調査報告書：スパイウェアの問題

岡　本　友（智）子

2004年12月24日～2005年1月14日，アメリカ合衆国インディアナ州ブルーミングトン市に所在するインディアナ大学ロースクール（Indiana University School of Law, Bloomington）において，研究課題「情報ネットワーク社会における個人の利益・価値相互間の調整と不法行為法の役割」に従事した。

以下，概要を挙げる。すなわち，インターネットは，あらゆる市民生活のなかで便利な道具として普及する一方で，利用者を悩ます問題も増加している。その中で，ネットワーク社会における法律問題，特に今回の調査においては，近年問題となっているスパイウェア（spyware）をとりあげ，スパイウェアの問題点，スパイウェアとプライバシー侵害，アメリカ合衆国における法的規制の動向と関連議論についての調査を行った。

スパイウェア（spyware）の問題点とは，一般にユーザが認知することなくユーザの情報を収集するソフトウェアがインストールされ，情報が収集される点にある。ユーザの許可を得ない情報の収集・利用は，ユーザのプライバシーを侵害するだけでなく，金融機関のアカウント，パスワード等が収集・悪用されれば，さらなる金銭的被害を生み出す可能性が存在する。

このようなスパイウェアが禁止・排除されることは望ましいように思われるが，ことはそう簡単ではない。そもそもスパイウェアは，単独でインストールされることは少なく，他のフリーソフトウェアと共にインストールされている。アドウェア会社は，マーケティング利用のためにポップアップ広告

を表示させるアドウェア（adware）をインストールし，それは利用者に告知していると主張している。さらに，収集・活用するユーザ情報は，マーケティング利用のためだけであり，ユーザの個人情報に関わるプライバシー侵害は犯していないと主張している。他方，フリーソフトウェアの魅力によりスパイウェアやアドウェアを容認しているユーザも多い。

しかし，ユーザには実際にどのような情報が収集されているかを技術的に認知することができず，多くのユーザを不安に落とし入れているのが，多くの調査から明らかになっている。

こうした中，連邦法レベルでは，2004年にスパイウェア規制法が検討された。10月5日に，「Securely Protect Yourself Against Cyber Trespass Act」（SPY ACT）が399対1で下院を通過したが，上院では審議未了となっている。

この「H. R. 2929」法案は，スパイウェアに関する不公正なあるいは詐欺的な慣行を禁じ，消費者から個人が特定できる情報を収集するソフトウェアに対して，事前にそのことを開示して承諾を取るよう義務付けている。法案では，ユーザがソフトウェアの使用許可を得ているかどうかを調べるために，ソフトウェア会社が通知・承諾なしにユーザのコンピュータと通信することは認めている。ネットワーク監視についても，セキュリティ，診断，技術サポート，修理，不正行為の検出・防止を目的としている限りは通知・承諾の条項を免除される。cookieも，ユーザによるWebサイトへのアクセスを可能にするためだけに使われている場合は免除される。この法案で禁じられているスパイウェア行為には，フィッシング，キー入力の内容の記録，ホームページの乗っ取り，コンピュータをシャットダウンしないと消せない広告などがある。違反者は最大300万ドルの民事罰金を科される可能性がある。

新たな第109回連邦議会の初日に，米下院のメアリー・ボノ議員はスパイウェア規制法案「H. R. 29」を再提出し，2005年早々に再度下院において審議が再開されている。なお，州法レベルでは，ユタ州をはじめカリフォルニア州等ですでに制定されている。

しかし，スパイウェア規制法の実効性，ならびにスパイウェア規制法の弊害が強く主張されている。例えば，2004年11月5日，連邦取引委員会（FTC）は，連邦議会に対し，スパイウェアは必要ではなく，既存の諸規制・法律により十分対処できるものであり，CAN-SPAM Actと同じように効果は疑問であると主張した。

これを実証するかのように，FTCは，2004年10月7日，ニュー・ハンプシャー地区の連邦地方裁判所に，スパイウェア配信業者スタンフォード・ウォレース氏（1990年代に悪質なスパマーとして知られていた）と彼が経営するSmartBot. net社・Seismic Entertainment Productions社に対して，スパイウェア（spyware）に関する不公正で詐欺的な取引行為に従事したとして，スパイウェア事件初の訴訟を提起した。ユーザのコンピュータにソフトウェアを密かにインストールし，こうしたプログラムはいったんインストールされるとWebブラウザの設定を変えてしまい，インターネットを介してユーザの動きを追跡し，ポップアップ広告を頻繁に表示させ，スパイウェア対策製品を購入するよう顧客を誘導するものである。

同年12月20日に，連邦地方裁判所は，被告らに対し，FTCに起こされた訴訟が決着するまでの間，ユーザのコンピュータにアドウェア（adware），スパイウェア（spyware）などの迷惑プログラムを密かにインストールする行為をやめるように，仮差止め命令（preliminary injunction）を下した。

FTCは，被告らがこれに同意したことを2005年1月4日に公表した。被告らは，予備審理（preliminary hearing）のスケジュールを同日まで避けており，本件について事実審理の日程は設定されていない。この命令が恒久的なものとなる。

2004年度時点では，スパイウェア（spyware）の防止は，法的規制よりも，啓蒙活動を通じた，安全なインターネットの利用とその方法を説くことにあるという議論が優勢を占めているように思われる。この主張は，法による予防・防止が効果をあげることができないことを主張していて，IT技術の開発

が先行する現代情報化社会にとって，法の役割が改めて問われている。

詳細は，拙稿「インターネット社会におけるプライバシー侵害と個人情報の保護ースパイウェア（spyware）問題を中心としてー」民商法雑誌133巻4・5合併号（2006年）参照。

[後記] 本稿は，科学研究費補助金の交付を受けた研究の成果の一部である。