

データ利活用に関わるプライバシー・個人情報の保護

東京大学大学院情報学環特任講師

国立国会図書館 非常勤調査員 生貝 直人

目 次

はじめに

I データ利活用と保護に関わる法制度

- 1 プライバシー・個人情報保護法制の課題
- 2 データ利活用に対応した制度改正の論点

II EUにおけるデータ利活用に向けた対応動向

- 1 EUのプライバシー保護に関わる基盤法制
- 2 EUにおけるデータ利活用に関わる状況
- 3 データ保護指令と民間の行動規範
- 4 一般データ保護規則の制定に向けた検討

III 米国におけるデータ利活用に向けた対応動向

- 1 米国のプライバシー保護に関わる基盤法制
- 2 FTCの施策と匿名化情報の取扱い
- 3 消費者プライバシー権利章典と民間の自主規制の強化

IV 諸外国の動向から見た我が国の制度改正への示唆

おわりに

【要 旨】

プライバシー・個人情報保護に関わる法制度は、消費者の権利利益を保護しつつ、多種多様なデータの利活用に基づく経済的・社会的価値の創出を進める上での基盤としての役割を果たす。本稿では、EU・米国におけるデータ利活用に関わる状況と制度改革の動向、特に匿名化されたデータの利活用枠組の整備や民間の自主的な取組の活用、プライバシー保護を専門とする第三者機関の役割等の論点を参照し、我が国において今後データ利活用とプライバシー保護の両立を可能とする制度枠組を実現するための課題を論じる。

はじめに

現在、ビッグデータと呼ばれる多種多様かつ膨大なデータの利活用による経済的・社会的価値の創出は、国際的に重要な立法課題として位置付けられている。特に個人に関わる情報を含むデータの利活用を進めていくためには、消費者のプライバシーを適切に保護すると同時に、企業の創意工夫に基づくイノベーションを妨げない法的環境を創出する、プライバシー・個人情報保護法制の設計が重要な役割を果たす。本稿では、我が国が今後データの保護と利活用を両立する制度設計を行う上での示唆を得ることを目的として、欧州連合（European Union: EU）・米国におけるプライバシー保護に関わる制度枠組と、データ利活用に向けた近年の対応動向の検討を行う。

I データ利活用と保護に関わる法制度

1 プライバシー・個人情報保護法制の課題

プライバシー・個人情報保護法制は、情報を規律する法制度であるがゆえに、変化し続ける情報技術、そしてそれを受けて形成される情報社会のあり方に整合的であることが求められる。ビッグデータやパーソナルデータ⁽¹⁾と呼ばれる多種多様なデータの利活用による価値創出が、今後の我が国の経済成長を左右する立法課題の一つとなる中、消費者の保護とデータの利活用をいかに両立させていくか、そしてグローバルな情報流通が日常的に行われる現代においていかに国際的整合性を有した制度枠組を実現するかは、今後の制度改正における主要な論点となる。

個人に関する情報を広く含むパーソナルデータの利活用において中心的な課題となるのが、事業者が消費者から収集したデータを、どのような条件の下で自由に利活用することができるかという点である。現行の「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」という。）においては、いかなるデータの利活用が合法的であるかが必ずしも明確で

* 本稿におけるインターネット情報の最終アクセス日は2015年1月20日である。本稿の内容は2015年1月20日までに入手可能な情報に基づいている。

(1) 我が国において「パーソナルデータ」という語は、個人情報保護法第2条第1項で規定されるような個人識別性を要件とせず、個人に関わる情報を総称する表現として用いられる。総務省「パーソナルデータの利用・流通に関する研究会報告書—パーソナルデータの適正な利用・流通の促進に向けた方策—」2013.6. 総務省ウェブサイト <http://www.soumu.go.jp/main_content/000231357.pdf> 本稿では、後述するEUの個人データ概念等外国法の保護対象情報を含め、個人に関わる情報を総称する必要がある際に、パーソナルデータの語を用いる。

はない部分が存在し、そのようないわゆる「グレーゾーン」の存在が企業の萎縮を招き、データの利活用を阻害していることが問題視されてきた。その典型的な問題として、法により保護されるパーソナルデータの範囲の曖昧さを挙げることができる。我が国の個人情報保護法では、保護の対象となる個人情報を「生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）」（第2条）としており、その定義に該当しないよう匿名化された情報には同法の規定は及ばない。

しかし、どの程度の匿名化を行えば個人の識別に至ることがないかという点に関しては、いまだ我が国はもとより、国際的にも標準的な理解は存在しないのが現状である。個人情報のデータベースから、氏名や住所などの直接個人を識別できるような情報を取り除いた上で外部へデータの提供を行ったとしても、特定のID等に関連付けられた履歴が長期間蓄積されているデータ等の場合には、その情報を解析し、他の情報と組み合わせるなどした場合に再度第三者が当該個人を識別することが可能となる、いわゆる再識別化（re-identification）のリスクが生じうる⁽²⁾。同時にそうしたリスクが消費者の不安を招き、データを利活用しようとする事業者が社会的な批判を浴びる事態をも考慮しなければならない⁽³⁾。データ解析技術の発展が、パーソナルデータの利活用に基づく価値創出の可能性を拡大する一方、新たなプライバシー・リスクをももたらし得る中で、いかにしてルールを明確化し、価値の高いデータを安全に利活用可能とするかが課題となっている。

2 データ利活用に対応した制度改正の論点

このような中、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）に2013（平成25）年に設置された「パーソナルデータに関する検討会」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」⁽⁴⁾に基づき、データ利活用を促進していくための個人情報保護法改正に向けた集中的な検討が進められてきた。2014（平成26）年6月には、2015（平成27）年通常国会における制度改正の方向性を示した「パーソナルデータの利活用に関する制度改正大綱」⁽⁵⁾（以下、大綱という。）が公表され、その具体化の作業が行われている。制度改正の論点は多岐にわたるが、主たる方針としては、大綱中の「制度改正内容の基本的な枠組み」⁽⁶⁾に示されるとおり、「本人の同意がなくてもデータの利活用を可能とする枠組みの導入等」、「基本的

(2) データ解析技術の進展により、従来の匿名化技術が有効性を持たなくなることの問題については、以下に詳しい。Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," *UCLA Law Review*, Vol.57, 2010.8, pp.1701-1777.

(3) このような問題が象徴的に現れた事例として、2013（平成25）年6月、JR東日本が保有するSuicaの利用者履歴情報を日立製作所に提供し、分析結果を用いたマーケティング情報を外部に提供・販売するとした計画に関わる一連の動きを挙げることができる。同事例は、履歴情報から氏名や住所等の情報を削除し、Suicaに付与されるID番号については他の形式に変換した上で日立製作所に提供するものであったが、利用者への事前の周知が十分でなかったことなどを背景として多くの批判的な反応を呼び、データの外部提供は見送られることになった。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の有識者会議「中間とりまとめ」受領について」2014.3.20. <<http://www.jreast.co.jp/press/2013/20140311.pdf>>

(4) 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見直し方針」2013.12.20. <<http://www.kantei.go.jp/jp/singi/it2/kettei/pdf/dec131220-1.pdf>>

(5) 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」2014.6.24. <<http://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20140624/siryous.pdf>>

(6) 同上, pp.7-9.

な制度の枠組みとこれを補完する民間の自主的な取組の活用」、「第三者機関の体制整備等による実効性ある制度執行の確保」の3点を主眼としている。以下、その概要を紹介する。

第一は、「本人の同意がなくてもデータの利活用を可能とする枠組みの導入等」である。個人情報保護法においては、個人情報の取得時において利用目的を本人に通知又は公表することが求められ、目的外での利用を行う場合や第三者への提供を行う場合には、原則として本人の同意を得なければならない。しかし、一度取得したデータについて新たな形態での利用を行うたびに本人の同意を得ることは、多様なデータ利活用ビジネスを行おうとする事業者にとって負担が大きいことから、消費者のプライバシー・個人情報保護に関わる適切な措置を施した上で、本人の同意を得ずとも一定の目的外利用や第三者提供を可能とする枠組を創設するものとされる。具体的には、通常の個人情報から氏名や連絡先等を取り除くなどの匿名化措置により、特定の個人が識別される可能性が低減されたデータの取扱いを定めることが念頭に置かれ、特に後述する米国の施策等を参考に、データの提供に当たり、当該データを利用した再識別を禁止するなどの措置を法定すること等が検討されている。

第二は、「基本的な制度の枠組みとこれを補完する民間の自主的な取組の活用」である。大綱では、法律により大枠を定めた上で、データ利活用の障壁となっているグレーゾーンの解消を図るため、政省令や規則、ガイドラインによってルールの詳細化を行うとともに、技術の進展や市場構造などの業界・分野ごとの性質を反映した、産業界の自主規制ルールを促進する枠組を新たに定めることとしている。自主規制ルールで定める内容としては、前述した個人の特定性を低減したデータへの加工方法などの法定事項と、分野ごとのリスクへの対応などの法定されていない事項の双方が想定される。自主規制ルールの策定主体となる民間団体等に対しては、消費者等を広く含んだマルチステイクホルダープロセス⁽⁷⁾に基づくルール策定を求め、個人情報保護を専門に所管する第三者機関が認定等を行い、実効性と適切性を確保するものとされる。

第三は、「第三者機関の体制整備等による実効性ある制度執行の確保」である。我が国の個人情報保護法においては、各省庁の大臣が所管分野ごとに監督・執行を行う、いわゆる主務大臣制を採用してきた。その制度枠組を、後述するEUの一元的な執行体制を参考に大きく変更し、法令や民間の自主規制ルールを実効性あるものとするため、「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」(平成25年法律第27号)の規定に基づき2014(平成26)年に設立され、特定個人情報(マイナンバー)の取扱いを専門に監督している特定個人情報保護委員会を改組した、独立性の高い第三者機関を中核とした監督・執行体制を整備するものとしている。第三者機関は、現行の個人情報保護法において主務大臣が有する権限・機能(助言、報告徴収、勧告、命令)に加えて、個人情報取扱事業者に対する指導・立入検査・公表等を行うことができるようにするものとされる⁽⁸⁾。

すなわち、パーソナルデータの利活用を可能とするための大枠の要件を法律で定めた上で、

(7) 「国、事業者、消費者、有識者等の関係者が参画するオープンなプロセスでルール策定等を行う方法」を指す。同上, p.8.

(8) 本稿は民間におけるデータ利活用に関わる法制度を主眼とするため詳述しないが、「行政機関の保有する個人情報の保護に関する法律」(平成15年法律第58号)、「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」(平成15年法律第59号)等に規定される、行政機関等の保有する個人情報の取扱いについても、第三者機関が関与する制度を設けるための検討が進められているところである。「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」総務省ウェブサイト <http://www.soumu.go.jp/main_sosiki/kenkyu/gyousei_personal/index.html>

より具体的なルールの内容を官民の協業的な方法で定めることでグレーゾーンの解消を図るとともに、第三者機関の一元的な執行体制の下でその実効性を担保することにより、データの利活用と保護の両立を図ろうとしていると見ることができる。これらの方針は、いずれもEU・米国をはじめとする諸外国の制度枠組と近年の制度改革議論を参考として検討されてきたものである。以下では、今後の法改正において焦点となる上記3点を中心に、EU・米国におけるプライバシー・個人情報保護の法制度を参照し、パーソナルデータの利活用に向けた匿名化等の措置に関わる対応、民間の自主的な取組の活用等の論点について、それぞれにおける施策の現状と制度改革の動向を確認していく。

II EUにおけるデータ利活用に向けた対応動向

1 EUのプライバシー保護に関わる基盤法制

EUのプライバシー保護法制の基盤となるデータ保護指令⁽⁹⁾は、指令(directive)というEU法の形式上、指令の求める基準を満たす具体的な国内法の整備や運用は、加盟各国⁽¹⁰⁾に委ねられる。一方、指令条文の最終的な解釈を行う司法機関として、ルクセンブルクに欧州連合司法裁判所(Court of Justice of European Union: CJEU)が置かれている。さらに欧州委員会には、データ保護指令第29条に基づき、各国のデータ保護機関及び欧州連合関連機関のデータ保護を監督する欧州データ保護監察官(European Data Protection Supervisor)により構成される29条作業部会(Article 29 Working Party)⁽¹¹⁾が置かれ、各国における法運用の指針等に係る意見(opinion)を数多く公表している。これらは、データ保護指令の解釈や運用を理解する上での重要な文書群として位置付けられる。

データ保護指令の特徴としては、主に次の4点を挙げることができる。第一に、対象の官民を問わない包括的な法形式を採っており、この点は政府部門と民間部門を別の法により規制する我が国とは異なる。第二に、各国国内法の監督・執行当局として、独立性の高いデータ保護機関(Data Protection Authority: DPA)を設置することが前提とされており、個別省庁の主務大臣が分野ごとの権限を有する、いわゆる主務大臣制を採る我が国とは異なる。第三に、実体的な側面として、保護対象となる個人データ⁽¹²⁾の利用の際には本人の同意を得なければならないとする、事前同意の原則を広範に採用している点である。第四に、個人データに対する本人の開示・修正・削除等の権利行使に関して、データ保護機関の罰則権限を背景とした、強制力の強い消費者の権利を法定している点である。

(9) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal of the European Communities*, 281, 23.11.1995, pp.31-50.

(10) EU加盟28か国に加え、データ保護指令に関しては、欧州経済領域(European Economic Area: EEA)に加盟するノルウェー・リヒテンシュタイン・アイスランドの3か国が対象に含まれる。

(11) "Article 29 Working Party - Justice." European Commission Webpage <http://ec.europa.eu/justice/data-protection/article-29/index_en.htm>

(12) 同指令の保護対象となる個人データとは、「識別された又は識別され得る自然人(以下「データ主体」という。)に関するすべての情報をいう。識別され得る個人とは、特に個人識別番号、又は肉体的、生理的、精神的、経済的、文化的並びに社会的アイデンティティに特有な一つの又はそれ以上の要素を参照することによって、直接的又は間接的に識別され得る者をいう(第2条(a))」とされ、我が国における個人情報保護法第2条に定義される「個人情報」とは異なる概念である。邦訳は堀部政男研究室「資料 EUデータ保護指令仮訳」総務省ウェブサイト <http://www.soumu.go.jp/main_content/000196313.pdf>による。

我が国やEU域外の各国にとって特に重要となるのは、第25条及び第26条に規定される個人データの第三国移転条項である。同条では、EU市民の個人データを第三国に移転するためには、当該第三国が個人データに関わる十分な保護水準を満たしていなければならないと規定され、2015年1月までに12か国が欧州委員会からその水準を満たすという認定を受けている⁽¹³⁾。その他の域外データ移転手段としては、EUが認定する共通契約枠組である標準的契約条項 (standard contractual clauses)⁽¹⁴⁾と、国際的な企業グループ内での情報移転を対象とした拘束的企業準則 (binding corporate rules)⁽¹⁵⁾が存在し、これらの枠組に参加する企業は、データ移転を行う先となる国がEUの認定を得ていなくとも、個別企業同士やグループ単位での域外データ移転を行うことができる。

2 EUにおけるデータ利活用に関わる状況

EUにおけるプライバシー保護法制には、前述したデータ保護指令における個人データの取扱いに関わる、消費者の事前同意を前提とした包括的な規定に加え、情報通信分野を対象とした電子通信プライバシー指令⁽¹⁶⁾が存在する。同指令では、電子通信サービスで取得される位置情報の取扱い等を規制するほか、インターネット上のプライバシー保護において主な議論の対象となる端末IDやウェブブラウザのクッキー (cookie) 等を含む端末蓄積情報について、「ユーザーの端末に蓄積された情報は、当該ユーザーがその利用目的等についての明確かつ包括的な情報を与えられている場合に限り利用可能であり、ユーザーはその利用を拒絶する権利を持たねばならない (第5条(3))」と規定し、事後的な利用の拒否を可能とする取扱いを求めている。さらに2009年に採択された同指令の改正⁽¹⁷⁾では、同規定は「ユーザーの端末に蓄積された情報は、当該ユーザーがその利用目的をはじめとする明確かつ包括的な情報を与えられた上で同意を得た場合に限り利用可能である」と改められ、必ずしも個人の特定を目的とするわけではない情報を含めた、パーソナルデータ全般に関わる消費者の事前同意を前提とした法制度を構築している。

(13) “Commission decisions on the adequacy of the protection of personal data in third countries.” European Commission Webpage <http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm> 米国に関しては国全体での認定は受けていないが、2000年に欧州委員会と米国商務省の間で締結されたセーフハーバー協定に企業が参加することにより、EUからのデータ移転を行うことができる。2015年1月時点では日本は認定国に含まれない。

(14) “Model Contracts for the transfer of personal data to third countries.” European Commission Webpage <http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm> 邦語による解説として、武井一浩ほか「モデル契約の概要」消費者庁『国際移転における企業の個人データ保護措置調査報告書』2010.3, pp.92-122.を参照。

(15) “Overview on Binding Corporate rules.” European Commission Webpage <http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm> 邦語による解説として、石井夏生利「BCRの制度的概要」消費者庁 同上, pp.58-91.を参照。

(16) 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 (Directive on privacy and electronic communications), *Official Journal of the European Communities*, 201, 31.7.2002, pp.37-47.

(17) Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance), *Official Journal of the European Union*, 337, 18.12.2009, pp.11-36.

一方でEUにおいても、匿名化されたデータに関してはデータ保護指令等の適用対象とはならないが、どのような技術的措置を施すことが適切な匿名化とされるかについての広範なコンセンサスは存在していないのが現状である。2014年に公表された29条作業部会「匿名化手法に関する意見」⁽¹⁸⁾の中でも、各種の技術的措置を検討した上で、完全に匿名化されたデータセットの作成は極めて困難であるという認識の下、個人を識別しようとするあらゆる合理的な手段を考慮し、ケースバイケースの判断が必要であるとしている。さらに加盟国においても、個人データの匿名化に関わる検討がなされており、2012年には英国情報コミッショナー事務局 (Information Commissioner's Office) がガイドライン⁽¹⁹⁾を公表している。ここでは、一度匿名化されたデータが、他のデータと組み合わせられるなどして再度個人識別可能となるリスクは予見できないという認識の下、事前のプライバシー影響評価 (Privacy Impact Assessment) の実施や、予期しない個人識別化等の事態が発生した際の事後的対応手順を定める等のガバナンス面での対応を推奨するほか、想定されるリスクが大きい場合には、匿名化したデータを外部に提供することについて消費者への同意を取るべきことなどが示されている。

3 データ保護指令と民間の行動規範

このような包括的な法的枠組と、強固な事前同意を前提とするEUのプライバシー保護法制においても、民間の自主的な取組の活用を重視した制度枠組が存在している。データ保護指令第27条においては、産業界による自主規制ルールの策定と、それに対する当局の関与を促す規定が置かれる。加盟国は多様な分野ごとの特性を考慮しつつ、各国法を正しく反映した業界団体等による行動規範 (Codes of Conduct) の策定を促さなければならない (27条(1))。各国のデータ保護機関は、その国内法との整合性を評価し、適切な行動規範と認められた場合には、消費者を代表する者の意見を求める必要がある (同条(2))。さらにEU全体に有効性を持つ行動規範を策定することも可能とされており、前述した29条作業部会がその指令や各国法との整合性を評価し、適切な行動規範と認められた場合には、消費者を代表する者の意見を求めた上で、欧州委員会が当該行動規範の周知を促すものとされる (同条(3))。指令及びそれに基づいて制定される各国法の規定を適切に反映することを要件とした上で、プライバシー保護に関わる多様な産業分野において詳細な画一的基準を定めることの困難さに鑑み、産業界自身による行動規範の策定と、その適切性を公的に担保することを求めているのである。特に前項で言及した匿名化措置に関しても、同条における行動規範によって定めることの有用性が指摘されている⁽²⁰⁾。

加盟国においては、業界・分野ごとの多くの行動規範が当局の認定を受けているほか⁽²¹⁾、EU全体レベルで29条作業部会により適切性が認められた行動規範として、国際線を運航する

(18) Article 29 Working Party, *Opinion 05/2014 on Anonymisation Techniques*, 2014.4.10. <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>

(19) Information Commissioner's Office, *Anonymisation: managing data protection risk code of practice*, 2012.11. <<https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf>>

(20) Directive 95/46/EC *op. cit.* (9), para. 26 of the preamble.

(21) EU各国におけるデータ保護指令27条に相当する条項の規定内容と運用状況については、Dennis D. Hirsch, "The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?" *Seattle University Law Review*, Vol.34 No.2, 2011, pp.439-480.に詳しい。特に同条に基づくルール形成が広範に用いられる、オランダにおける国内法と分野ごとの行動規範の策定状況については、Dennis D. Hirsch, "Going Dutch? Collaborative Dutch Privacy Regulation and the Lessons it Holds for U.S. Privacy Law," *Michigan State Law Review*, Vol.83, 2013, pp.83-166.を参照。

航空会社や旅行代理店によって構成される国際航空運送協会（International Air Transport Association: IATA）、及び欧州各国のマーケティング業界団体等が加盟する欧州ダイレクト・インタラクティブマーケティング連盟（Federation of European Direct and Interactive Marketing: FEDMA）によって策定されたものが存在する⁽²²⁾。さらに2011年には、世界各国で拡大するパーソナルデータを利用したオンライン広告に関するプライバシー保護基準を明確化するため、広告分野の業界団体である欧州広告規格連盟（European Advertising Standards Alliance: EASA）と欧州インタラクティブ広告協会（Interactive Advertising Bureau Europe: IAB Europe）が共同で行動規範の案を提出していたが、前述の電子通信プライバシー指令⁽²³⁾が定める規定、特に消費者からの事前同意取得への対応の不足を主な理由として、29条作業部会は同年、同行動規範の適切性を否定する判断を行っている⁽²⁴⁾。

4 一般データ保護規則の制定に向けた検討

このような中、2012年1月、欧州委員会により、現行のデータ保護指令を全面的に改正する「一般データ保護規則（General Data Protection Regulation）」の草案⁽²⁵⁾が公表された⁽²⁶⁾。当該規則案は、データ保護指令が加盟国で国内法が法制化されてはじめて効力を持つ法形式であるものを、域内全体において直接的な効力を持つ「規則（regulation）」に変更するものである。データ保護指令に基づき各国が異なる国内法を制定する状況は、国境を越えたデータ利活用を行う企業に高い対応コストを課すことになるため、法形式の規則への変更によりEU域内のプライバシー保護法制を完全に統一することで、国際的なデータ流通の活性化を実現しようとしているのである。内容面では、保護対象となる個人データの拡張⁽²⁷⁾、「消去権（忘れられる権利）」（第17条）や「設計及び初期設定によるデータ保護」（第23条）概念、「個人データのポータビリティ」を

(22) これら行動規範については、下記を参照。Neil Robinson et al., *Review of the European Data Protection Directive*, RAND Europe, 2009, pp.9-10. <http://www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR710.pdf> なおFEDMAの行動規範については、インターネットでの広告・マーケティング行為を対象に含むための付随文書（ANNEX）が2010年に29条作業部会によって適切性を認める結論が出されている。Article 29 Working Party, *Opinion 4/2010 on the European code of conduct of FEDMA for the use of personal data in direct marketing*, 2010.7.13. <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174_en.pdf>

(23) Directive 2002/58/EC *op.cit.*(16)

(24) Article 29 Working Party, *Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising*, 2011.12.8. <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_en.pdf>

(25) European 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, 2012.1. <[http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM\(2012\)_0011_EN.pdf](http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)_0011_EN.pdf)> 全文の仮訳については、個人情報の安心安全な管理に向けた社会制度・基盤の研究会編『個人情報の安心安全な管理に向けた社会制度・基盤の研究会報告書』日本情報経済社会推進協会, 2012. <<http://www.jipdec.or.jp/project/anshinkan/doc/2011/01.pdf>> p.82.以降を参照。その後の立法手続の中で、2013年11月に欧州議会市民的自由・司法・内務委員会から提出された修正案として、下記を参照。Draft European Parliament Legislative Resolution on the 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), 2013.11. <<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FTEXT%2FBREPORT%2BA7-2013-0402%2B0%2BDOC%2BXML%2BV0%2F%2FEN&language=EN>>

(26) 邦語による紹介として、藤原静雄「EUデータ保護一般規則提案の概要」『NBL』975号, 2012.4.15, pp.4-7; 石井夏生利「EU一般データ保護規則提案と日本の課題—欧州調査及び最新動向を踏まえて—」『InfoCom REVIEW』60号, 2013.7, pp.38-57.

要求する権利（第18条）の導入等、現代の情報環境に対応した、より強固なプライバシー保護を実現するための規定が含まれる。前述したデータ保護指令第27条に相当する第38条では、産業界が策定する行動規範が含む必要がある事項についてのより具体的な指定がなされており、特に欧州委員会によって適切性が認められた行動規範に関しては、委任法令（delegated act）や実施法令（implementing act）⁽²⁸⁾に基づく法的有効性の付与を可能とする規定が置かれている。

一般データ保護規則案は、従前のEUにおける個人データ・プライバシー保護のあり方を大きく変容させ得るものであるがゆえに、規制対象となる企業にとっては、新たな規制の内容が、具体的なデータ利活用の場面においていかに適用されるかが適時に明確化されることが必要になる。特に多種多様なデータの利活用に関して画一的な基準を定めることが困難な匿名化等の措置について、いかなる現実的なルール形成が進められるかをはじめとして、民間による行動規範の策定とその公的な評価の枠組は、EUの規制内容の具体的な運用を理解する上での重要な役割を果たすものと考えられよう。

Ⅲ 米国におけるデータ利活用に向けた対応動向

1 米国のプライバシー保護に関わる基盤法制

プライバシーの権利が最初に提唱されたのは19世紀米国においてであるが、米国には包括的な個人情報保護法制は現時点では存在していない。憲法修正1条に規定される表現の自由の重視、そして連邦政府の本来的な権限の範囲の問題など複数の要因が作用しているが、特にインターネット上のプライバシー保護法制に関しては、新たなビジネスモデルの柔軟な発展を重視する立場から、企業の自主規制による問題解決を基調とする対応を進めてきた背景がある⁽²⁹⁾。同時に米国では、連邦法において金融（公正信用報告法⁽³⁰⁾等）や医療分野（医療保険の相互運用性と説明責任法⁽³¹⁾）、13歳未満の子供に関する情報（児童オンライン・プライバシー保護法⁽³²⁾）、レンタルビデオ履歴（ビデオプライバシー保護法⁽³³⁾）等、特定の分野において個別の立法措置を行っている。さらに各州においても、プライバシー関連の州法は数多く存在しており、米国のプライバシー保護法制は、分野別・州別の重層的なネットワーク構造を有していると言うことがで

(27) 同規則案では「データ対象者（data subject）」を「特定された自然人、または管理者あるいはそれ以外の自然人や法人によって合理的な範囲で使用される手段をもって直接的または間接的に特定された自然人のことを意味する。特に、識別番号、位置データ、オンライン識別子の参照、またはその人物のアイデンティティに関する物理的、生理的、遺伝子的、精神的、経済的、文化的、または社会的な一つ以上の要素の参照によって特定された自然人のことを意味する（4条(1)）」と定義した上で、「個人データ」を「あるデータ対象者に関するすべての情報を意味する（4条(2)）」と定義しており（邦訳は、個人情報の安心安全管理に向けた社会制度・基盤の研究会編 前掲注(25)による）、現行指令では言及されないオンライン識別子等を明示的に含む、保護対象情報の拡張を行っている。

(28) 2009年のリスボン条約発効に伴い設けられた準立法手続であり、EUにおける指令や規則等の各種法令について、非本質的要素の変更（委任法令）や統一の実施（実施法令）を行うことを目的として、欧州委員会が独自の権限として法令を採択することができる。

(29) Federal Trade Commission, *FTC Staff Report: Self-Regulatory Principles For Online Behavioral Advertising*, 2009.2, p.11. <<http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavareport.pdf>>

(30) Fair Credit Reporting Act (Public Law 91-508)

(31) Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191)

(32) Children's Online Privacy Protection Act of 1998 (Public Law 105-277)

(33) Video Privacy Protection Act of 1988 (Public Law 100-618)

きる。

米国のプライバシー保護法制の中でも、連邦レベルでのプライバシー保護において中核的な役割を果たしているのが、消費者保護政策を所管する独立行政機関である連邦取引委員会（Federal Trade Commission: FTC）の権限を定めたFTC法第5条⁽³⁴⁾に規定される、「不公正（unfair）又は欺瞞的（deceptive）」な行為又は慣行を規制することができる権限である⁽³⁵⁾。同規定はプライバシー保護のみを目的とした規定ではない一般的な消費者保護法制だが、インターネット上のプライバシー保護に関しては、特に企業自らが消費者に提示したプライバシー・ポリシーへの違反等に対して積極的に適用され、企業による自主規制の実効性を確保する上で主要な役割を果たしている⁽³⁶⁾。FTCは同条を基盤として、EUや我が国のような包括的な立法と事前の消費者同意を前提とした形態とは異なる、産業界の自主規制に基づくプライバシー保護の施策を進めてきている。

2 FTCの施策と匿名化情報の取扱い

FTCは、近年のデータ利活用ビジネスの拡大に対応することを目的として、2012年3月に「急速な変化の時代における消費者プライバシーの保護」⁽³⁷⁾と題する文書を公表している。同文書の適用対象となる情報については、特定の消費者、コンピュータ又はデバイス等に合理的に結びつけられうる（reasonably linkable）データ全般とされ⁽³⁸⁾、EUと同様に、保護の対象となるべき情報を広範に定義している。その上で企業に対して、プライバシー保護に配慮したサービス設計を行うプライバシー・バイ・デザイン原則の推進、消費者がサービスの利用に当たって行うプライバシー関連の選択を簡潔なものとする、企業が保持・収集するデータへの消費者アクセスの向上を通じた透明性の実現を求めている。

さらに同文書では、プライバシー保護とデータ利活用の両立を図るための手法として、匿名化されたデータを第三者に提供可能とする枠組についての提案を行っている。そこでは、完全な匿名化の技術が存在しないことを前提に、同意取得や通知を行わずとも事業者がデータの利活用を行いうる要件として、①適切な匿名化措置を施し、②当該データの再識別化を行わないことを約束・公表し、③第三者に提供する場合には契約によりデータ提供先が再識別化を行わないことを約束させること、の3点を満たすことを提示している⁽³⁹⁾。当該要件は、技術的な匿名化措置の限界を制度的に補完する手段として、我が国の今般の法改正議論においても広く参照されたところである⁽⁴⁰⁾。

⁽³⁴⁾ Federal Trade Commission Act (15 U.S.C § 45)

⁽³⁵⁾ 同法に基づくFTCの権限の歴史的経緯と近年の運用状況については、Daniel J. Solove and Woodrow Hartzog, “The FTC and the New Common Law of Privacy,” *Columbia Law Review*, Vol.114, 2014.4, pp.583-676. が詳細な検討を行っている。

⁽³⁶⁾ 自主規制の促進と実効性確保に関わるFTCの施策の経緯については、生貝直人「オンライン・プライバシーと自主規制—欧米における行動ターゲティング広告への対応—」『情報通信学会誌』96号, 2010.12, pp.105-113. を参照。

⁽³⁷⁾ Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers*, 2012.3. <<http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>>

⁽³⁸⁾ *ibid.*, p.18.

⁽³⁹⁾ *ibid.*, pp.21-22.

3 消費者プライバシー権利章典と民間の自主規制の強化

このような中で、米国のプライバシー保護政策の大綱を示す形で策定されたのが、ホワイトハウスにより2012年2月に公開された「ネットワーク化された世界における消費者のデータ・プライバシー」⁽⁴¹⁾である。同文書は、消費者がネットワーク環境において有すべき「消費者プライバシー権利章典 (Consumer Privacy Bill of Rights)」⁽⁴²⁾と、その立法化提案を含んでいるが、そこで示された基本指針は、あくまで従前の自主規制を重視した政策姿勢を維持しつつも、その適切性と実効性を強化していくことに重点が置かれている。

まず、従来は産業界が主体となって策定してきたプライバシー保護のための自主規制ルールについて、企業に加えて法執行当局や技術専門家、そして消費者等を含む多様な主体が参加する、マルチステイクホルダープロセスに基づくルール形成を実現することを示している⁽⁴³⁾。ルール形成の会合は、国際的なインターネット・ガバナンスの領域において、政府や企業、消費者団体等を含めた多様な主体によるルール形成を担ってきた商務省の国家電気通信情報局 (National Telecommunications and Information Administration: NTIA) が主催することが念頭に置かれている。民間の自主規制の重要性を前提としつつも、そのルール形成過程に連邦政府が公式に関与することにより、自主規制ルールの適切性とプロセスの公開性を強く担保していくことを示しているのである。

さらに同文書は、消費者プライバシー権利章典を立法化した形での、新規の包括的プライバシー保護法制を立法することを連邦議会に求めている。ここで自主規制の枠組との関連で重要な点は、前述したマルチステイクホルダープロセスによって策定され、適切性を認定された自主規制ルールの遵守を約束した企業については、新法の直接執行対象から除外するという形で、企業が自主規制に参加するインセンティブをもたらそうとしていることである⁽⁴⁴⁾。当該方針に基づいた包括的なプライバシー保護立法はいまだ行われていないものの、NTIAの主導の下、同文書の公表直後からマルチステイクホルダープロセスに基づく自主規制ルールの策定作業が進められており、すでにモバイル分野でのプライバシー保護に関わる複数の素案が作成されている⁽⁴⁵⁾。

プライバシー分野における同種の規定としては、FTCが所管する児童オンライン・プライバシー保護法⁽⁴⁶⁾における条項が存在する。同法の下では、商用のウェブサイトが13歳未満の子供の個人情報を収集する際には、プライバシー・ポリシーの掲載と、収集時の親権者の同意を

(40) パーソナルデータに関する検討会等におけるFTCの当該要件に関わる議論経緯については、森亮二「パーソナルデータの匿名化をめぐる議論 (技術検討ワーキンググループ報告書)」『ジュリスト』1464号, 2014.3, pp.25-31.を参照。

(41) The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, 2012.2. <<http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>> 同文書の解説として、井樋三枝子「消費者プライバシー保護に関する権利章典」『外国の立法』No.252-1, 2012.7, pp.18-19. <http://dl.ndl.go.jp/view/download/digidepo_3507782_po_02520106.pdf?contentNo=1>を参照。

(42) ①消費者によるコントロール、②透明性、③文脈 (コンテキスト) の尊重、④セキュリティ、⑤アクセスと正確性、⑥適切な範囲での収集、⑦説明責任の7原則からなる。The White House, *ibid.*, pp.9-22.

(43) *ibid.*, pp.23-27.

(44) *ibid.*, pp.35-39.

(45) "Privacy Multistakeholder Process: Mobile Application Transparency." National Telecommunications and Information Administration Webpage <<http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency>>

(46) *op.cit.*(32)

得ることなどが定められ、違反した場合にはFTCによる制裁の対象となる。同法1304条(a)においては、業界団体等はFTCに対して自主規制ルール案を提出することができ、FTCに適切性を認定された自主規制ルールに参加する企業は、同法を遵守しているものとみなすという規定が置かれ、2014年12月時点では、Privacy Vaults OnlineやTRUSTeをはじめとする7つの団体⁽⁴⁷⁾による自主規制ルールが認定されている。

米国政府としては、このような民間の自主的な取組を基盤としつつも、自主規制ルールの形成プロセスやルール内容の適切性と実効性を強化していく手法を発展させることを念頭に、パーソナルデータの利活用に必要な規制の柔軟性と、消費者プライバシー保護の両立を、官民の協働により実現しようとしているのである。

IV 諸外国の動向から見た我が国の制度改正への示唆

EU・米国ともに、技術進化のさなかにあるパーソナルデータの利活用に対応した法制度は構築途上の段階にあるが、いずれも専門的な公的機関の関与の下、データを安全に利活用するために必要な技術的対応の限界を認識した上での制度的補強、そして民間の自主的な取組を促進・評価することによる法規制の具体化と確実性の担保を基調とした取組が進められている点は一定程度共通している。我が国においても、新たな第三者機関の権限・機能を検討するに当たり、データ利活用に必要な柔軟性と、確実な消費者保護の双方を担保する制度設計のあり方を考慮する上で参照すべき点は多いと考えられる。

インターネットを取り巻く技術的環境、そして国際的な法制度の状況が変化し続ける現代において、データの利活用と消費者保護を両立する法制度は、現時点での状況を前提として固定することは困難であり、常にその継続的な見直しと改善が必要となる。先行するEUや米国の施策を、法制度の枠組のみならず、制度運用や民間の取組の実態と変動を含め仔細に観察していくことが、我が国がデータの保護と利活用の両立、そして国際的整合性を有する法制度を実現していく上で不可欠の作業であると考えられる。

おわりに

2015(平成27)年には、我が国において個人情報保護法の改正に向けた本格的な制度改正の作業が進められる見込みのほか、諸外国においても、EUの一般データ保護規則の成立や、米国における消費者プライバシー権利章典に基づいた新たな立法作業の進展が見込まれるところである。我が国で個人情報保護法の改正が行われた後には、新たな法制度に対応した民間の側の自主規制ルールの策定等に向けた動きが必要になる。各国における、官民双方を主体とした新たなルール形成の動きが、いかにデータの利活用に基づく価値創出を実現しうるかが注目される。

(いけがい なおと)

(47) “COPPA Safe Harbor Program.” Federal Trade Commission Webpage <<http://www.business.ftc.gov/content/safe-harbor-program>> 児童オンライン・プライバシー保護法については、入江晃史「オンライン上の児童のプライバシー保護の在り方について—米国、EUの動向を踏まえて—」『情報通信政策レビュー』6号, 2013.3, pp.5-6. 総務省ウェブサイト <http://www.soumu.go.jp/iicp/chousakenkyu/data/research/icp_review/06/iric2013.pdf>を参照。