ＩＴにおける安全性（セキュリティー）

最近よく聞かれるセキュリティーという言葉は、安全性という意味の英語です。インターネットの世界では、特にセキュリティーが問題になります。というのは、インターネットは誰でも自由に使えるオープンなネットワークであるため、悪意を持った人も自由に使えるからです。
現在、インターネットを通してコンピューターのデータが勝手に書き換えられたり、盗まれたり、破壊されたりといった事件が頻発しています。このようなコンピューターの高度な技術を駆使した犯罪行為を行う人達をハッカーと呼ぶことがありますが、ハッカーとは本来、高度な技術者に対する尊称です。悪意を持った技術者は正式には、クラッカーと呼びます。
現在の情報化社会では、このような高度な技術を駆使した、いわゆるハイテク犯罪というものが多発化している一方で、高度な技術を必要としない、いわゆるローテク犯罪というものも多発化してきています。

ここでは、クラッカーその他の悪意を持った人達がどのような犯罪行為を行っているのかを解説し、対処方法を述べることにします。
詳しくは、下記の警視庁などのホームページを是非ご一読下さい。万一これらの犯罪にあった時は、警察に届けて、相談を受けてください。

警視庁：	http://www.keishicho.metro.tokyo.jp/haiteku/index.htm ℡　03-3431-8109
千葉県警：	http://www.police.pref.chiba.jp/safe_life/cyber_crime/ ℡　043-227-9110

１．コンピューター・ウイルス

クラッカーが行う悪事の一つとしてあげられるのが、コンピューター・ウイルスを作成してインターネット上にばら撒くという行為です。
コンピューター・ウイルス（以下、ウイルスと略す）とは、クラッカーによって仕掛けられた悪意のあるソフトウェアのことで、人体ではなくコンピューターに感染します。
ウイルスには、データやソフトウェアを盗み取ったり、破壊したり、書き換えたり、画面に勝手な文字や絵を描いたり、インターネットを通して他のコンピューターを攻撃したり、インターネットを渋滞状態にしたりと、様々なタイプのものがあります。また、潜伏期間をおいてから活動を開始するものが多く、現在パソコンが正常だからといって安心できるものではありません。例え自分のパソコンが被害を受けなくても、自分のパソコンが他人のコンピューターを攻撃するための踏み台にされるということもあります。
以前はフロッピー・ディスクを通してウイルスに感染することが多かったのですが、インターネットの普及した現在では、大部分はインターネット、特にＥメールを通して感染しています。しかもその感染力は、フロッピー・ディスク経由とは比較にならないほど大きくなっています。もはや、インターネットに接続したパソコン所有者にとって、ウイルス対策は不可欠である言えます。

万一ウイルスに感染し、ハードディスクの中のデータやプログラムが破壊された場合には、一旦ハードディスクにフォーマットをかけてから、OS（基本ソフト)から導入し直す（または、リカバリーCD-ROM でパソコン購入時の状態に復元する）といった作業が必要になってきます。その場合、個人で作成・保存したファイルは自分で復元する必要があるため、**予めパソコンが正常に稼動している時にバックアップを取っておく必要があります。**

最善の対処をするためには、ワクチン・ソフトと呼ばれるソフトウェアを使って予防及び駆除を行います。
ワクチン・ソフト（以下、ワクチンと略す）は、ウイルス駆除ソフトとかアンチウイルス・ソフトなどと呼ばれることもあります。著名なワクチンとしては、トレンドマイクロのウイルスバスターやシマンテックのNorton Internet Security（下記 URL 参照）などがあります。ウイルスは常に新型が開発されているため、ワクチンについても頻繁に更新が必要になります。最近のワクチンでは、更新作業をインターネット経由で自動的に行うものが主流になって来ています。

ワクチンをインストールしておけば、99.99%以上程度の確率で安全だと考えられます。（ワクチンといえども未知のウイルスには対応できませんので、100%安全が保障されるわけではありません。）

トレンドマイクロ:	http://www.trendmicro.com/jp/products/personal.htm
シ マ ン テ ッ ク：	http://www.symantec.com/region/jp/products/nis/

なお、トレンドマイクロのホームページ（http://www.trendmicro.co.jp/hcall/index.asp）には無料でウイルス検索を行ってくれるページもあります。

１．１．Eメールを通じてのウイルスの感染

ウイルスはＥメールに添付されることによって、他人のコンピューターに容易に送付されます。また、HTML形式のメールの場合には、ホームページの形式を利用したウイルス（後述）の送信方法もありますので、同じく注意が必要です。

自分のＥメール・アドレスをホームページに掲載するなどして一般公開している者は狙われやすいので、なるべくＥメール・アドレスを公開することは避けた方がいいでしょう。しかしウイルスは、いったん誰かのパソコンに感染すると、そのパソコンのアドレス帳に載っているＥメール・アドレスに片っ端からウイルス・メール（ウイルスの添付されたメール）を送るなどの仕組みがあるため、一般公開していないＥメール・アドレスも安心はできません。また、クラッカーがあてずっぽうのＥメール・アドレスにウイルス・メールを送ることもあります。

以下にウイルスの感染を防ぐための注意事項を述べます。

なお、下記の事項のうち、**デマ・ウイルスは単に人を騙すメールであって、ウイルスが組み込まれたメールではありません。ご自分で騙されないように気をつけて下さい。**デマ・ウイルス以外はワクチンによってほとんど対処できます。

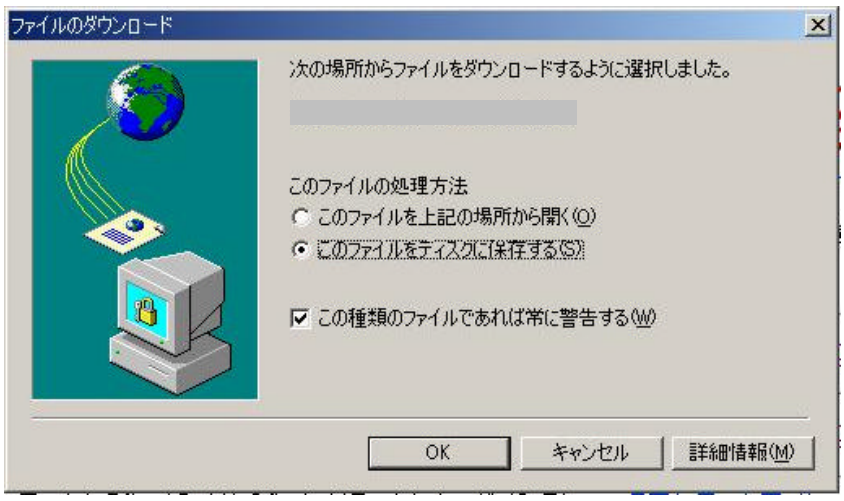
- 受信したメールに添付ファイルがついている場合は要注意です。特に、メールの送信者欄が消されている場合は、まずウイルスを含んだメール（以下、ウイルス・メールと略す）と考えられます。外国人とは付き合いがないにもかかわらず外国語のメールが来たという場合も怪しいですし、見知らぬ送信者から送られて来たメールも要注意です。また、ウイルス・メールは送信者のメール・アドレスを書き換えて他人を装ったり、あるいは、他人のコンピューターに感染した後、そのアドレス帳に書かれている宛先に勝手にウイルス・メールを送付する等の仕組みもあるので、送信者が知人のメール・アドレスになっていても信用はできません。添付ファイルがついている時は、開く前に送信者に直接確認することが望ましいでしょう。
- ウイルスは通常、実行可能なファイル形式でメールに添付されます。Microsoft の電子メール・ソフト(Outlook Express)の旧版には添付ファイルが自動的に実行できるような仕組みが組み込まれており、この仕組みを利用して感染するウイルスもあります。さらには Outlook Express ではプレビューウィンドウという、メールを自動的に開く画面まで用意されているため、開くつもりのないウイルス・メールが自動的に開かれてしまうということもあります。これを防ぐためには Outlook Express を最新版に更新し、また Outlook Express のメニュー・バーから「表示」→「レイアウト」を選択し、「プレビューウィンドウを表示する」の項目のチェック・マークをはずしておいて下さい。(Outlook を使用している場合にも同様の注意が必要です。)
- 添付ファイルが実行可能な形式かどうかは拡張子で判断できますが、Windows の通常の設定では拡張子が見えません。それを利用して、添付ファイル名を実行可能形式でないかのように見せかけているウイルス・メールもあります。騙されないようにするためにも、常に拡張子を表示するように設定変更しておくことをお勧めします。
- 添付ファイルが Word や Excel などのファイルの場合は、マクロ・ウイルスと呼ばれるウイルスが付着していることもあります。これは Microsoft の Office 製品に備わっているマクロと呼ばれるプログラム機能を利用したウイルスです。通常の Word や Excel の設定では、マクロを含んでいるファイルを開くときには警告のメッセージが表示されます。その場合は、「マクロを無効にする」ボタンをクリックすればマクロは実行されません。なお、ファイルの送信者にマクロの実行の可否を直接確認することが望ましいでしょう。念のため Office 製品の（マクロの）セキュリティー設定を確認しておくことを

お勧めします。

- 受信したメールがHTML形式メールの場合、その本文中のどこかをクリックするとウイルスがダウンロードされてくるという形式のウイルス・メールもあります。これはホームページを通じてウイルスに感染するのと同じ原理によるものです。（Outlook Express および Internet Explorer の古いバージョンでは、クリックなどの操作をしなくても勝手にウイルスがダウンロードされるという仕組さえあります。）これを防ぐためには、HTML メールを受け付けない電子メール・ソフトを使用するというのも一つの対処方法です。
  なお、Outlook Expressのデフォルトの設定では、作成するメールは自動的にHTML形式になってしまいます。HTML形式は本来のメールの形式ではないため、受信者側のEメール・ソフトによっては、HTML形式メールを見られないものもあります。HTML形式のメールを使用することは好ましいことではありませんので、以下のようにして設定を変更しておきましょう。
  Outlook Express のメニュー・バーより、「ツール」→「オプション」と選択し、「オプション」ウィンドウの中で「送信」タブをクリックし、「メール送信の形式」を「HTML形式」から「テキスト形式」に選択変更します。また、「受信したメッセージと同じ形式で返信する」のチェック・マークをはずします。最後に「OK」ボタンをクリックします。
  このように設定変更しても、Windows Update などの更新時にOutlook Express の設定が勝手に書き換えられることがありますので、更新時には再度確認が必要です。
- 嘘のウイルス情報を書いたデマ・ウイルスと呼ばれる種類のメールもあります。これはウイルスが組み込まれたメールではなく、人を騙すメールです。例えば「SULFNBK.EXE という名前のファイルはウイルスなのでファイル名で検索し、見つかったら直ちに削除してください。このウイルスは通常のワクチン・ソフトでは駆除できません。あなたのお友達にも早急にこのことを教えてあげてください。」といった嘘の情報が書かれたメールです。このメールを信じて指定されたファイルを削除すると、パソコンの OS（基本ソフト）が動かなくなったりします。こういったメールを信用してはいけません。ましてや、他の人たちにこのメールを転送したり、外国語で書かれたメールをわざわざ日本語に翻訳して転送するといった行為をしてはいけません。

１．２．ホームページを通じてのウイルスの感染

ホームページにアクセスしている時にもウイルスに感染することがあります。ホームページにアクセスしている時には、プログラムのダウンロードにご注意ください。通常はダウンロードの前に下図のようなウィンドウが表示されます。ホームページが信頼できないときや、必要のないファイルは、すべてキャンセル（「キャンセル」ボタンをクリックする）した方がよいでしょう。



また、下図のようなウィンドウが表示される場合はダウンロードするプログラムに電子署名(身元証明書)がついているので信頼性が増しますが、完全に信頼できるという保証はありません。例えプログラムの送り主が著名な会社であることがわかっても、その会社の中にクラッカーがいないとは断言できないからです。

ActiveX（アクティブエックス）と呼ばれる種類のプログラムは通常この形式で送られてきますが、ダウンロード後、直ちに自動的に実行されるものがほとんどです。安全のため、必要のないプログラムは「いいえ」ボタンをクリックして拒否した方がよいでしょう。あるいは、Internet Explorer の設定により、ActiveX を実行できないようにすることも可能です。

Internet Explorer の設定変更によって、ある程度セキュリティーを向上できますが、やはり**最善の対処方法はワクチンを使用することです。**

２．クラッカーの不正アクセス

クラッカーが行う悪事には、他人のコンピューターに勝手にアクセス（侵入）してデータを盗み読んだり、勝手にコンピューターを操作したり、ウイルスを送り込んだりするという行為もあげられます。したがって、何らかの対策を取っておかないと、知らない間にパソコンの中に入れておいた個人情報が盗まれたり壊されたりするということもあります。

本来、OS（Windows などの基本ソフト）は、このような外部からの不正アクセスを防ぐように作られているべきですが、現実にはセキュリティーの欠陥（セキュリティー・ホールと呼ぶ）が頻繁に発見されており、クラッカーに不正アクセスされることがあるのです。

クラッカーからの不正アクセスを防ぐ簡単な方法は、インターネットに接続しないか、あるいは、なるべく接続時間を減らし、クラッカーが入り込む確率を小さくすることです。ADSL や光ファイバーなどで常時接続している場合でも、パソコンの電源をこまめに切るなどして、なるべくコンピューターにアクセスできる時間を短くするべきです。また、インターネットに接続するパソコンと個人情報や機密情報を入れるパソコンを別にするというのも一つの対処方法です。

また、Windows Update（Windows を最新の状態に更新すること）をこまめに行って、セキュリティーの最新の修正を取り込んでおきましょう。ただし、その修正内容の中にさらにセキュリティー・ホールが含まれていることもありますし、Windows Update をした結果、かえって不具合が発生するということもまれにあります。

不正アクセスを防ぐ最善の方法は、ファイア・ウォール（不正アクセスを防御するソフトウェアあるいはハードウエア）を使用することです。トレンドマイクロのウイルスバスターにもファイア・ウォールの機能が含まれています。

不正アクセスはインターネットに接続している間に発生するだけではありません。

たとえば、スパイウェアと呼ばれるソフトウェアがあります。これは、外見上は有用なフリーウェア（無料で提供されているソフトウェア）の形態を取っていることが多く、表面上は有用なソフトウェアとして働いてくれますが、その裏でこっそりとパソコンの中に入っている個人情報を盗み取って記憶しておき、パソコンがインターネットに接続された時にその情報をインターネットに送り出すものです。いわば、スパイのような働きをするソフトウェアです。場合によっては普通の有料製品の形態を取っている場合も考えられ、外見だけでは通常のソフトウェアと区別がつきません。通常のウイルスと違って破壊行為を行わないので気が付きにくく、被害報告も少ないものです。

トレンドマイクロのウイルスバスターなどのソフトウェアにもスパイウェアをチェックする機能が含まれていますので、このようなソフトウェアを使ってスパイウェアを防ぐことをお勧めします。

他にも不正アクセスを招く要因になるものがいくつかあります。例えば、**ICQ（チャット）などを**利用して文字や音声でおしゃべりを楽しんでいる人も多いですが、これらを利用すると自分の IP アドレス（インターネットを電話網にたとえれば、電話番号のようなもの）を公開することにもなります。ICQ は普通、ファイア・ウォールを解除して使用する形を取るため、クラッカーに自分の居場所を知らせて、かつ、侵入口を開放していることにもなりかねません。不正アクセスの機会をつくる恐れがあるため、**なるべく利用しないようにしましょう。**利用するときは、ファイア・ウォールを有効にし、必要最小限のポート(通信窓口)だけを開けるようにしましょう。

ファイル交換ソフトあるいは**ファイル共有ソフト**と呼ばれるソフトウェアも IP アドレスを外部に知らせ、同様の危険をおかすことになりますので、基本的には利用しないようにしましょう。とくにこの種のソフトウェアは著作権法違反などの犯罪の温床になっていますので、ご注意ください。

また、インターネット上の掲示板（伝言版）に書き込みをすることも IP アドレスを知らせることになります。クラッカーが提供している掲示板だった場合、書き込みをした瞬間に不正侵入されるという可能性もあります。掲示板（伝言版）へもむやみに書き込まないようにしましょう。

３．インターネットを通過するデータの盗み読みや改竄

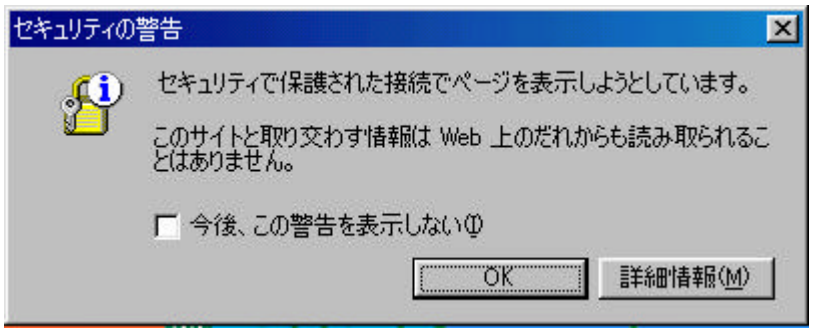
クラッカーが行う悪事には、インターネットを流れるデータを途中で盗聴したり（盗み読んだり）、書き換えたりといったものもあります。

インターネットでショッピングする時に、決済方法としてカード払いを選ぶ場合があります。この場合、クレジット・カード番号をインターネット上に送信することになりますが、なるべく避けた方がいいでしょう。クレジット・カード番号は秘密にすべき番号です。**どうしてもクレジット・カードを使いたい時は、SSL と呼ばれる安全な仕組みを使用しているホームページで行って下さい。**(SSL よりももっと安全な方法も存在しますが、残念ながら一般には普及していません）SSL を使うかどうかの選択形式になっているホームページでは迷わずに SSL を選択してください。あるいは自動的に SSL が使用されるホームページもあります。

SSL ではインターネットを通るデータが暗号化されるため、クラッカーにクレジット・カード番号を読み取られることはまずありません。SSL が使われていると Internet Explorer の右下の方に錠のアイコン（  ）が表示されますので直ぐわかります。錠のアイコンが出ていないホームページは危険ですので、クレジット・カード番号等の個人情報を送信しないようにして下さい。

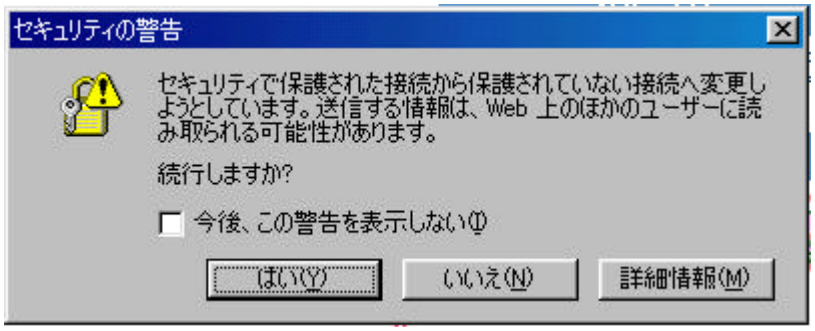
一般に、ショッピングなどの**プライベートな情報のやり取りは SSL 等の安全下で行うべきです。**例えば、暗号化がかかっていない状態だと、購入する商品や商品の送り先がクラッカーによってインターネット上で書き換えられるなど、取引情報が改竄される恐れもあります。

なお、SSL はつねに使われているわけではなく、購入手続きに入る段階など、必要な時だけに使用開始されるのが普通です。その切り替わりの時、すなわち、SSL で保護されていない Web ページから SSL で保護されている Web ページに変わろうとするときには、次のようなメッセージ・ウィンドウが出ますが、これは正常です。そのまま「OK」ボタンをクリックしましょう。



また、ショッピングの手続きが完了した後など、SSL で保護されている Web ページから SSL で保護されていない Web ページに変わろうとするときには下のようなメッセージ・ウィンドウが出ますが、これも正常で

す。ただし、保護されていない Web ページに入るということを意識しておいて下さい。これから以後は機密情報や個人情報を入力してはいけない、ということになります。



ただし、例え SSL が使われていたとしても、それだけで安全が完璧になるわけではありません。SSL によってインターネット上では暗号化が行われていても、ホームページの（お店の）コンピューター自身にセキュリティー・ホールがあるかも知れないからです。お店のコンピューターに一旦クレジット・カード番号などが渡ると、セキュリティー・ホールを通してクラッカーがその情報を読み取る可能性もあります。あるいは、お店のコンピューター担当者に悪い人がいると、その人が情報を盗み読んで悪用することも考えられます。結局のところクレジット・カード番号は使わない方が無難です。

なお、クレジット・カードは現実のお店でも、磁気カードがそのままコピーされて悪用されるなどの犯罪が頻発していますので、素性の不明なお店は避け、決済時に店員の行動をよく監視しておく必要があります。例えば、通常のクレジット・カード読み取り装置（CAT）にカードを通す以外に別の装置にもカードを通していたり、影に隠れてカードを操作したりしていたら、カードをコピーしている可能性があります。（現在、クレジット・カード業界では安全なＩＣカード（スマート・カード）への置き換えが進められていますが、過渡期には磁気カードを兼用したスマート・カードが使われるので、当分の間は従来の磁気カードの時と同じ犯罪に遭遇する可能性があります。）
また、カードの表面の文字が読み取られただけで悪用される恐れがありますので、レジに並んでいる時にも、ぎりぎりまでクレジット・カードを出さないようにするか、あるいは、なるべくクレジット・カードを隠して持つ（少なくとも番号と名義と有効期限を他人に見られないようにする）ように注意してください。

カード番号が盗み取られたり、カードがコピーされたりした可能性がある場合は、直ちにクレジット・カード会社に連絡して相談してください。
また、クレジット・カードでいつ何をいくらで買ったかは、日頃からきちんと記録するようにし、クレジット・カード会社から利用明細書が送られてきたら、必ずただちに内容を照合するようにしましょう。実際にクレジット・カードが悪用された形跡がある場合は、警察にも連絡して下さい。通常、クレジット・カードには保険がかかっているため、これらの損失は保険によってカバーされますが、そのためには警察への届出が前提になっている場合があります。

インターネット上のショッピングでは、その他さまざまな方法で、犯罪に遭遇する可能性があります。例えば、銀行振込を利用した場合にお金を振り込んでも商品が送られてこないとか、代金引換で受け取った商品の箱を開けてみたら、クズ同然のものが入っており、後でお店に連絡を取ってみたら、所在不明であったということもあります。**インターネット上のお店は、信頼性が確信できない限りは利用しない方が賢明でしょう。**
インターネット上のオークションやフリー・マーケットでも同様に詐欺事件が頻発しています。ショッピング同様、注意しましょう。

４．ダイヤルＱ２や国際電話への自動切換え

あるホームページ（特にアダルト・サイトなどに多い）にアクセスすると、特殊なソフトウェアがパソコンに組み込まれ、そのソフトウェアが勝手にダイヤルＱ２や国際電話の番号に電話を掛け直し、後で高額な電話料金が請求されるというものがあります。（請求額は小額の場合もあります。）
これらのほとんどは犯罪行為であり、警察に連絡すべきものです。

しかし、中には「このボタンをクリックするとダイヤルＱ２に接続します」などと明示してあるものもあります。この場合は犯罪にはあたらないということになってしまいますので、よく読んでから操作するように注意して下さい。(たとえ外国語で書かれていても、きちんと読んで意味を理解してから操作する必要があります。)

勝手にダイヤルＱ２や国際電話につなげられることを防ぐためには、ＫＤＤＩが無料で提供しているダイヤルアップ・チェッカー（http://www.kddi.com/topics/atx/image.html）などのソフトウェアを利用する方法があります。また、NTT や KDDI に連絡して、ダイヤルＱ２や国際電話の電話がかけられないようにしてもらうこともできます。

なお、電話（アナログまたは ISDN）経由でインターネットに接続している場合（電話線がパソコンにつながっている場合）にのみこの犯罪に遭遇する可能性があり、**ADSL や光ファイバーによるインターネット接続など電話を使わない形式ではこの犯罪に遭遇することはありません。**(ADSL は途中までは電話線を使っていますが、途中からスプリッターという装置で電話用の線とインターネット用の線を分けており、電話用の線はインターネット接続には使いません。つまり、電話経由でインターネットに接続しているわけではありません。とはいっても電話用の線をパソコンにつなげば、電話経由でインターネットに接続することも可能であり、わざわざこのようにした場合には上記の被害に遭遇する可能性もあります。)

５．ファイルの盗み読み

パソコンを修理に出している時に修理業者がハードディスクの中を覗くということもありうるため、**パソコンの中には暗証番号などの機密情報や個人情報は入れないようにするか、あるいは暗号化などの安全策を施しておくべきです。**

また、パソコンのハードディスクに書き込んだデータは通常の削除方法では完全には消えません。たとえごみ箱から削除しても完全には消えたわけではなく、単に（ハードディスク上に）削除されたという意味のマークがついているだけで、データそのものが消されたわけではないのです。最近ではデータ復元ソフトなどと呼ばれるソフトウェアが市販されており、これを使うことにより誰でもデータを復活できるようになっています。

したがって、削除したはずのファイルでさえも、パソコンを廃棄したり、他人に譲渡したり、修理に出したりするときに、盗み読まれてしまう恐れがあります。

こういったファイルの残存を抹消するための、ディスク完全削除ソフトも市販されていますが、パソコンを使用している最中にいきなり故障して修理に出したという場合にはディスク完全削除ソフトを実行できないでしょう。暗号化ソフトを使って暗号化しておいた場合でも、暗号化前のファイルが（見かけは削除されていても）ディスク上に残っている可能性があります。これにはディスク全体を完全削除するソフトでは対処できませんので、**ファイルを暗号化した直後に**弊社の「ディスク消えるんです！」などを使って（ディスク全体ではなく）**削除されたファイルだけを完全削除するという対処を行った方がよいでしょう。**

あるいは、個人情報や秘密のデータは一切ハードディスクに入れず、外部記憶媒体に保存するようにし、外部記憶媒体は絶対に他人には渡さないようにするという対処方法もあります。

なお、フロッピー・ディスク上のデータはディスク完全削除ソフトで完全削除できますが、CD-R はソフトウェアでは削除できません。**CD-R の場合は、ラベル面（レーザー光が当らない方の面）からナイフで細かく切り込みを入れることにより読み取り不可能にできます。**特に一番中心部に目録に相当するデータが入っていますので、集中的に切り込みを入れて破壊しておきましょう。(焼却してしまえばよいと思われるかも知れませんが、CD-R を燃やすことは法律や条例等の規制に抵触しますのでご注意下さい。)

６．他人のパソコンを直接操作しての悪用

たとえば、会社や個人宅に客として訪問してきた人の中にクラッカーがいると、応対者が目を離している隙に人のパソコンを勝手に操作して機密データを盗み取ったり、ウイルスを感染させたり、あるいは、パソコンに記憶されているユーザー名・パスワードをそのまま利用してインターネット・ショッピングするといった行為を行う可能性があります。この場合はファイア・ウォールでは対処できません。

（ピッキング等の行為によって）無断で入室し、パソコンだけを操作して跡形もなく立ち去るというクラッカーもあります。この場合、空巣と違って物が盗まれるわけではないため、ほとんど証拠が残らない場合があります。あるいは、会社の社員の中にクラッカーいて、コンピューター内の機密情報を盗み出したり、

顧客情報を流出したという事例もあります。

このような問題に対処するためには、パソコンや重要ファイルをパスワードで保護し、パスワードは自分以外には絶対にわからないようなものにしておく必要があります。

クラッカーは他人のパスワードを見つけ出したり推測したりして、他人のユーザー名で人のコンピューターにログインしたり、他人名義でインターネット上のサービスを利用しようとします。**パスワードは他人には推測できないような無味乾燥なものにし、絶対に他人に漏らさないようにして下さい。**

（なお、Windows95，98，Me は一見パスワードで保護できるように見えますが、実際はパスワードがわからなくても容易にログインできてしまい、安全ではありません。というよりも、最初からパスワード無しで使用しているのが普通です。安全にするためには、市販のセキリティー関連ソフトウェア製品を組み込んで、ロックがかかるようにしておくことが望ましいでしょう。）

ところで、Internet Explorer にはオートコンプリートという機能があり、インターネット・ショッピングなどでの入力項目（ユーザー名、パスワードなど）を自動的に記憶してしまいます。このままでは、クラッカーが無断で他人の部屋に侵入してパソコンを操作した際に、オートコンプリート機能で記憶されているパスワードを悪用して利用してしまうという問題があります。これは、ワクチンでもファイア・ウォールで防ぐことはできません。

このような問題に対処するためには、**以下のようにして Internet Explorer のオートコンプリート機能を停止しておきます。**

1. **Internet Explorer を起動し、「ツール」メニューから「インターネットオプション」を選択します。**
2. **「コンテンツ」タブをクリックして、「個人情報」の欄の「オートコンプリート」をクリックします。**
3. **「オートコンプリートの使用目的」欄の「フォームのユーザー名およびパスワード」のチェックをはずすと、パスワードの保存が停止されます。同様に「フォーム」のチェックもはずしておきましょう。パスワード以外にインターネットに送信される一般のデータも保存しなくなります。**
4. **「オートコンプリート履歴のクリア」欄の「パスワードのクリア」ボタンをクリックすると、現在まで記録しているパスワードが消去されます。**
5. **「OK」ボタンをクリックして設定完了です。**

７．電波の盗聴

最近、無線ＬＡＮ（ラン）という仕組みを使ってインターネットとパソコンの間を電波で中継している家庭も増えてきました。本来ＬＡＮとは建物・構内などの局地内におけるコンピューター間の通信ネットワークであり、家庭内の複数のパソコン同士でも通信できます。

インターネット・カフェなどでも無線ＬＡＮの環境を提供し、パソコンを電波でインターネットにつなげられるようにしている所もあります。

このような電波は建物の外にも漏れますので、盗聴が可能です。家庭内で**無線ＬＡＮを使用する場合は、暗号化の機能を使って**、盗聴されても解読できないようにすればいいのですが、**インターネット・カフェでは**勝手な設定はできませんので、**個人情報をインターネットで送信することはやめましょう。**

例え無線ＬＡＮを使っていなくても、パソコンの各装置から常に微弱電波が発信されているため、これを建物の外で盗聴することによってパソコンの入出力データを読み取ることも可能です。この盗聴方法は元々米国の国防総省で開発された技術であり、かなり高度な技術力を必要とするため、めったに遭遇することはないと思われます。対処方法としては、パソコンの周囲を金属板や細かい目の金網で囲むという方法があります。また、この電波漏れを防ぐためのシールド（電波を遮断する装置）も市販されています。

８．その他、ローテク犯罪など

以上は主にハイテク犯罪について説明してきましたが、ここからはローテク犯罪など、その他の注意事項について述べておきたいと思います。

最近、Ｅメールや郵便、電話などを通して、身に覚えのないアダルト・サイトなどの利用料を請求されるという事件が頻発しています。これに対し、家庭の誰かがアダルト・サイトにアクセスしたものと思い込ん

で支払いをしてしまう人もいます。数万円程度の料金が請求される場合が多く、支払い可能な額なので払ってしまった方が面倒がないと思ってしまうようです。しかし、これらの請求のほとんどはサギです。

また、家計が苦しい家庭で、預金口座に振込みがあり、何の振込みか覚えがなかったけれどお金を使ってしまったところ、後で闇金融らしき組織から法外な利息付で返済を迫られたという事件が頻発しています。

このようなローテク犯罪にまきこまれた場合は、警察に連絡し相談してください。

また、ワンクリック料金請求やフィッシング詐欺といった新手の犯罪も多発しています。これらは一見ハイテク犯罪のように見えますが、必ずしも高度な技術を使っているわけではなく、その多くは巧妙に人を騙そうするローテク犯罪の一種です。1 ページの警視庁のホームページなどを一読の上、この手のメールは一切無視するようにしてください。

インターネット上には、アンケートその他、さまざまな方法で個人情報（個人名、家族構成、住所、電話番号、Ｅメール・アドレス、インターネット接続の有無、家計の事情、預金口座番号、クレジット・カード番号など、個人や家庭に属する情報）を収集しているホームページがあり、そういった個人情報がさまざまな組織に売買されることも多いと言われています。こういった個人情報を買い取ったり、あるいは直接収集したりして、犯罪や押し売りに利用している組織も多いと言われています。

懸賞付きアンケートや無料サービス付きのアンケートに飛びつく人も多いようですが、アンケートに答えた内容が悪用されたり、プライバシーが侵害されたりする可能性があるということを考慮し、安易に個人情報を答えないように注意して下さい。その他いかなる場面においても、個人情報は極力外部に漏らさないように注意しましょう。

その他、インターネットの世界では、ねずみ講への勧誘、サギ行為、違法行為への勧誘、冒涜・名誉毀損行為など、さまざまな有害情報も流されています。また、出会い系サイトで知り合ったメール友達に騙されたり、犯罪に巻き込まれたりするといった事件も跡を絶ちません。

このようにインターネット上の情報は、マスコミなどの情報と違い（マスコミの情報も必ず信用できるわけではありませんが）、信頼性や安全性がまったく保証されていないということをよく認識しておきましょう。

最後に、特に児童保護の観点で述べておきますと、インターネット上には、わいせつ・中傷・暴力的話題など教育上好ましくないと考えられる情報もたくさん流れています。

これらへの対策としては、次のようにして Internet Explorer のフィルタリング機能（表示できるホームページを制限する機能）を利用することができます。

1. Internet Explorer のメニュー・バーから「ツール」→「インターネットオプション」と選択し、「コンテンツ」タブを選択します。
2. 「コンテンツアドバイザ」の「有効にする」ボタンをクリックし、「コンテンツアドバイザ」ウィンドウをよく読みながら、細かい設定を行います。（面倒な場合は、そのまま「OK」ボタンをクリックすれば最大の制限になります。）「OK」ボタンをクリックした後、「スーパバイザパスワードの設定」ウィンドウでパスワードを設定して「OK」ボタンをクリックします。以後、このパスワードを入力しない限り設定は変更できないようになります。

ただし、家庭でこういった設定を行ったところで、子供が他の場所へ行けば、好ましくない情報に触れる機会はいくらでもあると考えられます。こういった設定を行うことよりも、子供がこういった情報に触れても影響を受けないように、あるいは自主的にこういった情報を避けるように、何がどういう理由でどのように悪いのかをしっかりと子供に話しておくことの方が重要であるとも言われています。