成蹊大学理工学研究報告
J. Fac. Sci. Tech., Seikei Univ.
Vol.46 No.2 (2009) pp.69-80
（研究報告）

情報通信（ICT）技術の進展と法律問題（その２）

村上　仁己*1，尾形　哲志*2，樋口　政和*3，川崎　秀二*4

Development of Information and Communication Technologies and Its Impact on Legal Issue (2)

Hitomi MURAKAMI*1, Satoshi OGATA*2, Masakazu HIGUCHI*3, Shuji KAWASAKI*4

ABSTRACT：While the computer network is now indispensable in various aspects of our daily life, several problems are at the same time arising since the progress of Information and Communication Technologies (ICT) is too rapid for human philosophies, guidelines or rules to catch up with. The problems include copyright infringement to multimedia contents, invasion of privacy, security, and so on. In this series of papers, the authors are discussing the legal impacts caused by such ICT. Focusing on copyright problems, the legal impacts that development of ICT raise have been discussed in the previous paper. In this paper, we discuss the invasion of privacy in the internet society and related legal issues from two points of view, the leak of personal information and the privacy invasion.

Keywords：Internet, Privacy, Personal Information, Street view, N system

（Received September 24, 2009）

１．まえがき

「いつでも・どこでも・だれでもがコンピュータ・ネットワークを利用・活用しうる社会」。ICT 技術の進展によってもたらされたこのユビキタス環境は，社会事象の隅々にまでその影響を及ぼし，われわれの日常生活は良きにつけ悪しきにつけ，コンピュータ・ネットワークの利用なしには成り立たなくなってきている。その意味では，ネットワークは，すでに現在社会の基礎的なインフラストラクチャーと言っても過言ではない。

ネットワーク社会の進展は，情報の敷衍化，即時性，利用の簡便性など多くの利点，有用性を生み出す一方で，これまでには考えられなかった数々の解決を迫られる問題をも生じさせている。それらの問題は，社会のルールとして存在し，利害対立の解決手段としてきた「法」の想定する範囲をも超え，新たな社会規範を要請することになっている。前稿では，解決がせまられる課題として①プライバシーの保護の問題②知的財産権等との問題③電子商取引ルールの確立と電子マネーの問題④違法・有害情報，迷惑メールなどの問題⑤情報セキュリティの確保－－ の五つの課題に整理し，その内，②の知的財産としての著作権に焦点を当てて技術進歩と法律の関係を論じた[1)]。

前回取り上げた著作権の問題では，画像や音楽の記録がレコードやビデオテープなどのアナログ媒体から CD, DVD といったディジタル記録の媒体に変わり，品質劣化のない複製を可能にした技術進歩が著作者などの権利を侵害する可能性，そしてその対応としての著作権保護方策を取り上げた。技術進歩によって従来の考え方では創作者等の権利保護が難しくなっている状況に対して，法律等の規制をどのように作り直し，技術進歩によってもたらされた有用性を生かしつつ創作者などの権利をいかに保護するかが主題であった。ところが実際に行われた解決方策は，技術の進歩によって得られた画質や音質の保持また再現性の活用という利便性・有用性を制限し，その制限の実効性を担保する技術を要請するという弥縫策に終始した。これは，著作権保護すなわち従来の課金方式という考え方を所与のものとし，技術進歩による新たな事態を，従来の枠組みの中で処理するという後ろ向きの解決であった。本来，目指さなければならないことは，それが社会あるいはまた日常生活にとって有用性のある技術進歩であるならば，この成果を生かす方向での

*1：情報科学科教授 (hi-murakami@st.seikei.ac.jp)
*2：コア・マネージメント(株)代表取締役
*3：情報科学科ユビキタス研究室研究員
*4：情報科学科ユビキタス研究室客員研究員

新たな秩序作りである。

最近盛んに問題とされ，今回のテーマとして取り上げるプライバシー保護の問題も，技術進歩により顕在化し社会的に大きな問題となっているという点では，問題のあり様は前回論じた著作権の問題と同様である。

現代社会においては，個人の活動領域や範囲が拡がることによって要求が多様化し，これに応える社会制度も多岐にわたり整備されることなる。この各種社会制度の設計・構築に必要不可欠となるのが，要求の整理・分析であり，制度要求のよって立つところの個人の各種属性情報のデータ化である。ディジタル情報あるいはネットワーク技術の進歩は，これら情報の収集，蓄積，分析，移動などをきわめて簡易化した。集積された情報は，公的利用に留まらず経済活動全般にその利用の幅を広げ，作成されるデータベースそのものの価値をも高めた。

社会的な有用性を高めた情報集積，分析技術は，同時に個人のプライバシー問題を顕在化させる。情報の経済的価値が高まることが情報の漏洩を誘発し，情報の移動の簡便性が大量かつ頻発する事件・事故を起こすことに繋がった。有用な技術と，その技術に派生して起きる「負の事象」とも言える問題をどのようにコントロールするかが，今回のテーマである。

２．情報技術の進歩とプライバシーの保護

これまで，わが国ではそれほど大きな問題とは捉えられず，社会的な要請とも認識されてこなかった「プライバシーの保護」が，技術の進歩によって「個人情報の漏洩」という問題を産み，それによって「権利としてのプライバシー」の問題が顕在化した。

プライバシーの保護として論じられる問題は，大きく分けて二つの分野がある。一つは個人情報保護法に代表される諸法規が対象とする「個人情報データベース」という個人の属性情報等の漏洩などを巡る問題であり，他の一つは，グーグルストリートビュー等で問題とされた覚知なく見られている，あるいは ID タグ等による位置情報で行動を他者に把握されているなどの「個人生活への侵害」が主張される問題である。

本稿では，この二つの分野ごとに問題とされる現象，基因，技術的解決の可能性を論じていくこととするが，その前提として，問題とされるプライバシー権とはどういう権利なのかをまず整理しておくことにする。

2．1　プライバシー権

プライバシーという概念は，もともと近代以降の社会思想の中で生まれた「独立した個人」という概念に依拠する。独立した個人が自律的人格として存在するためには，一定の私的領域の存在が不可欠であり，プライバシー権とはその「私的領域を自らが保持する権利」を指すものと解せられる。

プライバシーという言葉が日本で登場したのは，三島由紀夫の『宴のあと』という小説を巡る裁判（注１）によるものとされており，この裁判を契機に日本においても個人の私生活を他者の目から秘匿したり干渉を排除することを個人の権利として認めるという主張が一般化した。この時点で認知されたプライバシー権，すなわち「個人の私生活に関する事柄を他者に秘匿しまた干渉されない状態を要求する権利」は，現在「伝統的（古典的）プライバシー権」と称される。

プライバシー権の概念も時代の要請により変化していく。変化する要因の一つは，個人の情報が自らの見聞き出来る範囲を否応なく逸脱していくという問題である。例えば，医療の分野を考えてみても，過去には担当する医師にのみ知られていた身体や疾病の情報が，現在では医療保険のレセプトにおいて医師・患者以外の第三者に知られることになる。「個人の私生活に関する事柄を他者に秘匿する」権利の主張は事実上破綻せざるを得ない。さらに，IT 技術の進展によって，コンピュータが情報を大量かつ簡便に処理・保管でき，情報通信ネットワークにより情報の移転が容易に行えるようになった。ここに至り，プライバシーの権利は，「ひとりで放っておいてもらう権利（the right to be let alone）」から，自己に関する情報をどのような内容で，どのような場面，時点で他者の利用に委ねるかを自らのコントロール下に置き決定することは当事者の権利，とする考えに変容する。

「自己情報コントロール権」とも「積極的プライバシー権」とも呼ばれるこの権利は，前記の「伝統的（古典的）プライバシー権」の発展概念とされ，プライバシー権の中心的概念とするのが通説となっている。具体的な例を示せば，国や地方自治体などの公的機関あるいは企業により集められ管理されている個人情報に関し，情報の当事者である個人がその管理・運用また情報の的確性等に対しコントロールする権利である。

この権利の内容をとりまとめ，その後の各国の法制化に影響を与えたのが，1980 年 9 月に OECD（経済開発協力機構）が採択し，後に「プライバシー・ガイドライン」と呼ばれるようになった「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に関する理事会勧告」（Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows

of Personal Data）である。OECD がこのガイドラインを作った目的は，情報化の国際的な流れの中で，各国間に情報コントロールの差による問題が発生することを防止し，併せて個人情報保護の法制化を促すことにあった。以下，日本を含む各国のプライバシー法制の基準ともなっているこの勧告で示された「8 原則」を簡単に紹介しておく。

(1) 収集制限の原則：個人データの収集には制限を設けるべきであり，データの収集は，適法かつ公正な手段によって，かつ適当な場合には，データ主体に通知又は同意を得て行うべきである。

(2) データ内容の原則：個人データは，その利用目的に沿ったものであるべきであり，かつ利用目的に必要な範囲内で正確，完全であり，最新なものに保たれなければならない。

(3) 目的明確化の原則：個人データの収集目的は，収集時よりも遅くない時点において明確化されなければならず，その後の利用は，当該収集目的の達成又は当該収集目的に矛盾しないでかつ，目的の変更毎に明確化された他の目的の達成に限定されるべきである。

(4) 利用制限の原則：データ主体の同意がある場合や法律の規定による場合を除いて，収集したデータを明確化された目的以外に利用してはならない。

(5) 安全保護の原則：個人データは，その紛失もしくは不当なアクセス，破壊，使用，修正，開示等の危険に対し，合理的な安全保護措置により保護されなければならない。

(6) 公開の原則：個人データに係る開発，実施，政策は一般に公開しなければならない。また，個人データの収集の実施方針等を公開し，データの存在，利用目的，管理者等を明示するべきである。

(7) 個人参加の原則：データ主体に対して，自己に関するデータの所在及び内容を確認させ，また自己に関する異議申立が出来，意義が認められた場合にはデータの消去，修正，完全化を保証するべきである。

(8) 責任の原則：データの管理者は，上記諸原則実施の責任を有するべきである。

2．2　個人情報保護法の成立

このような国際的潮流の中，西欧各国では個人情報の保護のための法律・制度が整備されていったが，わが国の法整備は遅々として進まず，情報保護法制は 2003 年 5 月の個人情報保護関連 5 法の成立（法律の施行は 2005 年 4 月 1 日）を待つことになった（注 2)。

本格的な法整備が遅れた理由は，それまでわが国の法制度においてプライバシーそのものの明文規定が無く，さらに言えば社会的にもプライバシーという概念の共通認識となるべき文化そのものが無かったことによるものと思われる（これは，「プライバシー」という言葉が未だに的確な日本語で語れないことにその証左を見ることが出来る)。少し寄り道になるが，今日，プライバシー権そのものに関してはさすがに権利を否定する議論はなく，明文規定は無くとも，個人がプライバシーを守る権利は先験的な権利として認められるとの説が有力で，その法的根拠としては日本国憲法第13条＝個人の尊重（注3）が規定する「幸福追求権」に包括的な権利として認められるとする考え方が一般的である。

2．3　保護関連５法

個人情報の保護の法体系は，基本法である「個人情報保護法」，国の行政機関及び独立行政法人における個人情報の取扱を定めた「行政機関個人情報保護法」と「独立行政法人等個人情報保護法」，手続法である「情報公開・個人情報保護審査会設置法」「整備法」の五本の法律（上記法律名はいずれも略称＝注4）により構成され，これに各地方公共団体が定める個人情報保護条例，さらに民間部門を24分野に分け各主務大臣が定めるガイドラインを加え形作られている（図1)。

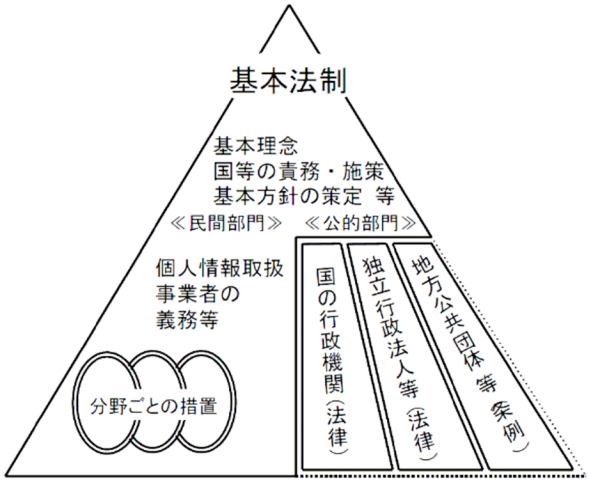

図１　個人情報保護法制の体系イメージ（首相官邸ホームページ「個人情報の保護」＝
http://www5.cao.go.jp/seikatsu/kojin/kaisetsu/index.html）

図１で見るとおりこの法体系は重層的かつ非常に大きなものとなっているが，これは各法及びガイドライン等が，それぞれの対象とする機関によって扱う情報が異なることによるもので，内容的には基本法である個人情報保護法に集約される。

法律は，「個人情報は，個人の人格尊重の理念の下に慎

重に取り扱われるべきものであることに鑑み，その適正な取り扱いが図られなければならない(＝法第３条)」と，プライバシー保護の原則を基本理念として明記した。そして，具体的には，個人情報取扱事業者（5000 件以上の個人情報を個人情報データベース等として所持し事業に用いている事業者）に情報データベースの取り扱いに関する義務を課す（主務大臣への報告及びそれに伴う改善措置の遵守＝違反事業者に対しては刑事罰を科す）ことで，個人情報を保護する枠組みを作っている。

上記の内容から判るように，この法律は「個人情報を保護の対象とする」ことを法制度として明確にするという積極的な性格を有するものである反面，そのための具体的な規定としては，個人情報データベースの漏洩という問題に対処することのみ企図した，情報管理の手続き規定に終始している。言い方を変えれば，「個人情報保護法」という通称を持つこの法律が規制するのは，個人情報の「データ」「データベース」の取り扱いに対してであり，「個人の情報」そのものではない（注 5)。

個人情報保護法の成立は，その一方で，法律の内容に対する過剰反応とも言うべき誤解をも生んでいる。小中学校の緊急連絡網リスト，社員名簿や同窓会名簿が作成できないという誤解，あるいは国勢調査や交番の巡回ノートへの回答拒否など，法律の主旨とは異なる過剰な権利主張が法律の成立にこと寄せた形で為されている。過剰反応や誤解が起きるのは，この法律が「個人情報の保護に関する法律」と名乗り，その名称からあたかも個人情報（一般的解釈では，いわゆるプライバシー）を保護する法律であるかのように誤解されるからでもある。

法律がその理念として明らかにしたとおり，個人情報の保護を謳う以上，法的に守るべき個人情報とは何を指すのか，明らかにする努力が必要であった。過剰反応や誤解，あるいは期待はずれとの評価はあるものの，図 2 からも読み取れるとおり，法律整備の主旨自体が，IT 社会のもたらす利便性にともなって生まれた「影」であるプライバシー等の個人の権利利益侵害の危険性や不安感増大に対処することにあり，国際ルールへの協調，また大きな社会問題ともなっている個人情報漏洩に対する緊急措置と解釈すれば，一定の評価はされるべきものと考えられる。さらに，本法律の根幹，すなわち「個人情報は保護されるべき情報」という，プライバシー権の原則を明文化したことの意義は，今後も追究されるべき課題であるプライバシー権の確立にとり大きな一歩といえるだろう。

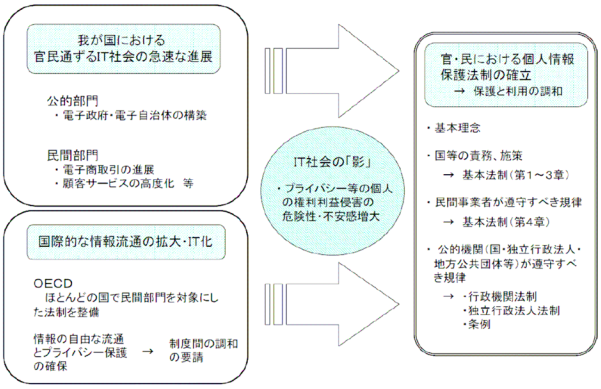

図 2　個人情報保護法制整備の背景（首相官邸ホームページ「個人情報の保護」＝
http://www5.cao.go.jp/seikatsu/kojin/kaisetsu/index.html）

３．個人データの流失とその原因

3．1　個人情報流失の実態

法律の施行後も個人情報の流失事故，事件は後を絶たない。個人情報の流失は以前から問題となっていたが，旧来の事故・事件では情報管理の不備，不注意によるものが多く，事故１件あたりの流出情報数でも数十から数百人分というものが多かった。ところがデータのディジタル化が進みさらにネットの普及という IT 化の進展にともなった最近の事例では，数十万人分，あるいは数百万件のデータと流失規模が桁違いの大きさになり，加えて経済的損失を伴う大規模流失事件が多発することとなっている。

大規模流失事件を例示的に見ると，2005 年 6 月にアメリカの情報処理会社が大手クレジットカード会社の顧客情報 4000 万件を流失させ，この流失事故により日本国内だけでも 1 億 1000 万円のカード不正使用が判明。翌 06 年にはインターネット接続会社の元社員が 450 万人分の顧客情報を流失させ，さらに 07 年には大手印刷会社のダイレクトメール作成業務にからんで 864 万人分の個人情報が流失，今年に入ってからでも三菱 UFJ 証券の元部長代理が会社データベースから 148 万件の顧客情報を引き出し名簿業者に転売をするという事件が起きている。

これら情報漏洩に関しては，関係業界企業が作る「NPO 法人日本ネットワークセキュリティ協会」が毎年調査報告書を公表している。公表資料から統計データとしての情報流失の実態を見てみたい。

直近の報告書は，今年 7 月に公表された「2008 年情報セキュリティインシデントに関する調査報告書」である。同報告書によれば，漏洩件数は前年に比べ大幅に増

加し，1373 件（対前年比 509 件の増加）となっている。増加の理由としては，「教育・学習支援業」「金融・保険業」「サービス業」「運輸業」など，多くの業種において全体的に漏えい件数が増加したこと，またある自治体が積極的に情報漏えい事件を公表したことが影響しているとしている。漏洩人数（情報数）は，723 万人と，個人情報保護法施行後では，最も少なく，かつ，初めて減少に転じた。漏洩人数の前年比減少は，漏えい人数が 100 万人を大きく超える大規模な個人情報漏が昨年は発生しなかったことによるもので，問題の沈静化あるいは解決に向かっていることとは一概に言えるわけではない。漏洩した情報の人数は，大規模な事件の発生の有無により大きく変動するので，前年比の増減だけでは，問題の拡がりの傾向を推測することは出来ないからである。一方，事件件数の増加は続いており，これは問題の拡散傾向を示しているものといえよう。

報告書では，発生した事件の件数や対象漏洩人数またその原因や経路の分析報告に併せ，これら事件による「想定損害賠償額」の試算なども行っており，昨年 1 年間に起きた漏洩事件による想定損害賠償総額を 2367 億円と試算している。賠償額の試算データはその算出方法とも併せ大変興味深いものであるが，それらは報告書をお読みいただくこととし，ここでは流失の原因分析を見ていくことにする [2)]。

3．2　情報の流失の原因（上記調査報告書から）

情報流失の原因比率を件数で見た場合，「誤操作＝35%」「管理ミス＝22%」「紛失・置き忘れ＝14%」「盗難＝11%」などが上位を占め，一方，流失事件をデータの対象人数で見ると「管理ミス＝69%」「不正アクセス＝12%」などとなっている。分類された原因項目の中身を見ると，「誤操作」は①紙媒体の誤配送②電子メールの誤送信③FAX による誤配送などで，「管理ミス」はその約半数が誤廃棄（誤って他の情報と一緒に廃棄）である（図 3，4）。

データには直接表れていないが，個々の事案ごとの事情を推し量れば，単純な個人的ミスや不注意の場合と，組織として情報保護に対する対応の無さ・拙さという問題の両方が予想されるが，いずれもが人為的な問題であり，解決は個々の現場での対応を望むしかない。人的ミスによる情報流失は，件数，対象人数ともに全体の過半を占めているが，いずれも 1 事件あたりの漏洩データは比較的少なく，個別被害者のプライバシー侵害は別として，社会的な影響は限定的なものに留まる。

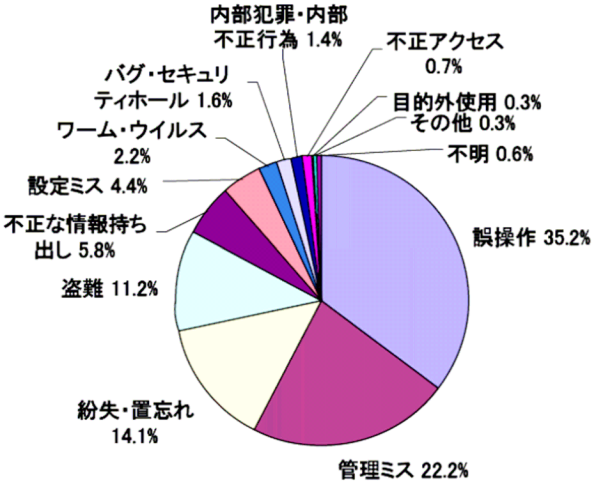

図 3　漏洩原因比率（件数）（NPO 法人日本情報ネットワークセキュリティ協会）
http://www.jnsa.org/result/2008/surv/incident/index.html「２００８年情報セキュリティインシデントに関する調査報告書」より転記

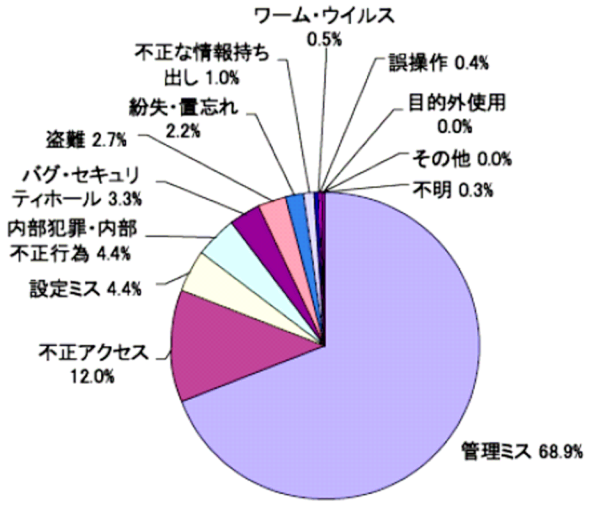

図 4　漏洩原因比率（人数）（NPO 法人日本情報ネットワークセキュリティ協会）
http://www.jnsa.org/result/2008/surv/incident/index.html「２００８年情報セキュリティインシデントに関する調査報告書」より転記

これに比し，発生件数こそ少ないものの「不正アクセス」による情報流失は，その規模や波及効果も大きい社会的な事件になる。昨年の上記報告書では人数比で 12%と原因の 2 番目となっているが，これは，既に述べたように昨年には大規模流失が起きていないことによるものである。過去 7 年間の集計データで見ると「不正アクセス」による 1 件あたりの漏洩人数は事件平均で 10 万人を超えており，事件件数の半数が 1～5 万人の漏洩とな

っている。これに比べ漏洩人数の集計で 7 割を占めた管理ミスによる事件ではその 3 分の 2 が，1 件あたり 10 人以下の漏洩人数となっており，ネットを通じた不正アクセスによる事件はまさに桁違いの数字となっている（このほか，IT に絡む原因による漏洩では「バグ・セキュリティホール」では事件平均で 1 万 4 千人の漏洩）（図 5）。

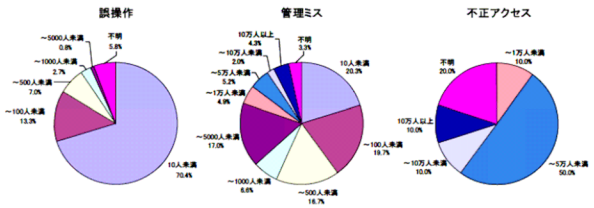

図 5　漏洩原因の人数区分（NPO 法人日本情報ネットワークセキュリティ協会）
http://www.jnsa.org/result/2008/surv/incident/index.html「２００８年情報セキュリティインシデントに関する調査報告書」より転記

以上の集計結果から見えてくる個人情報流失問題は，データを扱う人間の不注意や単純なミスを原因とする場合は，データの取扱方法や注意義務の徹底によってかなりのデータ流失の防止を図ることが出来ようが，その一方で管理体制の穴を突くデータの不法取得，さらにはインターネットを介した犯罪が一旦起こると，社会を揺るがすような大規模流失になることである。前者に関しての技術的措置としてはいくつかの内部管理・統制用のソフトが開発され市場にも流通しているが，それらも人為的ミスを減少させる仕組みを提供するに留まるもので，技術的解決という意味では範疇外の問題としか言えない。

これに対し，後者のネットなどでの情報流失は，論理的には技術的な防止措置が可能かつ必然な問題である。何故ならば，ネットなどからの情報流失は，操作ミスなどの過失による人為的なものを除き，ほとんどがセキュリティの欠陥を突いた技術犯罪であり，防止もまた技術的な対応によることが求められからである。

そして，これら対応技術の遅滞は，さらに重要かつ深刻な問題を生む可能性をも孕んでいる。現行の情報処理システムは，IT 技術の進歩によってもたらされた果実であり，現代社会・経済に不可欠なシステムである。しかしながら，情報漏洩によるプライバシー侵害の頻発を放置すれば，結果としてシステムそのものの見直し，あるいはまた，その有用性をも犠牲にする何らかの規制が加えられる事も想起されざるを得ない。

たとえばこのような情報漏洩対策として，企業ではいろいろな対策が模索されている。たとえばファイルダウンロード制限，あるいはファイルの転送制限などの手法が採用されている。また PC に多くの情報が蓄積されているのが漏えいの理由の 1 つとして，PC からメモリ機能を取り除いたシンクライアント PC の活用を行っている企業もある。ただしこれらは，最近の ICT による業務の効率化を阻害するものであり，また PC 能力の拡大を低下させるものである。また，シンクライアント PC のように，PC 機能を削減して，そのうえで PC の価格を上昇させる結果を招いている。これらの施策は，ICT の進展に関して，マイナス方向の施策と言わざるをえない。

４．個人データ漏洩への対応技術

4．1　情報流失を防ぐ技術とは

情報流失に対する技術的対応を考える前提としては，問題となる電磁情報ディジタル化されたデータベースの特質と，ネットがらみの情報流失特有の問題について，整理，確認をしておく必要があろう。

電子情報によるデータベースの特質としては①大容量化＝ディジタル技術によって，含まれる情報件数がきわめて大きなデータベースが，作成，利用の両面から可能となっていること②管理，移動の簡便性＝10 万件，100 万件のデータベースでも電子ファイルであれば PC 内の収納は勿論，CD 一枚で容易に持ち運びが出来，さらにネット配信を使えば瞬時の移動が可能なこと－－などが挙げられる。また，それらの情報がネット上で扱われ事件・事故が起きた場合は③漏洩先の追跡が不可能＝瞬時の移動が可能であることから再移転が繰り返されることによる際限のない拡散が起き，漏洩先の追跡，被害の拡大防止が不可能になること④回復不可能な被害＝情報がネット上で公開されれば，直ちに世界中を網羅する公開情報となってしまい，情報漏洩の被害回復は不可能になることなどが考えられる。さらには⑤意図しない犯罪＝ファイル交換ソフトなどによる意図しない情報漏洩が起き，被害者が犯罪者になることすらある－－などである（注 6：③の関連＝「情報の回収は困難」）。

上記の諸特性を踏まえ，情報流失・漏洩防止を技術的な観点から考えれば，対応策は以下の諸点に整理することが出来よう。まず，データの暗号化などデータの正規利用者以外にはデータを利用することが出来ないようにする技術（＝暗号化）。情報を保持する PC ないしサーバーなどからのファイル盗用への防止技術（＝PC 使用者の限定・特定），ネット配信中におけるファイルの不正取得への対処技術（＝不正アクセス防止）。そして上記③④

に対しては直接の防止は困難であろうが，ファイルの移動経路を把握することによる二次的な対策を施す方策が考えられなければならない。そして，常時ネット接続が状態となっている PC に意図せざる進入を防止するセキュリティ技術（＝ウイルス等防止）などが考えられる。

4．2　セキュリティ技術

セキュリティの脅威として，盗聴，改ざん，なりすまし，事実否認，がある。またこれらによる情報漏洩を防ぐ施策として，アクセス制御，暗号技術，生体認証などの認証技術などが行われている。これらの技術は，ICT とくにインターネットが普及したことで初めて日の目を見た技術であり，そういう意味で最も進展の激しい技術分野でもある。これらの方法についても，現在のところ完璧なものはない。以下に，2，3 最近の現状を紹介する。

4．3　不正アクセスの防止技術

不正アクセス対策の重要性が認識され，ファイアウォール等の不正アクセス対策が実施されるようになった。しかし，これら不正アクセスの手法が破られる事例が頻発することで，より高度な不正アクセス対策技術が求められている。

また，インターネットの普及が管理対象のネットワークの大規模化を促進したため，情報システムをトータルに守る仕組みとして個々の不正アクセス対策ツール群を統合的に効果良く，管理・運用することが重要となってきている。

最近では，監査支援技術である統合型セキュリティ診断ツールや侵入検知技術を発展させたおとり誘導による不正アクセス対策システムも実用化されている。

4．4　情報の暗号化技術

情報漏洩対策として有力な手法として，情報の暗号化がある。最近の暗号化技術の進展は目ざましく，ストリーム暗号やブロック暗号，あるいは共通鍵暗号や公開鍵暗号など多様な暗号が開発，使用されている。ただし，2006 年に発生した米小売大手の TJX Companies で起きた過去最大規模の顧客情報流出事件は，暗号化が万能でないことを示した。

暗号化技術があってもデータが暗号化されなければ何の価値もない。たとえばクレジットカード番号が暗号化されたままだとカードを処理することができない。そのため，データが「裸の」（つまり暗号化されていない）状態にある瞬間を狙ってそのデータが漏えいされることがある。暗号化技術の使用をどれだけ強く要求しようとも，TJX で暗号化が役に立たず，また多くの企業で暗号化が役に立たない可能性があると思われる理由は幾つかある。暗号化をめぐる問題点の 1 つが，弱い暗号の使用である。当初の DES（Data Encryption Standard）暗号化は，現在では多くのアプリケーションにおいてセキュリティが不十分だと考えられている。これは主として，鍵のサイズが 56 ビットというのは小さすぎるという理由による。DES の暗号鍵が短時間で解読された例もある。

共有鍵暗号方式は本質的にリスクが大きいといわれている。たとえば，鍵とデータを一緒に保管し共有鍵暗号方式を使っている場合，あるいはデータの鍵という名前のファイルを準備している場合，さらには，PC デイスプレイ上にポストイットに鍵情報を記入している例もあるなど，鍵を保管する場所があまりにも不用心な場合もある。笑うに笑えない話である。

公開鍵暗号化は，鍵の一部をデータの送信者に与え，別の一部を受信者に与えるという方式である。データの受信者は，鍵の公開部分を一般に公開することができる。しかしデータを暗号化するのは，鍵の非公開部分だけである。たとえば銀行の顧客は一方の鍵を使って銀行にアクセスし，銀行は自分たちが持っている鍵を使って照合することができる。このように，2 つの異なる鍵を使って暗号化が行われる。この公開鍵暗号は，鍵の保管の観点から共有鍵暗号より優れた暗号といえる。しかしながら，この公開鍵暗号についてもユーザにとって無視できない問題がある。暗号を使用することによる PC のパフォーマンス低下問題と仕組みの問題である。後者の仕組みに関しては，鍵の強度をどの程度にするか，鍵をどこに保管するか，誰がアクセスできるようにするかなど多岐にわたる。

セキュリティの確保のためには，システム全体についての脆弱性評価作業が必須となっている。ここではデフォルトの ID やパスワードをそのまま使っていないかチェックする，既知の脆弱性の有無を確認する，パッチを適用する，攻撃に対してデータベースを堅牢化するといった作業も含まれる。

５．技術進歩と個人生活への侵害

これまで述べてきたプライバシー問題は，個人情報を集積したデータベースでの漏洩による権利侵犯にあったが，既に本稿でも述べたようにプライバシー権にはもう一つの要請分野がある。「個人の私生活に関する事柄を他者に秘匿しまた干渉されない状態を要求する権利」に直

接関わる分野がそれである。この権利は，現在のIT社会の中でどのように扱われ，考えられていくべきなのであろうか。代表的な事例として「ストリートビュー」と「Nシステム」を，権利の一つと考えられる「肖像権」を中心命題として取り上げてみよう。

5．1　「ストリートビュー」とプライバシー問題

昨年夏，検索エンジンのグーグルが新しいサービスとして，「ストリートビュー」を日本に上陸させた。前年2007年5月にサンフランシスコで始められたこのサービスは，グーグルの地図サイトからストリートビューが提供されている道路上の任意の地点を選ぶと，地図や航空写真から路上風景のパノラマ写真の画面に切り替わり，その地点からの3次元方向が写真で見られるという，画期的な新サービスとして大変な話題を呼んだ。さらにこのサービスは，視野や視点を移動させたり拡大・縮小させたりすることも可能で，それら操作によって作られたオリジナルな映像を印刷し，またネットワークを通じて送信，ウェブサイトに表示することをも可能にした。ストリートビューはこれらの機能からインターネット時代の新しい「地図」の形との評価も得た。

評価や歓迎の声の一方で，ストリートビューは①予告も同意もなく撮影し公開されていること②個人宅の表札や家の内部まで見られる例があること③本人が見られたくない場面や姿が写っていること――などから，このサービスが「個人の生活を不当に侵害している」との批判が噴出した（注7）。ストリートビューは対象地域を拡げ続け，現在ではアメリカはじめ，フランス・イタリア・スペイン・オーストラリア・日本・ニュージーランド・イギリス・オランダへとサービス地点を拡大させているが，それにともなって各国でもプライバシーをめぐる論争が次々起きた。各国で問題とされた点は日本の場合とほぼ同様で，写されている対象物とそこから類推される個人生活への侵犯，個人の顔の可視性に対する懸念，写された者からの要請に基づく写真の削除問題，これらの諸問題に対処するべき苦情処理窓口の整備不足と不適な対応，等々が指摘された。これに対し，グーグル側でも指摘された問題への対応措置として，個人生活への干渉を避けるべく撮影場所を変え，また写真の鮮明度や顔の可視性などへの対処を行い，問題は一応の沈静化をみることになった。

5．2　「Nシステム」，監視カメラ

通称「Nシステム」と呼ばれる監視カメラシステムがある。正式には「自動車ナンバー自動読取装置」といい，警察が手配車両の追跡を目的として全国の高速道路や幹線道路上に設置している装置である。盗難車両の追跡を目的として導入されたこのシステムは，成田闘争やその後のオーム事件でも有効性が認められ，今では車に絡んだ犯罪捜査の重要なツールとされている。Nシステムの他にも類似の装置としては高速道路の入り口に設置されているAVIシステムがあるが，これらのシステムでは，装置設置場所を通過した全ての車両ナンンバーと運転席，助手席の搭乗者の画像が記録される。そして車のナンバーはセンターCPと照合され，映像の車両ナンバーが登録されている手配車両のナンバーと一致する場合には関係する警察署等に通報されるという仕組みである。

犯罪捜査には強力な手段であることは間違いがないが，被写体とされることになる運転者あるいは同乗者のほとんどは犯罪に関係のない者である。被写体となった者からみれば，Nシステム等によって，車を運転し搭乗するという日常の生活行動が警察という第三者に記録されることになる。「誰と」「何時」「誰の車で」「何処で」，という情報が記録される。当然のことながらプライバシー権の侵害との主張がされることになる。これに対し，設置者である警察は，このシステムが犯罪捜査の目的で設置されたもので，収得した情報のうち記録の対象は車両ナンバーデータだけ（顔の画像は消去）で，それ自体も捜査情報で非公開であることからプライバシー権の侵害はないとしている（注8）[3),4)]。

振り込め詐欺事件が多発する中での銀行ATMの監視カメラ，万引きや強盗の容疑者を特定することに資する監視カメラなども，犯罪防止や捜査補助目的のシステムとして急速に普及拡大をしてきている。これらの犯罪捜査を補助し防止するためのツールとされるシステム対しても，Nシステムで指摘されていると同様に，プライバシー保護の観点からは多くの疑問が提起される。

基本的な問題としては，個人の顔や体の画像データを収集すること，その行為自体が既に「伝統的プライバシー権」としては問題にされなければならない。厳密な言い方をすれば，撮影には許可が必要と言うことになるが，公益性との観点での整理が求められる。さらに，データの管理にも充分な配慮がなされなければならない。収集された画像のうちデータとして保存また解析・分析される対象画像は何か，そのデータはどのように管理・運用されるかなど，「自己情報コントロール権」の観点を踏まえた基準作りが，法制化を含め必要になろう。

Nシステムなどの捜査情報の取得システム，あるいは防犯のためのシステムの設置者は，これらのプライバシー侵害の批判を意識し，データの運用・管理やその規則・

基準に十分な配慮が為されていると主張するが，データ管理が厳格であるはずの警察組織においてもデータの漏洩事件・事故が発生している（注 9）。

5. 3　映像情報によるプライバシー侵害と技術的対応

情報は視覚，聴覚を通じて他者に伝えられる。プライバシーの対象となる個人情報も同様に，書類（電磁書類を含む）や画像・映像，また放送などの音声情報で伝播していく。データベースの漏洩事件・事故は書類による物であるが，前項で問題とした肖像権の侵害などの問題は，画像，映像情報によるものである。

ここでは，今回例示としたストリートビューと N システム・監視カメラで問題とされた点のうち技術介入余地のある問題点を確認しながら，これら問題を解消する技術を検証することにする。

ストリートビューで問題にされた点は，画像の中に「顔」や「姿」という直接情報，「表札」や「車のナンバー」などの個人を類推し特定出来る情報が公開されることによる個人のプライバシーが侵害されているとする指摘，また「干し物」や「おもちゃ」などの画像により生活の環境（例えば家族構成，女性の一人暮らし）が類推されることによる犯罪の誘発などであった。

これらの問題は，画像の内から問題となる特定部分を見せない（見えなくし，あるいは判然としない画像にする）技術によって解決することが出来る。画像の特定部分を見えなくすることは，画像全体の画質を下げる方法もあるが，この方法では，サービスの質を下げることになる。また，画像一枚ごとに「ぼかし」などの処理を行うことは技術的には容易であるがコストの面から難しい。これらの問題を解決するためには，予め処理を施す部分を特定し，自動認識機能で画像からその特定の部分を切り出し，処理を行うシステムが必要になる。自動認識とは，「人間を介さず，ハード，ソフトを含む機器により自動的にバーコード，磁気カード，カメラなどからデータを取り込み，内容を認識する」ことであり，その技術は，取り込むデータの種類によりいくつかに類別される。本稿では画像データを対象としていることから画像認識のことを意味する。画像認識では，画像データから対象物となる輪郭を抽出し，背景から分離した上で，その対象物が何であるかを分析する。人間なら無意識に行われている行為だが，コンピュータにとっては高度で複雑な処理となる。

監視カメラなどの場合は本来の目的である犯罪や事故の防止の観点から，逆に解像度のよいクリアな画像，影像が求められる。現在のカメラの性能は，付属的な機能である携帯電話のカメラを見れば判るとおり非常によくなっており，一定の撮影条件が満たされた場合には問題はない。ところが，監視カメラなどで必要とされる画像は，夜であったり対象物の動きが速かったりするなど撮影条件が悪い場合が多い。勿論，カメラやシステム全体の質を高めることにより，かなりの部分で問題は解決するが，これにはコストの問題がある。画質の悪い画像，映像から必要な情報を取り出す解析技術が求められることになる。この技術については，たとえば，画像・映像の一部をディジタルズームによって拡大するというような手法が考えられる。しかし，ほとんどの場合，画素が粗くなり，かえって見難い画像になる。また拡大による画質の劣化だけでなく，霧や大気の透明度の低下，カメラ自体の振動といった撮影環境により画像がぼやけてしまう場合もある。これに対して，超解像と呼ばれる技術がある。これは，おもに東芝と NEC によって開発された技術で，東芝では同一の対象を連続して撮影した複数の画像列を統合し，より鮮明な画像を得ることを実現している。NEC では，混色現象を元に戻すというアプローチで一枚のフレームから超解像を実現している。このような画質改善技術は，比較的演算量が多く，撮影環境や写っている対象物によって有効なアルゴリズムが異なるなど，現状の画像処理技術ではどのような場合にも使えるというわけではない。

一方において，映像解析では検知機能の高度化という流れもある。これは，たとえば施設や特定の区域に侵入した人や車を自動的に検知し，監視員に通知したり，事象に合わせて選択的に映像を保存する等，監視作業を自動化しようとするものである。画像の変化を検出するためさまざまな手法が開発されており，たとえば画像の濃度変化を検出する方法がある。あらかじめ記憶した標準パターンにあたる背景画像と対象画像との比較を行い，濃度差のある部分は何らかの変化があったとする背景差分方法が主流となっている。対象となる画像は日照状態が時々刻々変化するので，背景画像はそれに応じて更新する必要があり，その更新法や侵入者以外の移動物体に反応しない，動きの特性に注目した変化領域の抽出法等のアルゴリズムの開発が進んでいる。

5. 4　基本法の必要性＝「プライバシー権」を法律はどう扱っているか＝

ストリートビューや監視システムで見てきたプライバシー権，すなわち「個人の私生活に関する事柄を他者に秘匿しまた干渉されない状態を要求する権利」に関して法律はどのような規定をしているのであろうか。結論か

ら先に言えば，わが国にこれら権利に関する明文規定はない。現行の「個人情報保護法」では，目的外利用や第三者提供に本人の同意を必要とする条項，保有個人データの開示等の請求条項などがあり，考え方としては上記権利の保護が見られるが，プライバシーを「権利」とする，明文規定はない。既に前章で述べたとおり，現行の個人情報保護法が対象としている事象は，同法の２条３項で規定する個人情報取扱事業者の義務であって，個人情報の保護そのものではない。

個人情報の保護には先進的な西欧諸国では，人格権の一つとしてプライバシー権が認められている例が多い。紙数の関係で個々の国の例の詳述は出来ないが，プライバシーの権利を基本的人権の一つとして尊重する考え方は共通しており，権利を尊重するべき理由を概念的に記せば,「自己の情報を自らの意思でコントロールすることが出来なければ，その不安感から行動や発言にも規制が働き，移動や表現の自由といった基本的人権の行使を妨げ，個人の自由によって維持される社会という公益をも損なう」ことにあるとする。

わが国においてもプライバシー・個人情報の保護のあり方についての検討がなされなければならない。自己の情報を自らがコントロールすることが出来る，すなわち自らの個人情報の所在を確認でき，その情報の利用や目的について知り，利用を制限することができる，これがプライバシー保護の基本的な考え方であり，この考え方を具体化する「個人情報保護基本法（仮称)」を策定することが求められる。このような個人情報コントロール権を法律の制度として具体化することはかなりの困難が伴う，公益性との調整，あるいはこれらも基本的人権である「知る権利」「言論の自由」などとの調和が求められるからである。基本法の法制化にあたっては，まず「プライバシーは保護されるべき権利」であることを確認・明文化した上で，対立概念とも言うべき諸権利との線引きを行い，権利に一定の制限を設けることが検討課題となろう。

６．まとめ

前稿その１で紹介した著作権問題に引き続き，現在のインターネットの普及がもたらしたプライバシー問題について，私見を含め，現状と関連する法律との関係について紹介した。我々の基本的な考えは，大きくかつ急激に進展する ICT 技術を，法律でただやみくもに制限するのではなく，受益者である国民の立場に立ち，法律が関係者の利益を守る中立性を果たして欲しいことである。法制度が技術革新を阻害要因になることなく，技術革新の成果による新しいサービスの進展を促進させることを切に望むものである。

謝　辞

本研究の一部は，戦略的研究基盤形成支援事業の援助を受けていることをここに記し，謝意を表します。

参考文献

1）村上　仁己, 尾形　哲志, 川崎　秀二,「情報通信（ICT）技術の進展と法律問題（その１)」, 成蹊大学理工学研究報告, 第46巻, 第1号, 51－58ページ, 2009年3月

2）NPO法人日本ネットワークセキュリティ協会,『2008年情報セキュリティインシデントに関する調査報告書』: 平成21年8月17日, http://www.jnsa.org/result/2008/surv/incident/index.html

3）Nシステムの肖像権侵害事件「東京地裁　平成10年（ワ）第5272号　損害賠償事件」: 平成13年2月6日, http://www.translan.com/jucc/precedent-2001-02-06.html

4）Nシステムの肖像権侵害事件（２）「東京高裁　平成13年（ネ）第1113号　損害賠償請求控訴事件」: 平成13年9月19日, http://www.translan.com/jucc/precedent-2001-09-19b.html

5）村上　仁己,「ユビキタスネットワーク社会の実現を目指したトータル的なネットワークシステムの研究開発 －Ubilaプロジェクトの研究成果から－」, 第13回九州・国際テクノフェア, 2008年10月

注　釈

(1) 1961 年に元・外務大臣で東京都知事候補であった有田八郎氏が，小説『宴のあと』が自分の「私生活をみだりに明かされない権利（プライバシー権)」を侵すものであるとして東京地方裁判所に起した事件。裁判では原告側の主張するプライバシー権と被告側（三島由紀夫と出版社の新潮社）の表現の自由の主張とを争点とした。判決は原告の主張する「私生活をみだりに明かされない権利」を認め，被告側に 80 万円の損害賠償の支払いを命じた。プライバシー権を認めた初めての判断で,「プライバシー」という言葉とともに，その「権利」が社会的にも認められる端緒となった。

(2) わが国が個人のプライバシーに関わる情報の取扱等を法律で定めたのは，1988 年に公的機関を対象とした「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律」が最初である。そして翌 89 年には民間部門を対象とした「民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン」が当時の通産省により策定された。この法律と行政指導ともいえるガイドラインは，法には罰則規定がなくガイドラインには強制力がないことから，個人情報保護に関する法整備とは言い難いものであったとの筆者の考えから，本文では 2003 年の 5 法の成立をもって情報保護法制の整備としている。

(3) 日本国憲法第 13 条〔個人の尊重〕

『全て国民は，個人として尊重される。』

『生命，自由及び幸福追求に対する国民の権利については，公共の福祉に反しない限り，立法その他の国政の上で，最大限の尊重を必要とする。』

幸福追求権は，同条前段での個人尊重の原理に基づいた人権の根拠となる包括的な権利と考えられ，この幸福追求権に依る個々の権利は，法的救済を受けることができる具体的権利であると解される。

(4) 個人情報保護法の正式名称

「個人情報の保護に関する法律（平成 15 年 5 月 30 日法律第 57 号＝平成 17 年 4 月施行)」

(5)「データ」と「情報」

法律が誤解を生む原因の一つともなっている「データ」と「情報」という言葉の違いを述べておく必要がある。法律ではデータと情報を区別し，個人データについては安全管理義務を課す一方で，個人情報については管理者の良識に委ねている。法に言う「個人データ」とは「個人情報データベース等を構成する個人情報」であり，「個人情報データベース等」とは個人情報を含む情報の集合物である(容易な検索が要件)。本稿とも関連することなので，この法律に限らず解説をすれば，一般的に「個人データ」は「個人情報」という言葉で表される個人の属性に関わる情報の一部（例えば名前と電話番号等）を切り出し，その情報を収集の目的に従って整理されたものである。このため，「データ」としては名前がローマ字で書かれた「データ」と漢字で書かれた「データ」は同一人であっても別の「データ」となる。手書きや紙情報の「名簿」であれば，名前に漢字，ひらがな，カタカナ，ローマ字などの異なる表記が混在していても，見栄えはともかく名簿としての使用は可能であったが，IT 化されたデータベースでは統一した表示・記述形式でなければ別のデータ（別人）と理解される。「年金の 5000 万件のデータが失われた」との報道がされ大騒ぎになった事件の主原因もこのことで，紙情報から電子情報に転記するときの電子データに対する理解の不足が起こした問題でもあった。

(6：参考情報)『三菱ＵＦＪ証券の流出顧客情報，70 社が回収に応じず』(2009 年 6 月 25 日 読売新聞掲載記事＝全文)

顧客情報を転売目的で引き出すなどしたとして，三菱 UFJ 証券の元部長代理久保英明容疑者（44）が不正アクセス禁止法違反容疑などで逮捕された事件で，売却された約 5 万人分の顧客情報の流出先は，売却から 4 か月で計 96 社にまで拡大した。

このうち回収の求めに応じていないのは 70 社に上り，「貴重な情報で返却する必要はない」などと主張する業者もいる。三菱 UFJ 証券の担当者は「一度流出した情報を取り戻すのがこんなに難しいとは」と漏らしている。

同社によると久保容疑者が名簿業者 3 社に顧客情報を売却したのは 2 月中旬。内部調査を経て同社がこの事実を公表した 4 月 8 日時点の流出先は 13 社だった。

同社はその後，判明した流出先に対して，名簿の転売をやめるよう弁護士名で「損害賠償を負うこともある」とする警告書を送るなどして，回収作業を続けている。それでも情報の流出と拡散は止まらず，今月 25 日時点で計 96 社に情報が渡り，そのほとんどが不動産投資会社と先物取引業者だった。このうち回収の求めに応じていない 70 社は「警告書には法的な拘束力がない」「貴重な情報で返却する必要はない」という言い分を主張。同社側との話し合いも平行線のままという業者も多い。

こうした状況について，同社の担当者は「一度流出した情報を取り戻す作業がこれほど大変とは思わなかった」と語り，都内の名簿業者は「貴重な情報が載っている名簿ほど，裏取引されるため，拡散を食い止めるのは難しくなる」と打ち明ける。

同社は 25 日，久保容疑者の逮捕を受けて「被害拡大の防止に全力で取り組み，信頼回復に努めたい」とのコメントを発表。今後，弁護士や大学教授らで作る調査委員会からの報告を受け，情報流出の原因調査を進めるとしている。

(7)「ストリートビュー」のプライバシー問題

インターネット上で街並みの画像を閲覧できるグーグルの「ストリートビュー（SV)」について，地方自治体などから「差別助長に使われている」といった苦情や意見が総務省に寄せられていることが分かった。

同省の改善要請を受け，グーグル日本法人は 4 日，悪質なサイト運営者に削除要請を行うなどの対策を発表した。

改善策では，SV の二次利用が，名誉棄損やいじめ，嫌がらせなどにあたると本人から申告があった場合，同社が違法性などを判断し，サイト運営者に対し削除要請を行う。法的手段を取ることもあるという。

また，撮影中のエリアを公表するほか，削除要請の方法や電話番号などを記したパンフレットを用意し，ネットを使わない住民らにも情報提供するとしている。

SV を巡っては，「プライバシー侵害にあたる」などとして全国約 40 の地方議会（6 月 22 日現在）が国に規制を求める意見書を採択。総務省が約 1 か月間，意見を募ったところ，自治体や人権団体，弁護士会有志や個人などから計 49 件の意見が寄せられ，うち 10 件が「差別を目的とした書き込みに悪用されている」という指摘だった。

ネット上には SV の画像を転載し，被差別部落を一覧するサイトが乱立しており，意見を寄せた福岡県の担当者は「国は，こうした実態に目を向け対策を講じてほしい」としていた。

こうした声を受け，同省は，先月 27 日付でグーグルに対し，公開画像については，住民からの削除依頼に速やかに対応することなどを文書で求めていた。

グーグル日本法人は「これまでも改善策をとってきたが，総務省の要請を受け，一歩進んだ形で姿勢を示した」とコメントしている。（2009 年 9 月 5 日：読売新聞朝刊）

（8：参考情報）N システムの肖像権侵害事件

平成 10 年，東京地方裁判所に，N システムにより肖像権及び情報コントロール権を侵害されたとする者が，国に対し不法行為に基づく損害賠償の請求を求める裁判が起こされた。裁判の結果は，公益性を重視する裁判所の判断から，原告側の請求が棄却されるという結果に終わったが，プライバシーの保護の法的要請に関して裁判所も認め，N システムの運用に関しても一定の制限が必要とした。

読みやすい判決であり，プライバシーと監視システムの問題点が整理されている判決となっているので，その判決の全文を参考に供する。

N システムの肖像権侵害事件「東京地裁　平成 10 年（ワ）第 5272 号　損害賠償事件」

http://www.translan.com/jucc/precedent-2001-02-06.html

同上　控訴審「東京高裁　平成 13 年（ネ）第 1113 号　損害賠償請求控訴事件」

http://www.translan.com/jucc/precedent-2001-09-19b.html

(9) N システムの情報漏洩

2006 年，愛媛県警察の捜査員が Winny を使用した際に Antinny と思われるコンピュータウイルスに感染し，N システムが設置されている愛媛，香川，徳島の国道及び高速道路を通過した車のナンバープレート情報と通過日時が記録されたファイルが，他の捜査情報と共にインターネット上へ流出した事件も発生しており，この際流出した情報は約 10 日分，車両台数にして 10 万台超とされている。（2006 年 3 月 16 日：毎日新聞）