インターネットでの不正行為 その傾向と対策

インターネットが普及するにつれて、これまでになかった悪質な行為が多発してきています。今月から始まるこの連載では、JPCERT/CC（ジェイピーサート・シーシー／コンピュータ緊急対応センター）が、そういった不正行為について解説します。無意味に怖がることはありません。被害に遭わないためのセキュリティー知識を身に付ければ避けられることなのですから。

第一回 不正行為を避けるためのリテラシーとは

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

急速に膨れ上がったインターネット社会

近年、急激なインターネットユーザーの増加に伴い、インターネット社会が一気に膨張しました。この状況をよく観察してみると、新しくインターネット社会に参入してくるユーザーには、今まで個人的にパソコンを単なる趣味の道具として扱ってきた人や、あるいはまったくのコンピュータの初心者レベルの人が増えてきています。

それ以前に、本格的にコンピュータやインターネットを使っていたユーザーは、基礎的かつ必要最小限の技術的な知識はユーザーとしてのリテラシー（教養）であり、当然持つべきものとの共通の認識がありました。そして、コンピュータ・セキュリティー、あるいはインターネット・セキュリティーと呼ばれるセキュリティーの知識も、リテラシーの一部に含まれると理解されていました。

現在では、そのような意識は希薄になり、コンピュータ・リテラシーとしてのセキュリティー知識を持たぬまま、インターネット社会に参加しているというのが現状です。

一方、それらユーザーを受け入れる側のインターネット社会の実情を見てみると、セキ

ュリティ知識を持たぬままインターネットを安全に利用できるほどには、技術も社会的な制度も、まだまだ未成熟です。それが、現在のインターネットブームの1つの問題点であり、また、そこからある種の歪みが生まれてきています。

これは、基幹サイトやサーバーを管理する人だけではなく、すべてのユーザーに当てはまります。PCといえどもソフトウェアによって、多目的に利用できる機械です。しかも、最近は驚く程の高性能です。それゆえに、そのような機械を正しくコントロールし、利用してゆくには、操作技術のほかに、その環境や状況に関する知識や経験が同時に必要なのです。それは、自動車を運転するには、安全運転には機械的操作技術も必要ですが、それ以上に、路上において役に立つ知識や経験が大切であるというのと似ています。

都会になったインターネット

インターネット社会は、天国のように善人だけが住む世界でもなく、あるいは、無政府状態の世界でもありません。それは限りなく現実に近い社会です。

ただ、昔のように研究コミュニティーが利用者の中心であった小さな村ではなく、今や誰でもが入ってきて、仕事や日常の連絡、あるいはオンラインビジネスで利用する、巨大な都会へと変貌しています。そこには、それなりの悪意も、犯罪も、事故も存在するのです。

にもかかわらず、多くのユーザーはそういったリスクを気にとめることもなく、無防備のままに利用しているのが実情です。そして、実際にトラブルに巻き込まれています。この図式は、「日本人観光客は、海外でも日本の感覚で旅行するため、事故や犯罪の被害に遭いやすい」と言われているのとよく似ています。その場その場の状況に応じたセキュリティー・リスクを認識し、そのリスクに対して正しい対応をしていないため、トラブルに巻き込まれる場合がほとんどです。しかも、その対応といっても、その街や国に昔から長く住んでいる人にとっては、ごく日常的なレベルのことなのです。郷に入れば郷に従えの教えのとおり、そこでの日常的なリスクや暮らし方を知らなくてはなりません。

また、その社会での暮らし方をアドバイスするような情報がもっと多く提供される必要性があります。残念ながら、今まではアドバイスというよりも、事故や事件に対して興味本位に取り上げ、煽るような情報が多かったのも事実ですし、またその反対に、リスクに対してまったく無頓着な情報も同様に多かったのも事実です。

リスクに対して正しい対応をするためには、利用する1人1人が正しくリスクを認識し、より有用なアドバイスが簡単に手に入ることができる状況を作り出す環境を作り上げていく必要があります。

JPCERT/CC とは何か

さて、ここで私たち、JPCERT/CCのことを少しご紹介いたしましょう。

●

コンピュータ緊急対応センター（JPCERT/CC -- Japan Computer Emergency Response Team /Coordination Center：編集部注“ジェイピーサートシーシー”と発音）は、インターネットを安全に利用するため、不正アクセス対策などの活動を行うことを目的に1996年10月に設立した中立的な組織です。コンピュータネットワークを介して行なわれる不正アクセスに対応する活動、それに付随するセキュリティー情報の収集と分析、再発防止策の検討、情報の提供や普及などの業務を行ないます。

JPCERT/CCは、いわゆるカスタマーサービスといった類のサービスを提供する組織ではありません。不正アクセスを受けて問題を抱えている方と、その問題を技術面で支援できる方とが、それぞれの立場を離れて問題解決へ向けて協調して活動できるように調整する役割を担うセンターを目指しています。あくまでも、問題を主体となって解決するのは「当事者」であり、JPCERT/CCはそれを支援するという立場です。

外務省が出している海外旅行安全ガイド。
URL http://www.mofa.go.jp/mofaj/toko/leaf/passport/index.html

JPCERT/CCの役割と活動内容
不正アクセスを受けた方々からの情報提供の受け付け
被害状況の把握
侵入手口の解明
再発防止を目指した関連技術情報の提供
インターネットセキュリティーに関する技術情報の収集・分析
不正アクセス防止策の検討と勧告文書の発行
緊急時の関係者間の連絡網の整備
セキュリティー技術の普及・啓発
海外の関連機関との情報交換および緊急時の連携

JPCERT/CCの役割や活動範囲ではない相談事例
法律の相談
パスワードを盗んだ犯人を探してほしい
パソコンの使い方がわからない
インターネットにつなぐ方法を知りたい
インターネットを始めるので、プロバイダーを紹介して
サーバーやシステム設定のコンサルタント業務
通販でのトラブル相談
クレジットカードが他人に使われたときの対処相談
キャッシュカードから金が引き出されたときの対処相談

JPCERT/CCのホームページ。不正アクセスに関する最新の情報が入手できる。
URL http://www.jpcert.or.jp/

なぜ警察ではないのか

犯罪を構成するような不正アクセスが発生した場合、警察はおそらくその犯人を捕まえてくれるでしょう。しかし、それだけでは、すべての解決にはなりません。問題を解決をするためには、システムにおけるセキュリティー上の技術的弱点（セキュリティーホール）を解消することが重要です。もし、セキュリティーホールを解消せずに放置したままでおけば、何度でも同じ不正アクセスが発生するでしょう。

JPCERT/CCの活動の対象

JPCERT/CCが活動の対象としている不正アクセスとは、日本国内の組織およびユーザーへの、インターネットを経由したシステムへの不正侵入、破壊、妨害、またはそれを目的とした不正なアクセスで、その影響が広範囲に及ぶ可能性があるものです。

不正アクセスのトラブルが発生したら

もし不正アクセスのトラブルが発生したら、「不正アクセス情報 届出様式」に、必要な情報を添付してJPCERT/CCへお送りください。

不正アクセス被害状況の受け付け手順、連絡先などの詳細に関してはJPCERT/CCのウェブページに説明を掲載してあります。

個別に調査してくれるのか

届け出を受けた不正アクセスの内容を検討し、インターネットを経由した不正侵入、破壊、妨害、またはそれを目的とした不正アクセスで、その影響が広範囲に及ぶ可能性があるとJPCERT/CCが判断した場合には、個別に調査する場合があります。JPCERT/CCが個別対応を行うかどうかは「コンピュータ緊急対応センター不正アクセス情報 届出様式」の形式で届けていただいた情報によりJPCERT/CCで判断いたします。

秘密は守られるのか

届け出を受けた不正アクセスに関する情報は、届け出た方から特に許諾を得ない限り、外部へ開示することはありません。

この連載の提供するもの

インターネットを利用するうえで、日常的な知識として必要なセキュリティーに関するリテラシー（教養）と、ごく初歩的なユーザーが持っているセキュリティーの知識には大きなギャップがあります。本連載では、その日常的な知識として必要なリテラシーをユーザーが身につけて実践していくために必要な情報を提供していきます。

なお、本連載では、基本的な知識を中心とするため、システム管理者やコンピュータ技術者が必要とする専門的なセキュリティー知識の範囲すべてをカバーするものではないことをあらかじめお断りします。

どんなことがリテラシーなのか

電子メールは、よくハガキにたとえられるように、故意、偶然にかかわらず、その配送途中で誰かに見られてしまう危険性を常に伴います。この事実を知ることは、1つのリテラシー（教養）と言えるでしょう。

さて、電子メールはなぜハガキと同じなのかを考えてみましょう。電子メールの配送も、郵便と同じで、相手に届くまでにはいろいろな中継局（メールサーバー）を経由します。そのため電子メールは、配送途上にあるメールサーバー上で、一時的に保存されます。

受け取った電子メールがどのようなメールサーバーを経由しているかは、各電子メールのヘッダー部分にある“Received:”以下の部分に情報として記録されます。自分の受け取った電子メールがどのようなメールサーバーを経由してきたかを一度、じっくりと観察してみてください。

一時的に保存される以上は、配送途上にあるどのメールサーバー上でもメールの内容を見ることができます。

配送途中で電子メールが偶然に他人の目に触れてしまうケースとして多いのは、メールサーバーの不調で電子メールが配送できず留まってしまった場合や、なんらかの理由で相手先に届かず、エラーとなって管理者に宛先不明で届く場合です。

もちろん、多くの善良な管理者は秘密保持に努めてくれるでしょう。しかし、こんなことを想像してください。ある会社の社員と別の会社の社員が、あまり公にしたくないプライベートな情報を電子メールでやりとりしているとしましょう。その時、配送途中にあるメールサーバーのどれかが不調になり、その電子メールが途中のメールサーバーの管理者に届いたとしたらどうなるでしょうか。「王様の耳はロバの耳」の話を思い出せば、どのような状況になるかは想像がつきます。

もちろん悪意に満ちた電子メール覗きというのも考えられます。途中でいろいろなメールサーバーを経由して電子メールが届くわけですが、私達は1つ1つの経由するメールサーバーが、どのような人間により、どのような形で管理されているかを知るよしもありません。もし、どこかのメールサーバーに悪意を持つ管理者がいたら、そこのメールサーバーを経由する電子メールはアウトです。

プロバイダーやパソコン通信事業者は、電気通信事業法により厳しく情報管理を義務づけられています。しかし、一般の組織内におけるサイト管理では、明確な業務とは認められずにオーソライズされた管理者がいなかったり、運用規程があいまいであったりする場合もありますので、どこまできちんと管理しているかは、外部からはわかりません。

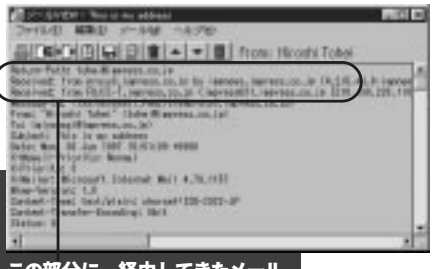
●

さて、このような知識を持つことによって、電子メールはハガキと同じようなものであるということがわかりました。この知識を得た後は、たとえば電子メールでクレジットカード番号を書いて送ることにどのようなリスクが伴うのかを、日常的な知識として思い浮かべられるはずです。これがリテラシーなのです。

次回から

次回は、「不正アクセスとは何か」についてお話したいと思います。「不正アクセス」の定義は、「システムを利用する者が、その者に与えられた権限によって許された行為以外をネットワークを介して意図的に行うこと」となります。もちろん、これだけには何のことなのか、わかりません。そこで、不正アクセスとは、具体的にどのようなものなのかを解説したいと思います。

まず、不正アクセスの全体像をつかんでもらってから、個々の問題となるテーマとその背景、および技術的問題点や対処法を続けていきたいと思います。



この部分に、経由してきたメールサーバーが表示される。

電子メールはいろいろなメールサーバーを経由してくる。その途中で間違って中身を見られてしまう可能性はある。あるいは、わざと見ようとする人も…。