RIETI 政策シンポジウム資料

個人情報はだれのものか

ネットワーク社会の費用と便益

池田信夫

要旨

個人情報保護法案をめぐる論争においては、プライバシーという言葉が曖昧に使われ、議論を混乱させている。今回の法案はデータベースを規制するものであって、メディア規制ではない。ネットワーク社会では、情報の自由な流通による便益とその乱用による費用のバランスに配慮することが重要であり、一方を絶対化すべきではない。本人に個人データの差し止め権を認める今回の法案は、表現の自由を侵害するおそれが強い一方､それが迷惑行為を防止する効果は疑わしい。こうした問題を効率的に防ぐには、個人データ利用者から「迷惑料」を取って市場メカニズムを活用するしくみも考えられる。

はじめに

プライバシーという言葉にほとんど縁のなかった日本社会で、最近にわかに「個人情報保護」が叫ばれるようになった。そのきっかけは、住民基本台帳ネットワークシステム（住基ネット）の稼動にともなって「国民総背番号」がつけられることへの心理的な嫌悪感だったと思われるが、その稼動の条件となるはずだった個人情報保護法案が 2001 年の通常国会に出ると、「メディア規制」だとして強い批判を浴び、さらに 2002 年の通常国会でも継続審議となり、同年の臨時国会では廃案になって作り直すという異例の事態になった（以下「法案」というのは、このもとの法案をさす）。

個人情報の流通は、社会がネットワーク化するのにともなって不可避的に生じるものであり、電子商取引を円滑にする機能もある。そのマイナス面ばかりを強調し、個人情報を完璧に保護するためにネットワーク化が阻害され、規制が強化されるようでは本末転倒である。個人情報をめぐる論議では、こうした情報ネットワーク全体の問題をそっちのけにしてメディア規制や背番号などの個別問題ばかり論じられ、費用と便益のバランスを考えない一面的な議論が行われる傾向が強い。本稿ではこうした混乱を整理するため、事実関係を明らかにしてプライバシーの概念を法的に検討し、技術の進展をふまえて各国の制度を比較して、個人情報保護のあり方を考える。

１．プライバシーとは何か

プライバシーの定義と分類

プライバシーは、いまだに訳語がないことからもわかるように、欧米に固有の、それも 20 世紀以降の新しい概念である。個人の行動が他人から隠せないのは、貧しい社会では当たり前であり、人類の大部分は共同体という「監視社会」に生きている。プライベートな空間が仕切られている欧米的な生活のほうが特殊なのである。西欧世界でも、private という言葉は「（共同体のものを）奪う」という意味の動詞から派生したものであり、それが肯定的な意味をもつようになったのは、ごく最近のことである。

プライバシーという言葉を最初に法律用語として使った Warren-Brendeis (1890)では、この言葉は有名人がメディアのゴシップ報道から逃れて「ひとりになる権利」として提唱されており、立法的な保障が求められていたわけではない。一般にプライバシーが話題になるのは、1970 年代以降、コンピュータ・ネットワークの発達によって一般人の信用情報や顧客情報が売買されるようになってからだが、これはひとりになる権利とは異なる「個人情報を隠す権利」である。

一般には、守るべきプライバシーという私有財産があるように思われがちだが、私の個人情報は私のものだろうか。たとえば私の歯の痛みは私しか知らないが、これは秘密であって、個人情報とはいわない。法案では、個人情報は「生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの」（第 2 条）と定義されているが、その典型である住民票データは私個人のものではない。住所は自治体の決めた区画だし、私の名前も私がつけたものではない。

「私が所有することが法的に認められている」という意味でも、個人情報は私のものではない。情報に所有権を設定する（他人の利用を制限する）ことが認められている例外は、著作権法で著者が自分の生産した情報をコントロールする場合だが、個人情報の生産者は多くの場合、本人ではない。顧客情報（データベース）を生産したのは、顧客ではなく企業であり、信用情報や医療情報は本人よりも銀行や病院のほうがくわしく知っているだろう。要するに、私についての情報のほとんどは私の情報ではないのである。

法的には、私についての情報を私の（コントロールできる）情報と定義することは可能だが、この定義によれば、たとえばこの論文は私が引用した論文の筆者全員のものになり、私は彼ら全員の同意がないとこの論文を発表できないことになる。このように一つの情報に関係者全員が拒否権をもつのは「アンチコモンズ」と呼ばれる最悪の状況であり、現実にも考えられない。

ではプライバシーを守ることには、どういう便益があるだろうか。たとえば前科を隠すことが法的な権利として認められるかどうかは、世界的にみても司法的な判断は一定していない。それを保護することによって、前科者の就職は容易になるだろうが、雇用主は（たとえば彼が常習的な窃盗犯だったら）損害をこうむる可能性があるし、他の求職者は不公

正な競争によって雇用機会を失う。信用情報も金融機関にとっては重要な情報であり、医療情報も電子化して病院間で共有し、診療や検査を効率化すべきだという意見もある。

一般的にいえば、プライバシーを守るというのは「自分自身についての情報を選択的に開示して周囲の世界を操作する」(Posner 1981:p.234)ことであり、それよって情報の非対称性が生じ、本人の行動の自由度は増すが説明責任がなくなり、他人はミスリードされる。通常は、これによって逆淘汰やモラル・ハザードなどの非効率性が生じるため、契約の設計などによって非対称性を減らすことが重要な問題であり、わざわざ情報の非対称性を作り出すことは望ましくない。したがって個人情報の保護は、個人的には好ましくても社会的には有害なので、その保護は最小限度とし、保護コストは基本的に本人が負担すべきである。このようにプライバシーという言葉にはいろいろな問題が混在しており、大きくわけると次の 3 つの類型に分類できる。

A. メディアの取材・報道
B. 通信の秘密
C. コンピュータ・ネットワークにおける個人データ流通

このうち A と B は今回の法案とは関係ないが、これらがプライバシーという曖昧な言葉で一くくりにされることが混乱の原因である。このため、法案ではプライバシーという言葉は使っていない。そのもとになったのは、OECD（経済協力開発機構）が決めた個人データ保護に関するガイドラインだが、これも対象を「個人データ」に限定している。本稿でも、プライバシーという言葉にともなう混乱を避けるため、以後個人データあるいは個人情報という言葉に統一する。

個人情報保護法は「メディア規制」か

この法案に対しては、新聞協会が「メディア規制」だとして反対を表明する意見書を出した[1]。彼らは「個人情報は適法かつ適正な方法で取得されなければならない」（第 5 条）という努力規定さえ拒否し、報道機関を適用対象から全面的に除外するよう求めた。これに対して、出版社やフリージャーナリストが「自分たちも除外しろ」と主張し、どの業界を除外するかという問題ばかりが論議になり、肝心の個人情報保護のあり方は置き去りにされてしまった。

今回の法案が規制の対象とするのは「個人情報データベース等」（第 2 条の 2）であってメディアではなく、しかも義務規定や罰則は「放送機関、新聞社、通信社その他の報道機関　報道の用に供する目的」には適用されない（第 55 条）。これほど包括的にメディアを除外した個人情報保護法は世界にも例をみないが、2003 年の通常国会に提出される予定の修正案では、報道機関を完全に適用除外にすると伝えられている。このように特定の業界

[1] http://www.pressnet.or.jp/info/iken20001016.htm

に「治外法権」を認めることは、メディアは個人情報を保護しなくてもよいと法的に宣言するに等しく、誤報や過剰取材から被害者を救済する道も絶たれてしまう。読売新聞は「透明性の確保」の原則（第 8 条）が取材源の秘匿を困難にするという理由で、この規定から報道機関を除外するよう求める個人情報保護法の「修正試案」を発表したが、取材源の秘匿は現在でも法的に認められている権利ではない。

さらに重大な問題は、このメディア規制反対論が新聞・放送・出版以外のメディアを無視していることである。特に世界最大の分散型データベースである WWW (World Wide Web) は今回の法案の対象だから、ホームページは原則として「主務大臣」の監督下に置かれることになる。報道機関だけが除外されたら、だれかが新聞社のホームページと個人のホームページに同じ違法な記述があると申し立てた場合、個人が行政処分を受ける場合でも新聞社は免罪される。これは憲法に定める表現の自由に差別を持ち込むものである。

表現の自由は、報道機関の言語表現だけを対象とするものではなく、ホームページにもデータベースにもプログラムにも等しく保障されなければならない。報道機関を適用除外にするなら、少なくともホームページを持つすべての企業や個人も除外しなければ、法の下の平等に反する。データベースには規制を求める一方、報道機関には絶対的な表現の自由を求めるダブル・スタンダードは、記者クラブ的な特権意識の産物であり、合理的な根拠がない。したがって以下では、報道機関を一般の企業や個人とは区別しない。

通信の秘密と「監視社会」論

プライバシーというとき、もう一つよく話題になるのは、電話などの盗聴である。日本では通信の秘密は憲法で定められている。通信の秘密を守ることによる利益は、第三者に聞かれるのを恐れないで自由に話せることだが、逆に完全な秘話性が保証されると、犯罪者が電話で連絡することも容易になる。この費用と便益は、犯罪者を対象とする傍受を法的な手続きによって認めれば分離可能である。その範囲を具体的にどう定めるかはむずかしい問題だが、原理的には解決不可能ではない。同様の問題は、電子メールなどにも生じるが、いずれにせよ通信の傍受を全面的に否定する理由は見当たらない。これは通常では人権侵害にあたる身体の拘束が逮捕状によって合法になるのと同じである。情報を身体よりも厳重に守る理由はない。

ただ米国のように捜査機関による通信傍受が日常化すると、犯罪に無関係な一般市民の私生活が警察に筒抜けになり、また政府に批判的な人物の行動が制約を受けるおそれもある。これに対して電子メールを暗号化する技術が発達し、その暗号技術の輸出を米国政府が規制したため、紛争が生じたことがあったが、この問題は結局、米国以外の国で強い暗号が開発されたため、輸出規制が無意味になって終わった。今でも日本でプライバシーというとき、この暗号問題をモデルにして「監視社会」対「市民の自由」という図式で論じることが多いが、これはプライバシー一般とは別の捜査手法の問題である。

米国の場合、冷戦時代から諜報活動が広く認められ、最近ではテロリスト対策という理

由で包括的な通信傍受が行われているといわれるが、日本では憲法上の制約が強いため、このような極端な監視活動は行われていない（むしろ検挙率が 2 割を切るなど、捜査能力の低下が深刻な問題である）。また今回の法案で規制の対象にしているのは、訪問販売やダイレクトメールなどの迷惑行為で、警察の捜査情報などとは無関係である。いずれにせよ通信の秘密は憲法で定められているので、この問題も除外する。

２．各国の規制

個人データ保護の費用と便益

個人データを守る技術は、インターネットではほぼ完成している。電子メールなどの内容は、PGP(Pretty Good Privacy)などの暗号技術で守れるし、電子商取引においては個人データはかなり厳重に保護されているのが普通であり、P3P(Platform for Privacy Preferences)[2]のような手順を使えば個人データの流通を本人がコントロールできる。私のデータに価値があるとすれば、その一部は情報を入力した（そしてマーケティングの対象となる）私にも帰属すべきだが、こうした交渉も P3P によって可能であり、その権利は特別な立法によって保障するまでもなく、通常の契約によって実現できる(Lessig 1999:pp.159-163)。

問題は、このような契約以外の形で本人がデータベースを（公権力を使って）コントロールする法律を作ることが望ましいかどうかである。たとえば私に債務不履行の経歴があるという情報を銀行 X が他の銀行 Y に知らせた結果、私が Y から融資を受けられなくなったとしても、その不利益は Y が真実を知ったことによる正当な行動であって、X が真実を知らせたことは非難できない。しかし、この情報を知った Z が私を「カネを出さないと他の銀行にもお前の信用情報を公表するぞ」と脅したら、これは恐喝である。また私が誤ってブラックリストに載って融資を受けられなくなったら、これも問題がある。つまり問題は個人データの流通ではなく、その悪用もしくは誤用なのである。

恐喝は刑法で罰すればよいし、クレジットカード番号の盗用のような犯罪も刑法に規定がある。名誉毀損は、民事的にも刑事的にも処理する法的手段がある。残るのは、犯罪にならない軽微な迷惑行為やデータの誤用だが、この程度の問題のために、データの流通そのものを本人が差し止める権利を認めることは弊害が大きい。たとえば X が私が多重債務者であることを隠して Y に私を紹介したら、Y は損害をこうむるかもしれないし、私がガンであることを隠して生命保険に入ったら保険金詐欺である。住基ネット（住民基本台帳ネットワークシステム）で問題になっている住所・氏名は、住民基本台帳法で閲覧自由になっている公開情報であり、厳重なセキュリティで保護するのは無意味である。

このように情報の種類によって費用と便益のバランスはさまざまであり、一律にあらゆる個人データを規制する法案には無理がある。また、この種の問題は社会のネットワーク

[2] 電子商取引などを行う際に、どのような個人情報をサイト側が収集するかを利用者が許諾するための電子的な手順。W3C(World Wide Web Consortium)によって標準化されている。http://www.w3.org/P3P/

化にともなって生じる情報の乱用による被害のごく一部であり、個人データだけを規制しても根本的な解決にはならない。特定の情報の流通を阻害することによって問題を解決しようとするのではなく、被害そのものを救済するしくみを考える必要がある。

欧米の個人情報保護法

1970 代から、コンピュータ・ネットワークの発達によって信用情報などが本人の知らない間に流通するようになったため、1980 年に OECD が個人データ保護のガイドラインを決めた[3]。これは「収集制限」「データの質」「目的の特定」「利用制限」「安全確保」「公開」「個人参加」「説明責任」の 8 原則からなり、特に重要なのは、「個人データは合法的かつ公正な手段によって、必要ならば本人がそれを認識または同意した上で収集しなければならない」とする収集制限の原則である。これは政府・民間を問わずあらゆる情報について、本人の同意なしに個人データを流通させることを禁止するもので、このガイドラインをもとにしてできた EU（欧州連合）のデータ保護指令が 1995 年に発効し、欧州各国でもこれに沿って国内法が制定された。

ところが、ちょうどこのころからインターネットが急速に普及し始め、大型機による閉じたネットワークを前提にした EU 指令をオープンなインターネットに適用すると、ほとんどすべてのウェブサイトが違法になってしまった。ホームページで個人名を引用した場合、本人に承諾を得ていないと、「収集原則」に違反したことになってしまうからである。

このため、欧州でも実際にはデータ保護法の運用はあまり厳格に行われていないが、スウェーデンでは EU 指令の前から「データ法」があり、個人データに厳重な規制を行っている。このため、動物愛護団体が毛皮業者のリストをホームページに掲載したり、消費者団体が銀行の取締役をホームページで批判したというだけで行政処分を受けるといった事件が相次ぎ、多国籍企業はスウェーデンからウェブサイトを引き上げている。

米国では、1974 年に「プライバシー法」が定められたが、これは欧州のようにすべての個人データを包括するものではなく、連邦政府の持つ個人データについて個人への公開の原則などを定めたものである。これは情報公開を定める「情報自由法」との関連で、情報公開に際してプライバシーを保護するとともに、プライバシーの名において情報公開が拒否されることを防ぐものである。

この原則は OECD の 8 原則をほぼ踏襲したものだが、適用の対象は連邦政府に限られており、民間については業界ごとに基準を定めて自主規制し、個別の判断は司法にゆだねる「セグメント方式」がとられてきた。州法では、欧州のような包括的な個人データ規制を行う州もあり、連邦レベルでも同様の規制を行うべきだという意見も根強いが、「自由な経済活動を阻害する」という議会や業界の反対で、連邦レベルでの立法化は見送られてきた。司法的な判断においても「プライバシー権」を広く認める傾向が次第に強まっているが、法曹界の主流は Posner (1981)のようにプライバシーの保護を無条件に認めることは合衆国

[3] http://www.kantei.go.jp/jp/it/privacy/houseika/dai11/11siryou5.html

憲法修正第 1 条（言論の自由）に抵触するという意見で、包括的なプライバシー権は立法的には認められていない。

ところが EU 指令では、その原則を守らない国への個人データの移転も禁止しているため、電子商取引で米国のサイトが本人の同意なしに個人データを収集すると欧州では違法となり、欧州の現地法人が行政処分を受けるおそれがある。これに対して米国政府が反発し、交渉の結果、EU 指令の基準を受け入れる米国企業については欧州との取引を認める「セーフ・ハーバー」という協定が結ばれた。しかし、現在この協定に加盟している企業は 250 社余りで、大部分の米国企業は（EU の基準では）非合法状態のまま欧州との電子商取引を行なっている。

日本の個人情報保護法案

個人データの法的保護が日本で問題になったのは、1999 年に住民基本台帳法が改正され、「国民総背番号」がつけられることになったのがきっかけである。行政については、すでに 1988 年に行政機関個人情報保護法が制定されていたが、そこから情報が民間に漏れた場合についての規制がないため、これを補完する目的で個人情報保護法案が作られた。

この法案は、これまでの欧米の法律を踏まえて慎重に作られている。基本的には OECD ガイドラインにもとづく包括的な規制だが、8 原則を 5 原則に集約し、個人データの収集については規制せず、保護の対象を第三者への提供だけに限定している。また「本人の同意」を「本人の適切な関与」に弱め、前半で基本原則（努力規定）を定めた上で、後半では義務と罰則を規定する二段構えになっており、後半の義務規定からは報道などいくつかの業界をネガティヴ・リストで除外している。

最大の問題は個人情報の提供に「本人の同意」を条件とする規定（第 28 条）だが、インターネットのサイトなどが自動的に違法になるのを防ぐため、「本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であって、次の各号に掲げる事項について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき」は個人情報を無断で公開してもよいとされている（第 28 条の 2)。要するに「同意しない」といえるようにしておけば、本人が明示的に拒否(opt out)の意思表示をしない限り、合法とみなすという考え方である。

しかしデータの収容されている本人がオプト・アウトしたら、政令で定める人数（5000 人以上になるといわれる）のデータを収容するサイトは、その要求に応じなければならない。この法案の対象とする「個人情報取扱事業者」には営利・非営利のウェブサイトが含まれるので、ほとんどの企業のウェブサイトは「違法」になるリスクを負っていると考えたほうがよい。たとえば、私が Google（世界最大の検索エンジン）に対して「私の個人情報を提供するな」と要求すると、Google の日本法人は私の名前の出ている 2000 余りのサイトをインデックスから削除しなければならない。これは技術的にはむずかしいことではないが、このとき削除はサイト単位で行われるので、私の名前を載せているドメイン全体が

（報道機関を除いて）Google で検索できなくなる。また住宅地図にも掲載を拒否できるようになるので、地図データベースにも大きな欠落ができるだろう。

さらに危険なのは、「２ちゃんねる」などの掲示板である。現在は匿名の掲示板で書かれた悪口を削除させるには、匿名の相手に対して名誉毀損などの訴訟を起こさなければならないが、今回の法案が成立すると、私の名前（個人情報）を掲載しているというだけで削除を求めることができる。いったんオプト・アウトすると、掲示板の管理者は二度とその個人についての発言が掲載されないよう注意する義務を負い、見逃した場合には損害賠償を求められる可能性もあるので、掲示板の運営はきわめて困難になろう。また違反行為が頻発する場合には行政処分を行うことができる（第 39 条）ので、トラブルが頻発する掲示板は閉鎖されるかもしれない。

修正案では、こうした問題点がほとんど改善されないで、5 項目の基本原則がすべて削除されて「個人の人格尊重」をうたうだけの抽象的な「基本理念」になり、義務規定から報道機関・学術研究機関・宗教団体・政治団体および著述業が除外される方向だという。基本原則は、OECD ガイドラインをもとにした個人情報保護法の柱であり、それを完全に削除するのでは、もはや基本法としての体をなしていない。

他方、この規制によって迷惑行為を防止する効果は疑わしい。現実には、すでに日本国民全員の住民データや地図データが CD-ROM で市販されており、新しいデータの取得を規制すると間違いが増えるだけである。個人データのみならず違法にコピーされた映像も WinMX などの P2P(Peer-to-Peer)ソフトウェアによってインターネットで流通しており、この種のソフトウェアでは差し止めは不可能に近い。結果的には、目につく大企業のウェブサイトだけが摘発や訴訟の対象になり、違法な情報はアンダーグラウンドで流通するだろう。個人データだけを規制しても、問題の解決にはならないのである。インターネットにおいて情報の流通を規制するのは無理であり、情報は入口（提供するとき）か出口（利用されるとき）でコントロールするしかない。入口では P3P のようなシステムで本人がコントロールし、出口では後にみるような制度で司法的に救済することが現実的である。

３．制度設計の考え方

自己情報コントロール権

法案の改正にあたって野党が求めているのは「自己情報コントロール権」を明記することである。そういう権利が言葉として明記された法律は世界に存在しないが、日本では「他人が自己についてのどの情報をもちどの情報をもちえないかをコントロールすることができる」（岡村・新保 2002:p.72）という包括的な差し止め権をさすことが多い[4]。しかし日本

[4]日本弁護士連合会は「憲法 13 条が定める個人の尊厳の確保、幸福追求権の保障の中に自己情報コントロール権が含まれる」と主張して「自己情報主権の確立」を求めているが、こういう権利が表現の自由を侵害するという認識が欠けている。http://www.nichibenren.or.jp/jp/katsudo/sytyou/jinken/00/2002_4.html

の法案は、自己情報コントロール権を認めていない。これは乱用の危険が大きいからである。日本の法案では、個人名を含む記述はすべて個人情報とみなされるので、EU 指令のようにオプト・イン（本人が同意しない限り違法）になっていると、きわめて広範な媒体（特にホームページ）がつねに「違法」になるリスクにさらされることになる。

では自己情報コントロール権を認めることにどのような意味があるだろうか。私の個人データは私の創作物ではないので、創作のインセンティヴを守るという経済的利益はない。個人データの乱用による被害を救済するという点ではどうだろうか。現在の法案の対象としているのはデータベースだから、被害として考えられるのは、名簿業者がデータを売買して、不要な電話勧誘や訪問販売が来るということだろうが、これはデータベースだけを規制しても防ぐことはできない。信用情報が誤ってブラックリストに載るといった被害も、事後的に訂正でき、こうした問題は現在でも通常の民事事件として処理されている。

行政に対するコントロールは民間とは区別して考えるべきだが、行政に対する請求権は現在の法律でも十分保証されている。米国のプライバシー法についても自己情報コントロール権という言葉が（日本で）使われることがあるが、これは連邦政府を相手とする情報公開請求権にすぎない。むしろ現在の行政個人情報保護法や住民基本台帳法では、情報の使途が細かく制限されているため、地方自治体が自主的に個人データの取扱いを決めて効率的に運用する余地がない。個人データの公的利用に関する法的な制限を緩和し、自治体の裁量を大幅に認めるべきである。何に使うかについては本人に事前に告知し、実際に何に使ったかについてもログ（アクセス記録）を取ることを義務づけ、紛争は徹底した情報公開によって解決すればよい。

通常の契約による以上の特別の権利を立法的に保障することに意味があるのは、個別に司法的に処理するコストが非常に高い場合である。特許権や著作権などは、定型的な手続きによって複雑な権利関係をモジュール化し、紛争処理を円滑に進めるという意味があるが、自己情報コントロール権の対象とするのは、以上みたように従来の民法や刑法あるいは行政法で処理できる問題であり、そういう権利を特別に認める便益はない。他方、それによってだれにでも他人の言論に介入する権利を与え、データベース全体を規制のもとに置くことによる社会的費用は大きい。ましてそれを不可侵の人権（あるいは人格権）として絶対化すると、柔軟な対応が困難になり、不要な紛争が多発して情報の創造を阻害することは著作権法でも明らかである。これを明記しない日本政府の判断は賢明である。

市場メカニズムによる解決

プライバシーに関心が集まるようになったのは、情報技術の限界的な便益が逓減し、その費用に目が向くようになったためだろうが、これは衣食住が足りると健康が気になるような「贅沢品」によくある錯覚である。個人データ漏洩の被害は限界的には大きく見えるかもしれないが、その絶対的な水準は情報技術のもたらす便益とは比較にならない。したがって問題は、漏洩をゼロにすることではなく、それを極小化するとともに情報の自由な

流通を保障し、いわばネットの便益を最大化することである。

個人データの流用のような外部効果をともなう紛争を処理するルールとしては、外部性をコントロールする資格(entitlement)を一種の財産権とみなし、その所有者（あるいは情報の利用者）に許諾権を与えることによって保護する財産ルール(property rule)と、外部性を発生させた者に事後的な賠償責任を負わせる責任ルール(liability rule)がある[5]。通常は、資格に所有権を設定して市場で取引するコストが低ければ、財産ルールによって市場で解決することが効率的だと考えられている(Coase 1960)。しかし消費者に無条件の資格を認めると、データを守るコストはすべて企業（あるいは行政）に転嫁できるので、過剰に強いセキュリティを求めてそれに「ただ乗り」する傾向が強い。

こうしたモラル・ハザードを防ぐには、データ保護のコストを内部化する制度設計が必要である。その一つの方法は、一定量の個人データを利用する資格を企業に与え、汚染物質の排出権のようにそれを取引することである。ただ Coase も強調するように、実際には情報のように外部性の大きい資源に所有権を設定して市場で取引するコストはきわめて高く、個人データを収集した企業が財産権を持つことには本人の抵抗も大きいだろう。したがって個人データの保護は、基本的には事後的な責任ルールで行うことが望ましい。

個人データ流通の費用と便益は単純なトレードオフの関係にあるわけではなく、両者を切り離して解決することは可能である。問題はデータの流通ではなく、それを悪用（誤用）した迷惑行為だから、その結果について民事的に救済すればよい。たとえば消費者が迷惑な電話勧誘や電子メールを受けたとき、第三者機関に申し立てて従量制の迷惑料を企業から取れるようにすることも考えられる[6]。あらかじめ勧誘を拒否する消費者のリストを作って「すべての勧誘を拒否する」「迷惑料の支払いによって勧誘を認める」など何段階かのオプションを設定し、拒否する人に勧誘を行った場合には禁止的に高い迷惑料を取るのである。リストへの登録や料金徴収の手続きをウェブサイトで行い、第三者機関が手続きを仲介すれば、名前を公開しなくても実装できよう。

これによって企業は勧誘を望む消費者だけに商品を売り込むことができ、迷惑料よりも高い利益を得られる場合には有料で勧誘を行う。勧誘を好まない消費者も迷惑料を得るので、双方が利益を得ることができる。勧誘以外の迷惑行為も、いくつかの類型に分類して標準料金を定めれば同様の責任ルールで解決できよう。たとえば名簿屋が無断で個人データを販売している場合には、差し止め権ではなく、その代金の何%かを請求する権利を認めればよい。被害額の算定が適正に行なわれれば、双方に選択の余地を与える責任ルールのほうが一方に差し止め権を与える財産ルールよりも効率的である（付録参照）。

---

[5] Calabresi-Memaled(1972)は、この他に譲渡不可能な(inalienable)権利も挙げている。これはプライバシーを「基本的人権」として守ることに相当するが、こういう絶対的な権利保護は多くの場合、柔軟な制度設計を困難にし、好ましくない。

[6] 電話勧誘を拒否するリスト(“don’t call” list)に挙げた消費者への勧誘を禁止する規制は、米国の 20 以上の州で実施されている。Ayres-Funk (2002)は、これを改良して 900 番電話を使って勧誘する企業から迷惑料を取るしくみを提案している。

民間による紛争処理

ただ、こうした軽微で多数の紛争を通常の司法機関で処理するのは無理なので、裁判よりも簡単な手続きで紛争処理を行う個人データ専門の ADR（代替的紛争処理機関）を創設することが望ましい。現在の法案では主務大臣の所管する「個人情報保護団体」が紛争を調停することになっているが、この種の紛争では行政が一方の当事者になるケースが多いことを考えると、これでは中立性が担保できない。

料金は個々の消費者と企業が交渉によって決めればよいが、個人データの場合には交渉コストが高すぎるので、従量制の迷惑料をあらかじめ決めておけばよい。この料率は平均的な迷惑のコストと等しく決めることが望ましいが、多少の誤差があっても責任ルールによる事後処理のほうが財産ルールによる差し止めよりも効率的になることが多い（付録参照）。料金の徴収は、いたずら電話や迷惑メールのように身元のわからない場合にはむずかしいが、身元を明らかにしない個人データの悪用には一律に「全面拒否」の場合の禁止的に高い料金を設定すればよい。

個人データの乱用が、法的に処理可能な形で顕在化するとは限らない。本人の知らない形でデータが悪用されて間接的に損害をこうむる場合もあるし、匿名の掲示板における中傷のように責任の不明な形で問題が生じることも考えられる。こういう場合の解決は、基本的には徹底的な情報開示によるしかない。そのためには、個人データを入手した経路を明かすログを記録して開示することを義務づけ、それを拒否した場合にはサービス提供主体が責任を負う（その代わり「本人同意」の規定を廃止する）というルールを設けることも一案だろう。これは現在のプロバイダー責任法でも定められている原則であり、このように他人の名誉を傷つけた場合には事後的に訴訟の対象になるという判例が定着すると、事前の抑止力ともなろう。

この提案は、どうしても個人データを守る必要があるなら、今回の法案のような直接規制よりも効率的な手段があることを示しただけで、それを積極的に推奨するものではない。個人データの保護による便益は限定的なので、ここまで社会的コストをかけて守る必要があるかどうかは疑問である。個人情報保護法は、基本原則に加えて事後的な処理で救済しきれない特殊な情報（戸籍、信用情報、病歴など）についての規制を個別に指定するガイドラインにとどめ、あとは司法的な解決にゆだねてはどうだろうか。この点で、ネガティヴ・リストのまま基本原則を廃止した修正案は最悪である。

ポジティヴ・リストにすると、それ以外は従来の「業法」による規制になって業界の利害が反映されやすいとか、多くの業界にまたがる企業をどう規制するのかなど厄介な問題もあろう。しかし個人情報の性格はもともとばらばらであり、信用情報と２ちゃんねるを同じ法律で規制する意味があるとは思われない。個別法で規制している米国で、さほど大きな問題が生じているという話も聞かない。

いずれにせよ、インターネットで流通する膨大な情報を、法律でコントロールするのは

限界があり、特に海外から来る迷惑メールやウイルスなどは防止しようがないので、最終的には社会的な規範によるしかない。たとえば、この ADR で「違法」と判定された企業をウェブサイトで公開するとか、大量に迷惑メールを出す業者を特定して警告する専門のデータベースを作るといった国際的な「評判メカニズム」を作れば、抑止効果はあるかもしれない。インターネットでは、基本的には情報は自己責任によって入口で守り、出口の問題は情報公開にもとづく合意によって解決するというルールを徹底すべきである。

住基ネット

以上のように個人データを立法によって守ることは弊害が大きいので、セキュリティなどの問題は第一義的には情報システムの設計によって技術的に解決し、通常の契約によって本人がコントロールすることが望ましい。ただ電子商取引サイトにアクセスするたびに複雑な契約を結ぶことは現実的ではないので、そういう手続きを自動化する P3P のようなツールの標準化を行政が支援することは意味があろう。また企業がその規約を守るとも限らないので、その検証を行う機関も必要だろう。これも TRUSTe のような非営利組織を活用すれば行政が直接関与する必要はないし、新規に立法する必要もない。

行政の電子化においては、「国民総背番号」をめぐる不毛な論争が続いている。住基ネットについては個人情報の絶対保護を求める野党や市民団体が、個人情報保護法案は廃案にしろと主張し、しかも住基ネットの運用に反対する理由が「個人情報保護法が成立していない」からだというのだから、わけがわからない。この矛盾した主張も、報道機関を特別扱いすることから生じている。データベースも含めれば、絶対的な表現の自由と絶対的な個人情報保護が両立しないことは明らかである。

また名寄せは「国民背番号」によって初めて可能になるわけではない。現在のデータベース技術を使えば、氏名や住所で全文検索して名寄せすることは容易であり、検索エンジンを使えば、市町村役場の情報を使うよりはるかに詳細な個人データが名寄せできる。インターネットこそ、最大のプライバシー侵害装置なのである。背番号反対論は 20 年ぐらい前のフィールド検索しかできなかった時代の遺物であり、MS ウィンドウズにさえ全文検索ツールが付属している今日では無意味である。背番号がないと、同姓同名などの間違いが増えるだけである。情報を隠したり不正確にしたりすることは問題の解決にはならない。

問題は検索キーではなく、データそのものを保護し、1 ヶ所に大量のデータを置かないことである。住基ネットでは、処理すべき住民データは市町村のサーバに分散しているのに、4 情報をわざわざ「全国センター」に集中して専用線で結んでいるため、コストがかさむばかりでなく、全国センターのセキュリティ負担が大きくなる。住民票や各種登録などのローカルな事務処理のために、大がかりな国民背番号をつけ、日本国民全員でも 100GBytes に満たないデータのために高価な専用線を引くのは無駄である。全国ネットワークが必要なのは、他の自治体への問い合わせやデータの更新のようなごくわずかの事務処理であり、インターネットで十分である。

さらに住基ネットとは別に、総合行政ネットワーク(LG-WAN)という全国ネットワークが構築され、公的な本人認証や電子署名は自治体が独占することになっている。しかし認証や電子署名は、すでに民間でビジネスが成立しており、政府がそれとは別のシステムを強制することは行政の簡素化に逆行する。現実には、こういうシステムの開発や運用は民間が受託するので、自治体は実質的な責任を持ちえない。政府は、こうした民間のシステムを監視する役割に徹すべきである。

こうして万全を期しても、コンピュータに絶対はない。住基ネットにおいても、事故の責任を追及されることを恐れた総務省が「絶対安全」を求めて住基ネットを自治体のネットワークとは別系統の専用線にしたことが行政ネットワークを混乱させ、事務処理の効率をかえって低下させている。このようにセキュリティを物理層で守るのは無意味であり、データを暗号化すればインターネットで十分である。重要なのは情報の性格に応じてどの程度のセキュリティを保障することが妥当かというランクづけであり、インターネットで現金も引き出せる時代に住所氏名を専用線で守るのは倒錯している。

実際には、弱いのは住基ネット本体よりも末端の市町村役場のサーバである。現在の住民基本台帳法でオンライン化されている程度の情報は、もれても大した問題はないが、どうしても心配な人には、オプト・アウトを認めればよい。たとえば住基ネットによるサービスの不要な人には、横浜市のように住民票コードを通知しないという選択肢もある。その代わり、インターネットでサービスを受けたい住民には、すべての行政情報をオンラインで 24 時間提供し、個人データ漏洩のリスクは本人が負えばよい。行政情報システムは、個人データも含めてインターネットに乗せることを前提にして設計すべきである。

世界各国で国民に一意の番号をつけているのは、第一義的には徴税事務のためであり、日本のように納税者番号を除外して背番号をつけている国はない。日本では、1980 年にいったん導入の決まったグリーンカード（少額貯蓄等利用者カード）が政治家の反対によって撤回されて以来、この問題はタブーになっているが、仮名口座などで課税をまぬがれている資金は GDP の 4%程度（約 20 兆円）あるとも推定される。この 1 割でも捕捉できるなら、行政情報化は十分メリットがある。政治的な困難を恐れず、納税者番号について議論すべきである[7]。

４．結び

「ビッグ・ブラザー」が中央集権的に情報を収集して国民を管理するというオーウェル的な監視社会のイメージはいまだに根強いが、現実には市町村役場よりも金融機関や電子商取引サイトのほうが大量の（しかも利用価値の高い）個人データを持っており、Amazon.

[7] 米国の社会保障番号は、公開情報なので納税者番号にも使われているが、日本の住民票コードは、非公開で変更も可能なので、納税者番号とは別にし、むしろ行政情報をインターネットで開放する際のパスワードとして使ったほうがよい。

com は私が過去に注文した本のデータから私の好みをかなり正確に推定できる。現代は、多数の「リトル・ブラザー」が互いに監視する相互監視社会なのである（東 2002)。これは、ある程度は情報社会に生きる上で避けられないコストであり、Amazon.com がそのデータを利用して本を推薦するように、必ずしも悪いことではない。今回の法案のように他人の言論に介入する包括的な権利を与えることは、かえって相互監視を強める危険な第一歩になりかねない。

また現在の電子政府計画には、何のために電子化するのかという目的意識が欠け、単なるインフラ整備として行なわれているという印象が強い。行政の電子化は、ほんらい行政改革の一環であり、現在の行政事務を単に電子的に置き換えるのではなく、まず業務を整理・縮小して民間にできることは民間にまかせ、行政組織を見直すことが第一である。オンライン化によって地方公務員を何万人へらすとか、住民税を何%減税するとかいう目標もなく、公共事業のような感覚で電子化のために電子化を行なうのでは、住民ばかりか自治体にも不信感を抱かれて当然である。

最大の問題は、行政情報システム全体の構造が時代遅れのビッグ・ブラザー型になっていることである。これは情報システムを高コストにし、行政効率を低下させるばかりでなく、情報の保護も困難にしている。ネットワークの構造は組織の構造と補完性を持っており、行政組織を分権化するにはオープンで分散的な行政ネットワークが不可欠である。現在のように電子化の細かい仕様まで総務省が自治体に通達していては、かえって中央集権が強まるおそれが強い。こうしたビッグ・ブラザーを作り出し、行政のインターネット化を阻害しているのが「プライバシー絶対保護」を求める市民運動だというのは皮肉である。

紛争処理を責任ルールによって行うことは、規制の効率性という以上の意味をもつ。それはルールの制定や実施の権限を立法機関から司法機関に移し、より分権的で柔軟な制度に変えることである。技術革新の急速なインターネット時代に、情報を立法によって守ることは有害無益な過剰規制を招きやすい。情報は当事者の合意によって守るべきであり、その基本は情報を徹底的に公開し透明にすることである。あらゆる行政情報をインターネットによって開放するとともに行政手続きをオンラインで可能にするオープン・ネットワークを作ることは、行政の効率化に役立つばかりでなく、真に分権化された自由な社会を築くきっかけとなろう。

参考文献

Ayres, I. and Funk, M.(2002) "Marketing Privacy: A Solution for the Blight of Telemarketing", http://islandia.law.yale.edu/ayers/mprivacy.pdf

Calabresi, G. and Memaled, A.D. (1972) “Property Rules, Liability Rules, and Inalienability: One View of the Cathedral”, *Harvard Law Review*, 85.

Coase, R. (1960) “The Problem of the Social Cost”, *Journal of Law and Economics*, 3, 1-44.

Kaplow, L. and Shavell, S. (1996) "Property Rules versus Liability Rules", *Harvard Law Review*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=56405
Lessig, L. (1999) *CODE and other Laws in Cyberspace*, Basic Books.
Posner, R. (1981) *Economics of Justice*, Harvard University Press.
Warren, S.D. and Brendeis, L.D. (1890) “The Rights to Privacy”, *Harvard Law Review*, 4:193-
東浩紀(2002)「情報自由論②」『中央公論』8 月号
岡村久道・新保史生(2002)『電子ネットワークと個人情報保護』経済産業調査会

付録　財産ルールと責任ルール

政府が不完全な情報しかもっていない場合には、消費者が事前の差し止め権をもつ財産ルールよりも一定額の迷惑料を支払って企業が個人データを利用する責任ルールのほうが効率的な結果をもたらす(Kaplow-Shavell 1996)。これは次のようにして示せる。

ある企業がある消費者のデータを利用して勧誘することを認めるかどうかを政府が判断する問題を考える。勧誘による消費者の迷惑を h、勧誘を止めることによる企業の損害を c とし、交渉が不可能だとすると、政府が c と h を正確に知っていれば、c≦h となる場合に限って消費者に差し止め権を与え、それ以外の場合には企業の自由にまかせることによって最善の状態を実現できる。同じ結果は、迷惑料 x を x = h に設定することによっても実現できるので、財産ルールと責任ルールは同一の結果をもたらす。

他方、政府の情報が不完全で、それぞれの期待値 c*、h*しか知らないとすると、財産ルールのもとでは政府は c*≦h*のときに限って消費者に差し止め権を与えることが効率的なので、社会的コストは C_p = min (c*, h*)となる。他方、責任ルールにおいて企業に迷惑料 x を課すと、企業は 0 < c < x の場合には勧誘を行わないで営業を制限されるコスト c を負担し、x < c の場合には勧誘を行なって消費者が迷惑 h を負担する。c の確率密度関数を f(c)とし、h = h*とすると、責任ルールによる社会的コスト C_d は

$$C_d(x) = \int_0^x cf(c)dc + \int_x^\infty h^*f(c)dc.$$

ここで $C_d(x)$を最小化する 1 階の条件は、$xf(x) - h^*f(x) = 0$、すなわち x = h*である。そのように x を設定すれば、0 < c < x の場合には $C_d < \int_0^\infty h^*f(c)dc = h^*$となるので、$C_d$ ≦h*。同様に x < c の場合には C_d < c*となるので、C_d≦c*。したがって C_d≦min (c*, h*) = C_p、すなわち責任ルールの社会的コストは財産ルールよりも低い。この結果は、正確に x = h*となっていなくても、C_d≦h*かつ C_d≦c*である限り成り立つ。消費者に差し止め権を与える財産ルールは x = ∞となる場合に、また企業に営業権を与える財産ルールは x = 0 の場合に相当する。