IIPS
Institute for
International Policy Studies
・Tokyo・

個人情報の蓄積・流通における問題
ーネット社会でのアイデンティティー

・平和研レポート・
主任研究員　広木　功

IIPS Policy Paper 309J
June 2004

財団法人
世界平和研究所

Institute for International Policy Studies
5th Floor, Toranomon 5 Mori Building,
1-17-1 Toranomon, Minato-ku
Tokyo, Japan 〒105-0001
Telephone (03)5253-2511 Facsimile (03)5253-2510

＜　目　次　＞

１．　はじめに

社会の情報化が進み、これまでの「実社会」に対し「ネット社会」という表現がされるようになってきた。この「ネット社会」では、個人に関するさまざまな情報が利用され、個人のアイデンティティが表現されるようになってきており、従来よりも個人情報の開示が進んできた。JIS Q 15001[1]によれば個人情報とは、『*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、または個人別に付けられた番号、記号その他の符号、画像若しくは音声によって当該個人を識別できるもの（当該情報だけでは識別できないが、他の情報と容易に照合することができ、それによって当該個人を識別できるものを含む。）*』　とされている。しかし、時間や空間の制限をうけにくいというネット社会の性質もあり、これら個人情報の流通が思わぬ被害をもたらすことも指摘されてきている。

個人情報の扱いについては、警備などセキュリティ目的での利用であっても、プライバシー保護には注意が払われているものの[2]、近年の生活安全上に対する意識の変化や技術の進化などは、プライバシーとセキュリティのバランスに影響を与えており、これまでのプライバシー概念を動揺させている。一方、情報のデジタル化がすすむことで個人の属性や行動に関する情報の蓄積利用が容易になり、経済的価値を持つようになってきている。民間においては、個人の情報保護よりも経済的利益が優先される形で情報利用が拡大される傾向にあり、基本情報（氏名、住所など）だけでなく、医療情報のようなさらに機微性の高い情報(センシティブ情報[3])の利用も進みつつある。公共部門においても住基ネット（住民基本台帳ネットワークシステム）のように、従来の様々なシステムに乗っていた個人に関する各種の情報が統合されて、電子ネットワーク上を流通する仕組みがつくられてきている。

---

[1] JIS Q 15001 は「個人情報保護に関するコンプライアンス・プログラムの要求事項」として平成 11 年 3 月 20 日付けで制定発行されている。

[2] 「早稲田大学の名簿提供事件B」において、最高裁は「承諾を得ずに個人情報を開示したのはプライバシー侵害で違法」との判断を示した。これは、江沢民・前中国国家主席が 1998 年秋に早稲田大学で講演した際、大学側が参加希望者 1400 人の名簿を警視庁に提供したのはプライバシー侵害として、当時学生であった計9人が損害賠償を求めたもの。名簿には名前のほか、学籍番号や住所、電話番号が参加希望者によって記入されていた。最高裁は「秘匿性が必ずしも高くない単純情報だが、みだりに他人に知られたくないと考えることは自然で、法的保護の対象となる」と指摘した。

[3] センシティブ情報：JISQ15001 において、原則として収集を禁止している以下のような特定の個人情報を指す。

・思想、信条、宗教
・人種、民族、門地、本籍地、身体・精神障害、犯罪歴、その他社会的差別の原因となる事項
・勤労者の団結権、団体交渉、その他団体行動に関する事項
・集団示威行為への参加、請願権の行使、その他の政治的権利の行使に関する事項
・保健医療、性生活

このような個人情報の蓄積・利用に対し、監視社会化につながるとする一部の抵抗もあるが、新たに生まれた技術を生かしてメリットを享受し社会を豊かにしていくためには、メリットとデメリットを科学的視点などから客観的に検証判断し、システムを導入することになる。しかし、「一度流出したデータの完全な回収・削除はほぼ不可能」と言われる現実も踏まえなければならない。個人情報の利用について本質的議論を充分にしていかなければ、「一時の利便性追求」や「心理的安心感のための監視」として濫用されることになり、個人のネット上におけるアイデンティティが脅威にさらされることになる[4]。個人情報を利用するシステムに対しては、技術開発・産業推進面だけでなく、法的な視点や社会感情にも配慮し、整合をとりつつ、社会の中のシステムとしての合意が必要であると考えられる。

本稿では、法的な解釈やプライバシー範囲の定義が目的ではないため、深く立ち入らないが、これらの個人情報の利用に関わる事例を取り上げ、ネット上のアイデンティティ保護における課題について考察する。

２．情報化と人格権

２－１．プライバシー概念の変容

（１）セキュリティとプライバシーとのバランスの変化

米国では 2001 年 9 月 11 日に発生した同時多発テロ事件以降、テロ防止のためにプライバシーよりもセキュリティを優先する傾向となってきた。空港などの重要施設では監視カメラの導入・運用など、あらたな手段・技術を用いて人物の移動に対する監視を強めている（２－２（４）参照）。

日本は最近まで他国に比べて治安が良いと評価されてきており、市民（住民）の行動を監視する必要性は高くなかった。どちらかといえば個人の行動や情報に関し、生活安全上のセキュリティよりもプライバシー保護が重視される傾向がある中で、情報の流通による権利侵害として、名誉毀損、プライバシー侵害、肖像権の侵害などが法的に判断されてきた。しかし、街頭犯罪の増加、検挙率の低下など治安が悪化してきており、セキュリティへの要望が高まってきている。

そして、米国と同様に日本でも、2002 年の日韓共催のサッカーイベント「2002 FIFA ワールドカップ」と同じ時期、セキュリティ対策として国際空港（成田、関空）に顔認識技術を使った監視カメラが導入されている[5]。設置の目的は、「広くテロ対策およ

[4] Sun Microsystems 社が立ち上げたリバティ・アライアンス・プロジェクトではネットワークアイデンティティの管理・運用の技術標準策定を目的としている。

[5] 2002 年 5 月に導入。ASCII24「監視カメラ、成田空港にも 財務省は『設置の告示はしない』」(2002 年 8 月 26 日)　http://ascii24.com/news/inside/2002/08/26/638136-000.html

び密輸取締りのために導入（財務省関税局）」と説明されているが、カメラの設置台数等、機器の具体的な内容については、「監視取締上支障が生じることから答えられない」とされている。空港だけでなく、鉄道駅などの施設、主要な街頭や商店街にいたるまで監視カメラが設置されるケースが増えてきているが、その施設利用者にはあまり認知されていないようである。

個人情報の取り扱いにも変化がみられる。技術の進化と情報のデジタル化が進んだことは、個人に関する各種情報の収集・結合を容易にし、従来なかった利活用を可能にした。たとえば、ビジネス拡大を目指す民間部門（企業）の活動においては、顧客に関する複数の個人情報を収集し組み合わせることにより、嗜好や購買行動を分析する行動が取られるようになってきた。これにより、以前は単なる顧客リストにすぎなかった氏名、住所などの個人情報が、新たな価値を生む財産的側面をもつように変わってきている。その反面、それは集積された個人情報がその本人の意図しない目的で利用される事態をも生んでおり、有形無形の被害（感情）を生じさせている面もある。

個人に関する情報の利用拡大については民間だけではなく、公共部門においても進みつつある。記憶に新しいものとして「住民基本台帳法の一部を改正する法律」が平成 11 年（1999 年）8 月 12 日に成立[6]し、住民基本台帳ネットワーク（いわゆる住基ネット）導入された[7]。この導入に際してはシステム自体の安全性をはじめとして、個人情報漏洩のリスクなどいくつかの問題点が提起されることにより、導入後もそのシステムの安全性の評価を巡って議論が続いた。住基ネットシステム導入による効果はまだ明らかになっていないが、その評価は、一時の感情的な議論ではなく、中長期的な視点でされるべきものである。

（2）“プライバシー”と個人情報の開示レベルの変化

憲法 13 条に由来するとされる人格権は、名誉権、プライバシー権、肖像権、氏名権などで構成される。これまで個人のプライバシー保護を考えるとき、情報による権利侵害として問題にされることが多いのは、名誉毀損、プライバシー侵害、肖像権侵害などであった。過去における各権利に関する判例として、以下のものを挙げておく。

＜これまでに人格権を構成するとされた各権利＞

① 名誉権：「人格権としての名誉権」（『北方ジャーナル』事件での最大判 1986〈昭和 61〉・6・11）

[6] 8 月 18 日に公布。
[7] http://www.soumu.go.jp/top/vol28c.html

② プライバシー権：「私事をみだりに公開されないという保障は」「いわゆる人格権に包摂されるが、なおこれを一つの権利と呼ぶことを妨げるものではない」（『宴のあと』事件での東京地判 1964＜昭和 39＞・9・28）
③ 肖像権：「何人も、その承諾なしに、みだりにその容ぼう・姿態を撮影されない自由を有する」として、憲法 13 条は「国民の私生活上の自由が」「国家権力の行使に対しても保護されることを規定している」（京都学府連でも事件での最大判 1969＜昭和 44＞・12・24）
④ 氏名権：氏名は個人を識別する機能とともに「個人の人格の象徴であって、人格権の一内容を構成する」（NHK 外国人氏名日本語読み事件での最 3 小判 1988＜昭和 63＞・2・16）

従来のプライバシーの権利とは、個々の人間関係の親密度・疎遠度に応じて異なっているものの、私的領域の事実を無断で公開されることを拒否して自己の私的生活の平穏を確保する法的利益がプライバシーの権利であったとされる（船越　2001）。そもそも、プライバシーの保護とは、マスメディアにより個人の私生活が不特定多数の人間に暴露されてしまう被害に対して起こった動きであった。

しかし、近年ではプライバシー保護に関して、「プライバシー」の意味が変わってきたとする言説が多く見られるようになった。それはつまり“伝統的プライバシー”である、「一人にしておいてもらえる権利」から、“情報プライバシー”として「自己の情報をコントロールする権利」[8]に変わったとするものである。この説に基づけば、「個人に関する情報」の所在と流通のコントロールが、重要な問題となってくる。

ネット社会において、ネット上の活動におけるアイデンティティ表現は、個人情報を使用するものとなっている。コンピュータネットワークによる情報化が進む以前では、個人の存在・行動に対する各種情報の開示は限定的であった。経済的利益の観点から個人の信用情報（収入、資産、負債など）は必要に応じて開示されていたものの、私事性の高い情報（家族状況、健康状態など身体情報、個人の思想信条など）は基本的に非開示の秘匿される対象であった。ところが、社会の情報化が進むなか、企業等

[8] 個人データのコントロールについて言及したものとして、以下が挙げられる。
・OECD による「プライバシー保護と個人データの国際流通についてのガイドライン（Guideline on the Protection of Privacy and Transborder Flows of Personal Data）」（1980）
http://www1.oecd.org/publications/e-book/9302011E.pdf
・EU による「個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州会議及び理事会の指令 1995（Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data）」
http://europa.eu.int/comm/internal_market/privacy/law_en.htm

がより高付加価値なサービスや経済的利益を追求するにつれて、ＣＲＭ[9]（顧客関係管理）やデータマイニング[10]などの手法・技術が考案され、私事性の高い非開示情報が次第に利用されることとなったことで、結果として消費者が意識しないうちに開示が進みつつある。例えば、美容エステティック企業はアンケートやモニターを通して、顧客の身体情報などを収集・分析し利用している。また、書籍のインターネット通販サイトにおいては、顧客ごとに書籍の検索履歴や購買履歴がサーバーに保存され利用されている。美容に関する情報はかなり私事性が高いと考えられるし、書籍の購買履歴も嗜好性が推測される情報となり得る。

こうして、個人の氏名、住所などに加えて与信のための信用情報、商品購買記録などが記録・蓄積されて利用が進んだ結果、本人の希望していない勧誘行為などが増加した。本人が意図しない目的にも個人情報が流用されるようになったことから、個人情報を利用された本人が被害感情をもつケースが増えてきている[11]。さらに、個人宛に、有料サービス利用料金、債権回収などの名目による架空請求が行われる事例が頻発しており、実際の被害も発生させている。（３－２（３）参照）

氏名、住所については、以前から社会的に開示される情報としての性格を持っていたが、電磁的な記録が普及する以前は多くがアナログ情報として紙上に記録されていた[12]。すなわち、記録された「紙」を閲覧できなければ情報の取得が不可能であるという物理的な限界があった。情報を目的外に流用する事例としては、一部の企業の社員名簿、大学や各種学校の OB 名簿などが売買される市場が小規模に存在し、ダイレクト

---

[9] CRM：Customer relationship Management。顧客情報の取得・分析を行い、効果的なマーケティング・営業戦略の立案支援を目的とする顧客関係管理（システム）

[10] データマイニング（data mining）：小売店の販売データや電話の通話履歴、クレジットカードの利用履歴など、企業に大量に蓄積されるデータを解析し、その中に潜む項目間の相関関係やパターンなどを探し出す技術。例えば、スーパーの販売データをデータマイニングで分析することにより、「ビールを買う客は一緒に紙オムツを買うことが多い」「雨の日は肉の売上が良い」など、項目間の相関関係を見つけることができる。また、クレジットカードの利用履歴を解析することにより、不正使用時に特徴的なパターンを見つけ出し、あやしい取引を検出するなどの応用も考えられる。
http://e-words.jp/w/E38387E383BCE382BFE3839EE382A4E3838BE383B3E382B0.html

[11] 例えば、20年ほど前であれば、雑誌の懸賞に応募する際に記入した氏名、住所、年齢、その他の情報は他の用途への流用がされる意識は少なく、応募する側も警戒することなく記入し提出していたと思われる。しかし、現在では懸賞はインターネット上で実施されるようになり、そこで記入した情報が他のダイレクトメール発送などに流用されるとの疑いを持たれるようになってきているのが実情である。本来、業者（他人）が知り得ないはずの子供の年齢を基にすると思われる、節句用品や学習教材等のダイレクトメールが突然届けられることが聞かれるようになって久しい。当然ながら、自発的に登録をした事情がない限り、「何故この業者が子供の氏名、住所、生年月日を知っているのか」と疑問に感ずることになる。

[12] 一部の企業システムにおいて、顧客情報としてデータ化されたもの以外には集積されておらず、情報の利用もその企業のシステムに閉じたものであった。

メールなどのマーケティングに流用されていたものの、紙媒体の流通数には限りがあったため、その利用は比較的限定されたものであった。

ところがコンピュータの普及が進み、ハードディスク、フロッピーディスク、ＭＯ、ＣＤ、ＤＶＤ等の電磁的な記録が一般的になり、複製も容易になってくると、通信回線、ネットワークなど電気的、論理的な接続があれば情報そのものの空間的な所在はどこでもよいことになり、情報へのアクセスは距離的な制限を受けない。さらに、過去に記録・蓄積された情報もネットワーク上のどこかに存在しさえすれば情報にアクセスできるようになったことで、時間的な制限も並行して消失してきた。

個人の氏名、住所やその他の私的な情報が電磁的に記録、蓄積されてコンピュータネットワーク上に置かれ、外部から何らかの形で記録情報の閲覧ができるとすると、誰がその情報にアクセス、利用できるかについてコントロールが必要になる。さらには、個人の情報だけでなく、個人・団体などに対する評価や記事などを閲覧させる場合に、誰がそれに対し責任を負うかを明らかにすることも不可欠である。

しかし、このような情報のコントロールという観点では、それが非常に困難なシステムがネットワーク上に生まれ、利用されているのが実情である。例えばインターネット上にある巨大掲示板「２ちゃんねる」では、不特定多数が閲覧し、かつ書き込める状態になっている。このような場では、法人・著名人だけでなく、一個人も容易に非難の対象とされるようになった。

少年犯罪の発生時には、たびたび加害者の実名や顔写真とされる情報が書き込まれ、法務省人権擁護局などから削除要請が出されている。この「２ちゃんねる」への書き込み内容の管理を巡り、これまでにいくつかの賠償請求がされてきた。管理人が中傷発言を削除しなかったことについて争われた 2002 年 6 月の判決[13]においては、「名誉毀損発言を知っていたのに削除せず、原告に経営上の損害や精神的苦痛を与えた」とし、賠償金の支払いと書き込みの削除を命じている[14]。このような場合では、書き込み内容の削除申請手続きがとられても、実際に削除されるまでには時間差があることにより、24 時間中不特定多数の人間に閲覧される。そして、悪質な書き込みがさらに追加されたり、他の掲示板などに内容のコピーが書き込まれて拡散する余地がある。書き込みによって攻撃を受けたという被害感情を持つ側からすれば、少なからず不満の残るものであろう。

---

[13] H14. 6.26 東京地方裁判所 平成13年(ワ)第15125号 損害賠償等請求
http://courtdomino2.courts.go.jp/kshanrei.nsf/$DefaultView/2075F93E3210745849256BED0030F3EF?OpenDocument

[14] 2002年12月25日東京高裁でも「匿名の発言について、被害者が責任追及することは不可能。匿名発言でも名誉棄損は成立し、管理運営者は、他人の権利を侵害する発言が書き込まれないようにし、被害が拡大しないよう直ちに削除する義務がある」「管理者は今も書き込みを削除しておらず、損害や精神的苦痛を与え 続けている」とし「2ちゃんねる」管理人側の控訴を棄却した。

この「２ちゃんねる」は、ある時期まで書き込み者の IP アドレスなどの記録（ログ）が残らない完全匿名の状態にされていた。さらに管理者が書き込み内容への削除要請に対して容易に削除を認めなかった[15]こともあり、誹謗中傷にあたるような書き込み、住所・氏名などの個人の情報、無断で人物画像（肖像）を閲覧させる行為などが放置され、従来であれば人格権の一部として認められた各権利を侵害しているとも思われる事例が複数発生し得る状態であった。その後に高裁で控訴が棄却され、「２ちゃんねる」では 2003 年 1 月 7 日からＩＰアドレスの記録（ログ）を開始し、完全匿名ではなくなっている。

（３）個人情報を利用する社会

現在の経済取引などに見られるように、個人情報（顧客データなど）を活用する電子商取引が発展するにつれ、企業の事業展開にとって個人情報の活用は重要なものとなり、人格権は財産権としての性格が強まってきている。

厳しい競争環境の中で、企業は新たな価値創造のために、できるかぎり多くの個人情報を収集・分析しようとすることになるが、これは言ってみれば企業によるプライバシーへの挑戦が進むという事態である。個人情報の利用については、ガイドラインや保護ポリシーを設けるようになってきてはいる[16]ものの、その判断は最終的には企業自身が行うものであり、取り組みには企業格差が出てきていることから、全てが安心できる状況にあるとは言えない。また、個人情報を収集する企業側に目的外流用の意思がないとしても、一度情報が外部に漏洩した場合、第三者により悪用される可能性がある。最初は限定的な流出であっても、デジタルデータ化された情報が複製・拡散していく可能性をゼロにすることは実質的に不可能である。システム構築・運用には経済面での限界があり、防止策を技術開発だけで実施することは困難でもある。つまり、収集蓄積された情報が流出するリスクはゼロにはならないことを現実として受け

---

[15] 掲示板書き込み内容の削除行為に関しては、インターネット上の無料掲示板サービス（ネオシティ）を利用した「交通問題掲示板」での発言をめぐり、中傷発言を書き込まれたとする参加者の要請により、掲示板事業者側が該当発言を削除した事例があった。その直後に、他者が、「これらの削除行為は『表現の自由』を侵害するものであり容認できない」、「掲示板事業者ネオシティと削除要請した参加者を法的措置に訴えるべき」として原告募集の広告を出した結果、その無料掲示板サービス全体が廃業するに至った事例があった。「表現の自由」と「人格権」の衝突により、結果的に掲示板事業者が廃業するという事態に至ったものである。 http://www.web-pbi.com/fjp/index_justice.htm

[16] “情報セキュリティ”確保に関し、セキュリティポリシーの策定や実施・運用のための包括的な枠組みとして ISMS（情報セキュリティマネジメントシステム）が挙げられる。ISMS の規格としては、1999 年に英国規格協会（ BSI ）が策定した BS7799 が事実上の標準となっている。BS7799 は2つのパートに分かれ、ISMS の具体的ガイドラインを定めた BS7799-1 は、2000 年に国際標準化機構（ ISO ）によって、ISO/IEC17799 として国際標準化された。日本では 2002 年に、ISO/IEC17799 を JIS X 5080 として JIS 規格化している。

とめるべきであろう。社会においては氏名・住所などの情報をはじめ、個人に関連する様々な情報がすでに流通してしまっており、このような「情報化」の進行はいわば不可逆的である。それらの情報はいろいろな形に蓄積・加工がなされ、それらを利用することで我々の生活に種々の便益をもたらしているのも事実である。

ここでインターネットを例に、デジタル化された情報（データ）の性質と、その流通における特徴を簡単に整理してみる。まず、情報の不揮発性という点である。情報がデジタル化される以前においては、出版物をはじめ音楽データなど、各種の情報は印刷物やレコードのようなアナログデータとして流通していた。これらは、その特性として複製をするコストの低減が容易ではなく、複製の段階ごとに劣化する性質を持っていた。複写機でコピーすれば鮮明さが減少するし、音楽レコードをカセットテープなどに録音すれば音楽情報にノイズが混入（ＳＮ比[17]低下による情報の劣化）していたのである。また、記録媒体の経時による物理的な劣化もあることから、情報の蓄積・流通においては制約があり、自然に情報が揮発していた。それにより、音楽データ複製に対する著作権保護の姿勢もある程度寛容であった。　しかし、デジタル情報は複製が容易であることはいまさら言うまでもない。複製行為において、コストが限りなく小さくでき、基本的に劣化もなく、不揮発性をもつ。

次にデータ流通の特徴について見てみる。アナログ情報の流通においては、情報を紙、磁気テープなどの記録媒体に収納し、媒体そのものを流通させていたため、記録媒体自体の存在が情報の流通に大きな影響を与えていた。紙媒体であれば、収容や保存の限界を迎えた時点で廃棄され、それはすなわち記録されている情報そのものの廃棄（情報の揮発）につながった。廃棄されなくとも、時間の経過とともに記録媒体は物理的に劣化していくため、情報が読み取れなくなるなどの劣化（揮発）が生じていた。ところが、情報がデジタル化され、インターネットなどのコンピュータネットワーク上に乗ると、その情報は劣化せずに無限に複製と流通ができるようになった。このことは、デジタル化された音楽ファイルがインターネット上でファイル交換システム[18]により複製を繰り返され、知的財産権の法的闘争につながったことを見れば明らかである。この無秩序ともいえるファイルの流通システム上に一度に置かれてしまったファイルは、それを完全に消去することは不可能と言われる。情報流通の秩序が変わりつつある現在の状況において、デジタル情報の不揮発性は重要な要素である。

[17] signal-to-noise ratio (SNR): 必要な信号レベルと不要な雑音レベルの比率。
[18] インターネットを利用して、ユーザのパーソナルコンピューター間でファイルを流通させる仕組み。ファイル交換、ファイル共有システムと称され、Napster、WinMX、Winny、BitTorrentなどがある。

２－２．個人情報利用の受容と権利侵害の問題

（１）情報流通システム導入時の議論（住基ネットの事例）

個人情報をネットワーク上にのせ流通をさせる形態のシステム事例として、住民基本台帳ネットワークシステム（以下、住基ネット）導入における問題を見てみる。ただし、問題点はいくつかに分かれ、中には「プライバシー保護の観点から憲法違反」との意見もあるが、本稿では憲法解釈には言及しない。

住基ネットは、平成１１年の住民基本台帳法の改正により、それまで各市町村単位で管理していた住民基本台帳のネットワーク化を図り、新たに付与される住民票コードを基に基本４情報（氏名、生年月日、性別、住所）を、行政機関に対する本人確認情報の提供や市町村の区域を越えて流通させるものである[19]。流通させる情報の内容の是非については割愛するが、もはや政府、自治体業務の電子化の必要性は論ずるまでもないことであり、社会の潮流から見ても避けることのできない流れであるといわざるを得ない。よって、個人情報の蓄積・利用がただちにプライバシー侵害になるとはいえず、「電子化すべきでない」という意見にはあまり説得力を見出せない。基本的には電子化を行うという前提において、「どのような形態でどのような情報を流通させるか」という議論が重視されるべきであろう。

導入時における、導入推進派と導入反対派の意見を見てみると、まず推進派の意見として

- 行政事務の効率化やサービスが向上する
- 住民票取得に必要な４情報のみが流通する（だから問題はない）
- インターネットとは異なり、サーバに閉域性がある（クローズド）システムなので外部からの不正な侵入はできない
- 内部の不正利用は住民基本台帳法改正による罰則の強化で防止できる

などが挙げられている。対して反対派の意見であるが、

- 当面、住民票取得以外のメリットがなく、費用対効果の面で問題がある
- いずれ「１１桁の背番号」に納税、犯罪歴など他の情報が結合されるおそれがあり、プライバシー侵害につながるのは必至である
- クローズドなシステムであっても、設定ミスなどにより不正侵入は起き得るし、各地方自治体のセキュリティ担当の人材確保も不十分である

[19] 総務省ホームページには、「住民基本台帳ネットワークシステムは、地方公共団体共同のシステムとして、居住関係を公証する住民基本台帳のネットワーク化を図り、4情報（氏名、生年月日、性別、住所）と住民票コード等により、全国共通の本人確認を可能とするシステムであり、電子政府・電子自治体の基盤となります」と説明されている。　http://www.soumu.go.jp/c-gyousei/daityo/

- 官民いずれかの悪意により、個人情報が漏洩しても、それを防ぐための個人情報保護法等の法整備が不十分である[20]

などと危険性を主張するものであった。

また、一部の自治体が安全性に不安があるとして、住基ネットへの接続を拒否したり、情報システムとしての脆弱性を独自に検証を始め、住基ネット稼動後も継続して検証されていたことなどから、システムへの信頼感は決して高いとは言えなかったと見られる。政府側も、「絶対に安心」という表現に終始した感があり、どのようなリスクが潜在し、その深刻度がどのくらいなのかについて十分な説明がされたかという疑問も残る。

これらの点について、システム導入にあたり、情報を管理する側（国）と管理される側の間での相互信頼の形成について、３－２（１）項で考察する。

（２） 増加する監視カメラ（英国、米国、日本）

（英国、米国）

英国では、1993 年 2 月に北イングランドのショッピングセンターで発生した誘拐事件[21]が、監視行為に対する市民感情に影響を与えたとみられている。この事件について、ショッピングセンターに設置されていたビデオカメラの映像がニュースなどで繰り返し放映されたことが、一般市民が監視カメラに対する意識が変化した契機と指摘されている[22]。その後の監視カメラシステム導入事例として、ロンドンのニューハム地区のケース[23]が挙げられる。治安の悪化していたこの地区に、1998 年 10 月 14 日から監視カメラ 300 台が設置され、Visionics 社[24]の FaceIT[25]という顔認識システムが導入された。これにより、監視カメラが通行人の顔を読取り、コントロールルームのコンピュータが犯罪者の顔写真データベースと照合を行い、一致した場合にはモニターしている警備員が監視を続けるという運用がされている。この結果、この地区の犯罪発生率は 2 年間で３０％以上も低下したとされる。この地区のケースでは事前に住民にアンケート調査が行なわれ、92％が賛成したことから導入が決められた経緯がある。

---

[20]「個人情報の保護に関する法律」。2005 年 4 月より全面施行される。
[21] 2 人の 10 歳の少年により 2 歳児が誘拐・殺害された事件。
[22] http://www.privacyinternational.org/
[23] http://www.spy.org.uk/n-mandrake.htm
[24] 現 Identix 社
[25] 顔認識のアルゴリズム例としては、①カメラ画像の入力、②顔位置検出、③顔特徴点の位置検出、④特徴量の抽出、⑤照合処理、となる。http://www.face-id.jp/s03-what/s03-2.html
詳細は Identix 社のホームページを参照。http://www.identix.com/

米国では、2001 年 2 月に『第 35 回スーパーボウル』の会場となった、フロリダ州のスタジアムでも監視カメラ画像を犯罪者顔写真データベースと照合し、一致すると警察管制室のスクリーンに通報する仕組みが運用された。この顔認識システムによる監視行為は、入場者には事前に通知されていなかったため、市民団体[26]からプライバシーの侵害にあたるとして非難されている[27]。他にも、フロリダ州タンパでは 2001 年 6 月に FaceIT システムが導入された。空港におけるテロリストの活動検知のため、ダラス・フォートワース空港、カリフォルニア・フレスノ空港、フロリダ・パームビーチ空港、ボストン・ローガン空港などで同システムが導入されている。また、2001 年 9 月 11 日に発生した同時多発テロによって、人権侵害よりもセキュリティが重視される傾向が急に強まり[28]、顔認識システムの普及が促進されたとの指摘がされる。

（日本）

国内における監視カメラの設置は、銀行の店舗内、ＡＴＭ（現金自動預払機）などの不正監視のための設置が主であったが、2002 年に日韓で共催されたサッカーワールドカップを機に公共空間への監視カメラの設置例が増えてきている。警視庁は 2002 年 2 月から東京・新宿歌舞伎町一帯に 50 台の街頭監視カメラを設置・運用[29]し、同 3 月にはその監視カメラを使用して初めて摘発をしている。渋谷センター街（10 台）と池袋西口（20 台）においても設置を行い、2004 年 3 月から運用を開始している。その他にも、商店街が独自に監視カメラを設置・運用するケースや、地域住民が自主的に設置しているケースなども見られる。2003 年 7 月に長崎県で発生した男児誘拐事件では、商店街の監視カメラにより記録されていた映像が捜査の手がかりとされた事例がある。このような事例に連動するように各地で生活安全上の関心として監視カメラ設置の動きが見られる。

一方、監視される生活者の意識に目を向けると、2003 年 9 月に株式会社富士総合研究所が実施した「家庭のセキュリティに関するアンケート調査」では、「公的空間への監視カメラの設置に対する意識」に関して聞いている。その研究レポート[30]によれば、「調査で対象とした各公的空間では、『ぜひ設置して欲しい』と『設置されていた方がよい』を合わせた、設置に前向きな声が 6～8 割台半ばを占めている」とし、さらに

---

[26] ACLU（米市民的自由連盟:American Civil Liberties Union）http://www.aclu.org/
[27] http://hotwired.goo.ne.jp/news/news/culture/story/20010206201.html
[28] 2001 年 10 月 12 日に，米 Harris Interactive が行ったアンケート調査によると、86％の回答者が，テロリスト発見のために顔認識技術を使うことを支持したという。
http://itpro.nikkeibp.co.jp/free/ITPro/USNEWS/20011013/5/
[29] 警察庁は平成 12 年（2000 年）2 月に「安全・安心まちづくり推進要綱」を制定し、街頭監視カメラの設置を推進している。
[30]「治安および公的空間の防犯に関する生活者の実態と意識」株式会社富士総合研究所
http://www.fuji-ric.co.jp/research/crimeprevention040604.html

「昨今の治安情勢の悪化により、犯罪に対する不安感がプライバシーに対する不安感を凌駕している現状がうかがえよう」と報告している。しかし「街頭監視カメラが野放図に設置されて利用されれば、公的空間を利用する人々の権利や利益が損なわれるおそれがある」とも述べており、監視カメラの設置・運用に関してはプライバシーに対する不安もある。

監視カメラの設置目的をみるとき、「事前の犯罪防止」か「事後の事実確認」かという疑問が残ることとなる。前者（事前の犯罪防止）が目的であれば、監視画像を常時確認する必要があり、後者（事後の事実確認）であれば画像データの蓄積と検索が必要となる。これらの際に、個人の肖像権がどのように扱われるべきかについては具体的な議論がされていない。どこまでが社会的受容限度内なのかが不明である。

以上のように、英米、日本での監視カメラ導入事例で見るとおり、犯罪防止を目的とする監視は増える傾向にある。生活者の意識としても、公共空間への監視カメラの設置・運用に対するニーズがあり、治安面で不安のある地域ほど高まる傾向にある。一方で全ての場所で監視されることが必要ということではなく、プライバシー保護のレベルは場所によって変化すると考えられることから、安易な設置・運用が推進されるべきではなく、本来は個別に具体的な議論が必要である。東京都杉並区では「防犯カメラの設置及び利用に関する条例[31]」を制定するなど、防犯カメラの設置や利用に関する基準を定めて濫用防止を図るなどの先進的な取り組みをしている。

今後も監視カメラの設置は増加していくと予想されるが、その設置・運用においては、犯罪に対する不安感とプライバシーに対する不安感のバランスを個別に議論し、監視されることへの不安に対してアカウンタビリティー（説明責任）がより重要になるといえる[32]。

（３）Ｎシステム（自動車ナンバー自動読み取りシステム）訴訟

一方で、日本の主要道路には通行する車両を監視するカメラが数多く設置されており、中でも「自動車ナンバー自動読み取りシステム（いわゆるＮシステム：以下Ｎ

[31] 東京都杉並区では、平成 16 年(2004 年)3 月 19 日に「防犯カメラの設置及び利用に関する条例」が成立し、同年 7 月 1 日から施行される。条例は、杉並区内の「道路、公園その他規則で定める多数の者が来集する場所に防犯カメラを設置しようとする場合」には、カメラ取扱者に「防犯カメラの設置及び利用に関する基準」を定めて杉並区長に提出する義務を課している。
http://www2.city.suginami.tokyo.jp/library/file/H16_J17.pdf

[32] 監視カメラ設置に関する法律案としては、「行政機関等による監視カメラの設置等の適性化に関する法律案」が平成15年7月に提出されている。
http://www.shugiin.go.jp/itdb_gian.nsf/html/gian/honbun/houan/g15601049.htm
http://www.shugiin.go.jp/itdb_gian.nsf/html/gian/keika/1D933FE.htm

システム）[33]」については、肖像権侵害であるとして東京など５都県 13 人のドライバーが損害賠償請求を行っている。Ｎシステム導入初期の８０年代には車両前部にあるナンバープレート付近のみを赤外線ストロボ発光により照射し撮影していた。これが９０年代になると、長時間照射となり、運転者および同乗者の顔にもライトが照射されるようになったとの指摘もされていた[34]。

原告は、「不当な監視により肖像権を侵害され、行動の自由も制限される」として損害賠償請求したものの、2001 年 2 月に東京地裁は請求を棄却している。「一時的に運転者が撮影されるとしても、すぐに消去されるので、肖像権を侵害するとは認められない」というのが棄却理由である。

ここでは法的解釈には立ち入らないが、このＮシステム設置・運用に関する問題点として、設置基準や運用ルールがほとんど明示されておらず、よって逸脱を規制する手段が用意されていないことを挙げておきたい。確かに自動車のナンバープレートは公開されているものであるから撮影・記録そのものは問題がないと仮定しても、デジタルデータとして記録されたナンバープレート情報は検索が容易なことから車両トレーサビリティを発揮し、間接的に所有者の行動が監視され得るという疑念や不信感につながる余地もある。

また、システムの合理性を考えてみると、充分に説明がされているとは言い難い面が見られる。Ｎシステムはナンバープレートに表示された文字・数字を認識するものの、現状ではナンバープレートそのものの真贋を識別する機能は備えていないと考えられるため、ナンバープレートを偽造して装着された場合には、識別能力を持たないと推定される。よって、監視対象車両をリアルタイムで摘発するには、システム上弱点を包含している可能性があり、一般市民の理解を広く得る上で、より説明がなされるべきといえる。

33　「自動車ナンバー自動読み取りシステム」は警察庁が1986年から導入しており、「自動車利用犯罪や自動車盗の捜査のため」（1999年警察白書）と説明されている。設置場所は公表されていないものの、全国で600ヵ所にも上るとの指摘もされている。

34【'99 プライバシー・シンポジウムレポート Vol.1】ネット社会のプライバシー議論――“犯罪捜査と個人のプライバシー”N システムの場合はどうか?（1999 年 10 月 5 日 ）
http://ascii24.com/news/i/topi/article/1999/10/05/print/604789.html

３．情報流通システム導入と情報のコントロール

３－１　情報コントロールにおける課題

（１）個人情報の流出と損害の事例

このところ、中小、大手企業の保有する顧客個人情報、また自治体住民などの個人情報が外部に流出する事例が相次いでいる。中でも、2003 年 10 月に明らかになった、大手コンビニエンスストアの運営する会員サービスにおける 18 万人を超える会員の情報が流出した[35]とされる事例においては、流出した情報によるとみられる債権回収詐欺などの二次被害[36]も報告されている。

大手コンビニエンスストア側は流出経路について調査を行い、サービス運営会社社員が流出させた可能性と、業務委託先の従業員がデータを流出させた可能性などが有力としたものの、最終的な特定は不可能であった。結果として、大手コンビニエンスストア側は被害者へ 1000 円相当のプリペイドカードを配布（総額約１億８千万円）して収拾を図ることとなった。

また、1999 年 5 月には京都府のある自治体で、22 万人もの住民基本台帳データ大量漏洩[37]事件が発生した。乳児検診システムの開発業務を委託された民間業者の再委託先のアルバイトが、データを持ち出したうえコピーして名簿業者に売却したことに関し慰謝料の請求が行われた。そして 2002 年 7 月の最高裁判決において、住民の権利が侵害されたとして慰謝料などの支払いを命じている[38]。この裁判において自治体側は、流出した住民データは「旧住民基本台帳法 11 条によって何人も閲覧できる、公開されている情報」であると主張したが採用されず、住民票データは個々の住民のプライバシー事項と認められた。そして自治体側の使用者責任とデータが完全に回収されたものかどうかは不明[39]として権利侵害を認めたものである。

---

[35] 被害者のうち、数十名が、会員登録の際に氏名や住所に特有の記号を使用（名前の一文字を違う漢字にするなど）していたため、流出が判定された。

[36] 具体的には、これらの個人情報を利用し、会員宛に様々なところから「債権回収詐欺郵便」が届いたというものであった。無作為な電子メールアドレス宛に送信される、インターネット有料サイト利用料の督促に関する架空の請求は以前からみられていたが、氏名などを含んでいないものが多く、架空であることが判断しやすかった。しかし、氏名、住所が記載されるようになると、利用を特定できないまま支払いをしてしまう事例がみられるようになった。また、流出した情報の内容によっては、戸別訪問の名簿として利用される可能性も考えられる。

[37] 漏洩データは、住民番号、住所、氏名、性別、生年月日、転入日、転出先、世帯主名、世帯主との続柄。

[38] 一人あたり、計1万 5 千円。（1万円の慰謝料と弁護士費用 5 千円）。仮に流出名簿22万人が請求すれば、慰謝料のみで約22億円となる計算である。

[39] 流出による具体的な被害が主張立証されなかったが、「不特定の者にいつ購入されていかなる目的でそれが利用されるか分からないという不安感を生じさせた」とし、精神的な苦痛を認定した。

これらの事例を参照すると、住基ネットで流通される基本４情報が流出した場合でも二次被害が発生する可能性があり、被害感情が高まることが予想される。

その他にも個人情報の流出は多数判明している。2004 年 2 月に 32 万人分（最悪の場合 200 万人規模）の顧客情報が流出したとされる信販会社の事例、同じく 2004 年 2 月に 450 万人[40]分もの顧客（加入者）情報が流出したとされる大手サービスプロバイダの例[41]など、より深刻さを増している。このサービスプロバイダの事例では、顧客開拓を急いだこともあり、顧客データへのアクセス権限の管理が杜撰であったことが指摘され、いくつもの改善策を講じることとなった。すでに述べたとおり、企業は顧客管理のためだけでなく、迅速な経営分析やサービス開発のために顧客情報を蓄積利用するようになってきており、その盲点が突かれた形である。

（２）コントロールを難しくする技術の進歩と企業の意識

技術の進歩は、情報の管理を難しくもしている。ネットワーク化が進んだコンピュータにおいては、ネットワークを経由した外部からの不正なアクセスも懸念される一方で、内部の人間による不正な情報アクセスや、人為的ミス[42]によりによる流出など、重要な課題として対策がとられるようになってきている。

例えば、製造・開発業務においては、無断での画像撮影により機密が漏洩するのを防止するために、デジタルカメラ付き携帯電話の持ち込みを制限する動きが広まっている。情報を扱う業務分野においては、以前はデータの可搬性を持たせる点でフロッピーディスクが主流であったが、その後大容量化、小型化が進み、ＭＯ（光磁気ディスク）、ユーザによる書き込みが可能なＣＤ、ＤＶＤ媒体や、ＵＳＢ[43]インタフェースを利用したスティックメモリ媒体などが普及してきた。ＵＳＢ型スティックメモリのような非常に小型化された媒体には、特に可搬性・汎用性に優れるメリットがあるが、このことがデータを無断で持ち出す行為を隠匿しやすくすることになる。企業などではこのような変化に対応し、業務用パソコンのインタフェースを制限して情報（データ）の無断持ち出しを防止する対策も採られつつある。運用の面では、情報へのアクセスに権限を設け、業務上必要な人間にのみ必要な権限を付与、アクセスログを記録する体制をとる例が増えてきている。しかし、相次いで発生した個人情報の流出事件

---

[40] 2004 年 6 月には660万人分に上るとの報道もされている。
[41] 同年6月には、サービスプロバイダが提供するIP電話の通話記録140万件も同時に流出していたとの報道もされている。
[42] 社内のみアクセス可能とすべき顧客情報ファイル等を、外部からアクセス可能な場所（ディレクトリ）に、うっかり置いてしまうミスなど。
[43] Universal Serial Bus：コンピュータに周辺機器を接続するためのシリアルバス規格。

を受けての対応を調査したアンケート[44]では、「個人情報保護に対して企業間格差が拡がる傾向がある」との報告もされており、問題が残る。

既に述べてきたとおり、あらゆるデータがデジタル化される現在では、データの複製は簡単で高速になっているため、僅かな盲点を突く形で大規模な不正流出が起こる可能性がある。コンピュータネットワークのハードウェア、ソフトウェア両面でセキュリティ上の脆弱性を潜在する状態であり、システムとして完全な状態とは言いがたい。さらに、データにアクセスする人間の側にも問題は潜在しており、いわば運用面での人的なセキュリティホールともいえる。これに対しては、データ扱う際には、持ち物のチェック、生体認識による本人認証[45]、動作の監視など、アクセス権限を付与された人間自身の権利を制限する方向に向かう可能性も考えられる。

（3） 氾濫する ID

（ID の窃盗・盗用）

インターネットなどコンピュータネットワークの普及につれて電子商取引が普及しており、コンピュータの画面上で個人の識別 ID やログインパスワードを入力する機会が増えてきた。個人識別 ID は単なる英数字ではなく、経済的な意味を持つようになってきたのである。それに伴い、この個人識別 ID を悪用されるリスクが増加していることも課題として挙げられる。　個人識別 ID は電子メール、ISP（Internet service provider）の会員メニュー、各種電子商取引などのサービス利用において個人を特定する重要なキーである。インターネットカフェの不特定多数のユーザーが使用する端末に、キーロガー[46]と呼ばれるソフトウェアが潜入されていたようなケースでは、そのソフトウェアにより入力した ID やパスワードが記録されてしまうことになる。その記録された ID、パスワード、クレジットカード番号などの記録を他人が入手・解析し、

44　三菱総研とNTTレゾナントが2004年5月に実施した「第2回企業の個人情報保護と情報セキュリティ対策に関する意識調査」による。相次ぐ個人情報漏えい事件を受け、企業の漏えい防止への取り組みが変化したかを、企業の情報システム担当者508人を対象にインターネットでアンケート調査した結果、「従来から対策を行っていた企業と、そうでない企業の取り組みに差が広がりつつある」としている。http://research.goo.ne.jp/Result/0405cl12/01.html

45 認証に使用する生体情報として使用されるのは、指紋、掌形、顔、虹彩、血管（手の甲の静脈パターン）、声紋、署名筆跡（筆順、筆圧、形状、スピードなど）、複合型（顔、声紋、指紋、署名など）等が挙げられる。

46 キーロガー：「*ユーザーがキー・ボードから入力した一連の文字シーケンス（キー・ストローク）を記録するための仕組み、またはそのためのシステム。あるパソコンにキーロガーを仕込んでおいて、あとで記録を解析すると、どんな文字を入力したかわかる。キー操作のログ（記録）を取るものという意味で、キーロガー（key logger）という*」とされる。 http://www.pc-view.net/Help/manual/1417.html
http://www.atmarkit.co.jp/icd/root/73/48825873.html

ID 所有者本人になりすまして悪用したとみられる事例[47]が発生している。キーロガーは、もともとはコンピュータシステム開発者の作業において、入力したキーストロークを再現する目的で利用されていたが、目的外に悪用されれば、端末使用者は記録されている認識ができず、ID やパスワードが漏れることになる。コンピュータウィルスやワームの中には、キーロガー機能を備え、記録した ID などを外部に送信するものも存在する。

また、携帯電話は普及とともに多機能化が図られてきており、電話番号リストや住所、氏名などの登録機能をはじめ、電子メール、ブラウザ機能などが盛り込まれてきた。さらに、電子チケットサービス、電子マネーやＩＤ機能を持たせる研究が進められて実用化されつつある。個人の所有する携帯電話機が個人情報を蓄積する機能を有するようになることで、新たな経済的価値が創出されつつあるといえる。このことから、今後は携帯電話機の盗難が増加する可能性があることも指摘されてきていることに対応し、携帯電話機に指紋認証機能が搭載されるなどの動きが見られる。

（技術者向け管理ツール）

キーロガーの他にも、コンピュータ技術者向けのツールの悪用例として、ネットワーク管理ツールに関しても問題が指摘されている。通常、企業が LAN などのネットワークを利用する場合にはシステム（ネットワーク）管理者を置き、保守運用を任せることになる。システム管理者は、各種の管理ツールを使用して不正なアクセスやデータのトラヒックを監視し、メンテナンスなども行う。しかし、これらの管理ツールは、電子メールなどのパケットと呼ばれるデータを他者が取り込む能力があり、悪用されれば通信内容が盗み見される恐れもある。

（フィッシング）

米国では社会保障番号と自宅住所がインターネット上で購入できる[48]と言われ個人情報の保護強化の必要性が指摘されてきた。他にも 2003 年頃からフィッシング（phishing[49]：造語）と呼ばれる詐欺が増加してきている[50]。これば電子メールなどを

---

[47]「ネットカフェで暗証番号盗む －1600万引き出し 2人逮捕 窃盗容疑などー」
http://www.yomiuri.co.jp/net/news/20030306ij52.htm

[48]「*カリフォルニア州に本部を持つ『納税者と消費者の権利財団』(FTCR)によると、米中央情報局(CIA)のテネット長官やアシュクロフト司法長官をはじめ、大統領の上級政治顧問カール・ローブ氏も含めてブッシュ政権の高官の社会保障番号と自宅住所を、各人につき 26 ドルで購入できた*」とされる。
http://www.wired.com/news/privacy/0,1848,60216,00.html

[49] http://www.wordspy.com/words/phishing.asp

[50]「*インターネットにはびこる詐欺の一つで，実在する企業の Web サイトに見せかけたサイトへユーザーを誘導し，クレジット・カード番号などを入力させて盗むことを指す*」とされる。

送付して実在する企業の Web サイトに見せかけたサイトへユーザーをＵＲＬリンクから誘導し，クレジット・カード番号などを入力させて盗むことを指す。この際には電子メール上に表記されたＵＲＬは実際には偽のサイトにリンクされており、さらに一部のＷｅｂブラウザに存在したセキュリティホール[51]を悪用してサイトのＵＲＬを偽装する方法などが指摘されている。2004 年 3 月、司法省はその手口、避けるための助言などをまとめたレポートを公表[52]している。

（架空料金請求）

日本においては、架空料金請求トラブル事例の増加[53]が顕著である。警視庁ホームページによれば、「利用した覚えのない有料電話情報、ツーショットダイヤル、ダイヤルＱ２と称する情報料等を請求する手紙、はがき、電子メール等が届く」というもの[54]である。また、「業者は同一業者で、金額やお客様番号も同じというケースもあり、悪質業者が送付する相手を無作為に抽出し、根拠のない請求書を大量に送付しているものと思われます。」としており、住所・氏名もしくは電子メールアドレスが送信宛先選出のキー項目となっていると考えられる。

架空料金請求トラブルに関して総務省によれば、有料アダルトサイト等の架空料金請求トラブルの受付件数が増えている。電気通信消費者相談センターが平成 15 年度（2003 年度）に受け付けた苦情・相談のうち、有料アダルトサイト等の情報料等をかたった架空料金請求トラブルの受付件数は 4,119 件に上り、総受付件数[55]のほぼ半分（46.8%）を占めている。これは前年度（555 件）と比較すると 7.4 倍に増加している。さらには携帯電話のメールサービスを利用した新しい請求の手口に対しても注意喚起されてきている[56]。

---

http://itpro.nikkeibp.co.jp/free/ITPro/OPINION/20040306/141018/

[51] Internet Explorer（IE）のセキュリティ・ホールにより、Outlook Express などのステータス・バーに表示される URL や，IE のアドレス・バーに表示される URL を偽装できたとされる。
http://itpro.nikkeibp.co.jp/free/ITPro/OPINION/20040306/141018/

[52] 米司法省によるレポート:″Special Report on Phishing,″ Department of Justice Criminal Division, March 2004. http://www.usdoj.gov/criminal/fraud/Phishing.pdf

[53]「架空料金請求トラブルに関する苦情・相談等が7倍超に急増（平成 15 年度における電気通信サービスの苦情・相談等の概要）」（平成 16 年 6 月 8 日）
http://www.soumu.go.jp/s-news/2004/040608_1.html

[54] 内容例としては、「有料アダルト番組提供会社から未納利用料金の債権譲渡を受けたと称する債権回収業者より、はがきやメールで利用料金の請求を受け、期限までに入金されなければ自宅まで請求に行く、その時は交通費も含めて請求する。」というもの等
http://www.keishicho.metro.tokyo.jp/seian/kougaku/kougaku.htm

[55] 電気通信消費者相談センターに寄せられた苦情・相談等の総受付件数の推移として、平成 11 年度:3,593 件、平成 12 年度:4,741 件、平成 13 年度:7,383 件、平成 14 年度:7,495 件、平成 15 年度:8,796 件となり、平成 13 年頃から急激な増加を見せている。

[56]「携帯電話事業者が提供する一部のサービスを利用して送られてくるメールに記載されたURL（出会い系サイト、アダルトサイト等）にアクセスした際に、「入口」等のボタンをクリックしただけで契約が成

（スパムメール）

電子メールアドレスは、個人とインターネット上のアイデンティティを結びつけるキーの一つであるが、その電子メールアドレスが企業などによって収集され、従来は郵便（ダイレクトメール）により行われていたマーケティングのための販売促進が、電子メールを通じて行われるようになった。このような本人意思によらないメールが氾濫するにつれ、スパム（spam）メール[57]と呼ばれるようになった。既出の架空料金請求メールもスパムメールに分類される。スパムメールはインターネットのトラヒックを無駄に増加させネットワーク資源を浪費することから、ネットを危機的な状況に向かわせているという指摘がされてきている。

（4）電子タグによるトレーサビリティの問題

ＲＦＩＤ[58]技術を利用した電子タグが近年特に注目を集めている。情報を記録したICチップを商品などに付け、電波や磁気で情報を読み取ることにより、商品情報の提供や、商品の追跡管理などの利用法が想定されている[59]ものである。これまで流通過程における情報記録手段としては、作成コストの安価なバーコードが多用されてきたが、それを上回る能力があるとして期待されているのが電子タグである。この電子タグの価格が低下するにつれ、具体的な商用での導入が見えてきつつある。米国などではすでに流通分野など一部での導入が始まっているところであるが、消費者のプライバシーを侵害するものとして非難もされている。例えば、電子タグの非接触で読み取り可

立するような利用規約を定め、当該契約に基づき入会金、会費等を請求してくるトラブル」に関する相談が増加しており、総務省は、平成16年4月21日にメールに記載されたURLへ不用意なアクセスをしないように注意喚起を行った。http://www.soumu.go.jp/s-news/2004/040608_1.html

[57]「 *WWW やNetNews などを通じて手に入れたe-mail アドレスに向けて、営利目的のメールを無差別に大量配信すること。インターネットを利用したダイレクトメール。インターネットではメール受信のための通信料は受信者の負担になるため、SPAM メールのように受信者の都合を考慮せず一方的に送られてくるこうしたメールは、極めて悪質な行為とされている。また、SPAM 行為は同内容のメールを一度に大量に配信するため、インターネットの公共回線に負荷がかかる点も問題となっている。最近はiモード携帯電話など、インターネット接続機能を持つ携帯電話に対するSPAM が社会的な問題になっている。*」とされる。http://e-words.jp/a/E382B9E38391E383A0E383A1E383BCE383AB.html

[58] RFID：Radio frequency identification。一般的には、RFIDとはID情報を埋め込んだタグから情報を無線によってやりとりする技術全般を指す。JR東日本の定期券Suica（スイカ）などの非接触ICカードも、同様の技術を用いている。

[59] 経済産業省ホームページによれば、「*電子タグとは、商品などの情報を記録したICチップをつけて、電波や磁気で情報を読み取るもので、消費者に商品の出所を情報提供するための商品の追跡管理（トレーサビリティ）や商品の低価格での提供を可能とする流通の効率化・効率的在庫管理（サプライチェーンマネージメント）に役立つものとして大きな期待が寄せられています。*」と説明されている。

能である性質はまだ広く理解されておらず、情報の取得・利用など運用のルールも詳細には議論されていないなどの点が問題として指摘されてきた。

そのような問題に対し、国内においては、平成 16 年（2004 年）6 月 8 日、経済産業省と総務省の協同により、電子タグを活用する事業者に向けた「電子タグのプライバシー保護に関するガイドライン」を策定、公表された。その中では、「商品に電子タグが装着してあることを表示すること」、「電子タグの読み取りが出来ないよう消費者が選択できるようにすること」などをはじめとするガイドラインが示されている[60]。

（5）利用履歴の集積とセンシティブ情報開示の可能性

書籍、音楽ＣＤや映画のＤＶＤ等を扱うインターネット通販サイトにおいては、顧客ごとに書籍の検索履歴や購買履歴がサーバーに保存され、販売活動に利用されるようになっている。例えば、ある顧客が書籍をオンラインで注文しようとするとき、その書籍名、ジャンルなどを元にして、サイト側はさらにお勧めの書籍を画面上に提示し、さらに顧客購買単価を上げようと工夫している。この時には他の顧客の購買傾向を蓄積・分析するなどした結果も反映されている。さらには、一度顧客が購入した商品履歴は蓄積されており、マーケットプレイスと呼ばれる中古品を流通させるサービスと連動され、それらを出品した場合の概算の販売額なども表示されるようになっている。これらは一見便利にみえるものの、購買や検索の履歴から顧客個人の嗜好性が収集・分析でき、限りなく蓄積されていくことが考えられる。このようなデータの蓄積は、住所・氏名のような基本的情報よりさらに私事性を増したセンシティブな情報であり、それらが目的外に利用されれば、被収集者個人の嗜好や思想信条が推定される手がかりになると懸念する声もある。現在のところは、利用するユーザー側が、通販サイトの情報管理をある程度信頼していることで成立している関係と思われる。こうした購買顧客に関するデータは多くの企業が収集したい項目となっていることから、情報の流出や承認のない目的外の流用には特に厳格な運用が必要と考えられる。

---

60 「電子タグのプライバシー保護に関するガイドライン」（平成 16 年 6 月 8 日公表）においては以下のような点が示されている。

- 電子タグが装着してあることの表示などの義務付け
- 電子タグの読み取りに関する消費者の最終的な選択権の留保
- 電子タグの社会的利益等に関する情報提供
- 電子計算機に保存された個人情報データベース等と電子タグの情報を連係して用いる場合における取扱い
- 電子タグ内に個人情報を記録する場合における情報収集及び利用の制限
- 電子タグ内に個人情報を記録する場合における情報の正確性の確保
- 情報管理者の設置
- 消費者に対する説明及び情報提供

http://www.meti.go.jp/policy/consumer/press/0005294/0/040608denshitagu.pdf

３－２．今後の課題

（１） システム導入における相互信頼の形成（リスクコミュニケーション）

（ｉ）リスク、コスト、ベネフィットのトレードオフ

リスクコミュニケーションを考えるうえでリスク情報とベネフィット情報の両面を捉えていく必要がある。新しい技術を企業や社会などへ導入する場合、それにより発生（または増加）するであろうリスクと、もたらされるであろうベネフィットに関して評価・判断をする必要があるのはいうまでもない。

科学技術や人間の諸活動はさまざまなリスクを伴うものであるが、同時にベネフィットもさまざまなものとなる。リスクとベネフィットの間にはトレードオフ性があり、あるリスクを削減するとベネフィットも失われることになる。他方、コストに着目すれば、コストとリスクにもトレードオフ性があり、リスク削減のためにはコストが必要になる。さらに、リスクだけをみても、発生し得るリスクというのは多数想定され、その中でどのリスクを選択すべきか判断するという、リスク間のトレードオフもある。

リスク、コスト、ベネフィットなど全てを評価し、かつ技術やシステム導入の可否を判断する際には、２つの段階が存在すると思われる。第一の段階は、科学者等による専門的な視点からの冷静な判断である。この段階では、できる限り定量的データに基づき、技術などに関する評価を行わなければならない。第二段階としては、技術やシステムを受け入れる側（社会）の判断である。この段階でもデータに基づいた冷静な判断が求められるが、専門家のような検証は難しいため、技術的・科学的視点によらない様々な思想・信条などに基づく価値観が介入してくることになる。

これまでのリスクに関する情報提供として、原子力でのＰＡ（public acceptance）が挙げられるが、送り手である行政や企業が質・量ともに圧倒的であることを利用したものという側面もあり、一方向性が強いことから限界があるとも指摘されている。現在の社会状況として、情報開示やインフォームド・コンセント等が重視されてきている。このような多様な価値観に基づく受け入れ側の感情（社会的感情）に対しても、十分に情報を提供し、公正な手続きを経て、合意を得ることが必要であると考えられる。

（ⅱ）住基ネットでのリスク、コスト、ベネフィット認識

リスクコミュニケーションの観点から、前述した住基ネット導入事例について、住民からみたベネフィットへの理解と、リスク受容の問題について考えてみたい。

主な反対意見としては、

① 費用対効果が疑問
② 将来的にプライバシーが侵害される恐れ
③ システムの安全性への不安
④ 法整備の不備

等が提示されていた。①についてはシステムコストとベネフィットの関係、②はプライバシー侵害リスク、③はシステムそのものの安全性、④は法制度を問題にしたものである。ここから、主に①、②、③に関して、リスク、コスト、ベネフィットの面を考察する。

＜リスクの認識：システムの安全性とプライバシー侵害への不安＞

この場合のリスクの認識においては、技術面でリスクと感情面でのリスクがあると仮定してみる。

まず、技術面の不安を生む原因のひとつに、住基ネットも採用しているＯＳ[61]（Windows、unix）や、関連するソフトウェア等のセキュリティホールによる脆弱性の存在がある。総務省では定期的に（危険度の高いものは随時）パターンファイルを全団体に配布するとしているが、運用開始後にセキュリティパッチが適用されていない端末があったことも報告されており[62]、全国自治体すべての端末を完璧に管理することは難しい。さらに、脆弱性の発見・公表は恒常化しており、セキュリティに対する不信感を形成している点は否定できない。

次に、感情的不安についてであるが、住基ネットでは、技術的な不信感（基本となるＯＳのセキュリティ問題ほか）に加え、感情的不安を打ち消すだけのベネフィットが感じられないのではないか。

システム導入のリスクは、コンピュータネットワークにある程度の知識がある人とそうでない人では受け止め方が違う。一定以上の知識があれば、技術的問題の範囲と深刻度をある程度は具体的に類推できるであろうが、知識（情報リテラシー）があまりない場合には、マスコミ等の問題点ばかりを指摘した報道で不安を過剰に煽られかねない。これらの点が、住基ネット導入において生産的でない議論が発生する理由の一つであったと考えられる。

---

[61]「*オペレーティングシステム：キーボード入力や画面出力といった入出力機能やディスクやメモリの管理など、多くのアプリケーションソフトから共通して利用される基本的な機能を提供し、コンピュータシステム全体を管理するソフトウェア。「基本ソフトウェア」とも呼ばれる。*」
http://e-words.jp/w/OS.html

[62]「『住基ネットにつながる庁内 LAN に脆弱性』, 長野県の実験結果で判明」（2003/12/16 日経 BP 社） http://itpro.nikkeibp.co.jp/free/SI/NEWS/20031216/137579/

不信感という社会感情の例として、原子力分野での事故情報の隠匿により醸成された不信感[63]が挙げられるであろう。その他にも、遺伝子組み替え農作物（GMO: Genetically Modified Organisms）に関して、第一世代の遺伝子組み替え農作物は除草剤耐性、害虫抵抗性など、生産者の側の便益のためのものであり、消費者側には訴求できるベネフィットがなかった。このため、一般消費者は少なからず否定的な感情をいだいているという見方[64]もある。

リスクがゼロにできるかと考えてみるとき、新たな技術を導入する場合には、得られるベネフィットとあわせて何らかのリスクが発生する。医薬品でいえば、薬効と副作用の関係にあたるものである。つまりリスクがゼロであることは有り得ないことを認識しなければならない。発生しうるリスクを限りなくゼロにしようとするならば、すべての行動が排除されてしまうからである。重要なのは、発生しうるリスクと、ベネフィットとのトレードオフを冷静に評価、判断することであり、この点を忘れると単なる感情論となり、議論は前進できないことになる。

＜コストとベネフィットの認識＞

住基ネット導入による住民への便益として、行政事務の効率化やサービスの向上がアピールされている。第１次サービス（2002 年 8 月 5 日以降）では「住民票の写しの添付省略」や「現況届の原則廃止」などが提供され、つづく第２次サービス（2002 年 8 月 5 日以降）では「住民票の写しの広域交付」「転入転出手続の簡素化」「希望者への住民基本台帳カードの交付」などがメニュー化されていた[65]。総務省は、住基ネットの構築、運営コストとして、構築コスト約 365 億円、運用コストが一年あたり 189 億円と見込んだ。住基ネット導入によるベネフィットとしては、行政側の手続き簡素化などによる経費節減で約 240 億円、住民側の手続き省略などで約 267 億円を見込めると試算していた。導入に際して、住民へベネフィットを訴求できたのかという疑問について、短期的視点と中長期的視点に分けて考えてみる。

まず、短期的視点であるが、住基ネットの運用により、パスポート交付や恩給受給において、行政機関への申請や届出に住民票の写しが不要となるメリットが謳われた。しかし、住基ネットシステム上で代行される業務に関して、市民が享受できるメリットを実感するには、日常の中でなされる頻度が高いイベントであることが必要である。実感として、パスポート申請は 10 年に一度で済むことから、一個人の生涯においての

---

[63] これは、95 年末に起こった動力炉・核燃料開発事業団の高速増殖炉の事故の際に、ビデオなどの情報が隠匿され、それまで「安全です」とアピールし続けてきた信頼感を損なうこととなった。

[64] （興銀調査:「植物バイオの「現流」」を探る　ー岐路に立つ遺伝子組み換え農作物 http://www.mizuhocbk.co.jp/pdf/ibj/1020_05.pdf）

[65] http://www.soumu.go.jp/c-gyousei/daityo/

申請イベント回数としてはそれほど多いとは言えないであろう。住民票の交付申請の頻度についても、個人による差が大きく、住民票の交付をそれほど必要としない住民が多いとすれば、直接的な便益の実感が薄く感じられることが考えられる。どちらかといえば、第１次、第２次サービス[66]での提供メニューは、住民側のベネフィットというより、行政側の情報システム化とネットワーク化を進める目的が主として認識され、住民が感情的に抱くリスクを、享受できる（と理解される）便益が上回っていないと捉えられたのではないだろうか。

ベネフィットの分かりやすさという点も重要である。住基ネット導入によって各種年金の現況届等が不要になり、従来年１回必要であった生存確認のための届出がシステム上で可能になっていくことも挙げられた。つまり、①年金支給機関は現況届等を年金受給者に郵送し、②受給者は現況届等に記入し、年金支給機関へ郵送、③年金支給機関は郵送された現況届等を受け付ける、という従来の一連の確認行為がシステム上で代行されることになる。これにより、支給機関側では発送作業、郵送代金[67]、受付け作業が省略でき、受給者側も記入作業、発送作業と郵送代金が省略できることになるから、支給機関、受給者ともにメリットを享受でき、実感もより高くなるはずである。加えて、郵送代金の削減というコストメリットだけでなく、支給機関側は発送・受付における負荷が減少するのであるから、その人員を再配置するなどしてコスト削減を目に見える形で実現していく必要があるのは言うまでもない。これらの点が市民に十分に説明され、かつ理解されないと、前述の遺伝子組み換え農作物のような、提供側の都合による改変としか認識されないのではないだろうか。

つぎに中長期的視点では、政府や自治体の電子化による行政事務の効率化は避けては通れないものであろう。そのためのシステムとして、いかに効率化に寄与するかが問われることとなるはずである。民間企業では良くも悪くも“リストラが必要”といわれて久しい。住基ネットが「行政リストラのためのツール」であるということを政府や自治体が自ら約束し、住民に認識されればベネフィットとして認められるようになるのではないだろうか。

---

[66] 2002年8月からの第１次稼動では、行政機関にパスポートの発行申請など各種届出などを行う際、住民票の写しを添付しなくても良いようになった。2003年8月25日からの第２次稼動では、さらに、住民票の写しが全国のどの市町村でも取れるようになるほか、希望者には、身分証明書にも使える「住民基本台帳カード」が発行されるようになっている。

[67] 年金給付対象者は年間3500万人（平成 15 年）に上るが、対象者には生存確認が毎年必要となる。この事務に、年金支給側（国）では80円の封書等、受給者は住民票の写し一通300円（2004 年横浜市の例）、郵送代金50円等の経費が必要。これから試算すれば、郵送料金のみで支給側で 28 億円（80 円*3500 万人）、受給側で 17.5 億円（50 円*3500 万人）が削減され、さらに受給側が負担する住民票の写し発行料金 105 億円（1 通 300 円として、300 円*3500 万人）が毎年削減できることになる。

（２） 生体情報などセンシティブ情報の利用

個人のセンシティブ情報（機微情報）に企業の関心が高いのは既に述べたとおりである。個人の趣味、嗜好にはじまり、より詳細で機微性の高い顧客データへのニーズは高まってきていると考えられる。また、バイオメトリクス技術などにより収集可能な生体情報にも関心が高まることが考えられる。

前述した監視カメラによる顔認識においても、顔の画像から特徴点と呼ばれるデータを抽出してデータとの照合を行うことから、この特徴点データの収集・蓄積についてどのように取り扱うかが未知の問題点である。特徴点によりある程度の精度をもって本人特定ができるとした場合、従来の肖像権との関係をどのように扱うべきであろうか。

医療分野においても、診療カルテの電子化など病院業務に変化が見られる。さらに、医療機関、検査機関などで個人のDNAのような遺伝情報を扱う機会も増えており、その取り扱いについては倫理指針が策定され[68]、収集蓄積や利用などを制限している。しかし、ヒト・ゲノム（人間の遺伝情報の総体）解析研究プロジェクトが世界的に展開されたように、情報としての経済価値が高まっていることから、厳格な運用が必要である。2004年５月に、「*シュワルツェネッガー・カリフォルニア州知事がなめた*」とされる「のどあめ」が、米インターネットオークション大手のイーベイに出品され落札されたという事例がある[69]。

DNA鑑定のための試料採取は比較的簡単[70]であり、企業だけでなく、一般の個人が他人の情報を取得することができる。このような、第三者により個人のDNA情報が取得される事態の増加も懸念される。このような生体情報が分散して蓄積されれば、それらが結合利用される可能性もあり、より深刻な事態を招きかねない。

（３） 情報コントロール能力

個人が自己の情報コントロールしようとする時、方法としては、技術的な解決、法規制での解決、運用（ユーザ教育など）での解決が考えられる。特に運用面では、情報を取り扱う際の意識による影響が少なくない。

---

[68]「ヒトゲノム・遺伝子解析研究に関する倫理指針」（平成 13 年 3 月 29 日、文部科学省・厚生労働省・経済産業省合同により告示）
http://www.mext.go.jp/a_menu/shinkou/seimei/genomeshishin/html/rinri_shishin.htm

[69] はじめ、「*シュワ氏のDNA*」として出品されたが、「人体の一部は売買の対象にできない」というイーベイの規定に違反するとして削除された。しかし、名目を変え、「*シュワ氏ののどあめ*」としてコレクター向けに再出品されたという。5月30日に US $15,099 で落札されている。

[70] 鑑定企業によれば、「通常の DNA 鑑定においては、頬の内側の口腔粘膜を綿棒で採取すればよく、鑑定に十分な DNA をそこから得られる」としている。

自己情報の取り扱いに対する、不安などの感覚には個人差がみられる。たとえば、「便利になればよく、プライバシー保護はあまり心配しない」、「便利さも大事だが、プライバシー保護も重要」、「便利さよりもプライバシー保護が重要」などのように多様な意見に分かれることが予想される。また、技術が高度化しているため、該当技術分野の専門知識を備えた者でないと、各種のシステムの技術的見地での安全性判断はかなり困難である。顧客（消費者）が自己の情報を企業等に預ける際には、企業側からの説明を鵜呑みにしがちであり、規約などを詳細に確認しないことも多いようである。企業側においても、預かる情報がどのような重要性、私事性を持つかの明確な指針を細部に渡って提示することはあまりなく、「充分に配慮して取り扱う」といった曖昧な記述にとどまるケースが多く見られる。しかしながら、すでに述べたとおり、個人の情報をまったく開示せずに生活していくことは非現実的な解である。社会における各種サービスは、すでにある程度の個人情報を開示することを前提に成立しているからである。ある程度の開示をしつつ、プライバシーの保護に関する視点から見た場合に問題となるのは、本人が意図しない個人情報が流通してしまう場合である。この問題への対応として一つの例を挙げれば、受けるサービスに応じて、どこまで詳細な情報を開示するかという、いわばＳＬＡ（Service Level Agreement）[71]のような考え方が求められるであろう。このところ国内ではユビキタス社会を標榜した取り組みが各所で進められているが、そこでは個人の属性情報などを、さまざまな場所に組み込まれたセンサーが読み取り、利用することでトレーサビリティも向上していくことから、プライバシー侵害リスクも増えていくと予想される。プライバシーに配慮しつつサービスの品質を確保するためには、システム設計においてＳＬＡは不可欠であり、同時に情報コントロールに関する個人への教育も重要になる。

一方で、Napster[72]に始まるP2P（PtoP）[73]という、いわば従来の秩序によらないデータ流通の仕組みが存在していることも問題点の一つである。これらはファイル交換ソフトやファイル共有ソフトと呼ばれ、個人ユーザーのコンピュータ間を直接結びつける仕組みであり、米国ではNapsterなどが社会問題化した。この流通の仕組みにデータファイルが乗せられると、違法なコピーが繰り返されることになる。日本でもWinnyと

---

[71] SLA（Service Level Agreement）：通信事業者などが、利用者に対してサービスの品質を保証する制度。個々の顧客に対して一定の基準値を守ったサービスの提供を保証し、基準を下回った場合には補償などが行われる。

[72]「*1999 年 1 月に発表された、インターネットを通じて個人間で音楽データの交換を行なうアプリケーションソフト。..流通している音楽データの多くが市販の CD などからの違法コピーであることから、Napster 社が全米レコード工業会(RIAA)に事実上の運営差し止め(著作権つき楽曲データの発見と排除)を求めて提訴されるなど、社会現象化した。*」http://e-words.jp/w/Napster.html

[73] P2P（PtoP）：(Peer to Peer)。「クライアント-サーバモデル」の対比にあたる用語で、多数の個人を直接接続して情報を共有する「PtoP」(Peer to Peer)と呼ばれるインターネットの新しい利用形態を示す。Napster が PtoP を提示した初めての大規模なサービスとされる。Napster はその後停止に追い込まれたが、Napsterのプロトコルを利用/拡張したWinMX等が今も稼働している。

いう流通の仕組みが一人の技術者により開発され、その匿名性などにより違法な複製を助長するとされた[74]。これらのファイル流通の仕組みは個人ユーザーの間を結ぶ仕組みであり、ユーザーが意識しないうちに違法なデータを所有することにもなり得る。個人のアイデンティティに関する情報がファイルとして流通することも危惧され、複製が繰り返される事態になれば、プライバシー保護の観点では重大な問題となりかねない。

ファイル交換（共有）システムの広がりについて、「（自分は）ファイルを他人に広めて著作権を侵害するつもりはないが、自分だけはファイルをコピーして利用したい」という意識の甘さがあると言われることがある。違法性のあるシステムが利用されないために、このような意識の改革は必要である。センシティブ情報の扱いについても、個人の情報に対する意識や倫理観の醸成は全ての問題解決の根底をなすものであろう。

４．　まとめ

以上、社会が情報化するなかで個人情報の利用は進んでおり、同時にプライバシー概念も変化してきている。また、生活安全上のセキュリティが重視されるのも世界的な傾向となってきており、個人を識別する技術の導入はますます進む状況にある。情報化に反対する意見もあるが、基本的には不可逆な流れであることを前提として、コスト・リスク・ベネフィットのバランスをとるための生産的な議論がされていくべきである。

情報化リスクの議論に関しては、個人情報の集積と流出のリスクや、もはや個人情報を利用しない生活が成り立たないことなどについて、繰り返し触れてきた。企業などは、個人情報を集積することで経済的価値を探求しており、ひとたびその情報が流出すれば無視できない二次被害も発生するようになってきている。住基ネットでいう「基本４情報」程度の内容であっても、それらは、「みだりに他人に知られたくない情報」で、「不特定の者にいつ購入されていかなる目的でそれが利用されるか分からないという不安感が生じる」という判断が、これまでの法的見解において示されていることも念頭におくべきであろう。進歩する技術は、メリットを生み出すと同時に、悪意の行為を助長する面も持っていることも常に指摘されるとおりである。コンピュータネットワークに関しては、「管理するためのツール」の存在そのものが脆弱性にもなり得ていることにも触れてきた。システムを導入・運用するにあたっては、技術

[74] 2004 年 5 月、著作権法違反を幇助するとして、開発者が逮捕されている。Winny は、「WinMX」で著作権法違反による逮捕者が出た後の 2002 年以降に急速に普及した P2P ソフト。

的に100％の安全は有り得ないことを理解し、妥当な受容レベルの設定が必要となる。

さらに、システム導入においては、利用者がリスクを受容するためにベネフィットを創出しつつ十分な理解を得ることが必要であることについても述べた。今後はさらに情報化が進み、よりセンシティブな情報が収集され利用される局面にあるが、倫理的な面などまだ議論の余地がある。新たなベネフィット創出のためには、個人情報の利用が欠かすことができない事実があり、そこではＳＬＡのように、享受するサービスと情報の開示レベルのバランスをとることが重要である。個人情報のコントロールにおいては、本人を含めて情報を取り扱う人間の問題も大きく、情報に対する意識や倫理観の確立も今後の重要な課題である。

＜参考文献＞

・ 船越一幸、「情報とプライバシーの権利」、北樹出版、2001.
・ 岡本浩一、今野 裕之、 「リスクマネジメントの心理学」、新曜社、2003.
・ 広田すみれ、坂上貴之、増田真也、「心理学が描くリスクの世界」、慶応義塾大学出版会、2002.
・ 白石孝（編），小倉利丸（編），板垣竜太（編）、「世界のプライバシー権運動と監視社会」、明石書店、2003.
・ 田島泰彦、斎藤貴男、「住基ネットと監視社会」、日本評論社、2003
・ Simson Garfinkel、橋本恵（訳）、「暴走するプライバシー DATABASE NATION」、ソフトバンクパブリッシング、2001.
・ 独立行政法人通信総合研究所（編）、東京大学社会情報研究所（編）、「世界インターネット利用白書」、NTT 出版、2002.
・ 岡田朋之（編）、松田美佐（編）「ケータイ学入門」、有斐閣、2002.
・ 岡村久道、「迷宮のインターネット事件」、日経 BP 社、2003.

広木　功（ひろき　いさお）

NTT 東日本より出向。
平成元年茨城大学工学部卒業。平成元年日本電信電話株式会社（NTT）入社。ネットワーク設備保守部門、同設備設計部門、法人営業本部を経て、平成 14 年より世界平和研究所主任研究員。

広木　功（ひろき　いさお）

NTT 東日本より出向。
平成元年茨城大学工学部卒業。平成元年日本電信電話株式会社（NTT）入社。ネットワーク設備保守部門、同設備設計部門、法人営業本部等を経て、平成 14 年より世界平和研究所主任研究員。