

8F-04 ネットビジネス業者の「プライバシー保護対策」評価の提案

辰己 丈夫[†] 山根 信二[‡] 白田 秀彰[‡]

[†]神戸大学発達科学部 [‡]岩手県立大学ソフトウェア情報学部 [‡]法政大学社会学部

1 はじめに

インターネットの普及により、さまざまな問題・事件・事故が発生するようになった。現在の状況を見る限りは、これらの問題に技術・法律・制度上のさまざまな対策がとられている。しかし、こういった対策を施しても、問題・事件・事故はいっこうに減少しないどころか、むしろ、利用者の増加を上回る速度で問題・事件・事故が増え続けている。したがって、より安全な情報化社会を実現するには、今までに考えられなかったような効力を持った新しい原則と仕組みの導入が必要になるだろう。

本発表では「プライバシー」に関わる問題を取り上げ、現在行なわれている技術・法律・制度での対策の問題点を指摘する。そして「プライバシー情報」に対する適切な取扱いが、経済的な利益を優先することと一致するような制度として、プライバシー情報に使用料金を設定すること、情報取扱業者の格付けシステムを作ること、そのうえで保険システムを整備することを主張する。

2 原理的考察: 「プライバシー権」と「プライバシー情報」

「プライバシー」という言葉は、さまざまな意味で濫用されている。そのため議論が収束しないことが問題を複雑にしてしまっている。(IT 関連におけるテクニカルタームにおいても「プライバシー」は個人に関わる情報に限らず「秘匿性 (secrecy) 一般」と混同されている [1, 2].)

多くの文脈で用いられているように「プライバシー」とは「個人が自分に関わる情報の流通をコントロールする権利」とすると「プライバシーと結びつく情報は必ずしも保護されなければならないものではない」と

いうことになる。ここには言葉の混乱がある。前者では「情報」のことを「プライバシー」と呼んでおり、後者では「権利」のことを「プライバシー」と呼んでいる。そこで、本発表では以後、前者を「プライバシー情報」、後者を「プライバシー権」と使い分ける。

2.1 個人情報とプライバシー情報となりうる条件

「プライバシー情報」は実際には多様な情報からなりたっている。例えば、Gandy[3] は個人情報を以下の 11 通りに分類している。(1) 身元確認や資格についての個人情報 (2) 財務情報 (3) 保険情報 (4) 社会的サービス情報 (5) 公的サービス情報 (6) 不動産情報 (7) 娯楽情報 (8) 消費者情報 (9) 雇用情報 (10) 教育情報 (11) 法的情報

こうした情報が「プライバシー情報」となるには一定の条件がある。例えば「氏名」はそれ単独では「プライバシー情報」ではない。「その氏名」が特定の個人(あるいは、集団)と結びつくことが必要である。ここでいう「結びつき」が「この人の情報かも知れない」という程度の弱いもの(噂)でもそれが「プライバシー情報」になることがあるが、いずれにせよ、特定の個人と無関係な「氏名」は「プライバシー情報」となりえない。

同じように考えると、生年月日・学歴などの情報も、それ単独では「プライバシー情報」とはならない。しかし、住所や電話番号などは、その情報単独では確かに「プライバシー情報」ではないが、住所ならそこを訪ねることができるし、電話番号ならそこに電話をかけることができるという点で、本質的に異なるタイプの「プライバシー情報」である。

このように考えると「プライバシー情報」において特徴的な性質は「個人と結びついているか、結びつけることが可能である」ということになる。

2.2 「プライバシー情報」の具体的内容は何が定めらるか

前節で取り上げた「プライバシー情報」の具体的な要素は、絶対的に定まっているものではない。本項では、この点について考える。

A Proposal of Rating on the Protection System of Net-users' Privacy

TATSUMI Takeo[†], YAMANE Shinji[‡] and SHIRATA Hideaki[‡].

[†]Faculty of Human Development, Kobe University.

[‡]Faculty of Software and Information Science, Iwate Prefectural University.

[‡]Faculty of Social Sciences, Hosei University.

tatsumi@qef.h.kobe-u.ac.jp, s-yamane@soft.iwate-pu.ac.jp, hideaki@orion.mt.tama.hosei.ac.jp

2.2.1 メディア依存性

例えば、「個人の氏名と電話番号が結びついた情報」は、「プライバシー情報」として考えられるが、これは、「電話」という社会インフラが出来上がって初めて有効となる「プライバシー情報」である。その意味で、対策が放置されたまま普及することを繰り返さないためには、まだ登場していない情報メディアに対しても、そのメディアが「プライバシー情報」を扱う可能性があるのかもしれないかを検討する必要がある。

2.2.2 探索空間依存性

例えば、最近引っ越してきた隣人の氏名を新聞記事データベースに入力することで、隣人の(報道されるような)犯罪(検挙)歴の有無がわかるようになった。高速で大容量のデータベースが存在しなければ、このような情報を入手することは不可能である。

こういった情報探索は、新聞縮刷版が紙でのみ提供されていた時代には、現実的に不可能であった。このように、主にデータベース技術を始めとする情報処理技術の進展による探索空間の拡張が行なわれることで、「プライバシー情報」の具体的な要素は変わることがある。

2.2.3 「プライバシー情報」と技術の変化

ここまで述べてきたように、「プライバシー情報」としてとらえることができる情報は、技術的な進歩によって大きく変化する。従って、「プライバシー保護」のための原理・原則を考えるならば、それは、新しいメディア・新しい情報処理技術の出現可能性も前提とした規制手法をとらざるえない。

このことは実際の方策を見ても明らかだと思われる。例えば、アメリカが採用している「メディア毎の「プライバシー保護」方針」では新しいメディアの登場に追い付かないし、EUが採用している「プライバシー情報毎の保護方針」では情報処理技術の進歩に対応できないことになり、いずれの場合も適宜、保護対象や保護方針を修正しながら運用をする必要が生じる。

3 「プライバシー情報」の収集と利用

本節では、「プライバシー情報」が、どのように収集されて、どのように利用されているかについて考える。

3.1 「プライバシー情報」の収集

「プライバシー情報」が集められているものの代表として名簿がある。この場合の「プライバシー情報」は、買取業者が正当な名簿受取人から手持ちの名簿を入手し、入力、データベース構築という手順をたどって構築されていた。いわば、不正に入手された情報である。他にも、名簿印刷業者や名簿取扱担当者から情

報が漏洩する「組織内犯罪」や「非常に条件のいいアルバイト募集広告」を使って履歴書から収集する「無知につけこんだ情報収集」という手の込んだ手法も現れつつある。

しかし、最近では「プライバシー情報」を利用者から直接、堂々と収集する方が一般的である。例えば、現在、多くの企業が商品購入の際に生年月日・年収・趣味・家族構成などを申込書に書かせている¹。そして、このとき記入されたデータは顧客リストとなり、新商品の広告などに使われる。こうして集められた「プライバシー情報」は、その企業にとって価値のある情報であるから、一般には企業外部に漏洩することはない。しかし、その企業が算出する価値を越える価格で外部から購入希望があった場合、「プライバシー情報」が企業外に持ち出される可能性を否定できない。

3.2 「プライバシー情報」の利用

「プライバシー情報」の利用には、「経済的な理由を持たないもの」と「経済的な理由を持つもの」がある。前者は、心理的・感情的な理由でストーカー行為や差別に代表される反社会的行為に結びつくことが多い。一方後者は、利用する側の動機が経済的な利益に限定されているため、必ずしも反社会的行為に結びつくとは限らない。

個人の趣向や癖などは「プライバシー情報」として考えることができるが、大多数の人は「それを全く他者に知られたくない」とは思っていない。例えば、ダイレクトメールは、商品を購入する予定のない人にとっては全く無駄で面倒なものであるが、商品を購入しようという意志ある人にとっては非常に便利なものである。「プライバシー情報」について考えるとき、こうした形での利用が進んでいることを前提として、「プライバシー情報」のコントロールを考え直す必要がある。

3.3 「プライバシー情報」の経済的価値

情報処理技術が発展するにつれて、これまでに述べてきたような「プライバシー情報」の利用が進み、「究極の情報化社会」ともいべき状況が出現する可能性がある。

例えば、この社会では、飲料メーカーは、自動販売機に多くの種類の飲料を平均的に充填し、もっとも広い可能性において想定される顧客の嗜好に応えるよう備えておく必要がなくなる。彼らは、ある時間における顧客とその人数、嗜好を高い確度で予測しうるため、自動販売機の商品構成と充填方法を最適化することができる。

もし、私たち人間の一つ一つの行動のほとんどが予

¹RFC2706[4] “ECML v1: Field Names for E-Commerce”では業界団体によって一定のフィールドが提案されているが、普及しているとは言いがたい。

測可能になれば、それに見合った経済システムができる。その世の中では、「プライバシー情報」をすべて秘匿することは不経済な行為となる。もちろん、「そんな世の中はいやだ」と言って逃げ出す人もいるだろうが、システムが進むとそのような人の存在さえも計算されるようになるだろう。

このような仮定を敷衍させると、情報化社会のいきつく先で、経済的効率性という理由の下に、「プライバシー情報」が保護されなくなる可能性を指摘できる。

それに対する別の解としては、経済的効率性を備えながら自由度の高いシステムが考えられる。すなわち、プライバシーを守りたいという人は、守ることが選択でき、しかもそれが経済原理に叶うようなシステムである。このシステムについては事例分析を行なった後であらためて提案する。

4 事例分析: 「プライバシー情報」の漏洩

インターネットは、コンピュータを使った蓄積交換型のコミュニケーションメディアである。また、すべての情報がデジタル化されて流通するために、コンピュータが最も得意とするデータ処理の能力によって従来では非常に手間のかかる情報の収集や分類、抽出といったことを誰もが容易に行えてしまう。また、一度蓄積されたデータはコピーされることによって幅広く流通し、理論的には未来永劫まで残る可能性がある。

こういった特性は、利用方法によっては非常に有用となる反面、残ってほしくない情報まで影響されることによって問題を引き起こす。こうしたことに加え、誰もが簡単に参加できることから、以前のようなコミュニティベースで発展していた時代には考えもつかないような事象を経験するようになった。

本節では、プライバシーに関連した事件・事故の具体的分析を通じて、問題を深刻にし対策を困難にする特徴について考察する。

4.1 人材派遣会社名簿流出事件

人材派遣会社の9万人分の名簿データファイルが、データベースシステム開発をしていた契約社員によって持ち出され、この社員が開設したweb pageで販売されていた[5]。従来の名簿流出事件では、多くとも数千人の情報が流出しただけに過ぎないが、この事件では、9万人というこれまでにない多量の「プライバシー情報」が流出した。そして、これらの「プライバシー情報」は、デジタル化された情報であるから、容易に複製・再利用されることになった。

更に問題を深刻にしたのは、女性派遣社員のリストに、その女性の容姿に関する情報が含まれていたことである。9万人の紙で印刷された名簿の中から、一定の条件を満たす人だけをすべて抽出することは容易で

はない。しかし、デジタル化された情報ならば、このようなことは簡単である。

そして、この事件は犯人逮捕後も問題を残すことになった。9万人分の名簿のすべてのページのコピーを作成することは容易ではない。したがって、紙の名簿ならば、印刷された名簿そのものを回収すれば良い。もしこの事件が、紙の名簿ならば犯人逮捕からまもなく、「プライバシー情報」も回収されたであろう。しかし、この事件における「プライバシー情報」はデジタル化された複製が容易なデータであった。そのため、事件後も、名簿に登録されていた電話番号に、いたずら電話などがかかり続けた。

4.2 京都府宇治市住民基本台帳データ流出事件

京都府宇治市の住民基本台帳データが、同市の乳幼児健診システムの開発に携わった元大学院生によって持ち出され、データが名簿業者に販売された[6]。この事件で特徴的なのは、22万件という情報量の大きさであると同時に、市の「電算組織に係る個人情報保護条例」の改定時期と事件発生から逮捕が重なった点である。

個人情報の保護については、各自治体において条例などで法的な対策がとられるようになってきている。例えば、すでにあった条例を、インターネットなどにおける犯罪にも適応できるように変更するなど、こういった対策の一つである。この事件では、旧法が廃止され、罰則規定が改定されたため、「事件が起こったときの法律」で罰することができないということで、不起訴処分となった。市は、この判断を不服として控訴をしている。

こういった問題点は、法律運用上の問題点であり、本来ならば「プライバシー情報」に固有の特徴を示した事件であるとはいえない。しかし、「プライバシー情報」の漏洩事件が頻発する現在、不十分な技術的理解のまま法令を廃止してしまったということは、この種の問題に対して、「急速に進歩する技術」と法律面との両方を見る「複眼的な対策」を立てることが難しいということを示唆している。

4.3 PHP 顧客情報漏洩事件

PHP研究所(京都市)のホームページで、同社から書籍やビデオを購入した1万6000人以上の「プライバシー情報」が、外部からアクセスできる状態になっていたことがわかった[6]。

この「プライバシー情報」への外部からのアクセスは合計62回であったが、情報が公開されてから対策がとられるのが早かったことが事件の影響を減少させる方向に働いた。そのため、先述の「容姿ランキング」のついた名簿の流出と異なり、犯罪に結びつく危険はより少ない。

この事件の特徴は「プライバシー情報」の公開が誰も意図せずに行なわれたことである。すなわち、前述した2件の事件と異なり、この「プライバシー情報」を犯罪に利用しようという意図をもった人はいなかった。にも関わらず「プライバシー情報」が漏洩していることは注目すべきである。紙に印刷されている情報ならば「知らず知らずのうちに誰でも見ることができる状態になっていた」ということはない。複雑なインターネットの成り立ちや、コンピュータの設定の問題が理解できない限り、この種の事故は無くならない。

5 「プライバシー保護」対策の現状

このように「プライバシー情報」の漏洩・利用による犯罪が発生するようになったことから、その対策を考える動きが起ころはじめている。本節では、技術・法律・制度・教育のそれぞれの立場において「プライバシー保護」「プライバシー情報」漏洩対策がどのように行なわれているかを取り上げる。

5.1 技術的対策

W3CのP3P[7, 8] (Platform for Privacy Preferences) ではサービスのプライバシー・プロポーザルに対して利用者が合意するという枠組みを設計中である。しかし、業者が合意にしたがってサービスを行うという保証はない(すでに、経営破綻した企業がそれまでのプライバシー・ポリシーに反して顧客情報の売却を行なう事例も起きている)。さらに各国の法律が対応することを期待するのは非現実的であろう。

5.2 法律的対策

日本では、内閣が設置した「高度情報通信社会推進本部の個人情報保護検討部会」(座長・堀部政男)が「わが国における個人情報保護システムのあり方について(中間報告)」を提出し、さらに「個人情報保護に関する法案」の私案[9]が発表されている。この法案では、本発表で「プライバシー情報」と呼んでいる個人情報を、その情報対象者の意図しない利用をする者(法の違反者)に対し、制裁を与えるというものである。

法律の骨子として、以下の項目が挙げられている。(1) 個人情報を収集する際には目的を明確化し、本人確認する。(2) 目的外の利用・提供を制限する。(3) データ内容の漏えい防止策を義務付ける。(4) 個人情報保有状況の公開と本人への開示を行なえるようにする。(5) 個人情報保護の責任者を明確化し、苦情処理・相談窓口を設置する。

これらの法案に対して、各業界団体などからのヒヤリングが行なわれていて、いくつかの修正を経て国会に提出・立法化される見込みである。

5.3 制度的対策

このような技術的対策による不可能性の追求や、法律的対策による制裁システムの構築の他に「プライバシー保護」に関心のある組織を公に認定することで「プライバシー保護運動」を推進しようという制度的対策も取られている。

まず、通商産業省から「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1997年3月4日に発表され、このガイドラインを受けて「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(JIS Q 15001)」[10]が作成された。この「要求事項」に遵守している組織は、(財)日本情報処理開発協会(JIPDEC)より「プライバシーマーク制度」の使用が認められ、広告などにこのマークを使用することができるようになる。

ここでチェックする「要求事項」は「システム監査」の立場から作られたもので、組織や体制づくりなどを中心にチェックを行なっているという点が特徴的である。

このような安全をうたったプライバシーシールを表示するプログラムはアメリカでも民間ベースで進められている[11]が、仮にそのシールが適正なものだったとしても、そのシールがない業者に対しては何も情報を得ることができない。また、現段階では携帯型文字端末での表示について配慮されているとは言いがたい。

先の技術的対策と同じく「罰則規定が無い」、そして、組織制度面に注目するために「時代に即応した技術的検討がなされていない」という問題点を指摘できる。

5.4 教育的対策

今までに述べてきたような技術的・法的・制度的な対策が行なわれてきても、実際にシステムを管理するのは人間であり、法的制裁を加えるのも人間であり、制度は人の組織から作られる。したがって、こういった対策をネットワーク利用者の間に浸透させるためには、教育の問題を避けて通ることはできない。

しかし、現在の教育課程における初等・中等教育においては「プライバシー保護」を目指した内容はほとんど扱われていない。むしろ、競争社会時代の遺産をひきずった形で、児童・生徒の氏名や成績に代表される「プライバシー情報」が、積極的に学内で公開されている。このような学校社会で育ってきた子どもたちに「プライバシー情報」のコントロールの必要性を説くことは容易ではない。

一方で、これらの「プライバシー情報」を、学校がインターネットを通じて発信することに対して、強い抵抗感が保護者や教員の間にある。これは、児童・生徒の「プライバシー情報」が学外からでも検索できるようになることへの抵抗・嫌悪感であると同時に、防犯上の観点からも必要になったからである。だが、そ

の抵抗・嫌悪感が「犯罪の温床であるインターネットに情報を公開する」という未知なものに対する恐怖心から不必要に増大されていることも否めない。

新たな対策としては、2003年から高等学校でも新課程による教育が始まり、新しい教科「情報」の授業が必修教科として設置される。新教科「情報」では「情報モラル」という言葉で、情報処理機器利用上の注意点などを取り上げている。しかし、プライバシー関連問題は、約70%の学生が履修すると見られている「情報A」では、全体の約5%以下の時間しか扱われる見込みが無い。また、約30%の学生が履修すると見られている「情報B」では、プライバシー関連問題は、ほとんど扱われる見込みが無い。情報モラルなどの話題を重点的に扱っている「情報C」を履修することになる生徒は、最新の予備調査によれば、0%という数字が出ている。したがって、2003年以降も、教育課程の充実によって「プライバシー保護」対策がとられるようになるとはいえないだろう。

6 「プライバシー情報」漏洩に対する補償システムの提案

6.1 ビジネスモデルの提案

前節で述べてきた各種の対策は、インターネットが普及した後の情報化社会における「プライバシー保護」という観点での総合的な方策とはいえないのが実情である。我々はそれに対して、技術的に十分な検討を前提に「評価と保険」を中心としたシステムを確立することと、それを十分なビジネスモデルとして成立させるべきであるという提案を行なう。

6.2 補償問題

「不良品の発売」や「不適切な表現を含む書籍・新聞の発売」などと比べ、「情報の望まれない開示」固有の問題点として、「回収不可能性」がある。不良品は回収すればよいが、一旦、不特定多数に公表された情報は回収できない。物理的な「モノ」と「(特にデジタル化された)情報」の特徴の違いが、深刻な形で出現した例といえるだろう。

この問題を技術的手法で解決するならば、「複製すべきでない情報を照会するサイト」を設置し、すべての複製装置(ネットワーク上のバッファなどを含む)が、情報の複製を行なうたびにネットワーク経由でこのリストに照会するように作ることを義務づけるしかない。現実には、無効なクレジットカードの番号はこのような形で提供され、クレジットカードを使うたびに、そのカードが使用可能かどうかの確認が行なわれる。だが、クレジットカードよりも更に広く、すべての情報の複製に際して、このようなシステムへの照会を行なうよ

うに義務づけるのは、現時点でのネットワークインフラでは非現実的である。

同様に、既に本発表で指摘したように、法的・制度的対策の完全性を主張するには、人的信用を保証する必要がある。

そこで我々は「望まれざる情報の開示」を完全に防ぐ技術・法・制度的な対策がないならば、そのような開示を防ぐ経済的システムの提供が必要であると考えた。すなわち「望まれざる情報の開示」には、犯罪防止効果を期待できる程度の補償を行なう必要があるという仕組みである。

この仕組みの基本的な考え方は、第三者による情報の利用に対して利用権の持ち主が代償を要求できるというものである。すなわち、ここで提案する補償システムは「プライバシー情報」の内容が変動するのに対して、「プライバシー権」を静的なものとしてとらえ、その権利侵害に対する一種の補償金という形で、使用料を設定する仕組みである。

6.3 評価機関の設置

次に必要となるのが「プライバシー情報保護」に関する評価機関の設置である。例えば「プロバイダーAは顧客の個人情報保護できる体制を構築しているが、プロバイダーBではそのような体制ができていない」というようなことを外部機関で評価する。

先述したように、個人情報は必ずしも保護される必要はない。利用者によっては自らの個人情報が他者に利用されても気にならない人や、あるいは積極的に自分の個人情報を開示する人もいる。そのような人にとっては、個人情報保護に熱心なプロバイダーよりも、利用料金の安いプロバイダーを選ぶことができるようになる。

この評価機関は、本発表で述べた「技術的」「制度的」「(社員)教育的」な対策を評価できる機関となることが求められる。また、すでに実績がある債権/財務の格付け機関[12]と同じく、評価基準についての情報公開が行なわれ、複数の評価機関を選択できることが望ましい。

6.4 「プライバシー情報」漏洩保険

補償システムと評価機関が整えば、それを計算根拠として、「『プライバシー情報』漏洩保険」が商品として成立することになる。したがって、先ほどの評価機関は、保険会社の共同出資による運営が望ましいといえる。

例えば、自動車保険の場合は、事故の多い車種ほど保険掛金が高くなるように設定される。「プライバシー情報」漏洩保険は、先ほどの評価機関のランキングを元にして、プロバイダー毎の掛金を設定すれば良い。

そして、このような「補償金システム」「プロバイダ格付けシステム」「プライバシー情報漏洩保険」がすべて有効に機能しはじめれば、「プライバシー情報市場」が形成されるようになる。

7 比較と評価

最後に、最近のプライバシー関連ビジネスとの比較を通じて、本発表が提案するモデルの評価を行なう。

米イーノニマス・コム社 (enonymous.com) の調査と評価は昨年に話題となった。同社が開発した『advisor』は、ユーザーがサイトを訪れると、そのサイトの「プライバシーポリシー」の格付けを1つ星から4つ星までの4段階で表示する。

この外部評価の試みは本発表で扱った「プライバシー情報」保護の評価機関と同じ方向性を持っているが、経済的モデルと評価方法が異なる。同社のサービスではビジネスモデルが確立しておらず、運営においてはオンライン広告料に依存し、またいわゆる「プライバシー保護団体」の支援を受けている [13]。それに対して本提案では、意図され公表されたプライバシーポリシーを評価するのではなく、技術的・制度的・(社員)教育的な評価に注目している。さらに、格付け機関と漏洩保険によるビジネスモデルを提案することで、選択と補償のための新たなシステムを示した。これは従来のプライバシー保護対策にはない新規のアプローチである。

8 おわりに

本発表では「プライバシー情報」という枠組を導入して、個人と情報の結びつきを分析した。特に、情報処理技術の発展が「プライバシー情報」の範疇を変えてしまうことと、昨今の「プライバシー情報」に関連する問題・事件・事故を取り上げた。

こういった問題の多くは、心理的な動機ではなく、経済的な要因が事件を広範囲かつ深刻にしていくことを指摘した。そこで、技術・法律・制度・教育などの対策のみならず、経済的な効力が「プライバシー情報」の適切な流通とコントロールを促す仕組みとして「プライバシー情報利用権」を確立して使用料金の算出を容易にすると共に、「プライバシー情報」の保護に関する格付け機関と保険制度の導入を提案し、類似サービスとの比較評価を行なった。

今後は、このような「プライバシー情報ビジネス」の成立可能性を議論するとともに、「格付け機関が調べるべき項目」を具体的に提案する予定である。また、不正アクセス防止法に違反しないようにしながら、プロバイダや一般企業の「プライバシー情報保護方針」を正確に調査するための技術開発も検討したい。

参考文献

- [1] Garfinkel, S. L.: Privacy, Please, *Information Security*, Vol. 3, No. 4 (2000), <http://www.infosecuritymag.com/apr2000/-logoff.htm>.
- [2] Shirey, R. W.: Internet Security Glossary, *Request For Comments* (2000), RFC 2828 (Also FYI 36) (Status: Informational), 212 pages.
- [3] Gandy, O. H.: *The Panoptic Sort: A Political Economy of Personal Information*, Westview (1993), Cited in 田畑暁生: 個人情報論序説, 人間科学研究, 神戸大学発達科学部 (1998).
- [4] Eastlake, D. and Goldstein, T.: ECML v1: Field Names for E-Commerce, *Request For Comments* (1999), RFC 2706 (Status: Informational).
- [5] 相池謙: "美人格つけ付き"九万人派遣社員リスト, 別冊宝島, 487, インターネット事件簿, pp. 43-45, 宝島社 (2000).
- [6] 毎日新聞: インターネット事件を追う, <http://www.mainichi.co.jp/digital/netfile/> (2000).
- [7] Reagle, J. and Cranor, L. F.: The Platform for Privacy Preferences, *Commun. ACM*, Vol. 42, No. 2, pp. 48-55 (1999).
- [8] Ackerman, M. S. and Cranor, L. F.: プライバシー保護のためのエージェント, *UNIX Magazine*, Vol. 15, No. 2, pp. 127-131 (2000).
- [9] 高度情報通信社会推進本部個人情報保護検討部会: 個人情報を保護するための「基本法」(私案) (1999).
- [10] (社)情報サービス産業協会: プライバシーマーク制度 (JIS Q 15001) における「システム監査ガイドライン第1版 (1999).
- [11] Benassi, P.: TRUSTe: An Online Privacy Seal Program, *Commun. ACM*, Vol. 42, No. 2, pp. 56-59 (1999).
- [12] 黒沢義孝: <格付け>の経済学, PHP 新書 069, PHP 研究所 (1999).
- [13] Reuters, : The New E-Industry: Privacy, *Wired News* (1999), October 11. <http://www.wired.com/news/business/-0,1367,31841,00.html>.

本研究は財団法人電気通信普及財団による平成11年度の研究調査助成を受けている。

本発表は、情報処理学会 第 62 回全国大会 (平成 13 年前期) 特別トラック (3) 講演論文集 (pp.111-116) に収録され、9 件の大会優秀賞のうち 1 つに選ばれた。

利用上の注意事項 ここに掲載した著作物の利用に関する注意 本著作物の著作権は(社)情報処理学会に帰属します。本著作物は著作権者である情報処理学会の許可のもとに掲載するものです。ご利用に当たっては「著作権法」ならびに「情報処理学会倫理綱領」に従うことをお願いいたします。

Notice for the use of this material The copyright of this material is retained by the Information Processing Society of Japan(IPSJ). This material is published on this web site with the agreement of the author(s) and the IPSJ. Please be complied with Copyright Law of Japan and the Code of Ethics of the IPSJ if any users wish to reproduce, make derivative work, distribute or make available to the public any part or whole thereof. All Rights Reserved, Copyright©Information Processing Society of Japan. Comments are welcome. Mail to address editj@ipsj.or.jp, please.

概要

インターネットが普及するにつれて、さまざまな問題が生じるようになってきた。そのなかでも「プライバシー関連」といわれる問題には、技術的対策、法律的対策、制度的対策などが考えられてきた。しかし、どの対策も完全にプライバシー情報の漏洩を防ぐことは出来ない。

プライバシー情報が持つ「回収不可能性」という特徴を考えると、こういった情報が洩れないようにする対策を考えるよりも、むしろ、洩れたときの補償システムを充実させる方法がより効果的である。そこで、本発表では、1. 「プライバシー情報利用補償金の算出の仕組み」2. 「プライバシー情報取扱業者の格付け」3. 「格付けに応じたネットワークカーズ保険」のそれぞれを成立させるべきであるという提案をする。そして、従来のプライバシービジネスとの比較評価を行なう。

Abstract

As the Internet became readily accessible to the general public, the term “privacy” came to refer to everything from personal information: name, birthday, sex, postal address, office, and so on. Current discussions on “privacy” tend to be about how to protect these information. For example, encryption method is technical idea, but this method is not perfect. The restrictions by the law which are related human privacy is no perfect also. The privacy mark system is adopted for these years. But this mark is not popular and this system do not work well.

Once someone's information are opened, we cannot collect nor trash all information. The garbage collection system of personal information do not work. So we insist to build 3 systems: 1. the system for evaluating fee of one's privacy information, 2. the ranking system for online trader/seller companies. 3. the insurance system based on the fee and the rank of trader/seller.