

サイバー犯罪相談窓口



スパイウェアについて

知らない間にパソコンに侵入し、キーボードの押下情報を読みとり盗聴者のパソコン等に自動送信するスパイウェアによる被害が拡大しています。

スパイウェア侵入



被害の形態として

- 自分の口座預金が知らないうちに他人の口座に送金されている。
- 利用した覚えがないのにクレジットカードの請求がきた。というもので、被害は個人に限らず企業や商店、銀行などにまで広がりを見せています。

被害者の共通点

- インターネットバンキングやネットショッピングでのクレジット決済等の利用者である。
- 不正送金などの被害を受ける前に、迷惑メールや苦情メールなどに添付されていた画像ファイルなどを開いたことがある。
- 心当たりがないところから突然届いたCDをインストールしたことがある。

などです。

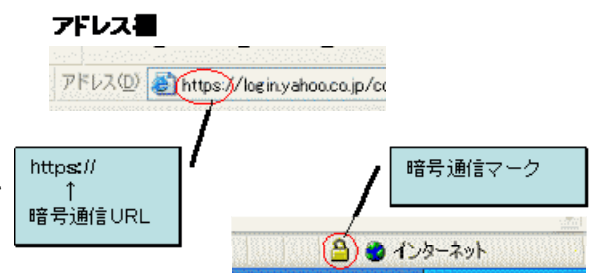
一説によると3割程度のパソコンは、悪意の有り無しに関わらず、何らかのスパイウェアが侵入しているという話もありますが、スパイウェアを意識して定期的に検査・駆除しているという方は少数のようです。

暗号化通信だと安心

インターネットバンキングやネットショッピングで取引を行う際、SSL(暗号化)通信モードになっていても安心はできません。

スパイウェアはキーボードのどのキーが押されたかを監視し送信しますので、パソコンから外部にデータを送信するときに暗号化処理が行われる暗号化通信ではカード番号やパスワードの漏洩を防ぐことはできません。

暗号通信モード(SSL)



インターネットエクスプローラー右下隅の表示

侵入しているか

スパイウェアは、その存在が知られないよう活動しますので、自分のパソコンにスパイウェアが侵入しているかどうかを見かけだけで見分けることは難しいのが実際です。

また、スパイウェアはコンピュータウィルスとは異なる種類のものであり、最近のウイルス対策ソフトではスパイウェアに対応したものもありますが、やはりスパイウェアに特化した検出・駆除ソフトでなければ見つけることは、難しいのかも知れません。

ネットショッピング



予防策

フリーのスパイウェア対策ソフト(SPYBOT、SPYPOT、SPYPODなど)やスパイウェア対応のセキュリティ対策ソフトなどを使用し定期的な検査・削除を行うことはもちろんですが、日頃の心がけとして、

- 心当たりの無いところからのメールは開かない。
- ダイレクトメール等で届くCDなどのプログラムをうかつに実行しない。
- 不審なサイトに不用意にアクセスをしない。
- カード番号やパスワードが必要なインターネットバンキングやネットショッピングを利用する際は、事前にスパイウェアの検査・駆除を行ってから利用する。

まとめ

スパイウェアによる被害は経済的ダメージが大きく、気づくのが遅いのが特徴です。安全にインターネットを楽しむためには、日常的な対策と自己防衛意識が大切です。