米国における情報セキュリティとプライバシー保護の状況

西村　孝(*)

インターネットを始めとする情報通信技術の進展に伴い我々の日常生活は格段に便利になったが、一方で情報の漏洩などにより個人のプライバシーが脅かされる様々な出来事が発生している。日本では個人情報保護法をきっかけに個人情報の保護に対する関心が高まり、情報漏洩防止のための教育や技術開発が盛んであるが、米国においては2005年春に連続して発生した10万人から100万人規模の個人情報漏洩事件をきっかけに個人情報を保護する情報セキュリティへの関心が高まった。しかも米国では事故や事件の後にはしばしば当事者間の訴訟問題が待っており、企業は情報漏洩のリスク対策として情報セキュリティを重視せざるを得ない状況になっている。本稿では、米国における情報漏洩の実態と情報セキュリティやプライバシー保護に関する種々の規制、プライバシー保護に向けた技術的取組み、情報漏洩を起こさないための対策と起こった後の対応策を紹介した。またプライバシー情報を能動的に活用することで利便を得ようという動きに対し、安心してこれを実行するためには技術開発だけにとどまらない法律、経済学、心理学など社会科学との連携の必要性を提言した。

1．はじめに

インターネットを始めとする情報通信技術(ICT)の進展に伴い、我々の生活は以前とは比較にならないほど便利になってきたが、一方で情報の漏洩などにより個人のプライバシーを脅かす様々な出来事が発生している。日本では個人情報保護法をきっかけに個人情報の保護に対する関心が高まり、情報漏洩防止のための教育や技術開発が盛んであるが、この米国においても状況はまったく同様で、プライバシーなどの個人情報を保護する情報セキュリティに対する関心は高い。Attrition.orgが運営するData Loss Archive and Database (DLDOS)(*1)は、米国を中心に発生した情報セキュリティに関する事件や事故を数多く紹介している。また米国社会の特徴としてこのような事故や事件の後には当事者間での訴訟に繋がるケースもあり、企業は情報漏洩のリスク対策の一環として情報セキュリティ問題を重要な課題として捉えている。

本稿では、米国における情報セキュリティとプライバシーの保護について、その実態と対策をいくつかの角度から紹介する。

2．深刻化するセキュリティとその実態

現在は、Googleなどにより提供される検索サービスを活用すれば即座に欲しい情報を手に入れることが可能であるが、ネットに仕掛けられた多くの罠(このようなウェッブサイトをボットと呼び、RBOT、SpyBOTなどがある)がID盗難やスパイウエアをインストールさせようと虎視眈々と利用者を待ち構えている。このボットは世界中にサイト数にして100万以上存在し、犯罪者にレンタルもされている。2005年の報告によれば、これらのサイトから発するインターネット詐欺(フィッシング(*2))の被害は24億ドル(*3)にも上ったとされている。

一方、電子メールは電話に次ぐ日常のコミュニケーション手段として普及しているが、ここにもウィルスメールやスパムメールが数多く放たれている。最近ではスパムメールに対応する処理に利用者は年間50時間ほどを費やしているとも言われている。

ウィルスについても今やパソコンに感染させるだけでなく、携帯電話や自動車搭載の電子機器にまで及んでおり、これらウィルスを販売するウィルスソースやボット・ソースもインターネット上に多数存在している。

ところで米国でプライバシー情報の漏洩問題が社会の関心事として一躍注目を浴びるようになったのは、2005年の春のことである。

事件の発端は、2005年2月、3万人のカリフォルニア州住民が信用調査会社ChoicePoint社から「情報主

(*) エヌティティデータ　アジルネット　エルエルシー　社長

(*1) 非営利のセキュリティサイトで、2000年以降に発生したデータ紛失について掲載しているオープンソースのデータベースである。

(*2) フィッシング(Phishing)：金融機関などからの正規なメールやウェッブサイトを装って暗証番号やクレジットカード番号などを搾取する詐欺のこと。

(*3) 被害総額を査定した調査機関によっても異なるため、真偽のほどは定かではない。

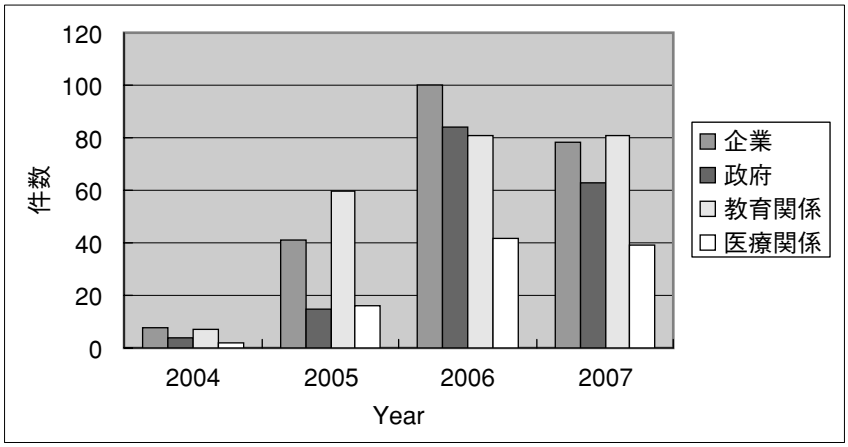
の許可を得ていない第三者」にその個人情報が開示されたという内容の手紙を受け取ったことに始まる。多くの消費者にとって「データブローカー」と呼ばれる新しい業種である同社の名前は初耳であったと思われる。「データブローカー」と称する企業は消費者の情報を収集・蓄積し、他社へ転売したり、顧客企業の要請に基づく職員の身元確認調査などのサービスの提供を専門にしている。同社は、情報を購入するフリをした顧客により、約14万5千人の個人情報(住所、ソーシャルセキュリティ番号、クレジットカード情報)を盗まれたと発表したため、プライバシー情報に影響を及ぼすデータ紛失事件として初めて大々的に報じられたのである。さらに同じ月に米国の銀行では最大手のBank of Americaが連邦職員向けカード保有者最大120万人のソーシャルセキュリティ番号の入った磁気テープを紛失する事故が発生、追うようにして情報サービス企業LexisNexis社データベースへのログインパスワード不正使用による侵入によって31万件の自動車免許証情報、ソーシャルセキュリティ番号の窃盗事件の発生(3月)、その後も大学、小売業界と短期間に情報漏洩による事件が相次いだ。

米国で起きた情報漏洩事件として規模の大きいものを表1に示す。2007年始めにマイアミのディスカウントストアT.J.Maxx and Marshallsの無線LANがハッキングされ、データベースに侵入されて9千4百万人の顧客情報が盗まれたとされるTJX事件(*4)、2006年、

	組織名	漏洩数	原因	情報種別	内部・外部	年
1	TJX	94,000,000	Hacking	Customer data	outside	2007
2	US Department of Veterans Affairs	27,000,000	Stolen Computer	SSN	outside	2006
3	Fidelity National Investment	8,500,000	Fraud	Customer date	Inside M	2007
4	TD Ameritrade	6,300,000	Hacking	NAA	outside	2007
5	Data Processors International	5,000,000	Hacking	Customer data	outside	2003
6	Citi group	3,900,000	Lost Media	SSN	outside	2005
7	Georgia State	2,900,000	Lost Media	SSN	outside	2007
8	Chase Card Services	2,500,000	Disposal-Accident	SSN	Inside	2006
9	LaSalle Bank	2,000,000	Lost Mediaq	SSN	outside	2005
10	Birmigham Veterans Affairs	1,835,000	Stolen Computer	SSN	outside	2007

DLDOSのデータより抽出

表1　米国で発生した大規模なプライバシー情報の漏洩事件

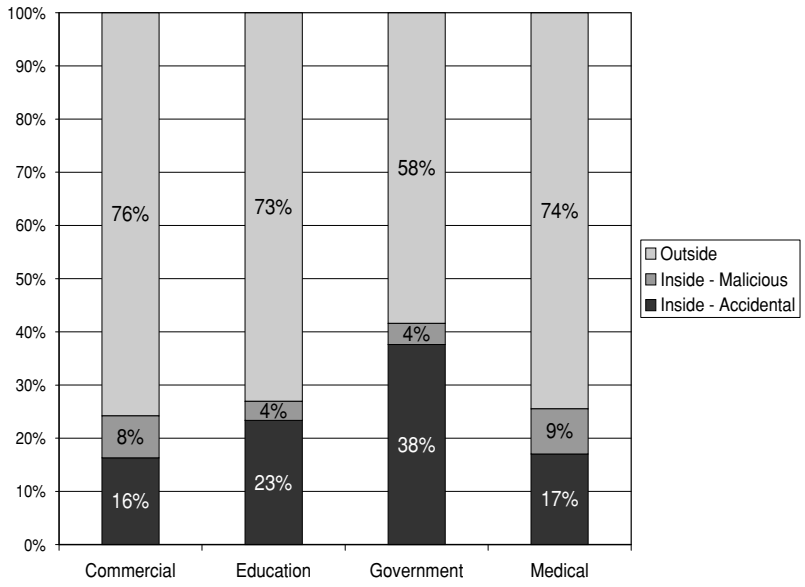


DLDOSのデータより作成

図1　業界別プライバシー情報漏洩件数

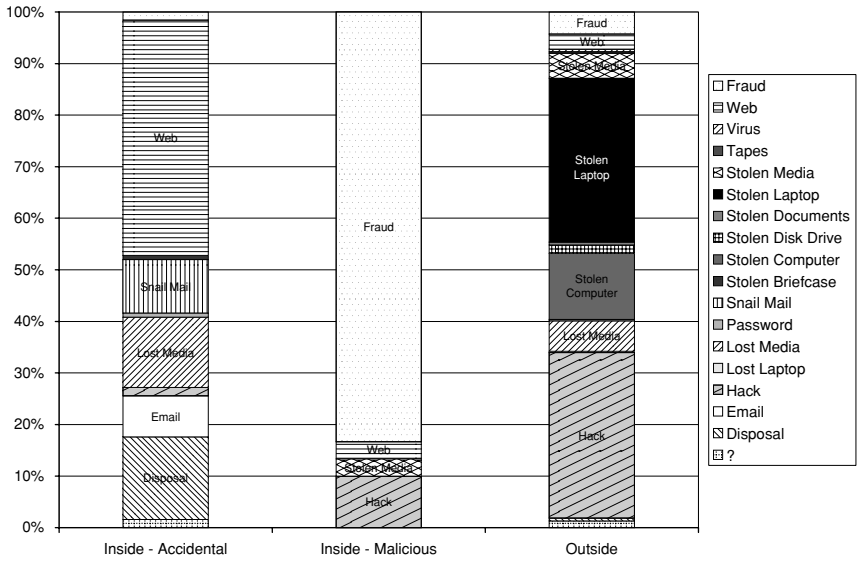
(*4)　9千4百万人分という数字は複数のクレジットカード情報からのダブルカウントを含むもので、4千6百万人分が正しいとする意見もある。
http://attrition.org/news/content/08-01-03.001.html

ラップトップコンピュータを盗まれたことにより２千７百万人に及ぶソーシャルセキュリティ番号の漏洩が発覚した米国退役軍人省事件などであるが、図１に示すように情報漏洩事件は企業は言うに及ばず、政府機関、教育機関、医療機関などいたるところで発生している。また図２、図３はDLDOSのデータベースからこれらの情報漏洩の原因を解析したものであるが、情報漏洩の原因の約3/4が部外者によるものであり、ラップトップコンピュータやメディアの盗難も60%近くを占めている。またネットへの不正侵入に起因したものは30%に及んでいる。さらに内部の者が悪意を持って実行したケースも５－10%程度の割合で発生しており、これらは多岐に亘る情報漏洩対策の必要性を示唆している。



DLDOSのデータより作成

図２　データへの脅威（2000 年～2006 年の統計から分析）



DLDOSのデータより作成

図３　データ紛失の要因（2000 年～2006 年の分析）

３．情報保護に関する規定

企業情報の流出やプライバシー情報の漏洩などに対し、消費者や投資家を保護する観点から米国政府、州政府それぞれのレベルで、企業の情報管理を徹底し、セキュリティ体制を確保することを義務付ける法律が制定されている。

連邦レベルでの代表的な法律として最初に上げられるのが 1999 年に制定された Gramm-Leach-Bliley Act（グラム・リーチ・ブライリー法）で、金融機関に対して消費者の金融情報の取り扱いに関するセキュリティとプライバシー管理を義務付けている。また、病院など医療関連機関に対して、患者情報の共有や暗号の利用を制限し、患者のプライバシーと情報のセキュリティの保護を義務付けた HIPPA（Health Insurance Portability and Accountability）、13 歳未満の児童をターゲットにしたウェッブサイトに対し、児童に関する情報を収集したり、それらの情報を第三者と共有する前にデータ収集方法の掲載と立証可能な親の同意の入手を義務付けた Children's Online Privacy Protection Act of 1998 などがある。

一方、州レベルの取組みとしてはカリフォルニア州がその先駆けとされているが、カリフォルニア州では州民の特定個人情報を電子的に保管している企業にシステムが侵害され、個人情報漏洩の可能性が発生した場合に、該当する住民への通知を義務付けた California Security Breach Information Act（2003 年施行）、カリフォルニア州でビジネスを行う金融機関に対し、顧客（州民）の個人情報を資本関係のない第三者機関と共有する場合に事前に書面による合意を得ることを義務付けた California Financial Information Privacy Act（2004 年施行）などがある。これらの法律がモデルとなって、ニュージャージー州をはじめ各州で、法律の制定、施行が検討され、個人情報（氏名、署名、ソーシャルセキュリティ番号、身体的特徴、住所、電話番号、パスポート番号、運転免許証など）の漏洩に対する報告義務などが規定されている。

また金融業界を始めとした業界団体も個人情報保護に対する自主的なガイドラインを設定している。例えば、クレジットカード最大手の VISA International は VISA カードの支払い処理を行うサービスプロバイダーや店舗に対し、情報セキュリティポリシーの策定と維持、データ保護対策の実施、セキュリティシステム、セキュリティプロセスの定期的チェックなど 12 項目に及ぶセキュリティ・リクワイアメントの遵守を義務付けた「利用顧客のための個人情報保護プログラム（Cardholder Information Security Program）」を 2001 年 6 月より実施している。

４．プライバシー保護技術とその取組み

「はじめに」でも述べたようにインターネットを取り巻く新しい技術が、個人のプライバシーに与える影響は非常に大きく、これを個人や社会への脅威と捉える向きも少なくない。しかし一方で、技術はプライバシーの保護を確かにすることもできるわけで、プライバシーの価値を重要視すればするほどプライバシー保護技術に対する役割と期待は膨らんでくる。特にプライバシー情報を保護しつつも上手に活用すればその経済的なメリットは大きいという指摘もなされている。以下では情報のセキュリティに関する技術のうち特にプライバシー保護のための技術と応用例、また企業や政府機関、学術団体などがアライアンスを組んで取り組む標準的な技術開発事例について概観する。

４．１　プライバシー強化技術（PET：Privacy Enhancing Technology）とその応用例

一般にプライバシー情報保護技術とは、暗号ソフト、データベースシステムにおけるデータの取り扱いやネットワークへのアクセス方法などを定めたポリシー（方針）、またこれらの取り決めを支援し、コントロールするためのソフトウエアなどを指す。個人情報流出などのリスクは、これらの技術を導入することによって初めて回避することが可能になる。しかしながらプライバシー保護技術の導入によって万全なプライバシー保護が可能になるわけではなく、情報を扱うユーザのセキュリティに対する意識や組織などの体制、またその運営などに依存していることは言うまでもない。プライバシー保護技術の例として、種々の暗号化技術、指紋、虹彩認証などの生体 ID 認証（バイオメトリックス）、データベースやネットワークなどの ID 管理、インターネット上の匿名化技術などが上げられるが、ここではこれら技術の活用例として無線 ID タグを利用したパスポートについて紹介する。

IC 無線タグ（RFID タグ）の機能を組み込んだパスポート（ｅパスポート）は日本でも 2006 年 8 月に発行が開始されたが、アメリカ、ヨーロッパなどの各国でもｅパスポートの発行は始まっている。RFID タグは固有の認識番号を持つ小さなチップであり、数センチから数メートルの距離からそのデータを読み取ること

ができる。日本ではJR東日本のSuicaがRFIDタグの応用例として知られるように、多くのRFIDタグは読取装置の電波からエネルギーを得、電池などのエネルギーを必要とせず情報の交換を行うことが可能である。このためeパスポートは入出国時における審査のスピードアップやパスポート盗難時にワールドワイドで不正利用を防ぐと同時に紛失したパスポートの発見のみならず、写真の流用やよく似た人物の不正流用、偽造パスポート製作に効力を発揮すると言われることから、その利便性が高く評価されている。

ところでこのRFIDタグの読取装置は電子工作の知識を持ってすれば数10ドルほどの部品代で読取装置を製作でき、誰にも知られずにその情報にアクセスすることが可能である。パスポートを携行することで、犯罪者にパスポートの重要情報を盗まれたり、また悪意がないとしても読取装置保有者に対し自ら自分の国籍などの情報を発信することになり、危険にさらされる可能性が常に存在する、という根本的な問題があり、RFIDパスポートの利便性は認めるもののプライバシー情報の保護については最重要課題とされてきた。

米国務省はRFIDパスポートについてはパスポートの表紙に電磁波遮蔽(RF Shielding)機能を組み込み、閉じられたパスポートのデータを遠隔から読み取られない工夫を取り入れたり、欧州共同体(EU)などの例に倣って基本アクセス制御と呼ばれる暗号化方式を採用してパスポートに物理的にアクセスできない限りデータにかけられた暗号を解読できない仕組みを導入し、発行に踏み切っている。また、さらに将来的にはチップの空きメモリ領域に生体情報である虹彩データや指紋データを保存し、本人確認の正確性を高める構想も検討されている。

4．2　プライバシー保護のための標準技術の開発

消費者のデータやアイデンティティ(身元情報)を守るソリューション開発が、企業や政府機関などによるアライアンスのもとで進められており、以下で紹介する。

(1)　PRIME(Privacy-Aware Identity Management)

PRIMEは、プライバシー保護機能を備えた身元確認システムの開発を目的に設立された団体で、ヨーロッパを中心に活動している団体である。人々は生活を営む上ではリアルの世界であれ、ネット上の仮想世界であれ、すべての取引において個人情報の交換が必要になる。リアルの世界では人々は社会生活を通じて、各自の個人情報を交換する場合にどの程度情報を開示すればいいかを判断することに慣れているが、ネットの仮想世界でこれを判断するのはかなり難しい。住所や電話番号、ソーシャルセキュリティ番号などに留まらず、医療・健康情報、金融情報、ショッピングのさいの嗜好などの情報とその利用は個人のプライバシーに大きな影響を与える可能性がある。PRIMEではこれらの情報を自ら管理でき、取引の際には必要最小限の情報だけを安全にしかも簡単に開示することが可能な手段の実現を目指している。

事務局はベルギーにあり、フランス、ドイツ、イタリアなど複数の国や組織に跨って構成された共同研究プロジェクトであり、ヨーロッパ地域のIBM、ヒューレットパッカード、T-Mobileなど IT業界のトップ企業も参画している。

これまでの成果としては、共同作業を伴う遠隔教育(eラーニング)向けや航空会社及び空港における乗客の処理などを含むいくつかのシナリオのプロトタイプが開発されており、その開発を通じて身元情報管理における問題の大きさを把握し、その標準的な解決法を見出すための国家と企業の知恵を集めた研究プロジェクトとして貢献が期待されている。

(2)　P3P (Platform for Preference Project)

P3Pは、ウェブサイトのプライバシーポリシーをユーザのソフトウエアが自動的に読み取り、理解可能な標準的なフォーマットに簡単に変換して公開できるというメカニズムの開発を目的として設立されたグループで、インターネット技術の標準化を推進しているW3C(World Wide Web Consortium)内の1組織として活動している。

このグループが目指す技術は、P3Pを利用するウェブサイトがそこで収集される情報の内容やその利用方法について自動的にユーザに通知し、P3P機能を備えたブラウザのユーザがそのウェブサイトにどのような内容の情報を開示するかを決断できるというものである。2006年にこのグループはその成果として標準仕様を公開したが、現在我々が利用する種々のウェブ上のサービスは、異なったプロバイダがそのバックエンドでアドホック的に構築しているものが多く、このような場合に複数のサイトとプライバシーポリシーを交渉しながらのブラウジングは複雑で、ユーザに混乱を与えかねず、プライバシー保護をより難しくするという評価がなされており、マイクロソフト社のインターネットエクスプローラやオープンソースのFirefoxなどの主要な閲覧ソフト(ブラウザ)には部分的にしか受

け入れられていない。

（３） Liberty Alliance

Liberty Alliance は IT、金融、通信、メディア、製造など業界をリードする企業と政府、教育機関などからなる大組織で、消費者のプライバシーと身元情報の安全性確保を目的に、連合的なアイデンティティ管理のための公開基準とガイドラインの策定を目指して設立された組織である。インターネットサービスの利用者が複数のウェブサイトに一度の認証でアクセスできるシングルサインオン・ソリューションの仕様はこのグループの成果であり、現在、教育、司法、医療、人事管理、通信、旅行など種々のセクターに跨った数多くの組織と数百万人に及ぶと言われるエンドユーザによって利用されている。またこの仕様を組み込んだ機器も世界中で広く使われている。

５．情報漏洩防止対策

これまで情報セキュリティ、特にプライバシー情報を取り巻く出来事とプライバシー情報を安全かつ簡単なやり取りで可能にする技術とその開発組織について述べてきたが、情報漏洩を防止するためには組織として一体となった取組みが必要であることは論を待たない。特に最近では、企業にとって情報漏洩が基本的に顧客のプライバシーに係わる問題に繋がるため、情報漏洩防止策と顧客のプライバシー保護をセットで捉える傾向が強い。

技術的な対策としては、情報をできる限り中央管理の下に置き、情報へのアクセス権限を設定し、アクセスした情報はアクセスした利用者のコンピュータに残さないシンクライアント（Thin Client）端末の導入、外部からの侵入を防ぐファイアウォールの設置、外部からの侵入を探知し、防止するシステム IDS（Intrusion Detection System）や IPS（Intrusion Protection System）の導入などが求められるが、ほとんどの企業においてはすでに大方の技術の導入は済んでいるものと思われる。

また技術的な対策に加え、組織とその運用面での対策も非常に重要であるとされている。企業では、「収集した顧客情報をどのように安全に管理するか」というセキュリティの面と「顧客情報をどのように取り扱うか」というプライバシーの両面から、情報保護体制を構築する必要性に迫られる。このためどの企業でも、情報のセキュリティ管理の総括責任者として Chief Privacy Officer（CPO）を設置し、プライバシーポリシーを策定し、これを遵守するためには社内研修などによる社員のセキュリティ意識の向上、業務プロセスの見直しなどを推進している。

一方、最新のセキュリティ技術を導入し、運用面で磐石な対策を実施したとしても情報漏洩のリスクを完全に除去することは事実上不可能と言ってよい。このため、リスク発生時に経済的損失を補償する「情報セキュリティ保険」が登場している。

情報セキュリティ保険では、一般に、ウィルスや悪意を持ったプログラムによって発生した損失、破損した重要な情報資産に対する被害、ネットワーク、情報システムへの攻撃によって妨害された事業被害、個人情報の漏洩やアウトソーシングなどによって発生した知的財産の侵害などの被害と訴訟のための費用、サイバー上の恐喝などに対処するための費用、サイバー攻撃などを受けた際の捜査協力への報奨金や信頼回復等のために要する広報活動の費用、サイバーテロ行為による被害補償、個人情報の窃盗による被害、などを対象としている。しかし保険を提供する保険会社は、個別に対象とする範囲やサービスの内容、補償条件などを様々に設定し、特徴を出している。例えば AIG 社は同社の AIG NetAdvantage でオンラインセキュリティ評価の無料実施や補償限度額２千５百万ドルを謳っており、CNAPro 社は当事者補償と第三者補償を謳っている。

情報漏洩の不祥事をマスコミが大々的に取り上げるようになった 2005 年当時に FBI と Computer Security Institute が実施した調査では、回答企業・機関 652 社のうち情報セキュリティ保険の利用は25%であったが、この情報セキュリティ保険市場は今後ますます成長していくものと見られている。

６．終わりに

個人のプライバシーを保護するという観点から情報セキュリティに関する米国の動向を概観した。個人のプライバシーはできる限りしまっておきたいと思う反面、プライバシー情報の一部を開示し、利用することによって、個人のみならず社会的にも利益を得ることが可能であるため、ビジネスとプライバシーの問題は今後もいろいろな角度から取り上げられ、議論されていくものと思われる。

人々はわずか 50 セントのクーポンのために個人情報を提供するというカーネギーメロン大学公共政策学部 Alessandro Acquisti 助教授による「スーパーマーケッ

トにおけるロイヤリティカードの発行に関する調査結果[*5]」は衝撃的であるが、個人が真にプライバシーの価値の重要性を認識し、開示する個人情報を自らコントロールして利便を得るような経済的取引を前提としたプライバシー情報の能動的活用は、プライバシー強化技術の発展とそれに伴う市場の形成によってますます盛んになるであろう。信頼のおける技術をベースに、安心して取引が行える環境を整備することが、喫緊の課題である。

プライバシー保護のための議論には、ネット上や情報システム上で発生しうる物理的な問題に対処する工学的アプローチのみならず、法律的、経済的、社会学的、心理学的な見地からそれぞれの専門知識を持ち寄った議論が必須である。技術を生かして生活を豊かにするためにも知恵の結集が求められている。

最後に本稿は、2007 年 11 月 29 日に日本大学法学部国際知的財産研究所開設記念シンポジウムにおいて「情報セキュリティとプライバシー保護」と題し講演した内容をもとに書き下ろしたものである。講演及び本稿執筆の機会を与えていただいた坂田桂三日本大学法学部長、山岡永知日本大学法学部国際知的財産研究所長、光田賢日本大学法学部教授、菅野政孝日本大学大学院法学研究科客員教授に感謝いたします。

（＊5） Privacy Lost: Does anybody care? by Bob Sullivan (http://www.msnbc.msn.com/id/15221095 に紹介されている。