インターネット

セキュリティセミナー

あとを絶たないセキュリティ事故

目次

[個人情報が盗まれる 2](#_Toc394398038)

[外部から攻撃される 2](#_Toc394398039)

[ウイルスに感染する 2](#_Toc394398040)

[ウイルスの種類 2](#_Toc394398041)

[情報や人にだまされる 3](#_Toc394398042)

[ホームページの閲覧 3](#_Toc394398043)

[サービスの利用 3](#_Toc394398044)

[その他 3](#_Toc394398045)

[フィッシング詐欺 3](#_Toc394398046)

[ワンクリック詐欺 3](#_Toc394398047)

インターネットはとても便利ですが、危険が潜んでいることを忘れてはいけません。世の中にお金をだまし取ろうとする人や他人を傷つけようとする人がいるように、インターネットの世界にも同じような悪い人がいるのです。

# 個人情報が盗まれる

インターネットに接続するときに入力するパスワードや、オンラインショッピングのときに入力するクレジットカード番号などの個人情報が盗まれて、他人に悪用されてしまうことがあります。個人情報はきちんと管理しておかないと、身に覚えのない利用料金を請求されることになりかねません。

# 外部から攻撃される

インターネットで世界中の情報を見ることができるというのは、逆にいえば、世界の誰かが自分のパソコンに侵入する可能性があるということです。しっかりガードしておかないと、パソコンから大切な情報が漏れてしまったり、パソコン内の情報を壊すような攻撃をしかけられたりします。

# ウイルスに感染する

「コンピューターウイルス」とは、パソコンの正常な動作を妨げるプログラムのことで、単に「ウイルス」ともいいます。ウイルスに感染すると、パソコンが起動しなくなったり、動作が遅くなったり、ファイルが壊れたりといった深刻な被害を引き起こすことがあります。ウイルスの感染経路として次のようなことがあげられます。

1. ホームページを表示する
2. インターネットからダウンロードしたファイルを開く
3. メールに添付されているファイルを開く
4. USBメモリなどの移動メディア

## ウイルスの種類

ウイルスには、次のようなものがあります。

| 種類 | 症状 |
| --- | --- |
| ファイル感染型ウイルス | 実行型ファイル（プログラム）に感染して制御を奪い、感染・増殖するウイルス。 |
| トロイの木馬型ウイルス | 無害を装い利用者にインストールさせ、実行するとデータを盗んだり、削除したりすることを目的としたウイルス。感染・増殖機能はないので、厳密にはウイルスとは区別される。 |
| ワーム型ウイルス | ネットワークを通じてほかのコンピューターに伝染することを目的としたウイルス。ほかのプログラムに寄生せず、自動的に増殖する。 |
| ボット（bot）型ウイルス | 他人のコンピューターを外部から操るためのプログラム。 |
| マクロウイルス | ワープロソフトや表計算ソフトなどに搭載されているマクロ機能を悪用したウイルス。ファイルを開いた時に感染する。 |
| スパイウェア | パソコン利用者に知られないように内部に潜伏し、データを外部に送信する。厳密にはウイルスとは異なり、マルウェアのひとつとされている。 |

# 情報や人にだまされる

## ホームページの閲覧

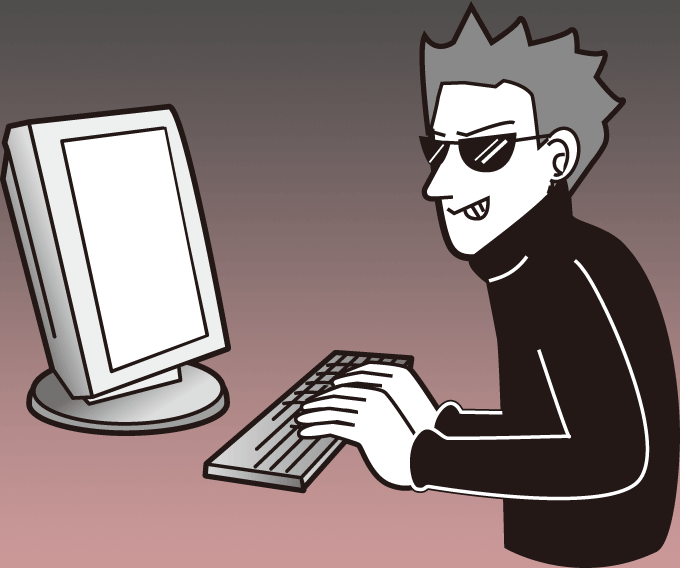
誰もが自由に情報を発信できるホームページ。その情報がすべて真実で善意に満ちたものとは限りません。内容が間違っていることもあるし、見る人をだまそうとしていることもあります。

## サービスの利用

巧みに誘い込まれて、無料だと思い込んで利用したサービスが、実は有料だったということも少なくありません。また、インターネットを通して新しい知り合いができるかもしれませんが、中には悪意を持って近づいてくる人もいます。安易に誘いに乗ると、危険な目にあう可能性があります。

例えばネットオークションの場合…

* 落札したけれど品物が届かない。
* 商品を購入したけれど商品が届かない。



## その他

### フィッシング詐欺

「フィッシング詐欺」とは、実に悪がしこい詐欺です。送信者名を金融機関などの名称で偽装してメールを送信し、メール本文から巧妙に作られたホームページへジャンプするように誘導します。そして、そのホームページに暗証番号やクレジットカード番号を入力させて、犯人のところに送信させるのです。

### ワンクリック詐欺

「ワンクリック詐欺」とは、クリックしただけなのに、表示されるホームページで利用料金を請求するような詐欺のことです。受信したメールに記載されているアドレスをクリックしてホームページを表示したところ、「会員登録が完了したので入会金を支払いなさい！」と一方的に請求されたというような事例も報告されています。ホームページに問い合わせ先やキャンセル時の連絡先などが表示されていることもありますが、絶対に自分から連絡してはいけません。便利なインターネットですが危険も潜んでいることを知っておきましょう。

コラム：ソーシャルエンジニアリングとは

物理的・人的手口によって重要な情報を入手し、その情報を悪用することを「ソーシャルエンジニアリング」といいます。技術的な知識がなくても、人間の心理的な弱点を突くことで誰でも簡単に情報を悪用できるため、警戒が必要です。

●なりすまし

「なりすまし」とは、上司、情報部門の人間、顧客などになりすまして、不正アクセスのための情報を聞き出した上で、盗んだIDやパスワードを使って正規のユーザになりすまし、コンピューターを悪用することです。

●トラッシング（ごみ箱あさり）

「トラッシング」とは、清掃員になりすますなどしてごみ箱をあさり、顧客情報、人事情報、商品開発情報などの情報を収集することです。

●盗み見

「盗み見」とは、パスワードを入力しているときにキーボードを見たり、肩越しにパソコンのディスプレイを見たり、席をはずしている人の机上にあるメモやノートを見たりすることです。

●情報の盗難、漏えい、紛失

情報の「盗難」とは、不正にシステムに侵入し、システム内の重要な機密情報を持ち出すことです。また、業務用のノートパソコンを社外に持ち出し置き忘れることで、重要な情報を「紛失」してしまうこともあります。

盗難されたり、紛失したりした機密情報は、第三者に「漏えい」する可能性があります。

●情報の改ざん

「情報の改ざん」とは、不正にコンピューターに侵入し、コンピューター内のデータを不正な手段で書き換えることです。

→参考資料：「情報を守るために気を付けること」

セキュリティセミナー配布資料

最終更新日：2015/4/1