情報社会の素描
-EUの関連法令を中心として-（2・完）

法律論叢第90巻第6号（2018.3）

【論　説】

情報社会の素描―EUの関連法令を中心として―(2・完)

夏　井　高　人

目　次

3　情報社会の制度的プロトコル部分

情報社会の制度的プロトコルの基本部分(132) は、今後更に綿密な検討を要するものの、現時点においては、制度設計上の総則的なプロトコル部分と制度設計上の各論的なプロトコルとに分けて考えることができる。

総則的なプロトコルには、制度設計上の内容的なプロトコルと立法手続上のプロトコルが含まれる。これらは情報社会に固有のものではないが、そのプロトコルの実装及び運用がネット上の情報提供を含む情報社会に特有の手段を基軸にして構築されるようになってきている点に着目すれば、今後、情報社会に特有の要素を抽出することによって一定の研究の深化が期待可能なのではないかと考えられる。

他方、各論的な様々なプロトコルの中では、データセットの定義の共通化に関するプロトコル、アクセス制御に関するプロトコルの 2 つが最も重要である。これらの中で、データセットに関するプロトコルは、その構成要素それ自体が電子データであることから、情報社会に固有のものと考えることができる。アクセス制御に関するプロトコルは、それ自体としては情報社会に固有のものではない部分を含むが、情報システムに格納されているデータや情報システムへのアクセスの制御に限定すれば、情報社会に固有の要素を考察可能である。

3．1　基本原則

3．1．1　基本的な権利及び自由の尊重

欧州連合の機能に関する条約（TFEU）の第6条（旧TEU第6条）は、その第1項において、「欧州連合は、ストラスブールにおいて2000年12月12日に採択され、諸条約と同じ法的価値をもつ2000年12月7日の欧州連合の基本的な権利の憲章に定める権利、自由及び基本原則を認める」と定めている。この憲章（Charter）(133)の現行の版は、2016年の版（2016/C 202/02, OJ C 202, 7.6.2016, p.389-405）である(134)。

欧州連合の基本権憲章（以下「憲章」という。）の中で宣言され、かつ、TFEUによって認められている基本的な権利及び自由は、EUの法制における基本的な保護法益を定めるものと解することができる。しかし、それらの権利の条項の大半は、その権利としての内容を示すだけであり、権利の行使のための具体的な手段・方法を示していない(135)。それは、より具体的な場面において、個々の法令の中で、手段的・技術的・人工的な権利として明確化されて定められることが多い。

憲章は、様々な権利を定めている。それらの中で、情報社会と特に密接な関連をもつ権利は、私生活の尊重の権利（第7条）、個人データの保護の権利（第8条）及び情報伝達の権利（第11条）である。加えて、知的財産は保護される（第17条第2項）。

憲章第7条は、「全ての者は、彼または彼女の私的な生活、家庭の生活、住居及び通信に対して尊重される権利をもつ」と定めている。これは、実質的にみて、個人の私生活と関連する利益、すなわち、プライバシーの利益の保護を意味するものと解される。プライバシーの利益は、情報社会とは無関係な場面でも多々成立可能なものであるが、情報社会との関係では、いわゆる通信の秘密(136)と関連する部分が特に密接な関連性をもつ。憲章の第7条にある「通信（communication）」もまた、電気通信のみに限定されるものではなく、紙の郵便物を含め、電気通信以外の様々な態様の通信に広く適用され得る。しかし、情報社会においては、インターネットを介して送受信される電子メールを含め、電気通信の秘密を確保することが重要であることは言うまでもない。また、「モノのインターネット（IoT）」の普及により、家庭内の個人の秘密が容易かつ包括的かつ継続的に暴露されるリスクが著

しく増大していることにも留意しなければならない(137)。

憲章第 8 条第 1 項は「全ての者は、彼または彼女に関する個人データの保護の権利をもつ」と定め(138)、この基本的な権利をより具体的に実現するための手段的な権利として、同条第 2 項は、「かかるデータは、特定の目的のために、公正に、かつ、当該の者の同意もしくは法令に定めるその他の根拠に基づいて、処理されなければならない。全ての者は、収集された彼または彼女に関するデータにアクセスする権利及びそのデータを正しく訂正させる権利をもつ」と定め(139)、そして、同条第 3 項は、制度的保障の一種として、「これらの規定の遵守は、独立の機関の監督に服する」と定めている(140)。これら同条第 2 項及び第 3 項の権利及び制度を定める法制が存在するということが「基本的に均等な」(141) レベルのデータ保護を意味することになる。

憲章第 11 条第 1 項は、「全ての者は、表現の自由をもつ。この権利は、意見をもつ自由、行政機関の介入を受けることなく、所在国に拘らず、情報及び思想を受領し伝達する自由を含む」と定めている。第 7 条の「通信」は、他者によって侵害されないことに保護法益としての重点があるのに対し、第 11 条第 1 項の「情報」に関する権利は、積極的に送信・受信・媒介（伝達）する自由を示すものである。ただし、これは「自由」であるので、そのような情報の送受信行為が「違法行為にはならない」という保障があるのにとどまる。ある情報の送受信または媒介（伝達）を他者に対して法的に強制できる権利ではない。複数の者の表現の自由が内容的または機能的に矛盾を発生させるときは、利益衡量によって解決せざるを得ず、その意味で、この自由は無限定な自由ではない(142)。

3．1．2　透明性の原則と説明責任

EU の「より良き立法のための機関間合意」(143) の第 32 項は、通常の立法手続における基本原則として、「誠実な協力（sincere cooperation）」、「透明性（transparency）」、「説明責任（accountability）」及び「効率性（efficiency）」を掲げている(144)。これらの中で、「誠実な協力」は、欧州議会、欧州連合の理事会及び欧州委員会の 3 者の間における協力関係を示すものであるので、安易に一般化できない側面があることを否定できないが、それ以外のものは、EU の機関以外の場合にも妥当する普遍性をもつ。とりわけ、「透明性」及び「説明責任」は、何らかのデータ管理を伴う場合の管理主体の法的責任に関して、EU の様々な立法の中

で明言されているところであり、横断的な適用のある基本原則であるという意味で、情報社会の法の各論的なプロトコルの重要部分を構成するものと考えることができる。

例えば、個人データ処理の基本原則を定める一般データ保護規則（GDPR）(145)の前文(58)は、「透明性」の意義について、「透明性の原則は、公衆またはデータ主体に伝達される情報が、明解であり、容易にアクセスでき、かつ、容易に理解できるものであること、そして、明解で平易な言語によるものであること、加えて、それが適切な場合には、視覚化技術が用いられていることを求める。そのような情報は、例えば、Webサイトを介して公衆に伝達される場合には、電子的な方式で提供され得る。オンラインの商業宣伝広告の場合のように、関与者の増加及び実務上の技術的な複雑性によって、彼または彼女の個人データが収集されるのかどうか、誰によって、何の目的のためであるのかをデータ主体が認識し、理解することを困難にされてしまっているような状況下においては、この原則は、特に関連性をもつものである。子どもが特別の保護を享受することに鑑み、処理が子ども向けのものであるときは、いかなる情報及び通信も、子どもが容易に理解することのできるような明確かつ平易な言語によるものでなければならない」と説明している(146)。そして、GDPR第5条の第1項(a)は、個人データは、「そのデータ主体との関連で、適法であり、公正であり、かつ、透明性のある方法で処理される（「適法、公正及び透明性」）」と定めている。また、同条第2項は、「管理者は、第1項について責任を負い、かつ、同項の遵守を説明することができるものとする（「説明責任」）」と定めている。この場合において、第1項(a)の「透明性」とは、適法性を説明できる状態にあることを意味し、第2項の「説明責任」は、適法性について説明を求められた場合に説明すべき義務を負い、かつ、現実にその説明を行うことを意味する。その限りにおいて、透明性と説明責任とは、論理的な意味で対になっている部分がある。

また、法へのアクセス報告書2015/C 97/03(147)の第72項は、EUのオープンデータに関し、「委員会決定2011/833/EUに基づく義務とは別に、欧州委員会の組織は、それらのためにつくられたデータまたはそれらによってつくられたデータを欧州オープンデータポータル（ODP）に反映させなければならず、他方、欧州委員会以外の機関、部局及びそれ以外の組織は、それに加わることを勧奨される。

このポータルは、共通のメタデータのカタログを介して、営利目的または非営利目的のために、範囲を拡大させ続けるデータの容易な検索、ダウンロード及び二次利用を誰でもできるようにする。このポータルは、EU の機関及び部局のデータの視認性及び発見容易性を拡大させており、また、EU の機関及び部局の公開性及び透明性に強力な貢献をしている」と述べ、また、委員会決定 2011/833/EU(148) の第 10 条は、EU の機関のオープンデータの二次利用における透明性の確保の具体的方法に関し、その第 1 項において「二次利用することのできる文書に適用される条件及び標準的な手数料は、事前に定め、それが可能かつ適切なときは、電子的な手段を介して、これを公表するものとする」と定め、同条第 2 項において「文書の検索は、二次利用可能な主要な文書の台帳のような、実務的な手立てによって促進される」と定めている。この場合における透明性とは、より具体的に、利用者のアクセスの容易性及び利便性が高いことを意味している(149) 。

3．1．3　バイデザイン及びバイデフォルトの原則

個人データ保護との関係におけるバイデザイン及びバイデフォルトの原則(150) の最も明確な定義は、GDPR にある(151) 。GDPR の第 25 条第 1 項は、「技能の水準、実装の費用、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発生確率と深刻度のリスクを考慮に入れた上で、管理者は、この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方法で実装するため、そして、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」と定めている。ここでの例示は、「仮名化」である。また、同条第 2 項は、「管理者は、その処理の個々の特定の目的のために必要な個人データのみが処理されることをデフォルトで確保するための適切な技術上及び組織上の措置を実装する。この義務は、収集される個人データの分量、その処理の範囲、その記録保存の期間及びアクセス可能性について適用される。とりわけ、そのような措置は、個人データが、その個人の関与なく、不特定の自然人からアクセス可能なものとされないことをデフォルトで確保する」と定めている。ここにおける例示は、アクセスコントロールである。そして、その実装の方法に関し、GDPR の前文(78) は、「とりわけ、バイデザインのデータ

保護及びバイデフォルトのデータ保護の原則に適合する措置を実装しなければならない。そのような措置は、就中、個人データの処理のミニマム化、可能な限り速やかな個人データの仮名化、職務及び個人データの処理に関する透明性、データ主体がデータ処理を監視できるようにすること、管理者が安全機能を開発し、向上させることができるようにすることによって、構成され得る」と説明している。要するに、単に安全性確保のための何らかの方策を講ずるというのではなく、より具体的なレベルで、個々の個人データ処理の特性に即して、個人データを保護するための技術的な手段または組織上の方策を事前に実装するということを意味する(152)。

このような手法は、個人データ保護以外の分野においても見られる。例えば、欧州委員会通知COM/2009/0691 finalでは、「セキュリティバイデザイン（security by design）」が強調されており、2017年1月25日のSecurity Union第4次進捗状況報告書COM/2017/041 finalの中でも「セキュリティバイデザイン」の概念が用いられている(153)。同報告書の脚注8によれば、ICAOの基本的な考え方に基づき、Air Traffic Management Master Plan等の中で「サイバーセキュリティバイデザイン（cybersecurity by design）」の考え方が進展しているとのことである。また、2017年10月18日のSecurity Union第11次進捗状況報告書COM/2017/0608 final(154)では、「プロテクトバイデザイン（protect by design）」が強調されている。ここでいう「プロテクト（protect）」とは、ハイブリッドな脅威、サイバー攻撃またはサイバー戦に対抗するための防護・防衛のことを意味するものである。指令2006/42/EC（OJ L 157, 9.6.2006, p.24-86）は、機械装置の安全性について「バイデザイン（by design）」を掲げている。

これらのEUの公式文書における「バイデザイン（by design）」は、EUの個人データ保護と関係する法令における「バイデザイン」と基本的に同じ機能をもつ手法を指している。今後、EUの法制においては、例えば、環境保護や消費者保護の分野等においても、「バイデザイン」の考え方が導入される可能性が高い(155)。以上のような意味で、「バイデザイン」は、横断的なプロトコル層の一部を構成するものと考えることができる。

ただし、この手法は、事前抑制が許されない分野においては禁忌である。例えば、表現の自由と関連する問題に関しては、原則として、バイデザインによる事前抑制は許されない。バイデザイン及びバイデフォルトの原則は、憲章に定める基本

的な権利を保護するために効果的であり合理性のある場合に導入されるべきものである。しかしながら、EU においては、現実には、ヘイトスピーチやテロリズム関連の表現行為等を含め、ある種の表現行為に対する事前抑制政策がかなり強力に推進されている。この場合の保護法益は、個人の保護法益ではなく、集団的な利益としての公共の利益（public interest）あるいは国家安全保障であることが多い。この公共の利益または国家安全保障の実質的内容、及び、平時と戦時が常に共存し、それが長期間にわたって持続するような状況（特に、国家によるサイバー攻撃が恒常化しているような状況）における保護法益の均衡を含め、今後の重要な検討課題の 1 つである(156)。

3．2　立法の再評価

上述のバイデザイン及びバイデフォルトという考え方は、事後対応ではなく、事前の準備と重視する考え方である。これは、マネジメントシステムにおける基本的な考え方（特に PDCA サイクルの考え方）を導入したものと理解することができる。すなわち、設計段階でリスク評価を行い、そのリスクをミニマムなものとするための設計を行い、その運用結果を評価した上で、更に改善を施すという手法である(157)。

前掲「より良き立法のための機関間合意」は、EU の機関である欧州議会、理事会及び欧州委員会による立法活動における基本原則を定めるものであるが、その中では、各種法律文書の立案に関する基本原則だけではなく、全ての立法活動に適用される評価（assessment）及び見直し（review）に関する基本原則及びその共通の実施方法の骨子も定めている。その重要な骨格部分は、EU によって制定された法令を実装（implement）し、執行する欧州委員会の責務として、当該法令の有効性や効率性等に関する定期的な評価を実施すること、その評価に基づいて当該法令の見直しをすること、その見直しに基づき、必要があれば、当該立法の改正提案または新規の立法提案を行うことなどが含まれる。そのような評価及び見直しの仕組みは、EU の近時の多数の法令の中に条文化されて組み込まれている。

このような立法活動のサイクルにおける PDCA サイクルと類似する基本構造は、国家機能としての立法及びその執行（行政）が全体として整合性のあるものとして機能するように意図的に統御されているという事実を意味するものである。そし

て、それは、古典的な三権分立の考え方とは別に、1個の国家組織としてのEUの統括的運営という理念を強く押し出しているものということもできる(158)。その意味で、EUの機関における立法活動の評価及び見直しのための基本原則は、情報社会の法制度においても、横断的なプロトコル層の一部を構成するものと考えることができる。

3．3　識別

情報社会は、およそ情報であるものが概括的に関係するものとして理解すべき場面もあるが、法制という観点においては、情報またはデータのそれ自体としての識別を必須の要素として成立している。情報またはデータの識別ができない場合、電子的な処理（processing）は、実行不可能である。それゆえ、情報社会は、分類（taxonomy）と区別（classification）を必須の要素として成立するものであるということもできる。このような本質をもつものであるからこそ、異なる分類または区別に服する要素が個人の保護法益と関係する場合、とりわけ、その分類及び区別が憲章の第1条に定める個人の尊厳と関係する場合、TFEUにも定めるとおり、平等（差別禁止）と多様性（diversity）の尊重も不可欠の規範的要素の1つとなるのである。このような論理関係が厳然として存在していることを無視した単純過ぎる理想論のようなものは、少なくとも、情報社会の法を考察する上では、無意味かつ無力である。

ところで、個人及び物品は、本来は、例えば、人や物体の形態自体のような視認によって確認可能な物的要素、紙や粘土板に書かれた文字や符号を含め、電子情報または電子データ以外の要素によっても識別可能なものである。むしろ、そうであるからこそ、古代から人類の社会組織が形成・維持可能なものとして存続してきた。しかし、情報社会の法を概観するという視点からは、個人及び物品の識別のために使用される基準、システム及び識別子がどのようなものであり、それによって「識別されること」の本質的意味を探究することが大事である(159)。

他方、ある情報またはデータが識別可能であるか否かと、当該情報またはデータが真正なものであるか否かとは無関係の問題である。同様に、特定の情報またはデータ及びその作成者が識別可能な場合であっても、その作成者の実在性及び生存の有無もまた、当該情報またはデータの識別性の有無とは無関係の問題であ

る。このことが最も顕著に法的検討課題として表出する例の 1 つとして、例えば、いわゆる「orphan works」と呼ばれる一群の作品であり、その著作権法上の処理が問題とされてきた。EU においては、いわゆる「orphan works」の問題に関して、指令 2012/28/EU(160) による対処が行われている。同指令は、情報社会指令 2001/29/EC を補完するものという位置づけが与えられている。

また、電子的な識別等が全部可能であっても、その可用性（availability）までは保証されない。例えば、人間の感覚器とりわけ視聴覚の器官に障害のある者にとっては、情報またはデータの可用性が大幅に制限されてしまう。そのことから、EU においては、例えば、視覚障害等のある者に対する権利保障を定めるマラケシュ条約を実装する指令 (EU) 2017/1564(161) 及び規則 (EU) 2017/1563(162) により、このような場合に関する法的対応が行われている。指令 (EU) 2017/1564 第 8 条により、情報社会指令 2001/29/EC の一部改正が行われた(163) 。

以上のような問題はあるが、ある情報またはデータの識別の問題は、それが電子的に処理されるものである限り、全てのシステムにおいて共通かつ横断的に発生する検討課題であり、かつ、EU においては、その識別基準の標準化を推進するための法制整備が着々と進められていることに鑑み、識別（identification）は、分野の別を問わず、情報社会の法におけるプロトコル層に属するものであると考える。

3．3．1　個人の識別

一般に、個人（an individual）の識別と個人の識別子（identifier）の識別とは異なる。個人の識別のためには識別子を要しない。例えば、絶海の孤島におけるロビンソン・クルーソーは、何ら識別子なしに自己を自己として識別している。その場合の識別基準は、「自我によって指示されるものであるか否か」だけである。これによってロビンソン・クルーソーは、フライデーと識別されるのである。これに対して、識別子は、多数の個人が存在する環境において、特定の個人を識別できたものとして社会的に扱うための擬制的な手段である(164) 。従って、特定の識別子が識別された場合であっても、そのことによって特定の個人が自動的に識別されたことには全くならない。

EU の電子識別規則 (EU) No 910/2014 は、このことを明確に意識した上で、電子署名及び電子シールに付される法人代表者の電子署名について、本人との連携を確保するための確認情報源（authoritative source）の確保を求めている(165) 。

確認情報源は、多種多様な要素（factor）で構成され得るが、1個または複数の要素によって特定の自然人を識別することができるものでなければならない。ここでいう識別とは、数学的な厳密さにおける証明のことを指すのではなく、当該社会における経験則に基づく推論として許容範囲内にあることを意味する(166)。それゆえ、環境及び状況によって異なる方式・態様・程度を示すものとなるのであるが、要するに、当該特定の社会集団において一定の閾値を超える納得度が得られるのであれば、それで足りる問題である。それゆえに、特定の自然人を識別できるということは、そのことによって常に本人として識別されているとは限らないということも意味する。ここでは、当該社会環境における閾値としての集団的な納得度が満たされているということだけである。自然人の識別とは、本質的にこのような社会的な評価によって構成されるものであり、相対的なものなのであって、数学及びその応用とは異なる。それゆえ、理論的には、常に反証が成立し得る潜在的な可能性が存続していると考えなければならない。

ある識別子がそれのみで直接に特定の自然人を識別する能力をもたない場合、その識別子は、諸々の要素（factors）の中の1つを構成するものに過ぎない。そして、そのような意味での要素の1つとしての識別子を含め、他の要素との組み合わせにより、閾値としての一定の社会的・集団的な納得度を超える状態に至れば、特定の自然人が識別されたものとして社会的に取り扱われる。識別子は、論理的には、そのような意味しかもたない。それゆえ、「識別子」という属性値をもつ符号またはデータであるというだけで、格別に高度な証明力をもつものと即断することは許されない(167)。そのような分類に服しているというだけのことである。

以上を前提とした上で、GDPR第4条(1)は、「個人データ（personal data）」の定義として、「「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（「データ主体」）に関する情報を意味する；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」と定めているから、識別可能な自然人を（推論によって）識別するために使用される要素となるものは、全て「個人データ」である。それゆえ、氏名や識別番号だけではなく、指紋、掌紋、DNAプ

ロファイル、顔画像のような生体要素や、あるいは、所在地や場所的移動を示す位置データも個人データの一種であることになる。そして、それらは、当該識別が行われる文脈の中においてのみ個人データとしての社会的機能を営むものである(168)。同様の条項は、EU の機関における個人データの処理に適用される規則(EC) No 45/2001、構成国の電気通信分野の組織における個人データの処理に適用される e プライバシー指令 2002/58/EC 及び構成国の警察組織における個人データの処理に適用される警察指令(EU) 2016/680 にもある(169)。

これらの自然人を識別するために用いられる諸要素の中で、理事会決定 2008/615/JHA(170) の適用のある個人データの技術仕様（XML によるデータ構造等）に関しては、理事会決定 2008/616/JHA(171) によって定められている。

自然人を識別する実際の方法としては、諸要素を個別的に用いて識別する場合だけではなく、複数の要素を組み合わせて識別が実行される場合（プロファイリング処理）もある。現実には、複数の要素を組み合わせないと特定の自然人を絞りこむことができないのが普通であるので(172)、そのためのデータセットを正規化して実行するプロファイリングの手法のほうがデフォルトであり、逆に単一の要素のみによる識別は稀有または偶然的であると考えるべきである。自動的なプロファイリングに関し(173)、GDPR の第 22 条第 1 項は、「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悪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。同様の条項は、他の個人データ保護法令の中にもある。GDPR の第 22 条第 1 項は、同条第 2 項により、契約の履行のために必要となる場合、データ主体の正当な利益を守るために必要となる場合、及び、データ主体の同意に基づく場合には適用除外となるが、データ主体の同意による場合に関し、同条第 3 項は、「そのデータの管理者は、データ主体の権利及び自由並びに正当な利益、少なくとも、管理者の側での人間の関与を得る権利、彼または彼女の見解を表明する権利及び判定を争う権利の安全性を確保するための適切な措置を実装」しなければならない旨を定めている。

3．3．2　物品の識別

物品の場合においても、識別の概念と識別子の概念に関しては、識別の対象が自然人を除く物体であるという点を除き、本質的には自然人における識別と全く同じ

である。

物品の識別のための手段としては、一般に、バーコードやRFIDが使用される。RFIDは、電波を用いるため、RFIDに関する法令の大多数は、周波数帯の割り当てやその行政監督を含め、EU及び構成国の電気通信法の分野に属する法令の一部として制定されている(174)。例えば、指令2002/96/ECを廃止して採択された指令2012/19/EU(175)及び指令2002/95/ECを廃止して採択された指令2011/65/EU(176)がそのような法令に該当する。

EUは、モノのインターネット（IoT）を促進し、更に、人工知能技術の応用としての自律的な装置の集合体の開発・普及を進めている。このような自律的な装置の集合体を構成する個々の自律的な装置・機器類は、「サイバー物理機器（cyber-physical object (CPO)）」と呼ばれ、CPOで構成されるシステムのことは、「サイバー物理システム（cyber-physical system (CPS)）」と呼ばれる(177)。EUにおける産業用ロボット政策(178)は、多様な製品及びサービスの開発をめざしているが、それらの中でも特にCPO及びCPSを基礎とする自律的な機器・装置群の自律的なネットワーク管理が重視されており、例えば、自律走行自動車や自律航行船舶による運送業務の自動化が現実の政策課題として重視されているようである。そのような自律的システムが社会の中に大量に投入される場合の影響を含め、自律的な機器・装置の相互自動識別、法的責任等についてElectronic Components and Systems Joint Undertaking (ECSEL)等の組織を中心にして、「Smart Cyber-Physical Systems」の構築を目標とする検討が重ねられている(179)。このようなCPSは、機械人形のような装置とは相当異なる姿をしており、ネットワーク全体が1個の産業用ロボットとして自律的に協調して動作するような仕組みであると表現することが可能である(180)。

他方、ある機器・装置の自動識別は、当該機器・装置に識別子及びその機能が存在するだけでは実現不可能なことである。例えば、ある物品にバーコードが付されていても、そのバーコードを読み取り、当該バーコードに記録されている情報を自動的に処理するためのシステムが存在しなければならない。RFIDのような電波を用いる電子的な識別子でもそのことは同じであり、また、CPOにおける相互的・自律的な相互識別でも全く同じである(181)。そして、当該識別子が移動体として存在している場合でも同じである。

このような識別子をもつ対象を識別する側のシステムと関連する EU の法令としては、例えば、自動的な道路交通管制及び国境管理並びにそれに依拠する各種応用サービスのために用いられる ITS システム(182) に関する指令 2010/40/EU がある(183) 。移動体である自動車の登録番号の識別処理と関連する法令としては、前掲理事会決定 2008/616/JHA がある。

3．3．3　空間情報のデータセット

空間情報（spatial Information）とは、ある特定の点としての情報を示すデータではなく、あるまとまった空間を示す諸要素（factor）の集合体であるデータセットを意味する。このデータセットは、プロファイルの一種として理解することもできるが、ある個体としての自然人または物体を識別するためのプロファイルではなく、その空間の中に自然人または物体を含むと否とを問わず、ある想定された空間を特定して識別するためのプロファイルであるという点が個人識別のためのプロファイルとは異なっている(184) 。

ある自然人または物体が移動体である場合、または、ある対象の構成要素または属性が時間的に変化もしくは遷移する性質をもつような場合、空間データとしての把握が有用性を発揮し得る場合が多いことから、その重要性が着目されている。そのため、世界各国においてその研究開発が進められている。ところが、データセットの互換性（compatibility）または相互運用性（interoperability）が確保されない場合、とりわけ、グローバルな環境では、収集された空間データの活用及び応用に自ずと限界が生ずる。

EU においては、そのような限界が域内市場の稼働に悪影響を与え、EU の国際競争力の増強の阻害要因となるという考えに基づき、空間情報のデータセットの標準を定める法令として INSPIRE 指令 2007/2/EC(185) が採択され、空間情報のデータセットの基本的な部分における互換性の確保が試みられている。EU の今後に関する予測としては、今後の空間情報の利用状況の推移を見守りつつ、かつ、関連技術の発展を待って、より詳密かつ多様な応用に耐える改正指令または改正規則が制定されることになるであろう(186) 。

3．4　アクセス制御

一般に、情報またはデータは、それが存在しているというだけでは社会的な意味

をもたない。このことは、過去の遺跡の遺物が客観的・物理的に存在していても、それが地中から発掘され、解析された後でなければ社会的な意味をもたないのと全く同じことである(187)。

他方において、一般に、ある情報またはデータに対するアクセスは、様々な方法により管理（control）され得る。しかし、そのアクセス管理のために制御手法は、2つの類型に大別して理解することが可能である(188)。

一方のアクセス制御手法は、ある対象へのアクセスを原則として禁止とした上で、一定の資格・許可・承認に基づき、特定の者だけにアクセスを認める手法である。一般に、情報アクセス権の問題として扱われている事柄の多くは、このような手法による管理が行われていることを前提としている。国、国の機関または地方自治体が保有する機密情報は、原則としてアクセス禁止とされた上で、一定の手続に従い、その情報の開示請求によるアクセス可能とされる。日本国の法制の下においては、国、国の機関または地方自治体等が保有する公文書の情報公開請求がそれに該当する。また、機密文書としての指定のある公文書の機密性の維持・管理は、この手法によることを前提とした上で、その機密性の程度に対応した開示の要件の段階的な管理の問題として理解することができる。民間部門における機密文書の管理の大部分は、企業における資産管理及び営業秘密の管理の問題の中に吸収されるであろう。

他方のアクセス制御手法は、ある対象へのアクセスを原則として無制約とした上で、一定の要件を満たす場合には禁止とする手法である。一般に、オープンデータの問題として扱われている事柄の多くは、このような手法による自由アクセスが事前承認され、実装されていることを前提としている。オープンデータは、アクセスの自由を保障するのみであるので、著作権法上の問題を含め、その権利関係については別の問題として考察しなければならない。著作権による保護のある作品及び実演等を内容とするオープンデータの二次利用（reuse）の問題の多くは、この範疇に含まれ得る。

これらのアクセス制御は、当該アクセスされる対象が誰かによって現実に管理されている場合、または、法的な意味において管理されるべきものである場合においてのみ、意味をもつ(189)。

3．4．1　情報アクセス権

EU においては、オープンデータとして公開される情報以外の情報を含む公文書は、欧州連合機密情報（EUCI）の区分に従って機密指定された場合を除き、アクセスを求めるための一般的な法令の適用を受ける。EU の機関が保有する公文書へのアクセスに適用される法令としては、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[190] があり、また、構成国の機関が保有する公文書へのアクセスに適用される法令としては、指令 2013/37/EU による改正後の指令 2003/98/EC がある[191]。

これらの法令に対応する日本国の法令は、行政機関の保有する情報の公開に関する法律（平成 11 年法律第 42 号）及び各地方自治体の情報公開条例である[192]。

3．4．2　オープンデータ

EU のオープンデータ政策、とりわけ、その二次利用に適用される規律に関し、EU の機関に適用される法令としては、前掲委員会決定 2011/833/EU があり、また、構成国に適用される法令としては、前掲指令 2013/37/EU による改正後の指令 2003/98/EC がある。これらのオープンデータ政策の国際経済的・国際政治的な背景となっている欧州の文化振興政策及び情報財産業政策ないし財政支援政策を示すものとしては、規則 (EU) No 1295/2013[193] がある。欧州連合機密情報（EUCI）の区分に従って機密指定された情報については、これをオープンデータとすることを得ない。

EU のオープンデータ政策を実現するためのポータルサイトの理念について、法へのアクセス報告書[194] の第 68 項は、「EU オープンデータポータル（http://open-data.europa.eu）の目標は、EU の機関、部局及びその他の組織のオープンデータの収集及び配布である。別の計画では、EU の構成国の地域ポータル、地方ポータル及び国内ポータルからのオープンデータをまとめて配布するオープンデータの汎欧州ポータルの構築を目標としている」と述べている。

日本国政府の関連文書としては、電子行政オープンデータ戦略（平成 24 年 7 月 4 日高度情報通信ネットワーク社会推進戦略本部決定）及びオープンデータ基本指針（平成 29 年 5 月 30 日 IT 本部・官民データ活用推進戦略会議決定）がある。

3．4．3　機密情報

EU は、国家主権をもつ構成国によって構成されている。国家機密の取扱いは、

当該構成国の国家主権と直接の関係をもつものである。一定の情報の機密性が確保されなければ国家としての主権を維持する上で深刻な悪影響を発生させ得る場合があり、最悪の場合には他国により侵略され、国家としての自律性が消滅してしまうことが十分にあり得る。各構成国の国家機密は、当該構成国の法令に従って規律される。これに対し、EUの機関及び組織が取扱う機密情報に関しては、EU法として定めるところに服する。この機関の中にはEUの司法裁判所及び一般裁判所（旧第1審判裁判所）も含まれる。これらの公的部門における機密情報のアクセス制御については、「知る必要の原則（need-to-know principle）」に従った区分が設けられている。

EU議会において取り扱われる機密情報に関しては、2011年6月6日の決定2011/C 190/02(195)及び決定2014/C 96/01(196)がある。これらの法令は、2010年10月20日の枠組み協定(197)及び一般的な外交及び安全保障分野における事項以外の事項に関する理事会によって保有される情報の欧州議会に対する送付及び欧州議会による取扱いに関する欧州議会と理事会との間の2014年3月12日の機関間合意2014/C 95/01(198)に基づくものである(199)。同機関間合意の第2条は、機密情報のアクセス制御の区分に関し、欧州連合機密情報（EU classified information (EUCI)）の区分に準拠して行われることを定めている。その区分の内容は、以下のとおりであり、この区分に従って指定された情報には、その区分に指定されていることを示すマーキングを施さなければならない。EUCIに基づく取扱いの詳細は、2011年3月31日の理事会決定2011/292/EU(200)を改正するものとして採択された2013年9月23日の理事会決定2013/488/EUに従う。

EU取扱注意（RESTREINT UE/EU RESTRICTED）
EU秘（CONFIDENTIEL UE/EU CONFIDENTIAL）
EU極秘（SECRET UE/EU SECRET）
EU機密（TRÈS SECRET UE/EU TOP SECRET）

EUの司法裁判所において文書提出命令等により当事者に開示される機密文書の取扱いに関しては、一般裁判所決定(EU) 2016/2387(201)がある。同決定に基づく機密情報のアクセス制御は、欧州連合機密情報（EUCI）の区分に準拠している。

EU の民間部門における多種多様な機密情報の中で企業等が保有する非開示情報及びノウハウの保護に関しては、営業秘密指令(EU) 2016/943 がある(202)。

日本国の公的機関における機密情報と関連する法令としては、特定秘密の保護に関する法律（平成 25 年法律第 108 号）があるほか、国際協定として、秘密軍事情報の保護のための秘密保持の措置に関する日本国政府とアメリカ合衆国政府との間の協定（2007 年 8 月 10 日）がある。機密情報の区分は、原則として、これらの法令及び協定並びにそれらの実施細則に従う。特定秘密の保護に関する法律第 1 条は、「この法律は、国際情勢の複雑化に伴い我が国及び国民の安全の確保に係る情報の重要性が増大するとともに、高度情報通信ネットワーク社会の発展に伴いその漏えいの危険性が懸念される中で、我が国の安全保障（国の存立に関わる外部からの侵略等に対して国家及び国民の安全を保障することをいう。以下同じ。）に関する情報のうち特に秘匿することが必要であるものについて、これを適確に保護する体制を確立した上で収集し、整理し、及び活用することが重要であることに鑑み、当該情報の保護に関し、特定秘密の指定及び取扱者の制限その他の必要な事項を定めることにより、その漏えいの防止を図り、もって我が国及び国民の安全の確保に資することを目的とする」と定めている。同条に示す内容が日本国における国家機密保護の基本原則である。

3．4．4　通信の秘密

通信の秘密（Confidentiality of Communication）は、一般に、通信媒介者が処理・保有する通信データへのアクセス制御とかかわる概念である。通信媒介者は、国または国の機関であることもあるし、電気通信事業者等の民間企業であることもあり得る。一般に、通信の秘密の内容は、大別すると、①国家機密、②企業秘密等のような民間組織等の秘密及び③私人の秘密の 3 種に分けて考えることができる。

ところが、情報社会の安全性確保に関して 5 で後述するところと同様に、通信媒介者等は、インターネット上のパケット通信（TCP/IP）の場合、パケットそれ自体の属性を事前に区分して媒介処理できないので、そのパケットが暗号化されたものであると否とを問わず、通信の秘密に関する規範は、全てのパケットの媒介処理に対して一律に適用されなければならない。電気通信における通信の秘密の確保において、正当事由（適法化事由）が存在する場合の例外処理という非常に困難な問題が発生する根源は、そのことにある。

通信の秘密に関して、EUの現行のeプライバシー指令2002/58/EC第5条第1項は、「構成国は、国内立法を通じて、公衆通信ネットワーク及び公衆が利用可能な電子通信サービスによる通信の秘密及び関連トラフィックデータの秘密を確保する。とりわけ、構成国は、第15条第1項に従い、そのようにすることが法的に認められる場合を除き、関係する利用者の同意なく、利用者以外の者によって行われる通信及び関連トラフィックデータの聴取、盗聴、記録保存、または、それ以外の傍受行為または監視行為を禁止する。本項は、秘密の原則を妨げることなく、通信の運搬のために必要な技術上の記録保存を妨げない」と定めている(203)。同指令の改正案COM/2017/010 final（2017/03 (COD)）の前文は、通信の秘密の保護の重要性を更に強調する内容のものとなっている。また、条項としても、同改正案第5条は、「電子通信データは、秘密のものである。この規則によって許容される場合を除き、聴取、タッピング、記録保存、モニタリング、スキャニング、または、それ以外の種類の電子通信データの傍受、サーベイランスもしくは処理のような、電子通信データに対する干渉は、禁止される」と定め、通信の秘密保護の趣旨を徹底している(204)。

3．5　個人データの保護

個人の識別及び識別子（特に生態要素の処理）に関して述べた部分（3.3.1）で示したような個人識別に用いられる要素という意味での「個人データ」の保護に関する規律は、およそそのような要素としての個人データの処理と関連するものである限り、原則として、EUの法令において横断的に適用される共通かつ横断的な制度的プロトコルの一部を構成するものであると考えられる。欧州委員会通知COM/2017/07 finalによって明確に示されているように、個人データの保護は、EUの域内経済の活性化及び国際競争力の強化という経済戦略における重要な戦術の一部でもあるので、その意味においても、EUの法制全体において横断的なプロトコルとして機能すべき必要性が高い(205)。

とりわけ、自然人の生体要素は、一般に、機微のデータ（sensitive data）として分類され、そのデータが不用意に使用され、または、濫用されることによる自然人のプライバシーに対する悪影響の重大性から、特に慎重な取り扱いが求められる(206)。

例えば、GDPR の第 9 条は、機微のデータを特別類型の個人データとし、同条第 1 項において、「人種的もしくは民族的な出自、政治的な意見、宗教上もしくは思想上の信条、または、労働組合への加入を明らかにする個人データの処理、並びに、遺伝子データ、自然人をユニークに識別することを目的とする生体データ、健康に関するデータ、または、自然人の性生活もしくは性的嗜好に関するデータの処理は、禁止される」と定めている。そして、同条第 2 項は、法令により同意による処理が禁止されている場合を除き、データ主体の同意がある場合、労働及び社会保障並びに社会保護の法律の分野において法令により認められている場合、関連法令に従い労働法上の団体協約によって合意が締結されている場合、データ主体の生存の利益の保護のためのやむを得ない事情が存在する場合、データ主体自身によって明白に公開のものとされるデータの場合、公衆衛生(207) の場合のような重要な公共の利益の目的のために処理が必要となる場合、予防医学、産業医学または社会福祉等の目的のために必要となる場合、医療上の必要性がある場合、または、公共の利益におけるアーカイブの目的、科学調査もしくは歴史調査の目的または統計の目的のために処理が必要となる場合等における処理について、同条第 1 項の例外を定めている。

これらの条項は、情報社会の法における横断的なプロトコル層の一部を構成する機微のデータの処理に関する一般的な規律の主要な内容を構成するものである(208) 。

以上のような意味における個人データの保護に関する規律の適用の実際の態様は、個人データ保護指令 95/46/EC 及び GDPR が示す基本原則を適用するという点では一致している。ただし、個々の法令に存在する現実の条文には何らかの修正が加えられているのが普通である。それは、それぞれの法令が適用される部門の特殊性を反映する修正として理解することができ、その意味において、それらの法令中のデータ保護条項は、特別法としての位置づけをもつ。そのような特別法としての修正がデータ保護指令 95/46/EC または GDPR の定める基本原則に反するものである場合、欧州司法裁判所によって無効の宣言が行われることがあり得る(209) 。

既に述べたものを除き、以下、EU の法制度上のプロトコル部分としての個人データ保護の規律の例について、幾つかの具体的な関連法令をあげる。ただし、網羅的ではない(210) 。

(1) EUの域内国境及び対外国境並びにシェンゲン圏の国境の管理

前述のEurosur[211]に適用されるEurosur規則(EU)No 1052/2013の第13条第1項は、個人データを処理するために国内状況映像表示機能を使用する場合、指令95/46/EC、枠組み決定2008/977/JHA[212]及びデータ保護に関する国内法上の条項に服する旨を定めている。

対外国境管理において使用される指紋データ、掌紋データ、顔画像データ、DNAプロファイル及び自動車登録番号の取扱いに関する理事会決定2008/615/JHA第24条ないし第32条は、指令95/46/ECに定める基本原則を踏まえ、個人データの保護に関する詳細な手続条項を定めている[213]。

Visa情報システム（VIS）[214]を用いた指紋データ等の照会に適用される理事会決定2008/633/JHA[215]第8条第1項は、個人データの自動的な処理と関連する個人の保護のための1981年1月28日の欧州評議会条約（ETS No 108）及びその追加議定書（ETS No 181）[216]並びに警察部門における個人データの利用を規律する欧州評議会閣僚委員会の1987年9月17日の勧告No R (87) 15[217]を考慮に入れるべきことを定めている。EUの構成国だけに適用のある個人データ保護指令95/46/ECではなく欧州評議会条約が参照されているのは、シェンゲン圏の範囲がEU構成国の範囲及びEFTA諸国の範囲とは異なることやEU加盟国であっても欧州評議会の条約加盟国には適用され得る規律によるべきものとの考慮に基づくものと考えられる。また、2008/633/JHA第14条は、VIS情報システムで処理される個人データの保護に関し、個人データ保護指令95/46/ECと同様の内容のデータ主体の権利について定めている。

国境管理の際に使用されるパスポート内のICチップに記録される顔画像データ及び指紋データに関し、ICAOのガイドラインを遵守する規律を定める理事会規則(EC) No 2252/2004[218]の第4条第1項は、個人データの保護に関するEUの適用がある旨を定めた上で、同条第3項は、当該文書の真正性の確認の目的及びその所持者の同一性の確認の目的のためにのみ、ICチップ内に記録された生体認証機能が参照され得ることを定めている。

国境管理に伴う税関業務の過程における税関情報システム（CIS）による個人データ処理には、理事会決定2009/917/JHAが適用される（前述の2.1.3参照）。同理事会決定の第3条ないし第30条は、個人データの保護に関し、詳細に定めている。

(2) 行政情報の共有（IMI）

域内情報システム（IMI）では一般的な行政情報の交換が行われる。IMI 規則 (EU) No 1024/2012[219] の第 13 条ないし第 21 条は、個人データの保護に関して定めており、特に同規則第 13 条は、「IMI 関係者は、別紙に列挙する欧州連合の法令の関連条項に定める目的のためにのみ、個人データを交換し、処理する」と定め、目的を限定している。ただし、同規則の別紙に定める目的は、数次にわたる改正により、増加を続けている（前述の 2.1.1 参照）。

(3) Europol、Eurojust 及び OLAF

EU の警察活動における個人データ処理には Europol 規則 (EU) 2016/794[220] が適用される[221]。同規則第 18 条第 1 項第 2 項は、情報処理活動の目的における個人データ処理の目的を限定している。Europol と Eurojust 及び OLAF との情報交換に関しては、同規則の第 21 条が定め、第三国等への個人データに関しては、第 24 条ないし第 28 条が定め、個人データ保護の詳細に関しては、第 29 条ないし第 50 条が定めている。

EU の刑事法務活動に関しては、Eurojust が所管するほか、2017 年 10 月 12 日の理事会規則 (EU) 2017/1939（OJ L 283, 31.10.2017, p.1-71）により設置された欧州検察局（European Public Prosecutors' Office (EPPO)）も所管する[222]。Eurojust における個人データ処理に関しては、理事会決定 2009/426/JHA（OJ L 138, 4.6.2009, p.14-32）による改正後の理事会決定 2002/187/JHA （OJ L 63, 6.3.2002, p.1-13）[223] が適用される。EPPO における個人データ処理に関しては、第 47 条ないし第 89 条が詳細に定めている。その詳細は省略する。

EU の財政を侵害する詐欺、横領及び背任行為等に関しては、OLAF が所管する。OLAF における個人データ処理に関しては、OLAF 規則 (EU, Euratom) No 883/2013（OJ L 248, 18.9.2013, p.1-22）が適用される。その詳細は省略する[224]。

(4) 著作権

情報社会指令 2001/29/EC の前文 (15) は、「この指令に基づく個人データの処理は、憲章の第 7 条及び第 8 条に基づく私的な生活及び家族の生活を尊重する権利並びに個人データの保護の権利を含め、基本的な権利を尊重するものであることが重要であり、また、そのような処理が、欧州議会及び理事会の指令 95/46/EC 及び指

令2002/58/ECを遵守することも重要なことである」と述べている。そして、視覚障害等のある者に対する権利保障を定めるマラケシュ条約を実装する指令(EU) 2017/1564[225]の第5条及び第7条は、視聴覚障害のある者（受益者）に対してそのような者が利用可能なフォーマットによるコンテンツを作成・頒布する認可団体が個人データの保護と関連するEUの法令を完全に遵守すべき旨を定めている。

4　情報社会のアプリケーション層を構成する法令

4．1　知的財産権

情報社会において、特許権、意匠権及び商標権と関連するものは極めて多い[226]。デジタルコンテンツに関しては、EUの著作権関連法令の該当する条項が適用される。データベースの保護に関しては、データベース指令96/9/EC（OJ L 77, 27.3.1996, p.20-28）があり、同指令の第7条ないし第11条は、「*sui generis* の権利」について定めている。

4．1．1　著作権

情報社会において、コンピュータシステム及びコンピュータソフトウェアは、不可欠の存在である。情報社会におけるデジタルコンテンツの規律に関する基本法令は、情報社会指令2001/29/ECである（前述の1及び3.3参照）。そして、EUにおいて、コンピュータソフトウェアの著作権による保護は、指令2009/24/EC[227]によって規律される。

視聴覚メディアの産業育成上の基本戦略は、創造性のある欧州プログラム（Creative Europe Programme (2014 to 2020)）を定める規則(EU) No 1295/2013によって定められている（前述の3.4.2参照）。また、視聴覚メディアの範疇に属するコンテンツを提供または媒介するプロバイダに関しては、視聴覚メディアサービス指令2010/13/EU（OJ L 95, 15.4.2010, p.1-24）が適用される。視聴覚メディアのレンタル権、貸与権及び公共貸出権（いわゆる「公貸権」）に関しては、指令2006/115/EC（OJ L 376, 27.12.2006, p.28-35）[228]により、また、視聴覚メディアの内容を構成する実演を行う実演家の権利の保護機関に関しては、指令

2006/116/EC（OJ L 372, 27.12.2006, p.12-18）(229) により、それぞれ強化が行われている。他方で、指令 2012/28/EU（OJ L 299, 27.10.2012, p.5-12）(230) により、作者不明作品（いわゆる「orphan works」）の法的取扱いが明確化されている。これらの法令は、ベルヌ条約、ローマ条約及び WIPO 条約に準拠するものではあるが、EU 法としての若干の修正が加えられている。

なお、著作権または関連権を侵害する行為の刑事処罰に関しては、検討すべき課題が非常に多い。とりわけ、EU の構成国を含め、諸国の刑事訴訟制度の相違との相関関係に基づいて処罰の実質を検討する必要があり、実体法上の法定刑だけを単純に比較することには危険が伴う。このような問題に関しては、今後、更に研究が深められるべきである(231)。

4．1．2　ソフトウェア特許

コンピュータソフトウェアの著作権による保護に関する指令 2009/24/EC の第 8 条は、特許による保護を妨げないと規定しており、また、情報社会指令 2001/29/EC 第 9 条にも同旨の規定がある。これらの条項は、特許による保護が成立可能な場合を前提とするものである。ところが、コンピュータソフトウェアの特許に関す指令案 COM/2002/0092 final が否決されているため、少なくとも EU 法のレベルでは、ソフトウェア特許に関する直接の根拠法令が存在しないことになる。

4．2　違法な表現行為

表現の自由は、無条件のものではない。他者の重要な法益または社会の基本的な秩序を侵害しない範囲内において、法によって妨げられることがないという意味での自由であり、かつ、本来自由であるべき行為が妨げられた場合において損害賠償や差止請求を含む何らかの法的救済を受けることができるという意味における自由である。

特に、他の者の重要な法益を積極的に侵害する意図による表現行為、または、合理的なものとして承認されている社会秩序を積極的に破壊する意図による表現行為は、その態様・程度・影響力等により、違法な表現行為として評価されることがあり得る(232)。

この場合において、違法と適法を分ける閾値となる評価基準が常に議論の的となってきた。しかしながら、国際的な合意である条約・協定等によってその判断基

準が示されている場合、それが当該国際合意の締約国においても法規範として機能することは明らかであり、それが当該締約国における違法な表現行為の判断基準の1つとして機能することになる。

EUにおいては、オンラインの違法な表現行為の規制に関する包括的かつ大規模な法改正が検討されている(233)。

4．2．1　ヘイトスピーチ

ヘイトスピーチの場合を含め、ヘイト犯罪（hate crime）の被害者の保護に関連するEUの法令として指令2012/29/EU（OJ L 315, 14.11.2012, p.57-73）がある。ヘイトスピーチそれ自体を直接の規制対象とするような法令としては、2008年11月28日の理事会枠組み決定2008/913/JHA（OJ L 328, 6.12.2008, p.55-58）がある。

欧州評議会の2003年1月28日のサイバー犯罪条約追加議定書（ETS No.189）は、コンピュータシステムを介して行われる人種差別行為及び外国人排除主義的行為並びにそれらの行為の扇動、媒介、教唆及び幇助等の関連行為を犯罪として処罰すべきことを定めている。これらの行為の処罰は、当然のことながら、表現行為の内容規制を含むものである。換言すると、これらの行為は、表現の自由の範囲内に含まれない。EUにおいては、理事会枠組み決定2008/913/JHA（OJ L 328, 6.12.2008, p.55-58）により、これらの行為が犯罪行為とされている(234)。

4．2．2　児童ポルノ

サイバー犯罪条約(235)の第9条は、児童ポルノであるコンテンツ及びコンピュータシステムを介する児童ポルノの頒布行為等を処罰すべき旨を定めている。サイバー犯罪条約に定める一般的なサイバー犯罪行為の禁止及び処罰は、指令2013/40/EU（OJ L 218, 14.8.2013, p.8-14）(236)によって実装されているが、児童ポルノの禁止及び処罰に関しては、指令2011/92/EU（OJ L 335, 17.12.2011, p.1-14）によって実装されている。同指令は、理事会枠組み決定2004/68/JHA（OJ L 13, 20.1.2004, p.44-48）の改正法令である。同指令により、同枠組み決定は、廃止され、同枠組み決定を参照する法令中の条項は、同指令を参照するものとして読み替えられる。

なお、視聴覚メディアサービス指令2010/13/EUの前文(61)は、「構成国の裁判管轄権の下にあるメディアサービスプロバイダは、いかなる場合においても、児

童の性的搾取及び児童ポルノとの闘いに関する 2003 年 12 月 22 日の理事会枠組み決定 2004/68/JHA に従い、児童ポルノの配布に関する禁止に服さなければならない」と述べている。

4．2．3　テロ行為の扇動

欧州評議会の 2005 年 5 月 16 日のテロリズムの防止に関する欧州評議会条約（ETS No.196）及び同条約の 2015 年 10 月 22 日の追加議定書（ETS No.217）は、テロリスト行為等の侵害行為に関する国際的な協力、並びに、テロリズム被害者の保護、弁償及び支援のために、テロリスト及びテロリストと関連する行為を犯罪として処罰することを定めている。

枠組み決定 2002/475/JHA[237] を全面改正する指令（EU)2017/541（OJ L 88, 31.3.2017, p.6-21）[238] は、「テロリストの脅威は、成長し、近年、急速に進化した。『外国人テロリスト戦闘員』と呼ばれる個人がテロリズムの目的のために海外渡航する。帰国する外国人テロリスト戦闘員は、全ての構成国にとって、高度の治安上の脅威を示す。外国人テロリスト戦闘員は、近時の幾つかの構成国内における攻撃及び陰謀と関連してきた。加えて、欧州連合及び構成国は、欧州内に留まりながら、海外のテロリストグループから刺激を受け、または、指示を受ける個人からの脅威の増大と直面している」（前文(4)）との認識に基づき[239]、第 3 条においてテロリスト行為を、第 4 条においてテロリストグループと関連する侵害行為を定義した上で、第 5 条において、「構成国は、第 3 条第 1 項の(a)ないし(i)に列挙する侵害行為のいずれかの実行を扇動する意図で、オンラインまたはオフラインの別を問わず、公衆に対してメッセージを配布し、または、それ以外の何らかの手段によってそのメッセージを利用可能にする行為について、テロリストの行為の美化による場合のように、直接または間接に、テロリスト行為の実行を奨めるような行為によって、1 または複数のそのような侵害行為が実行され得る危険性を生じさせる場合、その行為が意図的に実行されたときは、犯罪行為として処罰され得ることを確保するために必要となる措置を講ずる」と定め、第 6 条において、「構成国は、第三者に対し、第 3 条第 1 項の(a)ないし(i)または第 4 条に列挙する侵害行為のいずれかを実行すること、または、その侵害行為に寄与することを勧誘する行為について、その行為が意図的に実行されたときは、犯罪行為として処罰され得ることを確保するために必要となる措置を講ずる」と定めている。なお、テロリスト行

為に関するEuropol、Eurojust及び構成国間の情報交換に関して適用される理事会決定2005/671/JHA（OJ L 253, 29.9.2005, p.22-24）は、指令(EU)2017/541によって一部改正(240)され、交換可能な情報の適用範囲が拡大された。

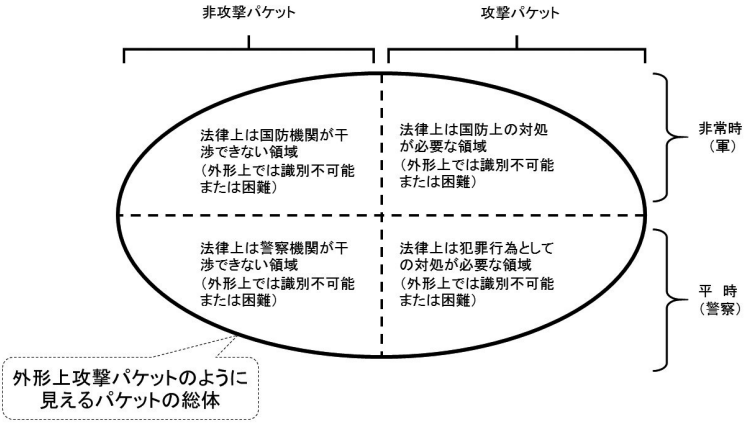
以上から、EUにおいては、テロリスト活動を構成する表現行為及びそれと関連する表現行為は、違法な表現行為であり、表現の自由の範囲内に含まれないことになる。その結果、違法なコンテンツの媒介者としてのプロバイダの責任及びその免除が問題となり得ることとなった。視聴覚メディアサービス指令2010/13/EUについても、テロ行為を扇動する表現行為等の規制と関連する条項を織りこむための法改正が検討されている(241)。

5　情報社会の安全性確保

情報社会における最大の脅威は、サイバー攻撃である。特に、IoTが普及しつつある現在、サイバー攻撃による被害は、社会全体の機能不全または経済的なインフラの破壊を招来し得るものとなっている。それゆえ、情報社会の安全性確保においても、サイバー攻撃への対応が不可欠の重要な課題となる。一般に情報セキュリティと呼ばれる分野がそれである。EUにおける関連法令としては、NIS指令(EU) 2016/1148(242)が最も重要な法令であると考えられる。日本国においては、サイバーセキュリティ基本法（平成26年法律第104号）及び同法に基づく関連法令による対応が実施されている。

ところが、サイバー空間における攻撃に用いられる攻撃用パケットを識別しようとすると、非常に厄介な問題と直面することになる。一般に、個別的なサイバー犯罪のための攻撃パケットと軍事目的によるサイバー戦のための攻撃パケットとを外見から識別することはできない（下図参照）(243)。

これらのパケットは、主観的な目的ないし意図が異なるだけで、それ以外の点では通常のパケットと全く異ならない。犯罪目的の攻撃パケットと軍事目的の攻撃パケットの場合においても、それらの攻撃が同一の種類に属するマルウェアや破壊用パケット等を現実の攻撃手段として用いている場合には、その使用の意図・目的という主観的要素が異なるだけで、攻撃パケットそれ自体としては全く同一であ



る。そして、その主観的意図それ自体は、パケットそれ自体の中で表現されることはなく、常にネットワークシステムやコンピュータシステムの外に存在している(244)。それゆえ、パケットそれ自体からは、そのパケットを使用する主観的意図を知ることができない。しかも、現実には、それらの様々な主観的意図をもった膨大な量の攻撃パケットと非攻撃パケットとが日常的に常に混在して存在している。それゆえ、現代社会は、戦時と平時が常に共存する状況に下にある(245)。

以上のような本質的な問題はあるが、EU 含め、世界各国の法制は、これらの本質的な問題への対処の段階にまでは至っていない。おそらく、この文脈における世界各国の立法者の基本的な認識・理解・知識が決定的に欠落してしまっているからではないかと想像される。

EU の法制に限定すると、例えば、現時点における対応としては、情報社会において戦時と平時が常に共存する状況が実在するという事実を明確に承認した上で、サイバーセキュリティ通知 JOIN(2017) 450 final、ハイブリッドな脅威報告書 JOIN (2017) 30、第 11 次進捗状況報告書 COM/2017/0608 final 及び EU Cybersecurity Agency としての ENISA の機能拡大に関する規則案 COM/2017/0477 final 及びサイバーセキュリティに関する報告書 JOIN(2017) 450 に示されているように、EU 及び構成国の警察機関と NATO 並びに ENISA との密接な連携によるサイバー攻撃に対する回復力の構築・増強及び効果的なサイバー防衛を基軸とする総合的な

対処（新たなサイバーセキュリティの枠組み）が立案され、EU全域におけるサイバーセキュリティ総合演習によって試され、関連各機関との交渉及び関連機関の設置を経て(246)、現実に実装される段階に到達していること、資金決済関連法令の改正により、銀行口座データを把握し、資金移動をより迅速・的確に把握するための努力が重ねられていること、テロリストの移動情報を確保するためにPNR情報の収集が強化されていることなどに留意しなければならない(247)。

いずれにしても、EUの現状及び近未来における組織構造上では、ENISAを中心とするEU全体の情報セキュリティ構造（EUの安全保障体制）が構築され、対外的には、EU Intelligence and Situation Center（INTCEN）及びその中にあるEU Hybrid Fusion Cellと共にNATOとの連携、EU域内的には構成国との直接の連携のほか、Europolの SIENA等のシステムを介した関連情報の交換の促進を伴う連携が強化され、警察関係（域内の治安維持）では、EPPO、Europol、Eurojust及びOLAFの協力関係とそれぞれの分野において構成国の該当部門の行政機関の連携が強化されると共に、IMIを介した一般行政情報の交換、SIS II、VIS及びCIS等を介した国境管理情報の交換、並びに、PIU等を介したPNR情報の交換が促進され、交換されるデータの構造または質の点では、空間データや各種プロファイルデータのような構造性をもったデータセットの交換が増加し、解析システムの点では、人工知能技術の応用が更に拡大されるようになるものと推測される。そのような情報の情報源としては、特別の機器・装置類だけではなく、ITSのような公共目的の交通管理ネットワークや民間の一般的なIoTネットワークからの大量の情報が転用され、利用されるようになるのではないかと思われる。それらの中には、広場や街路等の公共空間において監視カメラによって捉えられる情報やEurosurによる広域の国境管理情報も含まれることになる可能性が高い。そして、これらのデータや情報の論理的な意味における一元管理の実現のための方策が検討されている(248)。

このような急激な変化に伴い、EU市民のプライバシー保護上の問題や表現の自由の問題等が生じ得ることが十分に予測される。個人データ保護に関し、EUの個人データ保護政策全体を統括するEDPS、あるいは、GDPRに基づいて第29条作業部会を改組して設置される欧州データ保護委員会がどの程度の力を発揮できるかも全く未知数である。

そもそも、一般論として、EU 法の分野においては、国際人道法関連や環境法関連等のごく一部の特殊な領域における個別具体的な特殊問題に関する研究を除き、ほとんど何も研究されてこなかったのも同然の厳しい状態にある。まして、EU 法全体にわたる全分野横断的な研究成果は存在しなかった。このことは、警察関連や安全保障関連だけではなく、電子商取引・電子認証・電子決済や知的財産権や労働法の領域でも民刑の訴訟法の領域でも同じである(249)。とりわけ、EU 及びその構成国における情報社会の法の領域にある多種多様な法律問題、そして、その日本国法との比較法的な検討は、日本の法学研究者にとって、これからの極めて重要な課題であろう。

これらのような分野において既に存在する研究成果の中には、実定法として現実に存在する法令の条項を全く踏まえず、理想化された EU のような想念のみに基づくものも全く皆無というわけではない。しかし、EU は、現実に生きる欲望に満ちた人々を統治するための政治組織の一種なのである。政治的イデオロギーや空想から演繹されるようなものではなく、実定法の正確な解釈論及び関連公文書の精密な読解を踏まえた地道な法学研究の蓄積が望まれる。

6 まとめ

法律論叢誌の所定の頁数制限の関係により、2 回連載の形式で分割することになったが、以上で大野幸夫先生の 70 年の時を祝賀する論文として献呈する本稿における論述を終える。

本稿においては、主として EU の法令及び公式文書を素材にとり、EU における情報社会の概念を基軸として、情報社会における法の諸要素を解析した結果に基づき、その論理的な構造及びその必須の構成要素の相互関係と相互作用を示すことができたと考える。

一般に、電子化された情報社会だけではなく、情報を正確かつ迅速に握ることは、国家統治のための必須の要件の 1 つである(250)。それゆえ、中国においても日本においても、古代から、駅伝制(251)や飛脚・早馬のようなものを含め、様々な情報収集手段及び通信手段の構築が国家的に進められた。このような国家的な

仕組みは、かなり大きな額の国家予算を投入して管理・運営されるものであり、そのことによって寄食して生活する大量の人々が安定的に存在することを必須の前提とするものであることから、当該国家体制の崩壊と共に必然的に滅び去る運命にある。現に、律令時代の国道の大半は、地下に埋もれてしまい、その断片が時折発掘されて世間の注目を集めるまでは誰も知らない存在となってしまっている。現代の情報社会も基本的には同じ構造をしており、例えば、ウクライナにおいて発生した執拗なサイバー攻撃による大規模電源喪失の事態によって、同国の電力部門及び情報通信部門だけではなく国家機能そのものや産業界の全体が大規模な打撃を受けた事例をみれば容易に推論できるように、情報インフラの機能喪失は、国家及び社会組織の喪失と均等な結果を招来し得る。比喩的に言えば、肉体は存在していても神経系が全て機能しなくなることにより、統合体としての肉体が機能を喪失するような事態が生じ得るのである。

また、いわゆる情報財(252)のように、デジタルな存在であることを本質とする財は、全て機能しなくなる。このことは、いわゆる仮想通貨を含め、電子的な決済手段でも全て同じであるので、仮に世界規模で情報通信が機能不全になると、地球上のほぼ全ての資産が瞬時にして消滅したのと同じ結果をもたらすことになるであろう。電子的な決済機能が機能喪失すると、仮にそれがいかに巨額なものであるとしても、電子的な資産保有額を示す電子記録は、現在及び将来の交換価値を実現する手段を喪失することになるので、全て単なる電磁的記録に過ぎないものと化し、社会的・経済的には全く無意味なものとなってしまうのである(253)。

そのような深刻な状況下においては、無論、投資市場を含め、デジタル市場、デジタル経済ないし情報経済が全く成立しなくなる。実体経済を無視するものである限り、情報社会は、そのように極めて脆いものである。それゆえに、EUは、ENISAの機能拡大、EUとNATOとの情報戦の分野における協力関係の構築の動きを含め、急ピッチで、サイバー防衛戦略の構築・実装・運用を進めるのと同時に、EUのNIS指令等に見られるような官民の協力体制の構築の努力、を重ねているのである(254)。

一般に、統治組織・経済組織としてのEU及びその拡大・統合は、それ自体として、良い意味でも悪い意味でも、「巨大な実験」であると比喩的に評価・表現されることが多い。そのような評価は、正鵠を得た部分をもつと考えられる。しかし、

それは、単なる実験なのではなく、その実験に含まれる個々の施策の結果が有効性・有用性を示すものである限り、確実に EU の実質・実体へと変容を遂げるものであり、その意味において、人類社会全体の将来を推理・想定する上で、貴重な研究素材を提供するものであると言える。

それゆえ、EU における情報社会の法に関する調査・検討・考察は、公法・私法の分別の枠を超えて、全ての法解釈論において必須の思考過程を形成するものとなると考えられる。

本稿においては、電子的な司法救済や自動自力救済等を含め、本来であれば触れるべき重要な事項の多くについて、その言及・論述を割愛せざるを得なかった。これらの事項に関しては、別の機会に改めて論ずることとしたい。加えて、本稿の執筆に際して参考にした文献等の大多数について、頁数制限の関係からそれを明示することを断念した。全ての参考文献を列挙しようとすると、それだけで約 50 頁を要する。これらの参考文献は、本稿の脚注内に示す法と情報雑誌掲載の参考訳冒頭部分に列挙してある。訳語については、法と情報雑誌上で公表している参考訳におけるのと同様、原則として直訳とし、現在の日本国の関連法学分野において通有している訳語と異なる場合があるとしても、あえて EU の法令の一貫性のある訳語を優先するという観点から継続してきた現時点における検討結果を反映するものである。そのため、今後の検討の推移によっては、将来、修正することとなる部分があり得る。情報社会のアプリケーション層を構成する法令に関する論述は、頁数制限の関係により用意した原稿のほぼ全部をカットし、極めて簡略な要旨的な記述のみとした。情報社会のアプリケーション並びにそれと関連する具体的な電子商取引及びプロバイダ責任の分野に属する法令を網羅的に丁寧に概説しようとすれば、この部分だけでかなりの頁数を要することとなるので、本稿においては割愛を甘受し、他日を期したいと思う。情報社会のインフラ層の根幹を規律する基本的な通信法制に関しては、現在 EU 議会及び理事会において審理中の情報通信法の大改正（European Electronic Communications Code の提案）(255) の結果を待って論ずるべきである(256)。

以上のとおりであり、明治大学法学部において長年にわたり情報法及びネット取引法の科目を担当された大野幸夫先生から受けた公私にわたる御恩に報いるべく、併せて、大野幸夫先生及び野村豊弘先生から「情報法の体系書を書くべきである」

とのかなり強い御示唆を受け続けながらそれに全く応ずることなく今日まで至ったことの真の理由の一部を暗に明かしてその弁解とすべく、極めて簡略・拙劣なものとはいえ、EUの情報社会の法の解釈法学上の意義を考察した結果を論文として献呈する機会を得たことに感謝しつつ、本稿における論述を閉じる。

以上(257)

注

(132) 従来の概念で言えば、制度的保障と類似する面をもつが、個々の具体的な制度を保障するのではなく、一定の手続または手順を保障する点において異なっている。米法をベースに考えると、手続的正義として表現することも可能である。手続的正義に関しては、夏井高人「手続的正義―情報社会における社会構造の変化と正義の維持―」法とコンピュータ23号49～51頁(2005)で述べた。

(133) 欧州連合基本権憲章(2012/C 326/02)の参考訳は、法と情報雑誌1巻2号1～33頁にある。

(134) なお、2016年5月19日の欧州委員会報告書COM(2016) 265 finalも参照。

(135) 権利として表現されている保護法益が侵害された場合、通常の民事訴訟等の方法による救済(損害賠償)を求めることができることは当然のこととして、権利それ自体の行使として何が実行可能であるかが明定されていないという趣旨である。このことは、日本国憲法においても基本的には同じである。権利それ自体の具体的な実行方法及びその態様は、一般に、権利根拠法令とは別の制定法及び法解釈(判例法)によって定められる。EUの個人データ保護法令における様々な権利が、保護法益であるプライバシーの利益を保護するための手段的・技術的・人工的な権利であることに関しては、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巻2・3号181～245頁(2016)で詳論したとおりである。

(136) eプライバシー指令2002/58/ECの第5条第1項は、通信の秘密について、「構成国は、国内立法を通じて、公衆通信ネットワーク及び公衆が利用可能な電子通信サービスによる通信の秘密及び関連トラフィックデータの秘密を確保する。とりわけ、構成国は、第15条第1項に従い、そのようにすることが法的に認められる場合を除き、関係する利用者の同意なく、利用者以外の者によって行われる通信及び関連トラフィックデータの聴取、盗聴、記録保存、または、それ以外の傍受行為または監視行為を禁止する。本項は、秘密の原則を妨げることなく、通信の運搬のために必要な技術上の記録保存を妨げない」と定めている。また、このeプライバシー指令2002/58/ECを改正する規則案(COM(2017) 10 final)の前文(1)は、「欧州連合基本権憲章(以下「憲章」という。)の第7条は、全ての者の、彼または彼女の私的な生活、家庭の生活、住居及び通信を尊重する基本的な権利を保護している。人の通信のプライバシーに対する尊重は、この権利の重要な側面の1つである。電子通信の秘密は、いつ、どこへ向けて、誰に対し、その通信が送信されたのかを含め、通信当事者間で交換される情報及びその通信の外部要素が通信に関与する当事者以外の者に対して暴露されないことを確保する。秘密の原則は、起呼(call)、インターネットアクセス、インスタントメッセージアプリケーション、電子メール、インターネット電話の通話及びソーシャルメディアを介して提供され

る個人メッセージを含め、現在及び将来の通信手段に対して適用されなければならない」と述べている。

(137) Joint Communication（JOIN(2017) 450 final）は、サイバー攻撃によってそのようなリスクが増大していることを認めている。

(138) 日本国の個人情報保護法（平成 15 年法律第 57 号）及び日本国憲法には相当する条項がない。

(139) 日本国の個人情報保護法第 3 条は、個人情報の適正な取り扱いを定めている。アクセスの権利に関しては、日本国の個人情報保護法第 28 条が相当し、訂正の権利に関しては、日本国の個人情報保護法第 29 条が相当する。しかし、日本国の個人情報保護法中には、事前の同意の要件を定める一般的な条項は存在しない。

(140) 日本国の個人情報保護法第 59 条ないし第 74 条に定める個人情報保護委員会が独立の監督機関に相当する。

(141) Judgment of the Court (Grand Chamber) of 6 October 2015, *Maximillian Schrems v Data Protection Commissioner*, Case C-362/14, ECLI:EU:C:2015:650

(142) 利益衡量に関しては、「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 頁で詳論したとおりである。

(143) Interinstitutional Agreement between the European Parliament, the Council of the European Union and the European Commission on Better Law-Making（OJ L 123, 12.5.2016, p.1-14）

(144) これらの基本原則は、憲章に定めるものではない。それは、自然人の権利ではなく、統治のための基本原則だからである。このことから、一般に、人権保障と関連する問題を考察する上では、個人を中心とする人権という側面だけに着目するのでは、ものごとの半分しか見ていないということを認識することができる。諸々の人権を支えるための統治組織に適用される基本原則の考察が残りの半分である。情報社会の法の構造を解析する上で、横断的なプロトコル層の存在も重視すべき法哲学的な根拠の 1 つは、ここにもある。

(145) 脚注 12 参照

(146) Paul Voigt & Axel von dem Bussche, The EU General Data Protection Regulation (GDPR): A Practical Guide, Springer (2017) p.37 は、この前文 (58) で示されている「透明性」の概念が特に重要なものであり、この記述に留意して法律文書等の作成が行われるべきことを指摘している。なお、透明性及び説明責任の確保は、後述のバイデザイン及びバイデフォルトの保護の原則の適用対象となるため、当該データ処理システムの設計の段階から、透明性及び説明責任の履行を現実に確保できるように検討され、それが実装されなければならない。

(147) Report on access to law（OJ C 97, 24.3.2015, p.2-10）。なお、法へのアクセス報告書の参考訳は、法と情報雑誌 2 巻 6 号 136～158 頁にある。

(148) 委員会決定 2011/833/EU の参考訳は、同誌同号 159～169 頁にある。

(149) 日本国の行政手続法（平成 5 年法律第 88 号）第 1 条第 1 項は、「この法律は、処分、行政指導及び届出に関する手続並びに命令等を定める手続に関し、共通する事項を定めることによって、行政運営における公正の確保と透明性（行政上の意思決定について、その内容及び過程が国民にとって明らかであることをいう。第 46 条において同じ。）の向上を図り、もって国民の権利利益の保護に資することを目的とする」と定めている。これが日本国の法令における「透明性」の定義条項である。また、同法 20 条第 4 項は、

聴聞期日における審理方法に関し、「主宰者は、聴聞の期日において必要があると認めるときは、当事者若しくは参加人に対し質問を発し、意見の陳述若しくは証拠書類等の提出を促し、又は行政庁の職員に対し説明を求めることができる」と定めている。同条同項は、「説明責任」に関する条項の一種として理解することもできる。

(150) 脚注40参照

(151) Europol規則(EU)2016/794の第33条は、バイデザインのデータ保護として、「Europolは、データ処理がこの規則を遵守し、かつ、関係するデータ主体の権利を保護するような方法で、適切な技術上及び組織上の措置並びに手続を実装する」と定めるのみである。

(152) GDPRの第25条第3項は、バイデザイン及びバイデフォルトによる保護を標準化するため、個別のリスク評価及びシステム設計等によるものではなく、標準化された手法によるリスク評価及びシステム設計を外部評価機関によって認証するという方法も導入している。

(153) 米国の民間企業がこの考え方を導入して実施している事例としては、例えば、Amazon Web Serviceの「Introduction to AWS Security by Design A Solution to Automate Security, Compliance, and Auditing in AWS, November 2015」をあげることができる。

(154) 第11次進捗状況報告書(COM/ 2017/0608 final)の参考訳は、法と情報雑誌2巻11号156～176頁にある。

(155) 欧州委員会に対してロボット及び人工知能と関連する法令制定の検討を求める欧州議会の決議Report with recommendations to the Commission on Civil Law Rules on Robotics(2015/2103 (INL))(A8-0005/2017)の中では、高度な人工知能技術の開発研究について、特別の登録制度を設け、その登録の管理と監視のためにEUの特別の機関を設けることが提案されている。これも制度設計における事前の防護策の導入という意味においてバイデザインの一種と理解することも可能ではないかと考えられる。この決議は、民間部門における産業ロボット(Robotics)の開発及び人工知能技術の応用を想定しており、軍事目的によるロボット(Robot)の開発に関係する部分は除外されている。なお、ロボット法の制定を求める欧州議会決議の参考訳は、法と情報雑誌2巻5号438～492頁にある。

(156) ハイブリッドな脅威報告書(JOIN (2017) 30)参照

(157) 立法活動それ自体以外の分野における社会の重要な事項に対する評価(assessment)及びその評価結果に基づく政策の修正や新たな施策の構築と関連する立法例としては、環境影響評価に関する指令2001/42/EC(OJ L 197, 21.7.2001, p.30-37)、指令2011/92/EU(OJ L 26, 28.1.2012, p.1-21)、指令2014/52/EU(OJ L 124, 25.4.2014, p.1-18)がある。特に、指令2001/42/ECは、環境影響評価条約の戦略的な環境評価に関する議定書(Strategic Environmental Assessment (SEA Protocol, Kyiv 2003))に基づく法令である。また、EUにおいては、様々な分野における評価及び評価基準またはそのための技術標準に関する多数の法令が存在する。これらの評価及びその手法に関する分野横断的な研究は、これからの重要な課題の1つである。そのような研究においては、特定の分野だけに限定したものとすることが許されず、膨大な法情報の合理的かつ効果的な分類・整理手段の構築を要すると同時に、比較分野的な研究手法が必須となる。

(158) TFEUが「法の支配」の原則を欧州の基本的価値観の1つとして定めていることから、EUの機関による行政権の行使も法の支配に服する。これを具体化する手法として欧州議会による立法行為があると解することが可能であるとすれば、欧州議会、理事会及び

欧州委員会は、一体としての EU の行政機関における機能分担を示すものであると理解することは可能な範囲内にある。EU においては、モンテスキュー流の古典的な意味における三権分立は、存在しないと考えるべきである。そこにあるのは、欧州司法裁判所が分担する司法権の機能を別にすると、立法権と行政権とが統合された単一の「執行権」と TFEU が定める 3 つの機関（欧州議会、理事会及び欧州委員会）による機能分担である。逆に、統合された執行権というものが成立不可能な環境においては、EU における執行権の行使全体をマネジメントシステムの考え方によって統御することも物理的に不可能である。しかし、TFEU が欧州の基本的価値観の 1 つとして掲げる「民主主義」の原則がある以上、理念としての古典的な三権分立を完全に捨象することはできないので、そのような理念または建前が存在していることを示すものとして、EU の 3 つの機関による対等な合意として機関間合意が採択され、それら 3 つの機関による対等な相互協力という名目の下で統合された執行権の管理・運用を行うものとしたものであると理解するのが妥当である。EU の重要な法令の中でしばしば登場する「一貫性（consistency）」及び「整合化（harmonisation）」の概念は、このような文脈においても再検討されるべき余地がある。

以上について帰納法的に考察する場合、法規範が国権の行使のための道具であるという考え方がもっとも適合的である。のみならず、国家機関それ自体が道具の集合体であるという理解が最も妥当であることになる。それが道具の運用・管理である以上、企業のマネジメントにおけるのと同様、その統御・統治について、類似した基本原則の適用を考えることができることは、むしろ当然のことであろう。このことは、国または国権そのものを神聖視するような国家または社会組織を除き、ほぼ全ての種類・態様の国家体制について妥当する。とりわけ、社会組織それ自体をサイバネティクス（Cybernetics）の一種として認識する場合、事実として物理的に存在する国家組織及びその運用だけではなく、政治哲学上の理念・理想または政治的イデオロギーのような観念的な対象の存在及びその作用・機能もまた、一定の実効支配された領域における統御のための道具の一種として客観的に考察する姿勢が求められる。なお、夏井高人「サイバー犯罪の研究（九・完）―補遺・最近の法改正と裁判事例―」法律論叢 89 巻 1 号 143～198 頁 (2016)、前掲夏井高人「アシモフの原則の終焉―ロボット法の可能性―」、新保史生「ロボット・AI と法をめぐる国内の政策動向」人工知能学会誌 32 巻 5 号 665～671 頁（2017）参照。

(159) 結論的に言うと、全ての空間及び全ての次元において通有するという意味での絶対的な識別のようなものは、常に成立しない。論理的に可能な範囲としては、ある閉じた空間において、閾値として用いられる一定の基準の適用結果に基づき、相対的な意味で識別の成否という処理結果が導出されるのみである。これは、その閉じた空間の外から見れば相対的なものに過ぎないのであるが、その閉じた空間の中においては、絶対的なものとして機能し得る。人類社会は、そのような意味における相対的な結論を絶対的な結論であると錯覚することのできる曖昧性の能力をもっていたからこそ、他の高等生物種に対する相対的優位を維持しながら生存し続けることができたのである。なお、脚注 96 参照。

(160) 指令 2012/28/EU の参考訳は、法と情報雑誌 2 巻 11 号 105～120 頁にある。

(161) 指令 (EU) 2017/1564 の参考訳は、同誌同号 27～41 頁にある。

(162) 規則 (EU) 2017/1563 の参考訳は、同誌同号 42～50 頁にある。

(163) 同様の問題は、普通の電子商取引のために使用される場合を含め、通常の電子機器を用

いた一般的な通信の場合において更に深刻さを増加させる可能性がある。とりわけ、そのマンマシンインタフェイスとして平板のタッチパネルが専ら使用される場合、視覚に障害のある者に対するサポートが何もない環境だけが提供されることになる。マラケシュ条約に基づく世界各国の著作権法の改正等と関係する議論は、コンテンツの利用に焦点をあてて矮小化される傾向があるけれども、物事の本質が本当はもっと別のところにあることに留意しなければならない。

(164) 加えて、識別子として社会的に機能する符号または番号は、一般に、（アクセスに関する一定の制限の有無を無視して考えれば）公開情報として存在しており、完全な機密情報であることがむしろ少ないという事実にも留意すべきである。それゆえ、識別子であるというだけで特に法的保護に値すると常に即断するような法解釈上の態度は妥当ではない。正しくは、当該識別子が当該環境において果たすべき機能という側面から、個別・具体的に検討・考察することを要する。

(165) その細則は、委員会実装規則 (EU) 2015/1501 及び委員会実装規則 (EU) 2015/1502 に定められている。なお、前述の信頼サービス（2.2.3）参照。

(166) それゆえ、どの社会においても共通のものと想定する限り、それ自体が数学上の確実性を欠くという致命的な欠陥をもつとみなされているトマス・ベイズ（Thomas Bayes）の確率論に基づく証明による場合でさえ、常に偽となることを免れない。特定の自然人の識別のための推論は、個々の社会環境において相対的なものであり、かつ、定性的な要素を多々含むので、厳密な意味で共通の確率論的証明が成立する余地はない。精霊のような超自然的なものを超自然的ではない日常的なものと認識する社会においては、その度合いが更に著しい。ただし、トマス・ベイズ流の確率論に基づく推論方式は、事後的に、後付けの言及として説明の用に供することはできる。これは、いわゆる「法と経済」なる学派に共通にみられる現象であり、そのことのみで、この学派が真理という意味での概念や定義を提供するものではないことを自己証明していると認め得る。

(167) このことは、識別子の社会的有用性・重要性を否定する趣旨ではない。現実に存在する識別子が社会の中で多数・多様な社会関係を規律するためのツールとして用いられている場合、その有用性・重要性が高まることは当然のことである。しかし、それは、当該識別子が現実に社会の中で多種多様に使用されているという社会関係の結果として生ずることなのであり、識別子それ自体に内在するものではない。例えば、あるデータベースにおいて仮に用意されている識別子が実際には使用されていないような状況を考えてみると、当該現実には使用されておらず、何もパラメータをもたない符号として記録されているだけの識別子には、何も社会的な意味が発生しようがないということを考えれば、容易に理解できることである。例えば、宝くじに印刷された番号は識別子であるが、売れ残った宝くじの番号が仮に当選番号であったとしても、当選番号であるか否かとは無関係に売れ残りの宝くじが一律に破棄されるとすれば、その宝くじを現実に当選金と交換できる者が誰もいない以上、その当選番号を印刷した宝くじは、社会的には何の意味ももたない。単に識別番号として存在しているというだけのことである。

(168) 例えば、遺伝子は、人が生まれたときからもっているものであるが、識別の必要性（例：国境検問等の際に参照する必要性）が生じない限り、単に遺伝子があるというだけのことであり、それ自体として個人データであることを意識する必要性が生じない。しかし、何らかの意味で識別のための処理の前提として当該遺伝子データが収集される際には、識別という社会関係が発生していることになるので、その場面では当該遺伝子情報は、個人データとしての社会的・法的意味をもつことになる。極論すると、個人を識別

しようとする者が世界中に誰一人存在しない場合には、個人データが全く存在しないことになる。例えば、核戦争や深刻な疫病の蔓延によって世界中の人々が死んでしまい、最後の 1 人だけ生き残っている状況を想定すると、その者にとっては、（1 人しか存在しない以上）識別する必要性が全くなくなってしまっているので、個人データという概念も消滅することになる。要するに、行政目的または商業目的のために識別しようとする者が存在することから個人データの概念が社会的な重要性をもつことになると言い得る。それゆえ、識別を禁止すれば、同様に、個人データという概念の社会的有用性が消滅することになる。このように、個人データという法的属性は、相対的な社会的評価結果の一種のようなものであり、絶対値としての属性値ではない。そうである以上、憲章第 8 条に定める個人データの保護の権利もまた、一定の社会関係の下において生じ得る相対的な社会現象の一種であると言うべきであり、環境条件のいかんにかかわらず常に存在しているような物体的なものではない。このことは、プライバシーの利益においても同じである。

(169) 規則 (EC) No 45/2001 及び e プライバシー指令 2002/58/EC は、当初、個人データ保護指令 95/46/EC とセットのものとして一緒に改正される予定であった。このことは、欧州委員会の EU Data Protection Reform（Brussels, 25 January 2012）の中で示されていた基本方針であったが、その後、EU の機関、構成国の警察部門、構成国の電気通信部門を別の法令により改正するという方針に変更され、それらの部門を除いた部門に適用される条項及び一般的に適用される基本原則を定める条項を併せた法令として GDPR が制定された。この間、欧州データ保護監督官（European Data Protection Supervisor (EDPS)）は、実質的にみて均等な内容をもつ EU 内において一貫性のある法制を構築することが望ましいとの意見を述べ続けた。例えば、Opinion of the European Data Protection Supervisor on the data protection reform package（7 March 2012）がその例である。この EDPS データ保護法改正パッケージ意見書の参考訳は、法と情報雑誌 2 巻 8 号 257～371 頁にある。なお、脚注 38 及び脚注 39 参照。

(170) 理事会決定 2008/615/JHA の参考訳は、同誌 2 巻 2 号 155～181 頁にある。

(171) 小西知世氏（明治大学法学部准教授）との共訳による理事会決定 2008/616/JHA の参考訳は、同誌 2 巻 9 号 116～200 頁にある。

(172) 識別子（identifier）を要素（factor）の一種として理解すると、このことは自明である。ある識別子によって特定の自然人を識別するためには、実は、別の諸要素のデータセット（プロファイル）に基づく識別によって識別可能な状態となった本人というデータ集合が別に存在しており、そのデータ集合と当該識別子とが連携するものとして関連付けされなければならないので、実際のデータ集合は、識別子だけで構成されているのではなく、識別子であるデータ＋本人を識別可能とする諸要素データ集合によって構成されていることになる。現実の問題として、例えば、ある識別子を示す物件（例：パスポート）を所持していることによって特定の自然人を識別処理するという場面においては、それを現実に所持しているのが生きた自然人であるという事実＋所持しているという事実が別の諸要素によって識別され、それらが同一の空間内で同時に発生しているという事実が認識されなければならない。これらの基礎的な事実の識別が完了した後、当該識別子を示す物件内に同時に記録されている氏名や顔写真等の他の諸要素が複合的に照合されて識別処理されるのである。

一般に、識別子だけが存在している場合、それは、仮名化または匿名化の有無に拘らず、単なる符号またはデータの一種に過ぎない。それが自然人の識別処理の目的で使用

される場合、個人データとして法的に評価されるのである。その意味で、あるデータがもつ個人データとしての属性は、固定的なものではあり得ず、自然人の識別処理のために使用されるか否かという状況の相違により、相対的に評価され、決定されるものである。このことから、個人データの侵害の有無及びその程度を考察・評価する場合においても、どのような構成（要素集合）によるデータセットであるのかに特に注目すべきである。

他方において、一定の社会関係という文脈の中で識別子とされるタイプのデータの保護の必要性が相対的に高いことも否定されない。それは、社会内において濫用または悪用される危険性が高いからであり、そのために無権限でアクセスされる蓋然性が高いからである。例えば、DNA プロファイルのような識別力の高い生体データも同様である。これらは、論理的な意味における識別のメカニズムそれ自体に着目するのではなく、適法なものと違法なものとを含め、社会内における現実の需要の有無・程度及びその使用により生ずる事態に着目する影響評価の結果に従う価値判断である。それゆえ、ある特定の人間社会において、その社会基盤や社会生活の様式が変化すると、識別子というものに対する価値判断にもその変化が及ぶことがあり得る。例えば、かつての非電子的な時代においては、氏名が最も重要な識別子であったかもしれない。しかし、高度に電子化された現代の先進国においては、氏名を全く用いない別の識別子による識別が普通に行われている。例えば、指紋のような生体要素を識別子として使用するスマートフォンのアクセス管理がその例である。

(173) 日本国の個人情報保護法においては、第 2 条第 1 号所定の「他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるもの」が相当すると解される。この規定の文言からは明らかではないが、この条項の論理構造としては、「他の情報と容易に照合」することを必須の前提として「個人を識別」という結果を出力するような処理のために使用される情報の集合を指すことが明らかであり、その情報は、個々のものそれ自体としては、必ずしも個人情報に該当しないものを含むことになるので、GDPR における「要素（factor）」とほぼ同じものを指すと解することが可能である。

(174) 関連する文書として、2007 年 3 月 15 日の通知 COM/2007/0096 final がある。この通知の中では、RFID の利用に際して、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 が遵守されなければならないことが強調されている。

(175) OJ L 197, 24.7.2012, p.38-71

(176) OJ L 174, 1.7.2011, p.88-110

(177) European Commission, Cyber-Physical Systems: Uplifting Europe's Innovation Capacity, December 2013、Antonio Guerrieri, Valeria Loscri, Anna Rovella & Giancarlo Fortino (Eds.), Management of Cyber Physical Objects in the Future Internet of Things: Methods, Architectures and Applications, Springer (2016) 参照

(178) 脚注 24 参照

(179) 例えば、自然人が CPO を身体に装着し、または、身体内にインプラントすると、当該自然人が当該 CPO と関係する CPS のためのセンサー（端末機器類）として機能するような場合、その自然人は、電子情報ネットワークの一部を構成するサイボーグの一種へと変化することになる。そのシステムの自律的・自動的な管理・運用という側面においては、当該自然人の人間としての自律性がほぼ喪失することになる。このことは、憲

章第 1 条に定める人間の尊厳の尊重という基本原則と明確に矛盾する部分を含む。

この点について、EU の関連法令やロボット及び人工知能に関する政策文書等を検討する限り、当該自然人が当該システムの中に組み込まれてしまうことについて、当該自然人の任意の同意があることが適法化要件（正当事由）として考えられているように思われる。しかし、そもそも、「人間の尊厳を喪失させること」の同意は無効であることを一応措くとしても、そのような同意（consent）は、事前に説明を受けた上で、その説明の十分な理解に基づき、任意に与えられるものでなければならない。ところが、ごく標準的な自然人にとって、自分自身が電子情報ネットワークの部品として組み込まれてしまうことの本質的な意味を正しく理解することは無理である。ここにおいて、同意ベースの正当化事由を根拠とする政策論の推進には一種の虚構性が存在すると言わざるを得ない。

(180) このような考え方については、2016 年 11 月 12 日に開催された情報ネットワーク法学会第 16 回研究大会における大会記念講演「サイバー法の未来―サイバー領域の拡大」で概説したとおりである。その講演内容は、情報ネットワーク・ローレビュー 15 巻（2017）の講演録編 CD-ROM（ISBN:978-4-9909833-0-7）に PDF ファイル形式で収録されている。

(181) それぞれの自律的な CPO が自律的に相互認識するという場面においては、認識主体として認識処理システムが機能しており、かつ、認識対象として識別子が機能しているという点を見逃してはならない。また、この場合における識別は、自律的なものであるので、前述の識別と識別子との関係における論理構造がそのまま反映されることになる結果、実際には識別子を用いない個体識別が普通になると考えられる。例えば、当該自律的装置の外形的特徴といった要素の記録の蓄積（人間における経験に相当）により、人間が予め用意した識別子とは無関係な識別が自律的に実行されるような可能性がある。ここにおいても、自律的な機器・装置に対する人間の管理可能性または支配可能性が次第に崩れる危険性が内在されていると言える。この問題を考える上で最も重要なポイントは、人間は、識別子を識別子として明確に認識して行動することもあるが、一般的にはそのような行動をしておらず、むしろ、そうであることによって自律的に社会秩序が常時形成され続けているという普通の事実に気づくかどうかである。自律性（autonomous）の概念は、そのような恣意的とも表現し得るような一定の機能及び作用を一般的に含むものとして理解されなければならない。

(182) 日本国の高速道路における ETC システムに相当するシステムであるが、陸上交通とフェリーのような水上交通とをシームレスかつマルチモーダルに利用可能な状態をめざしている点において、拡張的であると言える。一般に、欧州においては、河川の交通及び海上の交通を含め、水上運送の重要性がかなり高い（前述の 2.1.4 参照）。

(183) 前掲ハイブリッドな脅威報告書 JOIN (2017) 30 の中では、テロ対策のために ITS システムで処理される様々な個人識別情報及び自動車識別情報の利用が示唆されている。

(184) 別の目的のために構築された空間情報のデータセットが個人識別の目的のために使用される場合には、GDPR を含め、関連する EU の個人データ保護法令が適用される。この場合、当該空間情報のデータセットを構築する当初の目的が個人データの処理と無関係な場合には、GDPR 等の個人データ保護法令に定める目的による制限の原則がそもそも適用されないので、注意を要する。このことは、日本国法の解釈においても同じであり、個人情報の取扱いと無関係に収集されたデータが後に個人情報の取扱いのために個人情報データベースの中に取り込まれる場合には、少なくとも、目的外利用にはなら

ないし、取得の際に(個人情報保護法が想定するような)個人情報の本人が存在する場合に該当しない可能性があることに留意しなければならない。これらの点に関しては、いずれの法制によっても明確に定められているわけではない。このことは、個人識別とは無関係なビッグデータからの一群のデータの移転の場合の対応及び法解釈においても同じである。

(185) INSPIRE指令2007/2/ECの参考訳は、法と情報雑誌2巻9号1～25頁にある。

(186) 人工衛星から提供される画像データその他の関連データに基づいて生成される地表の状況を示すデータセットが、国防及び国境警備を含め、軍事目的及び警察目的でも応用可能なことは言うまでもない。例えば、INSPIRE指令2007/2/ECの別紙Ⅲに列挙されている重点課題事項の5(人間の健康及び安全)は、「病状(アレルギー、腫瘍、呼吸器疾患等)の勢力の地理的分布、健康に対する影響を示す情報(バイオマーカー、生殖能力の低下、感染症の流行)、または、人間の健康状態を示す情報(疲労、ストレス等)であって、直接に(大気汚染、化学物質、オゾン層の枯渇、騒音等)または間接に(食品、遺伝子組換え生物等)環境の質と関連性をもつもの」と定めており、それ自体としては環境保護の目的のものであるが、それと同時に、長期的な影響を及ぼす公衆衛生上の問題の解決の目的や生物化学兵器への対応という側面における国防目的を実現するためのものでもあり得る。特に、Security Union第11次進捗状況報告書COM/2017/0608 finalでは、規則(EU) No 98/2013(OJ L 39, 9.2.2013, p.1-11)で指定された爆発物前駆物質の管理の徹底、並びに、生物化学兵器を用いたテロ攻撃への準備及び対応が強調されていることに留意すべきである。

(187) アクセスの対象が国の政府である場合においても基本的には同じであり、民主主義社会においては、単に政府が存在しているというだけでは足りず、国民が政府機関等にアクセスし、そこから得られた情報に基づいて政府機関を監視できる状態になっていることが重要である。英米における法哲学ないし政治哲学上の根拠に関しては、佐々木秀智「アメリカにおける政府への公衆のアクセスの法的根拠」法律論叢76巻6号57～114頁(2004)が参考になる。

(188) 裁判所における訴訟手続へのアクセスについても同様に考えることができる。EUの司法裁判所及び一般裁判所(旧第1審裁判所)においては、それぞれの裁判所の手続規則に従い、書面審理段階の手続に対しては、原則として、訴訟当事者及び訴訟参加人のみがアクセス可能であり、弁論段階の手続に対しては、原則として、公開の法廷において物理的に傍聴可能な員数の範囲内で当事者以外の者もアクセス可能である。なお、2016年改正欧州司法裁判所手続規則の参考訳は、法と情報雑誌2巻9号201～282頁にあり、2016年改正一般裁判所手続規則の参考訳は同誌同号368～449頁にある。

(189) 例えば、遠い宇宙空間を通過する電子線について、地球上の特定の自然人が観測を実行することは可能な場合があり、その場合、当該電子線に対するアクセスが行われたことになるし、その観測結果としてのデータは、当該観測者が専有するものとなるであろう。しかし、当該観測者は、その観測行為それ自体によって理論物理学的な意味において当該電子線の物理的な運動に対して何らかの力学的影響を与えたと考え得る現象が生じ得る可能性が皆無とは言えないとしても、その電子線の到来という現象それ自体を(人間の生体感覚器によって直接に認識処理可能な範囲にあるものとして)管理したわけではないし、(そのような意味において)管理可能なわけでもない。

(190) 規則(EC) No 1049/2001の参考訳は、法と情報雑誌2巻3号102～118頁にある。

(191) 指令2003/98/ECの参考訳は、同誌2巻9号48～59頁にある。指令2013/37/EUの

参考訳は、同誌同号 60～76 頁にある。指令 2013/37/EU による一部改正後の指令 2003/98/EC 参考訳は、同誌同号 77～83 頁にある。

(192) 実際の運用に関しては、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）が参考になる。

(193) 規則 (EU) No 1295/2013 の参考訳は、法と情報雑誌 2 巻 11 号 121～155 頁にある。

(194) 脚注 147 参照

(195) OJ C 190, 30.6.2011, p.2-15

(196) OJ C 96, 1.4.2014, p.1-51

(197) OJ L 304, 20.11.2010, p.47-62

(198) OJ C 95, 1.4.2014, p.1-7

(199) この機関間合意は、外交及び安全保障の分野にある事項の範疇に含まれない EU の機関における一般行政文書に広く適用されるものである。情報セキュリティの目的のための技術仕様等を示す文書、国民の犯罪歴や病歴等に関するデータを含め、機微のデータ（sensitive data）に該当する個人データを含む文書等もそのような機密区分を受ける文書に含まれ得る。それらの一般文書は、機密情報を含む文書として、指定された区分に対応する取扱いが行われなければならない。

(200) OJ L 141, 27.5.2011, p.17-65

(201) 一般裁判所決定 (EU) 2016/2387 の参考訳は、法と情報雑誌 2 巻 9 号 454～472 頁にある。

(202) 営業秘密指令 (EU) 2016/943 の参考訳は、同誌同号 489～514 頁にある。

(203) トラフィックデータの保持（retention）を認めるデータ保持指令 2006/24/EC は、欧州司法裁判所の先決裁定（joined Cases C-293/12 and C-594/12 及び C-203/15）によって全面的に無効なものと宣言された。なお、脚注 86 及び脚注 209 参照。

(204) 日本国における通信の秘密に関しては、夏井高人「サイバー犯罪の研究（三）―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 (2016) で詳論したとおりである。

(205) 個人データの移転は、物品やサービスの移転に必然的に伴うことがあり、その法的保護を均等なものとすることにより不合理な法的規制を排除すれば、物品やサービスの流通が円滑化するという発想に基づく。欧州委員会通知 COM/2017/07final の 3 では、「プライバシーは、取引される商品ではない」と述べられている。

(206) 従来のプライバシー保護という文脈とは別に、特定の遺伝子型をもつことを理由とする社会生活上の差別的な取扱いの危険性については、夙に指摘されてきたとおりである。加えて、少なくとも理論的には、特定の遺伝子型のある自然人だけに有効な生物化学的攻撃手段が成立し得ること、そのような生物化学的上攻撃手段を実行することにより、特定の遺伝子型をもつグループに属する自然人のみを選択的にジェノサイドすることが不可能ではないこと、そして、そのような攻撃手段の開発のためには、射程距離の測定または有効性評価のためには個人データ保護法令が適用されない個人識別不能データの集合または純粋な統計データの集合があれば足りるため、既存の個人データ保護法制の枠組みでは対処不可能である。

(207) 規則 No 1338/2008（OJ L 354, 31.12.2008, p.70-81）参照

(208) 同様の機微のデータの処理の一般的な禁止に関する条項は、規則 (EC) No 45/2001 第 10 条、警察指令 (EU) 2016/680 第 11 条第 2 項及び第 3 項、Europol 規則第 30 条第 2 項にもある。

(209) 具体的な判決事例として、前掲 *Schrems* 事件判決(脚注 141 参照)、EU とカナダ間の PNR 協定に関する 2017 年 6 月 26 日意見及びデータ保持指令 2006/24/EC に関する複数の先決裁定(joined Cases C-293/12 and C-594/12 及び C-203/15)がある。先決裁定 C-203/15 の邦訳としては、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」法と情報雑誌 2 巻 1 号 1〜40 頁があり、カナダ PNR 協定意見の邦訳としては、前掲「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」がある。なお、PNR に関しては、前述の渡航者情報管理(2.1.6)参照。EU の司法裁判所及び一般裁判所(旧第 1 審裁判所)と同様に、照会に対して裁判所が意見を示すことのできる機能は、EFTA 裁判所にもある。2010 年改正 EFTA 裁判所手続規則の参考訳は、同誌 2 巻 10 号 40〜80 頁にある。

(210) なお、前述の税関システム(CIS)に関する論述(2.1.3)も参照。

(211) 前述の SIS II に関する論述(2.1.2 (1))参照

(212) 脚注 68 参照

(213) 2017 年 9 月 7 日の Security Union 第 10 次進捗状況報告書 COM/2017/0466 final は、2008/615/JHA 及び 2008/616/JHA が現時点で有効な法令として、対外国境管理における生体認証データの処理のために適用される旨を述べている。また、理事会枠組み決定 2009/905/JHA(OJ L 322, 9.12.2009, p.14-16)は、2008/615/JHA 及び 2008/616/JHA に基づいて処理される指紋データや DNA プロファイル等の生体要素の調査研究機関(EN ISO/IEC 17025 を遵守する認証評価を得たフォレンジックサービスプロバイダ)に対する EU 法としての規律を定めている。理事会枠組み決定 2009/905/JHA の参考訳は、法と情報雑誌 2 巻 8 号 41〜47 頁にある。

(214) VIS 情報システムは、理事会決定 2004/512/EC(OJ L 213, 15.6.2004, p.5-7)に基づいて設置・運用されている。理事会決定 2004/512/EC の参考訳は、法と情報雑誌 2 巻 8 号 67〜74 頁にある。VIS 情報システムの設置場所に関しては、委員会決定 2006/752/EC(OJ L 305, 4.11.2006, p.13-14)が定めている。委員会決定 2006/752/EC の参考訳は、同誌同号 75〜79 頁にある。VIS 情報システムの中央システムと国内端末とのインタフェイスの構築に関しては、委員会決定 2008/602/EC(OJ L 194, 23.7.2008, p.3-8)が定めている。委員会決定 2008/602/EC の参考訳は、同誌同号 80〜90 頁にある。なお、前述の SIS II に関する論述(2.1.2 (1))参照。

(215) 理事会決定 2008/633/JHA の参考訳は、法と情報雑誌 2 巻 8 号 48〜66 頁にある。

(216) 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)の参考訳は、法と情報雑誌 1 巻 4 号 1〜20 頁にある。同条約の監督官及び国境を越えたデータの移転に関する追加議定書(ETS No.181)の参考訳は、法と情報雑誌 1 巻 4 号 21〜25 頁にある。

(217) 警察分野における個人データの利用に関する勧告 No. R(87)15 の参考訳は、法と情報雑誌 1 巻 6 号 140〜149 頁にある。

(218) 理事会規則(EC) No 2252/2004 の参考訳は、法と情報雑誌 2 巻 7 号 104〜117 頁にある。同規則を一部改正する規則(EC) No 444/2009 の参考訳は、法と情報雑誌 2 巻 7 号 118〜129 頁にある。

(219) 脚注 45 参照

(220) 脚注 88 参照
(221) Europol 規則 (EU) 2016/794 が制定・適用される前は、Europol 決定 2009/371/JHA の第 10 条、第 14 条、第 16 条ないし第 35 条が詳細に定めるのに加え、第 39 条第 6 項において「Europol は、Europol 職員と関連する個人データの処理について、規則 (EC) No 45/2001 の基本原則を適用する」と定めている。更に、Europol における個人データ及び機密情報の交換に関しては、2009 年 11 月 30 日の理事会決定 2009/934/JHA（OJ L 325, 11.12.2009, p.6-11）が制定され、Europol における個人データ処理のための解析ファイルに関しては、2009 年 11 月 30 日の理事会決定 2009/936/JHA（OJ L 325, 11.12.2009, p.14-22）が制定され、機密性確保のためのアクセス制御に関しては、2009 年 11 月 30 日の決定 2009/968/JHA（OJ L 332, 17.12.2009, p.17-22）が制定されていた。これらの法令は、Europol 規則 (EU) 2016/794 によって廃止された。これら廃止法令の参考訳は、いずれも法と情報雑誌 2 巻 2 号にある。
(222) 理事会規則 (EU) 2017/1939 第 100 条は、EPPO と Eurojust が相互に密接な関係を構築しつつ活動すること、同規則第 101 条は、EPPO と OLAF が相互に密接な関係を構築しつつ活動すること、同規則第 102 条は、EPPO と Europol が相互に密接な関係を構築しつつ活動することを定めている。
(223) 理事会決定 2009/426/JHA の参考訳は、法と情報雑誌 2 巻 4 号 36～80 頁にある。同理事会決定による改正前及び改正後の理事会決定 2002/187/JHA の参考訳は、同誌同号 81～152 頁にある。Eurojust における個人データの処理及び保護に関する規則及び同追加規則の参考訳は、同誌同号 153～194 頁にある。
(224) OLAF 規則 (EU, Euratom) No 883/2013 の参考訳は、同誌同号 1～35 頁にある。OLAF における個人データ保護のための内部規則であるデータ保護責任者（DPO）に関する決定の参考訳は、同誌 2 巻 3 号 172～183 頁にある。
(225) 脚注 161 参照
(226) 特許権、意匠権及び商標権と関連する EU の法令の邦訳は、日本国の特許庁の Web サイト上においてほぼ網羅的に公表されている。
(227) 指令 2009/24/EC の参考訳は、法と情報雑誌 2 巻 11 号 51～62 頁にある。
(228) 指令 2006/115/EC の参考訳は、同誌同号 63～76 頁にある。
(229) 指令 2006/116/EC の参考訳は、同誌同号 77～87 頁にある。
(230) 指令 2012/28/EU の参考訳は、同誌同号 105～120 頁にある。
(231) EU 構成国の比較法分野において非常に参考になる論文として、黒澤睦「親告罪・私人訴追犯罪・職権訴追犯罪としての著作権法違反 (1)―TPP をめぐる著作権等侵害罪の一部非親告罪化の動きを踏まえたドイツ・スイス・オーストリア・リヒテンシュタインとの比較法制史的考察―」法律論叢 89 巻 6 号 89～155 頁 (2017) がある。
(232) 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)、同「アメリカにおけるインターネット上の児童に有害な情報の規制」法律論叢 77 巻 6 号 57～114 頁 (2005)、丸橋透「「青少年有害情報」と民事責任」法とコンピュータ 29 号 65～81 頁 (2011) が参考になる。
(233) 2017 年 9 月 28 日の欧州委員会通知（COM(2017) 555 final）参照。なお、Union 第 11 次進捗状況報告書 COM/2017/0608 final（脚注 154）参照。
(234) 関連する文書として、欧州委員会の 2014 年 1 月 27 日の報告書 COM/2014/027 final がある。

(235) 脚注 7 参照
(236) 指令 2013/40/EU の参考訳・改訂版は、法と情報雑誌 2 巻 8 号 164～185 頁にある。
(237) 理事会枠組み決定 2002/475/JHA の参考訳は、同誌 2 巻 5 号 71～85 頁にある。
(238) 指令 (EU) 2017/541 の参考訳は、同誌 2 巻 8 号 1～29 頁にある。
(239) ハイブリッドな脅威報告書 JOIN (2017) 30 及び Security Union 第 11 次進捗状況報告書参照
(240) 理事会決定 2005/671/JHA の参考訳は、法と情報雑誌 2 巻 8 号 30～37 頁にある。一部改正後の理事会決定 2005/671/JHA の参考訳は、同誌同号 38～40 頁にある。
(241) 脚注 233 参照
(242) 脚注 11 参照
(243) 攻撃パケットと非攻撃パケットとが識別不可能または識別困難な状態で常に混在しているという事実は、通信の管理者であるプロバイダだけではなく、犯罪用パケットを監視する警察機関及び軍事用パケットを監視する防衛機関にとって、かなり深刻な問題をなげかけている。日本国における官民協力政策は、あくまでも平時における犯罪対策を主眼におくものである。EU における対応とは、その性質上、基本的に異なる部分がある。
(244) 攻撃者が自然人ではなく人工知能システムである場合、状況によっては、その人工知能システムの主観的な意図のようなものを事後的に解析できないわけではない。しかし、当該人工知能システム内または複数の人工知能システム間で交わされる人工言語のようなもの（通信のスキーム）が人類にとっては全く理解できないような全く未知のものである場合、「人類にとっては了解可能な解析が不可能である」という意味で、人類が管理可能なシステムの外にあるのと同じことになる。
(245) ネット上におけるデジタルな攻撃に加えて、超小型のドローン、サイボーグ化された小動物等を GPS の機能を用いて自動的に攻撃対象地まで到達させ、生物化学兵器を散布するような攻撃もサイバーとリアルを組み合わせた物理攻撃の一種であると考えられる。合成された人工生命体（ミュータント）による物理攻撃によっても同じ結果が得られる。人工生命体にチップを埋め込み、完全に自律的な人工知能システムによって遠隔操作することも可能である。理論的には、ナノテクノロジーの応用により、高度な知能や相互通信能力をもった殺人ウイルスや殺人細菌または微細なサイボーグを構築することは十分に可能な範囲内にある。これらを用いた複合的な攻撃またはハイブリッドな攻撃に対する防御が可能なのは、人間による制御・対応が可能な生物化学兵器に対してのみである。とりわけ、自己増殖可能で有毒な有機体ロボットまたは有毒ミュータントの場合、識別された個体を破壊したとしても、残存する個体からの更なる増殖が可能である以上、全体としての脅威を完全に消滅させたことにならない。また、理論的には、そのような生物化学兵器の分子構造上または生体構造上、それに対応するワクチンの製造が理論的にも実務的にもあり得ないようなものも存在し得るので、そのような場合には化学的な防御ができない。有機体ロボットをロボット（オートマトン）の一種とは認めない見解もあるが、そのような見解の論者は、悲惨なまでに愚かである。そのような意図的または無知・無思慮による誤った見解の論者らによって強力に支援されて、微細な人工生命体や遺伝子合成物である新種細胞塊の開発（イノベーション）がどんどん進展している現状に鑑み、全人類の絶滅の可能性は、現実の問題になっていると考えられる。
(246) 関連機関の設置の中には、EU Hybrid Fusion Cell を既存の EU 諜報及び情報センター（EU Intelligence and Situation Center）の組織内に創設すること、フィンランドに設置されたハイブリッド脅威に対抗するための欧州研究拠点（European Centre for

Countering Hybrid Threats）の活動開始が含まれる。これらの点に関しては、ハイブリッドな脅威報告書 JOIN (2017) 30 の中に説明がある。なお、本論とは直接の関係はないが、サイバースペースの拡大による軍事上の戦略及び戦術の根本的な変化に関しては、江畑謙介『情報と戦争』（NTT 出版、2006）がある。また、諜報機関による軍事目的以外の目的による国民の監視の問題に関しては、大野幸夫「スノーデン事件と情報法の課題」・『野村豊弘先生古稀記念論文集　知的財産・コンピュータと法』（商事法務、2016）987～1038 頁所収がある。

(247) ロボット及び人工知能と関連する法令制定の検討を求める欧州議会の決議（2015/2103 (INL)）（A8-0005/2017）では、高度な知的能力をもつ人工知能システムまたは自律的なロボット（autonomous robots）の研究・開発について登録所を設置し、EU の特別機関（EU Agency for Robotics and Artificial Intelligence）がそれらの研究・開発を監視するという構想が提案されている。前述のとおり、このような仕組みは、法制度上におけるバイデザインの応用と理解することが可能であるが、人類を滅亡させかねないようなシステムの研究・開発に対する事前監視という機能をもち得ることは言うまでもない。人類が制御可能なのはここまでである。この段階で、研究・開発の危険性を察知し、それを禁止または破壊しない場合、完成されたシステムが完全に自律的なものである場合には、その自律性のゆえに人類による制御を排除し得るものとなり得る。つまり、人類は、そのような完成されたシステムを制御不可能である。制御不可能な対象に対しては、法による統制も不可能である。このような制御不可能性の中には、電子化された世界規模の資金決済システム及び投資システムに対する完全に自律的な人工知能システムによる（場合によっては全ての人間の投資家を破綻させかねないような）干渉の制御不可能性というようなタイプの制御不可能性も含まれる。仮にそのようなシステムが電源供給の停止により機能停止させ得るものであったとしても、例えば、特定の国または集団がそのような高度の干渉を実行するだけの能力をもつ人工知能システムを物理的に所持しており、かつ、他国の財政機能及び金融・投資のための電子的なシステムを完全に破壊するために意図的にその人工知能システムを運用しているような場合には、自国以外の国々のためにそのシステムの電源供給を停止させることによってそのシステムによる干渉を停止することがないということにも十分に留意すべきである。この場合、そのようなシステムは、核兵器と同等またはそれ以上の攻撃力をもつサイバー兵器でもあることになる。それが現実に実行されるとき、世界の国々の国家主権は、理論的にも現実的にも消滅する。

(248) Security Union 第 11 次進捗状況報告書 COM/2017/0608 final の結論部分及びサイバーセキュリティ通知 JOIN(2017) 450 final 参照

(249) これは、従来の EU 法の学者の怠慢によるものではなく、基本的な素養として、日本国の六法全てに通暁し、それらと対応する EU 法の法令について網羅的・横断的な比較検討を実施可能なタイプの研究者がたまたま EU 法の領域には存在しなかったことによるものと推定される。しかし、このことは、EU 法に限定されるものではないので、日本国の大学院における法学教育が根本的なところで見直しを迫られているとも言い得る。

(250) 星名定雄『情報と通信の文化史』（法政大学出版局、2006）参照

(251) 永田英明『古代駅伝馬制度の研究』（吉川弘文館、2004）、舘野和己・出田和久編『日本古代の交通・交流・情報 1―制度と実態』（吉川弘文館、2016）参照

(252) いわゆる情報財の法的な意味における財産権性に関しては、夏井高人「情報財―法概念としての意義―」明治大学社会科学研究所紀要 52 巻 2 号 213～241 頁 (2014) で詳論し

たとおりである。

(253) 現時点においてそのような予測が存在しないわけではないが、それでもパニックが発生しないのは、バックアップシステムの存在及びそれが正常に機能すること等を含め、情報社会の機能が正常に稼働することを担保するための制度及び技術的・組織的な仕組みが存在していると信じられているからである。仮にそのような信頼が根底から損なわれるような事態が発生した場合、全てが無に帰すことが明確となるので、パニックが不可避となるだけではなく、地球上の圧倒的多数の資産家が瞬時にして無資産家と変容してしまうことになる。すなわち、「価値」なるものは、主観的な期待の一種に過ぎず、いかなる意味においても物理的な実体をもつものではない。その期待が維持可能であるのは、期待を実現するためのシステムが存在しており、かつ、そのシステムを国家の物理的な軍事力及び警察力が物理的に保護しているからである。国家権力が相対的に希薄な地域においては、当該地域における事実上の武力を握る勢力が国家の軍または警察が果たすべき機能を営んでいる。抽象的な経済理論や経営理論が支配しているわけではない。以上のような意味において、権力及び権利の本質における政治学上の「実力説」が常に正しい。単なる期待に過ぎないものであるのに、それを実体があり、かつ、実在する資産と同視する者に関しては、スペインの古い伝承を素材としてアンデルセンが翻案して公表したものであると伝えられる「裸の王様」の逸話が想起されるべきである。

(254) サイバーセキュリティ通知JOIN(2017) 450 finalによれば、EUにおけるサイバーセキュリティ技術及びその運用能力の向上は、この分野における産業育成策でもあり、この分野における国際的な競争力の拡充をめざすものでもある。そのことを読み落としてはならない。

(255) 脚注36参照

(256) 参考となる文献として、曽我部真裕・林秀弥・栗田昌裕『情報法概説』（弘文堂、2015）及び齋藤雅弘『電気通信・放送サービスと法』（弘文堂、2017）がある。

(257) 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。

（明治大学法学部教授）