Spyware: A View from the (Online) Street

スパイウェア:(インターネット)大衆の観点から

By Robin Poston, Thomas F. Stafford, and Amy Hennington

近年実施された“大衆レベル”のユーザを対象としたアメリカオンライン社の調査では，スパイウェアの蔓延を許しているのにもかかわらず，問題解決のための具体的な行動を起こす意思がないことが明らかとなった.

1 億人以上のインターネット利用者が，Lavasoft 社が無料で提供するアンチスパイウェアをダウンロードしている[2]ことからもわかるように，最近，アンチスパイウェアソフトウェアの利用が増えている．マイクロソフトを含めて著名な会社の中には，スパイウェアに関する問題に取り組み始めた会社もある．マイクロソフト社では，現在，ウインドウズユーザを対象として，自社のアンチスパイウェアソフトウェアのベータ版をダウンロードできるようにしている．しかしながら，米ガートナー社の調査では，スパイウェアの蔓延を最小化させるために，効果的で積極的な対処をしている回答者は 10%しかいない[5]と報告され，米フォレスター社の調査では，55%の消費者が，スパイウェアが何なのかを知っているにもかかわらず，40%しか，アンチスパイウェアのプログラムを日常的に動かしていない[7]と報告されている．

スパイウェアの脅威の深刻さと，インターネットユーザの認識不足を背景に，いくつかの法的なイニシアティブが進んでいる．連邦取引委員会(FTC)は，スパイウェアの定義づけに重点を置いている．Safeguard Against Privacy Invasion Act(SPPIA)法案では，スパイウェアを受け取るということのコンセンサスを提示し，そして特にスパイウェアが何であるかを定義しようとしている．そして，Software Principles Yielding Better Levels of Consumer Knowledge (SPYBLOCK)法案では，すべてのプログラムは，ユーザの意図どおりにインストールされるように動作しなければならないという要求を制定している[8,9,10]．したがって，アンチスパイウェアがどんどん利用できるようになるにつれて，現在のマスコミ報道はスパイウェアに対してより議論するようになり，さらに，より多くの法的なイニシアティブが導入されるようになる．

スパイウェアの問題に対する注目度が増す中で，インターネットユーザがセキュリティ脅威の本質を理解し，スパイウェアに対抗する行動を起こすことが求められている．脅威に対するユーザの認知度を評価するために，AOL 社は．スパイウェアに関するユーザの認知度や，スパイウェア対策の必要性を調べる調査を行った．調査は，1006 人の AOL ユーザの回答によって行われた．AOL ユーザの回答から，スパイウェアの認知度，スパイウェアの仕組みに対する知識，スパイウェア問題を解決しようとする姿勢，アンチスパイウェアによる対策に対する投資意欲に関して，貴重な見識を見出すことができた．

スパイウェアの認知と理解

調査では，ほとんどのユーザはスパイウェアをコンピュータのセキュリティ脅威として認知していることがわかった．回答者は，「以下にあげた脅威のうち，（もしあれば）どれを知っていますか？」という質問に対し，12 種

この調査から得られる最も重要なポイントは，おそらく，スパイウェア対策ソフト市場へ参入しようとする会社が参入について再考したくなるかも知れない点だ．

類のオンラインセキュリティ脅威のリストから選択して回答をした（図参照）．さまざまな脅威が現れているが，スパイウェアは 74.9%のユーザが認知していると答え，ウイルス，スパムに続き 3 番目によく知られていた．ほとんど同数の 74.2%の回答者が，スパイウェアは個人的な脅威になると認めていた．しかし，脅威に関する高い認識と知覚は，脅威の理解とは同一ではない．「スパイウェアはコンピュータに何をしますか？」という質問に対し，セキュリティ脅威によって引き起こされる特定の危険を実際に理解しているのは，回答者のうち 49.8%にすぎなかった．

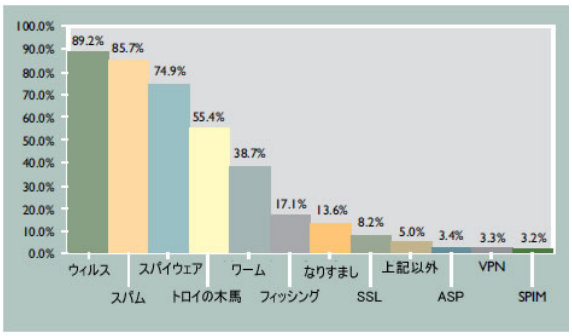

図 1 オンラインセキュリティ脅威のユーザ認知の割合

スパイウェア対策を利用する動機　ほとんどのユーザがスパイウェアを知っているにもかかわらず，多くのユーザは，スパイウェアによって引き起こされる問題を完全に理解していないようだ．そして，彼らは，これらの問題に対してどう対処したらよいのか，もしくは単純にどのような選択肢をとればよいのかを知らない．スパイウェア対策を講じていないユーザの，アンチスパイウェアソフトウェアのインストール予定に関する回答を，表 1 に示す．おおよそ 28%の回答者は，スパイウェア対策ソフトを利用しているのか否かを知らなかった．この数字は，スパイウェア対策ソフトをまったく利用していないと答えた回答者の比率(26.6%)と類似したものである．

スパイウェア対策ソフトを利用していないユーザ，もしくは利用したとしてもそれを知らないユーザを対象として，それに続く 2 つの質問に答えてもらった．この 2 つの質問は，スパイウェアに対しての安心感，そしてスパイウェア対策ソフトウェアのインストールへの関心度に関する質問である．「スパイウェア対策ソフトウェアをあなたのコンピュータにインストールすることで，どれくらいの安心感を得ることができますか？」という質問に対し，多くの回答者は安心であると答え，63.9%のユーザはこの考えは，適度な安心感を得るための最低限の方法であると答えていた．また，「あなたのコンピュータにスパイウェア対策ソフトウェアをインストールすることにどの程度関心がありますか？」という質問に対し，62.5%のユーザは，少なくとも何らかの関心を持っていると答えた．しかしながら，ユーザはインストールをしようとしない．表 1 では，70～74%の回答者が対策をとりたい考えているが，直ちにそれを行おうと思ってはいない．

アンチスパイウェア導入のための出費に対する意思　AOL 社で提供されているアンチスパイウェアサービスに，どの程度登録する意思がありますか？という質問に対し，ユーザの大多数(86.9%)が，以下の 3 つのいずれかで回答をしている．

必ず登録する
おそらく登録する
少なくとも ISP から提供されるスパイウェア対策ソフトウェアを登録するであろう．

しかし，これらのユーザのうち 44.8%が，実際にアンチスパイウェア対策サービスの登録が有償であった場合に興味があるかないかという点に関して，回答は要領を得ないものであった．12%のユーザしか，必ず登録すると

表 1 スパイウェア対策ソフトのインストールに関してのユーザの意思

あなたはスパイウェア対策ソフトインストールしていますか				
		いいえ	不明	合計
“いいえ”と答えた場合のみ，以下の質問に答えてください				452 (45%)
スパイウェア対策ソフトウェアインストール状況	現在インストールしているところである	7 (3%)	7 (2%)	14 (1%)
	インストール予定である	28 (10%)	29 (10%)	57 (6%)
	インストールする気はあるが，今すぐではない	187 (70%)	211 (74%)	398 (40%)
	インストールする気はない	46 (17%)	39 (14%)	85 (8%)
		268 (100%)	286 (100%)	554 (55%)
合計		268 (27%)	286 (28%)	1006 (100%)

答えなかった．AOL 社のスパイウェアサービスをどの程度，登録する意思があるかという質問に対しての回答の詳細を，表２A に示す．

1006 人の回答者は無作為に 755 人と 251 人のグループに分けられ，755 人のグループはスパイウェア対策サービスが有償だった場合，登録する意思があるのかについて答え，251 人のグループは，無償だった場合登録する意思があるのかについて答えた．アンチスパイウェアに投資する意思があるか否かの質問に対する答えを元に，さらに掘り下げた質問をした結果を表２B に示す．有償か無償かの違いで，登録する意思の程度に興味深い違いがある．実際，無償サービスだった場合，69%のユーザは必ず登録すると答えているのに対し，サービス料金として月々わずかな料金をインターネット利用料金の中に含ませた場合， 8.6%のユーザしか必ず登録すると答えていない．

産業界へのインパクト　この調査から得られる最も重要なポイントは，おそらく， スパイウェア対策ソフト市場へ参入しようとする企業がその参入について再考したくなるかも知れない点である．これは，スパイウェア対策機能を普通のセキュリティソフトウェアの一機能として追加する企業に比べて顕著となるだろう． 2004 年に，米ガートナー社は，良く知られているインタネットセキュリティソフトウェアや，アンチウイルスパッケージへのアンチスパイウェア機能搭載の遅れにより，単独のスパイウェアソフトウェアパッケージの需要が一時的に発生するであろうと予測した．しかし，この一時的な需要は，おそらく 2005 年以降までは続かないであろうとも予測した[6]．本稿で紹介されているデータによれば，インターネットユーザが，スパイウェア対策に特化した，スパイウェア対策単独の商品買うことはほとんど期待できないように見える．逆に，スパイウェア対策は，既存のインターネットサービスからの差別化の機能として提供されることを強く望まれるという指摘がある．

スパイウェアを潜在的なセキュリティ脅威として，インターネットユーザに一般的に認知されているという事実にもかかわらず，彼らは，市販されている解決策への投資に強い意欲がないように見える．AOL では，メインページであるログインページにおいて，アンチスパイウェアのソフトウェアを無料でダウンロードできるようにしている．そして，スパイウェア対策の現在の市場は，既存の商業インターネットサービスとの差別化のための，付加価値機能として存在しているように見える．

ユーザインパクト　AOL ユーザは，概して「ごく普通の」インターネットユーザとされている．ISP が市場を開拓しているので，ISP は，インターネットアクセスサービスの市場を的確に表現する傾向がある． AOL ユーザは，それなりに大衆ユーザの集団を表現している．AOL ユーザを対象とした以前の調査で，自分のインターネットの経験レベルはどの程度であると評価するかという質問に対して，参加者の 23%が自分のことを「ハイエンドな初心者」と評価しているのに対して，参加者の 35%が，自分のことを「初心者」として評価している[1]．したがって，インターネットサービスの基本となるユーザは，次に示すような行動を示す．インターネット大衆ユーザは，スパイウェアは問題であると認知しており，その問題から自分自身を防護したいと考えているが，対処するだけのスキルが不足していたり，スパイウェアのようなコンピュータセキュリティに関する脅威の重大性に

対する認識が不足していたりするせいで，彼らは自分を保護するために積極的な行動を起こさない．特にお金がかかる場合は，なおさらである．

表 2 AOL スパイウェア対策サービスへのユーザの登録

パネルA. AOLスパイウェアサービスに登録しますか？

	人数	割合	割合の積算
必ず登録する	123	12.2%	12.2%
おそらく登録する	301	29.9%	42.1%
登録するかどうかわからない	451	44.8%	86.9%
おそらく登録しない	96	9.5%	96.4%
絶対登録しない	35	3.5%	100.0%
合計	1006	100.0%	

パネルB. スパイウェア対策サービスが有償だった場合，もしくは無償だった場合，スパイウェア対策サービスに登録しますか？*

	有償だった場合	割合	無償だった場合	割合
必ず登録する	65	8.6%	174	69.3%
おそらく登録する	169	22.4%	47	18.7%
登録するかどうかわからない	249	33.0%	26	10.4%
おそらく登録しない	170	22.5%	2	0.8%
絶対登録しない	102	13.5%	2	0.8%
合計	755	100.0%	251	100.0%

* 回答者1006人のうち，755人には有償だった場合を回答してもらい，残る251人には無償だった場合を回答してもらった．

新しい AOL 社のスパイウェア対策サービスは，相当な額の独立した収入源が確保できる単独の商品としてではなく，セキュリティ強化のための付加価値サービスとして，評価されているようだ．AOL 社のスパイウェア対策機能強化のような，サービス提供が評価される限りでは，現在のサービスの強化として，もっとも適応しているように見える．この種のアドオンサービスを提供する AOL 社のような会社にとってもっとも大きな価値は，定期利用料よる売り上げを通して新しい収入源を開拓する動きと対立して，資本主義の競争においての優位性を維持することであろう．それゆえ，AOL 社はアンチスパイウェアソフトウェアのフリーダウンロードを勧めるだけではなく，アンチスパイウェア機能をユーザインターフェースに組み込む作業を継続していくべきである．さらに，同時に，スパイウェア脅威に対する積極的な対策を継続することの重大さを強調していくべきである．知識のあるインターネットユーザの中には，スパイウェアの脅威は理解しているが，この脅威に対抗した積極的な対策手段が必要であることを教えられなければならないユーザも存在する．アンチスパイウェアソフトウェアを発売するソフトウェア会社は，大衆レベルのユーザに対してのヘルプ機能に焦点を当てるべきである．ヘルプ機能とは，不要なスパイウェアの作用に対しての対処が緊急性を要することを理解させたり，自分を守るためにとるべき手順や，使うべきツールを教えたりすることが含まれる．

文献

1. America Online/National Cyber Security Alliance. AOL/NCSA online safety study. (Oct. 2004); www.staysafeonline.info/news/safety_ study_v04.pdf (accessed Apr. 13, 2005).
2. Beith, M. Spyware vs. anti-spyware. *Newsweek 1* (Jan. 2005), 30.
3. Earthlink. Most dangerous types of spyware increasing, states SpyAudit survey. (Feb. 2, 2005); www.earthlink.net/spyaudit/press/ (accessed Apr. 6, 2005).
4. Federal Trade Commission. Complaint for injunction and other equitable relief. (Oct. 2004); www.ftc.gov/os/caselist/0423142/041012comp0423142.pdf.
5. Girard, J. A field guide to spyware variations. Gartner Research (July 9, 2004), ID # TU-23-1453; www.gartner.com (accessed Apr. 6, 2005).

6. Leong, L. and Schroder, N. Stand-alone spyware blockers won't become separate market. Gartner Research (July 27, 2004), ID # DF-27-3133; www.gartner.com (accessed Apr. 13, 2005).
7. Lopez, M.D. and Charron, C. Spyware threat goes unchecked. Forrester Research, (Apr. 1, 2005); www.forrester.com/Research/Document/Excerpt/0,7211,36641,00.html (accessed Apr. 6, 2005).
8. Stafford, T.F. and Urbaczewski, A. Spyware: The ghost in the machine. *Commun. AIS 14*, (2004), 291–306.
9. Urbach, R.R. and Kibel, G.A. Adware/spyware: An update regarding pending litigation and legislation. *Intellectual Property & Technology Law J. 16*, 7 (2004), 12–16.
10. Volkmer, C.J. Should adware and spyware prompt Congressional action? *J. of Internet Law 7*, 11 (2004), 1–8.

Robin Poston
（rposton@memphis.edu） は，メンフィス大学のフォーゲルマン経営学部の経営情報システム分野の助手である．

Thomas F. Stafford
（tstaffor@memphis.edu）は，メンフィス大学のフォーゲルマン経営学部の経営情報システム分野の助手である．

Amy Hennington
（ahharris@memphis.edu）は，メンフィス大学のフォーゲルマン経営学部の経営情報システム分野の博士課程の学生である．

訳：平手勇宇（早稲田大学大学院・理工学研究科）