

# 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

メタデータ	言語: jpn 出版者: 明治大学法律研究所 公開日: 2017-12-01 キーワード (Ja): キーワード (En): 作成者: 夏井, 高人 メールアドレス: 所属:
URL	<a href="http://hdl.handle.net/10291/19113">http://hdl.handle.net/10291/19113</a>

【論 説】

# 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

夏 井 高 人

## 目 次

### 1 はじめに

### 2 検討

#### 2. 1 Personal data

- (1) 「個人データ」の概念
- (2) 「要素」の概念
- (3) 「識別可能な個人」の概念
- (4) 「処理」による適用対象の限定
- (5) 小括

#### 2. 2 Free movement (or free flow) of such data

- (1) 「data」の意義
- (2) 「such」の意義
- (3) 「個人データの保護」と「free movement of such data」との関係
- (4) 小括

#### 2. 4 Consent

- (1) 定義
- (2) 同意を正当事由とする処理
- (3) 小括

#### 2. 5 Safeguards

- (1) 多重構造
- (2) 用例
- (3) 小括

#### 2. 6 Consistency

- (1) 公共の利益の保護における一貫性確保の要求
- (2) 監督の関与における一貫性
- (3) 例外措置の適用における一貫性
- (4) 権利の制限における一貫性
- (5) 小括

### 3 まとめ

## 1 はじめに

日本国においては、平成 29 年（2017 年）5 月 30 日、個人情報保護法（平成 15 年法律第 57 号・最終改正平成 28 年法律第 51 号）が全面施行される。個人情報保護法は、最初の施行の時から 10 年以上を経て、同法に用いられている基本概念について論ずるべき点はほとんど存在しないと考えられているかもしれない。また、政府の審議会や個人情報保護委員会を含め、政府関係機関でもそのような取扱いが行われているように思われる。細かな事項を定める実施細則も整備されてきた。

しかし、一般論として、そのような政府関連機関等における過去の検討が、仮に基本的に誤った理解や認識を前提とするものであった場合、既決のものとして扱われている事項が実は未決であると考えべき場合、あるいは、立法及びその施行に錯誤的な要素があるものとして、将来の判決において無効の判断が示されること、または、本来あるべき解釈に基づいて政府関係機関等の見解が強制的に修正されるようなことが絶対に生じないとは断定できない。

このような観点から欧州連合（EU）における個人データ保護法制及びその基本的な構成要素について検討を加えてみると、日本国の憲法学、行政法学または個人情報保護法学の領域における代表的な見解の中には、EU における個人データ保護法制で用いられている基本概念を基準として判断すると、到底維持できないものがあるという事実、または、同一の用語によって表示され得る法概念であっても、米国や EU における当該法概念について当該地域における法制度上の公式解釈を提供することのできる最上位の裁判所の判例法が示す意味内容や当該条文それ自体（定義条項を含む。）をつぶさに検討してみると、その合理的な解釈から得られるものとは全く異なるものが含まれていることがあるという事実を認識・理解することができる<sup>(1)</sup>。

そして、一般論としては、この分野における学術上の見解に何か問題が存在するにも拘らず、そのような見解が日本国の政府関連機関等における公式見解の基礎となっているような場合には、上述のような国政上の深刻な問題が発生する原因の 1 つとなり得る。

とりわけ、EU 法の分野においては、実定法上で現実に用いられている法概念の意味内容及び機能・作用に関する理解の齟齬が伏在しているとすれば、今後の日本

国政府と EU との間の国際協定等の締結及びその法的効果にも深刻な悪影響を及ぼす危険性がある。そのため、この点に関しては、十分に留意しなければならない。例えば、欧州委員会（**the Commission**）との間の十分性の判定（**adequacy decision**）という重要な政策課題が存在することを念頭に置くと、個人データ保護と関連する法的課題に関しては、EU と日本国政府との間で、特定の概念の外形的な表現形式（符号）だけでなく、その概念内容の理解に関しても、可能な限り、一貫性ないし整合性を確保するための努力が尽くされなければならない。

そして、そのことはまた、個人情報保護委員会を含め、透明性（**transparency**）の原則ないし説明責任（**accountability**）の原則に基づく日本国政府機関の国民に対する公的な義務を果たす上でも重要なことである。

本稿は、上述のような問題意識を基礎とした上で、これまで行ってきた海外の個人データ保護及びプライバシー保護と関連する法制、とりわけ、近年における EU の法制の変化に着目し、主として、2016年4月27日に可決された欧州議会及び理事会の一般データ保護規則（EU）2016/679（以下「GDPR」という。）<sup>(2)</sup>を主要な素材としながら、比較法学及び法情報学の観点から、特に丁寧に検討してきた法律用語の中から（本稿の原稿の字数制限を考慮に入れた上で）本稿の文脈において重要と思われるものを選択し、そして、この分野における他の研究者の参考の用に供するという目的により、現時点における私見を披露し、広く世間からの批判を仰がんとするものである。

後述するように、個人データ保護と関連する EU の法制は大きく変動し続けており、本稿で示す私見が固定的または確定的なものとして維持可能なものであるとは全く考えていない。今後、同じ問題意識を堅持しつつ、その検討を継続し、更に深め、その後の検討結果を世に問うこともあるかもしれない。しかし、EU の法制が常に流動的であるがゆえに、そして、まさにそうであるからこそ、ある1つの時点における検討結果を記録として残す必要性はむしろ高いと考えられる。そうでなければ、EU の法制に関しては、いかなる研究者も、いつまでたっても、その研究成果を公表することが困難または不可能になってしまうことであろう。それゆえ、研究の対象である法現象それ自体が流動的なものであり、変化し得るものであるということを大前提とし、そのことを十分に意識した上で、現時点における研究成果の一部を公表することにする。

本稿においては、1つのテーマに基づいて構成された論文としての体裁をあえて放棄し、故石前禎幸氏の追悼の趣旨も兼ねるといふ趣旨から、同氏と関係の深い中村雄二郎氏（明治大学法学部名誉教授）の『術語集—気になることば』（岩波新書、1984）において採用されているスタイルをやや模したオムニバスのスタイルを応用して採用することにした。故石前禎幸氏が好んで研究対象としたトマス・ホブズ（Thomas Hobbes）の法思想ないし社会思想は、本稿の最も基底にある法哲学とも共通する要素を含むものである<sup>(3)</sup>。

これに対し、本稿においては、価値相対主義を基底としつつも、事実を踏まえた有意義な見解を何ひとつ示していないのも同然の John Rawls の著書には依拠しない。また、適用対象が限定されるという難があり、かつ、世間における安易な濫用の弊またはその危惧があるため、Lawrence Lessig の CODE 理論にも依拠しない。

本稿においては、ある法概念が変動しない質量をもつ物体のような固定的な意味内容をもつものではなく、ある概念を示す用語が社会の中でどのように機能するかという観点からの考察を重視した<sup>(4)</sup>。そして、そのような機能を果たすために行われる思考作用の中で、特に「Taking into account the interests of others」という意味での利益衡量の存在とその機能に着眼した。

一般に、利益衡量は、複数の相互に矛盾する利益が明確に主張されている場合に、それらの利益の優先劣後関係を検討・決定するような場合に用いられることの多い概念である。しかし、実は、個々の解釈者による個々の法律用語の解釈もまた、それ自体として、利益衡量の作用の一種である。

一般に、ある法律用語を示す語それ自体としてのデータは、単なる符号列に過ぎない<sup>(5)</sup>。そして、その符号列を「文字である」と認識して読み、理解し、用いようとする者の主観的な評価または判断によって、常にアドホックなものとして、その語のもつ意味がその語という容器の中に注入される。

それだけで済む場合には特に問題はない。しかし、同一の符号列に対して複数の異なる者が関連づけようとする意味内容は、大概の場合、若干なりとも異なるものであり、完全に一致することはあり得ない。より正確に言えば、その一致または不一致を測定するための方法は存在しない。その意味で、人間と人間との間における「完全な情報交換」は、常に不可能である（または、完全な情報交換が成立したことを証明するための手段が存在しない）。そして、そのような場面において混乱が

発生し得る。

また、一般に、法律用語は、ある社会的機能を果たすための道具（tool）の一種に過ぎない。その道具は、自己の判断やそれに基づく行為を正当化するために用いられることがしばしばある。その場合、その場面において保護法益となっているのは、それぞれの主観における一方的な保護法益の要求または欲求として自己認識される情念（passion）である。しかし、そのような法的利益の認識を合理的に行おうとすれば（換言すると、反作用としての不利益の発生を極小化または最適化しようとするれば）、それと矛盾する他の利益との利益衡量を自分の脳内で行い、他の法規範や法的利益の保護との矛盾が生じないような合理的な範囲内で自己が主張しようとする法的利益を再定義しようとするようになるであろう。

この過程で生成される正当化事由（justification or ground）もまた、それ自体として、自己の保護法益の優先性について法的な保護・承認を受けるための道具（tool）の一種である。その意味で、実体という意味での「正義（justice）」も存在しない。存在するのは、道具（tool）としての符号列である「正義」を用いた利益主張及びその調整原理だけである。それは、国家機関の権力の行使によって統御されることもあるし、実力によってのみ統御されることもある。前者の場合の中で、裁判官によって当該事案における「正義」が判断され、その判断に基づいてのみ国家権力が行使される場合（正確には、国家権力としての実力の行使が正当なものとして扱われる社会関係が存在している場合）、一般に、それを「法の支配（rule of law）」と呼ぶ例が多い<sup>(6)</sup>。

以上のような理解は、ジェレミー・ベンサム（Jeremy Bentham）の考え方やリアリズム法学等に基づく場合を除き、現在の一般的な法哲学の領域において普通に採用されているものとはやや異なるものであるかもしれない。しかし、学術としての法哲学が一切存在しないような社会状態を想定したとしても、事実の問題として、何らかの国家制度または社会組織が存在する限り、必然的に、単なる儀式や礼拝のようなものを含め、当該国家または社会における権力機能の行使のための正当化の理屈が考え出されることになるであろう。そのことを銘記しなければならない<sup>(7)</sup>。

更に、目下の法的利益だけを法的に保護することによって、自己にも帰属している別の利益が損なわれるリスクが生ずるときには、とりわけ、関連する複数の法的利益について、綿密な損得勘定・利害打算が即座に行われることになる<sup>(8)</sup>。その

意味で、判断者が当事者 1 名だけの場合であっても、単なる素朴な欲望の発露とその充足の場合を除き、程度と質の差こそあれ、何らかの意味での利益衡量は存在し、そのような意味での利益衡量の結果として、各人各様の主観的な再定義が成立し、それが正当性の根拠として主張されることになる。

その利益に関する主張がなされる場面において、表意者は、その主張内容を示すための道具 (tool) として、その道具である一定の符号列が法概念を意味するものとして相手方に受け取られることを期待する。その表意者は、そのようなものとして、その符号列を外に向かって表出する。通常、会話や通信その他の方法による意思内容の他者に対する伝達のプロセスにおいて理解されている用語 (term) とは、そのような意味における符号列のことを指す。それは、相手方にとって認識・理解される前の段階においては、書店の書棚に陳列されているだけで誰もその内容を知らない書籍と全く同様、物理現象としては単なる符号列の集合に過ぎない。人間が社会的動物として行動せざるを得ない範囲内では、このようなプロセスを避けて通ることはできない。

他方、裁判官の判断もまた主観の作用の一種に過ぎないことは明らかである。しかし、当事者の主観である判断とは異なり、裁判官の主観である判断結果は、当該管轄権のある範囲内での具体的な訴訟事件においては、国家権力によって強制され得る。この点が、当事者の単なる判断やその主張とは全く異なる。そして、裁判官は、その主観である判断を形成する過程で、当事者が保護法益として主張する利益を比較検討し、更に、他の訴訟事件に適用した場合に齟齬が生じないかどうか、自己の別の判断との矛盾をきたすことにならないかどうか等々の理論上の損得勘定・利害打算に基づく計算を自分の脳内で行う。その裁判官は、そのようにしながら、当事者の主張で用いられている定義の当否を計算処理し、そして、自己の判断のために必要となる語の再定義という思考プロセスを実行することになる<sup>(9)</sup>。すなわち、利益衡量である。

本稿では、以上のような意味での利益衡量または思考上の損得勘定・利害打算の実質的部分を慎重に考慮した上で、本稿でとりあげた幾つかの法律用語を素材として、若干の検討を試みた。少なくとも、EU の個人データ保護法制を理解するための法解釈学という文脈の上では、以上のような意味での利益衡量という思考プロセスを発動させ、自己の脳内におけるそのプロセスの機序を想像させる可能性のない

ような説明（学説）の類は、学術上の道具（tool）としての有用性をもたない。

本稿における検討の法哲学的な基礎は、権利や権力なるものの本質に関するいわゆる実体説ではなく、いわゆる関係説を基底とするものである<sup>(10)</sup>。それゆえ、実体説的な考察プロセスしか実行できない者にはまるで理解できない部分が多々あるかもしれないし、また、実体説を是とする者には到底受け入れ難い部分を多々含むものかもしれない。

しかしながら、本稿でとりあげた幾つかの法概念を理解する上で、実体説的なアプローチだけに頼ることは、明らかに危険である。仮にそれが危険ではない場合であっても、裁判規範というものを理解するために行われる思考作用の基礎として用いる上では、法学上の有用性がない<sup>(11)</sup>。

法論理学もまた同じであり、ある論理が国家権力によって強制される機序を考慮に入れるものでない限り、単なる論理学の一種に過ぎず、少なくとも法学の一種ではない。法は強制（執行）され得るものでなければ社会的に意味をもたないものである。その社会的メカニズムを理解した上で、その正当化のための道具（tool）の一種として、法における論理というものそれ自体をとらえなおすべき必要性がある。

本稿は、EUの個人データ保護と関連する全ての法令に対する完全に網羅的な調査を前提とするものではない。Eur-lexを含め、EUの公式の情報源から得た資料に基づいて調査検討した上で、翻訳すべきであると判断したものについては、法と情報雑誌<sup>(12)</sup>に掲載して公表してきた。しかし、EU法に属する法規範の中には、これまで調査・検討した法令以外に、基本的な法規範である制定法だけでも個人データ保護と関連する法令がかなり多数存在する。加えて、EUにおける主要な法源の1つである欧州司法裁判所（Cour de justice des Communautés européennes）及び欧州人権裁判所（Cour européenne des droits de l'homme）の判例法がある。これらのEUの関連法令及び判例法に対する調査・検討・訳出は、今後の重要な課題としてそのまま維持される。そして、その将来の調査・検討・訳出の結果は、今後も、法と情報雑誌の中で公表されることになるであろう。

他方、日本国の法令及び諸外国の法令を含め、全ての法令について、法律論叢誌編集委員会に対する本論文原稿提出期限である2017年4月12日までの時点における状態を前提としている。それゆえ、新規の立法または法案の提出、既に提出されていた法案の可決、修正または撤回、判決（欧州司法裁判所の先決裁定を含む）

または判例法による法令の法的効力の全部または一部の無効化等を含め、2017年4月12日以降の時点における法情報と関連する事情の変更は、仮にそれが本論文の内容に影響を与え得るものであるとしても、本論文の内容には反映されない。

なお、これまで、明治大学法と情報科目担当教員会議の研究会等の機会において、または、電子メールの交換によって、佐々木秀智氏（明治大学法学部教授）及び丸橋透氏（明治大学法科大学院講師・ニューヨーク州弁護士・ニフティ株式会社法務部長）との間で非常に有意義な意見交換を行ってきた。本稿を執筆するに際し、これらの意見交換から示唆を受けた事柄が少なくない。

## 2 検討

### 2.1 Personal data

#### (1) 「個人データ」の概念

1981年1月28日に署名のために開放され、1985年10月1日に発効した欧州評議会の個人データの自動的な処理と関連する個人の保護に関する条約 ETS No.108（以下、「個人データ保護条約」という。）の第2条は、「個人データ」について、「識別される個人または識別可能な個人（以下「データ主体」という。）に関連する情報を意味する」と定義している。

個人データ保護条約の説明書（Explanatory Report）の中には、「個人」の意味についての解説はないが、説明書の第28項は、「識別可能な個人（identifiable person）」の意義について、「容易に識別することのできる個人を意味する。非常に複雑な方法による個人の識別には適用されない」と説明している。ここでいう個人は、自然人（natural person）のことを指し、法人（legal person）を含めないとの趣旨と解される<sup>(13)</sup>。いずれにしても、この個人データ保護条約における「個人データ」の概念を出発点として、その後のEUの関連法令が構成されてきたと考えてはば間違いないであろう<sup>(14)</sup>。

例えば、EUの構成国に適用される1995年の個人データ保護指令95/46/EC<sup>(15)</sup>の第2条の(a)は、「個人データ」とは、「識別される自然人または識別可能な自然

人（以下「データ主体」という。）に関する全ての情報を意味する。識別可能な者とは、とりわけ、識別番号を参照することによって、または、彼の肉体的、生理的、精神的、経済的、文化的または社会的な同一性を示す1もしく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を意味する」と定義している。ここでは、同指令の条項が、自然人である個人に対してのみ適用されることが個人データの定義条項の中に盛り込まれ、そして、明確化されている。

EU (EC) の機関及び組織に直接に適用される規則 No 45/2001<sup>(16)</sup> の第2条(a) は、個人データ保護指令 95/46/EC と全く同じ定義条項を定めている。その改正提案<sup>(17)</sup> の第3条第1項(a) は、「管理者 (controller)」の定義を除き、「規則 (EU) 2016/679 にある定義」と定めているから<sup>(18)</sup>、GDPR の第4条(1) がそのまま適用されることになる。

GDPR の第4条(1) は、「個人データ」について、「識別される自然人または識別可能な自然人（以下「データ主体」という。）に関する全ての情報を意味する。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以上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。

この条項の第1文は、関連法令の定義条項における文言と全く同じであるが、識別可能な個人を識別するための要素中にある「識別子 (identifier)」の例示として、「氏名、識別番号、位置データ、オンライン識別子」が明示されている点には特に留意すべきである。識別子は、従来から識別可能な個人を識別するための要素の1つとして掲げられてきたものであり、一般的には、個人番号 (国民番号) のような個人識別番号がその代表的なものとして理解されてきた。しかし、ここに「氏名、識別番号、位置データ、オンライン識別子」が掲げられている以上、識別番号以外の要素も識別子として理解されるべき場合があることになる<sup>(19)</sup>。

位置データが識別子として掲げられているのは、現時点における位置データの取得が特定のスマートフォンの識別番号と関連付けられた上で当該スマートフォンの位置情報を取得する場合に用いられていること、捜査官による GPS 機能のある装置を用いた追跡の場合には当該個人が既に識別されており、その識別された個人

の氏名の別名 (**alias or synonym**) として当該位置データが用いられるためである。その結果、位置データに関しては、例外規定の適用がある場合を除き、関連するデータ保護の規則が適用されることになる<sup>(20)</sup>。

なお、オンライン識別子<sup>(21)</sup>との関連では、指令 2002/58/EC の改正規則案<sup>(22)</sup>において、特に電子通信サービスのエンドユーザの端末装置と関係する識別について、より詳細な定義と法的保護が提案されている<sup>(23)</sup>。

構成国の職務権限を有する機関 (**competent authorities**) すなわち構成国の法執行機関 (警察) 及び法務当局 (検察) に対して適用される指令 (EU) 2016/680<sup>(24)</sup> の第 3 条 (1) に定める「個人データ」の定義は、GDPR の第 4 条 (1) に定めるところと同じである。

Europol 規則 (EU) 2016/794<sup>(25)</sup> の第 2 条 (h) は、「個人データ」について、「データ主体に関する情報を意味する」と定義した上で、同条 (i) は、「データ主体」について、「識別される自然人または識別可能な自然人を意味し、識別可能な者とは、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、当該の者の肉体的、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 もしく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を意味する」と定義しているから、この定義は、GDPR の第 4 条 (1) に定める「個人データ」の定義と実質的に均等のものである。

以上から、EU の個人データ保護法制においては、警察機関を含む EU 及び構成国の全ての公的部門並びに民間部門を通じて、GDPR の第 4 条 (1) に定めるところと全く同一の「個人データ」の定義条項が適用されることになる<sup>(26)</sup>。

## (2) 「要素」の概念

上述の定義条項それ自体から理解できることは、「個人データ」とは、「要素 (**one or more factors**)」である情報のことを指すこと<sup>(27)</sup>、その要素である情報の種類・属性に限定はないこと<sup>(28)</sup>、そして、そのような要素の中の 1 個または複数個の要素を用いることによって、個人を識別するという処理を実行することができることだけが必須の要件となっているということである。

また、「全ての情報 (**any information**)」<sup>(29)</sup> について、その情報の種類・属性に限定はないので、これらの要素の中には、例えば、氏名、住所、性、生年月日

が含まれる。それゆえ、これらの要素は、いずれも個人データの一種である<sup>(30)</sup>。

例えば、住所について言えば、ある特定の住所によって示される特定の地理的場所に1人の者（自然人）しか居住していないこと（付加的なデータまたは情報）が明らかになっている場合には、その付加的なデータまたは情報と組み合わせることによって、当該住所という要素（情報）が特定の個人の識別子（identifier）として機能することがあり得る<sup>(31)</sup>。また、ごく例外的な場合ではあるが、例えば、刑事訴訟法の所定の手続に基づく逮捕または勾留により特定の個人を強制的に居住させている拘置施設等の拘置場所番号<sup>(32)</sup>は、当該の者が物理的に所在している空間を示す番号であるという付加的なデータまたは情報と組み合わせることによって当該個人の識別子となり得る<sup>(33)</sup>。

一般に、住民基本台帳法（昭和42年法律第81号）の第4条に基づいて登録されている住所は、公開のものということができるので、その意味で、法的保護の程度及び手法が他のものと異なり得るが、そのことによって、当該住民基本台帳データベースに登録されている特定の個人の住所のデータがその個人データ性（個人情報性）を喪失することにはならない<sup>(34)</sup>。

### **(3) 「識別可能な個人」の概念**

他方、「識別可能な個人」は、理論的には、あくまでも計算処理の出力として期待されている仮想的な個人である。実在するとは限らない。例えば、生年のデータだけが存在し、死亡のデータが存在しない個人については、現実には既に死亡していたとしても、生存する個人としての識別がなされる。それゆえ、当該個人の実在性の有無とは無関係に、個人の識別のために利用可能な要素は、カテゴリ（範疇）の問題としては、常に「個人データ」に含まれる。

一般に、当該要素が、世俗の世界において、およそ「個人データ」または「個人情報」の範疇に含まれるとは認識・理解されていないような要素であるとしても、それをを用いて現実に存在する個人を識別処理することが可能である限り、その要素は、個人データの処理の枠組みのために用いられる要素の中に含められる<sup>(35)</sup>。

要は、個人データであるそれぞれの要素（情報）のそれ自体としての性質、社会の中で営み得る機能、人間による判断の際に営み得る機能、当該特定の文脈において組み合わせられる他の要素（情報）との関係から生み出される相乗効果等を個別に評価した上で、その特定の文脈におけるそれぞれの要素（情報）の法的保護の程

度、または、その手法の相違及びその法的根拠を明確に認識・理解することが重要である<sup>(36)</sup>。

#### (4) 「処理」による適用対象の限定

個人データである要素としての情報は、もともと社会の中に散在しているのが原則である<sup>(37)</sup>。ただ、「それが特定の目的のために収集され、電子計算機によって自動的に処理され得るような状態となったときは、その処理の結果として、特定の個人のプライバシーの利益が損なわれるリスクが高まる」という蓋然性<sup>(38)</sup>が一般に肯定されていることから、当該処理を行う者に対し、当該個人データを管理する者としての安全配慮義務の一種として、当該要素である個人データの処理における様々な法的義務が定められるという論理構造及びそれに基づく法制度が存在しているだけである。

GDPRをはじめ、EUの個人データ保護法令は、上記のような意味における個人データ（識別要素である全ての情報）の全部に適用されるわけではなく、主として、個人データが管理者または処理者によって処理されること、そのような場合には、定型的にデータ主体のプライバシーの利益を害する蓋然性が高いと考えられることに着目し、その場合における管理者及び処理者の義務を定め、それを全ての構成国において均等なものとして適用することを目指している。

この「処理（processing）」の意義について、例えば、GDPRの第4条(2)は、「それが自動的な手段によって行われるか否かを問わず、収集、記録、編集、構成、記録保存、修正もしくは変更、検索、参照、使用、移転による開示、配布その他利用可能なものとする、整理もしくは結合、制限、消去または破壊のような、個人データもしくは一群の個人データについて実施される全ての業務または一群の業務のことを意味する」と定めている。「自動的な手段によって行われるか否かを問わず（whether or not by automated means）」とまとめてしまっていることとの関連で、例えば、ビッグデータ（big data）による非定型の大量のデータを用いた解析処理の場合を含め、当該情報が構成されてデータベース処理可能な状態になっているか否かを問わず、とにかく何でもかんでも処理可能であるような時代状況（関連技術の発展）の変化を認識・理解すべきである<sup>(39)</sup>。

ただし、GDPRの第2条第1項は、「その全部または一部が自動的な手段による個人データの処理に対し、並びに、自動的な手段以外の方法による個人データの処

理であって、それをファイリングシステム（**filing system**）<sup>(40)</sup>の一部を構成するものとし、または、ファイリングシステムの一部として構成することが予定されているものに適用される」と定めている。

そのことから、個人データそれ自体の定義を定める条項と **GDPR** の適用範囲を定める条項とを明確に分けて規定することによって、処理の対象にならないデータ（情報）であっても、**GDPR** の第 4 条 (1) に該当する限り、それは常に個人データであるという趣旨を明らかにしている。そのことはまた、「処理の対象となっているデータ（情報）だけが個人データである」というような限定手法を完全に排除する趣旨のものと理解することができる。

### (5) 小括

その要素（情報）を用いることによって、特定の個人を識別処理することが可能である限り、その要素（情報）は、管理者または処理者による処理の下にあるか否かを問わず、「個人データ（日本国法では「個人情報」）」である<sup>(41)</sup>。

処理されない個人データについては、原則として、**GDPR** をはじめとする **EU** の個人データ保護法令が適用されることはない<sup>(42)</sup>。

個人データに対して **GDPR** 等の個人データ保護法令が適用される否かの識別基準は、事物及び土地に関する管轄権等の一般要件を充足することを前提とした上で、当該情報が管理者（**controller**）または処理者（**processor**）によって処理されるか否かにより決定される（図 1）。

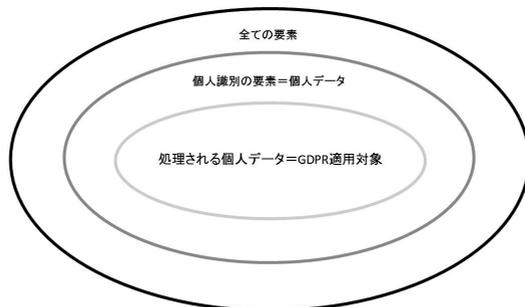


図 1：要素と法適用の関係

## 2. 2 Free movement (or free flow) of such data

「free movement of such data」または「free flow of such data」は、「such data」が単純に「personal data」を示すという理解（法解釈）を前提した上で、「個人データの自由な移転」または「自由な移動」と訳するのが通例である。例えば、堀部政男研究室訳の個人データ保護指令（95/46/EC）の仮訳では、「個人データの自由な移動」と訳されている。私も、従前の参考訳等では、慣例に従い、「個人データの自由な移転」と訳した。

他方で、「such data」との文言が他の条項とは関連しない独立のものであり、単純に「personal data」を言い換えただけのものであるという認識の下で、「個人情報」の自由な移転が他の条項によっては何らの制約も受けない独立した保護法益であると理解し、そのような理解を前提とした上で、「個人データの保護」という保護法益と「個人データの自由な移転」という保護法益とのバランスを単純に比較検討するという観点から立論する論考が多数みられる。また、「個人情報の自由な移転」が独立の保護法益であるとの理解を前提とした上で、例えば、いわゆる名簿業にみられるように、「個人情報」は、本来、自由に売り買いできるものである」との誤解のようなものが蔓延していることも事実である。

しかし、何らの制約も受けない無条件の「個人データの自由な移転」は、あり得ない。

### (1) 「data」の意義

「data」は、全ての個人データを指すことがない。個々の法令の適用対象となる個人データは、それぞれの法令によって異なるように限定されている。

例えば、GDPR の第 2 条第 2 項の (d) は、「公共安全への脅威に対する安全の確保及びその脅威の抑止を含め、職務権限を有する行政機関によって犯罪行為の防止、捜査、探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」には GDPR が適用されない旨を定めており、そのような場合には、GDPR ではなく指令 (EU) 2016/680 が適用される。また、同条第 3 項は、「欧州連合の機関、組織、事務局及び官庁による個人データの処理に関しては、規則 (EC) No 45/2001 が適用される」と定めている。

前述の規則 (EC) No 45/2001 の改正提案は、まさにこの欧州連合の機関及び組

織等に適用される場合の法令を GDPR の双子のようにして、ほぼ同一の法規範の下で、かつ、ほぼ類似の制度によって運用されるものに改正しようとするものである。

これら GDPR の第 2 条 (d) 及び同条第 3 項により、GDPR の「such data」が全ての個人データを指すものではないということが明らかである。しかも、GDPR は、当該個人データを適法に開示 (disclosure) し、または、他の構成国または第三国もしくは国際機関に対して移転 (movement of flow) することのできるための厳格な要件を定めているから、その要件を充足しない個人データは「such data」から当然に除外される。

これに対応して、指令 (EU) 2016/680 の適用対象となる個人データの範囲も限定される。同指令の第 2 条第 1 項は、「この指令は、第 1 条第 1 項に定める目的のための職務権限を有する機関による個人データの処理に適用される」と規定し、同指令の第 1 条第 1 項は、職務権限の目的として「公共の安全に対する脅威への防護及び防止を含め、犯罪行為の防止、捜査、検知もしくは訴追または刑罰の執行のため」と規定している。すなわち、指令 (EU) 2016/680 の適用は、構成国の法執行機関（警察）及び法務当局（検察）が処理する個人データに限定される。

指令 (EU) 2016/680 の正式名称の中には、「free movement of such data」が含まれているが、その「such data」は、構成国の法執行機関（警察）及び法務当局（検察）が処理する個人データに限定される。そして、同指令の第 1 条第 2 項 (b) は、「その交換が欧州連合の法律または構成国の法律によって求められる場合、欧州連合内での職務権限を有する機関の間での個人データの交換が個人データの処理と関連する自然人の保護に関する理由によって制限されることがなく、かつ、禁止されることもないことを確保する」と定めている。そのことから、同指令における「free movement」とは、ある構成国の法執行機関（警察）または法務当局（検察）と別の構成国の法執行機関または法務当局との間における情報交換のことを指すものとして限定され、そのような情報交換に関するものだけを意味する。ここでは、明らかに、「free movement of such data」が一般用語である熟語として成立する余地はない。

それゆえ、全ての種類の個人データを含むような意味での「free movement」または「free flow」は、あり得ない。

## (2) 「such」の意義

「such」は、当該法令におけるそのような厳重な限定のある個人データのみを指すもので、およそ個人データ一般を指すものとは考えられない。

より丁寧に言い換えると、「such」は、単純に「personal data」の言い換えとなっているのではなく、当該法令において、当該法令の適用対象である個人データ（personal data）に限定した上で、かつ、当該個人データを適法に開示（disclosure）し、または、他の構成国または第三国もしくは国際機関に対して移転（movement of flow）することのできるための全ての法律要件を充足しているということを絶対条件として、そのように要件を充足する個人データの移転のみを指すものとして用いられている。「such」にはそのような重要な意味があるのである。

このことから、直ちに、「free movement of such data」または「free flow of such data」だけを切り離して、独立の保護法益を示すものと解することが誤りであることを知ることができる。

## (3) 「個人データの保護」と「free movement of such data」との関係

そのように解釈すべきことについては、例えば、前述の規則（EC）No 45/2001の改正提案中でも明記されている。

同改正提案の前文(3)は、「欧州議会及び理事会の規則（EU）2016/679及び欧州議会及び理事会の指令（EU）2016/680は、2016年4月27日に採択された。規則が、個人データの処理と関連する自然人を保護し、かつ、欧州連合内における個人データの free movement を確保するための一般的な規則を定める一方、指令は、刑事に関する司法共助及び捜査共助の分野において、個人データの処理と関連する自然人を保護し、かつ、欧州連合内における個人データの free movement を確保するための特別規則を定めている」と述べている。

ここで前文(3)がGDPR（規則）の趣旨について述べている部分だけに着目すれば、「規則が、個人データの処理と関連する自然人を保護し、かつ、欧州連合内における個人データの free movement を確保するための一般的な規則を定める」とある以上、全ての個人データについて述べているかのように理解してしまうかもしれない。

しかし、前述のとおり、それぞれの法令が適用される個人データの範囲は、それぞれの法令において限定されているのであり、全ての種類の個人データを指す

ものとして「free movement」に言及することはあり得ない。このGDPRの前文(3)で言及する個人データもGDPRの第2条等によって限定された範囲内にある個人データのみである。そのようにして限定されたものであることを示す趣旨で「such」が用いられていると考えるのが妥当である。

同様のことは、GDPRにおける「free movement」を直接に規定する条項についても言うことができる。

GDPRの第1条第3項は、「The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data」と規定している。この条項だけを独立のものとして読んだ場合、「個人データの移転には個人データ保護の法令による制限はない」と解釈することは全く不可能というわけではない。そのような理解を前提にすると、「個人データの移転は常に自由である」という理解も成立し得ることになる。そのように解するとすれば、「GDPRが適用されることもない」ということになる。

しかし、GDPRの第1条第2項は、「This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data」と規定しているのである。すなわち、GDPRは、個人データの保護の権利（欧州連合基本権憲章第8条）の権利を保護するためにある。

もし同条の第2項と第3項とをそれぞれ独立した他の条項とは無関係に機能する規範であると理解するとすれば、ただそのことだけで、GDPRは、空中分解を起こしてしまうことになるであろう。

このような同一の条の中にある第2項と第3項の外見上の矛盾は、実は矛盾したものではないということが同条の第1項に示されている。すなわち、同条の第1項は、「This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data」と規定している。要するに、同条の第2項と第3項は、論理的な破綻が生ずることなく両立し得る場合にのみ、規範としての効力を有する。そして、その両立のための諸々の法律要件が第5条以下に縷々述べられているのである。

それゆえ、GDPRの特定の条項を解釈する場合には、当該条項だけを切り離し

て独立に解釈することが許されず、GDPRの全条文を頭に入れた上で、全ての条項が論理的な矛盾を起こすことなく成立し得る範囲内で合理的な解釈をしなければならない。

このことについて、GDPRの前文(10)は、「一貫性があり高いレベルでの自然人の保護を確保し、かつ、欧州連合内における個人データの支障のない移転の障碍を除去するためには、個人データの処理と関連する自然人の権利及び自由の保護のレベルを全ての構成国において均等のものとしなければならない。個人データの処理と関連する自然人の基本的な権利及び自由の保護のための法令の一貫性があり均質な適用を、欧州連合全域において確保しなければならない」と述べている。

すなわち、GDPRの第2条第3項における「for reasons connected with the protection of natural persons with regard to the processing of personal data」とは、構成国によって異なる内容の個人データ保護法令が国内法で定められており、それが法的な障壁ようになって個人データの移転の妨げとなることを認めないという趣旨に解するのが合理的であり、そのために不可欠な法令の内容の統一のためにGDPRが制定されたと理解するのが正しい<sup>(43)</sup>。

従って、GDPRの第1条第3項によっても、全く独立して、完全に無条件で、個人データの「自由な移転」が認められる余地は全くない。

これらの法令は、これらの法令が直接に適用される範囲内で、個々の構成国の国内法による独自の規制が設定されることを禁止し、そのような法制の相違が障壁のようになって、とりわけ、シェンゲン情報システムⅡ (Schengen II)<sup>(44)</sup>の利用、Visa情報システム (VIS)<sup>(45)</sup>におけるVisaの自動的な処理や域内市場情報システム<sup>(46)</sup>における前述のeID (eAT)システムのような電子的な識別子の利用が阻害されることを阻止し、または、Europol及びEurojustによる構成国間での捜査情報の共有(特に重大犯罪及びテロリスト犯罪に関する情報の共有)が妨げられないようにするというに最大の意味がある<sup>(47)</sup>。

これらの法的・経済的・社会的な利益は、あくまでもEU及びその構成国の利益なのであって、天賦人權または人類普遍の権利のようなものとは趣旨を相当に異にするものであると理解するのが妥当である。そして、それらの目的のために、当該利益と関連する規則や指令及びそれに基づいて制定される各構成国の国内法が適用され、その適用の範囲内において、それぞれの分野における個別的な個人データ

の（各構成国の国内法制上の相違による法的な障壁がないという意味で）支障のない移転が実現されるのである。

#### (4) 小括

GDPR、規則 (EC) No 45/2001 及び指令 (EU) 2016/680 を含め、EU の個人データ保護法令においては、それぞれの法令の制定目的に従い、それぞれの法令の適用対象とする個人データの範疇を異なるものとして定め、それによって、その法令が適用される個人データの種類を限定している。それらの法令において個別に定める一貫性のある法的義務を遵守することを絶対条件としてのみ、その移転が認められる。全く無条件での「自由な移転」は、理論上も実際上も法的には認められない。

EU の個人データ保護法令は、各構成国における法制の相違によって個人データの移転が妨げられるという問題を解決するための法的手段の 1 つなのであって、いわゆる「利活用」の場合を含め、個人データの無制約な移転や取引を独立した保護法益として認めるものではない。私生活（家庭）の中での小規模で個人的な情報の利用を含め、EU のいかなる法令によっても個人データの処理に法的規制のない場面を除き、個人データの移転は、デフォルトでは、自由ではない<sup>(48)</sup>。

それゆえ、「free movement of such data」または「free flow of such data」は、「個人データの自由な移転」ではなく、「そのデータの支障のない移転」と訳されるべきである。

以上の検討結果を踏まえ、これまで公表してきた参考訳の中で、慣例に従って「free movement」または「free flow」を「自由な移転」と訳した部分は、以後、全て「支障のない移転」と修正し、また、「free movement of such data」または「free flow of such data」は、「そのデータの支障のない移転」と修正する。

## 2. 4 Consent

### (1) 定義

GDPR の第 4 条(11) は、データ主体の「同意」について、「任意に与えられ、特定され、事前に説明を受けた上での、不明瞭ではない、データ主体の意思の表示を意味し、それによって、彼もしくは彼女が、その言辞または明確に肯定的な行動により、彼もしくは彼女に関連する個人データの処理の同意を表明するものを意味す

る」と定義している。この条項は、定義条項なのであるが、データ主体の意思の表示がGDPRの適用のある「同意」となるためには、手続的な要件として、「事前の説明を受けた上で」表示であること、かつ、形式的要件として、「不明瞭ではない」表示であること、かつ、実体的な要件として、「彼もしくは彼女に関連する個人データの処理の同意」を内容とするものであること、以上全ての要件の充足を求める条項でもある。

ところで、一般に、「consent」と類似する語は多数ある。例えば、「agreement」や「permission」がある。一般的な用例は別として、EUの個人データ保護法令の中では、「agreement」は、構成国間または構成国と外国もしくは国際機関との間の国際合意の一種である「協定」を示すことが多い。また、「permission」は、例えば、著作権者からその著作物の利用について「許諾」を与えるような場合に用いられることが多い。

また、「consent」は、「同意」または「承諾」と訳されるのが通例である。単なる同意ではなく、事前に説明を受け、その説明を理解した上で、任意に与えられる同意、すなわち、「インフォームドコンセント (informed consent)」に限定する意図で、意図的に、「consent」を「承諾」と訳す例もかなり多数存在する。そのような意図が明確である場合には、日本語の文章の中において、「承諾」と記すのが妥当であろう。

しかし、一般的な同意も「consent」であるという理解を前提にした上で、GDPRの適用との関係においては、前記第4条(11)に定める特別の要件を全部満たす同意のみがGDPRの適用を受ける「consent」であるとの論理構造を採用しているように見える。

つまり、GDPRには、広義の「consent」と狭義の「consent」とが共存しており、ただ、GDPRの適用による法的効果を得ることができるのは、狭義の「consent」だけであるという論理構造が存在するのである。

## (2) 同意を正当事由とする処理

GDPRの第7条は、GDPRの適用を受け、その効果を生じさせる「consent」を処理の正当事由とするための要件について、以下のように定めている。

1. 処理が同意に基づく場合、管理者は、データ主体が彼または彼女の個人

データの処理に同意しているということを説明できるようにする。

2. データ主体の同意が他の事項とも関係する書面上の宣言の中で与えられている場合には、その同意の要求は、他の事項と明らかに区別できる方法によって、理解しやすくかつ容易にアクセスし得る方式で、明瞭かつ平易な文言を用いて、表示される。この規則の違反行為を構成するそのような書面上の宣言は、いかなる部分についても拘束力がない。
3. データ主体は、彼または彼女の同意を、いつでも、撤回する権利をもつ。同意の撤回は、その撤回前の同意に基づく処理の適法性に影響を与えない。データ主体は、同意を与える前に、そのことについて情報提供を受ける。同意の撤回は、同意を与えるのと同じように、容易にできるものとする。
4. 同意が任意に与えられたか否かを判定する場合には、就中、役務の提供を含め、契約の履行が、当該契約の履行にとって必要のない個人データの処理に対する同意を条件とするものであるか否かについて、最大限に考慮に入れる。

この第7条の論理構造は、以下のとおりである。この場合の一般的な法律要件は、選択的なものではなく、その全てが充足されなければならない。特別の場合（書面上の宣言<sup>(49)</sup>による同意の場合）の法律要件は、当該要件が想定している場合に該当する場合（書面による宣言が求められる場合）においてのみ適用される。

（法律効果）

データ主体の同意をもって、個人データの処理の適法化事由<sup>(50)</sup>とすることができる。

（一般的な法律要件）

データ主体は、同意をする前に、同意をするために必要な情報の提供を受ける。

データ主体は、いつでも、容易に同意を撤回できる。

（特別の法律要件）

複数の事項についての同意を求める書面によって同意が行われる場合には、何についての同意を求めているのかを容易に識別可能なものとするために、他の事項と明らかに区別できる方法によって、理解しやすくかつ

容易にアクセスし得る方式で、明瞭かつ平易な文言を用いて、同意の対象を識別するために必要な事項を表示する。

この第 7 条の論理構造を理解しようとする場合、所定の要件を満たさない「consent」が存在することを前提にしなければ、上記の法律効果を発生させる「consent」の要件を定めることができないという自明の理を理解することができる。

### (3) 小括

GDPR の第 4 条 (11) 及び第 7 条の各条項は、所定の要件を満たさない「consent」について、別の語を用いて区別しようとしていない。

要するに、GDPR おいては、所定の要件を満たす狭義の「consent」と所定の要件を満たさない「consent」が存在する。そして、そのいずれかを判断する必要がある場合において、第 7 条第 4 項の判断基準が適用される場合があり得る。このような論理構造を採用していることを理解することができる<sup>(51)</sup>。

これらのことは、EU の他の個人データ保護法令においても、基本的には同じである。

以上のような理解を前提としつつ、ただ、法律学の専門家及び法解釈の専門家としては、原文を逐一あたって、正しい文脈理解に基づいてその法律要件及び法律効果を考えるべき職業上の義務があるとの考え方を踏まえ、EU の個人データ保護法令の参考訳においては、あえて、「承諾」として区別することなく、「consent」を「同意」と訳すことにしている。

## 2. 5 Safeguards

一般に、英語の「safeguard」は、名詞の場合と動詞の場合がある<sup>(52)</sup>。動詞の場合、その対象が保護法益である場合には直訳的に「安全を確保する」もしくは「安全性を確保する」と訳し、または、「protect」の言い換えとして「保護する」と訳すことが多い。これに対し、情報セキュリティ、国防、治安維持、警察活動等の関係では、同様に直訳的に「安全を確保する」もしくは「安全性を確保する」と訳し、または、「protect」の言い換えとして「防護する」もしくは「防衛する」と訳す例が多い。

## (1) 多重構造

「safeguards」は、それが名詞である場合、日本国の個人情報保護法令にみられる「安全確保の措置」（行政機関個人情報保護法第6条）または「安全管理措置」（個人情報保護法第20条）と同じ訳語またはそれに類似する訳語を用いて訳す例が多々みられる。

しかし、EUの個人データ保護法令は、法令それ自体が、全体として個人データないしプライバシーという保護法益を保護するための手段的・国家制度的・統治技術的な「safeguards」になっており、更に、その全体としての「safeguards」の中で、手段的・技術的・人工的な措置として、組織的な「safeguards」、技術的な「safeguards」及び法的な「safeguards」を定めるという「入れ子構造」になっている。そのことから、当該法令という集合の中に含まれる部分集合に過ぎないものを示すとしか理解しようのない「安全確保の措置」または「安全管理措置」という日本語だけで全ての場合の「safeguards」を表現することは、EUの法制の構造（structure）を見誤る危険性がある。

そのような日本国法令における意義との混同の危険を避けるため、意図的に別の訳語をあてて識別可能にすべきである。そのために、「safeguards」について、「安全性確保措置」という訳語を用いる。

以上の前提で、GDPRに定める安全性確保措置を検討すると、様々な態様のものが含まれていることに気づくことができる。それは、何らかの電子的・技術的な手段だけを指すものではない。とりわけ、法令等の中で、人間の心理に対して訴えかけることによって機能する守秘義務が安全性確保措置として定められている場合、あるいは、拘束的企業準則や約款の中で、当該拘束的企業準則等に服する者の一定の行動に関する義務が安全性確保措置として定められている場合がそうである。

## (2) 用例

GDPRの条項の中から重要と思われるものを探すと以下のような条項を見つけることができる。ただし、網羅的ではない。

（抽象的な条項）

GDPRの第9条第1項の特別類型の個人データ（special categories of personal data）すなわち機微のデータ（sensitive data）の処理禁止の

原則の例外の1つとして、同項の(b)は、労働保障法及び社会保障法の分野において<sup>(53)</sup>、「データ主体の基本的な権利及び利益のための適切な **safeguards** を定める構成国の法律による団体協約により認められていること」を条件として、特別類型の個人データの処理を認めている。ここでいう安全性確保措置の具体的な内容は、構成国の国内立法に基づく団体協約（労働協約等）<sup>(54)</sup>に委任されているので、第9条第1項の(b)の条項内では特定されていない<sup>(55)</sup>。

GDPR の同条同項の(d)は、「政治、哲学、宗教または労働組合の目的による財団、団体その他の非営利組織による適切な **safeguards** を具備する適法な活動の過程」においてその構成員等の個人データを処理する場合についても定めている。この「**safeguards**」もそれぞれの団体の中で定められるものなので、第9条第1項の(d)の条項内では特定されない。

GDPR の同条同項の(h)は、予防医学もしくは産業医学の目的のために、労働者の業務遂行能力の評価、医療上の診断、医療もしくは社会福祉または治療の提供、または、医療もしくは社会福祉の制度及びその役務提供の管理のための処理の場合において、それを適法化するための要件として、欧州連合の法律、構成国の法律、医療専門家との契約及び第3項に示す要件と並んで「安全性確保措置 (**safeguards**)」を定めている。「第3項に示す要件」とは、守秘義務のことを指す。それゆえ、法令、契約及びGDPR 第9条第3項の守秘義務以外のものであることまでは特定できるが、それ以上には特定することができない。合理的に解釈すれば、暗号化または仮名化のような技術的措置を指すのではないかと推測される。

GDPR の第10条は、有罪判決及び犯罪または保護措置と関連する個人データの処理について、法務当局の管理に基づく場合、または、「データ主体の権利及び自由のための適切な安全性確保措置」を定める欧州連合法または構成国の法律によってその処理が認められる場合に限り、適法となると定めている。安全性確保措置の内容は、欧州連合の法律または構成国の法律に委ねられているので、その内容を特定することができない。なお、ここでいう欧州連合の法律の中には、指令(EU) 2016/680、Europol 規則(EU) 2016/794、による決定 2009/426/JHA による改正後

の Eurojust 決定 2002/187/JHA 等が含まれると考えられる。

（例示のある条項）

GDPR の第 6 条第 4 項の (e) は、本人の同意のない場合において、当初の目的とは異なる目的のために処理が適法に行われるために、管理者が特に考慮に入れるべき (the controller shall...take into account, inter alia) 事項の 1 つとして、「適切な安全性確保措置 (safeguards) があること。それは、暗号化または仮名化 (encryption or pseudonymisation) を含むことができる」と規定している。この例示から、ここでいう安全性確保措置とは、データを物理的に保護するための技術的な手段の実装のことを指すと解される。

GDPR の第 25 条第 1 項は、バイデザイン及びバイデフォルトの原則により、処理開始前に実装すべき措置として、「データのミニマム化といったようなデータ保護の基本原則を実装するために設計された仮名化や効果的な方法で、その処理の中に必要な安全性確保措置を統合するための適切な技術上及び組織上の措置」を講ずるものと定めている。ここでは、仮名化が例示されていることから、主として技術的措置のことを指すと解されるが、個人データと関連する権利や利益の保護のために必要な措置を全部事前に具備することが求められていることから、技術的措置だけに限定されるものではないと解される。第 25 条第 1 項を当然の前提とするものであることから考えると、第 35 条第 7 項 (d) 及び第 36 条第 3 項 (c) も同様に考えることができる。

（推測可能な条項）

GDPR の第 23 条第 2 項 (d) は、データ主体の制限を定める国内法または管理者 (controller) の措置等の中に盛り込まれるべき事項として、「非違行為または違法なアクセスもしくは違法な移転を防止するための防護措置 (safeguards)」と定め、同様に、同項の (f) は、「記録保存の期間及び処理または処理の種類の性質、範囲及び目的を考慮に入れた上での適用可能な防護措置 (safeguards)」と定めている。文脈から、主として、技術的措置のことを指すと解されるが、それだけではなく、通常の情報セキュリティのための業務遂行の過程で採用・運用される防護措置一般を

含むものと解される。

(特定されている条項)

GDPR の第 46 条第 1 項は、欧州委員会による十分性の判定（第 45 条）が存在しない場合において、安全性確保措置（safeguards）を講じた処理による個人データの第三国または国際機関に対する移転を認めている。第 46 条第 1 項の安全性確保措置の具体的な内容は、同条第 2 項において、以下のように列挙されている。これらは、明らかに、技術的措置ではなく、認証、約款または国際協定等のような、当事者に対して規則の遵守を義務付ける法的根拠となる法律文書等が存在していることをもって、安全性確保措置（safeguards）としているということを理解することができる<sup>(56)</sup>。

- (a) 行政機関または行政組織間の法的拘束力及び執行力のある文書；
- (b) 第 47 条に従う拘束的企業準則；
- (c) 第 93 条第 2 項に示す審議手続に従って欧州委員会によって認められた標準データ保護約款；
- (d) 監督官によって承認され、かつ、第 93 条第 2 項に示す審議手続に従って欧州委員会によって認められた標準データ保護約款；
- (e) データ主体の権利に関するものを含め、第三国の管理者または処理者に対して適切な安全性確保措置を適用するための拘束力があり執行可能な約定を有する第 40 条による承認された行動準則；または、
- (f) データ主体の権利に関するものを含め、第三国の管理者または処理者に対して適切な安全性確保措置を適用するための拘束力があり執行可能な約定を有する第 42 条による承認された認証方法。

GDPR の第 28 条第 1 項は、処理者（processor）が自己の適格性を保証すべき事項の 1 つとして、「技術上及び組織上の安全性確保措置の実装」を掲げている。論理上、標準的な処理者が実装可能なもの、または、その実装を期待することが可能なものに限定されることを考慮に入れば、データ保護のための内部規則を定め、それを実装・運用すること、及び、技術的措置を実装・運用することを示すものと解することができる。

### (3) 小括

以上に述べたことは、GDPR以外のEUの個人データ保護法令全般についても同様に言えることである。

一般に、法令は、単なる文書ではなく、その法令が機能する国家または領域的組織の中で、特定の共通の価値観を基礎とし、その価値観に基づく社会の安全性を確保するための統治のための手段として構築された装置の一種である。

その装置として実際に機能している法規範それ自体が制定法（statutes）を記録する法令または判例（case law）を記録する判決文という物的な文書によって確定され検証可能な状態に置かれることもまた、そのような国家の装置としての法制度の健全性を確保するための安全性確保措置の一種である。

それゆえ、そのような装置としての構築目的、構造、機能及び作用並びにその実装後の実施実例である判例等を十分に検討した上で、そのような検討結果を反映するものとして、適切な訳語を選択するという学術研究上の安全性確保措置（safeguards）が常に講じられなければならない。

本稿の冒頭で述べたように、法令を記述するための語は、それを読む者各自の脳内においてそれぞれ異なるものとして処理される。その処理における一定の傾向性は、社会環境によって異なる。その社会環境はその社会の構成員の時間的変化に伴う更新によって常に変化し続ける。それゆえ、単なる符号列に過ぎない文書は、それが全く同一の符号列であるとしても、個々の歴史的時間及び社会環境によって異なるものとして機能し得る<sup>(57)</sup>。

そのためには、可能な限り網羅的に一次資料（原典）に直接にあたり、関連する個々の法令相互の間の論理的関係を丁寧に検証し、その歴史上の変化や変遷を検証し、その実装後の作用や反作用のようなものを確認・理解すること、そして、そうすることによって、国家の安全性確保装置としての法規範及びその実装・運用のための仕組みを理解するようにしなければならない。

そのような作業は終わることのない作業であるが、それは、情報セキュリティの世界における安全性確保（防護）のための管理策（control）それ自体が常に定期的に見直され、改善され続けるのと全く同じことである。

法解釈学の領域に限らず、一般に、学説というものは、過去における個人の単なる主観的な意見の表明を符号化したものの一種である。その主観的な意見の記述

としての符号列に過ぎないものが特段の必要性・合理性・妥当性がないのに学術の世界において支配的な機能を営むことは、認められない。学問の自由は、尊重されなければならない（日本国憲法第 23 条）。

それゆえ、私見を含め、学術上の特定の見解の合理性・有用性・妥当性を見直しまたは評価（review or evaluation）を常に行い続けることもまた、学術というもののそれ自体の安全性確保措置（safeguards）となっている。

## 2. 6 Consistency

EU の個人データ保護法制は、一貫性（consistency）の確保を求め、そのための仕組みを構築し続ける。

### (1) 公共の利益の保護における一貫性確保の要求

一貫性の確保の要求は、とりわけ、警察、防衛、テロ対策等のための構成国間での関連情報の共有が各構成国の国内法の相違によって妨げられることを防止するための度重なる法改正と法制度の拡充という歴史的過程の中に明確に示されている。

その情報共有の中には、重大犯罪及びテロリズム犯罪への対応という目的から、必然的に、大量の個人データの交換が含まれる。そのような個人データの交換が円滑に行われない場合、EU の安全が脅かされ、社会と市民の安全を守ることができない。

このような国家法益レベルでの保護法益の確保は、例えば、TFEU の Title V の「Area of Freedom, Security and Justice」<sup>(58)</sup>、とりわけ、その Chapter 4 の「Judicial Cooperation in Criminal Matters」及び Chapter 5 の「Police Cooperation」、すなわち、法執行機関（警察）及び法務当局（検察）の国際共助に関する諸々の条項の中に端的に表現されている。

この TFUE の各条項を実装するための EU の政策決定におけるその具体的な現れの 1 つとして、例えば、ストックホルム・プログラム<sup>(59)</sup> の「4.3.1. より効果的な法執行の連携（More effective European law enforcement cooperation）」は、「欧州連合の法執行協力の第 1 の目的は、典型的に国境を越える次元を有する様々な形態の犯罪と闘うことにある。テロリズム及び組織犯罪のみに焦点が当てられるべきではなく、欧州連合の市民の日常生活に深刻な影響をもつ国境を越える広範な犯罪にも焦点が当てられるべきである。Europol は、構成国の法執行機関の間

における情報交換のためのハブとなり、サービス提供者となり、そして、法執行職務のプラットフォームとならなければならない。欧州連合の理事会は、構成国の職務権限を有する機関に対し、適切な事案においては、可能な限り、共同捜査チーム（JIT）という捜査手法を用いることを勧奨している。Europol 及び Eurojust は、国境を越える主要な業務遂行に組織的に参加し、JIT が設置された場合には、その通知を受けるものとしなければならない」と述べている。

このような政策方針に基づき、従前の Europol 関連の法令<sup>(60)</sup>を統合して、Europol 規則 (EU) 2016/794 が制定された。

Europol の統合化された情報システム (SIENA)<sup>(61)</sup>では、構成国の法執行機関（警察）から提供される情報が処理され、各構成国の法執行機関の間で共有される。それらの情報は、Eurojust によって解析され、その解析結果が構成国の法執行機関によって共有される。また、構成国の法務当局（検察）の連携は、Eurojust によって行われる。EU 域外からの航空機による旅客情報は、PNR 指令 (EU) 2016/681<sup>(62)</sup>に基づいて収集され、税関情報は、理事会決定 2009/917/JHA<sup>(63)</sup>に基づき、CIS システムによって収集・処理され、そして、それらの情報は、必要に応じて、所定の安全性確保措置に従い、Europol を介して、各構成国の法執行機関の間で情報共有される<sup>(64)</sup>。

このような情報共有に伴う個人データを適法に行うための法律要件は、GDPR によっては与えられない。前述のとおり、重大犯罪及びテロリスト犯罪を含む犯罪行為の捜査及び起訴と関連する個人データの保護に関しては、GDPR が適用されないからである。この分野における EU の現行の制定法における最上位の法規範は、規則 (EC) No 45/2001 である。

前述の規則 (EC) No 45/2001 改正提案は、規則 (EC) No 45/2001 を GDPR とほぼ同一の内容をもつ法令へと改正し、EU 内における公的部門及び民間部門を通じて一貫性のある個人データの法的保護を確保し、そして、そのような EU 域内における均等な法的保護が存在することを前提として、EU 及び各構成国の法制の相違が情報交換の阻害要因とならないようにすること、すなわち、「支障のない移転 (free movement)」を確保することを目的とするものである。

## (2) 監督の関与における一貫性

規則 (EC) No 45/2001 及びそれを発展させて GDPR とほぼ同一内容のものとする

るための改正提案における基本的な骨格は、欧州データ保護監督官（EDPS）を統一的な監督機関として位置づけ、EDPSを中心として、GDPRにおける統一的な監督機関である欧州データ保護委員会（Board）との連携の中で、EU全域にわたる一貫性のある個人データ保護を図ろうとするものである<sup>(65)</sup>。

Europol及びEurojustは、EUの機関及び組織（institutions and bodies of the European Union）の中に含まれることから、規則（EC）No 45/2001及びその改正提案の枠組みの中で、直接的にEDPSの監督を受ける。

他方、構成国の一般的な行政機関の中で法執行機関及び法務当局等の捜査権限を持つ機関を除く機関の個人データ保護については、GDPRが直接に適用される結果、構成国の独立の監督官（independent supervisory authorities）による監督が行われる。これに対し、構成国の職務権限を有する機関（competent authorities）、すなわち、法執行機関（警察）及び法務当局（検察）に対しては、指令（EU）2016/680が適用され、その個人データ保護に関しては構成国の監督官が職務権限（competence）を有する。これらの構成国の監督官は、欧州データ保護委員会（Board）を介して、その監督業務の一貫性を確保する<sup>(66)</sup>。

分野別の個人データ保護法令も存在するが、電子通信分野において適用される指令2002/58/EC及び前述の改正提案が定める枠組みにおいては、構成国の監督官が個人データ保護について職務権限を有し、基本的にGDPRの枠組み内での1つの分岐的なものとして、その制度設計が図られている<sup>(67)</sup>。

そして、欧州データ保護監督官（EDPS）と欧州データ保護委員会（Board）は、密接に連携して行動することが求められている。ここにおいて、公的部門及び民間部門の一貫性のある個人データ保護を確保するための一貫性のある制度上の仕組みが提供されることになる。

しかし、個人データ保護における一貫性のある法制度とは、データ主体（日本国法では「本人」）がいかなる場面においても均等な態様・方法による法的保護を受けるということを意味しない。データ主体の権利の制限、分野別での保護の程度・保護が同一分野では一貫したものとなっていることをも意味する<sup>(68)</sup>。

### (3) 例外措置の適用における一貫性

例えば、民間部門及び公的部門を問わず、データ主体の同意がある場合には第三国または国際機関に対する個人データの移転をすることができ、また、データ主体

が身体的または法的に同意をすることができない場合において、データ主体または第三者の生存の利益を保護するために必要な場合には、第三国または国際機関に対する個人データの移転をすることができる。

このような規則は、元来、データ主体のプライバシーの利益を保護法益として個人データ保護制度が構築されており、当該データ主体が理解した上で同意する場合には利害調整（利益衡量）をすべき必要性がそもそも存在しない状況になる一方、他方で、データ主体が同意をすることができず、かつ、データ主体の生存の利益を保護するために必要な場面においては、データ主体のプライバシーの利益という保護法益よりもデータ主体の生存の利益という保護法益のほうが明らかに優越していることから、そのような利益衡量が疑問の余地なく成立すると認められるために、その合理性及び比例性が肯定されると言える。

#### (4) 権利の制限における一貫性

制限に関しては、例えば、警察分野においては、データ主体の自己の個人データに対するアクセスの権利は、特別の例外的な事情がある場合を除き、実質的にはほとんどないのも同然であり、権利の行使が認められる場合であっても、せいぜい、監督官から「確認した」との通知を受けることしかできないようになっている。そのようなものとして、一貫性のある制限が加えられる。

例えば、決定 2003/659/JHA 及び決定 2009/426/JHA による改正後の Eurojust 決定 2002/187/JHA の第 19 条第 1 項は、「全ての個人は、本条に定める要件に基づき、Eurojust によって処理される彼に関する個人データへのアクセスをもつ権利を有する」と定めるが、同条第 4 項は、「(a) そのようなアクセスが Eurojust の活動を危険に晒し得る場合；(b) そのようなアクセスが構成国の捜査を危険に晒し得る場合；(c) そのようなアクセスが第三者の権利及び自由を危険に晒し得る場合」には、個人データに対するアクセスは、拒否されると定めている。Eurojust の職務の特殊性を考えると、ほとんど常にこの拒否事由のどれかが成立するとと言えるであろう。

Eurojust における個人データの処理及び保護に関する規則<sup>(69)</sup> の第 20 条は、「全ての個人は、Eurojust 決定の第 19 条に定める要件の下で、Eurojust によって処理される彼または彼女に関する個人データに対するアクセスをもつ権利を有する」と定めるが、第 19 条第 1 項は、「(a) 重大犯罪に対する闘いを強化する際における

**Eurojust** の職務の遂行；または、(b) **Eurojust** が支援している構成国の捜査及び  
 訴追；または、(c) たとえそれが一時的なものであっても、(a) 及び (b) の文に示す  
 場合における公的な権限の行使と関係する監視、調査または規制上の職務；また  
 は、(d) 第三者の権利及び自由」に重大な支障が生じないことが明らかな場合にの  
 み、データ主体の権利の行使を認めるものと定めているから、やはり、実際には、  
 ほとんど常に権利行使が認められないことになると言えるであろう。

**Europol** 規則 (EU) 2016/794 の第 36 条第 1 項は、「全てのデータ主体は、合理的な期間内に、彼または彼女と関連する情報が **Europol** によって処理されているか否かに関する情報を得る権利を有する」と定めるが、同条第 6 項は、「(a) **Europol** がその職務を適正に遂行できるようにするため；(b) 安全及び公共の秩序を防護するため、または、犯罪を防止するため；(c) 構成国の捜査が危険に晒されないことを保証するため；(d) 第三者の権利及び自由を保護するため」に必要となる措置を構成する場合には第 1 項に基づく求めに対する返答における情報の提供を拒否するものと定めているから、**Europol** の職務の特殊性を考えると、ほとんど常にこの拒否事由のどれかが成立すると言えるであろう。

構成国の職務権限を有する機関すなわち法執行機関（警察）及び法務当局（検察）に適用される指令 (EU) 2016/680 の第 14 条は、「第 15 条により、構成国は、データ主体が、管理者から、彼または彼女に関する個人データが処理されているか否かの確認を得る権利、及び、処理されている場合には、その個人データ及び (a) 処理の目的及び法的根拠；(b) 関係する個人データの類型；(c) 個人データが開示された取得者または取得者の類型、とりわけ、第三国または国際機関の取得者；(d) 可能なときは、個人データが記録保存される予定期間、または、それが不可能なときは、その期間を決定するために用いられる基準；(e) 個人データの訂正または削除及びデータ主体と関係する個人データの処理の制限を管理者から得ることを求める権利の存在；(f) 監督官に対して異議を述べる権利及び監督官の連絡先；(g) 処理中の個人データの通知、及び、その入手元に関する利用可能な情報の通知に関してアクセスを得る権利を定める」旨を規定しているが、同指令の第 15 条第 1 項は、「構成国は、(a) 公的なもしくは法律上の照会、調査または手続の支障を避けるため；(b) 犯罪行為の防止、検知、捜査もしくは訴追または刑罰の執行の支障となるものを避けるため；(c) 公共の安全を防護するため；(d) 国家安全保障のため；(e)

他の者の権利及び自由を保護するため、関係する自然人の基本的な権利及び正当な利益を十分に尊重した上で、そのような部分的または完全な制限が、民主主義社会において必要であり、かつ、比例的な措置を構成する範囲内において、かつ、その限りで、データ主体のアクセスの権利の全部または一部を制限する立法措置を採択することができる」と定めており、そのとおりに構成国の法令が制定されることになると思われるが、実際には、第 15 条第 1 項の事由に該当する場合は圧倒的に多いものと思われる。

これらのようなデータ主体のアクセスの権利の制限は、犯罪捜査の特殊性（特に「捜査の密行性の原則」）によるものであり、犯罪捜査のための必要性が社会的に是認される限り、そのような法制になっていることそれ自体の適法性・有効性が欧州司法裁判所または欧州人権裁判所によって問題とされることはないであろう。

また、犯罪捜査の場合に権利の制限が行われることについては、規則 (EC) No 45/2001 にも根拠条項がある。

規則 (EC) No 45/2001 の第 20 条第 1 項は、「(a) 犯罪行為の防止、捜査、探知、発見及び訴追；(b) 通貨、財政及び税に関する事柄を含め、構成国及び欧州共同体の主要な経済上または金融上の利益；(c) データ主体の保護または他の者の権利及び自由の保護；(d) 構成国の安全保障、公共の安全と防護；(e) (a) 及び (b) に示す場合において、単発的なものを含め、行政機関の職務遂行と密接な関係を有する監視、検査または規制の職務」の場合には、EU (EC) の機関または組織が権利の制限をすることができる旨を定めている。

そして、前述の規則 (EC) No 45/2001 の改正提案の第 17 条は、データ主体のアクセスの権利を定めるが、同規則の第 25 条第 1 項は、その制限が基本的な権利及び自由の本質的部分を尊重するものであり、かつ、「(a) 構成国の国家安全保障、公共の安全または国防；(b) 公共の安全に対する脅威に対する防護を含め、犯罪行為の防止、捜査、検知もしくは訴追または刑罰の執行；(c) 欧州連合または構成国の一般的な公共の利益の上記以外の重要な対象、とりわけ、欧州連合または構成国の重要な経済的な利益もしくは財政的な利益、出納、予算及び税務上の事項、公衆衛生及び社会保障；(d) その電子通信ネットワークを含め、欧州連合の機関及び組織の内部的な防護；(e) 司法権の独立の保護及び司法手続の保護；(f) 規制を受ける職種における違背行為の防止、捜査、検知及び訴追；(g) (a) ないし (c) に示す場合に

において、一時的なものを含め、公的な権限の行使と関係する監視、監督及び規制の権能；(h) データ主体の保護、または、それ以外の者の権利及び自由の保護；(i) 民事訴訟の執行確保」を守るために民主主義社会において必要かつ比例的な措置である場合には、欧州連合の法令または欧州連合の機関及び組織の内部規則においてデータ主体の権利の制限を定めることができる旨を規定している。

なお、前述のとおり、**GDPR** は、犯罪捜査に関連する個人データについては、そもそも適用対象外となっているので、上記の **EU** の警察関連の法令と同様の権利制限条項をもたない。

### (5) 小括

**EU** の個人データ保護法制における一貫性とは、単純にいかなる場合でも同じような取扱いを受けるというような意味をもつのではなく、以上のような制限や例外も一貫性をもって適用されるという意味をもつ部分を含むものである。

それゆえ、一貫性の概念を理解する場合においても、特定の法令の特定の条項だけを独立のものとして吟味・検討するのではなく、当該条項が含まれている法令全体を検討して当該条項の位置づけを明確に理解することは無論のこと、それだけではなく、およそ当該条項と何らかの関係のありそうな法令全部について、過去の廃止法令に遡って、可能な限り網羅的に調べるといった研究態度が望まれる。

なお、政治学的な見地及び社会学的な見地から考察を深めれば、一貫性の確保の要求のもつ別の側面も見えてくるかもしれない。そのことは、とりわけ、前述の **TFEU** の **Title V** の条項との関係において見出しやすいかもしれない。

## 3 まとめ

以上、**EU** の個人データ保護法制を研究する上で気になる言葉（語・語句）の幾つかについて、これまで調査・検討してきた結果の要旨の一部を示した。

本稿で選択した語は、「**Personal data**」、「**Consent**」、「**Safeguards**」及び「**Consistency**」の 4 つである。他の語も予定したが、頁数の関係で割愛することにした。

一般に、いずれの語についても、法解釈論上の疑問の余地はないと思われるがちで

ある。しかし、それらの語を丁寧に検討した結果としては、必ずしもそうとは言えないと考える。

これらの語は、EUの個人データ保護法令の中でもキーとなるものばかりである。それゆえ、今後、更に丁寧に、EUの関連法令における用例との比較検討やEUの判例法におけるこれらの語句の理解の解析を含め、徹底した研究が尽くされるべきである。

本稿で触れたEUの個人データ保護のための諸法令の具体的な条文の翻訳（原則として直訳による全訳）は、法と情報雑誌の中で順次公表してきた。能力と研究努力の不足のため誤解に基づく誤訳が含まれているかもしれない。そのことは、本稿において述べたことについても同じである。それらについては、今後、更に関連法令や関連判例を涉猟し、その翻訳と考察を重ねる中でより正確な理解を獲得し、従前の誤りを修正し続けるということによって、その責を果たしたいと考える。

本稿の冒頭でも述べたとおり、絶えず変化し続けるEU法の領域に属する事柄について、その時点において可能な限り正確にとらえるための努力と考察を尽くした上で、ある特定の歴史的時点における肖像写真の断片のようなものを世間に示すことは、当該分野と関連する事項を研究対象とする法学研究者の重要な職務の一部であると考えられる。

研究テーマを温め続けながら、それをまとめて世に問う前に、一緒に酒を飲むこともできなくなってしまった故石前禎幸氏の追悼論文集に相当する法律論叢誌に寄稿すべく、本稿の原稿を起草しつつ、その感をますます強める。

仮にそれが不完全で誤りを含むものであったとしても、本稿が個人データ保護法制の研究の分野において、反面教師的な意味を含め、何らかの寄与となることができるのであれば、望外の喜びである。

以上<sup>(70)</sup>

## 注

- (1) 諸般の事情を考慮し、明示の具体的な指摘は一切避けるが、事実の問題として、少なくとも、現在までの日本国の憲法学及び行政法学の分野においては、EUの個人データ保護と関連する主要な法令を単独で、自ら直接に、かつ、網羅的に翻訳・検討し、その翻訳及び検討結果を学術雑誌等で公表して世間の批判を仰ぎ、自己の認識・理解の健全性の検証を積み重ねるという実証的な研究を重ねてきた研究者は、ただの1人も存在しない。従

来、この分野においては、関連分野における海外の著名な研究者の著作で述べられている学術上の理論を理解し、それを翻案した上で、自己の理論として紹介するというような例がかなり多い。そして、当該見解の基礎となっている学説が当地における実定法によって基礎づけられるものであるか否かを検討するための網羅的な情報調査が単独で行われた形跡を見出すことは、ほとんど不可能である。そのようなものは、学術上の思想の研究ではあり得ても、実定法としての法規範を直接に研究するものではあり得ない。それゆえ、例えば、「\*法の研究」と称しても、実際には、「\*法の權威であると自分が評価している\*氏の見解に関する紹介的研究」であること、または、そこでいう「\*法学」なるものが学説史の比較研究の一種である「『\*法学』学」に過ぎず、「\*法」それ自体の研究ではないことが決して珍しくない。無論、特定の学説を研究対象とする学術は成立し得るし、現に多数存在している。しかし、ある特定の学説を知れば、当該学説が対象とする学問領域に含まれる実定法上の条項について常に正しい解釈が可能であるという法則は、常に成立しない。一般に、学説は、特定の条項を解釈する上で参考とすることのできる判断材料の1つとなり得るものではあるが、当該条項そのものではなく、当該条項について適用可能な見解または評価の一種に過ぎないからである。このことは、判例（裁判例）でも全く同じである。先例としての合理性・有効性・有用性を喪失した判例は、判例変更によって後発的に無効化される。

他方、一般に、裁判官の世界では、当該事件において適用される法規範それ自体を直接に検討しなければならない場面が日常的に存在するので、上述のような問題の発生を避けることは可能であるが、それでも、問題の発生する機序を明確に意識することなく、過去の（權威あるとされる）学説や裁判例だけに安易に依拠し、自分自身の思索を放棄するようなタイプの者（または、自己がそのようなタイプの者であることを認識することさえできない者）が誤って任官してしまっているような場合には、同様の問題が発生し得る。このことは、法哲学ないし法思想の分野においても基本的には変わらないが、とりわけ法解釈学の分野においてはその弊が著しいことがある。忌むべきことである。

なお、この文脈において、「単独であること」及び「自ら直接に行うものであること」を重視するのは、一般に、共同研究の場合、語彙の問題を含め、共同研究者各自の脳内の世界が全く異なっているという理解に基づいている。少なくとも、法学における学術研究の分野においては、共同研究的な作業が意味のあるものとして成立可能なのは、当該研究組織における指導的な立場にある者に対する思想上、思考上及び研究手法上の絶対服従を必須の前提とする工房的な作業が行われる場合、または、研究対象を合理的に分割し、それが異なる語彙によって実施されても何ら支障のない場合のみである。ドイツ語ではなく日本語としてのいわゆる「シュレ」なるものは、前者の工房的なスタイルで研究を行う目的のために存在するものである。しかし、現時点の日本国においては、アカデミックハラスメントの主要な場となり得るため、禁止される。

- (2) 現時点において、GDPRの最も詳細な注釈書は、Juergen Kuehling und Benedikt Buchner (Hrsg.), *Datenschutz-Grundverordnung Kommentar: DS-GVO*, C.H. Beck (2017) である。GDPRの注釈書としては、他に、Alain Bensoussan (direction), *Règlement européen sur la protection des données: Textes, commentaires et orientations pratiques*, Larcier (2016) がある。概説書としては、Mariusz Krzysztofek, *Post-Reform Personal Data Protection in the European Union: General Data Protection Regulation EU 2016/679*, Kluwer (2016) がある。
- (3) 東京地裁判事を辞して明治大学法学部専任教授に転職した年に刊行した『ネットワーク

社会の文化と法』(日本評論社、1997)も同じである。同書には、任官早々から退官までの約14年間にわたる思索の結果が反映されている。その間、裁判官としての職務に精励する傍ら、通産省(当時)の第5世代コンピュータ開発の研究に伴う人工知能技術(特に、**Legal Reasoning**の領域)に関与する中で故石前禎幸氏と出逢い、私的に何度も意見交換を重ねたことが思い出される。

当時、法的推論の理論に関しては、固定的な文法規則・文法理論に基づく固定的な推論、古典的な意味における法実証主義の理論、そして、ペイズ流の確率計算を基礎とする推論の検証のような理論が主流であったし、その亜流である「法と経済」のような考え方も既に存在していた。当時、マービン・ミンスキー(**Marvin Minsky**)の理論の応用のような場合を含め、知識は自己完結的に記述可能なものであり、それゆえにコンピュータによる処理が可能なものであると考えられていた。当時、思考の主体によって主観的・恣意的に(かつ、ほぼ自動的に)再定義されるものであるという事実は既に広く認識されていたのであるが、ファジー理論として計算処理可能な範囲内にその問題を閉じ込める努力はなされたものの、基本的には、自己再定義のプロセスは、完全に無視されるものであった。なぜなら、そのような非固定制に基づく理論を前提とする場合、コンピュータによる自動処理ができなくなってしまうからである。複雑性の理論にしても、コンピュータによる計算処理が不可能なものは考察の対象から外されていた。

当時主流だった知識の記述可能性という信念は、フランスの百科全書派の啓蒙思想に由来するものかもしれないが、事実の問題としては、そのような信念の先例は、中国の『修文殿御覽』、『藝文類聚』、『太平御覽』及び『太平廣記』の中に既に見られる。

しかし、当時における人工知能研究の主流が採用していた基本的なアプローチの全てがほぼ意味のないものであることについては、故石前禎幸氏と私の両者に共通の基本的な認識であった。そのような共通認識を踏まえ、人工知能研究における他の関係者らとは全く別に、故石前禎幸氏と私だけは、全く別の観点からの人工知能の基本的な問題について意見交換をすることができた。それは、人間という存在それ自体に対する深い洞察を踏まえたものであった。

その後、年月を経て、現在の人工知能技術の主流は、約30年前におけるものとは全く異なる。この点については、過日、ザールラント大学のゲオルグ・ボルゲス(**Georg Borges**)教授とも私的に意見交換を行い、共通の理解を得た。現在の人工知能の理論及びその応用技術の主流は、新カント派を含め、古典的な認識哲学だけに依拠するものではなく、認知科学(**cognitive science**)ないし脳科学(**brain science**)及び関連諸科学の発展とその成果を踏まえたものである。そして、その実装は、自律的な学習に基づく自律的な能力の成長という要素(**autonomy**)をもつものである。その中には、知識の自己再定義の機能も含まれる。そのような機能の実装を支えるための機械装置やソフトウェアの発展そして数学理論の発展も著しい。その結果として、完全な人工生命体、遺伝子操作、ミュタントまたは(人間もしくはその他の動物の)サイボーグとしての有機体ロボットを含め、ノーバート・ウィーナー(**Norbert Wiener**)の意味におけるサイバネティクス(**Cybernetics**)として世界全体をとらえるべき時代が既に到来している。

故石前禎幸氏との邂逅は、私ができるような分野において今日に至るまで連続として研究を継続することとなった契機の1つとなっている。

- (4) この部分を執筆しながら、石前禎幸「ハートの社会行為論『法の概念』の読み換えのために」法哲学年報 Vol.984 (1985) 152 頁にある「開かれた構造(オープンテクスチュア)」との解釈(理解)を読んだ。

- (5) 例えば、「Tatbestand」という語は、ドイツ語及び刑法理論の素養のない者にとっては、単なる英語のアルファベットの列にしか見えず、その実体及び社会的機能を知ることができない。
- (6) 逆から言えば、国家権力としての実力の行使が正当なものとして扱われる社会関係が存在していない場合（特に破綻国家の場合）には、「法の支配」も存在しない。理念または思想だけで思考するだけで完結し、かつ、他者への働きかけを一切必要としない場合を除き、現象としての法を理解するためには、そのような視点を考慮することが不可欠である。
- (7) このような事実としての権力または正当化される暴力のための社会関係上での修辭または莊嚴の問題を考える上では、政治学の教科書及び研究書よりは、むしろ、フレイザー（永橋卓介訳）『金枝篇』（岩波文庫、2002）、ジョルジュ デュメジル（丸山静訳）『デュメジル・コレクション（1）～（4）』ちくま学芸文庫（2001）のような比較神話学の分野に属する書籍から示唆を受けることが少なくない。
- (8) なぜそうなるのかについては、古来、様々な考え方があつた。遺伝子から説明しようとするものとして、リチャード・ドーキンス（日高敏隆・岸由二・羽田節子・垂水雄二訳）『利己的な遺伝子（増補新装版）』紀伊國屋書店（2006）がある。
- (9) それゆえ、自然科学の領域における情報エントロピー理論が適用される余地はない。思考は、常にアドホックである。意思の伝達（communication）のようにみえる現象は、実際には断絶している。そこにあるのは、外界から受けた信号の自己内世界における再定義というプロセスだけである。ここでいう自己内世界とは、マルティン・ハイデッガー（Martin Heidegger）の「In-der-Welt-sein」と同義ではない。ただし、人間の思考なるものが脳神経細胞の場におけるある種の化学反応と電気信号の変換によって構成されている以上、それを解析することは可能であるし、それを生体脳の中に注入し影響を及ぼすことも可能である。ただ、当該生体脳における自己内世界の全容と機序を知ることが、その本人を含め誰にもできない。それは、タイムマシンが存在し得ない以上、当該個体である個人の過去の経験を再現することができないからである。主体としての「個人」及び他者としての「個人」は、いずれも過去の記憶が変容した諸要素の総体によって構成される。ただ、その記憶の総体が存在する場所が異なるだけである。このことは、松本恒雄・齋藤雅弘・町村泰貴編『電子商取引法』（勁草書房、2013）76～116頁（夏井高人分担執筆部分）で述べた。
- (10) 法学の領域における一般的な思考方法の説明に関しては、笹倉秀夫『法解釈講義』（東京大学出版局、2009）207～212頁が参考になる。
- (11) 立石龍彦「法律の論理Ⅱ」法律論叢 31 卷 5 号 77～87 頁（1958）参照
- (12) 法と情報雑誌（ISSN 24326089）は、非売品であり、発行部数が少ないため、通常、普通の図書館等には収蔵されていない。しかし、国立国会図書館には必ず納本されているので、国立国会図書館において、法と情報雑誌のバックナンバーを閲覧することができる。
- (13) 「個人」が法人を含まない以上、将来、自律型のロボットまたは人工知能システムに対して法人格が与えられることになったとしても、とりわけ、そのロボットが有機体で構築されたロボットであつて、外形上、ヒト（*Homo sapiens*）と全く変わらないものであつたとしても、それが法人であつて自然人ではない限り、この条約の適用はない。自然人のみに対する適用を前提とする法令である以上、このことは、その後の全ての個人データ保護法令においても同じである。その結果、当該ロボットが人間と同じような精神作用を営むものであつたとしても、そのロボットには保護法益であるプライバシーが成立し、個人データ保護法令によって法的に保護される可能性もないことになる。この

ような問題を考える上で参考となる文献として、Eric Hilgendorf (Hrsg.), *Robotik Im Kontext Von Recht Und Moral, Nomos* (2014)、Ugo Pagallo, *The Laws of Robots: Crimes, Contracts, and Torts*, Springer (2013)、ゲオルグ・ボルゲス（水津太郎訳）「「ベッパー」と法—新たな情報技術に対応する法改正は必要か—」法学研究 89 卷 7 号 57～86 頁（2016）がある。また、ロボットの定義を含め、ロボットと関連する基本的な法的課題に関しては、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 卷 4・5 号 175～212 頁で述べた。

- (14) 個人データ保護条約の成立過程において、当時の OECD における検討との密接な連携があったことについては、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 卷 2・3 号 181～245 頁で述べた。
- (15) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p.31–50)
- (16) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p.1–22)
- (17) Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (COM/2017/08 final)
- (18) 規則 (EC) No 45/2001 の改正提案 (COM/2017/08 final) の参考訳は、法と情報雑誌 2 卷 4 号 249～354 頁にある。
- (19) より正確には、「識別子」は相対的なものであり、絶対的なものではない。エドムント・フッサール (Edmund Gustav Albrecht Husserl) の意味でのノエシスとノエマという関係で考察してみても同じ結論になるであろうし、ヴェルナー・ハイゼンベルグ (Werner Karl Heisenberg) の意味での不確定性理論に基づいて検討しても、やはり同様の結果となるであろう。

そこまで詰めて考えるのではなく、俗的なレベルで考察する場合であっても、一般に、ある情報を基準とし、それ以外の情報を付加的な情報とした上で、要素集合の絞り込みを重ねることによって特定の個体（個人）の識別をすることが可能であるので、そのような意味においては、いかなる種類の情報も基準（識別子）として機能し得る。しかし、ここでいう「識別子」とは、その識別子を用いることによって直ちに特定の個人を識別可能なものとして一般に認識されているものの例示であると理解するのが妥当である。ただし、個々の情報による識別の可能性または容易性の程度は、社会環境の変化及び技術発展によって顕著に変動し得るものであるため、限定列举と考えることはできない。そのような留意点を踏まえた上で、より少ない要素（究極的には 1 個の要素）を用いることによって特定の個人を識別可能な場合、その要素が当該個人のプライバシーの利益を害する蓋然性もより高いものであると考えられる。そのような利益衡量の上になつて、ある要素が識別子であるか否かを価値判断するのが妥当である。

- (20) 最高裁判平成 29 年 3 月 15 日判決（平成 28（あ）第 442 号事件）参照

- (21) EU の Electronic identification (eID) に関しては、Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, (OJ L 257, 28.8.2014, p.73–114) がある。ドイツの電子身分証明書 (eAT) に関しては、Verordnung über Gebühren für Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgebührenverordnung - PAuswGebV) があり、Georg Borges, Rechtsfragen der Haftung im Zusammenhang mit dem elektronischen Identitätsnachweis, Nomos (2011) が参考になる。この関連で参考になる文献として、株式会社日立コンサルティング「海外における社会保障や税に関する番号制度と連携した民間サービスにおける ID の取扱いに関する実態把握のための調査」(平成 24 年 2 月) がある。
- (22) Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (COM(2017) 10 final)
- (23) 丸橋透氏との共同翻訳 (分担翻訳) による指令 2002/58/EC 改正規則提案の全訳である参考訳は、法と情報雑誌 2 巻 4 号 195～248 頁にある。
- (24) Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p.89–131)
- (25) Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p.54–114)
- (26) これらの定義条項の示す概念内容は、日本国における今後の立法及び法解釈にも反映されるべきである。ただし、従前の憲法学及び行政法学における通説的見解は、必ずしもそのようなものではない。既に実務上及び学術上の有用性を喪失しているものとする。
- (27) そのような要素は、当該個人の脳内に存在するものとして意識または認識される状態の場合もあるが、そもそも当該個人の脳裡には最初から全く存在せず、他人が保有するデータや情報である場合があるので (例：他人が知覚し、当該他人の脳内にだけ存在する記憶としての情報)、とりわけ、後者については、いわゆる「自己情報コントロール権」なる説が理論的に成立する余地が全くない。この説は、誤謬に基づく説である (この見解を社会運動の一種として残存させることは、各人の自由である。しかし、それは、社会運動の一種なのであって、学術の一部を構成するものではない)。
- (28) ただし、特別の属性値をもつ要素 (またはそのような属性をもつものとして誰かから評価され得る要素) の中で、人間の民主主義社会において基本的な権利を侵害するような差別を生じさせる蓋然性が高いと定型的に価値判断されるものは、特別類型のデータ (special categories of data) として、特別に厳格な法的規律を受ける。これは、特別類型のデータに関しては、通常の「プライバシー」という保護法益に加え、平等原則を侵害

- するような「差別を受けないこと」という保護法益もあると考えられるからである。
- (29) 「any」は、一般的な直訳としては、「何らかの」と訳すべきことになる。しかし、論理学上の集合としての個人データの中に含まれる情報を示す形容詞としては「全ての」と訳すのが正しい。
- (30) 前掲指令 2002/58/EC の改正提案中の前文(31) 参照
- (31) 通常の識別子として機能する場合は別に、感染症（特に法定伝染病）に対する対応や自然災害（特に激甚災害）に対する対応の場合を含め、住所を識別子として一定のグループに属する人々をまとめて行政措置の対象とすることが多々ある。グループとしてのプライバシー一般に関しては、Linnet Taylor, Luciano Floridi & Bart van der Sloot (Eds.), *Group Privacy: New Challenges of Data Technologies*, Springer (2017) が参考になる。
- (32) 関連する裁判例として、最高裁昭和 32 年 2 月 20 日判決・刑集 11 巻 2 号 802 頁がある。しかし、現代の社会においては、氏名が全く不明な者でも他の要素によって完全に識別・特定した上で、起訴し、公判を維持し、有罪判決をすることが可能である以上、この最高裁判決の理由の合理性は、昭和 32 年当時においてはともかくとして、現時点においては全く維持不可能であると考えられる。
- (33) 極論すると、数学的にはともかくとして、社会的な関係または法的評価においては、個人データの暗号化も仮名化も成立し得ないという問題がある。適用される技術の問題としての暗号または仮名化と、それがもつ社会的機能または法適用上の機能の問題とは別の問題として考えられなければならない。技術は、法を執行するための多種多様な手段の中の 1 つの選択肢に過ぎない。
- (34) 世間では、「住所」は「個人データ」または「個人情報」に該当しないとの俗説が流布されることがあるが、ある特定の法令の適用において当該法令の適用対象となるかという文脈における立論の場合を除き、無意味な見解である。同様のことは、不正アクセス禁止法（平成 11 年法律第 128 号）の適用において、「クレジットカード番号は特定電子計算機にアクセスするための識別符号に該当するか」という議論の中にも見られる。その解は、固定的に与えることができない。個別の事案において、「当該クレジットカード番号が識別子として用いられていることが一般に周知されているかどうか」等の付加的な要素を事情として考慮した上で、文脈の相違に応じて個別に検討されるべきである。そして、その場合においても、当該システムへのアクセスに害を与え得るものであるかどうかという利益衡量または利害打算による価値判断が行われる。
- (35) ただし、当該法令が生存する自然人だけに適用されると定められている場合、実際には、当該法令に定める権利の行使は、あり得ないことになる。その限度で、当該法令は、生存する個人に対してのみ適用される。しかし、今後、権利保護団体等に対するデータ主体の権利の行使する権限の授与並びにその権利の行使の結果としての損害賠償金の受領の権限という現行の EU の個人データ保護法制上の枠組みが更に強化されるとすれば、EU 法のレベルまたは構成国の国内法のレベルにおいて、当該個人が既に死亡している場合であっても、その故人である個人の相続財団を法人であるデータ主体として、当該故人である個人の権利行使の続行を認め、また、当該相続財団の代理者である団体に対する損害賠償金の支払いを認めるような法制の拡大や現行法の柔軟な解釈・運用が十分にあり得ると考えられる。このことは、自律型ロボットまたは人工知能システムに対して法人格を認めるべきであるか否かを考える上でも非常に重要である。
- (36) 個人データの処理が法的規制の対象となるのは、それによって当該データ主体のプライバシー侵害の蓋然性が高まると考えられているからである。それが微々たる可能性の程度で

あれば、法令による規律を考える必要性もないであろう。個別事案として民法上の損害賠償請求で解決すれば足りる。しかし、処理それ自体が一定の蓋然性を有すると仮定された以上、社会全体としての利益衡量が行われなければならない。何が個人データであるのかの問題についてもそのような観点が必要となることがある。個人データ保護の文脈においては、誰のプライバシーの利益も侵害しようのない要素（情報）であれば、とりたてて個人データの該当性の有無を検討する必要もないと考えられる。しかし、通常は個人データとは考えられていない要素（情報）であっても、プライバシーの利益を侵害する可能性が肯定される場合には、価値判断として、それを個人データとして扱うか否かが検討されなければならない。それは、自然科学における物性の確定とはかなり異なる思考作用である。それは、あくまでも、利益衡量（利害打算）を踏まえた価値判断である。

- (37) 個人データである要素（情報）は、直ちに電子計算機による自動処理を実行できるように構成されていることを要しない。それゆえ、いわゆる「散在情報」なる概念は、全く無用であるし、道具概念としても有用性をもたない。現時点では「散在情報」であっても、将来の時点で収集され処理される時点では明らかに個人データに該当することになるので、その意味でも「散在情報」の概念は意味がない。
- (38) 前掲規則 (EC) No 45/2001 の改正規則提案の前文 (38) は、「データ主体の権利及び自由に対するリスクの蓋然性及びその深刻度は、その処理の性質、範囲、過程及び目的を参照して判断されなければならない。リスクは、データ処理業務がリスクまたは高度なリスクを含むものか否かを定めることのできる客観的な評価に基づいて評定されなければならない」と述べている。
- (39) それによって法の適用範囲が法の目的を離れて不必要に拡大してしまうことを避けるため、GDPR の第 2 条第 2 項 (c) は、「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には GDPR の適用がないものとし、また、GDPR の第 40 条第 1 項は、マイクロ企業及び中小企業について、個人データの管理の方法を緩和するための措置を講ずる余地があることを定めている。
- (40) ファイリングシステムの該当性を判断する場合にも利益衡量による価値判断が行われる。一般に、検索が容易であれば、それが電子的な自動処理であるか否かに拘らず、データ主体のプライバシーの利益が損なわれる蓋然性が高まるという仮説がそこにある。そのことから、ある程度まで整理され構成されて閉じ込まれた紙の文書の束であっても、およそ容易に検索可能とは言えないようなものであれば、プライバシーの利益を損なう蓋然性も否定されることになるので、ファイリングシステムの該当性を否定するという判断がなされることになる。ここでもまた、数値化された指標に基づく物性の確定のような自然科学上の判断作業ではなく、利害打算に基づく価値判断がなされるのである。
- (41) 管理者が収集する前の情報は「個人データ」ではないとすれば、管理者は、いかなる場合においても「個人データ」を収集することができず、その開示を受ける取得者は、いかなる場合にも「個人データ」を取得することができないということになり、論理の破綻が生ずることを避けることができない。また、例えば、事業者 X のデータベース内において処理されている個人データでも事業者 Y の一切関知しない個人データは、事業者 Y との関係では常に「散在情報」であることになるが、事業者 X にとっては自己の管理下にある個人データであるので「散在情報」ではない。更に、現時点では誰も処理の対象としてない情報であっても、それが管理者によって収集されれば、明らかに、「個人データ」となる。換言すると、全ての情報は、常に潜在的な個人データである。その結果、「散在」という概念要素は、何らの属性値も示さない空虚なものであることになる。そして、

ビッグデータ（big data）による処理の場合には、このような問題が更に鮮明なものとなり、「散在情報」なる概念を用いたとたんに、明らかに論理破綻が生ずることになる。それゆえ、「散在情報」なる語は無用であり、かつ、有害である。

便宜上の名称としては、管理者の管理下でない情報については、個々の特定の処理について、個別に、かつ、相対的に、そのまま「管理者の管理下でない個人データ」または「管理者の管理下でない情報」とすれば、それで足りる。日本国の個人情報保護の法令では、「管理」または「処理」は「取扱い」になるので、個々の特定の取扱いについて、個別に、かつ、相対的に、「取扱いの下でない個人データ」または「取扱いの下でない情報」で足りるのであろう。ここでもまた、関係説的なアプローチだけが意味をもつ。

- (42) 処理の対象となっていない個人データについても権利性または法的利益性は認められるから、その侵害があるときは、民法（特に不法行為法）に基づいて損害賠償等の請求をすることができる。また、その侵害の結果として名誉毀損の状態が発生するときは、その加害者は、名誉毀損罪として処罰され得る。しかし、そのような法的救済は、個人データ保護法による救済とは別の一般的な救済の問題なので、個人データ保護の法令の中では（立証責任の転換に関する幾つかの条項を除き）特段の定めがないのが通例である。このような問題を考える場合、当該法令の適用の結果として生ずる法律効果に着眼して考察することが重要である。他の制定法または判例法によって特定の法律効果が生ずることが明らかな場合については、当該法令が適用されるのであり、個人データ保護の法令が適用されるのではない。したがって、個人データ保護のための法制の全体を正しく理解するためには、個人データ保護のための行政的規律（特に監督官による監督措置及びデータ保護責任者による内部統制）だけでなく、構成国の民法による損害賠償責任、刑法による処罰、行政訴訟法による行政訴訟、情報公開法による開示請求を含め、関連する法制度全体を見渡した上での考察が必須である。なお、この関連では、Gert Brüggemeier, Aurelia Colombi Ciacchi & Patrick O'Callaghan (Eds.), *Personality Rights in European Tort Law*, Cambridge University Press (2010), Patrick O'Callaghan, *Refining Privacy in Tort Law*, Springer (2013), Ronald J. Krotoszynski Jr., *Privacy Revisited: A Global Perspective on the Right to Be Left Alone*, Oxford University Press (2016) が参考になる。
- (43) このことは、GDPRの第45条に定める欧州委員会による十分性の判定（adequacy decision）の判断基準を考える上でも重要なことである。GDPRの各条項が許容する範囲を超えて、非常に強すぎる、または、非常に弱すぎる法的保護を定める法令をもつ第三国は、十分性の認められない国として扱われることになるであろう。その具体的な要件は、GDPRの第45条第2項に定められている。
- (44) European Commission, *Questions and Answers: Schengen Information System (SIS II)* (Brussels, 9 April 2013) が参考になる。
- (45) Regulation (EC) No 81/2009 of the European Parliament and of the Council of 14 January 2009 amending Regulation (EC) No 562/2006 as regards the use of the Visa Information System (VIS) under the Schengen Borders Code (OJ L 35, 4.2.2009, p.56–58)
- (46) Regulation (EU) No 1024/2012 of the European Parliament and of the Council of 25 October 2012 on administrative cooperation through the Internal Market Information System and repealing Commission Decision 2008/49/EC ('the IMI Regulation') (OJ L 316, 14.11.2012, p.1–11)

- (47) 改正提案書 (COM/2017/08 final) の説明用覚書 (Explanatory Memorandum) の 5 (その他の事項) 中にある第 62 条の解説参照
- (48) 表現の自由及び公共の利益等の優越する利益を優先させるために個人データ保護と関連する法令の適用が抑制され得る場合については、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—」で詳論したとおりである。なお、米国における表現の自由とプライバシーの利益との関係については、佐々木秀智「インターネット上の私的事実公表型プライバシー侵害とアメリカ合衆国憲法修正第 1 条」法律論叢 89 巻 6 号 221～258 頁 (2017) が参考になる。なお、関連する文献として、小倉一志『インターネット・「コード」・表現内容規制』(尚学社、2017)、Jeff Kosseff, *Cybersecurity Law*, Wiley (2017) がある。
- (49) 多数の項目が記載されている書面上で「以上を全部読み、了解しました」との趣旨の文言の箇所にチェックする方法、または、同様の箇所に署名をする方法などが考えられる。日本国においては、約款によって規律されている証券、金融、保険等の業界で用いられる契約書等の中で、そのような手法による包括的な同意の取得がむしろ常態化していると言える。しかし、中には、消費者契約法違反となり得るようなものも存在することを否定できない。
- (50) 適法化事由 (正当化事由) が全く存在しない「裸の個人データ処理」は、違法行為であるという論理構造を前提としている。それゆえ、日本国の俗説に多々みられるような性善説的な見解は全て否定される。デフォルトは悪 (違法行為) であり、その悪を適法行為 (正当事由のある行為) へと転換するための所定の要件の充足が求められる。その要件が充足されない限り、その処理 (取扱い) は、デフォルトのまま、悪 (違法行為) である。換言すると、要件を重装しない限り、個人データ処理の自由は存在しない。それゆえ、無条件の個人データの自由な移転もあり得ない。
- (51) 前掲 Kuehling/Buchner, DS-GVO の 260～281 頁に第 7 条の詳細な解説がある。
- (52) 本稿においては、慣例に従い、通常の見解可能な範囲内にある文法概念及び文法理論に基づいて論述した。ただ、私見としては、自然言語において、名詞と動詞を一般的に区別することは不可能であるという見解をもっている。文脈と状況に応じて、通常の見解において動詞として認識されているような言語的な作用が発現するだけのことであり、そのような作用を発現させるための用法を動詞と名付けることは可能であるが、その語それ自体の属性ではない。その場におけるアドホックな作用の一種に過ぎない。人間が書く文章のための言語は、実は人工言語であって、自然言語ではないので、文法構造をもっているように見えるし、また、そのように用いられる。しかし、現在の人類文明が減び、文字を含め、読み書きの文化が消滅した後、太古のネアンデルタール人と同じような生活をするしかないごく少数の人々が散漫に生き残ったというような状況を想定してみると、純粋な自然言語の世界においては、動詞と名詞の区別さえ必要ないということ即座に理解することができる。現代において一般に言語として認識されている読み書きのための言語の体系と語彙は、基本的には、官僚組織と領域支配のために当時の官僚等によって構築された人工的な産物に過ぎない。決して、自然言語ではなく、むしろ、コンピュータのためのプログラム言語に近縁のものである。

このようにして、法で用いられる用語や言語を理解する場合でも、それが人工言語としての一定の法則に従っている場合があるということを明確に認識することが重要である。そうすることによって、法の適用対象である世界では、人工言語としての言語が機

- 能しているわけではないかもしれないということに逆に気づくことができるのである。一般に、符号としての語だけが存在し、共通の規則としての語彙及び文法が存在しない場合（または、それを確認することができない場合）、当該の語以外の要素によって、その語が用いられる意図やその作用・結果のようなものを観察し、各自が主観的に評価し、自己満足的に納得する以外には何もできないのが普通である。
- (53) 日本国の法分野では、労働災害保険及び雇用保険等に関する法領域が該当すると解される。
- (54) ここでいう協約とは、日本国において普通にみられる個別の企業単位での労働協約のことではなく、横断的な同業労働者組合と経営団体との間の協約（集团的合意）のことを指し、そのような合意は、約款というよりは法規に近い法的拘束力を有する。
- (55) 前掲 Kuehling/Buchner, DS-GVO の 294～329 頁に詳細な解説がある。
- (56) GDPR の他の条項の中で第 46 条の安全性確保措置を参照しているときは、同条第 2 項の文書等を指すものと解すべきことになる。
- (57) 当該社会が侵略、戦乱、大規模災害等によって物理的に消滅した場合、物的な符号列のみが残ったとしても、その社会的な機能は失われる。人工知能技術の応用を含め、失われた古代の言語の解析技術がかなり進んできたとはいえ、ロゼッタストーンのような対訳文書が遺物として残されているような場合を除き、一度失われた言語や文化を再現することは不可能または非常に困難なことである。このような場合、国家という組織それ自体の安全性確保措置が機能せずに、その安全性が確保されなかったと理解することが可能である。これが国家の生存権の本質であるが、基本的には、トマス・ホップズのいうところの生存権と何ら異なるところがない。なぜなら、国家は、一定の集団を構成する人の集合を生存させるための装置の一種だからである。
- (58) 「Justice」に関しては、単純に「正義」と訳すことができるか否かについては、疑問がある。「Security」についても同じであり、その対象が領土または地理的な領域である場合には「安全保障」または「防護」または「防衛」と訳すのが正しい。しかし、本稿の主題ではないので、この点については他日を期したい。この点に関して参考となる文献として、南部朝和「EU におけるシェンゲン・アキ (Schengen acquis) と「自由、安全、司法の領域」の進展」平成法政研究 7 卷 2 号 167～216 頁 (2003)、須田祐子・前田幸男「シェンゲン情報システム (SIS) の現状と課題—「国境のないヨーロッパ」の国境管理と IT システム—」境界研究 3 号 1～13 頁 (2012)、岡部みどり「シェンゲン規範の誕生—国境開放をめぐるヨーロッパの国際関係」上智法学論集 57 卷 1・2 号 41～61 頁 (2013) がある。「Justice」を「正義」と訳すものとしては、高橋和「越境地域協力と国境管理—シェンゲン条約と人の移動の管理をめぐって—」山形大学法政論叢 50 号 76～102 頁 (2011) がある。
- (59) The Stockholm Programme - An open and secure Europe serving and protecting citizens (OJ C 115, 4.5.2010, p.1-38)
- (60) 理事会決定 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA 及び 2009/968/JHA
- (61) 駐日欧州連合代表部の公式ウェブマガジンである『EU MAG』の「Q1. 欧州テロ対策センター (ECTC) はどのような経緯で設立されたのですか?」の中にその説明がある。
- (62) Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ L 119, 4.5.2016, p.132-149)

- (63) Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes (OJ L 323, 10.12.2009, p.20–30)
- (64) Steve Peers, *EU Justice and Home Affairs Law Volume I: EU Immigration and Asylum Law* (4th edition), Oxford University Press (2016)、Steve Peers, *EU Justice and Home Affairs Law Volume II: EU Criminal Law, Policing and Civil Law* (4th edition), Oxford University Press (2016)、Maria Fletcher, Ester Herlin-Karnell & Claudio Matera (Eds.), *The European Union as an Area of Freedom, Security and Justice*, Routledge (2016)、Diego Acosta Arcarazo & Cian C. Murphy (Eds.), *EU Security and Justice Law: After Lisbon and Stockholm*, Hart Publishing (2014)、Diana-Urania Galetta, *Procedural Autonomy of EU Member States: Paradise Lost?: A Study on the “Functionalized Procedural Competence” of EU Member States*, Springer (2010)、G. Vermeulen & W. De Bondt, *EU Justice and Home Affairs: Institutional and policy development*, Maklu (2014)、Maik Martin, *Crime, Rights and the EU: The Future of police and judicial cooperation*, Justice Publication (2008)、Ángeles Gutiérrez Zarza (Ed.), *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe*, Springer (2014) が参考になる。
- (65) 日本国の法制度においては、EDPSに相当する国家機関が存在せず、行政機関を含む公的部門における独立の監督官による監督制度が実質的に欠落している。行政機関における独立の監督機関が実質的に存在しない以上、十分なレベルの法的保護のための法制度が存在するとは言えず、換言すると、一貫性のある法的保護のための仕組みが存在しているとは言えず、欧州委員会による十分性の判定は、ほぼ不可能と考えられる。EUとの間の個人データの交換は、十分性の判定が存在しない場合に適用される特例（拘束的企業準則、約款、認証、国際協定の締結等）の方法によらざるを得ないであろう。
- なお、約款や行動準則等の内容は、実質的にみてGDPRの関連条項が日本国においてもそのまま適用されるのと同然のものとしなければならない関係上、影響を受ける日本国内の法令や制度が存在する場合には、その手直しが避けられないのではないかと考える。なお、拘束的企業準則に関しては、Lokke Moerel, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfer*, Oxford University Press (2012) が参考になる。
- (66) 構成国における監督官の役割の中で通常あまり論じられていない職務に関しては、夏井高人「欧州連合の構成国における独立の個人データ保護監督官の職務」法律論叢 89 巻 6 号 309～363 頁で詳論したとおりである。
- (67) 電子通信分野において個人データ保護制度を一部修正するデータ保持指令 2006/24/EC の有効性に関しては、丸橋透「Tele2 Sverige AB 対スウェーデン郵政通信省 (C-203/15) 及び英国内務大臣対トム・ワトソン他 (C-698/15) 先決裁定事件欧州連合司法裁判所大法廷判決 (2016 年 12 月 21 日) ECLI: EU: C: 2016: 970 [参考訳]」法と情報雑誌 2 巻 1 号 1～40 頁が参考になる。
- (68) そのような法制上の相違が基本的な権利及び自由を侵害するものである場合には、欧州司法裁判所または欧州人権裁判所の先決裁定等により、法令それ自体の無効が宣言されることになる。日本国の最高裁は、そのような抽象的な違憲審査権はないとの見解を維持している。しかし、それは、日本国憲法がそのように明確に定めているためにそうであるわけではなく、いわば、最高裁判事の主観的な判断の一種に過ぎない。それゆえ、現

在の最高裁判事が異なる主観的な判断をすれば、最高裁は、いつでも即座に抽象的な違憲審査権をもつことになる。これが私見であるが、この私見が誤りであるとする場合には、憲法改正手続を経て、特別裁判所である憲法裁判所を設置する以外に方法はない。

(69) **Rules of Procedure on the Processing and Protection of Personal Data at Eurojust** (OJ C 68, 19.3.2005, p.1–10)

(70) 本稿は、科学研究費補助金共同研究基盤研究(A)知的財産権と憲法的価値・科研費研究課題番号 15H01928 の研究成果の一部である。また、EUの一般個人データ保護規則 GDPR の前文の日本語訳作成及びその研究に関して、KDDI 総合研究所から研究資金の提供を受けた。

(明治大学法学部教授)