第５回：ネットワーク・セキュリティ

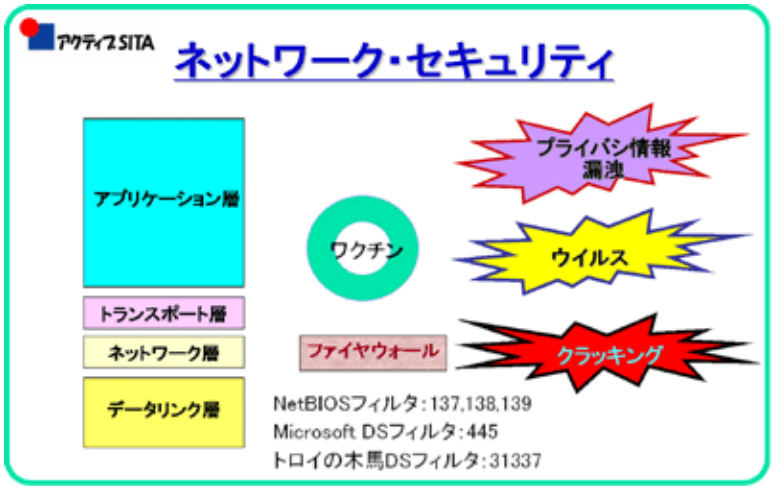
いきなり私事で恐縮ですが、番犬がなくなった悲しみがやっと癒えた頃、まさかの「空巣」に入られ、慌ててセキュリティ会社のシステムを設置しました。再び犬も飼いましたが、今度の犬は番犬にはなりそうもないので、当分セキュリティシステムの世話になって、気が緩まらず警戒しています。 もう一つ私事で、以前は「ウィルス」にやられたのか、風邪をひき、よく仕事を休んだのですが、この数年は風邪に罹っていません。体のコンデションと気の持ち様（ストレスなく、おおらかに）をうまく維持するよう心掛けています。

この様な日常生活の危険と対策と全く同じ様に、パソコンをインターネットにつなぐと、「空巣」や「ウィルス」が襲いかかり、パソコン・ユーザは気を緩めずに警戒が必要とされます。ADSL、CATV、FTTH等によるインターネット常時接続の環境では、危険に遭遇する可能性が益々高まっています。

今回は、内（家庭内LAN）と外（インターネット）ととらえ、ネットワーク・セキュリティについて解説します。

１．外（インターネット）にはどんな危険が潜んでいるのか？

家庭内LANを「家の中」とたとえてきましたが、玄関（**ルータ**）を設け、鍵をかけて（ポートを閉じて）ないと、外（インターネット）から空巣や強盗（**クラッカー**）に攻撃（**クラッキング**）されます。



人込みの中から帰宅すると、「うがいをしないと喉にバイ菌がついているよ」とよく子供の頃に言われました。外（インターネット）から何らかの媒体を介して、**バイ菌**や**ウィルス**（バイ菌とは「悪玉の細菌」の俗称、一方、**ウィルス**はバイ菌より小さい微粒子で、細胞に入り撹乱する）にかかる危険があります。

お店でクレジットカードを使い買い物をする時、「クレジットカードのコピーがとられ、悪用されるので注意するように」と海外旅行の時などによく言われます。似たように、インターネットの通信販売でクレジットカードを不注意で使うと、「プライバシ情報が漏洩」し、悪用されるケースが起こるとも言われています。

これらがインターネットで会う危険でしょうか。そこで、「クラッキング」「ウィルス」「プライバシ情報の漏洩」の３つに分けて、それらの危険さと対策を理解しましょう。なお、これらの「危険さ」は、私達の日常生活と同じで、恐れることではなく、「危険な敵を知る」ことが重要です。そして、あまりに厳しい「対策」をとるとインターネット本来の利便性を損なうので、利便性とセキュリティのバランスを考えていきましょう。

▲先頭へ

２．クラッキング

クラッカーの主な標的は、攻撃効果がある大企業や官公庁、大手ISPのサーバ類と言われていま

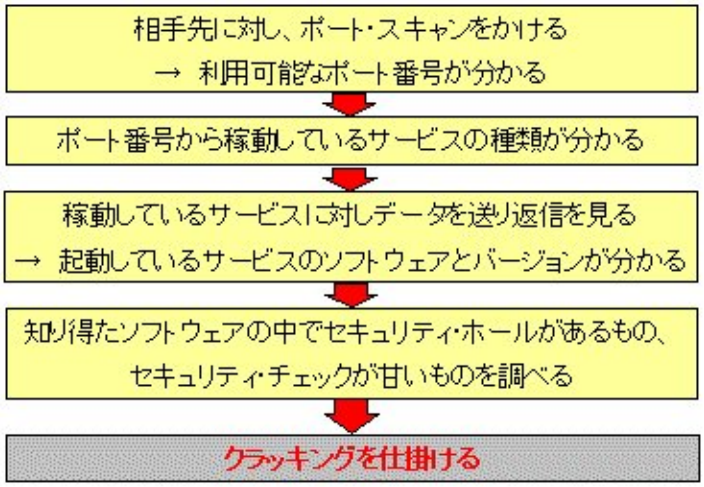
すが、一般の家庭内LANに侵入してきて、パソコンの中で破壊行為を働く可能性がない訳ではありません。破壊行為の中には、単にパソコン内のファイルを壊したり、個人情報を盗んだりするだけでなく、そこを踏み台にして、インターネットの他のサイトに攻撃をかけることに利用されることが一番の問題です。つまり、クラッカーの共犯者にされてしまうという、あまり日常生活ではない「犯罪グループへの連込み」が起こるのです。

常時接続の場合は特に危険が増しています。ルータは玄関の役割をするもので、不用なものを中に入れないためです。パソコン1台でインターネット接続している場合でも、そのパソコンをインターネットに直結せずにルータを介すことが必要です。ルータ購入の費用が発生し、ルータによりアクセス・スピードが落ちる場合もありますが、玄関に鍵をかけるようなもので、ルータは必需品と考えて下さい。 マンション共通のFTTH加入の場合も、各戸の入口ではルータを設置した方が安全です。なぜなら、マンションの入口にはルータが設置されますが、それだけではマンション内の各戸はオープンになっている状態だからです。また、CATV接続の場合もルータを各戸で入れていない場合があるようで、それでは隣近所にオープンになっている状態の可能性があります。

では、なぜルータが「玄関の鍵」の様な物なのかというと、インターネット（外部）とのやり取りにおいて、サービスにより、いろいろなポートが割り当てられていて（ウェブ閲覧のHTTPではポート80、メール通信のSMTPはポート25、POP3はポート110、ファイル転送のFTPではポート20と21 等々）通信が行われます（この連載講座の第2回を参照して下さい）。ルータはサービス毎にいろいろなポートを開き、サービスが終了すると、ポートを閉じる役割を果たしますが、ルータがないと、パソコンの動作が全て外から見られているイメージだと考えて下さい。

典型的な例として、2台のWindowsパソコンがファイルを共有していると、ポート番号137、138、139および445を使っています。その時、ルータなしでインターネット接続していると、外部からも2台のパソコンのファイルが容易に覗かれてしまいます。クラッカーによる悪意の覗きにあうと被害を受ける可能性があるのです。

クラッカーの進入の手口は、この様に行われると言われます。最近、皆さんは次



項で説明するウィルス・チェックをよく行なっておられるでしょうが、外部からのクラッカーの進入に対する安全性のチェックを行なっていますか？ セキュリティ・ソフトを販売している会社などのサイトに無料で行なえるセキュリティ・チェック・サービスがありますので、試して下さい。

例えば、http://www.symantec.co.jp/region/jp/securitycheck/などです。

外部からの侵入に対しLANを守るために機能を一般的に、「ファイアウォール」と言っています（下図はwww.atmarkit.co.jp/fsecurity/special/17fivemin/fivemin00.html から引用）。

ファイアウォールには２つの方式、即ち

①パケット・フィルタリング方式

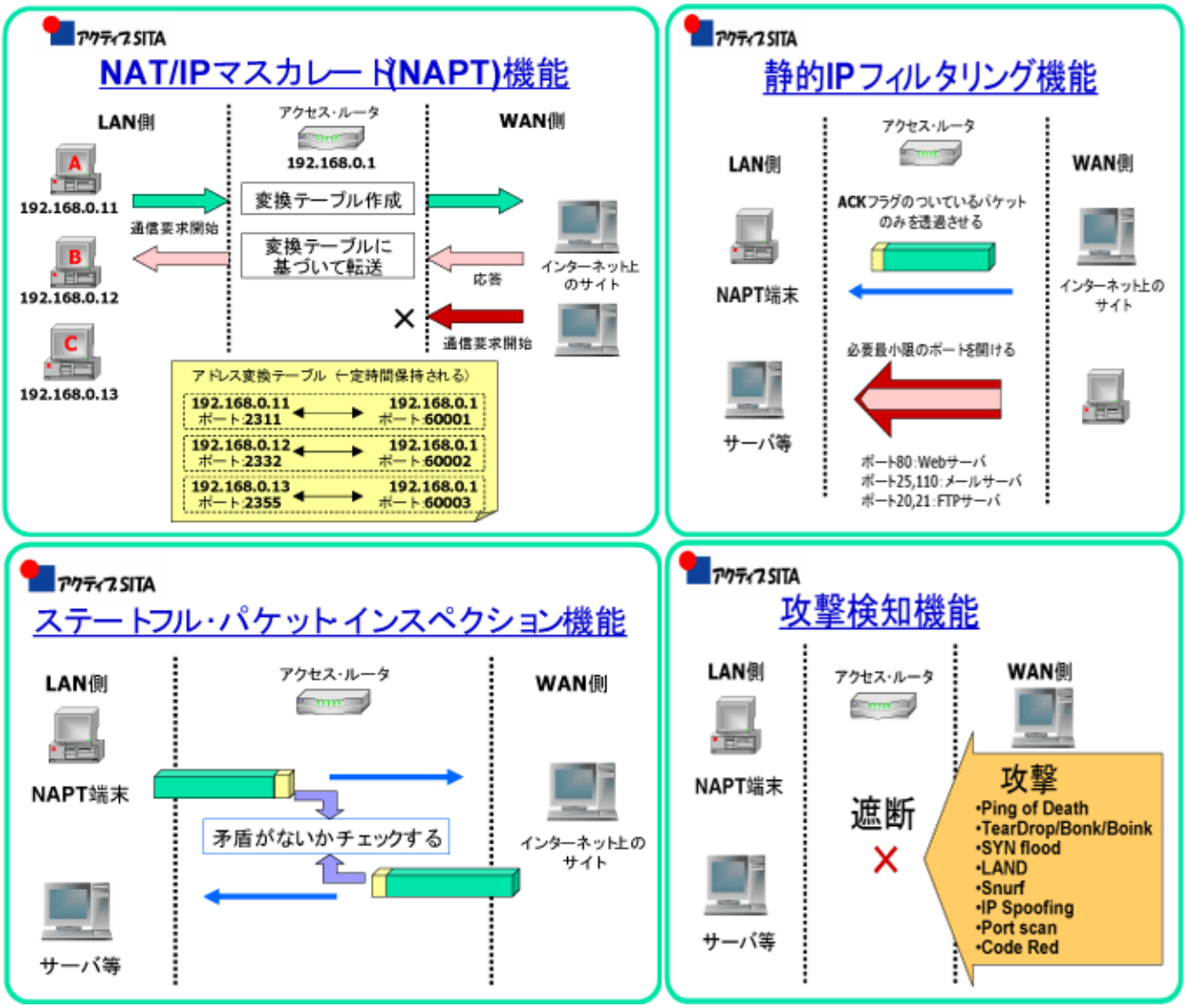
送信元や送信先のIPアドレス、ポート番号などによって通信データを通過させるかどうかを判断し、不正アクセスを防ぐことができます。OSI参照モデルの「ネットワーク層」で動作するファイアウォールで、家庭内LANでは、ルータで実現するのが一般的です。

② アプリケーション・ゲートウェイ方式

通信を中継するプロキシサーバ（代理サーバ）を利用し、LANとインターネット間で直接通信ができないようにする方式で、アプリケーション層のファイアウォールということになります。

本稿でこれまで「玄関の鍵」の役割と言ってきたルータには、最近、様々な機能が実装され、①に分類されるファイアウォール機能を発揮します。次の４つの図に示す機能がそれらで

す。



IPマスカレード機能は、LAN内の複数パソコンからのインターネット接続共有を可能とする機能ですが、IPアドレスとポート番号が変換されるため、外部からLAN内の各パソコンが隠されるという副次効果で、外部の攻撃を塞ぐことができるという訳です。

静的IPフィルタリング機能とは、パケットのヘッダ部のＩＰアドレスやポート番号などをチェックして通過させるかどうか判断します。先に、Windowsネットワークでは、ポート番号137～139および445はファイル共有などで使われるので、外部から侵入できないようにフィルタリングをしなければなりません。皆さんがお使いのルータに、それらのポートに非通過のフィルタリングが設定されているかどうか確かめておいて下さい（宿題!!）。

本講座2回目のFTP解説のところで、ルータの「IPフィルタ」の設定が、「接続先から受信 0.0.0.0/0（送信元） 0.0.0.0/0（送信先） TCP-SYN（プロトコール）（ポート番号は＊） 非通

過（アクション）」となっていて、FTPの受信できなかった事例をお話しました。これは、SYN Flood という攻撃を防ぐ設定なのですが、そのファイアウォール機能がFTP通信を阻害してしまうのです。これが利便性とセキュリティの板挟みということです。

ステートフル･パケット･インスペクション（Stateful Packet Inspection: SPI）機能（動的IPフィルタリング機能ともいう）はパケット・フィルタリング機能に加え、通信の状態をチェックして判断するものです。

さらに高度な機能は、攻撃（不正侵入）検知機能 (Intrusion Detection System)で、IPパケットのデータ部分も検証するものです。攻撃パターンをシグネチャと呼ばれる形でデータベース化しておき、ネットワークを流れるパケットデータとシグネチャとの突合せ処理をリアルタイムに行ない、不正侵入を検出する機能です。

サーバサイトの攻撃で、DoS攻撃(Denial of Service Attack) および DDoS攻撃(Distributed DoS Attack) があり、しばしば、大手ISPのサーバが攻撃されることがあります。ファイアウォールの機能と攻撃の強さのイタチゴッコが続いています。

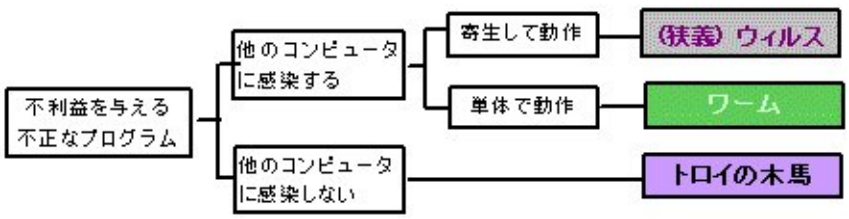
家庭内LANからWebサーバを公開する際は、ルータでポート番号80を常時通過にしておかなければならず、LAN全体が攻撃の対象になりやすいので、そのサーバだけルータなしで外部に接続し、他のLAN内のパソコン類はルータのIPフィルタリングをかけて守るという構成が考えられます。このとき、サーバは外部に晒される場所に置かれるので、DMZ(DeMilitarized Zone非武装地帯)に置くと言われています。外部のインターネット側に対するサービスを行なうサーバ類をDMZに配置し、それらに対し別のセキュリティ対策を施すのが企業等で行なわれているLAN構築手法です。

▲先頭へ

３．ウイルス感染

インターネットの危険さの中で、皆さんに最も馴染み深くなっているのが、ウィルスですね。ところで、広く一般にウィルスとは、悪意を持ってコンピュータのハードやデータを破壊する不正プログラム全般という定義ですが、本来のウィルスとは、それ自身では増殖できず他のプ

ログラムやデータに入り込んで機能するものなのです。そこで、広く一般にウィルスと言われている物は、３分類されます。

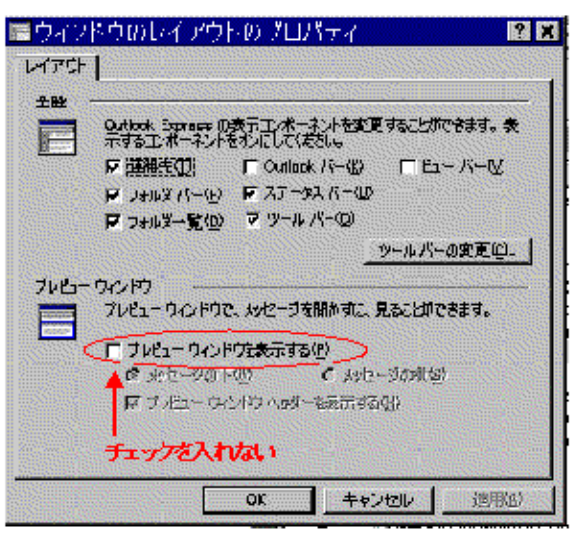


ウィルスの感染は、今や90%以上が電子メールに乗ってやってくると言われ、皆さんも迷惑な「ウィルス」添付ファイルのメールに悩まされていることを思いますが、その大多数は、左図に示す「ワーム」(蛆虫)です。

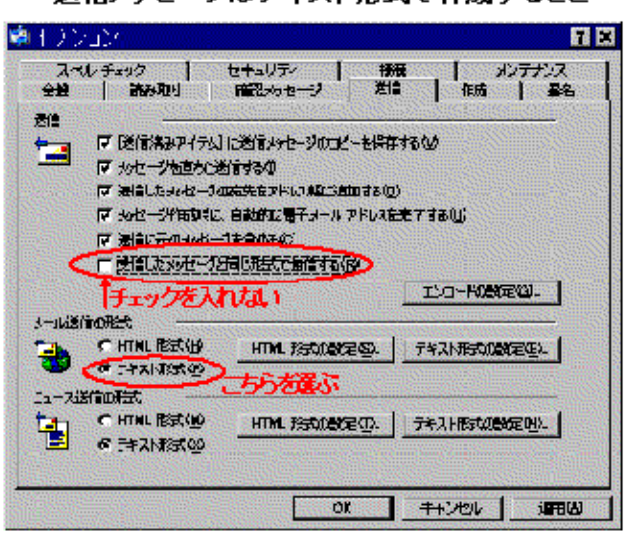
最近のワームのほとんどは、取りついたコンピュータの内のアドレス帳を盗み読み、自分自身のコピーを添付したメールを、ユーザに気付かれずに、送信し続けるという離れ業を演じています。今年1月にMydoom (マイドーム) と呼ばれるワームが数日のうちに世界に蔓延し、引き続き、スカイネット、ナチ、バグル、サッサーと続いていることは皆さんもよくご存知のところでしょう。「怪しいメールは開かない」が鉄則で、即削除すべきものです。

最も多く使われているメーラOutlook Expressでは、必ずUpdateを行ない、セキュリティホールを取り除いておくこと、またその設定でも次の2点は常識となっていますので、蛇足ですが、念を押しておきます。

プレビューウィンドウを表示しないこと



メッセージは全てテキスト形式で表示すること
→送信メッセージはテキスト形式で作成すること



ウィルスに罹らないためのユーザーの自衛策としては、アンチウイルスソフトが必須と言われ

ています。しかし、宣伝が盛んで「有名な」ソフトは高価で、毎年更新料が必要です。ですから、躊躇している人も多いのではないかと思いますが、そんな人には、フリーながら市販のアンチウイルスソフトと比べても遜色のない機能を備えているソフトがインターネットから入手できます。例えばhttp://ringonoki.net/tool/antiv/1-antiv.html には一覧表と簡単な解説があり参考になります。ここにも一覧表を示します。

ウイルス駆除ソフト	ダウンロード・サイト
AVG Anti-Virus Free Edition	http://free.grisoft.com/freeweb.php/doc/2/
AntiVir Personal Edition	http://www.free-av.com/
BitDefender Free Edition	http://www.bitdefender.com/
ANTIDOTE SuperLite	http://www.vintage-solutions.com/Japanese/Antivirus/Super/godownload.html

▲先頭へ

４． プライバシ情報の漏洩

パソコンを通しての個人情報の漏洩事例は多種あり、ここで説明し切れませんが、ショッピング･サイトなどで不可欠なクッキー(Cookie)から個人情報が漏れて危険だということを良く聞くので、クッキーについて解説します。

例えば、あるショッピング･サイトにメンバー登録し、ショッピングを行なおうとすると、サイトがクッキーを発行し、ユーザのブラウザが応答し、小さなテキストデータをパソコン内に保存します。商品を見て、買い物を決め、さらに買い物を続けても、同一ユーザであることが、サイト側に判るように、個人を特定するクッキーがユーザのパソコンからサイトに送られて、買い物が継続でき、さらに登録していた住所等にショッピング・カートが結び付くことができるのです。

皆さんのパソコンの中に、クッキーファイルがたくさん保存されていると思いますので、覗いてみて下さい。

・ Windows XPの場合：¥Documents and Setting¥＜ユーザ名＞¥Cookies

・ Windows 98の場会：¥WINDOWS¥Cookies

このフォルダにテキスト形式で保存されています。URLから判断し、心当たりのないファイルは削除しておきましょう。

さて、クッキーはインターネット・ショッピングには不可欠な技術なのに、危ないとはどういうことでしょう。クッキーファイルは、それを書き込んだサイトだけが読み出すことができます。 つまり、サイトAが書き込んだクッキーをサイトBは読み出すことはできません。もし、サイトBも読み出せるとしたら、サイトBがユーザの「なりすまし」でサイトAにログインし、ショッピングをすることができてしまうかも知れません。怪しいサイトにアクセスすると知らずのうちに悪意のあるソフトウェアで、パソコン内に保存されているクッキーが全て盗まれるとか、クラッカーが侵入し、クッキーファイルを盗み出すとかが、想定されます。そして、悪用されたら、大変です。それでは、クッキーを保存することを拒否（Microsoft Internet

Explorer (IE) の場合、「ツール」→「インターネット･オプション」→「プライバシ」タブ内で設定）できますが、ショッピングができなくなったり、会員制のサイトに入れなくなったりするので、不都合です。利便性と安全性のバランスが必要とされる一事例です。

▲先頭へ

５． 基本的な３つのチェック

ネットワーク･セキュリティほど、日々変化して不定で、難しいものはありません。パソコン･ユーザの心掛け、心の持ち様も影響するのですから。

ある程度、定期的にセキュリティのチェックを行い、安全対策を施しておくことも、日常生活での危機管理と似ています。ここで十分には説明できませんでしたが、次の３つ面での対策を、意識的に実行して下さい。

- **クラッキング → セキュリティホール対策(特にWindows Update)、ポート・チェック**
- **ウィルス　　→ ウィルス･チェック**
- **情報漏洩　　→ クッキーの整理、スパイウェア･チェック**

今回は、ここまでとし、次回は、ＬＡＮ構築の手順を具体的に解説し、本連載のまとめとします。
また次回にお会いいたします。

参考資料

［1］　‘ネットワーク･セキュリティ’ 神崎洋治・西井美鷹著 日経BPソフトプレス 2002.12.9

［2］　‘ウィルス＆セキュリティ110番’ セブンベストMOOK 27 2004.07 Vol.01 セブン新社

（第５回終り）