CHAPTER 9

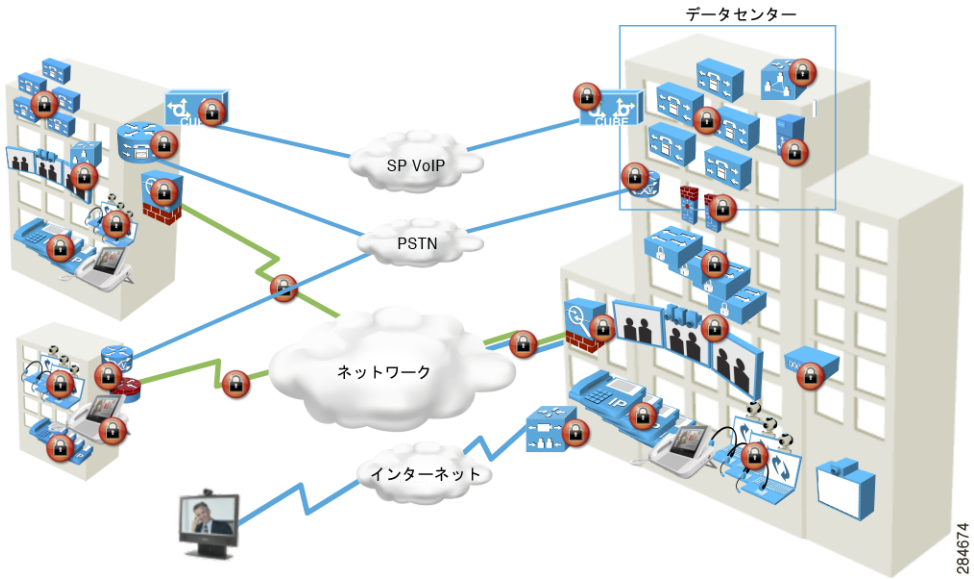
ビデオ コミュニケーションのセキュリティ

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。

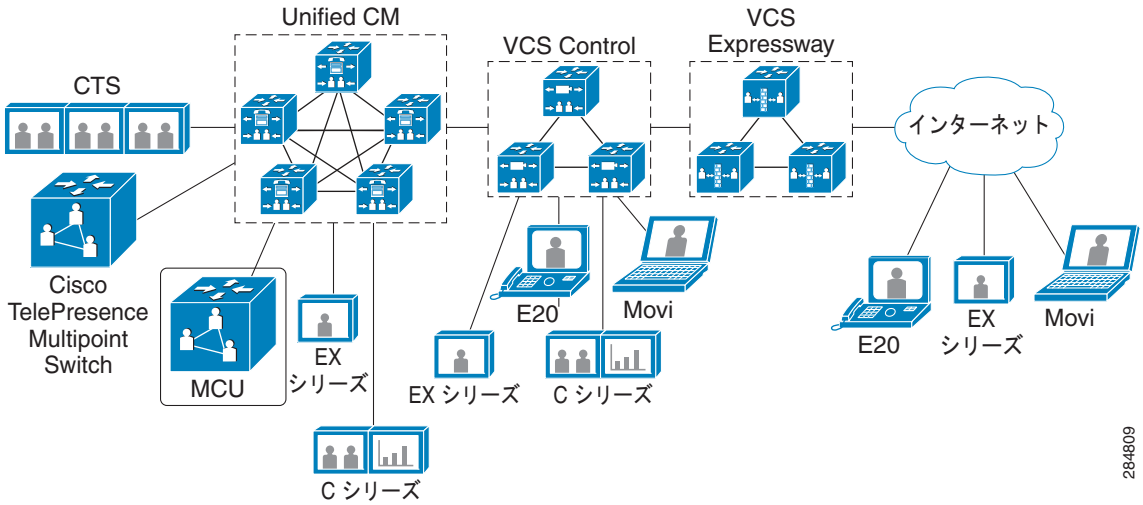
Cisco Unified CM で、コンフィギュレーション ファイルの暗号化を要求するデバイス セキュリティ プロファイルを作成できます。これにより、コンフィギュレーション ファイルは、Unified CM によりデジタル署名されるため、権限のないユーザによって変更されなくなります。

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