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。

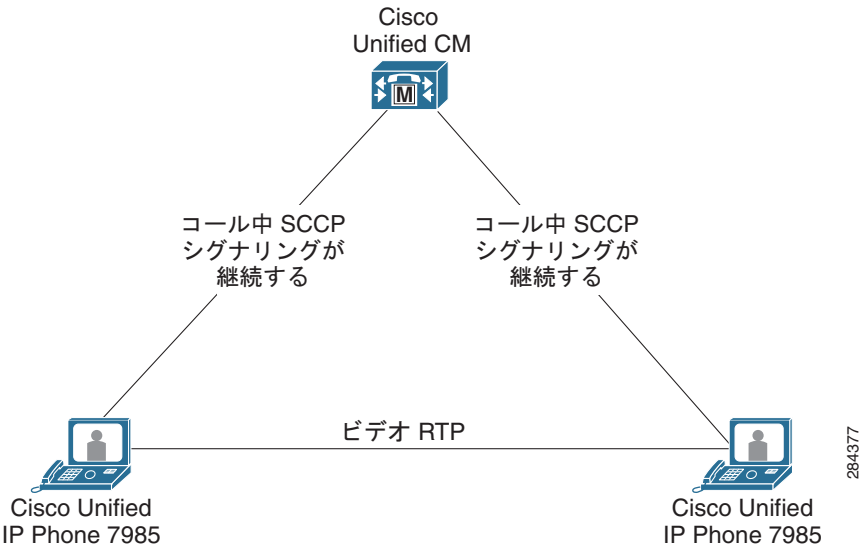
SCCP

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。

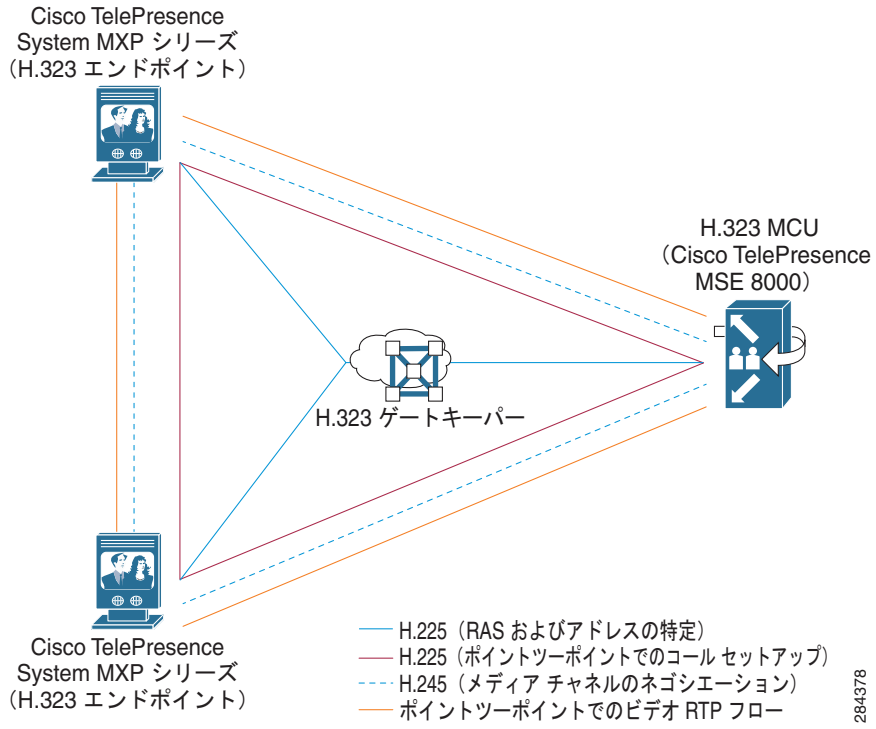
H.323

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。

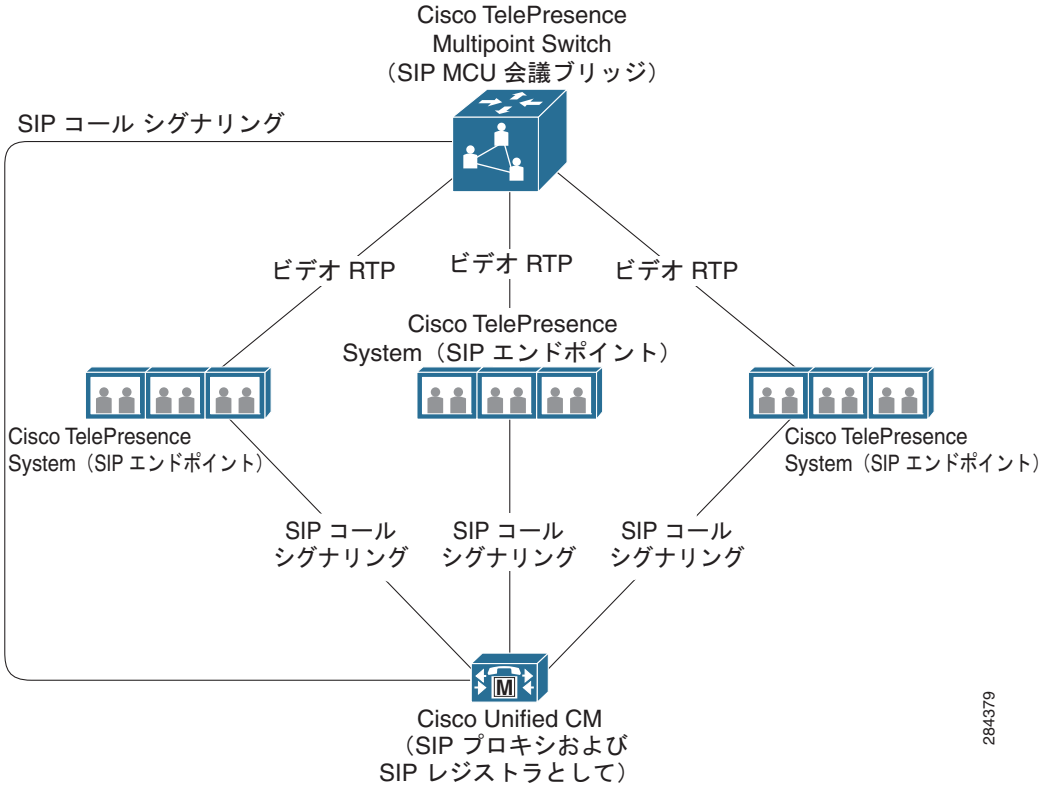
さらに、H.323 メッセージはバイナリ形式にエンコードされるため、適切なディセクタを使用することなくその内容を解釈することはかなり困難であり、プロトコル メッセージを実装した場合にはリトル エンディアンおよびビッグエンディアンのエラーが発生する可能性があります。H.323 メッセージは SIP メッセージよりサイズが小さいですが、帯域幅の差はほとんどありません。

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