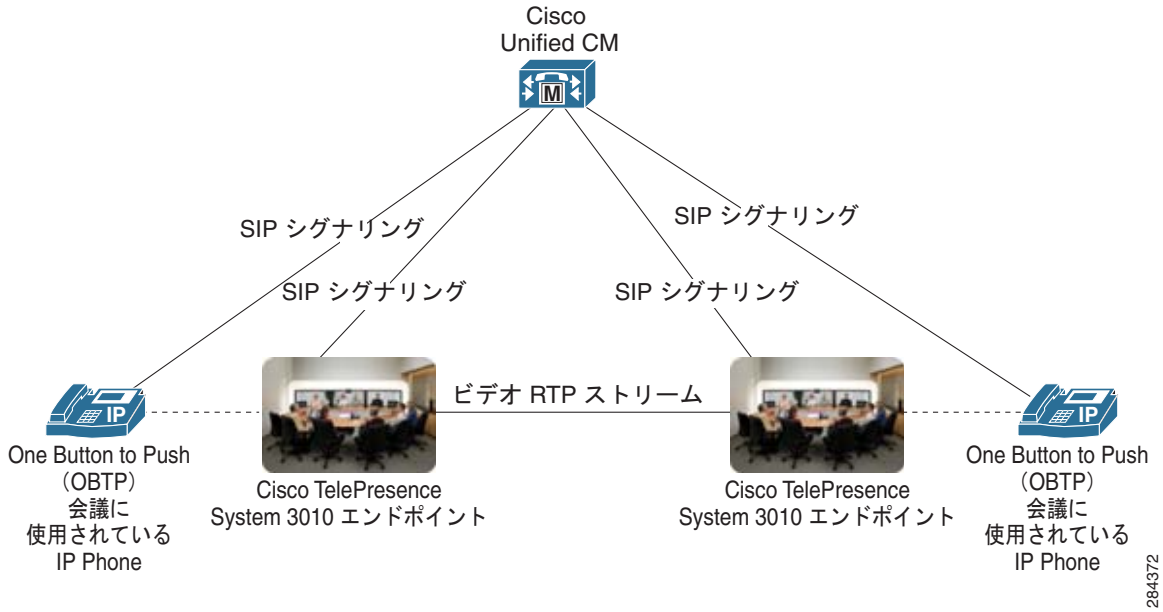
イマーシブ ビデオ会議

新しい方式によるビデオ会議の模索が続く中で、IP ビデオ ソリューションの新たな実装方法が考案されました。それが、テレプレゼンスと呼ばれるビデオ システムです。これは、相手を等身大に映し出すことができるため、遠隔地の会議参加者とより自然なコミュニケーションを取ることができます。初めて登場したテレプレゼンス システムは、値段が高いうえ専用のネットワーク環境が必要でもあったため、あまり導入されませんでした。2006 年、イマーシブ ビデオ会議の市場に進出したシスコは、ネットワークに関する膨大なノウハウを駆使して、本格的な統合型ネットワーク テレプレゼンス製品を開発しました。そして、イマーシブ ビデオ会議を開発する他社もシスコに追随して、統合型ネットワーク テレプレゼンス システムの開発に乗り出しました。

Cisco TelePresence には、従来の IP ビデオ テレフォニーと共通する点がいくつかあります。圧縮ビデオ フレームがユーザ データグラム プロトコル（UDP）でカプセル化されることで、IP ビデオ テレフォニーで使用されている同種のメディアにアクセスすることができるほか、IP ビデオ テレフォニーで使用されているビデオ形式と互換性が確保されます。ただし Cisco TelePresence には、IP ビデオ テレフォニーと共通点がある反面、一部異なる要素もあります。Cisco TelePresence では、特に大会議室での使用に適した高解像度のカメラおよびディスプレイが使用されます。Cisco TelePresence でも、コール制御はコール エージェントによって処理されますが、コール開始時にユーザがシステムを操作する方法は IP ビデオ テレフォニーとは異なります。

テレプレゼンス システムでは、高解像度カメラを使用して鮮明なビデオを撮影できます。このビデオはエンコードおよびデコードを経て、高解像度ディスプレイに表示されます、これによってビデオ エクスペリエンスは可能な限り維持されます。さらに、会議室がスタジオのような環境になるよう特殊な調整を行うことで、より現実感のある会議を実現できます。前述したように、エンド ユーザが会議を開始する際にテレプレゼンス システムを操作する方法は IP ビデオ テレフォニーとは異なります。テレプレゼンス システムは通常、ボタンを押して会議を開始できるメカニズムを備えています。Cisco TelePresence では、このようなセッション開始機能を One Button To Push（OBTP）と呼びます。図 3-9 は、イマーシブな Cisco TelePresence における基本的なポイントツーポイント コールでのメディアおよびシグナリングのフローを示したものです。

図 3-9　　イマーシブ テレプレゼンス



クラウドホスト型ビデオ ソリューション

クラウドホスト型ビデオ ソリューションは、インターネット経由でのビデオ コミュニケーションを可能にすることで、エンタープライズグレードのビデオ コラボレーションを手頃な価格で利用できるようにしたサブスクリプション ベースのサービスです。

このソリューション モデルがその他のソリューション モデルと大きく異なるのは、お客様はビデオ エンドポイント（Cisco TelePresence System EX90 や PC など）を用意するだけで、IP ビデオ インフラストラクチャの費用を先行負担しないという点です。ビデオ エンドポイントの多重化や制御は自社で行う必要がないため、インフラストラクチャに巨額の投資を行うことなくビデオ コラボレーションを実現することができます。このソリューション モデルでは、インターネット接続ができること、および IP ビデオ プロバイダーの登録が必要です。ただし、このソリューションを自社管理モデルに移行した場合でも、その IP ビデオ エンドポイントは再利用することができます。

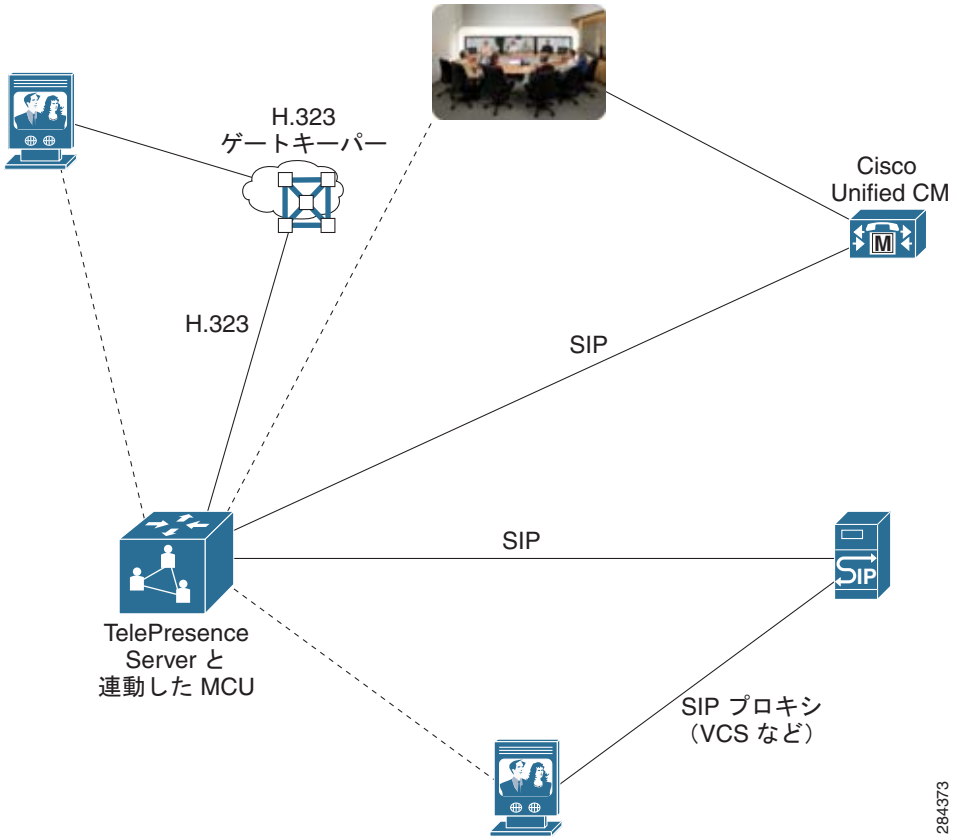
クラウドホスト型ビデオ ソリューションを使用すれば、IP ビデオ サービスを使用した分だけ料金を支払えばよいため、IP ビデオ インフラストラクチャの費用が大きな負担になるという問題は解消されます。この種のビデオ ソリューションとしては、ビデオ機能を備えた Cisco Callway や Cisco WebEx などがあります。これらのソリューションを使用すれば、管理作業のオーバーヘッドやインフラストラクチャへの投資費用を低く抑えながら、ユーザにビデオ サービスを提供することができます。

相互運用性

テクノロジーが進歩すれば必ず、新しいテクノロジーとレガシー テクノロジーとを連携させる形で運用する必要が出てきます。相互運用性は、異種の IP ビデオ テクノロジーを連携させるのに伴う問題を解消するためのものです。ただし適用できるのは、対象となるテクノロジーにより実装できる機能に限定されます。たとえば、ISDN 規格はテキストの転送に対応しているため、一部の ISDN 端末ではビデオ コール中に参加者のスクリーンにテキストを送信することができます。しかし、テキストの転送に対応していない規格が他のテクノロジーに実装されていれば、このテキストを ISDN ドメインの外部（IP ビデオ テレフォニーなど）に転送することは技術的に不可能です。

相互運用性は通常、異種テクノロジーの境界で機能する製品または製品スイートにより実現されます。一般に、ビデオ ソリューションの相互運用性を実現する製品（単独製品または製品群）には、ビデオ トランスコーダ、ビデオ ゲートウェイ、ビデオ会議ブリッジなどの種類があります。図 3-10 は、相互運用性の一般的なシナリオ（マルチポイント コントロール ユニット（MCU）による相互運用性の実現）を示したものです。

図 3-10　ビデオ会議システムにおける相互運用性



レガシー マルチポイント コントロール ユニット

初期のマルチポイント コントロール ユニット（MCU）アーキテクチャでは、実現するサービスや機能が制限されていました。これらのレガシー MCU は、コントローラ ブレードおよびデジタル シグナル プロセッサ（DSP）ブレードという 2 つの主要ハードウェア コンポーネントを備えていました。コントローラ ブレードは、ローカルの DSP 資産しか認識できないため、別の MCU の資産を認識し、それらをカスケードしてビデオ マルチポイント コールで使用することはできませんでした。さらに、特定の解像度しかサポートされておらず、トランスレーティングもサポートされていないか、サポートされていたとしても性能は低いものでした。

その後一部のレガシー MCU では高解像度ビデオがサポートされるようになったものの、大半のレガシー MCU では標準的な解像度のビデオしかサポートされないのが一般的でした。

シスコの IP ビデオ ソリューションで使用される主なテクノロジー

IP ビデオ ソリューションで使用されるテクノロジーは膨大な数に上ります。ここでは現在シスコの IP ビデオ ソリューションで使用されているテクノロジーについて説明します。シスコはこれらのテクノロジーを導入することにより、それまで懸案であったさまざまな問題を解決してきました。その 1 つがパケット損失です。この現象は、いずれの導入環境でも可能な限り回避されますが、それでも伝送メディアが制御できなくなると、場合によっては避けられないことがあります。このとき Cisco ClearPath を使用していれば、このパケット損失の影響を最小限に留めることができます。一方、テレプレゼンス相互運用プロトコル（TIP）を使用すると、マルチスクリーン システムで通信が行われている場合にどのビデオを表示するかなど、いくつかの問題を解決することができます。ここでは、次のテクノロジーについて説明します。

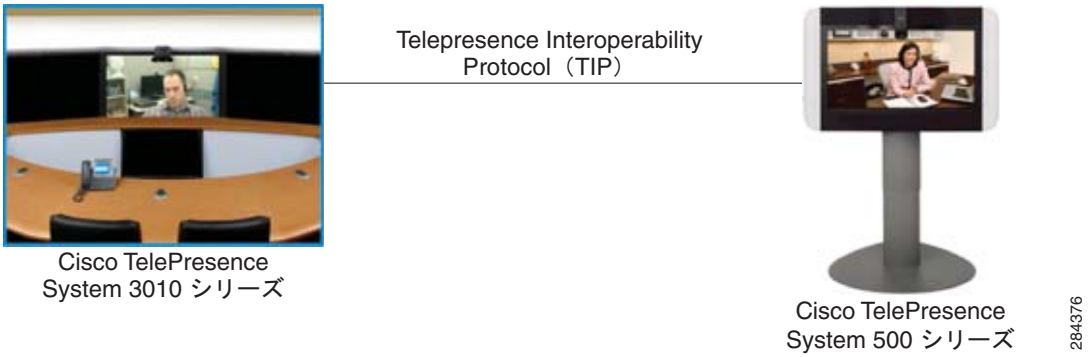
- 「テレプレゼンス相互運用プロトコル（TIP）」（P.3-14）
- 「ClearPath」（P.3-15）

テレプレゼンス相互運用プロトコル（TIP）

テレプレゼンス相互運用プロトコル（TIP）は元々シスコが開発したもので、後にオープン ソース プロトコルとして国際マルチメディア遠隔通信コンソーシアム（IMTC）に提供されました。TIP 規格では、マルチスクリーンおよびオーディオ ストリームを 2 つのリアルタイム転送プロトコル（RTP）フロー（ビデオ用および音声用にそれぞれ 1 つずつ）に多重化する方法が定義されています。これにより、マルチスクリーン エンドポイントとシングルスクリーン エンドポイントの併用のほか、ポイントツーポイント セッションおよびマルチポイント セッションが可能となります。また TIP の仕様には、リアルタイム転送プロトコル（RTP）アプリケーション拡張を使用して、セッションの確立時にプロファイル機能やメディア別フロー オプションを提示する方法についても定義されています。さらには、ストリーム中にデバイスからフィードバックを行う方法や復元メカニズムを作動させる方法も定義されています。

図 3-11 に図示されているように、TIP では、スクリーン（およびその音声）のスイッチングをどのように行うかが指定されていることで、さまざまなベンダーのマルチスクリーン IP ビデオ ソリューションの相互運用が可能になっています。TIP は、ビデオ エンドポイント、ビデオ トランスコーダ、ビデオ ゲートウェイ、および MCU（ビデオ会議ブリッジ）で使用されます。

図 3-11　実行中の TIP 多重化



ClearPath

Cisco ClearPath は、パケット損失が 15 % までであれば、それに伴う悪影響を排除することができるテクノロジーです。これは、さまざまなメディア復元メカニズムを組み合わせたダイナミックなテクノロジーです。たとえば損失メディアを使用している場合、ClearPath があるとパケット損失の影響を相殺することができるため、ユーザ エクスペリエンスが向上します。ClearPath はデフォルトで有効です。ビデオ コミュニケーションの両端でサポートされている場合に使用されます。ClearPath モードは **xConfiguration Conference PacketLossResilience Mode** コマンドによって設定されます。ClearPath 内のメディア復元メカニズムはすべて H.264 規格に準拠しているため、生成されるエンコード ビットストリームも H.264 に準拠しています。ClearPath は、コール セットアップ プロトコルに依存しないよう設計されているため、H.323 エンドポイント、SIP エンドポイント、および XMPP エンドポイントで使用できます。

ClearPath では次のようなテクノロジーによって、最良のユーザ エクスペリエンスが実現されています。

- 「ダイナミック ビット レート調整」（P.3-15）
- 「Long Term Reference Picture」（P.3-15）
- 「ビデオ対応の前方誤り訂正（FEC）」（P.3-15）

ダイナミック ビット レート調整

ダイナミック ビット レート調整は、使用できる可変帯域幅に合わせてコール レートを調整するものです。これにより、パケット損失の状況に基づいてコールの速度が上下します。ClearPath の場合、パケット損失が減少すると速度が上昇します。ClearPath では、RTCP を介して送信側プロアクティブ方式が使用されます。この場合、送信側では常に RTCP レシーバー レポートの確認が行われ、その内容に従ってビット レートが調整されます。

Long Term Reference Picture

長時間参照フレーム リカバリは、パケット損失の後に I フレームを使用することなくエンコーダ/デコーダの再同期化を行うための手法です。パケット損失が発生した場合は、従来の I フレームの代わりに修正 P フレームを使用することができます。これにより、フレームを復元するために転送するデータは約 90 % 少なくなります。

Long Term Reference Picture（LTRP）は、エンコーダおよびデコーダで保持される I フレームで、保持終了の明示的な信号を受信するまでその状態が維持されます。長時間参照フレームまたは LTRP の詳細については、「I フレーム」（P.3-5）を参照してください。

ビデオ対応の前方誤り訂正（FEC）

前方誤り訂正（FEC）では所定のアルゴリズムに従って、転送される情報に冗長性が付与されます。この冗長性があることにより、受信側では、メッセージのいずれかの箇所でエラーが発生した場合でもそれが一定数以下であれば、送信側に追加データを要求することなく、そのエラーを検出し訂正することができます。FEC では、受信側でエラーを訂正する場合、データの再送信を要求するためのリバース チャネルは必要ありませんが、その代わりとして、より高い転送チャネル帯域幅が常に必要となります。FEC では最も重要なデータ（通常は修正 P フレーム）が保護されます。これにより、それらのフレームは受信側で確実に受信されます。エンドポイントでは、帯域幅が 768 kbps を下回る場合 FEC は使用されません。また、1.5 % 以上のパケット損失が発生していない場合も FEC は適用されません。FEC の有効性は ClearPath によりモニタリングされます。FEC に有効性が認められない場合は、ClearPath により FEC の実行が中止されます。

CHAPTER 4

IP ビデオ ソリューションでのコール制御プロトコルと IPv6

プロトコルとは、デバイス間の通信に関する一連の仕様および規格を定めたものです。この章では、プロトコルについて網羅的な説明は行わず、プロトコルの機能や特性のうち、ビデオ コミュニケーションを取り扱ううえで重要度が高いものに重点を置いて説明します。

IP ビデオ ソリューションでのコール制御プロトコル

現在、多くの IP ビデオ ソリューションで使用されている主なコール制御プロトコルは、H.323、Session Initiation Protocol（SIP）、および Skinny Client Control Protocol（SCCP）です。

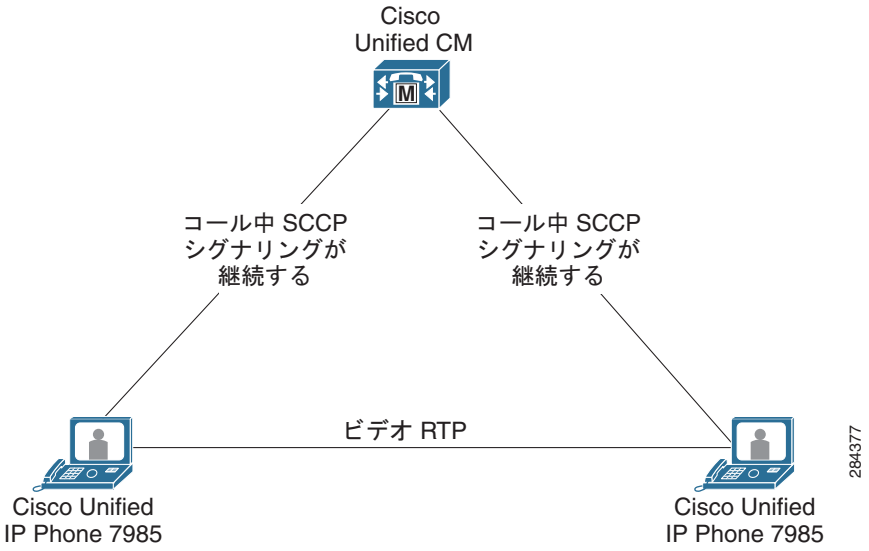
SCCP

Skinny Client Control Protocol（SCCP）は、シスコが IP テレフォニー アプリケーション用に初めて開発したものです。IP テレフォニーは進化する過程でビデオとの統合が行われました。それによって生まれたのが Cisco IP Video Telephony です。SCCP では、伝送制御プロトコル（TCP）が転送プロトコルとして指定されているほか、エンドポイントとアーキテクチャ上の関係（マスター / スレーブ関係とも呼ぶ）を持つコール エージェントが定義されています。SCCP と、このセクションで説明するその他のコール制御プロトコルとの最も根本的な違いは、このコール エージェントにあります。SCCP では、集中型のコール エージェントが採用されているため、他のコール制御プロトコルではまず不可能と思われる非常に高度なコール機能を実現することができます。

SCCP では、コール エージェントとエンドポイントとの間にマスター / スレーブ（クライアント / サーバ）関係が定義されているため、コール機能が実行されるためには、コール エージェントが常時エンドポイントから利用可能な状態にあることが必要です。そのため SCCP は、エンドポイントがコール エージェント コンポーネントとは独立に機能する必要がある環境には適さない場合があります。

図 4-1 は、Cisco Unified Communications Manager（Unified CM）をコール エージェントとして導入した場合の SCCP コール制御シグナリングの役割を図示したものです。

図 4-1　SCCP シグナリング



前述したように SCCP の仕様では、ビデオ環境において高度なコール機能がサポートされます。これらの機能のうち、保留、保留解除、ミュート、および会議は、通常の音声コールの場合とまったく同様に機能します。SCCP エンドポイントの機能の中で大きな特徴があるのは、アドホック ビデオ会議およびミュートです。アドホック ビデオ会議をサポートしているのは SCCP だけではありませんが、SCCP に加えて、予約なしのビデオ会議をビデオ エンドポイントに実装していることにより、ユーザはより簡単にアドホック ビデオ会議へ参加することができます。コール制御サーバが互換性のある SCCP MCU と連動している場合、ユーザは事前に会議の予約をしなくても、キーを 1 つ押すだけで SCCP ビデオ電話から会議を開始することができます。ここに、H.323 との大きな違いがあります。H.323 では予約なしの会議を確立する際、ユーザが常時接続の会議接続先にダイヤルする必要があります。

ビデオに関する SCCP のミュート機能も、他のプロトコルの場合とは動作に違いがあります。SCCP ビデオ端末上でミュートがアクティブになると、H.323 や SIP のミュート機能とは異なり、音声とビデオが同時にミュートになります。

SCCP では、ビデオ エンドポイント上で高度なコール機能が使用できるのは、そのテクノロジーおよびアーキテクチャが電話に類似しているためです。したがって、ビデオに対しても電話に似たレガシーな動作が一部強制されることになります。Uniform Resource Identifier（URI）ダイヤリングやデータ共有がサポートされていないのも、レガシーな動作に見られる特徴の 1 つです。このためビデオを導入する際に SCCP と他のプロトコルを併用する場合は、SCCP が持つアーキテクチャ上の制約を考慮することが重要です。表 4-1 は、SCCP で実装されないその他の機能をまとめたものです。ビデオに対して H.323 または SIP を併用する場合はこれらを考慮する必要があります。

表 4-1　SCCP で実装されない機能

SCCP で使用できない機能	結果	対処法（対処可能な場合）
ビデオ機能の動的な追加	音声コールをビデオ コールに切り替えられない	セッション開始時にビデオ機能が使用可能であること、およびブロードキャストされていることを確認する

表 4-1　SCCP で実装されない機能 （続き）

SCCP で使用できない機能	結果	対処法（対処可能な場合）
SCCP エンドポイントでの遠端カメラ制御（FECC）	リモート カメラの調整ができない	なし
ビデオ コーデックの再ネゴシエーション	再ネゴシエーションが行われるとコール セッションが終了することがある	なし

SCCP メッセージは 16 進数にエンコードされるため、伝送データから直接その内容を読み取ることは困難です。ただし、このエンコード メカニズムにより、SCCP メッセージは一般に他のコール制御プロトコルを使用したメッセージよりもサイズが小さくなります。たとえば、コール制御トラフィックが暗号化されていない場合、SIP 電話は平均 538 bps であるのに対し、SCCP 電話は平均 256 bps です。

この他、ビデオに対して SCCP を使用することにより、Secure Real-Time Transport Protocol（SRTP）およびトランスポート層セキュリティ（TLS）を介して、それぞれメディアおよびシグンナリングの認証および暗号化を行うことができるなどのメリットもあります。暗号化された場合、SIP 電話は平均 619 bps、SCCP ビデオ電話は平均 415 bps です。

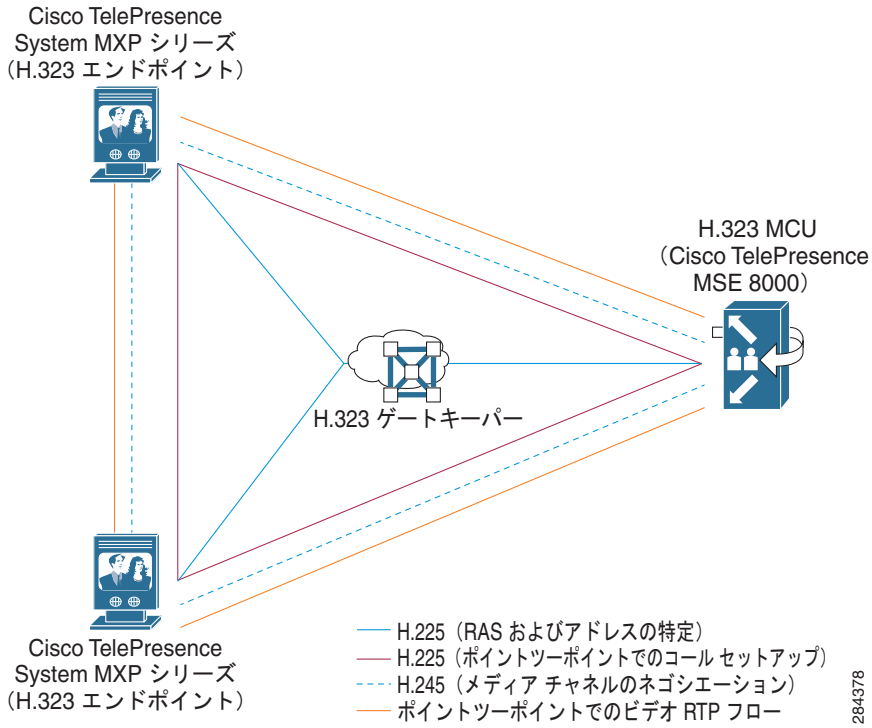
H.323

SCCP とは異なり、H.323 は単独の規格やプロトコルではなく、国際電気通信連合（ITU）の電気通信標準化部門（ITU-T）によって策定された複数のプロトコルおよび推奨事項を 1 つにまとめたものです。H.323 は、機能、想定される動作、および実装がきわめて厳密に定義されています。そのため H.323 は、通信ベンダーや通信プロバイダーの間の相互運用においては有利な立場にあります。H.323 の実装は、非常に明確に定義されているため、ベンダーの相互運用によって実現される事柄について、誤解が生じる余地はほとんどありません。

H.323 では、集中型のコール制御要素がなくてもユーザ間通信をサポートするピアツーピア プロトコル モデルが使用されます。H.323 は堅牢なため、さまざまなベンダーのエンドポイントとピアツーピア接続された、ゲートキーパーなどのコール制御要素が使用されるケースも珍しくありません。前述したように H.323 は複合的なプロトコルです。H.323 ピアでは、コール セットアップおよびコール アドミッション制御のネゴシエーションに H.225 が使用され、メディア チャネルのネゴシエーションに H.245 が使用されます。H.225 では、転送プロトコルとしてユーザ データグラム プロトコル（UDP）および TCP が使用されますが、H.245 で使用されるのは TCP のみです。これはファイアウォールには不便なように見えますが、H.323 はテレコミュニケーション業界に深く浸透しているため、ほとんどのファイアウォール ベンダーは H.323 パケットの効率的なインスペクションを実現しています。

図 4-2 は、ゲートキーパーをコール制御要素とした H.323 の使用例を図示したものです。

図 4-2　H.323 シグナリング



H.323 は、多種多様なビデオ会議機能を強力にサポートしています。中でも重要なのは、アプリケーション共有と遠端カメラ制御（FECC）です。H.323 エンドポイントでは、FECC に H.224 および H.281、データ共有に H.239 が使用されます。FECC およびアプリケーション共有が H.323 でサポートされていることは、アーキテクチャに関して H.323 と他のコール制御プロトコルとが大きく異なる点です。たとえば、SIP ではアプリケーション共有の実装方法が定義されていないのに対し、H.323 では Annex Q、および H.281 と H.224 の実装を通じてそれが明確に定義されています。H.323 の FECC の場合、カメラ制御命令は H.281 に組み込まれ、さらに H.224 でカプセル化されます。そのため RTP を使用すれば、既存のネットワーク インフラでも堅固な方法で FECC 命令を転送することができます。

H.323 では、アプリケーション共有についても、きわめて明確に定義されており、そのサポートは H.239 に従って行われます。H.239 では、予備的なビデオ チャネルの管理方法および追加方法が定義されているほか、追加したビデオ チャネルを介してアプリケーション ビデオを送信する方法も定義されています。さらに H.239 では、トークン システムを使用することにより、会議中同時に 1 人の参加者しかアプリケーション共有を利用できないようになっています。

H.323 と他のプロトコルとでは、一部の機能に大きな違いがあります。たとえば、一部の H.323 エンドポイントにはアドホック会議が実装されますが、H.323 ではそのアーキテクチャに、会議リソースのトラッキングを実行したり会議を確立したりするための集中型のコール制御要素は指定されていません。そのため、ほとんどの H.323 エンドポイントでは、アドホック会議を行う際にユーザが常時接続の会議ブリッジにダイヤルする必要があります。

また H.323 では H.235 によるメディア暗号化が定義されているものの、シグナリング暗号化の定義は H.323 の対象外であるという点も、H.323 と他のプロトコルとの違いの 1 つです。このため H.323 を実装する際、コール シグナリングを保護する必要がある場合は、TLS またはインターネット プロトコル セキュリティ（IPsec）を使用するのが一般的です。ただしベンダーが異なればコール シグナリングを保護する方法も異なるため、この場合にはベンダーが相異なるエンドポイント間の相互運用性に問題が生じる可能性があります。

H.323 の仕様は先進的ですが、H.323 の機能がサポートしているのはビデオと音声のみであり、インスタント メッセージやプレゼンスなどのサービスにまでサポートの範囲が拡張されることはありません。ビデオと音声以外の通信手段を追加的に組み込む可能性がある IP ビデオ ネットワークを設計する際は、H.323 が新しいサービスをサポートすることはないという点を十分考慮する必要があります。

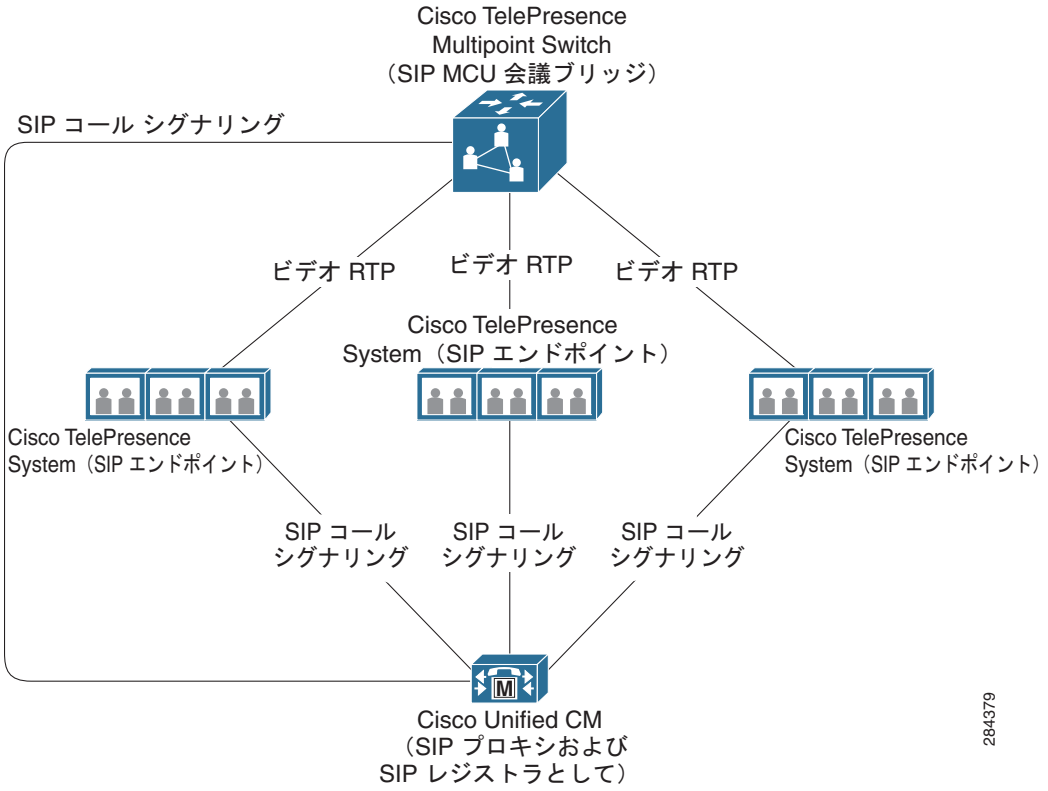
さらに、H.323 メッセージはバイナリ形式にエンコードされるため、適切なディセクタを使用することなくその内容を解釈することはかなり困難であり、プロトコル メッセージを実装した場合にはリトル エンディアンおよびビッグエンディアンのエラーが発生する可能性があります。H.323 メッセージは SIP メッセージよりサイズが小さいですが、帯域幅の差はほとんどありません。

SIP

Session Initiation Protocol（SIP）は、ピアツーピア プロトコルです。最も単純な実装では、SIP エンドポイント間で通信する場合、互いに相手の場所が認識できていれば、コール制御エンティティは必要ありません。ただし SIP では、エンドポイントからサービス、リソース、およびダイヤル可能な未知の接続先を利用できるように、クライアント/サーバ関係が定義されています。SIP は、インターネット技術特別調査委員会（IETF）によって定義されたもので、複数の Request for Comments（RFC）にまとめられています。SIP の根幹となるルールは RFC 3261 で定義されていますが、その他に SIP の規格に関する RFC が十数項目以上存在します。

企業への導入の際に SIP を使用した場合は、そのほとんどでコール制御要素（クライアント/サーバ モデル）が導入されます。それにより、機能の充実したユーザ エクスペリエンスを実現できるほか、ダイヤル可能なドメインの制御やコール制御の一元化が可能になります。SIP 要素には、ユーザ エージェント クライアント（UAC）およびユーザ エージェント サーバ（UAS）という 2 つの基本カテゴリがあります。他の要素への接続を要求する側の要素が UAS、その要求を受け取る側の要素が UAC です。セッション中、同一の要素がトランザクションごとに UAC になったり UAS になったりすることはありますが、対処するトランザクションは 1 つに限定されます。

図 4-3　SIP シグナリング



SIP は、音声通信およびビデオ通信の確立以外にも処理を行うことができるなどさまざまな観点から見て、テレコミュニケーション シグナリング プロトコルよりも通信セッション シグナリング プロトコルに分類するのが妥当です。SCCP および H.323 は単なるテレコミュニケーション プロトコルであるのに対し、SIP ではインスタント メッセージやプレゼンスなどを使用できます。SIP プロトコルの仕様には数多くのサービスをサポートできるという強みがありますが、その要因の 1 つとなっているのが、UAS 要素および UAC 要素では、認識できない事柄やサポートできない事柄が常に無視されるという事実です。ただし、これによってベンダー間の相互運用は煩雑になるため、場合によってはこの強みが SIP の短所の 1 つになることもあります。さらに SIP は、SCCP や H.323 に比べると仕様の内容が概略的であるため、ベンダー間の相互運用が円滑に行えない場合があります。たとえば SIP には、一部の機能を実装する方法が複数あります。同じ機能をベンダーごとに異なる方法で実装した場合、それらには互換性がありません。

他のコール シグナリング プロトコルで定義された機能の中には、SIP で定義されていないもの、またはそのコール シグナリング プロトコルの場合とは動作が異なるものが存在するという点にも注意が必要です。たとえば、RFC 4353 より以前には、アドホック会議の実装方法を定義した規格はなく、SIP の実装時には不明な点を補うためさまざまな手法が用いられました。Cisco IP Video Telephony の場合は、XML を使用して独自の手法を開発することによりアドホック会議が実装されました。

その他、アプリケーション共有も SIP では定義が不明確なものの 1 つです。実装の際には、'm'（media-type）属性を使用して、アプリケーション共有メディアを送信するタイミングおよび追加のビデオ チャネルを設定するタイミングを指定する場合があります。しかし、SIP ではこれらの機能を実装する方法が明確に定義されていないため、SIP ベンダー間のアプリケーション共有が円滑に行うことができません。

テキストベースである SIP では、8-bit Unicode Transformation Format（UTF-8）でエンコードされた ISO 10646 文字セットが使用されます。コール制御トラフィックが非暗号化モードの場合、SIP 電話は平均 538 bps であるのに対し、SCCP 電話は平均 256 bps です。SIP では、TCP または UDP を使用できます。SIP を実装する場合は通常、ポート 5060 が使用されますが、別のポート上で SIP を実装することもできます。

IP ビデオ ソリューションにおけるコール制御プロトコルの選択

IP ビデオ ソリューションの設計を問題なく行うためには、適切なプロトコルを選択することが重要です。不適切なプロトコルを選択すると、拡張性に関する問題が生じる可能性や、ユーザが目的の機能を実行できなくなる可能性があります。

IP ビデオ ソリューションまたはコール レッグ セクションに使用するコール制御プロトコルを選択する際は、次の点を考慮してください。

- 現在ユーザが必要としているコール機能、および将来実装を予定している機能は何か。（データ共有、暗号化など）
- どの転送プロトコル（TCP または UDP）を使用するか。コール制御プロトコルの中には、特定の転送プロトコルと相性の良いものがあります。
- ネットワーク アドレス変換トラバーサル（NAT-T）やディープ インスペクション（セキュリティ）などのネットワーク特性は必要か。場合によってはビデオ エンドポイントをファイアウォールの背後に配置する必要があるほか、NAT のサポートが必須である場合や、ペイロード暗号化が要件に含まれる場合もあります。
- どのような相互運用性が必要か（サードパーティの H.323 との相互運用性など）。また、どのようなタイプのエンドポイントおよび MCU を使用するか。全体の設計に合わせて選択したプロトコルをサポートしていないデバイスが、特定のコール レッグに含まれている場合があります。たとえば、常に音声が導入される IP PBX との相互運用性が必要となる一方、その IP PBX で H.323 が使用されているという場合があります。
- Business-to-Business（B2B）コミュニケーションは必要か。必要な場合は、B2B ベンダーを使用するのか、または第三者企業へ直接接続するのか。さらに B2B ベンダーを使用する場合は、その B2B ベンダーがどのコール制御プロトコルを実装しているのか。
- アプリケーション共有の要件をどのようなものにするか。たとえば、H.239 を必須とするか。

コール制御プロトコルの使用方法やロードマップについて収集できる情報が多いほど、意思決定のプロセスはより優れたものになります。目的のソリューションに特化または関連した追加情報があれば、プロトコルを選択する基準としてそれらを加味することを推奨します。

プロトコル選択のプロセスは、それに必要な情報をすべて収集した段階で開始することができます。プロトコルを選択する際は、次の点に十分な注意が必要です。

- 拡張性：収集した情報に基づいて、導入した IP ビデオ ソリューションが今後どの程度拡張されるか、またそれによって、選択されたプロトコルや導入されたコール制御要素にどのような影響があるのかを判断します。
- 使用例：目的通りの導入を実現するうえで重要性を持つコール フローや収集した要件に基づいて実際のシナリオを作成し、その内容を慎重に吟味しながらプロトコルがどのように影響するかを判断する必要があります。たとえば、ユーザがラップトップにアクセスせずビデオ エンドポイントを介してアプリケーションを共有するような場合であれば、プロトコルの選択肢は H.323 と SIP に絞られます。
- お客様の要件：要件の中には通常、使用例に関する要件にも拡張性に関する要件にも明確には分類できないものが存在します。プロトコルを選択するプロセスでは、要件に対してその重要性に応じた重みを割り当てることができます。

IP ビデオ ソリューションでの IPv6

IP バージョン 4（IPv4）は現在、割り当てることができるパブリック IP アドレスがほぼ枯渇状態にあります。ただし、大企業が運用を拡大できるように確保されたプライベート アドレスにはまだ余裕があります。とは言うもののモバイル デバイスでは、企業で使用される IP デバイスの台数が飛躍的に増加しており、こうした傾向が続けばいずれは IP version 6（IPv6）を実装して割り当て可能な IP アドレスの数を増やすことが必要となります。

そのため IPv6 を念頭に置いて今後の計画を立てておかないと、新型デバイスを接続できなくなったり、十分な Business-to-Business（B2B）機能を利用できなくなったりする懸念があります。ただし、現在でもプライベート アドレスには余裕があるため、こうした懸念が現実のものになるとしても、それはしばらく先のことです。

シスコではすでに、Cisco TelePresence C シリーズや Video Communication Server（VCS）など一部のデバイスで IPv6 をサポートする一方、IP ビデオ ポートフォリオのその他の製品にも IPv6 を組み込むための取り組みを進めています。ただし、現時点で IPv6 をサポートしている IP ビデオ機器の製造業者はそれほど多くありません。

ご使用のネットワークをどの時点で IPv6 に移行するかについての判断は、まず態勢を整え、そのネットワークの現状を把握し、IP アドレスの割り当てを追跡したうえで行うのが妥当です。IP ビデオ ソリューションを新たに導入する際は、選択した製造業者および製品に IPv6 の明確なロードマップがあることを確認した後、移行するためにどの程度の作業が必要になるかを把握し、それに基づいて計画を立てるようにしてください。

ご使用の IP ビデオ ソリューションで IPv4 デバイスと IPv6 デバイスのインターネットワーキングが必要な場合は、Cisco VCS を使用すれば IPv4 と IPv6 の間のアドレス変換を実行することができます。詳細については、次の URL にあるマニュアルを参照してください。

http://www.cisco.com/en/US/products/ps11337/prod_maintenance_guides_list.html

CHAPTER 5

QoS とコール アドミッション制御

ビデオ ストリームを構成するデータ パケットは、ネットワークを介して送信されます。パケットは、キューに入れられた順に宛先に到着します。シンプルなネットワークの動作では、最初にキューに入れられたパケットが最初に到着するパケットになります。単一の LAN スイッチでは、このプロセスはかなりシンプルになります。スイッチに、メディアを送信するポートと受信するポートがあるためです。ネットワークが増大するとともに、シナリオは、順序付けされたパケットの理想的世界から、順序付けされていないパケットの集まりに変わります。つまり、負荷を処理する十分なキャパシティがないネットワーク リンクを介して送信し切れない数のパケットが、同時に生成されます。このような現実的なシナリオでは、ネットワーク リンク間のパケット フローを制御するために、いくつかの方法が必要になります。

Quality of Service（QoS）

Quality of Service（QoS）を使用して、他のパケットより先に処理できる特定タイプのパケットを識別できます。異なるプライオリティを必要とするパケットに QoS 情報が挿入されます。

QoS は、高速道路とそれを利用する車に例えることができます。高速道路に例えられるのはネットワークです。ネットワークは、出発地から目的地まで移動する方法を車（QoS の場合はデータ パケット）に提供するからです。高速道路に十分な車線があり、事故がない場合、通常交通はスムーズに流れるので、移動時間は大部分のユーザに受け入れ可能な長さになります。しかし、交通量がピークのときは、事態はそれほどよくない場合があります。相乗り車線が役に立ちます。特定の基準を満たす車が、相乗り車線を利用し、交通渋滞をう回する特典を持ちます。また、救急車などの緊急公務には、他の交通量をう回できるさらに高いプライオリティが与えられます。一方、大型車や重い荷を積んだ車は、車線を余計に利用するため、交通を渋滞させる可能性があります。以上と QoS が似ているのは、QoS では特定のパケットがネットワークに優先的にアクセスし、キュー内の他のパケットより先に送信できるためです。

従来、IP パケットでは、3 ビットを使用して、IP Precedence またはタイプ オブ サービス（ToS）（RFC 791）が指定されていました。Differentiated Services（DiffServ）（RFC 2474 および RFC 2475）モデルでは、6 ビットを使用して、IP Precedence の値も保持されます。DiffServ モデルは、確認転送（RFC 2597）を使用してドロップ確率でさまざまなトラフィック クラスを定義するとともに、緊急転送（RFC 2598）を使用して低損失、低遅延、および低ジッター サービスを実現します。確認転送のクラスはさまざまなタイプのトラフィックをグループ化するのに使用され、ドロップ確率はパケットがドロップされ続けるトラフィックをグループ化するのに使用されます。緊急転送は、パケットのドロップと遅延による影響を受けやすい音声などのトラフィックに使用されます。

各トラフィック タイプには異なる QoS 値を設定できるため、ネットワークでは、高い QoS 値を持つと識別されたパケットは先に送信されます。表 5-1 に、さまざまな音声とビデオ トラフィックのタイプで使用される標準的な値をいくつか示します。

表 5-1　さまざまなトラフィック タイプの DiffServ コード ポイント（DSCP）値

トラフィック タイプ	レイヤ 2 サービス クラス（CoS）	レイヤ 3 IP Precedence	レイヤ 3 DSCP
コール シグナリング	3	3	CS3（24）
音声	5	5	EF（46）
ビデオ	4	4	AF41（34）
テレプレゼンス	4	4	CS4（32）

ボイスコールには、1 つのパケット ストリームしかありません。ビデオ コールにはビデオのストリームと音声のストリームの 2 つのストリームがあり、コールの両方のストリームに同じ QoS マーキングを設定する必要があります。

Cisco Unified Communications Manager（Unified CM）は、メディア パケット用に QoS をマーキングするエンドポイントをサポートします。音声パケットが EF（DSCP 値 46）としてマーキングされるのに対し、メディア パケットはビデオ デバイスにより AF41（DSCP 値 34）としてマーキングされ、TelePresence エンドポイントのトラフィックは CS4（DSCP 値 32）としてマーキングされます。すべてのコール シグナリングは CS3（DSCP 値 24）としてマーキングされます。

QoS は Cisco TelePresence Video Communication Server（VCS）で設定します。VCS がメディアおよびコール シグナリングを処理するからです。VCS に登録するエンドポイント（Cisco TelePresence System EX Series、C Series、Cisco IP Video Phone E20 など）は、そのエンドポイントのメディアを DSCP AF41 としてマーキングし、コール シグナリングが DSCP CS3 を使用するように設定する必要があります。

信頼境界

ネットワークのトラフィックは、ネットワークがそれを信頼できるようにするため、マーキングする必要があります。パケットを信頼するスイッチなどのネットワーク要素を信頼境界にすることができます。信頼境界を設定することは重要です。ネットワークの他の要素が QoS のためにパケットをあらためてマーキングしないで済むからです。アクセス スイッチは、IP Phone をそれとのアソシエーションに基づいて信頼することができます。Cisco のスイッチは、自身と Phone を関連付けるためにレイヤ 2 プロトコル、Cisco Discovery Protocol（CDP）を使用します。これらのスイッチは、CDP を使用して IP Phone を個々の音声 VLAN に配置します。これにより、アクセス スイッチはこれらの Phone を信頼して適切な QoS によりパケットをマーキングできるので、信頼境界を設定することができます。IP Phone がスイッチと関連付けできないか、あるいは信頼境界がアクセス スイッチまたはディストリビューション スイッチである必要がある場合、スイッチは、デバイスの IP アドレスあるいは、コールのためにシグナリングまたはメディアで使用される共通のポートなどの基準に基づいてパケットのマーキングを実施することで、信頼境界を作成することができます。

パケットのキューイング

ネットワークは、QoS を使用してさまざまなトラフィック タイプを識別し、プライオリティを設定する一方で、キューイング メカニズムを使用して順序に従ってパケットを転送し、フローを制御します。キューイングは、MAN ネットワークや WAN ネットワークなど、相互間のリンクが低キャパシティであるネットワークで広く使用されています。

ネットワークでよく使用されるキューイング メカニズムは次のとおりです。

- ファーストイン ファーストアウト（FIFO）

  このタイプのキューイングはシンプルで、同じ時間にキューに入れられたパケットはすべて同時に送信されます。パケットは、キューに入れられた順序で、スイッチまたはネットワークを介して送信されます。このタイプのキューイングは、パケット量の大きな変動がないネットワークで使用できます。

- プライオリティ キューイング（PQ）

  このタイプのキューイングでは、プライオリティが高いパケットが、プライオリティが低いパケットより先に送信されます。プライオリティ キューは、ボイスコールなど、遅延の影響を非常に受けやすい低帯域幅のトラフィックでよく使用されます。

- 重み付け均等化キューイング（WFQ）

  このタイプのキューイングでは、プライオリティ トラフィックおよび非プライオリティ トラフィックに対して複数のキューを使用します。これは、プライオリティの低いトラフィックがスタベーション状態にならないプライオリティ トラフィックを実現します。このメカニズムが使用されるのは、ネットワークで、プライオリティを必要とするトラフィック（音声トラフィックなど）や、ドロップできないビジネス アプリケーションなどの重要なトラフィックがある場合です。

- クラスベースの重み付け均等化キューイング（CBWFQ）

  このタイプのキューイングは、トラフィックをグループ化する複数のクラスと WFQ メカニズムを使用する一方で、カスタム キュー専用の帯域幅を用意します。このタイプのメカニズムは、ビジネス アプリケーションと結びついたインタラクティブな音声トラフィックおよびビデオ トラフィックで広く使用されています。このメカニズムには、さまざまなタイプの企業向けの導入に対して柔軟性があるというメリットがあります。

キューイング メカニズムは、組織のパケットでサービス クラス（CoS）を実現します。サービス クラスはレイテンシ、ジッター、および遅延の要件を保証するのに使用されます。また、それはリンクの帯域幅を効率的に使用して、組織が WAN リンクを介して送信できるトラフィックを見積もったり、目的のトラフィックをサポートできるようリンクを計画したりできるようにもします。

特定のキューがすべての帯域幅を使用しないように、トラフィックをポリシングすることが重要です。ポリシングは、特定タイプのトラフィックがリンクにおいて設定された使用制限を超えないようにします。ポリシングは、トラフィック シェーピングとともに、パケットのドロップを防止するほか non-critical トラフィックの処理を可能にするために必要です。

ビデオ コールでは、リップシンクの問題が発生しないよう、コールのビデオ ストリームと音声ストリームの両方を同じキューから送信することが重要です。ビデオ ストリームと音声ストリームで異なるキューを使用する場合、一方のストリームが他方のストリームより遅く到着するため、音声が遅延している間にその音声に関連するビデオが表示されたり、またはこの逆が起きたりします。

コール アドミッション制御

音声トラフィックとビデオ トラフィックがリンクの全帯域幅を使用せず、ビジネス アプリケーションなどの他の重要データのパケットがドロップしないようにするために、組織ではコール アドミッション制御を使用することができます。コール アドミッション制御は、サイト間の特定のリンクで使用可能なコール数を制限します。

リンクのコール数を制限する主な方法は、2 つあります。

- コールのカウント：この方法では、コール制御エージェントがロケーション間で使用可能なコール数をカウントします。同じタイプのコール別にのみカウントが行われるので、そのようなコールは、設定された音声コーデックおよび設定されたビデオ コーデックでは容易にカウントできます。
- 帯域幅：この方法はコールのカウントと基本的には同じですが、コールで使用される帯域幅の量をカウントする点が異なります。帯域幅のカウントには、音声コーデックのタイプとビデオ コールの帯域幅のタイプが使用されます。

コール品質を維持することが重要です。コールが WAN リンクを通過するときにリンクをオーバーサブスクライブすると、コール品質が低下する可能性があります。コール アドミッション制御は、リンクがコールでいっぱいにならないようにするために重要です。コール制御エージェントは、コールをルーティングする際に、コールを許可できるか、またはリンクがコールを処理できないかを判別します。これにより、ユーザは一貫したコール体験が可能になります。

Cisco Unified CM は、コール アドミッション制御を帯域幅方式でサポートします。これにより、さまざまなコーデック タイプおよびビデオ帯域幅タイプを含むコールが企業ネットワークでサポートできます。Unified CM は、地域のメカニズムを使用して、コーデックとビデオ帯域幅にコールごとのパラメータを指定します。また、Unified CM は、ロケーションのメカニズムを使用して、特定サイトの音声およびビデオ コールを制限するための帯域幅値を指定します。Cisco TelePresence VCS が使用する類似のメカニズムでは、リンクでコールごとの帯域幅を設定し、パイプでサイトに対して全コールの帯域幅を設定します。

コール アカウンティングのコール カウントおよび帯域幅方式では静的な設定値を使用しますが、実際のコールで使用される帯域幅はこの値より大きかったり小さかったりします。コールで使用される実際の帯域幅を特定するには、Resource Reservation Protocol（RSVP）が使用されます。このプロトコルは、メディアで使用されている実際のパスを確認して、コールに十分な帯域幅が使用可能かどうかを判定します。コールを処理できる帯域幅がパスのデバイスにない場合は、その状態が RSVP を介してレポートされ、コールが許可されない可能性があります。

Cisco Unified CM は、Cisco RSVP Agent という別個のメディア デバイスを使用し、ビデオ エンドポイントの代わりに RSVP を使用して、ネットワーク帯域幅についてネゴシエーションします。これにより、それを介した正確なアカウンティングが可能になります。

TelePresence コールでは、これらの技術によってユーザ エクスペリエンスを保証するためのトラフィックを可能にするようネットワークが設計されているため、コール アドミッション制御を使用しません。TelePresence のトラフィックは音声およびビデオとは異なる方法でマーキングされる、つまり別のキューに入れられるため、レイテンシと遅延が低く、ユーザ エクスペリエンスを保証することができます。

組織に複数のコール制御エージェントがある場合は、各エージェントが独自のコール アドミッション制御を行います。これらは、同時に動作しますが、相手の中を通過しているコールを認識できません。同じサイト内の 2 つの異なるコール制御エージェント間でコールが行われる場合、このコールの帯域幅を両方のエージェントがカウントします。これが WAN 帯域幅を使用しない場合でも、そうです。このため、組織内では、デバイスのコール アドミッション制御は、ただ 1 つのコール制御エージェントで行うことが重要です。

CHAPTER 6

ダイヤル プラン

固定電話および携帯電話のユーザは、番号をダイヤルして相手に電話します。番号ベースのダイヤルは、一般に E.164 または PSTN ダイヤルと呼ばれます。PSTN の番号には、国番号、市外局番、および市内番号などさまざまな要素があります。PSTN のサービス プロバイダーは、このダイヤルされた番号を市内番号、長距離番号、国際電話番号として解決し、発信者と受信者を接続します。同様に、組織では、外部ダイヤル トーンに 9 または 0 などのプレフィックスを使用して、サービスを識別します。ユーザはこのプレフィックスをダイヤルしてから、電話番号をダイヤルします。組織内の番号をダイヤルする場合にも、プレフィックスを使用することで、E.164 番号全体でなく短縮番号をダイヤルすることができます。組織によっては、簡略式のダイヤル プランを使用し、組織内のユーザが社内の同僚に電話するのに 4 桁または 5 桁の番号のみをダイヤルするようにしています。

これが、各ネットワークのユーザが相手に連絡できるよう、さまざまな会社、モバイル ネットワーク、および PSTN を接続するダイヤル プランの基礎になります。長距離電話や国際電話のコストを意識する組織では、番号ダイヤル プランを使用して電話を制限し、特定ユーザのみに長距離または国際電話のダイヤルを許可することができます。同様に、組織は、電話勧誘販売の業者からの迷惑電話をブロックできることも必要です。また、番号ベースのダイヤル プランを使用する場合は、電話ハッカーの侵入阻止方法も考えておく必要があります。

電子メールが導入されて以来、現代的なインターネットによるコミュニケーションが普及しています。電子メール アドレスは、ユーザを一意に識別する方法となり、いまや新しいアイデンティティになっています。このアイデンティティは、ユーザが Uniform Resource Identifier（URI）で表される場合にユーザに連絡するのに使用できます。チャットに使用されるインスタント メッセージでは URI が使用され、Voice over IP（VoIP）でも URI を使用してコールを送信します。URI の形式は *<user-id>*@*<domain-name>* です。この形式はユーザにとってわかりやすく、概して番号より記憶しやすいものになっています。

URI またはそれを使用するデバイスにコールがルーティングされるよう、URI で表されるエンティティを特定する高度なシステムが必要です。そのようなシステムでは、ドメインおよびそのドメインを表すサーバを識別できるだけでなく、コールも処理できることが必要です。少なくとも、ドメイン ネーム システム（DNS）などの外部の依存関係を考慮する必要があります。H.323 などのさまざまな VoIP プロトコルではこの目的で Electronic Numbering（ENUM）を使用する場合がありますが、この方式は広くは使用されていません。URI のダイヤルは、Web 技術に由来する SIP によりさらに一般的になりました。さまざまなタイプのダイヤル方式があることで、ユーザや企業はフレキシブルな方法で電話をかけることができ、到達可能性が提供されますが、それらさまざまなタイプのダイヤル エクスペリエンスをユーザに提供するシステム間のトランスレーションをうまく行うなんらかの方法が必要になります。

ダイヤル プランの依存関係

PSTN の広範な到達範囲について議論する場合、ダイヤル プランの依存関係を把握することが重要です。

- E.164 ベースのダイヤル プランでは、可変の桁数を使用できます。サービス プロバイダーとテレフォニー システムは可変長の着信者番号に対応できる必要があり、ユーザはそのような番号をダイヤルすることに慣れる必要があります。さまざまな長さの着信者番号がある場合、サービス プロバイダーによるそれらの番号の処理方法は、組織によるそれらの処理方法と異なります。サービス プロバイダーでは発信者 ID の番号を標準化する必要があるのに対し、組織では、ダイヤル イン（DID）または国固有のダイヤル プランのために番号を標準化する必要があり、このため発信番号または着信者番号をトランスフォームする必要が生じることがあります。
- 音声およびビデオ システムを外界に接続するには、PSTN または IP 接続で、他のデバイスとの間で発信および着信できることが必要です。IP ベースのシステムは、外部ネットワークへの接続を必要とし、直接ピアリングを使用するか、または IP ネットワークを介してダイヤル プランを解決するその他なんらかのメカニズムを使用する必要があります。
- IP ベースのネットワーク同士のダイヤル プランを解決するには、いくつかのメカニズムが必要です。
  - 番号ベースの発信には、Electronic Numbering（ENUM）が使用されます。ENUM により、E.164 の番号を対応する IP アドレスにトランスレーションすることができます。このサービスは ENUM サーバによって提供されます。このサービスのサブスクリプションとネットワーク接続が必要なほか、DNS サービスも必要です。
  - DNS サービス（SRV）は、URI によるダイヤルをサポートするシステムに必要です。DNS SRV のレコードは、ドメイン ネーム情報のほかに、H.323 または SIP プロトコル、UDP または TCP タイプ、およびコール エージェントが使用できる追加のパラメータなどのコール サービスに関する情報を提供します。コール エージェントはこの情報を使用してコールをホストに送信します。
- 1 人のユーザが、複数のエンドポイントまたはデバイスを持つことがあります。このような場合、単一の番号または URI がダイヤルされたときでも、ダイヤル プランではすべてのユーザ デバイスに到達できる必要があります。このため、番号ベースのシステムは共有回線をサポートする必要があり、URI ベースのシステムはエイリアスをサポートする必要があります。

番号ベースのダイヤル プラン ネットワーク

番号ダイヤル プランは最も広く導入されています。PSTN システムおよび H.323 システムでは、番号を使用してエンドポイントに到達します。PSTN システムおよび IP PBX システムでは、独自のダイヤル プランを持ち、エンドポイントに番号を割り当てています。エンドポイントにはダイヤル プランがあり、エンドポイントはコールをルーティングできるようダイヤル プランをシステムと共有するので、H.323 ネットワークはダイヤル プランをエンドポイントから取得します。これらのシステムのダイヤル プランを解決するために、ダイヤルされた番号の完全一致または最上位桁の一致が使用されます。

米国の E.911 ネットワークなどの緊急医療サービス ネットワークは、別のタイプの番号によるダイヤルを使用するシステムです。番号によるダイヤルは、サービスに到達するためだけでなく、発信者に到達するためにも使用されます。これは、救急医療サービスを提供するために発信者のロケーションに関する追加情報を使用できるからです。

URI ベースのダイヤル プラン ネットワーク

ソフトウェア ベースのビデオ エンドポイントを使用すると、URI に簡単にダイヤルできます。これは、ほとんどのアプリケーションでは、ワン クリック コール機能を提供することで、さらに簡単になっています。電子メール ID によって簡単にダイヤルできることは、ユーザにとって非常に魅力的です。大部分の導入では、Lightweight Directory Access Protocol（LDAP）などの一般的なディレクトリ サービスを使用して共通のアイデンティティ システムを参照し、ユーザがダイヤルできるよう電子メール ID を提供します。このため、組織の LDAP システム外への発信には、外部の依存関係が使用されます。

DNS は、インスタント メッセージ システムと同様に、ドメインを使用してコールをルーティングできるよう、ドメインに関する情報を提供します。DNS は、一般的ネットワークとして Business-to-Business（B2B）コミュニケーションに広く使用されている最も一般的なシステムです。DNS では、組織が相互に外部コールを行えるよう、組織への接続方法が入手可能です。

ダイヤル プランによるコールの解決

コール エージェントは、ダイヤル情報を使用して、コールをルーティングする方法を決定します。電話番号の一般的な処理方法では、番号の完全一致または、コール エージェントが処理するルートの最上位桁の一致が使用されます。エンドポイントには固有の E.164 番号があります。コール エージェントは、国固有の情報またはプレフィックス情報を識別して、個々のエンドポイントまたは着信者番号を処理するネイバーへのコール送信を決定することができます。また、コール エージェントは救急医療サービスおよび市内電話のコールを解決して、コールがローカル ゲートウェイに送信されるようにする必要があります。番号によるダイヤルの場合、ローカル エリア コードのコンセプトは、コールをローカル リソースに送信するか、またはローカルでないシステムに送信するかを識別する手段として役に立ちます。

デバイスを URI に登録することによっても、ユーザは固有性を利用できるようになります。コール エージェントが URI に基づいて宛先を識別できるようになるからです。複数のロケーションにまたがる複数のサーバで 1 つのドメインを処理できるため、コール エージェントはドメインおよび、特定の URI として登録されているサーバを解決できる必要があります。宛先のロケーションが使用不能な場合は、救急医療サービス、ローカル IP トランク、またはホップ オフ ゲートウェイへのコールの解決を決定するその他の方法が必要です。また、URI を使用して会議サービス用にルーティングする必要があるコール エージェントは、参加者に最も近い会議ブリッジを選択できる必要があります。

PSTN アクセス

外界への通信には、PSTN へのインターフェイスと IP ネットワークが必要です。ISDN 経由で PSTN に接続するゲートウェイは、PSTN への音声接続を可能にします。このゲートウェイは、番号ベースの PSTN ネットワークとのインターフェイスを取るときに、発信者番号と着信者番号を標準化する重要機能を備えています。PSTN ゲートウェイには、電話ハッカーの侵入阻止を使用する必要があります。

ボーダー要素または IP ゲートウェイは、サービス プロバイダーまたは一般のインターネットを介して、IP ベースの PSTN への接続を可能にします。このゲートウェイは、社内 IP ネットワークのトポロジ非表示機能とコールの標準化機能を備えています。このゲートウェイは、サービス拒否攻撃およびそれを危殆化する試行を防止する追加のセキュリティ対策を備える必要があります。

変換

コール エージェントは、発信者の情報を標準化するために、発信者番号および着信者番号を透過的に変更することで、ダイヤル プランを変換します。変換は、コールのユーザ情報を標準化する、コール エージェントの重要機能です。これは、応答されなかったコールの情報を中継するためにも重要です。これにより、ユーザが電話する時間があるときに、発信者に折り返しダイヤルできるからです。組織では、変換を使用して、発信者 ID をマスクしたり、標準化された一般的なフォーマットでコールバック情報を表示したりしています。PSTN コールでは、組織はユーザの社内番号を公開せずに、発信用のパブリック番号を使用します。URI ベースのシステムでは、変換を使用して、ドメイン内のコールおよび外部組織からのコールを標準化します。

また、組織によっては、DID を使用して社内ユーザを外部の ISDN 回線にオーバーサブスクライブします。これにより、組織はそのすべてのユーザにエンドポイントを提供すると同時に、外部コール用に適切な回線を選択することができます。URI への登録により、オーバーサブスクリプションの概念は、エンドポイントの番号範囲でなく、コールで使用されるキャパシティに制限されます。

ダイヤル プランの操作

コール ルーティングを支援するため、さまざまなシステム要素における発信者情報または着信者情報のいろいろな要素が変更されます。発信者情報を操作するのは、発信者または着信者に表示される情報が標準化されるようにするためです。これはまた、コールが応答されず、ユーザが不在着信または着信に関する情報を参照する必要がある場合にも役立ちます。番号によるダイヤル プランの場合、このような目標は簡単に達成できますが、URI によるダイヤルの場合、コール エージェントには目的の目標を達成するためのメカニズムが必要となります。

コール エージェントは発信者情報を操作してコールを解決します。コール エージェントは、番号を E.164 形式に変更してルーティングするために、市外局番を追加することができます。このような操作を実現するには、基本的なパターン マッチングおよび置換機能が必要になる場合があります。URI でのダイヤルの場合は、コール エージェントが URI を処理するために、ドメインの標準化を使用できます。英数字コンテンツの検索および置換機能を実現するには、正規表現を使用した精巧なメソッドが必要です。正規表現を使用すると、英数字の URI 形式に柔軟にマッチングできるようになりますが、数字によるダイヤル プランの操作ほど簡単ではない場合があります。

制限のクラス

一般に、組織では、ユーザによって特定のサービスへのアクセスを許可したり拒否したりします。最も一般的なケースは、長距離電話および国際電話に対する制限です。発信者および着信者に関する制限は、発信者番号および着信者番号を使用する場合は簡単に実装および導入できますが、URI によるダイヤルの場合は複雑になる可能性があります。また、制限を使用して、フリーダイヤルの宛先への発信と電話勧誘販売業者からの着信を防止することもできます。番号によるダイヤル プランは、1-888 のコレクト コール番号などの番号範囲を認識してコールをブロックするために使用できます。URI によるダイヤルでは、これは困難な場合があります。URI に基づいてコールを制限するには、制限する URI のリストが必要なだけでなく、これらの URI をコール エージェントが設定して、コールの制限クラス ポリシーを定義しておく必要があるためです。

CHAPTER 7

ビデオ ネットワークの導入ガイドライン

ビデオ ネットワークは、導入時に、可能な範囲で最高のユーザ エクスペリエンスを提供できるように設計、計画、および実装することが不可欠です。ビデオは、コール中にさまざまな参加者の認識の影響を受けるアプリケーションです。ミーティングやコラボレーション作業のビデオ ユーザの 1 人が満足の行くエクスペリエンスを持てない場合、その認識は他の参加者にもすぐに伝染しがちです。

以下の項で、ビデオ ネットワークを設計するための一般的ガイドラインを示します。

ビデオの導入トポロジの計画

ビデオ アプリケーションを導入する場合、組織のニーズを満たすために導入される、または導入する必要のある 1 つまたは複数のトポロジを選定し、計画する必要があります。現行のビデオ アプリケーションでは、主に以下のビデオ導入トポロジ モデルが使用されます。

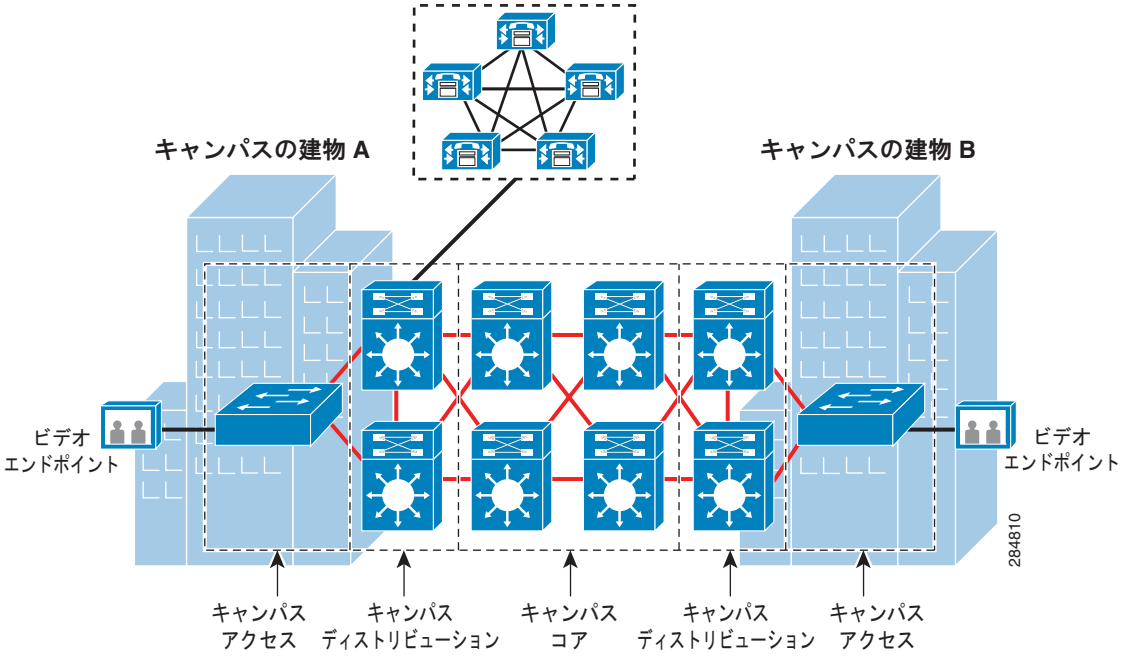
また、ビデオ アプリケーションでは、主に以下のコール処理モデルが使用されます。

以下の項で、これらの導入モデルの概要と、コール処理モデルおよびトポロジの選択ガイドラインを示します。

キャンパス内

ビデオのキャンパス内トポロジは、単一の企業サイトまたはキャンパスでビデオを提供することのみを目的としています。このトポロジ モデルは、ユーザをファシリティ間で移動させることなく、ミーティングの効率および生産性を向上させる必要のある企業に適しています。キャンパス内ビデオ導入モデルは、組織のニーズを満たすために、企業内トポロジ モデルおよび企業間トポロジ モデルとともに使用できます。図 7-1 に、単一サイト コール処理を使用したキャンパス内トポロジを示します。

図 7-1　　2 つのビルでのキャンパス内導入（ビデオ エンドポイント以外のすべてを一方のビルへ）



コール処理に関しては、単一サイト コール処理モデルおよびホステッド コール処理モデルが、キャンパス内ビデオ トポロジ モデルに適しています。どちらにするかの決定は、エンドポイントの密度、ネットワーク増大計画、必要な機能、およびコストに大きく依存します。

たとえば、ホステッド ビデオ コール処理導入モデルは、低コストの投資で、機能が非常に豊富なエクスペリエンスを提供します。ただし、いくつかのローカルなマルチポイント呼フローでは、ビデオ埋め込み型ビデオ リソースがない場合や、ユーザ密度が増大するとともにキャパシティが不足したために帯域とコストの関係が重大なファクタになっている場合に、メディア ストリームが構外に転送される必要が生じることがあります。

他方、単一サイト コール処理モデルには高い初期投資がかかります。これは、機能を利用するためにハードウェアやソフトウェアのライセンスが必要なためです。それでも、単一サイト コール処理モデルでは、導入後の低コストでのユーザ数増大が可能です。

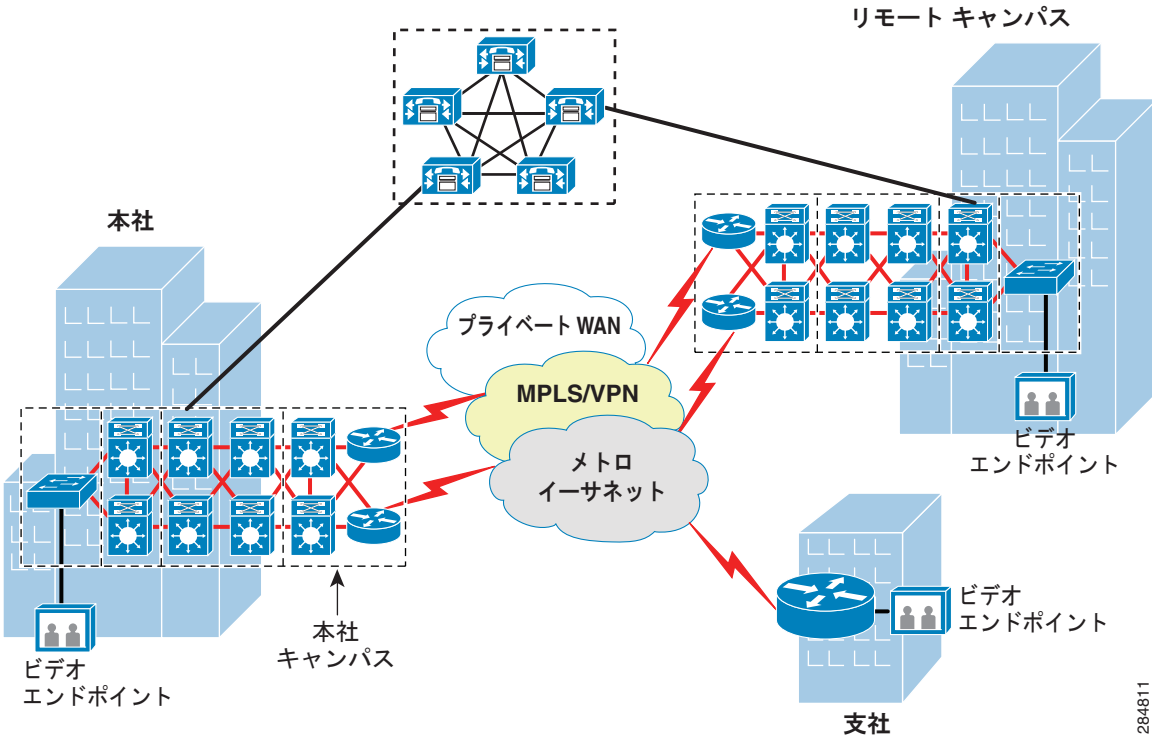
企業内

ビデオの企業内トポロジでは、同じ企業内の複数のサイトで、WAN を介してビデオ アプリケーションを使用することができます。企業内導入モデルは、従業員が社内ミーティングのために頻繁に遠距離まで出張する必要がある企業に適しています。企業内にビデオを導入すると、出張時間の節約と豊富な機能によるコラボレーションによって生産性が向上するだけでなく、出張旅費も削減できます。また、出張の必要がなくなるので、通常従業員のワーク ライフ バランスが改善されます。

企業内トポロジで複数のサイトにまたがるビデオを可能にするには、快適なビデオ エクスペリエンスを提供するため、高速な WAN リンクを利用する必要があります。WAN リンクのダイメンショニングの詳細については、「拡張性とパフォーマンス」（P.7-16）を参照してください。

図 7-2 に、複数サイト コール処理導入モデルを使用する企業内トポロジを示します。

図 7-2　複数のサイトへの分散型 Multi-Site Cisco Unified Communications Manager の導入



企業内導入では、複数サイト コール処理導入モデルまたはホステッド コール処理導入モデルを使用することができます。2 つのコール処理モデルのどちらにするかを決定する際は、キャンパス内の導入と同じ考慮事項が該当します。

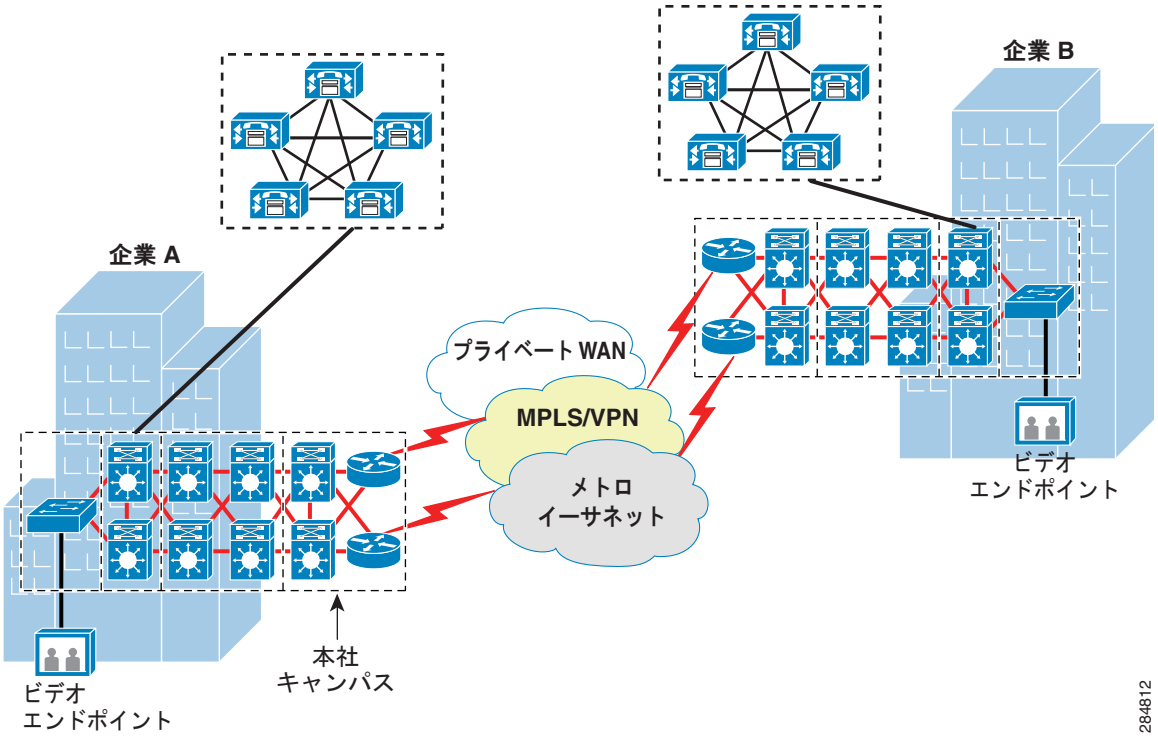
企業間（Business-to-Business（B2B））

企業間ネットワーク導入モデルは、企業内のビデオ エンドポイントを接続するだけでなく、企業内のビデオ エンドポイントが別の企業内のシステムに発呼できるようにします。企業間モデルは、複数の企業間の接続を含むようにキャンパス内モデルや企業内モデルを拡張したものです。これは Business-to-Business（B2B）ビデオ導入モデルとも呼ばれます。

企業間モデルは、柔軟性が最も高く、従業員が社内および社外ミーティングのために頻繁に遠距離まで出張する必要がある企業に適しています。企業内モデルが企業にとって持つメリットのほかに、B2B トポロジ導入モデルでは、従業員が、関連する出張の時間および費用のコストをかけずに、高度な顧客関係を維持することができます。

図 7-3 に、企業間トポロジおよび単一サイト コール処理を使用してコミュニケーションを行っている 2 つの企業を示します。

図 7-3　　各企業で単一サイト コール処理を使用した企業間（B2B）導入

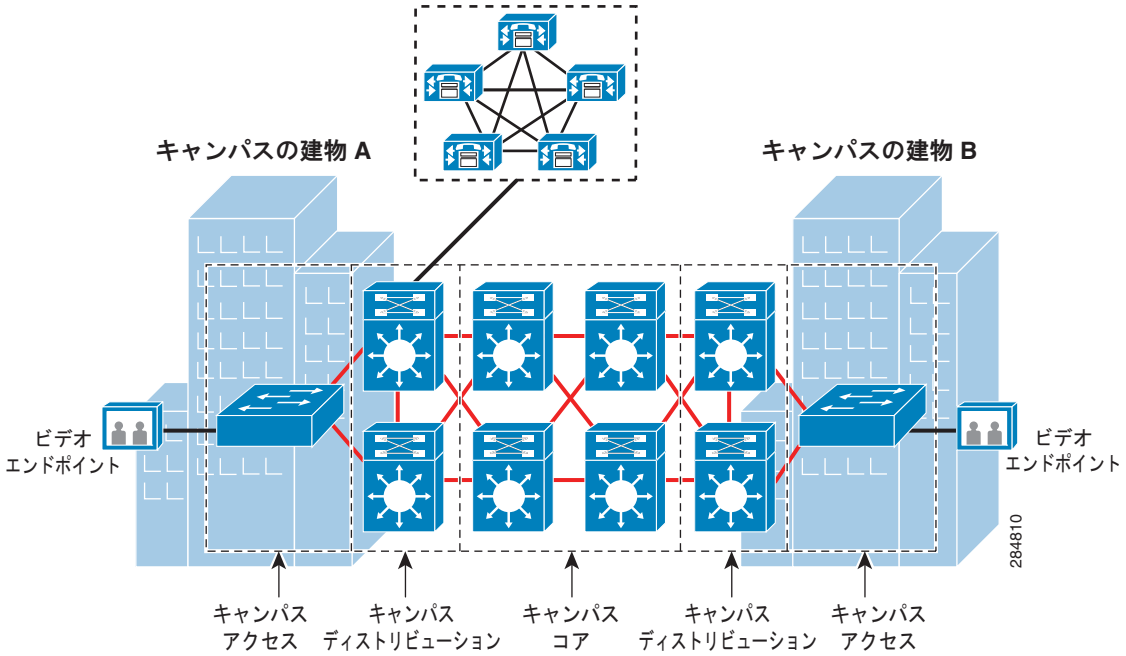


3 つのコール処理導入モデルはすべて企業間導入モデルと連携でき、キャンパス内導入および企業内導入と同じ考慮事項が該当します。

単一サイト コール処理

単一サイト コール処理モデルでは、コール処理は単一サイトのみを処理し、コール処理エージェントは処理されるエンドポイントと同じロケーションに存在します。コール処理エージェントとエンドポイントの距離は、その遠近に関係なく、LAN の速度のリンクで処理する必要があります。単一サイト モデルは、中規模の企業および政府機関に適しています。これらの組織は、1 つのサイトに存在し、基本的なビデオ コール処理ニーズがありますが、ネットワークが爆発的に増大しているか、ユーザ密度が非常に高いため、ホステッド ソリューションの帯域とコストの比率がひどく高くなっています。図 7-4 に、単一サイト コール処理を使用したキャンパス内トポロジを示します。

図 7-4　2 つのビルでのキャンパス内導入（ビデオ エンドポイント以外のすべてを一方のビルへ）

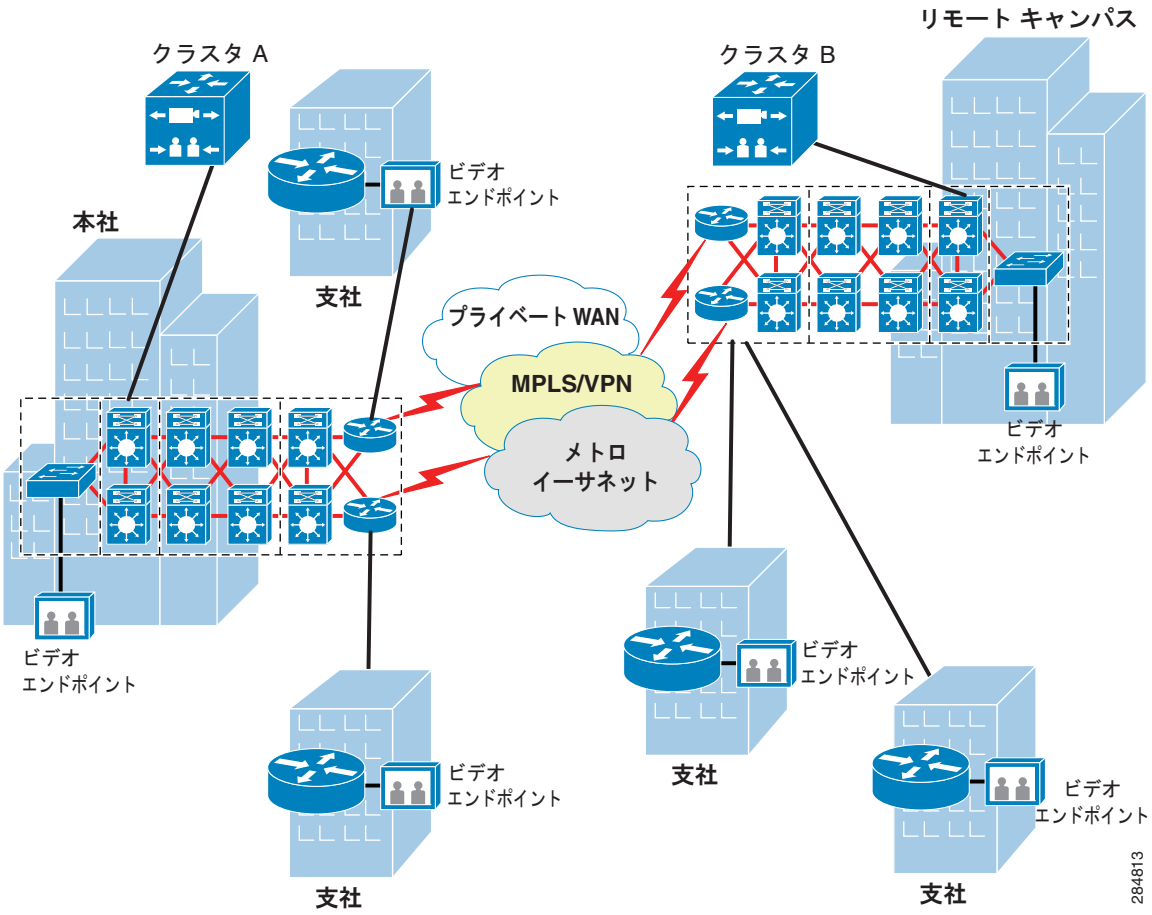


複数サイト コール処理

複数サイト コール処理モデルでは、すべてのコール処理エージェントが同じロケーションに存在してもかまいません（集中型複数サイト コール処理）。あるいは、ユーザ密度が高いか、またはサービスがきわめて重要なためにバックアップが必要な場合には、複数のロケーションに分散することもできます。

同じコール処理エージェント クラスタ内では、複数サイト コール処理は、集中型または分散型複数サイト コール処理モデルを使用して、さまざまなトポロジ（例、ハブ アンド スポーク トポロジおよび複数ハブ アンド スポーク トポロジ）を処理することができます。図 7-5 に分散型コール処理モデルを示します。このモデルでは、複数サイト コール処理導入により、コール処理サービスのための大規模な分散型コール処理モデル（複数ハブ アンド スポーク）に応じて、大きな集中サイトおよび複数のリモート サイトまたは支社サイト、ならびにホーム オフィス サイトまたは小さな支社が処理されています。

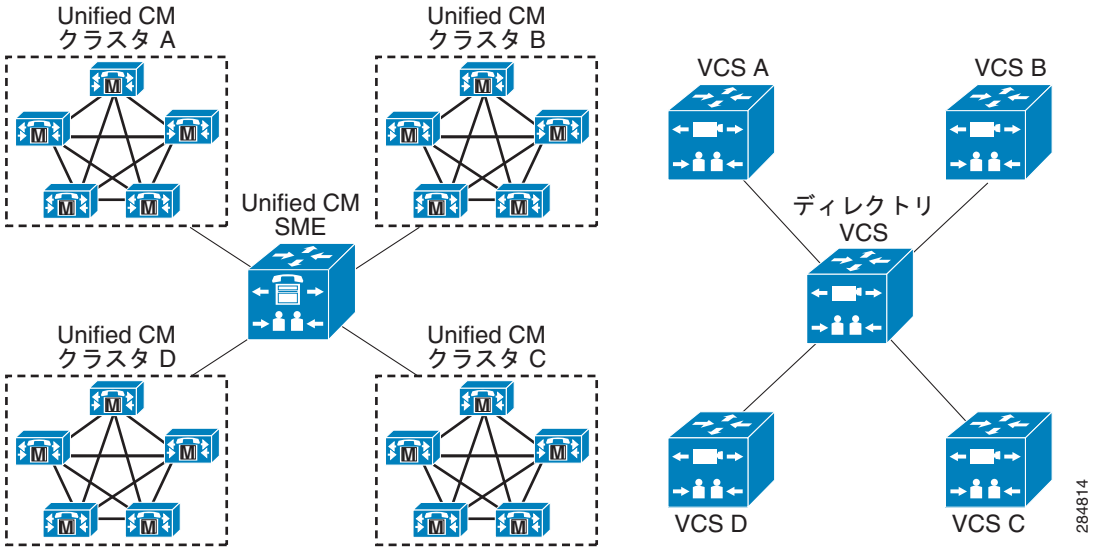
図 7-5　分散型複数サイト コール処理



複数サイト コール処理モデルに含まれる別の導入では、クラスタ化されたコール処理エージェントが、クラスタ間のコール ルーティングを集約するためだけに導入されたコール処理素を介して、他のクラスタ化されたコール処理エージェントと通信できます。集約コール処理エンティティの導入は、すべてのコール処理クラスタ間のフル メッシュ接続を実装しなくても済むというメリットがあります。その代わりに、さまざまなリーフ クラスタが相互に通信する際には集約コール処理要素と連携します。階層を作成し、ソリューション全体のキャパシティを増大できるよう正しくダイヤル プランを作成した場合は、新しいリーフ クラスタを追加したときでも、リーフ クラスタでのダイヤル プランの更新は必要ありません。

図 7-6 に、複数サイト集約コール処理導入の 2 つの例を示します。1 つは Cisco Unified Communications Manager Session Management Edition（SME）を使用している例で、もう 1 つは Cisco TelePresence Video Communication Server（VCS）をディレクトリ ゲートキーパーとして使用している例です。

図 7-6　　複数サイト集約コール処理導入の 2 つの例



（注）　H.323 ゲートキーパーではクラスタ（代替ゲートキーパー）の概念は使用できますが、H.323 ゲートキーパーは自己決定のコール ルーティング エンティティであるため、単一のゲートキーパーも、上記の議論においてはクラスタ化されたコール処理エージェントとみなされます。

ホステッド コール処理サービスとしてのビデオ

ホステッド導入モデルは、クラウドによって提供および管理されるサービスのことです。このサービスは、所有コスト（投資額）が低く、機能豊富なエクスペリエンスを提供する点で魅力的です。ホステッド ビデオ ソリューションは、中堅および中小企業をターゲットとし、それらの企業にエンタープライズ グレードのビデオを低コストで導入できるようにします。また、ホステッド ソリューションによっては、ビジネスが成長しても元の投資対象を維持できる移行パスが用意されています。

この導入モデルでは、コール処理要素以外のものもしばしば構外に配置されるため、いくつかのマルチポイント コール フロー シナリオではビデオ ストリームを構外に転送する必要があります。そのような場合、サービス ロケーションのユーザ密度が高いと、帯域を広くしてそれらを処理する必要が生じます。

コール処理トポロジとビデオ エンドポイントの選択ガイドライン

ビデオ ネットワークを導入または拡張するために適切な要素と導入モデルを選択することは、目的の機能、パフォーマンス、および拡張性を確実に実現するうえで有益です。それどころか、ビデオ ネットワーク用に不適切な要素やモデルを選択すると、組織が必要とする機能を実現するのに高コストの変更が必要となる場合もあります。

以下の項で、ビデオ ネットワーク用に要素および導入モデルを選択するための一般的ガイドラインを示します。

- 「コール処理モデルとコール処理エージェントの選択ガイドライン」（P.7-8）
- 「エンドポイントの選択ガイドライン」（P.7-9）
- 「ビデオ ネットワークの設計上の考慮事項」（P.7-9）

呼シグナリング プロトコルの選択の詳細については、「IP ビデオ ソリューションでのコール制御プロトコルと IPv6」（P.4-1）の章を参照してください。

コール処理モデルとコール処理エージェントの選択ガイドライン

適切なコール処理エージェントとその導入モデルおよびトポロジを選択するには、導入の設計フェーズで組織の要件に加えて以下の点を考慮することが重要です。

- 導入の成功基準としての使用目的を実現するためには、どの機能が必要か。例、SIP、SRTP、BFCP、または IPv6 ビデオ サポート。
- ビデオ エンドポイントは処理が必要なネットワークにすでに導入されているか。新しく選択したコール エージェントによるサービスが必要な以前のビデオ エンドポイント、および以前のビデオ ネットワークとの相互作用などに対する要件があるか。
- 導入に含める以前のビデオ要素がある場合、それはどのプロトコルを使用しているか、または使用できるか。例、マルチプロトコル エンドポイント（SIP および H.323）あるいはシングルプロトコル エンドポイント。
- コール制御プロトコルは選択されているか。選択されていない場合、特定のコール制御プロトコルに依存する機能はあるか。たとえば、H.239 は H.323 とともにのみ使用できます。
- ビデオ サービスを必要とするロケーションはどこか。そのユーザ密度はいくつか。個々のロケーションにとって冗長性はどれぐらい重要か。ユーザ密度が高いサイトごとに冗長性の用途をコール エージェントに提供すること（分散型コール処理）を推奨します。また、ユーザ密度が非常に高いと、特定のホステッド コール処理のコール フローでは、脅威（インターネット帯域利用率）となります。
- プロトコルのインターワーキングを使用するか。インターワーキングは特定の状況下でコール エージェントの配置に大きく影響します。これは、メディア ストリームが宛先に到達するためにコール処理エージェントを通過する必要が生じる場合があるためです。
- 処理する必要があるビデオ コールの最大数はいくらか。1 台の Cisco TelePresence Video Communication Server（VCS）7.0 の非トラバーサル コール数は最大で 500 です。これを超える残りのコールを処理するには、（クラスタ内に、またはスタンドアロンで）2 台目の VCS が必要です。

これらの考慮事項とお客様の要件、製品データ シート、および製品リリース ノートを考慮することで、選択するコール処理エージェントと使用するコール処理モデルおよびトポロジが決まります。たとえば、要件にアプリケーション共有技術としての BFCP の使用と、最大 2000 コールの処理が含まれている場合は、VCS クラスタが最適な選択となります。

エンドポイントの選択ガイドライン

ジョブに適切なエンドポイントを選択することは、コール処理エージェントの選択とほぼ同じぐらい重要です。お客様の要件に加えて、以下の点が選択の決定に役立ちます。

- H.323 と SIP のどちらのコール制御プロトコルが使用されるか。
- ビデオ会議には埋め込み型ビデオ リソースは必要か。そのような場合は、Cisco TelePresence System EX90 が適した選択肢です。
- どのようなビデオ解像度フォーマットが必要か。例、HD 720p。
- 選択しようとしている特定のエンドポイントとともにコールに関与する他のエンドポイントはどれか。例、Cisco Unified IP Phone 9971。
- どのようなアプリケーション共有技術が必要か。例、BFCP over UDP。
- モビリティ要件はどのようなものか。このエンドポイントはモバイル エンドポイント（コラボレーション タブレット）になるか。

これらの考慮事項とお客様の要件、製品データ シート、および製品リリース ノートを考慮することで、選択するエンドポイントが決まります。

ビデオ ネットワークの設計上の考慮事項

ビデオ ネットワークを設計する際には、インターワーキングの影響を考えることが重要です。インターワーキングを使用する場合、選択したコール処理エージェントに応じて、メディア ストリームがコール エージェントを通過する必要が生じることがあります。このため、コール処理エージェントがコールに関係するエンドポイントからリモートにある場合は、呼がポイント間で転送されないため、インターワーキングが帯域利用率に悪影響を及ぼす可能性があります。

また、DNS SRV レコードは通常拡張性を持たせるために使用されます（SRV レコードを使用すると、システムの統合に必要な SIP トランク数が減少する）が、コール処理エージェントは、DNS SRV レコードに対してはエンドポイント登録およびコール処理ピアリングに関して異なる方法で動作します。この動作の違いが異なるコール エージェントを統合する前に理解されていない場合に統合しようとすると、予期しない状況が発生する可能性があります。

ビデオ リソースの割り当て

処理する物理ロケーションが 1 か複数かに関係なく、ビデオ リソースの最適なネットワーク ロケーションを決定するために検討が必要となる考慮事項がいくつかあります。ビデオ リソースは専用、埋め込み型のいずれでもかまいません。埋め込み型ビデオ リソースは、エンドポイント内にあり、自身を含むエンドポイントに対してのみコールを処理します。他方、専用ビデオ リソースは、エンドポイントとは別のアプライアンス内にあり、自身にアクセスするすべてのエンドポイントを処理します。

必要なユーザ エクスペリエンス レベル（および通常、妥当な冗長性および可用性レベルも）を実現するには、ビデオ リソースを適切に分散することが必要です。考慮するファクタが多いほど、ビデオ リソースのロケーション決定が信頼できるものとなります。ビデオ リソースの最適な割り当てモデルおよびロケーションを決定する選択プロセスには、以下のファクタを織り込む必要があります。

- 支社で使用可能な帯域
- 帯域コスト
- リモートのビデオ リソースのコスト
- 本社およびリモート サイトの使用パターン
- コール エージェント ブリッジ グループ選択アルゴリズム
- ビデオ リソースのタイプ

導入に専用ビデオ リソースを割り当てるには、以下の基本モデルを使用することができます。

- 「集中型ビデオ リソース割り当て」（P.7-10）
- 「分散型ビデオ リソース割り当て」（P.7-13）

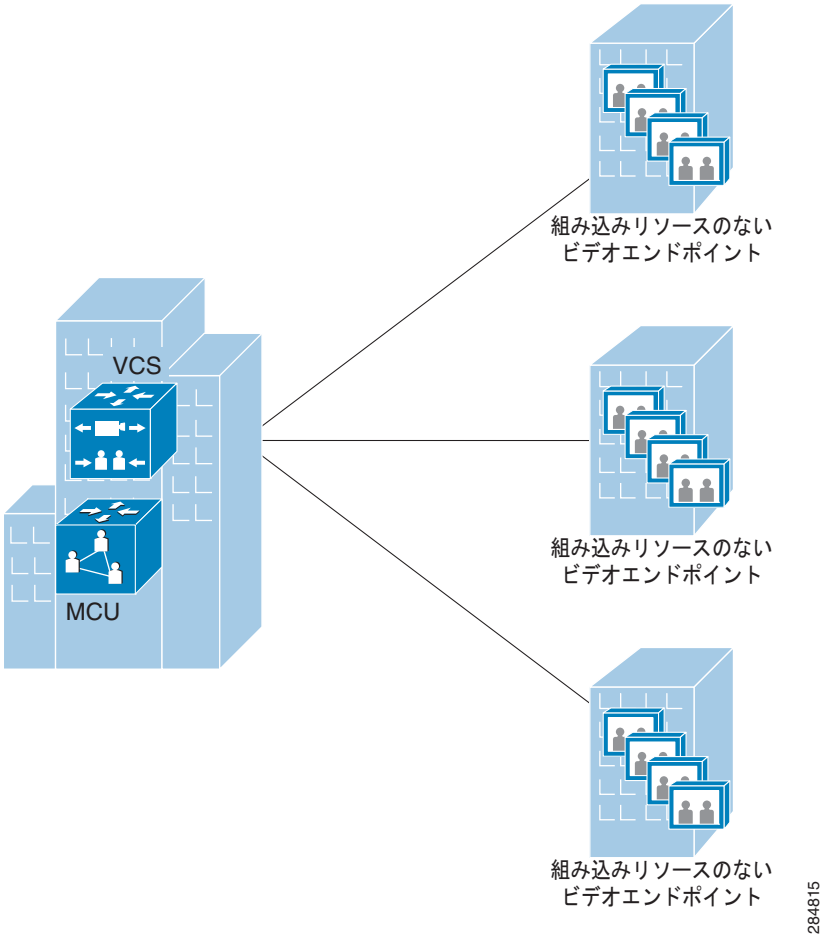
また、専用ビデオ リソース用のこれらのモデルと埋め込み型ビデオ リソースを組み合わせて、必要に応じてビデオ ストリームと音声ストリームソリューションのニーズにさらに適合するハイブリッド モデルを作成することができます。

集中型ビデオ リソース割り当て

リソースを同じロケーションに配置する合計コストがそれらを分散するコストより小さい場合は、集中型リソース割り当てを検討する必要があります。集中型リソース割り当てのフィジビリティも考慮する必要があります。たとえば、リソースの集中によりエンドポイントの状態が不適切（例、受け入れ不能なジッター）になる場合は、集中型リソース アーキテクチャが適さないシナリオがあります。

前述のように、「コール処理トポロジとビデオ エンドポイントの選択ガイドライン」（P.7-8）の項に示したファクタは、特定のシナリオに適合する最適なアプローチを選択する決定プロセスに織り込む必要があります。たとえば、図 7-7 に示すシナリオについて考えてください。本社にすべてのビデオ リソースを集中させた方が、コストが少なくて済むと考えがちですが、このようにリソースを集中すると、ハブとスポーク間の WAN リンクの帯域幅要件が増大するという副作用が生じます。また、WAN リンクで提供される帯域幅により、リモート サイトのマルチポイント会議キャパシティが制限されます。

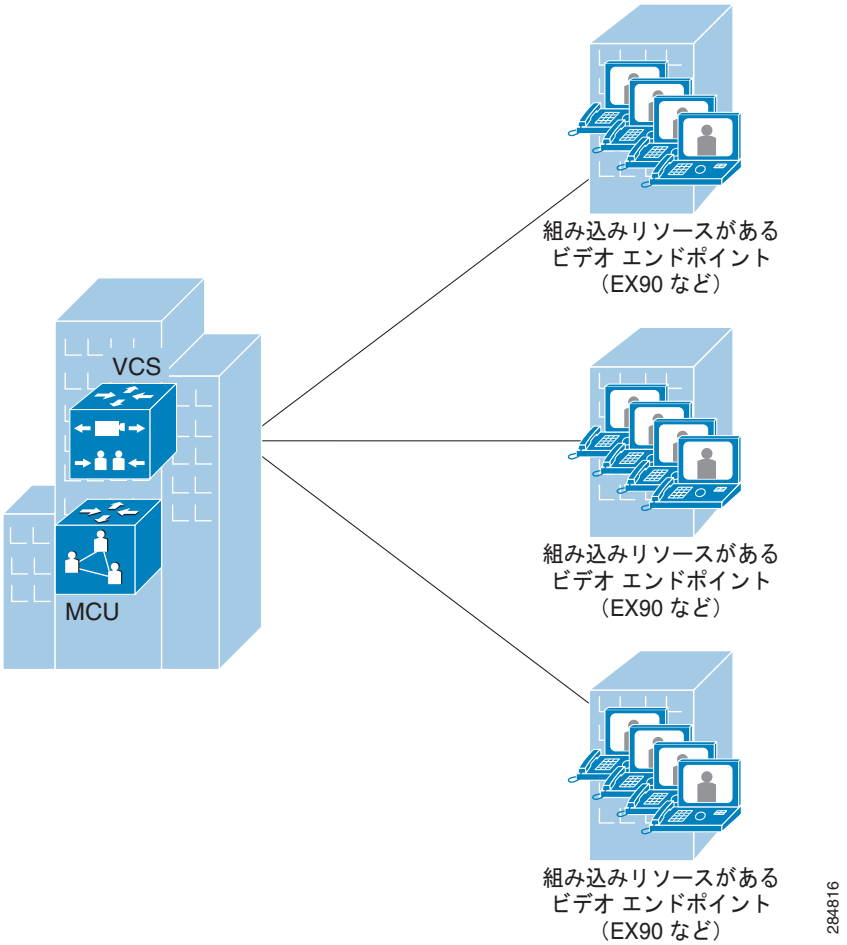
図 7-7　集中型専用ビデオ リソース（埋め込み型リソースはなし）を含むハブ アンド スポーク ネットワーク



リモート エンドポイントがあまり多くなく、その遠いロケーションと帯域利用率により、WAN リンクで転送されるメディア ストリームが悪影響を受けないシナリオには、集中型ビデオ リソース割り当てアーキテクチャが通常最も適しています。

前のシナリオを修正したものが、リモート サイトに埋め込み型ビデオ リソースがある図 7-8 のハイブリッドの例に示されています。このシナリオでは、集中型専用ビデオ リソースが使用されるのは、集中するロケーションに埋め込み型リソースがなく、ビデオ会議でビデオ エンドポイントを使用する場合か、またはビデオ会議の参加者数が、埋め込み型ビデオ リソースで処理できるキャパシティを超える場合に限ります。

図 7-8　集中型専用ビデオ リソースとリモート サイトの埋め込み型ビデオ リソースを含むハブ アンド スポーク ネットワーク



そのほかにも多くのシナリオが可能で、その場合、集中型ビデオ リソースのアプローチにはさまざまな方針や制限が適用できます。

分散型ビデオ リソース割り当て

さまざまなロケーションへの専用ビデオ リソースの分散には、いくつかのメリットがあります。その主なものは、WAN リンクの帯域幅を節約できることと、メディア ストリームに悪影響を与える可能性を減少できること（リソースの多くがローカルで終端されているため）です。ただし、分散型割り当てにはいくつかの制限もあります。たとえば、WAN リンクを通過する必要があるビデオ コールもあり、このようなストリームは WAN リンクの特性による制限を受けます。

分散型専用ビデオ リソースを導入するかどうかを決定する際には、以下の点を検討することで、ソリューションの費用対効果を最大化できます。

- ビデオ リソースのロケーションで予期されるビデオ コール使用パターンはどのようなものか。
- WAN リンクの現在の帯域幅で、ビデオ ストリームに悪影響を与えずに、リモート ロケーションで予期される使用パターンをサポートできるか。
- WAN リンクでのメディア送信の制限または副作用（存在する場合）は、意図している使用例で受け入れることができるか。
- 分散型の埋め込み型ビデオ リソースを使用することで、計画している使用例を実現できるか。
- 現在および計画のネットワーク トポロジで、ビデオ ソリューションは、分散型専用ビデオ リソースがなくても十分に拡張できるか。

さらに、専用ビデオ リソースに分散型割り当てを使用する場合は、ビデオ リソースの最適な配置場所を決定するために、コール制御要素のブリッジ選択アルゴリズムを理解することが重要です。たとえば、エンドポイントとリソースのタイムゾーンに基づいて専用ビデオ リソースを確保することができます。他の方法としては、ビデオのロケーションに基づくビデオ リソースの確保や、手動での確保があります。どの場合も、選択アルゴリズムを理解することの重要性は、ビデオ リソースを効率的に分散させるために、ストリームを最終的にどこで終端するかを理解する必要性に由来しています。

ビデオ対応ネットワークの作成

ビデオがビジネスにもたらす大きなメリットとして、高度なコラボレーション、出張費の削減、およびカスタマイズ可能なアドバタイズメントがあります。しかし、ビデオ アプリケーションは、基盤となるネットワーク インフラおよび IT 部門に課題ももたらします。たとえば、どのようにビデオ用にネットワークを設定するのでしょうか。どのように IT 部門はビデオを優先順位付けし、拡張する必要があるでしょうか。どのようにして彼らは他のアプリケーションが高帯域のビデオ ストリームに圧倒されないようにできるでしょうか。このような企業のビデオ アプリケーションをサポートするには、以下のサービスを提供する、厳重に管理されたネットワーク基盤が必要です。

最適化されたビデオ配信

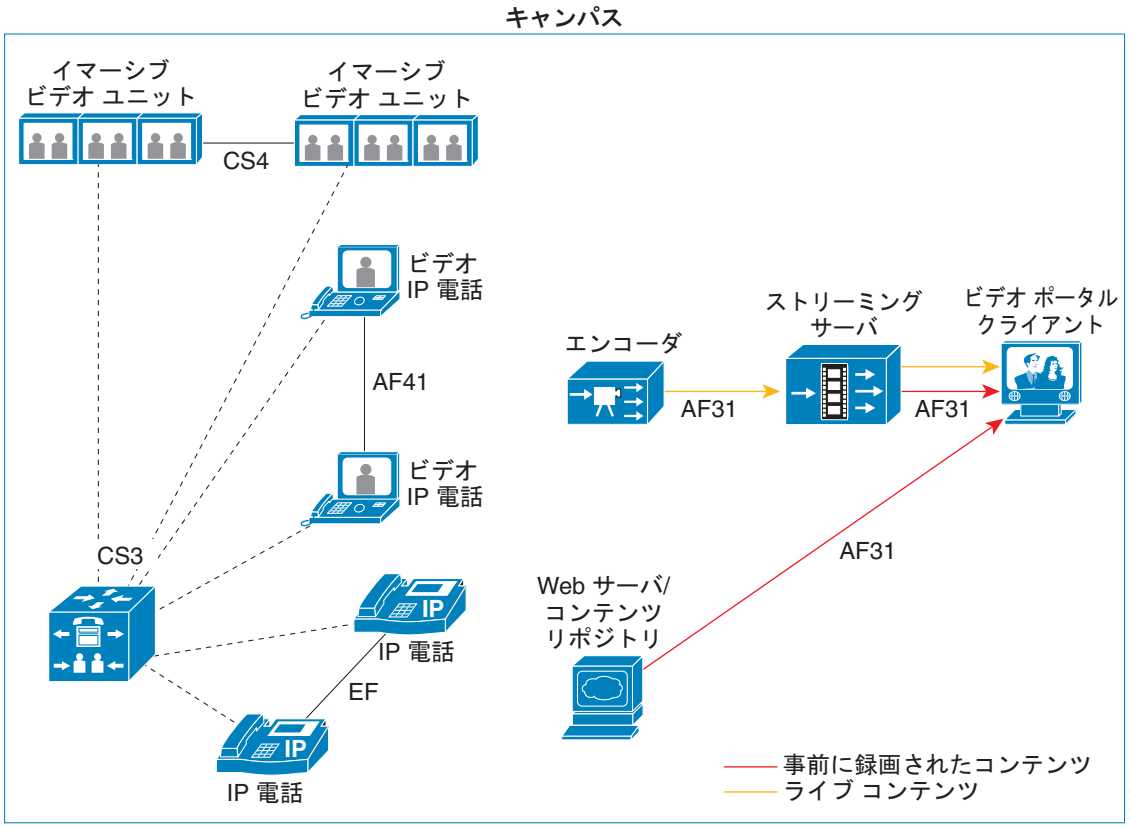
ビデオが効率的なコラボレーション ツールであるためには、ユーザ エクスペリエンスが高品質である必要があります。ユーザ エクスペリエンスの品質を保証するには、組織の要件を満たすよう、ビデオの配信を最適化する必要があります。以下の項で、ビデオ配信を最適化する方法についてのガイドラインを示します。

Quality of Service（QoS）

ビデオの配信を最適化する最初のステップは、対象となるトラフィックを識別し、個別の QoS（Quality of Service）を適用することです。QoS により、組織は、ビジネス クリティカルなビデオ ストリームとクリティカルでないビデオ ストリームを識別するとともに、選択したトラフィック タイプのレイテンシ、ジッター、および損失を受け入れ可能な範囲に抑えるアプリケーション インテリジェンスを実現できます。また、より良いビデオ エクスペリエンスを提供するために、可能な場合は、プライオリティ キューイングを他のキューイング メカニズムの上で使用する必要があります。統合ネットワーク（TelePresence と IP ビデオ テレフォニーを統合したネットワーク）の場合、シスコではアプリケーションごとに QoS クラスを分けることを推奨します。

図 7-9 に、同じネットワーク内で複数の IP ビデオ アプリケーションと IP 音声を統合している例を示します。この例では、イマーシブ ビデオ、ビデオ会議、ビデオ オン デマンド、および Voice over IP が識別されて、推奨されている QoS マーキングが割り当てられ、必要なサービス レベルを実現して過剰なプロビジョニング、つまりキュー内でのアプリケーションのオーバーラップを回避します。

図 7-9　統合ネットワークで推奨する QoS トラフィック マーキング



ビデオ ソリューションにおける QoS の詳細については、「QoS とコール アドミッション制御」（P.5-1）の章を参照してください。

コンテンツ共有技術

ビデオ ソリューションの一環として導入するエンドポイントに応じて、そのビデオ エンドポイントでサポートおよび必要とされるコンテンツ共有標準を考慮するとともに、それらがどのように統合され、または必要な場合は相互作用するかを考慮することが重要です。IP ビデオ ソリューションが使用するコンテンツ共有技術には、現在、Binary Floor Control Protocol（BFCP）、H.239、および自動コラボレートの 3 つがあります。コンテンツ共有機能を実現するのに、H.323 のエンドポイントは H.239 標準を使用するのに対し、SIP のエンドポイントは自動コラボレートまたは新しい標準である BFCP を使用することができます。

プレゼンテーション共有技術およびコンテンツ共有技術の詳細については、次の URL にある『*Cisco TelePresence Interoperability Deployment Guide*』を参照してください。

http://www.cisco.com/en/US/products/ps8332/products_device_support_tables_list.html

信頼性

ビデオ対応キャンパスのパフォーマンスおよび可用性は、プロアクティブにモニタし、ネットワーク全体で測定する必要があります。障害の場合の代替パスも提供して、ビデオ ソリューションの信頼性を保証する必要があります。高可用性のネットワークを設計する方法の詳細については、次の URL にある『*Campus Network for High Availability Design Guide*』を参照してください。

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns815/landing_cHi_availability.html

ビデオ アプリケーションのセキュリティ

ビデオ対応ネットワークは、ビデオ アプリケーションへの不正アクセスを防止するビデオ セキュリティをできれば常に組み込む必要があります。悪意のあるユーザからのスヌーピングと侵入からのトラフィックの保護と攻撃の緩和が不可欠であるとともに、悪意のあるユーザが許可されていないビデオを送信できないようにすることも必要です。ビデオ ネットワークのセキュリティを保護するには、ビデオのトラフィックを切り離すネットワーク仮想化技術から、外界には見えないトポロジのためのデータ VLAN または Session Border Controller（SBC）にあるソフトウェア クライアントでのトラスト リレー ポイント（TRP）の使用まで、さまざまな技術を使用できます。ビデオ ネットワークのセキュリティを保護する方法の詳細については、「ビデオ コミュニケーションのセキュリティ」（P.9-1）の章を参照してください。

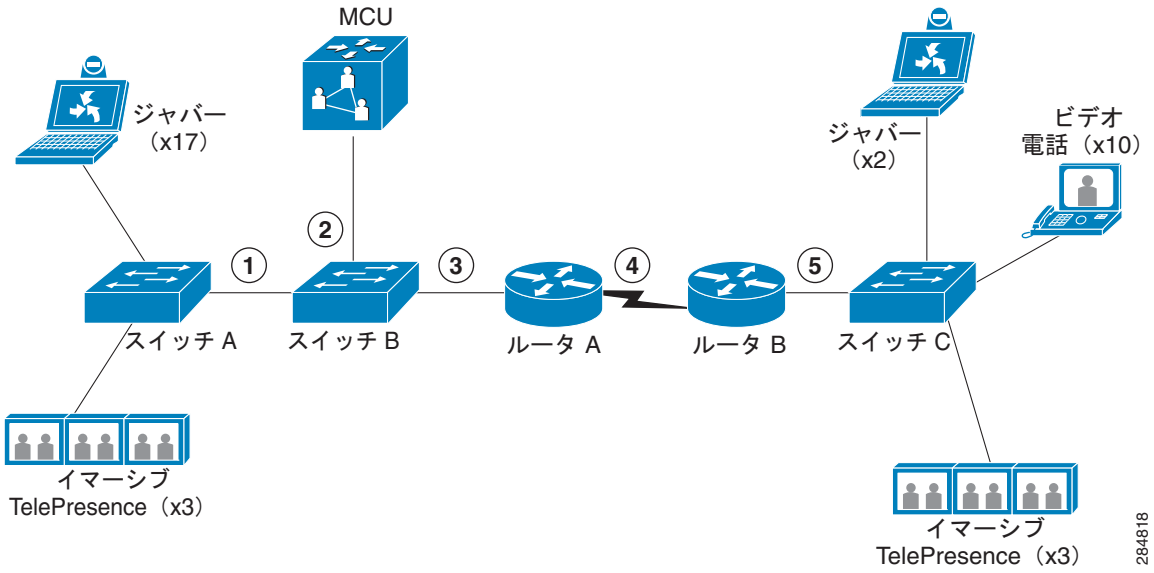
拡張性とパフォーマンス

導入されるビデオ アプリケーションやビデオ ユーザの増加とともに増大する帯域幅ニーズに対応するには、ネットワークの拡張性が重要になってきます。最適のパフォーマンスを維持するには、ネットワークは、高解像度ビデオ ストリームをサポートしたり、場合によっては複数の HD ビデオ ストリームを同時にサポートするよう拡張できるなど、より広い帯域にすぐに対応できる必要があります。したがって、導入するビデオ アプリケーションで生成されることが予想されるトラフィックに対し、適切にネットワークをサイジングすることが重要です。

ネットワークをサイジングする最初のステップは、エンドポイントおよびユーザの要件を把握することです。次に、会議およびポイントツーポイント コールのときのメディア フローの動作を決定します。続いて、音声およびデータのトラフィックならびに、信頼性を持たせるために必要となるバックアップ方式に関する考慮事項を追加します。図 7-10 に、本社キャンパスに 20 のイマーシブおよびデスクトップ ビデオ エンドポイントがあり、支社に 15 のその他のエンドポイントがあるシナリオの例を示します。この例で予期されている使用パターンは、次のとおりです。

- 本社のデスクトップ エンドポイントのユーザとイマーシブ エンドポイントのユーザは、ピークの発信回数が 7 回になります。
- 本社のエンドポイントは、支社との間のピーク発信/受信回数が 6 回になります。
- 本社デスクトップ エンドポイントのコールでは 1.3 Mbps を使用しているのに対し、イマーシブ エンドポイントでは 12 Mbps を使用しています。
- 支社のビデオ IP Phone では 1 Mbps、デスクトップ エンドポイントでは 1.3 Mbps、イマーシブ エンドポイントでは 12 Mbps が使用されます。
- ピーク時には、支社のユーザは最大 4 回発信し、本社との間では 6 回発信/受信（上記のとおり）します。
- 本社と支社のユーザは、サイト間で実行される 10 Mbps（連結）のデータ アプリケーションにアクセスする必要があります。

図 7-10　ビデオ対応ネットワークのキャパシティ要件の決定



上記の要件が単純化してあることは明らかです。非常に複雑なネットワークおよび導入では、要件およびサポートするアプリケーションが多くなります。しかし、前述の例の要件リストについては、以下のことを決定できます。

- 以下の最悪のシナリオを想定した場合、予想される最大の帯域利用率は、スイッチ A とスイッチ B の間のアップリンク（図 7-10 のリンク 1）ではビデオ ストリームで 49 Mbps です。
  - デスクトップ ビデオ エンドポイントのローカル マルチポイント コールに 7 人のユーザが参加している場合：

    7 X (1.3 Mbps) = 9.1 Mbps
  - イマーシブ エンドポイント（ローカルが 3 つ、リモートが 3 つ）のマルチポイント コールに 6 人のユーザが参加している場合：

    3 X (12 Mbps) = 36 Mbps
  - ローカル デスクトップ エンドポイント（ローカル ビデオ IP Phone が 3 つ、リモート ビデオ IP Phone が 3 つ）のマルチポイント コールに 6 人のユーザが参加している場合：

    3 X (1.3 Mbps) = 3.9 Mbps

（注） この帯域計算では、データ アプリケーションの追加帯域やその他必要な追加帯域（コール シグナリング用など）を考慮していません。LAN をダイメンショニングする前に、このような他の帯域要件を含めておく必要があります。

- 最悪のシナリオでは、以下を想定して、支社の WAN リンク（図 7-10 のリンク 5。ただし、リンク 3、4 と 6 には同じ考慮事項が該当する）でビデオ ストリーム用に 43.6 Mbps の帯域を使用します。
  - 4 つのビデオ電話間でのマルチポイント コールに 4 人のユーザが参加している場合：ローカルのマルチポイント コントロール ユニット（MCU）がないため、マルチポイント コールが行われるには、すべてのストリームが本社まで転送される必要があります。

    4 X (1 Mbps) = 4 Mbps
  - 5 つのデスクトップ ビデオ エンドポイント、1 つのビデオ電話、3 つのローカル エンドポイント（2 つのデスクトップ ビデオ エンドポイントおよび 1 つのビデオ電話）、3 つのリモート エンドポイントの間でのマルチポイント コールに 6 人のユーザが参加している場合：

    2 X (1.3 Mbps) + 1 Mbps = 3.6 Mbps
  - イマーシブ エンドポイント（ローカルが 3 つ、リモートが 3 つ）のマルチポイント コールに 6 人のユーザが参加している場合：

    3 X (12 Mbps) = 36 Mbps

（注）　この帯域計算では、データ アプリケーションに必要な追加の 10 Mbps やその他必要な追加帯域（コール シグナリング用など）を考慮していません。それらの要件も、サイジング プロセスの一部として追加する必要があります。

- 最後に、図 7-10 の MCU を処理するリンク 2 では、前の 2 つの帯域計算を考慮することで、ビデオ ストリームはピーク時に 92.6 Mbps でリンクを通過することを予想できます。

  49 Mbps + 43.6 Mbps = 92.6 Mbps

（注）　徹底的に検証済みで広く使用されている一般的なルールは、10 % のバーストとレイヤ 2 からレイヤ 4 へのネットワーク オーバーヘッドを吸収するために、ビデオ帯域を 20 % 過剰にプロビジョニングすることです。また、上記の計算は、例に示されている使用パターンの最悪シナリオに基づいていますが、すべてのビデオ ユーザが同時にビデオ コールを行うケース（100 % コール実行という）は考慮していません。

要するに、ビデオ対応ネットワークのキャパシティとパフォーマンスの設計では、望ましいコール実行率や予期される使用パターンによって大幅なレイテンシを生じずに、ビデオ転送を可能にする必要があります。コールごとに必要な帯域量の決定については、ご使用のエンドポイントのマニュアルを参照してください。

スタンドアロン型ビデオ ネットワークとの統合

前のビデオ ネットワーク ソリューションを置き換える場合でも、あるいは同じコール処理プラットフォーム要素のもとで前のビデオ ネットワーク ソリューションを統合しようとする場合でも、IT 部門にとって、統合は困難な課題となります。統合の選択肢とガイドラインを把握することは、統合を行う IT 部門とユーザにとって、把握しない場合より良い経験になります。

統合のアプローチは、使用するコール シグナリング プロトコルによって異なります。以下の項で、今日のビデオ ネットワークで最も広く使用されている 2 つのプロトコルの一般的ガイドラインを示します。

- 「スタンドアロン型 H.323 ビデオ ネットワークとの統合」（P.7-19）
- 「スタンドアロン型 SIP ビデオ ネットワークとの統合」（P.7-20）

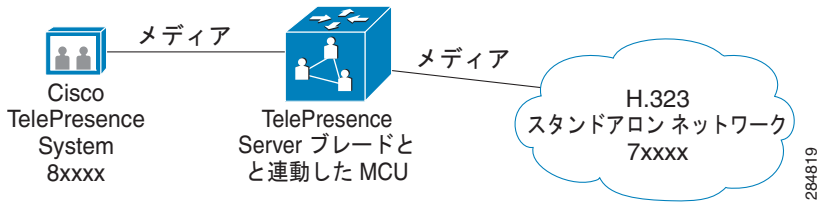
スタンドアロン型 H.323 ビデオ ネットワークとの統合

H.323 は、非常に洗練されたプロトコルで、マルチベンダー SIP 要素の場合よりかなり簡単に H.323 コール処理要素との相互運用性を実現します。ただし、H.323 は対応する SIP ほどサービスが豊富ではありません。たとえば、シスコでは、通話中のスピーカーが誰になるかによって画面を切り替える機能（smart switching）を実装していますが、この機能は H.323 ネットワークではネイティブで使用可能ではありません。

可能な場合は常に、ビデオ エンドポイントのネイティブな相互作用を使用して、エンドポイントを H.323 ネットワークに直接接続します。ただし、そのようにしても、smart switching などの必要な機能が失われない場合に限ります。不可能な場合、機能の保持が重要なときや、ポイントツーポイントの相互運用性がネイティブで得られないときは、ビデオ トランスコーダまたは相互運用性対応会議ブリッジを介して H.323 エンドポイントに接続します。オーバーラップのないダイヤル プランも推奨します。その理由は、コールを実行するのに次のビデオ システムへのホップが必要であることをコール処理エージェントに示すために、ネットワーク間でさまざまなアクセス コードを使用できるからです。

図 7-11 に、マルチポイント コントロール ユニット（MCU）を使用して Cisco TelePresence System をサードパーティの H.323 スタンドアロン型ビデオ ネットワークに接続する例を示します。

図 7-11　　スタンドアロン型 H.323 ネットワークの統合



スタンドアロン型 SIP ビデオ ネットワークとの統合

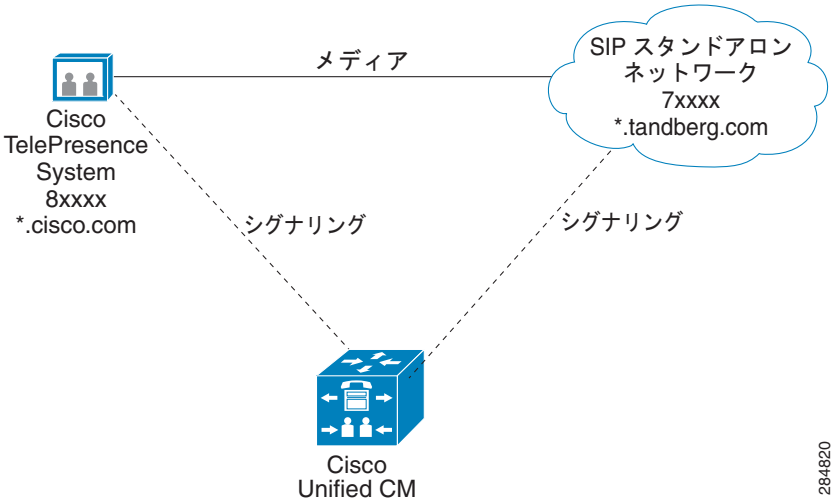
SIP ビデオ ネットワークは、H.323 ネットワークより機能が豊富で、すべてのエンドポイントでサポートされる場合は、非常に有益な機能を有効にすることができます。ただし、SIP は H.323 ほど洗練されていないため、それとの相互運用性は H.323 の場合より困難です。

エンドポイントが SIP 標準に厳密に準拠している場合、コール エージェントは、コール処理エージェント内で使用可能なネイティブのビデオ相互運用性機能を使用することができます。そうでない場合、ビデオ ネットワークは、ビデオ トランスコーダまたは相互運用性対応マルチポイント コントロール ユニットを使用して、相互にブリッジすることができます。

シスコでは、ビデオ ネットワーク間でオーバーラップ ダイヤル プランを使用せず、アクセス コードを使用して、ビデオ ネットワーク間をルーティングするようコール処理エージェントに指示し、桁間タイムアウトを回避することを推奨します。ダイヤル プランで Uniform Resource Identifier（URI）ダイヤルを使用する場合、シスコでは管理のしやすさから複数のドメインを使用することを推奨します。

図 7-12 に、Cisco TelePresence System と SIP 標準に基づくサードパーティ システムの統合を示します。この例では、ダイヤルのために、複数のドメインとともにネイティブの相互運用性を使用しています。

図 7-12　　スタンドアロン型 SIP ネットワークとの統合

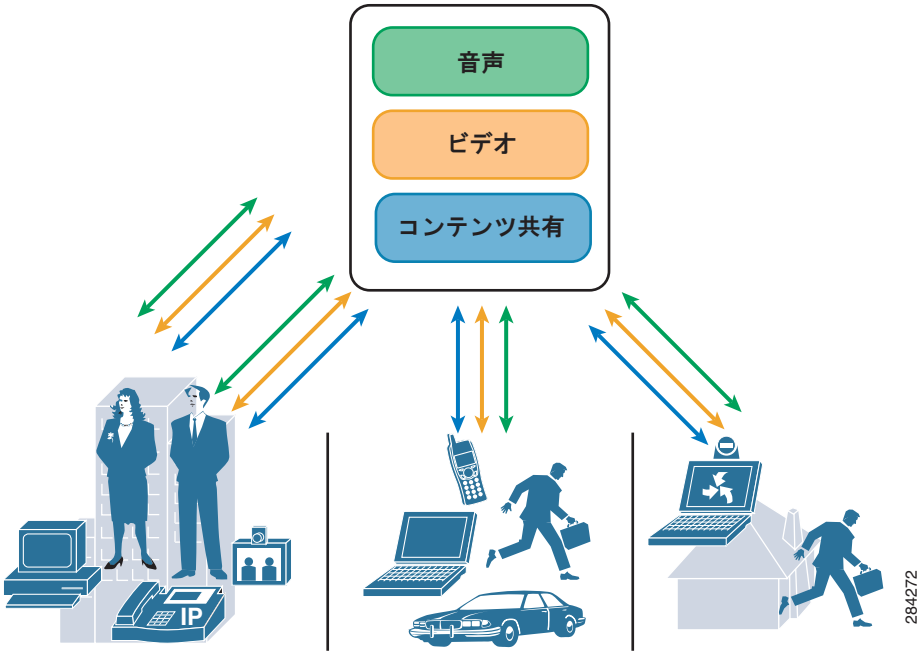


CHAPTER 8

コラボレーティブ会議

3 人以上のユーザが参加しているコールは会議になります。コラボレーティブ会議では、会議の参加者の一部または全員の音声、ビデオ、およびコンテンツが単一のストリームにミックスされ、このストリームが参加者に送り返されます。音声およびビデオは、マルチポイント コントロール ユニット（MCU）またはいくつかのマルチポイント デバイスによって処理されます。図 8-1 に、内部と外部両方の参加者、外勤職員と遠隔地の職員、または異なる組織からの参加者も含む会議を示します。

図 8-1　　コラボレーティブ会議の概念図



会議の種類

会議製品では、アドホック会議とスケジュール済み会議の 2 種類の会議がサポートされるのが一般的です。スケジュール済み会議には、スケジュール機能を提供するために Microsoft Exchange や IBM Domino などのカレンダー アプリケーションと統合されている Cisco TelePresence Management Suite（TMS）などの特別なツールが必要です。

アド ホック会議

アド ホック会議では、会議の開催者が会議を作成し、会議内容に関する事前通知を送信しないで、参加者に参加するよう依頼します。通常、会議の開催者は、エンドポイントの [Conference] キーを押して会議を作成し、参加者に電話して参加者を会議に追加します。[Conference] キーのないエンドポイントでは、会議を開催することはできませんが、会議への参加依頼を受けることはできます。アドホック会議用にリソースを予約することはできません。この会議を作成できるのは、会議作成時に十分なリソースが使用可能な場合に限ります。その場合、会議はコール処理エージェント（Cisco Unified Communications Manager など）によって制御されます。

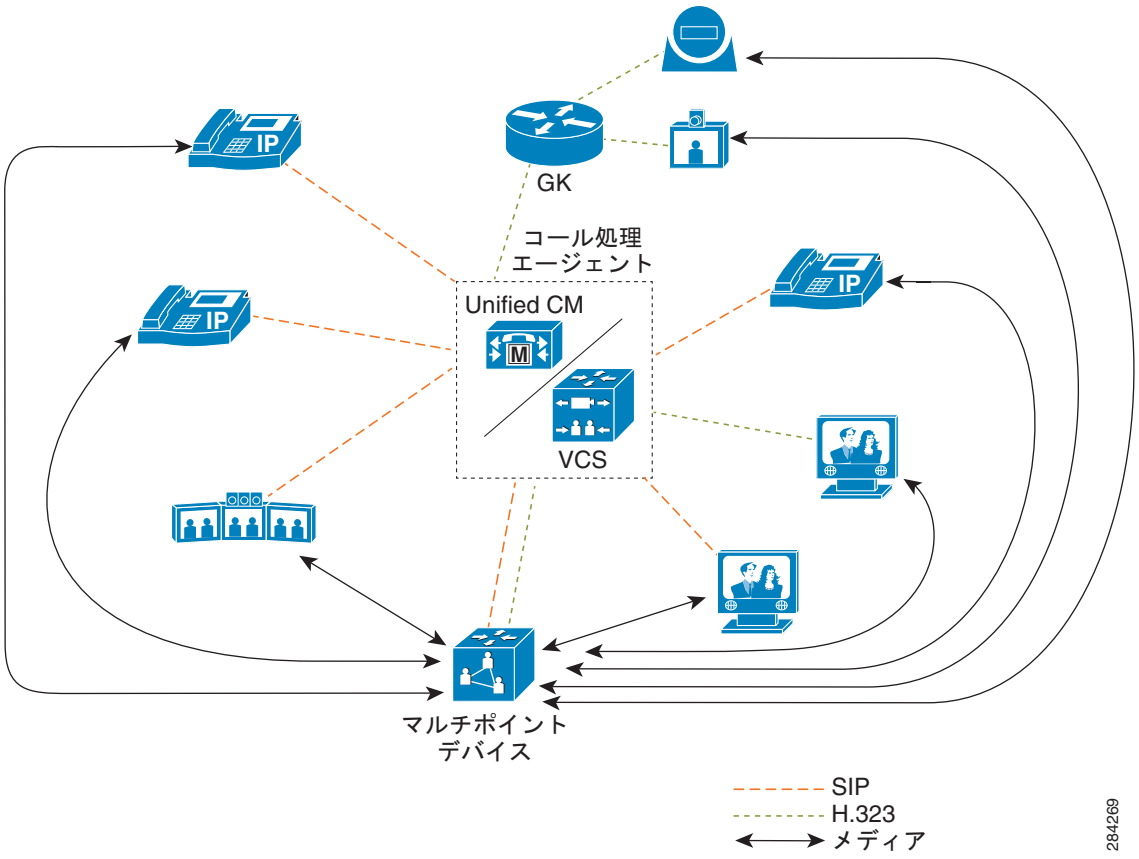
スケジュール済み会議

この種類の会議では、会議主催者は、製品のスケジュール ツールか、または会議製品のスケジュール機能と統合されたカレンダー アプリケーションを使用して、会議をスケジュールします。会議のリソースは、会議がスケジュールされたときに予約されます。リソースが不足している場合は、会議はスケジュールできません。会議に参加するには、参加者は、会議に直接ダイヤルするか、または会議への出席依頼に含まれる会議のリンクをクリックしてシステムにより参加者にコールします。この場合、マルチポイント デバイスが会議を制御し、コール処理エージェントがダイヤルされたコールを該当するマルチポイント デバイスにルーティングします。

会議のインフラストラクチャ

図 8-2 に示すように、コール処理エージェントとマルチポイント デバイスが会議インフラストラクチャの主な構成要素です。コール処理エージェントは、信号を処理し、エンドポイントのコールを制御します。スケジュール済み会議の場合、コール処理エージェントは、コールをマルチポイント デバイスにルーティングします。Cisco Unified Communications Manager（Unified CM）と Cisco TelePresence Video Communication Server（VCS）は、Cisco ビデオ会議製品で最もよく使用されるコール処理エージェントです。Unified CM が SIP を介して VCS と接続することで、一方のエージェントに登録されたエンドポイントが、他方のエージェントに登録されたエンドポイントとコールまたは会議することができます。

図 8-2　会議の構成要素



マルチポイント デバイスの主機能は、会議中にエンドポイントからメディア（音声とビデオ）を処理することです。一般に、コール処理エージェントとマルチポイント デバイスの接続は SIP または H.323 です。

会議のマルチポイント デバイス

マルチポイント デバイスは会議のインフラストラクチャの中心的構成要素で、ハードウェア ベースでもソフトウェア ベースでもかまいません。マルチポイント デバイスは、参加しているすべてのエンドポイントからのビデオ ストリームを処理し、全参加者の複合イメージを元のエンドポイント デバイスに送り返します。この複合ビューにより、全参加者は互いを同時に見ることができます。連続的プレゼンス ビューでは、複数のウィンドウ（参加者）をさまざまなレイアウトで表示できます。各レイアウトには、ウィンドウの 1 つを Voice-Activated にする機能があり、合成ビューに表示できるウィンドウの数よりも参加者の方が多い会議で役立ちます。

トランスコーディングと切り替え

マルチポイントのプラットフォームには、トランスコーディング アーキテクチャまたは切り替えアーキテクチャを使用できます。どちらのアーキテクチャにも、導入対象としてマルチポイントのプラットフォームを選択する際に検討に価するメリットがあります。

- **トランスコーディング** アーキテクチャには、着信したビデオ ストリームを復号化し、再度符号化してから転送する、高度なビデオ ハードウェアが含まれています。トランスコーディング アーキテクチャを使用する例としては、Cisco TelePresence Server、Cisco Media Experience Engine（MXE）、および Cisco Multipoint Control Unit（MCU）があります。
- **切り替え**では、高度なビデオ ハードウェアは不要ですが、代わりにソフトウェアを使用します。着信したビデオ ストリームとオーディオ ストリームは、コピーされて、会議の該当するエンドポイントにリダイレクトされます。このとき、ビデオ ストリームは操作されません。切り替えアーキテクチャを使用する例には、Cisco TelePresence Multipoint Switch があります。

表 1 に、マルチポイント プラットフォームのトランスコーディング アーキテクチャと切り替えアーキテクチャの利点と欠点を示します。

表 8-1　トランスコーディングと切り替えの比較

アーキテクチャ	利点	欠点
トランスコーディング	• アクティブ プレゼンスがサポートされます。[1] • エンドポイントが、さまざまな回線速度および解像度で接続できます。 • 通常、遠端カメラ制御（FECC）機能のあるエンドポイントでは、レイアウトをカスタマイズできます。 • エンドポイント間でビデオを拡張（トランスレート）できます。 • テレプレゼンス相互運用プロトコル（TIP）ベースのエンドポイントと標準プロトコル ベースのエンドポイントをサポートします。	• ビデオを復号化および再符号化するために、レイテンシが発生します。 • ポートあたりのコストが高くなります。 • 通常、拡張が困難です。
切り替え	• レイテンシが低くて済みます（10 ms 未満）。 • ポートあたりのコストが低くなります。	• 基本的なフルスクリーン ビデオ切り替えのみ可能です（アクティブ プレゼンスなし。各画面には 1 つのサイトのみ表示可能）。 • エンドポイント間で、単一の解像度およびフレーム レートについてサポートおよび合意する必要があります。[2]

1. アクティブ プレゼンスでは、1 つの画面で複数の参加者を表示します。その際、アクティブな参加者はフル スクリーンで表示され、その他の参加者は画像内の画像として画面の下部に重ねて表示されます。
2. スマート メディアを使用する Cisco TelePresence System Release 1.7 以降のデバイスでは、IP ネットワークの状態に応じてビデオ解像度を調整できます。

マルチポイントの導入ガイドライン

マルチポイント技術を導入する方法には、集中型の方法と分散型の方法があります。ユーザ エクスペリエンスの最適化、リソースのローカライズ、およびマルチポイント コールの信頼性保証を行える導入方針を検討することが重要です。マルチポイント ソリューションの導入方法を設計する場合は、以下の点を考慮してください。

- エンドポイント数。これにより、今度は必要なマルチポイント デバイス数が決まります。
- エンドポイントの地理的ロケーション。

これら 2 つのファクタにより、マルチポイントの導入方法（集中型または分散型）、マルチポイント デバイス数、およびマルチポイント デバイスの物理的ロケーションが決まります。

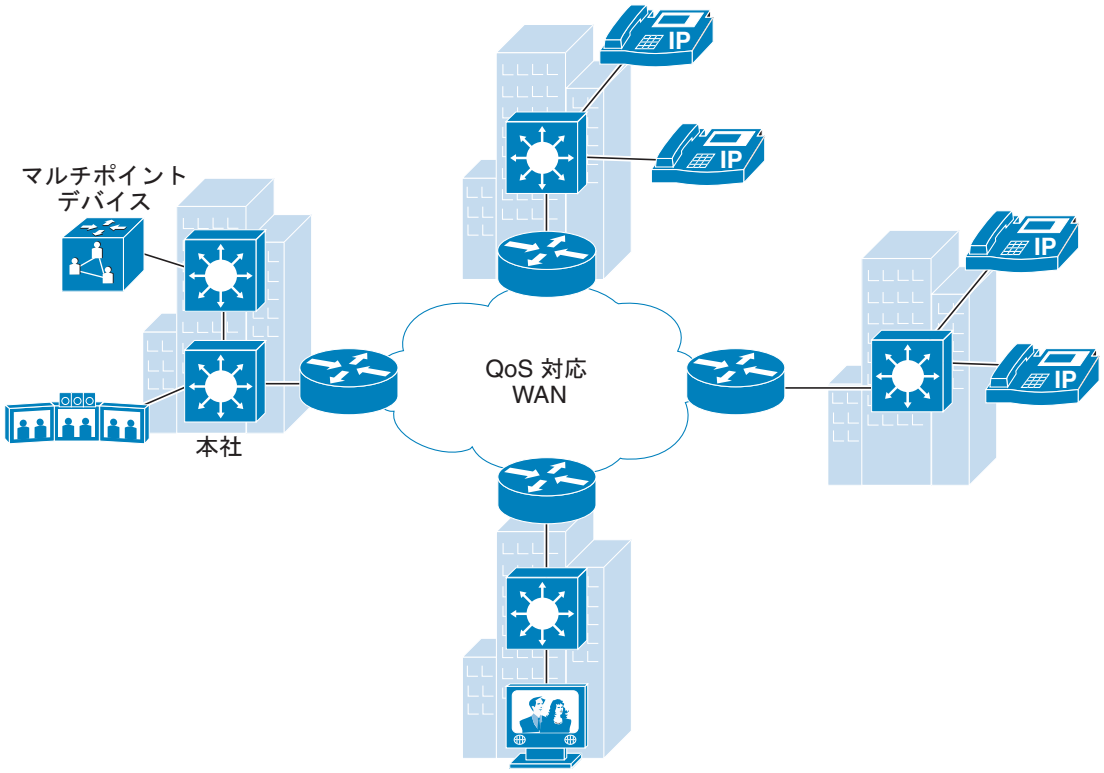
集中型の導入

集中型の設計は、少数のエンドポイントを含むマルチポイント デバイスの導入、または一部の地理的エリアのみへの大規模な導入に推奨します。

集中型の導入では、マルチポイント デバイスをリージョナル キャンパス サイトまたは本社のキャンパス サイトに配置でき、各リモート サイトでは必要な WAN 帯域幅（およびキャンパス内では必要な LAN 帯域幅）が使用可能です。シスコでは、エンドポイントの地理的ロケーションにおける中央にマルチポイント デバイスを配置することを推奨します（ただし、これが不可能なネットワーク レイアウトもあります）。マルチポイント デバイスを中央に配置することで、ネットワークの遠端のサイトにコールをバックホーリングすることによって不必要なレイテンシが発生することを防止できます。

図 8-3 に示す導入は、マルチポイント会議のレイテンシを最小化するために中央に配置したマルチポイント デバイスを使用する少数のエンドポイントを含んでいます。

図 8-3　集中型マルチポイントの導入



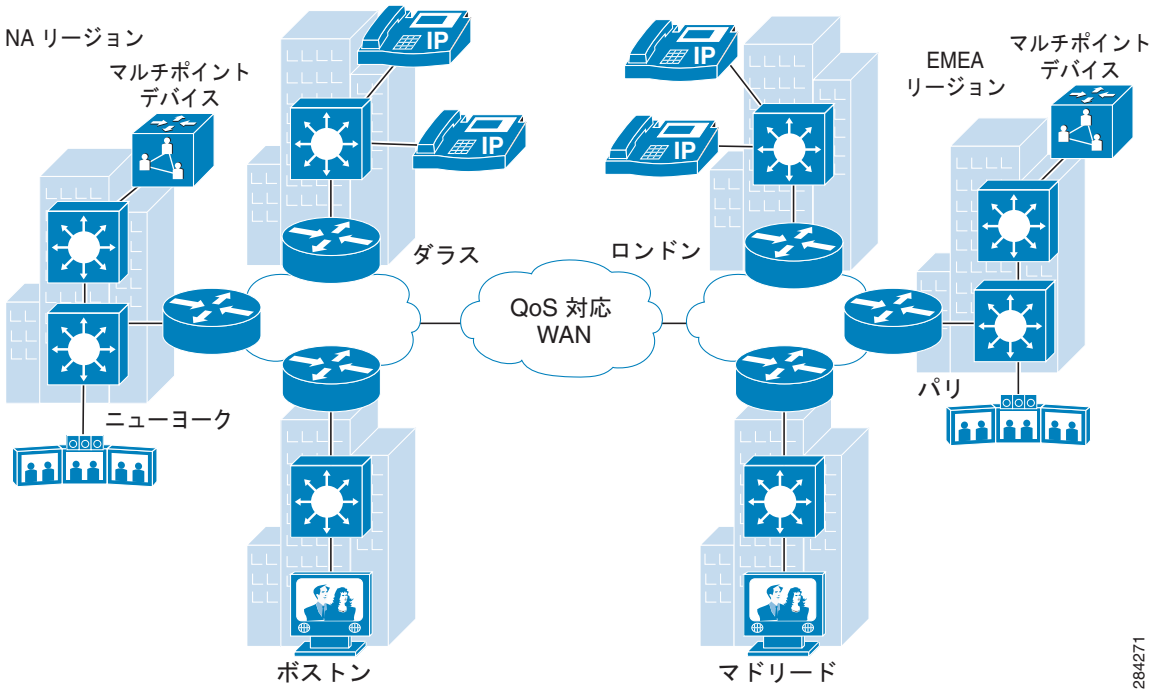
マルチポイント デバイスは、ネットワーク レイテンシがソリューションの要件に準拠しているサイトに配置する必要があります。また、サイトは、ネットワークに導入するエンドポイント数に十分な帯域幅でプロビジョニングする必要があります。帯域幅要件は、エンドポイントに最大限必要なコール レート、およびマルチポイント デバイスに接続するエンドポイント数に応じて異なります。必要なレートおよび解像度に対して特定のエンドポイントで必要となる最大帯域幅に基づいて、プロビジョニングを行ってください。ネットワーク レイテンシおよび帯域幅要件の詳細については、http://www.cisco.com にある個々のソリューション導入ガイドまたはソリューション設計ガイドを参照してください。

分散型の導入

シスコでは、大規模な導入、または地理的に離れた地域において少数のエンドポイントしか含まない導入に対しては、分散型構成を選択することを推奨します。マルチポイントをローカライズすると、ネットワークが増大しても、レイテンシを最小化して帯域幅を節約できる利点が非常に大きくなります。

図 8-4 に、マルチポイント デバイスを各地域（NA および EMEA）の中央に配置するとともに世界中に分散している導入を示します。

図 8-4　分散型マルチポイントの導入



分散型環境では、マルチポイント デバイスを配置するサイトは、ネットワーク レイテンシがソリューション要件に準拠し、サポートするエンドポイント数に十分な帯域幅を提供できることが必要です。

マルチポイント デバイスを導入する際には、以下の追加のガイドラインも順守する必要があります。

- 複数のマルチポイント デバイスを使用して、柔軟性があるマルチポイント ソリューション アーキテクチャを構築する。マルチポイント デバイスの 1 つが失敗した場合でも、動作しているデバイスから会議を再開できる。
- 大規模な会議の導入をサポートし、帯域幅使用量を最小化するため、マルチポイント デバイスをカスケード化する。マルチポイント デバイスをカスケード化するには、Cisco TelePresence Conductor を使用できる。
- Cisco TelePresence Conductor を使用して、会議の特性（例、地理的ロケーション、ビデオ品質）に基づいて会議用のマルチポイント デバイスを選定する。
- スケーラブルなマルチポイント ソリューションを構築できる導入を選択する。たとえば、エンドポイントを複数の地理的地域に導入していて、各地域のエンドポイント数の増大が予想される場合は、分散型マルチポイントの導入を使用する。
- トラフィックの負荷をマルチポイント デバイスに分散してリソース使用率が最大になるよう、ソリューションを設定します。
- シスコでは、大規模導入にはスケジュール オプションを使用することを推奨します。会議の作成が簡単になります。
- 可能な場合、シスコでは、エンドポイントがインターワーキングを行わなくてもネイティブ プロトコルで接続できるよう、MCU を異種環境に二重登録（SIP と H.323）することを推奨します。

マルチポイント ソリューションの選択

導入に適したマルチポイント ソリューションを決定する場合、複数のファクタ（組織の現在の導入と目的とするエンドポイントの組み合わせなど）を考慮するとともに、どのマルチポイント機能にプライオリティを置くかを決定する必要があります。マルチポイント ソリューションのアーキテクチャを設計する際に一般的に考慮する必要があるファクタは、以下のとおりです。

- アクティブ プレゼンス
- 拡張性
- ネットワーク レイテンシ
- エンドポイントのサポート
- マルチスクリーンで使用可能かどうか
- コラボレーション（コンテンツ共有）
- スケジューリング

エンドポイントに基づくマルチポイントの選択

マルチポイント デバイスを決定するときは、エンドポイントから開始します。以下のシナリオにあるように、エンドポイントの組み合わせによって、導入用のマルチポイント デバイス オプションを消去または決定できる場合があります。

- さまざまなビデオ形式、ビデオ コーデック、解像度、またはフレーム レートをサポートする異種のエンドポイントを含む導入では、最適のオプションはトランスコーティングとトランスレーティングを両方とも行えるマルチポイント デバイスです。そのような場合、Cisco TelePresence Multipoint Switch は、切り替えアーキテクチャに基づいているため、よい選択肢ではありません。
- テレプレゼンス相互運用プロトコル（TIP）ベースのエンドポイントと標準プロトコル ベースのエンドポイントを両方とも含む導入では、これらのプロトコル間で動作するビデオ ゲートウェイが必要です。たとえば、会議環境で、Cisco TelePresence System 3200 Series エンドポイント、Cisco IP Video Phone E20 エンドポイント、および Cisco TelePresence System EX90 エンドポイントのミックスと Cisco TelePresence Multipoint Switch が Cisco Unified CM に登録されている場合は、エンドポイント間の相互運用性を可能にする Cisco Media Experience Engine（MXE）が、追加する必要がある（予算面で）自明の選択肢となる可能性があります。

ただし、大部分の場合、複数の選択肢があるため、必要な機能を検討することも必要です。

機能に基づくマルチポイントの選択

会議導入でどの機能に最高のプライオリティを置くかに注目することで、マルチポイント ソリューションの選択肢を限定することができます。下記に、選択するマルチポイント ソリューションの決定に影響する機能のリストの抜粋を示します。

- テレプレゼンス相互運用プロトコル（TIP）ベースのエンドポイント、標準プロトコル ベースのエンドポイント、サードパーティ製プロトコルのエンドポイントに対するサポート
- マルチスクリーンまたはシングルスクリーンのサポート
- One Button To Push（OBTP）のサポート
- アクティブ プレゼンスまたは連続プレゼンス
- コンテンツ共有
- H.239、Binary Floor Control Protocol（BFCP）、または自動コラボレートによるコンテンツ共有トランスレーション
- WebEx OneTouch 統合
- エンドポイントからのレイアウト変更が可能
- （部屋と話者の間での）切り替えポリシーのサポート
- SIP および H.323 のサポート

各マルチポイント製品でサポートされる機能の一覧については、http://www.cisco.com にある個々の製品データ シートを参照してください。

会議リソースのキャパシティ プランニング

マルチポイント デバイスがサポートできるビデオ会議のタイプと数の決定には、複数のファクタが関与します。これらのサイジング ファクタは、マルチポイント製品によって異なります。また、マルチポイント デバイスは、ビデオ会議で標準解像度（SD）を使用する場合、高解像度（HD）を使用する場合より高いキャパシティをサポートすることができます。

会議のキャパシティは、以下のファクタによって決まります。

- ビデオ会議で必要とされる解像度のタイプまたはビデオ形式
- マルチポイント デバイスがサポートできる合計ポート数
- マルチポイント デバイスが各プロトコル専用に割り当てることができるポート数
- マルチポイント デバイスをカスケード化するかどうか

ビデオ会議で Cisco Integrated Services Router（ISR）上でブリッジとして Cisco 高密度パケット音声ビデオ デジタル シグナル プロセッサ モジュール（PVDM3）またはデジタル シグナル プロセッサ（DSP）の最新モデルを使用する場合は、Cisco Unified Communications Sizing Tool の DSP calculator を使用して会議のキャパシティを計算します。Cisco Unified Communications Sizing Tool（Unified CST）は、適切なログイン認証を持つシスコの従業員またはシスコのパートナーに http://tools.cisco.com/cucst で公開されています。

CHAPTER 9

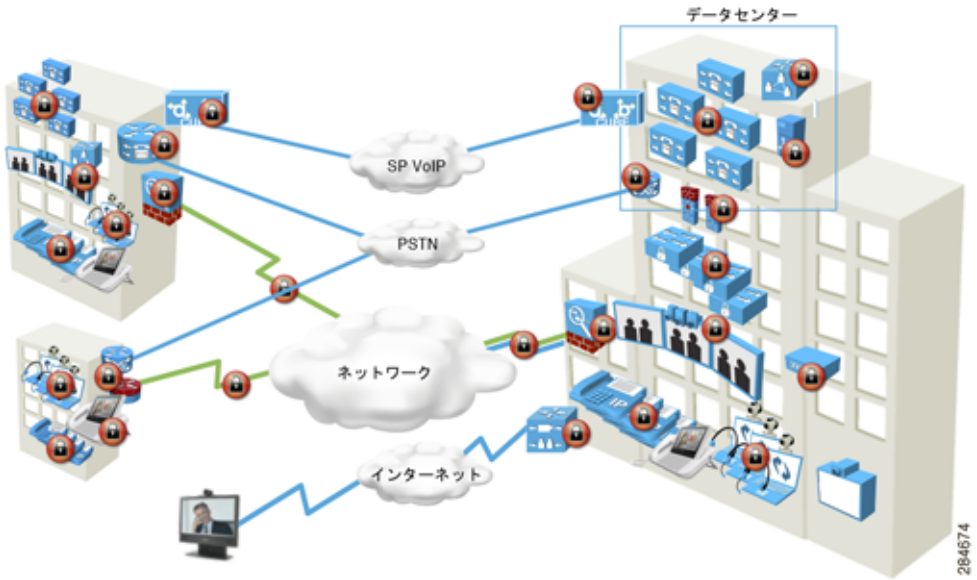
ビデオ コミュニケーションのセキュリティ

企業内の IP ネットワークにおけるビデオ コミュニケーションを保護するには、Unified Communications の構成要素と、通信ストリームが転送されるネットワーク インフラの両方に対するセキュリティを実装する必要があります。この章では、Cisco Unified Communications System および Cisco TelePresence Solution で使用可能な、企業の IP Telephony ネットワーク内のビデオ コールの整合性、信頼性、および機密性を保護する設計および実装オプションについて説明します。データ ネットワーク セキュリティの詳細については、次の URL で入手可能な Cisco SAFE Blueprint に関するマニュアルを参照してください。

http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html

シスコでは、セキュリティが保護されるように音声およびビデオ コミュニケーションを実装するため、企業内に導入されるすべてのネットワーク技術に関連するセキュリティ ポリシーを作成することを推奨します（図 9-1 を参照）。セキュリティ ポリシーは、ネットワーク内の機密データを特定し、ネットワーク内で転送する際にはデータを適切に保護します。セキュリティ ポリシーを配置すると、ネットワーク上のデータ トラフィックのタイプで要求されているセキュリティ レベルを定義するのに役立ちます。

図 9-1　　Cisco Unified Communication System のセキュリティおよび強化オプション



Cisco Unified Communications ネットワークを強化するには、認証された通信ストリーム、デジタル署名設定ファイルを確立、維持するとともに、Cisco Unified Communications コンポーネントと Cisco TelePresence コンポーネントの間のメディア ストリームおよびコール シグナリングを暗号化する必要があります。これらのセキュリティ機能のすべてがあらゆるネットワークに必要なわけではありませんが、これらの機能によりセキュリティ レベルを向上させることができます。

この章では、これらの機能の設計ガイドラインを示します。製品の設定の詳細については、ご使用の Cisco Unified Communications Manager（Unified CM）および Cisco TelePresence のバージョンに関する以下のセキュリティ ドキュメントを参照してください。

- 『*Cisco Unified Communications Manager Security Guide*』
  http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
- 『*Cisco Unified Communications System SRND*』
  http://www.cisco.com/go/ucsrnd
- 『*Cisco TelePresence Design Guide*』
  http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns819/landing_vid_tPresence.html

ネットワーク インフラのセキュリティ

ビデオ コミュニケーションを保護するには、コールを転送するのに使用されるネットワークを保護する必要があります。それには、アクセス ポートから始まってネットワークを経由してインターネットのエッジに至るまで、セキュリティのレイヤを構築します。シスコでは、不正アクセスからネットワーク インフラのデバイスを保護できるよう、ファイアウォール、アクセス コントロール リスト、認証サービス、およびその他のシスコ セキュリティ ツールを必ず使用することを推奨します。

ネットワーク デバイスへのアクセスを制限することは、インフラを保護するうえで最も重要な要件の 1 つです。一般的な企業ネットワークは、ルータ、スイッチ、ファイアウォール、および侵入防御システムなど、多くのコンポーネントから構成されています。攻撃者は、ネットワーク上のこれらのデバイスにたえずアクセスしようとしています。各デバイスの管理インターフェイスへのアクセスを制限することで、攻撃者がこれらのデバイスを危殆化する機会を削減できます。ネットワーク上のすべてのデバイスを適切に保護する必要があります。ネットワーク デバイスを管理者として管理するとともに運用面でも管理するには、Secure Shell（SSH）およびハイパーテキスト転送プロトコル セキュア（HTTPS）などのセキュリティで保護されたプロトコルを使用します。Telnet などのプロトコルで使用される、クリア テキストでのパスワードおよび設定情報の送信は、できるだけ避けてください。

インフラへのアクセスを保護するだけでなく、ネットワークの運用で使用されているサービスも保護する必要があります。これには、ドメイン ネーム システム（DNS）、ネットワーク タイム プロトコル（NTP）、ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）、ならびに Session Initiation Protocol（SIP）および H.323 などのシグナリング プロトコルがあります。これらのサービスは、ネットワークを正常に運用するために不可欠であり、攻撃者にとっての第一の標的でもあります。これらのサービスを 1 つでも混乱させることで、Unified Communications システムに対してサービス拒否と可用性の問題を引き起こすことができます。

独立した Auxiliary VLAN

シスコでは、Unified Communications 環境の RTP トラフィック（音声とビデオ）とデータ トラフィックのために、独立した VLAN を実装することを推奨します この構成では、すべての Cisco IP Phone と TelePresence エンドポイントをデータ VLAN から独立した音声 VLAN に配置します。この実装には次の利点があります。

- 音声ネットワーク コンポーネントとデータ ネットワーク コンポーネントの間のトラフィックを制限するための VLAN アクセス コントロール リスト（VACL）の設計が簡単になります。また、ネットワーク管理者がネットワークで管理によるアクセス制限を効率的に実装できるようになります。
- アドレス空間を確保し、外部ネットワークから音声デバイスを保護します。Voice VLAN または Auxiliary VLAN 上で電話機のプライベート アドレッシングを行うと、アドレスが確実に確保され、パブリック ネットワークを介して電話機に直接アクセスできないようになります。
- QoS（Quality of Service）の設定と管理を簡単に行えるようになります。また、信頼と QoS 機能を PC やその他のデータ デバイスまで拡張せずに、QoS の信頼境界を音声デバイスとビデオ デバイスまで拡張することができます。
- VLAN アクセス コントロール、802.1Q、および 802.1p タギングは、データ デバイスが情報をスプーフできないようにするとともに、パケット タギングによってプライオリティ キューにアクセスすることができます。

（注）　Cisco Unified IP Phones と Cisco TelePresence エンドポイントはサービス要件が異なっているため、これらを単一の VLAN に配置すると、通常のアクセス コントロール リストの設計が複雑になります。

デバイスのセキュリティ

Cisco Unified IP Phones と TelePresence エンドポイントには、自身を攻撃から保護するための複数の設定オプションが用意されています。ただし、これらのデバイスが初期設定時からデフォルトで強化されているとは考えないでください。セキュリティ機能は、エンドポイントに応じて異なり、以下のものがあります。

- 「HTTPS および SSH でのセキュリティ管理」（P.9-4）
- 「管理パスワード」（P.9-4）
- 「デバイスへのアクセス」（P.9-4）
- 「シグナリングおよびメディア暗号化」（P.9-4）

この機能の設定の詳細については、エンドポイントの管理者ガイドを参照してください。また、次の URL にある『*Cisco Unified Communications Manager Security Guide*』内の電話の強化に関する情報も参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

HTTPS および SSH でのセキュリティ管理

Cisco TelePresence エンドポイントでは、Secure Shell（SSH）および Hyper-Text Transfer Protocol over Secure Sockets Layer（HTTPs）による管理をサポートします。HTTP、HTTPS、SSH、または Telnet を使用したエンドポイントへのアクセスは、エンドポイント自体の [Network Services] 設定で設定できます。

Cisco Unified IP Phones は、HTTPS のみを使用するよう制限することも、HTTP と HTTPS の両方で使用可能にすることもできます。

管理パスワード

エンドポイントはデフォルトの管理パスワードで出荷されており、シスコでは、設置時にパスワードを変更することを推奨します。管理機能へのアクセスは、管理権限を認可されたユーザに制限する必要があります。

デバイスへのアクセス

エンドポイントは、定義されているロールおよび権限に基づいてアクセスを付与されたユーザに割り当てることができます。これらのユーザにパスワードおよび PIN 指定して、SSH または Telnet および web ベースのアクセスを使用可能にすることができます。パスワードを定期的に失効させ、変更するとともに、アイドル状態のときにログインをタイムアウトにするために、クレデンシャル管理ポリシーを実装する必要があります。これは、デバイスへのアクセスを検証済みのユーザに限定するために必要です。

ユーザ認証およびクレデンシャル管理の設定の詳細については、次のマニュアルを参照してください。

- 『*Cisco Unified Communication Manager Administration Guide*』
  http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
- 『*Securing Cisco TelePresence Products*』
  http://www.cisco.com/en/US/products/ps8332/products_installation_and_configuration_guides_list.html

シグナリングおよびメディア暗号化

サポートされる Cisco Unified Communications デバイス用にシグナリングおよびメディアを暗号化して、アクティブなコールまたはコールの確立時に対する傍受およびスパイ攻撃を阻止することができます。Unified Communications の導入で安全な通信とシグナリングを提供するプロトコルおよびメカニズムは、以下のとおりです。

- 「トランスポート層セキュリティ（TLS）」（P.9-5）。シグナリング トラフィックの暗号化に使用される。
- 「Secure Real-Time Transport Protocol（SRTP）および Secure Real-Time Transport Control Protocol（SRTCP）」（P.9-5）。メディアの暗号化に使用される。
- 「データグラム トランスポート層セキュリティ（DTLS）Secure Real-Time Transport Protocol（SRTP）」（P.9-5）。SRTP マスター キーのネゴシエーションや交換に使用される。
- 「デジタル証明書」（P.9-6）

- 「Certificate Authority Proxy Function（CAPF）」（P.9-6）
- 「証明書信頼リスト（CTL）」（P.9-7）

トランスポート層セキュリティ（TLS）

トランスポート層セキュリティ（TLS）は、2 つのアプリケーション間の通信に認証、データ整合性、および機密性を提供するために設計されたプロトコルです。TLS は Secure Sockets Layer（SSL）バージョン 3.0 をベースにしていますが、2 つのプロトコルには互換性はありません。最新バージョン、TLS 1.2 は、IETF RFC 5246 で定義されています。TLS はクライアント / サーバ モードで動作し、サーバとして動作する側面とクライアントとして動作する側面を持ちます。TLS は、ハンドシェイク プロトコルを使用し、クライアントとサーバが公開キー暗号化（デジタル証明書）を使用して互いを認証できるようにします。また、これにより、アプリケーション データが送信される前に、圧縮アルゴリズム、メッセージ認証アルゴリズム、暗号化アルゴリズム、および必要な暗号キーの信頼できるネゴシエーションが可能になります。

Cisco Unified CM、Cisco Unified IP Phones、および Cisco TelePresence System コンポーネント間での SIP シグナリングの暗号化およびデータの認証は、トランスポート層セキュリティ（TLS）プロトコルを使用して実装されます。また、TLS はさまざまな Cisco TelePresence コンポーネント間での web サービスのシグナリングの認証および機密保護のためにも使用されます。

シグナリング プロトコルの暗号化は、Advanced Encryption Standard（AES）を使用し、対称キーを使用して行われます。メッセージ認証は HMAC-SHA1 ハッシュ アルゴリズムを使用して行われます。キー材料のネゴシエーションは、TLS ハンドシェイク プロトコル層内でクライアントおよびサーバのキー交換メッセージを介してセキュリティが保護されて行われます。

Secure Real-Time Transport Protocol（SRTP）および Secure Real-Time Transport Control Protocol（SRTCP）

Real-time Transport Protocol（RTP）の音声およびビデオ メディア フローのデータ認証および機密保護では、ポイントツーポイントおよびマルチポイントの TelePresence 会議で Secure Real-time Transport Protocol（SRTP）を使用します。

Secure RTP（SRTP）および Secure Real-time Transport Control Protocol（SRTCP）はともに IETF RFC 3711 に定義されています。この RFC には、RTP の音声およびビデオ メディアならびに対応する RTCP ストリームに対して機密性およびデータ整合性を提供する方法が詳述されています。

SRTP では、暗号化は、128 ビット キーを使用した Advanced Encryption Standard（AES）アルゴリズムを使用して、RTP パケットのペイロードにのみ適用されます。また、SRTP では、メッセージ認証ハッシュ アルゴリズムとして HMAC-SHA1 も使用します。メッセージ認証は、RTP のペイロードだけでなく RTP のヘッダーにも適用されます。SRTP は、ヘッダー内の RTP シーケンス番号にメッセージ認証を適用して、リプレイ アタックを防止します。

SRTCP パケットで暗号化を使用する場合は、SRTP パケットの場合と同様に、ペイロードにのみ適用されます。ただし、メッセージ認証は RTCP のヘッダーと RTCP のペイロードの両方に適用されます。

データグラム トランスポート層セキュリティ（DTLS）Secure Real-Time Transport Protocol（SRTP）

データグラム トランスポート層セキュリティ（DTLS）は、ユーザ データグラム プロトコル（UDP）などのデータグラム トランスポート プロトコルを介した 2 つのアプリケーション間の通信に認証、データ整合性、および機密性を提供するために設計されています。このプロトコルは IETF RFC 4347

で定義されています。DTLS は TLS をベースにして、UDP の低信頼性を埋め合わせるためにシーケンス番号および再送信機能などのメカニズムを追加したものです。DTLS-SRTP は、DTLS 内で SRTP キー材料のネゴシエーションのために DTLS を拡張したものです。

Cisco Telepresence ソリューションでは、DTLS のハンドシェイクは TelePresence エンドポイント間で直接行われます。DTLS-SRTP セッションは、コール内の関連する Cisco Unified IP Phone を使用せずに、2 つのエンドポイント間の RTP メディア ストリーム内で、Cisco TelePresence コーデック間で確立されます。各コールでは、2 つの DTLS-SRTP ハンドシェイクが行われます。1 つは音声用、もう 1 つはビデオ メディア用です。暗号化およびこれらのストリームの認証のために、キーがネゴシエーションされます。

デジタル証明書

Cisco Unified Communications System は、公開キー インフラストラクチャ（PKI）機能の構成要素として X.509 v3 証明書を使用し、メッセージの暗号化および復号化に使用する公開キーおよび秘密キーを生成します。この PKI の実装により生成されるキーのペアのうち、秘密キーによりメッセージが暗号化され、暗号化されたメッセージは、2 つのデバイス間で交換される公開キーを使用した場合のみ復号化できます。秘密キーは、デバイス内に安全に保管され、けっして公開されません。公開キーは、X.509 デジタル証明書に属性として定義、公開されています。属性は、証明書にデジタル署名する認証局（CA）によって設定されます。デジタル署名自体は、認証局の秘密キーを使用して暗号化された、メッセージのハッシュです。認証局のデジタル署名は、受信者が認証局の公開キーを使用して検証できます。

証明書としては、製造元がインストールした証明書（MIC）またはローカルで有効な証明書（LSC）を使用できます。Cisco Unified Communications Manager（Unified CM）には、LSC が Cisco Certificate Authority Proxy Function（CAPF）によってインストールされるのに対し、MIC はプレインストールされます。MIC 証明書は、エンドポイントが最初の認証および Cisco Unified CM のセキュリティ フレームワークへの登録を実行するためのクレデンシャルとなります。MIC を使用する場合、Cisco CA 証明書および Cisco Manufacturing CA 証明書はルート証明書として機能します。

（注）　また、MIC は、Cisco TelePresence エンドポイント間でデータグラム トランスポート層セキュリティ（DTLS）セッションを確立するためにも使用されます。

Certificate Authority Proxy Function（CAPF）

Cisco Certificate Authority Proxy Function（CAPF）は、Cisco Unified CM の一部としてインストールされるソフトウェア サービスです。CAPF はデフォルトでは有効化されていないので、インストール後に設定する必要があります。CAPF は、Cisco Unified IP Phones および Cisco TelePresence エンドポイントのために、ローカルで有効な証明書（LSC）を発行します。CAPF は、自身の権限のもとで証明書に自己署名します。ただし、これは外部の認証局（CA）に証明書を要求するプロキシとして使用することもできます。Public-Key Cryptography Standard（PKCS）#10 証明書署名要求（CSR）を使用した、第三者認証局（CA）による証明書に署名することができます。

第三者 CA を使用する場合、CA により CAPF に署名できますが、電話機の LSC は、その後も CAPF により生成されます。自己署名した LSC を使用する場合は、CAPF 証明書がルート証明書になります。外部 CA を使用する場合は、CAPF が下位 CA として機能し、外部 CA がルート CA になります。

これらの証明書は、TLS で信号を送信する SIP などのプロトコルのために、安全な認証付きの接続を確立するために使用されます。

証明書信頼リスト（CTL）

CTL Provider は、Cisco Unified CM の一部としてインストールされるもう 1 つのソフトウェア サービスで、CTL Client と連携して証明書信頼リスト（CTL）を生成します。CTL Client は Cisco Unified CM サーバからダウンロードできるソフトウェア プラグインで、独立した Windows PC で実行されます。証明書信頼リスト自体は、Unified CM サーバにストアされた信頼できる証明書の定義済みリストで、Cisco エンドポイントにブート時にファイルとしてダウンロードされます。CTL は、Cisco Unified IP Phones および TelePresence エンドポイントがコール シグナリングのために TLS を介して SIP セッションを開始するときに信頼できる Unified CM サーバのリストを意味しています。CTL 自体の認証を可能するには、最低 2 つの独立した Cisco Universal Serial Bus（USB）ハードウェア セキュリティ キー（etoken）が必要です。これらの USB キーは Cisco Unified CM 製品に含まれていないため、別途購入する必要があります。これらのセキュリティ キーは、CTL クライアント プラグインを稼働している PC に CTL 生成プロセス中に挿入されます。

コンフィギュレーション ファイルの整合性と暗号化

Cisco TelePresence 装置および Cisco Unified IP Phones のコンフィギュレーション ファイルは、Cisco Unified CM 内にストアされます。これらのファイルは、エンドポイントにブート時にダウンロードされます。また、Unified CM 内でエンドポイントの設定に影響する設定変更が行われると、必ず自動的にコンフィギュレーション ファイルが Cisco TelePresence デバイスにダウンロードされます。さらに、コンフィギュレーション ファイルのダウンロードにより、デバイスがリセットされます。

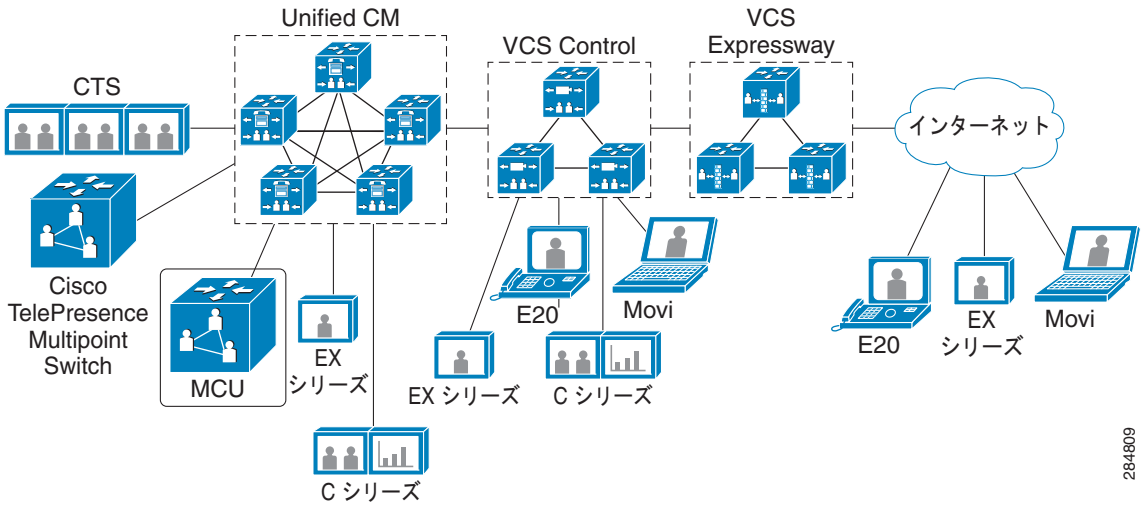
Cisco Unified CM で、コンフィギュレーション ファイルの暗号化を要求するデバイス セキュリティ プロファイルを作成できます。これにより、コンフィギュレーション ファイルは、Unified CM によりデジタル署名されるため、権限のないユーザによって変更されなくなります。

メディア暗号化の詳細

Cisco Unified Communication Manager（Unified CM）では、ボイス コール ペイロードの音声部分用に Secure Real-time Transport Protocol（SRTP）をサポートしていますが、ビデオ メディア用の暗号化はサポートしていません。Cisco Unified CM 8.6 以降のリリースに対し、Cisco TelePresence EX Series および C Series のエンドポイントがネイティブでサポートされるようになりましたが、これにはメディア暗号化のサポートは含まれていません。Cisco TelePresence System および Video Communication Server は、それらにネイティブで登録されているエンドポイントに対して SRTP をサポートします。Cisco TelePresence エンドポイントは、SRTP セッションを確立するための秘密キーの交換で、データグラム トランスポート層セキュリティ（DTLS）を使用します。

Cisco Unified CM、Cisco TelePresence System（CTS）、および Cisco Video Communication Server（VCS）は、SIP 用 TLS を使用した安全なシグナリングをサポートします。Unified CM、VCS、および CTS のために SIP トランクが使用される実装では、TLS を使用して SIP プロトコルのエンドツーエンド シグナリング暗号化がサポートされます（図 9-2 を参照）。

図 9-2　TLS を使用した Cisco TelePresence System、Unified CM、および Video Communication Server の統合



エンドツーエンドの SIP シグナリング暗号化を実装するには、TLS を使用するために Unified CM に VCS ネイバー ゾーンを設定する必要があります。この機能を使用するには、適切な機能キーのインストールが必要です。また、Unified CM が VCS サーバの証明書を信頼できることが必要です。それには、Unified CM および VCS で同じ認証局からの証明書を使用するか、または、共通のルート CA を使用しない場合は VCS サーバの証明書をエクスポートして Unified CM 信頼ストアにアップロードします。

この設定により、シグナリングが暗号化されますが、メディアのペイロードは保護されません。ビデオコールの暗号化には、エンドポイント間で DTLS を使用して、キー交換のために安全なチャネルを確立する必要があります。この後、そのチャネルを介して、メディア暗号化に使用される AES 暗号キーが渡されます。このメディア暗号化は、メディア暗号化をサポートするように設定された TelePresence エンドポイントで実装できますが、Unified CM IP Phone では動作しません。

設定の手順については、次の URL にある『*Cisco TelePresence Video Communication Server Cisco Unified Communications Manager Deployment Guide*』を参照してください。

http://www.cisco.com/en/US/products/ps11337/products_installation_and_configuration_guides_list.html

ファイアウォールおよびアクセス コントロール リストとの統合に関する考慮事項

安全な企業ネットワークでは、さまざまな種類の悪意ある脅威から自身を防御するために、ファイアウォールとアクセス コントロール リスト（ACL）を併用しています。ACL は、ローカル エリア ネットワーク（LAN）のアクセス エッジや LAN とワイド エリア ネットワーク（WAN）の交点など、ネットワークのさまざまな箇所のトラフィックのマーキング、シェーピング、およびポリシングを含む、QoS（Quality of Service）設定を適用するのにも頻繁に使用されます。また、ファイアウォールは、企業キャンパス内または 2 つ以上のキャンパス ロケーション間で、アクセス コントロールに使用することもできます。

Cisco Unified Communications System 内のサーバおよびエンドポイントでは、広範囲のポートとサービスを使用します。このため、ファイアウォールと ACL を使用してそれらを保護し、アクセスを制限するには、綿密な計画が必要です。ファイアウォールを導入するとネットワークの設計が複雑になるの

で、適正と見なされるトラフィックが通過するのを許可し、ブロックする必要があるトラフィックをブロックするようにファイアウォール、およびファイアウォールの周辺デバイスを配置および設定するときは、細心の注意が必要です。

音声およびビデオ デバイスで使用されるポートの動的特性のため、ファイアウォールを設定すると、Cisco Unified Communications System で使用されるさまざまなサービスに必要な広範囲のポートの開放を制御することができます。ファイアウォールのアプリケーション層インスペクション機能は、必要なポートとソケットを動的に開閉することで、トラフィックのフィルタリングを簡単に行えるようにします。これは、コールでメディア ストリームを確立するために埋め込まれた IP アドレッシング情報を取得するために、ディープ パケット インスペクションを実行します。ただし、これが正常に機能するには、ファイアウォールのインスペクション エンジンが Unified Communications コンポーネントの特定プロトコルでの実装をサポートしている必要があります。Cisco 適応型セキュリティ アプライアンス（ASA）5500 Series のファイアウォールでは、Unified Communications プロトコルのバージョン固有の実装がサポートされます。そのようになるには、実装される ASA のバージョンが、ネットワークの Cisco Unified Communications ソリューションのバージョンと互換である必要があります。一方をアップグレードするには、他方もアップグレードする必要があります。

Cisco ASA 5500 のファイアウォールは、インターフェイスに割り当てられた信頼レベルに基づいて、トラフィックを制限したり許可したりします。これにより、ネットワーク内でさまざまな信頼レベルが設定されます。セキュリティ レベルには、100（最も安全なインターフェイス）、から 0（安全性が最も低いインターフェイス）まで設定できます。これらは通常「内部」および「外部」と呼ばれます。デフォルトでは、セキュリティ レベルが高いインターフェイスのデバイスから開始されたトラフィックは、セキュリティ レベルが低いインターフェイスのデバイスに渡すことができます。そのようなセッションに対応する、低いインターフェイス セキュリティ レベルから高いセキュリティ レベルのインターフェイスへのリターン トラフィックは、動的に許可されます。この動作は、ポイントツーポイント コールで対称型ポート ナンバリングを使用する Cisco TelePresence エンドポイントでは正常に機能します。しかし、マルチポイント TelePresence コールは対称的に番号付けされたポートを常に使用できるとは限りません。

マルチポイント TelePresence コールでは、音声およびビデオのユーザ データグラム プロトコル（UDP）ストリームが Cisco TelePresence エンドポイントと Cisco TelePresence Multipoint Switch の間で転送されます。各エンドポイントは音声およびビデオ コールを持ちますが、Multipoint Switch は複数のエンドポイントからの UDP 音声およびビデオ ストリームをサポートする必要があるため、フローの UDP ポート番号は必ずしも対称的ではありません。このため、ファイアウォールが必要なメディア ポートを動的に開閉できるようにするには、SIP プロトコルを対象としてアプリケーション層のプロトコル インスペクションを設定する必要があります。

ファイアウォールにより、セキュリティ レベルの低いインターフェイスのデバイスから開始されたトラフィックを、セキュリティ レベルの高いインターフェイスのデバイスに渡すことは許可されません。この動作を変更するには、低いセキュリティ インターフェイス レベルの入力アクセス コントロール リスト（ACL）を使用します。高いセキュリティ レベルのインターフェイスに適用される入力 ACL は、高いレベルのセキュリティ インターフェイスから低いセキュリティ レベルに転送されるトラフィックを制限することにも使用できます。

また、Cisco ASA 5500 Series のファイアウォールを使用して、セキュリティ レベルが等しいインターフェイス同士を操作することもできます。それには、セキュリティが同じインターフェイス間のトラフィックを許可するコマンドを設定する必要があります。各インターフェイスには、ACL を適用することもでき、セキュリティ レベルが等しいインターフェイスに接続された特定のデバイスとプロトコルの間でのアクセスを個別に許可するために、スタティック変換を使用できます。

Cisco TelePresence コンポーネント間で許可する必要がある TCP および UDP ポートのリストについては、次の URL にある『*Securing Cisco TelePresence Products*』マニュアルを参照してください。

http://www.cisco.com/en/US/products/ps7315/products_installation_and_configuration_guides_list.html

Cisco Unified CM で使用されるポートのリストについては、次の URL にある『*Cisco Unified Communications Manager TCP and UDP Port Usage*』ガイドを参照してください。

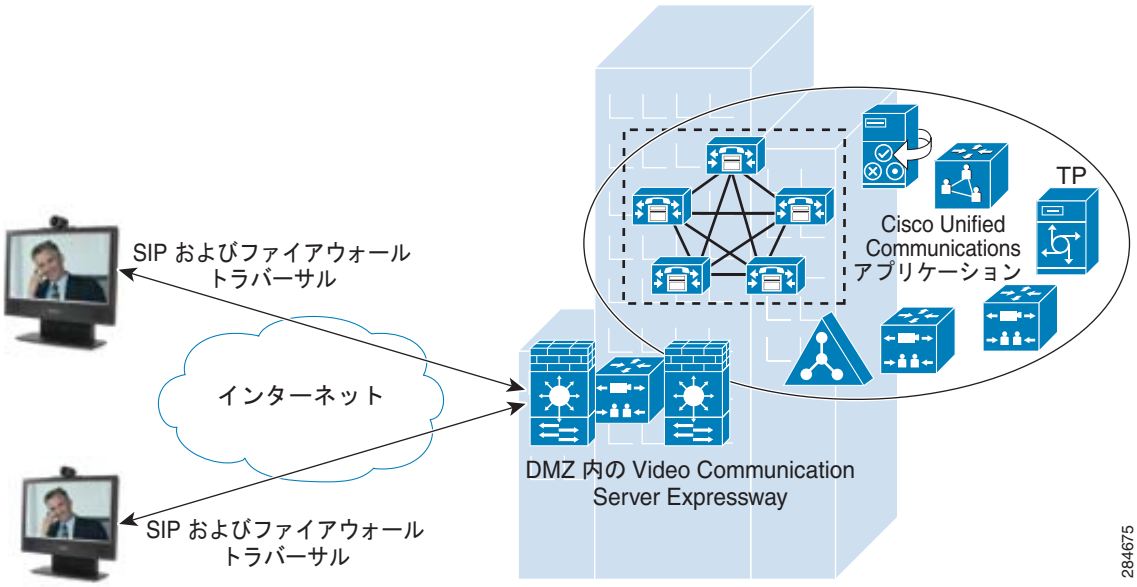
http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

DMZ でのファイアウォール トラバーサル

Cisco TelePresence Video Communication Server Expressway（VCS Expressway）は、企業ネットワーク外およびインターネットからデバイスへのビデオ コミュニケーション コールを確立することができます。外部の発信者がデバイスにアクセスできるようにするには、Cisco Unified Communications ソリューションで使用されるプライベート ネットワークの外部に VCS Expressway を配置する必要があります。これは、一般のインターネットまたは非武装地帯（DMZ）に導入できます。デフォルトでは、ファイアウォールは非請求の着信要求をブロックするため、VCS Expressway で VCS Control サーバとの常時接続を確立できるようにするには、ファイアウォールを設定する必要があります。

VCS Expressway を DMZ に配置することで、この実装がはるかに安全になります（図 9-3 を参照）。これは、音声およびビデオ トラフィックを処理する専用サーバとして VCS を使用するので、ファイアウォール設定の複雑性が減少します。これは、管理トラフィック、したがって内部のプライベート トラフィックを VCS Expressway に限定し、外部からのアクセスをブロックします。

図 9-3　　DMZ での VCS Expressway



GLOSSARY

A

AES 高度暗号化規格

ASA Cisco 適応型セキュリティ アプライアンス

B

B2B Business-to-Business

BFCP Binary Floor Control Protocol

bps ビット / 秒

C

CA 認証局

CAPF Cisco Certificate Authority Proxy Function

CBWFQ クラスベースの重み付け均等化キューイング

CDP Cisco Discovery Protocol

CIF Common Intermediate Format

CSR 証明書署名要求

CTL 証明書信頼リスト

CTS Cisco TelePresence システム

D

DCT Display Channel Table

DHCP Dynamic Host Configuration Protocol

DID ダイヤル イン

DiffServ Differentiated Services

DMZ 非武装地帯

DNS ドメイン ネーム システム

DNS SRV DNS サービス

DSCP DiffServ コード ポイント

DSP デジタル シグナル プロセッサ

DTLS Datagram Transport Layer Security

E

ENUM Electronic Numbering

F

FECC 遠端カメラ制御

FIFO ファーストイン ファーストアウト

fps フレーム / 秒

G

GDR Gradual Decoder Refresh

H

HD 高解像度

HMAC ハッシュベースのメッセージ認証コード

HTTP ハイパーテキスト転送プロトコル

HTTPS ハイパーテキスト転送プロトコル セキュア

I

i インターレース ビデオ形式

IDR	Instant Decoder Refresh
IEC	国際電気標準会議
IETF	インターネット技術タスク フォース
IME	Cisco Intercompany Media Engine
IP	インターネット プロトコル
IPSec	インターネット プロトコル セキュリティ
IPv4	IP バージョン 4
IPv6	IP バージョン 6
ISDN	Integrated Services Digital Network（総合デジタル通信網）
ISO	国際標準化機構
ISR	Cisco Integrated Services Router
ITU	国際電気通信連合
ITU-T	国際電気通信連合電気通信標準化部門

L

LDAP	Lightweight Directory Access Protocol
LSC	ローカルで有効な証明書
LTRP	Long Term Reference Picture

M

MAC	メッセージ認証コード
MCU	マルチポイント コントロール ユニット
MIC	製造元でインストールされる証明書
MPEG	Moving Picture Experts Group
MPLS	マルチプロトコル ラベル スイッチング
MSE	Cisco TelePresence メディア サービス エンジン
MSI	Cisco メディア サービス インターフェイス
MXE	シスコ メディア エクスペリエンス エンジン

N

NAT ネットワーク アドレス変換

NAT-T ネットワーク アドレス変換トラバーサル

NTP ネットワーク タイム プロトコル

O

OBTP One Button To Push

P

p プログレッシブ スキャン

PKCS 公開キー暗号化規格

PKI 公開キー インフラストラクチャ

PQ プライオリティ キューイング

PVDM3 Cisco 高密度パケット音声ビデオ デジタル シグナル プロセッサ モジュール

Q

QCIF Quarter Common Intermediate Format

QoS Quality of Service

R

RFC コメント要求

RSVP リソース予約プロトコル

RTCP リアルタイム転送制御プロトコル

RTP リアルタイム転送プロトコル

S

SCCP Skinny Client Control Protocol

SD 標準解像度

SIP Session Initiation Protocol

SME Cisco Unified Communications Manager Session Management Edition

SRTCP セキュア リアルタイム転送制御プロトコル

SRTP セキュア リアルタイム転送プロトコル

SSH セキュア シェル

SSL Secure Sockets Layer

T

TCP 伝送制御プロトコル

TCS Cisco TelePresence コンテンツ サーバ

TLS トランスポート層セキュリティ

TMS Cisco TelePresence Management Suite

ToS Type of Service

TURN Traversal Using Relay NAT

U

UAC ユーザ エージェント クライアント

UAS ユーザ エージェント サーバ

UDP ユーザ データグラム プロトコル

Unified CM Cisco Unified Communications Manager

Unified CST Cisco Unified Communications Sizing Tool

URI ユニフォーム リソース識別子

USB Universal Serial Bus

UTF Unicode Transformation Format

V

VCL 仮想チャネル リンク

VCS Cisco TelePresence Video Communication Server

VLAN 仮想ローカル エリア ネットワーク

VoIP Voice over Internet Protocol

W

WFQ 重み付け均等化キューイング

こ

コーデック COmpressor-DECompressor（またはコーダ / デコーダ）

INDEX

数字

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

X

あ

い

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

つ

て

と

に

ね

は

ひ

ふ

へ

ほ

ま

め

も

ゆ

よ

り

れ

ろ