「いざ」というとき役立つ基礎知識

「オークションで詐欺！」、「クレジットカードを不正利用！」。こういったニュースを目にするが、インターネットも現実世界と同じ。使い方を間違えたり注意を怠ったりしたら、犯罪に巻き込まれることだってある。でも現実にインターネットでセキュリティートラブルに遭ったらどうすればいいのだろう。そんな突然の悲劇を解決する方法がここにある！

喜多充成＋すずきひろのぶ＋吉川誠司

Illust:Hata Eiji

誰もが知りたかった！ セキュリティートラブル解決法

インターネットでの被害は こんな状況だ!

インターネット上でのセキュリティーの必要性については、ずいぶんとインターネットマガジンでも取り上げてきた。しかし、被害の実態まではなかなか把握できていなかった。そこで、本誌ではインターネットでセキュリティー上の被害を受けた300人に対して独自のアンケート調査を行った（結果は右グラフを参照）。

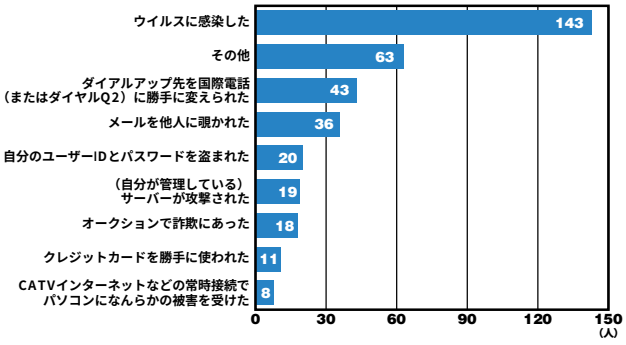
Q1では実際の被害状況について質問しているが、ウイルス感染が圧倒的に多いことがわかる。またアダルトサイトなどで見られる、国際電話などへのダイアルアップ先の変更も多い。やはり、無防備になりがちな状況でのトラブルが多くなる傾向のようだ。中には「掲示板に中傷のようなことを書かれた」（会社員・27歳）や「大量のメールを送られた」（パート・33歳）といった防ぎようのない被害も回答として多くみられた。

被害を受ける場面はやはり自宅（趣味などの利用）のほうが多いようだ（Q2）。企業では自宅とはまた違った傾向があるようだが、自宅の場合、システム管理者は当然いないので、すべての管理は個人に委ねられるのがその理由だろう。グラフにはないが、実際の被害金額も質問している。ほとんどは小額だが、中には10万円以上の被害を受けている人もいるようだ。

興味深いのは、やはり何らかの被害に遭ったあとにはおおむね対策を施しているところだろう（Q3）。また意外なのは、トラブルは結果的に解決され、かつそれを自分で行っているところだ（Q4、Q5）。「オークションで詐欺に会い、ホームページで被害者の情報を募って容疑者の居所をつかみ、最終的には弁済不可能で警察へ突き出す」（会社員・36歳）というツワモノもいる（この事件については実際にテレビニュースなどで放映されている）。

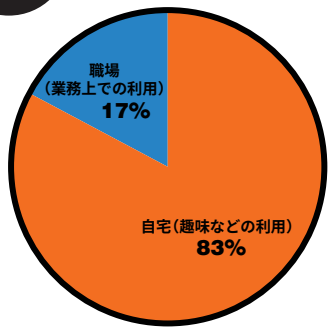
このように状況はさまざまだが、インターネット上のトラブルはとにかく後を絶たない。そこで「いざ」というときのセキュリティートラブル対処法を伝授しよう。

Q1.インターネットでどのような被害に遭いましたか？（複数回答可）

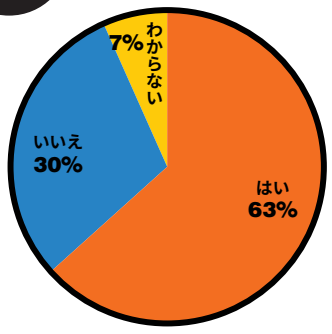


「その他」の項目では、同様に「オークションで取引のあった人から、用もないのに何度も電話がかかってきた」（専業主婦・32歳）のような金銭的な被害ではなく心理的な被害を受けるケースが多い。中には「登録しているサイトで個人情報が盗まれ、公開されてしまった」（主婦・64歳）といったトラブルに巻き込まれるような個人ではどうしようもない被害も。

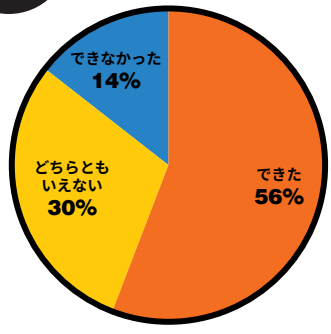
Q2.その被害にはどこで遭われましたか？



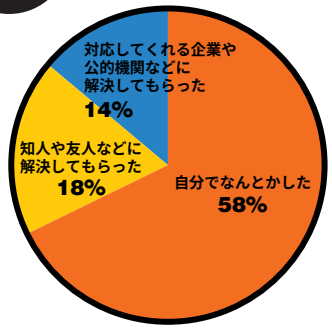
Q3.被害に遭ってから、何か対策をほどこしていますか？



Q5.その被害は解決できましたか？



Q6.どのようにして解決しましたか？（Q4で「解決できた」と答えた方に質問）



グラフにはないが、被害金額についてはほとんど小額で済んでいるようだ。ウイルスによってファイルが消去されてしまう場合は、金銭に換算できないという指摘もある。逆に企業では「400万円」の損害を被ったケースもあった。深刻な問題としては、クレジットカードの詐欺があるが、比較的小額の場合、本人すら気がついていないこともあるようだ。明細書の確認は常に心がけておきたい。状況はさまざまだが、詐欺などの場合、「警察の担当者自体がPCに対して詳しくなかったためどうにもならなかった」（自営業・27歳）といった泣くに泣けない状況も報告された。すべてを警察に頼るのも問題だが、社会全体がまだインターネットと完全に結びつかないがゆえの問題も存在している。

オークション：オークは競売を意味するが、実際のサイトはユーザー同士が売買を成立させる場となっている。ヤフーオークションやイーベイなどが代表的なサイトだが、匿名性を保てることから、詐欺などのトラブルが続出している。

どうする?

オークションサイトの相手にお金を盗られた!

■インターネット事件簿——❶

オークション詐欺は他人事ではない

大阪府在住のY氏は、あるオークションサイトで「人気のノートパソコン」が出品されているのを見て早速入札した。ところが入札が荒れ始めたので、Y氏は最高価格で入札した場合に15万円で購入するとの約束を事前に出品者にとりつける。最終的にY氏が最高価格で入札すると、翌日、出品者から「半金を先払いで郵便局の口座へ振り込んでください。入金確認後に即日発送します」というメールを受け取った。事前に交渉していたものの、多少の不安が残っていたY氏は、出品者の携帯電話に確認の電話をかけてみると、本人が出たので安心して代金を振り込む。ところが、その後一向にパソコンは送られて来ない。携帯電話に連絡を取ろうとしても留守番電話のままで、出品に使われたメールアドレスは解約されていた。伝えられていた住所と名前もデタラメだった。泣き寝入りするしかないのだろうか。

解決方法はコレだ!

- 同一人物にだまされた他の被害者がいないかどうか、掲示板などで呼びかける。
- 他の被害者情報と合わせて、最寄りの警察署に詐欺の被害届けを出す。

ここ最近多発しているネット詐欺の典型的な例だ。初めから詐欺目的の疑いが強いので、消費者が自力で相手を見つけだすことは困難だ。まずは警察に出向き、被害届けを出そう。捜査されるかどうかは別として、被害届けがないことには警察も動きようがないのだ。また、「だましとられた金額が少額だから警察が相手にしてくれないのでは?」と諦めてはダメ。1件1件は少額でも、こういったネット詐欺の被害者は複数いる場合が多いので、被害がまとまれば警察も動きやすい。もしかしたらすでに捜査が始まっているかもしれない。

詐欺事件の場合は派出所では対応していないので、居住区の警察署に行くこととなる。が、まだまだインターネットについてよくわかっていない警察官が多いので、いきなり専門用語を使わず、「詐欺に遭った」「だましとられた金額は○万円」「相手とは連絡が取れない」「インターネットで知り合った」という話し方をすると聞いてもらいやすいようだ。ただし、とりあえず話を聞いただけで調書を取られていない場合もあるので、相手の警察官の名刺くらいは必ずもらって帰るようにしたい。

被害者同士で横の連絡を取ることも大切だ。同じ人物が出品を継続しているようなら、掲示板に「商品が未着ですがどうなっていますか」と出すのも手だ。ほかに被害者がいれば情報を交換できるかもしれない。

また、国民生活センターや消費者センターなどでもネット詐欺の相談にのってくれる。詐欺かどうか確証の持てない場合は、最寄りのセンターを調べて相談してみよう。

1人1人の被害は小さくても、被害者が集まればさらなる被害の拡大と事件の再発を防げるはず。決して泣き寝入りしないでほしい。

これで万全! 対策ポイント

匿名性が高いネットでの個人売買にはトラブルがつきもの。詐欺に遭わないためには、利用者の管理がしっかりしている個人売買サイトを利用することがポイント。

利用に先立って身分証明書の提出などによるユーザー登録や、フリーメールによる登録を禁止しているサイトなら、かなり安心だ。

そして最も基本的なことだが、とにもかくにも「相手の身元確認を怠らない」ということ。相手がどんな理由を述べても、「氏名」「住所」「NTTの電話番号」の3つの確認だけは必ず取るようにしたい。そして、それが本当かどうか確認することも重要だ。

詐欺に遭ってから「デタラメだった」ではもう遅いのだ。実際にその住所宛てに郵便物を送って確かめるくらいの慎重さがほしい。

フリーメールや架空口座、プリペイド式携帯電話などの普及で、ますます匿名性が高まっているネット社会。不確かな相手にはお金を振り込まない、商品を送らない。これがネット詐欺から身を守るための最大の防御法だといえる。

フリーメール:メールアカウントを無償で取得できるサービス。ユーザー登録には、本人の個人情報を入力する場合がほとんどだが、厳密な調査は一切ないので匿名でメールアカウントが取得できる。匿名性を保てるという利点もあるが、裏を返せば犯罪にも使える。

どうする?

オンライン ショップから カード番号が流出?

■インターネット事件簿——❷

「番号だけ」のクレジットカードに注意

クレジットカードの請求書を受け取った東京都在住のF氏は、まったく身に覚えのない明細が請求書に記載されていることに気が付いた、しかも7件もである。調べてみるとクレジットカードの利用店舗は海外のアダルトサイトのようで、金額はそれぞれ6,000円前後、請求額は合計で約4万円にものぼる。

不正使用の疑いのあるそのクレジットカードは、F氏が数枚持つクレジットカードの中で、普段はまったく使用していないもので、もちろんアダルトサイトで使った覚えなどもない。だが、記憶をたどってみると、以前に一度だけインターネットを利用して、米国のオンラインショップでビタミン剤を購入したことを思い出す。「もしやその際に使ったクレジットカード番号が不正使用されたのでは」と再度そのサイトにアクセスしてみたが、すでにサイトは閉鎖されていた。クレジットカード会社に問い合わせようかとも思ったが、確証がないので困っている。

解決方法はコレだ!

- クレジットカード会社に連絡して「支払い異議申し立て」の手続きをとる。
- クレジットカード番号の使用停止と再発行を依頼する。

インターネット上でのクレジットカード決済は、本人を確認するシステムが確立されていないため悪用されやすい。クレジットカード番号と有効期限さえわかれば、誰でも本人になりすませるからだ。

F氏のケースは、ビタミン剤を購入したとき以外にクレジットカードを使っていないのなら、その際に送信したカード情報が何らかの形で流出して悪用された可能性がある。あるいは、クレジットカードナンバー生成ソフトなどによって作られたクレジットカード番号が、たまたまF氏のものと一致したか。可能性は2つに1つ。

いずれにせよ、身に覚えのないクレジットカード請求を受けたなら、まずは早急にクレジットカード会社に連絡して事情を話すこと。アダルトサイトの会費は通信販売と異なり購入者の特定が困難なため、クレジットカード会社も対応が鈍く、「ご本人で解約して下さい」と逃げ腰になるが、入会してもいないサイトの解約をする必要など一切ない。仮にクレジットカード会社が調査するとしても回答が出るまで3か月程度はかかり、その間も引き落としはされるが、最終的にF氏が利用したという事実確認が取れない限り代金は返金されることになる。同時に、本人確認をせずに決済を行ったクレジットカード加盟店側にはクレジットカード会社から「チャージバック」というペナルティーが課せられることになる。

不正に使われたクレジットカードについては、そのクレジットカード会社を継続するならば必ず番号を変えてもらうこと。あるいはこれを機会に、不要なクレジットカードを整理してしまうのもいいだろう。不必要に多数のクレジットカードを持っていると請求書のチェックがおろそかになり、不正請求に気が付かないこともあるからだ。

これで万全! 対策ポイント

クレジットカード番号を絶対に悪用されないための最終自衛策は「クレジットカードを持たないこと」。しかしそうもいかないのが現実なので、とりあえずは使うことのない余分なクレジットカードは持たないように心掛けたい。クレジットカードの数だけ、不正使用の危険があるからだ。また、クレジットカード番号の管理もしっかり行うこと。利用明細などからクレジットカード番号と有効期限が流出する可能性もある。

そして、インターネット上で使うクレジットカードは、普段使うものと分けておいたほうがいい。そうすることで、自信を持って「自分が使った代金でない」ことを主張できるからだ。また、クレジットカード番号を送信する際に暗号化して送るSSLは安全であるかのようにうたわれているが、受け取った相手が悪用したら意味がない。ファックスで送るのも誰の目に留まるかわからないので避けた方が賢明だ。店舗に本当に信頼があるかどうかは必ず事前に確認しておきたい。もちろん、日頃から自分でクレジットカードの利用状況などを記録しておく習慣を身につけておくことが、いざという時にもっとも効果的だろう。

SSL（エス・エス・エル／Secure Socket Layer）：ブラウザーとサーバー間で安全にデータをやり取りするためのプロトコル。米ネットスケープ社が開発し、マイクロソフトなどが採用している。認証と暗号の機能を持ち、ブラウザーとサーバーの間でお互いを確認したり、やり取りするデータを暗号化したりする機能を持つ。

どうする？ 覚えのない多額の国際電話料金を請求された！

■インターネット事件簿——❸

男性諸君！ アダルトサイトにご用心

インターネット歴半年のK氏はある日を境にプロバイダーへの接続が不調になる状況が続いていた。数日後、K氏のもとにKDDから請求書が送られてくる。海外に電話をかけた覚えはK氏にはなかったが、請求書を見てK氏は驚く。なんと金額は40万円。しかも電話をかけた先は東欧の“モルドバ”。明らかに間違いだと思ったK氏はKDDに問い合わせるが確かに利用しているという。よもやと思い不調だったパソコンを調べると、「ダイヤルアップネットワーク」のフォルダーに見覚えのないアイコンが……。ダイヤル先はモルドバの電話番号になっていた。いつもどおりのプロバイダーへダイヤルアップしていたつもりが、モルドバのプロバイダーへつながっていたようだ。一体なぜ？

解決方法はコレだ！

- 今後同様の被害に遭わないため、KDDに「発信停止」の依頼をする。
- 不要なダイヤルアップアイコンを削除する。

これは昨年4月より急増している悪質な国際電話接続プログラムによる被害だ。アダルトサイトを見ていると、いつしか訳の分からないプログラムをダウンロードさせられて、「モルドバ」や「セイシェル」、「ガイアナ」といった国へ強制的にダイヤルアップ接続させられるケースである。

利用者が支払う国際電話料金は、発信国と受信国の国際電話会社で分配され、受信国（この場合はモルドバ）でプロバイダーやアダルト番組の運営業者に数十パーセントのマージンが支払われるようになっている。つまり電話料金が高いほど各社のフトコロは潤うわけで、産業収入が低い国に限り、こういったケースが集中している。

とりあえずKDDには事情を話し、不当な方法による請求であることを伝えよう。しかし国内のダイヤルQ2と違って情報料ではなく通話料なので、支払い拒否はまず無理。泣き寝入りするしかない。

こうした場合、ダイヤルアップネットワークの設定を確認して、接続先が001で始まる国際電話番号になっていたら早急に設定を削除しよう。同様に0990で始まる番号ならダイヤルQ2だ。ダイヤルQ2の不当な情報料の請求が来た場合、NTTには支払いを拒否できる。NTTは業者に代わって情報料の回収を代行しているにすぎないからだ。ただしその場合、後日、業者から直接取り立てがあるが、納得がいかない不当な請求には断固支払いを拒否していい。

「ダイヤルアップネットワーク」に見覚えのないアイコンがあったら要注意

これで万全！ 対策ポイント

一度、痛い目に遭ってもやっぱりアダルトサイトは見に行きたい！　というならば、この際、自宅の電話からはダイヤルQ2と国際電話はかけられないように電話会社へ申請しておくことをおすすめする。これなら絶対に不当な請求が来ることはありえない。

事情があって国際電話は止められない場合は、接続先が国際電話やダイヤルQ2の場合に警告してくれる、エムソフトの「No!国際電話」Jumpをインストールしよう。

ただ、アダルトサイトの業者はいずれも強者揃い。技術的な仕掛けにも、消費者の心理分析にも長けているので、一度悪質な業者に捕まると思いがけない損害を被ることがある。

基本的にはアダルトサイトの「無料」という言葉はあてにならない。無料サイトで運営するからには「バナー広告」の広告料で収益を上げているか、国際電話接続やダイヤルQ2のプログラムをダウンロードさせるなどの仕掛けがあるはずということを心に留めておきたい。

Jump www.nifty.ne.jp/forum/femsoft/

モルドバ：東欧のウクライナとルーマニアの間に位置する共和国。1991年にロシア連邦より独立。

どうする?

もしかしたら電子メールが盗み読まれている?

■インターネット事件簿——❹

メール盗聴による悪質なストーキングの恐怖

都内に住む20代半ばの女性N氏のもとに、1か月ほど前から匿名の差出人からメールが頻繁に届くようになった。最初はどこかで自分のメールアドレスを知った見知らぬ誰かがいやがらせのメールを送っているのだと思い、N氏は気にも留めなかった。ところが、よくよくメールを読んでみると、なぜか親友とメールでしか交わしたことのない内容を、匿名メールの差出人は知っているようなのだ。それは、N氏が親友へ書いたメールについての批判や意見が書かれた形となっているという。不信に思ったN氏だが、彼女は独り暮らしで自宅でしかメールのやりとりをしないため、パソコンに保存されたメッセージを他人に盗み見られるという可能性は考えられない。もちろんメールの内容を他人に話した覚えもない。どうやらメールが盗聴されているとしか思えない。N氏は気味悪がってメールを誰にも送れないでいる。

解決方法はコレだ!

- メールアカウントのパスワードを変更する。
- トロイの木馬が仕掛けられていないかウイルスチェックを行う。

このような相談の場合、概して本人の思い過ごしが多い。実際に調べてみても盗聴されている形跡が見あたらないことがほとんど。しかし、メール盗聴は現実的に可能だ。

メールの盗聴手段として最も簡単なのは、サーバー管理者による盗聴。ただし、普通のプロバイダーであれば、1日に何万通もあるユーザーのメールをいちいち見るような環境ではないし、法律的にも電気通信事業法により「通信の検閲」は禁じられている。しかし電気通信事業者ではない一般の企業には、この法律は適用されない。したがって、通常の職務として有責者による検閲が許されている企業も多い。過去にシステム管理者がストーカーであった例もある。社内メールの私用は要注意だ。

身近な人間にパスワードが盗まれる場合もある。パスワードをパソコンにファイルとして記録していたり、メモで貼ってあったりしていれば、簡単にパスワードは盗まれる。また、知識のある人間ならば、社内ネットワークを盗聴してパスワードを盗むこともできなくもない。「トロイの木馬」と呼ばれるマシン遠隔操作プログラムによるハッキングも考えられる。これがインストールされるとメールの盗聴どころか、マシンを乗っ取られる。

最後にネットサーフィンをしている間に、見知らぬ第三者にメールアドレスとパスワードを抜き取られるケースも紹介しておく。ActiveXを悪用したハッキングであるが、インターネットエクスプローラを使っていて、セキュリティーレベルを「低」にしていて、メール設定で「パスワードを保存」にチェックをつけている場合に起こりうるのだ。以上のことはぜひ気を付けておいてほしい。

これで万全! 対策ポイント

メールを盗聴されるということは、プライバシーの流出でもある。くれぐれもパスワードの保管には十分気を付けたい。打ち込むのが面倒だからといって、メールソフトに保存したり、忘れっぽいから手帳にメモしたりしないことだ。これは社内などの共有スペースでは盗んで下さいと言わんばかりの行為だ。

また、メールソフトのパスワードだけに気を取られていると、席を外している隙にキーボードで打ち込んだ内容を記録するキーストロークレコーダーを仕込まれることだってある。さらにウェブメールに関しては、メールアドレスを知っている人間なら誰でも「ログオン」できる可能性があるので、クラッキングの的になりやすい。

他人に容易に推測される可能性のある名前や生年月日などはパスワードに使わないことも大切。トロイの木馬はウイルスの一種なので市販のウイルス対策ソフトで容易に発見・駆除できる。Activexによるクラッキングにはブラウザーの初期設定でActiveXをオフにしておくだけで対処できる。

トロイの木馬：ホメロスの叙事詩「イリアス」で知られるトロイの木馬になぞらえたクラックプログラム。一見、普通のプログラムに見えるが、コンピュータにインストールされると、そのコンピュータ内の情報を外部に送信したり、最悪の場合はコンピュータ自身を外部から操作できるようにしたりする。

どうする？

ウイルスに感染してメールをバラまいてしまった！

■インターネット事件簿――❺

ウイルスは他人にも大迷惑

K氏は自宅ではマッキントッシュ、仕事場ではウィンドウズとマッキントッシュを利用する、キャリア10年以上のパソコンユーザー。ウィンドウズは仕事上の必要から1年ほど前から使い始めた。
ある夜、古い友人から添付ファイル付きのメールを自宅のマッキントッシュで受け取った。だが拡張子が「.exe」の実行ファイルだったため中味を確認できず、翌朝、仕事場のウィンドウズマシンでそれを開いて感染した。
ウイルスを受け取った人からの電話で感染を知らされ一瞬戸惑ったK氏だったが、まる1日かけてなんとか復旧できた。しかし、不用意に実行ファイルを開いてしまったという事実はアドレスブックの約300人に周知徹底され、ウイルス感染者の「烙印」も消えることはない。

解決方法はコレだ！

- まず、ネットワークから切り離す（とくにワームの場合）。
- 二次被害を小さくするためウイルス送付先へ「緊急連絡」
- じゅうぶんな情報を集めた後、落ち着いて駆除作業を行う。

K氏がまずとった対策は、すぐにウィンドウズをLANから切り離すこと。次にマッキントッシュで復旧のための情報・ツールの収集や、ウイルス送付先の人々に対する情報提供を行い、二次災害は最小限で済んだ。

ただK氏の感染したPrettyParkが破壊的なウイルスでなかったのは単なる幸運にすぎなかった。ラブレターウイルスのように新しい、しかもファイルを壊すタイプのウイルスだったとしたら、ダブルクリックした時点で「アウト！」だったはずだ。「親しい人からのものであっても、怪しい添付ファイルは開かない」と肝に銘じておくしかないわけだが、しかしたとえば、自分が密かに想いを寄せる相手から「Subject:I Love You」が届いたとき、開かずに捨てられる人はどれほどいるだろうか。

K氏は感染後何人かの友人から「アウトルックエクスプレスはやめたほうがいいよ」とアドバイスも受けた。最もシェアの高いメールソフトは当然ながら標的にされやすい。これをやめるか、やめなくともアドレスブックをメールソフトに頼らないというのは、当座の防御策・二次感染防止策としては有効であろう。

またK氏は、マッキントッシュが使える状況にあったからこそなんとか1日で騒ぎを収めることができたのであって、これがもしパソコン1台しかない環境だったとしたら、情報収集の手足をもがれ、バラまいてしまった先に警報を送ることもできず、事態はもっと深刻なものになっていたに違いない。そんな経緯もあって、ファイルのバックアップ同様、「仕事環境のバックアップ」も用意しておくべきだと認識を新たにしたそうだ。つまり、複数のOS、複数のマシン、複数のメーラーでの運用を面倒がらずにやることにしたのである。

これで万全！対策ポイント

もちろんウイルスの予防にはアンチウイルスソフトが有効だ。少なくとも既知のウイルスに対しては、ワクチンソフトを導入して定義ファイルのアップデートを怠らない限りまず心配はないと思っていい。

しかしコンピュータを使っていく限り、未知のウイルスに対しての「万全の備え」は、実は存在し得ない。だがたとえ感染してファイルを破壊されたとしても（そこは諦めるしかない）、最後の線を守り通す心構えだけはしておきたい。まず「人に迷惑はかけない」こと。感染が発覚したら即ネットから切り離す。その時点ではもう遅いかもしれないが、やらないよりはマシである。次が「ネット接続を維持し、情報を収集する」こと。これが前述した「仕事環境のバックアップ」を意味する。同じ場所に2台は難しくても、仕事場と自宅の両方でPCを使っている人は多いと思う。小渕サンが突然倒れて臨時代理～後継選びがもたついたが、ああならないよう自宅と仕事場のPCの相互のファイルの共有・シンクロ方法やメールアカウントなどの設定を「どちらかがアウトになったら」という視点で見直すことをおすすめしておく。

LAN（ラン／Local Area Network）：コンピュータ同士を直接接続した小さなネットワークのこと。「社内LAN」などと表現する。電話回線や専用線などで接続するネットワークはWAN（ワン／Wide Area Network）という。

セキュリティー対策の最前線に見る

ウイルスという新たな「災害」への備え

喜多 充成

被害は突然やってくる

ある企業のネットワークセキュリティ担当者がこんなことを言っていた。「ここしばらく“妙に静か”なんです。大物が見あたらなくて。それがかえってブキミなんですけどね」

この話を聞いたのは5月2日、ちょうど「ラブレターウイルス」が世界を騒がせはじめる2日前のことだった。身を削って神経を尖らせているプロならではのアンテナが、ウイルス作者の出す妖気を感じ取っていたのだろうか――。

まあ、これはたまたまタイミングが合ったに過ぎないとしても、企業のネットワークインフラを預かるセキュリティ対策担当者の心構えはそこに集約されている。つまり「いつ来てもいいように備える」ということである。

災害対策と同様の備えを

現在、企業がもっと怖れるのはウイルス感染が信用問題に波及する事態だ。本誌の発行元インプレスでは、ある重役のウイルス感染をきっかけに、それまで個人個人に任されていたウイルス対策を、組織化して行うことにした。編集部・部署単位に担当者を置き、ウイルス定義ファイルのアップデートを定期的に実行・報告するいわば「ウイルス自警団」だ。個人としてやるべきことを組織として後押ししているわけで、まずまずの成果を上げていると言う。

一方、組織でなければできない対策というのもある。日本ユニシスでは、1995年から組織縦断のウイルス対策推進プロジェクトを設置。社員の自宅での使用はもちろん、退職者から関連会社まで使用許諾の範囲を広げたワクチンソフトのライセンスを購入し（というか、ベンダーに認めさせ）、同一のウイルス定義ファイルを利用できるようにしているという。さらに、ワクチン会社と密に連絡を取り合いながら、同時に実物のウイルスで、各社のワクチンソフトの評価を行って「通知簿」を作成しているというから徹底している。が、そこまでやっても「自宅のパソコンで感染してしまう懸念」は拭い切れない。社内外をつなぐトラフィックはすべて1か所で監視するため、社員の自宅からのアクセスでもすべてコールバック形式で会社のインターネットゲートウェイを経由する形を徹底させている。社内ネットワークとインターネットのすべての出入り口を監視するために、その「すべて」を「1か所」にしてしまい、そこをしっかり監視する方法が、最も効果の高い方法なのだ。

インフラそのものを堅牢に

「ウイルスバスター」で知られるトレンドマイクロは、この分野で「インタースキャンウイルスウォール」が圧倒的なシェアと、ウイルス捕捉数を誇っている。「ネットワークというインフラストラクチャーのセキュリティーを向上させるという、企業理念を体現した製品で、費用対効果の高さが認められ、導入企業が増えています」（同社営業担当）

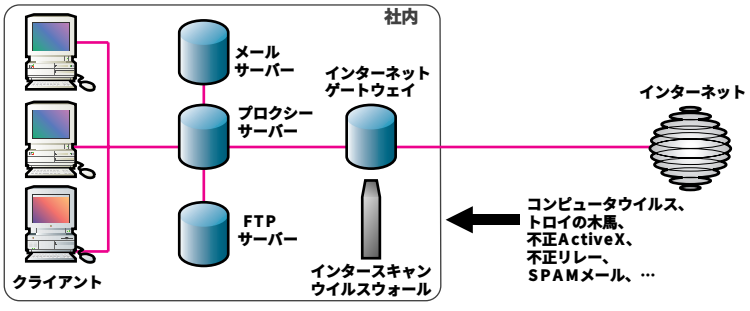
eDoctorのような、新種のウイルスに対抗する「地球防衛軍」的な組織が作った新鮮な「ウイルス定義ファイル」と、トラフィックを1か所に絞ってウイルスを見つけだす仕組み。この両輪でウイルスを捕まえるのは、管理コストや運用の手間まで含めて考えても、有効かつ実効ある手段になっているわけだ。ネット上では1日に5～6種の新種や亜種が発見されているというから、ウイルスの襲来は防ぎようがない。が、それで業務が止まったり、バラまいてしまったりという事態は避けなければいけない。

実は前ページの「K氏」とは筆者自身のこと。実体験からウイルス対策の結論を「仕事環境のバックアップ」としたが、今回取材してみて、その思いを強くした。不正侵入されたりスパムの踏み台にされたり、あるいは火災や地震、暴漢などによる物理的損壊まで想定した「セキュリティー」の備えの中に含まれているのである。

「ウイルスに対する備えは、24時間365日、休むわけにはいきません」と語る、トレンドマイクロの「eDoctorジャパン」の中山氏。

インタースキャンウイルスウォールのしくみ

インタースキャンウイルスウォールは、トラフィックをゲートウェイで監視することにより、ウイルスなどの侵入を一括して防ぐ。



ゲートウェイ：ネットワークとネットワークの間を制御するための中間ポイント、またはその制御を実行するサーバーのこと。ルーターに比べて高いレベルのアプリケーション層を制御するものを指すことが多い。

どうする?

CATVで接続したらパソコンがまる見え?

■インターネット事件簿——⑥

常時接続ではファイル共有に要注意

都内に住む会社員N氏は、居住地域のCATV会社がインターネット接続サービスを始めたのを機に、それまでのダイアルアップ接続からCATVインターネットに変更した。料金はダイアルアップ接続より幾分高額になるが、高速通信と常時接続ができるのが変更の理由だった。CATVインターネットに切り替えた当初は、接続環境の改善にすこぶる気をよくしていたが、あるときウィンドウズの「ネットワークコンピュータ」を開いてみると、見知らぬコンピュータの名前がずらずらと出てくるのに気が付いた。どうやらCATVインターネットに接続しているユーザーのコンピュータらしいことが判明したが、自分のコンピュータのフォルダーも他人から見えていたのかと思うと気味が悪い。この原因は新たなインターネット接続方法であるCATVのような常時接続型に多く見られるものだが、はたして対処するにはどうすればいいのだろう。

解決方法はコレだ!

- IPルーターを使って、家庭内LANと外部とを遮断する。
- フィルタリングソフトを使って、外部からのアクセスを防ぐ。

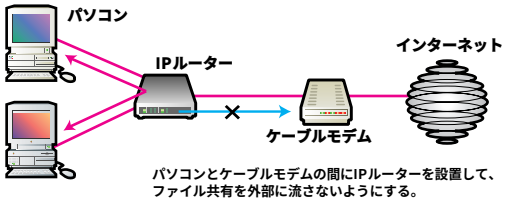
ファイル共有が見えてしまうというのはCATVだけの問題ではない。最近見かけるインターネット接続を提供しているインターネットマンションなどでも同様に起こっている。この原因はCATV会社のネットワーク、あるいはマンション内のネットワークが1つの大きなLANのような形になっているためだ。このため、家庭内LANでファイルを共有しているつもりでも、実はCATV全体でファイルが共有されてしまうといったことになる。

もっとも簡単な解決策はファイル共有をしないことだが、それでは家庭内LANを組んだ意味がない。ファイル共有にパスワードを設定する方法も考えられるが、これでは万全とは言えない。もちろん、何も設定しないよりはいいが、あいかわらず他人のネットワークコンピュータには見えてしまう。また、セキュリティーという点では、ウィンドウズのファイル共有だけが問題なのではない。どのようなOSでも、無防備に直接外部へ接続されていることによる脅威は同じである。

CATVでもこうした問題を防ぐために、ダイアルアップルーターのようなIPアドレスを変換するIPマスカレードやフィルタリングの機能を持つ機器の導入が必要になる。IPルーターと呼ばれる製品がそれで、簡単な設定でセキュリティーが確保できる。

FutureNet CR-20
メーカー:センチュリー・システムズ(株)
標準価格:54,800円(通販価格)
Jump www.centurysys.co.jp

IPルーターのしくみ



パソコンとケーブルモデムの間にIPルーターを設置して、ファイル共有を外部に流さないようにする。

これで万全! 対策ポイント

IPルーターの多くは接続するとすぐに使えるようになっているし、基本的なフィルタリングの設定も行われている。さらにセキュリティーを高めるためには外部からのアクセスを一律に禁止してしまうのが確実で安全だが、副作用として一部のプッシュ型情報送信アプリケーションが動作しなくなってしまう場合がある。

もし、あなたがパワーユーザーなら、古いパソコンにLinuxをインストールしてPCルーターにする方法もあるが、これにはかなりの知識が必要となる。そこで、より簡単な方法としておすすめなのが、ウィンドウズマシンにセキュリティー対策ソフトウェアをインストールすることだ。東陽テクニカの「BlackICE Defender」は、通信を監視して不正アクセスを防御するソフトウェアで、攻撃内容や侵入者の記録を保存する機能も持っている。ホームページから体験版もダウンロードできるので、常時接続の場合にはどのような攻撃を外部から受けるのかを一度見てみることをおすすめする。

Jump www.toyo.co.jp/security/

ダイアルアップルーター:一般にISDN回線でダイアルアップするために用いられるルーターのこと。ルーターはネットワークの制御を行う。パケットのフィルタリングなどのソフトウェア機能を持つものがほとんどで、ハブ機能やアナログポートといったハードウェアも備える。

どうする?
内部からの不正アクセスを防ぐには?

■インターネット事件簿――❼

不正アクセスは外部からとは限らない

専門商社のI社のシステムのセキュリティー対策は万全だった。外部からの侵入はファイアーウォールで防ぎ、ウェブやメールなどのサーバーについては、常に最新のシステムにアップデートしていた。だがある日、I社の取締役クラスしか知りえない情報が社外に漏れてしまった。しかも、あるウェブページに掲載されるというかたちでだ。公開方法がウェブページであったことから、外部の悪意を持った者が、インターネットから内部システムに侵入したのではという疑いがもたれたが、調査の結果そんな形跡は微塵もなかった。ところが、調査を進めていくうちに機密情報が保管されていたサーバーに内部ネットワークのあるコンピュータから不正に侵入を試みようとしていたことが判明した。どうやらこれが原因らしい。いわゆる内部犯行だ。社員からの不正な攻撃を防ぐ手立てはあったのだろうか?

解決方法はコレだ!

- スイッチングハブを導入して、ネットワーク盗聴を防ぐ。
- 重要なデータのやりとりにはIPSecなどの暗号技術を使う。

通常、セキュリティー対策というと外部からの不正アクセスをいかにして防ぐかという点に注意が払われる。もちろん、ウェブサーバーのように外部に公開しているサーバーは常にクラッキングの危険にさらされることになるし、ひとたびクラッキングされてしまうと企業としての信用にもかかわる問題になりかねない。したがって、どうしても外部からのクラッキングに目が行きがちだが、情報セキュリティーという観点からいけば最も脅威となるのが内部犯行なのだ。多段階で防御するファイアーウォールを構築していれば、たとえウェブサーバーに侵入できたとしても、その先にある内部ネットワークまではそう簡単に侵入できるものではない。その一方で、多くのネットワークは外部からの攻撃には対策を立てているが、内部からの攻撃については想定すらしていないことが多い。

何も対策を立てていないネットワークでは、ネットワーク盗聴ツールを使えばLANを流れるデータをいとも簡単に見ることができる。ネットワーク盗聴ツールといっても特殊なものではなく、ネットワークのトラフィックを監視するプログラムに少し改良を加えればできてしまうレベルだ。メールの内容やパスワードなども簡単に調べられ、しかもこうしたツールを使っていたという痕跡も残らない。

内部で流れるネットワークデータを守るのは非常に大変である。ネットワークを構築する時点から組み入れていかなければ効果的な防御はできない。さらに個別の対策も難しい。きちんとネットワーク全体のセキュリティポリシーを立てて、企画、導入、運用の段階にわたって対策を施し、正しく行われているかの監査を行う必要がある。

これで万全! 対策ポイント

内部からのネットワーク盗聴を防ぐには、LANのネットワークハブ装置をスイッチングハブにするのが効果的だ。通常のハブの場合、データは無関係なマシンにも流れてしまい、これがネットワーク盗聴ツールに狙われてしまう。スイッチングハブは、データを関係のないマシンには流さないことによってネットワークの効率を上げるための装置だが、こうした仕組みのために無関係なマシンからの盗聴もできなくなる。

しかし完全に安全にするには、やはり暗号技術を導入するほうがいい。UNIX系ではアプリケーションレベルの通信を暗号化するSSH、SOCKS、TSLといった方法が利用されている。TCP/IPプロトコルにはIPSecという通信パケットを暗号化する技術があり、徐々にいろいろなシステムで利用できるようになってきており、ウィンドウズ2000でもIPSecは標準で用意されている。こうしたプロトコルレベルでの暗号化を使えば、たとえ途中で盗聴に成功したとしても、解読はほとんど不可能だ。

IPsec(アイ・ピー・セック/Internet Protocol Security):IETFで標準化された、IPパケットを暗号化して送受信する方法。VPNを構築する際などに利用される。

どうする?

サーバーに外部から侵入された！

■インターネット事件簿——❽

ファイアーウォールも万能ではない

「人事院近畿事務局（大阪市中央区）のインターネットのホームページ（HP）にハッカーが侵入、HPのファイルの大部分が消去されていることが分かり、同事務局が28日夜明らかにした。同事務局によると、HP用のサーバーは不正アクセスを防ぐファイアウオールを設けていたが、破られたという。またこのサーバーへの不正アクセスは1万数千回に上っているという」（インターネットウォッチ2000年1月31日号・時事通信社発信の記事より）。今年1月末から2月頭にかけて、省庁関連のウェブサイトのウェブページ書き換えなどが相次いだ。一連の事件ではセキュリティー対策が考慮されていなかったのが原因だが、この人事院のようにファイアーウォールを設けていたところも遭っている。この被害を食い止める方法はあったのだろうか？

解決方法はコレだ！

- サーバープログラムは常に最新のものを使用する。
- セキュリティー情報に関するページを定期的にチェックする。

一連のクラッキング事件によって一躍有名になってしまった「ファイアーウォール」。このファイアーウォールとは外部からの侵入を防ぐためのシステムを指すのだが、別に特別な機材やソフトウェアを用意する必要はなく既存のシステムの設定を上手に利用するだけでファイアーウォールが構築できる。たとえば、基本的で最もシンプルなファイアーウォールは許可された通信のみを通すIPフィルタリングだが、この機能はダイアルアップルーターでも設定できる。

「公開ウェブサーバーに対してウェブページ要求を出す」というのは正しい通信なのでファイアーウォールを通過していく。たとえおかしなデータが届いたとしても、ウェブサーバーがエラーを返すからだ。

ところが、今回の省庁アタックで狙われた特定のウェブサーバーには古いバグがあり、これを狙われた。マスコミ報道で有名になったバッファーオーバーフローがそうだ。一見、通常のウェブページの要求のように見えるデータのためファイアーウォールは通過してしまうが、ウェブサーバーがそのデータを受け取ると任意のコマンドが実行できてしまうというもの。これは非常に危険なバグで、この手法を使えばそのままリモートログインすらできてしまう。これを防ぐにはウェブサーバーのソフトウェアをバグのないバージョンにアップデートする必要がある。もし、このバグを放置し、安易にファイアーウォール内にウェブサーバーを移動させると、本来防御している内側にまで侵入を許すポイントを作ってしまうことに注意しよう。

これで万全！対策ポイント

まず、管理者はウェブサイトで利用しているサーバープログラムの種類とバージョンが何であるかを把握するという、基本中の基本から始める必要がある。ずいぶん前にインストールしただけで、それ以来一度もメインテナンスしていないというようなサイトもまだまだ存在するからだ。

次に、ベンダーが用意しているサーバープログラムのメインテナンスに関するサービスサイトを定期的にチェックして、常に最新版のサーバープログラムを使うように心がけよう。さらに、JPCERT/CCやCERT/CCのウェブページを定期的にチェックすることも忘れずに。こうしたページでは、最新のセキュリティーホール情報が確認でき、ベンダーが公式にサポートする前でも、対応策を入手できる場合が多い。また、JPCERT/CCでは各種アナウンスをメールで送ってくれるサービスも用意されているので活用してみよう。

Jump www.jpcert.or.jp　Jump www.cert.org

リモートログイン：遠隔からコンピュータにログインすること。

本人確認と匿名性を両立

「ゼロ知識証明」の可能性

すずきひろのぶ

ゼロ知識証明による認証

インターネット上での匿名というと、オークション詐欺などを例に挙げて「匿名は危険だ」という短絡的な答えに結び付く。実は、この問題の本質は匿名であるかどうかではない。現実世界でもそうだが、誰であるかに関係なく支払い能力があるかどうかが問題なのだ。

たとえば誰が持とうと現金は現金だ。コンビニで買い物をするときに自分の身分を明らかにしてから現金を払うことをイメージすれば、その異常さは理解できるだろう。本来、お金があることを証明しさえすれば（あるいは品物を持っていることさえ証明すれば）、それが誰であろうと構わないはずだ。

さらに我々の現実世界では完全に匿名であることが必要な場合がある。たとえば選挙の投票がそうだ。投票は無記名で行われ、誰が誰に投票したか分からないことが保証されるというのが民主主義国家における選挙の原則だ。ネットワークを使った選挙投票であれば、「正当な選挙民であることを相手に提示して、その行使に当たっては完全に匿名である」という一見矛盾する技術が必要になってくる。

そこで出てくるのが「ゼロ知識証明」（Zero-Knowledge Proof）という技術だ。これは自分の持つ秘密の情報を隠匿しつつ、自分が秘密の情報を持っていることを示すマジックのような理論だ（❶）。ゼロ知識の「ゼロ」は漏れる知識がゼロだと言えばわかりやすいかもしれない。アイデアは1980年代初期に作られたが、この安全性の証明は数学的に難しく、受け入れられたのが1985年になってからになる。この方法を応用すると、たとえばサーバーに接続する際、接続を許されている正当なユーザー（クライアント）であることを証明しつつ、それがいったい誰なのかを秘密にできる仕組みもできる。

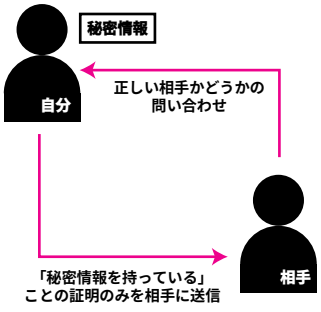
プライバシーを守る「Freedom」

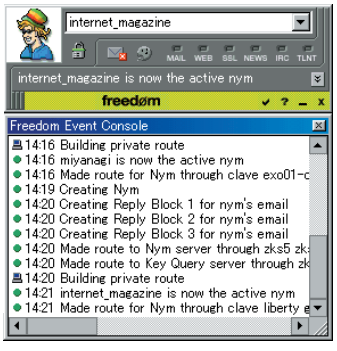
その名もZero-Knowledge Systems Jump というカナダにある会社が、この方法を使った究極のプライバシー保護ツールFreedomを開発した（❷）。全体システムは手元で使っているコンピュータからの情報漏洩を防ぎ、通信データを暗号化するFreedomというエージェントと、そのエージェントとバーチャルな秘匿ネットワークを形成し、実際のインターネットに乗り換えるためのFreedom Networkと呼ぶシステムからできている。このFreedomを使えば発信者はインターネット側では完全に匿名利用者だ。たとえFBIやNSAが追跡したとしても利用者を特定できる可能性は限りなくゼロに近い（❸）。

Freedomのような最先端システムがある一方で、現状のインターネット一般ユーザーレベルでは基本中の基本ともいえるデジタル署名による認証の利用方法や普及といったこともおぼつかない。まだまだゼロ知識証明のようにさらに進んだ技術が必要になるほどインターネットを取り巻く環境は成熟していないことは確かなようだ。

Jump www.zks.net

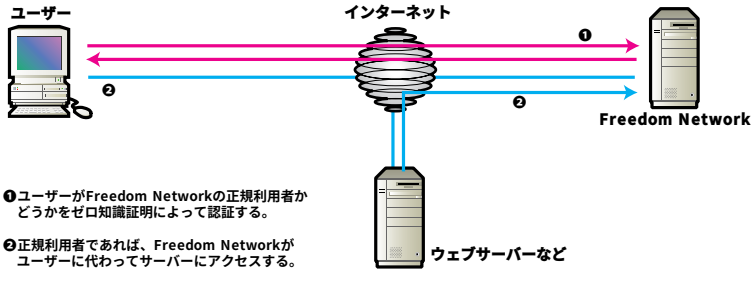
❶ゼロ知識証明





❷Freedomのクライアントソフト

❸Freedomの仕組み



エージェント：ユーザーの代理として稼動するプログラム。

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp