Symposium GDPR and Information Trust

シンポジウム「GDPR と情報信託の交錯」

羽賀由利子・長瀬貴志・
第一東京弁護士会司法研究委員会信託法研究部会

はじめに

本稿は、2018 年 12 月 15 日、金沢大学法学類と第一東京弁護士会司法研究委員会信託法研究部会が共同開催したシンポジウム「GDPR と情報信託の交錯」の記録である。

今日、情報は「21 世紀の石油」として経済的に重要な地位を占め、「第四次産業革命」とも呼ばれる社会の変革期を迎えている。情報流通に関する制度設計が急がれている現代において、情報流通に関連する法的問題の解決も喫緊の課題である。

本シンポジウムは、その中でも特に国境を超えるデータ流通についての法的問題に焦点を当て、とりわけ EU で成立した一般データ保護規則（General Data Protection Regulation: GDPR）との関係での検討に取り組んだ。

EU で制定され、2018 年 5 月に施行された GDPR は、第一義的には個人データ保護に関する EU 法であるが、削除権やデータポータビリティ権といった新たな概念が提唱されたことで、欧州域外からも注目を集めている。GDPR は、一定の場合には域外にも適用される可能性があり、さらには高額の制裁金も定められていることもあり、実務界からの関心も高い。

本シンポジウムでは、まず、国境を超える情報の取引に関心を有する筆者が、議論の基盤として、GDPR の概要とその背景について確認した。その上で、裁判官時代に総務省に出向され、個人情報保護法のご担当としても活躍された本学法務研究科の長瀬貴志先生より、個人情報保護法と GDPR との内容の異同や適用関係についてのご講演をいただいた。そして、現代の情報流通に

かかる問題点やその解決について、第一東京弁護士会司法研究委員会信託法研究部会の弁護士の先生方より、実務家の視点からのご議論をいただいた。同部会は、信託分野について実務の知見を活かした様々な活動に取り組んでおり、近々の導入をにらんで活発に議論されている「情報信託」も研究テーマの一つとしている。本シンポジウムでは、情報信託に関する様々な想定事例を挙げつつ、情報銀行という新たな業務形態にも言及する幅広い議論が展開された。

本稿は、シンポジウムで用いられた原稿を基礎としつつ、論文あるいは講演録の形で、加筆修正したものである。記録の公表にあたっては、ご登壇の先生方にはお忙しい中に原稿化にご対応いただいた。心より感謝申し上げる。本シンポジウムは 2018 年冬の開催であったが、その時点では生じておらず、その後何らかの変化があった事項についても、原稿化の段階で補完したことをここに記しておきたい。

なお、本シンポジウムの開催にあたっては、金沢大学法学類、民事法研究会から財政面を含め、様々な支援を頂戴した。ここに記して感謝申し上げる。

羽賀由利子

GDPR の沿革とその内容

金沢大学法学類　羽　賀　由利子

そして見ていると、見よ、白い馬が現れ、乗っている者は、弓を持っていた。彼は冠を与えられ、勝利の上に更に勝利を得ようと出て行った。（06:02）

（…）

すると、火のように赤い別の馬が現れた。その馬に乗っている者には、地上から平和を奪い取って、殺し合いをさせる力が与えられた。また、この者には大きな剣が与えられた。（06:04）

小羊が第三の封印を開いたとき、第三の生き物が「出て来い」と言うのを、わたしは聞いた。そして見ていると、見よ、黒い馬が現れ、乗っている者は、手に秤を持っていた。（06:05）

（…）

そして見ていると、見よ、青白い馬が現れ、乗っている者の名は「死」といい、これに陰府が従っていた。彼らには、地上の四分の一を支配し、剣と飢饉と死をもって、更に地上の野獣で人を滅ぼす権威が与えられた。（06:08）

——ヨハネの黙示録（日本聖書協会『聖書 新共同訳』）

はじめに

アメリカに本拠を置く巨大 IT 企業である Google、Apple、Facebook、Amazon のそれぞれの頭文字を取り、GAFA と呼びならわすようになって久しい。

2018 年、ニューヨーク大学スターン経営大学院教授であるスコット・ギャロウェイがこの四企業をヨハネの黙示録の四騎士になぞらえた書籍を上梓し[1]、

1　S. Galloway, The Four: The Hidden DNA of Amazon, Apple, Facebook, and Google (Portfolio,

その邦訳も好調に売り上げを伸ばしている[2]。

ヨハネの黙示録と言えば、キリスト教黙示文学の中で最も議論を呼んだ文書の一つであり[3]、美術や文学などの芸術分野にも大きな影響を与えているものである。そこに登場する黙示録の四騎士（Four Horsemen of the Apocalypse）は、オックスフォード英語辞典によれば、それぞれ「支配」、「戦争」、「飢饉」、そして「死」を示し、しばしば差し迫った大異変の行為者を意味するとされる[4]。このような不気味な存在に GAFA を準えたところには、巨大化する IT 巨人への危機感や脅威が看取される。

アメリカで台頭するこれらの巨人に対抗するように、欧州では、個人情報の保護を目的とした法規則が新たに策定された。EU 一般データ保護規則（General Data Protection Regulation; 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）である。一般に GDPR と略称されるこの規則は、1995 年のデータ保護指令（正式には、個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会指令。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）を、加盟国へ直接適用される規則（Regulation）へと格上げしたものである。

GDPR は 2016 年 4 月 27 日に採択され、2018 年 5 月 25 日に施行された。この GDPR は、後述の通りその適用範囲が欧州域外にも及び得ることから、採択前から大きな議論を呼び、特にアメリカからは、時に強い反発を招いてい

2018).

2　スコット・ギャロウェイ＝渡会圭子（訳）『the four GAFA：四騎士が創り変えた世界』（東洋経済新報社、2018）。

3　佐竹明『ヨハネの黙示録（上）序説』（新教出版社、2007）9-24 頁も参照。

4　なお、神学的には、さらに様々な解釈があるところである。佐竹明『ヨハネの黙示録（中）1-11 章』（新教出版社、2009）279-293 頁。

た。その背景には、欧州とアメリカとの間の産業政策の相違や、個人にかかる情報に対する価値観の異同がある。

そして、この GDPR については、我が国もまた無関心ではいられない。我が国の企業が適用対象となる可能性もあるし、欧州という一大法域で策定されたこの規則は、今後の個人データ保護法制の一つの基準ともなるからである。

GDPR は、1 条において、同規則の対象と目的を謳う。

(1) この規則は、個人データの処理に関して個人を保護するためのルールと、個人データの自由な流通のためのルールを定める。
(2) この規則は、自然人の基本的権利と自由、特に、個人データの保護における彼らの権利を保護する。
(3) 個人データの処理における個人の保護を理由にして、EU 域内の個人データの自由な流通を制限または禁止してはならない。

文言からも明らかな通り、GDPR は情報流通を前提としつつも、自然人の基本的権利として、自己の個人データをコントロールする権利を保障することを第一義としている。この点が、個人にかかる情報を収集し、それを活用する情報産業の利益と衝突する部分でもある。

本稿は、我が国におけるこれからの情報法制の整備、情報産業の発展のための一つの参考資料として、この GDPR の沿革とその内容を改めて確認するものである。紙幅の関係上、特徴的な点の概要の描写にとどまらざるを得ないが、GDPR については、邦語でもすでに多くの文献が公表されているところであり[5]、そちらを参照されたい。

5 きわめて多くの文献が公表されており、法学分野の概説的なものに限るとしても、書籍として、宮下紘『EU 一般データ保護規則』(勁草書房、2018) を中心に、中崎尚『Q&A で学ぶ GDPR のリスクと対応策』(商事法務、2018)、小向太郎・石井夏生利『概説 GDPR』(NTT 出版、2019)、等。論稿として、石井夏生利「EU 一般データ保護規則提案の動向 (1)〜(3)」NBL1025 号 (2014) 30 頁以下、同 1029 号 (2014) 30 頁以

1. GDPR の沿革と背景

まず、GDPR が策定されるその沿革を概観しておこう。前述の通り、GDPR の前身となるのは 1995 年の欧州データ保護指令である。指令とは、EU 法上、EU 加盟各国に国内法制の整備を要求するものである[6]。

欧州データ保護指令もまた、情報の流通に際して、自然人の基本的権利と自由、とりわけプライバシーの権利の保護を目的としたものであった（指令 1 条）。ところが、具体的な法制の内容は各国に委ねられたことから、EU 加盟各国のデータ保護制度の断片化を招来することとなってしまった。これが GDPR 策定の大きな契機となり（前文（recital）9 参照）、2012 年 1 月、欧州一般データ保護規則案が提案されることとなった。この規則案が、様々な議論の末に修正や変更も加えられたものの、2016 年採択、2018 年施行へとつながっている。

さて、GDPR の通奏低音となるのは、欧州の基本的価値としての個人データの保護である。GDPR の前文 1 は、「自然人が個人データ処理に関して保護を受けることは基本的人権である」と確認する。この見解は欧州における共通認

下、同 1031 号（2014）18 頁以下、生貝直人「EU 一般データ保護規則の可決と今後の論点」行政 & 情報システム 52 巻 5 号（2016）43 頁以下、石井夏生利「世界的な潮流から見た評価と第三国への影響（EU 一般データ保護規則）」Business Law Journal 9 巻 8 号（2016）75 頁以下、宮下紘「規則の特徴と対応」ビジネス法務 17 巻 8 号（2017）14 頁以下、島村智子「EU 一般データ保護規則（GDPR）の適用開始」外国の立法 276-1 号（2018）2 頁以下、宮下紘「EU 一般データ保護規則の概要と実務の法的課題」Law & Technology 80 号（2018）44 頁以下、石井夏生利「EU データ保護指令と EU 一般データ保護規則」法の支配 192-2 号（2019）2 頁以下、カライスコス・アントニオス「現代社会におけるデータの複合的性質：EU 一般データ保護規則及びその周辺領域の展開を中心に」法律のひろば 72 巻 5 号（2019）48 頁以下、中崎尚「GDPR 概説（特集 GDPR 完全施行に対する法務対応）」自由と正義 70 巻 6 号（2019）8 頁以下、藤原静雄「GDPR をめぐる法的課題：特色と留意点」ジュリスト 1534 号（2019）14 頁以下、等。また、ビジネス法務 17 巻 8 号（2017）、Business law journal 11 巻 4 号（2018）、ジュリスト 1521 号（2018）、Business law journal 11 巻 10 号（2018）、ビジネス法務 18 巻 12 号（2018）、自由と正義 70 巻 6 号（2019）等、様々な専門誌で特集も組まれ、注目の高さが伺われる。

6　中西優美子『EU 法』（新世社、2012）115-116 頁。

識であり、欧州連合の諸条約にも明文の規定が存在する。

例えば、基本権憲章 8 条 1 項は、「何人も、自己に関係する個人のデータ（personal data）の保護に対する権利を有する」とした上で、同条 2 項は、「そのようなデータは、当該者の承諾に基づいて、または法律に依って定められたその他の合法的基礎に基づいて、明記された目的のために公明正大に作成されねばならない。何人も、自己に関係する収集された情報のアクセスに対する権利及び情報の誤りを正す権利を有する」と定めている。そして、その遵守には、独立の機関による監督が求められる（同条 3 項）。

欧州人権条約第 8 条もまた、「すべての者は、その私的及び家庭生活、住居及び通信の権利を有する」（1 項）と明言する。個人に関する情報は、この私的生活の権利に含まれるものである。その上で、「この権利の行使については、法律の基づき、かつ国の安全、公共の安全若しくは国の経済的福利のため、また、無秩序若しくは犯罪防止のため、健康若しくは道徳の保護のため、又は他の者の権利及び自由の保護のため民主的社会において必要なもの以外のいかなる公の機関による干渉もあってはならない」（同条 2 項）として、個人にかかる情報の利用は、あくまでも法の赦す範囲において、限定的に認められるという態度を示す。欧州運営条約（TFEU）16 条 1 項も同様に、「何人も、自身に関する個人のデータ（personal data）の保護についての権利を有する」と明文で定めている。

このように、欧州においては、個人にかかる情報の保護が基本的人権として取り扱われ、諸条約において繰り返し明文で謳われている。この背景には、世界大戦中に個人の情報が悪用され、ナチスによるユダヤ人迫害といった悲劇へとつながったことへの反省がある[7]。情報の取り扱いの如何が人の生命すらも左右するとの感覚が、欧州では共有されている。それゆえに、諸条約の文言にもあるように、個人の情報・データの保護は「基本的人権」の一環なのである。

7 F. Bignami, European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining, 48 B.C. L. Rev. 609 (2007) pp. 609-610.

このことは、もちろん、GDPR の起草に際しても意識されていた。Jean-Claude Juncker 欧州委員会委員長は、「Towards a better Europe; a Europe that protects, empowers and defends」と題した 2016 年の一般演説（State of the Union Address）において、以下のように述べた。

> “Being European means the right to have your personal data protected by strong, European laws. Because Europeans do not like drones overhead recording their every move, or companies stockpiling their every mouse click. This is why Parliament, Council and Commission agreed in May this year a common European Data Protection Regulation. This is a strong European law that applies to companies wherever they are based and whenever they are processing your data. Because in Europe, privacy matters. This is a question of human dignity.”（下線は筆者による）

「欧州においては、プライバシーは重要問題である。これは、人の尊厳の問題である」。これが、GDPR の基本方針の一つと言える。GDPR の施行に先駆けて出された欧州委員会からの欧州議会へのコミュニケーションにおいても、「プライバシーは取引対象ではなく（Privacy is not a commodity to be traded）」、基本的に個人データ保護は「取引できない（non-negotiable）」ものと位置付けた上で、情報の流通がなされるべきことが指摘されている[8]。

GDPR は、個人の情報・データに関する「主権」[9] をその個人に取り戻すことを目的としている。この思想は、莫大な量の情報を収集し、そこから収益を得てきたアメリカ西海岸の超大手 IT 企業を標的とする。それゆえに、GDPR は欧州とアメリカとの間に緊張をもたらした。

8　Exchanging and Protecting Personal Data in a Globalised World, Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World (COM/2017/07 final).

9　武邑光裕『さよなら、インターネット』（ダイヤモンド社、2018）162 頁。

ここで留意すべきは、そもそも欧州とアメリカの間には、プライバシー概念の違いが存在するということである[10]。この点について、まず確認しておく必要があろう。

欧州は、プライバシーを人間の尊厳（dignity）ととらえる。例えば、1949年のドイツ憲法 1 条は、端的に、「人の尊厳は不可侵である（Die Würde des Menschen ist unantastbar.）」と定め、これを基本的価値と位置付ける。そして上述の通り、この不可侵の尊厳には、個人にかかる情報が含まれるのである。なお、同国ヘッセン州の 1970 年個人データ保護法は、世界初の個人情報保護法である[11]。

これに対して、アメリカはプライバシーを自由（liberty）に根差すものと解する。アメリカの権利章典は国家が「してはならない」ことを列挙するが、修正 4 条には「身体、家屋、書類および所有物の安全を保障される」権利が挙げられている。これはイギリスのチャタム伯ウィリアム・ピット卿の言葉の流れを汲むものであり[12]、つまり、自分自身の領域は国家から不可侵であって、干渉されないことを示している。

換言すれば、プライバシーは、片や欧州では、人の尊厳を保護するためにある者から他者に対する侵害を禁じるものであるのに対して、片やアメリカでは、国家からの個人の生活への不当な介入を禁じるものなのである。

---

10 P. M. Schwartz & K. -N. Peifer, Transatlantic Data Privacy Law, 106 Geo. L. J. 115 (2017) pp. 117-118 (“The roots of this “war” are found in the differing legal approaches to information privacy in the two jurisdictions. The differences are institutional, substantive, and, at the same time, elusive. Both sides recognize information privacy as an important value yet struggle to identify the meaning of core differences and the critical baseline for future collaboration.”).

11 村上聡「ビッグデータの利活用とプライバシー保護について」通信ソサイエティマガジン 29 号（2014）52 頁。

12 Sir William Pitt, Earl of Chatham, on the right of an Englishman to be secure in his home (1763): “The poorest man may in his cottage bid defiance to all the forces of the Crown. It may be frail – its roof may shake – the wind may blow through it – the storm may enter – the rain may enter – but the King of England cannot enter; all his forces dare not cross the threshold of that ruined tenement”.

根底に流れる思想のかような相違のゆえに[13]、プライバシーあるいは個人の情報・データに関しては、個人の保護を徹底すべしとする欧州と、自由がゆえに個人にかかる情報を収集し、そこから利益を得る活動も許容されるとするアメリカとの間で、大西洋を挟んだ戦争（transatlantic war）が生じているのである[14]。

GDPR を考える上では、このような欧州とアメリカの間の根本的な認識の違いを踏まえておかなければならない。それなしには、GAFA をはじめとする情報分野の企業活動に対して欧州が持つ危機感も、欧州の規制に対するアメリカの反発も、理解し難いものとなる。

2. GDPR の特徴

プライバシーあるいは個人情報に対する欧州の基本的な理念を踏まえた上で、GDPR の特徴的な部分をいくつか見ておく。GDPR は今後、個人の情報・データの保護に関する世界基準ともなる重要な存在ではあるが、紙幅の関係上、網羅的には紹介できないことをはじめに断っておく。

上述の通り、GDPR の前身は 1995 年の欧州データ保護指令である。この指令（Directive）を規則（Regulation）へと格上げしたのが GDPR であり、これには、(1) 個人データ保護に対する権利の強化、(2) EU 域内でのデータ保護に関するルールの一元化、(3) 国際的な（対域外を含む）データ保護の詳細なルールの策定、といった目的がある。

以下では、(1) を中心に、それぞれの目的のためにいかなる方策がとられているかを概観していく。

13　より詳細には、J. Q. Whitman, “The Two Western Cultures of Privacy: Dignity versus Liberty”, 113 Yale L. J. (2004) pp. 1151ff; J. -L. Halpérin, “Protection de la vie privée et privacy : deux traditions juridiques différents ?”, Nouveaux cahiers du conseil constitutionnel no. 48 (2015), p. 59 et s.; 宮下紘「プライバシーをめぐるアメリカとヨーロッパの衝突（1）」比較法文化 18 号（2010）131 頁以下を参照。

14　H. Farrell & A. Newman, The Transatlantic Data War: Europe Fights Back Against the NSA, 95(1) Foreign Affairs 124 (2016), pp. 124ff.

GDPR では、個人データの主体となる自然人をデータ主体（data subject）と称するので、ここでもその語を用いていくこととする。GDPR は、この「識別された自然人又は識別可能な自然人（「データ主体」）に関する情報」を個人データとして定義する（4 条 1 項）。ここには、データ主体の氏名や住所、写真、電子メールアドレス、口座情報、SNS への書き込み、医療情報、コンピュータの IP アドレス等、きわめて多様な情報が含まれる。

（1）個人データ保護に対する権利の強化：「自己情報コントロール権」の強化

第一の目的は個人データの保護である。より具体的には、データ主体の「自己情報コントロール権」の強化が意図されている[15]。「自己情報コントロール権」がプライバシーの権利を指し示すことはよく知られているところである[16]。

①データ主体の「同意」

データ主体が自分自身の情報に実効的にコントロールを及ぼすための方策として、「自由意思で与えられ、特定され、情報を与えられた、不明瞭でない（freely given, specific, informed and unambiguous）同意」の取得が義務付けられる（4 条（11）、7 条。前文 32 も参照）。これは、データ主体が自己の情報の利用について自身の判断を明確に下せるよう保障するものであり、データ主体の知らぬ間に、勝手に自己の個人データが処理されることは許されないことである、という GDPR の立場を明確に示している。

また、データ主体の同意を得るために、データ管理者からは、簡潔で、透明

15　前文 7 では「自然人は自身のデータにかかるコントロールを有する（Natural persons should have control of their own personal data.）」と端的に述べられている。

16　19 世紀末に Warren & Brandeis の著名な論文で「ほうっておいてもらう権利（right to be let alone）」として提唱されたプライバシーの権利であるが（S. D. Warren & L. D. Brandeis, “The Right to Privacy”, 4 Harvard Law Review 193 (1890) pp. 193ff）、1960 年の Prosser の 4 分類による議論の精緻化を経て（W. L. Prosser, “Privacy”, 48 California Law Review 383 (1960), pp.383ff. ①私的領域への侵入、②私事の公開、③世人への誤った印象の付与、④氏名・肖像の営利目的での無断使用、に分類される）、自己決定権の一環としての「自身にかかる情報をコントロールする権利（right to control one’s own information）」（A. F. Westin, Privacy and Freedom, Ig Publishing (reprint), New York, 1967, p.5）と位置付けられるに至っている。

性があり、わかりやすく、容易にアクセス可能な（concise, transparent, intelligible and easily accessible）形で、明確かつ平易な言葉（clear and plain language）を用いて、データ処理についての情報が提供されなければならない（12 条）。データの管理者は、これに基づき、わかりやすいプライバシーポリシー等の提供が求められることになる。これは、5 条 2 項に定められるデータ管理者の説明責任（accountability）を具体化するものでもある。

データ主体の同意は、「宣言または明らかな肯定的行為によって（by a statement or by a clear affirmative action）」、取得されなければならない（4 条（11））。すなわち、一般的な契約約款で包括的に同意がなされるだけでは不十分であり、書面ないし、記録された口頭による同意、あるいは電子的手段による宣言、または Web サイト上での同意ボックスのチェック、電子的フォームへの入力、電子メールの送信といった明確な行為が必要とされる。

現代では、様々な情報サービスの利用者となるデータ主体は様々な年齢層に及んでおり、若年層も SNS をはじめとするサービスを利用している。そこで GDPR は、子どもに対する特別の配慮もまた定めている（8 条）。未だ判断能力が成熟していない子どもの個人データの取り扱いは、成人のそれに比してより慎重になされなければならない。そこで、データ取得に際して法定代理人の同意が要件として課され（8 条）、同意取得の前提となる情報提供に際しても、格別の配慮が要求されている（12 条（1））。

②「新たな権利」

自己情報のコントロールという観点から、GDPR の中でも特に注目を集めている一つは、17 条に定められる「削除権（「忘れられる権利」）」であろう。削除権ないし忘れられる権利を GDPR に導入するかについては、起草段階でも活発な議論が行われ、欧州以外からも高い関心が寄せられていた。

忘れられる権利は、欧州司法裁判所の 2014 年 5 月 13 日先決裁定（ECJ Judgment 13 May 2014 (C-131/12) Google Spain v. AEPD and Mario Costeja González）

で言及された[17]。我が国でも、欧州での議論を背景として、忘れられる権利に言及する裁判例が出され（東京地裁平成 26 年 10 月 9 日仮処分決定（判例集等未登載）、さいたま地決平成 27 年 12 月 22 日（判時 2282 号 78 頁）[18]）、学界・実務界からも多くの論稿が公表されている[19]。

続いて、17 条に定められる削除権は、データ主体に対しては「不当な遅滞なく（without undue delay）」自己に関する個人データの消去を得る権利である。その裏返しとしてデータ管理者に対しては「不当な遅滞なく」個人データを消去すべき義務が課される。

データの消去を求め得る場合として、個人データの収集・処理の目的との関係でもはや必要ない場合、データ主体が同意を撤回し、かつ当該データ処理の

17 この ECJ 先決裁定の邦語評釈として、中西優美子「Google と EU の「忘れられる権利（削除権）」」自治研究 90 巻 9 号（2014）96 頁以下、中村民雄「EU 法判例研究：忘れられる権利事件」法律時報 87 巻 5 号（2015）132 頁以下、野澤正充「「忘れられる権利」（droit à l'oubli）とプライバシーの保護」L&T 70 号（2016）50 頁以下、野々村和喜「民事救済としての〈忘れられる権利〉について」同志社法学 68 巻 7 号（2017）971 頁以下。

18 なお、第一審では忘れられる権利は肯定されたものの、控訴審（東京高決平成 28 年 7 月 12 日）、上告審（最三決平成 29 年 1 月 31 日）では「忘れられる権利」という概念は否定されている。

19 伊藤英一「情報社会と忘却権：忘れることを忘れたネット上の権利」法学研究 84 巻 6 号（2011）165 頁以下、宮下紘「忘れられる権利：プライバシー権の未来」時の法令 1906 号（2012）43 頁以下、杉谷眞「忘れてもらう権利：人間の「愚かさ」の上に築く権利」Law&Practice7 号（2013）153 頁以下、上机美穂「忘れられる権利とプライバシー」札幌法学 25 巻 2 号（2014）59 頁以下、拙稿「「忘れられる権利」：忘れることを忘れた世界の新たな権利」コピライト 655 号（2015）44 頁以下、宮下紘「「忘れられる権利」をめぐる攻防」比較法雑誌 47 巻 4 号（2014）29 頁以下、宮下紘「ビッグデータ時代の「忘れられる権利」：プライバシー保護に日本なりの哲学を」Journalism 290 号（2014）94 頁以下、今岡直子「「忘れられる権利」をめぐる動向」調査と情報 854 号（2015）1 頁以下、石井夏生利「「忘れられる権利」をめぐる論議の意義」情報管理 58 巻 4 号（2015）271 頁以下、宮下紘『プライバシー権の復権：自由と尊厳の衝突』（中央大学出版部、2015）219-263 頁、宮下紘「「忘れられる権利」について考える」法学セミナー741 号（2016）1 頁以下、石井夏生利『個人情報保護法の現在と未来：世界的潮流と日本の将来像（新版）』（勁草書房、2017）87-116 頁、栗田昌裕「プライバシーと「忘れられる権利」」龍谷法学 49 巻 4 号（2017）305 頁以下、等。

法的根拠が他に存在しない場合、データ主体が個人データ処理に対する異議を述べ、かつ優先されるデータ処理の根拠がない場合か、ダイレクト・マーケティングへの異議を述べた場合、個人データが違法に取り扱われた場合、欧州法・加盟国法の遵守のためにデータ消去が必要な場合、16 歳未満（加盟国法によっては 13 歳以下）の情報社会サービスの提供に関連してデータ収集がなされた場合、が同条 1 項各号に列挙されている。

インターネット上に流布した情報は完全な消去が難しいことから、消すことが難しい入墨、「デジタル・タトゥー」と称される[20]。欧州では、この状況に対する危機感が以前から示されていた。欧州委員会の司法・基本権・市民権担当副議長である Viviane Reding は、「かつて言われたように「神は赦し忘れるのに、ウェブは決して忘れない」。だからこそ「忘れられる権利」は私にとってかくも重要なのだ（As somebody once said: “God forgives and forgets but the Web never does!” This is why the “right to be forgotten” is so important for me.）」と述べている[21]。このような思想を背景として、消去権ないし忘れられる権利は GDPR に導入された。

他の優れた先行研究でもすでに指摘されているが、消去権ないし忘れられる権利は、その提言時、強い反発を受けることとなった。その理由の一つには、ウェブからの情報の削除は、誰か（時には権力を有する側）にとって不利な情報を恣意的に削除することを許してしまい、ひいては歴史の修正にすらつながってしまうのではないか、という懸念がある。これに対して、欧州委員会は

20　この表現の初出は明らかではないが、2013 年の TED における Juan Enriquez による “Your online life, permanent as a tattoo” により広まったようである。Enriquez のプレゼンテーションは TED のウェブサイトで視聴できる（https://www.ted.com/talks/juan_enriquez_how_to_think_about_digital_tattoos（2019 年 11 月 5 日最終確認））。

21　V. Reding, Privacy matters: Why the EU needs new personal data protection rules; Brussels, 30 November 2010, available at http://europa.eu/rapid/press-release_SPEECH-10-700_en.pdf [latest access: 2019/11/05]. 忘却が赦しにつながるというのは、エレミヤ書 31 章 34 節の「(…) わたしは彼らの悪を赦し、再び彼らの罪に心を留めることはない」（日本聖書協会『聖書 新共同訳』）を意識したものであろうか。

忘れられる権利は「歴史の完全な消去の権利ではない」[22] と説明している。

このような反応の原因の一つには、「忘れられる権利」という表現の印象の強さがある。「忘れられる権利」はフランスの「忘却権（droit à l'oubli）」ないしイタリアの同じく「忘却権（diritto all'oblio）」を起源とすると言われる[23]。この「忘却」が、完全な過去の消去ととらえられたために批判を受けているが[24]、GDPR に定められる消去権の目的は情報の拡散の防止である。インターネットでいったん公開された情報の完全な削除は「一般的に不可能（generally impossible）」であるというのが GDPR も前提とするところであり、それでもなお削除すべきというスタンスでもない。

現代では、かつてと比較して情報収集がきわめて容易であり、インターネットを利用すると、数回のクリックで多くの情報が収集される。それをより加速するのが、検索エンジンの存在である。このため、これまでは「忘れられてきた」情報が、きわめて簡単に発掘されてしまう事態が起きるようになった。そこで、「より実務的（more practical）」な解決策として、検索エンジンの「リストから外す（delisting）」ことを考慮し、この「忘れられる権利」が設けられたのである[25]。

また、20 条に挙げられるデータポータビリティ権も、自己情報コントロール権の実現のための大きな要素である。データポータビリティ権とは、自身の

22 V. Reding, The European Data Protection Framework for the Twenty-first Century, 2 Int'l data privacy L. 1, 2012, p. 7.

23 F. U. Ahmed, Right to Be Forgotten: A Critique of the Post-Costeja Gonzalez Paradigm, 21(6) C.T.L.R. 175, 2015, p.176.

24 P. Hustinx, The Right to be Forgotten and Beyond: Data Protection and Freedom of Expression in the Age of Web 2.0, Oxford Privacy Information Law and Society Conference, June 12, 2012 を参照。なお、フランスの忘却権も、絶対的なものでは決してない。拙稿「フランスにおけるプライバシーと忘却：「忘れられる権利」の由来をたどって」金沢法学 60 巻 2 号（2018）123 頁以下。

25 European Network and Information Security Agency, The Right to be Forgotten: Between Expectations and Practice, 2012, p. 7, available at: https://www.enisa.europa.eu/publications/the-right-to-be-forgotten [latest access: 2019/11/05].

個人データを、管理者から一定のフォーマットで受け取り、他の管理者に移転する権利であり、自身の個人データを異なる管理者間で直接移転させる権利である。

現代社会では、個人に関する様々なデータを利活用し、例えば個別化医療のように、その個人のためにカスタマイズされたサービスの提供が、技術的には可能となっている。しかし、この種のサービスに対しては常にデータ主体となる個人のプライバシーの侵害への懸念と表裏一体の関係にある。

データポータビリティ権は、このような状況を背景としつつ、データ主体に個人データを還元することを保障する権利である。この権利を通して、データ主体は、これまでは様々なプラットフォーム等に分散していた自身のデータを集約・統合し、自分自身で管理できる。そして、データの利活用にあたっても、自身のニーズに応じて自分自身で選択した事業者に個人データを委ねることができる。

このような情報が膨大になれば、その管理は一個人では困難になるかも知れない。その時に、データ主体本人に代わってデータを管理・集約し、データ主体のニーズに従って第三者への提供などの利活用に携わるのが、後の章で言及される情報銀行（情報信託業務）である。

このように、データポータビリティ権は、今日の社会において情報が経済財として重要な位置を占めることを意識していることがわかる。その上でこの権利は、今日の社会の現状として、情報市場がアメリカの IT 巨人にほぼ独占されていることに対する対抗策として位置付けられていることも、きわめて興味深いところである[26]。

26　See, European Commission, Questions and Answers – General Data Protection Regulation, Brussels, 24 January 2018, available at https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_387 [latest access: 2019/11/05] (“The new right to data portability will allow individuals to move their personal data from one service provider to another. Start-ups and smaller companies will be able to access data markets dominated by digital giants and attract more consumers with privacy-friendly solutions. This will make the European economy more competitive.”).

③技術的手当て

上述のように、GDPR は個人情報の保護、そして自己情報コントロールを重視し、そのために新たな権利を明確に示している。その上で、技術的にもこれらの目的が達成されるよう、様々な定めを置く。

例えば、情報の流通に際して重要なセキュリティの強化のために、技術的安全性、認証制度等の整備を要求する。処理の安全管理について定める 32 条や、データ保護の認証に関する 42 条及びその認証機関について 43 条が、代表的な例として挙げられる。

そして、侵害が生じてしまった場合の対応についても明確に定めている。GDPR は、情報漏洩等の侵害が生じてしまった場合には、監督機関及び本人へ、迅速に通知・連絡する義務を定める（33 条、34 条）。データはいったん流出すると、詐欺被害や名誉毀損、財産的損失など様々な損害が生じる（前文 85 も参照）。そして、その対応が遅れるほどに、その被害は大きくなりがちである。それゆえ、GDPR は「迅速」な対応を義務として課している。

その他にも、GDPR では情報の管理者の義務の強化も定められる。25 条は、by design のデータ保護、by default のデータ保護について定める。これは 1990 年代にカナダで提唱された privacy by design に着想を得たもので[27]、GDPR においては、情報の管理者は、by design のデータ保護、by default のデータ保護の原則を採用した企業政策の策定と措置の実施が要求される。ここには、例えば個人データ処理の最小限化（minimising the processing of personal data）、個人データの即時仮名化（pseudonymising personal data as soon as possible）、個人データ処理の透明化（transparency with regard to the functions and processing of personal

27 See, A. Cavoukian, Privacy by Design: The 7 Foundational Principles, available at: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf (latest access: 2019/11/05). ここでは、①事後的にではなく事前に、②対症療法ではなく予防的、③システムのデザインに組み込まれたプライバシー、④ゼロサムではなく両立する関係の Positive-Sum、⑤ライフサイクルすべてを通した情報セキュリティ、⑥可視性と透明性、⑦ユーザー中心のプライバシーの尊重、が掲げられている。

data,)、データ主体のデータ処理監視（enabling the data subject to monitor the data processing)、情報管理者のセキュリティ構築及び改善（enabling the controller to create and improve security features）等が挙げられている（前文 78)。

より具体的には、管理者は情報処理の際に適切な技術的・組織的措置を講じなければならず、デフォルトとしてそれぞれ特定された目的の必要な範囲でのみデータ処理を行うことを確実にする措置を講じなければならない。

そして、これらの要請の実現を担保するため、データ保護影響評価（Data Protection Impact Assessment: DPIA）の実施や（35 条)[28]、データ保護責任者（Data Protection Officer: DPO）の設置（37 条）といった仕組みも準備されている。

さらに、個人データの漏洩など何らかの事態が生じた時の救済手段として、完全に独立した監督機関の設置が要求され（51 条)、その任務や権限、活動についても詳細な規定が置かれている（52〜59 条)。加えて、救済、法的責任及び制裁措置、損害賠償の権利についても明文の規定が置かれている（77〜79 条、82 条)。さらに、最も耳目を集めた一つである制裁金についても厳しい規定が設けられ（83 条)、データ管理者等の義務違反については、違反者の全世界の年間売上高の 2% か 1000 万ユーロのいずれか高い方、GDPR の基本原則違反については違反者の全世界の年間売上高の 4% か 2000 万ユーロのいずれか高い方が、制裁金として課されることになっている。日本では、例えばマイナンバー制度において、個人番号利用事務・個人番号関係事務等に従事する者が、正当な理由なく、業務で取り扱う個人の秘密が記録された特定個人情報ファイルを提供した場合に 4 年以下の懲役もしくは 200 万円以下の罰金（ある

28　これについて、29 条作業部会がガイドラインを示している。See, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 (Adopted on 4 April 2017, Revised and Adopted on 4 October 2017), available at: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 (latest access: 2019/11/05). 邦訳として、日本貿易振興機構（ジェトロ）海外調査部欧州ロシア CIS 課が、仮訳を公開している。https://www.jetro.go.jp/ext_images/world/europe/eu/gdpr/pdf/dpia.pdf（2019 年 11 月 5 日最終確認）を参照。

いはその併科）となっている（マイナンバー法 48 条）。これと比較しても GDPR の制裁金の額はきわめて大きく、情報を扱う企業にとっては重大な関心事項となることは容易に想像できる。

（2）EU 域内でのデータ保護に関するルールの一元化

GDPR は欧州における個人データの保護と流通のバランスを図るための規則である。すでに述べた通り、この前身として 1995 年のデータ保護指令が存在した。この指令を規則へ「格上げ」することにより、加盟国内においては単一ルールの直接的適用が可能となった。

これにより、かつて問題視されていた欧州域内における個人情報・個人データの保護レベルの差異の解消がはかられることとなった。さらに、監督機関の権限を明確化し（56 条）、その監督機関同士の協力、一貫性メカニズム（One-stop-shop）を導入することで（60〜62 条、63 条）、より実効的なシステムが構築された。

指令時代から、加盟国の監督機関と欧州データ保護監督官からなる 29 条作業部会が存在したが、これは法的拘束力を有する意見や勧告を示す組織ではなかった。そこで、GDPR では、拘束力のある決定を下す権限を有する欧州データ保護会議（European Data Protection Board; EDPB）が設置されている（68 条）。

（3）国際的な（対域外を含む）データ保護の詳細なルールの策定

最後に、GDPR が注目されるもう一つの理由として、第三国の管理者に適用される範囲（域外適用）が定められている点が挙げられる。

GDPR は、欧州域内に管理者や処理者が不在である場合であっても、一定の場合に域外適用を認めている（3 条 2 項）。①有償・無償を問わず EU 域内にいる個人に商品やサービスを提供している場合、② EU 域内での個人の行動を監視（モニタリング）している場合、である。この範囲は、前身であるデータ保護指令が定めていた、管理者が EU 域内に事業所を持つか、EU 域内の設備でデータ処理を行う場合よりも拡大している。

この規定により、我が国の事業者であっても、上述の状況に該当する場合には、GDPR が適用される可能性が生じる。すでに指摘した通り、GDPR は違反の場合の制裁金の額がきわめて大きいこともあり、事業者にとっては重大な関心事となっている[29]。

さらに GDPR は、加盟国ではない第三国へ個人データが移転する際に、欧州委員会が認定した十分なデータ保護の水準を確保していることを求める（「十分性認定」）。その基準は 45 条に列挙されており、この十分性認定がない第三国へデータ移転をする場合には、46 条に定められる適切な措置が講じられなければならない。2018 年 12 月現在では、日本は十分性認定を待つ段階である[30]。

多国籍企業においては、欧州域内のグループ企業から、域外のグループ企業へと情報を移転したいという要請もあり得る。このような企業グループ内での個人データ移転に関しては、拘束的企業準則（Binding Corporate Rules）を設け、各国の保護当局（Data Protection Authority; DPA）の承認を受ければ、個人データの移転が可能となることが定められた（47 条）。

このような十分性認定あるいは拘束的企業準則に従う個人データの移転以外は、GDPR は、第三国の行政機関からのデータ開示要求に対しても厳しい姿勢を示している（48 条）。これは、例えば Facebook 等の IT 企業がアメリカ国家安全保障局（NSA）等の国家機関に欧州市民の情報を提供していたように、欧州市民のプライバシーという基本権が保護されないような行為への対抗措置でもある[31]。ここにも、上に指摘した、大西洋を挟んだ戦争（transatlantic war）の

29　本邦で個人情報の保護に関する種々の業務を担当する個人情報保護委員会も、これに関心を寄せ、「各組織・企業等の業務への影響について、あらかじめ備えておく必要があ」るとして、ウェブサイトで GDPR に関連する資料の仮訳の公開などを行っている。https://www.ppc.go.jp/enforcement/infoprovision/laws/GDPR/（2019 年 11 月 5 日最終確認）を参照。

30　その後、2019 年 1 月 23 日、日本は十分性認定を得ている。

31　See, Panel for the Future of Science and Technology, How the General Data Protection Regulation changes the rules for scientific research, July 2019, pp. 13-14; available at: http://

一端を看取することができる。

結びに代えて

GDPR は、欧州という一大経済圏の法規則ということもあり、今後のデータ市場において無視することはできない大きな位置を占めるものである。

紙幅の制約からきわめて雑駁な解説に終始せざるを得なかったが、GDPR が欧州の価値観に深く根差したものであり、個人データの保護という側面から、基本的価値である個人の尊厳の保護を意識していることを描けていれば幸いである。

データの利活用という観点から見れば、GAFA に代表される情報企業を擁するアメリカの立場からは、当然データの取得や流通は促進されるべきとの流れになろう。しかし、それに対する反発も当然あり得るところである。とりわけ欧州がアメリカとこの点で対立するのは、本稿で述べた通り、根本的な価値観で異なる視点を有するからである。この点を無視しては、相互理解は進まず、溝は深まるばかりとなろう。

翻って我が国でも、データ利活用による経済的インパクトを重視し、只管その促進を叫ぶような、いささか乱暴にも感じられる論調も、時には見られる。例えば 2013 年の JR 東日本による Suica 乗降履歴データの販売に対して、消費者から「気持ち悪い」と反発が出たが[32]、これはなぜなのか。感情的反応にも思われるが、では、その感情はどこに根差すものか。新たな制度設計に際しては、そこまで丁寧に掘り下げることが必要になろうし、それはアカデミズムの責務の一つであろう。

スコット・ギャロウェイは GAFA を黙示録の四騎士に譬えたが、黙示録は

www.europarl.europa.eu/RegData/etudes/STUD/2019/634447/EPRS_STU(2019)634447_EN.pdf (latest access: 2019/11/05). 欧州司法裁判所の 2013 年の Schrems 事件（C-362/14）も参照。

32 「「Suica 乗降履歴販売」失策の教訓：パーソナルデータ活用 6 つの勘所」日本経済新聞（2013 年 12 月 19 日付）。

終末と、そして新たな天地創造を描くものである。情報とデータの世界には、すでに四騎士が現れた。今後、いかなる新たな天地となるのであろうか。

> わたしはまた、新しい天と新しい地を見た。最初の天と最初の地は去って行き、もはや海もなくなった。更にわたしは、聖なる都、新しいエルサレムが、夫のために着飾った花嫁のように用意を整えて、神のもとを離れ、天から下って来るのを見た。（21:01-02）
>
> （…）
>
> 彼らの目の涙をことごとくぬぐい取ってくださる。もはや死はなく、もはや悲しみも嘆きも労苦もない。最初のものは過ぎ去ったからである。（21:04）
>
> ――ヨハネの黙示録（日本聖書協会『聖書 新共同訳』）

＊ 本稿は、信託協会信託研究奨励金の成果の一部である。

個人情報保護法と GDPR について

金沢大学大学院法務研究科　長　瀬　貴　志

はじめに

この度，金沢大学法学類と第一東京弁護士会司法研究委員会信託法研究部会が共催する本シンポジウムにお招きいただき感謝するとともに，これより，我が国の個人情報保護法と GDPR について，我が国の個人情報保護法をベースに，GDPR との異同を説明する。

１．個人情報保護法と GDPR の関係

まずは個人情報保護法を説明するが，同法の目的については，同法の第１条に記載されており，「高度情報通信社会の進展に伴い個人情報の利用が著しく拡大していることに鑑み、個人情報の適正な取扱いに関し、基本理念及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め、国及び地方公共団体の責務等を明らかにするとともに、個人情報を取り扱う事業者の遵守すべき義務等を定めることにより、個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする」と非常に長い内容になっている。これは要するに，個人情報に関する個人の権利・利益の保護と、個人情報の有用性とのバランスを図ることを目的とした法律，という内容である。

これに対し，GDPR は，「個人データの処理に関する自然人の保護に関する規則および個人データの自由な流通に関する規則」とされている。

このように両者の内容を比較してみると，いずれもその目的はほぼ同じということができる。

このように，目的を同じくする規定となっているのは，いずれもいわゆる

OECD８原則に基づき，制定されているからである。OECD８原則とは，

・収集制限の原則（Collection Limitation Principle）
・データ内容の原則（Data Quality Principle）
・目的明確化の原則（Purpose Specification Principle）
・利用制限の原則（Use Limitation Principle）
・安全保護の原則（Security Safeguards Principle）
・公開の原則（Openness Principle）
・個人参加の原則（Individual Participation Principle）
・責任の原則（Accountability Principle）

といったことを内容としているが，これらの原則に基づき，各国や各地域が，個人情報の取扱いに関する法令を制定していること，そして個人情報の取扱いにつき，各国や各地域において，戦略的に利用していきたいというニーズがあること，このような共通する背景から，我が国の場合には個人情報保護法が制定され，EU においては GDPR が制定されたものであり，いわば，OECD８原則を親とした兄弟のような関係といえる。

ただ，欧州においては，我が国よりも個人情報の取扱いに関しては先んじており，いわば兄になり，我が国は弟のような関係となる。我が国に個人情報保護法が制定された 2003 年（平成 15 年）において，衆議院の記録を見ても，「1995 年に欧州連合で採択された『ＥＵデータ保護指令（Directive 95/46/EC）』に対して，日本としても何らかの対応が必要である」との認識の下に，個人情報保護法が我が国で制定されている。ただ，その時点で，個人情報漏えいに関する事件も頻発しており，そういった事件も法律制定の近因となったとも言われている。

ちなみにアメリカにおいては，個人情報とは異なるプライバシーという概念で個人に関する情報を扱っており，取扱いが異なることに注意が必要となるが，今回はこの点に関しての深入りはしない。

２．個人情報保護法と GDPR の相違点（総論）

このような兄弟関係にある個人情報保護法と GDPR だが，大きく 7 つの違いがある。

まずは保護の範囲である。個人情報保護法においては，「生存する個人で特定の個人を識別できるもの」がメインとなっているのに対し，GDPR では，「識別された，または識別できる自然人に関する情報」となっており，オンライン識別子，たとえば，クレジット番号やウェブサービスを利用するときに作成したユーザ名も含む内容となっている。この点は個人情報保護法の改正の検討においても協議された模様だが，我が国では採用されなかった。

次に，同意の有効要件である。個人情報保護法には，特に明記されていないが，GDPR においては，同意の任意性，特定性，明白性など，同意が有効となるための要件がかなり細かく記載されている。この点については後ほど詳細に説明するが，かなり厳しい内容となっていることに注意が必要である。

そして，データ主体が提供すべき情報の点である。個人情報保護法には何ら明記されていないが，GDPR においては，管理者の名称など，特定の情報の提供義務が規定されている。

また，越境移転規制でも若干の違いがある。いずれにおいても，原則として越境移転を認めず，ただ，一定の要件を課した上で，越境移転を認めているが，個人情報保護法においては，我が国と同等の保護水準があると個人情報保護委員会規則で定めた場合や同意などを要求しているのに対し，GDPR においては，十分性認定や同意などを要求している。

そして，域外適用についても大きく異なっている。個人情報保護法も GDPR も，一定の範囲で域外適用を規定しているが，個人情報保護法は現地の監督当局がルールを適用することを想定しているのに対し，GDPR においては，EU が直接 GDPR を適用することを想定している。この点に，欧州の個人情報保護に対する強い想いを感じることができる。

さらに，センシティブ・データについて，個人情報保護法は，人種や信条を

対象としているのに対し，GDPR では，人種，政治的見解，宗教的信念，遺伝子データなど，個人情報保護法と重なる部分とそれ以上の部分がある。

そして，救済・制裁金である。この点が極めて大きな影響力をもっており，個人情報保護法においては罰金を科すことも想定しているが，あくまで現地のルールの適用を想定しているのに対し，GDPR においては，EU 独自の巨額の制裁金を想定している。具体的には，最大で 2000 万ユーロ（約 25 億円）又は当該会計年度の全世界年間売上高の 4%の，どちらか高い方を制裁金として科すことが規定されている。

最後に，GDPR においては，一定の範囲ではあるが，未成年者の年齢の取扱いや，ヘルスケアデータの取扱いなど，特定の事項については，加盟国の裁量により異なる内容となる点に注意が必要である。特にドイツは GDPR よりも厳しい規制を設けていることもあり，注意が必要である。

以上が，個人情報保護法と GDPR の，大きな相違点である。

３．個人情報保護法と GDPR の相違点（各論）　－個人情報保護法における個人情報の取扱いをベースに－

（１）異同を検討する視点

では次に，個人情報保護法と GDPR の相違点について，細かく説明する。これから先は，個人情報保護法における個人情報の取扱い，すなわち，個人情報保護法の対象となる個人情報等の対象が何か，その取扱主体は誰か，個人情報等の取得はどのように行うか，管理はどのように行うか，その利用や提供，開示はどのように行うか，そして漏えいが生じたときにどうすべきか，といった観点から説明する。

（２）個人情報等の対象

まず，個人情報等の対象であるが，この点，個人情報保護法においては，「生存する個人に関する情報であり，かつ，氏名などにより特定の個人を識別できるもの，または，個人識別符号が含まれるもの」が対象とされている。こ

のように，一般用語としての個人情報全般ではなく，あくまで，生存している自然人に関するものであり，かつ，個人識別性を有するものが対象となっている。具体的には，本人の氏名や生年月日，住所はもちろん，防犯カメラに記録された情報などで本人が識別できる映像情報，特定個人を識別できるメールアドレスが特定の個人を識別できるものの代表例であり，また，個人識別符号の例としては，マイナンバーや運転免許証番号，DNA 塩基配列，指紋，静脈の形状などといったものが挙げられる。

そして，このような個人情報に加え，要配慮個人情報というものが規定されている。これは，「本人に対する不利益が生じないようにその取扱いに特に配慮を要するもので，政令で定められているもの」で，具体的には，人種，信条，社会的身分といった憲法にも規定されているようなものの外に，身体の障害や知的障害，健康診断結果，逮捕歴や保護処分歴などといったものが対象となる。

このように，個人情報保護法においては，個人情報そのものの外に，要配慮個人情報を加え，「個人情報等」として，その保護の対象としている。

このような個人情報保護法と比較し，GDPR においては，先に述べたとおり，「オンライン識別子」といったものもその保護の対象となっている。また，個人情報保護法にいう「要配慮個人情報」に相当するものとして，「センシティブ・データ」というものがあるが，要配慮個人情報よりも概念が広く，例えば，健康に関するデータについては，個人情報保護法では「機能の障害」という限定の範囲内であるものの，GDPR ではそのような限定はなく，データ主体の健康状態に関するすべてがその保護の対象となっている。また，性生活や性的嗜好に関するデータも，個人情報保護法には含まれていないものの，GDPR には含まれている。したがって，つい先日，ネット上でちょっとした騒ぎになった，TSUTAYA の店員が，自分の好きなアーティストを批判されて立腹し，その批判した客の「名前から性癖まで暴露可能」と書き込んだ件に関し，仮に性癖をアップロードしていたら，GDPR では制裁の対象となることに

なる。もちろん，我が国においても名誉毀損やプライバシー侵害の問題は出てくるが，それを個人情報として明確に法令にて規定している点が，大きな違いとなっている。

以上が個人情報等の対象の異同である。

（3）個人情報の取扱主体

次に個人情報の取扱主体であるが，個人情報保護法では，「個人情報データベース等を事業の用に供している者」がその取扱主体として，個人情報保護法の規制の対象となっている。そして，ここにいう「個人情報データベース」とは，「個人情報を含む情報の集合体であって，検索できるように体系的に構築したもの」と定義されている。また，「事業の用に供する」とは，反復継続して社会的に事業と認められるものであって，営利性や法人格の有無は問われないとされている。要するに，会社で顧客名簿を作った場合，それをもって個人情報取扱事業者となるし，同窓会が会員名簿を作ったときも，個人情報取扱事業者となる。なお，平成 27 年の個人情報保護法の改正前においては，5000 人以上の個人情報の取扱いがないと規制の対象とされていなかったが，同年の改正により，1 人でも個人情報を取り扱うと，この個人情報取扱事業者とされ，個人情報保護法の対象となったので，この点は注意を要する。したがって，小職のような地方の弁護士でも，以前は個人情報取扱事業者ではなかったものの，今は個人情報取扱事業者になってしまい，いろいろと気を付けないといけない立場になってしまった。

このような個人情報取扱事業者という取扱主体に加え，個人情報保護法は，匿名加工情報取扱事業者も規制の対象としている。これは，「匿名加工情報データベース等を事業の用に供している者」のことであるが，ここで注意すべきは，これはあくまでこのような匿名加工情報を作成したものではなく，匿名加工情報の提供を受けて事業の用に供している者が対象となっているという点である。では作成者は個人情報保護法の対象外かというとそうではなく，個人情報取扱事業者として取り扱われうることとなる。

以上が個人情報保護法上の個人情報等の取扱主体であるが，GDPR においては，「管理者」と「処理者」という概念が登場する。ごく大雑把にいえば，管理者は個人情報保護法にいう「個人情報取扱事業者」に，処理者は，個人情報取扱事業者の委託先に相当すると理解することができる。GDPR がこのような観点から主体を区別したのは，実際上，それぞれにおいて役割が異なることから，その義務内容もおのずと異なってくる，それに対応した区分ということである。

（4）個人情報の取得

次に個人情報の取得の場面であるが，個人情報保護法では，個人情報取扱事業者において，3 つの義務が適用される。まずは適正な取得であること，次に，利用目的の特定をし，通知及び公表をすること，最後に，第三者から提供を受ける際の確認や記録，保存義務があること，の以上である。ここでは，ひとまず，適正な取得という点について説明する。

これは別に難しい話でもなく，極めて常識的な内容であり，偽りその他不正な手段による個人情報の取得を禁止する，というもので，取得に際しては，原則として，同意に基づき，直接取得することとされている。

また，適正な取得という点に関し，要配慮個人情報の原則取得禁止が要求されている。これは，本人の知らないところで要配慮個人情報が取得され，差別的な取扱いがされることを未然に防止するという観点から要求される義務である。

今ほど，個人情報は本人の同意に基づき取得することが原則であると説明したが，実は，ここにいう「同意」というのが実は厄介なものであり，ここが GDPR との大きな相違点ともなっている。すなわち，個人情報保護法では，どのような同意があれば有効であったり適切であったりするか，という点に関して，何らルールが設けられていないものの，GDPR においては，有効な同意につき，極めて細かくルール化されている。簡単に説明すると，GDPR においては，同意には，任意性，特定性，明確性などが要求されており，例えば，同意

者と同意を受けた者の間のパワーバランスが偏っている場合には，任意性がないとして同意が無効となったり，また，どのような情報についての同意であるかが特定されていないということであれば，それをもって無効とされる，というものである。これに対し，我が国ではこのようなルール化はされておらず，場合によっては特定性を満たさない，いわゆる包括同意も有効ということになる場合もある。小職は，以前勤務していた総務省において，通信の秘密を取り扱っていたが，通信当事者の同意の有効性をどのように考えるか，これは非常に悩ましい問題であった。その点，GDPR においては，ルール化されているので，行政の担当者としてはやりやすいだろうな，という思いがある。ただ，あまりに硬直化していて，個人情報保護法における適切な利活用という側面が害される可能性もあることから，そのバランスをどう取っていくかが非常に難しく，かつ，重要となると思料する。

このように，同意をもって個人情報の取得が適法化されるという点は，GDPR も個人情報保護法も同じなのだが，その同意の有効性については，これほどまでに異なっている。これが何を意味するかというと，我が国の感覚で有効な同意を取ったとしても，GDPR 上はアウトになる可能性がある，ということを十分踏まえておく必要があるということである。したがって，GDPR の適用の可能性がある場合には，同意の取り方に注意を要することを認識する必要がある。

（5）個人情報の管理

次に，個人情報の管理であるが，個人情報保護法においては，2 つの規制がある。すなわち，情報の安全管理に関する規制，次に，データ内容の正確性の確保等に関する規制である。

まず，情報の安全管理に関する規制についてであるが，これは 3 つのものを含んでいる。すなわち，安全管理措置義務，従業員の監督義務，そして委託先の監督義務である。ただ，これらの義務について，事業者の事業規模にかかわらず，完全にフルバージョンのものを適用すると，事業規模によっては，あま

りに過大な要求を事業者にすることになりかねないことから，従業員 100 名以下の個人情報取扱事業者においては，組織的・人的・物理的・技術的安全管理措置を内容とする安全管理義務がかなり簡素化されている。

また，重要であるのが，委託先の監督義務である。従業員の監督義務は，事業者として，まだ目の届くところなのでイメージしやすいが，委託先となると目が届きにくく，それが個人情報の漏えいの原因の一つといえる。記憶に新しいところでは，ベネッセの個人情報保護の漏えい事件があったが，あの事件が典型例になる。このような点からも委託先の監督義務は非常に重要となる。

以上のような情報の安全管理に関する規制に加え，データ内容の正確性の確保も要求されている。すなわち，データ内容が正確であるように努めなければならないという点と，あと一つ，不要な個人情報は消去するよう努めなければならないという点である。特に不要な個人データについては，これを保持していても何もメリットがなく，むしろ漏えいの可能性を高めるだけなので，速やかに消去する，というのが，事業者にとってよい対応となると思料する。なお，いずれも努力義務とされており，法的義務とまではなっていない。

以上，個人情報保護法の説明である。GDPR においても，正確性の確保や不要なデータの消去が規定されているが，いずれも法的な義務とされている。この点においても，GDPR は厳しい義務を取扱主体に課していることとなる。

（6）個人情報の利用・提供・開示等

次に，個人情報の利用や提供，開示等であるが，個人情報保護法では，利用目的の範囲内での利用が可能であること，利用目的の範囲の変更は一定の範囲であれば可能であること，個人データの第三者への提供は，原則として事前の本人の同意が必要であること，個人情報の第三者への提供については提供先に関する記録の作成・保存義務があること，本人からの開示請求においては，原則として開示しなければならないこと，以上のことが定められている。

特に注意が必要となるのが，第三者への提供に際しての本人の同意であるが，これは，個人情報の取得に関する本人の同意と同様，特に要件が定められ

ているわけではないものの，その有効性については，注意しなければならないことも同様である。また，ここにいう「第三者」には，委託先は含まれない。従って，委託先に提供する場合には，本人の同意は不要となる。ただし，個人情報取扱事業者においては，委託先の監督義務があるので，漏えいした場合の責任は生じうることになる。なお，人の生命，身体又は財産の保護のために必要がある場合で，本人の同意を得ることが困難な時などにおいては，第三者への提供が可能となっている。

あとはトレーサビリティの関係で，提供先の記録の作成・保存義務が改正法で導入された。これは受領した時と同様，個人情報の追跡可能性を担保するための規定である。なお，本人への提供の場合については，解釈論上，作成・保存義務はないものとされている。

以上が個人情報保護法であるが，GDPR の方では，アクセス権や訂正権の外，削除権（消去権）というものが規定されている。この削除権（消去権）はいわゆる「忘れられる権利」として賑わった権利なのだが，規定上，「忘れられる権利」という文言はなく，あくまで削除権（消去権）となっている。

また，データポータビリティ権というものがあり，他の事業者へのサービスの乗り換えの際に個人データ主体が受け取る，または事業者同士で個人データのやりとりをしてもらうことができる，という内容の権利が規定されている。これは例えば，SNS やブログで別のサービスに引っ越しをする際に，非常に便利な権利である。

そして，プロファイリングを含むもっぱら自動処理に基づく決定をされない権利というものもある。これは，例えば契約のキャンセルや社会福祉に関する受給資格につき，自動処理のみに基づき決定されないことが具体例として挙げられている。

なお，取扱主体で扱うのが適切かもしれないが，GDPR においては，データ保護責任者（DPO）の配置が求められる場合がある。これは，いわば事業主の内部における独立した監視役のようなもので，その地位は，企業の最高経営層

に個人情報の取扱いに関して直接進言できる独立した立場であり，それゆえに，経営層の兼任ができないこととされている。

このデータ保護責任者は，GDPR の監督当局の問合せ先でもあり，高い専門性が要求され，その地位は非常に重要で，その責任も重大である。

この概念は，もともとドイツ法において採用されていたものであり，それが今般の GDPR 制定において採用されたものである。なお，個人情報保護法には，このような概念はない。

（7）個人情報等の漏えい等

最後に，個人情報等の漏えい等である。当然，個人情報等の漏えいは最も避けなければならないことであるものの，そもそも漏えいとはどのようなことか，また，それ以外に問題となる事象として，どのようなものがあるかを押えることが肝要である。漏えいとは，個人データが外部に流出することであり，内部に留まっている限り，漏えいとはならない。また，漏えい以外には，滅失や毀損がある。滅失とは，個人データの内容が失われることを意味し，毀損は，個人データの内容が意図しない形で変更されたり，利用不能な状態になることを意味する。そして個人情報保護法上，これらを合わせて，「漏えい等」という言い方をする。

ではこのような漏えい等が生じた場合に，事業者はどうしなければならないか，であるが，まずは被害の拡大の防止が必要となり，それに続いて調査及び原因の究明，影響範囲の特定，再発防止策の検討及び実施，影響を受ける可能性のある本人への連絡，そして事実関係及び再発防止策等の公表が必要となる。

ちなみに，漏えい等について，このような義務が課せられているが，漏えい等について，故意過失は関係なく，例えば，郵便配達員が誤って郵便物を違う人に配送した，いわゆる誤配送といったものも，当然にこのような義務を生じさせることとなる。

そして，個人情報保護委員会への報告義務もあるが，これは努力義務となっ

ている。個人情報保護委員会としては，当該報告を受けて，事例集を作成し，今後同様の漏えい等を国民が生じさせないよう，注意喚起をするために，このような報告を受けることとなっている。

以上は，個人情報保護法上の，漏えい等をした事業者の義務だが，もちろんそれ以外でも，民事上の責任，刑事上の責任，そして社会的な責任は当然，個人情報保護法とは別に生じることとなる。

他方，GDPR においては，データ侵害という概念で漏えい等を扱っており，「個人データに対する偶発的又は違法な破壊，滅失，変更，許可されていない開示又はアクセスをもたらすセキュリティ侵害」につき，72 時間以内の監督当局への通知，データ主体への遅滞のない通知がいずれも法的義務となっている。

なお，その対象は，個人情報保護法の漏えい等と重複することがほとんどのようだが，例えば，病院内で患者の重要な医療データが利用できなくなった場合でも，個人情報保護法では漏えい等の問題でないものの，GDPR においては，これも「データ侵害」として取り扱われる点が大きな違いである。

（8）越境移転

なお，インターネットの発達に伴い，情報がある国にのみ留まるということは皆無に等しく，その越境移転が常に問題となる。個人情報の越境移転について，両者は同様に第三国への移転を原則として禁止しているが，我が国と同等水準にあると個人情報保護委員会が規則で定める国においては越境移転が可能であることと同様に，GDPR においても，「十分性」要件を充たす国に対して，越境移転を可能としており，GDPR 上，我が国も十分性獲得に向けて鋭意努力している状況である。十分性が認められないと，EU 内にある日系企業が我が国に個人情報を移転させることが極めて困難となり，事業活動に大きな支障を生じかねない。その意味で，十分性の獲得は，我が国の経済活動にも大きな影響を及ぼす，非常に重要な作業である（なお，平成 31 年 1 月 23 日付けにて，我が国の十分性認定がなされた。）。ただ，仮に十分性を獲得したとして

も，欧州司法裁判所において，当該十分性認定が否定される可能性も残されており，例えば米国は，欧州との間のセーフハーバー協定による十分性認定がされていたのだが，欧州司法裁判所により当該十分性認定が否定されたという痛い目にあった経緯もある。その意味で，十分性を獲得したことで終わりではなく，絶えず EU の動向に注意する必要がある。

4　さいごに

以上，駆け足で個人情報保護法との比較で GDPR を説明してきた。同じ制度理念であっても，その国や地域における個人情報のアプローチは様々であり，GDPR は総じて我が国における個人情報保護よりも厳しく個人情報保護を図っている。しかしそれは個人データの積極的な利活用を阻害することにもなりかねず，どちらが正解ということはない。制度設計として，その両者をどうバランスを取っていくかが非常に重要であり，また，運用においても，そのような観点を持つことが肝要である。

さらに，説明したとおり，GDPR が我が国にも大きな影響を及ぼしかねないということもあり，弁護士としても，依頼主が GDPR に引っかかる活動をしないか，たえず注意喚起をしていく必要があることも理解できたと思う。その意味で，GDPR は決して他人事ではない，という点についても，注意していただきたい。

パネルディスカッション
「情報の信託的管理と弁護士の役割」

第一東京弁護士会司法研究委員会信託法研究部会*

第 1 シンポジウムの共同開催と本稿の目的

2018 年 12 月 15 日、金沢大学法学類と第一東京弁護士会司法研究委員会信託法研究部会（以下「当部会」という。）は、「GDPR と情報信託の交錯」と題するシンポジウムを共同開催した。

当部会は、このシンポジウムにおいて、「情報の信託的管理と弁護士の役割」をテーマにパネルディスカッションを実施した。

本稿は、当部会がこのパネルディスカッション実施にあたって研究した成果を講演録として発表することを目的とするものである[1]。

第 2 当部会の活動と GDPR

当部会は、これまで信託の活用の可能性に関する研究を行ってきており、書籍発行、雑誌掲載の形で成果物を発表してきた[2][3][4]。その研究において、医療情報管理における信託的視点の有用性を継続的に取り上げて研究対象とし、信認の下に他人の情報を預かるという「情報の信託的管理」の視点が有用であると

---

* 部会長・多賀亮介、副部会長・伊藤英之、菅野智巳、関由起子、田畑俊治、永島太郎

1 シンポジウムは 2018 年 12 月 15 日に実施されたものであるが、本稿は 2019 年 1 月 23 日に発行した EU と日本における相互の十分性認定承認等のその後発生した重要な事象を踏まえて加筆修正している。

2 第一東京弁護士会司法研究委員会信託法研究部会『社会インフラとしての新しい信託』（弘文堂、2010）

3 第一東京弁護士会司法研究委員会信託法研究部会『持続可能な社会を支える弁護士と信託 - 医療クラウド、産学連携、まちづくり -』（弘文堂、2012）

4 第一東京弁護士会司法研究委員会信託法研究部会『信託が拓く新しい実務 -6 つのケース解説と契約条項例』別冊 NBL156 号（商事法務、2016）

の考えを示してきた[5]。

現在、情報処理技術の発達によって、個人に関するデータを大量に集積したうえで利用することが可能となりつつある。経済やマーケティングの分野でも、個へのアプローチ及び集団処理から個の分析への変換が喧伝され、統計手法と脳科学の知見が結合し、膨大な未整理の情報から個人の属性との結びつきを「発見」していくことに経済的な価値が付与されている。単体では無価値に近い未整理の個人データが集積されることで価値を認められ、宝の山と呼ばれている。そうすると、未整理な膨大な情報を、誰が集めるか、保持するか、使っていいのか、が重要となる。これらのデータの対象者は生活者（または消費者）である。自分の生活・健康・嗜好・交友関係等の生活全般にわたる情報を他に委ねることをよしとするのか。一方で、生活上の便益ももはや捨てることはできない。情報の大量保有者に対して個人が声をあげることを期待することは困難であり、運用の目安となるルールを検討する必要がある。そのためには、信認と制度との枠組みを本質とする法的制度である信託の視点による検討が有益と考えて検討をすすめてきた。

この研究をさらに進めるに当たって、特に当部会の関心事となっていたのは、EU で 2018 年 5 月に施行された GDPR（General Data Protection Regulation 欧州一般データ保護規則）の日本企業への影響であった。GDPR は、域内のデータ管理者及び処理者だけにとどまらず、一定の場合（域内のデータ主体に対する商品又はサービスを提供する場合等）における域外のデータ管理者及び処理者にも適用される。さらにその規制内容は、データ管理者・処理者がデータ主体の権利を侵害した場合、最大で、2000 万ユーロ又は前年度の全世界総売上高の 4% の制裁金が科されるという厳しい規制になっている。そのため、日本企業にもその対策が求められていることが度々報道されているが、実態としては十分対策が進んでいないことが懸念される。

5　第一東京弁護士会司法研究委員会信託法研究部会・前掲注 (2)6 頁、同・前掲注 (4)10 頁。

第 3 事例検討

1 検討方針

そこで、当部会は、これまでの研究成果を踏まえ、GDPR の施行に伴い、想定すべき事例を 3 つ設定し、これらの事例から生ずることが想定される問題に対応するに当たって必要な視点として、行政、企業、個人のそれぞれの立場から、このケースにおいて生じ得る法的問題を検討した。具体的には、行政として EU のデータ保護監督機関は制裁金を課すことができるか、企業としてどのような対策を取るべきか、個人としてどのような権利侵害を主張できるかを検討した。

2 事例①「情報銀行」

(1) 想定事例

一つ目の事例は、情報銀行に関する事例である。

【事例①】
内閣府及び総務省が進めている情報銀行・情報信託の構想の活用事例の一つに、観光客向けのサービスがある。この活用事例で取り扱われる観光客データには、欧州居住者のパーソナルデータが含まれる場合があり、GDPR の適用が問題になるか？

(2) 情報銀行・情報信託

内閣府や総務省の構想では、情報銀行・情報信託という仕組みを作って、データの利活用を促進することを目指している。情報銀行とは、「パーソナルデータストア」（PDS）という仕組みを活用し、個人に関する様々なデータを預かって管理するとともに、必要に応じて、個人データを活用したいと考える事業者などに提供するものである。その構想は 2017 年 3 月の内閣官房「データ流通環境整備検討会」の AI、IoT 時代におけるデータ活用ワーキンググループの中間取りまとめで公表された。これを受け、2017 年総務省「情報通信審議会 情報通信政策部会 IoT 政策委員会 基本戦略ワーキンググループ」の

「データ取引市場等サブワーキンググループ取りまとめ」において、一定の要件を満たした情報信託機能を担う者が必要なのではないかという視点が取り上げられた。2017 年 11 月からは、総務省と経済産業省が合同で「情報信託機能の認定スキームの在り方に関する検討会」を開催し、2018 年 6 月、情報信託機能を担う者の認定基準、認定の仕組み等に関する指針が公表された。2018 年 10 月の報道[6]によると、総務省と IT の業界団体（一般社団法人日本 IT 団体連盟）が開催した情報銀行の事業者認定の説明会に 200 の企業の参加があったということであり、企業が情報銀行構想に対して高い関心を寄せていることが分かる。その後、2109 年 6 月、上記日本 IT 団体連盟の情報銀行推進委員会は、情報セキュリティやプライバシー保護対策等に関する認定基準に適合した「情報銀行」の認定を開始した[7]。この構想の中では例えば観光領域でのデータ活用が想定されているが、観光客データには欧州居住者のパーソナルデータが含まれる場合がある。そうするとこの構想をもとにしたデータ活用事例において日本所在の企業が GDPR の適用を受ける可能性がある。

(3) 行政の視点（制裁金問題）

GDPR 違反が認められる場合、監督機関は、制裁金を科すか否かを判断するが、その際、加盟国間で均等であること、個々の事案の評価に基づき、効果的、比例的かつ抑止的な対処を実現するために用いられることなどの原則を GDPR83 条 1 項及び「規則における制裁金の適用及び設定に関するガイドライン」は定めている。また、制裁金の額を判断する場合、考慮すべき事項として、①違反の性質、重大性、期間並びに損害の程度、②違反行為の故意又は過失、③データ主体が被った損害を軽減するためにとられた対応等、11 項目が挙げられている（83 条 2 項）。

GDPR の前身の EU データ保護指令時代に、加盟国のデータ保護当局

6　2018 年 10 月 19 日日本経済新聞 電子版「『情報銀行』説明会に 200 社 データ流通の枠組み始動」

7　2019 年 6 月 26 日日本経済新聞 電子版「三井住友信託銀、情報銀行 1 号に　IT 連が認定」

（DPA）から制裁金が科された事例としては、次の表に記載されたケースなどがある[8]。

国	違反行為	制裁金
ドイツ	スーパーマーケットが社員の私生活、財政状況等を体系的に監視し、データ保護責任者を任命しなかった	146万€（約1億8980万円）
イタリア（2017）	国際送金を行っている企業5社が、イタリアから中国への個人データ移転を本人の同意なしに行った	11万€（約1430万円）
スペイン（2013）	インターネット企業がプライバシーポリシー変更において、利用者に明確な情報提供をせず、その権利行使を妨げた	90万€（約1億1700万円）

日系企業についても、ソニーの子会社であるソニー・コンピュータエンタテインメント・ヨーロッパは、同社が管理・運営するプレイステーション・ネットワーク・プラットフォームがハッカーの侵入を受けて、数百万人規模の顧客の氏名、住所、E メールアドレス等が漏洩した件について、2013 年、イギリス当局から 25 万ポンド（約 3500 万円）の制裁金を科されている。当局は、制裁金を科した根拠として、セキュリティソフトのアップデートなど、不正処理を防ぐための適切な技術的手段がとられていなかったこと等を挙げている[9]。

また、GDPR 施行後、GDPR が日本企業に初めて適用されるかもしれないと報道されたことがある[10]。フランスのホテル予約サイトで不正アクセス事件が起き、同サイトに業務委託していた国内ホテル宿泊者の個人情報が漏えいしたことが発覚したという事案であった。この件では、委託元の多くの国内ホテルが、GDPR の規定に従い、個人データ侵害が発生した事実を監督機関に対し、72 時間以内に通知した（33 条）。

このような動向をみていくと、事例①、すなわち、欧州からの観光客向けの

8　宮下紘『EU 一般データ保護規則』（勁草書房、2018）303-305 頁
9　森大樹『日米欧個人情報保護・データプロテクションの国際実務』別冊 NBL162 号（2017）220-221 頁
10　2018 年 7 月 9 日ダイヤモンドオンライン（https://diamond.jp/articles/-/174282）

情報銀行サービスで GDPR に違反する行為があった場合も、巨額の制裁金が科される可能性は考えられる。

(4) 人権行使の視点

人権行使の視点からみると、GDPR17 条には、消去権（right to erasure）・忘れられる権利（right to be forgotten）と呼ばれる権利が定められている。これはデータ主体（data subject）が管理者（controller）に対して個人データを消去させる権利であり、管理者は一定の例外事由がある場合を除いて遅滞なく消去する義務があるとされている。この規定に基づく権利行使により、データ取扱に関するデータ主体の意思が適切に反映されることが期待される。

また、EU においては、忘れられる権利を認めた裁判例として、グーグルスペイン事件の 2014 年 5 月 13 日 EU 司法裁判所先決判決で検索結果の削除請求を認める判決があったことも知られている[11]。GDPR の消去権・忘れられる権利に関する規定が域外適用されるかという問題があるが、この点については、2019 年 9 月 24 日、EU 司法裁判所が「EU 域外での適用は義務ではない」との判断を示したとの報道がある[12]。

これに対して、日本の個人情報保護法で保護される個人情報の範囲は「特定の個人を識別することができるもの」（2 条 1 項）とされていて、GDPR の個人データ（personal data）に比べて狭く、また、利用目的違反又は不正取得の事実が判明しない限り利用停止・消去を求めることはできない（27 条）。日本において私的事項が本人に無断で漏洩されたり公開されたりした場合には、プライバシーを侵害するものとして、損害賠償請求権と差止請求権の二つの請求権を行使することが検討課題となる。一つ目の損害賠償請求権は、日本法でいうと不法行為に基づく損害賠償請求権であり、民法 709 条の問題になる。二つ

11　中村民雄「忘れられる権利事件」法律時報 87 巻 5 号（2015）132 頁、羽賀由利子「『忘れられる権利』- 忘れることを忘れた世界の新たな権利」コピライト 655 巻 55 号（2015）44 頁

12　2019 年 9 月 24 日 日本経済新聞 電子版「『忘れられる権利』EU 域内のみ ネット検索で司法裁」

目の差止請求権は日本法では法律上の明文の根拠はないが、プライバシーが物権のような排他性を持つ権利又は利益として認められるかという解釈上の問題になる。

プライバシー侵害事案での差止請求に関しては、名誉、プライバシー、名誉感情が侵害されたという事案において、「人格的価値を侵害された者は、人格権に基づき」差止請求ができるとした[13]。差止請求の要件事実としては、侵害行為が明らかに予想され、その侵害行為によって被害者が重大な損失を受けるおそれがあり、かつ、その回復を事後に図るのが不可能ないし著しく困難になると認められること挙げられた。ここで重要なのは、プライバシー侵害が直ちに人格権侵害であるとされているのではなく、人格的価値を侵害されたか否かは個別の事案によって判断されるという点であり、どのような場合に差止請求ができるかについての見通しを立てることが難しいことである。

また、人権行使の観点から、日本で近時話題になったものとして、プライバシー侵害を理由として、検索サイトからの削除請求が法的に認められるかが問題になった事案[14]がある。最高裁は、当該事実を公表されない法的利益が公表する理由に優越するかという比較衡量論を基準とし、「当該事実を公表されない法的利益が優越することが明らかな場合には、検索事業者に対し、当該URL等情報を検索結果から削除することを求めることができる」とし、結論としては削除請求を認めなかった。

このように人権行使の視点で見ると、EUと日本とでは人権行使の扱いが異なる。日本に居住する者がGDPRの適用を受けて人権行使する機会はほとんどなく、大半の場合は日本における前記判例法理の適用を検討しなければならない。日本においては、人権の保護を裁判で実現しようと思っても、コストなども含めて考えるとうまくいかないことが多いというのが現状である。データ管理のあり方については、人権保護以外の視点による解決の方向性も考えなけ

13　最判平成14年9月24日、判タ1106号72頁
14　最決平成29年1月31日、判タ1434号48頁

ればならない。

(5) 企業の視点

そこで、企業の対応をみていくと、GDPR の適用がある場合には、企業は GDPR の各条項を遵守し、GDPR への対応を行う必要があり、上記の制裁金を課されないように対応していくことが重要となる。

以下では、上記の人権行使と関連して、企業にとっても重要な問題である、個人データの侵害（個人情報の漏洩）が発生した場合についてみていく。

一度情報漏洩が起きると、企業の信用の低下は避けられず、顧客離れにより売り上げや営業利益が減少する可能性がある。また、原因の追求や再犯防止策がとられるまでサービスの提供等が出来なくなる可能性もある。さらに、漏洩後の対策等が求められるため、事案によっては調査委員会の設置、情報管理の規定及び体制、ガバナンス体制自体の見直しをしなければならない場合も考えられる。

直近では、2014 年に、ベネッセコーポレーションにおいて、個人情報が流出した事件があった。この事件では、責任部署にいた取締役 2 名が辞任したほか、大規模な顧客離れがおき、同社は経営赤字に転落するなど、事業運営に大きな影響が発生した[15]。

この点、日本においては、「個人データの漏洩等の事案が発生した場合等の対応について」（平成 29 年個人情報保護委員会告示第 1 号）[16] 等に定められた対応をとることになるが、GDPR では、個人データの侵害が発生した場合には、監督機関への通知義務（同第 33 条）及びデータ主体への個人データ侵害の通知義務（同 34 条）の厳格な義務が定められている。

次に、個人データの侵害が起こらないようにするために考えられる、企業の対策を、情報銀行・情報信託という観点からみていく。

15　渡部涼介『企業における「個人情報・プライバシー情報の利活用と管理」』（青林書院、2018）134-136 頁、145-149 頁

16　https://www.ppc.go.jp/files/pdf/iinkaikokuzi01.pdf

企業は、情報銀行の事業を行う場合には、委任をしたデータ主体に善管注意義務等を負うことから、同義務に基づき、個人情報の管理・利用することが必要となるほか、情報銀行の事業を行う企業、同企業からデータの提供を受ける企業は、個人情報保護法等の法令を遵守し、情報のセキュリティ基準を満たすこと等が必要となり、そのような企業のコンプライアンスを通じて、個人情報及び個人の権利利益が保護されることになる。

企業のコンプライアンスに対する姿勢は、投資家に影響を与えるため、特に上場企業では、コンプライアンスが自律的に機能することが期待できるといえる。例えば、最近では、環境（environment）・社会（social）・企業統治（governance）に配慮している企業を重視・選別して行う投資として、ESG 投資と呼ばれるものがある。2016 年末時点で、世界の ESG 投資の運用資産は 23 兆ドルに達すると言われている[17]。

特に情報銀行・情報信託においては、情報の保護につき情報を委任又は信託しようとするデータ主体が信頼できる体制の確保やデータ主体が関与し、自身の情報をコントロールできる体制の確保等が必要となるといえる。そして、そのような体制を確保することで、データ主体や社会の信認を得ることが出来れば、データの円滑な流通が図られ、横断的なデータの利活用が期待できる。

3 事例②「同意強制」

(1) 想定事例

二つ目の事例は、同意強制についてである。

【事例②】
米国企業 Google、Instagram、WhatsApp、Facebook は、ユーザに同意を強制しているとして、オーストリア非営利プライバシー保護団体「noyb」から、データ保護監督機関に対して GDPR 違反である旨の苦情申立てを受けた。どのような展開が予想されるか？

17　https://www.meti.go.jp/policy/energy_environment/global_warming/esg_investment.html

(2) 行政の視点

まず、行政の視点であるが、GDPR においては、個人データを取り扱ったり、移転したりするのに一定の要件を満たす必要があるとされており、データ主体の同意は、その要件の一つとなっている（6 条 1 項 (a)、49 条 1 項 (a)）。GDPR 及び「同意に関するガイドライン」では、同意の意義や条件について細かく規定しているが、ポイントは 4 つある。

まず、①データ主体の同意とは、自由になされ、特定され、情報を受けた、不明瞭でない意思表示を意味すると規定されている（4 条 11 項）。

このうち「自由」については、個人データの管理者とデータ主体間の力の不均衡が考慮され（前文 43 条）、例えば、雇用者が従業員から同意を自由に取得できる可能性は低いであろう。

そのほか、②データ主体はいつでも自分の同意を撤回する権利を有すること（7 条 3 項）、③有効な同意を取得したことの証明責任が管理者側に課されていること（7 条 1 項）、④一定の年齢の子どもについては、親権を有する者からの同意が必要であること、がポイントとして挙げられる[18]。

(3) 人権行使の視点

次に人権行使の視点であるが、前記のとおり、GDPR 域内のデータ主体は、GDPR17 条に基づき消去権・忘れられる権利を行使することができる。これに対して、前記のとおり GDPR 域外での適用は義務ではないとの EU 司法裁判所の判断があったと報道されている。

そこで、日本法での権利関係を見てみると、個人情報を取得した段階では、詐欺等の取得過程の違法性を立証できるようなごく例外的な場合は別として、個人情報保護法の利用停止・消去請求を求めたり、損害賠償請求及び差止請求の責任追及をしたりすることは難しい。他方で、第三者提供や漏洩行為があった段階では不法行為責任の問題になり得る。また、重要なデータで部外に漏れたときに被ることが予想される不利益が大きく、第三者提供や漏洩の蓋然性が

18　宮下・前掲注 (8)56-70 頁

高いという場合には、要件を満たす場面は限定的であるが、第三者提供・漏洩の前に差止請求できるかという問題になる。

ところで、事例②で苦情を申し立てた人権活動団体は、EU で注目を集めた裁判例に関わったことでも知られている。GDPR でもそうであるが、EU データ保護指令下でも、EU 域外へのデータの越境移転には規制があり、十分性認定を受けた国・地域への移転は規制の対象外となる。アメリカへのデータ移転に関しては、従前、十分性認定はなされていないものの経済的重要性に鑑みて協定によりセーフハーバーという特別な枠組みが取られていた。簡単にいうと、アメリカ企業の監督は、アメリカ側に任せ、EU 側は直接口を出さないという枠組みであった[19]。ところが、2015 年 10 月 6 日、EU 司法裁判所大法廷は、EU 機能条約 267 条の先決付託手続において、アメリカとの間で定めたセーフハーバー決定を無効とする判決を下した。その判決の発端となったのは、ウィーン大学の学生であったマクシミリアン・シュレムス氏がアイルランド、ルクセンブルク、ドイツの各国のデータ保護監督機関に対して行った Apple、Facebook、Skype、Microsoft、ヤフードイツによるプライバシー権及びデータ保護権の侵害に関する不服申立であった。EU 司法裁判所は、アメリカによるセーフハーバーの運用状況に鑑みて無効と判断したが、このような世界的に影響を及ぼす判決を引き出す活動をしたマクシミリアン・シュレムス氏の動向は注目を集めている。今回のテーマとなる事例②の話に戻すと、GDPR 施行直後に、グーグル等のアメリカ企業が同意を強制しているとしてデータ保護監督機関に不服申し立てを行ったのは noyb というオーストリアの団体であるが、その代表を務めるのが、先ほどのマクシミリアン・シュレムス氏であり[20]、それ故、世間の注目を浴びている。

19　中崎尚『Q&A で学ぶ GDPR のリスクと対応策』（商事法務、2018）58 頁、宮下・前掲注 (8)227 頁

20　2018 年 5 月 29 日日本経済新聞電子版「GDPR 施行、グーグルなど 4 社を監督機関に苦情申し立て」

(3) 企業の視点

まず、GDPR の適用範囲についてであるが、① EU 域内に管理者または処理者が設置された活動における個人データの処理がなされる場合、② EU 域内に管理者または処理者を設置していない場合でも、② a データ主体の支払いの有無にかかわらず、EU 域内の当該データ主体に対する商品またはサービスの提供に関連して EU 域内に在住するデータ主体の個人データの処理が行われる場合、② b データ主体の行動が EU 域内で生じる限りにおいてその行動の監視（モニタリング）に関連して EU 域内に在住するデータ主体の個人データの処理が行われる場合がある（同 3 条）[21]。

そして、GDPR が日本企業に適用される場合で、データ主体から同意を得る場合には、上記の GDPR の同意の条件を満たす必要がある。したがって、強制や消極的帰結の危険がある場合の同意は自由になされたものとみなされず、GDPR 違反となる[22]（4 条 11 項）。

事例②においては、データ管理者の立場が強く、また交渉の余地がなく、データ主体が損害を受けることなく同意を拒否することが出来ない状態であることから、自由になされた同意とはいえないことになり、GDPR 違反となると思われる。実際に、事例②と同様の事案において、フランスデータ保護機関情報処理・自由全国委員会は、個人情報利用の同意をユーザから得る手続が不適切だったなどとして、米グーグルに 5000 万ユーロ（約 62 億円）の制裁金を科すと報道された[23]。

以上からすれば、企業としては、同意をしないと一律にサービスを利用出来ないとするような運用は、自由になされた同意とはいえないことから、避ける必要がある。

21　宮下・前掲注 (8)26-29 頁

22　宮下・前掲注 (8)56-63 頁

23　2019 年 1 月 22 日日本経済新聞電子版「グーグルに制裁金 62 億円　仏当局、個人情報取得めぐり　米 IT 向け初の制裁」

4 事例③「域外移転」

(1) 想定事例

三つ目の事例は、EU 域外への持ち出しについての事例である。

【事例③】
欧州にある日本企業の海外子会社に出向中の日本人が、日本あるいは第三国に移転しようとする場合、欧州での医療データを移転先の域外に持ち出すことができるか？

(2) 行政の視点

行政の観点からは、個人データの EU（厳密には EEA（欧州経済領域））域内から域外への移転、再移転は、GDPR が定める要件が遵守される場合にのみ許容される（GDPR 44 条）。要件はいくつかあるが、中でも、移転先の第三国等が十分性認定（45 条）を受けているか否かが重要である。十分性認定とは、特定の国が十分なデータ保護のレベルを確保しているかどうかを欧州委員会が認定するというもので、十分性認定を受けた国に対しては、EU 域内からのデータ移転が許容されることになる（45 条）。日本については、個人情報保護委員会が協議を進めた結果、2019 年 1 月 23 日、欧州委員会により正式承認された。

データ移転先の第三国等が十分性認定を受けていない場合でも、一定の要件を満たせば個人データを移転することができる。例えば、十分なリスク説明を行った上で、データ主体の明示的同意が得られた場合（49 条 1 項前段 (a)）も例外的に移転が許容される。ただし、明示的な同意を得たか否かは相当厳格に判断されるので、事例③で医療機関がデータ主体の同意を根拠としてデータを移転しようとする場合、慎重な対応が必要となると考えられる。

(3) 人権行使の視点

次に人権行使の観点からみると、ポータビリティ権を定める GDPR20 条 1 項では、「構造化され一般的に利用され、機械可読性のある形式でデータを受領する権利」（right to receive）と、「別の管理者へ移行する権利」（right to

transmit）が定められている。法体系や言語の異なる EU 域外の管理者へ直接移行してもらうには、法律上、実務上の多くの困難が予想される。これに比べて、データを受領する権利の方が実現が期待できる。しかし、前記のとおり、EU 司法裁判所の忘れられる権利の域外適用を否定する判断を前提にすると、域外へのポータビリティが権利として認められるかは極めて不透明である。

また、データを受領する権利の権利行使が実効性を持つためには、医療データについて一般的に利用されている形式が何であるかという問題がある。GDPR でいう一般的に利用されている形式が、日本で利用できる共通の形式でないと意味がない。このように、データ主体にとって、データポータビリティを実現するためには、形式の統一という点が重要になる。また、データ主体の意向に従って、USB 経由で重要なパーソナルデータをメモリにポートアウトした場合、セキュリティ面で危険な状態に陥るが、そのようなことでよいのかという問題もある。

(4) 企業の視点

事例③はデータ主体がデータを域外移転しようとするケースであるが、日本企業の海外子会社が欧州在住の日本人のデータを預かり、域外に移転させたい場面も考えられるので、その場合に留意すべき事項を考えてみる。日本企業の海外子会社がデータ管理者であった場合、同子会社の立場からは、第三国への個人データの移転に関する GDPR の規定を遵守する必要がある（同第 5 章）。GDRR では、個人のデータを EU 及び欧州経済領域から、第三国へ移転する場合として、十分性認定に基づく移転（同第 45 条）、適切な保護措置に従った移転（同第 46 条）等を定めているが、日本の十分性認定が決定されたことは、上記のとおりである。

5 まとめ

このようにみていくと、データ主体・個人から信認・信頼を得られるようなデータの管理の在り方を目指すためには、個人による人権行使、行政による規

制、企業の努力というそれぞれ立場の視点をバランスよく配慮していくことが重要となってくる。

この点、弁護士は、(1) データ主体・個人の人権を守る役割、(2) 情報管理の規制やルールを考えたり解釈したりする役割、(3) 情報を管理する企業にアドバイスする役割に関与することができ、これらの視点にバランスよく配慮することがもっとも期待できる存在だといえる。

このような弁護士による積極的な活動を通じて、データ主体・個人と情報管理者との間のよい信認関係の形成を目指すべきだと提言したい。

また、シンポジウムでは、EU の権利意識は、日本と協調しやすいのではないかとの指摘もあり、弁護士の役割はより重要になるのではないかと思われる。

ところで、信託における信認は、元来は、特定の人又は集団に対する信頼が基本にある。信じ託された者は、信託の目的のために、信託の本旨に従い信託事務を処理する義務を負い、その務めをきちんと果たせる者であるとの信頼に応えなければならない。その信頼は、本来、信託としてなされる事業の目的との関係で受託者の個性を見ていくべきものであったが、情報管理との関係では、個々の情報提供者が、個々の情報の保有者を信用できるかについて判断に足りる情報を得ることあるいは提供を受けて判断するといったこと自体が困難であるし適当ともいえない状況にある。具体的な事業との関係から、あるべき情報管理を実現するための信頼に足りる制度を有していること、その制度を適切に運営していく人的・資本的な基盤を有していることなどから信頼を得ていく方向へ、情報管理のあるべき姿についてのビジョンを共有する姿勢に信頼を集う方向へと向かうと思われる。信認に基づいて必要な制度を形づくることを本質的に行う信託の視点から、今後現出する様々な制度や試みを検証していくことはその意味においても有益である。

6 シンポジウム後の動向

2018 年 12 月 15 日のシンポジウム終了後の GDPR をめぐる動向として大きなことは、2019 年 1 月 23 日、欧州委員会において日本の十分性認定が決定されたことである。これにより、欧州から日本へのパーソナルデータの移転の機会が増え、GDPR 適用事案が多く発生し、本稿で取り上げた課題への対策の必要性がますます重要になる。

また、時をほぼ同じくして、事例②と同様の事案について、フランスのデータ保護機関が米国 Google に制裁金 5000 万ユーロ（約 62 億円）を科すという報道が 1 月 22 日にあり、制裁金が科される事例の動向も注意が必要である。

さらに、9 月 24 日、EU 司法裁判所が「EU 域外での適用は義務ではない」との判断を示したとの報道もあったが、これは事例③と関連する。

当部会としては、このようにめまぐるしく変化する国内外の動向を注視しつつ、情報の信託的管理と弁護士が果たすべき役割について、今後も法学者との意見交換の機会を持ちつつ、研究を続けていきたい。