A Framework for Spyware Assessment

スパイウェア評価の枠組み

Merrill Warkentin, Xin Luo, and Gary F. Templeton

スパイウェア政策の策定は包括的な努力の成果でなければならず，スパイウェアが必ずしも悪者ではないということを反映すべきである．

情報技術社会が直面している最も挑戦的な問題の１つは，スパイウェアの脅威に対処することである．スパイウェアが個人と組織のプライバシーや生産性を脅かすようになったことから，対抗上，近年，研究や立法，さらには政策転換の動きが急激に起こっている．

全ての現象について言えることだが，適切な法令を施行する前に，社会や組織の政策立案者や，インターネットサービスの管理者や研究者のようなステークホルダーコミュニティで，定義が確立されていなければならない．本稿では，スパイウェアに関する今後の論議を導き体系づける枠組みを示すことにより，定義上の空白を無くす．そして，その枠組みの立法への適用方法を提案する．

スパイウェアの有名な定義の多くは，ユーザ（スパイウェアに潜伏されているマシンを持つ個人）に好ましくない影響[6]をもたらす不正[4]なインターネット通信[1,3]に焦点を当てるものである．この観点には２つの問題点がある．第一の問題は，我々はスパイウェアが持つ暗黙性への対策がますます難しくなっている点である．特にスパイウェアの多くは、他のセットになっているプログラムをインストールする直前のエンドユーザライセンス同意（EULAs）の中にスパイウェアのインストールの同意を忍ばせ，ユーザがスパイウェアを同時にインストールする機会を伺うという，ユーザにわかりにくいアプローチをとる．しかし，一般にユーザは，自分の行動を監視するソフトウェアをインストールしてしまうことには気づかずに EULAs を承諾するので，それは自覚のない同意であり，真のインフォームドコンセントではない．

第二の問題点は，スパイウェアは，多くの定義が暗に意味するように，必ずしもエンドユーザに損害を与えるとは限らない[9]ことである．つまり，遠隔ユーザ（スパイウェアの供給者）が，エンドユーザに損害を与えない方法でエンドユーザの行動を監視してもよいと考える．この理由から，我々はより様々なスパイウェアを説明するために，より包括的な考えを提案することにする．

ここで我々はスパイウェアを,「クライアントの行動を監視し，集めたデータを遠隔マシンに送るクライアント側のソフトウェア」と定義する．（後で，我々は４つの明確な基準を作り，より優れた特性を使ってスパイウェアを定義する.）この定義は，ソフトウェアがエンドユーザ（クライアントを使う個人）に知られることなく存在することを意味していないし，またスパイウェアから利益を得るエンドユーザを除外しない．

スパイウェアはクライアント側に常駐している．というのも，サーバサイドでのみ検出が可能なユーザ活動記録は，ユーザが自ら送信してきたものなので，その利用は合法であると言えるからである。提案する定義におけるソフトウェアで網羅できるのは，あらゆるスクリプトや実行可能なコード，あらゆるクッキー，クッキー同様にサーバから読み取り可能なクライアント側のデータ，サーバから読み取り可能な API やアプレットやソフトウェアの持つ機能などである．そのようなソフトウェアは組み込みのコンポーネントかスタ

「私にとっては結局，全ては行儀の良さということになる．つまり，私が誰かを家に招くとき，すなわちこの場合は私のコンピュータに招くとき，私は頼んだ時に動いて，頼んだ時に出て行ってくれることを期待しているのだ」

—CIIFF STEARNS(R-FL),

スパイ活動改正案を起草する理由について

ンドアロンアプリケーションのどちらかであることがある．監視される行動には，キーストロークやウェブサイトの閲覧や画像のダウンロードやデータの保存が含まれることもある．

この定義の下では，組織の内部で行われ，遠隔から行わない監視をスパイウェアとはみなさない．さらに，ソフトウェアコンポーネントがスパイウェアに分類されるためには，クライアント側のソフトウェアが存在しなければならない．例えば，レジでお得意様カードによって購入習慣を観察するために食料雑貨店主によって使われるソフトウェアはスパイウェアではない．けれども，もし買物客がオンライン食料雑貨店主を訪問し，クライアントに在住しているソフトウェアがユーザのクリック履歴を観察するために使われるなら，食料雑貨店主はスパイウェアを雇っていることになる．

提案の枠組み

これまで進められてきたスパイウェアの発見とその対策をサポートするため，我々は２つの重要な事柄に基づいた枠組みを提案する．その２つとはすなわち、ユーザの同意とユーザへの影響である。同意とは，ユーザがソフトウェアのインストールと実行を許可することを認めることを意味する．影響とは，コンポーネントがエンドユーザに有益な機能を提供することを意味する．同意と影響は本来，二値（１か０か）のものではないことに注意してほしい．同意と影響は連続値なのである．ユーザとソフトウェアとが互いに影響し合うとき，同意の度合いと影響の度合いには変化が見られる．例えば，ユーザの多くはクッキーをあいまいにしか理解せず，状況に応じてクッキーの理解が変わってしまう．この２つの観点をもとにした付随の図１は，スパイウェアの４つの明確な特徴付けを詳しく述べるものである．

第１に，Overt Provider とはユーザがその常駐に同意し，好ましい影響を受けるスパイウェアの一種である．Overt Provider は，アドウェアの普及を目的としたものである．アドウェアとは、電子商取引会社がユーザの行動の監視や解析をして，ビジネスプロモーションや広告に用いるものである．例えば，アドウェアは普及したスパイウェアの一種で，オンライン上の行動を監視し，精選品に応じた広告を出したりする．それは一般にＰ２Ｐや他のフリーのソフトウェアにバンドルされて蔓延する．

このようなＧＵＩＤを使用するスパイウェア

スパイウェアによる影響にも好ましい面があるため，ユーザは Overt Provider の使用の規制を嫌がる可能性がある．実際に Overt Provider の多くはユーザにとってある程度有用で便利なものである．スパイウェアのもっと有用な側面の１つは，よりユーザに役立つように，相互リンクされたウェブサイトのネットワークで共有される顧客情報（名前と住所と好みと連絡先など）を集めるために，世界で一つしか存在しない識別子（ＧＵＩＤ）を使用していることである．そして，個々のユーザはＧＵＩＤにより一意に識別される．は，ユーザにパスワードを付けさせ，例えば

地域情報や地域の天気，そしてユーザが望む製品情報などを提供する．

例えば，WhenU.com はアドウェアの会社で，ユーザが好むキーワードとＵＲＬと検索用語を分析して，顧客に掘り出し物とオンライン割引に関する情報を提供している．同様に，クライアント側にあるスパイウェアは，アプリケーションが応答しなくなった時などコンピュータ利用上の問題をユーザが解決するのを手助けすることができる．マイクロソフト社のエラー報告サービスはソフトウェアに起こる問題の原因を究明するのを手助けするために，マシンの構成とネットワーク接続に関するデータを集め，そのデータをオンラインクラッシュ分析サーバーに送り，その結果，サービスパッチが整備され利用できるようになる．（oca.microsoft.com/en/dcp20.asp を参照）

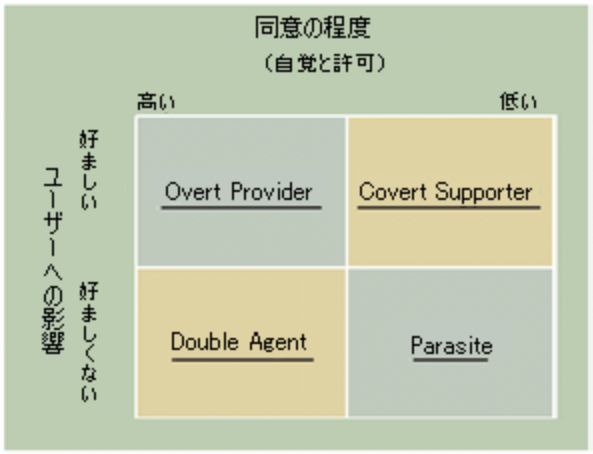

図１．スパイウェアの枠組み

第２に，Double Agent はスパイウェアの中でも特にひねくれた一種である．これはユーザの同意を得るが，エンドユーザに損害を与える．このスパイウェアは損害を与える情報（例えば，わいせつ文書や性能を低下させる設定やウイルス）を植え付けて，問題に対処したり不愉快なコンポーネントを取り除こうとするユーザにサービスの宣伝をする，しかしそのサービスはトロイの木馬のような好ましくない影響を広めるものである．このシナリオにはユーザとスパイウェアの供給者の間のひどい関係がある．この場合にはユーザはスパイウェアのインストールに気づかないかもしれないし，スパイウェアは様々な方法でインストールできるのである．例えば，他のアプリケーションとバンドルする方法や，他のプログラムのインストールの選択をはずすオプションを与えない方法や，冗長な EULA の同意書にスパイウェアの承諾を含ませるといった方法がある．

例えば，Xupiter はポップアップ広告を出し，デフォルトのホームページを変更し，間違ってタイプされた URL や不完全な URL を会員サイトにリダイレクトし，検索要求を商標のない検索サイトにリダイレクトする．いったん常駐すると，このソフトウェアはブックマークに Xupiter のリンクを加えたり，ブラウザの設定をデフォルトに戻すのを妨害することによってさらに増進する．Xupiter には強制的なプライバシーポリシーもあって，そこには，「会社」やその共同経営者が自動更新によってプログラムの修理とアップデートとアップグレードを届けると記されている． Xupiter は，他のアプリケーションと競合する可能性があり，Xupiter はそのアプリケーションを特定し，その会社は，可能ならいつでもその障害を解決する，とユーザはアドバイスされている。Xupiter には，影響下にあるコンピュータ上に，賭博ゲームのようなプログラムをダウンロードするバージョンもある[4].

第３に，Covert Supporter は好ましい影響を与える見えないソフトウェアである．例えば，helpdesk personnel は一般に，ネットワーク監視ソフトウェアによって遠隔からクライアントのスクリーンを監視することによってユーザを支援する．たいていのネットワークミドルウェアは，様々な営利目的のために管理者がネットワークトラヒックを監視したり観察するのを許可していて，侵入探知を行ったり会社のインターネットサービス利用規約の順守を確保したりする． Covert Supporter はまた，主にオンライン性能を高める目的で，ウェブサイトの閲覧やＥメールや IM コミュニケーションのようなユーザの活動を監視するように設計されているのが一般的である．

Covert Supporter の一般例はブラウザのクッキーである[7]，それは過去のユーザの行

動に基づいて，インターフェースを個人向けのものとし，ユーザに応じて製品販売を促進するポップアップ画面を出すこともある．Covert Supporter の例をもう 1 つ挙げるとComScore Network's Marketscore がある，それは無料でダウンロードできるアプリケーションであり，ネットサーフィンの速度を上げ，ウイルスから E メールを保護するものであるが，ユーザの癖を探知して産業研究のための統計データの収集もするものである．

システム性能の向上が望まれない状況もあることに注意しなければならない．特に，オンラインのわいせつ文書の流行などの危険が多くの親たちの関心事となっている．これらの危険を軽減するために，親たちは家庭のシステムにスパイウェアをインストールして遠隔から子供を監視し保護することができる．この種のスパイウェアは,ユーザ(子供)がその存在を知っていれば有効ではないだろう．

最後に，Parasite はユーザの同意を得ずに好ましくない影響を広めるスパイウェアである．ユーザの多くは，自分たちが悪意ある侵入者による遠隔からの持続的な監視下にあることに驚くのかもしれない．ユーザがあるURL を閲覧した時，ドライブバイダウンロードによって（閲覧の間，ずっと注意を払っていても）気付かないうちにスパイウェアを激増させる．このプログラムは性能を低下させるうえ，除去するのが可能な限り困難になるように設計されている．確かに，キーロガーは，慎重なユーザや組織の情報をも盗むことができるため，潜在的には最悪の種類のスパイウェアだ．

ユーザの多くは，Parasite から派生したスパイウェアについて，被害の程度と認識の難しさについて不満を言う．ユーザが（わいせつ文書のような）有罪になる情報にさらされる可能性や，ユーザの同意なしにプライバシーが侵害される可能性のために，Parasite は特にやっかいなのだ．Parasite の好ましくない影響で重大なものにはユーザと組織の利害関係の両方に与えるものがある．最もユーザに損害を与える影響にはプライバシーの侵害があり，そのプライバシーの侵害にはユーザの機密情報（例えば，銀行の口座番号や連絡先や社会保障番号）のデータ収集と記録があることがある．さらに，Parasite は攻撃を始めたり不正アクセスしたり性能を低下させるために，ユーザ名とパスワードを盗むことによって企業に影響を与える．攻撃には（重い CPU 処理とネットワークのバンド幅の占有によって）マシン性能を低下させたり，スパイウェア関連のアドレスにブラウザをリダイレクトしたり，ユーザの画面を悩ませるポップアップ広告を表示するものなどがある．

枠組みの法的規制への適用

合衆国における最近の立法活動は公共政策として基盤となるものであろう．同様に，他の国々においても，スパイウェアと定義されるある種のソフトウェアに適用するさまざまな法律を検討し制定している．尤も，普遍的に認められているスパイウェアの定義はないのだが．合衆国下院が 2004 年インターネットスパイウェア防止条例とスパイ条例を可決した．それは，コンピュータの制御をすること，ウェブブラウザのホームページを不正に改竄すること，正式な許可なしにウイルス対策ソフトの機能を無効にすること，正当と認められる範囲を超えるアクセスを故意にすること，スパイウェアの正当と認められないインストールによって損害を引き起こすこと，また秘密裏に個人情報にアクセスすることを禁止するものだった．すでに産業界の専門家はこの法律は効果がないだろうと言っている．

広義の表現が合法のソフトウェアを妨害し，電子商取引を抑制し，新たな法律上の義務を生み出すという理由で，この法律の初期の版は（合衆国の商工会議所などによって）反対された．スパイ条例は，消費者から個人の身元を確認できる情報を集める合法なソフトウェアには，選択通知と同意形態を明確に要求するものである．興味深いことにこの法律は，ユーザが非公認にインストールされたソフトウェアを持っているかどうか判断するために，同意も通知もなしにユーザのコンピュータを調べることをベンダーにも許可しているのである．

この法律の合衆国上院版は，現在検討中であり，消費者の知識をより高い水準にするソフトウェア原則条例であり，スパイ防止条例（ SPYBLOCK Act,Software Principles Yielding Better Levels of Consumer

Knowledge Act）としてよく知られていて，それはソフトウェアに以下のような特徴がある場合は厳格に公表を要求するものである．

・ユーザ情報を集めネットワークを介して第三者に送ること
・ポップアップまたは他の広告をユーザのマシンに出すこと
・例えばスパムを送るなどの処理をするためにユーザのコンピュータを乗っ取るような，ユーザがコンピュータを使って意図的にするどの処理とも関係のない目的のために，インターネットを介して第三者にメッセージやデータを送ること
・例えばユーザのブラウザの指定されたホームを自動的に変えることのような，ユーザの同意なしにユーザ設定を変更すること

（合衆国上院版と合衆国下院版は，法律となる前に，調印のため大統領に送られる「妥協法案」となってしまうことに注目してほしい．）

ユタ州はスパイウェアの法律が機能した合衆国で最初の州であり，その法律は間もなく法廷で検証されることになる．カリフォルニア，ニューヨーク，アイオワ，バージニア，そして他の州が間もなくユタの後に続くだろう．類似した欧州委員会のプライバシー要綱が 2002 年以来機能している．これらすべての法律の条例が，ソフトウェアに通知と同意と除去の容易さを求めるものである．しかし，（ユタ州の法律のように）より消費者志向であり，ソフトウェアの容認に厳格な姿勢をとるものもあれば，（カリフォルニア州の法律のように）より技術産業向けであり，法律が特定の既存の慣例を非合法化することを懸念するものもある．

提案する枠組みはスパイウェアの法律にもっと包括的な観点が強く必要であることを示すために用いることができる．我々は，効果的な政策規制（法律や企業の政策）を起草する際，そのあいまいさを，枠組みによって軽減することができると強く思う．本稿で述べたこれまでの政策，法律，そしてスパイウェア対策ソフトにおいては，同意と影響に対して十分に議論されておらず，本研究はスパイウェアの定義と記述を確立するものであるといえる．

どうして好ましい影響と好ましくない影響の違いが重要なのだろうか？立法府議員が明瞭なスパイウェアの定義無しに法律を制定すれば意図しない結果が起こる可能性がある．団体の合法的なネットワーク監視を違法なものとする法律や規則が書かれるかもしれない．行動やユーザの身元を追跡するクッキー全てを悪意のあるスパイウェアと十把一絡げにすることによってあいまいさが生まれる．我々は以下のような例を述べ，同意と影響が連続値であることを念頭に一連のスパイウェアの種類についてのより正確な認識を示す．

・クッキーはショッピングカートアプリケーションや個人を特定する手助けをするために，ネットスケープ社のソフトウェア技術者である Lou Montulli 氏によって考案された．これは一般的に使われているソフトウェアであり，何百万ものインターネットユーザに大きな利益をもたらすものである（ユーザの多くがクッキーの機能を無効にすると落胆する．これは，多くのメディアサイトに再ログインするのに再度パスワードを入力しな

どうして好ましい影響と好ましくない影響の違いが

重要なのだろうか？

立法府議員が明瞭なスパイウェアの定義無しに法律を制定すれば，
意図しない結果が起こる可能性がある．

ければならないからである．また，もはやお気に入りのウェブサイトから本や他の製品を買えないことに気付く)．

・Lavasoft Ad-Aware や Spybot Search や Destroy のような主要なスパイウェア対策製品が様々な合法的な製品をスパイウェアとして分類してきた．これらは ComScore Networks 社の Marketscore のような「リサーチウェア」と呼ばれる新しいウェブベースの製品区分を含み，Marketscore は合衆国で 100 万台以上の PC にインストールされている．リサーチウェアは数多くの有名な会社や大学やメディア支局に急速に採用されてきている．ComScore Networks 社と他のリサーチウェアの会社と産業界や学究的世界やメディアにおけるその顧客たちが関心を寄せていることは，たとえ自分のアプリケーションがユーザとクライアントの両方に好ましい機能的な利益をもたらすと顧客が思っていても，人気のあるスパイウェア対策ソフトがそのアプリケーションを除去の対象としていることである．

・Lavasoft 社の Ad-Aware は，アプリケーションがユーザの最近使ったファイルやユーザがデフォルトとして使用しているフォルダを記録しているなら，スパイウェアと判別する．この機能はユーザにとって明らかに有益なものであって，信用するユーザに除去をすすめるべきものではない．

現在，コンピュータが幅広く様々な製品に用いられていることを考えると,「自分たちの技術にも影響があるのではないか」と他の様々な技術も，この問題の行方に注目している．そして，もし誤った法律が起草されれば，我々に発信者番号通知サービスを提供する電話会社は，スパイウェアのインストールで有罪になるのだろうか？提案する法律の Motor Vehicle Event Data Recorder (MVEDR)技術への影響は何だろうか？MVEDR は一般に，自動車のブラックボックスと呼ばれ，電子的にドライバーの行動を監視し衝突後に保険会社に情報を提供するために，すでに 4000 万台以上の車に取り付けられていて，一般的には所有者の自覚と同意なしで自動車に取り付けられている．

結論

政策の明確な記述は常識に基づいたものでなければならない．Rep. Cliff Stearns はスパイ行為に，罰金，ブラウザの乗っ取り，キーストロークロギング，そして閉じることのできない広告を加える改正案を起草した．彼は「私にとって，全ては結局は行儀の良さということになる．つまり，私が誰かを家に招くとき，すなわちこの場合は私のコンピュータに招くとき，私は頼んだ時に動いて出て行ってくれることを期待しているのだ」と言う．しかし，法律（と法人組織の安全政策）は好ましい機能性を保護し促進するために，言葉で表すときには非常に注意を払わなければならない．

本研究の第一の貢献は定義を考えることである．Stafford 氏と Urbaczewski 氏はスパイウェアの進んだ研究として参考文献[10]の中でアジェンダを提案している．第一段階は，インターネットサービスコミュニティによる，スパイウェア問題についての十分な研究だ．本稿が貢献しているのは，使用状況に依存するスパイウェアの一般的な定義を提案した点だ．さらに，我々はスパイウェアに関する考えを体系付けるための正確な枠組みを述べている．我々は，開発者やソフトウェア販売会社や管理者や学者やユーザなどが，この領域で仕事をうまく処理するには，枠組みを確立して使うことは避けられないと思う．さらに言えば，提案した 4 つの分類は実際には様々な状況に適用できる．

スパイウェアに対する曖昧さは，多くの会社に十分なスパイウェア対策をやめさせる原因となってしまう．スパイウェアは（P2P やウイルスやワームやクラッキングのような）他のセキュリティの脅威ほどは理解されていない．したがって，本稿の貢献の 1 つとして，世界中に配置された何千ものスパイウェアを定義して分類するための包括的な枠組みを挙げることができる．この枠組みを使えば問題を処理する適切な解決策と戦略の発展が促進されるだろう．

枠組みの第二の貢献は明確な法律や政策の基準の進歩と確立につながる可能性がある考

察である．Stafford 氏と Urbaczewski 氏[10]は我々が法的で規制的な活動をたどらなければならないことを示唆している．ここで，我々はいくつか最近の立法活動を振り返り，提案する枠組みの必要性を示した．要約すると，政策立案者は好ましい影響をもたらすスパイウェアアプリケーションにはたとえ同意がなくても，その阻止は慎重にするべきなのである．

我々はスパイウェア訴訟での最も重大な危険は「乳児を浴槽の水とともに投げ出す」（訳注：「角を矯めて牛を殺す」，「細事にこだわり大事を逸する」という意味のことわざ）であると結論付ける．法律は，正当なソフトウェアの配布を，困難にしたり不可能にすることをするのだろうか？子供のインターネットの行動を監視するために「SpyBuddy Stealth Edition」を使う親は起訴される危険を冒すことになるのだろうか？電子社会の作るウェブサイトが，共有している情報についてユーザに適切に伝えなければ有罪になるのだろうか？スパイウェアが世界的にコンピュータ利用上の問題になり続けており，我々は世界社会に研究と政策のアジェンダを作るためにこの枠組みを使うことを強く求める．

文献

1. Ames, W. Understanding spyware: Risk and sesponse. *IT pro* 6, 5 (2004), IEEE Computer Society,25-29
2. Bruening, P.J. and Steffen, M. Spyware: Technologies, issues, and policy proposals. *J. Internet Law* 7,9 (2004),3-8
3. Chow, S.S.M., Hui, L.C.K., Yui, S.M., Chow, K.P. and Lu, R.W.C.: A generic anti-spyware solution by access control list at kernel level. *J. Systems and Software* 75, 1-2 (2005),227-234
4. Delio, M. Spyware and adware rogues' gallery. *InfoWorld* 40 (2004),35-41
5. eWeek. Bill sends spyware, adware purveyors down divided paths; www.eweek.com/article2/0,1759,1708763,00.asp(accessed Apr. 20, 2005)
6. Goth, G. Spyware: Menace, nuisance, or both? *IEEE Security Privacy* 1,3 (2003),10-11
7. Hormozi, A.M. Cookies and privacy. *Information Systems Security* 13,6(2005),51-60
8. Network Associates. Network Associates Introduces McAfee AntiSpyware—Essential Protection Against Spyware for Consumers (2004);www.net-security.org/press.php?id=1973(accessed Mar. 15, 2005)
9. Sariou, S., Gribbe, S.D. and Levy, H.M. Measurement and analysis of spyware in a university environment. In Proceedings of the *ACM/USENIX Symposium on Networked Systems Design and Implementation*(San Francisco, CA, 2004).
10. Stafford, T.F. and Urbaczewski,A.Spyware: The ghost in the machine. *Commun. AIS* 14 (2004), 291-306.
11. Urbach, R.R. and Kibel, G.A. Adware/spyware: An update regarding pending litigation and legislation. *Intellectual Property Tech. Law* J. 16,7 (2004),291—306.
12. Volkmer, C. Should adware and spyware prompt congressional action? *J. Internet Law* 7,11(2004),11—18

Merril Warkentin

(mwarkentin@acm.org)はミシシッピ州立大学ビジネス工業校の経営情報システムの教授である．

Xin Luo

(XL96@msstate.edu)はミシシッピ州立大学の経営情報システムの博士過程の学生である．

Gary F. Templeton

(gtempleton@cobilan.msstate.edu)はミシシッピ州立大学の経営情報システムの助手である．

訳：柳井佳孝（早稲田大学大学院・理工学研究科）