Web サービス時代の Electronic Commerce における個人情報の取扱

東京大学大学院法学政治学研究科修士課程

公法専攻公共政策専修コースⅠ　鈴木美和

序章

1990 年代に入りインターネットの商用利用禁止が解かれたことに伴い、インターネットは各個人へと普及し[1]、高度情報通信ネットワーク社会の一翼を担うインフラへと成長してきた。そして、このインターネットの飛躍的な普及により、電子的手段による商取引は大きな変革期を迎えることとなった。

プレ･インターネット時代において電子的取引として行われてきた Electronic Data Interchange（EDI・企業間取引）は、受発注データの交換等の企業間取引における業務の合理化・事務手続の簡素化を念頭に置き、信頼関係のある特定企業間で閉鎖的に専用線を利用するものであった。1990 年代以降、インターネットによる開かれたコミュニケーションが可能になると、中小企業や一般市民にも参加の機会が広まり、企業間取引に関する EDI においてインターネットを利用するものが出現したのに加えて、一般消費者を相手とした電子的取引が実現されるようになる。すなわち、インターネットの普及により、これを利用した企業間取引 EDI と一般消費者を相手とする電子的取引の両者を含む、Electronic Commerce（EC・電子商取引）が急速に広まってきたのである。EC の定義については、インターネット技術以外のネットワーク技術を利用するものを含める場合もあるが、本稿では財団法人日本情報処理開発協会 JIPDEC の定義に従って、「商取引（＝経済主体間での財の商業的移転に関わる、受発注者間の物品、サービス、情報、金銭の交換）を、インターネット技術を利用した電子的媒体を通して行うこと」とする[2]。ここで「インターネット技術」とは、TCP/IP スイートを利用したものを指す。

さらに、EC の発展形態として顧客や取引先との協同による統合商取引が注目を集めており、とりわけ ebXML（Electronic Business using eXtensible Markup Language）仕様への期待は大きい。同仕様は、1999 年に設立された業界団体である ebXML Initiative において、電子商取引分野における XML のボキャブラリ、通信方法、取引情報記述法等の世界標準を提供しグローバルな相互接続環境に基づく企業間取引を可能とすることを目指して作成されたものである[3]。また、ebXML1.0 仕様が策定された 2001 年には、ebXML のように

1　財団法人インターネット協会監修の『インターネット白書 2002』によると、2002 年 2 月末時点での日本のインターネット人口は 4,619 万 6 千人に達している。http://www.iajapan.org/iwp/参照。

2　財団法人日本情報処理開発協会 JIPDEC『日米電子商取引の市場規模調査－インターネット技術を用いた電子商取引規模の予測』（1999 年旧通商産業省）　http://www.jipdec.jp/chosa/andersen/tsld003.htm 参照。同協会の定義によると、ネットワーク回線には、公衆回線の他、専用 IP 網、インターネット VPN、衛星通信等が含まれる。また、欧州連合 EU の『eEurope2002』においても、「EC について決められた定義がある訳ではないが、一般的に、商品やサービスを売買するためのオンライン上での取り決めを伴う取引を指す」としている。EU Information Society eCommerce　*What is E-Commerce?* http://europa.eu.int/information_society/topics/ebusiness/ecommerce/1welcome/what_is_ecommerce/index_en.htm 参照。

3　@IT　XML 用語辞典　http://www.atmarkit.co.jp/aig/01xml/ebxml.html 参照。単純化すると、ebXML とは、企業間取引の標準インターフェイスのことであり、e ビジネスに XML を利用すべく取引情報を XML で表現するためのタグ名やスキーマ、XML 文書の交換方法やプロトコル等を定めた仕様のことである。

人間がオペレーターとして直接介在することなく利用できるインターネット上のサービスは、World Wide Web Consortium （W3C）により、Web サービスと定義された。Web サービスとは、大要、他のアプリケーションにデータとサービスを提供するアプリケーションロジックの基本単位であり、XML（eXtensible Markup Language）採用により統合を可能とするアプリケーション・コンポーネントのことである[4]。近い将来、ebXML や Web サービスを利用する EC が普及し、本格的な Web サービス時代が到来する。

EC は、通常の商取引より一層の迅速性・正確性・低コスト性等のメリットを有することから、その将来性に多大なる期待が寄せられている。特に欧州連合 EU やアメリカ合衆国では EC の積極的な推進政策が採られてきた。日本国内においては、高度情報通信社会推進本部の下に 1997 年に設置された電子商取引等検討部会が 1998 年に電子商取引等の推進に関する報告書を取りまとめて以来、2001 年公表の「e-Japan2002 プログラム」でも電子商取引の推進が示される等、積極的政策が進められている。

一方で、インターネットの飛躍的な普及を背景とする EC の推進に伴い、既存の法体系では対応し切れない、あるいはプレ・インターネット時代には問題とならなかった新たな法律問題が発生してきている。個人情報保護もそのひとつである。勿論、個人情報保護は EC や電子ネットワーク特有の問題ではない。しかし、電子ネットワーク上にあっては、非電子媒体によるよりも遥かに容易にプライバシーは侵害され得、その被害は広範に渡る。この危険性が広く認知されるにつれ、EC の主体となることへの懸念が増大しつつある。特に企業ドメインを越え情報が広く移転･伝達されるようになる Web サービス時代にあっては、Web の脆弱性が個人情報に新たな危機をもたらすものとして注目され始めている。

一般的な個人情報保護については、1980 年代から世界的に注目が寄せられてきた。当初は、積極国家現象下において膨大な個人情報を管理する行政機関が第一の侵害主体として想定されていた。しかし、近時の高度情報通信ネットワーク社会の進展に従い、多くの私企業もまた膨大な個人情報を蓄積したデータベースを構築し、プライバシー侵害の主体となり得る立場にある。かかる状況下にあって、我国でも個人情報保護法制の見直しが主張され、民間部門をも規制対象とした個人情報保護法の制定が検討されている[5]。

右法律が制定されるとすれば、EC における個人情報保護にも影響が及ぶことは必至である。そして、個人情報に関する安全性が確保されれば、EC の一層の発展が期待できるであろう。

---

ebXML の標準化作業は、2001 年 5 月より UN/CEFACT（United Nations Centre for Trade Facilitation and Electronic Business）及び OASIS に引き継がれている。

4 MSDN Online『Web サービス』 http://www.microsoft.com/japan/msdn/webservices/default.asp 参照。

5 第 151 回国会から継続審議となっていた個人情報の保護に関する法律案は、第 155 回国会（2002 年 12 月 13 日閉会）において廃案となり、内容を改変した新法案として第 156 回国会に提出される予定である。本稿では、2002 年 12 月現在、未だ新法案の内容が不明確であるため、第 155 回国会までに提出されてきた旧法案を個人情報保護法案として、検討の対象とする。

本稿では、EC における個人情報の取扱について考察し、既存の法制度や成立後の個人情報保護法が及ぼす影響、及び EC の分野を対象とする個別法の要否を検討する。第 1 章では、日本・EU・アメリカ合衆国における EC を含む IT 関連政策の具体的な推進状況及び EC の有用性、EC の現状について概観する。第 2 章では、EC における個人情報保護の必要性を検討する。第 3 章では、日本・EU・アメリカ合衆国での個人情報保護法制への取組みにつき EC との関連に着目しつつ概観し、日本の法制度のあり方を考察する。第 4 章では、第 3 章を前提とした上で、EC において個人情報の取扱が問題となる具体的場面とそれに対する各種法制度や個人情報保護法案による対処方法について考察する。

第 1 章　EC の推進

1991 年にインターネットの商用利用が可能になると、新たな商取引の場面を提供する媒体としてインターネットは瞬く間に注目を集めた。この動きを促進するかの如く、世界各国の政府は EC を含む IT 関連政策の推進を図ってきた。日本も例外ではない。

本章では、第 1 節で EC を含む IT 関連分野の積極的推進政策の概要をアメリカ合衆国・欧州連合 EU・日本に分けて概観した上で、推進が図られる理由である EC の有用性を第 2 節で考察し、実際の EC の発展の程度について EC の現状として第 3 節で触れる。

第 1 節　EC を含む IT 関連政策の具体的推進過程

まず、IT 関連政策の推進過程を具体的に概観する。

（1）アメリカ合衆国[6]

アメリカ合衆国は、1980 年代から大規模なコンピューティング・通信基盤の開発・展開を進め、連邦政府による包括的且つ統合的な情報技術政策研究開発 R&D[7]を立案・推進してきた。そして 1990 年代のクリントン＝ゴア政権において IT 関連政策の推進は本格化した。

1991 年に成立した 5 年間の時限立法である『高性能コンピューティング法（HPC 法；

6　財団法人日本情報処理開発協会 JIPDEC 先端情報技術研究所 AITEC『情報先進国の情報技術政策の動向』（2002 年）　http://www.icot.or.jp/FTS/REPORTS/H13-reports/PDF/H13-report-5.pdf 参照。また、先端 IT 研究・プロダクト情報『アメリカ連邦政府の先端 IT 研究と成果の商用化に関する情報』に全体像がまとめられている。http://www2.gateway.ne.jp/~h_tada/main.html 参照。

7　Research & Development の略

High Performance Computing Act of 1991)』の実行計画として、1992 年『高性能コンピューティング通信計画（HPCC 計画；High Performance Computing & Communications Program)』が開始され[8]、1993 年 2 月には、大統領選挙時の科学技術政策推進の公約に基づきゴア副大統領が『国家情報基盤構想（NII 構想；National Information Infrastructure)』を発表した。この NII 構想では、情報基盤整備の必要性と有効性が示されている。さらに 1993 年には『NII アジェンダ』が発表され、翌年の 1994 年には『GII 構想（Global Information Infrastructure)』がゴア副大統領により発表された。この GII 構想は、各国の NII を連結しグローバルな情報基盤を作るというものである。

1997 年に同副大統領は『グローバルな電子商取引のためのフレームワーク（A framework of Global EC)』を発表した。このフレームワークでは EC 推進のための 5 つの原則と 9 つの課題が示され、9 つの課題のひとつして個人情報の保護が挙げられている。

さらに 1996 年の HPC 法失効後の継承計画として『コンピューティング情報通信計画（CIC R&D 計画；Computing, Information, and Communications R&D Programs)』が開始され、HPCC 計画のような連邦政府主導型の戦略的情報技術研究開発計画の継続実施の必要性が説かれた。これに先駆けて、CIC R&D 計画の一環として 1996 年に『次世代インターネット構想（NGI；Next Generation Internet Initiative)』が発表され、NII 構想の早期実現が目指された。1998 年から NGI は本格的に開始し、『次世代インターネット法（Next Generation Initiative Research Act of 2000)』が成立した。一方で、1997 年から、CIC R&D 計画の一環あるいは別の枠組みで、特定の連邦機関の使命遂行能力を向上させることを目的とした戦略的 IT 研究開発構想・計画も推進されている。

1999 年 1 月には『21 世紀に向けた情報技術構想案（Information Technology for the Twenty-First Century（IT2))』を発表、IT に関する長期的且つ根源的な研究の強化や国家レベルの広域コンピューティング能力の向上及び情報革命における社会的・経済的インパクトを評価する研究の推進が主張された。2000 年 2 月には、HPCC 計画と IT２計画は合併され『情報技術研究開発計画（IT R&D Program)』に改称されることになり、主要な連邦 IT 研究開発計画は全て HPCC/CIC R&D 計画を核として一本化された。IT R&D Program の 2001 年度の重点分野である 11 テーマの中に、情報のセキュリティとプライバシーの管理・保証が挙げられている。

同年政局がブッシュ政権に変わると、それまでの積極的な IT 関連政策は変化し、目新しい IT 関連政策は打ち出されなかった。しかし、2001 年 9 月 11 日の同時多発テロ以降は、サイバースペースにおけるセキュリティ対策が推し進められている。10 月にはブッシュ大統領が『情報化時代における重要インフラ保護』との声明を発表、インフラ保護強化のた

---

[8] HPCC 計画は NII 構想を踏まえた計画であり、航空宇宙局 NASA やエネルギー省 DOE、国立科学財団 NSF、国防高等研究計画局 DARPA 等個々の連邦機関間にまたがる包括的・統合的な計画として策定された。

めの体制整備を行った。また、政府の情報ネットワークのセキュリティ向上を目的としたGOVNETの構築も発表された。

（2）欧州連合 EU[9]

EUにおけるIT関連政策は、1993年欧州委員会発表の『成長・競争力・雇用に関する白書』の中で情報通信インフラの重要性が指摘されたことに端を発する。1994年には、情報化社会において欧州の採るべき政策について提唱した『ヨーロッパとグローバル情報社会（Bungemann Report）』が発表され、以後のEU情報ハイウェイ具体化の指針となった。

1996年、『欧州におけるグローバル情報社会へのアクション・プラン（Europe at the forefront of the Global Information Society:Rolling Action Plan）』が発表され、1997年には改訂が出された。この中で示されたアクションが必要な領域4つの中には、EC導入に必要な環境の改善や、プライバシーに関するグローバルルール設定の必要性も含まれている。また同年には、今後世界的な発展が期待されるECに関して、欧州委員会が『電子商取引に関する欧州イニシアティブ（A European Initiative in Electronic Commerce）』を発表した。

EUレベルでの研究技術開発は、フレームワークプログラムとして実施されている。1998年から始まる第5次フレームワークプログラムにおける情報通信関連プログラムであるIST（User-friendly information society）は、ユーザーに重点を置き、情報の利用促進や教育に着眼するものである。ISTの重点活動分野として「新しい業務方法と電子商取引（New methods of work and electronic commerce）」が挙げられており、仕事における効率性や能率性の向上により、個人の生活の質が上昇するのみならず、競争力が増加することで失業率の低下が実現される、と繰り返されている。また、プライバシーを含む情報ネットワークにおけるセキュリティも重視されている[10]。2001年2月に提出され2002年1月に採択された第6次フレームワークプログラムにおいても、第5次におけるのと同様にISTへの莫大な投資（約36億ユーロ）が計画されており、ISTのプログラムテーマの中にはECやプライバシーを含むセキュリティの研究（同フレームワークプログラムでは、solving“trust and confidence”problem in the area of security, privacy･･･と表現）も含まれている[11]。

2000年には、EUレベルでのIT関連政策としてアクション・プラン『eEurope 2002』が欧州委員会から打ち出された。『eEurope 2002』の目標を実現するための11のアクション・プランの中には、ネットワークの安全性を高めること（e-security）や、環境を整備しECの加速を促進すること（e-commerce）も挙げられている[12]。また同年には、インタ

9 前掲注6参照。

10 IST Overview http://www.cordis.lu/ist/overv-1.htm#structure、http://www.cordis.lu/ist/ka2/welcome.html 参照。

11 IST in FP6 *KA2 Future Activities* http://www.cordis.lu/ist/ka2/future.htm 参照。

12 eEurope Action Plan http://europa.eu.int/information_society/eeurope/action_plan/index_en.htm

ーネットサービスプロバイダーISP の責任制限等、多岐に渡る事項を規定した EU 指令『域外市場における情報社会サービスのある法的側面とりわけ電子商取引に関する指令（Directive on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market）』[13]が出され、さらに欧州としての総合的な研究活動の統一を目標とした欧州研究領域（ERA；European Research Area）イニシアティブが提唱された。『eEurope 2002』を受けて、2002 年 5 月には『eEurope2005』[14]が採択された。この『eEurope 2005』では、セキュリティ（個人情報保護を含む）の確保された情報基盤の実現について繰り返し述べられている。

（3）日本[15]

日本の IT 関連政策の推進は、アメリカ合衆国や欧州連合 EU の状況と比較して決して早いものではなく、1994 年以降になって取組みが本格化する。1994 年 8 月に高度情報通信社会推進本部が設置され、1995 年 2 月 21 日に『高度情報通信社会に向けた基本方針』、1998 年 11 月 9 日に『高度情報通信社会推進に向けた基本方針』が決定され、これらに基づき『アクション・プラン』[16]が策定された。このアクション・プランでは、「短期的且つ優先的に取り組むべき施策と中長期的な課題とを明確にするため、基本方針中に掲げた『4 つの当面の目標（略）』に該当する施策と『その他の課題』にあたる施策とに分類」されており、4 つの当面の目標のひとつとして、「電子商取引推進のための環境整備」が挙げられている。

これと前後して、1997 年 9 月、高度情報通信社会推進本部の下に電子商取引等検討部会が設置され、1998 年 6 月、同部会は『電子商取引等の推進に向けた日本の取組み』[17]を公表した。この中では、民間主体の自由な競争による電子商取引等（本稿定義の EC を含む）推進の必要性を強調しつつ、民間経済主体が躊躇せず電子商取引等を本格的に導入できるよう、政府による環境整備が必要であるとしている。そして環境整備の個別論点のひとつとして、「プライバシー保護」を掲げている。

参照。

13 Directive2000/31/EC of the European Parliament and of the Council of 8 June2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, Official Journal L178, 17/07/2000p.0001-0016
http://europa.eu.int/information_society/topics/ebusiness/ecommerce/8epolicy_elaw/law_ecommerce/legal/documents/2000_386/sec_2000_0386_f_en_acte.pdf 参照。

14 eEurope2005 *An information society for all*
http://europa.eu.int/information_society/eeurope/news_library/documents/eeurope2005/eeurope2005_en.pdf 参照。

15 岡村久道・新保史生共著『電子ネットワークと個人情報保護―オンラインプライバシー法入門―』経済産業調査会 5～7 頁（2002 年）参照。

16 高度情報通信社会推進本部『高度情報通信社会推進に向けた基本方針－アクション・プラン－』（1999 年） http://www.kantei.go.jp/jp/it/actionplan/actionplan.html 参照。

17 高度情報通信社会推進本部電子商取引等検討部会『電子商取引等の推進に向けた日本の取組み』（1997 年） http://www.kantei.go.jp/jp/it/commerce/980622honbun.html 参照。

さらに 2000 年 7 月 7 日には、内閣に情報通信技術（IT）戦略本部を設置することが閣議決定され、同年 9 月 21 日には森内閣総理大臣が『e-Japan』構想を提唱、これを実現する法律として 11 月 29 日に『高度情報通信ネットワーク社会形成基本法』[18]いわゆる IT 基本法が成立した。この IT 基本法は、高度情報通信ネットワーク社会の形成に関する施策を迅速且つ重点的に推進することを目的としており（1 条）、「高度通信情報ネットワーク社会の形成は、電子商取引その他の高度情報通信ネットワークを利用した経済活動（略）の促進（中略）をもたらし、もって経済構造改革の推進及び産業の国際競争力の強化に寄与するものでなければならない」として（4 条）、EC の重要性を主張している。その上で、「高度情報通信ネットワーク社会の形成に関する施策の策定に当たっては、（中略）消費者の保護その他の電子商取引等の促進を図るために必要な措置が講じられなければならない」としており（19 条）、この「必要な措置」には個人情報保護も含まれると解される。

IT 基本法を受けて具体的な政策推進を提示した『e-Japan』戦略[19]が 2001 年 1 月 22 日の第 1 回 IT 戦略本部により公表された。『e-Japan』戦略は、IT 基本法 4 条を受け、重点政策分野として電子商取引を挙げており、「2002 年度までに誰もが安心して電子商取引に参加できる精度基盤と市場ルールを整備し、電子商取引の大幅な普及を促進する」としている。また、重点計画作成を IT 戦略本部の義務とする IT 基本法 35 条に基づき『e-Japan』戦略をさらに具体化するものとして、同年 3 月 29 日には『e-Japan 重点計画』[20]が決定され、個人情報の保護に関する基本法制の整備を含む具体的施策が提示された。同年 6 月 26 日に公表された『e-Japan2002 プログラム』[21]においても、電子商取引等の促進が分野別施策として挙げられる中で、個人情報の保護にも触れられている。また、同年 12 月 13 日には、「電子政府・電子自治体の実現を始めとした公共分野における最先端の IT 化の実現に資する実証実験」として『e！プロジェクト』の実施も表明された[22]。2002 年 5 月には、『e-Japan 重点計画』の改訂として、『e-Japan 重点計画－2002－』[23]が決定され、『e-Japan 重点計画』以来の 1 年間の電子商取引等の発展を踏まえた上で、「企業等における IT 活用の促進」や「消費者保護対策の充実（個人情報保護を含む）」において一層具体的な施策が提示されている。

---

18 IT 戦略本部『高度情報通信ネットワーク社会形成基本法』（2000 年）
http://www.kantei.go.jp/jp/it/kihonhou/honbun.html 参照。なお、IT 基本法は 2001 年 1 月 6 日より施行されている。

19 IT 戦略本部『e-Japan』戦略（2001 年）
http://www.kantei.go.jp/jp/it/network/dai1/0122summary_j.html 参照。

20 IT 戦略本部『e-Japan 重点計画－高度情報通信ネットワーク社会の形成に関する重点計画－』（2001 年） http://www.kantei.go.jp/jp/it/network/dai3/3siryou40.html 参照。

21 IT 戦略本部『e-Japan2002 プログラム～平成 14 年度 IT 重点施策に関する基本方針～』（2001 年）
http://www.kantei.go.jp/jp/it/network/dai5/5siryou2.html 参照。

22 内閣官房・総務省・経済産業省・国土交通省『e！プロジェクト（平成 13 年度補正予算関連）の実施について』（2001 年） http://www.kantei.go.jp/jp/singi/it2/others/e-pro011213.html 参照。

23 IT 戦略本部『e-Japan 重点計画 - 2002（案）』（2002 年）
http://www.kantei.go.jp/jp/singi/it2/dai13/13siryou6.html 参照。

以上のように、インターネット時代到来に伴い、アメリカ合衆国を始めとして、IT 関連政策の重要な一部分を占めるものとして巨額の費用を投じ EC の積極的な推進が図られてきた。EC に特有の有用性が認められるためにかかる政策が採用されてきたと考えられる。それでは、EC の有用性はいかなるものか。次節で考察する。

第 2 節　EC の有用性

プレ・インターネット時代から行われてきた企業間取引 EDI は、互いに信頼関係を有する企業同士の間で、閉鎖的な専用線等のネットワークを使用してルーティーン化した単純な電算処理を電子的に行うことで、主に受発注データの交換等における業務の合理化・事務手続の簡素化を図るものであった[24]。すなわち、特定者間において予め定められた標準に従って取り交わされる継続的な取引を前提としていたのである[25]。この電子データ交換導入により、入力作業の省力化・データ精度の向上・ペーパーレス化が実現され、コスト低減が可能となる[26]。財団法人日本情報処理開発協会 JIPDEC 電子商取引推進センターの 2002 年 5 月発表『国内企業における EDI 実態調査-2002-』においても、電子データ交換によるメリット・期待する効果として、事務処理コスト低減（58.5%）や省力化（56.1%）、重点顧客とのパートナーシップ強化（41.3%）が挙げられている。

1990 年代に入りインターネットの商用利用禁止が解かれインターネット時代が到来すると、開かれたネットワークが実現する。このサイバースペース上では、不特定多数者が低コストで多様な取引を行うことができる。そして、インターネットが一般市民社会へ普及したことで、サイバースペースにおける商取引の主体が、EDI では大企業に限られていたのが、一般消費者や中小企業まで広がった。電子商取引 EC の普及である。

EDI と比較した EC の特徴及び有用性は、以下のようにまとめられる[27]。

24　EDI 推進協議会の定義によると、EDI とは、「異なる企業間で、商取引のためのデータを、通信回線を介して標準的な規約（可能な限り広く合意された各種規約）を用いて、コンピューター（端末を含む）間で交換すること」とされている。http://www.ecom.jp/jedic/what_edi/what.htm 参照。

25　かつては各企業の使用するデータ形式等は標準化されず異なったため取引先毎に異なる端末を使う必要性やデータ形式の変換の必要性があり、この多端末化や変換の必要性は EDI が進展するにつれ一層大きな弊害となる。しかし、EDI は多数の異なる企業でも必要な情報をコンピューターと通信を使って自由に交換ができるところに大きな特徴があり、これを最大限に生かすには標準化が必要、との主張がなされるようになる。財団法人日本情報処理開発協会 JIPDEC 電子商取引推進センター発表『国内企業における EDI 実態調査-2002-』(2002 年) によると、2002 年 5 月時点で、国内標準である CII 標準の採用は 49.3%、国際標準である UN/EDIFACT の採用は 13.0%となっている。
http://www.ecom.or.jp/jedic/activity/jittai2002.pdf 参照。

26　岡村久道・近藤剛史著『インターネットの法律実務』新日本法規出版 310～311 頁（1997 年）参照。

27　高橋和之・松井茂記編『インターネットと法』有斐閣 96～101 頁（1999 年）、*Impact of E-Commerce on the Economy*　The Robert Emmett McDonough School of Business at Georgetown University（1999）　http://www.msb.edu/faculty/culnanm/ec/Briefings/chanwf.htm 参照。

第 1 に、迅速性・正確性・大量性が挙げられる。定型化や標準化により、コンピューターによる大量処理及び迅速且つ正確な情報の取扱が可能となる。正確性・大量性については従来の EDI においても実現されていたことであるが、迅速性についてはインターネット利用による EC の大きな特徴といえる。すなわち、意思表示の受発信が隔地者間であっても殆どリアルタイム性をもって行われることが可能となったのである[28]。また、迅速性は、国境を越えた取引を瞬時に行うことを可能とし、国際化の進展に貢献する性質ともいえる。

第 2 に、不特定多数者による多様な取引が可能となり、取引の主体が大企業から一般消費者や中小企業まで広がった点が挙げられる。従来の EDI では閉鎖的な特定企業間において取引が行われていたのが、開かれた企業間取引 Business-to-Business:BtoB や Business-to-Consumers:BtoC といった大衆向け取引、Consumers-to-Consumers:CtoC といった一般消費者同士の取引までも可能となった。さらに、両者の複合形態として BtoBtoC という新たな形態も登場している。Web サービスプロバイダー（B_p）から提供されたサービスを利用して Web サービスリクエスター（B_r）がエンドユーザーにサービスを提供する構造である（$B_p$toB$_r$toC）[29]。この BtoBtoC の基礎とされているのが Web サービスである。閉鎖的な EDI では取引当事者間に信頼関係が存在したが、開かれた BtoB・BtoC・CtoC・BtoBtoC では当事者間に信頼関係が存しないことも多く、これにより当事者の意思の不一致や準拠法の不一致が頻繁に起こり得るため、紛争が生じ得る可能性も高まった。

第 3 に、取引費用の削減が挙げられる。企業側としてはコンピューターによる受注自動処理を行うことで、人件費や広告費の削減が可能となる。また、中間者の排除により消費者としても安価に購入できる他、交通費や移動の労力をかけることなく取引が可能となる。電子マネー等により決算が行われるとすれば専用端末の設置等の取引環境整備に新たに膨大な費用を要することにもなりかねないが、それでもなお全体として要する費用は現実社会の取引と比較して相当程度低くなると予想される。

第 4 に、インターネット上で情報を開示しておくことにより、C 消費者が商品の性能や価格、特性等や当該 B 企業自身について予め十分な知識を備えて現実社会の取引に臨むことが可能となるため、現実社会における取引も効率化され得ることが挙げられる。

第 5 に、インターネットの開放性により、C 消費者は従来よりも遥かに大量の情報を取得可能となったことで同種製品の性能や価格の比較等が可能となったため、C 消費者が B 企業との現実社会における取引において強い交渉力を有し得ることが挙げられる。

第 6 に、取引データベース生成と活用という特性が挙げられる。コンピューターで制御可能な取引データの集積によってデータベースを構築し、管理情報を収集・加工・分析す

28　この迅速性により、隔地者間ではタイムラグがあることを前提としていた民法 96 条、526 条等の規定が却って不都合性を帯びることとなった。

29　@IT『国内での Web サービスの利用はどれだけ進んでいるか？』
http://www.atmark.co.jp/fxml/tanpatsu/20webus/websvc02.html 参照。国内では KDDI が Web サービスプロバイダーとして代表的である。一方 Web サービスリクエスターの事例は未だ多くない。

ることが可能となるのである。インターネット上でかかる特性を利用したものとして、クッキーCookie がある。クッキーとは、ユーザー情報やアクセス履歴等の情報を Web ブラウザと Web サーバ間でやりとりするための仕組みのことである[30]。クッキーを利用すれば特定の端末からのアクセス状況を確実且つ継続的に捕捉できるため、インターネット上で EC を行うにあたり消費者の個別のニーズに対応したサービスを提供することが可能となる。しかし、クッキーにより情報主体が不知のうちに個人情報が収集され得ることから、個人情報保護との関係で問題視する声が高まっている。詳細については第 4 章第 1 節第 1 項で検討する。

EC の以上のような有用性に着目し、アメリカ合衆国や欧州連合 EU では以前から積極的な EC 推進政策が採られてきており、日本でも近時急速に推進が進められてきたのである。

第 3 節　EC の現状

第 1 節及び第 2 節で検討したように、EC は限りない有用性への可能性を有することから、日本でも積極的に推進政策が採用されてきた。かかる政策の結果として、EC は実際に発展してきたのか。

総務省統計局統計センターの『平成 13 年事業所・企業統計調査概数集計による電子商取引の状況』によると[31]、平成 13 年 10 月 1 日時点における、通信回線を利用した電子データ交換による取引の導入企業数は 169,826 企業となっており、調査対象となった全企業（1,617,250 企業）に占める導入率は 10.5％との結果が出ている。そして、その 8 割がインターネット利用による EC[32]を導入している。同調査では、インターネット以外の通信回線

30　アスキーデジタル用語辞典　http://download.desk.ne.jp/win/3/00031/4063.html 参照。同辞典は、続けて「ページにアクセスすると、Web サーバは Set-Cookie という HTTP 拡張ヘッダに適用するドメイン名、パス、有効期限などの内容を書いて、ブラウザに送信する。ブラウザ側はそのヘッダの内容をローカルの HDD にテキストファイルで保存しておき、次回そのサイトを訪れたときには Web サーバ側に Cookie を送信する。Cookie の内容は CGI や JavaScript から参照できるため、パラメータ(値)に応じてページを書き換えたり、送信するページを切り替えたりといったことが可能である。なお、Web ブラウザ側は、サーバからの Cookie の送信を受け入れないように設定することもできる。」としている。

31　企業産業別にみると、金融・保険業で EC 導入率が最も高く、EC 導入企業の中でもインターネットを利用している割合が最も高いのはサービス業である。また、取引内容別にみると、EDI では受発注各々が 5 割を超えている一方、狭義の EC では、受注が 8 割を超え、次いでアフターサービス他が 3 割弱となっている。総務省統計局統計センター『平成 13 年事業所・企業統計調査概数集計による電子商取引の状況』http://www.stat.go.jp/data/jigyou/2001/kekka.htm 参照。

また、財団法人日本情報処理開発協会 JIPDEC 電子商取引推進センターの前掲注 25 の調査は、EDI 導入に積極的な JEDIC 所属企業を対象としていることから、国内全体の平均状況より進んだ結果を示している。これによると、回答社中 78.2％が EDI を実施しており、利用通信回線ではインターネットが最多で 68.5％となっている。もっとも、他の回線の割合は減少しているものの利用数は減少しておらず、従来型とインターネット型の共存関係が明確になってきていると同調査は指摘する。

32　前述のように、本稿では、このインターネットを利用した電子データ交換による取引を電子商取引 EC と定義する。

利用も含め、全企業に占める企業間取引 EDI 導入率は 8.0%、一般消費者取引（狭義の EC）導入率は 4.0%となっている。

また、経済産業省と電子商取引推進協議会 ECOM 及び株式会社 NTT データ経営研究所の共同調査として 2002 年 3 月に発表された『平成 13 年度電子商取引に関する市場規模・実態調査－2001 年の現状と 2006 年までの展望－』によると[33]、2001 年のインターネット利用企業間取引（BtoB）の市場規模は 34.0 兆円であり、前年の 21.6 兆円から 60%の成長率を示している。また、電子商取引化率は 5.04%を示し、2006 年には 17%を超えると予想されている。これは、BtoB には行政機関向け EC（Business-to-Government:BtoG）も含まれるところ、『e-Japan』戦略の実施に伴い 2003 年、2004 年には中央政府及び地方自治体の電子入札システムが構築され、電子入札・電子調達の急拡大が見込まれるためである。一方、一般消費者を相手とする EC （Business-to-Consumers:BtoC）の 2001 年の市場規模は 1 兆 4,840 億円であり、前年の 8,240 億円から 80%の成長率を示したものの、電子商取引化率は 0.55%に留まる。2006 年の予想も 5.8%程度と見込まれている。

以上の資料からは、インターネットの商用利用開始からの約 10 年間における EC の普及を窺うことが可能である。しかし、他の政策から優先的に且つ巨額の費用を投じて進めてきた過程に見合う程度の成長率とは認め難い。特に BtoC の普及率は未だ微々たるものである。既に見たように EC の有用性は計り知れないにもかかわらず、十分な発展が実現されていないのが現状なのである。

第 2 章　EC における個人情報保護の必要性

第 1 章で検討したように、EC の有用性は計り知れず、各国においても IT 関連政策推進の中で度々EC の発展を大きなテーマとしている。日本でも遅ればせながら EC の重要性が認識され、今や IT 関連政策の一翼を担っているといえる。

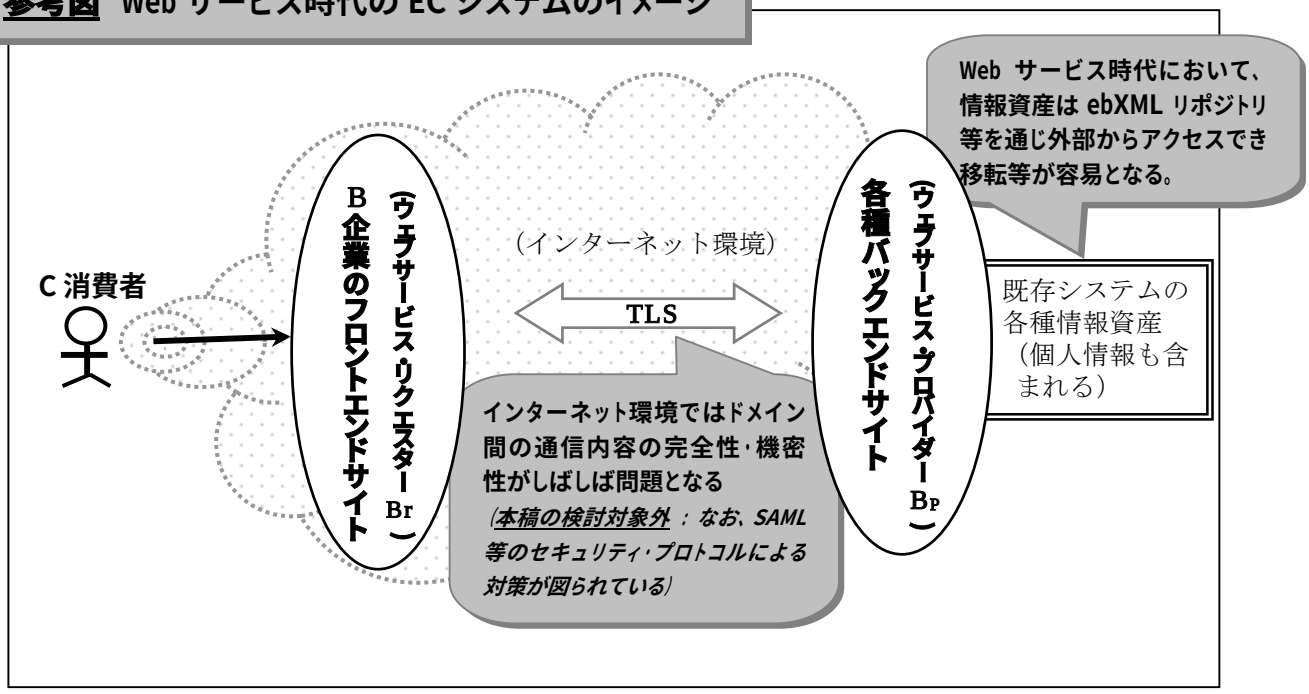
しかし同時に、EC 推進に関連した個人情報保護やプライバシーへの配慮も強調されているが、日本では未だ十分な個人情報保護体制が確立されていない。そして、積極的推進政策が採用されている割には EC が普及しているとは言い難いことの一因は、電子契約への不安感とともに個人情報の取扱に関する危機感にもあるといえる。

EC で情報セキュリティが問題となる場面は、大きく 2 つに分けられる。第 1 の場面は、通信内容の完全性や機密性が問題となる場面である。例えば通信経路においてメッセージが盗み見られたり改竄されたりするような場合が挙げられる。この第 1 の場面に対しては、

33　電子商取引推進協議会（ECOM）『平成 13 年度電子商取引に関する市場規模・実態調査－2001 年の現状と 2006 年までの展望－』（2002 年）　http://www.ecom.jp/home/20020218_2_Press.pdf 参照。

通信の暗号化や電子署名及び電子認証制度により対応することが検討されている。第 2 の場面は、Web の脆弱性が問題となる場面であり、例えば有効な取引の過程で授受された個人情報が提供先で不適切な取扱を受ける場合や、取引に付随して一方当事者による不適切な個人情報の収集がなされた場合が挙げられる。EC における情報セキュリティ問題としては従来から第 1 の場面が注目を浴びてきたが、Web サービス時代の到来に伴い第 2 の場面に対する問題意識が急増している。この第 2 の場面は、個人情報の適切な取扱すなわち個人情報保護の問題となり、BtoC における C 消費者の個人情報及び BtoB において売買の対象となる等で利用される個人情報の保護が特に問題となる。以下、本稿はこの第 2 の場面について検討するものである。

参考図 Web サービス時代の EC システムのイメージ



※ ***Web サイトの脆弱性について → 本稿の主な検討対象***

C 消費者が訪れ個人情報を入力するフロントエンド、及び個人情報を含む営業情報も格納されるバックエンドの双方において、Web サイトの脆弱性にまつわる問題は発生し得る。なお、P3P 仕様対応のフロントエンドサイトでは、C 消費者は自己のプライバシーポリシーにサイトが適合しているかを自動的にチェックできる（34 頁参照）が、Web サイトの脆弱性にまつわる問題に対しては有効性に疑義がある。

個人情報保護の要請は本来 EC に特有の問題ではない。にもかかわらず EC 推進との関係でその必要性が繰り返されるのはなぜか。EC における個人情報に対する脅威は、通常の場合といかなる相違点を有し、なぜ保護の必要性が高いのか。

本章では、一般的な個人情報保護の必要性に触れた上で、EC 特有の、消費者（Consumer:C）を含む情報主体からの要請及び企業（Business:B）からの要請を検討する。

第 1 節　一般的な個人情報保護の必要性

個人情報とは、一般的には個人に関する全ての情報を示す。現行の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、及び個人情報の保護に関する法律案は、「個人情報」を他の情報と容易に照合することができそれにより個人識別可能となるものも含む個人識別情報（以下では総称して個人識別情報とする）と規定しており、一般的な個人情報よりも狭く定義付けている[34]。

個人情報保護法案は、法案中に記述はないものの、プライバシー保護を目的とすると解されている。1999 年 11 月に個人情報保護検討部会から出された『我が国における個人情報保護システムの在り方について（中間報告）』[35]においても、「Ⅰはじめに」の随所でプライバシー保護の視点が示される他、「Ⅱ個人情報保護システムの基本的考え方 1 個人情報保護の目的」の中でプライバシー概念に触れる等、プライバシー保護目的を前提とした記述が見られる。

そもそもプライバシー権は憲法 13 条で保障されると解されるが、その意義については、かつては消極的に「私生活をみだりに公開されないという法的保障ないし権利」と考えられていた[36]。しかし、コンピューターが出現しデータバンク社会が到来すると、憲法 13 条が保障する人格的自律権を実質化するため、より積極的にプライバシー権を捉える必要性が出てくる。そこで現在では、プライバシー権を「自己に関する情報をコントロールする権利」すなわち自己情報コントロール権と意義付けるのが通説となっている。自己情報コ

34　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
第 2 条 2　個人情報　生存する個人に関する情報であつて、当該情報に含まれる氏名、生年月日その他の記述又は個人別に付された番号、記号その他の符号により当該個人を識別できるもの（当該情報のみ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、それにより当該個人を識別できるものを含む。）をいう。
個人情報の保護に関する法律案
http://www.kantei.go.jp/jp/it/privacy/houseika/hourituan/327houan.html 参照。
第 2 条　この法律において「個人情報」とは、生存する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等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。

35　高度情報通信社会推進本部個人情報保護検討部会『我が国における個人情報保護システムの在り方について（中間報告）』（1999 年）　http://www.kantei.go.jp/jp/it/privacy/991119tyukan.html 参照。

36　東京地判昭和 39 年 9 月 28 日判例時報 385 号 12～32 頁『宴のあと事件』参照。

ントロール権は、個人の自律領域[37]を保護することで自律的な社会関係の形成を尊重すべく、自己に関する情報がいかにして収集・保有・利用されているかを自ら把握し、誤りがある場合には訂正や抹消を求めるという、請求権的側面を有する権利である[38]。

かように解すると、自己情報コントロール権を及ぼしめるべき事項か否かは、自律的な社会関係形成を期待できる事項か否かすなわち個人の自律領域に属する事項か否かに関わることになる。

プライバシー侵害は、名誉侵害と異なり真実性の証明[39]によっても侵害の程度は緩和されず、むしろ真実であればあるほど侵害の程度は大きくなるという性質を有する。また、事後的な救済により保護し得るものではなく、一度侵害されると回復困難である[40]。そこで、ある情報が個人の自律領域に属する側面を有し、これを自らコントロールさせないことがプライバシー侵害につながりかねない場合には、広く自己情報コントロール権を及ぼしめるべきである。そして、ある情報が特定の個人を識別するもの又は識別可能なものである場合には、当該情報は個人の自律領域に属する側面を持つことになるため、かかる情報を自己情報として当該個人が自らコントロールすることが憲法 13 条の人格的自律権保障の趣旨に合致する。以上の趣旨から、現行の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、及び個人情報の保護に関する法律案でも個人識別情報を保護対象としていると解される。

もっとも、個人情報保護法案は包括的基本法としての法律案であり個人識別情報該当性という形式的判断のみで自己情報コントロール権を及ぼしめるか否かを常に決するべきではなく、問題となる個人情報の性質や場面を考慮し実質的に自律的な社会関係形成を尊重すべきか否かを検討していくことが人格的自律権の趣旨に合致するのはいうまでもない。

第 2 節　C 消費者を含む情報主体からの個人情報保護の要請

では、EC における個人情報保護につき、いかなる特有の必要性があるのか。まず C 消費者を含む情報主体からの要請を検討する。

そもそもコンピューター利用の特性として、容易性・大量性がある。個人情報が第一次的に収集・蓄積される場面において、情報主体が特定の情報を書き込み又は選択し送信をクリックするのみの作業で済む。そして、その後コンピューターを利用すれば、紙媒体を利用して収集した情報とは異なり、各情報主体から収集した個人情報を集積して直ちにデ

37　私見としては、プライバシーとはこの個人の自律領域のことであると考える。

38　野中俊彦他著『憲法 I（新版）』有斐閣 251～252 頁（1999 年）、Charles Fried : *Privacy*　77 Yale Law Journal 475（1968）参照。

39　刑法第 230 条の 2 参照。

40　長谷部恭男著『憲法学のフロンティア』岩波書店 119 頁（1999 年）参照。

ータベース化することが可能である。このデータベース化により、蓄積された特定の個人情報ファイルを検索することも極めて容易となる。また、収集される個人情報の詳細も多岐に渡ることが可能となる。

しかし、インターネットを利用する EC の特性は以上に留まらない。EC といえども現実社会における特定人に関する契約関係を築くものである以上、EC を利用する際に現実社会における本人を特定し得る個人情報を提供することが必然的に要求される場面がある。一方で、Web サービス時代のインターネットの利用による個人情報の収集・蓄積には、以下のような特性とそれに伴う特有の問題が生じている[41]。

第 1 に、コンピューターの特性である容易性・大量性がインターネットと結び付くことで、蓄積された膨大な個人情報ファイルであってもインターネットを介し直ちに他者へ譲渡し得、第二次的に収集・蓄積され得るという点が挙げられる。ebXML 仕様等によりリポジトリに情報を大量に集積することが容易となったことで、この第二次的な収集・蓄積は現実的な問題となっている。さらにインターネットを利用することで個人情報データベースを他人に譲渡することも飛躍的に容易となる。

第 2 に、広範囲への頒布可能性が挙げられる。これは、蓄積された個人情報をインターネット利用により不特定多数の他人に対して売買等により譲渡することが可能である、ということである。前述のように（第 1 章第 2 節参照）、EDI と比べて EC では不特定多数者が取引相手として想定されており、互いに信頼関係が存在しないことと対応しているといえよう。この広範囲への頒布可能性により、インターネットを利用して個人情報が不当に公表されたり悪用されたりすると、リポジトリが世界中に公開されることのある現状に鑑みて、原理的には世界中の至る所で当該情報を取得可能であるため、被害が極めて甚大となる可能性が高い。

第 3 に、本人の不知が挙げられ、特にクッキー使用につきユーザーが不知である場合が多いことが問題となっている。すなわち、クッキーに関し一般的に認識されているとは言い難いうえ、たとえクッキー使用そのものを認識していてもいかなる個人情報が収集されているのかは認識し難く、その結果ユーザー自らが主体的に個人情報を提供した場合と異なり不知のうちに収集・蓄積されてしまうことが問題視されている。この本人不知の特性は、インターネット利用による収集方法の多様性と結び付く。インターネットを利用することにより、オンラインユーザー登録やユーザー調査等によっても個人情報の収集が可能である他、申込書や注文書中で特定の個人情報を EC により商品を購入する際に要求し、入力又は選択しない限り購入作業に進めず当該 EC やサイトを利用できないシステムにすること等も可能であり、インターネットを利用しない場合と比較して一層多種多様な方法により個人情報を収集し得る。かかる状況では、いついかなる個人情報がいかなる方法によ

41　岡村・新保・前掲注 15・84、416 頁、平野晋著『電子商取引とサイバー法』NTT 出版 232 頁（1999 年）参照。

り収集されているのか本人が知ることが困難な場合も多い。また、一度収集・蓄積されたいかなる個人情報がその後インターネットを介して誰に譲渡されたか、情報の流通につき自ら把握することが、容易性や広範囲への頒布可能性と結びついて極めて困難であることも挙げられる。さらに、本人不知の特性がこの容易性や広範囲への頒布可能性と結びつくと、本人の知らないところにおける収集時の目的以外での利用や漏洩・改竄・悪用等の危険性も一層高まる。

第 4 に、情報相互の結合可能性も、やはり容易性・大量性と結びつくことによって、個人情報への危険性を高めるものとなっている。すなわち、収集・蓄積された各個人情報は断片的なものであっても、互いにインターネット上や現実社会における個人情報と容易に結合されることにより、個人識別可能性が生じ又は一層高まると共に、売買等による譲渡の対象となる価値も生じる。これがさらに広範囲への頒布可能性と結びつけば、膨大な個人情報がインターネット上で飛び交うことによって、個人が特定されることが頻発しかねない。

以上は、インターネット利用による個人情報の収集・蓄積の特殊性から、Web サービス時代のインターネットを利用する EC では実社会におけるよりも一層個人情報保護の必要性が高いことを示すものである。

しかしインターネット利用の特性は必ずしも個人情報保護の必要性を導くのみではない。

そもそもインターネットは不特定多数人に向けて開かれた通信である。すなわち、インターネット上の個人情報は、個人の自律領域に属する側面を有し得るとともに、公然性をも帯びるのである[42]。とすれば、完全に個人の自律領域にのみ属する場合と比べて保護の程度は弱いとも考えられるのである。インターネット上の個人情報を考える際には、かかる点にも留意する必要があろう。

第 3 節　B 企業からの個人情報保護の要請

第 2 節で検討したように、C 消費者等の情報主体からの個人情報保護の要請は極めて高い。しかし、B 企業にとっても、EC 促進に当たり個人情報が保護されていることは望ましく、むしろ積極的に必要ですらあるといえる。既に第 1 章第 3 節で示したように、EC を行う企業数は未だ少数ではあるものの年々増加の一途を辿っている。かかる状況下にあっては、情報主体の不安要因を名実共に除去し、且つ安全性につき中立的な立場から何らかの正当性を与えられることによって、情報主体からの信頼を獲得し企業価値を上昇させて他企業との差別化を図ることが、自らの存続を確実なものとするためである。

42　実社会における個人情報も一定の公然性を有することがあるが、インターネットにおいてはその程度が遥かに大きい。

2002 年 3 月発表の電子商取引推進協議会 ECOM による『EC で取り扱われる個人情報に関する調査報告書（ver.4.0）』[43]では、B 企業がプライバシーマークを取得する際の動機やメリットとして以下が挙げられている。すなわち、プライバシーマークを対外的に表示することで信頼を確保し事業機会の増大を図ることや、企業としての社会的認知度を上げることである。特に顧客データ取扱企業にあっては死活問題であることが窺われる。また、プライバシーポリシーを取得した多くの企業が、社内業務のマネジメント改善を整えるべく社内啓蒙や教育に取り組んでいる点は、個人情報保護に対する企業としての関心の高さを示している。さらに興味深いのは、プライバシーマーク取得後、同マークの取得が企業活動に必須となる制度への展開（例えば入札の条件とする等）を望む企業が多いとの指摘である。ECOM による同調査は、B 企業にとっても取り扱う個人情報保護の要請が高いことを示している。

第 3 章　個人情報保護法制の各国における推進状況

個人情報保護のために各国はいかなる法整備を行ってきたのか。本章では、個人情報保護法制の発端ともいうべき 1980 年の OECD ガイドラインを始めとする経済協力開発機構 OECD の動向を概観した上で、主に EC の分野に関し、欧州連合 EU とアメリカ合衆国の個人情報保護法制の状況をまず検討する。続いて、EU やアメリカ合衆国と比較して遅れをとっている日本の状況について検討する。

第 1 節　経済協力開発機構 OECD の動向[44]

1980 年 9 月 23 日に OECD において採択された『プライバシー保護と個人データの国際流通についての理事会勧告（Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data）』（以下、OECD ガイドライン）[45]は、20 年以上が経過した現在でもなお個人情報保護の指針としての役割を担っている。特にこのガイドラインで示された OECD8 原則、すなわち①個人デ

43　電子商取引推進協議会 ECOM 個人情報保護 WG『EC で取り扱われる個人情報に関する調査報告書（ver.4.0）』（2002 年）参照。

44　堀部政男「電子商取引とプライバシー」ジュリスト 1183 号 77～80 頁参照。

45　Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, O.E.C.D.Doc.C(80)58(Final) http://www.oecd.org/EN/document/0,EN-document-43-1-no-24-10255-43,00.html 参照。

ータはデータ内容の十分な把握の下に適正且つ公正な手段により収集されるべきとする、収集の原則（Collection Limitation Principle）、②個人データは利用目的に沿って使用されなければならず、その範囲で正確・完全・最新性を保つべきとする、データ内容の原則（Data Quality Principle）、③個人データ収集時に遅滞なくデータ収集目的を明確にすべきとする、目的明確化の原則（Purpose Specification Principle）、④個人データは明確化された目的外で原則として利用すべきでないとする、利用制限の原則（Use Limitation Principle）、⑤個人データは滅失・漏洩・毀損・改竄・開示等の危険から安全保護措置により保護されるべきとする、安全保護の原則（Security Safeguards Principle）、⑥個人データに係わる開発・運用・政策については一般的な公開政策が採られるべきであり、且つデータ管理者の識別手段が容易に利用できるようにすべきとする、公開の原則（Openness Principle）、⑦自己に関するデータの保有・内容・異議申立て等が認められるべきとする、個人参加の原則（Individual Participation Principle）、⑧データ管理者は各原則を実施するための措置を講ずる責任を負うべきとする、責任の原則（Accountability Principle）は、各国の国内法整備に当たっても指針としての意義が大きい。

翌 1981 年、欧州評議会は『個人データの自動処理に係る個人の保護に関する条約（Convention for the protection of Individuals with regard to automatic processing of personal data）』[46]（以下、個人データ保護条約）を発布し、同条約は 1985 年に発行された。同条約の内容は OECD ガイドラインに対応しているが、条約としての性質から加盟国への拘束力を有するものである。

1997 年以降、本来的にボーダーレスな性格を有する EC においては国際的ルール整備こそが EC 促進を支えるとの認識のもと、OECD は EC への取組みを本格化する。同年 11 月には「電子商取引の障壁・障害の除去（Dismantling the Barriers to Global Electronic Commerce）」をテーマとする電子商取引に関する国際会議がフィンランドで開催、これを受けて翌 1998 年 10 月には「国境なき世界：グローバルな電子商取引の可能性の実現（A Borderless World:Realising the Potential of Global Electronic World）」との会議（いわゆる OECD 電子商取引に関する閣僚級会議；OECD Ministerial Conference）がカナダのオタワにおいて開催され、『グローバル・ネットワークにおけるプライバシー保護に関する閣僚宣言（Ministerial Declaration on the Protection of Privacy on Global Network）』[47]が採択された。同宣言においては、「個人情報が正当に尊重されつつ収集・取り扱われること」や「プライバシーや個人情報の保護等がグローバル・ネットワークの信頼性を高める重要な要素であること」等の考慮事項が掲げられるとともに、「DECLARE THAT」として、「グローバル・ネットワークにおけるプライバシー保護に関する公約を再確認すること」等が

---

46 Convention for the protection of Individuals with regard to automatic processing of personal data, ETS No.108 http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm 参照。

47 Ministerial Declaration on the Protection of Privacy on Global Network, M.C.E.C. Annex to C(98)177/FINAL http://ottawaoecdconference.com/english/announcements/reg10r2e.pdf 参照。

宣言されている。また同年には、情報・コンピューター・通信政策委員会（ICCP；Committee for Information, Computer and Communications Policy）のもとに設置された情報セキュリティ及びプライバシー作業部会（WPISP；Working Party on Information Security and Privacy）が『オンライン・プライバシー・ポリシー・ステートメント・ジェネレーター（Privacy Policy Statement Generator）』[48]を作成した。これは、EC における C 消費者の信頼向上寄与を目的とした、B 企業や団体によるプライバシー・ポリシー・ステートメント作成支援ツールである。

1999 年 12 月 9 日には、OECD 理事会は『電子商取引消費者保護ガイドライン（Recommendation of the OECD Council Concerning Guidelines for Consumer Protection in the Context of Electronic Commerce）』[49]を採択した。同ガイドラインは、EC における BtoC 取引を対象とし、C 消費者の信頼を築きバランスの取れた B 事業者（企業）と C 消費者の関係の確立に C 消費者保護が不可欠であるとしている。「PART TWO GENERAL PRINCIPLES」中において「Ⅶ. PRIVACY」として、前述の『グローバル・ネットワークにおけるプライバシー保護に関する閣僚宣言』を考慮に入れつつ OECD ガイドラインの 8 原則に沿って BtoC 取引が行われるべきことが示されている。

2002 年 9 月 16 日には、1992 年 11 月の『情報システムのセキュリティのためのガイドラインに関する理事会勧告』に代替する、『情報システム及びネットワークのセキュリティのためのガイドラインに関する理事会勧告－セキュリティ文化の普及に向けて（Guidelines for the Security of Information Systems and Networks -toward a Culture of Security-）』[50]が公表された。ここでは、情報システムへの参加者に関し、「Ⅲ. PRINCIPLES」として、①認識（Awareness）、②責任（Responsibility）、③対応（Response）、④倫理（Ethics）、⑤民主主義（Democracy）、⑥リスクアセスメント（Risk Assessment）、⑦セキュリティの設計及び実装（Security design and implementation）、⑧セキュリティマネジメント（Security management）、⑨再評価（Reassessment）の 9 原則が掲げられている。

第 2 節　欧州連合 EU における状況

一般に欧州諸国はオムニバス方式による個人情報保護法制を採用している。すなわち、公的部門・民間部門を問わず全分野を包括する立法により包括的な保護を図っている。

1985 年に欧州評議会による個人データ保護条約が発効すると、各国において法整備の動

48　Privacy Policy Statement Generator　http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm 参照。

49　Recommendation of the OECD Council Concerning Guidelines for Consumer Protection in the Context of Electronic Commerce　http://www.oecd.org/pdf/M00000000/M00000363.pdf 参照。

50　Guidelines for the Security of Information Systems and Networks -toward a Culture of Security- http://www.oecd.org/doc/M00034000/M00034478.doc 参照。

きが高まる。一方、1992 年の EU 発足に伴い EU 内における個人情報の流通は一層活発になったが、個人データ保護条約に基づく各国の国内法整備には統一性がなかった。そこで、1995 年、各国国内法の統一性ある整備を目指し『個人データ処理に係る個人の保護および当該データの自由な移動に関する 1995 年 10 月 24 日の欧州議会及び理事会の 95/46/EC 指令（Directive95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection individuals with regard to the processing of personal data and on the free movement of such data）』（以下、EU 指令）が採択された[51]。この EU 指令により、EU 加盟国は同指令に準拠する国内法整備が要求されることになった。もっとも、同指令は EU 加盟国以外の国家にとっても重要な意義を有する。すなわち、EU 指令 25 条は、個人データを第三国へ移転する場合につき当該第三国が適切なレベルの個人データ保護（"adequate" level of privacy protection）を確保していることを要求しているのである。これにより、EU 加盟国以外の国家が EU 加盟国から個人情報を取得する際に、当該国家が適切なレベルの個人情報保護措置を講じていないとして取得を禁じられる可能性がある。EC はインターネット利用によりボーダーレスな性質を本来的に有するところ、この 25 条は、EU 加盟国以外の国家及び EU 加盟国にとって、EC 推進を阻害する大きな要因ともなりかねないものである。

第 3 節　アメリカ合衆国における状況[52]

欧州諸国がオムニバス方式による法整備を採用しているのに対し、アメリカ合衆国ではセクトラル方式、すなわち法規制の対象を限定して民間部門については自主規制を原則とし、必要に応じて部門ごとに当該特定領域に適用される個別法を制定する方式が採用されている。

（1）法規制

1974 年、まず公的部門の有する情報について『プライバシー法（Privacy Act）』が制定された。しかし、EC では一般私人間、特に私企業の収集・蓄積する個人情報の取扱が問題となるのであり、同法では対処し得ない。

51　Directive95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection individuals with regard to the processing of personal data and on the free movement of such data, 395L0046, Official Journal L281, 23/11/1995 p.0031-0050 http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett 参照。

52　岡村・新保・前掲注 15・121～138 頁参照。

アメリカ合衆国では、商務省（Department of Commerce）に加えてホワイトハウス及びアメリカ合衆国連邦通商委員会 FTC（Federal Trade Commission）も取り組みを進めてきた。

ホワイトハウスの取り組みとしては、1997 年にクリントン政権が発表した『グローバルな電子商取引のためのフレームワーク』における 9 つの課題のひとつして個人情報の保護が挙げられている点等、前述第 1 章第 1 節第 1 項のとおりである。

独立行政委員会である FTC は、企業自らが宣言した情報慣行に違反した場合には FTC 法 5 条に基づいて必要な執行を行い得、かかる権限に基づき、以前よりインターネット上での消費者の個人情報保護を推進してきた[53]。FTC はかかる推進政策を通じ、1998 年 6 月 4 日『オンラインプライバシーに関する議会への報告書（Online Privacy:A Report to Congress）』[54]を提出、7 月 21 日にはオンラインプライバシー一般に関する包括的立法モデルを提言した。この立法モデルにおいては、「ｉ制定法上の個人情報プライバシー保護基準」中の４つの「公正な情報慣行」として、告知/認知、選択/同意、アクセス/参加、セキュリティ/保全の４つが示されている。また FTC は、インターネットとコンピューターに関しては自主規制が好ましく、かかる自主規制プログラムが有効に働くには、４つの「公正な情報慣行」の遵守と効果的な「執行メカニズム」が不可欠であり、自主規制を補強するものとして立法案を提案している。続いて、前述の報告書を受けて、同年 10 月 21 日には『児童オンラインプライバシー法（Children's Online Privacy Protection Act of 1998）』（以下、COPPA）[55]が制定された。

また、国会でも EC における個人情報の取扱を視野に入れた法案が提出されている。第 107 国会に提出されたものとしては、消費者インターネットプライバシー強化法案（Consumer Internet Privacy Enhancement Act）[56]や消費者オンラインプライバシー及び開示法案（Consumer Online Privacy and Disclosure Act）[57]、グローバルインターネット自由法案（Global Internet Freedom Act）[58]が挙げられる。しかし、民間部門の個人情報について自主規制を原則とするアメリカ合衆国では法制化への反対が強く、未だ成立には至っていない。

53　平野・前掲注 41・237 頁参照。なお、（社）国際商事仲裁協会等が運営する ADR Japan2002 年 4 月のレポート（ADR JapanADR 関連トピックス『FTC（econsumer.gov、電子商取引の消費者保護一般）』http://www.adr.gr.jp/report.html 参照）によると、FTC の見解として、EC についても FTC 法 5 条を始めとする一般的ルールの適用により問題解決を図るのが FTC の立場である、というものを示している。

54　Federal Trade Commission, Online Privacy : A Report to Congress（6/98）

55　Children's Online Privacy Protection Act of 1998, 15 U. S. C. §§6501 - 6505, Pub.L.No.105-277（1998）　http://www.ftc.gov/ogc/coppa1.htm 参照。

56　Bill H.R. 237 - Consumer Internet Privacy Enhancement Act　http://thomas.loc.gov/cgi-bin/query 参照。

57　Bill H.R. 347 - Consumer Online Privacy and Disclosure Act　http://thomas.loc.gov/cgi-bin/query 参照。

58　Bill H.R. 5524 - Global Internet Freedom Act　http://thomas.loc.gov/cgi-bin/query 参照。

（2）自主規制

もっとも、以上のような法規制は存在するものの、セクトラル方式の採用は民間部門における自主規制を原則とする。そこで、アメリカ合衆国においては自主規制が進んでおり、第三者認証制度が活発に行われている。

第三者認証制度は、認証機関が第三者として一定の審査基準に従い申請者の個人情報保護施策を審査し、基準を満たす場合にプライバシーマークの使用を許諾（マーク使用許諾契約を締結）するものであり、いわば第三者による品質保証制度の一種である。かかる第三者認証機関としては TRUSTe[59]（1997 年 10 月より運営開始）や BBBOnLine[60]（1998 年 6 月より運営開始）が代表的である。また、民間の自主規制を推進する団体として、OPA（オンラインプライバシー連合；Online Privacy Alliance）[61]が 1998 年に結成された。この団体は、オンライン上及び EC における個人情報保護を促進する自主規制の推進を目的とする[62]世界的規模の団体であり、TRUSTe や BBBOnLine 等の第三者認証制度も推奨している。OPA 発表の『自主規制の効果的な執行（Effective Enforcement of Self Regulation）』[63]は第三者機関によるマーク制度の指針を示すものであり、この中で OPA は、シンボルやシールの付与により認識しやすいプログラムに参画することがオンライン上の事業者が信頼を獲得する最善の方法であるとし、第三者認証による執行プログラムを支援する、としている。そして、かかるプログラムに要求される事項を掲げる[64]とともに、プライバシーポリシーのシールプログラムへの適合性を定期的に再検査することや消費者からの苦情処理手続のあり方についても触れている。なお、OPA は法規制については反対を表明している。

2002 年 9 月にアメリカ合衆国インフラ保護委員会が発表したパブリックコメント『THE NATIONAL STRATEGY TO SECURE CYBERSPACE』においては、インターネットセキュリティに関する責任を主に個人や事業者に課すものとしている[65]。そして、個人や事業者がサイバースペースにおける自身の役割を果たし得るには、6 つの手段、すなわち、認識及び情報（Awareness and Information）、技術及び手段（Technology and Tools）、訓練及び教育（Training and Education）、役割及びパートナーシップ（Roles and Partnership）、

---

59 TRUSTe http://www.truste.org/参照。

60 BBBOnlineR Privacy Program http://www.bbbonline.org/businesses/privacy/index.html 参照。

61 OPA http://www.privacyalliance.org/、平野・前掲注 41・249～251 頁参照。

62 OPA は *OUR MISSON* の中で“The Online Privacy Alliance will lead and support self-regulatory initiatives that create an environment of trust and that foster the protection of individuals' privacy online and in electronic commerce.”としている。http://www.privacyalliance.org/mission/参照。

63 OPA *EFFECTIVE ENFORCEMENT OF SELF REGULATIO*N http://www.privacyalliance.org/resources/enforcement.shtml 参照。

64 遍在性、包括性、アクセス可能性、経済的に取得可能な価格であること、完全性、深遠性が挙げられている。

65 The President's Critical Infrastructure Protection Board *THE NATIONAL STRATEGY TO SECURE CYBERSPACE* http://www.whitehouse.gov/pcipb/cyberstrategy-draft.html 参照。

連邦の主導（Federal leadership）、協調及び危機管理（Coordination and Crisis Management）が必要としている。

（3）セーフハーバー

以上のように、自主規制の原則と法規制により民間部門における個人情報の保護が図られているが、1995 年に採択された EU 指令 25 条は、アメリカ合衆国の個人情報保護政策に多大な影響を与えた。

同条によりアメリカ合衆国が適切なレベルの個人データ保護（”adequate” level of privacy protection）を確保していないと評価されると、同国と欧州連合 EU との間の個人データ移転が不可能となり EC が阻害され、両者にとって多額の損失となる可能性が高い。そこで、アメリカ合衆国は商務省を中心としてセーフハーバー協定を提案し、2000 年 3 月 14 日、EU との間で合意が成立することになった。セーフバーバー協定とは、EU 加盟国から個人情報を取得するアメリカ合衆国内の企業が自ら同協定への加盟を商務省へ希望しこれが認められた場合に、EU 指令 25 条の適切なレベルの個人データ保護の確保という要件を満たすと看做され、EU 加盟国からの個人情報取得が同条によって阻害されない、とするアメリカ合衆国及び EU 間の協定である。法的規制ではなく、あくまでも民間部門は自主規制が原則、というアメリカ合衆国の姿勢が貫かれている点が特徴的といえよう。

このセーフハーバーでは[66]、加盟は自主判断に任されることが確認され、加盟する場合には 7 つの基本原則を満たし且つプライバシーポリシーを宣言することが要求されている。7 つの基本原則とは、①取得目的等の告知（NOTICE）、②データの第三者移転や目的外利用についての選択（CHOICE）、③データの第三者移転が認められる要件の確保（ONWARD TRANSFER）、④データの取扱におけるセキュリティの確保（SECURITY）、⑤データの完全性や正確性及び目的外利用の禁止（DATA INTEGRITY）、⑥個人による訂正・修正・削除請求というアクセスの保障（ACCESS）、⑦実効性確保のためのメカニズム（ENFORCEMENT）であり、OECD8 原則に大部分で対応した形となっている。

第 4 節　日本における状況

以上のような OECD の動向、欧州連合 EU 及びアメリカ合衆国の法制に対して、日本の法制はいかなるものか。

66　International Safe Harbor Privacy Principles
http://europa.eu.int/comm/internal_market/en/dataprot/news/data4.pdf、
http://www.export.gov/safeharbor/sh_documents.html、
http://www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm 参照。

1980 年の OECD ガイドライン以降、日本では個人情報保護政策として、公的部門のみを対象とするセグメント方式が採用されてきた。セグメント方式とは、公的部門と民間部門を各々別個の法規制により規律する方式で、必要に応じて個別の特定分野を規制する法制定がなされるセクトラル方式とは区別される。セグメント方式の採用は、公的部門については 1988 年制定の『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』により規制、民間部門については各省庁が作成した法的拘束力のないガイドラインに則り各業界の自主規制に委ねる、という形で現れてきた。

（1）自主規制

EC や電子通信事業に関わるガイドラインとしては、旧通商産業省による『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』[67]やサイバービジネス協議会による『サイバービジネスに係る個人情報の保護に関するガイドライン』[68]、電子商取引推進協議会 ECOM による『民間部門における電子商取引に係る個人情報の保護に関するガイドライン』[69]、旧郵政省による『電気通信事業における個人情報保護に関するガイドライン』[70]、日本商工会議所による『電子商取引における個人情報の保護に関するガイドライン』[71]等が挙げられる。

1998 年、通商産業省（当時）はガイドライン遵守のインセンティブを与えるべくプライバシーマーク制度を創設し、続いて日本工業規格『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）』[72]が制定された。この JIS Q 15001 は、財団法人日本情報処理開発協会 JIPDEC によるプライバシーマーク付与の審査基準となっている。また、2001 年より JIPDEC は BBBOnLine と相互認証制度を開始している。プライバシーマーク制度の詳細については本章次節第 4 項で検討する。

2002 年 3 月 29 日には、経済産業省が『電子商取引等に関する準則』を策定した[73]。これ

67　旧通商産業省『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』（1997 年）　http://www.jipdec.jp/security/guideline/privacy-guideline.html 参照。

68　サイバービジネス協議会『サイバービジネスに係る個人情報の保護に関するガイドライン』（1997 年）http://www.ejf.gr.jp/fmmc2/501.html 参照。

69　電子商取引推進協議会 ECOM『民間部門における電子商取引に係る個人情報の保護に関するガイドライン』（1998 年）　http://www.ecom.or.jp/protection/kaisetu.html 参照。

70　旧郵政省『電気通信事業における個人情報保護に関するガイドライン』（1998 年）http://www.soumu.go.jp/joho_tsusin/whatsnew/guideline_privacy_1.html 参照。

71　日本商工会議所『電子商取引における個人情報の保護に関するガイドライン』（2000 年）http://mark.cin.or.jp/guideline.htm 参照。

72　日本工業規格『個人情報保護に関するコンプライアンス・プログラム（JIS Q 15001）』（1999 年）http://privacymark.jp/ref/jisq15001.pdf 参照。

73　経済産業省商務情報政策局情報経済課『電子商取引に関する準則について』（2002 年）http://www.meti.go.jp/topic/data/e202329bj.html 参照。同準則は、同年 7 月 30 日に改訂された。経済産業省商務情報政策局情報経済課「『電子商取引等に関する準則』の改訂について」

は電子商取引等に関する様々な法的問題点につき民法等の関係する法律がいかに適用されるかの解釈を示すものであり、自主規制を支援するものとなろう。準則である以上法的拘束力はなく、また個人情報保護についての直接の規定はない。

また、個人情報保護に直接資するものではないが、IT セキュリティ確保を実現すべく、IT セキュリティ体制を第三者機関が客観的に評価し且つかかる評価が適正な方法であることを認証する制度として、2000 年 7 月に JIS X 5070 が規格化された。JIS X 5070 は ISO/IEC15408 に基づくものであり、これにより国際標準に準拠した信頼性の高いセキュリティ水準の確保が実現可能となる。2002 年 6 月には、経済産業省及び独立行政法人製品評価技術基盤機構が IT セキュリティの国際相互承認スキームである CCRA（Common Criteria Recognition Arrangement）への参加を表明した[74]。さらに、情報セキュリティマネジメントシステム（ISMS）のガイドラインである ISO/IEC17799 が 2001 年 12 月に発行され、日本では JIS X 5080 として規格化された[75]。ISO/IEC17799 は、世界で初めての情報セキュリティマネジメントシステム規格である英国規格 BS7799 をベースとしたものであり、組織内の情報セキュリティの範囲を明確にする際の規範・基準となるものである。これに従い、EC に関与する B 企業においてセキュリティ確保に向けたマネジメントが組織的に行われることで、EC サイトの安全性・信頼性確保にも有効に働くことが期待される[76]。

（2）個人情報保護法案

以上のような自主規制が進む一方で、1995 年に EU 指令が採択されると、EU 加盟国からの個人データ移転につき移転先国に適切なレベルの個人情報保護（”adequate” level of privacy protection）の確保を要求する前述の EU 指令 25 条との関係で日本も民間部門を含めた個人情報保護法制を整備する必要に迫られる。一方で、既に第 1 章第 1 節第 3 項で検討したように IT 関連政策の推進の中で高度情報通信ネットワーク社会の実現には個人情報保護の確保が不可欠であることが再三指摘され、また 1998 年の住民基本台帳法改正とも相俟って、1999 年に個人情報保護検討部会が設置された。同部会は同年 11 月に『我が国における個人情報保護システムの在り方について（中間報告）』（以下、中間報告）[77]を公表し、「Ⅲ個人情報保護システムの在り方 1 基本的考え方」として、官民を通じた基本原則の確立・保護の必要性が高い分野での個別法整備・自主規制等の促進を「組み合わせて最適なシステムとして構築することを基本とすることが適当」であり、「中核となる基本原則等

---

http://www.meti.go.jp/topic/data/e20730aj.html 参照。

74 経済産業省商務情報政策局『IT セキュリティ評価・認証制度に係る国際相互承認への参加について』（2002 年） http://www.meti.go.jp/kohosys/press/0002844/0/020618itsecurity.htm 参照。

75 財団法人日本情報処理開発協会 JIPDEC『情報セキュリティマネジメントシステム適合性評価制度 ISMS 認証基準（Ver.1.0）』 http://www.isms.jipdec.or.jp/doc/JIP-ISMS100-10.pdf 参照。

76 もっとも、ISO/IEC の取得には費用を要するため事実上中小企業は取得が困難である。

77 前掲注 35 参照。

を確立するため、全分野を包括する基本法を制定することが必要」としている。続いて 2000 年 1 月には個人情報保護法制化専門委員会が設置され、同年 10 月『個人情報保護基本法制に関する大綱』（以下、大綱）[78]が決定、大綱に基づき 2001 年 3 月『個人情報の保護に関する法律案』[79]が作成された。この法律案では[80]、個人情報を取り扱う全ての者に対して基本原則遵守を要求[81]した上で、個人情報取扱事業者すなわち個人情報データベース等を事業の用に供している者[82]に対しては義務規定の対象とする[83]、という二段構造を採用している。基本原則は、①当該個人情報の利用目的の明確化及び目的外利用の禁止という、利用目的による制限（4 条）、②個人情報の取得方法についての、適正な取得（5 条）、③個人情報を正確且つ最新の内容に保つべきとする、正確性の確保（6 条）、④個人情報の取扱に当たっての安全性の確保（7 条）、⑤個人情報の取扱に当たって当該本人が適切に関与すべきという、透明性の確保（8 条）であり、OECD8 原則を意識したものとなっている[84]。個人情報取扱事業者の義務規定は、基本原則に則り法的義務を課すものである。具体的には、①に関しては、利用目的の特定（20 条）、利用目的による制限（21 条）及び第三者提供の制限（28 条）、②に関しては適正な取得（22 条）、③に関してはデータ内容の正確性の確保（24 条）、④に関しては、安全管理措置（25 条）、従業者の監督（26 条）及び委託先の監督（27 条）、⑤に関しては、取得に際しての利用目的の通知（23 条）、保有個人データに関する事項の公表等（29 条）、開示（30 条）、訂正等（31 条）及び利用停止等（32 条）がある。これらの各規定は、基本原則が努力規定であるのと異なり法的義務であるため、違反した場合には主務大臣の報告徴収や助言、勧告及び命令の対象となり（36 乃至 39 条）、これに従わない場合には懲役又は罰金による刑罰が課され得るものである（61 条等）。以上の個人情報保護法案は第 155 回国会（2002 年 12 月 13 日閉会）において廃案となったものの、改変を加えた新法案が第 156 回国会に提出され継続して審議される予定である。

78　情報通信技術（IT）戦略本部個人情報保護法制化専門検討委員会『個人情報保護基本法制に関する大綱』（2000 年）　http://www.kantei.go.jp/jp/it/privacy/houseika/taikouan/1011taikou.html 参照。

79　情報通信技術（IT）戦略本部『個人情報の保護に関する法律案』（2001 年）
http://www.kantei.go.jp/jp/it/privacy/houseika/hourituan/327houan.html 参照。

80　個人情報の保護に関する法律案
http://www.kantei.go.jp/jp/it/privacy/houseika/hourituan/327houan.html 参照。
　前掲注 5 で示したように、本稿は旧法案を検討の対象とする。

81　第 3 条　個人情報が個人の人格尊重の下に慎重に取り扱われるべきものであることにかんがみ、個人情報を取り扱う者は、次条から第 8 条までに規定する基本原則にのっとり、個人情報の適正な取り扱いに努めなければならない。
　なお、第 156 回国会提出予定の新法案において、基本原則は基本理念として改変される予定であるが、具体的内容については未だ明らかでない（2002 年 12 月現在）。

82　第 2 条 3　この法律において「個人情報取扱事業者」とは、個人情報データベース等を事業の用に供している者をいう。・・・

83　第 5 章　個人情報取扱事業者の義務等（第 20 乃至 54 条）

84　収集の原則（Collection Limitation Principle）中の可能な限り収集にあたり本人の同意を得るべきとする点や、公開の原則（Openness Principle）を欠く等、必ずしも内容は同一ではない。

（3）個人情報保護法以外の法による規制

包括的基本法たる個人情報保護法が不存在の現行下でも、EC を規制する法は存在する。

まず、EC における消費者保護の法として、特定商取引に関する法律（以下、特定商取引法）[85]及び割賦販売法が挙げられる。インターネット利用により一般消費者が EC に参画する BtoC 又は CtoC は、特定商取引法所定の「通信販売」（2 条 2 項）に該当し、同法の適用を受け、広告に際し一定事項の表示義務が課せられ（11 条）、また誇大広告が禁止される（12 条）。しかし、個人情報保護目的の法でないため、これを直接規制する規定は特に存在しない。また、BtoC においてはクレジットカードによる決済の方式が採られることが多く、割賦販売法の「割賦購入あっせん」（2 条 3 項）として同法の適用を受ける場合がある。すなわち、表示規制や広告規制（30 条 2 項、5 項）、販売条件や支払条件に関する書面交付義務（30 条の 2）等の規制対象となる。もっとも、特定商取引法同様に消費者保護目的法ではあるが個人情報保護は目的とされておらず、個人情報保護規定は定められていない。

2001 年に成立・施行された電子消費者契約及び電子承諾通知に関する民法の特例に関する法律（以下、電子契約法）も EC における消費者保護に資する[86]。C 消費者が操作ミスによって意図しない申し込みをした場合、民法 95 条本文の「要素ニ錯誤アリタルトキ」として無効な意思表示となるが、表意者たる C 消費者に重過失が認められるのが通常であることから、同条但書により無効主張不可とされることが多い。これを EC においても徹底すると、コンピューターを利用する場合には操作ミスが多く、またインターネット等の回線では即座に情報が伝達されてしまうため、C 消費者に酷な結果となる可能性が高い。そこで、電子契約法 3 条は、BtoC において C 消費者が申し込みを行う前に申し込み内容等を確認する措置を B 事業者側が講じない場合には、民法 95 条但書を排除し、要素の錯誤による意思表示は無効とされることとした。電子契約法も個人情報保護を目的とするものでない。

EC における個人情報保護に資する法としては、電気通信事業法や不正アクセス行為の禁止等に関する法律（以下、不正アクセス禁止法）が挙げられる。

インターネットサービスプロバイダーISP は第二種電気通信事業者に該当し、電気通信事業法で規定する検閲の禁止（3 条）や通信の秘密（4 条）の規制を受ける。通信の秘密は、そもそも憲法 21 条 2 項で保障されており、表現の自由の保障及びプライバシー保護の見地から、通信内容のみならず通信の存在自体についても秘密性保持が要求されると解されている[87]。この点につき、インターネットは公然性を有する通信であることから、同様の通信

85　なお特定商取引法は、2000 年改正により、「訪問販売等に関する法律」との名称から改名された。

86　経済産業省商務情報政策局情報経済課『電子契約法について－～電子消費者契約及び電子承諾通知に関する民法の特例に関する法律～の施行にあたって－』
http://www.meti.go.jp/policy/consumer/warehouse/cp_news/61/e-contract.pdf 参照。

87　大阪高判昭和 42 年 12 月 25 日判例タイムズ 218 号 226～228 頁参照。

の秘密が保障される必要はないとの見解もある[88]。しかし、インターネットを利用する場合であっても一概に公然性があるとはいえず、また公然性がある場合でも、いかなる程度の公然性をもって通信の秘密の保障を排除し得るほどの公然性といえるのか不明確であることから、憲法上の保障を排除するには未だ更なる検討が必要と思われる。かかる点は、通信と放送の融合の観点から問題となるところである。

1999 年に制定された不正アクセス禁止法[89]により、アクセス制御機能を有する特定電子計算機に不正にアクセスしサーバ内の情報等を盗み見る行為（3 条）や、ID やパスワード等の他人の識別符号を当該利用者の承諾なく提供する行為（4 条）が禁じられ、罰則が課される（8、9 条）。同法により、個人情報に関するセキュリティ確保が少なからず実現し得る。

第 5 節　日本の法制のあるべき姿

前節で検討したように、日本では従来セグメント方式が採用されてきたが、個人情報保護法案が成立すれば、欧州諸国のようなオムニバス方式に接近するものとなり得、大きな転換となる。そこで、日本の個人情報保護に関する法整備のあり方について、今一度検討してみたい。

（1）全体像

個人情報の取扱が問題となる場面は多種多様に渡る。そこで、業界や分野毎に個別に対応することで、柔軟な対応が可能になるとも思われる。しかし、第 2 章第 1 節で検討したように今日の個人情報保護の必要性は疑う余地がない。業界毎の異なる要請の前提として、各分野を横断する最低限の個人情報保護への要請があるのである。かかる最低限の要請については、業界毎の個別の対応に委ねるのでは個人情報保護の核となる最低ラインが各業界により異なるという結果になり得るため、包括的基本法により統一的に対応すべきである。そして、最低限の法規制を整えた上で個別分野について自主規制により対応するのであれば、最低限の権利保護を確保しつつ各業界の実情に即した柔軟な環境整備が可能となる。この際、個人情報には要保護性の程度が様々なものが含まれており、個別分野や情報の種類によっては自主規制よりも強制力ある法により保護を担保すべきものもあるため、これらについては必要に応じて個別法の制定で対応することも検討すべきであろう。

結局、中間報告で示されたような、包括的な最低限の基本法制定→個別分野・情報の種

88　内山晴康・横山経通編者『インターネット法－ビジネス法務の指針－（第 3 版）』社団法人商事法務研究会 86～87 頁（2001 年）参照。

89　不正アクセスの禁止等に関する法律
http://www.meti.go.jp/policy/netsecurity/fusei_access_law.htm 参照。

類ごとに自主規制又は法規制、という法整備が望ましいと考える。ここで重要なのは、いかなる個人情報をいかなる法形式で保護することが自己情報コントロール権及び人格的自律権の見地から実質的な保護につながるのか、という点である。

（2）個人情報保護法案

では、まず個人情報保護法案は包括的基本法として最低限のものか。

本稿では、EC との関係に注目することに主眼を置いているため、同法律案の詳細については EC と関連する場面について適宜第 4 章で検討することにするが、本原則が OECD8 原則という国際的ガイドラインに大部分において従っている点及び個人情報取扱事業者の義務がかかる基本原則に則っている点からは包括的基本法として最低限といえよう。

もっとも、個人事業取扱事業者の義務規定の適用除外（55 条）にいかなる者を該当させるべきかについては、報道の自由[90]等の憲法上の人権との関係で、別に検討が必要である。

（3）個別法による対応

次に、EC における個人情報は個別法による対応を必要とするか。

1999 年の中間報告では、「Ⅱ個人情報保護システムの基本的考え方 4 個別法等(1)個別法の整備」として、特に機密性が高く漏洩の場合の被害が甚大と予想されるものとして、信用情報や医療情報、電気通信情報が挙げられている[91]。信用情報や医療情報が高度に sensitive な情報であることは容易に首肯し得るが、電気通信情報が挙げられている点は注目される。21 世紀の電気通信として高度情報通信ネットワークが想定されていると思われるところ、IT 関連政策推進の中で高度情報通信ネットワーク社会実現に個人情報保護の確保が不可欠であることが再三指摘されている（既に第 1 章第 1 節第 3 項で検討）ことに対応していると考えられる。

本項では、まず EC を法により規制することの妥当性を検討し、続いて EC における個人情報につき個別法を要するか、検討する。

ⅰ．法規制という手段を採ることの必要性

インターネットを含むサイバースペース上での種々の問題については、技術開発により対応することが最も直接的であり、且つ実効性がある。このことは個人情報保護であっても同様である。しかし、対応策として利用される技術を乗り越える新たな技術が開発され

90　なお、報道の自由は憲法 21 条 1 項で保障されると解されている。

91　前掲注 35 参照。

ればもはやその対応策は意味を持たず、新たな対応策を開発する必要性が出てくる。技術革新のスピードを考慮すると、技術による対応ではいたちごっこにならざるを得ず、結局のところ一時的な対応が可能となるのに過ぎなくなるのである[92]。そこで、何らかの手段によりルールを定める必要性が出てくる。

この点、ローレンス・レッシグ教授は、著書『Code and other laws of cyberspace』[93]において、サイバー空間の法規制の可能性につき次のように主張している。サイバースペースには多数の場所が存在し、その性質はコードのアーキテクチャの内容によって決定される。空間を形成するコードのアーキテクチャは、各々のコード作成者により作成・支配され、サイバースペースの中での活動は全てコードにより左右される。サイバースペースは、本来的に自由な空間ではなくむしろコードによりコントロールされた空間なのである。一方、社会における規制手段たる 4 つの方法、法・社会規範・市場・アーキテクチャは各々相互に依存し合っており、法により他の 3 つの手段を改変することは可能である。そして、サイバースペースのコードのアーキテクチャも、法の強制により良くも悪くも改変可能である。すなわち、政府や政府の連合がコードに対し強制力を行使しコードのアーキテクチャを改変することによって、法によるサイバースペースのコントロールが可能である、と指摘するのである。

かかるレッシグ教授の議論は、サイバースペースを理想的な自由空間と捉えてしまうナイーブな見解に、法以外の手段による規制への視点を与える点で、傾聴に値する。

レッシグ教授の議論から、2 点を導くことが可能である。

第 1 は、サイバースペースの問題について技術対応にのみ期待することの危険性である。サイバースペースをコントロールするコードは民主的過程により決せられたものではなく、コード作成者により一方的に作成されるものであるためである。

第 2 は、技術革新の速さを理由として自主規制や法規制等によるルールを否定する見解の不当性である。確かに今日の技術革新のスピードに鑑みると、技術による対応ではいたちごっことなり十分な対応が期待できないのみならず、現段階の技術を前提としてルールを定立しても新たな技術により容易にこれらのルールを回避し得るように思われる。しかし、コードに最低限要求すべき事項としてのルールであれば、新たな技術が出現した場合にもこれをルールの下に置くことは十分可能である。

以上を前提とし、EC につき政府が介入する法規制という手段を採るべきか、検討する。

EC を含む IT 関連政策においては、民間主導且つ政府は可能な限り不介入とすることが原則とされてきた。前述の電子商取引等検討部会による『電子商取引等の推進に向けた日本の取組み』においても、「Ⅲ．電子商取引等推進に当たっての原則」として、「電子商取引等の発展は民間主導で行われるべきであ」る一方「政府の役割は、このような民間活力

92　林紘一郎・牧野二郎・村井純監修『IT2001 なにが問題か』岩波書店 268 頁（2000 年）参照。

93　Lawrence Lessig : *Code and other laws of cyberspace*　Basic Books（1999）参照。

を引き出す環境の整備が基本」であり、「不必要な規制や制限を課すことを避けるべきであ」るとされている[94]。この方針は『e-Japan 重点計画』[95]及び『e-Japan 重点計画－2002－』でも踏襲されており、後者では「Ⅰ．基本的な方針 3.基本方針（1）官民の役割分担」として「民間が主導的役割を担う」ことが原則とされ、「政府は、自由且つ公正な競争の促進、規制の見直し等の市場が円滑に機能するような環境整備」や「民間の活力が十分に発揮されるための環境整備を行わなければならない」としている[96]。また、アメリカ合衆国における『グローバルな電子商取引のためのフレームワーク』でも、5 原則の中で民間主導及び政府が産業界による自主規制（industry self-regulation）を奨励すべきことが示されている（第 1 章第 1 節第 1 項参照）。

かかる民間主導の原則を徹底すれば、ガイドラインや契約による自主規制こそ、EC に対するルールとして望ましい姿とも考えられる。確かに自主規制によれば各々の業界の実情に即した柔軟性のある環境整備が実現可能である。また、EC の急速な進展にも追いつき得る。しかし、自主規制を築く側である B 企業が自らに好都合な自主規制を作成する誘因は十分に存在し、特に業界を通じるガイドラインの形態を採った場合には、保護されるべき C 消費者等の情報主体は選択の余地を奪われ一方当事者としての立場が不当に弱められるおそれが否定できない。BtoC で考えてみると、例え自主規制が講じられたとしてもそれが一方的に B 企業側から提示されるものである以上、契約システムが事前に一方的に構築されているために C 消費者側が当該システムを甘受して契約を行うのでなければ全く取引できない、という点を克服できないのである。さらに、Web サービス時代の $B_{p}toB_{r}toC$ においては、バックエンドたる $B_{p}toB_{r}$ の ebXML 実装による標準化に伴い、フロントエンドたる $B_{r}toC$ も標準化される傾向にある。これにより、BC 間で予め契約の内容が画一的・一方的に定められ、迅速且つ低コストでの取引が可能となる。しかし、C 消費者が契約の内容について交渉により干渉することができず、一方的な契約内容に納得・妥協して取引を行うか又は取引を全く行わないかという all or nothing になる可能性が高い。原則として私的自治が妥当する分野であるにもかかわらず、交渉の余地が殆どないため私的自治が十分に機能しないおそれが高いのである。そこで契約を支援するものとして最低限のルールを定める必要がある。その際、自主規制のルールを採用すると、自主規制もまた B 企業側から一方的に構築されるものである以上、C 消費者の契約上の地位を確保するという目的が十分に達せられない。そこで、中立的な法による規制の手段を採ることにより、最低限の公益を図りつつ情報主体の権利を保護することが必要といえるのである。EC における個人情報の収集や利用に関しては、第 2 章第 2 節で検討したように本人が不知である場合が極めて多く、自主規制では情報主体の不知を利用し得る点に鑑みても、法規制は望ましいといえよう。

---

94 前掲注 17 参照。
95 前掲注 20 参照。
96 前掲注 23 参照。

そして以上のような法規制は、B 企業にとっても利益となる。なぜなら、当該法遵守の姿勢を示すことにより C 消費者からの信頼を確保し、安定的な経営が一層実現され易くなるためである。

とはいえ民間主導の原則には変わりはなく、政府による環境整備として最低限の法規制に留めるべきである。このことは EC が（BtoG を除き）私的自治の妥当する私人間の契約関係であることにも合致する[97]。

なお EC は、その開放性から、国境を容易に越えるボーダーレスな性質を有するものであり、一国のみでの規制では限界がある[98]。そこで、国際機関や諸外国等との調整による、国際的な整合性のあるルール整備の必要がある点には留意すべきである。『電子商取引等の推進に向けた日本の取組み』[99]や『e-Japan 重点計画』[100]、『e-Japan 重点計画－2002－』[101]等でも、「電子商取引等の促進」の中での施策として「国際的な環境整備」すなわち「電子商取引に関する制度調和を構築し、国際整合性ある IT 社会を形成する」ことが繰り返されている[102]。

ⅱ．EC における個人情報保護の個別法の要否

それでは、法による最低限のルールが必要としても、EC における個人情報保護については個別法を要するか。本章本節第 2 項のように、個人情報保護法案はそもそも最低ラインを確保する包括的基本法であるところ、EC の分野ではこれのみでは不十分なのか。

前述の『Code and other laws of cyberspace』において、レッシグ教授はサイバースペースにおけるプライバシーについて次のように示している[103]。

サイバースペースにおいては、個人が自己情報をコントロールできないアーキテクチャが既に形成されており、現実社会より遥かに効率的なモニタリングが可能となっている。モニタリングされた大量の個人情報をプロファイリングすることで、テレビコマーシャルと比較不能なほどの大衆操作が容易となり、また階級区別による差別化が可能となる。か

97　また、EC の公共財的な特性からも強制介入の余地が導かれる。第 1 章で検討したように、EC には種々の有用性があり、そのため各国の政策としても積極的な推進が図られている。そして EC が安定的に促進されるためには、安全性や信頼性についての予見可能性の確保が必須である。すなわち、EC 推進政策と EC における個人情報保護政策は相反するものではなく、EC 推進を掲げる各国政府としては個人情報保護の確立を同時に実現する必要があり、そのために法という強制介入手段が必要とされるのである。もっとも、この EC の公共財的特性は法による規制の理論的理由とはならず、付随的なものにすぎない。

98　かかる点を捉えてサイバースペースを法で規制することを無意味とする見解もあるが、サイバースペースのボーダーレス性は、法規制の困難さを示すに過ぎず法規制の必要性を否定するものではない。

99　前掲注 17 参照。

100　前掲注 20 参照。

101　前掲注 23 参照。

102　前掲注 20 における 4.(3)5.(ウ)、前掲注 23 における 3.(4)④参照。

103　Lawrence Lessig・前掲注 93・142～163 頁参照。

かる脅威への対応としては、法規制により直接ルールを強制する仕組みとコードにより規制する仕組みが考えられるが、後者が望ましい、とする。コードは確かに一方的にコード作成者が作成するものであるが、当該コードを受け入れるか否かにつき交渉が可能である点に注目するのである。そして、コードの構築にあたり、集団的行動による民主的過程を通じてプライバシー保護に資するコードを実現していくべきである、とする。

以上のようなレッシグ教授の議論に対しては批判の声も強い。電子プライバシー情報センター（EPIC；Electronic Privacy Information Center）の理事であるマーク・ローテンバーグ氏は、Fair Information Practices すなわち公正な情報慣行に着目する。これは、FTC が 1998 年に提言した包括的立法モデル（本章第 3 節第 1 項参照）において自主規制プログラムを有効に機能させるために不可欠とされた、告知/認知、選択/同意、アクセス/参加、セキュリティ/保全の 4 つの「公正な情報慣行」と同義であると思われる。氏は、公正な情報慣行により成文法や行政慣行、コードにプライバシーの規範が組み込まれるとする。こうしてできたコードがさらに法に再編成されることもある。また、法が特定のコードを形成しさらにそれが法へ組み込まれることもあるが、根底にあるのは公正な情報慣行であり、レッシグ教授はこの事実を無視している、と主張するのである[104]。

確かに、氏が指摘するように OECD ガイドラインやアメリカ合衆国プライバシー法の根底には公正な情報慣行の観念があるといえる。そして、サイバースペースにおける個人情報を規制するコードにも公正な情報慣行は組み込まれていることが多いと思われる。なぜなら、公正な情報慣行遵守の姿勢を示すことは、C 消費者からの自社に対する信頼性確保につながるためである。

もっとも、公正な情報慣行がどの程度コードに組み込まれているかはコードによって多種多様であり統一性は必ずしも期待できず、むしろ個人情報保護のために最低限確保すべき要請が確保されていないコードが存在する可能性もある。また、告知/認知と言っても、いかなる程度の告知/認知を示すのかは必ずしも明らかでない。他の 3 要素についても同様である。結局、公正な情報慣行という概念がコードに組み込まれていることが多いと言ってもそのことに過度に期待することはできず、コードに公正な情報慣行が自生的に体現されているとは限らないのである。

私見としては、次のように考える。

EC 個別法の要否については、個人情報保護に関する包括的基本法以上の個別法が EC に対する最低限の法規制といえるかが問題である。個人情報保護法案は現実社会/サイバースペースの区別をせず横断的に各分野を包括する基本法であり、各分野に共通の最低ラインを確保するものである。しかし、第 2 章第 2 節及び第 3 節で示したように、インターネッ

---

104 Mark Rotenberg : *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)* 2001 Stanford Technology Law Review 1（2001）http://stlr.stanford.edu/STLR/Articles/01_STLR_1/参照。

トの特性から EC では個人情報保護の必要性が特に高く、現実社会における一般的な個人情報と比較して法により確保すべき最低限の要請が高い。インターネットの特性に配慮せず、EC においても個人情報保護法案により最低限の要請のみ確保する、とするのでは、人格的自律権を確保するという自己情報コントロール権の趣旨が全うされず、妥当でない。そこで、インターネットの特性及びそこから導かれる個人情報保護の高度の要請を考慮した個別法が必要と解する。

前述のように、レッシグ教授はプライバシー保護に資するコードを民主的に構築しこれにより保護を図ることが望ましいとする。レッシグ教授は Platform for Privacy Preferences（P3P）[105]について触れているが、P3P がプライバシー保護に真に資する技術となり得るのか否かは、P3P コードの実装が始まったばかりである現段階では、必ずしも判然としない。

近時の技術革新のスピードを考慮すると、法により特定の技術を強制することは、実効性に疑義がある。特定の技術の強制ではなく技術中立の立場でコードに最低限要求すべき事項を法が強制するのであれば、技術が目まぐるしく革新を繰り返す中でシステムアーキテクチャが変革した場合にも、最低ラインとしての法の要求が常に確保され、法目的が実現され得る。よって、技術中立の立場でコードへの最低限の要求事項を法が強制する、という形でのルール作成が望ましいといえる。前述のロテンバーグ氏の議論に照らすと、FTC 包括的立法モデルと同様、公正な情報慣行を法に組み込むべきであると考えるのである。

ⅲ．EC において保護すべき個人情報の範囲

では、EC 個別法では、いかなる範囲の個人情報をいかに保護すべきか。

前述のように（第 2 章第 1 節参照）個人情報とは個人に関する全ての情報のことであり、要保護性も多種多様に渡るため、その全てを同列に論じることは妥当でない。そして、当該情報から特定の個人を識別可能である場合に、個人の自律領域侵害の問題が生じ得る。例えば、ある人の趣味や嗜好、収入等が明らかであっても、当該個人が特定不可能であれ

105　P3P は、Web サイトが標準形式においてプライバシープラクティスを表現することを可能にし、ユーザーエージェントがその標準形式データを自動的に取り込んだり容易に処理したりすることを可能にする仕様である。そのために、マシンが理解できる（machine readable）形式である XML 言語を用いてプライバシーポリシーが記述される。この仕様が適切に実装された場合、マシンは、ユーザーの意思決定に基づいたポリシーとアクセスしたサイトのポリシーの整合性を比較しユーザーに報告することができるようになり、自動意思決定も可能となる。これを用いれば、アクセスするあらゆるサイトでプライバシーポリシーを逐一読む、という必要はなくなる。W3C　*The Platform for Privacy Preferences 1.0 (P3P1.0) Specification W3C Recommendation 16 April 2002*　http://www.w3.org/TR/2002/REC-P3P-20020416/ 参照。

また、P3P を評価するものとして、*Developments in the Law : The Law of Cyberspace -Ⅳ.Internet Regulation Through Architectural Modification : The Property Rule Structure of Code Solutions-* Harvard Law Review 112. Issue No.7（student-authored)（1999）http://www.harvardlawreview.org/issues/112/7_1634.htm 参照。

ば、個人の自律領域が侵害されたことにはならない。個人情報保護法案で個人識別情報を保護の対象としていることは既に指摘したとおりである（第 2 章第 1 節参照）。

以上のことは EC でも該当するのか。

第 2 章第 2 節で検討したように、インターネットを利用する EC において個人情報が取り扱われる場合には、現実社会におけるよりも遥かに容易に収集及び他の個人情報との結合をなし得る。収集された個々の情報からは特定の個人を識別することが不可能であっても、新たに他の情報を取得しこれと直ちに結合することで特定の個人を識別することは、現実社会とは比較し得ないほど手間がかからず迅速に行い得るのである。しかも、情報主体たる本人がその過程を把握することは現実社会より一層困難である。さらに、一旦不適切な取扱がなされると、被る被害は甚大となる可能性が高い。すなわち、EC においては、現実社会より遥かに個人識別可能性が生じプライバシーが侵害されるおそれが高いことに加えて、プライバシーが侵害された場合の被害も現実社会より遥かに大きいものとなり得るのである[106]。以上のような EC の特殊性を考慮することなく現実社会における保護と同程度の保護で足りるとすることには、賛同できない。

確かに、個人識別可能性が生じて初めて個人の自律領域に属する事項として法的保護を与えるべき価値が生じる。しかし、上述のように EC において個人識別可能性が生じることが極めて容易である点に鑑みると、個人を識別する徴表ともいうべき個人情報そのものに何らかの保護を予め与えておく、ということも考えられるのではないか。そもそも個別法は、当該分野の特殊性や格別の個人情報保護の必要性を考慮し、当該分野の実情に即した環境整備として制定すべきものであるところ、個別法による保護の対象を包括的基本法たる個人情報保護法案と同様に解する必然性はない。むしろ、EC 個別法では、上述のようなインターネット及び EC の特性に配慮し、あらゆる個人情報について倫理規定又は努力義務として最低限の保護を与えて適切な取扱を促すとともに、個人識別情報については法的保護を与える、という方式も考えられよう。個人情報保護法案が、個人情報を取り扱う全ての者に基本原則遵守の努力義務を課した上で個人情報取扱事業者に法的義務を課す、という主体により区別した二段構造を採用していることは既に述べた（本章第 4 節第 2 項参照）。私見は、包括的基本法によるこの二段構造を前提として、さらに EC において保護の客体により区別した二段構造の採用を提案するものである。かかる提案は、Web サービス時代の EC の特性にも合致する。すなわち、ebXML 仕様等のリポジトリに集積された個人情報の検索容易性は一層高まり個人情報相互の照合も極めて容易となったため、単独では個人識別可能性のない個人情報の取扱にも予め努力義務を課すことが、EC における個人情報保護の最低ラインを確保する上で望ましいといえるのである。ここで、個人情報にも努力義務のみならず法的義務まで課すべきとも思われる。しかし、EC では匿名性を完全に確保して取引し得る場合もあり、また企業活動の円滑性・迅速性を不当に制限すれば EC 促進は著し

106　侵害行為は、現時点においては熟練したハッカー等によりなされると考えられる。

く阻害されかねないことから、個人情報に対しては努力義務に留めるべきであろう。

以上のような私見は、インターネットを利用する EC が不特定多数人を取引主体として想定し、公然性を帯び得る点への配慮に欠けるようにも思われる。確かにインターネットを利用することが公然性につながる場合もある。例えば、インターネット上での掲示板やチャット、動画や音声の配信コンテンツ等は公然性を有するものとして典型的といえる。しかし一方で、インターネット上には電子メールのように電話やファックスによる通信に類似した性質を有するものもある[107]。すなわち、当該情報の提供・利用される状況から、公然性を帯びた情報か否かが決せられるのである。EC について考えてみると、確かに不特定多数人を取引主体として想定してはいるが、C 消費者を含む EC における情報主体が自らの個人情報を提供又は提供や利用に同意する際、当該情報が公然と利用されることに許容しているとは客観的にも当然認められない場合が殆どであろう。とすれば、公然性を帯びた情報とはいえないはずなのである。

（4）自主規制

さらに、自主規制のあり方も再度検討する必要がある。EC を視野に入れた法制度が未だ整備されていない状況にあっては、自主規制による対応を完備する必要がある。また、本来的にボーダーレスな性格を有する EC においては国内法適用にも限界があり、自主規制に委ねざるを得ない領域も存在し得る。

自主規制を促進する第三者認証制度も、法整備のなされていない状況では特に実効性が期待される。なぜなら、業界を通じるガイドラインの形態を採った場合に中立性を欠くおそれがあることは既に指摘したが（本章本節第 3 項参照）、業界を限定しない第三者認証制度によれば一定の中立性を確保することも可能となるためである。国内法適用に限界がある点は自主規制の必要と同様である。

前節で触れたように、日本でも各種ガイドラインの他、第三者認証制度として 1998 年から財団法人日本情報処理開発協会 JIPDEC によりプライバシーマーク制度が採用されている。1999 年より、JIPDEC は日本工業規格『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）』をプライバシーマーク付与の審査基準としてきた。JIS Q 15001 は、民間事業者が策定すべき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を取りまとめた規格である。すなわち、民間事業者の個人情報保護に関する社内管理体制の基本モデルを提示し第三者認証制度の準拠となることを想定して規格化されたもの、と指摘される[108]。

107　電子メールの秘匿性を確保するものである S/MIME を利用すれば、電子メールは一層ファックスに擬せられることが可能となろう。S/MIME については、@IT 『S/MIME でセキュアな電子メール環境をつくる！』 http://www.atmarkit.co.jp/fsecurity/special/04smime/smime01.html 参照。

108　岡村久道編著『インターネット訴訟 2000』ソフトバンクパブリッシング 215～216 頁（2000 年）参

プライバシーマーク制度は、言うまでもなくオンラインビジネスのみならず自動処理の個人情報を取り扱うあらゆる事業者を対象とするものであるが、EC においては C 消費者が適切な個人情報保護体制を整備している B 企業を選別する際の判断基準となり得、また B 企業としては自己の個人情報保護管理体制について客観的に正当性を付与してもらい且つそれを対外的に表明できることになり、EC の分野でも有用性が期待される。そして、同制度はプライバシーマークを付与された認定事業者に法的義務を課すものではないが、実効性を担保するため、付与機関（JIPDEC）及び指定機関（JIPDEC が指定したプライバシーマーク審査機関）による実態調査や改善勧告や指導、ひいては認定取消やマーク使用契約の解除の手段が講じられる[109]。プライバシーマークの有効期間は 2 年間であり、更新を希望する認定事業者は 2 年毎に更新申請をし、そのたびに最新の審査基準が課せられることになる。

2001 年 6 月より、JIPDEC は BBBOnLine と提携し、『JIPDEC・BBBOnLine プライバシー相互認証プログラム』が開始された[110]。既にプライバシーマークを付与された認定事業者は、相互承認プログラムに参加することで BBBOnLine のプライバシーシールプログラムの認証を受けたと看做されることになり、自社の英語版 Web サイト上で BBBOnLine のマークを使用することが可能となる[111]。かかる相互認証制度は、ボーダーレスな性格を有する EC において個人情報を保護するシステムとして、実効性が期待される。

なお、第三者認証制度のあり方については、国際的な調和を図る観点からも、前述の（本章第 3 節第 2 項参照）OPA による『自主規制の効果的な執行（Effective Enforcement of Self Regulation）』が指針として参考になろう[112]。

第 4 章　EC において個人情報の取扱が問題となる具体的場面

前章において、個人情報保護法制の推進状況について概括的に検討した。本章では、EC で具体的に個人情報の取扱が問題となる場面ごとに、個人情報保護法案及び現行の法制度下における個別の対処法を検討してみる。

照。

109　財団法人日本情報処理開発協会 JIPDEC プライバシーマーク事務局『プライバシーマークの申請受付について』（2002 年）　http://privacymark.jp/appl/new.html 参照。

110　財団法人日本情報処理開発協会 JIPDEC プライバシーマーク事務局『JIPDEC・BBBOnLine プライバシー相互認証プログラム　相互承認マークの付与申請受付について』（2001 年）
http://privacymark.jp/appl/rbbbol.pdf 参照。

111　BBBOnLine プライバシーシールプログラムはオンライン上の活動のみを対象としているため、紙媒体活動に対して利用することはできない。

112　前掲注 63 参照。

まず、契約前の段階では、商品の宣伝広告や C 消費者の勧誘において個人情報の不適切な取扱がしばしば問題視される。いわゆるクッキー利用によるバナー広告やスパムメールがこれに当たり、一般消費者を対象とする BtoC で通常問題となる。第 1 節で検討する。

契約締結及び契約履行の段階では、個人情報の収集に関する適正な説明と同意 Informed Consent や児童による承諾の有効性が問題となる。この点については第 2 節で検討する。なお、通信内容の完全性や機密性が問題となる場面に対する暗号化や電子署名及び電子認証の問題や、決済方法の安全性を図るための電子マネーの問題[113]も近時注目されているが、第 2 章で示したように本稿は Web の脆弱性から生じる問題に焦点を当てているため、本稿では触れないこととする。

契約終了後の段階では、収集済み個人情報の取扱が問題となる。特に、情報が第三者提供される場合や、B 企業間での営業譲渡や合併により各々の企業が有する個人情報が組み合わされる場合が挙げられる。第 3 節で検討する。

最後に第 4 節において、個人情報の取扱が適切に行われなかった場合の対応として、当事者及びサイバーモール運営者の責任を検討する。

第 1 節　契約前の段階

EC に参加する意思を有していても、そもそもいかなるサイトが提示されており、そのどれが自分のニーズや嗜好に合致したものか判別することは、一般消費者には通常困難である。そこでは、クッキーにより自動的に収集された個人情報に基づき Web サイト上に掲載されるバナー広告や、商用の電子ダイレクトメールであるスパムメールが利用されることが多い。しかし、クッキーやバナー広告、スパムメールには、それぞれ個人情報保護との関係で問題点が大きい。

（1）クッキー[114]

ｉ．問題の所在

クッキーとは、Web サーバが消費者の端末のハードドライブに植え込んだテキストファイルのことである。クッキーを発行する Web サイトを閲覧する際、利用した端末に自動的

113　EC においてはクレジットカードによる決済が通常であるが、オンライン上にクレジットカード番号を書き込むことには多大な危険性が伴い、このことが EC 促進を阻害する一因ともなっている。そこで、電子マネーの構築によりかかる危険を排除することが注目されている。

114　岡村・新保・前掲注 15・414～431 頁、Richard S.Taffet; Gabriel M.Nugent : *Privacy Protection at Internet Activities*　国際法務戦略 Vol-Ⅹ.10　37～43 頁参照。

に保存されるもので、ユーザーが記入したユーザー名やパスワード等の他、当該サイトを閲覧した日時や頻度、閲覧者に固有の番号を記録することができる。クッキーを発行するサイトの閲覧時に何らかの個人情報を入力すると、再閲覧時に端末が個別的に識別され当該端末からのアクセス状況を確実且つ継続的に捕捉できることから、ユーザーの趣味や嗜好が相当程度把握可能となり、これを利用して個々人の趣味・嗜好に合わせたサービス提供（バナー広告の提示等）が可能となる。ユーザーの側としても、同一のサイトを閲覧した際に既に記入した内容を再記入する必要がなくなったり、自らの趣味・嗜好に合うサービスの提供を受け得るようになったりするというメリットがある。そして、クッキーの設定を変更して、再閲覧時に特定可能とするか否かを利用者側で決定することが可能である。

しかし、そもそもクッキーについての端末ユーザーの認識が未だ薄いため本人不知の状態で個人情報が収集されたり、自らクッキー拒否の設定をし得るとはいえ、初期設定では受入設定となっており拒否すると利用できないサイトも多数存在し、クッキーを受け入れざるを得ない状況が存在したりすることから、問題視する声も高い。確かにクッキーで収集される個別の情報は単なる統計的な閲覧事実に過ぎない場合が多い。しかし、再閲覧時に新たに別の個人情報を入力すれば、既にクッキーに保存されている他の個人情報と結合又は現実社会における個人情報と結合されることで、特定の個人が識別可能となり得る。しかも、結合により作成された個人情報データベースは、極めて多岐に渡り詳細なものとなる可能性が高い。かかる点がクッキーに起因する問題点である。

ⅱ．法規制

日本でのクッキーに関する議論は、近時になり問題視する声が高まってきたに過ぎず、直接規制する法は存在しない。しかし、個人情報保護法案が成立すれば、一定程度での規制が実現され得る。

すなわち、同法案では個人情報取扱事業者の個人情報の取得につき、23 条で本人への利用目的の通知・公表を要求している。詳細は本章次節第 1 項で検討するが、当該規定により情報主体は個人情報が取得された場合の利用目的については認知し得ることになる。

しかし、同法案では取得にあたっての情報主体の同意は要求されていないため、一方的な取得行為も可能となる。

また、2 条 1 項所定の「個人情報」（すなわち個人識別情報）に該当しない限り同法案は適用されないところ、クッキーで収集される情報は、それ自体は統計的な閲覧事実に過ぎない場合が多く、単独では個人識別情報該当性が否定される可能性も高いが、前述のように他の個人情報と結合することで特定の個人が識別可能となり得る。そこで、同条項の「(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む)」という部分の該当性が積極的に判断されるのでなければ、同法案での

対処は困難となる。

不正アクセス禁止法での対処も考えられる。同法 3 条は、電子計算機のアクセス制御機能による特定利用の制限を一定の行為により免れ、制限された特定利用をし得る状態にさせる行為を禁止しているところ、本人がクッキー拒否設定をしているにもかかわらずこれを免れクッキーを利用するとすれば同条に該当し得るが、単なるクッキー利用の事実のみでは「制限されている特定利用」といえず同条で対処し得ない。

アメリカ合衆国では、電気通信プライバシー法や通信傍受法、コンピューター使用詐欺及び濫用法違反が主張されるケースも生じている。

ⅲ．裁判例

アメリカ合衆国のリーディングケースとして、2001 年 3 月に出されたダブルクリック社事件判決がある[115]。

ダブルクリック社はオンライン上で広告を配信する広告配信会社である。同社は、提携する Web サイトを閲覧したユーザーのハードディスクにクッキーを記憶させ、これに基づき Web サイト上にバナー広告を掲載していた。クラスアクションとして提起された訴訟において、電気通信プライバシー法（ECPA ; Electronic Communications Privacy Act）[116]第 2 章、通信傍受法（Federal Wiretap Act）[117]18 U.S.C. § 2511(a)、コンピューター使用詐欺及び濫用法（Computer Fraud and Abuse Act）[118]18 U.S.C. § 1030(2)(c)に該当しないかが争われた。まず ECPA 第 2 章違反の点については、Web サイトは同 2 章の「users」に該当するところ、クッキー設定につき各 Web サイトが許可を与えていることから、同 2 章の適用除外に該当するとされた。次に通信傍受法 18 U.S.C. § 2511(a)違反の点についても、各 Web サイトが傍受に同意している以上、違法でないとされた。コンピューター使用詐欺及び濫用法 18 U.S.C. § 1030(2)(c)違反の点については、原告が損害を立証していないこと、及びブラウザをクッキー拒否に設定又は同社の Web サイトから容易且つ低廉にオプトアウトクッキーをダウンロードし得る[119]ことから、却下された。もっとも当該判決は、クッキー等を利用したオンライン上での個人情報の収集は立法問題としても検討され始めている点、及び相次ぐ法案提出について付言している。

ダブルクリック社については、合併に伴う個人情報の結合に関して FTC の調査及びその後の和解という経過があるが、この点については本章第 3 節第 2 項で検討する。

---

115 *In re DoubleClick Inc. Privacy Litigation*, 00 Civ. 0641, 154 F. Supp.2d 497 (S.D.N.Y., March 28, 2001) http://www.nysd.uscourts.gov/courtweb/pdf/D02NYSC/01-03797.PDF 参照。

116 Electronic Communications Privacy Act, 18 U.S.C. § 2701, et. Seq.

117 Federal Wiretap Act, 18 U.S.C. § 2710, et. Seq.

118 Computer Fraud and Abuse Act, 18 U.S.C. § 1030, et. Seq.

119 DoubleClick Inc. *Cookies* http://www.doubleclick.com/us/corporate/privacy/privacy/cookies.asp?asp_object_1=&参照。

ⅳ．小括

クッキーの利用は、B 企業のみならず C 消費者にとってもフォームへの再度の記入の手間を省き得る面や種々のサービス提供を受け得る面でメリットがあるため､C 消費者に事実上広く受け入れられている。

しかし、いついかなる記録が記憶されるのかについて不知、又は少なくとも十分な把握が困難な状態でデータベース上に自己像が形成されていくことは、自律的な社会関係形成の尊重という自己情報コントロール権の趣旨に反するものである。にもかかわらず、個人情報の収集にあたり情報主体の同意を要求していない個人情報保護法案では、情報主体による十分な関与は期待できない。各種ガイドラインにおいては収集時の同意を要求するものも多く（詳細については本章次節第 1 項参照)、これらを積極的に活用することや、Web サイト上のプライバシーポリシーにおいてクッキー利用の有無を明確化することが望まれる。その際、クッキーにより収集される情報が具体的にいかなる情報かという点や、オプトアウトの方法についても明示すべきである[120]。

また、第 3 章第 5 節第 3 項のように私見としては EC 個別法制定が必要と解するが、かかる EC 個別法で個人情報の収集時にも本人の同意が必要となれば（詳細は本章次節第 1 項)、クッキーにより自動収集する際にも本人の同意が必要ということになる。

情報主体の十分な関与を経てこそ、広告への信頼性が生じ、クッキーの効用が生かされる。この点を再度認識すべきであろう。

（2）バナー広告

バナー広告とは、Web サイト管理者が広告掲載希望企業又は広告配信業者と契約することにより同サイトに掲載された広告のことである。C 消費者は、サイト上のバナー広告に興味を持った場合、そのバナー広告をクリックするだけで当該企業のサイトにアクセスすることが可能となる。

バナー広告は通常クッキーを利用して行われる。クッキーの利用により、特定の端末を使用する個人の趣味や嗜好を調査し、これに適合するようなバナー広告を配信することで、インターネットを利用しない場合と比較して遥かに効果的・効率的な広告が可能となる。

以上のように、バナー広告の問題は前項で検討したクッキーと同様の問題に起因する。

120　前述（第 3 章第 5 節第 3 項参照）の P3P を用いてクッキー利用の有無をプライバシーポリシーにおいて明確化することも現段階では一応の実効性があると考えられる。もっとも、P3P は BptoBrtoC のフロントエンドたる BrtoC においてオプトインシステムとして機能するものであるところ、バックエンドたる BptoBr におけるオプトアウトシステムは未だ構築されていない。現段階では、WS-Privacy がバックエンドのオプトアウトシステムとして注目され始めている。

（3）スパムメール[121]

ⅰ．問題の所在

スパムメールとは、商業電子ダイレクトメールのことであり、通常、一方的且つ不特定多数アドレス宛に大量に送信されるものである。日本では、携帯電話の利用による電子メール授受が一般化した 2000 年頃から、主に携帯電話アドレス宛のいわゆる「迷惑メール」として問題が顕在化してきたものである。スパムメールは、クッキーにより直接収集された個人情報やバナー広告のクリックにより作成されたクッキーから得た個人情報に基づき、送信されることが多い。すなわち、スパムメールの問題は、個人情報の取扱に伴う問題から派生する問題である。

インターネット利用以外のダイレクトメールによっても、一方性・大量性という性質は同様である。しかし、これらにより大量広告しようとすると、人件費や郵送費・通話料、印刷代等のコストが莫大になり、且つそれを送信者側が負担することになる。スパムメールの場合には、大量に送信したとしても送信に要するコストは微々たる額に過ぎない一方で、ユーザー側は受信を事実上強制されることになるため、受信にかかる費用を余儀なく負担させられる場合が多く、また受信したスパムメールの内容を確認し必要ないと判断すれば削除する、という時間及び労力を負担させられることになる。

さらに、スパムメールの送信者（いわゆるスパマー）は多数存在するため、ひとつのアドレス宛に膨大な量のスパムメールが送信される状況も起こり、ユーザーのメールボックスやインターネットサービスプロバイダーISP のサーバに過負荷がかかる結果､機能不全となり、本来必要なメールのやりとりに支障をきたす事態も生じている。

すなわち、インターネット利用以外のダイレクトメールでは、送信者の側で自ら送信を躊躇するインセンティブが働くのに対し、スパムメールの場合にはかかるインセンティブは働かず、むしろ電子メールを一方的に送信することにより、メールの受信者や ISP に対し一方的にコスト負担の不利益を被らせ得る点が問題なのである。ここでは、広告の内容の妥当/不当が問題となるのではなく、スパムメールを一方的に送信すること自体が問題となっている。

ⅱ．法規制

以上のようなスパムメールに対し、日本ではいかなる法規制がなされるか。

まず、個人情報保護法が成立すれば、これにより一定の規制が可能となる。すなわち同

121　岡村・新保・前掲注 15・437～484 頁、岡村・前掲注 108・131～140 頁、西村総合法律事務所ネット・メディア・プラクティスチーム編著『IT 法大全』日経 BP178～202 頁（2002 年）参照。

法案 28 条 2 項は、本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止し得ることを前提として、1 乃至 4 の各号所定事項につき予め本人に通知又は本人が容易に知り得る状態においている場合には、本人の同意なく第三者へ提供し得ることを定めている[122]。この規定により、保有されている情報のうち当該本人が識別される個人データについては、これが第三者たるスパマーへ提供される場合に、各号所定事項を少なくとも本人が容易に知り得ない限り、本人が自らスパマーへの提供の停止を要求し得ることになる。スパマーが提供者となる場合も同様である。もっとも、かかる本人の求めによる第三者提供停止はオプトアウトと呼ばれるが、一般的なオプトアウト方式は第三者提供のみならず発信者への発信停止を求め得るものであるところ、個人情報保護法案ではこの点までは認められていない。そして、当該本人の個人データにつき第三者提供の有無を判断するのは容易でない点に鑑みても、法案 28 条 2 項のスパムメールへの有効性には疑問が残る。

既存の法としては改正特定商取引法[123]がある。2002 年 4 月、特定商取引法が改正されたことにより、C 消費者が受け取りを希望しない旨の連絡を「販売者又は役務提供事業者」（通常スパマーも該当すると解される）に行った場合には、その C 消費者に対する「電磁的方法による広告」（スパムメール）再送信を禁止すること（12 条の 2）及び C 消費者による「販売者又は役務提供事業者」への連絡方法の表示が義務付けられること（11 条 2 項）になった。すなわち、発信者への発信停止を求めるオプトアウト方式が定められたのである。

また、2002 年 4 月には、いわゆるスパムメールへの対応策として特定電子メールの送信の適正化等に関する法律[124]が制定された。同法律は、改正特定商取引法と同様のオプトアウト方式を認めている（4 条）他、スパマーが自らの送信アドレスを偽ることが多いことに鑑み、架空電子メールアドレスによる送信の禁止を定めている（5 条）。一方で、ISP に対しては「特定電子メール」（通常スパムメールも該当すると解される）による支障防止に資するユーザーへの情報提供や技術開発・導入の努力義務を設け（9 条 1、2 項）、第一種電気通信事業者には架空電子メールアドレスにより送信された「特定電子メール」について役務の提供を拒み得ることを定めている（10 条）。

122　個人情報の保護に関する法律案
http://www.kantei.go.jp/jp/it/privacy/houseika/hourituan/327houan.html 参照。
第 28 条 2　個人情報取扱事業者は、第三者に提供される個人データについて、本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であって、次の各号に掲げる事項について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているときは、前項の規定にかかわらず、当該個人データを第三者に提供することができる。
1　第三者への提供を利用目的とすること。
2　第三者に提供される個人データの項目
3　第三者への提供の手段又は方法
4　本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること。

123　改正特定商取引法
http://www.meti.go.jp/policy/consumer/warehouse/tokushoho/spammail/tsh_020701.pdf 参照。

124　特定電子メールの送信の適正化等に関する法律
http://www.soumu.go.jp/joho_tsusin/top/pdf/meiwaku_01.pdf 参照。

アメリカ合衆国では、連邦法レベルでは規制の必要性が主張され法案提出は続いているものの、未だ法制定はされていない一方で、州レベルでは 2002 年 10 月現在 18 の州においてスパム規制法が制定されている[125]。

欧州連合 EU においては、受信者が事前に同意している場合のみ当該スパムメールの送信は認められるとするオプトイン方式の主張とオプトアウト方式の主張が対立し、加盟国の国内法でもいずれかに統一されていない。

iii．裁判例

スパムメールが具体的に問題となった事例について次に検討する。

日本で最初にスパムメール送信差止請求がなされた事件は、ニフティサーブスパムメール送信差止請求訴訟である。この事件は、ニフティの会員に付与されるアルファベット 3 文字に数字 5 桁を配列した識別番号がニフティ会員の電子メールの送付先となっていることに被告が着目し、ランダムにアルファベット 3 文字に数字 5 桁を組み合わせ識別番号とし大量の猥褻なスパムメールを継続的に送付した行為に対し、ニフティが送信差止の仮処分を求めた事例である。浦和地決平成 11 年 9 月 9 日は、ニフティの申立てを相当とし、ニフティサーブの会員に対するスパムメールの送信差止の仮処分を認めた[126]。

また、NTT ドコモ迷惑メール送信差止請求訴訟について、東京地決平成 13 年 10 月 29 日もスパムメール送信差止の仮処分決定を出した[127]。本事件は、090 で始まる 11 桁の電話番号に「@docomo.ne.jp」を付したものを電子メールアドレスとして登録しているユーザーが多いことに着目した被告が、090 に続く 8 桁の数字部分にランダムな数字をあてはめ不特定多数のユーザー及びユーザーの存在しないメールアドレス宛にいわゆる迷惑メールを大量且つ継続的に送信していたことに対し、電子メール送受信サービスを行っていた第一種電気通信事業者である原告 NTT ドコモ株式会社が送信禁止仮処分を申し立てたものである。本決定では、NTT ドコモの「所有する電気通信設備が通常予定している処理能力を超えた大量の電子メールが送信されたことから、その処理等を余儀なくされた結果、同電気通信設備が機能障害を起こし」たことを認定した上で、業者の行為が NTT ドコモの「電気通信設備に対する所有権を侵害しているものと評価でき」、NTT ドコモの「警告後も依然として従前と同様の方法により本件電子メールの発信を大量且つ継続的に行ってきたこと等の事情に照らすと」同行為が「正当な営業活動として法的保護の対象とされているとはいえない」とした。また、「機能障害に至らない場合であっても」「予定された処理能力を超える大量の電子メールの処理を余儀なくされたことから、同電気通信設備の機能の低下を惹起」

125　ワシントン州法（1998 年 6 月施行）やネバダ州法（1998 年 7 月施行）等。
126　浦和地決平成 11 年 3 月 9 日判例タイムズ 1023 号 272～277 頁参照。
127　東京地決平成 13 年 10 月 29 日判例時報 1765 号 18～25 頁参照。

しており、同設備に対する「所有権を侵害したものとみることができ」るとしている。

スパムメールの被害が早くから顕在化していたアメリカ合衆国でリーディングケースとなっているのは、コンピュサーブ対サイバープロモーションズ社及びサンフォード・ワレス事件である[128]。ISP であるコンピュサーブを通じてコンピュサーブ利用者に向けてアメリカ合衆国最大のスパムベンダーであるサイバープロモーションズ社（創業者サンフォード・ワレス）が大量のスパムメールをコンピュサーブの利用規則に反し、またスパムメール防止用のソフトウェアを技術的に出し抜き、継続的に送付したことに対し、コンピュサーブが同社によるスパムメール送信を禁止する仮処分命令を裁判所に求めた事件である。判決において裁判所は、コンピューターに送られる電子信号は他人の財産への侵入と看做されるに足りる有形もしくは物理的な性質を有すると認定した上で、スパムメールに対応する時間やコンピューターシステムの運営力に及ぼされる影響が損害となるとし、不法行為責任を認定した。その結果、原告コンピュサーブの請求は認容され、同社によるスパムメール送信禁止仮処分命令が初めて出された。

ⅳ．小括

スパムメールに関しては、スパムメールの受信者がスパマーを特定することが困難なため事後的な救済では不十分なことも多く、まずは事前予防的措置を採ることが考えられる。

前述のように、日本では、改正特定商取引法及び特定電子メールの送信の適正化等に関する法律においてオプトアウト方式によるスパムメール受信拒否が採用されている。この点、EU で主張が強いオプトイン方式によるほうが、受信する商業広告を自ら決することが可能となり、自律的な社会関係形成に資し、憲法 13 条で保障される人格的自律権の趣旨に合致するとも思われる。しかし、スパムメールは電子メールという手段を利用して商業広告を行うものであり商業広告の自由は営業の自由の一環といえるところ、営業の自由は憲法 22 条 1 項の職業選択の自由に含めて保障されると解され、スパムメールといえども送信行為には一応の憲法上の保障が及んでいる。そして、商業広告について一般消費者がオプトインを行うことは、当該広告の存在について不知である場合が多いことから通常困難である点に鑑みると、一旦はスパムメールによる広告を認めた上でオプトアウトの道を開くことにより当該個人情報の保護及び人格的自律権を実現していく、という方式が、商業広告の自由も憲法上の保障を受けることから見ても望ましい。

もっとも、オプトアウトが実効性を有するのでなければ意味がなく、特定電子メールの送信の適正化等に関する法律 18 条で規定されている、6 条規定の命令に違反した場合の罰

---

128 *CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015 (S.D.Ohio, February 3, 1997) http://www.jmls.edu/cyber/cases/cs-cp2.html、土谷喜輝等編『インターネットをめぐる米国判例・法律 100 選改訂版』ジェトロ 188～189 頁（2001 年）参照。

金制度の活用の他、事後的な救済手段の確立も検討しておくべきである。

スパムメールが送信される際には、インターネットの匿名性を利用し、特定電子メールの送信の適正化等に関する法律の制定後は同法で禁止されるにもかかわらず送信アドレスが偽られることが多く、スパマーを特定することは事実上困難である。また、電気通信事業法 4 条の通信の秘密の義務を負うことが多いスパマーの契約 ISP は、送信者たるスパマーに関する照会を拒否することも多い。かかる状況では、損害を受ける受信者としては自己の契約する ISP に被害を訴え改善措置を要求するという手段を講じることになり、結局 ISP が自身に帰属する損害を主張してスパマーに責任追及し ISP とスパマー間の問題に移行する傾向が強いのが実情である。

そこで、ISP が民事保全手続により送信禁止仮処分を求めるとしても、被保全債権及び損害をいかに捉えるかが問題となる。NTT ドコモ事件のように端的に被保全債権を所有権とし、所有権に基づく妨害排除請求権とすることが単純であるが、ニフティ事件の場合にようにコンピューターシステムがリース契約に基づく場合にはかかる構成は困難であり、占有訴権の積極的活用を再検討すべきとの指摘もされている[129]。また、上記の裁判例では、日本・アメリカ合衆国ともに広告の内容の不適当性ではなくスパムメールを一方的且つ大量的に送信すること自体を問題視し損害を認定していることが窺われる。たとえ通常一般人が不快感を抱く内容の広告の送付であろうと営業の自由の一環として憲法上保障される行為である。としても、電子メールの一方的・大量的送付という手段を採ることにより、受信者の側が費用や時間・労力の負担を事実上強制され、また ISP に機能障害の不利益を被らせるに至った場合、もはや憲法上保障される営業行為とはいえないのではないかが問題となるのである。かく解すると、一方的且つ大量的な電子メールの送付という手段自体から損害を認定することは妥当であり、当然、受信者の費用や時間・労力の負担を損害とし受信者が不法行為責任をスパマーに追及することも可能であろう。

第 2 節　契約締結及び履行の段階

実際に EC に参加し契約を締結・履行する際には、契約の目的を達するため必然的に個人情報を提供しなければならないことも多い。例えば、EC においてある動産の売買契約を締結した場合に当該動産の届け先を明確にしなければならないような場合が挙げられる。必然的に個人情報を提供しなければならないとしても、そのことにより直ちに当該個人情報がいかようにも利用され得ることに同意したとは当然ならず、最大限の配慮をもって取り扱う必要がある。Informed Consent の必要性及び内容の問題である。

129　岡村久道「ニフティ電子ダイレクトメール仮処分決定について」判例タイムズ 1041 号 73～78 頁参照。

また、情報主体が児童である場合に、個人情報の取扱に関し児童が自ら同意する場合や個人情報を提供する場合に、親の関与を必要とするかが問題となり得る。

（1）Informed Consent

ｉ．個人情報保護法案

OECD8 原則で要求されている収集の原則（Collection Limitation Principle）、目的明確化の原則（Purpose Specification Principle）及び個人参加の原則（Individual Participation Principle）に従うと、一般に個人情報を収集・利用する際には情報主体に対し適正な説明と同意すなわち Informed Consent が要求されることになる。個人情報保護法案でも、個人情報取扱事業者の義務として Informed Consent に資する制度を規定している。

まず、新たに個人情報を取得した際には、本人に対し利用目的の通知・公表が要求される（23 条 1 項）。同 2 項では、個人情報取扱事業者が契約やアンケート等により直接情報主体から取得する場合には予め本人に対し利用目的を明示しなければならないとする。また、3 項により、利用目的が変更された場合にも本人に通知・公表しなければならない。かかる 23 条各項を EC との関係で見てみると、EC が行われる際に個人情報が取得される場合、例えば B_1toB$_2$において特定の個人情報が企業間で移転する場合には、1 項により取得側の B_2企業が情報主体に対し利用目的を通知・公表しなければならない。また、BtoC において C 消費者が契約締結の際に Web 上のフォームに自ら必要事項を記入する場合には、2 項で「契約書その他の書面」に続けて「（電子的方式・・・を含む）」とあることから同項が適用され、予め情報主体に対し利用目的を明示することが要求される[130]。1、2 項に従い示された利用目的が変更された場合に 3 項が適用されるのは当然である。

既に保有されている個人データ[131]については、29 条 1 項各号において規定されている。すなわち同条 1 項は、当該個人情報取扱事業者の氏名又は名称（1 号）や全ての保有個人データの利用目的（2 号）、本人からの利用目的通知請求（同条 2 項所定）・保有個人データの開示請求（30 条所定）・訂正、追加又は削除請求（31 条所定）・利用の停止又は消去請求（32 条所定）がなされた場合の手続（3 号）、その他政令規定次項（4 号）、を本人が知り得る状態に置くことを要求している。1 号は責任主体明確化のためであり、OECD8 原則の責任の原則（Accountability Principle）に対応しているといえよう。3 号は、個人参加の原則（Individual Participation Principle）を全うすべく、情報主体による利用目的通知や開示、訂正、追加又は削除、利用停止や消去の請求を、実効あらしめるためである。同条により、

130　P3P の利用による通知も考えられる。

131　個人情報の保護に関する法律案
http://www.kantei.go.jp/jp/it/privacy/houseika/hourituan/327houan.html 参照
第 2 条 4　この法律において「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をいう。

BtoC、BtoB を問わず個人データが保有されている場合には、1 項各号所定の事項につき情報主体に明らかにすることが要求される。

個人情報保護法案で情報主体の同意が規定されているものとしては、21 条の目的外利用についての本人の同意及び 28 条の第三者提供についての本人の同意である。すなわち、21 条は目的外に当該情報を利用する場合（1 項）及び合併等により個人情報を取得し承継前の利用目的外で利用する場合に（2 項）予め本人の同意を得ることを要求している。これらの規定は EC においても当然適用され、一定程度の Informed Consent が実現されるといえる。また、取得・保有されている情報を第三者へ提供する場合には、原則として本人の同意が必要とされる（28 条 1 項）。これにより、B_1toB_2において個人情報が企業間で移転する場合に、譲渡側の B_1企業は情報主体の同意を得ることが必要となる。BtoC においても、取得・保有されている C 消費者の個人情報が第三者へ提供される場合には、当該 C 消費者の同意が必要となる。

ⅱ．裁判例

個人情報の収集について Informed Consent が実現されなかったことに起因する事件として、アメリカ合衆国でのジオシティーズ事件が挙げられる[132]。この事件は、ジオシティーズ社の Web サイトにおける個人情報の取扱に関し自ら規定した規則の遵守を怠ったことについて、アメリカ合衆国連邦取引委員会 FTC が申し立て、裁判手続ではなく FTC の同意審決という審査手続で是正措置が採られたものであり、インターネットプライバシーに初めて FTC が関与した事件である。

具体的には、ジオシティーズ社の Web サイトを利用する際、オンライン上のフォームに個人識別情報を含めた特定の情報を記入することや広告主から広告やサービスを受けることの選択が要求されていたが、当該 Web サイトにおいて、収集された個人情報は広告やサービスを受ける目的にのみ利用されることや情報主体の同意なく第三者へ提供されないことが表示されていた。しかし実際には、個人識別情報を含めて同意なく第三者へ提供されていたことが判明した、というものである。

同意審決において、FTC は同社による表示が偽り（misrepresenting）すなわち欺瞞的表示であり、欺瞞的表示をした上で個人情報を収集したことは不正取引手段にあたるとした。そして、同社が個人情報を収集又は利用する際に目的を偽ってはならないこと、同社の Web サイト上でプライバシーポリシーを表示し、収集される情報や利用目的、第三者提供され

---

132 *In re GeoCities, Inc.*, 63 Fed. Reg. 44624 (August 20, 1998)、*Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case -Commission Establishes Strong Mechanisms for Protecting Consumers' Privacy Online-* http://www.ftc.gov/opa/1998/9808/geocitie.htm、
平野・前掲注 41・240～241 頁、土谷・前掲注 128・160～161 頁参照。

る相手方、情報へのアクセスや削除の仕方を示すこと等が定められた。

また、同社は子供向けのサイトで収集した児童に関する個人情報は自社が保持すると表示していたが、実際には第三者へ提供し当該第三者が児童向けサイトを運営することを認めていた。この点について同意審決は、同社が 12 歳以下の児童の個人識別情報を収集する際には親の明示的な同意を要求することとした。

ⅲ．小括

ⅰで見たように、個人情報を新たに取得する場合（23 条）及び既に保有している個人情報（29 条）について、個人情報保護法案でも利用目的や各種手続について一定の「説明」が要求されており、EC にも適用される。しかし、目的外利用（21 条）や第三者提供（28 条）の場合のような情報主体の「同意」まで要求されているものではなく、この点で個人情報保護法案では Informed Consent が実現されているとは言い難い。

Informed Consent は、その名のとおり、適切に提供された情報に基づき「同意」することをも意味するからである。OECD8 原則のひとつたる収集の原則（Collection Limitation Principle）において可能な限り情報主体の同意を得て収集されることが要求されているのも、個人情報についての Informed Consent を広く認めていく方向性の現われといえる。個人情報保護法案ではかかる規定はないため、自らの個人情報が取得又は保有される際に、一方的に利用目的等一定事項の通知を受けるのみであり、当該利用目的に同意しかねる場合にも取得・保有を拒否することは認められておらず、当該情報が事実に反する場合の削除請求（31 条）や目的外利用や不当な第三者提供がなされた場合の利用停止又は消去請求（32 条）をなし得るのみである。

しかし、EC における個人情報の取扱の特質として、本人が不知の間に収集・利用・改竄等され易い点が挙げられることに鑑みると（第 2 章第 2 節参照）、EC において個人情報が取り扱われる場合に 31 条や 32 条の手段を講じるのは事実上極めて困難といえる。特に Web サービス時代にあっては、情報主体が不知のまま個人情報が転々流通する可能性が高い。

とすれば、EC においては、少なくとも収集の際に情報主体の同意を要求し、可能な限りの Informed Consent を実現することが、自己に関する情報を自らコントロールすることで個人の自律領域を保護し自律的な社会関係形成を尊重しようとした、自己情報コントロール権としてのプライバシー権保障（憲法 13 条）の精神に合致すると思われる。また、一度侵害されると回復困難というプライバシー権の性質に鑑みても、収集時の同意は必要ではないのか。私見としては、既に示したように EC における個人情報の取扱を対象とした個別法を制定すべきと考えるが（第 3 章第 5 節第 3 項参照）、かかる EC 個別法においては収集時の同意を要求することが望ましいと考える。

この点について、既存のガイドラインでも収集時の同意を要求しているものは多数見受

けられる。例えば、旧通商産業省による『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』[133]では、情報主体から直接収集する場合及び間接的に収集する場合に、利用目的等の一定事項を通知するとともに、収集・利用・提供に関する同意を得ることが要求されている（8、9 条）。日本商工会議所による『電子商取引における個人情報の保護に関するガイドライン』[134]でも 7、8 条において、日本工業規格 JIS Q 15001[135]でも 4.4.2.4 及び 4.4.2.5 において直接収集・間接収集について同様の規定が設けられている。また、サイバービジネス協議会による『サイバービジネスに係る個人情報の保護に関するガイドライン』[136]においては、3 条で収集目的明確化を要求するとともに 8 条 1 号で収集される個人情報等の内容を情報主体に周知する措置を採るよう努めるべきとしている。本ガイドラインの「解説」では、サイバービジネスにおいては、アクセス・ログ等、現在は個人識別情報でないものの将来他の情報と照合することで個人識別可能性が生じ得る情報が取り扱われている点に着目し、情報主体が収集の事実を認識する必要性が述べられている。EC 個別法制定を検討する際にこれらが参考となるのは言うまでもない。

そして、ジオシティーズ事件の FTC 同意審決は、個人情報の適正な収集の要求を確認するものとして日本における取扱を検討する上でも参考となろう。

なお、一旦は収集につき同意を与えたものの、何らかの理由により同意を取り下げたいと考えた場合のオプトアウトも保障されるべきである。なぜなら、オプトアウトが保障されなければ同意を躊躇する可能性が高まり、当該個人情報の収集が必然性を帯びる場合（例えば EC により動産の売買契約を締結し当該動産の届け先を明示する場合という前述の場合）にも情報提供が躊躇されることになれば、EC 促進は著しく阻害され得るためである。

21 条及び 28 条で規定する合併等の場合や第三者提供は、契約履行後に通常問題となるので、本章第 3 節で改めて検討する。

（2）児童による自己に関する個人情報の処分

個人情報の取扱に関し情報主体たる児童が同意する場合や自ら個人情報を提供する場合、親の関与を必要とする見解がある。

アメリカ合衆国における前述の COPPA がかかる見解を顕著に示している。すなわち COPPA は、SEC.1303.(ｂ)REGULATIONS において、Web サイト上で 13 歳未満の児童から個人情報を収集する場合に、収集される情報とその利用方法・開示手続を Web サイトで示すこと、収集・利用・開示につき親の明確な同意を得ること、親からの要求があれば

133 前掲注 67 参照。
134 前掲注 71 参照。
135 前掲注 72 参照。
136 前掲注 68 参照

児童から収集した個人情報を示すこと、既に収集済みの個人情報の利用や将来の新たな収集を親が拒否する機会を提供すること、等を要求している[137]。また、プライバシーマーク制度 TRUSTe においても、Web サイト上で 13 歳未満の児童から個人情報を収集する際には、COPPA に従い別途規定された『TRUSTe 児童プライバシーシールプログラム（The TRUSTe Children's Privacy Seal Program）』の要求に従わねばならないとして、特別の配慮を要求している[138]。

しかし、個人情報保護法案には児童の個人情報に関する特別の規定はなく、日本工業規格 JIS Q 15001 においても同様である。

オンライン上では取引相手が児童であるか否か容易には判別し得ず、認証の問題とも絡み問題は複雑である。もっとも、ある情報が当該児童自身の個人情報であるのみならず、児童の個人情報が同時に親を含む家族の個人情報である場合もあり、判断能力が十分とはいえない児童がオンライン上で安易に個人情報を提供等してしまうと、被害が甚大となるおそれも高い。特に Web サービスにおいて本人不知の特性が強いことに鑑みても問題は大きい。包括的基本法たる個人情報保護法案で何らかの規定を設けることは困難であろうが、財団法人日本情報処理開発協会 JIPDEC によるプライバシーマーク制度や EC 個別法で児童からの個人情報の収集につき特別の配慮を加えることも十分考えられるであろう。

先述のジオシティーズ事件において、同意審決は、同社が 12 歳以下の児童の個人識別情報を収集する際には親の明示的な同意を要求することとしたが。同意審決がなされた 1998 年 8 月当時 COPPA は未制定の状況下にあった（なお、COPPA 制定は 1998 年 10 月 21 日）。COPPA 制定により、13 歳未満の児童から個人情報を収集する際に親の明確な同意が必要となったことから、当該同意審決の同内容は一般的に維持されることになったといえる。

第 3 節　契約履行後の段階

契約が締結・履行され、両当事者がもはや契約関係の拘束下になくなった後も、既に収集された個人情報の取扱はなお問題となる。契約終了に伴い当初の目的に従った利用が実現された後に、新たに当初の目的外で利用する場合[139]や不適切な管理により漏洩・毀損する場合[140]も挙げられようが、特に問題となるのは、当該個人情報が両当事者以外の第三者に提供される場合や企業間の営業譲渡や合併に伴い移転される場合である。本節では以上を個別に検討する。

137　前掲注 55 参照。

138　前掲注 59、The TRUSTe Children's Privacy Seal Program http://www.truste.org/programs/pub_child.html 参照。

139　法案第 21 条の問題となる。

140　法案第 25 条の問題となる。

（1）第三者提供

ⅰ．個人情報保護法案

本章第 2 節第 1 項で検討したように、個人情報保護法案においては個人情報を第三者へ提供する場合について 28 条で本人の同意を要求している。既に取得・保有された個人情報は、当初の目的に従った利用が終了した後もそれ自体が売買の対象物たる価値を有する場合が多く、しかもインターネット利用により容易且つ迅速に、本人が不知の間に提供されることが可能である。そこで、かかる提供に際して情報主体たる本人に Informed Consent を実現し、関与の機会を与えるのが 28 条である。この第三者提供も、EC に限らず個人情報が取り扱われるあらゆる場面で問題となり得るが、特に Web サービス時代の EC では容易性・迅速性及び本人不知の特性が強まることと相俟って問題は深刻である。28 条違反が認められる場合には、情報主体は 32 条に従い提供停止を求めることができる。

第三者提供については、提供に情報主体たる本人の同意が必要となる「第三者」の意義が問題となる。法案では同条 4 項 1 乃至 4 号において規定されており、取扱委託がなされた場合の受託者（1 号）、事業承継がなされた場合の承継者（2 号）、共同利用者（3 号、但し本人への通知等が必要）は「第三者」に含まれない。2 号の例としては、明文上の合併の他、相続や営業譲渡、会社分割等が含まれると解される。また、3 号の例としては、親子会社やグループ企業間での共同利用が挙げられる[141]。

ⅱ．裁判例

第三者提供に関しては、現実社会の場面において日本でも以前から問題となっている。

例えば、東京地判平成 2 年 8 月 29 日の事案では、マンションの販売業者がマンション購入申込書に記載された購入者の勤務先の名称及び電話番号を同マンション管理の委託が予定されている会社に開示したことがプライバシー侵害となり損害賠償請求され得るかが問題となった[142]。この点につき判決では、勤務先の名称及び電話番号はプライバシーに属するとした上で、情報主体が承諾していなかったにもかかわらず第三者たる管理委託予定会社に開示したことは「プライバシーの侵害行為に該当する」とした。もっとも、「プライバシー開示行為の態様も社会的にみて相当な範囲内」であったこと及び情報主体に「特に異議がないものと信じたことには相当の理由があった」ことから、「開示は違法性を欠き不法行為を構成しない」とし請求を却下した。同事件では、承諾を欠くプライバシー該当情報の第三者への開示がプライバシー侵害行為となることを認めた点に意義がある。

141　藤田康幸著『個人情報保護Q＆A』中央経済社 109～110 頁（2001 年）参照。

142　東京地判平成 2 年 8 月 29 日判例タイムズ 751 号 161～167 頁参照。

また、東京地判平成 3 年 3 月 28 日の事案では、銀行が住宅会社と共催でアパート経営勉強会を行うべく顧客に案内状を送付した際、顧客の住所氏名及び顧客番号を記した宛名ラベルを貼付した封筒の投函を当該住宅会社に依頼した行為が顧客情報の漏洩にあたり損害賠償請求が認められるかが問題となった[143]。判決は、「取引銀行が職務上知り得た右の私的な情報を」「第三者に漏泄した場合には、原則として債務不履行責任あるいは不法行為責任を負」い、それは「共同事業のために利用する際にもあてはまる」として、プライバシーとの言葉の使用を避けつつも共同事業者への開示であっても守秘義務違反となる場合があることを認めた。もっとも、本件では当該第三者が封筒表面の記載に全く関心を有していなかったことから、少なくても守秘義務違反の漏泄行為とはいえないとした。

東京地判平成 10 年 1 月 21 日の事案では、加入電話契約者が NTT に対し電話帳に氏名・電話番号・住所の掲載拒否を求めたにもかかわらず掲載されたことがプライバシー侵害となるとして不法行為に基づく損害賠償請求及び電話帳の廃棄を求める広告配布請求がなされた[144]。判決では、「他人に知られたくない指摘事柄をみだりに公表されないという利益（プライバシーの利益）は」「個人の私的事柄をみだりに第三者へ公表したり、利用することを許さず」「法的保護の対象となる」とした上で、「氏名・電話番号・住所は、法的に保護された利益としてのプライバシーに属する」とした。もっとも、本件では「被告に害意ないし故意は存しなかったこと」等から慰謝料額は 10 万円程度とされ、また「少なくとも本件において」広告配布請求を認めるのは困難であるとした。同判決の意義は、氏名・住所・電話番号といった個人情報の中でも基本的個人情報がプライバシーに属し第三者提供の場面を含み法的保護の対象となるとされた点及びプライバシー侵害状態除去のための広告配布請求が認められる余地を残した点にある。

東京高判平成 10 年 2 月 26 日の事案では、個人信用情報が個人信用情報センターに登録されることの適法性が争われたが、同判決はこれを適法とした[145]。本判決は、本件の個人信用情報の登録制度を適法な制度とした上で[146]、有効期間内の支払いについては「会員規約の効力が維持される」ところ、同「規約により生じた客観的な取引事実に基づく信用情報」の登録及び利用につき予めの同意があった本件では同意条項に基づき登録をなし得るとした。本判決は、個人信用情報の登録につき予めの同意を欠く場合にプライバシー侵害となるか否かについて判断するものではないが、なお侵害となり得る余地を残すものといえる。

143　東京地判平成 3 年 3 月 28 日判例タイムズ 766 号 232～241 頁参照。

144　東京地判平成 10 年 1 月 21 日判例タイムズ 1008 号 187～191 頁参照。

145　東京高判平成 10 年 2 月 26 日金融法務事情 1526 号 59～65 頁参照。

146　登録制度自体の適法性につき、同判決は「消費者の信用情報の登録・利用について」「消費者本人の同意を得なければならない」点や「情報の開示先」が「一定の範囲に限定」されている点、開示は「与信取引の判断に必要な場合に限」られている点から、登録制度は「公共性・公益性を有し、合理性のある制度」であるとした。もっとも、個人信用情報の登録制度の適否については、本稿の射程から外れるため深く検討することを避ける。

ⅲ．小括

情報主体の同意を欠いて個人情報が第三者に提供される場合は、自己情報コントロール権たるプライバシー権侵害が顕著に現れる場面である。第 2 章第 1 節で既述のように、自己情報コントロール権は個人の自律領域を保護することで自律的な社会関係の形成尊重を図る権利であるところ、情報主体の同意なく当該個人に関する情報が自由に流通されるとすれば、もはや社会関係を自律的に形成することは著しく困難となる。上記の現実社会の場面での各裁判例で、一定の個人情報を同意なく第三者へ開示することがプライバシー侵害行為ないし類似行為になると積極的に判断しているのも、かかる意識に基づいていると解し得る。

そして、個人情報自体に取引対象としての価値が生じ易い一方、Web サービス時代の EC では情報流通を容易且つ迅速になし得、情報主体が不知の間に提供される可能性が高く、情報主体が関知した時点では既に取り返しのつかない事態に至っているおそれも高い。Web サービス時代の EC における第三者提供の際に情報主体の関与を認め可及的に保護する必要性は特に高いのである。

（2）営業譲渡や合併の場面

近年、企業間における営業譲渡や合併は珍しくない。営業譲渡や合併がなされると、これに伴い個人情報が移転し、移転先の個人情報と結合することによって、個人識別性が生じる可能性がある。例えば、B_1企業が B_2企業に吸収合併され、各々の保有していた個人情報はそれ自体では個人識別可能性のない単なる統計情報であったとしても、両企業の個人情報データベースが合併に伴い結合することにより特定の個人が識別可能となる個人情報データベースが構築される場合等である。本章本節第 1 項で検討したように、事業承継がなされた承継者は法案 28 条 4 項 2 号により「第三者」に含まれないため、同法案ではかかる場合にも情報主体たる本人の同意は必要とされないことになる。

2000 年、クッキーを利用して個人情報を収集していたダブルクリック社が、ダイレクトマーケティング事業を営み現実社会における個人識別情報を保有するアバクス・ダイレクト社を買収したことで、両企業の各々保有する個人情報の結合が問題となった。ダブルクリック社は、自社がクッキー利用により得た個人情報と現実社会の個人識別情報を組み合わせることで効果的なバナー広告を実現するとの計画を発表した。この計画に対し批判が相次ぎ、各州の検事総長も参加した FTC による調査が開始された[147]。批判を受けて、同社はオンライン上の個人情報保護基準が確立されるまでは当該計画を見合わせることを発表し、また同調査では、ダブルクリック社が個人識別情報を目的外には利用しておらず買収

147　同調査では、他に eBay や eToys、Amazon.com も調査対象とされた。

に伴い個人情報の結合もしていないことが明らかになった。2002 年、同社は各州との和解に至った。

個人識別情報と結合せずバナー広告の効果を挙げることも可能であり、ダブルクリック社の計画が強い批判を受けたのも首肯し得る。なお、同社がオンライン上の個人情報保護基準の欠如を指摘している点には注目される。C 消費者を含む情報主体のみならず、B 企業側にとっても個人情報保護法制の整備は有益であり、重大な関心事なのである。

営業譲渡や合併等の場合に個人情報保護法案で情報主体の同意が要求されていないのは、かかる場合にまで要求すると企業の自由な組織再編を阻害することを懸念し調和を図ったものと解される。しかし通常の第三者提供の場面と同様の問題が生じる以上、運用として、同意か少なくとも通知を可能な限り行うことが望ましく、B 企業への信頼にもつながる。自主規制としてガイドラインで要求することや、EC 個別法で検討され直すことも考えられる。

第 4 節　当事者及びサイバーモール運営者の責任

前節までにおいては、EC における個人情報の取扱に関していかに情報主体の関与を認めていくべきか、について考察してきた。本節では、情報主体が十分に関与し得ず、当該個人情報の漏洩や毀損等の損害が発生した場合に当事者及びサイバーモール運営者が負う責任について検討する。

（1）当事者の責任

EC において契約関係にある者同士は、互いに債務不履行責任（民法 415 条）を負う。BtoC の際に C 消費者の個人情報が適切に取り扱われることが契約内容となっている場合（例えばプライバシーポリシーで示されている場合[148]）には、当該個人情報の不適切な取扱をもって債務不履行責任を B 企業に問い得る。直接的には契約内容となっていない場合にも、安全配慮義務を根拠に債務不履行責任を問い得る場面も考えられる。安全配慮義務とは、契約関係という特別な社会関係に入った以上、当該法律関係の付随義務として当該契約の履行にあたり相手方の生命や身体・財産に危害が及ばないよう配慮すべきであるという、信義則（民法 1 条 2 項）上の義務のことである[149]。また、BtoB、BtoC を問わず、不正アクセス禁止法等の既存の法や法律成立後の個人情報保護法に違反する場合には、取扱を行った当該 B 企業に対し不法行為責任（民法 709 条等）を問い得るのは当然である。

しかし、直接不適切な取扱を行った B 企業に対し、情報主体である個人が債務不履行責

148　プライバシーポリシーは契約内容となっていると解するのが自然である。

149　最判昭和 50 年 2 月 25 日民法判例百選Ⅱ[3]12～13 頁参照。

任や不法行為責任を追及していくには、当該個人の側で、匿名性の強いインターネット上で取引主体となっている当該 B 企業を現実社会の特定企業または特定人と同定することが必要となるが、これは事実上困難である。そこで、サイバーモールの運営者に対し責任追及していくことが考えられるが、サイバーモール運営者と情報主体とは直接の契約関係にないため、契約責任である債務不履行責任は問い得ないのが原則である。それでは、サイバーモール運営者にはいかなる責任追及もなし得ないのか。項を改めて検討する。

（2）サイバーモール運営者の契約責任

前述のように、情報主体と直接の契約関係に立たないサイバーモール運営者は債務不履行責任を負わないのが原則である。

もっとも、サイバーモール運営者が営業主体であると誤認するような外観が備わっている場合に、商法 23 条の類推適用により、名板貸人と同様の表見責任を負い、本来の営業主体たる B 企業と連帯責任を負うことが考えられる。この点、最判平成 7 年 11 月 30 日は、スーパーマーケットのテナントであるペットショップに関し、当該ペットショップの営業主体がスーパーマーケットであると誤認するような外観を備えていたとして、商法 23 条類推適用により名板貸人と同様の責任を負うとした[150]。かかる判例法理は、EC におけるサイバーモール運営者と営業主体たる B 企業との関係にもあてはまると解され、営業主体がサイバーモール運営者であるかのような外観が存在する場合に、サイバーモール運営者が営業主体たる B 企業と連帯して債務不履行責任を問われ得ることになる。かかる責任追及を回避するには、営業主体を明確に示す必要がある。

また、特にサイバーモール運営者がインターネットサービスプロバイダーISP であった場合に、ISP の過失により個人情報が不当に流出・漏洩されたような場合には、インターネット接続に関する契約違反として ISP に対し債務不履行責任を負い得る。

（3）サイバーモール運営者の不法行為責任

不法行為の要件を満たす場合には、情報主体はサイバーモール運営者に対し不法行為責任を追及することが考えられる。この点では、ネットワーク管理等を行うサイバーモール運営者に注意義務が認められるかが問題となる[151]。

150　最判平成 7 年 11 月 30 日重版平成 7 年商法[1]79～80 頁参照。

151　近時は、アプリケーションサービスプロバイダーASP が自らサイバーモール運営者となったり ASP からサーバ上のディスクスペースがレンタルされサイバーモールが運営されたりすることが多い。ASP とは、ネットワークを介してアプリケーション機能を提供するサービス事業者のことである。@IT Insider's Computer Dictionary［アプリケーションサービスプロバイダー］ http://www.atmarkit.co.jp/icd/root/00/61967900.html 参照。本来企業内の IT 部門が管理しているサーバをデータセンター（ASP センター）に置きインターネットの回線を使って利用、すなわちアプリケーショ

ネットワーク管理者の責任としては、インターネット上の名誉毀損に関するインターネットサービスプロバイダーISP の不法行為責任について議論が進んでいるところなので、以下でまず参照してみたい。

ｉ．名誉毀損に関してのアメリカ合衆国の法理[152]

インターネット上で名誉毀損行為が行われた場合、匿名性が高く行為者への責任追及が困難であるため、ISP へ責任転嫁することが考えられる。不法行為法の目的のひとつたる被害者の救済を実現するには ISP への責任追及を認める必要性が高い一方で、ISP は表現の自由（憲法 21 条 1 項）の担い手として公共的役割を有するところ、安易に ISP の注意義務違反を認めると表現の自由に対する萎縮的効果が生じるおそれが高い。そこで、両者の調整の要請が出てくる。

アメリカ合衆国における名誉毀損法理では、本や新聞等の出版社や発行者は（第一次的・狭義の）パブリッシャーpublisher として作者と同様の有過失責任を負い、一方で本屋や新聞スタンド、図書館のような頒布・伝達等の役割を果たすに過ぎない者はディストリビューターdistributor（又は第二次的パブリッシャー）として名誉毀損資料の存在につき少なくとも知り得る合理性が存在しない限り責任を負わないとされる。このように原告の立証責任の程度に相違が設けられるのは、不適切性について関与する機会の有無による。

かかる法理はサイバースペース上でも適用されるとされ、一般に ISP は実質的に編集権を持たない限りディストリビューターとしての責任を負うのみであり、十分な編集権を行使する場合にのみパブリッシャーとしての責任を負う、とされてきた[153]。しかし、かく解すると、編集権を積極的に行使して名誉毀損行為の自主規制に努めた ISP ほどパブリッシャーとして重い責任が課されることになる。そこで、不都合性を回避すべく、通信品位法 230 条 c が制定され、真摯な自主的行為を行った ISP がパブリッシャーと看做されてはならないと規定された[154]。

同条項が新たな問題を提起する。すなわち、同条項で免除される責任の範囲は、狭義のパブリッシャーとしての責任に留まるのか、それとも広義のパブリッシャーとしての責任まで含めてディストリビューターとしての責任も免除されるのか、という問題である。こ

ンをレンタルまたはリースする形式で再販するサービスの提供者を示す。ASP のサービスは、ネットワークのアウトソーシングビジネスである。

152　平野・前掲注 41・175～185 頁、平野晋「ユーザーの名誉毀損行為に対する ISP の民事責任（上）」判例タイムズ 1002 号 38～45 頁、平野晋「ユーザーの名誉毀損行為に対する ISP の民事責任（下）」判例タイムズ 1003 号 81～88 頁参照。

153　*Cubby Inc. v. CompuServe Inc.,* 776 F. Supp. 135 (S.D.N.Y. ,October 29, 1991) http://www.jmls.edu/cyber/cases/cubby.txt、*Stratton Oakmont, Inc. v. Prodigy Service,* 23 Media L. Rep. (BNA) 1794, (N.Y. Sup. Ct., May 24, 1995)　http://www.jmls.edu/cyber/cases/strat1.html 参照。

154　47 U.S.C.A. § 230 (1996)

の点につき裁判所は、ゼラン対 AOL 事件において、後者と解すると判示した[155]。しかし、当該判決には批判も強い。すなわち、当該判決は、通信品位法 230 条 c の目的を ISP に対する萎縮的効果を防止すること及び自主規制を奨励することとし、パブリッシャーのみならずディストリビューターの責任を負わせることもかかる目的に反するとしているが、名誉毀損を知っていた場合にも常に一切の責任が免除されるとすれば、却って自主規制奨励を阻害するおそれが高い、というものである。そこで、ディストリビューターとしての責任免除までは認めていない規定と解しつつも、同条項の趣旨に鑑みて責任を緩和し、少なくとも知り得る合理性が存在する場合に一定の作為義務を課し、これを怠る場合にいわば条件付の責任としてディストリビューターとしての責任を負う、と解することも考えられる。

以上の法理を単純化すれば、表現の自由との調和の観点から編集権による関与の程度に着目しつつ自主規制奨励の観点も加味し ISP の責任を認めていく法理といえる。

ⅱ．名誉毀損に関しての日本の法理

日本でも、インターネット上の名誉毀損行為に関しネットワーク管理者の責任が問われた事件は近時になり頻発している。

初めて裁判所が判断を下したものとして、ニフティサーブ事件がある。この事件では、ニフティサーブ（当時）の電子会議室への発言が名誉毀損に当たるにもかかわらず発言の削除を怠ったとして、システムオペレーター及びニフティが損害賠償請求された。東京地判平成 9 年 5 月 26 日は、シスオペは名誉毀損について「具体的に知ったと認められる場合には」「必要な措置をとるべき条理上の作為義務」を負い、これを怠った場合には不法行為責任（民法 709 条）を負うことになり、当該シスオペを雇用していたニフティは使用者責任（民法 715 条）を負うとした[156]。しかし、控訴審たる東京高判平成 13 年 9 月 5 日は、シスオペ及びニフティに対する責任を棄却した[157]。シスオペは削除権限を有するが、本件で直ちに削除しなかったのは議論の積み重ねにより発言の質を高めるとの考えに従ったものであり、削除相当発言について被害者に「遅滞なく」「注意を喚起した他」削除の「措置を講じる手段について了解を求め」たのち、削除要求を受けて削除をした等の行動に照らすと、「権限の行使が許容限度を超えて遅滞したと認め」られないため、シスオペの削除義務違反及びこれを前提とするニフティの使用者責任を否定したのである。

また、都立大学内で対立するグループの一方グループに属する者が都立大のパソコン教室のシステム内に開設したホームページ上に名誉毀損文書を掲載したという都立大事件に

155　*Zeran v. America Online, Inc.,* 958 F.Supp. 1124 (E.D. Va. ,March 21, 1997) http://www.jmls.edu/cyber/cases/zeran.html、土谷・前掲注 128・174～175 頁参照。

156　東京地判平成 9 年 5 月 26 日判例時報 1610 号 22～44 頁参照。

157　東京高判平成 13 年 9 月 5 日　http://courtdomino2.courts.go.jp/kshanrei.nsf/参照。

おいても、ネットワーク管理者の削除権限の有無が争点となった。東京地判平成 11 年 9 月 24 日は、「管理者が削除権限を有するのは」当該ネットワーク全体の「信用の毀損を防止する必要があるからであり」被害者保護のためというわけではないとした。そして、「管理者においては当該文書が名誉毀損にあたるかどうかの判断も困難なことが多」く「名誉毀損行為の被害者に被害が発生することを防止すべき私法上の義務を負わせることは原則として、適当ではない」とし、防止義務を負うのは「極めて例外的な場合に限られ」、本件ではかかる例外的場合にあたらず、本件でネットワーク管理者は削除義務を負わないとした[158]。

以上のように、日本でも一定の場合にネットワーク管理者に作為義務を認め、これを怠る場合に責任追及し得るとの方向性にあるといえる。もっとも、各裁判例において作為義務が発生する要件については一定していない。

2001 年に成立した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（以下、プロバイダー責任制限法）[159]は、ISP を含む特定電気通信役務提供者が責任を負う場合があることを明確化している。すなわち同法は、不特定の者によって受信されることを目的とする電気通信（2 条 1 号「特定電気通信」）による情報の流通により権利侵害があった場合に、特定電気通信役務提供者が、送信防止措置を採ることが技術的に可能であり、且つ権利侵害につき同提供者が悪意であるか（3 条 1 項 1 号）又は情報の流通を知り権利侵害についても知り得る場合（3 条 1 項 2 号）でない限り、同提供者が被権利侵害者に対し損害賠償責任を負わないことを定めている（3 条 1 項）。同条項は免責規定の形式を採用しており、各号に該当することにより直ちに損害賠償責任を負うことにはならない。

Web サイト上で名誉毀損という不法行為がなされた場合、本来的な責任はネットワーク管理者ではなく行為者にあり、第一次的には行為者に責任追及されるべきである。また、名誉毀損該当性の判断は容易でなく、名誉毀損に該当し得る行為を知ったことにより直ちに責任を負う、というのではネットワーク管理者に著しく酷である。責任を負う場合の要件につきさらなる検討が必要といえよう。

ⅲ．名誉毀損に関する法理を EC に適用することの可否

以上の法理は、EC のサイバーモール運営者について直ちに適用可能とはいえない。なぜなら、EC の過程でサイバーモール運営者が果たす役割は店舗出展の場の提供であり、表現の自由の担い手としての役割は EC においては希薄化されているためである。すなわち、表現の自由との調和という要請は低い。また、保護利益についても名誉毀損の場合とは異な

158　東京地判平成 11 年 9 月 24 日判例時報 1707 号 139～146 頁参照。
159　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 http://www.soumu.go.jp/joho_tsusin/top/pdf/jyoubun.pdf 参照。

っており、保護の要請はむしろ高い。すなわち、名誉毀損の場合には真実性の証明により当該本人は救済の余地があるが、プライバシー権は真実であればあるほど侵害の程度が大きく、Web サービス時代の EC の特性と相俟って（第 2 章第 2 節参照）一度侵害されること自体が甚大な被害を生むおそれが高い。これらの点からは、サイバーモール運営者に厳格な責任を要求することは可能とも思われる。

もっとも、営業主体たる B 企業と契約関係にあるとはいえ匿名性が強いインターネット上の取引について、取引の場の提供者に過ぎないサイバーモール運営者が当該取引において個人情報が適切に取り扱われているか否かを逐一チェックすることは事実上不可能に近く[160]、そもそもセキュリティホールに気づくこと自体も一般的に困難である。とすれば、表現の自由との調和という要請が低くとも、直ちに厳格な責任を要求することは妥当でなく、サイバーモール運営者に要求可能な期待可能性を考慮した上で責任を負わせるべきである。

このように、名誉毀損に関する ISP の責任法理は、ネットワーク管理等を行う者として期待される役割及び保護利益が異なるため、直ちに適用可能ではないが、同様にネットワーク管理等に従事し直接の行為者ではないサイバーモール運営者に対して不法行為責任を追及する法理としてなお参考となろう。

そして、ISP の関与の程度により立証責任の程度に差を設けるアメリカ合衆国の法理は、EC の個人情報の取扱の場面でも同様の考え方が可能である。すなわち、サイバーモール運営者は本来なら情報を機械的に伝達する機能のみが期待されているところ、個人情報の取扱について実質的に関与する場合にのみ不適切な取扱を行った B 企業と同様の責任を負い、それ以外の場合には不適切な取扱につき少なくとも知り得る合理的理由があるときに限り責任を負う、と考えることができる。そして、積極的に介入しようとした場合には、実質的関与といえる場合にも厳格な責任は排除し、条件付きで後者の緩やかな責任を負わしめるに留めるとすべきである。その際の条件としては、サイバーモール運営者の期待可能性を考慮し、当該不適切な取扱やセキュリティホールについて通常のサイバーモール運営者であれば認識しているものであり且つ当該 B 企業に対して警告を発する等の手段を講じていないこと、を挙げることが考えられる。

また、日本におけるプロバイダー責任制限法は、前述のように不特定の者によって受信されることを目的とする電気通信の送信（2 条 1 号「特定電気通信」）による情報の流通により権利侵害がなされた場合を対象としている（3 条）ことから、EC の場面に適用することは困難である。

160　憲法第 21 条 1 項及び電気通信事業法第 3 条の禁止する検閲に該当するおそれもある。

終章

本稿では、Web サービス時代の EC における個人情報の取扱として、大きく 2 点を中心として検討した。第 1 の点は、EC の個人情報保護を特定の対象とする個別法を制定する必要性の有無について、第 2 の点は、包括的基本法たる個人情報保護法案及び現在存在する自主規制システムによる EC における個人情報保護の可能性について、である。そして、第 1 の点につき、現実社会と異なる EC の種々の特性から、個別法を必要とするとの見解を示し、第 2 の点については場面により EC では不十分性が生じることから対応策が必要であることを示した。

以上のような私見については、批判も予想されるところである。

20 世紀後半に至るまで殆どが現実社会でのみ行われてきた契約による商取引が、インターネットという技術の発達によりサイバースペースをも舞台に繰り広げられるという現実を、いかに捉えるか。議論の焦点はこの点にある。近時の技術革新は目まぐるしく、追いつくことはおろか、変化を認知することすら困難となっている。かかる現実に直面し、それでもなお憲法 13 条が保障する人格的自律権を実質的に確保するには、いかなる手段が必要か。結論は容易には出ない。

本格的な Web サービス時代は数年で訪れるであろう。回復困難性というプライバシー権の性質に鑑みると、悠長に構えて時代の到来をただ待つべきでなく、現段階でルールを検討し構築しておく必要がある。そして、EC の特性に考慮した最低限のルールを法で定めることが、契約における C 消費者の支援という観点からも、また有用性の高い EC の安定的な発展という観点からも、望ましい。すなわち、新たな時代に直面し、かつて経験したことのないほどの大きな変化の中で、変化しない/すべきでない普遍的な価値を確保するために、法による技術中立的なルールの定立という手段を今一度評価すべきと考えるのである。私見においても、EC が契約関係であることから私的自治の原則が妥当すると考える点は、強調しておきたい。私的自治が十分に機能しないおそれが高いことに鑑み、最低限の環境整備を整える方向性を模索しているのである。

個人情報保護法案は、2002 年 12 月 13 日閉会の第 155 回国会において廃案となり、改変を加えた新法案が第 156 回国会に提出され成立に向けて再スタートを切る予定である。しかし、その精神及び保護すべき価値は変わらない。そして、人格的自律権を確保すべく自己情報コントロール権たるプライバシー権を全うするためには、権利主体たる国民が、自ら主体としての意識を持つ必要性があることも、付言しておく。

サイバースペースという主体性の確保が困難な世界で契約関係を築くということが、自己情報コントロール権ひいては人格的自律権確保の見地に鑑みていかなる問題を提起する

か。未だ不透明な点が多く、今後のさらなる議論に期待したい。

ただ、サイバースペース上の取引であっても取引による直接的且つ間接的効果は現実社会に生きている我々に帰属する、ということは明白である。

参考文献等

岡村久道・新保史生共著『電子ネットワークと個人情報保護―オンラインプライバシー法入門―』経済産業調査会（2002 年）
平野晋著『電子商取引とサイバー法』NTT 出版（1999 年）
高橋和之・松井茂記編『インターネットと法』有斐閣（1999 年）
長谷部恭男著『憲法学のフロンティア』岩波書店（1999 年）
野中俊彦他著『憲法Ⅰ（新版）』有斐閣（1999 年）
成田雅彦著『SOAP/WSDL/ebXML　web サービス・アプリケーション開発技法』ソフト・リサーチ・センター（2002 年）
高橋秀雄著『電子商取引の動向と展望』税務経理協会（2001 年）
林紘一郎・牧野二郎・村井純監修『IT2001 なにが問題か』岩波書店（2000 年）
内山晴康・横山経通編者『インターネット法－ビジネス法務の指針－（第 3 版）』社団法人商事法務研究会（2001 年）
岡村久道編著『インターネット訴訟 2000』ソフトバンクパブリッシング（2000 年）
岡村久道・近藤剛史著『インターネットの法律実務』新日本法規出版（1997 年）
岡村久道・近藤剛史著『インターネットの法律実務（新版）』新日本法規出版（2002 年）
西村総合法律事務所ネット・メディア・プラクティスチーム編著『IT 法大全』日経 BP（2002 年）
平野晋・牧野和夫著『判例国際インターネット法－サイバースペースにおける法律常識－』プロスパー企画（1998 年）
藤田康幸著『個人情報保護 Q&A』中央経済社（2001 年）
土谷喜輝等編『インターネットをめぐる米国判例・法律 100 選改訂版』ジェトロ（2001 年）
菊沢正裕他共著『情報リテラシー』森北出版株式会社（2001 年）
名和小太郎・大谷和子共著『IT ユーザの法律と倫理』共立出版（2001 年）
坂野直人著『情報セキュリティーの仕組みと対策』中央経済社（2002 年）
岡田仁志著『サイバー社会の商取引』国立情報学研究所監修（2002 年）
佐々木良一他共著『インターネット時代の情報セキュリティ』共立出版（2000 年）
田渕治樹著『国際セキュリティ標準』オーム社（2001 年）
Efraim Turban 等共著『E－コマース電子商取引のすべて（日本語訳）』ピアソンエデュケーション（2001 年）
サイバーロー研究会著『サイバースペース法』日本評論社（2000 年）
セコム株式会社サイバーセキュリティ研究会編『サイバーセキュリティ入門』東洋経済新報社（2000 年）
電子商取引推進協議会 ECOM 個人情報保護 WG『EC で取り扱われる個人情報に関する調査報告書（ver.4.0）』（2002 年）
電子商取引推進協議会 ECOM 国際連携グループ『海外における EC 推進状況調査報告書 2001』（2002 年）
根田正樹共著『Ｑ＆Ａインターネット・電子商取引の法務と税務』ぎょうせい（1999 年）
Bradley Dunsmore 等共著『実践インターネットセキュリティ（日本語訳）』ＢＮＮ（2001 年）
堀部政男「電子商取引とプライバシー」ジュリスト 1183 号 77 頁
牧野和夫「アメリカ法務最前線(38)電子商取引の現状について(9)個人情報の保護に関する法的問題について」国際商事法務 Vol.27No.7、840 頁
牧野二郎「ネットワークと個人情報」法律時報 896 号 19 頁
司会・内田貴「座談会・電子取引法制度整備の課題」ジュリスト 1183 号 2 頁
多賀谷一照「個人情報保護と電子通信事業」ジュリスト 1190 号 64 頁
村千鶴子「個人情報利用取引に関する被害の実情」ジュリスト 1114 号 69 頁
清野幾久子「個人情報利用取引と個人情報保護制度」ジュリスト 1114 号 75 頁
神田秀樹「電子化時代の法整備と民事法」ジュリスト 1215 号 16 頁
松本恒男「消費者法と個人情報保護」ジュリスト 1190 号 52 頁
阪本泰男「サイバー社会の課題と展望」ジュリスト 1117 号 143 頁
内閣官房 IT 担当室「IT 基本法の概要」ジュリスト 1195 号 77 頁
弥永真生「電子取引と EU 諸国の取組み」ジュリスト 1183 号 136 頁
曽野裕夫「電子取引の法的基盤整備」ジュリスト 1183 号 145 頁
財団法人インターネット協会　http://www.iajapan.org/
総務省　http://www.soumu.go.jp/
経済産業省　http://www.meti.go.jp/

EDI 推進協議会　http://www.ecom.jp/jedic/
財団法人日本情報処理開発協会 JIPDEC　http://www.jipdec.jp/
電子商取引推進協議会 ECOM　http://www.ecom.jp/index.html
アスキーデジタル用語辞典　http://download.desk.ne.jp/win/3/00031/4063.html
首相官邸情報通信技術（IT）戦略本部　http://www.kantei.go.jp/jp/singi/it/index.html
先端 IT 研究・プロダクト情報　『アメリカ連邦政府の先端 IT 研究と成果の商用化に関する情報』
http://www2.gateway.ne.jp/~h_tada/main.html
日本商工会議所　http://mark.cin.or.jp/
サイバービジネス協議会　http://www.ejf.gr.jp/
日本工業規格　http://privacymark.jp/
@IT　http://www.atmarkit.co.jp
東京地判昭和 39 年 9 月 28 日判例時報 385 号 12 頁『宴のあと事件』
大阪高判昭和 42 年 12 月 25 日判例タイムズ 218 号 226 頁
浦和地決平成 11 年 3 月 9 日判例タイムズ 1023 号 272 頁
東京地決平成 13 年 10 月 29 日判例時報 1765 号 18 頁
岡本久道・平野晋・夏井高人「サイバー法とは何か？」判例タイムズ 984 号 71 頁
平野晋・相良紀子「解説『Zeran 対 AOL』事件」判例タイムズ 985 号 64 頁
平野晋「ユーザーの名誉毀損行為に対する ISP の民事責任（上）」判例タイムズ 1002 号 38 頁
平野晋「ユーザーの名誉毀損行為に対する ISP の民事責任（下）」判例タイムズ 1003 号 81 頁
東京地判平成 2 年 8 月 29 日判例タイムズ 751 号 161 頁
東京地判平成 3 年 3 月 28 日判例タイムズ 766 号 232 頁
東京地判平成 10 年 1 月 21 日判例タイムズ 1008 号 187 頁
東京高判平成 10 年 2 月 26 日金融法務事情 1526 号 59 頁
最判昭和 50 年 2 月 25 日民法判例百選 II [3]12 頁
最判平成 7 年 11 月 30 日重版平成 7 年商法[1]79 頁
東京地判平成 9 年 5 月 26 日判例時報 1610 号 22 頁
東京高判平成 13 年 9 月 5 日　http://courtdomino2.courts.go.jp/kshanrei.nsf/
東京地判平成 11 年 9 月 24 日判例時報 1707 号 139 頁
岡村久道「ニフティ電子ダイレクトメール仮処分決定について」判例タイムズ 1041 号 73 頁

Charles Fried : *Privacy*　77 Yale Law Journal 475 (1968)
Impact of E-Commerce on the Economy　The Robert Emmett McDonough School of Business at Georgetown University (1999)　http://www.msb.edu/faculty/culnanm/ec/Briefings/chanwf.htm
Lawrence Lessig : *Code and other laws of cyberspace*　Basic Books (1999)
Mark Rotenberg : *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*　2001 Stanford Technology Law Review 1 (2001)
http://stlr.stanford.edu/STLR/Articles/01_STLR_1/
Developments in the Law : The Law of Cyberspace -IV.Internet Regulation Through Architectural Modification : The Property Rule Structure of Code Solutions-　Harvard Law Review 112. Issue No.7 (student-authored) (1999)　http://www.harvardlawreview.org/issues/112/7_1634.htm
Steven Hetcher : *Changing the Social Meaning of Privacy in Cyberspace*　Harvard Journal of Law & Technology Volume15, Number1 Fall2001 (2001)
http://jolt.law.harvard.edu/articles/pdf/15HarvJLTech149.pdf
David Bender; Danice M. Kowalczyk : *Avoiding Intellectual Trespass in the Global Marketplace: Encryption & Privacy in E-Commerce*　Virginia Journal of Law and Technology SYMPOSIUM2000-VOL.5, ISS.2 (2000)
http://www.vjolt.net/vol5/symposium/v5i1a2-Bender_Kowalczyk.html
Jennifer Bresnahan : *Personalization, Privacy, and the First Amendment:A Look at the Law and Policy Behind Electronic Databases*　Virginia Journal of Law and Technology　FALL2000-VOL.5, ISS.3 (2000)　http://www.vjolt.net/vol5/issue3/v5i3a08-Bresnahan.html
U.S. Department of Commerce : *Digital Economy 2002* (2002)
http://www.esa.doc.gov/508/esa/DIGITALECONOMY2002.htm
John E.Blacker,Jr; R Nathan Randall : *Liability in the U.S. for Release of Private Information on e-Commerce Web Site*s 国際法務戦略 Vol-X.10　18 頁

Richard S.Taffet; Gabriel M.Nugent : *Privacy Protection at Internet Activities* 国際法務戦略 Vol-X .10 37 頁
欧州連合 EU http://europa.eu.int/index_en.htm
IST http://www.cordis.lu/ist/home.html
OECD http://www.oecd.org/
欧州評議会 http://conventions.coe.int/
TRUSTe http://www.truste.org
BBBOnlineR Privacy Program http://www.bbbonline.org/businesses/privacy/index.html
OPA http://www.privacyalliance.org/
アメリカ商務省 http://www.export.gov/
The John Marshall Law School http://www.jmls.edu/
FTC http://www.ftc.gov/
United States District Court, Southern District of New York http://www.nysd.uscourts.gov/
DoubleClick Inc. http://www.doubleclick.com/
THOMAS Legislative Information on the Internet – U.S. Congress on the Internet http://thomas.loc.gov/
マイクロソフト社 http://www.microsoft.com/japan
W3C http://www.w3.org/
In re DoubleClick Inc. Privacy Litigation, 00 Civ. 0641, 154 F. Supp.2d 497 (S.D.N.Y., March 28, 2001) http://www.nysd.uscourts.gov/courtweb/pdf/D02NYSC/01-03797.PDF
CompuServe Inc. v. Cyber Promotions, Inc. , 962 F. Supp. 1015 (S.D.Ohio February 3,1997) http://www.jmls.edu/cyber/cases/cs-cp2.html
In re GeoCities, Inc., 63 Fed. Reg. 44624 (August 20,1998)
Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case -Commission Establishes Strong Mechanisms for Protecting Consumers' Privacy Online- http://www.ftc.gov/opa/1998/9808/geocitie.htm
Cubby Inc. v. CompuServe Inc., 776 F. Supp. 135 (S.D.N.Y. October 29,1991) http://www.jmls.edu/cyber/cases/cubby.txt
Stratton Oakmont, Inc. v. Prodigy Service, 23 Media L. Rep. (BNA) 1794, (N.Y. Sup. Ct. May 24,1995) http://www.jmls.edu/cyber/cases/strat1.html
Zeran v. America Online, Inc., 958 F.Supp. 1124 (E.D. Va. March 21,1997) http://www.jmls.edu/cyber/cases/zeran.html

謝辞

本稿執筆に当たっては、非常に多くの方から御協力を頂きました。特に、御多忙にもかかわらず筆者の拙文を熱心に読み御指導にあたって下さった指導教官の宇賀克也教授（東京大学大学院法学政治学研究科教授）、東京大学法学部生時代から筆者を温かく導いて下さった長谷部恭男教授（東京大学大学院法学政治学研究科教授）、12 頁の参考図の提供を始めインターネット及びコンピューター技術に不透明であった筆者に技術的サポートをして下さった木村吉博氏（電子商取引推進協議会 ECOM 研究員・東京大学大学院新領域創世科学研究科博士課程）には、深く感謝の意を表します。また、東京大学大学院法学政治学研究科において共にリサーチ・研究活動に精進した友人たちを始めとする数多くの友人、筆者をいかなるときも支えてくれる家族に、この場をもって心より感謝致します。