インターネットでの不正行為その傾向と対策

路地裏、繁華街、そして自室。実生活において、なにかしらのアクシデントが起こる可能性はどんな場所でも常にあります。でも、私たちは家から一歩も出ないわけにはいきません。私たちは、身の回りにどんな危険があるか、そのリスクを知ることでアクシデントを避ける術を知っています。インターネットもまた、実生活とそんなに変わらない心構えが必要なのです。今回は、そんなちょっとした心構えについてお話ししていきます。

第5回
自ら負うべきさまざまなリスクについて---AT YOUR OWN RISK

JPCERT/CC（コンピュータ緊急対応センター）
URL http://www.jpcert.or.jp/

インターネットを使うにあたり、不正アクセスや不正アクセスには当たらないが、不当な妨害や不快な思いをするといういろいろなリスクが発生します。今回は、そのリスクの中で、自分の責任で負うべきリスクとそのリスクの自覚について考えてみたいと思います。

個人情報を公開するリスク

インターネット上での個人情報の問題というのは、いくつかの段階があります。一番軽い段階は、自分のメールアドレスを自動的に収集されてしまい、ダイレクトメールが送られてくるレベルでしょう。このような不特定多数のメールアドレスに送られるダイレクトメールの類は、SPAM（スパム）と呼ばれます。

インターネットを使っている人のほどんどは、商品広告などのダイレクトメールを電子メールで受け取った経験があると思います。どこかのインターネット上の通販会社に電子メールを送った記憶もなく、何で知ったのか不思議に思うことがあるでしょう。

これは、SPAMの専門会社が存在していて、インターネット上で公開されているありとあらゆる情報から、自動的に電子メールのメールアドレスを抽出しているのです。ネットニュース、ウェブページ、メーリングリスト、その他可能なかぎりの情報源から自動的に収集しています。そのような会社は300万以上のメールアドレスを収集していると言われます。その収集したメールアドレスを売ったり、あるいは送付するのを代行したりする専門会社が海外には存在します。

あるいは、そこまで大規模ではなくてもなんらかの手段を使ってメールアドレスを収集して、自社広告のダイレクトメールを送る会社もあります。

インターネット上で積極的に電子メールを利用している人は、同時にそのメールアドレスがどこからか漏れ出し、ダイレクトメール業者に知られてしまうというリスクも負うことになるのです。

しかし、この程度であれば、インターネット上に限らず現実社会でも経験している現象

です。郵便受けには、毎日のようにいろいろな広告が投げ込まれていますし、また、知らない業者からのダイレクトメールが送られてくることもしばしばです。それ以上にSPAMが盛んなのは、インターネットでの電子メールの送付コストが、現実社会で印刷物や郵便料金にかかるコストに比べると非常にわずかだからです。非常に少ない反応率でも、わずかなコストで大量に送ることによって、それをカバーしているのです。

ですから、SPAMに対する非難を気にしないような業者がSPAMを行うのは、避けられないものがあります。無視して消してしまえばいいだけですが、多少なりとも無駄な通信コストを負担しなければならないのは、割り切れない気持ちになります。また、ポルノの通信販売や必要もないダイエット食品のダイレクトメールが次々と送られてくるのは、あまり気分のいいものではありません。

システム側でSPAM業者のアドレスを事前に登録して受け付けないようにしたり、あるいは、届いたメールの文を見て自動的に捨ててしまうようなソフトウェアもあるようですが、結局はイタチごっこで、決定的な解決方法はありません。電子メールを活用する以上は避けられないリスクなのです。

善意ばかりではない

次の例は、少々深刻です。よく雑誌などで、インターネットの活用事例として自己紹介や、自分の個人情報を出しているウェブページを紹介しているものがあります。そのような雑誌記事を見て、「ウェブページとは、自己紹介をするような場なのか」というように理解している人がいます。

しかし、その前に個人情報をインターネットで公開するということは、新宿や渋谷のような大都会で、自分の個人情報を壁に張り付けるということと同じだということを認識して欲しいと思います。必ずしも、善意の人のみが、その個人情報にアクセスしているわけではないのです。

「莫大なウェブページの中から自分のページを見つけだすというのは、非常にわずかな確率でしかない」と思っている人もいることでしょう。しかし、必ずしもそうとは言い切れません。ある出版社がインターネット上で公開しているウェブページ上で個人情報を出している女性のページ一覧を集めて興味本位な取り上げ方をしたという例がありました。掲載にあたって本人の承諾はとらなかったそうです。その結果、取り上げられた女性に、不特定多数の人から気分を害するようなメールが次々と送られて来たそうです。最後は、結局それまで使っていたメールアドレスを放棄せざるえなかったとのことです。このような事例は極端で、非常に稀だと思いますが、今後も同じような事例が出てこないとは限りません。個人情報を公開する危険性を低く見積もるべきではありません。

電子メールのメールアドレスを一般に公開するのも、個人情報をウェブページ上に公開するのも、そのリスクさえ十分に理解して公開しているのなら、第三者がその是非を議論すべきことではないと考えます。

本稿の目的は、あくまでも、存在するリスクを知らないということに対して注意を促すということです。その点をよくご理解ください。

自分で用意したCGIを使うリスク

CGI（Common Gateway Interface）は、WWWサーバーの機能をさまざまに拡張するための枠組みを提供するものです。その中でもプログラムのインターフェイスとしてウェブページを利用するものは、CGI-BINプログラムといいます。ここでは単にcgiあるいは、cgiプログラムと呼ぶことにします。

一般ユーザーが、自分でcgiを使えるようなインターネットサービスプロバイダーが数多くあります。また、一般ユーザーが使うようなcgiプログラムは、あちらこちらで公開されています。ところが、cgiプログラムの多くは、最小限のプロトタイプ的な仕様を実現しているだけで、例外的な入力に対する処理や、不正な利用に対してはまったく考慮されていないようです。そしてそのためトラブルを起こしています。

たとえば、よくある例としては、BBSのような仕様をもったcgiプログラムに対する嫌がらせや妨害です。この簡易BBS cgiプログラムというのは、ウェブページをインターフェイスとして、自由な入力を許し、入力されたメッセージはウェブページに反映されるというものです。多くは、入力されたメッセージを単純にウェブページの最後に追加するだけのごくごく単純なcgiプログラムです。認証や入力のアクシデントといったことを特別考慮しているようなものは、あまりないようです。

この簡易BBS cgiプログラムは、多くのものが「誰でも」、「いつでも」、「いくらでも」、好きなことが書き込めるような仕様になっています。しかし、ここで少し考えてください。制限のないアクセスを許しているウェブページは、新宿や渋谷のように不特定多数が訪れる場所のようなものです。もし、新宿や渋谷の人通りの多い所に、何でも書き込んで構わない掲示板があったら、いったいどんなことになるでしょうか。

ユーザーが、自分の思うとおりに簡易BBSのようなcgiプログラムを作ったり使ったりするのは、そのサイトの管理者の判断であり、また、ユーザーの判断でしょう。これも、第三者が口を挟むべきことではありません。しかし、そのような仕様の機能が中途半端なcgiプログラムが引き起こすトラブルは、そのプログラムを作ったり使ったりする者が背負っているリスクであることは確認するまでもありません。もし、そのリスクを認識せずに使うと、その認識のずれによって大きなトラブルとなる可能性があるでしょう。

ソフトウェアを使うリスク

ウェブページを見るために、私たちはウェブブラウザーを使います。ウェブブラウザーとてソフトウェアですから、何かしらのバグ（ソフトウェアの不具合）があります。

こう断言すると驚く方がいるかもしれませんが、ソフトウェアとは、そんなに完全なものではありません。特に新しい機能を加えた

後や、開発が終わったばかりの新しいソフトウェアには、まだ発見されないバグが潜んでいます。

問題は、そのバグがいつ、どのような形で現れるかです。もし、そのバグがたとえ深刻なセキュリティーホールであったとしても、そのリスクは使用する側が背負うことになります。ウェブブラウザーのセキュリティーホールを突き、WWWサーバー上のあるページをアクセスすると、突然コンピュータのディスクの中身を全部消してしまうようなプログラムの存在も否定できません。そのような潜在的なリスクは、常に潜んでいます。

もちろんきちんとした会社や組織の持つウェブページだけにアクセスするだけなら、そのようなサイトで故意にシステムを破壊するような罠は仕掛けられていないでしょうから、問題はほとんどないと考えてよいでしょう。ネットサーフなどと称して、あちこちのサイトにむやみにアクセスしている場合は、その罠に出会うリスクがぐっと上がります。

幸いなことに、通常は、上記のような致命的なソフトウェアのバグは、見つかり次第改良され、対処されたバージョンが短期間でリリースされます。問題は、そのような最新の情報をユーザーが知っているかどうかです。そして、その新しいバージョンを入手しているかです。

もし、広く問題点が知られている状態で、いつまでもセキュリティーバグをもったウェブブラウザーを使い続けることは、誰が考えても、かなり問題があるのは明らかです。

情報コントロールのリスク

情報のコントロールとして、最近よく話題になるのが、チェーンメールやデマメールです。もっとも有名なのは、“ Good Times ”というコンピュータウイルスに関するチェーンメールとデマメールです。今もどこかで「Good Timesというサブジェクトのついたメールは、コンピュータウイルスに感染しているメールなので注意するように」というデマが電子メールとして流れていることでしょう。

このチェーンメールとデマメールの特徴は、受け取った人が、善意でそのデマを自分の知っている人に流すことです。口コミで伝わるデマとは異なり、電子メールは、まったく「同じ内容」を「簡単に」、そして「すぐに」送れます。したがって、そのデマの伝搬は無制限にインターネット上に広がっていきます。

もしかするとこのGood Timesウイルスのデマの最初は、誰かを担ぐための単なる冗談だったのかもしれません。なぜなら、そもそもメールのサブジェクトにわざわざGood Timesと書いて送ってくることは非常に不自然だからです。理由や発端はともかく、現在でもGood Timesのデマは、死に絶えていません。

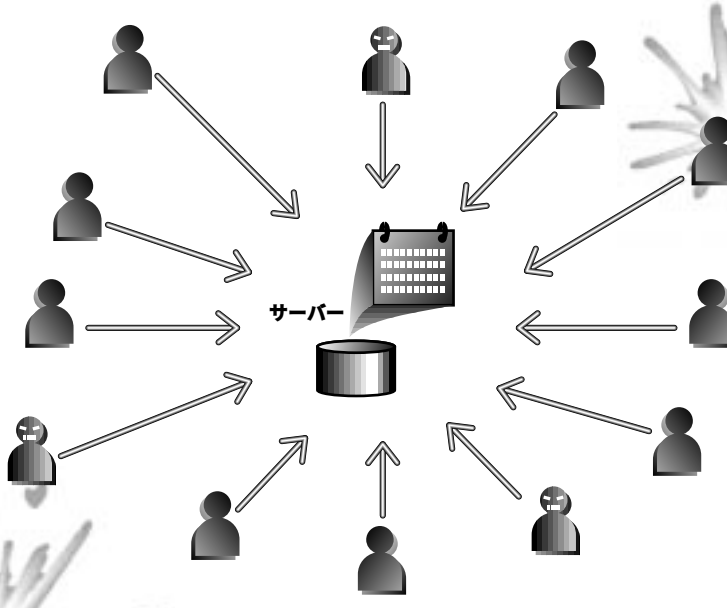
このリスクは何でしょうか。それは、不確実な情報に踊らされることです。このようにデマが流れるのは、別にインターネットのようなメディアに限らず一般社会でもあります。たとえば過去によく知られた例として「当たり屋情報」の怪文書があちこちに流れたというのがあります。これは、もっともらしい手口や自動車のナンバーまで詳細に書かれたもので、いろいろな会社などの間をFAXという媒体を使って流れていました。

もっともらしい内容が電子メールという新しくて非常に伝達の早いメディアに乗ってしまうと他のメディアでは見られない妙な説得力があります。そのようなメディアの特性を知ることによって、あなたが不確実な情報に踊らされるリスクを減らすことができます。

ソフトウェアの取得に関するリスク

インターネット上では自由にコピーして利用できるプログラムが多くの良心的な作者によって作成され、そして、あちらこちらのサイトで公開されています。そのようなボランタリーな精神があるからこそ、インターネットやコンピュータはさらに便利に使えるようになるのでしょう。これは称賛されるべきインターネット文化、あるいはインターネット

図A CGIを利用したプログラムを使う場合のリスク
不特定多数のアクセスを許すということは、どんな人がアクセスするか分からないというリスクを負う。



精神といえるでしょう。

その配布方法のタイプですが、UNIXでの配布の場合はソースコードという形で公開されているケースが多く、パーソナルコンピュータに配布される場合は、すぐに使えるようにコンパイルされた実行バイナリーという形で公開されているケースが多いという傾向があります。

パーソナルコンピュータ場合、心配なのは、その実行バイナリーがウイルスに侵されているかもしれないということです。しかし、これは故意にウイルスをばらまいているわけではありません。知らぬ間に自分のパーソナルコンピュータがウイルスに侵されており、そして知らぬ間に配布用の実行バイナリーにそのウイルスが付着してしまうのです。

●

このようなウイルスの伝染は、インターネットに限らず、日常の業務の範囲ですらも発生してしまう厄介な問題です。現在では、業務などでパーソナルコンピュータを使っている人は、実行バイナリーのやり取りやフロッピーのやり取りでウイルスが移らないように、ウイルス検知ソフトウェアを常用している人が多くなってきています。

一方、パーソナルコンピュータをもっぱらホビーやまったく個人的な範囲でしか利用しない人は、頻繁に実行ファイルやフロッピーを他の人とやり取りするわけではないので、あまりウイルス感染には神経を使ってはいない傾向があります。

管理がしっかりした信頼のおけるサイトから取る場合はあまり心配はないでしょうが、ソフトウェアを公開しているサイトのすべてが必ずしもきちんと管理しているわけではありません。また、管理者がウィルスに対して、どんなに努力しても完全ということはありません。ウイルスを自動的に検知するソフトを準備するといった事前の備えや、どのサイトが安全かを見抜くのは、ユーザーのリスク管理と言えるでしょう。

自己責任がキーワード

インターネット利用の責任の論理は、常に利用者が自己責任において利用するという点で一貫しています。ある意味で大人の論理です。しかし、多くのユーザーは、それに戸惑っています。なぜなら、インターネットは「これだけお金を払っているのだから、これだけのサービスは受けたい」というコストに対するサービスが与えられる場だと思っているからです。この意識は捨てなければなりません。

インターネットは、不特定多数の利用者がネットワークに接続することによって、集まってきている所です。参加資格があるわけではなく、誰かがコントロールしているわけでもないのです。

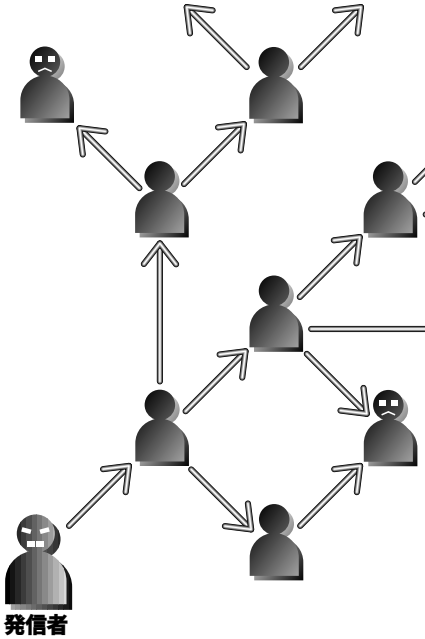
しかも、地域や国境といった地理的隔離もありません。これは何を意味するかというと、ネットワーク的には、どんな所に住んでいても、自由に大都会の繁華街に行けるということと同じです。情報の地域差ということでは差がなくなるわけですから、これはある意味ではすばらしいことです。しかし、大都会の繁華街は、一部の人にとっては、日常の風景であり、そのリスクも判断できるので安全でしょうが、必ずしもすべての人にとって日常の風景ではありませんし、また、安全であるとは限りません。

まとめ

インターネットを使うときは、常に頭の片隅にリスクということを思い出しながら使用しなければいけません。しかし、それは別にインターネットに限ったことではありません。本稿は、インターネットも現実社会と何ら変わらないという、ごく当たり前のことを再確認したにすぎないのです。

JPCERT/CCでは、本連載のバックナンバーをウェブサイト上で公開しております（PDF形式）。
URL http://www.jpcert.or.jp/magazine/beginners.html

図B チェーンメール伝搬の構造はデマと同じ



チェーンメールの広がり方は、口コミのデマとは比較にならない速度で広がる。これらのメールに対しては、無視してだれにも転送しないことだ。善意のつもりが、実はチェーンメールを広げていることになる。毅然として無視するためには、チェーンメールとは何かを知る必要がある。