IS SPYWARE AN Internet Nuisance or Public Menace?

スパイウェアはインターネット上の迷惑行為で済むのか，それとも社会の脅威となるのか？

Qing Hu and Tamara Dinev

なぜ大多数のユーザは自分のPC上にスパイウェアが存在することを許しているのか．調査の結果によって，ユーザがスパイウェアに対してどう行動するかということに，様々な要因が影響していることを示せた．

近頃メディアがスパイウェアに注目することによって，プライバシーの侵害や，インターネットへの無料アクセスの裏に隠れたコストが露呈してきた．これらはフリーウェアやシェアウェアが関係している．たいていのスパイウェアプログラムは，アドウェアという，どちらかというと良性のカテゴリのものである．アドウェアとは，ユーザのWebサーフィンの履歴によって目的のポップアップ広告を表示するものである．それに対して，悪質なスパイウェアは，ユーザのキーストロークを記録し，その情報をスパイウェアの所有者に送ってしまう．そのような情報は，正当なデータマイニングをする目的に使われるかもしれないし，IDを盗むことによってお金にからんだ犯罪に使われてしまうかもしれない．

コンピュータウイルスは，多くのユーザに恐怖を与えたり，組織に何百万ドルもの被害を与えたりする．しかし，スパイウェアは，こうしたインターネット上の悪質なソフトウェアとは異なっている．すなわち，その悲惨な結果が予測されるということとは裏腹にユーザはそんなに深刻な反応を示さない[4,10]. たいていのユーザはオンライン上のフリーウェアやシェアウェアのソフトを手に入れる代償にスパイウェアを受け入れているか，単にその存在とその結果もたらされる被害に気づいていないかである[9]．「スパイウェアを消したらネットサーフィンもファイル交換もできないよ．なんで大学側は学生自身の好きなようにコンピュータを使わせてくれないのさ．学校のセキュリティチームの方がスパイウェアよりもよっぽど迷惑さ.」と，キャンパス内からスパイウェアサーバへのアクセスを制限することを決めた大学に対して，ある学生は語っていた．

スパイウェアは，コンピュータウイルスよりも妨害や被害が少ないというわけでは決してない．かの有名なウイルス，「I Love You」のようなウイルスは，企業のネットワークやインターネット全体に深刻な混乱をもたらしたが，スパイウェアも法人個人問わず同等の被害を引き起こす可能性がある[10]．最悪のシナリオはおそらくこうだ．社外秘の顧客データが社内のコンピュータから漏洩することによって，法規制の遵守という努力が無駄になり，法の脆弱性が広がってしまう[6].

さらに言えば，スパイウェアに侵されたシステムからスパイウェアを取り除くのは，コンピュータウイルスを取り除くことよりも困難である．多くの場合，スパイウェアの侵入を防ぐのはウイルスのそれよりも困難であり，スパイウェアを除去するのはウイルスの除去よりも複雑である．企業のコンピュータに普及している多くのウイルス対策ソフトは

スパイウェアを検知できないし[1]，多くのスパイウェアは消去されても自身を自動的に再インストールする機能を持っている．きちんと除去するためには，対スパイウェアの特別なソフトウェアが必要なのである．

コンピュータの知識			
階級	全体 (%) N=229	MIS/CS(%) N=140	ビジネス(%) N=74
基礎レベル	48.4	31.4	80.8
上級レベル	26.7	31.4	19.2
開発者レベル	24.9	37.1	0
スパイウェアの認識			
聞いたことがない	2.3	2.2	2.7
詳細は知らない	12.2	7.2	20.3
やるべきことが分からない	23.5	19.4	31.1
やるべきことが分かる	17.2	14.4	21.6
完全に認識しており、防御法も分かる	44.8	56.8	24.3

表1．コンピュータの知識とスパイウェアの認識

さて，インターネットユーザのスパイウェアに対しての行動が十分でないというのはどう説明するか．たいていのユーザがスパイウェアを気にも留めていないというのは事実であろうか．スパイウェアに対するユーザの行動を理解するために，まずはユーザの態度と，何がその態度に影響するかを理解しなければならない[10]．スパイウェアからの防衛とスパイウェア除去に対する態度とその後に続く行動について明らかにするために，我々はスパイウェアについての調査報告を行う．

調査手法について

インターネットユーザがスパイウェアに対して明らかに消極的であるということを理解するために，合衆国南東に位置するある州立大学の情報学（IS）の専門家と学生の調査を行った．調査法は，Azjen 氏が考案した「計画行動理論（TPB: Theory of Planned Behavior）」という理論モデルを参考にした．TPB は，人の行動は対象行動を実行しようとする意図によって決まるものである，という考えに基づいた理論である．行動意図は次の 3 つの要素によって決定される．行動に対する態度（ATB: Attitude Toward the Behavior），主観的規範（SN: Subjective Norm），知覚行動制御性（PBC: Perceived Behavioral Control）である．ATB は，対象行動を実行することが良いことか悪いことかの判断力を参照する．SN は，当該行動を実行するかしないかを決める社会的圧力の認知のことである．そして PBC は，その行動を実行することが容易か否かを知覚する力を参照する．図 1 に[1]で提案されている TPB の関係図を示す．

行動	全体 (%) N=229	MIS/CS (%) N=140	ビジネス専攻 (%) N=74
しない	12.2	7.9	20.3
たまに	16.7	15.7	18.9
時々	23.9	25.7	21.6
たいてい	32.9	34.3	27.0
常に	14.4	16.4	12.2

表2．スパイウェアに対する行動（除去とコンピュータの防衛）

スパイウェア独特の背景を考慮し，行動意図を決定する 3 つの要素に影響を与える，いくつかの要素を導入した．その中で最も重要な要素は認識である．しかし，認識の重要性を指摘する研究はわずかしかない．これは，IT の導入は個人レベルの話というよりも職場レベルの話であり，認識というのは技術受容（technology acceptance）の文献で語られるような組織の初期行動ではなく，各ユーザの初期行動に関連しているた

[1] この状況は将来変化するかもしれない．例えば，McAfee 社は増加しているスパイウェアに対する防衛手段を，企業向けのアンチウイルス製品に年内には導入すると最近発表した．

ユーザがスパイウェアに対して行動を起こすかどうかは，そのタスクを実行しようとする意図があるか，あるいは手段（ツールやスキル）を持っているか，によるところが大きい．意図は，そのようなタスクを実行しようという態度や，（自分の社会グループの仲間や影響力の大きい人物からの）社会的圧力，関連する手段によって決定される．

めである．例えば，社会学において政治的・社会的な不正行為と戦う時，あるいは医学において病気から身を守る時には，人々を立ち上がらせ認識してもらうのが重要であるということが広く知られている．既存の技術が，企業や個人に利益を与えるようにできているのに対し，スパイウェアは「問題，脅威，病気」を抱える技術である．ゆえに，スパイウェアの研究においても技術受容の認識の重要性は考慮されるべきであるといえる．さらに私たちは，有名な技術受容モデル（TAM: Technology Acceptance Model）における2つの重要な要素を，スパイウェアとアンチスパイウェアの技術に対するユーザの態度と行動の判断材料として加えた．その要素とは，有効性の知覚と容易性の知覚である．

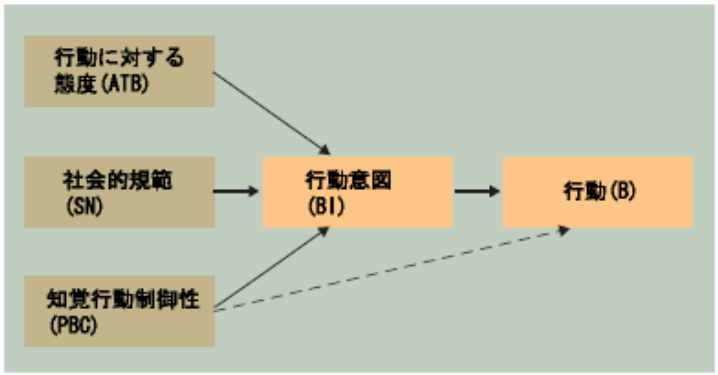

図 1. 計画行動理論（TPB）（[1]より採用）

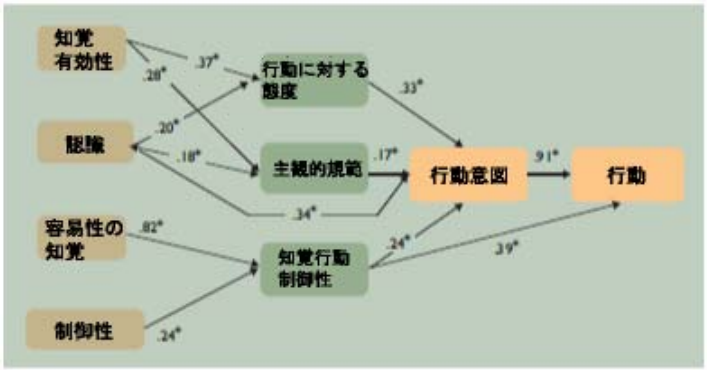

図 2. スパイウェアに対するユーザの行動の決定要素

我々は，上で説明してきた理論モデルをもとに調査手法を作り上げた．TPB と TAM の文献の内容が有効であるので，我々が独自に手法に追加した認識という要素を除いては，既存の要素を使うことにした．本手法では，まずは明確性・整合性・正当性を示すために，著者らのプログラミングクラスの学生を使って予備テストを行った．予備テストの結果を基に，手法に多少の改良を施し，結果をこの研究のための Web サイトに掲載した．我々は，授業期間中に経営情報システム（MIS）やビジネスクラスの学生に，オンライン上で質問に答えてもらった．また，大学の卒業生の情報学専門家たちにも研究に協力してくれるよう E メールを送った．3 週間超の調査の結果，オンラインで 229 人の回答が得られた．ただし，そのうちの 7 人の回答は回答不足により使えないため，サンプルから除いた．残りの回答者のうち，62%は男性，38%が女性であった．また，63%は MIS か CS の学位取得者あるいは学位取得を目指すもので，34%はビジネス関連の学位取得者あるいは学位取得を目指すもので，3%は他学問の学位取得者であった．学歴に関する情報は表 1，2 に示してある通りである．

スパイウェアというものを聞いたことがない，詳しくは知らな

いと答えた回答者が少ない（15%以下）という点は興味深い点である．もっともなことだが，この割合はMISかCSの学位取得者でない，あるいは学位取得を目指すものでない人の方が高い（23%）．しかし，AOL社の最近の調査では90%以上の回答者が，スパイウェアがどんなものかを知らないと答えており，それよりは非常に割合が低い[9].

表1, 2からは違った側面も見られる．MISかCSの学位取得者あるいは学位取得を目指している回答者は，ビジネス関連の回答者よりもスパイウェアについてずっと詳しいということが分かる．これは驚くことではない．しかし面白いことに，スパイウェアに対して実際に行動を起こした回答者の割合というのは，MISかCS関連であろうとなかろうと非常に低いのである．このことは我々の研究課題である「なぜユーザはスパイウェアに関心がないのだろうか？」という疑問を一層強める．

この疑問の答えを明かし，我々のモデルをテストするため，LISRELというソフトウェアを用いて調査結果を解析し，スパイウェアに対するユーザの行動のキーとなる判断材料を特定した．診断の統計解析結果により，調査手法の有効性とモデルの予測能力は，一貫性と有効性を持っている，ということが示された．興味深いことに，スパイウェアからコンピュータを守るためにユーザがなぜ積極的に対策をするのかということと，何がユーザをそのような方向に導くのかという，行動モデルの主要素の間には明らかに関連があった．構造方程式モデルの結果を図2に示す．図中の数字は，各要素間の関連性の強さを示す統計的な指標である．またアスタリスク（＊）は，統計値が1%レベルで有効であることを示している．

認識は，行動を起こす際のキーとなる判断材料である．認識という要素は，スパイウェアの侵入を防ぐこととスパイウェアの除去を行うことに対して，ユーザが積極的な行動を起こすための，最も重要な決定要素として現れたのは明らかである．認識はATBやSNだけではなく，防衛や消去を行おうという意図，つまりは防衛や消去を実際に行うという行動にまで直接影響を与える．この結果は，スパイウェアがユーザに加えるかもしれない損害の可能性にユーザが気付けば，自分自身を守ろうという行動に出る可能性が強いということを示している．自分のシステムがスパイウェアに侵されているとユーザが認識すれば，スパイウェアを除去しようとする可能性は高くなるだろう．AOL社が調査した「80%以上のコンピュータがなぜスパイウェアを持っているのか」ということ，また「自分のコンピュータがスパイウェアに侵されている人のうち，約90%の人がその侵食を知らない，あるいはスパイウェアがどんなものなのかを知らない」ということが，認識の欠如によるものだと説明できるだろう[9]．構造方程式モデルの中の認識は，単に「知っている」か「知らない」かの単一の区分に分けられるわけではなく，スパイウェアとアンチスパイウェア技術の知識の度合いを示すために，多彩な項目を使って測定された心理学的構築図なのだ，ということを強調したい．

有効性の知覚は，行動のためのやる気を向上させる．認識がスパイウェアに対するユーザの行動を決定する重要な要素ではあるが，我々の調査結果はこうも示している．それは，ユーザが自身のコンピュータを防御し，正常にするという行動を取ろうという良好な態度を根付かせるためには，スパイウェア対策プログラムの有効性を知覚することもまた必要に違いない，ということである．有効性の知覚（PU: Perceived Usefulness）という要素は，ATBとSNに対する態度を決定する強固で重要な要素である．なぜPUがATBに影響を与えるのかというのは直感的に分かる．しかし，SNに対するPUの影響はただちに分かることではない．社会的圧力がどのように形成され，社会グループの一員にどう影響するのかを詳しく見てみると，次のことが分かる．社会グループの一員が，ある行動が有用性および利益性を持つと信じた時に限り，その行動に関する社会的規範によってその人の行動は徐々に形成され形作られていくのである．このように，有効性の知覚は，社会的規範の構成および行動時における社会的規範の影響よりも上位に位置しなければならない．

容易性の知覚は行動までの最後のハードルである．ユーザがある技術を採用するかどうかを決める時には，容易性の知覚が重要であると，技術受容の文献では長く認められてき

家庭や企業のコンピュータへのスパイウェア侵入の猛威は，ネットワーク経済の基礎を脅かし，法や財政の広範囲に影響を及ぼす．

た．アンチスパイウェアの習慣と，そのためのツールをユーザが受け入れるか，というケースにおいても例外はないようである．我々の調査結果では，容易性に関連した 2 つの要素，アンチスパイウェアプログラムの容易性の知覚（PEOU: Perceived of Ease Of Use）とスパイウェアに対しての行動を起こすときの知覚制御（PC: Perceived Controllability）が，知覚行動制御（PBC: Perceived Behavior Control）の決定要素となると示している．PBC は行動の容易性の知覚と定義されており，それは予想される障害や支障，過去の経験が反映されると想定されるので，PEOU がなぜ決定要素のうちの 1 つなのかが理解できる．さらに言えば，知覚制御の度合いの高さは確信の度合いの高さを示しており，それが高ければ高いほど知覚行動制御性の度合いも高くなる．

スパイウェアの場合，もしユーザが感染したコンピュータを正常にするためのアンチスパイウェアプログラムの使い方を知っていれば，またスパイウェアの侵食を防ぐためにコンピュータの設定の経験があれば，そのような行動に出る時は高度の制御が可能であろう．一方，スパイウェアに対して有利な行動を取ろうとする態度があり，そうしようと思っていたとしても，コンピュータを正常にできないという恐怖感，スパイウェアによって引き起こされている現状よりも，システムを変更することによってより深刻な事態になってしまうかもしれないという恐怖感から，行動に出ることができないかもしれない．なぜスパイウェアの存在に気づいている回答者の割合が，スパイウェアに対して行動を起こす回答者の割合よりもずっと高いのか，ということがこのことによって説明できるであろう．

態度，主観的規範，知覚行動制御から行動へ．行動に対する態度や主観的規範が良好であればあるほど，また PBC が高くなるほど，個人が検討中の行動をしようとする意図が強くなる，と TPB では断定している[1]．スパイウェアの状況を見ると，我々の解析結果はこの理論をサポートする強力な証拠となる．図 1 で示した本理論の関係はすべて構造方程式モデルの資料でサポートされているものである．ユーザがスパイウェアに対して行動を起こすかどうかは，そのタスクを実行しようとする意図があるか，あるいは手段（ツールやスキル）を持っているか，によるところが大きい，ということが調査結果によって示される．意図は，そのようなタスクを実行しようという態度や，（自分の社会グループの仲間や影響力の大きい人物からの）社会的圧力，関連する手段によって決定される．結局，それはキーとなる 4 つの決定要素にまで帰着する．その要素とは，スパイウェアの認識，知覚行動有効性，知覚行動制御性（ツールやスキル，経験），知覚行動容易性のことである．

結論

家庭や企業のコンピュータへのスパイウェア侵入の猛威は，ネットワーク経済の基礎を脅かし，法や財政の広範囲に影響を及ぼす．しかし，多くのコンピュータユーザは現状に甘んじており，意図的にしろそうでないにしろ，スパイウェアとその所有者によるプライバシーの侵害をあからさまに許しているように見える．

我々の調査によると，たいていの場合そのような行動は合理的な決定から来るものではなく，インターネット時代におけるプライバシーとセキュリティの密接な関係を理解していないことによるものである．それは本質的に単純な問題にまで下げることができる．それは，その存在を知らずに，どうやって問題を解決するのか，ということである．

スパイウェアはもはやインターネット上だけの問題ではない．控えめに言っても，スパイウェアはマーケティング従事者による国民の信頼を手玉にとったものである．最悪の場合，個人法人問わず財政に損害を与えたり，法的に何か影響があったりするようなコンピュータ犯罪となる．スパイウェアに打ち勝つ最も有効な方法は，まずは一般ユーザに教育を施し，スパイウェアとその結果もたらされ

る脅威を知ってもらうことである．そして次に防衛と除去のためのツールを与え，訓練をすることである．いくつかの主要なシステムやウイルス対策ソフト会社が，対スパイウェアのプログラムを製品に組み込むことで，人々に自信を持たせ，今日のコンピュータウイルスの認識と制御と同じくらいのレベルまで，スパイウェアの抑制を進めることができるであろう．

文献

1. Ajzen, I. Attitudes, *Personality, and Behavior*. The Dorsey Press, Chicago, IL, 1988.
2. Cha, A.E. Computer users face new scourge. *Washington Post* (Oct.10, 2004).
3. Davis, F.D. Perceived usefulness, perceived ease of use and user acceptance of information technology. *MIS Q. 13,* 3, 31–40.
4. Delio, M. Spyware on my machine? So what? *Wired News* (Dec. 6, 2004).
5. Gutner, T. What's lurking in your PC? *BusinessWeek* (Oct. 4, 2004).
6. Johnson, M. Spyware wake-up call. *Computerworld* (May 3, 2004).
7. Mitchell, R.L. Spyware sneaks into the desktop. *Computerworld* (May 3, 2004).
8. O'Brien, T.L. and Hansell, S. Barbarians at the digital gate. *New York Times* (Sept. 19, 2004).
9. Roberts, P. AOL survey finds rampant online threats, clueless users. *Computerworld* (Oct. 25, 2004).
10. Stafford, T.F. and Urbaczewski, A. Spyware: The ghost in the machine. *Commun. AIS 14* (2004), 291–306.
11. Vijayan, J. Microsoft acquires antispyware vendor giant. *Computerworld*(Dec. 16, 2004).

Qing Hu （qhu@fau.edu） は，フロリダ州ボカラトンにある，フロリダアトランティック大学，ビジネス学部，情報技術・業務管理学科の助教授である．

Tamara Dinev （tdinev@fau.edu）は，フロリダ州ボカラトンにある，フロリダアトランティック大学，ビジネス学部，情報技術・業務管理学科の助手である．

訳：杉田秀（早稲田大学大学院・理工学研究科）