「プライバシー外交」のためのプライバシー

石井夏生利[1]

要　旨

プライバシー権の提唱国である米国では、消費者プライバシー保護に向けた取組が行われる一方で、2001 年 9 月 11 日の同時多発テロ以降、国家安全のためにプライバシーを犠牲にする傾向が顕著である。今日では、プライバシー権の理念すら希薄化しているとも考えられる。

他方、欧州では、個人データ保護は基本的権利であるとの考えに立脚し、データ保護分野における国際的な立場を強化する態度を見せている。

日本では、2013 年 9 月より、「パーソナルデータに関する検討会」が設置され、第三者機関設置等に向けた検討が進められてきた。2013 年 12 月 20 日には、高度情報通信ネットワーク社会推進戦略本部において、「パーソナルデータの利活用に関する制度見直し方針」が決定された。今後、日本は、国際的な情報発信力や交渉力を高めていくべきであるが、その際に、個人情報保護法制の根底に存在するプライバシー権の捉え方について、法改正を見据えた上で、考えておく必要がある。

以上の問題意識に基づき、本稿では、2013 年 6 月に米国で関係者と意見交換を行った結果等をもとに、プライバシーに関する米国の現在の考え方を整理し、日本におけるプライバシー権の捉え方を提示することとした。

キーワード：プライバシー外交、パーソナルデータ、国家安全、FTC、プロファイリング

1. はじめに

プライバシー権の提唱国である米国は、消費者プライバシー保護に向けた取組を行う一方、2001 年 9 月 11 日の同時多発テロ以降、国家安全のためにプライバシーを犠牲にする傾向が顕著である。

他方、人権思想発祥の地といわれる欧州は、個人データ保護を基本的権利ないしは人権であると捉えており、「欧州連合の機能に関する条約」（Treaty on the Functioning of the European Union）第 16 条 1 項や、欧州連合基本権憲章（Charter of Fundamental Rights of the European Union）第 8 条 1 項において、全ての者は自らに関する個人データを保護する権利を有する旨の定めを設けている。また、人権及び基本的自由の保護のための条約（Convention for Protection of Human Rights and Fundamental Freedoms）第 8 条第 1 項は、「全ての者は、その私的な家庭生活、住居、及び通信を尊重してもらう権利を有する」と定めており、同条項はプライバシー権の根拠規定に位置づけられている。

[1] 筑波大学図書館情報メディア系　准教授

欧州連合（European Union, EU）では、欧州委員会によって、2012 年 1 月 25 日、「個人データの取扱いにかかる個人の保護と当該データの自由な移動に関する欧州議会及び理事会の規則（一般データ保護規則）提案」[2]が提出された。一般データ保護規則提案は、1995 年 10 月 24 日に採択された「データ保護指令」（「個人データの取扱いに係る個人の保護及び当該データの自由な移動に関する 1995 年 10 月 24 日の欧州議会及び理事会の 95/46/EC 指令」）[3]を改正するものである。同提案は、2013 年 10 月 21 日、欧州議会の市民的自由・司法・内務委員会（Committee on Civil Liberties, Justice and Home Affairs）（LIBE 委員会）によって、修正の上可決され、2014 年 3 月 12 日、その本会議で可決された。しかし、規則の成立に関しては、閣僚理事会での承認が残されているため、当初予定の 2014 年 5 月を大幅にずれこみ、同年末を期限とすることで EU 関係者が合意したと報じられている（2014 年 3 月 26 日現在）。

一般データ保護規則提案は、加盟国の立法措置を必要とする「指令」から、立法措置なくして直接適用される「規則」への変更、第三国への越境適用、「削除権」や「データ・ポータビリティの権利」等のデータ主体の権利、「データ保護・バイ・デザイン」、「個人データ侵害の通知/連絡制度」、及び、「データ保護影響評価」の導入、第三国への個人データ移転に当たっての「十分な保護レベル」を認定する際の独立監視機関の必要性、第 29 条作業部会から欧州データ保護会議への改組、高額な制裁金の措置等、数々の個人データ保護措置を設けている。こうした措置を設ける 1 つの背景には、米国が多数の巨大インターネット企業を抱え、世界中の個人情報を収集・利用している現状に対処する意図があると考えられる。いいかえると、欧州では、越境データ流通の覇権を握るべく、人権としてのプライバシーを盾にアメリカに対抗する様子が見られる。

日本は、1930 年代頃より、英米法の示唆を受けながらプライバシー権論議を発展させてきた。個人情報保護法制の制定が意識されるようになった 1980 年代頃以降は、経済協力開発機構（Organisation for Economic Co-operation and Development, OECD）のプライバシー・ガイドラインや、EU のデータ保護指令などの国際動向の影響を受けつつ制度実現に向けた歩みを進め、2003 年 5 月 23 日、個人情報保護関連五法を制定させた。

個人情報の保護に関する法律（以下「個人情報保護法」という。）は、「個人情報は、個人の人格尊重の理念の下に慎重に取り扱われるべきものであることにかんがみ、その適正な取扱いが図られなければならない」ことを基本理念とする（第 3 条）。「個人情報の保護に関する基本方針」（2004 年 4 月 2 日閣議決定・2008 年 4 月 25 日、2009 年 9 月 1 日一部変更）は、この基本理念を受け、「法第 3 条は、個人情報が個人の人格と密接な関連を有するものであり、個人が『個人として尊重される』ことを定めた憲法第 13 条の下、慎重に取り扱われるべきことを示すとともに、個人情報を取り扱う者は、その目的や態様を

---

[2] *Commission Proposal for a Regulation of The European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data* (General Data Protection Regulation), COM (2012) 11 final (Jan. 25, 2012), http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf. 規則提案検討の経緯・ポイント等は、新保史生「EU の個人情報保護制度」ジュリスト第 1464 号（2014 年 3 月）38-44 頁参照。

[3] Council Directive 95/46, 1995 O.J. (L 281) 0031-0050 (EC).

問わず、このような個人情報の性格と重要性を十分認識し、その適正な取扱いを図らなければならない」と記している。個人情報保護法は、2005 年 4 月 1 日の全面施行からまもなく 10 年を迎えようとしているが、その解釈の背景には、憲法第 13 条後段の「生命、自由及び幸福追求に対する国民の権利」が存在してきたといえる。

憲法第 13 条後段とプライバシー権に関しては諸説あるものの、憲法学の中で最も大きな影響を与えたのは、佐藤幸治京都大学名誉教授である。同教授は、1970 年に発表した「プライヴァシーの権利（その公法的側面）の憲法論的考察（一）（二）」[4]において、憲法第 13 条後段の幸福追求権を根拠に、「自己に対する情報をコントロールする権利」を保護し、それによって実現しようとする利益あるいは価値は「個人の尊厳」であると主張した。そして、同教授は、プライバシー権を「個人が道徳的自律の存在として、自ら善であると判断する目的を追求して、他者とコミュニケートし、自己の存在にかかわる情報を開示する範囲を選択できる権利」であると定義した [5]。日本がこれまで様々な場面で行ってきた個人情報保護論議の中には、「コントロール」の意味するところを精査することなく「プライバシー権は自己情報コントロール権である」との主張が展開される場面も見られたが、佐藤教授が「自己の存在にかかわる情報を開示する範囲を選択できる権利」と説明していた点には留意しなければならない。

最近では、2013 年 6 月 14 日、高度情報通信ネットワーク社会推進戦略本部決定に基づき「パーソナルデータに関する検討会」（委員長：堀部政男一橋大学名誉教授）が設置され、同検討会は、2013 年 9 月 2 日より個人情報保護法改正に向けた議論を行った。その結果を受け、上記戦略本部は、同年 12 月 20 日、「パーソナルデータの利活用に関する制度見直し方針」を決定した。この見直し方針は、①ビッグデータ時代を迎えた現在において、個人情報保護法制定当時には想定されていなかったパーソナルデータの利活用が行われるようになり、個人情報及びプライバシーに関する社会的な状況は大きく変化していること、②企業活動がグローバル化する中、国内に世界中のデータが集積し得る事業環境の整備を進めるためにも、海外における情報の利用・流通とプライバシー保護の双方を確保するための取組に配慮し、制度の国際的な調和を図る必要があることを認識し、制度見直しに向けた方針を明らかにした。同方針の中では、「プライバシー」という言葉が複数回用いられ、第三者機関による国際的な執行協力、他国へデータ移転を行う際の保護対策や海外事業者への国内法適用等が検討事項に掲げられている。2014 年 6 月には大綱を決定し、2015 年の通常国会に、個人情報保護法改正案を提出することが予定されている。

これまでの日本は、個人情報保護法の制定や、第三者機関の設置等において、欧米から大幅に遅れを取ってきた。しかし、今後の日本は、国際的な情報発信力や交渉力を高め、「プライバシー外交」を積極的に行う必要がある [6]。そして、個人情報保護法を改正して

---

[4] 佐藤幸治「プライヴァシーの権利（その公法的側面）の憲法論的考察（一）－比較法的検討－」法学論叢第 86 巻第 5 号（1970 年）1 頁以下、同「プライヴァシーの権利（その公法的側面）の憲法論的考察（二）－比較法的検討－」法学論叢第 87 巻第 6 号（1970 年）1 頁以下。佐藤教授のプライバシー権をめぐる種々の研究成果は、佐藤幸治『現代国家と人権』（有斐閣、2008 年）の中に、ほぼそのままの形で収録されている。

[5] 佐藤幸治『憲法』（青林書院、第 3 版、昭和 56 年）453-454 頁。

[6] 「プライバシー外交」という言葉を最初に用いたのは、堀部政男特定個人情報保護委員

「プライバシー外交」を行うことを考えた場合、制度設計の重要性はさることながら、その根底として、日本は何をプライバシーの要素とすることができるのか、あるいは、今後はどのようなプライバシー侵害に着目すべきか、という点を改めて考えておく必要がある。

以上の問題意識により、本稿では、プライバシー権の提唱国である米国の状況を取り上げることとする。具体的には、米国におけるプライバシー論議の展開、2001 年 9 月 11 日の同時多発テロ以降における個人情報取扱状況、米国への訪問調査結果等を整理しつつ、「プライバシー外交」のための「プライバシー」を検討したい。

2. 米国におけるプライバシー・個人情報保護論議の展開

2. 1. プライバシー権の提唱と展開

始めに、米国におけるプライバシー権の発展を改めて概観する。

プライバシー権は、1890 年に、サミュエル・D・ウォーレン（Samuel. D. Warren）氏とルイス・D・ブランダイス（Louis. D. Brandeis）氏が、ハーバード・ローレビューに「プライバシーの権利」（The Right to Privacy）（以下「ウォーレン&ブランダイス論文」という。）[7]を発表し、「ひとりにしておかれる権利」を提唱したことから始まった。これが執筆されなかったならば、プライバシーの権利という考え方は、承認されることにならなかったかもしれないし、仮にそうでないとしても、かなり遅れて認められることになったであろうといわれている [8]。この権利は、伝統的プライバシー権ともいわれる。

ウォーレン&ブランダイス論文は、「ひとりにしておかれる権利」を多義的に理解し、様々な形で説明した。それを 2 つのカテゴリに分類すると、第 1 は、「秘密を守る権利、孤独を守る権利、思想・信条・感情をあらゆる形式における公開から保護される権利」であり、不可侵権として位置づけられる。第 2 は、「各個人が通常、自己の思想や心情、感情をどの程度他人に伝えるべきかを決定する権利」又は「公開の行為を完全にコントロールする」権利である。この説明は、不可侵権というよりは、個人に公開の決定権を与えるという意味で、後述する現代的プライバシー権（自己情報コントロール権、情報プライバシー権等ともいわれる）に親和性を持つ。

その後、カリフォルニア大学バークレー校で学部長を務めたウィリアム・L・プロッサー（William L. Prosser）教授は、1960 年 8 月、カリフォルニア・ロー・レビューに、「プライバシー」（Privacy）と題する論文を発表した [9]。これは、ウォーレン&ブランダイス論文が発表された後に、米国で提起された多くのプライバシー侵害訴訟を不法行為の観点から整理・分類し直した論文である。プロッサー教授の分類した 4 類型－不法侵入（Intrusion）、私的事実の公開（Public Disclosure of Private Facts）、公衆の誤認（False

---

会委員長（一橋大学名誉教授）である。堀部教授の研究成果は数多く存在するが、プライバシー外交を取り上げた最近のものに、堀部政男「プライバシー・個人情報保護の国際的整合性」同編著『プライバシー・個人情報保護の新課題』（商事法務、2010 年）1 頁以下がある。

[7] Samuel. D. Warren & Louis. D. Brandeis, *The Right to Privacy*, 4 HARV.L.REV.193 (1890).

[8] 堀部政男『現代のプライバシー』（岩波書店、1980 年）25 頁。

[9] William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960).

Light in the Public Eye)、盗用（Appropriation）－は、第 2 次不法行為リステイトメントに取り入れられた [10]。

1960 年代中葉になると、特にコンピュータ化との関係で、監視社会への懸念という、新たなプライバシー問題へと関心が寄せられるようになった。かかる事態への対応に大きな影響を与えたのは、現代的プライバシー権の提唱である。この権利を論じた著書として世界的に有名なものは、コロンビア大学のアラン・F・ウエスティン（Alan F. Westin）名誉教授が 1967 年に発表した『プライバシーと自由』（Privacy and Freedom）[11]、ニューヨーク大学法科大学院のアーサー・R・ミラー（Arthur R. Miller）教授が 1971 年に発表した『プライバシーへの攻撃』（The Assault on Privacy）[12]である。

ウエスティン教授の『プライバシーと自由』は、「プライバシーとは、個人、グループ又は組織が、自己に関する情報を、いつ、どのように、また、どの程度他人に伝えるかを自ら決定できる権利である」[13]と定義し、日本でも数多くの文献で引用されてきた。同教授は、この著書の中で、「自己に関する情報」を保護対象にする一方、プライバシーの基本的状態を「孤独」、「親密さ」、「匿名性」、及び、「沈黙」であると論じている。とりわけ、「沈黙」が最も繊細なプライバシーの状態であり、望まない侵入に対して心理的な障壁を作ることであると説明されている。あわせて、教授は、これらの状態を保護することによって得られるプライバシーの効果を、個人の自律、感情的自由、自己評価、及び、通信の制限及び保護の 4 つに分類した [14]。このことから、同教授の論じるプライバシー権は、基本的には私的な状態を保護するものであり、個人に対し、自律性、自己実現、精神的安定を与えるために、自らに関する情報の提供について、自ら決定できる権利であると理解することができる。

ところで、ウエスティン教授の定義は、グループ又は組織を含んでいる。しかし、ミラー教授の『プライバシーへの攻撃』によって、プライバシー権は、個人を権利主体とするものとして捉えられ、かつ、情報の流通規制を含む形で理解されるようになった。

そして、ミラー教授は、「最近、法律家や社会学者は、効果的なプライバシー権の基本的特質は、自己に関する情報の流れをコントロールする個人の能力－社会関係や個人の自由を維持するのにしばしば不可欠な力－であるという結論に達するようになった。これと相関的に、個人が自己に関する情報の流れを統制する栓のコントロールを奪われるならば、ある程度までその者は栓を操作することができる人々や機関に屈従することになる」と論じている [15]。ここでは、プライバシー権は、情報の流れをコントロールする能力であると説明されており、日本で理解されてきた「自己情報コントロール権」は、この定義の影響を受けて発展したと考えられる。

そして、現代的プライバシー権を具体的に論じたウエスティン教授は、著書の中で立法

---

[10] 判例法上のプライバシー権の発展経緯は、拙著『個人情報保護法の理念と現代的課題：プライバシー権の歴史と国際的視点』（頸草書房、2008 年）121 頁以下。
[11] ALAN F.WESTIN, PRIVACY AND FREEDOM (1967).
[12] ARTHUR R. MILLER, THE ASSAULT ON PRIVACY (1971).
[13] WESTIN, *supra* note 11, at 7.
[14] *Id.* at 31-39.
[15] MILLER, *supra* note 12, at 25.

提案を行い、ミラー教授も法律の必要性を説いている。こうした立法提案に呼応するように、米国は、1970 年以降、公的部門では 1974 年プライバシー法（Privacy Act of 1974）[16]、民間部門では 1970 年公正信用報告法（Fair Credit Reporting Act of 1970, FCRA）[17]等のセクトラル方式によるプライバシー保護法を数多く成立させるようになった[18]。

1974 年プライバシー法が制定される過程において、連邦保健教育福祉省（United States Department of Health, Education, and Welfare（当時））は、自動個人データ・システムに関する長官の諮問委員会（Secretary's Advisory Committee on Automated Personal Data Systems）を設置し、同委員会は、1973 年 7 月、「記録、コンピュータ及び市民の権利」（Records, Computers, and the Rights of Citizens）[19]という報告書を発表した。この中で、個人のプライバシー概念の再定義がなされており、ウエスティン教授による現代的プライバシー権の定義が登場している。

また、この報告書は、公正情報実務諸原則（Fair Information Practice Principles, FIPPs）の出発点となる諸原則を掲げている点でも重要である。同報告書の第 3 章「プライバシーのための安全保護」（Safeguards for Privacy）は、「現行法のもとでは、個人のプライバシーは、恣意的又は濫用的な記録保管業務に対して、不十分な保護が与えられているにすぎない。こういう理由から、また、コンピュータ時代にふさわしい記録保管業務の基準確立の必要性という理由からも、すべての自動個人データ・システムに対する、合衆国の『公正情報実務に関する法』（Code of Fair Information Practice）の制定」を勧告した。

そして、同報告書は、自動個人データ・システムに対する「保護措置要件」（"Safeguard Requirements"）として法的効力が与えられることになるであろう 5 つの基本原則を明らかにした。1974 年プライバシー法の各規定は、この 5 原則が基本となっている。

「(1) その存在自体が秘密になっている、いかなる個人データ記録保管システム（personal data record-keeping systems）も存在してはならない。

(2) 個人は、自己に関するいかなる情報が記録の中にあり、またそれがどのように利用されているかを見出す方法がなければならない。

(3) 個人がある 1 つの目的のために取得された自己に関する情報が、その承諾なしにその他の目的のために利用され、又は使用されることを防止する方法がなければならない。

(4) 個人が自己に関する識別可能な情報の記録を訂正又は修正する方法がなければならない。

(5) 識別可能な個人データの記録を作り出し、保有し、利用し、又は頒布するいかなる組織も、データの信頼性をその意図した用途のために確保しなければならず、また、そのデータの誤用を防止するための合理的な予防措置を講じなければならない。」

---

16 Privacy Act of 1974, 5 U.S.C. § 552a (2012).

17 Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681 *et seq.* (2012).

18 米国のプライバシー保護立法は、拙著・前掲『個人情報保護法の理念と現代的課題：プライバシー権の歴史と国際的視点』419 頁以下。

19 Secretary's Advisory Committee on Automated Personal Data Systems, HEW, *Records, Computers, and the Rights of Citizens* (1973).

2．2．学界によるプライバシーの多義的理解

米国のプライバシー権論議に関しては、その後も膨大な著書・論文等が公表されてきたものの、ウォーレン&ブランダイス論文やウエスティン教授の『プライバシーと自由』のような、国内外で多大な影響を与えたものは登場していない。

そのような中で、近時注目すべき著書の 1 つに、ジョージ・ワシントン大学のダニエル・J・ソロブ（Daniel J. Solove）教授による『プライバシーの理解』（Understanding Privacy）[20]という本がある。同書は 2008 年に発表され、日本でも 2013 年に邦訳が出版された。同教授は、カリフォルニア大学バークレー校のポール・M・シュワルツ（Paul M. Schwartz）教授とともに、「情報プライバシー学派」の代表格といわれる人物である。

『プライバシーの理解』の冒頭には、包括的なプライバシーの概念は存在せず、むしろ地形図を作るときのように、目に見える風景を丁寧に研究することによって、プライバシーのあり様を地図化しなければならないと記されている。

同書の章立ては以下の通りであり、各章では、概ね次のようなことが論じられている。

第 1 章「プライバシー：未整理の概念」

プライバシーは、自由主義及び民主主義にとって不可欠であり、国際的に関心を集めているが、包括的で混乱しており、極めて複雑な概念である。しかし、従来型アプローチには限界が存在し、基礎的概念が十分には理論化されていない。そこで、政策立案及び法的解釈に正しい道筋をつけるために、プライバシーの概念化に向けた新しいアプローチが必要である。

第 2 章「プライバシー理論とその欠陥」

法律実務家、法学者、哲学者、心理学者及び社会学者による従来型のアプローチは、統一的かつ単一の概念としてプライバシーを理解し、共通の基準を抽出することを通じて、プライバシーの定義付けを試みるものであった。従来型研究は、6 つのカテゴリー①ウォーレン&ブランダイス論文によるひとりにしておかれる権利、②他者による望まないアクセスから自己を保護する能力、③ある種の事柄の他者からの秘匿化、④個人情報のコントロール、⑤ある人のパーソナリティや個性/個別性、尊厳の保護、⑥ある人の親密な関係や人生の奥深い部分に関わる諸側面についてのコントロールやアクセス制限－に分類される。しかし、いずれの理論も、プライバシーのリスクに関係するものを全て包含した場合には広きに失し、より狭い共通基盤を設ければ、あまりに限定的となる。従来型のプライバシー理論は共通分母を発見することができず、既存の論議には限界がある。

第 3 章「プライバシーの再構築」

プライバシーを概念化する新しいアプローチが必要であり、プライバシー理論には、次に掲げる 4 つの利点がある。

（1）プライバシーは、1 つの共通した特徴を持つものではなく、種々の関連する類似要素で構成されるという発想に基づくべきである（方法）。

（2）トップダウンではなく、ボトムアップ方式を採用し、数多くの個別状況からプラ

---

[20] DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008). 邦訳は、大谷卓史訳『プライバシーの新理論』（みすず書房、2013 年）を参考にした。

イバシー概念の一般化を試みるべきである（一般性）。

（3）プライバシー理論は、あまりに可変的で不確かなものであってはならず、また、永久的又は広範囲に及ぶ有用性を持つべきではない（可変性）。

（4）プライバシーの概念やプライバシー保護は、それ自体で存在するわけではない。プライバシー理論は、プライバシーへの欲求を生み出す個々の問題に焦点を置くべきである（焦点）。

第 4 章「プライバシーの価値」

プライバシーに価値を帰属させるためには、プラグマティズム的方法による説明が適切である。プライバシーは、個人の権利でもなければ普遍的な価値を持つものでもなく、特定の状況においてプライバシーが持つ社会的重要性を基礎に決定付けるべきである。プライバシーは個人の特権という主観的な問題ではなく、社会が何を保護することを適切と考えるかという問題である。

第 5 章「プライバシーの類型論」

プライバシーに影響を与える特定の活動は、(a) 情報収集（監視、尋問）、(b) 情報処理（集約、識別、非セキュリティ、二次利用、個人の排除）、(c) 情報拡散（守秘義務違反、開示、暴露、アクセス可能性の増大、脅迫、盗用、曲解）、(d) 侵害（侵入、意思決定への介入）の 4 つに分類される。この分類は、包括的な原理に基づくものではなく、諸問題に焦点を当てたボトムアップのアプローチである。その目的は、「プライバシー」という用語の内在的意味を説明することから、問題の本質へと議論を移すことにある。

第 6 章「プライバシー：新しい理解」

第 5 章の枠組みを通じてプライバシーを理解することには利点が存在する。また、プライバシーの概念化は必要であり、前記分類法によって、最終的には、プライバシーの法体系を形成し、概念化の道筋をつけるための議論の出発点となることを目指す。

このように、『プライバシーの理解』は、最終的にはプライバシーの概念化を目標にしつつも、従来型のアプローチを捨て去るべきこと、プライバシー侵害をもたらす個別の問題から、プライバシーの概念を多義的に、文脈を重視して捉えるべきことを提案した。ただし、この多義的に捉える発想は必ずしも新しいものではなく、ウォーレン&ブランダイス論文の段階から認識されていたことでもある。

ところで、同書は、第 3 章のうち、「焦点」との関連で、「個人の選好」（individual preferences）に焦点を当ててプライバシー理論を展開することに言及した。しかし、個人はプライバシーに対して多様な態度や信念を抱くことから、「個人の選好」を用いて、うまく機能する法的保護制度を構築することは実質的に不可能であると論じられている。

3. 国のセキュリティ強化と消費者プライバシー保護

3. 1. 国家安全とプライバシー

個人情報の取扱いに目を向けると、米国では、同時多発テロ以降、個人に関する情報を取り扱うのは公的部門か民間部門か、特にその目的は何であるかによって、全く異なるアプローチが取られている。

公的部門が個人に関する情報を取り扱う場面では、判例法上、犯罪捜査のための通信傍受等との関係で、連邦憲法修正第 4 条の定める「不合理な捜索、逮捕又は押収」に該当す

るか否かが争われてきた。この問題について、連邦最高裁判所は、2012 年 1 月 23 日、連邦捜査局（Federal Bureau of Investigation, FBI）等において、令状失効後に、コカイン販売等の被疑者が利用する車体に GPS 装置（Global Positioning System）を取り付け、公道上を走行する同車両の走行経路を追跡した行為について、修正第 4 条に違反すると判断し、注目を集めた[21]。この判決は、同条の今後の解釈に影響を及ぼすリーディング・ケースとなる可能性が高いといわれている。判決後、FBI 法務顧問のアンドリュー・ワイズマン（Andrew Weissmann）氏は、現在使用されている 3,000 の GPS 装置の電源を切ると発言し[22]、ロン・ワイデン（Ron Wyden）上院議員らによる位置情報プライバシー及び監視法案及び他の同種法案[23]が提出されるなどの動きも見られた[24]。

しかし、問題が「テロ対策」の場合には、プライバシー・個人情報保護を犠牲にしても、国の安全を優先すべきという価値判断が働き、それが米国社会の共通認識となってきたと考えられる。米国で行われてきた様々な監視計画のうち、世界的に注目を集めたのは、PRISM 計画である。

2013 年 6 月 6 日、米国ワシントン・ポスト紙と英国ガーディアン紙は、米国の国家安全保障局（National Security Agency, NSA）による PRISM 計画を報道した。これは、テロ対策を目的に、マイクロソフト（Microsoft）、グーグル（Google）、ヤフー（Yahoo!）、フェイスブック（Facebook）、パルトーク（PalTalk）、ユーチューブ（YouTube）、スカイプ（Skype）、AOL、アップル（Apple）の各社から、外国の標的が利用する電子メール、チャット（動画、音声）、ビデオ、写真、蓄積データ、VoIP（Voice over Internet Protocol）、ファイル交換、ビデオ会議、ログインなど標的の活動に関する通知、ソーシャルネットワーキングの詳細などを、NSA と FBI が上記各社から収集するという計画である[25]。

この問題が明るみに出た後の 2013 年 6 月 8 日、国家情報長官（Director of National Intelligence）のジェームズ・R・クラッパー（James R. Clapper）氏は、PRISM に関する概要報告書を公表した。それによると、PRISM は秘密のデータ収集又はデータマイニ

---

[21] United States v. Jones, 132 S. Ct. 945, 181 L. Ed. 2d 911 (2012). 詳細は、土屋眞一「捜査官が GPS により公道を走る被疑者の車を監視することは、違法な捜索か？－最近のアメリカ合衆国連邦最高裁判決」判例時報第 2150 号 3-8 頁（2012 年 7 月）、湯淺墾道「位置情報の法的性質－United States v. Jones 判決を手がかりに－」情報セキュリティ総合科学第 4 号 171-182 頁（2012 年 11 月）。

[22] Julia Angwin, *FBI Turns Off Thousands of GPS Devices After Supreme Court Ruling*, WALL ST. J., (Feb. 25, 2012, 3:36 PM), http://blogs.wsj.com/digits/2012/02/25/fbi-turns-off-thousands-of-gps-devices-after-supreme-court-ruling/.

[23] 同法案は 2011 年に提出された後、2013 年に再提出された。Geolocation Privacy and Surveillance Act of 2013, S. 639, 113th Cong. (2013); Online Communications and Geolocation Protection Act of 2013, H.R. 983, 113th Cong. (2013); Geolocational Privacy and Surveillance Act of 2013, H.R. 1312, 113th Cong. (2013).

[24] 土屋・前掲「捜査官が GPS により公道を走る被疑者の車を監視することは、違法な捜索か？」3、7 頁、湯淺・前掲「位置情報の法的性質－United States v. Jones 判決を手がかりに－」172 頁。

[25] *NSA slides explain the PRISM data-collection program*, WASH POST, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (last updated Jul. 10, 2013).

ング計画ではなく、「裁判所の監視のもと、電子通信サービスプロバイダから、政府が法律上認められた外国諜報情報の収集を容易にするために利用される政府内部のコンピューターシステム」であると述べている。概要報告書では、法律上の根拠は 1978 年外国諜報監視法（Foreign Intelligence Surveillance Act of 1978, FISA）[26]の 2008 年改正法第 702 条であると記載され、米国政府は一方的に電子通信サービスプロバイダのサーバから情報を収集せず、法律上の要件に則って収集していること、「合衆国人」（United States Person）[27]を意図的に標的とすることは許されていないこと、第 702 条に基づく諜報情報の収集は立法・行政・司法分野による広範な監督制度に服していることなどが説明されている。

2008 年 FISA 改正法第 702 条 [28]は、司法長官と国家情報長官の共同許可により、個別の裁判所命令を経ることなく、最長 1 年の間、国外にいると合理的に信じられる合衆国人以外の者を標的に、外国諜報情報の取得を認める規定である。共同許可は、司法長官と国家情報長官の共同認証を承認する裁判所命令、又は、緊急事態が存在する旨の両長官の判断のいずれかに基づくことが求められる [29]。

PRISM 計画を暴露したのは、中央情報局（Central Intelligence Agency, CIA）の元技術職員であったエドワード・スノーデン（Edward Snowden）氏であり、この人物は、2013 年 8 月 1 日、ロシアから 1 年間の滞在許可を受け、現在はロシアに滞在している。

米国政府がテロ対策のために情報を収集する際には、国家安全保障令状（National Security Letter, NSL）の方法を用いることもできる。2001 年愛国者法（USA PATRIOT ACT of 2001）[30]は、1986 年電子通信プライバシー法（Electronic Communications Privacy Act of 1986, ECPA）[31]の「電話料金及び取引記録への対諜報目的のアクセス」[32]の規定を改正し、捜査機関が情報収集を行える範囲を拡大した。この規定によると、FBI の長官等は、国際テロリズム又は秘密諜報活動を防止するための捜査活動であることを書面により証明すれば、裁判所命令等を得ることなく、有線通信サービス又は電子的通信サービスプロバイダに対し、氏名、住所、サービスの期間及び電話料金記録といった通信にかかる情報の開示を要求することができる。上記各プロバイダ又はその職員等は、FBI 長官等において、合衆国の国家安全、犯罪・テロ対策・諜報対策の捜査への不法な妨害等への危険が生じうることを証明した場合には、FBI による情報又は記録へのアクセスに関する守秘義務を課せられる。NSL はその濫用的運用が問題視されている。

また、愛国者法は、FISA を改正し、「国際テロリズム又は秘密諜報活動に対抗するため

---

[26] 50 U.S.C. §§ 1801-1885c (2011).

[27] 合衆国の市民、適法に永住権を認められた外国人、合衆国市民若しくは適法に永住権を認められた外国人を相当数の構成員とする権利能力なき社団、又は合衆国で設立された法人が含まれる。ただし、外国勢力である法人や社団は含まない。

[28] 50 U.S.C. § 1881a (2011).

[29] 50 U.S.C. § 1881a (a),(c)(2),(i)(3)(2011).

[30] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. 107-56, 115 Stat. 272 (codified as amended in scattered sections of 18 U.S.C., 50 U.S.C.).

[31] Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2522, 2701-2712, 3121-3127 (2012).

[32] 18 U.S.C. § 2709 (2012). NSL については、岡本篤尚『《9・11》の衝撃とアメリカの「対テロ戦争」法制―予防と監視―』（法律文化社、2008 年）127 頁以下。

の授権された捜査活動」に関する場合には、通信関連以外の記録を提出させられるようにした[33]。FBI 長官等は、合衆国人が関係しない外国諜報情報を取得し、又は国際テロリズム若しくは秘密諜報活動の防止を目的とする捜査のために、有形物（帳簿、記録類、書類、資料その他のものを含む。）の作成を求める命令を請求する権限を有する。これにより、電話のメタデータ収集を行うことができる。捜査の実施は、大統領命令第 12333 号[34]に基づき司法長官によって承認された指針に従うこと等が条件付けられている。同令第 2.3 条以下は、諜報機関が合衆国人に関する情報を収集、保有等する場合を規定している。

その他、愛国者法は、1978 年金融プライバシー権利法を改正し、金融機関に、顧客又は事業者の金融記録を FBI に提出させることを可能にした[35]。同様に、1970 年公正信用報告法も改正され、信用報告機関は、消費者が口座を有する全金融機関の名称及び連絡先や、消費者の氏名、住所、勤務先等を FBI に提出することを義務付けられた[36]。

その後も NSA の情報収集問題は度々報じられた。2013 年 10 月 24 日には、ドイツのメルケル首相を含む、世界の指導者 35 人の電話を盗聴していたことが明るみに出て、米国は欧州から厳しい批判を受けた。2014 年 1 月 15 日には、NSA が世界各地の 10 万台近いコンピュータに情報収集用のソフトウェアを埋め込むなどして、主に中国を監視していることも報じられた。

オバマ大統領は、こうした一連の問題を受け、2014 年 1 月 17 日、NSA 改革案を発表した[37]。そこでは、通信情報収集活動は適法な安全保障目的に限定し、普通の人々の電子メールや電話を見境なく閲覧するためには用いないこと、諜報機関は、対諜報活動や対テロのような特別の安全保障要件を満たした場合にのみ当該データを利用すること、差し迫った安全保障上の目的がない限り、親密な友好国や同盟国の指導者の通信を監視しないこと、大量のメタデータ収集計画を停止し、政府以外の機関が政府の必要とするデータを保管できるような仕組みを設けることなどが明らかにされた。ただし、これまでの活動には濫用はなかったこと、歴史的に、米国の安全と自由は情報収集活動によって守られてきたことも強調された。

しかし、プライバシー及び市民的自由監視委員会（Privacy and Civil Liberties Oversight Board）は、2014 年 1 月 24 日、「愛国者法第 215 条に基づき実施された電話記録計画及び外国諜報監視裁判所の運用に関する報告書」（Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT ACT and on the Operation of the Foreign Intelligence Surveillance Court）を公表した。同委員会は、NSA の電話記録計画は、連邦憲法修正第 1 条及び第 4 条に基づく懸念を提起するとの立場に立ち、愛国者法に基づく電話記録収集計画の停止、外部の法律家による外国諜報監視裁判所

---

33 50 U.S.C. § 1861.
34 46 Fed. Reg. 59, 941 (Dec. 4, 1981).
35 12 U.S.C. § 3414 (a)(5)(A).
36 15 U.S.C. § 1681u. 岡本・前掲『《9・11》の衝撃とアメリカの「対テロ戦争」法制―予防と監視―』129 頁。
37 White House, *Remarks by the President on Review of Signals Intelligence* (Jan. 17, 2014), http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

の支援、透明性向上を含む 12 項目の勧告事項を取りまとめている [38]。なお、委員会は、NSA の情報収集を適法とする委員と違法とする委員に分かれた。

また、グーグルは 2010 年から、マイクロソフト（スカイプを含む）、フェイスブック、アップルは PRISM 問題を受け、各国政府から情報開示要請のあった件数を開示するようになった。これらの企業は、NSA 改革案が出たところで、透明性レポートの改善について合意したと報じられ、FISA や NSL に基づくリクエスト数、ユーザー数/アカウント数（1,000 件単位）を明らかにするようになった [39]

NSA の情報収集活動は裁判上も争われている。コロンビア地区連邦地方裁判所は、2013 年 12 月 16 日、電話のメタデータを大量に収集する NSA の計画は修正第 4 条に違反する実質的可能性が高いとの判断を下したが [40]、ニューヨーク南地区連邦地方裁判所は、同年 12 月 27 日に適法と判断し、連邦地裁レベルでの判断は分かれている。

3．2．消費者プライバシー保護

民間部門に目を向けると米国では、「消費者プライバシー保護」への取組を進めており、日本でも注目を集めている。

3．2．1．消費者プライバシー権利章典

2012 年 2 月 23 日、オバマ大統領は、「ネットワーク社会における消費者データプライバシー：グローバル化したデジタル経済において、プライバシーを保護しイノベーションを促進するための枠組み」（Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy）（以下「消費者データプライバシー」という。）[41]と題する政策大綱に署名した。この政策大綱は、「消費者プライバシー権利章典」と題する 7 原則、法的に執行可能な実施基準、「不公正若しくは欺瞞的行為又は慣行」に関する連邦取引委員会（Federal Trade Commission, FTC）の法執行権限、国際的相互運用可能性を主な要素に掲げている。消費者プライバシー権利章典は、FIPPs から発展してきた原則である。

表 1　消費者プライバシー権利章典

第 1 原則 個人のコントロール	消費者は、企業が消費者からいかなる個人データを収集し、どのように利用するかについて、コントロールを行使する権利を有す

[38] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT, http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf (2014).

[39] 例えば、Google 透明性レポート（http://www.google.com/transparencyreport/userdatarequests/US/）。

[40] 裁判所は、NSA のメタデータ収集を禁止し、政府に対して収集したメタデータの破棄を命じたが、重大な国家安全の利益に照らして、命令の行使を停止した。

[41] White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 23, 2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

	る。
第 2 原則 透明性	消費者は、プライバシー及びセキュリティの実務について、容易に理解できアクセス可能な情報を得る権利を有する。
第 3 原則 状況の尊重	消費者は、企業において個人データを収集し、利用し、そして開示する際には、消費者がデータを提供する状況に適合した方法によることを期待する権利を有する。
第 4 原則 安全性	消費者は、安全かつ責任を持って個人データが取り扱われる権利を有する。
第 5 原則 アクセス及び正確性	消費者は、データの機微性及びデータが不正確な場合に消費者に不利な結果をもたらすリスクに適した態様において、利用可能な書式によって、個人データにアクセスし、訂正する権利を有する。
第 6 原則 制限的収集	消費者は、個人データを収集及び保有する企業に適切な制限を課す権利を有する。
第 7 原則 責任	消費者は、企業が個人データを取り扱う際に、プライバシー権利章典を確実に厳守するための適切な措置とともに行わせる権利を有する。

消費者プライバシー権利章典のうち、第 1 原則及び第 2 原則は、後述する FTC のプライバシー・レポートでも取り上げられており、米国のプライバシーを構成する主な要素であるといえる。

まず、第 1 原則は、現代的プライバシー権を受け継ぐ内容となっている。同原則に関しては次のように説明されている。

「企業は、消費者に対し、消費者が他者と共有する個人データに対し、また、企業が個人データを収集、利用、開示する方法に対する適切なコントロールを与えるべきである。企業は、企業が収集し、利用し、開示する個人データの規模、範囲及び機微性に対応するとともに、個人データに関する利用の機微性にも対応する形で、容易に利用されアクセス可能な仕組みを消費者に与えることによって、これらの選択を可能にするべきである。企業は、消費者に対し、個人データの収集、利用及び開示に関する意味のある決定を下せるような時期及び方法を提示し、明確で簡明な選択を与えるべきである。企業は、消費者に対し、最初に同意を付与する方法と同様に、同意を撤回し又は制限するための、アクセス可能で容易に利用できる方法を示すべきである」。この説明文は、個人データの収集、利用、開示に関する意味のある決定を「選択」と表現しており、そのための容易かつアクセス可能な仕組みを提供すべきことを求めている。同様に、同意の撤回又は制限も「選択」に含まれる。

個人のコントロールには 2 つの側面が存在すると説明されている。第 1 は、企業によるデータの収集時に、問題の個人データに関して、データセットにその活動が含まれる個人の数（規模）、データセットに反映された活動、興味、期間の範囲（範囲）、機微性にとって適切な、データの共有、収集、利用、及び開示に関する「選択」を提供することである。例えば、サーチエンジン、広告ネットワーク、オンラインソーシャルネットワーク等、個

人のインターネット利用履歴に関する大部分にアクセスする企業は、徐々に、個人の行動に関する詳細なプロフィールを蓄積することができる。また、オンライン上での行動ターゲティング広告を提供するために、第三者による個人データの収集も行われるが、この広告の仕組みは、異なるウェブサイトを超えて、個人の消費者ー又は少なくともそのデバイスーを追跡できる広告ネットワークを展開させる。このような第三者も「選択」を提供しなければならない。

コントロールの有するもう 1 つの側面は、選択に対する消費者の責任である。消費者データプライバシーによれば、消費者は、個人データの利用や共有に対する自らの選択を評価し、その選択に責任を負うべきと記されている。

第 2 原則の「透明性」は、「消費者がプライバシーのリスクを意味ある形で理解し、個人のコントロールを行使できるようにするために、企業は、自らがいかなる個人データを収集し、そのデータがなぜ必要であり、どのようにそれを利用し、そのデータをいつ消去し又は消費者のデータを匿名化するか、及び、第三者と個人データを共有する可能性の有無及び共有する目的について、最も有用な時及び場所において、明確な説明を提供すべきである」と説明されている。これは、第 1 原則の前提として求められる原則である。

また、消費者データプライバシーは、プライバシー権利章典の立法化にも言及した。同章典の 7 つの諸原則は、実施基準を通じて関係者に実行を促すとともに、議会と協力して、立法化を通じてこれらの権利を制定することが意図されている。

2014 年 2 月 28 日現在、諸原則の立法化は実現していないものの、政府監査院（Government Accountability Office, GAO）は、2013 年 9 月に「情報再販者：消費者プライバシーの枠組に、技術及び市場の変化を反映させる必要性」（INFORMATION RESELLERS: Consumer Privacy Framework Needs to Reflect Changes in Technology and the Marketplace）と題する報告書を公表し、「情報再販者」（information resellers）を含め、民間企業間の個人情報の収集・販売を司る包括的連邦プライバシー法の必要性を主張した[42]。

3．2．2．FTC プライバシー・レポートとオンライン・プロファイリング

3．2．2．1．FTC プライバシー・レポート

FTC は、2010 年 12 月 1 日、事業者及び政策立案者向けの枠組案としての「急変する時代の消費者プライバシー保護」（Protecting Consumer Privacy in an Era of Rapid Change）と題するスタッフ中間報告を公表し、2012 年 3 月 26 日に FTC の報告書として最終取りまとめを行った[43]。最終報告書は、「プライバシー・レポート」と呼ばれており、

---

[42] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-13-663, INFORMATION RESELLERS: CONSUMER PRIVACY FRAMEWORK NEEDS TO REFLECCT CHANGES IN TECHNOLOGY AND THE MARKETPLACE (2013), http://www.gao.gov/assets/660/658151.pdf.
なお、セキュリティ侵害との関係では、2014 年 1 月 8 日に、「2014 年パーソナルデータ・プライバシー及び安全法案」が提出された。これは、大手小売チェーンであるターゲット社から、2013 年終わりに 4,000 万件のクレジットーカード及びデビットカードの情報が漏えいし、2014 年 1 月には、さらに 7,000 万件の情報漏えいが発覚した事故の発生などを受けて提出されたものである。Personal Data Privacy and Security Act of 2014, S.1897, 113th Cong. (2014).

[43] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid*

消費者データプライバシーを受ける内容となっている。

FTC は、消費者保護の一環として、民間部門のプライバシー保護関連法の執行を担う機関であり、米国におけるその役割は重要である。FTC は、2013 年 12 月 31 日現在、全分野で 74 の法律を所管しており、そのうち、消費者保護の分野に関わる法律は 56 本である[44]

FTC の法執行権限には、監督権限、準立法的権限、準司法的権限がある。

監督権限に関しては、FTC 法に基づく一般的な情報収集及び調査権限のほかに[45]、サピーナ（subpoena）による証人喚問や証拠文書の提出[46]、民事審査請求（Civil Investigation Demand）[47]等の強制的な調査権限などがある。FTC は、調査の結果、法的措置を講じるべきと判断した場合には、審判手続によって排除命令を下すこととなり、その根拠規定が FTC 法第 5 条の定める「不公正若しくは欺瞞的行為又は慣行」（unfair or deceptive acts or practices）[48]である。ただし、かかる準司法的権限によらずとも、実際は、同意命令（consent order）により処理されることが多い。また、FTC は、準立法的手続としての規則制定権及びその違反等に対する提訴権を有している。規則制定権は、迷惑メール防止法である「2003 年キャン・スパム法」[49]、1998 年児童オンライン・プライバシー保護法[50]、1970 年公正信用報告法[51]、1999 年金融サービス近代化法[52]、1996 年健康保険の移動性及び責任性に関する法律[53]などに基づいている。これらの法律は、FTC に法執行権限を委ねており、違反行為を「不公正若しくは欺瞞的な行為又は慣行」に該当すると定め、提訴権等を付与している。

FTC 法第 5 条が存在感を見せるのは、セクトラル方式の法律が適用されない分野におい

Change, Recommendations for Businesses and Policymakers (Mar. 26, 2012), http://ftc.gov/os/2012/03/120326privacyreport.pdf.

44 Federal Trade Commission, *Statutes Enforced or Administered by the Commission*, http://www.ftc.gov/ogc/stat3.shtm (last visited, Feb. 28, 2014).

45 15 U.S.C. § 46(a).

46 15 U.S.C. § 49.

47 15 U.S.C. § 57b-1.

48 15 U.S.C. § 45(2012). 詳細は、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第 8 号〇頁以下（後日追加）。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（平成 20 年度）」105 頁以下（牧山嘉道担当執筆）参照。

49 Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 15 U.S.C. §§ 7701-7713 (2012); Can Spam Rule, 16 C.F.R. pt. 316 (2013).

50 Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (2012); Children's Online Privacy Protection Rule, 16 C.F.R. pt. 312 (2013).

51 *Supra* note 17; Fair Credit Reporting Act Rules, 16 C.F.R. pts. 600-698 (2013).

52 Financial Services Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codified in relevant part at 15 U.S.C. §§ 6801-6809 and §§ 6821-6827, as amended); Privacy of Consumer Financial Information, 16 C.F.R. pt. 313 (2013); Standards for Safeguarding Customer Information, 16 C.F.R. pt. 314 (2013).

53 Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 26 U.S.C., 29 U.S.C., 42 U.S.C.); Health Breach Notification Rule, 16 C.F.R. pt. 318 (2013).

て、民間事業者の自主的取組を担保する場面である。自主的取組に関する「不公正若しくは欺瞞的な行為又は慣行」の典型例は、事業者がプライバシー・ポリシーに違反して個人情報を取り扱う場合である。最近では、グーグルがサファリ利用者のオプト・アウト設定を回避してウェブ閲覧履歴の追跡及び広告表示を行っていた行為について、2012 年 8 月 9 日、2,250 万ドル（当時のレートで約 17 億 7,000 万円）の制裁金を支払う旨を同意したことが公表された。2014 年 1 月 15 日には、アップルが、児童のアプリ内課金を親の同意なく行っていたことについて、少なくとも 3,250 万ドル（約 33 億 8,000 万円）を消費者に返金することで、同意に達した旨が発表された。

また、FTC の活動については、法執行のみならず、種々の報告書を公表している点も重要である。FTC では、電子商取引の普及に伴い、1990 年代後半頃より、消費者プライバシー保護への取組を積極的に行うようになり、特に、2007 年頃からは、行動ターゲティング広告との関係で、重要な報告書をいくつか公表した。プライバシー・レポートはその 1 つである。

プライバシー・レポートは、個人識別可能情報との関係で適用範囲 [54]を検討したこと、「プライバシー・バイ・デザイン」（Privacy by Design）、「単純化された消費者の選択」、「透明性」という 3 つの柱を枠組みに据えたこと、消費者選択の 1 つとして、追跡拒否（Do Not Track）の仕組みを提案したこと等において、米国のプライバシー保護に関する考え方を示した重要な報告書である。このレポートが示した枠組勧告の要旨は、次の通りである [55]。

表 2　プライバシー・レポートが示した枠組勧告の要旨

範囲 最終的範囲：枠組は、特定の消費者、コンピュータ又は装置と合理的に結びつけられる消費者データを収集又は利用する全ての営利事業者に適用される。ただし、当該事業者が、年 5,000 人未満の消費者の非センシティブデータのみを収集し、第三者との間でそのデータを共有しない場合は、この限りではない。
プライバシー・バイ・デザイン 基本原則：企業は、組織全体並びに製品及びサービス開発の各段階で、消費者プライバシーを促進すべきである。
A.　実体的原則 最終原則：企業は、データセキュリティ、合理的な収集制限、健全な保存及び破棄の実務、並びにデータの正確性など、実体的なプライバシー保護を実務に組み込むべきである。
B.　実体的原則を実施するための手続的保護 最終原則：企業は、製品及びサービスのライフサイクル全体にわたって、包括的なデータ管理手順を整備すべきである。
単純化された消費者の選択 基本原則：企業は、消費者の選択を単純化すべきである。

[54] 本稿では言及しないが、いわゆる FTC3 要件については、拙稿「アメリカにおけるビッグデータの利用と規制」ジュリスト 2014 年 3 月号 32 頁以下。

[55] このレポートに含まれる最終的なプライバシー枠組勧告は、議会がプライバシー立法を検討する際の助けとなることも意図している。ただし、枠組が現行の法的義務を超える範囲では、現行法に基づく法執行活動や規則のひな形の役割を果たすものではない。

A.　選択を要しない実務 最終原則：企業は、取引若しくは企業と消費者の関係に関する状況に即した実務、又は、法により義務づけられ若しくは個別に権限を与えられた実務のために消費者データを収集及び利用する前に、選択を提供する必要はない。
B.　企業は、他の実務のため消費者に選択を与えるべきである。 最終原則：選択が要求される実務に対し、企業は、消費者が自らのデータに関する決定を下す時期及び状況において、選択を提供すべきである。企業は、（1）データ収集時に主張されたものと実質的に異なる態様で消費者データを利用する、又は、（2）一定の目的のためにセンシティブデータを収集する前に、積極的な明示的同意を得るべきである。
透明性 基本原則：企業はプライバシー実務の透明性を高めるべきである。
A.　プライバシー通知 最終原則：プライバシー通知は、プライバシー実務をより良く理解し比較できるようにするために、より明瞭、簡潔かつ標準化したものにすべきである。
B.　アクセス 最終原則：企業は、自らが保有する消費者データへの合理的なアクセスを提供すべきであり、アクセスの範囲は、データの機微性及びその利用の性質に見合うようにすべきである。
C.　消費者教育 最終原則：全ての関係者は、商業的データプライバシー実務に関して消費者を教育する努力を拡大すべきである。
立法面の勧告 議会は、基本的なプライバシー法を制定すべきであり、データセキュリティ及びデータブローカーの立法化も必要である。同時に、産業界は、自主規制への取組を加速すべきである。
今後 1 年間にわたる 5 つの主要分野
1　DNT の仕組みの推進 2　携帯電話サービス提供事業者によるプライバシー保護の改善 3　データブローカーによる消費者情報の収集利用をコントロールするための立法化提案 4　ISP（Internet Service Provider）や OS（Operating System）提供者等の大規模プラットフォーム事業者による消費者行動の追跡への対応 5　FTC 法第 5 条に基づく執行可能な自主規制基準の推進

「プライバシー・バイ・デザイン」は、カナダのオンタリオ州のプライバシー・コミッショナーであるアン・カブキアン（Ann Cavoukian）氏が提案し、世界的に普及した考え方である。「選択」及び「透明性」は、消費者プライバシー権利章典の中にも掲げられており、これらは、アメリカの重視する FIPPs の主たる要素を表している。

3．2．2．2．オンライン・プロファイリング

消費者データプライバシー及び FTC の報告書を通じて見ると、着目すべきプライバシー侵害のある側面を見出すことができる。ここでは、「プロファイリング」の問題を取り上げる。

「プロファイリング」は、消費者プライバシー権利章典の第 1 原則の説明でも言及されているところであるが、より遡ると、FTC が 2000 年 6 月に公表した「オンライン・プロファイリングに関する報告書」（Online Profiling: A Report to Congress）[56]において、次

[56] FTC, *Online Profiling: A Report to Congress* (Jun. 2000)
http://www.ftc.gov/reports/online-profiling-federal-trade-commission-report-congress.

のように、詳細なプロフィールが形成されることによるプライバシー問題が検討されている。

「一旦収集されると、消費者データは解析され、第三者の情報源からの人口統計データ及び『サイコグラフィック』[57]なデータ、消費者のオフラインの購買データ、又は、調査及び登録書式を通じて消費者から直接収集した情報と結びつけることができる。この強化されたデータにより、広告ネットワークは、各消費者の興味や嗜好について様々な推論を行えるようになる。その結果が、個々の消費者の好み、ニーズ、及び購買習慣を予想しようと試みる詳細なプロフィールで、それにより広告企業のコンピュータは、消費者個別の興味を直接狙った広告をどのように提供するかを瞬時に決定できる。広告ネットワークが作成したプロフィールは、極めて詳細なものとなり得る。

ネットワーク広告企業が置いたクッキーは、その企業が提供するウェブサイト上で消費者を追跡することができ、その結果、全く共通点のない無関係なウェブサイトにまたがってデータを収集できるようになる。また、広告ネットワークが用いるクッキーは一般的に無期限であるため、その追跡は、長期にわたって行われ、個人がインターネットにログオンするたびに再開される。この『クリックストリーム』情報が第三者のデータと結び付くとき、こうしたプロフィールが数百もの異なるデータフィールドを含むこともあり得る。

ネットワーク広告企業とそのプロファイリング活動は、ほぼどこでも行われるが、消費者には見えないことがほとんどである。消費者が訪れるウェブサイトで目にするものは、表示されるウェブページの継ぎ目のない不可欠な部分として表れるバナー広告だが、ウェブページには消費者に何ら通知をせずにクッキーが置かれている。消費者が訪問するウェブサイトが、広告ネットワークの存在とデータ収集を通知しない限り、消費者は、オンライン上の活動が監視されていることに全く気付かないであろう。」

その後、FTC は、2007 年 12 月 20 日、「オンライン上の行動広告：実行可能な自主規制諸原則に向けた議論の動向」（Online Behavioral Advertising: Moving the Discussion Forward to Possible Self-Regulatory Principles）を取りまとめている（2009 年改訂）[58]。この報告書を検討する段階では、2007 年 11 月に対話集会（“Ehavioral Advertising Town Hall”）が開催され、その参加者からプロファイリングに関する指摘がなされた。そこでは、消費者にはデータ収集が見えないこと、実務に関する現行の開示に欠点が存在すること、消費者に関する詳細なプロフィールを作り上げて蓄積される可能性があること、健康、資産又は子供に関するセンシティブデータを含むデータを行動広告のために収集し、それが誤った手に落ち、又は予想外の目的のために利用されるリスクが存在することへの言及があった。

「プロファイリング」は、ここ数年の間に、EU の一般データ保護規則提案や欧州評議

---

[57] 潜在顧客を分類する際に用いられる消費者のライフスタイル、態度、価値観、信条などの測定技術、消費者の価値観を意味する。

[58] Federal Trade Commission Staff Report, *Self-Regulatory Principles For Online Behavioral Advertising: Tracking, Targeting, and Technology* (Feb. 12, 2009), http://www.ftc.gov/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral.

会の閣僚委員会勧告[59]などでも取り上げられており、ビッグデータ時代では、プロファイリングに対応する保護措置を考える必要性が高まっている。

4. 2013 年インタビュー

筆者は、米国のプライバシーの動向を調査すべく、2013 年 6 月、FTC、商務省（Department of Commerce）、電子プライバシー情報センター（Electronic Privacy Information Center, EPIC）の関係者と意見交換を行った。プライバシー・個人情報保護をめぐる動向は日々変化しており、2013 年 6 月のインタビュー時点から変更された事柄もあるが、それぞれの担当者から聞いた話を部分的に取り上げることとする。

4. 1. FTC

① 法執行

・法執行の実施例は多い。プライバシー・レポートでは、各州で制定されているデータ侵害法を連邦レベルで制定すべきという指摘もある。

・FTC は、連邦のプライバシー法の執行者であるが、その他にも多くのアクターが存在している。カルフォルニア州は代表的な州であり、グーグルやアップルなども州の規律に従っている。

・FTC は市場を見ており、スタッフはニュースや新聞だけでなく、企業ニュースや　消費者の苦情等から情報を集めている。消費者からは、去年は合計で約 100 万の苦情があった（プライバシー以外を含む）。もし、企業の情報漏えいに関する情報が入ってきたら、これらの苦情等を証拠として確認している。また、FTC にはモバイル研究所があり、携帯デバイスからどの情報がどこに蓄積されるかを確認できる。COPPA 規則の改訂によって影響を受けると思われる 90 社に教育レター（education letter）を送付した[60]。

② 包括的連邦プライバシー法の制定等

・どの程度時間がかかるのか、法制化されたときの所管組織がどこになるのか等、予想することは難しい。

・グーグル、フェイスブック、コムスコアは、プライバシー・ポリシーを侵したことで、民間から訴訟提起されている。データブローカーについては、FCRA に基づき個人信用調査機関（credit bureau）への提訴等がなされている。今後、データブローカー法といったものが制定されると、このような状況に対応できるのかもしれない。

・データ侵害通知に関する連邦法が制定される可能性は分からない。

③ EU 一般データ保護規則提案

---

[59] 2010 年 11 月 23 日「プロファイリングの状況における個人データの自動処理に関する個人の保護についての閣僚委員会の加盟国に対する CM/Rec（2010）13 勧告」（*Recommendation CM/Rec (2010) 13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling*, CM/Rec (2010) 13 (Nov. 23, 2010), https://wcd.coe.int/ViewDoc.jsp?id=1710949）。

[60] Press Release, *FTC Sends Educational Letters to Businesses to Help Them Prepare for COPPA Update* (May 15, 2013), http://www.ftc.gov/opa/2013/05/coppa_education.shtm.

・重要な点は、情報の相互運用性である。我々はセーフハーバー・プライバシー協定[61]の重要性を指摘している。相互運用性に関する主な関心は執行協力である。法執行を世界的に展開するための情報を EU からも取得できるのかという点が重要になる。
・セーフハーバー・スキームが終了した場合は、FTC 以外の多くのアクターとの議論が必要となる。他には、EU の十分性（adequacy）を、国レベルではなく企業レベルで構築するという点が重要であると認識している。
・「忘れられる権利」[62]の執行は非常に難しい。米国と EU には文化的な違いがある。米国では表現の自由の権利が強い。

2013 年 6 月のインタビュー結果は以上の通りであるが、その後、筆者は、同年 9 月 25 日から 26 日にかけて開催された第 35 回データ保護・プライバシー・コミッショナー国際会議（International Conference of Data Protection and Privacy Commissioners）に参加した。そこでは、コミッショナーのジュリー・ブリル（Julie Brill）氏がプレゼンテーションを行い、具体例と共に、積極的な法執行を実施している旨の説明が行われた。この会議は、欧州のコミッショナーが主要メンバーとなっていることから、対外的には法執行を通じてプライバシーを担保している旨を強調する意図があると考えられる。

また、FTC は、2014 年 1 月 21 日、セーフハーバー・プライバシー協定に違反した企業名を公表するなど、欧州向けの情報を発信している[63]。

4．2．商務省

商務省では、越境データ流通に関する担当者、及び、モバイルプライバシーの実施基準策定に関する担当者と意見交換を行った。両者ともに、プライバシー権利章典の法制化について、包括的な連邦法制定の必要性には一定の理解を示しつつも、具体的な法制化の時期は見通しが立っていないとの見解を示した。実施基準策定に関する担当者からは、法制化された場合には、全ての企業が（プライバシー諸原則への）準拠を求められ、違反すると FTC から法執行を受けることから、企業が行動規範を遵守した場合には、FTC の法執行から外すためのセーフハーバーを設け、企業に遵守のインセンティブを付与すべきとの立場が示された。

EU の一般データ保護規則提案の十分性に関して、越境データ流通の担当者からは、国レベルではなく企業レベルの十分性が重要であり、柔軟性が求められるとの話があった。

---

[61] 1995 年 EU データ保護指令は、十分なレベルの保護措置を講じていない第三国に対するデータ移転制限条項を定めている。セーフハーバー合意は、データ移転制限に伴う取引障壁を取り除くため、EU と米国の間で 2000 年に締結された協定である。セーフハーバーに加入を希望する組織は、セーフハーバー原則を自主的に遵守し、それを商務省に自己認証することにより参加が認められる。

[62] 欧州議会の LIBE 委員会の採択案では、「忘れられる権利」という言葉は削除され、「削除権」へとタイトルが変更された。

[63] Press Release, *FTC Settles with Twelve Companies Falsely Claiming to Comply with International Safe Harbor Privacy Framework* (Jan. 21, 2014), http://www.ftc.gov/news-events/press-releases/2014/01/ftc-settles-twelve-companies-falsely-claiming-comply.

4．3．EPIC

EPIC は、1994 年に設立され、ワシントン D.C.に拠点を置く権利擁護団体である。団体の性格上、プライバシー保護への考え方は、FTC や商務省とは大きく異なる。

EPIC は、2013 年 6 月の PRISM 問題が発生した後、連邦最高裁判所に対し、NSA に国内通話記録の収集を許可した外国諜報監視裁判所の命令を無効とするよう求める文書を提出するなど[64]、市民のプライバシーを保護するための活動を積極的に行っている。

インタビュー結果は以下の通りである。

① 米国の消費者プライバシー保護の状況について

・過去 20 年にわたり、FTC 法第 5 条は、消費者プライバシー保護のベースラインとなっており、法的問題に対処してきた。グーグルやフェイスブックに対する同意命令で成功したが、制裁金は企業の発展可能性からすると高いとはいえない。

・FTC 法第 5 条は、プライバシー法ではなく、取引規制法であり、権限の限界がある。FTC はセキュリティを規制する権限を持たない。

・消費者プライバシー権利章典の 7 原則は、共同規制的モデルであり、マルチステークホルダープロセスが採用されている点が問題である。行動規範の策定にも数年を要する。

・企業が消費者プライバシー権利章典の原則に違反した場合、市民は、州の司法長官又は FTC に苦情を申し立てることはできるが、自らが訴訟を提起する方法は用意されていない。州の司法長官や FTC は、何が侵害を構成するかについての（消費者の）理解を信頼しないかもしれない。集団訴訟による解決に辿り着くには、消費者がその訴訟に参加しなければならず、制約がある。

② 消費者プライバシー権利章典の立法化の目処

・今年ではなく、おそらく来年でもない。その原因には 3 つの要素がある。第 1 は、どの程度、マルチステークホルダープロセスや共同規制手続が立法化を後押しする流れとなるか、という点である。消費者団体が手続に参加できず、手続の適法性が失われれば、立法化への圧力が強まる。マルチステークホルダープロセスが継続的かつ広範囲に進展すると、立法化への後押しは出てこない。政府がこのプロセスを最良であると判断すれば、立法化と同様の代替手段として扱われる。第 2 は、どの程度、消費者プライバシーがイデオロギー的対立を生むのかという点である。グーグルやフェイスブックのような事業者は、ロビー活動を強化し、いくつかの事例に成功している。第 3 は、どの程度、新しい技術の発展が平均的な消費者のプライバシーを侵害すると考えられるのか、という点である。グーグルグラスのようなウェアラブルコンピュータと顔認証を連結させると、深刻なプライバシー侵害が生じうる。しかし、新しい技術が普及するのに要する時期は不明で、5 年ほどかかることもありうる。

③ EU 一般データ保護規則提案

・採択されるまでにはいくつかの変更があるであろう。一般データ保護規則提案の効果には、グローバルな保護レベルを上げることなどがある。多国籍企業やグローバル企業にと

---

64 Electronic Information Privacy Center, *On Petition for a Writ of Mandamus and Prohibition, or a Writ of Certiorari, to the Foreign Intelligence Surveillance Court* (Jul. 8, 2013), https://epic.org/EPIC-FISC-Mandamus-Petition.pdf.
連邦最高裁は、2013 年 11 月 18 日、理由を付さずに EPIC の申立を却下した。

って、統一的なデータ保護基準を適用することは、多様な基準を適用するよりも、経済的に効率的である。
・「忘れられる権利」[65]について、表現の自由との矛盾を来すことなくこの権利を実施する 1 つの方法は、インターネットに散在する情報全てに適用するのではなく、サービス提供者や企業において利用可能な個人データに適用することである。例えば、フェイスブックの利用者が自らの個人情報を消したい場合には、サービス提供者にとって利用可能であった情報を消去対象とすべきである。
・欧州委員会が提案した 2%[66]の制裁金は、事業者にとって必ずしも不当な負担にはならない。なぜなら、DPA（Data Protection Authority）には、違反の深刻性に応じた裁量があることから、違反があれば自動的に 2%が課せられるわけではない。法執行機関が、正当な範囲を超えて懲罰的な執行を行わないことを信頼すべきである。
・事業者の反応はかなり消極的である。他方で、法律違反は事業を行う上でのコストでもある。米国には多くの労働環境の安全に関する法があるものの、違反への制裁は極めて軽い。事業者は、違反して罰金を払う方がコストは低いため、遵守しようとせず、その方が危険である。

4．4．インタビューによる示唆

米国は、柔軟性を重視し、企業が自らの約束を違えた場合に、FTC に個別的な法執行を委ねるという方式により、プライバシーを保護するというスタイルを取っている。消費者プライバシー権利章典に関しては、連邦レベルでの立法化は現実的ではないとの共通的立場が示された。また、政府関係者によるルール制定への考え方は、①自主的な行動規範、②企業による遵守表明、③違反の場合の個別的法執行、④行動規範が遵守された場合のセーフハーバーという 4 つの要素を含めるという点で共通しており、特に欧州に対しては、企業レベルの「十分性」を主張するとともに、FTC の役割の重要性を強調する傾向にある。

ところで、2013 年 6 月は、ちょうど PRISM 問題が発覚した時期であり、米国の政府関係者も EPIC も、この問題が欧州に与える影響を十分には予測していない様子であった。しかし、NSA による情報収集が次々と発覚したことは、米国のプライバシー保護体制に影響を与える可能性がある。例えば、欧州委員会は、2013 年 11 月 27 日、「EU 市民と EU 内で設立された企業の観点によるセーフハーバーの機能に関する欧州議会及び閣僚理事会への伝達文書」（Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU）[67]を公表し、米国に対し、13 項目の勧告を示すとともに、2014 年夏までに改善策を提示するよう求めている。米国がこの勧告に

---

65 欧州議会の LIBE 委員会改正案では、「忘れられる権利」という表現は削除されている。
66 欧州議会の LIBE 委員会改正案では、1 億ユーロ、又は企業の場合は全世界の年間総売上の 5%までの制裁金へと変更されている。
67 *Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU*, COM (2013) 847 final (Nov. 27, 2013), http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf.

対応するか否かは不透明であるが、セーフハーバーの見直し論議には引き続き留意する必要がある。

5.「プライバシー外交」のための「プライバシー」

以上を踏まえ、日本が「プライバシー外交」を行うにあたって、米国の議論からどのような示唆を受けることができるかを検討する。

まず、改めて認識すべきことは、米国と日本の違いである。米国は、プライバシー権の提唱国であり、プライバシー論議の先進国でもあった。しかし、特に同時多発テロ以降、政府機関はテロ対策を目的に個人に関する情報を見境なく大量収集するようになり、個人のプライバシーは軽視されているといわざるを得ない。民間部門に関しては、FIPPs を実施するための政策的取組が進められてきたが、消費者データプライバシーや FTC の各レポートでは、「消費者プライバシー」は権利としては扱われていない。欧州が人権保障を盾にプライバシー外交を行うのとは対照的である。

日本は、プライバシー論議の後進国であるが、英米法の影響を受けながら、権利を発展させてきた。プライバシー権は、解釈上、憲法第 13 条後段に根拠づけられている。また、日本に国際テロの具体的な脅威が生じたことはないため、米国のように、国の安全を過度に優先する状況は生じていない。

このように、米国と日本では、相違点が多く、単純に比較検討することはできないが、それでもなお、2 つの事柄との関係で、米国の示唆を受けることができると考える。

第 1 は、プライバシーの要素をどのように見出すかという点である。

米国のプライバシー論議を振り返ると、伝統的権利が提唱され、現代的権利へと発展してきたが、両者は別々の権利ではなく、伝統的権利の中に現代的権利の萌芽を見ることができる。それは、ウォーレン&ブランダイス論文が分類した 2 つのカテゴリー不可侵権と公開に対する個人の決定権ーのうち、後者と関係する。後者は、「各個人が通常、自己の思想や心情、感情をどの程度他人に伝えるべきかを決定する権利」又は「公開の行為を完全にコントロールする」と説明されている。現代的権利を説いたウエスティン教授の『プライバシーと自由』は、プライバシー権を「自己に関する情報を、いつ、どのように、また、どの程度他人に伝えるかを自ら決定できる権利」と定義している。このように、ウォーレン&ブランダイス論文とウエスティン教授の定義は、「自己に関する事柄の提供を決定する」という要素において共通点が見られる。

その後、米国は、ウエスティン教授やミラー教授の立法提案を受け、種々のプライバシー保護法を制定するようになった。米国のいくつかの法律は「プライバシー」という名を用いているが、その内容は、個人データ（個人を識別できる情報）を保護するための法律である。また、前記の通り、1974 年プライバシー法を制定する過程では、合衆国保健教育福祉省による「記録、コンピュータ及び市民の権利」が公表された。この報告書は、個人のプライバシー概念を再定義する中で、ウエスティン教授による現代的プライバシー権の定義を取り入れ、また、「公正情報実務に関する法」との関連で、FIPPs のもととなる諸原則を掲げた。

このように、伝統的プライバシー権から現代的プライバシー権、FIPPs は、一連の流れをもって捉えることができる。

1970 年代以降、公的部門は 1974 年プライバシー法、民間部門はセクトラル方式の法制によってそれぞれ運用されてきた。民間部門では、1990 年代半ば頃より、FTC が消費者プライバシー保護のための取組を積極的に行うようになった。

2001 年の同時多発テロは、公的部門と民間部門の違いを一層際立たせることとなった出来事である。これ以降、「テロ対策」が特別扱いされ、諜報機関による個人情報の収集・利用は極めて緩やかな要件で認められるようになり、プライバシーや個人情報よりも国の安全を優先する強い傾向が見られるようになった。オバマ大統領は、NSA への批判を受け、2014 年 1 月 17 日に改革案を発表したものの、NSA の過度な情報収集に揺り戻しが生じるか否かは明らかでない。コンピュータ化による監視社会に対処するために登場した現代的プライバシー権は、提唱国である米国では忘れられたに等しい状況になっている。

民間部門では、自主規制を基本に FTC の法執行で担保するというスタイルが取られてきたが、ここ 1、2 年の間で、FIPPs を法典化した包括的な連邦法の制定が論じられるようになった。

消費者プライバシー権利章典のうち、第 1 原則「個人のコントロール」は、個人データの収集、利用、開示に関する意味のある決定を行うことを意味し、それが「選択」と表現されている。この原則は、現代的プライバシー権を最も直接的に実現する原則といえる。第 2 原則「透明性」は、「コントロール」を提供するための前提として求められる。「選択」と「透明性」は、FTC のプライバシー・レポートの枠組勧告にも取り上げられている。

このように、プライバシーは「権利」とは位置づけられないものの、民間部門との関連では、現代的プライバシー権の流れを汲んだ「選択」と「透明性」が、米国流の消費者プライバシーを構成する主な要素であるといえる。

日本が「パーソナルデータの利活用に関する制度見直し方針」に基づき個人情報保護法改正案を作成する際には、国際的にみてもクリアな制度を作るべく、一定の理念に基づく強固な骨組みの制度設計を行うべきであり、制度の根幹をなす基本原則が必要になると考えられる。その際には、プライバシーの主な要素をどのように把握し、制度に生かすのかという点が課題となる。

第 2 は、着目すべき新たなプライバシー侵害の側面を見出すことができるという点である。

本稿で取り上げたソロブ教授の著書は、「プライバシー」の概念について、包括的な原理を模索する従来型アプローチを否定し、諸問題に焦点を当てて類型的に捉えようと試みた。「プライバシー」は極めて文脈依存性が高い性質を有することから、多義的に理解すべきとする同教授の主張には説得性がある。

プライバシー権提唱から 120 年が過ぎ、その間、社会の発展とともに、プライバシーは様々な場面で登場してきた。ネットワークが急速に発展し、ビッグデータ時代を迎えた現在、個人に関する情報は大量に集積・解析され、実在の本人とは異なる人物像が、デジタルデータのみで形成されるようになってきている。その問題を捉えるのが「プロファイリング」である。

2000 年 6 月の「オンライン・プロファイリングに関する報告書」では、本人は、自らの預り知らないところで情報を収集・解析され、詳細なプロフィールを形成され、趣味や嗜好を推測されてしまうという問題が指摘された。欧州評議会の勧告や EU の一般データ

保護規則提案でもプロファイリングが取り上げられており、情報の収集・解析、利用のもたらす問題は、欧州と米国で共通しているということができる。

これに対し、日本におけるプライバシー権は、東京地方裁判所 1964（昭和 39）年 9 月 28 日の『宴のあと』事件判決 [68]以降、「私生活をみだりに公開されないという法的保障ないし権利」であると理解されてきた。最高裁判所は、「プライバシー」という言葉を長年にわたって回避してきたが、2003（平成 15）年 9 月 12 日の早稲田大学講演会名簿提出事件判決 [69]では、氏名、学籍番号、住所、電話番号のような個人識別等のための単純な情報であっても、「本人が、自己が欲しない他者にはみだりにこれを開示されたくないと考えることは自然なことであり、そのことへの期待は保護されるべきものである」と述べ、「このようなプライバシーに係る情報は、取扱い方によっては、個人の人格的な権利利益を損なうおそれのあるものであるから、慎重に取り扱われる必要がある」と判示し、不法行為の成立を認めた。また、住民基本台帳ネットワークシステムに関する 2008（平成 20）年 3 月 6 日付最高裁判所判決 [70]は、「憲法 13 条は、国民の私生活上の自由が公権力の行使に対しても保護されるべきことを規定しているものであり、個人の私生活上の自由の一つとして、何人も、個人に関する情報をみだりに第三者に開示又は公表されない自由を有するものと解される」と述べている。個人情報保護法の運用に関しても、いわゆる「過剰反応」の発生等、第三者提供や漏えいに主な関心が集められてきた。

個人情報保護法は、成立後 10 年以上が経過してからようやく改正へと動き出した。今後もネットワークの進展から遅れを取りつつ改正がなされると仮定すれば、既存制度の一部改正では、改正後の 10 年間に生じる新たな問題に対応できない可能性は否定できない。したがって、制度設計に際しては、プライバシー侵害の一側面にとらわれるべきではなく、新たな侵害の側面にも光を当てて検討することが望ましい。プロファイリングはその 1 つである。

2013 年 12 月 20 日に閣議決定された「パーソナルデータの利活用に関する制度見直し方針」では、個人データを加工して個人が特定される可能性を低減したデータに関して、第三者提供における本人の同意を要しない類型、共同利用やオプト・アウト等第三者提供の例外措置の要件の明確化」というように、現行法の規定を前提に見直すことが予定されている。しかし、同見直し方針が「プライバシーに配慮したパーソナルデータの利活用は、グローバルに対処すべき課題」と述べているように、個人情報保護法の改正法は、国際的に通用するものでなければならない。そのためには、プライバシーの多義性に基づき、侵害の諸側面に応じた制度設計が求められる。

本論文は、2011 年度独立行政法人日本学術振興会科学研究費助成事業若手研究 B（課題番号 23730116）「ライフログの利用とプライバシー・個人情報保護に関する比較法的研究」による成果である。

---

68 東京地判昭和 39 年 9 月 28 日下民集 15 巻 9 号 2317 頁。
69 最二小判平成 15 年 9 月 12 日民集 57 巻 8 号 973 頁。
70 最一小判平成 20 年 3 月 6 日判タ 1268 号 110 頁。