Title	インターネット時代の個人情報保護 : 実効的な告知と国家の両義性を中心に
Sub Title	Protection of personal information in the Internet era
Author	山本, 龍彦(Yamamoto, Tatsuhiko)
Publisher	慶應義塾大学大学院法務研究科
Publication year	2015
Jtitle	慶應法学 (Keio law journal). No.33 (2015. 10) ,p.181- 219
JaLC DOI	
Abstract	
Notes	論説
Genre	Departmental Bulletin Paper
URL	https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=AA1203413X-20151023-0181

インターネット時代の個人情報保護

――実効的な告知と国家の両義性を中心に――

山　本　龍　彦

Ⅰ．はじめに
Ⅱ．実効的な告知および同意・選択
Ⅲ．国家の両義性
Ⅳ．おわりに

Ⅰ．はじめに

本稿は、「インターネット時代の個人情報保護――個人情報の『定義』とプロファイリングを中心に」（以下、「前稿」と呼ぶ）[1] の続編である。本稿は、前稿で行った問題提起を踏まえて、本人「同意」の虚構性を改善するための手続・方法、具体的には、事業者等による利用目的や第三者提供の有無等の「告知（notice）」を実効化し、利用者による同意・選択の機会を実質的に確保するための手続・方法をどのように具現化していくのか（→Ⅱ）、インターネット空間と国家との関係をどのように考えていくのか（犯罪捜査などを目的とした捜査機関による同空間への立入りを適切に統制しながら、同空間の秩序形成に対する国家の積極的な役割をどのようにして担保していくのか。→Ⅲ）について若干の考察を加えるものである。

1）山本龍彦「インターネット時代の個人情報保護――個人情報の『定義』とプロファイリングを中心に」阪本昌成先生古稀記念論文集『自由の法理』（成文堂、2015 年秋刊行予定）。

Ⅱ．実効的な告知および同意・選択

1. 問題の所在

前稿で述べたように、プロファイリングないしこれに基づくパーソナライズドされた（差異化された）情報の提供が個人の権利・自由に重大な影響を与えるとすれば、それらの実施については、基本的に情報主体本人の同意が必要となるように思われる。また、周知のように、個人情報保護法（以下、「法」と呼ぶ）は、「個人情報」を「特定された利用目的の達成に必要な範囲を超えて」取扱う場合（いわゆる目的外利用。法 16 条 1 項）、あるいは「個人データ」[2] を第三者に提供する場合（いわゆる第三者提供。法 23 条 1 項）には、原則として本人の同意が必要であるとしている。これらの同意は、本人から「あらかじめ」なされることが要求され（いわゆるオプトイン方式）、情報の利活用を望む事業者にとってしばしば重い足枷になっている。そこで、少なからぬ事例において、事業者は、「利用目的」を――プロファイリングも包含しうるようなかたちで――あらかじめ比較的広くとり[3]、これを「公表」し[4]、情報の取得時に当該利用目的に関して同意があったものとみなしている。また、第三者提供についても、改正個人情報保護法案（以下、「法案」と呼ぶ）は、①第三者提供が利用目的に含まれることや、第三者提供される個人データの項目等について「本人が容易に知り得る状態」に置くことで公表するなどし、②オプトアウトの権利の存在およびその行使の具体的方法についても①と同様の方法で本人に告知し、③これらの事項について個人情報保護委員会に届け出た場合（法案 23 条 2 項）は、当該個人データの第三者提供について本人の同意があるものとみなしている（本人が上記②の権利を行使しない限りで、第三者提供について黙示的な同意があるものとみなされるわけである。なお、後述のように、個人情報保護委

2）「個人情報データベース等を構成する個人情報」のことをいう（法 2 条 4 項）。
3）もちろん、法律上は、利用目的は「できる限り特定しなければならない」（法 15 条 1 項）。
4）保有個人データに関する事項の公表を求める法 24 条 1 項等を参照されたい。

員会は、上記③の届出があったときは、当該届出にかかわる事項を公表しなければならない。法案 23 条 4 項）。

このように、日本の個人情報保護法制は、建前としては個人情報の利活用について広くオプトイン（本人の事前同意）を要求しつつも、実際には比較的広範な利用目的と第三者提供の可能性を「公表」することを担保に、「オプトアウト」（事後的選択の機会が保証されていることを前提とした、黙示的同意の擬制）を容認しているといってよいであろう。そうすると、ここで重要となるのは、この「公表」が実際に機能しているのか、すなわち、情報主体は実際に公表された文書（プライバシー・ポリシー等）を読み、その内容を理解しているのか、情報主体にオプトアウトの機会が実質的に与えられているのか、ということになろう。仮に我が国の個人情報保護法制が、公表・告知（notice）と同意・選択（choice）の実効性――オプトアウトの現実の availability――に少なからず依存しているとすれば、これらの問いに対し、いずれも肯定的な回答が与えられなければならない。

しかし、現実は、それとは逆の回答を示しうるように思われる。たとえば、上記「公表」は、多くの場合、ウェブサイトにおけるプライバシー・ポリシーの掲示によって行われるが、「社会科学における調査研究は、消費者がプライバシー・ポリシーを読んでいないか、理解していないこと、選択がどのように枠づけられるかに強く影響されること、不正確な多くの予見を抱いていることを明らかにしている」[5]。ある研究によれば、「調査対象の 64％が、スーパーマーケットが顧客の購入履歴等を他の企業に売ることを許されていることを知らないとされ、75％が、『ウェブサイトがプライバシー・ポリシーを有している場合に、それは当該ウェブサイトが私の情報を他のウェブサイトや企業と共有しないことを意味する』と誤信している」[6] とされる。たしかに、プライバシー・ポリシーは、難解な法律用語で長々と――フェイスブックのプライバ

5）Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583, 667（2014）.

6）*Id*.

シー・ポリシーは合衆国憲法よりも多くの文字（5,830 字）を含んでいる！[7]――書かれていることが多く、人間の限定合理性（bounded rationality）[8]や認知的限界（cognitive limitation）・認知的バイアス[9]からみても、これを読み、理解することは相当に困難といわざるをえない。実際、平均的な利用者は、オンライン上で出くわしたすべてのプライバシー・ポリシーを読み終えるのに、1日で 40 分かかるという。これは、利用者がプライバシー・ポリシーを真面目に読んだ場合、1 年で 244 時間、80 歳を寿命とすれば 1200 日――人生の 3 年以上――もかけなければならないことを意味する[10]。このような“現実”を考慮すれば、＜公表・告知 - 同意・選択＞モデルに依拠する個人情報保護制度は、現状において破綻しているともいえよう[11]。プライバシー・ポリシーは、利用者ないし消費者の権利保護のための文書というより、現実には企業の免責のための文書と化しているからである[12]。FTC のプライバシー・レポートも、「ほとんどのプライバシー・ポリシーが、企業のデータ実践を消費者に伝えることに関して概して無益（ineffective）である」という点につき、広範な

7）M. Ryan Calo, *Against Notice Skepticism in Privacy（and Elsewhere）*, 87 Notre Dame L. Rev. 1027, 1054（2012）.

8）Herbert a. Simon, Models of Man 196（1957）.

9）*See e.g.,* Jon D. Hanson & Douglas A. Kysar, *Taking Behavioralism Seriously: The Problem of Market Manipulation*, 74 N.Y. U. L. Rev. 630, 635（1999）.

10）Aleecia McDonald & Lorrie Cranor *The Cost of Reading Privacy Policies*, I/S: A Journal of Law and Policy for the Information Society, 2008 Privacy Year in Review issue（http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf#search='Aleecia+McDonald+%26+Lorrie+Cranor+The+Cost+of+Reading+Privacy+Policies', at 17-18）.

11）アメリカにおける＜告知 - 選択＞モデルの破綻を指摘する論者として、フレッド・ケイトやヘレン・ニッセンバウムなどがいる。*See e.g., Fred H. Cate, The Failure of Fair Infromation Practice Principles, in* Consumer Protection in the Age of ‘Information Economy’ 341, 343（Jane K. Winn ed., 2006）; Solon Barocas and Helen Nissenbaum, On Notice: The Trouble with Notice and Consent（Oct. 2009）, available at（http://www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf）（manuscript at 6）.

12）Omer Tene and Ponetsky, *To Track od “Do Not Track”: Advancing Transparency and Individual Control in Online Behavioral Advertising*, 13 Minn. J. L. Sci.& Tech. 281, 314（2012）.

コンセンサスが形成されている、と指摘している[13]。

2. 議論

⑴ アカデミズムにおける提案として

このような“現実”から、＜告知 - 選択＞モデルに長く依拠してきたアメリカでも、消費者の自律的な選択や市場の競争メカニズムを重視する同モデルを放棄して、より直接的で実体的な制約ないし義務を事業者に課していくべきであるという考え（直接規制モデル）が有力に説かれるようになってきている[14]。しかし、この見解は、技術革新や競争を妨げ、経済の活力を削ぐ可能性が高いこと、個人情報の利活用（パーソナライズドされた情報の配信等）を望む消費者の選好や自律を害しかねないこと、規制をなすに当たり政治過程にかかる負担が大きいことなどから、実際の政策への影響はいまだ限定的である[15]。むしろ、アメリカにおいては（後述するようにEUにおいても）、＜告知 - 選択＞モデルの基本的な枠組みを維持したうえで、行動経済学や心理学の知見を積極的に参照しつつ、より効果的な告知方法の導入や、利用者の選択機会の実質的な確保を目指す方向がとられているように思われる。

たとえば、カロ（M. Ryan Calo）は、人間の生理的・心理的反応を利用した「直感的告知（visceral notice）」の導入を主張している。カロは、人間の認知的限界に触れたうえで、「言葉が情報を伝える唯一の手段ではない」[16]と指摘し、その例として、デジタルカメラの人工的なシャッター音や、電気自動車等の人工的なエンジン音を挙げる。前者について、カロは、デジタルカメラによる被写体の同意なき撮影を防止するには、かかる行為につき事後に制裁を科したり、

13）Fed. Trade Comm'n, Protectig Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers 61（2012）, *available at*（https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf）［hereinafter Privacy Report］.

14）前掲注 11）参照。

15）*See* Calo, *supra* note 7, at 1048-1050.

16）*Id*. at 1034.

“デジタルカメラで同意なく撮影するべからず”と街頭に貼り紙を出すよりも、「シャッター音」をカメラに組み込み、周囲に対し撮影を直感的に――「音」として――知らせる方がはるかに効果的であるというのである[17]。また、後者についても、本来はエンジン音の出ない電気自動車等による人身事故を防止するには、標識等で――文字により――歩行者に注意を喚起するよりも、偽のエンジン音を自動車に組み込み、直感的に危険を察知させる方がはるかに効果的であるという[18]。このような例を踏まえて、カロは、オンラインプライバシーの保護にも直感的告知が有用であり、また必要であると主張するのである。彼によれば、「オンラインプライバシーにおける重要な問題の1つは、人々が、多様な企業や他の当事者によって当たり前に追跡されているにもかかわらず、人々がそれに気づいていない」という点にあるが、「アバター〔擬人化されたアイコン〕や、それと同種のデザインを組み込むこと」により「プライバシー・ポリシーができないような方法で、追跡されているという事実を人々に体感させる」ことができる[19]。カロは、このような直感的告知は、①消費者にインターネット広告会社等に追跡されていることを実際に気づかせ、②この追跡を侵害的で不快であると感じた場合には、それを拒否（オプトアウト）する実質的な機会を与えることになると指摘している[20]。カロの言葉を借りれば、「こうしたデザイン的介入（design intervention）は、プライバシー・ポリシーよりもはるかにわかりやすいかたちで、追跡の事実を伝えるものとなろう」[21]（ただしカロは、最終的には、デザイン心理学に基づく直感的告知とともに、要求に応じて利用可能となる詳細かつ専門的な告知も必要になるとしている）[22]。

17）*Id*. at 1036.

18）*Id*.

19）*Id*. at 1039.

20）「たとえば、インターネット上のそれぞれの広告ネットワークが、当該ネットワークが利用者を追跡しているという事実を示すために、スクリーンの下部にアバターをもつことを想像してほしい。利用者は、このアバターをクリックして、追跡からオプトアウトしうる（気が散るならば、アバターを隠すかもしれない）」。*Id*. at 1040.

21）*Id*.

また、カーネギーメロン大学の研究グループは、彼らのいう「プライバシー・ナッジ（privacy nudges）」に取り組んでいる[23]。「ナッジ（そっと押す）」とは、人間は周囲の環境やアーキテクチャによってその行動を大きく左右されるという行動経済学の知見[24]を踏まえて、環境・アーキテクチャを人為的に操作・デザインすることで、人間がよりよい決定を行う手助けをすることを意味する。「柔らかなパターナリスティックな介入（soft paternalistic intervention）」[25]とも称される考え方である。上述の研究グループは、これをオンラインプライバシーの世界にも応用し、利用者が自らのプライバシーに関してより良い決定・選択を行うことができるよう、環境的・デザイン的に「ナッジ」すべきであるというのである。たとえば彼らは、タイミングよくスクリーン上にショート・メッセージを出現させるなど、利用者がウェブサイト側に提供しようとしている情報がもつプライバシー上の含意をリアルタイムで利用者に知らせるインターフェイス・デザインを組み込むべきであるなどと主張している[26]。これも、カロの提案と同様、人間の認知的限界や認知的バイアスを真剣に受けとめて、「言葉」よりも――「言葉」とともに――「デザイン」によって＜告知‐選択＞の実効性を高めようとする見解であると位置づけることができる[27]。コーネル大学の研究などでは、実際にこうしたデザインが、利用者のプライバシー意識（awareness）を高め、自己に関する情報に対するコントロールを向上

22）*Id*. at 1062.

23）Rebecca Balebako et al., *Nudging Users Towards Privacy on Mobile Devices*, Workshop on Persuasion, Influence, Nudge and Coercion Through Mobile Devices（PINC at CHI-11）, http://ceur-ws.org/Vol-722/paper6.pdf#search='Nudging+Users+Towards+Privacy' ; Alessandro Acquisti. *Nudging privacy*: *The behavioral economics of personal information*. Security & Privacy, IEEE 7（6）:82−85（2009）.

24）たとえば、リチャード・セイラー＝キャス・サンスティーン（遠藤真美訳）『実践　行動経済学』（日経 BP 社、2009 年）参照。憲法学からの応答として、柳瀬昇「行動主義的な法と経済学の展開可能性」駒澤大学法学部研究紀要 69 号（2011 年）79 頁以下。

25）Omer Tene and Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 16 Yale J. L. & Tech. 59, 97（2013）.

26）Balebako et al., *supra* note 23; Tene and Polonetsky, *supra* note 25, at 97.

させると指摘されており[28]、ブラウザのアドオンとして、一部実現もされている（たとえば、Mozilla 社の Firefox ブラウザのアドオンである Collusion は、クッキーによって追跡されている状況をリアルタイムで可視化し、利用者“X”の行動追跡のために協力している広告ネットワークの範囲等を明らかにする）[29]。

⑵ 現実の規制として――「目立つ」から「感じる」へ？

アメリカにおいては、「規制者の提示するガイドラインは、これまでみてきたいくつかのアカデミックな提案のように革新的なものではなく、また義務的なものでもないが、今後の方向性のためにこうした業績を参照する意思を示してきている」[30]。実際に、アメリカにおけるいくつかの規制は、既に「告知が〔スクリーン上の〕目立つ場所に置かれること、可視的な特定のフォントを用いることを要求して」おり、「そのような規制は、最終的には、より直感的なデザイン的要素を要求または促進するような方向に拡張されるであろう」とも指摘されている[31]。

たとえば、カリフォルニア州のオンラインプライバシー保護法（California Online Privacy Protection Act of 2003）は、同州居住の「消費者に関する個人識別可能情報（personally identifiable information）を、インターネットを通じて収集する商業的ウェブサイトまたはオンライン・サービスの運営管理者は、そのプライバシー・ポリシーを、当該ウェブサイト上に目立つかたちで（conspicuously）

27）もっとも、カロは、以下のように述べ、自らの直感的告知論とプライバシー・ナッジ論との違いを説明している。「直感的なプライバシー告知の目標は、データが収集されているという意識や、関連する諸問題や諸事実に対する意識を作り出すことにあるのであり、消費者が〔データを〕提供すること自体を制止することにあるのではない。換言すると、告知の目標は、選好を操作することにあるのではなく、消費者に対して、彼らが自らの選好に基づいて行動するために必要な情報を与えることにある」。Calo, *supra* note 7, at 1046.

28）Tene and Polonetsky, *supra* note 25, at 98.

29）*Id*.

30）Felix T. Wu, *The Constitutionality of Consumer Privacy Regulation*, 2013 U. Chi. Legal F. 69, 77（2013）.

31）Calo, *supra* note 7, at 1059.

掲示しなければならない」[32]と規定している。また同法は、運営管理者が、当該プライバシー・ポリシーにおいて、「運営管理者が収集する個人識別可能情報の項目および運営管理者が当該情報を共有するかもしれない第三者を明示すること」、「プライバシー・ポリシーの実質的変更について消費者に告知するプロセスを記述すること」、「通時的で、第三者のウェブサイト〔等〕……を跨ぐような消費者のオンライン活動に関する個人識別可能情報の収集に対する選択権を行使する能力を消費者に付与するウェブブラウザ〔追跡拒否（do not track）〕……のシグナル〔等〕……に対して、運営管理者がいかに対応するのかを開示すること」、「消費者が運営管理者のウェブサイトまたはサービスを利用したときに、他の当事者が消費者のオンライン活動に関する個人識別可能情報を収集しうるかどうかを開示すること」、「〔追跡拒否に対する対応の開示のために〕……当該プライバシー・ポリシー上に、消費者の当該選択を可能にするためのプログラムまたはプロトコルに関する記述を含むオンライン上の場所へのハイパーリンクを明確かつ目立つような形式で提供すること」などを求めている[33]。さらに同法は、アイコンにより、プライバシー・ポリシーを実際に掲示しているウェブページへリンクさせる場合には当該アイコンの色、テキストリンクによりリンクさせる場合は、その文字や大きさについて規定するなど、プライバシー・ポリシーを「目立つかたちで」掲示するための具体的方法についても規定している[34]。

このように、カリフォルニア州では、法律により公表・告知のあり方を具体的に規定し、その実効化を図ろうとしていること自体興味深いが、2013年1月には、州司法長官が、モバイル・プライバシーに関する報告書を公表し、アプリケーション開発者は、センシティブ情報を収集するか、当該アプリケーションの基本的機能には必要のない個人識別可能情報を収集する場合には、利用者により効果的に警告（alert）するため、「特別な告知（special notices）」を行

32）Cal. Bus. & Prof. Code §22575（a）.
33）Cal. Bus. & Prof. Code §22575（b）.
34）Cal. Bus. & Prof. Code §22577（b）.

うべきであると勧告していることが注目される[35]。「カリフォルニア州の報告書は、特別な告知をどのようにデザインするかについて具体的に述べているわけではないが、実際の開示が、プライバシー・ポリシーにおける説明以上の何かを要求しうる、という発展途上中の認識（recognition）を反映している」[36]といえよう。

また、連邦レベルでも、たとえばFTCは、2012年のプライバシー・レポートにおいて、「企業はそのデータ実践の透明性を高めるべきである」との一般原則（Baseline Principle）の下、業界に対し、「プライバシーに関する説明を、より明確に、より簡潔に、より標準化（standardized）して行うこと」を求めている[37]。具体的に、同レポートは、機械可読ポリシー（machine-readable policies）やアイコン等を、透明性を改善し、告知の実効性を高める方策として積極的に推奨している。ここで、機械可読ポリシーとは、消費者のウェブブラウザのようなソフトウェア・ツールが自動的に読み取れるよう、標準的なコンピュータ言語で書かれた、ウェブサイトのプライバシー実践に関するステイトメントを意味する[38]。このような機械可読ポリシーをブラウザが読み込むと、「ブラウザは、当該ポリシーと消費者の……プライバシー選好とを比較し、かかる選好が当該消費者の訪れているウェブサイトの実践と合致しないことを消費者に知らせることができる」[39]。「もし消費者が自己に関する情報を第三者に売却するようなウェブサイトを訪れたくないと考えるならば、彼は、こうしたポリシーを認識し、かかるウェブサイトをブロックする……または警告を発するようなルールを設定することができる」[40]。プライバシー・レポートは、

35）Office of the Attorney General of California, *Privacy on the Go: Recommendations for the Mobile Ecosystem* 12（Jan 2013）, online at（http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/privacy_on_the_go.pdf#search='Office+of+the+Attorney+General+of+California+%2C+Privacy+on+the+Go'）.

36）Wu, *supra* note 30, at 76.

37）Privacy Report, *supra* note 13 , at 60.

38）*Id*. at 62.

39）*Id*.

「プライバシーに関する消費者の意思決定を単純化（simplify）するために、……機械可読ポリシーの使用と、アイコンや標準化されたポリシー・ステイトメントを組み合わせる」ことが有効であるとする識者の見解を紹介している[41]。

以上は、あくまでFTCの勧告的意見にとどまるものであるが、FTCは、その執行手続においても、いわゆる同意裁決（consent order）[42]に署名した企業に対して、効果的な告知のための具体的な手続を遵守するよう要求し、たとえば、位置の追跡プログラムが起動していることを利用者に告知するためのアイコンを利用することを求めている[43]。このようにみると、アメリカでは、行政機関による執行の場面でも、公表・告知の実効性に着目し始めていること、具体的には、プライバシー・ポリシーの形式的な審査にとどまらず、ウェブサイトやソフトウェア・プログラムのデザインないしアーキテクチャ的諸要素を考慮し始めていることがわかる[44]。

EUにおいても、規則提案に対する欧州議会の修正案（2014年）が、「標準化された情報ポリシー」の規定を追加し、アイコン等を用いた告知を要求するなど[45]、アメリカと同様、利用者の視覚等に訴えるような、より実効的な告知方法を法的に重視する方向を示し始めている。

3. 日本

以上みてきたように、アメリカやEUでは、従来の＜公表・告知 - 同意・選択＞モデルには一定の限界があるとの共通了解に基づき、その改善に向けて

40）*Id*.

41）*Id*. モバイルの文脈につき、*id*. at 63.

42）FTCの執行手続については、小向太郎「米国FTCにおける消費者プライバシー政策の動向」情報通信政策レビュー（総務省情報通信政策研究所）第8号（2014）100頁以下等参照。

43）*See* In re Aspen Way Enterprises, Inc., FTC File No. 112 3151, No. C-4392, at 5（F. T. C. Sept. 25, 2012）.

44）*See* Solove and Hartzog, *supra* note, at 669.

45）石井夏生利『個人情報保護法の現在と未来』（勁草書房、2014年）133頁、小林慎太郎『パーソナルデータの教科書』（日経BP社、2014年）134頁等参照。

一定の努力がなされてきたといってよい。とくに、アイコンの導入といったデザイン上の工夫による視覚的・直感的な告知は、法的な要求にもなりつつあると考えてよいであろう。では、日本の状況はどうであろうか。

前記(1)ではそれほど強調しなかったが、日本においても、告知方法について一定の前進はある。たとえば、オプトアウトによる個人データの第三者提供について、法は、第三者への提供を利用目的とすること、第三者に提供される個人データの項目、オプトアウトの権利の存在等につき、「あらかじめ、本人に通知し、又は本人が容易に知りうる状態に置いているとき」、明確な本人同意のない第三者提供を認めるものとしている（法 23 条 2 項）。これに対し、法案は、通知・公表事項として、「〔オプトアウトに関する〕本人の求めを受け付ける方法」を追加し、オプトアウトまでの導線を示すことを事業者に要求したうえ、こうした事項につき、「個人情報保護委員会規則で定めるところにより」、通知または公表するときに、上述の第三者提供を認めることとしている（法案 23 条 2 項。これらの手続に関する違反は、同委員会の勧告・命令の対象となる。法案 42 条）。さらに、個人情報保護委員会は、この届出があったとき、「当該届出に係る事項を公表しなければならない」とされた（法案 23 条 4 項）。いま述べた個人情報保護委員会による公表が一覧性のあるかたちで、同委員会のホームページなどでなされれば、情報主体は、当該ホームページを閲覧することで、自らの情報を保有する事業者の情報実践を知り、事業者の指示する「方法」に従ってオプトアウトの手続をとることが可能となる。その意味では、法案においては、従前よりも＜公表・告知 - 同意・選択＞の実効性が向上したと考えることもできる。

しかし、法案が要求する多くの公表（匿名加工情報の作成および第三者提供に関する公表〔36 条 3 項・4 項〕、保有個人データの利用目的の公表〔24 条 1 項〕等）は、個人情報保護委員会のホームページ等において一覧性のあるかたちで追加的に公表されるわけではない。そうすると、情報主体への告知という点で、やはり事業者自身による公表がポイントとなるが、その実効性や有効性を担保するような規定が、法案自体に置かれているわけではない。アメリカや EU で積

極的に議論されているような、アイコン等やブラウザ設定を用いた告知方法が、法律レベルで要求されているわけではないのである。ただ、経済産業省の2014年の調査報告書[46]は、消費者に対して行ったアンケート調査の結果を踏まえて、「写真、画面イメージ、キャラクター等の活用」や、「レイアウトや情報の流れに関する工夫」といったインターフェイスデザインが、プライバシー・ポリシーの「わかりやすさ」の実現のために重要であると指摘している[47]。また、一般社団法人インターネット広告推進協議会（JIAA）による「行動ターゲティング広告ガイドライン」は、2014年2月の改定により、「行動ターゲティング広告での行動履歴情報の利用における透明性の確保と消費者関与の機会の確保のために、広告内や広告周辺に共通のアイコンを表示して、情報の取扱いやオプトアウトの手段を消費者に知らせるための分かりやすい仕組み（インフォメーションアイコンプログラム）の導入」を推奨している[48]。

ここで改めて法案を参照すると、オプトアウトによる第三者提供を規定する法案23条2項は、同規定のいう通知・公表が、「個人情報保護委員会規則の定めるところにより」行われることを要求していることに気づく（法案36条3項は、匿名加工情報の作成に関する公表も委員会規則で定めるところによる、と規定している）。また法案は、個人情報保護委員会に「認定個人情報保護団体」を認定する権限を与え、当該団体が、「消費者の意見を代表する者その他の関係者の意見を聴いて、この法律の規定の趣旨に沿った指針」（個人情報保護指針）を作成することを認めている（法案53条）[49]。さらに法案は、個人情報保護委

46）経済産業省『パーソナルデータ利活用ビジネスの促進に向けた、消費者向け情報提供・説明の充実のための『評価基準』と『事前相談評価』のあり方について』（2014年3月26日）。

47）経済産業省・前掲注46）74−75頁参照。小林・前掲注45）167−168頁も、「消費者の理解を促進するためには、インターフェイスデザインは記載内容と同様に重要なのである」と指摘している。

48）JIAA・News Release「『プライバシーポリシー作成のためのガイドライン』と『行動ターゲティング広告ガイドライン』を改定」（2014年3月24日）（http://www.jiaa.org/dbps_data/_material_/common/release/guideline_release_140324.pdf）。

員会に規則制定権を付与するとともに（法案 65 条）、個人情報の適正な取扱いの確保を図るための基本方針を策定する権限を与えている（法案 52 条 1 号）。このようなルール形成に関する法案の枠組み[50]の下で、個人情報保護委員会は、事業分野別ガイドラインや、JIAA ガイドラインのような自主規制の一部を規則等に取り込み、あるいは、JIAA のような団体を「認定個人情報保護団体」として認定し、そのガイドラインを「個人情報保護指針」と位置づけることによって、先述のような公表・告知に関する新たな取組みを個人情報保護法の規制レジームに反映させていくことができるように思われる[51]。

もっとも、このような公表・告知方法の規制が、憲法 21 条の表現の自由と抵触しうることには注意が必要である。特定の告知方法を強制することは、「強制された言論（compelled speech）」に当たる可能性があるからである[52]（消極的表現の自由の侵害を構成しうる）。しかし、次の点に配慮することで、こうした憲法上の問題は回避できるように思われる。すなわち、一定の視覚的・直感的な告知を要求するとしても、その目的は、あくまでも情報主体が自らのプライバシー選好に基づいて行動するために必要な情報を与え、知らせること――“告知”――にとどまるべきであり、この選好を操作すること――“誘導”――であってはならない、ということである。アメリカ連邦控訴裁判所による R.J. Reynolds Tobacco Co. v. FDA 事件判決[53]（2012 年）は、アメリカ食品医薬品局（Food and Drug Administration, FDA）が、タバコのパッケージに記載するようタバコ会社に強制した視覚的な警告を、表現の自由を保障する修正 1 条に違

49）法案は、対象事業者が指針を遵守するよう、必要な措置をとる義務を認定個人情報保護団体に負わせている（法案 53 条）。

50）このような、業界による自主規制の策定に国家が一定程度関与する仕組みのことを、純然たる自主規制と区別して、「共同規制」と呼ぶことがある。後掲注 96）参照。

51）宍戸常寿も、認定個人情報保護団体をとおした、マルチステークホルダープロセスによるルール形成を通じて、オプトアウトの具体的な仕組みや、第三者提供等に関する本人同意の具体的な方法が発展していくことが「期待される」としている。宍戸常寿「個人情報保護法制」論究ジュリスト 2015 年春号 44 頁。

52）See Wu, *supra* note 30, at 72.

53）696 F.3d 1205（D.C. Cir. 2012）.

反すると判断したものであるが、そこでポイントとされたのは、強制したメッセージが、「純粋に事実的で議論の余地のない」情報ではなく、煽動的で、喫煙は悪であるとの特定の観点に立脚して喫煙者や潜在的喫煙者を怖がらせ、喫煙を思いとどまらせようとするものであった、ということであった。こうした判決の存在を踏まえると、事業者の情報実践に関する視覚的・直感的な告知も、仮にそれが「告知」の限界を超え、情報の利活用は悪であるとの特定の観点に立脚して情報主体を特定の行動に「誘導」する場合には、消極的表現の自由を不当に侵害するものとして違憲と評価されることはありうるように思われる[54]。我が国においても、公表・告知の実効化と、利用者の選択機会の実質的保障は喫緊の課題となりうるが、憲法21条との関係で、誰が、どのような形式で（法律か、規則か、指針か、自主規制か、等々）、どのような内容の告知および選択のあり方を要求するのかが具体的に問題となろう。

Ⅲ．国家の両義性

1．プライバシー侵害者としての政府

⑴　問題の所在

我が国の最高裁は、憲法13条は「みだりにその容ぼう・姿態……を撮影されない自由」[55]や、「みだりに指紋押なつを強制されない自由」[56]を保障していると述べてきた。こうした判例から、我々は、憲法13条により国家、とりわけ捜査機関から、個人情報をみだりに収集されない自由を有していると一般に考えられている[57]。また、憲法21条2項は、「通信の秘密」を規定している。このような憲法条文から、国家は、インターネットを媒介とした他者とのやりとりに関する記録（通信内容そのものに関する情報や通信履歴等）をみだ

54）See Calo, *supra* note 7, at 1070-1071.
55）最大判昭和44年12月24日刑集23巻12号1625頁。
56）最判平成7年12月15日刑集49巻10号842頁。
57）下級審のものとして、仙台地判平成24年3月26日判時2149号99頁。

りに収集すること、こうした記録をとおして我々のオンライン活動を理由なく監視することは憲法上禁止されていると考えてよい。

しかし、ここで注意を必要とするのは、インターネット空間が、基本的には、民間事業者によって「創造」[58] された民間インフラであるということである[59]。このことが捜査機関の活動に与える影響はきわめて大きい。たとえば、警察は、現実世界における道路等の公共インフラへは自由にエントリーできる。また、そこにおいては、警察は、人の往来を基本的には自由にチェックできるのである（この公共インフラにおいて怪しい行動をとる者がいれば、警察官はその者に直接アクセスし、警察官職務執行法2条1項に基づく職務質問等を行うこともできるであろう）。しかし、インターネット空間の場合、そうはいかない。この仮想世界は、それ自体、「私的」な空間であるから、そこでの「人」の往来や行動を警察がチェックし、把握するには、かかる〈世界〉の「創造主」[60] である民間事業者（主としてISPや携帯電話事業者）の協力がどうしても必要になるのである。比喩的にいえば、このインフラ管理者が、自ら構築した仮想世界のゲートを開放しない限り、基本的には――ハッキングやクラッキングなどの手段で強行的に侵入するならば話は別であるが[61] ――捜査機関はそこに立ち入

58）四方光は、「携帯電話事業者やISP等のネット・インフラ提供者は、いわばサイバー空間の創造主であ〔る〕」と述べている。四方光「我が国におけるサイバー犯罪の現状と若干の犯罪学的及び刑事政策学的考察」法学新報117巻7・8号（2011年）432頁。

59）もちろん、通信事業者が純然たる私人かどうかについては争いがあるが、憲法学の多数説は、通信事業者およびその職員に対して憲法が直接適用されるという考えは採用していない。宍戸502頁。なお、仮に、かつて国営企業であった日本電信電話株式会社や国際電信電話株式会社について憲法の直接適用を認めるとしても、ISPのように、もともと国営的性格を有しない企業に同じ論理は認められるかは疑問である。

60）四方・前掲注58）432頁。

61）このように国家自身が、スパイ・プログラムのインストールなどを通じて、秘密裡に情報システムに侵入して情報を取得する行為を「オンライン捜索」と呼ぶことがある。ドイツの連邦憲法裁判所は、2008年2月27日、このような手法を、一般的人格権の特別な具象化である「情報技術システムの秘匿性と十全性に対する基本権」を侵害し、違憲であると判断している（BVerGE 120, 274）。高橋和広「IT基本権論に関する一考察」六甲台論集61巻1・2号（2015年）39頁以下参照。

ることができない（以下、この問題を、便宜上「ゲート問題」と呼ぶ）。現実世界の公共的な交通網をとおって、ある商店を訪れるという人の行動を、捜査機関は直接把握できるのに対して、仮想世界の――民営の――交通網をとおって、ある「商店」（ウェブサイト）を訪れるという「人」の行動を、捜査機関はISP等の手を借りて、いわば間接的にしか把握できないというわけである。

いま述べたゲート問題は、インターネット空間において国家は、個人のプライバシーを直接には侵害できない――個人情報を直接には収集できない――ということを意味する。ゲートキーパーである通信事業者の協力的な行為を通じて、国家はこれを間接的・二次的にしか侵害できないのである[62)]。そうすると、個人のプライバシーないし個人情報は、かかる通信事業者と国家との間に一定の緊張関係が存することによって実効的に守られ、逆に、両者の間に蜜月の関係が成立することによって徹底的に侵害される。

実のところ、インターネット空間においてプライバシーの最大の侵害者となりうるのは、ISP等の通信事業者である。もちろんここで、現在、ISP等が最大の侵害者であるといいたいわけではない。なりうる資源を有している、といっているだけである。

どういうことか。インターネットの通信は、「パケット」に分けて行われる。このパケットが、「交通網」をとおって送信先に伝達されるのであるが、この交通網には、「ルータ」という中継地点が複数存在している。パケットには、その行先等を示す「ヘッダ情報」が付されており、ルータがこのヘッダ情報を読み取ることで、行先までパケットを伝達していくことになるのである。専門技術的な正確性を欠くが、敢えて現実世界とのアナロジーを用いれば、「パケット」は情報を載せる車両、「ヘッダ情報」はこの車両のフロント部分に取り付けられた、行先や車両の種類等を表示する情報（たとえば、バスのフロント部分には、当該バスの系統とともに「○×行き」との表示がなされている）、「交通

62）これは電話回線についても同じことがいえる（いわゆる通信傍録も、通信事業者の協力がなければ実行できない）。インターネットの発展により、こうしたゲート問題が遍在するようになったということができようか。

網」は道路、「ルータ」はジャンクションということになろう。ISP は、この「道路」と「ジャンクション」を管理し、車両の流れを制御していることになる。そこでは、ISP が、道路の渋滞を解消する措置を講じたり（たとえば、迂回するルートをとらせる）、交通の流れを妨げるような「大型トラック」――動画に代表される、大容量の情報を搭載したパケット――の運行を制限すること（いわゆる帯域制御）がある（ISP によるこうした制御が恣意的に行なわれてはならないというのが、いわばネットワーク中立性の原則である）[63]。また、このような交通の制御を行うために、ISP がジャンクション（ルータ）において車両検問を行い、「積荷」（パケットの内容）等を検査することがある（パケットの内容にまで踏み込んで深く点検することになるため、「DPI（Deep Packet Inspection）」[64] と呼ばれる）。要するに、ネットワーク管理者である ISP は、交通制御の名の下に、パケットの内容にまでかかわる個人に関する情報をほぼ無制限的に収集することができる立場にあるわけである（もちろん、ISP は、ヘッダ情報に含まれる IP アドレスと特定個人とを紐付ける情報を保有している）。

以上のようにみると、ISP 等は、やる気にさえなれば、インターネットを通じた特定個人の行動を、ほぼ全面的に把握することができると考えられる（もちろん、電気通信事業法上の「通信の秘密」に関する諸規定が、こうした行為を法的に制限しているわけであるが）[65]。これに対し、国家は、この交通網に自由に立ち入れないうえ[66]、仮に立ち入れたとしても、IP アドレス等のオンライン識別子と特定個人とを紐付ける情報をもたないがゆえに、直ちに特定個人の行動を追跡することができない。ここにおいては、ISP 等と国家との間に、圧倒的な情報の非対象性が存在することになるのである。

しかし、先にも触れたように、国家が、ISP 等の管理するゲートを突破し、犯罪捜査等の目的のために ISP 等を自由に「使用」することができるように

63）小向太郎『情報法入門〔第 3 版〕』（NTT 出版、2015 年）81 頁。

64）DPI に関する最新の論点については、林紘一郎＝田川義博「『心地よい DPI（Deep Packet Inspection）』と『程よい通信の秘密』」情報セキュリティ総合科学 4 号（2011 年）3 頁以下参照。

なったとき、あるいは、ISP 等と国家が蜜月の関係に入ったとき、状況は一変する。国家は、インターネット上における特定個人の行動を網羅的に把握し、その足跡（通信履歴等）に基づき、特定個人に関する詳細なプロファイルを作成することができるからである。そうすると、インターネット空間における、国家によるプライバシー侵害を考えるうえでの論点は、ISP 等が事実上管理する同空間のゲート開閉をどのような要件で認めるか、より一般的にいえば、ISP 等と国家との適切な緊張関係をどのように維持・構築するか、というところにある。

⑵ 議論

アメリカでは、インターネット空間のゲート、あるいは ISP 等と国家との間の壁は、電子通信プライバシー法（Electronic Communications Privacy Act, ECPA）によって管理されている。同法は、捜査機関がどのような個人情報を取得したいのか（情報の性質）によって、ゲートの開閉要件を変えるという考え方を採用している。たとえば、①特定の加入者情報ないし取引記録（氏名、住所、IP アドレス、メールアドレス等）や、ログインやログアウトしたときの IP アドレス、日付、時間については、捜査機関が ISP 等に対して召喚状（subpoena）を送付することによって入手可能とされる。この召喚状は、裁判所の審査を必要としないため、上述のゲート開閉の要件を最も緩く設定するものといえる（た

65）近年、ISP 等とインターネット広告会社が協力して、利用者のインターネット上の行動を追跡・分析することに強い懸念が表明されている。クッキー情報がウェブサイト単位での追跡を可能にするものであるのに対し、DPI に関する情報は、インターネットにおける利用者の全行動の追跡を可能にする。ただし、現在のところ、主要な ISP は、DPI の広告的利用は、利用者の同意がない限り行わないとの立場を維持しているようである。Omer Tene and Ponetsky, *To Track od "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising*, 13 Minn. J. L. Sci.& Tech. 281, 299（2012）. また、経済産業省「利用者視点を踏まえた ITC サービスに係る諸問題に関する研究会」第二次提言（平成 22 年 5 月）も、「DPI 技術を活用した行動ターゲティング広告の実施は、利用者の同意がなければ通信の秘密を侵害するものとして許されない」との見解を示している。

66）ただし、いわゆるオンライン捜索につき、前掲注 61）参照。

だし、この召喚状によって入手できる情報は、上述のような情報に限られる）。

他方、②当該アカウントから送信された特定のメールに関連づけられたメールアドレスや、メールの内容ではないヘッダ情報（送信元 IP アドレス、宛先 IP アドレス、日時のフィールド等）については、ECPA 上の裁判所命令を要するとされる。捜査機関がかかる命令を求める場合、裁判官に対し、入手したい情報が現在進行中の犯罪捜査に関連しており、重要であることを示す具体的な事実を提示しなければならない。

さらに、③ ISP 等が保存しているメールや画像等の内容、利用者の検索キーワードに関する情報については、裁判官が発付する捜索令状を要するとされる。捜査機関がかかる令状を求める場合、裁判所に対し、犯罪に関連する特定の情報が、捜査を行う特定の場所に現在あると信じる「相当な理由（probable cause）」を示し、かつ、捜索の対象等を特定しなければならない。ECPA は、通信の「内容」に関する情報については、それだけ先述のゲート開閉の要件を厳しく設定していると考えることができる（ただし、通信内容をリアルタイムで傍受する場合には、いわゆる傍受命令が必要となり、上述の捜索命令よりもさらに厳格な要求を満たさなければならない）。なお、捜査機関が前述したような通信履歴（通信ログ）に関する情報をリアルタイムで取得したい場合には、裁判官からいわゆるペンレジスター命令を得なければならない。しかし、その要件は厳格でなく、捜査機関は進行中の犯罪捜査と関連していることを示せば足りるとされている。

このように、ECPA を概観すると、アメリカでは、通信の「内容」にかかわるか、通信の「外容」ないし履歴にかかわるかによって、また、通信後に ISP 等によって保存されている情報か、通信中の情報か（リアルタイムでの取得か）によって、ゲート開閉の要件――ISP 等と国家との“距離”――を変えていることがわかる[67]。こうした ECPA の基本的な規律枠組みに対しては、捜査機関が入手を希望する情報の性質によってゲート開閉の要件に一定の差を設ける

67）概略について、山本龍彦「アメリカにおける対テロ戦略と情報プライバシー」大沢秀介＝小山剛編『自由と安全』（尚学社、2009 年）140 頁以下参照。

ことは首肯しうるとしても、「内容」情報とそうでない情報との間に、保護のレベルに関するコントラストをつけ過ぎなのではないか――通信履歴等を入手するに当たっての開閉要件が緩すぎるのではないか――との批判がある[68]。インターネット空間においては、通信履歴等の非内容的情報であっても、それらを広範に収集、蓄積、分析することによって、その者の思想傾向等を一定の精度でプロファイリングすることが可能となるからである。また、通信後か通信中（リアルタイム）かで、入手に関するハードルが変わることについても批判がある。

そこで、グーグル、マイクロソフト、アップル、アマゾンなどの名立たるIT関連企業が参加している「デジタル・デュー・プロセス（Digital Due Process）」連盟（coalition）[69]は、以下のような方向でのECPA改正を提案している（以下は、同連盟がECPA改正の際に考慮すべきと主張する4つの原則を、一部抜粋して要約したものである）。

（i） 第1原則：「政府機関は、……ECPAが適用対象とする事業者に対して、公衆にとって容易にアクセスされえない通信を開示するよう要求できるが、それは、通信が行われてからどれくらい経過したか、保存の手段・状態はどのようなものか、通常の業務の遂行における当該通信へのプロバイダーのアクセス・利用はどのようなものかにかかわらず、相当な理由の証明に基づいて発付された令状がある場合に限られる」。

第1原則の背景：「政府は、利用者の私的通信またはオンライン上の保存文書を開示するようISPに強制する前に、相当な理由に基づく捜索令状を得なければならない」。「この原則は、法が伝統的に、電話のコール、……保存ファイル、文書、インターネット『クラウド』において保存された私的な内容または『ク

68）*See e.g.*, Daniel J. Solove, *Reshaping the Framework: Electronic Surveillance Law*, 72 Geo. Wash. L. Rev. 1264, 1287-1288（2004）.

69）Digital Due Process, *Modernizing Surveillance Laws for the Internet Age, available at*（http://digitalddueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163）.

ラウド』を通じて伝達される内容――私的なEメール、……テキスト・メッセージ、ワープロを使用した文書、……写真、インターネット検索ワード等――について規定してきたセーフガードに対して適用される」。

(ii) 第2原則：「政府機関は、移動体端末に関する位置情報を提供するよう、事前または事後に、ECPAが適用対象とする事業者に要求し、またはアクセスすることができるが、それは、相当な理由の証明に基づく令状に基づく場合に限られる」。

第2原則の背景：「政府は、携帯電話その他の移動体端末の位置を、事前または事後に追跡する前に、相当な理由に基づく捜索令状を得るべきである」。「リアルタイムでなされる携帯電話の追跡には捜索令状が要求されるが、保存された位置データへのアクセスに対しても同じ基準が適用されうるというのが、多くの裁判所が到達した結論であり、本原則の支持する結論でもある」。

(iii) 第3原則：「政府機関は、……ダイヤルした番号情報、Eメールの宛先・宛名情報その他のデータを提供するよう、事前にまたはリアルタイムで、ECPAが適用対象とする事業者に要求し、またはアクセスすることができるが、それは、司法審査および、政府機関が少なくとも……〔従来求められていたもの〕よりも厳格な証明をなしたこと〔事実的証明。後述の「背景」を参照〕を裁判所が認めた後にのみ可能である」。

第3原則の背景：「Eメール、インスタント・メッセージング、テキスト・メッセージング、電話その他の通信技術を用いて、ある個人がいつ、誰と通信をしたかに関する取引データをリアルタイムで得る前に、政府は、裁判所に対して、当該データが正当な犯罪捜査と関連するものである（relevant）ことを証明するべきである」。「2001年に、『ペンレジスターおよびトラップ＆トレイス装置』――電話により、個人がいつ、誰と通信をしたかに関する取引データをリアルタイムで得る技術――に関する法が、インターネットにおいてなされる通信をモニタリングできるようなかたちで拡大された」。「この原理は、入手しようとする情報が、現在捜査中の犯罪と関連している（relevant）と信じるに足る合理

的根拠の事実的な証明（factual showing）に基づき、当該データに対する監視要請の司法審査を組み込むことによって、同法を、現代の情報技術に適合するようアップデイトするものである」。

(iv) 第4原則：「保存通信法（Stored Communications Act, SCA）が、情報獲得のための召喚状を認めるとき、政府機関は、当該召喚状を、特定のアカウントまたは特定の個人に関連した情報についてのみ用いることができる。特定されないすべての要求は、司法的な承認に服しなければならない」。
第4原則の背景：「被疑者を捜査している過程で、……通信その他のオンライン・サービスの、複数の不特定的な利用者に関する取引データを得る場合、事前に、政府は、裁判所に対して、当該データが当該犯罪捜査のために必要であることを証明すべきである」。「本原則は、政府が、捜査と関連する特定の個人の記録を求めるのではなく、電話またはインターネット利用者の一定のカテゴリーに対して、広く大量の情報を得るために召喚状を用いるような状況に対処するものである」。その例として、たとえば、「ある特定の日に、ある特定のウェブサイトを訪れたすべての者に関する情報を広く要求するケース」が考えられる。「あるクラスに属する特定されない個人に関する情報を包括的に得ようという要求は、独特（unique）のプライバシー上の利益にかかわるために、本原則は、そのような大量のデータが、ある捜査と関連していることを裁判所に示す、という〔比較的厳格な〕基準を適用している」。

いまみてきたような提案は、大要、通信履歴のような非内容的情報の保護を――「内容」情報の保護と同レベルとはいわないまでも――底上げし、かつ、リアルタイムか保存された状況か、というタイミングによる取得基準のバラツキを抑制しようという狙いを有するものといえよう。

なお、グーグルは、グーグルおよびユーチューブが受け取った捜査機関からのデータの開示要請に具体的にどのように対応してきたかを、インターネット上で積極的に公開している。この「Google 透明性レポート」によれば、アメ

リカの捜査機関からの開示要請に対して、グーグルは以下のように対応してきたとされる[70]。

レポート対象期間	利用者データの要請	利用者数・アカウント数[71]	一部のデータが生成された要請の割合[72]
2014年7～12月	9,981（5,755）	20,986（13,141）	78%（76%）
2014年1～6月	12,539（8,211）	21,576（13,917）	84%（84%）
2013年7～12月	10,574（7,044）	18,254（11,999）	83%（84%）
2013年1～6月	10,918（7,458）	21,683（15,770）	83%（84%）
2012年7～12月	8,438（5,784）	14,791（10,390）	88%（88%）
2012年1～6月	7,969	16,281	90%
2011年7～12月	6,321	12,243	93%
2011年1～6月	5,960	11,057	93%
2010年7～12月	4,601	—	91%
2010年1～6月	4,287	—	—
2009年7～12月	3,580	—	—

※括弧内は、召喚状に基づく開示要請への対応を示している。

この表をみる限り、裁判官の審査を経ない召喚状による開示要請の件数が実際には非常に多く、また、応諾率も高いことがわかる。後述するように制度上の相違があるために単純に比較できないが、日本の捜査機関からの開示要請に対するグーグル側の対応は、以下のとおりである[73]。

レポート対象期間	利用者データの要請	利用者数・アカウント数	一部のデータが生成された要請の割合
2014年7～12月	131	236	81%
2014年1～6月	121	164	77%
2013年7～12月	111	134	60%
2013年1～6月	194	266	58%
2012年7～12月	124	149	62%
2012年1～6月	104	133	86%
2011年7～12月	90	117	59%
2011年1～6月	75	82	87%
2010年7～12月	72	—	90%
2010年1～6月	56	—	—
2009年7～12月	44	—	—

(3) 日本[74]

後述のように、日本には、捜査機関が、通信履歴をはじめとする通信関連情報を取得・保存・利用等する際の手続を具体的に定めた特別の立法は存在しない（もっとも、リアルタイムで通信を傍受する際の手続を具体的に規律した特別の立法として、通信傍受法〔犯罪捜査のための通信傍受に関する法律〕がある）。しかし、刑事訴訟法は、2011（平成23）年の「情報処理の高度化等に対処するための刑法等の一部を改正する法律」を受けて、通信履歴や位置情報など、ISPや携帯電話事業者等が取扱う情報の取得を意識した規定を設けるに至った。

たとえば、刑訴法218条1項および219条1項は、捜査機関は、裁判所の発する令状により、ISPなどのデータの保管者等に命じて、必要なデータ（通信履歴等）を記録媒体に記録または印刷させたうえ、その記録媒体を差し押さえることができると規定している（いわゆる「記録命令付差押え」。ISP等をして、サーバコンピュータ等に保管されている通信履歴をCD-R等に記録等させて、これを差し押さえる）。このような規定により、捜査機関は、一般的・抽象的な理由でインターネット空間に立ち入り、ISP等にアクセスすること、あるいはISP等を媒介に利用者の個人情報にアクセスすることが禁止される。捜査機関は、令状の請求に当たって、被疑者等の氏名、罪名はもちろん、記録等させるべきデータなどをできる限り特定しなければならず、特定の犯罪の嫌疑およびその犯罪と差押対象との関連性が認められるか（正当な理由があるか）といった観点から、独立の第三者である裁判官による審査を受けなければならないからである。その意味では、我が国の現行法は、捜査機関に対して、通信の「内容」

70）Google透明性レポート（http://www.google.com/transparencyreport/userdatarequests/）。本文中の表は、同ウェブページに掲載されている表に、形式面でのアレンジを加えたものである。

71）要請において指定された利用者またはアカウントの数を示している。

72）全面的または部分的に応諾した要請の比率を示している。

73）前掲注70）参照。

74）以下の記述については、尾崎愛美氏（慶應義塾大学大学院法学研究科公法学専攻後期博士課程・刑事訴訟法専攻）から懇切丁寧なアドバイスをいただいた。ここに記して感謝申し上げる次第である。もちろん、記述の誤りはすべて筆者の責任である。

にはかかわらない通信履歴等の取得についても、比較的高いハードルを課しているといえる。

しかし、捜査機関の側だけに高いハードルを課しても、国家に対するインターネット上の個人情報保護は貫徹されない。捜査機関とISP等との関係が緊密で、ISP等が自発的に捜査機関に協力しようとし、利用者に関する情報を提供しようとする場合、「通信の秘密」（憲法21条2項、電気通信事業法4条）の要請が実際に機能するか、疑問がないではないからである。たとえば、ISP等が、裁判官の審査を経ない捜査関係事項照会（刑訴法197条2項）に自発的・積極的に回答することが許されるならば、上述したような厳格な令状手続はほとんど意味のないものとなる[75]。この点で、ゲートキーパー[76]としてのISP等の側の情報提供行為に対してどのような制約が課されているかをみることが重要となる。

経済産業省の「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」23条2項は、通信の秘密の観点から、ISP等の通信事業者は、通信履歴につき、裁判官の発付した令状に従う場合等、違法性阻却事由がある場合を除いて、外部提供してはならないと規定している。この規定からは、上述の照会に応じて捜査機関に通信履歴を提供することは、違法性が必ずしも阻却されないために、原則として許されないものと解される[77]。個人データの第三者提供を原則として禁止する法23条が、一般的な個人データについて、照会に応じた提供を認めている（むしろ義務づけている）と解されている[78]ことと比較すると、通

75）周知のとおり、捜査関係事項照会の性質については、これを強制処分とみる説と任意処分とみる説とが対立しているが、法律上、これへの応諾（報告）を直接強制する手段はない。宇藤崇＝松田岳士＝堀江慎司『刑事訴訟法』（有斐閣、2012年）107頁参照（堀江慎司執筆）。

76）「ゲートキーパー」という言葉は、Jonathan Zittrain（成原慧ほか訳）「オンライン上のゲートキーピングの歴史（1）」知的財産法政策学研究28号（2010年）117頁以下から着想を得ている。

77）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年総務省告示第695号。最終改正平成25年総務省告示第340号）の解説』39頁参照。

78）宇賀克也『個人情報保護法の逐条解説〔第4版〕』（有斐閣、2013年）109頁。

信履歴に対して――通信の秘密に由来する――特別な保護が与えられていることがわかる[79]。また、ガイドライン 26 条 1 項は、位置情報についても、通信履歴と同様、裁判官の発付した令状に従う場合等、違法性阻却事由がある場合を除いて、外部提供してはならないと規定している。さらに同条 3 項は、通信事業者は、捜査機関の要請により GPS 位置情報の取得を求められた場合に、①画面表示や移動体端末の鳴動等の方法により、当該位置情報が取得されていることを利用者が知ることができるときであって、②裁判官の発付した令状に従うときに限り、当該位置情報を取得できるものと規定している[80]。このようにみると、通信事業者によるインターネット空間のゲート開閉についても、主に裁判官の発付した令状によって厳格にコントロールされているといえる（先述のように、通信事業者の側が、任意に利用者情報を捜査機関に提供することは原則として許されない）。

以上のことから、日本では、少なくとも法制度上は、捜査機関と ISP 等との「境界」（ゲート）は、裁判所によって厳格に管理されていると考えることができる。日本の場合、通信内容（メールの内容等）とは異なる通信履歴等の取得・提供についても、捜査機関と通信事業者の双方に比較的高いハードルが課されていることが、とくに注目される。たとえば、ISP 等に保存されたメールの内容も、通信履歴等も、刑訴法上はともに「差押え」の対象とされ、ともに裁判官の発付する令状を要するとされるのである（刑訴法 218 条、219 条等参照）。⑵で述べたように、この点、アメリカでは、通信履歴を含む通信に関する情報

79）なお、刑訴法は、2011 年の改正を受け、捜査機関は、記録命令付差押えをするために必要があるときは、通信事業者等に対し、通信履歴のデータのうち必要なものを特定し、30 日を超えない期間を定めて、これを消去しないよう書面で求めることができると規定している（刑訴法 197 条 3 項。特に必要がある場合は、30 日を超えない範囲内で延長できるが、通じて 60 日を超えることができない）。

80）①の要件については、GPS 位置情報を取得されていることを被疑者等に知られることになり、実効性のある捜査が困難になるとの理由から、削除の方向で改正されることが予定されている。『『電気通信事業における個人情報保護に関するガイドライン』の改正について（案）』（平成 27 年 3 月）10−12 頁。

と通信内容に関する情報とが峻別され、前者を取得する場合の要件は、後者を取得する場合の要件よりも相当緩やかに設定されている。しかし、これも⑵で触れたように、こうした峻別論に対しては、通信履歴や位置情報であっても、それらにより高度なプロファイリングが可能になるといった観点等から批判もあり、ECPA の改正などが主張されているところである（デジタル・デュー・プロセス連盟の提案等を参照）。こうした状況を踏まえると、厳格な峻別論をとらず、「通信の存在自体を知られたくないという場合もあることや、実質的に内容が推測できてしまう場合もある」[81] といった理由から、通信履歴等にも一般に厚い保護を与える[82] 日本の法制度は一定の評価を受けうるものなのかもしれない。

しかし、「通信履歴」や「位置情報」といっても、それには様々な種類のものがあるのであり、これを一律に捉えてよいか、という問題も指摘できる。たとえば、不特定多数者の閲覧を許しているような公開型のウェブサイトや掲示板に関する通信（「公然性を有する通信」と呼ばれる）には、通信の秘密の保護が及ばず[83]、かかる「通信」に関する履歴等のプライバシー性も――特定者間で行われる典型的な「通信」に関する場合よりも――低く見積もられるべきであるとの見解がある。また、位置情報にも、①「基地局に係る位置情報」

81）小向・前掲注 63）78-79 頁。

82）もともと、日本では、ヨーロッパの伝統的な理解と同様、「通信の秘密」の対象を、「通信の内容のみならず通信の存在それ自体に関する事実」も含め、広く捉えてきた。宍戸常寿「通信の秘密に関する覚書」高橋和之先生古希記念『現代立憲主義の諸相（下）』（有斐閣、2013 年）496 頁参照。それは、憲法学における多数説が、「通信の秘密」の保護を、「表現の自由との密接な関わり合いを認めながらも、私生活の秘密ないしプライバシーの権利の保護の一環として」捉えてきたことと関係している（「通信の秘密の趣旨がもっぱら表現の自由に存するのならば、表現すなわち通信内容だけが本来的な保護対象であり、発信者名等の通信の存在それ自体に関する事実は保護範囲外」となる）。宍戸・同上 500 頁。こうした見解に対して、通信の秘密の対象を限定的に捉える最近の議論については、林＝田川・前掲注 64）3 頁以下参照。

83）高橋和之「インターネットと表現の自由」ジュリスト 1117 号（1997 年）32 頁、同『立憲主義と日本国憲法〔第 3 版〕』（有斐閣、2013 年）236 頁参照。「公然性を有する通信」については、長谷部恭男『憲法〔第 6 版〕』（新世社、2014 年）230-231 頁も参照されたい。

（これはさらに、(a)移動端末が着信等の前提として基地局に送る位置登録情報と、(b)個々の通信の際に利用される基地局情報とに分類される）や、②「GPS 情報」（個々の通信を成立させるために必要ないが、より精度の高い位置情報である）など、種々のものがある[84]。ガイドライン等では、①は通信の秘密に関連して（(b)は通信の前提となるものであるから、通信の秘密に準じて）、②は通信の秘密にはかかわらないものの「高いプライバシー性を有する情報」として、いずれも高いレベルの保護が与えられるべきとされる[85]。

今後は、インターネット空間の特質を踏まえて、「通信履歴」、「位置情報」の分類や、各位置づけを具体的に検討し、各位置づけにふさわしいゲート開閉要件を確定していくべきであるが、その際には以下の点を軽視すべきではないように思われる。

1 つは、処分の直接の名宛人である ISP 等は、情報主体本人ではなく、その情報を保護することに必ずしも高いモチベーションを有していない、ということである（ISP 等にとっては、“お客様”の大事な情報である。しかし、“お客様”の情報に過ぎないとみることもできる）。この点で、それ自体はプライバシー性の高くない情報であっても、そのゲート開閉要件をある程度高く設定しておくことにも理由はあるように思われる。

もう 1 つは、繰り返し指摘しているように、それ自体プライバシー性の高くない通信履歴等も、集積され、統合されれば、情報主体の思想傾向等を明らかにしうる、ということである。もちろん、このようなプロファイリングに対する懸念は、直接には、取得後の通信履歴等の取扱いにかかわるもので、この懸念を、取得行為そのものをめぐる議論に反映させるべきではないとの考えもありえよう。しかし、先述のように、現状、取得後の通信履歴等の保存・利用・

84）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 年総務省告示第 695 号。最終改正平成 25 年総務省告示第 340 号）の解説』（平成 25 年 9 月）44-46 頁参照（以下、「ガイドライン解説」と呼ぶ）。なお、Wi-Fi のアクセスポイントを単位とする位置情報である「Wi-Fi 位置情報」については、総務省『位置情報プライバシーレポート』（平成 26 年 7 月）を参照。

85）ガイドライン解説・前掲注 84）46 頁、総務省『位置情報プライバシーレポート』6-7 頁。

管理等のあり方を具体的に規律した特別の立法はない。そうである限りは、「水際」としての取得行為に高いハードルを課しておくこと――ゲート開閉要件を厳格にしておくこと――にも理由があるように思われる[86]。公私一体的な、巨大なデータベースの出現を防ぐためにも、国家とインターネット空間との、あるいは国家とISP等との適切な緊張関係を維持するための要件設定が重要となろう。

2. プライバシー保護者としての国家

⑴ 問題の所在――インサイダー／アウトサイダー

これまで、プライバシー侵害者としての国家の姿を描出してきたが、もちろん、国家にはプライバシー保護者としての側面もある。たとえば、立法府は、2012（平成24）年に不正アクセス禁止法を改正し、①フィッシング行為、②他人のID・パスワードの不正取得行為・保管行為を新たに可罰化し、③他人のID・パスワードを提供する行為の処罰範囲を拡大した。ここで、①フィッシング行為とは、「アクセス管理者が公開したウェブサイト又はアクセス管理者が送信した電子メールであると利用者に誤認させて、アクセス管理者がID・パスワードの入力を求める旨の情報を閲覧させようとする」行為で、「当該情報を閲覧した利用権者にID・パスワードを入力させてだまし取ることを企図しているもの」[87]をいう（違反者は1年以下の懲役または50万以下の罰金が科される。7条、12条4号）。このような立法は、オンライン上でなされる不正な個人情報取得行為の一部を刑罰をもって禁止し、それによりインターネット利用者の個人情報を保護するものといえる（もちろん、不正アクセス禁止法の目的は、直接には不正アクセスの禁止にあるが）。

86）取得後の情報の取扱いを規律する具体的な立法があれば、取得に関するハードルは下げられてよいとする見解（取引的アプローチ）については、山本龍彦「監視捜査における情報取得行為の意味」法律時報87巻5号（2015年）60頁以下参照。

87）警察庁・サイバー犯罪対策「不正アクセス行為の禁止等に関する法律の解説」（https://www.npa.go.jp/cyber/legislation/）。

ただ、プライバシー保護者としての国家の役割を、インターネットとの関連で考える場合、より重要になると思われるのは、“インサイダー”によるプライバシー侵害的アーキテクチャに対し、国家がどのようにかかわるか、であろう。ここで“インサイダー”とは、インターネット・インフラに深くかかわる民間事業者（ISP やブラウザ提供企業等）を意味している。上述のようなフィッシング行為は、主に、こうしたネット・インフラの構築とは直接かかわらない“アウトサイダー”が、インフラを利用して、間接的に利用者のプライバシーを侵害しようとする行為である（プライバシー侵害者としての国家も、その意味では“アウトサイダー”である）。他方、“インサイダー”によるプライバシー侵害は、自らがデザインしたインフラそれ自体によって、あるいはアーキテクチャそれ自体によって、直接的に利用者のプライバシーを侵害しようとする行為である。これは、人為的なものでありながら、利用者にとっては自然的・中立的・不可視的・構造的なものであるがゆえに、個々の利用者によるコントロールは事実上不可能なものであるといえる。もちろん、民間事業者である“インサイダー”が、利用者の信頼を低下させ、競争上不利となるようなプライバシー侵害を試みるはずはないとも思われるが、上述のようなアーキテクチャの不可視性や ISP 等の希少性ゆえに、利用者の選択可能性は実質的に制限されており、市場の抑止力が、常に、うまく機能するわけではない。

そうすると、“インサイダー”が、自らの経済的利益のために――ISP 等の保有している情報量は天文学的なものであり、これを販売したときの利益は計り知れない――自らが管理するインフラないしアーキテクチャを、プライバシー侵害的にデザインすることも考えられる（たとえば、マーケティングを目的とした DPI 技術の設計、サードパーティークッキーを初期設定〔デフォルト〕で許容するようなブラウザの設計）。1 で行った検討とあわせて考えれば、インターネットが民間のインフラであるということは、国家（捜査機関）によるプライバシー侵害に対してはプライバシー保護的に機能する反面で、“インサイダー”によるプライバシー侵害については、これを放任・助長する方向に機能しうるのである。かくして、ここでも重要になるのは、国家とインターネット空間と

の“距離”である。国家自身がプライバシー侵害者となりうることを踏まえれば、国家は、この空間に近づき過ぎてはいけない。しかし、インターネット空間を構築・デザインする“インサイダー”がプライバシー侵害者[88]となりうることを踏まえれば、そこから遠ざかり過ぎてもいけないのである。では、国家は、この空間の設計ないし秩序形成にどこまで、またどのようにかかわるべきなのであろうか。

⑵ 議論

アメリカでは、FTC が中心となって、2000 年代後半から、「追跡拒否（Do Not Track, DNT）」機能をブラウザに組み込むことが強く提案されている。DNT とは、インターネット利用者が、サードパーティークッキー[89]等によるオンライン行動の追跡を拒否することを可能にするためのブラウザベースのメカニズムのことをいう（利用者がブラウザ上に設定された追跡拒否を「オン」にすると、ブラウザから広告配信事業者等に追跡拒否の信号が送られる）。FTC は、利用者による「追跡」可否の実質的な選択のためには、このようなアーキテクチャの組み込みが非常に重要であると考えているのである[90]。Ⅱの考察を踏まえれば、オンライン・プライバシーの保護には、これを実効化するためのアーキテクチャないしデザインが不可欠であるとさえいえるであろう。

こうした FTC の提案を受けるかたちで、たとえば、アメリカのマイクロソフト社は、ブラウザ（Internet Explorer 10）の初期設定（デフォルト）で DNT をオンにする方針（オプトイン方式）を表明し、アップル社は、ブラウザ（Safari）

88）ネット企業の権力性が「自由」に与える影響について、曽我部真裕「自由権」法学セミナー 688 号（2012 年）12 頁以下、大屋雄裕「分散する規制、分散する主体」Mobile Society Review　未来心理 11 号（2008 年）6 頁以下参照。

89）サードパーティークッキーについては、山本・前掲注 1）。

90）*See* Fed. Trade Comm'n, Protectig Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers 66（2010）, *available at*（https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf）［hereinafter Preliminary Report］.

で、サードパーティークッキーを初期設定でブロックする仕組み（やはりオプトイン方式）を取り入れることとなった。他にも、モジラ社が、ブラウザ（Firefox 22）においてサードパーティークッキーを初期設定でブロックする仕組みを取り入れようとした。このようなブラウザ企業――前節の言葉を使えば“インサイダー”――の自主的な取り組みは、オンライン・プライバシーを保護するとの観点から大いに歓迎されるべきもののように思われる。しかし、現実には、このようなブラウザ企業の初期設定に対して、インターネット広告業界が強い抵抗を示すこととなった。広告業界からすれば、＜クッキー等を通じたインターネット利用者の行動追跡→プロファイリング→ターゲティング広告＞という 1 つのビジネス・モデルが、こうしたブラウザの初期設定によって傷つけられることになるからである（初期設定として、オプトインをとるかオプトアウトをとるかは、広告業者にとっては死活問題となる。文脈が異なるが、臓器提供の率は、臓器提供についてオプトインをとる国とオプトアウトをとる国で大きく異なる）[91]。いいかえれば、広告業界にとって、“インサイダー”であるブラウザ企業による初期設定は、一方的で不公正な「権力」の行使となるのである。

実際、ターゲティング広告にかかわる米ヤフーは、Internet Explorer 10 から DNT 信号が送られてきても、これを尊重しないとの「強硬措置」をとることを表明し（2012 年 10 月）[92]、グーグルは、Safari のクッキー拒否設定を迂回して利用者のウェブサイトの閲覧記録を実際に収集していたようである [93]。つ

91）臓器提供がオプトインの国では、文化的には類似しているものの、オプトアウトをとる国と比して、臓器提供率が低い傾向にある。たとえば、オプトアウトをとるスウェーデンの臓器提供率は 85.9％であるのに対して、オプトインをとるデンマークでは 4.25％、オプトアウトをとるオーストリアでは 99.9％であるのに対して、オプトインをとるドイツでは 12％である。Omer Tene and Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 Nw. J. Tech. & Intell. Prop. 239, 261-262（2013）.

92）井上 健太郎「米ヤフー、IE10 の『Do Not Track』初期設定を無視する方針を表明」ITpro（2012 年 10 月 29 日）（http://itpro.nikkeibp.co.jp/article/NEWS/20121029/433292/）。小林・前掲注 45）87 頁も参照されたい。

まり、“インサイダー”によるブラウザの初期設定は、たとえそれがプライバシー保護的なものであるとしても、その設定・変更につき、ステイクホルダーであるインフラ利用者（ここでは広告会社）等の理解を得ることなく、一方的に行われれば――手続的な公正が担保されなければ――、実際上無視ないし軽視され、かえって利用者のプライバシー侵害を助長させることになるのである。

また、サードパーティークッキーを初期設定においてブロックするFirefox 22も、広告業界からは、「広告業界に対する最初の核爆弾投下（nuclear first strike against the ad industry）」であるなどと激しく糾弾され[94]、一旦はその実装を延期させられている。このような例は、インフラ構築にかかわる“インサイダー”が、その利用者（ここでは広告会社）の圧力に屈し、あるいはそれと同調・結託し、一般利用者（エンド・ユーザー）を置き去りにしたかたちで、プライバシー侵害的なアーキテクチャをデザインすることがありうることを示している。先に触れたISPのサービス設備（ルータ等）で行われるDPI（本来はトラフィックのセキュリティ等を目的とするものである）についても、ISPと広告会社（広告配信事業者）が手を組んで、これをマーケティングのために利用する可能性を指摘する論者も少なくない[95]。

以上のようにみると、インターネット空間の具体的な秩序形式ないしアーキテクチャの構築は、ISPやブラウザ企業といった“インサイダー”のみによって行われるべきではなく、広告会社や一般利用者（エンドユーザー）も含めた多様なステークホルダー（マルチ・ステークホルダー）が参加する公正なプロセスを通じてなされるべきであるといえよう[96]。インターネットは、たしかに民間インフラであるが、プライバシー保護のレベルは、このインフラないしアーキテクチャのデザインに決定的に依存しているがゆえに、そのデザインの

93）Fed. Trade Comm'n, *Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser Aug. 9, 2012*, *available at*（https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented）.

94）Tene and Polonetsky, *supra* note 25, at 82.

95）*See e.g.*, Tene and Ponetsky, *supra* note 12, at 298-299.

形成には一定のデュー・プロセスが求められる、ということである。この点で、国家が、かかるプロセスに関与する必要性は高いといえる。しかし、他方で国家は、このプロセスを占拠し、その一切を公的領域に移すべきではない。インターネット空間を構成するアーキテクチャの高度の専門性、技術的進歩の圧倒的な速度、国家（自身）によるプライバシー侵害の可能性などから、このプロセスは、国家から一定程度自律的であるべきである。国家は、マルチステークホルダーを含む公正なプロセスを実現・維持し、このプロセスを経た「自主規制」に一定の民主的正統性ないし法的身分を付与するといった役割に自らを限定すべきであるといえよう[97]。

⑶ 日本

法案のベースとなったIT総合戦略本部「パーソナルデータの利活用に関する制度改正大綱」（以下、「改正大綱」と呼ぶ）[98]では、「〔パーソナルデータの自由な利活用が許容されるのかが不明確な〕グレーゾーンの内容や個人の権利利益の侵害の可能性・度合いは、情報通信技術の進展状況や個人の主観等複数の要素により時代とともに変動するものであることから、これらに機動的に対応することを可能とするため、社会通念等も踏まえつつ、法律では大枠を定め、具体的な内容は政省令、規則及びガイドラインにより対応する。また、これと併せ民間の自主規制ルールの活用を図ることとする」[99]（傍点筆者）と書かれていた。ここでは、プライバシーの保護と関連する具体的なアーキテクチャやブラウザの初期設定等が、民間の自主規制ルールによって規律されることが示唆

96）マルチステークホルダープロセスについては、高度情報通信ネットワーク社会推進戦略本部『パーソナルデータの利活用に関する制度改正大綱』（2014年6月24日）8頁（Ⅱ2）参照（以下、「改正大綱」と表記する）。さらに、宇賀克也＝宍戸常寿＝森亮二「鼎談　パーソナルデータの保護と利活用に向けて」ジュリスト1472号（2014年）70頁参照。

97）次項で述べるように、これは講学上の「共同規制」を意味している。共同規制については、何といっても生貝直人『情報社会と共同規制』（勁草書房、2011年）を参照されたい。

98）改正大綱・前掲注96）参照。

99）改正大綱・前掲注96）8頁（Ⅱ2）。

されている。改正大綱では、さらに、こうした民間団体による自主規制ルールが、「消費者等も参画するマルチステークホルダープロセス」によって形成されること、この団体ないしルールの認定等に（国が設置する）第三者機関が積極的に関与すること、それにより、自主規制ルールの正統性と実効性を確保することが必要であると述べられている[100]。こうした「自主規制」は、法の外で、国の設置する第三者機関の関与なく策定される狭義の自主規制ではなく、法の枠内で（法の定める目的を実現するために）、当該機関とのかかわりにおいて策定される「共同規制（co-regulation）」に近いと指摘されている[101]。「共同規制」とは、「企業や業界団体が行う自主規制（self-regulation）に対し、政府が一定の介入・補強を行うことによって、公私が共同で問題を抑止・解決していく政策手法」[102]などと説明される規制レジームである。この点、たとえば宍戸常寿は、改正大綱のいう「自主規制」は、「講学上の『共同規制』に当たる」と理解したうえで、その意義は、単純な自主規制では“インサイダー”や事業者らによってプライバシー侵害的なルールないしアーキテクチャが生み出されかねない――「オオカミに羊の番をさせる」ことに由来するリスクがある――ことから、「第三者機関が自主規制のルールの認定や自主規制団体の監督をしっかり行う体制を整備」し、消費者を含むマルチステークホルダーが参加しての「公正な手続」を実現・維持するところにある、と指摘している[103]。

法案は、こうした「共同規制」のプロセスを明確に制度化するまでには至らなかったが、その考え方を一部採用している。たとえば、法43条は、主務大臣の認定した「認定個人情報保護団体」（以下、「認定保護団体」と呼ぶ）が、「この法律の規定の趣旨に沿った指針」（個人情報保護指針）を作成・公表し、対象事業者に同指針を遵守させるために必要な措置をとるよう努めなければならないとしていたが、法案は、①認定保護団体の「認定」権限を個人情報保護

100）改正大綱・前掲注96）8頁（Ⅱ2）。
101）宇賀＝宍戸＝森・前掲注96）70頁（宍戸常寿発言）。
102）生貝・前掲注97）i頁。
103）宇賀＝宍戸＝森・前掲注96）70頁（宍戸常寿発言）。

委員会に移したうえ、②認定保護団体が指針を作成するに当たって「消費者の意見を代表する者その他の関係者の意見を聴〔く〕」ことを求め、③個人情報保護委員会に、同指針の届出を受けたうえで、これを公表することを義務づけ、④対象事業者が同指針を遵守するために必要な措置をとることを認定保護団体に義務づけた（法案 53 条）。法案は、認定保護団体の手になる指針が定める事項として、「匿名加工情報に係る作成の方法」（法案 53 条 1 項）を例示したが[104]、指針の対象はもちろんこれに限定されるわけではない。指針によって、「わかりやすいオプトアウトの仕組みや、第三者提供等に関する本人同意の標準化等」に関するルール形成が期待されるとの指摘[105]があることを踏まえれば、プライバシー保護に関連するようなブラウザの初期設定やアーキテクチャのデザインを含む具体的なルールを、公と私との協働的なかかわり合いのなかで不断に発展させていくことが求められるように思われる。国家は、この局面においては、マルチステークホルダーを含む公正なルール形成プロセスを実現・維持する役割、このプロセスを経て形成されたルールに正統性と実効性を付与する役割を積極的に果たさなければならず、またその役割に自らをとどめおかなければならない、ということになる。

Ⅳ．おわりに

以上、前稿[106]および本稿は、インターネット空間において個人情報を保護しようとする場合の問題を概観したうえで、これらの問題に対するアメリカや EU の取組み、さらには、個人情報保護法の改正（2015 年）に一部具現化されている日本の取組みについて紹介し、若干の考察を加えてきた。前稿の「はじめに」でも触れたように、このような小論がまず目指したのは、この分野のフロンティアをできるだけ専門的・技術的にならないかたちで描き出すことで、

104）匿名加工情報については、山本・前掲注 1）参照。
105）宍戸・前掲注 51）44 頁。
106）山本・前掲注 1）。

多くの法学者と＜問題＞を共有することにあった。ただ、筆者としては、それだけでなく、この分野に含まれる＜問題＞が、実は理論的な奥深さを有している、ということを法学者の間で共有できれば、とも考えていた。インターネットと個人情報といった問題は、ともするとプライバシー権論の単なる延長、応用問題であるとか、その極度に専門化された一現象に過ぎないと過小評価されることがある。もちろん、プライバシー権論と連続していることは事実であろうが、無数のコード、アーキテクチャ、アルゴリズムによって構築されるこの仮想世界における個人情報の保護には、より一般的で理論的な＜問題＞が付着している。秩序形成の問題である。

本論でも度々示唆したように、改正個人情報保護法（案）は、実のところ、実体法というより、手続法あるいは権限配分の法である。これをもっぱら実体法として捉えると、痛い目に合う。同法案において核心的な保護対象とされる「個人情報」とは何か、反対に、基本的に自由な利活用が可能となる「匿名加工情報」とは何か、違法との評価を受けうる第三者提供とは具体的にどのような行為をいうのか、といった問いの直接的な解答を同法案のなかに求めても、確実に徒労に終わるからである。改正個人情報保護法（案）は、もちろん、こうした問いに抽象的な解答を与えるものではあるが（そして、そのこと自体、重要な意味をもつのであるが）、基本的には、その具体的な解答を、誰が――個人情報保護委員会なのか、認定個人情報保護団体なのか、事業者自身なのか、等々――、どのように――マルチステークホルダープロセスに個人情報保護委員会が関与するような共同規制的レジームなのか、純然たる自主規制的レジームなのか、等々――決めるのかを決めている[107]のである。いわばそれは、ガバナンスの、あるいは秩序形成のための基本法なのである。

そして、そうなるのには十分な理由がある。インターネット空間における個人情報保護は、「法」だけでは実現されない。たとえ、法的言語として「個人情報」を定義し、その保護やセキュリティのあり方を規定したとしても、それ

107）H.L.A. ハートのいう「二次ルール」ということになる。H.L.A. ハート（長谷部恭男訳）『法の概念〔第 3 版〕』（筑摩書房、2014 年）140-141 頁参照。

は、コンピュータ言語――コードないしアーキテクチャ――をとおしてしか実現されない。したがって、「法」は、個人情報保護の全体としての方向性（抽象的・一般的な理念ないし目標）と、その方向性を適切かつ具体的に実現するための秩序を提示することに、自らの役割をとどめおかざるをえないのである。しかし、このことは、「法」の後退では、ない。コンピュータ言語を「母語」とするような“インサイダー”が制定・プログラミングするコードがインターネット空間における個人情報保護の命運を実際上握っているからこそ、「法」がその方向性を照らし出し、この制定・プログラミングを適切に統制していく必要があるのである。インターネットという、仮想――ではあるが、我々が日常生活を強く依存させている――世界は、「法」を知らない「コード」の世界であってはならない。我々は、そこに、「法」と「コード」が調和するコスモスを作り出さなければならないのである[108]。インターネット時代の個人情報保護が、この＜問題＞を内在させている以上、それは、プライバシー権論の単なる応用問題にはならない。

＊再校中の 2015 年 8 月 29 日の報道によれば、改正個人情報保護法案は、同年 9 月 3 日に成立する見通しであるという。

108）こうした問題関心を共有していると思われるものとして、生貝・前掲注 97）、成原慧「情報社会における法とアーキテクチャの関係についての試論的考察」情報学環紀要情報学 81 号（2011 年）55 頁以下、同「代理人を介した表現規制とその変容」マス・コミュニケーション研究 80 号（2012 年）249 頁以下などがある。