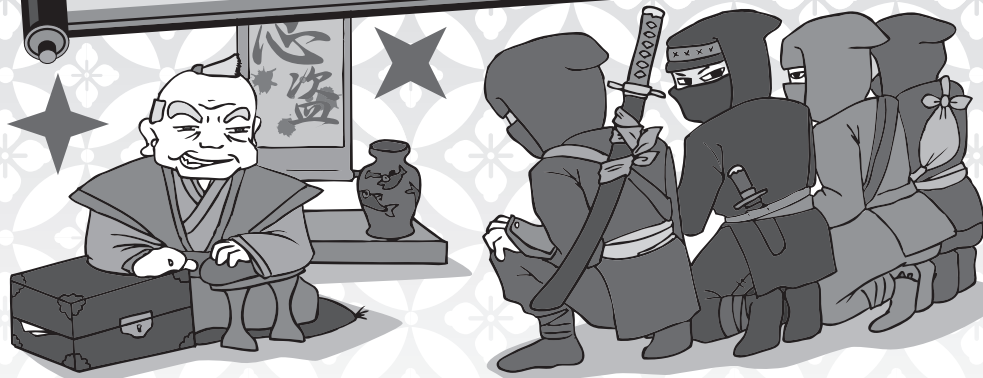


# 徹底解明! スパイウェアの謎



ひと頃比べ、コンピュータウイルスに感染して大騒ぎになるケースは減っているように感じる。しかしこれは、ウイルスそのものが減っているわけではなく、むしろ巧妙になっていることを意味する。そんな中、最近にわかに注目を集めているのが「スパイウェア」を利用した犯罪行為だ。ではこのスパイウェアは、従来のウイルスなどとどう違うのだろうか。

文・株式会社ラック サイバーリスク総合研究所 先端技術開発部 新井 悠

編集・石山俊浩

## 認知度は上がりつつある スパイウェア

今から3年ほど前、2005年から2006年にかけて、急速に国内の小売市場へスパイウェア対策専用製品が投入された。これは同時に、古くから存在していた「マルウェア(Malware: Malicious Software)\*」に、新たな脅威としてスパイウェアが台頭してきたことを意味する。実際、当時スパイウェアを悪用した国内の検挙事案が発生し、

社会問題として大きく取り上げられたこともあるだろう。現在では、それらスパイウェア対策専用製品に並んで、従来からあるウイルス対策ソフトにもそれらの対策機能が取り込まれたことで、市場としては一息ついた状態となっている。しかしながら、スパイウェアの脅威自体がなくなったわけではない。

スパイウェアの脅威については、新聞やインターネットなどを通じて、実際の事件などが報道されるにつれ、一般に浸透していったといえる。たとえ

ば、独立行政法人情報処理推進機構(IPA)が2007年12月に明らかにした「情報セキュリティに関する脅威に対する意識調査(2007年度第1回)」によれば、「ボット」や「セキュリティ対策の押し売り行為」は、なかなか市民権を得られていない一方で、スパイウェアはフィッシングやワンクリック不正請求といった言葉と同様の高い認知度を示

\*: 従来より「コンピュータウイルス」と呼ばれてきたが、現在ではこの呼称が一般的になっているため、本稿ではこの表記に統一する。

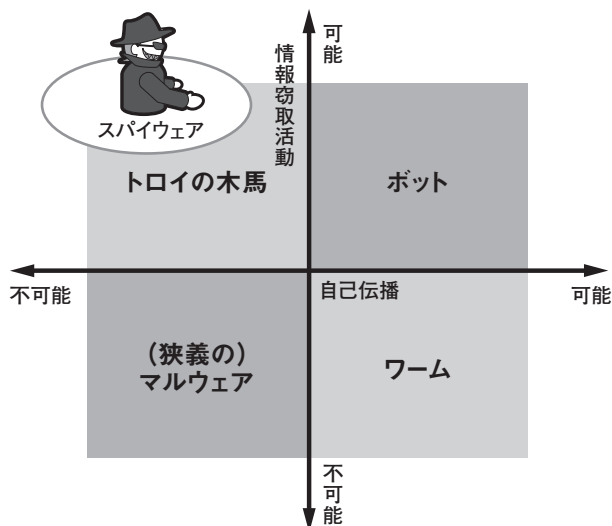


図1 マルウェアのカテゴリ分け

カテゴリ	感染活動内容
ボット	遠隔からネットワークを通じてコマンドを受信し、その意のままに活動させられるマルウェア。コマンドを送信する指令サーバをCommand and Control (C&C)サーバと呼び、指令サーバを操作する攻撃者はハーダー (Herder: 牧夫) と呼ばれる。スパム送信やDDoS攻撃に使用されることもある。
トロイの木馬	元々は「正規の、あるいは正当なソフトウェアになりすまして、悪意ある活動を行なうソフトウェア」を指している。今では、自己増殖活動を行わないマルウェア全般を指すような使われかたをしている。このカテゴリの小分類に含まれるスパイウェア以外の例として「バックドア」や「ダウンローダ」がある。
ワーム	自己増殖することに特化している。大発生すると、その生成トラフィックにより、ネットワーク的な障害を発生させることもある。
狭義のマルウェア	ほかのファイル(exeやDLLなど)の一部を改変し、その処理に変更を加えることで感染を成立させる。自己増殖機能はなく、潜伏期間が長い。

表1 マルウェアのカテゴリと感染活動



しているのだ。

認知度の高さの一方で、スパイウェア、ひいてはマルウェア全般を巡る様相はこの数年で様変わりしている。なぜならば、先に述べた「セキュリティ対策の押し売り行為」は、スパイウェアに関連した反社会的な組織の活動の1つ、と見ることもできるからだ。本稿では、これら最新動向を含む説明を行なったうえで、有効な対策を読者に提供することを目的とする。なお、本稿では広く使用されているWindowsを利用している読者を想定した内容となっている点に注意されたい。

### スパイウェアの定義と区分

まず、現在では悪意あるソフトウェア、すなわち誰かのPCに危害を加えるソフトウェア全般はマルウェアと呼ばれている。スパイウェアはマルウェアの一種である。そしてマルウェアは、近年では金銭目的のために作成されたことで、そうした換金性のある情報をPCから盗み出すことを主たる機能として持っている。したがって、スパイウェアという名称が一般に広まった当初、その定義に含まれるとされていた「『金銭目的』であることがスパイウェアの特徴の1つである」ということは、現在ではあまり意味をなさず、マルウェア全体を指すことに近くなってしまった。

スパイウェアの定義については、旧来から多くの議論がなされており、どこまでをその意味するところにするか、不明瞭なままであった点も多い。しかし昨今の検挙事案の報道状況を見ると、新聞やTVでは「感染者に気付かれないように情報を盗むマルウェア」と呼ぶことが多いようである。これに従

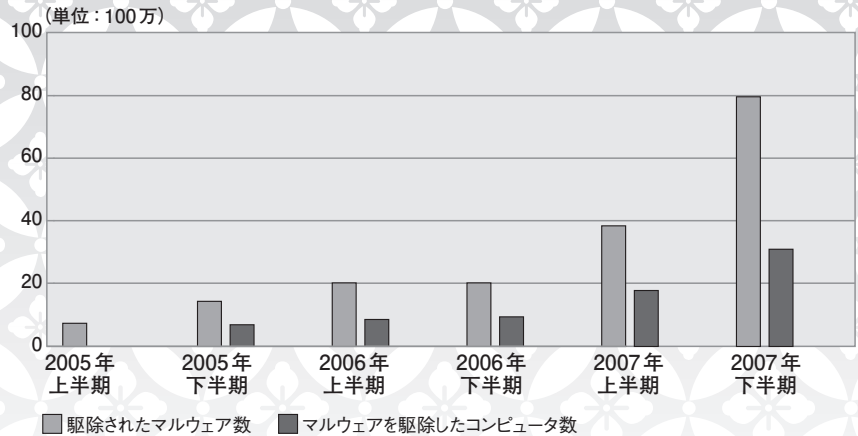


図2 マルウェアの傾向(出典: マイクロソフト)

い、本稿でのスパイウェアの定義は「自己増殖機能を持たないマルウェア(トロイの木馬)の一種であり、特定の情報を利用者にわからないように窃取するもの」とする。視覚的にわかりやすくしたものを図1に、それぞれのカテゴリの説明を表1に示す。

### スパイウェアの現況

スパイウェアの現況を知るために、いくつか統計資料を紹介したい。

まず、スパイウェアを含むマルウェア全体の傾向は図2のようになる。これは、マイクロソフトが月1回のペースで

提供している「悪意あるソフトウェアの削除ツール」によって駆除されたマルウェア数と駆除されたコンピュータ数の、2005年から2007年にかけての半期ごとのデータである。このように、全体の母数のトレンドとしては、明らかに右肩上がりの感染拡大を見せている。

では、全体の内訳を見てみよう(図3)。図中のマーキングは筆者が追加したものだが、駆除数の上位5つのうち、実に2つがスパイウェアなのである。したがって、全体的な傾向として、スパイウェア感染の数は依然として多く、また伸びてきている、といってよいのではないだろうか。

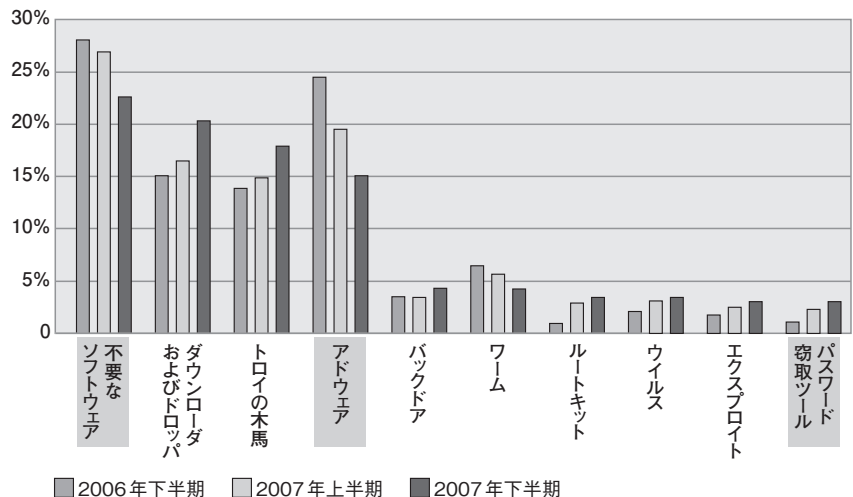


図3 LiveOneCareによる駆除数の内訳(出典: マイクロソフト)