ソーシャル・メディアの発展と個人情報保護を中心とした運営責任

内　布　　光

目　次

Ⅰ　はじめに

近年のソーシャル・メディアの発展には目覚ましいものがあり、フェイスブック（Facebook）[1)]などにより手軽に情報交流ができるようになった半面、ツイッター（Twitter）による情報漏えいや電子掲示板による中傷誹謗などが社会的な問題となっている。

このソーシャル・メディアという言葉についての正式な定義はないが、IT用語辞典“e-Words”[2]によれば「インターネット上で展開される情報メディアのあり方で、個人による情報発信や個人間のコミュニケーション、人の結びつきを利用した情報流通などといった社会的な要素を含んだメディアのこと」としている。つまり、インターネットを経由した個人と個人、個人と組織、組織と組織の間の情報交流それ自体が一種のコミュニティとなり、それが社会に広く浸透することにより、社会的な影響力を持つようなメディアといえる。

特に、インターネットを利用した個人間の情報発信・交流の場としてのソーシャル・メディアは、フェイスブックなどに代表されるソーシャル・ネットワーキング・サービス（略称「SNS」）[3]として発展・普及してきた。世界的に数多くの人々がSNSを手軽に利用できるようになったことにより、これが「アラブの春」[4]において大勢の市民によるデモの連絡手段となったように、重要かつ新たなメディアとしての地位を確立するに至っている。

一方、SNSに代表されるソーシャル・メディアは、その使い方によっては益にも害にもなり得る。ソーシャル・メディアを利用して発信・交流される情報は、ありとあらゆる内容・種類のものが含まれ、かつ膨大な量であるからである。

このような膨大な量の情報は、欧米では、一般にビッグ・データ（Big Data）[5]と呼ばれている。このビッグ・データとは、もともと情報通信、特にインターネットの発達にともなって爆発的に増大した構造化されていない莫大な量のデータのことをいう。このように膨大な量の情報のことを欧米ではビッグ・データと呼ぶのに対して、わが国では、ビッグ・データの言葉は殆ど使われず、一般的に「ライフ・ログ（Life Log）」[6]の言葉が用いられている。そして、様々な局面で発生した巨大な情報の集まりであるビッグ・データ又はライフ・ログを分析することで、ビジネス傾向の特

定、病気の予防、犯罪の対策などに役立てることができるといわれている。

ソーシャル・メディアとビッグ・データ又はライフ・ログとの関係は、いわば「ニワトリと卵」の関係に似ているが、いずれにせよソーシャル・メディアの発展とともに、ビッグ・データ又はライフ・ログと呼ばれる膨大な量の情報が発生し、それが更にソーシャル・メディアによって流通することなどにより、通信の秘密、個人情報保護、知的財産保護などの観点から新たな問題が生じ、深刻化している。本稿では、この関係から生じる問題のうち個人情報保護を中心とした事業者責任の問題に焦点を絞り考察する。

Ⅱ　ソーシャル・メディアとライフ・ログ

1　ソーシャル・メディアの意義

ソーシャル・メディア、中でもフェイスブックに代表される SNS は、友人・知人間のコミュニケーションの場や新たな人間関係を構築する場を提供する会員制のサービスである。つまり、主として個人間の情報交流等がインターネット上で自由に行えるようになっているコミュニティ型のウェブサイト[7)]である。

従来からインターネット上の情報発信や交流の手段（場）として、電子メール、電子掲示板、ツイッター、ブログなどがあり、これらも広い意味ではソーシャル・メディアとして捉えられている。しかし、これらは、いずれも基本的には「1 対 1」ないしは「1 対不特定多数」に対して一方的に情報を発信しっぱなしという、いわばワンウェイ型のメディアとなっている。もちろん、この発信に対して返信したり書き込みしたりすることはできるが、これも基本的には「1 対 1」で行われる。

そして、このようなインターネットを利用した情報交流の場は、いわば仮想空間となっており、そこでは情報発信者の顔が見えないという特質を

有している。この特質から正体不明者として、あるいは他人に成りすますことにより何でもすることができ、いわば無法地帯となりやすい。例えば、名誉棄損やプライバシー侵害を惹き起こすような他人を中傷・誹謗する情報の発信、著作権侵害情報の垂れ流しや他人に成りすました詐欺等の犯罪などの問題が、インターネット社会の脆弱性やマイナス面として、従来から指摘されていた。

現在、ソーシャル・メディアは、インターネットを利用したICT[8)]サービスの主力をなすものであるので、これらの問題を避けることができない。しかし、これらの問題が生じやすいのは、ツイッター、ブログ、電子掲示板などのワンウェイ型メディアによる場合が圧倒的に多い。なぜなら、これらのソーシャル・メディアは、その殆どが会員制（閉鎖型）でなく、誰もが自由・勝手に情報を発信できるという特徴を有する、いわば開放的なメディアだからである。これらのメディアが仮に会員制をとっている場合であっても、そこでは無名や匿名での情報発信を許している。つまり、これらのワンウェイ型メディアでは、当該サービスの提供・運営者（プロバイダ）は、単に、情報交流の場として当該メディアを提供しているだけであって、常時、当該メディア上の情報内容について監視し、必要に応じてその内容を修正・削除するなどの管理行為を一切行っていない。従って、これらのワンウェイ型メディアを利用した情報交流の場における秩序維持は、基本的には各利用者のモラル等[9)]に依存している。

これに対して、フェイスブックに代表されるSNSは、コミュニティ型すなわち双方向の対話型（インタラクティブ型）のメディアという特徴を有している。つまり、SNSは、もともと友人・知人間のコミュニケーションを円滑にする手段や場として開発・提供されたものであり、素性がはっきりした利用者同士で安心して情報交流ができることを目的としている。従って、このSNSは、必然的に会員制を採用し、会員以外の者が勝手に、その情報交流（コミュニケーション）の場に立ち入れないという特徴を有

する、いわば閉鎖的なメディアである。そして、SNS は「友達の友達は、友達」的に普及・拡大していく。現在でも、原則として実名での会員登録しか受け付けないことから、自ずと利用者同士の自制が働きやすい。この結果、このメディアを利用した情報交流の場においては、ワンウェイ型メディアに比べてきちんとした秩序・統制がとれている。

このような利点をもつインタラクティブ型メディアである SNS は、従来の主流であったツイッター、ブログ、電子掲示板などのワンウェイ型メディアに代わり、今では、ソーシャル・メディアの中核的地位を占めつつある。

2　ライフ・ログの意義

ソーシャル・メディアの発展・普及に伴い、ライフ・ログと呼ばれる多種多様な膨大な量の情報が流通している。もともとライフ・ログは、この言葉（英語）が表しているとおり、人間の生活・行動（life）に関する記録（log）であるから、ソーシャル・メディア上にも膨大な量のライフ・ログが溢れている。そして、このライフ・ログという膨大な量の情報を分析することによって、様々なビジネス・チャンスに結びつけることも可能である。しかし、一方では、これら情報と諸権利との関係が不明確なために、新規ビジネスの展開が円滑に進まないなどといった課題も生じているので、ライフ・ログと諸権利との関係を整理することが求められている。

そこで、総務省では「利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会」を設置して、このライフ・ログについても検討しているので、以下、その内容を簡単に紹介する。

なお、この研究会は、新たな ICT サービスの登場や新技術を活用した情報の流通などにより、通信の秘密、個人情報保護、知的財産保護などの観点から新たな課題が生じたり、深刻化したりしているという背景から設置されたものである。

そして、この研究会は、平成21年8月に「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会」第一次提言[10]を公表した。この第一次提言では、ライフ・ログの定義付けやICTサービスにおける活用の実際などについて検討しているが、ライフ・ログ活用サービスの法的課題の検討については積み残していた。

そこで、更に個人情報保護法やプライバシー等との関係から検討を重ね、平成22年5月に「利用者視点を踏まえたICTサービスに係る諸問題に関する研究会」第二次提言[11]を公表した。この第二次提言では、特に、ライフ・ログ活用サービスに関する検討結果を「より信頼されるサービスに向けて（配慮原則の提言）」としてとりまとめ、併せてディープ・パケット・インスペクション技術[12]を利用した行動ターゲティング広告[13]についても検討している。

なお、この第二次提言で提言している「配慮原則」とは、具体的には以下の6項目である。

①広報、普及・啓発活動の推進
②透明性の確保
③利用者関与の機会の確保
④適正な手段による取得の確保
⑤適切な安全管理の確保
⑥苦情・質問への対応体制の確保

3　ライフ・ログの法的性質

従来から、ICTサービスの中には様々な法的問題が包含されていることが指摘されていた[14]が、ソーシャル・メディアもインターネットを利用したICTサービスの一つであるから、この例外ではなく、幾つかの法的問題を抱えている。

そして、今日では、ソーシャル・メディアの世界規模での爆発的な普及

に伴い、インターネット上ではビッグ・データ又はライフ・ログと呼ばれる膨大な量の情報が流通している。

なお、ライフ・ログは、私たちの日々の生活（life）に関する様々な情報をいうので、ライフ・ログは、ビッグ・データの一部に含まれる。すなわち、ライフ・ログは、狭義では生活（life）に関する情報を指すが、通常、膨大な量の情報となっているので、広義にはビッグ・データの一部として捉えることができる。

また、ライフ・ログは、私たちの日々の生活（life）に関する様々な情報であるから、この中には当然のことながら、プライバシー情報や信用情報等などの個人情報を多分に含んでいることになる。

例えば、代表的な SNS であるフェイスブックについて見てみる。ここで公開されている情報の内容を見ると、当該利用者がまず登録しなければならない「基本データ」という情報としては、氏名、生年月日、性別、血液型のほか、職歴と学歴、住んだことのある場所、交際関係と家族、連絡先情報などがある。そのほかに当該利用者の宗教・信仰や政治観、その他好きなスポーツ・音楽、趣味・趣向などの情報も登録・公開することができるようになっている。これらの情報は、まさしくライフ・ログであり、かつ個人情報である。

なお、ここでいう個人情報とは、ひと言でいえば「特定人を識別できる情報」であり、個人情報保護法[15]2 条 1 項では、「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。」と定義している。また、EU では、一般に個人情報は「個人データ（personal data）」と呼ばれているが、個人情報保護法 2 条 4 項では、個人データは「個人情報データベース等[16]を構成する個人情報をいう。」と定義している。

このように個人情報は、特定人にかかわる一切の情報を指すから、この個人情報には、フェイスブックの「基本データ」として登録されるような情報から、いわゆるプライバシーに係る情報（プライバシー情報）や病歴・犯罪歴等の他人に知られたくない情報（センシティブ情報）、預金・ローンの金額や保有財産状況などの信用情報に至るまで、さまざまな内容・種類の情報が含まれている。

また、フェイスブックなどのソーシャル・メディア上では、世界中の何億人、何十億人ものライフ・ログが登録・発信・公開されているので、それらの膨大な量の情報がインターネットを介して世界中で流通していることになる。

そこで、これらのライフ・ログは、その利用のされ方によっては、社会全体にとっては利益になったり、情報主体（本人）にとっては不利益になったりする。例えば、ライフ・ログを行動ターゲッティング広告などに活用することにより新規ビジネスに結び付けることができるなど、社会・経済の発展に貢献させることもできるし、その一方では、それが不正に加工・処理され、利用等されたりすると、当該情報主体（本人）の名誉棄損やプライバシー侵害などの悪影響を及ぼすことにもなる。

Ⅲ　ICT サービス事業者と個人情報保護

1　ICT サービス事業者の意義

ソーシャル・メディア、中でもフェース・ブックなどの SNS では、世界規模で、多くの個人情報を含むライフ・ログなどの膨大な量の情報が流通しているが、SNS を含む ICT サービスを提供・運営している事業者（以下「ICT サービス事業者」又は単に「事業者」という）には、どのような法的責任が負わされているのであろうか。つまり、これらの事業者は、一般に、当該サービスの提供・運営等を通じて、各利用者のプライバシー

情報を含む個人情報を取り扱い、あるいは通信の秘密に触れる立場にあるから、何らかの法的責任を負っていると考えられる。

このことを検討する前に、まず、ICT サービス事業者とは何か、すなわち、どのような事業者を ICT サービス事業者というかについて見てみる。

そこで、ICT サービス事業者が提供しているサービス内容や形態（いわゆる事業内容）に着目して区分すると、大きくは次のとおり 5 つに分けることができる。もちろん、これらの事業者の中には、二つ以上のサービスを提供している事業者もある。

① 検索エンジン・ポータル事業者（例：Yahoo や Google など）
② 電子商店街（オンラインモール）事業者（例：楽天など）
③ SNS 事業者（例：Facebook など）
④ IPS 事業者[17]（例：NTT コミュニケーションなど）
⑤ 電話事業者、特にインターネットと接続している携帯電話事業者（例：NTT ドコモなど）

以上の事業者は、電気通信事業法（昭和 59 年法律第 86 号）で規定する「電気通信役務」[18]を提供している場合も多い。この場合は、同法の「電気通信事業者」に該当する。そして、この電気通信事業者に該当する事業者は、電気通信事業法による規制を受けることになるが、この規制については後述する。（「Ⅳ ICT サービス事業者の責任」参照）

2　日本における個人情報保護

わが国においては、ICT サービス事業者が、そのサービス（事業内容）を通じて個人情報を取り扱う（保有する）場合は、個人情報保護法により各種義務が課せられる。なお、この個人情報保護法は、いわゆる民間部門全体を適用対象とした法律であり、行政機関や独立行政法人等が保有する個人情報の保護については、この法律と同時に制定された別の法律[19]が適用される。

ところで、個人情報を取り扱っている民間部門は、病院、学校、銀行・保険・クレジット会社、スーパー・デパート等、様々な業種に分かれている。そして、これらの業種ごとに、それぞれが主として取り扱う個人情報の内容は、例えば、病院では病歴等の患者情報、学校では出席記録や成績などの生徒・学生情報、銀行では預金・ローンなどの金融情報などのように異なっている。

個人情報保護法は、このように多種多様の個人情報を取り扱っている民間部門の個人情報取扱事業者に適用されるため、おのずと同法で規定する内容も包括的で抽象的にならざるを得ない。例えば、「個人情報取扱事業者の義務」として、利用目的の特定（同法第 15 条）、適正な取得（同法第 17 条）、安全管理措置（同法第 20 条）、委託先の監督（同法第 22 条）、第三者提供の制限（同法第 23 条）[20]などを定め、「民間団体による個人情報の保護の推進」として、主務大臣による認定個人情報保護団体の認定（同法第 37 条）、苦情処理（同法第 42 条）、個人情報保護方針の作成・公表（同法第 42 条）などを定めている。また、同法第 56 条～第 59 条には罰則規定もあるが、この内容は、主務大臣からの勧告措置命令に違反した個人情報取扱事業者に対する 6 月以下の懲役または 30 万円以下の罰金（同法第 56 条）や主務大臣の報告徴収に従わない個人情報取扱事業者又は認定個人情報保護団体に対する 30 万円以下の罰金（同法第 57 条）など、いわば行政処分違反に関するものであり、個人情報保護に関する義務違反を直接罰するものではない。

このように個人情報保護法は、民間部門の業種（セグメント）ごとに個人情報の取扱いが異なっていることを前提に、民間部門全体を適用対象として制定されているので、その内容は包括的・抽象的であり、この法律の適用を受ける民間部門の各事業者は、同法をそのまま個人情報保護に関する具体的な行動規範とすることができない。

一方、民間部門では、一般に業種ごとに事業者団体（いわゆる業界団

体）が結成・組織されている。そして、これらの業界団体の中には、個人情報保護法第 37 条に基づく「認定個人情報保護団体」の認定を受けている団体[21]もあり、当該業種における個人情報の取り扱い実態に則した「個人情報保護ガイドライン」等を制定するなど、個人情報保護の推進活動をしている団体もある。このように個人情報保護について、民間部門では実質的には業界団体を中心とした自主規制[22]により取り組んでいる。

ICT サービス事業者の事業内容には、検索エンジン・ポータル事業、SNS 事業、電話事業などがあるが、それぞれの事業内容によって、その取り扱う個人情報の内容・量、取り扱いの形態・関与度なども異なっている。そこで、各事業者は、自らの事業内容に合わせて、適切でかつ実施可能な「個人情報保護コンプライアンス・プログラム」[23]を策定・実施して、個人情報保護に取り組むことが期待されている。

3　欧米における個人情報保護

ICT サービス、中でも SNS は、ビッグ・データ又はライフ・ログと呼ばれる個人情報を含む膨大な量の情報を世界規模で流通させている。このようにわが国と外国間で個人情報を含む情報の交流が行われているので、個人情報保護は、各国が統一的に取り組むべき国際的な課題といえる。しかし、現在のところ、これに関する国際条約は存在せず、基本的には、それぞれの国の取り組みに任されている。

わが国では、前述のとおり、個人情報保護法等を制定し、併せて民間レベルでは業界ガイドラインの制定やプライバシーマーク制度[24]などにより取り組んでいる。これに対して日本以外の国では個人情報保護にどのように取り組んでいるのであろうか。

ここでは、欧州と米国における個人情報保護への取り組み状況を概観してみる。なお、欧州については、欧州の主要国の殆どが加盟（現在 27 カ国）している欧州連合すなわち EU（European　Union）を中心にとりあ

げる。

(1)　欧州各国（EU）

欧州各国における個人情報保護への取り組みの歴史は古いが、EU としての統一的取り組みは、1995 年 11 月に「個人データ保護に関する指令（Directive　95/46/EC）」[25]の採択から始まった。なお、欧州では、個人情報のことを「個人データ（personal data）」と呼んでいる。

この個人データ保護指令（以下「1995 年指令」という）では、特に、第三国への個人データの移転（transfer of personal data to third countries）に関して、第 25 条（Article 25）に「加盟国は、十分なレベルの保護を確保（ensure an adequate level of protection）していない第三国には、個人データを移転してはならない」旨規定していた。ここでいう「第三国」の中には、当然に日本も含まれる。

この 1995 年指令は、わが国にも大きなインパクトを与え、日本国内における個人情報保護の機運を急速に高め、前述の個人情報保護法制定等にもつながったという経緯がある。そして、この 1995 年指令第 25 条に対応するため、わが国の事業者は、加盟国から標準契約条項（Standard Contract Clauses）又は BCR（Binding Corporate Rule）についての承認を得ることで、EU 域内から日本への個人データの移転を可能としている。

その後、EU では、個人データ保護に関係する幾つかの指令（例えば、2002 年 7 月 12 日の「電子通信分野における個人データ処理及びプライバシー保護に関する指令」など）が出されている。このような「指令（Directive）」は、EU 加盟国に対して、その内容を国内法に反映することを義務付ける効力を有しているが、加盟国は、国内法の事情に合わせて反映させるために、結果的には、各国の法規制はバラバラで統一されていない。

そこで EU は、その後の個人データの取扱い環境の変化に合わせて、各加盟国の個人データ保護についての法規制を統一するため、2012 年 1 月

25 日に個人データ保護に関する提案（Commission Proposals on the data protection）として「規則（Regulation）」[26]を公表した。なお、今回、EU が提案（propose）した「規則」は、その内容が加盟国に対して従前の「指令」よりも強い拘束力を有することになる。

今回の規則のうち、事業者にとって直接関係する主要な事項は、次の 3 点である。

① データ主体（個人）の権利の拡大（第 17 条及び第 18 条関係）

② 処理のセキュリティ（Security of processing）（第 30 条関係）

③ 通報等の義務化（第 31 条及び第 32 条関係）

特に、①については、データ主体（個人）に対して「忘れてもらう権利（Right to be forgotten and to erasure）」（第 17 条）や「データ・ポータビリティに関する権利（Right to data portability）」（第 18 条）などの権利の拡大を図っている。

また、③については、「個人データ侵害に関する監督機関への通報（Notification of a personal data breach to the supervisory authority）」（第 31 条）や「個人データ侵害に関するデータ主体への通知（Communication of a personal data breach to the data subject）」（第 32 条）を義務付け、情報漏えいから 24 時間以内に監督機関に通報しない場合（第 31 条に違反した場合）は、200 万ユーロ・総売上の 20% の課徴金が課せられるなど、厳しい内容の罰則となっている。

(2)　米国

米国における個人情報保護は、連邦法等による法規制ではなく、基本的には民間部門での自主規制に委ねられている。

米国も EU の 1995 年指令第 25 条でいう第三国に該当するので、EU 域内から個人データの移転を受けるためには、同条でいう「十分なレベルの保護」を確保しなければならない。

そこで、米国商務省は、欧州委員会（EC）との間で、個人情報保護指令の遵守を確認する手続き、いわゆる「セーフ・ハーバー（safe harbor）」[27]を定めている。この要件として利用者への通知や選択肢の提供等が挙げられるが、これに参加する事業者へは、プライバシー保護プログラムへの参加や自主規制の開発、遵守状況の商務省への報告などの義務を負わせている。従って、米国の主要法人は、この「セーフ・ハーバー」に参加・遵守することで、EU 全域からの個人データの移転を可能としている。

なお、1995 年指令第 25 条による規制は、あくまでも EU 域内から第三国への個人データの移転を対象としたものであり、第三国から EU 域内への個人データの移入については何ら規制がない。

その後米国でも、近年のソーシャル・メディアの発展・普及に伴い、前述の日本の場合と同様に、そこで流通するビッグ・データ、中でもライフ・ログの活用による法的問題についての対応が必要となってきた。

そこで、米国連邦取引委員会（Federal Trade Commission：通称「FTC」）が 2009 年 2 月に発表した行動ターゲティング広告における自主規制の原則案を受けて、2009 年 7 月に、米国の 5 つの業界団体[28]が「共同ガイドライン（Self-Regulatory Principles for Online Behavioral Advertising）」を公表している。

この共同ガイドラインでは、以下の 7 項目を柱としている。

①教育の原則（消費者啓発の強化）
②透明性の原則（データ収集の公表）
③消費者管理の原則（選択肢の付与）
④データセキュリティの原則（安全性確保、データ保存期間の限定）
⑤内容変更の原則（変更時の事前同意取得）
⑥機密データの原則（児童、医療、金融等関連データの保護強化）
⑦ 説明責任の原則（執行状況の報告）

Ⅳ　ICT サービスと事業者の責任

1　個人情報流出等による事業者責任

ICT サービス事業者は、そのサービス提供に伴い個人情報を取り扱う場合が多いため、わが国における個人情報事業者の法的義務、民間部門における個人情報保護に関する自主規制などについて述べてきた。

近年、事業者が取り扱っている個人情報が紛失・流出し、ネット上で公開され、あるいは不正利用されたなどの事故又は事件を耳にすることが多い。このような事故・事件に巻き込まれた事業者は、その流出等により生じた損害について賠償責任（民事責任）を負うべきかが問題となる。

以下、個人情報流出等による事業者責任について検討する。

(1)　個人情報流出等は不法行為を構成するか

民法は、いわゆる不法行為として第 709 条に「故意または過失によって他人の権利又は法律上保護される利益を侵害した者は、これによって生じた損害を賠償する責任を負う。」と規定し、次条（同法第 710 条）では「他人の身体、自由若しくは名誉を侵害した場合又は他人の財産権を侵害した場合のいずれであるかを問わず、前条の規定により損害賠償の責任を負う者は、財産以外の損害に対しても、その賠償をしなければならない。」と規定している。

そこで事業者は、その取り扱っている個人情報の流出、不正利用等によって当該個人情報の主体が損害を被った場合、民法第 709 条によりその賠償責任を負わされる場合がある。このような個人情報の流出、不正利用等は、民法第 709 条でいう不法行為すなわち“他人の権利又は法律上保護される利益を侵害する行為”を構成する可能性があるからである。つまり、個人情報は、一般に当該情報主体（本人）のプライバシーや名誉等を化体した情報を包含している場合が多く、また個人情報保護法等で保護されて

いることを勘案すると、まさに、他人の権利又は法律上保護される利益（法益）に該当する場合もあり得る[29]からである。

しかし、個人情報保護法は、ある程度まとまった量の個人情報を取り扱う事業者[30]を適用対象として、個人情報の適切な取り扱いをさせるために規制しており、この規制によって、個々の個人情報の主体（本人）のプライバシー権等の権利又は法益の侵害を防ぐことにある。従って、個々の個人情報は、その内容等に照らして、民法第 709 条でいう“他人の権利又は法律上保護される利益（法益）”に該当するかを検討する必要がある。

そして、仮に当該個人情報が民法第 709 条でいう“他人の権利又は法律上保護される利益（法益）”に該当する場合であっても、故意又は過失による行為すなわち当該個人情報の流出、不正利用等があっただけでは不十分である。つまり、その不正利用等の行為（原因）により当該個人情報主体に損害が生じたという事実（結果）、すなわち不正利用等と損害との間には因果関係があることが必要である。

なお、当該個人情報の流出、不正利用等は、事業者自身でなく、実際にそれを取り扱っている担当者等の従業員や当該取扱業務の委託先によって行われる場合が多い。この場合の事業者の責任については後述する。

(2)　どのような損害が生じるか

個人情報の流出、不正利用等によって、実際に当該個人情報の主体（本人）に何らかの損害が生じる場合があるが、この場合、本人は、どのような損害を受けるのであろうか。

事業者が取り扱っている個人情報が、プライバシー情報、機微情報（センシティブデータ）、信用情報など本人のプライバシー・名誉・信用等に係る情報によって構成されている場合は、それが流出等すると、直ちに、本人に対するプライバシー[31]や名誉などの権利又は法益の侵害に結びつく可能性は高い。そして名誉棄損や信用失墜等がされると、本人は、それに

よって社会的地位等を失うほか精神的苦痛を被ることが多い。これらの信用回復費用や精神的苦痛などは、一般的に、民法第 710 条の財産以外の損害として認識できる。

しかし、これ以外の情報、例えば、氏名、年齢、学歴・職歴、血液型、出身地などのフェイスブックの基本データに該当するような情報だけで構成されている個人情報については、それが単に流出しただけでは、直接、当該個人情報主体（本人）の権利や法益を侵害することにはならないし[32)]、また、それにより損害が生じるとは限らない。通常、このような基本データに該当する情報は、様々な通知や連絡等のコミュニケーションをとるための不可欠の情報であり、一般に、本人の利益に資するように利用されることが予定されているからである。

そして、フェイスブックなどのソーシャル・メディア上では、本人がこれらの情報を積極的に公開している場合も多々見かけられるが、この場合、これらの情報が広告等のダイレクトメールにも容易に利用されることを覚悟すべきである。なお、これらの情報といえども、スパムメール（迷惑メール）等の一般に嫌がられる行為に不正利用等されると、本人に対して精神的苦痛等を与えるなどの損害が生じることになる。

(3)　個人情報の流出等と損害の関係

事業者は、その保有する個人情報をコンプライアンス・プログラム等により厳格に管理しているので、通常では、個人情報の流出等は生じないはずである。そして万一、それが流出したとしても、その事実を誰も知らなければ、直ちに当該個人情報の主体（本人）に損害が生じることはない。仮に本人に損害が生じるとしたら、流出した当該個人情報を誰か（第三者）が公開・不正利用等して、当該個人情報主体（本人）の権利又は法益を侵害した場合であろう。また、判例及び従来の通説は、不法行為に基づく損害賠償の範囲を定めるときは、債務不履行による損害賠償の範囲に関

する民法第 416 条の規定が類推適用される[33]ので、当該不法行為と損害との間には相当因果関係[34]が必要とされている。これに対して「民法第 416 条が相当因果関係を定めているとの理解も、また同条を不法行為に類推適用する解釈も、ともに疑問がある。」[35]との批判もある。

このように個人情報の流出等により当該個人情報主体（本人）に損害が生じる場合を見ると、通常、流出した個人情報が公開や不正利用等され、その結果、本人の権利又は法益が侵害されることにより損害が生じるという一連の事実の流れが存在する。この一連の事実の流れの中で、個人情報の流出と公開や不正利用等とが同時に行われる場合もあるが、これにより本人の権利又は法益が侵害されたとしても、必ずしも損害が発生するとは限らない。この一連の事実の流れの中で、それぞれ前後する事実の関係、すなわち個人情報流出と公開・不正利用等との関係、公開・不正利用等と権利・法益侵害との関係、権利・法益侵害と損害発生との関係、という関係は、前の事実を原因として後の事実が結果として生ずるという事実が連続して存在しなければならない。つまり、「あれがなければ、これはない」という意味での本来の因果関係を「事実的因果関係」というが、それぞれ前後する事実の間には、この事実的因果関係が必要である。

なお、民法第 416 条は、損害賠償の範囲、すなわち「どこまでの損害を賠償させるべきか」についての規定であり、伝統的な通説は「相当因果関係に立つ損害とは、当該債務不履行によって現実に生じた損害のうち、当該場合に特有な場合を除き、かような債務不履行があれば一般に生ずるであろうと認められる損害だけ、という意味である。」[36]としている。

以上のことから、個人情報の流出（最初の原因）により直ちに本人に損害（最終結果）が生じるとは限らない。そこで、事業者が民法第 709 条の不法行為責任（損害賠償責任）を問われる場合は、事業者の故意又は過失により、その保有する個人情報が流出等し、その結果、当該個人情報主体（本人）の権利又は法益を侵害し損害を与えたという一連の事実の間には

相当因果関係が認められるときである。しかし、この因果関係の立証責任は損害を被った本人にあるとされているので、実際には、この立証のハードルはかなり高いものがある。

(4)　従業者等の行為に対する事業者責任

個人情報の流出等により当該個人情報主体（本人）に損害が生じて、民法第 709 条の不法行為が成立した場合であっても、実際の不法行為者は事業者自身でなく、当該事業者の業務として個人情報を実際に取り扱っている従業者など（以下「従業者等」という。）であることが多い。

また、ICT サービスでは、その特質上、当該事業者、その従業員及び委託先以外の第三者（例えば、ハッカーや不正利用者など）が個人情報の不正利用等を行うこともあり得る。このように第三者が事業者側から流出した個人情報を不正利用等の不法行為をした場合において、仮に、事業者にその流出につき過失があったとしても、その流出と第三者の不法行為の間には相当因果関係を認めることはできない。この場合、不法行為の責任を問われるは、事業者でなく、当該不法行為をした第三者である。

なお、個人情報保護法は、事業者に対して従業者等の監督義務（同法第 21 条及び第 22 条）を負わせているが、この義務違反に対する罰則（刑事責任）や損害賠償責任（民事責任）についての規定を何ら置いていない。このことから仮に、従業者等の過失等により個人情報を流出等しただけでは、個人情報保護法上、事業者は、何ら責任を問われることはない。

では、事業者が保有している個人情報につき、従業者等が当該個人情報主体（本人）に損害を与えた場合は、直接、事業者自身が、その賠償責任を負わなければならないのだろうか。

民法は、使用者責任として「使用者は、被用者がその事業の執行について第三者に加えた損害を賠償する責任を負う」（第 715 条第 1 項柱書）としているが、この場合でも、「使用者が被用者の選任及び事業の監督につ

き相当の注意をしたとき、又は、相当の注意をしても損害が生じたときは、この限りでない」（同条同項但書）と規定している。

従って、従業者等（被用者）が個人情報の取扱業務中に、当該個人情報主体（本人）に損害を加えた場合、事業者（使用者）は、原則として、その損害賠償の責任を負わなければならない。しかし本人に損害を与えた場合であっても、事業者が従業者等に対して、個人情報の取扱いについて適切な手順を定め、必要な教育を施すなどの相当の注意をしていたときは、民法第 715 条第 1 項但書によって事業者は損害賠償責任を免れる。

事業者が、個人情報保護コンプライアンス・プログラムを策定し、これに基づき社内規程や管理体制の整備、従業者等に対する教育・監査などを実施していることは、民法第 715 条 1 項但書でいう「相当の注意」をしていることを証明するための有力な材料（証拠）となる。

2　個人情報流出等以外の事業者責任

ICT サービス事業者は、そのサービス提供に伴い個人情報を取り扱うことが多いので、その保護義務やその流出等による損害賠償責任を負わなければならない場合があるが、これ以外に、どのような法的義務及び責任を負わなければならないのだろうか。

ICT サービスの内容や形態は、前述したとおり様々であるので、そのサービス内容・形態によって事業者の法的義務等が異なるが、電気通信事業法でいう電気通信役務事業者に該当する場合が多い。そこで、電気通信事業法上の事業者義務を明らかにする。次いで、ICT サービス提供に伴う責任として、このサービスの特質から生じるリスクに着目して、SNS を中心としたソーシャル・メディアに焦点を当てて、事業者責任を検討する。この場合、その提供するサービスにおける事業者の役割・立場によって、通常、法的責任が異なってくることが考慮する必要がある。

(1)　電気通信事業法上の義務

ICT サービス事業者は、そのサービス内容・形態によって電気通信事業法の規制を受ける電気通信事業者に該当する場合が多い。同法では、電気通信事業者に対して、どのような法的義務を負わせているのであろうか。

まず、電気通信事業法では、電気通信事業者が他人の通信を媒介し、あるいは電気通信設備を提供するサービスを取り扱っているという立場にあることから、その取扱中に係る通信は検閲してはならず（同法第 3 条)、通信の秘密は侵してはならない（同法第 4 条）と規定している。

また、電気通信事業者は、電気通信役務の提供について、原則として不当な差別的取扱いをしてはならない（同法第 6 条）が、この一方では、天災地変その他の非常事態が発生したときなどは、電気通信事業者は、災害救援、秩序の維持、公共の利益のため緊急に行うことを要するなどのために必要な事項を内容とする通信を優先的に取り扱わなければならない（同法第 8 条第 1 項）などの義務が負わされている。

電気通信事業法では、以上のとおり電気通信事業者が負うべき義務については規定しているが、電気通信事業者の責任については、特に、具体的な規定を置いていない。

(2)　サービスの特質による法的リスク

ICT サービスのうち電話や電子メール（同報送信を除く）などの電話・通信サービスは、通常、特定の利用者同士が「1 対 1」で対話（通信）をしているので、そのサービスの事業者（例えば、電話会社など）は、いわば当該通信の手段あるいは道具を利用者側に提供しているだけである。

このような電話や電子メールの内容は、通信の秘密に該当するため、電気通信事業法による検閲等の禁止などの規制がかかるので、いわゆるブラックボックスとして取り扱われている。従って、意図的に盗聴等を行わない限り、どのような内容の通信が行われているかなど、一切、わからない。

例えば、電子メールの内容が、仮に特定の送信先を中傷誹謗するものであったとしても、その電子メールが何らかの理由で当該送信先以外の不特定多数の第三者に知れ渡らない以上、すぐには名誉棄損・信用失墜等を論じる必要はない。

しかし、このような電子メール等とは異なり、今日のSNSなどソーシャル・メディアにおいては、不特定多数に対して情報が発信され、交流される形態となっているものも多い。そこで、一旦、これらを利用して違法情報（例えば、違法コピーした著作権侵害情報）や有害情報などが発信されると、その情報内容に応じた損害や法的問題が生じる。ソーシャル・メディアもインターネット上のサービスという特質から、特に、違法ドラッグ・銀行口座売買などの犯罪や青少年の非行の温床にもなりやすいので、警察庁のサイバー犯罪対策や地方自治体のネットパトロール[37]などにより、犯罪防止に努めている。これらは基本的に利用者の問題（犯罪など）であるが、当該事業者は、犯罪捜査・予防への協力等の名目で当局から発信者情報の開示請求を受ける場合があり得る。この場合、事業者は、この発信者情報の開示請求にどのように対応するかが問題となる。

また、電子商店街（オンラインモール）事業者は、そのモールで取り交わされる電子商取引について、単なる売り手と買い手の取引の場を提供しているだけの場合、又は、ある程度当該取引の仲介まで行っている場合、売り手の代理をしている場合など、当該取引への関与度によって、当該取引に係る法的リスク（特に、取引法上の責任）は大きく異なってくる。

なお、SNS事業者は、オンラインモール事業者に似ている。すなわち、SNSは、オンラインモール事業者が提供しているオンラインモール（電子商店街）のように、会員間のコミュニケーション（情報交流）の場を提供している。従って、SNS事業者が、会員間の情報交流にどの程度関与しているかによって、事業者として負うべき法的責任は異なる。

(3)　事業者のサービス上の役割・立場

ICT サービスが様々な形態・内容で提供されるようになったのに伴い、そのサービスを提供している事業者（運営管理者を含む。以下「事業者等」という。）の責任を追及する裁判事例[38]も増えてきた。このような事業者等の法的責任を論ずる場合、当該事業者等が、当該サービスにおいて、どのような役割又は立場であるかが問題とされるが、これには以下のとおり大きくは二つに分かれる。

一つは、事業者等が提供するサービスを利用して取り交わされる情報について、自由にコントロールできる役割又は立場にある場合である。すなわち、事業者等が、そのサービス上の情報を制限でき、加工し編集でき、削除することもできるという運営・管理の権限を有している場合である。このような事業者等は、いわば雑誌出版社のような立場である。例えば、雑誌出版社は、出版する雑誌についての企画・編集に関する一切の権限を持っている。つまり、自由に企画した内容に従って様々な記事（情報）を取捨選択し、それを修正・加工するなどして編集している。

もう一つは、事業者等には当該サービス上の情報を処理・加工・削除するなどの運営・管理の権限はなく、単に、当該情報の伝達役いわば「導管(conduit)」の役割しかない場合である。このような立場の事業者等は、いわば水を家庭に送り届けるだけの役目を持つ導管（水道パイプ）に似ている。つまり、導管は、その中を何が流れているかは一切関係なく、また、きれいか水が流れているか、濁っている水が流れているかわからない。従って、ICT サービスの事業者等が導管のような役割・立場である場合は、その提供しているサービス上で流通している情報の内容について一切関知せず、かつ修正・削除等手を加えることなどできない。

これは「導管理論（conduit　theory)」と呼ばれる米国で生まれた考え方で、もともと「信託を単に受益者のために所得を稼得・分配するための手段・導管とみて課税する」（有斐閣「経済辞典」）という信託課税に関す

る考え方の一つとしてあったものである。そして米国では、早くも 1995 年には、ICT サービスにおける事業者等の法的責任が問われた裁判事例[39]に初めて導管理論が採用されている。その後米国では、ICT サービス上の情報等についての事業者等の責任を、連邦法（通信品位法、青少年オンライン保護法及びデジタルミレニアム著作権法）によって制限[40]している。

以上のことから、ICT サービスの事業者等が、その提供しているサービスの内容について、どのような役割又は立場にあるかによって、法的責任は大きく変わってくる。

従って、ICT サービスの事業者等の責任を論じる場合には、その事業者等が当該サービス上で流通する情報に対して、どの程度の運営管理の権限を有するかなどの役割又は立場を見極めた上で検討する必要がある。

3　プロバイダ責任制限法とソーシャル・メディア

新しい形態のソーシャル・メディアの相次ぐ出現・普及に伴い、そのサービスに係る新たな法的問題・トラブルも次から次へと生じている。これらの殆どが当該サービスを利用している者に係る問題であるので、先ずは利用者自身がこれらに対処しなければならない。しかし、これら法的トラブル等の中には、そのサービスを運営している事業者等の不法行為による民事（損害賠償）責任までも追及するものが増えてきている。

このような事業者等の損害賠償責任を論じる場合、前述したとおり、そのサービスについて、当該事業者等が、どのような役割・立場にあるかが重要になる。

わが国においても、古くは 1997 年（平成 9 年）のパソコン通信の電子会議室を舞台とした事件[41]を皮切りに、インターネット上の電子掲示板やファイル交換サービスなどを舞台とした名誉棄損や著作権侵害について、その事業者等の責任が争われた幾つかの裁判事例[42]が出てきた。

このような背景のもと、2001 年（平成 13 年）に「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（平成 13 年法律第 137 号）」（以下、「プロバイダ責任制限法」という。）が制定された。そこで、このプロバイダ責任制限法について、ソーシャル・メディア、特に SNS との関係から簡単に触れておく。

(1)　プロバイダ責任制限法の概要

プロバイダ責任制限法は、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請求権について定めている（同法第 1 条）。一般に、広く電気通信事業者のことを「プロバイダ」というので、同法も「プロバイダ責任制限法」の通称で呼ばれている。

同法でいう『特定電気通信』とは、「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（電気通信事業法第 2 条第 1 号）の送信（公衆によって直接受信されることを目的とする電気通信の送信を除く。）をいう。」（同法第 2 条第 1 号）と定義されている。具体的には、インターネット上のウェブページ、電子掲示板などの不特定者に受信されるソーシャル・メディアは該当するが、電子メールのように特定の者の間で「1 対 1」で行う通信はこの対象外となる。従って、SNS 中でもフェイスブックは、もともと友達（特定者）間の情報交流を目的としているから、プロバイダ責任制限法でいう「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（電気通信事業法第 2 条第 1 号）の送信」という特定電気通信に該当しない。

また、『特定電気通信役務提供者』とは「特定電気通信設備（特定電気通信の用に供される電気通信設備）を用いて他人の通信を媒介し、その他特定電気通信設備を他人の通信の用に供する者という。」（同法第 2 条第 3 号）と定義されている。典型的には、電気通信事業者に当たるプロバイダが該当するが、営利目的の事業者に限定していないため、電気通信事業者以外の者も含まれる。具体的には、ホスティングプロバイダ[43]、インター

ネット接続プロバイダ（IPS 事業者）などの事業者のほか、電子掲示板管理者など[44]もこれに該当する。このことから、以下、同法でいう特定電気通信役務提供者のことを「プロバイダ等」という。

そして、プロバイダ責任制限法は、プロバイダ等の損害賠償責任の制限（同法第 3 条）及び発信者情報の開示請求等（同法第 4 条）について定めているが、ここでは、以下、プロバイダ等の損害賠償責任の制限についてだけ検討する。

(2)　プロバイダ等の損害賠償責任の制限

そもそも SNS、例えばフェイスブックでは会員制を採っているので、他人の権利を侵害する情報（例えば、著作権侵害情報、名誉侵害情報などの権利侵害情報）などの流通はないとの前提に立ってサービスが提供されている。また、このような SNS の事業者等は、そのサービス上で流通する情報等の内容については一切関知せず、それが権利侵害情報であるか知るよしがなく、いわゆる「導管」の役割・立場である。従って、このような事業者等は、当該サービス上で権利侵害情報が流通し、その情報に起因して発生した損害については「導管理論」により一切の民事責任が免れると考えられる。

一方、インターネット上の電子掲示板、ツイッター、ブログなどの不特定者に受信されることを目的としているソーシャル・メディアでは、当該サービス上で流通する権利侵害情報によって損害を受けた被害者から、当該事業者等に対して損害賠償請求がなされるか可能性がある。

プロバイダ責任制限法は、このような場合を想定して制定された法律であり、同法では、プロバイダ等の損害賠償責任の制限について、プロバイダ等が当該サービスで流通する他人の権利侵害情報につき、以下のとおり、(a) 送信防止措置を講じなかった場合（同法第 3 条第 1 項）と（b）それを講じた場合（同条第 2 項）との二つに分けて定めている。

すなわち、プロバイダ等が、(a) 送信防止措置を講じなかった場合には、当該侵害情報による被害者に生じた損害について、(b) 送信防止措置を講じた場合には、それにより当該情報の発信者に生じた損害について、それぞれの損害賠償責任を制限（免除）するものである。

なお、ここでいう送信防止措置とは、発信者が不特定の者に対して権利侵害情報を送信することを防止する措置のことである。

(a)　送信防止措置を講じなかった場合（第 3 条第 1 項）

プロバイダ等が他人の権利を侵害する情報につき送信防止措置を講じなかった場合は、送信防止措置を講ずることが技術的に可能であり、かつ、プロバイダ等が当該情報の流通によって他人の権利が侵害されていることを知っていたとき、又は知ることができたと認めるに足りる相当の理由があるときでなければ、プロバイダ等は、当該情報の流通により他人の権利を侵害し損害が生じたとしても、その損害賠償責任を負わない。

(b)　送信防止措置を講じた場合（第 3 条第 2 項）

プロバイダ等が必要な限度の送信防止措置を講じた場合、その措置によって発信者に損害が生じたとしても、以下のいずれかに該当するときは、当該プロバイダ等は、発信者に対して損害賠償責任を負わない。

① プロバイダ等が当該情報の流通によって他人の権利が不当に侵害されていると信じるに足りる相当の理由があったとき

② 当該情報の流通による被害者から侵害情報等を示して送信防止措置を講ずるよう申出があった場合に、プロバイダ等が発信者に対し当該送信防止措置を講ずることに同意するかを照会した場合であって、発信者がその照会を受けた日から 7 日を経過しても、それに同意しない旨の申出がなかったとき

(3)　事業者等の責任

SNS 以外のソーシャル・メディア、特に、電子掲示板、ツイッター、ブログなどは、プロバイダ責任制限法でいう「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（電気通信事業法第 2 条第 1 号）の送信」である特定電気通信に該当し、これらのサービスの事業者等は、プロバイダ等（同法の特定電気通信役務提供者）に該当する場合が多い。

従来から、電子掲示板、ツイッター、ブログなどのサービス上で流通する情報に起因して様々な問題・トラブルが生じていたので、これらの中の一部のサービスでは、事業者等が当該サービス上で流通する情報について、積極的に問題・トラベル発生の芽を摘むなど介入しているものもある。つまり、事業者等が当該サービス上で流通する情報の内容等を監視し、他人の個人情報・中傷・誹謗情報、わいせつ情報[45]、権利侵害情報などを発見した場合、あるいは当該情報による被害者等からの要請があった場合には、当該情報の強制削除などの措置を講じることもある。

このような事業者等がプロバイダ責任制限法上のプロバイダ等に該当する場合、当該事業者等は、サービス上で流通する情報に権利侵害情報があることを知り、又は知ることができる立場にあるので、プロバイダ責任制限法 3 条の適用対象者となる。

従って、このような事業者等いわゆるプロバイダ等は、当該権利侵害情報について送信防止措置を講じることが技術的に可能な場合は、必要な限度でこれを講じなければならず、これを講じないときは、被害者に生じた損害について賠償責任を負わなければならない。しかし、この措置を講じることが技術的に不可能な場合は、その責任は負わなくてよい。(同法第 3 条第 1 項)

なお、必要な限度内で送信防止措置を講じた場合において、その措置が当該情報の流通によって他人の権利が不当に侵害されているとプロバイダ等が信じるに足りる相当の理由に基づき講じられたときは、プロバイダ等

は発信者に生じた損害について賠償責任は負わなくてよい。また、プロバイダ等が被害者からの申出により必要な限度で送信防止措置を講じる場合、発信者にその措置を講ずることにつき同意するかを照会し、その照会した日から 7 日以内に、発信者から同意しない旨の申出がなかったときも、発信者への損害賠償責任を負わなくてよい。（同法第 3 条第 2 項）

V　おわりに

本稿では、現在世界中で圧倒的多数の人々が利用しているソーシャル・メディア、中でもフェイスブックに代表される SNS に着目して、個人情報保護など事業者等の責任の在り方について検討した。

SNS などのインターネット利用を前提としているソーシャル・メディアでは、無法地帯といわれるインターネットの匿名性等に起因して様々な法的問題が新たに次から次へと生じていることがわかった。このような法的問題の多くは、ソーシャル・メディア利用を容易に実現したスマートフォーンの爆発的普及とも相まって、今や私たちの身近な問題となって深刻化している。

一方、ソーシャル・メディアのネットワーク（インターネット）上では、ビッグ・データやライフ・ログと呼ばれる膨大な量の情報が全世界規模で流通している。中でも SNS、例えばフェイスブックは、友達同士（特定の会員間）のコミュニケーションを図る目的で情報交流するためのインターネット利用のサービスであるので、このサービスの特性上、ライフ・ログと呼ばれる情報がインターネット上に流通する危険性が高い。このライフ・ログと呼ばれる情報の内容は、私たち人間の生活・行動等（life）に関する記録（log）であるので、この殆どが個人情報（生存する特定人を識別できる情報）である。そこで、これらのソーシャル・メディアのサービス事業者は、特に、取り扱っている個人情報が外部に流出する危険性が

高いことに留意し、当該サービスに適合させたコンプライアンスプログラムを策定・実施することで個人情報保護に努めるべきであろう。

しかし、インターネット上に様々な内容の情報を流通させるのは、ソーシャル・メディアを利用している一人一人の利用者に他ならない。従って、SNS などソーシャル・メディアの利用においては、私たちは、いつでも加害者になり、被害者にもなり得るということを忘れてはならない。先ずは、一人一人の利用者が有害情報や他人の権利を侵害する情報等を発信しないことである。

これらの権利侵害情報等の流通に関して、ソーシャル・メディアの事業者や運営管理者等が対処できる問題は限られている。これらの事業者等は、従来から、その予防・解決措置に腐心しているが、何者かが引き起こす成りすまし犯罪などの発生を完全に防止することはできないので、この対応は警察等の当局に依存せざるを得ない。

なお、権利侵害情報による被害者に生じた損害についての事業者等の民事責任（損害賠償責任）に関しては、米国では古くから「導管理論」により事業者等の責任を否定した判例が出されていた。わが国の判例でも、この導管理論の考え方に沿ったものがあるが、特に、損害賠償責任追及を受ける可能性が高い「1 対不特定多数」で情報を発信する形態の電気通信サービス（例えば、電子掲示板など）の事業者等については、いわゆるプロバイダ責任制限法の適用対象とした。この結果、同法の適用対象の事業者等（プロバイダ等）は、同法第 3 条第 1 項により、技術的に可能な場合は、権利侵害情報の送信防止措置を講じなければ、原則として被害者に生じた損害について賠償責任を負わなければならない。ただし、権利侵害情報の送信防止措置を講じることが技術的に不可能な場合は、これを講じなくても損害賠償責任を免れる。

（完）

註

1)　フェイスブック（Facebook）とは、2004 年当時、ハーバード大の学生だったザッカーバーグが学内の学生同士の交流を図るために開設した会員制（実名登録）の SNS。その後、徐々に全米の学生に開放されたが、当初は、大学のメールアドレス（「.edu」ドメイン）を所有する学生のみに参加は限られていた。2006 年には、英語版が一般に開放され、世界中で利用できるようになったが、2008 年には日本語版でも公開され、国内利用者は、2011 年 9 月には 1 千万人を超えたといわれている。

2)　IT 用語辞典；http: //e-words.jp/

3)　ソーシャル・ネットワーキング・サービス（Social Networking Service；SNS）は、インターネット上で個人間のコミュニケーションができるようにした会員制サービス。代表的なソーシャル・ネットワーキング・サービスとして、日本最大の会員数を持つミクシィ（mixi)、モバイル向けのグリー（GREE)、モバゲー（Mobage)、海外では世界最大の会員数を持つフェイスブック（Facebook)、それに次ぐマイスペース（Myspace）などがある

4)　アラブの春（Arab Spring）は、2010 年のチュニジアの暴動から始まり、2011 年にかけてアラブ各国において発生した、前例のない大規模反政府（民主化要求）デモや抗議活動を主とした騒乱の総称

5)　欧米では、膨大な量の情報（データ）のことをビッグ・データ（big data）と呼んでいるが、情報技術分野では、通常のデータベース管理ツールなどで取り扱う事が困難なほど巨大な大きさのデータの集まりのことをいう。

6)　ライフ・ログ（life log）とは、いわゆる生態的情報であり、人間の生活・行い・体験（life）を映像・音声・位置情報などのデジタルデータとして記録に残すことである。

7)　www（world wide web）システムを使ったインターネット上の文書を「ウェブページ（web page)」と呼ぶが、ウェブサイト（web site）は、このような多くのウェブページを 1 冊の本のようにひとまとめにして公開して

いるインターネット上の場所のこと

8) ICT は、「Information and Communication Technology」の略語で、情報通信技術のこと。従来は IT（情報技術）の言葉が広く使われていたが、近年は、これに Communication（通信）の言葉を付け加えた「ICT」の言葉の方が国際的には広く使われている。

9) これらインターネット利用者が守るべき最低限のルールや倫理的基準のことを「ネチケット」と呼んでいる。この「ネチケット」は、「ネットワーク・エチケット（network etiquette）」を一つの言葉にまとめた造語である。

10) 第一次提言；http://www.soumu.go.jp/main_content/000035957.pdf

11) 第二次提言：http://www.soumu.go.jp/main_content/000067551.pdf

12) ディープ・パケット・インスペクション技術（略称；DPI 技術）とは、インターネット接続業者（通信プロバイダ）側で、情報を丸ごと読み取る技術を広告に使う手法だが、個人の行動記録が丸裸にされて本人の思わぬ形で流出してしまう危険もある。つまり、通信プロバイダのサーバーに専用の機械を接続し、利用者がサーバーとの間でやりとりする情報を読み取る。どんなサイトを閲覧し、何を買ったか、どんな言葉で検索をかけたかといった情報を分析し、利用者の興味・嗜好に応じた広告を配信する。

13) 行動ターゲティング広告について、一般社団法人インターネット広告推進協議会（JIAA）は、平成 22 年 6 月に改訂した「行動ターゲティング広告ガイドライン」を公表した。このガイドラインでは「行動履歴情報から利用者の興味・嗜好を分析して利用者を小集団（クラスター）に分類し、クラスターごとにインターネット広告を出し分けるサービスで、行動履歴情報の蓄積を伴うものをいう。」と定義している。なお、前掲・第一次提言では、行動ターゲティング広告の具体例として Google（グーグル）の「アドワーズ」を例示している。

14) 例えば、前掲・第一次提言でも、Google のストリートビューなどの「インターネット道路周辺映像提供サービス」については、個人情報保護法に違反するのではないか、住宅地の家屋や人を無断で撮影して公開することはプライバシーや肖像権の侵害ではないかなどの問題が各方面から提起されていると指摘している。

15) 個人情報保護法の正式名称は、個人情報の保護に関する法律（平成 15 年

5 月 13 日法律第 57 号）

16）「個人情報データベース等」とは、個人情報保護法第 2 条第 2 項で「個人情報を含む情報の集合体であって、コンピュータなどにより特定の個人情報を容易に検索できるように体系的に構成したもの」と定義している。

17）IPS とは、「Internet Provider Service」の略で、インターネットへの接続サービスなどを行うことをいう。このサービスを行う IPS 事業者は、一般に「通信プロバイダ」と呼ばれている。

18）電気通信事業法では、電気通信役務とは「電気通信設備を用いて他人の通信を媒介し、その他特定電気通信設備を他人の通信の用に供することをいう。」（第 2 条第 3 号）と定義し、電気通信事業とは「電気通信役務を他人の需要に応ずるために提供する事業（放送法第 118 条 1 項に規定する放送局設備供給役務に係る事業を除く）をいう。」（同条第 4 号）と定義している。なお、電気通信とは、有線・無線を問わず（同条第 1 号）ので、また、電気通信設備とは、電気通信を行うための機械、器具、線路その他の電気的設備をいう（同条第 2 号）

19）個人情報保護法とは別の法律として、同法と同時に、行政機関が保有する個人情報については「行政機関個人情報保護法（平成 15 年法律第 58 号）」、独立行政法人等が保有する個人情報については「独立行政法人個人情報保護法（平成 15 年法律第 59 号）」という二つの法律が制定された。

20）個人情報保護法第 23 条第 1 項では、個人情報取扱事業者は、原則として、あらかじめ本人の同意を得ないで個人データを第三者に提供してはならないが、法令に基づく場合など幾つかの場合を例外としている。平成 23 年 10 月 26 日東京高裁判決（金融・商事判例 1380 号 52 頁）では、第三債務者である金融機関に対する弁護士照会（個人データの第三者提供）は、法令に基づくものであるから回答すべしと判示した。

21）平成 23 年 3 月 31 日現在、生命保険業の（社）生命保険協会、病院の（社）全日本病院協会、クレジット業の（社）日本クレジット協会など計 38 団体が、個人情報保護法第 37 条に基づき主務大臣から認定を受けた「認定個人情報保護団体」となっている。

22）この自主規制は、各事業者が所属する業界団体が中心となって当該業界における個人情報の取扱いの実態に合わせて策定した「業界ガイドライン」

を基に行っている。

23) コンプライアンス・プログラムは、一般に、個人情報保護のための管理体制や内部規定等の整備、休業員に対する教育や監査などについて、PDCAサイクルのマネジメントシステムとして策定することになるが、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(JISQ 15001)」に準拠することが望ましい。

24) 民間部門における個人情報保護の自主的取り組みの一環として、個人情報保護コンプライアンス・プログラムの民間認証制度として、一般社団法人日本情報経済社会推進協会（JIPDEC）を認証機関とした「プライバシーマーク制度」が創設された。この認証（マークの使用許諾）を受けるためには、事業者の個人情報保護コンプライアンス・プログラムの内容が日本工業規格「JIS Q 15001」に適合していることが必要であり、2012年6月18日現在、12,597の事業者がプライバシーマークを取得している。

25) EU個人データ保護に関する指令：http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

26) EU個人データ保護に関する規則（案）：http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

27) セーフ・ハーバーは、EU加盟の1カ国から標準契約条項（Standard Contract Clauses）又はBCR（Binding Corporate Rule）の承認を受けることにより、EU全域からの個人データの移転ができるというもの

28) 4A‘s、ANA、CBBB、DMA、IABの5団体

29) 最高裁平成15年9月12日第二小法廷判決（判例タイムズ1134号）では、大学の講演会への参加学生の学籍番号、氏名、住所及び電話番号を無断で警察に開示した行為はプライバシー侵害として不法行為を構成すると判示し、東京地裁平成21年1月21日判決（判例タイムズ1296号235号）でも、原告の配偶者の氏名・住所、親族の経営する会社の名称・本支店の所在地・電話番号をインターネット上の掲示板に書き込んだ事件がプライバシーを侵害すると判示した。

30) 個人情報保護法が適用される「個人情報取扱事業者」から「その取り扱う個人情報の量及び利用方法からみて個人の権利利益を害するおそれが少ないのものとして政令で定める者」は除外している（同法2条3項5号)。つ

まり、この適用除外事業者は、その取り扱う個人情報の量として、当該個人情報によって識別される特定個人の数が 5 千を超えなければ該当する（同法施行令 2 条）。

31）東京地裁昭和 39 年 9 月 28 日判決（下級裁判所民事裁判例集 15 巻 9 号 2317 頁「宴のあと事件」）では、「プライバシー権は、私生活をみだりに公開されない権利」とし、この権利侵害に対しては、侵害行為の差止及び精神的苦痛による損害賠償を認めた。

32）さいたま地裁平成 23 年 1 月 26 日判決（判例タイムズ 1346 号 185 号）では、判例雑誌に掲載された判決文中の当事者名が実名のまま表示されたことについて、プライバシー侵害による不法行為は成立しないと判示した。

33）大審院連合部大正 15 年 5 月 22 日判決（大審院民事判例集 5 巻 386 頁「富喜丸事件」）は、物損の金銭的評価の基準時に関するリーディングケースとされているが、この判決では、民法 416 条が「相当因果関係」の基準を定めたものであることを前提に、この規定を不法行為（損害賠償の範囲）にも類推適用すべきと判示した。

34）最高裁昭和 38 年 1 月 25 日第二小法廷判決（民事判例集 17 巻 1 号 77 頁）など

35）内田貴「民法Ⅱ債権各論」東京大学出版会、396 頁

36）我妻栄「新訂 債権総論（民法講義Ⅳ）」岩波書店、118 頁

37）ウェブサイト、特に、プロフィールサイトやブログ及び電子掲示板では、いじめ、非行、犯罪など青少年が被害者にも加害者にもなり得るので、ネットパトロールは、地方自治体単位に公立中・高校生を対象に、これらへの書込頻度が高い自己又は他人の個人情報、中傷・誹謗・わいせつ情報などがないかをパトロール（監視）する青少年ネット被害防止対策事業のこと。

38）電子掲示板等への名誉棄損等の情報の書き込みは、被害者以外の利用者（個人）が行うことが多いが、、一般に、その書き込みの削除等は、被害者が直接行うことができないので、当該電子掲示板の管理者に依頼することになる。このことからプロバイダ責任制限法が制定された後の判例を見ると、この電子掲示板管理者の削除義務違反を追及した判例として、東京地裁平成 16 年 5 月 18 日判決（判例タイムズ 1160 号 147 頁）、名古屋地裁平成 17 年 1 月 21 日判決（判例時報 1893 号 75 頁）、東京地裁平成 18 年 11 月 7 日判決

（判例タイムズ 1242 号 224 頁）などが続出している。また、動画投稿サイト運営会社等が著作権侵害動画ファイルをサーバーに蔵置し、これを各ユーザーのパソコンに送信しているとして、差止及び損害賠償の訴えを受けた判例として、東京地裁平成 21 年 11 月 13 日判決（判例タイムズ 1329 号 226 頁）がある。

39）「導管理論」が米国の ITC サービスに係る裁判で最初に登場したのは、ニューヨーク州高等裁判所 1995 年 5 月 24 日判決（「Stratton Oakmont Inc. and Daniel Porush vs. Prodigy Service Company」事件）である。この裁判では、原告（Stratton Oakmont）が被告（Prodigy）の電子掲示板に、正体不明の投稿者によって原告を中傷誹謗するメッセージが掲載されたので、被告を名誉棄損で訴えたが、導管理論により事業者である被告の責任を認めなかった。

40） 例えば、1996 年改正の通信品位法（Communications Decency Act of 1996）は、わいせつ情報等へのアクセス制限措置をした場合の民事責任の制限をしているが、双方向通信サービス提供者は、別の情報コンテンツ提供者の情報については発行者（publisher）や代弁者（speaker）として扱わず、アクセス制限のため妥当な措置を誠実に講じたことによる損害については民事責任を負わないとしている。

41） 東京地裁平成 9 年 5 月 26 日判決（判例タイムズ 947 号 125 頁「ニフティサーブ事件」）は、ICT サービス事業者の責任が問われた最初の判例である。この事件では、ニフティサーブ（事業者）が主宰するパソコン通信の「フォーラム（電子会議室）」に、書き込まれた名誉棄損（不法行為）の発言について、これを運営管理する権限を持ったシスオペが注意しただけで削除せずに放置し必要な措置を取らなかったこと（作為義務違反）について、主宰者（ニフティサーブ）の使用者責任を認めた。

42） プロバイダ責任制限法が制定される前で、事業者等の責任が争われた裁判事例としては、東京地裁平成 11 年 9 月 24 日判決（判例タイムズ 1054 号 228 頁）、東京地裁平成 14 年 6 月 26 日判決（判例タイムズ 1110 号 92 頁）、東京地裁平成 15 年 1 月 29 日判決（判例タイムズ 1113 号 113 頁）、東京地裁平成 15 年 6 月 26 日判決（判例時報 1869 号 46 頁）、東京地裁平成 15 年 7 月 17 日判決（判例時報 1869 号 46 頁）などがある。

43)　ホスティングとは、顧客が自前の設備などを持たずにインターネット上で情報やサービスを配信するのをサポートするため、インターネットに接続した事業者のサーバー（コンピュータ）の機能を、遠隔から顧客に利用させるサービス。

44)　最高裁平成 22 年 4 月 8 日第一小法廷判決（民事判例集 64 巻 3 号 676 頁）では、「最終的に不特定の者に受信されることを目的として特定電気通信設備の記録媒体に情報を記録するためにする発信者とコンテンツプロバイダとの間の通信を媒介する経由プロバイダは，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 2 条 3 号にいう特定電気通信役務提供者に該当する。」と判示した。

45)　わいせつ情報等は、刑法第 175 条（わいせつ物頒布等）違反、児童売春・児童ポルノ法（平成 11 年法律第 25 号）違反、出会い系サイト規正法（平成 15 年法律第 83 号）違反などの犯罪に該当するものもある。（この場合、プロバイダ等は、警察等への通報や捜査への協力が要請される。）