情報社会の素描 -EUの関連法令を中心として- （1）

メタデータ	言語: jpn 出版者: 明治大学法律研究所 公開日: 2018-03-28 キーワード (Ja): キーワード (En): 作成者: 夏井, 高人 メールアドレス: 所属:
URL	http://hdl.handle.net/10291/19275

法律論叢第90巻第4・5合併号（2018.2）

【論　説】

情報社会の素描―EUの関連法令を中心として―(1)

夏　井　高　人

目　次

1　はじめに

情報社会（Information Society）については、様々な立場から様々な意見が述べられてきた(1)。しかし、それらに共通しているのは、単なる情報を基盤とする社会という意味ではなく、電子的な情報のやりとりが人間社会の中で非常に大きな役割を果たすような状況、とりわけ、電子的な情報が情報ネットワークを介して伝達されるような状況を念頭に置いているということである(2)。

電子技術が発展した社会における対応は、欧州においても検討され続けてきた。例えば、欧州共同体の個人データ保護指令 95/46/EC[3] が採択されたのは、1995 年のことであり、欧州共同体の電子商取引指令 2000/31/EC が採択されたのは、2000 年のことであり、電子商取引の基礎となる欧州共同体の電子署名指令 1999/93/EC[4] が採択されたのは 1999 年のことであり、情報通信ネットワークに特化した個人データ保護のための欧州共同体の電子通信プライバシー指令 2002/58/EC[5] が採択されたのは、2002 年のことであり、欧州共同体の情報社会指令 2001/29/EC[6] が採択されたのは、2001 年のことであり、そして、欧州評議会のサイバー犯罪条約（Convention on Cybercrime ETS No.185）[7] が締結されたのは、2001 年のことである。

このような電子的な仕組みが人間社会の中でその重要性を高めるにつれ、電子データや電子機器の脆弱性を悪用する濫用事例や犯罪が深刻化した。また、ノーマルな電子取引においても、ネット上の行為者が一体誰であるのかを識別・特定しなければ契約の履行ができないようなタイプの取引においては、その同一性の識別・特定が不可欠のものとなる。これらの問題が適正に解決されない限り、電子的な市場（EU においてはデジタル単一市場[8]）を安全に運営し、経済発展と競争力の強化を図ることもできない[9]。そこで、電子的な同一性（electronic identity）の証明を保証する制度を確立し、そのための組織としての信頼サービス（trust service）の適格性を定めるために、2014 年に EU の電子識別規則 (EU) No 910/2014[10] が採択され、また、EU レベルの連携したサイバーセキュリティ体制を構築するために、2016 年に NIS 指令 (EU) 2016/1148[11] が採択され、加えて、より高度化・グローバル化・複雑化した情報社会におけるプライバシー保護のために、2016 年に EU の一般データ保護規則 (EU) 2016/679（GDPR）[12] が制定された。

以上のほか、電子的なネットワークが普及する以前に普通の人間社会において生起していたほぼ全てのタイプの法的問題が写像のように電子ネットワークの上で問題とされるようになり、しかも、その影響の及ぶ範囲が国境を越えて世界中に波及することが多々あるため、上記のような関連法令が頻繁に改正されながら現在に至っている。とりわけ、ある情報の発信者と送信者が識別可能であるとしても、セマンティックな問題である情報内容の真偽の判定とその保証には非常に大きな問題があり、いわゆる Fake ニューズの問題を含め、目下のところ最も大きな検討課

題の1つとされている(13)。

他方、リスボン条約以後のEUに関する限り、それらの解決策の基軸は、一貫性（consistency）の確保と関連法令の整合性（harmonisation）の獲得にあると言える。その進展と共に、EUの憲法に相当する欧州連合の機能に関する条約（TFEU）に法的な正当性根拠をもつものとはいえ、EUの構成国の国家主権が徐々に希薄化しつつあることは否定しようがない。

これは、ネットワーク社会における普遍的な原理の1つと考えられる「単一化（unification）の現象形態の一種と考えることができる(14)。そして、モノのインターネット（IoT）や人工知能技術（AI）の発展は、良い意味でも悪い意味でも、その単一化を更に強力に推し進めるものとなっている。これは、欧州連合基本権憲章（Charter）(15)において基本的な価値の1つとして認められている多様性の原理と根本から矛盾する要素を含むものである。

このような社会変動の予定されたベクトルとは異なるベクトルも出現している。それは、ハイブリッドな脅威（Hybrid threats）(16)という語に象徴的に示されるような、社会のインフラとしての電子的なネットワークを利用した社会秩序の根本的な破壊行為である。それが国家によるサイバー攻撃（State sponsored Cyber attack）である場合(17)、理念的にはサイバー戦（Cyberwar）(18)が常時発生しているものとみることも可能であり、私は、そのような状況のことを「戦時と平時が常に共存する状況」と表現してきた。これに対応するためのサイバー防衛は、常時監視を必須のものとするため、非常に近い将来、少なくともネット上のプライバシーは消滅してしまうことになるであろうし、IoTが普及しているところでは物的な生活におけるプライバシーも有名無実のものとなってしまうことであろう(19)。

それから更に将来の情報社会がどのようなものになるかについては、誰にもわからない。

比較的近未来の予測として、電力網に対する執拗なサイバー攻撃に屈して、全世界がブラックアウトし、経済崩壊してしまうというシナリオ(20)、世界的な電子マネーの大規模な普及により、国家の通貨管理権限が全く有名無実のものとなり、誰かよくわからない電子的な金満家によって世界の全ての政府が支配されるようになるというシナリオ(21)、その誰かよくわからないその金満家が、実は、人間ではなく人工知能システムであるというようなシナリオ(22)、単純労働だけではなく、

かなり高度な知的労働を含め、人間が行ってきた仕事の大半がロボットや人工知能システムに奪われてしまい、収入のない圧倒的多数の人々が取引社会に参加できなくなる結果、資本主義が消滅してしまうというシナリオだけではなく(23)、生存し、そして、文化を維持する基礎的な収入を得ることさえできなくなった人類が、野生動物である類人猿と同程度まで劣化してしまうというシナリオ、あるいは、よくある世紀末的な映像作品や SF 小説の中で描かれているような、崩壊した社会の中で古代的な暴力支配だけが維持されることになるというシナリオ、情報ネットワークに接続されたサイボーグなど半機械的な改造人類だけが生き残るというシナリオなど、様々な未来予測が可能である(24)。

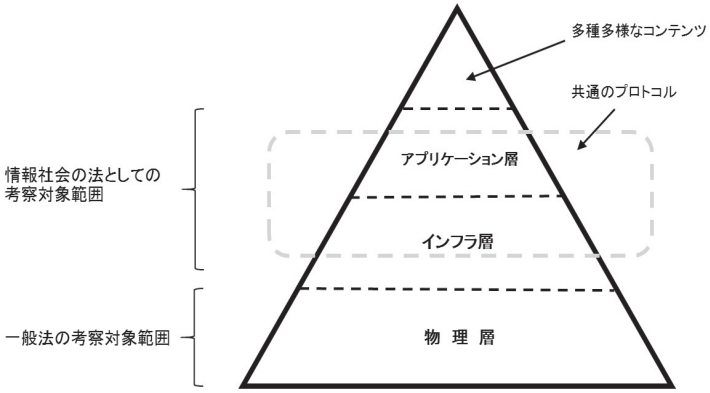
すなわち、現在の情報社会は、その担い手が人間ではなく人工知能システムに移行可能な段階にまで来てしまっている以上、1789 年のフランス革命よりもはるかに重大かつ深刻な意味で、人間社会の基本的なかたちを根本から変えてしまうような段階、または、人間社会を消滅させてしまうかもしれないような段階まで来ているということができる(25)。そのような意味での最終段階においては、自由主義の思想や社会主義の思想を含め、全てのタイプの哲学やイデオロギーが完全に無意味な存在となり得る。

これらの現象は、これまでの情報社会の進展の延長の上にある。それゆえ、その変化のベクトルを知ることは、そのベクトルを修正するための最後の救済を得るためのヒントを提供する可能性のあるものであるとも言い得る。

そこで、本稿においては、EU の法制を例にとり、EU の情報社会がどのようなものとして構想され、どのように管理されるべきものと考えられているのかを理解するために、EU における情報社会の関連法制を素描的に概観しようと思う。EU の法制を素材として選択するのは、それが EU のデジタルアジェンダにみられるような情報社会の実現に向けた統一的な目標を実現するために、組織的かつ構造的かつ意図的に構築され続けている社会的な装置の一種であるからである(26)。無論、アドホックな法令等も存在するが、それらは、全体的な観察の下においては、誤差の問題として評価し得るか否かの検討対象となし得る程度の範囲内にある。

本稿における素描の視点は、関連法制の枠組み全体をインフラ層とアプリケーション層とに分けた上で、それとは別にその枠組の中で適用されプロトコルを考察することから始まる。これは、情報処理システムにおける OS 層、アプリケーショ

ン層及びプロトコルの概念上の区分けに概ね対応するものである(27)。情報処理システムにおける物理層に該当し得る法令、例えば、電源を確保するための電力網それ自体と関連する法令、通信ポートに相当する通信衛星や地上局等の施設・設備・装置それ自体と関連する法令等については、本稿における論述の対象から外すことにした(28)。EUの判例法を含め、裁判事例は、アプリケーション層に含まれるものではなく、アプリケーション層で現実に処理されるコンテンツの実施例に過ぎないので、本稿においては特に重要なものを除き、取り扱わないこととする。しかし、このことは、事例の研究が価値の乏しいものであることを意味しない。事例は、アプリケーション層を構成する法制度の運用実態を知る手掛かりを得る重要な資料の1つであり、そして、事例の研究は、帰納法的に（名目上の制度設計ではなく）現実に運用されている制度の姿を知るための基本手法の1つである(29)。アプリケーション層の表層には、裁判事例以外にも無数の多種多様なコンテンツの群れが存在するが、これは、法規範ではなく、法規範の適用対象となる事象を構成するものである。これらの関係を模式的に示すと、以下のとおりとなる。



このように、情報システムという観点から法制度を整理して考えるという視点は、伝統的なドグマティシュとしての法学においては馴染みのないものかもしれないが、有用性という点ではその優劣があまりにも明白過ぎるので、あえて旧来のドグマティシュに対する批判は行わない。旧来のドグマティシュの中でもとりわけ

日本国の「学派」上の理論[30]は、現時点において西欧では誰からも支持されていないが、グローバルな情報社会においても誰にも使われる可能性がない。加えて、本稿における情報システムとの類比という手法は、ニクラス・ルーマン（Niklas Luhmann）の「システム論」におけるオートポイエーシス（autopoiesis）の発想とは基本的に異なるものである。EU の立法者の立法行動をオートポイエーシスによって説明することは無論可能であるが、それは、社会学的な意味における EU の立法活動の構造と運動の理解にはなり得るものであるにしても[31]、実定法という意味での法規範の機能論的な構造解析それ自体には全く寄与しない。EU の立法者は、哲学によるのではなく、EU のデジタル単一市場の円滑な稼働と EU の国際的な競争力の確保という実務的な要請をゴールとする要求仕様としてとらえた上で、その要求仕様の内容である機能（function）を実現するための法制度上の基本的な設計レベルにおける要求事項を構築している。その基本的な設計レベルの要求事項は、かなり人工的なものであり、常に実装（implementation）とその評価（assessment）と見直し（review）と制度の改善（amendment）を考慮に入れている。これは、通常のマネジメントシステムの理論における PDCA の発想と同じものであり、実務的（practical）なものであると理解することは可能である。

そのような仮説的な前提にたって考えた場合、情報システムの設計における基本的な発想との類比という視点をもつことが、最も有用性の高いものであると考える。そして、異なる政治思想及び国家体制をもつ多数の構成国によって構成されている EU において、TFEU によって示されている政治哲学上の基本的な価値観を除き、特定の政治思想や政治哲学だけが EU の立法機関において常に優位となることはあり得ないことであると考えられる。それゆえ、特定の法思想または政治思想の立場のみから EU の立法活動を説明しようとする試み、あるいは、社会主義法や国際人道法を含め、ある法学領域に属する特定の法理論のみに立脚して EU の法制全体を説明しようとする試みも常に失敗することになる。EU は、それ自体として、巨大な社会的装置の一種であるので、事実としてのその装置の構成要素を丁寧に観察し、その観察結果に基づいて素直に解析することから始めなければならないのである。

本稿においては、以上の諸要素を慎重に考慮した上で、情報社会に関する EU の法制の構造（抽象モデル）の洞察をめざす。ただし、頁数の関係等から、本稿にお

いて示す個々のEU法に対応する日本法との詳細な比較法的検討については、別の機会に譲ることとする。そして、本稿に示される立法例から何を得るかは、各人の自由に任されている。

本稿において検討対象とする法令は、2017年10月31日以前の時点において存在する法令または存在していた法令であり、それよりも後に可決または提案された法令及び法令案を含まない。本稿における公法と私法の分別は、従来の一般的な考え方に基づくものではあるが、あくまでも便宜的なものである。公法と私法とを厳格に峻別すべきであるという趣旨のものではない。

2　情報社会の制度的インフラ部分

情報社会の制度的インフラ部分に属する法令の中で共通の基本的な部分を構成するのは、情報通信それ自体を規律する法令である。日本国においては、電気通信事業法（昭和59年法律第86号）、有線電気通信法（昭和28年法律第96号）及び電波法（昭和25年法律第131号）並びにそれらの附属法令がそれに該当する。これらの情報通信それ自体を規律する法令全てに精通することなく、情報社会の法を論ずることは、原理的に不可能なことである(32)。

EUにおける情報社会の制度的インフラ部分に属する法令として基本的なものは、EU全体に共通の電気通信ネットワーク及び電気通信サービスの法的枠組みを定める指令2002/21/EC（OJ L 108, 24.4.2002, p.33）、構成国の電気通信ネットワーク及び電気通信サービスの許認可または届出並びに電気通信事業者の権利及び義務を定める指令2002/20/EC（OJ L 108, 24.4.2002, p.21）、電気通信ネットワーク及び電気通信設備へのアクセス及び相互接続を定める指令2002/19/EC（OJ L 108, 24.4.2002, p.7）、電気通信ネットワーク及び電気通信サービスに関するユニバーサルサービス及び利用者の権利を定める指令2002/22/EC（OJ L 108, 24.4.2002, p.51）、EUのレベルにおける電気通信分野の監督機関を定める規則(EC) No 2011/2009（OJ L 337, 18.12.2009, p.1）及びEU内の携帯電話ネットワークのローミングに関する規則(EU) No 531/2012である(33)。これらの基本的な法令及びそれらの附属法令による規律に基づいて定められている各構成国の

規制当局は、国内規制当局（National regulatory authorities (NRAs)）と呼ばれる。日本国の省庁では、その所管業務の相違に応じて、総務省及び経済産業省がそれに該当する。

指令 2002/21/EC の第 2 条 (a) は、「電気通信ネットワーク」について「伝送システム、並びに、適用可能なときは、スイッチングもしくはルーティング装置及びそれ以外の資源であって、運搬される情報の種類を問わず、衛星通信ネットワーク、固定式（インターネットを含め、回線及びパケット交換）及び移動体の地域ネットワーク、信号の伝送の目的で使用される範囲内で送電線システム、ラジオ及びテレビ放送のために使用されるネットワーク、並びに、ケーブルテレビネットワークを含め、有線により、無線により、光により、または、それ以外の電磁的手段により、信号を運搬することのできるものを意味する」と定義し(34)、同条 (c) は、「電気通信サービス」について「通常は有償のサービスであって、電気通信サービス及び伝送サービスを含め、その全体または主要部分において、電子通信ネットワーク上の信号の運搬を構成するものを意味するが、サービスの提供行為、または、電子通信ネットワーク及び電子通信サービスを用いて送信されるコンテントに対する管理権の行使を含まない」と定義し(35)、そして、同条 (d) は、「公衆通信ネットワーク」について、「その全体または主要部分において、公衆が利用可能な電子通信サービスの提供のために使用される電子通信ネットワーク」と定義している。これらの定義は、NIS 指令 (EU) 2016/1148 を含め、他の関連法令中においても参照・引用され、または、それらの関連法令中において同趣旨の定義条項が設けられている。

これらの情報通信の制度的インフラを定める法令は、その関連法令を含め多岐にわたるものであり、また、その後の改正が重ねられてきたことから、これらを統合して 1 つの法典（European Electronic Communications Code）としてまとめるための EU 指令の立法提案(36) があり、その審議が重ねられている。

この EU の電子通信法の統合的な改正法案は、同時に審議されている電子通信プライバシー指令 2002/58/EC の改正案(37) 及び EU の機関に適用される個人データ保護法令である規則 (EC) No 45/2001（OJ L 8, 12.1.2001, p.1）の改正案(38) とも密接に関連するものであり(39)、加えて、日本国の電気通信政策及び個人情報保護政策にも直接に大きな影響を与え得るものである。特に、電子通信分野における情報セキュリティ及び個人データ保護の制度的な枠組みの統一化をめざしてい

る点には注目すべきである。日本国の法学においては、一般に、これらの事項は、孤立した特殊分野に属するものとして、他の分野と切り離されて独立に研究対象とされることが多い。しかし、情報セキュリティの基本要素は、通信分野を含め、情報社会と関連する全ての法制において「安全性（safety）」の問題として当該法制の中にビルトインされており、また、後述のとおり、個人データのバイデザイン（by design）及びバイデフォルト（by default）の保護(40)は、情報社会における全ての法律行為及び情報処理システムにおいて必須のものとして導入されなければならないことから、それらの法律行為の（自動的に付加される）法律要件の一部となっていると同時にそれらの情報処理システムの（自動的に付加される）要求事項（requirements）の一部を構成していると理解しなければならない(41)。ただし、日本国の一般的な法学の世界においては、そのような認識は、まだ普及していない(42)。

2．1　公法

EUにおける公法としての情報社会のインフラに関する法令は、その附属法令を含めると、かなり多数ある(43)。ここでは、それらの法制の全部に触れることは不可能であるので、基本的な法制に関し、本稿の論述との関係において必要最小限の範囲内で述べることにする。なお、公法上で極めて重要な法的課題を多数含む情報セキュリティ関連、テロ対策関連及び捜査機関等における情報共有関連の事項に関しては、後述することとし、ここでは、主として、一般的な行政行為と関連するものについて述べる。

2．1．1　域内市場情報システム（IMI）

委員会決定2008/49/EC（OJ L 13, 16.1.2008, p.18）(44)は、「IMI」と略称される域内市場情報システム（Internal Market Information System）の設置を定め、この委員会決定は、その後、規則(EU) No 1024/2012（OJ L 316, 14.11.2012, p.1）(45)によって全面改正された。このIMIは、域内市場における電子商取引と関連するものではなく、域内市場に関する構成国間及び構成国と欧州委員会との間の情報交換のための基盤システム（ソフトウェアアプリケーション）の1つである。IMIは、EUの行政機関における行政情報の交換のためのシステムであるという意味で、日本国における電子政府の基本システム（e-Gov）の一部及び政府機関

の内部インフラの一部と対応するものと考えることができる。

規則 (EU) No 1024/2012 の第 3 条第 1 項は、IMI を用いる情報交換が認められる適用範囲に関し、「IMI は、個人データの交換を含め、構成国の職務権限を有する機関の間、及び、欧州連合の職務権限を有する機関と欧州委員会との間の行政協力を定める欧州連合の機能に関する条約（TFEU）の第 26 条第 2 項の意味における域内市場の分野の欧州連合の法令の実装のために必要な構成国の職務権限を有する機関の間、及び、欧州連合の職務権限を有する機関と欧州委員会との間の行政協力のために用いられる。これらの欧州連合の法令は、別紙に列挙される。」と定めている。

この別紙とは、規則 (EU) No 1024/2012 の末尾に添付される別紙のことを指し、別紙のみの改正によって、IMI を介して交換可能な行政情報の種類を追加することができる。委員会決定 2008/49/EC の採択の当初における IMI の適用範囲は、理事会指令 2006/100/EC（OJ L 363, 20.12.2006, p.141）による改正後の専門資格の認定に関する欧州議会及び理事会の 2005 年 9 月 7 日の指令 2005/36/EC（OJ L 255, 30.9.2005, p.22）及び域内市場におけるサービスに関する欧州議会及び理事会の 2006 年 12 月 12 日の指令 2006/123/EC（OJ L 376, 27.12.2006, p.36）とされていたが、その後の別紙の改正によって、IMI により交換可能な情報の種類がかなり増えており、規則 (EU) 2016/1628（OJ L 252, 16.9.2016, p.53）による改正後の規則 (EU) No 1214/2011 の別紙Ⅱでは、以下の法令に定める情報を交換可能なものとして、その適用範囲が拡大されている。

1. 域内市場におけるサービスに関する欧州議会及び理事会の 2006 年 12 月 12 日の指令 2006/123/EC（OJ L 376, 27.12.2006, p.36）の第 6 章、第 39 条第 5 項、並びに、第 15 条第 7 項（後者の条項に定める通知が指令 98/34/EC に従って行われない限り）
2. 専門資格の認定に関する欧州議会及び理事会の 2005 年 9 月 7 日の指令 2005/36/EC（OJ L 255, 30.9.2005, p.22）の第 4 条 a ないし第 4 条 e、第 8 条、第 50 条第 1 項、第 2 項及び第 3 項、並びに、第 56 条
3. 国境を越える医療における患者の権利の適用に関する欧州議会及び理事会の 2011 年 3 月 9 日の指令 2011/24/EU（OJ L 88, 4.4.2011, p.45）の第 10 条

第 4 項

4. ユーロ圏の構成国の間の陸路による国境を越えるユーロ現金輸送業務に関する欧州議会及び理事会の 2011 年 11 月 16 日の規則 (EU) No 1214/2011（OJ L 316, 29.11.2011, p.1）の第 11 条第 2 項
5. 「SOLVIT」―域内市場問題解決ネットワークの利用のための基本原則に関する 2001 年 12 月 7 日の欧州委員会勧告（OJ L 331, 15.12.2001, p.79）の第 1 章及び第 2 章
6. 役務の提供の枠組み内における従業者の配属に関する欧州議会及び理事会の 1996 年 12 月 16 日の指令 96/71/EC（OJ L 18, 21.1.1997, p.1）の第 4 条
7. 役務の提供の枠組み内における従業者の配属に関する欧州議会及び理事会の 1996 年 12 月 16 日の指令 96/71/EC の執行並びに域内市場情報システムによる行政協力に関する規則 (EU)2024/2012（IMI 規則）の改正に関する欧州議会及び理事会の 2014 年 5 月 15 日の指令 2014/67/EU（OJ L 159, 28.5.2014, p.11）の第 6 条、第 7 条、第 10 条第 3 項及び第 14 条ないし第 18 条
8. 構成国の領土から違法に移動された文化財の返還及び規則 (EU)2024/2012 の改正に関する欧州議会及び理事会の 2014 年 5 月 15 日の指令 2014/60/EC（OJ L 159 28.5.2014, p.1）の第 5 条及び第 7 条
9. 非道路移動機械の内燃機関のガス状及び粒状汚染物質排出規制及び型式承認の要件、規則 (EU) No 1024/2012 及び規則 (EU) No 167/2013 の改正並びに指令 97/68/EC の改正に関する欧州議会及び理事会の 2016 年 9 月 14 日の規則 (EU) 2016/1628（OJ L 252, 16.9.2016, p.53）の第 44 条

これらの法令名だけでは明確とは言えないが、IMI の解釈・運用のレベルの問題として、例えば、渡航文書不正防止行動計画（COM/2016/0790）(46) の「Ⅱ. 行動計画」の「1. 識別子の登録」は、欧州連合内における公文書の提示を簡素化する (EU) 2016/1191 が構成国で発給される出生証明書及び婚姻証明書が、証印のない別の認証のあるものとして承認され得ることとの関連で、「これは、例えば、公文書の真正性に関する疑いがある場合において、本人確認文書の真正性を確認するために、域内市場情報システム（IMI）を介する構成国相互の通信による行政協力を導入することによって、不正行為に対する闘いを強化するものである」としてお

り、後述の EU の対外国境警備やテロ対策の関係を含め、実質的には相当広範囲の利用が可能となっていると理解することができる。

また、規則 (EU) No 1214/2011 の第 11 条により、IMI を介した構成国間の行政協力及び構成国と欧州委員会との間の行政協力が積極的に行われるものとされた。規則 (EU) 2016/1628 による改正後の規則 (EU) No 1214/2011 の別紙Ⅰは、IMI を介した行政協力を行うことのできる適用範囲を定めているが、この行政協力の範囲もまた、今後、別紙改正によって更に拡大されることになるであろうと推測される(47)。

ところで、IMI で交換される情報の中には機密性の高いものが含まれる。その機密性の保持に関し、規則 (EU) No 1214/2011 の第 10 条第 1 項は、「各構成国は、国内立法または欧州連合の立法に従い、その構成国の IMI 関係者及び IMI 利用者に対し、職業上の秘密に関する規定、または、それ以外の均等な機密保持義務の規定を適用する」と定め、同条第 2 項は、「IMI 関係者は、別の IMI 関係者からの IMI によって交換された情報の秘密扱いを求める要請が、その IMI 関係者の権限の下で仕事をする IMI 利用者によって尊重されることを確保する」と定めている。

同様に、IMI を介して交換される情報には、大量の個人データが含まれる。そのような個人データの保護・管理に関し、規則 (EU) No 1214/2011 の第 3 章（第 13 条ないし第 17 条）は、かなり詳細な条項を設けている(48)。

しかしながら、上述のとおり、IMI による情報交換の適用範囲が拡大され、IMI が EU の機関及び構成国の行政機関との間の情報交換のためのプラットフォームとしての実質を強化するにつれ、そこで適用される情報セキュリティの基本原則及び個人データの基本原則に齟齬や矛盾が生ずる危険性があることを否定できない。これらの問題は、EU の情報社会を構成する後述のプロトコル部分に共通の問題でもあり得る。今後、IMI の現実の運用に関する実態調査を含め、更に研究が深められるべき部分である。

2．1．2　国境管理システム（SIS II、EUROSUR、EUCARIS、EURODUC）

(1)　SIS II

SIS II は、シェンゲン圏内における自由通行を可能とするために、シェンゲン圏内のシェンゲン諸国の国境通過の際の渡航文書の点検等を電子化すると同時に、シェンゲン圏における関連情報の交換・共有を強化するためのシス

テムである。

このシステム（SIS II）は、従前のシェンゲン情報システム（SIS）の運用実績を踏まえ、第2世代のシェンゲン情報システム（SIS II）の設置、運用及び利用に関する2006年12月20日の規則(EC) No 1987/2006（OJ L 381, 28.12.2006, p.4）及び2007年6月12日の理事会決定2007/533/JHA（OJ L 205, 7.8.2007, p.63）に基づいて開発・設置された(49)。これに伴い、従前の関連法令は、廃止または改正された。

規則(EU) 2016/399（シェンゲンボーダーコード）（OJ L 77, 23.3.2016, p.1）(50)は、規則(EC) No 562/2006（旧シェンゲンボーダーコード）（OJ L 105, 13.4.2006）を全面改正する法令であり、EUの陸上国境、空港及び港等の国境通過地点における渡航文書の点検・確認方法について統一的な方法を詳細に定めている。そこにおける基本的な原理は、EUの市民及び一定の電子的な通過許可証を所持する者については、可能な限り簡易な自動処理による迅速な国境通過を保証すると同時に、そうでない移民申請者等に対する審査をより精密化し、併せて、テロを防止するという目的のために、関連データベースの参照・照会等の電子的な手段の導入・利用を大きく推進する内容となっている。SIS IIは、そのような関連データベースの1つとしても位置付けられる。それゆえ、本来は、シェンゲン圏のためのシステムであったものが、現時点ではEUの構成国全体によっても活用可能な状況へと移行しつつあると考えることも可能であろう。欧州という地域は、EUの構成国によって構成されるEUの地域とシェンゲン協定に基づくシェンゲン圏とが重なっている部分があり、かつ、EFTA諸国による欧州経済領域（EEA）が別のものとして隣接しておりながら、EUとEFTA諸国との協定によりEFTA諸国でありながらEUの法制にも服し、EUのリソースを利用可能な国家が存在するというかなり複雑な構造となっているため、すこぶるわかり難い部分が多いけれども、別の国際組織を媒介者として、より大きな連携へ向けた動きもあることに留意すべきである(51)。

SIS IIによって自動処理される様々なデータの中で、査証（visa）(52)の自動処理に関しては、VIS規則(EC) No 767/2008（OJ L 218, 13.8.2008, p.60）(53)が定めている(54)。そのデータの中には生体認証データも含まれ、

後述のとおり、そのような生体認証データ（指紋データ、顔画像データ、DNA プロファイル）の処理のための技術仕様等も統一されている。ただし、ダブリン条約に基づく難民申請者の指紋データは、後述の EURODUC によって処理される。

SYS II は、「中央 SIS II（Central SIS II）」、中央 SIS II と構成国の国内システム（National SIS II）とを接続するためのインフラシステムによって構成されている。また、必要なデータ及び情報の交換に必要となる各種情報は、「SIRENE Bureaux」から提供される(55)。SIS II 全体の安全性確保のため、委員会決定 2010/261/EU（OJ L 112, 5.5.2010, p.31）が採択された。

これらの SIS II によって処理されるデータの参照・検索に関して、並びに、そのようなデータが国境警備及び構成国内の治安維持のために構成国の国境警備機関及び警察機関によって使用され、また、他の構成国の警察機関等との間で交換される場合、更に Interpol と連携する場合に関しては、指令 (EU) 2016/680（OJ L 119, 4.5.2016, p.89）(56) 及び規則 (EU) 2016/1624（OJ L 251, 16.9.2016, p.1）(57) によって定められている。これらのような制度上及びシステム上の統合または連携の強化、あるいは、対外国境及び域内国境における検問は、数年前のトルコ及び北アフリカ諸国からの大量移民問題が深刻化して以来、更に強化される傾向にある。そのための関連法令としては、例えば、規則 (EU) 2017/458（OJ L 74, 18.3.2017, p.1）(58) がある。

その後、「Entry/Exit System」の使用に関し、規則 (EU) 2016/399（シェンゲンボーダーコード）の改正提案が行われた結果(59)、規則 (EU) 2017/458 により、規則 (EU) 2016/399 の関連改正が行われた(60)。この一部改正後の規則 (EU) 2016/399 の第 8 条により、EU の対外国境においては、SIS（SIS II）、Interpol の盗難及び紛失の渡航文書のデータベース（SLTD）、並びに、盗まれ、不正使用され、紛失し及び無効とされた渡航文書の情報を含む国内データベースを参照・照会して検問が行われることとなった。第三国の国民に関しては、原則として SIS II の照会によるものとされているけれども、一定の在留資格をもつ者に関しては、規則 (EC) No 767/2008 の第 18 条に従い、Visa 情報システム（VIS）の照会によるその査証の所持者の同一性の確認及びその査証の真正性の確認によることとされている（規則 (EU) 2016/399 第

6 条参照）。

日本国の法制においては、EU の SIS II で取り扱う種類に属するデータを含め、出入国管理や公安関係において取り扱うデータは、非常に多くの法令で関係している(61)。

(2) EUROSUR

規則 (EU) No 1052/2013（OJ L 295, 6.11.2013, p.11）(62) に基づいて設けられた European Border Surveillance System（EUROSUR）は、EU の対外国境における監視カメラ等の画像情報を自動的かつ集中的に管理するための国境監視システムである。

EUROSUR の「状況映像表示機能（Situational pictures）」は、イベントレイヤ、運用レイヤ及び解析レイヤの 3 つの階層で構成され（同規則第 8 条）、また、地理的範囲に対応して、「国内状況映像表示機能（national situational picture）」（同規則第 9 条）、「欧州状況映像表示機能（European situational picture）」（同規則第 10 条）及び「共通対外情報映像表示機能（Common pre-frontier intelligence picture）」（同規則第 11 条）の 3 つのモードをもつ。この機能には共通の追跡監視ツールが具備されている（同規則第 12 条）。欧州状況映像表示機能及び共通対外情報映像表示機能は、原則として、船舶番号の確認のためにのみ使用される（同規則第 13 条第 2 項）。国内状況映像表示機能が個人データ処理のために使用される場合、個人データ保護指令 95/46/EC に服する（同規則第 13 条第 1 項）。

構成国は、それぞれ独自の国境監視制度をもち、それぞれの国境監視システムを管理・運用しているが、これら構成国のシステムが EU 内において連携して運用され、必要なデータの交換が行われるのでなければ、効果的な対外国境管理を実施することができない。なお、規則 (EU) 2016/1624 の中でも関連事項が定められている。

(3) EUCARIS

現代の陸上交通の大部分は、自動車によって行われる。移動体である自動車の自動識別と自動的な国境検問を実現するためには、自動車登録番号の統一とそのデータの情報共有及びデータ交換が必須のものとなる。欧州自動車及び運転免許情報システム（EUCARIS）は、そのためのシステムである。

このシステムは、基本的に、指令 2011/82/EU（OJ L 288, 5.11.2011, p.1）及び指令 (EU) 2015/413（OJ L 68, 13.3.2015）に基づいて運用されるが、国境警備及びテロ対策との関係では、理事会決定 2008/616/JHA（OJ L 210, 6.8.2008, p.12）(63) の別紙の定めを介して、理事会決定 2008/615/JHA（OJ L 201, 6.8.2008, p.1）(64) によっても運用される。これらの理事会決定は、現在でも有効な法令として維持されている (65) 。なお、国境を越える自動車盗と関連する法令として、理事会決定 2004/919/EC（OJ L 389, 30.12.2004, p.28）がある。

(4) EURODUC

EURODUC は、庇護に関するダブリン条約に基づいて採択された理事会規則 (EC) No 2725/2000（OJ L 316, 15.12.2000, p.1）の第 1 条第 1 項により設置された庇護申請者の指紋情報のデータベースシステムである (66) 。

EURODUC は、欧州委員会内にある管理組織である中央ユニット、及び、構成国と中央ユニットとの間で指紋の照会をするための中央データベースシステムで構成されている。構成国は、データベース内のデータの維持管理及び安全性確保について責任を負う。

2．1．3　税関システム（CIS）

理事会決定 2009/917/JHA（OJ L 323, 10.12.2009, p.20）(67) には、税関がその職務を遂行するために税関情報システム（CIS）によって個人データを自動処理する場合の関連条項が含まれている。税関は、指令 (EU) 2016/680 によって廃止された枠組み決定 2008/977/JHA（OJ L 350, 30.12.2008, p.60）(68) の中でも触れられている。そして、理事会決定 2009/917/JHA の前文 (3) は、「税関当局が共同して活動し、かつ、捜査共助及び刑事に関する司法共助の枠組みにおいて処理される個人データの保護に関する理事会の 2008 年 11 月 27 日の枠組み決定 2008/977/JHA 及び警察分野における個人データの利用に関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（以下「勧告 No R (87) 15」という。）に含まれている基本原則を考慮に入れた上で、非合法な取引に関する個人データ及びその他の関連データについて、そのような情報の管理及び送信のための新たな技術を用いて交換できるようにする手続を定めることによって、税関当局間の協力関係を強化することが必要である」と述べている (69) 。

税関情報システム（CIS）で処理されるデータの種類に関し、理事会決定2009/917/JHAの第16条第1項第1副項柱書は、「捜査ファイルからのデータは、第15条第2項に定める目的のためにのみ、税関ファイル識別データベースの中に登録される。データは、以下の類型のもののみとする」と定め、「(a) 構成国の職務権限を有する機関によって開かれた捜査ファイルの対象であり、または、対象とされたことのある個人または企業であって」、「(i) 関係する構成国の国内法により、国内法の重大な違反行為を実行している、もしくは、実行していた、または、その実行に加担している、もしくは、加担していたとの嫌疑を受けた者」、「(ii) そのような違反行為が発生したことを内容とする通報の対象とされた者」または「そのような違反行為に対する行政上または司法上の制裁の対象であった者」に該当する者と定めている。そして、同条第1項は、登録されるデータの内容として、「(a) 個人については、名前、婚姻前の旧姓、姓、旧姓及び別名、出生の日付及び場所、国籍及び性」、「企業については、商号、商取引上の名、住所、VATの識別子、消費税識別番号」と定めている。

理事会決定2009/917/JHAの第20条は「枠組み決定2008/977/JHAは、この決定内に別の定めがない限り、この決定に従って行われるデータ交換の保護について適用される」と定めており、構成国の税関当局によるデータ処理に関し、個人データ保護指令95/46/ECの特則として機能している(70)。

構成国の税関当局のシステムでは、当該構成国で入出国する者のAPI（Air Passenger Information）(71)も処理されていると推定されることから(72)、必要に応じ、税関情報システム（CIS）を介して構成国間で交換されるものと推測される。ただし、その実際の取扱いに関しては、日本国において調査・研究がほとんど行われていないので、今後、綿密な調査研究を要するものと考える(73)。

2．1．4　交通管制システム（ITS）

指令2010/40/EU（OJ L 207, 6.8.2010, p.1）(74)の第1条第1項は、「この指令は、欧州連合内における、とりわけ、構成国間の国境を越える、高度交通システム（ITS）の統一的かつ一貫性のある開発及びその利用を支援する枠組みを定め、かつ、その目的のために必要となる一般的な要件を定める」と、同条第2項は「この指令は、第2条に示す優先分野の中における活動のための仕様の開発を定め、また、それが適切なときは、必要な技術標準の開発を定める」と、同条第3項は、「こ

の指令は、道路交通の分野における ITS アプリケーション及びそのサービスに対して、並びに、それ以外の態様の交通と ITS とのインタフェイスに対して、国家安全保障に関する事項及び国防上の利益において必要な事項を妨げることなく、適用される」と、それぞれ規定している。そして、同条第 1 項第 2 項が参照する第 2 項第 1 項は、仕様及び技術標準の開発及び利用のための優先分野として、以下の分野を指定している。

― Ⅰ. 道路データ、交通データ及び旅行データの最適な利用、
― Ⅱ. 交通及び貨物運送を管理する ITS サービスの連続性、
― Ⅲ. ITS 道路の安全性及び防護アプリケーション、
― Ⅳ. 自動車と交通基盤との関連付け。

この ITS の優先事項の中で、Ⅰ及びⅡは、主として、非接触方式による自動車の識別を EU 内において一貫性のある方法で実現するために求められるものであり、また、Ⅲ及びⅣは、Ⅰ及びⅡが実現されることを前提とした上で、ITS によって実行可能な基本的な機能を応用する各種サービスの開発・提供をめざすものであると言える。これらの ITS が実現すべき機能の大部分は、日本国の高速道路においては、既に実現されているが、一般道においては、必ずしもそうであるとは言えない。

ITS は、EU における陸上運送及び海上運送の滞りのない円滑な接続を実現しようとするシステム及びそのアプリケーションの総体を指す概念である。ITS によって提供されるべきサービスのより具体的な要求仕様は、指令 2010/40/EU の第 3 条により、以下のとおり定められている。

(a) EU 全域におけるマルチモーダルな旅行情報サービスの提供；
(b) EU 全域におけるリアルタイムの交通情報サービスの提供；
(c) それが可能なときは、利用者に対して無償の、道路の安全性と関連するミニマムで統一的な交通情報の提供のためのデータ及び手順；
(d) EU 全域における相互運用可能な eCall の整合性のある提供；
(e) トラック及び業務用車両のための安全かつ防護された駐車場のための情報サービスの提供；

(f) トラック及び業務用車両のための安全かつ防護された駐車場のための予約サービスの提供

これらは、情報システムの連携運用による国境通過管理の機能を含むものであり、人間の担当官による国境検問から生ずる渋滞を避け、EU域内における経済の活性化と環境汚染の防止も制度趣旨の中に含められている。

ところで、一般に、欧州だけではなく、世界規模で自動走行自動車の開発とその実用走行のための実験が繰り返されている(75)。特に、貨物自動車の完全無人化技術が急速に進んでおり、トラック運転手の広域的な大量失業という社会問題があることもさることながら、トラック運転手の休養のためのサービスエリア情報提供の必要性が消滅するという要求仕様面での根本的な設計変更が必要となると同時に、貨物自動車のような大型自動車の暴走による悲惨な事故の防止を含め、安全性の面を強化した関連法令の見直しが求められることになるであろう。いずれにしても、このような人工知能技術の開発・応用の状況を踏まえると、今後、ITSは、自動走行自動車と人間が操縦する自動車が混在する状況を合理的に管制するためのシステムとして発展することになるであろうと予測される(76)。

他方、ITSは、自動識別された車両の移動を追跡する機能をもつことから、テロ対策等のためにも応用されることが期待されている(77)。

以上のほか、関連する法令として、通行料金の自動支払に関する規則(EU) 2015/751（OJ L 123, 19.5.2015, p.1）がある。

2．1．5　電子通行証

EU域内におけるEU市民の移動の自由（通行の自由）を更に確保するため、指令2004/38/EC（OJ L 158, 30.4.2004, p.77）が採択された。この指令に基づいて居住カード等が発行される。また、高度な専門家等のEU域内の長期滞在者のための在留資格カードと関連する法令として、理事会指令2009/50/EC（OJ L 155, 18.6.2009, p.17）があり、就学者のためのカードと関連する法令として、指令(EU) 2016/801（OJ L 132, 21.5.2016, p.21）がある。これらのカードは、一定の要件の下で、EU域内国境における通行証として使用することができる(78)。

国境検問の場合を含め、一定の要件の下で、自己の本人確認のために使用することのできる運転免許証に関しては、指令2006/126/EC（OJ L 403, 30.12.2006,

p.18)、委員会規則 (EU) No 36/2010（OJ L 13, 19.1.2010, p.1）及び委員会決定 (EU) 2016/1945（OJ L 302, 9.11.2016, p.62）がある。

他方において、理事会規則 (EC) No 2252/2004（OJ L 385, 29.12.2004, p.1）[(79)] により、電子的なパスポート内の電子チップに生体認証データを記録することが定められている[(80)]。電子的なパスポートの安全性確保に関しては、規則 (EC) No 444/2009（OJ L 142, 6.6.2009, p.1）[(81)] により、理事会規則 (EC) No 2252/2004 の一部改正が行われた[(82)]。この一部改正後の理事会規則 (EC) No 2252/2004 の第 4 条は、以下のように定めている。

第 4 条

1. データ保護の法令を妨げることなく、パスポートまたは渡航文書の発給を受ける者は、そのパスポートまたは渡航文書の中に記録されている個人データを確認する権利をもち、かつ、それが適切なときは、その訂正もしくは削除を求める権利をもつ。

2. この規則もしくはその別紙の中で定める場合を除き、または、構成国の国内法に従い、構成国から発給されるパスポートもしくは渡航文書の中で示される場合を除き、機械読取可能な方式によるいかなる情報もパスポートまたは渡航文書の中に記録されない。

3. 生体認証データは、そのような文書を発給するために収集され、パスポート及び渡航文書の記憶媒体の中に記録保存される。この規則の目的のために、パスポート及び渡航文書の中にある生体認証機能は、以下を確認するためにのみ用いられる：

(a) パスポートまたは渡航文書の真正性；

(b) パスポートまたはそれ以外の渡航文書を作成することが法律によって求められている場合、直接に利用可能な対照機能によって、その所持者の同一性。

付加的な安全性機能の確認は、国境を通過する人の移動を規律する規則に関する欧州共同体のコードを設ける欧州議会及び理事会の 2006 年 3 月 15 日の規則 No 562/2006（シェンゲンボーダーコード）第 7 条第 2 項を妨げることなく、行われる。マッチングの失敗は、それ自体としては、対外国境の通過の

目的のためのパスポートまたは渡航文書の有効性に影響を与えない。

これらの電子的なカードは、一般的な決済手段としての電子カードと同様、常に偽造または変造に相当する行為の脅威に晒されている。そのような情報セキュリティ上の問題に対処するための関連法令としては、指令98/84/EC（OJ L 320, 28.11.1998, p.54）、理事会決定2014/243/EU（OJ L 128, 30.4.2014, p.61）、理事会決定(EU) 2015/1293（OJ L 199, 29.7.2015, p.3）がある。これらのほか、上述のIMIを介した行政サービスを受けるための場合等のe-cardに関する提案が行われている(83)。

電子的な個人識別子（electronic identification (eID)）による同一性識別の信頼性確保のための制度設計に関しては、後述する(84)。

2．1．6　渡航者情報管理（PIU）

PNR指令(EU) 2016/681（OJ L 119, 4.5.2016, p.132）(85)は、航空機搭乗者の予約情報であるPNRの管理と利用の方法及びそのための構成国の組織（PIU）を定める。

同指令の前文(13)は、PIUに関し、「PNRデータは、明確性を確保し、かつ、航空会社の費用を低減することを確保するために、関連する構成国内にある単一の指定された搭乗者情報部局（以下「PIU」という。）に対して移転される。PIUは、1つの構成国の中に異なる支部局をもつことができ、また、複数の構成国が1つのPIUを共同で設置することもできる。情報共有を促進し、かつ、相互運用性を確保するために、構成国は、関連する情報交換ネットワークを介して、構成国相互間での情報交換をしなければならない」と述べている。

データそれ自体としてのPNRは、国際機関ICAO（International Civil Aviation Organization）が定める技術標準及び運用指針に準拠して各国の航空会社が設計・実装・運用するものであるが、構成国の警察機関等がPNRを入手すれば、重大犯罪の容疑者等が搭乗した航空機が当該構成国に到着する前に、その到着予定を知り、事前の対応策を講ずることができると考えられている(86)。PIUは、航空会社からPNRを入手し、必要なPNRを当該構成国の警察機関に提供し、または、他の構成国のPIUの要請に応じて、要請されたPNRを提供する。構成国のPIU間におけるデータ交換について、同規則の前文(24)は、「Europolの安全な情報交換ネットワークアプリケーション（SIENA）を介して行われるEuropolと

の連携を通じて、構成国間における PNR データと関連する情報の安全な交換が確保されなければならない」と述べている。PNR 指令 (EU) 2016/681 の第 10 条は、Europol の権限の行使が理事会決定 2009/371/JHA（OJ L 121, 15.5.2009, p.37）(87) に基づくものとされなければならない旨を定めているが、この理事会決定 2009/371/JHA は、2017 年 5 月 1 日に全部廃止され、同日から、Europol 規則 (EU) 2016/794（OJ L 135, 24.5.2016, p.53）(88) が適用（施行）されることとなったため、同日以降、Europol 規則に基づいて Europol を介する構成国間の PNR の交換が行われることになる。

EU における PNR の収集は、テロ対策及び重大犯罪対策の一環として行われる (89) 。PNR 指令 (EU) 2016/681 の第 4 条第 1 項は、構成国の PIU の職務権限について「テロリスト犯罪または重大犯罪の防止、検知、捜査または訴追」と定めている。テロリスト犯罪の定義は、理事会枠組み決定 2002/475/JHA（OJ L 164, 22.6.2002, p.3）(90) によって与えられる。重大犯罪の定義は、PNR 指令 (EU) 2016/681 の別紙Ⅱの中で定められている (91) 。

PNR は、それ自体として個人データの一種であり、かつ、必然的に機微のデータ（sensitive data）を含むことになるため、プライバシー侵害の懸念が常にある。Europol を介するデータ処理に関しては、前記 Europol 規則 (EU) 2016/794 に従ったデータ保護が行われ、構成国の PIU に関しては、個人データ保護指令 95/46/EC 及び GDPR に従って制定される各構成国のデータ保護法令に基づいて規律されることになるが、PNR 指令 (EU) 2016/681 の第 13 条は、構成国の PIU に適用される特則を定めている。なお、PNR の国際的な移転におけるデータ保護に関しては、その法令の適用に関し、疑問が生ずることが少なくない (92) 。また、PNR の収集のテロ対策措置としての有効性の評価が十分に行われているかどうかについても問題があることは、上述の API の場合と同じである。

PNR は、その基本的な部分において上述の API と重複する部分をもっている。それゆえ、重大犯罪対策のための構成国の警察機関の活動と上述の税関情報システム（CIS）を用いる構成国の税関当局の活動とが競合する部分がある。

日本国においても、各航空会社から提供される PNR は、NACCS が一元管理するとされておりながら、実際には、NACCS 経由で移転される API 及び PNR を管理・保存しているのは、日本国の税関当局及び警察機関である。

2．1．7　消費者保護データベース

1996年7月8日の理事会決議（OJ C 224, 1.8.1996, p.3）は、行政機関による法令の執行に関し、それぞれの分野を担当する構成国の行政機関の間の協力関係の構築・増進を要求している。規則(EC) No 2006/2004（OJ L 364, 9.12.2004, p.1）は、消費者保護の分野における構成国の行政機関の間の協力に特化して、その要件を定める法令である(93)。そして、規則(EC) No 2006/2004では、個々の自然人としての消費者に対する侵害行為ではなく、一定の集団としての消費者の集団的利益に対する侵害を示す概念として、「共同体内侵害（intra-Community infringement）」が用いられている（第3条(a)）。この集団的な利益の侵害は、構成国の域内国境を越えて広域的に発生し得るものである。それゆえ、EUレベルの法令に基づく規律が必要となる。そして、このような構成国の域内国境を越える集団としての消費者の利益を保護するための施策を実現するための構成国間の協力を規律するという点において、規則(EC) No 2006/2004の公法的な性格が濃厚であると言える。EUの対外国境を越える第三国との間における情報交換に関しては、第14条に規定がある。

規則(EC) No 2006/2004の第4条第1項は、構成国間における職務権限を有する行政機関及び単一の連絡部局(94)を指定すべきものと定めている。構成国間における情報交換は、この連絡部局を介して行われる。

規則(EC) No 2006/2004の第10条第1項第1文は、「欧州委員会は、第7条、第8条及び第9条に基づき欧州委員会が取得した情報を欧州委員会が記録保存及び処理する電子的なデータベースを維持管理する」と定め、同条第1項第2文は、「このデータベースは、職務権限を有する行政機関のみが照会できるようにされる」と定めている。この条項の示す同規則の第7条は、構成国の職務権限を有する行政機関が、共同体内侵害が現に発生している場合、または、共同体内侵害が発生していると疑うべき合理的な根拠がある場合において、関係する別の構成国及び欧州委員会に対してそのことを通知すべき義務、要請を受けた場合に、必要に応じて他の行政機関と協力しながら、要請された情報を収集し、これを提供すべき義務等を定め、同規則の第8条は、構成国の職務権限を有する行政機関が、別の構成国の行政機関から要請を受けた措置を、要請を受けた構成国内において遅滞なく執行すべき義務等を定め、同規則の第9条は、異なる構成国の職務権限を有する機関が市場調

査及び執行活動において協力すべき義務等を定めている。これらすべての職務の遂行に際し、構成国の職務権限を有する行政機関の間において、必要な情報交換が行われる。

そして、同条第 1 項第 3 文は、「データベースに記録保存するための情報を通知すべき彼らの責任及びそのデータベースに含められる個人データの処理に関し、職務権限を有する行政機関は、指令 95/46/EC の第 2 条(d)に従い、管理者とみなされる」と定めている。要するに、欧州委員会は、構成国の関係官庁が個人データの管理者（controller）として記録保存及び処理する個人データの物的記録場所を提供する責任だけを追い、指令 95/46/EC との関係では管理者とはならないということが示されている。しかし、EU の機関に適用される規則(EC) No 45/2001 との関係においては、個人データの管理者としての立場にあると解される。

なお、IMI を介して規則(EC) No 2006/2004 に基づく消費者保護と関連する情報が交換されるようになる見込みであることは、上述のとおりである。このような統合が更に進んだ場合、構成国の国内データベース間の直接の相互参照が行われることもあり得るのではないかと考えられる(95)。

2．2　私法

EU における私法としての情報社会のインフラに関する法令は、その附属法令を含めると、かなり多数ある(96)。ここでは、それらの法制の全部に触れることは、頁数の制限等から不可能であるので、EU の電子商取引、電子決済及び信頼サービス(97)と関連する法制に絞って述べることにする。

2．2．1　電子商取引

電子商取引指令 2000/31/EC（OJ L 178, 17.7.2000, p.1）は、EU における電子商取引の基本法令である。

電子商取引指令 2000/31/EC は、「指令（directive）」という法形式を採用している。このため、EU の構成国は、電子商取引指令 2000/31/EC に定める条項を遵守する内容の国内法を制定しなければならない。同指令の第 22 条第 1 項は、同指令に定める内容を構成国が国内法化すべき期限を 2002 年 1 月 17 日よりも前と定めている(98)。

電子商取引指令 2000/31/EC の第 1 条第 1 項は、同指令の立法目的について、「こ

の指令は、構成国間における情報社会サービスの支障のない移動を確保することによって、域内市場の適正な稼働に貢献しようとするものである」と規定している。ここでいう「情報社会サービス（information society service）」の定義は、同指令の第2条(a)にあり、「指令98/48/ECによる改正後の指令98/34/EC第1条(2)の意味におけるサービスのことを意味する」と定義している。指令98/48/EC（OJ L 217, 5.8.1998, p.18）は、EUの法令の中で用いられる用語を総括的に定める指令98/34/EC（OJ L 204, 21.7.1998, p.37）の第1条に新たな(2)を挿入して改正するものである。同改正後の指令98/34/EC第1条(2)は、「サービス（service）」の意義について、以下のとおり定義している。

(2) 「サービス」とは、情報社会サービス、換言すると、通常は、有償で、隔地者間において、電子的な手段により、かつ、サービスの受信者の個別の要求がある際に提供されるサービスのことを意味する。

この定義の目的のために：

― 「隔地者間」とは、当事者が同時に現在することなく、そのサービスが提供されることを意味し、

― 「電子的な手段により」とは、隔地者間で、（データの圧縮を含め）データの処理及び記録保存のための電子的な機器により、基本的に送信及び受信され、かつ、有線により、無線により、光学的手段により、または、それ以外の電子的な手段により、そのサービスの全体が送信され、運搬され、及び、受信されるサービスのことを意味し、

― 「サービスの受信者の個別の要求」とは、個別の要求に基づき、データの送信を介して、そのサービスが提供されることを意味する。

この定義に包摂されないサービスを示す一覧は、別紙Vに定める。

この指令は、以下のものには適用されない：

― ラジオ放送サービス、

― 指令89/552/EECの第1条(a)の適用のあるテレビ放送サービス。

そして、同改正後の指令98/34/ECの別紙Vは、隔地者間で提供されるのではないサービスの例として、電子的に処理されるものであっても当事者が現在すること

を要する医療行為、旅行代理店における航空機チケットの予約、ゲームアーケードにおけるビデオゲーム等の行為をあげ、電子的な手段により提供されるのではないサービスの例として、電子機器を使用していても物体の提供を伴う行為である銀行 ATM における現金の引き出し、そこへの出入りが電子的に行われるものであって現実の出入りを要する自動車専用道路の利用、ディスクに記録したソフトウェアの流通等のオフラインのサービスをあげ(99)、サービスの受信者の個別の要求に応じて供給されるのではないサービスとして、テレビ放送、ラジオ放送等を列挙している。

他方、電子商取引指令 2000/31/EC と電子商取引に関する他の国際的な協定等との関係及び第三国において電子商取引に関して適用される法令との関係について、同指令の前文(58)は、「この指令は、第三国内において設立されたサービスプロバイダから提供されるサービスに対して適用してはならない；ただし、電子商取引の国際的な側面に鑑み、欧州共同体の法令が国際的な規範と一貫性のあるものであることを確保することが適切である；この指令は、国際機関（就中、WTO、OECD、UNCITRAL）の中における討議の結果を妨げない」と述べている。この「WTO」とは TRIPs の協議のことを、「OECD」とは、OECD Forum on Electronic Commerce のことを、そして、「UNCITRAL」とは、UNCITRAL の The Model Law on Electronic Commerce (MLEC)(100) の協議のことをそれぞれ指すものと解される。

また、EU の個人データ保護法令との関係について、電子商取引指令 2000/31/EC の前文(14)は、電子商取引に伴う個人データの移転に関し、個人データ保護指令 95/46/EC 及び通信分野における個人データ保護指令 97/66/EC(101) が適用される旨を述べている。指令 97/66/EC は、その後廃止されており、現時点では、2002 年に採択された電子通信プライバシー指令 2002/58/EC が適用されるものと読み替えられなければならない(102)。

加えて、電子商取引指令 2000/31/EC は、消費者保護関連の公法上の規制を含め、様々な法令との関連性をもっている。それらの中で主要なものは、前文(11)に掲げられている。そのような法令の中には、消費者契約における不当な契約条項の禁止に関する理事会指令 93/13/EEC（OJ L 95, 21.4.1993, p.29）、消費者契約に関する指令 97/7/EC（OJ L 144, 4.6.1997, p.19）、不当な宣伝広告の規制に関する理事

会指令84/450/EEC（OJ L 250, 19.9.1984, p.17）[103]、消費者の信用供与契約の規制に関する指令87/102/EEC（OJ L 133, 22.5.2008, p.66）[104]、投資サービスの規制に関する理事会指令93/22/EEC（OJ L 141, 11.6.1993, p.27）[105]、パッケージ旅行の規制に関する理事会指令90/314/EEC（OJ L 158, 23.6.1990, p.59）、消費者向け製品の価格表示における消費者保護に関する指令98/6/EC（OJ L 80, 18.3.1998, p.27）、タイムシェアベースで不動産を利用する権利の購入する契約における購入者の保護に関する指令94/47/EC（OJ L 280, 29.10.1994, p.83）[106]、消費者保護のための簡易な手続による差止請求に関する指令98/27/EC（OJ L 166, 11.6.1998, p.51）[107]、製造物責任に関する理事会指令85/374/EEC（OJ L 210, 7.8.1985, p.29）[108]、消費財の販売及び保証に関する指令1999/44/EC（OJ L 171, 7.7.1999, p.12）、並びに、家庭用医薬品の販売の規制に関する理事会指令92/28/EEC（OJ L 297, 13.10.1992, p.8）[109]等の法令が含まれる。電子商取引の一方当事者が消費者に該当する場合、これらの法令が優先して適用される。日本国においても、特定商取引に関する法律（昭和51年法律第57号）、景品表示法（昭和37年法律第134号）及び消費者契約法（平成12年法律第61号）等の関連法令に精通していなければ、電子商取引と関連する電子的な法律行為を正しく法解釈できないので、基本的には、EUにおける法適用の構造と同じである[110]。

既述のところを総合すると、結局、EUの電子商取引法制を正確に理解するためには、基本的な法規範である民法及び商法並びに基本的な企業会計原則を踏まえるべきことは当然の前提とした上で、上述のWTO、OECD及びUNCITRALの関連文書を正確に理解すると同時に、電子商取引に必然的に随伴する個人データの処理と関連するEUの諸法令に精通し、かつ、後述の電子決済及び電子認証（信頼サービス）に関連する諸法令とそれらに附属する技術仕様文書を精密に理解し、加えて、EUの情報通信に関する基本法制や上述の公法に属する法制を含め、関連するEUの公法上の規制を正確に認識し、かつ、電子商取引の安全性を確保するための情報セキュリティ関連の法令及び関連文書を丁寧に咀嚼・理解する能力をもつための工夫をする必要があり、更に、欧州委員会の各種文書に示されているような今後の政策論を踏まえた確実性の高い将来展望を行う必要があることになる[111]。

以上の総論的な事項を踏まえた上で、以下、電子商取引指令2000/31/ECに定める重要な諸点について簡潔に述べる。

(1) 事前許認可を義務とすることの禁止

電子商取引指令 2000/31/EC 第 4 条第 1 項により、第 2 項に定める指令 97/13/EC（OJ L 117, 7.5.1997, p.15）(112) の適用のある場合を除き、情報社会サービスのプロバイダの業務について、構成国の関係当局の許認可を要するものとすることができない。

(2) 情報社会サービスのプロバイダの表示義務

電子商取引指令 2000/31/EC 第 5 条第 1 項により、情報社会サービスのプロバイダは、その名称、設立地の住所、プロバイダ業務の詳細、及び、商号登録等をしている場合にはその登録番号等の識別子等を表示しなければならない。日本国の法令では、特定商取引に関する法律施行規則（昭和 51 年通商産業省令第 89 号）第 8 条及び第 12 条が対応する規定である。

(3) 商業宣伝広告の通信であることの表示

電子商取引指令 2000/31/EC 第 6 条により、商業宣伝広告であること及び参加条件等を明瞭に表示しなければならない。

(4) 望まない商業宣伝広告の禁止

電子商取引指令 2000/31/EC 第 7 条により、電子メールを使用して行われる通信が受信者の望まない通信である場合、その旨を明瞭に表示しなければならない。電子通信プライバシー指令 2002/58/EC 第 13 条にも同旨のより詳細な条項がある。「望まない通信（Unsolicited communications）」に該当する電子メールとは、いわゆる「スパムメール」のことである。日本国の法令では、特定電子メールの送信の適正化等に関する法律（平成 14 年法律第 26 号）が対応する。

(5) 契約法上の法律効果の確保

電子商取引指令 2000/31/EC 第 9 条により、構成国は、電子的な手段による法律行為（特に契約）の法律効果を確保するための措置を講ずる。また、同指令第 11 条により、電子的な手段による契約締結の際の意思表示の到達の手順を確保する。日本国の関連する法令としては、電子消費者契約及び電子承諾通知に関する民法の特例に関する法律（平成 13 年法律第 95 号）がある。

(6) プロバイダの免責

電子商取引指令 2000/31/EC 第 12 条ないし第 14 条により、一定の要件を

充足する限り、データのキャッシュ、ホスティング等について、プロバイダが損害賠償責任を免れることができる。また、第15条により、プロバイダは、一般的な監視義務を負わない。日本国の関連する法令としては、特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律（平成13年法律第137号）がある。

2．2．2　電子決済

情報社会における電子的な手段を用いた電子商取引の内容が契約である場合、一般的な民法及び商法の関連条項に加え、上述の電子商取引指令2000/31/ECに定める関連条項の適用により、契約の要素である意思表示の到達時点及び契約成立時点が確定され、また、上述の関連公法によって、その契約内容及び法律効果に一定の規制が加えられる。

これとは別に、情報社会サービスが有償で提供される場合、その電子的決済に関係する規律を明確化することも重要なことである。このことは、同時に、課税の基準時を確定するという意味ももつ。

EUにおける電子決済関連法令は、多数存在し、比較的頻繁に改正が繰り返されている。それらの法令は、それ自体の法的性質としては、本質的に公法に属するものである。しかし、公法である電子決済関連法令を遵守することは、私行為である全ての電子商取引において当然の前提条件となっているという意味で、重要である(113)。

そこで、ここでは、本質的には公法に属する法令ではあるが、私法上の電子契約の枠組みを決定するものであり、それが情報社会の中で適法に機能することを支えるための重要な法規範という趣旨で、EUの電子決済に関する法令をとりあげる。電子決済に関する法令は、情報財取引ないし知的財産取引を含め、それが有償のものである限り、全ての電子商取引と関係し、かつ、その電子商取引にかかる課税と関係する。

ただし、関連法令の数が非常に多いので、それらの法令の中で特に重要と思われるものについて、簡潔にその概要を述べる。

(1) 決済サービス指令(EU) 2015/2366及び電子マネー指令2009/110/EC

決済サービス指令 (EU) 2015/2366（OJ L 337, 23.12.2015, p.35）[114] は、決済に関する基本的な法令である。同指令の第 1 条第 1 項は、構成国が、(a) 与信機関による決済、(b) 電子マネー機関による決済、(c) 郵便振替取扱機関（post office giro institutions）による決済、(d) 決済機関による決済、(e) 欧州中央銀行及び国内中央銀行、並びに、(f) 構成国またはその地域行政機関もしくは地方行政機関による決済の区別をつけるべきことを定め、また、同条第 2 項は、決済サービスにおける要件及び情報の透明性を確保すること、並びに、決済サービスの利用者及び提供者の権利及び義務を規定すべきことを定めている。情報社会サービスとの関係においては、(a) 与信機関による決済及び (b) 電子マネー機関による決済が非常に重要である。ここでいう電子マネーとは、電子的な前払式支払手段のことである。

電子マネーに関し、決済サービス指令 (EU) 2015/2366 の第 42 条は、電子マネー決済機関が提供すべき情報を定め、同指令第 63 条は、電子マネー決済機関の特例を定めている。また、同指令第 111 条により、電子マネー指令 2009/110/EC（OJ L 267, 10.10.2009, p.7）が大規模に改正された。この改正後の指令 2009/110/EC の第 3 条第 4 項及び第 5 項は、構成国が、電子マネーによる決済を承認すべきことを定めている[115]。

加えて、決済サービス指令 (EU) 2015/2366 の第 114 条により、従前の決済サービスに関する指令 2007/64/EC（OJ L 319, 5.12.2007, p.1）は、2018 年 1 月 13 日をもって廃止される。

これらの指令に対応する日本国の法令は、資金決済に関する法律（平成 21 年法律第 59 号）及び前払式支払手段に関する内閣府令（平成 22 年内閣府令第 3 号）である[116]。

(2) 送金情報規則 (EU) 2015/847

送金情報規則 (EU) 2015/847（OJ L 141, 5.6.2015, p.1）は、従前の規則 (EC) No 1781/2006（OJ L 345, 8.12.2006, p.1）の改正規則である[117]。

この規則は、資金洗浄及び国際テロとの闘いと関連する FATF 勧告に基づくものである。同規則第 1 条は、「この規則は、送金に関与する少なくとも 1 の決済サービスプロバイダが欧州連合内に設立されている場合、資金洗浄及びテロリストへの資金提供の防止、検知及び捜査の目的のために、何らかの通貨

による送金に伴う送金者及び被送金者に関する情報の提供に関して定める」と定めている。

問題は、同規則の適用範囲（どのような支払手段による送金に関する情報について同規則が適用されるか）であるが、その適用範囲を定める同規則の第 2 条第 3 項第 1 副項により、同規則は、原則として、カード決済及び電子マネー決済には適用されない。しかし、同項第 2 副項により、個人対個人の送金のために、支払用カード、電子マネー手段、携帯電話その他の前払い方式もしくは後払い方式のデジタル決済または IT 決済が使用される場合には適用される。

この規則に対応する日本国の法令は、組織的な犯罪の処罰及び犯罪収益の規制等に関する法律（平成 11 年法律第 136 号）である。

(3) 決済口座指令 2014/92/EU

決済口座指令（OJ L 257, 28.8.2014, p.214）の第 2 条(22)は、「資金（funds）」について、「銀行券、硬貨、口座預金（scriptural money）、並びに、欧州議会及び理事会の指令 2009/110/EC 第 2 条(a)に定義する電子マネーのことを意味する」と定義している。

(4) 口座決済要件(EU) No 260/2012

口座決済要件規則(EU) No 260/2012（OJ L 94, 30.3.2012, p.22）は、口座振込、口座振替、自動引落による決済と関係する技術上及び業務上の要件を定めている。その適用対象は、決済サービス指令(EU) 2015/2366 の第 1 条第 1 項に定めるところと同じであり、電子マネー機関による決済を含めている。

以上のような電子的な決済は、その決済システムそれ自体としての情報セキュリティが確保されており、かつ、資金決済に伴う個人データの保護が確保されたものでなければならない。

それらに加え、電子的な決済の適法性要件の充足という観点からも、情報社会における適正な課税の確保という観点からも、当該決済が実行される当事者の本人性（authenticity）が保証されなければならない。これは、当該決済システムによって実行される決済処理の安全性の問題である。ところが、決済機関自身では、当該決済機関以外の決済当事者の本人性を確認することができない。それゆえ、第三者による本人確認の仕組みが必要となる。情報社会において、そのような本人確認の

ための電子的な仕組みを提供するのは、後述の信頼サービス（trust service）の役割である。

金融機関等の決済機関自身による顧客の本人確認と関係する日本国の法令としては、犯罪による収益の移転防止に関する法律（平成 19 年法律第 22 号）がある(118)。同法第 2 条第 2 項は、「特定事業者」を定義しており、その中に金融機関が含まれる。同法の細則として、犯罪による収益の移転防止に関する法律施行令（平成 20 年政令第 20 号）、犯罪による収益の移転防止に関する法律施行規則（平成 20 年内閣府・総務省・法務省・財務省・厚生労働省・農林水産省・経済産業省・国土交通省令第 1 号）、犯罪による収益の移転防止に関する法律の規定に基づく事務の実施に関する規則（平成 19 年国家公安委員会規則第 9 号）がある。

2．2．3　信頼サービス

情報社会における文書は、基本的に、電子化された文書（電磁的記録）である。

電磁的記録である電子文書に関しては、それが紙の文書と均等な法的効果を与えられること（書面性の要件の充足）、その作成者の同一性を識別可能なこと（真正性の確保）が重要である。これらの要件を充足するための基本的な法的仕組みは、電子署名等の電子的な証明手段及び認証方法に関する法令によって提供される。

他方において、電子署名は、それが何らかの電子的な処理の実行によって機能するものであり、通常は電気通信回線を介してネットワーク上で実行されるものであることから、極めて高度な情報セキュリティ上の要求事項を満たすものでなければならない。そのための技術的手段として、電子的な暗号技術が用いられるのが通例である。そして、そこで用いられる暗号技術が正常に機能していることを保証するための第三者機関による電子的な保証の仕組みが必要となる（電子認証・電子証明）(119)。この保証は、使用される暗号技術や通信技術の仕様及び設定により程度の差がある。それゆえ、一般に、情報セキュリティ上の安全性の程度と電子署名における真正性の確実性の程度とは、正比例する関係にある(120)。その情報セキュリティ上の安全性の評価においては、情報セキュリティ上のリスクの存在・態様・程度を正確に理解・測定できなければならない。その意味において、電子署名及び電子証明と関連する法令を解釈・運用しようとする場合、後述の情報セキュリティ及びサイバー犯罪に関する基本的な法令の理解が必須のものとなる(121)。

(1) 電子署名指令 1999/93/EC

EU における電子署名及び電子認証に関する基本的な法令は、電子署名のための欧州共同体の枠組みに関する欧州議会及び理事会の 1999 年 11 月 13 日の指令 1999/93/EC（OJ L 13, 19.1.2000, p.12）であった。

この電子署名指令 1999/93/EC は、電子識別規則 (EU) No 910/2014（OJ L 257, 28.8.2014, p.73-114）の第 50 条により、2016 年 7 月 1 日をもって廃止された。

(2) 電子識別規則 (EU) No 910/2014

電子識別規則 (EU) No 910/2014 の第 1 条は、同規則の目的に関し、「他の構成国の通知された電子識別スキームの範囲内にある自然人及び法人の電子識別手段を構成国が承認する場合における要件を定め」、「信頼サービスのための規定、とりわけ、電子的なやりとりのための規定を定め」、そして、「電子署名、電子シール、電子タイムスタンプ、電子文書、電子登録配達サービス及び Web サイト確認のための認証サービスに関する法的枠組みを設ける」ものとしている。

同規則が採用した手法は、互換性のない電子署名手段・電子証明手段を異なる構成国間で相互運用できるようにするため、各構成国の独自の電子署名手段・電子証明手段に関する基本的な仕様に関する情報を欧州委員会のデータベースに集め、そこに登録され、EU 官報によって公示された他の構成国の電子識別スキームについて、それぞれの構成国が承認し、その承認を受けた電子識別スキームに基づくものである限り、適格電子証明として扱うという方法である。このような手法を採用することにより、各構成国の行政機関や企業が新たな技術的手段を開発・導入することを妨げることなく、電子的な証明の相互運用を可能とすることができ、それによって、EU 域内国境を越える電子的なやりとりを組成する電子文書や電子的処理の真正性及び信頼性の共通の制度的基盤を確保することを目指している。構成国は、欧州委員会に対して自国の電子識別スキームを通知すべき義務を負わないが、同規則に基づく相互承認の手続による利益を得るためには、その電子識別スキームを通知しなければならない。この電子識別スキームの適格性、保証レベル、通知方法等については、同規則第 7 条ないし第 9 条が定めている。

通知される電子識別スキームは、それ自体として、十分に安全性が確保された

ものでなければならないため、その安全性が欠落している場合またはその安全性が損なわれた場合の法的責任に関し、同規則第 10 条及び第 11 条は特則を定めている。

信頼性の程度に関しては、相当する国際標準に依拠しつつ、「低（low）」、「十分（substantial）」及び「高（high）」の 3 つのレベルを使用可能なものとし、問題となる電子的なやりとりにおける機密性の程度に応じてそれらを使い分けるという基本方針が採用されている。

この信頼性の程度を証明するためのサービス「信頼サービス（trust service）」であり、そのサービスを提供する組織が「信頼サービスプロバイダ（trust service provider）」である。信頼サービスの概念は、「デフォルトでは信頼性がゼロであること」を当然の前提とするモデルであり、いわゆる「性善説」的な発想は微塵も含まれていない。信頼サービスプロバイダが提供する業務の範囲について、同規則の第 3 条 (16) は、「(a) 電子署名、電子シールもしくは電子タイムスタンプ、電子登録配達サービス、及び、それらのサービスと関連する認証明書の作成、検証及び有効性確認」、「(b) Web サイト確認証明書の作成、検証及び有効性確認」または「(c) 電子署名、電子シールもしくはそれらのサービスと関連する証明書の保存」のいずれかであると定義している。

信頼サービスプロバイダは、情報社会における電子的なやりとり（electronic transaction）の真正性等の電子的な証明という重要な職務に従事するものであることから、同規則第 19 条は、特別の安全性確保義務を定め、また、同規則第 13 条及び第 15 条は、その法的責任に関する特則を定めている。また、同規則第 15 条は、障害者のアクセスに関する国連条約に基づき、障害者への適切な対応に関して定めている。更に、同規則第 17 条及び第 20 条、により、信頼サービスプロバイダは、当該プロバイダが所在する構成国の監督機関による厳格な監督に服さなければならない。

適格信頼サービスプロバイダが提供する適格信頼サービスについては、同規則第 23 条により、EU 信頼マークが付与される。同規則 24 条は、適格サービスプロバイダの業務について定めている。

そして、同規則第 25 条ないし第 48 条は、電子署名、電子シール、電子タイムスタンプ、電子登録配達サービス、Web サイト確認、電子文書の順に分けて、

電子証明と関連する各論的な事項について定めている。

(3) 電子識別規則 (EU) No 910/2014 の細則

電子識別規則 (EU) No 910/2014 を実装するためのより具体的な要求仕様は、同規則に基づく委任により、同規則の細則である委員会実装決定 (EU) 2015/296（OJ L 53, 25.2.2015, p.14）[122]、委員会実装決定 (EU) 2015/1505（OJ L 235, 9.9.2015, p.26）[123]、委員会実装決定 (EU) 2015/1506（OJ L 235, 9.9.2015, p.37）[124]、委員会実装決定 (EU) 2015/1984（OJ L 289, 5.11.2015, p.18）[125]、委員会実装決定 (EU) 2016/650（OJ L 109, 26.4.2016, p.40）[126]、委員会実装規則 (EU) 2015/806（OJ L 128, 23.5.2015, p.13）[127]、委員会実装規則 (EU) 2015/1501（OJ L 235, 9.9.2015, p.1）[128] 及び委員会実装規則 (EU) 2015/1502（OJ L 235, 9.9.2015, p.7）[129] によって定められている。

これらの細則を通じて、情報セキュリティの確保に関しては、ISO/IEC 27001（ISMS 適合性評価基準）に定める標準に準拠すべきことが明確にされている。また、個人データ保護に関しては、個人データ保護指令 95/46/EC 及び規則 (EC) No 45/2001 に従うべきことが明確にされている[130]。

EU における電子署名・電子認証・電子文書に関する法制は、以上のように統合されたのであるが、今後、仮想通貨を含む電子決済における証明の問題に対応する法令が必要になると見込まれること、他方において、量子コンピュータ技術や人工知能技術の応用により、現在の電子署名・電子認証・電子文書の技術的基盤となっている暗号技術の多くが反故にされてしまう危険性が高いため、そのような事態に対応する新たな法的枠組みが必要となること、そして、自律型のロボットを含め、自律的な人工知能システム間の電子証明の仕組みが、人間によっては全く理解できない要素の組み合わせによって実行されるような事態（人間がその証明の数学的解析を実施し、検証することが非常に困難または不可能となるような事態）が当該システムによって自動生成され得ること[131] などを併せ考えると、今後も、この分野における EU の法制は、激しく変化し続ける可能性があることに十分に留意すべきである。

このような近未来的な検討課題が存在することを認識した上で、現行の EU の

電子署名及び電子認証に関する日本国の法令としては、電子署名及び認証業務に関する法律（平成 12 年法律第 102 号）、電子署名及び認証業務に関する法律施行令（平成 13 年政令第 41 号）、電子署名及び認証業務に関する法律施行規則（平成 13 年総務省・法務省・経済産業省令第 2 号）、国家公安委員会電子署名規則（平成 15 年国家公安委員会規則第 7 号）、電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律（平成 14 年法律第 153 号）、電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律施行令（平成 15 年政令第 408 号）、電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律施行規則（平成 15 年総務省令第 120 号）がある。

また、現行の EU の電子文書に関する日本国の関連法令としては、「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」（平成 16 年法律第 149 号）と「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律の施行に伴う関係法律の整備等に関する法律」（平成 16 年法律第 150 号）、工業標準化法に係る民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律施行規則（平成 17 年厚生労働省・農林水産省・経済産業省・国土交通省令第 7 号）、中小企業等協同組合法に係る民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律施行規則（平成 17 年内閣府・財務省・厚生労働省・農林水産省・経済産業省・国土交通省令第 4 号）、外国為替法令に係る行政手続等における情報通信の技術の利用に関する法律施行規則（平成 16 年内閣府・総務省・財務省・文部科学省・厚生労働省・農林水産省・経済産業省・国土交通省・環境省令第 2 号）、内閣府の所管する金融関連法令に係る民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律施行規則（平成 17 年内閣府令第 21 号）、個人情報保護委員会の所管する法令に係る行政手続等における情報通信の技術の利用に関する法律施行規則（平成 26 年特定個人情報保護委員会規則第 2 号）等がある。

（続く）

注

(1) 最近刊行された書籍の中では、トマス・リッド（松浦俊輔訳）『サイバネティクス全史―人類は思考するマシンに何を夢見たのか』（作品社、2017）及びエミリー・アンテス（西

田美緒子訳）『サイボーグ化する動物たち―ペットのクローンから昆虫のドローンまで』（白揚社、2016）が興味深い。

(2) 夏井高人『ネットワーク社会の文化と法』（日本評論社、1997）では、1997年当時における世界の状況を踏まえ、それから後の時代に生起し得る法的課題を検討した。ところが、電子技術の発展の速度は著しく、当時の予測では50年程度先のこととして漠然と考えていたことがほぼ全て実現されてしまっている。逆から言えば、その時点では「今後の課題」として提示した問題の多くが現実に対処しなければならない検討課題となってしまっている。

(3) 個人データ保護指令95/46/ECの参考訳・改訂版は、法と情報雑誌2巻5号332～365頁にある。

(4) 電子署名指令1999/93/ECは、電子識別規則(EU) No 910/2014によって廃止された。

(5) 指令2002/58/ECの参考訳・改訂版は、法と情報雑誌2巻5号158～187頁にある。

(6) 情報社会指令2001/29/ECの参考訳は、同誌2巻11号1～26頁にある。

(7) サイバー犯罪条約（ETS No.185）の説明書の参考訳は、同誌1巻6号1～132頁にある。

(8) COM(2015) 192 final、COM/2017/0228 final

(9) A Digital Single Market Strategy for Europe - COM(2015) 192 final参照

(10) 電子識別規則(EU) No 910/2014の参考訳は、法と情報雑誌2巻10号147～196頁にある。

(11) NIS指令(EU) 2016/1148の参考訳・改訂版は、同誌2巻8号120～163頁にある。

(12) 規則(EU) 2016/679（GDPR）の参考訳・改訂版は、同誌2巻5号188～331頁にある。

(13) Luciano Floridi & Phyllis Illari (Eds.), The Philosophy of Information Quality, Springer (2014)が参考になる。なお、後掲ハイブリッドな脅威報告書（JOIN (2017) 30）においても重点的な課題の1つとして述べられている。

(14) 前掲『ネットワーク社会の文化と法』参照

(15) 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。

(16) ハイブリッドな脅威報告書（JOIN (2017) 30）の参考訳は、同誌2巻8号91～119頁にある。

(17) ENISA, Securing the Cyber Space in the Light of State Sponsored Activities, May 2017

(18) William D. Bryant, International Conflict and Cyberspace Superiority: Theory and Practice, Routledge (2017)

(19) James Scott, Metadata: The Most Potent Weapon in This Cyberwar: the New Cyber-kinetic-meta War, Createspace Independent Publishing Platform (2017)、IEEE, Security certification and labelling in Internet of Things, DOI: 10.1109/WF-IoT.2016.7845514

(20) Mason Rice & Sujeet Shenoi (Eds.), Critical Infrastructure Protection X: 10th IFIP WG 11.10 International Conference, ICCIP 2016, Arlington, VA, USA, March 14–16, 2016, Revised Selected Papers, Springer (2016)

(21) Michael Brenner, Kurt Rohloff, Joseph Bonneau, Andrew Miller, Peter Y. A. Ryan, Vanessa Teague, Andrea Bracciali, Massimiliano Sala, Federico Pintore, Markus Jakobsson (Eds.), Financial Cryptography and Data Security: FC 2017 International Workshops, WAHC, BITCOIN, VOTING, WTSC, and TA, Sliema,

Malta, April 7, 2017, Springer (2017) として刊行される予定の同ワークショップにおける議論が参考になる。

(22) 擬似 AI または似非 AI ではなく、真の AI の本質は、人間により予測・制御できない自律性（autonomous）をもつということに尽きる。いわゆる「AI ネットワーク」に関する議論の大部分は、真の AI とは関係がない。

(23) Nick Bostrom, Superintelligence: Paths, Dangers, Strategies, Oxford University Press (2016)、Martin Ford, Rise of the Robots: Technology and the Threat of a Jobless Future, Basic Books (2015)

(24) 人工知能（AI）または自律ロボットによる影響との関係については、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 巻 4・5 号 175～212 頁 (2017)、同「ロボット法の制定を求める欧州議会決議 [参考訳]」法と情報雑誌 2 巻 5 号 438～492 頁 (2017) の冒頭部分で述べたとおりである。脳科学の動きを踏まえた応用研究に関しては、人工知能学会誌 32 巻 6 号 (2017) に収録された関連論考がある。

(25) ロボットまたは人工知能の権利主体性に関しては、Nathalie Nevejans, Traité de droit et d'éthique de la robotique civile, Les Etudes Hospitalières édition (2017)、Markus Häuser, Do robots have rights? The European Parliament addresses artificial intelligence and robotics, CMS News 06.04.2017 が参考になる。

(26) 関連するものとして、植月献二「欧州デジタルアジェンダ―2013～2014 年の重点分野―」外国の立法 254–2 号 8～9 頁 (2013)、佐々木勉「欧州における電気通信政策の新展開と理論動向 (1)」Infocom review 33 号 37～57 頁 (2004)、同「欧州における電気通信政策の新展開と理論動向 (2)」Infocom review 34 号 116～146 頁 (2004) がある。

(27) 情報セキュリティの分野においても、同様の階層（レイヤ）に分けてリスク及びインシデント対応が検討されるのが通例である。そのような情報セキュリティの仕組みは、主として技術的な対応及び管理運用面の対応によって構成されるものであるが、情報社会に関する法制は、同様の目的のための法的対応の部分を含むものであるので、一体として考察されなければならない場合が多々ある。このことは、個人データ保護やプライバシー保護の場面においても全く変わらない。それゆえ、情報セキュリティと関連する考察を欠くような法学研究及びその研究結果は、ほぼ無力または無意味なものであることが決して珍しくない。これらは、統合的に検討・考察の対象とされなければならず、職業人としては、それが可能な者のみがその分野における研究に従事すべきである。

(28) 情報社会と直接または間接に関係する物体を規律する法令、例えば、施設・設備の所有権、使用権及び担保権等に関する法令は、構成国の民法等の一般私法である。これらについては、例えば、電波や放射線等と関連する特別の規制や制限に服するような部分を除き、情報社会とは関係のない施設・設備におけるものと基本的に変わるところがない。情報社会の担い手である企業等に関しても同様であり、構成国の商法や会社法等の一般私法が適用される。ただし、通信事業者に関しては、競争法上及び消費者保護法上の特別の規制に服するのが通例である。これら経済法等の領域に属する問題に関しては、本稿においては検討を割愛した。

(29) それゆえに、特定の社会思想、法哲学、法学上の解釈論に無理にあてはめることを前提とするような事例研究は、厳に慎まなければならない。あくまでも即物的な姿勢が望まれる。

(30) 個人データの保護と関連するいわゆる「自己情報コントロール権」なる概念は、日本国にのみ存在する贋作的な概念であり、EU にも米国にも存在しない。このことは既に何度も述べてきたとおりであるので、本稿においては繰り返さない。一般に、日本国の学術・

文芸においては、意図的な概念の贋作、あるいは、意図的なものではないにしろ誤解に起因する結果的な贋作的概念がしばしば発生する。その例の 1 つとして、南画の分野における「四君子」なる概念の贋作の可能性については、夏井高人「四君子考」明治大学教養論集 526 号 5～23 頁 (2017) の中で述べた。一般に、ある事象の構造を描写し、その構造に何らかの名称を付すことは、通常の学術に該当するもので、特に異とすべきものではなく、それ自体としては学問の自由の範囲内に属する。しかし、特定の国または地域の法制度を日本国で紹介する際、ある意図に基づき、実在しない法制度や学説等をあたかも存在するものの如く述べれば、それは概念の贋作の範疇に属することになる。

(31) 例えば、欧州委員会（European Commission）にみられるような EU の官僚組織の自動的な肥大化運動の社会学的な解析や説明等のためには適しているかもしれない。

(32) テレビ放送やラジオ放送は、当該国家によって統制された内容の放送番組を一方的に流すことによって各国政府による国民の思想統制のために、あるいは、国際的な宣言工作のために利用可能な一方向の情報伝達手段の 1 つとして長らく利用されてきたもので、それらの放送を規律するために各国の放送法が存在する。しかし、このようなテレビ放送やラジオ放送は、本稿の対象とする情報社会とは無関係のものである。

(33) 他に関連する法令として、無線装置及び電気通信端末の互換性に関する指令 1999/5/EC（OJ L 91, 7.4.1999, p.10–28）がある。

(34) 指令 2002/21/EC は、情報通信に関する基本的な枠組みを定める法令であり、その定義条項の中で、テレビ放送やラジオ放送を含め、通信を実現するための具体的な手段の相違を問わないという姿勢を示している点には留意すべきである。俗に「通信と放送の融合」なる概念が唱えられることがあるが、そのような「融合」なる概念は、理論的にも実際的にも成立し得ない。テレビ放送及びラジオ放送を含め、情報通信のための具体的な手段は、最初から最後まで常に同一の範疇に属する情報通信手段の一種である。「融合」は、異なる範疇に属するものの混合の場合に用いられるべきであり、もともと同一の範疇に属するものが融合することはあり得ない。ただ、テレビ放送やラジオ放送の特性を示すとすれば、それは、一方向の通信手段の一種であり、かつ、国民の思想統制や対外的な宣伝工作等のために国家によって使用されることを主たる目的として存立しているという点に求められる。このことは、テレビ放送やラジオ放送の内容に決定的な影響をもつ大規模な宣伝組織や宣伝機関（特に国営の組織・機関）や国営の新聞機関等についても原則として妥当する。

(35) この定義は、電子通信サービスとは、信号の運搬それ自体、すなわち、いわゆるキャリアとしての業務と、キャリアによる信号の運搬というインフラ構造の上に構築される各種情報サービス（かつての VAN 等の付加価値サービス、インターネットサービスプロバイダ（ISP）による各種サービス提供等）とは異なるものだとの観念を基礎としている。これは、おおまかに言えば、旧電気通信事業法上の一種事業者と二種事業者との関係に対応するものである。このような区別は、国家統治の基本部分にかかわるものであり得る情報通信の分野における特定の企業による独占によって国家統治上の重大なリスクが生ずることを避けるという趣旨も含まれているが、純粋に企業活動という側面に限定して考察するとしても、例えば、仮に情報通信のためのインフラ部分の通信事業者と巨大なクラウドサービス企業が実質的に同一企業である場合、このような区別は有名無実のものとなると同時に、競争法（独占禁止法）上の問題が直ちに生ずることになることは、明らかである。これらに関連する文献として、大野幸夫「VAN 取引の法律問題」ジュリスト増刊ネットワーク社会と法 63～70 頁 (1988)、佐藤真紀「EU の電気通信政策と競争法

—EU 電子通信市場における競争法の役割—」慶應法学 35 号 205～231 頁 (2016)、西村暢史「欧州情報通信政策における競争法的思考」比較法雑誌 45 巻 1 号 45～86 頁 (2011) がある。

(36) COM(2016) 590 final

(37) 指令 2002/58/EC の改正案 COM(2017) 10 final の参考訳は、法と情報雑誌 2 巻 4 号 195～248 頁にある。

(38) 規則 (EC) No 45/2001 の改正案 COM/2017/08 final の参考訳は、法と情報雑誌 2 巻 4 号 249～354 頁にある。提案理由の第 7 章にある改正案第 62 条の説明として、「他の欧州連合の法令が本条を参照する場合の構成国の監督官との連携した監督の枠組み内における EDPS の義務を定める。それは、単一の連携した監督のモデルの実装を求める。そのモデルは、Eurodac、シェンゲン情報システムⅡ、Visa 情報システム、または域内市場情報システムのような大規模な IT システムの連携した監督のために用いられ得るだけではなく Europol のように、EDPS と構成国の機関との間の特別の連携のモデルが設けられている場合において、幾つかの欧州連合の部局の監督のためにも用いられ得る。欧州データ保護委員会は、その委員会内での効果的で連携した監督を確保するための単一の場として機能しなければならない」とある部分は、極めて重要である。

(39) EDPS 意見書（Opinion 5/2017）及び EDPS 意見書（Opinion 3/2015）では、GDPR との同時適用（施行）の重要性が強調されている。EDPS 意見書（Opinion 5/2017）の参考訳は、法と情報雑誌第 2 巻第 6 号 177～216 頁にある。EDPS 意見書（Opinion 3/2015）の参考訳は、法と情報雑誌第 2 巻第 6 号 217～238 頁にある。

(40) 堀部政男・一般財団法人日本情報経済社会推進協会（JIPDEC）編『プライバシー・バイ・デザイン』が参考になる。

(41) 分野の別を問わず、日本国法の解釈・運用においても、これらの点を看過または無視することは許されない。なお、裁判所、検察庁及び警察関係の官庁等においては、近時、情報社会の分野の範疇に含まれる法的課題及び関連電子技術に関する調査研究にかなり積極的になってきている。法学全般にわたり、法律実務家が法学理論家を既に凌駕していると評価することも可能である。

(42) EU における近時の情報通信法制一般に関しては、寺田麻佑『EU とドイツの情報通信法制—技術発展に即応した規制と制度の展開』（勁草書房、2016）がある。

(43) 日本国の行政法学におけるこの分野の網羅的な比較法研究は、皆無である。

(44) 委員会決定 2008/49/EC の参考訳は、法と情報雑誌 2 巻 9 号 84～92 頁にある。

(45) 規則 (EU) No 1024/2012 の参考訳は、同誌同号 93～114 頁にある。

(46) 渡航文書不正防止行動計画（COM/2016/0790）の参考訳は、法と情報雑誌 2 巻 9 号 473～488 頁にある。

(47) 規則 (EU) No 1214/2011 の第 29 条第 3 項は、消費者保護法の執行のために職責を負う国内機関の間の協力に関する欧州議会及び理事会の 2004 年 10 月 27 日の規則 (EC) No 2006/2004（消費者保護協力規則）（OJ L 364, 9.12.2004, p.1）に従って設置される消費者保護協力システム内、並びに、IMI 内における行政協力への適用拡大が予定されていることを明らかにしている。

(48) 委員会決定 2008/49/EC に基づいて採択された IMI で交換される個人データの保護に関する委員会決定 2008/49/EC は、規則 (EU) No 1214/2011 の第 27 条により廃止された。

(49) SIS II に関しては、Libor Klimek, European Arrest Warrant, Springer (2015) p.138 の脚注内に解説がある。また、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) が参考になる。

(50) 規則 (EU) 2016/399（シェンゲンボーダーコード）の参考訳は、法と情報雑誌 2 巻 7 号 1～82 頁にある。

(51) 例えば、NATO との連携に関しては、前掲ハイブリッドな脅威報告書（JOIN (2017) 30）が参考になる。

(52) EU における査証（visa）の発給に関する法令としては、規則 (EC) No 810/2009（Visa コード）（OJ L 243, 15.9.2009, p.1）がある。

(53) VIS 規則 (EC) No 767/2008 の参考訳は、法と情報雑誌 2 巻 5 号 1～59 頁にある。VIS 規則 (EC) No 767/2008 は、規則 (EU) 2016/399（シェンゲンボーダーコード）によって一部改正されている。

(54) 国境警備を含め、警察機関等の国際協力に関しては、Maria Fletcher & Ester Herlin-Karnell, Claudio Matera (Eds.), The European Union as an Area of Freedom, Security and Justice, Routledge (2016) が参考になる。

(55) 委員会決定 2008/333/EC（OJ L 123, 8.5.2008, p.1）参照

(56) 指令 (EU) 2016/680 の参考訳は、法と情報雑誌 2 巻 1 号 41～140 頁にある。

(57) 規則 (EU) 2016/1624 の参考訳は、同誌 2 巻 6 号 1～98 頁にある。

(58) 規則 (EU) 2017/458 の参考訳は、同誌 2 巻 7 号 83～96 頁にある。

(59) COM(2016) 196 final

(60) 規則 (EU) 2017/458 による改正後の規則 (EU) 2016/399 の第 8 条の参考訳は、法と情報雑誌 2 巻 7 号 97～103 頁にある。

(61) 規則 (EU) 2016/399（シェンゲンボーダーコード）と直接に対応する日本国法は、出入国管理及び難民認定法（昭和 26 年政令第 319 号）である。また、規則 (EU) 2016/399 と密接に関連する PNR に関して対応する日本国法は、出入国管理及び難民認定法施行規則（昭和 56 年法務省令第 54 号）、とりわけ、同施行規則第 52 条（報告する義務）並びに旅券法（昭和 26 年法律第 267 号）及び旅券法施行規則（平成元年外務省令第 11 号）である。このほか、関連する法令として、航空法（昭和 27 年法律第 231 号）、空港法（昭和 31 年法律第 80 号）、港則法（昭和 23 年法律第 174 号）、河川法（昭和 39 年法律第 67 号）、海上運送法（昭和 24 年法律第 187 号）、海上運送法施行規則（昭和 24 年運輸省令第 49 号）、国際海上物品運送法（昭和 32 年法律第 172 号）、船員法（昭和 22 年法律第 100 号）、船員法施行規則（昭和 22 年運輸省令第 23 号）、船舶職員及び小型船舶操縦者法（昭和 26 年法律第 149 号）、船舶法（明治 32 年法律第 46 号）、道路運送車両法（昭和 26 年法律第 185 号）及び貨物自動車運送事業法（平成元年法律第 83 号）がある。

(62) 和訳として、加藤浩訳「欧州国境監視システム（EUROSUR）を創設する 2013 年 10 月 22 日の欧州議会及び理事会の規則 (EU)No 1052/2013」外国の立法 262 号 32～47 号 (2014) がある。

(63) 理事会決定 2008/616/JHA の参考訳は、法と情報雑誌 2 巻 9 号 116～200 頁にある。

(64) 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。

(65) 第 9 次効果的で真に安全な欧州連合に向けた月次進捗報告書（COM(2017) 407 final）の「Supporting the full implementation of EU measures」の項参照

(66) 佐藤以久子「欧州共通の庇護制度（CEAS）」桜美林論考法・政治・社会 5 号 63～81 頁 (2014)、岡部みどり「出入国管理のための対外政策に関する分析―EU 近隣諸国政策との関連に焦点を当てて」上智ヨーロッパ研究号 7 号 89～105 頁 (2015) が参考になる。

(67) 理事会決定 2009/917/JHA の参考訳は、法と情報雑誌 2 巻 2 号 1～30 頁にある。
(68) 枠組み決定 2008/977/JHA の参考訳は、同誌 2 巻 1 号 141～169 頁にある。
(69) 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。
(70) 理事会決定 2009/917/JHA は、その後の法令によって廃止されていないので、現時点においても有効であり、2018 年 5 月に一般データ保護規則 (EU) 2016/679（GDPR）が適用（施行）された後においても GDPR の特則として機能し続けるものと解される。
(71) API は、渡航者を識別するための情報である。航空機の搭乗者の予約情報は、PNR（Passenger Name Record）と呼ばれ、API と共通する部分（基本的な識別子の部分）とそれ以外の部分とがある。これらの情報は、テロ対策の上でも重要なものと考えられている。ただし、これらの情報が実際にテロ対策において効果的かつ合理的に用いられたか否かについての有用性評価は、これまでのところ明らかにされていない。API の処理と関連する指令 2004/82/EC（OJ L 261, 6.8.2004, p.24）の参考訳は、法と情報雑誌 2 巻 5 号 60～70 頁にある。API 及び PNR を含め、搭乗者データのプライバシー問題に関しては、Olga Mironenko Enerstvedt, Aviation Security, Privacy, Data Protection and Other Human Rights: Technologies and Legal Principles, Springer (2017) が参考になる。
(72) 日本国においては、API の管理及び処理は、基本的に、税関の所管業務とされている。
(73) CIS で処理されるデータの開示を求める場合の運用指針として、CIS Supervision Coordination Group, A Guide for Exercising the Right of Access to the Customs Information System (December, 2015) が公表されている。
(74) 指令 2010/40/EU の参考訳は、法と情報雑誌 2 巻 9 号 27～47 頁にある。
(75) 2017 年 1 月 27 日に採択された前掲ロボット法の制定を求める欧州議会決議 2015/2103(INL)（A8–0005/2017）の S 項では、欧州議会の認識として、「アメリカ合衆国、日本、中国及び韓国のような海外の複数の国々は、産業用ロボット及び AI と関連する規制措置を検討し、一定の範囲内では、既にそのような措置が講じられており、また、幾つかの構成国も、そのような勃興しつつある技術の応用を考慮に入れるため、法律上の標準の起草または法改正の策定に反映させ始めている」と述べられている。
(76) 将来、全ての自動車が自動走行自動車となり、人間が操縦・運転することがなくなると、運転免許制度を含め、現在の道路交通の法制度が全面的に無意味なものとなると考えられる。おそらく、自動車は、レガシーな自動車を特殊な場所で私的に楽しむような場合を除き、これを所有するものではなく、全てバスやタクシーのように利用するものとなることであろう。その結果、危険の分散の原理に基づく現在の損害保険制度も完全に崩壊する。事前の保険料を分担して徴収するというモデルではなく、もし事故が起きれば、高度な人工知能システムによって全国民の分担額を事後的に日単位で計算し直して自動的に分担課税する税方式に社会制度が全般的に変更されることになると予測され、その場合には、自動車事故と関連する損害保険業務に従事する企業活動が消滅することになる。それと同時に、現在あるような意味での保険学や保険法学もまた、その社会的必要性を失い、消滅することになるであろう（強いて言えば、産業史学または法史学の一部として残される可能性はある）。簡単に言えば、現在のように自動車の所有者・保有者に対して自賠責保険を強制加入させ、個々の運転者が任意保険契約を締結するのではなく、自動走行自動車の運行サービスの提供者または自動走行自動車の製造者が負担すべき損害賠償の担保を国民全員に対して強制する仕組みへの全面的な変更が必至であると考えられる。しかし、仮にそのような税方式への転換が行われると予測する場合、自動走行

自動車を開発・製造・販売することそれ自体は企業活動の自由の範囲内に含まれるとしても、そのような特定のごく少数の私企業の経済的利益確保のゆえに、当該企業とは関係のない者が圧倒的多数を占める国民全員が強制的に賠償担保課税の対象とされることの合憲性に関しては、現時点から徹底的に検討しておかなければならないと考える。

なお、人工知能技術の発展は、世界規模で、「物の所有による支配・利用」から「役務の提供・利用」への巨大な社会制度上の変動をもたらし得るものである。立法者は、このような巨大な変化を踏まえた対応を迫られている。その意味では、近時の日本国の民法改正において、役務の提供・利用を主軸とする基本法令への根本改正が行われなかったことは、甚だ遺憾なことである。同様に、今回の民法改正においては、動産と不動産と情報財の区別なく、全体を一体として権利義務の対象とするような「集合財」の社会的重要性の観点も欠如している（「集合財」の基本的な考え方については、法律論叢誌上で連載中の夏井高人「艸―財産権としての植物―」参照）。立法担当者の先見性の完全な欠如を証明するものであると言える。とまれ、改正は行われたのであり、改正後の民法は、ごく限られた（GDPで言えば、国の経済全体に対しては全く影響力がない程度に小さな規模の）レガシーな特殊状況においてのみ適用可能な古典法令として生き延びることになるであろう。

(77) 前掲ハイブリッドな脅威報告書（JOIN (2017) 30）参照

(78) 他に旅客機のパイロットや客室乗務員、地上勤務者等の空港関係者に限定して適用されるEUの個人識別関係法令もある。裁判所、軍当局、その他の特殊機関または特殊施設等における個人識別に関しても特別の法令や個別の規則等が多数存在する。これらの詳細は省略する。

(79) 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。

(80) 技術仕様等は、ICAOのDocument 9303（Machine Readable Travel Documents）に準拠する。

(81) 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。

(82) 規則 (EC) No 444/2009 による改正後の理事会規則 (EC) No 2252/2004 の参考訳は、同誌同号130～133頁にある。

(83) COM(2016) 823 final 及び COM(2016) 824 final

(84) 食肉等のトレーサビリティのために用いられる電子IDに関しては、規則 (EU) No 653/2014（OJ L 189, 27.6.2014, p.33）がある。

(85) PNR指令 (EU) 2016/681 の参考訳は、法と情報雑誌2巻3号119～155頁にある。

(86) 一定の種類のデータが継続的かつ義務的に保存され続ける点において、PNRの収集・保存の仕組みは、データ保持指令2006/24/EC（OJ L 105, 13.4.2006, p.54）における枠組みと共通する部分がある（データ保持指令2006/24/ECの参考訳は、法と情報雑誌1巻5号47～65頁にある）。そのことから、PNRにおけるプライバシー問題は、その本質部分において、データ保持指令におけるプライバシー問題と共通する部分をもつ。しかし、日本国の憲法学会においては、この問題に関しては、ほぼ等閑視されている。日本国の法学における蛸壺的構造の悪弊がこの分野においても顕著である。一般に、クラウドと人工知能が普及する時代においては、発生する法的課題も分野横断的なものとなることが多くなる結果、縦割りの分野による制度設計はほとんど意味をもたなくなる。極論すると、職業人である法学研究者としては、人工知能技術やビッグデータのようなデータベースを調査研究のための道具として自由自在に駆使し、網羅的に全ての事柄に対処できる者だけが生存可能となることであろう。そこでは、既存の個々の法学理論は、応用

のための判断基準としてではなく、それ自体として批判的な検討の対象として扱われることが多くなるのであり、在来の理論を固守し、その応用のみを法学の方法論として理解するようなタイプの研究手法は、適者生存法則の下で、急速に廃滅してゆくことになると予想される。これらの現象は、前掲『ネットワーク社会の文化と法』で述べた「単一化（unification）」の現象形態の一種として理解することも可能である。

(87) 理事会決定 2009/371/JHA の参考訳は、法と情報雑誌 2 巻 2 号 31～98 頁にある。

(88) Europol 規則 (EU) 2016/794 の参考訳は、同誌 2 巻 3 号 1～101 頁にある。

(89) 石垣泰司「欧州統合と対テロ政策―EU 対テロ政策形成過程における加盟国、欧州委員会および欧州議会の役割―」日本 EU 学会年報 27 号 55～74 頁 (2007) 参照

(90) 理事会枠組み決定 2002/475/JHA の参考訳は、法と情報雑誌 2 巻 5 号 71～85 頁にある。

(91) 日本国における定義は、組織的な犯罪の処罰及び犯罪収益の規制等に関する法律（平成 11 年法律第 136 号）によって与えられている。

(92) 丸橋透「搭乗者名データの移転及び処理に関するカナダと欧州連合間の協定案の適合性に関する欧州連合司法裁判所への諮問事件 1/15 独立弁論官 MENGOZZI 意見書（2016 年 9 月 8 日言渡し）（欧州議会から欧州連合司法裁判所に提出された諮問手続き）[参考訳]」法と情報雑誌 2 巻 5 号 366～437 頁 (2017)、同「搭乗者名記録 (PNR) データの移転および処理に関するカナダと欧州連合間の協定案に関する欧州議会からの意見請求事件 (1/15) 欧州連合司法裁判所 (大法廷) 意見 (2017 年 7 月 26 日)ECLI: EU: C: 2017: 592 [参考訳]」法と情報雑誌 2 巻 8 号 186～256 頁 (2017)、同「カナダ国境サービス庁による国家安全保障目的での旅行者のシナリオベース標的絞り込みについてのカナダプライバシーコミッショナーオフィスのプライバシー監査報告（2017 年 9 月 21 日）[参考訳]」法と情報雑誌 2 巻 10 号 21～39 頁 (2017) が参考になる。

(93) 関連する法令の翻訳として、右近潤一「資料・消費者の権利に関する欧州議会及び理事会の指令に関する提案（試訳）」京都学園法学 60・61 号 71～111 頁 (2010) がある。関連する論文として、川和功子「消費者像についての一考察（一）」同志社法學 63 巻 3 号 1459～1475 頁 (2011) がある。

(94) 原文は、「a single liaison office」であるが、構成国の連絡部局（a single contact point）のことを意味するものと解される。

(95) 他に、日本国の消費者の借入金限度額を規律するための法令及び制度と同様の法令及び制度が EU にも存在する。これらの法令及び制度は、金融秩序の安定という側面と消費者保護という側面を併有するものと理解することができる。その詳細については、省略する。

(96) 日本国の民法学及び商法学におけるこの分野の網羅的な比較法研究は、極めて貧弱である。なお、基本的な問題に関しては、夏井高人『電子署名法―電子文書の認証と運用の仕組み―』（リックテレコム、2001）で述べたとおりである。また、「本人確認（authentication）」の法的意義及び問題点に関しては、松本恒雄・齋藤雅弘・町村泰貴編『電子商取引法』（勁草書房、2013）の分担執筆部分である第 3 章「本人認証」（76～116 頁）で述べたとおりである。他に Arno R. Lodder & Andrew D. Murray (Eds.), EU Regulation of E-Commerce: A Commentary, Edward Elgar (2017)、Jeffrey Belson, Certification and Collective Marks: Law and Practice, Edward Elgar (2017) が参考になる。

(97) 信頼サービス（trust service）は、厳密には、私法と公法の両方に関係しており、特に EU の法制においては公法に属する部分が非常に重要である。しかし、本稿のこの部分では、私法の領域と関連するものに限定して、信頼サービスについて述べる。

(98) 日本国においても比較的良く知られている立法例として、ドイツ連邦のマル

チメディア法（Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz - IuKDG)）の2001年改正法がある。この2001年改正は、電子商取引指令2000/31/ECに定める要件を充足するためのものである。2001年改正後のマルチメディア法の和訳として、米丸恒治訳「情報サービスおよび通信サービスの大綱条件の規制のための法律―いわゆるマルチメディア法」・多賀谷一照・松本恒雄編『情報ネットワークの法律実務2』（第一法規、加除式出版物）7301～7326頁所収がある。

(99) これらのサービスは、「そのサービスの全体が送信され、運搬され、及び、受信されるサービス」に該当しない。

(100) 和訳として、内田貴訳「電子商取引に関するUNCITRALモデル法（試訳）」・前掲『情報ネットワークの法律実務2』7175～7185頁所収がある。電子商取引指令2000/31/ECの各条項について正確に理解するためには、UNCITRALのモデル法及び日本国の関連法令との逐条的かつ精密な比較検討作業が必須であるが、本稿においては、頁数の関係から割愛する。

(101) 指令97/66/ECの参考訳は、法と情報雑誌1巻5号66～83頁にある。

(102) 2018年5月18日以降は、個人データ保護指令95/46/ECではなく、一般データ保護規則(EU) 2016/679（GDPR）が適用される。また、本稿の執筆時点である2017年11月現在、電子通信プライバシー指令2002/58/ECの改正のための審議が行われている。

(103) その後、誤解を招く商業宣伝広告及び比較広告の規制に関する2006/114/EC（OJ L 376, 27.12.2006, p.21）により、廃止された。

(104) その後、消費者に対する信用供与契約に関する指令2008/48/EC（OJ L 133, 22.5.2008, p.66）により、廃止された。

(105) その後、金融商品市場に関する2004/39/EC（OJ L 145, 30.4.2004, p.1）により、廃止された。

(106) その後、指令2008/122/EC（OJ L 33, 3.2.2009, p.10）により、廃止された。

(107) その後、消費者保護指令2009/22/EC（OJ L 110, 1.5.2009, p.30）により、廃止された。

(108) 理事会指令85/374/EECの参考訳は、法と情報雑誌2巻10号278～291頁にある。

(109) その後、指令2001/83/EC（OJ L 311, 28.11.2001, p.67）により、廃止された。

(110) 日本国における関連法規制に関しては、経済産業省「電子商取引及び情報財取引等に関する準則」（平成29年6月）、公正取引委員会「消費者向け電子商取引における表示についての景品表示法上の問題点と留意事項」（平成14年6月5日・平成15年8月29日一部改正）が参考になる。

(111) 情報社会の基本的な法令を理解するためには、法学の分野における古典的な縦割り構造の分野・部門を全て完全に無視し、横断的な知識を統合して用いることのできる能力が求められる。それゆえ、今後の各大学の法学部における基本設計についてもまた、根本的なところで抜本的な構造転換が求められることになる。また、この分野における学術研究においては、前掲『ネットワーク社会の文化と法』の中で述べた「意思主義」から「処理主義」への変遷という世界規模の大きな動きを正確に理解した上での立論が必須である。

(112) その後、電気通信ネットワーク及び電気通信サービスのための共通の規制枠組みに関する指令2002/21/EC（OJ L 108, 24.4.2002, p.33）により、廃止された。

(113) 私法上の契約における当然の前提条件（いわゆる「法定条件」の一種）であるとみるこ

とも可能である。私法上の法律行為の自由は、完全に無条件の自由なのではなく、強行法の定める範囲内においてのみ自由である。このような場合において、もともとそのような規制による制限の範囲内のみで法律行為が成立していると考えるべきか、それとも、表示された意思の内容に従って成立した法律行為が公法上の規制等によって強制的に修正を受けると考えるべきか、それとも、法律行為には何らの修正も加えられないが、執行力が制限されると考えるべきかという問題は、検討に値する法解釈論上の課題の 1 つである。その検討を行う場合においても、古典的な法理論上のドグマに固執することなく、事実を直視する解釈姿勢が求められる。

(114) 吉村昭彦・白神猛「欧州における決済サービスの新たな法的枠組み：決済サービス指令の概要」金融研究第 28 巻 1 号 119～172 頁 (2009) に詳細な解説がある。

(115) 従前の電子マネー指令 2000/46/EC (OJ L 275, 27.10.2000, p.39) は、指令 2009/110/EC の第 21 条により、廃止された。

(116) 関連する文献として、檜垣拓也「「資金決済法」に基づく新しい国際送金サービスの特徴と法的課題―EU「決済サービス指令」と各取引約款との比較検討を中心にして」国際商取引学会年報 14 号 149～161 頁 (2012)、小梁吉章「仮想通貨の法律構成」広島法科大学院論集 13 号 1～23 頁 (2017)、高松志直「電子マネーおよび仮想通貨に対する強制執行」金融法務事情 65 巻 11 号 50～58 頁 (2017)、片岡義広「仮想通貨の規制法と法的課題（上）」NBL 1076 号 53～60 (2016)、同「仮想通貨の規制法と法的課題（下）」NBL 1077 号 82～89 頁 (2016)、高橋郁夫「フィンテックの法と制度」情報処理 57 巻 9 号 877～882 頁 (2016)、南波浩史・渡部美沙「種類別貨幣流通量に電子マネーが及ぼす影響について」徳島文理大学研究紀要 82 号 43～52 頁 (2011)、大野幸夫「電子マネー・電子決済と問題点」知財管理 49 巻 6 号 709～728 頁 (1999) がある。

(117) Karl-Friedrich Lenz「Bitcoin と資金洗浄―EU の 2015 年資金洗浄立法および FATF の 2015 年報告（Guidance）を中心に」青山法務研究論集 11 巻 1 号 1～22 頁 (2016) が参考になる。

(118) 金融機関等による顧客等の本人確認等及び預金口座等の不正な利用の防止に関する法律（平成 14 年法律第 32 号）は、犯罪による収益の移転防止に関する法律の全面施行により、平成 20 年（2008 年）3 月 1 日に廃止された。

(119) 論理的には、いかなる認証手段も、突き詰めれば自己認証に収束する。特に、物理的な存在としての特定の自然人の本人性の確認は、何らかの物理的な手段によって 1 回的に行われるだけであり、電子的な手段による証明は、全て、その 1 回的に行われる本人性の確認手続に依拠せざるを得ないという本質的な脆弱性を第三者認証であることによって解消することができない。その意味で、第三者認証であるということそれ自体では何ら保証の程度を向上させることにはならない。しかし、多数の証明機関が相互依存の中で連鎖的・多重的な証明を実行し、それらが全て一致した場合においてのみ、当該課題に対する証明が成立する場合、仮にそれらの証明機関のどれかが不正操作等により正常に機能していないとすれば全体としての証明の一致という結果を得られない道理であるので、その意味で、連鎖的・多重的な第三者認証は、単一の自己認証よりも保証の程度が高いことが明らかである。

ただし、そのような証明の連鎖におけるトップレベルの証明機関が不正操作等により正常に機能しない場合、あるいは、全ての証明機関において共通に使用される重要な符号が改変される場合には、連鎖的・多重的に実行されることによる保証は、全く意味をなさない。これが連鎖的・多重的な証明システムの最大の欠陥である。そして、その欠

陥は、巨大なクラウドサービスプロバイダによって、そのプラットフォームの利用者について行われる仮想的な多重証明が実は同一の機関による同一のシステムを使用した証明に過ぎないような場合には、最も深刻な様相を呈することになるであろう。このような場合、連鎖的・多重的にみえる証明は、仮想のものに過ぎず、極論すれば、単純な自己認証の一種が存在しているのに過ぎないことがあり得る。一般に、数学モデルそれ自体と現実のシステム運用との間の乖離があり得るということに十分に留意しなければならない。

(120) 前掲『電子署名法―電子文書の認証と運用のしくみ』25頁参照

(121) 情報セキュリティ上のリスク及びその刑事法的な対応については、法律論叢誌上において連載して公表した夏井高人「サイバー犯罪の研究（一）～（九・完）」において詳論したとおりである。

(122) 委員会実装決定(EU) 2015/296の参考訳は、法と情報雑誌2巻10号197～206頁にある。

(123) 委員会実装決定(EU) 2015/1505の参考訳は、同誌同号207～222頁にある。

(124) 委員会実装決定(EU) 2015/1506の参考訳は、同誌同号223～230頁にある。

(125) 委員会実装決定(EU) 2015/1984の参考訳は、同誌同号231～239頁にある。

(126) 委員会実装決定(EU) 2016/650の参考訳は、同誌同号240～245頁にある。

(127) 委員会実装規則(EU) 2015/806の参考訳は、同誌同号246～251頁にある。

(128) 委員会実装規則(EU) 2015/1501の参考訳は、同誌同号252～260頁にある。

(129) 委員会実装規則(EU) 2015/1502の参考訳は、同誌同号261～277頁にある。

(130) 2018年5月18日以降は、個人データ保護指令95/46/ECではなく、一般データ保護規則(EU) 2016/679（GDPR）が適用される。また、本稿の執筆時点である2017年11月現在、規則(EC) No 45/2001の改正のための審議が行われている。

(131) もし人類の生存を最優先の価値として維持するのであれば、そのような人間にとって全く理解不可能な処理を実施するシステムを物理的に完全に破壊してしまうという対応以外に有効な手立てがないと断言できるか否かという点についても慎重に検討が行われるべきである。その場合において、前掲「アシモフの原則の終焉―ロボット法の可能性―」で提示したサイバネティクス法（Cybernetics law）という意味でのサイバー法の観点からの考察が必須となる。従来の人間と人間でないものを完全に分離する法理論（法哲学）及び生物と非生物とを完全に分離する法理論（法哲学）を基礎とする限り、この深刻な課題に対して全く対処することができない。そして、そこで構築される新たな概念枠組みは、古典的な法理論（法哲学）におけるそれとは相当異なるものとなる可能性が高い。このような私見の当否は別として、将来の法理論（法哲学）がどのようなものになるかについては予測の域を出ないが、現時点における過渡的な法哲学の様相を紹介するものとして、亀本洋「中間法律関係」法律論叢90巻1号67～78頁(2017)があり、非常に参考になる。

（明治大学法学部教授）