

シスコの自己防衛型ネットワークによる 情報漏洩 / データ盗難の防止

概要

多くの企業では、データセンター、外出中の社員、および業務上のパートナーにまで自社のネットワークを広げ、アクセスの利便性によって生産性を向上させています。しかし、このように多様な接続が使用されるようになると、重要な情報資産が盗まれる危険性が高まります。社員や信頼している部内者が情報漏洩 / データ盗難に（場合によっては、無意識のうちに）加担している場合さえ少なくありません。シスコシステムズの独自の統合化セキュリティソリューションでは、既存のコンピューティング、ネットワーク、およびセキュリティプラットフォームを使用して、外部および内部からの情報漏洩 / データ盗難から企業を保護することができます。

セキュリティの展望

コンピュータとネットワークの技術によって、企業経営は効率化され、より効果的な顧客サービスが可能になっています。しかし、業務ネットワークのモビリティが向上し、アクセスが容易になるにつれて、セキュリティ上の課題も増えています。ワイヤレス ネットワーキング、社員のリモート アクセス、および在宅勤務の普及によって、悪意のあるユーザやコードがネットワークに侵入する入り口が増えています。

ネットワーク セキュリティは新しい分野であるため、有能なセキュリティ専門家を見つけるのは容易ではありません。企業はセキュリティ費用を捻出できず苦勞する場合があります。通常、ネットワークや IT に関する費用は Return On Investment (ROI; 投資対効果) に基づいて正当化されますが、ネットワーク セキュリティは従来からコスト センターとみなされてきました。しかし、ネットワーク インフラストラクチャ上での業務を安全かつ効率的に遂行するためには優れたネットワーク セキュリティが必要であることを、どの企業も認識し始めています。長期的には、ネットワーク セキュリティは企業の経費節減につながります。

情報漏洩 / データ盗難における課題

企業の場合、多くの窃盗には企業の知的財産が含まれており、競合他社に売って利益を得るために盗まれます。ある企業からの報告^{*}によると、セキュリティ関連の金銭的損失の最も大きな要因は機密情報の盗用で、平均的な被害額は 1 件あたり 270 万ドルに上ります。また、社員の社会保障番号や顧客のクレジット情報などの ID 情報も狙われます。最近の研究では、調査の対象となった顧客の 70 パーセント以上が、銀行口座番号、社会保障番号、およびクレジット カード情報の盗用に不安を抱えています^{**}。

盗用はさまざまな方法で行われます。社外にいるハッカーがネットワークの防御を破って侵入しようとするかもしれません。また、社員の後ろについてビルに忍び込み、コンピュータを使用して情報を盗もうとするかもしれません。社員、請負業者、ビジネス パートナーなどの信頼している人々が利益を得るために、または復讐のために情報を盗む場合もあります。業界レポートによると、情報システムへの不正アクセスの 70 パーセント、および経済的な損失をもたらした侵入の少なくとも 95 パーセントは社員によるものです^{*}。企業はこれらの各ケースに対する予測と防御を継続的かつ組織的に実施する必要があります。

* 出典：CSI/FBI Security Study、2003

** 出典：Gartner Research、2004

情報漏洩 / データ盗難を防止するために、企業は暗黙的な信頼ではなく、明示的な信頼に基づく新しいセキュリティ パラダイムに適応する必要があります。今後は、すべての社員をネットワーク上で信頼できるユーザとみなすことはできません。ユーザの信頼性に関するこの新しい考え方を実行するために、企業は次の内容を実施する必要があります。

- 企業の正式なセキュリティ ポリシーを作成し順守する
- 信頼できるユーザであることを確認する
- 信頼できる認証済みユーザにアクセス権限を与える
- ネットワークのエンドポイント（デスクトップ、サーバ、およびラップトップなど）を侵入から保護する
- 内部および外部の攻撃からネットワーク リソースを保護する（ルータ、スイッチ、およびワイヤレス アクセス ポイントなど）
- データ伝送と音声通信を保護し、信頼できるユーザのプライバシーと機密性を確保できるようにする

シスコの自己防衛型ネットワーク戦略

多くの場合、情報漏洩 / データ盗難はネットワークやセキュリティの管理スタッフが気づかないうちに行われます。ネットワークに疑わしい動作があれば、セキュリティ システムが迅速かつ自動的に対応しなければなりません。そのためには、ネットワークおよびネットワークの管理者が疑わしい動作の事前認識、脅威が実際に存在するかどうかの識別、および情報漏洩 / データ盗難への適切で迅速な対処を行うことができるように、ネットワークのあらゆる部分に完全に統合されたセキュリティ システムが必要です。シスコの自己防衛型ネットワーク戦略では、情報漏洩 / データ盗難からの総合的な保護の枠組みが明確に示されています。企業は、ルーティング、スイッチング、ワイヤレス、およびセキュリティ プラットフォームにおける既存の投資を活用して、自己防衛型ネットワークを展開することができます。自己防衛型ネットワークは、企業の内部および外部からのセキュリティ上の脅威の識別、防御、および対応を行う上で役立ちます。ネットワーキングとセキュリティの技術とサービスをインテリジェントに連携させて、業務上のセキュリティに関する独自のシステムティックな方法を提供しているのはシスコだけです。

シスコの自己防衛型ネットワーク戦略は、3 つの分野で構成されており、それぞれに固有の狙いがあります（図 1）。これらのシステムが一体となって、企業情報の盗用を発見し阻止します。

図 1 シスコの自己防衛型ネットワークのコンポーネント



シスコのセキュア コネクティビティ システム

すべての企業において、プライバシーは重要な懸案事項です。ユーザは、電話やコンピュータによる通信の内容はプライベートなもので、他人に許可なく内容を覗かれたくないと考えています。シスコのセキュア コネクティビティ システムでは、Virtual Private Network (VPN; 仮想私設網) を使用して、パブリック ネットワークやプライベート ネットワークを流れる情報の完全性と機密性を保護することにより、データ、ビデオ、および Voice over IP (VoIP) 通信の盗用を阻止します。

シスコの攻撃防御システム

ネットワークは外部と内部の両方の攻撃に耐えられるように設計する必要があります。情報漏洩/データ盗難を防ぐために、シスコの攻撃防御システムは、デスクトップやサーバなどのエンドポイントを対象とする不正な活動を防止し、ネットワーク上の任意の場所における疑わしい動作の検出、特定、および阻止を行います。

シスコの信頼性およびアイデンティティ管理システム

ネットワーク インフラストラクチャにおける最初の防御ラインは、ネットワークにアクセスしているユーザまたはデバイスの特定、アクセスしているデバイスの状態の把握、およびリソース権限の識別です。シスコの信頼性およびアイデンティティ管理システムは、信頼できるユーザおよび信頼できるデバイスのみを企業のネットワークに接続させ、信頼できるユーザおよびリソースにアクセス許可された情報だけを取得させることによって、情報漏洩/データ盗難を防止します。

外部からの情報漏洩/データ盗難の防止

情報漏洩/データ盗難は最近に始まったことではありません。しかし、インターネットが高度に発展したため、企業の外部から情報が盗み出される場合があります。企業やネットワークの外部および内部から情報を盗む方法は数多く存在します。たとえば、ハッカーは「man-in-the-middle」攻撃として知られる方法を用いて、パブリック ネットワークを流れる情報を傍受することができます。あるいは、悪意のあるソフトウェアを使用して企業のコンピュータに侵入し、サーバやデスクトップへの「バックドア」を仕掛けることもできます。キャンパス環境にワイヤレス LAN が普及したため、ハッカーは企業の建物の外をうろついて保護されていないワイヤレス アクセス ポイントを探し出すこともできます。シスコの統合化セキュリティ ソリューションを使用すると、企業の外部にいるハッカーからネットワークを多面的に保護することができます。

信頼性のあるユーザおよびアクセス権限の確認

ネットワーク 環境を保護するために最初に行う べきことは、ユーザのアイデンティティ および接続権限の確認です。シスコの信頼性およびアイデンティティ 管理システムでは、Cisco Catalyst[®] スイッチおよびルータに統合されている 802.1X や Authentication, Authorization, and Accounting (AAA; 認証、許可、アカウントリング) 機能などの標準的な認証プロトコルと認証技術を使用して、ユーザのアイデンティティを確認します。ユーザのアイデンティティが確認されると、アクセス権限が付与されます。Cisco Secure Access Control Server (ACS) は、ネットワーク アクセスのポリシー制御を行います。Cisco Secure ACS を使用すると、ネットワーク管理者は、ネットワーク セグメントにアクセス可能なユーザの限定、ユーザおよびユーザグループに許可するネットワーク サービスの制限、およびネットワーク内での全ユーザの行動の記録ができます。

信頼性のあるデバイスの確認

ネットワークにアクセスする前に、デバイスがエンドポイントのセキュリティ ポリシーに適合していることを確認する必要があります。シスコの Network Admission Control (NAC) ソリューションでは、デバイスのシステム ステータスがセキュリティ ポリシーと比較されます。Trend Micro 社や IBM 社などの業界のパートナーと連携することにより、ネットワークはエンドポイントが設定されたセキュリティ ポリシーに適合しているかどうかを判別し、エンドポイントのネットワーク アクセスの可否をインテリジェントに判断します。

機密情報を伝送するパブリック ネットワークの保護

リモート アクセスと在宅勤務は企業の生産性向上に役立ちますが、ネットワーク運用スタッフはパブリック ネットワークから企業のネットワークへアクセスできるようにしなければなりません。シスコのセキュア コネクティビティ システムは、保護されていないネットワークを経由して伝送される情報のプライバシーを確保できるようにします。

Cisco Remote Access VPN ソリューションは、Secure Socket Layer (SSL) や IP Security (IPSec) の規格を使用して、ブランチ オフィスや離れた場所にいる社員の所まで保護された企業ネットワークを拡張します。これらのソリューションでは、セキュリティ レベルの最も高いユーザ認証とデータ暗号化規格が使用されているため、正当なユーザだけがネットワークにアクセスできます。たとえ誰かに通信を傍受されても、データは判読できません。

幅広い OS に対応したソフトウェア アプリケーションである Cisco VPN Client を使用すると、リモート アクセス VPN (E コマース、モバイル ユーザ、および在宅勤務アプリケーションを含む) のセキュアな接続を実現できます。Cisco VPN Client は、シスコ製ルータ、Cisco VPN 3000 シリーズ コンセントレータ、および Cisco PIX[®] セキュリティ アプライアンスなどのシスコのヘッドエンド プラットフォームでサポートされています。

ハッカーの侵入の防止

一般的に、ハッカーは企業のネットワークにアクセスする前に、企業のネットワークをスキャンして脆弱な入り口やデバイスを探します。次に、ハッカーは一般的なアプリケーションのトラフィック (Web アプリケーションの HTTP トラフィックなど) に変更を加えてネットワークに侵入しようとします。ネットワークベースの Intrusion Detection System (IDS; 侵入検知システム) および Intrusion Prevention System (IPS; 侵入防御システム) は、ネットワークを流れるすべてのトラフィックを分析し、スキャン行為の発見、攻撃パターンの識別、および脅威の抑制処置を行います。これによって、ハッカーのネットワークへの侵入が阻止されます。

シスコの総合的な IPS ソリューション ファミリーには、ルータ、スイッチ、およびワイヤレス アクセス ポイントに組み込まれたソフトウェア機能、Cisco Catalyst スwitch の高性能な専用ハードウェア モジュール、およびスタンドアロン型の強力なアプライアンスなどがあります。シスコの IPS ソリューションを使用すると、小規模オフィス、ブランチ オフィス、および企業ネットワークでの脅威に対する優れた防御を実現できます。

無線の保護

企業はキャンパス ネットワーキング環境での利便性と費用対効果の高いソリューションとしてワイヤレス LAN を使用しています。残念なことに、ワイヤレス ネットワークへのアクセスは容易です。大半のワイヤレス ネットワークは 802.1X によるユーザ認証を行い、スタティックなデータ暗号化を使用してワイヤレス ネットワークを保護していますが、それでも一般的なセキュリティ侵害がいくつか存在します。

ワイヤレス アクセス ポイントが、故意または無知にかかわらず、正しく設置されていないために、認証されていないユーザにネットワーク アクセスが許可される場合があります。このような「不正な」アクセス ポイントは、Cisco Structured Wireless Aware Network (SWAN) アーキテクチャ内の IDS に類似した機能を使用すればすぐに発見できます。Cisco SWAN はアクセス ポイントおよび Cisco Catalyst 6500 シリーズ モジュールに組み込まれています。Cisco SWAN では、不正なアクセス ポイントの場所が正確に特定されるため、ネットワーク管理者はそれを容易に発見して無効にすることができます。

現在使用されているワイヤレスのスタティックな暗号鍵は、一般に入手可能なハッキング ツールを使用して破ることができます。シスコのワイヤレス ソリューションは、一時鍵による暗号化ソリューションを組み込んだ Wi-Fi Protected Access (WPA) 業界標準を使用しています。シスコのワイヤレス ソリューションを使用すると、有線ネットワークと同等な安全性が確保されたワイヤレス ネットワークを実現できます。Cisco SWAN および Cisco Catalyst 6500 シリーズ スイッチでは、有線ネットワークとワイヤレス ネットワークは一体化されており、セキュリティも万全です。これらを使用すると、設定、管理、およびセキュリティ ポリシーの適用を容易に行うことができます。

内部からの情報漏洩 / データ盗難の防止

多くの企業は、建物の警備に相当な金額を費やしています。ドアの鍵、カードキーの許可証、さらには監視カメラや警備員などがその例です。これらは多くの侵入者を思いとどまらせていますが、こうした防御を破って建物内に侵入する者もいます。ただ単に社員のあとを付いてきて防御をかいくぐる場合もよくあります。情報漏洩 / データ盗難が社員や信頼できる内部者によって行われる場合もあります。多層構造の防御システムを使用すれば、許可されていない社員、請負業者、または訪問者が企業の情報にアクセスして盗み出すのを効果的に防ぐことができます。

セキュリティ「アイランド」の構築

ネットワークを外部の不正侵入者から保護する上で、ファイアウォールは不可欠です。ファイアウォールはネットワークセキュリティとして重要な役割を担っています。ファイアウォールはネットワークグループ間にある施錠されたドアとカードキーによるアクセスにあたる機能であり、ネットワーク内にセキュリティ「アイランド」を構築します。ファイアウォールによって、あるグループのユーザが他のネットワークグループのリソースにアクセスするのを防ぐことができます。たとえば、エクストラネット上のパートナーとサプライヤが、財務部門、人事部門、および経理部門にある機密情報にアクセスできないようにすることができます。

シスコは完全なファイアウォール機能を業界で最も幅広く揃えており、あらゆる規模のネットワークに対応できます。ファイアウォール機能はすべてのシスコ製ルータと Catalyst スイッチに組み込まれています。高性能な処理を必要とする用途向けには、Cisco Catalyst スイッチ用のファイアウォールハードウェアモジュールが用意されています。Cisco PIX セキュリティアプライアンスで提供される強力なスタンドアロン型のファイアウォールファミリーは、ホームオフィス、ブランチオフィス、キャンパス、およびデータセンター環境を保護します。

ユーザワークグループの保護

シスコの信頼性およびアイデンティティ管理システムソリューションでは、ユーザがいる場所ではなくユーザのアイデンティティに基づいてユーザをワークグループまたは VLAN（仮想 LAN）にセグメント化できます。たとえば、キャンパスおよびブランチオフィスのなかで、自社のセキュリティを犠牲にせずに訪問者にもインターネットアクセスを提供したいと考えます。ネットワークの運用スタッフは、訪問者を企業ネットワークの他の部分から区切り、インターネットアクセスだけを付与できるように、Guest VLAN を構築* することができます。VLAN を使用して組織上の機能を区切ることもできます。たとえば、マーケティング VLAN 上にあるマーケティングサーバへアクセスできるのは、マーケティングスタッフとして認証および識別されたユーザだけになります。VLAN 機能はすべての Cisco Catalyst スイッチに内蔵されています。

* 対応機種については、各 Catalyst スイッチの製品資料を参照してください。

スパイ、スヌーピング、およびスプーフィングの防止

有効な認証およびログインアクセスを持つ信頼性のある社員が、一般に入手可能なソフトウェアを使用して、ネットワーク上を流れる社員データ（IP フォンの通話やパスワードなど）を「スパイ」する場合があります。また、ワームや「トロイの木馬」型アプリケーションを介して不正なアプリケーションがデスクトップ、ラップトップ、およびサーバに追加され、パスワード、アカウント番号、および社員情報などの企業情報が盗まれる場合もあります。ツールによっては、ネットワークをだましてユーザ A がユーザ B に「なりすまし」、ユーザ A がユーザ B の情報にアクセスすることもできます。Cisco Catalyst シリーズの統合化セキュリティ機能には、こうした攻撃から防御するための幅広いセキュリティメカニズムが組み込まれています。情報漏洩/データ盗難を防ぐことができ、また、すでに情報漏洩/データ盗難が進行中の場合には、それを迅速に抑止できます。Cisco Catalyst シリーズの統合化セキュリティ機能は、Cisco Catalyst スイッチ内で使用できるソフトウェアフィッチャセットです。また、Cisco Security Agent (CSA) は、企業内のホストシステムに存在するスパイウェアを抑制します。CSA を使用すると、キーボードの「フッキング」やネットワーク外への接続などの、侵入動作を行うダウンロード済みおよびインストール済みのアプリケーションだけでなく、システム上にダウンロードおよびインストールされるすべてのソフトウェアがユーザに通知されます。Cisco Catalyst シリーズの統合化セキュリティ機能や CSA などのソリューションは、今日の企業において最も一般的に見られる悪意のあるアクティビティを抑制できます。

ネットワークのセキュリティ状態の監視と管理

大規模な分散型ネットワークでは、すべてのネットワークデバイス、セキュリティデバイス、およびセキュリティサービスの統合監視を使用して、IT スタッフはネットワークを効率的に監視できます。

CiscoWorks VPN/Security Management Solution (VMS) では、VPN、ファイアウォール、ネットワーク IPS、およびホスト IPS の設定、監視、およびトラブルシューティングを一元的に行う Web ベースのツールが統合されているため、企業の生産性向上につながります。ルールおよび設定をネットワーク全体に適用できるため、ネットワーク全体でのセキュリティポリシーの展開が大幅に簡素化されます。

シスコの自己防衛型ネットワークによる情報漏洩 / データ盗難の防止

情報漏洩 / データ盗難は企業にとって最も被害の大きいセキュリティ侵害です。米国内で 2003 年に発生した事件の 1 件あたりの被害額は平均で 270 万ドルに上ると報告されています*。世界全体で見ただけの被害総額は、はるかに大きくなります。セキュリティ侵害による被害は、生産性の低下から金銭的な損失まで広い範囲に及びます。

情報漏洩 / データ盗難の多くは社内内で発生しているため、企業はネットワークの内部と外部の両方を保護する必要があります。シスコの統合化セキュリティ ソリューションを使用すると、企業は既存のネットワーク インフラストラクチャと人材投資を最大限に活用して、自己防衛型ネットワークを構築することができます。シスコの自己防衛型ネットワークはネットワークにセキュリティ機能を統合し、既存のネットワーク インフラストラクチャを活用し、Total Cost of Ownership (TCO; 総所有コスト) を抑えながら企業の資産を保護します。運用スタッフは、ネットワーク上にいるユーザ、ユーザの所在地、およびユーザがアクセスしようとしている情報を把握できるようになるため、ネットワーク化された組織の効率化と生産性向上により多くの時間を使えるようになります。

シスコはネットワーキングおよびセキュリティ ソリューションにおける業界トップの企業です。ネットワーキングとセキュリティの技術とサービスをインテリジェントに連携させて、業務上のセキュリティに関する独自のシステムティックな方法を提供しているのはシスコだけです。セキュア コネクティビティ、攻撃防御、および信頼性およびアイデンティティ管理によって構成されるソリューションの 3 本柱に基づいて、シスコは幅広い統合化セキュリティ ソリューションを提供し、情報漏洩 / データ盗難からあらゆる規模の企業を保護します。

情報漏洩 / データ盗難からの企業の保護およびシスコの自己防衛型ネットワーク戦略の詳細については、<http://www.cisco.com/jp/solution/netsol/security/> を参照してください。

* 出典 : 2004 CSI/FBI Computer Crime and Security Survey

©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。



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