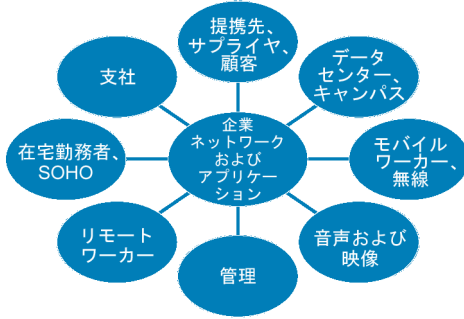


セキュアコネクティビティに求められているものとは？

通信における機密性を確保することは、今日のビジネスに不可欠です(図1)。企業がインターネットの柔軟性と効率を利用して、自社のネットワークを支社、在宅勤務者、顧客、提携先へと拡張するにつれて、セキュリティが最重要課題となります。企業は外部との通信、そして内部の有線無線のインフラストラクチャ上で送信される情報を保護する必要があります。同様に、既存のネットワークインフラストラクチャを使用して新しくビジネスを強化するようなサービスを提供する場合には、音声およびビデオも保護する必要があります。

内外の通信におけるプライバシーを保護できなかった場合には、企業の機密情報やユーザ記録が危険にさらされて企業の評判に傷がつき、新しいビジネス構想に迅速に対応できなくなるかもしれません。

図1 すべての通信におけるプライバシーの保護



ビジネスが直面する問題とは？

現在多くのビジネスが直面しているジレンマは、すべての情報のプライバシーと完全性を維持しつつ、生産性を高め、新しいビジネスアプリケーションを使用可能にし、ビジネス効率を向上させるような、管理しやすい通信インフラストラクチャを効率的に構築することにあります。さらに、多くの企業は、政府や産業規制により情報のプライバシーを保護するよう求められています。オーバーレイソリューションを採用すれば、一部の要件を満たすことは可能であっても、柔軟性が制限されて管理的な負担が生じ、費用が増大する可能性もあります。

シスコのセキュアコネクティビティソリューション

シスコシステムズのセキュアコネクティビティソリューションは、企業のアプリケーションおよびネットワークアクセスをリモートオフィス、モバイルユーザ、提携先に拡張する場合も、あるいは統合型IPソリューションを導入する場合も、すべての通信の機密性と完全性を保証します。シスコのセキュアコネクティビティソリューションは、ネットワークのセキュリティ体制を劇的に向上させるものであり、自己防衛型ネットワークには不可欠の要素です(図2)。

図2 シスコによるセキュアコネクティビティの技術



サイト間VPN — サイト間VPNは、専用線やフレームリレーなど従来のWANサービスに代わる費用効果の高いサービスで、支社、ホームオフィス、またはビジネスパートナーのサイトを会社のネットワークに接続します。サイト間VPNソリューションは複数のプロトコルをサポートし、ネットワークの柔軟性とスケーラビリティを大幅に向上させます。このソリューションには次のようなものが含まれます。

Cisco IOS® VPN セキュリティルーター — Cisco IOS ソフトウェアが動作する、業界でもっとも広く使用され、さまざまなVPNソリューションに対応可能な製品ファミリーです。Cisco IOS ソフトウェアの使用により、企業は、非常に複雑なトポロジーであっても簡単に、安全な接続を確保して、拡張することができます。また、Cisco IOS 拡張セキュリティフィーチャセットは、豊富なVPN機能、ステートフルファイアウォール、侵入保護に加えて、Quality of Service (QoS; サービス品質)、マルチプロトコル、マルチキャスト、アドバンスドルーティングをサポートします。Dynamic Multipoint VPN (DMVPN) やCisco Easy VPN独自のポリシー/コンフィギュレーションブッシュ機能などの先進機能により、少ない設定内容で、配置が大幅に簡略化されます。

Cisco PIX® セキュリティ アプライアンス — このアプライアンスは、ネットワークセキュリティサービス(ステートフルインスペクションファイアウォール、プロトコルおよびアプリケーションの細部におよぶ検査)、インライン侵入保護、マルチメディアおよび音声セキュリティをサイト間VPNおよびリモートアクセスVPNと融合させたものです。配置が容易なこのアプライアンスは、強力な多層の防御を優れた価格と性能で提供します。

Cisco Catalyst® 6500 シリーズ スイッチ — IP Security (IPSec) VPN サービスモジュールが、高性能でスケーラブルなVPNのスループットをCisco Catalyst 6500 シリーズスイッチ上で提供します。これにより、安全な接続をスイッチングインフラストラクチャに統合することが可能となり、データセンターやキャンパス全体に費用効果の高いセキュリティを提供します。

リモートアクセスVPN — モバイルワーカーやリモートワーカー、および提携先は、ISPのダイヤルインフラストラクチャまたはブロードバンド通信を使用して、安全に企業のリソースに接続することができます。Cisco VPN 3000 シリーズ コンセントレータは、IPSec およびクライアントレス Secure Sockets Layer (SSL) 接続を同時にサポートする、高性能かつスケーラブルで柔軟なソリューションを提供します。

セキュアワイヤレス — Cisco ワイヤレスセキュリティスイートは、Cisco Structured-Wireless Aware Network (SWAN) フレームワークを介して総合エンドツーエンドの無線ネットワークを提供します。有線ネットワークと無線ネットワークを統合することにより、業界の先端を行くセキュリティ、管理性、スケーラビリティ、信頼性を実現し、ビジネスに不可欠なインフラストラクチャやデータを保護します。

セキュアIPコミュニケーション — Cisco IP コミュニケーションは、IPテレフォニー、統合メッセージング、IPビデオ/音声会議、IPビデオ配信、コンタクトセンターのためのソリューションを安全に提供します。Cisco IP テレフォニーソリューション固有のセキュリティ機能を、シスコのルーティング、スイッチング、セキュリティの機器による安全なサービス差別化機能と統合することにより、企業はプライバシーを維持しながら、効率と生産性を高めるコンパジドソリューションを配置することが可能になります。

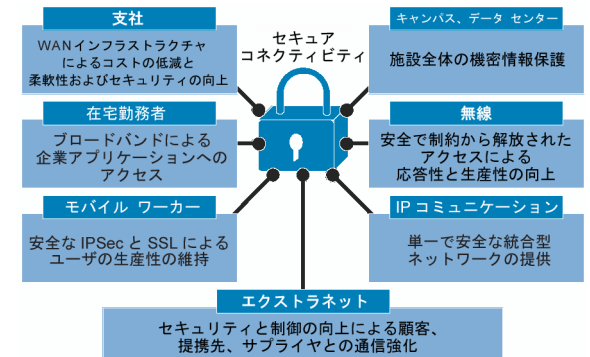
セキュリティ管理と監視 — 管理システムは、セキュリティサービスと監視アクティビティを、効率かつ安全に提供する必要があります。制御と運用の可視性は、グラフィカルデバイスマネージャを使用しても、CiscoWorks VPN/Security Management Solution (VMS) や Cisco IP Solution Center (ISC) などのシステムレベル管理プラットフォームを使用しても、同様に保証されます。

セキュアコネクティビティによる利益とは？

規模にかかわらず、すべてのビジネスにおいてインターネットの偏在性と効率を十分に活用したサービス提供が可能になります。そして、変化の激しい今日の接続要件にも迅速に適應できるようになります(図3)。セキュリティをネットワークのファブリックと統合することにより、シスコのセキュアコネクティビティソリューションは次の利点を提供します。

- 費用を抑えながら、柔軟性と応答性を高めます。
- 使用負担を軽減し、一元化された管理およびポリシー実施による制御を強化します。
- 既存のインフラストラクチャおよび知識ベースを使用することにより、Total Cost of Ownership (TCO; 総所有コスト) を削減します。
- 生産性およびビジネス効率の向上により利益率を向上させます。

図3 セキュアコネクティビティによるビジネスの強化



シスコのセキュアコネクティビティソリューションを選ぶ理由

シスコのセキュアコネクティビティソリューションを使用することで、内外の通信のプライバシー、完全性、耐障害性を高い費用効果で確保しながら、応答性、生産性、ビジネス効率を低い使用負担とTCOで強化することができます。包括的なシスコのセキュアコネクティビティソリューションは、どのようなユーザ環境でも安全なサイト間、リモートアクセス、エクストラネット、音声、映像、無線のすべてをサポートします。

詳細については、次のURLにアクセスしてください。

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

© 2005 Cisco Systems, Inc. All rights reserved.

Cisco, Cisco Systems, および Cisco ロゴは米国およびその他の国における Cisco Systems, Inc. の商標または登録商標です。この文書で説明した商品、サービスはすべて、それぞれの所有者の商標、サービスマーク、登録商標、登録サービスマークです。この資料に記載された仕様は予告なく変更する場合があります。