パソコンのセキュリティー対策

昨今、コンピュータを狙ったウイルスや詐欺が日常的に飛び交うようになりました。被害は愉快犯的な軽微なものから致命的なものまで様々です。
パソコンは外部からの侵入をブロックする機能を備えていますが、犯罪者は様々な方法でパソコンへの侵入を試みます。

良くある方法がトロイの木馬のような罠を仕掛けたメールです。パソコンに被害を与えるプログラムを添付ファイルで送って来たり、メールの中に悪意のあるホームページに誘導する URL（青字に青色のアンダラインがひかれているホームページへのリンク情報）を送ってきたりします。
これらのメールは魅力的だったり、逆に、対応しないと問題になるぞというような脅迫めいたものだったり、官公庁や著名な企業/団体を語ったり、ついつい操作する気にさせますが、添付ファイルを開いたり、URL をクリックすると被害を発生させます。

また、取引銀行等からのメールのように見せかけ、銀行等のホームページそっくりの画面でログインを促し、パスワードを盗みだすオレオレ詐欺のようなケースもあります。

これらの例では、メールの送信者やメールの内容を慎重に確認し、「何かおかしい、心当たりがない」と感じたら、メールを捨てるか、誰かに相談するのが賢明です。

メールの代わりに、パソコンの画面にメッセージを表示し、その中のボタンを押すと問題を起こすケースもあります。「パソコンに異常があるので、解決するためにボタンを押してください」のようなメッセージで、つい押してしまいますが、無視しないといけません。メッセージを消去できない場合、パソコンを再起動してください。

ユーザの手を借りず、パソコンの中のプログラムのガードの弱い部分を利用してパソコンに侵入する方法もあります。プログラムの開発者はガードの弱い部分がわかると修正版を発行するので、プログラムアップデートを確実に実行し、プログラムを最新の状態にしておくことが望まれます。

プログラムのインストール、USB メモリ等を使ったファイルのやり取り等、外部からの取り込みも注意が必要です。プログラム、ファイル、USB メモリ等がウイルスに感染しているとそれが持ち込まれます。氏素性のはっきりしないプログラムはインストールしない、USB メモリをパソコンに挿入した時は USB メモリのウイルスチェックを行ってからファイルを取り出すことが求められます。

有料のセキュリティーソフトを使用されている方がおられると思います。セキュリティーソフトを使用していない Windows パソコンでは、有料ソフトほどの機能はないものの、Windows Defender というマイクロソフト社製セキュリティーソフトが動作しています。これらのソフトがあれば安心していられる訳ではありません。犯罪者は常に新らたな方法を考案し、セキュリティーソフトといたちごっこを繰り返しています。また、セキュリティーソフトごとに機能/性能が異なり、全ての問題に対応できる訳ではありません。セキュリティーソフトに頼らず、上記に記載したようなパソコン使用者の注意深い対応が必要です。

万一に備えて、定期的に必要なデータをバックアップしておきましょう。致命的な被害に合った時に、Windows やプログラムは入手できますが、データは復元できない場合があります。セキュリティーの問題だけでなく、ハードウエア/ソフトウエアのトラブル時も有効です。