ソリューション概要

シスコが提唱する自己防衛型ネットワーク

コンピュータ技術の進歩に伴い、企業のコミュニケーションやデータストレージにもコンピュータネットワークがますます重要になっています。しかし、ハッカーによる不正侵入が氾濫し、感染力および破壊力の強いウィルスが次々に出現している現在、必要なときに確実にネットワークを使用できるようにするには、どうすればよいのでしょうか？

ネットワーク セキュリティ強化の必要性

ネットワークは、さまざまな情報をオープンにすることを目的に設計されました。ネットワークのセキュリティについては、考慮されてはいましたが、最大の関心事ではありませんでした。1990年代に入るまで、ネットワーク セキュリティとは「物理的な安全」を意味しました。エンド ステーション、ネットワーク サーバ、およびメインフレームが警備された建物内に設置されている限り、ネットワークは安全とされていたのです。

1990年代初め、企業はインターネットへの接続を開始しました。この変化は、ネットワーク セキュリティに新たな弱点を発生させることになりました。建物のドアに鍵をかけるだけでは、ネットワークを保護できなくなり、企業はネットワーク セキュリティに関する新たな技術とポリシーを模索し始めました。

外部との接続については、ファイアウォールおよびネットワーク ポリシーを使用し、ネットワークの境界を防衛しました。これらのデバイスやポリシーは、ビジネスに不可欠なアクセス性を保持しながら、内部ネットワークを保護できるように設計されました。しかし、Slammer、SoBig、MSBlasterといった高度なウィルスやワームの出現によって、これらのポリシーではネットワークを十分に保護できなくなってきました。

内部ネットワークのセキュリティは、大半がユーザIDおよびパスワードに基づくもので、アプリケーションの保護機能の一部として組み込まれました。このころの社員のコンピュータは一般にデスクトップ型で、ネットワーク上では「信頼できる」存在だったのです。ところが、ノート型コンピュータが登場し、急速に普及しました。ノート型コンピュータは生産性を向上させましたが、同時にリスクも増大させました。「内部」のネットワークと「外部」のネットワークとの間を行き来する社員は、知らないうちにウィルスやワームに感染している可能性があります。そうなれば、ネットワーク境界からの侵入と同様に、重要なビジネス アプリケーションの基盤が破壊される危険があります。また、内部の人間による攻撃も増加しました。現在、企業で発生しているネットワーク セキュリティ違反の半数以上は、不満を抱く社員がウィルスを投入したり、恨みを持つ社員がネットワークに不法侵入するといった内部の犯行によるものです。

さらに、ワイヤレス ネットワーキングの普及により、社員が安全性に問題のあるワイヤレス アクセス ポイントを社内に持ち込んで利用するようになり、攻撃者に新たな入口を提供する結果となりました。

このような状況の変化を考えれば、従来のネットワーク セキュリティ モデルでは、現在のネットワークを十分に保護できないことは明らかです。

侵入手段の多様性

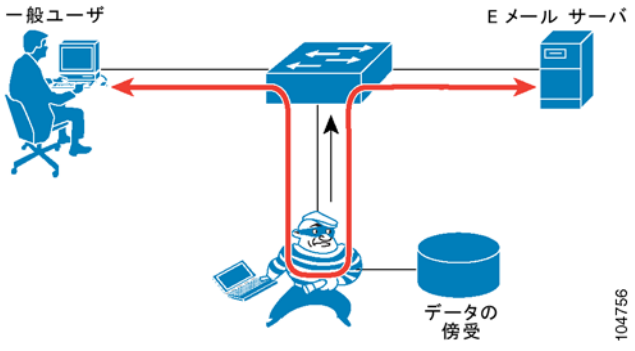
インターネットが出現しはじめた当初は、ネットワークを攻撃するには、きわめて高度な知識とスキルが必要でした。当然ながら、このような専門知識を持つ人間はごく少数だったので、攻撃の数もそれほど多くはありませんでした。

しかし現在では、スキルをもったハッカーは何倍にも増え、インターネットには、使いにくさはあるものの、各種のハッキング ツールが出回っています。もちろん、これらのツールにはネットワークの仕組みが利用されてはいますが、初心者でも簡単に使うことができるようになっています。これにより、ネットワークのリスクは著しく増加しました。

危険性の高い攻撃のタイプをいくつか紹介します。

- man-in-the-middle 攻撃 — MAC アドレスまたは IP アドレスなどの識別子を偽って、不正デバイスがゲートウェイなどのネットワーク デバイスに「なりすます」攻撃です。正規デバイス宛てのトラフィックは、すべて不正デバイスに送信され、侵入者は、パスワードやアドレスなどの情報が含まれたパケットを読み取ることができます。
- Denial of Service（DoS）攻撃 — ネットワークへのアクセスを取得した不正デバイス、または感染した正規デバイスが発信したトラフィックでネットワークが溢れ、ゲートウェイなどの主要デバイスが正規リクエストに応答できない状態になる攻撃です。DoS攻撃は、ネットワーク サーバなどに対して集中的にしかけられることもあります。この場合、ネットワーク全体にトラフィックが溢れることはありませんが、特定のデバイスが過負荷となり、サービス不能状態となります。また、Distributed Denial of Service（DDoS）攻撃という新しいタイプの攻撃では、ネットワーク上の複数のデバイスから同時にDoS攻撃が開始され、さらに大きな被害をもたらします。
- MACベースの攻撃 — man-in-the-middle攻撃と同様に、正規のトラフィックにアクセスして情報を盗む目的で使用されます。プログラムまたはスプリクトを使ってスイッチのアドレス テーブルを満杯にし、スイッチがアドレスを学習できないようにします。すると、トラフィックはスイッチ上の全ポートにフラッディングされる結果となり、ハッカーのパケット傍受を簡単にします。また、「macof」などのツールでMACフラッディングを発生させた場合には、DoS攻撃と同じ効果があります。

図1 man-in-the-middle攻撃



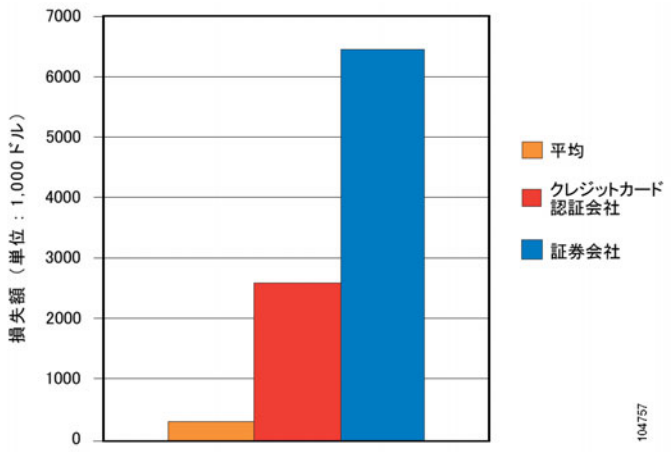
ダウンタイムによる多大な損害

これらの攻撃は、単純に迷惑だというだけではありません。ネットワークの停止、機密情報の漏洩、企業の収益とパフォーマンスの低下といった問題を引き起こします。現在の攻撃は、以前よりもはるかに急速に進行するので、より大きな被害が発生します。

1980年代から1990年代ごろのネットワーク管理者は、何日間または何週間もかけて、特定の攻撃に対する戦略を開発していました。2000年から2002年にかけて、ウィルスやワームの性能が高くなると、数時間のうちに対応しなければならなくなりました。現在では、ネットワーク管理者は、わずか数秒間で攻撃に対応する必要があります。たとえば、最近のSQL Slammerワームは8.5秒ごとに倍増します。3分あれば実行されるスキャンの数は1秒に5,500万回となり、わずか1分で1 Gbpsのリンクが停止します。

攻撃によって、ネットワークのデータ センターが1時間ダウンした場合、どうなるでしょうか。Meta Groupによれば、データセンター アプリケーションのダウンタイム1時間当たりの平均損失額は、33万ドルです。Strategic Research Corporationは、それがクレジットカード認証会社のデータセンターであれば、損失額は260万ドルに及ぶと発表しています。さらに、証券会社のデータ センターならば、650万ドルもの損害が発生します。

図2　データ センターのダウンタイムによる損失



また、新しいプライバシー保護法では、ネットワークから機密情報が第三者の手に渡った場合、厳しい刑罰の対象になります。たとえば、Health Insurance Portability and Accountability Act（HIPAA;医療保険のポータビリティと説明責任に関する法律）では、医療に関する電子機密情報のセキュリティが守れなかった場合、1回の漏洩に対して、最高25万ドルの罰金または5年間の懲役が課せられます。

自分には起きるはずはない

自社にはそのような損害が起きるはずがないと考えたいとしても、統計を調べれば、これが誤った判断であることは明らかです。2002年にCSI/FBIが企業400社を対象に行ったコンピュータ犯罪およびセキュリティに関する調査では、全企業の90%以上に何らかのセキュリティ違反があると報告されています。推定損失は総額で4億5,500万ドルを超えます。機密情報の漏洩だけで1億7,000万ドルの損害に達しており、回答企業の75%が、不満を抱く社内の人間による攻撃の可能性を認めています。

最新の戦略とは

今、企業に必要とされているのが、防御的なネットワーク セキュリティ モデルであることは言うまでもありません。攻撃を防止するには、外部からの侵入を許さず、かつ内部の信頼性を保持できるような包括的なモデルの設計が必要です。

具体的な目標は、次のとおりです。

- 外部ハッカーがネットワークにアクセスできないようにする。
- 認可されたユーザだけがネットワークにアクセスできるようにする。
- 内部ネットワークで、故意または不注意による攻撃を発生させない。
- ユーザのタイプを分類し、それぞれに異なるアクセス権限を提供する。

これらを有効に実施するにはユーザに気づかれず、簡単に管理でき、業務を妨げない方法でセキュリティポリシーを実施する必要があります。

そのためには、次の条件を満たすソリューションが必要です。

- ネットワークのインフラストラクチャに完全に統合されたネットワーク セキュリティ
- ネットワークの保護、攻撃の防止、および自己回復力
- 「誰が」ネットワークにアクセスでき、「何を」実行できるのかの管理

シスコの自己防衛型ネットワーク

シスコの自己防衛型ネットワークは、意図的または不注意による、内部または外部からの破壊性のある攻撃からネットワークを保護するためのシスコ製品および機能です。

シスコの自己防衛型ネットワークは、IPネットワーキングとセキュリティ技術の**コラボレーション**です。そのため、ルーティング、スイッチング、データ、音声、ビデオ、ワイヤレス、ストレージなどのIPサービスを組み合わせたソリューションとなっています。

また、いろいろなプラットフォーム（専用セキュリティデバイス、ルータ ベースのセキュリティ、スイッチ ベースのセキュリティなど）とテクノロジー（ファイアウォール、脅威保護、Authentication, Authorization and Accounting [AAA;認証、許可、アカウンティング]、URLフィルタリング、802.1Xなど）に対する既存の投資を活用して、必要な機能を柔軟に配備できます。

このソリューションは、LAN、ワイヤレスLAN、キャンパス、メトロ、エッジ、サービス プロバイダー、ブランチオフィスを含めたネットワーク全体にわたって、PCおよびサーバなどの全プラットフォームに組み込まれたセキュリティ機能を統合する

ことによって、包括的な戦略を提供します。
シスコの自己防衛型ネットワークには、脅威に対する防衛、信頼できる境界の確立と認証、安全なビジネス コミュニケーションといった主要なセキュリティ課題を達成するためのコンポーネントが統合されています。

- **脅威に対する防衛** — 悪意のある攻撃および不注意による攻撃から、ネットワークを保護します。脅威に対する防衛は、さらに詳細な目標に分けられます。
  - **境界の防衛**:シスコの統合型ファイアウォールやIntrusion Detection System(IDS;侵入検知システム)を使用してネットワーク エッジを強化し、侵入および攻撃から保護します。
  - **内部の保護**:Catalyst® Integrated Security機能を使用して、新しい技術を使った内部攻撃からネットワークを保護します。
  - **エンドポイントの保護**:Cisco Security Agentを使用して、ホストへの感染および損害を未然に防ぎます。
- **信頼性および認証** — ネットワークにアクセスできる人物と、実行できる内容を管理します。これらの管理には、ネットワークへの不正なワイヤレス アクセスを防止できるCisco IdentityおよびCisco Wireless LAN Security Suiteを使用します。
- **安全な接続** — 内部および外部の音声とデータ通信の機密性を保護します。シスコの統合IP Security(IPSec)VPNにより、音声およびデータの保護が提供されます。

また、Quality of Service(QoS;サービス品質)を使用してDoS攻撃を受けた場合のネットワーク アクセスを確保したり、シスコの新しいNetwork Admission Control(NAC)ソリューションを使用して、モバイル ユーザの不注意によるウィルス感染からネットワークを保護するといったことも重要です。

シスコの自己防衛型ネットワークのコンポーネント

シスコの自己防衛型ネットワークには、次のコンポーネントが含まれます。

- シスコの統合ファイアウォール サービスサービス
- シスコの統合型IDS/IPS
- シスコの統合型IPSec VPN
- Catalyst Integrated Security機能
- Cisco Identity
- Cisco Security Agent
- Cisco Wireless Security Suite
- Cisco Structured Wireless-Aware Network(SWAN)

Cisco Catalyst 6500シリーズ スイッチには、シスコの統合ファイアウォール モジュール、統合型IDS/IPSモジュール、統合型IPSec VPNモジュール、Catalyst Integrated Security機能などの数多くのコンポーネントが実装できるため、Catalyst 6500シリーズは統合型セキュリティ プラットフォームの1つとなっています。

シスコの統合ファイアウォール サービスモジュール

ファイアウォールの機能は、時代とともに変化してきました。現在のファイアウォールは、もはや企業ネットワークを外部の不正アクセスから保護するだけではありません。企業ネットワーク内においても、特定のサブネット、ワークグループ、またはLANへの不正アクセスを阻止します。

Cisco Catalyst 6500 Firewall Service Module(FWSM)では、デバイス上の任意のポートをファイアウォール ポートとして設定し、ネットワークのインフラストラクチャにステートフルなファイアウォール セキュリティを統合します。

Cisco PIX®テクノロジーを採用し、Cisco PIX オペレーティングを実装しているシスコのFWSMは、リアルタイム処理が可能な内蔵システムであり、セキュリティ ホールおよびパフォーマンス低下の原因となるオーバーヘッドを削減します。また、主要な保護機能としては、着信トラフィックと発信トラフィックを管理するステートフルなコネクション型ファイアウォール機能を提供します。FWSMは、送信元および宛先のアドレス、ランダムTCPシーケンス番号、ポート番号、および接続の追加TCPフラグに基づいて、各セッションにセキュリティ ポリシーを適用します。

シスコの統合型IDS/IPS

ネットワーク エッジを防御するための戦略は、外部者による侵入を検知し、阻止することです。シスコは、ネットワークへの着信トラフィックをモニタし、疑わしい動作を管理者に通知するIDS製品ラインを完備しています。最新のIDS製品の1つには、Catalyst 6500シリーズに実装できる統合型IDSモジュールがあります。

従来、ネットワーク管理者は、スイッチのSPANポートに外部IDSセンサを接続し、ネットワーク トラフィックをモニタしていました。Catalyst IDSモジュールを搭載すれば、IDS機能がスイッチ本体に統合されるので、スイッチのバックプレーンで直接トラフィックをモニタできます。より詳細なレベルでネットワーク トラフィックにアクセスできるので、SPANポートに外部IDSセンサを接続する場合よりも、制約が少なくなります。

他のCisco IDSネットワーク アプライアンスと共通のコードが使用されているCatalyst IDSモジュールは、広範囲の攻撃を検知します。IDSモジュールのシグニチャ エンジンは、スイッチに影響を与えずに、新しい「ハッカー シグニチャ」があったときには簡単に更新できます。また、IDSモジュールでは、複数のVLAN上のトラフィック(ISL [スイッチ間リンク]および802.1qの両方)を同時にモニタできます。

Catalyst IDSモジュールでは、次のカテゴリの攻撃を検知できます。

- **脆弱性** — ログイン試行の失敗、TCPハイジャックなど、ネットワークへの不正アクセスまたはシステム破壊の可能性のある動作を検知します。
- **DoS攻撃** — Trinoo、TFN、SYNフラッドなど、帯域またはコンピューティング リソースを浪費して正常な運用を妨害しようとする動作を検知します。
- **調査** — ICMPスキャン、ポート スキャンなど、「攻撃チャンス」を判別するためにネットワークを偵察またはマッピングする動作を検知します。この動作は、攻撃者が実際の攻撃をする前に実施されます。
- **不正利用** — コーポレート ポリシーの違反を試みる動作を検知します。これは、ネットワーク トラフィックのなかに特定の文字列がないかを調べるようにセンサを設定することで検知します。

シスコの統合型IPSec VPN

重要な広帯域ビジネス アプリケーションの普及により、大規模な主要オフィスでは、あらゆる場所への接続性と、帯域幅の増大が必要になりました。多数の企業が、新たな接続要件を満たすために、従来のWANをサイト間VPNおよびリモート アクセスVPNに変更したり、これらのVPNをサポートできるようにWANを増強しています。

Cisco Catalyst 6500シリーズ スイッチにVPNを組み込めば、外部デバイスを増設したり、ネットワークを変更することなく、ネットワークの安全性を確保できます。IPSec VPNモジュールでは、ネットワーク サービスに暗号化、認証、および整合性が統合されるので、キャンパス エッジでの安全なVPN終端、Voice over IP（VoIP）やストレージ エリア ネットワークなどの統合ネットワーク サービスを安全に配備できます。

IPSecを統合することによって、専用線またはフレームリレー環境から、コスト効率の良いVPN相互接続にスムーズに移行できます。

Catalyst Integrated Security機能

ファイアウォールの内側からの攻撃に対抗するための新しいセキュリティ機能が、Cisco Catalystスイッチ ファミリーに追加されました。ファイアウォールの内側からの攻撃は、通常、有効なネットワークデバイスのIPアドレスまたはホスト名に「なりすます」ことによって実行されます。Cisco Catalystスイッチに追加された機能は、以下のとおりです。

- ポート セキュリティ
- DHCPスヌーピング
- ダイナミックAddress Resolution Protocol（ARP）検査
- IPソース ガード

ポート セキュリティ

ポート セキュリティでは、MACベースの攻撃を防止できます。ネットワーク管理者は、ポート セキュリティを使用して、許可するMACアドレスまたは最大MACアドレス数をポート単位で制限できます。特定ポート上で許可するMACアドレスは、管理者がスタティックに設定するか、スイッチがダイナミックに学習します。

特定ポート上のMACアドレスが最大数を超えるか、許可されていない送信元MACアドレスのフレームが検出されると、セキュリティ違反が発生します。この場合、ポートがシャットダウンされるか、SNMPトラップが生成されます。ダイナミックまたはスタティックなセキュアMACアドレスについては、ポート セキュリティによって、無動作または定義済みインターバルによるエージングを設定できます。ポート セキュリティによりポートの使用を制限することによって、ポートに指定されていないMACアドレスを持つステーションからのアクセスを阻止できます。

DHCPスヌーピング

侵入者は、ネットワークにDHCPサーバを接続し、そのセグメントに対するDHCPサーバの役割を「代行させる」ことがあります。これにより、偽のDHCP情報を発信して、デフォルトのゲートウェイおよびネーム サーバ（DNSおよびWINS）がハッカーのコンピュータになるようにクライアントの宛先を変更します。宛先を変更することによって、ハッカーはman-in-the-middle攻撃をしかけ、エンド ユーザに気づかれることなく、ユーザ名とパスワードなどの機密情報にアクセスできます。この攻撃を阻止するには、DHCPスヌーピングを使用します。

DHCPスヌーピングは、エンド ユーザに接続している信頼できないスイッチ ポートと、DHCPサーバまたは他のスイッチに接続している信頼できるスイッチ ポートを区別するポート単位のセキュリティ機構で、VLAN単位で有効化できます。

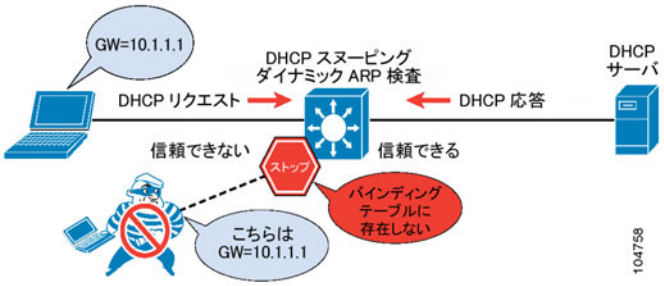
DHCPスヌーピングを使用すると、DHCPリクエストに応答してクライアントにネットワーク情報を配信できるのは、許可されたDHCPサーバだけに限定されます。また、クライアント ポート上のDHCPリクエストにはレート制限が設定可能なので、個々のクライアントまたはアクセス ポートからのDHCP DoS攻撃の影響を軽減できます。

ダイナミックARP検査

ARPには認証機能はありません。悪意のあるユーザにとって、同じVLAN上にある他のホストのARPテーブルを操作することは実に簡単です。悪意のあるユーザは、攻撃者のMACアドレスとデフォルト ゲートウェイのIPアドレスを使用して、サブネット上の他のホストに非送信請求ARP応答（gratuitous ARP パケット）を送信します。このARP操作によって、さまざまなman-in-the-middle攻撃が可能となり、ネットワーク セキュリティ上の脅威になります。

ダイナミックARP検査は、無効のARP応答またはGratuitous ARP応答を同じVLAN上の他のポートに転送しないことによって、man-in-the-middle攻撃を阻止します。図3に示すように、信頼できないポート上では、ダイナミックARP検査によってすべてのARPリクエストおよび応答がインターセプトされます。インターセプトされた各パケットは、(DHCPスヌーピングにより収集された)有効なIP-MACバインディングであるかどうかが検証されます。

図3　ダイナミックARP検査



拒否されたARPパケットはスイッチのログに記録され、監査されます。信頼できるポート上の着信ARPパケットは、検査の対象になりません。

IPソースガード

IPソースガードは、Catalystスイッチを対象とした独自のCisco IOS®ソフトウェア機能で、IPスプーフィングの軽減に役立ちます。この機能は、悪意のあるホストが、ネイバのIPアドレスを不正取得することによってネットワークを攻撃することを阻止します。

IPソースガードでは、各ポートで送信元IPアドレスによるIPトラフィック フィルタリングをワイヤ スピードで実行します。IP/MAC/スイッチ ポート間のバインディングに基づいて、ポート単位のVLAN ACLがダイナミックに生成されます。バインディング テーブルは、DHCPスヌーピング機能またはスタティックな登録によって設定されます。IPソースガードは、アクセス層の信頼できないスイッチ ポートに適用されます。

Cisco Identity

ネットワークにおけるリソースの誤使用および不正アクセスの多くは、内部の送信元から発生しています。Cisco Identityは、いくつかのシスコ製品を組み合わせて認証、アクセス制御、およびユーザ ポリシーを提供し、ネットワークの接続性およびリソースを安全に保護する統合ソリューションです。

Cisco Identityでは、802.1XおよびExtensible Authentication Protocol (EAP)を併用して、RADIUSサーバなどの認証サーバに認証情報(ユーザID、パスワード、セキュリティ キーなど)を送信します。

シスコが企業に提供するのは、安全な認証フレームワークです。これにより、企業はユーザ モビリティを管理し、ネットワーク リソースへのアクセスの許可および管理に関連するコストを削減できます。また、ユーザの生産性が向上し、運用コストの削減にもつながります。

Cisco Identityは、次のような利点を提供します。

- **各レベルのユーザに優れた柔軟性と移動性を提供するインテリジェントな適応性** — ユーザとネットワーク リソース間の信頼関係を定義するポリシーを使用してユーザ プロファイルおよびグループ プロファイルを作成することにより、有線または無線ネットワークのすべてのユーザに対してAAAを簡単に適用できます。アーキテクチャによって安全性が保持されているという柔軟性は、Networked Virtual Organization(NVO)を実現するための主要な要素です。
- **認証、アクセス制御、およびユーザ ポリシーの組み合わせによる、ネットワークの接続性とリソースに対する安全性の確保** — ポリシーは物理ポートではなくユーザおよびデバイスに関連付けられるので、ユーザに大きな自由度と移動性が提供され、かつIT管理が簡素化されます。ポリシーの適用とダイナミックなプロビジョニングによって、管理が容易になるとともに、拡張性が増大します。
- **ユーザの生産性向上と運用コストの削減** — 有線または無線ネットワークのアクセスに優れたセキュリティと柔軟性が提供されるので、各業務の相互協力や新しいプロジェクト チームの発足に対して迅速に対応でき、信頼できるパートナーやベンダーのための安全なアクセスを可能にし、会議室の接続セキュリティを強化できます。ポリシーを集中管理することで、ネットワーク アクセスの安全性を柔軟に確保できるため、MACレベルのポート セキュリティ技術に比べて、時間、複雑性、および業務が削減されます。

Identityおよび802.1Xは、(Catalyst 6500、4500、3550、および2950スイッチを含む)すべてのCisco Catalystスイッチ、Cisco ACSサーバ、およびCisco Aironet®アクセス ポイント上でサポートされます。

Cisco Security Agent

サーバおよびデスクトップ コンピュータ(エンドポイント)が保護されていなければ、どのようなセキュリティ対策も効果はありません。エンドポイントへの攻撃は通常、探索、侵入、継続、伝播、麻痺という段階で進行します。

エンドポイント セキュリティ技術の多くは、初期段階での保護(しかも、シグニチャが既知の場合のみ)を提供します。Cisco Security Agentは、不正侵入の全段階を通して、ホストが受ける悪影響を未然に防止します。特に、既知のシグニチャが存在しない新しい攻撃からホストを保護するように設計されています。

Cisco Security Agentは、発生する前に 悪意のある動作を検出して阻止するという点で、従来のエンドポイント セキュリティ ソリューションよりも優れています。したがって、企業のネットワークおよびアプリケーションの脅威となる潜在的な既知および未知のセキュリティ リスクを回避できます。

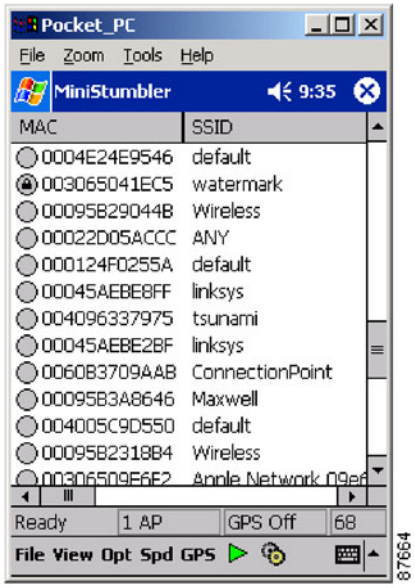
Cisco Security Agentは、重要なデスクトップおよびサーバ上にインストールするホスト型エージェントで、CiscoWorks VPN/Security Management Solution（VMS）を実行している管理センターへの報告を行います。これらのエージェントは、管理インターフェイスおよびエージェントと管理センター間の通信に、HTTPおよびSecure Sockets Layer（SSL）プロトコル（128ビットSSL）を使用します。

アプリケーションが処理を開始するとき、エージェントはその処理をアプリケーションのセキュリティ ポリシーと照合し、処理継続の「許可」または「拒否」をリアルタイムで決定し、リクエストをロギングすべきかどうかを判断します。悪意のある動作を「阻止」することが目的なので、ポリシーを更新しなくても、デフォルトのポリシーによって既知および未知の両方の攻撃が防止されます。エージェントと管理センター コンソールの両方で、相互に関連付けが行われます。この相互関係により、エージェントの精度は著しく向上し、正常な動作を妨げることなく、実際の攻撃なのか誤動作なのかを識別できます。また、管理センターでは、ネットワーク ワームまたは分散スキャンなどのグローバルな攻撃を特定できます。

WLANセキュリティ

適切に配備されていないワイヤレス ネットワークは、攻撃者の格好の標的になります。図4は、標準速度で走行する車両から、Personal Digital Assistant（PDA）を使用して無料のワイヤレス スキャン アプリケーションを実行し、ワイヤレス ネットワークをキャプチャしたものです。ここでは、68の個別ネットワークが識別されています。これらのネットワークのほとんどは、セキュリティ制限をまったく受けることなくアクセスできます。

図4　通勤途中で実施したNetStumbler.comのMiniStumblerによるキャプチャ



一般的に、これらの無防備なネットワークが存在するのは、社員が自分の利便性のためにIT部門に無断でアクセス ポイントを取り付けてしまうためです。

残念ながら、このようなアクセス ポイントを使用する社員には、部外者による企業ネットワークへの侵入を防ぐためのネットワーク セキュリティ機能に関する知識が、ほとんどありません。また、一般的にユーザ配備のワイヤレス ネットワークに使用される消費者レベルのアクセス ポイントは、攻撃者による企業ネットワークへのアクセスを阻止するような企業レベルのセキュリティ対策をサポートしていません。

無防備なアクセス ポイントがネットワーク セキュリティの脅威になることは事実ですが、これは防止できるものです。これらのアクセス ポイントを検出することは当然必要ですが、導入されたあとに検出するよりも、許可されていないアクセス ポイントを最初から拒絶するほうが効果的です。

次の方法で、無防備なアクセス ポイントがネットワークに接続されないようにします。

- 802.1XおよびTKIP機能を備えたCisco Wireless Security Suiteを使用して、IT部門がサポートしている安全なWLANインフラストラクチャを社員に提供します。これにより、無防備なアクセス ポイントを使用する必要がなくなります。
- Cisco Structured Wireless-Aware Network（SWAN）を実装し、無防備なアクセス ポイントと干渉を検出する機能を使用してローカルRFを分析することにより無防備なアクセス ポイントを検出するか、無線用のネットワーク解析装置を使用してネットワークの到達範囲を定期的に調査することで無防備なデバイスの位置を特定します。
- 企業のエッジ スイッチ上で802.1Xを実装し、ネットワークへのアクセスを阻止することによって、無防備なアクセス ポイントがネットワークに接続できないようにします。

Cisco Wireless Security Suite

Cisco WLAN（および企業WLAN全般）のソリューションには、Cisco Aironetファミリー製品およびCisco Compatible WLANクライアントデバイス対応のCisco Wireless Security Suiteを使用することで提供される、いくつかの安全性に関する配備オプションがあります。このソリューションは、Wi-Fi Protected Access（WPA）と呼ばれるWi-Fi Allianceセキュリティ規格を完全にサポートしています。Cisco Wireless Security Suiteを適切に配備することによって、ネットワーク管理者は、企業レベルのセキュリティと保護を備えたWLANを実現できます。

Cisco Wireless Security Suiteは、ユーザ単位およびセッション単位の相互認証方式として、IEEE 802.1Xおよび各種のEAPタイプをサポートしています。シスコの拡張セキュリティ ソリューションは、Cisco LEAP、EAP-Transport Layer Security（EAP-TLS）のほか、Protected Extensible Authentication Protocol（PEAP）などEAP-TLS上で動作するプロトコルおよびEAP-Tunneled TLS（EAP-TTLS）のすべてをサポートしています。802.1Xは、有線および無線ネットワーク上での認証を規定したIEEE標準規格です。この規格により、WLANに、クライアントと認証サーバ間の確実な相互認証が提供されます。また、ユーザ単位およびセッション単位のダイナミックな暗号キーが提供されるので、管理業務の負荷が軽減され、スタティックな暗号キーに関

するセキュリティ上の問題が解消されます。
IEEE 802.1XおよびEAPをサポートするアクセス ポイントは、Cisco Secure Access Control Server（ACS）などの認証サーバとワイヤレス クライアント間のインターフェイスとして動作します。

また、アクセス ポイントでVLANをサポートすることによって、複数のセキュリティ ポリシーを同時に適用できます。ネットワーク管理者は、VLANを構築することで、Wired Equivalent Privacy（WEP）、802.1X/TKIP、オープン アクセス、またはAdvanced Encryption Standard（AES）などの各種のセキュリティ オプションを使用してユーザを分割できます。

Cisco SWAN

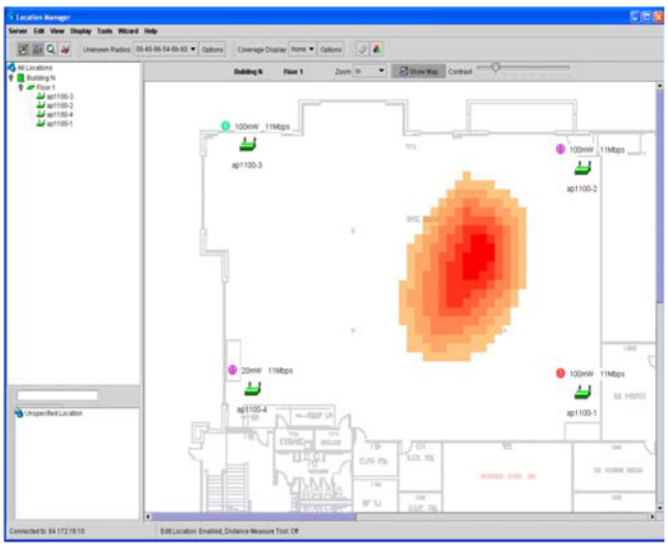
Cisco SWANは、Cisco Wireless-Awareインフラストラクチャ製品の統合WLANソリューションで、Cisco Aironetアクセス ポイントの安全な配備および管理の最適化によってWLANの総所有コストを最小限に抑えます。Cisco SWANには、4つの主要コンポーネントが含まれます。

- Cisco IOSソフトウェアを実行するCisco Aironetアクセス ポイント
- CiscoWorks Wireless LAN Solution Engine（WLSE）
- Cisco Secure ACSなどのIEEE 802.1X認証サーバ
- Wi-Fi認定ワイヤレスLANクライアント アダプタ

Cisco SWANは、有線LANと同レベルのセキュリティ、拡張性、信頼性、容易な配備、および管理機能をWLANに確実に提供します。Cisco SWANでは、中央またはリモートに配備する数百から数千のCisco Aironetアクセス ポイントを、単一の管理コンソールで管理できます。WLAN管理の複雑さが軽減されることによって、ネットワークのセキュリティも強化されます。

Cisco SWANには、CiscoWorks WLSEが含まれています。これは、善良な社員または悪意のある外部侵入者によって導入されたRogue（不正な）アクセス ポイントを検出、検索、および削減します。

図5　無防備なアクセスポイントの位置を示す CiscoWorks WLSEのロケーション ビュー



無防備なアクセス ポイントの位置は、これらのアクセス ポイントが接続しているスイッチ ポートの詳細情報とともに、CiscoWorks WLSE Location Manager（図5）に表示されます。

セキュリティ ツールとしてのQoS

無意味なトラフィックを流してデバイス間のリンクを過密状態にし、正当なトラフィックの宛先への到達を妨害するというタイプの攻撃があります。Cisco IOSソフトウェアのQoS機能を使用し、トラフィックを分類して優先順位を設定することで、このタイプの攻撃からリンクを保護できます。たとえば、一般的なユーザが送信するトラフィックは、通常、20 Mbps未満で送信されます。これに対し、攻撃者から発信されるトラフィックは、20 Mbps以上になることが多いものです。したがって、20 Mbps以上のトラフィックにプライオリティ1（低い優先順位）を設定し、20 Mbps未満のトラフィックにプライオリティ2（高い優先順位）を設定すれば、攻撃が発生しても正規ユーザのデータを確実に転送できます。さらに、ユーザまたは攻撃によるトラフィック量がどんなに多くても、ネットワーク管理者が主要デバイスに確実に到達できるようにするために、SSH、Telnet、およびSNMPトラフィックにプライオリティ4を指定します。

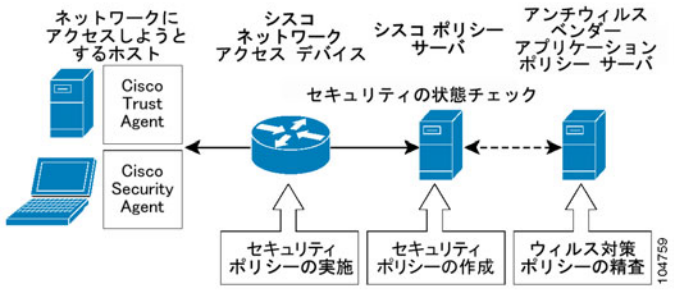
このようにQoSを使用すれば、管理トラフィックを常に確実に転送でき、正規ユーザのトラフィックも攻撃によって発生したトラフィックよりも優先的に転送されるので、ブラスト型の攻撃による影響を回避できます。

Cisco Network Admission Control（NAC）

社員が、企業ネットワークで使用するPCを、ワイヤレス ホットスポットのあるカフェ、インターネットにアクセスできるホテル、または自宅で接続した場合、ネットワークに新たなリスクが発生します。これらの公衆ネットワークには、企業ネットワークと同等の保護機能は提供されていないので、社員のPCがウィルスに感染する可能性が高くなります。

Cisco NACは、ネットワーク自身が感染しているユーザのデバイスを検出して隔離し、ネットワークへの影響を防止します。アクセスを許可するかどうかは、デバイスにインストールされたウィルス対策ソフトの状態やOSパッチレベルなどの情報に基づいて決定されます。Cisco NACは、条件を満たしている信頼できるエンドポイントデバイス（PC端末、サーバ、PDA）だけにネットワークへのアクセスを「許可」し、条件を満たしていないデバイスからのアクセスは「拒否」します。

図6　Cisco NAC



Cisco NACには、次のコンポーネントが含まれます。

- **Cisco Trust Agent** — エンドポイント システムに常駐するソフトウェアで、複数のセキュリティ ソフトウェア クライアント(ウィルス対策ソフトウェアなど)からセキュリティ状態の情報を収集して、アドミッション コントロールを実行するシスコ ネットワーク アクセスデバイスにこれらの情報を伝送します。
- **ネットワーク アクセスデバイス** — アドミッション コントロール ポリシーを実施するネットワークデバイス(ルータ、スイッチ、ワイヤレス アクセス ポイント、セキュリティ機器など)です。これらのデバイスは、ホストにセキュリティの「信頼性」を問い合わせ、ネットワーク アドミッション コントロールの決定を行うポリシー サーバに、これらの情報を伝送します。
- **ポリシー サーバ** — Cisco Secure ACSです。ネットワーク アクセスデバイスから伝送されたエンドポイントのセキュリティ情報を評価し、適用するアクセス ポリシーを決定します。
- **管理システム** — CiscoWorks VMSを統合したもので、Cisco NACのコンポーネントを管理します。

まとめ

多くの企業にとって、もはやネットワークは、人材の次に重要な資産となっており、保護する必要性が増大しています。現在のネットワーク攻撃の速度および損害の大きさ、また、将来的に攻撃がさらに悪化する可能性があることを考慮すると、ネットワークのセキュリティは「攻撃に対応する」だけでは不十分です。これからのセキュリティは「攻撃を事前に防ぐ」ものでなければなりません。この目標を達成する最善の方法は、ネットワーク インフラストラクチャのすべてのポイントにセキュリティ インテリジェンスを備えることです。ネットワーク セキュリティは、企業の最大の弱点になり得ることに留意する必要があります。

シスコは、ネットワーク セキュリティに熟練しています。以前から自社ネットワークのセキュリティ ポリシーを構築および実践するとともに、総合的なセキュリティ ソリューション群を開発してきました。

脅威に対する防衛から、信頼性および認証、安全な接続の確保まで、シスコは現在の企業に必要とされるセキュリティ対策のすべてに対応します。

CISCO SYSTEMS

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

04.09