欧州連合の構成国における独立の個人データ保護監督官の職務

法律論叢第 89 巻第 6 号（2017.3）

【論　説】

欧州連合の構成国における独立の個人データ保護監督官の職務

夏　井　高　人

目　次

1　はじめに

EU の一般個人データ保護規則（Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC・以下「一般個人データ保護規則 GDPR」という。）(1) の第 6 章（第 51 条ないし第 59 条）は、独立の行政機関（independent administrative authorities）(2) として、個人データの保護に関する監督官（supervisory authority）(3) について定めている。

この個人データの保護 (4) に関する監督官という独立の行政機関は、欧州評議会

(1) 一般に、「GDPR」との略称で呼ばれることもある（ドイツ語では、Datenschutz-Grundverordnung (DSGVO) となる。）。その全文訳は、夏井高人「個人データの処理と関連する自然人の保護及び個人データの自由な移転並びに指令 95/46/EC の廃止に関する欧州議会及び理事会の 2016 年 4 月 27 日の規則 (EU) 2016/679（一般個人データ保護規則）[参考訳]」法と情報雑誌 1 巻 3 号 1～186 頁にある。なお、同規則の前文の部分の訳文は、KDDI 総合研究所の Web サイト上で公開されている。

(2) 独立行政機関については、駒村圭吾「アメリカにおける独立行政機関と権力分立―中央銀行の独立性の理論的基礎に向けて―」白鴎法學 16 号 31～54 頁（2000）、清田雄治「フランスにおける「独立行政機関 (les autorites administratives independantes)」の憲法上の位置―CNIL の法的性格論への覚書」立命館法學 2008 年 5・6 号 1471～1501 頁（2008）が参考になる。

(3) 監督官は、国家組織の一種である行政機関の名称であり、行政官の職務名ではない。そのため、「監督官」ではなく、「監督機関」、「監督局」または「監督庁」との訳語をあてている例もある。また、監督官は、「プライバシーコミッショナー（privacy commissioner）」あるいは「データ保護の番人（data protection watchdog）」と呼ばれることもある。環太平洋諸国では、個人データ保護のための公的機関の名称として「プライバシーコミッショナー」が用いられることが比較的多い。ただし、国によって法制がかなり異なるため、名称のみから同一または類似の機能を有する国家機関であると安易に推定することは危険である。個人データ保護に関する監督官制度について国際的な調査をした結果を示す報告書としては、諸外国等における個人情報保護制度の監督機関に関する検討委員会（代表・藤原靜雄）「諸外国等における個人情報保護制度の監督機関に関する検討委員会・報告書」（平成 23 年 3 月）があり、また、関連する報告書として、諸外国等における個人情報保護制度の運用実態に関する検討委員会（代表・藤原靜雄）「諸外国等における個人情報保護制度の運用実態に関する検討委員会・報告書」（平成 19 年 1 月）及び諸外国等における個人情報保護制度の実態調査に関する検討委員会（代表・藤原靜雄）「諸外国等における個人情報保護制度の実態調査に関する検討委員会・報告書」（平成 20 年 3 月）がある。

(4) EU の個人データ保護法制における保護法益に関しては、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

の 1981 年の個人データ保護条約（Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ETS No.108）(5) の中には存在しなかった(6)。

その後、EU の 1995 年の個人データ保護指令（Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data）(7) の第 6 章（第 28 条）により、EU の構成国は、個人データの保護に関する監督機関である独立の行政機関として監督官を設置すべきことが定められた。同規則の前文第 62 項は、「完全に独立してその権限を行使する監督官を構成国に設けることは、個人データの処理と関連する個人の保護における重要な要素である」と述べている。

この指令を受け、欧州評議会の個人データ保護条約（ETS.108）にも監督官に関する条項が付加された。

すなわち、2001 年 11 月 8 日、欧州評議会の個人データの自動的な処理と関連する個人の保護に関する条約監督官及び国境を越えたデータの移転に関す

データ保護規則との関係を含めて―」法律論叢 89 巻 2・3 号掲載予定で詳論したとおりである。同論説においては、個人データに関する様々な権利がプライバシーという保護法益を守るための技術的・手段的・人工的な権利であり、一定の階層構造を有しているという知見を明らかにした。

(5) 個人データ保護条約 ETS No.108 の全文訳は、夏井高人「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）[参考訳]」法と情報雑誌 1 巻 4 号 1～20 頁にある。また、その説明書の全文訳は、同「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の説明書 [参考訳]」同誌同号 26～61 頁にある。

(6) 欧州評議会の個人データ保護条約（ETS No.108）と同時進行的に OECD のプライバシー保護のためのガイドラインの策定作業が進められ、その結果が、OECD 理事会勧告（1980 年 9 月）として公表された。この間における世界各国のプライバシー保護をめぐる動向については、堀部政男『プライバシーと高度情報化社会』（岩波新書、1988）が詳しい。1970 年代における OECD のプライバシー保護のための活動を示す公式の資料としては、OECD, Policy issues in data protection and privacy (1976) 及び OECD, Transborder Data Flows and the Protection of Privacy (1979) が公表されている。OECD のプライバシーガイドラインは、2013 年に改正されている。改正ガイドラインに関しては、堀部政男・新保史生・野村至『OECD プライバシーガイドライン―30 年の進化と未来』（JIPDEC、2014）が詳しい。

(7) 個人データ保護指令 95/46/EC の全文訳は、夏井高人「個人データの自動的な処理と関連する個人の保護及び個人データの自由な移転に関する欧州議会及び理事会の 1995 年 10 月 24 日の指令（Directive 95/46/EC）[参考訳]」法と情報雑誌 1 巻 5 号 1～46 頁にある。

る追加議定書（Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows ETS No.181）(8) が締結され、その第 1 条により、同条約の加盟国は、独立の行政機関として監督官を設置すべきことが定められた。

同追加議定書の前文には、「個人データの処理と関連する個人の効果的な保護にとって、完全に独立してその職務を遂行する監督官が重要であるということを認識し」とある。EU の構成国は、1995 年の個人データ保護指令 95/46/EC により、既に監督官を設置すべき義務を負っているのであるから、同追加議定書は、主として、EU の構成国ではない条約加盟国（非欧州連合諸国）との関係で意味を有する。

個人データ保護指令 95/46/EC は、欧州連合の構成国に対して直接の効力を有する法規範ではない。同指令は、構成国に対し、指令に定める内容のとおりに各構成国の自国の法令を制定する義務を負わせる法規範である。そして、構成国は、同指令の実装（implementation）として、個人データ保護のための監督機関である各構成国における独立の行政機関 (9) を設置し、これを運用してきた。この監督官の具体的な存在形式（組織構成）や具体的な権限の内容及び行使の態様は、構成国内に 1 つの監督官だけが設置されているのか複数の監督官が設置されているのかを含め、各国の国家体制及び各構成国において適用可能な法令によって異なる (10)。

その後、個人データ保護指令の特別法として、通信分野における個人データの処理及びプライバシーの保護に関する欧州議会及び理事会の 1997 年 12 月 15 日の指令 97/66/EC (11) が制定され、更に、同指令の改正指令である電子通信分野にお

(8) 追加議定書の全文訳は、夏井高人「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 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）[参考訳]」法と情報雑誌 1 巻 4 号 21〜25 頁にある。

(9) 構成国によっては、行政機関ではなく議会の機関として設置している例もある。それは、国家体制の相違に基づく。なお、共産主義国や権力集中制のような国家体制にある国では、どのような国家制度として設計されている場合であっても、監督官が国家機関としての独立性を維持することは原理的に不可能である。このような問題については、Serge Gutwirth, Ronald Leenes, Paul de Hert & Yves Poullet (Eds.), European Data Protection: Coming of Age, Springer (2013) pp.395–406 が参考になる。

(10) 独立の行政機関である監督官の構成員（委員）として現実に監督業務に従事する者の選任の基準も構成国により異なる。

(11) 指令 97/66/EC の全文訳は、夏井高人「通信分野における個人データの処理及びプラ

ける個人データの処理及びプライバシー保護に関する欧州議会及び理事会の指令 2002/58/EC(12) が制定された。これらの指令においては、監督官に関する条項が含まれていなかった。しかし、指令 2002/58/EC の一部改正により、情報セキュリティと関連する監督官の職務が定められるに至った。

これらの指令に定めるのと同様の監督官の職務は、ネットワーク及び情報システムの安全性に関する指令 (EU) 2016/1148 の中にも規定されている(13)。

2001 年 12 月 18 日、個人データ保護指令 95/46/EC に基づき、直接的効力を有する法規範として、欧州共同体の機関及び組織による個人データの処理と関連する個人の保護及び個人データの自由な移転に関する規則 (EC) No 45/2001(14) が制定された。規則 (EC) No 45/2001 においても、独立の行政機関である監督官の制度及びその職務権限が定められている(15)。

イバシーの保護に関する欧州議会及び理事会の 1997 年 12 月 15 日の指令（Directive 97/66/EC）[参考訳]」法と情報雑誌 1 巻 5 号 66～83 頁にある。

(12) 指令 2002/58/EC の全文訳は、夏井高人「電子通信分野における個人データの処理及びプライバシー保護に関する欧州議会及び理事会の指令（2002/58/EC）（プライバシー及び電子通信指令）[参考訳]」法と情報雑誌 1 巻 2 号 117～162 頁にある。

(13) 電子通信を用いた商取引の過程では個人データの移転が必然的に伴うのであるが、電子商取引に関して制定された域内市場における情報社会サービスの法的側面とりわけ電子商取引に関する欧州議会及び理事会の 2000 年 8 月 8 日の指令 2000/31/EC の第 1 条第 5 項 (b) は、同指令が個人データ保護指令 95/46/EC との関係では適用されない旨を規定している。他方、域内市場における電子商取引のための電子識別及び信頼サービス並びに指令 1999/93/EC の廃止に関する欧州議会及び理事会の 2014 年 7 月 23 日の (EU) No 901/2014 の中には、電子商取引と関連する個人データ処理については個人データ保護指令 95/46/EC が適用されることを定める条項及び電子識別等に関する職務権限を有する監督機関が個人データ保護に関する監督官と協力して職務を遂行すべきものと定める条項があるが、監督官の特別の職務に関して具体的な定めを設けているわけではないので、本稿においては検討を割愛する。なお、規則 (EU) No 901/2014 の条文の部分の和訳としては、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）の巻末に収録されている米丸恒治「指令 1999/93/EC の廃止ならびに域内市場における電子取引のための電子識別及び信頼役務に関する 2014 年 7 月 23 日欧州議会および理事会規則第 910/2014 号（2014 年 8 月 28 日 EU 官報 L257/73 頁）（試訳）」がある。

(14) 規則 (EC) No 45/2001 の全文訳は、夏井高人「欧州共同体の機関及び組織による個人データの処理と関連する個人の保護及び個人データの自由な移転に関する規則（(EC) No 45/2001）[参考訳]」法と情報雑誌 1 巻 2 号 74～116 頁にある。

(15) 規則 (EC) No 45/2001 の第 1 条第 2 項、第 24 条ないし第 26 条に定める欧州データ保護監督官（the European Data Protection Supervisor）は、構成国の行政機関ではなく、統治組織としての欧州連合の行政組織における個人データの処理業務を監督すべき職責を有する独立の行政機関である。本稿の目的は、主として構成国の監督官の職務の検討

欧州共同体（欧州連合）の行政機関及び構成国の行政機関の一種である警察等による犯罪捜査の過程で処理される個人データの保護に関しては、特別法として、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 2008 年 11 月 27 日の理事会枠組み決定 2008/977/JHA 及び同枠組み決定の改正指令である犯罪行為の防止、捜査、検知もしくは訴追または刑罰の執行のための職務権限を有する機関による個人データの処理と関連する自然人の保護及び個人データの自由な移転並びに理事会枠組み決定 2008/977/JHA の廃止に関する 2016 年 4 月 27 日の欧州議会及び理事会の指令 (EU) 2016/680 が制定されている。これらの警察関係の枠組み決定及び指令中には、犯罪捜査等と関連して処理される個人データの保護と関係する監督官の職務についての特別の条項がある。

加えて、テロ対策を主たる目的として制定されたデータ保持指令 2006/24/EC 及び搭乗者記録指令 (EU) 2016/681 の中にも、警察、通関当局、諜報機関または軍当局等による個人データの収集と関連する監督官の職務に関する条項がある。

そして、個人データ保護指令 95/46/EC の実質的な改正法であり、直接的な効力を有する一般個人データ保護規則 (EU) 2016/679 では、独立の行政機関である監督官の職務及び権限がより詳細に規定され、その権限が強化されている。

日本国においては、長らく、EU における独立の行政機関としての監督官に相当する国家機関が存在しなかった(16)。その意味において、個人情報保護に関する日本国の法制は、監督官（supervisory authority）という独立の国家機関の存否という点では、1995 年の個人データ保護指令第 25 条第 1 項に定める「十分なレベルでの保護」の要件を全く満たしていない状態が続いていたと断定することができ

にあるので、欧州データ保護監督官については、その存在について触れるのみとする。

(16) 情報公開・個人情報保護審査会設置法（平成 15 年法律第 60 号）に基づいて設置された個人情報保護審査会は、部分的には、EU の監督官が担うべき職務の一部を担当していたと評価することは可能である。しかし、個人情報保護審査会は、その権限及び機能の点において、EU の監督官と同等または均等の国家機関であるとは到底言えない。この点が非常に重要である。現在、個人情報保護審査会は、内閣の重要政策に関する総合調整等に関する機能の強化のための国家行政組織法等の一部を改正する法律（平成 27 年法律第 66 号）の施行に伴い、平成 28 年 4 月 1 日に内閣府から総務省に移管されている。しかし、それは、EU の監督官におけるのと同じような意味での独立の行政機関では該当しない。なお、個人情報保護審査会の実際の業務に関しては、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。

る(17)。

平成27年法律第65号による個人情報保護法（平成15年法律第57号）の改正により、日本国の法制度中においても、独立して職務を遂行する国家機関である個人情報保護委員会が加えられることとなった(18)。これによって民間部門に関する限り、日本国においても、EUの法制における監督官と類似する国家機関が設けられたことになる。しかしながら、後述するとおり、公的部門（行政機関・独立行政法人等）に関しては、国家機関としての独立の監督機関（監督官）は存在しない（ただし、例外として、特定個人情報（個人番号）と関連する業務処理に関しては、個人情報保護委員会が監督権限を行使することができる場合がある。）。

本稿は、EUの法制において、EUの機関及び構成国に設置された監督官がどのような職務を遂行すべき行政機関であるのかについて、その本来的な職務である個人データの保護について検討し、次いで、その付随的な職務である情報セキュリティ、犯罪捜査及びテロ対策と関係する職務について検討した上で、日本国の法制との比較法的な観点からの考察を行い、その検討結果を明らかにすることを目的とする(19)。

(17) 同規則第25条第2項の法解釈として、監督官という国家機関の存在までは求めていないと解する場合には、この点に関しては、反対の結論となる。しかし、一般個人データ保護規則第45条第2項は、十分性の判定の際に考慮すべき要素として、監督官という国家機関が存在していることを当然の前提としている。これは、個人データ保護指令の時点から既に監督官という国家機関が存在することが十分性の判定のための必須の要件となっており、ただ、それが条文の上では明確ではなかったために、一般個人データ保護規則第45条第2項によってこの点が明確化されたと解するのが妥当である。

(18) 平成28年法律第63号による改正前の行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号・以下、改正前の法律及び改正後の法律を通じて「個人番号法」という。）によって設置された特定個人情報保護委員会は、個人情報保護法に定める個人情報保護委員会に改組された。改組前の特定個人情報保護委員会は、個人番号に関する職務権限のみを有するもので、個人情報及び個人データの保護に関して全般的な独立の権限を有する行政機関ではなかった。なお、特定個人情報制度に関しては、藤原靜雄監修・東京都特定個人情報保護実務研究会編『Q&A 特定個人情報保護ハンドブック 番号法に基づく条例整備から運用まで』（ぎょうせい、2015）がある。

(19) 世界的には、行政機関ではない監督機関の活動が注目されている。欧州連合基本権憲章第43条に基づく公的なオンブズマン制度も行政機関ではなく、欧州議会によって選任された構成員によって組織される。また、監督に相当する業務を遂行する私的な組織や団体も多数ある。これらの中で私的な組織や団体による監督に関しては、Rodney Bruce Hall & Thomas J. Biersteker (Eds.), The Emergence of Private Authority in Global Governance, Cambridge University Press (2002) が参考になる。

2　個人データ保護と関連する監督官の職務

2．1　個人データ保護指令 95/46/EC における職務

個人データ保護指令に定める監督官の職務の中で主要なものは、個人データを処理する予定の管理者(20)から当該個人データを処理する前にその通知を受けること（第 18 条）、管理者が当該データ処理を開始する前に事前の点検を行うこと（第 19 条）、第 18 条に基づいて管理者から通知を受けた内容を一般に公表し、職務遂行のために必要な情報を議会や行政機関に照会してこれを入手し、管理者に違反行為がある場合には法務当局に対してその侵害行為について通告すること（第 21 条）、管理者による処理業務について調査し、必要に応じて処理業務の停止や個人データの廃棄等を命ずること（第 28 条第 3 項）、データ主体から異議があったときは、適切に聴聞し、必要な対処をし、その結果を関係者に対して通知すること（第 28 条第 4 項）、個人データ保護指令 95/46/EC の構成国における実装・運用を監視すること（第 28 条第 1 項）、構成国において個人データ保護のための法令や行政規則等を制定する際に、該当する国家機関（議会、行政機関等）と協議をすること（第 28 条第 2 項）、他の構成国の監督官から要請を受けたときはその権限内で協力をすること（第 28 条第 6 項）、定期的に活動報告書を作成すること（第 28 条第 5 項）、各構成国を代表して、第 29 条第 2 項によって設置される作業部会（Article 29 Working Party）の構成員となり、その審議に参加すること（同条同項）、その作業部会の議題を発議すること（同条第 7 項）等である。

2．2　一般個人データ保護規則 (EU) 2016/679 における職務

個人データ保護指令 95/46/EC の実質的な改正法である一般個人データ保護規則 GDPR の第 4 条 (21) は、「監督官」の定義として、「第 51 条に従い構成国によって設置される独立の行政機関のことを意味する」と定めている。

そして、同規則第 51 条第 1 項は、「各構成国は、処理と関連する自然人の基本的な権利及び自由を保護し、かつ、欧州連合内における個人データの自由な移転を促

(20) 管理者（controller）は、日本国の法制では、行政機関及び個人情報取扱事業者が相当する。

進するために、この規則の適用を監視することに責任を有する 1 または複数の独立の行政機関を定めなければならない（以下「監督官」という。）」と定めている。ここに定めているのは、監督官がその職務の遂行を通じて保護しようとしている保護法益を明確にするものと考えられる。この「自然人の基本的な権利及び自由」という保護法益を具体的に保護するための技術的・手段的・人工的な権利である個人データの権利と関連する具体的な職務については、別途、第 55 条ないし第 67 条（特に第 57 条及び第 58 条）に詳細な規定がある。

すなわち、一般個人データ保護規則 GDPR の第 57 条は、次のように定めている。

(a) この規則の適用を監視し、執行し；
(b) 処理と関連するリスク、規則、安全性確保措置及び権利についての公衆の認識及び理解を促進し、とりわけ、子ども向けの活動について格別の注意を払い；
(c) 構成国の法律に従い、自国の議会、政府その他の機関及び組織に対し、処理と関連する自然人の権利及び自由の保護に関する立法上の措置及び行政上の措置について、助言し；
(d) この規則に基づく管理者及び処理者の義務について、それらの者に対する認識を促し；
(e) 要請に応じて、この規則に基づくデータ主体の権利の行使について、いかなるデータ主体に対しても情報を提供し、また、それが適切であるときは、その目的のために、他の構成国の監督官と協力し；
(f) データ主体によって申立てられた異議、または、第 80 条に従い、組織、団体もしくは協会から申立てられた異議に対処し、必要な範囲内で、異議申立てのあった事項について調査し、かつ、とりわけ更に調査することまたは他の監督官と協力することが必要な場合には、合理的な期間内に、異議申立人に対し、進捗状況及び結果を通知し；
(g) この規則の一貫性のある適用及び執行を確保するという観点から、情報の共有及び相互支援の提供を含め、他の監督官と協力し；
(h) 他の監督官または行政機関から提供された情報に基づく場合を含め、この規則の適用に関する調査を行い；
(i) 個人データの保護に対して影響を与えるものである限り、関連する発展について、とりわけ、情報通信技術の開発及び商業活動の動向について注視し；
(j) 第 28 条第 8 項及び第 46 条第 2 項の (d) に示す標準約款の条項を定め；
(k) 第 35 条第 4 項によるデータ保護影響評価の要件に関するリストを作成し、維持管理し；
(l) 第 36 条第 2 項に示す処理業務に関して助言し；
(m) 第 40 条第 1 項による行動準則の起草を奨励し、第 40 条第 5 項により、意見を提供し、かつ、十分な安全性確保措置を定める行動準則を承認し；

(n) 第 42 条第 1 項によるデータ保護の認証方法、データ保護シール及びデータ保護マークの設置を促進し、かつ、第 42 条第 5 項による認証の基準を承認し；
(o) それが適用可能なときは、第 42 条第 7 項に従って発行される認証の定期的な再評価を行い；
(p) 第 41 条による行動準則を監視する組織の承認のための基準及び第 43 条による認証機関の承認のための基準を策定して公表し；
(q) 第 41 条による行動準則を監視する組織の承認及び第 43 条による認証機関の承認を行い；
(r) 第 46 条第 3 項に示す契約条項及び公文書の条項を承認し；
(s) 第 47 条による拘束的企業準則を承認し；
(t) 欧州データ保護委員会の活動に貢献し；
(u) この規則の違反行為及び第 58 条第 2 項に従って講じられた措置に関する内部資料を保管し；かつ、
(v) 個人データの保護と関連するその他の職務を遂行しなければならない。

これらの一般個人データ保護規則 GDPR の第 57 条に定める職務の中で指令 95/46/EC にはなかった職務及びより明確化または権限強化された職務としては、(b) の普及活動に関する職務、(f) 及び (g) の共同活動に関する職務、(h) 及び (i) の情報収集に関する職務、(k) の事前影響評価、(j)、(l) ないし (s) の標準約款、行動準則、拘束的企業準則及び認証に関する職務、(t) の欧州データ保護委員会（第 68 条）に関する職務をあげることができる。

(k) の事前の影響評価に関して、一般個人データ保護規則 GDPR の第 35 条は、以下のように規定している。すなわち、同規則に定める影響評価[21]は、監督官の一般的及び個別的な監督の下で実施されるものである。

(21) 事前の影響評価については、六川浩明・新保史生・村上康二郎・伊瀬洋昭『プライバシー影響評価 PIA と個人情報保護』（中央経済社、2010）、瀬戸洋一「行政情報システムへの適用を考慮したプライバシー影響評価手法の開発」産業技術大学院大学紀要 1 号 79～91 頁（2007）が参考になる。この分野における個人データ保護指令 95/46/EC 第 29 条の作業部会による公式報告書としては、Opinion 04/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force (00678/13/EN) (Adopted on 22 April 2013) がある。UMIL（Università degli Studi di Milano）の報告書としては、Stelvio Cimato (ed.), Privacy-Preserving Computation in the Cloud (ICT-609611/D31.1/1.0) (1 November, 2013) が公表されている。

1. 処理の性質、範囲、遂行過程及び目的を考慮に入れた上で、ある類型に属する処理、特に新たな技術を用いる処理が、自然人の権利及び自由に対する高度なリスクを発生させるおそれがある場合には、管理者は、処理の前に、予定している処理の個人データの保護に関する影響の評価を行わなければならない。類似の高度のリスクを示す一群の類似の処理業務について、単一の評価を実施することができる。

2. 管理者は、データ保護影響評価を行う場合において、その指名をしているときは、データ保護責任者に対して助言を求めなければならない。

3. 第1項に示すデータ保護影響評価は、とりわけ、以下の場合に求められる：

(a) プロファイリングを含め、自動的な処理に基づく自然人の人格的側面についての機械的で広範な評価の場合、及び、それに基づく判断が自然人に関係する法的効果を発生させる場合、または、自然人に対して同様の重大な悪影響を与える場合；

(b) 第9条第1項に示す特別類型のデータまたは第10条に示す有罪判決及び犯罪行為と関連する個人データの大規模な処理の場合；または、

(c) 大規模に公衆がアクセス可能な領域のシステムによる監視の場合。

4. 監督官は、第1項によるデータ保護影響評価の義務に服する処理業務の種類のリストを公表しなければならない。監督官は、第68条に示す欧州データ保護委員会に対し、そのリストを通知しなければならない。

5. 監督官は、また、データ保護影響評価が必要となる処理業務の種類のリストを公表することができる。監督官は、欧州データ保護委員会に対し、そのリストを通知しなければならない。

6. それらのリストがデータ主体に対する物品もしくは役務の提供と関連する処理行為または複数の構成国におけるデータ主体の行動の監視と関連する処理行為を含んでいる場合、または、欧州連合内における個人データの自由な移転に重大な影響を与え得るものである場合には、第4項及び第5項に示すリストを作成する前に、職務権限を有する監督官は、第63条に示す一元的な仕組みを適用しなければならない。

7. 評価は、少なくとも以下の事項を含むものとしなければならない：

(a) 予定されている処理業務の体系的な記述、及び、適用可能なときは、管理者の求める正当な利益を含め、処理の目的；

(b) 目的と関連する処理業務の必要性及び比例性についての評価；

(c) 第1項に示すデータ主体の権利及び自由に対するリスクについての評価；及び、

(d) データ主体及び他の関係者の権利及び自由を考慮に入れた上で、個人データの保護を確保するための、及び、この規則の遵守を説明するための、安全性確保措置、防護措置及び仕組みを含め、リスクに対して対処するために用意されている手段。

8. 関係する管理者または処理者によって第40条に示す承認された行動準則が遵守されていることは、当該管理者または処理者によって遂行される処理業務の影響を評価するに際し、とりわけ、データ保護影響評価の目的のために、十分に考慮に入れられなければな

らない。
9. それが適切であるときは、管理者は、予定されている処理について、商業上の利益、公共の利益または処理業務の安全性を妨げることなく、データ主体またはその代理者から意見を求めなければならない。
10. 第 6 条第 1 項の (c) または (e) による処理が、管理者が服する欧州連合の法律または構成国の法律の中に法的根拠を有する場合において、その法律が、特定の処理業務または一群の処理業務を規律しており、かつ、当該法的根拠を採択する過程における一般的な影響評価の一部としてデータ保護影響評価が既に行われている場合には、第 1 項ないし第 7 項は、適用されない。ただし、構成国が、処理行為の前にそのような評価が行われることが必要であるとしている場合は、この限りではない。
11. 必要があるときは、管理者は、遅くとも処理業務によってリスクの変化が示された時点において、データ保護影響評価に従って処理が遂行されているか否かを評価するために、再評価を行わなければならない。

第 35 条第 4 項及び第 5 項並びに第 57 条 (t) にある欧州データ保護委員会（European Data Protection Board）は、個人データ保護指令 95/46/EC の第 29 条により設置された作業部会（Article 29 Working Party）を改組して設置された欧州連合の機関である（第 68 条）。欧州データ保護委員会は、欧州連合全体の個人データ保護法制の執行に関する統括的な職責を有し、欧州連合の機関における個人データ保護を統括する欧州データ保護監督官（the European Data Protection Supervisor）と共同して活動し、かつ、構成国の監督官の間での情報交換や紛議の解決並びに国際的な情報交換や共同活動等の欧州連合全体と関連する職務を遂行する。欧州データ保護委員会の委員は、各構成国の監督官等によって構成される。

2. 3　職務遂行上の判断基準

監督官は、一般個人データ保護規則 GDPR の第 57 条に基づき、基準・ガイドラインの策定等を通じて個人データ保護のための具体的な行動規範の形成に関与し（同条 (j)、(k)、(m)、(n)、(p)）、また、一般的な広報活動等を通じて個人データの保護のための様々な活動を行う（同条 (b)、(c)、(d)、(e)）。そして、監督官は同規則第 59 条に基づき、年次報告書を作成して公表する。これらの職務は、具体的な紛争案件に対して直接に対処するという性質を有する職務ではなく、いわば一般的な監督に属するものである。

他方、構成国の監督官は、具体的な案件と関係する職務も遂行する（同条(a)、(f)、(h)、(l)、(v)）。この具体的な案件に対応するための権限は、同規則の第58条に定められている。同条第1項は調査権限について、同条第2項は是正権限について、そして、同条第3項は助言の権限について定めている。

1. 各監督官は、以下の全ての調査権限を有する：
(a) 管理者及び処理者に対し、及び、適用可能なときは、管理者の代理者または処理者の代理者に対し、監督官がその職務を遂行するために求められる情報の提供を命ずること；
(b) データ保護監査を実施する際に、調査を行うこと；
(c) 第42条第7項により発行される認証について再評価を行うこと；
(d) 管理者及び処理者に対し、この規則の違反行為が申立てられていることを通知すること；
(e) 管理者及び処理者から、その職務を遂行する上で必要となる全ての個人データ及び全ての情報に対するアクセスを得ること；
(f) 欧州連合または構成国の手続法に従い、データを処理する装置及び手段を含め、管理者及び処理者の全ての施設に対するアクセスを得ること。
2. 各監督官は、以下の全ての是正権限を有する：
(a) 管理者または処理者に対し、予定されている処理業務がこの規則の定めに違反するおそれがあるとの警告を発すること；
(b) 処理業務がこの規則の定めに違反する場合には、管理者または処理者に対し、注意処分を発すること；
(c) 管理者または処理者に対し、この規則による彼または彼女の権利を行使するデータ主体の要求に従うように命ずること；
(d) 管理者または処理者に対し、それが適切であるとき、指定した方法により及び指定した期間内に、この規則の定めを遵守して処理業務を行うように命ずること；
(e) 管理者に対し、データ主体に対する個人データの侵害を通知するように命ずること；
(f) 処理の禁止を含め、一時的な制限または確定的な制限を命ずること；
(g) 第16条、第17条及び第18条により個人データの訂正もしくは削除または処理の制限を命ずること、及び、第17条第2項及び第19条により個人データの開示を受けた取得者に対して、そのような行為についての通知をするよう命ずること；
(h) 認証を取り消すこと、もしくは、認証機関に対し、第42条及び第43条により発行した認証を取り消すように命ずること、または、認証の要件に適合しない場合、もしくは、適合しなくなった場合には、認証機関に対し、認証を発行しないように命ずること；
(i) 個々の事案の状況に応じて、本項に示す措置に加え、または、その代わりに、第83条による行政罰を科すこと；

(j) 第三国または国際機関の取得者に対するデータの移転の停止を命ずること。

3. 各監督官は、以下の全ての承認及び助言の権限を有する：

(a) 第 36 条に示す事前協議手続に従い、管理者に対し、助言すること；

(b) 個人データの保護と関連する全ての事項について、率先して、または、要請に応じて、自国の議会、構成国の政府に対し、または、構成国の法律に従い、その他の機関及び組織並びに公衆に対して、意見を発すること；

(c) 構成国の法律が事前の承認を要するものとしている場合には、第 36 条第 5 項に示す処理を承認すること；

(d) 第 40 条第 5 項による行動準則草案について意見を発し、それを承認すること；

(e) 第 43 条により認証機関を承認すること；

(f) 認証を発行し、及び、第 42 条第 5 項に従い認証の基準を承認すること；

(g) 第 28 条第 8 項及び第 46 条第 2 項の (d) に示す標準データ保護約款を承認すること；

(h) 第 46 条第 3 項の (a) に示す契約条項を承認すること；

(i) 第 46 条第 3 項の (b) に示す行政文書を承認すること；

(j) 第 47 条による拘束的企業準則を承認すること。

一般個人データ保護規則 GDPR の第 77 条第 1 項は、「他の行政上の救済または司法上の救済を妨げることなく、全てのデータ主体は、データ主体が彼または彼女と関係する個人データの処理がこの規則に違反するものと考えるときは、特に、彼または彼女の居住地の構成国、就業場所の構成国または違反行為があると主張する場所の構成国において、監督官に異議を申立てる権利を有する」と定めている。これは、①行政訴訟法や民事訴訟法及び民事保全法に定める司法上の救済ができること、そして、②司法上の救済とは別に、個人データの処理と関係する何らかの侵害行為があると考えるデータ主体が監督官に対して異議申立てをすることができることを定めるものである。すなわち、通常の司法機関による解決とは別に、独立の行政機関である監督官が紛争解決機能を有するということを示している。監督官は、この異議申立てがあったときは、調査結果に基づき、是正命令等の職務権限を行使し、必要に応じて罰則を適用する。

一般個人データ保護規則 GDPR の第 58 条第 2 項 (i) の罰則を適用する権限については、同規則第 83 条にその内容が詳細に定められている。

同規則第 83 条第 1 項は、「各監督官は、第 4 項、第 5 項及び第 6 項に示されているこの規則の違反行為に関して本条による行政罰が、個々の個別の案件において、

効果的であり、比例的であり、かつ、抑止力のあるものとして、科されることを確保しなければならない」と規定し、基本的な判断基準が、罰則の「有効性」、「比例性」及び「抑止力」であることを示している(22)。これらの条項は、刑事裁判でいえば、量刑における判断基準に相当するものと考えられる。同条第2項は、そのような意味での量刑の基準に相当する判断要素を更に細かく定め、複数の違反行為がある場合の対処については同条第3項が「管理者または処理者が、意図的にまたは落度により、同じ処理業務または関係する処理業務について、この規則の複数の条項に違反する場合には、行政罰の総額は、その最も重い違反行為について定められた金額を超えることができない」と規定している。

この行政罰は、裁判所における審理を要する刑事罰としての罰金ではなく、行政罰としての制裁金の一種であり、官庁（行政機関）としての監督官がその判断に基づいて科することができるものであることを原則とするが、構成国に行政罰の制度が存在しない場合には、裁判所によって科される刑罰（罰金）とすることができる。

この点について、同条第9項は、「構成国の司法制度が行政罰を定めていない場合には、本条は、効果的で監督官により科される行政罰と均等な効果を有する司法救済を確保しつつ、その罰金が職務権限を有する監督官によって手続が開始され、そして、職務権限を有する自国の裁判所によって科されるような方法で適用することができる。そのいずれの場合においても、科される罰金は、効果的であり、比例的であり、かつ、抑止力のあるものでなければならない」と規定している。TFEUに定める基本原則(23)に基づき、国家制度ないし国家組織それ自体に対しては欧州連合が干渉することができないということに起因しており、国家制度が異なっているために実装不能となる場合があり得るということが予め（規則制定過程における折衝等を通じて）明らかになっていたため、このような措置が講じられた(24)。

(22) 欧州連合基本権憲章第49条に基づく。
(23) 中西優美子『EU法』（新世社、2012）36～50頁、M. ヘルデーゲン（中村匡志訳）『EU法』（ミネルヴァ書房、2013）44～54頁、111～121頁
(24) 前文第151項には、「デンマーク及びエストニアの法制度は、この規則に定める行政罰を認めていない。行政罰に関する定めは、デンマークにおいては、権限を有する自国の裁判所によって刑事罰として科されるものとし、そして、エストニアにおいては、監督官によって軽罪処罰の枠組みの中で科されるものとするという方法で適用することができる。ただし、これらの構成国におけるそのような法令の適用が監督官によって科される行政罰と同等の効果を有する場合に限る。それゆえ、権限を有する自国の裁判所は、罰金を

具体的な違反行為及びそれに対する行政罰の金額の上限については、同条の第 4 項ないし第 6 項によって、以下のとおり規定されている。

> 4. 以下の条項の違反行為は、第 2 項に従い、1000 万ユーロ以下の行政罰に服するものとし、または、企業の場合には、直前の会計年度における世界全体での売上総額の 2 %以下の金額、もしくは、いずれか高額のほうの行政罰に服するものとしなければならない：
> (a) 第 8 条、第 11 条、第 25 条ないし第 39 条並びに第 42 条及び第 43 条による管理者及び処理者の義務の違反行為；
> (b) 第 42 条及び第 43 条による認証機関の義務の違反行為；
> (c) 第 41 条第 4 項による監視機関の違反行為。
> 5. 以下の条項の違反行為は、第 2 項に従い、2000 万ユーロ以下の行政罰に服するものとし、または、企業の場合には、直前の会計年度における世界全体での売上総額の 4 %以下の金額、もしくは、いずれか高額のほうの行政罰に服するものとしなければならない：
> (a) 同意の条件を含め、第 5 条、第 6 条、第 7 条及び第 9 条による処理の基本原則；
> (b) 第 12 条ないし第 22 条によるデータ主体の権利；
> (c) 第 44 条ないし第 49 条による第三国または国際機関内の取得者に対する個人データの移転；
> (d) 第 9 章に基づいて採択された構成国の法律による全ての義務(25)；
> (e) 第 58 条第 2 項により監督官によって行われた命令、処理の一時的もしくは確定的な制限またはデータ移転の停止への不服従、または、第 58 条第 1 項に違反するアクセス提供の失敗。
> 6. 第 58 条第 2 項に示す監督官の命令に対して服従しない行為は、本条の第 2 項に従い、2000 万ユーロ以下の行政罰に服するものとし、または、企業の場合には、直前の会計年度における世界全体での売上総額の 4 %以下の金額、もしくは、いずれか高額のほうの行政罰に服するものとしなければならない。

加えて、一般個人データ保護規則 GDPR 第 83 条第 5 項(e)、同条第 6 項及び同法第 84 条第 1 項相互の論理的関係については、やや不透明な部分が残るが、この点を一応措くと、同法第 83 条第 6 項は、監督官による是正命令がまず行われ、それに対して服従しない管理者（日本国の個人情報保護法では取扱事業者）に対して

科すべしとする監督官からの勧告を考慮に入れなければならない。いずれの場合においても、罰金は、効果的で、比例的で、抑止力のあるものでなければならない」とある。

(25) 日本国政府は、EU の全ての構成国の関連法制を常に継続的に調査し、どのような行為が違反行為となるのかについて正確な法情報を収集した上で、その調査結果を国民に開示・公表すべきことになろう。

罰則（行政罰）の適用があるという手続構造を採用している。

また、同法84条第1項は、「構成国は、この規則の違反行為、とりわけ第83条による行政罰に服さない違反行為に対して適用可能な他の刑罰に関する法令を定めなければならず、また、その法令が実装されることを確保するために必要となる全ての措置を講じなければならない。その罰則は、効果的であり、比例的であり、かつ、抑止力のあるものでなければならない」と定めており、行政罰とは別に、刑事罰による制裁を定めている。

2．4　不適切な職務遂行があった場合の是正・司法救済

一般個人データ保護規則GDPRの第78条第1項ないし第3項は、監督官の処分に対する不服申立について、以下のとおり定めている。

> 1. 他のいかなる行政上の救済または裁判外の救済をも妨げることなく、個々の自然人または法人は、それらの者と関係する監督官の法的拘束力のある決定に対する効果的な司法救済を得る権利を有する。
> 2. 他のいかなる行政上の救済または裁判外の救済をも妨げることなく、第55条及び第56条により職務権限を有する監督官が異議申立てに対して何も対処しない場合、または、第77条により申立てられた異議の進捗状況もしくは結果についてデータ主体に対して3か月以内に通知をしない場合には、個々のデータ主体は、効果的な司法救済を得る権利を有する。
> 3. 監督官の判断に対する訴訟手続は、監督官が設置されている構成国の裁判所で提起されなければならない。

また、一般個人データ保護規則GDPRの第83条第8項は、監督官による罰則の適用について、「本条による監督権の権限の行使は、効果的な司法救済及び適正手続の保障を含め、欧州連合及び構成国の法律に従い、適切な手続上の安全性確保措置に従うものとしなければならない」と規定している。この安全性確保措置（safeguards）(26)とは、主として、職務の適正を担保するための法的措置のこと

(26) 日本国の個人情報保護法第20条は、安全管理措置として「個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない」と定めている。また、行政機関個人情報保護法第6条第1項は、安全確保の措置として、「行政機関の長は、保有個人情報の漏えい、滅失又はき損の防止その他の保有個人情報の適切な管理のために必要な措置を

を意味する。その中には、各構成国の法制に従い、権限行使それ自体の適切さを担保するための手続（行政手続・情報公開・不服申立・懲戒処分）が定められ、また、監督官の構成員（委員）の職務上の守秘義務が定められていることなどを意味すると解される。

3　個人データ保護以外の監督官の職務

3. 1　情報セキュリティ

個人データの安全性は、データの法的属性や社会的機能という観点から、プライバシーを保護法益とする個人データ保護という側面を有すると同時に、データ処理それ自体の防護という観点から、情報セキュリティという側面をも有する。通信回線を介してデータ交換を行う情報システム(27)では、特にこのことが顕著である。

いずれの観点に基づく場合でも、データの完全性・機密性・可用性が直接の保護の対象となる(28)。しかし、個人データの法的保護という場合には、データの完全

講じなければならない」と定めている。これらの「措置」は、技術的な措置及び組織的な措置の両方を含むものであり、EU の法制における「safeguards」とほぼ同様の法的意義を有するものと解することができる。安全性確保のための技術的な措置に関しては、様々な国際的な技術標準が策定されており、各国とも基本的にはそのような技術標準を判断基準として政策を遂行している。安全性確保のための組織的な措置の中でマネジメントシステムとして国際的に標準化されている部分についても同様であるが、事柄の性質上、各国の国家体制や社会環境等の相違により大きく異なる部分がある。これに対して、安全性確保のための法的な措置という観点からは、今後、綿密な比較法的検討及び比較社会制度論的な検討を尽くした上で、合理的な立法提案を重ねる必要がある。

(27) 日本国の法制上では、インターネットを含む電子通信上のプライバシー保護に特化した内容をもつ一般的な個人情報保護法令は存在しない。ただし、関連する法令として、個人情報保護法、電気通信事業法（昭和 59 年法律第 86 号）、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）、私事性的画像記録の提供等による被害の防止に関する法律（平成 26 年法律第 126 号）及び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。なお、法令ではないが、日本国政府のガイドラインとして、総務省総合通信基盤局消費者行政課・消費者庁取引対策課「特定電子メールの送信等に関するガイドライン」（平成 23 年 8 月）がある。

(28) 一般に、情報セキュリティマネジメントの領域においては、「機密性（confidentiality）」は「承認されていない個人、組織、プロセスに対して情報を利用可能なものとせず、か

性・機密性・可用性を保護することによって、保護法益であるプライバシーの権利が保護されるという規範の階層構造が存在する。情報セキュリティにおいては、データの完全性・機密性・可用性を保護することによって、保護法益である情報システムによるデータ処理の安全性に対する信頼が保護されるという規範の階層構造が存在する。後者の「信頼（trust）」は主観的な期待またはそのような期待の総体に過ぎないものであるので、その信頼が確実なものであることを担保するための何らかの社会的な仕組みが必要となる(29)。

EUにおいては、情報通信における個人データの保護を目的とする特別法として、電子通信プライバシー保護指令2002/58/EC、そして、情報セキュリティの確保を目的とするネットワーク及び情報システムの安全性に関する指令(EU) 2016/1148がある。これらの指令中には、情報セキュリティ上のリスク及びインシデントに対する対応と関連する監督官の特別の職務に関する条項がある(30)。

3．1．1　電子通信プライバシー保護指令2002/58/ECにおける職務

電子通信プライバシー保護指令2002/58/ECは、電子的な手段を用いて行われる通信分野における個人データの保護を目的としている(31)。同指令の第1条は、以下のように定めている。

1. この指令は、電子通信分野における個人データの処理と関連する基本的権利及び自由、

つ、開示しないこと」と、「完全性（integrity）」は「正確であり完全であること」と、そして、「可用性（availability）」は「承認された組織の要求に応じて利用可能でありアクセス可能であること」と定義されている。

(29) 一般に、デフォルトは「信頼ゼロ」であることを大前提とした上で、一定程度の信頼を付与するための社会的な仕組みとして認証による信頼の確保が試みられており、現実に様々な認証機関が機能している。

(30) 一般に、同一の組織・機関が情報セキュリティと個人データ保護の両方の業務に従事する場合、規範の衝突（トレードオフの状態）が発生することがあり得る。このような問題については、論者の立場により様々な見解があり得るが、本稿では検討を割愛する。なお、この問題については、Serge Gutwirth, Ronald Leenes & Paul de Hert (Eds.), Reforming European Data Protection Law, Springer (2015) pp.253–289が参考になる。

(31) 通信分野におけるプライバシー保護の問題に関して、1990年代後半の世界各国の関連法令の比較法的検討結果を示すものとして、Blanca R. Ruiz, Privacy in Telecommunications: A European And An American Approach, Kluwer Law International (1997) があり、参考になる。

とりわけプライバシーの権利の均一なレベルでの保護を確保し、かつ、欧州共同体の中におけるそのようなデータの自由な移転及び電子通信機器類と役務の自由な移転を確保すべきことが求められる構成国の法令を、整合性のとれたものとする。

2. この指令にある条項は、第 1 項で示した目的のために、指令 95/46/EC の特則を定め、これを補完する。更に、この指令にある条項は、法人である加入者の正当な利益の保護を提供する。

3. この指令は、欧州連合条約の第 5 款及び第 6 款が適用されるような欧州共同体設立条約の適用範囲外の活動には適用されない。また、公共の安全、防衛、構成国の安全保障（その活動が構成国の安全保障上の事柄と関連するときは、構成国の経済発展を含む。）及び刑事法の分野に属する構成国の活動にも適用されない。

第 1 条第 3 項にある欧州連合条約（The Treaty of European Union）の第 6 款（Title 6）については、警察枠組み決定 2008/977/JHA との関連で後述するとおり、現在では、統合後の現行の欧州連合の機能に関する条約（TFEU）の第 82 条第 1 項となっている。また、欧州連合条約の第 5 款（Title V General provisions on the Union's external action and specific provisions on the common foreign and security policy）は、現行の TFEU の第 205 条、第 218 条、第 329 条、第 331 条が相当する。これらは、犯罪捜査及びテロ対策と関連する部分を多く含むもので、同条第 3 項は、この分野に関しては、電子通信プライバシー保護指令 2002/58/EC が適用されないことを明らかにしている。しかしながら、情報セキュリティ上の課題は、公的部門と民間部門の別を問わず、共通に存在するものである。

ところで、電子通信プライバシー保護指令 2002/58/EC の立法当初の条項の中には個人データ保護の職務を遂行する監督官に関する条項が含まれていなかった(32)。しかし、その後、指令 2009/136/EC(33) により、電子通信プライバシー保護指令

(32) 電子通信プライバシー保護指令 2002/58/EC の前身的な指令である通信分野における個人データの処理及びプライバシーの保護に関する欧州議会及び理事会の 1997 年 12 月 15 日の指令 97/66/EC の中にも監督官に関する条項は存在しない。なお、指令 97/66/EC は、指令 2002/58/EC の第 19 条により、2003 年 10 月 31 日に廃止された。

(33) Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of

2002/58/EC の第 4 条（安全性）の条項が大幅に改正され、情報セキュリティ業務との関連で、プロバイダから個人データの侵害の事実の通知を受けること、プロバイダが通知をしない場合には通知するように督促すること、通知を要すべき事柄について運用指針を策定すること（同条第 3 項）、並びに、指令第 29 条の作業部会（一般個人データ保護規則施行後は、欧州データ保護委員会（同規則第 68 条）と読み替える。）の委員としての活動を通じて、関連する書式等を制定することが定められている(34)。

この個人データの侵害は、指令 2009/136/EC による改正により付加された第 2 条 (i) において、「欧州共同体の公衆が利用可能な電子通信サービスに関する法令と関係において、移転され、記録保存され、または、その他の処理がなされる個人データの、偶発的または違法な、破壊、喪失、改変、無権限による開示またはアクセスを導くような安全性に対する侵害のことを意味する」と定義されている。

この定義は、一般的な情報セキュリティの領域における情報セキュリティの侵害と基本的に同じである。ただ、情報セキュリティの領域では「情報財」の完全性・機密性・可用性が保護法益になるのに対し、個人データ保護の領域では個人データの完全性・機密性・可用性が保護法益となる。そして、一般に、個人データは、情報財の概念に包摂される情報の類型の一種としてとらえることが可能である。このような観点からすれば、そもそも個人データ保護法制は、情報財の安全性を確保するための保護法制の一種であると理解することも可能となる。

論理的には以上のような関係になっているのであるが、実務上のあり方を想定してみると、個人データの侵害についての通知内容は、実質的には、個人データの形態をとっている情報財の安全性に対する侵害についての通知内容とほぼ常に一致することになり、相互に区別することは難しいし、データの保護の要否の判断及び保護のための具体的な手段の選択という場面においては、その区別の実益がないことが少なくないということを理解することができる(35)。

このことは、情報セキュリティに特化した別の指令（(EU) 2016/1148）によっ

consumer protection laws (OJL 337/11)

(34) 条文中では「職務権限を有する行政機関（competent authorities）」と定められているが、この行政機関（官庁）とは、個人データ保護監督官のことを指すと解すべきである。

(35) 保護法益に関する観点の相違から、損害賠償請求訴訟における訴訟物が異なるものとして構成され得ることは別の問題である。

て、より明確なものとされている。

3．1．2　ネットワーク及び情報システムの安全性に関する指令 (EU) 2016/1148 における職務

ネットワーク及び情報システムの安全性に関する指令 (EU) 2016/1148（以下「NIS 指令」という。）における監督官の職務については既に別稿において触れたとおりである(36)。その要点を再説すると、欧州連合における個人データ保護の法的枠組みは、原則として、コンピュータによって自動処理される個人データの保護を目的とするものであることから、コンピュータシステム及び電子データの技術的側面における保護を主眼とするネットワーク及び情報システムの安全性に関する指令に基づく様々な活動は、個人データの法的側面における保護を主眼とする個人データ保護監督官の業務と関連性をもたざるを得ない。そして、欧州連合における一貫性のある保護を達成するためには、監督官自身による異議の処理や行政監督権の行使及び裁判所による判断を含む法的な対処（これは、個人データ保護法制による。）といったような本来の職務だけではなく、情報システムの安全性を確保するための組織的な仕組みとの連携により、技術的な対処（これは、NIS 指令の枠組みに従う。）にも従事すべきことになる。

本稿においては、監督官の職務という観点から、NIS 指令における職務をやや詳しく検討しようと思う。

NIS 指令の第 1 条第 2 項は、同指令の目的として、以下のように定めている。

> (a) ネットワーク及び情報システムの安全性に関する自国の戦略を策定すべき構成国の義務を定め；
> (b) 構成国間での戦略上の共同活動と情報交換を支援・促進し、かつ、構成国間における信頼と機密を発展させるための共同グループを創設し；
> (c) 構成国間での信頼と機密の発展に寄与し、かつ、迅速で効果的な運用上の共同活動を促進するためのコンピュータセキュリティインシデント対応チームネットワーク（以下「CSIRT ネットワーク」という。）を創設し；
> (d) 重要サービス運営者及びデジタルサービスプロバイダに対する安全性確保及び通知の

(36) 前掲「EU の行政機関に適用される個人データ保護規則における基本概念―個人データ保護条約及び EU 一般個人データ保護規則との関係を含めて―」参照

義務を設け；
(e) 自国の担当官庁、連絡部局並びにネットワーク及び情報システムの安全性に関する職務を有する CSIRT を設置すべき構成国の義務を定める。

NIS 指令全体の構想としては、欧州連合全体が ENISA（European Network Information Security Agency）(37) の主導によるネットワーク情報システムセキュリティ戦略（Network and Information Security Strategy）の下に、関係する全ての構成国が参加するかたちで、一元的な連絡システムを通じて情報交換及び模擬演習等を実施する仕組みが構築される。

構成国は、構成国としての情報伝達の一貫性を確保するために、連絡部局（single contact point）という官庁（行政機関）を設置し（第 8 条）、これが欧州連合全体との連絡のための各構成国の接続点となる。構成国内には CSIRT（Computer Security Incident Response Team）(38) が設置され、CSIRT がインシデント情報の収集・伝達やリスクに関する情報交換のための主要な任務を遂行する（第 9 条）。この枠組みの中では、構成国内における関連組織間の共同活動（第 10 条）及び構成国と欧州連合との共同活動（第 11 条及び第 12 条）並びに国際的な連携（第 13 条）の重要性・必要性が重視されている。

重要インフラの運営者及び情報システムの提供者には、当該システムの安全性を確保すべき義務（第 16 条）並びに CSIRT に対してインシデントについて通知すべき義務がある（第 14 条、第 16 条）。この点について、NIS 指令の前文第 40 項は、「インシデントに関する情報は、一般市民及び企業、とりわけ中小企業にとっ

(37) ENISA は、一般に、「欧州ネットワーク情報セキュリティ庁」と訳されている。ENISA の活動内容は日本語に訳された各種ガイドライン等によって理解することができる。例えば、いずれも独立行政法人情報処理推進機構（IPA）の訳による「クラウドコンピューティング：情報セキュリティ確保のためのフレームワーク情報セキュリティ確保のためのフレームワーク」（2009 年 11 月）及び「クラウドコンピューティング：情報セキュリティに関わる利点、リスクおよび推奨事項情報セキュリティに関わる利点、リスクおよび推奨事項」（2009 年 11 月）が公表されている。

(38) CSIRT は、NIS 指令の草案の段階では、CIRT（Computer Incident Response Team）とされていた。実質的には同じような職務を遂行する組織を指すので、別名（Synonym）として扱われることが多い。日本国における公式の CIRT としては、JPCIRT コーディネーションセンター（JPCIRT CC）があり、CSIRT の団体としては、日本コンピュータセキュリティインシデント対応チーム協議会（Nippon CSIRT Association）がある。

てその重要性を増してきている。幾つかの事例では、そのような情報は、自国と関係するインシデント及びその発生に主に焦点を当てて、特定の国の言語を用い、自国のレベルで Web サイトを介して既に提供されている。企業が次第に国境を越えて業務を遂行し、市民がオンラインサービスを利用していることを考えると、インシデントに関する情報は、欧州連合レベルで集約された形態で提供されるべきである。CSIRT ネットワークの事務局は、Web サイトを運用し、または、既存の Web サイト上に専用ページを設置し、企業の利益と必要性に特に焦点を絞って、欧州連合内で発生して主要なインシデントに関する情報を一般市民が利用できるようにすることが望まれる。CSIRT ネットワークに参加する CSIRT は、機密または機微の情報を除き、その Web サイト上で公表されるべきインシデント情報を任意に提供することが求められる」と述べている。

どのようなネットワークが重要インフラのネットワークとして扱われるかの詳細については構成国が指定すべきものであるが、NIS 指令の別紙Ⅱ（Annex ⅠⅡ）は、電力事業者、送電システム事業者、石油パイプライン事業者、石油の生産、精製、施設管理、貯蔵及び送油の事業者、ガス事業者、航空運輸事業者、海上貨物事業者、港湾施設事業者、高度道路交通システムの管理者、証券取引所、DNS プロバイダ等を列挙している。

監督官は、以上のような NIS 指令の枠組みの中で、インシデント対応が個人データに対する侵害を発生し得る場合には、担当官庁と協力して対処しなければならない（第 15 条第 4 項）。また、監督官は、法執行機関（警察）と共に、担当官庁及び連絡部局の共同活動に関して協議に応じなければならない（第 8 条第 6 項）。

この点について、NIS 指令の前文第 63 項は、「多くの場合において、インシデントの結果として個人データが被害を受ける。この文脈においては、職務権限を有する行政機関とデータ保護監督官は、インシデントから生ずる個人データ侵害に対抗するための関連する全ての事柄について協力し、かつ、情報交換をしなければならない」と述べている。

要するに、監督官は、個人データの保護を目的とする独立の行政機関ではあるが、国防やテロ対策とも直結する情報システムの安全性確保という場面においても、一定の重要な役割を果たすことが期待されているということができる。したがって、この文脈においては、個人データ保護のための監督官は、単なる人権擁護

組織ではない。

3．2　犯罪捜査

犯罪捜査の過程では様々な個人データが収集される。捜査機関は、行政機関であるので、捜査機関における個人データの処理に関しては、欧州共同体の機関及び組織による個人データの処理と関連する個人の保護及び個人データの自由な移転に関する規則 (EC) No 45/2001 が適用されるのが原則であり（一般個人データ保護規則 GDPR 第 2 条第 3 項）、また、前科・前歴や有罪判決のような個人データは、構成国の法令によって定めるところに従い、法務当局によってのみ保存されなければならない（同規則第 10 条）。

このような犯罪捜査の過程で処理される個人データの法的保護に関しては、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 2008 年 11 月 27 日の理事会枠組み決定 2008/977/JHA（Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters・以下「警察枠組み決定」という。）が制定されていた。

この警察枠組み決定は、2016 年 4 月 27 日に制定された犯罪行為の防止、捜査、検知もしくは訴追または刑罰の執行のための職務権限を有する機関による個人データの処理と関連する自然人の保護及び個人データの自由な移転並びに理事会枠組み決定 2008/977/JHA の廃止に関する 2016 年 4 月 27 日の欧州議会及び理事会の指令 (EU) 2016/680（Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA・以下「警察指令」という。）によって、改正された(39)。

(39) 関連する欧州委員会の通知として、Safeguarding Privacy in a Connected World - A European Data Protection Framework for the 21st Century (COM(2012) 9 final) がある。

警察枠組み決定は、2018 年 5 月 6 日に廃止されるが（警察指令第 59 条第 1 項）、その廃止の日までは法規範としての有効性が維持される(40)。

警察指令は、同指令が EU 官報（Official Journal of the European Union L 119）によって公示された日である 2016 年 5 月 4 日の翌日である同年 5 月 5 日に発効（施行）となった（同指令第 64 条）。

警察枠組み決定及び警察指令には、犯罪捜査等の過程で処理される個人データの保護と関係する監督官の職務に関する条項がある。これらの条項は、一般法である個人データ保護指令 95/46/EC 及び一般個人データ保護規則 GDPR 並びに規則 (EC) No 45/2001(41) との関係では、一般法と特別法の関係にあると理解することができる(42)。

3．2．1　警察枠組み決定 2008/977/JHA における職務

警察枠組み決定の第 1 条第 1 項は、「この枠組み決定の目的は、刑事分野において、捜査共助及び刑事に関する司法共助の枠組みにおける個人データの処理と関連して、高いレベルでの公共の安全を保障しつつ、欧州連合条約の第 6 款に定める自然人の基本的な権利及び自由とりわけプライバシーの権利の高いレベルでの保護を確保することである」と規定している。

ここで引用されている欧州連合条約（The Treaty of European Union）の第 6 款（Title 6 Provision in police and judicial cooperation in criminal matters）は、英国の国家的な立場を尊重して欧州連合への加盟を可能とするための第 21 追加議定書の第 6 条 a によって一定の調整がなされた(43)。また、欧州連合条約の第

(40) 経過措置については、第 63 条に規定されている。なお、関連する欧州委員会の通知として、Safeguarding Privacy in a Connected World - A European Data Protection Framework for the 21st Century (COM(2012) 9 final) がある。

(41) 個人データ保護指令 95/46/EC 及び一般個人データ保護規則 GDPR 並びに規則 (EC) No 45/2001 は、公的部門（行政機関等）と民間部門の両方に適用される。ただし、一般個人データ保護規則 GDPR の第 2 条第 3 項により、欧州連合の機関については、規則 (EC) No 45/2001 が適用される。これらの相互関係については、前掲「EU の行政機関に適用される個人データ保護規則における基本概念―個人データ保護条約及び EU 一般個人データ保護規則との関係を含めて―」で述べた。

(42) 警察の活動における個人データ保護と関連する様々な法的問題については、Cristina Blasi Casagran, Global Data Protection in the Field of Law Enforcement: An EU Perspective, Routledge (2016) が詳細に論じている。

(43) 2016 年の国民投票によって英国は欧州連合からの離脱を決定することとなった。その社

6款は、欧州の機能に関する条約（TFEU）との統合の結果、現在では廃止された。TFEUの統合の結果、旧欧州連合条約の第6款で規定されていた条項の中で自然人の基本的な権利及び自由とりわけプライバシーの権利の高いレベルでの保護に関しては、現行のTFEUの第16条が該当する条文となっており、また、同様に、捜査共助及び刑事に関する司法共助に関しては、現行のTFEUの第82条第1項が該当する条項となっている(44)。

そして、同決定の第1条第2項は、犯罪行為の防止、捜査、検知もしくは訴追または刑罰の執行のために個人データが構成国間で移転もしくは利用される場合、または、構成国と欧州連合の機関の間で移転もしくは利用される場合(45)について、「この枠組み決定に従い、構成国は、自然人の基本的な権利及び自由とりわけプライバシーの権利を保護しなければならない」と規定している(46)。

警察枠組み決定は、データ主体の権利の保護のために監督官（supervisory

会的・経済的・政治的な背景については様々な見解がある。国際的な諜報活動という側面から考察すると、英国の諜報機関にとって、欧州連合の個人データ保護法制が大きな足かせとなってきたことは否定しようのない事実である。後述のデータ保持指令を無効とする欧州司法裁判所の先決裁定は、英国が離脱を決意する隠れた真の引き金となっていた可能性が疑われる。このことは、国連の関連機関をはじめ世界各国の人権団体等から集中的に非難の的とされてきた捜査権限法案（Investigatory Powers Bill）が、英国の欧州離脱決定の後になって、その可決・制定に向けて急速に事態が進展することとなったという歴史的事実によっても支持され得る。

(44) TFEUの第82条第1項に基づき、指令2014/41/EU（Directive 2014/41/EU of the European Parliament and the Council of 3 April 2014 regarding the European Investigation Order in criminal matters）が制定されている。同指令の制定の際、欧州データ保護監督官は、意見書（OJ C 355, 29.12.2010, p.1.）を提出したが、実質的には「特に意見はない」という内容になっている。

(45) 構成国間における前科・前歴に関する情報の交換は、ECRIS（European Criminal Records Information System）という自動処理システムを介して一元的に行われる。なお、この関連では、Priscillia Hunt, Beau Kilmer & Jennifer Rubin, Development of a European Crime Report: Improving safety and justice with existing crime and criminal justice data, European Commission (2009) 及び Els De Busser, Blueprint for an EU criminal records database: Legal, politico-institutional and practical feasibility, Maklu (2002) が参考になる。

(46) 欧州委員会の報告書として、Report from the Commission to the European Parliament and the Council on the implementation of Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from criminal record between Member States (COM(2016) 6 final) がある。

authorities）が関与することを定めている。

同枠組み決定の前文第 24 項は、この枠組み決定に定める監督官と個人データ保護指令 95/46/EC の監督官との関係について、「指令 95/46/EC に基づいて構成国で既に設置されている監督官は、この枠組み決定に基づいて設置されるべき自国の監督官によって遂行されるべき職務について責任を負うものとみなされる」と述べている。

また、同枠組み決定の第 25 条第 1 項は、構成国の監督官（national supervisory authorities）に関して、「各構成国は、この枠組み決定によって構成国が採択した法令の構成国領土内における適用について助言し、それを監視することに責任を有する 1 または複数の行政機関を定めなければならない。これらの行政機関は、それらに与えられた職務権限を行使するについて、完全に独立してこれを行わなければならない」と規定し、同条第 3 項は、「各監督官は、個人データの処理と関連する権利及び自由に関していかなる者から申立てられた異議についても聴聞しなければならない。関係者は、その異議の結果について通知を受けるものとしなければならない」と規定している。

そのことから、個人データ保護指令 95/46/EC の監督官と警察枠組み決定の監督官は、実際には同一の行政機関であるように読める。ところが、その職務内容を個別に検討してみると、一般個人データ保護規則 GDPR の第 37 条ないし第 39 条に規定するデータ保護責任者（data protection officer）の職務に該当するものと理解することも可能である。

例えば、監督官が関与すべき場面に関して、警察枠組み決定第 10 条第 1 項は、「個人データの移転は、全て、そのデータの適法性を検証し、かつ、データの完全性及び安全性が正常なものであることを確保するために、記録化または文書化されなければならない」と定めた上で、同条第 2 項は、「第 1 項に基づいて行われる記録化または文書化は、データ保護の管理について職務権限を有する監督官に対し、その要請に応じて、通知されなければならない。職務権限を有する監督官は、この情報を、データ保護のため並びに正常なデータ処理及びデータの完全性と安全性を確保するためにのみ用いなければならない」と定めている。ここに規定されている内容は、情報セキュリティの専門家であるデータ保護責任者（data protection officer）の職務内容であって、監督官（supervisory authorities）の職務ではな

いようにも読める。

しかしながら、警察枠組み決定の第17条第1項は、データ主体のアクセスの権利(47)に関して以下のとおりに規定しており、この内容は、明らかに監督官（supervisory authorities）の職務内容である。なお、警察枠組み決定における「管理者（controller）」とは、犯罪捜査に従事する法執行機関（警察）や前科・前歴データを管理・保存する法務当局等の行政機関のことを指す。

> 1. 全てのデータ主体は、合理的な期間内に、無条件で、かつ、過剰な遅延もしくは費用負担なく、以下の事項の要求に対する回答を、以下の者から受ける権利を有する：
> (a) 少なくとも、彼に関連するデータが移転もしくは利用されたか否か、及び、処理されているデータの開示を受けもしくはその伝送を受けた取得者もしくは取得者の類型に関する情報に関して、管理者または自国の監督官から確認を得ること；
> (b) 少なくとも、必要な全ての検証が実施されているということについて、自国の監督官から確認を得ること。

ここに定める権利は、「確認」を得ることが限度であり、個人データ保護規則95/46/EC及び一般個人データ保護規則GDPRの定めるアクセスの権利の内容とは相当に異なる。これは、当該データが処理されている状況（犯罪捜査の過程における処理、前科・前歴データの保存等）の特殊性に起因するものと考えることができる。

加えて、警察枠組み決定の第17条第2項は、アクセスの権利の例外について、以下のとおりに定めている。

(47) 犯罪記録へのアクセスの権利に関しては、Serge Gutwirth, Yves Poullet, Paul de Hert & Ronald Leenes (Eds.), Computers, Privacy and Data Protection: an Element of Choice, Springer (2011) pp.111–137が参考になる。なお、データ主体のアクセスの権利は、主として、このシステムで開示可能な個人データ及び関連情報との関係で問題となり得る。日本国においては、一般に、情報公開法に基づく情報公開請求（開示請求）という観点から論じられることが多い。しかし、国民が有する一般的な情報公開を求める権利と、データ主体の「アクセスの権利（知る権利）」を実現するための手段的・技術的・人工的な権利としてアクセスの権利とは、法制度上の性質を異にする別のものとしてとらえる必要がある。それは、一般的な情報公開制度における保護法益は一般的な公共の利益であり得るのに対し、犯歴データ等へのアクセスの権利は、適切でない個人データの自動的な処理に伴う当該個人の私生活の権利に含まれるプライバシーの利益に対する社会からの脅威の除去という私的な法益の保護としての法的性質が強いからである。

2. 構成国は、当該制限が、関係者の正当な利益について十分に配慮し、必要かつ比例性原則に則った措置である場合には、以下のために、第 1 項 (a) による情報へのアクセスを制限する立法措置を採択することができる：

(a) 公的もしくは適法な研究、捜査または訴訟手続の阻害を避けるため；

(b) 犯罪行為の防止、検知、捜査及び訴追または刑罰の執行の妨げとなることを避けるため；

(c) 公共の安全を防護するため；

(d) 国家の安全を防護するため；

(e) データ主体を保護するため、または、他の者の権利及び自由を保護するため。

このようなアクセスの制限があった場合やそもそも全く拒絶されてしまった場合の法的救済措置について、警察枠組み決定の第 17 条第 3 項は、「アクセスの拒否または制限は、全て、データ主体に対して書面によって行われなければならない。同時に、その決定が根拠とする事実関係及び法的根拠もまた、彼に対して通知されなければならない。後者の通知は、第 2 項 (a) ないし (e) に基づく理由がある場合には、省略することができる。これら全ての場合について、データ主体は、彼が職務権限を有する自国の監督官、法務当局または裁判所に対して不服申立をすることができるということを告知されなければならない」と規定している。同様に、同枠組み決定の第 18 条第 1 項は、「データ主体は、この枠組み決定から生ずる個人データの訂正、削除または停止に関する第 4 条、第 8 条及び第 9 条に従って管理者がその義務を遂行することを管理者に対して期待する権利を有する。構成国は、データ主体がこの権利を管理者に対して直接に行使するものとするか、または、職務権限を有する自国の監督官を介して間接的に行使するかについて定めなければならない」、「また、構成国は、見直しの措置が講じられたことについて、データ主体が職務権限を有する自国の監督官から通知を受けるべきものとすることを定めることができる」と規定している。

以上から、警察枠組み決定における監督官とは、個人データ保護指令 95/46/EC に規定する監督官と同一のものを指すと解する。ただ、上記のようにデータ保護責任者の職務に相当する内容を示す条項も存在することから、職務内容の相違に応じて、構成国が異なる機関・組織に職務を分掌させるように法令を制定することを認

めていると解釈することのできる余地がある(48)。

いずれにしても、これらの監督官の職務は、法執行機関（警察）による犯罪捜査のための行為それ自体とは異なるものであるし、前科・前歴のデータを保管する法務当局の職務とも異なる。しかし、警察枠組み決定における監督官の職務は、法執行機関（警察）による犯罪捜査等の活動と密接な関連を有するものである。

3．2．2　警察指令 (EU) 2016/680 における職務

警察指令第１条第１項は、「この指令は、公共の安全に対する脅威への防護及び防止を含め、犯罪行為の防止、捜査、検知もしくは訴追または刑罰の執行のための職務権限を有する行政機関による個人データの処理と関連する自然人の保護に関する規律を定める」と規定している。

ここでいう職務権限を有する行政機関（competent authorities）とは、犯罪捜査を行う法執行機関（警察）や前科・前歴データを保存する法務当局のことを指す。そして、同条第２項は、「この指令に従い、構成国は、(a) 自然人の基本的な権利及び自由並びにとりわけ自然人の個人データの保護の権利を保護し、かつ、(b) 欧州連合内の職務権限を有する行政機関による個人データの交換について、当該交換が欧州連合の法律または構成国の法律によって求められる場合において、個人データの処理と関連する自然人の保護と関係しているという理由によって禁止されることがなく、制限されることもないことを確保しなければならない」と規定している。

この目的条項に示されているとおり、この指令は、基本的には、法執行機関（警察）や法務当局の権限行使に伴う個人データの処理について法的保護のための安全性確保措置（safeguards）を定めると同時に、欧州連合内の各構成国における個

(48) この点については、今後、欧州連合における各構成国の法令及びその実際の運用を踏まえた比較法的・実証的な研究が尽くされることを期待したい。一般に、日本国においては、EU の規則及び指令のレベルでの研究及び EU の指令や規則の解釈を示す欧州司法裁判所及び欧州人権裁判所の判例の研究は比較的よくなされているものの、EU の指令や規則を実装する構成国の法令やその解釈を示す構成国裁判所の判例についての比較法的な研究は、かなり手薄であるということができる。これは、構成国の言語が多岐に分かれており、同一の研究者が全ての言語及びその言語を用いた法令や判例について全て精通することが不可能または非常に困難なことに起因するものと推定される。このような場面においてこそ、共同研究という学術上の研究方法の利点が最大限に活かされるべきであり、そのための研究費の支援策が講じられるべきである。

人データ保護のための法規範を整合性のとれたものとすることによって、単に個人データであるというだけの理由で個人データの交換が妨げられないようにし(49)、構成国の法執行機関（警察）の間での犯罪捜査目的での個人データの交換の妨げとなる法的障害を除去すること(50)を目的とするものとして理解することができる。

警察指令は、その全部または一部が自動的な方法で処理される個人データについて適用され、また、自動処理される個人データ以外の個人データであってもファイリングシステムの一部を構成する個人データ、もしくは、ファイリングシステムの一部を構成する予定の個人データについても適用される（第 2 条第 2 項）。それゆえ、自動処理及び検索の対象とすることを全く予定していない個々の孤立した個人データについては、この指令が適用されることはない(51)。ここでいうファイリン

(49)「デフォルトは悪」であるので、単に個人データの交換（処理）だけで本来は違法行為となるということを大前提としている。そのような大前提があること踏まえ、各構成国は、違法行為を適法行為とするための法的根拠（legal basis）を定めている。これは、刑事訴訟における強制処分が法律に基づかなければならないのと同じことである。ただ、その法律が区々になっている場合には、構成国間における個人データの移転（交換）に支障が生ずることになるので、その整合性を確保しなければならない。整合性が確保された状態では、整合性のある共通の法的根拠が構成国に存在していることになるので、当該法律に従って行われる個人データの移転（交換）は、適法な移転行為であり、単なる移転行為（違法行為）ではない。

(50) この警察指令は、「個人データの交換」だけを独立の目的としているわけではない。そして、同指令は、いわゆる「利活用」と呼ばれる場合を含め、犯罪と関連する個人データの域内市場における商業的な流通を促進しようとする意図を全く有していない。一般に、EU における個人データ保護法制において個人データの「自由な移転」と呼ばれるものは、文脈から切り離されて個人データの流通それ自体を促進しようとするものではなく、特定の目的に基づく情報システムによる個人データの処理が域内市場において支障なく円滑に行われるようにするため、個人データ保護のための法制の相違が非関税貿易障壁のように作用しない状態とすることを目的としている。単に販売・流通させることだけを目的とするような個人データの処理は、自己目的的なものであり、適法な特定の目的に基づく個人データの処理としては認められない。この警察指令においても、犯罪捜査やテロ対策等の特定の目的のために構成国の法執行機関（警察）相互での情報共有を円滑に行うことが目的であり、そのために、各構成国における警察関連の個人データ保護法制の相違に伴う不合理な障壁を解消しようとするものである。この個人データの交換（処理）は、欧州連合または構成国の法律に基づくものであることを要するので、合意または契約による交換をすべきことが法律によって定められている場合を除き、構成国間の合意または契約のみをその法的根拠（legal basis）とすることができない。

(51) この点は、個人データ保護指令 95/46/EC 及び一般個人データ保護規則 GDPR においても基本的には同じである。日本国においては、従来、関連する EU の法令の原文（一次資料）を詳細に検討しないまま、特定の理屈に基づいて無理にあてはめた個人情報保護理論を述べる書籍や論説等が決して少なくなく、その中には、電子的な自動処理を前提と

グシステム（filing system）について、同指令の第3条(6)は、「個人データの構成された集合体であって、機能上または地理上における集中型、放射状型または分散型の別を問わず、特定の基準に従ってアクセスすることのできるものを意味する」と定義している(52)。

警察指令は、警察枠組み決定の改正法として制定されたものであるので、その内容は非常によく似ているが、個人データ保護の職務を遂行する監督官の関与に関してはより詳しく規定されている。

警察指令の第4条は、個人データ保護の基本原則として、以下のとおりに定めている。

1. 構成国は、個人データが以下のとおりであることを定めなければならない：
(a) 適法かつ公正に処理されること；
(b) 特定の、明示かつ適法な目的のために収集され、かつ、その目的に適合しない方法で処理されないこと；
(c) それが処理される目的との関係において十分であり、関連性があり、かつ、過剰でないこと；
(d) 正確であり、かつ、必要があるときは、最新のものに維持されること；それが処理される目的を考慮した上で、不正確なデータが遅滞なく消去または訂正されることを確保するための全ての合理的な手立てが講じられなければならない；
(e) それが処理される目的のために必要な期間内においてのみ、データ主体の識別を許す方式で保存されること；
(f) 無権限の処理または違法な処理に対する防護、事故による喪失、破壊または毀損に対する防護、適法な技術上の措置または組織上の措置を用いることを含め、個人データの適切な安全性を確保する方法で処理されること。
2. 第1条第1項に定めるいずれかの目的のために、個人データを収集する目的とは別の目的のための同じ管理者または別の管理者による処理は、以下の場合においてのみ認められる：

しない個人データについても広く包含するものとして個人情報保護法制やプライバシー保護法制を論ずるものがないわけではない。特に一定の政治思想的志向性の強い著作や世界中のどこにおいても是認され得ない独自の理解に基づくような著作ではそのような傾向が顕著であった。しかし、少なくとも、EUの法制がどのようなものであるかを正確に認識・理解するという文脈の中では、とりわけ、法情報論という枠組みの中では、それらの一定の傾向性をもったアプローチとは異なる客観的かつ検証可能という意味での実証的なアプローチが採用されるべきである。

(52) この定義は、一般個人データ保護規則GDPRの第4条(6)に定める定義と同じである。

(a) 当該個人データをそのような別の目的のために処理することについて、管理者が、欧州連合または構成国の法律によって認められている場合；及び、
(b) 欧州連合または構成国の法律に従い、当該目的による処理が必要であり、かつ、適切である場合。

3. 第 1 条第 1 項においては、同じ管理者または別の管理者による処理は、公共の利益におけるアーカイブ、科学調査、統計または歴史調査の目的による利用であって、データ主体の権利及び自由のための適切な安全性確保措置に服するものとして行われるものを含むことができる。

4. 管理者は、第 1 項、第 2 項及び第 3 項の遵守について責任を有し、そのことを説明することができるものとしなければならない。

第 4 条の第 3 項の統計の目的、科学調査及び歴史調査の目的による個人データの処理は、一般に、個人データ保護法制における例外処理または適用除外の事項とされている事項である(53)。

欧州評議会の個人データ保護条約（ETS No.108）の第 9 条第 3 項は、「統計の目的または科学調査の目的で用いられる自動的な個人データファイルに関して、データ主体のプライバシーの侵害の明白なリスクがない場合には、法律によって、第 8 条の b、c 及び d に示す権利の行使の制限を定めることができる」と定めており、また、一般個人データ保護規則 GDPR の前文第 156 項は、「構成国は、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行われる個人データの処理のための安全性確保措置について定めなければならない。構成国は、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を達成するために個人データの処理がなされる際には、特別の要件の下に、データ主体のための適切な安全性確保措置を条件として、通知義務、並びに、訂正の権利、削除の権利、忘れられる権利、処理の制限の権利、データの可搬性の権利及び異議を述べる権利に関し、その細目及び特例を定めることが認められる」と述べている。

(53) 統計の目的による処理における安全性確保に関しては、工藤弘安・大屋祐雪・山田茂・森博美「官庁統計制度と統計調査の現状」日本統計学会誌 22 巻 3 号 613～654 頁（1993）、森博美「諸外国における行政情報の統計利用の現状とわが国統計の課題」経済志林 73 巻 3 号 817～869 頁（2006）、Josep Domingo-Ferrera & Vicenç Torrab, Disclosure risk assessment in statistical data protection, Journal of Computational and Applied Mathematics, Volumes 164–165 pp.285–293 (2004) が参考になる。

警察指令の第4条第4項の「説明」は、いわゆる透明性の原則（transparency）または説明責任の原則の現れの一種と理解することができる。とりわけ、アクセスの権利に基づく情報開示の要求において意味がある（ただし、公共の利益等に基づく一定の制限がある。）。また、第4項のアーカイブ（archiving）は、公共の利益のために行われる場合に限定され、営利目的の場合を含め、私的な目的の場合を含まない(54)。

警察指令の第5条は、個人データを保存することのできる期間制限に関して、「構成国は、個人データの消去のために、及び、個人データを記録保存すべき必要性の定期的な見直しのために、適切な期間制限を設けることを定めなければならない」と規定している。

そして、警察指令は、データ主体の権利として、情報の開示を求める権利（第13条）、管理者から確認を得る権利（第14条）、訂正または削除を求める権利（第16条）を定めている。これらの権利の中で、第13条の権利及び第14条の権利は、従来はアクセスの権利とされていたものを更に細分化した権利である（第15条にアクセスの権利の制限についての規定がある。）(55)。

警察指令の第17条は、データ主体が自ら直接に権利を行使するのではなく、監督官によって権利を行使する場合の確認の手続について、以下のとおりに定めている。

> 1. 第13条第3項、第15条第3項及び第16条第4項に示す場合について、構成国は、データ主体の権利が職務権限を有する監督官を介することによっても行使できるようにすることを定める措置を採択しなければならない。
> 2. 構成国は、管理者がデータ主体に対して第1項により監督官を介して彼または彼女の

(54) 民間の検索エンジンサービスの提供のために行われる自動的なデータ収集が警察指令第4条第4項のアーカイブに含まれるか否かは、大きな検討課題の1つである。この問題は、公共の利益のために活動する主体が公的機関に限定されるのか、それとも、営利企業も含まれるのかという問題を含んでいる。一般に、私的な施設としての博物館、美術館または図書館等が一般公衆の利用を認めている場合、そのような私的な施設が「公共の利益のためには存在していない」と断定することは難しい。なお、一般に、情報システムにおけるデータのバックアップ処理は、アーカイブに含まれないと理解されている。しかし、ビッグデータのような場合については、十分に検討がなされているとは言えない状況にある。

(55) これらの条項は、既述の警察枠組み決定に定めるアクセスの権利と対応するものである。警察指令におけるアクセスの権利の法的性質についても、警察枠組み決定におけるのと同様に考えることができる。

権利を行使することができることについて通知すべきものと定めなければならない。
3. 第 1 項の権利が行使される場合、監督官は、データ主体に対し、少なくとも、監督官によって全ての必要な確認がなされたことまたは評価が行われたことを通知しなければならない。また、監督官は、データ主体に対し、彼または彼女の司法救済を受ける権利について通知しなければならない。

他方において、警察指令は、管理者（警察、法務当局等）が個人データの処理をする場合には、その処理を開始する前にデータ保護影響評価を実施しなければならず（第 27 条）、かつ、監督官と事前協議をすべきこと（第 28 条）を定めている。これは、一般個人データ保護規則 GDPR の第 35 条に定める事前評価及び同規則の第 36 条に定める事前協議と同趣旨のものである。警察指令の第 28 条は、以下のとおり定めている。

1. 構成国は、以下の場合においては、管理者または処理者が、新たに編成されるファイリングシステムの一部を構成する処理を行う前に、監督官と協議すべきことを定めなければならない：
(a) 第 27 条に規定するデータ保護影響評価の結果が、リスクを軽減するための措置が管理者によって講じられていない場合に高度のリスクを生じさせる可能性があることを示している場合；
(b) 処理のタイプが、とりわけ、新しい技術、仕組みまたは手順を用いる場合に、データ主体の権利及び自由に対する高度のリスクを含んでいる場合。
2. 構成国は、処理に関して、自国の議会によって採択される立法措置またはそのような立法措置に基づく行政規則上の措置の草案を準備する間、監督官が相談に応ずるべきことを定めなければならない。
3. 構成国は、第 1 項による事前協議の対象となる処理業務のリストを監督官が策定することができることを定めなければならない。
4. 構成国は、管理者が、第 27 条によるデータ処理影響評価の結果を監督官に提供することを定めなければならず、また、処理の適合性、とりわけ、データ主体の個人データの保護に対するリスク及び関連する安全性確保措置について監督官が評価することができるようにするその他の情報を提供することを定めなければならない。
5. 構成国は、本条の第 1 項に示す予定されている処理がこの指令により採択された法令に違反する場合、とりわけ、リスクを適切に特定し、それを軽減していない場合、監督官が、協議の要請を受けた時から 6 か月以内に、管理者に対し、または、それが適切なときは処理者に対し、書面による助言を提供することを定めなければならず、また、第 47 条

に示す監督官の権限を行使することができることを定めなければならない。この期限は、予定されている処理の複雑性を考慮に入れて、1か月延長することができる。監督官は、管理者に対し、または、それが適切なときは処理者に対し、協議の要請を受けた時から1か月以内に、遅延の理由を付して、その期限延長について通知しなければならない。

一般に、民間企業の場合においては、事前の影響評価や監督官との事前協議に関して違和感をもつ者は比較的少ないであろうと考えられるが、警察指令における「管理者（controller）」とは法執行機関（警察）または前科・前歴データを管理・保存する法務当局のことを指すので、構成国の国家権力作用の中でも特に機密性の高い部分について監督官が関与するという事実に留意しなければならない。

例えば、問題となる処理が犯罪捜査のための前歴データの処理に基づくプロファイリングシステムにおける個人データの処理である場合、あるいは、犯罪防止のための監視システムにおける個人データの処理である場合(56)、その個人データ処理影響評価の結果を示す文書の中には高度の機密事項が含まれることがあり得るし、事前協議の内容も同じである。ここでもまた、監督官は、単なる人権擁護のための組織・団体ではあり得ないことを理解することができる。

以上を前提として、警察指令における監督官の職務は、多岐にわたるが、第41条ないし第49条において監督官の職務権限、義務等について定めているほか、監督官の共同活動（第26条）、データ主体の権利の侵害があった場合において管理者が72時間以内に監督官に連絡すべき義務及びその場合における監督官の関与（第30条、第31条第4項）、データ保護責任者の連絡先についての通知（第32条第4項）、監督官とデータ保護責任者との共同活動（第34条(d)）、データ移転の際の監督官の関与（第36条第2項、同条第3項、第37条第2項及び同条第3項）等を定

(56) スティーヴン・スピルバーグ監督及びトム・クルーズ主演の映画『マイノリティ・リポート（Minority Report）』（2002年）に描かれている監視システムは、2002年当時においてはSF（science fiction）の一種であったかもしれない。しかし、現時点では、この映画の中で描かれていることの大部分が既に普通の現実の一部となってしまっている。そのシステムは、犯罪の防止（探知及び行動予測）の目的で設置・運営されている監視システムであるので、警察指令(EU) 2016/680の適用がある。この映画のストーリー上の結末では、監視システムそれ自体に問題があることが判明し、その監視システムの利用が禁止されるということになっている。これを同指令の適用に引き直して考え見ると、監督官が第16条及び第47条に基づき、処理業務の禁止または制限を命ずべき場合に該当するものとして理解することができる。

めている。

警察指令の第 46 条第 1 項は、監督官の職務について定めている。その内容は、前述の一般個人データ保護規則第 57 条に定めるところとほぼ同じである。

また、警察指令の第 47 条は、以下のとおり、監督官の権限について定めている。

> 1. 各構成国は、監督官が効果的な調査の権限を有することを法律によって定めなければならない。この権限は、少なくとも、処理されている全ての個人データに対するアクセス及び監督官の職務を遂行するために必要となる全ての情報に対するアクセスを管理者及び処理者から得る権限を含むものとしなければならない。
> 2. 各構成国は、監督官が、例えば、以下のような効果的な是正権限をもつことを、法律によって定めなければならない：
> (a) 管理者または処理者に対し、予定されている処理業務がこの指令により採択された法令に違反する可能性があるという注意を発すること；
> (b) 管理者または処理者に対し、それが適切であるときは、指定された方法により、指定された期間内に、とりわけ、第 16 条による個人データの訂正もしくは削除または処理の制限を命ずることによって、この指令により採択された法令を遵守して処理業務を遂行するように命ずること；
> (c) 禁止を含め、一時的または確定的な制限を加えること。
> 3. 各構成国は、監督官が、第 28 条に示す事前協議手続に従い、管理者に対して効果的な助言をする権限を有すること、また、監督官が、率先して、または、要請に応じて、構成国の自国の法律に従い、構成国の議会及び政府その他の機関及び組織並びに公衆に対し、個人データの保護の上での問題に関して、意見書を送付する権限を有することを法律によって定めなければならない。
> 4. 本条によって監督官に対して与えられた権限の行使は、欧州連合基本権憲章に従って欧州連合の法律及び構成国の法律に定められている効果的な司法救済及び適正手続を含め、適切な安全性確保措置に服するものとしなければならない。
> 5. 各構成国は、この指令によって採択された法令を執行するために、この指令に従って採択された法令の違反行為について、監督官が、法務当局に対して通告する権限を有すること、及び、それが適切なときは、訴訟を提起することまたは訴訟手続に関与する権限を有することを、法律によって定めなければならない。

警察指令第 47 条に定める権限の内容は、前述の一般個人データ保護規則第 58 条に定めるところとほぼ同じであるが、極めて強力なものである。特に、同条第 1 項の全ての個人データに対するアクセスの権限は重要である。データ主体は、監督

官を介して確認の結果の通知を得ることしかできないかもしれないが、監督官は、法執行機関（警察）等が処理している全ての個人データにアクセスしてその内容の正確性等を調査することができる。また、同条第2項の是正権限は、管理者である法執行機関（警察）や前科・前歴データを管理・保存する法務当局の行為や処理者の行為に対して優越的な公権力を行使することができるものとして制度設計されている(57)。

なお、第47条にいう「処理者（processor）」とは、個人データの管理者（controller）である法執行機関（警察）等からの指示または委託を受けて個人データの処理業務を遂行する者のことを意味する。例えば、法執行機関（警察）や法務当局から委託を受けて犯罪捜査関連のデータの処理や分析の業務を遂行するセキュリティ関連企業やデータベース企業等のことを指す(58)。また、第4項の欧州連合基本権憲章の

(57) 個人データ保護指令95/46/EC及び一般個人データ保護規則GDPRに定める第三国における個人データの保護の十分性の判定においても、当該第三国において、個人データ保護のための監督機関がこのような強力な権限を有しているか否かが考慮事項に入れられる可能性はある。しかしながら、例えば、行政機関個人情報保護法において最高の監督機関として位置付けられている総務大臣でさえ、法務大臣及び警視総監に対して、警察指令が定めるような禁止等の措置を講ずる権限を有していない。それは、総務省は、法務省所管の業務に対して干渉する権限を全く有していないからである。総務大臣が他の省に属する行政機関の業務について監督機関としての機能を営むことができないのは、そのような日本国の国家行政組織法上の事情による。

(58) 一般に、軍当局や諜報機関等においては、民間の関連企業と特別の契約を締結し、業務処理の一部を委託したり、あるいは、民間企業から派遣を受けた従業者を諜報機関等の業務の遂行に従事させたりしていることが多い。そのような契約企業や個別の契約に基づく従業者のことを、一般に、「contractor」と呼んでいる。アメリカ合衆国のNSA（National Security Agency）内において、契約による従業者Edward Snowdenによって内部機密情報の大規模漏洩事件があったことは周知のとおりである。漏洩したデータの中には、大量の個人データが含まれている。この事件がアメリカ合衆国の諜報機関ではなく、欧州連合内の構成国の警察組織または諜報機関において発生したと仮定した場合、システムの構築及び運用の際のENISA及び個人データ保護監督官の関与によってそのような情報漏洩事故を防止することができたか否かという点が問題となり得る。しかし、日本国においては、警察や諜報機関の分野及び情報セキュリティの分野と関連するEUの法制に精通する法学研究者が皆無に近いために、そもそもこの分野における法制の解釈論ができないという問題があり、その結果として、学術的に意味のある研究成果もまた皆無という状態となっている。一般に、一定の傾向性のある研究者や団体等からの批判や非難を避けるため、法学研究者がそのような分野での学術上の調査・研究に従事することを回避しようとする傾向があることもまた否定することのできない事実である。しかしながら、耳あたりの良い事柄だけを研究するのであれば、素人でもできる。プロの研究者は、困難を回避してはならない。

条項とは、第 47 条の効果的な救済及び公正な裁判を受ける権利のことを指す(59)。

他方、警察指令が定める法執行機関（警察）の犯罪捜査や法務当局の前科・前歴データの保存と関連する監督官の職務の中には、刑事訴訟手続における弁護人の弁護活動上の行為と関連するものが多々含まれているものの、監督官の権限及び活動と刑事訴訟手続上の弁護人の職務及び活動との相互関係については、やや曖昧な部分が残る(60)。

しかしながら、警察指令第 42 条第 1 項により、監督官は、「この指令に従ってその職務を遂行し、その権限を行使するについて完全に独立して行動する」ものと定められており、監督官の活動と刑事訴訟における弁護人の活動とが相反する利害状況を発生させることがあるとしても、その刑事訴訟における弁護人の活動によって監督官の権限行使が妨げられることはあり得ない。その意味で、監督官は、弁護士が有する訴訟法上の権利よりも優越する権限を有する公権力主体の一種である(61)。

3．3　テロ対策

3．3．1　データ保持指令 2006/24/EC における職務

公衆が利用可能な通信サービスまたは公共通信ネットワークの提供と関係して生成または処理されるデータの保持並びに指令 2002/58/EC の改正に関する欧州議会及

(59) 最新の改正を踏まえた現行の欧州連合基本権憲章の全文訳は、夏井高人「欧州連合基本権憲章（2012/C 326/02）[参考訳]」法と情報雑誌 1 巻 2 号 1～33 頁にある。

(60) 日本国においては、従来、個人データ保護のための監督官制度それ自体が存在していなかったためほとんど注目されることのなかった検討課題の 1 つであるが、EU においても研究が始まったばかりであり、十分な検討がなされているとは認め難い。しかし、刑事訴訟手続と個人データの保護のための監督官の関与とで利害が相反するような場合を含め、今後、十分な研究を尽くし、それぞれの職務が適正かつ円滑に遂行されるようにしなければならない。

(61) このことは、刑事訴訟における弁護人との関係において監督官が敵対的な立場にあるということを意味しない。例えば、被疑者または被告人がアクセスの権利を行使し、法執行機関（警察）に対して確認を求める場合、当該被疑者または被告人の弁護人は、被疑者または被告人の代理人として、監督官を介して、必要な確認を求めることができる。ただし、日本国の法制においては、このような確認手続を支持するための刑事訴訟法上の根拠条項はない。しかし、弁護士法第 23 条の 2 第 1 項は、「弁護士は、受任している事件について、所属弁護士会に対し、公務所又は公私の団体に照会して必要な事項の報告を求めることを申し出ることができる」と規定しているので、この規定を根拠とすることは可能であると解される。

び理事会の 2006 年 3 月 15 日の指令 2006/24/EC（Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC・以下「データ保持指令」という。）(62) の第 9 条第 1 項は、「構成国は、保持されたデータの安全性に関して第 7 条に従い構成国によって採択された法令のその領土内における適用を監視することについての職責を有する 1 または複数の行政機関を設置しなければならない。その行政機関は、指令 95/46/EC の第 28 条に示す監督官と同じ機関とすることができる」と規定し、同条第 2 項は、「第 1 項に示す機関は、同項に示す監視を行う際、完全に独立して行動する」と規定している。この条項では、個人データ保護指令 95/46/EC の監督官とは異なる監督機関が存在し得ることを前提にしているが、実際には、個人データ保護指令 95/46/EC の監督官と同一のものであると考えて差支えないと思われる。

データ保持指令の有効性については、様々な議論がなされてきた(63)。ドイツ連

(62) 全文訳は、夏井高人「公衆が利用可能な通信サービスまたは公共通信ネットワークの提供と関係して生成または処理されるデータの保持並びに指令 2002/58/EC の改正に関する欧州議会及び理事会の 2006 年 3 月 15 日の指令（Directive 2006/24/EC）[参考訳]」法と情報雑誌 1 巻 5 号 47～65 頁にある。

(63) 関連する文献として、石崎靖敏「セキュリティとプライバシのバランス―EU のデータ保持指令をめぐる議論―」信学技報 106 巻 175 号 51～58 頁 (2006)、David Wright & Reinhard Kreissl (Eds.), Surveillance in Europe, Routledge (2014)、David Barnard-Wills, Security, privacy and surveillance in European policy documents, International Data Privacy Law Volume 3 Issue 3 pp.170–180 (2013)、Lukas Feiler, The Legality of the Data Retention Directive in Light of the Fundamental Rights to Privacy and Data Protection, European Journal of Law and Technology, Vol.1 Issue 3 (2010)、Francesca Bignami, Privacy and Law Enforcement in the European Union: The Data Retention Directive, Chicago Journal of International Law vol.8 pp.233–255 (2007) 及び Jeremy Warner, The Right to Oblivion: Data Retention from Canada to Europe in Three Backward Steps, University of Ottawa Law & Technology Journal vol.2 No.1 pp.75–104 (2005) がある。個人データ保護指令 95/46/EC 第 29 条の作業部会による公式報告書としては、Article 29 Data Protection Working Party, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) (16/EN WP 237) 及び Article 29 Data Protection Working Party, Opinion 5/2002 on the

邦憲法裁判所など各国の裁判所で判断が示されていたが(64)、その後、2014 年 4 月 8 日、欧州司法裁判所の先決裁定（Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others）によって無効と判断された(65)。それゆえ、現時点では、同指令における監督官の職務について論じてみても実益がないかもしれないが、今後、同種の法令が再び制定されることはあり得ることであるので、指令それ自体が無効とされた点は一応措いて、同指令に定める監督官の職務について検討することとする。

データ保持指令第 7 条は、同指令に基づいて保持されるトラフィックデータ等について、以下のような安全性確保措置（safeguards）を求めており、監督官は、その安全性確保措置の実施状況が適正であるか否かについて監督権限を有する。

> 指令 95/46/EC 及び指令 2002/58/EC に従って採択された法令を妨げることなく、構成国は、公衆が利用可能な電子通信サービスの提供者及び公共通信ネットワークの提供者が、ミニマムのものとして、この指令に従って保持されるデータに関する以下のデータ防護原則を尊重することを確保しなければならない：
>
> (a) 保持されるデータは、当該データがネットワーク上にある場合と同程度の品質を有するデータであり、かつ、それと同程度の防護及び安全性に従うものとしなければならず；
>
> (b) データは、事故による破壊もしくは違法な破壊、事故による喪失もしくは改変、無権限のもしくは違法な記録保存、処理、アクセスまたは開示に対してデータを防護するための適切な技術上及び組織上の措置を講じられるものとしなければならず；
>
> (c) データは、特に承認された者のみによってアクセスされ得ることを確保するための

Statement of the European Data Protection Commissioners at the International Conference in Cardiff (9–11 September 2002) on mandatory systematic retention of telecommunication traffic data (11818/02/EN/Final WP 64) が公開されている。

(64) 前掲 Computers, Privacy and Data Protection: an Element of Choice pp.3–23 参照。なお、この関連では、Serge Gutwirth, Ronald Leenes & Paul de Hert (Eds.), 及び Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection, Springer (2016) pp.411–463 が参考になる。

(65) 丸橋透「EU データ保持指令と無効判決の検討」情報ネットワーク法学会第 16 回研究大会予稿、今岡直子「イギリスにおけるデータ保全及び調査権限法の制定―EU データ保全指令の無効裁定を踏まえて」外国の立法 264 号 3～12 頁、Franziska Boehm & Mark D. Cole, Data Retention after the Judgement of the Court of Justice of the European Union, The Greens/EFA Group in the European Parliament (2014)、Chris Jones & Ben Hayes, The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy, 及び SECILE – Securing Europe through Counter-Terrorism – Impact, Legitimacy & Effectiveness (2013) が参考になる。

適切な技術上及び組織上の措置を講じられるものとしなければならず；かつ、
(d) アクセスされ保存されたデータを除き、データは、保持期間が終了した時点で破壊されなければならない。

データ保持指令に定めるトラフィックデータの保持（retention）は、サイバー犯罪条約 ETS No.185(66) に定めるトラフィックデータの一時的な保全（preservation）とは異なる制度である。

データの保持（retention）は、通信サービスのプロバイダが取扱う通信のトラフィックデータについて、通常の業務処理に必要な期間を経過後であっても、一定期間、包括的に保持し続けることを義務化した上で、必要に応じて、法執行機関（警察）、諜報機関、軍当局等が、プロバイダに対して、保持してあるトラフィックデータの提供（開示）を要求することができるというものである。これに対し、サイバー犯罪条約に定めるトラフィックデータの一時的な保全は、法執行機関（警察）が、特定の具体的な刑事事件について、犯罪捜査のために必要があるときは、特定の被疑事件に関係するトラフィックデータに限定して、一定期間、消去しないで保存しておくように要請することができるとした上で、その後に刑事訴訟法に定める差押令状に基づいて当該保存してあるトラフィックデータを差押えるというものである。したがって、この両者は、その法的性質を全く異にするものである(67)。

(66) サイバー犯罪条約に関する経済産業省サイバー刑事法研究会（座長・山口厚）による調査結果としては、経済産業省サイバー刑事法研究会報告書「欧州評議会サイバー犯罪条約と我が国の対応について」（2002年4月）がある。サイバー犯罪と関連する立法史に関しては、Stein Schjolberg, The History of Cybercrime 1976–2014, Cybercrime Research Institute GmbH (2014) が詳しい。サイバー犯罪に関する OECD における検討結果としては、OECD, Computer Related Crime: Analysis of Legal Policy (1986) が公表されている。現在ではサイバー犯罪（Cybercrime）として認識されている犯罪行為を含め、最も初期の時期においてコンピュータ犯罪（Computer crime）について検討した書籍としては、Donn B. Parker, Crime by Computer, Charles Scribner's Sons (1976) がある。その日本語訳は、ドン・B. パーカー（羽田三郎訳）『コンピュータ犯罪』（秀潤社、1977）として出版されている。日本国における初期のコンピュータ犯罪関連立法に関しては、米澤慶治編『刑法等一部改正法の解説』（立花書房、1988）が詳しい。

(67) サイバー犯罪条約の説明書（Explanatory Report）の第149項ないし第169項にデータの一時的な保全（preservation）とデータの保持（retention）の相違に関する詳細な説明がある。説明書の第151項は、「『データの保全』は、『データの保持』と区別されなければならない。一般的な言語においては類似する意味があるけれども、それらは、コンピュータの利用との関係では別の意味を有している。データを保全することとは、記録

以上を前提とした上で、データ保持指令の第 5 条第 1 項は、保持されるべきデータの類型について、詳細に定めている。なお、同条第 2 項は、「通信の内容を明らかにするデータは、この指令によって保持することができない」と規定しているので、以下に示される類型のデータは、データの内容を含まないものであることが前提となっている(68)。

データ保持指令は、監督官の関与について、第 9 条の規定を設けているが、前述のとおり、その内容は、監督官が関与するということだけを定めるもので、その関与の具体的な内容については何も定めていない。それゆえ、監督官が、トラフィックデータの保持命令や保持されたトラフィックデータの開示要求それ自体について直接に関与するわけではない。これらの命令や要求は、法執行機関（警察）、諜報機関または軍当局の専権として実施される。

しかし、そのような命令や要求を受けた情報システムのプロバイダは、当該命令や要求がデータ保持命令の定める範囲を超過するものであると判断した場合にお

保存された方式で既に存在しているデータについて、現在の品質または状態を変化または劣化させるかもしれないことがないように保護されている状態を維持することを意味する。データを保持することとは、現在生成されているデータを将来に向かって誰かが保有している状態を維持することを意味する 。データの保持は、現時点におけるデータの蓄積及び将来の時点に向けたその維持または保有を含意している。データの保持は、データの記録保存の過程である。他方で、データの保全は、記録保存されたデータを防護され安全な状態に維持する行為である」と説明している。

(68) データの内容を含まない場合であっても、単に通信経路の追跡を超えて、プロファイリング手法の応用により、一定の内容的評価や属性評価が可能であることは、当然の前提である。その意味では、「内容を示すデータ（コンテントデータ）でなければプライバシー侵害はない」と考えることは不可能である。ただ、トラフィックデータの保全・保持とコンテントデータの保全・保持とでは、直接的なプライバシー侵害の程度及び態様が異なることは現時点でも変わらない。

なお、プロファイリングやデータマッチングにより断片的なデータから一定の推論が可能であることによるプライバシー侵害の可能性については、様々な書籍や論説等において既に詳細に論じられている。この点について、比較的楽観的な見解を示すものとしては、Julia Lane, Victoria Stodden, Stefan Bender & Helen Nissenbaum (Eds.), Privacy, Big Data, and the Public Good: Frameworks for Engagement, Cambridge University Press (2014) がある。悲観的な見解を示すものとしては、Daniel J. Solove, The Digital Person: Technology And Privacy in the Information Age, New York University Press (2006)、Alexander Halavais, Search Engine Society, Polity (2008)、Simson Garfinkel, Database Nation: The Death of Privacy in the 21st Century, Oreilly (2001) 及び David Brin, The Transparent Society: Will Technology Force Us To Choose Between Privacy And Freedom?, Perseus Books (1998) がある。

いて、当該命令や要求に対して何らかの異議申立または不服申立をすることを認める構成国の法令が存在するときは、当該法令に基づいて異議申立をすることができるはずである(69)。第9条の規定は、そのような場面における監督官の関与を想定するものと考えられる。

ところが、監督官が異議の当否を判断する際には、形式的な要件該当性の有無のみで判断を形成することができない場合があり得る。例えば、国際的な大規模テロの脅威が持続しているような状況においては、そのような状況が存在していることを示す疎明資料が法執行機関（警察）や諜報機関等から与えられ、そのような疎明資料に基づいて監督官がその判断を形成することになるであろう。それゆえ、そのような場面においては、監督官は、たとえ直接的には国家のテロ対応活動に積極的に関与することにはならないとしても、総体的には、国家としてのテロ対応活動の一部を担っていることになる(70)。

なお、データ保持指令の前文第14項には、「電子通信と関連する技術は、急速に変化しており、職務権限を有する行政機関からの正当な要求が増加するかもしれない。助言を得るため、そして、これらの事項に関するベストプラクティスの経験の共有を奨励するために、欧州委員会は、構成国の法執行機関、電子通信産業の事業者団体、欧州議会の代表、及び、欧州データ保護監督官を含むデータ保護監督官で構成されるグループを設置する予定である」と書かれている。

3．3．2　搭乗者記録指令(EU) 2016/681における職務

テロ犯罪及び重大犯罪の防止、検知、捜査及び訴追のための搭乗者記録（PNR）の利用に関する欧州議会及び理事会の2016年4月27日の指令(EU) 2016/681（Directive (EU) 2016/681 of the European Parliament and of the Council

(69) 日本国の法制においては、刑事訴訟法に基づく命令については刑事訴訟法に規定する手続に従って不服を申し立てることができる。しかし、一般に、警察当局からの任意の協力要請があった場合については、形式的には行政処分が存在しないので、行政処分の存在を必須の前提とする行政不服審査の申立てや行政訴訟の提起等によって不服を申し立てることができない。そこでは、ある種の「ambivalent」な相互意識に依拠した奇妙な均衡関係が存在しているということができる。

(70) 日本国の個人情報保護委員会に関しては、そのような職務の存在が全く想定されていない。そもそも、個人情報保護委員会が警察庁所管の業務及び法務省の関係各局の業務に関与することそれ自体が想定されていない。

of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime・以下「搭乗者記録指令」という。）は、航空機や船舶等の搭乗者名の記録 PNR[71] に含まれる個人データの保護について定めている。

搭乗者記録指令は、テロ対策を目的として各構成国の法執行機関（警察）が搭乗者記録に含まれるデータや情報を共有する必要性を認めつつ、そのような共有のための構成国間及び構成国と第三国間での個人データの移転に伴う当該搭乗者（旅客）のプライバシーに対する脅威を排除し、搭乗者の記録 PNR と関連する個人データを保護するために、構成国の監督官の関与を定めている（第 6 条第 7 項、第 13 条第 5 項(c)、第 13 条第 6 項、同条第 8 項）[72]。

搭乗者記録指令第 15 条第 1 項は、構成国の監督官が PNR の個人データ処理に関する監督業務を遂行するために、警察枠組み決定 2008/977/JHA の第 25 条を適用するものと定め、また、同条第 2 項は、「構成国の監督官は、個人データの処理と関連する基本的な権利の保護という観点から、第 1 項に基づく活動をしなければならない」と定めている。そして、同条第 3 項及び第 4 項は、以下のとおりに定めている。

> 3. 各監督官は：
> (a) データ主体から申立てられた異議に対処し、事実関係を調査し、かつ、データ主体に対し、合理的な期間内に、その異議の進捗状況及び結果について通知しなければならず；
> (b) 率先して、または、(a) に示す異議に基づいて、自国の法律に従い、処理の適法性を検証し、調査、監督及び監査を実施しなければならない。
> 4. 各監督官は、要請に応じて、データ主体に対し、この指令により採択された法令に定める権利の行使について、助言をしなければならない。

4 日本法との比較検討

(71) 前掲 Computers, Privacy and Data Protection: an Element of Choice pp.171–199
(72) 日本国の国際空港における入手国管理に伴う個人情報の処理について、個人情報保護委員会が監督権限を行使することのできる根拠法令は存在しない。

4．1　個人データ保護指令 95/46/EC 及び一般個人データ保護規則 GDPR との相違

(1) 公的部門における独立の監督機関（監督官）の不存在

日本国の行政機関においては、総務大臣が個人データ処理に関する業務を統括すべき立場にある（行政機関個人情報保護法第 49 条及び第 50 条）。行政機関個人情報保護法第 49 条及び第 50 条に定める総務大臣の権限は、平成 28 年法律第 51 号の完全施行後には、改正後の第 51 条の 2 第 2 項、第 51 条の 4 ないし第 51 条の 7 により個人情報保護委員会の権限となる。しかし、この改正によっても、監督官は、行政機関による「行政機関非識別加工情報」の処理に関して一定の権限を行使し得るのみであり、それ以外の普通の個人データの処理に関しては個人情報保護委員会としての権限を行使することができない。そして、総務大臣に対して独立の監視権限を行使することのできる国家機関は存在しない。

総務大臣自身は、行政機関において処理される個人データの管理者（controller）及び処理者（processor）の統括責任者なのであって、監督者（supervisory authority）ではない。一般に、監督機関から監督を受けるべき管理者と監督権限を行使する独立の監督機関を同一の行政機関が兼ねることはできない(73)。

他方、日本国の個人番号法の第 21 条第 1 項は、「総務大臣は、委員会と協議して、情報提供ネットワークシステムを設置し、及び管理するものとする」と規定している（ただし、個人情報保護委員会には総務大臣に対する強制力をもった監督権限があるわけではない）。また、同法 28 条は業務開始前の影響評価及び事前協議（評価書の内容が不適切である場合の特定個人情報ファイルの取扱いの承認及び不承認）に関して定め、同法第 29 条の 3 は事後的な定期検査等を定め、第 29 条第 4 項は事故発生の場合の報告義務を定めている（ただし、これらの行為の違反行為があっても、その違反行為に対する罰則は定められていない）。このように、個人番号と関連する個人データの処理に関しては EU の個人データ保護法制と比較的類似する個人情報保護制度が導入されていると言える。

以上から、日本国の公的部門（行政機関・独立行政法人等）においては、実質的

(73) 同様に、総務大臣が策定する各種ガイドラインは、自己管理（self-regulation）のための行動指針とはなり得ても、独立の行政機関である監督機関（監督官）としての監督権限行使のための根拠となる法規範または行動指針とすることができない。

にみて、特定個人情報（個人番号）と関連する業務処理、前述の行政機関個人情報保護法に定める行政機関非識別加工情報と関連する業務処理等の例外的な場合を除き、普通の個人データの業務処理に関しては、個人データの保護に関する独立の監督機関（監督官）が存在しない。

(2) データ処理への監督官の事前の関与（個人データ影響評価、事前協議）

個人データ保護指令 95/46/EC に定める監督官の職務の中で、同指令第 18 条、第 19 条、第 21 条、第 28 条第 4 項については、日本国の法制は全く対応していない。一般個人データ保護規則中の同旨の内容を定める条項についても同じである。

前述の特定個人情報（個人番号）と関連する事項等の例外的な場合を除き、日本国の法制においては、個人情報（個人データ）の処理は、基本的に自由である。極めて特殊な場合を除いては、個人データの処理の開始前に適用される法的規制が基本的に存在しない。例えば、個人情報取扱事業者が業務処理を開始する時点において監督官庁に届け出る義務が存在しないので、事業者による個人データの処理について監督官庁が事前に点検をしたり協議したりする機会がない。その意味で、日本国の法制は、個人番号制度と関連する部分を除いては、EU の法制と全く異なるものであると言わざるを得ない(74)。

しかし、今後の日本国の個人情報保護法制の解釈・運用に際しては、「デフォルトは悪」という前提から出発し、安全性確保措置をデフォルトで具備することによって適法性根拠（legal basis）を獲得するという基本的枠組みを念頭に置く必要があると考えられる。このような発想の転換は、これまでの政策論とはかなり異なるものであるので、その浸透には相当の時間がかかるものと予想される。

そこで、当面は、JISQ 15001 等の工業規格によって定められている標準的な運用の仕組みに準拠している事業者であるか否かによって、その個人情報保護の適否を判定するという方法によらざるを得ない。

(74) 日本国の個人情報保護法制の立法史を調べてみると、旧行政管理庁（現在の総務省行政管理局）が権限を有し、海外の立法動向に関する情報を含め、個人データ保護法制と関連する情報を独占していた部分がかなり大きいということを理解することができる（前掲法と情報雑誌 1 巻 4 号に収録した個人データ保護条約の冒頭解説及び脚注（訳注）参照）。法解釈学及び法史学の分野に属する問題ではなく法社会学の分野に属する問題を多く含むかもしれないが、今後、この点に関する徹底した調査研究を尽くした上で、あるべき個人情報保護法制の立法体制に関する提言がなされるべきである。

(3) 標準的な行動準則等の認証

一般個人データ保護規則 GDPR の第 57 条の (n) 及び (o) に定める認証に関する業務は、日本国においては、従来、一般財団法人日本情報経済社会推進協会（JIPDEC）が所掌してきた。しかし、認証の中立的という観点を考えると、今後は、何らかの調整を要することになるのではないかと思われる(75)。

(4) データ主体（本人）からの異議申立て（苦情申立て）に対する対処

日本国の個人情報保護委員会に関しては、個人データの本人各自から直接に異議申立て（苦情の申立て）を受け、当該事案において必要があるときは一定の強制的な措置を含む権限の行使をするような制度的な仕組みが導入されていない。

行政機関による個人データの処理との関係では、一般的な行政不服審査の申立てまたは行政訴訟の提起によることとなる。民間部門における個人データとの関係では、個人情報保護法に定める各種の訴訟の提起及び関連する民事保全処分の申立てによることとなる。しかし、個人情報保護委員会が訴訟参加できるようにするための立法的手当はなされていない。

(5) データ主体（本人）に対する助言

EU の個人データ保護法制においては、構成国の監督官の重要な職務の 1 つとして、データ主体（本人）が個人データ保護上の権利を行使する際に適切に助言を行うという職務がある。しかし、現行法上、個人情報保護委員会がそのような相談業務に従事することは想定されていない。

一般に、日本国の弁護士会や法テラスにおいて行われている法律相談においては、一般的な教示をすることが可能である。しかしながら、単に誰かが一般的な教示をすれば良いというのではなく、個人データの保護について責任を有する専門機関である監督官が助言をするということが重要である。日本国の制度設計においては、そのような制度は導入されていない。

仮に個人情報保護委員会が法テラスや各地方自治体の担当者等に相談業務を委

(75) 仮に個人情報保護委員会から JIPDEC に対して事務の委任をすることによって対処しようとする場合、個人情報保護委員会と同様の独立性が確保されていることを要し、かつ、公平・中立的な立場で職務を遂行し、守秘義務を完全に履行できるような制度的な仕組みを構築する必要がある。そのためには、従来のような会員企業をとりまとめて日本国政府の政策を遂行するための組織から一般企業とは一線を画する監督官庁的または本来の意味での監査法人的な組織へと変貌を遂げる必要があるであろう。

嘱することができるとする法令を定めるとした場合、個人情報保護と関係する相談については個人情報保護法に精通した担当者が応対する必要がある。

それゆえ、そのような担当者を育成するために、大学教育または大学院教育において、EU の個人データ保護法制及び米国のプライバシー保護法制・判例を正確に踏まえた上で、個人情報保護法の分野において行政機関や企業内で専門家として活動することのできる者を養成するための制度上の仕組みを確立し、必要な予算措置を講ずることが必要である(76)。

それと同時に、個人情報保護の分野において高度な専門性を有する者であり、かつ、個人情報保護法及びプライバシーマーク制度（JIS Q 15001）についての実務経験が豊かである者であることを認証するための公的認証制度について、その精度及び信頼性を高めるための国家的な方策が講じられるべきである。

(6) 地方自治体における監督機関（監督官）の不存在

日本国においては、各地方自治体に監督官が設置されていない。それゆえ、各地方自治体の監督官の代表が委員となって個人情報保護委員会を構成するという制度的仕組みも存在しない。

この点については、国家連合である EU と日本国の地方自治制とを同列に扱うことはできない。しかし、例えば、ドイツ連邦においては、連邦全体を監督する監督官とは別に、州（ラント）や市の監督官も制度として存在しており、構成国の中

(76) EU の個人データ保護法制における個人データ保護責任者（data protection officer）が遂行すべき職務に相当する業務に従事する者の日本国における資格認定制度上の認定資格としては、公認情報セキュリティ主任監査人、公認情報セキュリティ監査人、情報セキュリティ監査人補、情報セキュリティ監査アソシエイト、公認情報システムセキュリティ専門家（CISSP）、公認情報システム監査人（CISA）、公認情報セキュリティマネジャー（CISM）、情報セキュリティアドミニストレータ、テクニカルエンジニア（情報セキュリティ）、情報セキュリティスペシャリスト、システム監査技術者、GIAC（Global Information Assurance Certification）、ISMS 審査員、公認内部監査人（CIA）等がある。しかし、これらは、法律関係の専門職ではない。法律関係の専門家である弁護士は、司法試験の受験科目を中心に勉強するが、個人情報保護法制について勉強をしていない場合が圧倒的に多い。大学法学部及び法科大学院においてサイバー法及び個人データ保護法制と関連する科目を設置しているところは非常に少ない。特に EU の個人データ保護法制について精通している法学部教授は稀有である。しかしながら、このように高等教育において必要な制度的仕組みが設けられていないという事実は、第三国へのデータ移転の際の十分性判定との関係においても極めて重要な判断要素の 1 つとなっていることに留意すべきである。

でも複数の監督官が階層構造をなして設置されていることがあるということを理解することができ、そのような観点からの考察をすることは可能である。

そして、日本国において、もしEUと類似する制度的仕組みを構築するのであれば、各都道府県に独立の地方行政機関として監督官を設置した上で、個人情報保護委員会がそれらの地方自治体の監督官を統括し、日本国の領土内において一元的で一貫性のある個人情報の保護を実現するという国家システムを構築することになるであろう。このような国家制度を構築する上では、労働基準法に規定する労働基準局及び労働基準監督署の仕組み、権限及び相互関係を参考にすることができる。ただし、現在の日本国の国情（特に財政状況及び立法能力）を前提とする限り、個人情報保護に関して、そのような法改正がなされる可能性は皆無である。

個人情報保護委員会の組織構成に関しては、国情の相違から、その前提を全て欠いていると言わざるを得ない。

(7) 対外的な共同活動及び相互支援

日本国は欧州連合の構成国ではないので、形式的には全く無関係であるが、仮に個人情報保護委員会が欧州連合の構成国または国際機関等から要請を受けた場合、個人情報保護委員会が事実上対応することは可能と思われる。ただし、個人情報保護委員会の対外関係と関係する明確な権限を定める法令は存在しない(77)。

(8) 罰則の適用

日本国法においては、是正の措置命令を発することなく違反行為があれば直ちに行政罰を適用することが可能である場合（いわゆる直罰規定の場合）が非常に少ないという点が異なっている。

一般に、行政機関による是正措置に服従しない行為に対する罰則は、公権力の発動としての是正措置の実効性を法的に担保するためのものであり（行政措置への不服従に対する制裁措置）、違反行為に対する直接的な制裁措置ではない。

この点について若干敷衍して考えてみると、EUの法制と日本国の法制における基本的な構造上の相違に基づくものであることを認識することができる。

(77) 欧州評議会のサイバー犯罪条約（ETS No.185）に基づく国際協力に関しては、法務省及び警察庁において関連各国において対応する行政機関等と密接に連絡をとりあう体制が既に構築されているが、個人データ保護との関係では、少なくとも公式には、そのような国家制度上の仕組みはない。

すなわち、EU の個人データ保護法制における個人データの処理に関する限り、何らの具体的な目的もなく、かつ、データ主体（本人）の同意などの法的根拠（legal basis）もなく(78)、個人データを処理する行為は、違法行為である（デフォルトは悪）。

これに対し、日本国の制度においては、個人情報の取得に際して、当該個人情報の本人に対して通知し拒否する機会を与える必要がなく、その時点では本人に対して目的を示す必要もなく、同意を得る必要もないことから、形式上、何ら積極的な適法要件がなくても、個人データを取得し、その個人データを取扱う行為が違法行為となるものではないと理解されている（性善説）。それゆえ、デフォルトにおいて違法ではないとされている行為に対する直罰があり得ないことは必然的な結果であると考えられる。

このような性善説の立場では、何か問題が生じた場合には、そのような問題が生じたときに、個別的に是正勧告を行い、その是正勧告に従わない事業者のみに対して罰則を適用すれば足りることになる。

以上の点に関しては更に時間をかけて綿密に検討することを要するものの、概略としては、法制の基本的骨格は、本質的に異なるものである。法制の骨格が異なる以上、非常に多くの場合において、個人データの保護のために個人情報保護委員会が関与できる前提を欠いていることになる。そのことが個人データの第三国移転における十分性の判定に非常に大きな影響を与え得ることは、誰の目にも明らかである(79)。

(78) 個人データの取得などの行為それ自体が自己目的となっている場合には、特定の具体的な目的に基づく取得（処理）として扱うことができない。また、他に移転することのみを目的とする取得も認められない（移転という処理について具体的な処理目的を要する。）。それゆえ、個人データの収集それ自体が自己目的となっている場合（例：趣味としての収集）や他に移転することのみが目的となっている場合（例：名簿業）は、データ主体（本人）の同意があるなどの場合を除き、少なくとも EU の法制下においては適法行為ではない。

(79) 一般個人データ保護規則 GDPR の第 83 条第 7 項は、「第 58 条第 2 項による監督官の是正権限を妨げることなく、各構成国は、当該構成国内に設けられている行政機関及び行政組織に対して行政罰を科すかどうか及びその範囲に関する法令を定めることができる」と規定している。すなわち、監督官は、行政機関に対して是正措置を命ずる権限は有するものとしなければならないけれども、行政機関に対して罰則を科す権限を認めるか否かについては構成国の立法裁量に任せるという趣旨である。日本国の行政機関個人情報保護法及び独立行政法人等個人情報保護法においては、行政機関及び独立行政法人等に対して個人情報保護委員会が罰則を科すことのできる権限は定められていない。この罰

4．2　NIS 指令 (EU) 2016/1148 との相違

日本国のサイバーセキュリティ基本法（平成 26 年法律第 104 号）の第 16 条は、「国は、関係府省相互間の連携の強化を図るとともに、国、地方公共団体、重要社会基盤事業者、サイバー関連事業者等の多様な主体が相互に連携してサイバーセキュリティに関する施策に取り組むことができるよう必要な施策を講ずるものとする」と定めている。

抽象的には、ここに規定する「多様な主体」の中に個人情報保護委員会が含まれると解することのできる余地はある。

しかしながら、同法の立法の趣旨からすると、情報セキュリティの確保によって守ろうとする保護法益が明確ではなく、第 1 条に「インターネットその他の高度情報通信ネットワークの整備及び情報通信技術の活用の進展に伴って世界的規模で生じているサイバーセキュリティに対する脅威の深刻化その他の内外の諸情勢の変化に伴い、情報の自由な流通を確保しつつ、サイバーセキュリティの確保を図ることが喫緊の課題となっている状況に鑑み、我が国のサイバーセキュリティに関する施策に関し、基本理念を定め、国及び地方公共団体の責務等を明らかにし、並びにサイバーセキュリティ戦略の策定その他サイバーセキュリティに関する施策の基本となる事項を定める」とあることからすると、情報セキュリティの確保それ自体を自己目的とする再帰的な構造の法律だと理解することができる。換言すると、手段であるはずの情報セキュリティの確保によって守ろうとする保護法益が存在しない法令であるとも考えられる。その結果、個人データ保護法制の保護法益であるプライバシーの利益が保護法益として特に明確に意識されているとは考えられない。

また、NIS 指令は、その指令案(80) の段階では日本国のサイバーセキュリティ基本法と類似する部分を少なからず有するものであったが、その後の審議過程の中でその構造を大きく変化させたものとなっており、可決された NIS 指令と日本国の

則に関する限り、関係各国の立法裁量に任されている以上、個人データの第三国移転における保護の十分性の判定における判断材料とされることもないと考えることができる。

(80) NIS 指令の草案の全文訳は、夏井高人「欧州連合内においてネットワーク及び情報システムのセキュリティに関する高度で共通の水準を確保するための措置に関する指令案（ネットワーク情報セキュリティ指令案：NIS 指令案）[参考訳]」法と情報雑誌 1 巻 1 号 1～50 頁にある。

サイバーセキュリティ基本法との類似性はかなり希薄化したものとなっている。

他方で、個人情報保護委員会の職務権限として、情報セキュリティの確保との関係において他の行政機関等と協力することを定める法令は存在しない。

従って、サイバーセキュリティ基本法との関係において個人情報保護委員会が関与する余地はない。

5　まとめ

以上で本稿における検討を終える。

EU の構成国における監督官（supervisory authority）は、1980 年代にはあまり意識されていなかったけれども、1995 年の個人データ保護指令 95/46/EC が制定されて以来、欧州評議会の個人データ保護条約の一部改正（追加議定書の締結）を含め、関連する個人データ保護法制の中において基軸的な制度的仕組みとして構築され、法改正が重ねられるにつれ、その権限が次第に強化されてきた。それと同時に、犯罪捜査、国防、情報セキュリティと関連する国家的機能と関係をもつ機会が増えることともなった。現時点における監督官は、単純な人権擁護組織等ではなく、国家制度上、非常に重要な機密情報に接する可能性がある特殊な独立行政機関として成長を続けている。

これを日本国の法制と比較してみた場合、個人情報保護法の平成 27 年（2015 年）改正により個人情報保護委員会が設置されるまでの間の期間においては、個人情報保護のための職務権限を有する独立の行政機関である監督機関は存在しなかった。同法の改正等によって設置された個人情報保護委員会の権限をみると、民間部門においてさえ、その権限はかなり限定的なものである。それは、個人情報保護委員会に関する条項の立法に問題があるのではなく、そもそも個人情報保護法制の基本的な構造に問題があると言える。とりわけ、個人データの処理（取扱い）に関して、原則を違法行為とせず、特に条件を付さなくても適法行為として扱っている点は、致命的な立法上の欠陥である。

他方において、公的部門（行政機関及び独立行政委員会等）に関しては、現時点においても独立の行政機関としての監督機関は存在しておらず、個人情報保護委員

会が関与することのできる事項は、特定個人情報（個人番号）と関連する業務処理など、極めて限定されたものとなっている。

以上の点を踏まえただけでも、EU の個人データ保護指令 95/46/EC 及び一般個人データ保護規則 GDPR が求める個人データの第三国移転における法的保護の十分性を認めることができず、その十分性の判定を得ることは不可能である。日本国の行政機関及び日本国の企業としては、十分性の判定によるのではなく、同指令及び同規則に定める特例に基づく例外的処理によって事態を乗り切る以外に方法はない(81)。

以上のとおり、本稿では、EU における個人データ保護のための監督官制度における本来的な職務及びそれとは別の特殊な職務についての検討を行い、日本国の法制度との比較検討結果を示した。

論じ足りない部分があるが、別稿において更に論ずることとしたい(82)。また、本稿を執筆するに際して、EU の警察指令(EU) 2016/680、データ保持指令 2006/24/EC、搭乗者記録指令(EU) 2016/681 と日本国の法制との相違に関しても調査・検討を行ったが、字数制限の関係で、その検討結果を本稿の中に盛り込むことができなかった。他日を期することとしたい。

以上(83)

（明治大学法学部教授）

(81) さしあたっては、東京オリンピック（2020 年）に参加するための各国の選手団及び一般旅行客並びに開催準備のための渡航者等の搭乗者記録 PNR として処理される個人データのやりとり（飛行機のチケット予約や宿泊施設の予約を含む。）について、個人情報保護委員会が監督権限（行動準則の策定権限、報告徴収権限、立入調査権限、是正勧告権限、罰則の適用権限）を行使できるように立法的手当をした上で、個人データの第三国移転における法的保護の十分性の判定によるのではなく、特例に基づく個別的対処を真剣に検討する必要がある。

(82) 関連する様々な法律上の問題について、前掲法と情報雑誌 1 巻 3 号に収録した一般個人データ保護規則 GDPR 全文訳（参考訳）の脚注（訳注）の中で私見を示した。

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