初心者を悩ますWindowsのネットワークトラブル
第４話　攻撃から身を守る

加　藤　浩　樹

Ⅰ．はじめに

これまで３回にわたり，いわゆるWindowsパソコンの初心者を対象として，ネットワーク利用における困りごととその対処法などについて紹介して参りました。お役に立ちましたでしょうか。まだ足りない，あるいは，出るべきことが書かれていない，という読者も数多くいらっしゃると思いますが，紙面に限りもあることですし，そのあたりはどうかお許しください。今は昔と違って情報セキュリティ関連の情報も，本屋や有名なホームページといった目に付くところで意外にわかりやすい形態で流れていますので，このシリーズで触りきれなかった話題については，そちらの方を探索してくださるようお願いします。

今回は，前回の最後で予告をしましたように，Windowsにおけるネットワークセキュリティについて少し掘り下げて書いてみよう，などと思っておりましたが，タイミングが良いのか悪いのか，Windowsのセキュリティホールを悪用するMS-BLASTなるものが蔓延し，新聞やテレビなどでもさかんに報道されています。今これをお読みになっている貴方も，もしかしたら被害に遭われたのかもしれませんね。

Windowsシステムを標的としたネットワーク攻撃や，電子メールを介して蔓延するコンピュータウィルスなどの被害が後を絶たないのにはさまざまなところに原因があると思いますが，そもそもセキュリティホールだらけのオペレーティングシステムをそのまま販売してしまっているMicrosoftにも大きな原因があります。

Windowsはスイスチーズのようなもの，という話もあるようですが，現状ではその穴だらけのソフトウェアを買ったユーザが自分の手で穴ふさぎを行っていかないと，いずれユーザ自身がチーズの穴にはまってしまうのです。

こんなことならWindowsなんてやめてしまって，他のオペレーティングシステムを使って平和に暮らしたいとお考えの方，多いのではないでしょうか。でも世間にはWindowsとその上で動くOfficeなどのアプリケーションソフトがあふれています。仕事の関係でWindowsから逃げられない人も少なくないのではないかと思います。仕方ないですね。世の流れです。

そこで今回は，とりあえずどのようなことに気を付けていれば，妙な攻撃に耐えながらWindowsと平和に暮らしていけるかということを述べていきたいと思います。

中には「○○と言うソフトを買ってインストールする」という話も出てきます。そんなことに使う金があったら，かの高名な△△先生の御本を買いたいという人がいらっしゃるかもしれませ

ん。でも，Windowsのセキュリティ対策ソフトに金を出し惜しみして，後で大穴に落ちて泣くのは貴方です。これも世の流れとあきらめることをお勧めします。苦情はＭＳへ。

Ⅱ．Windowsはどこがあぶないか

ここでは手始めに，ネットワークにつながっているWindowsコンピュータに対して降りかかった災難について，主なものを紹介します。そのようなことは先刻承知，という読者の方は読み飛ばしてください。

パスワードを設定していなかったために侵入されたというような「極めて初歩的なミス」による危険性や，電話などで上手にパスワードを聞き出されてしまったといういわゆる「ソーシャルエンジニアリング」に関するようなことについては，ここでは触れません。参考文献(1)などをご覧ください。

１．セキュリティホール

あらためて言うまでもないことですが，Windowsというソフトウェアにはバグが多い，ということは広く知られていることです。バグというのは製造段階で見逃されてしまったソフトウェアの内部エラーのことですが，数多くのユーザがそのことについて知らないか，知っていてもあまり危機感を持たぬままにコンピュータを使っているのが現状です。

内部エラーを含んだままでソフトウェアが売り出されてしまうのは，何もWindowsに限ったことではありません。人間が作るものですから，どこのメーカのソフトウェアでも必ずどこかにミスがあります。でもそのミスがどの部分にあるかによって，ユーザが受ける被害の大小が変わってきます。

もしバグがネットワーク接続機能に関係する部分に存在すると，多くの場合それは「セキュリティホール」と呼ばれ，「システムの脆弱性」という言葉で表現されると同時に，注意喚起の対象となります。

セキュリティホールというのは，それを悪用する攻撃者（以下，クラッカー）に対してネットワーク経由の不正アクセスや破壊行為を許してしまう，文字どおりの抜け穴です。この穴は，ある特定のデータ群の転送にさらされると簡単に口を開けてしまいます。

セキュリティホール悪用の代表的なものにバッファーオーバーフロー攻撃というものがあります。バッファーというのはコンピュータのメモリ上に作られるデータ格納領域の一種で，入力された信号が実際に処理されるまでの間，一時的に溜めておくバケツのようなものです。このバッファーの管理を適正に行っているプログラムと行っていないプログラムがあり，この管理の不適正さをクラッカーが悪用します。

バッファーを正しく管理していないプログラムが動作しているコンピュータに対して，バッファーの容量を超える大きなデータが送りつけられると，バッファーがオーバーフロー，つまりバケツがあふれてしまい，メモリ上の整然としたデータ配置が破壊されて，そこにクラッカーが好きな命令を実行できる場所ができてしまいます。もし攻撃対象となったプログラムがオペレーテ

ィングシステムの重要な動作に関わるものだった場合，クラッカーが実行する命令はシステム管理者が行う命令と同格になるので，結果的にコンピュータの動作は完全にクラッカーに乗っ取られ，

- 強制シャットダウン，強制再起動などの機器動作妨害行為
- コンピュータに保存されているデータの削除，改竄，盗み取り行為
- 不正動作プログラムの設置による継続的な乗っ取り行為
- つぎなる攻撃先への経由点，「踏み台」としての利用行為

などの破壊行為が行われます。

セキュリティホールが開いたままで放置しておくことは極めて危険です。クラッカーの攻撃を許すことで，極秘・重要データの紛失や漏洩といった直接的な被害だけでなく，踏み台とされることで他の場所に損害を与えてしまうという間接的な被害も起こり，場合によっては，そういった間接的被害を防ぐ努力を怠ったという理由で，被害者から法的な責任を求められることがあるかもしれません。

ではどう対処すればいいのでしょうか。方法はいくつかあります。

ひとつはセキュリティホールの元となっているシステムのバグを解消するために配布される修正プログラムをコンピュータにインストールすることです。あるいはその修正プログラムが出てくるまでの間コンピュータのネットワーク関連設定を適宜操作して応急処置をすることもできます。クラッカーの不正なアクセスを感知して遮断する機能を持つソフトウェアも市販されています。

詳細は後の方で紹介します。

２．コンピュータウィルス

コンピュータウィルスとは，多くの方がすでにご存知のように，不正な動作をすることを意図して作られたプログラムのことです。もちろんコンピュータと言った場合，それはWindowsだけではありません。MacOSやUNIX/Linux，BSDなど，Windows以外のオペレーティングシステムで動いているコンピュータは世界中に数多くありますが，最近ではコンピュータウィルスというとそのほとんどがWindowsを標的にしたものです。あらゆるオペレーティングシステムの中で，Windowsの上で動作するウィルスを作るのが最も簡単であるのと同時に，Windowsが世界中で最も普及しているからなのかもしれません。

トレンドマイクロ・ホームページの「ウィルス対策基礎知識」[(2)]に出ているように，コンピュータウィルスには，ファイル感染型やシステム領域感染型，マクロ型やトロイの木馬型のものなど数多くの種類がありますが，コンピュータが感染し，発病すると，ユーザの意図しない不正な動作が始まります。

不正動作の種類や程度の大きさはウィルスの種別や動作形態などによってさまざまに分かれます。その時その時の流行のようなものもあるようですが，最近の傾向としてはつぎのようなものが目立ちます。

ⅰ．不特定多数の宛先に勝手にメールを送信する
Outlook，Outlook Expressのアドレス帳を勝手に利用し，登録されているアドレスに対してメールを大量に送りつける。

ⅱ．コンピュータを勝手にシャットダウン，再起動する
コンピュータが動作中にもかかわらず，ユーザの意図しないタイミングでシステムを勝手にシャットダウン，あるいは再起動してしまうことで，正常な利用を阻害する。

ⅲ．データを勝手に削除，あるいは改竄する
コンピュータに保存されているデータを勝手に削除，あるいは内容変更してしまい，多くの場合復旧不能となる。

ⅳ．データを勝手にどこかへ転送する
コンピュータに保存されているデータを，ウィルス作者が指定したインターネット上の某所に転送することで，重要なシステム情報や極秘文書などを盗み取る。

ⅴ．キー・ロガーを仕込んでキー入力を監視する
キー・ロガー（キーボード入力を監視するプログラム）をシステムに仕込んで，キー入力検知結果をウィルス作者に転送することで，パスワードやクレジットカード番号を盗む。

ⅵ．システムにバックドア（裏口）を作る
システムに勝手にネットワーク接続の裏口を開設し，そこを通じてクラッカーがさまざまな破壊行為を行えるようにする。

また近ごろのウィルスには電子メールの添付ファイルという形で蔓延するものが多く存在しますし，前に述べたWindowsのセキュリティホールを悪用して活動するものも存在します。テレビや新聞で話題になっているMS-BLASTはWindows2000/XPを標的とし，システムに存在する「DCOM RPCの脆弱性」というセキュリティホールを突いて強引に感染しようとします[3]。

これらの被害を防ぐにはどうしたらいいのでしょうか。とりあえずすぐにできることで，確実に効果のあることと言えば，ウィルス対策ソフトの導入です。いろいろなメーカーの対策ソフトが市販されていますし，インターネットには無料のソフトウェアも流れていますが，定評のある市販品を選ぶのが一番安心ではないかと思います。また，対策ソフトを単に導入しただけでは不充分で，導入後も日ごろの気遣いが重要になります。

詳細は後述します。

３．スパイウェア

「スパイウェア」という呼び名は，もしかするといわゆる初心者ユーザの皆様にはあまりなじみがないものかもしれません。参考文献[4]によれば，スパイウェアとは，ユーザの同意を得ずにコンピュータにインストールされ，ひそかにユーザの情報を収集したり，広告を表示させたり，勝手にコンピュータを利用したりするソフトウェアの総称です。

アプリケーションソフトウェアの一部としてインストール時に主プログラムの陰に隠れて勝手に組み込まれる場合や，スパイウェア配布機能を仕込んだホームページを見ることで自動的に突

っ込まれてしまうなどの手法でコンピュータに入り込んで来ます。つい先日も某大手検索エンジン会社のホームページにアクセスしたとき，PCに搭載しているスパイウェア検知ソフトが反応し，不要なプログラムが突っ込まれようとするのを防いでくれました。

ユーザの承諾を得ずに勝手にインストールされてユーザの知らないところで望まれない活動を行うという点ではトロイの木馬型ウィルスと似ていますが，スパイウェアはウィルスではないのでウィルス対策ソフトでは検知できません。ウィルスプログラムには独特の不正動作コードが存在します。対策ソフトはそれを頼りに検出を行いますが，プログラムとしてみた場合スパイウェアには不正コードは含まれていません。したがって検出できないのです。

またスパイウェアはWindowsのセキュリティホールとは無関係です。あくまでも正常なプログラムとして正常な手順を踏んでインストールされるので，抜け穴を悪用する必要もありません。ということは，抜け穴対策やウィルス対策を徹底しているコンピュータにおいてもスパイウェアは自由に動くことができるというわけです。

だからといって放置しておくのはあまり良いことではありません。中には勝手に走らせておかないとWindowsシステムの動き自体が変になってしまうスパイウェアもあるようですが，ほとんどのものがスパイウェア供給元に利益があるだけでユーザにとって何の得にもならないもののようです。

また，例えプログラムの形態が正常なものだといっても，その動作がユーザの知らない間にひそかに行われることが多いという事情を考えれば，ウィルス同様に駆除するのが望ましいと思います。

でもどうやって駆除すればいいのでしょうか。

幸いなことに，インターネットには高機能でしかも無料のスパイウェア対策ソフトが流通しているので，それを使います。

詳細は後の方に書きます。

Ⅲ．セキュリティホール対策

ここではWindowsシステムのセキュリティホール対策について，一般のユーザがすぐにできてしかも効果のある方法を紹介します。大きく分けて２つの手法があります。

まず，ソフトウェアメーカーがインターネットなどを通じて配布するエラー修正ソフトをコンピュータにインストールすることです。その操作をするための代表的なものがWindows Update[5]ですが，他にもあります。

つぎに，エラー修正ソフトの配布がメーカーの技術的な理由などで遅れた場合，配布が行われるまでの間の一時しのぎとして，コンピュータのネットワーク設定を適宜変更して応急対策とすることです。いわゆる「運用で逃げる」という手法です。何かの内部エラーを含んだプログラムがネットワーク機能の一部として動いているからセキュリティホールができるわけですので，そのプログラムを一時的に止めてしまえば穴もとりあえずふさがります。でも止めてしまうことでネットワークの使い勝手が悪くなることもあります。いずれにしてもバグは残ったままですので，

本質的な解決とは言えません。

また，いわゆるセキュリティ対策ソフトを導入して，不正侵入行為を検知・遮断することで，ここで紹介する方法と合わせ技にして防御するという手もありますが，これについては別項目を設けて後ろの方で触れます。

それでは以下，順に紹介していきます。

１．Windows Update

Windowsには最近になって特に多くのセキュリティホールが頻繁に発見されます。さらにそれが広い範囲に大きな被害を与えるようなネットワーク攻撃の温床になることが多いため，発見されるたびにMicrosoftが批判の対象となっています。

Windowsに限らず，ソフトウェアに新しいセキュリティホールが発見されると，よほど悪質なメーカーでないかぎり，その穴をふさぐためのいわゆるバグフィックスやアップデート，バージョンアップという修正プログラムを，何らかの形で供給してきます。ユーザがそれを自分のコンピュータにインストールすることで，その穴を悪用した攻撃に対する耐性を得ることができます。

供給形態はさまざまです。ソフトメーカーのホームページからのダウンロードや，メーカーからの有償あるいは無償のCD-ROM郵送配布，パソコン関連雑誌の付録CD-ROMによる供給や，さらに近頃では例のMS-BLASTの影響によりパソコンショップ店頭での配布も行われるようになりました。

それらの供給形態の中には，メーカーのサーバと手元のコンピュータが交信をしてシステムの更新状況をチェックすることで，半自動，あるいは全自動でエラー修正プログラムのダウンロードとインストールを行う仕組みがあります。それがMicrosoftのWindows Updateです。

Windows Updateの詳細については拙著[5]などをお読みいただきたいのですが，Microsoftのホームページにも関連情報が多く出てくるようになりました。また最近になってMicrosoftのテレビCMの最後のところで「Windows Updateを行いましょう」という趣旨の一言が出るのを見たときは驚きました。

Windowsのセキュリティホール対策の第一歩として，このWindows Updateの実行が重要になります。

やり方については，ほとんどの場合難しいことは何もありません。初めての人は取っ付きにくいかもしれませんが，何度かやって慣れればできます。また，いままで長期にわたりUpdateをしなかったコンピュータで実行すると，エラー修正の量が膨大になっているためにいささか時間と手間がかかります。でも一度辛抱すれば，後は新しいセキュリティホールが発見されるたびに少しずつ更新していくということになるので，作業に苦痛は伴いません。

起動方法はいくつかありますが，一番手っ取り早いのはInternet Explorerのメニューで，ツール（T）からWindows Update（U）とクリックすることで始められます。

図１　WindowsXPにおけるWindows Update

Windowsシステム本体だけでなく，Internet Explorer，Outlook Express，Media Playerなどの各種組み込みソフトウェアの修正プログラムの配布準備が整うと，Windows Updateのホームページに公開されますので，日頃から注意して利用を心がけるようにしましょう。

大学という職場の場合，特に教員に関して困った事情があります。多くの教員がそれぞれの研究室に自分で責任を持つべき専用のネットワーク端末を持っていますが，それらの教員に対して，減給や降格，左遷といった罰則を伴う強制力をもってWindows Updateの実行を義務付けることは困難だと思います。どんなに奨励しても，「何度言ってもやってくれない」という人間を完全になくすことはできないでしょう。罰があるか，あるいは自分に火の粉が飛んでくるようなことがなければ，特に偉い人ほど，動かない人は動きません。

だからと言って，アブナイWindowsをアブナイまま放置することはできません。セキュリティ対策の実行により，自分のコンピュータを守るだけでなく，周りの人にも迷惑を掛けないようにしなければいけません。

「面倒だからやりたくない」という人々も含めて，自分自身が大きな被害を受けて泣きを見る前に，Windowsセキュリティ対策の最低ラインであるWindows Updateを忘れずに実行しましょう。

２．Office Update

Office Update，これは前の項目タイトルの書き間違いではありません。Windows Updateと類似のサービスとして実在するものです。Windows Updateホームページの上の方にある「Officeのアップデート」というところをクリックするとつながります。

図２　Office Update

Officeも大きなプログラムですから，必ずバグがあります。Windowsと同じMicrosoft製品なので，オペレーティングシステムの根幹部分と連携して動作する機能がOfficeにもあり，そこにバグがあると結果的にセキュリティホールになることもあります。実際に９月４日には，Windowsの脆弱性情報と同時にWord/Excel/PowerPointなどの複数のアプリケーションに影響のある「Officeの脆弱性」情報がMicrosoftから公開されました。

一部報道[6]によれば，「Office製品に含まれるVisual Basic for Applications(VBA)の脆弱性を悪用され，最悪の場合，悪意のあるユーザによって，PC上で任意のプログラムを実行される恐れがある」ということです。

こういう問題を解消するためには，Office Updateを実行し，問題を抱えているプログラムを修正プログラムと入れ替える必要があります。やり方には技術的な知識は必要なく，Windows Updateと同じく単に慣れの問題です。図２のところで，ちょうど真ん中あたりにある「検索」というところをクリックしてスタートします。初めてOffice Updateを行う場合は，自動コンポーネ

ントのインストールに関するデジタル署名情報が出ますので「はい」をクリックしてつぎに進みます。やがて，コンピュータに搭載されているOfficeの更新状況がチェックされ，結果が表示されます。

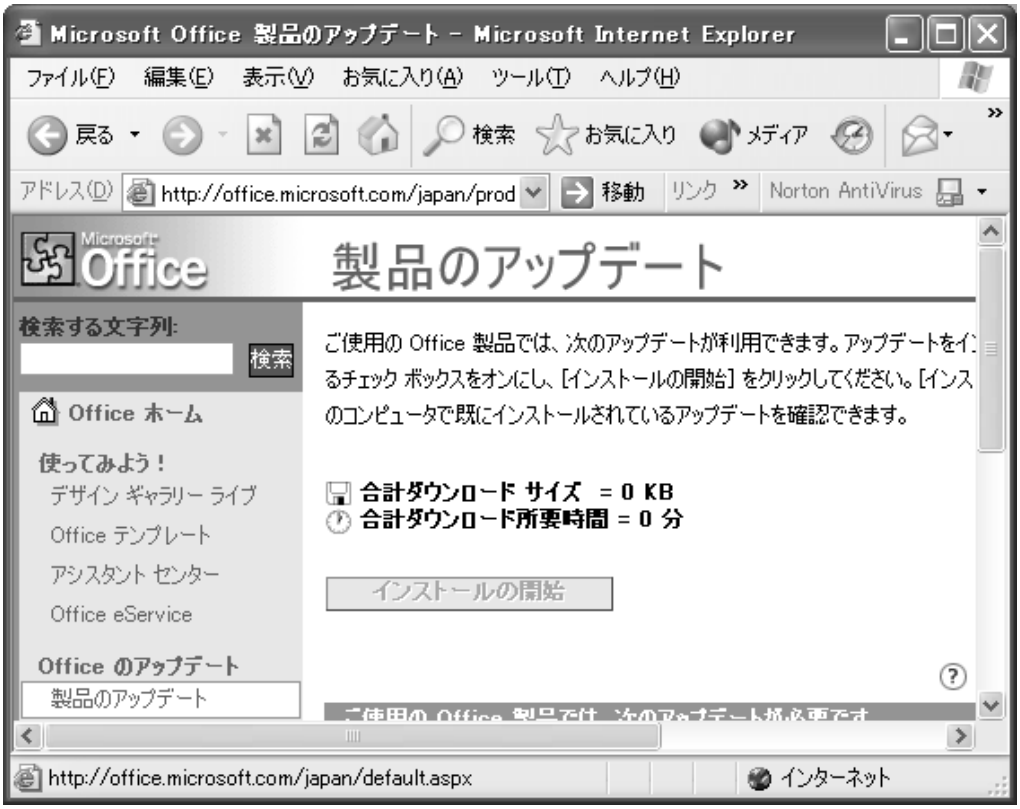

図３　Office更新状況調査結果

図３では「合計ダウンロードサイズ」が０KBになっていますが，これはこの図を採取したコンピュータのOfficeが最新の状況になっているからで，未更新部分が多いほどサイズは大きくなりますし，更新プログラムが下の方にリストアップされてきます。図３ではかなりの部分が隠れていますが，実際にアクセスしてウィンドウを大きくすれば，いろいろなボタン類が出てきて，画面を見ながらクリックしていけば操作できるように作られています。

Office Updateは，そのやり方自体は大して難しくありませんが，リストアップされてくる修正プログラムの導入順序というものに少し気を遣う必要があります。このことはWindows Updateにおいても同様に気を遣うべき作法のひとつ[(5)]ですが，順序を間違えるとUpdate処理が前に進みません。もちろんそういうときは警告と説明のメッセージが出た上で処理が一時停止するので，間違えて実行した結果システムを壊してしまう，という心配は全くありません。

Microsoftのソフトウェア製品には，Service Pack ？（？は整数）という形のマイナーバージョンアップがあります。これは各ソフトウェア製品の発売開始の後に発見されたバグや不手際をある時点ですべてかき集めて一つのパッケージとし，インターネットやCD-ROMの形でユーザに配

布されるものです。発売から時間が経過しているものほど上の？は大きく，新しくなっています。

Office Updateをするときには，まずその時までに出ているService Packを古いものから順にすべてインストールした後でないと，最新の修正プログラムをダウンロード・インストールすることができません。でも通常は，画面の説明を読めばどういう順序で導入すればいいかがわかるようになっていますし，おおむね新しいものほど下の方にリストアップされてきます。画面をよく見て慎重に行えば問題ないでしょう。

またOffice Updateの実行には，その時コンピュータに搭載されているOfficeを最初にインストール時に使用したCD-ROMが必要になります。Microsoftの説明によれば，これは著作権侵害行為を確認するためのものではなく，あくまでも技術的な仕様のようですが，CD-ROMを入れずにOffice Updateを開始すると，途中で止まり，正しいCDをコンピュータに入れないとつぎに進まなくなります。もちろん途中で入れて，画面に出るメッセージに適宜答えればUpdateは継続しますが，このメッセージには初心者にとって少しわかりにくい表現も使われているので，面倒を避けるために，あらかじめCDをコンピュータに入れておいてからUpdateをはじめるというのも良い方法です。

ソフトの質の良い悪いは別として，Microsoft Officeを日頃の仕事に積極的に使っている人，あるいは使わざるを得ず我慢しながら利用している人は多いと思います。近頃は大学の情報リテラシー系の授業においても，Microsoft Officeの使い方を教えるものが多く，いつの間にか逃げられない状況が作り出されてしまっています。

例えば，９月４日に発表されたOffice関連のセキュリティホールで影響を受けるソフトウェア製品は，

Visual Basic for Applications SDKバージョン5.0/6.0/6.2/6.3
Word 97/98/2000/2002
Excel 97/2000/2002
Access 97/2000/2002
PowerPoint 97/2000/2002
Publisher 2002
Project 2000/2002
Visio 2000/2002
など

となっています[6]。ここにあるWord2002とはWord XPのことですので，ほとんどすべてのOffice製品に脆弱性があるわけです。このようなソフトウェアを使い続けるためのコンピュータを不正な攻撃から守るためには，Windows Update同様，Office Updateの実行にも気を配っていかなければなりません。

Office Updateは表立って報道されることもあまりなく，Office製品を使っていてもそれらしきメッセージなどは出てきません。だからといってセキュリティホールをそのままにしておけばいずれ悪用されることもあります。そういうところに危機感を持たずに，ろくな対策もせずに使っ

ている一般ユーザが多いというところにクラッカーは付け込んで来ます。

何か被害を受けたらその時は若い者に復旧処理をさせればいいと考えている偉い人はどこにでもいると思いますが，いくらその人に権力があっても，攻撃によって消されてしまったデータを元に戻すことは簡単ではありません。日頃から必要最低限の危機感を持ち続け，Office Updateも忘れないようにしましょう。

３．インターネットオプションで一時しのぎ

WindowsシステムやOfficeのセキュリティホールが発見されたにもかかわらず，Microsoftの対応に時間がかかって修正プログラムの配布が遅れることがまれにあります。また，問題の種類によってはWindowsの仕様上の理由で解決策がなく，長期にわたり対策が施されないままのものもあります。このような場合には，システムのネットワーク関連設定を適切に操作することで，当面の危機を回避することができます。

この方法はインターネット上でよく「運用で逃げる」などと表現されていますが，あくまでも応急処置です。アップデートが配布され次第，それをインストールする必要があるのは言うまでもありません。

具体的なネットワーク設定は，Windowsの「インターネットオプション」で行います。これは前回第３話[7]で一部紹介したものですが，そこでは基本的機能の設定方法についてのみ説明しました。今回は残りのセキュリティ関連設定について述べていきます。

なお，第３話の時と同じく，ここで説明する設定はWindows本体のネットワーク機能とInternet Explorer及びOutlook Expressなどに有効なものです。NetscapeやMozilla，Operaなどのブラウザに関する諸設定は，それぞれのソフトウェアで行いますが，そちらについては各ソフトのオンラインヘルプ等をご覧ください。

インターネットオプションを画面に出すには，まず画面左下の「スタート」をクリックして，「コントロールパネル」をクリックします。

WindowsXPの場合，このコントロールパネルのアイコン配置が２種類あります。小さなアイコンの右側に長々と説明が付けられている表示形式は「クラシック表示」というもので，インターネットオプションのアイコンが出ています。そこをクリックすれば開きます。大きなアイコンにタイトルだけが付いた形式は「カテゴリの表示」というもので，続いて「ネットワークとインターネット接続」をクリックすることでインターネットオプションが出てきます。クリックして開きましょう。

XP以外のWindowsについてはコントロールパネルの表示形式は１種類だけです。インターネットオプションをクリックして開きます。

すると，

図４　インターネットのプロパティ

というウィンドウが現れます。これはWindowsXP Professionalのもので，他のWindowsでは若干見た目が異なりますが，内容はほとんど同じです。

今回は「セキュリティ」,「プライバシー」,「詳細設定」について説明していきますが，もし「運用で逃げる」という設定を行うとしても，初心者の人にお勧めできる設定箇所は限られています。

設定項目に精通しているユーザなら多くの部分に手を入れてチューンアップすることも可能ですが，いわゆる初心者の人があまり良くわからないままに適当に設定変更してしまうとシステムの動作がおかしくなることもあります。またチューンアップにより防御力が高くなると，その引きかえに，ネットワーク上のアブナイかもしれないものに接したときには，何らかのメッセージが出る場合があります。その内容と対応法がよくわからないために，かえってコンピュータが使いにくくなってしまっては困りものです。

もし，ユーザに負担の少ない形でもっといろいろな設定して，攻撃耐性を高めたいという場合は，後の方で紹介するセキュリティ対策ソフトウェアを導入しましょう。エレガントな防衛力のために必要となると設定を自動的にしてくれます。

ⅰ．セキュリティ

図４で「セキュリティ」タグをクリックすると，

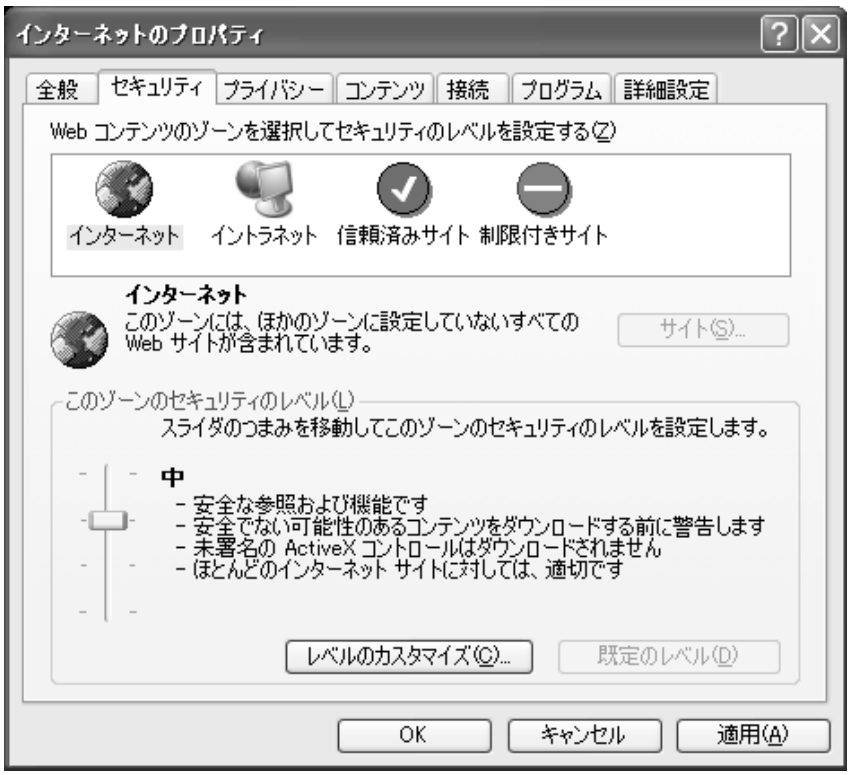

図５　セキュリティの設定

というような表示に切り替わります。

これは主にInternet ExplorerでWWWを利用する際のセキュリティ機能を設定するものですが，Outlook ExpressでHTMLメールを受信した場合などは内部的にInternet Explorerが呼び出されることで内容表示をしますので，そういった関連のソフトウェアにも影響のあるところです。

４つ並んでいるアイコンのうち，「インターネット」以外の３つはつぎのようなものです。

- イントラネット：所属している組織内部のネットワークにあるWebサイト
- 信頼済みサイト：攻撃してこないと信頼できるWebサイト
- 制限付きサイト：攻撃をしてくる可能性があるWebサイト

それぞれのアイコンをクリックすると，ウィンドウ内の右側の方にある「サイト」というボタンが押せるようになります。そこにユーザが，上の３つに該当するホームページのアドレスをそれぞれ入力することで，コンピュータは自動的に信頼したり防御したりできるようになります。ただしこれは必ずしも登録しなくても構いません。一般ユーザの皆様で登録をしている人は少数派だと思います。

図ではスライダが「中」になっています。これがWindowsのインストール時デフォルトですが，他には「高」，「中低」，「低」の３レベルがあります。スライダをドラッグすれば「中」以外に設

定を変えることはできます。

レベルが高いほど安全ですが，その代わりに機能が限られ，ホームページによってはすべての仕掛けを利用できず楽しめないことがあります。逆にレベルが低いほどインターネットと目の前のコンピュータの間にあるハードルが低くなって，さまざまなWWWの仕掛けを利用することができますが，その分防御が甘くなるので，悪意のある仕掛けが隠されているホームページを閲覧したときにはその餌食になる可能性があります。

通常は「中」で構わないでしょう。

もしも日頃から，兵器や薬物などのホームページやクラッカー御用達のような少し危険な匂いのするホームページ，そしてあくまでも研究上の必要に迫られてエロネタのホームページを見ることが多いというユーザは，スライダを「高」にしておいた方がいいかもしれません。危険な仕掛けはそういったホームページに潜んでいることが多いようです。

ただし，単純に「高」にするだけだと，Internet Explorerの使い勝手が悪くなるだけでなく，レベルが高いといってもまだ抜け穴的な部分は残っています。

そこでさらにチューンアップをして操作性と防衛力を両立させたいという人は，まずスライダを「中」にしておいて，つぎに「レベルのカスタマイズ」ボタンをクリックして設定ウィンドウを開き，セキュリティのカスタム設定を行います。

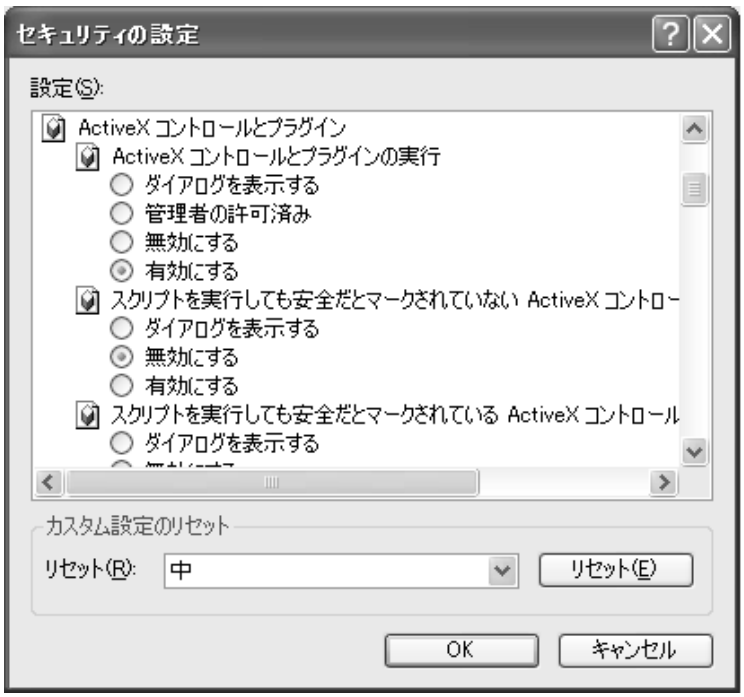

図６　カスタム設定ウィンドウ

この図６を採取したコンピュータにはセキュリティ対策ソフトのひとつであるNorton Internet Securityをインストールしてありますので，この部分はすでに自動的にカスタム設定になってい

ます。

セキュリティ対策ソフトがインストールされていなくても，図にあるような各項目を適宜クリックすればカスタム設定を手動で行えますが，その場合はすでに各設定項目について，それはどの機能に関することか，ひとつひとつ選ぶとそれぞれどういう結果が得られるか，ということを熟知している方が安全です。人からの話の聞きかじりと推測だけで，あまり良くわからないままに適当に設定を変えてしまうと，上にも書いたように動作全体がおかしくなるかもしれません。

Yahooなどで，キーワードに「インターネットのプロパティレベルのカスタマイズ」というように入れて検索をすれば，カスタム設定に関する情報は得られますが，やはり初心者の皆様には，そういった設定を自動で行ってくれるソフトの購入をお勧めします。サーバ用途なら高価ですが，普通のパソコンレベルの用途なら１万円以下で買えます。

ⅱ．プライバシー

図４で「プライバシー」タグをクリックすると，

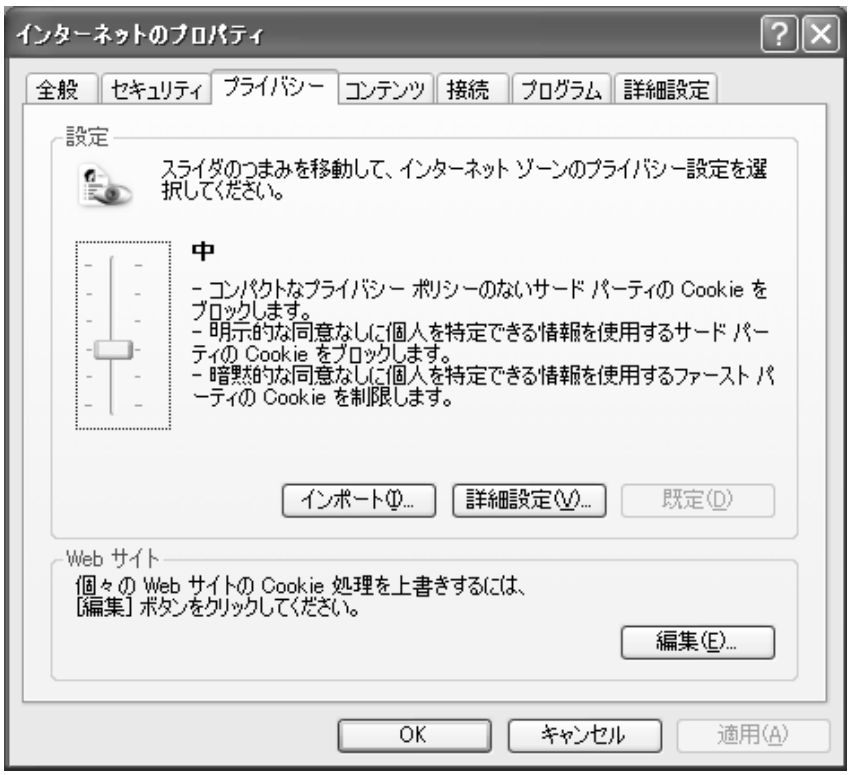

図７　プライバシーの設定

という表示に切り替わります。

プライバシー設定とはCookie設定のことです。Cookieとは，Internet Explorerなどのブラウザであるホームページを閲覧したときに，そのサーバ，あるいは提携している別のサーバから送られてくる小さなデータの塊です。ブラウザは受け取ったCookieを所定のフォルダに保存します。

次回同じホームページを閲覧すると，保存されているCookieがサーバに読み取られます。その内容によってサーバは，一見さんか常連か，さらにインターネットショッピングの場合はどういう趣味を持つ客か，などということを評価し，それに合わせたホームページの内容を表示します。

ある意味で便利な機能ですが，この仕組みが逆に危険であるということが時々指摘されます。ユーザの個人情報を何の暗号処理もせずにCookieに載せて使用するサーバがインターネットにはありますが，アブナイCookie処理は特に明示もされずに陰で行われるので，知らない間に大切な情報が外部に漏れてしまうこともあります。

そういった危険を，すべてではないにしてもある程度防ぐため，Cookie設定が必要になってきます。

ここにもセキュリティ設定と同じく左側にスライダがあります。図ではシステムデフォルトの「中」になっていますが，他にも「すべてのCookieをブロック」からはじまって，高，高－中，中，低，「すべてのCookieを受け入れる」まで，各レベルがあります。スライダを動かすと右側に説明が出るので，各レベルがどういう結果をもたらすか，わかると思います。

通常はスライダによる設定で十分ですが，もし心配なら詳細設定を行います。なお「インポート」ボタンは，カスタム設定をファイルから読み込むためのものですので，とりあえず無視しても構わないでしょう。

「詳細設定」ボタンをクリックすると，

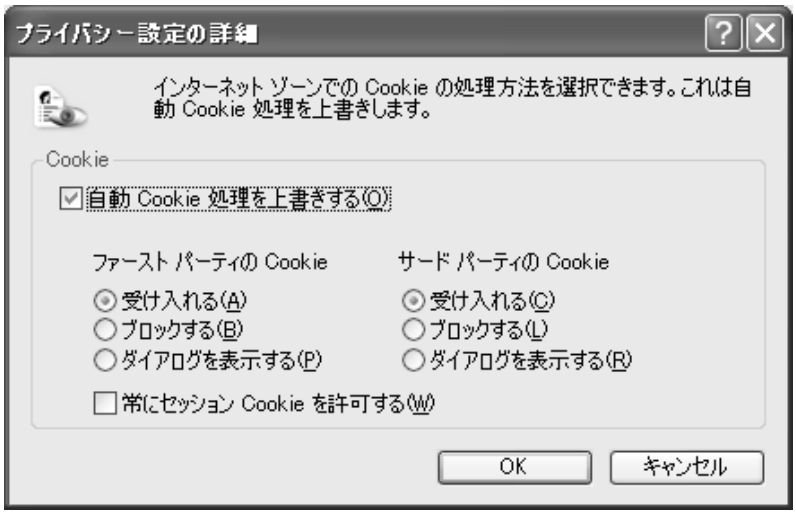

図８　Cookie詳細設定

Cookieの詳細設定が出てきます。通常Cookieは自動処理になっており，図中の「自動Cookie処理を上書きする」のところにチェックが入っておらず，それ以下の項目は選択できないようになっていますが，ここではあえて手動処理を行う状態を載せました。

ファーストパーティというのは接続したホームページがあるWWWサーバのことで，サードパーティとはCookie処理に関してファーストパーティと提携している他のサーバのことです。それ

ぞれについてCookieを受け入れるかブロックするか決めて設定します。また「ダイアログを表示する」というのは，Cookieが飛んできたときにその内容をスクリーン上に表示して，受け入れの可否をユーザに決めさせようとするための設定項目です。飛んでくるたびにメッセージが出るので少し面倒ですが，内容を見てから決めるというのも安全な手段の一つです。

なお，「常にセッションCookieを許可する」というところは，特に必要がなければチェックをはずしてOFFにしておけばいいでしょう。

また，このCookie処理についてもNorton Internet Securityのようなソフトを使えば，もっと詳細に，しかも自動でやってくれます。

ⅲ．詳細設定

図４で「詳細設定」タグをクリックすると，

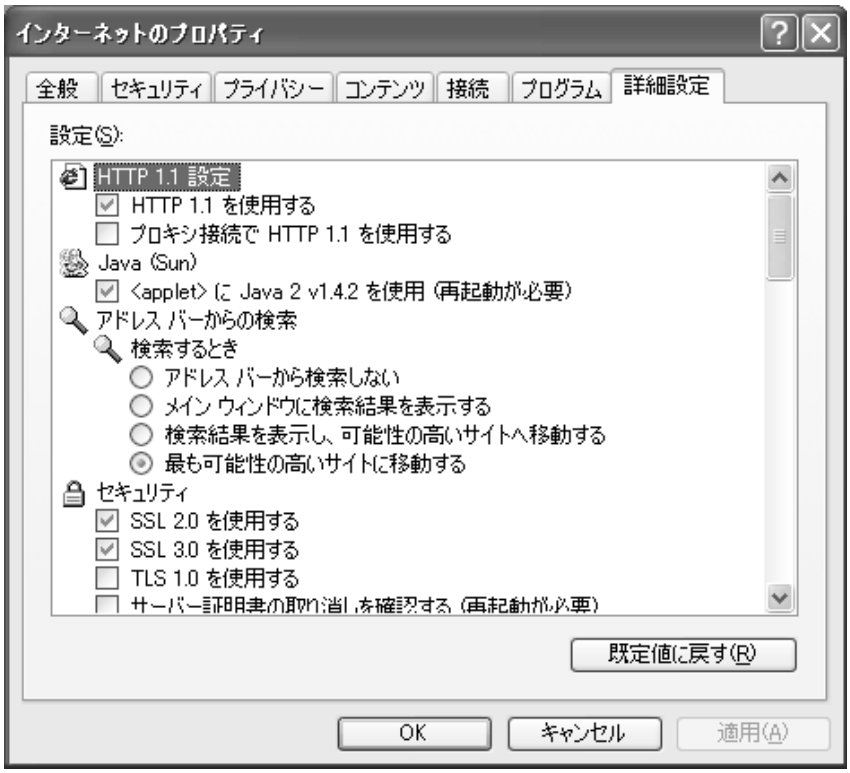

図９　詳細設定

インターネットの詳細設定が出てきます。

図中，「Java（Sun）」，となっているところが２行ほどあります。これはSun Microsystems製のJava（TM）2 Runtime Environment, Standard Editionというものをインストールしているため，ここに出ていますが，同じ機能はMicrosoft Java Virtual MachineとしてWindowsに組み込みとなっていますので，特に必要がなければ入れる必要はありません。

詳細設定においても，通常は触らずに，すでにでき上がっている設定のままで十分だと思いま

すが，もしも図の下の方に２つある「SSL…を使用する」のチェックがどちらかひとつでも外れているようなら，チェックを入れてONにしておきましょう。

SSLというのは，オンラインショッピングやインターネットバンキングなどのホームページと安全にデータをやり取りする際に使われる仕組みで，入力した個人情報は暗号化されて相手サーバに届きます。チェックが外れているとその暗号化機能が働きませんので，ここだけは一度確認しておいた方がいいかもしれません。

また，スクロールをすると下の方に「ブラウザを閉じたとき[Temporary Internet Files]を空にする」という設定項目があります。Temporary Internet Filesとは前回第３話[7]で説明した一時キャッシュのことですが，これがあまりに大きくなりすぎると，ハードディスクの特にCドライブに空き容量が乏しいときに，システム全体で重大な障害を招くことがあります。ディスク容量に心配がある場合は，この設定項目をONにするのが良いでしょう。

ⅳ．Outlook及びOutlook Expressのプレビュー

Windowsで電子メールを利用するソフトとしてOutlookやOutlook Expressを使っている人は多いと思います。OutlookはMicrosoft Officeに同梱されていますし，Outlook Expressにいたっては最近ではWindowsに組み込みになっています。

利用者が多いにもかかわらず，これらのソフトを使用するべきではない，という意見もインターネットなどで頻繁に目にすることができますが，使うべきではないと言われるのには理由があります。それはこの２つのソフトを使うことがウィルス蔓延の原因となる場合が多いからです。

OutlookとOutlook Expressには「プレビュー」という機能があります。新着メールが届くと，メールのタイトルの下に本文の一部が表示されるというものです。皆様も目にされていると思いますが，このプレビューがONになっていると，それによって「メールを見るだけで感染する」という種類のウィルスが蔓延するのです。ですから，安全のためにプレビューはOFFにしておいた方がいいのです。

Outlookの場合は，まず受信トレイの中身を表示しておいて，表示メニューから，

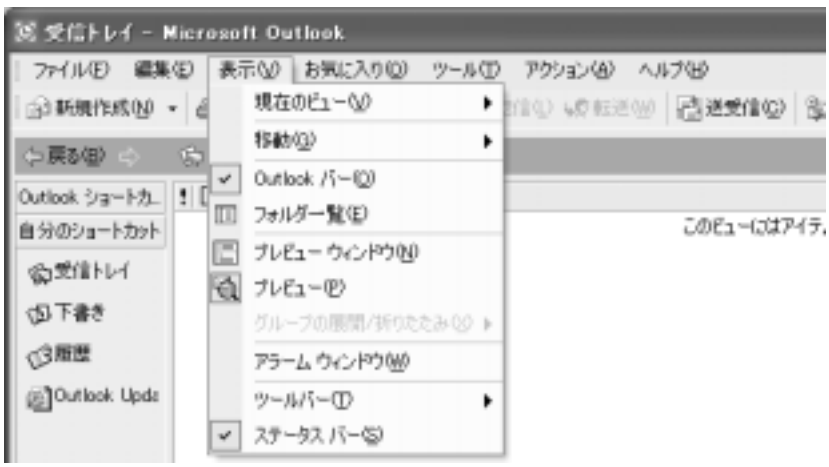

図10　Outlookのプレビュー設定

プレビューウィンドウを適宜クリックすることで，メールの「プレビュー」が出ないようにします。図中，受信トレイが空っぽになっているのは，私がOutlookを使っていないからです。

つぎにOutlook Expressの場合は，メニューで表示（V）からレイアウト（L）をクリックして出てくるウィンドウで設定します。

図11　Outlook Expressのプレビュー設定

図の下の方で，「プレビューウィンドウを表示する（P)」というところのチェックをはずしてあります。これがプレビューOFFの状態です。

プレビューを気に入って愛用されている方もいると思いますが，危険性があるという評判のある機能なのですから，泣いて馬謖を斬るがごとき覚悟でOFFにしましょう。

Ⅳ．Windowsセキュリティ対策ソフトウェア

ここではWindowsにおけるセキュリティ対策用のソフトウェアについて紹介します。

ここまでに述べたように，Windowsシステムのネットワークセキュリティを確保するためには，Windows UpdateやOffice Updateなどのサービスの利用や，適切なネットワーク設定の実施などに留意する必要がありますが，残念ながらそれだけでは不十分です。

これらの対策法はすでにあきらかになっているシステムの欠陥を修正するためには有効ですが，まだ知られていない新しいセキュリティホールをクラッカーが先に発見して悪用してくる攻撃には無防備な可能性があります。ましてコンピュータウィルスに対しては，専用のウィルス対策ソフトウェアを導入する以外にシステムを守る方法はありません。

Windowsにおけるこの手のソフトウェアで，昨今の状況から必ず導入するべきものは大きく分けて２つ，パーソナルファイアーウォールとアンチウィルスです。

パーソナルファイアーウォールというのは，ソフトウェアでパソコンにファイアーウォール機能を持たせるものです。通常のネットワーク管理に使用するファイアーウォールと違い，基本的にパーソナルファイアーウォールをインストールしたコンピュータのみを自己防衛するように設計されていて，そのコンピュータに対して外部からやってくる不正アクセスの検知・遮断や，内部から個人情報やCookieなどの重要データが漏れ出すのを防ぐ，などの機能があります。

アンチウィルスは文字通りコンピューターウィルス対策ソフトのことです。すでに発見済みのウィルスを検出・駆除するだけでなく，未発見の新種ウィルスに関しても高い耐性を持つように設計されています。

これらのソフトでは，既知の攻撃手法やウィルスをメーカーが解析して作成した「定義ファイル」というものを内蔵しており，それに基づいてコンピュータが被害を受けていないかどうかをチェックするとともに，同時に内蔵している独自の解析プログラムによって，新種の不正な信号やウィルスを検知して新手の攻撃に備えます。さらにメーカーは，インターネットを通じて新しい不正アクセス攻撃の種類や新種のウィルスに関する情報を常に収集しており，それによって「定義ファイル」を日々更新しています。

パーソナルファイアーウォールもアンチウィルスも，単に一度インストールするだけでは全く駄目で，この「定義ファイル」というものを常にダウンロードなどして，ソフトウェアを最新の状態に保たなければ，新種の攻撃に耐えることはできません。さもなければインストール後１，２日で対策ソフトは「古すぎる」状態になってしまいます。

幸いなことに最近のセキュリティ対策ソフトでは自動化が進み，各種設定やコンピュータの健康維持がほぼ自動的に行われるだけでなく，「定義ファイル」やプログラムアップデートのダウンロード・インストールも，特に設定を変更しない限りデフォルトで自動実行になっていますので，ユーザの負担はかなり軽減されています。

ただしバージョンアップに関しては基本的に自動化されておらず，別途購入などの手順が必要です。近頃はほぼ毎年新しいバージョンが発表されていますので，最新の安全を手に入れたければ，毎年買わなくてはなりません。これもWindowsの宿命と割り切って考えるしかありません。

これらのソフトはインターネットから無料のものをダウンロードして利用することもできます。このシリーズの第１話[8]で紹介したZone AlarmとAVG Antivirusですが，やはり名のとおった市販品の方が機能も確実ですし，信頼性も高いのではないかと思います。

現在，パソコン用セキュリティ対策ソフトとして，

- どこのパソコンショップでも売っている
- 手頃な購入価格
- 高機能でメーカーのサポート体制も充実
- 何よりも評判が良い

などの条件を満たし，かつパーソナルファイアーウォールとアンチウィルスが同時に手に入る商

品は，シマンテックのNorton Internet Securityと，トレンドマイクロのウィルスバスターです。機能的に若干差がある両者ですが，両方とも能力面では業界のトップクラスということになっていますので，どちらか一方を選べばいいでしょう。

なお両方購入して一緒にインストールしても，かえってシステム動作が変になるだけですのであまりお勧めできません。どちらか１つで十分です。

２つのソフトを使っての感想はつぎのようなものです。皆様が購入なさる際の参考にはなると思います。

Norton Internet Security

・インストールは実に簡単で定義ファイル更新も全自動。

・アンチウィルスは動作が機敏。

・ファイアーウォールは高機能だが初心者には少し難解な場合有り。

・設定など少し複雑な部分があるが，できる人には満足感有り。

ウィルスバスター

・インストール自体は簡単だが，ライセンスキーをなくすと面倒。

・アンチウィルスは少し動作が重い。

・ファイアーウォールは機能的にNortonより少し簡単だが，手間要らず。

・ユーザインタフェースが見易く，とにかく簡単でお気楽。

なお，値段はともに6,000～7,000円の範囲です。大学生協などでアカデミック品を買えばもっと安いでしょう。詳細は，各メーカーのホームページ，

シマンテック：　http://www.symantec.com/region/jp/index.html

トレンドマイクロ：http://www.trendmicro.com/jp/home/enterprise.htm

をご覧ください。製品情報だけでなく，コンピュータウィルスの基礎知識についてもかなり有益な情報が公開されており，相当に勉強になると思います。

なお，コンピュータ防御用のソフトでさらに高機能で安全確実なものをお望みの方にはお勧めの品があります。 http://www.blackice.jp/で紹介されているBlackICE PC Protectionです。このホームページには「MS BLAST亜種も未然に予防」と書かれています。

これについて紹介し始めるとキリがなくなるのでやめますが，現在使用していて満足しています。Norton Internet Securityと同時インストールで全く問題がないので，かなり高度な防御が可能になります。興味のある方は一度お試しください。

Ⅴ．スパイウェア対策

スパイウェアという言葉は，特に初心者の皆様にとってはあまり聞きなれないものだと思います。これも一種のソフトウェアですが，スパイという名前が付いているからといって，隣のあの人をスパイするためのものではありません。そういう他人をスパイするソフトは別に存在しますが，ここでそれについては触れません。

この文章の前半でも紹介しましたが，スパイウェアとは，このソフトを知らない間にコンピュ

ータに突っ込まれたあなた自身がスパイされるというタイプのものです。コンピュータウィルス同様に，できればスパイウェアも検出・駆除を行う方がいいでしょう。

駆除には専用のソフトを使いますが，有名なものは，

・Spybot Search & Destroy：無料，http://security.kolla.deからダウンロード

・Ad-aware：　　無料，http://www.lavasoft.deからダウンロード

の２種類です。

もう１つPestPatrol（http://www.pestpatrol.jp）というのがありますがこちらは有料で，９月10日発売で，定価は8,500円ということです。

現在２つの無料ソフトを使用していますが，機能的には問題ないと思います。特にSpybotの方にはアンチウィルスソフトのリアルタイムスキャナーのような機能があり，前半で紹介したように，ある有名検索エンジンのホームページにアクセスしたとたんにスパイウェアの転送を検知し，遮断してくれました。インストールも使用も簡単ですので，スパイされているかどうか心配なさっている方にはお勧めです。インストールして，あなたのコンピュータを一度スキャンしてみてください。おそらく，「えっ！？何これ？」とお思いになるでしょう。

Ⅵ．大団円

以上をもちまして，「初心者を悩ますWindowsのネットワークトラブル」と題して４回にわたりお送りしてきたシリーズは千秋楽でございます。ここまでお付き合いを賜りましたこと，厚く御礼申し上げます。

なお，このシリーズは，情報連携基盤センターニュースVol.１ No.１に掲載の拙著[5]よりとおしてお読みいただくと，一層話がつながります。

それではまたの機会にお目にかかります。まず無理なこととは思いますが，いつの日かWindowsがもっとましなオペレーティングシステムになることを期待しながら，お開きとさせていただきます。

参考文献

（１）Ross Anderson：「情報セキュリティ技術大全」日経BP社（2002）

（２）http://www.trendmicro.com/jp/security/general/overview.htm

（３）http://www.symantec.co.jp/region/jp/sarcj/data/w/w32.blaster.worm.html

（４）HACKER JAPAN 7　2003 JUL. 白夜書房（2003）

（５）加藤浩樹：「Windows Updateのすすめ」名古屋大学情報連携基盤センターニュース，Vol.１ No.１（2002）pp61-89

（６）http://headlines.yahoo.co.jp/hl?a=20030905-00000098-myc-sci

（７）加藤浩樹：「利用者向け講座：初心者を悩ますWindowsのネットワークトラブル　第１話　概説とWWW関連トラブル」名古屋大学情報連携基盤センターニュース，Vol. 2　No. 1（2003）pp28-54
（８）加藤浩樹：「利用者向け講座：初心者を悩ますWindowsのネットワークトラブル　第３話　基本的なネットワーク設定について」名古屋大学情報連携基盤センターニュース，Vol. 2　No. 3（2003）pp300-319

（かとう　ひろき：名古屋大学大学院国際開発研究科）