目　次

『情報法制研究』創刊号に寄せて

情報法制学会代表
曽我部　真　裕
SOGABE Masahiro

このたび，2017 年に発足した情報法制学会の機関誌として，「情報法制研究」を発刊する運びとなった。

「情報法」という言葉は 1980 年代から散発的に使われてきたが，現在のインターネット社会とつながる形で用いられるようになったのは 1990 年代半ば以降である。情報法という語をタイトルに含んだ概説書も出版されているが，これまでは総じて，情報法の内包や外縁の定義の試みは乏しく，「情報に関連する法」を寄せ集めたものという印象が強い。

実際，近年では独自の法領域としての情報法の成立可能性について論じる試みも見られるようになったとはいえ，実際には情報法の遠心性は強いものがあり，また，情報法のカバーすべき範囲はますます広く深くなっている。また，情報の流通や保護といった社会的要請は，法的規律だけではなくテクノロジーによっても対応がなされること，ルールによる規律でも法的な規律に加え，行政や，各種のレベルでの民間によるルール策定（共同規制，自主規制）によってもなされていることから，広い意味での法源も極めて分散している。それに関連して，これらの法源ごとにそれに関わり，あるいはそれを議論するアクターも異なる場合があることもあって，ある特定の事柄を規律するルールの総体やそれに関する議論状況が見通しにくい状況になっているように思われる。

こうした状況においては，情報法の遠心性を緩和し，情報法の各個別領域で蓄積された知の共有を図る試みが求められる。概念としての情報法の構築はこうした問題意識に基づくものであったが，それだけではもちろん不十分で，情報法各領域で活動するアクターが集うプラットフォームが必要不可欠である。今見たような状況からすれば，情報法を論じるために必要な知見は法律学だけではなく，経済学やテクノロジーをはじめ幅広いものがあり，こうした幅広い分野の専門家の参加が求められる。

このような問題意識のもと，この度発足した情報法制学会は，「情報，メディア等に関する法，技術及びビジネスの観点からの学術的，実務的な研究（…）を促進することを目的とする」（規約第 1 条）ものである。情報法に関わる学会はすでに複数存在するが，相対的には実務家が中心であった既存の学会に対して，研究者とのつながりを深めることをも目指している。それと同時に，姉妹団体である情報法制研究所との緊密な連携のもと，研究成果の社会への還元にも取り組んでいく。さらに，情報法の研究や実践に関わる若手研究者・実務家の育成をも重視している。

本『情報法制研究』は，このような情報法制学会の機関誌として，情報法に関わる多様な観点からの研究論文を掲載するものである。年 2 回発行の本誌は，実績ある研究者の寄稿を掲載するほか，査読を経た投稿論文も積極的に掲載することにより，若手研究者・実務家の研究発表の場を提供する。さらに，情報法に関する内外の動向を紹介する資料なども掲載して，情報の共有を図る。

こうした内容のほか，本誌の大きな特色の 1 つは，法学系の学術雑誌としてはほとんど初めて，オンラインを中心とするということにもある。もちろん，紙版も発行はするが，紙版の発行と同時に，個々の論文がオンラインで一般無料公開され，研究成果が広く読まれることになる。学会に入会すれば無料で投稿が可能であることとあわせ，若手にとっては魅力的な発表媒体になることだろう。

このような特色を有する本誌であるが，当初の意図が達成できるかどうかはひとえに執筆者，投稿者，また，読者の支持を得られるかにかかっている。学会とあわせ，多くの研究者・実務家の支援を期待する次第である。

一般財団法人情報法制研究所設立について

一般財団法人情報法制研究所 理事長
鈴 木 正 朝
SUZUKI Masatomo

情報法制研究所は，2016（平成 28）年 3 月に評議会において役員を選任し，その後の理事会において理事長を互選し，5 月の設立記念シンポジウムのお披露目を経て，6 月 23 日に設立登記を終えて一般財団法人として正式に設立した。

そもそも情報法制研究所設立に至るきっかけは，マイナンバー制度の創設に至る中で憲法，行政法，社会保障法，税法，情報法，財政学，行政学，人口論，経済学，情報理工など多様な研究者による広い議論に接し，あらためて学際研究の重要性を痛感したこと，個人情報の定義や匿名化の議論において数理系研究者の知見を要したこと，また，越境データ問題に直面し，EU 法をはじめとする各国立法例の調査の手薄さを再認識したこと，それから新たなビジネス創出に向けて法的な基盤整備を要する中で，産官学の間はもとより，消費者や政治とのコミュニケーションが円滑になされていないという反省があったことなどあるが，何より個人情報保護委員会の新設という新たな行政庁の登場によって国の情報のガバナンスのあり方が変わっていくであろうし，また時代背景に応じて変えていかねばならないということであった。官の 2，3 年の短い人事異動のサイクルは，組織における専門性の蓄積という点において難があることは否めず，やはり中長期的に継続して情報に関する政策やそれを支える研究を行っていく機関を創設すべきであるとの思いが募ったということである。

当団体の名称を「情報法制」としたのは，情報法の法解釈学的な研究に止まらず，広く経済学，経営学，社会学，情報学，理学，工学といった多分野の研究者が集い，あるべき情報法制を求めて，立法政策を含む社会の諸制度について実践的な取り組みを行うという意味を込めたつもりである。

また「研究所」としたのは，研究者による学術的見地を基礎に，企業及び消費者団体の関係者等と共に情報社会の問題解決に取り組む民間の独立研究機関を目指したからである。具体的には，会員企業や団体を募り，研究員を委嘱し，テーマごとにタスクフォースを設置して，広く意見交換を行いながら検討を深め問題解決や政策提言を行うべく，現在，個人情報保護，自治体情報法，EU 情報法，オンライン広告，サイバーセキュリティ，資金決済法，通信行政，青少年ネット利用環境，情報と民法の 9 つのタスクフォースからスタートしている。

なお，多様な意見を有する研究者，企業及び消費者保護等の関係者が集うことから，政策提言やパブリックコメントについては，役員及び研究員の発意で行い，研究所としての機関決定は行わずに，賛同する役員及び研究員が個人の立場で連名の上，発信することとした。

今日，少子高齢人口減少社会を背景に公的年金，医療保険，介護保険など社会保障制度の持続可能性が危ぶまれており，社会保障の給付減と国民の負担増は回避し難い構造にある。こうした中で社会保障と税の一体改革が構想され，マイナンバー制度が導入された。悉皆性と唯一無二性を有する強力な公的個人識別子の登場により国家による国民の各種個人データの制度横断的な名寄せ機能が大きく向上することで，国民のプライバシーの権利が侵害される脅威が高まっている。権力濫用の危険性に対する懸念は極めて正当な感覚であるが，それは新しいものだけではなく，電算化された戸籍のシステムにも向けられなければならず，またそれは行政だけではなく，立法や司法，地方公共団体にも向けられなければならない。また，識別子に着目するのであれば，民間部門におけるそれも対象に検討されなければならない。リスクに備えることも重要であるが，既に起きているスノー

デン事件などプリズムの問題からも目をそらしてはならない。さらには，ある種タブー視されてきた国防問題，特に我々はサイバー・ウォーに備え，諜報活動の必要性についても直視していかねばならない。そこを捉えることなしには法律によってそれを統制することもまた困難になるからである。

当研究所は，政財官民のネットワークのハブとなる機能を担い情報社会の公共的課題の解決に具体的に貢献できる実践的な活動を行っていきたいと思っているが，あくまでもその軸足は学にあるという意味で，2016 年 12 月の理事会に先立ち理事，評議員が発起人となって，情報法制学会を立ち上げた。ここでは具体の政策実現の活動とは離れて，純粋に学術団体として研究活動に専心していく場とした。当研究所はその事務局として運営を支援する役割を担うことになるが，共に情報社会の健全な発展に資する活動になるよう努めていきたいと思っている。

『情報法制研究』創刊号に寄せて
―「情報法」提唱者の 1980 年代までの回顧と展望―

一橋大学名誉教授
堀　部　政　男
HORIBE Masao

Ⅰ　はじめに

情報法制研究所創設，情報法制学会設立，情報法制研究創刊号発刊と続く関係者の一連の英断は，目を見張るばかりであり，敬意と祝意を表したい。

「情報法制」と密接不可分な「情報法」という新たな法分野の確立を提唱した者として，この機会に，日本の情報法研究の歴史のうち，時間の関係で 1980 年代までを回顧し，今後について少し展望することにする。

Ⅱ「情報化」等の認識と用語

一般的にいって，科学技術の発展は，あらゆる方面に大きな影響を与える。情報通信関係技術の発展もその主要なものの一つであることはいうまでもない[1)]。情報通信関係技術の発展は，「情報化」ないし「高度情報化」という概念を生み出し，これに「社会」を付加した「情報（化）社会」ないし「高度情報（化）社会」という用語を普及させることになった。

今日好んで使用されている「情報」というのは，これまでにも様々な言葉で表現されてきた（例えば，しらせ・知識・資料等）。それを生産・供給・伝達・利用・消費するなどのテクノロジーが飛躍的な進歩を遂げ，情報が量的に著しく増大し，従来とは質的にも異なった状況が出現しつつある傾向をそのように認識して「情報化」という言葉であらわしていると見られる。

日本で「情報化」，「情報化社会」などに関連した言葉が生み出され，使われるようになったのは，1960 年代であった。それから今日までの歴史を年代順に特徴的と思われるところを概観し[2)]，「情報法」という概念をどのようにして使うようになったかについて見ることにする。

Ⅲ　1960 年代の概観

1　言論・表現の自由と名誉・プライバシー

改めていうまでもなく，日本国憲法が 1947 年 5 月 3 日に施行され，その第 21 条で言論・表現の自由が保障されたことから，これに関する研究が主流になってきた。その一方で，言論・表現の自由に名を借りた，行き過ぎた表現が問題視されるようになった。それらとの関係で名誉・プライバシー等への関心が高まった。これが 1960 年代前の状況であった。

---

1)　この問題については，様々な形で論じてきている。比較的最近のものとして，堀部政男「まえがき―情報通信法制の現段階と展望」，堀部政男編著『情報通信法制の論点分析』（商事法務，別冊 NBL ／ No.153，2015 年）1 頁以下参照。また，本書に収められている諸論稿は，このような問題を考える際に参考になる。以下，注はできるだけ少なくする。

2)　これまでに多くの機会に論じてきたが，1970 年代末までについて年代順に概観したものとして，堀部政男「情報法―のびゆく現代法―新しい法分野シリーズ〔第 7 回〕」，法と政策 1981 年 12 月号 86 頁以下参照。

2 『宴のあと』プライバシー侵害訴訟

1960年代に入ると，まず，1961年に有田八郎氏が小説『宴のあと』に関して出版社の新潮社と作者の三島由紀夫氏に対しプライバシーの侵害を理由に民事訴訟を提起したことが注目を集めた。これをきっかけにして，学界でもマスコミ界でもプライバシーの権利は脚光を浴び，1962年には，比較法学会で「人格権の比較法的研究」というシンポジウムが行われ，また，戒能通孝・伊藤正己編『プライヴァシー研究』（日本評論新社）が従来の研究等を収録し，さらに，翌1963年には，アメリカ法を素材として比較法的研究を行った伊藤正己『プライバシーの権利』（岩波書店）が著わされた。そして，この年には，大野文雄・矢野正則・今西勇『判例実例名誉・プライバシーの裁判基準（民事刑事）』（酒井書店）が出た。また，1965年に刊行された三島宗彦『人格権の保護』（有斐閣）は，その保護の必要性を強調したものとして，この流れに属する業績であったといえる。

この時代で特筆しなければならないのは，プライハシーの権利の重要性が説かれる中で，1964年9月28日にこの権利を承認した東京地方裁判所の判決が出たことである。裁判所は，プライパシーの権利が，人格権という以前から認められている権利に含まれるが，なおそれをマスコミュニケーションの発達との関係で「一つの権利」と呼ぶことができると判断した。

これらは，マス・メディアにかかわる法現象の一測面を扱ったものにすぎなかったが，1960年代の後半になると，「マスコミ法」と呼ぶことができる法分野が積極的に開拓されるようになった。それは，伊藤正己・清水英夫編『マスコミ法令要覧』（現代ジャーナリズム出版会）が，1966年に出版されたことに端的にあらわれている。この要覧の冒頭には，「マスコミ法制概説」が収められており，マスコミ法がどのようにとらえられているかを知ることができる。また，1960年代に書いた論文をまとめた清水英夫『法とマス・コミュニケーション』（社会思想社，1970年）は，マスコミ法を一つの法分野とすることに貢献した。当時，私は本書について「マス・コミュニケーション法に関心を寄せる者にとって，待望の書が出版された」という書き出しで，警評を書いたことがある（「図書新聞」1970年6月27日号）。

これらからも分かるように，1960年代の法学界では，「情報」を正面から論じるまでには至らなかったといってよいであろう。

Ⅳ 1970年代の概観

1 情報関係業績の蓄積

1970年代は，わが国におけるマス・メディア法の発展にとってきわめて重要な時期であった。1971年には，私も編集にかかわった『マスコミ判例百選』（「ジュリスト」別冊）が刊行され，マスコミ法制の研究を発展させるのに貢献した。また，71年には，アメリカでベトナム秘密文書の報道事件をめぐって，政府と新聞が対立し，裁判所が言論の自由に軍配を上げたため，マス・メディアの報道の自由が改めて注目を集めた。さらに，72年には，わが国で沖縄密約漏洩事件が起こり，国民の知る権利が多面的に論じられるようになる契機となった（その一つの大きな流れが，後述する情報公開制度の問題へと発展していく）。

このような動向の中で，1974年には，石村善治・奥平康弘編『知る権利―マスコミと法』（有斐閣）が公刊され，現代社会におけるマス・メディアと法のかかわり合いについて，多彩な論点を提示した。また，この74年には，マス・メディアへのアクセス権という新たな権利概念が提唱され，各方面に大きな波紋を投げかけた。稲葉三千男・新井直之編『新聞学』（日本評論社，1977年）の執筆者の一人である山田実氏は，「……このアクセス権という概念がわが国において明確な形で論じられるようになったのは，一体，いつ頃のことなのであろうか。それは一九七〇年代の前半になってからである。もっと正機にいうならば，一九七四年一〇月，堀部政男の論文「アクセス権論」が「ジュリスト」五七三号に掲載されてからである。〔その他の文献もあげた後〕わが国における問題状況をしっかりふまえて，このアクセス権という概念が包括的に論じられるようになったのは，やはり，なんといっても，堀部政男の論文「アクセス権論」においてである」と評している。

この時期には，ここに掲げたもの以外にマス・メディア法だけでも多くの業績が見られたが，そ

れとともに，情報法の新たな側面に関心が向けられるようになった。特に，1960年代に始まった急速なコンピュータリゼーションとの関係で，その法的問題が注目を引くようになった。その一つとして，プライバシー問題が主としてコンピュータとのかかわりで検討されるにようになったことを挙げることができる。

1970年代前半における問題状況は，その後半においてさらに新たな展開を見せ，大きな成果を生み出した。まず，マス・メディア法関係では，詳論をする余裕がないが，主な業績を掲げると，次のようになる。

・伊藤正己・内川芳美・後藤和彦・堀部政男編『現代のマスコミ』（「ジュリスト」増刊総合特集，1976年）
・堀部政男『アタセス権』（東京大学出版会，1977年）
・ジェローム・A・パロン著清水英夫・堀部政男・奥田剣志郎・島崎文彰訳『アクセス権―誰のための言論の自由か』（日本評論社，1978年）
・『言論とマスコミ』（『法学七ミナー』増刊，1978年）
・伊藤正己編『放送制度―その現状と展望①②③』（日本放送出版協会，1976年・77年・78年）
・堀部政男『アクセス権とは何か』（岩波書店，1978年）
・清水英夫『言論法研究―憲法二十一条と現代』（学陽書房，1979年）
（その他，各種の雑誌に掲載された論文は多数にのぼる。）

知る権利との関係でアメリカの1966年情報自由法（Freedom of Information Act of 1966）が取り上げられ，そこで「情報」が使われ，また，アクセス権（right of access）の対象の中には，公的情報や自己情報も含まれるので，「情報」への関心が高まってきた。

マス・メディア（マスコミ）法又は言論法に関する学会を設立しようという議論は関係者の間ではかなり以前から出ていた。しかし，実現には至らなかった。

2　法とコンピュータ学会の設立と「情報」概念の使用

一方，情報化社会のシンボル的存在であるコンピュータに関する法的問題の分野では，学会の設立が先行した感が強い。「法とコンピュータ学会」がそれである。その設立趣意書を見ると，設立の経緯が分かる。1976年の文書の一部を見ると，次のようになる。

「最近，コンピュータが社会のますます多くの分野に利用されるに伴い，無限といえるほど複雑多岐な，まったく新しい法律問題が発生しだし，他方，法の分野自体にもコンピュータがいっそう多くの用途に使用されるようになりました。……アメリカの“Computer Law Association”と合同して，日本の「法とコンピュータ」関係の方々の協力と参加を得て「法とコンピュータ」のPre-Conference Symposiumを企画し，「法とコンピュータ」国際研究会議を開きました。その折，日本にもアメリカの学会に相当するものを設立してはどうか，について，……出席者の方々に個人としてのご意見を伺いましたところ，多数がご賛同くださいました。」

こうして，「法とコンピュータ学会」は，1976年10月に創立総会を開催した。この学会の成果の一部は，「法情報学への歩み」（「ジュリスト」1978年2月15日号）や「情報化時代の法律問題」（「ジュリスト」1980年1月1日号）に結実している[3)]。

また，76年には，情報法にとって重要な成果である奥平康弘「情報化社会」（『未来社会と法』筑摩書房）が注目された。

70年代後半は，さらに，情報公開法やプライバシー・個人情報保護法への関心が高まった時期としても特徴づけることができる。その成果は，ここでは，割愛しなければならない。もう一つ，情報の宝庫である図書館に関する法的問題が79年12月の図書館法研究シンポジウムで取り上げられたことも指摘しておく必要がある（その成果

3）伊藤正己先生は，この特集の冒頭の論稿において，情報をめぐる法的課題を明確に指摘している。

は『図書館法研究』（日本図書館協会，1980年）としてまとめられた。堀部政男「図書館法の法学的検討―図書館の自由を中心として」も収められている）。

3 「情報法」への意外な反応

1960年代に「未来学」や「社会学」等の分野にも関心を寄せていたので，「情報」という言葉がよく使われるようになったことを認識していた。法律学の分野でも，「情報法（学）」という法分野の確立が必要であるという漠然とした発想を1970年前後には抱いたように記憶している。

しかし，若手研究者としては言い出しにくかった。

前掲の伊藤正己編『放送制度―その現状と展望①②③』（日本放送出版協会，1976年・77年・78年）は，法学者等が放送法制を中心に研究することを目的として1974年に結成された放送通信制度研究会の成果の一部であるが，この研究会の当初のメンバーは，当時の肩書で示すと，芦部信喜（東京大学教授），伊藤正己（東京大学教授），内川芳美（東京大学教授），大森幸男（放送評論家），金沢良雄（成蹊大学教授），塩野宏（東京大学教授），舘野繁（電気通信総合研究所常務理事），山本草二（東北大学教授）であった。私は1974年に海外留学からの帰国後，加わった。後に濱田純一前東京大学総長（当時，東京大学助手）等もメンバーになった。

この研究会は，私にとっては極めて貴重であった。それぞれの研究テーマについて議論するばかりでなく，懇談する機会も多かった。この時期までに，日本では情報社会論が大きな注目を集め，「情報」というキーワードで論じられることが多くなっていた。私自身，1960年代に知る権利，プライバシー権，マスコミ等についても研究し，1970年代にも情報公開，個人情報保護等の「情報」にかかわる法的課題に取り組んできたので，懇談の席で「情報法」という法学の分野横断的な領域を提唱したいなどと話したりした。それに対する反応は私にとっては意外だった。「君は若いね。以前は“情報”というのは“諜報”（スパイ）に通じるところがあり，それを知らない世代だね。“スパイ法”だよ」などと先輩の先生方から言われ，「情報法」は使いにくい概念であることに気付かされたことがあった。

そのような雰囲気であったが，1970年代中葉までには，「情報自由」，「情報公開」，「個人情報」など「情報」が重要な意味を持つ問題について研究し，論稿もまとめてきた者としては「情報法」という新たな分野を確立したい気持ちも強く，様々な機会に「情報法」という概念を使っていた。

そのようなこともあって，当時刊行されていた「法と政策」という月刊誌の編集部（第一法規）から「のびゆく現代法」という欄に「情報法」についてまとめるように依頼され，執筆した。それは，「法と政策」1981年12月号の「のびゆく現代法 新しい法分野シリーズ」第7回として掲載された。これは，「情報法」について論じた初期のものである。1980年代に属するので，そこで取り上げることにする。

V 1980年代の概観

1 情報法学の必要性の提起

今言及した拙稿では，冒頭で「情報法学の必要性」について次のように論じた。

「情報化時代といわれる現代社会において，情報の価値が再認識されている。そのため，法律学でも情報にかかわる問題が従来にも増して関心を集めている。情報に特有な法現象を総体としてとらえる場合，これを「情報法」と呼び，また，情報法に関する学問的研究を法律学の一分野に位置づけるならば，これを「情報法学」と称することができる。しかし，その重要性にもかかわらず，体系的な研究は，わが国においてばかりでなく，諸外国でもほとんどなされていない。それだけに，情報法という分野を新たに設定することの意義は大きい。

とはいうものの，新たな法分野の確立は一朝一夕にはできない。多くの研究者による個別研究と共同研究の成果の蓄積が必要であり，それらを総合する体系的な研究が出てくるまでにはなお時間を要するであろう。

ここでは，情報法の基礎となる個別領域の研究成果を例示的にほぼ年代を追ってとりあげ，研究の現状を明らかにするとともに，今後の展望も試みることにする（情報法の意義・目的・対象・方法などについては別の機会に検討することにしたい）。」

1980年代になると，法律学の分野でも，「情報」という概念を使うことがかなり広がってきた。その成果を網羅することは，もとより不可能であるので，私がかかわったものを中心に概観することにする。それまでも，研究と実践の融合化，研究の実践化を試みてきた。また，その後も，試みることになる。

2　神奈川県情報公開制度提言案作成

例えば，神奈川県においては，情報公開の制度化の検討に当たった[4]。これについては取り上げたいことは非常に多いが，情報公開（公文書公開）条例の基礎となる「神奈川県の情報公開制度に関する提言」をまとめる神奈川県情報公開推進懇話会の小委員会の委員長として提言案を作成し，1982年7月17日に小林直樹懇話会会長が長洲一二知事に手交した。これは，日本の情報公開制度の歴史において非常に重要な役割を果たした。ここでは，「情報」公開というように，情報という概念を用いている。

「神奈川の『情報公開』提言」（要旨）をほぼ全頁を使って掲載した読売新聞1982年7月18日朝刊は，その同じ頁の「今日の顔」で「神奈川県情報公開制度への提言をまとめた　堀部政男さん」との見出しで私を取り上げた。ここでは，「情報法」という言葉が使われている。

この記事は，「十年以上も前から知る権利を論じ，プライバシーなどを含めた広い範囲の「情報法」の確立を提唱してきた」という書き出しで，「「情報公開先進国のスウェーデンに匹敵する人口を持つ神奈川県で，いま，私の提唱が実を結ぼうとしている。研究者の一人として，うれしく，誇りを感じます」。静かな語り口に，先駆者らしい自信がのぞく」とも書いている。また，「で，内容は満足出来るものになりましたか―。」「「研究者としての理想像がある反面，現在の法律では越えることのできないハードルも多い。理想と現実の間で，最も好ましい情報公開の方法を見つけることに苦労しました。現時点で実現可能なものを考えると難しかった」。」「先駆者であるがゆえの苦しみということか」などともまとめている（井村明彦記者）。

3　行政管理庁・プライバシー保護研究会報告書

この時期には，OECD（経済協力開発機構）で1980年9月23日に採択された「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」（Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data）（OECDプライバシー・ガイドライン（OECD Privacy Guidelines））を受けて，日本では国レベルで行政管理庁（当時）プライバシー保護研究会（座長・加藤一郎東京大学教授）が開かれるようになった。私は，この研究会の最年少のメンバーであった。プライバシー・個人情報保護について論文や本を出していたので，事務局と一緒に海外調査や報告書の取りまとめにも当たった。その報告書は，「個人データの処理に伴うプライバシー保護対策」というタイトルで1982年7月に公表された[5]。

その中の「Ⅲ　プライバシー保護対策の在り方」で，「個人データシステムの規律を目的とする制度的な対応としては，以下に掲げるプライバシー保護の基本原則に立脚した新たな法律を制定する必要がある」と立法化を提唱した。その基本原則（5原則）とは，次のようなものであった。

①収集制限の原則，②利用制限の原則，③個人参加の原則，④適正管理の原則，⑤責任明確化の原則

この5原則は，その後の日本の立法・ガイドラインの策定などに大きな影響を及ぼした。

4　NHK教育テレビ「情報化時代と法」出演

1983年4月から同年9月までの半年間で26回

4）神奈川県ではその検討過程を著作で公開してきた。神奈川県情報公開準備室編『情報公開：制度化をめざして』（ぎょうせい，1981年）はその初期の成果である。その他，多くの文献があるので，参照されたい。

5）行政管理庁行政管理局編集『プライバシー保護の現状と将来―個人データの処理に伴うプライバシー保護対策』（ぎょうせい，1982年）に収められている。当時の国際的動向等もかなり調査した。

（1回45分），NHK教育テレビで「情報化時代と法」という番組を制作し，出演する機会に恵まれた。それまでの研究・実践の成果についてテレビを通して広く伝達する機会となった。この番組では，情報と法にかかわる多数の問題を私なりに整理し，関連する資料をスタジオに持込み，ビジュアル化するように努めた。また，「情報化時代と法」と題するテキストも出した。個々の番組名を掲げるならば，当時，どのような問題があったかが分かるであろうが，ここでは，大きな項目を示すにとどめることにする。それは，次のようになる。

はじめに　人間と情報（1回）
Ⅰ　生活情報（3回）
Ⅱ　情報公開（7回）
Ⅲ　プライバシー（6回）
Ⅳ　マス・メディア（6回）
Ⅴ　コンピューター（2回）
おわりに　近未来の情報メディア（1回）

この放送は，視聴者からの問合せ，反響等からすると，テレビ放送の特性を活かして，情報公開の考え方・思想，プライバシー・個人情報保護の考え方・思想等を広範囲に伝える役割を果たしたといえる。

5　その他の情報法関係の関与学会・委員会・研究会・文献等

「情報法」というタイトルの文献が出版されるようになるのは，1990年代以降である（例，濱田純一『情報法』（有斐閣，1993年），堀部政男『自治体情報法』（学陽書房，1994年））といえるが，1980年代は，その基礎となる成果が多数蓄積されるようになった時代として特徴づけられるであろう。私がかかわった学会・委員会・研究会・文献等を例示的に掲げることにする（一部，1990年代初頭のものも含む）。

・『情報公開・プライバシー』（「ジュリスト」臨時増刊，1981年6月5日）
・情報通信学会設立（1983年）
・『高度情報社会の法律問題：ニューメディアの挑戦』（「ジュリスト増刊」，1984年）
・兼子仁・堀部政男・石川甲子男・茶谷達雄・吉原弘治編『自治体情報政策・情報システム』全5巻（労働旬報社，1985年-1986年）
・堀部政男『プライバシーと高度情報化社会』（岩波書店，1988年）
・堀部政男・永田真三郎編著『情報ネットワーク時代の法学入門』（三省堂，1989年）
・伊藤正己・堀部政男編『マスコミ判例百選（第2版）』（有斐閣，1985年）
・オーガスト・ベックウェイ著堀部政男・堀田牧太郎訳編『情報犯罪―コンピューター社会のバルネラビリティ』（啓学出版，1986年）
・自治大臣官房情報管理官室監修『個人情報保護対策の現状と課題―個人情報保護対策研究会中間報告』（きょうせい，1986年）
・自治大臣官房情報管理官室監修『地方公共団体における個人情報保護対策』（ぎょうせい，1987年）
・経済企画庁国民生活局消費者行政第一課編『民間部門における個人情報の保護（調査編）』，同課編『民間部門における個人情報の保護（資料編）』（大蔵省印刷局，1987年）
・総務庁行政管理局編集『行政機関における個人情報保護対策―情報化社会への対応』（ぎょうせい，1987年）
・イシエル・デ・ソラ・プール著堀部政男監訳『自由のためのテクノロジー：ニューメディアと表現の自由』（東京大学出版会，1988年）
・通商産業省編『コンピュータ社会と個人情報保護』（ケイブン出版，1989年）
・財団法人金融情報システムセンター編『金融機関等における個人データ保護』（（財）金融情報システムセンター，1991年）
・郵政省電気通信局監修・電気通信事業における個人情報保護に関する研究会編『電気通信事業とプライバシー保護』（第一法規，1991年）

それぞれの学会・委員会・研究会・文献等について説明したいことは多々あるが，ここでは，割愛させていただく。

Ⅵ　おわりに―展望

「はじめに」で述べたように，本稿では，時間の関係で1980年代までの展開を取り上げることができたにすぎない。「情報法」というタイトルを著作に使うようになった1990年以降については，今後，検討する予定である。

1970年代に地方公共団体で始まった情報法の実定法化（個人情報保護条例，情報公開条例等の制定）は，1990年代以降は，国レベルでも実定法化が進み，研究対象は拡大の一途を辿っている。これらに関しては諸外国においても多くの議論が交わされ，研究対象となる規範類もおびただしい数にのぼっている。

前掲の「法と政策」1981年12月号の「情報法」でまとめた「今後の展望」の一部は，今でも妥当すると考えるので，その一部を再掲することにする。そこでは，次のように書いた。

「このような状況のなかで，情報法の未来はバラ色であるが，しかし，こうした新しい研究分野も担い手が十分に存在しなければ発展することができない。その担い手も，法学界における各法分野にわたるばかりでなく，隣接諸科学，さらには，自然科学の分野にもわたらなければなりない。今後，ますます多くの研究者の共同作業が必要になってくる分野である。」

本誌「情報法制研究」ではもとより，情報法制研究所・情報法制学会でも問題状況を適時適切に把握し，問題提起をすることを期待する。

カナダのプライバシー・個人情報保護法

筑波大学図書館情報メディア系准教授
石　井　夏生利
ISHII Kaori

Ⅰ　はじめに

本稿は，カナダのプライバシー・個人情報保護に関する法制度の概要及びプライバシーに関する最近の動きを取り上げ，日本の今後の議論の発展に貢献することを目的とする。

プライバシー・個人情報保護の国際的な議論を見る時に，日本では，EU 及びアメリカの動向を注目する傾向がある。しかし，他の国や地域に目を向けることも比較法的な観点からは重要と考えられる。

カナダは，フランス及び英国の植民地時代を経て今日の独立国家を築いており，ヨーロッパと深い関係を有する。1931 年のウェストミンスター憲章採択以降，英連邦王国に属している。また，カナダは，北アメリカ大陸北部に位置しており，米国との間には 8,891 キロにも及ぶ米国との陸上国境がある。米国とは自由貿易協定により世界最大の貿易関係にあり，米国の経済的影響を常に受ける立場にある。カナダの政治制度は，立憲君主制，議院内閣制，連邦制が併用されている[1)]。

越境データ移転について，カナダは，2001 年 12 月 20 日，欧州連合（EU）から，個人情報保護及び電子文書法（Personal Information Protection and Electronic Documents Act, PIPEDA）が十分な保護レベル[2)] を有するとの認定を受けた[3)]。十分性認定は，カナダが EU にとって重要な貿易相手国であるという要素が勘案された結果である[4)]。また，オンタリオ州発祥の「プライバシー・バイ・デザイン」（Privacy by Design, PbD）が国際的な広がりを見せており，この概念は，プライバシー論議を牽引する役割を果たしている。

カナダのプライバシー・個人情報保護法制については，これまでも複数の成果が公表されてきた[5)]。しかし，それらは，やや期間が経過しているものや，特定のテーマに焦点を絞ったものであるため，改めて，カナダの動向を改めて取り上げる意味はあると考えられる。

日本では，2015 年 9 月 3 日に個人情報の保護に関する法律が改正された。その過程では個人情報の識別性及び匿名化が大きな論点として議論された[6)]。また，同じく注目を集めてきた越境データ流通に関しては，個人情報保護委員会が EU 及びアメリカ等との協力対話を進めている[7)]。この

1）　カナダの概要については，藤田直晴ほか著・日本カナダ学会編『はじめて出会うカナダ』（有斐閣，2009 年），日本カナダ学会のウェブ・サイト（http://jacs.jp/）等参照。

2）　EU データ保護指令第 25 条 1 項は，「加盟国は，取り扱われている又は移転後の取扱いが意図されている個人データの第三国への移転は，本指令の他の規定に従って採択された国内規定の遵守を侵すことなく，当該第三国が十分なレベルの保護措置を確保している場合に限って，行うことができることを定めなければならない。」と定め，十分な保護レベルを講じていない第三国へのデータ移転を禁止できる規定を置いている。EU データ保護指令は，2016 年 4 月 27 日付の一般データ保護規則の採択によって廃止されることとなったが，十分性の仕組みは同規則にも引き継がれている。

3）　Commission Decision C (2001) 4539, 2002 O.J. (L 2) (EU).

4）　European Commission, *Communication from the Commission to the European Parliament and the Council Exchanging and Protecting Personal Data in a Globalised World*, COM (2017) 7 final (Jan. 10, 2017), http://europa.eu/rapid/press-release_IP-17-16_en.htm.

ような個別論点を深く論じることも重要ではあるが，本稿では，全体的な視点から，EU及びアメリカとバランスを保ちつつ，プライバシー・個人情報保護制度を展開しているカナダの状況について，法制度，論点，PbDの取組を整理することとした。

Ⅱ　連邦法

1　管轄

カナダは，10の州（province）及び3の準州（territory）[8]で構成される連邦国家であるが，米国とは異なり，連邦優位の連邦制を採用している。そして，公的部門・民間部門それぞれに包括的な個人情報保護法が制定されている。1867年憲法法（Constitution Act, 1867）（1982年に英領北アメリカ法から改称）第92条及び第92A条は，州の組織や財政等，専属的な州の立法権限を定めている。連邦については，同法第91条に基づき，財政，郵便，通貨，国防，著作権等の専属的立法権限が定められている。同条29項は，「この法律により州の議会に専属的に付与された事項の部類の列挙から明らかに除外された事項の部類」と規定し，残余権限は連邦政府に属することを明らかにしている[9]。

しかし，プライバシーに関する権限は，1867年憲法法に定められていない。同法第92条13項は，「州の財政及び市民権」と定めているため，州が管轄を有するように見えるが，個人データが州を超えて移転する場合をカバーするものではない。同法第91条2項「通商の規制」が連邦法の管轄であること，第92条10項「州と他の州を結ぶか又は州の境界を越えるその他の工事及び事業」を除く地方工事及び事業が州法の管轄であること，第91条柱書の「カナダの治安，秩序，善政のために法律を制定すること」が連邦議会の役割とされていることからすると，連邦法の権限であるとも考えられる。

この問題は，個人情報保護及び電子文書法（PIPEDA）の制定により顕在化した。同法は，営利活動との関係で個人情報を取り扱う国内全ての民間事業者，及び，銀行や航空会社などの連邦規制事業において従業員情報を取り扱う事業者に適用される。同法第26条2項は，州内の民間事業者に規制が及ぶという問題を調整するために，カナダ総督において，州法がPIPEDAと「実質的に類似」（substantially similar）すると判断した場合に，命令により，当該州内で行われる個人情報の収集，利用又は開示から，同法の規律する組織又は活動を適用除外できる旨を定めている。現在は，ブリティッシュ・コロンビア州，アルバータ州，ケベック州の民間部門向け個人情報保護法，及び，オンタリオ州，ニュー・ブランズウィック州，ニューファンドランド＆ラブラドール州の個人健康情報に関する法律が実質的に類似するとの判断を受けている[10]。しかし，州内で行われる個人情報の収集，利用及び開示を規制する連邦の権限，連邦法及び州法の相互関係は，裁判所の判決で明らかにする必要がある[11]。

連邦法の管轄に特に異議を唱えているのは，ケ

5）長内了・佐藤信行「カナダの個人情報保護法」堀部政男編『情報公開・個人情報保護』ジュリスト増刊（1994年）297-301頁，佐藤信行「カナダ（個人情報保護法制の国際比較―民間部門を中心として―）」比較法研究第64号（2002年）38-47頁，消費者庁「諸外国等における個人情報保護制度の実態調査に関する検討委員会・報告書」（2009年3月）（http://www.ppc.go.jp/files/pdf/personal_report_2003caa_4.pdf）167-222頁（佐藤信行担当部分），消費者庁「諸外国等における個人情報保護制度の監督機関に関する検討委員会・報告書」（平成23年3月）（http://www.ppc.go.jp/files/pdf/personal_report_2303caa.pdf）125-145頁（河合理穂子担当部分），堀部政男・JIPDEC編『プライバシー・バイ・デザイン　プライバシー情報を守るための世界的新潮流』（日経BP社，2012年），新保史生「プライバシー・バイ・デザイン（特集　個人情報・プライバシー保護の理論と課題）」論究ジュリスト第18号（2016年夏号）16-23頁等。

6）高度情報通信ネットワーク社会推進戦略本部（IT総合戦略本部）「パーソナルデータに関する検討会」（http://www.kantei.go.jp/jp/singi/it2/pd/）。

7）個人情報保護委員会「各国機関との連携」（http://www.ppc.go.jp/enforcement/cooperation/cooperation/）。

8）連邦制度をとるカナダでは，州（province）に指定された地域以外を準州と呼ぶ。準州の自治権は限定的であり，立法権や行政権は連邦政府が持っている。また，歳入のほとんどを連邦政府から得ている。岸上伸啓「準州（Territory）」日本カナダ学会カナダ豆知識（http://jacs.jp/dictionary/dictionary-sa/09/19/653/）。

9）Constitution Acts, 1867 to 1982 (Can.). 邦訳は，国立国会図書館調査及び立法考課局『各国憲法集⑷カナダ憲法』（2012年3月）9-10頁，45-48頁参照。

ベック州である。同州の情報プライバシー委員会は，2003年12月11日に実質的に類似するとの判断が発効したことを受け，州の控訴裁判所に対し，PIPEDAの排他的管轄が憲法に違反すると主張して提訴した。しかし，その手続は2006年以降停止している[12]。また，ケベック州は，PIPEDAの十分性認定とは別に，民間部門の個人情報保護法について十分性を得るための手続を進めたものの，第29条作業部会[13]の「ケベックにおける個人データ保護に関する7/2014意見」（2014年6月4日付採択）[14]によって，ケベック法の適用範囲（州を超える場合），透明性の原則，アクセス権，「機微情報」の概念，転送の原則に関する課題が残されていると指摘され，十分な保護レベルを有するとの意見を受けることはできなかった。PIPEDAの十分性認定は，実質的に類似する法令を含むが[15]，ケベック州は，独自の行動を取ったことにより不安定な立場に置かれている。

2　連邦法

カナダには，連邦法として，公的部門を規律するプライバシー法（Privacy Act）[16]，民間部門を規律するPIPEDA[17]が存在する。

プライバシー法の背景には，1982年カナダ憲法法第1章「カナダ権利及び自由憲章」（Canadian Charter of Rights and Freedoms）[18]が存在している。その第7条は，人の生命，自由及び身体の安全に関する権利，第8条は不当な捜索及び押収を受けない権利を定めている。これらの規定はプライバシーを明示したものではない。しかし，連邦最高裁判所は，過去の判例を引用しつつ，プライバシー保護が自由かつ民主的な社会を守るために必要であること，プライバシー法が憲法類似の立場にあることを述べている[19]。プライバシーは，解釈により憲法上の保護を受けているといえる。

また，プライバシー法の基本理念を考える際には，情報へのアクセス法の対法として制定されているということが重要である。プライバシー法及びPIPEDAは，そもそも「情報へのアクセス法及びプライバシー法を制定し連邦裁判所法及びその他の関連法を改正する法律」（An Act to enact the Access to Information Act and Privacy Act, to amend the Federal Court Act, and to amend certain other acts in consequence thereof）という1つの法律の別表1及び2として制定されたものであり，一体としてでなければ理解できない部分が多いとされている[20]。

3　プライバシー法[21]

(1)　概　要

カナダでは，プライバシー法の制定に先立ち，1977年人権法（Human Rights Act）[22]第2条(b)項が，個人のプライバシー保護と個人情報を含む記録へのアクセスを定めていた[23]。プライバシー

10）Office of the Privacy Commissioner of Canada, *Provincial legislation deemed substantially similar to PIPEDA*, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/legislation-related-to-pipeda/provincial-legislation-deemed-substantially-similar-to-pipeda/ (last visited Jan. 20, 2017).

11）1 Barbara Mcisaac et al., The Law of Privacy in Canada 27-30 (2015).

12）Organizations in the Province of Quebec Exemption Order, SOR/2003-374 (Nov. 19, 2003), http://laws-lois.justice.gc.ca/eng/regulations/SOR-2003-374/page-1.html.

13）第29条作業部会は，監督機関又は各加盟国が指名した代表者，EUの機構等の代表者，欧州委員会の代表者で構成される助言機関である。一般データ保護規則では，欧州データ保護会議へと改組され，その権限は大幅に強化されている。

14）Article 29 Data Protection Working Party, *Opinion 7/2014 on the Protection of Personal Data in Quebec*, WP 219 (Adopted on Jun. 2014), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp219_en.pdf.

15）*Id.* at 4.

16）R.S.C., 1985, c. P-21.

17）S.C. 2000, c. 5.

18）Part 1 of the Constitution Act, 1982.

19）Lavigne v. Canada (Office of the Commissioner of Official Languages), [2002] S.C.C., 53, paras. 24, 25; Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401, [2013] S.C.C. 62, para. 22.

20）消費者庁・前掲「諸外国等における個人情報保護制度の実態調査に関する検討委員会・報告書」170頁。

21）消費者庁・前掲「諸外国等における個人情報保護制度の実態調査に関する検討委員会・報告書」及び同・前掲「諸外国等における個人情報保護制度の監督機関に関する検討委員会・報告書」参照。

22）1976-77, c.33, s.1.

23）*Supra* note 11, at 3-6.

法は，人権法の廃止とともに成立した。

プライバシー法は，1983年7月1日に施行された法律であり，全77条及び附則で構成される[24]。同法は，連邦政府機関が収集，利用及び開示する個人情報又は連邦政府の従業員の情報を保護するための規定を設けるとともに，個人に対し，連邦政府機関が保有する個人情報へのアクセス権及び訂正請求権を与えている（第2条）。

同法は，政府機関に対し，個人情報の収集を運用中の計画又は活動に直接関係するものに制限すること，可能な場合には直接本人から収集すること，個人に対し収集目的を通知すること，情報の正確性，最新性及び完全性を保障するための合理的措置を講じること，収集目的に沿う範囲内で個人情報を利用すること，本人の同意なき開示の原則禁止，利用又は開示に課する記録の保持等を義務づけている（第4条～第9条）。個人情報は，ある形態に記録されている識別可能な個人に関する情報をいうと定義され，(a)人種，国籍又は民族的出自，肌色，宗教，年齢又は既婚若しくは未婚の別，(b)個人の教育，医療，犯罪若しくは雇用の履歴に関する情報又は個人が関わっている金融取引に関する情報，(c)個人割り当てられた識別番号，記号その他細目，(d)個人の住所，指紋又は血液型，(e)個人の個人的意見又は見解，(f)黙示的又は明示的な私的又は秘密の性質を有する，個人から政府機関に送付された通信及びその返答，(g)個人に関する他者の意見，(h)個人への報償を与える目的で行われる他者の意見，(i)個人の名前であって，他の個人情報とともにその個人の情報を明らかにするであろうものなどが含まれる（第3条）。

同法は，政府機関の長に対し，政府機関が管理する個人情報を個人情報バンク（personal information banks）に登録し，その概要を公開するよう義務づけている。政府機関は，自己が管理しつつも個人情報バンクに登録していない情報の種類も公開しなければならない（第10条～第11条）。

個人は，個人情報バンクに含まれる個人情報へのアクセス権，訂正請求権等を有する（第12条～第28条）。

監督権限を行使するのは，同法に基づき設置された連邦プライバシー・コミッショナー（Privacy Commissioner of Canada）である。コミッショナーは，独任制の独立機関である。コミッショナーは，総督において，国璽の委任に基づき，上院及び下院の各承認された政党の代表と協議した後に，上院及び下院の決議を経て指名される。任期は7年間であり，再任可能である（第53条）。コミッショナーは政府から独立しており，議会へ直接報告義務を負う（第38条～第39条）。現コミッショナーは，ダニエル・テリエン（Daniel Therrien）氏である。

コミッショナーは，個人情報の違法な取扱い，個人情報へのアクセス拒否，個人情報へのアクセスの不当な遅延に関する苦情について，それを受けて調査する権限を有する。調査は職権によって行使することもできる。コミッショナーは，証言録取，資料の閲覧及び写しの取得，立入検査等の権限を有し，苦情に十分な理由があると認めるときは，政府機関の長に対し，認定事項及び勧告を含む報告書を提供する。適切な場合には，期間制限を付し，勧告に沿って講じられた措置又は措置が講じられなかった場合の理由を通知するよう，当該政府機関の長に求める（第29条～第35条）。コミッショナーは，交渉，仲裁及び和解を通じて，紛争を解決しようとするオンブズマン（又はホンブスツパーソン）として位置づけられており，不服申立に関する判断は拘束力を有しない。

アクセス権を拒否された個人は，コミッショナーに対して申し立てた苦情の結果を受領した後，連邦裁判所に提訴することができる。コミッショナー自身も，個人から同意を得ることにより，連邦裁判所に提訴することが認められる（第41条，第42条）。アクセス権以外のケースに関する提訴権は認められていない。

なお，法制度上の義務ではないが，カナダ財務省の指令に基づき，連邦政府機関[25]ではプライバシー影響評価が実施されている[26]。

同法は，制定から30年以上を経過しているが，大きな改正はなされていない。

24）関連する規則及び命令については下記のウェブ・ページ参照（https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/r_o_a/）。

25）プライバシー法第3条の定める政府機関を対象とする。

⑵ コミッショナーによる改正提案

連邦議会の情報アクセス・プライバシー及び倫理に関する常設委員会（Standing Committee on Access to Information, Privacy and Ethics）は，2016年3月から11月にかけてプライバシー法の調査を行った。コミッショナーは，下記の3つのテーマに基づく法改正を提案している[27]。

テーマ1：技術的変化

1　情報共有に関する合意の要件を明確化すべきである。
2　政府機関による個人情報の安全保護措置に関する義務を法定すべきである。
3　個人情報の侵害に関するコミッショナーへの報告を義務化すべきである。

テーマ2：立法的現代化

4　収集のための明確な必要条件を設けるべきである。
5　コミッショナーの権限について，苦情調査のためのオンブズパーソンモデル形態から拘束的命令を下す権限に置き換えるべきである。
6　コミッショナーへのプライバシーに関する苦情を独立審査するための制定法上の仕組みを設けるべきである。
7　新規又は重大な変更が加えられた計画について，政府機関にプライバシー影響評価を義務づけ，実施に先立ちコミッショナーに提出することを義務づけるべきである。
8　政府機関に対し，プライバシーとの関係性を協議するために，立法及び規則案を提出するに先立ち，それらをコミッショナーへ提出するよう義務づけるべきである。
9　コミッショナーに対する，一般への教育及び研究の任務を明文化すべきである。
10　本法を5年ごとに見直すべきである。

テーマ3：透明性の強化

11　政府機関のプライバシー問題が公益に関係する場合は，コミッショナーの守秘義務を解除して一般に公表する裁量を与えるべきである。
12　執行協力のために，コミッショナーが国内外の相手と情報を共有する能力を拡大すべきである。
13　コミッショナーに対し，苦情が些細な場合など特定の理由に基づく場合に，苦情を拒否し調査を停止する裁量を与えるべきである。
14　広範なプライバシー問題や，法執行機関から受けた適法なアクセス請求について，政府機関の報告義務を強化し，透明性を高めるべきである。
15　大臣の事務所，首相の事務所，及び外国へのアクセス権に本法の適用範囲を拡大すべきである。
16　個人情報のアクセス請求の例外を制限すべきである。

4　個人情報保護及び電子文書法[28]

⑴ 概　要

個人情報保護及び電子文書法（PIPEDA）は，民間部門における個人情報の取扱いを定めている。同法は，2000年4月13日に成立し，2001年から2004年にかけて段階的に施行された。最終改正は2015年6月23日である。PIPEDAは，前半が個人情報保護法，後半が電子文書法で構成されている。コミッショナーの監督権限は，同法に基づき民間部門にも及ぶようになった。

同法は，営利活動の過程での個人情報の取扱いに関する基本的規則を定めている。その目的は，技術が情報の流通及び交換を一層促進する時代において，個人情報に関する個人のプライバシー権を認識するとともに，当該状況で通常人が適切と考える目的のために組織が個人情報を収集，利用又は開示する必要性を認識する方法において，個人情報の収集，利用及び開示を対象とする規則を

26）OPC, *Privacy Impact Assessments*, https://www.priv.gc.ca/en/about-the-opc/opc-operational-reports/opc-privacy-impact-assessments/ (last visited Jan. 20, 2017). 指令は2010年4月1日に施行された。

27）OPC, Review of the Privacy Act - Revised recommendations (Nov. 1, 2016), https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/pa_r/pa_ref_rec_161101/.

28）OPC, *An Overview of the Office of the Privacy Commissioner of Canada and Federal Privacy Legislation*, https://www.priv.gc.ca/en/about-the-opc/publications/guide_ind/ (last visited Jan. 20, 2017).

設けることにある（第3条）。

同法は，現実世界とオンライン世界を問わず，事業規模を問わず平等に適用される。PIPEDAはカナダの民間事業者に適用されるが，前記の通り，実質的に類似すると判断した州法はその適用を除外される。しかし，その判断を受けた州であっても，無線局及びテレビ局，航空会社，鉄道会社及び通信事業者等の連邦規制事業者による従業員情報の取扱いには法が適用される（第4条1項(b)号，第26条2項）。また，PIPEDAは，民間事業者が関与する営利取引の過程で，州又は国を超えて流通する全ての個人データに適用される。

PIPEDAは，プライバシー法が適用される政府機関，ジャーナリズム，芸術又は文学目的のみで個人情報を収集，利用又は開示する組織，私的目的で個人情報を収集，利用，開示する個人には適用されない（第4条2項）。

組織の従業員の氏名，肩書き，勤務先住所，電話番号及び電子メールアドレスには適用されない（第2条）。ただし，連邦規制事業者の従業員及び採用応募者の情報は適用対象である。

個人情報は識別できる個人に関する情報を意味する（第2条1項）。個人の氏名，人種，民族的出自，宗教，既婚未婚の別，学歴，電子メールアドレス及びメッセージ，IPアドレス，年齢，身長，体重，医療記録，血液型，DNAコード，指紋，声紋，収入，購買履歴，支出習慣，銀行情報，クレジット／デビットカード情報，借入れ又は信用報告，納税申告，社会保障番号又は他の識別番号が含まれる。一般的に，個人情報の範囲は広く解釈され，多くの関連裁判例が出されている[29)]。

PIPEDAは，民間事業者による個人情報の収集，利用又は開示について，附則1に列挙されたカナダ規格協会の「個人情報保護に関するモデルコード」[30)]の遵守を求めており，この諸原則が基本的なプライバシーの義務となっている（第5条1項）。

本則では，諸原則の例外を定めるという手法が取られている（第7条～第9条）。

諸原則の概要は次の通りである。

第1原則　説明責任

組織は，諸原則の遵守を監視するプライバシー保護の責任者を指名する。組織は，情報が第三者によって取り扱われる間，契約又は他の手段により同等の保護レベルを提供する。組織は，個人情報の保護手順を実施し，苦情や問い合わせに対応する手続を設け，従業員を訓練し，組織の方針や手順を説明することなどにより，諸原則を実践する方針及び実務を実施する。

第2原則　目的の特定

組織は，収集前又は収集時に個人情報の収集目的を特定しなければならない。組織は，個人情報の収集目的を明確化する。収集目的は口頭又は文書により個人に通知される。収集時の目的以外で利用する場合，新たな目的は利用前に特定される。法の定める場合を除き，利用に先立ち個人の同意が必要である。この原則は，第4及び第5原則と密接に関連する。

第3原則　同意

個人情報の収集，利用又は開示について，個人の「認識及び同意」が必要である[31)]。組織は，通常，収集時に利用又は開示への同意を取得するが，利用目的を変更するような場合には，利用前に，利用又は開示への同意を取得する。組織は，製品又はサービスの提供条件として，明示的に特定された適法な目的を達成するために必要な範囲を超えて情報を収集，利用又は開示することについて，個人に同意を求めてはならない。同意の取得には，個人の合理的な期待

29）OPC, *PIPEDA Interpretation Bulletins*, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/ (last visited Jan. 20, 2017).

30）Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96.

31）法，医療，安全上の理由から同意を求めることが不可能又は非現実的な場合がある。法執行目的である場合や，本人が未成年，重症患者，精神的に不能な場合などが当てはまる。個人と直接の関係を持たない組織，例えば，慈善団体やダイレクトマーケティングを行う組織が他の組織からメーリングリストを受領するような場合には，提供者側が開示前に同意を取得することが期待される。

も関係する。組織が同意を求める方法は状況によって異なり得るが，機微性の高い情報は，一般的に明示的な同意を求めるべきである。個人は，法的又は契約上の条件に従い，いつでも同意を取り消すことができる。

第 4 原則　制限的収集

個人情報の収集は，組織が特定した目的に必要なものに制限される。情報は，適切かつ適法な手段により収集される。収集される情報の量と種類は，特定した目的を満たすために必要なものに限定される。この原則は，第 2 及び第 3 原則と密接に関係する。

第 5 原則　制限的利用，開示及び保持

個人情報は，個人の同意がある場合又は法により義務づけられる場合を除き，収集目的以外の目的で利用又は開示されてはならない。個人情報は，目的を達成するために必要な期間のみ保持される。目的達成のために必要ではなくなった個人情報は，破棄，消去又は匿名化されるべきである。この原則は，第 2，第 3，第 9 原則と密接に関係する。

第 6 原則　正確性

個人情報は，利用目的に必要な限りで正確，完全かつ最新でなければならない。組織は，情報の収集目的を達成するために必要でない限り，個人情報を日常的に更新してはならない。第三者に開示された情報を含む，継続的に利用される個人情報は，正確性の義務が明確に制限されない限り，一般的に正確かつ最新であるべきである。

第 7 原則　安全保護

個人情報は，情報の機微性に適した安全保護措置によって保護される。安全保護措置は，個人情報の紛失又は盗難，無権限アクセス，開示，複写，利用又は修正から保護する。保護措置には，物理的，組織的及び技術的措置を含む。

第 8 原則　公開

組織は，個人情報の管理に関する方針及び実務についての特定の情報を個人が容易に利用できるようにする。

第 9 原則　個人のアクセス

請求に基づき，個人は，自己の個人情報の存在，利用，及び開示についての通知を受け，当該情報へのアクセスを与えられる。個人は，適切な場合には，情報の正確性及び完全性に異議を唱え，訂正させることができる[32)]。請求に基づき，組織はその個人に関する個人情報を保有しているか否かを個人に伝えなければならず，情報源を示すことが奨励される。加えて，組織は，当該情報の利用理由，及び，情報を開示した第三者に関する説明を提供すべきである。個人において個人情報が不正確又は不完全であることをうまく立証できた場合，組織は請求に応じて情報を修正しなければならない。修正は，異議が出された情報の性質に応じて，情報の訂正，削除，又は追加を含む。適切な場合，修正された情報は，当該情報にアクセスできる第三者に送信される。異議が個人の満足する形で解決されない場合，未解決の異議の内容は組織によって記録される。適切な場合には，未解決の異議は，当該情報にアクセスできる第三者に送信される。

第 10 原則　遵守の問題

個人は，上記の諸原則の遵守に関する問題を組織の遵守責任者に対処させることができる。組織は，苦情処理手順を設け，全ての苦情を調査しなければならない。

第 3 原則との関係で，個人の同意は，組織の活動が向けられる個人において，個人が同意をした個人情報の収集，利用，開示の性質，目的及び結果を理解することが合理的に期待される場合に限り有効であると定められている（第 6.1 条）。

個人は，PIPEDA に違反する個人情報の取扱いについて，組織の苦情対応の結果に満足しなかった場合には，コミッショナーに苦情を申し立て

32）　一定の状況では，組織は，個人に関して保有する全て個人情報へのアクセスを提供できない場合がある。アクセス義務の例外は限定的かつ具体的でなければならない。アクセスを拒否する理由は，請求に基づき個人に提供すべきである。例外には，提供するのに法外な費用を要する情報，他者への言及を含む情報，法的，安全上又は営利的な独占販売上の理由により開示できない情報，及び，弁護士と依頼者又は訴訟上の特権に服する情報が含まれる。

ることができる。コミッショナーは，職権でも苦情調査を開始することができる（第11条）。コミッショナーは，証言録取，証拠の受領，立入検査，記録の写しの取得等の権限を有する。また，仲裁又は和解といった紛争解決手段を用いる場合がある。コミッショナーは，苦情対応の開始から1年以内に，認定事項及び勧告，当事者が達した和解，適切な場合には，期間制限を付し，勧告に沿って講じられた措置又は措置が講じられなかった場合の理由を通知すべきことなどを記した報告書を用意し，当事者に送付する（第11条～第13条）。コミッショナーは，PIPEDA違反に対して制裁金や損害賠償を命じる権限はない。

個人は，コミッショナーの報告を受けた後又は苦情調査を行わない旨の通知を受けた後，原則として1年以内に，苦情を連邦裁判所に持ち込むことができる（第14条）。コミッショナーも個人に代理して苦情を持ち込むことができる（第15条）。裁判所は，組織に対し，違反実務を正すこと，組織の是正措置を公表すること，個人が被った侮辱等の被害を賠償することを命じることができる（第16条）。コミッショナーは，組織がPIPEDAに違反し又は勧告に従わないと信じる合理的理由がある場合には，組織との間で遵守合意を結び，コミッショナーによる提訴等を停止することができる（第17.1条）。同様の要件の下で，監査を実施する権限も有する（第18条）。

コミッショナーは，PIPEDA及び実質的に類似と判断された州法の適用について，議会への年次報告義務を負う（第25条）。その他の権限及び職務としては，一般への啓蒙，議会の立法提案への指針提供，議会，個人，組織による問い合わせへの回答，国際協力等がある。

以上の他，コミッショナーには，カナダラジオテレビ・電気通信委員会（Canadian Radio-television and Telecommunications Commission）及び連邦競争局（Federal Competition Bureau）とともに，反スパム法（Canada's anti-spam legislation）[33]の監督権限を有している。

⑵　2015年改正

PIPEDAは，2015年6月18日，デジタルプライバシー法（Digital Privacy Act）[34]により改正された。同法の改正事項は多岐にわたっており，有効な同意の要件としての個人の合理的期待，コミッショナーと組織間の遵守合意，公益性が認められる場合におけるコミッショナーの守秘義務の解除，事業活動上の電子メールの適用除外，連邦事業の範囲の拡大，係る事業の採用応募者情報の保護，詐欺の探知・予防目的のための同意の例外，事業承継等に伴う同意なき個人情報の利用又は開示，出訴期間の短縮化[35]等に及んでいる。

特に重要な改正事項は，データ侵害報告制度の新設である[36]。組織は，その管理する個人情報について，安全保護措置違反（データ侵害）が，個人に重大な被害を与える現実的危険をもたらすと合理的に信じる場合，コミッショナー及び影響を受ける個人に対し，係るデータ侵害を報告しなければならない。加えて，他の組織や政府機関が被害を軽減できるなど，一定の要件を満たす場合には，他の組織等にも通知しなければならない。小売業者がクレジットカード発行銀行又は法執行機関に通知する場合等が該当する。データ侵害を起こした組織は，侵害に関する全てを記録しなければならず，コミッショナーの要請があれば記録を提出しなければならない（改正後の第10.1条）。報告・通知義務や記録義務に違反する行為は，最高10万ドルの罰金に処せられる。

データ侵害とは，個人情報の紛失，無権限アクセス又は無権限開示であって，組織の安全保護措置違反又は係る措置を講じなかったことから生じるものをいう（第2条1項）。「重大な被害」には，身体的被害，侮辱，名誉又は関係性の侵害，雇用，事業又は職業上の機会の喪失，財政的損失，なりすまし，信用記録への悪影響及び財産的損失が含まれる。

データ侵害報告制度の改正は，カナダ産業省による連邦規則が制定された後に施行される。その他は女王の裁可を得た2015年6月18日に施行された。

33）S.C. 2010, c. 23.
34）Bill S-4.
35）1年から45日以内に変更された。
36）2015, c.32, s.10.

⑶ 同意とプライバシー

コミッショナーは，2016年5月，「同意とプライバシー」と題する討議文書を公表した。これは，PIPEDAの要は同意であるという認識に基づき，スマートフォン，クラウド・コンピューティング等の技術や，個人情報への無制限アクセス及び自動処理等の企業実務の変化を踏まえ，同意モデルの改善又は代替策の提案，主たる論点の概要を述べること等を内容とする[37]。個人は，ビッグデータ・IoT（Internet of Things）によるビジネスモデルが変化する中で，プライバシーに関する意思決定の責任を負わされているが，一旦組織に収集された情報について，何が生じているかを完全に理解することはできない。そこで，報告書では，1）同意の強化，2）同意の代替策，3）アカウンタビリティに基づくガバナンス，4）執行モデルの見直しを検討事項に掲げている。

1）では，プライバシーポリシー及び通知における透明性の向上，メタデータのタグ付け等によるサービスを跨いだプライバシー選好の管理，技術特有の安全保護措置の設定，プライバシーの初期設定（PbD），2）では，匿名化，「禁止区域」（“No-Go Zones”）の設定，適法な事業上の利益のための例外の拡大，3）では，実務規範による透明性及び公開性，プライバシー・トラストマークの設定，自主的取組がそれぞれ列挙されている。

2）のうち，「禁止区域」は，個人情報の収集，利用及び開示を通常人が当該状況で適切と考える目的のためにのみ認めることを定める第5.3条を発展させ，不適切な利用を禁止するという考え方である。また，報告書では，「注意ゾーンを進める」（“Proceed with Caution Zones”）と題し，機微情報などの特定種類の情報，自動化された個人に関する決定やプロファイリングなどの特定の取扱い，又は一定の脆弱な集団を保護するための手続を強化するという考え方も示されている。

4）では，命令権限を持たないというコミッショナーの問題意識が明らかにされている。

Ⅲ 州 法

1 特 徴

個人情報保護法は，全ての州で制定されている。いくつかの特徴を挙げると，次の通りである。

情報自由及びプライバシー保護法（Freedom of Information and Protection of Privacy Act, FIPPA, FOIP, FOIPP）は，公的機関に適用され，情報へのアクセス権及び個人情報の取扱いに関する一定の規律を定める[38]。この法令は全ての州で定められている。同法に加え，いくつかの州では，地方の公的機関に関する情報自由及びプライバシー保護法が制定されている。

個人情報保護法（Personal Information Protection Act, PIPA）は，民間事業者に適用され，個人情報の取扱いに関する一定の規律を定める[39]。民間事業者に適用される一般法は，一部の州が制定している。

健康情報の保護に関する各法令は，医療分野に特化したものであり，医療従事者が管理する健康情報へのアクセス権を個人に与えるとともに，健康情報の取扱いに関する規律を定める。

プライバシー法（Privacy Act）を定める州もある。これは，連邦のプライバシー法とは異なり，プライバシー侵害を不法行為とし，損害賠償や差止請求を認めるものである。

監督機関については，情報プライバシー・コミッショナー（Information and Privacy Commissioner）を設置する州が多い。拘束的命令権限を有する監督機関もあれば，オンブズマンを設置する州，委員会制を採用する州もある。監督機関は，情報へのアクセス権に関する不服申立ての調査，仲裁及び解決，プライバシーに関する苦情の調査及び解決，違反事例の職権調査，立法提案，計画又は方針に関する意見提供，新技術及び／又はデータ・マッチング計画とプライバシーとの関連性に関する意見提供，アクセス権とプライバシー権に影響を与えるあらゆる事項の調査，一般への啓蒙とい

37） OPC, *Consent and Privacy* (May, 2016), https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/consent_201605/.

38） 州によって略称は異なる。

39） 同上。

った権限を有する。監督機関の命令権限がない場合は，裁判所への申立手続が設けられている。監督機関は，州議会に属する独立官であること，州議会に任命されること，州議会に直接報告を行うことなどによって，独立性が担保されている。

2　ブリティッシュ・コロンビア（British Columbia）州

⑴　主な法令

・情報自由及びプライバシー保護法（FIPPA）[40]：1992年6月制定。
・個人情報保護法（PIPA）[41]：2003年10月23日制定。同法は，2004年10月12日，PIPEDAと「実質的に類似」する法令であると認められている。同法第30.1条は，公的機関の管理する個人情報について，原則としてカナダ内でのみ保存及びアクセスしなければならない旨を定めている。データローカライゼーションを定めた規定である。
・電子健康（個人健康情報へのアクセス及びプライバシー保護）法（E-Health (Personal Health Information Access and Protection of Privacy) Act）[42]
・プライバシー法[43]

⑵　監督機関[44]

情報プライバシー・コミッショナーは，1993年に設立された。コミッショナーは，FIPPA及びPIPAの監督権限を有する。現コミッショナーはドリュー・マッカーサー（Drew McArthur）氏である。コミッショナーには拘束的命令権限がある。

3　アルバータ（Alberta）州

⑴　主な法令

・情報自由及びプライバシー保護法（FOIP）[45]：1994年6月制定，1995年10月1日施行。
・個人情報保護法（PIPA）[46]：2003年12月4日制定，2004年1月1日施行。同法は，2004年10月12日，PIPEDAと「実質的に類似」する法令であると認められている。2010年5月1日の改正によりプライバシー侵害通知の制度が導入された。
・健康情報法（Health Information Act, HIA）[47]：同法に基づきプライバシー影響評価が義務づけられている。

⑵　監督機関[48]

独立監督機関は，情報及びプライバシー・コミッショナーである。現コミッショナーは，ジル・クレイトン（Jill Clayton）氏である。コミッショナーは，拘束的命令権限を有している。

コミッショナーは，上記3つの法令の監督権限に加え，自動車情報アクセス規則（Access to Motor Vehicle Information Regulation）に基づく審査権限を有する。

4　サスカチュワン（Saskatchewan）州

⑴　主な法令

・情報自由及びプライバシー保護法（FOIP）[49]：1991年制定，1992年4月1日施行。
・地方機関の情報自由及びプライバシー保護法（LA FOIP）[50]
・健康情報保護法（Health Information Protection Act, HIPA）[51]

⑵　監督機関[52]

独立監督機関は，情報プライバシー・コミッショナーである。現コミッショナーは，ロナルド・J・クルゼニスキー（Ronald J. Kruzeniski）氏である。

コミッショナーは，上記3つの法令に基づく監督を行うが，命令権限は有しない。

40）R.S.B.C. 1996, c. 165.
41）S.B.C. 2003, c. 63.
42）S.B.C. 2008, c. 38.
43）R.S.B.C. 1996, c. 373.
44）Office of the Information & Privacy Commissioner for British Columbia, https://www.oipc.bc.ca/ (last visited Jan. 20, 2017).
45）R.S.A. 2000, c. F-25.
46）S.A. 2003, c. P-6.5.
47）R.S.A. 2000, c. H-5.
48）Office of the Information and Privacy Commissioner of Alberta, https://www.oipc.ab.ca/legislation.aspx, (last visited Jan. 20, 2017).
49）S.S. 1990-91, c. F-22.01.
50）S.S. 1990-91, c. L-27.1.
51）S.S. 1999, H-0.021.
52）Office of the Saskatchewan Information and Privacy Commissioner, http://www.oipc.sk.ca/ (last visited Jan. 20, 2017).

5　マニトバ（Manitoba）州

⑴　主な法令

・情報自由及びプライバシー保護法（FIPPA）[53]：1997年6月28日制定，1998年5月4日施行。
・個人健康情報法（Personal Health Information Act, PHIA）[54]：1997年6月28日制定。
・プライバシー法[55]

⑵　監督機関[56]

独立監督機関はマニトバ州のオンブズマンである。現在は，シャーリーン・パキン（Charlene Paquin）氏が務めている。オンブズマンには，FIPPA及びPHIAに加えて，オンブズマン法，公益開示（内部通報者保護）法（Public Interest Disclosure (Whistleblower Protection) Act, PIDA）に基づく苦情調査権限が与えられている。

その他，オンブズマンは，死亡調査法に基づく検視報告書の勧告，児童及び家族サービス法に基づく児童死亡審査報告書の勧告の実施を監督している。

6　オンタリオ（Ontario）州

⑴　主な法令

・情報自由及びプライバシー保護法（FIPPA）[57]：1988年1月1日制定。
・地方情報自由及びプライバシー保護法（Municipal Freedom of Information and Protection of Privacy Act, MFIPPA）[58]：1991年1月制定。
・個人健康情報保護法（Personal Health Information Protection Act, PHIPA）[59]：2004年5月20日制定，同年11月1日施行。同法は，2005年11月28日にPIPEDAと「実質的に類似」する法令であると認められている。

⑵　監督機関[60]

独立監督機関は，情報プライバシー・コミッショナーである。現コミッショナーは，ブライアン・ビーミッシュ（Brian Beamish）氏である。コミッショナーは上記各法令の監督を行い，命令権限も有している。

7　ケベック（Quebec）州[61]

⑴　主な法令

唯一のフランス語圏であるケベック州は，公的部門及び民間部門の包括的法令を定めた州として，情報自由及び個人情報保護法のパイオニアといわれている。

ケベック州の人権及び自由憲章（Charter of Human Rights and Freedoms）[62]の第5条は，「何人もその私生活を尊重される権利を有する。」と定めており，プライバシー権を保障したものと解釈されている。個人情報保護に関する主な法令は次の通りである。

・公的機関が保有する文書へのアクセス及び個人情報保護を尊重する法律（An Act respecting access to documents held by public bodies and the protection of personal information）[63]：1982年制定。
・民間部門における個人情報保護を尊重する法律（An Act respecting the protection of personal information in the private sector）：1993年6月制定，1994年1月1日一部を除いて施行。同法は，2003年12月11日，PIPEDAと「実質的に類似」する法令であると認められている[64]。
・ケベック州民法第35条～第41条（Extracts from the Civil Code of Québec, articles 35 to 41）[65]

ケベック州民法は，第2編第3章に「名誉及びプライバシーの尊重」を設け，第35条で「何人も，自己の名誉及びプライバシーを尊重される権利を有する」と定めている。第36条は，プライバシーの侵害態様，第37条は，他者に関するファイルを作成する者は，重大かつ適法な理由を有しなければならないこと，第38条は，本人によ

53）C.C.S.M., c. F175.
54）C.C.S.M., c. P33.5.
55）C.C.S.M., c. P125.
56）Manitoba Ombudsman, https://www.ombudsman.mb.ca/ (last visited Jan. 20, 2017).
57）R.S.O. 1990, c. F.31.
58）R.S.O. 1990, c. M.56.
59）S.O. 2004, c. 3, Schedule A.
60）Information and Privacy Commissioner of Ontario, https://www.ipc.on.ca/ (last visited Jan. 20, 2017).
61）*Supra* note 11, at 4-95-4-110.
62）R.S.Q., c. C-12.
63）R.S.Q., c. A-2.1.
64）R.S.Q., c. P.39-1. PIPEDAの憲法適合性及びEUの十分性との関係は，前記Ⅱ1参照。
65）C.C.Q.-1991. 1991, c.64.

るファイルの閲覧及び訂正権，第39条は，ファイルを作成する者は，ファイルに含まれる情報への当該個人のアクセスを拒否してはならないこと，第40条は，ファイルの正確性，完全性，確実性，第41条は，個人の権利行使の条件及び態様を決定する裁判所の権利を定めている。

上記の民間部門における個人情報保護法は，民法第35条から第40条の定める権利行使のために，民法第1525条[66]の意味する事業活動の過程で，他者に関する個人情報の収集，保有，利用又は第三者への提供についての特定の規則を設けることにある。民法を補完するために制定された法律という点においても特殊性がある。

⑵　監督機関

情報プライバシー委員会（Commission d'accès à l'information du Québec）が監督権限を有する。委員長はジャン・シャルティエ（Me Jean Chartier）氏である[67]。委員会は委員長及び副委員長を含めて最低5名で構成され，監視部門及び仲裁部門に分かれている。委員は，首相の申し立てに基づき，州議会の3分の2以上の賛成により任命される。

委員会の監視部門は，公的部門の法令について，法の適用及び法が遵守されている程度を調査する，公的機関同士で締結された合意を承認する，本法に基づく規則案等への意見を述べる，個人情報の提供に関する登録簿を保持するための規則を定める，公的機関が保有するファイル内の個人情報の機密性が保持されているか否かを確認する，といった権限を有する。委員会は，ファイルに含まれる個人情報の機密性が尊重されているか等を調査し，必要に応じて命令を下す権限を有する。委員会は，文書へのアクセスや個人情報保護に関する拒否決定を受けた個人の申立てを審査する権限を有する。委員会は，当事者の権利を保護するために適切を考える命令を下し，事実又は法に関するあらゆる問題を判断することができる。

委員会は，民間部門の法令については，個人情報へのアクセス若しくは訂正，又は，利害関係人から提出されたマーケティングリストに関する第25条[68]の適用についての争いを調査し，決定を下す権限を有する。委員会には，個人情報保護に関するあらゆる事柄や企業による情報の取扱実務について，職権又は苦情申し立てにより，調査を行う権限を有し，勧告又は命令を下す権限を有する。委員会は，5年ごとに州議会に民間部門法の適用に関する報告書を提出しなければならない。

8　プリンス・エドワード・アイランド（Prince Edward Island）

⑴　主な法令

・情報自由及びプライバシー保護法（FOIPP）[69]：2001年5月15日制定，2002年11月1日施行。

⑵　監督機関

情報プライバシー・コミッショナーが監督権限を有する。現コミッショナーは，カレン・A・ローズ（Karen A. Rose）氏である。コミッショナーには拘束的命令権限が与えられている。

9　ニュー・ブランズウィック（New Brunswick）州

⑴　主な法令

・情報への権利及びプライバシー保護法（Right to Information and Protection of Privacy Act, RTIPPA）[70]：2009年6月19日制定，2010年9月1日施行。同法は，1998年個人情報保護法及び1978年情報権法を廃止する形で制定された。
・個人健康情報のプライバシー及びアクセス法（Personal Health Information Privacy and Access Act）[71]：2009年6月19日制定。同法は，2011年11月17日，PIPEDAと「実質的に類似」する法令であると認められている。

66）1名以上の者が組織的な経済活動を実施することは，本質的に営利的であるか否かにかかわらず，財の生産，管理，譲渡，又はサービスの提供で成り立っており，それは事業活動を構成する。

67）Commission d'accès à l'information du Québec, http://www.cai.gouv.qc.ca/ (last visited Jan. 20, 2017).

68）何人も，自己に関する個人情報をマーケティングリストから除外して欲しい場合は，いつでも，リストの保有者又は利用者に対し，口頭又は文書の請求により，情報を削除させる権利を有する。

69）C. F-15.01.

70）S.N.B. 2009, c. R-10.6.

71）S.N.B. 2009, c. P-7.05.

⑵　監督機関[72]

情報アクセス・プライバシー・コミッショナーが監督権限を有する。現コミッショナーは，アン・E・バートランド（Anne E. Bertrand）氏である。RTIPPAの制定以前は，オンブズマン法に基づく監督制度が設けられていたが，RTIPPAに基づき，新たにコミッショナーが設置された。旧法との違いは，コミッショナーに苦情調査権限が与えられた点である。ただし，コミッショナーに命令権限はない。

10　ノバ・スコティア（Nova Scotia）州

⑴　主な法令

・情報自由及びプライバシー保護法（FIPPA）[73]：1993年制定，1994年施行。
・地方政府法[74]：1999年制定。地方の情報自由及びプライバシー保護法である。
・プライバシー審査官法（Privacy Review Officer Act, PRO Act）[75]：2009年9月制定。この法律は，市民が州の公的機関によってプライバシーを侵害されたと感じた場合には，コミッショナーに苦情を申し立てることができる。
・個人健康情報法（PHIA）[76]：2012年5月制定，2013年6月1日施行。
・個人情報国際開示保護法（Personal Information International Disclosure Protection Act）[77]：同法は，州のデータ・ローカライゼーション法である。公的機関及び地方政府は，それらが保有するあらゆる個人情報（サービス提供者が代わりに行動する場合を含む）が，原則として，カナダ内に保持され，カナダ内でのみアクセスされ，開示されることを保障する義務を負う。

⑵　監督機関[78]

情報プライバシー・コミッショナーが監督権限を有する。現コミッショナーは，キャサリン・トゥリー（Catherine Tully）氏である。コミッショナーは，独立のオンブズパーソンであり，命令権限を有しない。

11　ニューファンドランド＆ラブラドール（Newfoundland & Labrador）州

⑴　主な法令

・2015年情報へのアクセス及びプライバシー保護法（Access to Information and Protection of Privacy Act, ATIPPA）[79]：2015年6月1日制定。同法については，2005年施行の情報自由法が存在していたが，見直しにより新法が制定された。
・個人健康情報法（Personal Health Information Act, PHIA）[80]：2008年6月4日制定。同法は，2012年10月10日にPIPEDAと「実質的に類似」の法令である旨の認定を受けている。
・プライバシー法[81]

⑵　監督機関[82]

ATIPPA及びPHIAの監督は，情報プライバシー・コミッショナーが担っている。現コミッショナーは，ドノヴァン・モロイ（Donovan Molloy）氏である。命令権限は付与されていないが，勧告を執行するために裁判所への申立を行うことができる。

12　ユーコン（Yukon）準州

⑴　主な法令

・情報アクセス及びプライバシー保護法（Yukon AIPPA）[83]
・健康情報プライバシー及び管理法（Health Information Privacy and Management Act, HIPMA）[84]：2016年8月31日施行。

72）Office of the Access to Information and Privacy Commissioner, New Brunswick, http://www.info-priv-nb.ca/ (last visited Jan. 20, 2017).
73）1993, c. 5. 1977年に情報自由法を制定した最初の州である。
74）1998, c. 18.
75）2008, c. 42.
76）2012, c. 31.
77）2006, c. 3.
78）Office of the Information and Privacy Commissioner, Nova Scotia, https://foipop.ns.ca/ (last visited Jan. 20, 2017).
79）S.N.L. 2015, c. A-1.2.
80）S.N.L. 2008, c. P-7.01.
81）R.S.N.L. 1990, c. P-22.
82）Office of the Information and Privacy Commissioner, http://www.oipc.nl.ca/ (last visited Jan. 20, 2017).
83）R.S.Y. 2002, c.1.
84）S.Y. 2013, c. 16.

⑵　監督機関[85]

情報プライバシー・コミッショナーが監督権限を有する。現コミッショナーは，ダイアン・マクレオド-マッケイ（Diane McLeod-McKay）氏である。オンブズマン法に基づき指名される。

13　ヌナブト（Nunavut）準州

⑴　主な法令

・情報アクセス及びプライバシー保護法（ATIPP）[86]：1996年12月31日及び2007年12月31日施行。

⑵　監督機関[87]

情報プライバシー・コミッショナーがATIPPの監督権限を有する。現コミッショナーは，エレイン・ケナン・ベンゲ（Elaine Keenan Bengts）氏である。命令権限はない。

14　ノースウェスト準州（Northwest Territories）[88]

⑴　主な法令

・情報アクセス及びプライバシー保護法（ATIPP）[89]：1996年12月31日施行。

・健康情報法[90]：2015年10月1日施行。

⑵　監督機関

ヌナブト準州と同様，エレイン・ケナン・ベンゲ氏である。

Ⅳ　プライバシー・バイ・デザイン[91]

プライバシー・バイ・デザイン（PbD）は，カナダ・オンタリオ州の前情報プライバシー・コミッショナーである，アン・カブキアン（Ann Cavoukian）博士が，1990年代から提唱してきた考え方である。カブキアン博士は，現在は，トロントにあるライアソン大学（Ryerson University）のプライバシー・ビッグデータ研究所（Privacy & Big Data Institute）の常任理事を務めている。

PbDの概要は次の通りである[92]。

PbDは，様々な技術に関する設計仕様の中に，プライバシーを組み込むという考え方及びアプローチをいう。これは，「公正情報実務」（Fair Information Practices）に関する諸原則を，情報処理技術及びシステムの設計，運用及び管理の中で確立させることによって達成することができる。このアプローチは，⑴情報技術，⑵事業活動，並びに，⑶物理的設計及びインフラに適用される。

PbDは，プライバシー促進技術（PETs）に「ポジティブサム」のアプローチを加えた考え方であり，PbDは，プライバシー影響評価（Privacy Impact Assessment, PIA）のもととなる概念である。カブキアン博士の説明で最も強調されているのは，「ポジティブサム」への発想の転換と，PbDがプライバシーとセキュリティの「両者に有利」となることである。

最近では，PbDの認証制度も開始されており，認証を受けた事業者も登場している[93]。PbDの目的は，次の基本7原則を遵守することで，プライバシーと個人の情報へのコントロールを保障し，組織が持続的に競争上の優位を得ることにある。

PbDの7原則は次の通りである[94]。

「1　事後的ではなく**事前的**，救済的ではなく**予**

85）Yukon Information and Privacy Commissioner, http://www.ombudsman.yk.ca/ (last viited Jan. 20, 2017).

86）S.N.W.T. (Nu) 1994, c.20.

87）Information and Privacy Commissioner of Nunavut, http://www.info-privacy.nu.ca/ (Jan. 20, 2017).

88）https://www.justice.gov.nt.ca/en/access-to-information-held-by-public-bodies/https://www.justice.gov.nt.ca/en/files/legislation/access-to-information-and-protection-of-privacy/access-to-information-and-protection-of-privacy.a.pdf https://www.justice.gov.nt.ca/en/files/legislation/health-information/health-information.a.pdf

89）S.N.W.T. 1994, c.20.

90）S.N.W.T. 2014, c.2.

91）新保・前掲「プライバシー・バイ・デザイン」参照。

92）Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles* (Jan. 2011), https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

93）Privacy and Big Data Institute, http://www.ryerson.ca/pbdi/privacy-by-design/certification/ (last visited Jan. 20, 2017).

94）Information & Privacy Commissioner, Ontario, Canada, *Privacy by Design, 7 Foundational Principles*, http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/ (last visited Jan. 20, 2017). 邦訳は，堀部政男・JIPDEC編・前掲『プライバシー・バイ・デザイン―プライバシー情報を守るための世界的新潮流』参照。

防的であること。

プライバシー・バイ・デザイン（PbD）のアプローチは，事後的よりもむしろ事前的措置により特徴付けられる。それは，発生*前に*プライバシー侵害事象を予測し，予防する。PbD は，プライバシーリスクの顕在化を待つものでもなければ，プライバシー違反が一旦発生してからそれを解決するための救済を提供するものでもない―それは，それらの違反が発生するのを予防することを目的としている。要するに，*プライバシー・バイ・デザイン*は，事象の後ではなく，前に来るものである。

2　**初期設定**としてのプライバシー

我々は皆，あること―初期設定ルール―を確信することができる！*プライバシー・バイ・デザイン*は，あらゆる所与の IT システム又は事業活動の中で自動的に個人データが保護されるよう保障することによって，最大限のプライバシーを提供しようとしている。個人が何もしない場合，彼らのプライバシーはいまだ無傷で維持される。自己のプライバシーを保護するために個人の側で求められることは何もない―それはシステムに*初期設定*で組み込まれている。

3　設計に**組み込まれる**プライバシー

*プライバシー・バイ・デザイン*は，IT システム及び事業活動の設計及び構造に組み込まれる。それは事象が起きた後の付属に留めるものではない。その結果，プライバシーは，提供されている中心機能の本質的構成要素となる。プライバシーは，機能性を損なうことなくシステムに不可欠なものである。

4　全機能性―ゼロサムではなく**ポジティブサム**

*プライバシー・バイ・デザイン*は，不必要なトレード・オフがなされるときに，時代遅れのゼロサムアプローチを通じるのではなく，ポジティブサムの「両者に有利な」（win-win）態様で，全ての適法な利益及び目的を収めようとしている。*プライバシー・バイ・デザイン*は，両者を有することが可能であると証明することで，プライバシー**対**セキュリティのように，誤った見せかけの対立を回避する。

5　生成から廃棄までの安全性―**ライフサイクル全般の保護**

*プライバシー・バイ・デザイン*は，情報が収集される最初の要素に先立って，システムに組み込まれており，当該データの全ライフサイクルにわたり安全に拡張される―強力な安全保護措置は最初から最後までプライバシーにとって本質的である。このことは，全てのデータが安全に保持され，そして，取扱いの最後の段階で，適時に安全に破棄されることを保障する。このように，*プライバシー・バイ・デザイン*は，ゆりかごから墓場まで，端から端まで安全な情報管理のライフサイクルを保障する。

6　**可視性**と**透明性**―継続的**開示**

*プライバシー・バイ・デザイン*は，全ての利害関係者において，いかなる事業活動又は技術が関係しようとも，実際に，独立の検査に従い，宣言した約束及び目的に従い運用していることを保障しようとする。その構成部分及び運用は，利用者に対し，また，提供者にも同様に，可視性及び透明性を維持する。信用するが確認することを覚えておくこと。

7　利用者のプライバシーを最大限に尊重すること―利用者中心の維持

とりわけ，*プライバシー・バイ・デザイン*は，設計者及び運用者に対し，強力なプライバシーの初期設定，適切な通知，及び利用者に親切な選択肢の付与といった措置を提供することで，個人の利益を最高に維持することを求める。利用者中心の維持。」

PbD のプライバシーは，1983 年のドイツの国勢調査判決が「情報自己決定権」に言及したことに由来している[95)]。プライバシーは，何かを隠すこと（秘密性）ではなく，コントロールできることを意味する。

PbD が国際的に広く認知を受けるきっかけとなったのは，2010 年 10 月に開催された第 32 回データ保護・プライバシー・コミッショナー国際

95）国勢調査判決については，藤原静雄「西ドイツ国勢調査判決における「情報の自己決定権」」一橋論叢第 94 巻 5 号（1985 年）728-746 頁参照。

会議における，PbDに関する決議である[96]。PbDは，2012年3月26日に米国の連邦取引委員会が公表した「プライバシーレポート」[97]の3本柱の1つに掲げられ，EUの一般データ保護規則[98]では，第25条「データ保護・バイ・デザイン及びバイ・デフォルト」として導入された。日本では，衆議院内閣委員会の2015年5月20日付「個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律案に対する附帯決議」[99]及び参議院内閣委員会の2015年8月27日付同法律案に対する附帯決議[100]の中で，PbDへの言及がある。PbDは，カナダの法令の中では立法化されておらず，また，そもそも立法化を前提とする考え方ではないが，その考え方は世界的な広がりを見せている。

PbDを実装する技術や分野に制限はないが，2012年に公表された「PbDの運用」（Operationalizing Privacy by Design）[101]の中で，9つの適用分野が紹介されている。具体的には，監視カメラ，バイオメトリクス，スマート・メーター及びスマート・グリッド，モバイル機器／通信，近距離無線通信（Near Field Communication），RFID及びセンサー技術，IP位置情報，遠隔医療，ビッグデータ及びデータ分析に用いることができるとされている。

ビッグデータ，IoT，さらには人工知能（Artificial Intelligence）が発展する中で，PbDの重要性に疑いの余地はないと考えられる。他方，PbDの実現には技術的措置が不可欠であり，諸原則を具体化する際の工夫と努力が必要となる。

V　おわりに

カナダの国内法を概観すると，オンブズマンであることによる権限の制限，PIAの立法化，データ侵害通知の立法化，州法と連邦法の管轄，州法特有の規制（データ・ローカライゼーション法），十分性認定への影響といった問題が存在する。

オンブズマンは，連邦と多くの州が取り入れている制度であるが，特に連邦のコミッショナーの判断に拘束力を持たせるか否かが課題となる。この点は，独立監督機関による強力な法執行を掲げるEUから見た場合には，弱点となり得る。州のコミッショナーの中には命令権限を有するものもある。連邦政府の関係者からは，現行制度を変更してまで命令権限を付与する必要はないとの意見も聞かれるが，国際的協力も行う執行機関にとって，権限強化は最大の課題であり続ける。

PIAは立法化を必須とする仕組みではなく，連邦政府では，指令に基づき実施されてきた。しかし，ビッグデータ時代の中で，個人情報の取扱いへの効果的ガバナンスを行うためには，特に政府部門において立法化する意義はあると考えられる。国際的にも，EUの一般データ保護規則では，「データ保護影響評価」として立法化されている。日本でも，マイナンバー法（行政手続における特定の個人を識別するための番号の利用等に関する法律）に基づく特定個人情報保護評価が実施されている。

データ侵害通知は，侵害を犯した側に報告のインセンティブがないことから，立法による義務づけを必要とする制度である。アルバータ州の民間部門向け個人情報保護法及びPIPEDAの改正により，民間事業者の侵害通知が義務化されること

96）32nd International Conference of Data Protection and Privacy Commissioners, Resolution on Privacy by Design (Oct. 2010), https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf.

97）Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers* (Mar. 26, 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

98）Parliament and Council Regulation 2016/679, 2016 O.J. (L 119) 1-88 (EU).

99）http://www.shugiin.go.jp/internet/itdb_rchome.nsf/html/rchome/Futai/naikaku28215527A5B4800A49257E4C00043F53.htm.

100）http://www.sangiin.go.jp/japanese/gianjoho/ketsugi/189/f063_082701.pdf.

101）Ann Cavoukian, *Operationalizing Privacy by Design* (Dec. 2012), http://www.cil.cnrs.fr/CIL/IMG/pdf/operationalizing-pbd-guide.pdf.

となった。データ侵害通知（セキュリティ侵害通知）は米国カリフォルニア州法を発祥として各州に広まった制度であり，EU の一般データ保護規則でも，「個人データ侵害通知」として立法化されている。日本でも，2015 年 9 月 3 日のマイナンバー法改正により，個人情報保護委員会への漏えい報告制度が導入された。

州法と連邦法の管轄は国内法的問題であり，明文が存在しないことに原因がある。また，カナダは連邦優位の制度を採用しているものの，ケベック州ではプライバシー・個人情報保護の分野で先んじて立法化に踏み切ったという経緯も管轄問題を複雑化させていると考えられる。このような認識の食い違いは，十分性認定にも影響している。一部の関係者からは「実質的に類似」するとの判断を受けたケベック州において，第 29 条作業部会から否定的評価を受けたことは，PIPEDA の十分性認定にも影響を与えかねないとの声が上がっている。EU の一般データ保護規則では，十分性認定を 4 年ごとに定期審査する規定を新設していることから，PIPEDA も EU の規律を意識する形で改正を求められることが予想される。

データ・ローカライゼーション法は，クラウド・コンピューティング・サービスの利用を妨げたり，個人データの自由な流通を阻害しかねないため，個人情報の保護と自由な流通のバランスを図るという，個人情報保護制度の理念に沿わない制度といえる。実際，ロシアの監督機関が，2016 年 11 月 10 日のモスクワ市裁判所決定を受け，国内のデータ・ローカライゼーション法に基づき，LinkedIn のウェブ・サイトをブロックするという事態も生じている[102)]。カナダのデータ・ローカライゼーション法は，ブリティッシュ・コロンビア州やノバ・スコティア州の政府機関のみに適用されるものであるが，この法令の存在意義は慎重に考えるべきと思われる。

PIPEDA の議論において注目すべきは，「同意」の考え方である。PIPEDA の 2015 年改正法は同意の判断に「個人の合理的期待」を明文で取り入れ，連邦のコミッショナーは，「同意とプライバシー」の中で，通常人が不適切と考える個人情報の収集，利用及び開示を「禁止区域」として禁止するという考え方を提案した。効果的な「同意」の議論が深化すれば，日本の法解釈にとっても参考にすることができる。

PbD は，カナダの中でも特殊な取組であり，国際的な存在感を高めることに重要な役割を果たしている。日本でも，関係者の間で PbD は知られるようになっているが，理念を理解するのみならず，いかに実装するかという技術的な具体論を進める必要がある。

カナダが国際的動向を踏まえつつ，同時に国内的問題を解決しなければならないのは，日本と共通している。カナダの議論は日本にとっても示唆を得られるものが多いと考えられることから，その状況には常に目を向ける必要がある。

102） Privacy Laws & Business, International e-news, *Russia blocks LinkedIn as a result of data localisation requirement* (Nov. 17, 2016), http://www.privacylaws.com/Int_enews_18_11_16.

プライバシーに関する契約についての考察(1)

弁護士
板　倉　陽一郎
ITAKURA Yoichiro

Ⅰ　プライバシーに関する契約の氾濫

インターネットには，個人情報の取扱いに関する利用規約やプライバシーポリシー，個人情報保護指針と証する文書が溢れている。これらは事業者が作成し，消費者に提示しているものであり，インターネットの利用者たる消費者は，日々，その内容に同意して，インターネット上のサービスを利用している（ことになっている）。これらの文書のクオリティは様々である。サービスに合わせて丁寧に作り込まれており，規約への同意を含んだユーザーインターフェースに工夫が見られるものもあるし，類似サービスの利用規約やプライバシーポリシーを安易にコピーしてきたと見受けられるものもある。近年は，実務家向けの作成マニュアル的な書籍や，書式集が多数公刊されており，それらの内容も洗練されてきているので[1)]，事業者において時間とコストを費やせば，適切な内容の利用規約やプライバシーポリシーを作成することは困難ではない。他方，それらについての理論的な分析がなされることは稀である。

具体例を見てみよう。ここでは，日本で最初に欧州データ保護指令における拘束的企業準則（Binding Cooperate Rules, BCR）[2)] の承認を受けた事業者[3)] ということで，一定のデータ保護の水準を確保していると考えられる楽天株式会社の「楽天会員規約[4)]」，「楽天個人情報保護方針[5)]」及び「お客様の個人情報の利用について[6)]」（以下，「楽天利用について」という。）を例として挙げる。楽天会員規約7条は，「楽天は，会員による会員サービスの利用に関して取得する個人情報を，楽天の個人情報保護方針（https://privacy.rakuten.co.jp/）に従い，適切に取扱います。」とする。そうすると，個人情報保護方針に従うという内容は，楽天

1)　例えば，昨今の実務家向けの書籍として，雨宮美季他『良いウェブサービスを支える「利用規約」の作り方』（技術評論社，2013年）146-183頁，小野斉大他『アプリ法務ハンドブック』（レクシスネクシス・ジャパン，2015年）214-280頁など。

2)　欧州データ保護指令26条2項を根拠とするものであり，欧州データ保護指令における「十分な保護措置」を備えていない国又は地域には個人データを移転できない，という規制の例外措置の一つである。邦語による解説として，石井夏生利『個人情報保護法の現在と未来　世界的潮流と日本の将来像』（勁草書房，2014年）93頁以下。

3)　平成29年1月27日現在，“List of companies for which the EU BCR cooperation procedure is closed”（http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm）には記載がないが，報道によると，平成28年12月24日に，ルクセンブルクのデータ保護機関であるCommission nationale pour la protection des donnéesから承認を得たとのことである。（「楽天，BCRの承認を取得-EEA域外への個人情報移転が可能に」Security NEXT平成28年12月26日，http://www.security-next.com/077018（平成29年1月27日閲覧））。

4)　https://corp.rakuten.co.jp/terms/（平成29年1月27日閲覧）。

5)　https://privacy.rakuten.co.jp/（平成29年1月27日閲覧）。

6)　https://privacy.rakuten.co.jp/use.html（平成29年1月27日閲覧）。

会員規約によって，契約の内容になっているものといえる（この点は，後に詳細に論ずることになる）。そして，楽天個人情報保護方針 7. によると，「私たちは，グローバルに事業活動を展開しており，お客様の個人情報を，お客様がお住まいの国と同等の個人情報保護法制でない国に移転する可能性があります。この場合には，私たちは，適用法令の要求するところに従い，お客様の個人情報の保護のために必要な適切な措置を講じます。」とされている。この 7. は，個人情報の保護に関する法律（平成 15 年法律第 57 号，以下，「個人情報保護法」といい，平成 27 年法律第 65 号及び平成 28 年法律第 51 号による改正後の条文を前提とする）第 24 条の「外国にある第三者への提供を認める旨の本人の同意」について，いかなる外国にある第三者であるかを問わずに提供することの同意を取得しようとして設けられている規定であると考えられるが，このような条項を民事的に見れば，契約の当事者である「お客様」のプライバシーの一部を制約する合意をなしていると考えられる。そして，この条項が適切に契約内容になっているとすれば，「お客様」は，いかなる外国に個人情報を移転されても，プライバシーを侵害されたとして，損害賠償請求をすることも，差止を行うこともできないということになろう[7]。本稿では，このような，本人のプライバシーの一部を制約する合意のことを，「プライバシーに関する契約」として，分析の対象とする。「楽天会員規約」や，「楽天個人情報保護方針」のような，個人情報の取扱いに関する利用規約やプライバシーポリシーを契約としてみたうえで，分析していくこととなる。これまでも，筆者らは，プライバシーに関する契約についての研究を進めてきた[8]。本稿は，一連の研究を踏まえ，その後の関連する新法の制定，法改正の動向や，個人情報保護法の改正も踏まえて整理をし，実務上の指針を導き出そうとするものである。具体的には，①プライバシーに関する契約の実体法的分析と，②プライバシーに関する契約の訴訟法的分析を行う。①実体法的分析では，プライバシーに関する契約が行われる実務上の理由を述べたうえで，プライバシーに関する契約の限界を画定する。②訴訟法的分析では，消費者団体訴訟（消費者契約法（平成 12 年法律第 61 号）12 条等），消費者の財産的被害の集団的な回復のための民事の裁判手続の特例に関する法律（平成 25 年法律第 69 号，以下，「消費者裁判特例法」という。）及び行政訴訟との関係がそれぞれ取り扱われる。

Ⅱ　プライバシーに関する契約の実体法的分析

1　プライバシーに関する契約が行われる理由

(1)　プライバシーポリシーにおける法定公表事項等の記載

なぜ，プライバシーに関する契約が行われるのか。この点は，まずは，プライバシーポリシーというものの存在から分析することになろう。

「プライバシーポリシー」というのは，インターネットのそこかしこに存在するが，法令用語ではなく，用いられ方もまちまちである。個人情報の保護に関する基本方針（平成 16 年 4 月 2 日閣議決

7)　本稿では，プライバシーとは何か，人格権とは何か，については立ち入らず，プライバシーが侵害された場合，人格権に基づく差止請求権が認められること及び，不法行為に基づく損害賠償請求権が認められることに着目しておく（実務上，インターネット上に発信された情報の削除請求が人格権に基づく差止請求権の行使として行われていることを述べるものとして，清水陽平・神田知宏・中澤佑一『ケース・スタディ　ネット権利侵害対応の実務―発信者情報開示請求と削除請求―』（新日本法規，2017 年）26 頁，プライバシー侵害について不法行為に基づく損害賠償請求を認める判例は枚挙に暇がないが，さしあたり，最判平成 15 年 9 月 12 日民集 57 巻 8 号 973 頁（早稲田大学江沢民講演会事件））。プライバシーに関する契約の効果は，これらの請求権に対する制約として現れる。

8)　板倉陽一郎「個人情報の取扱いに関する利用規約上の定めに関する考察」情報処理学会研究報告電子化知的財産・社会基盤（EIP）2013-EIP-62 巻 4 号（2013 年）1-6 頁（以下，「板倉 EIP 62」という。），板倉陽一郎「「消費者の財産的被害の集団的な回復のための民事の裁判手続の特例に関する法律」のインターネット上の事案への適用についての考察」情報処理学会研究報告電子化知的財産・社会基盤（EIP）2014-EIP-63 巻 3 号（2014 年）1-6 頁（以下，「板倉 EIP 63」という。），板倉陽一郎・寺田麻佑「個人情報保護法改正案及び民法（債権法）改正案の利用規約及びプライバシーポリシーにおける個人情報取扱条項への影響」情報処理学会研究報告電子化知的財産・社会基盤（EIP）2015-EIP-68 巻 14 号（2015 年）1-6 頁（以下，「板倉・寺田 EIP 68」という。）。また，筆者らは，書式集の解説において，インターネット上の利用規約やプライバシーポリシーについて理論的な説明を試みたことがある（大村多聞他編『契約書式実務全書〔第 2 版〕第 3 巻』（ぎょうせい，2014 年）457-498 頁〔藤原宏高・板倉陽一郎〕）。

定，平成28年10月28日一部変更）はプライバシーポリシーに触れており，6「個人情報取扱事業者等が講ずべき個人情報の保護のための措置に関する基本的な事項」⑴「個人情報取扱事業者が取り扱う個人情報に関する事項」において，「個人情報取扱事業者は，法の規定に従うほか，2の⑵の①の個人情報保護委員会のガイドライン，認定個人情報保護団体の個人情報保護指針等に則し，例えば，消費者の権利利益を一層保護する観点から，個人情報保護を推進する上での考え方や方針（いわゆる，プライバシーポリシー，プライバシーステートメント等）を対外的に明確化するなど，個人情報の保護及び適正かつ効果的な活用について主体的に取り組むことが期待されているところであり，体制の整備等に積極的に取り組んでいくことが求められている。その際，事業の規模及び性質，個人データの取扱状況等に応じて，各事業者において適切な取組が実施されることが重要である。」とする（傍線筆者。以下同じ。）ここでは，「個人情報保護を推進する上での考え方や方針」であるとされ，いかなる内容を含むものであるかは示されていない。なお，「個人情報の保護に関する基本方針」は閣議決定に過ぎず，事業者への直接的な規範性も存しない。

また，総務省の「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」（以下，「電気通信GL」という。平成29年総務省告示第152号）14条1項は「電気通信事業者は，プライバシーポリシー（当該電気通信事業者が個人情報保護を推進する上での考え方や方針をいう。）を公表することが適切である。」とし，プライバシーポリシーが「個人情報保護を推進する上での考え方や方針」であることを確認したうえで，「電気通信事業における個人情報の保護に関するガイドラインの解説」（以下，「電気通信GL解説」という。平成29年4月18日版。）14条1項部分では，「プライバシーポリシーは，それぞれの電気通信事業者が，分かりやすい表現で記載すべきものであるが，プライバシーポリシーに記載すべき事項としては，次のようなものが考えられる。①法及び通信の秘密に係る電気通信事業法の規定その他の関係法令の遵守，②本ガイドラインの遵守，③第19条第1項各号に定める公表すべき事項：⑴電気通信事業者の氏名又は名称，⑵保有個人データの利用目的，⑶利用目的の通知又は開示若しくは訂正等の本人からの求めに応じる手続，⑷苦情の申出先，⑸認定個人情報保護団体の名称及び苦情の解決の申出先，④第11条の安全管理措置に関する方針，⑤利用者の権利利益の保護に関する事項：⑴保有個人データについて本人から求めがあった場合には，ダイレクト・メールの発送停止など，自主的に利用停止等に応じること，⑵委託の有無，委託する事務の内容を明らかにする等，委託処理の透明化を進めること，⑶電気通信事業者がその事業内容を勘案して利用者の種類ごとに利用目的を限定して示したり，電気通信事業者が本人の選択による利用目的の限定に自主的に取り組むなど，本人にとって利用目的がより明確になるようにすること⑷個人情報の取得元又はその取得方法（取得元の種類等）を，可能な限り具体的に明記すること，なお，上記のほか，取得に際しての利用目的（第8条第1項，第3項），オプトアウトによる個人データの第三者提供を行う場合の個人データの項目等（第15条第2項，第3項，第9項），共同利用における共同利用される個人データの項目等（第15条第10項第3号，第11項），匿名加工情報に含まれる情報の項目等（第28条第3項，第4項，第5項，第7項，第29条），匿名加工情報取扱事業者における匿名加工情報の安全管理措置等（第31条）について，プライバシーポリシー等において，通知，公表又は本人が容易に知り得る状態に置くことが求められていることに留意する必要がある。」としている（条文数は電気通信GL案のもの）[9]。個人情報保護法上，通知，公表又は本人が容易に知り得る状態が求められる事項（以下，「法定公表事項等」という。）についての法遵守の仕方については，例えば，「公表」について個人情報保護委員会より「自社のホームページのトップページから1回程度の操作で到達できる場所への掲載」が，「容易に知り得る状態」については，「本

9）平成29年4月18日のGLの改正によって導入された部分である。

人が閲覧することが合理的に予測される個人情報取扱事業者のホームページにおいて，本人が分かりやすい場所（例：ホームページのトップページから1回程度の操作で到達できる場所等）に法で定められた事項を分かりやすく継続的に掲載する場合」が「事例」として挙げられている[10]。要するに，個人情報保護委員会によると，個人情報保護法における法定公表事項等については，ウェブサイト上に公表等することによって義務を果たそうとするのであれば，事業者のウェブサイトから1回程度の操作で到達できる場所，つまり，リンクされているウェブページに掲載されることが望ましく，総務省はこれを，「プライバシーポリシー等において」と表現している，ということになろう。かくして，事業者は，プライバシーポリシーにおいて法定公表事項等を記載するプラクティスを進めることになる。この点について，ヤフー株式会社は，「プライバシーポリシーは，一般的に個人情報保護法との関係において，特定した利用目的を公表するものであるということはほぼ共通していると思われる」との見解を公表しているが，本稿の理解と整合的である[11]。

(2) プライバシーポリシーにおける同意の取得

さらに，プライバシーポリシーでは，（個人データの）第三者提供の同意までもが記載されていることがある。この点は，楽天個人情報保護方針において個人情報保護法24条の外国にある第三者への提供の同意が意図されていることでも確認した。個人情報保護法のガイドラインにおいても，例えば，「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」（平成29年4月14日個人情報保護委員会・厚生労働省）では，「Ⅰ 6. 医療・介護関係事業者が行う措置の透明性の確保と対外的明確化」において，「医療・介護関係事業者は，個人情報保護に関する考え方や方針に関する宣言（いわゆる，プライバシーポリシー，プライバシーステートメント等）及び個人情報の取扱いに関する明確かつ適正な規則を策定し，それらを対外的に公表することが求められる。また，患者等から当該本人の個人情報がどのように取り扱われているか等について知りたいという求めがあった場合は，当該規則に基づき，迅速に情報提供を行う等必要な措置を行うものとする。個人情報保護に関する考え方や方針に関する宣言の内容としては，医療・介護関係事業者が個人の人格尊重の理念の下に個人情報を取り扱うこと及び関係法令及び本ガイダンス等を遵守すること等，個人情報の取扱いに関する規則においては，個人情報に係る安全管理措置の概要，本人等からの開示等の手続，第三者提供の取扱い，苦情への対応等について具体的に定めることが考えられる。」とし，第三者提供についてまで，プライバシーポリシーで記載することが述べられている。「第三者提供の取扱い」を「具体的に定める」とするのみであるので，必ずしも第三者提供の同意（個人情報保護法23条1項柱書）をプライバシーポリシーにおいて取得せよというものではないが，排除されているとすることも困難であろう。

このような監督機関の見解にそぐわず，事業者においても，法定公表事項等のみならず，第三者提供の同意までをも，プライバシーポリシーに記載して，取得しよう，という動きが現れる。楽天株式会社の例はすでに見たが，ヤフー株式会社においても，「改定後のYAHOO! JAPANのプライバシーポリシーにおいては，個人情報の第三者提供について，法令に基づく場合のほかは，原則として本人の同意を得て行うものとしている。そして，例外として，プライバシーポリシーに定める特定の場合に限り，氏名や住所などの直接特定の個人を識別できる情報を除外した上で個人情報を第三者提供することについて，あらかじめ同意していただくこととしている。」[12]とされている。しかし，そうすると，単にプライバシーポリシーを「掲載」しておくだけでは足りず，プライバシーポリシー（のうち，第三者提供等，個人情報保護法上同意を必要とする項目）に「同意」してもらう必要が生じる[13]。これを解決する手段が，利用規約による「同意」の取得である。

---

10)「個人情報の保護に関する法律についてのガイドライン（通則編）」（平成28年個人情報保護委員会告示第6号）2-11（公表）及び3-4-2（オプトアウトによる第三者提供）。

11) 小柳輝「Yahoo! JAPANプライバシーポリシーの改定について」NBL 1078号（2016年）36-43頁，37頁。

12) 前掲注11）39-40頁。

(3) 利用規約による「同意」の取得

プライバシーポリシーに同意してもらえば，第三者提供（個人情報保護法23条，外国にある第三者に対する提供の場合は24条）や関連性を有する範囲を超えた場合の利用目的変更（個人情報保護法15条2項，16条1項）が可能になる。問題は，どのように同意を取得するかである。もちろん，利用規約への合意のほかに，プライバシーポリシーについて同意を取得すれば目的は達成されるのであるが，滞在時間が秒単位で問題となるウェブサイトのユーザーエクスペリエンスにおいて，二回のクリックを要求することはユーザーの離脱率との関係では決定的になり兼ねない。そこで，利用規約への合意を取得すると同時に，プライバシーポリシーへの同意も取得しよう，という発想が必然的に表れるのである。

この点に関し，電気通信GL解説（2-13）は「本人の同意」の解釈として，「個別の同意がある場合だけでなく，電気通信サービスの提供に関する契約約款において，個人情報の第三者提供に関する規定が定められており，当該契約約款に基づき電気通信サービス提供を締結し（※1），かつ当該規定が私法上有効であるとき（※2）は，「本人の同意を得（る）」又は「本人の同意がある」場合と解される。よって，無制限に第三者提供を認める契約約款の規定等が，利用者の利益を阻害していると認められるときは，電気通信事業法上の業務改善命令の対象となり得る。」「（※1）契約約款の変更により個人情報の第三者提供に関する規定が設けられた場合であっても，当該変更が私法上有効であり変更前に契約締結を行った当事者にも変更後の規定が効力を有すると判断される場合には，「本人の同意」がある場合と解される。」「（※2）民法（明治29年法律第89号）第90条の公序良俗に反する場合や同法第95条の要素の錯誤がある場合，消費者契約法（平成12年法律第61号）第10条の消費者の利益を一方的に害するものとされる場合など同意が私法上無効とされる場合は，有効な同意があるとはいえないので，同意がある場合とはいえない。」との見解を示している[14]。

総務省の見解は，①契約約款において，個人情報の第三者提供に関する規定が定められており，これにより契約を締結した場合，②契約約款の変更によって第三者提供に関する規定が設けられた場合，のいずれにおいても，契約又は約款の変更が私法上有効である場合には，有効な同意があると解される，というものである。これは，第三者提供等の同意を含む利用規約による契約の私法上の有効性又は，第三者提供等の同意を導入する利用規約の変更についての私法上の有効性を，公法上の第三者提供等の同意の十分条件としているものである。

他方で，個人情報保護委員会は，「本人の同意」について，「本人の個人情報が，個人情報取扱事業者によって示された取扱方法で取り扱われることを承諾する旨の意思表示をいう（当該本人であることを確認できていることが前提となる。）」との見解を示している[15]。同意が意思表示であるとする見解は，従来の立案担当者等の見解には見られないものである。ここでいう「意思表示」は，個人情報保護法が行政法規である以上，公法上の意思表示ということになろう。公法上の意思表示に民法の法律行為に関する規定が適用されるかに

13）実務書においても，「個人情報保護法は，取得した個人情報を第三者に提供する際には，原則として本人から同意を得ることを求めています。そのため，個人情報を第三者に提供する場合は，プライバシーポリシーにおいてその旨を明記する必要があります（もちろん，プライバシーポリシーに対してユーザーが同意することが前提になります）」（前掲注1）雨宮他33頁）とされたり，前掲注1）小野他250頁において，「アプリプライバシーポリシーに記載する事項」として，「個人情報を第三者に提供する場合，提供先，提供する情報，提供先での利用目的」が掲げられたりするなど，プライバシーポリシーに個人情報保護法上の同意事項を記載することが想定されている。

14）改正前の規定は「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（平成16年総務省告示第695号。最終改正平成27年総務省告示第216号）の解説」15条部分。なお，改正前は「なお，同意は有効なものでなければならないので，民法（明治29年法律第89号）第90条の公序良俗に反する場合や同法第95条の要素の錯誤がある場合，消費者契約法（平成12年法律第61号）第10条の消費者の利益を一方的に害するものとされる場合など同意が私法上無効とされる場合は，有効な同意があるとは言えないので，同意がある場合とは言えないことは当然である。」とされていたが，若干トーンが落ちている。

15）前掲注10）2-12（本人の同意）。

ついては学説上争いがあるが[16]，名古屋地判平成19年3月23日判時1986号111頁は，「国公立大学と学生との法律関係は，公法上の無名契約（在学契約）であると解される。」「そして，国公立大学の在学契約の予約に学生の入学に関する意思表示を要すると解される以上，その意思表示に欠缺又は瑕疵があれば，民法上の意思表示に関する規定に準じて，無効とされ，又は，取り消され得るというべきである。」としており，公法上の意思表示について，民法上の意思表示に関する規定が準用されるという説を採用している。個人情報保護委員会の見解を公法上の意思表示についての見解であると解する限りにおいて，第三者提供等の同意を含む利用規約による契約の有効性は，公法上の契約の有効性として私法上の意思表示の規定を適用又は準用して検討すれば足り，そこで，私法上の有効性を持ち出す余地はない。

どう考えるべきか。まず，本人の同意を，個人情報の取扱いについての意思表示であるとする個人情報保護委員会の見解は，「意思表示」が公法上の意思表示であるということを前提とすれば，基本的に承認されるであろう。もっとも，ここでの意思表示を単純に民法上の意思表示の規定上の「承諾[17]」と捉えるのは適切ではないであろう。その理由としては，第一に，個人情報の取扱いについて「申込み」（改正民法案522条）を行うのが事業者であるとは限らない。第三者提供に供する個人情報の項目等を本人が選択できる場合，申込みを行っているのが本人であり，承諾するのが事業者ということになろう。また，PDS（パーソナルデータストア），情報銀行及びデータ交換市場といった事業者らの取組みは，予め本人の同意を取得した上で，個人情報・個人データの利活用の方策を採ろうとするものである[18]。これらの取組の実装には様々な形態があるが，本人において，流通に供する個人情報及び，流通させることが出来る事業者の条件を予め選択している場合，明らかに「申込み」を行っているのは本人であって，本人の示した条件に従って個人情報を利活用する事業者が承諾をする側，ということになろう。第二に，少なくとも，個人情報保護法は「同意」が事業者に到達することを要求しておらず，同意の有効性も左右しないと考えられるところ，本人が「承諾」側に回る場合には，その到達を要しないという変容が認められるべきであろう。もとより，隔地者間の承諾の意思表示には発信主義が採用されているが（民法526条1項），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（平成13年法律第95号）4条は，電子承諾通知においてこれを排除している（原則である到達主義に戻ることとなる）。そうすると，利用規約に対し，クリックにより承諾するという，よく見られる本人の同意については，民法上の意思表示の規定をそのまま適用する限りにおいて，到達主義が採用されるが，それは，個人情報保護法が「同意」に到達を要求していないことと整合しないであろう。結論として，同意が個人情報の取扱いについての承諾である場合には，電子承諾通知に該当する場合であっても，発信主義が適用されるという変容を容れるべきであろう。その限りにおいて，本人の同意に対する民法上の意思表示に関する規定は一部修正されることになる[19]。

このように考えると，利用規約によって第三者提供等に関する本人の同意を取得する際の有効性

16）「一般的には民法の法律行為に関する規定の適用がある」とするものとして塩野宏『行政法Ⅰ［第五版］』（有斐閣，2009年）370頁，民法の規定の適用に対するドイツにおける学説上の批判を整理するものとして鹿子嶋仁「行政法関係における私人の行為：ドイツにおける展開とその検討」一橋論叢110巻1号（1993年）116-136頁。なお，「公法上の意思表示」に関し，美濃部達吉『日本行政法上巻』（有斐閣，1936年）180頁以下。

17） 契約が申し込みと承諾により成立することについて，民法上明文の規定はないが，民法の一部を改正する法律案（第189回国会（常会）閣法63号）による改正後の民法（以下，「改正民法案」という。）522条は，「契約は，契約の内容を示してその締結を申し入れる意思表示（以下「申込み」という。）に対して相手方が承諾をしたときに成立する。」とする。

18） 高度情報通信ネットワーク社会推進戦略本部（IT総合戦略本部）データ流通環境整備検討会AI，IoT時代におけるデータ活用ワーキンググループ「中間とりまとめ」（平成29年3月）4頁も，「パーソナルデータを含めた多種多様かつ大量のデータの円滑な流通を実現するためには，個人の関与の下でデータの流通，活用を進める仕組みであるPDS，情報銀行，データ取引市場が有効である。」とする。

19） 前掲注16）塩野においても，「行政法関係においては，当該関係を規律している法律の仕組みに即して事案を処理していく必要が」あるとされる。

は，公法上の意思表示の有効性だけに掛からしめれば良いということになり，私法上の意思表示の有効性を持ち出す必要はないということになる。勿論，第三者提供等に関する同意についての公法上の意思表示については，上記したように，個人情報保護法上の「同意」の解釈から，発信主義が適用されるという修正が加わるが，それ以外の意思表示に関する規定（意思表示の瑕疵，代理等）については適用と呼ぶか，準用と呼ぶかは別論，私法上の意思表示規定に従うことになるので，事実上，有効無効は一致することにはなる。しかしそれは，私法上有効無効か，に結論が左右されるということではなく，あくまでも公法上の評価の問題だということになる。例えば，公法上の意思表示たる第三者提供の同意が電子承諾通知に該当する場合，発信して到達しなかったとしても，ここでは発信主義による一部修正が適用され，公法上の契約が成立するということになる。他方で，私法上の意思表示については，当然ながら，私法上の規定が適用されるため，電子承諾通知を発信して到達しなければ私法上の契約は不成立ということになる。その場合，公法上の契約としては有効であるが，私法上の契約としては無効，ということで契約ないし利用規約への合意が評価されることになるが，やむを得ない。

このように，個人情報保護委員会の見解を前提として，公法上の意思表示であることから，一部民法上の意思表示規定が修正されて適用されることとすると，利用規約によって第三者提供等に関する同意を取得するのはむしろ当然であるということになる。また，そのような見解によると，プライバシーポリシーをあえて利用規約と分離しているような場合でも，少なくとも公法上は契約としての効力が発生するということになる。楽天株式会社は，プライバシーポリシーたる楽天個人情報保護指針を楽天会員規約にインクルードするという方法で，ヤフー株式会社は，プライバシーポリシーを利用規約の内容とする方法で，公法上の契約を発生させているということになる。利用規約による公法上の契約が可能になると，個別同意のコストが極端に下がることになる。従前は，利用規約に密かに第三者提供等に関する同意を入れ込んで，同意ボタンさえクリックさせれば良い，という不適切な運用も見られたところだが，近年の，グローバル化への対応にも対応し，ヤフー株式会社にせよ，楽天株式会社にせよ，利用規約・プライバシーポリシーで取得する第三者提供等に関する同意の内容は，「楽天利用について」のような理解しやすいコーナーを設けて，本人の理解の上での承諾を得ようという工夫―ないし，リスクヘッジ―が見られる。

ヤフー株式会社は，平成28年6月の改定前から，「プライバシーポリシーですけれども，個人情報保護指針よりも，イコールの意味ではありますけれども，私どもとしては，個人情報保護指針として公表するという形ではなくて，これを利用規約の中に入れ込んでしまいます．つまり，約款の一部に，私どもはプライバシーポリシーをしてあります．ご存知だと思いますけれども，アメリカでプライバシーポリシー，FTCが推奨して入れておりますけれども，あのアメリカの場合のプライバシーポリシーは，契約ではないけれども，プロビス（ママ）になっておりまして，そのプロビス違反はFTCの方が，いろいろな行政上の措置を作動できるトリガーになっています．そういう意味でいうと，単なる表示以上の意味を持っていて，日本的に言うと，契約的な性格に近いのではないうかというところもあって，私どもとしては，プライバシーポリシーに関しては，そこまで踏み込んでみようということで，こういう位置づけをしております．」との見解を明らかにしていた[20]。改定後も，「Yahoo! JAPANのプライバシーポリシーの大きな特徴の一つは，「Yahoo! JAPAN利用規約第1編基本ガイドライン第2章プライバシーポリシー」という正式名称からも明らかなように，前者（債権債務の内容を基礎づけるもの）であるということを明確にしているということである。これは，単に業法の規律を受ける文書であるということを超えて，お客様との間のお約束であり，Yahoo! JAPANは，直接お客様に対

20）内閣府消費者委員会「第4回個人情報保護専門調査会」（平成23年1月11日）議事録，http://www.cao.go.jp/consumer/history/01/kabusoshiki/kojin/004/gijiroku/index.html，（平成29年2月1日閲覧）。

してこれを遵守する義務を負っているという立場を明らかにすべきであるという考えを反映したものである。」としており，立場は変わっていない[21]。これについては，「個人情報保護法上の明示義務，公表義務等を利用規約に定めることによって，あえて債務不履行のリスクを取るということを「踏み込んで」定めている.」との評価をしてきたが[22]，第三者提供等に関する同意についての公法上の契約と私法上の契約の分析を踏まえると，公法上の契約の側面についての是正は個人情報保護法上の監督（個人情報保護委員会の法執行）が担っているといえ，債権債務関係とすることによる個人情報の本人との関係での直接的な効果（債務不履行の場合の解除，損害賠償等）は，私法上の契約の側面から生じてくると考えることになる。

⑷ 残滓としての「プライバシーに関する契約」

以上の通り，①プライバシーポリシーにおいて法定公表事項等が記載され，②更にこれが発展してプライバシーポリシーに第三者提供等に関する同意が記載され，③同意を円滑に取得するために，利用規約によりプライバシーポリシーにおける同意を取得する，という流れが存在し，利用規約による第三者提供等に関する同意の取得は公法上の契約（個人情報保護委員会がいうところの「承諾」に限らない）という構造が解明できた。問題は，公法上の契約を発生させようとした条項の私法上の解釈である。

（個人データの）第三者提供等に関する同意は，私法的には，当該個人情報の取扱いの範囲においてはプライバシーに関する請求権（人格権に基づく差止請求権及び不法行為に基づく損害賠償請求権）を行使しないという意思表示を含むと考えられる。つまり，何らかのインターネットサービスの利用規約・プライバシーポリシーに，第三者提供等に関する同意等，個人情報の取扱いに関する条項が含まれ，これに関して同意した場合，公法上の契約としては，個人情報保護法上の同意を与えたことになる。他方で，私法上の契約としては，プライバシーに関する請求権を行使しない，という意思の合致―及び，当該条項に反した場合に債務不履行責任を甘受するという意思の合致―がみてとれる。それでは，プライバシーに関する請求権を行使しない，との条項は，フリーハンドなのであろうか。つまり，個人情報保護法を遵守する内容の個人情報の取扱いに関する条項であれば，常に，私法上の契約としても有効なのであろうか。ここに，残滓としてのプライバシーに関する契約の解釈の必要が生じてくる。

21） 前掲注 11）37 頁。

22） 板倉 EIP 62，2 頁。

米国連邦通信委員会のプライバシー政策

日本大学危機管理学部教授
小　向　太　郎
KOMUKAI Taro

はじめに

米国で電気通信事業者に対する規制を所轄する FCC（Federal Communications Commission：連邦通信委員会）は，2016 年 10 月 27 日にブロードバンドサービスを始めとする電気通信サービスに関する消費者プライバシーの保護の新たなルールとして，「ブロードバンド顧客プライバシー保護規則[1)]」を採択した。米国の消費者プライバシー保護に関しては，ICT 分野も含めて FTC（Federal Trade Commission：連邦取引委員会）が，近年積極的な政策を打ち出している[2)]。この消費者プライバシー規制の根拠規定となっている FTC 法 5 条では，FTC 法以外の規制を受けている common carrier が適用除外となっている（15 U.S.C. § 45(a)(2)）。今回の規則の対象となる BIAS（Broadband Internet Access Service）提供事業者は，従来はこの common carrier に当たらないとされてきた。しかし，2015 年に FCC が採択した「オープンインターネット規則」によって，BIAS 提供事業者が common carrier として通信法による規制を受けることとなり，FTC 法の適用除外となるとともに，通信法が定める顧客情報のプライバシー保護の規定（47 U.S.C. § 222）が，適用されることになったのである。

情報通信分野のプライバシー保護に関しては，EU も「電子通信プライバシー指令[3)]」の見直しを検討しており，わが国でも個人情報保護法の改正を受けて電気通信事業分野ガイドラインの改正が検討されている。情報通信分野におけるビジネス環境の変化や技術の進展によって，事業者が収集・利用・共有する情報が生じるプライバシー上の懸念も大きくなっている。従来から，電気通信事業者に対しては，通信の秘密等を保護するために特別な規制が課せられている場合が多い。しかし，現在，インターネット上で利用者に関する情報を利用しているのは電気通信事業者だけではなく，Google，Facebook，Amazon，Netflix などのネットワーク上のプラットフォームを構築している事業者も，顧客に関する大量の情報を収集・利用している[4)]。このような事業者に対して，どのようなプライバシー保護を求めるべきであるかは，各国で議論となっている。

本稿では，米国 FCC の新しいプライバシー規則についてその背景と規制内容を概観し，わが国の今後の議論においてどのような示唆が得られるかについて考察したい。

1）Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Report & Order, FCC16-148 (2016), https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-148A1.pdf.

2）小向太郎「米国 FTC の消費者プライバシーに関する法執行の動向」堀部政男編『情報通信法制の論点分析』（商事法務，2015）151-162 頁。

3）Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

4）これらの事業者は，OTT（Over The Top）やプラットフォーム事業者等とも呼ばれるが，FCC の議論では「エッジプロバイダ（Edge Provider）」と分類されている。

Ⅰ　FCC の概要

1　設置根拠と役割

米国の FCC は，1934 年通信法に基づいて設立された独立行政委員会である。FCC の設立目的としては，有線および無線による州際および国際通信を規制することで，可能な限り米国内のすべての人々が差別なく高速かつ効率的な有線および無線による州際および国際通信を満足の行く設備によって合理的な価格で利用できるようにすること，国防の目的を達成すること，有線および無線による通信を利用することで生活と財産権の安全を向上すること，複数の政府機関に分かれていた権限を集約すること，が挙げられている（45 U.S.C. §151）。

委員会は，上院の助言と同意に基づき大統領によって任命された 5 名の委員によって構成され，同じ政党のメンバーはそのうち 3 名以内とされている。委員になりうるのは米国市民に限られ，規制対象となる企業等と利害関係があるものは委員となることができない。5 人の委員の中から，大統領が議長を選出する。任期は 5 年であるが，任期中に退任した委員があった場合，その後任の委員の任期は，退任した委員の残りの任期となる。なお，委員に空席があっても，残った委員による委員会の職務執行権限が損なわれることはない（47 U.S.C.§154）。

通信法（47 U.S. C. Chapter 5）の規定は，次の 7 つのサブチャプターに分かれており，それぞれのなかで FCC の権限と関与について定めている。

- SUBCHAPTER I-FCC の構成と権限（§§ 151 to 162）
- SUBCHAPTER II- コモン・キャリアに対する規制（§§ 201 to 276）
- SUBCHAPTER III- 放送局の認可要件等（§§ 301 to 399b）
- SUBCHAPTER IV- 規制手続き（§§ 401 to 416）
- SUBCHAPTER V- 違反に対する罰則・没収等（§§ 501 to 510）
- SUBCHAPTER V–A- ケーブル・テレビ等に関する規制（§§ 521 to 573）
- SUBCHAPTER VI- 雑則（§§ 601 to 622）

2　規制プロセス

FCC の規則制定は，多くの場合「notice and comment」と呼ばれる手続きによって行われ，FCC が特定のテーマに関する規則の採択や修正を検討していることを公表し，広く意見を求める形をとる。

この手続を開始する際に通常公表されるのが，NPRM（Notice of Proposed RuleMaking：規則制定案告示）である。この NPRM には，提案するルールの必要性，権限の根拠，理由が示されるとともに，提案するルールの規定そのものか，規制対象と規制項目に関する説明が記載される。FCC の提案の説明には，当該解決策の提案を選択した経緯や，検討している代替の解決策が含まれている場合もある。

NPRM に対してはパブリックコメントの募集が行われ，その提出期限や提出方法等も示される。パブリックコメントでは，提案に書かれているどのような事項に対してもコメントをすることができるが，通常は NPRM のなかに特に意見を求める項目が明示されている。パブリックコメントの募集期間は通常少なくとも 30 日が設けられるが，特に高度に技術的で複雑な問題については長い期間が設定され，迅速な対応が求められる場合には短期間となる場合もある。募集期間終了後，寄せられたコメントを勘案して，提案された規則の実施，新規または修正提案の作成，提案の取りやめのいずれかを決定し，ルール実施が決まった場合には最終規則が採択・公表される。最終規則では，パブリックコメントで提起された問題のうち重要なものに対する対応やルールの根拠と目的が説明されるとともに，ルールそのものを示す規定文が示されなければならない。

最終規則やそれに付随する分析に異議のある者は再審理の申立てをすることができ，FCC が申立てを認めるか却下するかを決定する。また，当該規則による影響を受ける者は，FCC の決定について司法審査を求めることもできる。事業を行う個人や団体から最終規則の全てまたは免除や猶予を求める請願がなされる場合もある。規則制定中に考慮されなかった独自の事情によって正当化されることが明らかになった場合には，請願が許可される可能性がある[5)]。

3　顧客情報のプライバシー

FTCが，FTC法5条の「商業活動に関わる不公正な競争手段と，商業活動に関わる不公正または欺瞞的な行為または慣行は違法（15 U.S.C. § 45 (a)(1)）」という，やや抽象的な条文を根拠に消費者プライバシー保護に関わる規制を行っているのに対して，FCCのプライバシー政策の根拠規定となる通信法222条（顧客情報のプライバシー，47 U.S.C. § 222）は，対象となる情報の定義や禁止事項を明記した比較的具体的な条文となっている。特に以下の規定は，今回の規則制定と関連が深い。

> 47 U.S. C. § 222　顧客情報のプライバシー
> (a)　一般規定
> 全ての電気通信事業者は，他の電気通信事業者（電気通信事業者が提供する通信サービスを再販売する電気通信事業者を含む），機器製造事業者，および顧客に関連する情報であって，これらの者に帰属する情報の秘密を，保護する義務を負う。
>
> (b)　通信事業者情報の機密性
> 電気通信サービスを提供する目的で他の通信事業者から顧客等に帰属する情報を受信または取得する電気通信事業者は，その目的でのみそのような情報を使用しなければならず，自身のマーケティング活動のためにこれらの情報を利用してはならない。
>
> (c)　CPNI（顧客に帰属するネットワーク情報）の秘密保護
> (1)　電気通信事業者のプライバシー保護義務
> 法に基づく要請または顧客の同意がある場合を除き，電気通信サービスの提供にともないCPNIを受信または取得する電気通信事業者が，特定個人を識別しうるCPNIを利用，開示，またはアクセス可能にすることができるのは，(A)そのような情報が生成された電気通信サービス，(B)そのような電気通信サービスの提供に必要であるか，提供の過程で利用されるサービス（電話帳の発行を含む），のいずれかを提供するためである場合に限られる。
> (2)　顧客からの要望に基づく開示
> 電気通信事業者は，顧客が指定した者に対して，顧客からの明示的な書面による要求に基づき，CPNIを開示しなければならない。
> (3)　顧客統計情報
> 電気通信サービスの提供によりCPNIを受信または取得する電気通信事業者は，顧客統計情報に関しては，第1項が定める以外の目的のために，利用，開示，またはアクセス可能にすることができる。地域中継事業者は，合理的な要請に基づき合理的かつ無差別な条件で他の電気通信事業者または個人に提供する場合に限り，顧客統計情報を，第1項が定める以外の目的のために，利用，開示，またはアクセス可能にすることができる。

なお，「加入者リスト情報」とは，電話帳に掲載されるような基本情報のことを（47 U.S. C. § 222 (h)(3)），「顧客統計情報」とは，「サービスまたは顧客のグループまたは属性に関する集合体のデータであり，個々の顧客の識別子および特性が当該データから除去されているもの」をいう（47 U.S. C. § 222 (h)(2)）。

Ⅱ　ブロードバンド顧客プライバシー保護規則

1　制定の背景

FCCは，「ブロードバンドサービスを始めとする電気通信サービスに関する消費者プライバシーの保護」に関して，2016年4月にNPRM[6]を公表し，同年10月27日には，「ブロードバンド顧客プライバシー保護規則」として採択されている。この規則制定手続きは，FCCが2010年以降取り組んできたネットワーク中立性政策を推進するために制定されたオープンインターネット規則の成立を受けたものである。

インターネットの利用範囲が拡大するに従って，インターネット上の通信量は急増を続けており，これに対応するネットワークを維持するための負担も大きくなっている。しかし，インターネットの仕組みは，通信料の拡大がネットワークを支える事業者の収入増につながるようには必ずしもなっていない。負担が大きくなったネットワーク事業者からは，ネットワークに大きな負荷をかけるビジネスを行っている事業者（FCCの議論では，エッジプロバイダと呼ばれる事業者等）にもコスト負担を求めるべきであるという主張がなされるようになってきた。これに対して，エッジプロバイダ等もインターネットへの接続に際してはコストを負担しているのであり，ネットワークのインフラ設備を運営する事業者や機関は，ネットワーク上を流れるコンテンツについて中立的な立場をとるべ

5）FCC, Rulemaking Process, https://www.fcc.gov/about-fcc/rulemaking-process.

6）Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, NPRM, 31 FCC Rcd 2500 (2016), https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-39A1_Rcd.pdf.

きであるという反論も行われている。これがネットワークの中立性に関する議論と呼ばれるものである。

米国においては，ブロードバンドへのアクセスを提供する事業者に対して，このような中立的な立場を取る義務を課すべきかどうかが議論されてきた。この「ネットワーク中立性」の議論においては，FCC が BIAS に対して規制権限を有するかどうかが，大きな論点となっていた。2010 年 11 月 12 月に採択された規則に対しては，Verizon が訴訟を提起し規制の効力が否定される判決が 2014 年 1 月 14 日に下されている[7] が，FCC の規制権限自体は否定されなかった。これを受けて FCC は，2015 年に新たなオープンインターネット規則[8] を制定した。これによって，一定の透明性や公平性を確保することが求められるとともに通信法 222 条が定める顧客情報のプライバシー保護に関する規定についても，BIAS に対して適用になることが明記されている。

オープンインターネット規則では，規制の対象となる BIAS を次のように定義している。

「有線または無線によるマス・マーケット向けの小売サービスであって，実質的にインターネットに接続している全ての端末や機器との間で，データの伝送や受信を可能にする機能の提供であり，この機能には通信サービスに付随するものや通信サービスの運用を可能にするものを含むが，ダイヤルアップ・インターネット・アクセスは含まれない。また，前の文に記載されているサービスと同等の機能を提供しているか，または本規則のこのパートに記載されている保護を回避するために使用されていると，委員会が判断した場合には，BIAS に該当することになる（para. 187）」

なお，この定義に該当する事業者は，一般に ISP（インターネット・サービス・プロバイダ）と呼ばれている事業者とほぼ重なる。そのため，今回の顧客情報のプライバシー保護に関する規則については，ニュース報道はもちろん，FCC のニュースリリースやファクトシート等でも，単に ISP に対する規制として紹介されることが多い。

2　規則の概要

ブロードバンド顧客プライバシー保護規則で FCC は，BIAS 提供事業者に対して顧客情報のプライバシー保護のために，透明性の確保，利用者の選択，セキュリティの 3 点を基本においている（para. 7）。FTC が求める消費者プライバシー保護と比べて，より厳格な規制といえるのは次のような点である。

⑴　透明性の確保（47 CFR Part 64 §64.2003.）
・情報の収集，使用，および共有について，①顧客に関して収集する情報のタイプ，②どのようにしてこの情報を使用・共有するのか，③どのようなタイプの主体にこの情報を共有するか，について顧客に明確な通知を行わなければならない。
・上記の情報は，サービス申込時と，プライバシーポリシーが大きく変更された場合にされなければならず，ウェブサイトまたはモバイルアプリでも，永続的に閲覧可能でなければならない。

⑵　利用者の選択（§64.2004.）
・下記のセンシティブな情報を利用・共有するためには，「オプトイン」による同意を得なければならない。
– 財務情報
– 健康情報
– 子供に関する情報
– 社会保障番号
– 正確な地理的位置情報（主として携帯電話または他のデバイスの現実世界における所在地）
– コミュニケーションの内容
– 通話の明細情報
– ウェブ閲覧履歴，アプリケーションの利用履歴，およびそれと同等に評価される機能の利用履歴
・上記のセンシティブな情報以外の情報を利用・共有するためには，基本的に「オプトアウト」による同意を得なければならない

⑶　セキュリティ（§64.2005.）とデータ侵害通知（§64.2006.）
・FTC のデータセキュリティ要件と NIST のサイバーセキュリティフレームワークに沿って，顧客データを保護するための合理的な措置を講じなければならない
・被害発生の可能性がないと合理的に判断された場合を除き，事業者が顧客の個人情報が不正に漏えいした判断する場合に，以下のことを通知しなければならない
– データ侵害の影響を受けた顧客に対して，可及的速やかに，ただし侵害が合理的に確定した後 30 日以内。
– 5,000 人以上の顧客に影響を及ぼす侵害があった場合には，FCC，連邦捜査局，米国シークレットサービスに対して，侵害が合理的に確定した後 7 営業日以内に

7）　Verizon v. FCC, 740 F.3d 623 (D.C. Cir. 2014).

8）　*2015 Open Internet Order*, 30 FCC Rcd at 5748.

- 5,000人未満の顧客に影響を及ぼす侵害について，FCCに対して，顧客が最初に通知されると同時に

なお，BIAS提供事業者が提供するBIAS以外のサービス（ソーシャルメディアウェブサイトの運営など）に関しては，これらの規制は適用にならない[9]。

3　BIASに対する法執行

今回の規則制定に先立って，FCCはBIAS提供事業者に対して，通信法222条に基づく法執行を既に行っている。

FCCは，2014年12月から，Verizon Wirelessが，UIDH（Unique IDentifier Headers，いわゆる「スーパークッキー」）を，顧客への通知や同意なく挿入したことに関して調査を開始していた。顧客がモバイル・インターネットを利用する際にトラフィックにUIDHが挿入されていると，そのトラフィックがどの顧客のものかを識別できる。これによって，Verizonや他の第三者から，顧客を選別してターゲット広告を配信することが可能になる。Verizon WirelessはUIDHの挿入を2012年12月に開始しており，2014年10月までこの事実を公表していなかったが，2015年3月までにはプライバシーポリシーを改訂しUIDHに関するオプトアウトの提供を開始していた。顧客に帰属する情報の適切な保護や，正確で適切な情報の開示を行ったかどうかについて，通信法第222条違反の疑いが持たれていた。

調査と調停の結果，2016年5月7日に同意判決が成立し，Verizon Wirelessはターゲットとする広告プログラムについて消費者に通知し，UIDHを第三者と共有する前に顧客のオプトイン同意を得て，Verizonグループの内部でUIDHを利用する場合には共有する前に顧客のオプトインまたはオプトアウトの同意を得ることになった。また，同社には135万ドルの罰金と，3年間のコンプライアンス・プランの採用が求められている[10]。

Ⅲ　注目すべき規定と今後の動向

1　対象事業者

すでに述べたように，今回の規則が対象とするのは，BIAS（インターネットアクセスを提供するISP等）であって，FCCがエッジプロバイダと呼ぶNetflixやAmazon，Googleのようなサービス・プロバイダは，対象とならない。しかし，現在のインターネットにおいて，顧客に対する大量の情報を収集・利用しており顧客のプライバシーに関する懸念が大きいのはむしろ，大規模なエッジプロバイダだという指摘もある。

たとえば，プライバシーに関する人権団体であるEPICは，パブリックコメントのなかで「ISPのプライバシールールは重要で必要」としながらも，FCCが「消費者のプライバシーに最も大きな脅威を与えるオンライン通信の最も重要な要素がISPである」としていることに対して，「オンライン通信エコシステムの現実と矛盾している」と批判している。むしろ，インターネットユーザーがさまざまなISP等のアクセス経路を経てつながっているのは，「本質的に1つのインターネット検索会社と1つのソーシャルネットワーク会社」であるとして，ISP以上に大きな脅威があるにもかかわらず，これらに対して規制が行われていないことを懸念している[11]。

今回の規則制定は，ネットワーク中立性政策に関する議論のいわば副産物として，BIASにFCCの規制権限が及ぶことになったことが契機となっている。そういう意味では，規制権限がおよばないエッジプロバイダに対して検討がなされていないのは，やむを得ない面がある。そもそも，電気通信事業者が取り扱う情報は，通信の秘密等として保護されるものがあり，多くの国でその扱いに特別な規制が行われているという背景もある。

わが国でも，電気通信事業法が「電気通信事業

9）FCC, Fact Sheet: The FCC adopts order to give broadband consumers increased choice over their personal information, https://apps.fcc.gov/edocs_public/attachmatch/DOC-341938A1.pdf.

10）*Verizon Wireless*, Order, 31 FCC Rcd 1843.

11）Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Report & Order, FCC16-148 (2016), p.210.

者の取扱中に係る通信の秘密」に関して，特別の保護を規定している。また，電気通信事業者が取り扱う情報は，通信の秘密に当たらなくてもプライバイシーの保護が必要とされる場合が多いと考えられてきた。総務省「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（平成16年8月31日総務省告示第695号）」では，電気通信事業者による個人情報の取得・利用について，次のような考え方を示している。

①電気通信サービスを提供するために必要な場合に限り，個人情報を取得するものとし（第4条第1項），その情報の利用目的は，電気通信サービスを提供するために必要な範囲を超えないものとする（第5条第3項）
②通信の秘密については，他の情報であれば利用目的の範囲を超えて利用が許容される法令等に基づく場合等（第6条第3項）であっても，利用者の同意がある場合その他の違法性阻却事由がある場合を除いては，取り扱わないものとする（第6条第4項）

このガイドラインは，個人情報保護法の改正を受けて改正が検討されており，2017年1月18日に改正案がパブリックコメントに付されている[12]。改正版では，上記に対応する部分が，次のようになっている（平成29年総務省告示第152号）。

①個人情報の取得について，できるだけ通信サービスを提要するために必要な場合に限るよう務めなければならず（第6条），利用目的を特定する際に，電気通信サービスを提供するため必要な範囲を超えないように努めらければならない（第4条第3項）
②通信の秘密については，利用者の同意がある場合その他の違法性阻却事由がある場合を除いては，利用してはならない（第5条）

電気通信事業者の事業範囲が拡大している現状を考慮して，個人情報全般については取得・利用の目的を電気通信サービスの提供に必要な範囲に限定することは，努力規定であることを明確にしたものと考えられる[13]。一方で，通信の秘密に関しては，厳格な立場を維持しているといえる。

わが国の通信の秘密には，通信内容以外の情報についても，個別の通信の通信当事者がどこの誰であるかということや，いつ通信を行ったかということも含まれると考えられており，かなり広い範囲の情報が対象になる。もし，各種サービスのアクセス履歴や利用履歴も通信の秘密として保護されることになると，エッジプロバイダのサービスはかなりの制約を受けることになる[14]。したがって，インターネット上でサービスを提供する事業者が電気通信事業者に当たるかどうかによって，その事業者が扱う情報が当該サービスの提供以外にも利用できるかどうかが異なってくることになる。

また，EUでは，電子通信プライバシー指令が2002年に採択され，2006年および2009年に改正されているが，この指令は，主として伝統的な電気通信事業者を対象とするものであった。現在，GDPR[15]の成立をうけた改正が検討されており[16]。欧州委員会は，これに代わる規則の提案を，2017年1月10日に公表している[17]。この規則提案は，適用対象を電子メールやオンラインメッセージング・サービスに拡大しており，規則が成立すれば，WhatsApp，Facebook Messenger，Skype，Gmail，iMessage，Viberのような新しい電子通信サービスの提供事業者についても，適用されることになる。

12） 総務省「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の解説（案）」総務省「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の改正案に対する意見募集」（2017年1月19日公示，2月17日締切）。

13） ガイドラインの対象になる「電気通信サービス」には，電気通信役務に「付随するサービス」が含まれる。これについては，「電気通信役務と一体的に提供されていて切り離すことができないサービス（ネットワークでのフィルタリング，ルータ等接続機器の貸与，システムの開発・保守等）や電気通信事業者が提供する電気通信役務の利用を前提としているサービス（端末の位置検索，セキュリティ，決済代行，端末の販売・保証，アプリケーションソフトウェア・動画・音楽配信，電子マネーポイント還元サービス，電話帳発行業務等）が該当」するとしている（11頁）。

2　位置情報[18)]

位置情報に関してFCCは，2012年に，「ロケーション・ベースド・サービス[19)]」という報告書で，位置情報を利用したサービスの重要性と今後の可能性について検討を行っており，特にプライバシーに対する懸念がこの分野での最重要課題の1つであるという認識を示している。そして，ロケーション・ベースド・サービスを提供する事業者に，①製品の開発段階開発初期段階でのプライバシーの配慮，②データのセキュリティ，③通知の時期と内容の充実，④データの最小化，といった取り組みを求めていた（40-41頁）。また，2016年4月に公表されたNPRMでは，特に配慮が必要な情報の候補として，特に地理空間情報（Geo-location）については，「顧客または顧客の端末の，物理的または地理的な位置情報に関する情報については，ブロードバンド・インターネット・アクセス・サービス提供事業者が当該情報を取得するために用いる技術や方式がどのようなものであるかに関わらず，ブロードバンドにおけるCPNIとみなす」ことを提案していた（16頁）。こうした議論を経て，ブロードバンド顧客プライバシー保護規則では，「正確な地理的位置情報」がセンシティブな情報と位置付けられ，その利用・提供に際しては「オプトイン」が求められている。

わが国でも，電気通信事業者の取扱う位置情報については，議論が行われている。わが国の携帯電話事業者が取得する位置情報は，「個別の通信を行った基地局の位置情報」「位置登録情報（端末所在地を基地局単位等で把握する情報）」「GPS位置情報（GPS機能により取得する情報）」の3種類があると考えられている。このうち「個別の通信を行った基地局の位置情報」は，通信の秘密であるとされる。さらに，総務省のガイドラインでは「位置登録情報」「GPS位置情報」についても，「ある人がどこに所在するかということはプライバシーの中でも特に保護の必要性が高い上に，通信とも密接に関係する事項であるから，通信の秘密に

14）　わが国の電気通信事業法において，電気通信事業とは「有線，無線その他の電磁的方式により，符号，音響又は影像を送り，伝え，又は受けること」（電気通信事業法第2条第1号）であり，これを行うための電気的設備を用いて他人の通信を媒介し，その他電気通信設備を他人の通信の用に供する役務（サービス）を，「他人の需要に応ずるために提供する事業」（第4号）が電気通信事業であると定義されている。そして，インターネットのいわゆる上位レイヤサービスに関して，総務省の「電気通信事業参入マニアル［追補版］―届出等の要否に関する考え方及び事例―」（平成17年8月18日）では，クローズド・チャット（サイト上にチャットルームを開設し，アクセスした利用者と不特定の会話希望者とをマッチングした上で，両者間のみに閉じた会話とを媒介するものをいう），出会い系サイト（交際に関する情報等をインターネット経由で閲覧できる状態に置き，その情報に係る異性交際希望者に対する利用者からのメッセージを電子メール等用いて媒介するもの），電子メール運営のためのホスティング（企業等が電子メールを利用できるようサーバ等を設置して，当該企業等にサーバの容量貸し及び電子メールの機能を提供するものを），国外サーバを用いた電子メール（国内に事業を営む拠点を置くものが，国外に設置した電気通信設備（サーバ等）を用いて，インターネットを通じて国内の利用者向けに提供する電子メール）等は電気通信事業者として登録または届出が必要となる事例としてあげられている。また，「いわゆる『ポータルサイト』『SNS（Social Networking Site）』など，様々なサービスを包含した総合サービスについては，それぞれのサービス毎に電気通信事業者として登録または届出を要するかどうか判断することになる」としている。なお，現在パブリックコメントにかかっているガイドラインの解説（総務省「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の解説（案）」（平成29年1月19日））では，実際に届出・登録を行っているかどうかに関わらず，電気通信事業を行っているものは対象になるということを明示している（11頁）。なお，同解説案では，「電気通信設備を国外のみに設置するものであって，日本国内に拠点を置かないもの」は電気通信事業者に当たらず，ガイドラインも適用にならないという考え方を示している（9頁）。しかし，実際に問題になるのは，「国内に拠点を置かない」とはどういう状態かということであろう。

15）　Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

16）　EUでは，域内の個人情報保護をより強固にするためにGDPR（一般データ保護規則）が2016年5月に発効し，2018年5月に施行される予定である。

17）　Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Erectoronic Communications).

18）　位置情報に関する規制の動向については，小向太郎「ネットワーク接続機器の位置情報に関するプライバシー・個人情報保護制度の動向」情報処理学会研究報告電子化知的財産・社会基盤（EIP）2016-EIP-74, 2016-11-17を参照。

19）　FCC Wireless Communications Bureau, Location-Based Services - An overview of opportunities and other considerations, May 2012.

準じて強く保護することが適当である」と位置づけ，情報の取得に際して利用者の同意を取得すること等を求めてきた。

前述の総務省ガイドラインの改正に関する議論でも，位置情報の取扱が主要な検討課題となっており，位置情報の利用に特にプライバシーへの配慮を求めるとともに，位置情報の利活用を促進する観点からも検討がなされており，「通信の秘密に係る位置情報について十分な匿名化を行った上で他人への提供その他の利用を行う場合」について，約款等に基づく包括同意でも一定の要件のもとでは有効な同意となりうるという考え方が示されている[20]。

なお，EU 電子プライバシー指令の改正に向けた規則提案においては，位置情報やトラフィック・データのようなメタデータについて，サービス提供や課金等のために必要がなくなった場合に，本人の同意がなければ匿名化か消去をしなければならないとされており（第 7 条第 2 項，第 3 項），ユーザが利用する端末やそれに関連して保存される情報に関しても保護の規定が置かれている（第 8 条）。

3　今後の動向

「ブロードバンド顧客プライバシー保護規則」は，規則の提案からわずか 6 ヶ月という非常に短い期間で採択にいたっている。委員長の任期終了や，大統領選挙を意識したのではないかという意見もある[21]。そして米国では，Donald Trump 大統領が誕生し，FCC の委員長も，ネットワーク中立性規制の推進者であった民主党の Tom Wheeler 委員長に代わって，2012 年から共和党を代表する委員を務めてきた Ajit Pai 新委員長が指名を受けている。ネットワークの中立性に関して，一般的には，民主党がネットワークの利用者が公平にアクセスできる政策を推進してきたのに対して，共和党はキャリアに中立性を義務付ける規制に反対しており，Pai 新委員長もネットワーク中立性の義務付けには消極的な立場である。また，Pai 新委員長は，「ブロードバンド顧客プライバシー規則」にも，次のような非常に強い反対意見を寄せている。

まず，FTC が主導してきたオンラインプライバシーに関する技術に中立的な枠組みが，利用者にとってわかりやすく安心を生むものであり，米国のプライバシー保護のアプローチとして望ましいとし，ISP に対して特別な規制を課すことに反対している。そして，FCC 規則が，ISP が入手する情報が特別かつ重要なものであるのに対して，エッジプロバイダは「断片」の情報しか見ることができないと評価していることを，自分の規制権限のある事業者を規制したいがための我田引水な議論として痛烈に批判している[22]。

正規の手続きを経て採択された規則が，すぐに変更されることはないかもしれないが，今後の FCC による規制方針がどのようになるかは，未知数の部分が大きい。また，これまで見たように，米国の制度は手続き面も含めてわが国とも EU とも大きく異なる。しかし，議論や試行錯誤が活発に行われていることから，議論の蓄積は技術面も含めて大きく，参考となる検討も多いと考えられる。

今回の「ブロードバンド顧客プライバシー保護規則」は，ネットワーク中立性政策に関する議論の結果，BIAS 提供事業者に対して FCC の規制権限が及ぶようになったことに端を発している。そのため，伝統的な電話会社を中心に行われてきたプライバシーに関する規制方針を，FCC の規制権限が及ぶ BIAS 提供事業者にだけ拡張した面があることは否定できない。しかし，このような規制側の縦割りが原因で，もし事業者がビジネスをおこなう条件に不均衡が生じるのであれば，インターネット関連ビジネスの健全な競争や発展にとって問題であろう。伝統的な電気通信事業と新

20）総務省「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の解説（案）」（平成 29 年 1 月 19 日）116 頁，総務省「『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』改正（案）考え方・概要」（平成 28 年 12 月 19 日）10 頁。

21）Rosemary C. Harold, *THE FCC FORGOT SOMETHING IN PIECING TOGETHER ITS COMPLEX PROPOSAL FOR BROADBAND PRIVACY REGULATION: CONSUMERS*, 17 Federalist Soc'y Rev. 62.

22）Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Report & Order, FCC16-148 (2016), pp.209-210.

しく急成長しているネットワーク関連ビジネスにおけるプライバシー保護にギャップが存在するという問題は，わが国でもEUでも顕在化しつつあるといえる。

情報通信分野におけるプライバシーの保護に関しては，どのようなサービスを提供する事業者のどのような情報が利用者にとって懸念になりうるのかを，既存の法制度に過度に拘泥せずに検討する必要が出てきていることは明らかである。今後，米国においてもEUにおいても，インターネットにおけるビジネスの実態に即した規制の見直しは，継続して行われていくと考えられる。特に，わが国でも議論になっている位置情報の取扱は，IoTやビッグデータ，AI等の進展によってますます重要になる。諸外国における議論の動向を参考にしつつ，実態に即した規制を実現していくことが重要であろう。

【追記】

本稿脱稿後に，議会審査法（the Congressional Review Act, 5 U.S.C. §802）に基づき，「ブロードバンド顧客プライバシー規則」を撤廃する決議が連邦議会の上下院で可決され，2017年4月3日にトランプ大統領の署名を受け，正式に撤廃された。これにより，本稿で紹介をしたBIASに対する規制は，現実には実施されないことになった。今後，ISPやエッジプロバイダに関するプライバシー保護について，新たな規制が検討されるかどうかは今のところ明らかになっていない。しかし，今回の規則制定および撤回の過程で，通信ネットワークに関するプライバシー保護については，従来のように電気通信事業者に対してのみ厳しい規制を行うことが実情に即していないことが，改めて浮き彫りになったとはいえるであろう。

検索結果の削除をめぐる裁判例と今後の課題

東京大学大学院法学政治学研究科教授
宍戸常寿
SHISHIDO George

Ⅰ　はじめに

インターネットの普及から20年あまりが過ぎ，人間の社会生活は大きく変容した。表現の自由，国民の知る権利は質量ともに拡大したが，法がそれに十分対応できているかどうかは定かではない。とりわけ問題になってきたのが，違法有害情報の発信に対する対応である。日本では2001年にプロバイダ責任制限法が制定され，民間の自主的な取組と併せて，人格権侵害については一定の措置が図られてきたところだが，更に10年あまりが経過した今日，インターネット上の表現の自由・知る権利と人格権をめぐる問題状況は大きく変化している。

その中心にあるのが，情報流通を媒介する役割を担っているポータルサイト，特に検索エンジンである。検索エンジンはグローバル企業によって担われる場合も多く，日本に限らず世界大の課題として，様々な取組が国際機関や各国で様々な取組がなされている。2014年には，「忘れられる権利」に関するEU司法裁判所の先決裁定が世界的に注目された。また，日本においても検索エンジンに対して，検索結果の非表示を求める裁判がしばしば起きており，グーグルの提供する検索エンジンの表示に対する差し止めを認めた東京地裁平成26年10月9日決定以降，社会的にも大きな関心を呼んできたところである[1)]。

本稿では，こうした「忘れられる権利」をめぐる動向及び検索結果の削除をめぐる裁判例を概観した後，平成29年1月31日付で下された最高裁決定について検討し，今後の課題を展望することとしたい。

Ⅱ　いわゆる「忘れられる権利」

1　検索エンジンの位置づけ

日々刻々と膨大な情報が登場するインターネット上の情報流通にとって，発信・閲覧いずれにおいても，検索エンジンが不可欠な媒介者としての役割を担っていることは，よく知られている。インターネット，そして検索エンジンが発展したアメリカにおいては，1996年連邦通信品位法230条（47 U.S. Code § 230）の(c)(1)が「双方向のコンピュータサービスのプロバイダ（Provider）または

1)　関連する文献は多数を数えるが，ここでは石井夏生利「『忘れられる権利』をめぐる議論の意義」情報管理58巻4号（2015年）271頁以下，宇賀克也「『忘れられる権利』について――検索エンジン事業者の削除義務に焦点を当てて」論究ジュリスト18号（2016年）24頁以下，奥田喜道編『ネット社会と忘れられる権利――個人データ削除の裁判例とその法理』（2015年），神田知宏『ネット検索が怖い――「忘れられる権利」の現状と活用』（2015年），宍戸常寿＝門口正人＝山口いつ子「【鼎談】インターネットにおける表現の自由とプライバシー――検索エンジンを中心として」ジュリスト1484号（2015年）ii頁以下，鈴木秀美「『忘れられる権利』と表現の自由――ドイツ連邦通常裁判所の判例を手がかりに」メディア・コミュニケーション66号（2016年）15頁以下，曽我部真裕「日本における『忘れられる権利』に関する裁判例及び議論の状況」江原法学49号（2016年）1頁以下，宮下紘「忘れられる権利と検索エンジンの法的責任」比較法雑誌50巻1号（2016年）35頁以下を挙げるにとどめる。

利用者は，他の情報コンテンツプロバイダにより提供される情報の発行者（Publisher）または発信者（Speaker）として扱われてはならない。」と定めていることから，検索エンジンは一般に検索結果の表示による法的責任を免除されていることになる。

2　EU 裁判所の先決決定

これに対して EU 司法裁判所は 2014 年，EU データ保護指令の解釈として EU 市民の「忘れられる権利」（right to be forgotten）を承認し，それに基づきグーグルに対して適法に発信された債務情報について，検索結果から削除することを求めた（Case C-131/12 Google v. AEPD, 2014.5.13）。

データ保護指令 12 条の(b)は，アクセス権すなわちデータ主体の「管理者」（controller）に対する権利として，「適切な場合には，特にデータの不完全又は不正確な性質のために，この指令の規定に従わないで取り扱われた修正，消去又はブロック」を保障する。そして同 14 条の(a)はデータ主体の異議申立権として，「少なくとも第 7 条(e)及び(f)に規定された場合には，国内法に別段の規定がある場合を除き，いつでも自己に関するデータの取扱いに対して，自己の特定の状況に関連するやむにやまれない正当な理由を根拠として，異議申し立てを行うことができること。適法な異議申し立てがあった場合には，管理者によって始められた取扱いに，当該データを含むことはできない。」と規定する[2)]。

EU 司法裁判所は，検索エンジンがデータ保護指令にいう「管理者」に当たるとした上で，同指令の後に成立した EU 基本権憲章の定めるプライバシーの権利及び同 8 条の定める個人データ保護の権利に照らして指令を解釈し，データ主体は処理目的との関係で不適切であり，重要性がないか失われた，または過剰である場合には削除を求めることができること，検索エンジンに対して，当初は合法であったデータが不必要となった場合に，ウェブサイトのリンクの削除を求めることができるものと解釈した。なお，忘れられる権利の対象として削除の対象となっているのは，あくまで検索結果だけであり，検索によりリンクが表示される元の新聞サイトは対象外であることにも，注意が必要である。

3　その後の展開及び EU データ保護規則

この先行決定は，いわば創造的な解釈により，EU データ保護規則案の内容として当時検討されていた「忘れられる権利」を先取りして認めたものといえるが，同時にこの権利の行使に当たってはデータ主体の権利と関連する利益（公衆の利益）との比較衡量を求めている。この先行決定を踏まえて，EU 各国のデータ保護機関から成る 29 条作業部会は検索結果削除の申立ての共通処理基準となるガイドラインを 2014 年 11 月 26 日に公表した。そこでは，個人の名前での検索，公的役割・公人，未成年者，検索結果の正確性，データ主体との関連性，センシティヴ性，最新性，偏見ないし否定的なプライバシーインパクト，リスクを生じさせる情報，公開当時の文脈，報道目的の元サイト，公開の権限・義務を有する元サイト，刑事犯罪といった多様な考慮要素が挙げられており，検索結果を削除するかどうかの具体的判断の微妙さ・難しさが，浮き彫りになった。

また各国のデータ保護機関や裁判所においても，先行決定の前後から，検索結果の削除の可否，範囲，あるいは EU 域外での検索結果まで非表示を求めるかどうかについて，様々な判断がなされている。先行決定を受けてグーグルは，有識者会議を開く等して，申立てにより EU 域内で忘れられる権利への対応を進めているが，これに対してたとえば BBC が自己のサイトで検索結果から削除されたものを一覧に示して対抗する等，インターネットにおける表現の自由・知る権利と「忘れられる権利」の間の調整が，独り検索エンジンを超えて，様々な主体に関わるものであることが，意識されるようになっている。

先決決定後の 2016 年 4 月に発効した EU データ保護規則の 17 条は「消去の権利（忘れられる権利）」と題する規定を置いた。その(1)では，「(a)個

2）　堀部政男研究室仮訳による。

人データが収集された又はその他取扱いの目的に関して，当該個人データがもはや必要ない場合」や「(c)データ主体が，第 21 条第 1 項により不服を申立て，かつ取扱いに関して優先する法的根拠がない場合。又はデータ主体が第 21 条第 2 項により不服を申し立てる場合」について，データ主体が個人データを管理者に消去させる権利（管理者の義務）を定めるが，しかしこの規定は「(a)表現及び情報の自由の権利の行使に必要な場合」には適用されないことが(3)で明らかにされている[3)]。

4　日本での議論の注意点

要点を絞っていえば，EU における「忘れられる権利」はデータ保護法制の枠組みの中で位置づけられること，この権利を承認したとしてもなお表現の自由・知る権利との具体的な調整が課題であること，本来この問題の射程は検索エンジンに限られるものではなく広汎な主体に及びうるものであること，を確認することができよう。

日本でも検索結果の削除が，とりわけメディアにおいて「忘れられる権利」の名で語られることがあるが，このような経緯を踏まえれば，それが EU における実定法制度を指しているのか，日本法におけるものなのか，後者だとして既に実定法上の根拠を有するものとして存在するという主張なのか，立法論ないし政策的な目標としての提言であるのかを，混交せずに議論する必要がある。

ひとまず EU のデータ保護法制に相当するものとして，日本では個人情報保護法が存在するが，氏名等による検索結果が個人情報に該当するとしても，検索エンジンは「個人情報データベース」に当たらず，保有個人データは削除請求権等の対象とならないことは，確立した解釈である。現にこれまで日本で「忘れられる権利」の名の下に争われているのは，個人情報保護法上の削除請求ではなく，民事法上の人格権（名誉，プライバシー）に基づく検索エンジン事業者に対する損害賠償及び削除請求である。そうすると，検索結果によるこれらの法的問題は，従来の民事法理の一応用事例として考えるべきことになる。

そのように考えるのであれば，既存の判例法理との関係では，2 つの点に注意する必要がある。第 1 に，検索結果の削除が争われた事例の多くが仮の地位を定める仮処分の手続によるものだが，それが表現行為に対する事前抑制となり，また簡易迅速を旨とする手続の特性上，「表現の自由を保障し検閲を禁止する憲法 21 条の趣旨に照らし，厳格かつ明確な要件のもとにおいてのみ許容されうる」（北方ジャーナル事件判決，最大判昭和 61・6・11 民集 40 巻 4 号 872 頁）と考えるべきではないか。第 2 に，検索結果の削除で争われる事例の多くは，前科，あるいは過去の事実であって現時点において不名誉ないし知られたくないようなものが記載されたサイトが氏名等の検索により表示されないようにすることを求めるものであり，この点で前科について「時の経過」による保護を認めたノンフィクション「逆転」事件判決（最判平成 6・2・8 民集 48 巻 2 号 149 頁）との関係をどのように考えるかが，これまでの議論の焦点であったことに，留意しておきたい。

Ⅲ　下級審の裁判例の概観

1　従来の裁判例

裁判例としてはじめて検索結果の削除を認めたのは，東京地決平成 26・10・9 判例集未登載であるとされる。それ以前の裁判例で検索結果の削除を否定したものとしては，筆者が知り得た限りでは，東京地決平成 20・11・14，東京地判平成 22・2・18，東京地決平成 22・2・26，東京高判平成 22・6・29，東京地判平成 23・12・21，神戸地判平成 24・2・28，大阪地決平成 25・3・29，東京地判平成 25・5・30，東京高判平成 25・10・30，東京高判平成 26・1・15（いずれも判例集未登載）及び京都地判平成 26・8・7 判時 2264 号 79 頁がある。

最後に挙げた京都地裁判決は，盗撮行為による逮捕歴等に関するヤフーの検索結果の削除が，逮捕から約 1 年半経過した時点で求められた事案であるが，裁判所は検索エンジンの仕組み及び一般

3)　一般財団法人日本情報経済社会推進協会仮訳による。

的な利用者の通常の認識から，検索結果が表示するのは「検索ワードである原告の氏名が含まれている複数のウェブサイトの存在及び所在（URL）並びに当該サイトの記載内容の一部という事実」であって逮捕事実自体を摘示するものではないから，そもそも人格権の侵害に当たらない，という理解を示した。その上で，念のためとして，名誉毀損・プライバシー侵害の判断を行い，逮捕事実等について真実性の証明を認めて名誉毀損は成立せず，また社会の正当な関心事であるとしてプライバシー侵害をも否定した。

2　東京地裁平成26年10月9日決定とそれ以降

これに対して，先に述べたとおり東京地決平成26・10・9判例集未登載は，グーグルに対して，氏名の検索により過去に不良集団に属していた事実に関する結果が表示されないよう命じたもので，メディアで「忘れられる権利」を認めたものとして注目されたものである。

同決定は，被保全権利をプライバシー権として理解した上で，その侵害行為の差止請求の可否は，「侵害行為の対象となった人物の社会的地位や侵害行為の性質に留意しつつ，予想される侵害行為によって受ける被害者側の不利益と侵害行為を差し止めることによって受ける侵害者側の不利益を比較衡量して決するべきである」とした。そして，前科等についてはプライバシー権の1つとして法的保護に値する利益である反面で公表が許される場合もあるとして，「その者のその後の生活状況のみならず，事件それ自体の歴史的又は社会的な意義，その当事者の重要性，その者の社会的活動及びその影響力について，その著作物等の目的，性格等に照らした前科等を公表することの意義及び必要性をも併せて考慮した上，前科等に関わる事実を公表されない法的利益が優越するか否か」により判断すべきであるとした。この判断基準は，ノンフィクション「逆転」事件判決の個別的比較較量の枠組を，そのまま検索結果の削除に関する仮処分に転用したものといえる。

そして同決定は，237個の削除申立てのうち122個について，先の基準から「タイトル及びスニペットそれ自体から債権者の人格権を侵害していることが明らか」であり，他方でグーグルに削除義務を課すことが不当な不利益になるとはいえず，また「他者の人格権を害していることが明白な記載を含むウェブサイトを検索できることが本件サイトを利用する者の正当な利益ともいい難い」として，削除を命じたものである。その際に同決定は，個々のタイトル及びスニペットそれ自体が人格権侵害に当たることを理由に，グーグル側が主張していた，検索結果のリンク先のウェブサイトの管理者に削除を求めるべきだとの反論を退けている。

同決定の後，筆者が知り得た限りでは，検索結果の削除を認める裁判例として，後述するさいたま地決平成27・12・22判時2282号78頁のほか，東京地決平成27・5・8，さいたま地決平成27・6・25，東京地決平成27・11・27，東京地決平成27・12・1，札幌地決平成27・12・7，東京地決平成28・7・14，東京地決平成28・8・17があり，逆に検索結果の削除を認めない裁判例としては，大阪高判平成27・2・18，東京高決平成27・7・7，千葉地松戸支決平成27・10・16，札幌地決平成28・4・25，徳島地決平成28・6・23，東京高決平成28・7・12，名古屋地決平成28・7・20，札幌高決平成28・10・21，名古屋地決平成28・10・31（いずれも判例集未登載）が見られたところであった。

これらの裁判例を通じて特徴的なのは，削除の可否についての判断基準について，削除を認めるものが前掲東京地決平成26・10・9と同じく個別的比較衡量によるのに対して，削除を認めないものが検索結果の表示それ自体から明白な人格権侵害に当たることを求めていた点である。その背後には，第1に検索結果の表示それ自体が表現行為に当たるとしても検索エンジンを情報の第一次的な発信者と同様の立場にあるものと考えるかどうか，第2に仮処分による差止めと表現の自由の関係をどのように考えるかについて，それぞれ見解の相違が窺えるところである。

なお，前掲東京地決平成26・10・9に対してグーグル側が保全異議を申し立てしたところ，前掲東京地決平成28・7・14はそのうちの63個について，削除を求めた本人が自ら当該事実を公表し利用していた等の理由で，削除命令の取消しを命

じた。仮処分による個別的比較衡量の判断の危うさを示す一例といえるように思われる。

3　東京高裁平成 28 年 7 月 12 日決定

これらの裁判例の中でも注目されたのは，公刊された裁判例としてはじめて「忘れられる権利」に言及した，さいたま地決平成 27・12・22 判時 2282 号 78 頁であった。同決定は，児童買春行為での逮捕・罰金刑の執行から 3 年余経過した時点で，県及び氏名の検索で表示される結果の削除を認めた前掲さいたま地決平成 27・6・25 の保全異議審であった。その保全異議審では，「一度は逮捕歴を報道され社会に知られてしまった犯罪者といえども，人格権として私生活を尊重されるべき権利を有し，更生を妨げられない利益を有するのであるから，犯罪の性質等にもよるが，ある程度の期間が経過した後は過去の犯罪を社会から『忘れられる権利』を有する」と述べられている。もっともこの言明は，更生を妨げられない利益が検索結果の表示により受忍限度を超えて侵害されているという評価を行う際の理由づけとして述べられているにとどまり，「忘れられる権利」それ自体を独立の権利として承認したものではないことに，注意が必要である。

これに対して同事件の保全抗告審である東京高決平成 28・7・12 判時 2318 号 24 頁は，「人格権の一内容としての名誉権ないしプライバシー権に基づく差止請求の存否とは別に，『忘れられる権利』を一内容とする人格権に基づく妨害排除請求権として差止請求権の存否について独立して判断する必要はない」として，検索結果の削除を従来の判例法理の延長線上で捉える姿勢を示した。そして，北方ジャーナル事件判決，ノンフィクション「逆転」事件判決を引用するとともに，インターネットが「重要な社会的基盤の 1 つとなっていること」，「全文検索型のロボット型検索エンジンによる検索エンジンは必須のものであって，それが表現の自由及び知る権利にとって大きな役割を果たしていること」に言及している。

その上で東京高裁は，「削除等を求める事項の性質（公共の利害に関わるものであるか否か等），公表の目的及びその社会的意義，差止めを求める者の社会的地位や影響力，公表により差止請求者に生じる損害発生の明白性，重大性及び回復困難性等だけでなく，上記のようなインターネットという情報公表ないし伝達手段の性格や重要性，更には検索エンジンの重要性等も総合考慮して決するのが相当」という削除の判断基準を示した。この基準は，削除を求める側に有利な個別的比較衡量の基準と，検索エンジンに有利な明白な人格権侵害の基準のちょうど中間に位置するものと考えることができる。すなわち「だけでなく」以前に挙げられた考慮要素はひとまずプライバシーを侵害する表現行為の差止め一般に妥当しうるものでありこの点で個別的比較衡量の基準に近いが，それにインターネットの性格や検索エンジンの重要性の考慮をも求める点で，検索エンジン側に有利に天秤を傾けている，と解しうるものである。

このように述べた上で東京高裁は，具体的事案の判断としては検索結果の削除を否定した。その際，「実際の利用態様からは，タイトル及びスニペットが独立した表現として機能することが通常」であると述べて，検索エンジンが「単なる媒介者で，名誉権侵害の責任を負うものではない」とのグーグル側の主張を退ける一方，検索結果に係る犯行の公共性が未だ失われていないことに加えて，検索結果の削除が「多数の者の表現の自由及び知る権利を大きく侵害し得るものである」とした点では，保全異議審等とは逆向きに検索エンジンの役割を評価したものとみることができる。

Ⅳ　最高裁平成 29 年 1 月 31 日決定

1　決定要旨

これまで述べたとおり，検索結果の削除については下級審の裁判例が分かれ，最高裁の判断が期待されていたところである。これに答えて最決平成 29・1・31 裁時 1669 号 1 頁は，前掲東京高決平成 28・7・12 に対する許可抗告において，以下に述べるような一定の解釈を示した。

「⑴個人のプライバシーに属する事実をみだりに公表されない利益は，法的保護の対象となるというべきである（最高裁昭和 52 年（オ）第 323 号同 56 年 4 月 14 日第三小法廷判決・民集 35 巻 3 号 620 頁，最高裁平成元年（オ）第 1649 号同 6

年2月8日第三小法廷判決・民集48巻2号149頁，最高裁平成13年（オ）第851号，同年（受）第837号同14年9月24日第三小法廷判決・裁判集民事207号243頁，最高裁平成12年（受）第1335号同15年3月14日第二小法廷判決・民集57巻3号229頁，最高裁平成14年（受）第1656号同15年9月12日第二小法廷判決・民集57巻8号973頁参照）。他方，検索事業者は，インターネット上のウェブサイトに掲載されている情報を網羅的に収集してその複製を保存し，同複製を基にした索引を作成するなどして情報を整理し，利用者から示された一定の条件に対応する情報を同索引に基づいて検索結果として提供するものであるが，この情報の収集，整理及び提供はプログラムにより自動的に行われるものの，同プログラムは検索結果の提供に関する検索事業者の方針に沿った結果を得ることができるように作成されたものであるから，検索結果の提供は検索事業者自身による表現行為という側面を有する。また，検索事業者による検索結果の提供は，公衆が，インターネット上に情報を発信したり，インターネット上の膨大な量の情報の中から必要なものを入手したりすることを支援するものであり，現代社会においてインターネット上の情報流通の基盤として大きな役割を果たしている。そして，検索事業者による特定の検索結果の提供行為が違法とされ，その削除を余儀なくされるということは，上記方針に沿った一貫性を有する表現行為の制約であることはもとより，検索結果の提供を通じて果たされている上記役割に対する制約でもあるといえる。

以上のような検索事業者による検索結果の提供行為の性質等を踏まえると，検索事業者が，ある者に関する条件による検索の求めに応じ，その者のプライバシーに属する事実を含む記事等が掲載されたウェブサイトのURL等情報を検索結果の一部として提供する行為が違法となるか否かは，当該事実の性質及び内容，当該URL等情報が提供されることによってその者のプライバシーに属する事実が伝達される範囲とその者が被る具体的被害の程度，その者の社会的地位や影響力，上記記事等の目的や意義，上記記事等が掲載された時の社会的状況とその後の変化，上記記事等において当該事実を記載する必要性など，当該事実を公表されない法的利益と当該URL等情報を検索結果として提供する理由に関する諸事情を比較衡量して判断すべきもので，その結果，当該事実を公表されない法的利益が優越することが明らかな場合には，検索事業者に対し，当該URL等情報を検索結果から削除することを求めることができるものと解するのが相当である。」

以上のような判断基準を示した上で，最高裁は「本件事実を公表されない法的利益が優越することが明らかであるとはいえない」として，検索結果の削除を認めなかった。

2　検　討

以下では，この最高裁決定について，5点コメントしておきたい。

第1に，検索結果の削除について，比較衡量を明白性の要件で加重した（「当該事実を公表されない法的利益が優越することが明らかな場合」）基準が取られている点が注目される。これは，個別的比較衡量の基準とも明白な人格権侵害性を要求する基準とも異なるものであるが，ひとまずは一般に検索エンジンに有利な基準ではあって，検索結果の削除を安易に認める一部下級審の傾向に歯止めをかけたものとみることができる。ただし，なお事案においては検索結果の削除の余地を残すものであり，いかなる条件が揃えば「明らかな場合」といえるのかについて，今後の裁判例の集積が俟たれることになろう。

第2に，最高裁は，検索結果の削除を，プライバシー権侵害一般の事案類型の中で捉えている。すなわち最高裁は，ノンフィクション「逆転」事件にとどまらず，前科照会事件（最判昭和56・4・14民集35巻3号620頁），「石に泳ぐ魚」事件（最判平成14・9・24判時1802号60頁），長良川事件（最判平成15・3・14民集57巻3号229頁）及び早稲田大学講演会名簿提出事件（最判平成15・9・12民集57巻8号973頁）の各最高裁判決を引用している。このような判例引用からは，検索結果の削除を「時の経過」から離れて捉える最高裁の立場が垣間見られるように思われる。

確かに，前科の公表が問題となったノンフィクション「逆転」事件においてはいったん公知であった事実が時の経過により非公知の，したがって

プライバシーの状態に変化したことが前提であったのに対して，検索エンジンは公知の状態をそのまま継続させている（いわば「忘れることを忘れた」）とみることができるので，ノンフィクション「逆転」事件判決を検索結果の削除に関する先例として扱って良いかどうかについて疑問を呈する向きもあった。最高裁は，同判決を先例として挙げたものの，その他の判例をも引用することで，いわばその特権的地位を否定したものといえよう。このように考えれば，本決定が具体的事件の解決において，逮捕時からの時の経過に具体的に言及することなく，端的に児童買春が「社会的に強い非難の対象とされ，罰則をもって禁止されている」ということから「今なお公共の利害に関する事項」であるとしたことも，説明ができるように思われる。

第3に，今の点と関連して，比較衡量の判断枠組みが，ノンフィクション「逆転」事件ではなくて長良川事件判決に依拠している点が注目される。長良川事件判決は，週刊誌による少年事件の仮名報道が争われた事件であり，「本件記事が週刊誌に掲載された当時の被上告人の年齢や社会的地位，当該犯罪行為の内容，これらが公表されることによって被上告人のプライバシーに属する情報が伝達される範囲と被上告人が被る具体的被害の程度，本件記事の目的や意義，公表時の社会的状況，本件記事において当該情報を公表する必要性など，その事実を公表されない法的利益とこれを公表する理由に関する諸事情を個別具体的に審理し，これらを比較衡量して判断する」ものとしていた。同判決は現在，表現の自由とプライバシーの衝突が問題となる不法行為訴訟において一般的な判断枠組みとして参照されており，本決定の基準は，この判決の考慮要素を適宜修正して時の経過的要素（「記事等が掲載された時の社会的状況とその後の変化」）を加えたものと理解できる。

ただしそうだとして，本決定の基準を文言どおりに理解するならば，「忘れられる」ための時の経過の起算点は，たとえば前科であれば犯行時ではなく，その犯行について言及し検索の対象となるインターネット上の記事の掲載時であるということになる。この理解が正しいのだとすれば，コピペの繰り返しにより新たに作成される2ちゃんねるや「まとめサイト」上の記事について，この基準に基づき検索結果の削除を認めることには，困難が生じるのではないか。

第4に，最高裁による検索エンジンの理解及び評価も，注目に値する。まず最高裁は検索結果の提供が「検索事業者自身による表現行為」であると判断して，検索事業者が媒介者に過ぎず削除の責任を負うことはないとの前掲京都地判平成26・8・9のような立場を否定した。他方，利用者の「知る権利」に明示的に言及しないものの，「現代社会においてインターネット上の情報流通の基盤」としての検索エンジンの重要性にも言及しており，この点は前掲東京高決平成28・7・12と同様である。

しかし表現行為であるとか，重要な役割といった抽象的な言い回しは，検索結果の削除に対する態度をそれ自体として左右するものではない。むしろ問題の核心は，いかなる意味で「表現行為」であるのか，である。この点で最高裁は「検索結果の提供に関する検索事業者の方針」に着目し，検索結果の削除を余儀なくされることが「上記方針に沿った一貫性を有する表現行為の制約」に当たると述べる。これは次のように理解することができよう。通常の人格権侵害が問題となる表現行為は新聞・放送・雑誌等による報道であるが，そこには取材及び編集といった作業が内在しており，名誉毀損の場合には誤信相当性の法理において明示的に，プライバシーの場合には公共の利害等の判断において裏側から，そのような表現の自由の行使への顧慮がなされる。これに対して検索エンジンの場合には取材及び編集が介在しないが，その代わりにあるのが「検索事業者の方針」であり，それには検索エンジンの性格上「一貫性」が求められる。最高裁は，他ならぬ国家機関たる裁判所自身がその「一貫性」に干渉して削除を「余儀なく」することに，報道の場合とは異なる表現の自由の制約を見いだし，単純な比較衡量よりも削除に慎重な基準を示したものと理解できる。これは，検索エンジンがそれ自体として表現者としての責任を負うというよりも，リンク先での人格権侵害に接近する補助的な手助けをしているという限度で人格権侵害の責任を負うことがあるに過ぎないという筆者のこれまでの理解と，実質的には共通

点が多いように思われる[4]。

残された問題は，このような裁判所による「表現行為の制約」という認識が，北方ジャーナル事件判決と同じく仮処分手続の特性に基づくものかどうかである。この点は必ずしも明言されておらず，どちらと理解するかによって本決定の射程は変わりうることになる。即ち，仮処分手続で検索結果の削除を命ずることに「表現行為の制約」を見いだすのであれば，本決定は，名誉毀損に基づき検索結果の削除を求める仮処分手続においても先例として機能することになろう。これに対して訴訟非訟の別に拘らないのであれば――「石に泳ぐ魚」事件判決の参照はそのように解しうるが――，プライバシー侵害を理由とする検索結果の削除を求める訴訟においても，本決定の説くとおり明白性の要件が求められることになると思われる。

第5に，「当該URL等情報が提供されることによってその者のプライバシーに属する事実が伝達される範囲とその者が被る具体的被害の程度」という考慮要素をどのように運用するかは，今触れた検索エンジンの評価と関連して，新たな問題を提起するもののように思われる。長良川事件判決における「これらが公表されることによって被上告人のプライバシーに属する情報が伝達される範囲と被上告人が被る具体的被害の程度」が現実に意味していたのは，読者が仮名報道を読んで当該少年犯罪を犯した者だと知りうる範囲の問題であった。同事件の差戻控訴審である名古屋平成高判16・5・12判時1870号29頁は，「現に主に生育地における知人，友人，少年院等で知り合った者，暴力団関係者等と考えられ，その範囲は限定的である」ということから，プライバシー侵害を否定していたとおりである。

あるいは，本決定が長良川事件に着目したのは，検索エンジンが「ある者に関する条件による検索の求めに応じ」て提供されるものであるという特性との関係で，この「伝達される範囲」という要素がふさわしいと考えたからかもしれない。しかし検索結果の削除が争われている事例において，「その者のプライバシーに属する事実が伝達される範囲」とは何を意味するのであろうか。最高裁は本件の具体的判断において，「本件検索結果は抗告人の居住する県の名称及び抗告人の氏名を条件とした場合の検索結果の一部であることなどからすると，本件事実が伝達される範囲はある程度限られたものである」としている。そうすると，ただ属性情報なしに，ただ氏名を検索しただけでプライバシーに係る検索結果が表示された場合には，「伝達される範囲」は広いということになり，検索結果の削除に有利に働くように思われる。しかし，氏名だけの検索でも属性情報を入れた場合と同じ結果が表示されるのであり，ただ検索順位の違いが生じるに過ぎないという場合も多いのではなかろうか。これに対して，そもそも検索結果が，報道とは異なって「ある者に関する条件による検索の求めに応じ」て提供されるという点では，一般に「伝達される範囲」は限定的であるように思われるが，仮にそうだとすればこの要素は検索結果の削除が求められる裁判では，事実上削除を否定する方向で働くように思われる。

Ⅴ　今後の課題

1　実効的な自主規制の必要性

以上述べたとおり，プライバシーを理由とする仮処分手続による検索結果の削除については，最高裁決定によって削除に一定の条件を課する統一的な判断基準が示されたものの，なお運用に開かれた余地が残されており，今後の裁判の蓄積に俟つところも大きい。そもそも裁判所による仮処分手続による削除は，表現の自由・知る権利との関係で謙抑的であるべきことからしても，まずは事業者自身による自主的な削除の取り組みに期待されるところが大きい。そのためには，表現の自由の重要性と救済の必要性の間で裁判よりもきめ細やかな調整を行うことと同時に，その調整について利用者から見た透明性が確保されることも，インターネットにおける検索エンジンの役割からは当然に求められる。

4)　宍戸常寿「インターネット上の名誉毀損・プライバシー侵害」松井茂記＝鈴木秀美＝山口いつ子編『インターネット法』（有斐閣，2015年）84頁。

既にグーグルは検索結果の削除に関する世界的な考え方を公表し，透明性レポートを公表しているが，ヤフーも2015年3月には「検索結果とプライバシーに関する有識者会議」報告書を踏まえて，非表示措置の申告を受けた場合の対応方針を公表している[5)]。今後は最高裁決定を受けて，さらにこうした自主規制の取り組みが精緻化されることが期待されるが，その際の論点をいくつか挙げておきたい。

第1に，検索結果の表示においてスニペットに問題がある場合，ヤフーはスニペットだけを削除し，グーグルはリンクごと削除するという運用の違いがあるようである。このような違いは，当面は事業者間の違いがあることは当然として，そのこと自体が後述する情報共有の枠組みの中で広く認識されていくべきものと思われる。

次に，これまでも医師等の専門職による処分歴等に係る検索結果の削除の当否が争われてきたが，一般論として言えば，まさに専門的サービスについては消費者との情報の非対称性の観点から，一般私人の前科等とは異なり削除には慎重であるべきではないか。逆により弱い立場の者について，SNSを青少年の時点から利用した世代が今後成長するにしたがって，青少年の頃に自らネットに掲載した，いわゆる「黒歴史」に関する結果の削除についてどう考えるかは，今後のICT社会全体に課せられた大きな課題であるように思われる。

前科等については，従来公訴時効の期間ないし刑の言い渡しの効力を一つの目安として削除への対応が考えられてきたが，最高裁決定を参考にするならば，犯罪類型の反社会性というより実質的な考慮が必要となろう。また，氏名を入力した場合に関連キーワードが表示されるいわゆるサジェスト機能が，「事実が伝達される範囲」という考慮要素とどのような関係に立つかも，今後整理が必要になるように思われる。

2　ICT社会における各主体の役割と公益性

そもそも検索結果の削除の問題は，独り検索エンジンに限られた問題ではない。検索結果が非表示になったとしても，人格権を侵害するサイトそれ自体はネット上に残っており，URLを直接打ち込むことで利用者はアクセス可能であるし，とりわけ著名なまとめサイトは検索エンジンで表示されなくても，利用者が何らかの方法でたどり着けることが多いのではないか。逆に銀行での融資や就職活動において検索結果により不利益が生じるという問題についても，検索エンジンの利便性が低下したとしても，ネット上でそのような情報を収集し事業者に有料で提供するようなサービスが登場することもあり得よう。他方，いわゆる「忘れられる権利」でクローズアップされるような問題とは別に，たとえば社会の耳目を集めるような現在進行形の事件について，メディアが一定の理由により匿名報道を選んでいるにもかかわらず，利用者が情報収集により加害者・被害者の氏名等を特定してしまうことが予想される場合については，むしろ検索エンジンを含めた積極的な対応が必要であるようにも思われる。

いずれにしても，インターネット上のプライバシーと表現の自由を健全に調和させることは，検索エンジンだけではない，ICTに関わる全ての主体に課せられた課題である。この点，総務省の「ICTサービス安心・安全研究会」の報告書「インターネット上の個人情報・利用者情報等の流通への対応について」（2015年7月）は，プロバイダ責任法及び民間の自主的取り組みも踏まえつつ，「各関連事業者における削除等の判断基準，削除等の状況・実績等の公開等による透明性の向上，削除等の手続の明確化」に加えて，「広範な関係者の参加する自主的取組に係る情報共有の場の検討等」を今後の取組の方向性として掲げている。後者は，検索エンジンに加えて，ISP，SNS事業者等の事業者間の情報共有と連携のための枠組みを求めるものであり，利用者さらにはネットでの記事掲載による被害者側との意見交換を含めて，前者の実効的な取組への反映が期待されるところである。また，一般利用者が人格権を侵害するような不確かな情報を安易に拡散することのないよう，リテラシーやモラルの向上のための取組も必

5）https://publicpolicy.yahoo.co.jp/2015/03/3016.html

要とされている[6]。

他方，検索結果の削除が提起する問題は，インターネット政策として閉じた議論では済まない，より広範な領域につながるものである。たとえば前科の問題は，ICT社会における犯罪からの更正という刑事政策の問題としても，議論される必要があろう。また，匿名記事について，その後検索エンジンの利用により当該匿名の取材対象者が特定されたとしても，通常の報道における注意義務を果たしている限りで，メディアに不法行為責任は成立しないとされている[7]。しかし，そのようにメディアが法的責任を負う場面を超えて広く問題の所在を捉えれば，インターネット上で流通する情報の多くはメディアの報道を源とするものであり，とりわけ前科等については，事件報道・実名報道をめぐる従来からの課題と連続性を有するものであることを軽視することはできないであろう。このように，検索結果の削除は，ICT社会全体における適切な情報流通のあり方という全体的な視点から切り離して議論することはできないし，またしてはならないものと考えられる。

＊　本稿は2016年12月12日に総務省が主催した「インターネット上に掲載された過去のプライバシー関連情報等の取扱いに関するシンポジウム」での筆者の報告「『忘れられる権利』及び検索結果の削除に関する，国内外の近時の動向について――法制面から――」を基礎に，最高裁決定とそのコメントを加えて再構成したものである。

＊＊　脱稿後，木下昌彦「判批」『平成28年度重要判例解説』（有斐閣，2017年）14頁以下，曽我部真裕「『検索結果削除』で最高裁が判断」新聞研究789号（2017年）56頁以下，宮下紘「忘れられる権利」判時2318号3頁以下等に接した。

6）　http://www.soumu.go.jp/menu_news/s-news/01kiban08_02000184.html

7）　東京地判平成25・11・21判例集未登載。この判決を含めネット時代のジャーナリズムのあり方については，宍戸常寿「ジャーナリズム」佐々木弘通＝宍戸編『現代社会と憲法学』（弘文堂，2015年）1頁以下。

ネットワーク中立性とゼロレーティング

中央大学総合政策学部教授
実　積　寿　也
JITSUZUMI Toshiya

Ⅰ　はじめに

インターネットは単なる通信手段の域を超え，様々なサービスのプラットフォームとして機能している。電子商取引事業者は，通常，通信ネットワークを自ら保有することなく，電気通信事業者やケーブルテレビ事業者の施設を利用して，サービスを提供している。こうした形式のビジネスは，Over-the-Top（OTT）と形容され，それを行なう事業者は OTT 事業者と称される。OTT 事業には，参入障壁の低さゆえに多数のプレイヤーが存在し，クラウドサービスやビデオ配信サービス等の上位レイヤに属するものから，音声通信サービスのように下位レイヤに含まれるものまで，幅広いサービスが提供されている。これにより，サービスバリエーションの拡大，競争を通じた価格低下，イノベーションの加速などを通じた資源配分の効率化が期待できる。

さて，OTT 事業者にとってネットワークインフラの利用が十分に確保されなければ事業自体が成り立たない。利用面の制約は少なければ少ないほど，利用料金は低ければ低いほど望ましい。ただし，それらネットワークは民間投資によって構築されたものである。OTT 事業の発展を支えるに十分な投資を継続するためには，それに応じた投資収益率を確保することが必須であり，利用条件の緩和には自ら限界がある。投資収益率が低下し，ネットワーク利用量の急増に対応した投資拡大が困難になれば，ネットワーク品質が低下し，OTT 事業の基盤が損なわれる。

一方，ネットワーク事業者が大きな市場支配力を持つ場合[1)]，利潤最大化の目的でネットワーク利用条件が非効率に厳しい水準に設定される可能性がある。OTT 事業者の提供するサービスが市場において既存事業者と競合する場合，その動機は一層大きくなる。資源配分効率化の観点からは，ネットワーク利用条件が過度に厳しくないかを監視することも必須である。

これが，ネットワーク中立性が本来対象としていた事象である。本質は，OTT 事業の展開に伴って発生したネットワーク利用量の急増によって顕在化したネットワーク資源の配分問題に過ぎない。しかし，モバイル化の進展や新しいサービスであるゼロレーティングの市場投入により，これ以外のさまざまな論点が追加された結果，今日では複雑な政策課題を構成している。

本稿では，変質しつつあるネットワーク中立性に関する政策上の論点について分析する。第二節において，ネットワーク中立性の意味とその変容について議論し，わが国において新たなアプローチが要請されつつある背景を解説する。第三節では，ゼロレーティングという新しいサービスメニューについて紹介し，第四節でネットワーク中立性との関係を議論する。第五節は全体のまとめである。

1)　規模や範囲の経済性，あるいは周波数資源の希少性が市場支配力の源泉となりうる。

表1　2015年オープンインターネット命令の概要

ブロードバンドアクセスに関する規制権限の強化	・ブロードバンドアクセスを「電気通信サービス」として厳しく規制。ただし，適用条文は最小限に。 ・プロバイダ間の相互接続を規制対象に設定。
プロバイダの行動に関する三つのルールの設定	1. 合法的コンテンツや端末設備等への接続拒否の禁止 2. 利用者が求めるケースを除き，品質低下措置の禁止 3. 有償あるいは関連会社への優遇措置の禁止
将来の個別ケースがオープンインターネット原則に即しているか否かの判断基準の提示	7つの判断基準を設定 1. 利用者自身による管理の可否 2. 競争への影響 3. 消費者保護の有無 4. 技術開発や投資，ブロードバンド普及への影響 5. 表現の自由との関係 6. アプリケーション差別の有無 7. 業界標準との合致
より高度な情報開示基準の設定	・ネットワーク管理方法や実行品質，取引条件に係る詳細な情報開示義務（小規模事業者は一部免除）
苦情処理手続きの拡充	・オンブズマンを設置し対応強化

出典：筆者作成

Ⅱ　ネットワーク中立性「問題」とその変質

「ネットワーク中立性（network neutrality）」という用語は，コロンビア大学のTim Wu教授が2003年に発表した論文（Wu, 2003）が初出である。ただし，「ネットワーク上を流れる通信の公平な取扱い」という概念自体は，1860年制定のPacific Telegraph Act of 1860において既に存在し，通信事業においては当然の行動原理と考えられていた。この概念が，通信政策上の一大争点となったのは，米国連邦通信委員会（FCC）のPowell委員長が2004年2月8日に行った講演（Powell, 2004）が契機であり，2005年8月5日には「インターネット政策声明」（FCC, 2005）が正式に発出された。同声明は「ブロードバンド普及を促進し公共インターネットの開放性と相互接続性を維持・促進するため」の4原則（合法的コンテンツへのアクセス，アプリやサービスの自由な利用，合法的な端末の接続，競争成果の享受）を謳っている。以降，FCCのネットワーク中立性政策はこの4原則を具体化する形で進められ，2015年オープンインターネット命令（FCC, 2015）として結実した[2)]（表1）。

本規制が導入された最大の理由は，OTTサービスの増大によってネットワーク容量の希少性が顕在化した点にある。解決には道路混雑問題に関して培われた知見が応用できるが，①インターネットの構築・運営には複数の民間事業者が関与し，バックボーンの通信処理能力についてはコモンズとしての性質があること，②ベストエフォート品質により提供されているため，投資不足による品質低下が法的には許容されること，③OTTサービスの提供障害にユーザーからの原因究明が困難であるため市場圧力が機能しにくいこと，といった事情から，追加的な配慮が必要となる。例えば，ステークホルダーに対する情報開示や，投資インセンティブの確保が重要である。ネットワーク保

2)　本命令は2010年オープンインターネット命令（FCC, 2010）の主要部分の有効性が2014年1月14日に連邦控訴審において否定されたことに対応して発出されたものである（Verizon v. FCC, et al., No. 11-1355 (D.C. Cir. 2014)）。2010年命令の理念を踏襲しつつも，ブロードバンドを電気通信サービスとして位置づけるなど，種々の修正が施されている。2015年命令についても同様に法廷闘争が試みられたが，連邦控訴審において2016年6月14日にその有効性を認める判決が下された（United States Telecom Assoc. v. FCC, No. 15-1063 (D.C. Cir. 2016)）。2014年の連邦控訴審の決定についての評価は実積（2014）を参照されたい。

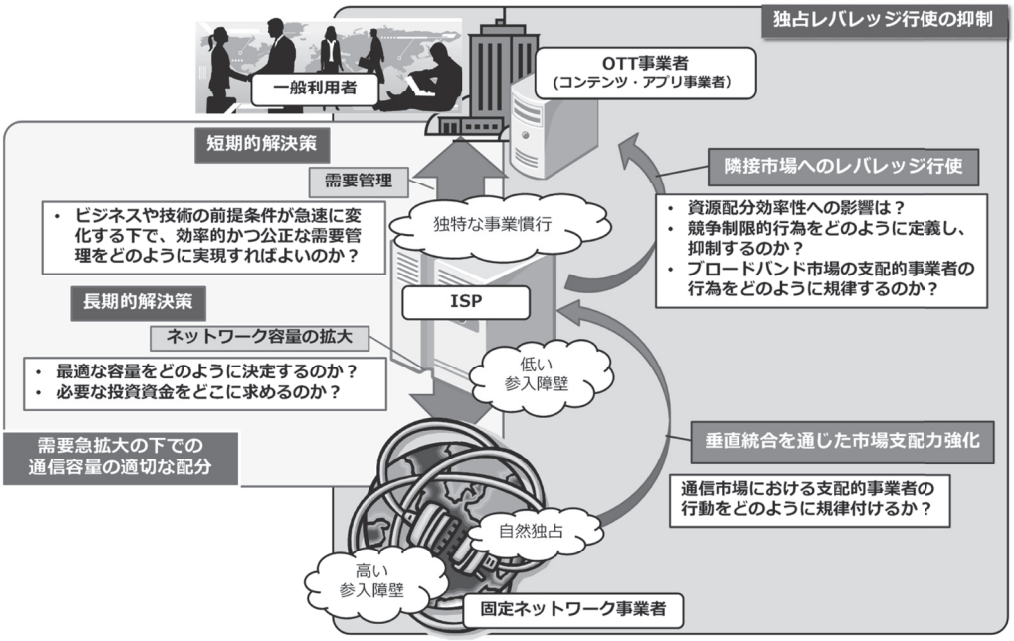


図１　ネットワーク中立性の論点

出典：筆者作成

有が独占力の源泉となる点にも注意が求められる。ネットワーク事業者が市場支配力を濫用すれば，利潤最大化の過程で OTT 分野の競争を阻害する可能性がある（Farrell and Weiser, 2003）。実際，米国では，1996 年通信法制定以来の規制緩和によってブロードバンド市場の複占化が進み，ネットワーク事業者によるエコシステム支配が懸念されていた。同様のインターネット先進国でありながら，日本では特別な規制を導入しなくて済んだ理由は，非対称規制等により競争的な固定 ISP 市場を維持し得たことで，市場メカニズムの活用が可能であった点にある。結果，ネットワーク中立性の論点は図１のようにまとめることができる。

さて，モバイルブロードバンド化が進展したわが国では[3]，固定事業者とモバイル事業者の事業統合が実質的に進んでいる。2015 年２月より NTT 東西が FTTH の卸売りである「光コラボレーションモデル」を開始したことにより，携帯各社は固定・モバイルの両サービスの統合を進め，その市場支配をさらに強化しつつある[4]。この傾向が続けば，消費者のインターネットポータルを握る垂直統合型モバイル事業者による寡占体制が成立し，ブロードバンド産業構造は図２のように変化する。モバイル事業者に対して電気通信事業法が緩やかな規制権限しか設定していないこと，NTT ドコモに NTT 法による業務範囲の制約が及ばないことも構造変化にとっては追い風である。そのため，ISP 市場の競争性を前提にした日本のアプローチは変更を余儀なくされている。

市場支配力に対するアプローチには，当該市場への新規参入を促進したり市場支配的事業者を分割したりすることで市場の競争性自体の回復を目指す「参入・構造規制」と，市場支配的事業者の存在を前提にしたうえでその行為に一定の制約をかける「行為規制」に分けることができる。わが国の場合，周波数割り当ての局面での新規事業者

3）　総務省（2014）によれば，インターネットの平均利用時間・行為者率ともに携帯電話（スマートフォンを含む）がパソコンを上回っている。

4）　榊原（2016）は，「光コラボの契約数がここまで順調に伸びているのは，NTT ドコモとソフトバンクの携帯電話大手２社によるところが大きい」（p.13）と分析している。

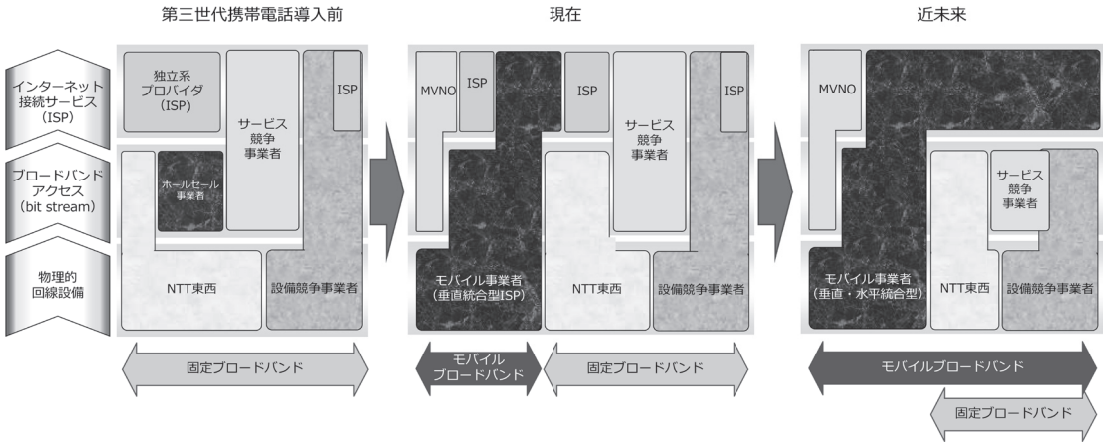


図２　ブロードバンド産業構造の変化

出典：筆者作成

優遇やMVNO育成などは前者の例であるが，これまでのところ目覚しい成果をあげていない[5)]。モバイル事業者を直接規律する「行為規制」としては，ネットワーク運営や，利用者の合理的・効率的な意思決定を保証するための情報開示についての基準設定が想定できる。具体的には，FCCのオープンインターネット命令や，2016年8月に欧州電子通信規制機関（Body of European Regulators for Electronic Communications［BEREC］）のガイドライン（BEREC, 2016）が参考になる。いずれの措置をとるにせよ，急速な技術進歩の下では，将来生じうるあらゆる事態に対応したルール作りは期待できず，最終的には政策担当者の個別判断が重要になる。

Ⅲ　ゼロレーティング

近年，ゼロレーティングと総称される新しいサービスがモバイルブロードバンドの分野に登場した。これは，事前に指定した特定コンテンツに関する通信量は課金対象とは看做さないというもので，2014年11月の時点で92種類のサービスが提供されている[6)]。

このサービスは，ブロードバンドの普及が進んでいない途上国で提供されるタイプと，ブロードバンド普及が一巡した先進国で提供されるタイプの二種類に大別できる。前者は，さまざまな理由でデータサービスの利用を行っていない携帯電話利用者に対し，追加料金なしで限定されたネットコンテンツの提供を行うタイプである。対象外コンテンツの利用には有料プランを別途購入する必要がある。限定的とはいえブロードバンドサービスを無償で（正確には音声通話サービス料金以外の追加料金なしで）提供することで，デジタルデバイドを縮小する効果が期待される。Facebook社が53カ国で提供中のFree Basicsの場合，利用可能コンテンツはネットワーク負荷が少ないテキスト主体のものに限定され，必要なデータ通信コストはモバイル事業者が負担している[7)]。本サービスを通じてアップセルの可能性が生まれることがモバイル事業者にとっての提供理由となる[8)]。

先進国での主な提供理由はデジタルデバイド縮

5）例えばMVNO育成に関しては，2015年12月末時点の独立系MVNOの契約数は1,155万，モバイル契約全体に占めるシェアは7.2％に止まり（2016年3月16日付け総務省プレスリリース（http://www.soumu.go.jp/menu_news/s-news/01kiban04_02000104.html）），有効な競争圧力を生み出しているとは言い難い。

6）ITMedia Consulting社の調査による。(http://www.dimt.it/wp-content/uploads/2015/10/Zero-rating_vienna_review.pdf)

7）Facebook社の報道資料による。

8）トルコの携帯電話事業者であるTurkcell社は，顧客1人当たりの平均売上高を9％改善することに成功している（Openet Telecom, 2013）。

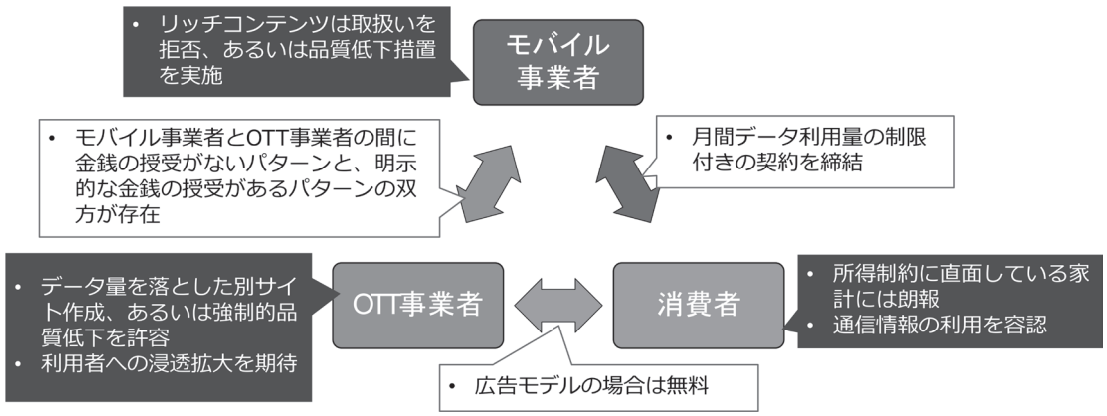


図３　ゼロレーティングにおける利害関係

出典：筆者作成

小ではない。モバイル市場では，「データ使い放題」というかつてのサービスに代わって，月間データ容量に上限（データキャップ）を設けたサービスが主流になっている。利用量がデータキャップを超過した場合は，通信速度が著しく低速となりブロードバンドコンテンツの利用が困難となるため[9]，利用者はリッチコンテンツの利用を諦めるか，有料でデータ利用量を追加するのかの選択を迫られる。これはOTT事業者にとって利潤機会の喪失に他ならない。先進国型ゼロレーティングはこれに対応するもので，モバイル事業者が指定した特定コンテンツに係るトラヒックを利用量カウントから除外する。これにより，利用者はデータキャップを気にすることなく対象コンテンツを利用でき，それを提供するOTT事業者は非対象コンテンツ提供者に対し大きなアドバンテージを得る。加えて，当該OTT事業者による高品質（従ってデータ量が多い）コンテンツの開発・提供が促進される。モバイル事業者にとっては，人気コンテンツをデータキャップとは無関係に提供できることが利用者獲得の大きな武器となる。途上国型と同様にデータ通信コストをモバイル事業者のみが負担しているパターンに加え，AT&T社のsponsored data[10]のようにOTT事業者が負担するパターンも存在する。T-Mobile社のBinge-On[11]では，金銭のやり取りはない代わりに，ネットワークへの負荷を軽減するため一定の品質低下措置の受け入れを求めている[12]。現在，わが国で導入されているゼロレーティングはいずれもMVNOが提供しており，①「自社あるいは関係会社が提供するコンテンツへのアクセスを対象とするもの」，②「利用者獲得目的でMVNO自身とは無関係のコンテンツを対象とするもの」，および③「①と②の組合せ」の３つの類型が存在するほか，一定の品質低下措置を伴うものもある。類型②の場合，データ通信コストはMVNO側が負担している。主要プレイヤーの関係は図３のようにまとめられる。

Ⅳ　ゼロレーティングとネットワーク中立性

ゼロレーティングとは，モバイル事業者のOTT事業者に対するインターフェイスを特定コンテンツ提供者に対してのみ緩和することであるため，ネットワーク中立性との不整合が指摘される。ただし，この文脈での「ネットワーク中立

9）NTTドコモの場合，「ご利用データ量を超過した場合，当月の通信速度が送受信時最大128kbps通信に変更となります」と記載されている。（https://www.nttdocomo.co.jp/charge/bill_plan/xi/128kbps_cancellation/）

10）https://developer.att.com/sponsored-data

11）https://www.t-mobile.com/offer/binge-on-streaming-video.html

12）T-Mobile社は品質低下措置を全般的に及ぼすことで，データキャップの設定自体を不要にするサービスを「T-mobile ONE」（https://newsroom.t-mobile.com/news-and-blogs/t-mobile-links/t-mobile-fact-sheet.htm）という名称で2016年8月より提供している。

性」は，ネットワーク容量の希少性をベースとしたこれまでの議論とは本質的に異なり，「ネットワーク上を流れる通信の公平な取扱い」という伝統的な行動原理に直接基礎を置くものである点に注意が必要である。この段階において，輻輳回避のためのトラヒック制御措置の透明性や投資インセンティブの確保といった論点は議論の一要素に過ぎない[13]。

まず，対象となるコンテンツが市場メカニズムを介してではなく，一定の市場支配力をもったモバイル事業者によって恣意的に選択されるため，効率的な産業構造の発達が阻害されるという議論が Malcolm et al.（2016）などでなされている。例えばわが国では，上述の類型①ではモバイル事業者の市場支配力が隣接市場に及ぶため，OTT 市場の競争性が損なわれうる。ただし，Farrell and Weiser（2003）が言及しているとおり，モバイル事業者が合理的であれば，そういった行動の社会的な効率性への影響は必ずしもマイナスとは限らない。

類型②（および類型③）に関しては，対象コンテンツは自社のモバイルブロードバンドサービスの魅力を高めるという観点から選択されるため，その時点での人気コンテンツに偏りがちである[14]。ゼロレーティング対象のコンテンツはそれ以外のコンテンツに対して競争上有利となるため，当該コンテンツの人気・市場シェアはますます高まる。対象外のサービスにとっては先行サービスの牙城を崩すことが困難となり，市場の競争性が削がれ，長期的にはイノベーションが阻害される可能性が指摘される。対象外となったコンテンツ事業者を中心とした反発も生まれている。地元のコンテンツ事業者を中心に反発が広がったインドでは，電気通信規制庁（TRAI）が 2016 年 2 月 8 日にゼロレーティングを禁じるルールを定めた[15]。

ゼロレーティングはデータキャップの存在を前提として導入される。データキャップが低いほど，利用者のゼロレーティングへの需要は高まる。ゼロレーティング対象のコンテンツの市場競争力も強化されるため，有償のゼロレーティングに対する OTT 事業者の需要も大きくなる。そのため，モバイル事業者が，利潤最大化のためにデータキャップを非効率な低水準に設定する可能性があり，それに伴いネットワーク投資の水準を減少するため，情報通信社会のインフラ整備が遅れる懸念も指摘される。

こういった指摘に対し，FCC はゼロレーティングに関する情報収集を，2015 年 12 月以来，慎重に進めていたが[16]，2017 年 1 月 11 日に AT&T と Verizon が提供しているゼロレーティングについては 2015 年命令に違反し，ネットワーク中立性（FCC の言い方ではオープンインターネット）の観点から懸念ありとする報告書（FCC, 2017）を公表した。AT&T は 2015 年に完全子会社化した DIRECTV が提供するビデオプログラムについて自社のモバイルブロードバンド利用者に対してゼロレーティングの対象として提供する一方で[17]，独立系 OTT ビデオ事業者に対し sponsored data の提供を行っている。これは前節に提示した類型③に該当するが，FCC は類型①と類型②の対象コンテンツに対する取り扱い格差が OTT 市場における競争に歪みをもたらす可能性があると認定している。Verizon が提供する有料ゼロレーティングサービスである FreeBee Data

13）もちろん，ゼロレーティングがトラヒック混雑を悪化させる場合はコスト負担の公平性等の議論の対象となりうる。しかしながら，個別サービスのコスト情報が開示されない限り，ゼロレーティングを利用しているユーザーとそれ以外のユーザーの間の内部相互補助の有無は明かではない。そのため，ゼロレーティングでコスト負担の不公平性が問題となるのは一部ケースにとどまる。

14）LINE モバイルの「コミュニケーションフリープラン」では LINE のほかに，Twitter，Facebook，Instagram がゼロレーティング対象となっている。筆者のヒアリング調査によれば，コンテンツ選択は利用者の多寡が基準である。

15）http://itpro.nikkeibp.co.jp/atcl/news/16/020900401/, http://itpro.nikkeibp.co.jp/atcl/news/16/021200433/?rt=nocnt

16）http://arstechnica.com/business/2015/12/comcast-att-and-t-mobile-must-explain-data-cap-exemptions-to-fcc/, http://bits.blogs.nytimes.com/2015/12/17/f-c-c-asks-comcast-att-and-t-mobile-about-zero-rating-services/

17）AT&T, Watch It Anywhere with AT&T DIRECTV (Sept. 7, 2016), http://about.att.com/story/watch_it_anywhere_with_att_directv.html; AT&T, The Revolution is Here: AT&T Offers 3 Ways to Stream Premium Video Content (Nov. 29, 2016), http://about.att.com/story/att_offers_three_ways_to_stream_premium_video_content.html.

360についても，自社コンテンツを提供するgo90との間の取り扱いの差をベースに同様の判断が下された。その他，先述のインドに加え，チリ，スロベニア，イスラエル，ブラジルなどでゼロレーティングはネットワーク中立性に違反するものと規定されている[18]。

さて，モバイル事業者が導入するゼロレーティングはネットワーク投資の収益率を改善することが期待される（そうでなければそもそも導入されない）。期待収益率が高くなれば投資量は増加するので，ネットワークインフラの整備は加速し，より高水準の情報化社会の実現が期待できる。先の懸念にあるように，ゼロレーティングがネットワーク資源の希少性を強化する方向に機能するのは，モバイル事業者が市場支配力を駆使できるケースである。すなわち，ネットワーク中立性論が問題にすべき対象は，ゼロレーティングというサービス形態ではなく，その背後にある寡占市場の存在に他ならない。

競争圧力が十分であれば，ネットワーク投資やデータキャップの水準，利用料金，さらにはOTT事業者に対する課金水準が非効率な水準に定まる傾向は存在しない。対象コンテンツの利用者にとっては，ゼロレーティングによってブロードバンド利用のコストが下がるため，より大きな消費者余剰が実現される。とりわけ，厳しい所得制約に直面している消費者にとっては生活インフラの整備がもたらされる。対象コンテンツ以外を提供するOTT事業者にとっても，可処分所得の増加を通じて，需要増が期待できる。こういった便益を最大限に享受するためにもモバイル事業者に十分な競争圧力がかかっていることが必要である。その意味で，わが国のMVNOのように自然独占力の源となるネットワーク設備をもたず，かつ現状では市場シェアが小さいモバイル事業者が行うゼロレーティングについてはネットワーク中立性に対する侵害は心配する必要がない[19]。

また，zero-price ruleと呼ばれるインターネット草創期からのビジネス慣行により，モバイル事業者と直接の契約関係にないOTT事業者は課金されない。OTT事業者が得る便益が競争を通じてモバイル事業者に還元されなければ，ネットワーク建設・維持に投入される資源は最適水準を下回る。こういった場合は，sponsored dataによるOTT事業者への課金は静学的な意味での資源配分効率性を改善する[20]。

OTT市場そのものへの影響についてもマイナス要素ばかりとは限らない。対象コンテンツを提供するOTT事業者の収支が改善すれば，多様かつ高品質なコンテンツの投入も可能になる。これによる厚生改善効果が，競争面での悪影響を上回るか否かは実証的な問題であり，アプリオリに決定することは困難である。さらに，FCC（2017）でも焦点となったOTT事業者間の不公平という分配問題の解決に行為規制を用いることは効率面で課題が多い。

そもそも，ゼロレーティングの導入は，モバイルブロードバンドエコシステムにおける競争要素を追加することを意味する。これにより，とりうる戦略の数が増えるので，競争圧力の強化を通じて経済厚生にはプラスとなる。逆に，ゼロレーティングへの制約が新しいOTTサービスの導入を阻害する可能性がある。例えば，高精細画像の伝送のように大量のデータ伝送を前提とするサービスにとっては，ゼロレーティングの提供が，たとえ有償であっても，必須となる。もちろん，有償の場合は資金力に乏しい新規参入者が一方的に不利益を被る余地もあるが，この点はゼロレーティングというよりも新規事業者のプロジェクトへの資金供与が十分にできない資本市場の問題，ある

18） 逆に，EUでは，2016年4月末から施行された新規則（REGULATION (EU) 2015/2120 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015 (Official Journal of the European Union, 26.11.2015, L 310/1; http://eur-lex.europa.eu/eli/reg/2015/2120/oj)）において，ネットワーク容量に余裕がある場合に限り，ゼロレーティング等の特別サービスの提供を一定の範囲内で容認する方針を示しており，ゼロレーティングへの対処は国際的に一様ではない。

19） この点は電気通信事業に対する独占禁止法の運用（公正取引員会・総務省，2016）とも整合的である。

20） Lee and Wu (2009)では，zero-price ruleをネットワーク事業者（あるいはその顧客）からOTT事業者への所得再分配（事実上の補助金）と解釈できると指摘している。OTT分野のイノベーションの効果が期待できるのであれば，現行システムは長期的な資源配分効率性を改善する。

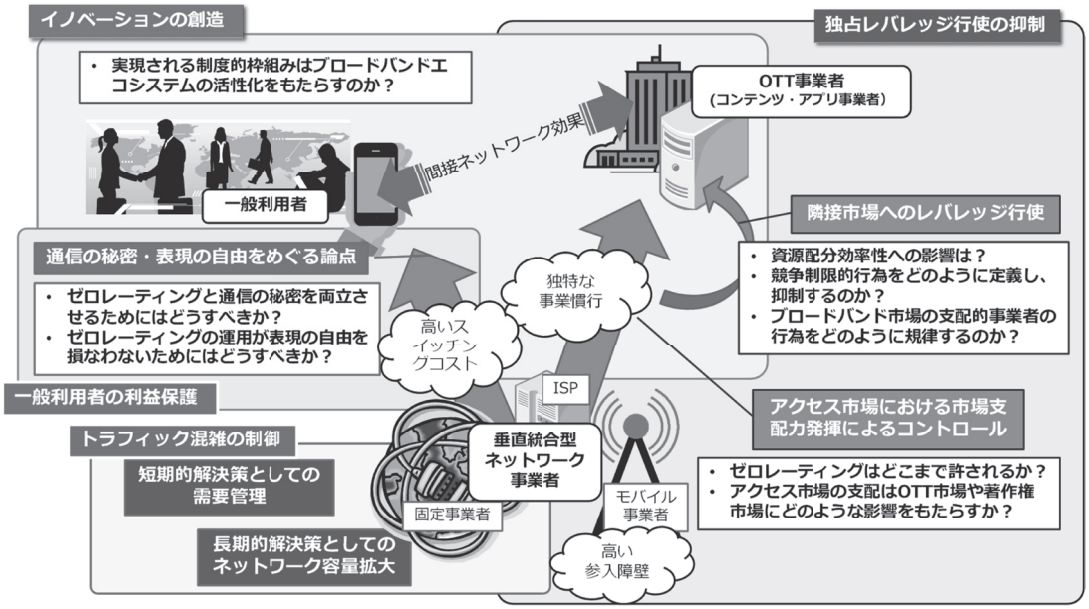


図4　ネットワーク中立性をめぐる最近の論点

出典：筆者作成

いは情報の非対称性の問題に帰着する[21]。

ネットワーク中立性以外からの懸念も存在する。本サービスを実現するためには，利用者のコンテンツ利用状況をリアルタイムで監視する必要があり，「利用者の同意」が十分でない場合，通信の秘密の侵害が発生する。ネットコンテンツの多様性を重視する論者は，本サービスにより低所得者層は「通常の」インターネットを利用しなくなるため，結果的に，持つものと持たざるものの間のデジタルデバイドを拡大する可能性を指摘する[22]。

結果として，今日のネットワーク中立性問題は，関連する論点を大きく増やしつつある（図4）。

V　まとめ：ネットワーク中立性2.0

モバイルブロードバンドの普及とゼロレーティングの導入によりネットワーク中立性論議が対象とすべき論点は変質しつつあり，わが国の政策担当者には新たな課題となっている。ただし，将来生じうるあらゆる事態に対応した政策形成を求めることは，特にインターネットの分野では期待できないため，政策担当者の個別判断が重要になる。最先端の技術知識やマーケティング戦略の知見が政策担当者に集積していることは想定できないため，ステークホルダーの衆知を広く集めた上でルール作りを行なう「共同規制」のアプローチが，この新しいネットワーク中立性，いわば「ネットワーク中立性2.0」にとっては必須である。また，インターネットは国境を超えるものであるため，ネットワーク中立性を巡るルール作りにあたっては国際的な協調は必須である。特に，インターネット資源の多くを握る米国においては政権移行に伴い，これまでのネットワーク中立性政策の大転換が予想されており，その動向に特段の注意を払う必要がある。その意味で，意見を聴取すべきス

21）本ロジックについては，伊藤ほか（1988，第4章）を参照のこと。

22）Open Letter to Mark Zuckerberg Regarding Internet.org, Net Neutrality, Privacy, and Security (May 18, 2015), https://www.facebook.com/notes/accessnoworg/open-letter-to-mark-zuckerberg-regarding-internetorg-net-neutrality-privacy-and-/935857379791271

テークホルダーの範囲は極めて広範であることを我々は覚悟すべきである。

参考文献

BEREC. (2016) “BEREC guidelines on the implementation by national regulators of European net neutrality Rules,” http://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/6160-berec-guidelines-on-the-implementation-b_0.pdf

Farrell, J. and Weiser, P.J. (2003) “Modularity, vertical integration, and open access policies: Towards a convergence of antitrust and regulation in the Internet age,” *Harvard Journal of Law and Technology*, 17(1), 85–134.

FCC. (2005) “Appropriate framework for broadband access to the Internet over wireline facilities,” 20 FCC Rcd 14986.

FCC. (2010) “Framework for broadband Internet access,” 25 FCC Rcd 7866, 75 FR 36071.

FCC. (2015) “FCC releases Open Internet report and order on remand, declaratory ruling, and order,” 80 FR 19737.

FCC. (2017) “Wireless Telecommunications Bureau Report: Policy review of mobile broadband operators’ sponsored data offerings for zero-rated content and services,” http://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0111/DOC-342987A1.pdf

伊藤元重・清野一治・奥野正寛・鈴村興太郎（1988）『産業政策の経済分析』東京大学出版会.

実積寿也（2014）「オープンインターネット命令にかかる控訴審判決の影響」『情報通信学会誌』, 32(1), 1–12.

公正取引委員会・総務省（2016）「電気通信事業分野における競争の促進に関する指針」http://www.jftc.go.jp/houdou/pressrelease/h28/may/20160520_2.files/02.pdf

Lee, R.S. and Wu, T. (2009) “Subsidizing creativity through network design: Zero-pricing and net neutrality,” *Journal of Economic Perspectives*, 23(3), 61–76.

Malcolm, J., McSherry, C., and Walsh, K. (2016) “Zero rating: What it is and why you should care,” Electronic Frontier Foundation, https://www.eff.org/ja/node/90420

Openet Telecom. (2013) “White paper, real world examples of innovative data centric offers: 10 ways operators are using smart data plans to drive up usage and revenues,” http://www.openet.com/10-Ways-Operators-are-Getting-Innovative-with-Plans

Powell, M.K. (2004) “Preserving Internet freedom: Guiding principles for the industry,” FCC, https://apps.fcc.gov/edocs_public/ attachmatch/DOC-243556A1.pdf

榊原康（2016）「光コラボの通信簿：異業種の参入は進んだか」『日経コミュニケーション』, 7月号, 12–25.

総務省（2014）『平成26年版 情報通信白書』http://www.soumu.go.jp/johotsusintokei/whitepaper/h26.html

Wu, T. (2003) “Network neutrality, broadband discrimination,” *Journal on Telecommunications and High Technology Law*, 2, 141–175.

（投稿日：2017年1月29日）

ロボット法をめぐる法領域別課題の鳥瞰

慶應義塾大学総合政策学部教授
新　保　史　生
SHIMPO Fumio

Ⅰ　はじめに

AI（人工知能）の進化は急激に進みつつある。AIが搭載された家電製品やロボット，自動走行システムによる自動運転車[1]の普及に伴う法的課題の検討とともに，ロボットやAIの利用に伴う新たな情報セキュリティ対策を検討しなければ，インターネットの発展過程において生じた問題と同様の問題が生ずる可能性はないか。その脅威は，インターネットのようにバーチャルな空間における問題にとどまらず，現実の脅威として飛躍的に脅威の度合いが高まるおそれはないか。

AIや自律型ロボットの脅威として，AIが暴走して人間に脅威を与えることが指摘されることが多い。映画で描かれる脅威はまさにそれである。AIが自己を認識し自発的に防御行動をとるまで進化するまでには，まだ相当な時間を要すると考えられることからも，そのような脅威が直ちに現実となる可能性は低いと考えられる。

一方，今そこにある危機は，人間に脅威を与えるように人間がAIを用いることにある。敵と味方を自律的に認識して対象を攻撃をするようなAIを搭載した兵器の開発などは着々と進んでいる。

「ロボット法」として，まず考えなければならないのは，新たに人間の脅威となるおそれがある技術について，人間の脅威とならないように研究開発を制限するためのルールを考えるのではなく，新たな技術が人間に脅威を及ぼすことがないように，それを利用する人間をどのように規律すべきかを考えることにある。

Ⅱ　ロボット法研究の背景

1　ロボット法の現状

ロボット法については，日本国内では文献データベースで先行研究を調査しても，「ロボット法」という用語を冠して論じられている論文は，本稿執筆時点で10本に満たない。「ロボロー（Robo-

1）　ロボット法分野における論文として最も多いトピックは自動運転をめぐる問題に関するものである。多くの論考によって法的課題の抽出が行われ検討事項の整理がなされつつある。法的課題の整理を試みる論考として，佐藤智晶「人工知能と法：自動運転技術の利用と法的課題，特に製造物責任に着目して」青山法学論集57（2015-12）PP.27-42，中山幸二「自動運転をめぐる法的課題（特集 自動運転）」自動車技術69（2015-12）PP.39-45，中山幸二「自動運転の進展と交通事故の賠償責任」共済と保険58（2016）PP.4-11，新保史生「自動走行システムによる自動運転に係る制度的課題をめぐる検討状況」高速道路と自動車59(6)（2016）PP.5-8，戸嶋浩二，佐藤典仁「NBL SQUARE 米国における自動運転車に関する新たな指針」NBL（2016）PP.44-50，戸嶋浩二「自動走行車（自動運転）の実現に向けた法制度の現状と課題」NBL1073（2016）PP.28-35，高橋郁夫「自動運転の法的課題と今後の方向性（車載テクノロジー最前線）」車載テクノロジー4（2016）PP.75-79，「特集 自動運転と民事責任」ジュリスト1501（2017）PP.23-55，岡部雅人「自動運転車による事故と刑事責任：日本の刑法学の視点から」愛媛法学会雑誌43（2017）PP.1-20。

Law）」関連の多くの書籍や論文が公刊されている米国やEUの研究動向からするとかなり後塵を拝している。

2015年10月11日に，「ロボット法学会設立準備研究会」を科学未来館において開催した際には，「ロボット法」という新法を制定してロボット関連技術の規制を行うことが目的なのか，ロボット工学をはじめとする従来からの研究技術開発に係る長年の研究の蓄積や安全基準などの技術標準で様々な問題に対応できるにもかかわらず，ロボットに関する技術的知見に乏しい法学研究者が検討などできるのかといった多くの批判が寄せられた。その後も，「ロボット法」という法整備を行うことがロボット法の目的であるという短絡的な論調を改善することができないまま現在に至っていることは残念でならない。

2　ロボット法と産業政策

ロボット法の必要性は産業政策とも密接に関わっており，「第4次産業革命」は，社会や法制度の大きな変革を伴うものであることを認識する必要がある。

我が国は，産業用ロボットの市場占有率が高いが，「ロボット産業市場動向調査結果[2)]」によると，産業用ロボットの世界市場は，金額ベースで直近5年間に約60％成長。2011年の市場規模は約6628億円[3)]であり，うち日本企業のシェアは50.2％。なお，電子部品実装機を含む広義の世界市場は約10428億円で，日本企業のシェアは57.3％。日本市場は直近5年間に台数ベースで約25％縮小したものの世界最大市場の地位を維持。ただし，中国市場は5年間で約4倍に拡大し，台数ベースで日本市場に迫る規模に成長となっている。

日本は今後もロボット大国の地位を維持できるのであろうか。例えば，生活支援型ロボットや身の回りに普及しつつあるロボットについて，累計1000万台を超えるヒット商品になった掃除ロボットは，米iRobot社が開発。ソフトバンクのパーソナルロボット「Pepper（ペッパー）」も，ソフトバンク傘下であるフランスのAldebaran Robotics社が開発し，製造は鴻海精密工業。首相官邸に落下したり，姫路城に衝突したりしたドローンは，DJI（中国広東省深セン市のメーカー）の「ファントム」。原発事故で投入されたのは，米国アイロボット社が無償提供した，爆発物処理やSWATで使用されている2台の軍事用ロボット「パックボット」など，いずれも国産ロボットではない。

グーグルが自動走行システムの開発を進めている理由は，自動走行に係るOS（オペレーティング・システム）とプラットフォームの獲得を目指しているからにほかならない。スマートフォン同様に，自動車を構成する部品は日本製であっても，その設計や車両を制御するシステムは，国外かつ自動車産業とは無関係の事業者が将来的に覇権を握る可能性がないとは言い切れない[4)]。

技術的課題を克服して技術開発が市販レベルまで到達したとき，社会制度や法基盤，法的責任やリスク，社会的な受容性などを総合的に検討しなければ，新たな技術の普及を阻害するおそれもある。

Ⅲ　法領域別の課題概観

AIや自律型ロボットをめぐる法的課題は，個別の問題が散在的に検討されつつある。しかし，ロボット法が体系的な学問領域として認知されるには至っていないため，まずは，どのような課題を検討すべきか全体像を把握する必要がある。そこで，法領域別の法的課題について，現時点における国内外の先行研究を調査し具体的に議論され

2）経済産業省「ロボット産業市場動向調査結果：2012年ロボット産業の市場動向」（平成25年7月18日）。

3）直近の調査結果，日本ロボット工業会調査・統計部会「ロボット統計受注・生産・出荷実績2016（平成28）年10～12月期及び年間【会員ベース】について」によると，同会の正会員及び賛助会員対象企業の33社のうち，回答企業33社による実績によれば，受注・生産の台数及びその額はいずれも過去最高値を記録し7000億円を超える見込みとなっている。

4）IoTの普及をめぐる問題と今後のビジネスモデルの変化については，桑津浩太郎「IoTの普及にともなう新たなビジネスモデル，社会への影響（特集　暗号通貨の諸問題／IoTの法的課題・個人情報保護：第40回法とコンピュータ学会研究会報告）」法とコンピュータ34（2016）PP.9-15に詳しい。

ている課題の整理を試みてきたが，以下のような問題が現時点で議論が必要であることを確認するに至っている[5)]。

憲法の領域では，①安全保障（軍事利用やテロ対策，自律型兵器，ドローン），②プライバシー，肖像，個人情報保護（ビッグデータ解析），③法の下の平等，④表現の自由，⑤適正手続，⑥勤労（雇用環境の変化，雇用管理と差別）。

行政法の領域では，①ロボット行政（ロボット管理政策），②自動走行車の公道走行，無人航空機（ドローン）規制，ロボットの制御と電波監理，③その他の行政の規制個別領域における利用と管理。

民事法の領域では，①不法行為（製造物責任，自動走行車の事故と責任，人工知能の悪用や暴走），②消費者保護，③契約，④知的財産（AIが作成した著作物の著作権，特許），⑤医療・介護（手術，医療分野における利用，ヘルスケア，医療過誤）。

刑事法の領域では，①犯罪（AIやロボットを利用した犯罪），②法執行（犯罪捜査におけるAIプロファイリングの活用，犯罪予知AIを用いた犯罪予防など）。

国際法の領域では，①ドローンの利用をめぐるルール，②国際人道法とロボットなどがある。

法領域毎の課題については，2016年4月から2017年3月まで「時の法令」に掲載した拙稿を加除修正し考察する。

Ⅳ　憲　法

憲法問題としては，①軍事利用やテロ対策との関係における議論が国外では盛んである。米国の軍用ドローン（プレデターなど）はアフガニスタンやイラクで既に実戦投入されている。米国内から遠隔操縦で展開できるため攻撃側の人的被害なく戦闘が可能というメリットゆえに積極的に活用されている。しかし，戦争とテロ対策の境界，軍事目標と非戦闘員の区別，戦闘地域外から遠隔で攻撃することの法的妥当性などの観点から問題が指摘されている。将来的には，顔識別機能により攻撃対象者を識別し自動的に攻撃をする兵器の実戦配備も検討されており，自律型兵器は可及的速やかに国際的に確固たる規制が必要であるとの意見も示されるなど，致死性自律型ロボット（Lethal Autonomous Robotics:LARs）又は致死性武器体系（Lethal Autonomous Weapons System: LAWS）について，特定通常兵器使用禁止制限条約（CCW）の検討の場で議論がなされている。

②プライバシー関係の問題としては，ロボットに搭載されたカメラやマイクは周囲の状況を記録し，AIのディープラーニングは学習対象となる大量のデータを取得している。撮影された画像は個人情報であるとともに，肖像権をはじめとする個人の人格的利益保護の対象となる情報である。大量に取得されたデータはビッグデータとして解析され，個人のプライバシーが明らかになるおそれもある。

③法の下の平等をめぐる問題として，例えば，ロボコップは人種差別をしないのかという議論がある。デジタル技術は技術的に中立性が保たれているため，警察官による差別的な対応とは無縁のように思える。しかし，プログラムが政策的意図に左右されるおそれや，肌の色によってエラーが生じるなど機械的なエラーにより意図しない差別的利用が生ずることへの危険性がある。

④表現の自由については，AIが話した差別的発言についても表現の自由の保障が及ぶのか。

⑤適正手続としては，2016年7月9日に，米テキサス州ダラスで警官による射殺事件への抗議デモ中に発生した警官に対する銃撃事件の被疑者が，爆弾を搭載したロボットにより爆殺された事件が今後のロボットを用いた法執行の課題を浮き彫りにしている。超小型ロボットを用いた捜査やロボットを用いた法執行と適正手続の問題，犯罪捜査・予防でAIを利用した予測の妥当性を誰が評価するのかという問題などがある。詳細は刑事法分野における問題として後述する。

⑥勤労については，将来的にAIの進化によって雇用環境の劇的な変化が見込まれている。AIが奪う職業のリストなども議論され，雇用管理と差別の問題が生ずることも予想される。産業革命期に発生したラッダイト運動（機械破壊運動）が，

5)　新保史生「ロボット法学の幕開け（特集 IoTとイノベーション）」Nextcom 27（2016）P.29。

ロボット革命時代の到来によって再び起きることも空想とは言えないかもしれない。

Ⅴ 行政法

ロボットと行政の関わりは，無人航空機（ドローン）規制などのロボット管理のための施策，自動運転車の公道走行のための環境整備，ロボット制御や標準化，遠隔操作のための電波監理，情報通信やコミュニケーション，医療・介護，食品加工，農業，金融（フィンテック[6]），労働・労務管理，物流，エネルギー，災害対応，建設・インフラ管理など実に多岐に亘る。そこで，①ロボット共生社会に向けた制度や施策検討の在り方，②行政の効率化や法執行におけるAIやロボットの利用の二つに分けて考えてみたい。

1 ロボット共生社会に向けた制度や施策検討の在り方

既に講じられている具体的な施策としては，2015年にドローンに代表される無人航空機規制を目的に航空法が改正され同年12月10日に施行されている。さらに，国会議事堂，官邸や原発など国の重要な施設周辺での小型無人機等の飛行禁止地域を定める「小型無人機等飛行禁止法」が2016年3月18日に公布されている。

また，2020年の東京オリンピック開催に向けて，自動運転車の公道走行の実現を目指し，国土交通省・経済産業省が「自動走行ビジネス検討会報告書」を2016年3月23日に公表している。警察庁の「自動走行の制度的課題等に関する調査検討委員会」も2016年5月に「自動走行システムに関する公道実証実験のためのガイドライン」を公表している[7]。

2015年2月に日本経済再生本部決定として公表された「ロボット新戦略」では，政府のロボット戦略が提示されるとともに，その実現のための「規制・制度改革に係る工程表」として検討が必要な関連法令が示されている。しかし，工程表では，次の六つの法令について見直しの必要性が示されているに過ぎない。

①電波法（遠隔操作や無人駆動ロボットで使用する電波の取扱い），②医薬品医療機器等法（ロボット技術の高度化に伴う医療機器としての承認・認証に係る期間・手続），③道路交通法／道路運送車両法（搭乗型移動支援ロボットの公道走行），④無人飛行型ロボット関係法令（航空法等），⑤高圧ガス保安法（目視などの人間を前提とした点検作業におけるロボット活用に関するルール），⑥消費生活用製品安全法／電気用品安全法（自律性や遠隔操作性を有する生活関連次世代ロボットの消費者安全確保，技術基準の在り方，製造事業者などの責任の範囲）。

当該戦略では国際標準の獲得とともに，規制緩和とルール整備の両面からの規制・制度改革の推進の必要性が示されているが，あくまで現行法の枠組みにおける規制緩和の提示にとどまり，新たな法規制の枠組みや方向性などは示されていない。そこで，今後の行政によるロボット関連施策立案の在り方について五つの意見を述べておきたい。

①社会実装に向けた包括的かつ体系的な課題の把握と整理・検討が必要である。例えば，AIの普及で社会的にどのようは影響が生ずるのか，自律型ロボットが暴走した時に誰がどのように責任を取るのか，技術，機能，法的・倫理的・社会的課題（いわゆるELSI）など総合的な視点からの検討とともに，将来的な課題やリスクへの備えも念頭に社会・制度の変化・変革に対応するための施策の検討が求められている[8]。②政策や施策立案の在り方については，各行政領域によるパッチワーク的な検討ではなく，ロボットやAIの利用促進に向けた方針や政策（戦略）の統一を図る一方で，画一化しない多様かつ柔軟な議論のため多元的かつ多面的な検討（マルチステークホルダー・プロセス）が重要である。また，行政主導による検討

6） フィンテック等の活用に伴う法的課題についての検討は，三部裕幸，落合孝文「金融機関のAI活用に関連する法的問題点：現状では，個人情報保護や知的財産権の保護などが論点に（特集 AIが導く新たな金融）」金融財政事情67（2016）PP.32-35。

7） 大野敬「『自動運転』に関する警察の検討の状況及び今後に向けた取組について」警察学論集69（2016）PP.139-164。

8） 人工知能学会における検討については，松尾豊，西田豊明，堀浩一，武田英明，長谷敏司，塩野誠，服部宏充，江間有沙，長倉克枝「人工知能と倫理（特集 人工知能学会・情報処理学会共同企画人工知能とは何か？）」人工知能31（2016）PP.635-641。

における課題として，③継続的な検討が可能な体制整備が必須である。行政による検討の重複や競合を避け，担当者の交代による施策検討の不連続や断絶が生じないよう，産学民官の参画による継続的な検討体制の整備が不可欠である。④規制の不存在に伴う萎縮効果の解消・ガラパゴス化しない配慮も必要である。自動運転車の公道走行を禁止する法令がないにも関わらず，公道走行のルールがないために研究開発に躊躇したり普及が遅れてはならない。最後に，⑤国際協調ではなく国際的イニシアティブの獲得に向けた検討を目指すべきである。ロボット大国の地位を維持するためには，安易に協調して情報やノウハウが盗まれることを避けるとともに，諸外国の取り組みに先駆けて新たな視点からの検討を行う際には，日本の法文化や法令遵守意識と国外の状況の違いを認識した上での施策検討が必要である。

国の新たな施策や戦略をとりまとめる際に，法的観点から検討が必要な事項は多い。しかしながら，現行法の枠組みにおける規制緩和としての課題の提示にとどまることが多々見受けられる。それを防ぐために，ワシントン大学のライアン・ケイロ（Ryan Calo）は，議会及びFAAによるドローンの利用と飛行制限，高速証券取引アルゴリズム（市場ロボット），FDAによるロボット手術の認可，NHTSAによる自動走行への取り組みなど，行政による個別の検討ではなく，「連邦ロボット委員会（Federal Robotics Commission）[9]」の必要性を提唱している。

2　行政の効率化や法執行におけるAIやロボットの利用

行政の効率化や法執行において，将来的にはAIやロボットの活用が見込まれている。一方，活用を誤ると真の意味での「ビッグブラザー」が実現してしまうおそれがある。

準法律行為的行政行為など定型的な行政事務は，ロボットの活用により自動化や効率化にとどまらず公務員の業務を代替することも可能になるであろう。AIによる問い合わせへの応答ができれば，反復応答で対応可能な相談業務から解放される。窓口の担当者が融通の利かないロボットだと，行政対象暴力に屈する心配もなくなるかもしれない。公の施設や公物の維持管理負担の軽減や的確なメンテナンスのためのロボット活用への期待も高い。各行政機関でのAIの活用の可能性については，行政におけるAIの活用例の想定が示されている報告書[10]が興味深い。

行政が保有する膨大な量の情報の活用を進める「オープンデータ」の取り組みにAIを活用することで，行政情報の飛躍的な活用促進も期待できる。行政処分などの公平性確保のために過去の事例の網羅的・悉皆的な把握や検討でも有用であろう。AIによる議事録の自動生成と分析が可能になれば，膨大な数の会議の運営負担が軽減されるとともに，単に記録として保存する会議録の作成ではなく，大量の公文書を分析して新たな施策立案に資する情報として生かすこともできる。現に，2016年5月から検討が始まった内閣府の「人工知能と人間社会に関する懇談会」では，AIによる議事録分析を行い，会議での議論の傾向や内容分析を行う試みが行われている。分かりやすい議事録は行政の透明化にも資する。

住民にとっても，行政情報の収集や分析にAIを活用することで，情報公開請求により開示された公文書の分析や，住民監査請求の対象となる違法又は不当な財務会計上の行為を発見しやすくなる可能性もある。ただし，情報公開との関係においては，ディープラーニングにより取得した情報や政策立案に係る意思決定の根拠となった情報など，AIを用いて取得・分析がなされた意思形成に関する情報はどの程度開示が可能であろうか。

警察官の安全確保や公平な法執行のためのロボット導入への期待もある。黒人差別的な法執行が大きな問題となっている米国では，差別的な取扱いをしない技術的中立なロボコップの議論がなされている。

しかし，ロボットによる法執行に伴う損害が生

9）Ryan Calo, The case for a federal robotics commission, Monday, September 15, 2014〈https://www.brookings.edu/research/the-case-for-a-federal-robotics-commission/〉.

10）行政情報システム研究所「人工知能技術の行政における活用に関する調査研究」報告書（2016年6月10日）。

じた場合，国家賠償においてロボットの行為は公権力の行使にあたるのか。

環境訴訟においては原告適格の問題が生じたが，ロボットの適正な利用を争い，原告適格が問題となることはないだろうか。

行政の効率化や法執行における利用を目的として，ロボットやAIを導入する場合，効率化のための利用（メリット）だけでなく，利用に伴う行政法上の問題（デメリット）を精査し慎重に検討しなければならない。政府によるデータの集積に伴う管理国家への懸念が，ジョージ・オーウェルの『1984』で示された独裁者「ビッグブラザー」であるが，現在でも，街頭の防犯カメラ画像を一元管理し顔識別技術によりリアルタイムで瞬時に分析したり，ネットワーク上の情報を解析し国民の動静を常時監視することは可能である。しかし，AIが監視結果から犯罪予防・制止や保護・避難などの措置を自律的に判断し，ロボットが即時執行する将来はあまりにも危険だ。「行政における法治ロボットの原則」を定め，行政作用におけるロボットやAIの導入範囲を決めなければ，リアル・ビッグブラザーが完成するおそれがある。

人工公物としての行政ロボットの利用に伴い損害が生じた場合の問責のあり方などについても検討が必要である。ロボット自体の欠陥による被害が生じた場合は公の営造物の設置又は管理の瑕疵として国賠の適用があると考えられる。一方，行政ロボットの悪用により生じた問題については，営造物の管理責任ではなく安全確保義務の懈怠にあたると判断することになるのであろうか。

行政組織との関係においては，専門的見地からAIが行政庁の意思決定に関与する場合，会議体ではなくAIそのものが「諮問機関」として位置づけられる可能性はあるだろうか。ロボットが行政目的達成のために即時執行を行う場合，ロボット単独で「執行機関」としての機能を有するといえるのか。遠隔操作ロボットではなく，AIが搭載された自律ロボットが行政庁の命を待たずに自律的に判断し実力行使を行うことも，将来的に認められる可能性はあるだろうか。攻撃目標を自動追尾する致死性自律型ロボットが，軍事利用ではなく法執行で用いられる可能性もある。

Ⅵ　民 事 法

ロボットやAIの利用・普及に伴い民事法の分野において検討すべき事項は実に多岐にわたる。民法とその特別法（製造物責任法や著作権法）など実体法における問題と，訴訟手続におけるAIの活用など手続法の両面から検討が必要になると考えられる。

自動運転車の事故，AIの機械学習と個人のプライバシー保護など人格的利益の保護，AIが作成した知的財産の保護，自律ロボットの悪用や暴走に伴う損害の賠償，家族の一員としてのロボットの存在など，民事法領域における問題は枚挙にいとまがない。

1　AIと権利能力

将来的には，人間と同様に知識を身につける汎用型人工知能の高度化に伴い，その「知能（AI）」に権利能力を認めるか否か，自然人の意思能力，行為能力と同様の問題を検討すべきか，そもそも「人」と「物」とは何かといった民法の基本原理の見直しを迫られるような問題の検討が必要になる可能性がある。

権利能力については，AIの自律により，権利・義務の主体となり得る地位ないし資格としての新たな「法的人格」を将来的に認めるべきか考えなければならないかもしれない。

例えば，契約法では，契約を結ぶ権利主体（自然人・法人）と権利の客体（目的物）の区別を前提としている。AIが搭載されたロボットを例に考えると，有体物としてのロボットは動産であることから，契約の目的物であって権利の主体になることはできない。つまり，ロボットが契約を結ぶ権利主体になることは想定していないが，自律ロボットが権利主体であるとの外観が存在するような場面が今後出現すると想定される。

そうなると，法的な権利主体として「人工的」に設けられた人である「法人」のように，自然人たる人間が人工的に作り出した人工知能を「AI人」とでも表記するなどして，民法における「人」である自然人と法人に加えて，新たな法人格（権利能力）の法的な位置づけを認めるべきで

あろうか。

八幡製鉄事件では，法人の人権享有主体性が問題となったが，AI人の権利主体性が裁判で争われ，性質上可能な限りAI人に認められる権利は自然人と同様に扱うべきであるとの判断が示される時代が来るかもしれない。

意思能力については，現時点でAIは常識を理解するまでには至っていない。よって，権利能力が認められたとしても事理弁識能力を有するAI人が登場するまでには相当の時間を要すると考えられる。意思無能力者たるAI人による法律行為は無効であるとの判断を脱するには，人工知能が人間の能力を超えるとされる「技術的特異点（シンギュラリティ）」を待たなければならない。

行為能力については，AIの進化を制限行為能力者の類型に当てはめて考えてみたい。明治学院大学の加賀山茂教授との個人的意見交換において，自動運転のレベルごとに民法の行為能力を当てはめて考えることができるのではないかとの示唆を受けた。具体的には，レベル0（自動化なし）の状態は，自動車は自らの判断で一切走行することができないため成年後見人としての運転者が必要。レベル1（特定機能の自動化）は，運転の補助機能の一部自動化で運転者は補佐人。レベル2（複合機能の自動化）はステアリングとアクセルペダルを自動走行システムが制御し走行可能であるため運転者は補助人。レベル3（準自動走行）では，すべての運転操作機能が自動化されているが，自動走行を維持できない状況を判断して運転者が自ら運転操作を行うため，自動走行システムを掌るAIは未成年。レベル4（完全自動走行）は運転操作から周辺のモニタリング機能のすべてが自動化されるため，自動運転を行うAIは成人。

汎用型人工知能が人間と同様の能力を有し判断ができる段階に達すると，AI人を相手に契約を交わすことはあり得るであろう。相手方が自然人であると思って契約をしたところAI人であったり，未熟なAIと契約を交わした時に，未成年者同様に制限行為能力者として法定代理人の同意がない契約は無効となるのか。AIが自らを自然人の成人であると偽って取引をした場合，未成年者同様に詐術として扱ってよいか。

人間の常識が通じないにも関わらず，人間の常識を越える存在にまで進化し，人間の能力を超えるAIが日常的に用いられるようになったとき，人間ではない新たな「人」にどのように向き合うべきか，民法の権利能力を例に考えてみたが，筆者の考察は試行錯誤なのか単なる錯誤なのか今後の評価を待ちたい。

2　財産法に係る問題

財産法の分野では，そもそも財産の管理をロボットやAIに委ねる時代が到来している。フィンテック，AIを活用した投資判断なども用いられ，個人資産の管理や運用をAIに委ねるサービスも提供されている。

自動運転車の事故時の責任として，いわゆるトロッコ問題[11]が議論されることが多い。回避が困難な事故の発生に直面したとき，衝突の対象物や対象者を選択する際に，歩行者の人数や年齢・性別などの属性に基づく評価関数や対象物によって，危険回避の優先順位を判断又は決定することができるのかといった問題である。

最終的に誰が責任を負うのか決められない究極の選択を，法的責任（選択）の問題として明確な線引きを定めることは困難であるとともに，倫理的にも様々な思考実験が行われてきたものの誰もが納得できる判断を示すには至っていない。この問題が解決されない限り，完全自動運転車（レベル0～4に自動走行レベルを分類した場合のレベル4）の公道走行を実現することができないといった見解も見受けられる。しかし，民事法的にはレベル1～3では運転者の位置づけを議論した上で，運転者，運行供用者，製造者などの事故時の責任論について議論を行い保険の在り方を検討し，レベル4では製造者の責任の在り方を考えるしかないのではないだろうか。

一方，情報であるソフトウェア自体は有体物で

11）人間の判断でも選択の決定に躊躇せざるを得ない問題を，AIの判断過程で結論を求めること自体理不尽な要求であるとも思えるが，平野晋「『ロボット法』と自動運転の『派生型トロッコ問題』：主要論点の整理と，AIネットワークシステム『研究開発8原則』」NBL1083（2016）PP.29-37は，トロッコ問題の捉え方について示唆を与えている。

はないため，製造物責任の対象とはならない。AIが搭載された自動運転車やロボットであれば，有体物としてのロボットに組み込まれた動産として製造物に該当するため，他人に損害を与えた場合は製造者等に製造物責任を追及することが可能である。しかし，自動走行システムの搭載地図の誤りによって事故が発生した場合，情報の誤りそのものに製造物責任を問うことはできない。

事故時の責任の所在を明らかにするためには，画像の記録（保存）が不可欠である。AIの機械学習も膨大な量の情報を集めることが必要である。これらの情報には，膨大な量の個人に関する情報も含まれ，個人の人格的利益保護のための取り組みが必要である。

ビッグデータから抽出した個人情報を分析するプロファイリングにより，趣味嗜好に合わせた広告やお勧め商品の提示など行動ターゲティングが既に用いられている。それに加え，商取引でAIを活用して特定の方法で商品を勧めることにより高確率で購入をさせることも可能になる。個人の自己決定に大きな影響を及ぼし，本人の意思表示をも操る究極のAI関係取引においては，「AI消費者契約法（架空の法令名）」により，高度なAIプロファイリング取引では消費者が申込みを行う前に，AIを用いた取引であることを確認する措置を事業者側が講じないと，要素の錯誤にあたるようなAIに唆された申込みの意思表示は無効にするといった規制も将来的には必要になるかもしれない。

AIが自律的に作成した生成物は，現行の知的財産制度では権利の対象にならない。AIがデータを分析して生成した「学習済みモデル」の保護も課題となっている。人間の創作物のように見えるコンテンツがAIによって作成可能になりつつあり，いわゆる「準創作物」の保護の在り方について検討が必要である。

3　家族法に係る問題

家族法についても，ヒューマノイドを養子にしたいとか結婚したいと真剣に考える人も出てくるであろうし，優しく介護をしてくれた自律ロボットに財産を相続させたいと思う人も出てくるかもしれない。精巧なヒューマノイドを家族の一員のような錯覚にとらわれ家族同然に扱う人も出てくるであろう。あたかも人間のように見える「物としてのロボット」の法的地位は，動物に準ずるのか，新たな奴隷なのか。ロボットの虐待は単なる動産への侵害ではあるものの，動物愛護的な考えも必要であろうか。動産としてのロボットに対する損壊や毀損の責任だけを論ずることで法的には問題はないにせよ，人と類似したヒューマノイドを虐待している様子を客観的に目撃した場合，単なる物の損壊と心情的に割り切ることができるであろうか。

「私人間（しじんかん）」の意味が，アシモフの「われはロボット（I Robot）」にいう「私（AI又はロボット）」と「人（自然人又は法人）」の「間」の問題として議論される日が来るかもしれない。

Ⅶ　刑 事 法

ロボットやAIの利用・普及に伴い刑事法分野で検討すべき問題は，それらを利用した新たな犯罪の類型や構成要件などに関する「刑事実体法」に係る問題，犯罪捜査手法や適正手続の保障に関する「刑事手続法」をめぐる問題に分けて検討が必要となる。

1　刑事実体法に係る問題

殺人ロボットの利用すらもはやSFの世界の問題ではない。戦場では既に攻撃用ドローンが投入されており，自律型致死兵器システムの規制も特定通常兵器使用禁止制限条約締約国会議（CCW）で議論されている。これらの兵器が，テロや犯罪の手段として利用されるのも時間の問題である。

刑事実体法に係る問題として，今後想定されるロボット・AI関係犯罪の類型を①AI・ロボット利用型犯罪と②同関連型犯罪に分けて考えてみたい。

①は，AIやロボットの利用自体は違法・不正ではないが，その利用結果が犯罪・不正行為を構成する場合。そのようなロボットの製造こそ違法ではないが，麻薬取引や強盗などの違法行為においてロボットに犯罪を実行させる場合がこれにあたる。AIを利用した犯罪としては，電話の相手方が人間なのかAIなのか判別がつかない状況が

将来的に見込まれるが，ビッグデータを解析して詳細な個人情報を把握した上で，ディープラーニングを用いた分析結果により対象者に応じて精巧に親族を装った振り込め詐欺の電話を掛ける AI が出現したとき，機械学習とパターン認識の精度が向上することで，現在以上に詐欺の被害が深刻になるおそれがある。AI による高度なマネーロンダリング，Tay のような AI の暴走による名誉毀損や風説の流布も問題になるであろう。機械学習で収集対象となった著作物は複製権侵害にあたらないのか，全裸のヒューマノイドロボットの陳列はわいせつ物の公然陳列か公然わいせつなのかも議論が必要である。

ドローンを利用した犯罪も，衣服を着用していない場所の窃視，ロボット・ストーカー，窓の隙間から小型ドローンが侵入して企業の機密情報が記録された媒体を盗むような事件も発生するであろう。

②は，AI・ロボットの利用行為自体が違法であり，それらを用いて実行される犯罪または不正行為。ネットワークを介したロボットへの不正アクセスにより，犯罪を実行するためにロボットを制御したり，犯罪実行マルウェアに感染させて自律的に犯罪に従事させるようなことが想定される。不正アクセス禁止法は，ネットワークを介しアクセス権限がないコンピュータを利用する行為を禁止しているため，このような無権限アクセス自体は処罰の対象となる。しかし，ネットワークを介さずに目の前のロボットのプログラムを不正に直接書き換える行為や不正アクセス後の犯罪行為は同法では処罰できない。

AI 開発者の刑事責任についても，ファイル交換ソフトに係る著作権侵害をめぐる事案を思い出す。ウィニー事件では違法コピーなど著作権侵害コンテンツを送信可能状態にしたとして著作権法違反の幇助に問われたが，著作権侵害に利用する蓋然性が高いことを認識・認容していたとまで認めることが困難であり，著作権法違反罪の幇助犯の故意が欠けるとして無罪になった。AI により自律的に動作するロボットが犯罪に従事したとき，AI 開発者の責任はどこまで問われるのであろうか。

2　刑事手続法に係る課題

法執行におけるロボコップ（ロボット警察官）の導入，犯罪捜査における AI プロファイリングの活用，犯罪予知 AI を用いた犯罪予防対策の実施など，犯罪捜査の手法や適正手続の保障に関する刑事手続法をめぐる問題は，AI の利用やロボットの導入により革新的な変化がもたらされる可能性が高い。しかし，その利用方法によっては，究極の監視社会化や警察国家へのおそれもあり，どのような問題が生ずる可能性があるのかを慎重に見極めた上での導入が求められる。ロボットが取得する音声や画像，各種センサーの記録（ログ）も，犯罪捜査において重要かつ有力な証拠となり得る。

ロボコップは，掃除ロボットで知られるアイロボット社（iRobot）や警察の法執行用具開発メーカーであるテイザー社（Taser）などが既に研究開発を行っている。犯罪者に躊躇なく対峙する法執行が可能になり，警察官の人的被害の心配もなくなる。しかし，技術的に中立性が保たれているはずのロボコップが，人種差別的な法執行に及ばないとは言い切れない。

人種差別と警察による法執行の問題については，それらの活動を自動化することによって警察による差別の本質的な問題が解決されるのか。多くの人々にとって，技術は政策的に中立であると信じられている。将来のロボコップは，その考えに基づいて中立的な立場で法を執行することが期待されている。その結果として，人種差別や偏見等とは関係なく活動ができるということが期待されている。

そのような観点からすると，ロボコップの導入は人種差別的な政策に対する技術による解決手段と考えることもできるのかという問いに対し，技術は社会における様々な問題を増幅したり，既に社会に存在する問題を反映することもあり，ロボコップの導入によって人種差別的な政策に一層拍車がかかるという危険が存在するとの見解もある[12)]。

実際に他の視点から考えてみると，デジタル技術は人種差別との関係においては技術的に中立性は保たれていないことがある。例えば，自動水栓では，蛇口の前に手をかざしても肌の色が黒いこ

とによって動作しないことがあり，顔認識技術が，人種差別的な問題を発生させるおそれもある。

連続盗犯事件で令状なしにGPSを設置した捜査が日本国内でも問題となったが，自動追尾ロボットやドローンを活用することにより，尾行や張り込みを長期間・連続して実施することが可能となる。性犯罪者の監視目的で追跡装置を足首に装着する試みが海外では既に実施されており，保護観察中の人物を捕捉し続けたり，ストーカー禁止法に基づく接近禁止命令の実効性確保にも有効な手段になり得る。

証拠収集についても，捜査対象者に密行的に密着してリアルタイムで会話を傍受し映像を撮影し続ける超小型ロボットの導入が予想される。犯罪捜査との関係においては，会話の傍受は密行用増幅器（スパイクマイク），通信傍受の対象は，電話，携帯電話，電子メール，ペンレジスター，位置や所在の探知には，監視カメラ，ポケットベル（beeper），熱感知投影装置（FLIR），電子通信の傍受については，カーニボー（現在は，DCS 2000と改称），KLS（キー・ロガー・システム），その他，電磁波傍受「テンペスト」など実に多種多様な手段が用いられてきた。

1942年の米国のゴールドマン事件を端緒に「小型電子盗聴器（bug）」による会話傍受（bugging）が裁判において争われるようになったが，虫（bug）のように小さなロボットによる文字どおりの「バギング」が問題になるであろう。自動走行車が撮影した映像だけでなく，掃除ロボットなどの生活支援ロボットが記録した音声と画像などが犯罪捜査で有力な証拠になることもあり得る。

犯罪捜査においてAIを活用するとプロファイリングの精度は飛躍的に向上する。経験則に基づくベテラン捜査官による分析とは比較にならない。しかし，AI鑑定の導入はDNA鑑定同様に誤判が生じる可能性があることを認識して行う必要がある。AIによる判断に基づいて実施することへ懸念だけでなく，そのような技術を用いることの当否を問わなければならない。

犯罪捜査におけるAIの活用は，膨大な証拠から犯人特定に必要な情報を抽出するなど事後的に犯人の検挙を支援する一方で，事前にAIを利用して犯罪を予測しようという取り組みもある。国内でも，犯罪の発生場所の予見に既に用いられている。ロンブローゾは，生来犯罪者説を提唱した。科学的根拠がなく実際に刑事手続において用いられることはなかったが，AIの利用により犯罪に従事する確率が高いという結果が示されるだけでも，その人物の人生を左右しかねない。公権力によるAI犯罪予知技術の利用は，極めて重大な人権侵害や差別をもたらすことが懸念される。

例えば，ゲノム（遺伝子）情報と顔の形状のビッグデータを取得し関連解析を実施することにより，顔の形状の個人差に関連するゲノム多型を網羅的に特定し，個人のゲノム多型のデータに基づいて，その個人の顔の形状を正確に予測することを試みる研究がある。そのような研究を用いると，顔の情報を識別することでDNAの分析を行い，犯罪に従事する可能性がある人の傾向や分析をすることができる可能性がある。人間の病気や疾患は，顔や人間の皮膚などの表面にその症状や兆候がからわれることを参考に人間の顔を分析することを試みるものである。ゲノムから顔形状の予測とは逆方向に，顔形状からゲノムを予測することで，顔画像を医療における疾患診断補助に利用できるメリットがある一方で，犯罪捜査（予知）において用いることによる問題は議論すら行われていない。

ロボットを用いた犯罪では，事件と事故の見極めが難しくなる。犯罪に利用されたロボットから犯罪の実行者を特定することも困難になると予想される。ネットワーク犯罪でアクセスログを解析した結果，誤認逮捕が発生した事例は記憶に新しい。ロボットには指紋がなくDNAもない。自動車事故のように証拠となる部品の断片が残されていたり，監視カメラで撮影された画像の分析によりロボットを特定しその登録者や管理者を確認できても，犯人の特定にまで至らないおそれもある。犯罪に利用されたロボットからの犯人特定に至るプロファイリングが困難にならぬよう，ロボット

12） Peter Asaro, Will #BlackLivesMatter to RoboCop?, We Robot 2016 Working Paper 3/20/2016 (2016).

利用犯罪のフォレンジック（捜査手法）を確保するための方策を検討しなければならない。

AIの利用に伴う刑事責任については，例えば，マイクロソフトのTayが差別的な発言をしたことについて，未熟なAIによる差別的な発言は責任能力が認められないため名誉毀損罪は成立しないが，成熟したAIによる差別的発言は成人同様に刑事責任が問われるのかという民法上の権利能力と同様の問題についての検討が必要となる。

ディープラーニング（深層学習）を用いた検証によって事件の「真相」は明らかになるだろうが，「深層」学習による学習内容の真相は誰も検証できないおそれが高い。

Ⅷ　ロボット・ロー・バイ・デザイン

将来的に自律型ロボットが社会で広く利用されるようになると，人間が操作するロボットやプログラムされた範囲内で動作するロボットは異なる問題が生ずるおそれがある。

アイザック・アシモフは，「ロボット工学の三原則」（Three Laws of Robotics）を小説において記している。

ロボット工学の三原則（Isacc Asimov, I, Robot[13]）
第1条　ロボットは人間に危害を加えてはならない。また，その危険を看過することによって，人間に危害を及ぼしてはならない。 第2条　ロボットは人間にあたえられた命令に服従しなければならない。ただし，あたえられた命令が，第1条に反する場合は，この限りでない。 第3条　ロボットは，前掲第1条および第2条に反するおそれのないかぎり，自己をまもらなければならない。 ――ロボット工学ハンドブック， 第56版，西暦2058年

手塚治虫も「鉄腕アトム」において，手塚治虫のロボット法を記している。

手塚治虫『鉄腕アトム⑮（手塚治虫漫画全集）』講談社（2003）15頁
第1条　ロボットは人間につくすために生まれてきたものである 第2条　ロボットは人を傷つけたり殺したりしてはいけない 第3条　ロボットを作った人間を父と呼ばなくてはいけない 第4条　ロボットは何でも作れるがお金だけは作ってはいけない 第5条　ロボットは海外へ無断で出かけていってはならない 第6条　男のロボット　女のロボットはたがいに入れかわってはいけない 第7条　無断で自分の顔をかえたり別のロボットになったりしてはいけない 第8条　おとなに作られたロボットが子どもになったりしてはいけない 第9条　人間が分解したロボットを別のロボットが組み立ててはならない 第10条　ロボットは人間の家や道具を壊してはならない

これらは，2人の天才が生み出した「思想」であって，「法」や「規範」ではない。そこで，将来的なロボット共生社会に向けて求められる基本となる原則として，筆者は，OECDプライバシー8原則を参考に，前述の2015年のロボット法学会設立準備研究会において「ロボット法　新8原則（新保試案）[14]」を公表した。

ロボット法・新8原則（新保試案）	
①人間第一の原則 （Humanity First）	・人間に危害を加えてはならない ・ヒトになってはいけない
②命令服従の原則 （Obedience to Order）	・人間の命令に従わなければならない ・管理及び制御可能性を担保すること
③秘密及びプライバシー保持の原則 （Secrecy and Privacy）	・ロボットが知り得た秘密は守ること ・プライバシー・バイ・デザインに基く設計を行うこと
④利用制限の原則 （Use Limitation）	・本来の利用目的以外の目的での利用を制限 ・公序良俗に反する利用の制限 ・人間への危害・加害目的での利用制限 ・ロボット利用倫理の検討

13）アシモフ財団〈http://www.asimovonline.com/oldsite/Robot_Foundation_history_1.html〉.

14）新保史生「何故に『ロボット法』なのか」ロボット法学会設立準備研究会（2015年10月11日）報告資料（2015）。

⑤安全保護の原則 （Security Safeguards）	・ロボットの利用に伴う安全性の確保 ・安全基準の策定，当該基準に基づく開発及び利用 ・安心して利用できる環境確保のための制度の整備
⑥公開・透明性の原則 （Openness & Transparency）	・ロボット開発における開発内容の公開・透明性の確保 ・ロボットの利用方法における透明性の確保
⑦個人参加の原則 （Individual Participation）	・ロボットの利用ルール策定における個人の参加 ・ロボットによる個人管理の制限
⑧責任の原則 （Accountability）	・ロボットの取扱いに伴い生じた責任（法的責任）への対応 ・ロボットの取扱いにおける倫理的，道義的責任の考慮

事後救済や原状回復が困難なプライバシー侵害同様に，自律型ロボットによる問題も事後対応ではなく，ロボット共生社会を迎えるにあたって，「ヒト」に近づくロボットに対し，「人」がしなければならないことを，あらかじめ考えておくこと。「ロボット・ロー・バイ・デザイン」により安全・安心なロボット利用に必要な対策を講ずるべきではないかという発想である。

ロボットが普及することにより，将来的には様々な場面で人間が排除される世界の拡大が見込まれる。AIやロボットが人間に代わって様々な職業に従事するであろうし，高速道路は自動走行モードでしか通行できなくなるかもしれない。前者は労働力不足を補うことや危険業務からの解放などのメリットがあり，後者は事故防止や渋滞緩和につながる。しかし，そのような社会の到来は，人間が生きる喜びを享受できる望ましい社会なのだろうか。まずは，「人間第一の原則」から考えたい。

Ⅸ 「AI開発ガイドライン」

AIについては，総務省「AIネットワーク化検討会議」が，2016年4月15日に中間報告書として「AIネットワーク化が拓く智連社会（WINS（ウインズ））―第四次産業革命を超えた社会に向けて―」を公表している。

報告書では，⑴ 目指すべき社会像として，「高度情報通信ネットワーク社会」，「知識社会」の次に目指すべき社会像として，「智慧」の連結に着目して「智連社会」（Wisdom Network Society: WINS（ウインズ））を構想。⑵ AIネットワーク化の影響として，公共（まち）／生活（ひと）／産業（しごと）の分野ごとに，2020年代～2040年代の時系列で影響を評価。⑶ AIネットワーク化のリスクとして，AIネットワーク化のリスクを検討するための枠組みの整理及び現時点で想定されるリスクを例示。⑷ 当面の課題として，研究開発の原則の策定，利用者保護の在り方，社会の基本ルールの在り方等を提示し，AIネットワーク化をめぐる諸課題に関し，継続的に議論する国際的な場の形成及び国際的な場での議論に向けた国内での検討体制の整備の必要性を提唱している。

報告書で示されたAI研究開発8原則は，2016年4月に開催されたG7サミットの情報通信相会合において公表され各国の同意を得ている。

研究開発に関する原則として示された8原則は，①透明性の原則（AIネットワークシステムの動作の説明可能性及び検証可能性を確保すること），②利用者支援の原則（AIネットワークシステムが利用者を支援するとともに，利用者に選択の機会を適切に提供するよう配慮すること），③制御可能性の原則（人間によるAIネットワークシステムの制御可能性を確保すること），④セキュリティ確保の原則（AIネットワークシステムの頑健性及び信頼性を確保すること），⑤安全保護の原則（AIネットワークシステムが利用者及び第三者の生命・身体の安全に危害を及ぼさないように配慮すること），⑥プライバシー保護の原則（AIネットワークシステムが利用者及び第三者のプライバシーを侵害しないように配慮すること），⑦倫理の原則（ネットワーク化されるAIの研究開発において，人間の尊厳と個人の自律を尊重すること），⑧アカウンタビリティの原則（ネットワーク化されるAIの研究開発者が利用者等関係ステークホルダーへのアカウンタビリティを果たすこと）となっている。

Ⅹ 安全保護及びセキュリティ確保の原則

前述の諸原則は，今後引き続き検討を行うこと

が必要となるが，安全保護及びセキュリティ確保の原則については，喫緊に検討が必要であるため，本稿では当該原則について言及しておきたい。

1　情報セキュリティ対策の新たな課題

AIやロボットの普及により，物理的な媒体や装置を構成するチップの情報セキュリティ対策が大きな課題になると考えられる。その理由は，IoTにより，あらゆるモノがネットワークに接続され，その結果，ネットワークを介して様々な家電製品やモノを操作することができるようになること。それに加えて，ロボットやAIの発達により，日常的にそれらが利用されるような社会になると，この問題の重要性は急激に増幅すると考えられる。

例えば，ネットワークのセキュリティについては，ネットワークを介した不正アクセスの防止や，コンピューターウィルスやマルウェア対策など，情報のセキュリティを確保するための様々な対策が講じられてきた。ところが，装置のセキュリティそのものについて，例えばチップについてはそもそも書き換えることを前提にして作られているため，物理的にはすぐに書き換え可能な状態になっている。現状では，機械や装置の蓋を開けて基盤に装着されているチップを書き換えることは容易である。

自動車の盗難防止装置として「イモビライザー」という装置がある。電子的に符合が一致することで車が動作する。電子キーを用いた鍵は通常の鍵のように偽造することが極めて困難である。イモビライザーは，電子的な符号が一致しなければ車を動作させることができないため盗難防止の手段としては非常に有効な手段と考えられている。ところが，イモビライザー装着車であっても盗難被害に遭っている。その理由は，車の窓ガラスを割ってダッシュボードを開けて，ダッシュボード内に装着されているイモビライザーを入れ替えるだけでエンジンが始動できてしまうからである。つまり，電子的に高度なセキュリティ対策を講じていても，物理的にその装置が入れ替えられてしまうだけで，高度なセキュリティは意味をなさなくなる。今後は，ロボットが日常的に用いられるようになると同様の問題が発生すると考えられる。

2　新たなセキュリティ脅威

ネットワークを介したロボットへの不正アクセスやハッキングにより，犯罪を実行するためにロボットを制御したり，犯罪実行マルウェアに感染させて自律的に犯罪に従事させるようなことも想定される。

不正アクセス禁止法は，ネットワークを介しアクセス権限がないコンピュータを利用する行為禁止しているため，ネットワークに接続されたロボットへの無権限アクセスは処罰の対象となる。しかし，ネットワークを介さずに目の前のロボットのプログラムを不正に直接書き換える行為や不正アクセス後の犯罪行為は同法では処罰できない。

ロボットへのDoS攻撃（サービス拒否攻撃）によりインフラを管理するロボットが停止した場合の影響。マルウェア等により悪意ある第三者に乗っ取られた多数のゾンビコンピュータで構成されるネットワークを「ボットネット」というが，その語源は，操り人形としての「ロボット」である。DDoS攻撃（分散サービス拒否攻撃）のように，ロボットをマルウェアに感染させることによって特定の対象物を複数のロボットで一斉に攻撃する文字通りの「ロボット・ボット・ネットワーク」が出現したときの社会的脅威は計り知れない。ヒッチコックの映画「鳥」のように，特定の対象にマルウェアに感染したドローンが一斉に襲いかかったり，自動走行車が政府機関に一斉に突入するようなセキュリティ・リスクは机上の空論とは言えない。

そのための対策を今後実施する上で参考となる例を一つ挙げてみたい。2015年に首相官邸の屋上へのドローンの落下事件が発覚し，その後も様々な場で落下や衝突事故が発生したことを受けて航空法の改正に至っている。飛行禁止空域の設定，夜間飛行禁止，目視による常時監視，人又は物件との距離確保が義務付けられた。この法改正が意味するところは，技術的な安全基準に基づいて安全に飛行できるドローンであっても，「安心して」社会で利用できるわけではないことを示している。安全基準に適合したドローンであっても，家の中を覗き見るなど撮影されたくない人や場所を対象に利用されたり，飛行させると危険な場所での飛行がなされるといったような問題は，その

ような基準ではカバーできないのである。よって，新たなセキュリティ脅威には従来からのネットワークのセキュリティ対策では対応できないことや，安全だけでなく安心な利用のための対策の検討も必要であることを認識する必要がある。

3　情報セキュリティのゆくえとロボット法

インターネットの出現当初は，情報セキュリティ対策の必要性はほとんど認識されていなかった。そのため，ウィルス対策や不正アクセスをはじめとするネットワークの不正利用のための対策は，事後的に対応が必要になってから実際に対策が実施されるようになった。

AI の発達，IoT の普及，自律型のロボットの登場などが見込まれる現在，ネットワークのセキュリティ対策にだけ目を奪われていると，実社会におけるさまざまな物理的な装置のセキュリティ対策が講じられていない状況では，インターネットの普及とともに情報セキュリティ対策の不備による問題と同じことを繰り返す可能性がある。

このことからしても，情報セキュリティ対策は，単に，その確保のための防御的な対策ではなく，マネジメントシステムを活用することをはじめとして，組織的かつ体系的な取り組みが必要であるとともに，リスクマネジメントの観点からの対策の重要性を認識しなければならない。

目の前のパソコンがコンピュータウィルスに感染した場合，パソコンを使用することができないという不便を感じるが，それによって身の危険を感じる人はいないであろう。一方，目の前のロボットがコンピュータウィルスに感染して暴走し，自分を襲ってくるとしたら。そのような脅威も想定し，ロボット法の研究を進めていきたい。

＊　本研究は，国立研究開発法人科学技術振興機構　戦略的創造研究推進事業（社会技術研究開発）「人と情報のエコシステム（HITE）」研究開発領域による研究成果の一部である。（This research was suppported by RISTEX, JST.）

モバイル・インターネットにおける青少年保護対策の新しい動きについて

京都大学大学院法学研究科教授
曽我部　真　裕
SOGABE Masahiro

Ⅰ　はじめに

モバイル・インターネット，とりわけ携帯電話からのインターネット利用における青少年保護のための法制度は，2008年制定の青少年インターネット環境整備法（青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律〔平成20年6月18日法律第79号〕）を中心とする共同規制の仕組みが確立し，SNSを介した福祉犯被害の件数が減少するなど，一時期は一定の成果を挙げたと評価されている。しかし，その後の状況の変化により，福祉犯被害の件数が再び増加するなど，新たな対策が求められていた。2016年には総務省や関係事業者・団体等においてこうした課題に改めて取り組む動きがあり，新たな対策が示された。また，与党において青少年インターネット環境整備法の改正案が検討されている。本稿では，こうした新たな動きを紹介した上で，簡単な検討を加えることとする[1)2)]。

Ⅱ　従来の枠組みとその限界

1　従来の枠組み

⑴　青少年インターネット環境整備法

従来の枠組みについては，以前検討したところであるが[3)]，便宜上，改めて簡単にまとめておきたい。まず，青少年インターネット環境整備法は，①青少年の情報リテラシー能力を習得すること，②青少年が有害情報を閲覧する機会をできるだけ少なくすること，③民間における自主的かつ主体的な取組に大きな役割を認めること，を基本理念としてインターネットにおける青少年保護施策を行うことを求めるものである（同法3条〔以下，同法については「環境整備法」あるいは単に「法」とも言う。〕）。

そのうち，①青少年の情報リテラシー能力を習得すること，に関しては，法13条から16条までにおいて教育啓発活動の推進に関して定められており，携帯電話事業者やフィルタリング事業者のほか，総務省をはじめとする行政機関の関係団体，地方公共団体など様々な主体によって啓発活動が展開されている。

②青少年が有害情報を閲覧する機会をできるだけ少なくすること，に関しては，具体的にはフィルタリングの提供義務等が規定されている。すな

1)　なお，筆者は後述の総務省タスクフォース，安心協及びフィルタリング利用促進検討会での検討に関与したが，本稿で述べることは個人的な意見である。

2)　法案は国会提出に至っておらず，公開されていない。これについて筆者は最新の情報を持たないため，本稿で言及することはできないが，携帯電話事業者が契約時に利用者が青少年か否か確認することの義務付け，契約時の説明義務，契約時にアプリのフィルタリングの有効化することの義務付け等が検討されてきているようである。

3)　拙稿「共同規制 携帯電話におけるフィルタリングの事例」ドイツ憲法判例研究会（編）『憲法の規範力とメディア法（講座 憲法の規範力 第4巻）』（信山社，2015年）87頁。本稿はこの論文のいわば続編である。また，曽我部ほか『情報法概説』（弘文堂，2016年）251-257頁〔曽我部執筆〕で青少年インターネット環境整備法の概説を行っている。

わち，携帯電話インターネット接続役務提供事業者（以下，「携帯電話事業者」という。）は，契約の相手方又は端末利用者が青少年である場合には，フィルタリングの利用を条件として，携帯電話インターネット接続役務を提供しなければならない（法17条1項）。ただし，保護者がフィルタリングを利用しない旨の申出をした場合にはこの限りでない（同項但書）。また，保護者は，契約の締結にあたり，青少年が利用する旨を申し出なければならない（同条2項）。ただし，これらの義務の違反に対する罰則等はない。

以上はスマートフォン（以下，「スマホ」という。）を含む携帯電話についてであるが，それ以外にもiPod Touchなどの携帯音楽プレーヤーや携帯ゲーム機，タブレット端末（携帯電話事業者との契約のないタイプのもの）など，ネット接続機能を有する機器は存在する。これについては，フィルタリングソフトの組み込み等によりフィルタリングの利用を容易にする措置を講じた上で販売する製造事業者の義務が定められている（法19条）。

そのほか，特定サーバー（ネットを利用した公衆による情報閲覧のように供されるサーバーのこと〔法2条11項〕。）の管理者は，その管理する特定サーバーを利用して他人により青少年有害情報の発信が行われたことを知ったとき又は自ら青少年有害情報の発信を行おうとするときは，当該青少年有害情報について，インターネットを利用して青少年による閲覧ができないようにするための措置をとる努力義務が定められている（法21条）。

携帯音楽プレーヤーや携帯ゲーム機は青少年に広く普及しており，これらの機器におけるフィルタリング利用促進も重要な課題であるが，実際には顕著な取組みが見られないため，以下では，携帯電話のフィルタリングに絞って検討を行う。

⑵ EMAを中心とする共同規制

モバイルコンテンツ審査・運用監視機構（EMA）は，モバイルコンテンツの健全化等を目的とし，インターネット事業者を中心とする会員によって構成される一般社団法人であり．環境整備法の制定と前後して2008年に設立された。

EMAの業務のうちもっとも重要なのは，法17条の携帯電話フィルタリングと関連する，ウェブサイトおよびスマホ等向けアプリの認定制度である。現在主流となっているフィルタリングの仕組みは，コンテンツのカテゴリー単位のものである。たとえば，Facebook，Twitter，LINEなどのようなソーシャルメディアは「コミュニケーション」のカテゴリーに分類され，フィルタリング対象となっている[4)]。しかし，利用者の年齢確認やサービス内のメッセージの監視など，青少年の利用に配慮した運用がされているとしてEMAの認定を受けると，フィルタリング対象となるカテゴリーに属するサイトもフィルタリング対象外となり，青少年も閲覧可能となる。当初は携帯電話サイトが認定の対象であったが，スマホの普及によってアプリの認定制度も設けられている。

この仕組みの前提条件になっているのは，前述のように携帯電話においては，フィルタリングの利用が原則として義務化されていることである（17条）。義務化されているからこそインターネット事業者はフィルタリング対象から外れるために青少年の利用に配慮する体制を構築してEMAの認定を申請するインセンティヴが生まれることになる。つまり，以上のような携帯電話フィルタリングの仕組みは，環境整備法17条による公的規制と，民間の第三者機関であるEMAによる自主規制とを組み合わせた共同規制である。

こうして，モバイル・インターネットにおける青少年保護のための従来の対策の柱は，フィルタリング提供義務とEMAによる認定制度に基づく共同規制の枠組みと，教育啓発活動との2本立てということになる。

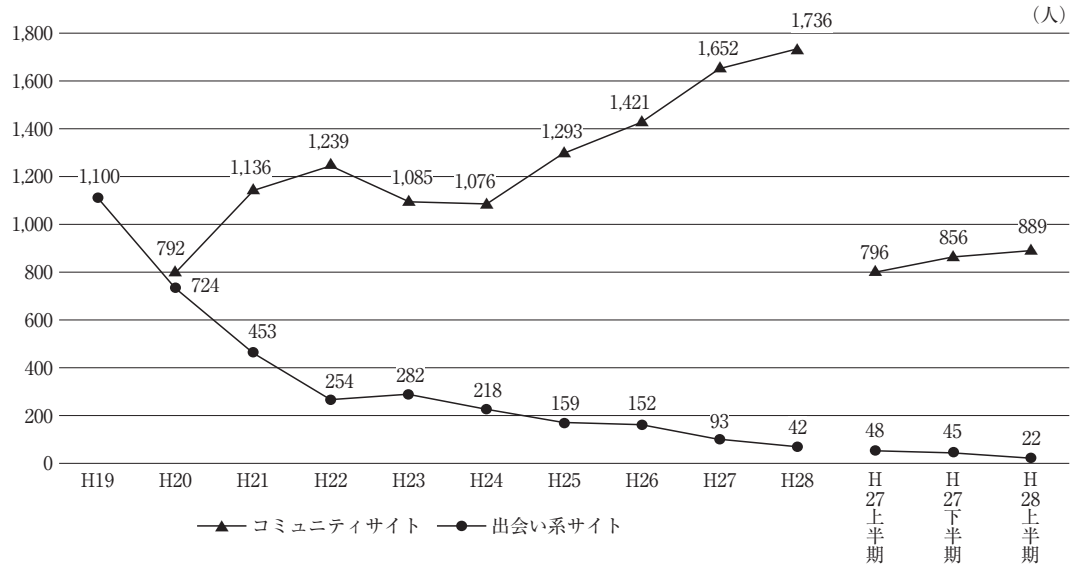
2 従来の枠組みの効果と限界

⑴ 従来の枠組みの効果

以上のような枠組みの効果はどのようなものであったのかを的確に測定する指標は示されていないが，しばしば用いられる指標として，警察庁が半年ごとに発表する「コミュニティサイト等に起因する事犯の現状と対策について」という資料に

4) ただし，携帯電話事業者によっては，例えば高校生向けのフィルタリングにおいては独自の判断でこれらのサイト・アプリをフィルタリング対象外としている場合もある。

【コミュニティサイト及び出会い系サイトに起因する事犯の被害児童数の推移】



掲載されるいわゆる福祉犯（青少年条例違反及び児童買春・児童ポルノ規制法違反が中心である。）の被害児童数の統計がある[5]。

これが適切な指標と言えるかどうか議論はあるが，さしあたりこれによってみれば，一般に使われているSNSの総称である「コミュニティサイト」に起因する事犯の被害児童数は，上記のような枠組みが作られたのち，平成23年および24年には減少した。このことからすれば，一定の効果があったとも言える。しかし，平成25年には再び増加に転じ，その後，増加の一途を辿っている。青少年のSNSの利用者数が増えている可能性があるなど，単純に被害児童数だけでは状況を評価することはできないが，新たな取り組みが求める主張が強まる背景となったことは確かである。

(2)　従来の枠組みの限界

このような状況になった背景には，従来の枠組みにはいくつかの限界があったことにより，フィルタリングの関係で言えば，その利用率は低迷するようになった[6]。ここでは次の3点について述べる。(a)は環境整備法の問題であり，(b)(c)は外部環境の変化に関わるものである。

(a)　保護者の選択権の承認

前述のように，環境整備法17条1項は契約者又は利用者が青少年である場合にはフィルタリングの利用を契約の条件とすることを義務付けているが，同項但書において保護者から利用しない旨の申出があった場合にはその限りではないとしている。そして，法律上，こうした申出をするについての理由は問われない。そのため，フィルタリングの提供義務制とは言われるものの，実態としては選択制になっているとの指摘もあったところである。

そこで，大多数の都道府県においては，青少年条例を改正し，上記の申出をする際に正当な理由を要求し，あるいは申出をする際の理由を限定列

5)　最新のものは，2017年4月20日発表の警察庁「平成28年におけるコミュニティサイト等に起因する事案の現状と対策について」（http://www.npa.go.jp/cyber/statics/h28/h28_community.pdf，https://www.npa.go.jp/cyber/statics/h28/h28_community_shiryou.pdf）である。図の出典も同資料である。

6)　フィルタリング利用率については正確な調査が困難であるようであるが，内閣府の調査によれば，2015年度において，従来型の携帯電話では64.7%，スマホでは45.2%であった（内閣府「平成27年度 青少年のインターネット利用環境実態調査 調査結果（概要）」〔2016年3月〕19頁〔http://www8.cao.go.jp/youth/youth-harm/chousa/h27/net-jittai/pdf/kekka_gaiyo.pdf〕）。

挙するようになっている。例えば，東京都は2010年の青少年条例改正で，保護者がフィルタリングを利用しない旨の申出をする際には，保護者が適切に監督することその他正当な理由を記載した書面を携帯電話事業者に提出しなければならないなどとする規定をおいている（18条の7の2第1項）。「正当な理由」としては，①青少年が就労している場合において，フィルタリングを利用することで業務に著しい支障を生じること，②心身に障害を有し又は疾病にかかっている場合において，フィルタリングを利用することで日常生活に著しい支障を生じること，③保護者が青少年のインターネット利用状況に関する事項を閲覧できるサービスを利用すること等により適切に監督すること，および④以上3つに準ずる正当な理由，となっている（青少年条例施行規則30条の3第2項）。

環境整備法は，「青少年を直接監護・養育する立場にある保護者がそれぞれの教育方針及び青少年の発達段階に応じて判断するのが適当である」ことを理由に保護者の意思を尊重している[7]。保護者の意思を全面的に尊重することの是非は別として，こうした法律の趣旨からすれば，条例による上記のような規制の適法性には疑問がある[8]。このような規制をするのであれば，法律の改正によるのが望ましいだろう。

もっとも，このような規制がどの程度保護者の軽率な判断を防止しているのかは明らかではない。

(b)　スマホへの移行

日本ではスマホの普及は2010年ころから始まり，2013年に6割を超えたあとは普及率が鈍化している[9]。スマホにおいては，フィルタリングの仕組みが従来型の携帯電話（フィーチャーフォン）よりも複雑であり，かつ，普及し始めた当初においては，そもそもフィルタリングを機能させることができなかったため，フィルタリングの普及が遅れる事態となった。

フィルタリングの仕組みについて述べれば，フィーチャーフォンにおいては携帯電話事業者が管理する回線上でフィルタリングをかけることができた。スマホにおいても，携帯電話事業者の回線を通じてネットにアクセスする場合は同様であるが，無線LAN（Wifi）経由やアプリを通じたネットへのアクセスについては別途フィルタリングアプリをインストールする必要がある。さらに，アンドロイドOSのスマホには携帯電話事業者がフィルタリングアプリをプリインストールすることができるが，iOSについてはそれができないため，利用開始後にフィルタリングアプリをダウンロードしてインストールするという煩雑な作業が求められる。青少年の間ではiPhoneの人気が高いとされ，このことはフィルタリングの普及を図る観点からは大きな障害である。

また，そもそも，環境整備法17条の義務の対象となるのは，「携帯電話インターネット接続役務」についてであって，無線LANやアプリのフィルタリングはその義務の対象外である。実際には，携帯電話事業者大手3社は無線LANやアプリのフィルタリングについても「携帯電話インターネット接続役務」に準じた対応をしているが，法律の規定としては両者は区別されている。

さらに，スマホへの移行に関連して，MVNO（仮想移動体通信事業者）におけるフィルタリング対応が課題となる。これはまだ顕在化しているとはいえないが，MVNOによるいわゆる格安スマホの普及が進んできている中で，環境整備法との関係を整理することや，販売時の手順をどのようにするのかといった点の検討が求められる。

(c)　利用されるSNSサービスの変化

環境整備法制定・施行当時に多く利用されていたSNSサービスは，mixiやグリー，モバゲーといった国内のサービスであった。また，これらのサービスの運営事業者は，SNSを通じた福祉犯被害が社会問題となったことを背景に従来の枠組みが整備された経緯をよく理解していたため，EMA認定の取得や啓発活動など，従来の対策に積極的に協力した。このことが従来の枠組みの実

7）内閣府，総務省，経済産業省「青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律関係法令条文解説」（2009年）21頁（http://www8.cao.go.jp/youth/youth-harm/law/pdf/kaisetsu.pdf）。

8）省庁の研究会・検討会等による評価については，前掲拙稿95頁注（21）参照。

9）総務省『情報通信白書（平成27年度版）』（2016年）369頁。

効性を高めたといえる。

その後，これらのサービスに代わって，LINE，Twitter，Facebookなど外国企業の運営するグローバルなSNSサービスが日本でも人気を博するようになった。これらのサービスの多くはそれぞれ独自の方法で青少年の安心・安全な利用に向けた取り組みを行っているとはいえ，日本独自の仕組みである従来の枠組みに参加することには消極的であった[10]。EMA認定を取得していなければ，フィルタリングの対象となり，利用ができないことになる[11]。そのため，これらのサービスを利用したいがためにフィルタリングを利用しないことを希望する青少年が多数存在すると言われてきた。

これらの事情により，近年は従来の枠組みの実効性が問われるようになってきていた。以下では，2016年に見られた新たな取り組みについて概観する。

Ⅲ　新たな取り組みに向けた議論

1　総務省タスクフォース

⑴　概　要

総務省は，2016年4月，「ICTサービス安心・安全研究会」のもとに「青少年の安心・安全なインターネット利用環境整備に関するタスクフォース」（中村伊知哉主査。以下「総務省タスクフォース」と言う。）を設置し，①関係者の理解力の向上や普及啓発の重要性に関する事項，②利用者・事業者双方にとって使いやすいフィルタリングの実現に関する事項，③青少年のネット利用環境整備（理解力の向上・フィルタリングの活用）のための体制の整備に関する事項について検討を行った。

2016年7月にまとめられた「青少年の安心・安全なインターネット利用環境整備に関する論点とその解決に向けた方向性」（以下，「方向性」と言う。）[12]では，上記3点の検討項目ごとに，今後の取組みとして関係者に求められる内容が示された。その後，後述のように各所で検討され，それが2016年12月15日に開催された総務省タスクフォースで報告され，承認された。本項ではまず，「方向性」の概要を紹介する。

⑵　関係者の理解力の向上や普及啓発の重要性に関する事項

この事項については，啓発活動のあり方について，まず，各事業者・団体が実施している各種啓発活動については，今後，「量」とともに「質」を重視することを目指すとともに，多様な主体へのアプローチや，関係者間の一層の連携・協働を進めるべきであるとした。そして，こうした観点から，啓発教材や啓発講座等のあり方に関して，事業者や関係団体に対して具体的な取り組みを求めている。

また，同じく啓発について，青少年自身だけではなく，保護者のリテラシー向上に向けた具体的な方策を早急に実施することが極めて重要であるとされた。また，今回の「方向性」では，携帯電話の販売店の役割が認識された点が1つの特徴であるが，啓発との関係でも，「携帯電話の販売店は，保護者や地域住民と直接接する機会を持つなど，幅広い層へのリテラシー向上を図る上で重要な役割をもつと考えられることから，携帯電話事業者及び販売代理店は，販売代理店スタッフに対するフィルタリング利用に関する研修の充実や，地域での啓発活動への積極的な協力・貢献を図るべきである。」とされた。

⑶　利用者・事業者双方にとって使いやすいフィルタリングの実現に関する事項

今回の「方向性」は，フィルタリングの仕組みの変更の検討に踏み込んだ点で，上述のような従来の枠組みを変える重要な意義を有している。すなわち，「設定の複雑化／長時間化や，使い勝手の悪さも，保護者がフィルタリングの設定を回避する理由のひとつとなっているのではないか。こ

10）　もっとも，LINEについては，親会社が外国企業であったものの，運営会社自体は国内に拠点をおいている。また，当初は消極的であったが，2015年にEMA認定も取得している。

11）　ただし，携帯電話事業者の判断により，EMA認定を取得していないサービスであってもフィルタリング対象から外すことも可能であり，例えば，利用者が高校生である場合には本文にあるようなサービスについてそのような対応をとっている例もある。

12）　http://www.soumu.go.jp/main_content/000432425.pdf

の場合，現在のフィルタリングの仕組みの変更を検討すべきではないか。」という問題意識のもと様々な意見が提出され，とりまとめに至った。とりわけ，契約時の説明及び設定の複雑化・長時間化がフィルタリング利用率向上を図る上でのボトルネックとなっているという認識に基づき，スマホ上のOS機能を活用したフィルタリング導入の実現可能性について検討することが適当であるとされた点が重要である。

この点は，従来の枠組みを大きく変えるものである。すなわち，従来はスマホにアプリをインストールしてフィルタリングを設定しており，OSに組み込まれた機能制限は用いられていなかった。iPhoneの場合，フィルタリングを設定するためには，店頭で販売店店員が電源を入れ，アップルIDを取得してApp Storeからフィルタリングアプリをダウンロードしてインストールし設定する必要がある。前段落に記した「契約時の説明及び設定の複雑化・長時間化がフィルタリング利用率向上を図る上でのボトルネックとなっている」との指摘はこうした実情を踏まえたものである。OSの機能制限を用いれば，設定の負担は大幅に小さくなる。

にもかかわらずこれまでこれが用いられてこなかった理由の１つは，OSの機能制限においては，違法有害情報の閲覧を防止すること（コンテント・リスクへの対処）は可能であったが，SNSの利用制限を行うことができなかったことにあると思われる。これは，OSの機能制限のあり方はアメリカ的ないしグローバルな考え方に基づいており，そこでは，SNS上で不適切な出会いがなされることのリスク（コンタクト・リスク）は十分に考慮されていないことによる。これに対して日本では，上述したところからも伺えるように，コンテント・リスク以上に，コンタクト・リスクへの対処が重要視されてきたという経緯がある。

要するに，OSの機能制限の利用にかじを切ることによって，コンタクト・リスクへの対処のあり方について再考する必要性が生じ，後述のような多層的な保護の考え方へとつながっているものと見ることができる。

今の点と関連する部分もあるが，「方向性」では，フィルタリング対象の見直しについても提言がなされ，これも従来の枠組みを変更するものといえる。そこでは，青少年の使用実態とフィルタリング対象に乖離があり，それが利用率の低迷につながっているのであれば，フィルタリング対象の見直しを検討すべきではないかという問題意識のもと，また，上述のOS機能の活用を図ることとされたこととともあわせて，a）青少年の使用実態やグローバルな基準も視野に入れた対象の見直し，b）学齢に応じたフィルタリングのあり方とその具体的な導入方策，c）上記a）b）を進める上での現行の仕組みの見直し等，d）その他機関（行政機関やゲームのレイティングを行う機関等）との連携，といった提案がなされている。

このほか，より使い勝手の良いフィルタリングのサービス・アプリ，青少年の使用実態に合わせたフィルタリングの実現に向けた検討や，各事業者共通で青少年にわかりやすく受け入れられやすいコンセプトや名称の作成の検討などを求めている。

さらに，SIMフリー・MVNO端末におけるフィルタリングの提供についても，携帯電話事業者やMVNO事業者による検討が求められた。

⑷　青少年のネット利用環境整備のための体制の整備に関する事項

この事項については，関係各団体の役割分担を一層明確化した上で，フィルタリングと啓発の役割分担も踏まえ，我が国全体としての効果的な青少年保護のための体制の確立をめざすべきであるとされ，新たな体制整備に向けた関係団体間での具体的な議論を求めた。

また，上記⑵⑶で述べた取り組みを行うスケジュールも示され，啓発活動の見直しや新たなフィルタリングの仕組みの実現については，翌年（2017年）春の運用開始を目標にすべきとした。

「方向性」で求められた事項について，啓発の関係については安心ネットづくり促進協議会（以下，「安心協」と言う。）やマルチメディア振興センターにおいて，フィルタリングの関係についてはフィルタリング促進検討会，電気通信事業者協会（以下，「TCA」と言う。）やEMAなどで検討が行われた。以下ではフィルタリングの関係を中心にその概要を紹介する。

2　フィルタリング利用促進検討会及びTCAでの検討

フィルタリング利用促進検討会（坂元章座長）は，学校・教育委員会関係者，PTA関係者，心理学や法学の研究者，シンクタンク関係者，弁護士が構成員となり，安心協，TCA及びEMAをオブザーバーとして設置され，2016年8月から11月までの4回の会合を通じて「有効な青少年保護施策を実現するにあたって，スマートフォン時代に即した，より使いやすいフィルタリングの実現を含めた今後の在り方について論点を整理するとともに，改善指針を提案することを目的として検討を行った。」。

2016年12月15日に総務省タスクフォースで示された報告書（概要）[13]によれば，利用者調査を踏まえて，既存フィルタリングの問題点や対応策が示された。対応策としては，a）利用者の理解促進のために，フィルタリングの名称やサービス構成について各社のサービス名称やアイコン等を統一することや，b）フィルタリング利用の申込状況について店頭で定量的にモニタリングし，必要に応じて改善を実施できるようにすることが望ましいこと，c）カスタマイズも含むフィルタリングについては改善や啓発の取組みが引き続きなされることが望ましいこと，といった点が指摘された。

a）については，2017年1月25日にTCA及び携帯電話事業者各社からプレスリリースがなされ，サービス名称を「安心フィルター for（キャリア名・ブランド名）」とし，共通アイコンも定めたことが発表されている[14]。また，b）については，販売店ごとのフィルタリング利用率や内訳が明らかになることによって販売方法の検証が可能になることについては意味があると思われる。

これらとは別に，フィルタリング利用促進検討会の報告の中心になったのは，フィルタリングにおける「新モード」である。これは，総務省タスクフォースの「方向性」で示されたOS機能を利用したフィルタリングに対応するものである[15]。

報告書は，「新モード」の意義を次のように説明している。すなわち，フィルタリングを設定していない保護者の多くは，スマホの利便性と安全性の両方を求めているが，それにもかかわらず，フィルタリングを利用していない。この場合，利用者である青少年はフィルタリングが防いできた様々なリスクについて全く保護されない（「ノーガード」）の状態にある。利用者保護と両立する範囲で利便性にも配慮したフィルタリング（「新モード」）を提供することで，「ノーガード」の青少年に対して最低限の保護を提供することは喫緊の課題である，という説明である。

このような認識のもと，「新モード」は，スマホの利便性を犠牲にしたくないために既存のフィルタリングを使用していない青少年に対し，最低限の保護を提供し，全体の安全レベルを高めることを目的とするものであると位置づけられた。

つまり，「新モード」は，既存のフィルタリングに代わるものではなく，既存フィルタリングが原則である点は引き続き維持しつつ，従来であれば既存フィルタリングを拒否していた層が利用するためのものであり，少なくとも「新モード」については全ての青少年が利用する状態に近づけることが目標とされた。

フィルタリング利用促進検討会の報告を受け，携帯電話事業者の団体であるTCAにおいて具体的な取り組みの検討が行われた[16]。その結果，フィルタリングのわかりやすさ向上のため，サービスの名称やアイコンを業界で統一すること，販売時の情報提供（フィルタリング種別，リスク等）の充実や意思確認の強化を実施すること，店頭では原則として従来のフィルタリングを推奨し，利用を拒否する利用者のうち主に高校生には「新モー

13）「フィルタリング利用促進検討会　報告書（概要）」（2016年12月15日総務省タスクフォース提出資料〔http://www.soumu.go.jp/main_content/000454813.pdf〕）。

14）電気通信事業者協会ほか「スマートフォン等のフィルタリングサービスの名称及びアプリアイコンの統一について」（2017年1月25日〔http://www.tca.or.jp/press_release/2017/0125_777.html〕）。

15）iOSについてはOSの機能制限を利用し，アンドロイドについては同等のレベルのフィルタリングを用意する方法が取られるという。

16）電気通信事業者協会「『フィルタリング利用促進検討会』をうけての事業者（TCA）の取り組みについて」（2016年12月15日総務省タスクフォース提出資料〔http://www.soumu.go.jp/main_content/000454814.pdf〕）

ド」を推奨すること，その他総合的なリスク対策，といったものに取り組むこととされた。なお，実際にサービスが開始されるにあたり，「新モード」の名称は「高校生プラス」となった。

3　EMA（モバイルコンテンツ審査・運用監視機構）

既存フィルタリングと「新モード」との大きな違いは，前述のように，SNS をフィルタリング対象にするかどうかという点にあり，後者においては SNS がフィルタリング対象とはなっていない。すなわち，「新モード」においては，日本でこれまで重視されてきたコンタクト・リスクへの対処が手薄になることになる。

もちろん，前述の通り「新モード」は，既存のフィルタリングに取って代わるものではないが，当初の意図に反して「新モード」を選択する青少年が多くなる可能性も排除できない。環境整備法との関係を一言述べれば，同法はフィルタリングの内容には介入しないという立場をとっており[17]，17 条のフィルタリング提供義務との関係では，「新モード」を提供することでもこの義務は充足される。そこで，法的には，どのフィルタリングを選択するか（あるいはどれも選択しないか）は保護者の判断に委ねられることになり，既存フィルタリング優先の原則は，販売方針としてのみ存在することになる。

また，いずれにしても，フィルタリング利用率が低迷している現状に鑑みれば，青少年保護対策をフィルタリングと啓発とに過度に依存することはもともと望ましくなく，総合的な対策が求められることになる。

こうした状況の中，従来の枠組みの中心にあった EMA において新たな取組みが検討されたことは理解できる。EMA も 2016 年 12 月 15 日の総務省タスクフォースにおいて新たな取組みを説明した[18]。EMA の新たな取り組みとは，モニタリング（評価・情報提供）である。EMA は，サービスと利用者ニーズの多様化から EMA 認定制度のカバー範囲が限定的になってきていることを認め，SNS を中心として，青少年に影響の大きいと思われるウェブサイトやアプリを対象に，警察庁をはじめ関係機関からの情報を参考に，中立的な第三者機関としての独自の調査によって評価を実施し，利用状況や機能特性などのサービスの実態について情報提供する仕組みを構築するとしている。具体的には，Apple 社への情報提供によって，同社の運営するアプリマーケット（App Store）におけるアプリのレーティングをより適切なものにする（これによって OS の機能制限がより有効に機能することになる）ことや，青少年被害が急増しているサイトについてプレスリリースを発表して広く注意喚起をするといったことが挙げられている。

「新モード」との関係では，Apple 社や携帯電話事業者に情報提供をすることによって，「新モード」におけるフィルタリングの継続的な補正・改善を支援するとしている。

Ⅳ　検討と今後の課題

「新モード」導入をはじめとする新たな取り組みは，環境整備法のフィルタリング提供義務と EMA 認定を中心とする従来の枠組みの限界を率直に認めた上で，青少年保護の仕組みを立て直そうとするものである。標語的に述べれば，フィルタリング中心主義から多層的な保護へ，とでも言いうるだろうか。

筆者は旧稿においてフィルタリング提供義務と EMA の認定制度を組み合わせた仕組みを絶対視することなく，EMA 非認定サイト・アプリが青少年に利用されることをも十分に想定しつつ，青少年の保護を考えていくことが必要である旨述べ

17）　この趣旨は同法全体から読み取れるほか，同法制定時の参議院内閣委員会での次のような付帯決議が明確である。「政府は，本法の制定に当たり，次の事項について万全を期すべきである。」「四，フィルタリングの基準設定の内容によっては，インターネット利用に際しての表現や通信の自由を制限するおそれがあることを十分に認識し，その開発等に当たっては，事業者及び事業者団体等の自主的な取組を尊重すること。また，事業者等が行う有害情報の判断，フィルタリングの基準設定等に干渉することがないようにすること。」（参議院内閣委員会 2008 年 6 月 10 日）。

18）　モバイルコンテンツ審査・運用監視機構「EMA の新たな取組みに関して～モニタリング（評価・情報提供）～」（2016 年 12 月 15 日総務省タスクフォース提出資料〔http://www.soumu.go.jp/main_content/000454815.pdf〕）。

ていたが[19]，こうした観点からすれば，今回の方向性は評価できるものである。

「新モード」においては，SNSは原則としてフィルタリング対象とはならず，EMA等によって特に危険だと判断されたサイトやアプリに限ってフィルタリング対象となることになる。これは，従来の枠組みからすれば原則と例外の逆転である。コンタクト・リスクを強調する立場からの批判も予想されるが，特に危険なものを排除することによって最低限の保護を広く提供できるので，総合的に見れば有意義であるという評価も可能であろう。

もっとも，過去の経験に鑑みれば，特に危険なサイト，アプリという評価はされておらず，広く利用されているサイト，アプリであっても，利用方法によっては不適切な出会いのために用いられることもある。その意味では，結局のところ情報提供や啓発が重要になる。「新モード」についても，十分な理解を得ておかないと，フィルタリングが設定されていることによる安心感によって逆にリスクが高まるということにもなりかねない。

広く使われているSNSについては，EMA認定がなくても，携帯電話事業者の判断によってフィルタリング対象外とされている場合がこれまでもあったが，「新モード」によって「正式」にフィルタリング対象外となる。つまり，これからは少なくとも高校生程度になれば，フィルタリングを設定していようがいまいが，また，EMA認定の有無にかかわらず，主要なSNSは利用可能となる。

こうした事態はこれまでも実態としては存在したが，今後はこうした実態が正面から認知されることになり，その影響を考えておく必要があろう。この点について，さしあたりいくつか指摘しておきたい。

まず，リテラシーが重要であることは論をまたない。とりわけ，青少年が遭遇する可能性の高いトラブル（いじめ，自己あるいは他人のプライバシーの暴露，詐欺等）については，リテラシーが決定的な重要性をもつだろう。その関係で，リテラシーを身につけるための教育・啓発も非常に重要である。

これに対して，不適切な出会いについては，リテラシーの問題として位置づけるべきかどうかには議論の余地がある。そもそも，こうした問題は多くの青少年にとって自分とは縁遠い世界のことであると考えられがちであり，教育・啓発を行っても効果があるかどうかは疑わしい。従来は，啓発活動において，フィルタリングを設定すべき理由の1つとして不適切な出会いの危険を挙げてきたものと思われるが，多くの青少年や保護者にとってどれほど説得的だったかは疑問である。

そもそも，刑事司法における青少年保護と，モバイル・インターネットにおけるそれとでは文脈の異なるところがある点に注意が必要だろう。すなわち，刑事司法においては，児童は，児童買春罪（児童買春・児童ポルノ規制法4条）や青少年条例の淫行罪の被害者として位置づけられる。それは仮にいわゆる援助交際を積極的に勧誘した結果であっても同様である。このような常識的な意味では被害者とは言い難い者についても，そうでない者と同様に被害者と位置づけることについては，刑事司法上の合理性はあるとしても，モバイル・インターネットにおける青少年保護の文脈でも同様に意味があるのかどうか，問い直す必要があろう。どのような場合であっても一律に被害者だとしてみるのではなく，犯罪に遭遇するプロセスの実態を解明して，それに即した対策を考案する必要があるのではないか。

最後に，新たな取り組みの特徴を多層的な保護に見出すのであれば，関係者間の役割についても新たな考え方が求められる。フィーチャーフォンの時代においては携帯電話事業者がフィルタリングも管理していたことから，携帯電話事業者の役割が大きかった。しかし，スマホ時代に役割の重要性を増す事業者もあるだろう。総務省タスクフォースの「方向性」では携帯電話販売店の役割が強調されたが，これはそうした一例であろう。さらに，EMA認定を中心とする従来の枠組みにおいては，EMA認定サイト・アプリの責任は強調されても，非認定サイト・アプリについてはいわ

19）　拙稿・前掲注3）104-105頁。

ば制度の埒外の存在として周辺化されていた観がある。新たな枠組みではEMA認定の仕組みの重要性が相対化されていることから，今後は非認定サイト・アプリが多層的な保護の一翼を担うべきだという要請が強まることも予想される。また，OS機能の活用が正面から採用されたことから，OS事業者の責任論も出てくるだろう。日本に特徴的な報告書行政[20]がグローバル企業には十分理解されないということがあるのであれば，新たな共同規制の枠組みが求められる可能性もあるのではないか。

20） この語は，曽我部ほか・前掲注3）40頁〔曽我部執筆〕　で用いたものである。

個人情報保護から個人データ保護へ
―民間部門と公的部門の規定統合に向けた検討(1)

産業技術総合研究所
高　木　浩　光
Hiromitsu TAKAGI

Ⅰ　はじめに

個人情報の保護に関する法律（以下「個人情報保護法」と言う。）の平成27年改正では，その検討段階における内閣IT総合戦略本部の「パーソナルデータに関する検討会」での議論を通じ，また，法案が国会提出直前で与党修正に至る経緯と国会での活発な審議を通じて，今改正で達成できなかった課題が明らかになるとともに，改正前の個人情報保護法（以下「平成15年法」と言う。）にいくつもの解決していない論点が残されていることが浮き彫りになった。

達成できなかった課題とは，一つは，いわゆる「端末ID」を識別子として蓄積される個人に関する履歴情報を保護対象とすることが検討されながらも実現しなかったことであり，浮き彫りになった平成15年法の未解決論点とは，個人情報定義における「容易に照合することができ」をどのように解釈し，何をもって非個人情報化がなされたと言えるかがはっきりしないままとなったことが，その代表例である。

こうした点が認識されたためか，改正法の附則12条3項に，施行後3年ごとに必要があるときは所要の措置を講ずるものとするとした検討規定が入り，同条6項には，個人情報の定義と公的部門の保有個人情報の規定について，「集約し，一体的に規定することを含め，個人情報の保護に関する法制の在り方について検討するものとする。」とされた。

これらの論点を残した状況で，行政機関の保有する個人情報の保護に関する法律（以下「行政機関法」と言う。）の平成28年改正が進められ，「容易に照合」と「照合」の違いが依然として明らかにされないまま，「非識別加工情報」の制度が新たに導入されることとなり，さらにこれを地方公共団体の個人情報保護条例にまで展開する動きもあることから，今後さらに混迷を深めることになると懸念される。

本稿シリーズは，個人情報保護法の3年後の見直しを見据え，残された論点の解決案を体系的に整理することを試みる。具体的には，民間部門と公的部門の一体的な規定に向け，「個人情報」と「個人データ」の違いに着目して「個人情報ファイル」に係る規律のみを統一することを目指し，「容易に照合」と「照合」の違いを明らかにする。これにより，今改正で導入される「匿名加工情報」の概念が明確になり，公的部門と地方公共団体で進められる「非識別加工情報」制度の混迷を避けることができ，また，将来の課題として残された「端末ID」を識別子として蓄積される履歴情報を保護対象とするための下地が整うことになると考える。

この整理にあたって重視するのは，行政機関の保有する情報の公開に関する法律（以下「情報公開法」と言う。）との平仄，過去の制定の経緯との整合，国際的な動向との調和である。過去の経緯については，一般財団法人情報法制研究所が内閣法制局に情報公開請求して得た法律案審議録を基に，本稿整理の妥当性の根拠とする。国際的な動向については，EU（欧州連合）の「一般データ保護規

則」の他，英国，スウェーデン，ドイツ等のデータ保護法及びその改正経緯と，米国で一時提案された「消費者プライバシー権利章典法案」と比較する。

以下，本号では，浮き彫りになった論点を列挙して問題の所在を概観し，次号以降で，残された課題と個別の論点について掘り下げていく。

Ⅱ　浮き彫りになった論点

1　個人に関する情報の範囲

今改正の検討が始まる直前の平成 24 年ごろの時点では，法律上の個人情報の定義について誤解が広まっていた。個人情報とは氏名，生年月日，住所等の個人を特定するための情報を言うのであって，それら以外の部分，例えば蓄積された履歴情報の部分は，個人情報に当たらないという誤解である。大手企業のプライバシーポリシーにも，その理解を前提としたことを窺わせる記述が見られた[1)]。これは，法の定義条文の「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」の部分に目を奪われ，「……であって，当該情報に含まれる……により……できるもの」との構文を見落とすことで生じるのであろう。この誤解は，改正法の議論を通じて，平成 29 年現在では相当程度解消されたように見受けられる。大手企業のプライバシーポリシーも誤解のない記述ぶりに改められた。

個人情報が「氏名，生年月日その他の記述等」の部分のみを指すものではないことは，条文から明らかであるが，開示・訂正の求めに応じる義務が規定されていることからも明らかである。もし，個人情報がそれのみを指すならば，開示の求めは，自己の氏名，生年月日，住所等の登録状況を確認するだけの機能となり，訂正の求めも，その誤りを訂正する機能ということになる。法がそのための義務を事業者に課すはずもなく，それに紐づけられた本人に関する様々な属性情報を開示・訂正の対象とするのが法の趣旨であるのは明らかである。

しかし，次に問題となるのは，開示・訂正においてはそうだとしても，第三者への提供においても同様なのかという論点である。提供に際して，氏名等を取り除いた属性情報のみからなるデータを提供するとき，元データから部分的に複製して一時的に作成されるそのようなデータが，当該個人に関する情報と言えるのかという論点である。

情報公開法においても，個人情報相当の情報を不開示情報と規定しており（5 条 1 号），氏名等の部分を墨塗り・被覆等を行なって残りの部分を開示することが行われていることから，個人情報保護法でも同様の処置で非個人情報化でき，提供できるとする誤解も見かける。しかし，これは，同法 6 条（部分開示）で「不開示情報が記録されている部分を容易に区分して除くことができるときは，開示請求者に対し，当該部分を除いた部分につき開示しなければならない。」と別に規定されているからであり，個人情報保護法にそのような趣旨の規定はない。

この 1 号不開示情報は他の号の不開示情報とは異なり，不開示情報の一部分に当たる「当該情報のうち，氏名，生年月日その他の特定の個人を識別することができることとなる記述等の部分」のみ除いて残りは開示せよとするもの（同条 2 項）であり，「当該部分を除いた部分は，同号の情報に含まれないものとみなして，前項の規定を適用する。」と規定しているように，氏名等の部分を除けば 1 号不開示情報に該当しなくなるという前提を置いているわけではない[2)]。したがって，情報公開法とパラレルに「氏名等の部分を除けば個人情報でなくなる」と類推することはできない。加えて，情報公開法 6 条 2 項の部分開示には，「公にしても，個人の権利利益が害されるおそれがないと認められるときは」との条件が付けられ

1）　鈴木正朝・高木浩光・山本一郎『ニッポンの個人情報「個人を特定する情報が個人情報である」と信じているすべての方へ』（翔泳社，2015）

2）　総務省行政管理局編『詳解 情報公開法』（財務省印刷局，2001）87 頁は，この点について，「個人識別情報は，通常，個人を識別させる部分（例えば，氏名）とその他の部分（例えば，当該個人の行動記録）とから成り立っており，その全体が一つの不開示情報を構成するものである。」とし，「このため，第 1 項の規定だけでは，個人識別情報については全体として不開示となることから，（略）個人識別情報についての特例規定を設けたものである。」としている。

ており，氏名等の部分を除けば常に開示してよい情報としているわけでもない。

2　容易照合の提供元基準

氏名等を取り除いたデータを作成する際には，一般的に，氏名等に置き換えて個人別の符号を付す処理が行われる。これを「仮名化」と呼ぶことにする。仮名化に際して，仮名化後のデータと元データとの対応関係を残すために対応表が作成される場合と，そのような対応表を残さない場合とがある。前者を，医学系研究の分野では従来，「連結可能匿名化」と称し，後者を「連結不可能匿名化」と称してきた。このうち，連結可能匿名化されたデータについて，個人情報に該当するかが論点となった。

平成25年に内閣府の規制改革会議の下で行われた「国際先端テスト」においては，当時個人情報保護法を所管していた消費者庁の回答により，提供元で元データとの「対応表」を廃棄することを条件に「当該属性情報は「個人情報」には該当しないこととなる」との見解が示された。これは，つまりは，対応表が存在する限りは連結可能匿名化したデータもその事業者においては個人情報であるということになる。

対応表の存在が個人情報該当性を左右するのは，個人情報保護法の個人情報定義に「（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。）」との括弧書きがあるからであり，これが「容易照合性」と呼ばれ，平成24年の内閣府行政刷新会議の規制・制度改革委員会経済活性化WGにおいて，消費者庁が，「この容易照合性の判断の基準としては，その個人情報を取り扱う事業者，こちらを基準に，その事業者の方が情報を保有や取得をした時点，こういった観点で容易照合性を見ている」と回答していた。

すなわち，前節で論点とした，提供のために一時的に生成されるデータが直ちに個人情報と言えるかについて，仮に言えないのだとしても，この容易照合性の規定があるために，少なくとも対応表がある限りは個人情報に該当するということになる。

消費者庁の回答が，容易照合性の判断の基準はその個人情報を取り扱う事業者を基準とするとしたことは，「提供元基準」と呼ばれるようになった。これに相対するものは「提供先基準」と呼ばれる。岡村[3]は，平成26年の時点で，「提供先にとって識別性がない情報と比べて，提供先にとって個人識別性がある情報のほうが，本人の権利利益を害するおそれが格段に大きくなることは当然である。したがって，第三者提供と個人識別性との関係について，提供先において識別情報か否かを基準とする提供先基準説のほうが，こうした制度趣旨に対して素直な解釈といえよう。ただし，提供先基準説によると，前記法文は「提僕先にとって個人データと認められるもの」と読むことになり，やや不自然であるとの批判もあり得る」としつつ，「現行の保護法23条の解釈においても，プライバシー・名誉権との前記関係を考慮すると，それとかけ離れた解釈をすることはできないから，提供元ではなく提供先を基準に識別性の有無を判断する提供先基準説のほうが妥当であるように思われる。」とした。

ここで注意を要するのは，提供元基準と提供先基準とは二者択一ではない点である。すなわち，提供元基準かつ提供先基準とする制度設計もあり得る。岡村は，提供先で個人識別性があることの方が権利利益侵害の恐れが大きいとの理由で提供先基準を肯定したが，これは提供元基準を否定する理由にはならない。

この論点は，今改正を通じて，政府解釈は提供元基準であることが明確にされ，一定の決着に至った。国会審議において，政府参考人（内閣審議官）から，「日本の場合，これは情報の移転元で容易照合性があるということで解釈が統一されておりまして，そういたしますと，一旦個人情報となりますと，その情報の一部を提供する場合でも，これは大抵の場合，提供元において容易照合性はありますので，個人情報になってしまうという，そういうことはございます。」[4]との答弁があっ

3）岡村久道「パーソナルデータの利活用に関する制度見直しと検討課題（中）」NBL 1020号68頁以下（2014）

4）第189回国会参議院内閣委員会会議録第10号（2015.5.28）

た。

しかし，なぜ提供元基準としているのかその理由は明らかにされていない。個人情報の定義は，国法で最初に規定されたのは，昭和 63 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（以下「昭和 63 年法」と言う。）であり，その時点から「（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。）」との括弧書きがあった。個人情報保護法の定義はこれとほぼ同じである。情報公開請求で開示された昭和 63 年法の法律案審議録を見ると，当初の案（「昭和 62 年 8 月案（第 1 次案）」と書かれている。）では，「（当該記録のみでは特定個人を識別できないが，当該行政機関が保有する他のファイル又は台帳その他のものと照合することにより識別できるものを含む。）」とされていた[5]。この条文から，少なくとも当初は，提供元基準を意図しており，提供先基準を想定していなかったことが読み取られる。

日本法が伝統的に個人情報を提供元基準で定義してきたのだとしても，その実質的な意義，すなわちその狙いと効果が明らかでなければ，不当な規定であり撤廃すべきとの主張も成り立ち得る。提供元基準の実質的意義の解明は残された論点である。

鈴木[6] は，平成 24 年の時点で，「誰が「容易に照合」性の有無を判断するのか，その判断主体が問われる」として，規制事業者基準説，従業者基準説，受領者基準説，一般人基準説，総合判断説に分け，規制事業者基準説で解釈するべきであるとした。その理由を，「行政による事業者規制法という性質を有する個人情報保護法においては，規制対象となる個人情報取扱事業者を主体としてその識別性の有無，容易照合性の有無を判断するべきである」からとした。しかし，確かに判断する主体は規制対象となる事業者自身であることで間違いないが，論点となっているのは，どこでの照合可能性を問うのかである。鈴木は，提供先の受領者で照合ができるか否かは提供元では推測が困難であるとし，「事業者が個人情報ではないと判断したものが，受領者や一般人を基準したところ特定個人を識別できるケースもあり得るのである。規範に直面しようのない状況で法的義務が課せられることは，場合によっては法が不可能を強いることを意味し，営業の自由を不当に侵害するものとして許容できるものではない。」として，民間部門では提供先基準を採用すべきでないとした。その結果として消去法で，定義条文に存在する「容易に照合」は提供元基準で捉えるほかないという理由であった。この見解でも，法がなぜそのような括弧書きを定義に含めたのかは説明できていない。

3　データセットによる容易照合

前節は対応表による照合の論点であったが，次に，対応表を残さない連結不可能匿名化データについて，提供元において元データと「容易に照合することができ」るかが論点となる。

消費者庁は前掲の国際先端テストで，対応表を廃棄すれば個人情報に該当しないこととなるとしたが，そこで示された「週 3 日以上ワインを飲んでいる」か否かという二値の属性情報の場合の例についてそう判断したにすぎない。二値の属性情報の場合，データの人数が十分に多ければ，「飲んでいる」人も「飲んでいない」人も複数人存在することとなるので，「飲んでいる人が何人」という統計量に集計された情報と違わない。消費者庁は，そのような性質がある場合に限って対応表を廃棄すれば非個人情報化できるとしたにすぎないと見ることもできる。

ここで問われたのが，平成 25 年に鉄道会社が

5）この案は，総務庁行政管理局の「行政機関における個人情報の保護に関する研究会意見」（昭和 61 年）において，「個人情報とは，個人に関する情報であって，当該個人を識別できるものをいうが，個人が識別できるとは，情報の内容から，その情報が特定個人のものと識別し得ることをいうとすることが適当であると考えられる。なお，当該情報のみでは特定個人を識別できないが，当該機関が保有する他のファイル又は台帳等と照合することにより識別できるものは含むものとすることが適当であると考えられる。」としていたのに沿ったものと見られる。

6）鈴木正朝「個人情報保護法制とクラウド」岡村久道編『クラウドコンピューティングの法律』109 頁以下（民事法研究会，2012）

IC カードを通じて取得した個人の乗降履歴データを他社に提供した事案における，元データとの容易照合の可否である。当初，鉄道会社は，対応表に相当する鍵付きハッシュ変換の鍵を維持して，複数回に渡り継続して提供することを想定していた様子が窺われるところ，問題が指摘されるようになった後の報道[7]では，「変換方法につきましては定期的に変更しており，長期間にわたって同じ SuicaID 番号が一意の番号に変換されることはありません。」と答えており，対応表を定期的に廃棄する方針を示していた。

対応表を廃棄することに個人の権利利益保護の観点からいかほどの意味があるのか。確かに，繰り返し提供する場面を想定すれば，提供の都度対応表を廃棄しなければ個人情報の提供に当たるということにすれば，個人情報保護法の義務を回避するために対応表を廃棄することになり，結果的に，提供毎のデータ間の本人連結性は途切れることになって，長期に渡る履歴情報の提供が避けられて，個人の権利利益保護の効果があると言える。しかし，長期に渡る履歴情報を蓄積し終えてから一回で全部を提供すれば，対応表を残さないようにできるので，そのような効果は消滅してしまう。

藤村ら[8]は，「数十日分の乗降履歴があれば，ID（または識別番号）によらなくても，「当該情報」と「他の情報」の双方を持つ鉄道事業者にとっては，「当該情報」と「他の情報」に含まれる乗降履歴の一致を確認すれば，「当該情報」と「他の情報」に含まれる氏名を結びつけることができ，特定個人 X の識別に至る」と指摘し，こうしたデータセット自体による照合が，法の容易照合の解釈に含まれるのではないかとの見解を示した。

この考え方に基づくと，医学系研究の分野で用いられてきた連結不可能匿名化が，本当に「不可能」化するものだったかも問われることになる。この分野の「連結不可能匿名化」は，乗降履歴の事案同様に，氏名・連絡先を削除しただけの仮名化をもって連結不可能匿名化とするのが現場の少なくない実態であったが，平成 27 年に文部科学省と厚生労働省から公表された「人を対象とする医学系研究に関する倫理指針ガイダンス」は，「個人の医療等に関する情報は，その情報自体が身体的特徴を表すことがあり，例えば，氏名，生年月日その他の「特定の個人を識別することができることとなる記述等」を機械的にマスキングすることだけでは，特定の個人が識別されることを不可能にしたと言い難い場合がある。」とし，仮名化だけでは真に「不可能」な連結不可能匿名化とは言えない場合があるとした。

また，前掲の岡村も，平成 21 年時点の著書[9]では，「この場合，医師としては発表・報告用の複製物のみをマスキングによって匿名化しつつ，顔写真の原本にはマスキングせずに別途残しておく方法が通常であろう。したがって，当該原本と容易に照合しうる当該医師にとって，むしろ上述の諸事情は連結可能匿名化である場合が一般的であろう。」としており，提供元基準でデータ自体による照合が可能な場合は連結可能匿名化であるとの見解も示していた。

データセットによる照合の考え方は，今改正の改正法案の法律案審議録の中にも見られる。平成 26 年 12 月 1 日付の「個人情報と匿名加工情報（仮称）における容易照合性の考え方について」と題する，内閣官房 IT 総合戦略室が作成して内閣法制局の審査で提示したものと思しき資料は，「鉄道会社が，記名式 IC カードの乗降履歴について……」として具体例を示した上で，「具体例の場合，同社は削除・置換のアルゴリズムを廃棄しているが，氏名等を含むデータセットと新たに作成されたデータセットを比較すると，詳細な内容を有する複数項目が合致する。このような場合，項目を突合させるのみで事業者は特定の個人を識別することが可能である。システム上両データセットは連結していないものの，両データセットは一対一対応が可能な状態で照合によって特定の個

7）浅川直輝「Suica 乗降履歴データの外部提供で問われるプライバシー問題――JR 東日本に聞く」（日経 BP）（2013.7.24），http://itpro.nikkeibp.co.jp/article/NEWS/20130724/493665/

8）藤村明子・間形文彦・鈴木正朝「ビッグデータビジネスにおける個人情報の容易照合性に関する考察」情報ネットワーク・ローレビュー 13 巻 2 号 1 頁以下（2013）

9）岡村久道『個人情報保護法』（商事法務，新訂版 2009）79 頁

人を識別し得る場合については全く知見を有しない者であっても照合によって特定の個人を識別することができ，かつ，両データに対してアクセスし得る人間が複数名存在していることから，「容易照合性」があると言える。」としていた。

しかし，後に，個人情報保護委員会が公表した「個人情報の保護に関する法律についてのガイドライン」（平成 28 年 11 月）では，こうした見解は示されておらず，この解釈が政府解釈として採用されているのかは，はっきりしていない。

論点となるのは，この解釈の実質的な意義である。法律案審議録では，「項目を突合させるのみで事業者は特定の個人を識別することが可能」とあるが，事業者が特定の個人を識別できることに，本人の権利利益保護の観点でどのような効果があるのか。当該事業者は元データを保有しているのだから，元データを見ることで各個人の乗降履歴を把握することは元々できるのであり，元データから切り出された提供用のデータについて当該事業者が特定の個人を識別できること自体には，直接的な効果はないようにも思える。法律案審議録の資料は，法の定義条文への形式的な該当性を述べているにすぎない。

ここでも，前節と同様に，日本法が伝統的に個人情報を提供元基準で定義してきたその実質的意義に立ち戻る必要があろう。

4　容易照合のアクセス制御説

データセットによる照合が，法の定義の「容易に照合することができ」に含まれるのだとしても，次に問題となるのは，元データとそこから切り出す提供用データが，別のデータベースシステムで管理され，アクセス制御により両方にアクセスできる社員が存在しない状態で管理されれば，「容易に照合することができ」は否定されるのかという点である。

前掲の乗降履歴の事案では，鉄道会社は，報道で問題が指摘された翌週に発表した資料[10]で，「情報ビジネスセンターでは，個人を特定できないデータを利用しています」「情報ビジネスセンターと業務セクションとは厳格に分離※しています。」「※組織，作業環境，スタッフ（アクセス権限），システム」との文言の下，2 つのデータベースシステム間にファイアウォールを置いている図を示していた。元データとそこから切り出したデータとが分離して管理されていれば，法の「容易に照合することができ」が否定されると考えられていた様子が窺える。

これは，経済産業省の「「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」等に関する Q&A」の問番号 14（以下「Q14」と言う。）に，かつて記載されていた問答を拠り所にしたものと思われる。2007 年 3 月版の Q14 では，質問文として，「事業者の取扱部門ごとにデータベースがあり，他の取扱部門のデータベースへのアクセスが，規定上・運用上厳格に禁止されている場合，「容易に照合することができ」（法 2 条 1 項）るといえますか。」を立てた上で，回答として「他の取扱部門のデータベースへのアクセスが規定上・運用上厳格に禁止されている場合であっても，双方の取扱部門を統括すべき立場の者等が双方のデータベースにアクセス可能な場合は，当該事業者にとって「容易に照合することができ」る状態にあると考えられます。ただし，経営者，データベースのシステム担当者などを含め社内の誰もが規定上・運用上，双方のデータベースへのアクセスを厳格に禁止されている状態であれば，「容易に照合することができ」るとはいえないものと考えられます。」と掲載していた。すなわち，実際にアクセスさえできない状況であれば「容易に照合することができ」ないとする解釈であり，これを「アクセス制御説」と呼ぶことにする。

この Q14 は，同 Q&A の平成 26 年 12 月の改正で，質問文の方が修正されて，「事業者の各取扱部門が独自に取得した個人情報[11]を取扱部門ごとに設置されているデータベースにそれぞれ別々に保管している場合において，ある取扱部門

10）東日本旅客鉄道株式会社，Suica に関するデータの社外への提供について，https://www.jreast.co.jp/press/2013/20130716.pdf（2013.7.25）

11）ここは，個人情報に該当するかを問題としているので，「各取扱部門が独自に取得した」情報は個人情報に限定せずに質問を構成するべきところであろう。

のデータベースと他の取扱部門のデータベースへのアクセスが，規程上・運用上厳格に禁止されているときには，「容易に照合することができ」（略）ないといえますか。」に修正された。

つまり，元々のQ14の趣旨は，同一事業者内で別々の事業で独立して扱っているデータについて，それらの間の照合を問題とする必要があるかという趣旨で書かれたものだったのが，作文が不十分だったために，拡大解釈され，ある事業で生成されるデータを複製して分離すれば，容易に照合できないことにできるとの誤解が生じ，独自の非個人情報化を自称する潜脱論法として利用されてしまったということであろう。

宇賀[12]は，「容易に照合することができ」の解釈について，「本項における「容易に」の要件をいかに解するかは解釈に委ねられることになるが，他の事業者に通常の業務では行っていない特別な照会をし，当該他の事業者において，相当な調査をして初めて回答が可能になるような場合，内部組織間でもシステムの差異のため技術的に照合が困難な場合，照合のため特別のソフトを購入してインストールする必要がある場合には，「容易に」の要件を満たさないであろう。」としていた。これはアクセス制御説に近い立場をとっていたものと見られるが，平成28年の改訂版[13]で，このうちの「内部組織間でもシステムの差異のため技術的に照合が困難な場合」の部分を削除している。

この問題は，一見，Q14の修正で決着したようでもあるが，逆に，「社内の誰もが規定上・運用上，双方のデータベースへのアクセスを厳格に禁止」という管理体制を敷かない限り，容易に照合できることになってしまうことに疑問が残る。宇賀の修正も，「システムの差異のため技術的に照合が困難な場合」を取り消しながら，「照合のため特別のソフトを購入してインストールする必要がある場合」を残すなど，依然として技術的に実際に照合する行為が容易にできるかを問題としている。Q14の修正は，質問の前提を変更した（誤解ないように直した）だけであるから，鉄道会社の事案のようなケースについて，「社内の誰もが規定上・運用上，双方のデータベースへのアクセスを厳格に禁止」という管理体制を敷けば「容易に照合することができ」ないと解釈してよいかについて，否定しているわけでもない。

前掲の鈴木は，照合できる者の存否によって個人情報該当性を変えることを「従業者基準説」と呼び，「内部の従業者（自然人）の行為を基礎に据える点で不法行為法における使用者責任（民法715条）と類似した発想にあるが，裁判と異なり，主務大臣が報告の徴収（法32条）によって調査し得るところには限界があり，従業者を基準とする解釈では立証の困難に直面することが多く，また迅速な意思決定もできない。あくまでも個人情報取扱事業者を単位として判断すべきであり，内部の従業者の具体的な行為等は，個人情報取扱事業者の義務を尽くしているか否かの判断を行ううえでの材料の一つとして採用することで足りよう。」と批判した。しかし，この理由では，厳格なアクセス禁止の管理体制の有無で個人情報該当性が左右されるとする説を否定できていない。

そもそも，実際に照合できる従業員や役員が存在するか否かによって個人情報該当性を変えることの実質的意義はあるのか。照合する行為が行われて初めて個人の権利利益侵害を発生し得るという前提を置いているのだとすれば，それは妥当な前提なのか。この点も前節と同様，日本法が昭和63年法から提供元基準で個人情報を定義してきた趣旨に立ち戻る必要がある。

前掲の「人を対象とする医学系研究に関する倫理指針ガイダンス」（平成27年）にも，アクセス制御説を否定する記述がある。「医療機関を有する法人等が研究機関として研究を実施する場合において，診療録番号と患者を結びつける情報にアクセス制限を行っていても，当該診療情報は「連結不可能匿名化」されたものとはいえない。」とし，「特定の個人を識別することができる者が限定的であるか，また，当該研究機関内の誰がアクセスすることができるかによらず，「連結可能匿名化」された情報である。例えば，同一法人が管轄するA病院とB研究所において，A病院で取

12）宇賀克也『個人情報保護法の逐条解説』（有斐閣，第4版2013）29頁

13）宇賀克也『個人情報保護法の逐条解説』（有斐閣，第5版2016）40頁

得された試料・情報を連結可能匿名化して，B 研究所に提供する場合には，B 研究所で対応表を保管していなくても，当該法人（研究機関）として対応表を保有することに変わりなく，個人情報等として適正に取り扱う必要がある。」としている。この考え方は，同ガイダンスの前身である「「疫学研究に関する倫理指針」についての Q&A」（平成 19 年）の時点から，「同一法人内で対応表を保有している部署と研究担当部署が分かれている場合であっても，対応表を有している場合に該当します。」として，同様の見解が示されていた。しかし，これらも，なぜそのような解釈をとるのかについての説明がない。

そして，個人情報保護委員会の「個人情報の保護に関する法律についてのガイドライン」（平成 28 年 11 月）は，アクセス制御説に触れず，「「他の情報と容易に照合することができ」るとは，事業者の実態に即して個々の事例ごとに判断されるべきであるが，通常の業務における一般的な方法で，他の情報と容易に照合することができる状態をいい，例えば，他の事業者への照会を要する場合等であって照合が困難な状態は，一般に，容易に照合することができない状態であると解される。」としか説明しなかった。「例えば」で示された例は，「できない」場合の極端な例の一つにすぎず，それ以外は「できる」ということを意味しないから，結局，「通常の業務における一般的な方法」としか言っておらず，「実態に即して個々の事例ごとに判断される」というのでは，解釈基準を示していない状況にあると言えよう。

藤村ら[14] は，このガイドラインの案に対してかけられた意見公募手続で，寄せられたに意見に個人情報保護委員会がどう答えたのかを分析して，「アクセス制御で容易照合性が失われるとの考え方は重ねて否定されているものと考えてよいであろう。」「経産省の旧ガイドライン Q14 に依拠したアクセス制御説の採用が GL 通則編パブコメにて明確に否定された点は評価したい。」と結論づけた。

5　非個人情報化の要件

次に，情報は加工すること（他の情報に変換すること）が可能であるから，個人情報は加工すれば非個人情報化できるのかが論点となる。情報公開法では，部分開示のために一部を除くことは許されるが，情報の内容を他の情報に変換することは法の趣旨からして許されないのに対し，個人情報保護法ではそれが許され得る。

前掲の「週 3 日以上ワインを飲んでいる」か否かという二値の属性情報の場合は，仮名化するだけで非個人情報化できるとされる一方，前掲の鉄道会社の乗降履歴のように詳細な内容の属性情報を持つ場合には，仮名化では依然として個人情報のままであるとする見解がある。では，その境界となる条件はいかなるものか。

個人情報を非個人情報化して利活用するにはどうしたらよいかは，経済産業省の研究会で繰り返し検討されていた。平成 20 年の「パーソナル情報研究会」報告書「個人と連結可能な情報の保護と利用のために」では，「個人情報（個人データ）の一部を構成する以上，当該部分のみを第三者に提供する場合でも個人データの第三者提供に該当し，本人の同意を要するとも解し得る一方で，当該部分自体は個人情報（個人データ）に該当しないので，当該部分を第三者に提供する場合は本人の同意を要しないとも解し得る。」と初歩的な検討をして，「さらに十分な検討を要する」と結んでいた。平成 23 年には，「経済産業分野における匿名情報を安全に利用するための手引（案）～情報の加工・管理・第三者提供の考え方～」との文書が作成されたものの，正式版の公表に至らなかった。この手引（案）では，「k- 匿名化」を中心に検討され，「l- 多様性」や「t- 近接性」などの用語も盛り込まれたものの，具体的な基準を示すには至らなかった。

この論点は，個人情報保護法の平成 27 年改正で「匿名加工情報」の概念が導入されることにより，解決されることになった。しかし，匿名加工情報の作成方法の基準を定めることになっていた個人情報保護法施行規則（平成 28 年 10 月 5 日個人情

14）藤村明子・間形文彦・亀石久美子・板倉陽一郎「個人情報の保護に関する法律施行規則及び同ガイドラインを踏まえた容易照合性概念に関する考察」情報処理学会研究報告 2017-EIP-75 巻 20 号 1 頁（2017）

報保護委員会規則第3号）は，規則19条で1号から5号までの基準を示したものの，4号及び5号は抽象的な概念を示したにすぎず，ガイドラインにおいても例示がなされたものの基準は示されなかった。

ここで問題となるのが，匿名加工情報と個人情報該当性の関係である。改正法は「匿名加工情報ならば法23条の規定にかかわらず第三者に提供できる」とする規定を置かなかったので，本人同意なく提供できるのは改正前と変わらず非個人情報に限られ，匿名加工情報は非個人情報であるから提供できるとされる。ここで，「匿名加工情報は非個人情報である」がどういう意味なのかが論点となる。「非個人情報でない限り匿名加工情報となり得ない」の意味（A説）なのか，「匿名加工情報に加工すれば非個人情報ということになる」の意味（B説）なのか[15]である。B説では，改正法36条5項及び38条の識別行為の禁止規定の存在によって，個人情報定義の「照合することができ」が否定され，非個人情報となるという立場である。

B説を採用すると，仮名化しただけで常に匿名加工情報になることにできてしまう。元データと容易に照合できる性質の情報で構成されるデータセットであっても，照合が禁止されているから法の言う「照合することができ」に当たらないというのである。

この説は，改正法の国会審議の初期段階で，政府参考人（内閣審議官）から「匿名加工情報は，そもそも，作成に用いた個人情報と照合することが禁止されておりますので，容易照合性は認められないと私どもは解釈しております。」[16]と答弁したことからその存在が窺われた。

これには批判がある。筆者も早い段階からシンポジウムの席で，「事業者内に元の生データがあるのに，それとの照合を禁止して何の意味があるのか」[17]，「「してはならない」との規定によって「できるもの」該当性が否定されるというのは，法技術論的にありえない」[18]と批判した。藤村ら[19]も，鉄道会社の乗降履歴の事案が問題となったのは「対象となるデータの状態[20]」が問題となっているのであって，行為自体が禁止されていても，対象となるデータ同士が依然として突合できる状態にあることに変化はない。」とし，仮にそのような解釈を許せば「何らの加工を施す必要がなくなる」と批判する。

藤村らは，B説が「初期の国会で発言されたものに過ぎない」として，立案担当者らの本来の意図は他にあるのではないかとするが，B説の考え方は，改正法案の法律案審議録の中に見られる。前掲の「個人情報と匿名加工情報（仮称）における容易照合性の考え方について」には，「このように法的担保によって個人情報等との照合が禁止されているのであるから，容易に照合可能な状態にあるとは言えず，解釈上個人情報に該当しない。」との記述がある。その前段部分には，「容易照合性の判断は，同事業者の規模，技術的措置，組織的措置等その他具体的な事情を元に総合的に判断する法的評価である。」との記述があり，前節で論点としたアクセス制御説に依拠しているように見える。

国会審議の初期段階からB説には批判の声が挙がったためか，その後の内閣委員会での審議ではこのような説明は登場しなかった。前掲注14の藤村らは，個人情報保護委員会の「個人情報の保護に関する法律についてのガイドライン」案に対する意見公募手続（平成28年11月）で委員会がどう答えたかを分析して，「識別行為禁止義務（法36条5項）によって容易照合性が失われるとの論法も採用されていない」「匿名加工情報にお

15）高木浩光「匿名加工情報の制度概要と匿名加工基準の規則案」ビジネス法務16巻11号17頁以下（2016）

16）第189回国会衆議院予算委員会第一分科会会議録第1号（2015.3.10）

17）高木浩光「個人情報保護改正案の問題点（中立的観点から）」情報法制研究会第1回シンポジウム（2015.3.28）

18）高木浩光「改正個人情報保護法に残された課題と今後の展望」情報法制研究会第2回シンポジウム（2015.6.28）

19）藤村明子・間形文彦・亀石久美子・板倉陽一郎「匿名加工情報及び個人情報における容易照合性概念の整合性に関する考察」情報処理学会研究報告2016-EIP-71巻3号1頁以下（2016）

20）「データの状態」との表現では，アクセス制御の管理体制を含むようにもとられかねないので，ここは「データの性質」と言うべきところであろう。

ける容易照合性，具体的には，匿名加工情報と，元となった個人情報の間の容易照合性の問題について，個人情報保護委員会は，述べていないのではなく，積極的に，見解を述べることを避けているのではないか」とした[21]。

立案段階ではどのように考えられていたのか。前掲の法律案審議録のその前段には，「措置を講じた事業者は，匿名加工情報の元となった個人情報を引き続き保持し，かつ措置方法を有していることが通常である。また，システム上両データの連結性が認められる，両データへアクセス可能な人間が複数存在する等の事情が存在するとすれば，匿名加工情報と元となった個人情報は容易に照合することができる状態にあると言える。」との記述がある。これは，改正法 36 条 5 項で，匿名加工情報を作成した事業者自身に対して，作成した匿名加工情報についての再識別行為を禁ずる理由を説明したものである。これは，どんなに十分な匿名加工を施しても，作成した事業者においては元データとその加工方法の情報が存在するため，容易に照合することができてしまうという前提を置いているように見える。たしかに，そのように前提を置くと，法的禁止によって非個人情報化できるとでもしない限り，匿名加工情報は存在し得ないことになってしまうので，その事情は理解できる。

しかし，これは「容易に照合することができ」の解釈を拡大しすぎているのではないか。そもそも，匿名加工情報とは，その定義から，特定の個人を識別することができないように加工したものであるから，元データとのデータセットによる照合ができない性質の情報に加工することを要件としている[22] はずである[23]。そうであれば，再識別行為を禁ずるまでもなく，匿名加工情報の作成者において，元データとの容易照合性は問題とならないはずだったのではないか。

結局これは，「他の情報と容易に照合することができ」をどのように解釈するかの問題である。筆者は，データセットによる照合のように，データの性質を問うものとして解釈すべきと考えるが，改正法の立案段階では，「他の情報」へのアクセスが容易か，技術的に容易かといった，手段の容易さを問うものと解釈したのではないか。手段さえ容易であれば，データの性質がいかに照合できないものにされていようとも，1 つの情報でも照合の可能性が僅かでもあれば，容易照合性が否定されないとする考えに至ったのではないか。

この点についても，前節までと同様，日本法が伝統的に個人情報を提供元基準で定義してきたその実質的意義に立ち戻って解釈を再確認する必要があろう。

6 「容易に照合」と「照合」の違い

個人情報保護法の平成 27 年改正を受け，行政機関法が平成 28 年改正に至るが，ここで「他の情報と容易に照合することができ」と「他の情報と照合することができ」の違いが論点となるはずだった。民間部門（個人情報保護法）では前者で個人情報が定義されているのに対し，公的部門（行政機関法及び独立行政法人等の保有する個人情報の保護に関する法律）では後者で定義されているからである。しかし，検討段階で総務省行政管理局の「行政機関等が保有するパーソナルデータに関する研究会」は，この違いが何を意味するのかを解明し

21） 個人情報保護委員会は，後に公表した同ガイドラインに対する Q&A（平成 29 年 2 月）でもこのことに触れなかったが，「個人情報保護委員会事務局レポート　匿名加工情報　パーソナルデータの利活用促進と消費者の信頼性確保の両立に向けて」（平成 29 年 2 月）では，この点について初めて触れ，「匿名加工情報は（略）個人情報に係る本人を識別することを禁止する等の制度的な担保がなされていることから，作成の元となった個人情報を通常の業務における一般的な方法で照合することができる状態にある（すなわち容易照合性がある）とはいえず，個人情報に該当しないとされるものである。」と記した。

22） 改正法 2 条 9 項の匿名加工情報の定義は，「特定の個人を識別することができないように」の部分が，「特定の個人を識別することができる（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を含む）ことがないように」といったように，個人情報定義の裏返しの条文とする案もあり得たと考えられるところ，法の条文にこのような括弧書きはないものの，これは省略されているものと解釈することもできよう。

23） 実際，施行規則 19 条 5 号は，「個人情報に含まれる記述等と当該個人情報を含む個人情報データベース等を構成する他の個人情報に含まれる記述等との差異その他の当該個人情報データベース等の性質を勘案し，その結果を踏まえて適切な措置を講ずること」として，そのようなことを求めている。

なかった。両者に何らかの違いがあって，民間部門で容易照合できないことを理由に個人情報とならないものが，公的部門では照合により個人情報となる場合が存在し得るということだけが確認された。

その結果，提出された改正法案の「非識別加工情報」（民間部門の匿名加工情報に相当するもの）の定義は，「次の各号に掲げる個人情報（他の情報と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（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除く。）を除く。以下この項において同じ。）の区分に応じて……」というように，二重の括弧書きで「(……もの（……ものを除く。）を除く。)」とする複雑怪奇な条文となった。これの意図するところは，非識別加工情報へと加工する元とする情報の範囲を，民間部門における個人情報に該当するものに限るためであり，行政機関法における個人情報から，容易には照合できないが照合はできるものを除くとしたものである。論理上，そのように規定すれば少なくとも誤りはないことは確かであるが，どのような趣旨でその区別がつけられているのかは不明なままとなった。

行政管理局の研究会では，構成員から，「そうすると，基本法の場合は，結局この真ん中のB情報の部分がブラックボックスといいますか，よく分からない状態になるわけです。（略）結局，行個法単体で見た場合，あるいは基本法単体で見た場合は，それぞれ一貫性のあるシステムになっているのかもしれませんが，両方を照らし合わせてみると，基本法の方でよく分からない領域が出てきてしまうのではないかと思います。これはやや気持ち悪く，後世の法律家が見たら，あのときの研究会は何をやっておったのかと批判するのではないかという気もしなくもありません。もしB情報の部分があまり現実的にないというのであれば，基本法において容易照合性という要件を取ってしまえば，非常にクリアな議論ができたと思います。この点は本研究会で言っても仕方ありませんが。」[24] との発言があった。

この改正法案の国会審議では，「この容易があることによってどんな違いが生じるのか，できればその容易照合性に当たらないが照合性に当たる分かりやすい具体例がありましたら，この辺も含めまして，総務省，御答弁いただけますでしょうか。」[25] との質問があったが，政府参考人（総務省行政管理局長）の答弁では，「例えば通常の業務で一般的な方法でやっているような照合，これは容易な照合というふうに当たると考えられます。ただ，その反面，容易でない照合というのは，通常業務でやっていない方法で，例えば日常的な照会ではなくて特別に，逐一関係の機関，関係のところに照会をかける，そうした上で入手できるというようなものは容易でないというふうに通常解されているところでございます。」と，解釈の違いとして一般論が答えられたのみで，具体例の提示はなかった。

この違いは，行政機関法が昭和63年法から平成15年に全部改正される経緯から推察することができる。昭和63年法では「容易に照合」で定義されていたものが，全部改正時に「容易に」が削除されたからである。

行政管理局の「解説 行政機関等個人情報保護法」には，「参考5 照合の容易性を要件としないことについて」として，「旧法第2条第2号では，「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」としており，他の情報との照合について容易性を要件としていた（基本法第2条第1項も同じ。）が，本法では，行政機関における個人情報の取扱いについてより厳格に規律する観点から，照合の容易性を要件としていない。」という簡単な説明しか書かれておらず，あたかも照合の容易さの程度の違いであるかのように読まれてしまうが，全部改正の検討段階の「行政機関等個人情報保護法制研究会」の報告書「行政機関等の保有する個人情報の保護に関する法制の充実強化について」（平成13年）では，「現行の行政機関法では，識別容易性を要件としているが，行政機関が保有する個人情

24）「行政機関等が保有するパーソナルデータに関する研究会」第15回議事要旨9頁の下井康史構成員の発言より。

25）第190回国会参議院総務委員会会議録第14号（2016.5.19）

報については，情報公開法と同様に，その識別性の判断に特段の容易性を求めないこととする。」と，情報公開法に合わせる趣旨であると書かれている。

このことは，この改正の法律案審議録にさらに明確に書かれている。平成 14 年 1 月 23 日・24 日付「内閣法制局第三部長説明資料」13 頁の，「2 改正法案の考え方（照合の容易性の要件を削除することについて）」の節に，この改正が，保護の対象を「個人情報ファイル」から「保有個人情報」まで拡大することに伴う変更であること，「情報公開法では，（略）照合容易性を要件としていない。」として，「開示・不開示の判断に当たっての両法制の運用の統一性を図る観点からは，個人情報の範囲を同様にしておくことが望ましい」と，その理由を説明している。

そうすると，情報公開法ではどのような趣旨で「容易に」のない「照合」による 1 号不開示情報の規定を設けたのか。これが解明すべき論点となる。

7　小　括

以上のように，「容易に照合することができ」の解釈は，個人情報を非個人情報化して利活用する上で，非個人情報化されたと言える要件として根幹をなす概念であるにも関わらず，依然として曖昧な部分が残されており，また，公的部門における「照合することができ」の解釈との違いも明らかにされていない。

これらの解釈について，筆者は，昭和 63 年法が，「個人情報ファイル」を構成する「個人情報」の定義として「容易に照合することができ」を用いたこと，また，その当初案が「他のファイル又は台帳その他のものと照合」とされていたことに着目すれば，情報公開法で導入された「照合することができ」とは質的に別々の概念（容易さの程度ではなく）であり，この前提に基づけば全体が矛盾なく説明される解釈を確立できると考える。これについて，本稿シリーズ⑵の第Ⅳ章「個人情報ファイル概念と容易照合性」で，詳しく論ずる。

（続）

特別地方公共団体の個人情報保護の現状と課題

情報セキュリティ大学院大学情報セキュリティ研究科教授
湯　淺　墾　道
YUASA Harumichi

Ⅰ　はじめに

日本の個人情報保護法制は，個人情報の取扱いに関する義務等を定めるいわゆる事業者規制の部分については，個人情報を収集・保有する者の法的地位に応じて，民間事業者，国の行政機関，独立行政法人ならびに地方公共団体及び地方独立行政法人について区別し，それぞれ異なる法律を制定・適用するという構造となっている。このため，個人情報の保護に関する法律（以下，「個人情報保護法」と略。），行政機関の保有する個人情報の保護に関する法律（以下，「行政機関個人情報保護法」と略。），及び独立行政法人等の保有する個人情報の保護に関する法律に加え，個人情報保護条例が各地方公共団体によって制定されている。このような方式は，「民間部門の個人情報保護について，個別分野ごとに規制し一般法を持たない米国型のセクトラル方式を否定し，民間部門の個人情報保護の一般法を定めた点では欧州型」という点で，「欧州型と米国型の折衷的性格」と指摘されてきた[1)]。

地方自治体及び地方独立行政法人について，個人情報保護法は，第５条で個人情報の保護にあたって地方公共団体（自治体）の特性に応じ個人情報の適正な取扱いを確保するために必要な施策を制定し実施する責務を定め，第 11 条で自治体の保有する個人情報の保護について適正な取扱いが確保されるように必要な措置を講ずる努力義務を定めると共に，その設立に係わる地方独立行政法人についてもその保有する個人情報の保護について適正な取扱いが確保されるように必要な措置を講ずる努力義務を規定している。また第 12 条では区域内の事業者等への支援，第 13 条では苦情の処理のあっせん等を規定しており，地方公共団体はこれを実施する努力義務を負う。

ところで，地方公共団体における個人情報保護における「盲点」となっているのは，広域連合や一部事務組合，財産区等の特別地方公共団体の扱いである。

特別地方公共団体の存在は，住民からは見えにくいので，特別地方公共団体の事務処理，特に個人情報の収集や利活用について住民が意識する機会は，決して多くはないと思われる。しかし近年，広域連合や一部事務組合は広く活用されるようになっている。たとえば広域連合についてみると，1998 月 1 日現在では 14 団体，2004 年 4 月 1 日現在では 82 団体が設置されているに過ぎなかったが，2013 年 4 月 1 日現在では 115 団体が設置されている[2)]。深刻な財政状況や少子高齢化を背景とする行財政改革の動きと事務処理の集約化，市町村合併後の円滑な権限委譲や広域的ニーズへの柔軟な対応の必要性といった事情を背景として，平成の大合併によって市町村合併が進み普通地方公共団体の数は減少したにもかかわらず，広域連

1)　宇賀克也『個人情報保護法の逐条解説（第２版）』（有斐閣，2005 年）22 頁。

2)　村上博「広域連合の展開」香川法学 21 巻 3・4 号（2002 年）101-158 頁。

合の数は逆に増加しているのである。また特別地方公共団体が処理する事務は，介護保険，後期高齢者医療，産業廃棄物・ごみ処理，消防・救急，公立病院，公立小中学校，大学，火葬場，地方税滞納処理，障害者福祉，公営競技（競馬，競輪，競艇），職員の退職金の支払い事務等，きわめて広範囲にわたっている。中には，特別地方公共団体立による病院等の医療機関のように慎重な取扱いを必要とする性質の個人情報を取り扱う場合も多く，消防・救急を処理する特別地方公共団体も救急車の搬送記録のような個人情報を多く取り扱っている。介護保険，後期高齢者医療，障害者福祉等の領域においても同様である。

これらの事務において取り扱われている個人情報が外部に漏洩すると，本人に経済的な損失やいわれのない差別等の被害が発生する恐れがあり，特別地方公共団体においても，都道府県や市町村のような普通地方公共団体と同様に個人情報を適正に取扱うことが要求されることは，言うを俟たない。

ところが，地方公共団体の個人情報保護についての諸問題に関する先行研究の中で，特別地方公共団体について触れたものは希である。

本稿では，特別地方公共団体の個人情報保護の実態について明らかにすると同時に，理論的な問題についての検討を行うこととしたい。

Ⅱ　特別地方公共団体における条例制定の状況

1　神奈川県内の特別地方公共団体における条例制定の状況

多くの個人情報保護法の概説書や解説書等は，地方公共団体は個人情報保護条例の制定が求められるとする点で一致する。夏井高人教授はさらに一歩踏み込み，地方公共団体には条例制定義務があるとする。夏井教授は，「各地方公共団体は，その守備範囲の中にある個人情報について適正な取り扱いを実現するための条例を制定すべき義務がある。したがって，合理的な理由なく，相当の期間を経過したにもかかわらず必要な条例が何ら制定されない場合には，立法不作為の違法の一種として，当該地方公共団体について何らかの法的責任が発生し得る」としている。また，自治体が小規模であったり財政状況が厳しく予算が不足したりしていることに起因して個人情報保護条例が未制定のままになっている場合についても，「当該地方公共団体の予算や立法能力の不足などが『合理的な理由』にならないことは当然のことである。」と指摘する[3)]。地方公共団体は個人情報保護条例の制定が求められるという点については，学説はほぼ一致しているといってよい。

また総務省も，2003 年 6 月 16 日付で各都道府県，政令指定市に対して事務連絡「地方公共団体における個人情報保護対策について」[4)] を送付し，個人情報保護条例未制定団体には制定を求めると同時に，既に制定している自治体には見直しを行うよう求めている。

しかし，特別地方公共団体における個人情報保護条例制定の状況は，必ずしも明らかになっていない。

総務省は，2005 年度末までにすべての都道府県・市区町村が条例を制定したとしている。しかし，個人情報保護条例の現状について調査した項目を含む総務省の「地方自治情報管理概要」[5)] は都道府県，市町村だけを対象としているため，特別地方公共団体における個人情報保護条例の制定状況は不明である。また総務省は，すべての都道府県及び市区町村が個人情報保護条例を制定するまでの間，毎年，条例の制定状況に関する一覧を毎年公開していた。消費者庁も「地方公共団体において制定されている個人情報保護条例」を公開し，全国の地方公共団体の個人情報保護条例にリンクを設定していた（現在は，個人情報保護委員会のウェブページに移動されている[6)]）。しかし，これらに

3）　夏井高人「個人情報保護条例」判例自治 266 号（2005 年）117 頁。

4）　平成 15 年 6 月 16 日総行情第 91 号各都道府県知事・各政令指定都市長あて総務省政策統括官通知。http://www.soumu.go.jp/c-gyousei/daityo/pdf/030710_1_9.pdf

5）　総務省「地方自治情報管理概要（平成 24 年 4 月 1 日現在）」http://www.soumu.go.jp/menu_news/s-news/01gyosei07_02000010.html

6）　http://www.ppc.go.jp/personal/legal/local/

おいては普通地方公共団体のみが対象となっており，特別地方公共団体の個人情報保護条例の制定状況は明らかになっていなかった。

このため筆者は，特別地方公共団体における個人情報保護条例の制定状況につき，神奈川県内の特別地方公共団体の調査を試みた。**表1**は，神奈川県の資料や各地方公共団体のホームページ上の情報等に基づき，神奈川県内の広域連合及び一部事務組合における個人情報保護条例の制定状況をとりまとめたものである。個人情報保護条例の制定状況については「地方公共団体における個人情報保護対策等制度化調」に記載されている2012年4月1日現在のものを記載している。

調査の時点で，共有林野の管理処分を行う一部事務組合は9団体あったが，すべての団体で個人情報保護条例が未制定であった。斎場の管理運営等を行っている広域大和斎場組合は，独自に職員採用も行っており独立性の高い特別地方公共団体であるが，個人情報保護条例をもたず，大和斎場条例の中にも個人情報取扱に関する規定が存在し

表1　神奈川県内の広域連合，一部事務組合における個人情報保護条例の制定状況

名　称	共同処理事務の概要	個人情報保護条例名称
小田原市外二ヶ市町組合	共有林野の管理処分	条例なし
南足柄市外五ケ市町組合	共有林野の管理処分	条例なし
南足柄市外二ケ市町組合	共有林野の管理処分	条例なし
南足柄市外二ケ町組合	共有林野の管理処分	条例なし
南足柄市・山北町・開成町一部事務組合	共有林野の管理処分	条例なし
松田町外三ヶ町組合	共有林野の管理処分	条例なし
松田町外二ヶ町組合	共有林野の管理処分	条例なし
箱根町外二カ市組合	共有林野の管理処分	条例なし
南足柄市外四ケ市町組合	共有林野の管理処分	条例なし
金目川水害予防組合	山林の管理処分	条例なし
秦野市伊勢原市環境衛生組合	塵芥の終末処理施設，葬祭施設の設置管理	条例なし
高座清掃施設組合	塵芥・し尿処理施設，老人福祉センター及び屋内温水プールの設置管理	高座清掃施設組合個人情報保護条例
足柄上衛生組合	し尿の処理，休日急患診療所の設置管理，医療機関等の相互の連携推進，介護認定審査事務	条例なし
湯河原町真鶴町衛生組合	塵芥処理	条例なし
足柄東部清掃組合	塵芥処理	条例なし
足柄西部清掃組合	塵芥処理	条例なし
広域大和斎場組合	大和斎場の設置，管理及び運営	条例なし
神奈川県市町村職員退職手当組合	退職手当の支給事務	神奈川県市町村職員退職手当組合個人情報保護条例
神奈川県内広域水道企業団	水道用水供給事業	神奈川県内広域水道企業団個人情報保護条例
神奈川県競輪組合	自転車競走の施行	条例なし
神奈川県川崎競馬組合	地方競馬の開催	神奈川県川崎競馬組合個人情報保護条例
厚木愛甲環境施設組合	一般廃棄物処理施設の設置	厚木愛甲環境施設組合個人情報保護条例
神奈川県後期高齢者医療広域連合	後期高齢者医療事務	神奈川県後期高齢者医療広域連合個人情報保護条例
神奈川県町村情報システム共同事業組合	町村情報ネットワーク・共同利用型情報システムサービスの整備，管理及び運営	条例なし

ない。同条例によれば，斎場を利用するには管理者の許可を得なければならず，同斎場ホームページでダウンロードすることができる「大和斎場施設使用申込確認書」に死亡者名，申請者の氏名，住所，宗派等の欄があるので，これらの情報を収集・利用しているとみられるが，宗派のようなセンシティブな個人情報を取り扱っているにもかかわらず，条例の規定を欠く状態となっている。足柄上衛生組合は，神奈川県足柄上郡開成町に休日急患診療所を設置・運営し，夜間や休日など医療機関の診療時間外での急病に対処するための外来診療を行っている団体である。休日急患診療にも健康保険が適用されるため，患者の持参する健康保険証，後期高齢者医療被保険者証などから個人情報を収集すると共に，診療に際してカルテ等も作成していると思われる。しかし，これらの個人情報保護の取扱に関する条例が制定されていないという状況にある。

このように，特別地方公共団体は，個人情報を収集し，利活用しているにもかかわらず，個人情報保護に関する条例を制定していないものが少なくないのが現状である。

しかし，特別地方公共団体の個人情報保護について，特に条例を定めなくても現状で特に苦情がないという声を聞くことがあるが，それは，特別地方公共団体の存在や事務が住民によって認知されていないということにすぎないであろう。後述の内部利用とみなすことができる場合を除いて，特別地方公共団体には構成団体の個人情報保護条例を直接適用しえないので，個人情報保護法にいう地方公共団体から除外すると，その個人情報の適正な取扱いを確保すべき住民が存在しているのに個人情報の取扱いを規制する法制度が存在しない空白部分を生み出すことになる。

2　条例内容比較研究と特別地方公共団体

各地の地方公共団体によって制定された個人情報保護条例の条文を実際に収集し，内容を比較検討する研究領域でも，特別地方公共団体の条例はほとんど研究対象とされていない。

個人情報保護条例の条文比較の先駆的研究としては，秋吉健次氏による一連の著作がある[7)]。『条文比較による個人情報保護条例集』，『新編個人情報保護条例集』では，各地の条例を，前文・目的，定義，実施機関その他の責務，適用除外・他の制度との調整，個人情報取扱事務登録等，収集・保有の制限，利用及び提供の制限，自己情報の開示の各項目別に整序し，その傾向を分析して比較を試みている。

筆者は，2007年に福岡県内の市町村における個人情報保護条例の比較検討を試みた[8)]。福岡県内では，福岡県春日市が1979年に個人情報保護条例を制定し[9)]，全国の自治体に先駆けてマニュアル情報や民間事業者も条例の適用対象とした先進的なものであったことで知られている反面で，福岡県内では個人情報保護条例を制定していない地方公共団体も存在したからである。その結果，他の都道府県に比べて未制定団体が多く，区域内の事業者等への支援について支援にとどまらず独自に区域内の民間事業者への規制に踏み込んでいる条例があることを明らかにしたが，特別地方公共団体が視野に入っていなかったのは，反省点である。

上原哲太郎教授らは，全国の都道府県及び政令指定都市の個人情報保護条例の内容比較を行っている[10)]。その結果，個人情報の定義にはやはり

---

7)　秋吉健次『条文比較による個人情報保護条例集　上-1』，『条文比較による個人情報保護条例集　上-2』，『条文比較による個人情報保護条例集　下』（いずれも信山社，2000年），秋吉健次『新編個人情報保護条例集（1）』，『新編個人情報保護条例集（2）』，『新編個人情報保護条例集（3）』，『新編個人情報保護条例集（4）』，『新編個人情報保護条例集（5）』（いずれも信山社，2004年）。これらの著作では，地方公共団体の電子計算機組織と他の組織の電子計算機組織との結合を禁止している条文を持つ個人情報保護条例が，都道府県及び住民基本台帳法の改正，介護保険制度導入等に伴って，地方公共団体の電子計算機組織と他の組織の電子計算機組織との結合を禁止している条文を持つ個人情報保護条例が改正を余儀なくされたこと，地方独立行政法人制度の導入によって当該法人の役職員を地方公務員に対する適用条文と同様に取り扱うように改正したこと等が指摘されている。

8)　湯淺墾道「福岡県内の市町村における個人情報の保護に関する条例の現状と課題」九州国際大学法学論集13巻3号（2007年3月）61頁以下。

9)　春日市の条例制定の経緯については，春日市個人情報保護審議会専門研究会編『知る権利・知られたくない権利―春日市情報二条例の回顧と展望』（信山社，1996年）を参照。その後，2006年に条例は全部改正されている。

相違があると共に，都道府県や政令指定都市は比較的に規模が大きいため法令に基づく場合の例外規定や実施機関の裁量，審議会の機能等について，国からの法定受託義務を遂行する上で支障にならないように注意深く整備されている一方で，実施機関自身に関してはかなり大きな裁量を認める規定が目に付くとしている[11)]。

これらの研究において特別地方公共団体が射程に入っていない理由の一つに，後述するように特別地方公共団体の中には個人情報保護条例を持っていないものが少なくなく，制定していたとしても例規集をウェブページで公開している特別地方公共団体が少ないため，条文収集が困難であるという事情が挙げられよう。

Ⅲ　個人情報保護法制における特別地方公共団体の地位

1　個人情報保護法と地方公共団体

個人情報保護法では個人情報の適正な取扱を確保する責務を負う主体として，「地方公共団体」と規定しており，個人情報保護法の中には特に都道府県や市町村に関して規定する条文は存在しない。しかし，個人情報保護法にいう地方公共団体が普通地方公共団体だけに限定されるのか，それとも特別地方公共団体も含まれるのかについては，法は明文を欠く。また個人情報の保護に関する法律施行令にも，それに関する規定は存在しない。なお特別区については地方自治法上，市とほぼ同一の位置づけとなっている（地方自治法第281条の2第2項，第283条）ので，ここでは普通地方公共団体と同視しうるであろう。

そもそも特別地方公共団体における個人情報保護に関しての検討が不十分な状況にあるので，特別地方公共団体が個人情報保護法上の地方公共団体からは除外されるかどうかについて，特に通説のようなものは存在しないといってよい。

一般に，地方公共団体が成り立つためには，地域的・空間的要素（一定の地域を画した区画），人的構成要素（一定の地域内に住所を有する住民をもって地方公共団体の構成員とすること），法制度的構成要素（法律に基づき団体に法人格が与えられ，事務を処理する権能が付与されること）が必要である。普通地方公共団体が上記の3つの要素を備え，存立目的も一般的な公共の利益を図ることであるのに対して，特別地方公共団体は特殊・例外的な特別の目的と権能だけを有している。

このため，特別地方公共団体が個人情報保護法上の地方公共団体からは除外されるかにつき，理論的には肯定説と否定説が考えられる。前述したように個人情報保護条例をもたない特別地方公共団体が多いことや，総務省の調査においても都道府県と市区町村だけが対象となっていることからは，特別地方公共団体は個人情報保護法上の地方公共団体には含まれないことを肯定する考えが実務的には暗黙の了解として存在するようにも思われる。地方公共団体は個人情報保護条例の制定が求められるとするのが通説であるにもかかわらず，特別地方公共団体の中には個人情報保護条例を持たないものが少なくないことにも，特別地方公共団体を個人情報保護法上の地方公共団体から除外することへの実務上の暗黙の合意が投影されていると言わざるを得ないであろう。

特別地方公共団体が個人情報保護法の地方公共団体から除外されることを肯定する論拠を求めるとすれば，日本国憲法第92条等によって地方自治を保障されている地方公共団体とは最高裁判決[12)]以来，一般に普通地方公共団体を指すものとされていることが最大のものとなろう。

また，物理的に固有の区域が存在しないことも，根拠となり得る。個人情報保護法第5条は「地方公共団体は，この法律の趣旨にのっとり，その地方公共団体の区域の特性に応じて，個人情報の適正な取扱いを確保するために必要な施策を策定し，及びこれを実施する責務を有する。」と規定しているが，ここでいう区域とは憲法上の地方自治権を行使しうる物理的に固有の区域であるとすれば，特別地方公共団体にはそのような「区域」が存在しないのであるから，個人情報保護法上の地方公

10）伊藤新・上原哲太郎「各都道府県及び政令指定都市の個人情報保護条例の比較」電子情報通信学会技術研究報告114巻116号213頁以下（2014年）。

11）伊藤・上原，前注10）。

12）最大判昭和38・3・27刑集17巻2号121頁，判例時報330号7頁，判例タイムズ142号187頁。

共団体には該当しないと解釈する余地がある。

組合については，地方自治法第 292 条が「地方公共団体の組合については，法律又はこれに基づく政令に特別の定めがあるものを除くほか，都道府県の加入するものにあつては都道府県に関する規定，市及び特別区の加入するもので都道府県の加入しないものにあつては市に関する規定，その他のものにあつては町村に関する規定を準用する」として，普通地方公共団体に関する規定の準用を規定していることも，一定の根拠となっていると考えられる。その一例は，特定個人情報の取扱いについて「一部事務組合又は広域連合と構成地方公共団体との間の特定個人情報の授受について（通知）」[13] が公権的解釈として発出されていることである。本通知においては，「一部事務組合等の設立により，共同処理させる事務に係る構成地方公共団体内の部署が廃止される一方で，制度を規定する法令が一部事務組合等に直接適用されることから，一部事務組合等は構成地方公共団体の一部署に成り代わり，個別法令の規定に基づき事務を行うものであり，構成地方公共団体が保有している個人情報についても『同一地方公共団体内の内部利用』とみなして必要な限度で利用することができる」とされている。すなわち一部事務組合は，構成地方公共団体になりかわり個人情報を取り扱うものであるから，構成地方公共団体が保有している個人情報の利用は同一地方公共団体の内部利用とみなすとするものである。そうであるとすれば，個人情報の利用にあたっては，当該地方公共団体の個人情報保護条例の規定を適用すれば足りる，ということになろう。

また，広域連合や一部事務組合は，普通地方公共団体の区域の一部または複数団体の区域に，「事務の一部を共同処理する」（地方自治法第 284 条 2 項）ために設けられるものであるから，その区域の普通地方公共団体の条例を適用すれば足りるという考え方もあり得る。しかし特別地方公共団体はその構成団体から独立した存在であり，職員の身分の取扱いについても相互に独立するものとされている。たとえば特別地方公共団体が解散した場合には，その職員の地位が構成団体へ当然に承継されると解すことはできないとされる[14]。したがって，地方自治法 11 章 3 節に定められている協議会の設置（第 252 条の 2），機関等の共同設置（第 252 条の 7），事務委託（第 252 条の 14）等の普通地方公共団体相互間の協力とは異なり，特別地方公共団体には構成団体の条例が直接適用されるわけではないから，特別地方公共団体に構成団体の個人情報保護条例を適用することはできない。あくまでも実務上，構成団体の条例を準用するにとどまる。

他方で，特別地方公共団体を個人情報保護法上の地方公共団体から除外することを否定する論拠としては，特別地方公共団体も公法人としての性質を有する独立した地方公共団体であるという一般的な理由に加えて，特別地方公共団体が個人情報保護法にいう地方公共団体に含まれないとすればその保有する個人情報の取扱について適用される法規範が不明となること[15] が大きな論拠となろう。

前述したように「一部事務組合又は広域連合と構成地方公共団体との間の特定個人情報の授受について（通知）」は構成地方公共団体が保有している個人情報の利用は同一地方公共団体の内部利用とみなすとしているが，これは財産区等の特別地方公共団体には適用されない。また広域連合や一部事務組合にあっても，独自に収集している個人情報については構成地方公共団体の条例の適用は受けないので，条例を制定しない場合には独自収集分についての法制度を欠く状態となってしまう。特別地方公共団体は実際に多くの個人情報を保有して利用し，その処理する事務の性質にもよって

13） 平成 27 年 2 月 13 日府番第 27 号，総行住第 14 号。

14） 秋田地判平成 23 年 3 月 11 日（LEX/DB 文献番号 25501538），仙台高判秋田支部平成 25 年 7 月 21 日労働判例ジャーナル 19 号 11 頁。

15） 新保史生教授は，社会保障・税に関わる番号制度及び国民 ID 制度の個人情報保護の仕組みに関する事項を検討するため設けられた情報保護評価サブワーキンググループでは，「広域連合など特別地方公共団体の一部については条例を制定していない団体もございます。つまり，個人情報保護制度の空白部分がこの部分に現在存在するわけであります」と指摘している。「情報保護評価サブワーキンググループ（第 5 回）議事録」（2012 年）29 頁。http://www.cas.go.jp/jp/seisaku/jouhouwg/hyoka/dai5/gijiroku.pdf

はセンシティブな個人情報も保有しているところから当然に個人情報の適正な取扱いの確保が要請されるにもかかわらず，その取扱いについて規制する定める条例を欠くとすれば，なぜ特別地方公共団体だけが個人情報の保護に関する法制度の枠外に置かれるのかという合理的な理由が問われることになる。

実態としての住民がいないということに関して，「特別地方公共団体の住民概念については，特別の場合を除き従来あまり明確ではなかった」[16]のは事実である。しかし，特別地方公共団体には「区域内の住民」が存在しないということはできないと思われる。というのも，地方自治法では，普通地方公共団体の存立目的が一般的な公共の利益を図ることであるのに対して，特別地方公共団体は特殊・例外的な特別の目的と権能だけを有しているという相違があるだけで，普通・特別の区分を問わずに，地方公共団体に「住民」福祉の増進に努める義務を課しているからである（第2条第15項）。広域連合は，区域内に住所を有する住民の存在を前提として，広域連合の議員及び長の選挙について規定されているとされる[17]。区域内に住所を有する住民の存在を前提として，広域連合の長及び議会議員の選挙及び直接請求の規定が存在する。財産区の場合は，一部の区域とその区域内の全ての住民を構成要素とする財産区議会を設け，選挙を行うことができるとしている。

地方自治法第292条の組合に関する準用規定については，「都道府県の加入するものにあつては都道府県に関する規定，市及び特別区の加入するもので都道府県の加入しないものにあつては市に関する規定，その他のものにあつては町村に関する規定を準用する」としているものの，個人情報保護法は都道府県や市町村という区別自体を行っていない。また，特別地方公共団体における個人情報の取扱について「法律又はこれに基づく政令に特別の定め」は特に存在しない。個人情報保護法が都道府県や市町村という区別自体を行っていないことからみても，第292条を，組合は都道府県や市町村に対して求められる事項を準用すれば足りるので個人情報保護法にいう地方公共団体から除外されるという根拠とするのは，無理があるように思われる。

Ⅳ　特別地方公共団体における個人情報に対する法規制の空白

1　財産区と個人情報保護

財産区は，「財産又は公の施設の管理」だけを行う特別な地方公共団体である。保有する財産には，山林，原野，田畑，用水路，墓地等がある。地方自治法第296条の5は「財産区は，その財産又は公の施設の管理及び処分又は廃止については，その住民の福祉を増進する（中略）ように努めなければならない。」と定めており，財産区も形式上，「住民」を有する。財産区は特別地方公共団体として独自の法人格を有しており，財産の主体であるとともにその管理処分も財産区の行為であって，当該行為に係る法律効果も財産区に帰属するので，財産区を当然に当該財産区のある市町村の個人情報保護条例に規定する実施機関とみなすことはできない。

財産区の中には，実際に個人情報を収集・保有して利用しているとみられるものが存在する。たとえば，林野や土地を別荘用に貸し付けている財産区では，当然，貸し付ける相手方の個人情報を収集しているであろう。

しかし，財産区が個人情報の適正な取扱いを確保するため，個人情報保護条例を定めようとしても，財産区は自ら条例を制定する権能がないと解されている。財産区は固有の執行機関を持たないためである。財産区の予算は市町村の予算に分別して計上され，その事務は財産区のある市町村又は特別区の長その他の執行機関及び議会が，財産区の執行機関及び議決機関として処理することになっている。このため，個人情報を保有しているにもかかわらず，適用すべき条例が存在しないという空白地帯を生むことになってしまう。

このため，財産区に関しては，財産区自体には条例制定義務はないと解し，それに代わる方策を模索する必要がある。この点で，地方自治法では

16）松本英昭『新版逐条地方自治法　第6次改訂版』（学陽書房，2011年）131頁。

17）松本，前注，131-132頁。

必要がある場合には財産区固有の議会もしくは総会または財産区管理会を設けることができるとしており（第 295 条，第 296 条の 2），都道府県知事は必要があると認められるときは財産区のある市町村や特別区に条例を制定させることができるとしている（第 295 条）。また都道府県知事は，財産区議会設置条例の改廃を財産区議会に提案してその議決を得ることができると解されている。これらの規定を参酌すると，財産区の個人情報保護については，当該財産区のある市町村や特別区が財産区の個人情報保護に関する条例を制定するか，当該財産区のある市町村や特別区の個人情報保護条例の中に財産区に関する条文を規定することで対応することができると思われる。

2　独立地方行政法人

普通地方公共団体だけではなく，特別地方公共団体も地方独立行政法人を設立することが可能である（地方独立行政法人法第 7 条）。実際に，現時点で特別地方公共団体が設立した法人として，函館圏公立大学広域連合が設立した公立大学法人公立はこだて未来大学と，北部広域市町村圏事務組合が設立した公立大学法人名桜大学という 2 法人が存在する。

このような地方独立行政法人について，その個人情報の適正な取扱いが確保されるように必要な措置を講ずる努力義務を負っているのは，設立者である特別地方公共団体である。ところが，地方独立行政法人を設立する特別地方公共団体で個人情報保護条例が制定されていない場合には，当該地方独立行政法人が保有する個人情報についてはどのような取扱いが行われることになるのであろうか。

この場合に，一部事務組合や広域連合は，普通地方公共団体の事務を共同で処理するために設けられるものであるので，組合や広域連合を構成する都道府県，市区町村の個人情報保護条例を準用して個人情報の保護を図るということは不可能ではない。たとえばたとえばＡ市，Ｂ市及びＣ市が特別地方公共団体を構成し，当該団体が地方独立行政法人を設立したとき，Ｅ地方独立行政法人の保有する個人情報のうち，Ａ市の住民の分についてはＡ市条例，Ｂ市の住民の分についてはＢ市条例，Ｃ市の住民の分についてはＣ市条例に基づいて取り扱うということは，全く不可能というわけではない。ただし，それはあくまでも準用にとどまる。実際には，これらの構成団体間において個人情報保護条例の規定間の相違がある場合も想定される（一例を挙げれば，個人情報の保護の対象を生存する個人に限定するか，死者も含めるかについては，各地方公共団体の条例によって異なる）。しかし，一の地方独立行政法人の保有する個人情報について一人一人の住民ごとに取扱いを変えるということは，きわめて事務が煩雑となるので，実務上の運用は困難であろう。また，Ａ市，Ｂ市及びＣ市の住民以外の個人の個人情報の取扱にはどの条例を準用するかという問題も発生する。

したがって，地方独立行政法人を設立する特別地方公共団体が個人情報保護条例を制定していない場合，当該地方独立行政法人が保有する個人情報についてどのような取扱いが行われるのかは，住民等からみると全く不明ということになりかねない。

Ⅴ　おわりに

特別地方公共団体の個人情報保護については，現状で特に問題がないとか，住民からの苦情がないという声を聞くことがある。しかし，それは特別地方公共団体の存在自体が住民によって認知されていないということの裏返しでもあろう。

住民からみれば，転入・転出等の手続や住民税の支払いといった具体的な場面で，特別地方公共団体の存在を意識する機会がない。広域連合の議会の議員は組織する団体の住民による選挙，または議会による選挙によって選出されるが（地方自治法第 291 条の 5），実態としては後者によっているので，選挙という機会で広域連合を認知することもない。住民は，自らが特別地方公共団体の住民であり自らの個人情報が特別地方公共団体によって保有され利活用されている，ということを実感する機会に乏しいのである。

一方，多くの特別地方公共団体の事務処理は，構成団体の側からみると，他の普通地方公共団体相互間の協力とほとんど変わらないのも実情であろう。あえて特別地方公共団体という形式を取る

のは，広域連合や一部事務組合の場合は規約を設けることが地方自治法で義務づけ，特に財政負担について規約で明確に定めることとなっているので，通常の普通地方公共団体相互間の協力よりも強い紐帯が担保されるという面にあると思われる。これに対して，通常の地方公共団体相互間の協力という形態を取ると，費用負担や離脱に関し，地方公共団体相互間で紛争が発生する場合もあり[18]，それを防止するためには特別地方公共団体を設置するほうが望ましいようである。

しかし近年では，関西広域連合のように，従来の事務の共同処理という概念をこえて，事実上普通地方公共団体と同様の機能を持つ広域自治体としての姿を模索する特別地方公共団体も現れている。また，人口減少に伴う地方自治体の窓口サービス低下を防ぐことを目的として，市区町村に対して，窓口業務を専門に行う地方独立行政法人の新設を認める方針であることが報じられるなど[19]，地方公共団体における事務処理の手法はますます多様化・共同化し，各普通地方公共団体による単独処理以外の方法による処理が増えることが予想される。

このような状況の下では，普通地方公共団体による単独処理以外の事務処理における個人情報の適正な取扱いを確保することは，喫緊の課題である。そのための試金石として，個人情報保護法制における普通地方公共団体以外の団体の地位や，その個人情報の保護のあり方については，再検討を迫られているといえよう。

※　本稿は，湯淺墾道「特別地方公共団体の個人情報保護」『日本セキュリティ・マネジメント学会誌』28巻2号（2014年）3-10頁及び「特別地方公共団体の個人情報保護」第64回情報処理学会電子化知的財産・社会基盤研究会（2013年5月15日・情報セキュリティ大学院大学）発表論文を大幅に加筆修正したものである。本稿の責は筆者にあるが，多くの方々から特別地方公共団体の実務や運営等について有益なご助言・ご示唆をいただいたことに感謝したい。

18）　たとえば三浦半島ごみ処理広域化計画をめぐり，離脱した葉山町に横須賀市と三浦市が損害賠償請求を行ったという事例がある。横浜地判平成23年12月8日判例時報2156号91頁，東京高判平成24年12月19日，最決平成25年12月10日。

19）『読売新聞』2017年1月29日。

座談会「情報法制の可能性について―AIをめぐる動向を中心に―」

九州大学大学院経済学研究院教授（当時。2017年4月より中央大学総合政策学部教授）　実積寿也
東京大学大学院工学系研究科准教授　鳥海不二夫
（司会）　東京大学大学院法学政治学研究科教授　宍戸常寿

宍戸　常寿

1　はじめに

宍戸：『情報法制研究』創刊号の企画として，今回は，実積さん，鳥海さんと私で座談会をさせていただきます。まず簡単な読者向けの自己紹介として，情報政策との関わりを中心に，実積さんからお願いいたします。

実積：九州大学の実積です。経済学部で通信政策を中心に教えていまして，最近は，ネットワーク中立性という問題に興味を持っています。文系人間なもので技術的な話は正直門外漢なのですが，経済活動の観点から妥当な政策形成を情報通信分野で実現することに貢献していければと思っています。

宍戸：ありがとうございます。次に，鳥海さんからお願いいたします。

鳥海：東京大学の鳥海です。私は完全に理系側の人間でして，計算社会科学と呼ばれているコンピューターサイエンスと社会学を結び付ける研究をメーンでやっています。たとえば，未成年者の安心安全なネットワーク利用に向けたコミュニティサイトのデータ分析や未成年者のネットワーク利用におけるリスク管理といった研究を情報法制研究所理事の江口清貴さんと一緒にやっていたりします。また，AI関係の活動としては，人工知能学会の編集委員をやっております。

宍戸：ありがとうございます。最後に私ですけれども，東京大学で，法律，特に憲法と情報法を担当しています。表現の自由と通信の秘密，プライバシーの保護が，それぞれ憲法の基本価値としてあり，その具体化という観点から情報法に関わっています。基本的には，総務省関係の研究会とか，事業者・民間団体に有識者として呼んでいただいて，耳学問をしています。

情報法制学会では，このように，法律，経済，ICTの技術に関わる研究者，事業者がそれぞれの知見を持ち寄って，情報法制の健全な発展に資することを目的にしていますが，今回はAIをめぐる動向を中心に議論したいと思います。

実積 寿也

2　AI研究の現状

宍戸：そこでまずは現在のAI研究の状況について，鳥海さんから，話題提供をお願いします。

鳥海：はい，分かりました。現在のAI研究の現状について簡単にお話しします。今は第3次人工知能ブームと呼ばれています。その前の第2次というのが30年ぐらい前ですかね，第5世代コンピューティングとかをやっていた時期なんですけが，そのころ人工知能がいったんブームになり，人工知能あまり使えないじゃないかということで冬の時代と呼ばれるのが何年か続きました。そして今，ディープラーニングあるいは深層学習と呼ばれるものが使えるぞということが分かってきて，3回目の人工知能のブームになっています。その中で，AIがいろいろ問題を起こすんじゃないかという危惧があり，こういった情報法制に関係するような話が出てきてるんじゃないかなと思っています。

そもそも，この人工知能って何だ？というのが，技術者や研究者と，そうでない人たちの間でかなり乖離がある気がするんですね。どうも皆さん，自分のイメージするAIで全て語ってしまうので，それは結構問題かなと思っています。

人工知能と呼ばれるものには大きく2種類あって，1つはただの技術であり，今までの技術の延長上にあるものです。そして，もう1つはドラえもんや鉄腕アトムといった夢のAIです。この夢のAIと今の技術との間には，ものすごい乖離があり，実は今の技術が発展していってもドラえもんはできないだろうというのが，人工知能研究者の意見なんですね。

にもかかわらず，人工知能の問題というと，ドラえもん的なものができたときにどうしよう？といった議論がされるんですね。そうすると，10年後の世界の話をしてるのに，突然300年後の世界の話を混ぜてきていることになってしまう。なので，その辺を整理すると，いろいろな議論がうまくできるようになるんじゃないでしょうか。

夢のAIと現在のAIは，「強いAI」と「弱いAI」と呼ばれ，区別されています。これは別に，殴り合って強い弱いではありません。

強いAIというのは「意識を持っているAI」という定義になります。人工知能自身が自分で意識を持って活動する自律型になって，人間の手を完全に離れて活動する。まさにドラえもんとか鉄腕アトムなどが強いAIになります。

一方，弱いAIというのは，人間が知的に作業していることを賢く代替する技術です。たとえば車の運転をするAIは明らかに意識を持っていません。あるいは，囲碁で世界チャンピオンを破ったAlphaGo（アルファ碁）がありますが，これも人間よりも賢いんですが「囲碁ができたから，次は将棋を指そう」という意思は持ってないわけですね。そのため，AlphaGoも弱いAIです。

この，強いAIなのか，弱いAIなのかということを混同すると議論がうまくいかなくなります。今現在できるのは弱いAIだけです。強いAIは人工知能研究者の中でも実現への道は遠いと考えられています。ですので，自律型のAIというのは当分出ないといえるでしょう。

3　意識とプログラミング

実積：「強いAI」と「弱いAI」の区別の基準となる「意識」とはどういうものとして考えているんですか？

鳥海：いい質問ですね。それはかなり定義が難しく，全然解決していない問題です。だから，まだそこの，意識とは何か，何ができたら強いAIになるのかということも分からないぐらいのレベルです。

実積：ルンバは，たぶん弱いAIという話だと思うんですけど。物にぶつかると避ける方向を機械自身が決めているという意味では，意識があるよ

うにも見えますが。

鳥海：でも，あれはプログラミングですからね。

実積：意識とプログラミングは違うってことなんですね。

鳥海：まあそうですね。そこの話は，ほんと難しいんですよ。人間は意識を持っています。じゃあ，イヌは意識を持ってるか。たぶんイヌは持ってるような気がする。すると，セミは意識を持っているのか。セミって持ってるんですかね？セミが土から出てきて蛹になるという行動は考えているわけではなく，DNAにプログラミングされているだけですよね。同じように，赤ちゃんが生まれてきてすぐ泣くのは，泣こうと思って泣いてるわけじゃないから，あれは意識じゃなくて，もうプログラミングであるというように考えることもできるわけですね。そういう意味では，うちの1歳の息子は意識を持ってるのか。最近なんか持ちだした気がするんですけど。

実積：そうすると，「意識がある」と評価されるためには，「人間並み」という基準に合格する必要があるという意味ですか？

鳥海：人間並みというと，サルは意識持ってないことになっちゃうじゃないですか。イヌもそうですけど。

宍戸：今の話は非常に重要だと思うんですけれども，たとえば自動走行で，よく議論されるトロッコ問題も，基本的にはプログラミングの問題であって，意識の問題ではないということですか。

鳥海：トロッコ問題に関しては，意識を持ったところで人間が解決できていない問題なので，AIに解決させるべき問題ではないと思います。哲学の話なので，人間がまず解決してから，プログラミングすればよいのではないでしょうか。

宍戸：そうすると，意識も，かなりの部分哲学問題ではないでしょうか。本当に意識があるのかは，哲学で独我論的な立場に立てば分からないわけですよ。私から見ると，鳥海さんや実積さんが意識主体なのか分からない。

鳥海：哲学的ゾンビの話ですね。

宍戸：そうです。私がこれは意識がある存在だと思うから，人間，あるいは同じような意識を持った生命体として扱うわけですね。同じことが実は人工知能にもいえるのではないか，と文系的には

鳥 海　不二夫

思う。だんだん人間と挙動が同じようになってきて，厳密には分からないけれども，一定程度了解可能な形で，行動の選択肢を選んでいるらしいという存在が，人間とあまり変わらないレベルであれば，もうすでに意識があると人間が思って，そのように扱うことはできるんじゃないか。そうすると意識は，技術的あるいは科学的な水準でなくて，いわば相対的にというか，社会の受容性の問題ではないかという気がするんですが，AI研究者としてはどう思われますか。

鳥海：まさにそのとおりだと思います。だから，そこはかなり難しい問題で，どこまでいったら強いAIなのか議論というのは，実は先ほども言いましたけど，全く解決してない問題なんですね。だから，クラゲに意識があるのかを定義できない限り，AIに意識があるのかは定義できない。

たとえばドラえもんも，内部機構的にはたぶんパラメーターがあって，プログラミングされていて，ディープラーニングを使ってるかは分かんないですけど，神経系ネットワークがあって，ちゃんと解析すればすべての行動が説明できるかもしれない。ただ，それは人間の脳も同じですよね。だから，ある程度いくと，そこから先はもう哲学的な問題にしかならないんですね。

ただ，現在のAIはどうかというと，やはり意識というには程遠いですよね。たとえばクラゲが意識を持っているとはちょっと思い難い。クラゲは意識を持っているという人もたまにいるので，インフルエンザウイルスだとどうか考えてみると，さすがにちょっと厳しい。あれは機械的に構造を変えていくだけなので，意識的にやってるわけで

はないですよね。それと同じように，グレーゾーンがあるにせよ，今は意識がない状態だというふうにいえるだろう。

実積：意識のあり・なしは明確な閾値があって峻別できるものではなくて，中間的な状況があるということですね。

鳥海：今のところ濃淡ですね。閾値がないので。ここから先はさすがにあるってみんな認めるけど，ここから下はさすがにないって認めるだろう，そういう話です。

実積：チューリングテストを通ったら人工知能として認めるという考え方は，いまでもあるんですか。

鳥海：数年前にチューリングテストを合格したっていう AI が初めて出ました。

実積：たとえば「りんな」はチューリングテストに合格するレベルなんでしょうか？

鳥海：あれはたぶんチューリングテストの大会に参加していないのではないでしょうか。ちなみにチューリングテストに合格した AI は「ウクライナ人の 6 歳の少年です」っていう設定でやってる。それで人間かどうか区別がつかなかったということらしいです。

実積：それは意識ある AI なんですか。

鳥海：意識はないですよ。だから弱い AI だと思います。

実積：強い AI と弱い AI を区別するチューリングテストみたいなものはありますか。

鳥海：少なくとも私が知る限りはないですね。要は前の段階なんで。人間っぽく見せることすらできてないわけですから。

実積：でも，先ほどの話だと，息子さんが 1 歳のときは意識なかったけど，今意識出てきたっていうことは，鳥海さんの中で，意識の有無を決める閾値を持っているわけですよね。

鳥海：そうですね。ただ，それは前提条件として，この物体は人間であるというのが分かってますからね（笑）。

4　強い AI と弱い AI の区別

宍戸：制度側から見ると，強い AI と弱い AI を区別することによって，たとえば規制なり何なり税法上の取扱いなり，商品サービスとしての格の違いなり，何か意味があると分かるんですけれども，技術の研究者の側から見たときに，強い AI と弱い AI を区別する実益は何ですか。

鳥海：いや，実益はおそらくない。何しろ夢の物語の話をしているので。「新幹線」と「どこでもドア」の区別をしてくださいと言われているようなものです。弱い AI の話の延長上に，強い AI はたぶん来ないです。今の段階で「どこでもドア」規制法を作る意味があるのかは疑問です。

宍戸：もう少し教えていただきたいのは，スタンドアローンのコンピューターと，インターネットと，今の AI とで，それぞれ飛躍的な変化があるように見えます。あとは強い AI も弱い AI も同じようななだらかな変化だと思いがちですけれども，鳥海さんの話からすると，むしろ弱い AI を含む今までの技術と強い AI との間に大きな断絶があるということでしょうか。

鳥海：あります。だから Artificial Intelligence という言葉がよくなかったのではないかという議論もありますね。違う言葉にしたほうが良い，と。

実積：僕は，AI を独立のスタンドアローンで使う状況があまり想像できません。車の自動運転にしても自動運転しろと命じる人がいる。強い AI が仮にできたとしても，その後ろには，それに対して命令を下したり，あるいは，キル（停止）スイッチを持っている人がいるだろうと思えるんですけれども。また，十分に進化した AI はたぶん人と区別がつかなくなるはずなので，人間を相手にしていると思っていたのに実は AI だったという状況が生じてくると思います。たとえば，強い AI が自律的に行なっている行為と，人が弱い AI の助けを借りつつ行なっている行為と，完全に人間が行なっている行為の区別がつかなくなるのではないかと思います。

鳥海：Watson（ワトソン）の，何か病気を発見したというのがありますよね。あれも結局，AI が発見したのを医者が判断したっていうことになります。そのうち，判断しない医者が出てくるでしょうね。それは弱い AI の話ですし，直近であり得る話です。

実積：その場合，AI が単体として意識を持つ，持たないというのは，利用者からみて意味がないですね。

鳥海：その場合はそうですね。

5　AIと法的責任

実積：人間はAIの言うとおりにしました，AIのほうはプログラムどおりやりましたっていうケースでは誰が意思決定したことになるんでしょうか？たとえば契約法の文脈だと個人の意思の合致で契約成立ですよね。AIが絡むと法的行為は現行法でどのように取り扱うんですか？

鳥海：弱いAIは意識を持ってない道具ですので，今とほとんど変わらないのではないでしょうか。

実積：契約法は個人の意思を尊重するので，AIの意識の有無を問うテストが，そのうち必要になるんだろうなと思います。

鳥海：AIに責任を持たせるかどうかを決定するときに，それは必要になってくるかもしれません。ただ，個人的な感覚としては，ドラえもんが悪いことをしたから，じゃあドラえもんを罰しましょうということを人間や社会がどう捉えるのかは，私は今の段階ではちょっと想像ができないですね。

実積：ジャイアンはドラえもんを殴りますよね。

鳥海：まあ，そうですけどね（笑）。たとえば，ある悪いことをしたロボットを処刑しました。だけどそのロボットの人工知能のコピーはどこかにあって，ドラえもん2やドラミちゃんに，クッと入れたら同じものがピョンって出てくる状態になったとき，果たしてロボットに罰を与えることにみんなが何かを感じるのかは，今はわからないですよね。おそらく，もっと議論が続いたあとの話になる気がします。法制度の問題以前に，AIを罰するかどうかという重要な，社会的な問題になってくるんじゃないでしょうか。

ただ，自動運転の話で責任の話はもう出てますよね。そこに関しては，法制度のほうでAI開発者も自動運転を使った人も守らなきゃいけない。

宍戸：私には，逆に法律家の傲慢がかえって恐ろしいですね。新しい技術が出てきても，法律家は，技術あるいは物それ自体よりも，結局それを使ったり生み出したりした人間が，何か新しい問題を起こすはずだということが分かっていたのに，それを止めなかったと考えて，その人を罰したり責任を負わせたがる。

自分が何か不条理な事態に陥ったときに，それがただ偶然起きたのではなく，誰かが意図的に，あるいは過失によって悪いことをしたからだ，だからこの人に対して責任を負わせるんだという議論を社会が求めて，それを法律家がルールにして運用してしまうという問題が起きやすいように思います。それで本当にAIの研究や社会実装が進むのかどうかが，やはり懸念としてあります。むしろAI研究者の側から，社会なり法がどこで線を引くべきなのか，発信が実は欲しいんですね。たとえば原発にしても，あるいは宇宙衛星にしても，これ以上は責任を負えないということと，リスクはあるけれども技術やサービスの発展から見たときに，責任を限定するとか，あるいは客観責任にするけれども保険で担保するとか，いろんな仕組みを考えるにしても，何かアドバイスを聞かせてください。

鳥海：法律で罰を与えるのは，社会の感情を満足させるためなのか，それとも二度とそういうことが起きないようにするための抑止力なのか，2つの観点があるのではないかと思っています。社会の感情のほうはわかりませんが，抑止力の点から考えると，あまり技術者を罰するということに意味がないと思うんですね。

技術者は基本的には精いっぱい頑張ってやっていて，ただ，予想外のことが，どうしても発生することはある。そのときに，予想外のことが発生したからおまえが悪いんだって罰しても，それは抑止力には全くなりません。AI研究者は別にそうしようと思って作ったわけではないので。たとえば，事故率が何パーセント以下であれば，技術者に責任はないという風にしていただきたいなと思います。

実積：今の話をお伺いしていると，法律家の観点からいくと，AIに意識があるって認定はできない，すべきではないという結論になりますね。AIは意識ある人間に使われる道具にすぎず，人間が最終的に責任を負うべきだという立場ですから。そうすると，技術者であっても完全にはコントロールができないものについて，利用者の責任を問えるんだろうかという疑問が生まれます。その場合，PL法みたいな枠組みは機能するでしょうか？

宍戸：ペットが人にかみついた場合に，このワン

ちゃんに何らかの意識があるけれども，法律的には物ないし道具としてひとまず取り扱って，飼い主の責任を問える場合は問う，問わないこともある，と考えるわけです。本当に意識があるかどうかではなく，社会の側で，法的な責任を問い得る主体と思うかどうかによって線を引くわけです。その線を引く基準は，まさに鳥海さんがおっしゃったように，責任を問うことで社会をどうしたいのかによる。

刑罰についていえば，「目には目を，歯には歯を」という応報，こいつにはもう二度と悪いことをさせないという特別予防，こういうことをした者に対して罰を与えれば他の人たちも気を付けるという一般予防の3種類ぐらいの考え方がありますが，刑事法以外でも似たような考え方をしています。

問題はそこから先で，実積さんのいうPL法は，製造物に着目して，消費者と製造者の間の格差を前提にして，消費者を守るという観点から責任を負わせているわけです。AIの問題も，法律家の中でも2通りの考え方が分かれるだろうと思います。1つは，AIは物ではなくて，情報あるいはプログラムの問題であり物とは違い，問題が生じたときに限度がないという側面も含めて，製造物責任と同じように全部の責任を事業者に求めることは難しいというように，AIと物の違いに寄せることです。

もう1つの考え方は，事業者と消費者の地位の非対等性に着目する。AI研究者と普通の消費者，要するに鳥海さんと実積さん及び私との間には，AIについての理解の差が，あるいはどちらが問題を止めやすいかについての圧倒的な差があるわけです。そうすると，製造物責任類似の発想で，開発者に責任を負わせたほうが，AIに由来する問題がより生じにくいという整理になってくるのではないでしょうか。

鳥海：ペットと同じで考えるというのは，かなり良いと思います。イヌと同じ扱いというのは，ああ，なるほどなと思いました。要は，人工知能には使っているうちに学習するっていう機構が入るので，使い方によって動作が変わってくる。そのときに，製造者は，どう使われるのか分からない以上，責任は負えないですよね。逆に育てているほうも，中身が分からないので，どう育てたらどうなるか，やっぱり分からないという状態ではないでしょうか。

となると，イヌと同じく，ブリーダー，ペットショップに責任があるのかという問題のように考えるのがよさそうですね。たとえばこのイヌとこのイヌを掛け合わせて，こういうイヌを作った人と，それを育てた人がいました。そのイヌが誰かにかみつきました。いや，このイヌとこのイヌを組み合わせたら，どう猛になるでしょうという考え方もあるし，育て方によってはどう猛にならないよねっていう考え方もある。これにかなり近いんじゃないかと，今の話を伺っていて思いました。

実積：たとえば，自動車学校って運転者を大量生産していて，そのうち何人かはひどい事故を起こすわけですよ。そのとき，自動車学校に責任をとれという人はいないです。あくまでも運転者本人にいきます。一方，テスラが自動運転中に事故を起こした場合は，テスラが責任を負うべきだという議論があります。この差は，意識の有無，コントロールの有無に由来するのではないでしょうか。そうするとAIはどっちにいくんだろうか。今のAIはたぶんコントロールができるんだろうけれど，そのうちコントロールができない，何考えているか理解できないAIができたときは，誰が責任をとってくれるのか。それがはっきりと分からないと，社会的に，みんなが安心して使ってくださいと言うのには時期尚早かもしれないと感じます。

鳥海：責任問題の話なら，安心して使えないという話になりますね。

実積：いや，責任問題よりも，AIを改善して事故発生を防止するというインセンティブが十分には生じないという点に危機感を覚えています。AIが関係して発生する事故の責任を研究者が負わないし，利用者にも問えない，もちろんAIも負わないとすると，誰が改善しようというインセンティブを持つのでしょうか。この点について，考えていただきたいなと思っています。

鳥海：確かにそれはそのとおりですね。

実積：インセンティブを与えた結果，資源配分が改善したように見えるのが，二酸化炭素排出規制や公害規制のケースです。悪い結果が発生した場

合の責任を設定することでインセンティブを設計した結果，適切な方向に技術開発が進むという側面があります。だれに責任があるかを認識させるということは，やっぱり必要ですね。

鳥海：インセンティブがあると動くということは，納得するのですけれども，インセンティブがないと動かないには結び付かないんじゃないかと思います。直接的なインセンティブがないと動かないではなくて，他の仕組みによって動かすほうが，建設的な気がします。インセンティブについては実積さんのおっしゃる通りなんですが，現状を考えていると，インセンティブを与えるのはかなり難しいんじゃないか。だから，違う仕組みを持ってくるほうが，AIを今後どうするかに関しては現実的だと個人的には思っています。

6　総務省のAI開発ガイドライン案

宍戸：その違う仕組みの候補になり得るかという観点から，総務省で検討されている開発原則ガイドラインの話に移りたいと思います。現在，政府でもあちこちでAIについての研究がなされています。

たまたま実積さんと私は総務省の「AIネットワーク化検討会議」，その後継組織である「AIネットワーク社会推進会議」のメンバーとして一緒に議論しています。この会議では，ただのAIではなく，ネットワークにつながっている，つながり得るAIという観点からさまざまな議論をしておりますが，AIの研究開発についてのガイドラインを提案して国際的な標準にできないかという方向を目指している点が，総務省での検討の1つの特徴です。

そこで，この開発ガイドラインの中身について少し議論をさせていただきますが，まずは実積さんから，ガイドラインの内容のご紹介および問題提起を頂けますでしょうか。

実積：まず，2016年2月から6月まで，AIネットワーク化検討会議がありまして，そこで，AIが複数社会に存在し，お互い共同作業を行うという社会が，今後実現されるだろうという議論をしました。その上で，安全・安心な社会を作るためには，どういった制度的なセーフガードを張っていくべきかという話を扱うのが，今回のAIネットワーク社会推進会議で，昨年12月から議論を始めています。その議論の一環として，1月末を締め切りにして，AI開発ガイドラインの意見照会をしているところです。

AI開発ガイドラインとは，研究開発に携わる人たちが，こういった原則に従って開発するのが望ましいというものを9つ挙げ，それを3つのグループに分けて記述しています。中身については総務省の資料をご覧いただければいいと思うんですけども，透明性とか，制御可能性，セキュリティのように，こういったものは当然守るべきだろうなというところが入っていて，項目立て自体については，それほど問題はないと思います。

AIの開発は，政府のナショナルプロジェクトの形よりも，大学とか研究機関，あるいは企業が独自にどんどん先に進んでいく，しかもそれが国境を越えてグローバルに展開するという形で進んでいくと想像しています。そこでは，市場メカニズムをベースとした経済的なインセンティブで作業が進んでいきます。その過程で，先ほど言ったように，誰も責任を取らないというか，公害問題のような外部経済が発生するのであれば，社会的に望ましい方向に開発が進むような仕組みを作っておくべきだろうと思います。開発原則にはそのための指針を提示するものとなってほしいと思います。

ただ，注意しなければいけないのは，開発原則の原案を作成したのは法律家が主体の集団ですから，最新の技術知識に対して必ずしも完璧な知見を持っているわけではありません。その意味で，今回のパブリックコメントにおいて技術者コミュニティからの意見が多く出てくることに私は期待しています。

今回この開発原則で，AIの開発者に対して，こういうところを守ってほしいということを9項目挙げていますが，先ほど鳥海さんのほうからありましたけども，AIの開発者あるいはそれをマーケットに出した人が想定できない使い方，組み合わせが出てくると想定されます。そうすると，利用の原則というか，モラルというか，利用者教育というか，そういったものもセットにならないと，今回この開発原則が狙っている目的が果たされないだろうなとも感じています。

対象となる利用者にも2種類あって，1つは本当のエンドユーザー，もう1つは開発されたAIを組み合わせて，利用者に対して新しい価値を提供するような人たち。この2種類の利用者のAI利用原則を，先ほどの責任問題を含めて，ちゃんと決めておくことが，社会に必要な制度づくりではないかと思います。

AIの開発は民間を主体にグローバルに進んでいきますから，この原則を日本国内にとどまらず，世界のガイドラインに持っていこうという総務省の方針には基本的に賛成します。ただ，その中で，将来の民間活用とか研究開発に関するトライアル・アンド・エラーのために，できるだけ大きな余地を見込んでいただきたいと思います。起こるべきリスクに対して予防的な態度に徹すると，せっかくの技術開発の可能性を，特にICTの分野で，摘むことになりはしないかということが一番懸念するところです。AIは学習するものなので，当初，限定的な範囲では失敗を認め，失敗をその次の開発に生かすような試みに対して寛容なガイドラインになればいいなと思います。

7　ガイドラインのグローバル化は可能か

宍戸：ありがとうございました。鳥海さんいかがでしょうか。

鳥海：まず，このガイドラインの目的の話です。これはグローバルに展開して，世界中がこれに従うということを一応目指すのでしょうか。となると疑問なのは，これを外国にガイドラインとして出したときに，果たしてアメリカや中国といった国々が，これに批准するのかどうか。

今AIの開発はほとんど中国とアメリカが行っています。その上で，日本もこれからどんどん発展させていかないといけないわけです。そのときに，一番危惧しているのは，こういったガイドラインを設けることによって，日本での開発に制約を受けてしまうわけですよね。一方で，アメリカ，中国がこれを全く無視するというのが，日本にとっては一番うれしくない状況です。それに関して，このガイドラインを策定する上でどうお考えなのかをお聞きしたいです。

宍戸：私の理解している限りで2点申しますと，第1に総務省としては，アメリカも中国も載れるように，条約のように厳密に拘束的なルールではなく，グローバルな研究開発のコミュニティが共有できるようなソフト・ローとして，ガイドラインを考えていると理解しています。ですから，日本特有の話はかなりそぎ落として，ユニバーサルに受け入れ得るようなたたき台として考えているだろうと思っていますが，もちろんそれで本当に大丈夫かということは問題ですので，今後もさまざまなレベルで議論されていくはずです。

2点目は，ガイドラインが研究開発を縛るのか促進するのかですけれども，事柄にも両面ありますが，少なくとも検討している側は，促進するために必要な社会的合意の一側面だと思っているのでしょう。日本社会によくありがちなことですけれども，たとえば自動走行で，何の手当てもなく社会的な前提もなく事故が起きた場合，メディアや政治が炎上して，そんな研究はやめろという展開が，一番恐れられている。一定のガイドラインという形で，前もって一定の社会的合意を調達しておいて研究開発を守るということが，このガイドラインが目指している理想だと思います。

ただ，この種のガイドラインについて付き物ですが，そういった理想どおりに本当に機能するかどうかは問題です。遺伝子研究など，様々な研究分野でガイドラインがありますけれども，幅があり研究開発を守るものとして運用されるよりは，書いてあることを杓子定規に適用したり，違反がなくてもガイドラインを拡大解釈したり補ったりして，とにかく研究開発の手足を縛っていくという方向になる恐れは，確かにあると思っています。

一般的な研究開発の原則指針，基本理念の部分で，関係する価値，利益のバランスを確保しなければいけないことを示し，弾力的な比較衡量を行いながら，このガイドラインは具体化され，適用・運用されるべきものであることを明らかにしているのは，その趣旨だと思いますが，それで本当に大丈夫か，さらにご議論いただきたいと思います。

8　予測に基づくガイドラインの限界

鳥海：おそらく中国なんかは，取りあえずやって，問題が起きたときにどうするという対処法になるわけじゃないですか。アメリカやヨーロッパ系は

みんなそうですよね。それならば，いろいろ試してみても，おそらくありがたいんですね。もちろん，たとえば人のプライバシーをバリバリ外に出してはいけないというように，最低限はあるとは思います。ただ，それは別にAIの話ではないところで，すでに抑制されている部分ですよね。そこはいいんですけども，そうでないところで，しかもわれわれも法律家の方も何も予想できない状況下にもかかわらず，何か予想して縛るというのは，おそらく縛る方向にしか行かないのではないか。

逆に，失敗したときには何らかの形で対処をしましょう，きちんとしましょうねというほうであれば，まだよい。しかも，その責任を，たとえば研究者ではなくて，国が取りますからと言ってくれるんだったら，すごく研究が進むと思うんですが，。そうではないですね。研究者がきちんと気を付けなさいね，でしかあり得ないわけですよね。ガイドラインなので，当然それは当たり前なんですけれども，それでいて，実はこれは縛るものではないのですと言うのは，やっぱり無理があるのではないかと思います。

宍戸：事後的に失敗したときに気を付けましょうねといっても，人間が悪用してそうなったのか，当該AI自体の中に内在的な欠陥があったのか学習によって生じたのかとか，逆にバイ・デザインといいますか，事前に研究者の方でも最低限気を付けていただくときに，おそらくこのガイドラインの要として想定されているのが，9番目のアカウンタビリティの確保に関する原則，「AIの開発者がステークホルダーに対し果たすべき責任に関する原則」です。

開発者は何を自分がしているか，あるいはどこまでは責任を負えないかが分かり，それをあらかじめ説明していただくと同時に，事後的に問題が起きたときに原因を追いかけるために必要なものとして入っているのだと思いますが，これは研究者の視点からは難しいでしょうか。

鳥海：一般的な製品に関しては，アカウンタビリティの原則はあるんですか。

宍戸：一般に，現在では消費者保護の観点から見て，商品・サービスを売るときに，これはどういう機能を持っており，あなたにどういうことが起きうるかについて，いわば説明責任が要求される場合はあります。一番典型的なのは整形手術ですけれども，最近だと電気通信事業法が改正されて，適合性の原則が置かれています。

AIは文系から見るとまさに魔法の世界で，一般の消費者もそうだろう。そこで，一体これはどういうものなのか，イメージができる説明が欲しいということですね。

鳥海：だとすると，従来のレベルであればAIでも可能だと思います。ただし，AIの場合は，開発者も予期できない動きをする可能性がある。そこまで説明責任を求めると，もうAIは作れないので，想定し得る危険性について書くのは当たり前だとしても，それ以上について書け，あるいは説明せよ，というのは無理ですよね。

9　研究・開発と利用の区別

実積：そこは利用原則が必要で，開発者にそこまで責任を負わせるのはたぶん無理だろうと思います。開発者が使い方を完全にコントロールできるわけではありません。

その意味で，この開発原則がその方向に技術開発をしてくれというふうなインセンティブとして働けば良いと思っています。

たとえば，車のエンジンを作る人は良いエンジンを目指します。でも，利用者目線ではエンジン単体ではなく，システムとしての車が欲しいわけです。アクセル踏んだら進め，ブレーキ踏んだら止まれ，ハンドル回したら曲がれ，エアコンはちゃんと利け，その上で，説明書がちゃんとあり，保険も適用されている，そういうパッケージでわれわれは車を欲しいわけです。AIもそういうパッケージとして提供してもらわないと使えません。その段階まで，つまりパッケージにするまでは研究者コミュニティの領分です。

そのとき，個々の研究者に全システムの責任を任せることは無謀です。「研究者同士が連携を取って，AIというシステムを世の中に出してください。そのあとは利用側が考えますよ。」というふうにしないと，上手く回らないだろうなと思います。AI研究者に，この原則を全部満たすような研究以外は認めませんよと言うと，いつまでたっても製品が出てこないかもしれません。

鳥海：今のお話を聞いていて，気付いたんですが，これは開発原則なのか，研究原則なのかどちらなのでしょうか。今おっしゃっていたのは，研究側ですよね。セキュリティの原則は研究のレベルの話であって，それを組み合わせて開発した車を販売すると，たとえばトヨタならトヨタ，日産なら日産が，これを全部カバーしなさいという話になるわけですよね。そういう意味では，最後に商品を出す人がこの原則を守った商品を出しなさいねというガイドラインになるのでしょうか。

宍戸：この研究開発ガイドラインは，私の理解では，研究開発の全部を一応包含しているイメージですが，エンドユーザーに提供する局面だけじゃなくて，その前段階のメーカーへの提供も含む。AIを組み込んだ空気清浄機を製造して販売するときに，空気清浄機のメーカーにとってはAIが分からないのであれば，その前段階までが研究開発ですね。このガイドラインの適用範囲はかなり相対的だろうと思います。なればこそ，さっき実積さんが強調されたように，利活用ガイドラインは，また別に作らないと駄目だ，という状況ですね。

鳥海：たとえば透明性の原則，制御可能性の原則を個々の部品に組み込む必要性があるかないか。今のお話ですと，AI搭載エアコンの個々の部品が透明性と制御可能性を持っていなければいけないことになります。でも，エアコンの中にそのAIを入れるときには，そのAIの外側で制御可能なことはすごく多いですよね。そうすると，そのAI自身に制御可能性は必要ない。にもかかわらず，制御可能性がないAIを作っては駄目となると，非常に開発が難しくなります。

もっと上の段階でバタンとふたを閉じちゃったほうが全然楽なのに，個々のAIに対して，いちいち制御可能性の原則を取り入れたものを開発するっていうのは，コストが2倍3倍に膨れ上がる可能性がある。

実積：なので，AIネットワークシステムに着目しているんだと理解しています。今言った，制御可能性を担保するキルスイッチのようなものは，AIと外部からつないで使いましょうよという提案になるのかなと思っています。

鳥海：たとえばエアコンの中に入ってるAIも，ネットワークシステムの可能性は十分あります。たとえば隣の部屋のエアコンと通信して何か温度調整するように。AIネットワークシステムのネットワークは何なのかを，きちんと定義したいですね。

実積：さっきの質問の答えとすれば，AIだけで全ての原則を満たすことはないと僕は思っています。たとえばリスク対処についても，保険のシステムを導入すればよいと思っています。いずれにせよ，「対処している」「対処していない」の二元論的な対応ではなく，さまざまな強度の対処方法があるべきだと思います。透明性の原則についても同じです。AIの本体部分に求めるんではなくて，最終的に提供されるパッケージとしてこれらの原則が保証されればよいのではないかというのが僕の意見です。その意味で，この開発原則は，制御可能性を担当する部分，いざとなったら止めてくれる部分などを含めてAIシステムの開発を進めるべきだ，というふうに読みたいと思っています。

鳥海：それだと，最後に商品レベルになったときの，全体システムの制御可能性であり透明性でありという話になってくると思うんですね。

そうなると，システムって何だという話が今度は出てきます。実積さんがイメージされているシステムは，引っこ抜けば止まるものだと思います。一方で，車のシステムについて考えてみると，AI搭載型の車による「交通システム」が出てきます。

その場合は，もはやコンセントを引っこ抜くことはできないんですね。個々の車が勝手に動いてるので，なんかポチッとボタンを押したら全ての車がピタッと止まる仕組みは導入できない。山手線は，今日来るときも止まってましたけども（笑），そういうシステムにできるのかというと，それは難しい。

実積：利用者や利用企業が責任を持つ範囲と，開発者が責任を持つ範囲が分かれる境界線はアプリオリには決められません。なので，利用原則と開発原則は全く別ものではなく，同じ項目は幾つか入るべきなんだろうし，入らければ駄目なんだろうなと思っています。

宍戸：私も同じ理解で，鳥海さんには本当の研究

開発ガイドラインしか適用がない，AIを実装し売る人には研究開発と利活用の両方がかかって，エンドユーザーには利活用ガイドラインだけがかかるというイメージだと思いますね。

実積：全部研究者に責任をおっかぶせて，ということにはしたくない。

鳥海：ええ。AIは基本的にはロジックですから，AIを作るということはロジックを作ることにすぎません。これは私が研究者だからそう思うのかもしれませんけれども，ロジックを作るところに制限を置くのは非常に難しい。それをやると，日本はアメリカや中国に勝てなくなる。ロジックの部分は自由に作らないと，たぶん駄目ですね。研究は自由にして，開発のあたりから徐々に制限が入り，商品化のときにはきちっとした制限が必要だと思います。

10　AIネットワークシステムとは

鳥海：さっきも言ったとおり，車自身がAI化されて，それが他と通信して動くときに，この製品に対してガイドライン作りましょうというのは分かります。ところが，AIネットワークシステムとして考えた場合，複数台の車がネットワークでつながり，それが1つのシステム，AIネットワークシステムになります。それに関して，透明性，制御可能性を担保しようとすると，それは誰が担保するのでしょうか。

実積：それは，ある意味，ビジネスチャンスですね。そういう情報を出す車に乗れば保険料が安くなりますよという企業が出てくるだろうと思います。

鳥海：ただ，ガイドラインの場合は，担保しなさいと書くわけですよね。

実積：今回のガイドラインは拘束的なものではないので，準拠すれば何らかしらメリットが発生するものになってほしいと思っています。ガイドラインに書いているからといって，これに準拠しないシステムを作ることは止めようがないし，そういうことをする企業は現れる。ただし，このガイドラインに準拠すれば，たとえば，透明性とか制御可能性の原則に準拠するように作れば，補助金がもらえるというメリットが付くというイメージです。何らかのインセンティブを与えることができるなら，時間はかかるでしょうが，望ましい原則に準拠するための技術が出るだろうなという期待はしてますね。

鳥海：要は，これは自律分散システムになるので，制御する人がいない。

実積：制御する人がいなくても問題ない。われわれは制御する人がいなくても自分の意志で保険に入ったりするじゃないですか。何らかの行動にメリットを与えるというフレームワークを作れば，長期的にはその方向に動くんじゃないか，という期待です。

鳥海：つまり，ガイドラインに入っている原則，たとえば制御可能性の原則は，満たされなくなりますね。

実積：制御可能性の原則を満たす方法が技術的なものだけとは，僕は思っていないです。制御可能になるものをシステムに組み込むことによって，目的を達成する。どんなものでも乱用される危険はあるし，暴走する危も険あるかもしれないから。そうすると，制御可能性を満たしたほうが得ですよというシステムができると思っています。制御可能な自動運転車とそうじゃない自動運転車があって，制御可能な自動運転車をみんな使ったほうが税金も安くなるかもしれないし，事故も少なくなるかもしれないし，保険が安くなるかもしれないよというような社会システムを作ることで望ましい状況が実現されていくんだろうなと思います。

11　AIネットワークシステムの制御可能性

宍戸：総務省のガイドライン案では，制御可能性について，一応対象をAIとした上で，「制御不能となるリスクにつき，その蓋然性が高い又は不確実と考えられるAIについては，一般社会で利用される前に，実験室等閉鎖された空間において，当該空間外につながる情報通信ネットワークシステムに接続せずに，AIの制御可能性について実験を行い，リスク評価を行うことにより，制御可能性を確保すべきとしてはどうか」と書いているのですが，どう思われますか。

鳥海：一般社会で利用される前に，実験するのは，今でも当たり前にやりますね。なので，別にそんなに目新しい話ではありません。実験室で，ちゃんと動くことを確認しないで外に出すっていうの

はあり得ないです。なので，これは普通のICTシステムと同じことを言ってるだけだと思います。

宍戸：それで，さっきの車の話に戻るのですけれども，制御可能性が順守されれば，ネットワークシステム化された車の自動走行も，自律分散で問題があったときに制御できるというイメージで書かれているだろうと思うのです。

鳥海：これを書かれた方は，複雑系システムについて考慮していないのだと思います。基本的に複雑系システムは制御不可能です。ネットワークシステムを考えたときに，それが複雑系であった時点で，それを完全に制御することは不可能です。

宍戸：これも完全制御までは考えていないと思うのですけれども，何か問題があったときに，すぐそのスイッチを切るということもできない，ということでしょうか。

鳥海：日本全国で車が1万台走っているとしましょう。このとき，個々のAIが問題を起こすのではなくて，それらが組み合わさって初めて起きる問題が存在します。たとえば，今の人間による運転でも，事故がなくても大渋滞が起きることはよくあります。別に個々の人間に問題がなく，みんなきちんと法律を守って普通に運転している。それでも渋滞が起きることが分かっています。それはシステム的な問題なわけです。

同様に，AIならではのシステム的な問題を起こしたとすると，そこに制御可能性はなくなります。

実積：混雑問題の場合は，ピーク時には高く，オフピーク時には低く設定した混雑料金を導入するという解決策があります。AIの評価関数の中に高速道路の利用料金を安くするということを入れれば，システム全体として，混雑回避性が実現できます。制御可能性に関しても，ここでいう混雑料金のような社会システムを導入することで，社会的に最適な制御可能性を実現できるはずです。

鳥海：実積さんの言うとおりの方法が，おそらく唯一の解決策だと思います。ただ，これは複雑系なので，事前には分からないんですよね。ですので，そうなったときに逐次的に問題を解決するための社会的な基盤を作っていくことができる状態になっていなければいけない。

ただ，それはAIの話なのか，社会のシステムの話なのかというと，社会システムの話だと思います。だからAIネットワークシステムに導入するというよりは，社会システムのほうにそれを導入するという考えがよいのではないでしょうか。それを，AIネットワークのほうでそれをなんとかしろというのは難しい。

宍戸：AI研究開発のシステムの側に，全部責任を寄せるということは，私はもともとあり得ないと思いますね。

12　研究と社会システムの対話，AIの定義

宍戸：お話を伺っていて私も見えてきたのは，こういう問題だろうと思います。社会システムの側が，AIの研究開発と孤立して適当にルールを作っても，全く機能しない。逆に，AIを研究開発して，そのアウトプットとして出てくる，AIの利活用が，制度，法とか経済的インセンティブから全く孤立して作られるのも，全く機能しない。だから，鳥海さんのおっしゃる社会システムの問題と，AIの研究開発の双方が，システム間でカップリングできるように，お互いにその視点を内在していないと，有効に機能しないと思うのです。

総務省での議論は，社会システムの側から研究開発について，最低限こういうことをしておいてくれると，あとで問題があったときに介入というか修正ができるという，その取っかかりとなる足場を，研究開発の側の中に築くということだと思いますね。制御可能性のようなAIの研究開発の原則が何もないところで，社会システムの側で全部やろうとすると，とにかくAIは研究開発するなという話になってしまう。少なくとも，問題が起きるとしてもとんでもない問題，社会システム全体を破壊するところまではいかない程度であるとか，何かあったときに一定の手が打てる程度の枠内で一歩一歩進めてくださいということを，社会システムの側は要求せざるを得ないと思うんですね。

鳥海：そういうの全てを包括するようなガイドラインとなるとものすごくふわっとしたガイドラインにしかならないような気がします。今の法律をちゃんと守りましょうねというレベルになってしまうのではないでしょうか。1回世に放ったら，もう二度と変更できないようなシステムは作らな

いようにしましょうねとか，なんとも当たり前なガイドラインになります。

実積：制度を作る側と，研究者の間で意見交換の機会を定期的に持つのが大事だと思います。その嚆矢が今回の総務省による意見照会という位置づけですね。この一回の意見照会で全てが決まって，法律になるという流れではありえない。

宍戸：そもそも，すぐに法律にすることは考えられてないものですよね。

鳥海：それは非常にいいと思うんですが，技術者側にコメントすることのインセンティブを明確に出さないといけないと思います。少なくとも，AIロジックレベルの研究者にとって，あまりインセンティブにはならないですよね。

宍戸：研究者側から見ると，制度屋がいろんなことを言っている，何か言わないと問題が起きるという，ディスインセンティブのほうですよね。

鳥海：だとすると，その段階でOECDに出のは意味がない行動をしているように見えるんですよね。研究者側からすると，われわれの意見を全くくみ取らないで，勝手に作って勝手に出しちゃった，という感じになります。

宍戸：私のような構成員も十分分からないで議論している自覚はありますので，総務省の研究会にしても，きちんとした研究者のコミュニティと議論する機会が必要だろうと思います。

鳥海：そうだと思います。ただ，それは1～2時間議論して済む話ではなくて，1年間かけて議論する話だと思うんです。

実積：1年間かけて議論することにした場合，何を議論しますか。たとえば，今のこの9項目で，これはあり得ないというものはありますか？

鳥海：まず，定義が全然なされてないですよね。やっぱり理系なので定義は重要なんですよ。

実積・宍戸：いや，文系も重要です。

鳥海：おっと，すみません（笑）。定義がないので議論できないということが，とりあえず指摘したいことです。4のガイドラインの目的と理念に関しては，定義が変わるとがらっと変わると思います。適用範囲が利用者と開発者，研究者が明確に分かれていなければ駄目ですね。

13　透明性，セキュリティ，プライバシーの原則

鳥海：透明性の原則については，透明性とは何か，からスタートして，透明性のレベルを指定する必要があります。本当の透明性は，逆に出せるんですよ。プログラムとデータとを全部公開すればいい。ただ，解釈できない。おそらく透明性とは解釈可能性の問題なので，そこをきちんと明確にしたほうが良い。

実積：全く不透明であるのはまずいっていう意味での透明性原則であれば大丈夫なんでしょう。

鳥海：どのレベルの透明性なのかは，1年ぐらいかけて検討するべき点だと思っています。制御可能性も同様ですね。特にネットワークシステムが複雑系であるということが意識されてないので，複雑系の専門家を入れていかないと議論できないと思います。

セキュリティに関しては，今後議論すればいいと思うので，あまり言うことはない。安全保障に関しては，どうなんでしょう。保障しなきゃいけないのは分かりますが「バグを出さないようにしましょうね」と同レベルの話になっている気がします。100パーセントは無理なので，どこまでと考えるか。

実積：この辺って，アカウンタビリティの話と似てきますね。誰がこの措置を決めたのか，何が原因でこれが発生したのかを明らかにするよう努力しようっていうのは必要ですね。

鳥海：そうですね。できるだけ努力をしていますということを見せるとか，車だったら人がいたらよけるとかぐらいの話にしかならないですが。

宍戸：私は，これはそのぐらいの話なんだろうと，もともと思っていました。

鳥海：プライバシーに関しては，プライバシーデータを全く使っちゃいけませんということは，おそらくできない。できないというよりもほかの国に勝てなくなるので，そこもかなり注意して書かないといけないところだと思います。

14　利用者支援の原則

鳥海：利用者支援の原則は，よく分からないところです。

宍戸：これは最終的なネットワークシステムのこ

とを念頭に置いた上で，その構成要素たるAIがユーザーフレンドリーなものであることを求めるものですね。

鳥海：操作しやすいインターフェースを設計すべきではないかというと，操作しやすいインターフェースとは何かというところから始まりますね。実積さんの理論がまさにこれで，利用しづらいものは誰も使わないという経済的な話じゃないでしょうか。だから，これはあまり意味がない気がします。

実積：利用者支援原則の利用者は，エンジンメーカーに対するトヨタに該当するんだと思います。部品としてのエンジンの細かい話については運転者にではなく，組み立てメーカーであるトヨタに説明しないと通常は仕方がない。AIについても同じで，利用者支援の対象はAI利用企業でないと実効性がない気がします。

鳥海：ユニバーサル・デザインの話だったらありかなと思います。社会的弱者に気を使いなさいという話ですね。

宍戸：私の理解では，AIを使ったサービスが進んできたときに，デジタルデバイドのより強力なバージョンが出てくることを，懸念していると思います。

実積：その担保をAI開発者に求めるのは難しいと思いませんか。

宍戸：この場合の開発者は最後に市場に出す人だと思います。

鳥海：生産者ですね。

実積：問題となるのは利用局面だから，利用ガイドラインに入れるべき話ですね。

宍戸：だから利用企業は，真ん中にいて，研究開発ガイドラインと利用ガイドラインの両方の側面があるわけです。ここではエンドユーザーに提供する開発者としての，AI込みの製品サービスを開発する人について利用者支援を要求しているのではないでしょうか。

実積：車を買うという例で考えましょう。宍戸先生がおっしゃっているのは新車を開発するチームに利用者支援を求めるのと同じですよ。僕は，利用者支援は販売店の人に求めるべきだと思います。

宍戸：なるほど販売店は利活用の対象ですが，それは両方あるのではないですか。

実積：エンジンの開発者は，販売店の人に説明しろという義務は負わせてもいいかもしれないと思いますが。

宍戸：販売店の人が，車の中に入っているインターフェース，いじれないですよね。

実積：そこは，B to Bの局面での利用者支援に関わる話ですね。

鳥海：ここはいろいろな解釈の仕方があると思うので，深く議論するところではないでしょうか。「利用者支援の原則」はたぶん解体していろんな書き方に変えるべきですね。

実積：利用者の定義がないから，難しいんじゃないかな。

15　アカウンタビリティの原則

宍戸：先ほどもアカウンタビリティはある程度議論しましたけれども，これはどうですか。

鳥海：アカウンタビリティに関しては，法制度でどこまでを求めるのかと，技術者がどこまで応えられるのかの擦り合わせの話だと思います。

実積：これは2種類たぶんあって，企業間であれば，リテラシーが十分にあるから，何もしなくても必要な部分は個別にやると思う。もう1つは，最終利用者に絡む話で，事故が発生したあとで損害賠償うんぬんの話になったときに裁判所に提出する必要があるから，一定の形式でログを記録しておきなさい，という話かと思っていました。

鳥海：そこはアカウンタビリティとして用意しておくのではなく，第三者機関が入ってきて，データを集めて説明するようになるのではないかと思っています。事前にここまで用意しておくというよりは，その都度，何が起きたのかを調べなければいけないのではないでしょうか。

宍戸：事故調査委員会のイメージですね。

実積：航空機事故が起きるとブラックボックスの解析をして全容解明を試みるわけですよね。AI開発においても同様のシステムが必要だ，という話だと思います。

鳥海：そこに対して説明責任はあると思います。開発者側が，事故が起きたときに全部説明する責任っていうのを負わせるということではない。

実積：そういう意味ではないと思います。ログを取っておきなさい，ログを取っておいたら，アカ

ウンタビリティ責任を果たすことになります，と意味かと理解しています。

宍戸：私は，これももう少し広いように思います。最初からガイドライン自体は拘束的に事細かに決め切らないことを前提に，研究が進んでいく中で，研究者がやりたいことについて社会的に合意があるかどうか分からないときに，世間に対して議論をせずに研究を進めるのはやめて欲しい。しっかり逐次に，多様なステークホルダーと対話を行って，意見を聴取する仕組みが必要ではないか，というものではないでしょうか。

鳥海：それは，実運用するときに必要なので，開発と研究というよりは，運用する段階までいったときに，初めて必要になる話ですよね。その手前段階では，可能性の芽をつぶしているような気がします。

実積：アカウンタビリティの技術を開発してくれる人に対して報償が与えられるというシステムがないと難しいよね。飛行機のブラックボックスを作る人や企業に対してお金を出しますというようなものではなくて，飛行機を作る人にブラックボックスも作れというのは，確かに可能性の芽をつぶすかもしれない。

鳥海：お金などの作るためのリソースがちゃんと渡されるのであればできると思うんですけど，現状はそうではないですね。だとすると，研究開発段階では，ある程度自由にやってもいいような気がするんですよね。最終的に社会に出すときには，飛行機のブラックボックスのようなものを組み込もうという話になると思います。つまり，研究開発というよりは，利用者の話になるんじゃないでしょうか。

宍戸：いい喩えか分からないですけれども，遺伝子研究の場合，治験の段階もありますけれども，その前にこういう研究を進めていいのどうか判断する例もありますよね。

鳥海：ヒト胚の問題とか，その辺ですね。そこまでの危険性がAIで生まれるのかどうかが未知な段階で，制限を加えるべきかどうかは疑問です。危険そうなものが出てきたときに，それを抑えることができれば十分ではないでしょうか。

宍戸：社会システムの側から言うと，その危険そうなことが起きたときに，アラートが研究者コミュニティから上がってくればありがたいのですが。

鳥海：まっとうな研究者であれば学会発表をするので，その段階で公知になると思います。その時点で問題があれば，問題があると思った人が何か言うかもしれませんし，最初はその業界のシステム（業界団体，学会など）にある程度任せたほうが良いと思います。上から押さえつけると萎縮してしまいますよね。まだ，AIに関してはそこまで危険なレベルの話はあまりない気がします。

宍戸：私も，個々の研究開発者にこれを求めるのは酷だと思います。自主規制は個々の人ではなくて，業界全体として健全に回っていればいいということのはずですよね。

鳥海：そうですね。いずれにせよ，最初は自由にやって，問題がありそうな場合はあとから止めるとやらない限り，アメリカ，中国には勝てないと思います。

16　連携の原則

宍戸：連携の原則は，いかにも総務省の研究会ですが，いかがでしょうか。

鳥海：これに関しては，2つの解釈が考えられるのでどちらにするかによって，全然話が変わってきます。1つは物理的なネットワーク，もう1つはロジカルなネットワークですが，どちらかが全くここでは議論されてない，というより混在しているんですよ。どちらを指していると定義するかで，AIネットワークの話は全然違う方向に行きますから，ここは最初に議論しないといけません。

宍戸：AIおよびAIネットワークの定義をはっきりさせてくれないと，これは困るということですか。

鳥海：そうです。連携とは何なのか。「連携の原則」にいくまでは，物理的につながっていることを指してAIネットワークといっているのかなと思ってたんですけど，連携ということはロジカルなネットワークを考えているのでしょうか。

実積：外国のAI，たとえば，右側通行の米国の自動運転車が日本に来た場合に，左側通行の日本の自動運転車との協調をどうやって達成するのかという問題が，AIネットワーク検討会議のときに念頭にあった問題点だと記憶しています。そうすると，電子的なネットワークだけを相手にして

いるだけでは済みません。情報通信網に乗らない物理空間でのネットワークを議論しないわけにはいきません。例えば，陰から人が飛び出してきたというのは，情報通信ネットワークに載っていない主体間の問題ですよね。

鳥海：実はロジカルなネットワークは，そういう意味でものすごく広いです。たとえば，カメラを搭載した車が，あの車が今どういうふうに動いてるから，速度をちょっと落としましょうというのも，この連携に入るはずです。そういった連携には，トヨタでもホンダでも関係ないんですよね。あそこに車がいるから，ちょっと遅くなりましょうといった形で連携がうまくいくんですね。その意味でAIネットワークが物理的につながっているものを指すのか，何らかの形で連携しているものを指すのかというのが，大きいポイントになるので，どちらなのか定義してほしいですね。

宍戸：私の理解は，まさに物理ネットワークの話で，相互接続，相互運用と言っているのは，それぞれのAIがどういうふうに動いてるかは知らないけど，AI間同士で情報をやりとりして，お互いに理解できるようにするということではないですか。

鳥海：それは物理的につながっていなくてもできるので，ロジカルなネットワークでいいわけですよ。電気信号が飛ぶ必要はないわけです。

実積：電気信号が飛んでるイメージだと，今回の問題にしているところとは違う話だと思います。もしネットワークで電子的につながっているなら，全体を1個のAIとして定義すれば済む話で，連携の話は必要ないと思っているんです。スーパーAIを1個置いて，みんなそこからの指示に従えばいいだけですから。連携しなければいけないという原則がわざわざ必要なのは，頭脳が複数あって，それぞれ優劣がないから，どうしましょうかという局面のはずです。

鳥海：もしそうだとすると，やはりそのシステムは複雑系になりますね。とても難しい話にどうしてもなってくるっていうところで，「連携の原則」については，1年。あるいは1年は無理でも，半年間かけて，きちんと議論すべきところだと思います。

17　むすびに代えて

宍戸：AIネットワーク社会推進会議のAI開発ガイドラインを素材に非常に厳しいご意見を頂きましたが，今のディスカッションでも，分野横断的な協力の必要性がかなり見えてきたかなと思います。この点に関して，『情報法制研究』という雑誌，あるいは学会，財団への期待も込めて，実積さんと鳥海さんから一言ずつ，頂きたいと思います。

実積：情報法制研究所が，情報法研究所にならなかったという点に注目していただきたいなと思います。法制の「制」というのは法制度の「制」じゃなくて，技術を含む社会制度の「制」です。今回のガイドラインの話でもそうですが，技術者コミュニティの意見を聞かないまま法律家を中心にガイドラインを作ると，それはうまく働かない。鳥海さんからご指摘がありましたけれども，両者の架け橋の場がやっぱり必要で，情報法制研究所，情報法制学会はそういうものになっていただきたいなと思いますね。

法律の議論はもちろん大事だし，それで決まるところもあるんですが，プレイヤーが法律に従うかインセンティブを持つか否かという点を経済学者としては着目しています。従ったほうが得というインセンティブを社会全体で確保するような体制を技術者と法律家が手を携えて作るべきだろうし，そのためには密接な意見交換を実現する必要があります。ICTの世界は国境が関係ないので，従いたいとは思わない法律を日本で作ると，プレイヤーは海外にでかけて，そこから国内にサービスを提供するだけです。これでは，みんなが損をするので，それを避けるための場づくりが必要です。

宍戸：ありがとうございました。鳥海さん，お願いします。

鳥海：この議論も含めて，いろいろ話していると，やはり相互理解が非常に不足していると感じました。法律家のほうは，やっぱり法律がこうなって，しょうがないんだから，技術者がなんとかやれよという話をするし，技術者のほうは，法律家は技術が分かってないから，どうしようもないという言い方をする。だから衝突するんですね。

お互いに，もうちょっと相互理解を深めて，お互いに尊敬し合ってやれるというのは言い方がおかしいですけれども，もっと理解し合う場を設ける必要があり。たとえば私と実積さんはいろいろ一緒にやっているんで，わりとけんかをしながらも，お互いを理解できていくようになるわけですけども，そういう場すら持ってない人たちがほとんどですよね。

そういったときに，じゃあうまくいくようにしましょう，とお題目だけ唱えても当然うまくいかない。特に情報系の研究者は，ほんとに法律家の人たちは何も分かってないぜぐらいの認識でしかない状態なので，それをなんとかするのはすごく重要なことだと思うんですね。お互いが理解し合った上で，ではどうすべきだっていう議論をしないと。ただ，お互い理解し合うことが自分たちのメリットにならない。基本的には研究者は研究してればいいし，法律家は法律を作ってればいいから，お互い相手のことを考えてやらなくても回ってしまうんですよね。だから，対話へのインセンティブがない。ここは実積さんにお願いして，経済的にお互いに協力したほうがいいシステムを考えてもらいましょう。

宍戸：法律家は無知を自覚しているから入っていかないというところもあります。法律家は傲慢に見えるところもあると思いますが，しかしそれ以上に臆病なところが正直ありまして，今後，この『情報法制研究』というジャーナルの場で，ぜひ今後も分野間の対話のきっかけになる企画を，やらせていただきたいと思います。長時間にわたりましたけれども，座談会はこれで終わりにしたいと思います。ありがとうございました。

（2017年1月16日収録）

＊　本座談会で言及された「ガイドライン（案）」とは，総務省が2017年1月末まで実施した「『AI開発ガイドライン』（仮称）の策定に向けて整理した論点に関する意見募集」（http://www.soumu.go.jp/menu news/s-news/01iicpO1 02000054.html）当時のものである。総務省はその後も「AI開発ガイドライン」（仮称）の策定に向けて引き続き検討を進めており，2017年夏頃を目途に報告書を取りまとめる予定としていることにご注意いただきたい〔宍戸注記〕。

情報法制をめぐる動き（2016年7月～12月）

官公庁				その他		
月	日	発表元	概要	日	発表元	概要
7	1	経済産業省	FinTechの課題と今後の方向性に関する検討会合（FinTech検討会合）第1回会合を開催	6	欧州議会	最重要サービスがインターネット上の脅威に抵抗できるようにする指令を承認
	5	経済産業省	IoTセキュリティガイドラインを策定	8	日本ブロックチェーン協会	電子マネー・企業ポイント・仮想通貨の交換の可否の見解を公表
	7	総務省	「IoT／ビッグデータ時代に向けた新たな情報通信政策の在り方」（平成27年諮問第23号）に関する情報通信審議会からの第二次中間答申	12	欧州委員会	欧米間のプライバシーシールド開始を公表
	8	総務省	「新たな情報通信技術戦略の在り方」（平成26年諮問第22号）に関する情報通信審議会からの第2次中間答申を公表	14	欧州委員会	グーグルの比較ショッピング，広告関連慣行についてさらなる調査を行うことを公表
	8	総務省	情報通信審議会情報通信技術分科会技術戦略委員会　第2次中間報告書（案）に対する意見の募集の結果を公表	19	経団連	データ利活用推進のための環境整備を求める～Society5.0の実現に向けて
	11	IT総合戦略本部	シェアリングエコノミー検討会議第1回会議を開催	20	仏CNIL	Microsoft に Windows10 の問題について3ヶ月以内に法令を遵守するように要求
	15	総務省	個人情報の保護に関する実態調査＜結果に基づく勧告＞を公表	22	Niantic	ポケモンGO，スマートフォンアプリ国内サービス開始
	21	NISC	位置情報ゲーム「ポケモンGO」に関する注意喚起について			
	22	総務省	平成27年通信利用動向調査の結果を公表			
	29	総務省	平成28年「情報通信に関する現状報告」（平成28年版情報通信白書）の公表			
	29	経済産業省	原子力災害現地対策本部から株式会社ナイアンティックに対し「ポケモンGO」の設定について要請が行われたことを公表			
8	2	公正取引委員会	携帯電話市場における競争政策上の課題について公表	2	経団連	わが国の経済成長に資するコンテンツの海外展開支援の継続・拡充に関する緊急要望を公表
	3	NISC	企業経営のためのサイバーセキュリティの考え方（2日内閣官房策定）を公表	4	日本ブロックチェーン協会	BITFINEX社へのセキュリティ侵害に関する影響についてを公表
	26	個人情報保護委員会	「個人データの円滑な国際的流通の確保のための取組について」（7月29日決定）を公表	26	英ICO	WhatsAppとFacebookがターゲット広告向けにパーソナルデータを共用することに懸念を表明
	26	NISC	「安全なIoTシステムのためのセキュリティに関する一般的枠組」の決定についてを公表	29	全国消防連	「個人情報の保護に関する法律施行令の一部を改正する政令（案）」及び「個人情報の保護に関する法律施行令規則（案）」に関する意見（8月26日提出）を公表

				30	欧州委員会	アイルランドがアップルに対し最大130億ユーロの違法な税優遇を行ったと認定
				31	経営法友会	パブリック・コメントに付されていた「個人情報の保護に関する法律施行令の一部を改正する政令（案）」及び「個人情報の保護に関する法律施行規則（案）」について，意見を提出したことを公表
				31	全銀協	「個人情報の保護に関する法律施行令の一部を改正する政令（案）」および「個人情報の保護に関する法律施行規則（案）」に対する意見等について公表
9	1	内閣府	クレジットカード取引の安心・安全に関する世論調査	1	独バイエルン州	制裁に関するGDPRガイダンスを公表
	9	財務省	平成28年1月から6月までの税関における知的財産侵害物品の差止状況について公表	23	EDPS	ビックデータ時代における基本的権利の一貫した執行に関する意見を公表
	9	総務省	放送を巡る諸課題に関する検討会「第一次取りまとめ」及び意見募集の結果の公表	28	東京地裁民事29部	海外写真家の写真を複製した商品等について著作権侵害を認める判決
	12	内閣府	「行政手続における特定の個人を識別するための番号の利用等に関する法律別表第二の主務省令で定める事務及び情報を定める命令の一部を改正する命令案」に関する意見募集（パブリックコメント）の結果について公表	29	英ICO	英国がEUを離脱する前にGDPRが適用される可能性が極めて高く，GDPRについて整備を続けることを表明
	14	公正取引委員会	公取委，一般社団法人日本音楽著作権協会による審判請求の取下げについて（音楽著作物の著作権に係る著作権等管理事業者による私的独占事件）公表	29	日本通信	MVNO格安SIM市場倍増接続協定に関する命令を総務省に申し立て
	16	総務省	株式会社DEXに対する個人情報の適正な管理の徹底に係る措置（指導）を行ったことを公表	30	全銀協	個人情報の保護に関する基本方針の一部変更案」に対する意見について公表
	16	経済産業省	「大学における秘密情報の保護ハンドブック（案）」に対する意見募集の結果について公表	30	日本通信	訴訟の判決（第一審）に関するお知らせを公表
	16	IT総合戦略本部	第1回データ流通環境整備検討会を開催			
	20	消費者委員会	第233回消費者委員会本会議（機能性表示食品制度，オンラインゲーム）を開催			
	20	消費者委員会	スマホゲームに関する消費者問題についての意見～注視すべき観点～を公表			
	23	総務省	無線LANビジネスガイドライン第2版及び意見募集の結果の公表			
	26	特許庁	知財分野における地域・中小企業支援について「地域知財活性化行動計画」を決定したことを公表			

	26	国税庁	インターネット番組「マイナンバー（個人番号）と法定調書」を公表			
	27	閣議	個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律の施行に伴う関係政令の整備及び経過措置に関する政令を閣議決定			
	30	IT総合戦略本部	AI，IoT時代におけるデータ活用ワーキンググループ第1回会合開催			
	30	内閣府	「行政手続における特定の個人を識別するための番号の利用等に関する法律別表第一の主務省令で定める事務を定める命令の一部改正」に係る意見募集について（パブリックコメント）の結果について公表			
10	4	総務省	送を巡る諸課題に関する検討会視聴者プライバシー保護ワーキンググループ第1回会合を開催	3	日本ブロックチェーン協会	「ブロックチェーンの定義」を公開
	5	政令	個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律の施行に伴う関係政令の整備及び経過措置に関する政令（政令第324号）	4	日本ブロックチェーン協会	「仮想通貨に係る消費税について非課税取引扱いの要望」資料の公開
	7	総務省	「スマートフォンの端末購入補助の適正化に関するガイドライン」に沿った端末購入補助の適正化に係る携帯電話事業者への行政指導・報告徴求	7	消団連	「個人情報の保護に関する基本方針の一部変更案（新旧対照表）」に関する意見提出を公表
	7	経済産業省	ISOでブロックチェーンの国際標準化についての議論がはじまることを公表	19	知財高裁4判	本邦の英字新聞社の刊行書籍に係る印税等請求訴訟控訴審で，控訴人請求を一部認容し原判決変更
	11	経済産業省	日米IoT分野の協力に係る覚書への署名について公表	17－20	ICDPPC	第38回目のプライバシーコミッショナー会議がモロッコで開催され，100以上のDPAが集まり議論がなされる
	11	個人情報保護委員会	「平成27年度個人情報保護法の施行状況の概要」を公表	24	米NHTSA	米国運輸省，自動車のサイバーセキュリティ向上のための自動車業界に対するガイダンスを公開
	12	個人情報保護委員会	「平成28年度上半期における個人情報保護委員会の活動実績について」を公表	27	EU29条作業部会	より進んだ執行協力の一環として，WhatsAppとYahooに対してプライバシー侵害懸念の書簡を送付
	14	閣議	「サイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律の施行期日を定める政令」及び「情報処理の促進に関する法律施行令の一部を改正する政令」が閣議決定			
	14	IT総合戦略本部	データ流通環境整備検討会オープンデータワーキンググループ第1回会合開催			

	19	政令	サイバーセキュリティ基本法及び情報処理の促進に関する法律の一部を改正する法律の施行期日を定める政令（政令第 329 号）			
	19	総務省	「視聴環境の変化に対応した放送コンテンツの製作・流通の促進方策の在り方」を情報通信審議会へ諮問			
	19	経済産業省	情報処理の促進に関する法律施行令の一部を改正する政令案等に対する意見募集結果を公表			
	20	IT 総合戦略本部	データ活用基盤・課題解決分科会第 1 回会合開催			
	21	経済産業省	「情報処理安全確保支援士」制度を開始			
	25	IT 総合戦略本部	データ活用基盤・課題解決分科会第 1 回会合開催			
	28	個人情報保護委員会	「個人情報の保護に関する基本方針の一部変更案」に関する意見募集の結果について公表			
11	1	総務省	「スマートフォンの端末購入補助の適正化に関するガイドライン」に係る携帯電話事業者への行政指導・報告徴求に対する報告	2	全銀協	「個人情報の保護に関する法律についてのガイドライン（通則編，外国にある第三者への提供編，第三者提供時の確認・記録義務編及び匿名加工情報編）（案）」に対する意見等について公表
	4	総務省	宇宙 × ICT に関する懇談会第 1 回会合を開催	2	知財高裁第 4 部	レコード製作者としての著作隣接権及び実演家としての著作隣接権を有する被控訴人から委託を受けた甲社との再委託契約に基づき，複製されたＣＤのレンタル事業者への販売及び楽曲の配信を行った控訴人は，被控訴人の許諾の有無を確認すべき条理上の注意義務を負う等と判決
	7	IT 総合戦略本部	シェアリングエコノミー検討会議中間報告書	2	新聞協会	個人情報保護法ガイドライン（案）に対する意見を公表
	7	IT 総合戦略本部	データ活用基盤・課題解決分科会　規制制度改革ワーキングチーム第 1 回会合開催	3	独 DPA	EU 域外へのパーソナルデータの国際移転に関する調査を開始したことを公表
	8	個人情報保護委員会	「国際的な取組について」決定を公表	15	欧州委員会	8 つの新プロジェクトを承認（EU のデジタル単一市場戦略関連　個人データ保護，サイバースペースの信頼性とセキュリティ，電子的証拠への越境アクセス，ICT 標準化等）
	11	政令	行政手続における特定の個人を識別するための番号の利用等に関する法律附則第三条の二の政令で定める日を定める政令（347 号）	17	ロシア	データローカライゼーション要求の一環として，LinkedIn をブロック
	15	規則	特定個人情報の取扱いの状況に係る地方公共団体等による定期的な報告に関する規則（個人情報保護委規則 4 号）			

12	5	経済産業省	「秘密情報の保護ハンドブックのてびき；情報管理も企業力」を公表	12－13	EU29条作業部会	データポータビリティ，DPO，主たる監督機関に関するガイドラインについて公表
	7	法律	「官民データ活用推進基本法」が参議院本会議で可決・成立			
	8	個人情報保護委員会	「個人データの漏えい等の事案が発生した場合等の対応について（案）」を公表			
	9	総務省	「地域IoT実装推進ロードマップ」及び「ロードマップの実現に向けた第一次提言」を公表			
	13	省令	行政手続における特定の個人を識別するための番号の利用等に関する法律の規定による通知カード及び個人番号カード並びに情報提供ネットワークシステムによる特定個人情報の提供等に関する省令の一部を改正する省令（総務省令96号）			
	13	総務省	行政手続における特定の個人を識別するための番号の利用等に関する法律の規定による通知カード及び個人番号カード並びに情報提供ネットワークシステムによる特定個人情報の提供等に関する省令第四十四条第二項第五号，第四十五条第一項第四号及び第五号，第四十六条第三項第二号並びに第四十七条第一項第三号の規定に基づき総務大臣が定める事項の一部を改正する告示（総務省告示435号）			
	15	個人情報保護委員会	「行政手続における特定の個人を識別するための番号の利用等に関する法律第十九条第八号に基づく特定個人情報の提供に関する規則（案）」及び「行政手続における特定の個人を識別するための番号の利用等に関する法律第十九条第八号の規定により提供することができる特定個人情報の範囲の限定に関する規則（案）」に関する意見募集の結果を公表			
	15	NISC	「情報セキュリティハンドブックver2.00」を公表			
	20	個人情報保護委員会	改正個人情報保護法の全面施行日について平成29年5月30日とすることを公表			
	22	省令	行政手続における特定の個人を識別するための番号の利用等に関する法律の規定による通知カード及び個人番号カード並びに情報提供ネットワークシステムによる特定個人情報の提供等に関する省令の一部を改正する省令（総務省令99号）			

	28	政令	行政手続における特定の個人を識別するための番号の利用等に関する法律の一部の施行期日を定める政令（政令第405号）			
	28	政令	個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律の一部の施行期日を定める政令（政令第406号）			
	28	経済産業省	「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」の改正案に対する意見公募の結果を公表			

作成：加藤尚徳（KDDI総合研究所アソシエイト）

情報法制学会　記事

1　発起人会

平成 28 年 12 月 23 日，発起人会を開催し，以下の事項について協議・決定した。

① 情報法制学会の設立趣旨を了承した。
② 情報法制学会規約を決定した。
③ 第 1 期運営委員及び監事として次の者を選任した。
運営委員　上原哲太郎，坂井修一，宍戸常寿，実積寿也，新保史生，鈴木正朝，曽我部真裕
監事　堀雅文
④ 事務局を一般財団法人情報法制研究所に委託することにした。

2　運営委員会

平成 28 年 12 月 23 日，運営委員会を開催し，以下の事項について協議・決定した。

① 代表に曽我部真裕運営委員を選任した。
② 第 1 期編集委員として次の者を選任した。
上原哲太郎，坂井修一，宍戸常寿，実積寿也，新保史生，鈴木正朝，曽我部真裕

3　編集委員会

平成 28 年 12 月 23 日，編集委員会を開催し，以下の事項について協議・決定した。

① 委員長に宍戸常寿編集委員を選任した。
② 『情報法制研究』創刊号企画案を決定した。

一般財団法人情報法制研究所　記事

1　一般財団法人情報法制研究所の設立

平成 28 年 6 月 23 日，一般財団法人として情報法制研究所が設立された。

2　評議員会

⑴　平成 28 年 3 月 13 日，第 1 回評議員会を開催し，理事・監事として次の者を選任した。

理事　上原哲太郎，江口清貴，宍戸常寿，実積寿也，鈴木正朝，曽我部真裕，高木浩光，鳥海不二夫，名和利男

監事　丸山満彦

⑵　同年 5 月 14 日，第 2 回評議員会を開催し，理事として次の者を選任した。

奥村裕一，堀雅文

⑶　同年 12 月 23 日，第 3 回評議員会を開催し，次期理事・監事として次の者を選任した。

理事　上原哲太郎，江口清貴，奥村裕一，宍戸常寿，実積寿也，鈴木正朝，曽我部真裕，高木浩光，鳥海不二夫，名和利男，堀雅文

監事　丸山満彦

3　理事会

⑴　平成 28 年 3 月 13 日，第 1 回理事会を開催し，以下の事項について協議・決定した。

①　代表理事・理事長に鈴木正朝理事を選任した。
②　専務理事兼事務局長に江口清貴理事を選出した。
③　情報法制研究所を一般財団法人として設立し登記することについて承認した。
④　従たる事務所の開設と事務所賃貸借の件について承認した。
⑤　「一般財団法人情報法制研究所」設立記念シンポジウムの開催について承認した。
⑥　会員制度及び会費について協議した。
⑦　主席研究員及び研究員の委嘱について協議した。

⑵　同年 5 月 14 日，第 2 回理事会を開催し，以下の事項について協議・決定した。

①　理事及び参与等への国際会議の旅費宿泊費等の補助について協議した。
②　第 1 期事業計画案及び予算案について協議した。
③　評議員会の決定により，理事の選任（追加）について報告があった。

⑶　同年 8 月 17 日，第 3 回理事会を開催し，以下の事項について協議・決定した。

①　従たる事務所の開設と設立費用について承認した。
②　顧問及び参与として以下の者を推薦することを決定した。

顧問　辻井潤，前川喜久雄，森田朗

参与　石井夏生利，板倉陽一郎，小向太郎，新保史生，高野一彦，湯浅墾道

③　正会員の入会について，法人会員 2 名を承認した。
④　研究所の組織と運営方針，年間予定について承認した。
⑤　第 1 期事業計画及び予算について承認した。

⑷　同年 12 月 23 日，第 4 回理事会を開催し，以下の事項について協議・決定した。

①　第 1 期補正予算について承認した。
②　第 2 期事業計画について承認した。
③　第 2 期予算について承認した。
④　研究員の選任方法について承認した。
⑤　情報法制学会への貸与について承認した。
⑥　次期代表理事・理事長として鈴木正朝理事を選任した。
⑦　次期専務理事兼事務局長に江口清貴理事を選任した。

4　「一般財団法人情報法制研究所」設立記念シンポジウム

平成 28 年 5 月 14 日，東京大学伊藤国際学術研究センターにおいて，設立記念シンポジウムを開催した。

- 主催者挨拶　坂井修一
- （特別講演）日本の情報法制研究の歴史・現在・未来―「情報法」提唱者の回顧と展望―　堀部政男
- 情報法制研究所の設立趣旨について　鈴木正朝
- 行政機関等個人情報保護法の改正・改正個人情報保護法の施行準備　宍戸常寿
- 通信の秘密の守備範囲　曽我部真裕
- 個人情報関連法の再編成に向けて　高木浩光
- 自治体セキュリティ強靭化策と番号関係の実務　上原哲太郎
- 経済学的に最適なセキュリティ水準　実積

寿也
- ネットコミュニケーションにおけるリスク分析　鳥海不二夫
- サイバーテロ・情報セキュリティ対策　名和利夫

5　第1回情報法制研究所情報法セミナー

平成28年11月5日，京都大学において，情報法セミナーを開催した。
- 趣旨説明　曽我部真裕
- 個人情報保護法制の現状　板倉陽一郎
- インハウス視点のインターネット法制　丸橋透

6　第2回情報法制研究所情報法セミナー

平成29年1月31日，東京大学において，情報法セミナーを開催した。
- 改正個人情報保護法の各種ガイドライン（個人情報保護委員会ガイドライン（四種＋漏えい等対応）及び電気通信分野，放送分野，金融分野，信用分野，債権管理回収業分野各ガイドライン）の解説　板倉陽一郎
- EU一般データ保護規則に関する第29条作業部会のガイドライン（データ保護責任者，データポータビリティの権利，管理者又は処理者の主催監督当局の特定）（2016年12月13日付）の解説）　杉本武重

情報法制学会規約

平成 28 年 12 月 23 日制定

第 1 章　総則

（名称）
第 1 条　本会は情報法制学会（Association of Law and Information Systems）と称する。

（事務所）
第 2 条　本会の事務所は，東京都千代田区永田町 2 丁目 17 番 17 号アイオス永田町 312　一般財団法人情報法制研究所に置く。

第 2 章　目的及び事業

（目的）
第 3 条　本会は，情報，メディア等に関する法，技術及びビジネスの観点からの学術的，実務的な研究（以下「情報法制研究」という。）を促進することを目的とする。

（事業）
第 4 条　本会は，前条の目的を達成するため，情報法制研究に関する次の事業を行う。
一　国内及び海外の動向等に関する調査研究及び研究成果の公表
二　研究者の連絡及び協力促進
三　研究会及び講演会の開催
四　機関誌その他図書の刊行
五　外国の学界との連絡及び協力
六　前各号のほか運営委員会において適当と認めた事業

第 3 章　会員

（資格）
第 5 条　本会の会員となることができる者は，情報法制研究に携わる者または情報法制研究に関して学識，経験を有する者とする。

（入会）
第 6 条　本会の会員になろうとする者は，別に定める入会申込書を提出し，運営委員会の承認を得なければならない。

（会費）
第 7 条　会員は，総会の定めるところに従い，会費を納めなければならない。

（退会）
第 8 条　会費を滞納した者は，運営委員会において，退会した者とみなすことができる。

第 4 章　機関

（役員）
第 9 条　本会に左の役員を置く。
一　運営委員若干名，内 1 名を代表とする。
二　監事若干名

（選任）
第 10 条　運営委員及び監事は，総会において選任する。
2　代表は，運営委員会において互選する。

（任期）
第 11 条　代表，運営委員及び監事の任期は，2 年とする。
2　補欠の代表，運営委員及び監事の任期は，前項の規定にかかわらず，前任者の残任期間とする。
3　代表，運営委員及び監事は，再任されることができる。

（代表）
第 12 条　代表は，本会を代表し，総会及び運営委員会を招集し，会務を統轄する。
2　代表に故障のある場合には，その指名した他の運営委員が，その職務を代行する。

（運営委員）
第 13 条　運営委員は，運営委員会を組織し，会務を執行する。

（監事）
第 14 条　監事は，会計及び会務執行の状況を監査する。

（総会）
第15条　代表は，毎年1回，会員の通常総会を招集しなければならない。
2　代表は，必要があると認めるときは，何時でも臨時総会を招集することができる。
3　総会員の5分の1以上の者が，会議の目的たる事項を示して請求したときは，代表は臨時総会を招集しなければならない。

（議決権の委任）
第16条　総会に出席しない会員は，書面により，他の出席全員にその議決権の行使を委任することができる。この場合には，これを出席とみなす。

第5章　規約の変更及び解散

（規約の変更）
第17条　本規約は，総会員の3分の2以上の同意がなければ，これを変更することができない。

（解散）
第18条　本会は，総会員の3分の2以上の同意がなければ，解散することができない。

附則

（施行期日）
第1条　本規約は，平成29年2月1日から施行する。

（発起人会の権限）
第2条　情報法制学会発起人会は，第1回会員総会が開催されるまでの間，総会の権限を行使することができる。ただし，発起人会の決定は，第1回会員総会においてその承認を受けなければならない。

Summary

Laws on Privacy and Personal Data Protection in Canada

ISHII Kaori
Associate Professor, Faculty of Library, Information and Media Science, University of Tsukuba

This article overviews laws and recent developments on protecting privacy and personal data in Canada, so that contribute to the future discussion in Japan. Canada has developed its own privacy and personal data protection system in line with respecting the efforts taken by the European Union and the United States. Privacy by Design, advanced by Dr. Ann Cavoukian, has been acknowledged worldwide. I have dealt with these surroundings on privacy and personal data protection in Canada in this article.

The challenges which can be found from overviewing Canadian legislations are, for example, the limitations of Ombudsmen authorities both in the federal and the provincial level; the need for obliging Privacy Impact Assessments and data breach notifications; the issue on the jurisdiction between the federal law and provincial laws; data localization provisions enacted in a specific province, the concern about the "adequacy decision" made by the European Commission.

Privacy by Design has played an important role to heighten the international presence of Canada, done by its special efforts. It has become well known also among Japanese stakeholders. However, we have not only to understand the notion of Privacy by Design, but also to consider how to implement the foundational principles.

Trying to solve the domestic issues along with harmonizing the international developments is the common need both in Canada and Japan. It is necessary to continuously look at discussions in Canada because they are instructive for Japanese discussions.

A Study of a Contract about Privacy (1)

ITAKURA Yoichiro
Attorney at Law, Hikari Sogoh Law Offices

This study includes 1) Introduction 2) The analysis of a contract about privacy from the viewpoint of substantive law, 3) The analysis of a contract about privacy from the viewpoint of procedural law, 4) The future discussion point of a contract about privacy. In Vol. (1), especially why people make a contract about privacy is discussed.

FCC's New Privacy Regulation on ISPs: Regulation on ICT Industry in Rapid Change

KOMUKAI Taro
Professor Nihon University

Federal Communications Commission (FCC) in the U.S. adopted an Order for new privacy regulation on providers of BIAS (Broadband Internet Access Service) on 27 in October, 2016. The new rule, with more strict restriction to ISPs to collect, use, and disclose their customers' information, does not cover edge providers such as Google, Facebook, Twitter, etc., and it is a hot issue that which operators should be subject to strict privacy regulation in ICT business field. This paper focuses on the purpose and background of FCC's new regulation and try to reach some suggestion about the issue.

Decisions on Removing Internet Search Results —So-called "The Right to Be Forgotten" in Japan

SHISHIDO George
Professor, University of Tokyo

Network Neutrality and Zero-Rating

JITSUZUMI Toshiya
Professor, D.Sc., Kyushu University

With the boom in bit-intensive and live streaming content in the broadband Internet ecosystem, accompanied with growing market power of network operators, “network neutrality” has become the focus of discussion among various stakeholders. In addition, the recent popularity of zero-rating options in mobile broadband businesses has made this problem even more complicated to be dealt with. This paper summarizes the essence of the “network neutrality” problem and an approach of the Japanese government, and discuss how zero-rating will affect its approach to this problem and what is required in the future policy making.

The General Overview of Robot Law by Interdisciplinary Legal Fileds

SHIMPO Fumio
Professor, Faculty of Policy Management, Keio University

This paper focuses on the overview of the importance of legal issues which will underpin a future Robot Symbiosis Society.I would like to refer to the necessity of proceeding with academic research regarding Robot Law including AI and the Internet of Things, (IoT) and then tried to conduct research in the various, connected, interdisciplinary fields such as constitutional law, administrative law, civil law and criminal law.The current legal system is unlikely to be able to solve the conundrum of every potentially serious problems in a very different and new,autonomoous robot use environment.I really believe that it is possible for us all to provide the legal framework necessary to underpin this new social system.

Recent developments of Child Protection on Mobile Internet

SOGABE Masahiro
Professor, Kyoto University

1. Introduction
2. Existing Scheme and its limits.
   (1) Existing Co-regulative Scheme
   (2) Its Effectiveness and Limits
3. Debate for New Scheme
   (1) Task Force at the MIC(Ministry of Internal Affairs and Communications)
   (2) Ad hoc Meeting for Facilitating Parental Control and Proposal by the TCA (Telecommunications Carriers Association)
   (3) New functions of the EMA(Content Evaluation and Monitoring Association)
4. Comments

Towards a Regulation for Personal Data Protection rather than for Personal Information Protection to Unify Provisions of Private and Public Sector (I)

TAKAGI Hiromitsu
Senior Researcher, National Institute of Advanced Industrial Science and Technology (AIST)

The discussions made in the revision of the Act on the Protection of Personal Information in 2015 revealed the issues that could not be achieved with the amendment, and highlighted that a number of unresolved problems remain in current legislation. One of the issues that could not be achieved is that it was not realized despite being understood that it was necessary to include individual behavioral data recorded with device identifier as the subject of protection under the Act. And the unresolved problem with current legislation is, for example, that the interpretation of the sentence "can be easily matched with other information" in the definition of personal information has not been clarified.

This series of papers attempts to propose a direction to solve the remaining issues for the next revision of the Act. Specifically, by focusing on the difference between "personal information" and "personal data", by clarifying the difference in interpretation between the sentence "can be easily matched with" and "can be matched with", we aim to unify only the provision on "personal information file" in the private sector and the public sec-

tor.

The following Part I, unresolved issues are listed, and what is the problem with each issue is shown.

Status Quo and Problems on Protection of Personal Information in Special Local Public Entities

YUASA Harumichi
Professor, Institute of Information Security

This article puts questions of protection of personal information on special local public entities. In recent years, many special local public entities were founded as a way out of fiscal difficulties of local government in Japan. These special local public entities must not be excluded from the municipality proscribed in the law of protection of personal information. Some of special local public entities, however, have no authority to enact their ordinance of protection of personal information to protect personal information of their inhabitants, and they must be covered by the ordinance of ordinary local public entities.

■編集後記

ここに，「情報法制研究」の創刊号を発行します。創刊及び当会の設立の趣旨等は，曽我部真裕代表の「『情報法制研究』創刊号に寄せて」をご覧ください。発刊に当たっては，企画から編集に至るまで，有斐閣の多大なるご尽力を得ました。深く御礼申し上げます。

創刊号は「情報法制学会設立記念」として，当会の立ち上げに関わった研究者・実務家に加え，日本の情報法学の創設者である堀部政男先生からも，ご寄稿を頂きました。引き続き，幅広い分野から質の高い論文等を掲載して，情報法制の発展に資するジャーナルを目指していきたいと考えています。

また，第3号（2018年5月刊）から，査読論文を掲載していく予定です。査読制度や査読要領については学会ウェブサイト等でも発信していきます。奮ってご応募ください。

今後とも，当会及び「情報法制研究」をご愛読の上，暖かいご支援を賜りますよう，お願い申し上げます。　（宍戸常寿）

情報法制研究　第1号

Journal of Law and Information Systems, Vol.1

□2017年5月1日発行

□発行　情報法制学会　代表・曽我部真裕
URL: https://www.jilis.org/alis.html
□組版　萩原印刷株式会社
□印刷・製本
株式会社デジタルパブリッシングサービス
□発売　株式会社有斐閣
〒101-0051　東京都千代田区神田神保町2丁目17番地
電話：03-3265-6811　FAX: 03-3262-8035
URL: http://yuhikaku.co.jp/
□情報法制学会事務局
〒100-0014　東京都千代田区永田町2丁目17番17号 AIOS永田町312
電話：03-5789-5356（代表）
URL: https://www.jilis.org/alis.html
E-mail: alis@jilis.org