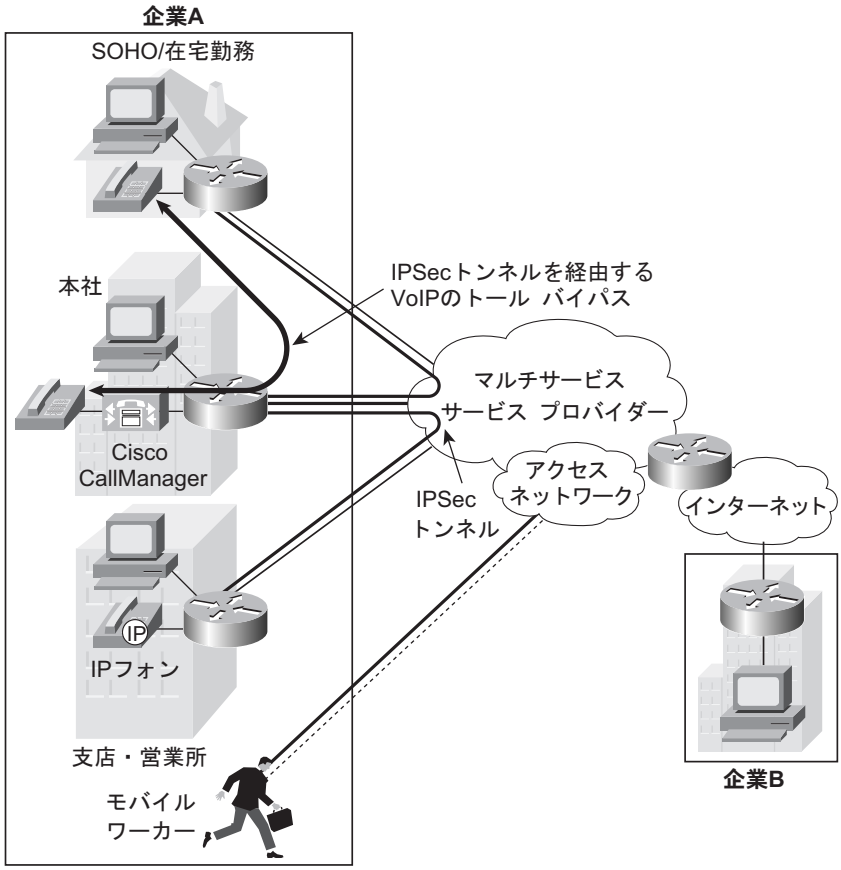
ホワイト ペーパー

データ / 音声 / 映像対応 IPSec VPN ソリューション — IPSec VPN（ V^3PN ）

ソリューション概要

Virtual Private Network（VPN; 仮想私設網）は、専用線、フレームリレー、または ATM（非同期転送モード）による専用線と同様のサービスを利用できるネットワークとして、低コストかつ柔軟性の高いソリューションを提供します。VPN を利用すると、在宅勤務者およびモバイル ユーザによるシームレスなリモート アクセスおよび費用効果の高いリモート オフィス接続が可能になります。VPN では、共有ネットワーク上で暗号化 VPN トンネルによるセキュアなネットワークを活用することにより、企業データ ネットワークの費用を大幅に節約します。しかし、多くの企業が統合ネットワークの導入に向かいつつある今、VPN にも新たな機能が求められています。シスコが提供するデータ / 音声 / 映像対応の VPN（V^3PN）を使用すれば、費用効果の高い VPN を活用しながら、品質や信頼性を損なうことなく、音声と映像をデータ ネットワークに追加できます。図 1 は、IPSec VPN を利用して、マルチサービス サービス プロバイダーの公衆網に専用ネットワークを構築し、音声とデータを安全に送信する方法を示したものです。

図 1
音声 / 映像対応 IPSec VPN



このソリューション概要では、ビジネスを運営するうえで、配置上の検討事項、実現可能なテクノロジー、製品、そしてシスコ V^3PN ソリューションの価値を実証する 2 つのケース スタディについて記載します。

ビジネス要因

市場における業務拡張と激しい競争の中にあって、企業のネットワーク管理者は、本社、支社、自宅、外出先のどこにいる社員にでも、音声、映像、データによるサービスを配信するネットワーク ソリューションを探し求めています。ビジネスの要因には次のものがあります。

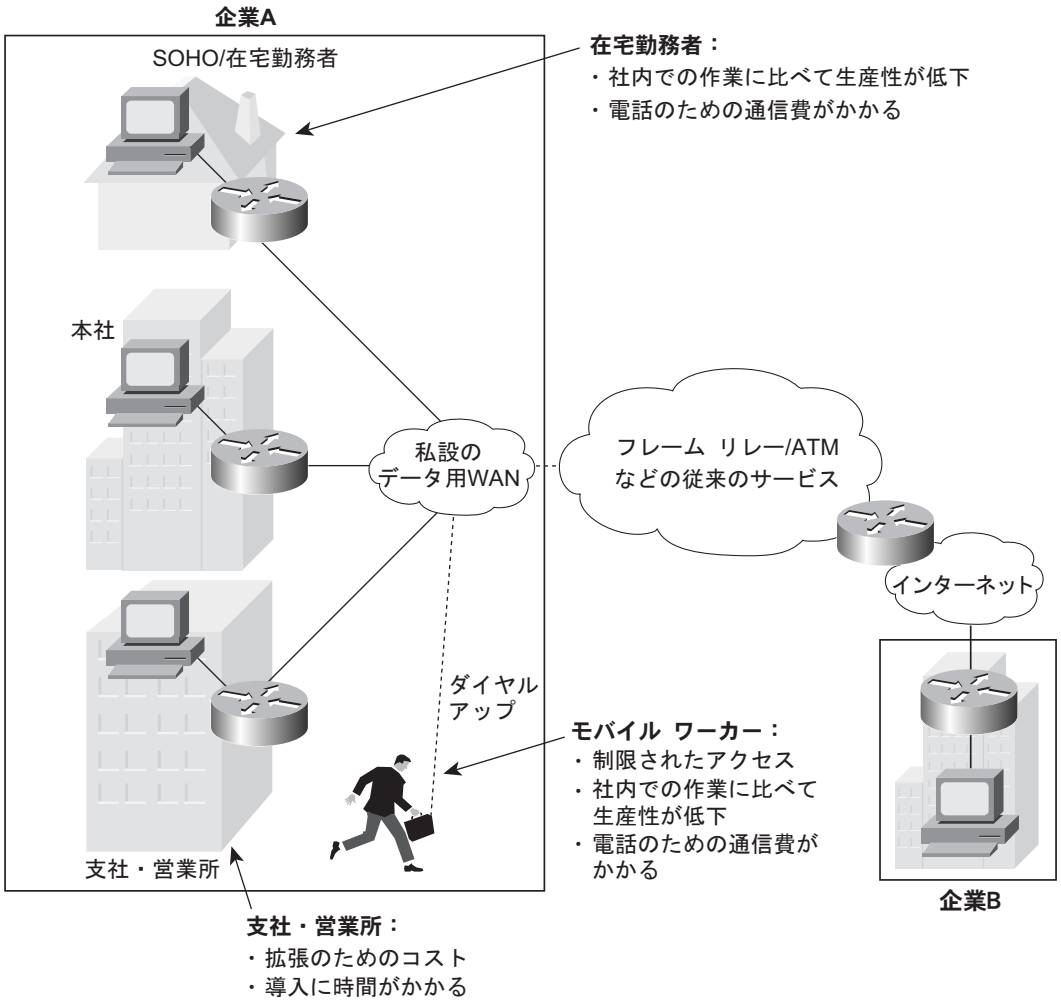
- **コスト削減** — 企業は、音声、映像、データのサービスを 1 つの IP ネットワークに統合し、より経済的で効率的な方法で、社員に配信する必要があります。コスト削減には、ネットワーク運用コスト、WAN 送信コスト、在宅勤務者とモバイル ワーカーのアクセス コスト、通話料の削減が含まれます。
- **従業員の生産性の向上** — 自宅やホテルからでも高速インターネットへアクセスできるようになり、企業はネットワークを在宅勤務者やモバイル ワーカーにまで拡張して、これらの社員が企業のネットワークと同じ音声、映像、データのサービスへアクセスできるようにする必要が生じています。
- **市場への迅速な対応** — 企業は、市場の需要に適格に対応し、新しい支社や販売オフィスを開設したら、これを迅速にネットワークに接続する必要があります。

以下に、この拡張しつつあるモバイル業務環境でビジネスを行う際の問題点と、Cisco V^3PN IPSec VPN ソリューションを利用してこれらの問題点を克服する方法について述べます。

現状の課題

企業ネットワークやサービスを支社、在宅勤務者、モバイル ワーカーにまで拡張しようとすると、それぞれに固有の課題が生じ、新しいテクノロジーを導入する必要が生じます。図 2 は、これらの課題とその詳細、そして具体例を示したものです。

図 2
ビジネス上の課題



課題には次のようなものがあります。

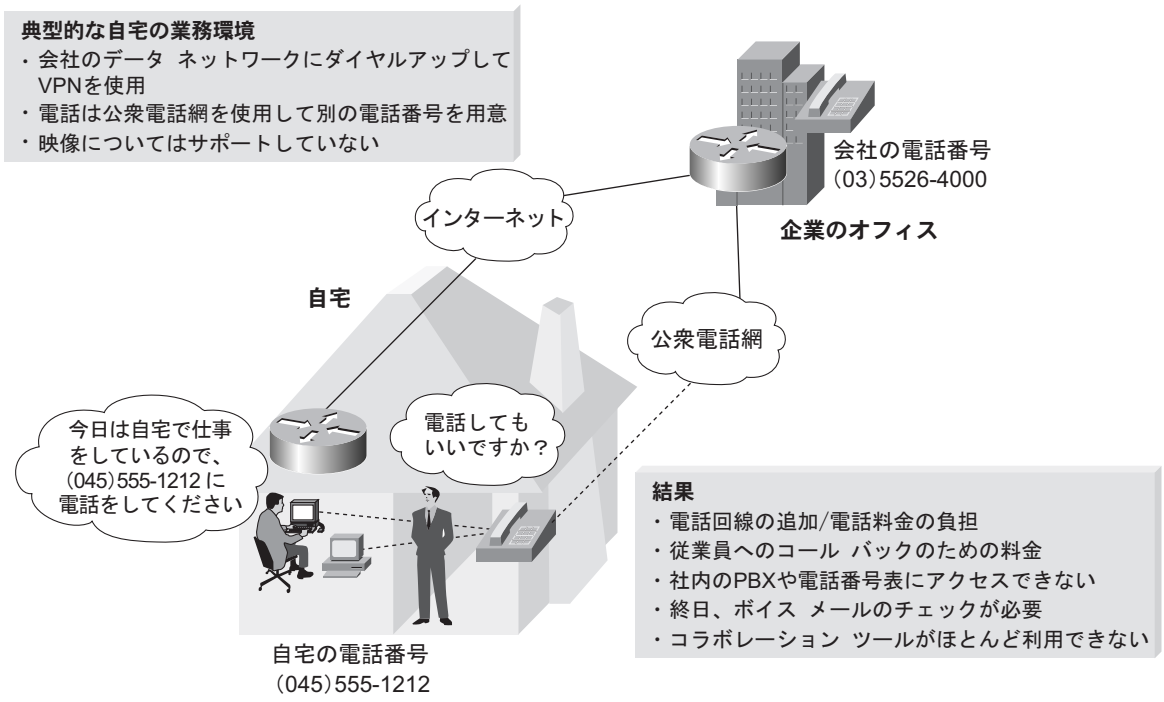
- **支社・営業所** — 私設網と同様のパフォーマンスとセキュリティの厳しい要件を満たしながら、専用線、フレーム リレー、または ATM 回線を使用するよりも低いコストで迅速に企業ネットワークに支社・営業所のネットワークを追加できること
- **在宅勤務者 / モバイル ワーカー** — 在宅勤務者およびモバイル ワーカーに、高レベルのセキュリティを備えながら、オフィスにいるのと同レベルの生産性を提供すること

たとえば、在宅勤務者は、通常ダイヤルアップ モデムまたは ISDN 回線を使って企業のデータ サービスにアクセスします。多くの場合、通話料金には、毎月の基本接続料金に加えて、フリーダイヤルによる料金が加算されます。こうした接続は低速リンクであるため、生産性は低く、コストは高くなります。

Digital Subscriber Line（DSL; デジタル加入者線）、ケーブル高速インターネット アクセス、新 VPN テクノロジーの出現により、企業データ サービスへの高帯域アクセスによるコストを低減し、在宅勤務者の生産性を大幅に向上させることができるようになりました。ただし、企業音声サービスへのアクセスはほとんど存在していません。一方で、自宅にいる社員が電話を使って業務を行うのは、とても非効率的です。在宅勤務者は、家庭用の電話を使用するか、携帯電話を使用するか、あるいは別料金を支払って仕事用に回線を追加す

るしかありません。そうすると、在宅勤務者は最低 2 本の電話番号と 2 つのボイスメール ボックス（仕事用と家庭用）を持ち、これらすべての着信電話をやり繰りしなくてはなりません。図 3 は在宅勤務の課題を示したものです。

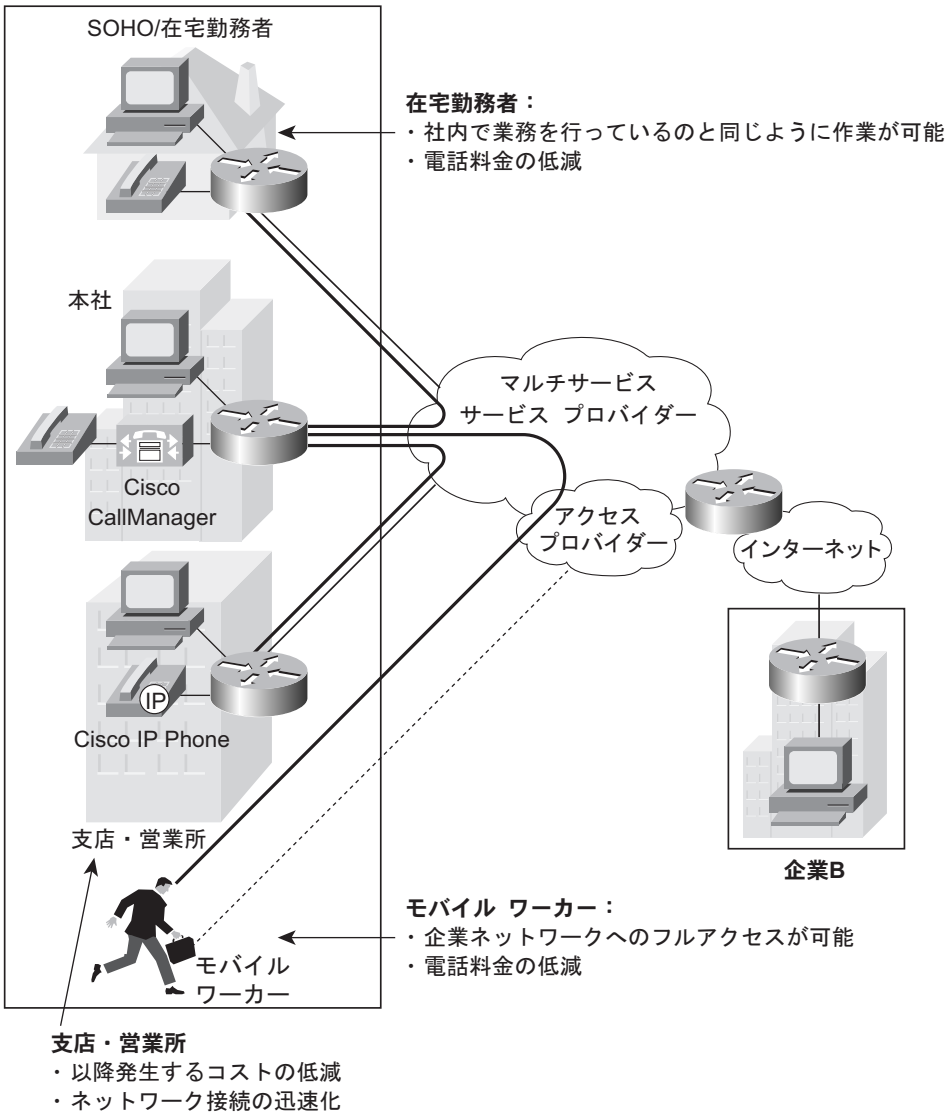
図 3
典型的な在宅勤務者の課題



Cisco V^{3}PN ソリューション

Cisco V^{3}PN ソリューションは、専用ネットワークと同等のパフォーマンスおよびセキュリティの厳しい要件を維持しながら、低コストでマルチサービス WAN を実現し、社員の生産性を最適化する、新しいリモートアクセス手段です。このソリューションの使用により、すべてのユーザが場所を問わず安定的に企業ネットワークに接続できます。図 4 は、従来の企業ネットワークへの接続と比較しながら、Cisco V^{3}PN ソリューション使用の利点を示したものです。

図 4
Cisco V^{3}PN ソリューション



ソリューションの検討事項

ここでは、Cisco V^{3}PN ソリューションを配置する際にネットワーク管理者が検討すべき事項について説明します。

QoS

- 音声と映像の品質は、ネットワーク リンクが脆弱であれば低下します。したがってエンドツーエンドの Quality of Service（QoS; サービス品質）が重要になります。レイテンシ、ジッタ、パケット損失はすべて音声と映像の品質の低下につながります。ネットワーク管理者は、十分な音声および映像品質を維持するために、企業 LAN だけでなく、サービス プロバイダーが提供するサービス レベルを把握する必要が

あります。このドキュメントのなかでは、複数のサービス（音声、映像、データ）をサポートするために必要となる低レイテンシ帯域幅および SLA（サービスレベル アグリーメント）を提供するマルチサービス サービス プロバイダーについて述べます。

セキュリティ

- **送信セキュリティ** ― 公衆アクセス ネットワークおよびバックボーン ネットワークを横断するトラフィックは、適切なセキュリティ確保が必要です。IPSec VPN は、（暗号化を使用した）データ機密、データ完全性、加入ピア間のデータ認証によりこのセキュリティを提供します。
- **ネットワーク セキュリティ** ― シスコのファイアウォールは、VPN などのあらゆる公衆ネットワークにとって重要であるステートフルな周辺セキュリティを提供します。VPN に音声と映像を展開する場合は、ファイアウォールを横断するすべてのマルチサービス トラフィックをステートフルに検査することが重要です。
- **侵入検知** ― ネットワーク境界保護を追加し、侵入者やワームなどの悪意あるトラフィックから IP テレフォニー ホストを遮蔽して、Cisco V^{3}PN を確保するためには、侵入検知が不可欠です。

ネットワーク アベイラビリティ

- **冗長コンポーネントとパス** ― コンポーネントまたはサービス プロバイダー ネットワークの障害時に高速で自動的にネットワークを回復させるには、クリティカルなコンポーネント（VPN ヘッドエンド）およびデータ パスの冗長をサポートする必要があります。

ネットワークとサービスのインターオペラビリティ

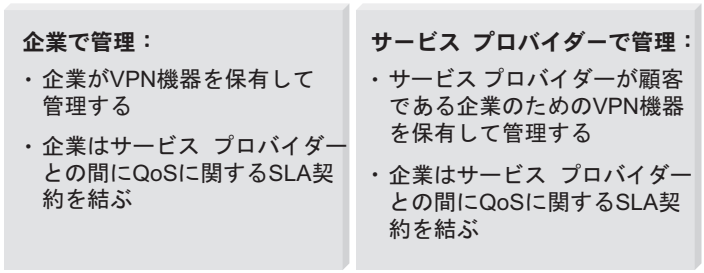
- **QoS および IPSec の相互作用** ― IPSec は、QoS マーキングを含めてパケットを暗号化します。したがって、IPSec 暗号化トラフィックについても QoS をサポートできる VPN デバイスを持つことが、VPN で通話品質の音声と映像においてきわめて重要な要素です。
- **VPN でのマルチキャスト サポート** ― 音声および映像のトラフィックの多くはマルチキャスト です。IPSec は、本来マルチキャスト トラフィックをサポートしません。VPN でマルチキャストをサポートできる VPN デバイスを持つことが Cisco V^{3}PN ソリューションにおいてきわめて重要です。
- **低レイテンシ ネットワーク トポロジーのサポート** ― レイテンシとジッタを低減するには、メッシュ ネットワーク トポロジーを持つことが重要です。VPN デバイスは、基本的なハブアンドスポークだけなく、メッシュ トポロジーもサポート可能である必要があります。
- **VoIP プロトコル用のファイアウォール サポート** ― 多くのファイアウォール ソリューションでは、ステートフルにトラフィックを検査できないため、IP テレフォニー トラフィックのパススルーが必要です。IP テレフォニーをサポート可能なファイアウォールを持つことが、Cisco V^{3}PN ソリューションのセキュリティにおいてきわめて重要です。

サービス管理オプション

ビジネスの中核ではない業務をアウトソーシングする傾向が高まり、専用 VPN の規模が拡大して複雑になるにしたがい、企業はサービス プロバイダーを採用して VPN を管理しようと考える場合もあるでしょう。企業は、Customer Premises Equipment（CPE; 顧客宅内機器）を管理して、サービス プロバイダーと SLA の交渉を行うことも、サービス プロバイダーに CPE を含む WAN 全体を管理させることもできます。

次に、通話品質の音声および映像をサポートするのに必要なマルチサービス サービス プロバイダーおよび一般 SLA 要件について説明します。

図 5
VPN サービス管理オプション



マルチサービス サービス プロバイダー

企業が V^{3}PN ソリューションを配置する際に直面する重要なステップは、マルチサービス サービス プロバイダーを見つけて、SLA 契約を結ぶことです。シスコは、マルチサービスをサポートするために IP ネットワークを調整する大手のサービス プロバイダーと密接に連携して、企業のお客様が優秀なマルチサービスのサービス プロバイダーを識別できるよう、Cisco Powered Network プログラムを開発しました。

一般的な SLA 要件

SLA 交渉における基本は、高品質の音声、映像、データ送信をサポートするのに必要なレイテンシ、ジッタ、パケット損失バジェットを、ネットワークのセクションごとに把握することです。ネットワーク管理者は、ネットワークの LAN セクションのバジェット値を決定し、その値を使用して SLA で交渉した制限を設定する必要があります。以下に、Cisco Powered Network 指定の資格を持つマルチサービスのサービス プロバイダーがサポートすべきレイテンシ、ジッタ、パケット損失メトリックを示します。サービス プロバイダーは、ネットワーク アベイラビリティやトラフィックのタイプに基づく保証帯域幅など、他のメトリックを提案する場合があるので注意が必要です。

- レイテンシ（米国または欧州内で 60 ms 以下）
- ジッタ（20 ms 以下）
- パケット損失（0.5% 以下）

マルチサービスのサービス プロバイダー選択についての詳細は、次の URL をご覧ください。

Cisco Powered Network

http://www.cisco.com/jp/cpn/

導入モデル

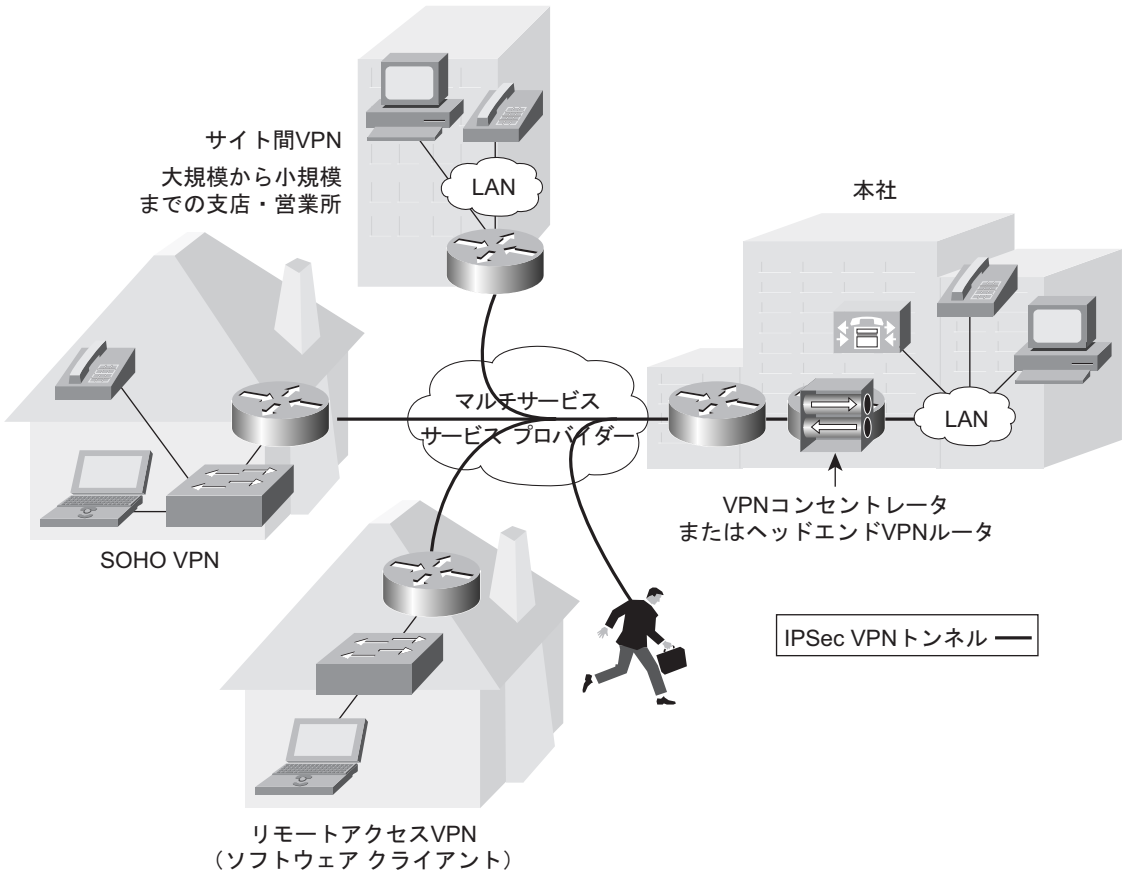
Cisco V^{3}PN ソリューションはサイトツーサイト、Small Office/Home Office（SOHO）、リモート アクセスという 3 つの導入モデルをサポートします。各モデルは同様のテクノロジーとトポロジーを使用しますが、サービス プロバイダー ネットワークに要求されるサポート レベルはそれぞれ異なります。次のセクションでは、導入モデルを図示し、異なったレベルのサービス プロバイダー サポートをそれぞれ示します。図 6 は、Cisco V^{3}PN 配置モデルを複合したものです。

一般的な VPN 配置アーキテクチャの詳細については、次の URL をご覧ください。

SAFE BLUEPRINT ― SAFE: VPN IPSec Virtual Private Networks in Depth（英語）

http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a00801dca2d.shtml

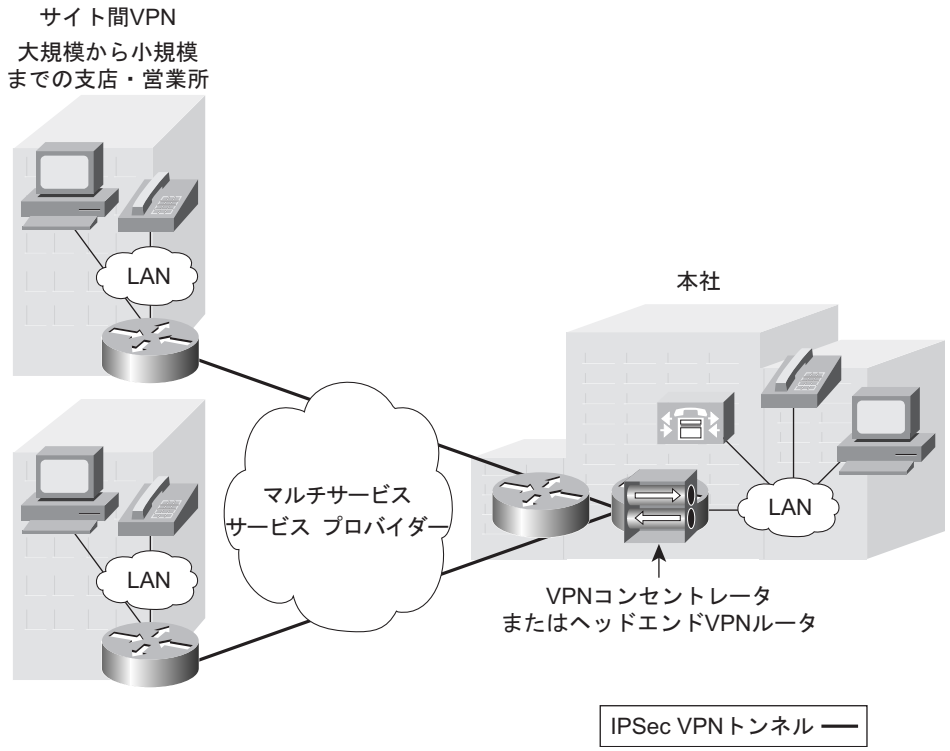
図 6
V3PN 配置モデル



サイト間 VPN の導入モデル

サイト間 VPN の導入モデルは、企業本社と支社・営業所との間の IPSec トンネルで構成されます。この導入モデルは、バックボーン マルチサービス サービス プロバイダーを利用して、ハブアンドスポークおよびメッシュ トポロジーをサポートすることで、従来の企業 WAN と同じ機能を提供します。バックボーン サービス プロバイダーは、ネットワークをアップグレードしてマルチサービスをサポートする最初のプロバイダーです。このプロバイダーは、マルチサービス VPN によって、WAN に代わるソリューションを、迅速に企業に提供します。図 7 は、サイト間 VPN のハブアンドスポーク型での導入例です。

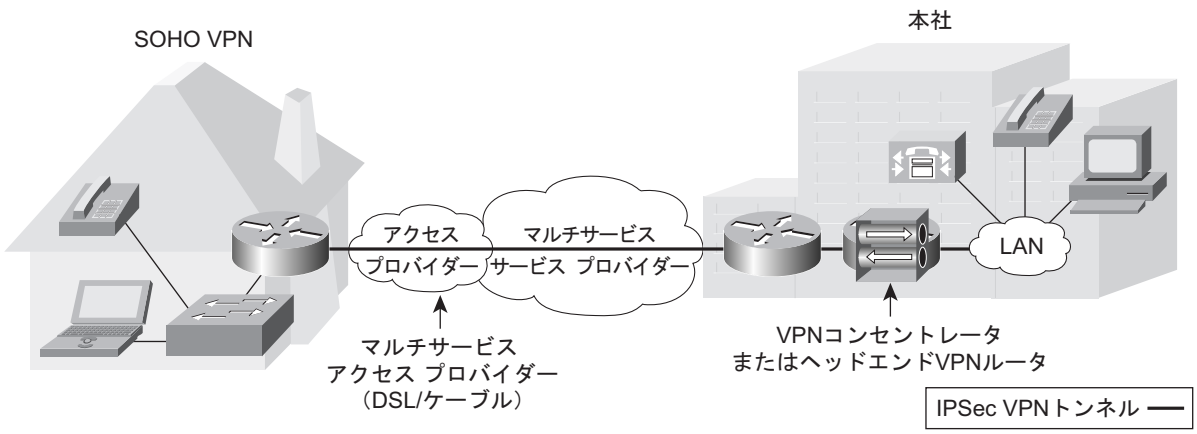
図 7
サイト間 VPN の導入モデル



SOHO VPN の導入モデル

SOHO 配置モデルは、企業本社と SOHO（すなわち在宅勤務者）との間の IPSec トンネルで構成されます。この導入モデルは、複数のマルチサービス サービス プロバイダー（すなわちバックボーンおよびアクセス）を利用して、従来のハブアンドスポーク WAN と同じ機能を提供します。シスコは、アクセス プロバイダーとバックボーン プロバイダーの両方と密接に連携して、このエンドツーエンド マルチサービス機能を簡易化し、V^3PN SOHO ソリューションの送信オプションを提供します。図 8 は、SOHO VPN を導入し、VPN 接続が複数のサービス プロバイダーを横断する様子を示しています。

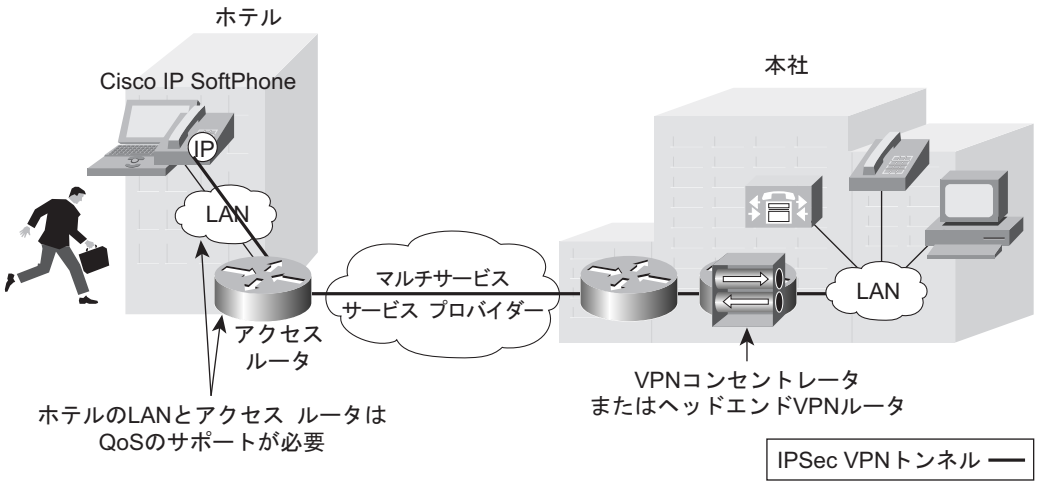
図 8
SOHO VPN の導入モデル



リモート アクセス VPN の導入モデル

リモート アクセス VPN の導入モデルは、企業本社とモバイル ワーカーのラップトップ コンピュータ間の IPSec トンネルで構成されます。この導入モデルも、複数のマルチサービス サービス プロバイダー（すなわちバックボーンおよびホテル ネットワーク）を利用して、「高速」な企業リモート アクセス ネットワークを提供します。図 9 は、リモート アクセス VPN を導入して、VPN 接続が複数のサービス プロバイダーを横断する様子を示しています。

図 9
リモート アクセス VPN の導入モデル



テクノロジー

QoS ツール

エンドツーエンド QoS は、VPN で通話品質の音声および映像サービスを配信するうえで非常に重要となります。シスコは、Cisco IOS® ソフトウェアで利用できる数多くの QoS ツールが、VPN 機能と連携して動作するようにしました。ここでは、Cisco V^{3}PN ソリューションを配置するときにネットワーク管理者が検討すべき QoS 問題と、シスコがそれぞれの問題に対応するために提供しているツールについて説明します。

IP テレフォニー ネットワーク設計の詳細については、下記の URL をご覧ください。

CISCO IP TELEPHONY SOLUTION — Design Guides（英語）

http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns268/networking_solutions_design_guidances_list.html

エンドツーエンドQoSに必要な基本ステップを以下に示します。詳細については次のセクションで述べます。

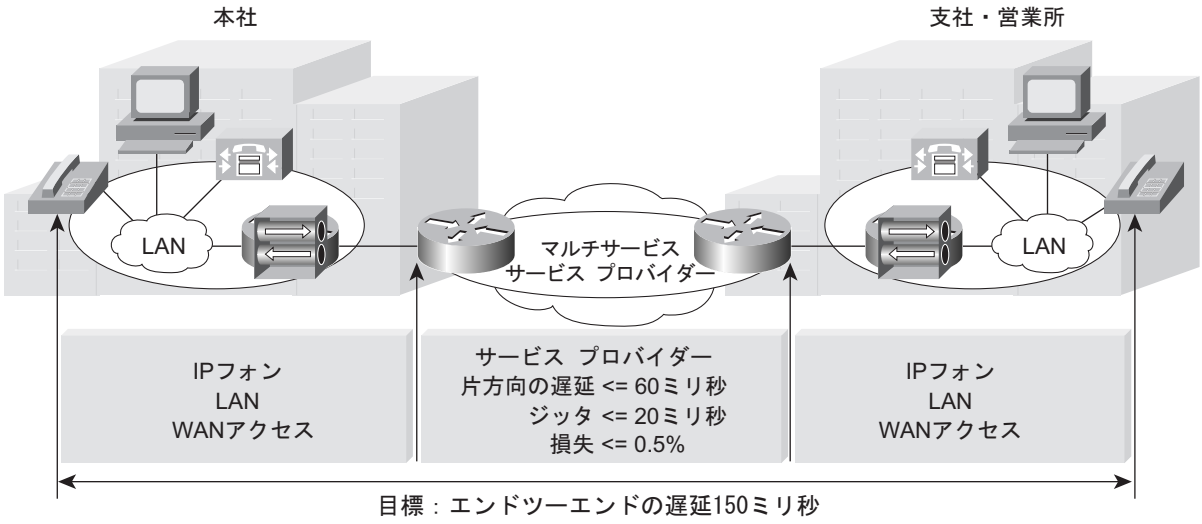
ステップ 1. トラフィックが適切なクラスのサービスに割り当てられるよう、サービス プロバイダーによる分類と適格に一致するように音声、映像、およびデータ トラフィックを分類します。

ステップ 2. LAN と企業エッジ ルータに適切な QoS ツールを実装して、サービス プロバイダー ネットワーク方向に、トラフィックを正しくキューに入れます。

ステップ 3. Call Admission Control（CAC）を実施して、アクセス リンクの横断を許可される音声および映像の数を制限します。

図 10 は、通話品質の音声および映像送信のための推奨エンドツーエンド レイテンシ、ジッタ、パケット損失を制限する目標と、それを管理する QoS を示したものです。

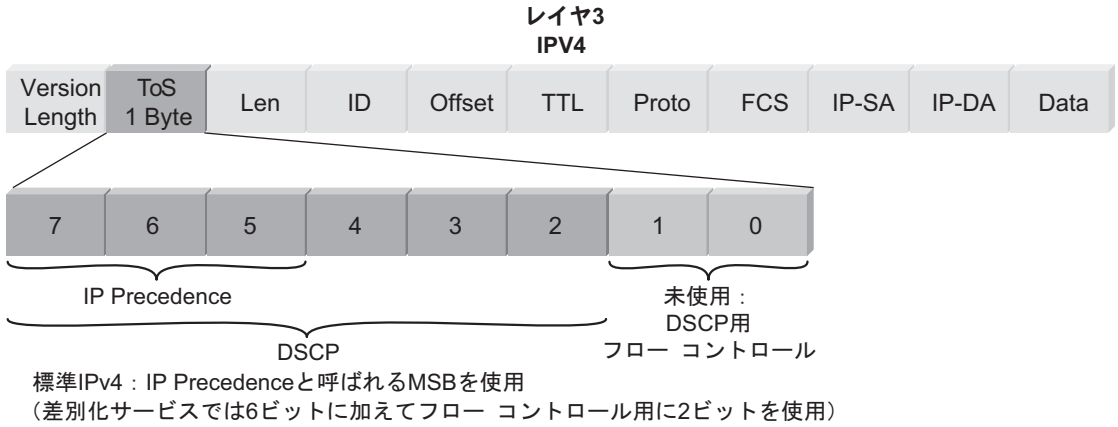
図 10
エンドツーエンド QoS 管理



分類

分類とは、パケットまたはフローに特定のプライオリティをマーキングすることです。分類は、企業 LAN のワイヤリング クローゼットか、IP フォンなどの音声 / 映像エンドポイントの内部で行われます。ネットワーク内でプライオリティ処理を行うためには、パケットの IPv4 ヘッダにある Type-of-Service（ToS）バイトに IP Precedence または Differentiated Services Code Point（DSCP）ビットでマーキングを行う必要があります。図 11 は、ToS フィールドと、IP Precedence および DSCP QoS マーキングに使用されるビットを示しています。

図 11
QoS レイヤ 3 分類



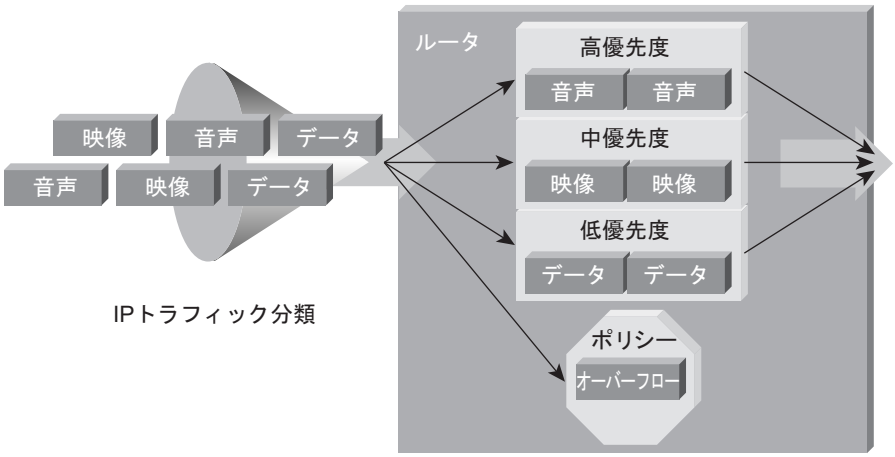
前述のとおり、このマーキングは、エンドポイント（たとえば、IP フォン）か、企業のエッジ ルータでパケット内に書き込まれます。これは、サービス プロバイダーのネットワーク内でパケットに与えられるサービスのクラスを決定するための選択基準となります。また、IP Precedence 値と DSCP では、同じフィールドを使用していることに注意してください。これは 2 つのマーキング方式の互換性を保つため意図的に行われているものであり、シスコ製装置は両方をサポートしています。エンドポイントを DSCP で分類するように設定していたとしても、パケットは IP Precedence ベースの QoS ネットワークで適切に処理されます。実際、エッジ ルータによっては、1 つの方式を別の方式に変換するように設定することさえできます。

キューイング

キューイング ツールは、パケットまたはフローを分類に基づいて複数のキューのうちの 1 つに割り当てて、ネットワーク内で適切な処理が行われるようにします。データ、音声、映像が同じキューに入れられた場合、パケット損失や様々な遅延がさらに発生しやすくなります。出力側インターフェイスに複数のキューを使用し、音声パケットをデータ パケットとは異なったキューに入れることにより、ネットワークの動作は大幅に予測可能になります。

インターフェイス キューイングは、データ ネットワーク内で音声品質を保証するうえでもっとも重要な機構の 1 つです。これは、非常に制限された量のネットワーク リソースを求めて多くのトラフィック フローが競い合っている WAN では、さらに重要になります。トラフィックが分類されると、その処理要件を満たすインターフェイスの出力側キューにフローを置くことができます。Voice over IP（VoIP）は、パケット損失と遅延への許容値が極端に低いため、高優先度のキューに入れる必要があります。ただし、他のトラフィック タイプにも特定の帯域幅と遅延の特性がある場合があります。これらの要件は、Cisco IOS ソフトウェアの Low-Latency Queuing（LLQ; 低遅延キューイング）で対応します。図 12 は、分類に基づくトラフィックのキューイングを示したものです。

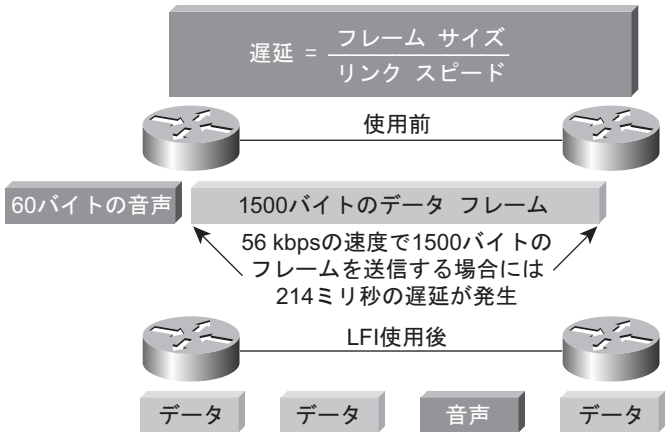
図 12
トラフィック分類に基づくキューイング



Link Fragmentation and Interleaving（LFI）

低速 WAN 接続（768 kbps 以下の速度）の場合、大きなフレームをデータ ストリームに流す際にはジッタの発生を抑えるために LFI が必要です。LFI ツールは、エンドツーエンド遅延を正確に予測するため、大きなデータ フレームを一定のサイズの小片に細分化したり、フローのなかに音声フレームを挿入したりする場合に使用されます。図 13 に示すように、このツールは音声トラフィックが大きなデータ フレームの背後で遅延するのを防ぐことにより、ジッタを低減しています。

図 13
フレーム遅延を低減するための LFI ツールの使用

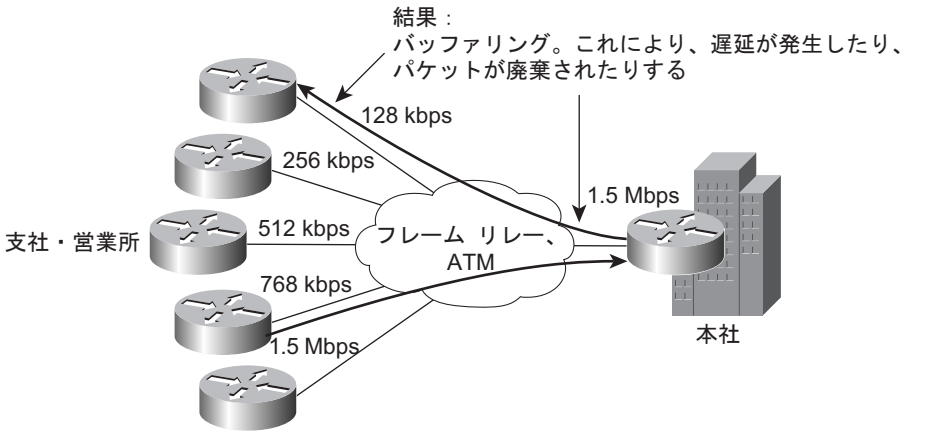


トラフィック シェーピング

ATM およびフレーム リレーのネットワークでは、物理アクセス速度は 2 つのエンドポイント間で異なりますが、トラフィック シェーピングは、これらの速度の不一致が原因で輻輳したネットワークのインターフェイス バッファから生じる、過度の遅延を防止するのに使用されます。トラフィック シェーピングは、送信元ルータから宛先ルータまでのフレームの送信レートを測定するツールです。この測定は通常、送信インターフェイスの回線または回路のレートよりも小さい値で行われます。このレートで測定が行われるのは、ハブアンドスポーク トポロジーで一般的な回線速度不一致を解消するためです。

たとえば、図 14 に示すように、小規模の WAN 接続を行っているリモート サイトが多く集束されると、中央サイトで規定された帯域幅または回線速度のオーバーサブスクライブが生じることがあります。

図 14
バッファリングによって引き起こされる遅延



つまり、Cisco IOS ソフトウェアで使用可能なこれらの QoS ツールのすべてが、VPN 機能と連携して V^3PN ソリューションを実装可能にします。

Call Admission Control（CAC）

CAC は、音声フローが音声通話のために割り当てられた最大規定帯域幅を超えないようにする機構です。

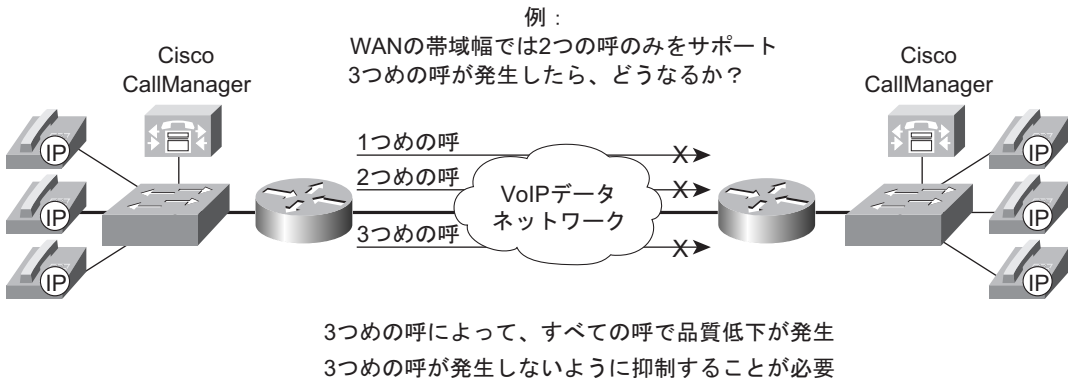
音声、データ、そして場合によっては映像アプリケーションをサポートするのに必要な帯域幅を規定するための計算を行ったあとは、音声が割り当てられた帯域幅の部分をオーバーサブスクライブしないようにする必要があります。通常、QoS 機構は、音声をデータから保護するために使用されますが、CAC は音声を音声から保護するために使用されます。図 15 にこれを示します。図 15 は、2 つの同時音声通話をサポートするよう帯域幅が規定されている環境です。3 つめの音声コールの進行が許可されると、3 つのコールすべての品質が低下します。この音声品質の低下を防ぐために、Cisco CallManager（CCM）および Cisco IOS ゲートキーパに CAC を規定して、3 つめのコールをブロックします。

CAC の詳細については、下記の URL をご覧ください。

CISCO IP TELEPHONY SOLUTION — Design Guides（英語）

http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns268/networking_solutions_design_guidances_list.html

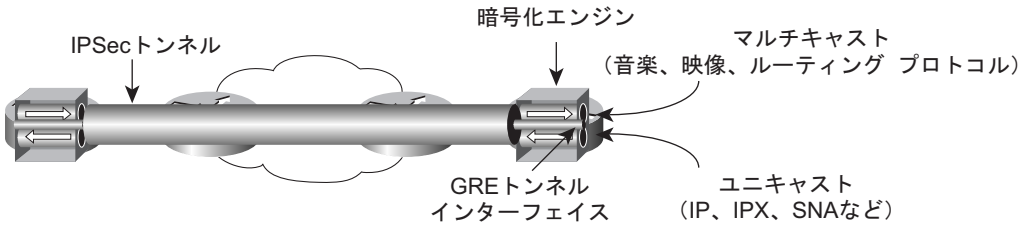
図 15
CAC



IPSec により保護された GRE

IPSec に保護された Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）トンネルは、V^3PN ソリューションの重要なコンポーネントです。これは、さまざまなトラフィック タイプとトポロジーでの安全な送信を提供し、ネットワークのアベイラビリティをダイナミック ルーティングによって保証します。図 16 は、IPSec により保護された GRE トンネルを示したものです。

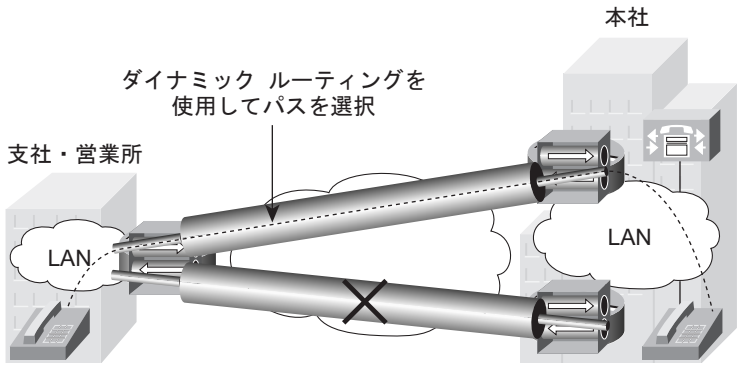
図 16
IPSec により保護された GRE



- **多様なトラフィック タイプ** — GRE はユニキャスト トラフィックとマルチキャスト トラフィックの両方の送信をサポートし、IP および非 IP プロトコル（たとえば、Internetwork Packet Exchange [IPX]、System Network Architecture [SNA] など）のどちらのトンネリングにも有用です。
- **多様なトポロジー** — 論理的には、GRE はエンドポイント間のポイントツーポイント トンネルであり、ハブアンドスポークとメッシュ トポロジーをサポートします。音声または映像の品質を維持するために遅延を最小化しなくてはならない場合、遠いエンドポイントまでのトンネルを設定できるため、ハブ サイトを横断するために複数の暗号化サイクルに遭遇するようなことがなくなります。
- **独立エンタープライズ ルーティングと IP アドレス指定** — IP パケットは GRE ヘッダ内部に置かれ、IP データグラムでカプセル化されてリモートエンドへ「トンネル」されます。VPN デバイス上でトンネルを終端されるので、企業アドレス スペースとルーティング情報は、他の顧客またはサービス プロバイダーのアドレス スペースやルーティング情報とは独立したものとなります。そのため、企業にも、サービス プロバイダーにも最大の柔軟性が提供されます。
- **ネットワーク アベイラビリティ** — 本来、IPSec は効果的なフェイルオーバー機能をサポートしませんが、V^3PN ソリューションは、ダイナミック ルーティングと GRE を組み合わせて使用することにより、この問題に対処します。IPSec トンネルは、リモート ピアからの確認応答またはフィードバック機構なしにデータを送信するため、IPSec エンドポイントには、そのリモート ピアが到達可能なのかどうかを判断する方法がありません。したがって、リモート ピアがダウンしたり、到達不能であったりした場合、IPSec エンドポイントはデータを「ブラック ホール」と呼ばれる場所へ盲目的に送信し続けます。

V^3PN ソリューションは、ダイナミック ルーティング プロトコルを IPSec に保護された GRE トンネルで使用し、リモート ネットワークの到達可能性を追跡します。ハイ アベイラビリティのためにダイナミック ルーティングを使用しているリモート サイトは、それぞれが互いにヘッドエンドとなっている、IPSec に保護された GRE トンネルを 2 つ確立します。ルーティング更新は両方のトンネルを横断してリモート サイトへ到達し、次に宛先ネットワークへの最適なパスを持つヘッドエンドへトラフィックを転送します。図 17 は失敗したリンクと、トラフィックがどのように有効なパスへと方向転換したかを示したものです。

図 17
ダイナミック ルーティングを使用してネットワーク アベイラビリティを確保

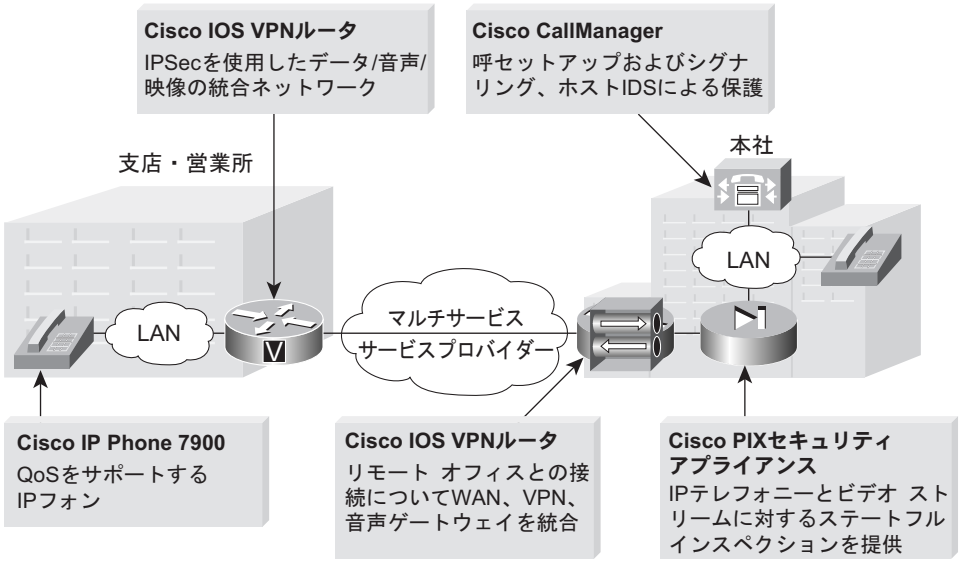


製品

IP テレフォニーや映像、IPSec VPN、セキュリティ製品などをエンドツーエンドで提供しているシスコは、Cisco V^3PN ソリューションによる統合型ネットワーク ソリューションを提供するうえでの確かな地位を築いています。シスコが開発した V^3PN ソリューションを導入することにより、IPSec VPN でマルチサービスのインターオペラビリティが保証され、統一されたネットワーク デザイン ガイダンスおよびサポートが提供されます（図 18）。

- **Cisco IOS VPN ルータ** — Cisco 1700、2600、3600、3700、7200 シリーズなどのシスコ ルータは、V^{3}PN ソリューションの基礎となる製品です。Cisco VPN ルータは、ルーティングのほかに、VPN でのマルチサービス トラフィックのための暗号化や QoS の機能を提供します。リモート サイトでは、Cisco IOS VPN ルータが、VPN、テレフォニー、WAN アクセス、ファイアウォールのワンボックス ソリューションとして機能するため、費用効果の高いリモート オフィス ソリューションが実現されます。
- **Cisco CallManager** — Cisco CallManager（CCM）は、IP テレフォニー インフラストラクチャのためのスケーラブルな呼制御とシグナリング サービスを提供します。
- **Cisco IP Phone** — シスコの IP フォンは、従来の電話と同じユーザ インターフェイスですが、ディレクトリ サービスやニュース フィードなどの強力な機能が利用できます。
- **Cisco IOS 音声ゲートウェイ** — Cisco IOS 音声ゲートウェイは、VoIP ネットワークから公衆電話網への接続を提供します。
- **Cisco PIX® セキュリティ アプライアンス** — Cisco PIX セキュリティ アプライアンスは、H.323 Session Initiation Protocol（SIP）や Skinny などのプロトコルを含む音声 / 映像トラフィックのステートフル インスペクションを提供します。
- **Cisco IDS Host Sensor** — IDS Host Sensor は、リアルタイム解析を行い、CCM などの IP テレフォニー機器に対するセキュリティ攻撃への対応を行います。

図 18
シスコ製品



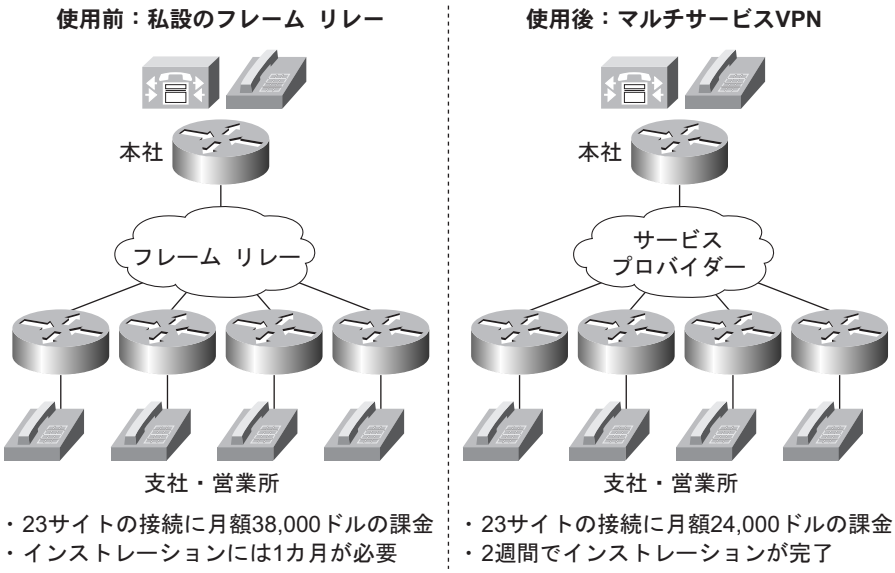
ケーススタディ

次の 2 つのケーススタディは、V^{3}PN ソリューションが専用フレーム リレー WAN ネットワークに代わる低コスト製品を提供し、在宅勤務者に費用効果と生産性の高い作業環境を提供している様子を示したものです。

サイト間 VPN

専用フレーム リレー ネットワークと Cisco V^{3}PN ソリューションを費用面で比較しています。この企業では、繰り返される月々の課金についてコストを大幅に節約できることを認識しました。フレーム リレーの半分の期間でインストールが完了するうえに、1 年につき 168,000 ドル以上の節約となりました（図 19）。

図 19
V^{3}PN サイトツーサイト VPN ケース スタディ



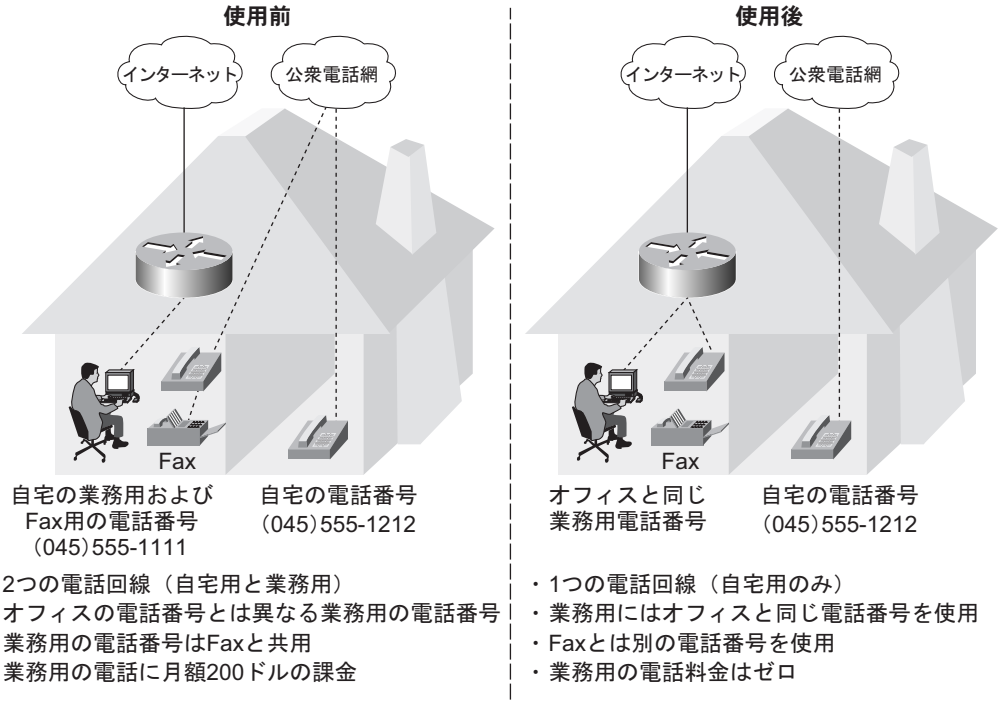
リモート アクセス VPN

SOHO における V^{3}PN ソリューションのコストを算出してみます。

在宅勤務者は、PC にインストールされた VPN Client を使用して企業のデータ ネットワークにアクセスしているとします。ただし、VPN を経由して企業の音声サービスにアクセスすることはできないので、自宅からの電話は面倒なものになっていました。この在宅勤務者の場合、自宅の電話番号のほかに業務用の電話回線を追加して、その料金を支払っています。そのため、2 つの電話番号およびボイス メールボックス（会社にあるものと、自宅のもの）を持ち、これらすべての着信電話をやり繰りする必要があります。業務用の電話回線の基本料金と長距離通話料金により、毎月の総電話料金は 1 カ月あたり約 200 ドルになります。

そこでこの会社は、V^{3}PN ソリューションを導入し、これを IP テレフォニーと統合して、企業オフィスで従業員が利用できるのと同じデータと音声サービスを提供しました。これにより、月々の膨大なビジネス回線と長距離電話料金を節約することができます。また、在宅勤務者は、マルチサービスのサービス プロバイダーからの高速接続へ接続される VPN ルータを利用して、企業ネットワークへの安全な IPSec トンネルを確立しました。この在宅勤務者の IP Phone は、適切な Cisco CallManager の IP PBX（構内交換機）に登録され、割り当てられた企業電話番号でプロファイルを受信して、すべてのスピード ダイヤルや企業ディレクトリを利用できます。この在宅勤務者の生産性は、企業のオフィスにいる人々と同等になったうえに、会社のコストは大幅に低下しました（図 20 参照）。

図 20
リモート アクセス ケーススタディ



まとめ

IP テレフォニーと IPSec VPN 両方に対してエンドツーエンドでの製品およびアーキテクチャを提供するシスコは、V^3PN ソリューションによる統合型ネットワーク ソリューションを提供するうえでの地位を確かなものにしています。シスコが開発した V^3PN ソリューションを配置することにより、企業 LAN だけでなくサービス プロバイダー ネットワークでのコンポーネントとテクノロジーのインターオペラビリティが保証され、統一されたネットワーク デザイン ガイダンスとサポートが提供されます。

参考資料

セキュア コネクティビティ ソリューション

http://www.cisco.com/jp/solution/netsol/security/scsol/

SAFE BLUEPRINT — SAFE: VPN IPSec Virtual Private Networks in Depth（英語）

http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a00801dca2d.shtml

シスコシステムズ株式会社

URL: http://www.cisco.com/jp/
問合せ URL: http://www.cisco.com/jp/go/contactcenter/
〒 107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館
TEL: 03-6670-2992
電話でのお問合せは、 以下の時間帯で受付けております。
平日 10:00 ～ 12:00 および 13:00 ～ 17:00

お問合せ先

05.04