IT 社会における個人情報保護

明治大学教授・弁護士

夏井高人

1 はじめに－問題状況

日本国においても民間部門及び独立行政法人のための個人情報保護法が制定され、既存の行政部門における個人情報保護法や情報公開法と併せて、個人情報保護のための法制整備が一応完了したかのような感がある。

しかし、公的部門（司法・立法・行政）のうち立法部門及び司法部門のための個人情報保護法は存在しない。また、行政部門のための個人情報保護法は、電子計算機で処理される電子化された個人情報の保護を目的とするものであって、現時点もなお大量の存在している非電子的な個人情報（紙に記録された名簿等）をカバーする法律ではない。しかも，民間部門用の個人情報保護法は、法の適用を免れるための抜け道がたくさんあるため悪徳業者にとっては何らの痛痒も感じさせない法律である一方で，他方では，主務大臣による行政監督権限行使の問題を含め，まともな事業者に対しては過重な負担を与える法律である。

そして、これらの法律は、個人のために具体的なプライバシー保護のための権利を承認するものではない。一般市民は、あいかわらず、不法行為（民法 709 条）に頼りながらプライバシー侵害に対する民事的救済を求めたり、人格権としてのプライバシー権に頼りながらプライバシー侵害の予防や排除を求めたりするしかない。つまり、一般市民は、いまだ明確かつ具体的な権利としてのプライバシー権を獲得しているとは言えない。

このような法的状況にありながら、現実社会における技術革新やビジネス手法は日々進歩し続けている。とりわけ IT 分野ではその変化が著しい。それに伴って一般市民のプライバシーが侵害される機会と規模が飛躍的に増大しつつあるというのが正しい現状認識である。

e-Japan 及び e-Japan II もプライバシー侵害の可能性を増加させる危険性がある。たとえば、これら政府の IT 政策は、ユビキタス社会の実現とそのための技術開発の促進をうたいながら、それに伴うプライバシー侵害を抑止するための方策についてはほとんど何も考慮しようとしていない。そのため、もしこのままの状態で政府の IT 政策が推進された場合、国民が気づいたときにはいつのまにか「いつでも誰でもどこでも」個人情報を取られまくられるというユビキタスなプライバシーゼロ社会になってしまっているという可能性が非常に高い。

本稿では、上記のような問題を抱えている近未来の IT 社会像を前提にして、プライバシー保護のために考えなければならない幾つかの視点を提供する。

2 現行法の解釈－プライバシー保護法ではない

現行の個人情報保護法は、プライバシー保護法ではない。あくまでも、行政機関、独立行政法人、企業などが国民や顧客の個人情報を収集する際に遵守すべき手順を定め、すでに収集した個人情報の管理・運用・処分をするための準則を定めるものであるのに過ぎない。したがって、収集されていない個々の市民の個人情報やプライバシーは、これらの法律によってカバーされているわけではない。ここで個人情報とプライバシーとを分けて記述しているのは、それが一致しない場合があるからである。

法に定める「個人情報」とは、ある情報が特定の個人に関する情報であると識別することのできる情報のみを指している。しかし、一般に、プライバシーの中には、たとえば匿名の表現行為のように具体的な特定の個人に属する情報であると識別することのできない情報が多く含まれている。また、誰にも収集されていない個人情報を収集されないで自分だけのものとしてとっておく権利は、まさにプライバシー権のコアの部分に属する権利なのであるが、そのようなタイプの情報は、個人情報保護法によって保護される情報ではない。これらのプライバシーは、民法の解釈・運用によってのみ保護され得るだけである。そして、個人の ID 情報の違法複製行為（ID 窃盗）やそのような情報の無権限使用行為については、何らの処罰法令も存在しない。

さらに，法の適用対象となるのは，主としてデータベースや名簿のように体系的に検索可能な状態となっている個人データのみである。法は，世界中にばらばらに散在しているプライバシー情報を保護対象としているのではない。

国民は、個人情報保護法の適用範囲がどれくらいなのかということとその限界とについて十分に認識・理解すべきだろう。そして，そのための知識を獲得する権利があるし、そのようにするために十分な説明を求める権利を有する。とりわけ政府は、そのような要請に対し誠実に答えるべき国家的な義務があるといえるだろう。政府と国家には、真の意味で国民のプライバシーを保護するための法制整備を更に推進すべき義務があるのである。

3 国際調和－EU2002 年プライバシー保護指令

プライバシー保護をめぐる世界の状況は，日々著しく変転し続けている。

一般に、日本国においては「日本で適用される法律のことだけ考えていればよい」というような悪しき風潮もないではない。しかし、インターネットを基盤とする IT 社会では、プライバシー問題もグロバールでボーダーレスな性質をもつものとして存在する。プライバシー侵害を防ぎ、プライバシーを守るための法的手段も国際的な調和の中で構築されなければならない。

このような観点からは、EU の 2002 年プライバシー保護指令（Directive/2002/58/EC）の存在が極めて大きい。これは、既存の個人情報保護法制定のモデルともなった EU の 1995 年個人データ保護指令（Directive/95/46/EC）を更に強化し補完するために、特に電気通信分野におけるプライバシー保護について定めるものである。

この 2002 年指令においては、個人情報の収集について必要な「事前の同意（consent)」の要件が強化され、Opt-In によるプライバシー保護の姿勢がより明確なものとされている。とりわけ、他人の通信の傍受（interception)、電子機器を利用した位置情報の収集（location

data)、商業広告用電子メールの送信などの現代的な問題に関しては詳細な条項が定められている。

日本国においては、これらの問題の多くについて十分な保護法が存在しているとはいえない。

スパムメールを規制する法律は存在するが不十分である（完全な Opt-In を採用した法律に改正すべきである。）。

通信事業者が関与する通信については傍受が禁止されるが家庭内や企業内の無線 LAN の傍受を禁止する法律はない（ただし，総務省は，来年中を目処に，暗号化された無線通信の傍受を禁止する電波法改正法案の提出を検討している。）。

位置情報に関しては，街頭の監視用モニターの多くについて，「ここにカメラが設置されている」という明確な表示がされないままに設置されている。公道において監視がなされる場合，自治体等は，それを実施していることを事前に明瞭に通知しなければならないのに，そのことが理解されていない。まして，カーナビや携帯電話その他のモバイル機器による位置情報の取得について，ユーザの位置情報を取得する際の事前同意をとり，利用目的等を告知する手段は，全くといってよいほど確立されていないで放置されているのに等しい。

しかし、プライバシー保護における国際調和というものを考えると、EU の 2002 年指令の存在は非常に大きなものであり、十分に研究を尽くした上で、その日本国への導入を積極的にかつ早急に検討すべきだろう。

4 個人情報保護のための方法－複合的な対応

上記のように，個人情報保護法は、個人情報保護のための部分的な機能を営むことしかできない。

したがって、プライバシー侵害を未然に防ぐために、プライバシー侵害が発生するメカニズムやプライバシー保護のための知識や方法等についての啓蒙普及をはかり、プライバシー保護に関する個人の自覚を促す諸施策を実施し，侵害を抑止する技術やシステムの開発・導入を強く促進し、企業や学校等の部分社会における自主的なプライバシー保護指針の策定・運用を支援するような政策論を樹立することが強く求められる。

5 新たな産業政策－プライバシー保護の義務化

e-Japan や e-Japan II に定める基本方針に従い、日本国は、IT 国家へと変貌をとげるために、その技術基盤の整備を進めてきた。その政策を遂行するために、数多くの審議会、委員会、研究会等も設置され、様々な関連研究が鋭意実施されてきた。そのこと自体には、よい結果をもたらすものが多く含まれている。たしかに、IT 社会の実現によって国民生活はより豊かなものとなってきたし、今後も IT によって享受できる利便性が大幅に向上していくことになるだろう。

しかし、これら審議会の検討結果の中では，プライバシー保護のための具体策が十分に盛り込まれているわけではない。今後は，プライバシー侵害を防止するための機能を最初

から内蔵した機器の開発を義務付け，そのような機能のない機器を開発・製造を禁止するといった思い切った政策論を検討すべきである。たとえば，一般消費者向けの取引において使用される RFID（Radio Frequency Identification）については，商品の販売と同時に RFID としての機能を喪失させる機能（deactivation function または kill function）の実装を義務付けるべきである。

６ 責任の明確化－非違行為に対する厳正な処罰

IT 社会は，基本的にボーダーレスな性質を持っており、デジタルデータ化された個人データが容易に、大量に、瞬時に複製・移転可能な存在である。そのため，仮にプライバシー侵害が発生するとすれば、その被害の大きさや影響が及ぶ範囲は、今後ますます拡張・拡大されることはあっても縮小されることはない。

プライバシー保護のために、たとえどのように効果的な対策を講じたとしても、プライバシー侵害の発生をゼロにすることはできない。それは、どの社会の中にも一定割合で悪いことを平気でやる人間が含まれており、それを防ぐ方法が存在しないからである。

名著『アウトサイダー』の著者として知られるコリン・ウイルソンは、「人間の脳は２つに分かれており、その片側には神が住んでいるが、もう一方には悪魔が住んでいる」と言っているが、これが人間の本質である。実際に、これまで発生した現実の個人情報漏洩事件の中には、自治体住民や顧客等の個人情報を取り扱い、その保護について責任を負うべき技術者や管理者などによる犯行や非違行為が多数含まれている。

そして、ルールを無視して他人のプライバシーを食い物にするような者の発生を完全に防止するための効果的な防止手段が存在するとは思われない。

したがって、そのような不埒な輩に対しては、事後的な対応として、現行法が許す可能な限りの厳重処罰を励行すべきである。

このことは、個人情報保護法に定める罰則のほか、とりわけ住民基本台帳の管理を担当する公務員に適用される国家公務員法や地方公務員法、電子メールの送受信等に関与するプロバイダに適用される電気通信事業法その他の関連法令に含まれる罰則の解釈・運用に際しても、十分に考慮されるべきである。