

報 告

電子社会における
匿名性と可視性・追跡可能性
—その対立とバランス—



平成20年（2008年）7月24日

日本学術会議

法学委員会「IT社会と法」分科会

この報告は、日本学術会議「IT社会と法」分科会の審議結果を取りまとめ公表するものである。

日本学術会議「IT社会と法」分科会

委員長	池田 眞朗	(第一部会員)	慶應義塾大学大学院法務研究科教授
副委員長	堀部 政男	(連携会員)	一橋大学名誉教授
幹事	野澤 正充	(連携会員)	立教大学大学院法務研究科教授
	青山 善充	(第一部会員)	明治大学法科大学院院長
	井上 由里子	(連携会員)	神戸大学法学研究科教授
	岡村 忠生	(連携会員)	京都大学大学院法学研究科教授
	金山 直樹	(連携会員)	慶應義塾大学法務研究科教授
	鈴木 秀美	(連携会員)	大阪大学大学院高等司法研究科教授
	泉水 文雄	(連携会員)	神戸大学法学研究科教授
	園田 寿	(連携会員)	甲南大学法科大学院教授
	多賀谷 一照	(連携会員)	千葉大学法経学部教授
	松村 良之	(連携会員)	千葉大学法経学部教授
	松本 恒雄	(連携会員)	一橋大学大学院法学研究科教授

要 旨

1 作成の背景

情報通信技術の急速な進展に伴い、現代社会では、インターネットを用いた名誉毀損やプライバシー侵害、電子商取引における詐欺や迷惑メールの問題など、その匿名性を利用した様々な問題が生じている。半面、個人情報のネットワークシステムへの蓄積やネットワークの追跡技術も進展し、個人情報に対する捕捉可能性が高まった結果、その私的領域への侵入が可能となり、個人のプライバシーが暴かれる危険性も高まっている。

これらの問題状況を踏まえて、本委員会では、「電子社会における匿名性・追跡可能性・可視性」をテーマに、慎重な審議を経て、本報告をとりまとめた。

2 現状及び問題点

近代化、都市化の進行とともに社会の匿名性が増大してきた。そして、近年における情報通信技術（ICT）の急速な進展に伴い、この匿名性の問題は、大きく変容している。すなわち、一方では、匿名性の極端な進行であり、具体的には、迷惑メール、ネット上における名誉毀損、あるいはネットを用いた詐欺など、匿名の加害者による違法行為が頻繁に行われている。他方では、このような匿名性と不可視性の半面、個人情報のネットワークシステムへの蓄積と、ネットワークの追跡技術の著しい進展に伴い、個人情報に対する追跡可能性と捕捉可能性は著しく高まっている。その結果、人々は、プライバシーの曝露の危険性と、私的領域への侵入の危険性、そして欺罔行為に遭う危険性にさらされている。もっとも、情報通信技術の発展は、追跡可能性と可視性とを実現することによって、人々の生活や取引における安全・安心を実現しているという側面も有している。

このように、現代社会は、情報通信技術の著しい進展とともに、匿名の社会のようでありながら、可視性の高い社会という、微妙な均衡の上に成り立っている。そこで、本報告においては、「電子社会における匿名性、追跡可能性、可視性」が問題とされる7つのトピックをとりあげてこれらのバランスを検討するとともに、プライバシー情報の取得に対する市民意識調査の分析も加えた上で、電子社会における法制度設計に関して若干の提言を行うこととした。

3 報告の内容

電子社会における匿名性・追跡可能性と可視性に関する諸問題について、以下のような検討を行った。

(1) 名誉毀損・プライバシー侵害の書込みについては、匿名者の表現の自由は保護に値せず、その可視性および追跡可能性を最大限に認めるべきである。

(2) 迷惑メールについては、国内的には、電子メールの追跡可能性が確保され、今後の大幅な減少が期待される。しかし、海外において発信された迷惑メールの減少のためには、海外のISPや規制当局との連携が不可欠である。

(3) 個人情報の流通については、個人情報保護法によって取り扱いに関するルールが確立した。しかし、最新のテクノロジーにより、自己情報の追跡可能性は失われ、そのコントロールは不可能となっている。そこで、自己情報コントロール権を超えた「自己情報保護期待権」を認めるべきである。

(4) ネット販売については、インターネットによる詐欺の被害を防止するために、システム構築者の最低限の法定責任を認める立法が望ましい。

(5) 債権取引については、匿名性を排除し、可視性および追跡可能性のある電子記録債権を導入したことは適切である。しかし、これが本来の目的である中小企業の資金調達の活性化につながるよう、その周知を徹底させるとともに、利用者の便益を十分に考慮した制度基盤の整備を行う必要がある。

(6) 租税申告の電子化は、納税義務者と課税物件とを正確に結びつけることを可能とする技術であり、納税者を個人として尊重する税制を実現しうるものである。しかし、国が個人とその取引とを個別に把握することに対しては、プライバシーの観点からは問題もあり、電子化が個人の匿名性を奪う方向にも作用することには注意が必要である。

(7) ネットの匿名性と有害情報の規制については、民間の中立的な第三者機関が行った情報の評価を前提に、それぞれのユーザーが自主的に情報をコントロールできる仕組みを構築することが望ましい。

(8) プライバシー侵害については、市民意識を調査すると、侵害自体が可視性の低いものになってきているところに問題が見出せ、プライバシー保護について、可視性の高い形での法律的技術的制度を確立することが必要である。

以上の分析から、結論として、IT化の制度設計においては、匿名性と可視性・追跡可能性との最適バランスを探求すべきことを提言する。

目 次

1	はじめに	1
2	名誉毀損・プライバシー侵害の書込み	2
3	迷惑メール	4
4	プライバシー・個人情報の流通	7
5	ネット販売	10
6	電子記録債権と匿名性・可視性・追跡可能性	13
7	租税におけるアイデンティフィケーションと電子化	16
8	ネットの匿名性と有害情報規制	19
9	プライバシー侵害に対する人々の意識 —情報の悪意の取得と関連させて	22
10	おわりに —まとめと若干の提言	24

1. はじめに

近代化、都市化の進行とともに社会の匿名性が増大してきたが（それは、社会的にはコミュニティの崩壊という形で表れる）、ここ 10 年の電子技術、ネットワーク技術の進展（それは、現実世界からバーチャルワールドへという変化を含んでいる）に伴って、この匿名性の問題は大きな変化を受けているように思われる。すなわち、一方では匿名性の極端な進行である。それは人々の日常生活の世界で非常に強い形で進行している。具体的には、迷惑メール、ネット上における名誉毀損、あるいはネットを用いた詐欺のように、加害者がバーチャルな世界で匿名で現れるだけで、不法行為がまかり通るのである。他方で、この一見したところの、一般のネットワークユーザーが抱く匿名性と不可視性のうらで、個人情報のネットワークシステムへの蓄積と、ネットワークの追跡技術の著しい進展に伴って、個人情報に対する追跡可能性と捕捉可能性は著しく高まり、我々は、プライバシーの曝露の危険性と、私的領域への侵入の危険性、そして欺罔行為に遭う危険性にさらされているのである。

すなわち、現代社会は、電子技術、ネットワーク技術の著しい進展とともに、匿名の社会のようで、可視性の高い社会という、微妙な均衡の上に成り立っているのである。

本報告は、以下 2 から 8 までで個別の論点を扱い、9 で、情報取得とプライバシー侵害というテーマに限ってであるが、そのような IT 社会の構成員たる市民の意識の問題を考察する。個別論点は、情報、プライバシー、知財、電子契約、債権取引、租税、刑事、と多岐に渡り、日本学術会議法学委員会の IT 関係研究者の知見を横断的に集める形を取ることができたと考える。以上の考察をふまえ、末尾においてまとめと若干の提言を行う。

2 名誉毀損・プライバシー侵害の書込み

(1) 侵害行為の特質

名誉を毀損されまたはプライバシーを侵害された被害者は、加害者に対して、損害賠償の請求（民 709 条）をすることができるほか、侵害行為の差止めまたは毀損された名誉の原状回復（民 723 条）を求めることができる。しかし、インターネットによる名誉毀損やプライバシーの侵害においては、①加害者（情報発信者）が匿名であるため、その特定が難しい。しかも、②インターネットによる情報の発信は、誰でも容易に行うことができ、かつ、③一瞬のうちに全世界のコンピュータに配信される。これに対して、従来の名誉毀損・プライバシー侵害の事例においては、加害者が特定され、その媒体もマスメディアなどに限定されていた。しかも、マスメディアを利用できる者は限られているため、侵害の拡大にも限界があった。したがって、インターネットによる名誉毀損などでは、加害者をどのように特定するか、そして、その侵害が拡大する前に、どのようにその侵害を防ぐかが重要である。

(2) 情報発信者の特定（追跡可能性）

被害者が加害者に対して損害賠償請求をするためには、匿名の加害者を特定しなければならない。そこで、被害者は、プロバイダに対して、侵害情報の発信者の情報を開示するよう求める必要がある。その法的根拠となるのが、平成 13 年 11 月 30 日の「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」（プロバイダ責任制限法）である。同法 4 条 1 項によれば、開示請求は、次の 2 つのいずれにも該当する場合にのみ、行うことができる。すなわち、「侵害情報の流通によって当該開示の請求をする者の権利が侵害されたことが明らかであるとき」（1 号）、および、「当該発信者情報が当該開示の請求をする者の損害賠償請求権の行使のために必要である場合その他発信者情報の開示を受けるべき正当な理由があるとき」

（2 号）である。そして、この要件が満たされれば、被害者は、プロバイダに対し、発信者に関する以下の情報の開示を請求することができる。すなわち、①発信者その他侵害情報の送信に係る者の氏名又は名称、②その住所、③発信者の電子メールアドレス、④侵害情報に係る IP アドレス、および、⑤侵害情報が送信された年月日・時刻である（特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律第 4 条第 1 項の発信者情報を定める省令）。他方、プロバイダは、開示請求を受けたときは、原則として、「開示するかどうかについて当該発信者の意見を聴かなければならず、かつ、「当該発信者情報をみだりに用いて、不当に当該発信者の名誉又は生活

の平穩を害する行為をしてはならない」。それゆえ、プロバイダは、発信者に対して損害賠償責任を負うおそれもある。そうだとすれば、結局は、プロバイダが裁判外で開示請求に応じることはなく、現実には開示請求訴訟が提起されよう。

(3) 差止請求の問題点

プロバイダに対する侵害情報の削除等の差止請求の可否については、規定がない。そこで、人格権に基づく差止請求権が問題となり、これが認められることは、最高裁判例によって明らかである（最大判昭和 61・6・11 民集 40 卷 4 号 872 頁—北方ジャーナル事件）。もともと、この判決は、「言論、出版等の表現行為により名誉侵害を来す場合には、人格権としての個人の名誉の保護（憲法 13 条）と表現の自由の保障（同 21 条）とが衝突し、その調整を要することとなるので、いかなる場合に侵害行為としてその規制が許されるかについて憲法上慎重な考慮が必要である」とした（なお、最判平成 14・9・24 判時 1802 号 60 頁も参照）。インターネットによる名誉毀損等の書込みに対しても、同様に被害者は、人格権に基づく差止請求権をプロバイダに対して行使できると解すべきである。その際には、次の 2 点に留意すべきである。第 1 に、最高裁の事案はいずれも、表現の自由という民主主義の根幹的な人権と人格権との衝突が問題となるものであった。しかし、ここで問題となるのは、名誉毀損やプライバシー侵害など、表現の自由の保護の範囲外のインターネットへの書込みである。第 2 に、最高裁の事案は、事前抑制に関するものであり、差止請求の可否は慎重な検討を要する。これに対して、プロバイダに対する侵害情報の削除要求は、すでに表現されたものを不適切であるとして削除するものである。しかも、放置しておく、その情報はさらに範囲を拡大し、被害者の人格権の回復が困難となるおそれが大きい。そうだとすれば、プロバイダに対する差止請求は、より積極的に認められてよいであろう。

(4) 小括

匿名者の表現の自由は、名誉毀損等の侵害事例では保護に値せず、その可視性および追跡可能性を最大限に認めるべきである。

3 迷惑メール

(1) 迷惑メールの氾濫

一方的に送信されてくる広告を内容とした迷惑メールの数は、増加を続けており、世界中でやりとりされている電子メールのうちの7～8割は迷惑メールだと言われている。これは、電子メールには、送信コストが安い、送信作業の自動化・大量送信が可能、自ら送信設備を設置して送信することもできるなどの特徴があるためである。

迷惑メールの横行によって、受信者側には、確認して削除する手間、誤って必要なメールを削除するリスク、不愉快な文面を読まされる精神的苦痛、出会い系サイトやワンクリック詐欺などの悪質商法に誘い込まれる危険性、メール到達の遅れなどが生じており、また、メールの送受信を媒介するインターネット・サービス・プロバイダ（ISP）にも設備状況のための負担増が生じている。当初は、携帯電話への送信が主であったが、法規制を背景とした携帯電話事業者の約款ベースでの対策が一定の成果をあげたことから、現在は、パソコンへの迷惑メールが圧倒的多数を占めるようになっている。また、海外から、外国語による迷惑メールのみならず、日本語の迷惑メールも多数送信されてきている。

このような事態に対処するために、2002年の「特定商取引に関する法律」（以下、「特商法」）の改正により、消費者が電子メールによる広告の受け取りを希望しない旨の連絡を事業者に行った場合には、その消費者に対する今後の広告の送信を禁止するとともに、そのような連絡が可能となるように、消費者が事業者に対して連絡する方法の表示が義務づけられた。同年には、「特定電子メールの送信の適正化等に関する法律」（以下、「特定メール法」）も成立した。特定メール法でも、対象は広告メールであり、改正特商法と類似の規定（ただし、特商法とは異なり業種や商品等の限定はない）のほかに、架空メールアドレス宛の送信の禁止、一時に多数の架空アドレス宛に送信がなされた場合の通信事業者の役務提供拒否権等も定められた。特定メール法は、2005年に、送信に用いたメールアドレス等の送信者情報を偽った送信を禁止するとともに、その違反に対して刑罰を科す等の法執行の強化を図るための改正がなされた。いずれの法律においても、一方的に送り付ける広告メールについては、件名欄に「未承諾広告※」と記載することが統一して義務づけられた。

(2) 電子メールにおける追跡可能性の欠如

しかし、このような法規制にもかかわらず、冒頭に指摘したように、とり

わけパソコンにおける迷惑メールは増加の一途をたどっている。これには、①送信者情報の偽装が容易であるという現在のメールシステムの技術的欠陥や、②インターネットに直結した他人のコンピュータにウィルスを送り込むことによって事実上のっとり（「ゾンビPC」、「ボット化」と呼ばれる）、そこを中継点にした迷惑メールの送信が広く行われていること、言い換えれば、電子メールに技術的追跡可能性が確保されていないことに原因があるとともに、ISPにとって追跡可能な場合であっても、③アドレスを含む送信者に関する情報が通信の秘密としてきわめて強く保護されているため、受信者側でそれを把握することができないという法的追跡可能性の遮断に原因がある。この例外として、「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」（プロバイダ責任制限法）による発信者情報開示請求の制度が存在するが、適用される場合が限定されており、迷惑メールの送信元の開示請求には使えない。

（3）電子メールにおける追跡可能性の確保

そこで、一方で、送信者情報を偽ったメールを中継しないようにするための種々の技術（送信ドメイン認証制度やアウトバウンドポート 25 ブロック等）の開発、導入を進めることによって、技術的追跡可能性の確保が図られた。

他方で、送信に用いたメールアドレス等の送信者情報を偽った送信を禁止し、違反に刑事罰を科すという特定メール法の 2005 年改正がなされたねらいの一つは、違反を犯罪とすることによって、警察による捜査令状に基づく ISP からの送信者情報の把握を可能にし、追跡可能性を回復することにあつた。さらに、2008 年の通常国会では、法執行に必要な限度で、ISP から契約者に関する情報の提供を求める権限を総務大臣に付与する特定電子メール法の改正案が成立した。

また、2008 年の通常国会では、従来のオプトアウト制（今後送信しない旨の通知を受けた場合にのみ当該アドレスへの送信禁止）からオプトイン制（送信の事前承諾のない受信者への送信の禁止）へと規制をより厳しくすることが、特定電子メール法の改正と特商法の改正の双方に盛り込まれた。

従来から、迷惑メールの法規制における最大の争点は、オプトイン規制かオプトアウト規制かであった。従来のオプトアウト規制の狙いは、今後の広告メールの受信を望まない場合にはその旨を広告主や送信者に通知し、以降の広告メールの送信について禁止することによって、広告主の営業の自由と受信者のプライバシーの保護を両立させようとするところにあつた。しかし、送信者情報を偽った迷惑メールの追跡可能性がないことにより、受信拒否の

返事を送ることは、生きたアドレスであることを悪質業者に教えるという結果になり、一層の迷惑メールの増加の引き金になりかねない。そのため、消費生活センター等では、受信拒否の通知を送らないようにとの、法律の趣旨に反した消費者啓発をせざるをえないという倒錯した状況にあった。

今回の改正によるオプトイン規制への転換により、オプトアウト規制の場合に比べて、迷惑メールの法律違反の立証が格段に容易になり、さらに、法律違反の迷惑メールについて、総務大臣にISPに対する契約者情報の提供を求める権限が与えられることにより、追跡可能性をかなりの程度回復することが可能となった。

（４）海外との連携の必要性

このように国内的には、電子メールについての技術的追跡可能性がある程度まで確保され、また、法的追跡可能性も部分的に回復したことによって、国内発の迷惑メールの大幅な減少が期待されるが、海外発の迷惑メールの減少のためには、海外のISPや海外の規制当局との連携が不可欠である。そのための積極的イニシアチブを日本がとることが求められる。

4 プライバシー・個人情報の流通

(1) プライバシー・個人情報のコントロール不可能性の認識

① 共通テーマとの関連性

電子社会におけるプライバシー・個人情報は、共通テーマである「電子社会における匿名性と可視性・追跡可能性」ないしその反面である「電子社会における識別性と不可視性・追跡不可能性」と様々な局面で関係している。例えば、匿名性のある個人情報は、日本の個人情報の保護に関する法律（平成15年法律第57号）の定義（2条）からすると、「個人情報」には該当せず、また、その取扱いはブラックボックス化して可視性は失われ、さらに、本人の意図しないところに流通し、追跡可能性は無意味になっている側面が飛躍的に増大してきている。

電子社会におけるプライバシー・個人情報の流通については、それ以前の社会におけるプライバシー・個人情報の保護の延長線上で論じることが可能な側面と新たな視点が必要な側面とがある。

② 情報化社会の進展とプライバシー・個人情報の保護論議の展開

個人情報保護の基礎にあるプライバシー権については、様々な議論はあるが、プライバシー権は、「ひとりにしておかれる権利」(right to be let alone)（伝統的プライバシー権）という消極的な権利から、「自己情報コントロール権」(right to control one's own information)（現代的プライバシー権）という積極的な権利を含むものへ発展するようになったと理解することができる。

また、ヨーロッパでは、このようなプライバシー権について議論しながら、データ保護の立法化も論じられるようになった。

1970年代に入ると、プライバシー・個人情報の保護への立法的対応が実現し、また、それをめぐる議論が活発化してきた。それは、今日でも国際的には続いているが、その比較的早い段階で議論を集約したのが、OECD（Organisation for Economic Co-operation and Development, 経済協力開発機構）の「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)（1980年9月23日に採択）であった（「プライバシー・ガイドライン」として引用されることがある）。これは、国際的に大きなインパクトを与え、日本も大きな影響を受けている。

③ 日本の個人情報保護法の意義と限界

ヨーロッパでは、1970年代からデータ保護法が制定されるようになったが、日本では、国レベルにおいてはそれらのデータ保護法先進国よりも20年以上も遅れて、2003年5月23日にようやく参議院本会議で個人情報保護法（正式には「個人情報の保護に関する法律」）が可決成立した。これは、同年5月30日に公布・一部施行された。全面施行されたのは、2005年4月1日であった。しかし、同じ日に成立し、同じ日に公布され、同じ日に施行された個人情報保護関係の法律は、他にもある。それは、行政機関・独立行政法人等に関する個人情報保護法等である。

日本の国レベルで個人情報の取扱いに関するルールが確立したことの意義は大きいですが、個人情報にかかわる新たな問題には必ずしも対応することができず、限界がある。

④ 最新テクノロジーとプライバシー・個人情報の保護の必要性

いつの時代にも新しいテクノロジーが出現し、法の世界ではその対応のあり方が論じられる。プライバシー・個人情報も、最新テクノロジーの挑戦を受けている。

このような問題についても、1980年にプライバシー・ガイドラインを策定したOECDで議論してきている。それらも踏まえて最新テクノロジーとプライバシー・個人情報の保護のあり方について見ることにする。

最新テクノロジーは、個人情報の収集、蓄積、利用等の方法に新たな問題を投げかけている。次のような例をあげることができる。

- ・個人情報の蓄積が安価になり、削除する方が蓄積するよりも費用がかかる。そのため、個人情報は削除されずに蓄積され続けることになる。
- ・マウスをクリックするだけで個人情報は瞬時に移動し、それには事実上費用がかからない。
- ・サーチエンジン、位置情報サービス、RFID（電子タグ）、センサーなどに見られるように、個人情報処理のツールは強力で、至る所にあり、また、安価であるため、個人情報は検索、リンク、トレースが容易な面もある。

これらの例においては、自己情報の追跡可能性はほとんど失われ、コントロールは不可能になってきている。

(2) 自己情報保護期待権の提唱と保護のメカニズム構築の必要性

① 自己情報コントロール権を越える権利概念の考案

これらの例に見られる個人情報の流れに対応してプライバシー・個人情報

の保護のあり方が検討されなければならない。自己情報コントロール権は、個人が自己の情報がどこにあるかを推測し、しかもそれを保有している者に開示請求等の権利を行使することが可能な状態を前提としている。しかし、最近では、コントロールが困難な状況にある。そのため、自己情報コントロール権を越える権利概念を考案しなければならないと考える。

② 自己情報保護期待権の構築

上記のような状況においては、自己情報コントロール権というよりも、「自己情報保護期待権」とでもいうような権利性の低い概念で表現することが考えられる。これを英語で仮に表現してみるならば、**legitimate expectation of one's own information protection** とでもなるであろう。

最新テクノロジーとの関係では、このような期待権を構築し、その保護策について、国内的にはもとより、国際的にも、メカニズムを考案しなければならない。その最近の例については後述する。

③ 3つの権利概念の併存と状況対応の権利主張の必要性

自己情報保護期待権は、不可視的状況において、自己情報追跡可能性が失われる状況で主張すべきであるが、前述の「ひとりにしておかれる権利」も「自己情報コントロール権」も、併存しており、自己情報が置かれている状況で主張することができるので、それぞれそうすべきである。しかし、最新テクノロジーとの関係では、自己情報保護期待権を明確に意識し、侵害が生じたと感じる場合には、保護のメカニズムの発動を要請すべきである。

④ OECD プライバシー保護法執行における国際協力勧告（2007年）

プライバシー・個人情報情報が瞬時にして国境を越えて地球を駆け巡る状況に対応することも踏まえ、2005年からプライバシー保護法の執行に関する国際協力について検討してきた。これに直接かかわってきたが、2007年6月12日に「プライバシー保護法の執行における越境協力に関する勧告」(Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy)を採択した。

各主権国家が自己の主権に基づいてプライバシー・個人情報保護を制定する現代世界においては、各主権国家が相互に協力することが肝要である。

OECDのメカニズムも、自己情報保護期待権に対応可能である。そのような期待権を保護するためには、関係者が期待権にすぎなくなっていることを認識し、それに応じられるように最善の措置を講じることが必要であることを強調したい。

5 ネット販売

(1) はじめに

ネット販売に特有の詐欺が横行している。それは、売手・買手の双方についてありうる。代金を受け取っても品物を渡さない、別の品物を渡す、金を払うつもりがないのに落札して物品を受け取る等が、その手口とされている。この点につき、「最近ではネットオークション詐欺被害者の補償制度を導入するオークションサイトがほとんどであるが、被害特定から補償までの手続きが煩雑であったり、あるいは被害認定が受けられない場合もあり、依然として自己防衛が必須である」とされている（ウィキペディア「オークション詐欺」）。

だが、ネット取引においては自己責任・自己防衛といったところで、そこには自ずから限界がある。法的な対応ないし規制が求められるゆえんである。

以下では、まず、法的検討の出発点として、サイト運営者の地位を明らかにし(2)、その上で、現状として、サイト運営業者が用意している補償制度の内容の問題点を検討し(3)、最後に、若干の提言を行う(4)。

(2) サイト運営者の法的地位

サイト運営者は、決してネット販売を通じて行われる取引の契約の当事者になることはない。たとえば、ある会社の利用規約では、会社側はあくまでも「利用者が商品等の出品、入札または落札を行うためのシステムを提供し、これにより出品者と落札者との間で本取引を行う機会を提供」するに留まり、「本取引に係る契約は出品者と落札者との間で直接成立するものであり、当社は本取引に係る契約の当事者とはなりません」とされている。

だが、サイト運営者は、出店者および購入者との間で、仲介サービスを提供する契約をしている。とくに、出店者は、月額の利用料（月2万～5万円）および「システム利用料」として売り上げの2%～6.5%をシステム運営者に支払うことになっている。購入のための利用者も、システム運営会社との合意の下に取引に参加しており、しかも、その支払う代金の一部は「システム利用料」の名目で必ず運営会社に支払われることになっている。したがって、ネット販売のシステム自体によって被害が生じないようにすることは、システム管理者としての当然の責任だといえるべきである。つまり、事業として財貨交換の場を提供した者の責任が明確化されなければならないと考えられる。

そもそも、ネット取引は、サイト運営者の構築・維持するシステムなしには成立しえない。サイト運営者は、むしろ積極的にビジネスモデルとしてネット販売という取引システムを構築したわけであって、その場に立ち入った

がために被害を受けた者に対しては、システム構築者としての責任が認められるべきである。システム構築者責任は、銀行カード盗難の場合において債権の準占有者に対する弁済といえるかという点をめぐる判例の発展によって認められつつある責任であり、これが銀行の約款の自由に対する規制法理として働いている。これが今後のネット取引規制の〈基本原理〉として認められるべきだと考える。

(3) 補償規定

すでに各社によって補償規定の整備が進められている。その代表的なものを1つ検討しよう。

ある会社の提供する補償規定によると、要件は、①詐欺罪の被害であること、②金銭を払ったにもかかわらず商品が届かないか、商品を送付したにもかかわらず代金が支払われない場合である。そこで除外されるのは、「送付された商品の破損・瑕疵・欠陥等による損害や、商品の数量・外観・性能・品質・精度等に関する出品者と落札者の見解の相違に基づく紛争など民事上の債務不履行に該当する場合」、および、「取引のキャンセルおよび解除（商品到着後の返品にかかわるトラブルも含む。）による場合」である。しかも、「相手方の氏名・住所・電話番号を確認せずに取引をした場合など、社会通念上、取引に際して利用者に求められる注意義務を欠いたと認められる取引」についても、除外となる。その上、補償金を受けるに際しては、落札価格から20%を控除した額しか補償とならず、補償限度額は、50万円を上限と定められている。

こうした約款では、たとえば偽物を掴まされた者は補償の対象外となる結果、たとえば詐欺業者から何らかの物が送られてきた者は一切の補償を受けることができないわけである。

(4) 提言

被害者救済の場面において、ネット取引参加者をいかに守るのかの点も含めて、運営会社同士に競争させ、その優劣を利用者に判定させるのも一つの考え方だろう（市場モデル）。だが、商品の性能や価格と異なり、約款の優劣は競争には馴染みにくい。したがって、最低限の部分を立法的に手当すべきである（規制モデル）。

この点、すでに、プロバイダ責任制限法はあるが、それはむしろ責任を制限する方向の立法であった。今回は、システム構築者としての最低限の法定責任を負わせる立法が望ましい。責任の内容に応じて、運営会社は、予防策を中心とする最適のシステムを作り出すことができるはずだと考える。まず、

責任を法定し、それを避けるためのシステムを構築させることが望まれる。被害がでても賠償されるシステムよりも、そもそも被害が出ないシステムのほうが優れていることはいうまでもない。

法的な規制の導入に対しては、批判もあるだろう。ある会社は補償制度を導入するにあたって、「現金先払い決済だけの店舗は掲載を認めず、カード決済や代金引換えなどの決済方法を必ず導入してもらおう。会社内部の管理も、店舗チェックを1カ月単位から日々のモニタリングに変えるなど、より一層強化していきたい」という声明を発表している。責任についての法的規制ができれば、当然、その対応が強化されるはずである。これまでのように、各企業の自主的努力に期待し、それでも被害の蔓延が止まらない場合にだけ立法が介入するという戦後型の立法からの脱却が望まれる。「責任あるIT社会」構築のためには、被害者の犠牲の上に成り立つ法制度ではなく、被害者を作らない法制度をめざすべきだからである。具体的には、プロバイダ責任法を改正するなり新たな立法措置を講じるなりして、事業者の法的責任を明確化すべきであることを提言する。

6 電子記録債権と匿名性・可視性・追跡可能性

(1) はじめに

債権取引においては、権利取得・移転・実現の確実性と、権利者の情報保護とのバランスが問題になる。平成19年6月に公布された電子記録債権法(平成20年以内に施行)は、法人の金銭債権について、その取引の安全を確保することによって事業者の資金調達の円滑化を図る観点から、電子債権記録機関が調製する記録原簿への電子記録をその発生、譲渡の要件とする「電子記録債権」という、従来の指名債権でも手形債権でもない、新類型の債権を創設した。これは、内閣府のIT戦略の指針に沿った、世界でも最先端の立法である。この電子記録債権は、指名債権と手形のそれぞれが持つ短所を克服する方向で性格づけがされた。すなわち、手形においては、その「紙」に権利を化体させることからくる発行、管理、交換上の不便さと、印紙税の負担等から実務において近年利用が激減している現状があり、他方で指名債権にはその権利取得の不確実性(二重譲渡や譲渡禁止特約の問題)や権利実現の不確実性(一般に債務者の資力担保がない)があることから、それらの欠点をなくし、簡易かつ確実に債権の移転・回収が図れる制度が望まれたのである。

(2) 電子記録債権の可視性と追跡可能性

電子記録債権は、従来の指名債権や手形よりも可視性をもつ。またいわゆる追跡可能性についても、限定された範囲での機能を有する。

第一に、債務者からみた可視性である。電子記録債権の場合、内容がその記録によって定まるだけでなく、発生・移転のいずれもが、電子債権記録によらなければならない。つまり、発生にも移転にも電子債権記録をすることが効力要件である(ただし消滅については、支払等の電子記録は効力要件ではなく、弁済、相殺等(支払等)がなされると、原則として、支払等記録を待つことなく電子記録債権が消滅する)。そこで、可視性は、電子記録債権の情報開示の問題(どのような者が記録を見ることができるか)にかかるが、少なくとも債務者は、常に電子記録原簿の情報を得ようとすれば得ることができる。したがって、これまでの、裏書によって手形が回り回って思いがけない取得者から突然に請求されるに至った(債務者にとっての取得者の匿名性)という問題は起こらないことになる。さらに言えば、手形と異なり、取得者つまり電子記録債権名義人として記録されうる者はおそらく当該電子債権記録機関と取引を開始する段階で一定の審査を受けることとなり、かつその電子債権記録機関と提携する金融機関での当座預金口座開設の際には、金融機関との関係で一定の信用調査を受けることになる。そしてその名称が電

子債権原簿上に記録されるのである。したがって、たとえば反社会的組織が電子記録債権の名義人となることは、ある程度の困難が伴うと思われる。これらの点は、現在の手形にない可視性かつ安全性といえよう。

他方指名債権の場合は、本来の存在自体は、債権者債務者を明示する形で確実に存する。また移転の場合の可視性は、民法上の通知・承諾で対抗要件を具備する場合は、債務者のところに移転情報が集まる構造の対抗要件（民法 467 条）であるため、債務者にとって思いがけない譲受人からの突然の請求ということは、対抗要件の観点から見れば本来はありえない。しかし、サイレントで（対抗要件を具備せずに）譲渡しておいて、譲受人が譲渡人からの譲渡通知と共に請求してきたという場合は、手形の場合と同様な状況が生じうる。したがって、少なくとも債務者が現在の債権者を捕捉できるという意味の可視性は、電子記録債権の場合には大幅に向上することになる。

一方、電子記録債権においては、多数の債権属性情報が任意的記録事項として記録可能であるため、情報保護の観点から、譲渡履歴までは開示されないのが原則である。ただ、債務者保護との関係では、記録上の債務者が、発生や譲渡の記録における債権者、譲受人や質権者等に対して人的抗弁を有するときは、当該債権者等から電子記録名義人に至るまでの一連の譲渡記録等において譲受人や質権者として記録されている者の氏名・名称や住所の開示が請求できるとされた。その意味で、いわゆる追跡可能性のほうは、限定された範囲で存在するのであって、それほど十分ではない。

第二に、譲受人にとっての可視性である。電子記録債権の場合は、譲受人は記録の確認によって手形と同程度の確実性をもって債権の存在を把握し権利を取得しうるし、さらには手形以上に詳細な債権の属性情報を任意的記載事項によって知りうる利点がある。これは、付帯する取引約定等も含めて移転の対象としたいローン債権の譲渡などに大きな活用の道を開くものである。

第三に、利害関係を持つ者にとっての可視性であるが、電子記録債権を譲り受けようとする者は、自ら電子債権原簿の閲覧はできない仕組みになっており、現在の債権者等（電子記録名義人）から間接的に記録データの提供を受けるなどして情報を得る必要がある。これは、手形と比べるとはるかに多い債権の属性情報が記録できるのであるから、情報保護の観点からみれば当然といえよう（本分科会の 2007 年 10 月シンポジウム『21 世紀電子社会の法的課題—情報流通と情報保護』始関報告参照）。取引社会における情報公開と情報保護の調節点がここに見出されるといってもよい。

（3）電子記録債権の惹起するであろう問題

問題は、このような可視性を持つことがすべて望ましいのかという点にあ

る。わが国の取引社会においては、いまだに残る債権譲渡に対する偏見がある。つまり、債権譲渡は、危機的状況に陥った当事者が、資金繰りや当座の返済のためにその場しのぎに行う取引という側面も過去には強かったため、正常業務の資金調達として確立した今日でも、債権を譲渡するような会社は危ないのではないかという信用不安を惹起する可能性が残っているのである。それを避けるために債権譲渡特例法（平成10年施行、平成16年からは動産債権譲渡特例法）によって創設された債権譲渡登記の場合は、第三債務者に知らせずに登記によって第三者対抗要件を得ることができる制度を作ったという事実もある（ただし同登記の最大の眼目は、個々の債務者への通知または承諾を必要としている民法上の対抗要件を、譲渡情報を大量に磁気データに入れて登記することによって代替し債権の流動化を簡略化にするという点にあった）。もっとも、債権譲渡登記で第三者対抗要件を得た譲受人は、それだけでは債務者に情報が与えられないため、対債務者対抗要件は別途通知をしないと得られないことにされており、情報の秘匿による不利益もある。

また、現在本法の施行準備段階において、電子記録債権の記録手続き等を行ううえでの中小企業のデジタル・ディバイドの問題も議論されている（取引金融機関が記録を代行するという議論もあるが、取引データの漏えいという意味からは適切でないとされる）。

（４）小括

基本的には、債権取引から匿名性を排除し、可視性、追跡可能性を高めるのは正しい方向であり、電子記録債権の導入は推奨すべきものである。ただ、この新制度が大企業の業務の効率化にのみ資することになっては本末転倒であり、本来の目的である中小企業の資金調達の活性化につなげなければならない。

いずれにしても、この電子記録債権が、それによって信頼性・確実性のある債権取引ができるということを社会に広く認識させるためには、記録の改ざんを防ぐシステムや、電子債権記録機関の側で生じたトラブルについての記録機関の責任の明示と並んで、このような可視性の観点を周知せしめることが必要かつ有益であると考えられる。

利用者としての中小企業のITレベル、デジタル・ディバイドの問題も含め、学術会議としては、一方で適切な市民への啓蒙を行い、他方では政府に対し、本来利益を受ける利用者となるべき中小企業等の便益を十分に考慮した制度基盤整備を助言する必要があるだろう。

7 租税におけるアイデンティフィケーションと電子化

(1) 電子申告と本人確認

国税の申告、納付などをインターネットを通じて行う、国税電子申告・納税システム (e-Tax) の運用が 2004 年 2 月より開始されている。この制度は、1993 年 10 月に公表された第三次臨時行政改革推進協議会の最終答申における電子政府構想 (国や地方公共団体の各種業務のオンライン化) とともに準備が開始されたものである。しかし、e-Tax の利用は伸び悩んでいる。その理由として、事前の開始届出と電子証明書の取得があげられている。これらは、いずれも納税者の本人確認に関して必要とされる手続であるが、特に電子証明書の取得に時間、費用、手間がかかることが、e-Tax 普及の障害となっているといわれてきた。

この問題を改善するため、2009 年 1 月 4 日より、開始届出の完全なオンライン化により、納税者の ID、パスワード等が即時発行される制度に改められるとともに、特に負担が大きいとされた電子証明書については、税理士等が納税者の申告等データを作成し、送信する場合に限り、税理士等の電子署名を付与し、税理士等の電子証明書の添付のみで送信ができることとされた。この制度改正により e-Tax がどの程度普及するかは、まだ明らかではない。また、税理士による送信であれば、なぜ本人の電子証明書が不要となるのかについて、必ずしも説得的な論拠は示されていない。こうした動きから浮かび上がるのは、申告・納税を納税者本人が行ったことを確認する手続の重要性、そして、そのコストの大きさである。

(2) 推計課税と取引の特定

では、なぜ e-Tax において、本人性がこれほど問題となるのだろうか。従来の紙ベースの申告においても、他人が勝手に行った申告は当然に無効である。にもかかわらず、申告の本人性に関する問題はほとんど起きなかった。

60 年前のシャープ勧告直後を振り返ろう。当時は、申告納税制度が導入されたばかりであった。申告とは、納税者自らが支払うべき税額を確定する公法上の行為である。したがって、行政処分 (賦課決定処分) という権力性は、原則として排除されている (申告が誤っていた場合にのみ行政処分 (更正処分) が可能であるが、しかしその場合も、通常は納税者の「自主的な」修正申告により処理される)。このことが、税制の民主的と言われたゆえんである。

しかしながら、申告は納税者の取引事実に課税要件規定を適用して算出されるものであるから、納税者が自らの取引事実を記録していることが前提となる。つまり、個別取引を特定できることが前提として存在している。とこ

ろが、このような取引の特定は、特に農家等で根付いておらず、結局、間接事実を用いた推計による税額の算出、すなわち、推計課税が幅広く行われた。

推計課税において、納税者が失うものは大きい。何ら客観的な数値に基づかず、担当者の（主観的）判断により税負担が決まるということ自体が、納税者としての基本的な権利を奪うものであるという評価さえ行われている。戦後の租税行政の歩みは、このような推計課税を減少させ、納税者の記帳に基づく実額課税を普及させることを目標としたものであったといえる。

（3）金融商品課税と人の担税力

納税者の本人性は、電子化前においては、全く問題とならなかったのだろうか。おそらく、すぐに思い付くであろうことは、納税者番号や廃止されたグリーンカードであろう。これらは、特に預貯金や株式取引に関して、取引個々にこれを行った納税者を特定し（いわゆる名寄せ）、マル優といわれる非課税枠の適正な管理や、金融資産性所得に対する総合課税（損失と利益の通算、基礎控除等の所得控除、累進税率の適用など）を実現しようとするものである。当時、グリーンカードに係る所得税法等の改正法案が成立したことから、国税庁は、その実施のため、巨大な電子計算機を導入している。

周知のように、グリーンカードに係る所得税法等の規定は実施をみないまま廃止され、納税者番号はフォーマルな形では導入されていない。プライバシーの問題がその理由とされる。

しかし、歴史を振り返ると、納税者の特定と本人性の確認ができないから、金融商品に対する総合課税が実施されなかったのではなく、逆に、総合課税を政策的に放棄したために、本人性を確認する行政手続が確立しなかったことが理解される。すなわち、1950年代のシャープ勧告の崩壊といわれる状況の中で、有価証券譲渡益が非課税とされ、預貯金利子は源泉徴収のみで課税関係を終了することができることとされた（申告不要）。後者は源泉分離課税と呼ばれるが、後に上場株式の譲渡益に対する課税にも導入されている。源泉分離課税では、納税者の特定が不要であり、また、取引についても、収入金額（譲渡対価または受取利息）さえ把握できれば、原価や必要経費といった控除項目を一切考慮せずに、実施可能である。徴税は、証券会社や金融機関が、源泉徴収義務者、すなわち税務官庁のエージェントとして行う。

他方で、賃金等の給与所得に目を向けると、そこでは、やはり源泉徴収制度が導入されながら、納税者の本人確認が行われ、総合課税が行われてきた事実が存在する。

このように見ると、金融商品への源泉分離課税においても、納税者が失っているものが大きいことに気づく。それは、人的非課税や基礎控除、累進課税

を受け、個人の担税力に応じた税を負担することである。つまり、課税において、一人の人間として扱われることである。

(4) アイデンティフィケーションの実現するもの

納税義務は、納税義務者と課税物件（所得、財産、消費など）を結びつけることによって発生する。これら2つの要素を正確に特定できなければ、公正、公平な課税は実現できない。電子化は、2つの要素を正確に結びつけることを可能とする技術である。

もちろん、電子化は、情報漏洩や改ざん等の情報セキュリティ・リスクを伴う。また、国が個人とその取引を個別把握して結びつけることに対しては、プライバシーの観点からの不快感や反発があることも事実である。国がそのような事実を乱用することがないかも懸念されよう。このような問題は決して過小評価すべきではない。電子化が、個人の匿名性を奪う方向にも作用することには、注意が必要である。

しかし、同時に、電子化によるアイデンティフィケーションが、納税者を一人の個人として尊重する税制を実現しうることに、目を向けるべきである。

8 ネットの匿名性と有害情報規制

(1) 有害情報規制の動き

インターネットの掲示板を通じて殺人や強盗などの共犯者を募ったり、自殺の具体的な方法やその手助けを請け負ったり、仲間内だけで誹謗中傷の書き込みを行って特定個人に対する陰惨なイジメを繰り返したりと、以前は考えられなかったような事件が相次いでいる。インターネットの利便性が高まる中で、ネットの影の部分もまた色濃くなり、現実の社会に深刻な影響を与えている。このような状況下で、ネットを流れる反社会的な情報について一律に何らかの規制をすべきだという意見が次第に強くなっている。

もちろん、ネットの情報であっても、明確に犯罪性を帯びている場合には、その発信者を特定し、逮捕し、処罰することは現状でも可能であり、現に多くのネット犯罪者が検挙され、処罰されている。一般にネットの世界は匿名性が支配すると言われていたが、発信者の技術的な追跡可能性が100%ではないにしても、かなりの程度、発信者を特定することは可能なのである。しかし、今問題になっている情報規制は、警察力を及ぼすことが原則的に困難な犯罪以前の反社会的な情報、あるいは一般に有害な情報の規制である。たとえば、不特定多数の者に対して犯罪を呼びかけることは、一部の特別な法律で処罰されている以外は違法ではない。「どんな仕事でもやります」と(闇の)掲示板に書き込むことも違法ではない。自殺の具体的な方法を不特定多数に対して掲示板で明らかにすることも、現行刑法で取り締まることは難しい。このような犯罪以前の、反社会的情報に対して社会としてどのように対応するかが問題となっているのである。

(2) 匿名制の問題

ネットにおける匿名制を原則的に廃止し、情報発信者が容易に特定されるような制度的な仕組みを導入すべきだという意見がある。たとえば、すべてのインターネット・ユーザーに対して、現実社会の実名とリンクした「ネットID」を付与して、掲示板への書き込みなどに際して、IDの入力を求めるようにすれば、反社会的な情報を有効にコントロールすることができるというのである。確かに、発信者の身元が容易に割れれば、反社会的な情報は激減するだろう。しかし、すでにそのような制度を導入している韓国で、反社会的な情報に関する問題が解消されているかといえば決してそうではない。韓国では、すべての国民に固有の番号を付与し、ネットにおける書き込みなどに際してほとんどのサイトがその番号の入力を要求してきたが、性的な情報や、誹謗中傷、自殺などの不穏な情報に関する問題は相変わらず深刻であ

る。韓国の例を見ていると、個人への追跡可能性を承知のうえで、堂々と反社会的情報を書き込む例が多く、追跡可能性を制度的・技術的に高めても、それが有害情報規制の根本的な解決になりえないのではないかと思われる。有害情報のコントロールよりも、むしろ、情報発信の萎縮効果、プライバシー侵害の可能性、また他人への成りすましの危険性などの方が深刻な問題になっている。

(3) フィルタリングの問題

では、情報の受信の局面で有害情報をコントロールすることはどうか。たとえば、一定内容の情報を遮断する技術的な仕組みである「フィルタリング」には、問題はないのだろうか。

フィルタリングについては、あらかじめ情報内容を評価しておくことが前提となり、それを誰がどのように行うかが重大な問題となる。

以前、政府部内の機関が、青少年へのアクセスが好ましくないと判断した一定内容の情報については、青少年へのその遮断がプロバイダなどに義務づけられるべきであるという意見があった。しかし、このような一括遮断方式には問題がある。一つは、規制対象となる「青少年への有害性」をどのように定義し、判断するかである。凶書の（青少年への）「有害性」が争点になった平成元年の最高裁判決（最判平成1・9・19刑集43巻8号785頁）があるが、判決文では要するに、「害があるから、有害だ」という無内容のレトリックが繰り返されているにすぎない。確かに、都道府県のいわゆる青少年健全育成条例では、一定の基準に基づいて有害図書規制がなされているが、これはあくまでも地域の実情を前提に、表現の自由の保障と「有害性」の判断に苦悩しながらも、少しでも健全な情報環境のためにと、個別に慎重な判断がなされているのである。政府の主導で行う全国一律の情報規制には、情報流通の一括規制という意味で基本的な問題がある。もう一つは、政府主導で行う情報規制に伴う大きな萎縮効果である。個人情報保護法が施行されて、個人情報の有用性を損なう過保護現象が社会問題となっているが、情報規制についても政府が一律に大きな法の網をかぶせることによる過度の反応が懸念される。

(4) 有害サイト対策法の成立

本年6月11日、「青少年が安全に安心してインターネットを利用できる環境整備法」（有害サイト対策法）が成立した。本法は、携帯電話会社やネット接続会社に対し、18歳未満の児童が使う携帯やパソコンにフィルタリングサービスの提供を義務付けているが、罰則がなく、親がフィルタリングを

不要と判断した場合は、フィルタリングは解除される。また、「有害情報」の具体的な定義は避けて、有害情報の基準策定や判定は民間の第三者機関が行うという内容になっている。

フィルタリングの仕組みにおいては、民間の中立的な第三者機関が行った情報の評価を前提に、それぞれのユーザーがその評価を前提に自主的に情報をコントロールできる仕組みが望ましい。その意味で、法律は基本的に妥当な方向を示していると思われる。しかし、フィルタリングの技術開発などを行う民間団体は「総務大臣及び経済産業大臣の登録を受けることができる」とし、国が情報の流れに関与する可能性が完全に排除されたわけではない。

「有害」とは何かが明確に定義できなくとも、子どもを何から守りたいかは親なら直感的にわかる。そのような意味で、有害情報規制に国の関与を避け、それを個別にかつ民間の自主規制にまかせるのが、自由な情報流通を前提にさまざまな制度を構築している日本のやり方として望ましいことだと思われる。

9 プライバシー侵害に対する人々の意識—情報の悪意の取得と関連させて

(1) 調査の概要

「1 はじめに」に述べたような微妙な均衡に立っている現代社会のネットワーク電子技術についての法制度の制度設計を考える際に、人々がこのような現代社会において、プライバシーの侵害をどう考えているかを知ることは重要な一つの前提であると思われる。

我々は、他の目的の調査と同時に行うという形で、人々のこの問題についての捉え方を探るべく質問票による意識調査を行った。概要は以下の通りである。①調査方法：千葉市内の住宅区域4地域に合計1000票の調査票を投函し、返信用封筒で返答を求める、②実査：2008年2月、③有効回答：174票。ランダムサンプルではないこと、回収率が高くはないことから、回答者のバイアスがあることが推測されるが、回答者は都市近郊の人々の意識の一応の傾向を示していると見るのが可能であろう。なお、回答者の年齢分布と性別からは、回答者の高齢者への偏りが見られる。

質問票の内容としては、(a)書店で、定価1000円の本を読み通した、(b)訪問先の机の上に封筒に入れて置いてあった他人の健康診断表を密かにのぞき見た、(c)ラーメン屋で、主人が門外不出にしているスープの作り方のメモを、密かに書き写した、(d)定価1万円のソフトを友達から借りてコピーして使っている、(e)他人の家の庭に黙って入り、家の中をのぞき見た、という5問についてそれぞれどの程度悪い行為かを7点尺度(1-7、①悪くない②悪い行為だが、③に比べれば軽い③スーパーでの100円相当の商品の窃盗に相当④スーパーでの1000円相当の商品の窃盗に相当⑤スーパーでの1万円相当の商品の窃盗に相当⑥スーパーでの10万円相当の商品の窃盗に相当⑦⑥よりも悪い行為)で評定させた。

すなわち、広い意味の情報の適切ではない探索収集行動のうち、プライバシー侵害的なものと、経済的価値のある情報の違法収集的なものを、有体物の窃盗(万引き)との相対比較という尺度で評定させたのである。

(2) 主要な知見

まず第1に、これら5つの行動を全体としていかなる構造で理解しているかを、因子分析を用いて分析した(なお、表、数値などは省略)。結果は、2因子と理解することが適切で、(b)健康診断書覗き、(c)ラーメンスープ、(e)家の覗き、がひとまとまりであり、(a)立ち読みはそれとは別なものとして理解されている。そして、(d)ソフト違法コピーは両方の因子にまたがっている。そこからわかるように、人々は、プライバシーの侵害と経済的利益の侵害を

識別して捉えており、(c)ラーメンスープはその行動形態がパーソナルであるので、プライバシーの侵害と同視されている。

第2に、悪性度の評価については、それぞれの設問の平均値を見ると、(a)立ち読みは悪性度は弱く2.5、他はかなり悪性度が高いという評価である。すなわち、(e)家の覗き5.8、(c)ラーメンスープ5.2と高く、(b)健康診断書覗き4.5、(d)ソフト違法コピー4.4がほぼ同じ数値で並ぶ。これを見ると、侵害された利益、権利の大きさもさることながら、侵害の態様が悪性度の判断にとって重要な要素となっていることが推測される。

第3に、この調査票では、別の目的のために、Q12-2で「一般的に、犯罪者に対して裁判所の下す刑罰はあなたから見ると、厳しいと思いますか、甘いと思いますか」を5点尺度で尋ねている。結果を見ると、(b)健康診断覗き、(e)家の覗きを、窃盗に比べて相対的に悪性度が高いと判断する人が、裁判所の刑罰が軽いに傾いており、他の3問にはそのようなことは見られない。

第4に、上記のような反応が男女、年齢によって差があるかを見ると、高齢者の方が有体物の窃盗に比して、(e)家の覗き、(d)ソフトのコピーの悪性度評価に寛大である。この種の新しいタイプの権利侵害（プライバシーの侵害とか知的財産についての侵害）の評価は若年層の方が敏感なのであろう（古典的な立ち読みについては、有意差はないがむしろ傾向は逆である）。性別については、有意な差は見られなかった。

（3）結語にかえて

上記の調査によれば、プライバシーの侵害に敏感な人が、裁判所の下す刑罰は甘いと答えており、これは、他の犯罪に比べて、プライバシーの侵害について刑事司法が甘いと感じていることの反映であろう。また、若い人の方がプライバシーに敏感であることも、そのことと整合的である。しかし、他面では侵害された権利利益の大きさよりも、侵害の態様が悪性度の判断に大きく影響しているらしいことが示された。

すなわち、人々はますますプライバシーに敏感になると予想されるが、電子技術、ネットワーク技術の進展に伴い、侵害自体が可視性の低いものになってきている。問題は、人々が可視性の低いプライバシー侵害（自分のプライバシーが侵害されているかどうかもわからない）をどのように捉えているかであり（不可視性ゆえ、プライバシー侵害の不安、プライバシーが侵害されたかもしれないという認知は実際以上に大きくなるかもしれない）、プライバシー保護についての、可視性の高い形での法律的技術的制度の確立と、他面では、人々がネットワーク技術について適切なリテラシーを獲得することが重要であろう。

10 おわりに—まとめと若干の提言

以上、本報告は、2から8までで想定される代表的な論点を分析し、9で、そのような電子社会の構成員たる市民が、現在どのような意識でこれらの問題に対応しようとしているのかを考察する手法を、情報取得とプライバシー侵害というテーマに限ってであるが、試験的に検討した。

これらの検討から明らかになったことは、「はじめに」に記した「電子技術、ネットワーク技術の著しい進展とともに、匿名の社会のようで、可視性の高い社会という、微妙な均衡の上に成り立っている」この現代社会を、今後適正に発展させていくためには、さまざまな社会制度の設計の中に、「電子社会における匿名性と可視性・追跡可能性の対立ないしバランス」という観点を積極的に取り入れていかなければならないということである。

具体的には、①匿名性を高めるべき（維持すべき）場面と、②可視性を高めるべき場面、③ことに追跡可能性を高めるべき場面が存在し、また場合によってはそれらが「混在」するのである（たとえば、プライバシー・個人情報保護においては、個人情報の匿名性を維持しつつも、個人の側からの、自己の情報が漏えいしていないことの確認ができるしくみ—ある意味での個人の側からみた可視性の確保—を作る必要性が論じられる）。しかも、勿論のことながら、①と②、③とは、多くの場合に背反する要請となる。

したがって、現代社会の電子化・IT化の制度設計ないし法整備においては、まずは個々の場面でそれらの各要素を十分に分析したうえで、匿名性・可視性・追跡可能性の、量的・質的な最適バランスを図る必要があるといえる。

本報告の結論そして主たる提言は、この点に存する。これまで、IT化の社会制度構築ないし法整備においては、それぞれの主目的に即して、「情報の匿名化による保護」とか、「情報の可視化による流通」など、いずれかの側面にやや単純に比重をかけた議論がされてきたように感じられるものも少なくない。今後は、諸要素のバランスを考慮した、より総合的・多角的な検討が望まれるのである（さらに付言すれば、IT化の制度設計において、いわゆるデジタル・ディバイドの問題はさまざまに議論されてきたが、導入される社会の構成員たる市民のほうの意識格差等の問題がどれだけ検討されてきたかという点も指摘されるべきであろう。IT化に対する市民意識のレベルや、その地域あるいは世代による格差も十分に検討されないと、せつかくの新制度が根付かないことも容易に想定できるからである。）

本報告書がわが国の電子社会の適切な発展に寄与することを願って結びとする。