

EUの行政機関に適用される個人データ保護規則における基本概念

-個人データ保護条約及びEU一般個人データ保護規則との関係を含めて-

メタデータ	言語: jpn 出版者: 明治大学法律研究所 公開日: 2017-03-31 キーワード (Ja): キーワード (En): 作成者: 夏井, 高人 メールアドレス: 所属:
URL	http://hdl.handle.net/10291/18551

【論 説】

EUの行政機関に適用される個人データ保護規則における基本概念

—— 個人データ保護条約及びEU一般個人データ保護規則との関係を含めて ——

夏 井 高 人

目 次

- 1 はじめに
- 2 欧州連合 (EU) における個人データ保護法制の基本的な枠組み
 2. 1 保護法益
 2. 1. 1 プライバシーの権利
 2. 1. 2 情報の自由
 2. 1. 3 個人データの侵害
 2. 1. 4 矛盾と解決策
 2. 2 法的枠組み
 2. 2. 1 個人データ保護条約 ETS No.108 及び追加議定書 ETS No.181
 2. 2. 2 個人データ保護指令 95/46/EC
 2. 2. 3 行政機関個人データ保護規則 (EC) No 45/2001
 2. 2. 4 一般個人データ保護規則 (EU) 2016/679
 2. 2. 5 ネットワーク及び情報システムの安全性に関する指令 (EU) 2016/1148
 2. 2. 6 欧州における個人データ保護のための法制度全体の関係
2. 3 行政機関個人データ保護規則への反映
- 3 個人データ保護の基本原則
 3. 1 原則
 3. 1. 1 欧州評議会閣僚委員会の決議
 3. 1. 2 個人データ保護条約 ETS No.108 第 5 条
 3. 1. 3 個人データ保護指令 95/46/EC 第 6 条
 3. 1. 4 行政機関個人データ保護規則 No 45/2001 第 4 条
 3. 2 データ主体の権利
 3. 2. 1 個人データに関する情報へのアクセスの権利
 3. 2. 2 個人データの訂正を求める権利
 3. 2. 3 個人データの処理の停止を求める権利
 3. 2. 4 個人データの削除を求める権利
- 4 権利の制限
- 5 第三国への個人データの移転
- 6 データ主体の情報の自由 (可搬性)
- 7 まとめ

1 はじめに

2016年4月27日、欧州議会及び欧州連合理事会は、「個人データの処理と関連する自然人の保護及び個人データの自由な移転並びに指令95/46/ECの廃止に関する欧州議会及び理事会の2016年4月27日の規則(EU)2016/679」⁽¹⁾（以下「一般個人データ保護規則GDPR」という。）を可決した。同規則は、2018年5月25日から適用（施行）となる。

一般個人データ保護規則GDPRは、欧州連合の全ての構成国に直接に適用される。同規則の条文の末尾には「この規則は、その全部について拘束力があり、かつ、全ての構成国において直接に適用可能である」との宣言がある。それゆえ、法規範としての名称は「規則(Regulation)」となっているものの、その法規範としての実質は、「法律(Act)」である。規則は、直接的(self-executing)な法的効力を有しない条約や指令等とは基本的に異なる。

2018年5月25日以降、欧州連合の全ての構成国は、同規則の施行のために必要な細則を定める自国の法令と併せ、一般個人データ保護規則GDPRの条項を自国の国内法として適用することになる。その結果として、一般個人データ保護規則GDPRは、国際的裁判管轄権や準拠法を踏まえた上で、日本国と各構成国との間における国際的な契約上の問題その他の法的問題との関係でも直接に適用され得る。

2018年5月25日（施行日）に至るまでの移行期間内は、従前の「個人データの処理と関連する個人の保護及び個人データの自由な移転に関する欧州議会及び理事会の1995年10月24日の指令95/46/EC」⁽²⁾（以下「個人データ保護指令95/46/EC」という。）が適用される。

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

<http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN> [2016年9月24日確認]

(2) 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 (OJ L 281 p.31, 1995)

<http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:1995:281:FULL&from=FI> [2016年9月23日確認]

ところで、規則の適用対象に関して、一般個人データ保護規則 GDPR の第 2 条第 3 項は、欧州連合の行政機関における個人データ処理については、「欧州共同体の機関及び組織による個人データの処理と関連する個人の保護及び個人データの自由な移転に関する 2000 年 12 月 18 日の規則 (EC) No 45/2001」⁽³⁾（以下「行政機関個人データ保護規則 No 45/2001」という。）が適用されると規定している。

行政機関個人データ保護規則 No 45/2001 は、リスボン条約により欧州連合が成立する以前に制定されたものであるため、規則の名称も欧州連合の行政機関ではなく欧州共同体の行政機関を前提とするものであるが、一般個人データ保護規則 GDPR の第 2 条第 3 項により、同規則に適合するように修正されるため、行政機関個人データ保護規則 No 45/2001 中で「欧州共同体 (the Community)」とある部分は、自動的に「欧州連合 (the Union)」と読み替えられ、そのように適用されることになる。

また、行政機関個人データ保護規則 No 45/2001 と個人データ保護指令 95/46/EC の関係に関しては、直接的な効果のない指令 (Directive) という法形式を採用している個人データ保護指令 95/46/EC ではなく、実質的には法律 (Act) である規則 (Regulation) という法形式を採用している行政機関個人データ保護規則 No 45/2001 が欧州連合 (欧州共同体) の行政機関に対して直接に適用される法規範となっている⁽⁴⁾。

行政機関個人データ保護規則 No 45/2001 は、日本国の法令では、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・以下「行政機関個人情報保護法」という。）に相当する法令である。その法規範としての重要性が極めて高いものであるのにも拘らず、従来、日本国においては、同規則があまり注目されてこなかった。

(3) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:en:PDF> [2016 年 9 月 24 日確認]

(4) 行政機関個人データ保護規則 No 45/2001 の条文中で個人データ保護指令 95/46/EC の条文が参照されている場合には、参照された個人データ保護指令 95/46/EC の条文が準用または適用されたことになる。

しかしながら、後述するように、欧州連合における個人データ保護法制は、民間部門（**private sector**）については主として一般個人データ保護規則 **GDPR** が適用され、欧州連合の公的部門（**public sector**）については主として行政機関個人データ保護規則 **No 45/2001** が適用され、構成国の公的部門には構成国の関連法令が適用される。

これらの規則及び構成国の法令において保護法益として法的に保護されている法的な利益は共通である。すなわち、欧州の個人データ保護法制におけるデータ主体の保護法益は、データ主体（本人）のプライバシーの権利である。そして、プライバシーの権利を保護するための手段的・技術的・人工的な権利として、様々な「データ主体の権利」を認めている。

他方において、個人データの処理をする管理者の保護法益も明確に認められている。それは、情報の自由（個人データの自由な移転）である。

このプライバシーの権利及び情報の自由のいずれもが、直接には欧州人権条約（**The European Convention on Human Rights**）に由来するものだと考えられる。これらの権利と自由は相互に矛盾する要素を含んでいることから、その調和または整合性の確保が必要となる。後述のとおり、欧州連合域外の諸国（第三国）に対する個人データの移転に関する問題（十分性）もそのような調整または整合性の確保と関連する課題の一部として理解しなければならない。

欧州連合における個人データ保護のための基本的な枠組み（**framework**）を理解する上で、その保護法益を正確に把握することは、それ自体として非常に重要なことである。のみならず、今後、これら行政機関個人データ保護規則 **No 45/2001** 及び一般個人データ保護規則 **GDPR** という 2 つの重要な規則が欧州連合において直接に適用されることになることから、これらの規則が保護法益とするプライバシーの権利及び情報の自由の相互関係を丁寧に考察した上で、更に、日本国との間のデータ移転との関係における法令の適用を十分に検討しなければならない。

本稿で指摘する問題点等は、法と情報雑誌の誌上において一般個人データ保護規則 **GDPR** の参考訳⁽⁵⁾ 及び行政機関個人データ保護規則 **No 45/2001** の参考訳⁽⁶⁾ 並

(5) 一般個人データ保護規則 **GDPR** の全訳は、法と情報雑誌 1 巻 3 号 1～186 頁にある。以下「一般個人データ保護規則参考訳」という。

(6) 行政機関個人データ保護規則 **No 45/2001** の全訳は、法と情報雑誌 1 巻 2 号 74～116 頁にある。以下「行政機関個人データ保護規則参考訳」という。

びにこれらの規則と関連する条約及び指令等を訳出し公表するにあたって特に慎重な検討を要した事項を含んでいる⁽⁷⁾。それらについて、更に考察を進めた結果を本稿において示したいと思う。

本稿は、法解釈学に関する論文であるが、手法としては法情報学及び法史学を基礎とする調査及び考察を重視した検討結果に基づき、欧州のデータ保護法制における基本概念の由来に関する知見を提供すること、そして、それらが行政機関個人データ保護規則 No 45/2001 中ではどのように現れているかに関する知見を提供することを目的とする。

2 欧州連合（EU）における個人データ保護法制の基本的な枠組み

2.1 保護法益

個人データの保護法制と関連する法的な利益すなわち保護法益に関しては諸説ある。その見解がいかなるものであるにしても、個人データの保護法制における保護法益に関する学説や理論は、それぞれの学問の自由の領域に属するものである。

しかしながら、事実の問題として、「欧州における個人データ保護法制において何が保護法益としてとらえられてきたのか」を認識・理解するという社会科学上の調査研究の目的のためには、通常法解釈学⁽⁸⁾の手法または思弁だけに頼るのではなく、法情報学（Legal Informatics）や法社会学（Sociology of law）のアプローチを重視した検討を行うことも重要なことであり、かつ、有用である⁽⁹⁾。

(7) 前掲の2つの参考訳中では、結論を出さずに保留したまま訳注においてその旨を注記した部分が少なくない。本稿においては、その後の検討結果を踏まえ、より正確な検討結果を示したいと考える。そのため、本稿において述べる事項と前掲の2つの参考訳内の注記と異なる内容を示す部分があるときは、本稿によって修正される。訳語についても同じである。

(8) 欧州連合における人権条項の実装と解釈に関しては、Bjarte Thorson, *Individual Rights in EU Law*, Springer (2016) pp.43–80が参考になる。

(9) 情報社会を準備したゲーテンベルグ以降の活字技術及びその後の様々な情報技術が人類の文化と社会に与えた影響を認識・理解する上では、マーシャル・マクルーハン（森常治訳）『ゲーテンベルクの銀河系—活字人間の形成』（みすず書房、1986）、マーシャル・マクルーハン（栗原裕・河本仲聖訳）『メディア論—人間の拡張の諸相』（みすず書房、1987）が参考になる。情報通信技術が社会と法制度全体に与える影響に関しては、夏井

個人データの法的保護に関して、欧州で最初に制定された法規範は、1981年1月28日の欧州評議会の個人データ保護条約 ETS No.108 (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data) である。個人データ保護条約 ETS No.108 の説明書 (Explanatory Report)⁽¹⁰⁾ によれば⁽¹¹⁾、個人のプライバシーの権利 (the right of personal privacy) 及び欧州人権条約第 10 条第 1 項に規定する情報の自由 (freedom to hold opinions and to receive and impart information and ideas) がその保護法益である。

2. 1. 1 プライバシーの権利

プライバシーの権利の理解については、諸説ある⁽¹²⁾。その概念は、時代と共に変化し続けている⁽¹³⁾。一般に、「プライバシーの利益」ないし「プライバシーへの期待」は、一定の社会環境と個人との関係の中で成立するものであるので、社会環境の変化及び自然人の意識や思想の変化に同期して変化し続ける。それゆえ、この概念を固定的または物的にとらえることは妥当ではなく、これを関係的または機能的なものとしてとらえる必要がある。

高人『ネットワーク社会の文化と法』(日本評論社、1997)で述べた。同書は、Alvin Toffler, *The Third Wave*, Bantam Books (1980) に示されている世界観をベースとしている。最近の書籍の中では、Luciano Floridi, *The 4th Revolution*, Oxford University Press (2014) が参考になる。

(10) Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca434> [2016年9月23日確認]

(11) 個人データ保護条約 ETS No.108 及び追加議定書 ETS No.181 並びにその説明書の全訳は、法と情報雑誌 1 巻 4 号 1~20 頁及び同誌 26 頁~58 頁にある。

(12) 堀部政男『プライバシーと高度情報化社会』(岩波新書、1988)、新保史生『プライバシーの権利の生成と展開』(成文堂、2001)、石井夏生利『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』(勁草書房、2008)、Ronald J. Krotoszynski, Jr., *Privacy Revised: A Global Perspective on the Right to Be Left Alone*, Oxford University Press (2016)、Serge Gutwirth, Yves Poullet, Paul de Hert & Ronald Leenes (Eds.), *Computers, Privacy and Data Protection: an Element of Choice*, Springer (2011) 及び Serge Gutwirth, Ronald Leenes & Paul De Hert (Eds.), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, Springer (2016) が参考になる。

(13) 一般に、「後の法理論のほうが古い法理論よりも進化している」という前提を採ることに は慎重であるべきである。古典的でも正しい理論や不動の真理が存在する一方で、他方では、「古典的な理論を乗り越えた」と自称する粗雑な理屈や偽理論も存在する。

このような観点からすると、現時点においても、プロッサー（William L. Prosser）の4種類の理論⁽¹⁴⁾を乗り越える理論構成は存在しないと考えられる⁽¹⁵⁾。一般に、プロッサーの理論は、過去のものだと勝手に思いこんでいる論者が決して少なくない。しかし、高度に情報化が進んでいる現代社会とりわけサイバー空間において、プライバシーをめぐる諸問題を考察する場合には、プロッサーの理論の学術上の価値及び実務上の有用性は絶大である。

プロッサーの類型論は、サイバー空間においてこそ、まさにその真価を発揮することができるであろう。とりわけ、一般個人データ保護規則GDPR及び行政機関個人データ保護規則No 45/2001の中に定める「自動的な個人データの処理（プロファイリング）のみに基づく自然人の人格的な側面の判定の拒絶の権利」に関して考察する上では、プロッサーの類型論とりわけその第3類型（Publicity which places the plaintiff in a false light in the public eye）⁽¹⁶⁾及び第4類型（Appropriation, for the defendant's advantage, of the plaintiff's name or likeness）の十分な理解と応用が不可欠である⁽¹⁷⁾。

「プライバシーの権利」の概念それ自体についての理論構成を一応措いて、欧州評議会の個人データ保護に関する専門家委員会が個人データ保護条約ETS No.108を起草した際に理解していた「プライバシーの権利」の概念について検討してみると、個人データ保護条約の説明書第4項は、欧州評議会・議員会議の勧告第509号（1968年）⁽¹⁸⁾に由来するものである旨を述べている。

(14) William L. Prosser, *Privacy*, California Law Review vol.48 pp.383–423 (1960)

(15) 伊藤正巳『プライバシーの権利』（岩波書店、1963）は、内容的には、前掲William L. Prosser, *Privacy*とほぼ同一なので、この『プライバシーの権利』を読めば、プロッサーの理論の概略を理解することができる。

(16) Bruce A. McKenna, *False Light: Invasion of Privacy*, Tulsa Law Review, Vol.15 Issue 1 pp.113–140

(17) 欧州において個人データ保護条約ETS No.108が起草され、また、国際機関であるOECDのプライバシーガイドラインが策定された1980年当時においては、プライバシーの権利のより積極的な側面が重視されるようになっており、その対外的効力（物権的請求権的な法的効力）が注目されるようになっていた。例えば、Arthur R. Miller, *Assault on Privacy: Computers, Data Banks, & Dossiers*, University of Michigan Press, 1971がその例である。ただし、同書は、ドイツ民法学流の物権的請求権及びそれに類する権利のことを述べているわけではない。

(18) Parliamentary Assembly Recommendation 509 (1968): Human rights and modern scientific and technological developments

欧州評議会・議員会議の勧告第 509 号の第 3 項には、「欧州人権条約の第 8 条によって保護されるプライバシーの権利に対する脅威」との文言があり、同勧告の第 4 項、第 6 項及び第 8 項にも同様の文言がある。

そこで、欧州人権条約第 8 条をみると、同条約の第 8 条第 1 項は、「すべての者は、その私的及び家族生活、住居及び通信の尊重を受ける権利を有する」⁽¹⁹⁾と規定している。要するに、欧州個人データ保護条約 ETS No.108 の起草者達の頭の中にあつたのは、私生活の保護及び通信の秘密の保護という文脈における「プライバシー」の概念である。この意味でのプライバシーが物的に侵害を受けることはあり得ることで、それは、プロッサーの類型では第 1 類型 (Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs) 及び第 2 類型 (Public disclosure of embarrassing facts about the plaintiff) に属する。

しかし、個人と関連する情報(データ)が第三者によって大量に処理され、それが第三者によって流布される事態が恒常的なものとなると、事実の問題として、第三者からの誤った「評価」によって、私人の現実の私生活に対する侵害的な結果が生ずることがあり得る。

欧州評議会・議員会議の勧告第 509 号及び個人データ保護条約 ETS No.108 の説明書の中にはそのような脅威に対する危惧感が濃厚に示されており、そのような脅威を抑制または排除するための技術的かつ人工的な権利として「個人データに関する権利」といったようなものが構想されたものと推定される。

すなわち、「個人データに関する権利」は、自然権(天賦人権)の一種ではない。

確かに、その後の欧州連合基本権憲章⁽²⁰⁾の中には、欧州人権条約第 8 条第 1 項に相応する条項(第 7 条)が設けられ、しかも、同憲章の第 8 条では「個人データに関する権利」が別の権利として規定されている⁽²¹⁾。

<http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=14546&lang=en> [2016 年 9 月 25 日確認]

(19) 薬師寺公夫・坂元茂樹・浅田正彦編『ベーシック条約集 2106』(東信堂、2016)の記による。

(20) The Charter of Fundamental Rights of the European Union

<http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=en> [2016 年 9 月 25 日確認]

(21) 欧州連合基本権憲章は、2000 年に制定されたが、リスボン条約締結に伴い、2012 年に一部改正がなされている。その全訳は、法と情報雑誌 1 巻 2 号 1~33 頁にある。

すなわち、同憲章第8条第1項は、「全ての者は、彼または彼女と関係する個人データの保護の権利を有する」と規定し、同条第2項は、「かかるデータは、特定の目的のために公正に、かつ、当該個人の同意もしくは法令に定めるその他の根拠に基づいて処理されなければならない。全ての者は、収集された彼または彼女に関するデータにアクセスする権利及びそのデータを正しく修正する権利を有する」と規定し、そして、同条第3項は、「これらの規範の遵守は、独立の行政機関の監督に服する」と規定している⁽²²⁾。

同条第2項に定めるアクセスの権利及び訂正の権利は、個人データ保護条約で定められた原則を欧州連合基本権憲章上の権利として再構成したものとして理解することができる。同条第3項は、個人データ保護監督官を独立の行政機関とするという点についての制度的保障の一種と解される。

現在の欧州連合基本権憲章は、欧州連合の機能に関する条約（TFEU）に基づく国家秩序または国家体制に基づくものである。同条約には、構成国の国家主権の維持及び国防等と関連する特例が存在し、非常事態の下にある場合には、人権の停止をすることができる。そうである以上、基本権憲章に定める人権の本質が国家権力といえども停止することのできない権利という意味での自然権（天賦人権）ではないということが明らかである。このことは、欧州人権条約に定める人権についても基本的には同じである。

欧州連合基本権憲章に定める人権は、法規範の階層構造の上位にある権利である以上、より具体的な権利を構成国が制定する際の価値判断の基準となるべきものであることは当然のことであるが、人工的な規範の体系の一部をなす構成要素の1つに過ぎない。このことは、同憲章の第49条第2項の存在からも論証することができる。

欧州連合基本権憲章第8条に定める個人データに関する権利は、技術的・手段的な権利の一種として理解すべきである。そして、その技術的・手段的な権利を行使することによって保護しようとしている真の保護法益は、プライバシーの権利である。ただし、技術的・手段的な権利というものが必要になった歴史的・経済的・社会的背景としては、プロセッサの種類の第3類型及び第4類型に属するような侵害

(22) Dirk Ehlers (Ed.), *European Fundamental Rights and Freedom, De Gruyter Recht* (2007) pp.411–417

が顕著になったということがある。このことを明確に念頭に置いて法解釈を進める必要がある⁽²³⁾。

以上述べてきたようなプライバシーの権利を保護法益とし、その保護法益を法的に保護するための技術的・手段的・人工的な権利として個人データの権利が定められるという法規範の基本的な階層構造は、欧州連合における個人データ保護法制の保護法益を構成するものであり、それは、一般個人データ保護規則 GDPR 及び行政機関個人データ保護規則 No 45/2001 においても、そのままのかたちで維持されていると解される。

2. 1. 2 情報の自由

情報の自由に関しても諸説ある⁽²⁴⁾。「情報の自由」は、法学の領域においてのみならず、社会学や経済学等の分野においてもしばしばとりあげられる。また、法学だけに限定しても、分野によって異なる趣旨で「情報の自由」の概念が用いられることがある。例えば、著作権法の領域においてかなり限定された文脈で論じられることがある⁽²⁵⁾。

しかしながら、欧州の個人データ保護の基本的な法的枠組みを認識・理解する上で最も重要なものは、やはり、個人データ保護条約 ETS No.108 及びその説明書である。説明書の第 19 項は、「情報の自由」が表現の自由について定める欧州人権条約第 10 条及び市民的及び政治的権利に関する国際規約（B 規約）の第 19 条に由来するものだと説明している。

欧州人権条約第 10 条は、「すべての者は、表現の自由の権利を有する。この権利

(23) このようなタイプの問題について検討する際には、「デジタルパーソン (digital person)」という概念は全く不要である。この概念は、古くからある「ペルソナ (persona)」を現代の情報環境という文脈における「自己と他者」の関係論の中で再配置したものと考えられる。しかし、そのような哲学的思索を一応措いて、純然たる法解釈論の範囲内で考察した場合、サイバー空間において本人のプライバシーの利益の侵害を惹起し得る情報の総体は、プロッサーの古典的な類型論の中に全て吸収して考えることができる。同様に、いわゆる法と経済に属する諸説もまた、知識遊戯の一種に過ぎず、法解釈論の場及び訴訟の場（特に要件事実の関係）では、ほぼ無意味である。

(24) 情報の自由を扱った書籍として、山口いつ子『情報法の構造—情報の自由・規制・保護』（東京大学出版会、2010）がある。ただし、論旨難解の部分が多い。

(25) 関連する論説として、原絵理「著作権者の権利と情報の自由—ベルヌ条約の規定とその変遷」出版研究 33 号 221～241 頁、小野寺夏生「データベースに関する権利と責任—欧米における最近の動向から—」情報管理 34 巻 9 号 801～818 頁、金子敏哉「出版権のこれまでとこれから—研究者の立場から」ジュリスト 1463 号 49～54 頁がある。

は、公の機関から干渉を受けることなく、かつ、国境と無関係に、意見を持つ自由、情報と考えを受ける自由及びそれらを伝達する自由を含む。本条は、国家が、放送事業、テレビ事業または映画事業について免許を要するものとするを妨げない」と、同条第2項は「これらの自由の行使は、義務及び責任を伴うものであり、かつ、法律が定める手続、条件、制限または刑罰であって、民主主義社会において、国家安全保障の利益、領土の完全性の維持もしくは公共の安全の利益により、無秩序もしくは犯罪を防止するため、健康もしくは道徳を保護するため、他者の信用もしくは権利を保護するため、機密のものとして受けた情報の開示を防止するため、または、司法機関の権威及び公平性を維持するために必要なものを課することができる」と規定している⁽²⁶⁾。

他方、市民的及び政治的権利に関する国際規約（B規約）第19条第1項は「すべての者は、干渉されることなく意見を持つ権利を有する」と、同条第2項は「すべての者は、表現の自由についての権利を有する。この権利には、口頭、手書き若しくは印刷、芸術の形態又は自ら選択する他の方法により、国境とのかかわりなく、あらゆる種類の情報及び考えを求め、受け及び伝える自由を含む」と、そして、同条第3項は「2の権利の行使には、特別の義務及び責任を伴う。したがって、この権利の行使については、一定の制限を課することができる。ただし、その制限は、法律によって定められ、かつ、次の目的のために必要とされるものに限る。
(a) 他者の権利又は信用の尊重 (b) 国の安全、公の秩序又は公衆の健康若しくは道徳の保護」と規定している（外務省訳による）。

要するに、ここに掲げられている「情報の自由」の実質的内容とは、表現の伝達形態の一種である「情報」を受ける自由及びそのような「情報」を伝える自由を認めるというものである⁽²⁷⁾。

ここでいう「情報」は、電子データ化された情報に限らないが、人間による表現

(26) William A. Schabas, *The European Convention on Human Rights: A Commentary*, Oxford University Press (2015), pp.444–482

(27) 「個人の表現」の伝達方式として「情報」を理解するのではなく、情報それ自体の財産的価値を承認し、財産権としての情報財というものを観念する場合には、「情報の自由」とは、「財産権である情報財が支障なく移転可能であること」を意味することになる。この文脈では、思想・信条の自由と切り離して、純粋に財産権としての考察が必要となる。これらの点については、夏井高人「情報財—法概念としての意義—」明治大学社会科学研究所紀要52巻2号213～241頁で述べた。

の一形態であることを要する。そのことから、人間の意思による影響を受けないで電子装置等によって自動的に生成された電子的な符号の集合⁽²⁸⁾は、この「情報」に含まれないことになる。また、動物行動学⁽²⁹⁾の見地からは別の見解もあり得ようが、ここでの文脈においては、野生動物が用いる各種の情報伝達のための動作等⁽³⁰⁾を含まない。

そして、「情報」は、あらゆる種類の情報を含むので、その中には個人の人格的側面に対する評価に対して影響を与え得るものが含まれ得ることになる。そのような属性をもった情報は、個人と関連する情報として認識され、更にその中の一定の属性を有するものが個人データとして保護されるという理論構成が採用されている。この場合、情報の自由の側からみれば、個人データの保護は、情報の自由に対する制約要素となる。

情報の自由について、それが無限定の自由ではなく、一定の制限が最初から存在すること、すなわち、何らかの制約要素（制約条件）が存在することは、上記の欧州人権条約第 10 条第 2 項及び市民的及び政治的権利に関する国際規約（B 規約）第 19 条第 2 項から明らかである。

個人データ保護条約 ETS No.108 が個人データの法的保護を定めたことは、欧州人権条約第 10 条第 2 項に示される抽象的な制約条件の中の一定の属性を有するものについて、より明確に定めたものであると理解することも可能であろう。更に、一般個人データ保護規則 GDPR が定める「忘れられる権利（削除権）」（第 17 条）や自動的なプロファイリングのみに基づく人格的側面の判定に対する拒絶の権利（第 22 条）は、そのような制約条件の中でも特に強い法的保護が求められるものについて、具体的な手続条項を伴う手続的・技術的権利として明定したものであ

(28) したがって、完全に自律的なものである限り、人工知能やロボットには「情報の自由」が成立しない。

(29) コンラート・ローレンツ（日高敏隆訳）『ソロモンの指環—動物行動学入門』（早川書房、1975）、デズモンド・モリス（日高敏隆訳）『裸のサル—動物学的人間像』（河出書房新社、1969）が参考になる。

(30) 野生動物のものである限り、どれがどのように高度な知的作用（脳機能の発揮・発現）を含むものであっても、「情報の自由」が成立しない。人間の細胞を組み込み、外見上は人間と全く相違のないミュータントの場合においても、それは人工的に製造された合成生物（雑種）なのであってホモサピエンスではない以上、同様である。サイボーグの場合であっても、脳以外の組織が人間のものであり、脳組織が完全に人間以外のものに置き換えられている場合には、同じである。

ると理解することができる⁽³¹⁾。

他方、個人データ保護指令 95/46/EC、一般個人データ保護規則 GDPR 及び行政機関個人データ保護規則 No 45/2001 に定める個人データの自由な移転（free movement or free flow）は、無制約な個人データの売買や譲渡のことを意味するものではなく、上記のような制約条件を当然に伴うものとしての個人データを含む情報の伝達の自由という文脈においてのみ理解されるべきである。

従って、欧州の法制における個人データの「自由な移転」は、いわゆる「利活用」の場合を含め⁽³²⁾、個人データの無制約な商業利用を推進する政策的意図を全くもっていない。

一般個人データ保護規則 GDPR 及び行政機関個人データ保護規則 No 45/2001 の定める内容を仔細に検討してみると、例えば、電子商取引の過程における契約成立の際の法的対応⁽³³⁾については、同規則内に合理的な規律が定められている。そ

(31) 忘れられる権利の本質は、プライバシー侵害行為に対する妨害排除請求または妨害予防請求を実現するための権利である。それは、プライバシーの権利を守るための技術的・手段的な権利である。同じ目的は別の手段によって達成することもできる。例えば、問題のある事業者に対して「忘れられる権利」を行使して削除を求めるのではなく、当該事業者が違法行為を行っていることを明らかにし、監督官庁の措置命令によって当該事業を営業停止の状態とする場合、あるいは、そのような措置命令がなされたことを苦にして当該事業の経営者が自殺してしまったといったような場合には、問題の発生が根元から全て遮断されることになる。この設例の場合、手段の相違があるだけで、どちらの方法によってもプライバシーの権利に対する妨害の排除または予防に成功したことになる。それゆえ、「忘れられる権利」は、手段的・技術的・人工的な権利の一種である。

(32) 一般に、個人データを匿名化または仮名化すれば自由に移転することができるとの誤解があるように思われる。仮名化や匿名化は、それが永久的または半永久的なものであり、かつ、法的な権限を有する者以外は実名に戻すことができず、かつ、実名で個人データを利用する場合にはそれが収集された目的の範囲内で行われなければならないという原則がある。ところが、マーケティング目的で流通している個人データは、それが流通する過程では匿名化または仮名化されていたとしても、実際にマーケティングが実行される時点では実名化されていなければマーケティングの目的を達成することが不可能である。このような事例では、流通過程では部分的に匿名化または仮名化の措置が行われているかもしれないが、全体としてみると「仮名化も匿名化もない状態」にあるものとして判断すべきである。すなわち、原則として、違法行為である。なお、この関連では、Julia Lane, Victoria Stodden, Stefan Bender & Helen Nissenbaum (Eds.), *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, Cambridge University Press (2014) pp.276–295 が参考になる。

(33) 一般個人データ保護規則参考訳の前文(40)の訳注、第6条第1項(b)、第7条第4項及びその訳注、第13条第2項(e)、第20条第1項(a)、第22条第2項(a)、第28条第3項、第4項、第6項、第9項及びそれらの訳注並びに第49条第1項参照

して、欧州連合全体としては域内市場における電子商取引の活性化を含め、域内市場全体がより豊かなものとなることを期待していることが明らかである。しかし、その場合に行われる個人データの国境を越えた移転は、これらの規則が明確に定める個人データの法的保護という制約条件を完全に遵守した上で行われることが絶対条件となっている。そして、無制約の個人データの売買等はそもそも全く念頭にない。このことは、後述の個人データ処理の場合においては目的による制限によって限定がなされていることから明らかである。普通に考えた場合、欧州連合の立法者の意思は、無制約な個人情報（個人データ）のいわゆる「利活用」なるものには全く反対の立場を採っていると理解すべきである⁽³⁴⁾。

このことは、一般個人データ保護規則 GDPR の第 2 条第 4 項により同規則の制定後においても法的有効性を維持する「域内市場における情報社会サービス特に電子商取引の法的側面に関する欧州議会及び理事会の指令 2000/31/EC」（以下「電子商取引指令」という。）との関連においても同じである。また、同様に、一般個人データ保護規則 GDPR の第 95 条により同規則の制定後においても法的有効性を維持する「電子通信分野における個人データの処理及びプライバシー保護に関する欧州議会及び理事会の指令 2002/58/EC」（以下「プライバシー及び電子通信指令」という。）との関連においても同じである⁽³⁵⁾。

なお、一般個人データ保護規則 GDPR は、主として大規模に電子的な処理が行われる場合に適用されるものである。それゆえ、同規則第 2 条第 2 項 (c) は、「自然人によって純粹に私的な行為または家庭内の行為の過程において行われる場合」には、同規則が適用されないものと定めている。このような場合には、欧州人権条約第 10 条第 1 項に定める情報を受ける自由または情報を伝送する自由が原則どおりに適用される⁽³⁶⁾。

(34) 一般個人データ保護規則参考訳の前文(6)の訳注、前文(13)の訳注及び前文(39)の訳注参照

(35) この指令の全訳は、法と情報雑誌 1 巻 2 号 117～162 頁にある。

(36) この場合でも、欧州人権条約第 10 条第 2 項の適用があることは当然のことである。例えば、特段の公益上の目的を有することなく、かつ、事実を証拠によって証明できるわけでもないのに、単に他人のゴシップ情報を公開したり、誹謗中傷または名誉毀損の目的で私事を公開したりすれば、同条約第 2 項による責務に反するものとして違法行為となる。そのような情報の発信が機械的に自動収集されたデータの自動的な結合と自動的な公衆送信可能化によって無限定に実行される場合、人間の意思活動が介在しない以上、正当

2. 1. 3 個人データの侵害

個人データと関連する権利の本質を理解する上で、一般個人データ保護規則 **GDPR** に導入された「個人データの侵害（**personal data breach**）」という概念に触れておく。同規則の第4条(12)は、「個人データの侵害」について、「偶発的または違法な、破壊、喪失、改変、無権限による開示またはそれに対する無権限のアクセスを導くような、移転、記録保存その他の処理がなされる個人データの安全性に対する侵害のことを意味する」と定義している。これは、個人データの侵害の定義なのであって、個人データと関連する権利の侵害の定義ではない。

そこで、個人データの侵害があった場合にどのような権利が侵害されたことになるのかについて検討してみると、一般個人データ保護規則 **GDPR** の第33条第1項は、「個人データの侵害が発生した場合には、管理者は、不適切な遅滞なく、かつ、それが実施可能であるときは、その侵害に気づいた時から遅くとも72時間以内に、第55条に従って職務権限を有する監督官に対し、その個人データの侵害について通知しなければならない。ただし、その個人データの侵害が自然人の権利及び自由に対するリスクを生じさせるおそれがない場合には、この限りではない」と規定し、同規則第34条第1項は、「個人データの侵害が自然人の権利及び自由に対する高度なリスクを発生させる可能性がある場合、管理者は、そのデータ主体に対し、不適切な遅滞なく、その個人データの侵害について通知しなければならない」と規定し、同条第4項は、「管理者がデータ主体に対して個人データの侵害についてまだ通知をしていない場合には、監督官は、その個人データの侵害が高度なリスクを発生させる可能性について考慮した上で、そのようにすべきことを要求することができ、または、第3項に示す要件のいずれに該当するかを判断することができる」と規定していることを知ることができる。

そして、一般個人データ保護規則 **GDPR** の第70条第1項(h)は、個人データ保護委員会の職務として、「第34条第1項に示す個人データの侵害が自然人の権利及び自由に対する高度なリスクをもたらす可能性のある状況に関して、本項の(e)に従い、運用指針、勧告及びベストプラクティスを発行すること」と規定していることを知ることができる。

これらの条項から理解することができることは、個人データそれ自体に何らかの

な評論活動や学術活動に該当する余地は全くなく、常に違法行為となる。

権利があるわけではなく、個人データが違法または不当な扱いを受けた場合に、その結果として、当該個人データと関連するデータ主体の「権利または自由 (rights or freedom)」に何らかのリスクが発生する場合には、各条項に定める法的効果が発生するということである。

2. 1. 4 矛盾と解決策

プライバシーの権利の保護と情報の自由との間では、ときとして、矛盾や利害の衝突が生ずることがある。そのことは、個人データ保護条約 ETS No.108 の起草者達によって明確に認識されていた。例えば、同条約の第 9 条第 2 項 (b) は、「データ主体または他人の権利及び自由」を保護するために必要があるときは個人データに関する権利の行使を制限するための例外条項 (特例) を制定することができるものと規定し、その趣旨について、説明書の第 58 項は、「データ主体自身の利益 (例えば、精神状態に関する情報) または第三者の利益 (例えば、出版の自由、営業秘密等) といったような私人の重要な利益と関係している」と説明している。欧州の個人データ保護立法における調和の達成または整合性の確保の試みは、このような条約加盟国各国の立法裁量に任せるところから開始された。

その後、条約の非加盟国である欧州域外の諸国へ向けた個人データの移転の場合には、そもそも条約の定める個人データ保護の枠組みが適用されないことが明確に認識された。その結果、条約については、1999 年の追加議定書 ETS No.181 によって問題を解消するための追加的な改正がなされた。また、欧州共同体 (後の欧州連合) では、個人データ保護指令 95/46/EC、行政機関個人データ保護規則 No 45/2001 及び一般個人データ保護規則 GDPR が制定され、より詳細に手続を構築するかたちで、個人データ保護の法的枠組みを欧州域外の国々 (第三国) に対しても適用可能なものとする制度的枠組みが構築され続けている。

そのような法的な枠組みの中には、権利と自由との衝突や矛盾を解決し、整合性を確保するための手段も含まれる。「個人データの自由な移転」がデータ主体のプライバシーの権利を保護するための適切な安全性確保措置が講じられていることを絶対条件とするという基本原理は、2016 年 4 月に制定された一般個人データ保護規則 GDPR の前文中では、更に明確なものとして述べられている。

ここにおいて理解すべきことは、法解釈学において、利益考量をする場合の判断基準が各国の自由に任されているわけではない時代に突入しているという事実で

ある⁽³⁷⁾。EUの近時の立法を見る限り、法的に保護されるべき諸価値の調整原理は、抽象的な権利のレベルにおいて一般的に目標や指針が定められているだけではなく、それを実現するための具体的な手段を伴うことが多くなってきている。そのような傾向は、とりわけ一般個人データ保護規則GDPRにおいては、更に顕著なものとなっている。欧州の法制における諸価値の調整原理を理解するためには、関連法令の中で定められている技術的・手段的な調整原理の存在根拠や運用の基本原則を咀嚼・理解しながら、妥当な利益考量がなされなければならない。

2. 2 法的枠組み

2. 2. 1 個人データ保護条約ETS No.108及び追加議定書ETS No.181

個人データ保護条約ETS No.108⁽³⁸⁾は、法律ではなく条約（国際合意）であるとはいえ、個人データの法的保護のための世界で最初に成立した法規範である。加盟国を欧州評議会の構成国に限定しておらず、非構成国もこの条約に加盟している。

個人データ保護条約ETS No.108は、当時、プライバシーガイドラインの策定作業を進めていたOECDの理事会と密接な連絡を取り合いながら、OECDに加盟している非欧州圏の諸国代表（アメリカ合衆国、日本、オーストラリア、カナダ）も起草作業に参加して起草された。同条約は、1981年1月28日、署名のため開放され、1985年10月1日、所定の要件を満たす批准国数に達したため、発効した。

個人データ保護条約ETS No.108は、欧州共同体が加入することができるようにするため、1999年6月15日に改正された。その後、個人データ保護条約ETS No.108は、2001年11月8日に署名のために開放された追加議定書ETS No.181⁽³⁹⁾によって改正された。この追加議定書は、所定の要件を満たした2004年7月1日に

(37) この点については、夏井高人「手続的正義—情報社会における社会構造の変化と正義の維持」法とコンピュータ23号49～51頁で論じた。

(38) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108> [2016年9月23日確認]

(39) Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows

<https://www.coe.int/web/conventions/full-list/-/conventions/treaty/181> [2016年9月23日確認]

発効した。この追加議定書により、監督官（行政機関）を独立の行政機関とすること、及び、第三国への個人データの移転について、当該第三国が個人データ保護条約 **ETS No.108** に定めるのと均等の法的保護を与えていることを条件とすることが定められた⁽⁴⁰⁾。

個人データ保護条約 **ETS No.108** は、1980 年に起草され、1981 年に締結された古い法規範である。しかし、この条約で採用された新たな法概念や条項上の表現は、その後の関連指令や規則等にもそのまま踏襲されている場合が多い。また、既存の国際条約等から借用された表現や条項等については、個人データ保護条約 **ETS No.108** の説明書の中でその旨が解説されている。これらのことから、この説明書は、関連する概念や表現の起源・由来を知るという法情報学上の調査目的のためには極めて重要な資料の 1 つとなっている。ただし、後の時代に制定された指令や規則において、個人データ保護条約 **ETS No.108** と同一またはほぼ同じ表現が踏襲されている場合、時代背景や社会背景が異なっているため、1980 年代であれば容易に理解できたことであっても、その後の時代においては何を意味するのか不明となってしまうものもある。そのような場合でも、語や表現の起源を知ることにより、どのように修正して読み理解すべきかを正しく認識することができる。

個人データ保護条約 **ETS No.108** は、公的部門と民間部門の両方に対して適用がある。しかしながら、日本国の法制においては、行政機関個人情報保護法によって全面改正された行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律（昭和 63 年法律第 95 号・以下「昭和 63 年行政機関個人情報保護法」という。）のモデルとなっていると理解することができる。

行政機関個人情報保護法及び昭和 63 年行政機関個人情報保護法は、公的部門に適用されるが、民間部門には適用されない。行政機関個人情報保護法及び昭和 63 年行政機関個人情報保護法には個人データ保護条約 **ETS No.108** の追加議定書 **ETS No.181** による一部改正は反映されていないため、独立した行政機関としての個人データ保護監督官の制度は導入されていない⁽⁴¹⁾。

今後、欧州の個人データ保護法制を研究する場合には無論のこと、日本国の法制

(40) これは、同条約を後述の個人データ保護指令 95/46/EC における基本的な法的枠組みと一致する内容のものとするための改正である。

(41) この点に関しては、行政機関個人データ保護規則参考訳の中で詳論したとおりである。

との比較法的な研究を行う場合、あるいは、OECDのプライバシーガイドライン（1980年9月23日）⁽⁴²⁾やその改訂版であるプライバシーフレームワーク（2013年6月11日）⁽⁴³⁾との関係に関する研究を行う場合においても、個人データ保護条約ETS No.108及び同条約と関連する様々な法律文書に関する研究が深められるべきである。

2. 2. 2 個人データ保護指令95/46/EC

個人データ保護指令95/46/ECは、1995年10月24日に欧州議会において議決され、1995年11月23日にEC官報（Official Journal of the European Communities）で公示された。

この個人データ保護指令95/46/ECは、民間部門と公的部門の両方に適用されるものとして制定されたが、指令（Directive）という法形式を採用しているため欧州共同体（欧州連合）の機関及び構成国に対する直接的な効力を有する法規範ではない。一方では、欧州共同体（欧州連合）が法的行為（legal acts）や実装行為（implementation acts）によってそれを実装することにより、指令に定める規範内容が欧州共同体（欧州連合）の機関において直接的な効果を発生させ、他方では、構成国が自国の制定法（国内法）を各国の議会の議決によって制定し、それを実装することによって、指令に定める規範内容が構成国において直接的な効果を発生させるという論理構造を有している⁽⁴⁴⁾。

(42) OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

<http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprivacyandtransborderflowsofpersonaldata.htm> [2016年9月23日確認]

(43) The OECD Privacy Framework

<http://www.oecd.org/sti/ieconomy/privacy.htm> [2016年9月23日確認]

(44) 指令（Directive）という法形式は、直接的効力（self-execution）を有しないという点では直接的な効力を有しない条約と同じである。しかし、条約が国際合意であり、国家間の契約の一種であるのに対し、指令は、欧州議会の議決によって制定される法規範の一種であって、それ自体として契約（合意）とは異なる性質を有している。可決された指令は、構成国を拘束し、構成国は、指令に定めるのと均等な法令を制定して直接的に適用可能な法規範を形成すべき義務を負う。欧州連合それ自体としては、実装行為（implement acts）や委任行為（delegated acts）によって欧州連合の機関等に直接的な効力を生じさせる法規範を形成しなければならない。これらの行為は、法的行為（legal acts）とも呼ばれる。要するに、法規範制定行為のことを指す。現実には、欧州委員会の決議等によってその実装行為が行われる。

個人データ保護指令 95/46/EC は、その後の日本国の個人情報保護法制に対して大きな影響を与え、平成 15 年における行政機関個人情報保護法による昭和 63 年行政機関個人情報保護法の全面改正、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。）及び独立行政法人等の保有する個人情報の保護に関する法律（平成 15 年法律第 59 号・以下「独立行政法人個人情報保護法」という。）の制定を促した⁽⁴⁵⁾。これは、同指令の第 25 条及び第 26 条に定める第三国に対する個人データの移転の制限が日本国の産業界にも大きな影響を与えると考えられたためである。

個人データ保護指令 95/46/EC の前文(9)には、プライバシーの権利と情報の自由との間の調整ないし整合性の確保について、「各国が近似する法律をもてば、その保護の均等性の結果として⁽⁴⁶⁾、構成国は、個人の権利と自由とりわけプライバシーの権利の保護と関連する理由によって構成国間における個人データの自由な移転を禁止することができなくなることであろう」と述べられている。

しかし、日本国においては、個人データの「自由な移転 (free movement)」との部分だけが文脈とは無関係に切り取られ、身勝手な解釈の下に「利活用」と称して商業利用のために濫用される傾向が強く、極めて遺憾なことである。個人データ保護指令 95/46/EC の前文の各所において何度も繰り返し述べられているように、「自由な移転」だけが独立して価値を有するのではなく、プライバシーの権利と情報の自由とを調和させ、整合性を保つことに力点があるので、これら 2 つの権利及び自由は常に対になったものとして理解し、そのように解釈し、そのように表現しなければならない。

この第三国に対する個人データの移転に関する制限は、同指令が指令 (Directive) という法形式を採用していることから、構成国の立法裁量によって個人データ保護のための規律の具体的内容及びその手続が区々になってしまった部分がある。これは、構成国の立法権それ自体には干渉しない指令という法形式を採用した以上、

(45) 地方自治体のレベルでは、各地方自治体において個人情報保護条例が制定された。地方自治体の個人情報保護に関しては、夏井高人・新保史生『個人情報保護条例と自治体の責務』（ぎょうせい、2007）で詳論した。

(46) [訳注] 構成国の完全に独立した立法権の行使による「プライバシーの権利が情報の自由か」という二者択一的な立法政策論ではなく、両者の調和または整合性を確保するための新たな法的枠組みが必要であるという共通認識を反映する趣旨と解される。

不可避のことである。

そのため、一般個人データ保護規則 GDPR では、その点に関する反省点が率直に述べられている⁽⁴⁷⁾。そして、そのような認識に基づき、欧州連合の規則 (Regulation) という直接的に効力のある法形式を採用した⁽⁴⁸⁾。同規則では、個人データの第三国移転に関する制限と十分性の要件についても、より詳細かつ強力な条項が設けられている。

2. 2. 3 行政機関個人データ保護規則 (EC) No 45/2001

行政機関個人データ保護規則 No 45/2001 は、欧州共同体設立条約 (The Treaty

(47) 一般個人データ保護規則 GDPR の前文 (9) 及び (10) 参照。とりわけ、前文 (9) には、「指令 95/46/EC の目的及び諸原則は、今なお有効である。しかし、この指令は、欧州連合内における個人データ保護の実装における非整合性、法的な不確実性、そして、とりわけオンラインの行為に関して自然人の保護に対する重大なリスクがあるという一般的な認識が拡散することを防止できなかった」とある。私見としては、オンラインの行為について重大なリスクが存在することは事実であり、制定された一般個人データ保護規則 GDPR (特に第 17 条の「忘れられる権利」や第 22 条の自動的なプロファイリングのみに基づく人格的側面の判定を拒絶する権利の導入) によってもそのリスクを低減することは困難であると考ええる。今後は、アメリカ合衆国、中華人民共和国及びロシアを含む世界の主要各国を法的に拘束する条約によって、自動的なプロファイリング、ロボットク及びその他の人工知能技術の応用に関するものを含め、ある状況下においては、ある類型に属する企業活動それ自体を全面禁止し、または、そのための手法それ自体を全面禁止するという方向へと進まざるを得ないであろう。

(48) 一般個人データ保護規則 GDPR の前文 (104) ないし (108)、第 45 条参照。日本国政府や日本国の関連する経済団体等では、一般個人データ保護規則 GDPR の草案の段階から調査研究を重ねてきており、それなりの見通しの下に、近時における個人情報保護法、行政機関個人情報保護法及び独立行政法人個人情報保護法の改正がなされた。しかし、それらの検討結果は必ずしも十分なものとは言えず、欧州における立法の見通しもかなり甘いものとなっていたと評価せざるを得ない (関連文献は、行政機関個人データ保護規則参考訳及び一般個人データ保護規則参考訳の各冒頭で示したとおりである)。結論的には、個人情報保護法、行政機関個人情報保護法及び独立行政法人個人情報保護法の 3 つの法律について、更に徹底した法改正 (特に個人情報保護委員会の権限強化と独立予算の確保) が必要である。なお、この間の時期における調査研究結果に基づくものとしては、堀部政男・鈴木正朝・石井夏生利・岡村久道・高野一彦・新保史生・松前恵環・小向太郎『プライバシー・個人情報保護の新課題』(商事法務、2010)、石井夏生利『個人情報保護法の現在と未来』(勁草書房、2014) がある。平成 27 年の個人情報保護法の改正に関する解説書としては、瓜生和久『一問一答 平成 27 年改正個人情報保護法』(商事法務、2015)、日置巴美・板倉陽一郎『平成 27 年改正個人情報保護法のしくみ』(商事法務、2015) がある。改正法の問題点を指摘するものとしては、新保史生「改正個人情報保護法の論点」憲法研究 48 号 29～55 頁がある。

on the establishing the European Community)⁽⁴⁹⁾ の第 286 条第 1 項を実装するために制定された。行政機関個人データ保護規則 No 45/2001 は、2000 年 12 月 18 日に欧州議会で議決され、2001 年 1 月 12 日に EC 官報で公示され、2001 年 2 月 1 日に発効（施行）となった。

行政機関個人データ保護規則 No 45/2001 の適用対象は、主として、欧州共同体（欧州連合）の行政機関（the institutions and bodies set up by, or on the basis of, the Treaties establishing the European Communities）である（同規則第 1 条）。この規則は、その内容面において、個人データ保護指令 95/46/EC を公的部門（public sector）において実装するための法令であると理解することができる⁽⁵⁰⁾。この規則は、民間部門（private sector）には適用されない。民間部門に適用される規則は、2016 年 4 月 27 日に制定された一般個人データ保護規則 GDPR である。

同条約第 286 条第 1 項は、「1999 年 1 月 1 日以降、この条約により、または、この条約に基づいて、個人データの処理と関連する個人の保護及び個人データの自由な移転に関する欧州共同体の行為が欧州共同体の機関及び組織に対して適用される」と規定している。ここでいう「欧州共同体の行為（Community acts）」とは、欧州共同体の法規範制定行為のことを指し、欧州連合設立以降においては「法的行為（legal acts）」と呼ばれているものと同じである⁽⁵¹⁾。

行政機関個人データ保護規則 No 45/2001 の前文(1)は、「条約の第 286 条は、欧州共同体の機関及び組織に対して、個人データの処理と関連する個人の保護及び個人データの自由な移転に関する欧州共同体の行為を適用することを求めている」と

(49) 「旧 EC 条約」とも呼ばれる。この条約は、欧州連合を設立するためのリスボン条約（The Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community）の発効により失効した。

(50) 個人データ保護指令 95/46/EC は、直接適用される法的効果を有しないのに対し、行政機関個人データ保護規則 No 45/2001 は直接適用される法的効果を有する。その意味で、行政機関個人データ保護規則 No 45/2001 は、個人データ保護指令 95/46/EC の特例ではない。欧州共同体（欧州連合）の公的部門における個人データ保護指令 95/46/EC の実装である。

(51) 「法律行為」と訳す例もある。権力組織である法人としての欧州連合の法律行為として理解することは可能であるが、民法上の法律行為とは異なるので、混同を避けるため、「法行為」との訳を採用せず、「法的行為」と訳すことにしている。他方、「法行為」と訳す例もある。しかし、「法行為」では、日本語として何を意味するのか理解し難いという問題がある。また、法規範制定行為は、法令としての立法行為と行政機関の規則制定行為を含むものなので、「立法行為」または「法律制定行為」のみを意味するものではない。

述べている⁽⁵²⁾。また、同規則第1条は、「欧州共同体の機関及び組織は、この規則に従い、自然人の基本的な権利及び自由、とりわけ個人データの処理と関連するプライバシーの権利を保護しなければならない、かつ、欧州共同体の機関及び組織の間または指令95/46/ECを実装する構成国の自国の法律に従う取得者に対する個人データの自由な移転を制限または禁止してはならない」と規定している。

この第1条の論理構造を検討すると、「プライバシーの権利を尊重すること」を確保し、かつ、「個人データの自由な移転を禁止しないこと」を確保することが規範内容として示されている。この両者の法的要求が同時に成立するようにしなければならないので、プライバシーの権利のみを保護して情報の自由を制限することはできないし、かつ、情報の自由だけを優先してプライバシーの権利の保護を放棄または犠牲にすることもできない。その両者の調和または整合性の確保が求められるなければならない。

行政機関個人データ保護規則 No 45/2001 は、欧州連合の行政機関の間での相互協力や欧州連合内での一貫性のある規則の適用を目的として、欧州連合の独立の機関として、欧州連合個人データ保護監督官（European Data Protection Supervisor）を設置するものとしている（同規則第41条）。

なお、TFEUが定める補完性原則との関係から、欧州連合の構成国の公的部門に適用される個人データ保護法に関しては、別途調査研究されなければならない。従来、個別的で断片的な調査結果は存在するが、欧州連合の構成国全部についての比較法的な検討結果は存在しない。EU法その他の関連学会において、今後の最重要課題の1つとして、この分野における法情報学的研究及び比較法的研究が強力に推進されることを期待する。

2. 2. 4 一般個人データ保護規則 (EU) 2016/679

一般個人データ保護規則 GDPR は、2016年4月27日に欧州議会で議決され、2016年5月4日にEU官報（Official Journal of the European Union）で公示された。発効（施行）の日は、2018年5月25日である。

一般個人データ保護規則 GDPR は、主として、民間部門における自然人の個人

(52) この欧州共同体設立条約第286条第1項の条文と行政機関個人データ保護規則 No 45/2001の前文(1)の文言を比較してみると、前文(1)は条約第286条第1項をそのまま引用しているのと同じであることを理解することができる。

データの自動的な処理について適用される（同規則第 2 条第 1 項）。公的部門については、行政機関個人データ保護規則 No 45/2001 が適用されるため、一般個人データ保護規則 GDPR が適用されない（同規則第 2 条第 3 項）。また、特に經由プロバイダの責任に関して、電子商取引指令 2000/31/EC⁽⁵³⁾ の法的効力が維持される（同規則第 2 条第 4 項）。同様に、プライバシー及び電子通信指令 2002/58/EC の法的効力が維持される（同規則第 95 条）。しかし、個人データ保護指令 95/46/EC は、2018 年 5 月 25 日に廃止となる（同規則第 94 条第 1 項）⁽⁵⁴⁾。

一般個人データ保護規則 GDPR の第 1 条第 2 項は、「この規則は、自然人の基本的な権利及び自由、並びに、とりわけ個人データの保護に関する彼らの権利を保護する」と規定している。また、同条第 3 項は、「欧州連合内における個人データの自由な移転は、個人データの処理と関連する自然人の保護と関係する理由のゆえに制限されることも禁止されることもない」と規定している。

同条第 2 項及び第 3 項に分けて定められている点は、行政機関個人データ保護規則 No 45/2001 の第 1 条において同一の条項内で定められていることと相違しているが、内容的には同じ趣旨のものと解すべきである。従って、一般個人データ保護規則 GDPR の第 1 条第 2 項と同条第 3 項は独立して存在しているのではなく、第 2 項が規定するプライバシーの権利を保護すると同時に、個人データの自由な移転を保障しなければならないのである。その両者の調和または整合性を確保することが重要である。そのために、一般個人データ保護規則 GDPR においては、個人データの移転について、原則として、安全性確保措置が講じられていることを絶対条件としている⁽⁵⁵⁾。プライバシーの権利を保護する措置による安全保障のない個人データの移転は、原則として、認められない。

(53) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:HTML> [2016 年 9 月 24 日確認]

(54) 個人データ保護指令 95/46/EC との関係は、行政機関個人データ保護規則 No 45/2001 の場合と同様であり、一般個人データ保護規則 GDPR は、個人データ保護指令 95/46/EC の特則ではない。同規則は、同指令の民間部門における実装である。

(55) 一定の要件を満たす場合には、例外的扱いが認められる。その例外の解釈及び問題点の詳細については、一般個人データ保護規則参考訳で述べた。

一般個人データ保護規則 GDPR は、構成国が個人データ保護のための職務を遂行する責任と権限を有する独立の行政機関である監督官（supervisory authority）を設置し（同規則第 51 条）、これら構成国の監督官の間での相互協力や欧州連合内での一貫性のある規則の適用を目的として、欧州連合の独立の機関として、欧州連合個人データ保護委員会（European data protection board）を設置するものとしている（同規則第 68 条）。

公的部門における独立の行政機関である監督官の最上位の機関として欧州連合個人データ保護監督官（European Data Protection Supervisor）が設置されているのに対応して、民間部門における独立の行政機関である監督官の最上位の機関として欧州連合個人データ保護委員会（European data protection board）が設置される。

なお、欧州連合の機能に関する条約（TFEU）の定める補完性原則との関係から、一般個人データ保護規則 GDPR は、欧州連合の構成国の行政機関が行う自然人の個人データの自動的な処理には適用されない（同規則第 2 条第 2 項 (b)）。この関係においても、構成国の公的部門における個人データ保護法制に関する法情報学的または比較法的な研究が尽くされなければならない。

2. 2. 5 ネットワーク及び情報システムの安全性に関する指令 (EU) 2016/1148

NIS 指令案として審議を続けてきた欧州議会は、2016 年 6 月 6 日、ネットワーク及び情報システムの安全性に関する指令⁽⁵⁶⁾を可決した⁽⁵⁷⁾。この指令は、2016 年 7 月 19 日に EU 官報で公示され、同日、発効（施行）となった（同指令第 29 条）。

ネットワーク及び情報システムの安全性に関する指令は、欧州連合のネットワークシステム及び情報システムの一貫性のある安全性確保を目的とするものである。ここでいう「ネットワークシステム」とは、主として、官民の重要インフラと関連するネットワークシステム（特に行政機関が監督する重要インフラのネットワーク

(56) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

<http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN> [2016 年 9 月 24 日確認]

(57) ネットワーク及び情報システムの安全性に関する指令の全訳は、法と情報雑誌 1 巻 2 号 34～73 頁にある（以下「ネットワーク及び情報システムの安全性に関する指令参考訳」という。）。ただし、本稿により、訳語の一部を改める。

システム)のことを指し、情報システムとは、主として、民間企業が運営する広域のネットワークシステム(特にクラウドコンピューティングサービス)のことを指す⁽⁵⁸⁾。これらのシステムの運営者(管理者)は、情報セキュリティ上のリスクやインシデントについて通知義務を負い、それぞれの管理するシステムの安全性を確保するための防護措置を講ずる義務を負うほか、欧州連合のENISA(European Network and Information Security Agency)や構成国のCSIRT(NIS指令案の段階ではCERT)と連携して、相互に密接に連絡を取り合い、欧州連合内での共同の防護策としての模擬攻撃演習等に参加することが定められている。

ネットワーク及び情報システムの安全性に関する指令の前文(63)は、「多くの場合において、インシデントの結果として個人データが被害を受ける。この文脈においては、職務権限を有する監督官⁽⁵⁹⁾とデータ保護監督官⁽⁶⁰⁾は、インシデントから生ずる個人データ侵害に対抗するための関連する全ての事柄について協力し、かつ、情報交換をしなければならない」と述べ、同指令の第8条第6項は、「職務権限を有する監督官及び単一連絡場所は、それが適切であり自国の法令に基づくものであるときは、自国内の関連法執行機関及び個人データ保護監督官と協議し、これらと共同活動をしなければならない」と規定している。ここでいう「単一連絡場所(single point of contact)」とは、物体としての場所のことではなく、一元的な連絡を確保するための行政機関または官署のことを意味する。

要するに、欧州連合における個人データ保護の法的枠組みは、原則として、コンピュータによって自動処理される個人データの保護を目的とするものであるので、コンピュータシステム及び電子データの技術的側面における保護を主眼とするネットワーク及び情報システムの安全性に関する指令に基づく様々な活動は、個人

(58) もともとの概念は、欧州評議会のサイバー犯罪(ETS No.185)に対応する情報システムに対する攻撃及び欧州委員会枠組み決定2005/222/JHAの改正に関する欧州議会及び欧州連合理事会の2013年8月12日付指令2013/40/EUの第2条(a)にも見られるが、より明確には、NIS指令案の中で示されている。指令2013/40/EUの翻訳(前文を除く)及びNIS指令案の全訳は、法と情報雑誌1巻1号に収録されている。

(59) ネットワーク及び情報システムの安全性に関する指令参考訳では「competent authorities」を「担当官庁」と訳したが、「職務権限を有する監督官」と改める。構成国の監督官のことを指す。

(60) ネットワーク及び情報システムの安全性に関する指令参考訳では「data protection authorities」を「データ保護庁」と訳したが、「データ保護監督官」と改める。欧州連合の監督官のことを指す。

データの法的側面における保護を主眼とする個人データ保護監督官の業務と関連性をもたざるを得ないのである。そして、欧州連合における一貫性のある保護を達成するためには、監督官自身による異議の処理や行政監督権の行使及び裁判所による判断を含む法的な対処（これは、個人データ保護法制による。）だけではなく、情報システムの安全性を確保するための組織的な仕組みとの連携により、技術的な対処（これは、ネットワーク及び情報システムの安全性に関する指令の枠組みに従う。）にも従事すべきことになる。

法執行機関（警察）との連携に関しては、ネットワーク及び情報システムの安全性に関する指令、行政機関個人データ保護規則 No 45/2001 及び一般個人データ保護規則 GDPR の全ての中にそれと関連する条項が存在する。

このように独立の行政機関である個人データ保護監督官は、国家安全保障や国防と関連する部分を含め、情報セキュリティ関連の行政機関や法執行機関（警察）とも連携してその職務を遂行しなければならない。換言すると、個人データ保護監督官は、単なる人権擁護機関ではない。

他方において、一般個人データ保護規則 GDPR の中では、様々な場面で、安全性確保措置（Safeguards）について規定されている。この安全性確保措置は、契約や行政規則を含め法的なものを含むので、物体としての何らかの防護措置を施す場合だけを指すものではないが、情報セキュリティと関係する部分では物的な防護措置や情報セキュリティ専門家の配置等の組織的な対応を意味することもある。そして、個人データ保護監督官は、そのような技術的または組織的な安全性確保措置の適否についても判断し、必要に応じて適切に行政措置を講じなければならない。このような場面において監督官として行動する者にはそのような職務遂行能力が求められることになる。

加えて、一般個人データ保護規則 GDPR 第 37 条ないし第 39 条の定める個人データ保護責任者（data protection officer）は、情報セキュリティの専門家であることが要求されるところ、個人データ保護監督官は、その個人データ保護責任者に対する監督業務も遂行しなければならない。このことから、監督官及び安全性確保措置の本質を理解するためには、それ自体として関連する条項を検討するだけではなく、ネットワーク及び情報システムの安全性に関する指令やサイバー犯罪と関連する指令や規則等の中に規定されている条項についても網羅的な検討を要する

ことになる。

欧州連合における個人データ保護の組織構造を正確に認識・理解するためには、ここまで述べてきたような情報セキュリティ組織との関係についても十分に注意を払いながら総合的な考察をしなければならない。従来の法学研究においては、この点に関する視点が欠落していたか、または、非常に希薄であったと評価せざるを得ないので、特に銘記すべき事柄である⁽⁶¹⁾。

2. 2. 6 欧州における個人データ保護のための法制度全体の関係

以上を踏まえ、法制の変化の概要をまとめると、以下のとおりとなる。

1980年～1995年における個人データ保護のための法制度は、個人データ保護条約 ETS No.108 及びこれに基づく構成国の法令のみが存在しており、民間部門及び公的部門の両者について同条約が適用されていた。

1995年～2001年における個人データ保護のための法制度は、従前の個人データ保護条約 ETS No.108 の適用を残したままで、民間部門及び公的部門ともに、個人データ保護指令 95/46/EC 及びこれに基づく構成国の法令が適用されていた。

2001年～2016年における個人データ保護のための法制度は、民間部門については従前のままであるが、欧州共同体（欧州連合）の行政機関に関しては、行政機関個人データ保護規則 No 45/2001 及びこれに基づく構成国の法令が適用されることとなった。

2016年～2018年における個人データ保護のための法制度は、一般個人データ保護規則 GDPR の施行準備時期であるため、従前と同じである。ただし、個人データ保護指令 95/46/EC に基づいて講じられた措置に関しては、その法的効力を維持するものの、措置の細部の解釈については一般個人データ保護規則 GDPR に定めるところに従ってなされる可能性がある。とりわけ、欧州司法裁判所（Cour de justice des Communautés européennes）及び欧州人権裁判所（Cour européenne des droits de l'homme）の判例法となる裁定や判決では、そのような解釈傾向が顕著となる可能性が高い。

そして、2018年5月25日以降は、個人データ保護指令 95/46/EC が廃止され

(61) 脅威に対する対応に関して、法的な対応、技術的な対応及びマネジメントによる対応の長所と短所については、夏井高人監修『IT ビジネス法入門—デジタルネットワーク社会の法と制度』（Tac 出版、2010）263～265 頁で述べた。

る。その結果、欧州個人データ保護条約 ETS No.108 の関係は従前のままとしながら、民間部門については一般個人データ保護規則 GDPR 及びこれに基づく構成国の法令が適用され、公的部門については行政機関個人データ保護規則 No 45/2001 及びこれに基づく構成国の法令が適用される⁽⁶²⁾。理論的には、全ての部面において個人データ保護法制が実装されたことになると考えられる⁽⁶³⁾。この2018年5月25日以降の法適用関係の概略を図示すると、図1のとおりとなる。

	欧州連合	構成国
公的部門（行政機関）	行政機関個人データ保護規則 No 45/2001	構成国の法令
民間部門	一般個人データ保護規則 GDPR	

図1：2018年5月25日以降における法適用関係

加えて、ネットワーク及び情報システムの安全性に関する指令(EU) 2016/1148との関連において、個人データ保護監督官は、法的な面で個人データ保護に関する職務権限を行使するだけでなく、国家安全保障や国防が関係する事項を含め、情報セキュリティとの関連でも欧州委員会及びENISAと連携して重要な役割を担うことになる⁽⁶⁴⁾。

2.3 行政機関個人データ保護規則への反映

以上を踏まえ、欧州連合（欧州共同体）の個人データ保護法制において保護法益とされているプライバシーの権利及び情報の自由が、行政機関個人データ保護規則 No 45/2001 中では具体的にどのようなかたちで反映されているのかについて検討する。

「個人データの処理と関連する個人の保護及び個人データの自由な移転」との表現は、個人データ保護指令 95/46/EC の標題「個人データの処理と関連する個人の

(62) 欧州連合と構成国との間の国家上の権限分配に関しては、中西優美子『EU権限の法構造』（信山社、2013）及び同『EU法』（新世社、2012）が参考になる。

(63) 自動処理されない個人データや小規模事業者による個人データ処理等のように、厳しい法的規制を加える必要がないとされている領域について空白が存在することは、立法者によって予定されていることである。

(64) 日本国の個人情報保護委員会に関しては、少なくとも法律上の権限分配を考察する限り、このような情報セキュリティ関連の情報共有と関連する職務権限はない。

保護及び個人データの自由な移転に関する」をそのまま承継するものである。

個人データ保護指令 95/46/EC の前文(1)は、「平和と自由を維持・強化し、構成国の憲法及び法律並びに欧州人権条約によって認められている基本的な権利を基盤とする民主主義を促進し」と述べた上で、前文(2)において、「データ処理システムは、人間に奉仕するために設計されている。そして、自然人の国籍及び居住地とは無関係に、自然人の基本的権利及び自由、特にプライバシーの権利が尊重されなければならない、そして、それは、経済と社会の発展、取引の拡大及び個人のより良い生活に寄与するものでなければならない」と述べている。

これらの価値観は、既述の個人データ保護条約 ETS No.108 の中で個人データ保護法制における保護法益とされているものと実質的に同じである。そして、同指令の前文(11)は、「この指令に含まれている個人の権利及び自由、とりわけプライバシーの権利の保護という原則は、個人データの自動的な処理と関連する個人の保護のための 1981 年 1 月 28 日の欧州評議会条約に含まれているものに従うものであり、かつ、これを増強するものである」と述べている。この文言から、個人データ保護指令 95/46/EC は、個人データ保護条約 ETS No.108 が定めているプライバシーの権利と情報の自由の尊重という基本的な価値観を承継し、これを堅持するものとして理解することができる。そして、その価値観は、前述の欧州共同体設立条約第 286 条第 1 項を介して行政機関個人データ保護規則 No 45/2001 に承継されている。

すなわち、プライバシーの権利及び情報の自由は、個人データ保護指令 95/46/EC 及び欧州共同体設立条約第 286 条第 1 項を介して行政機関個人データ保護規則 No 45/2001 の中に盛り込まれ、同規則における個人データ保護の真の保護法益として定められていると解すべきである。

行政機関個人データ保護規則 No 45/2001 における「個人データの処理と関連する個人の保護」とは、理念的には、「個人のプライバシーの権利の保護」と同じであり、また、「個人データの自由な移転」とは、「情報の自由」と同じである。そして、「プライバシーの権利（個人データ処理と関連する個人の保護）」及び「情報の自由（個人データの自由な移転）」の両者について、既述のような制限があることから、それらは、無制約な権利及び自由としては認められていない。

3 個人データ保護の基本原則

3.1 原則

3.1.1 欧州評議会閣僚委員会の決議

欧州における個人データの法的保護のための最初の法規範となった欧州評議会の個人データ保護条約 ETS No.108（1981年）は、欧州評議会の閣僚委員会決議第22号（1973年）及び同決議第29号（1974年）に示された基本指針に基づき起草された。

閣僚委員会の第22号決議は、民間部門におけるプライバシー保護と関連するものである。その別紙（ANNEX）には、以下のとおりに基本的な指針が記載されている⁽⁶⁵⁾。

1. 記録保存される情報は、正確なものでなければならず、かつ、最新の状態に保たなければならない。
一般に、個人の親密な私生活に関する情報または不当な差別をもたらすかもしれない情報は、記録保存してはならず、もし記録保存する場合には、他に伝達してはならない。
2. 情報は、それが記録保存される目的との関連において適切なものであり、かつ、関連性を有するものでなければならない。
3. 情報は、詐欺その他の不正な手段によってこれを取得してはならない。
4. 一定の類型に属する情報については、その保管または利用の期限を指定する規則が定められなければならない。
5. 適切な承認がない場合には、情報は、それが記録保存された時の目的とは異なる目的のために利用されてはならず、かつ、第三者に対して伝送されてはならない⁽⁶⁶⁾。

(65) 閣僚委員会決議第29号は、公的部門における個人データ保護に関するものである。その別紙（ANNEX）には、多少の表現の相違はあるものの、決議第22号とほぼ同内容の原則が記載されている。

(66) [訳注] 一般に、個人データの目的外利用と第三者提供とは異なる出来事であると理解されている。しかし、特段の事情のない限り、当該個人データの当初の取得者が有していた当該個人データの処理の目的は、当該取得者のためのものであるはずであり、第三者のた

6. 一般原則として、関係する者は、彼に関して記録保存されている情報、それが記録保存される目的及びその情報の個々の開示の詳細について知る権利を有する。

7. 不正確な情報を正確なものとするため、及び、利用が終了した情報または違法な方法で取得された情報を削除するために、全ての手立てが講じられなければならない。

8. 情報の侵害または濫用に対して、注意が払われなければならない。

電子的なデータベースは、当該情報を入手する権限を有しない者がデータベースによって保持されているデータにアクセスすることができない情報システム、及び、意図的なものであるか否かを問わず、情報の誤伝達を検出する情報システムを装備するものでなければならない。

9. 記録保存された情報へのアクセスは、その情報を知ることについて正当な理由を有する者だけに限定されなければならない。

電子的なデータベースの運用従業者は、データの濫用を避けるための行動規則及び特に職業上の守秘義務に関する規則によって拘束されるものとしなければならない。

10. 統計データは、集計結果の形態の場合においてのみ、及び、その情報を特定の者と連結することが不可能な方法による場合においてのみ、これを開示することができる。

3. 1. 2 個人データ保護条約 ETS No.108 第 5 条

欧州評議会閣僚委員会の決議に示された基本原則は、以下のとおり、個人データ保護条約 ETS No.108 の第 5 条（データの品質（Quality of data））として条文化された。

自動的に処理される個人データは：

- a 公正かつ適法に取得され、処理されなければならない；
- b 特定の適法な目的で記録保存されなければならない、かつ、その目的と適

めのものではないから、第三者に対する提供は、それだけで当初の目的に反する行為であると評価することは可能である。それゆえ、第三者提供について改めて本人の同意を得るということは、別の目的による処理について同意を得ることと実質的にみて同義となる。

合しない方法で利用してはならない；

c それ記録保存される目的との関係において、十分であり、関連性があり、かつ、過剰ではないものとしなければならない；

d 正確なものでなければならず、必要があるときは、最新の状態のものとしなければならない；

e そのデータを記録保存する目的のために必要がある期間内に限り、データ主体の識別を許容する方式で維持されるものとしなければならない。

第5条の(a)は、OECDのガイドライン（1980年9月23日）⁽⁶⁷⁾にある収集制限の原則（**Collection Limitation Principle**）とほぼ同旨である。同原則は、「個人データの収集は制限されなければならない。いかなる個人データの収集も適法かつ公正な手段によらなければならない。かつ、それが適切なときは、データ主体に周知し、または、その同意を得て収集しなければならない」と定めている。

第5条の(b)は、OECDガイドラインの目的の特定の原則（**Purpose Specification Principle**）とほぼ同旨である。同原則は、「個人データが収集される目的は、遅くともデータ収集の時点までに特定されなければならない。収集の後の利用は、当該目的及び個々の目的の変更の度に指定された目的を満たすものであり、かつ、当該目的と適合する範囲内に限定されなければならない」と定めている。

第5条の(c)及び(d)は、OECDのガイドラインにあるデータの品質の原則（**Data Quality Principle**）とほぼ同旨である。同原則は、「個人データは、それが用いられる目的と関係するものであり、かつ、その目的のために必要な範囲内のものとならなければならない。かつ、正確であり、完全であり、最新のものとされていなければならない」と定めている。

以上から、欧州評議会における個人データ保護条約ETS No.108の起草者とOECD理事会におけるガイドライン起草者との間で完全な共通認識と相互承認が得られていたということを知ることができよう⁽⁶⁸⁾。

(67) 堀部政男／一般財団法人日本情報経済社会推進協会（JIPDEC）編・アン・カブキアン（JIPDEC 訳）『プライバシー・バイ・デザイン—プライバシー情報を守るための世界的新潮流』（日経BP社、2012）、堀部政男・新保史生・野村至『OECD プライバシーガイドライン—30年の進化と未来』（JIPDEC、2014）が参考になる。

(68) 欧州評議会の個人データ保護条約ETS No.108とOECDのガイドラインとの関係に関

第 5 条の (e) に関しては、欧州評議会の個人データ保護条約 ETS No.108 が締結された 1980 年代当時の記録媒体の主流が磁気テープまたは磁気ディスクパックであり、紙テープやパンチカードもまだ使用されていた時代であった。このような時代背景ないし技術水準を考慮に入れないと、第 5 条の (e) の合理的な解釈が困難であるようにも読める。この点について、OECD のガイドラインの策定過程で用いられている語句に着目した文案の変化に関する研究結果⁽⁶⁹⁾によれば、この第 5 条の (e) は、過渡的で中途半端な文言のまま、欧州評議会によって採択されてしまい、その後も踏襲されているものである可能性がある。他方において、OECD のガイドラインでは、個人データ保護条約 ETS No.108 の第 5 条の (e) に相当する文言を含む文案が最終的には廃棄されてしまったようである。

このように、個人データ保護条約 ETS No.108 の第 5 条 (e) については検討の余地があるとはいえ、全体としてみると、同条に定める基本原則がその後の個人データ保護法制の骨格をほぼ決定づけることになったと考えられる。

3. 1. 3 個人データ保護指令 95/46/EC 第 6 条

個人データ保護指令 95/46/EC の第 6 条（データの品質と関連する諸原則）は、以下のとおり、個人データ保護条約 ETS No.108 の規定を基礎としつつも、データ保護の基本原則について更に細かく規定している。

1. 構成国は、個人データが以下のようにすべきものと定めなければならない：
 - (a) 公正かつ適法に処理されなければならない；
 - (b) 特定され、明示であり、適法な目的で収集されなければならない、かつ、これらの目的と適合しない方法で別の目的により処理されてはならない。歴史調査、統計または科学調査のための別の目的による処理は、構成国が適正な安全性確保措置を定めている場合には、目的と適合しないものとみなしてはならない；

しては、従来、必ずしも十分な検討がなされてきたとは言えない状況にあった。今後は、関連する他の分野における立法史も含め、急激に電子化ないし情報化が進んだ時代の立法の変化に関する総合的な研究が尽くされるべきである。

(69) Normann Witzleb, David Lindsay, Moira Paterson & Sharon Rodrick (Eds.), *Emerging Challenges in Privacy Law: Comparative Perspectives*, Cambridge University Press (2014) pp.306–307

(c) それが集められる目的または別の目的により処理される目的との関係において十分であり、関連性があり、かつ、過剰ではないものでなければならない；

(d) 正確であり、かつ、それが必要なときは、最新のものとしなければならない。それが集められる目的または別の目的により処理される目的との関係を考慮に入れ、不正確または不完全なデータが消去または訂正されることを確保するための全ての合理的な手立てが講じられなければならない；

(e) データが集められる目的またはそれを別の目的で処理する目的のために必要となる期間内に限り、データ主体を識別することができる方式で保存するものとしなければならない。構成国は、歴史、科学または統計の利用のための期間内に限り記録保存される個人データについて、適切な安全性確保措置を定めなければならない。

2. 管理者は、第1項の遵守を確保しなければならない。

欧州共同体（欧州連合）の構成国は、この第6条が定めるところに準拠して、各国の個人データ保護法を制定した。

3. 1. 4 行政機関個人データ保護規則 No 45/2001 第4条

行政機関個人データ保護規則 No 45/2001 の前文(8)は、「個人データ保護の諸原則は、識別された個人または識別可能な個人と関連する全ての情報について適用される。ある個人が識別可能かどうかを判定するためには、管理者によっても他の全ての者によっても当該個人を識別するために合理的に用いられそうな全ての手段を考慮に入れなければならない。保護のための諸原則は、そのデータ主体を全く識別することができないように匿名化されたデータに対しては適用されない」と述べ、そして、行政機関個人データ保護規則 No 45/2001 の第4条（データの品質（Data quality））は、以下のように規定している。

1. 個人データは：

(a) 公正かつ適法に処理されなければならない；

(b) 特定の、明示かつ適法な目的のために収集されなければならない、かつ、その目的に適合しない方法で別の目的で処理なされてはならない。歴史、

統計または科学の目的により収集された個人データの別の目的による処理は、とりわけ、他の目的のために当該データが保有されることのないようにするため、または、特定の個人と関連する措置もしくは判断をする際の支援に用いられることがないようにするために、管理者が適切な安全性確保措置を講じている限り、この規則に適合しないものと判断してはならない；

(c) その収集と別の目的による処理は、その目的との関係において十分であり、関連性を有するものであり、かつ、その範囲を超えないものでなければならない；

(d) 正確なものでなければならない。その必要があるときは、最新のものに保たなければならない。それが収集される目的及び別の目的で処理される目的に照らし、不正確なデータもしくは不完全なデータの消去及び訂正を確保するための全ての合理的な手立てが講じられなければならない；

(e) データが収集される目的またはそれを別の目的で処理する目的のために必要となる期間内に限り、データ主体を識別することができる方式で保存するものとしなければならない。欧州共同体の機関及び組織は、歴史、統計または科学の利用のための期間内に限り記録保存される個人データについては、匿名化された方式で保存すべきこと、または、それが不可能なときは、データ主体の識別についてのみ暗号化すべきことを定めなければならない。いずれの場合においても、歴史、統計または科学以外の目的でデータを利用してはならない。

2. 管理者は、第 1 項の遵守を確保しなければならない。

これらの条項は、個人データ保護指令 95/46/EC の第 6 条とほぼ同じである。このことから、行政機関個人データ保護規則 No 45/2001 における基本的な価値判断は、個人データ保護指令 95/46/EC によって示されている価値判断に依拠するものであり、行政機関個人データ保護規則 No 45/2001 は、それを欧州共同体（欧州連合）の実定法となるものとすべく実装するものとして理解することができる。

ただし、行政機関個人データ保護規則 No 45/2001 の第 4 条第 1 項 (e) では、個人データの匿名化に関する規律が付加されている。一般個人データ保護規則 GDPR

では、匿名化（仮名化）⁽⁷⁰⁾と関連する条項が更に拡大されている。

3.2 データ主体の権利

欧州の個人データ保護法制における保護法益がプライバシーの権利及び情報の自由であること、その両者の権利及び自由の調和または整合性の確保が重要であること、並びに、自然人の個人データに関する権利の法源、とりわけ、欧州連合基本権憲章の第8条第2項がデータ主体のアクセスの権利及び個人データの訂正を求める権利を定めていることについては、既に述べたとおりである。

欧州の個人データ保護法制においては、これらの保護法益の確保を実現するための手段的・技術的・人工的な権利が構築され続けてきた。

そのような手段的な権利の表現形式で特徴的なのは、「管理者から～を得る権利（the right to obtain from controller …）」という表現が用いられていることである。これは、作為請求という側面からみれば当然のことかもしれないが、実体的な権利という側面からみると、一定の条件の下において、管理者が本来保有している管理権の一部をデータ主体が代位行使的に強制行使することができる権利として理解することが可能である⁽⁷¹⁾。そして、このように解することによってのみ、管理者が本来固有のものとして保有している権利がいつの間にかデータ主体の権利となってしまうような混乱を避けることができる。データ主体の手段的・技術的な権利は、プライバシーの権利の侵害を回復するため、その侵害を阻止するため、または、その侵害の予防のための物権的請求権⁽⁷²⁾に類似する対外的な法的効力（請求力・執行力）を有する人工的な権利である。

行政機関個人データ保護規則 No 45/2001 の第2章第5節（第13条ないし第19条）は、データ主体の権利について規定している。これらの権利は、いずれも手段

(70) データの匿名化（仮名化）に関しては、Khaled El Emam & Luk Arbuckle（木村映善・魔狸監訳・笹井崇司訳）『データ匿名化手法—ヘルスデータ事例に学ぶ個人情報保護』（オライリー・ジャパン、2015）が参考になる。

(71) これらの点については、一般個人データ保護規則参考訳の第15条第1項(e)の訳注及び第18条第1項(c)の訳注で述べた。

(72) 物権的請求権の一種である所有権に基づく妨害排除請求権の場合でも、本体となる権利は所有権なのであって、妨害排除請求権ではない。この場合、保護法益である所有権を保護するための手段的・技術的な権利としての妨害排除請求権というものが観念されるだけのことであり、妨害排除請求権だけが独立の権利として存在しているわけではない。

的・技術的な権利として理解することが可能である⁽⁷³⁾。

以下、これらの権利の概要及び日本国法との関係について述べる。

3. 2. 1 個人データに関する情報へのアクセスの権利

行政機関個人データ保護規則 No 45/2001 の第 11 条第 1 項 (e) は、管理者がデータ主体から個人データを取得する際に、データ主体に対して提供すべき情報の 1 つとして、「彼または彼女に関するデータにアクセスする権利及びそのデータを訂正する権利の存在」を掲げている。すなわち、管理者（行政機関）は、データ自体が個人データの開示及び訂正を求める権利を有することを理解し、その権利の存在を通知しなければならない。

これは、欧州連合におけるデータ主体の「同意 (consent)」が単なる承諾 (agreement) ではなく、事前に説明を受け理解した上での同意すなわちインフォームドコンセント (informed consent) であることと密接な関係を有する⁽⁷⁴⁾。同意の前提となる説明の内容を構成する情報が十分でない場合、更に情報の提供を求めることができる法的地位が認められていなければ、そもそもインフォームドコンセントという法的枠組みが瓦解してしまう道理である。

行政機関個人データ保護規則 No 45/2001 の第 2 条 (h) は、「データ主体の同意」とは、「任意に与えられ、特定され、事前に説明を受けた上での、彼もしくは彼女の意思の表示を意味し、それによって、データ主体が、彼もしくは彼女に関する個人データが処理されることについての彼もしくは彼女の同意を表明するものを意味する」と定義している⁽⁷⁵⁾。

同様の規定は、管理者が個人データのデータ主体以外の者から個人データを取得

(73) 行政機関が保有する個人データと関連するプライバシー保護一般については、Daniel J. Solove & Paul M. Schwartz, *Information Privacy Law 3rd Edition*, Wolters Kluwer (2009) pp.597-713 が参考になる。

(74) インフォームドコンセントを原則とすることから、事後承諾は基本的に認められない。その点において、事後承諾を是認する日本国の個人情報保護法制は、完全に失格である。なお、この関連では、Eleni Kosta, *Consent in European Data Protection Law*, Martinus Nijhoff (2013) が参考になる。

(75) 日本国法においては、個人情報保護法、行政機関個人情報保護法及び独立行政法人個人情報保護法のいずれにおいても「事前の同意」を原則的な要件として定めていない。一般個人データ保護規則 GDPR の中にはデータ主体の同意を要件とする条項が多数ある。また、行政機関個人データ保護規則 No 45/2001 の中には、同意を要件とする条項が少なからず存在する。その部分に関する限り、日本国の法制は、完全に失格である。

する際のデータ主体に対する通知に関する第12条第1項(e)にもある。日本国の法制に即して言い換えると、例えば、個人データの第三者提供を受けた取得者は、個人データの本人から当該個人データを取得したのではないことから、取得の時点で、当該個人データの本人を探し出し、所定の通知をしなければならない⁽⁷⁶⁾。

そして、同規則の第13条は、「アクセスの権利 (Right of access)」を定めている。データ主体は、管理者（行政機関）から、以下の事項について、無料で、無制限で、情報の提供を得ることができる。

- (a) 彼または彼女に関するデータが処理されているのか否かに関する確認；
- (b) 少なくとも、処理されている業務の目的、関係するデータの類型、データが開示される取得者または取得者の類型に関する情報；
- (c) 処理されているデータの判読可能な形式での通知及びその収集源に関する利用可能な情報；
- (d) 彼または彼女に関する自動化された決定プロセスに含まれる論理に関する知識。

日本国の法制においては、行政機関の保有する情報の公開に関する法律（平成11年法律第42号・以下「情報公開法」という。）に基づく情報公開請求によって同じ結果を得ることができるかもしれない。しかし、情報公開法に基づく請求の場合、同法第5条各号及び同法第6条により、情報が開示されないことがあり得る。この点において、データ主体に関する情報であれば無制限で提供しなければならないものとする行政機関個人データ保護規則 No 45/2001 の第13条とは法制度が異なる。また、情報公開法は、個人データの保護とは関係のない場合を含む一般法なのであって、個人データ保護に目的が限定された法令ではない。行政機関個人情報保護法第10条は、行政機関が個人情報ファイルを保有しようとする場合、予め総務大臣に対して通知しなければならない旨を規定しているが、これは個人データの本人に対する通知ではない。

行政機関個人情報保護法第12条は、個人データの開示の請求について規定して

(76) 日本国の法制では、そのような仕組みになっただけでなく、完全に失格である。

いる⁽⁷⁷⁾。この規定は、行政機関個人データ保護規則 No 45/2001 の第 13 条のアクセスの権利と同等の内容を定めるものと解釈することが可能である。

しかし、同規則第 13 条 (d) に属する情報の提供は、日本国の行政機関個人情報保護法第 12 条に基づく開示請求によっては期待できない可能性が高い。そもそも、自動的なデータ処理に基づく自動的な判定で用いられるロジックについて知悉している行政機関の職員はほぼ皆無であり、知らないことまたは理解できないことについては返答のしようがないからである。これは、大まかな仕様の決定までは行政機関が行うが、システムで用いられるコンピュータプログラムの詳細設計まで関与することが減多にないことに起因する。当該行政機関の長が詳細設計について決済する場合であっても、その内容を理解した上で決済する例は稀有に属する。総合職の行政官にはそのような能力が最初から求められておらず、総合職の国家公務員試験の内容にはそのような能力を判定するための事項が盛り込まれていない。したがって、仮に日本国の国民が、行政機関個人データ保護規則 No 45/2001 の第 13 条 (e) に定めるような情報の開示を求めても、それを得ることはほとんど期待できない。

ところが、日本国政府は、国をあげて人工知能技術の応用・導入を推進しており、現に行政機関としての業務遂行上でも何らかの法的効果を生じさせ得るような自動判定技術が導入されつつあることを考慮すると、少なくとも行政機関の長は、人工知能の基本的な仕組みを理解している者であることを要し、当該行政機関において用いられているシステムの基本仕様と処理の流れを説明できる状態になっていなければならない（あるいは、そのような内容の説明をするための部署を設置し、専門の職員を配置しなければならない）。そして、そのような行政事務の自動処理が根拠法令の予想していない結果をもたらす可能性があることを発見したときは、当該システムの利用を停止する権限を有するものとしなければならない。

一般に、人工知能技術の応用それ自体は、単なる技術的な問題かもしれないが、人工知能技術が一定の論理の自動生成と自動判定を必然的に伴うものである以上、そのような自動生成される論理と自動判定の流れが根拠法律の定める判断基準及び判断の流れと完全に一致するものであり、かつ、それから外れることが絶対にあり得ないような物理的な仕様になっていることが、当該人工知能技術を応用・導入

(77) 独立行政法人個人情報保護法第 12 条も同様である。

するための絶対条件である。それにも拘らず、一般に、完全に自律型の人工知能システムにおいては、そのシステムが自律型であるがゆえに、その絶対条件が常に無視される可能性が高い⁽⁷⁸⁾。従って、本来の意味での完全に自律型の人工知能システムの利用は、行政機関においては、法の支配の原則に反する事態の発生を阻止または防止することができないという理由で⁽⁷⁹⁾、常に禁止されなければならない。

視点を転じて、このデータ主体のアクセスの権利とプライバシーの権利との関係について検討してみると、管理者（行政機関）が保有し処理しようとしている（または、処理している）個人データに関する情報をデータ主体が得ることは、自己のプライバシーの権利に対する侵害、とりわけプロッサーの類型における第3類型及び第4類型の侵害の有無を自分で判断するために必須の前提となっている。換言すると、神の目からすればプライバシーの侵害の有無は客観的に既に確定している事実なのであるが、神にあらざる人間であるデータ主体が何らかのかたちでプライバシーの権利に対する侵害があるのか否かを認識するためには、そのような脳内での主観的な認識・判断機能を作用させるための外部的信号すなわち情報の取得が必須となる。そのことから、アクセスの権利は、それ自体として何か意味があるのではなく、データ主体が、客観的には、プロッサーの類型における第3類型及び第4類型の侵害のような社会現象・状況ないし環境の中に存在しているという事実を認識・理解し、それによってプライバシーの権利の侵害が発生しているのか否かを判断するための手段的・技術的・人工的な権利（法的装置）であることになる。換言すれば、この権利（法的装置）は、データ主体のための社会的なセンサー（検出装置・探知装置）の一種に属する。

(78) バイデザインの原則に従い、当該システムの運用の根拠となっている日本国の法令及び関連法令・判例・学説並びに諸外国の関連情報によって示される法規範を適正・妥当に、かつ、比例性原則に従って解釈運用するだけの能力を当該人工知能システムにビルトインし、それを有効に機能させることは、物理的に不可能なことである。

(79) 同様の理由により、民間企業であっても、法令順守（コンプライアンス）が強く求められる業種にあっては、完全に自律型の人工知能システムの導入が禁止されなければならない。仮にそのようなシステムを導入し利用した場合、その利用によって発生する全ての損害について当該事業者が損害賠償責任を負うものとすべきである。この場合、一般個人データ保護規則GDPRに定める立証責任の転換規則に則り、当該事業者は、「いかなる意味においても責任を負うことがない」ということを主張・立証しなければならず、現実にはそのような主張・立証はできないので、事実上、無過失責任を負うことになる。この法理は、行政機関における個人データの処理についても応用されるべきである。

したがって、この手段的・技術的・人工的な権利（法的装置）の利用が阻害された場合、それによって生ずる損害は、データ主体のプライバシーの権利それ自体の侵害から生ずる損害とは別のものとして理解される必要がある⁽⁸⁰⁾。この点については、従来、あまり深く議論されていないようなので、今後、更に検討を要する。以下、他の種類の権利についても同じである。

3. 2. 2 個人データの訂正を求める権利

行政機関個人データ保護規則 No 45/2001 が、個人データの取得の際に、データ主体に対して訂正の権利の存在を通知すべき義務を定めていることは、アクセスの権利について述べたところと同じである。

そして、同規則第 14 条は、「不正確または不完全な個人データ (inaccurate or incomplete personal data)」について、管理者（行政機関）から、訂正を得る権利について規定している。この表現は、個人データ保護指令 95/46/EC を介して、個人データ保護条約 ETS No.108 に由来するものと考えることができる。このことは、欧州評議会閣僚委員会決議第 22 号の別紙に定める事項との関連について前述したとおりである。

日本国の行政機関個人情報保護法第 27 条は、開示決定に基づき開示を受けた保有個人情報等について訂正の請求をすることができる旨を定めている⁽⁸¹⁾。

しかしながら、行政機関個人データ保護規則 No 45/2001 の第 14 条は、訂正を

(80) 物体である監視用モニタが違法に破壊された場合または使用不能とされた場合であっても、特段の事情がない限り、当該監視用モニタの物体としての損害及びその利用によって得られる期待権的な利益と関連する損害だけが考慮されるべきであり、当該監視用モニタの設置によって守ろうとしている家屋や建物それ自体が侵害されたわけではないので、当該家屋や建物と直接に関係する法益の侵害があったものとして理解することはできない。他方において、当該監視用モニタの破壊等の有無を問わず、当該監視用モニタによって守ろうとしている家屋や建物と直接に関係する法益の侵害が発生した場合には、その法益侵害による損害の賠償が検討されなければならない。これをアクセスの権利にひきなおして考えてみると、アクセスの権利はプライバシーの権利を守るための手段・技術の一種に過ぎないので、アクセスの権利に対する侵害の有無に拘らず、データ主体のプライバシーの権利の侵害の有無が検討されなければならないことになる。より具体的には、アクセスの権利を行使して管理者（行政機関）から情報を入手しなくても、別の経路を通じてプライバシーの権利に対する侵害があることを認識しているときは、直接に、プライバシーの権利の侵害を理由として、損害賠償請求の訴えを提起することができるはずである。

(81) 独立行政法人個人情報保護法第 27 条も同様である。

求める個人データについて何らの限定もしていない。仮に同規則第14条を日本国法と合わせるように改正するとすれば、アクセスの権利（第13条）によって知ることのできた情報に基づく場合に限り、第14条の訂正を求める権利が成立するものとしなければならないであろう。しかし、そのような法改正はあり得ない。したがって、日本国においても、開示決定に基づき開示を受けた保有個人情報等ではない場合であっても、特に制限を設けることなく、不正確または不完全なものが客観的に存在するときは、その訂正を求めることができるように、行政機関個人情報保護法の改正がなされるべきである。

一般に、開示請求から訂正請求までの流れを当該行政機関が把握し統制できるようにしようという発想がもし存在するとすれば、そのような発想それ自体が最初から誤っていると考える。仮にそれを不意打ち的なものまたは不当なものと感じることがあったとしても、いついかなる場合においても不正確または不完全な個人データの訂正の要求に対応できるような体制・組織を構築し、そのための予算を整えることが重要である。不正確または不完全な個人データを維持し続けることは、結果的に、適切・有効な行政事務の遂行に対して致命的な支障を発生させることがあり得るから⁽⁸²⁾、不正確または不完全なデータの訂正は、個人データの本人だけではなく、当該行政機関自身にとっても大きな意味を有するものである⁽⁸³⁾。

他方、この訂正を求める権利とプライバシーの権利との関係について検討してみると、不完全なデータまたは不正確なデータは、そのデータを認識対象として判断を行う者またはそのデータを処理対象として自動的な判定処理を行うシステムについて、誤解や誤判定の結果をもたらすことが明らかである。そして、そのような誤解や誤判定によって、最悪の場合には社会からの阻害や差別が生じ得ることも容易に想像できることである。換言すると、そのような不当な結果の発生は、一般的な予見可能性の範囲内にある。すなわち、不完全または不正確なデータの存在は、

(82) 一般論として、国防またはテロ対策のための各種データの管理の場合、記録されている重要な情報（データ）が不正確または不完全なものであるときは、誤認された個人に対して不当に公権力が行使される危険性があるというだけでなく、状況によっては、その誤認が原因となって、国家滅亡の危機を招くことさえあり得る。

(83) 功利主義的な観点からすると、訂正請求の門を拡げておけば、訂正の要求が寄せられることによって不完全または不正確なデータの存在を認識することができることになるから、国家予算による職権探知だけに依存する場合と比較して、はるかに経済的である。

プロッサーの類型における第3類型の侵害を発生させ得る典型的な場合の1つとなっているといえることができる。

そのような侵害が既に発生しているときは、未来に向けての侵害の発生継続を阻止するために、また、そのような侵害がまだ発生していないけれども発生するおそれがあることが合理的に証明できる場合にはそのような損害の発生を抑止または防止するために、手段的・技術的・人工的な権利の一種である訂正を求める権利が行使されるものと理解することができる⁽⁸⁴⁾。

3. 2. 3 個人データの処理の停止を求める権利

行政機関個人データ保護規則 No 45/2001 の第 15 条第 1 項は、以下の場合には、管理者（行政機関）から、データの停止を得ることができると規定している。

- (a) データ主体によってその正確性に異議があった場合。そのデータの正確性（完全性を含む）を管理者が確認するまでの間について；
- (b) 管理者がその職務を遂行する必要がなくなっているのに、管理者が証明のためにそれを維持しなければならない場合；
- (c) 処理が違法なものであり、かつ、データ主体が消去ではなくその停止を求める場合。

日本国の行政機関個人情報保護法第 36 条は、行政機関個人データ保護規則 No 45/2001 の第 15 条第 1 項 (c) の場合の一部に相当する違法な保有の場合について、

(84) 民事訴訟における訴訟物との関係で、言い換えると、本権はプライバシーの権利であり、それから派生するものとして、訂正を求める権利を考えることができる。それは、物件的請求権における妨害排除請求権または妨害予防請求権と類似の手段的な訴訟上の請求権として構成することができる。なお、権利の法的性質に関する学説として、財産権説と人格権説との争いがあるかのような誤解が存在する。しかし、財産権説は、主として、ドイツ法を知らない英米法ベースでの議論の中にあり、人格権説は、主として、ドイツ法における表現形態を重視するものなのであって、実質的には同じだということを理解しなければならない。このことを正しく理解しないでなされるような議論は、無知・不勉強または異なる法制に対する偏見・差別の誇りを免れることができないであろうし、また、議論それ自体として不毛でもある。なお、プロッサーは、プライバシーの本質について、それは、不法行為（tort）ではなく 4 つのタイプの出来事の複合体（complex）であるとの趣旨を述べている。法社会学的な観点からのアプローチであり、それを米国の判例法の解析のために合理的に応用し、後にはその条文化に成功しているところにプロッサーの偉大な功績がある。

利用停止を求めることができる旨を規定している⁽⁸⁵⁾。同規則第1項(a)及び(b)に相当する場合の定めはない。

また、同規則第15条第4項は、「彼または彼女のデータの停止を求め、その停止を得たデータ主体は、そのデータの利用再開の前に通知されなければならない」と定めているが、日本国法上ではこれに相当する規定が存在しない。

行政機関個人データ保護規則 No 45/2001 の第15条第1項(a)のような場合には、日本国の法制においても民事保全法に仮処分の制度があるが、問題なのは、行政機関の行為については公定力が認められている関係で、行政機関との関係においては、仮処分的な一時停止の制度を認め難いという点にある⁽⁸⁶⁾。特に個人データの処理それ自体は公権力の行使としての行政処分に該当しないのが普通であるので、一時的な停止を求めることが困難である。日本国法において行政機関個人データ保護規則 No 45/2001 の第15条第4項に相当する法令が存在しないのは、このように一時停止を求める法的根拠が希薄であることと密接な関連性を有している。

いずれにしても、日本国の行政機関個人情報保護法が定める利用停止の制度は、かなり限定的なものであり、欧州連合の行政機関個人データ保護規則 No 45/2001 の第15条の定める制度とは相当異なるものであることだけは明らかである。

他方、利用停止の求めが是認されるような状況を考えてみると、プライバシーの権利との関係では、プロセッサの類型における第3類型及び第4類型の侵害がある場合に該当すると理解することができる。

3. 2. 4 個人データの削除を求める権利

行政機関個人データ保護規則 No 45/2001 の第16条は、個人データの処理が違法である場合、管理者（行政機関）から、当該データの削除を得る権利について規定している。

日本国の法制中には、相当するものはない。

利用停止と削除との関係についてみると、利用停止は一時的・暫定的な措置ではない。正当な権限による場合と無権限による場合（例：不正アクセス）の別を問わず、データが存在している限り、それが第三者に開示される危険性が常に残存している。例えば、2014年、Yahooの利用者約5億人分の個人データが何らかの違

(85) 独立行政法人個人情報保護法第36条も同様である。

(86) 行政事件訴訟法第25条参照

法行為によって外部に流出し、そのアカウントを用いて他人がアクセスすることが可能な状態にあったが、その事実が2016年9月まで通知されなかったため、世界規模で大きな社会問題となった。類似の事例は、日本国においても、2014年のベネッセコーポレーションにおける事件を含め、数えきれないほど多数ある。理論的には、無権限アクセス（不正アクセス）を完全に阻止する技術的な方法は存在しないので、行政機関の電子計算機システムについても一定確率で無権限アクセス（不正アクセス）が発生し、あるいは、内部者による個人データの違法な持ち出し行為が発生する可能性が常に存在している。それゆえ、処理の必要のなくなった個人データは、物理的に削除され、または、匿名化ないし仮名化等の安全性確保措置を講じた上で保管されなければならない。

このような個人データの削除等は、個人データの管理者（行政機関）として、当然になすべきことであり、自主管理のための行動指針（プライバシーポリシー）によって規律可能なことである⁽⁸⁷⁾。しかし、管理者（行政機関）の怠慢により適正に削除等がなされないことは理論的にも現実的にも十分にあり得ることである。そのため、個人データのデータ主体（日本国法では、「本人」）に削除等を求める権利を認めるかどうかは、立法政策の問題ではある。しかしながら、日本国法において相当する条項が存在しないということは、個人データの第三国移転と関連する個人データの保護の充分性の判定の際にはかなり大きな影響を有する事項であると考えられる。とりわけ、一般個人データ保護規則 **GDPR** において、特例として設

(87) 現行の行政機関個人情報保護法では、総務大臣が、EUにおける欧州個人データ保護監督官、個人データ管理者、個人データ処理者及び個人データ保護責任者の地位を全部兼有しているような法制となっており（行政機関個人情報保護法第10条第1項、同条第3項、第47条第2項、第49条第1項、同条第2項、第50条、第51条）、本来は独立した行政機関として個人データ保護監督官の地位にあるべき個人情報保護委員会（平成27年法律第65号により設置され、平成28年法律第51号により、「行政機関非識別加工情報」等に関する行政機関における個人データの取扱いにも一部関与する権限を付与された。）が個人情報保護のために行政機関による個人データの管理運用の監督に関与できる余地は極めて乏しい。総務大臣は、行政機関における個人データの管理運用に関しては管理者の立場にあるので、総務大臣が独立の行政機関である個人データ保護監督官となることは、理論上、あり得ないことである。現行法に基づく総務大臣の監督なるものは、実質的には、管理者による自己管理（self-regulation）の一種に過ぎない。すなわち、日本国の行政機関における個人データの法的保護の法制度には、本来の意味での（独立の行政機関としての）個人データ保護監督官が行政機関である総務大臣を監督するという法制度が欠落していると言わざるを得ない。

置されている関係国の行政機関の間で交わされる文書という安全性確保措置を用いる場合、削除請求権が法律によって定められていないということが致命的な欠点となる可能性が高い。つまり、一般個人データ保護規則 GDPR の第 46 条第 2 項 (a) 及び同条第 3 項 (b) の定める行政文書等による特例の適用を受けることができなくなる可能性が高い⁽⁸⁸⁾。このことは、立法の不作為により、日本国の国益が深刻に阻害されていることを意味する。

他方、プライバシーの権利との関係について検討してみると、個人データの処理の停止は、一時的・暫定的な禁止であるのに対し、削除は絶対的・恒久的な禁止となる。そのことから、プライバシーの権利に対する侵害の可能性という観点からも、同様に、停止は一時的・暫定的な侵害の防止措置となり、削除は絶対的・恒久的な侵害の防止措置となり得る。それゆえ、プライバシーの権利の保護という観点からは、停止の制度が存在することは、削除の制度を設置することの必要性を低減させるものではなく、逆に、その必要性を明確にするものである。そして、この場合におけるプライバシーの侵害の実質的内容は、プロセッサの類型における第 3 類型及び第 4 類型の侵害だけではなく、第 1 類型及び第 2 類型の侵害を帰結することになる場合もあり得ると考えられる。とりわけ、既に処理されなくなり、保管されているだけのデータは、特定の個人の過去の秘匿すべき事実を示す内容を含んでいる可能性があることを正確に理解しなければならない。そのようなデータは、管理者（行政機関）によっては全く有用性がなく、興味を引くこともないデータかもしれないが、犯罪者にとっては涎の流れるようなデータであるかもしれない。個人データの安全性の確保は、そのような観点からも検討されるべきである。正常な道徳心や倫理をもつ者だけで社会が構成されているのだとすれば、そもそも個人データ保護の法制など最初から必要のない道理である⁽⁸⁹⁾。

(88) 行政文書等による特例を受けるためには、当該第三国において法的な執行力のある合意であることを要する。この法的な執行力は、とりわけ行政機関の場合、法的根拠が法令に定められていなければならないが、しかも、通常の民事におけるような民事訴訟法及び民事執行法の適用を受けないことが非常に多いという事実留意すべきである。すなわち、行政文書等による特例の適用を円滑かつ完全に受けるためには、かなり大がかりな関連行政法の改正を要する。それよりは、行政機関個人情報保護法及び独立行政機関個人情報保護法並びに関連する政令の改正だけで対応した方が簡単なのではないかと思われる。

(89) この関係では、Theo Tryfonas (Ed.), *Human Aspects of Information Security, Privacy, and Trust: 4th International Conference, HAS 2016, Held as Part of HCI*

4 権利の制限

保護法益であるプライバシーの権利と情報の自由とが矛盾・衝突する場合には、その両者の調和または整合性の確保が必要になることは既に述べたとおりである。しかし、プライバシーの権利と矛盾・衝突する法的利益は、情報の自由だけではない。とりわけ、個人データの管理者が行政機関である場合、それが行政機関であるがゆえに、公益上の理由による権利の制限が問題となり得る。

行政機関個人データ保護規則 No 45/2001 の第 20 条第 1 項は、そのような公益上の理由による制限を行うことができる場合について、以下のとおり規定している。

- (a) 犯罪行為の防止、捜査、探知、発見及び訴追；
- (b) 通貨、財政及び税に関する事柄を含め、構成国及び欧州共同体の主要な経済上または金融上の利益；
- (c) データ主体の保護または他の者の権利及び自由の保護；
- (d) 構成国の安全保障、公共の安全と防護；
- (e) (a) 及び (b) に示す場合において、単発的なものを含め、公権力の行使と密接な関係を有する監視、検査または規制の職務。

第 20 条第 1 項 (a) は、個人データ保護条約 ETS No.108 の第 9 条第 2 項 a に定める「犯罪行為の抑止」との条項に由来するもので、個人データ保護指令 95/46/EC の第 13 条 (d) にも同じ規定がある。

第 20 条第 1 項 (b) は、個人データ保護条約 ETS No.108 の第 9 条第 2 項 a に定める「構成国の財政上の利益の保護」との条項に由来するもので、個人データ保護指令 95/46/EC の第 13 条 (e) にも同じ規定がある。

第 20 条第 1 項 (c) は、やや特殊である。「データ主体の保護」は公益上の理由によるものであるが、「他の者の権利及び自由の保護」の場合には、本来であれば、私的自治の原則に従い、私人間で解決可能な問題であっても、公権力が介入したほうが妥当である場合と私的自治に任せることなく公権力が介入しなければなら

International 2016, Toronto, ON, Canada, July 17–22, 2016, Proceedings, Springer (2016) が参考になる。

い場合とが含まれる。その意味で複合的な構造をもつ条項であると言える。この「データ主体の保護」及び「他の者の権利及び自由の保護」は、個人データ保護条約 **ETS No.108** の第9条第2項 **b** に由来するもので、個人データ保護指令 **95/46/EC** の第13条 **(g)** にも同じ規定がある。

第20条第1項 **(d)** は、個人データ保護条約 **ETS No.108** の第9条第2項 **a** に定める「構成国の安全保障、公共の安全の保護」との条項に由来するもので、個人データ保護指令 **95/46/EC** の第13条 **(a)** 及び **(b)** にも同旨の規定がある。

第20条第1項 **(e)** は、個人データ保護条約 **ETS No.108** の第9条第2項 **a** に定める「犯罪の抑止」との条項に由来するもので、個人データ保護指令 **95/46/EC** の第13条 **(f)** に同旨の規定がある。

以上の権利の制限は、公益上の理由による制限である。しかし、ここでいう公益上の理由は、欧州連合の機能に関する条約（**TFEU**）に定める基本的な価値観を共有することができる諸国における公益上の理由でなければならない点に留意すべきである。すなわち、ここでいう公益上の理由ないし公共の利益の実質的な価値判断は、民主主義、基本的な権利及び自由の尊重並びに法の支配を最も重要な価値観としてその基盤とする社会において成立可能なものでなければならない⁽⁹⁰⁾。逆から言えば、民主主義及び法の支配とは一致しない価値観、例えば、全体主義国家や独裁主義国家における価値観は、当該国においては別として、欧州連合の法令の適用との関係では、公益上の理由または公共の利益としては全く認められない。

次に、行政機関個人データ保護規則 **No 45/2001** の第20条第2項は、「科学研究のみの目的でデータが処理される場合、または、統計処理の遂行のみの目的のために必要な期間を超えない範囲内の一定期間、データを個人識別可能な状態で保存する場合には、第13条及び第16条は、適用されない。ただし、データ主体のプライバシーを侵害するリスクが明らかに存在しないこと、及び、特に当該データが特定の個人に対する措置または決定を講ずるために用いられないことを確保するための適切な法的安全性確保措置を管理者が定めていることを要する」と規定している。この条項は、個人データ保護条約 **ETS No.108** の第9条第3項に由来するもので、個人データ保護指令 **95/46/EC** の第13条第2項とはほぼ同じものである。

(90) Serge Gutwirth, Ronald Leenes & Paul de Hert (Eds.), *Reforming European Data Protection Law*, Springer (2014) pp.3–33

以上に述べたところと同様の権利の制限は、民間部門に適用される一般個人データ保護規則 **GDPR** にもある。

一般個人データ保護規則 **GDPR** の第 23 条第 1 項は、その柱書において「データの管理者もしくは処理者が服する欧州連合または構成国の法律は、立法措置という方法によって、第 12 条ないし第 22 条に規定する義務及び権利と当該立法措置による条項とが適合する限り、第 12 条ないし第 22 条及び第 34 条に規定する義務及び権利の範囲を制限することができる。ただし、そのような制限は、基本的な権利及び自由の本質的部分を尊重するものであり、そして、以下の事項の安全を確保するために、民主主義の社会において必要であり、かつ、比例的な措置である場合に限る」と規定した上で、以下のとおり列挙している。

- (a) 国家安全保障；
- (b) 防衛；
- (c) 公共の安全；
- (d) 公共の安全に対する脅威に対抗する防護及び抑止を含め、犯罪行為の防止、捜査、検知もしくは訴追または刑罰の執行；
- (e) 欧州連合または構成国の公共の利益におけるその他の重要な対象、とりわけ、欧州連合または構成国の重要な経済的または財政的な利益；通貨⁽⁹¹⁾、予算及び税制上の事項、公衆衛生及び社会保障を含む；
- (f) 司法権の独立の保護及び司法手続の保護；
- (g) 規制を受ける職種における倫理違背行為の防止、捜査、検知及び訴追；
- (h) (a) ないし (e) 及び (g) に示す場合において、一時的なものを含め、公権力の行使と密接な関係を有する監視、監督及び規制の機能⁽⁹²⁾；
- (i) データ主体の保護または他の者の権利及び自由の保護；
- (j) 民事訴訟の執行確保。

(91) [訳注] 「monetary」については、文脈から、別の訳語のほうが適切だと思われ、一般個人データ保護規則参考訳ではそのようにしたが、原文（英文）が他の類似条項と同じであることから、本稿においては揃えて「通貨」との訳語をあてることにした。

(92) [訳注] 行政機関個人データ保護規則 No 45/2001 の第 20 条第 1 項 (e) では「task」となっているが、一般個人データ保護規則 **GDPR** の第 23 条第 1 項 (h) では「function」となっている。実質的には同じものを意味すると考えられる。

この一般個人データ保護規則 GDPR の第 23 条第 1 項柱書に定める内容は、上記のように、「公共の利益」が欧州連合の基本的な価値観を基盤とする社会における公共の利益であることを明確にしている点、及び、制限を設ける場合には、構成国の法律（立法）によるべきことを定めている点で重要である。

この条項のように、立法によるべきものと定められている事項については、法規範ではない運用指針（ガイドライン）、行政機関のみに適用のある内部規則、拘束的企業準則を含む契約や約款等によることができない（いわゆる「法律事項」）。そして、EU の個人データ保護関連の法令中において法律事項として定められている事項について、日本国において、法律に基づき執行可能なものとして法制度が構築されていない場合、個人データの第三国移転との関係では、十分なレベルでの法的保護があるとの判定（同規則第 45 条第 1 項）を得られないという結果となり得る。

なお、一般個人データ保護規則 GDPR の第 23 条第 1 項の (a) ないし (j) の中で、(f)、(g) 及び (j) が行政機関個人データ保護規則 No 45/2001 の第 20 条第 1 項に列挙する事項と異なっている。

一般個人データ保護規則 GDPR の第 23 条第 1 項 (g) は、一般個人データ保護規則 GDPR に定める第三国または国際機関への個人データの移転の際の特例として承認された標準約款や拘束的企業準則が規定されたことから、それらへの遵守確保の必要性が高まったことによるものではないかと推定される。これらの契約ベースでの自主管理（self-regulation）の場合、法規ではないにしても、内部的規律を強めれば強めるほど、個人データと関連する権利の行使を制限すべき必要性が高まるといふ一般的な傾向を認めることができる。

5 第三国への個人データの移転

ここまで述べてきたとおり、欧州における個人データ保護法制の保護法益は、プライバシーの権利と情報の自由（個人データの自由な移転）である。

しかし、一方の保護法益であるプライバシーの権利は、情報の自由とは基本的に無関係な公共の利益及び他人の権利・自由とも矛盾・衝突することがあり、その場合には一定の制限を受ける。そこで更に考えてみると、「私人による情報の自由」

は、他人の権利・自由の一部として理解することができる。また、「国や行政機関による公的な目的による情報の移転」は、公共の利益の一部として理解することができる。「私人による情報の自由」及び「国や行政機関による公的な目的による情報の移転」は、最も広い意味では同じ「情報の自由」の中に含まれるものとして理解することができる。その情報の自由の主体が私人である場合には、それは、広い意味での表現の自由の一部であることになる。これに対し、その情報の自由の主体が国や行政機関である場合には、表現の自由の一部であるのではなく、それ自体として公務の遂行の一部となっている。

ここにおいて、最も広い意味では同じ情報の自由であっても、その主体の相違により、法的性質がかなり異なるものであることを認識することができる。これらの権利及び自由並びに公共の利益の相互関係をモデル化してまとめると、図2のようになる。

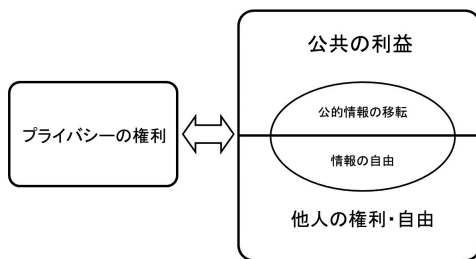


図2：権利・自由の矛盾・衝突

以上のような関係が成立している場合において、権利または自由の矛盾・衝突があるときは、既述のように、調和または整合性の確保のための何らかの措置が講じられることになる。既述のデータ主体の権利の制限は、このような調整原理の一部であると解することができる。

しかし、そのような調整原理が円滑に機能するのは、全ての権利・自由または利益の当事者について、同一の裁判権及び同一の法令が適用されるという条件が満たされる場合のみである。例えば、図2において、公共の利益の主体が外国であり、しかも、民主主義を否定する国家であった場合、権利・自由・利益の調整をするための基本的な価値観が異なっていることから、そもそも利害調整が成立しない。判

断基準としての度量衡が全く異なっている場合には、均衡しているのか均衡していないのかを測定しようがないことは、自明である。そのため、欧州連合の指令や規則に服しない領域に対して個人データが移転すると、単に欧州諸国の国家主権が及ばないというだけではなく、欧州域内において通用している価値観とは異なる価値観の下で特定の個人データが処理されるという結果が生じ得ることを避けることができない。

この関係を別の言い方で表現すると、同じ価値観を基盤とする環境においては、プライバシーの権利と情報の自由（個人データの自由な移転）の均衡点を得ることは可能であり、その均衡点を維持するように公権力を発動することも可能である。これに対し、異なる価値観を基盤とする環境においては、プライバシーの権利と情報の自由（個人データの自由な移転）の均衡点を得ることは不可能または困難であり、その均衡点を維持するように公権力を発動することも不可能または困難である⁽⁹³⁾。

このような問題があることは、個人データ保護条約 **ETS No.108** の起草者達にも十分に認識されていたし、その前段階における欧州評議会の閣僚委員会によっても認識されていたと考えられる。ただ、個人データ保護条約 **ETS No.108** が締結された **1981** 年当時においては、まだ欧州共同体がきちんとした形で成立していたわけではなく、欧州圏内の諸国の国境をまたぐ個人データの法的保護を考えるだけで精いっぱいだったと理解するのが妥当である。それゆえ、個人データ保護条約 **ETS No.108** では、第 **12** 条ないし第 **17** 条により、関係する欧州評議会構成国相互の国際的な相互支援体制を構築することにより、他の国に所在するデータ主体の権利の保護を図るという方式が採用されている。

このような方式は、欧州評議会の構成国及び非構成国の条約加盟国の間では、どうにか機能し得るものであろう。しかし、個人データ保護条約 **ETS No.108** の非加盟国との間では何らの法的拘束力も生ずることはないので、経済のグローバル化の進展と共に、欧州諸国及び欧州諸国と国際合意を締結する非欧州諸国だけを前提

(93) 現実にはそのような問題が顕在化することは意外と少ない。それは、異なる国家的価値観を有する国家間でのデータ移転であっても、その後の貿易上の不都合の発生を避けるという利害打算から、少なくとも外見上では欧州の規律を遵守しているようにしているからである。そこにあるのは、同じ規範に基づく法的な利害調整ではなく、素朴な損得勘定のみである。

とする方式ではデータ主体のプライバシーの権利を保護することができないということが明らかとなったものと思われる。この場合、普通の経済原理に基づき、個人データは、個人データの輸出入を禁止する法令が存在しない限り、自由にどの地域にでも移転する。しかし、それによってデータ主体のプライバシーの権利に何らかの侵害的な結果が発生しても、その利害を調整する機能を果たすことができる法的または政治的な仕組みが存在しないという状況が存在していることになる。

この問題を解決すべく、1995年の個人データ保護指令 95/46/EC は、欧州共同体（欧州連合）の構成国に対し、同指令の定める法的保護と均等の法的保護を与える国でない限り、第三国に対する個人データの移転を認めないという法令を制定するように命ずるという方策を採用することとなった。このことについて、個人データ保護指令 95/46/EC 第 25 条は、次のように規定している。

第 25 条 原則

1. 構成国は、処理されている個人データまたは移転の後に処理される予定の個人データについて、この指令の他の条項に従って採択された自国の条項を妨げることなく、当の第三国が十分なレベルでの保護を確保している場合のみ、第三国に対する移転をすることができるものと定めなければならない。
2. 第三国による保護のレベルの充分性は、データ移転業務または一群のデータ移転業務と関連する全ての状況を考慮に入れて、評価されなければならない。とりわけ、データの性質、処理業務の目的及び期間、発信国及び最終的な到達国、当の第三国において有効な一般的及び分野別の法律の定め、及び、当該国において遵守されている職業上の規則及び安全性確保措置が考慮に入れられなければならない。
3. 構成国及び欧州委員会は、第三国が第 2 項の意味における十分なレベルでの保護を確保していないと判断する場合には、相互に情報提供をしなければならない。
4. 欧州委員会が、第 31 条第 2 項に規定する手続に基づき、第三国が本条の第 2 項の意味における十分なレベルでの保護を確保していないと判断する場合には、構成国は、当の第三国に対する同じタイプのデータの移転を阻止するための必要な措置を講じなければならない。

5. 欧州委員会は、第4項によってなされた判断の結果生じた事態を解決するという見地から、適切な時に、協議を開始しなければならない。
6. 欧州委員会は、第31条第2項に示す手続に従い、第三国が、その国内法または特に第5項に示す交渉の結果に基づき妥結した国際協定に基づき、個人の私生活、基本的な自由及び権利について、十分なレベルでの保護を確保していると判断することができる。
構成国は、欧州委員会の決定を遵守するために必要となる措置を講じなければならない。

この個人データ保護指令95/46/ECが採択された後、2001年11月8日、個人データ保護条約ETS No.108の追加議定書ETS No.181が署名のため開放された、その第2条は、個人データ保護指令95/46/ECの第25条と実質的にほぼ同じ内容を定めており、所定の手続を経て、同追加議定書の内容が個人データ保護条約ETS No.108の中に組み込まれることになった。

この追加議定書の第2条は、次のように規定している。

各加盟国は、条約の加盟国ではない国または組織の国家主権に服する取得者に対する個人データの移転について、当該の国または組織が予定されている個人データの移転について十分なレベルでの保護を確保している場合においてのみ認められるものとすることを定めなければならない。

この議定書の第2条第1項の特例により、各加盟国は、以下の場合には個人データの移転を認めることができる：

- a 自国の法律が以下の理由によることを定めている場合；
 - データ主体の特別な利益；もしくは、
 - 公正な優先する利益、とりわけ、重要な公共の利益；または、
- b 移転について責任を有する管理者によって安全性確保措置（契約条項によることができる）が講じられており、かつ、自国の法律に基づき、職務権限を有する行政機関によって、それが十分なものであるとの判断がなされている場合。

個人データ保護指令 95/46/EC の第 25 条第 1 項の要件は、その後、「十分性」の要件と呼ばれることとなった。この要件は、一般個人データ保護規則 GDPR にもそのまま承継されている。この「十分 (adequate)」との概念は、欧州の法制に基づく個人データの保護と均等 (equivalent) という意味だと解される⁽⁹⁴⁾。

このようなやり方は、同じ価値観を共有できる国家間でなければ情報の自由 (個人データの自由な移転) を認めないというものである。価値観の異なる国家との関係では、形式的には情報の自由 (個人データの自由な移転) が禁止されたのと同じ結果となるが、そもそも価値観が異なっているので、情報の自由を禁止したことにならない。ある政策が禁止と判断されるか否かを判定するためには、同じ価値観が存在していることを前提としなければならないからである。

かくして、プライバシーの権利との間で調和または整合性の確保が求められる情報の自由 (個人データの自由な移転) は、形式的に情報の自由の問題の範疇に属するかどうかという問題よりも、そのような基本的な権利及び自由を共通の土俵の上で判定することが可能かどうかというより基盤的な問題の考察の必要性を認識させることになる。同一の基盤の上では、尺度を同一にすることができるが、同一の基盤であることが保障されない場合には尺度が尺度としての意味を持たない。

そして、行政機関個人データ保護規則 No 45/2001 においても、個人データの第三国移転に関して、個人データ保護指令 95/46/EC による欧州委員会の判断 (決定) が存在することを前提とした上で、同規則の第 9 条第 1 項は、以下のように規定している。

取得者の国家または取得者である国際機関において適切なレベルでの保護が確保されており、かつ、管理者によって遂行される権限の範囲内にある職務をすることができるようにするためにのみデータが移転される場合には、その場合においてのみ、欧州共同体の機関及び組織以外の者であって、95/46/EC

(94) 「均等 (equivalent)」の概念は、特許法の領域においても見られる。形式上または外見上は異なっても問題としないが、実質的にみて同価値であるか否かが判断の対象とされる。それは、形式によるのではなく、むしろ、法律効果または社会に及ぼす実質的な影響に着目するものである。特許法における均等論に関しては、松本重敏・大瀬戸豪志『比較特許侵害判決例の研究—均等論を中心として』(信山社、1996)、村林隆一・小谷悦司『特許裁判における均等論—日米欧三極の対比』(経済産業調査会、2003)がある。

を遵守して採択された自国の法令に従わない取得者に対して、個人データを移転することができる。

この第9条第1項にいう「欧州共同体の機関及び組織以外の者であって、95/46/ECを遵守して採択された自国の法令に従わない取得者」とは、第三国のことを意味する。しかし、欧州共同体（欧州連合）の行政機関以外の個人データの取得者であって、個人データ保護指令95/46/ECによって拘束されない非構成国に関する規定なので、第三国から欧州共同体（欧州連合）の行政機関に対して移転される個人データについて規律するものではない。

一般個人データ保護規則GDPRの第5章（第44条ないし第50条）では、基本的な骨格は、個人データ保護指令95/46/ECの第25条と同様のものとしたままで、充分性の判定がなされない場合の特例に関する条項が更に追加されている。

一般個人データ保護規則GDPRの第44条は、第三国または国際機関に対する個人データの移転に関する基本原則として、以下のように定めている。

第三国または国際機関から別の第三国または国際機関に対する個人データの更なる移転の場合を含め、現に処理されている個人データまたは移転の後に処理されることが予定されている個人データは、この規則の他の条項に従い、管理者及び処理者によって本章に定める要件が遵守される場合においてのみ、第三国または国際機関に対して、移転することができる。本章の全ての条項は、この規則によって保障される自然人保護のレベルが低下しないことを確保するために適用されなければならない。

第三国または国際機関における個人データの法的保護の充分性に関する判定に関する条項は、一般個人データ保護規則GDPRの第45条で規定されている。同条第1項は、以下のように規定している。

欧州委員会が、当の第三国、第三国内の地域もしくは1以上の特定の分野または国際組織が十分なレベルでのデータ保護を確保していると判定した場合には、第三国または国際機関に対する個人データの移転を行うことができる。

その移転は、いかなる特別の許可も要しない。

ここで「いかなる特別の承認も要しない」と定めている趣旨は、欧州委員会による十分性の判定は、包括承認の一種であり、かつ、個々の個人データの移転について個別の許可や承認を要しないという趣旨である。

そして、一般個人データ保護規則 **GDPR** の第 45 条第 2 項には、欧州委員会による十分性の判定に際して考慮されるべき事項が以下のように列挙されている。

(a) 法の支配、人権及び基本的自由の尊重、一般的な関連立法及び分野別の関連立法（公共の安全、国防、国家安全保障及び犯罪法、及び、行政機関による個人データへのアクセスを含む。）、並びに、そのような立法、データ保護の法令、職業上の規則及び防護措置（他の第三国または国際機関に対する個人データの転送に関する法令であって、当該第三国または国際機関が遵守する法令を含む。）の実装、判例法、並びに、効果的で執行可能なデータ主体の権利、その個人データが移転されつつあるデータ主体のための行政上の救済及び司法上の救済措置；

(b) 適切な執行権限を含め、データ保護の法令の遵守を確保し、かつ、執行することについての責任、データ主体がその権利を行使する際に支援し助言することについての責任、及び、構成国の監督官と協力することについて責任を有する 1 以上の独立の監督官が第三国内に存在し、または、国際機関が服するそのような監督官が存在し、かつ、それが効果的に機能していること；並びに、

(c) とりわけ、個人データの保護と関連して、関係する第三国もしくは国際機関が加盟している国際的な約定または法的拘束力のある条約もしくは協定から生ずる義務、並びに、多国間システムまたは領域システムへの参加から生ずる義務。

一般個人データ保護規則 **GDPR** の第 45 条第 2 項 (a) において、「一般的な関連立法及び分野別の関連立法」が「公共の安全、国防、国家安全保障及び犯罪法、及び、行政機関による個人データへのアクセスを含む」ものとして規定されていることは極めて重要である。要するに、理念の問題として、欧州連合の基盤となってい

る基本的な価値観（民主主義、基本的な権利及び自由の尊重、法の支配）があるというだけでは足りず、現実的なものとして、そのような理念を確保できるような実効的な領土支配のある国家であることを求めている。国家の領土が実効的に支配されていない場合、その国家の国家主権なるものは名目的なものに過ぎず（例：亡命政権）、理念を国家として強制し保護することができない。それゆえ、国家安全保障や国防を含め、基本的な価値観を守るための領土の実効支配が存在することが十分性の判定の重要な要素となっているのである。

一般個人データ保護規則 GDPR の第 45 条第 2 項 (a) は、国家制度として、公的部門（**public sector**）及び民間部門（**private sector**）における個人データの保護を監督する独立の行政機関すなわち個人データ保護監督官が存在することを十分性の判定の重要な要素として定めている。日本国の法制においては、民間部門に関する限り、改正された個人情報保護法によって設置された個人情報保護委員会が独立の行政機関としてその監督機能を果たすことができるであろう⁽⁹⁵⁾。しかし、公的部門（行政機関）に関しては、日本国の行政機関個人情報保護法が定めるところでは、EU の法制における管理者、処理者、データ保護責任者及びデータ保護監督官の全ての地位を総務大臣が全て兼有するような法制となっている。換言すると、行政機関に関しては、実質的にみて独立の監督機関が存在しないのと同然である。そのことだけで、一般個人データ保護規則第 45 条第 2 項 (b) の要件との関係では、明らかに失格であると言わざるを得ない。現行法において総務大臣に帰属している監督機能（特に EU における欧州個人データ保護監督官が有している監督権限と同じ内容の監督権限）は、全て個人情報保護委員会が有するものとして、行政機関個人

(95) 個人データのデータ主体（日本国法では、「本人」）の権利保護が十分でないこと、特に同意と通知の要件が失格であり、また、プライバシーの権利を守るための手続的・技術的権利の構成に問題があること、加えて、個人データの第三者移転と関係する法規制が完全に失格であることは、既述のとおりである。従って、これらの点に関しては、個人情報保護法の抜本的な改正が求められる。なお、2016 年 9 月現在の時点において、日本国の個人情報保護委員会が有効に機能していないとの批判がないわけではない。法令によって定める権限が乏しいことを指すのであれば、そのとおりである。しかし、法令に定める権限を行使していないという意味で批判がなされているのであるとすれば、それは、かなりの外れなものと言わざるを得ない。個人情報保護委員会は、2016 年 9 月の時点では、まだ設立されたばかりの状態であり、組織構成及び予算が確定しておらず、活動の根拠となる規則や政令等も整備されていないので、その機能を開始するための準備中の段階にあると理解すべきである。

情報保護法及び独立行政法人個人情報保護法の全面改正がなされるべきであろう。

ところで、一般に、素人考えでは、包括承認がなくても個別に許可や承認を得れば良いのではないかと考えるかもしれないが、企業経営という観点から考えると、個々の個人データの移転の度に個別に手続のための時間を浪費し、個別に手数料を徴収され、しかも、確実に許可または承認が得られる保証が何もない状態に置かれ続けるリスクというものはかなり深刻なものとなり得る。欧州連合の法的または経済的な世界戦略は、このような第 45 条第 1 項による包括承認（十分性の判定）を得ることをインセンティブとしつつ、欧州連合の基盤となっている共通の基本的な価値観（民主主義、基本的な権利及び自由の尊重並びに法の支配）を共有できる国とそうでない国とを選別し、価値観を共有できる国との間の国際関係を優遇しつつ、欧州連合における法的保護を世界規模で拡大するというにあると考えられる。すなわち、一般個人データ保護規則 GDPR は、個人データの法的保護のための単なる特別法一種ではない。少なくとも個人データの第三国移転と関係する条項に関する限り、欧州連合の国際戦略上の法的装置の一種としての機能を有するものである。

なお、一般個人データ保護規則 GDPR の第 45 条第 1 項に定める十分性の判定を得られない場合、各種の特例に基づく国際的な個人データの移転の方法（第 46 条ないし第 49 条）も準備されている。その詳細についての論述は、省略する。

6 データ主体の情報の自由（可搬性）

以上述べてきたことは、データ主体のプライバシーの権利と個人データの管理者（事業者及び行政機関）の情報の自由（個人データの自由な移転）との対抗関係という図式を前提とするものである。

しかし、データ主体（本人）が自己決定権に基づき、自己の保有する情報を利用または他者に移転することは、そもそもデータ主体（本人）の自由の領域に属する。その意味では、データ主体（本人）もまた、情報の自由を享有することができる。ただ、ここでは、本人の意思に基づく利用と処分しか存在しないため、そもそも法的議論が発生しないという特徴がある。

一般個人データ保護規則 **GDPR** は、データ主体が本来的に保有している情報の自由を確保するための手段的・技術的・人工的な権利の拡張を試みている。一般個人データ保護規則 **GDPR** の第 20 条（データの可搬性の権利）は、以下のように規定している。

1. データ主体は、以下の場合において、彼または彼女が管理者に対して構成され、通常用いられ、かつ、機械処理可能な方式で提供した彼または彼女と関係する個人データを受領する権利、及び、その個人データを処理した管理者から妨げられることなく他の管理者に対してその個人データを移転する権利を有する。

(a) その処理が第 6 項第 1 項の (a) もしくは第 9 条第 2 項による同意を根拠とする場合、または、第 6 条第 1 項の (b) による契約を根拠とする場合；及び、

(b) その処理が自動的な手段によって行われる場合。

2. 第 1 項による彼または彼女のデータの可搬性の権利を行使する際には、データ主体は、それが技術的に可能な場合には、ある管理者から他の管理者へと直接に個人データを移転する権利を有する。

3. 本条の第 1 項に示す権利の行使は、第 17 条を妨げない。この権利は、公共の利益においてまたは管理者に与えられた公的な権限の行使において行われる職務の遂行のために必要となる処理については適用されない。

4. 第 1 項に示す権利は、他の者の権利及び自由に対して悪影響を及ぼしてはならない。

この権利は、本来であれば管理者が有している管理権に対してデータ主体が干渉し、管理者の権限を代位行使的に強制実行する権利（法的装置）として理解することができる。そしてまた、この権利が現実に行使される段階では、伝統的な法制度の体系に対して相当程度の影響を与えることが予想される。

この可搬性の権利が保護するプライバシーは、プロッサーの 4 つの種類の全てと関連し得るものである。

一般に、「サイトひっこしサービス」のようなものがプロバイダ利用契約の中に

最初から含まれている場合には、この権利は、少なくとも当該プロバイダとの関係においては既に実装されていると言える。しかし、そうでない場合には、可搬性の確保を内容とする法定の契約強制のようなものが存在しているのに、その法定の契約強制が利用契約の文面上には反映されていないということになる。しかし、この例の場合、可搬性の確保が法定の契約強制である以上、利用者である契約当事者は、プロバイダに対して、契約上の文言の有無とは無関係に、契約上の権利として可搬性の実施を請求し得るはずである。この場合、営利を目的とする私企業であっても、民主主義社会における自然人の基本的権利及び自由の総体としての公共の利益（**public interest**）とりわけ総体としてのデータ主体自身に認められている情報の自由の確保のために、当該プロバイダは、契約の自由と企業活動の自由の一部を制限されることになる。

他に様々な影響があり得る。例えば、企業の関係では、独占禁止法（競争法）の適用の問題が生じ得ることであろう。また、消費者保護との関係では、可搬性の原則を阻害するような消費者契約や約款における拘束力を法令によって強制的に解除することが議論されなければならない。場合によっては、労働協約の解釈・運用と関連して、労働法の分野においてもその影響が波及する可能性がある⁽⁹⁶⁾。

この権利に相当する権利を定める日本国の法令は存在しない。しかし、個人データの第三国移転の十分性判定との関係では、無視することが許されない権利の1つである。本稿においては、今後の重要な検討課題として示唆するのにとどめる。

(96) 例えば、ある労働者 X がそれまで所属していた労働組合 A をやめ、別の労働組合 B に所属することとした場合において、労働組合 A のサーバ上で A が管理している X 保有の個人データをまとめて労働組合 B のサーバ上に移転するような架空の事案を考えると、この事案において、労働組合 A と労働組合 B とが政策方針や政治思想等において対立関係にあるときは、X の保有する個人データをまとめて労働組合 A のサーバから労働組合 B のサーバに移転することができないという事態が発生し得ることであろう。このような場合において、日本国の労働基準局がどの程度までどのような態様で労働組合 A 及び労働組合 B に対して公権力を行使し、労働者 X の労働者としてのプライバシーの権利を守ることができるかについては、ほとんど不明である。今後、研究が深められなければならない。

7 まとめ

本稿における検討により、欧州連合（EU）の個人データ保護法制における真の保護法益は、プライバシーの権利及び情報の自由であること、その法的な調整手段を提供するために長年にわたる改善と工夫の努力が重ねられてきたということ、並びに、それらの法源を明らかにすることができたと考える。そこにおいて用いられている基本概念は、一貫して、プライバシーの権利（**the right to privacy**）である。そのプライバシー（**privacy**）の実質的内容は、プロセッサの4類型の理論によって説明することが可能である。それと同時に、プライバシーの権利を守るための手段的・技術的・人工的な権利として、様々なタイプのデータ主体の権利が構成され続けてきたという事実を明らかにすることもできたと考える。

欧州連合の法理論は、法哲学のレベルでの抽象的な保護法益を行政活動、企業活動及び司法の場で効果的かつ合理的に実現するための具体的な手続的・技術的・人工的な法的手段・法的装置を伴うものとして法制度全体が構成されるようになってきている。今後も、社会環境の変化と共に、新たな手段的・技術的・人工的な権利がそのカタログに追加されることになるであろう。それは、司法救済のためには、権利という法律構成をしないと、損害賠償請求のような民事訴訟において訴訟物を構成する際に難があり、欧州連合基本権憲章第47条に定める「効果的な救済を求める権利⁽⁹⁷⁾」の妨げとなるというプラクティカルな理由に基づく。

このように、保護法益を守るための手段としての手続的・技術的・人工的な権利の豊富さが増し続けているにもかかわらず、真の保護法益は一貫している。それは、個人の「ささやかな私事」である。このことを正確に理解するか否かによって、この分野における法解釈論の健全性・有用性が大きく左右されることになるであろう。

一般に、従来日本国における法学教育においては、哲学のレベルで抽象的に「人権」ないし「基本権」が論じられることが多かった。そこでは、真の保護法益と手段的・技術的・人工的な権利とを分別せず、等しく全て人権の一種として扱われることになる。しかし、そのような考え方を維持したままでは、不毛な神学論争を産むことはあっても、法解釈論上及び法律実務上で合理的な解決を得ることは難

(97) Explanation relating to the Charter of Fundamental Rights (2007/C 303/02) pp.29–30

しい。規範の階層構造を正確に認識し、保護法益と手段的・技術的・人工的な権利とを明確に分別することが重要である。今後の大学法学部においては、法哲学のレベルにおける観念としての保護法益とそれを実現するための具体的な法的装置との相互関係について、法情報学の観点を強化したものとしての法令と判例の詳細な解釈及び実務慣行の法社会学的考究によって、より現実的に理解させるような法学教育が望まれる。

他方において、特定の国家間において、個人データ保護のための法制度における保護法益の基礎となっている基本的な価値観を承認することができない場合には、そもそも価値観が異なることになるので、国家的価値観が均等であることを前提とする合理的な交渉の余地はない。そこでは、素朴な損得勘定すなわち経済原理だけに頼る事実上の解決策しかない。そのような事実の解決策は、世界的な経済情勢の変化により簡単に全崩壊してしまう危険性を常に帯有している。

これに対し、保護法益の基礎となっている価値観を承認することができる場合には、その法概念としての表現形式である保護法益を承認することもできるし、それを具体的に実現するための手段的・技術的・人工的な権利の設計・実装・運用を合理的に考えることもできる。後者については、欧州連合基本権憲章においても明確に認められている民族自決主義と多様性という価値観から必然的に生ずることになるある種の「差異」の存在を当然の前提とした上で、その差異を合理的に調整するための補正的な法制度上の仕組みを構築することも可能となるであろう。

結局、欧州連合の個人データ保護法制が日本国を含む第三国に対して突きつけているのは、単に手段的・技術的・人工的な権利を承認することだけではない。むしろ、基本的な価値観を共有することができるかどうか問われていると考えなければならぬ。上記の図2で説明すると、「公共の利益」の実質的内容である民主主義、基本的な権利及び自由の尊重並びに法の支配等といった基本的な価値観が均等なものとして現実に存在しているかどうか問題なのである。そうでなければ、同じ内容を示すものとして「公共の利益」を観念することができず、結果的に、利害の調整が原理的に不可能という状態に陥ることになる。

このような状況をどのように理解し、国家レベルにおいてどのような政策的判断をすべきかについては、直接的には為政者である内閣の責務であると言わざるを得ない。しかし、日本国は民主主義の国家である。そうである以上、為政者に対して

どのような政策を採るべきかを決定する権限（主権）を国民が明確に行使することが実は最も大事なこととなる。

その大前提として、欧州の個人データ保護法が単に個人データを法的に保護するための特殊な特別法の一つというよりもはるかに大きな政治的意味をもつものだという認識をもつことが重要である。プライバシーの権利と情報の自由（個人データの自由な移転）との調整原理が合理的に機能するような制度的仕組みが存在しているかどうかという問いかけは、より抽象的には、民主主義、基本的な権利及び自由の尊重並びに法の支配という共通の基本的な価値観を基盤とした上で、人権保障と経済原理との調和または整合性の確保のための国家的な機能が現実に存在するか否かが問われていると言い換えることができる。本稿がそのような理解を得るための一助となることができれば、望外の喜びである。

以上⁽⁹⁸⁾

(明治大学法学部教授)

(98) 本稿は、科学研究費補助金共同研究基盤研究(A)知的財産権と憲法的価値・科研費研究課題番号15H01928の研究成果の一部である。