EUの個人データ保護法令と他の関連立法との関係に関する検討

法律論叢第91巻第4・5合併号（2019.1）

【論　説】

EUの個人データ保護法令と他の関連立法との関係に関する検討

夏　井　高　人

目　次

1　はじめに

2018年5月25日、EUの一般個人データ保護規則(EU) 2016/679（GDPR）（OJ L 119, 4.5.2016, p.1-88）が適用開始（施行）となった。GDPRの適用開始により、従前の個人データ保護指令95/46/EC（OJ L 281, 23.11.1995, p.31-50）は、廃止された。

GDPR は、EU の構成国の民間部門及び公的部門（行政機関等）に直接適用される(1)。他方、EU の機関及び組織（institutions and bodies）に関しては、規則 (EC) No 45/2001（OJ L 8, 12.1.2001, p.1-22）が適用される(2)。GDPR の統括的な監督機関は、EU レベルでは個人データ保護委員会（EDPB）であり、構成国レベルでは各国の国内監督機関である。また、規則 (EC) No 45/2001 の統括的な監督機関は、欧州データ保護監督官（EDPS）である。そして、後述のとおり、これらの代表的な個人データ保護法令に加え、EU(3) においては、個人データ保護と関連する複数の法令が存在しているほか(4)、非常に多数の法令の中に個人データ保護条項が存在し(5)、現に適用されている。

ところで、EU の法令の中で個人データ保護（プライバシー保護）とは直接の関係のない法令、あるいは、少なくとも個人データ保護を当該法令の制定目的としていない法令、または、個人データ保護（プライバシー保護）とは全く異なる法益保護を目的とする法令が、現在のデータ駆動型経済(6) またはデータ経済(7) の動きの中で、結果的に相互に密接な関係をもつことがある。この場合の相互作用のメカニズムは、誰にでも容易に理解可能なものとそうではないものとが含まれる。特に後者の場合、情報処理及びデータ産業の基本構造の理解がないとわかりにくい面があり得るが(8)、少なくとも現時点においては、あくまでも法適用関係の分析という観点から論理的な考察が可能な範囲外にあるわけではない。そして、これらは、情報法及びサイバー法の全体構造(9) の中で、動的な作用及び機能をもつものとして理解されるべきものである(10)。

本稿においては、2018 年 10 月 30 日の時点において有効に適用されている EU の個人データ保護法令の概要を簡単に示した上で、個人データ保護（プライバシー保護）を直接の目的としない他の法令との相互関係について、EU の機関が保有する文書への公衆のアクセスに関する法令との関係（3.1.1）、文書へのアクセスの権利と関連する法令と EU の機関に適用される個人データ保護法令との関係（3.1.2）、オープンデータ政策と関連する法令との関係（3.1.3）、データベース関連法令との関係（3.2.1）及び非個人データ関連法案との関係（3.2.2）の順に、EU の代表的な関連法令及び立法案の例を示しながら検討し、今後の日本国におけるデータ経済及び電子通信技術の発展に伴う法制整備及び法解釈論の構築に資すること、とりわけ、最も広い意味における情報財(11) の憲法的価値の考究に資することを目的と

する(12)。

2　EUの個人データ保護法令の体系

GDPRの適用（施行）の日である2018年5月25日よりも前である2016年の時点におけるEUの個人データ保護法制の体系に関しては、既に別稿において詳論したとおりである(13)。ここでは、2018年10月30日の時点において有効なEUの個人データ保護法令の体系の概略を示す。ただし、多数の法令の中にある個別の個人データ保護条項に関しては割愛し、主として個人データ保護を目的とする法令のみを示すことにする。

2．1　GDPRの適用範囲

GDPRの第2条第1項及び後文は、GDPRが、EUにおける個人データのファイリングによる処理の全てに直接に適用されることを定めた上で、その第2条第2項、同条第3項及び同条第4項において適用除外を定めることにより、その適用範囲を限定している。

2．1．1　GDPR第2条第2項

GDPRの第2条第2項は、GDPRが適用されない分野として、以下のものを定めている。

(a) 欧州連合法の適用範囲外にある活動の過程で行われる場合；
(b) 構成国によって欧州連合条約第5款第2章の適用範囲内にある活動が行われる場合；
(c) 自然人によって純粋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；
(d) 公共の安全への脅威に対する防護及びその脅威の防止を含め、職務権限を有する機関によって犯罪行為の防止、捜査、検知もしくは訴追または刑罰の執行のために行われる場合。

GDPRの第2条第2項(a)は、EUのjurisdictionが及ばない領域に関する適用除外であり、国際法上の基本原則に基づくものである。

GDPR の第 2 条第 2 項(b)に定める欧州連合条約（TEU）の第 5 款第 2 章の条項とは、主として、統合後の欧州連合の機能に関する条約（TFEU）の第 24 条（旧 TEU 第 11 条）ないし第 46 条に定める EU 及びその構成国の国際関係、外交及び国防に関する事項のことを指す。これらの公共の利益は、自然人の法益である個人データと関連する保護法益（プライバシーの利益）よりも優越するという趣旨と解される(14)。

GDPR の第 2 条第 2 項(c)は、純粋に私的な行為に関して、GDPR の適用を除外している。仮にそうしないとすれば、個々の私人が些細な私的事項に関しても個人データの管理者（controller）としての義務を負うことになるので、それを避けるための条項である(15)。

GDPR の第 2 条第 2 項(d)は、犯罪捜査活動における適用除外を定める。これは、犯罪捜査に関しては個人データ保護の法令が存在しないという趣旨ではなく、犯罪捜査の特殊性に鑑み、別の特別法によって規律するという趣旨である(16)。そのための特別法として、指令(EU) 2016/680（OJ L 119, 4.5.2016, p.89-131）が定められた(17)。同指令は、全ての構成国の警察機関及び検察機関に対して適用される。

2．1．2　GDPR 第 2 条第 3 項

GDPR の第 2 条第 3 項第 1 文は、「欧州連合の機関、組織、事務局及び部局による個人データ処理に関しては、規則(EC) No 45/2001 が適用される」と定めている。その結果、EU の機関及び組織における個人データの処理に関しては、GDPR ではなく規則(EC) No 45/2001 のみが適用されることになる。

この GDPR の第 2 条第 3 項第 1 文に定める「機関及び組織」には、欧州議会、理事会及び欧州委員会(18)も含まれ、更に、欧州司法裁判所のような EU の司法機関及び EU の警察関連機関等も含まれ、EU の個人データ保護における統括機関である EDPS 及び EDPB も規則(EC) No 45/2001 に服さなければならないのであるが(19)、司法機関及び警察関連機関等については特別法令が存在する(20)。また、軍や諜報機関等は、規則(EC) No 45/2001 との関係においても GDPR の適用除外となると解される。

加えて、GDPR の第 2 条第 3 項第 2 文は、「規則(EC) No 45/2001 及び個人データのそのような処理に適用可能な同規則以外の欧州連合の法令は、第 98 条に従い、

本規則の基本原則及び規定に適合するように調整される」と定め、GDPRの第98条は、「欧州委員会は、それが適切なときは、処理と関連する自然人の統一的で一貫性のある保護を確保するため、個人データの保護に関する他の欧州連合の法的行為を改正するための立法の提案書を送付する。これは、欧州連合の機関、組織、事務局及び部局による処理と関連する自然人の保護並びにそのデータの支障のない移動に関する規則と特に関係するものである」と定めている。この提案書として、COM/2017/08 final[21]が提出され、2018年10月30日現在、審議中である。

2．1．3　GDPR第2条第4項

GDPRの第2条第4項は、「本規則は、指令2000/31/ECの適用、とりわけ、同指令の第12条ないし第15条にある中間介在サービスプロバイダの法的責任に関する規定の適用を妨げない」と定めている。その趣旨について、GDPRの前文(21)は、「同指令は、構成国間における情報社会サービスの支障のない移動を確保することによって、域内市場の適正な稼働に貢献することを求めるものである」と述べている。

GDPRの第2条第4項が定める「指令2000/31/EC」とは、電子商取引指令2000/31/EC（OJ L 178, 17.7.2000, p.1-16）のことを指す[22]。そして、同指令の第12条ないし第15条にある中間介在サービスプロバイダ（intermediaries）の法的責任とは、サービスプロバイダが同指令第12条の「単なる導管（mere conduit）」である場合、第13条の「キャッシング（caching）」である場合、第14条の「ホスティング（hosting）」である場合において、法的責任を負わないことを指す。すなわち、GDPRによって定められる法的義務及び法的責任の適用除外条項である。これらのデータ処理の態様の中で、単なる導管は、通信経路を提供するだけの極めて短時間で終了するサービスを意味し、キャッシングは、機械的な処理のための短時間の記録保存処理を意味する。これに対し、ホスティングは、一定期間継続して行われる記録保存（storage）を伴う点が異なる[23]。

そして、指令2000/31/ECの第15条第1項は、「構成国は、プロバイダに対し、第12条、第13条及び第14条の範囲内にあるサービスを提供する際、彼らが送信または記録保存する情報を監視すべき一般義務を課してはならず、違法な行為であるとの徴候を示す事実または状況を積極的に探索すべき一般的な義務を課してもならない」と定めているから、サービスプロバイダは、個人データと関連する違

法行為を積極的に探知する義務を負わない。しかし、この場合においても、個人データのデータ主体から何らかの積極的な苦情申立てがあった場合等には、管理者（Controller）としての義務を履行しなければならない場合があり得ることまで排除する趣旨ではないと解される。このことは、GDPR の第 17 条に定める削除権（忘れられる権利）の条項（特に同条第 2 項）からも明らかである(24)。

2．2　構成国の法令

GDPR は、規則（Regulation）の一種であるので、構成国の機関及び組織（立法機関、司法機関、行政機関並びにこれらの機関と均等な組織及び機関）に関しては、上述の適用除外事項を除き(25)、GDPR の条項が直接に適用される(26)。ただし、一般論として、各構成国の行政行為等の特殊性(27)のゆえに、各構成国の個々の法令の中においても個別に個人データ保護と関連する条項が定められている場合、その内容が GDPR の定める条項と内容的に矛盾しないように修正されることを要することがあり得ることに留意すべきである(28)。

GDPR に定める条項に基づき構成国に対して委任された事項に関しては、実質的には、指令（Directive）の場合と同様の実装行為が必要となる。各構成国は、それらの委任事項に関し、GDPR の各条項に定める条件を遵守して適切に実装（立法）することになる(29)。

他方、各構成国の監督機関（competent authorities）は、それぞれの構成国の国家体制を反映して異なる組織構造をもつものであるので、各監督機関の国家組織法が GDPR とは別に存在しなければならない。国家体制の相違は、監督機関が行使できる制裁の権限にも影響を及ぼす。そのため、事前に判明している事項に関しては、GDPR の中でそのための手当てが施されている(30)。

更に、EU の構成国は、例えば、以下のような個人データ保護と関連する特別法令である指令を実装する国内法令を採択し、適用（施行）しなければならない(31)。

e プライバシー指令 2002/58/EC（OJ L 201, 31.7.2002, p.37-47）(32)
警察指令 (EU) 2016/680（前掲）(33)
PNR 指令 (EU) 2016/681（OJ L 119, 4.5.2016, p.132-149）(34)
API 指令 2004/82/EC（OJ L 261, 6.8.2004, p.24-27）(35)

NIS指令(EU) 2016/1148（OJ L 194, 19.7.2016, p.1-30）[36]

これらの特別法令は、その適用対象となる事項の特殊性に鑑み、それらの対象事項に特化した個人データ保護の制度を定めるものである[37]。例えば、しかし、PNR指令(EU) 2016/681及びAPI指令2004/82/ECは、国際旅客運送並びに国境を越える重大犯罪及びテロリスト犯罪対策と深い関係をもつものであり[38]、また、NIS指令(EU) 2016/1148は、国境を越える重大犯罪及びテロリスト犯罪対策並びに国防と深い関係をもつものであり[39]、その意味で、上述のGDPR第2条第2項の適用除外と関係する法令であると解し得る。しかし、これらの指令は、いずれも、根本的にはTFEU第16条[40]に基づくプライバシーの利益の法的保護を法哲学上の基礎とするものであり[41]、そして、プライバシーの利益とこれらの特別法令が関係する他の保護法益との間の合理的かつ比例的な相互関係の調整、及び、他の関連法令との整合性・一貫性の確保を目的とするものである。

3　他の関連法令との関係

以下、GDPR及び規則(EC) No 45/2001に代表されるEUの個人データ保護法令とEUの主要な関連法令との相互関係について検討する。このような考察のためには、欧州における重要な判例法及び構成国の関連法令の検討が不可欠であるが、本稿の主たるテーマと密接に関連するデータベース保護指令96/9/EC（OJ L 77, 27.3.1996, p.20-28）の有用性等に関し、欧州委員会から委嘱を受けた組織であるThe Joint Institute for Innovation Policy (JIIP)による極めて詳細な調査検討結果報告書[42]が既に公表されているので、本稿においては、必要に応じて関連部分を照会するのにとどめる。

3．1　情報アクセス権を認める法令との関係

3．1．1　規則(EC) No 1049/2001と規則(EC) No 45/2001との関係

EUの法令において、一定の情報への「アクセス（access）」の概念及び「アクセス制御（access control）」の概念によって、その法令の作用・機能を考察する

ことが可能な一群の法令が存在する(43)。そのようなタイプの法令の中には、情報アクセス（public access）と関連する法令(44)、オープンデータ（open data）と関連する法令(45)、機密情報（classified information）(46)と関連する法令及び通信の秘密（confidentiality of communication）(47)と関連する法令が含まれる。ここでいうアクセス制御とは、標準的な情報処理及び情報マネジメントの考え方におけるアクセス制御の考え方を基盤とするものであり、制御対象であるデータ（情報）及び利用者のアクセスの可否に関し、その決定権限をもつ者及びその権限の範囲、権限行使のための判断基準、並びに、行使された権限の適法性・妥当性を争うための不服申立手段を含むものである(48)。ただし、これは、統治のための手段としての法制度がもつ機能（function）及び相互作用（interaction）という観点からのモデル化に基づくものであるので、個々の法令の立法上の沿革、法制史上の位置づけ、保護法益の法理論上の位置づけ及びその批判等とは一応別の視点に基づくものである(49)。

これらの事項の中で、国家機関が保有する様々な情報へのアクセスの権利を保障するための法令と個人データ保護（プライバシー保護）のための法令との間には、時として矛盾が生ずることがあり、その調整のための判断基準が常に議論の対象とされ続けてきたし(50)、日本国においてもこの問題と関連する裁判例が多数ある(51)。

EU において、EU の公文書に対する公衆のアクセス（public access）の権利を保障する根拠法規は、TFEU 第 15 条（旧 TEU 第 255 条）である。すなわち、TFEU 第 15 条第 3 項第 1 副項は、「欧州連合の市民、並びに、構成国内に居住または登録した事務所をもつ自然人または法人は、本項に定める基本原則及び条件により、媒体の別を問わず、欧州連合の機関、組織、事務局及び部局の文書へアクセスする権利をもつ」と定めている(52)。ここに「本項に定める基本原則及び条件」とあるアクセス条件を具体的に定める法令は、規則 (EC) No 1049/2001（OJ L 145, 31.5.2001, p.43-48）(53)である(54)。

規則 (EC) No 1049/2001 の前文は、「高度に機微な内容であることを理由として、一定の文書は、特別の取扱いを受けるものとしなければならない。そのような文書の内容を欧州議会に対して連絡するための手順は、機関間合意を通じて策定される」と述べている。この高度に機微な内容（highly sensitive content）」とは、主とし

て、機密文書（classified documents）のことを指し、また、「機関間合意」とは、「Interinstitutional Agreement of 20 November 2002 between the European Parliament and the Council concerning access by the European Parliament to sensitive information of the Council in the field of security and defence policy (2002/C 298/01)」のことを指す。そして、同規則の前文(11)は、「原則として、機関の全ての文書は、公衆にとってアクセス可能なものでなければならない。しかしながら、一定の公共の利益及び私的利益は、適用除外によって保護されなければならない。機関は、その職務を行うためのその機関の能力を防護するために必要な場合には、その文書の内部的な調査及び授受を防護する権利を有するものとしなければならない。適用除外の検討に際しては、機関は、欧州連合の全ての分野において、個人データの保護に関する欧州共同体の立法の中にある基本原則を考慮に入れなければならない」と述べている。すなわち、EUの機関及び組織が保有する公文書の開示の許否を決定する際、当該機関及び組織は、当該文書の機密指定区分(55)及び個人データとしての保護の要否・程度に関し、比例性原則に従って判断しなければならない。個人データの場合のアクセスの許否の判断基準に関し、規則(EC) No 45/2001の前文(15)の第2文もまた、「個人データを含む文書へのアクセスの要件を含め、文書へのアクセスは、その適用範囲に欧州連合条約の第5款及び第6款を含む欧州共同体設立条約の第255条に基づいて採択される規定によって規律される」と述べていることから、結局、規則(EC) No 1049/2001に定める基準が、その原則的な判断基準であることになる(56)。

規則(EC) No 1049/2001の第4条は、例外として文書へのアクセスを拒否するための判断基準を定めている。特に同条第1項は、以下のように定めている。

> 機関は、開示が以下に対する保護を妨げる場合には、文書に対するアクセスを拒否する：
>
> (a) 以下に関する公共の利益：
>
> —公共の安全；
>
> —国防及び軍事上の事項；
>
> —国際関係；
>
> —欧州共同体または構成国の金融上、財政上または経済上の政策。

(b) 個人データの保護と関連する欧州共同体の立法に従い、プライバシー及び個人の完全性。

日本国の「行政機関の保有する情報の公開に関する法律（情報公開法）」（平成 11 年法律第 42 号）に定める条項と対照すると、規則 (EC) No 1049/2001 の第 4 条第 1 項 (a) に定める「公共の利益」は、情報公開法第 5 条第 1 号に、規則 (EC) No 1049/2001 の第 4 条第 1 項 (b) に定める「個人データの保護」は、情報公開法第 5 条第 3 項に対応するものである。「プライバシー」は、欧州連合基本権憲章の第 7 条に、「個人の完全性」は、同憲章第 3 条によって保障されている。ここに定めていることは、基本原則のみである。しかし、EU におけるより具体的な判断基準及び法の適用関係の実際を知るためには、平凡ではあるが、帰納法的な考察方法、すなわち、日本国における情報公開と個人情報保護との間の調整の場合と同様、判例法または実例を知るという方法以外に効果的な方法が存在しないと考えられる(57)。

他方、規則 (EC) No 1049/2001 の第 4 条第 1 項 (a) に定める「個人データの保護と関連する欧州共同体の立法」とは、上述のとおり、一般法令としては、個人データ保護指令 95/46/EC（2018 年 5 月 25 日以降は、GDPR）のことを、EU の機関及び組織に適用される法令としては、規則 (EC) No 45/2001 のことを、そして、電子通信と関係する個人データ処理に関しては、e プライバシー指令 2002/58/EC のことを指す。それゆえ、公文書の開示が当該文書に含まれている個人データへのアクセスまたは個人データの移転を必然的に伴うものである場合、これらの個人データ保護法令に定める要件の充足性が検討されなければならない。その場合、規則 (EC) No 1049/2001 に定める要件とこれらの個人データ保護に定める要件との論理的な関係の検討が不可避のものとなるのである。

3．1．2 *European Commission* v *The Bavarian Lager Co. Ltd.*

この点に関する判例としては、*European Commission* v *The Bavarian Lager Co. Ltd.*, Case C-28/08 P, 29 June 2010, ECLI:EU:C:2010:378(58) 及び *Gregorio Valero Jordana* v *European Commission*, Case T-161/04, 7 July 2011, ECLI:EU:T:2011:337(59) を代表的なものとして挙げることができる。特に、前者が重要である。

European Commission v *The Bavarian Lager Co. Ltd.* 事件の概要は、以下

のとおりである。

ドイツビールの輸入会社であるBavarian Lagerが英国内の飲食店において輸入ビールの販売をしようとしたけれども、英国内の多数の居酒屋経営者が醸造会社と独占的な販売契約を締結していたため、Bavarian Lagerは、英国内におけるドイツビールの販売ができなかった。

ビール供給令1989 SI 1989/2390に基づき、2000店を越えるパブの保有権をもつ英国の醸造会社らは、樽の中で醸造され、かつ、1.2％を超過するアルコール濃度をもつことを条件とするという同令の第7条第2項(a)の条件に基づくことを条件として、これらの飲食店の経営者が別の醸造業者からビールを購入できるようにすることを要求した。この条件を定める条項は、「ゲストビール条項（GBP)」として知られている。しかし、英国外で製造されるビールの大半は、GBPの意味における「樽ビール」とは認定されていなかったため、その条項の適用範囲外にあった。

Bavarian Lagerは、GBPが競争制限と均等な影響をもち、したがって、EC条約の第30条（改正後はEC条約の第28条）に違反すると考え、1993年4月3日、欧州委員会に対し、このような居酒屋の運動を適法とする英国の法令（Order 1989 SI 1989/2390）がEC条約と適合しない旨の異議申立をした。

欧州委員会は、調査の結果、英国の法令がEC条約と適合しない旨の判断をし、その書簡を英国政府に送付した。

域内市場及び金融サービス事務総局（DG)、英国政府の関係省庁及び欧州ビール醸造同盟（CBMC）の代表による会合が1996年10月11日に開催されることとなった。Bavarian Lagerがその会合への出席を認めるよう要求したところ、欧州委員会は、その会合への出席を認めることを拒否した。

1997年3月15日、英国の通商産業省は、ゲストビールである樽ビールとして瓶ビールを販売できるようにするGBPの改正案をアナウンスした。その結果、欧州委員会は、英国政府への意見書の送付を停止する扱いとした。そして、改正GBPが1997年8月22日に発効したため、以後、欧州委員会が英国政府に対してこの件に関する意見書を送付することはなかった。

1998年7月8日、Bavarian Lagerは、欧州オンブズマンに対し、1996年

10 月 11 日の会合の出席者名を明かすように求めた。欧州オンブズマンと欧州委員会との間で交渉が行われ、欧州委員会からこの会合の出席者 20 名に対して個人データの開示に同意するか否かの照会が行われところ、14 名からは同意が得られたが 6 名からは拒否の回答があったので、欧州委員会は、Bavarian Lager に対し、同意を得られた者の氏名を開示した。

2003 年 12 月 5 日、Bavarian Lager は、電子メールにより、1996 年 10 月 11 日の会合の出席者の氏名を含む文書（P/93/4490/UK）の開示を要求した(60)。

欧州委員会は、2004 年 1 月 27 日、出席者の一部について同意を得ることができなかった等の理由により、同意を得られていない出席者の氏名を伏せたものであれば開示可能である旨の回答をした。そこで、Bavarian Lager は、規則 (EC) No 1049/2001 の第 7 条第 2 項に定める期限内である 2004 年 2 月 9 日、電子メールにより、参加者の氏名を含む 1996 年 10 月 11 日の会合の議事録全部の開示を申請した。欧州委員会は、2004 年 3 月 18 日、Bavarian Lager の申請を却下する決定をした。

Bavarian Lager は、一般裁判所（General Court）(61) において、欧州委員会の開示申請却下決定の取消しを求める訴えを提起した。

一般裁判所は、2007 年 11 月 8 日、規則 (EC) No 45/2001 と規則 (EC) No 1049/2001 との関係、特に、個人データの処理（processing）の概念について検討を加えた上で、「規則 (EC) No 1049/2001 の第 4 条第 1 項 (b) に基づく適用除外は、限定的に解釈されなければならず、かつ、プライバシー及び個人の完全性を現実的かつ特別に損ない得る個人データのみと関連するものである」と判示し、欧州委員会の開示申請却下決定を取消す旨の判決をした。

欧州委員会は、この一般裁判所の判決に対して控訴し、英国政府等が控訴審の手続に訴訟参加した。

控訴審である司法裁判所（大法廷）は、2010 年 6 月 29 日、独立弁論官の意見(62) を聴取した上で、規則 (EC) No 1049/2001 に基づいて個人データを含む文書へのアクセス（開示）を申請する場合、その申請が規則 (EC) No 45/2001 の条項（第 8 条及び第 18 条を含む）に適合するものであることを要し、それゆえ、開示を求める者が同規則第 8 条 (b) に定める正当な理由を示す

ことを要するとの解釈を前提にした上で、原審における規則(EC) No 45/2001と規則(EC) No 1049/2001との関係に関する解釈には誤りがあること、プライバシー及び個人の完全性に関する原審の解釈が極端に狭すぎること、会合参加者の氏名を除いた議事録へのアクセスのみでBavarian Lagerが入手を求める議事内容の情報提供が満たされ得ること、当該会合の参加者が個人データ開示について同意を与えていないこと、参加者の個人データの開示を求める正当な理由が存在すること、及び、規則(EC) No 45/2001第8条(b)に定めるデータ主体（会議参加者）の正当な利益が損なわれるおそれがないことを推定することをBavarian Lagerが証明していないことなどを理由に、原審判決には法令適用の誤りがあるとして、原審判決を破棄する旨の判決をした。

なお、この事件の控訴審におけるEDPSの答弁書(63)が公表されている。

この控訴審（司法裁判所）の判断の中に示されている規則(EC) No 45/2001と規則(EC) No 1049/2001との法適用関係に関する法解釈は、非常に興味深いものであり、今後、更に深く研究されるべき価値と必要性があるが(64)、整理のため、規則(EC) No 45/2001の第8条に定める要件を示すと、以下のとおりであり、これらの要件を満たす場合においてのみ、EUの機関または組織は、第三者に対して個人データを移転できる(65)。

(a) 公共の利益において、または、公的な権限の行使により行われる職務の遂行のためにそのデータが必要となることを取得者が証明する場合；または
(b) そのデータを移転させる必要性があること、及び、データ主体の正当な利益が損なわれるおそれがあると推定すべき根拠が存在しないことを取得者が証明する場合。

European Commission v *The Bavarian Lager Co. Ltd.*事件におけるBavarian Lagerは、「公共の利益において、または、公的な権限の行使により行われる職務の遂行のために」当該議事録の開示を求めているわけではないので、規則(EC) No 45/2001の第8条(a)の場合に該当せず、同条(b)の該当性の有無のみが問題となり得る(66)。一般に、同規則第8条(a)に該当する場合として

は、（EU の機関または組織ではない）構成国の行政機関または地方政府の行政機関が、EU（EC）の機関または組織から事務委託または嘱託を受けて職務を遂行する場合、その職務の遂行の過程において、EU（EC）の機関または組織が管理者（controller）となっている個人データの取得者（個人データの移転を受ける第三者）となる場合などがあり得る。

European Commission v *The Bavarian Lager Co. Ltd*. 事件においては、規則 (EC) No 45/2001 の条項の適用関係のみが論じられているが、EU の他の個人データ保護法令の適用が問題となり得る場合においても、それが均等な論理構造もつ場合、同様の判断手順が必要となる。

3．1．3　オープンデータ関連法令との関係

EU のオープンデータ政策は、一方において、法理念的には、公衆の情報アクセス権の保障という機能をもち、他方において、EU のデジタル単一市場政策ないしデータ駆動型社会政策及びデータ経済政策の重要な柱でもある(67)。

オープンデータ政策に関する EU の基本法令は、公的部門の情報の二次利用に関する欧州議会及び理事会の 2003 年 11 月 17 日の指令 2003/98/EC（OJ L 345, 31.12.2003, p.90-96）である。同指令は、指令 2013/37/EU（OJ L 175, 27.6.2013, p.1-8）により一部改正されているが(68)、その再改正の提案が行われており（COM(2018) 234 final）、目下、審議中である。

指令 2003/98/EC の前文 (5) は、「域内市場を設ける主要な目的の 1 つは、欧州共同体全体のサービスの発展に資する条件をつくり出すことである。公的部門の情報は、デジタルコンテント製品及びデジタルコンテントサービスのための重要な基本素材であり、無線のコンテントサービスの開発のより重要なコンテント素材となることであろう。この文脈においては、国境を越える広い地理的な広がりも重要である。公的部門の情報を二次利用できる可能性が広がれば、就中、欧州の企業の潜在力を開発することができるようにし、経済成長と雇用の創出に貢献することができる」と述べ、また、前文 (9) は、「この指令は、構成国における既存のアクセスの制度の上に構築され、文書へのアクセスのための国内法令を修正するものではない。この指令は、市民または会社が、関連するアクセス制度に基づき、それらが特別の利益をもつことを証明することができる場合においてのみ文書を得ることができる場合には、適用されない」と述べている。すなわち、オープンデータ政策の

眼目は、公的部門が保有するデータへのアクセスが認められている場合において、そのアクセスにより獲得されたデータの二次利用に伴う（著作権及び著作者人格権に基づく翻案、翻訳、編集、修正、頒布等の禁止または制限を含め）様々な法的制限（特にEUの構成国によって異なる法的制限）を可能な限り除去し、そのデータを活用（二次利用）して作成される新たなデジタルコンテント及びデジタルサービスの増加と品質向上にある。このことは、一般に、単にアクセスが認められているだけではなく、アクセスによって入手したデータの利用が法的に保障されているのでなければ、データにアクセスする意味の相当部分が意味を喪失してしまうので、特に重要である。ただし、指令2003/98/ECの前文(24)は、「この指令は、情報社会における著作権及び関連する権利の一定の側面の整合性確保に関する欧州議会及び理事会の2001年5月22日の指令2001/29/EC、並びに、データベースの法的保護に関する欧州議会及び理事会の1996年3月11日の指令96/6/ECを妨げない」と述べており、著作権及びデータベースの権利（*sui generis*の権利）と関連する他の法令の適用関係を丁寧に考察しなければならない。

以上のような前提を踏まえた上で、指令2003/98/ECの第3条は、「構成国は、公的部門の組織によって保有される文書の二次利用が認められる場合、第3章及び第4章に定める条件に従い、営利目的または非営利目的のために、これらの文書が二次利用できることを確保する。それが可能なときは、文書は、電子的な手段を介して利用できるようにされる」と定め、同指令の第3章は、電子的なフォーマットによる提供の促進（第5条）、原価主義による手数料の計算（第6条）、標準的な許諾条件の推奨（第8条）等を定め、また、同指令の第4章は、差別の禁止（第10条）及び独占合意の禁止（第11条）を定めている。そして、同指令の第1条第4項は、「この指令は、欧州共同体の法律または国内法に基づく個人データの処理と関連する個人の保護のレベルを低下させることがなく、かつ、いかなる方法でも害することなく、並びに、とりわけ、指令95/46/ECに定める義務及び権利を変更しない」と定めている。

指令2003/98/ECを一部改正する指令2013/37/EUの前文(11)は、「この指令は、個人データの処理と関連する個人の保護及びそのデータの支障のない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に従い、個人データの保護と関連する基本原則を完全に遵守して実装され、適用されなければならな

い。とりわけ、同指令に従い、構成国が、個人データの処理を適法なものであるための要件を定めなければならないことに注意すべきである。更に、個人データが、そのデータが収集された際の、特定され、明示であり、かつ、正当な目的と適合しない方法により、別の目的で収集されるために処理されてはならないことは、同指令の基本原則の 1 つである」と述べ、前文(34)は、「この指令は、基本的な権利を尊重し、かつ、個人データの保護（第 8 条）及び財産権（第 17 条）を含め、欧州連合基本権憲章によって認められた基本原則を尊重する。この指令にあるいかなる条項も、人権及び基本的な自由の保護に関する欧州条約と適合しない方法で解釈してはならない」と述べている(69)。

指令 2003/98/EC の再改正提案（COM(2018) 234 final）の提案理由説明書は、基本的な権利（Fundamental rights）との関係に関し、「この提案は、基本的な権利の遵守の面において特別の問題を示していない。この提案は、個人データの保護の権利（基本権憲章第 8 条）に沿うものである」と述べている。しかし、提案されている改正法の前文(24)は、「プライバシー、個人データの保護、営業秘密、国家安全保障、正当な商業上の利益と関係する不安、及び、第三者の知的財産権と関係する不安は、適正に考慮に入れられなければならない」と述べ、前文(32)及び前文(33)は、個人データ及び企業秘密と関係するデータの匿名化に要する費用の負担について触れている。

更に、指令 2003/98/EC の再改正提案（COM(2018) 234 final）の第 1 条第 2 項(g)は、オープンデータへの無制約のアクセスの原則の例外として、「個人データの保護を根拠とするアクセス制度のゆえに、その文書へのアクセスが排除または制限される文書、並びに、同制度のゆえにアクセス可能とされている文書の構成部分であって、その個人データの二次利用が、個人データの処理と関連する個人の保護に関する法律と適合しないものとして法律によって定められている個人データを含むもの」との条項（指令 2013/37/EU による改正後の指令 2003/98/EC の第 1 条第 2 項(cc)）を踏襲している。指令 2013/37/EU による改正によって追加された第 1 条第 2 項(cc)は、指令 2003/98/EC の適用除外を定める第 1 条第 2 項(c)の「国内の安全の保護（すなわち、国家安全保障）、国防または公共の安全」及び「統計上の秘密または商業上の秘密」(70)という同指令の適用除外事項に新たな適用除外事項を追加するものである。

以上のとおりであるので、個人データを含む文書は、原則として、オープンデータ政策の対象から適用除外され、または、大きく制限されているが、個人データを含む文書であっても、当該文書の外形的な特徴に基づいて個人データの有無が適正に識別され、当該個人データについて匿名化処理等が施される限り、オープンデータ政策の適用対象となり得る(71)。このことは、後述の非個人データの移転の場合でも同じである。

しかしながら、匿名化処理等が施されている個人データのように表面的には完全に非個人データのような取扱いを受けているデータであっても、その匿名化処理が施された個人データがプロファイリング（profiling）等のために使用されるときは、匿名化された状態のままで個人データとなることがあり得る。暗号化された個人データの場合においても、その暗号化された符号列もまた符号列の一種に過ぎない以上、それ自体として、識別子として機能することがあり得る。それゆえ、暗号化されたデータが常に識別力のないデータと等価であるというような理解は、誤りである。暗号化された元のデータの内容を推知可能であるかどうかという問題と、当該暗号化された後の符号列がそれ自体として識別力をもつか否かという問題とは、全く別の問題である。そして、個人データ保護法令は、当該符号列（データ）に特定の個人の識別力があるか否かという判断基準のみを用いて個人データの概念を構築しているという非常に重要な部分を理解しなければならない。

特に、GDPRの第4条(1)第1文は、「個人データ」を「識別された自然人または識別可能な自然人（「データ主体」）に関する情報を意味」すると定義しているが、当該「情報」それ自体が個人識別性をもつことを要件としていない。識別可能な自然人と関連する情報は全てGDPRにおける「個人データ」に該当し得る。そして、同条(1)第2文は、「識別可能な自然人とは、とりわけ、氏名、識別番号、位置データ、オンライン識別子のような識別子を参照することによって、または、当該自然人の肉体的、生理的、遺伝的、精神的、経済的、文化的または社会的な同一性を示す1または複数の要素を参照することによって、直接的または間接的に、識別され得る者のこと」であると定義している。暗号化されたデータまたは匿名化されたデータであっても、ある自然人の同一性の識別のために参照される「要素（factors）」の1つであり得ることは疑う余地が全くなく、それらの要素がそれ自体として個人識別性をもつことを要件としていない。これは、ビッグデータ分析や

プロファイリングのような例を想定しなくても当然の理であり、実際には、世界に存在する全ての情報要素が（潜在的[72]には）常に個人を識別するために参照される「要素」という意味での個人データであり得る[73]。その個人識別性が顕在化するのは、まさに、個人識別の目的のための当該要素であるデータが処理される時点においてである。それゆえ、固定的な定性要素として「個人データ性」を考えることは余り意味のあることではなく、まずどのような処理が実行されようとしているのかを考え、その処理の目的との関係において当該処理対象であるデータに対して個人データ保護法令が適用されるか否かを検討すべきである[74]。それゆえ、「匿名化されたデータ＝非個人データ」という図式は、（論理的には）成立しない[75]。ここでは、個人識別性を処理対象であるデータの性質として理解するのではなく、何らかのデータを処理する目的[76]が個人識別であるときは、当該処理に用いられる全てのデータは個人識別のための要素という意味での個人データとなると理解しなければならない。

そして、GDPRは、第4条(4)において「プロファイリング」を「自然人と関連する一定の人格的側面を評価するために、とりわけ、当該自然人の業務遂行能力、経済状態、健康、個人的嗜好、興味関心、信頼性、行動、位置及び移動に関する側面を分析または予測するために、個人データの利用によって構成される、全ての形態の、個人データの自動的な処理」を意味するものと定義した上で、第22条第1項において、「データ主体は、プロファイリングを含め、自動化された処理のみに基づいて、彼もしくは彼女に関する法的効果を発生させ、または、彼もしくは彼女に対して類似の影響を及ぼす判定の対象とされない権利をもつ」と定めている[77]。

EUの個人データ保護法制上ではこのように定められており、事後的にせよ、当該個人データのデータ主体から何らかの権利行使を可能とする法制またはそのような自動処理による法律効果の発生を阻止する法制を構築し、プロファイリングによる濫用的な影響を排除し得る方策を試み続けているものと理解することは可能である。これは、仮に匿名化措置を施した個人データであっても、また、それ自体としては個人データではないデータであっても、ビッグデータを用いたプロファイリング等による関係性の推論が自動的かつ極めて短時間で大量に実行可能となってしまっている現実[78]を踏まえたものと考えられる。

以上のことは、基本的には、日本国の個人情報保護法制における特定個人情報及

び匿名加工された個人情報との関係においても同じである。上述のとおり、ある個人データが暗号化等により匿名化されたとしても、個人情報は、それが電子計算機によって処理可能な何らかの符号列であり続ける限り、符号列それ自体としての識別力を失うことはないので、日本国の関連法令は、それ自体において自己矛盾が存在する(79)。

以上を要するに、オープンデータ政策を推進する上で、個人データとして認識できない非個人データ及び匿名化された個人データのみをオープンデータとして自由なアクセスを認める場合、その後の（プロファイリング等の）自動処理による個人識別性の回復の可能性が常に存在する以上、そのことを踏まえた法政策が検討されなければならない。それを前提とした上で、現実に問題が発生した場合には、問題発生時点において個人データとして識別可能なデータの処理を実施する者の法的義務及び権利が検討されなければならないことは当然のこととして、その問題が自動処理等による識別性の回復が実行される前の段階において非個人データとしてアクセスを認めた者の法的責任も検討されなければならない。これは、今後の重要な検討課題である。そのような検討を行う場合、匿名化等を施しただけでは個人識別性の回復可能性を完全に消滅させることが原理的に不可能なことであることを明確に認識・理解することが重要である。そして、それゆえに、（高度な人工知能技術の応用の場合を含め）現代及び近未来の極めて高度な情報処理技術の環境を前提とする限り、当該匿名化等の措置を施したというのみでは完全な免責事由とはなり得ないことを正しく理解すべきである(80)。

3．2　その他の法令との関係

情報へのアクセス及びアクセスの結果獲得した情報やデータの二次利用（特にデータ経済振興政策）と関連するが、直接的にはEUの機関及び組織が保有する文書へのアクセス及びオープンデータ政策とは目的を異にする関連法令との関係について、若干の検討を試みる。これらの諸点に関しては、欧州委員会において詳細な調査検討が進行中であることから、それらの調査検討結果を尊重した上で更に深く検討を加えなければならないが、そのためには、そのような調査検討結果を可能な限り素早く正確に把握・理解する努力を継続する必要性がある。

3．2．1　データベース関連法令との関係

データベース保護指令96/9/EC(81)は、データベースに関し、著作権による保護と*sui generis*の権利による保護の2つの態様を定めている。前者は、ベルヌ条約第2条(5)に定める「素材の選択又は配列によって知的創作物を形成する百科辞典及び選集のような文学的又は美術的著作物の編集物」(82)の著作権による保護と基本的には同じものである(83)。後者は、「作成された（created）」データで構成されるデータベースではなく、他から「獲得された（obtained）」で構成されるデータベースの保護を目的とするものである(84)。データベース保護指令96/9/ECの第8条は、*sui generis*の権利によって保護されるデータベースからのデータの抽出（extraction）及び二次利用（re-utilizing）に関する利用者の権利も定める(85)。

データベース保護指令96/9/ECの前文(48)第1文は、「この指令の目的は、データベース構築者の収益を守る手段としての適切かつ統一されたレベルのデータベースの保護を与えることであって、基本的な権利、すなわち、人権及び基本的な自由の保護のための欧州条約第8条の中で認められているプライバシーの権利を保護するために策定された整合性のある規定に基づき、個人データの支障のない流通を保証するためのものである個人データの処理と関連する個人の保護及びそのデータの支障のない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とは異なるものである」と述べつつ、その第2文において「この指令の条項は、データ保護立法を妨げるものではない」と述べている。それゆえ、データベース保護指令96/9/ECは、EUの個人データ保護法令の条項と抵触しないように解釈・運用されなければならない。知的財産権の一種としての著作権及び*sui generis*の権利は、個人データ保護法令の条項を無効化（override）できない。

しかしながら、委員会スタッフ作業文書SWD(2018) 146 finalでも詳しく触れられているとおり、データベースの利用に関しては、データベース保護指令96/9/ECに定める条項に違反しない限り、契約（約款）(86)による規律のほうが一般的である。それゆえ、実際問題としては、データベースの利用と関連する契約（約款）の条項の個人データ保護法令との適合性が吟味されなければならず、構成国の監督機関もそのような職責を負う。

すなわち、GDPRの第25条第1項は、「最新技術、実装費用、処理の性質、範囲、過程及び目的並びに処理によって示される自然人の権利及び自由に対する様々な

蓋然性と深刻度のリスクを考慮に入れた上で、管理者は、本規則の要件に適合するものとし、かつ、データ主体の権利を保護するため、処理の方法を決定する時点及び処理それ自体の時点の両時点において、データのミニマム化のようなデータ保護の基本原則を効果的な態様で実装し、その処理の中に必要な安全性確保措置を統合するために設計された、仮名化のような、適切な技術上及び組織上の措置を実装する」と定め、当該個人データの処理がデータベースの利用という形態で提供される場合、この「組織上の措置」の中にはそのデータベースの利用のための契約（約款）が含まれる。すなわち、当該契約（約款）は、GDPR第25条第1項を満たすものでなければならない。規則(EC) No 45/2001が適用される場合でも同様である。

また、GDPRの第35条は、個人データ処理の管理者が個人データ処理を開始する前にデータ影響評価を実施しなければならないことを定めているから、当該個人データの処理がデータベースの利用という形態で提供される場合、そのデータベースの管理者は、そのデータベースの利用に適用される契約（約款）の内容を含めて事前の影響評価を実施しなければならない。そして、GDPRの第36条第1項は、「そのリスクを削減させるために管理者によって講じられる措置が存在しなければ自然人の権利及び自由に対して高度のリスクをもたらすおそれがあるということを第35条に基づくデータ保護影響評価が示している場合、管理者は、その処理を開始する前に、監督機関と協議する」と定め、更に、同条第2項は、「第1項に示す予定されている処理が本規則に違反し得るとの見解を監督機関がもつときは、とりわけ、管理者がリスクの特定及び削減について不十分であるときは、その監督機関は、協議の要請を受理した時から8週間以内に、その管理者に対し、及び、適用可能なときは、処理者に対し、書面による助言を提供し、また、第58条に示す権限中のいずれかを用いることもできる。この期限は、予定されている処理の複雑性を考慮に入れた上で、6週間延長できる。その監督機関は、その管理者に対し、及び、適用可能なときは、処理者に対し、協議の要請を受領した時から1か月以内に、その遅延の理由を付して、そのような期限延長を通知する。これらの期限は、監督機関が協議のために求めた情報を入手するまでの間、その進行を停止させることができる」と定めている。

監督機関は、以上のようなGDPR第35条の事前評価の適正性・合理性・説得性を審査する能力をもち、かつ、第36条の事前協議を効果的に実行するための能力

をもたなければならないのである。当該個人データの処理がデータベースの利用という形態で提供される場合、それら全ての過程において、監督機関は、当該データベースの利用に適用される契約（約款）が個人データ保護法令の条項を遵守し、これに適合するものであるか否かを判断する能力をもたなければ、その職責を果たしているとは言えない。

以上のことは、日本国の個人情報保護委員会及び個人情報保護審査会並びに裁判所の職務にも直接の影響を与えるものである。特に、EU との間で個人データの第三国移転に関する判定（GDPR 第 45 条第 3 項）が行われた場合、または、日本国と EU との間においてそれと均等な相互承認が行われた場合には、EU におけるとの均等な個人データの保護を日本国内において提供しなければならず、そのように提供されているか否かをこれらの機関が担うことになるので、これらの機関の職務に従事する者は、情報処理及び個人データ保護に関するかなり熟達した知識と能力が要求されることになるであろう(87)。

以上のほか、非個人データであるデータの国境を越える流通のためには、知的財産権（特に著作権）と関連する調整も必要になる。関連する法令として、オンラインコンテント可搬性規則 (EU) 2017/1128（OJ L 168, 30.6.2017, p.1-11）(88) がある。詳細は、割愛する。

3．2．2　非個人データ関連法案との関係

個人データ保護法制と非個人データ保護法制とが交錯する領域における本質的な問題の所在は、上述の「オープンデータ関連法令との関係」（3.1.3）において述べたところと基本的には同じである。ここでは、EU における非個人データの流通促進政策(89) と個人データ保護法令との関係の要点のみを簡略に述べる。

委員会通知「共通の欧州データ空間に向けて」COM(2018) 232 final(90) は、「欧州委員会は、データ集約型産業の枠組み条件を向上させるための重要な措置を既に実装した。一般データ保護規則（OJ L 119, 4.5.2016, p.1.）と共に、EU は、データ経済の持続的な発展のための前提条件であるデジタル信頼のための堅固な枠組みをつくり出した。一般データ保護規則は、高いレベルのデータ保護を保証している。2018 年 5 月 25 日に発効となる新たな法令によって影響を受ける者は全て、全面的な遵守を確保する必要がある。信頼できる受容可能なデータ技術に基づく将来の競争上の優位性のための基礎を構築するため、EU のデータ保護法令によっ

て与えられたEU内における個人データの支障のない移動は、2017年9月に提案された規則案（COM(2017) 495 final）に基づき、非個人データの支障のない流れによって補完されることになる」と述べている。

規則案（COM(2017) 495 final）の第4条第1項は、非個人データに関し、「欧州連合内におけるデータの記録保存またはそれ以外の処理の所在は、特定の構成国の領土に限定されてはならず、かつ、別の構成国における記録保存またはそれ以外の処理は、公共の安全を根拠として正当化される場合を除き、禁止または制限されてはならない」と定め、同条第2項は、「構成国は、指令(EU) 2015/1535を実装する国内法に定める手続に従い、欧州委員会に対し、データの新たなローカル化要件を導入する法令案、または、既存のデータローカル化要件の変更を行う法令案を通知する」と定めている(91)。ここでいう「データローカル化要件」とは、「構成国の法律、規則または行政規則に定める義務、禁止、条件、制限またはそれ以外の要件であって、データの記録保存もしくはそれ以外のデータ処理の所在を特定の構成国の領土内に限定するもの、または、別の構成国内における記録保存もしくはそれ以外のデータ処理の所在を妨げるもの」のことを意味する（同規則案第3条第5号）。

このような非個人データの支障のない移動と個人データ保護との関係に関し、規則案（COM(2017) 495 final）の前文(9)は、「個人データの処理と関連する自然人の保護に関する法的枠組み、とりわけ、規則(EU) 2016/679、指令(EU) 2016/680及び指令2002/58/ECの法的枠組みは、この規則によって影響を受けない」と述べ、前文(29)は、EUの法令の中にしばしばみられる定型文言ながら、「この規則は、基本的な権利を尊重し、とりわけ、欧州連合基本権憲章によって認められた基本原則を尊重しなければならず、かつ、個人データの保護の権利（第8条）、事業遂行の自由（第16条）並びに表現及び情報伝達の自由（第11条）を含め、これらの権利及び基本原則に従って解釈され、適用されなければならない」と述べているので、非個人データの移動に関する法令と個人データの移動に関する法令との間に矛盾が生ずる場合には、個人データ保護法令のほうが優先的に適用されることになる(92)。

このような基本的な法的枠組みを前提とした上で、規則案（COM(2017) 495 final）の前文(10)は、「この規則は、利用者の施設に存在しているか、データの記録保存またはそれ以外のデータ処理サービスプロバイダにアウトソースされている

かを問わず、全てのタイプの IT システムの利用を含む最も広い意味におけるデータの記録保存またはそれ以外のデータ処理に適用されなければならない。この指令は、データの記録保存（Infrastructure-as-a-Service (IaaS)）から、プラットフォーム上のデータ処理（Platform-as-a-Service (PaaS)）またはアプリケーションによるデータ処理（Software-as-a-Service (SaaS)）まで、異なるレベルの密度のデータ処理を包摂しなければならない。これらの異なるサービスは、データの記録保存またはそれ以外のデータ処理が、サービスプロバイダと消費者または企業利用者との間におけるオンライン市場の中間介在行為のような、異なるタイプのサービスに付随するサービスに過ぎないものである場合を除き、この規則の適用範囲内にあるものとしなければならない」と述べている(93)。

しかしながら、既述のとおり、非個人データと個人データとの境界は、当該データそれ自体の固定的属性として決定することができず、社会的関係または社会的文脈の中で初めて決定され得るような場合が多々ある(94)。例えば、非個人データのみで構成されるデータベースから抽出されるデータが（プロファイリング等により）個人識別の目的で処理される場合、社会的には、当該データは、非個人データとしてではなく、個人データとして収集されることになるのであるが、当該データベースの標準約款がそのような利用を想定していない場合、監督機関としては何を監督すべきであるのかが明確ではない。理論的には、当該データベースの管理者が利用者に対してその利用目的を査問・吟味し、関連する全ての個人データ保護法令の条項に適合すると判断した上でなければ当該データベースの利用を許可しないような組織上及び技術上の安全性確保措置が講じられているか否かが監査されなければならないであろうが、その具体的な方法を確定することは、かなり困難なことである(95)。

特に、規則案（COM(2017) 495 final）が想定しているようなクラウド上のデータ処理及び仮想データ処理の場合、監督機関の所在地及び管轄権の及ぶ範囲とは全く無関係に物理処理システムが存在しているのが普通であるので、その困難性が特に顕著であり、かつ、著しい(96)。

このような個人データ保護のための監督機関の監督のためのものとは限らないが、非個人データの移動と関連する法令に関して監督権限をもつ機関によるデータへのアクセスに関し、規則案（COM(2017) 495 final）の第 5 条第 1 項は、「この

規則は、職務権限を有する機関が、欧州連合法または国内法に従い、その公的職務の遂行のためにデータへのアクセスを要求し、そのアクセスを得るための権限を害さない。職務権限を有する機関に対し、そのデータが別の構成国において記録保存され、または、それ以外の処理をされていることを根拠として、そのアクセスを拒否してはならない」と定めている(97)。

これらの諸点に関しては、規則案（COM(2017) 495 final）が提案中の法案であり採択された法令ではないこともあるが、今後、関連法令全部を含め、更に検討を要することだけは確かである(98)。

4　まとめ

本稿において述べたように、現代社会においては、個々のデータそれ自体としては個人識別性がないと認められる場合であっても、極めて高度なデータ処理、特に、人工知能技術、ビッグデータ技術及びプロファイリング技術を応用した分析により、個人識別の目的のために利用可能な状況となっているという事実を明確に認識した上での法政策及び法解釈が求められている。高度であり汎用性のあるデータベースシステムは、潜在的には、高度な個人データ処理の目的のために使用可能なものであることが多いと考えられるが、そのようなシステムについてバイデザインの原則及びバイデフォルトの原則（GDPR第25条）をどのように適用すべきであるか、特に、そのような原則の適用・遵守を監督機関が監査・監督するための能力を客観的にもっているといえるか否かに関しては、謎のままであると言わざるを得ない。このことは、組織内のデータ保護責任者（Data Protection Officer）及び組織外の第三者監査機関や第三者認証機関(99)においても全く同じである。現代の最先端技術は、現時点におけるその質及び量において、既に人間または人間の組織による監査・監督の能力をはるかに超えてしまっている可能性がある。このことは、憲法論または法哲学の側面に沿って言うと、「現代社会においては、人類が人権保障のための現実的な能力及び手段を喪失しつつある」と換言することもできる。そのようにして高邁な理論や政治的イデオロギーを振りかざすだけでは全く無力な時代に人類全体が突入してしまっている以上、現実に存在する情報処理技術

の本質と機能、そして、それらを用いたシステムが誰によってどのように運用されているのかを正確に認識・理解した上で、意味のある理論及び方策が検討されなければならない。そのような検討において最も重視されなければならない判断基準は、実効性（effectiveness）及び比例性（proportionality）である。

頁数制限のため、ごく簡単に触れることしかできなかった部分、特に仮想化システム及び仮想化技術(100) との関係並びに製造物責任指令(101) との関係については、他日を期したいと思う。

以上（2018 年 10 月 26 日脱稿）(102)

（明治大学法学部教授）

注

(1) 夏井高人「委員会通知 COM(2018) 43 final [参考訳]」法と情報雑誌 3 巻 5 号 115～132 頁 (2018) 参照。

(2) 夏井高人「規則 (EC) No 45/2001 [参考訳・改訂版]」法と情報雑誌 2 巻 5 号 111～146 頁 (2017) 参照。

(3) 本稿においては、特に明示しない限り、現在の EU（European Union）において有効な法令及び提案されている法案を示すという趣旨で「EU」との語を用いる。この場合、文脈により、現在の European Union という意味での EU のみならず、その前身である European Community 及び European Communities（European Economic Community、European Atomic Energy Community 及び European Coal and Steel Community）の時代を含め、総称的に用いることがある。これは、現行の法令でありながら、リスボン条約以前の時代に採択され、発効し、現在でも EU 域内において有効な法令が多数存在するためである（日本国においても、その立法手続上、現行の日本国憲法が大日本帝国憲法の改正法として制定されたことからも理解できるとおり、明治時代と現在では国名が異なるけれども、国家である日本国としての国際法上及び実力上の同一性は失われていない。日本国憲法は、形式的には改正後の法令であるので、そもそも「不磨の大典」の類ではあり得ない）。また、文脈により、2018 年 10 月 30 日現在の時点における European Union の地理的範囲（EEA 諸国を除く EU の主権の及ぶ範囲）を指すものとして「EU」との語を用いることがある。なお、EEA 諸国の法制に関しては、Carl Baudenbacher (Ed.), *The Handbook of EEA Law*, Springer (2015) が参考になる。

(4) EU の電子通信部門（電気通信部門）における個人データ保護法制及び現在の法改正の動向に関しては、夏井高人「欧州共同体のオープンネットワーク提供（ONP）指令に基づく基本要件―通信の秘密条項及び個人データ保護と関連する規定の概要―」法律論叢 91 巻 2・3 号掲載予定で述べたとおりである。なお、EU（EEC, EC）における通信の自由化に伴う ONP 指令の採択から 2002 年改正を経て 2009 年改正に至るまでの EU の通信法制と競争法制との関係については、Christian Koenig, Andreas Bartosch, Jens-Daniel Braun & Marion Romes (Eds.), *EC Competition and Telecommunications Law*, Wolters Kluwer (2009)、Laurent Garzaniti & Matthew O'Regan (Eds.), *Telecommunications, Broadcasting and the Internet: EU Competition Law and Regulation (3rd edition)*, Sweet & Maxwell

(2010)、Andrej Savin, *EU Telecommunications Law*, Edward Elgar (2018) が参考になる。

(5) GDPR 以外の個人データ保護と関連する法令の非網羅的な一覧は、夏井高人「規則 (EU) 2016/679（一般データ保護規則）[参考訳・再訂版]」法と情報雑誌 3 巻 5 号 1～114 頁 (2018) の冒頭部分において示したとおりである。EU の個人データ保護及びプライバシー保護の全体像を知るためには、GDPR のような代表的な法令を調査・検討するだけでは全く足りず、関連法令全部を可能な限り調べ、特に法令または条項の適用関係（優先劣後関係）に関し、それらの法令または条項との間の相互関係を十分に理解しなければならない。個人データ保護指令 95/46/EC が適用されていた当時、日本国内においては、「個人データ保護指令 95/46/EC さえ理解すれば EU の個人データ保護法制全体を理解できる」といった類の誤解が流布されていたことがあるが、GDPR についても同じ愚を繰り返してはならない。

(6) 夏井高人「データ駆動型経済通知 COM(2014) 442 final [参考訳]」法と情報雑誌 3 巻 4 号 129～147 頁 (2018) 参照。

(7) 夏井高人「欧州のための人工知能通知 COM(2018) 237 final [参考訳]」法と情報雑誌 3 巻 9 号 198～232 頁 (2018)、同「欧州データ空間通知 COM(2018) 232 final [参考訳]」同誌 3 巻 10 号 107～127 頁 (2018)、同「欧州委員会スタッフ作業文書 SWD(2018) 146 final [参考訳]」同誌同号 144～200 頁 (2018) 参照。

(8) 夏井高人「アシモフの原則の終焉―ロボット法の可能性―」法律論叢 89 巻 4・5 号 175～212 頁 (2017)、同「ロボット法の制定を求める欧州議会決議 [参考訳]」法と情報雑誌 2 巻 5 号 438～492 頁 (2017) 参照。

(9) 夏井高人「情報社会の素描―EU の関連法令を中心として―（1）」法律論叢 90 巻 4・5 号 135～181 頁 (2018) 及び同「情報社会の素描―EU の関連法令を中心として―（2・完）」同誌 90 巻 6 号 165～211 頁 (2018) 参照。

(10) 第 5 世代移動体通信技術（5G）を含め、最新の情報技術の発展が（現代及び将来の）社会及び法制度に与える影響に関しては、本稿における考察の対象外とする。他日を期したい。

(11) 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 (2014) 参照。

(12) 脚注 5 参照。

(13) 夏井高人「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―」法律論叢 89 巻 2・3 号 181～245 号 (2016) 参照。

(14) GDPR の前文 (16) 参照。

(15) GDPR の前文 (18) は、「私的な行為または家庭内の行為は、手紙のやりとり及び宛名の保管、または、そのような行為の過程で行われるソーシャルネットワーキング及びオンラインの行為を含み得る」と説明している。

(16) GDPR の前文 (19) 参照。

(17) 指令 (EU) 2016/680 は、指令（Directive）であるので、構成国に対して直接に効力をもつわけではなく、各構成国は、同指令に定める内容を実装する国内法令を採択し、適用しなければならない。同指令の実装期限は、2018 年 5 月 6 日と定められている（同指令第 63 条第 1 項第 1 副項）。それゆえ、同指令の現実の運用を正確に知るためには、各構成国における同指令の実装法令の条項及び関連文書等を丹念に調査・検討する必要がある。

(18) 欧州委員会の長である Jean-Claude Juncker 氏も規則 (EC) No 45/2001 に完全に服さ

なければならない。

(19) 日本国の個人情報保護法制においては、いずれの法令も明示に適用を受けない国家機関が多数存在することが定められている。行政機関個人情報保護法（平成 15 年法律第 58 号）の中にも適用除外条項がある。例えば、国の象徴である天皇、立法機関である国会、行政機関である内閣府（同法第 2 条第 1 項第 2 号）、日本国憲法上の特別行政機関である会計検査院（同法第 2 条第 1 項第 6 号）、司法機関である裁判所に適用される一般的な個人情報保護法令が存在しない。換言すると、これらの分野に関しては、個人情報保護における明確な法の支配が存在しない。また、会計検査院法第 5 節（行政機関個人情報保護法第 19 条の 2 ないし第 19 条の 6）は、個人情報保護審査会を定めているが、個人情報保護審査会自体それ自体は行政機関個人情報保護法の適用を受けないと解される（同法第 2 条第 1 項第 6 号）。そして、日本国の最高裁は、「裁判所が司法行政事務に関して保有する個人情報の取扱要綱」を定めているが、これは法律ではなく、強いて言えば、内部的な運用指針の一種に過ぎない。日本国の法制においては、EU における EDPS、EDPB 及び構成国の監督機関並びに司法裁判所のいずれもが、関連する個人データ保護法令に完全に服さなければならないのとは全く異なり、日本国の国家機関としては、個人情報保護における明確な法の支配の下にある不服申立機関が全く存在しないことになると解される（GDPR 第 45 条第 1 項 (a) 参照）。これらのことは、今後のグローバルな規模でのデジタル化社会またはデータ駆動型経済社会の到来により、現在におけるデータ処理とはまるで比較にならない大量の個人データが自動処理される時代が必ず到来することを考えると、日本国の国家政策における致命的な欠陥であると考える以外にない。そのことは、もし何らの改善も見られない場合には、日本国の産業界にとっても再起不能な結果を招く致命的な打撃を与えることになるであろう。

(20) 個人データの保護と関連する EU の特別法令に関しては、前掲「情報社会の素描―EU の関連法令を中心として―（1）」及び「情報社会の素描―EU の関連法令を中心として―（2・完）」の中で既に詳細に述べた。

(21) 夏井高人「規則 (EC) No 45/2001 の改正案 [参考訳]」法と情報雑誌 2 巻 4 号 249～354 頁 (2017) 参照。

(22) 夏井高人「電子商取引指令 2000/31/EC [参考訳]」法と情報雑誌 3 巻 1 号 110～141 頁 (2018) 参照。電子商取引指令 2000/31/EC は、情報社会サービスに適用される。同指令の第 2 条 (a) は、「情報社会サービス」について、「指令 98/48/EC による改正後の指令 98/34/EC の第 1 条 (2) の意味におけるサービスのことを意味する」と定義している。指令 98/34/EC（OJ L 204, 21.7.1998, p.37-48）及び指令 98/48/EC（OJ L 217, 5.8.1998, p.18-26）は、指令 (EU) 2015/1535（OJ L 241, 17.9.2015, p.1-15）の第 10 条及び別紙 III によって、2015 年 10 月 7 日をもって廃止された。その経過等に関しては、指令 (EU) 2015/1535 の前文 (1) の脚注内に解説がある。「情報社会サービス」との語は、指令 98/48/EC による改正によって出現したものであり、同指令による改正後の指令 98/34/EC の第 1 条 (2) 第 1 副項は、「サービス」について、「情報社会サービス、換言すると、通常、対価を得るために、隔地者間で、電子的な手段により、かつ、サービスを受ける者の個別の要求に応じて提供されるサービスのことを意味する」と定義し、それに続けて、「隔地者間で」、「電子的な手段により」及び「サービスを受ける者の個別の要求に応じて」の意義を定義している。現行の指令 (EU) 2015/1535 の第 1 条第 1 項 (b) 第 1 副項は、「サービス」について、指令 98/48/EC による改正後の指令 98/34/EC の第 1 条 (2) 第 1 副項の定義を踏襲した上で、「隔地者間で」について、「当事者が同時に現在することなく、その

サービスが提供されることを意味し」（第2副項(i)）と、「電子的な手段により」について、「（デジタル圧縮を含め）処理のための電子装置及びデータの記録保存によって、サービスが最初に送られ、その到達地において受領され、かつ、有線により、無線により、光学的な手段により、または、それ以外の電磁的な手段によって、その全体が送信され、運搬され、受領されることを意味し」（第2副項(ii)）と、そして、「サービスを受ける者の個別の要求に応じて」について、「個別の要求に関するデータの送信を介してそのサービスが提供されることを意味する」（第2副項(iii)）とそれぞれ定義し、加えて、同指令の別紙Iの中で細目的な定義を更に定める旨を規定している（第3副項）。他方、サービスプロバイダの業務一般に関しては、サービス指令2006/123/EC（OJ L 376, 27.12.2006, p.36-68）が定めるところである。同指令の第34条は、同指令の実装・運用においては、個人データ保護指令95/46/EC及びeプライバシー指令2002/58/ECに服するべき旨を規定している。これらの点を含め、夏井高人「指令(EU) 2015/1535 [参考訳]」法と情報雑誌3巻7号1～20頁(2018)、同「指令98/34/EC [参考訳]」同誌同号21～39頁(2018)、同「指令98/48/EC [参考訳]」同誌同号51～66頁(2018)参照。

電子商取引指令2000/31/ECは、消費者のオンライン取引を主たる適用対象とする法令である。現代のネットワーク化されたデジタル社会において最も大きな額の取引が日々実行されている金融部門及びその関連部門における法令に関しては、夏井高人「電子マネー指令2009/110/EC [参考訳]」同誌2巻12号1～23頁(2017)、同「決済サービス指令(EU) 2015/2366（PSD2）[参考訳]」同誌3巻2号1～115頁(2018)、同「金融商品市場指令2014/65/EU（MiFID II）[参考訳]」同誌3巻3号1～175頁(2018)、同「金融商品市場規則(EU) No 600/2014（MiFIR）[参考訳]」同誌3巻4号1～79頁(2018)及び同「OTCデリバティブ規則(EU) No 648/2012 [参考訳]」同誌3巻8号1～96頁(2018)参照。金融商品の取引及び仮想通貨取引と関連する国際犯罪及びテロリスト犯罪等の犯罪行為としての側面に関しては、同「FinTech通知COM(2018) 109 final [参考訳]」同誌3巻8号181～200頁(2018)参照。

(23) Arno R. Lodder & Andrew D. Murray (Eds.), *EU Regulation of e-Commerce: A Commentary*, Edward Elgar (2017), p.50参照。

(24) GDPRの第17条第2項は、「忘れられる権利（right to be forgotten）」の具体的な内容として、「管理者が個人データを公開のものとしており、かつ、第1項によって、その個人データを削除すべき義務を負っている場合、その管理者は、利用可能な技術及びその実装費用を考慮に入れた上で、技術的な手段を含め、その個人データを処理している管理者に対して、そのデータ主体が、そのデータ主体の個人データへのリンクまたはそのコピーもしくは複製物が、その管理者によって削除されることを請求した旨の通知をするための合理的な手立てを講ずる」と定めている。この条項は、例えば、インターネット上でホスティング（hosting）のサービスを提供するプロバイダが削除義務を負う場合に適用され得る。キャッシング（caching）と称するサービスを提供するプロバイダの場合であっても、例えば、そのサービスを全体的（包括的）に考察した場合において、そのサービスの実質がクラウド上でミラーサイトを仮想的に提供するようなサービスに該当すると判断可能なときは、純粋に機械的な処理のための短時間のキャッシングの一種であると認めることができず、（経済学的な意味または経営理論上のビジネスモデルとしての分類ではなく）法適用の関係においては、ホスティングの一種に該当するものと考えるべきである。また、そのような実質的にみて仮想的なミラーサイトのサービスを提供するクラウドベンダは、「単なる導管（mere conduit）」であると理解することもできない。

(25) 警察・検察関係については、GDPR の特別法である指令 (EU) 2016/680 が適用されることは、既述のとおりである。ただし、指令 (EU) 2016/680 の適用のない分野に関し、EU 司法裁判所の判例法により、構成国が適用除外事項に対して個人データ保護条項を定めることは、一定範囲で認められている。すなわち、個人データ保護指令 95/46/EC に関する判例ではあるが、*Lindqvist*, Case C-101/01, 6 November 2003, ECLI:EU:C:2003:596 があり、そのパラグラフ 98 は、「On the other hand, nothing prevents a Member State from extending the scope of the national legislation implementing the provisions of Directive 95/46 to areas not included within the scope thereof, provided that no other provision of Community law precludes it」と判示している。これを現行の GDPR にあてはめて読み替えると、構成国は、EU 法の中に禁止条項が存在しない限り、GDPR に定めない事項に個人データ保護を拡張する条項を国内法として定めることが可能であると解釈できる。なお、Daniel Rücker & Tobias Kugler (Eds.), *New European General Data Protection Regulation: A Practitioner's Guide*, Nomos (2017), p.22 参照。個人データ保護と関連する判例法全般に関しては、Laraine Laudati(OLAF Data Protection Officer), *Summaries of EU Court Decisions relating to Data Protection 2000-2015*, OLAF(28 January 2016) が参考になる。

(26) 例えば、構成国の行政機関が管理者（controller）である場合、GDPR に定める個人データの管理者としての権利及び義務並びに関連手続等に関する条項が全て直接に適用される。処理者（processor）、データ保護責任者（data protection officer）に関しても全く同じであるが、特に、データ保護責任者の職務の独立性に関する条項の直接適用が重要である。これらの事項について国内法を定める場合、GDPR の関連条項と全く同じ内容の条項にしなければならず、もし構成国の国内法の中にそのような法令または条項が存在しない場合には、該当する GDPR の関連条項を直接に適用して活動及び判断を行うことになる。

なお、構成国の行政機関または職員であっても、EU の機関として活動する場合には、EU の機関及び組織に適用される規則 (EC) No 45/2001 が適用されることになる。例えば、BEREC 規則 (EC) No 1211/2009（OJ L 337, 18.12.2009, p.1-10）に基づく個人データ処理に関し、構成国の代表で構成される BEREC 及びその事務局との関係においては規則 (EC) No 45/2001 が適用され、構成国の国内規制当局（NRA）との関係においては GDPR（2018 年 5 月 24 日以前の時点においては、個人データ保護指令 95/46/EC に基づいて各構成国において実装された国内法令）が適用され、また、電子通信と関係する個人データ処理に関しては BEREC 及び事務局並びに NRA のいずれについても e プライバシー指令 2002/58/EC に基づいて各構成国において実装された国内法令が適用される（寺田麻佑『EU とドイツの情報通信法制―技術発展に即応した規制と制度の展開』（勁草書房、2017）、夏井高人「BEREC 規則 (EC) No 1211/2009 [参考訳]」法と情報雑誌 3 巻 10 号 1～17 頁 (2018) 参照）。それゆえ、一般に、EU の構成国の機関において適用される個人データ保護法令を正確に知るためには、当該行政行為がどのような法的性質をもつものであるのか、その行政行為の根拠法令は何であるのかが精密に検討されなければならない。

この点に関し、日本国の法制においては、国の委任事務として自治体の機関またはその職員が活動する場合の法適用の関係が曖昧な場合があり、例えば、当該自治体の個人情報保護条例のみが適用されると解されるような混乱した状況にある。しかし、それが国の委任事務である以上、自治体住民（国民）は、国の行政機関等として、行政機関個人

情報保護法（平成15年法律第58号）及び独立行政機関等個人情報保護法（平成15年法律第59号）が適用されること、そして、同一内容の国の委任事務に関しては、異なる自治体においても全て均等な取扱い（treatment/handling）を受けると合理的に期待することについて、法的利益があることを認識・理解すべきである。一般に、法的安定性を確保するため、国の委任事務に関しては、適用される法令の明確化が望まれる。

(27) EU及びその構成国の行政行為の特徴や基本構造に関しては、Carol Harlow, Päivi Leino & Glacinto Della Cananea (Eds.), *Research Handbook on EU Administrative Law*, Edward Elgar (2017)が参考になる。

(28) 各構成国の関連条項の全てが正確に修正されているとは想定し難いし、修正されたはずの箇所の中にも誤りがあり得る。GDPRそれ自体の中においてさえも（誤記を含め）多数の誤りが存在している。それらの誤りの中の重要なものについては、2018年5月23日付けの「Corrigendum to Regulation (EU) 2016/679」として、EU官報上で修正箇所が公表されている（OJ L 127, 23.5.2018, p.1-5）。

(29) Müge Fazlioglu, *What the GDPR Requires of and Leaves to the Member States*, CIPP/US
https://iapp.org/media/pdf/resource_center/GDPR-Derogations-Whitepaper-FINAL.pdf [2018年10月19日確認]

(30) 制裁に関して、GDPRの第84条、前文(151)参照。

(31) 脚注20参照。

(32) 夏井高人「指令2002/58/EC [参考訳・改訂版]」法と情報雑誌2巻5号158～187頁(2017)、丸橋透・夏井高人「指令2002/58/ECの改正案 [参考訳]」同誌2巻4号195～248頁(2017)参照。なお、脚注4参照。

(33) 脚注17参照。

(34) 夏井高人「PNR指令(EU) 2016/681 [参考訳]」法と情報雑誌2巻3号119～155頁(2017)、丸橋透「搭乗者名記録(PNR)データの移転および処理に関するカナダと欧州連合間の協定案に関する欧州議会からの意見請求事件(1/15)欧州連合司法裁判所（大法廷）意見(2017年7月26日)ECLI:EU:C: 2017:592 [参考訳]」同誌2巻8号186～256頁(2017)、同「カナダ国境サービス庁による国家安全保障目的での旅行者のシナリオベース標的絞り込みについてのカナダプライバシーコミッショナーオフィスのプライバシー監査報告（2017年9月21日）[参考訳]」同誌2巻10号21～39頁(2017)、Olga Mironenko Enerstvedt, *Aviation Security, Privacy, Data Protection and Other Human Rights: Technologies and Legal Principles*, Springer (2017)参照。

(35) 夏井高人「API指令2004/82/EC [参考訳]」法と情報雑誌2巻5号60～70頁(2017)参照。

(36) 夏井高人「NIS指令(EU) 2016/1148 [参考訳・改訂版]」法と情報雑誌2巻8号120～163頁参照。

(37) 犯罪立証のための証拠としての通信データの捜査機関による一時的な保持(retention)を確保するために、データ保持指令2006/24/EC（OJ L 105, 13.4.2006, p.54-63）が制定されていた。しかし、欧州司法裁判所の*Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, Joined Cases C-293/12 and C-594/12, 8 April 2014, ECLI:EU:C:2014:238により、同指令は全部無効であると判断された。その結果、同指令は、2014年4月8日をもって無効な法令となった。それゆえ、構成国は、同指令を実装・運用すべき義務を

負わない。なお、データ保持指令 2006/24/EC は、欧州評議会（Council of Europe）のサイバー犯罪条約（CETS No.185）に定める提出命令（production order）及び保全命令（preservation order）に関して直接に定める法令ではないが、これらの命令と密接な関連をもつ法令であった。ところが、データ保持指令 2006/24/EC が無効となった結果、構成国の法令に基づく捜査令状を他の構成国において執行する場合の間接的な手続である EU 捜査命令（EIO）を定める指令 2014/41/EC（OJ L 130, 1.5.2014, p.1-36）を除くと、提出命令及び保全命令と関連する EU の統一的な法令が存在しないこととなり、各構成国の国内立法に任される状況となっている。このような状況は、国境を越える犯罪行為に関し、EU 域内における統一的かつ迅速な捜査活動を妨げるものである。そのため、現在、これらの命令と直接に関係する規則案 COM(2018) 225 final が提案され、審議されている。同提案に関しては、丸橋透「刑事における電子証拠の欧州提出命令及び欧州保全命令に関する欧州議会及び理事会の規則提案 COM/2018/225 final [参考訳]」法と情報雑誌 3 巻 8 号 201～275 頁が参考になる。なお、夏井高人「サイバー犯罪条約（ETS No.185）の説明書 [参考訳]」同誌 1 巻 6 号 1～132 頁 (2016)、同「指令 2014/41/EU [参考訳]」同誌 3 巻 7 号 199～245 頁 (2018)、同「指令 2014/42/EU [参考訳]」同誌同号 246～262 頁 (2018)、同「委員会通知 COM(2018) 226 final [参考訳]」同誌同号 328～357 頁 (2018)、丸橋透「Case C 362/14 *Maximillian Schrems v Data Protection Commissioner* ECLI:EU:C:2015:650 [参考訳]」同誌同号 358～397 頁 (2018) 参照。

(38) 夏井高人「安全の欧州連合第 11 次進捗状況報告書 COM (2017) 608 final [参考訳]」法と情報雑誌 2 巻 11 号 156～176 頁 (2017)、丸橋透「域内治安、国境及び移住分野の EU 中央情報システム間の相互運用性の枠組みを定める欧州議会と理事会の 2 つの指令案の影響評価書（委員会スタッフ作業文書）SWD/2017/0473 final 及びその要旨 SWD/2017/0474 final　[参考訳]」同誌 3 巻 1 号 199～332 頁 (2018) 参照。

(39) 夏井高人「ハイブリッドな脅威報告書（JOIN(2017) 30）[参考訳]」法と情報雑誌 2 巻 8 号 91～119 頁 (2017)、同「安全の欧州連合第 15 次進捗状況報告書 COM(2018) 470 final [参考訳]」同誌 3 巻 10 号 85～106 頁 (2018)、同指令 (EU) 2018/843 による改正後の指令 (EU) 2015/849 [参考訳] 同誌 3 巻 8 号 276～328 頁 (2018) 参照。

(40) TFEU 第 16 条第 1 項は、「Everyone has the right to the protection of personal data concerning them」と定め、第 2 項は、「The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities」と定めるが、第 3 項は、「The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union」とも定めている。

(41) これらの諸点に関しては、Hielke Hijmans, *The European Union as Guardian of Internet Privacy: The History of Art 16 TFEU*, Springer (2016) が参考になる。なお、個人データ保護と関連する権利の保護法益がプライバシーの利益であることについては、前掲「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―」及び夏井高人「欧州連合における個人データ保護の諸要素に関する考察」法律論叢90巻1号79～125頁(2017)で述べたとおりである。

(42) JIIP, *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases: Final report - Study*, European Commission (2018)、JIIP, *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases: Annex 1, In-depth analysis of the Database Directive, article by article*, European Commission (2018)、JIIP, *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases: Annex 6, Country grids*, European Commission (2018)及びJIIP, *Study in support of the evaluation of Directive 96/9/EC on the legal protection of databases: Annex 7, Bibliography*, European Commission (2018)。なお、前掲「欧州委員会スタッフ作業文書SWD(2018) 146 final [参考訳]」参照。

(43) 前掲「情報社会の素描―EUの関連法令を中心として―(2・完)」178～183頁参照。

(44) 夏井高人「法へのアクセス報告書[参考訳]」法と情報雑誌2巻6号136～158頁(2017)参照。

(45) 前掲「欧州データ空間通知COM(2018) 232 final [参考訳]」参照。

(46) 夏井高人「サイバー犯罪の研究(5)―サイバーテロ及びサイバー戦に関する比較法的検討―」法律論叢86巻2・3号85～133頁(2013)、同「委員会勧告(EU) 2017/1584 [参考訳]」法と情報雑誌3巻7号293～327頁(2018)、前掲「ハイブリッドな脅威報告書（JOIN(2017) 30）[参考訳]」参照。

(47) 前掲「欧州共同体のオープンネットワーク提供（ONP）指令に基づく基本要件―通信の秘密条項及び個人データ保護と関連する規定の概要―」、夏井高人「サイバー犯罪の研究(3)―通信傍受に関する比較法的検討―」法律論叢85巻6号363～420頁(2013)参照。

(48) 日本国の法令中において、このような意味におけるアクセス制御の考え方を明確に採用したものとしては、不正アクセス行為の禁止等に関する法律（平成11年法律第128号）がある。しかし、この法律だけに限定されることなく、ある者からの管理された情報へのアクセスの可否を制御することを目的とする法令は、全てアクセス制御の考え方によってモデル化して説明することが可能である。

(49) 例えば、歴史上の事実を根拠とする法制史を踏まえた法理論研究においては、米国における情報の自由の考え方とEUにおける公衆の情報アクセスの考え方とでは、交錯する部分と異なる部分とが存在する。それぞれの地理的領域または主権の及ぶ範囲における法の伝統の相違が存在しながら、新たな法制度や法理論を相互に参照または模倣するという現代のグローバルかつ混合的な社会環境の下においては、そのようなことが頻繁に発生する。それゆえ、逆から言えば、特定の単一の伝統的な法理論（Dogmatisch）だけで特定の法制度を完全に説明し尽くすことができると考えることは、極めて危険なことであるし、その成功の可能性は皆無に近い。

他方において、EUの法制及びこれに準ずる各国の法制においては、自己と関連する個人データの処理（processing）に関する情報の開示を求める権利が認められており、日本国の個人情報保護法制においても、例えば、個人情報保護法（平成15年法律第57号）の中にそのような条項が存在する（第28条、第32条、第34条参照）。これに対し、米国においては、その判例法上、自己情報管理権のような権利が認められておらず、個別の関連法令の中でプライバシー情報の開示が定められることがある程度である一方、民事訴訟

及び刑事公判においては、連邦証拠規則によって、かなり強力であると同時に秘密保護の手続ももつディスカバリ（証拠開示）の手続が定められており、実体法の側面からだけではなく訴訟手続法及び証拠法の側面からも十分な検討を尽くした上でなければその全体像を正しく理解することができないという意味で、EU とはその法制をかなり異にしている。この分野における日本国の法制は、全体としては、米国の法制よりも EU の法制との親和性がかなり高いと言えるが、仔細に検討すれば、混合的なものであるし、また、律令制度の伝統が日本国の法制の基層に存在しているので、ある単一の法制または法理論のみで説明し尽くすことが本来的に不可能な法制に属する。それゆえ、個人データの処理に関する情報の開示請求に関しては、それぞれの法制の全体構造を常に意識した丁寧な検討が要求されることになる。以上のような問題はあるが、自己と関連する個人データの処理に関する情報へのアクセスの権利またはその制度に関する社会的な関心には極めて高いものがあり、特に、国家機関によるいわゆるサーベイランスとの関係において、盛んに議論されている。例えば、Clive Norris, Paul de Hert, Xavier L'Hoiry & Antonella Galetta (Eds.), *The Unaccountable State of Surveillance: Exercising Access Rights in Europe*, Springer (2017)、Wolf J. Schuenemann & Max-Otto Baumann (Eds.), *Privacy, Data Protection and Cybersecurity in Europe*, Springer (2017)、David Wright & Reinhard Kreissl (Eds.), *Surveillance in Europe*, Routledge (2016) が参考になる。刑事におけるデジタル証拠に関しては、Thomas K. Clancy, *Cyber Crime and Digital Evidence: Materials and Cases*, LexisNexis (2014) が参考になる。

また、（プロッサーの 4 類型における）プライバシーの一部から派生して独自の発展を遂げ、現時点においては、非精神的利益である純粋に商業的利益を目的とする財産権の一種として理解されるに至っている米国におけるパブリシティ権と関連する判例法に関しては、全く別の検討を要する場合がある。これらの点に関しては、佐々木秀智「パブリシティ権とアメリカ合衆国憲法修正第一条」法律論叢 84 巻 2・3 号 331〜364 頁 (2012) が参考になる。他方、財産権としてのパブリシティ権の範疇に属さない純粋に精神的な利益としてのプライバシー情報の商業利用の問題に関しては、財産権としてのパブリシティ権に関する研究が盛んになるにつれ、逆に深い学術研究が乏しくなってしまったという奇妙な社会現象が見られる。その責任の大半は、例えば、特定の分野における法学研究者や実務法律家等の中に少なからず見られるような、視野の狭さ、一般的な不法行為法上の基本原則の勉強不足、そして、他の法分野及び法哲学との関連性に十分に留意する研究姿勢の希薄さにあると考えられる。しかし、このような学術上の傾向は、今後、SNS ベンダやクラウドベンダによる利用者のプライバシー情報の濫用的な商業利用事例との関係において、逆転する可能性が高い。特に、目下審議中の EU の e プライバシー規則案が採択されると、当該研究者の力量に大きく依存するものとはいえ、財産権としてのパブリシティ権に関する議論とは全く別に、著名ではない単なる個人の精神的側面としてのプライバシー情報の第三者による商業利用に関する研究（特に違法行為類型に関する研究）が大幅に進展する可能性があると考えられる（前掲「指令 2002/58/EC の改正案 [参考訳]」参照）。

なお、この問題と関連する法哲学上の一般的な理解を扱うものとしては、Luciano Floridi (Ed.), *The Onlife Manifesto: Being Human in a Hyperconnected Era*, Springer (2014)、Linnet Taylor & Luciano Floridi & Bart van der Sloot (Eds.), *Group Privacy: New Challenges of Data Technologies*, Springer (2017) が参考になる。この問題と関連する不法行為法（Tort Law）上の基本原則に関しては、George C.

Christie, Joseph Sanders & W. Jonathan Cardi, *Cases and Materials on the Law of Torts (Fifth Edition)*, West (2012)、Vincent R. Johnson, *Advanced Tort Law: A Problem Approach*, LexisNexis (2010)、Gert Brueggemeier, Aurelia Colombi Ciacchi & Patrick O'Callaghan (Eds.), *Personality Rights in European Tort Law: The Common Core of European Private Law*, Cambridge University Press (2010)、William Lloyd Prosser, W. Page Keeton, Dan B. Dobbs, Robert E. Keeton & David G. Owen (Eds.), *Prosser and Keeton on Torts (Fifth Edition)*, West (1984) が参考になる。

(50) 佐々木秀智「アメリカ情報自由法の「中核目的」とプライバシー情報開示の判断基準」法律論叢 73 巻 1 号 1～86 頁 (2000)、同「アメリカにおける連邦政府保有情報の電子的公開と個人情報保護」情報ネットワーク・ローレビュー 3 巻 51～67 頁 (2004)、湯淺墾道「自治体の情報公開制度の現状と課題」九州国際大学法学論集 18 巻 3 号 155～187 頁 (2012)、堀部政男「情報公開法・個人情報保護法の提唱と実現」法律時報 75 巻 11 号 60～64 頁 (2003)、森田明『論点解説 情報公開・個人情報保護審査会 答申例』（日本評論社、2016）参照。

(51) 最高裁平成 21 年 12 月 17 日判決・裁判集民事 232 号 649 頁、最高裁平成 21 年 1 月 15 日決定・民集 63 巻 1 号 46 頁、最高裁平成 18 年 7 月 13 日判決・裁判集民事 220 号 749 頁、最高裁平成 13 年 12 月 18 日判決・民集 55 巻 7 号 1603 頁、最高裁判決平成 13 年 5 月 29 日・裁判集民事 202 号 235 頁、最高裁判決平成 13 年 3 月 27 日・民集 55 巻 2 号 530 頁参照。

(52) 基本的な考え方に関しては、Leonor Rossi & Patricia Vinagre e Silva, *Public Access to Documents in the EU*, Hart Publishing (2017) が参考になる。

(53) 夏井高人「欧州議会、理事会及び欧州委員会の文書に対する公衆のアクセスに関する規則 (EC) No 1049/2001 [参考訳]」法と情報雑誌 2 巻 3 号 102～118 頁 (2017) 参照。

(54) 規則 (EC) No 1049/2001 の前文 (4) 参照。

(55) 脚注 43 参照。

(56) 後掲 *European Commission* v *The Bavarian Lager Co. Ltd*. 参照

(57) EDPS による関連資料として、Public access to documents containing personal data after the *Bavarian Lager* ruling（Brussels, 24 March 2011）が公表されている。

(58) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62008CJ0028 [2018 年 10 月 22 日確認]

(59) https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=ecli:ECLI:EU:T:2011:337 [2018 年 10 月 22 日確認]

(60) Bavarian Lager の意図は、英国の居酒屋組合の代表や醸造会社の代表等が問題の会合に出席しており、英国政府に対して何らかの圧力をかけたことを証明したかったのではないかと推測される。その行為が EC（EU）の競争法に違反する強制制限行為となる場合、仮にその行為が英国法の下においては適法行為であるとしても、Bavarian Lager は、別の行政訴訟または民事訴訟を提起し、更に、司法裁判所において、その英国法が EC 条約に違反する無効な法令である旨の意見判決を得ることができるかもしれないと考えたのであろう。本件は、法社会学的な観点からすると、別の考察も可能であるかもしれないし、単純に濫訴の類であるかもしれないが、本質的には競争制限の違法性を実質的な争点とする事案であると同時に、証拠開示（ディスカバリー）の手続と関連する論点を含むものである。そして、そのような観点から考察する場合、規則 (EC) No 1049/2001 の第

8 条 (b) の解釈論としては、法廷における立証の必要性が個人データの開示を求める「正当な事由」を構成するか否かが検討されなければならない（EU の各個人データ保護法令の関連条項参照）。

(61) 訴訟提起時点においては、第一審裁判所（the Court of First Instance）との名称をもっていたが、リスボン条約に基づき、2009 年 12 月 1 日、一般裁判所（the General Court (EGC)）と改称された。控訴審である司法裁判所判決の 2010 年 6 月の時点では改称後の名称となっていたため、控訴審判決の中では原審を「General Court」と表記している。なお、夏井高人「2016 年改正欧州司法裁判所手続規則 [参考訳]」法と情報雑誌 2 巻 9 号 201～282 頁 (2017)、同「2016 年改正欧州司法裁判所規程 [参考訳]」同誌同号 283～303 頁 (2017)、同「2016 年改正一般裁判所手続規則 [参考訳]」同誌同号 368～449 頁参照。

(62) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62008CC0028 [2018 年 10 月 23 日確認]

(63) https://edps.europa.eu/sites/edp/files/publication/09-06-16_pleading_c-28-08p_en.pdf [2018 年 10 月 23 日確認]

(64) 形式論理の側面だけではなく、第 1 審裁判所である一般裁判所が情報アクセスの権利（情報の自由）を重視する価値判断を基礎としているのに対し、控訴審である司法裁判所が個人データ（プライバシー）の保護を理由に、情報アクセスの権利（情報の自由）に対して冷たい態度を採っている基本的なメカニズムの側面においても研究の余地がある。加えて、この事件のような事案の場合、司法裁判所規程及び司法裁判所規則の解釈上、控訴審の審理において口頭弁論を開くことを要するか否かに関しても若干の検討の余地がある。

(65) 規則 (EC) No 45/2001 第 8 条は、EU（EC）の機関及び組織以外の者に対する個人データの移転のための要件を定めている。この事件の第 1 審原告である Bavarian Lager は、欧州委員会に対して会合参加者の氏名を含む議事録全部の開示を求めているので、その議事録の開示は、個人データの移転を含む文書の開示に該当する。そして、Bavarian Lager は、EU の機関または組織ではなく、民間の事業者であり、かつ、EC（EU）の構成国である英国の事業者として個人データ指令 95/46/EC を実装する英国の国内法の適用を受けるので、同規則第 8 条が適用される。なお、EU（EC）の組織及び機関の間における個人データの移転の場合には、同規則第 7 条が適用される。個人データ指令 95/46/EC の適用のない第三国または国際機関に対する個人データの移転の場合には、同規則の第 9 条が適用される。

(66) Franziska Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice: Towards Harmonised Data Protection Principles for Information Exchange at EU-level*, Springer (2012), pp.167-169 参照。

(67) 前掲「欧州データ空間通知 COM(2018) 232 final [参考訳]」119 頁参照。同通知は、「EU の欧州委員会は、欧州産業のデジタル化の取り組みの一部として、就中、Horizon 2020 計画に基づき、産業データプラットフォーム及び革新的なハブに対する資金支援を与えることにより、産業界を支援するための行動を既に執った。これらの仕事の継続として、2018 年～2020 年、Horizon 2020 に基づく（特に「産業データのプラットフォーム及び個人データのプラットフォーム」の）調査研究及び技術革新の措置は、信頼性があり、安全なプラットフォームの開発、並びに、（データ保護立法のような）関連立法の遵守を容易にしつつ、専有的な産業データ及び明らかな個人データの安全な共有のためのプライバシーに留意した分析手法の開発を促進する」ものであるとも述べている。

(68) 夏井高人「指令 2003/98/EC [参考訳]」法と情報雑誌 2 巻 9 号 48～59 頁 (2017)、同「指令

2013/37/EU [参考訳] 」法と情報雑誌 2 巻 9 号 60～76 頁 (2017)、同「指令 2013/37/EU による一部改正後の指令 2003/98/EC [参考訳] 」法と情報雑誌 2 巻 9 号 77～83 頁 (2017) 参照。

(69) ここで「財産権（the right to property）」として示されている権利は、主として、営業秘密のような知的財産権及びそれが不正に開示された場合にはインサイダー取引となり得る公開前の取引情報のよう機微の情報を含め、重要な企業情報と関連する商業的な権利のことを指すと解される。前者の営業秘密に関しては、夏井高人「営業秘密指令 (EU) 2016/943 [参考訳]」法と情報雑誌 2 巻 9 号 489～514 頁 (2017) 参照。後者の重要な企業情報には、知的財産権（特に営業秘密）として保護されない情報が含まれるが、営業秘密として保護されない情報であっても、日本国の法制の下においては、例えば、不法行為訴訟では、正当に保護されるべき法的利益に該当することがあり得るし、また、その情報が無権限で第三者に開示された場合、刑事上では、（商法・会社法・証券取引法上の罰則の適用があり得るほか）刑法に定める業務妨害罪を構成することがあり得る。

(70) ここでいう「商業上の秘密」とは、主として、営業秘密のことを指すと解される。

(71) 前述の指令 2003/98/EC の再改正提案（COM(2018) 234 final）の前文 (32) 及び前文 (33) 参照。これは、GDPR の第 6 条第 4 条 (e) と関連するものである。GDPR の第 6 条は、個人データの処理の適法性という要件を定めるものであるが、例外の要件に該当するものとしてデータ主体の同意に基づかないで個人データが処理される場合において考慮に入れられるべき安全性確保措置（safeguards）の例として、「暗号化または仮名化を含めることができる」と述べている。これは、比例性の原則に基づいて考慮されるべきものであり、当該個人データの法的保護の要否、保護の性質及びその程度の相違に対応して適正な保護手段・方法が適用されなければならない。

(72) ここで「潜在的」という表現を用いているのは、個人識別の目的で処理対象とされるのでなければ個人データにはならないということも意味する。例えば、個人データを収録した紙の冊子である名簿が名簿として使用されるときはその名簿に含まれる情報は、個人情報または個人データとなる。例えば、その名簿を利用してダイレクトメールを発送し、商業宣伝広告メールを送信する行為は、二次利用としての個人データの処理に該当し得る。これに対し、その冊子を物理的に溶解してパルプ原料の一部として再利用する処理の場合は、その名簿に含まれる情報の破毀または破壊の処理が自動的に含まれるとしても、その処理それ自体としては、個人データの処理ではない。ただし、名簿の破毀または破壊について、当該個人データのデータ主体の何らかの権利が残存している場合、当該名簿の破毀または破壊によってその権利の行使が不可能な状態となるので、別の問題が発生し得る。後者の場合において、一般に、法定の個人データ保存期間を経過した後に当該個人データを破棄することは、単に法定の義務を履行する行為に該当するのに過ぎず、原則として、破棄の時点で当該データ主体の同意を得る必要性もないので、当該データ主体の何らかの権利の侵害となることはない。なお、私人が不要となった書籍や雑誌等を廃棄する行為は、純粋に私的な行為として GDPR の適用対象外の行為となる。その廃棄について、環境保護の目的のための法定のリサイクル義務がある場合（日本国の法令としては、廃棄物の処理及び清掃に関する法律（昭和 45 年法律第 137 号）第 4 条の 2 参照）、当該書籍や雑誌の内容を探査することなく機械的に物理的な破壊や再利用加工が実行されるのであれば、公共の利益に基づく処理として例外処理に該当し得る。しかし、リサイクル業者が当該書籍や雑誌を転売して利益を得る目的のために、その書籍や雑誌の内容の全部または一部をデータベース化する行為は、個人データの処理に該当

し得る。本来は法定のリサイクル処理のために設置されたゴミの収集場所から価値のある書籍や雑誌だけを選抜して持ち去る行為は、個人データと関連する法令上の問題を発生させることに加え、窃盗罪に該当し得る（窃盗罪の成否に関しては、最高裁平成 19 年 12 月 18 日決定・裁判集刑事 294 号 869 頁、垣見隆禎「世田谷区清掃・リサイクル条例事件」自治総研 411 号 58～78 頁 (2013) 参照）。

(73) あるデータ主体を識別するために参照される「要素」である「情報」が「データ主体に関する情報」に含まれないという論理は成立し得ない。

(74) 既に滅びた文明社会において識別子として使用されていたと推定される絵文字等が遺物として残存していたとしても、その識別子の論理的な体系、文法、処理態様等に関する情報が消滅してしまっているときは、当該遺物は、単なる遺物であり、識別子ではない。換言すると、識別子であるという属性も固定的な定性ではなく、何らかの処理との社会的関係性の中でのみ成立する属性である。このことは、現時点において未解読の古代文字でも同じである。ただし、未来のある時点において当該古代文字の解読に成功すれば、その時点以降においては、個人識別性を回復し、個人データの一種として評価されるようになることがあり得る。これは、了解可能性という社会的関係性の中で成立する現象であり、当該文字それ自体の問題ではない。全ての記号論理学も同じである。そのことは、特定の記号論理学上の理論を説明するための符号は、どのようなものにも置き換えることが可能であることによっても自己説明的に証明される。これらのことは、常識に属する。

(75) この点において、GDPR の中には、ある種の論理的な破綻または自己矛盾が内包されている。

(76) 人工知能技術の応用が発展しつつある現代社会においては、データ処理の「目的」は、人間の精神作用の発現として設定された主観的意図という意味での「目的」に限定されず、それが社会的機能として個人識別を論理的な要素として含むものである限り、システムによって自律的・自動的に生成されたもの（自動生成された処理行程等）も含まれると解すべきである。ここにおいてもまた、「意思主義」を捨て「処理主義」に移行すべき必然性が存在する。

(77) Paul Voigt & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, Springer (2017) の 180～182 頁の脚注の中で示されている文献及び判例参照。

(78) Vicenç *Torra, Data Privacy: Foundations, New Developments and the Big Data Challenge*, Springer (2017)、Brent Daniel Mittelstadt & Luciano Floridi (Eds.), *The Ethics of Biomedical Big Data*, Springer (2016)、Serge Gutwirth, Ronald Leenes & Paul De Hert (Eds.), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*, Springer (2016)、Els J. Kindt, *Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis*, Springer (2013)、Jean Paul Isson, *Unstructured Data Analytics: How to Improve Customer Acquisition, Customer Retention, and Fraud Detection and Prevention*, Wiley (2018)、Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Crown (2016) 参照。なお、脚注 49 の中で示した文献も参照。

(79) 行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）の附則（平成 27 年法律第 65 号）の第 12 条は、政府が「行政機関の保有する個人情報の保護に関する法律第 2 条第 1 項に規定する行政機関が保有する同条第 2 項

に規定する個人情報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）第2条第1項に規定する独立行政法人等が保有する同条第2項に規定する個人情報（以下この条において「行政機関等保有個人情報」と総称する。）の取扱いに関する規制の在り方について、匿名加工情報（新個人情報保護法第2条第9項に規定する匿名加工情報をいい、行政機関等匿名加工情報（行政機関等保有個人情報を加工して得られる匿名加工情報をいう。以下この項において同じ。）を含む。）の円滑かつ迅速な利用を促進する観点から、行政機関等匿名加工情報の取扱いに対する指導、助言等を統一的かつ横断的に個人情報保護委員会に行わせることを含めて検討を加え、その結果に基づいて所要の措置を講ずるものとする」と定めている。また、個人情報保護法第2条第9項は、「匿名加工情報」について、「当該個人情報に含まれる記述等の一部を削除すること」または「当該個人情報に含まれる個人識別符号の全部を削除すること」により、「特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であって、当該個人情報を復元することができないようにしたものをいう」と定め、行政機関個人情報保護法第2条第8項は、「非識別加工情報」に関し、同様に定めている。しかし、この程度の措置であれば、現代の最先端のプロファイル技術を用いて容易に個人識別可能な個人データに復元可能または再構成可能なことは自明または常識の部類に属するので、これらの条項は、ほぼ無意味な条項である。それゆえ、これらの条項を遵守しただけでは、個人識別性のない情報としてビジネスの道具とすることは、極めて危険である。当該データがいかなる手段・方法によっても個人識別不可能であることを自動的に論証することを可能とするような手法が検討されなければならない。しかし、一般に、ある符合列が社会生活の中で識別子としての効用を発揮するか否かは、その符号列それ自体とは直接的には無関係な社会的文脈の問題であり、符号列それ自体によって全て解決することなど最初から不可能な問題に属する。個人識別の問題それ自体が符号それ自体の問題ではなく社会的文脈の問題である限り、それは基本的に無理なことである。それゆえ、今後の検討課題としては、問題のレイヤを適切に区分した上で、データの個人識別性の有無を重視せず（特に、量子コンピュータが普及するとほぼ全ての暗号が無意味化することが確実であるので、暗号理論等の関連数学理論も重視せず）、個々のデータの濫用の有無（社会的実害の有無）を重視した法理論及び法制の確立が望まれる。

(80) 一般に、個人データのマネジメントは、技術的側面だけに限定されることがない。EUの個人データ保護法令は、基本的に、組織的な措置と技術的な措置を求めており、かつ、個人データの管理に失敗したときは、かなり強力な制裁措置が加えられる仕組みとなっている。これを理論的に分析すると、技術的な措置は、事前の予防においては効果的なものであるかもしれないが、時間を過去に遡ることなどできない以上、個人データの管理の失敗が現実に発生してしまったときは、当該技術的措置が当該インシデントに関しては「無力であった」という事実を自ら証明する効果しかもたない。それゆえ、技術的措置のみを過信するマネジメントは、愚劣なものでしかない。組織的な措置も、それが予防措置である限り、原則として、技術的措置と同じような性質または特徴をもつ。法的制裁は、基本的には事後的な報復措置ではあるが、報復による個別の特別予防効果及び一般予防効果をもち得るという点で技術的措置とはかなり異なるものである。それゆえ、EUの個人データ保護法令は、違反行為に対する制裁が抑止力をもつものでなければならない旨を定めている。管理者や処理者以外の第三者に対する報復としての処罰及び法執行は、原則として、罪刑法定主義に則り、明確な刑罰法令及び刑事手続法令に従って実行される。そして、これらを全体に適切に運用するためには、合理的かつ機能的なマネジ

メント組織の構築が不可欠である。

(81) 夏井高人「データベース保護指令 96/9/EC [参考訳・改訂版]」法と情報雑誌 2 巻 12 号 73～92 頁参照。

(82) 公益社団法人著作権情報センター（CRIC）の訳による。

(83) 日本国の著作権法は、第 2 条第 1 項第 10 号の 3 において、「データベース」について、「論文、数値、図形その他の情報の集合物であって、それらの情報を電子計算機を用いて検索することができるように体系的に構成したものをいう」と定義し、第 12 条第 1 項において「編集著作物」について、「編集物（データベースに該当するものを除く。以下同じ。）でその素材の選択又は配列によって創作性を有するものは、著作物として保護する」と定義している。

(84) 委員会スタッフ作業文書 SWD(2018) 146 final24～25 頁、85～86 頁参照。同作業文書の 3 頁及び脚注 6 においては、限定的な解釈を示す欧州司法裁判所の判例法として、*Fixtures Marketing Ltd v. Oy Veikkaus Ab* (C-46/02, 9/11/2004), *Fixtures Marketing Ltd v. Svenska Spel Ab* (C-338/02, 9/11/2004) *British Horseracing Board Ltd v. William Hill* (C-203/02, 9/11/2004) *Fixtures Marketing Ltd* v. *OPAP* (C-444/02, 9/11/2004) を挙げている。

(85) 脚注 42 参照。

(86) 2020 年 4 月 1 日から施行される改正民法（債権法）の第 548 条の 2 は、第 1 項において、定型約款の定義を定めた上で、第 2 項において、「前項の規定にかかわらず、同項の条項のうち、相手方の権利を制限し、又は相手方の義務を加重する条項であって、その定型取引の態様及びその実情並びに取引上の社会通念に照らして第 1 条第 2 項に規定する基本原則に反して相手方の利益を一方的に害すると認められるものについては、合意をしなかったものとみなす」と定めている。

(87) データベースの利用に伴う個人データの第三国移転が十分性の判定によるのではなく標準約款に基づいて行われる場合に関しては、GDPR 第 46 条第 2 項参照。

(88) 夏井高人「オンラインコンテント可搬性規則 (EU) 2017/1128 [参考訳]」法と情報雑誌 3 巻 6 号 114～132 頁参照。

(89) 脚注 7 参照。

(90) 脚注 7 参照。

(91) 脚注 22 参照。

(92) 規則案（COM(2017) 495 final）の条項中には個人データ保護法令との適用の優先順序それ自体を明示に示す条項が存在しないが、同規則案の第 2 条第 1 項が「欧州連合内における個人データ以外の電子データ」に適用されると規定しおり、また、第 3 条第 1 号が同規則案における「データ」について、「規則 (EU) 2016/679 の第 4 条 (1) に示す個人データ以外のデータを意味」すると定義していることから、その反対解釈として、個人データと関連する処理には同規則案の中に定める条項が適用されないと解することになる。同規則案の前文の中で示されているのは、その法解釈である。

(93) ここで中間介在行為に触れているのは、前述（2.1.3）の GDPR 第 2 条第 4 項による電子商取引指令 2000/31/EC の中間介在プロバイダ免責条項との調整と関係するものであると考えられる。

(94) このことは、当該データそれ自体の固定的な定性として識別性の有無を問うことができないということとパラレルな問題である。

(95) 日本国においては、本来的には、個人情報保護委員会がそのような職責を担うべきもの

であると解される。

(96) 同様の困難性は、テロリズム及び組織犯罪対策においてもみられる。なお、脚注39参照。

(97) 第5条第1項第2文は、監督機関からアクセスを求められたデータ管理者の受忍義務を定めるものである。しかし、この条項の反対解釈により、データ管理者は、当該データがEU域外に存在していること、または、EU域外で処理されていることを根拠として、アクセスを拒否できることになる。問題は、クラウド上に存在しているように見えるデータへアクセスするための端末装置がEU域内に存在している場合、または、当該クラウドのミラーサーバがEU域内に物理的に所在している場合、第5条第1項第2文が適用され、アクセス拒否が可能となるか否かである。私見としては、クラウドに関しては、個々の要素を分断して考えるのではなく、システム全体を包括的に理解して法解釈に反映させるべきであると考える。それは、クラウドベンダが、そのような実体としての所在と仮想的な所在とが不明瞭なシステムとして意識的かつ積極的に構築し、そのシステムによって国境を越えてサービスを提供し、そのサービスの提供から利益を得ているからという経済的・社会的な要素を重視した利益衡量に基づく。これらの根拠の中の「実体としての所在と仮想的な所在とが不明瞭なシステムとして意識的かつ積極的に構築」という部分は、法理論または判例法上の規範としての「禁反言の法理」の応用的な部分を含む。

(98) クラウドコンピューティングと関連する法律問題全般を扱うものとして、一般財団法人ソフトウェア情報センター編『クラウドビジネスと法』（第一法規、2012）及び岡村久道編『クラウド・コンピューティングの法律』（民事法研究会、2012）、Georg Borges & Jan Geert Meents (Hrsg.), *Cloud Computing: Rechtshandbuch*, C.H. Beck (2015) がある。

(99) 藤原靜雄監修・新保史生編『JIS Q 15001:2017 個人情報保護マネジメントシステム要求事項の解説』（日本規格協会、2018）参照。

(100) European Cloud Initiative(2018/C 252/26)(OJ C 252, 18.7.2018, p.258-272)、Communication: European Cloud Initiative - Building a competitive data and knowledge economy in Europe (COM(2016) 178 final)、European Parliament resolution of 10 December 2013 on unleashing the potential of cloud computing in Europe（OJ C 468, 15.12.2016, p.19-29）、Communication: Unleashing the Potential of Cloud Computing in Europe (COM(2012) 529 final) 参照。なお、脚注8参照。

(101) 夏井高人「製造物責任に関する理事会指令 85/374/EEC [参考訳]」法と情報雑誌2巻10号278～291頁(2017)、同「製造物責任指令報告書 COM(2018) 246 final [参考訳]」同誌3巻9号269～280頁(2018)参照。

(102) 本論文は、文部科学省私立大学戦略的研究基盤形成支援事業（平成23年～平成27年度）及び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。