



全体像をしっかりと理解する! **セキュリティ A to Z**

現在のネットワーク環境におけるセキュリティ対策は、従来型のポイントエンド、シングルポイントのものでは、まったく対応できなくなってきました。この「セキュリティ A to Z」では、企業ネットワークを取り巻くさまざまな脅威の実態を整理し、いま企業にとって本当に必要となるセキュリティ対策の基礎知識を習得していきましょう。

【技術編】 ネットワーク脅威とセキュリティの基礎知識

1	<p>ネットワークセキュリティの概念と脅威の種類 02</p> <p>そもそも脅威とは何か?企業ネットワークのどこが弱いのかを把握しましょう。ここを理解すればセキュリティ対策の勘所が見えてきます。</p> <p>【講義内容】</p> <ul style="list-style-type: none"> ● 脅威とその種類 ● 企業ネットワークの脆弱性 ● ネットワークセキュリティの概念
2	<p>内外からの不正侵入メカニズムとそのソリューション 08</p> <p>敵の手口を見極めましょう。不正侵入と攻撃のメカニズムを理解し、外部・内部からの攻撃に対する効果的な対策を解説します。</p> <p>【講義内容】</p> <ul style="list-style-type: none"> ● 不正侵入と攻撃のリスクとメカニズム ● ファイアウォールとDMZ ● 不正侵入検知とその進化
3	<p>コンピュータウイルスの脅威とそのメカニズム 14</p> <p>コンピュータウイルスは常に進化しています。その種類や個々の対策をまとめ、必要となるネットワーク全体でのソリューションについて考察します。</p> <p>【講義内容】</p> <ul style="list-style-type: none"> ● コンピュータウイルスとその種類 ● コンピュータウイルスへの対応策 ● ネットワーク全体に必要なソリューションとは
4	<p>企業ネットワークと認証技術 21</p> <p>ネットワークを守る方法の1つは、問題のあるコンピュータを接続しないことです。そのカギとなる認証技術とアクセス制御をしっかりと学びましょう。</p> <p>【講義内容】</p> <ul style="list-style-type: none"> ● 認証工程とアクセス制御技術 ● クライアント/サーバシステムと成りすまし・否認 ● 認証システムの問題点とソリューション
5	<p>セキュリティに不可欠な暗号化技術 27</p> <p>いつでも、どこからでも企業ネットワークにアクセスできるようになった現在では、暗号化技術は不可欠です。その基本を整理しましょう。</p> <p>【講義内容】</p> <ul style="list-style-type: none"> ● 盗聴を防止するための暗号化と復号化 ● 暗号化の基本メカニズム ● 暗号化とカプセルングによるVPNの実現
6	<p>統合型セキュリティシステムの概念 34</p> <p>これからのセキュリティ対策は、統合化されたセキュリティシステムが必要です。自衛するためのアプローチ方法を説明しましょう。</p> <p>【講義内容】</p> <ul style="list-style-type: none"> ● ネットワーク規模のセキュリティシステム ● 統合型セキュリティシステムのメカニズム ● 侵入検知から自己防衛型セキュリティへの進化

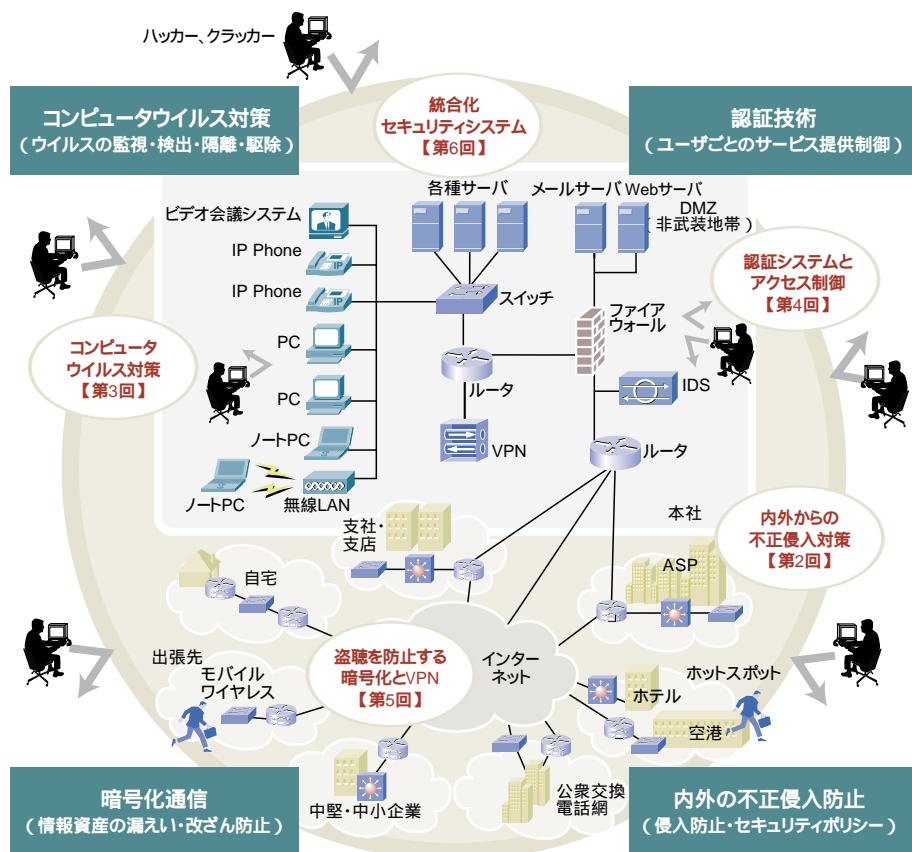


【第1回】ネットワークセキュリティの概念と脅威の種類

はじめに

企業ネットワークを多くの脅威から守るためには、これらすべての脅威に対する防衛機能を持った統合的なセキュリティシステムの構築が不可欠です。つまり、部分的に存在する複数の脆弱点を統合管理し、全域にわたる強固なネットワークセキュリティを実現しなければ、企業内外、善意・悪意を問わず存在するリスクを回避することはできないのです。本サイトでは、統合化セキュリティシステム構築のために必要となる基礎的な知識を連載形式で段階を踏んで解説していきます。本連載を最後までお読みいただければ、企業ネットワークに対するセキュリティの全体像をご理解いただけると思います。入門講座として簡単に読み進むことができるように構成しています。どうか肩の力を抜いて、お気軽に読み進んでください。

企業ネットワークを取り巻くさまざまな脅威【第1回】



1-1【LAN】

Local Area Network

敷地内や建物のフロア内など、限られた領域内に敷設されるコンピュータネットワークであり、複数のPCや周辺機器を相互的に接続し、さまざまな資源を共有することが可能となる。一般的にツイストペアケーブルを用いて100Mbps～1Gbpsで情報のやり取りを行うが、現在では光ファイバや無線などを用いたLANの普及も進みつつある。

1-2【サーバ】

Server

アクセスユーザにサービスを提供する専用コンピュータ。サーバにアクセスしてサービス提供を受けるコンピュータは、クライアント (client) と呼ばれている。

1-3【ストレージデバイス】

Storage Device

ストレージとは外部記憶装置のことだが、ここでいうストレージデバイスとは、ネットワーク対応の大容量記憶装置のこと。直接ネットワークに接続し、ファイルサーバとして利用することが可能。

1-4【情報資産】

企業内で用いている情報は、たとえば財務経営情報や人事情報、顧客情報や製品情報など多岐に渡る。これら企業にとっての価値ある情報は、単なるデータの存在を超え、重要な資産である場合が多い。よってこれらは情報資産と呼ばれる。情報資産の外部漏洩は、時として企業に致命的なダメージを与えることとなるため、十分な配慮が必要となる。

1-5【脅威】

情報セキュリティ管理システム (ISMS) において脅威とは、要求されるセキュリティの管理レベルを下回る水準にまで、保障の度合いを引き下げる潜在的な要因とされている。また、脅威とは何も外部からの攻撃に限定されているわけではなく、たとえば、ユーザがPCを利用しながら飲む一杯のコーヒーにおいても、PCIにこぼしてしまう可能性から、脅威の一つとなり得ることを認識しておく必要がある。

1

脅威とその種類

脅威とは何か?

ネットワークセキュリティを理解するには、まずその必要性を認識しなければなりません。限られた領域内に敷設されたコンピュータネットワークをLAN(Local Area Network)¹⁻¹と呼びます。LANはすでに大手企業のほぼ100%、中小企業においても高い割合で敷設・導入され、利用されています。また、現在では一般家庭においてもLANの普及率が高まりつつあります。

LANには、PC(Personal Computer)や**サーバ(Server)**¹⁻²などのコンピュータ、プリンタ、**ストレージデバイス(Storage Device)**¹⁻³などの各種周辺機器が接続されます。コンピュータやストレージデバイスには、企業の機密情報や個人情報など、外部に漏洩したり、改ざんや消去されては困るさまざまなデータが格納されています。つまり、私たち個人や企業は、**情報資産**¹⁻⁴の多くをLAN内に保存していることになります。

情報資産は、あくまでもデジタル化されたデータであることから、悪意ある第三者による盗聴や改ざん、破壊などのリスクをはらんでいます。このような情報資産に対して危機的状況をもたらす外的要因を**脅威**¹⁻⁵と呼びます。脅威はセキュリティリスク(Security Risk)と表現される場合もあります。

さまざまな形態が存在するリスク

脅威とはどこからやってくるものなのでしょうか。これについては、ネットワークの内外にそのリスクが潜んでいます。しかも形態や種類はさまざまです。ここでは、そのすべてを簡単にふれておくことにしましょう。

そもそも情報資産をリスクにさらす外的要因とは、地震や災害などの環境リスクや、**OS(Operating System)**¹⁻⁶やソフトウェアの不具合といったシステムリスク、機器の故障や障害、内外からの攻撃などといった運用リスクも存在します。

なお、ネットワークセキュリティでは、運用リスクとシステムリスクを中心としたソリューションを実現することで、より安全なネットワーク環境を実現することが目的となります。

ネットワークにおける脅威の種類とは?

現在、PCの多くは、各種アクセスサービスを介することで、インターネットに常時接続されています。また、企業ネットワークにおいても、インターネットや**WAN(Wide Area Network)**¹⁻⁷に接続されているものも少なくありません。このように、外部との接続がなされたPCやLANでは、悪意ある第三者が、意図して不正侵入を試みるリスクも高くなります。

仮に、不正侵入を許してしまった場合、多くの脅威がそこに発生することでしょう。たとえば、情報資産の盗聴、改ざん、破壊行為などが挙げられます。コンピュータウイルスをLAN内部に仕掛けられることにより、機密情報の漏洩や企業ネットワークの停止など、多大な被害へと波及することもあることでしょう。また、外部からの攻撃により、企業ネットワークやサーバがダウンすることで、企業のサービス提供が停止状態に陥ることもあります。

さらには、ネットワークを介した電子商取引において、客や業者に成りすます**成りすまし**¹⁻⁸や、業務や商品の発注をしたにもかかわらず、あとでこれを否定する否認行為などもネットワークシステムの脅威といえそうです。このように、ネットワークにおける脅威とは、さまざまな種類が存在するのです。これらを図1にまとめます。

1-6【OS】

Operating System

コンピュータを動作させたり、コンピュータとソフトウェアの仲介役を果たす専用のソフトウェアで、基本的な機能を担うことから、基本ソフトとも呼ばれている。ちなみにWindowsや、UNIX、Linux、FreeBSD、MacOSXなど、よく耳にするものは、すべてOSの名称である。

1-7【WAN】

Wide Area Network

電気通信事業者によって提供される広域ネットワークのこと。本支社間や取引先間のLANなどを相互的に接続する場合、専用線を敷設したのでは多大なコストがかかってしまう。このためあらかじめ敷設されたこれらの広域ネットワークに対する利用ニーズが高まった。なお、WANのサービスには多種他品目が用意されており、企業ユーザは必要に応じてコストに見合うサービスの選択ができるようになっている。

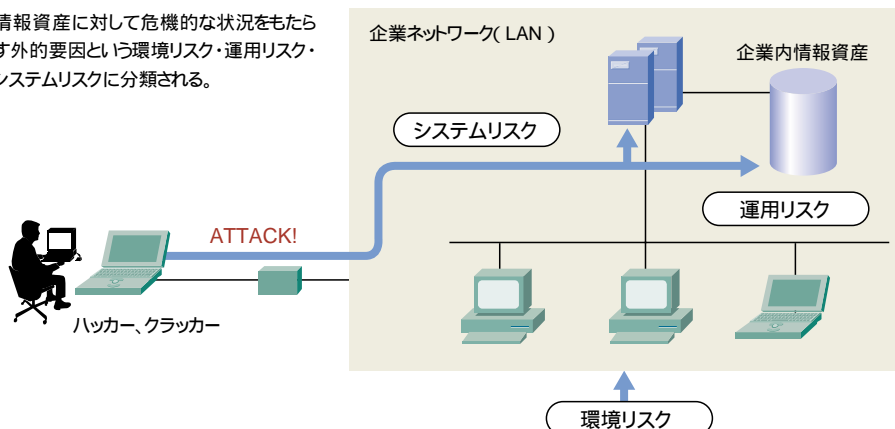
1-8【成りすまし】

コンピュータネットワークを介した情報のやり取りにおいては、互いに相手の顔や声を確認するといった認証行為が容易にはできない。この脆弱点を突いて広がった不正行為が成りすまし。IDやパスワードが漏洩すれば、誰もが容易に成りすますことができるし、電子商取引において、第三者に成りすまして物品を購入するなどの犯罪も目立っている。

1

図1 脅威とその種類

情報資産に対して危機的な状況をもたらす外的要因という環境リスク・運用リスク・システムリスクに分類される。



- 環境リスク : 地震や災害などビル・コンピュータルームの脆弱性)
- 運用リスク : スタッフのセキュリティポリシー(意識レベルの低下)
企業内業務の運用手順(運用手順ミス)
企業ネットワークのシステム運用(不正侵入・ウイルス侵入)
- システムリスク : 不正侵入(情報資産の漏洩・改ざん・盗聴・ウイルス)
攻撃(外部からの攻撃によるサービス停止)
OS・業務システムの不具合
アクセス数・ネットワーク内トラフィックの急増
コンピュータ・周辺機器の故障など

1-9【企業ネットワーク】

最近の企業ネットワークの利用形態は多岐に及んできている。単なる情報や周辺機器の共有のみならず、IP電話やテレビ会議システムを実現するための伝送路としても用いられる。つまり、企業ネットワークとは、単なるコンピュータネットワークを超えた複合的な情報ネットワークとして機能しているわけである。

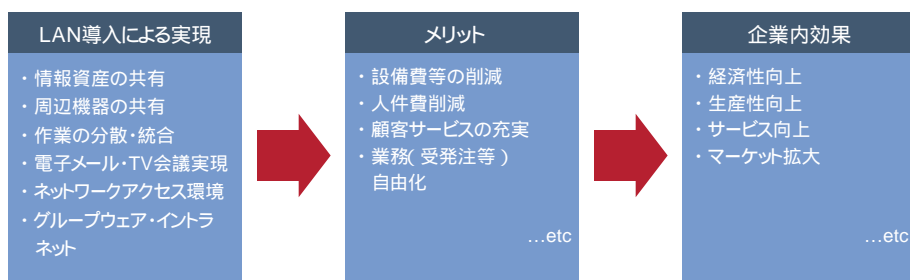
企業ネットワークの脆弱性

企業ネットワークとそのメリット

企業ネットワーク¹⁻⁹とは、企業内に敷設されるLANを意味しますが、これは大手企業のみならず、中小企業に至るまで、大変高い普及率で推移するまでになっています。このような普及率に至る背景には、企業ネットワークがもたらす多大な利便性が存在するはずですが、実は、この利便性こそが脆弱性を生む原因ともなるのです。ここではまず、企業ネットワークがもたらすメリットについて理解しておくことにしましょう。

企業ネットワークのメリットとは、LANのメリットと同様です。LANを構築することによって実現可能なこととは、図2に示すように、複数存在します。また、これらが実現することにより、無駄な経費やロス、人件費などを削減することが可能となるため、経済性の向上を図ることが可能です。一方、作業の分散や統合、コミュニケーションの充実などを実現することにより、生産性の向上、さらにはサービスの向上を図ることもできます。

図2 企業ネットワーク(LAN)のメリットと効果



1

企業ネットワークの基本的なトポロジ

次に、企業ネットワークのトポロジを見てみることにしましょう。ちなみに**トポロジ (TopoLogy)**¹⁻¹⁰とは、ネットワークの「構成」を意味する言葉です。

現在、企業ネットワークとして敷設されるLANは、下図に示すように、インターネットに常時接続され、それぞれのPCからWebのブラウジングやメールのやり取りが可能です。また、昨今ではテレビ会議システムやIP電話の導入により、映像や音声情報の伝送路としても、企業ネットワークは機能します。これらは全国の本支社や得意先などのコミュニケーションに用いられることから、多くの場合、**IPネットワーク**¹⁻¹¹などのWANを介して、相手先のLANと相互接続される場合も少なくありません。LAN間接続が可能となると、企業間の受発注などのすべてをデジタルデータとしてやり取りする**EDI (Electronic Data Interchange)**¹⁻¹²や**Web-EDI (Web-Electronic Data Interchange)**を実現することもできます。

さらには、外部で活動するスタッフが企業ネットワークにアクセスし、情報資産を利用したり、スケジュールの管理などを行うことができるように、**ダイヤルアップIP**¹⁻¹³接続用のアクセスポイントが設置されている場合もあります。最近は無線LAN化することにより、企業内のどこからでも自由にアクセスできる環境を実現している企業ネットワークも多くなりました。このように、企業ネットワークとは、多種の情報を取り扱うとともに、ほかのネットワークと手をつなぎ、あらゆる方向からのアクセスを可能とすることで、多くの利便性を生み出しているネットワークであることが分かります。

利便性が生み出す脆弱性

しかしこの利便性は、脆弱性を生み出す要因にもなり得ます。まず、インターネットやIPネットワークなど、外部のネットワークと相互的に接続されたトポロジの場合、そのネットワークからの攻撃を受ける可能性があります。ダイヤルアップIP接続のアクセスポイントも、電話番号とIDやパスワードなどの情報が漏れた場合、誰もが成りすまして不正侵入を果たす入り口になってしまう。また、無線LANの場合、外部からの不正侵入を、無条件に許してしまうリスクもあるのです。そして、不正侵入を許してしまえば、情報資産の盗聴や改ざん、破壊など、多くの脅威に直面しなければならないことになります。このように、利便性の拡大を目的として、外部との接点を増やした場合、その分だけ脆弱性も拡大させてしまうことになるわけです。

また、これらの接点を介してウイルスなどの**ワーム (Worm)**¹⁻¹⁴が企業ネットワーク内に侵入した場合、ネットワーク内部の情報資産が汚染されたり、このことにより、ネットワークによって実現していたサービス提供を停止せざるを得ないことにもなりかねません。

さらに、ウイルス汚染は、比較的短い時間において、接続されるほかの企業ネットワークへと感染し、被害を拡大してしまうリスクさえあるわけです。

そこで、利便性を拡張しながらも、脆弱性を最小限にとどめ、重要な情報資産を安全に守るための対策が不可欠となります。これを踏まえて、次に話を進めることにしましょう。

1-10【トポロジ】

TopoLogy

本文でも説明しているように、構成を意味する。ネットワークポロジには、トラフィックの流れなど認識するための論理トポロジと、ネットワークの接続形態を表現する物理トポロジが存在し、各々は用途に応じて用いられている。

1-11【IPネットワーク】

Internet Protocol Network

IP (Internet Protocol) という通信手順を用いて通信を行うコンピュータネットワークであり、電気通信事業者によって提供される。IPはインターネットの通信手順でもあり、よってIPネットワークを介することで、インターネットと同様のサービスのやり取りを、本支社間や取引先間を結んだ私的な企業ネットワークとして実現することができる。

1-12【EDI】

Electronic Data Interchange

(電子データ交換)

企業内で用いる情報や書類などをデジタル化し、ネットワークを介してやり取りするための技術を用いる。得意先との受発注などを自動化する際にも用いられる。なお、現在はインターネットやIPネットワークを介すとともに、これをWebベースで実現するEDも存在する。これをWeb-EDIという。Web-EDIは、やり取りをHTTPというWebのプロトコルで実現する。このため、新たに通信部分を開発する必要がなく、単にWebサーバとWebブラウザがあれば実現するため、比較的導入コストを低く抑えることが可能となる。

1-13【ダイヤルアップIP接続】

アカウント(利用資格)を所有するプロバイダのホストサーバに対して、一般の公衆電話網やISDNを介してPCを接続することをいう。接続時のPCとプロバイダ間においては、PPP(Point-to-Point Protocol)という通信手順が用いられる。電話回線などを介してインターネットに接続し、サービスを利用するための接続方法の一つである。

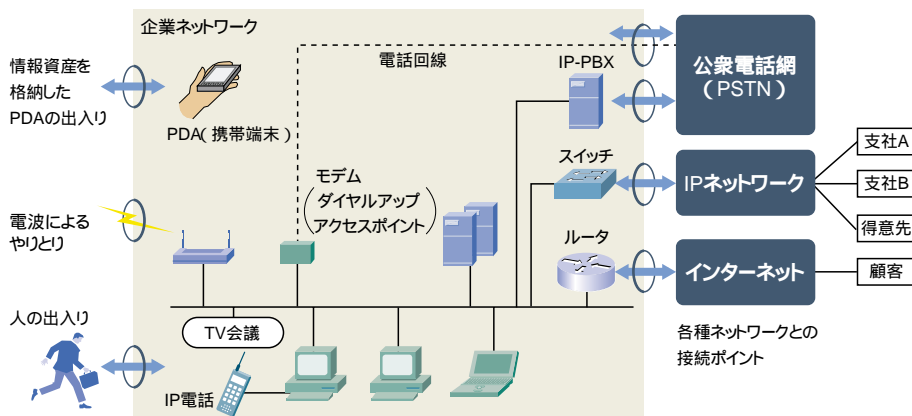
1-14【ワーム】

Worm

人為的に作られたプログラムであり、自己増殖を繰り返しながら、さまざまな破壊活動を行うコンピュータウイルスのこと。

1

図3 企業ネットワークの基本的トポロジと脆弱性



企業ネットワークを機械的に利用するために、利便性を高めるトポロジにすると、それに比例して出入口がふえ、脆弱性が増してしまふ。(出入口のすべては、不正侵入やウイルス侵入、情報漏洩などのリスクを発生させる)

1-15【ネットワークセキュリティ】

ネットワークセキュリティは、一つのネットワーク内に存在する複数のホストやホスト内の情報資産に対する保全措置をいう。これに対して、一台のコンピュータやPCなどに限定した保全措置は、ホストセキュリティと呼ばれている。

ネットワークセキュリティの概念

ネットワークセキュリティとは？

今回は、企業ネットワークの利便性や機能が高まるのに比例する形で、脆弱性も増してしまい、数多くの脅威にさらされてしまうという流れを学んできました。これらについては、すべてのネットワークが抱える問題です。だからといって何もせずに見過ごすわけにはいきません。なぜなら、脅威は時に多大な損失を発生させることもあるため、企業ネットワークとしてのLANやLAN内の情報資産を守るための何らかの対応策やシステムが不可欠なのです。このような脅威に対する対応策を総称して、**ネットワークセキュリティ(Network Security)**¹⁻¹⁵と呼びます。

つまり、ネットワークセキュリティは、企業ネットワークの利便性や機能などを高めながらも、数々の脅威から情報資産を守ることでできる強固な安全対策を実現するものといえます。

ネットワークセキュリティの重要性

では次に、ネットワークセキュリティの重要性について確認しておくことにしましょう。

日本において企業ネットワークの導入が一般化してきたのは、インターネットが普及し始めた1990年代のことでした。企業ネットワークの歴史とは、まだまだ浅いものであるため、ネットワークセキュリティの認識度を、あまり重要なものとしてとらえていない企業も存在するといえます。しかし、企業の情報漏洩が大々的に取り上げられるようになって、徐々にではありますけれども、ネットワークセキュリティの重要性が認識されつつあります。

外部との接続がなされている企業ネットワークでは、全体の90%が何らかの形でセキュリティの損害を被っているとされています。このなかで外部からの脅威が75%であり、残りの25%は内部の脅威であるとの数字もあります。また、情報漏洩のみならず、外部からの不正侵入による情報資産の盗聴や改ざん、さらには、外部からの攻撃やウイルス感染による電子商取引や企業内システム、全提供サービスの機能停止など、多くの脅威が存在します。これらが発生することにより、企業は、生産性低下や売上の減少、さらには信用の失墜など、非常に多大な損害を被る可能性があることを忘れてはなりません。

このような事態に陥らないためにも、企業は企業ネットワークに対するネットワークセキュリティ対策に取り組んでいく必要があるのです。

1

ネットワークセキュリティの実現プロセス

企業がネットワークセキュリティに取り組む場合、全社的な意識の向上が不可欠となります。そこで企業全体において、ネットワークセキュリティの方針を打ち立てることになります。これをインフォメーションプロテクションポリシー(Information Protection Policy:情報保護指針)もしくは**セキュリティポリシー(Security Policy)**¹⁻¹⁶と呼びます。

また、セキュリティには、「機密性:Confidentiality」、「保全性/安全性:Integrity」、「有効性/可用性:Availability」の3つの要素が不可欠となります。つまり、機密性と保全性を重視するために有効性を欠いてしまうと、生産性や対顧客サービスの低下を引き起こしてしまうことになるため、全体のバランスを考慮する必要があります。

さて、企業が実際にネットワークセキュリティに取り組む場合、これを踏まえううえで、物理的セキュリティ対策と論理的セキュリティ対策の双方を同時に遂行していく必要があります。物理的セキュリティ対策とは、システムを構築するうえで不可欠となる機器や設備などハードウェアのセキュリティ対策を意味します。また、これに対して、論理的セキュリティ対策とは、OSやアプリケーションなどを含むソフトウェアシステムのセキュリティと、システムの管理・運用体制、スタッフのセキュリティに対する意識改革などを意味します。

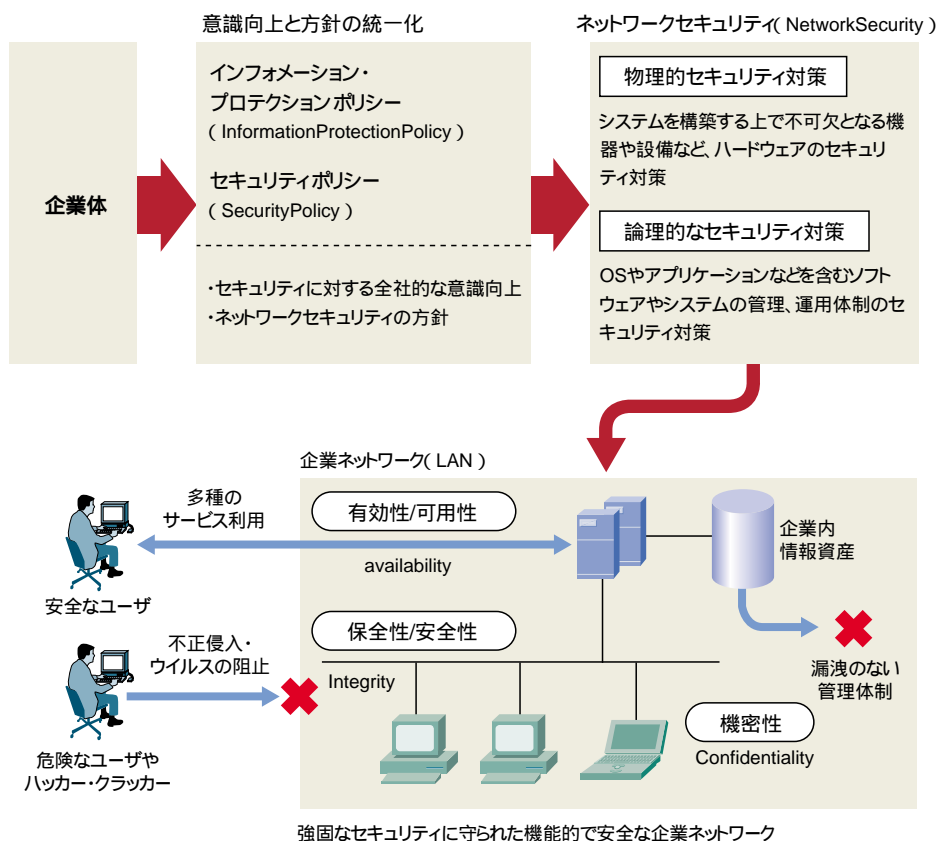
ネットワークセキュリティは、これらのすべてを総合的に実現することにより、初めて強固なものとして機能することになり、多くの脅威を寄せつけない安全な環境を実現することができるのです。

1-16【セキュリティポリシー】

Security Policy

セキュリティポリシーは、セキュリティ対策における基本的な方針を記した文書のことをいうが、用いられている意味合いとしては、さらに広いものがある。たとえば企業内のセキュリティに対する意識を示すこともある。また、セキュリティソフトウェアやファイアウォールなどの設定条件やそのファイルについてをセキュリティポリシーと呼ぶこともある。

図4 ネットワークセキュリティの実現プロセス





【第2回】内外からの不正侵入とそのソリューション

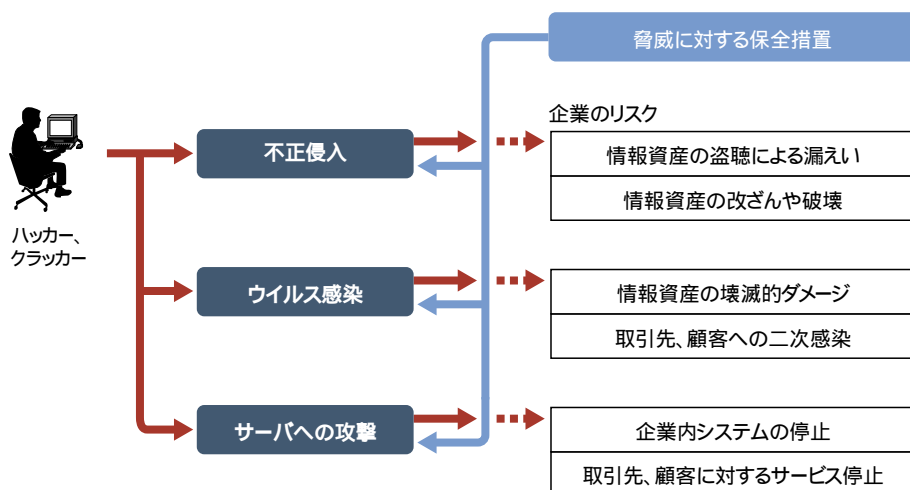
不正侵入と攻撃のリスクとメカニズム

不正侵入と攻撃のリスク

今回は、脅威のなかでも特に大きな損害を発生させるリスクをはらむ、不正侵入と攻撃について見ていくことにしましょう。第1回で説明したように、不正侵入を許してしまうと、さまざまな二次の被害を被ってしまいます。また図1のように、ウイルスがネットワーク内を汚染したり、外部から企業内のサーバに攻撃を仕掛けられたりすることで、さらに深刻な事態に陥ることもあります。

このように、企業ネットワークに対する不正侵入と攻撃は、企業に対して多大な損害を与えることがあるので、企業ネットワークを構築した場合は、これらの脅威に対する保全措置をあらかじめ万全な状態にしておくことが不可欠です。

図1 脅威と企業のリスク



不正侵入を可能とする基本的手法とは

次に、不正侵入について、もう少し詳細に見ていくことにしましょう。

不正侵入の手法は、多くの方法が考えられます。最も容易にネットワークへ侵入する方法は、外部からのアクセスを許可する企業ネットワークにおいて、これを利用するユーザのIDとパスワードを何らかの方法で入手したり、解析したりしたうえで、そのユーザに成りすまして不正侵入を果たすものです。IDとパスワードを、ディスプレイの脇に貼りつけるユーザや、これらの情報をメールで同僚などに教えるなどの甘い管理体制が一般化している企業の場合、第三者がIDとパスワードを知る機会是比较的が多くなります。つまり、外部からの不正侵入を助長する要因とは、組織内部にも存在するわけです。昨今問題となっている顧客情報など、情報資産の漏洩も内部の犯行であることから、前回で学んだセキュリティポリシーやインフォメーションプロテクションポリシーに対する企業全体の取り組みは非常に重要なものとなります。ちなみにパスワードを解析する行為は**パスワード攻撃**²⁻¹と呼ばれます。また、内部スタッフがスイッチなどに細工を施すことで、他ユーザのケット内容を盗聴する**パケットスニファ**(Packet Sniffer)²⁻²攻撃もあります。

2-1【パスワード攻撃】

通常パスワード情報は、暗号化された形で保存されているため、パスワード情報ファイルを手したとしてもパスワード自体が漏洩することはない。しかし、パスワードは、一定のアルゴリズムによって暗号化されるため、たとえば辞書の単語を一つひとつ同じアルゴリズムにかけて暗号化し、それをパスワードファイルと照合することで、少なくとも辞書に載っている単語をパスワードにしているものは解析されてしまうことになる。ちなみにこの作業は、専用ツールを用いれば、短時間で行うことが可能である。

2-2【パケットスニファ攻撃】

Packet Sniffer

100BASE-TX以降のLANにおいて、LAN上を流れるケット(フレーム)は、目的の相手以外に流れることはないが、スイッチを操作することでこれを強制的に特定の端末へ送ることを実現するツールが存在する。これを用いれば、第三者がこれを盗聴することが可能となる。ちなみにスニファとは、くんと臭いを嗅ぐ動作や臭い探知器などの意味を持つ。盗聴の可能性は内部にも存在するわけである。

2-3【コマンド】

Command

通常はキーボードからコンピュータに対して与える命令をいう。OSには、さまざまなコマンドが用意されており、これらを用いて、データ管理やネットワーク制御などを行うことが可能。なお、コマンドは通常、Windows環境の場合DOS窓やコマンドプロンプトから、UNIXやLinuxの場合はxtermなどの端末エミュレータから行う。

2-4【ツール】

Tools

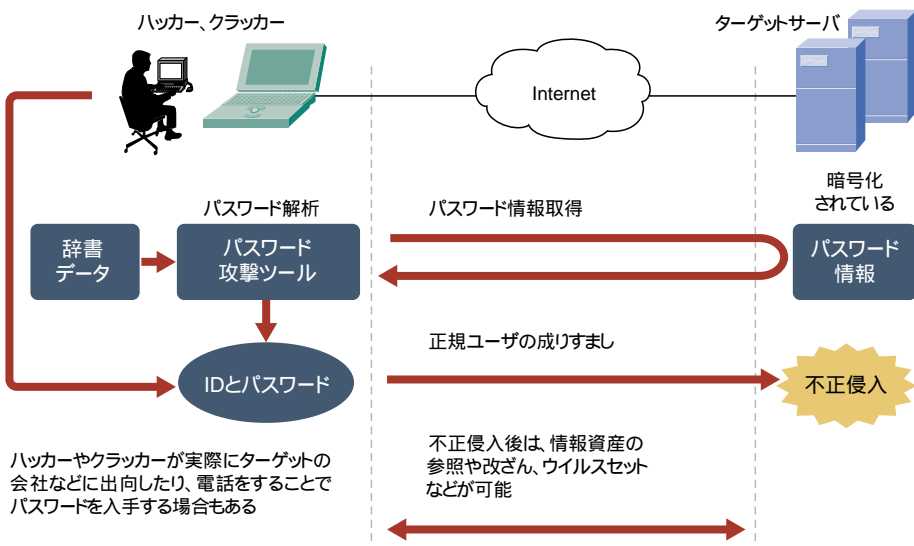
特定の処理を行うために用いられるソフトウェアであり、道具としての利用価値を持つためこのように呼ばれる。また、ソフトウェアの1機能を指す場合もある。

2

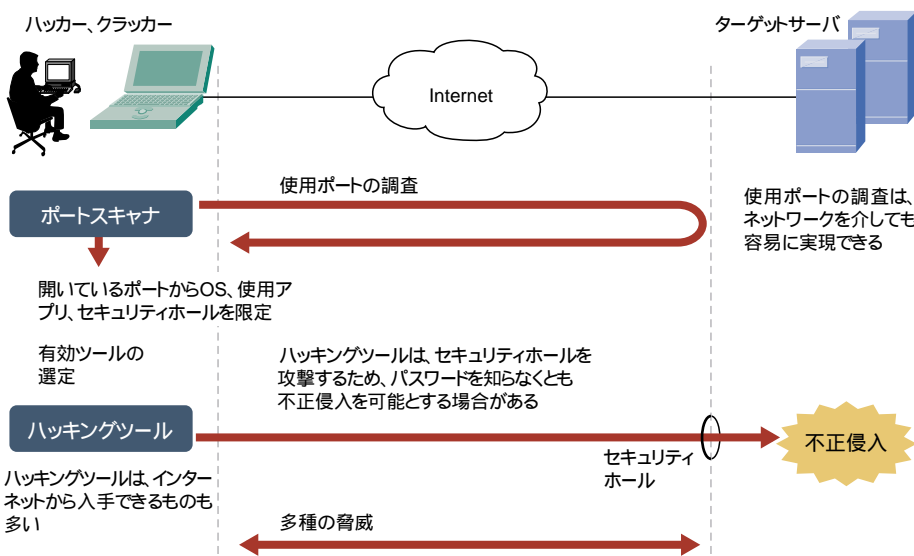
一方、**コマンド (Command)**²⁻³や**ツール (Tools)**²⁻⁴を利用した外部からの不正侵入も多く存在します。たとえば、相手先のコンピュータへの**パケット (Packet)**²⁻⁵の到達可能性を調査するためのコマンドとして**ping (Packet InterNetwork Groper)**²⁻⁶があります。これを用いることで、まずインターネットに接続されるコンピュータを見つけ出します。次に、そのコンピュータに対して、情報の出入り口となる**ポート (Port)**²⁻⁷を調べる**ポートスキャナ (Port scanner)**²⁻⁸と呼ばれるツールを用いることで、セキュリティホールが存在するか否かを調査できます。また、特定のセキュリティホールが発見された場合、これを逆手にとった内部への侵入用の専用ツールを用いれば、不正侵入が可能となる場合があります。なお、このようなアプリケーションのプロトコルに存在するセキュリティホールを突いた攻撃は、**アプリケーションレイヤ (Application Layer) 攻撃**²⁻⁹と呼ばれています。

図2 パスワード攻撃やツール類を用いた不正侵入

パスワード攻撃と不正侵入



ツール類を用いた不正侵入



2-5【パケット】

Packet

LANやインターネットの場合、伝送路をすべてのユーザで共有する必要があるため、やり取りするデータは、小さなデータ単位に分割して送信され、受信先で復元するという方式を採用している。このデータの分割単位をパケットという。パケットにはそれぞれ送信元や宛先などのアドレス情報を含むパケットヘッダーが付加されている。パケットは宅配便で送られる荷物の一つひとつ同様のイメージで各地を中継し、目的地へと送り届けられる。

2-6【ping】

Packet InterNetwork Groper

ネットワークでは、接続されたほかのコンピュータや機器が遠隔地に存在する場合もあるため、相手の状態を調べるのが困難な場合が多い。このため、これを知るためのプロトコルがICMPであり、ICMPを用いて手軽に相手の状態を確認することが可能なコマンドも存在する。これがpingである。pingは、WindowsやLinuxなど、多くのOSで対応している。

2-7【ポート】

Port

現在のコンピュータやPCでは、複数のプログラムを同時に機能させることができるが、このプログラムの一つひとつが、ほかのコンピュータやPCのプログラムの一つと通信をする際、互いのやり取り番号を決定しておく必要がある。これがポート番号であり、また、番号に対応する入出力部分がポートだ。通信を行う際、対応するポートを開かなければやり取りができないが、このポートがセキュリティリスクともなる。

2-8【ポートスキャナ】

Port scanner

コンピュータが特定ポートを用いて外部と通信を行う場合、必ずそのポートを開かなければならない。ポートスキャナは、特定のコンピュータのどのポートが開いているかを調べるためのツールである。開いているポート番号が分かると、そのコンピュータが用いているOSやアプリケーションなどを特定できる場合があり、そこから弱点を探ることも可能となる。

2-9【アプリケーションレイヤ攻撃】

Application Layer

サーバ上では多くのサーバソフトウェアが機能している。このアプリケーションのプロトコルに存在する脆弱性やセキュリティホールを突いた攻撃をいう。実際にはHTTPやFTP、メールのやり取りに用いるsendmailなどの脆弱性を突き、不正侵入を図る。

2

外部からのサービス拒絶攻撃

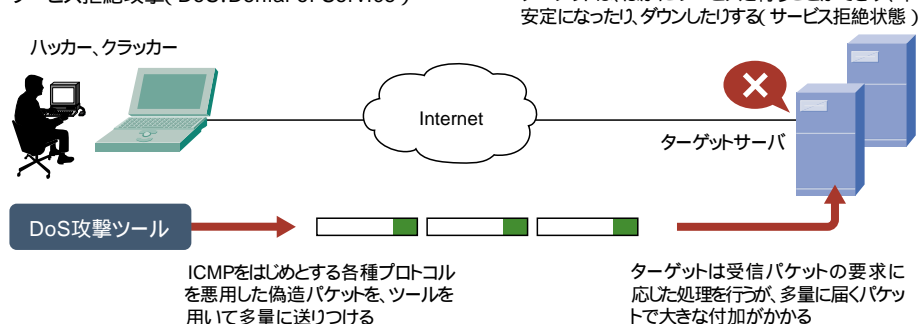
サービス拒絶攻撃(DoS:Denial of Service)²⁻¹⁰とは、文字どおり、サーバのサービスを不能状態に陥れることを目的とした攻撃で、この攻撃を受けたサーバのサービスは不安定、もしくは停止状態に陥ります。サービス拒絶攻撃は、サービス不能攻撃とも呼ばれます。

この攻撃の実現手法も多岐にわたりますが、代表的なものにICMP攻撃があります。**ICMP(Internet Control Message Protocol)**²⁻¹¹とは、ネットワーク内の機器同士で通信を行う際、一方に異常が発生した場合など、その状態を送信元に通知したり、診断したりする機能を持つ**プロトコル(Protocol:通信手順)**²⁻¹²です。ICMP攻撃とは、これを悪用することによって実現します。

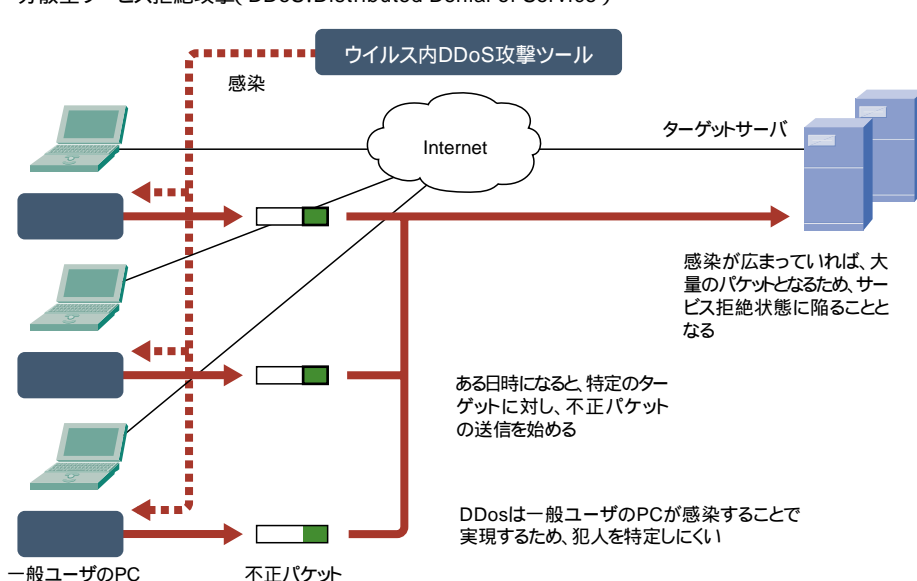
たとえばICMPには、始点制御メッセージタイプ4という機能がありますが、この偽造パケットを送信することで、ゲートウェイの転送速度を著しく下げたり、問題を発生させたりできます。また、経路変更メッセージタイプ5という機能の偽造パケットを送信することで、特定ルータの経路をクラッカーの意図する経路へと変更することが可能になる場合もあります。さらに、これらの攻撃を行うためのツールが存在したり、特定の日時に特定のサイトを攻撃する機能を持つウイルスも存在する場合もあり、数十万、数百万のPCなどから同時刻に攻撃を受け、サービス停止に陥るケースもあるのです。ちなみにこれは、**分散型サービス拒絶攻撃(DDoS:Distributed Denial of Service)**²⁻¹³といえます。

図3 DoS攻撃とDDoS攻撃

サービス拒絶攻撃(DoS:Denial of Service)



分散型サービス拒絶攻撃(DDoS:Distributed Denial of Service)



2-10【サービス拒絶攻撃】

DoS

(Denial of Service)

電子商取引のサイトがこの攻撃を受けた場合、顧客からの注文を受けることができなくなるため事態は深刻なものとなる。サービス拒絶攻撃は、ICMPなどのセキュリティホールを巧妙に狙うものと、単に大量のパケットを送りつけることによってサーバの負荷を増大させるものとに分類される。

2-11【ICMP】

Internet Control Message Protocol

インターネットを中心として用いられるプロトコル、TCP/IPには、あらかじめ用意されている通信機器の状態問い合わせプロトコルが存在する。これがICMP(Internet Control Message Protocol)だ。ICMPでは、問い合わせ方法と、それに応答する方法が規定されている。このため、通信機器やコンピュータ間で、状態の問い合わせと応答を、ネットワークを介しても行うことが可能となっている。

2-12【プロトコル】

Protocol

(通信手順)

インターネットには、異なるOSを実装するさまざまなメーカーのPCが接続されているが、問題なく双方向でやり取りすることができる。これは、インターネットに接続する際には、あらかじめ示し合せておいた通信手順を用いることが決められており、すべてのOS環境ではこの取り決めに基づいて通信を行うためである。この取り決めをプロトコルと呼ぶ。ちなみにインターネットにおけるプロトコルとは、数多くのプロトコルによって構成され、この総称をTCP/IPと呼ぶ。

2-13【分散型サービス拒絶攻撃】

DDoS

(Distributed Denial of Service)

ウイルス内に仕込まれているものが多く、ある日時になると、決められたサイトに対して不正パケットを送りつける。仮にこのウイルスが世界全域に多数感染していたならば、ターゲットとされたサイトがどのような状態となるかは、誰にでも容易に想像がつくに違いない。

2

ファイアウォールとDMZ

不正侵入や攻撃に対する保全対策

不正侵入やサービス拒絶攻撃などによって多大なる損害が発生するリスクがあるため、企業において、これらから身を守るための保全対策が不可欠となることについては、すでにふれたとおりです。次にこの保全対策を実現するための基本的な手法について、話を続けていくことにしましょう。

不正侵入や攻撃に対する保全対策実現の前段階として、企業規模で必要となるものに、インフォメーションプロテクションポリシー、もしくはセキュリティポリシーがありました。また、物理的セキュリティ対策と論理的セキュリティ対策の双方によって実現するセキュリティアーキテクチャが、強固なネットワークセキュリティを実現するためには必要でした。

一般に、企業ネットワークのセキュリティ対策には、不正侵入や攻撃の仕掛けにくいトポロジの構築が重要となります。つまり、このトポロジを実現することにより、これらの脅威から企業ネットワークを守ることが可能となるのです。そして、これにはファイアウォールという機器を用いて、DMZというゾーンを構築する必要があります。次にこの説明を進めます。なお、ここで紹介する保全対策は、最低限のセキュリティとなります。なぜなら、ファイアウォールに存在するセキュリティホールを攻撃することで、不正侵入を行う**スプーフイング** (Spoofing) ²⁻¹⁴などの攻撃も存在するからです。

ファイアウォールの基本機能

ネットワークセキュリティの重要性が浸透しつつある昨今では、ファイアウォールという言葉や機能もまた、広く知られてきています。

ファイアウォール (Fire wall) ²⁻¹⁵とは、「防火壁」のことであり、外部からの不正侵入や攻撃を阻止するための機器をいいます。現在、ファイアウォールの多くは、高度な機能を持つものとなっていますが、PCに、専用ソフトウェアをインストールすることで実現することも可能です。また、ファイアウォールは、外部からの攻撃を阻止する必要上、企業ネットワークと、インターネットやWANなど、外部のネットワークの接点に配置され、機能します。

ここで、ファイアウォールの機能を簡単に理解しておくことにしましょう。企業ネットワーク内のPCが、インターネットにアクセスしてサービスを受けるためには、PCと外部のネットワーク上に存在する相手先のサーバがやり取りをする必要があります。たとえば、Webのブラウジング時には、PCとWebサーバが、メールをやり取りする際には、PCとメールサーバがやり取りをしているわけです。ファイアウォールは、このやり取りの中間に介在することで、正しくない情報や、ウイルスに感染した情報を検知し、これを排除します。また、あらかじめ設定したサービスや情報以外のパケットが到達した場合にも、これを拒否するなどのフィルタリング機能を持つことで、企業ネットワーク内を常に安全な状態に保とうとするものです。

DMZ構築による企業ネットワークの保全

最近、企業のホームページを発信するWebサーバは、**データセンター** (Data Center) ²⁻¹⁶内に置くことが一般化してきています。しかし、企業ネットワーク内にWebサーバなどを配置し、不特定多数の顧客に対してサービスを提供する場合、インターネットと企業ネットワークの間にDMZを配置するのが基本的なネットワークポロジとされています。

DMZ (DeMilitarized Zone: **非武装地帯・緩衝地帯**) ²⁻¹⁷とは、ファイアウォールによって外部ネットワークと企業ネットワークの間に構築されるネットワークをいいます。一般的に、不

2-14【スプーフイング】

Spoofing

スプーフ (spoof) とは「騙す」という意味合いを持つ。ルータは、外部からの不正パケットを排除する機能を持つが、中には脆弱な部分を持つ製品も存在する。このルータに対して、たとえば内部からの要求に回答したパケットであるかのような偽造パケットを大量に送りつけることで、ファイアウォール内のネットワークを攻撃できる場合がある。これがスプーフイングだ。

2-15【ファイアウォール】

Fire wall

ファイアウォールは、さまざまなプロトコルに対応した情報のフィルタリングを可能とする。また、そのプロトコルの条件に合致したものを通過させるといった詳細動作を設定することもできる。このため、企業ネットワークに不要なデータすべての侵入を排除することも可能だ。ただし、ファイアウォールの設定条件を厳しくすると、その分、外部ネットワークへのアクセス時に取り扱えるサービスやデータの種類の制約が厳しくなるため、有効性を低下させることにもなる。ファイアウォールの設定にはバランスが要求される。

2-16【データセンター】

Data Center

自社情報やサービスの発信には、インターネットに常時接続されたWebサーバやアプリケーションサーバが不可欠となる。しかしこれを1日24時間安全な形で維持するためには、相応の管理運営コストがかかる。このため、これら顧客サーバを預かるとともに、これを安全な環境下でインターネットに常時接続する専門の代行業者が登場した。これがデータセンターだ。データセンターは、IDC (Internet Data Center) とも呼ばれている。

2-17【DMZ】

DeMilitarized Zone

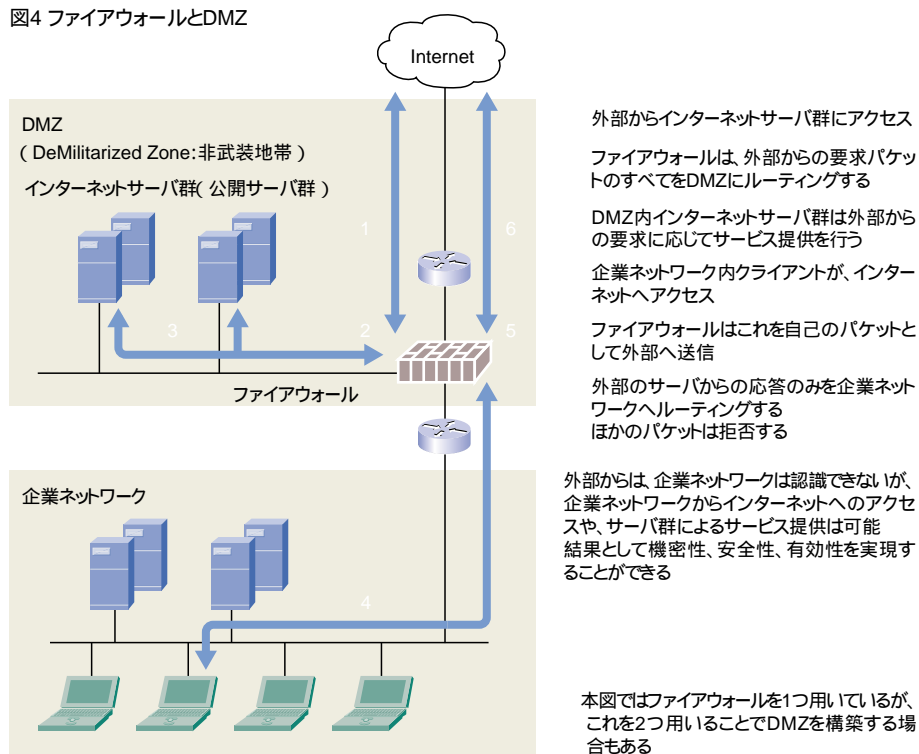
(非武装地帯・緩衝地帯)

外部とのやり取りが必要なサーバ群は、当然のことながら外部から認識できる位置に置かれていなければならない。しかしその一方で、企業ネットワークの内部は、外部から完全に隠れさせる必要がある。この両者のニーズをDMZは実現する。

2

特定多数に対してサービスを提供するためのサーバ群をここに配置します。外部ネットワークとDMZの間にあるファイアウォールは、配置されたサーバに対しての要求や、企業ネットワークからへ向けての応答などを通過させます。また、企業ネットワーク内部から外部への要求のすべてについては、ファイアウォールがこれを代理することが一般的です。つまり、外部ネットワークからはDMZ以外、企業ネットワークの存在は見えません。つまり、ネットワークセキュリティを高めながらも、企業ネットワーク内部から、外部ネットワークへのやり取りを実現する、機密性、保全性、有効性を同時に実現するためのトポロジだといえます。

図4 ファイアウォールとDMZ



2-18【セキュリティホール】

Security hole

セキュリティホールは、OSやアプリケーションソフトウェア、プロトコルなどすべてに存在するリスクがある。なお、OSの場合、セキュリティホールが発見されると、製造元では短い期間でこれを改修するためのパッチソフトウェアが公開される。これをインストールすればセキュリティホールは埋まる。しかし、これを放置しておく、非常に大きなリスクとなるので注意が必要だ。セキュリティホールが発覚すると、それを攻撃するツールもまた、ネットワーク上で公開される場合がある。これを用いれば、ネットワークの知識を何ら持たないユーザであっても、不正侵入や攻撃を行うことが可能となるからだ。

不正侵入検知とその進化

阻止するだけでは不十分な保全対策

企業ネットワークにファイアウォールを設置した場合、不正侵入や攻撃などのリスクを低減させることが可能です。ただしこれでは、万全とはいえません。なぜなら、ファイアウォール自体にセキュリティホールが存在する場合がありますからです。**セキュリティホール (Security hole)**

²⁻¹⁸とは、ハードウェアやソフトウェアの設計上のミスや、プログラミング段階におけるバグなどを原因として発生するセキュリティ上の弱点を意味します。これらは人為的なミスであり、まったく発覚しないものも存在します。このため、悪意ある第三者が、たまたまセキュリティホールを発見した場合、そのOS (Operating System) やシステムなど保全性はその瞬間に失われることになるのです。

このため、守りのみならず、仮に侵入を許してしまった場合、これをシステム管理者に通知したり、侵入経路や不正侵入者などを特定するための追尾を行うことも、ネットワークセキュリティには重要です。これを実現するシステムがIDSです。

2

IDSによる不正侵入検知

IDS (Intrusion Detection System: **侵入検知システム**)²⁻¹⁹とは、その名の通り、外部からの不正侵入を検知するシステムをいいます。IDSは、製品によって機能はさまざまですが、中心となる機能は、ネットワーク上を流れるトラフィックの監視となります。**トラフィック (Traffic)**²⁻²⁰とは、ネットワーク上を流れる情報やその量を意味する言葉ですが、このトラフィックが通常のサービスや量を逸脱した場合、これを異常状態と認識し、あらかじめ登録したシステム管理者への電話連絡や、不正侵入や攻撃の経路の特定、さらには、必要に応じて異常トラフィックの発生元からのアクセスを遮断したりする機能を持ちます。また、IDSによっては、企業ネットワーク内部のユーザがダウンロードしたソフトウェアやデータ、受信したメールの添付ファイルなどのすべてを監視し、ウイルス感染を検知した段階で、自動的にこれを隔離し、必要に応じて駆除するなどの機能を持つものもあります。

なお、これらの監視や検知は、通常**ログ (Log)**²⁻²¹としてIDSが記録に残すことから、これをもとにセキュリティ対策を再検討し、ファイアウォールやIDSなどに対する設定値を最適化することも可能となります。

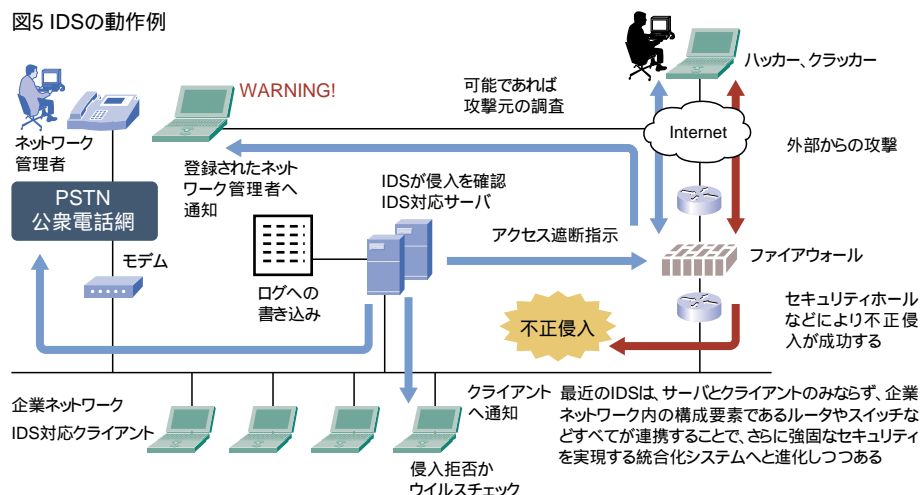
IDSと機器の連携による強固なネットワークセキュリティ

これまでのIDSは、企業ネットワーク内のサーバ、もしくはそれぞれのクライアントに対してインストールを行うことで、企業ネットワーク内の統合システムとして、総合的に機能するものが一般的でした。このため、企業ネットワーク内の一部のコンピュータやPCにおいて、監視制御や接続制御を実現するものがほとんどであり、ネットワーク全体の統合化システムを実現するまでにはいたっていませんでした。

昨今では、ネットワークセキュリティシステムの高機能化ニーズが進み、さらに強固な安全性を実現するための統合化システムも登場しています。たとえば、IDSの制御をコンピュータやPCのみで行うのではなく、企業ネットワークの構成要素であるスイッチやルータといった通信機器をも含めた連携動作を実現するものもあります。企業ネットワーク全体を、ネットワークセキュリティシステムとしてとらえてしまおうというものです。

このシステムにおいては、たとえば、企業ネットワーク内の1つのルータが外部からの攻撃を検知した場合、これを、ネットワーク管理者やIDSが機能するサーバに通知するとともに、アクセス拒否の指示を、ほかの全ルータやスイッチに対して瞬時に指示することが可能です。つまり、外部からの脅威に対して、企業ネットワーク全体で防御体制をとることが可能となるわけです。今後のIDSは、徐々にこの形態へ移行することが予想されています。

図5 IDSの動作例



2-19【IDS】

Intrusion Detection System

（侵入検知システム）

IDSでは、不正侵入の際に発生する典型的なトラフィック種類やパケット数など、特定の侵入パターンから、これらを検出する機能を持っている。このパターンのことをシグネチャ (Signature) と呼ぶ。

2-20【トラフィック】

Traffic

ネットワーク上を流れるデータ量のこと。通常、コンピュータネットワーク内でやり取りされるデータは、パケット、もしくはフレームといった細かい情報の単位に分割されてやり取りされる。ところが多くのユーザが一度にネットワークを利用して情報をやり取りしようとすると、規定の量を超えたトラフィックが発生することもある。企業ネットワークなどLANを構築する場合には、トラフィックを十分に考慮した設計が不可欠となる。

2-21【ログ】

Log

サーバがネットワーク上で動作し、多くのユーザからの要求に応える場合、そのすべては、さまざまな形態で記録される。この記録情報をログという。ログには、アクセスユーザのIPアドレスやアクセス時間、処理内容など多くの情報を含む場合が多い。また、ログを集計し表として出力するなどの解析機能を持つソフトウェアも多い。



【第3回】コンピュータウイルスの脅威とそのメカニズム

コンピュータウイルスとその種類

コンピュータウイルスとは何か

今回はコンピュータウイルスについて、その実態から対応策に至るまで、ひととおり学んでいくことにしましょう。そもそもコンピュータウイルスとはどのようなものなのでしょうか。

コンピュータウイルス(computer virus)とは、私たちが感染するウイルスとはまったく異なるものであり、コンピュータやPC上で動作するソフトウェアの1種です。このソフトウェアが「ウイルス」と呼ばれるのは、ネットワークや記憶媒体などを介することで、コンピュータからコンピュータへ、ファイルからファイルへと自己増殖を繰り返すようにつくられているためです。また、コンピュータウイルスに感染した場合、動作が不安定になったり、情報資産の多くを失ったりする被害を被ることになります。

現在、コンピュータの多くは、LANやインターネットなど、コンピュータネットワークを介することで、ほかのコンピュータとのやり取りが可能となっています。このため、1台のコンピュータがウイルスに汚染されると、ほかのコンピュータへと非常に短い期間で汚染が広がるリスクを生みます。コンピュータウイルスは、ネットワークセキュリティに対する大きな脅威として、社会的にも問題化しています。

コンピュータウイルスの種類と動作メカニズム

次にコンピュータウイルスの種類とメカニズムについて見ていくことにしましょう。コンピュータウイルスの種類としては、さまざまな概念と分類が存在します。ちなみに、感染する対象に注目するならば、3つの種類に分類することができます。

1つ目の**ブートセクタ感染型ウイルス**³⁻¹とは、コンピュータが起動する際の情報書き込まれているハードディスク内の**ブートセクタ(Boot Sector)**³⁻²や、**パーティションテーブル(Partition Table)**³⁻³などの**システム領域**³⁻⁴に感染するタイプのウイルスです。このため、コンピュータのスイッチを投入した段階で、OSとともにウイルスが**起動しメモリに常駐**³⁻⁵します。そして、フロッピーディスクをはじめとする記憶媒体を用いる際、OSの機能の一部としてふるまうことで、その記憶媒体に複製を作成し、ほかのコンピュータへと感染を広げます。次の**ファイル感染型ウイルス**とは、コンピュータ内のファイルのなかで、主に**COMやEXE**³⁻⁶などの実行ファイルに感染するタイプのウイルスです。実行ファイルとは、各種ソフトウェアやツール、コマンドなど、コンピュータを動作させるのに不可欠なものです。実行ファイルに感染した**ファイル感染型ウイルス**は、その**実行ファイル**³⁻⁷が実行された際、同時に起動し、自己増殖やファイルの破壊などを行うものです。

最後の**マクロ感染型ウイルス**もまた、ファイルへ感染するタイプのウイルスですが、実行ファイルではなく、マクロ機能を持ったアプリケーションの文書ファイルなどに感染するものです。**マクロ(Macro)**³⁻⁸とは、何度も繰り返す処理や複雑な操作手順をあらかじめ定義しておき、一連の処理を自動的に実行できるようにするプログラミング機能をいいますが、この形態で感染し、文書ファイルが開かれた段階でウイルスが機能するものです。メールに添付されて送られてきた**DOCファイル**³⁻⁹を開いたところ、ウイルスに感染したという経験をお持ちの方も少なくはないことでしょう。これがマクロ感染型ウイルスです。なお、このウイルスは、ファイル感染型ウイルスとして分類される場合もあります。また、発症あとにブートセクタへ感染するなど、複合的な動作機能を持つものも存在します。

3-1【ブートセクタ感染型ウイルス】

ファイル感染型ウイルスであっても、ブートセクタ感染型ウイルスと同等の機能を持つものがある。コンピュータ間の初期感染にファイルを経路として用いながらも、1度コンピュータ内で動作すると、ブートセクタに感染することで、以降OSとともに起動しようとするタイプのウイルスだ。

3-2【ブートセクタ】

Boot Sector

パーティションの先頭に存在する部分であり、OSを起動するために必要な情報が書き込まれている。このため、コンピュータの電源が投入された際には、まずハードディスク内のこの部分を参照したうえで、OS起動動作へと移行する。よってこの部分にウイルスが感染した場合、OS起動と同時にウイルスも起動し、メモリに常駐することとなる。

3-3【パーティションテーブル】

Partition Table

ハードディスク内の先頭に位置する部分に書き込まれているパーティション情報。もしくはそれを書き込むための領域をいう。パーティションテーブルの情報を読み込むことで、パーティション領域の分割認識が可能となる。

3-4【システム領域】

システム領域とは、主にOSが用いる領域を指す。システム領域は、ハードディスク内のみならずメモリ内にも存在する。一方、ユーザが利用する領域のことをユーザ領域と呼ぶ。

3-5【メモリに常駐】

プログラムのすべては、メモリ上に展開されたうえで実行される。メモリに常駐とは、常にメモリ上で動作する様をいう。たとえば、サーバソフトウェアは、常に動作し続けることで、クライアントからのサービス要求に応えることができる。これはまさに、メモリに常駐することによって実現するものである。

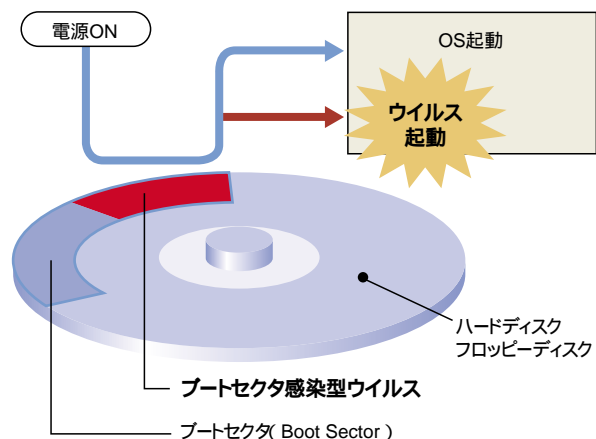
3-6【COMやEXE】

Windows環境における実行ファイルであり、COMやEXEなどの拡張子が付加されている。

3

図1 コンピュータウイルスの種類と動作メカニズム

ブートセクタ感染型ウイルス

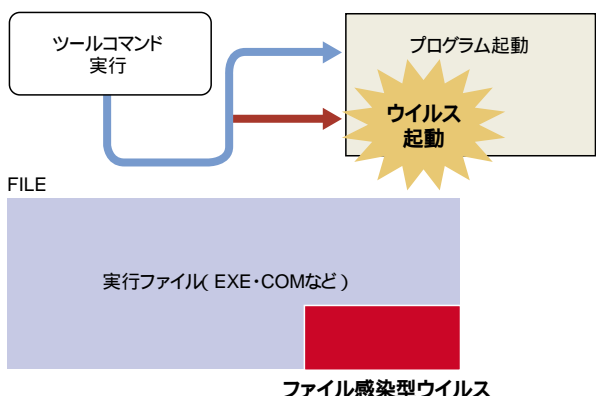


ハードディスクやフロッピーディスクなどのブートセクタ部に感染する

コンピュータの電源投入時、コンピュータはOSの格納場所を知るためにブートセクタを読みに行く

OS起動と同じタイミングでウイルスが起動しメモリに常駐する

ファイル感染型ウイルス

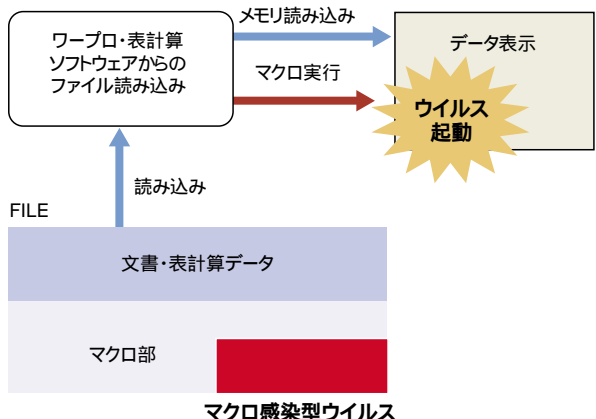


実行形式のファイルに感染する

このファイルをユーザが実行する

するとプログラムが起動すると同時にウイルスが起動し、メモリに常駐する(ブートセクタに常駐するものもある)

マクロ感染型ウイルス



ワープロや表計算ソフトウェアに対応するデータファイルのマクロ部に仕込まれている

ソフトウェアによってこのファイルを開く

データがメモリに読み込まれると同時に表示される。マクロ実行時ウイルスが起動し、メモリに常駐する(ブートセクタに感染するものもある)

3-7【実行ファイル】

実行ファイルとは、メモリにロードされた際にすぐに実行できるように、あらかじめオブジェクト形式で展開されたプログラムコードが格納されている。なおWindows環境において、実行ファイルに感染するウイルスのことを、PE(Portable Executive file)型ウイルスと呼ぶ。

3-8【マクロ】

Macro
ワープロソフトや表計算ソフトには、ユーザが実行すべき動作を、あらかじめ記述しておき、連続実行する機能が備わっている。これをマクロ機能という。マクロはそれぞれのデータファイル内に保存されるが、これを悪用することも可能。たとえば文書内にマクロ言語で記述したウイルスを密かに書き込んでおくことで、マクロ感染型ウイルスを作成することができる。

3-9【DOCファイル】

Documentファイル。マイクロソフト社のWordで用いる文書ファイルのこと。このファイルにもマクロ感染型ウイルスを忍ばせることができる。

3

動作で分類されるウイルスの種類

コンピュータウイルスは、動作で分類されるとともに、それぞれに異なる名称がつけられることもあります。たとえば、ほかのファイルを媒体とせず、単独で存在し、機能するプログラムであり、自らを複製することによって、ハードディスクの空き領域を占有したり、ファイルを破壊するウイルスを**バクテリア (Bacterium)**³⁻¹⁰と呼ぶ場合があります。また、ネットワークを介してほかのコンピュータに複製を送り込むことで、自己増殖を繰り返すプログラムをワーム (computer worm)、決められたアクセス回数や日時に動作を開始し、データの破壊を行うプログラムを**論理爆弾 (Logic Bomb)**³⁻¹¹と呼びます。

さらには、システム内に密かに入り込み、あたかも正しいコマンドやツールであるかのような動作を行いながら、その裏でデータの破壊やパスワードなどを盗聴し、特定のファイルに書き込んだり、メールを用いて外部に送信するなどの機能を持つプログラムを**トロイの木馬 (Trojan Horse)**³⁻¹²と呼びます。

なお、ウイルスのなかには、複数の機能を併せ持つものも多く、明確に分類することのできないものも存在します。

図2 動作で分類されるウイルスの種類

ウイルス	動作
バクテリア (Bacterium)	単独で存在し、機能する。自らを複製することにより、ハードディスクの空き領域を占有したり、ファイルを破壊する
ワーム (computer worm)	ネットワークを介してほかのコンピュータに複製を送り込むことで自己増殖を繰り返す
論理爆弾 (Logic Bomb)	決められたアクセス回数や日時に動作を開始し、データの破壊を行う
トロイの木馬 (Trojan horse)	コマンドやツールに成りすまし、データの破壊やパスワードの盗聴などを行う

複数の機能を併せ持つものも多い。この場合、明確な分類はできない

コンピュータウイルスの発症動作

次にコンピュータウイルスの動作について見ていきましょう。ウイルスは感染後、どのような悪事を働くことになるのでしょうか。ウイルスがコンピュータに感染すると、その直後、もしくは一定の潜伏期間を置いたあとに動作を開始します。これを発症と呼ぶ場合があります。

主だった動作としては、ディスプレイへの何らかのメッセージ表示、ディスプレイに表示された情報の改ざん、ハードディスク内のファイルの改ざんや破壊などが挙げられます。また、ハードディスク内の自己複製の作成など、多くのファイルに分身を感染させます。さらには、メールなどを介して複製をほかのユーザに送りつけるものや、ネットワークに接続されるコンピュータのセキュリティホールを探し出して攻撃を開始するもの、コンピュータ内部に保存された情報を、無作為にほかのユーザへ送信するものもあります。

一方、コンピュータウイルスは、自分の存在を隠すための多くの機能を持っています。たとえば、コンピュータウイルスには、ハードディスクの読み込み制御を操作したり、自らを暗号化するものもあります。これらは**ステルス (Stealth)**³⁻¹³機能と呼ばれます。また、感染と同時に突然変異を起こすことで、ウイルス対策ソフトの検知を免れようとするものもあります。コンピュータウイルスの機能は、年々巧妙化が進んできているのが現状です。

3-10【バクテリア】

Bacterium

バクテリアは、ファイルなどに感染するのではなく、単独で機能するとともに、自己増殖を可能とするプログラムとして、ウイルスと差別化されている。

3-11【論理爆弾】

Logic Bomb

アクセスした回数をカウントし、一定回数を超えた段階で発症する。論理爆弾に対して、一定の潜伏期間を経て発症するウイルスは、時限爆弾と呼ばれることもある。

3-12【トロイの木馬】

Trojan Horse

あるネットワークやサーバにアクセスする際、いつでもIDとパスワードの入力ガイダンスが表示されたなら、これを疑うユーザは非常に少ない。トロイの木馬は、この弱点を逆手に取り、正規の認証プログラムとすりかわる形でパスワードの搾取を行う。搾取情報は一時的に隠しファイルなどに置いておき、外部との通信タイミングが発生した段階で、特定の場所に向けて送信するなどの機能を持つ。場合によっては、多数のパスワードが搾取される。

3-13【ステルス】

Stealth

ステルスには、人目を忍ぶといった意味合いがある。レーダーに検知されないようにつくられた戦闘機をステルス戦闘機と呼ぶが、ウイルスにおけるステルス機能も同様であり、感染したファイルシステムから隠れる機能のことをいう。この機能を持ったウイルスの場合、たとえばファイラーなどで表示されないため、感染の発覚が遅れ、被害を拡大してしまうことがある。

3

図3 コンピュータウイルスの発症動作



- ・ ディスプレイへの何らかのメッセージ表示
- ・ ディスプレイに表示された情報の改ざん
- ・ ハードディスク内のファイルの改ざんや破壊
- ・ 自己複製の作成(ブートセクタ感染含む)
- ・ メールを介した複製や情報資産の送信
- ・ セキュリティホールへの影響
- ・ 自らの存在を隠すためのステルス機能

コンピュータウイルスへの対応策

感染の確認方法

今までの説明により、コンピュータウイルスのおおよそのイメージはご理解いただけたことでしょう。コンピュータウイルスの感染は、ファイルの破壊のみならず、システムやコンピュータの停止などさまざまな問題を引き起こすため、多大な損害を被ることもなりかねません。そこで、コンピュータウイルス感染への対応策を、あらかじめ個々に講じておく必要があります。

一般に、感染したコンピュータウイルスが発症すると、プログラムやソフトウェアが立ち上がりにくくなったり、全体に処理が遅くなるなどの症状が出始めます。これは、感染したウイルスが、**マイクロプロセッサ (Microprocessor)**³⁻¹⁴の負荷をまったく考慮せずに、ほかのファイルやコンピュータに感染するための処理を行うことによるものです。また、ハードディスクの領域が極端に少なく、まったく知らないファイルが数多く増える、ドライブのアクセスランプが点滅し続けるなどの症状が発生することもあるため、これらに該当する場合には、念のためウイルス感染を確認する必要があるかもしれません。

ウイルス感染の確認は、ウイルス対策ソフトウェアの開発元サイトへアクセスすることで、簡単に行うことができます。これについては、無料サービスとして提供されているものが多いため、定期的に行うとよいでしょう。

ウイルス対策ソフトとその機能

さて、このサービスによってウイルスが検出された場合には、次にどのようなことを行う必要があるのでしょうか。ウイルス確認サイトでは、確認と同時にウイルスを駆除してくれるものもあります。しかし、ウイルスによっては容易に駆除できないものもあります。このような場合には、ウイルス対策ソフトウェアを必要とします。**ウイルス対策ソフトウェア (Anti-virus Software)**³⁻¹⁵とは、ウイルスの監視や駆除を行うソフトウェアであり、**ワクチン (Vaccine)**³⁻¹⁶などとも呼ばれています。これらは、監視、検出、隔離、駆除などの機能を持っています。

ウイルス対策ソフトウェアは、メモリに常駐し、ウイルス感染や、感染によるシステムの異常動作を常時監視します。たとえば、定期的にハードディスクを巡回したり、ダウンロードやメールなど、外部からコンピュータ内にデータが入力される段階で、これを監視するのです。仮に感染の可能性のあるファイルが検出されたなら、まずこのファイルを、ほかのファイルに感染しない環境へ隔離したうえで駆除にあたります。これらの処理は、一連の流れとして自動化されたものや、イベントに応じてユーザの指示を仰ぐものなど、ソフトウェアやその設定によって異なります。

現在、企業の多くはLANを導入していますが、ウイルス対策ソフトウェアの形態もこれに対応してきており、LAN全体を監視するものから、それぞれのサーバを独自に監視するもの、クライアント用の監視ソフトまで、用途に応じたものが用意されています。

3-14【マイクロプロセッサ】

Microprocessor

CPUは、レジスタやキャッシュ領域など、さまざまな機能を有するユニットによって構成されるが、このなかで演算機能を持つユニット部をマイクロプロセッサと呼ぶ。CPU自体をプロセッサと呼ぶ場合もある。

3-15【ウイルス対策ソフトウェア】

Anti-virus Software

ウイルス対策ソフトウェアは、アンチウイルスソフトウェアや、ワクチンと呼ばれる。一般的に感染の監視と検知、隔離、駆除などの一連の機能を持ち合せている。また、ウイルス情報を常に最新に保つため、開発元の情報が更新された段階でこれを自動的にダウンロードする機能を持っている。

3-16【ワクチン】

Vaccine

ワクチンもウイルス対策ソフトウェアと同様だが、ウイルス情報をワクチンと呼ぶこともある。

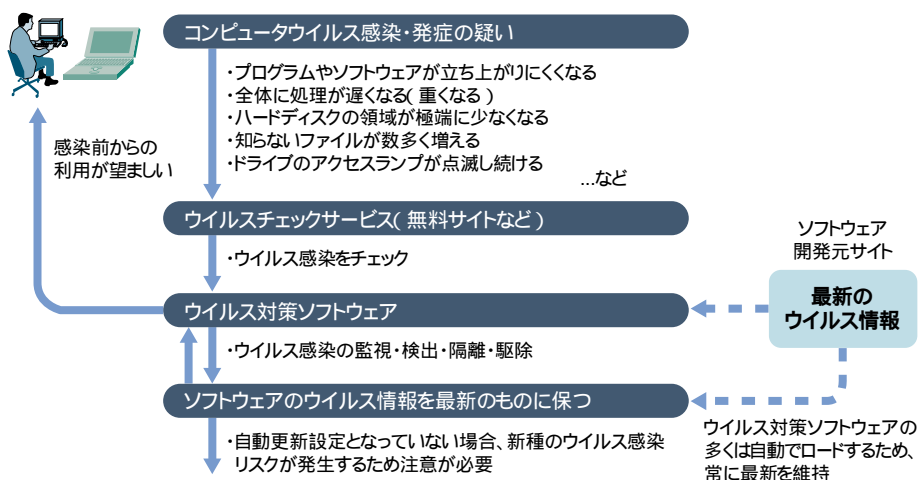
3

個々のユーザに不可欠な対応策とは

最近のウイルス対策ソフトウェアは、どれも非常に多機能であり、文字どおりウイルスの及ぼすリスクへに対抗する強力な戦力となります。ただし、ウイルス対策ソフトウェアの多くは、ウイルスの種類ごとにその検出と対策のためのウイルス情報が必要となります。つまり、ウイルス対策ソフトウェアで検出や駆除ができるのは、ウイルス情報として盛り込まれたものに限定され、それ以外のウイルスは、検出すらできない場合があります。ウイルス対策ソフトウェアの多くは、最新の**ウイルス情報**³⁻¹⁷を自動的にダウンロードする機能を持っています。しかし、常に最新のウイルス情報がダウンロードされているか否かについては、ユーザごとに確認が必要となります。

仮に、最新のウイルス情報がダウンロードされないまま、ウイルス情報にない新種のウイルスに感染した場合、ユーザが気づかない間に、ハードディスクやネットワーク全体に感染を広げてしまう可能性もあります。この点については、十分な配慮が不可欠となります。

図4 コンピュータウイルスへの対応策



3-17【ウイルス情報】

ウイルス対策ソフトウェアも、プログラムであることから、ウイルスの検知や駆除には、それを実行するための基本情報が必要となる。これがウイルス情報である。ウイルス情報に存在しない新種のウイルスに感染した場合、これを駆除する手立てがないため、被害を拡大させてしまう。ウイルス情報は常に最新の状態でなければならない。

ネットワーク全体に必要なソリューションとは

ネットワーク規模のウイルス対策

現在、コンピュータの多くは、単独で機能するよりも、むしろLANなどのネットワークに接続された状態で利用されることが一般的です。このため、個々のウイルス対策を行うのと同時に、ネットワーク規模でのウイルス対策も行う必要があります。たとえば、企業ネットワークの場合、その内部には、企業の重要な情報資産や、停止してはならない業務システムなどが存在します。また、企業ネットワークの多くは、ほかのネットワークと相互的に接続し、情報をやり取りする必要があるため、ネットワーク規模のウイルス対策がなされていなければ、ネットワーク全域に感染が及び可能性もあり、多大な損害を被るリスクを持つからです。

なお、ウイルス対策ソフトウェアには、ネットワーク規模で統合し、ウイルス対策にあたる製品も登場してきています。単体のウイルス対策ソフトウェアは、個々のコンピュータにインストールして用いますが、ネットワーク対応のウイルス対策ソフトウェアは、サービスを提供するサーバや共有ストレージ部などで機能するとともに、個々のウイルス対策ソフトウェアとも連携をとりなが

3

らウイルスに対抗します。また、グループウェアや**イントラネット (Intranet)**³⁻¹⁸などの業務システムと密着した形で、ネットワーク全体のウイルス対策にあたるものもあります。現在、企業の多くはLANを導入していますが、ウイルス対策ソフトウェアの形態もこれに対応してきており、LAN全体を監視するものから、それぞれのサーバを独自に監視するもの、クライアント用の監視ソフトまで、用途に応じたものが用意されています。

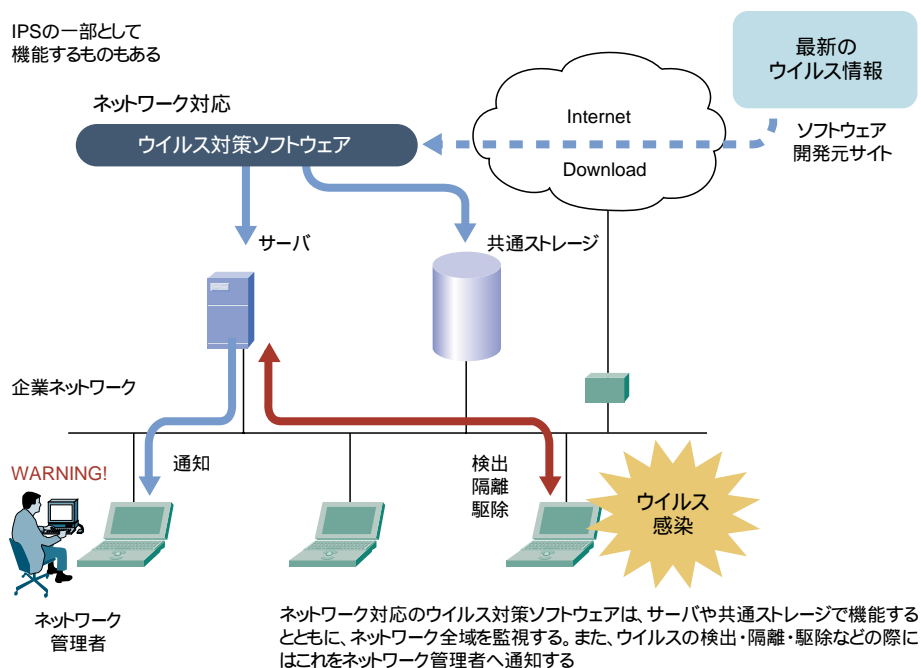
進化するネットワーク対応ウイルス対策ソフト

ネットワーク対応ウイルス対策ソフトウェアは、年々機能を向上し続けているものが多く、すでに**IDS (Intrusion Detection System)**³⁻¹⁹の一部として機能する製品もあります。このような製品の場合、ネットワーク全体の監視制御を1カ所のコンピュータで一元管理できるものが一般的です。仮にネットワークに接続されるコンピュータの1台がウイルスに感染した場合には、これを**ネットワーク管理者**³⁻²⁰や個々のユーザに通知します。これらの工程は、すべてログに記録され保管されます。

また、ネットワークに接続されるコンピュータが多くなると、ウイルス対策をまったく行っていない脆弱な環境が混入する確率も増大します。このため、ネットワーク対応ウイルス対策ソフトウェアでは、ネットワークを巡回し脆弱環境を持つコンピュータを検出する機能が重要となります。インターネットやWANなどのネットワークを介した遠隔監視機能を持つものも増えつつあります。

さらには、ネットワークがウイルスに汚染された場合の対応機能も重要です。これについては、感染と同時に駆除までの対応を図ると同時に、感染前のクリーンな環境へ容易に復旧できるか否かがポイントとなります。ネットワーク対応ウイルス対策ソフトでは、この復旧作業を機能として持つものも存在します。

図5 コンピュータウイルスへの対応策



3-18【イントラネット】

Intranet

企業ネットワーク内において、インターネットと同様のTCP/IPプロトコルを用いた通信を実現することで、WebサーバやFTPサーバなど、インターネットで享受できるサービスのすべてを、企業ネットワーク内で実現しようとするネットワークの形態。ちなみにこれを本支社間や得意先間で実現するものをエクストラネットと呼ぶ。

3-19【IDS】

Intrusion Detection System

侵入検知システムのこと。現在ではネットワーク規模のウイルス対策ソフトウェアと一体化して機能する場合が多い。

3-20【ネットワーク管理者】

コンピュータシステムや企業ネットワークを管理する責任者をシステム管理者と呼ぶ。企業ネットワークの規模によっては選任のネットワーク管理者やネットワーク管理部署の配置が不可欠となる。また、システム管理者のスキルは、そのまま管理するネットワークのセキュリティに反映してしまうため、高度な専門知識を有するスタッフを配置する必要がある。なお、独立行政法人・情報処理推進機構によって「システムアドミニストレータ」の資格試験が行われている。ネットワーク管理者養成には、この試験の合格を最初の目標として設定する場合が多い。

3

ウイルスの「ふるまい」に着目した対応策

今までの説明からもご理解いただけるように、最近のネットワーク対応型のウイルス対策ソフトは、多くの機能をもつ統合化セキュリティシステムへと進化してきています。しかし、ここにはまだ弱点が残されています。ウイルス対策ソフトウェアは、あくまでも発見された既存のウイルス、もしくはそれと同等の機能を持つウイルスに対してのみ機能するものであり、それ以外の未知のウイルスには対応ができない場合があるという点です。

このため、最近ではウイルス対策ソフトのベンダーと通信機器メーカーが協業し、互いに補間することでこれまでとは違った新しい対応策を実現し、こうした弱点を克服しようという動きも出てきています。その一例がウイルスの「ふるまい」に着目した対応策です。これについて少し具体的に見ていきましょう。

ウイルスが起こす何らかのアクションとは、かならずOSの機能を利用して実現しています。これらは、周辺機器への情報の読み書き、ポートを介したデータ通信、さらには**レジストリ (Registry)**³⁻²¹の改ざんなどに代表されます。また、ウイルスがこれらのOS機能呼び出す際、実際には、OSの**システムコール (System Call)**³⁻²²を利用します。この「ふるまい」に着目した対応策では、ウイルス自体を監視すると同時に、システムコールの異常な呼び出しを監視します。つまり、ウイルスが行う悪意ある行動自体も監視しようという発想です。これによって、たとえウイルス情報として認識されていなかった新しいウイルスであっても、その「ふるまい」によってこれを検知することが可能となり、取りこぼした新種のウイルスによって企業システムなどのネットワークが汚染されるリスクを回避できます。今後は、このような新しいアプローチによる統合的なウイルス対策が普及していくことでしょう。

3-21【レジストリ】

Registry

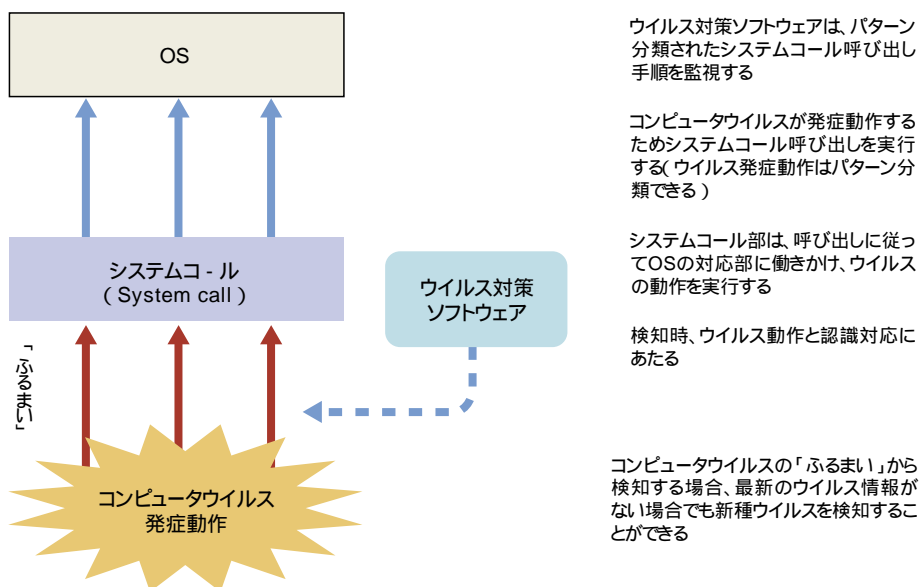
OSやアプリケーションソフトウェアが動作するうえで必要となる設定情報が書き込まれたデータベースであり、通常はソフトウェアが必要に応じて自動設定を行う。ユーザが独自に設定することも可能だが、設定ミスによっては、動作が不安定になったり起動できなくなる場合もある。コンピュータウイルスは、自分が動作しやすい環境をつくったり、自分の存在を隠べいしたりするために、レジストリの書き換えを行う場合がある。

3-22【システムコール】

System Call

OSは、コンピュータを動作させるうえでの基本的な制御を行うが、これらの機能はユーザがプログラムから利用することも可能となっている。そして、この際用いるのがシステムコールだ。システムコールに対して、動作に対応するコードや動作条件パラメータを引き渡すと、システムコールではこれを解析し、OSのそれぞれの機能を動作させる。ちなみにUNIXやLinuxなどの場合、システムコールが呼び出されると、直接カーネルに働きかけることで指示どおりの基本動作を実現する。

図6 ウイルスの「ふるまい」に着目した対応策





【第4回】企業ネットワークと認証技術

認証工程とアクセス制御技術

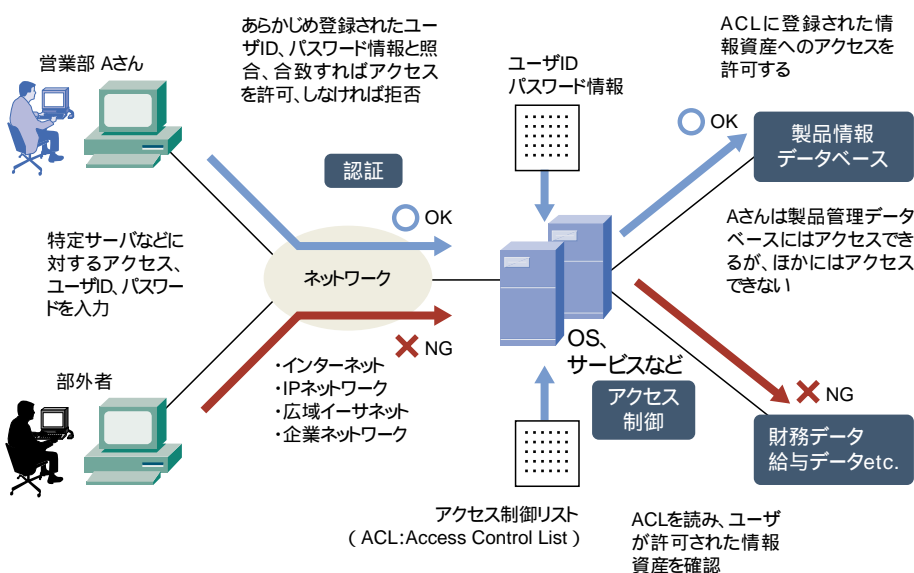
認証とは何か

企業ネットワークにおいて、認証は不可欠かつ非常に重要な技術の1つといえるでしょう。今回はこの認証技術を中心にお話を進めることにしましょう。

そもそも認証とは何でしょうか。「認証」という言葉を一般的な国語辞典で調べると、「一定の行為が正当な手続きで行われたことの証明」となっています。私たちは、日常生活においても、いたるところで認証行為を行っています。たとえば、会社や学校内に立ち入る際の、学生証や社員証の提示行為、書類などへの捺印やサインなど、本人であることの証明は、そのすべてが認証行為であるといえるでしょう。また、これを企業ネットワークにおけるネットワークセキュリティに置き換えて考えると、ネットワークやネットワーク内情報資産などに対して、内外のユーザがアクセスしてこれを利用する場合、その行為が正当なユーザによる正当な利用であるか、証明を行うことが認証行為ということになります。

つまり、**認証 (Authentication)** とは、ネットワークやネットワーク内のサービス、情報資産、特定のアプリケーションなどを利用する際、ユーザIDやパスワードを用いることで、本人の正当性を検証する作業を指します。

図1 認証とアクセス制御



4-1【ユーザID】

User Identification

ユーザを識別する記号のこと。現在ではネットワーク接続時やサーバアクセス時、アプリケーション利用時などさまざまな場所で、対応するユーザIDの入力が不可欠となっている。

4-2【パスワード】

Password

暗証コードのこと。ユーザIDと対で利用することが多い。短い言葉や生年月日、電話番号、家族氏名、キーボード配列、辞書に掲載のある単語などをパスワードに利用している場合、容易にこれを解読されてしまう場合がある。パスワードは分かりにくく、しかも長い英数字文字列で構成すると安全性が増す。

4-3【UNIX】

ユニックスと読む。米AT&Tベル研究所によって1969年に開発された。マルチユーザマルチタスクを実現するOSで、現在では大型コンピュータからPC対応まで幅広く移植され活用されている。

4-4【Linux】

リナックス、リヌクス、ライナックスなどと読む。UNIXを参考として一から作成されたOSであり、フリーで入手することができる。Linus B. Torvalds氏によって作られ、GPL (General Public License) のもとで配布される。Linuxは、実際にはOSの核となるカーネル部分を指す。よって、Linuxを利用するためには、各種のソフトウェアやツールなどを集めてパッケージ化されたディストリビューションを入手することとなる。現在、数多くのディストリビューションが登場している。

4-5【Windows Server】

マイクロソフト社によって開発されたサーバ専用OS。Windows NT 3.1、Windows NT 4.0、Windows 2000 Server、Windows Server 2003へ進化するとともにニーズ別に複数のエディションが提供されている。ちなみに現在パーソナルOSとして普及するWindows XPは、このサーバOSの流れをくむOSの1つである。

4

基本的な認証工程

さて、次に基本的な認証工程について簡単に見ていくことにしましょう。認証技術は、先にもふれたように、ネットワークやネットワーク内のサービス、情報資産、特定のアプリケーションなどさまざまなものに用いられています。皆さんは、家を出てから会社に到着し、PCの電源を入れて特定のアプリケーションやネットワークサービスを利用するまでの間、どのくらいの認証工程を必要としているでしょうか。毎日複数の認証工程を必要としている方も、決して少なくないでしょう。

認証におけるやり取りで、個人の**ユーザID (User Identification)**⁴⁻¹と**パスワード (Password)**⁴⁻²を入力する方法が、最も一般的な動作です。たとえば、UNIX⁴⁻³やLinux⁴⁻⁴、Windows Server⁴⁻⁵などのサーバ専用OSのすべては、**マルチユーザマルチタスクOS (Multi-User Multi-Task OS)**⁴⁻⁶であるため、これらを利用する際は、必ずユーザIDとパスワードの入力が要求されます。ユーザIDとパスワードを、あらかじめOS側に登録しておけば、OSは、入力されたこれらの情報が、登録情報と等しいかをチェックするだけで、相手が正規ユーザであることを認識し、アクセスを許可することができます。

アクセス制御

認証工程によって、正規ユーザであることが証明された場合、それを許可したシステムやサーバでは、ユーザに対して、すべての権限を与えて良いものでしょうか。たとえば、営業部に所属する一社員が、企業ネットワークに正規ユーザとしてアクセスをしたとしましょう。彼は製品情報データベースにアクセスし、営業先からでも、製品の詳細スペックを調べてプレゼンテーションに利用することができます。しかし、一般公示前の企業内財務データや人事データ、さらには役員報酬や給与などの**データベース (Database)**⁴⁻⁷へも自由にアクセスできるとしたら、いくら彼が正規ユーザであるとしても、問題があるでしょう。つまり、企業ネットワークにおいては、単にネットワークアクセスの認証工程を実施するだけでは、問題があるということです。

よって、認証工程と同時に、企業ネットワークやシステムが行うべき制御が存在します。これが**アクセス制御**です。**アクセス制御 (Access Control)**⁴⁻⁸とは、ネットワークやネットワーク内サービス、情報資産別のアクセス可否をユーザごとに制御することを指し、一般的なサーバOSだけでなく、各種データベースやネットワーク対応のアプリケーションにおいても設定することが可能です。また、この設定情報を**アクセス制御リスト (ACL: Access Control List)**⁴⁻⁹と呼びます。アクセス制御は、認証工程の際、アクセス制御リストを参照することで実施されます。なお、アクセス制御リストはネットワークを構成するルータもしくはスイッチの設定情報、たとえば特定のインタフェースやVLANでのパケット通過の許可や拒否などの設定を指す場合もある。

認証 (Authentication)	アクセス制御 (Access Control)
ネットワークやネットワーク内サービス、情報資産、OSや特定のアプリケーションなどの利用に際し、ユーザIDやパスワードを用いることで、本人の正当性を検証する作業	認証工程の後、アクセス制御リストの情報をもとに、ネットワークやネットワーク内サービス、情報資産別のアクセス可否をユーザ毎に制御する

4-6【マルチユーザマルチタスクOS】

Multi-User Multi-Task OS

サーバOSとは、複数ユーザがアクセスし、リモート環境で用いる機能を備えている。これがマルチユーザ機能である。一方、マルチタスクとは、1台のコンピュータで、複数の処理を同時にこなす機能のことである。つまり、マルチユーザ機能を持つOSは、基本的にマルチタスク機能も持ちあわせている。

4-7【データベース】

Database

データの貯蔵やその操作、検索を実現するための情報管理技術をいう。また、データベースソフトウェアは、大容量のデータを整理・保存し、効率的に検索できる環境を提供する。通常これをデータベース管理システム (DBMS: Data Base Management System) と呼ぶ。

4-8【アクセス制御】

Access Control

アクセスユーザごとにユーザの動作を制限するための制御を指す。UNIXやUNIX系OSのすべては、ユーザごとに、ファイル単位のアクセスや書き込みなどを詳細に制御することができる。また、最近のネットワーク対応アプリケーションソフトウェアにおいても、詳細なアクセス制御が可能になってきている。

4-9【アクセス制御リスト】

ACL: Access Control List

ネットワークの構成要素には、ルータやスイッチなど、さまざまな通信機器が存在する。これらは、あらかじめ設定した情報をもとに、トラフィックを制限したり、特定のユーザやデバイスによるネットワークの使用を制限する機能を持っている。これらの設定情報、もしくは実際の制御機能を、アクセス制御リストと呼ぶこともある。

4

クライアント / サーバシステムと成りすまし・否認

クライアント / サーバシステムとは

ネットワークセキュリティにおける成りすましや否認行為を説明するうえで、クライアント / サーバシステムについて簡単に整理しておく必要があります。なぜなら、これらの行為は、基本的に2つのコンピュータ間の通信において発生し得る脅威であるためです。

クライアント / サーバシステム (Client / Server System) とは、クライアントとサーバという2つの異なる立場をとるもの同士が、やり取りをすることによって成り立つコンピューティングシステムをいいます。

サーバ (Server) とは、サービスを提供する立場のコンピュータ、もしくはソフトウェアであり、クライアント (Client) とは、サービスを受ける側のコンピュータ、もしくはソフトウェアを指します。例えるならば、店を構えてサービスを提供する業者がサーバ、その店を訪れてサービスを受けたり物を買入したりする消費者がクライアントということになります。ところで、実際の店において、万引きや強盗などが発生するものの、一般に成りすましや否認という犯罪行為をあまり聞かないのはなぜでしょうか。これは、実際の店と顧客、サーバとクライアントには、大きな相違点が存在するからにはほかありません。それは、相手との実際の対面がなされるか否かという点です。つまり、クライアント / サーバシステムにおいて、やり取りを行う両者は、あくまでも遠隔地に存在するコンピュータであることから、相手の顔や表情を見ながら取引をすることができないのです。

成りすましと否認

さて、クライアント / サーバシステムとその問題点についてご理解いただいたうえで、次に成りすましと否認についても、簡単に整理しておくことにしましょう。なお、これらは第1回においても簡単に説明しています。ここでは、復習の意味も含めて読み進んでみてください。

成りすましとは、正規ユーザや特定の人間、業者などに成りすますことにより、不正侵入や、物品の購入、金銭の移動などによる搾取などを行う犯罪行為をいいます。ネットワークの場合、アクセスユーザとなる相手の顔が見えないので、仮に正規のユーザIDとパスワードが漏洩してしまえば、容易に成りすましによる不正侵入が起こってしまいます。また、**電子商取引 (Electronic Commerce)**⁴⁻¹⁰の場合、業者に成りすまして架空の取引を行い、金銭を盗み取ったり、ユーザに成りすまして商品を盗み取るなどの犯罪が発生することも考えられます。このため、ネットワーク利用ユーザや、企業ネットワークを持つ企業において、成りすましに対する何らかの対応策が不可欠となるのです。

一方、否認とは、商取引後に否定する行為をいいます。現在では、**B to B**⁴⁻¹¹、**B to C**⁴⁻¹²、**C to C**⁴⁻¹³など、数多くの形態の電子商取引が存在します。このため、あらゆる商品の購入や販売が可能となるだけでなく、企業間の契約などもインターネット上を介して行われています。しかしこれらもまた、コンピュータ同士のやり取りであることから、たとえば大量の注文を受けて出荷したものの、後にこの注文を否認するなどの行為もあり得ない話ではありません。よって、電子商取引を行う企業では、注文が確実に行われたかという行為自体を立証するための何らかの技術が不可欠となります。

4-10【電子商取引】

Electronic Commerce

Eコマースなどともいう。ネットワークを利用した商取引のこと。インターネットの爆発的な普及により、電子商取引市場も急速に拡大した。電子商取引の場合、実際に店舗を構える必要がないため、小資本での参入が可能だ。また、対象とする顧客は全世界であることから、商圏の制約を受けることがない。インターネット利用者の7割以上が、電子商取引の経験者とされる。

4-11【B to B】

Business to Business

ビジネスとは企業を意味する。つまり、企業間取引を意味する。現在ではインターネットやIPネットワークを介した、企業間の自動取引が多く利用されるようになってきている。EDIやWeb-EDIなどがB to Bを実現するために利用されている。

4-12【B to C】

Business to Consumer

ここでいうConsumerとは、一般消費者のこと。つまり、企業と一般消費者間の取引を意味する。インターネットを利用したショッピングなどの形態がこれに相当する。

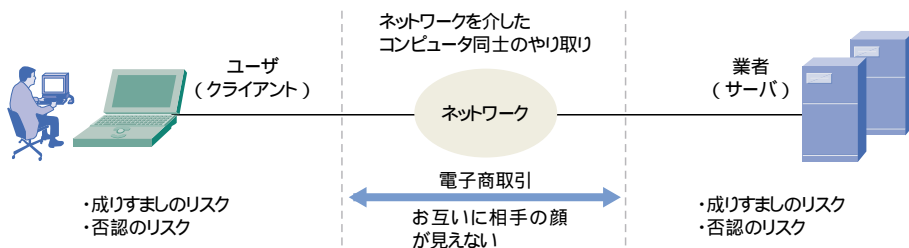
4-13【C to C】

Consumer to Consumer

一般消費者同士の取引のこと。一般消費者の直接的な商取引としては、あまりなじみがないかもしれない。しかし、特定の業者が手助けをする形であれば、この商取引は現在、インターネットで活発にやり取りされている。ネットオークションがまさにC to Cであるからだ。

4

図2 クライアント/サーバシステムと電子商取引のリスク

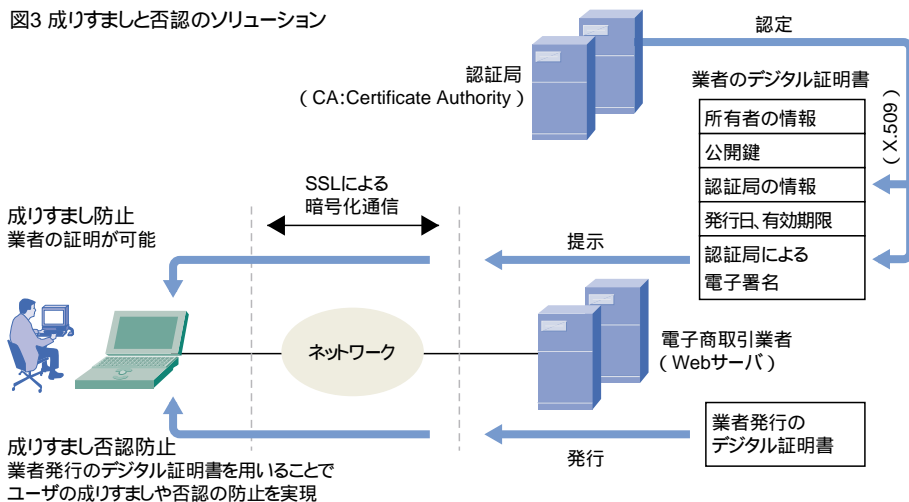


成りすましと否認のソリューション

電子商取引の多くは、実際には、サーバとクライアントといったコンピュータ間でやり取りされる取引といえます。これに起因し、成りすましや否認行為が発生するわけです。これらの解決策として最も簡単な方法は、正しい業者であるか、確実に注文を本人が行っているかなどの証明を、第三者信用機関によって行う対応策が考えられます。

現在の電子商取引の多くは、**Webサーバ(Web Server)**⁴⁻¹⁴と**Webブラウザ(Web Browser)**⁴⁻¹⁵間における**HTTP(HyperText Transfer Protocol)**⁴⁻¹⁶通信によって実現します。また、このなかでも、個人情報のやり取りや、成りすまし、否認行為防止として、HTTPに対して**SSL(Secure Socket Layer)**⁴⁻¹⁷によるデータの暗号化機能を付加した**HTTPS(Hypertext Transfer Protocol Security)**⁴⁻¹⁸というプロトコルを用います。通常のホームページのやり取りにおける情報は、**平文(Plain Text)**⁴⁻¹⁹によってネットワーク上を流れますが、これを暗号化することで、ネットワーク上での盗聴を防止するやりとりがHTTPSというわけです。また、このSSL通信を実現するためには、所有者の情報と公開鍵、認証局情報、発行日や有効期限などの情報を含むデジタル証明書を用います。**デジタル証明書(Digital Certificate)**⁴⁻²⁰とは、電子商取引における身分証明書に相当するものであり、身分証明書発行機関である**認証局(CA:Certificate Authority)**⁴⁻²¹による電子署名が付加されます。つまりデジタル証明書は、その所有者が作成するとともに、認証局が認定し署名したデータ群です。よって、業者がユーザにデジタル証明書を提示することで、正しい業者であることが証明できます。また、業者がユーザごとにデジタル証明書を発行し、これを元にユーザが取引をするといった工程を踏むことで、明らかに正しい注文を行ったことや、途中で改ざんがされていないなどの証明を行うことが可能となるのです。

図3 成りすましと否認のソリューション



4-14【Webサーバ】

Web Server

一般ユーザがWebのブラウジングを行う場合、特定のURLをWebブラウザソフトで指定することにより実現しているはずだ。この場合、Webブラウザソフトが、URLに対応するIPアドレスのWebコンテンツ配信サーバにアクセスをし、情報の提供を要求している。この配信サーバをWebサーバと呼ぶ。

4-15【Webブラウザ】

Web Browser

Webブラウザは、Webの閲覧を行う際に利用するソフトウェアのことである。Webブラウザとしては、Internet ExplorerやOpera、Netscape Navigator、Mozillaなどが有名だ。また、これ以外にも、Mosaic View、SlipKnot、Lynx、Emacs-W3、NetShark、EasyView、MacWebなど、これまでの歴史のなかで多くのWebブラウザが存在した。

4-16【HTTP】

Hyper Text Transfer Protocol

Webにおいて、Webコンテンツをやり取りする際に用いられている通信プロトコル。Webブラウザがこのプロトコルに則した形でHTML情報を要求すると、Webサーバがこれに応じた情報を配信、一方Webブラウザでは、必要となる画像などを再度要求するとともに、これらの情報をWebページとして表示している。これらのやり取りの手順をHTTPでは規定しているわけである。

4-17【SSL】

Secure Socket Layer

WebサーバとWebブラウザの間でやり取りするデータを暗号化することが可能な、インターネットで安全に通信を行うための暗号化通信プロトコルである。SSLは、米ネットスケープ・コミュニケーションズ社によって開発された。当初この機能は、Netscape Navigatorへの対応が図られたが、現在ではInternet Explorerを始めとする多くのWebブラウザに実装されている。

4-18【HTTPS】

HyperText Transfer Protocol Security

HTTPにおけるやり取りは、テキスト部分などに暗号化が施されていない。このため、HTTPでそのままやり取りする情報は、ネットワーク上で盗聴される可能性があり、電子商取引における個人情報のやり取りには適さない。そこで、HTTPの動作をそのまま行うことができるものの、やり取りされる情報を暗号化できる新たなプロトコルが加わることとなった。これがHTTPSである。

4

認証システムの問題点とソリューション

認証システムの問題点

先に認証技術の基礎的な部分について学びました。アクセスユーザが、あらかじめ登録したユーザIDやパスワードを入力することで、正規ユーザであることを証明する一方、ネットワークやサーバ、アプリケーション側では、これを確認したうえでアクセスやサービス提供を許可するというものでした。当初、この認証工程を設けることで、ネットワークやサーバは、常に安全な環境を維持できるとされました。しかし最近では、非常に脆弱なセキュリティとして、問題視されるようになってきています。ユーザIDやパスワードが、悪意ある第三者に漏洩してしまった場合、成りすましによる不正侵入が、いとも簡単に起こってしまうからです。また、実はUNIXやLinuxにおいては、ユーザのパスワードに対応する情報を、ほかのユーザが参照することができる場合もあります。このパスワードファイルは、暗号化されているため、簡単に解読することはできませんが、ユーザが短い文字列や辞書などに存在する単語をそのまま利用していた場合、比較的容易に解析がおこなわれてしまうこともあるのです。

このため、今後の認証システムにおいては、簡単な情報だけで正規ユーザであるか否かを判断するのではなく、二重三重の技術が不可欠なのです。また、これらの認証システムは、実際のセキュリティシステムにすでに組み込まれているものもあります。

精度が向上しつつある認証システムとその種類

基本的な認証工程とは、ユーザIDとパスワードのやり取りによるものですが、これでは盗聴による漏洩などが発生した場合、容易に不正侵入を許してしまいます。そこで、パスワード自体を毎回変更する**ワンタイムパスワード**(One Time Password)というシステムが開発されました。ワンタイムパスワードとは、文字通り1回限りの使い捨てパスワードを用いることで、本人認証を行うものです。ただ、1回限りでは、毎回パスワードを示し合わせる必要があり、非常に手間がかかりそうです。しかし、これらの制御は、サーバとクライアントの双方で機能する専用のソフトウェアによってやり取りされるため、ユーザに負担をかけることはありません。また、パスワードが毎回変化するので、これを盗聴しても意味がありませんし、漏洩したとしても、不正侵入には利用できません。

一方、先にもふれたように、SSLでは、オプションとしてクライアント認証機能も用意されているため、サービス提供者側が発行したデジタル証明書をクライアントにあらかじめ発行しておくことで、サーバ側がクライアント認証を実現することができます。

さらには、今後ネットワークにおける本人認証でも普及することが予想される技術として、**バイオメトリクス**(Biometrics:生物計測学的認証)とは、あらかじめ登録した顔形や指紋、手のひらの静脈パターン、網膜情報をデータベース化しておき、その都度、カメラやセンサーなどで得た本人のものを照合することで本人認証を行うものです。バイオメトリクスによる本人認証の場合、成りすましの脅威を大方回避することが可能となります。本人しか持ち得ない生体的特徴を、本人認証の照合データとして用いるとともに、これを暗号化してやり取りすることで、比較的容易に、強固な認証を実現することができるわけです。

4-19【平文】

Plain Text

暗号化されていないテキストを平文という。これに対して、暗号化されたテキストを暗号文と呼ぶ。

4-20【デジタル証明書】

Digital Certificate

電子商取引における身分証明書に相当するものであり、ITU(国際電気通信連合)が1988年に勧告した電子鍵証明書などの標準仕様であるX.509で規定されるデータ群のこと。デジタル証明書には、証明すべき所有者の情報と公開鍵、認証局情報、発行日や有効期限などの情報が含まれる。また、身分証明書発行機関である認証局(CA)による電子署名が、これらに附加される。認証に際する問題とは、ネットワークを介してやり取りされる公開鍵が誰によって作成されたか特定しにくい点だ。デジタル証明書の場合、認証局としての第三者信用機関が、公開鍵を作成した相手を証明する。公開鍵の出所が保証されていれば、これを用いてやり取りを行うことで、相手方が成りすましていないことを確認することができる。

4-21【認証局】

CA(Certificate Authority)

電子商取引で用いられるデジタル証明書や電子身分証明書などを発行する第三者信用機関のこと。

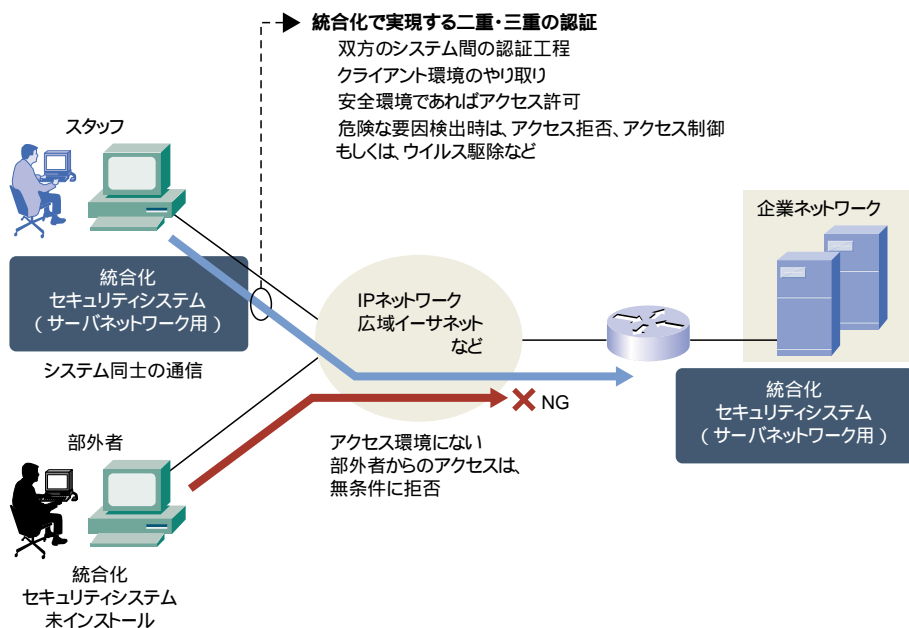
4

統合化によって進化する認証システム

現在の統合化セキュリティシステムは、今まで学んできた認証システムとアクセス制御を組み合わせることで、より強固なセキュリティを実現しようとしています。ここでは、最後にそのメカニズムの一部を簡単にご紹介しておくことにしましょう。

外部からのアクセスについての基本的な認証工程とは、現在でもユーザIDとパスワードが中心となっています。しかし、仮に企業ネットワークのセキュリティを考えた場合、インターネットなど公のネットワークとは異なり、アクセス対象ユーザを限定することが可能となります。つまり、スタッフや得意先などにアクセスが限定されるため、認証システムも、これらのユーザを対象とすればよいわけです。すなわち、対象となるアクセスユーザのすべてに、クライアント用統合化セキュリティシステムのインストールを義務付ければ、このソフトウェアをインストールしていないユーザからのアクセスを排除することができるはずです。また、インストールしてあったとしても、通常の認証工程を通過できなければ、アクセスはできません。さらに、通常の認証工程を通過したとしても、クライアント内にウイルスなどの感染やその可能性を検出した場合、提供サービスを限定したり、これを駆除するための専用サイトへのアクセス制御を、統合化セキュリティシステムが自動で行うことも可能となります。つまり、統合化セキュリティシステムを、全クライアントも含めた形で実現することで、さらに強固なセキュリティを実現することができるわけです。

図4 統合化によって進化する認証システム



5



【第5回】セキュリティに不可欠な暗号化技術

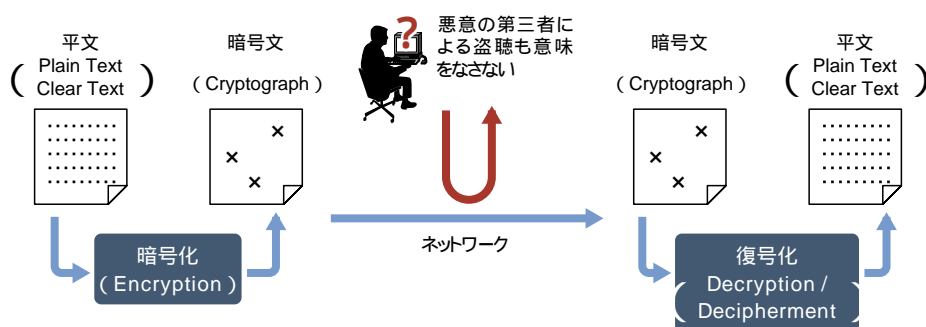
盗聴を防止するための暗号化と復号化

暗号化とその必要性

今回は暗号化技術について学んでいくことにしましょう。ネットワークコンピューティングにおいて、いまや暗号化技術は不可欠なものです。それは、ネットワークを介した通信が、何らかの伝送媒体を介してデータ伝送されるからです。遠隔地に存在するコンピュータやPCが通信を行う場合、その情報は、無線やメタリックケーブル、光ファイバケーブルなど、多くの伝送路によって伝送されており、その際、多くのルータやスイッチなどの、通信機器による中継処理を経由しています。そして、この部分において、悪意ある第三者が中継情報を盗聴することも可能です。つまり、ネットワークコンピューティングにおいては、伝送途中にデータを捕まえて、これを盗聴や改ざんされるリスクがあるのです。

そのため、このリスクを低減させる措置が必要となります。最も簡単な方法は、盗聴されるようなネットワークを利用しないことですが、広域ネットワークすべてを自分の管理下に置くことは困難です。そこで、悪意ある第三者がデータを盗聴しても、これを解読できない形で伝送する方法が用いられるようになりました。これが暗号化です。つまり**暗号化(Encryption)**⁵⁻¹とは、誰もが読み取ることのできる平文(Plaintext/Cleartext)を、あらかじめ決められた規則に則って、読み取ることのできない形式、つまり暗号文(Ciphertext)へ変更することを指します。ところで、暗号化されたデータが、盗聴や改ざんされることはなくても、宛先の相手を読み取らなければ意味がありません。そこで、暗号化されたデータを元のデータ(平文)へ戻す作業が必要になります。これを**復号化(Decryption/Decipherment)**⁵⁻²と呼びます。つまり暗号処理とは、暗号化と復号化という工程によってはじめて成り立つのです。暗号化処理には、大きく分けて、共通鍵暗号方式と公開鍵暗号方式があります。次にこれらについて説明をしていきましょう。

図1 暗号化と復号化



5-1【暗号化】

Encryption

暗号化は、通信途中の悪意ある第三者による盗聴や改ざん防止に役立つが、それ以外では有料コンテンツの配信などにも用いられている。これらは、基本的に暗号化されたコンテンツを配信するが、料金を支払ったユーザにのみ与えられた鍵、もしくは機器によって復号化し、それを利用することが可能である。

5-2【復号化】

Decryption/Decipherment

暗号化された情報を参照するには、これを元の平文へ復元する必要がある。これが復号化であり、強固で安全な暗号方式ほど、暗号化、復号化のプロセスは複雑で、CPUへの負荷も大きくなる。最近ではこれらの処理工程を完全にチップ化し、ハードウェア的に処理するものも多くなっている。これなら、暗号化と復号化が複雑になっても、CPUに負荷をかけなくて済む。

5

共通鍵暗号方式(Common Key Cryptosystem)

暗号処理は、暗号化と復号化の過程で鍵(Key)⁵⁻³を用いる方法が一般的です。コンピュータにおける暗号処理の鍵は、64ビットや128ビットなど、多くのビット列からなる数値を使います。つまりこの数値でデータの置き換えを行うことにより、暗号化しているわけです。これを踏まえて、共通鍵暗号方式を見ていくことにしましょう。

仮に、東京本社LANに保存されている社外秘データを、大阪支社LANへ転送すると想定してみましょう。このデータを平文のままインターネット経由で転送する場合、途中で盗聴や改ざんのリスクが発生するので、ある鍵を用いてこれを暗号化したうえで、大阪支社へと転送します。一方、大阪支社では、届いたデータを平文へ復号化しなければなりません。この際、東京本社で暗号化したときに用いた鍵が必要となります。つまり、暗号化通信を行う両者では、互いにあらかじめ示し合わせた同一の鍵を持っている必要があります。このように、暗号化と復号化に同じ鍵を用いる暗号方式を**共通鍵暗号方式(Common Key Cryptosystem)**⁵⁻⁴と呼びます。共通鍵暗号方式は、同じ2つの鍵を使用するので、対称鍵暗号方式(Symmetric Key Cryptosystem)と呼びます。また、鍵自体秘密にしておく必要があるため、秘密鍵暗号方式(Secret Key Cryptosystem)と呼ばれることもあります。

共通鍵暗号方式は、鍵を共有することから、暗号化、復号化、それぞれの処理工程を単純化しやすいというメリットを持つ反面、この鍵が第三者に漏れしただ段階で、暗号化が無意味になってしまうデメリットがあります。

公開鍵暗号方式(Public Key Cryptosystem)

共通鍵暗号方式は、情報をやり取りする両者が同じ鍵を利用する暗号方式でした。一方、両者が異なる鍵を用いて情報をやり取りする暗号方式もあります。しかもこの方式は、鍵を一般公開してしまうというユニークなものです。これを公開鍵暗号方式と呼びます。

公開鍵暗号方式(Public Key Cryptosystem)⁵⁻⁵では、暗号化するための鍵と復号化するための鍵の二つを用意することで、暗号化と復号化を行います。公開鍵暗号方式で実際に暗号化通信を行うためには、まず情報を受信する側が送信元に対して、暗号化に用いる鍵を送信します。これが公開鍵となります。送信元では、この公開鍵を用いて、情報を暗号化します。この場合、公開鍵で暗号化しているので、誰もがこれを復号できそうに思えます。しかし公開鍵暗号方式において、公開鍵で暗号化された情報は、同じ鍵では復号化できない仕組みになっています。暗号化された情報は、受信側にある、公開鍵とペアの秘密鍵でしか復号化できないのです。このため、公開鍵や公開鍵によって暗号化された情報が、悪意ある第三者の手に渡っても、これを解読することはできないのです。公開鍵暗号方式は、2つの異なる鍵を用いることから、非対称鍵暗号方式(Asymmetric Key Cryptosystem)とも呼ばれています。

また、公開鍵暗号方式は、電子署名への応用も可能です。この場合、自分の秘密鍵で暗号化した情報を相手に送り、相手方は受け取った情報を公開鍵で復号化します。公開鍵で復号化するので、暗号化自体は意味をなしません。誰もが復号化することが可能だからです。ただし、公開鍵で復号化できるということは、秘密鍵で確かに暗号化したという証になるため、送信元の情報であることが証明できます。つまり、電子的な署名として機能するのです。このように公開鍵暗号方式は、暗号以外の用途でも用いられています。

5-3【鍵】

Key

暗号方式で文字どおりキーとなるのが、この鍵の存在だ。鍵がなければ暗号化や復号化ができないが、仮に鍵が盗聴された場合、暗号方式は無効化してしまうからだ。なお、暗号方式における鍵とは、実際には数値であり、この数値を用いた計算により暗号化が実現できる。そのためこの値は、大きなものでなければ解読されてしまう。しかしあまりに大きな値の場合、暗号化と復号化に時間がかかりすぎ、CPUに負荷をかけすぎると副作用も発生する。

5-4【共通鍵暗号方式】

Common Key Cryptosystem

共通鍵暗号方式は、データをやり取りする両者が、同一の鍵を持っている必要がある。そのため、鍵自体のやり取りは、盗聴されない安全な方法で行うなど細心の注意が必要だ。ただし、暗号化と復号化の工程自体は、公開鍵暗号方式に比べてシンプルになるので、高速な処理を実現できる。よって、大量の情報を暗号化して送る場合には、共通鍵暗号方式が用いられることが多い。

5-5【公開鍵暗号方式】

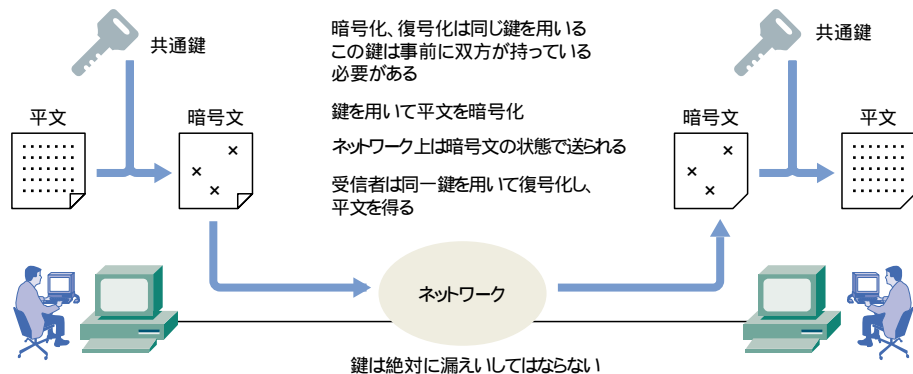
Public Key Cryptosystem

公開鍵暗号方式は、公開された鍵で暗号化すると、それと対になる秘密鍵でしか復号化できない。よってこの方式では、公開鍵の漏れいを心配する必要がない。公開鍵暗号方式は、RSA方式や楕円曲線暗号方式、ElGamal方式などを基本アルゴリズムに採用している。

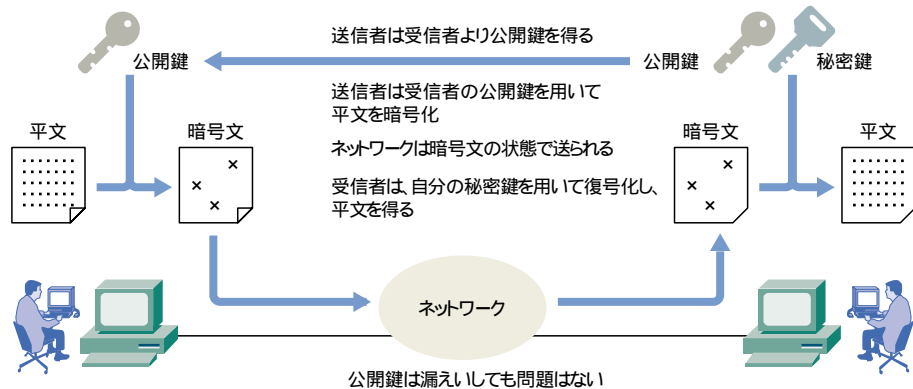
5

図2 共通鍵と公開鍵の暗号方式の相違

共通鍵暗号方式



公開鍵暗号方式



5-6【換字】

Substitution

平文の文字を、別の数字や記号、文字などに置き換える暗号処理のこと。1文字を別の1文字に置き換えることもあるが、1文字を複数文字に対応させることもある。一般に換字には、暗号化、復号化に際して対応表が用意されるが、これが共通鍵として機能することとなる。

5-7【転置】

Permutation

「あんごう」という単語も「うんあご」と並び替えてしまえば、意味を成さないひらがなの羅列になってしまう。しかしこの並び替えの法則を、あらかじめ両者間で示し合わせておけば、これを復号化し、元の平文を得ることができる。これが転置式暗号だ。

5-8【ハッシュ関数】

Hash Function

数字や文字の羅列を入力し、これに対応した固定長の擬似乱数であるハッシュ値を発生させる演算手法。UNIXなどのパスワード情報は、ハッシュ関数によってハッシュ値に変換し保管されており、元のパスワード情報を管理していない。ユーザがパスワードを入力すると、これをハッシュ関数に通して得るハッシュ値によって、正しいかどうかを判断する。なお、ハッシュ関数は一方方向性関数であり、ハッシュ値から元のパスワードを予測することは不可能である。ハッシュ関数にはRSA Data Securityの開発したMD5 (Message Digest 5) が多く用いられる。MD5では、必ず128ビット(16バイト)のハッシュ値を得ることができる。

暗号化の基本的メカニズム

暗号化の基本的メカニズム

暗号化とは、先に説明したように、送信すべき平文を決められた規則に従い、第三者が読み取れない形式へと変更することです。次に実際の暗号化メカニズムについて、学んでいくことにしましょう。

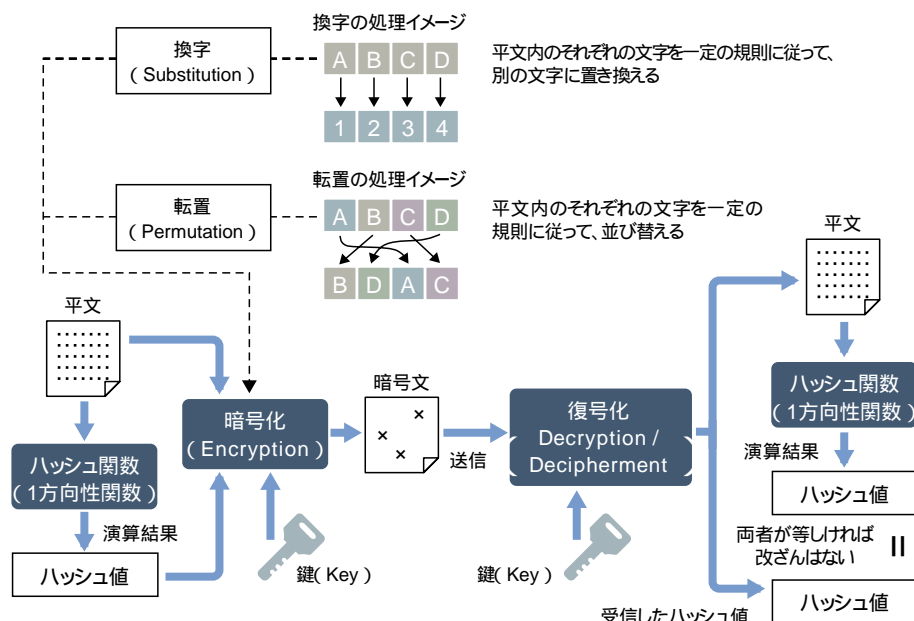
暗号化は、容易に解読されることのないよう、複雑な工程を経る構造になっています。しかしこの工程も、突き詰めていけば、換字と転置と呼ばれる比較的理解しやすい2つの処理の組み合わせによって成り立っているといえます。**換字 (Substitution)**⁵⁻⁶は、平文内の各々の文字を、一定の規則に従って、別の文字に置き換える処理をいいます。また、**転置 (Permutation)**⁵⁻⁷は、平文内の各々の文字の位置を、一定の法則に従って並び替える処理を指します。つまり暗号化とは、一定の規則に従って文字を置き換えたり、文字位置を入れ替えたりする処理なのです。

また暗号化では、通信途中の改ざんをチェックすることができるシステムも必要になります。これには、固定長の擬似乱数を発生させる**ハッシュ関数 (Hash Function)**⁵⁻⁸を使います。ハッシュ関数は、順方向への計算が容易である一方、その逆方向への計算が困難な関数

5

なので、**一方向性関数(One-Way Function)**⁵⁻⁹と呼ばれます。平文をハッシュ関数に入力することで得たハッシュ値を、平文と一緒に暗号化して送信するのです。すると受信側は復号化により平文とハッシュ値を取り出せます。また、平文を送信元と同様のハッシュ関数に入力し、送られてきたハッシュ値と同じ値を得ることができれば、平文が改ざんされていないことを証明できるのです。

図3 暗号化の基本的メカニズム



共通鍵暗号方式に採用された暗号方式

次に、長い間用いられてきた代表的な暗号方式であるDESについて、その暗号化メカニズムを簡単に見ていくことにしましょう。**DES(Data Encryption Standard)**⁵⁻¹⁰は、IBM社によって開発された共通鍵暗号方式のひとつです。DESは、1960年代にすでにその暗号化メカニズムが発表され、1977年には米国の政府機関であり、工業関連の技術標準化団体である**米国標準技術局(NIST:National Institute of Standards and Technology)**⁵⁻¹¹によって連邦標準規格として採用されています。

DESは、ブロック暗号と呼ばれる方式を採用しています。**ブロック暗号(Block Cipher)**⁵⁻¹²とは、暗号化の対象データを固定長のブロック単位で処理する共通鍵暗号方式を意味します。ブロック暗号には**Feistel型**⁵⁻¹³や**SPN型**⁵⁻¹⁴などがありますが、DESではFeistel型を用います。なお、コンピュータの高速化に伴い、DESでは暗号の安全性が不十分になったため、**トリプルDES(Triple DES:3DES)**⁵⁻¹⁵という暗号方式も登場しています。これは、文字どおりDESを三重に組み合わせることで、DESの脆弱性を補うものです。

また、米国標準技術局は1997年、次世代の暗号化標準としての**AES(Advanced Encryption Standard)**⁵⁻¹⁶の公募を行い、応募のなかから、「Rijndael」という暗号方式を選びました。「Rijndael(ラインダール)」は、ベルギーの暗号開発者であるJoan Daemen氏とVincent Rijmen氏によってSPN型を採用し開発された暗号方式です。SPN型のSPN(Substitution Permutation Network)は、換字と転置の工程によって成り立つブロック暗号です。AESは、ソフトウェアやハードウェアに対する実装が容易なため、現在ではさまざまなソフトウェアやデバイスに組み込まれています。

5-9【一方向性関数】

One-Way Function

入力、処理、出力の流れに不可逆性を持った関数。たとえば $y=f(x)$ において、 x を与えられ、 y を算出するのは容易だが、 y を与えられても、 x を導き出すことが困難な関数である。出力値から入力値を求めることが困難な特性を暗号化に適用して、解読のリスクを限りなく少なくしようとするものである。

5-10【DES】

Data Encryption Standard

DESが連邦標準規格として採用されたのは、暗号化アルゴリズムの公開とともに、あらゆる攻撃に実際に行い、その安全性を証明したことによる。DES以前にも暗号方式は存在したが、それまでの方式は、アルゴリズムが公開されていないブラックボックス的なものであったため、安全性の確認が得られなかった。

5-11【米国標準技術局】

NIST

(National Institute of Standards and Technology)

1988年、それまでのNBS(National Bureau of Standards)が再構築される形で誕生したのがNISTだ。工業技術の標準化支援団体だが、標準暗号化技術の策定機関として広く知られている。

5-12【ブロック暗号】

Block Cipher

平文を一定のブロック毎に分割したうえで、各々を暗号化する方式を指す。このブロック暗号は、通常換字と転置の処理を複雑に組み合わせることで構成される。なお、ブロック暗号に対して、平文を1ビット、もしくは1バイト単位で逐次的に暗号化する手法をストリーム暗号、もしくは逐次暗号と呼ぶ。

5-13【Feistel型】

フェステル氏によって開発されたことからこの名称がつけられた。

5-14【SPN型】

ブロック暗号を構成する方法は、Feistel型と同様だが、1回のラウンドでブロック全体を処理する場合が多い。

5

公開鍵暗号方式の定番・RSA

一方、公開鍵暗号方式で用いられる暗号方式として、RSAが挙げられます。RSA(Rivest-Shamir-Adleman Scheme)は、Ronald Rivest氏、Adi Shamir氏、Leonard Adleman氏、3人の開発者のイニシャルから名付けられました。RSAは暗号化と復号化に、巾乗剰余演算を使用しています。たとえば、ある数を何回も乗算し、 n で割った余りをとる計算を、コンピュータは瞬時に行うことができます。しかしその逆算、つまり素数の籍を因数分解することは、瞬時にできません。これを応用して、解読されにくい強固な暗号化をするものです。この不可逆性は、たとえば、水に絵の具を混ぜるのは簡単でも、その色水から、水と絵の具を分離するのは難しいといえ、イメージが分かりやすいでしょう。この性質を応用し、先に説明した一方向性関数を作成することで、解読困難な暗号文を作ろうというわけです。

なお、公開鍵暗号方式では、今後、楕円曲線暗号が普及することが予想されます。楕円曲線暗号(ECC:Elliptic Curve Cryptosystem)とは、1985年、偶然にも、Koblitz氏とMiller氏がほぼ同時に考案した公開鍵暗号方式で、文字どおり楕円曲線という数式を用いて、公開鍵と暗号鍵を作成し、これにより暗号化と復号化を実現するものです。楕円曲線暗号は、RSAの4分の1から8分の1程度の鍵の長さで、RSAと同等の安全性を確保できます。このため、RSAに比べて暗号化と復号化に際して負荷が少ないとされています。

図4 暗号方式(暗号アルゴリズム)の種類

暗号方式	暗号アルゴリズム	説明
共通鍵暗号方式	DES (Data Encryption Standard)	IBM社によって開発されたブロック暗号 1977年、米国標準技術局により連邦標準規格に
	トリプルDES (Triple DES / 3DES)	DESの脆弱性を補うために、DESを三重に 組み合わせることで暗号化する
	AES (Advanced Encryption Standard)	Rijndael(ラインダール)という暗号方式を公募から採用 DESに次ぐ暗号方式
公開鍵暗号方式	RSA (Rivest-Shamir-Adleman-scheme)	巾乗剰余演算を用いて、暗号化を実現する
	楕円曲線暗号 (ECC:Elliptic Curve Cryptosystem)	楕円曲線という数式を用いて暗号化する RSAより短い鍵で、同等の安全性を実現できる

5-15【トリプルDES】

Triple DES(3DES)

トリプルDESには、3つの鍵を用いるEEE方式と、2つの鍵を用いるEDE方式がある。EEE方式とは、暗号のE(encryption)に3処理、つまり3回の暗号化処理を行う。また、EDE方式のD(decryption)である復号化処理を、2つの暗号化処理の間で行うことで、最終的に暗号文を得ようとするものである。

5-16【AES】

Advanced Encryption Standard

AESは実質的に、DESの後継となる暗号方式だ。AESは、ブロック長や鍵長を、128、192、256ビットの3種類から選択することが可能であり、より柔軟度の高い暗号化を実現することができる。

5-17【VPN】

Virtual Private Network

仮想私設網と訳される。インターネットなど公のネットワーク内に、あたかも私設網であるかのような安全な通信環境を構築する技術。現在ではOSやアプリケーションなどで実現することができるが、ルータやファイアウォールも、この機能を持つものが多くなった。

暗号化とカプセルングによるVPNの実現

VPNによって実現する安全な通信環境

これまで、インターネットやIPネットワークなど、公の広域ネットワークにおける情報の盗聴や改ざんのリスクと、それを防止する暗号化技術について、学んできました。暗号化技術は、盗聴や改ざんの防止には役立ちますが、実際、ユーザが暗号化や復号化を意識して行うのは大変です。また、これをソフトウェアが自動的に行うと、CPUに負荷をかけてしまうため、効率のよい通信環境とはいえなくなります。つまり安全性を重視するために、ある程度、個々のPC環境のパフォーマンスや手間を犠牲にしているのです。

そこで、個々のパフォーマンスや手間を犠牲にせずに、しかも公のネットワークを利用した安全な通信をするためのメカニズムが登場しました。これがVPNです。VPN(Virtual Private Network)⁵⁻¹⁷とは、公のネットワーク内に、第三者による盗聴や改ざんなどのリスクのない仮想的なプライベートネットワークを構築することで、安全な通信環境を実現します。もともと、本社と支社に構築された各々の企業ネットワークを、安全な通信環境で相互接続する場合は、専用線などを用いるのが一般的でしたが、これでは多大な運用コストがかかります。しかし、VPNを利用することで、比較的安価なWANやインターネットを利用しながらも、安全な通信ができるようになりました。

5

VPN実現のための基本的メカニズム

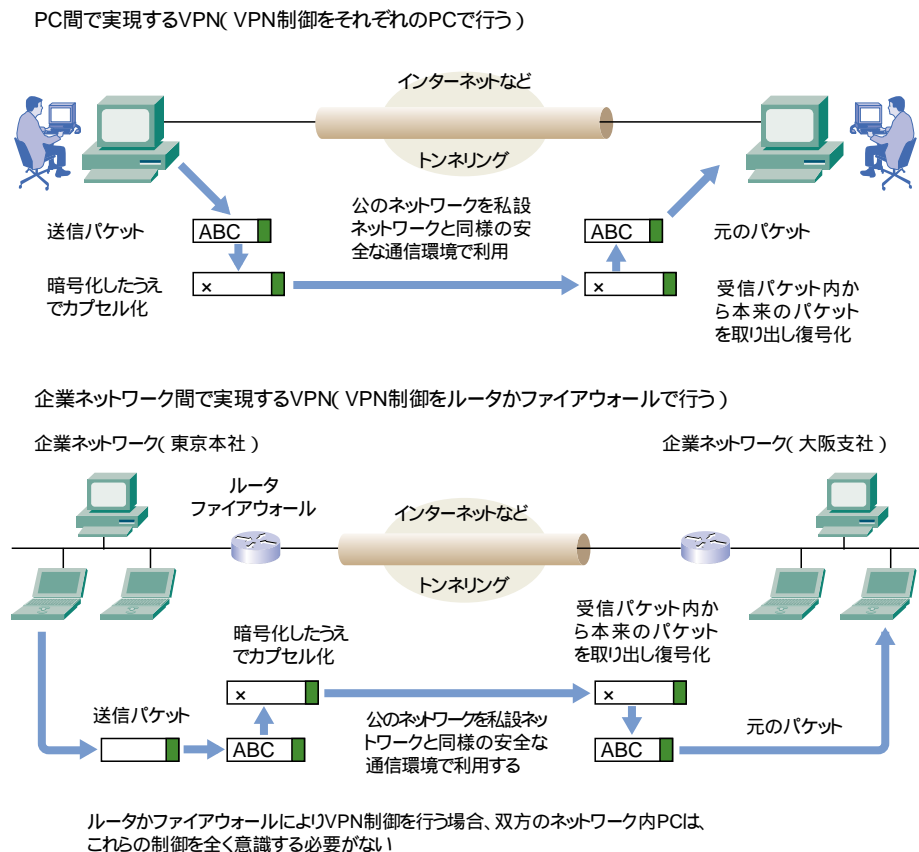
VPNは、公のネットワーク内に、どのようにして仮想的なプライベートネットワークを構築するのでしょうか。

もともとVPNの利用目的は、盗聴や改ざんのない安全な通信環境を、公のネットワーク内に実現することです。たとえば、東京本社と大阪支社を、インターネットなど公のネットワークで相互接続したとします。このままでは、やり取りされる情報が盗聴されかねないため、それぞれのPC内で、やり取りする情報を自動的に暗号化して送信し、受信時に自動的に復号化するソフトウェアを用いると想定してみましょう。これなら、ユーザが意識せずに東京本社と大阪支社間に安全なプライベートネットワークを構築できるはずですが、ただしこの場合、それぞれのPC環境で暗号化と復号化を行うので、その分パフォーマンスの低下をまねいてしまいます。

そこで、これらの処理すべてを、インターネットと本支社ネットワークの接点に存在するルータが行うこととしてみましょう。ルータは、内部から外部へ向けたパケットの内容を暗号化し、これを新たなパケットで包んで送信します。また、外部から届いたパケットに対しては、パケット内の情報を取り出して復号化し、内部へと中継します。これなら、本支社内のそれぞれのPCでは、暗号化や復号化などの処理を一切行うことなく、公のネットワークを利用した安全な通信環境を得ることが可能になるはずですが。

なお、一連のVPN制御は、公のネットワーク内に専用のトンネルを構築して安全な通信環境を実現していることから、**トンネリング(Tunneling)**⁵⁻¹⁸と呼ばれることもあります。

図5 VPN実現のための基本的メカニズム



5-18【トンネリング】

Tunneling

トンネリングとは、特定のプロトコルでやり取りされるネットワーク内に、ほかのプロトコルのパケットを通過させる手法。実際には、既存のパケットを、通過させるネットワークが用いるプロトコルに対応したパケットでカプセル化する。IPv4パケットを、IPv6ネットワーク上に通過させるなどの場合にも用いられる。

5

VPNで用いられる暗号化プロトコル

次にVPNで用いられている暗号化プロトコルを学ぶことにしましょう。

現在VPNで用いられている暗号化プロトコルのなかで、最も一般的なものに、IPsecとSSLがあります。

IPsec(Security Architecture for Internet Protocol)⁵⁻¹⁹は当初、インターネットプロトコルなどの標準化組織であるIETF(Internet Engineering Task Force)⁵⁻²⁰がVPN(Virtual Private Network)の標準プロトコルとして規定したものです。もともと、インターネットやIPネットワークを介した情報は、パケットの単位に分割されてやり取りされていますが、IPsecは、これに暗号化機能を追加したものとイえます。なお、IPsecは、**認証ヘッダ(AH: Authentication Header)**⁵⁻²¹、**暗号ペイロード(ESP: Encapsulating Security Payload)**⁵⁻²²、**IPペイロード圧縮(IPComp: IP payload compression)**⁵⁻²³、**IKE(Internet Key Exchange)**⁵⁻²⁴の4つのプロトコルで構成されています。またIPsecは、暗号方式としてDESやAESを用います。

さらに、**SSL(Secure Sockets Layer)**⁵⁻²⁵もVPNに利用されています。このVPNを**SSL-VPN**⁵⁻²⁶と呼びます。私たちがインターネットにアクセスしてさまざまな情報を得る場合、HTTP(Hyper Text Transfer Protocol)と呼ばれるプロトコルによって、Webの情報提供を受けています。また、Webサーバに住所氏名やカード番号など、個人情報を送信する場合、ネットワーク上での改ざんや盗聴を避けるため、サイトの多くが、HTTPS(Hypertext Transfer Protocol Security)と呼ばれる暗号化機能付プロトコルを使っています。SSL-VPNは、このプロトコルを利用することで、暗号化や認証を実現し、クライアントとサーバ間に一時的なVPNを構築します。

このため、サーバにアクセスしてきた不特定多数との1対多の関係で、いつでもVPNを構築することができます。またその際、クライアント側は特別なソフトウェアを必要としません。仮に特別なセキュリティ制御を行う場合でも、WebブラウザがWebサーバからJavaアプレットをダウンロードして組み込むようにしておけば、ユーザはプログラムを意識することなく、Webサーバとの間にVPNを構築し、安全な通信環境を得ることができるのです。

図6 VPNで用いられる暗号化プロトコル

使用プロトコル	暗号アルゴリズム
IPsecによるVPNの実現 (Security Architecture for Internet Protocol)	IPsecは暗号化や認証などの機能を持ったIP(Internet Protocol)である(DESやAESを用いる) これを用いることでVPNを実現できる
SSLによるVPNの実現 (Secure Socket Layer)	暗号化にSSLを用いる 業者が不特定多数のユーザ間とVPNを実現する際に用いられる 場合が多い(HTTPSを用いる)

5-19【IPsec】

Security Architecture for Internet Protocol

インターネットなどのネットワーク上で、分割データとしてやり取りされるパケットは、IPというプロトコルを用いて、相手先まで送り届けられる。IPsecは、単にパケットを届けるだけでなく、これに暗号化や認証機能を付加したプロトコルといえる。

5-20【IETF】

Internet Engineering Task Force

インターネットの最新技術標準化促進団体。

5-21【認証ヘッダ】

AH

(Authentication Header)

やり取りされるデータを認証するためのプロトコル。

5-22【暗号ペイロード】

ESP

(Encapsulating Security Payload)

文字どおり暗号化するためのプロトコルであり、IPパケットの機密性を確保する。また、オプションとして認証を行うことが可能なため、安全性も確保できる。

5-23【IPペイロード圧縮】

IPComp

(IP Payload Compression)

IPsecを用いてやり取りするパケットの内容を圧縮するためのプロトコル。これを用いることで、本来のデータより少ない量で通信することができる。

5-24【IKE】

Internet Key Exchange

パケットの暗号化・復号化に不可欠な鍵を、通信を行う両者間で安全にやり取りするためのプロトコル。暗号ペイロードを実現するための準備段階で機能するもの。

5-26【SSL】

Secure Sockets Layer

米ネットスケープ・コミュニケーションズ社によって開発された技術。Webサーバとクライアント間で、相手の認証を行ったり、やり取りされる情報をネットワーク上で盗聴されないよう、暗号化することができる。

5-25【SSL-VPN】

Internet Key Exchange

SSLを用いることで実現するVPN。業者がアクセスユーザとVPN環境でやり取りする場合などに用いられる。



【第6回】統合型セキュリティシステム の概念

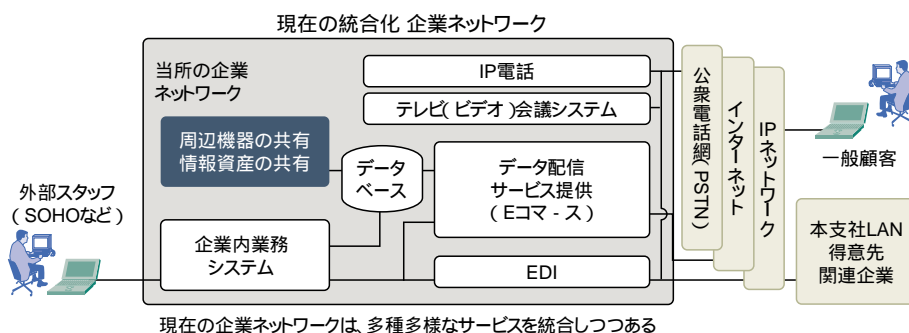
ネットワーク規模のセキュリティシステム

統合化されつつある企業ネットワーク

セキュリティ A to Z 技術編も、今回でいよいよ第6回目を迎えました。第1回から第5回にわたって、皆さんはネットワークの脅威とセキュリティの基礎について、多くの知識を学ばれたと思います。今回は総集編として、いよいよ統合型セキュリティシステム の概念について見ていくことにしましょう。

そもそも、統合型セキュリティシステム は、なぜ企業ネットワークに必要となってきたのでしょうか。これは近年、企業ネットワーク自体が、多くのネットワークやサービス、機能を統合化したことで、企業の中核として機能しはじめていることに起因します。もともと企業ネットワークの多くは、システム単位で存在し、それぞれがホストコンピュータと、それに接続された端末によって構成されるものでした。しかし現在では、ひとつの企業ネットワーク内に複数のシステムやデータベースが機能しています。また、企業ネットワークは、IPネットワークや**広域イーサネット (Wide Area Ethernet)**⁶⁻¹などを介することで、関連企業や本支社との接点を持ちます。公衆電話網を介して外部スタッフがアクセスをすることもありますし、インターネットを介することで、不特定多数のアクセスユーザにサービス提供することもあるでしょう。加えて、テレビ会議システムや**IP電話 (Internet Protocol Telephone)**⁶⁻²などの**ストリーミング (Streaming)**⁶⁻³用データもやり取りされるなど、多種多様なトラフィックを扱う統合化ネットワークへと進化してきているのです。

図1 統合化されつつある企業ネットワーク



増大しつつある新たな脅威

このように、ネットワークは企業活動にとって、なくてはならないインフラストラクチャとなりつつあります。一方で、企業ネットワークをターゲットとした新たな脅威が増大しつつあることも、認識しておかなければなりません。

たとえば、コンピュータウイルスが登場し、これが脅威と認識された1980年代は、ブートセクタ感染型ウイルスが主流であり、ウイルスの感染媒体もフロッピーディスクなどに限定されていました。このため感染スピードは遅く、感染範囲も限定的なものでした。ところが、ネットワークが世界規模へと拡大するにつれて、マクロ型ウイルスやワーム、DoS攻撃など、ネットワーク機能を最大限に利用した新たな脅威が登場し始めました。ネットワークを介したウイルスの場合、数分から数時間で、世界全域に感染域を広げてしまうこともあります。

さらには、特定のOSやアプリケーションに存在する、各種セキュリティホール の脆弱性を突い

6-1【広域イーサネット】

Wide Area Ethernet

イーサネットはLANプロトコルのひとつ。このプロトコルを用いて構築される都市規模のネットワークを広域イーサネットと呼ぶ。イーサネットは、インターネットのようにルータを必要とせず、すべてスイッチという通信機器を用いる。スイッチはルータに比べて安価なので、比較的低コストでネットワークが構築できる。また、使用プロトコルがイーサネットであるため、企業ネットワークで用いるイーサネットとの親和性が高く、シームレスな接続が可能になる。

6-2【IP電話】

Internet Protocol Telephone

IPネットワーク (IP network) を介して、音声を取り取りする電話サービスをIP電話という。IPネットワークとは、IP (Internet Protocol) という通信プロトコルを用いて通信をするコンピュータネットワークだ。ちなみに、インターネットもIPを用いたネットワークであるため、インターネットを利用したインターネット電話 (Internet telephone) も、IP電話に含まれる。ただし一般にサービス提供されているIP電話とは、独自のIPネットワークを構築して、これをIP電話網として使用している。こうして、より高品質な音声転送を実現している。

6-3【ストリーミング】

Streaming

TV会議やIP電話、さらにはインターネットを介した映像配信サービスにおけるデータは、リアルタイムでやり取りをするだけでなく、それをそのまま再生する必要がある。このように、データのやり取りと再生を同時に行う方式を、ストリーミングという。ストリーミングデータを円滑にやり取りするための機能を持つツールも存在する。また、専用のアプリケーションソフトが、データの揺らぎなどを制御することで、滑らかな映像を表示することができる。

6

たハッキング(Hacking)⁶⁻⁴やクラッキング(Cracking)⁶⁻⁵、これを容易に実現できるツール類の流通など、さまざまな複合型脅威が登場しています。そしてこれらを要因として、企業ネットワークへの不正侵入や攻撃が急増したのです。

一方、内部の脅威が増大しつつあることも忘れてはなりません。外部からアクセスするスタッフのPCがウイルス汚染している場合もあるため、不正侵入のみならず、アクセスユーザのPC環境自体までもが脅威となりつつあるのです。

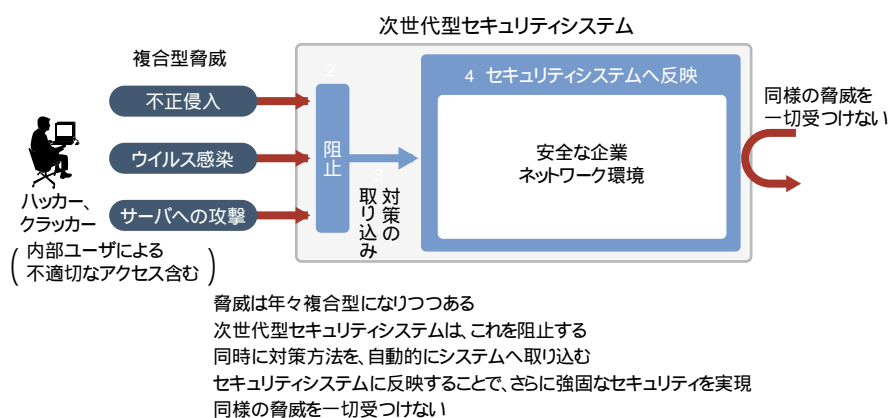
求められる次世代型セキュリティシステム

企業ネットワークが不正侵入や攻撃を受けた際の被害について、これまで各所で学んできました。では、企業ネットワークが複合型脅威から身を守るには、どのような保全対策が必要なのでしょう。

今までの小規模LANなどは、企業の一部として存在するネットワークが、ウイルスに汚染したり、外部から攻撃を受けても、その時点でウイルス除去、システムの復旧作業などの対応を取れば、深刻な事態に陥る確率は、むしろ低いといえました。しかし現在の企業ネットワークが、外部からの複合型脅威によって機能停止を余儀なくされた場合、企業にとって致命的な被害を被ることも十分に考えられます。このため、不正侵入やウイルス感染、外部攻撃など複数の脅威が出現した時点でこれを阻止するとともに、その方法をセキュリティシステムに自動的に組み込むことができるリアルタイムな対応機能が必要なのです。

また複合型脅威に対抗するには、一部のセキュリティを高めるのではなく、企業ネットワーク全域の脆弱性を払拭し、全体が手と手を取り合うネットワーク規模の統合化セキュリティが不可欠なのです。

図2 次世代型セキュリティシステム



6-4【ハッキング】

Hacking

合法的ではあるものの、ネットワークに対して通常とは異なる方法でアクセスすることをハッキングと呼ぶ。ちなみに、ハッカーとは、もともとコンピュータに関する深い知識を持つ有能なプログラマーに与えられる尊称として用いられていた。しかし現在では、不正侵入などの違法行為を意味する言葉として用いられることが多くなった。

6-5【クラッキング】

Cracking

不正侵入などの非合法的なアクセスをいう。また、クラッキングを行う者のことをクラッカーと呼ぶ。厳密には、クラッカーはハッカーと区別して用いられるが、現在その境界は不明確になりつつある。

6

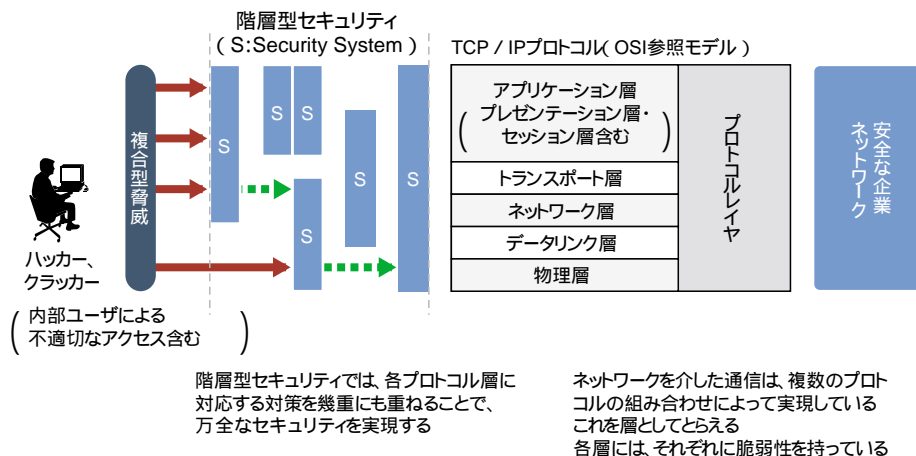
統合化セキュリティのメカニズム

階層型セキュリティの概念

ネットワークを介して情報をやり取りするには、複数の通信プロトコルが不可欠です。通常、通信プロトコル同士は、お互いに手を取り合って機能するので、ひとつひとつのプロトコルをレイヤ(Layer:層) ⁶⁻⁶という概念でとらえ、複数のレイヤを積み重ねることで、ネットワーク全体の機能が成り立つものと考えます。

同様に統合化セキュリティシステムも、外部からの脅威に対抗する手段をレイヤごとに考え、それぞれでアクセス制御を行う手法が用いられています。これを階層型セキュリティと呼びます。つまり階層型セキュリティ ⁶⁻⁷とは、複合型脅威を階層分類したうえで、そのひとつひとつに対応したセキュリティ対策を行い、結果として万全な統合化セキュリティを実現するものです。階層型セキュリティは、統合化セキュリティに不可欠な考え方のひとつです。また、階層型セキュリティは、個々のPC環境の保全機能と、通信機器との連携によるアクセス制御技術やアクセス認証技術によって実現します。

図3 階層化セキュリティの概念



個々のPC環境の保全機能

次に、統合化セキュリティのメカニズムを見ていくことにしましょう。企業ネットワークを守るには、まず企業ネットワークにアクセスするPCの一台一台を、ウイルス感染などの脅威から守る必要があります。個々のPCの環境を守ることで、企業ネットワークへの被害を未然に防ぐのです。

個々のPC環境を守るためのウイルス対策ソフトウェアは、現在では多くのベンダからリリースされています。これらは、開発元から提供されるウイルス情報によって、最新のウイルスに対する監視や検出、隔離、駆除機能を行います。ウイルス対策ソフトウェアは、自動的に最新のウイルス情報をダウンロードするので、新しいウイルスに対応することも可能です。しかし仮に、ウイルス情報にも登録されていない新種のウイルスが存在した場合、その検出や駆除ができないことも考えられます。

そこで新たなPC環境の保全策として、ウイルスのふるまいに注目したセキュリティシステムが開発されています。このシステムの基本的な機能については、第3回でご紹介しました。これを用いれば、ウイルス情報にない新種のウイルスであっても、感染拡大などの二次的被害を未然に防ぐことができます。

6-6【レイヤ】

Layer(層)

複数のプロトコルを組み合わせることで、ネットワークを介したさまざまなサービスが実現している。レイヤとは、複数のプロトコルを階層的にとらえる概念のひとつである。

6-7【階層型セキュリティ】

内外の脅威は、一方向から不正侵入や攻撃を仕掛けてくるとは限らない。OSやアプリケーションのセキュリティホール、企業内のセキュリティポリシーの脆弱性を突いたソーシャルエンジニアリング、さらには、ネットワーク構成や通信機器の脆弱性を突くものもある。これらの脅威から身を守るためには、一過性のセキュリティや単体のセキュリティではとても対応できない。そのため、考えうる脆弱性のすべてにセキュリティ対策が不可欠となる。階層型セキュリティは、これら複数のセキュリティを階層構造でとらえ、結果として抜けのない強固なセキュリティを実現する考え方だといえる。

6

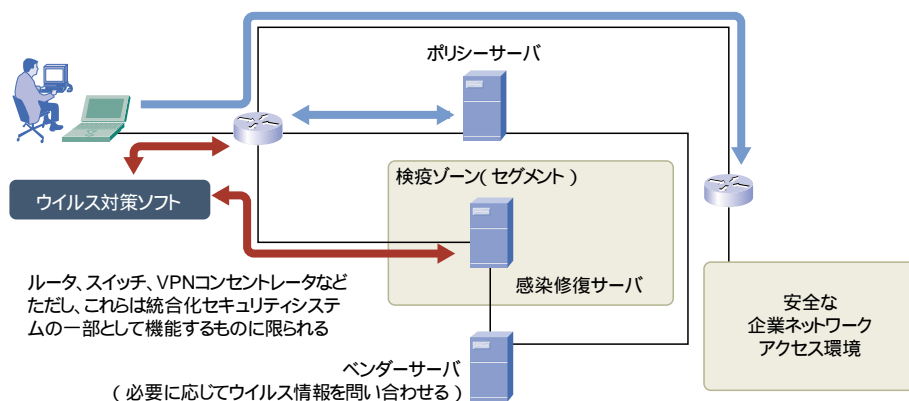
通信機器との連携によるアクセス認証機能

企業ネットワークには、一般的に利便性向上や外部へのサービス提供を目的として、外部とのアクセスポイントが複数用意されています。たとえば、ダイヤルアップ接続用のアクセスポイント、インターネットや各種WANとの接続部分、無線LANのアクセスポイントなどがこれに相当します。またこれらの各種アクセスポイントには、VPNコンセントレータ⁶⁻⁸やルータ(Router)⁶⁻⁹、スイッチ(Switch)⁶⁻¹⁰、ワイヤレスアクセスポイント(Wireless Access Point)⁶⁻¹¹などの各種通信機器が置かれ、それぞれにアクセス制御やアクセス認証を行います。

企業ネットワークにおける統合化セキュリティには、これら通信機器が個々に機能するのではなく、すべてが連携したうえで、統合的なアクセス認証機能を実現する必要があります。

仮に、ある企業ネットワークのルータに対して、インターネットなど、外部からアクセスがあったと想定してみましょう。統合化セキュリティシステムにおけるルータは、まず、アクセスユーザのPC環境を調べ、これを元にポリシーサーバ(Policy Server)⁶⁻¹²に対して認証の是非を問い合わせます。ここでポリシーサーバがベンダーサーバ(Vender Server)⁶⁻¹³とのやり取りの結果、アクセスユーザのPC環境に問題ありと判断したとします。この場合、ルータはアクセスユーザのアクセスを拒否するか、もしくは検疫セグメント内の感染修復サーバへ接続します。すると、感染修復サーバは、アクセスユーザのPC環境を、認証可能な状態へ修復する措置を行うのです。これら一連の工程が介在すれば、外部からのアクセスユーザのPCが汚染されていても、アクセスする段階で、必ず修復されることとなります。通信機器との連携によるアクセス認証機能の実現で、常に安全な企業ネットワーク環境を保持することができるのです。

図4 通信機器との連携によるアクセス認証機能



ユーザが企業ネットワークの入口であるインテリジェントルータへアクセスする
ルータはユーザのウイルス対策ソフトとやり取りを行い、ユーザのPC環境を調査する
ルータはポリシーサーバに認証の是非を問い合わせる

仮に認証できる環境でない場合、ルータはユーザを検疫ゾーン内感染修復サーバと接続
修復サーバとウイルス対策ソフトにより、ユーザのPC環境が安全なものに修復される
ルータは、認証が許可された安全なユーザを企業ネットワークに接続する
結果として企業ネットワークの保全が確保される

6-8【VPNコンセントレータ】

企業ネットワークに数百人以上のリモートアクセスユーザがアクセスし、業務などを行うといった形態の場合、その1人ひとりVPNを実現するには、企業ネットワーク側で多大な負荷を要することになる。このため、リモートアクセスの接続部分に、VPNを実現する専用機器を設置するケースが多い。これがVPNコンセントレータだ。VPNコンセントレータは、100人～10,000人のユーザが同時にVPN環境でアクセスすることができる。この規模の違いにより、多くのグレードが商品化されている。

6-9【ルータ】

Router

インターネットをはじめとするIPネットワークは、複数のネットワークが相互的に接続されたり、多くの専用線同士が網の目状に張り巡らされた形で構築されている。ルータは、相互的な接続部に設置される中継機器であり、到達したパケットの宛先を解析し、正しいリポートへこれを中継する役目を担っている。IPネットワークに不可欠な構成要素のひとつといえるだろう。

6-10【スイッチ】

Switch

スイッチは、LANや広域イーサネットにおけるフレームの中継器。ルータがIPネットワーク(ネットワーク層)におけるIPパケットの中継を行う一方で、スイッチはイーサネット(データリンク層)におけるイーサネットフレームの中継を行う。ルータよりも構造的にシンプルで価格も安い。ちなみに100BASE-TXなど、ごく一般的なLANのスイッチであれば、PCショップなどで手軽に入手することができる。

6-11【ワイヤレスアクセスポイント】

Wireless Access Point

無線LANにアクセスする機器の総称。実際には、ベースステーションや無線スイッチ、無線ハブなど、機能に応じてさまざまな製品が販売されている。また、ブロードバンドルータがワイヤレスアクセスポイントの機能をあわせ持つものも多い。

6-12【ポリシーサーバ】

Policy Server

ここでいうポリシーサーバとは、認証情報を持ち、外部からのリモートアクセスユーザの認証判定を行うサーバをいう。なお、認証にはRADIUS(ラディウス:Remote Authentication Dial-In User Service)など、専用の認証方式を用いる場合が多い。

6

侵入検知から自己防衛型セキュリティへの進化

人間の免疫システムに見る自己防衛型機能

統合化セキュリティシステムはさらに進化し、自己防衛型セキュリティを実現するまでになってきています。自己防衛型セキュリティとは何でしょうか。自己防衛型セキュリティは、人間の免疫システムを例にあげると分かりやすいでしょう。

私たち人間には、あらかじめ免疫システムが備わっています。これはたとえば、風邪を引き起こす菌やウイルスが体内に侵入した際、マクロファージやNK細胞が、これらを食べたり破壊したりする機能です。私たちの身体は、この免疫システムに守られて、健康を維持することができるのです。

ちなみに、風邪のときに服用する風邪薬は、免疫システムの機能を促進する環境づくりは行いますが、これらが直接風邪を治しているわけではありません。あくまでも、人間が持つ免疫システムが機能することで、人間は風邪に勝つことができるのです。

自己防衛型ネットワークのご概念

自己防衛型セキュリティは、このような人間の免疫システムの機能を、企業ネットワークに取り入れたものだといえます。人は、風邪に感染しても、一時的な休養を取れば復帰することができます。企業ネットワークにおいても、同様の考え方を取り入れることで、統合化セキュリティシステムを一歩先へ進める段階にきています。そしてこれを実現するのが**自己防衛型ネットワーク (Self Defending Network)**⁶⁻¹⁴なのです。

企業ネットワークには、内外の多くのユーザがアクセスします。この環境を維持しながら、ウイルスの混入を100%阻止するのは難しいことです。しかし、仮にウイルスに感染しても、その瞬間に自己防衛機能が働けば、少なくとも、感染から派生する多くのリスクは未然に防ぐことができるはずだ。自己防衛型ネットワークは、企業ネットワークの構成要素の多くが、互いにやり取りを行うことで連携動作し、強固なセキュリティを実現しようとするものです。ネットワーク規模の連携動作が可能になれば、たとえば、ネットワークの一部に対する攻撃を検知した場合でも、ネットワーク全体で防御体制をとることができます。

自己防衛型ネットワーク実現のために

最後に自己防衛型ネットワーク実現のための構成要素をまとめておくことにしましょう。

まずは、ファイアウォール、IDSなどによって企業ネットワークと外部との境界エリアを強化します。また、通信機器との連携によるアクセス認証機能により、内部ネットワークのセキュリティを強化します。さらには、PC環境の保全機能によって、エンドポイントセキュリティを強化するといった統合的なアプローチを実施するのです。なお、企業ネットワークを、本支社間や関連企業のLANと相互接続する必要がある場合は、**IPsecVPN**⁶⁻¹⁵によって、万全なコネクション環境を確保する必要があります。これらを図5にまとめます。

先にもふれているように、自己防衛型ネットワークは、複数のセキュリティシステムを別々に機能させるのではなく、ネットワークの構成要素のすべてが手と手を取り合うことで、統合化セキュリティを実現します。また、なんらかの攻撃やウイルス感染が発生しても、即座に自動対応し、これを修復する階層型セキュリティが必要です。自己防衛型ネットワークを実現するには、ネットワークの構成要素全体が連携動作することのできる統合化セキュリティシステムが不可欠なのです。

6-13【ベンダーサーバ】

Vendor Server

ベンダーとは、製品の製造メーカーや販売企業、販売代理店のことを指す。ここでいうベンダーサーバとは、ウイルス対策ソフトウェアの製造元のコンピュータであり、ポリシーサーバが認証判定の際、アクセスユーザのウイルス情報が最新のものであるか否かをチェックしたり、ウイルス情報が新たに更新されているかなどの問い合わせを行う。

6-14【自己防衛型ネットワーク】

Self Defending Network

企業ネットワークを人体の免疫機能と同様にとらえ、総合的なセキュリティ対策を自動的に行う。本来は、何らかの障害が発生した際には、多くの時間と人員を投入してこの復旧にあたるが、これをネットワークが自動的に行うものである。今後、この自己防衛型ネットワークが進化すれば、さらに強固なセキュリティが実現していくに違いない。

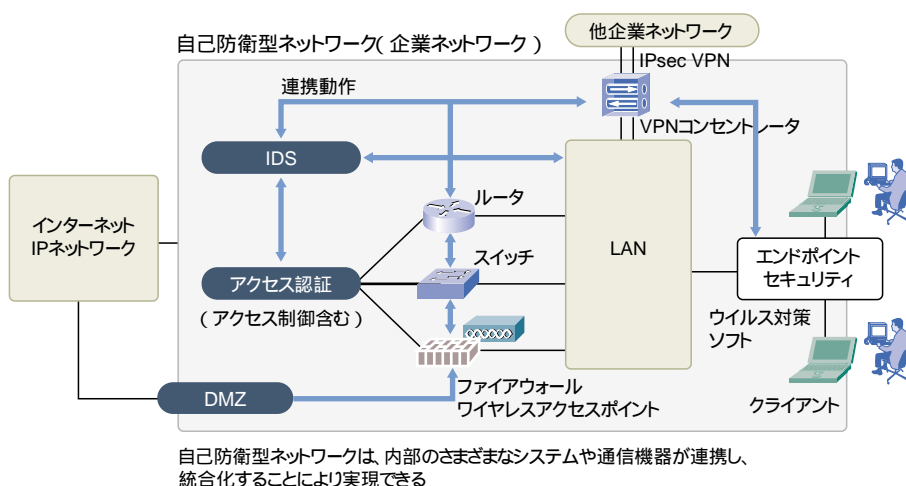
6-15【IPsecVPN】

IPsecについては第5回で学んでいるが、覚えていただいているだろうか。IPsecは、IPv4ではオプション、IPv6では標準で対応する暗号化プロトコルであり、パケット内容を暗号化してやり取りすることができる。IPsecVPNは、このプロトコルを利用することで、VPNを構築する技術である。

6

皆さんが6回にわたって学ばれたことは、今後の企業ネットワークをリスクから守るためのセキュリティ対策や、これを実現するための基礎知識として役立つことでしょう。個々のセキュリティを万全にするだけでなく、自己防衛型ネットワークを構築することで、複合型脅威に対する強固なセキュリティが実現できることを、本サイトによってご理解いただければ幸いです。最後までお読みいただき、誠にありがとうございました。

図5 自己防衛型ネットワーク



シスコシステムズでは、これまで6回にわたって紹介してきたセキュリティ対策を、すでに総合的、包括的に提供しています。たとえば、サーバおよびデスクトップコンピューティングシステム(エンドポイント)における、悪意のある動作を防止するためのセキュリティソフトウェア製品群、CSA(Cisco Security Agent)、ウイルスやワームなどの新しい脅威から被害を最小化するために提唱するマルチベンダープログラム、NAC(Cisco Network Admission Control)、さらには、脅威の種類、レイヤやシステムのライフサイクルとの関係を総合的にとらえ、多段階層で防衛することでネットワークに対する脅威を限りなく軽減する、**シスコ統合化セキュリティソリューション**など、さまざまなソリューションをご用意しています。そしてこれらは、企業ネットワークにおける万全なセキュリティ環境への指針に基づいた新たなセキュリティ戦略、SDN(Self Defending Network:自己防衛型ネットワーク)構想として統合することで、強固なセキュリティを実現するのです。