

# スパイウェア対策ソフトの紹介

総合情報基盤センター  
技術専門職員 小野 隆久

## 1. はじめに

学外に対して大量通信を行ったPCの調査依頼を管理者にお願いしたところ、調査の結果AntiVirusで検出されなかったスパイウェアなどのウィルスに感染していました。

総合情報基盤センターで貸し出しを行っているAntiVirusは、スパイウェアにも対応はしているものの全てのスパイウェアには対応できていないのが現状です。そのため、スパイウェア対策としてスパイウェア専用の対策ソフトが必要になってきています。

## 2. スパイウェアの種類と侵入経路

スパイウェアは、PC情報、個人情報、Webの閲覧履歴などを収集しマーケティング会社など、スパイウェアの作成元に送信するアプリケーションソフトのことです。

スパイウェアの種類には、オンラインバンキングのユーザーID/パスワードからクレジットカード番号までユーザのキーストロークをすべて記録する「キーロガー」、フリーウェアやファイル共有ツールに付随し、ポップアップ広告を表示させたりオンライン活動履歴を収集したりする「アドウェア」、hostsファイルやWebブラウザの設定を書き換えてユーザーが意図しないサイトに誘導する「ブラウザハイジャッカー」などがあります。

スパイウェアの侵入経路には、フリーウェアやシェアウェアなどとセットで配布されるケース、Webサイト閲覧時にスパイウェアがダウンロードされてしまうケース、メール経由でインストールされるケースなどがあります。

スパイウェアは、ユーザ登録の情報を収集する目的と明記されていたり、ホームページやメールの添付ファイルなどに組み込まれていたりするため、ユーザは知らないうちに自分でスパイウェアをインストールしてしまうケースがほとんどです。

## 3. スパイウェアに感染したときの症状

スパイウェアに感染すると情報の収集を行うだけでなく、PCに下記のような症状が出ます。

- (1) ブラウザの最初のページが書き換えられ、修正しても元にもどってしまう
- (2) お気に入りに変なサイトが登録され、消しても消しても再生する
- (3) ポップアップウィンドウが常に、あるいは時々勝手に出る
- (4) 新しい接続が作成され、ブラウザを立ち上げると勝手に接続してしまう
- (5) 総合情報基盤センターから大量通信を行っているときと連絡があったとき
- (6) カーソルが勝手に動いたり、PCが不安定で動作が遅く、よく固まる
- (7) 終了時にエラーが出て終了できない
- (8) 急にスパムメールが沢山来るようになった

こういった症状が出たらスパイウェアに感染している可能性がありますので、AntiVirusやスパイウェア対策ソフトなどでスパイウェアのスキャンを行ってください。

## 4. スパイウェア対策ソフト

スパイウェアを検出・駆除するときは、ウィルス対策ソフト(AntiVirusなど)では検出できないスパイ

ウェアがありますので、スパイウェア専用の対策ソフトによるスパイウェアのスクリーンが必要になります。

代表的なフリーウェアのスパイウェア対策ソフトには、

- (1) Microsoft社 Windows Defender
- (2) Lavasoft社 AD-Aware 2007 Free
- (3) PepiMKSoftware社 Spybot Search&Destroy 1.2

があります。

なお、スパイウェア対策ソフトと称したスパイウェアもありますので、ご注意ください。

#### (1) Windows Defender

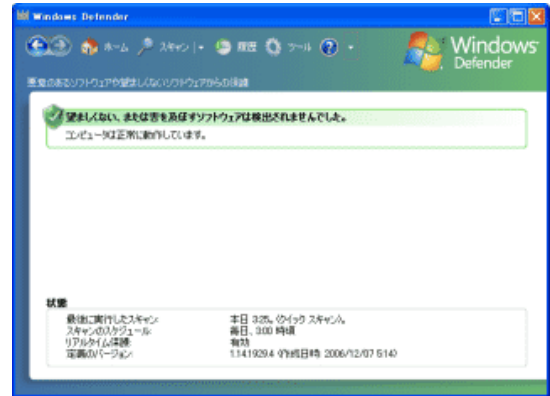
Windows Defenderは、Microsoft社がMicrosoft正規ユーザーに対して無償で提供しているスパイウェア対策ソフトです。

Windows Defenderの最低システム要件は、次のとおりです。

- \* CPUはIntel Pentium 233MHz以上、Pentium IIIを推奨
- \* OSはWindows XP SP2以降、Windows Vista、Windows Server 2003 SP1以降
- \* 64MBのRAM(最低)、128MB RAM(推奨)
- \* 20MBのハードディスクの空き容量
- \* Microsoft IE(Internet Explorer)6以降
- \* ネットワークに接続されていること
- \* Windows Installer version 3.1以上

Windows Defenderの主な機能は以下の5つがあります。

- \* スパイウェアの検出・削除
- \* スパイウェアスキャンのスケジュール設定
- \* スパイウェアの侵入ブロック機能
- \* トロイの木馬などのウイルスにも対応
- \* Windows Updateによるスパイウェア更新定義ファイルの自動更新機能



#### (2) AD-Aware

AD-Awareは、スウェーデンのLOVASOFT社によって開発されたスパイウェア対策ソフトで、フリーウェア版(AD-Aware 2007 Free)とシェアウェア版(AD-Aware SE Plus)の2種類があります。

AD-Awareの主な機能は以下の4つがあります。

- \* スパイウェアの検出・削除
- \* オプションで指定したフォルダやドライブのみ指定しての個別スパイウェアスキャン
- \* トロイの木馬などのウイルスにも対応
- \* スパイウェア更新定義ファイルの半自動更新機能



#### (3) Spybot Search&Destroy

Spybot Search&Destroyは、PepiMKSoftware社によって開発されたフリーウェアの日本語表記可能なスパイウェア対策ソフトです。

Spybot Search&Destroyの主な機能は以下の6つがあります。

- \* ボタン操作一つで日本語表記に変換可能、日本語以外にも多くの言語に対応しています
- \* 既に侵入してしまったスパイウェアの検索 & 削除機能
- \* ブラウザのセキュリティを強化する常駐保護機能
- \* スパイウェアの強制的なダウンロードを検出しユーザーに知らせる
- \* トロイの木馬などのウイルスにも対応



\* 検出結果の詳細を表示（スパイウェア名称、形式など）

## 5 . おわりに

総合情報基盤センターで、WindowsXP SP2 とWindowsVista でWindows Defender とAntiVirus を併用して使っていますが、今のところ不具合等は起きていません。

AntiVirus で検出できなかったスパイウェアに感染した場合、手作業によるPCの復旧にはかなりの専門知識と時間を要します。そのため、スパイウェアの検出・駆除専用のスパイウェア対策ソフトの導入でホームページの閲覧などのネットワーク利用がさらに安全なものになると思います。