ネットワークセキュリティの基礎

クリストファ　レーディ

White Paper #101

APC
Legendary Reliability™

要約

セキュリティに関する問題は、近年、増加しています。セキュリティ上の脅威が複雑になるにつれて、ネットワークの保護に必要なセキュリティ方法も複雑になってきました。データセンタのオペレータ、ネットワーク管理者などのデータセンタ専門家は、現在のネットワークを安全に展開し管理するために、セキュリティの基礎を理解する必要があります。このホワイトペーパーでは、ファイアウォール、ネットワークトポロジ、セキュリティ保護プロトコルなど、安全なネットワークシステムの基礎について説明します。また、ネットワークのセキュリティを保護する上でより重要で最良の方法も紹介します。

はじめに

現在、ビジネスネットワークとITインフラのセキュリティを保護するには、包括的な方法と、脆弱性と関連する防御策を的確に把握することが必要です。このような知識があってもネットワークへの侵入やシステムへの攻撃を完全に防ぐことはできませんが、ネットワークエンジニアに知識があれば、一般的な問題をある程度排除し、損害の可能性を大幅に減少させ、不正アクセスを迅速に検出できます。攻撃の量と複雑さは過去にないほど増大しているため、企業の規模にかかわらず、慎重にセキュリティ対策を実施する必要があります。**図1**は、CERT® Coordination Center（インターネットセキュリティ専門のセンター）の調査報告で、各年で発生するセキュリティ問題が急上昇していることを示しています。

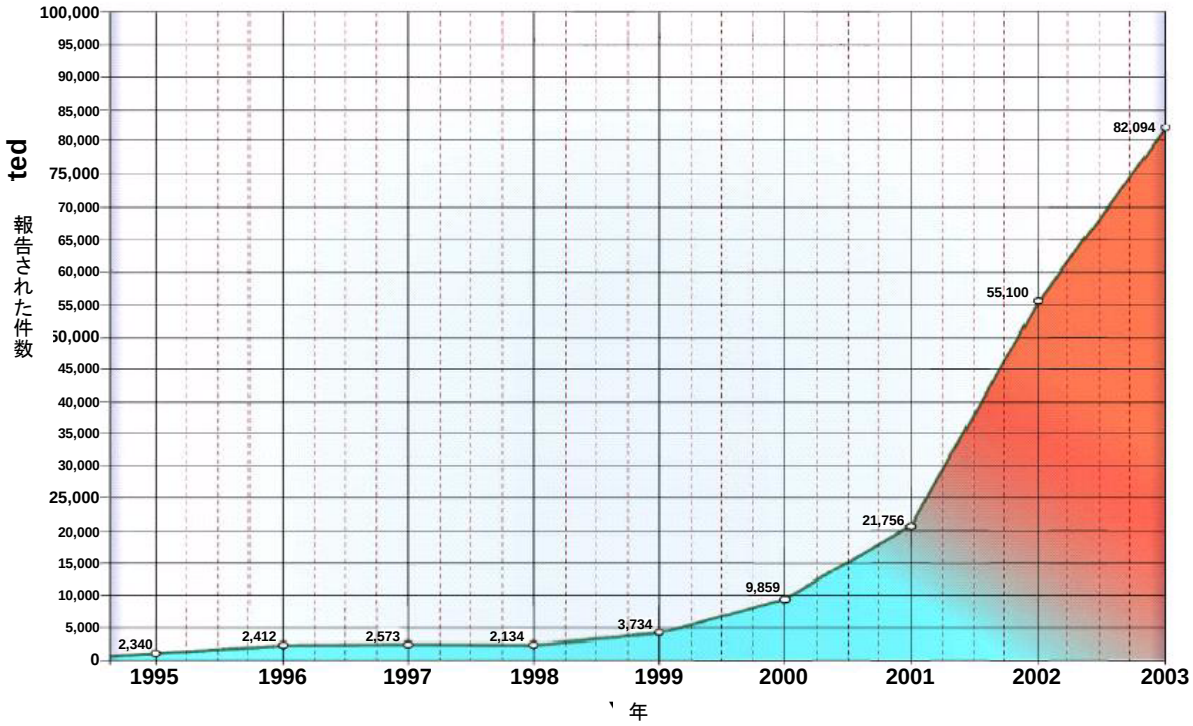

図1 - 各年のセキュリティ問題 - CERT.ORG

このホワイトペーパーでは、セキュリティについての基本的な前提の他に、ネットワーク、コンピュータホスト、インフラのネットワーク構成要素に関する最良の方法についても説明します。「唯一のセキュリティ対策方法」というものは存在しないため、最適な方法は、読者とシステム開発者の判断に委ねられます。

人的問題

どのようなセキュリティ対策を講じたとしても人的資源が最大の弱点です。パスワードやアクセスコードなどによる情報の保護は、ほとんどのセキュリティシステムの基本ですが、これらを注意深く遵守している人は必ずしも多くありません。セキュリティシステムでは通常、アクセスを制御し、身元を確認し、機密情報の漏洩を防ぐために、複数の方法を採用しており、システムにアクセスするためには、一般に 1つ以上の「パスワード」が必要です。このパスワードが漏洩したり盗まれたりした場合、パスワードで保護されていたシステムは不正ユーザにアクセスされる可能性があります。そして、多くの場合、初歩的な方法でシステムは不正アクセスされます。システムのパスワードを記載した付箋をコンピュータモニタの横に貼る行為は愚行のようでも、実際には多くの人が行っています。また、特定のネットワーク機器で、工場出荷時のデフォルトパスワードを変更しないということもあります。UPSに接続するネットワーク管理インターフェイスとして機能する機器がその一例です。UPSは、小容量の場合でも、100サーバに対応可能な大容量の場合でも、セキュリティ体系から看過されがちです。このような機器でユーザ名やパスワードがデフォルトのままにされた場合、デバイスの種類と発行されたデフォルトの権限さえわかればアクセスできるため、不正アクセスは時間の問題です。サーバシステムが、Webサーバやメールサーバに関する強固なセキュリティプロトコルで保護されている場合でも、セキュリティ保護されていないUPSの電源を切って入れ直すだけでサーバは破損する可能性があります。

セキュリティの全体像

規模にかかわらず、「企業」のセキュリティを効果的に保護するには、わかりやすく包括的なセキュリティが必要です。多くの組織では、セキュリティポリシーが作成されず、実践もされていません。この理由は明らかにセキュリティ保護にはコストがかかるというものです。このコストは、資金の面だけでなく、複雑さ、時間、効率で測定できます。セキュリティを保護するには、資金を投入し、作業手順を増やし、その手順が完了するのを待ちます（または、第三者を必要とする場合もあります）。

現実に、セキュリティプログラムの実行は困難です。通常、ある程度の「コスト」を伴い、適度な範囲のセキュリティを実現するスキーマを選択する必要があります（ほとんどの場合、「わかりやすく、包括的な」という条件よりも簡単です）。ここでの重点は、システム全体にわたる各側面で、知識に基づいて判断することと、ある程度、予測された方法を意識して採用することです。十分に保護されていない領域が認知できれば、少なくともその領域を監視して、問題や侵害を判断することができます。

セキュリティの基本

ネットワークの知識

保護する対象を明確に理解していなければ効果的なセキュリティ対策を行うことはできません。どのような規模の組織でも、一連のドキュメント、資産、システムを備えています。このような各要素には、組織にとって必要度に応じた相対値を、何らかの方法で割り当てる必要があります。たとえば、検討が必要な対象には、サーバ、ワークステーション、ストレージシステム、ルータ、スイッチ、ハブ、ネットワーク、通信回線の他、プリンタ、UPS、HVAC（精密空調機器）などのネットワーク構成要素があります。その他に、このタスクで重要な側面として、設備の場所と相互の依存性に関する注意をドキュメント化することもあります。たとえば、多くのコンピュータは、UPSなどの電源バックアップシステムに頼っています。さらに、UPSを管理している場合、UPS自体もネットワークの一部である場合もあります。

また、HVACや空気清浄機などの環境設備が存在することもあります。

脅威についての理解

次の手順は、**表1**に示すように、前述の各構成要素に対して考えられる「脅威」を特定することです。脅威は、内部と外部の両方に原因が考えられ、人的要因によるもの、自動化されたもの、または予期できない自然現象によるものがあります。自然現象は、セキュリティ上の脅威ではなく、システムが正常動作する上での脅威に分類するのが適切かもしれませんが、1つの問題から別の問題に派生することもあります。たとえば、停電によって防犯ベルが鳴ることがあります。停電は、意図的な事故の場合もありますが、落雷などの自然災害による場合もあります。どちらの場合でも、セキュリティは失われます。

表1 - 各種脅威とその結果の一覧

脅威	内部/外部	脅威の結果
ウィルス付きの電子メール	外部の送信元、内部での使用	電子メールシステムに感染し、結果的に組織全体に感染が広がります。
ネットワークウィルス	外部	保護されていないポート経由で侵入し、ネットワーク全体が不正アクセスされる可能性があります。
Webベースのウィルス	内部から外部サイトを参照	参照中、システムに不正アクセスされ、結果的に他の内部システムにも影響が及ぶ可能性もあります。
Webサーバ攻撃	外部からWebサーバに対して	Webサーバにハッカーが不正アクセスすると、他の内部システムからネットワークに接続するアクセス権を取得する可能性があります。
サービス拒否攻撃	外部	Web、電子メール、FTPなどの外部サービスを使用できなくなる可能性があります。 ルータが攻撃されると、ネットワーク全体が停止することもあります。
ネットワークユーザ攻撃（内部の従業員）	内部から任意の対象に対して	従来の境界ファイアウォールでは、この攻撃に何も対処できません。内部セグメントのファイアウォールの場合、損害を軽減できます。

物理的セキュリティ、内部での保護

多くの専門家がすべてのセキュリティは物理的セキュリティから始まるという意見に同意します。マシンやネットワークの攻撃ポイントに対する物理アクセスを制御することは、セキュリティのあらゆる側面において最も重要です。内部サイトに対して、任意の物理アクセスを可能にすると、サイトの大部分が公開されていることになります。一般に、物理アクセスが可能かどうかによって、ファイル、パスワード、資格情報などあらゆる種類のデータのセキュリティ保護が実現されます。幸い、この問題に対処できるアクセス制御機器や安全なキャビネットは各種揃っています。データセンタとネットワークルームの物理的なセキュリティ保護の詳細については、APCホワイトペーパー #82『Physical Security in Mission Critical Facilities』を参照してください（URL：http://www.apc.com）。

ネットワーク境界にファイアウォールを配置して保護

サイトの基本的な物理セキュリティを別にすると、次に最も重要な側面は、企業ネットワークの内部から外部、および外部から内部へのデジタルアクセスを制御することです。多くの場合、アクセス制御とは、外部（一般的にインターネット）への接続ポイントを制御することを意味します。中規模から大規模の企業では、ほぼインターネット設備があり、社内ネットワークがインターネットに接続しています。小規模の企業や個人住宅でも、インターネットの常時接続が大幅に増えています。このような環境の中では外部インターネットと内部イントラネットとの境界を区切ることは、セキュリティにとって重要な課題です。内部イントラネットは「信頼された（trusted）」側と呼ばれ、外部インターネットは「信頼されてない（un-trusted）」側と呼ばれることがあります。一般にはこの呼称で問題ありませんが、次に説明するように必ずしも具体的ではありません。

ファイアウォールは、制御された防壁を使用して、イントラネットにおける送受信のネットワークトラフィックを管理するメカニズムです。ファイアウォールは、基本的にアプリケーション固有のルータで、アプライアンスサーバなどの専用組み込みシステムで実行されることもありますが、一般的なサーバプラットフォームで実行されるソフトウェアプログラムの場合もあります。通常、こうしたシステムには、ネットワークインターフェイスが2つあります。1つはインターネットなどの外部ネットワーク用のもの、もう1つは内部イントラネット用です。ファイアウォールのプロセスによって、一方から他方へ通過可能なデータを厳格に制御することができるのです。使用するファイアウォールの種類は、トラフィック量、保護が必要なサービス、必要な規則の複雑さなどの要因によって異なり、ごく単純なものから複雑なものまで、さまざまな種類があります。ファイアウォールを通過可能にするサービス数を増やすほど、ファイアウォールの要件は複雑になり、正規のトラフィックと不正なトラフィックの区別が困難になります。

それでは、ファイアウォールで保護できるものと保護できないものは何でしょうか。
ファイアウォールの正確な設定を行えば、ある種のサービス拒否（Denial of Service/DoS）攻撃など、外部の脅威から保護する適切な手段になります。しかし不正な設定では、ファイアウォールは大きなセキュリティホールになる危険性があります。ファイアウォールに備わっている基本的な保護機能のほとんどは、ある送信先に対するネットワークトラフィックをブロックする機能です。送信先には、IPアドレスや特定ネットワークサービスのポートなどがあります。サイトで外部からWebサーバへのアクセスを提供する場合、全てのトラフィックをポート80（標準のHTTPポート）に限定することができます。通常、このような制限は、信頼されていない側が発信元のトラフィックにのみ適用されます。信頼された側からのトラフィックは制限されません。メール、FTP、SNMPなど他のトラフィックは、ファイアウォールを通過してイントラネットに到達することができません。単純なファイアウォールの例を**図2**に示します。

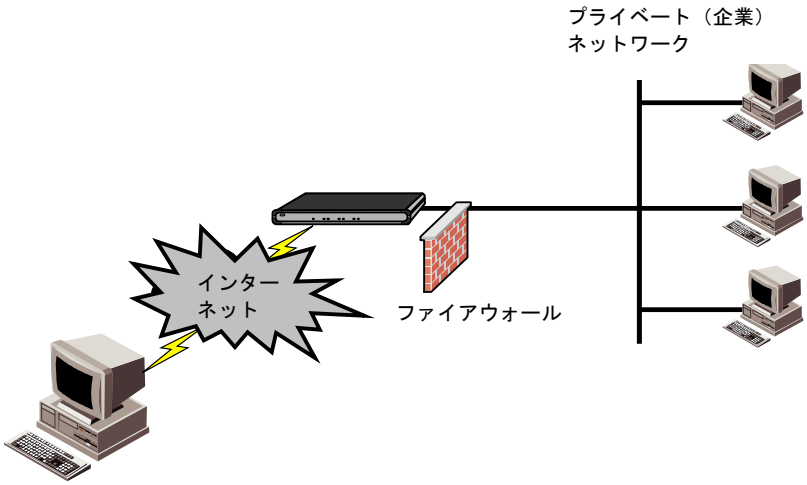

図2 – 単純なファイアウォールとネットワーク

より身近な例として、個人住宅や小規模の企業のケーブルルータやDSLルータを利用するユーザが、ファイアウォールを使用する場合を取り上げてみましょう。一般に、こうしたファイアウォールは、外部からのアクセスをすべて制限し、内部が発信元のサービスだけを許可するように設定されます。勿論、いずれかの場合でも、外部からのトラフィックをすべてブロックしているファイアウォールではありません（すべてブロックされていたとすれば、Webサーフィンや Webページの取得は不可能です）。ファイアウォールの実行内容は、外部からの接続要求を制限することです。最初の例では、内部からの接続要求はすべて外部に渡されます。その接続で実行される後続のデータ転送も、同様に外部に渡されます。一方、外部からは、Webサーバへの接続要求のみが許可され、データが渡されます。その他はブロックされます。この例では、内部から外部への接続だけが実行可能なので、より厳格な設定ということができます。

ファイアウォール規則が複雑な場合、いわゆる「ステートフルインスペクション」技術を利用できます。この方法は基本的なポートのブロック方法と併せて使用され、トラフィックの動作とシーケンスを監視して、スプーフ攻撃やサービス拒否攻撃を検出します。規則が複雑になるほど、ファイアウォールに必要な処理能力が増大します。

多くの組織が直面する問題の1つは、イントラネットのセキュリティを厳格に保護しながら、Web、FTP、電子メールなどの「公的な」サービスに対する正規のアクセスを可能にする方法でしょう。一般的な方法としては、DMZ（demilitarized zone/非武装地帯）と呼ばれる区域を構成します。このDMZとは、冷戦時代の言葉をネットワークに転用した表現です。DMZのアーキテクチャには2つのファイアウォールがあります。1つは外部ネットワークとDMZとの間にあり、もう1つはDMZと内部ネットワークの間にあるものです。パブリックサーバはすべてDMZに配置します。このように設定すると、パブリックサーバに対するパブリックアクセスを許容するファイアウォール規則を指定しながら、内部のファイアウォールですべての受信接続を制限することが可能になります。DMZを構成することで、パブリックサーバは、1つのファイアウォールサイトの外側に単に配置されるよりも、高度に保護することができます。**図3**に、DMZの使用例を示します。

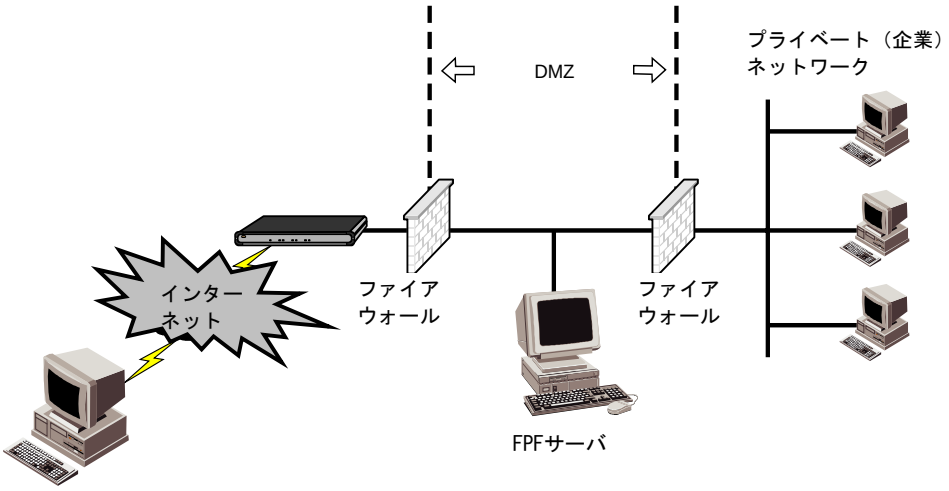

図3 – DMZを使用した二重ファイアウォール

また、各種イントラネット境界で内部ファイアウォールを使用すると、内部からの脅威や、インターネット境界のファイアウォールを通過してしまったワームなどによる損害を軽減することができます。このようなファイアウォールは待機状態で実行しておいて、通常のトラフィックパターンはブロックせず、問題が発生したときに厳格な規則に切り換えることもできます。

ワークステーションのファイアウォール

最近認知され始めた重要なネットワークセキュリティ要因に、ネットワーク上の全ノードまたは全ワークステーションが潜在的セキュリティホールになり得るということがあります。過去には、基本的に、ファイアウォールやサーバに注意が払われていましたが、Webの出現やインターネットアプライアンスなど新しい分類のノードが急増したことでネットワーク保護の次元が増えました。多様なワームウィルスプログラムがコンピュータに侵入し、侵入先のコンピュータを使用して一層増殖し、さらにシステムに危害を及ぼす場合もあります。組織で内部システムを「ロックダウン」すると、こうしたワームの多くを停止したり、防御したりすることができます。ワークステーションのファイアウォール製品を使用して、個々のホストでポートの送受信アクセスをすべてブロックできます（これはホストの一般的な要件ではありません）。さらに、組織の外部に対する不審な接続をブロックするという内部側のファイアウォール規則があれば、組織の外部に対するワームの拡散を防ぐことができます。内部での複製と外部での複製の両方を減らすことができます。多くの場合、すべてのシステムで、使用する必要がないポートをすべてブロックできるようにする必要があります。

基本的なネットワークホストセキュリティ

ポートのロックダウンと実行するサービスの最小化

ネットワーク機器やコンピュータの多くは、デフォルトでさまざまなネットワークサービスを立ち上げ、これらのサービスがワームやトロイの木馬等による攻撃のきっかけになりえます。ほとんどの場合、このデフォルトサービスは不要です。サービスを無効にすることでポートがロックダウンされると、このような危険性は軽減します。ファイアウォールのセクションで後述しますが、デスクトップやサーバでも、ネットワークのファイアウォールと類似する基本的なファイアウォールソフトウェアを実行して、そのホストで不要なIPポートへのアクセスをブロックしたり、特定ホストからのアクセスを制限したりすることができます。外部の防御が破られた場合や他の内部的な脅威に対する場合、内部の保護を実現するには、このようなソフトウェアを使用することが重要です。ホストを高度に保護できる、デスクトップ向けのファイアウォールソフトウェアパッケージは数多くあります。たとえば、Windows XP Service Pack 2には、基本的なファイアウォール機能が備わっています。

ユーザ名とパスワードの管理

「はじめに」で述べたように、ユーザ名やパスワードに関する不適切な管理が多くの企業ネットワークに共通してみられる問題です。高性能で集中管理された認証システム（詳細は後述）で問題を軽減することもできますが、ユーザ名とパスワードについて、多大な効果が期待できる基本的な指針があります。

1. 配偶者名、お気に入りのスポーツチームなど、わかりやすいパスワードを使用しないこと。
2. 数字と記号を混在させた長いパスワードを使用すること。
3. 定期的にパスワードを変更すること。
4. デフォルトの権限を変更すること。

コンピュータや設備に、上記の規則を実施できるポリシーが組み込まれていなければ、ユーザ自身がこの規則を遵守することにします。規則（4）については、実環境でデフォルトの権限が存在するかどうかテストすることができます。

アクセス制御リスト

設備やホストの多くは、アクセスリストが設定できます。アクセスリストには、対象の機器にアクセスする資格を有するホスト名やIPアドレスが定義されています。たとえば、組織ネットワークの内部からネットワーク設備に対するアクセスを制御する方法は一般的で、これにより外部のファイアウォールを破るような種類のアクセスからネットワーク設備を保護できます。このような種類のアクセスリストは重要な最後の防壁として機能します。また、アクセスプロトコルごとに規則が異なるため、デバイスによっては非常に効力を発します。

機器とシステムに対するアクセスのセキュリティ保護

データネットワークは、侵害やデータ盗聴の可能性から常に保護されているとは言えないため、付属するネットワーク機器のセキュリティを向上するために、複数のプロトコルが作成されてきました。一般に、懸念される課題には認証と非公開（暗号化）の2つがあります。システムと通信をセキュリティ保護する上で、この2つの要件に対処する多様なスキームとプロトコルが存在します。認証の基本について検討したうえで、暗号化について説明します。

ネットワーク機器向けの認証

認証は、ネットワーク構成要素（特にネットワークインフラ機器）に対するアクセスを制御する場合に必要です。認証には、一般的なアクセス認証と機能の認可という2つの事項が関連します。一般的なアクセス認証は、特定ユーザが、対象の要素に任意のアクセス権を持つかどうかを制御する方法です。通常、これは「ユーザアカウント」という形式で考えられます。認可は個々のユーザの「権限」に関係します。たとえば、認証されたユーザは何が可能になるでしょうか。また、機器を設定できるでしょうか。それともデータの参照のみでしょうか。**表2**では、主な認証プロトコルとその機能、関連するアプリケーションをまとめています。

表2 – 主な認証プロトコルのまとめ

プロトコル	機能	プロトコルの用途
ユーザ名/パスワード	プレーンテキスト、記憶されるトークン	Telnet、HTTP
CHAP（Challenge Handshake Authentication Protocol）	パスワードのハッシュと時間的に変化するデータを使用して、直接的なパスワード送信を防ぐ	MS-CHAP、PPP、APC HTTP、Radius
RADIUS (Remote Authentication Dial-In User Service	CHAPパスワード、直接的なパスワード、認可、アカウンティング方法	Telnetのバックエンド、SSH、SSL、Microsoft IAS Serverのフロントエンド、ネットワーク機器の一般的な中央認証方法
TACACS+ (Terminal Access Controller Access Control System Plus)	認証、認可、アカウンティング、完全な暗号化のサポート	Cisco SystemによるTACACSの独自拡張、中央認証、一部のRAS（Remote Access Service）用途
Kerberos	サービスの認証と認可、完全な暗号化	Telnet、Active Directoryと統合したMicrosoftのドメイン認証サービスのように、Kerberos対応のアプリケーション

デバイスへのアクセスを制限することは、ネットワークのセキュリティ保護で最も重要な側面の1つです。インフラ機器自体でネットワークとコンピュータ設備の両方に対応しているため、インフラ機器のセキュリティが危うくなるとネットワーク全体やリソースも破損する可能性があります。皮肉にも、多くのIT部門では、サーバを保護し、ファイアウォールを設定し、アクセスメカニズムをセキュリティ保護するために多大な労力を払っているにもかかわらず、基本的な機器の一部は初歩的なセキュリティのままとなっています。

最低でも、すべての機器に、簡単に推測されない（10文字で英数字と記号を混在させた）ユーザ名とパスワードの認証が必要です。ユーザ数とユーザの認可内容はいずれにも制限が必要です。セキュリティ保護されていないリモートアクセス方法の場合（つまり、ユーザ名とパスワードが暗号化されずにネットワークで渡される場合）は注意が必要です。また、パスワードは、3か月ごとなど、適切な頻度で変更する必要もあります。また、グループパスワードを使用している場合、従業員が退職するタイミングで変更します。

中央認証方法

a）機器のユーザ数が多数である場合、またはb）多数の機器がネットワークにある場合は、中央認証方法が適切です。従来の中央認証は、(a) の状況で発生する問題（最も一般的な問題はリモートネットワークアクセス）を解決するために使用しており、ダイヤルアップのRASなどリモートアクセスシステムではRASネットワークユニット上のユーザ管理は不可能でした。また、任意のネットワークユーザが、既存のRASアクセスポイントのどこでも使用する可能性がありました。すべてのRASユニットに全ユーザ情報を置いて最新の状態に保つことは、大規模な企業ユーザの場合、RASユニットの処理能力を超え、管理が非常に困難になります。

RADIUSやKerberosなどの中央認証システムでは、中央管理されているユーザアカウント情報を使用して、この問題を解決しています。ユーザアカウント情報には、RASユニットや他の設備から安全にアクセスでき、このような中央管理のスキームを使用すると、複数の場所ではなく1か所に情報を格納できます。つまり、多くの機器でユーザを管理するのではなく、1か所でユーザ管理をすることができるのです。また、ユーザ情報（パスワードなど）を変更する必要がある場合、1回のタスクで実行でき、ユーザの退職時には、そのユーザアカウントを削除することで中央認証を使用するすべての設備にアクセスできなくなります。通常、大規模なネットワークで認証が中央管理されていない場合の共通の問題は、すべての場所のアカウントを削除することなのです。RADIUSなどの中央認証システムは、通常、MicrosoftのActive DirectoryやLDAPディレクトリなど、他のユーザアカウント管理スキームとシームレスに統合することができます。この2つのディレクトリシステム自体は認証システムではありませんが、中央管理のアカウント格納メカニズムとして使用されます。多くの場合、RADIUSサーバは、RASや他のネットワーク機器とRADIUSプロトコルで通信できるため、ディレクトリに格納されているアカウント情報にも安全にアクセスできます。これがRADIUSとActive Directoryのブリッジ接続で、MicrosoftのIASサーバが実行している内容です。この方法は、RASユーザとRAS機器に中央認証機能が提供されるだけでなく、アカウント情報がMicrosoftドメインアカウントと統合されるということも意味します。**図4**では、Active Directoryドメインに対する認証時に、ネットワーク構成要素のActive Directoryサーバと RADIUSサーバの両方として機能する、Windowsドメインコントローラを示しています。

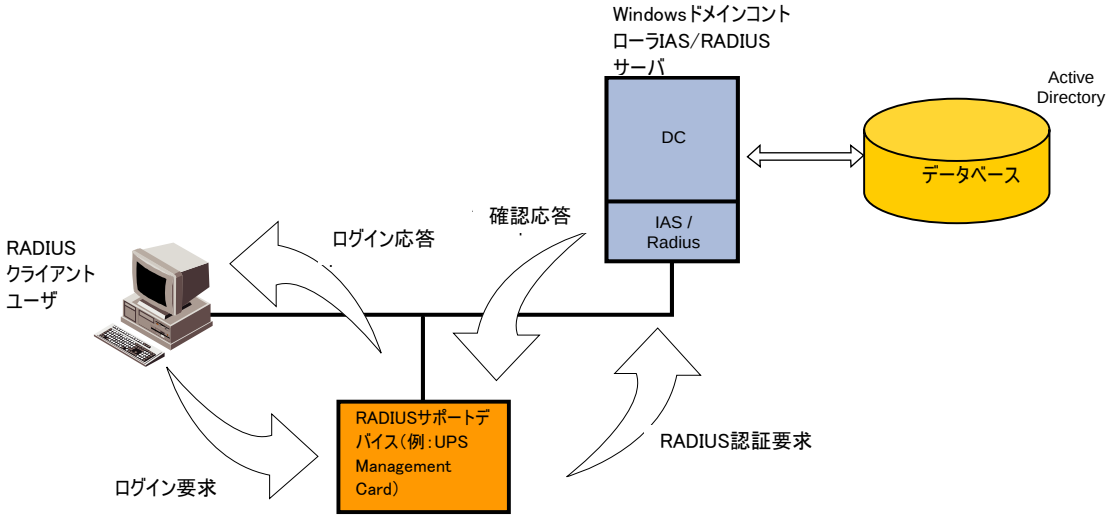

図4 – Windowsドメインコントローラ

暗号化と認証によるネットワークデータのセキュリティ保護

ネットワーク構成要素、コンピュータ、またはシステム間で交換される情報の漏洩に関する問題が重要になります。第三者が銀行口座にアクセスしたり、ネットワークで転送される個人情報を取得したりすることは望ましいことではありません。ネットワークでのデータ漏洩を防止するには、第三者(何らかの方法でネットワーク転送中にデータを取得する可能性がある)が転送データを読むことができないように、暗号化を取り入れる必要があります。データを「暗号化」するには多くの方法があります。ここでは主な方法について説明します。UPSシステムなどネットワーク機器に関する懸案事項は、従来、UPS電圧や電源コードの電流などのデータを保護するということでしたが、現在では、ネットワーク機器に対するアクセス制御が大きなものになっています。

セキュリティ保護されていないネットワーク(インターネットなど)でアクセスを実行する場合、ユーザ名とパスワードなど、認証の資格情報を漏洩しないことが重要です。組織のプライベートネットワーク内でも、このような資格情報を保護することが最良の方法です。まだ一般的ではありませんが、多くの組織では認証の資格情報だけでなく、すべての管理トラフィックをセキュリティ保護する(暗号化する)ポリシーを実施し始めています。いずれにしても、何らかの暗号化方法を取り入れることが必要です。

データの暗号化は、特定の暗号化アルゴリズム(3DES、AESなど)を使用して、プレーンテキストデータ(入力)と秘密キーを組み合わせて実行します。結果(出力)として暗号文が作成されます。暗号文をプレーンテキストに変換できるのは、秘密キーを持っている人物(またはコンピュータ)のみです。この基本的な方法論は、セキュアプロトコルの中心部分です(後述します)。暗号化システムの基本を構成するもう1つの要素は「ハッシュ」です。ハッシュ方法では、何らかのプレーンテキストの入力と、ときにキー入力を取り入れて、ハッシュと呼ばれる大量の数値を算出します。この数値は、入力サイズにかかわらず固定長(ビット数)です。キーを使用してプレーンテキストに戻すことができる可逆的な暗号化方法とは異なり、ハッシュは一方通行で

す。ハッシュからプレーンテキストに戻すことは数学的に不可能です。ハッシュは、各種のプロトコルシステムで特別なIDとして使用されます。これは、ディスクファイルでデータの改ざんを検出する、CRC（Cyclic Redundant Check/巡回冗長検査）のようなデータのチェックメカニズムが実現できるためです。ハッシュは、データ認証方法として使用されます（ユーザ認証とは異なります）。ネットワークで転送中に第三者がデータを密かに変更しようとすると、ハッシュ値が変化するため、改ざんが検出されます。**表3**に、暗号化アルゴリズムの基本的な比較と使用方法を示します。

表3 – 主な暗号化アルゴリズムのまとめ

アルゴリズム	主な用途	プロトコルの用途
DES	暗号化	SSH、SNMPv3、SSL/TLS
3DES	暗号化	SSH、SNMPv3、SSL/TLS
RC4	暗号化	SSL/TLS
Blowfish	暗号化	SSH
AES	暗号化	SSH、SSL/TLS
MD5	ハッシュ、メッセージ認証コード	SSH、SNMPv3、SSL/TLS
SHA	ハッシュ、メッセージ認証コード	SSH、SNMPv3、SSL/TLS

セキュアアクセスプロトコル

SSHやSSLなど各種プロトコルは、各種暗号化メカニズムを取り入れて認証方法と暗号化によってセキュリティを実現しています。実現するセキュリティのレベルは、さまざまな要因で変わります。たとえば、使用する暗号化方法、転送データへのアクセス、アルゴリズムのキー長、サーバとクライアントの実装、そして最も重要な要因が人的要因です。精巧な暗号化スキームでもユーザのアクセス情報（パスワードや証明書）を第三者が入手すると全く役に立ちません。パスワードを書いた付箋をコンピュータのモニタに貼り付けることは危険な行為です。

SSHプロトコル

Secure Shell（SSH）クライアント-サーバプロトコルは1990年代半ばに開発されました。その目的は、コンピュータコンソールやシェルに対して、リモートから保護されず、安全ではないネットワークでアクセスする安全なメカニズムを実現するためでした。SSHは、ユーザとサーバの認証に対応し、クライアントとサーバ間で交換されるすべてのトラフィックを完全に暗号化することで、これを実現しました。SSHには、V1とV2という2つのバージョンがあり、提供する暗号化方法に多少違いがあります。さらに、V2には、ある種の「攻撃」に対して高度な保護機能があります。つまり、第三者が、交換データを妨害、偽造、または変更しようとすると、攻撃と見なします。

SSHは、セキュアアクセスプロトコルとしてコンピュータコンソールに何年も使用されてきましたが、従来、UPSやHVAC機器など、二次的なインフラ設備にはそれほど採用されていませんでした。ただし、ネットワークと対応するネットワークインフラは企業の業務にとって重要となってきており、すべての設備に安全なアクセス方法を使用することが一般的になりました。

SSL/TLSプロトコル

SSHは、コマンドラインのような管理向けのコンソールアクセスの場合にセキュアプロトコルとして一般的でしたが、Secure Socket Layer（SSL）や後のTransport Layer Security（TLS）プロトコルが、Webトラフィックや他のプロトコル（メールに使用されるSMTPなど）をセキュリティ保護する場合の標準的な方法となりました。TLSは最新バージョンのSSLであり、一般には、SSLがTLSという用語と同義で使用されています。SSLとSSHの主な違いは、プロトコルに組み込まれたクライアントとサーバの認証メカニズムに関する点です。TLSは、IETF（Internet Engineering Task Force）の規格としても承認されていますが、SSHは、ドラフト版の規格としてより広範に展開されているにもかかわらず、完全にはIETFの規格となりませんでした。SSLは、HTTPのWebトラフィックを保護するセキュアプロトコルのため、「HTTPセキュア」を示すHTTPSとも呼ばれます。NetscapeとInternet ExplorerのいずれもSSLとTLSに対応しています。このようなプロトコルを使用すると、サーバ証明書という形式でサーバの正式な認証がクライアントに対して作成されます。クライアントは証明書でも認証できますが、ユーザ名とパスワードが最も一般的に使用されています。SSLの「セッション」は暗号化されるため、認証情報とWebページのデータは安全です。SSLは銀行や他の商用サイト等セキュリティを保護するWebサイトで常に使用されます。このようなサイトでは、一般にクライアントはパブリックインターネット経由でアクセスするためです。

ネットワーク機器をWebベースで管理する方法が最も一般的となったため、その管理方法の保護は極めて重要です。企業においてすべてのネットワーク管理をセキュリティで保護して、さらにHTTPなどのグラフィカルインターフェイスも利用する場合には、SSLベースのシステムを使用します。前述のように、SSLではHTTP以外の通信も保護できます。HTTPベース以外のクライアント機器を使用している場合も、確実にセキュリティ保護するにはアクセスプロトコルにSSLをシステムに取り入れます。どのような場合でもSSLを使用することで、共通の認証スキームと暗号化スキームで標準プロトコルを使用するという利点もあります。

ネットワークセキュリティの最良の方法

セキュリティポリシーを慎重に検討すると、ネットワークのセキュリティは大幅に向上します。ポリシーには、複雑で扱いにくいものや、基本的で直接的なものもありますが、多くの場合、ポリシーは単純で、最も有効とわかっています。たとえば、中央管理されたアンチウィルス更新システムとホストスキャナを組み合わせて、新しいシステムや古いシステムを検出する場合があります。このようなシステムでは、セットアップ、中央管理、ソフトウェアの展開機能が必要ですが、通常、最新のオペレーティングシステムではいずれも使用可能です。一般に、より複雑な問題に集中できるように、ポリシーと適切に自動化されたツールを使用して、システムにおける明確なセキュリティホールを減らします。企業のネットワークセキュリティポリシーには、一般に次のような項目があります。

- パブリックネットワークとプライベートネットワークの接続すべてにファイアウォールを設置
- ファイアウォールのルールセットのバージョンを制御し、中央管理で展開
- 外部リソースを二重のファイアウォールに配置（DMZに配置）
- すべてのネットワークで、不要なネットワークポートを閉じ、不要なサービスを無効化
- すべてのネットワークホストに、中央管理のアンチウィルスソフトをインストール
- すべてのネットワークホストで中央管理のセキュリティアップデートを利用
- RADIUS、Windows/Kerberos/Active Directoryなどの安全な中央認証
- パスワードポリシー（3か月ごとに変更すること、「安全なパスワード」にすることなど）でユーザを中央管理
- 新しいホストや古いシステムを積極的にネットワークスキャン
- 不審な動作についてネットワーク監視
- 事件の対応メカニズム（ポリシー、マニュアル、自動化など）

上記の一覧は、ポリシーに含める必要がある重要な項目です。他にも、項目が考えられますが、ポリシーの種類と範囲を決めるときは、企業規模、リスク分析、費用、業務への影響など、各要因のバランスをとることが重要です。前述のように、一般的には、システムの分析から開始して、次に業務を分析します。明確に定義されていなくても、小規模の企業であっても、ある程度のセキュリティポリシーが必要です。これは、企業規模にかかわらず全てのネットワークが攻撃対象になる可能性があるためです。

結論

ワーム、ウィルス、巧妙なクラッカーなど、ネットワークに対する脅威が増大しているため、プライベートネットワーク内でも、セキュリティはオプションとは考えられなくなりました。サービスの稼動時間やシームレスなアクセスを維持するには、UPSやHVAC（精密空調機器）などの物理的インフラ設備を含め、すべての設備でセキュリティを保護することが重要です。企業全体でセキュリティを実現し維持することは、通常、管理作業の増加を意味します。従来、これがセキュリティの普及に対する最も大きな障壁でした。

しかし今日では、たった1つのワームやウィルス攻撃に対して必要なネットワークの修復時間が、適切に企業のセキュリティを保護するために先行投資した場合の時間と比較して、長くなることがよくあります。幸い、ネットワークシステム管理にかかるコストを削減して、さらにネットワークのセキュリティを向上するシステムやソフトウェアの選択肢が数多くあります。定期的なソフトウェアの更新、デバイスすべてのロックダウン、中央管理と安全なアクセス方法の使用など、基本的な事項を実行していても、リスクを削減するには多くの手順が必要となる可能性があります。適切なセキュリティポリシーを採用し、ネットワークを高頻度で監査する習慣があれば、ネットワーク全体を一層高度に保護することができます。

著者について

クリストファ　レーディは通信に関する技術研究のディレクタで、米国ロードアイランド州にあるAPC本社に勤務しています。コンピュータとマイクロプロセッサシステムのプログラミングと設計に18年間携わり、現在は、通信システム、IPネットワーク、セキュリティ、組み込みシステムの調査と設計を中心に活動しています。APCでは、10年間にわたり組み込みネットワークの製品群を管理してきました。ブラウン大学のバイオエレクトリカルエンジニアリングで、理学士号を取得しました。米国や海外で開催される組み込みシステムの会議（Embedded Systems Conference）には、委員会のメンバーとしてだけではなく、レギュラースピーカとして参加しています。著書には、『Journal of Physiology』、『Communications Systems Design』、『Embedded Systems Programming』、『EE Times』などがあります。