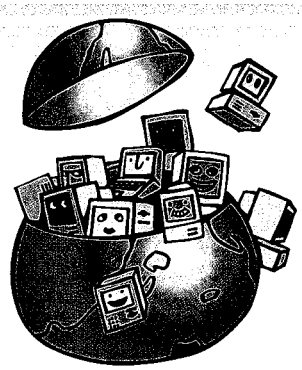


電脳博士Mr.HIROSEの ITこぼれ話

第9回

「セキュリティの疑問」

ITプランナー　廣瀬隆夫

オレオレ詐欺や紙幣の偽造など、悪質な犯罪が後を絶ちませんが、インターネットの世界でも、巧妙な詐欺や迷惑行為が増えています。インターネットの利用者は日本国内だけでも6千万人、世界では8億人を超えたと言われていますが、使っている人は必ずしも善意を持った人たちばかりではありません。しかも、インターネットには国境がなく検閲なしで何処からでも、攻撃される危険性があるのです。

インターネットに接続されたあなたのパソコンの中の個人情報を狙って、地球の裏側から悪意を持った人が覗いているかもしれないのです。

今回は、このようなインターネットの怖い部分でもあるセキュリティの疑問にお答えしていこうと思います。

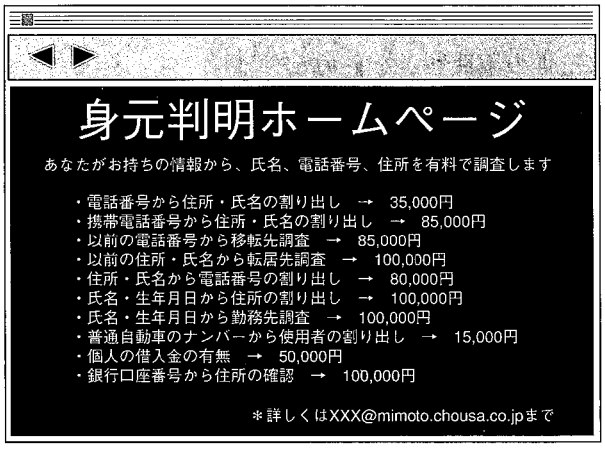
個人情報ってそんなに大事なものなの？

会社や自宅に、突然知らない会社からセールスの電話がかかってきて不愉快な経験をされた方も多いと思います。あなたの名前や電話番号という個人情報が何処かで漏れて、それが使われたのです。個人情報というのは、それを知ることで個人を特定できる、氏名、住所、年齢、性別、生年月日、電話番号、体重、血液型、病歴、資産などを指します。このような情報が知られてしまうと犯罪に巻き込まれたり、迷惑な押し売りに悩まされたりと大変な迷惑を被ることになります。昨年起こったインターネットプロバイダのYahoo！BBから450万人もの個人情報が流出した事件では、全ての会員に500円の商品券が配られましたが、それが原因で受けるかもしれない迷惑行為を考えると情報漏えいの対価としては少なすぎると思います。

個人情報が今になって、なぜ騒がれ始めたのかというと、インターネットの普及に要因があります。個人情報は今では殆どがパソコンで取り扱いが可能なデジタル情報で蓄積されています。一度インターネットに、個人情報が放たれてしまうと、コピーが容易で劣化しないというデジタルの特性で透明な水槽の中にインクをたらしたようにあっという間にインターネット全体に広まってしまいます。水槽を透明な状態に戻せないように個人情報の回収は難しく、流れた個人情報がどのような経路でどんな業者の手に渡っているかの追跡は事実上困難なのです。

インターネットの裏の世界では、個人情報を持ちだす密通者と探偵事務所、電話勧誘業者などの個人情報を必要とする業者の間に流通経路が確立されていると言われています。インターネットを検索すると「車のナンバーから個人の氏名や住所を調査します」というような身元調査サイトを見つけることが

図1　身元判明ホームページのイメージ



出来ます。ストーカーが、このようなサイトから身元を割り出して殺人事件にまでに発展したケースもあるのです。ID、パスワードの不正使用を禁じる「不正アクセス禁止法」や4月から施行される個人情報を守る目的の「個人情報保護法」という法律もありますが、個人の情報は命の次に大事な物として、自分がしっかり管理する必要があります。

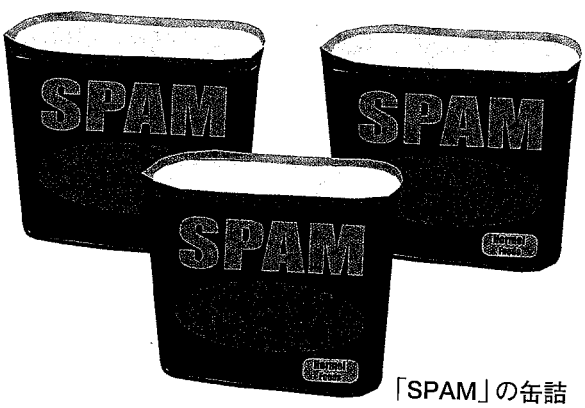
スパムメールって何？

インターネットを使っていると、知らない人からメールが来ることがあります。殆どが出会い系サイトへの勧誘や、何もしないでお金が儲かる話、無料でケーブルテレビが見れる装置や激安のソフトの売り込みなど、いかがわしい内容ばかりです。このように一方的に送りつけられてくるメールはスパムメールと呼ばれています。あなたの財布の中身を狙って、何処かでメールアドレスを入手して密かに送ってきたのです。インターネットの掲示板への書きこみ、アンケート調査への回答、無料ソフトのユーザ登録などでメールアドレスを記入した覚えはありませんか。

スパムメールの名前は、モンティ・パイソンというイギリスのコメディー番組の中で「SPAM、SPAM、SPAM・・・」と連呼するシーンが由来と言われています。ちなみに、この「SPAM」は美味しい豚肉の缶詰で、決して粗悪品ではありません。これらのメールの中には、詐欺行為のメールやウイルスメールも含まれており、クリックしたとたんに、「入会ありがとうございました」などと強制的に入会させられたり、不正請求のメールが届いたりする危険性がありますので注意が必要です。そのような不審なメールを受け取ったときは、返事を出さずに黙って消すのがもっとも賢い対処の仕方です。それでも、繰り返しメールが来るようでしたら、しかるべき団体に連絡することをおすすめします。

財団法人日本データ通信協会
迷惑メール相談センターのURL
http://www.dekyo.or.jp/soudan/top.htm

図2　SPAMの缶詰



「SPAM」の缶詰

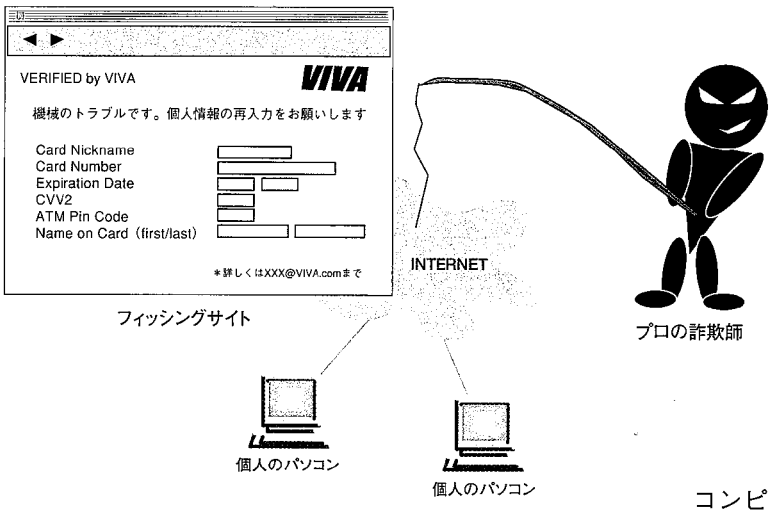
フィッシング詐欺って何？

最近は、テレビで盛んに取り上げられていますので、ご存知の方も多いかと思いますが、近年急増しているインターネットを使った詐欺行為です。本物そっくりの偽メールやサイトを使って、不特定多数のインターネットユーザから個人情報を盗み取るものです。米国では、何十億円に上る被害が出ているようで、日本でも昨年発生したVISAを偽るフィッシング詐欺や、Yahoo！にそっくりのフィッシングサイトがニュースで話題になりました。こうした一連の詐欺の手口はお年寄りを狙った「振り込め詐欺」のように、新たな手口が登場してくることが予想されますので注意が必要です。

フィッシングのスペルは、「Fishing」ではなく「Phishing」になっています。ユーザを釣りあげることから「Fishing」が語源であることは明らかですが、「Phishing」になった理由には2つの説があります。一つは、情報を撹乱するためにハッカーが自分たちだけで通用する単語を作ったという説。もう一つは、「洗練された」（sophisticated）の「ph」を取ったという説です。

その手口は、ユーザに偽りの情報を記載した電子メールを送りつけ、本物と非常に良く似た偽のフィッシング目的のWebサイトへ言葉巧みに誘導し、ユーザのIDやパスワードなどの個人情報を入力させて盗みだしてしまうものです。Webサイトは非常に巧妙に出来ており本物と区別がつきません。フィッシング詐欺には犯罪組織が関わっている場合が多く、彼

図3　フィッシング詐欺



らにIDやパスワードなどが渡ってしまうと、金融機関からあっという間に現金が引き出されてしまったり、ショッピングサイトで高価な物品を購入されたりと大変な被害を被ることになります。また、フィッシングサイトは国外に設置されることが多く、証拠隠滅のためにすぐに消されてしまうために取り締まることが非常に困難になっています。

個人がフィッシングにだまされないように気をつけるポイントは、心当たりのないメールや添付ファイルを不用意に開かないことです。また、Webサイトで個人情報を入力する時は、URLが正しいかどうか、SSL（セキュア・ソケット・レイヤー）暗号化通信中を示す閉じた鍵のマークがブラウザに表示されているかどうか、などは最低限確認していただきたいと思います。インターネットの世界では、IDとパスワードは預金通帳と印鑑に相当するものですので、厳重に管理する必要があります。経済産業省や総務省、警察庁なども本格的にフィッシング詐欺に関する対策を始めていますが、被害に会わないためには自分で騙されないように注意するしかありません。

コンピュータウイルスは本当に感染するの？

コンピュータウイルスは、勝手にパソコンの中に感染し潜伏期間を経て増殖し、最悪の場合はファイルやデータを破壊してパソコンを使えないようにしてしまいます。この行動パターンが人に感染するインフルエンザなどのウイルスと酷似しているためにウイルスと呼ばれています。その実態は電子メールの添付ファイルやホームページ閲覧などによって外部から送り込まれたコンピュータに侵入する悪意を持って作られたプログラムのことです。数年前まではフロッピーディスクを介しての感染もありましたが、最近はインターネット経由がほとんどです。

コンピュータウイルスの感染経路には以下のようなものがあります。

【電子メールの添付ファイルをクリック】

電子メールの添付ファイルとして送信されたウイルス入りのファイルを誤ってクリックすると、プログラムが実行されてウイルスに感染してしまいます。

【ウイルスに感染したホームページの閲覧】

Webブラウザで閲覧した時には、ホームページ上のコンテンツは自動的にダウンロードされて実行され、ウイルスが埋め込まれたホームページを見ただけで感染してしまいます。

【HTMLメールによる感染】

HTMLメールであればホームページによる感染と同様にメールをプレビューしただけでウイルスに感染してしまいます。強制的にウイルスメールを送りつけることができます。

【ネットワークのファイル共有】

ウイルスによっては、感染したパソコンに接続されているファイル共有用のネットワークドライブ経由で感染していくタイプのものがあります。

【マクロプログラムの実行による感染】

マイクロソフト社のOfficeアプリケーション（Word、Excel、PowerPoint、Access）のマクロ機能を利用して感染するタイプのウイルスです。感染したドキュメントを開いただけでファイルの書き換えや削除な

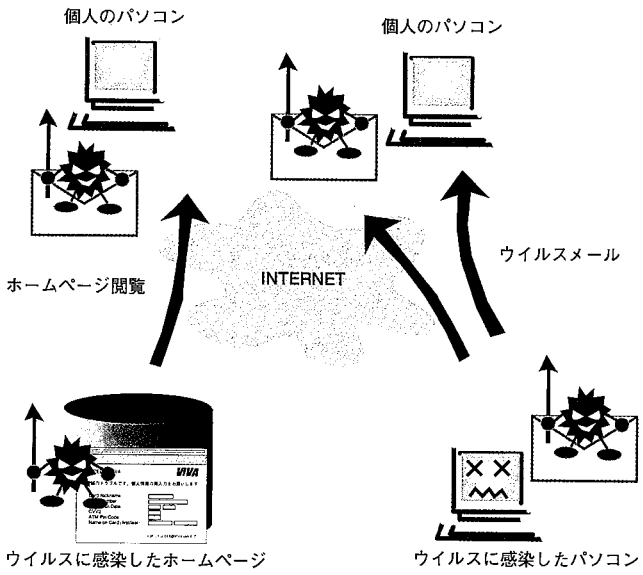
どが行われてしまいます。

それでは、実際に感染するとどんなことになるのかを代表的なウイルスであるNimda（ニムダ）を例にとってご紹介しましょう。Nimdaは、その感染方法が多彩であったことや手口が巧妙であったことで、2001年に大流行したウイルスです。世界中で200万台のパソコンが感染したと言われています。Nimdaという名前は、管理者を意味するAdminを逆から書いたもので管理者権限を奪い取るという怖い意味が込められているのだそうです。

このウイルスに感染すると、パソコンの受信トレイに保存されているメールアドレスを勝手に選んでウイルスメールを送りつけたり、共有ファイルへのウイルスのコピー、Webサーバーへの攻撃など、知らないうちに加害者にされてしまいます。送りつけられたウイルスメールは、セキュリティホールがあるOutlookを利用している場合には、電子メールをプレビューしただけでウイルスに感染してしまいます。次々に攻撃をしかけますのでネットワークは大混乱に陥ります。潜伏期間があり駆除されたと思っても、しばらくすると発症するという挙動も被害を長引かせています。

このようなウイルスに感染したくなかったら、パソコンにウイルス対策ソフトを導入しておく必要があります。インフルエンザの流行に備えてワクチン注射をしておくのと同じ事です。ウイルス対策ソフトはパソコンの電源がオンであるときには常に起動した状態になっており、外部から受け取るデータを常時監視することで、インターネットやフロッピーディスクなどからコンピュータがウイルスに感染することを防ぎます。また、送信する電子メールのウイルスもチェックしてくれます。パソコンがウイルスに感染してしまった場合には、コンピュータからウイルスを除去する治療の機能も持っています。ウイルスは常に新種が出来ますので、ウイルスの駆除方法が書かれたウイルス定義ファイルを最新のものに更新しておかないと効果がありません。最新のウイルス定義ファイルはインターネットやCD-ROMなどで配布されていますので常に最新のものにしておく必要があります。

図4　ウイルスの挙動



どんな人が悪さをしているの？

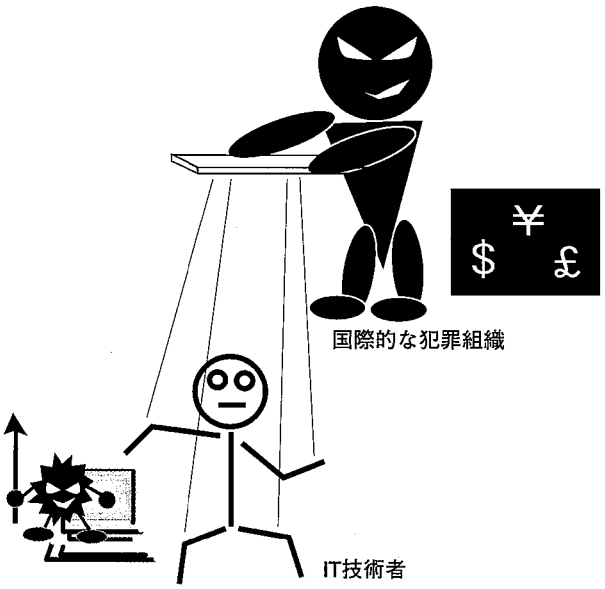
顔の見えないインターネットの世界でどんな人がウイルスを作ったりスパムメールを送りつけたりしているのでしょうか。インターネットが今のように広まる前には、コンピュータに興味を持ってる中高生が暇つぶしや自己顕示のために掲示板に面白半分にいたずらをする程度のものでした。今では、金銭目当ての詐欺行為が平然と行われており、IT業界から人材を投入したりして警察も捜査の手を広げています。

コンピュータ犯罪というとハッカーが夜中にこっそりやっているというイメージがありますが、それほど単純なものではありません。本来、ハッカーとはコンピュータやネットワークの高い技術を持った人々のことで犯罪者ではないという主張が根強くあります。アップルIIを開発したスティーブ・ウォズニアクやGNUプロジェクトのリチャード・ストールマン、Linuxの開発者であるライナス・トーバルスなどはハッカーと呼ばれています。ハッカーの中には「このプログラムにはバグがあり、このままではシステムが無防備で危険だ」ということを開発会社に知らせるためにプログラムを作る人もいます。それがウイルスとして蔓延して結果的に沢山の人に迷惑をか

けてしまうということもあります。そのような破壊活動をしている人たちはクラッカーと呼ばれています。このようなハッカーやクラッカーは技術には興味がありますが、お金儲けには興味がない人が多いのです。

本当に怖いのは、インターネットの匿名性を悪用して、金銭目的の詐欺行為をする人たちです。その中には国際的な犯罪組織が関わっていることもあります。ハッカーの開発したプログラムがサイバーテロリストやプロの詐欺師の手に渡り、悪用されるというケースもあります。また、フィッシング詐欺のようにハッカーと手を組んで計画的で大規模な詐欺行為が行われていることもあります。科学者が悪の手先に使われるというフィクションの世界が現実に行われているのです。電子メールやホームページというとゲーム感覚のお遊びの世界と思いがちですが、裏で怖い人たちが関わっている場合もあるということを心得ておいた方が良いでしょう。

図5　犯罪者とは



パスワードだけで大丈夫？

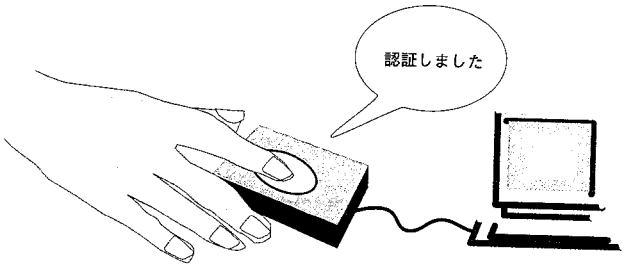
スキミングという手段で、キャッシュカードの情報を盗みだして偽造カードを複製し、類推したパスワードを使って預金を引き出してしまう事件が多発しています。類推されているパスワードは、生年月日や電話番号などの個人情報に含まれる数字が多いと言われています。財布の中には、カードや現金だけでなく、免許証や診察券なども入っており、そこに書かれた個人情報から類推されているのです。何千万円もの預金が入っている口座なのにパスワードが数字4桁ではあまりにも脆弱すぎます。しかも、パスワードの管理は個人に任されていて、難しいパスワードを設定してしまうと忘れてしまうし、覚えやすいものは簡単に類推されてしまうということで、この仕組み自体に根本的な脆弱性があります。

パスワードは時代劇で忍者が使っている、「山」「川」というのと原理的には同じで、知られてしまったら何の意味もありません。コンピュータの性能が何千倍にも上がりこんなに使いやすくなったのに一番大事な個人の認証の仕組みが大昔のコンピュータシステムのままというのはおかしいと思います。今後、サービスの電子化が進み、ショッピング、銀行取引、株式投資、税の申告、役所への各種届け出など、あらゆるサービスがインターネット経由で可能になりますが、今のパスワードの認証の仕方では不安がいっぱいです。そこで、様々な認証の仕組みが検討されています。その中で実用的でセキュリティ強度が高いと言われているのが本人の身体的特徴により個人を特定するバイオメトリクス認証という方式です。

バイオメトリクス認証の考え方は脳が人を認識するのと同じメカニズムを利用しており、その人物が「誰か」という身体的特徴に基づいて認証するものです。パスワードや暗証番号のように人が記憶できるものは忘れたり、盗まれたりする可能性があります。人が持ち歩く鍵やICカードは紛失、窃盗、あるいは偽造される恐れがあります。バイオメトリクスは人物が「誰か」ということ、つまり万人が持つ固有かつ不変の特徴に基づいているため、失ったり、忘れたり、盗まれたり、偽造されたりする心配がありません。バイオメトリクスはセキュリティの高さと利便性を合わせ持つ認証技術です。現在、実用化されているバイオメトリクス技術には指紋認証、顔認証、網膜パターン認証、虹彩パターン認証、掌形認証、静脈認証、声紋認証、筆跡認証などがあります。空港

のテロ対策や銀行のATMで使われ始めています。

図6　バイオメトリクス人認証



バイオメトリクス認証（指紋認証）

インターネットではどんなことに気をつけたら良いの？

インターネットを安全に利用するためには、あなた自身がインターネットの危険性をきちんと理解する必要があります。パソコンの画面だけを見ていると自分だけの世界だと錯覚しがちですが、インターネットは色々な人が行きかう公道と考えるべきです。鍵を掛けていなければ空き巣に入られますし、危険物が落ちているかもしれません。スリに会ったりや言葉巧みに押し売りされるかも知れません。また、自分が加害者にならないための注意も必要になります。今までご紹介したウイルスや迷惑メール、フィッシング以外に、気を付けたいポイントをご紹介します。

【インターネット接続時の注意】

インターネットに参加するとISP（インターネットサービスプロバイダ）からグローバルIPアドレスが与えられますが、これはインターネットに公開された住所のようなもので逆に外からハッキングされる可能性があります。その対策としてWindowsやアプリケーションソフトにはパッチと呼ばれる修正用プログラムを適用して、ソフトウエアを最新に保っておくことが大切です。また、外部からのアクセスに制限をかけるブロードバンドルータやファイアウォールソフトを導入すると、さらに安全性を高めることができます。

【掲示板やホームページへの書込時の注意】

いたずらのつもりでも、本人に断りなく、個人の氏名や住所、写真、私生活上の事実や秘密など、プライバシーに関わる情報を掲示板やブログ、ホームページなどで公開してしまうと、取り返しのつかない事態を引き起こすことがあります。あっと言う間に伝搬してしまう危険性があるからです。このような行為は、その人に精神的苦痛を与えるだけでなく、犯罪に悪用されたり、プライバシーや肖像権の侵害、名誉毀損等によって訴えられる可能性もありますので、掲示板やホームページへの書込は新聞の情報覧に載せるくらいの慎重さが必要です。

【チェーンメールの注意】

チェーンメールとは、手紙でも流行った「不幸の手紙」の電子メール版です。電子メールを受け取った人が次々に知人に電子メールを転送することで、ねずみ算式に広まっていく電子メールのことです。募金の呼びかけなどの善意の殻をかぶったものもあります。電子メールは転送が楽でコストが安いため、手紙と比べて広まる速度が速いことも、問題を大きくする一因となっています。チェーンメールが広まると、ネットワークに不要な負荷をかけるだけでなく、デマの情報が広まってしまう可能性があるため、メールを他の人に転送する際には、注意が必要です。

今さら聞けない？パソコンミニ用語集

SSL（Secure Sockets layer）	米国ネットスケープ社が提唱する、ネットワーク間でデータを転送する際のセキュリティ機能を付加する仕組みのこと。
プレビュー（preview）	事前に全体像を見ることや、その機能。ワープロ、フォトレタッチ（写真に後から手を加えて修正すること）、ドロー系（描画）等のソフトに備わっていることが多い。
マクロ機能	よく使われる手順を予め定義しておき、必要なときに呼び出して使う機能のこと。
GNU（GNU's Not Unix、グニュー）	リチャード・ストールマン氏などの「ソフトウェアは広く無償で提供すべきもの」という思想に基づくソフトウェア開発活動。
バグ（bug）	“虫”から“機械などの欠陥”の意に転じ、プログラムにおける誤りを指す。