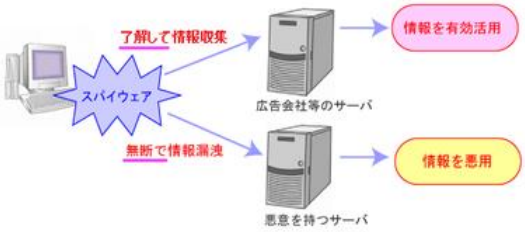
スパイウェア

パソコンを使用するに当たって、「メールに添付されたファイルを不用意に開けないように」や、「配信元が分からないプログラムを勝手にインストールしないでください」といった注意を受けたことはありませんか？これは「ウィルス」や「スパイウェア」などの悪質なものが流行していて、これらの操作でパソコン内に侵入するおそれがあるからです。
「ウィルス」については「ウィルス、ワーム、トロイの木馬」のページで触れましたので、ここでは「スパイウェア」について解説します。

スパイウェアとは、コンピュータの中に入り込んで、どのようなサイトをよく見ているかなどのユーザーの行動や、個人情報を収集し、ユーザーの気づかないうちに、収集した情報を特定の企業・団体・個人等に自動的に送信するソフトウェアのことを言います。

スパイウェアはすべて悪質というわけではありません。
ソフトウェアの品質を保つために、あるいはマーケティング活動としてユーザーの意識やニーズをつかむために、ソフトウェア開発会社にユーザーの利用状況や障害情報などを送信するスパイウェアを組み込むことがあります。この種のものは、通常はソフトウェアの「エンドユーザー使用許諾契約」（利用規約）に情報を送信する機能を組み込むといった旨の説明が記載されていて、インストール時にはこの利用規約に同意が求められます。



スパイウェアには悪意のあるものとないものがあります
（出典：東京経済大学「スパイウェアの基礎知識」）

その一方で、スパイウェアがあるとは知らせずにソフトウェアを使用させて、ユーザーの行動を監視したり、個人情報を盗むという悪質なものもあります。スパイウェアが問題視されるのは、この種のスパイウェアにより、ユーザー名、ID、パスワード、クレジットカード番号などが流出して、実害が生じることにつながるからです。

悪質なスパイウェアの侵入方法・感染経路は、主に以下の4通りが考えられます。

1. オンラインソフトやフリーソフトのインストール時に侵入する
2. メールの添付ファイルをクリックしたことで侵入・感染する
3. ホームページなどの閲覧によって侵入・感染する
4. 第三者が故意にインストールする

1 が最も多く、利用条件をよく読まずに承諾して、気づかずにソフトウェアと一緒にスパイウェアをインストールしてしまった、ということのないように気をつけましょう。また、極めて悪質な場合は、利用条件に情報を送信する機能については一切触れていないこともありますので、オンラインソフトやフリーソフトのインストールは避けた方が無難です。

ウィルスとの違い

スパイウェアの目的は、ユーザーがどのようなサイトをよく見ているかの行動を監視したり、パソコン内にある個人情報を盗むことであるので、パソコン内で目立つことなく活動します。そのため、基本的には、スパイウェアに感染していても、いつもどおりにパソコンを使用できます。いつもどおりにパソコンをユーザーに使用させることで、パソコン内にある個人情報やユーザーの行動を外部に流出させ続けます。

一方、ウィルスの目的は行動などを監視することではないので、パソコンの挙動に影響を与えるものが多く、悪質なものではハードディスクに記録されているファイルを消去したり、コンピュータが起動できないようにしたりするものまであります。
さらに、ウィルスはその「ウィルス」という名前のとおり増殖する仕組みを持ち、パソコン内のファイルに自動的に感染したり、ネットワークを介して、他のパソコンに感染したりという増殖・感染という仕組みを持っています。これに対して、スパイウェアは増殖・感染という仕組みを持っていません。

スパイウェアへの対策

スパイウェア対策としては、他のコンピュータウィルスと同様に、まずはパソコンのセキュリティ対策を行い、OS やセキュリティソフトを最新の状態にしておくことが重要です。こうした一見とても初歩的・基本的に思えるようなことが最も効果的なのです。

この他に、怪しいサイトをむやみに閲覧しない、怪しいメールに添付されているファイルを開かない、無料ソフトをダウンロードする際には使用許諾書などをしっかりと読み

リスクを把握する、どうしてもソフトをダウンロードする際には信頼できるサイトからダウンロードするということがポイントになってきます。

自分を守るのは自分という意識で家の防犯対策をするように、パソコンの防犯対策も行いましょう。