見極めが難しいスパイウェア

スパイウェア

- キーロガーを仕掛けて個人情報などを盗む
- 表示サイトを変更するブラウザハイジャッカー
- PC の遠隔操作による不正使用
- 突然音や画像表示をするジョークプログラム
- ポップアップ表示させるアドウェア

侵入経路

- フリーソフトダウンロード
- メール添付ファイル
- 閲覧した Web ページからの侵入
- 遠隔操作による不正ダウンロード

スパイウェアは、個人の情報や PC 内のファイルを知らない間にネットを使って外部に送信するなどのスパイ行為や、悪質な広告表示やコンピュータに重大な問題があると偽りメッセージを出し購入を促すなどを行うソフトウェアです。
定義が曖昧なため、不正とは言い切れないような広告目的のものや、アプリの仕様で必要な情報として入手することをユーザに許可させているものなどもあるため、必ずしも犯罪であるとは決めつけれないようなソフトウェアもあります。
一方悪意を持ったマルウェアとなる、ユーザの ID, パスワードや、カード情報を盗むものなどもあるため対策が必要です。
代表的なケースは、フリーソフトなどをダウンロードするときに、有用なアプリに埋め込まれていてインストールしてしまうようなパターンです。他には、OS やブラウザのセキュリティホールを利用して特定の Web ページを閲覧している間にインストールされてしまったり、スパイウェアのプログラムがメール添付されてきてクリックするとインストールされてしまうようなパターンです。
スパイウェアによる被害は、そのプログラムにより広告表示で不快にさせるものから、CPU やメモリを消費してスローダウンさせるものや、キーロガーを使って、ログインする際に ID やパスワードなどの機密情報が盗まれ情報漏洩してしまう悪質なものまで多種多様です。
一般的なウィルスとは挙動が違い、主なスパイウェアは自己複製して増殖するようなことはなく、こっそりと情報を盗むことが目的なので、ファイルを削除したり、PC をロックするようなわかりやすい悪質な振る舞いがみられません。
最近では、多くの Web マーケティング用のツールも Cookie を利用して閲覧履歴をトラッキングしていたり、Cookie の内容をもとに広告配信するような手法も多くみられ、どこまでが犯罪と呼べるかが難しいために何をスパイウェアとして登録するかも、スパイウェア対策ソフトのメーカー側でも困っているようです。
こうしたことから、セキュリティ対策ソフトばかりに依存せず、社内のセキュリティポリシーに従い、許可されたプログ以外はダウンロードを禁止し、OS やブラウザも社内で推奨されるバージョンに常に更新し、不審なメールは開かないようにすることが大切です。
スパイウェアは、気づかないうちに監視されていたり、外部に情報を送信されてしまう危険があるため、アンチスパイウェア機能の導入はもちろん、PC のパフォーマンスなどを気にかけて、常に監視し注意することが必要です。