CHAPTER 16

音声セキュリティ

この章では、IP テレフォニー ネットワークを保護するためのガイドラインと推奨事項について説明します。この章のガイドラインに従うことは、安全な環境を保証するものではなく、ネットワーク上のすべての侵入攻撃を防止するものではありません。この章の目的は、テクノロジーに伴うリスクや利点について情報に基づいた選択ができるように、十分な情報を提供することです。リスク、利点、およびコストを慎重に考慮してから、任意のテクノロジーを配置してください。適切なセキュリティを達成するには、適切なセキュリティ ポリシーを確立し、そのセキュリティ ポリシーを適用する必要があります。また、ハッカーおよびセキュリティ コミュニティでの最新の動向を常に把握し、信頼性の高いシステム管理プラクティスによりすべてのシステムを保守および監視する必要があります。

この章で説明するセキュリティ ガイドラインは、IP テレフォニー テクノロジーおよび音声ネットワークに関連したものです。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 Web サイトで入手可能な 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/go/safe

この章では、集中型のコール処理について説明しますが、分散型コール処理については説明しません。WAN を介したクラスタ化は含まれていますが、Survivable Remote Site Telephony（SRST）などのローカル フェールオーバー メカニズムは含まれていません。この章では、ヘッドエンド障害が発生したときに、すべてのリモート サイトが、ヘッドエンドまたはローカル コール処理バックアップへの冗長リンクを使用できることを前提としています。基本的にここでは、ネットワーク アドレス変換（NAT）と IP テレフォニーの間の対話については説明しません。この章では、すべてのネットワークプライベート アドレスが指定されており、重複する IP アドレスが含まれていないことも前提としています。

セキュリティ ポリシー

この章では、企業が、すでにセキュリティ ポリシーを配置していることを前提としています。関連付けるセキュリティ ポリシーがない場合は、いかなるテクノロジーも配置しないようにお勧めします。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。各データ タイプで独自のセキュリティ ポリシーが必要な場合もあれば、必要でない場合もあります。

企業ネットワークにデータ用のセキュリティ ポリシーが存在しない場合、この章で任意のセキュリティ推奨事項を有効にする前に、セキュリティ ポリシーを作成する必要があります。セキュリティ ポリシーがないと、ネットワークで有効なセキュリティ機能が設計どおりに動作しているかどうかを検証する方法がありません。またセキュリティ ポリシーがないと、ネットワーク内で実行されるすべてのアプリケーションやデータ タイプに対してセキュリティを有効にする、体系的な方法がありません。

（注）　この章で説明するセキュリティに関するガイドラインと推奨事項に従うのは重要ですが、実際の企業のセキュリティ ポリシーを制定するには、この章のガイドラインと推奨事項だけでは不十分です。任意のセキュリティ テクノロジーを実装する前に、社内セキュリティ ポリシーを定義する必要があります。

この章では、ネットワーク上の音声データを保護するために使用可能な、シスコシステムズネットワークの機能と機能性について詳しく説明します。保護する対象のデータ、そのデータ タイプで必要な保護の程度、およびその保護を提供するのに使用するセキュリティ技法をどのように定義するかは、セキュリティ ポリシーによって異なります。

Voice over IP（VoIP）が含まれるセキュリティ ポリシーで困難な問題の 1 つは、通常、データ ネットワークと従来の音声ネットワークに存在するセキュリティ ポリシーの結合です。ネットワークへの音声データ統合のすべての側面が、導入済みのセキュリティ ポリシーまたは社内環境の適切なレベルで保護されていることを確認してください。

適切なセキュリティ ポリシーの基本は、ネットワーク内でデータの重要度を定義することです。重要度に応じてデータをランク付けしたら、データ タイプごとに、セキュリティ レベルを確立する方法を決定できます。それから、ネットワークとアプリケーション機能の両方を使用して、適切なレベルのセキュリティを達成できます。

要約すると、セキュリティ ポリシーを定義するには、次のプロセスに従います。

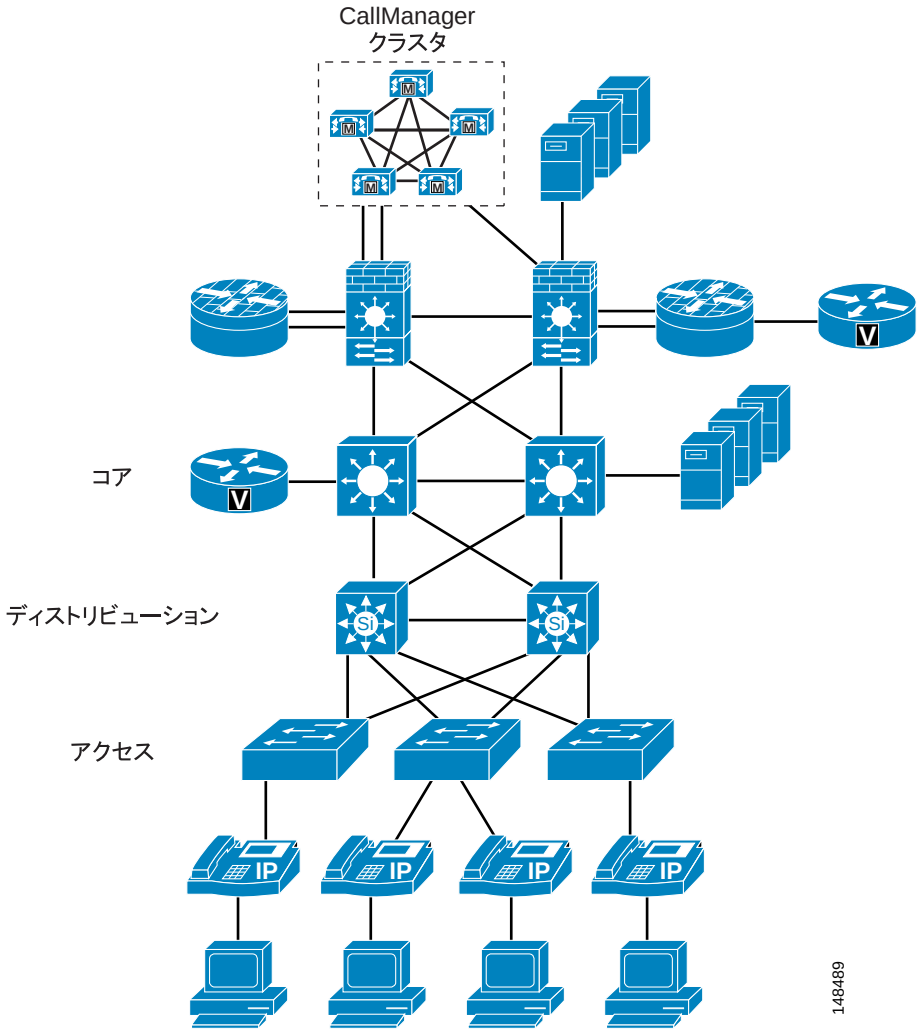
- ネットワーク上のデータを定義する。
- データの重要性を定義する。
- データの重要性に基づいてセキュリティを適用する。

セキュリティ レイヤ

この章では、最初にユーザが PC に接続できる電話機ポートについて説明します。また、電話機がネットワークを介して、アクセス スイッチ、ディストリビューション レイヤ、コア レイヤ、最後にデータ センターに到達する方法について説明します（図 16-1 を参照）。アクセス ポートからネットワーク自体に至るまで、セキュリティ レイヤの上にレイヤを構築します。各機能について説明するにあたり、社内セキュリティ ポリシーの観点から考慮する必要がある、それぞれの利点と欠点について説明します。

たとえば、図 16-1 は、IP テレフォニー ネットワークを使用することの利点と欠点の両方を示しています。音声製品は IP を使用してすべてのデバイスに接続するため、ネットワーク内の任意の場所に配置できます。この特性を使用すると、ネットワークの設計者は、VoIP アプリケーションを配置するのが物理的にも論理的にも簡単な場所に、デバイスを配置できます。しかし、簡単に配置できるということは、セキュリティがより複雑になることを意味します。接続性があるところであればネットワーク内のどこにでも、VoIP デバイスを配置できるからです。

図 16-1　セキュリティ レイヤ



IP アドレッシング

論理的に分離された VoIP ネットワークに流入および流出するデータを制御する上で、IP アドレッシングが重要になる場合があります。ネットワーク内で IP アドレッシングを適切に定義するほど、ネットワーク上のデバイスの制御は簡単になります。

このマニュアルの他の項で説明されているとおり（P.3-4 の「キャンパス アクセス レイヤ」を参照）、RFC 1918 に基づいた IP アドレッシングを使用する必要があります。このアドレッシング方式では、ネットワークの IP アドレッシングをやり直すことなく、IP テレフォニー システムをネットワークに配置できます。音声エンドポイントの IP アドレスは適切に定義されていて理解しやすいので、RFC 1918 を使用すると、ネットワーク内の制御をより適切に実行できます。すべての音声エンドポイントが 10.x.x.x. のネットワーク内でアドレッシングされていると、アクセス コントロール リスト（ACL）、およびこれらのデバイスが受信または送信するデータのトラックは単純になります。

利点

音声配置のために適切に定義された IP アドレッシング プランがあると、VoIP トラフィックを制御するための ACL の書き込みが簡単になり、ファイアウォールの配置に役立ちます。

RFC 1918 を使用すると、スイッチごとに 1 つの VLAN を簡単に配置でき、Voice VLAN を、スパニング ツリー プロトコル（STP）ループから保護できます。スイッチごとに 1 つの VLAN を配置するのは、キャンパスの設計におけるベストプラクティスです。

経路集約を正しく配置すると、ルーティング テーブルを、音声配置の前と同じ大きさか、それよりわずかに大きい程度に保つのに役立ちます。

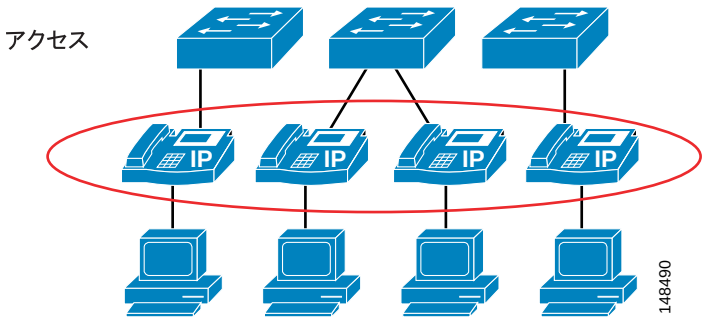
欠点

ルーティング テーブルが正しく設計されていなかったり、経路集約が使用されていなかったりすると、ルーティング テーブルは大きくなる場合があります。

電話機のセキュリティ

Cisco IP Phone には、VoIP ネットワーク上のセキュリティを強化するための組み込み型の機能があります。これらの機能を電話機単位で有効または無効にして、VoIP 配置のセキュリティを強化できます。セキュリティ ポリシーは、電話機の配置に応じて、これらの機能を有効にする必要があるかどうか、および有効にする必要がある場所を判別するのに役立ちます（図 16-2 を参照）。

図 16-2　電話機レベルでのセキュリティ



電話機のセキュリティ機能の設定を試みる前に、次のリンクで入手可能なマニュアルを参照して、特定の電話機モデルでそれらの機能が使用可能であることを確認してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/sec_vir/ae/sec413/secuphne.htm

電話機の PC ポート

電話機には、通常、PC を接続するための電話機の背面のポートを、オンまたはオフにする機能があります。この機能は、そのタイプの制御が必要な場合に、ネットワークにアクセスするためのコントロール ポイントとして使用できます。

セキュリティ ポリシーおよび電話機の配置状況によっては、特定の電話機の背面にある PC ポートを無効にする必要があります。このポートを無効にすると、電話機の背面にデバイスを接続したり、電話機自体を介してネットワークにアクセスしたりできなくなります。ロビーのような一般的なエリアに設置した電話機の場合、通常はポートを無効にします。ロビーでは物理的なセキュリティが非常に弱いため、ほとんどの企業では、制御されていないポートから不特定のユーザがネットワークにアクセスするのを許可しません。セキュリティ ポリシーで、電話機の PC ポートを経由してデバイスがネットワークにアクセスするのを許可しない場合は、通常の作業エリアに設置した電話機でも、ポートを無効にすることがあります。配置された電話機のモデルによっては、Cisco CallManager は、電話機の背面の PC ポートを無効にできます。この機能の有効化を試みる前に、次のリンクで入手可能なマニュアルを参照して、特定の Cisco IP Phone でこの機能がサポートされていることを確認してください。

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

利点

電話機の PC ポートを無効にすると、電話機からネットワークへのアクセスを禁止する必要があるエリアに電話機を配置できます。これにより、電話機の背面の PC ポートが有効であればアクセス可能だったはずのネットワークへのアクセスが制御されます。

欠点

電話機の PC ポートが無効な場合、ネットワーク アクセスを必要としているユーザで、アクセスのための承認を得ているユーザごとに、ネットワーク アクセスを提供する個別のイーサネット ポートを追加する必要があります。ユーザは、イーサネット ジャックを電話機から切断し、別のデバイスに接続することを試行できます。

Gratuitous ARP

ネットワーク上の他のデータ デバイスと同様、電話機が従来のデータ攻撃を受けることがあります。電話機には、企業ネットワークで発生する可能性がある、いくつかの一般的なデータ攻撃を防止する機能があります。そのような機能の 1 つは、Gratuitous APR（Gratuitous Address Resolution Protocol、つまり GARP）です。この機能は、電話機に対する man-in-the-middle（MITM; 中間者）攻撃を防止します。MITM 攻撃では、攻撃者は、エンド ステーションをだまして自らがルータであると信じ込ませ、ルータには自らがエンド ステーションであると信じ込ませます。この方式では、ルータとエンド ステーションの間のすべてのトラフィックが攻撃者を経由するようになり、攻撃者は、すべてのトラフィックをロギングしたり、データの会話に新しいトラフィックを注入したりできるようになります。

Gratuitous ARP は、攻撃者がネットワークの音声セグメントにアクセスできた場合に、攻撃者が電話機からのシグナリングや RTP 音声ストリームを取り込むことから電話機を保護するのに役立ちます。この機能で保護されるのは電話機だけです。インフラストラクチャの残りの部分は、Gratuitous ARP 攻撃から保護されません。スイッチ ポートには電話機とネットワーク デバイスの両方を保護する機能があるので、Cisco インフラストラクチャを実行している場合、この機能はそれほど重要ではありません。これらのスイッチ ポートの機能の説明については、P.16-12 の「スイッチ ポート」を参照してください。

利点

Gratuitous ARP 機能は、電話機から発信されてネットワークに至るシグナリングおよび RTP 音声ストリームに対する従来の MITM 攻撃から、電話機を保護します。

欠点

別の電話機から発信されたかネットワークを経由して到達するダウンストリーム シグナリングおよび RTP 音声ストリームは、電話機のこの機能では保護されません。保護されるのは、この機能が有効になっている電話機からのデータのみです（図 16-3 を参照）。

デフォルト ゲートウェイがホット スタンバイ ルータ プロトコル（HSRP）を実行している場合、HSRP 設定でデフォルト ゲートウェイの仮想 MAC アドレスの代わりにバーンドイン MAC アドレスが使用されている場合、およびプライマリ ルータが新しい MAC アドレスを持つセカンダリ ルータにフェールオーバーした場合、電話機はデフォルト ゲートウェイの古い MAC アドレスを保持できます。このシナリオでは、最大 40 分間の障害が発生することがあります。発生する可能性があるこの問題を避けるため、HSRP 環境では常に仮想 MAC アドレスを使用してください。

図 16-3　Gratuitous ARP は導入先の電話機は保護するが他のトラフィックは保護しない

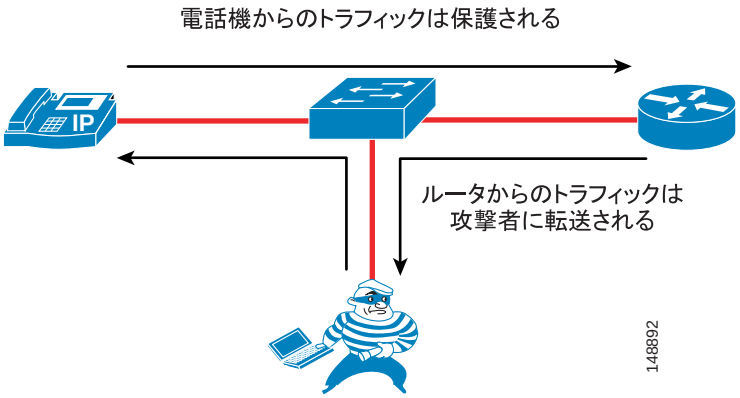


図 16-3 が示しているとおり、Gratuitous ARP 機能を持つ電話機からのトラフィックは保護されますが、エンドポイントに、データ フローを保護する機能がない可能性があるので、攻撃者が別のエンドポイントからのトラフィックを見ることができる場合があります。

PC Voice VLAN へのアクセス

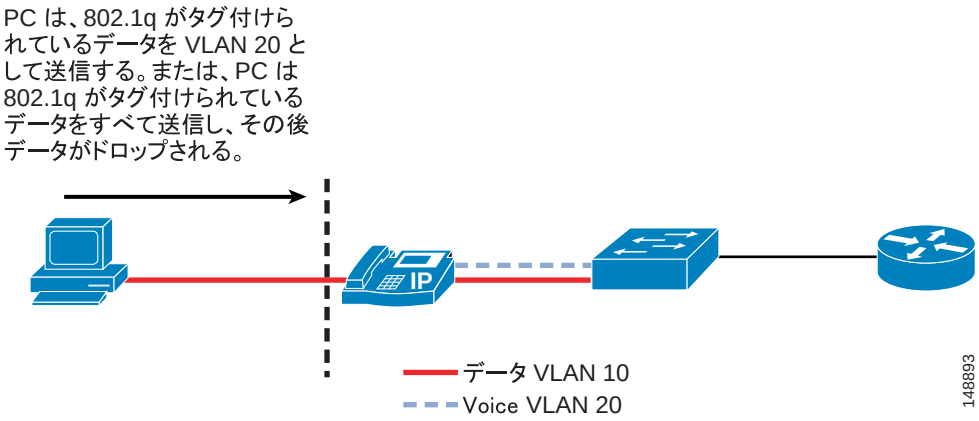
スイッチから電話機までに 2 つの VLAN が存在するので、電話機は、望まないアクセスから Voice VLAN を保護する必要があります。電話機では、電話機の背面から Voice VLAN に入り込む、望まないアクセスを防止できます。PC Voice VLAN Access 機能は、電話機の背面にある PC ポートから Voice VLAN への任意のアクセスを防止します。この機能を無効にすると、電話機の PC ポートに接続されたデバイスが、電話機の背面の PC ポートに到達する Voice VLAN を宛先とした 802.1q タグ付き情報を送信することにより、VLAN を「ジャンプ」して Voice VLAN にアクセスすることは許可されません。設定している電話機に応じて、この機能は 2 つの方法のいずれかで動作します。高機能の電話機では、電話機の背面の PC ポートに着信する Voice VLAN を宛先とした、すべてのトラフィックをブロックします。図 16-4 に示す例の場合、PC が、電話機の PC ポートに対して Voice VLAN トラフィック（このケースでは 200 の 802.1q タグ付き）の送信を試行すると、そのトラフィックはブロックされます。この機能が動作する他の方法は、電話機の PC ポートに着信する、802.1q タグ付きのすべてのトラフィック（Voice VLAN トラフィックに限らない）をブロックする方法です。

現在、アクセス ポートからの 802.1q タギングは、通常は使用しません。この機能が、電話機のポートに接続された PC の要件に含まれている場合、802.1q タグ付きパケットが電話機を通過するのを許可する電話機を使用する必要があります。

電話機の PC Voice VLAN Access 機能の設定を試みる前に、次のリンクで入手可能なマニュアルを参照して、特定の電話機モデルでそれらの機能が使用可能であることを確認してください。

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

図 16-4　電話機の PC ポートから Voice VLAN へのトラフィックのブロック



利点

PC Voice VLAN Access 機能は、攻撃者が、電話機の背面にある PC ポートを経由して、制御されていないデータを Voice VLAN に送信することを防止します。

欠点

電話機に接続されているデバイスが 802.1q タグ付きパケットを送信することが、通常は許可されている場合、これらのパケットはドロップされます。ほとんどのエンド ステーションでは、アクセス レイヤでこの機能を実行することが許可されていません。この機能がネットワーク内で通常の動作と見なされる場合、この機能が動作することは許可されません。

Web アクセス

各 Cisco IP Phone には、デバッグを実行したり管理目的で電話機のリモート ステータスを確認したりするのに役立つ、Web サーバが組み込まれています。Web サーバは、電話機が、Cisco CallManager から電話機にプッシュされたアプリケーションを受信するのを可能にします。この Web サーバへのアクセスは、Cisco CallManager 設定の Web Access 機能を使用して、電話機で有効または無効にできます。この設定は、グローバルで行うことも、電話機ごとに有効または無効にすることもできます。

利点

電話機の Web アクセスを有効にすると、電話機やネットワークの問題をデバッグするときにその電話機を使用できます。電話機からの Web アクセスを無効にすると、ユーザまたは攻撃者は、VoIP ネットワークに関する情報をその電話機から入手できません。

欠点

電話機からの Web アクセスを無効にすると、ネットワークや VoIP の問題をデバッグするのがより困難になります。Web サーバがグローバルで無効だが、デバッグの参考として必要な場合、Cisco CallManager の管理者は、電話機のこの機能を有効にする必要があります。この Web ページにアクセスする機能は、ネットワークの ACL で制御できます。ネットワーク オペレータは、この機能を使用して、必要なときに Web ページにアクセスできます。

Web アクセス機能を無効にすると、電話機は、Cisco CallManager からプッシュされるアプリケーションを受信できません。

アクセス設定

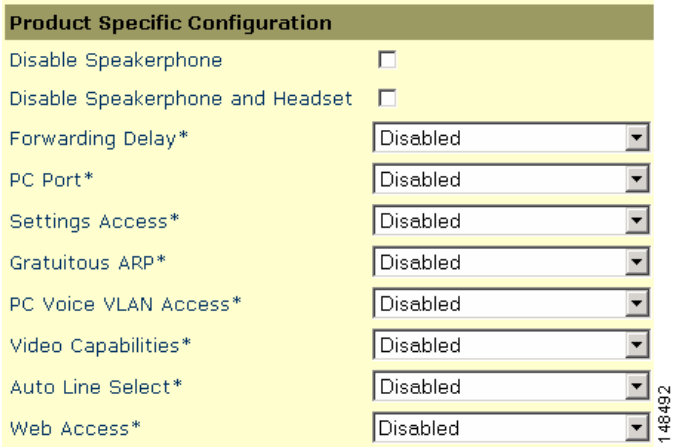
各 Cisco IP Phone にはネットワーク設定ページがあり、そのページには、電話機が動作するのに必要な多くのネットワーク要素や詳細情報がリストされます。攻撃者はこの情報を使用して、電話機の Web ページに表示される情報の一部と共に、ネットワーク上で調査を開始できます。たとえば、攻撃者は設定ページを参照して、デフォルト ゲートウェイ、TFTP サーバ、および Cisco CallManager の IP アドレスを判別できます。これらの断片的な情報が、音声ネットワークにアクセスしたり、音声ネットワーク内のデバイスを攻撃したりするのに使用される場合があります。

このアクセスを電話機ごとに無効にすることにより（図 16-5 を参照）、エンド ユーザまたは攻撃者が、Cisco CallManager IP アドレスや TFTP サーバ情報などの追加情報を取得するのを防止できます。

電話機の設定ページの詳細については、次の Web サイトで入手可能な『Cisco IP Phone Authentication and Encryption for Cisco CallManager』を参照してください。

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

図 16-5　Cisco CallManager の Phone Configuration ページ



利点

電話機設定ページへのアクセスを無効にすると、エンド ユーザおよび攻撃を仕掛けようとしている人が、ネットワークに関する詳細情報や音声システムで使用される VoIP 情報を見ることはできません。この機能を無効にしたときに保護される情報には、電話機の IP アドレス、電話機の登録先の Cisco CallManager、および電話機が最後に呼び出したデバイスなどの情報が含まれます。

欠点

電話機設定ページへのアクセスを無効にすると、エンド ユーザは、スピーカー ボリューム、連絡先、呼び出しタイプなど、通常は制御可能な多くの電話機設定を変更できなくなります。電話機インターフェイスについてエンド ユーザに課される制限により、このセキュリティ機能を使用することが現実的ではない場合があります。

Voice VLAN および CDP

電話機に IP アドレスが与えられる前に、電話機は、電話機とスイッチの間で実行される Cisco Discovery Protocol（CDP）ネゴシエーションを使用して、配置先として適切な VLAN を判別します。このネゴシエーションにより、電話機は「Voice VLAN」内のスイッチに対して 802.1q タグ付きのパケットを送信でき、音声データと、電話機の背後にある PC から送られる他のすべてのデータはレイヤ 2 で分離されます。Voice VLAN は電話機が動作するための要件ではありませんが、ネットワーク上の他のデータからの追加の分離を提供します。

利点

Voice VLAN は、スイッチから電話機に自動的に割り当てることができます。これにより、レイヤ 2 およびレイヤ 3 で、音声データと、ネットワーク上の他のすべてのデータが分離されます。分離した VLAN には Dynamic Host Configuration Protocol（DHCP）サーバで別個の IP スコープを与えることができるので、Voice VLAN を使用すると、異なる IP アドレッシング スキームを実行できます。

アプリケーションは、電話機からの CDP メッセージを使用して、緊急電話コール中に電話機のロケーションを判別するのを支援します。電話機が接続されているアクセス ポートで CDP が有効ではない場合、電話機のロケーションを判別するのは特に困難です。その場合、Cisco ER は 911 コールで電話機のロケーションを判別できません。

欠点

通常は電話機に送られる CDP メッセージから情報が収集され、その情報が一部のネットワークを検出するために使用される可能性があります。

電話機の認証および暗号化

Cisco CallManager では、音声システム内の電話機に対して複数のレベルのセキュリティを適用するように設定できます。ただし、電話機でこれらの機能がサポートされている必要があります。導入済みのセキュリティ ポリシー、電話機の配置、および電話機サポートに応じて、社内の必要に合せてセキュリティを設定できます。

特定のセキュリティ機能に対する Cisco IP Phone モデルのサポート状況の詳細については、次の Web サイトで入手可能なマニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/

電話機および Cisco CallManager クラスタでセキュリティを有効にするには、次の Web サイトで入手可能な『Cisco CallManager Security Guide』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/sec_vir/ae/sec413/

利点

Cisco CallManager でセキュリティ機能が正しく設定されている場合、サポートされているすべての電話機で、次の機能を使用できます。

- 完全性 : 電話機に対する TFTP ファイル操作およびトランスポート レイヤ セキュリティ（TLS）シグナリングを許可しません。
- 認証：電話機のイメージは、Cisco CallManager から電話機に対して認証され、デバイス（電話機）は Cisco CallManager に対して認証されます。電話機と Cisco CallManager の間のすべてのシグナリング メッセージは、認可されているデバイスから送信されるときに検証されます。
- 暗号化：サポートされているデバイスで、盗聴を防止するためシグナリングとメディアを暗号化できます。
- Secure Real-time Transport Protocol（SRTP）: Cisco IOS MGCP ゲートウェイでサポートされています。Cisco Unity もボイスメールの SRTP をサポートしています。

欠点

Cisco CallManager は、メディア サービスが使用されていない単一クラスタにおける、2 つの Cisco IP Phone の間のコールの、認証、完全性、および暗号化をサポートしています。ただし、すべてのデバイスまたは電話機の認証、完全性、または暗号化を提供しているわけではありません。ご使用のデバイスがこれらの機能をサポートしているかどうかを判別するには、次の Web サイトで入手可能なマニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/

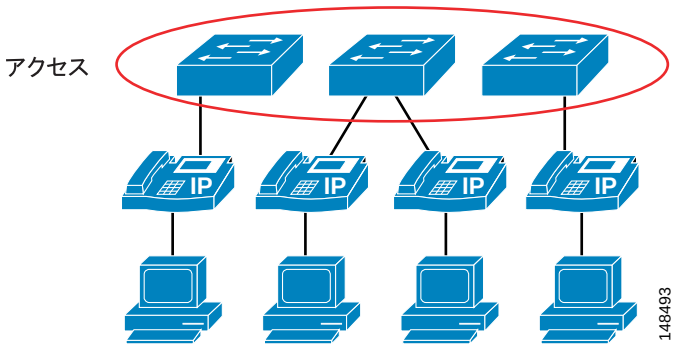
クラスタを混合モードで設定すると、自動登録は動作しません。混合モードは、デバイス認証に必要なモードです。クラスタにデバイス認証が存在しない場合、つまり、Cisco Certificate Trust List（CTL）クライアントがインストールおよび設定されていない場合、シグナリングまたはメディア暗号化を実装することはできません。VoIP がファイアウォールおよびネットワーク アドレス変換（NAT）を通過するのを可能にするアプリケーション レイヤ ゲートウェイ（ALG）も、シグナリング暗号化では動作しません。暗号化されたメディアでは、一部のゲートウェイ、電話機、または会議はサポートされません。

スイッチ ポート

Cisco スイッチ インフラストラクチャには、データ ネットワークを保護するために使用できる多くのセキュリティ機能があります。ここでは、ネットワーク内の VoIP データを保護するため、Cisco Access Switch で使用できるいくつかの機能について説明します（図 16-6 を参照）。この項では、現在のすべての Cisco スイッチで使用可能なすべてのセキュリティ機能について説明するのではなく、シスコが製造する多くのスイッチで使用されている一般的なセキュリティ機能をリストします。ネットワーク内に配置された特定の Cisco デバイスで使用可能なセキュリティ機能の追加情報については、次の Web サイトで入手可能な適切な製品マニュアルを参照してください。

http://www.cisco.com

図 16-6　電話機が接続される代表的なアクセス レイヤ設計



ポート セキュリティ：MAC CAM フラッディング

スイッチ ネットワークに対する典型的な攻撃は、MAC 連想メモリ（CAM）フラッディング攻撃です。このタイプの攻撃では、スイッチに対して大量の MAC アドレスによるフラッディングが実行され、スイッチは、エンド ステーションが接続されているポートを判別できなくなります。デバイスが接続されているポートを判別できない場合、スイッチは、そのデバイスが宛先になっているトラフィックを VLAN 全体にブロードキャストします。これにより、攻撃者は、VLAN 内のすべてのユーザに到達するすべてのトラフィックを見ることができます。

macof などのハッカー ツールを使用した悪意のある MAC フラッディング攻撃を許可しないようにするには、それらのポートの接続性要件に基づいて、個々のポートへのアクセスを許可されている MAC アドレスの数を制限します。悪意のあるエンドユーザ ステーションは、macof を使用して、ランダムに生成された送信元 MAC アドレスからランダムに生成された宛先 MAC アドレスへの MAC フラッディングを発信できます。送信元と宛先の両方がスイッチポートに直接接続されている場合もあれば、送信元と宛先が IP Phone を経由して接続する場合もあります。macof ツールは非常にアグレッシブなツールで、通常は、Cisco Catalyst スイッチの連想メモリ（CAM）テーブルを 10 秒未満でいっぱいにすることができます。CAM テーブルがいっぱいなので、後続のパケットは取得されないまま残され、フラッディングが発生します。これは、攻撃先の VLAN の共有イーサネット ハブ上のパケットと同じほど破壊的で危険です。

MAC フラッディング攻撃を抑制するには、ポート セキュリティまたはダイナミック ポート セキュリティのいずれかを使用できます。許可メカニズムとしてポート セキュリティを使用する必要がないカスタマーの場合、特定のポートに接続する機能に対応する数の MAC アドレスを持つダイナミック ポート セキュリティを使用できます。たとえば、1 台のワークステーションが接続されているポートの場合、取得する MAC アドレスの数を 1 に制限できます。1 台の Cisco IP Phone と、その

背後に 1 台のワークステーションが接続されているポートの場合、電話機の PC ポートに 1 台のワークステーションを接続するには、取得する MAC アドレスを 2 に設定できます（1 つは IP Phone 用、1 つは電話機の背後にあるワークステーション用）。以前であれば、トランク モードでポートを設定する旧来の方法により、この場合の設定は 3 つの MAC アドレスになります。電話機ポートの設定でマルチ VLAN アクセス モードを使用する場合、この場合の設定は 2 つの MAC アドレスになります。1 つは電話機用、1 つは電話機に接続された PC 用です。PC ポートに接続するワークステーションがない場合、そのポートの MAC アドレスの数は 1 に設定する必要があります。これらの設定は、スイッチ上のマルチ VLAN アクセス ポート用です。トランク モードに設定されているポート（電話機と PC が接続されているアクセス ポートでは推奨されていない配置）では、設定が異なる場合があります。

ポート セキュリティ：ポート アクセスの防止

MAC アドレスによりポートで指定されているデバイスからのアクセスを除く、すべてのポート アクセスを防止します。これは、デバイスレベルのセキュリティ許可の 1 つの形式です。この要件は、デバイス MAC アドレスの単一のクレデンシャルを使用してネットワークへのアクセスを許可するときに使用します。ポート セキュリティ（非動的形式）を使用する場合、ネットワーク管理者は、すべてのポートに MAC アドレスを静的に関連付ける必要があります。これに対して、動的ポート セキュリティを使用する場合、ネットワーク管理者は、スイッチで取得する MAC アドレスの数を指定するだけです。その後、ポートに最初に接続するデバイスが適切なデバイスであるとの前提に基づき、一定期間、それらのデバイスにのみポートへのアクセスを許可します。

この期間は、固定タイマーまたは非活動タイマー（非持続アクセス）のいずれかで決定するか、永続的に割り当てることができます。永続的に MAC アドレスを割り当てる機能は、Cisco 6000 スイッチでは*自動設定*と呼ばれ、Cisco Catalyst 4500、2550、2750、または 2950 スイッチでは*スティッキ*と呼ばれます。どちらの場合も、スイッチのリロードまたはリブートが発生しても、取得された MAC アドレスはポートで保持されます。

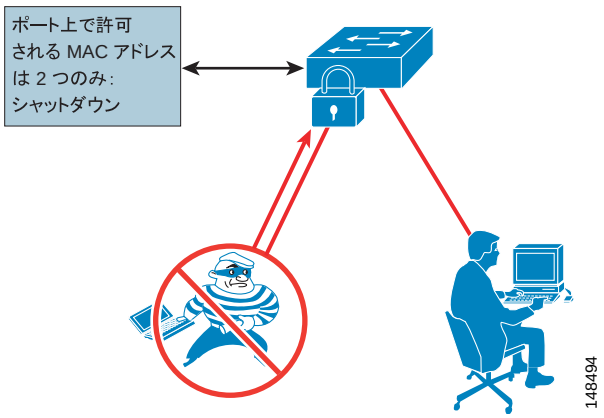
自動設定またはスティッキを使用した MAC アドレスの持続割り当ては、コマンドを使用してのみクリアできます。現在、Cisco Catalyst スイッチング プラットフォーム全体で最も一般的なデフォルト動作は、非持続動作です。この動作は、Cisco CatOS Release 7.6（1）が持続的になる前に、唯一有効だった動作です。デバイス モビリティに対し、静的ポート セキュリティまたは持続性のある動的ポート セキュリティによるプロビジョニングは行われません。最重要の要件ではありませんが、MAC フラッディング攻撃は、特定の MAC アドレスへのアクセスを制限することを目的としているポート セキュリティにより暗黙的に防止されます。

セキュリティ面を考慮すると、ポート アクセスを認証および許可するためのより強力なメカニズムがあります。MAC アドレス許可ではなく、ユーザ ID およびパスワード クレデンシャルに基づいたメカニズムです。MAC アドレスだけでは、ほとんどのオペレーティング システムで簡単にスプーフィングまたは偽造されます。

ポート セキュリティ：不良ネットワーク拡張の防止

ハブまたは無線アクセス ポイント（AP）を経由する不良なネットワーク拡張を防止します。ポート セキュリティは 1 つのポートでの MAC アドレスの数を制限するので、ポート セキュリティを、IT で作成されたネットワークへのユーザ拡張を抑制するためのメカニズムとして使用することもできます。たとえば、ユーザ方向のポート、または単一の MAC アドレス用にポート セキュリティが定義された電話機のデータ ポートに、ユーザが無線 AP を接続した場合、無線 AP 自体がその MAC アドレスを占有し、背後にあるデバイスはネットワークにアクセスできません。（図 16-7 を参照）。一般的に、MAC フラッディングを停止するのに適切な設定は、不良アクセスを抑制するためにも適切です。

図 16-7　MAC アドレス数の制限による不良ネットワーク拡張の防止



利点

ポート セキュリティは、攻撃者がスイッチの CAM テーブルに対してフラッディングを実行したり、すべての受信トラフィックをすべてのポートに送信するハブに VLAN を転送したりするのを防止します。また、エンドポイントにハブまたはスイッチを追加することにより、認可されていないネットワークの拡張を防止します。

欠点

MAC アドレスの数が正しく定義されていないと、ネットワークへのアクセスが拒否されたり、エラーによりポートが無効化されてすべてのデバイスがネットワークから削除されたりする場合があります。

設定例

（注）　この設定例は、これらの機能をサポートするために適切なコード レベルを実行しているスイッチに基づいています。電話機へのトランク モードは実行されません。

次の例は、データ ポートにデバイスが接続されている電話機に対して、ダイナミック ポート セキュリティを使用してアクセス ポートを設定する Cisco IOS コマンドを示しています。

```
switchport access vlan 10
switchport mode access
switchport voice vlan 20
switchport port-security
switchport port-security maximum 2
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
```

上記の例のコマンドは、次の機能を実行します。

- **switchport port-security** *x/x* **enable**

  このコマンドは、指定したモジュール / ポートでポート セキュリティを有効にします。

- **switchport port-security violation restrict**

  このコマンドが、推奨されている設定です。デフォルトでは、ポートを無効にします。ポートを **restrict** すると、ポートは、MAC アドレスの最大数に達するまで MAC アドレスを取得し、その後は新しい MAC アドレスの取得を停止します。ポートの設定がデフォルトの **disable** の場合、MAC アドレスの最大数に達すると、ポートはエラーを無効化し、電話機の電源を切ります。ポートを再有効化するデフォルト タイマーは、5 分です。導入済みのセキュリティ ポリシーによっては、ポートを無効にすることにより電話機をシャットダウンせずに、ポートを制限した方が適切な場合があります。

- **switchport port-security aging time 2**

  このコマンドは、MAC アドレスからのトラフィックがない状態で、その MAC アドレスをポートで保持する時間を設定します。一部のスイッチと電話機の間の CDP 通信を考慮に入れると、推奨されている最小時間は 2 分です。

- **switchport port-security aging type inactivity**

  このコマンドは、取得した MAC アドレスをタイムアウトするために、ポートで使用されるエージングのタイプを定義します。

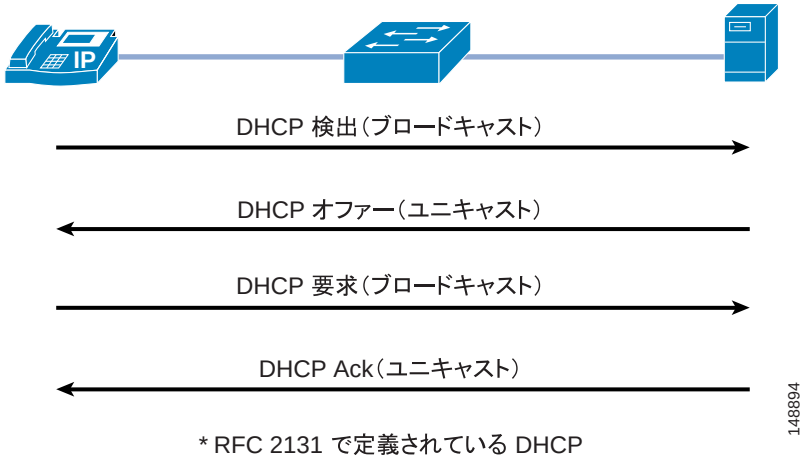
DHCP スヌーピング：不正な DHCP サーバ攻撃の防止

Dynamic Host Configuration Protocol（DHCP）スヌーピングは、承認されていない DHCP または不正な DHCP サーバがネットワーク上で IP アドレスを分配するのを防止します。具体的には、ポートが応答することが許可されている場合を除き、DHCP 要求へのすべての応答をブロックします。ほとんどの電話機配置では DHCP を使用して複数の電話機に IP アドレスを提供しているので、スイッチで DHCP スヌーピング機能を使用して、DHCP メッセージングを保護する必要があります。不正な DHCP サーバは、クライアントからのブロードキャスト メッセージに応答して不正な IP アドレスを分配したり、IP アドレスを要求しているクライアントを混乱させたりすることを試行できます。

DHCP スヌーピングを有効にすると、デフォルトでは、VLAN のすべてのポートが、信頼されていないポートとして扱われます。信頼されていないポートとは、予約済みの DHCP 応答を行うことが許可されていない、ユーザ方向のポートのことです。信頼されていない DHCP スヌーピング ポートが DHCP サーバ応答を行うと、ブロックされて応答されません。このように、不正な DHCP サーバが応答することが防止されます。ただし、正当に接続された DHCP サーバまたは正当なサーバへのアップリンクは、信頼する必要があります。

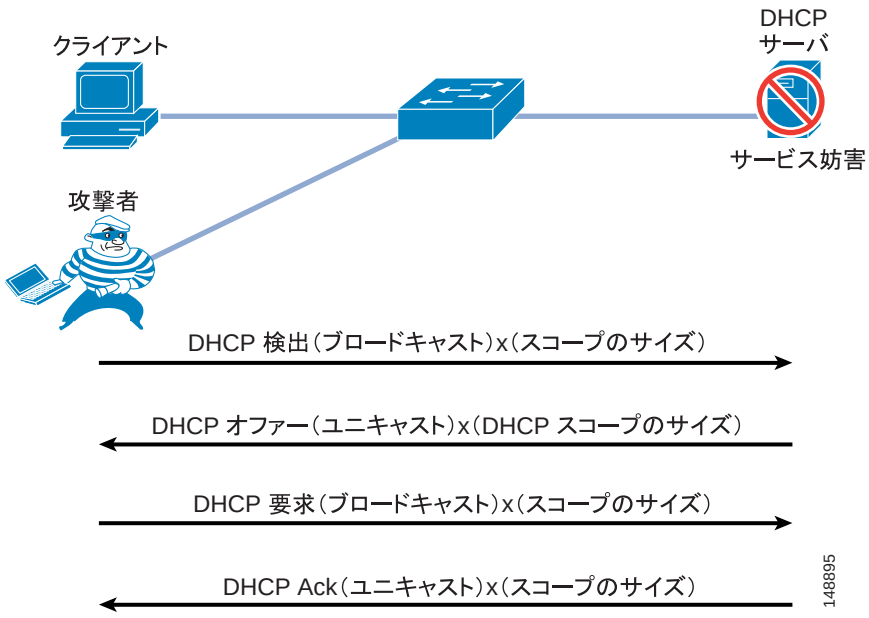
図 16-8 は、DHCP サーバから IP アドレスを要求するネットワーク接続デバイスの通常の操作を示しています。

図 16-8　DHCP 要求の通常の操作



ただし、攻撃者は、単一の IP アドレスではなく、VLAN 内で使用可能なすべての IP アドレスを要求できます（図 16-9 を参照）。これは、ネットワークへのアクセスを試みている正当なデバイスのための IP アドレスが存在しないことを意味します。IP アドレスがないと、電話機は Cisco CallManager に接続できません。

図 16-9　攻撃者は VLAN で使用可能なすべての IP アドレスを取得できる



利点

DHCP スヌーピングは、承認されていない DHCP サーバがネットワークに配置されるのを防止します。

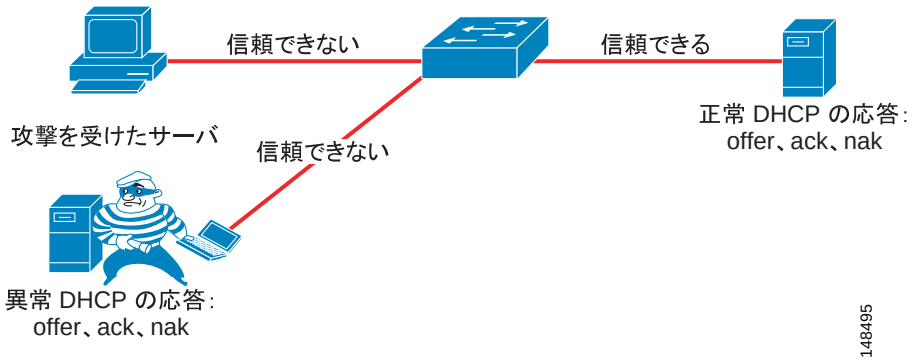
欠点

この機能が正しく設定されていないと、認定ユーザの IP アドレスが拒否される場合があります。

DHCP スヌーピング：DHCP スターベーション攻撃の防止

Gobbler などのツールを使用した DHCP アドレス スコープ スターベーション攻撃は、DHCP DoS 攻撃（サービス拒絶攻撃）を仕掛けるために使用されます。Gobbler ツールは、ランダムに生成される異なる送信元 MAC アドレスから DHCP 要求を実行するので、ポート セキュリティを使用して MAC アドレスの数を制限することにより、Gobbler ツールが DHCP アドレス スペースをスタービングするのを防止できます（図 16-10 を参照）。ただし、高度な DHCP スターベーション ツールでは、1 つの送信元 MAC アドレスから DHCP 要求を実行でき、DHCP ペイロード情報も多様です。DHCP スヌーピングを有効にすると、信頼されていないポートで、送信元 MAC アドレスと DHCP ペイロード情報が比較され、それらが一致しない場合は要求が失敗します。

図 16-10　DHCP スヌーピングを使用した DHCP スターベーション攻撃の防止



利点

DHCP スヌーピングは、単一のデバイスが、特定の範囲内のすべての IP アドレスを取得するのを防止します。

欠点

この機能が正しく設定されていないと、認定ユーザの IP アドレスが拒否される場合があります。

設定例

次の例は、データ ポートにデバイスが接続されている電話機に対して、DHCP スヌーピングを使用してアクセス ポートを設定する Cisco IOS コマンドを示しています。

- グローバル コマンド

```
ip dhcp snooping vlan 10, 20
no ip dhcp snooping information option
ip dhcp snooping
```

- インターフェイス コマンド

```
no ip dhcp snooping trust (Default)
ip dhcp snooping limit rate 10 (pps)
ip dhcp snooping trust
```

上記の例のグローバル コマンドは、次の機能を実行します。

- **ip dhcp snooping vlan 10, 20**

  このコマンドは、DHCP スヌーピングが有効になっている VLAN を特定します。

- **No ip dhcp snooping information option**

  DHCP アドレスをリースするのに Option 82 情報が要求されないようにするため、このコマンドを使用する必要があります。Option 82 情報は DHCP サーバでサポートされている必要がありますが、ほとんどの企業サーバは、この機能をサポートしていません。Option 82 は Cisco IOS DHCP サーバでサポートされています。

- **ip dhcp snooping**

  このコマンドは、スイッチで、グローバル レベルでの DHCP スヌーピングを有効にします。

上記の例のインターフェイス コマンドは、次の機能を実行します。

- **no ip dhcp snooping trust**

  このコマンドは、DHCP サーバからポートに着信する情報をすべて信頼しないようにインターフェイスを設定します。

- **ip dhcp snooping limit rate 10**

  このコマンドは、DHCP スヌーピングが最初に設定されるときにインターフェイスで設定される、デフォルトのレート制限を設定します。この値は、導入済みのセキュリティ ポリシーに合せて変更できます。

- **ip dhcp snooping trust**

  このコマンドは、DHCP サーバから DHCP 情報を送信するときに経由するポートに対して実行します。DHCP 情報の送信元のポートを信頼できない場合、いずれのデバイスも DHCP アドレスを受信しません。この情報がクライアントに到達するようにするには、DHCP サーバが接続されている最低 1 つのポート（アクセス ポートまたはトランク ポート）を設定する必要があります。このコマンドは、固定 IP アドレスが与えられていて、IP アドレスを取得するために DHCP を使用しないポートに接続されている、任意のデバイスを信頼するためにも使用できます。DHCP サーバへのアップリンク ポート、または DHCP サーバへのトランク ポートも信頼する必要があります。

DHCP スヌーピング：バインディング情報

DHCP スヌーピングには、DHCP サーバから正常に IP アドレスを取得する、信頼されていないポートの DHCP バインディング情報を記録するという機能もあります。バインディング情報は、Cisco Catalyst スイッチ上のテーブルに記録されます。DHCP バインディング テーブルには、各バインディング エントリの IP アドレス、MAC アドレス、リース長、ポート、および VLAN 情報が格納されます。DHCP スヌーピングから取得されたバインディング情報は、DHCP サーバで設定された DHCP バインディング期間（つまり、DHCP リース時間）の間、有効です。DHCP バインディング情報は、ARP 応答を、DHCP でバインディングされているアドレスに限定する目的で、Dynamic ARP Inspection（DAI）の動的エントリを作成するときに使用されます。DHCP バインディング情報は、IP パケットの送信元を、DHCP でバインディングされたアドレスに限定するために、IP ソース ガードでも使用されます。

次の例は、DHCP スヌーピングからのバインディング情報を示しています。

- Cisco IOS のバインディング情報の表示：

```
show ip dhcp snooping binding
MacAddress          IpAddress     Lease(sec)     Type            VLAN Interface
----------          ---------     ----------     -------------   ---- ---------
00:03:47:B5:9F:AD   10.120.4.10       193185     dhcp-snooping   10
FastEthernet3/18
```

- Cisco CatOS のバインディング情報の表示：

```
ngcs-6500-1> (enable) show dhcp-snooping bindings
MacAddress          IpAddress       Lease(sec)      VLAN      Port
------------------  --------------- ----------      ----      -----
00-10-a4-92-bf-dd   10.10.10.21          41303      10        2/5
```

DHCP スヌーピングのために各タイプのスイッチに格納できるバインディング テーブル エントリには、最大制限があります（この制限を判別するには、使用するスイッチの製品マニュアルを参照してください）。スイッチのバインディング テーブル内のエントリ数が気になる場合は、バインディング テーブルのエントリがより早くタイムアウトになるように、DHCP 範囲のリース時間を短縮できます。リースが期限切れになるまで、これらのエントリは DHCP バインディング テーブルに残されます。言い換えると、エンド ステーションがそのアドレスを持っていると DHCP サーバが判断するかぎり、これらのエントリは DHCP スヌーピング バインディング テーブルに残されます。ワークステーションまたは電話機を切断しても、これらのエントリはポートから除去されません。

Cisco IP Phone がポートに接続されており、それを別のポートに移動した場合、DHCP バインディング テーブルには、同じ MAC アドレスと IP アドレスを持つがポートが異なっている 2 つのエントリが含まれることがあります。この動作は、通常の動作と見なされます。

Dynamic ARP Inspection の要件

Dynamic Address Resolution Protocol（ARP）Inspection（DAI）は、ルータのスイッチに接続されたデバイスに対する Gratuitous ARP 攻撃を防止するために、スイッチで使用される機能です。Dynamic ARP はすでに説明した電話機の Gratuitous ARP 機能と似ていますが、LAN 上のすべてのデバイスを保護するので、単なる電話機の機能ではありません。

基本的な機能である Address Resolution Protocol（ARP）を使用すると、ステーションで MAC アドレスを ARP キャッシュ内の IP アドレスにバインドできるようになり、これにより 2 つのステーションが LAN セグメント上で通信可能になります。ステーションは、ARP 要求を 1 つの MAC ブロードキャストとして送出します。要求に含まれる IP アドレスを所有するステーションは、要求元のステーションに、ARP 応答を（IP アドレスと MAC アドレスと共に）送ります。要求元のステーションは、その応答を、ライフタイムの制限がある ARP キャッシュにキャッシュします。ARP キャッシュのデフォルトのライフタイムは、Microsoft Windows では 2 分間、Linux では 30 秒間、Cisco IP Phone では 40 分です。

また ARP は、Gratuitous ARP と呼ばれる機能を提供します。Gratuitous ARP（GARP）は、要求がなくても送信される ARP 応答です。通常の使用法では、MAC ブロードキャストとして送信されます。GARP メッセージを受信する、LAN セグメント上のすべてのステーションは、この非請求 ARP 応答をキャッシュに入れます。この非請求 ARP 応答により、送信者が、GARP メッセージに含まれる IP アドレスのオーナーであることが認定されます。Gratuitous ARP には、障害時に別のステーションのアドレスを引き継ぐ必要があるステーションを正当に使用します。

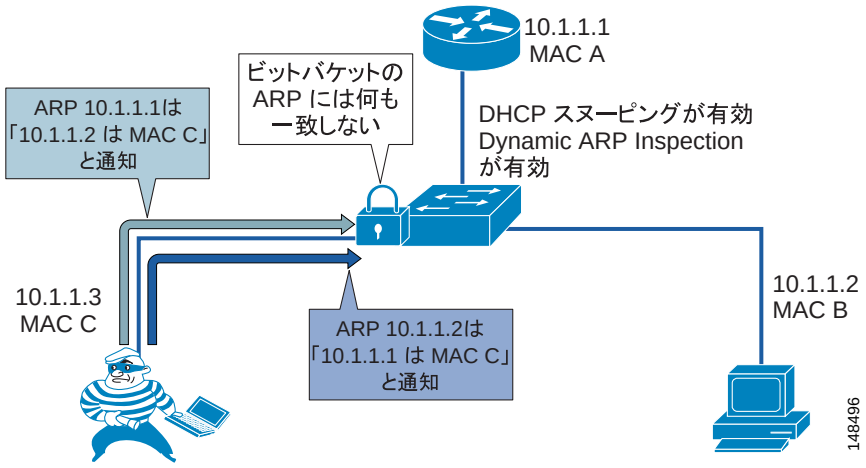
ただし、Gratuitous ARP は、別のステーションの身分を不正にかたること目的とした悪質なプログラムにより悪用される可能性もあります。悪質なステーションが、相互に通信しているその他の 2 つのステーションのトラフィックを自らにリダイレクトすると、GARP メッセージを送信したハッカーが中間者になります。ettercap などのハッカー プログラムは、このことを精密に行うため、GARP メッセージをブロードキャストするのではなく、「プライベートな」GARP メッセージを特定の MAC アドレスに発行します。これにより、攻撃の犠牲者は、自分のアドレスに対する GARP パケットを見ることができません。Ettercap は、プライベートな GARP メッセージを 30 秒ごとに繰り返し送信することにより、ARP ポイズニングを有効な状態に保持します。

Dyamic ARP Inspection（DAI）は、信頼されていない（またはユーザ報告の）ポートからのすべての ARP 要求および応答（Gratuitous または非 Gratuitous）を検査して、それらが ARP オーナーからのものであることを確認するために使用します。ARP オーナーとは、ARP 応答に含まれている IP アドレスに一致する、DHCP バインディングが置かれているポートのことです。DAI 信頼済みポートからの ARP パケットは検査されず、それぞれの VLAN にブリッジされます。

DAI の使用

Dynamic ARP Inspection（DAI）では、ARP 応答または Gratuitous ARP メッセージを正当化するために、DHCP バインディングが存在している必要があります。ホストで、アドレスを取得するための DHCP が使用されていない場合、そのホストを信頼するか、ホストの IP アドレスと MAC アドレスを対応付けるために ARP 検査用のアクセス コントロール リスト（ACL）を作成する必要があります（図 16-11 を参照）。DHCP スヌーピングと同様、DAI は VLAN ごとに有効化されます。すべてのポートは、デフォルトで、信頼できないポートとして定義されます。DAI で DHCP スヌーピングからのバインディング情報を活用するには、DAI を有効化する前に、VLAN で DHCP スヌーピングを有効化する必要があります。DAI を有効化する前に DHCP スヌーピングを有効化しないと、VLAN 内のいずれのデバイスも、ARP を使用して、デフォルト ゲートウェイを含む VLAN 内の他のデバイスに接続できません。その結果、VLAN 内のすべてにデバイスに対するサービスを、自ら拒否することになります。

図 16-11　DHCP スヌーピングおよび DAI を使用した ARP 攻撃の防止



DAI のユーザにとって DHCP スヌーピング バインディング テーブルは重要なので、バインディング テーブルのバックアップを取ることは重要です。DHCP スヌーピング バインディング テーブルは、ブートフラッシュ、ファイル転送プロトコル（FTP）、リモート コピー プロトコル（RCP）、スロット 0、および Trivial File Transfer Protocol（TFTP）にバックアップできます。DHCP スヌーピング バインディング テーブルをバックアップしないと、スイッチのリブート中に、Cisco IP Phone でデフォルト ゲートウェイとのアクセスが失われる場合があります。例として、DHCP スヌーピング バインディング テーブルをバックアップせず、回線電源の代わりに電源アダプタを使用して Cisco IP Phone を使用している場合を想定します。この場合、リブートの後にスイッチがバックアップされると、電話機用の DHCP スヌーピング バインディング テーブル エントリが存在しないので、電話機はデフォルト ゲートウェイと通信できません。これを回避するには、DHCP スヌーピング バインディング テーブルのバックアップを取り、電話機からトラフィックが流れ始める前に古い情報をロードする必要があります。

利点

DAI を使用すると、攻撃者がネットワーク内で ARP ベースの攻撃を仕掛け、レイヤ 2 で攻撃者に隣接する人々の間のトラフィックを妨害または探知するのを防止できます。

欠点

この機能が正しく設定されていないと、認定ユーザへのネットワーク アクセスが拒否される場合があります。DHCP スヌーピング バインディング テーブルにデバイスのエントリがない場合、そのデバイスでは、ARP を使用してデフォルト ゲートウェイに接続できず、そのためトラフィックを送信できません。固定 IP アドレスを使用する場合、これらのアドレスを DHCP スヌーピング バインディング テーブルに手動で入力する必要があります。リンクがダウンのときに、DHCP を再度使用して IP アドレスを取得することをしないデバイスがある場合（一部の UNIX または Linux マシンはこのように動作します）、DHCP スヌーピング バインディング テーブルをバックアップする必要があります。

設定例

次の例は、DHCP スヌーピングおよび Dynamic ARP Inspection を使用してアクセス ポートを設定する Cisco IOS コマンドを示しています。

- グローバル コマンド

```
ip dhcp snooping vlan 10,20 (required)
no ip dhcp snooping information option (required without option 82 dhcp server)
ip dhcp snooping (required)
ip arp inspection vlan 10,20
ip dhcp snooping database tftp://172.26.168.10/tftpboot/cisco/ngcs-dhcpdb
```

- インターフェイス コマンド

```
ip dhcp snooping trust
ip arp inspection trust
no ip arp inspection trust (default)
ip arp inspection limit rate 15 (pps)
```

上記の例のグローバル コマンドは、次の機能を実行します。

- **ip arp inspection vlan 10,20**

  このコマンドは、Dynamic ARP Inspection（DAI）が有効になっている VLAN を特定します。

- **ip arp inspection trust**

  ip dhcp snooping trust と同様、このコマンドは、ルータなどの信頼済みデバイスが ARP メッセージに応答するのを許可します。このコマンドは、使用するルータ用のポートで設定する必要があります。そのように設定しないと、ルータは DHCP スヌーピング バインディング テーブルに含まれないので、ルータはいずれの ARP 要求にも応答できません。

- **no ip arp inspection trust**

  この設定は、VLAN 上のすべてのポートのデフォルト設定です。信頼を有効にする必要があります。

- **ip arp inspection limit rate 15 (pps)**

  このコマンドは、インターフェイス上の ARP メッセージで許可されている、1 秒当たりのパケット数の最大数のグローバル デフォルト値を設定します。この値を超えると、インターフェイスは有効になります。この動作が問題になる場合は、制限を増加または減少させるか、**none** に設定することができます。

- **ip dhcp snooping database tftp://172.26.168.10/tftpboot/cisco/ngcs-dhcpdb**

  このコマンドは、DHCP スヌーピング バインディング テーブルのバックアップを TFTP サーバに作成します。DHCP スヌーピング バインディング テーブルは、ブートフラッシュ、FTP、RCP、スロット 0、および TFTP にバックアップできます。

上記の例のインターフェイス コマンドは、次の機能を実行します。

- **no ip arp inspection trust**

  このコマンドは、ポート上で DAI を有効にし、DHCP スヌーピング バインディング テーブルを基にすべての ARP をチェックします。

- **ip arp inspection limit rate 15 (pps)**

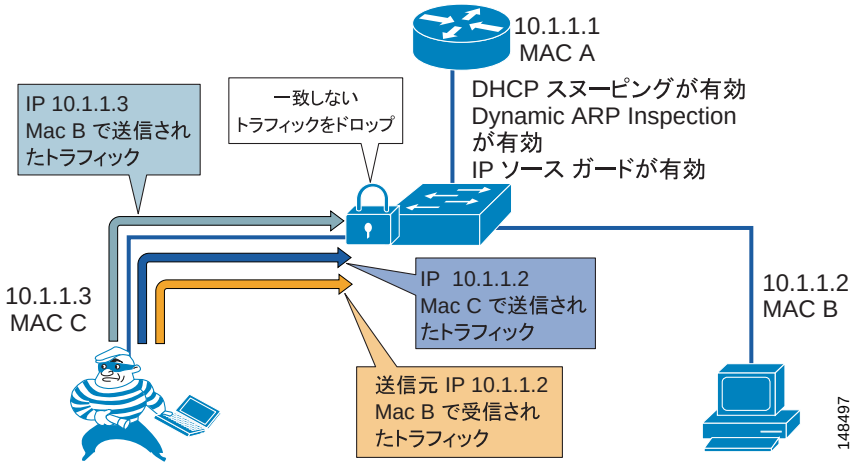
  このコマンドは、インターフェイス上の ARP メッセージで許可されている、1 秒当たりのパケット数の最大数を指定します。インターフェイスが、指定された数を超える ARP メッセージを 1 秒間に受信する場合、ポートは無効化されます。導入済みのセキュリティ ポリシーによっては、デフォルト値（15 pps）が最適な設定の場合があります。1 秒間に 15 個を超える ARP メッセージをポートが受信するときに電話機を無効化しない場合は、レート制限を **none** に設定できます。この設定では、電話機は有効なままです。

IP ソース ガード

ARP スプーフィングに加えて、攻撃者は IP アドレス スプーフィングも仕掛ける場合があります。この方法は、第二の当事者に対して DoS 攻撃を行うときに一般的に使用されます。この方法では第三の当事者を介してパケットが送信されるため、攻撃システムの ID がマスクされます。単純な例として、攻撃者は、攻撃先の第二の当事者の IP アドレスを送信元にしながら、サードパーティ システムに ping することがあります。ping の応答は、サードパーティ システムから第二の当事者に転送されます。スプーフィングされた IP アドレスを基にしたアグレッシブ SYN フラッディングは、サーバを TCP ハーフセッションで氾濫させる別の一般的なタイプの攻撃です。

IP ソース ガード（IPSG）機能を呼び出すと、DHCP スヌーピング バインディング テーブルの内容に基づいて ACL が動的に作成されます。この ACL は、トラフィックの送信元が DHCP バインディング時に発行された IP アドレスであることを保証し、スプーフィングされた他のアドレスによりトラフィックが転送されるのを防止します。DHCP スヌーピングは IP ソース ガードの前提条件ですが、DAI は前提条件ではありません。ただし、IP アドレス スプーフィングに加えて ARP ポイズニングおよび中間者攻撃を防止するため、IP ソース ガードだけでなく DAI も有効にすることをお勧めします（図 16-12 を参照）。

図 16-12　IP ソース ガードを使用したアドレス スプーフィングの防止



IP アドレス スプーフィングを使用すると、攻撃者は、アドレスを手動で変更するか、アドレス スプーフィングを行うように設計された hping2 などのプログラムを実行することにより、有効なアドレスになりすますことができます。インターネット ワームは、送信元を偽装するためスプーフィング技法を使用する場合があります。

設定例

次の例は、IP ソース ガードを使用してアクセス ポートを設定する Cisco IOS コマンドを示しています。

- IP ソース ガードを有効にする前に有効にする必要があるコマンド

```
ip dhcp snooping vlan 4,104
no ip dhcp snooping information option
ip dhcp snooping
```

- インターフェイス コマンド：このコマンドは、DHCP Option 82 を指定せずに IP ソース ガードを有効にします。

```
ip verify source vlan dhcp-snooping
```

追加情報

ネットワーク セキュリティに関する追加情報については、次の Web サイトで入手可能な Cisco マニュアルを参照してください。

- http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper0900aecd8015f0ae.shtml
- http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008014870f.shtml

QoS

QoS（Quality Of Service）は、企業ネットワーク用のすべてのセキュリティ ポリシーで、重要な部分を占めます。一般的に、QoS はネットワーク内のトラフィック重要度の設定と考えられていますが、ネットワークに入ることが許可されるデータの量も制御します。Cisco スイッチの場合、電話機からイーサネット スイッチにデータが送られるときのコントロール ポイントはポート レベルにあります。アクセス ポートでネットワークのエッジに適用される制御が多いほど、ネットワークでデータを集約するときに発生する問題は少なくなります。

ロビーに設置された電話機の例ですでに説明したとおり、アクセス ポート レベルでトラフィックの十分なフロー コントロールを提供することにより、攻撃者が、ロビー内のそのポートから DoS 攻撃を仕掛けるのを防止できます。QoS 設定ではポートに送信されたトラフィックが最大レートを超えることが許可されていますが、トラフィックは Scavenger Class レベルに定義されているので、この例の設定は、本来ほどアグレッシブではありません。よりアグレッシブな QoS ポリシーを使用すると、ポリシーの最大制限を超える量のトラフィックはポートでドロップされ、その「不明な」トラフィックがネットワークに入ることはありません。VoIP データにエンドツーエンドで高い優先度を与えるには、ネットワーク全体で QoS を有効にする必要があります。

QoS の詳細については、第 3 章「ネットワーク インフラストラクチャ」、および次の Web サイトで入手可能な『*Enterprise QoS Solution Reference Network Design（SRND）Guide*』を参照してください。

http://cisco.com/go/srnd

利点

QoS を使用すると、ネットワーク内のトラフィックの優先度だけでなく、任意の特定のインターフェイスを通過できるトラフィックの量も制御できます。ネットワーク内の音声 QoS をアクセス ポート レベルで配置するのに役立つ、Cisco Smartports テンプレートが作成されました。

欠点

QoS 設定が標準的な Cisco Smartports テンプレートの範囲外の場合、大規模な IP テレフォニー配置では、設定が複雑になり管理が難しくなることがあります。

VLAN アクセス コントロール リスト

VLAN アクセス コントロール リスト（ACL）を使用すると、ネットワーク上を流れるデータを制御できます。Cisco スイッチには、VLAN ACL 内でレイヤ 2 ～ 4 を制御する機能があります。ネットワーク内のスイッチのタイプによっては、VLAN ACL を使用して、特定の VLAN に流入または流出するトラフィックをブロックできます。また、VLAN ACL を使用して VLAN 内のトラフィックをブロックし、VLAN 内のデバイス間で発生する処理を制御することもできます。

VLAN ACL を配置する計画がある場合、VoIP ネットワーク内で使用される各アプリケーションで電話機が正しく動作するようにするにはどのポートが必要かを検証する必要があります。通常、任意の VLAN ACL は、電話機が使用する VLAN に適用されます。これにより、アクセス ポートでのコントロールを、アクセス ポートに接続されているデバイスに近づけることができます。

必要なポートを判別するには、次の製品マニュアルを参照してください。

- Cisco Catalyst 3750 スイッチ
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750/12225sed/scg/swacl.htm
- Cisco Catalyst 4500 シリーズ スイッチ
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/12_2_25s/conf/secure.htm
- Cisco Catalyst 6500 シリーズ スイッチ（Cisco IOS を実行）
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/acl.htm
- Cisco 6500 シリーズ スイッチ（Cisco CatOS を実行）
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_5/confg_gd/acc_list.htm

次の例は、Cisco 7960 IP Phone のトラフィックだけが VLAN でブートおよび機能するのを許可する、VLAN ACL を示しています（インライン コメントは、ACL の各行の目的を示しています）。この例の VLAN ACL は、Cisco CallManager Release 4.1 で使用するポート用です。この例では、次の IP アドレス範囲を使用します。

- 電話機の範囲は 10.0.20.*
- サーバの範囲は 10.0.10.*
- ゲートウェイの範囲は 10.0.30.*
- デフォルト ゲートウェイは 10.0.10.2 および 10.0.10.3
- DNS サーバの IP アドレスは 10.0.40.3

（注）　製品で使用されるポートの最新のリストを取得するには、ネットワーク上で実行している製品のバージョンに応じて適切なマニュアルを参照してください。アプリケーションがアップデートされたとき、または OS がアップデートされたとき（またはその両方）、ポートは変更されます。この注意事項は、電話機を含む、ネットワーク内のすべての VoIP デバイスに適用されます。

```
20 permit udp host 10.0.10.2 eq 1985 any
30 permit udp host 10.0.10.3 eq 1985 any
!permit HSRP from the routers
40 permit udp any any eq bootpc
50 permit udp any any eq bootps
!permit DHCP activity
60 permit udp 10.0.10.0 0.0.0.255 range 49152 65535 10.0.20.0 0.0.0.255 eq tftp
70 permit udp 10.0.20.0  0.0.0.255 range 1024 5000 10.0.10.0 0.0.0.255 range 49152 65535
80 permit udp 10.0.10.0 0.0.0.255 range 49152 65535 10.0.20.0  0.0.0.255 range 1024 5000
!permit the tftp traffic from the tftp server and phone
90 permit udp 10.0.10.0 0.0.0.255 range 49152 65535 host 10.0.40.3 eq domain
100 permit udp host 172.19.244.2 eq domain 10.0.10.0 0.0.0.255 range 49152 65535
!permit DNS to and from the phone
110 permit tcp 10.0.10.0 0.0.0.255 range 49152 65535 10.0.20.0  0.0.0.255 eq 2000
120 permit tcp 10.0.20.0  0.0.0.255 eq 2000 10.0.10.0 0.0.0.255 range 49152 65535
!permit signaling to and from the phone.
130 permit udp 10.0.10.0 0.0.0.255 range 16384 32767 10.0.10.0 0.0.0.255 range 16384 32767
140 permit udp 10.0.0.0 0.0.255.255 range 16384 32767 10.0.10.0 0.0.0.255 range 16384 32767
150 permit udp 10.0.10.0 0.0.0.255 range 16384 32767 10.0.0.0 0.0.255.255 range 16384 43767
!permit all phones to send udp to each other
160 permit tcp 10.0.10.0 0.0.0.255 range 49152 65535 10.0.20.0  0.0.0.255 eq www
170 permit tcp 10.0.20.0  0.0.0.255 eq www 10.0.10.0 0.0.0.255 range 49152 65535
180 permit tcp 10.0.20.0  0.0.0.255 range 49152 65535 10.0.10.0 0.0.0.255 eq www
190 permit tcp 10.0.10.0 0.0.0.255 eq www 10.0.20.0  0.0.0.255 range 49152 65535
!permit web access to and from the phone
200 permit ICMP any any
!allow all icmp - phone to phone, gateway to phone, and NMS to phone
220 permit udp 10.0.30.0 0.0.0.255 rang 16384 327676 10.0.10.0 0.0.0.255 rang 16384 32767
!permit udp to the gateways in the network for pstn access
```

この ACL の例が示しているとおり、ネットワーク内で IP アドレスが適切に定義されているほど、ACL を書き出して配置するのが簡単になります。

VLAN ACL を適用する方法の詳細については、次のマニュアルを参照してください。

- Cisco Catalyst 3750 スイッチ
  http://www.cisco.com/en/US/products/hw/switches/ps5023/products_configuration_guide_book09186a0080464bdc.html
- Cisco Catalyst 4500 シリーズ スイッチ
  http://www.cisco.com/en/US/products/hw/switches/ps4324/products_configuration_guide_book09186a008011c8a5.html
- Cisco Catalyst 6500 シリーズ スイッチ（Cisco CatOS 対応）
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_5/confg_gd/
- Cisco Catalyst 6500 シリーズ スイッチ（Cisco IOS 対応）
  http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_book09186a00801609ea.html

利点

ACL は、VLAN に入るまたは VLAN から出るネットワーク トラフィックを制御する機能、および VLAN 内でトラフィックを制御する機能を提供します。

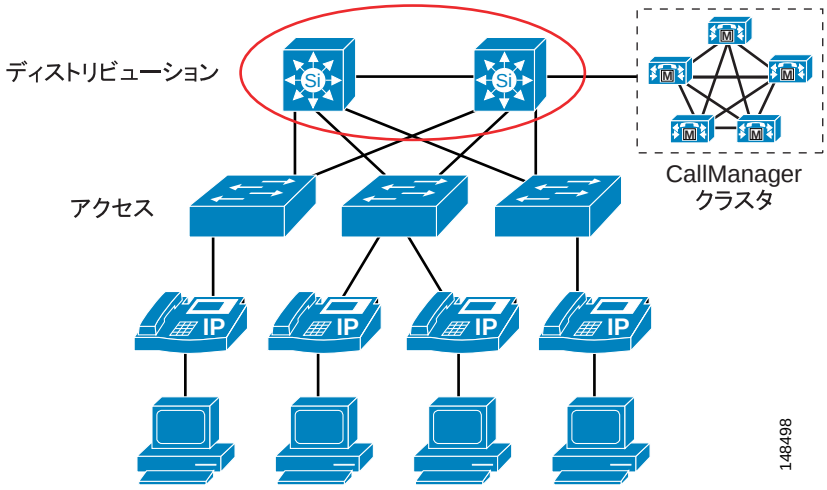
欠点

VLAN ACL を、モバイル性の高いアクセスポート レベルで配置および管理するのは非常に困難です。これらの管理上の問題があるので、ネットワークのアクセス ポートに VLAN ACL を配置するときは注意が必要です。

ルータのアクセス コントロール リスト

VLAN ACL と同様、ルータにも、ポートごとにインバウンド ACL およびアウトバウンド ACL の両方を処理する機能があります。最初のレイヤ 3 デバイスは、音声およびデータ VLAN を使用するときの音声データと別タイプのデータとの間の境界ポイントです。境界ポイントでは、2 つのタイプのデータが、相互にトラフィックを送信することが許可されます。VLAN ACL とは異なり、ルータ ACL は、ネットワーク内のすべてのアクセス デバイスには配置されません。その代わり、ネットワーク全体にルーティングするすべてのデータを準備する場所である、エッジ ルータで適用されます。これは、各 VLAN のデバイスがネットワーク内でアクセス可能なエリアを制御するために、レイヤ 3 ACL を適用するのに最適な場所です。レイヤ 3 ACL をネットワーク全体に配置することにより、トラフィックが収束する場所で、デバイスを相互に保護できます（図 16-13 を参照）。

図 16-13　レイヤ 3 のルータ ACL



レイヤ 3 に配置可能な ACL には、多くのタイプがあります。一般的なタイプの説明と例については、次の Web サイトで入手可能な『*Configuring Commonly Used IP ACLs*』を参照してください（シスコ パートナーとしてのログインが必要）。

http://cisco.com/en/US/partner/tech/tk648/tk361/technologies_configuration_example09186a0080100548.shtml

導入済みのセキュリティ ポリシーに応じて、レイヤ 3 ACL は、非 Voice VLAN からの IP トラフィックがネットワーク内の音声ゲートウェイにアクセスするのを禁止するという単純な設定にも、他のデバイスが VoIP デバイスと通信するために使用する個別のポートや時間を制御するという詳細な設定にもできます。ソフトフォンが導入されていないと仮定すると、Cisco CallManager 、音声ゲートウェイ、電話機、および音声専用サービスで使用される他の任意の音声アプリケーションに対する、すべてのトラフィック（IP アドレス別、または IP 範囲別）をブロックするための ACL を書き込むことができます。この方法により、レイヤ 3 ACL を、レイヤ 2 または VLAN ACL よりも簡素化できます。

この例では、次の IP アドレス範囲を使用します。

- 電話機の範囲は 10.0.20.*
- VoIP サーバの範囲は 10.0.10.*
- ゲートウェイの範囲は 10.0.30.*
- ネットワーク内の他のすべてのデバイスの範囲は 192.168.*.*

```
10 deny ip 192.168.0.0 0.0.255.255 10.0.10.0 0.0.0.255
!deny all non voice devices to the voip servers
20 deny 192.168.0.0 0.0.255.255 10.0.30.0 0.0.0.255
!deny all non voice devices to the voip gateways
30 deny 192.168.0.0 0.0.255.255 10.0.20.0 0.0.0.255
!deny all non voice devices to communicate with the phones ip addresses
```

利点

レイヤ 3 では、より簡単に ACL を管理および配置できます。レイヤ 3 は、ネットワーク内の音声データおよび他の非音声データにコントロールを適用できる最初の機会です。

欠点

ACL が高精度および詳細になると、ネットワーク内のポート使用法の変更が原因で、音声だけでなく、ネットワーク内の他のアプリケーションも遮断される場合があります。

ネットワークにソフトフォンがある場合、電話機への Web アクセスが許可されている場合、または Attendant Console を使用するか、Voice VLAN サブネットへのアクセスが必要な他のアプリケーションを使用する場合、ACL の配置と制御はさらに難しくなります。

インフラストラクチャの保護

VoIP データがネットワークを横断するときのデータの安全性とセキュリティは、データを転送するデバイスと同程度にしかすぎません。導入済みのセキュリティ ポリシーで定義されているセキュリティ レベルによっては、ネットワーク デバイスのセキュリティを向上させる必要がある場合もあれば、VoIP トラフィックを転送するのにすでに十分に安全な場合もあります。

ネットワーク全体のセキュリティを向上させるためにデータ ネットワークで実行できる、多くのベストプラクティスがあります。たとえば、攻撃者がパスワードをクリア テキスト形式で見ることができないように、Telnet（パスワードをクリア テキスト形式で送信します）を使用して任意のネットワーク デバイスに接続する代わりに、Secure Shell（SSH、Telnet の安全な形式）を使用できます。Cisco.com Web サイトでは、ネットワーク内のセキュリティ全般に関する多数のマニュアルを入手できます。導入済みのセキュリティ ポリシーと共にこれらのマニュアルを使用し、インフラストラクチャで必要なセキュリティを判別してください。

次のリンクは、Cisco.com で入手可能なセキュリティ関連マニュアルをリストしています。

- Best Practices for Cisco Switches（ログイン認証が必要）
  http://cisco.com/en/US/partner/products/hw/switches/ps663/products_tech_note09186a0080094713.shtml
- SAFE：A Security Blueprint for Enterprise Networks
  http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008009c8b6.shtml

セキュリティの概要

従来の PBX は、通常、安全な環境にロックされますが、IP ネットワークも同じように扱う必要があります。VoIP を伝送する各デバイスは VoIP PBX の一部です。通常の一般的なセキュリティ プラクティスを使用して、これらのデバイスへのアクセスを制御する必要があります。ユーザまたは攻撃者が、ネットワーク内のデバイスの 1 つに物理的にアクセスできる場合、あらゆる種類の問題が発生します。強力なパスワード セキュリティがあり、ユーザまたは攻撃者がネットワーク デバイスに侵入できない場合でも、それらのユーザや攻撃者がデバイスを切断してすべてのトラフィックを停止することにより、ネットワークの大破壊を引き起こす可能性はあります。

全般的なセキュリティ プラクティスの詳細については、次の Web サイトで入手可能なマニュアルを参照してください。

- http://www.cisco.com/go/safe/
- http://www.cisco.com/web/about/ac123/iqmagazine/archives/q2_2005/addressing_network_security.html

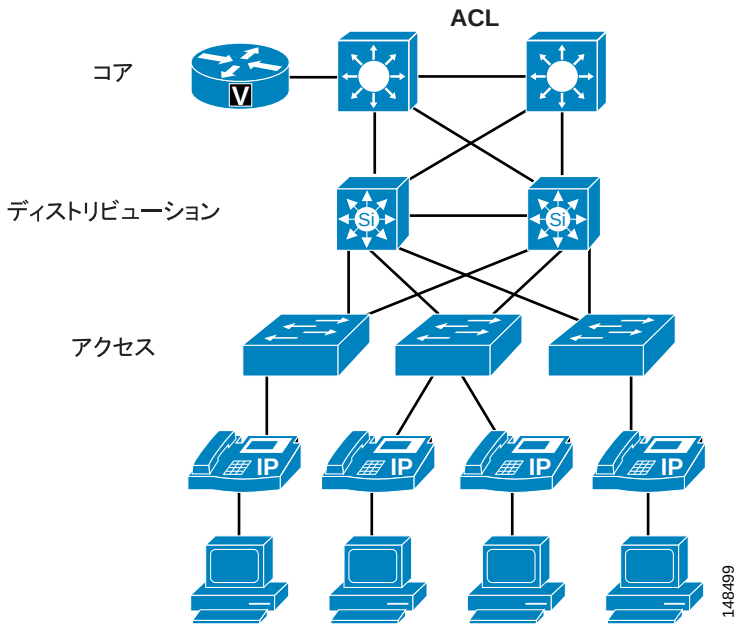
ゲートウェイおよびメディア リソース

ゲートウェイおよびメディア リソースは、VoIP コールを公衆網コールに変換するデバイスです。外部コールが配置された場合、ゲートウェイまたはメディア リソースは、VoIP ネットワークにおいてすべての音声 RTP ストリームが流れる数少ない場所の 1 つです。

VoIP ゲートウェイおよびメディア リソースは、ネットワーク内のほぼすべての場所に配置できるので、導入済みのセキュリティ ポリシーによっては、VoIP ゲートウェイまたはメディア リソースを保護することが、他のデバイスを保護することより難しいと見なされる場合があります。しかし、ネットワーク内のどこで信頼が確立されているかによりますが、ゲートウェイおよびメディア リソースを簡単に保護できる場合もあります。ゲートウェイおよびメディア リソースが Cisco CallManager により制御される方法が関係していますが、シグナリングがゲートウェイまたはメディア リソースに到達するために通るパスがネットワーク内で安全と見なされている部分にある場合、単純な ACL を使用して、ゲートウェイまたはメディア リソースに送る、またはそこから戻るシグナリングを制御することができます。ゲートウェイ（またはメディア リソース）と Cisco CallManager のロケーションの間のネットワークが安全と見なされない場合は（ゲートウェイがリモートの支店に置かれている場合など）、インフラストラクチャを使用してゲートウェイおよびメディア リソースへの IPSec トンネルを構築することにより、シグナリングを保護できます。ほとんどのネットワークでは、通常、2 つの方式（ACL および IPSec）の組み合せにより、これらのデバイスが保護されています。

ここでは、ネットワークのエッジで QoS を使用しているので、攻撃者が Voice VLAN に侵入してゲートウェイおよびメディア リソースの場所を判別できた場合、ポートの QoS により、攻撃者がゲートウェイまたはメディア リソースに送信できるデータの量が制限されます（図 16-14 を参照）。

図 16-14　IPSec、ACL、および QoS を使用したゲートウェイおよびメディア リソースの保護



電話機で SRTP が有効な場合、一部のゲートウェイおよびメディア リソースでは、ゲートウェイに対する Secure RTP（SRTP）および電話機からのメディア リソースがサポートされます。ゲートウェイまたはメディア リソースが SRTP をサポートしているかどうかを判別するには、次の Web サイトで入手可能な適切な製品マニュアルを参照してください。

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

IPSec トンネルの詳細については、次の Web サイトで入手可能な『*Site-to-Site IPSec VPN Solution Reference Network Design （SRND）*』を参照してください。

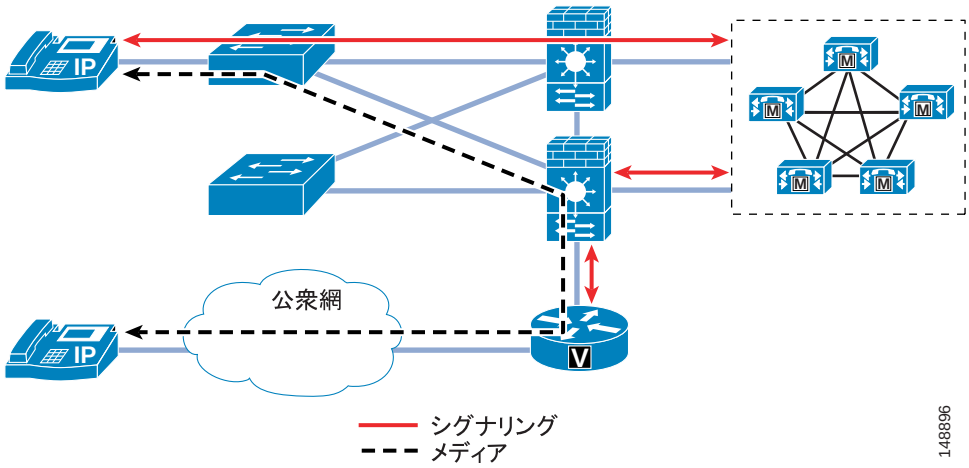
http://www.cisco.com/go/srnd

ゲートウェイの周囲へのファイアウォールの配置

コールの送信元である電話機と、公衆網ネットワークへのゲートウェイとの間にファイアウォールを配置する場合、注意が必要な問題が生じます。ステートフル ファイアウォールは、Cisco CallManager、ゲートウェイ、および電話機の間のシグナリング メッセージの内容を参照し、コールの実行を許可するための RTP ストリーム用のピンホールを開けます。通常の ACL で同じことを行うには、RTP ストリームで使用されるポート範囲全体を、ゲートウェイに対して開放する必要があります。

ネットワーク内にゲートウェイを配置する方法は 2 つあります。つまり、ファイアウォールの背後に配置する方法と、ファイアウォールの前面に配置する方法です。ゲートウェイをファイアウォールの背後に配置する場合、そのゲートウェイを使用している電話機からのすべてのメディアは、ファイアウォールを通過する必要があります。また、これらのストリームがファイアウォールを通過するようにするには、追加の CPU リソースが必要です。次に、ファイアウォールでは、これらのストリームの制御が追加され、ゲートウェイが DoS 攻撃から保護されます（図 16-15 を参照）。

図 16-15　ファイアウォールの背後に配置されたゲートウェイ



ゲートウェイを配置する 2 番目の方法は、ファイアウォールの外側に配置する方法です。電話機からゲートウェイに送信される唯一のデータ タイプは RTP ストリームなので、そのゲートウェイに送信可能な RTP トラフィックの量は、アクセス スイッチの QoS 機能により制御されます。Cisco CallManager からゲートウェイに送信されるのは、コールをセットアップするためのシグナリングだけです。ネットワーク内で、信頼できるエリアにゲートウェイが配置されている場合、Cisco CallManager とゲートウェイの間で許可する必要がある唯一の通信は、そのシグナリングです（図 16-15 を参照）。RTP ストリームはファイアウォールを通過しないので、この配置方式では、ファイアウォールの負荷が低下します。

利点

ACL とは異なり、ほとんどのファイアウォール設定では、シグナリングがファイアウォールを経由しているかぎり、Cisco CallManager が電話機とゲートウェイに対して、それらの 2 つのデバイスの間で使用するように指示している RTP ストリーム ポートだけが開放されます。また、ファイアウォールには、DoS 攻撃用の追加機能や、対象トラフィックを参照して、攻撃者が禁止動作を行っていないかどうかを判別するための Cisco Intrusion Detection System（IDS）シグニチャがあります。

欠点

P.16-33 の「ファイアウォール」の項で説明したとおり、ファイアウォールが、すべてのシグナリング、および電話機からゲートウェイへの RTP ストリームを参照する場合、キャパシティが問題になることがあります。また、音声データ以外のデータがファイアウォールを通過する場合、ファイアウォールを通過するコールがファイアウォールにより影響されないように、CPU 使用率を監視する必要があります。

アクティブまたはスタンバイ モードでは、Cisco Adaptive Security Appliance（ASA）および Cisco Private Internet Exchange（PIX）のフェールオーバー時間の最小設定は 3 秒です。Cisco Firewall Services Modules（FWSM）の最小タイマー設定も、3 秒です。引き継ぐ必要があるとスタンバイ ユニットが判別した場合、ファイアウォールでは、すぐにフェールオーバーが発生します。ステートフル フェールオーバーが設定されている場合、プライマリ ファイアウォールを通過するデータの状態は、フェールオーバー ユニットに渡されます。このようにして、フェールオーバーの前に実行されていたすべてのことが保持されます。しかし、プライマリ ユニットまたはそのユニットに対する接続性に全面的な障害が発生した場合、ゲートウェイにトラフィックが渡されない時間が、ASA または PIX の場合は 3 秒以上、FWSM の場合は 3 秒間発生します。つまり、ファイアウォールでのフェールオーバーを強要する、ある種類の障害が発生した場合、RTP ストリームは最低 3 秒間停止します。

ファイアウォール

ファイアウォールを ACL と組み合せて使用すると、VoIP デバイスと通信することが許可されていないデバイスから、音声サーバおよび音声ゲートウェイを保護できます。VoIP で使用するポートには動的な特性があるので、ファイアウォールを配置すると、VoIP 通信で必要な広範囲のポートの開放を制御するのに役立ちます。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。

VoIP ネットワークには、固有のデータ フローがあります。電話機はクライアント / サーバ モデルを使用してコール セットアップ用のシグナリングを生成し、Cisco CallManager はそのシグナリングを使用して電話機を制御します。VoIP RTP ストリームのデータ フローは、ピアツーピア ネットワークに似ており、電話機またはゲートウェイは、RTP ストリームを介して相互に直接通信します。ファイアウォールがシグナリング トラフィックを検査できるようシグナリング フローがファイアウォールを経由しないようにする場合、ファイアウォールが、会話用の RTP ストリームを許可するのにどのポートを開放する必要があるかを判別できないので、RTP ストリームがブロックされることがあります。

正しく設計されたネットワークにファイアウォールを配置すると、すべてのデータがそのデバイスを経由するように強制できるので、キャパシティとパフォーマンスについて考慮する必要があります。パフォーマンスには、遅延の量が関係しています。ファイアウォールに高い負荷がかかっている場合やファイアウォールが攻撃されている場合は、1 つのファイアウォールにより遅延の量が増大することがあります。VoIP の配置に関する原則では、FWSM、ASA、または PIX の通常使用時の CPU 使用率を 60% 未満に抑えます。CPU の使用率が 60% を超えると、VoIP 電話機、コール セットアップ、および登録に影響が出る可能性が高まります。CPU の使用率が継続的に 60% を超えると、登録済みの VoIP 電話機は影響を受け、進行中のコールの品質は低下し、新しいコールのコール セットアップは問題を抱えます。CPU 使用率が 60% を超えた状態が続くと、最悪の場合、電話機の登録解除が始まります。このことが発生すると、電話機は Cisco CallManager への再登録を試みるようになり、ファイアウォールの負荷はさらに増大します。この状態が発生すると、結果的に、登録解除と Cisco CallManager への再登録の試行を繰り返す電話機の連続ブラックアウトが発生します。ファイアウォールの CPU 使用率が継続的に 60% 未満に落ち着くまで、この連続ブラックアウトは続き、すべてまたはほとんどの電話機が影響を受けます。現在、ネットワーク内で Cisco ファイアウォールを使用している場合、ネットワークに VoIP トラフィックを追加するときは、トラフィックが悪影響を受けないように、CPU 使用率を注意深く監視してください。

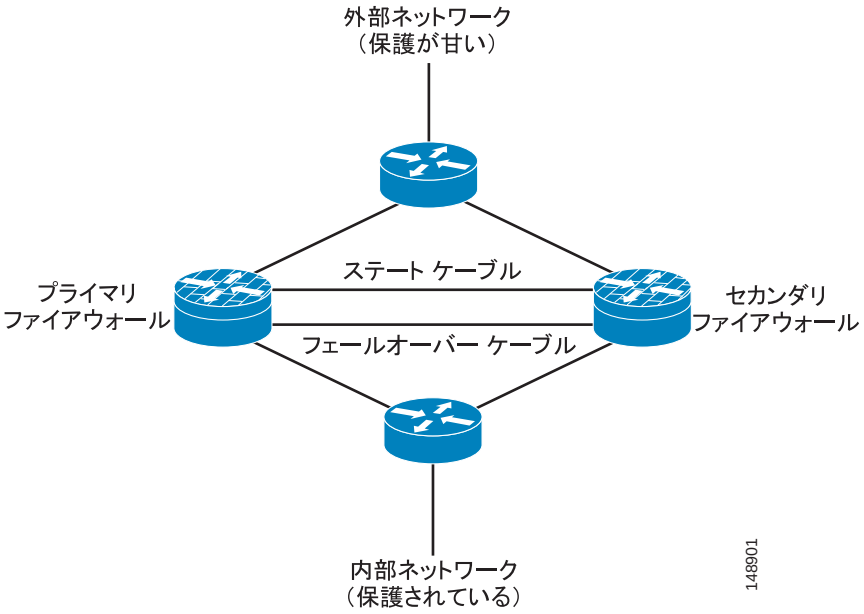
ファイアウォールを配置する方法はいくつもあります。この項では、ルーテッドおよび透過の両方のシナリオにおける、アクティブ / スタンバイ モードの ASA、PIX、および FWSM について集中的に説明します。この項で説明する各設定は、ファイアウォール設定の音声セクション内で、シングル コンテキスト モードで設定されたものです。

すべての Cisco ファイアウォールは、マルチ コンテキスト モードまたはシングル コンテキスト モードのいずれかで実行できます。シングル コンテキスト モードでは、ファイアウォールは、ファイアウォールを通過するすべてのトラフィックを制御する単一のファイアウォールを指します。マルチ コンテキスト モードでは、ファイアウォールは複数の仮想ファイアウォールを指します。これらのコンテキストまたは仮想ファイアウォールにはそれぞれ独自の設定があり、異なるグループまたは管理者が制御できます。ファイアウォールに新しいコンテキストを追加するたびに、ファイアウォールの負荷およびメモリ要件は大きくなります。新しいコンテキストを配置するときは、音声 RTP ストリームが悪影響を受けないように、CPU 要件を満たしていることを確認してください。

ASA または PIX と FWSM の機能性の相違点

図 16-16 は、ネットワーク内の冗長ファイアウォールを論理的に表現しています。配置方法は、ルーテッド設定と透過設定で同じです。

図 16-16　冗長ルーテッドまたは透過ファイアウォール



Cisco Adaptive Security Appliance（ASA）および Cisco Private Internet Exchange（PIX）は、Cisco Firewall Cisco Firewall Services Modules（FWSM）とは異なる方法で動作します。ASA または PIX 内では、より信頼性が高いインターフェイスに ACL がないかぎり、そのインターフェイスからのすべてのトラフィックは信頼され、そこから出て、より信頼性が低いインターフェイスに到達することが許可されます（図 16-17 を参照）。たとえば、ASA の内部インターフェイスまたはデータ センター インターフェイスからのすべてのトラフィックは、ASA から出て、ASA の外部インターフェイスに到達することが許可されます。ASA/PIX 上のより信頼性の高いインターフェイスに任意の ACL を適用すると、他のすべてのトラフィックは拒否（DENY）され、ファイアウォールは FWSM と同様に機能するようになります（図 16-18 を参照）。

図 16-17　Cisco ASA または PIX の機能

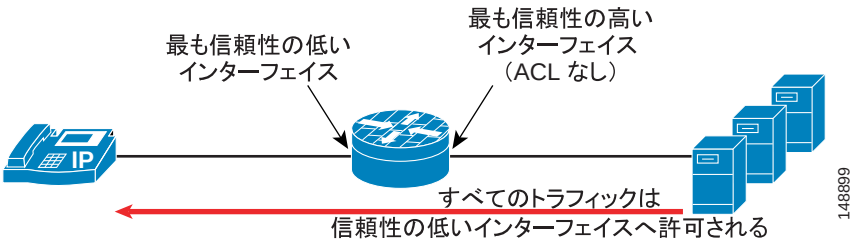
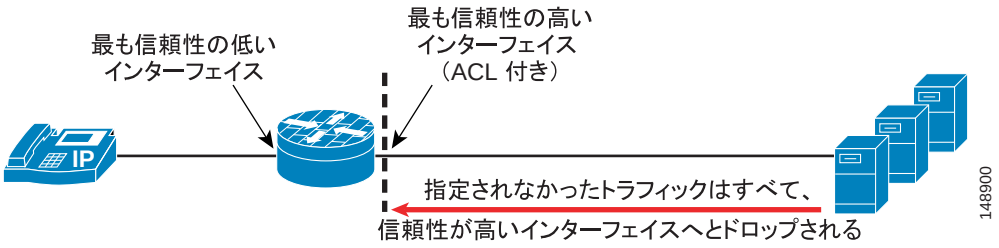


図 16-18　Cisco FWSM の機能



ファイアウォールの全般的な利点

ファイアウォールは、ネットワーク上で実行されるアプリケーションのために、ネットワークのセキュリティ コントロール ポイントを提供します。トラフィックがファイアウォールを通過する場合、ファイアウォールは、VoIP 会話用にポートを動的に開く機能も提供します。

Application Layer Gateway（ALG）機能を使用すると、ファイアウォールを通過するトラフィックがファイアウォールで検査され、そのトラフィックが、ファイアウォールで予期されていたタイプのトラフィックかどうかが判別されます。たとえば、HTTP トラフィックが本当に HTTP トラフィックなのか、あるいは攻撃なのかが判別されます。それが攻撃だった場合はそのパケットをドロップし、そのパケットがファイアウォールの背後にある HTTP サーバに到達するのを許可しません。

ファイアウォールの全般的な欠点

ファイアウォールでは、すべての VoIP アプリケーション サーバまたはアプリケーションがサポートされているわけではありません。ファイアウォール、またはファイアウォール内の ALG でサポートされていない一部のアプリケーションには、Cisco Unity ボイスメール サーバ、Attendant Console、IPCC Enterprise、および IPCC Express が含まれます。トラフィックがファイアウォールを経由して流れるのを許可するため、これらのアプリケーション用の ACL を書き込むことができます。

バージョン 3.0 より前の Cisco FWSM では、SCCP フラグメンテーションがサポートされていません。電話機、Cisco CallManager、またはゲートウェイから別の VoIP デバイスに送信される SCCP パケットが断片化されている場合、断片化されたパケットが FWSM を通過するのは許可されません。断片化が、バージョン 2.*x* のコードを実行する FWSM で発生した場合、シグナリング トラフィック用のファイアウォールの ALG 機能を使用せずに、ACL を使用する必要があります。この設定では、FWSM を通過するシグナリング トラフィックが許可されますが、シグナリングがファイアウォールを通過するときにパケットの検査は実行されません。

ネットワーク上で実行しているアプリケーションがネットワーク内のファイアウォールのバージョンでサポートされているかどうか、および ACL を書き出す必要があるかどうかを判別するには、次の Web サイトで入手可能な適切なアプリケーション マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/ipcvoice.htm

ルーテッド ASA および PIX

ルーテッド モードの ASA または PIX ファイアウォールは、接続されているネットワーク間のルータとして機能します。各インターフェイスには、異なるサブセット上の 1 つの IP アドレスが必要です。シングル コンテキスト モードでは、ルーテッド ファイアウォールは Open Shortest Path First（OSPF）およびパッシブ モードの Routing Information Protocol（RIP）をサポートしています。マルチ コンテキスト モードは、静的ルートのみをサポートしています。拡張するルーティング要件に対するセキュリティ アプライアンスに依存するのではなく、アップストリーム ルータおよびダウンストリーム ルータの拡張ルーティング機能を使用することをお勧めします。ルーテッド モードの詳細については、次の Web サイトで入手可能な『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/multisec/asa_sw/v_70/config/index.htm

利点

ルーテッド ASA または PIX ファイアウォールは、QoS、NAT、およびボックスへの VPN 終端をサポートしています。これらの機能は、トランスペアレント モードではサポートされていません（P.16-36 の「トランスペアレント ASA および PIX」を参照）。

図 16-16 は、アクティブ スタンバイ モードのルーテッド設定と透過設定の両方における、ファイアウォールの論理配置を示しています。ルーテッド設定では、ASA または PIX 上の各インターフェイスに IP アドレスが与えられます。トランスペアレント モードでは、ASA または PIX をリモートで管理するための IP アドレスの他には、インターフェイス上に IP アドレスは与えられません。

欠点

トランスペアレント モードとは異なり、デバイスはネットワークで参照することができ、それが原因で攻撃ポイントになる場合があります。ルーティングの一部はファイアウォールで実行可能なため、ルーテッド ASA または PIX ファイアウォールをネットワークに配置すると、ネットワークのルーティングが変更されます。ファイアウォールに存在する、使用する予定のすべてのインターフェイスでは、IP アドレスも使用可能でなければなりません。そのため、ネットワーク内のルータの IP アドレスを変更する必要が生じる場合もあります。ASA または PIX ファイアウォールを経由してルーティング プロトコルまたは RSVP を許可する場合、トラフィックが外側（または信頼性の低い）インターフェイスを通過するのを許可するため、ACL を内側（または最も信頼性の高い）インターフェイス上に配置する必要があります。ACL では、最も信頼性が高いインターフェイスから出るのを許可される、その他のすべてのトラフィックも定義する必要があります。

トランスペアレント ASA および PIX

ASA または PIX ファイアウォールは、レイヤ 2 ファイアウォール（「Bump In The Wire」または「ステルス ファイアウォール」とも呼ばれる）として設定できます。この設定では、ファイアウォールに IP アドレス（管理目的のものを除く）は与えられず、すべてのトランザクションはネットワークのレイヤ 2 で行われます。ファイアウォールはブリッジとして動作しますが、レイヤ 3 のトラフィックは、拡張アクセス リストで明示的に許可しないかぎり、セキュリティ アプライアンスを通過できません。アクセス リストなしで許可されるトラフィックは、Address Resolution Protocol（ARP）トラフィックだけです。

利点

この設定には、ファイアウォールが動的ルーティングを一切行わないため、攻撃者がファイアウォールを見つけることができないという利点があります。ファイアウォールがトランスペアレント モードでも動作するようにするには、静的ルーティングが必要です。

この設定では、ファイアウォールに合せてルーティングを変更する必要がないので、より簡単に既存のネットワークにファイアウォールを配置できます。またこの設定は、ファイアウォール内でいずれのルーティングも行わないため、ファイアウォールの管理やデバッグも簡単に実行できます。ファイアウォールはルーティング要求を処理しないので、通常は、**inspect** コマンドと全体のトラフィックを使用したときのファイアウォールのパフォーマンスの方が、同じファイアウォール モデルとソフトウェアがルーティングを実行する場合よりも高くなります。

欠点

トランスペアレント モードでは、ファイアウォールで NAT を使用することはできません。ルーティングのためにデータを渡す場合、同じファイアウォールをルーテッド モードで使用する場合とは異なり、トラフィックを許可するためにファイアウォールの内側と外側の両方で ACL を定義する必要があります。Cisco Discovery Protocol（CDP）トラフィックは、デバイスが定義済みの場合でも、デバイスを通過することはありません。直接接続される各ネットワークは、同じサブネット上に置かれている必要があります。コンテキスト間でインターフェイスを共有することはできません。マルチ コンテキスト モードを実行する計画の場合は、追加のインターフェイスを使用する必要があります。そのトラフィックがファイアウォールを通過するのを許可するには、ACL で、ルーティング プロトコルなどのすべての非 IP トラフィックを定義する必要があります。トランスペアレント モードでは QoS はサポートされていません。マルチキャスト トラフィックは、拡張 ACL が設定されているファイアウォールを通過するのを許可されますが、これはマルチキャスト デバイスではありません。トランスペアレント モードでは、VPN 終端はファイアウォールでサポートされていません。ただし、管理インターフェイス用の終端を除きます。

ASA または PIX ファイアウォールを経由してルーティング プロトコルまたは RSVP を許可する場合、トラフィックが外側（または信頼性が低い）インターフェイスを通過するのを許可するため、ACL を内側（または最も信頼性が高い）インターフェイス上に配置する必要があります。ACL では、最も信頼性が高いインターフェイスから出るのを許可される、その他のすべてのトラフィックも定義する必要があります。

トランスペアレント モードの詳細については、次の Web サイトで入手可能な『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/multisec/asa_sw/v_70/config/index.htm

ASA および PIX の設定例

次の設定例は、ファイアウォールが ASA および PIX ソフトウェア Release 7.04 の音声に対して動作するように設定するための、ポートおよび **inspect** コマンドをリストしています。これはあくまでも例にすぎません。任意のファイアウォールを配置する前に、ネットワーク内で使用されているすべてのアプリケーションから取得したポート リストを確認する必要があります。この設定例は、音声セクションのみを示しています。

```
!
!
object-group service remote-access tcp
 description remote access
 !Windows terminal
 port-object range 3389 3389
 !VNC
 port-object range 5800 5800
 !VNC
 port-object range 5900 5900
 port-object range 8080 8080
 port-object eq ssh
 !SSH
 port-object eq ftp-data
 !FTP data transport
  port-object eq www
 !HTTP Access
 port-object eq ftp
 !FTP
 port-object eq https
 !HTTPS Access
object-group service voice-protocols-tcp tcp
 description TCP voice protocols
 CTI/QBE
 port-object range 2428 2428
 !SIP communication
 port-object eq ctiqbe
 !SCCP
 port-object range 2000 2000
 !Secure SCCP
 port-object range 2443 2443
object-group service voice-protocols-udp udp
 !TFTP
 port-object eq tftp
 !MGCP Signaling
 port-object range 2427 2427
 !DNS
 port-object eq domain
 !RAS
 port-object range 1719 1719
 !SIP

!Object Group applied for remote-access
access-list OUTSIDE extended permit tcp any any object-group remote-access
!Object Group applied for voice-protocols-tcp
access-list OUTSIDE extended permit tcp any any object-group voice-protocols-tcp
!Object Group applied for voice-protocols-udp
access-list OUTSIDE extended permit udp any any object-group voice-protocols-udp
! Object Group applied for remote-access
access-list inside_access_in extended permit tcp any any object-group remote-access
! Object Group applied for voice-protocols-tcp
access-list inside_access_in extended permit tcp any any object-group
voice-protocols-tcp
! Object Group applied for voice-protocols-udp
access-list inside_access_in extended permit udp any any object-group
voice-protocols-udp

!Failover config
ip address 172.19.245.3 255.255.255.248 standby 172.19.245.4
failover
```

```
failover lan unit primary
failover lan interface failover GigabitEthernet0/3
failover polltime unit 1 holdtime 3
!Lowest and fastest setting for failover
failover polltime interface 3
failover link failover_state GigabitEthernet0/2
failover interface ip failover 192.168.1.1 255.255.255.0 standby 192.168.1.2
failover interface ip failover_state 192.168.0.1 255.255.255.0 standby 192.168.0.2

!
!Default inspection with inspects enabled
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect h323 h225
  inspect h323 ras
  inspect skinny
  inspect sip
  inspect tftp
  inspect mgcp
```

FWSM ルーテッド モード

ルーテッド モードでは、FWSM がネットワークのルータ ホップと見なされます。このモードでは、接続されているネットワークの間で NAT が実行されます。また、OSPF またはパッシブ RIP（シングル コンテキスト モード）を使用できます。ルーテッド モードでは、コンテキストあたり最大 256 個のインターフェイスがサポートされています。シングル モードでは、すべてのコンテキストに分割された最大 1,000 個のインターフェイスがサポートされています。

利点

ネットワーク内のルーテッド デバイスとして、FWSM は、ルーティング機能、およびトランスペアレント モードで使用可能でない他のすべての機能をサポートしています。

欠点

トランスペアレント モードとは異なり、ルーテッド デバイスはネットワーク上で参照することができ、それが原因で攻撃ポイントになる場合があります。ネットワークにデバイスを配置するには、IP アドレッシングとルーティングの設定を変更する必要があります。

FWSM トランスペアレント モード

トランスペアレント モードでは、FWSM は「Bump In The Wire」または「ステルス ファイアウォール」として動作し、ルータ ホップではありません。FWSM はインターフェイスの内側と外側で同じネットワークに接続しますが、各インターフェイスは異なる VLAN に置かれている必要があります。ダイナミック ルーティング プロトコルまたは NAT は必要ありません。ただし、ルーテッド モードと同様、トランスペアレント モードでも、トラフィックの通過を許可する ACL が必要です。トランスペアレント モードでは、オプションで EtherType ACL を使用して、非 IP トラフィックを許可することもできます。トランスペアレント モードでは、内側インターフェイスと外側インターフェイスの 2 つのインターフェイスのみがサポートされています。

透過ファイアウォールを使用すると、ネットワーク設定を簡素化できます。トランスペアレント モードは、ファイアウォールを攻撃者から見えないようにするためにも便利です。ルーテッド モードではブロックされるトラフィックのために、透過ファイアウォールを使用することもできます。たとえば、透過ファイアウォールで、EtherType ACL を使用したマルチキャスト ストリームを許可できます。

利点

この設定には、ファイアウォールがルーティングを一切行わないため、攻撃者がファイアウォールを見つけることができないという利点があります。この設定では、ファイアウォールに合せてルーティングを変更する必要がないので、より簡単に既存のネットワークにファイアウォールを配置できます。またこの設定は、ファイアウォール内でいずれのルーティングも行わないため、ファイアウォールの管理やデバッグも簡単に実行できます。また、非 IP トラフィックと IP マルチキャスト トラフィック、静的 ARP インスペクション、および MAC 移動検出と静的 MAC をブリッジできます。

欠点

トランスペアレント モードでフェールオーバーを使用するときにループを回避するには、Bridge Port Data Unit（BPDU）転送をサポートしているスイッチ ソフトウェアを使用し、BPDU を許可するように FWSM を設定する必要があります。トランスペアレント モードでは、NAT、ダイナミック ルーティング、またはユニキャストのリバース パス フォワーディング（RPF）チェックはサポートされていません。トランスペアレント モードの FWSM に NAT 0 はありません。

FWSM の設定例

次の設定例では、ファイアウォールを FWSM ソフトウェア ReleaseRelease 2.3.*x* の音声に対応させるために使用する、ポートと **inspect** コマンドをリストします。これは例にすぎないので、ファイアウォールを配置する前に、使用中のネットワークで使用されているすべてのアプリケーションからポートのリストを取得して確認する必要があります。この設定例は、音声セクションのみを示しています。

```
fixup protocol h323 H225 1720
!Enable fixup  h3232 h225

fixup protocol h323 ras 1718-1719
!Enable fixup h323 RAS

fixup protocol mgcp 2427
!Enable fixup  mgcp

fixup protocol skinny 2000
!Enable fixup

fixup protocol tftp 69
!Enable fixup

object-group service VoiceProtocols tcp
  description CCM Voice protocols
  port-object eq ctiqbe
  port-object eq 2000
  port-object eq 3224
  port-object eq 2443
  port-object eq 2428
  port-object eq h323
!Defining the ports for TCP voice

object-group service VoiceProtocolsUDP udp
  description UDP based Voice Protocols
  port-object range 2427 2427
  port-object range 1719 1719
  port-object eq tftp
!Defining the ports for UDP voice

object-group service RemoteAccess tcp
  description Remote Acces
  port-object range 3389 3389
  port-object range 5800 5809
  port-object eq ssh
  port-object range 5900 5900
  port-object eq www
  port-object eq https
!Defining remote access TCP ports

access-list inside_nat0_outbound extended permit ip any any
!

access-list phones_access_in extended permit tcp any any object-group RemoteAccess log
notifications interval 2
access-list phones_access_in extended permit tcp any any object-group VoiceProtocols
log notifications interval 2
access-list phones_access_in extended permit udp any any object-group
VoiceProtocolsUDP log notifications interval 2
access-list phones_access_in extended deny ip any any log notifications interval 2
access-list outside_access_in extended permit tcp any any object-group VoiceProtocols
log notifications interval 2
access-list outside_access_in extended permit tcp any any object-group RemoteAccess
log notifications interval 2
access-list outside_access_in extended permit udp any any object-group
VoiceProtocolsUDP log notifications interval 2
!Access lists applying the object groups defined above for inside and outside
```

```
interfaces

access-list outside_access_in extended deny ip any any log notifications interval 2
access-list inside_access_in extended deny ip any any
!Deny all other traffic

access-list phones_nat0_outbound extended permit ip any any
!

failover
failover lan unit primary
failover lan interface flan vlan 4050
failover polltime unit 1 holdtime 5
failover polltime interface 15
!Failover config - 15 seconds
failover interface-policy 50%
failover link flin vlan 4051
failover interface ip flan 1.1.1.1 255.255.255.252 standby 1.1.1.2
failover interface ip flin 1.1.1.5 255.255.255.252 standby 1.1.1.6
nat (inside) 0 access-list inside_nat0_outbound_V1
access-group outside_access_in in interface outside
access-group inside_access_in in interface inside
```

データ センター

データ センター内では、セキュリティ ポリシーを使用して、VoIP アプリケーション サーバで必要なセキュリティを定義する必要があります。Cisco VoIP サーバは IP に基づいているので、データ センター内で、他にある時間に敏感なデータに適用するセキュリティを、これらのサーバに適用することができます。

データ センターの間で WAN でのクラスタ化が使用されている場合、データ センター内とデータ センター間の両方に適用されている追加のセキュリティは、クラスタ内のノード間で許可されている最大往復時間に収まる必要があります。ネットワーク内のアプリケーション サーバ用に導入されているセキュリティ ポリシーに、Cisco VoIP サーバが含まれている場合、そのセキュリティを使用する必要があります。また、すでに配置されている任意のインフラストラクチャ セキュリティを使用することもできます。

データ アプリケーション用に適切なデータ センター セキュリティを設計するには、次の Web サイトで入手可能な『*Data Center Networking:Server Farm Security SRND*』（『*Server Farm Security in the Business Ready Data Center Architecture*』）のガイドラインに従うことをお勧めします。

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

アプリケーション サーバ

Cisco CallManager セキュリティ機能のリスト、および有効にする方法については、次の Web サイトで入手可能な『*Cisco CallManager Security Guide*』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/english/ipp7960/sec_vir/sec413/index.htm

任意の Cisco CallManager セキュリティ機能を有効にする前に、それらの機能が、ネットワーク内のこれらのタイプのデバイスに関する企業セキュリティ ポリシーで指定されている、セキュリティ要件を満たしていることを確認してください。

Cisco CallManager およびアプリケーション サーバ上の Cisco Security Agent

Cisco Security Agent は、VoIP および VoIP サービスを提供するのにシスコが使用する、ほとんどのアプリケーション サーバで使用されています。Cisco Security Agent ソフトウェアは、サーバとの間のトラフィックの動作と、サーバ上でアプリケーションが実行される方法を調べて、すべてが正常かどうかを判別する、ホスト侵入防御ソフトウェアです。異常と見なされるものが見つかった場合、Cisco Security Agent ソフトウェアはそのアクティビティが発生するのを阻止します。たとえば、Cisco CallManager にソフトウェア パッケージをインストールすることを試みるウイルスがあり、そのような事態が以前発生したことがない場合でも、ウイルスがインストールを実行することは阻止されます。ただし、Cisco Security Agent は感染を防止するだけで、一度感染したサーバをクリーンにすることはできないので、サーバにはアンチウイルス ソフトウェアが引き続き必要です。

Cisco CallManager サーバでの Cisco Security Agent の実行に関する追加情報は、次の Web サイトで入手可能です。

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

マネージドではない Cisco Security Agent

シスコは、自社サーバ用のデフォルト Cisco Security Agent ポリシーを開発しました。このポリシーにより、VoIP サーバで必要なすべての機能は正しく機能し、同時に、既知および不明な攻撃が VoIP サーバに影響することは防止されます。最低でも、このマネージドではないバージョンの Cisco Security Agent をインストールおよび実行する必要があります。このソフトウェアは、アプリケーションとオペレーティング システムを、ウイルスやワーム攻撃から保護します。これらのタイプの侵入からの最大限の保護を得るには、常に最新バージョンの Cisco Security Agent ソフトウェアがサーバにインストールされていることを確認してください。マネージドではないエージェントがサーバにインストールされていると、攻撃のログは、エージェントがインストールされているシステムでのみ参照できます。特定のタイプのアラームが発生したので書き込まれた可能性があるログファイルをチェックするには、各システムにログインする必要があります。

利点

マネージドではない Cisco Security Agent は、既知および不明の攻撃、ワーム、およびウイルスから各システムを保護します。

欠点

Cisco Security Agent を管理対象外モードで実行すると、アラームは相関されません。システムのログ ファイルを参照するには、各システムに個別にアクセスする必要があります。マネージドではない Cisco Security Agent をアップグレードする場合、新しいクライアントをインストールした後、通常は、クライアント設定を有効にするためシステムをリブートする必要があります。何らかの理由によりシステムが感染した場合、Cisco Security Agent は、そのシステムをクリーンにすることはできません。セキュリティを保持し、システムを保護するには、システムでアンチウイルス ソフトウェアも実行する必要があります。

マネージド Cisco Security Agent

マネージド Cisco Security Agent は、管理対象外バージョンと同じように動作しますが、管理コンソールに、追加の利点がいくつかあります。管理対象システムを実行すると、すべてのシステムからのすべてのアラームを 1 つのコンソールで受信できます。また、この機能では、異常な状態が重大なレベルに達したときに、そのことを電子メールまたはポケットベルで通知するように設定できます。

利点

マネージド Cisco Security Agent では、マネージドではないシステムと同じ保護が提供されるだけでなく、エージェントの制御も行うことができます。この制御により、アップデート時にシステムに負荷をかけることなく、イベントの相関、管理コンソールへのグローバル レポートの返信、エージェントの Cisco Security Agent 設定のアップグレードを実行できます。

欠点

別個のサーバに、管理対象エージェントのグローバル モニタリングと設定用の別々のソフトウェアが必要です。何らかの理由によりシステムが感染した場合、Cisco Security Agent は、そのシステムをクリーンにすることはできません。セキュリティを保持し、システムを保護するには、システムでアンチウイルス ソフトウェアも実行する必要があります。

アンチウイルス

ソフトウェアを実行することが承認されているすべての IP テレフォニー サーバおよび VoIP アプリケーション サーバで、承認済みのアンチウイルス ソフトウェアを実行する必要があります。ネットワーク内の他のサーバと同様、アンチウイルス ソフトウェアは、コールの処理に影響するワームやウイルスの感染から、Cisco CallManager サーバを保護します。Cisco Security Agent はシステムの感染をクリーンにできないので、Cisco Security Agent 以外の防御ソフトウェアもシステムにインストールする必要があります。感染したシステムをクリーンにできるのはアンチウイルス ソフトウェアのみです。

Cisco CallManager サーバでのアンチウイルス ソフトウェアの実行に関する追加情報は、次の Web サイトで入手可能です。

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

利点

アンチウイルス ソフトウェアは、アプリケーション サーバが感染して、パフォーマンスが低下するのを防止するのに役立ちます。

欠点

アンチウイルス ソフトウェアの管理には、いくらかのオーバーヘッドが含まれます。さらに、Cisco CallManager および VoIP アプリケーション サーバへのインストールで、ソフトウェアのバージョンが承認されていることを確認する必要があります。

サーバに関する一般的なガイドライン

Cisco CallManager およびその他の VoIP アプリケーション サーバは、通常のサーバとして扱わないでください。システムの設定時に行う任意の操作が、開始を試みているコール、または進行中のコールに影響する場合があります。他のビジネスクラス アプリケーションと同様、大規模な設定の変更は、電話の会話を遮断することがないようメンテナンス ウィンドウで行う必要があります。

アプリケーション サーバ用の標準的なセキュリティ ポリシーは、VoIP サーバには不十分な場合があります。電子メール サーバや Web サーバとは異なり、音声サーバでは、画面をリフレッシュしたり、メッセージを再送信したりすることは許可されていません。音声通信は、リアルタイムのイベントです。VoIP サーバ用のセキュリティ ポリシーでは、音声システムの設定または管理に関連付けられていない作業が、VoIP サーバで決して行われないことを保証する必要があります。ネットワーク内のアプリケーション サーバで通常のアクティビティと見なされるアクティビティ（インターネット サーフィンなど）でも、VoIP サーバで行うことはできません。

また、シスコは VoIP サーバ用に適切に定義されたパッチ システムを提供しています。IT 組織内のパッチ ポリシーに基づいて、このパッチ システムを適用する必要があります。シスコシステムズにより承認されている場合を除き、OS ベンダーのパッチ システムを使用する通常の方法でシステムにパッチを適用しないでください。すべてのパッチは、シスコシステムズの指示に従ってシスコまたは OS ベンダーからダウンロードし、パッチ インストール プロセスに応じて適用する必要があります。

Cisco CallManager 用に OS を強化する方法の詳細は、Cisco CallManager サーバの C:\Utils\SecurityTemplates ディレクトリにリストされています。導入済みのセキュリティ ポリシーで、デフォルト インストールで提供された以上の OS のロック ダウンが要求されている場合は、OS の強化手法を使用する必要があります。

さまざまなソフトウェア パッチが、次の Web サイトで入手可能です。

http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml

（注）　このリンクにアクセスするには、Cisco.com ログイン アカウントが必要です。

上記のサイトには、VoIP サーバに重要なパッチを適用する必要が生じたときに電子メールで通知する通知ツールも含まれています。

利点

アプリケーション サーバを他のアプリケーション サーバのようではなく PBX のように扱う場合、一般的なサーバ セキュリティ プラクティスを実施すると、ウイルスやワームを減らすのに役立ちます。

欠点

追加のセキュリティ機能を設定すると、一部の Cisco CallManager 機能が低下する場合があります。また、アップグレードを正常に実行するには、追加のセキュリティで無効になっている一部のサービスを有効にする必要があるため、アップグレード中は特に注意が必要です。

ロビーに設置された電話機の例

この項の例は、物理的なセキュリティが低いロビー エリアのようなエリアで使用する、電話機およびネットワークを設定する 1 つの方法を示しています。この例に出てくる機能は、いずれもロビーに設置する電話機で要求されている機能ではありませんが、導入済みのセキュリティ ポリシーで、より強固なセキュリティが必要とされている場合は、この例でリストされている機能を使用できます。

いずれのユーザも電話機の PC ポートからネットワークにアクセスできないようにするため、電話機の背面の PC ポートを無効にして、ネットワーク アクセスを制限する必要があります（P.16-5 の「電話機の PC ポート」を参照）。また、攻撃を仕掛けようとしている人が、ロビーに設置された電話の接続先ネットワークの IP アドレスを参照できないように、電話機の設定ページも無効にする必要があります（P.16-9 の「アクセス設定」を参照）。電話機の設定を変更できないという欠点は、通常、ロビーに設置された電話機では問題になりません。

ロビーに設置された電話機が移動される可能性は非常に低いため、電話機には固定 IP アドレスを使用できます。固定 IP アドレスを使用すると、攻撃者が電話機を切断して接続することにより新しい IP アドレスを取得するのを防止できます（P.16-4 の「IP アドレッシング」を参照）。また、電話機を切断すると、ポートの状態が変化し、電話機は Cisco CallManager から登録解除されます。ロビーに設置された電話機のポートでこのイベントをトラッキングするだけで、だれかがネットワークへの接続を試行しているかどうかを判別できます。

電話機の静的ポート セキュリティを使用し、MAC アドレスを取得することを許可しない場合、攻撃者は、そのアドレスを発見できたときに、自らの MAC アドレスをその電話機の MAC アドレスに変更しなければなりません。動的ポート セキュリティを無制限タイマーと共に使用して、MAC アドレスを取得する（取得したアドレスは解除しない）場合、MAC アドレスを追加する必要はありません。これにより、電話機を交換しないかぎり、MAC アドレスをクリアするためにスイッチ ポートを変更せずにすみます。MAC アドレスは、電話機の底面のラベルにリストされています。MAC アドレスをリストすることがセキュリティの問題と見なされる場合は、ラベルを除去し、デバイスを識別するための「ロビー用」というラベルに置き換えることができます（P.16-12 の「スイッチ ポート」を参照）。

ポートまたはポートが接続されているスイッチに関する情報を攻撃者がイーサネット ポートから参照できないように、単一の VLAN を使用し、ポートで Cisco Discovery Protocol（CDP）を無効にできます。この場合、電話機の E911 緊急コール用のスイッチに CDP エントリは与えられません。緊急番号をダイヤルするときは、ロビーに設置された各電話機に、ラベル、またはローカル セキュリティ用の情報メッセージのいずれかが必要です。

ポート上に DHCP は存在しないため、DHCP スヌーピング バインディング テーブルに静的エントリを定義できます（P.16-15 の「DHCP スヌーピング：不正な DHCP サーバ攻撃の防止」を参照）。DHCP スヌーピング バインディング テーブルに静的エントリを定義すると、VLAN で Dynamic ARP Inspection を有効にして、攻撃者が、ネットワーク上のレイヤ 2 ネイバーの 1 つに関する他の情報を取得するのを防止できます（P.16-19 の「Dynamic ARP Inspection の要件」を参照）。

DHCP スヌーピング バインディング テーブルに静的エントリが定義されていると、IP ソース ガードを使用できます（P.16-22 の「IP ソース ガード」を参照）。攻撃者が MAC アドレスと IP アドレスを取得でき、パケットの送信を開始した場合、正しい IP アドレスが設定されたパケットだけを送信できます。

電話機が動作するのに必要なポートと IP アドレスのみを許可する、VLAN ACL を書き込むことができます（P.16-25 の「VLAN アクセス コントロール リスト」を参照）。次の例には、ネットワークへのアクセスを制御するための、レイヤ 2 または最初のレイヤ 3 デバイスのポートに適用可能な非常に小規模な ACL が含まれています（P.16-27 の「ルータのアクセス コントロール リスト」を参照）。この例は、ロビー エリアで使用されている Cisco 7960 IP Phone に基づいています。電話機への Music on Hold または電話機からの HTTP アクセスは使用しません。

この例では、次の IP アドレス範囲を使用します。

- ロビーに設置された電話機の IP アドレスは 10.0.40.5
- Cisco CallManager クラスタのアドレス範囲は 10.0.20.*
- DNS サーバの IP アドレスは 10.0.30.2
- HSRP ルータの IP アドレスは 10.0.10.2 および 10.0.10.3
- ネットワーク内の他の電話機の IP アドレスの範囲は 10.0.*.*

```
10 permit icmp any any
! Allow all icmp - phone to phone, gateway to phone and NMS to phone

20 permit udp host 10.0.10.2 eq 1985 any
!Allow HSRP information in, do not allow out

30 permit udp host 10.0.10.3 eq 1985 any
! Allow in from HSRP neighbor

40 permit udp host 10.0.40.5 range 49152 65535 10.0.20.0 0.0.0.255 eq tftp
! Using ip host from ephemeral port range from phone to the TFPT server  port 69
(start of tftp)

50 permit udp 10.0.20.0 0.0.0.255 range 1024 5000 host 10.0.40.5 range 49152 65535
!Using IP subnet from TFTP server with ephemeral port range to ip host and ephemeral
port range for phone

60 permit udp host 10.0.40.5 range 49152 65535 10.0.20.0 0.0.0.255 range 1024 5000
! Using host from phone to TFTP server with ephemeral port range to ip range and
ephemeral port range for TFTP (continue the TFTP conversation)

70 permit udp host 10.0.40.5 range 49152 65535 host 10.0.30.2 eq domain
! Using IP host and ephemeral port range from phone to DNS server host

80 permit udp host 10.0.30.2 eq domain host 10.0.40.5 range 49152 65535
! Using IP from DNS server to phone host ip and ephemeral port range

90 permit tcp 10.0.40.5 range 49152 65535 10.0.20.0 0.0.0.255 eq 2000
! Using IP host and ephemeral port range from phone to CCM cluster for SCCP


100 permit tcp 10.0.20.0 0.0.0.255 eq 2000 host 10.0.40.5 range 49152 65535
! Using IP range and SCCP port to phone IP host and ephemeral port range


110 permit udp 10.0.0.0 0.0.255.255 range 16384 32767 host 10.0.40.5 range 16384 32767
! Using IP range and ephemeral port range from all phones or gateways outside a vlan
to the IP host to phone

120 permit udp host 10.0.40.5 range 16384 32767 10.0.0.0 0.0.255.255 range 16384 43767
! Using IP host and ephemeral port range from vlan to all other phones or gateways

130 permit udp host 172.19.244.3 range 1024 5000 host 10.0.40.5 eq snmp
!From IP host of NMS server and ephemeral port range (Different for Windows vs Sun) to
IP host of phones and SNMP port (161)

140 permit udp host 10.0.40.5 eq snmp host 172.19.244.3 range 1024 5000
! From IP host of phone with SNMP port (161) to IP host of NMS server and ephemeral
port range
```

ロビーに設置された電話機用の基本的な QoS の例

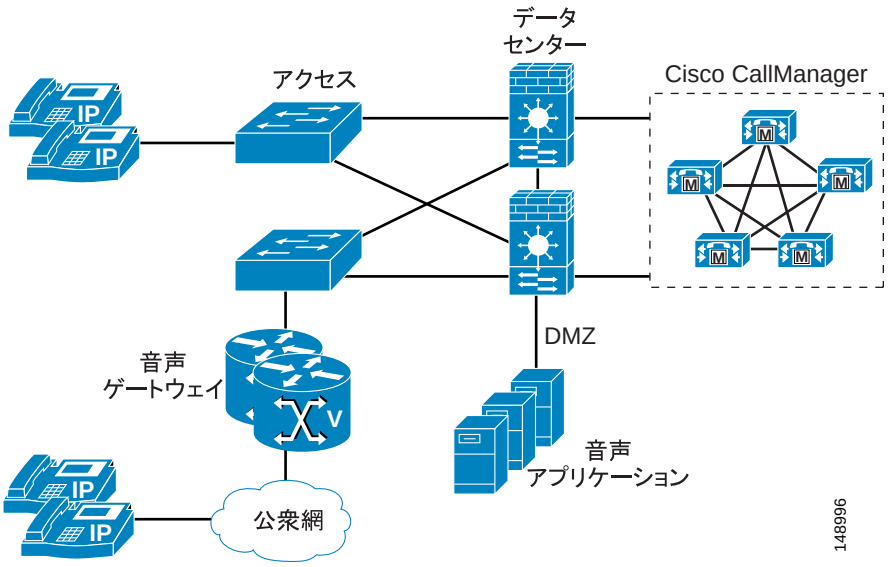
音声ストリームを G.729 に設定し、ポートに送信可能なトラフィックの量を、QoS を使用して制限します（P.16-24 の「QoS」を参照）。QoS 最大値を超えても、トラフィックは、一般的な企業ネットワークで優先度が最低のトラフィックである CS1 つまり Scavenger Class にリセットされます。

```
CAT2970(config)#mls qos map policed-dscp 0 24 46 to 8
! Excess traffic marked 0 or CS3 or EF will be remarked to CS1
CAT2970(config)#
CAT2970(config)#class-map match-all LOBBY-VOICE
CAT2970(config-cmap)# match access-group name LOBBY-VOICE
CAT2970(config-cmap)#class-map match-all LOBBY-SIGNALING
CAT2970(config-cmap)# match access-group name LOBBY-SIGNALING
CAT2970(config-cmap)#exit
CAT2970(config)#
CAT2970(config)#policy-map LOBBY-PHONE
CAT2970(config-pmap)#class LOBBY-VOICE
CAT2970(config-pmap-c)# set ip dscp 46 !Lobby phone VoIP is marked to DSCP EF
CAT2970(config-pmap-c)# police 48000 8000 exceed-action policed-dscp-transmit
! Out-of-profile Lobby voice traffic (g.729) is marked down to Scavenger (CS1)
CAT2970(config-pmap-c)#class LOBBY-SIGNALING
CAT2970(config-pmap-c)# set ip dscp 24 !Signaling is marked to DSCP CS3
CAT2970(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
! Out-of-profile Signaling traffic is marked down to Scavenger (CS1)
CAT2970(config-pmap-c)#class class-default
CAT2970(config-pmap-c)# set ip dscp 0
CAT2970(config-pmap-c)# police 56000 8000 exceed-action policed-dscp-transmit
! Out-of-profile data traffic is marked down to Scavenger (CS1)
CAT2970(config-pmap-c)# exit
CAT2970(config-pmap)#exit
CAT2970(config)#
CAT2970(config)#interface GigabitEthernet0/1
CAT2970(config-if)# service-policy input LOBBY-PHONE !Applies policy to int
CAT2970(config-if)#exit
CAT2970(config)#
CAT2970(config)#ip access list extended LOBBY-VOICE
CAT2970(config-ext-nacl)# permit udp any any range 16384 32767 !VoIP ports
CAT2970(config-ext-nacl)#
CAT2970(config-ext-nacl)#ip access list extended LOBBY-SIGNALING
CAT2970(config-ext-nacl)# permit tcp any any range 2000 2002 !SCCP ports
CAT2970(config-ext-nacl)#end
CAT2970#
```

ファイアウォールの配置例（集中型配置）

この項の例は、Cisco CallManager が背後に配置されているデータ センター内に、ファイアウォールを配置する 1 つの方法を示しています（図 16-19）。この例では、Cisco CallManager は、ファイアウォールの外側のすべての電話機が 1 つのクラスタに含まれる集中型配置に置かれています。この配置内のネットワークには、社内データ センター内でルーテッド モードで設定されたファイアウォールがすでに含まれているので、ゲートウェイの配置を決定する前に負荷が確認されます。ファイアウォールの平均的な負荷を確認した後、CPU に対するファイアウォールの負荷を 60% 未満に保つため、すべての RTP ストリームがファイアウォールを横断しないようにすることが決定されました（P.16-31 の「ゲートウェイの周囲へのファイアウォールの配置」を参照）。ゲートウェイはファイアウォールの外側に配置されています。Cisco CallManager とゲートウェイの間の TCP データ フローを制御するため、ネットワーク内の ACL を使用します。電話機の IP アドレスは適切に定義されているので、ACL は、電話機からの RTP ストリームを制御するためネットワークにも書き込まれます（P.16-4 の「IP アドレッシング」を参照）。音声アプリケーション サーバは非武装地帯（DMZ）に配置されています。Cisco CallManager との間のアクセス、およびネットワーク上のユーザへのアクセスを制御するため、ファイアウォールで ACL を使用します。この設定では、インスペクションを使用してファイアウォールを通過する RTP ストリームの量を制限します。これにより、既存のネットワークに新しい音声アプリケーションを追加したときの、ファイアウォールに対する影響を最小に抑えられます。

図 16-19　ファイアウォールの配置例



まとめ

この章では、ネットワーク内の音声データを保護するために有効にできるセキュリティのうち、一部のみを取り上げました。ここで取り上げた手法は、ネットワーク内のすべてのデータを保護するためにネットワーク管理者が使用できる、すべてのツールのサブセットにすぎません。逆に、ネットワーク全体のデータで必要なセキュリティのレベルによっては、これらのツールでさえ、ネットワークで有効にする必要がない場合もあります。セキュリティの方法は、注意深く選択してください。ネットワーク内のセキュリティが高くなると、それに応じて、複雑度や問題のトラブルシューティングも増加します。各企業の責任で、リスクと組織の要件の両方を定義し、ネットワークとネットワークに接続されたデバイスに適切なセキュリティを適用する必要があります。