資料２

個人情報保護制度に関する主な国際的動向

Ⅰ　ＯＥＣＤ（加盟国 34（日本含む））

○　1980 年「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」決定
（Recommendation of the Council concerning Guidelines governing the protection of Privacy and Transborder Flows of Personal Data 23 September 1980）

○　以下に示す、いわゆるＯＥＣＤ８原則を主な内容とするもの。
勧告には、加盟国に対する拘束力はないが、各国においては、この８原則を踏まえた法的措置等がとられており、いわば事実上の国際標準となっている。

ＯＥＣＤ８原則	
①　収集制限の原則	⑤　安全保護措置の原則
②　データ内容の原則	⑥　公開の原則
③　目的明確化の原則	⑦　個人参加の原則
④　利用制限の原則	⑧　責任の原則

○　我が国においては、まず行政機関が保有する個人情報に関し、８原則に即した保護の在り方が検討され、1988 年「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律」制定

・　民間部門に関しては、当初、ガイドラインに基づき対応
（基本的なガイドラインに加えて、各事業分野別に策定）
・　2003 年に、「個人情報保護法」制定（民間部門を対象とした法整備）
その際、行政機関法も改正（現在の「行政機関の保有する個人情報の保護に関する法律」。また、「独立行政法人等の保有する個人情報の保護に関する法律」も制定）
・　地方自治体においては、条例に基づき対応

○　その後、ＯＥＣＤ理事会において、以下の勧告が採択

・　2007 年「プライバシーを保護する法の施行における越境協力に関する理事会勧告」
・　2013 年　プライバシーガイドラインの改正
（当初のガイドライン策定から 30 周年を期に見直しを行ったもの）

いずれも、上記８原則に変更を加えるものではない。
（2013 年の改正は、全面的な改訂の形をとっているが、1980 年の内容の基本を維持しつつ、追加すべき点を加えているもの）
2013 年ガイドラインにおける新たな内容（追加事項）として、国における実施（national implementation）に関し、プライバシー執行機関について、以下のとおり記述されている。

19. ガイドラインを履行するにあたり、加盟国は以下の事項を実施すべきである。
（c）プライバシー執行機関（複数形）を設立して維持し、当該機関の権限を効果的に行使し、客観的かつ公正で一貫した基準に基づく決定を行うために必要な管理組織、リソース、技術的専門知識を備え、
19. In implementing these Guidelines, Member countries should:
c) establish and maintain privacy enforcement authorities with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis;

これに関する解説が、補足説明覚書（Supplementary explanatory memorandum）に記されている（2007 年勧告にも関連）。
＜当該部分の抜粋は参考１＞
プライバシー執行機関に関して、国によっては「管理組織、リソース、技術的専門知識」を単一の組織（in a single entity）に統合することができない場合があり、それらの組織を全体として執行制度を備えているものとして認めることができるとしている。

なお、本項の検討の過程において、以下のような議論があったとされている。

本項の検討の過程においては、単独（Independent）[1]の機関が必要であるとの意見がＥＵから示されていた。一方、米国からは、単独の機関を設置することが困難であるとの見解が表明された。その理由として、合衆国憲法第２条第３節において、「大統領は法律が忠実に執行されるよう配慮し、合衆国のすべての官吏の任命を発令する」と定められており、大統領は連邦政府の行政府を統轄する立場にあることがあげられる。大統領は、連邦行政機関を管理する広範な権限を有し、規則、規制、大統領命令を発することができ、行政府のすべての省庁の長官および幹部の任命権限も有する。それゆえに、大統領の権限を監視監督する機関を設置することは、憲法上認められていないといった考えがある。また、諜報活動を行っている行政機関をはじめとして、それらの機関とは別個の単独の機関による監視が適当ではないまたは実質的に監視をすることが困難な行政組織の問題もある。
なお、わが国も、個人情報保護法の執行は、個人情報の取扱業務を所管する各省の主務大臣が執行する形態をとっている。そのため、単独の機関が統一的な執行機関として個人情報保護法の執行にあたる形態とはなっていない。よって、米国と同様に、単独の執行機関という要件はわが国の現行法制度においても適合するものではない。
以上の理由から、米国の意見表明にわが国も同調し、「単独の機関」という文言は削除された。

（慶応義塾大学　新保史生教授「第３章 ＯＥＣＤプライバシーガイドライン改正の詳解」より抜粋。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

1：全体の文脈が明らかではないが、Independent にはむしろ独立という意味合いが強いとも考えられる。

未来』（2014 年、JIPDEC））

○　ＯＥＣＤガイドラインにおける個人情報の定義と対象範囲について、

・　ＯＥＣＤガイドラインにおける定義は以下のとおりとなっている。

1. 本ガイドラインにおいて、
（b）「個人データ」とは、識別された又は識別されうる個人（データ主体）に関するすべての情報を意味する。
1. For the purposes of these Guidelines:
b) “Personal data” means any information relating to an identified or identifiable individual (data subject).

・　対象は公的部門、民間部門双方となっている。

Ⅱ　ＥＵ

１．1995 年ＥＵデータ保護指令

（「個人データの取扱いに係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令」
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）

○　加盟国における個人データの取扱い等に関する共通的な法制度を求めるもの。
ただし、標記の“ＥＵデータ保護指令”は加盟国を直接拘束するものではなく、加盟国は一定の裁量権の下に国内法として整備することとなるという性格のもの。
（なお、現在加盟国内で直接適用されることとなるＥＵ規則案の策定を調整中（後述））

○　プライバシー保護等の観点から、個人データの取扱い（民間部門、公的部門の双方が対象として考えられる）について定めるとともに、第三国（域外国）への個人データの移動に関し、第三国が十分なレベルの保護を確保している場合に限る（only if, the third country in question ensures an adequate level of protection.）と規定している。（“十分性”の確保）

○　この“十分性”の問題は、基本法に関するこれまでの議論でも取り上げられてきたところであり、これに関するＥＵデータ保護指令の主な内容等は以下のとおりとなっている。
（現在、ＥＵの“十分性”の認定を受けているのは 11 カ国・地域[2]。日本は含まれていない（未申請））

・　指令第 25 条第１項において、「加盟国は、（中略）個人データの第三国への移動は、

[2] 欧州委員会に十分性を認定された国・地域は、スイス、カナダ、アルゼンチン、ガーンジー島、マン島、ジャージー島、フェロー諸島、アンドラ、イスラエル、ウルグアイ、ニュージーランド

当該第三国が十分なレベルの保護を提供している場合に限られる」ことを規定（先述のとおり）。

・　同条第２項において、「第三国における保護レベルの十分性は、一連のデータの移転作業を取り巻く全ての環境に照らして査定されるものとする」と規定。

（The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations）＜第 25 条の全文は参考２＞

○　また、これに関しては、作業文書（Working Document）が策定され（1998 年）、十分性が何を意味し、個々の場合にどのように判断されるべきかの枠組みの概要が示されている。

作業文書は、十分な保護を構成する要素として、

（ｉ）内容原則（Content Principles）

（ii）手続上・実務上のメカニズム（Procedural/ Enforcement Mechanisms）

を挙げている。

○　内容原則には次の諸原則が含まれる。

１）目的制限の原則

２）データの質と相応性の原則

３）透明性の原則

４）セキュリティの原則

５）アクセス、訂正、および異議を唱える権利

６）二次移転の制限　等

○　手続・実務上のメカニズムに関しては、

・　総論的部分において、第三国において適用されるデータ保護規則の内容のみならず、当該規則の有効性を確保するために整備される制度についても検討する必要があるとし、欧州でのこれまでの（各国の立法の）傾向の一つとして、例えば、監視や苦情調査の機能を持つ監督機関（複数形）の設立（such as the establishment of supervisory authorities with monitoring and complaint investigation functions）をあげるとともに、

・　手続上・実務上のメカニズムの項目において、欧州では、独立した権限機関の形での「外部監督」制度が、データ保護コンプライアンスシステムの必要な機能であることも広く合意[3]されている（There is also broad agreement that a system of 'external supervision' in the form of an independent authority is a necessary feature of a data protection compliance system.）ことなどを記述し、データ保護の十分性を評価する基盤を設けるために、データ保護手続きシステムの根本的な目

[3] broad agreement（仏：on s'accorde largement）：大筋合意

的を明らかにする必要があるとしている。＜作業文書第１章：保護が十分かどうかの評価の原文は参考３＞

・　“十分性”に関するこれらいずれの記述においても、監督機関の在り方に関しては、欧州各国の状況が基本認識として述べられているものであり、十分性の評価に当たっての具体的な基準等として示されているものではない。

・　なお、現行指令第 28 条において、域内国における監督機関の在り方に関して規定されている。具体的には、第１項において以下のとおり規定されている。

第 28 条　　監督機関 Article 28　Supervisory authority 1.各加盟国は、１つ又は複数の公的機関が、本指令に従って加盟国が採択した規則の国家領域内での適用を監督することに責任を有することを規定するものとする。 このような機関は付託された職務を、完全に独立して遂行するものとする。 1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive. These authorities shall act with complete independence in exercising the functions entrusted to them.

○　また、現行指令第 26 条（免除（Derogations））は、十分性が確保されていない第三国へ個人データを移転する際の条件を規定している。
（十分な（個人データ保護の）保証を与える標準的な契約条項として欧州委員会が決定する契約によってデータを移転する場合など。日本の事業者が欧州からのデータ移転を行う場合、多くはこれによっている。）

２．2012 年ＥＵデータ保護規則提案
（「個人データの取扱いに係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の規則」提案
Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Inofficial Consolidated Version 22 October 2013))

○　現在、提案段階にあるもの（各国と内容等について協議中）。
（決定されれば、これ自体が域内各国で国内法としての効果を持つものとなる。）
今後の調整状況を注視する必要。

○　第三国のデータ移転に際しての”十分性”に関しては、第 40 条、第 41 条に規定。監

督機関に関しては、第 41 条第２項に規定。

第 41 条 十分性認定のある移転

Article 41　Transfers with an adequacy decision

2.　保護水準の十分性の評価を行うとき、欧州委員会は以下の要素を考慮に入れるものする。

2. When assessing the adequacy of the level of protection, the Commission shall give consideration to the following elements:

(a)　（略）

(b) データ主体によるその権利行使を支援し助言を行うために、並びに連合及び加盟国の監督機関と協力するために、対象となる第三国又は国際機関において、データ保護ルールの順守確保につき十分な制裁権限も含めた責任を負う独立監督機関が 1 つ以上存在し、かつ効果的に機能していること。

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or international organisation in question responsible for ensuring compliance with the data protection rules, including sufficient sanctioning powers, for assisting and advising the data subjects in exercising their rights and for co-operation with the supervisory authorities of the Union and of Member States;

(c)　（略）

3～8　（略）

３．ＥＵの十分性に関する補足等

（１）現在の日本の状況に関して

・　日本の（個人情報保護に関する）体制に関しては、権限が分散し、公的機関の監視や個人の権利利益の保護が不十分であるとＥＵから指摘されている、との見解が日本国内の文献等で示されている（例：小林慎太郎『パーソナルデータの教科書』p.115（2014 年、BP 社）[4]）。ただし、これまで公的部門の執行体制が不十分であるとの正式な見解が示されたことは無い。

---

[4] この見解については、正式な文書に記されたものはなく、根拠としては、2009 年４月 23 日、ブリュッセルで開催されたデータ保護会議の際の欧州委員会司法自由安全総局(European Commission Directorate-General-Justice,Freedom)データ保護課(Unit D5-Data Protection)ペチャコバ事務官（ＥＵ事務局 Desk Officer（当時））のプレゼンテーションの中の、

・日本は、個人の私生活にかかわる個人データ及び基本権に関して十分なレベルの保護を提供している国であるとは、ＥＵによってまだ考えられていない。

・十分性認定手続を開始するためには、日本の代表部によってなされる公式の要請が欧州委員会に提出されなければならない。

等の部分が考えられる。（上記は、2011 年３月経済産業省委託調査（野村総合研究所実施）の中に示されている。（関連部分抜粋は参考４））

これに関しては、参考で示したペチャコバ事務官の見解の全体を見る限り、同事務官の十分な保護を提供している国としてＥＵによってまだ考えられていないとの見解は、具体的な根拠を示しておらず、単にその段階において日本が十分性認定を受けていない（日本として公式要請はしておらず、ＥＵ側として認定を開始するために詳細な分析を行うことを考えているとの趣旨が述べられている）という程度の意味あいと捉えられる。なお、同委託調査においては、日本の国内事業者を対象とした当時のヒアリング結果として、ＥＵのデータ保護指令に至急対応しなければならないという声はあまり見られず、過剰な規制は望ましくないという意見が多く寄せられた、としている。

（２）ＥＵデータ指令における個人情報の定義について

・　ＥＵデータ指令第２条において

> (a)「個人データ」とは、識別された、又は識別され得る自然人（データの対象者）に関する全ての情報を意味するものとする。識別され得る自然人とは、特に識別番号又は身体的、生理的、精神的、経済的、文化的、並びに社会的アイデンティティーに特有な一つ又は複数の要素を参照することによって、直接的又は間接的に識別され得る者をいう。
>
> (a) 'personal data ' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified , directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological , mental , economic, cultural or social identity;

と定義されている。

・　このように、ＥＵでは、保護対象となる個人情報は広く捉えられている。（これに関して、小林慎太郎『パーソナルデータの教科書』p. 112 において、ＥＵでは、「パーソナルデータは基本的にすべて保護の対象となる。また、パーソナルデータの収集・利用に当たっては、「オプトイン」方式で明示的に本人の同意を取得することを求めている。」と記載されている。）

・　我が国において、“個人特定性低減データ”を本人の同意なく利活用する仕組みを導入する場合、一方でＥＵにおけるパーソナルデータに関する保護の考え方との整合性をどう考えるか、内容原則に係る“十分性”の認定のための必要な条件を満たすのか、という点に留意する必要があるのではないか。

Supplementary explanatory memorandum to the revised recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data (2013)
プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告改正の補足説明覚書（2013）

Privacy enforcement authorities
プライバシー執行機関

Neither the 1980 Guidelines nor the 2007 Recommendation explicitly call for the establishment of privacy enforcement authorities, although the latter instrument assumes their existence and recommends their endowment with effective powers and authority. The revised Guidelines define and make explicit the need to establish and maintain "privacy enforcement authorities".（略）
1980 年ガイドラインと 2007 年勧告は、どちらもプライバシー執行機関の設置を明示的には要求していない。しかし、2007 年勧告は、プライバシー執行機関の存在を想定しており、プライバシー執行機関の効果的な執行及び監督権限を具備することについて勧告している。改正されたガイドラインは「プライバシー執行機関」を定義し、その設置と維持の必要性を明確にしている。（略）

The definitions of "laws protecting privacy" and "privacy enforcement authorities" allow for flexibility in application.（中略）a "privacy enforcement authority" refers not only to those public sector entities whose primary mission is the enforcement of national privacy laws, but may for example also extend to regulators with a consumer protection mission, provided they have the powers to conduct investigations or bring proceedings in the context of enforcing "laws protecting privacy".
「プライバシーを保護する法」と「プライバシー執行機関」の定義は、柔軟に適用することができるものである。（中略）「プライバシー執行機関」は、主要任務が国内のプライバシー法の執行を担う公的分野のプライバシー執行機関のみならず、たとえば、消費者保護を所掌事務とする規制機関が「プライバシー保護法」の執行にも関連する調査を実施したり訴訟を提起する権限を有している場合も含む。

A new provision in Part Five ("National Implementation") calls on Member countries to establish and maintain privacy enforcement authorities with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an "objective, impartial and consistent basis" [paragraph 19(c)]. This formulation has been adapted from the 2012 OECD Recommendation on Regulatory Policy and Governance (OECD, 2012a). In the context of the Guidelines, it refers to the need for privacy enforcement authorities to be free from instructions, bias or conflicts of interest when enforcing laws protecting privacy. There exist a variety of mechanisms across Member countries for ensuring the necessary impartiality

of privacy enforcement authorities in the exercise of their privacy protection functions. Paragraph 19(c) focuses on the practical impact of such mechanisms, which should ensure that these authorities can take decisions free from influences that could compromise their professional judgment, objectivity or integrity.

第 5 部（「国内実施」）に新たに定められた項目は、プライバシー執行機関を設置し維持することを加盟国に求めており、当該機関は、「客観的かつ公正で一貫した基準」に基づく決定を行うために必要な管理組織、リソース及び技術的専門知識を備え、執行権限を効果的に行使することが求められる。ここで示されている体系は、2012 年の規制政策及びガバナンスに関する理事会勧告（OECD,2012a）に基づくものである。ガイドラインの文脈では、プライバシー執行機関がプライバシーを保護する法を執行する際に、命令、偏向、又は利害衝突から独立していることが必要である。各加盟国には、プライバシー執行機関がプライバシー保護のための執行権限を行使する際に必要な公平性を確保するためのさまざまな仕組みが存在する。第 19 項（c）は、プライバシー執行機関が職務上の判断、客観性又は誠実性を損なうおそれがある影響を受けずに決定できることを保証する仕組みに係る実質的な効果に焦点を当てている。

In some countries, the term “privacy enforcement authority” can also refer to a group of bodies that collectively enforce laws protecting privacy. For example, oversight of public sector data controllers may involve multiple bodies from different branches of government, who may also have the authority to issues guidelines or other data usage requirements. The “governance, resources, and technical expertise” called for in paragraph 19(c) may not, in such a case, be embodied in a single entity, but rather be found in the enforcement system as a whole.

一部の国では、用語「プライバシー執行機関」は、プライバシーを保護する法を共同で執行する機関のグループを指すこともある。たとえば、公共分野のデータ管理者の監督は、政府の異なる部門に属する複数の機関に関係することがあり、当該機関は、ガイドラインの策定や他のデータ利用要件を課す権限を有することがある。そのような場合、第 19 項（c）で要求されている「管理組織、リソース、技術的専門知識」を単一の組織に統合することはできないが、それらの機関全体として執行制度を備えているものとして認めることができる。

The 2007 Recommendation underlined the need for privacy enforcement authorities to be endowed with the resources and authority necessary to (a) deter and sanction violations of laws protecting privacy; (b) permit effective investigations, including the ability to obtain access to relevant information, relating to possible violations of laws protecting privacy; and (c) permit corrective action to be taken against data controllers engaged in violations of laws protecting privacy. The resources of privacy enforcement authorities should be commensurate with the scale and complexity of data processing operations subject to their oversight. The new provision also calls for empowering privacy enforcement authorities with sufficient technical expertise, which has become crucial in light of the increasing complexity of data uses. This reinforces the emerging trend within privacy enforcement authorities to retain staff with a technical background.

2007 年勧告は、プライバシー執行機関が（a）プライバシーを保護する法の違反に対して防止策と制裁措置を講じ、(b）プライバシーを保護する法の違反の可能性に関して、それに関連する情報にアクセスする能力を含む有効な調査を許可し、(c）プライバシーを保護する法の違反に関与したデータ管理者に対して是正措置を講じることを許可するために必要なリソースと権限を与える必要性があると示している。プライバシー執行機関のリソースは、監査対象となるデータ処理作業の規模と複雑さに比例すべきである。この新しい項目は、プライバシー執行機関が十分な技術的専門知識を有することによって権限を強化することも要求している。こうした知識は、データの利用が一層複雑化する中で非常に重要なものとなっている。これは、プライバシー執行機関が技術的な基礎知識を備えたスタッフを維持する近時の動向を明確に指示するものである。

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

ＥＵデータ保護指令（「個人データの取扱いに係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令」）

Article 25　Principles

第 25 条　　原　則

1. Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

1. 加盟国は、処理されている、又は後に処理される予定の個人データの第三国への移動は、当該第三国が十分なレベルの保護を提供している場合に限られることを規定するものとする。但し、本指令に従って採択された国内規定に対する遵守を害しないことを条件とする。

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in those countries.

2. 第三国によって提供される保護レベルの適切性は、一連のデータの移転作業を取り巻く全ての環境に照らして査定されるものとする。特にデータの性質、提案された処理作業の目的及び期間、データの移転元の国及び最終目的国、当該第三国で効力を有する一般的な及び分野別の法律、当該第三国で遵守されている職業上の規則、及び防衛上の措置が考慮に入れられるものとする。

3. Member States and the Commission shall inform each other of cases where the consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.

3. 加盟国及び委員会は、第三国が第２項の意味の枠内で適切な保護のレベルを確保していないと考える場合に、互いに情報を交換するものとする。

4. Where the Commission finds, under the procedure provided for in Article 31(2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article Member States shall take the measures necessary to prevent the transfer of data

of the same type to the third country in question.

4. 委員会は、第３１条２に規定されている手続きに基づいて、第三国が本条の第２項の意味の枠内で、適切なレベルの保護を確保していないことを認定した場合には、加盟国は当該第三国に同種のデータの移転を妨げるために必要な措置を取るものとする。

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the funding made pursuant to paragraph 4.

5. 委員会は適切な時に、第４項に従って行われた認定から生じた状況を修正するために交渉を行うものとする。

6. The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission's decision.

6. 委員会は第３１条２に規定されている手続きに従って、個人のプライバシー権、基本的自由及び権利の保護に対する第三国の国内法、又は委員会が特に第５項で触れた交渉の結果に基づいて実施した国際的介入によって、本条第２項の枠内で適切なレベルの保護を確保していることを認定することができる。

加盟国は、委員会の決定に従うために必要な措置を取るものとする。

Working Party on the Protection of Individuals with regard to the Processing of Personal Data
Working Document
Transfers of personal data to third countries：Applying Articles 25 and 26 of the EU data protection directive（Adopted by the Working Party on 24 July 1998）
個人データの処理における個人保護に関する作業部会
作業文書
第三国への個人情報の移転について　EU データ保護指令第 25 および 26 条の適用
（1998 年７月 24 日作業部会採択）

CHAPTER ONE: ASSESSING WHETHER PROTECTION IS ADEQUATE
第 1 章：保護が十分かどうかの評価

(1) What constitutes 'adequate protection'?
（1）「十分な保護」を構成する要素とは？

The purpose of data protection is to afford protection to the individual about whom data are processed. This is typically achieved through a combination of rights for the data subject and obligations on those who process data, or who exercise control over such processing. The obligations and rights set down in directive 95/46/EC build upon those set down in Council of Europe Convention N°108 (1981), which in turn are not dissimilar from those included in the OECD guidelines (1980) or the UN guidelines (1990). It would therefore appear that there is a degree of consensus as to the content of data protection rules which stretches well beyond the fifteen states of the Community.

データ保護の目的は処理されるデータの該当者に保護を提供することである。これは通常、データ主体に対する権利と、データを処理する者またはデータ処理の管理を行う者に課せられる義務の両方を考慮することによって達成される。この義務と権利については、EU 指令 95/46/EC に定められているが、この指令は 1981 年の欧州評議会第 108 条約（Council of Europe Convention No.108）の規定に基づいており、さらに同条約規定は、OECD ガイドライン（1980）または国連ガイドライン（1990）に含まれる内容と類似していると言ってよい。したがって、データ保護規則の内容については、欧州共同体の 15 カ国を大きく超えて一定のコンセンサスがあると考えられる。

However, data protection rules only contribute to the protection of individuals if they are followed in practice. It is therefore necessary to consider not only the content of rules applicable to personal data transferred to a third country, but also the system in place to ensure the effectiveness of such rules. In Europe, the tendency historically has been for data protection rules to be embodied in law, which has provided the possibility for non-compliance to be sanctioned and for individuals to be given a right to redress. Furthermore such laws have generally included additional procedural mechanisms, such as the establishment of supervisory authorities with monitoring and complaint investigation functions. These procedural aspects are

reflected in directive 95/46/EC, with its provisions on liabilities, sanctions, remedies, supervisory authorities and notification. Outside the Community it is less common to find such procedural means for ensuring compliance with data protection rules. Parties to Convention 108 are required to embody the principles of data protection in law, but there is no requirement for additional mechanisms such as a supervisory authority. The OECD guidelines carry only the requirement that they be 'taken into account' in domestic legislationand provide for no procedural means to ensure that the guidelines actually result in effective protection for individuals. The later UN guidelines, on the other hand, do include provisions on supervision and sanctions, which reflects a growing realisation worldwide of the need to see data protection rules properly enforced.

しかしながら、データ保護規則は実際に守ってこそ個人の保護に役立つ。したがって、第三国に移転される個人情報に適用される規則の内容のみならず、当該規則の有効性を確保するために整備される制度についても検討する必要がある。欧州では従来、データ保護規則は法律として制定される傾向にあり、規則を遵守しなければ処罰される可能性と個人には救済を得る権利が与えられる可能性を規定してきた。さらにそのような法律には一般的に、追加の手続き的メカニズムが含まれている。たとえば、監視や苦情調査の機能を持つ監督機関の設立である。このような手続き面は、責任、制裁措置、救済措置、監督機関、通知に関する規定により、指令 95/46/EC に反映されている。共同体外部では、データ保護規則の遵守を確実にするためのこうした手続き的手段はあまり見られない。108 条約締約国は、データ保護の原則を法制化することが求められるが、監督機関などの追加的メカニズムに対する要求はない。OECD ガイドラインは、国内法でガイドラインを「考慮する」旨を要件として述べているだけで、ガイドラインが個人のための効果的な保護を実現するための手続き的手段について規定してはいない。一方、後に作成された国連ガイドラインは、監督と制裁に関する条項を含んでいるが、これはデータ保護規則が正しく実施される必要性に対する認識が、世界的に高まっていることを反映したものである。

Against this background it is clear that any meaningful analysis of adequate protection must comprise the two basic elements：the content of the rules applicable and the means for ensuring their effective application.

このような背景において、十分な保護の分析を有意義にするためには、分析は２つの基本要素から成り立つものでなければならない。それは適用される規則の内容とその効果的な適用を確実にする手段である。

Using directive 95/46/EC as a starting point, and bearing in mind the provisions of other international data protection texts, it should be possible to arrive at a 'core' of data protection 'content' principles and 'procedural/enforcement' requirements, compliance with which could be seen as a minimum requirement for protection to be considered adequate. Such a minimum list should not be set in stone. In some instances there will be a need to add to the list, while for others it may even be possible to reduce the list of requirements. The degree of risk that the transfer poses to the data subject will be an important factor in determining the precise

requirements of a particular case. Despite this proviso, the compilation of a basic list of minimum conditions is a useful starting point for any analysis.

指令 95/46/EC を出発点として使い、他の国際的なデータ保護文書の規定を念頭におけば、データ保護「内容」原則と「手続上・実施上」要件の「中核」に到達できるはずである。そしてそれらの遵守が、保護が十分とみなされるための最低条件と考えることができるだろう。その場合、最低限のリストは確定してしまってはいけない。場合によって、リストに項目を追加する必要が生じるだろうし、要件リストの項目を減らせることもあるかもしれないからである。移転がデータ主体に及ぼすリスクの度合いは、特定の事例について厳密な要件を定めるうえで、重要な要因となるだろう。とはいえ、最低条件の基本リストを作成することは、どのような分析にとっても出発点として有効である。

(i) Content Principles

（i）内容原則

The basic principles to be included are the following:

含めるべき基本原則は以下の通りである。

1) the purpose limitation principle - data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer. The only exemptions to this rule would be those necessary in a democratic society on one of the grounds listed in Article 13 of the directive.2

1）目的制限の原則――データは特定目的のために処理され、その後は移転の目的と矛盾しない範囲でのみ使用または伝達されるものとする。この原則の適用除外となるのは、指令の第 13 条に列記された根拠の中の一つの項目に基づいて、民主主義社会で必要とされる場合に限る 。

2) the data quality and proportionality principle - data should be accurate and, where necessary, kept up to date. The data should be adequate, relevant and not excessive in relation to the purposes for which they are transferred or further processed.

2）データの質と相応性の原則――データは正確であり、必要に応じて最新に保たれるものとする。データはそれが移転され、またはさらに処理される目的に照らして、十分であり、関連しており、過剰であってはならない。

3) the transparency principle - individuals should be provided with information as to the purpose of the processing and the identity of the data controller in the third country, and other information insofar as this is necessary to ensure fairness. The only exemptions permitted should be in line with Articles 11(2)3 and 13 of the directive.

3）透明性の原則――個人はデータ処理の目的と第三国のデータ管理者の身元(identity)に関する情報および公正を期するために必要と考えられる範囲の情報を提供されるものとする。適用除外として認められるのは、指令の第 11 条（2）項 および 13 条に一致する場合のみである。

4) the security principle - technical and organisational security measures should be taken by the data controller that are appropriate to the risks presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process data except on instructions from the controller.
4) セキュリティの原則――データ処理がもたらすリスクに見合う技術的且つ体系的なセキュリティ対策を、データ管理者が講じるものとする。データ処理者を含め、データ管理者の権限下で働く者は、管理者の指示による以外のデータ処理をしてはならない。

5) the rights of access, rectification and opposition - the data subject should have a right to obtain a copy of all data relating to him/her that are processed, and a right to rectification of those data where they are shown to be inaccurate. In certain situations he/she should also be able to object to the processing of the data relating to him/her. The only exemptions to these rights should be in line with Article 13 of the directive.
5) アクセス、訂正、および異議を唱える権利――データ主体は、自分に関わる処理された全データのコピーを入手する権利、および示されたデータが不正確である場合にはこれらのデータを修正する権利を有するものとする。一定の状況においては、データ主体は自分に関わるデータの処理に異議を唱えることもできるものとする。これらの権利の適用除外は、指令の第 13 条に一致する場合のみとする。

6) restrictions on onward transfers - further transfers of the personal data by the recipient of the original data transfer should be permitted only where the second recipient (i.e. the recipient of the onward transfer) is also subject to rules affording an adequate level of protection. The only exceptions permitted should be in line with Article 26(1) of the directive (These exemptions are examined in Chapter Five.)
6) 二次移転の制限――最初のデータ移転のデータ受領者による個人データのさらなる移転は、2 番目の受領者（二次移転の受領者）もまた、十分なレベルの保護を提供する規則に従う場合に限られる。認められる適用除外については指令の第 26 条（1）項に一致する場合のみである。（これらの適用除外については第 5 章で考察する。）

Examples of additional principles to be applied to specific types of processing are:
特殊な種類の処理に適用される追加原則の例は、以下の通りである。

1) sensitive data - where 'sensitive' categories of data are involved (those listed in article 8 of the directive4), additional safeguards should be in place, such as a requirement that the data subject gives his/her explicit consent for the processing.
1) 機密データ―「機密」分類のデータ（指令の第 8 条 に記載）が含まれている場合、たとえばデータ主体がデータ処理に関して明示的な同意を与えるという要件など、追加の保護条項を講じるものとする。

2) direct marketing - where data are transferred for the purposes of direct marketing, the data subject should be able to 'opt-out' from having his/her data used for such purposes at any stage.

2）ダイレクトマーケティング――ダイレクトマーケティングの目的でデータが移転される場合、データ主体が、どの段階でもそのような目的のために自分のデータが使用されることを「オプトアウト（拒否）」できるようにするものとする。

3) automated individual decision - where the purpose of the transfer is the taking of an automated decision in the sense of Article 15 of the directive, the individual should have the right to know the logic involved in this decision, and other measures should be taken to safeguard the individual's legitimate interest.

3）自動処理による個人に関する決定――データ移転の目的が指令の第 15 条が意味するところの自動処理による決定を行うことである場合、当該個人はこの決定に関わる必然性を知る権利を有するものとし、当該個人の正当な利益を守るための方策が講じられなければならない。

(ii) Procedural/ Enforcement Mechanisms

（ii）手続上・実施上のメカニズム

In Europe there is broad agreement that data protection principles should be embodied in law. There is also broad agreement that a system of 'external supervision' in the form of an independent authority is a necessary feature of a data protection compliance system. Elsewhere in the world, however, these features are not always present. To provide a basis for the assessment of the adequacy of the protection provided, it is necessary to identify the underlying objectives of a data protection procedural system, and on this basis to judge the variety of different judicial and non-judicial procedural mechanisms used in third countries.

欧州では、データ保護原則を法に盛り込むことが広く合意されている。また、独立した権限機関の形での「外部監督」制度が、データ保護コンプライアンスシステムの必要な機能であることも広く合意されている。しかし世界の他の国・地域では、このような機能は必ずしも存在していない。提供されているデータ保護の十分性を評価する基盤をもうけるために、データ保護手続きシステムの根本的な目的を明らかにする必要がある。そしてそれを基に、第三国で使用されている様々な司法および司法以外の手続き上のメカニズムを見極める必要がある。

The objectives of a data protection system are essentially threefold:

データ保護システムの目的は、3 つの大きな柱から成り立っている。

1) to deliver a good level of compliance with the rules. (No system can guarantee 100% compliance, but some are better than others). A good system is generally characterised by a high degree of awareness among data controllers of their obligations, and among data subjects

of their rights and the means of exercising them. The existence of effective and dissuasive sanctions can play an important in ensuring respect for rules, as of course can systems of direct verification by authorities, auditors, or independent data protection officials.

1）良好な規則遵守レベルを実現すること。（どんなシステムも 100 パーセントの遵守を保証することはできないが、他より優れているシステムはある。）優れたシステムでは、一般的に、自らの義務に対するデータ管理者たちの意識が高いレベルにあり、データ主体は自らの権利とそれらの行使方法に対する意識が高い。効果的で抑止力のある制裁は、規則の尊重を確実にするうえで重要な役割を果たし、もちろん当局、監査人、または独立したデータ保護官による直接的な検証システムも同様の役割を果たす。

2) to provide support and help to individual data subjects in the exercise of their rights. The individual must be able to enforce his/her rights rapidly and effectively, and without prohibitive cost. To do so there must be some sort of institutional mechanism allowing independent investigation of complaints.

2）個人のデータ主体が権利を行使することに支援と援助を供与すること。個人はそれぞれの権利を迅速且つ効果的に、そして法外な費用を必要とせず行使できなければならない。そのためには、苦情について独立した調査を可能とする何らかの制度的メカニズムがなければならない。

3) to provide appropriate redress to the injured party where rules are not complied with. This is a key element which must involve a system of independent adjudication or arbitration which allows compensation to be paid and sanctions imposed where appropriate.

3）規則が守られなかった場合に被害を被る当事者に対して、適切な救済策を提供すること。これは重要な要素であり、必要に応じて補償が支払われ、制裁が科せられることを可能にする、独立した裁定または仲裁システムが含まれなければならない。

資料２－参考４

国際的整合性の観点から見た我が国の個人情報保護制度に対するコメント

１．経済産業省委託調査　平成 22 年度我が国情報経済社会における基盤整備（経済産業分野を対象とする個人情報保護ガイドライン等の見直し及び普及啓発に係る調査研究）報告書　平成 23 年３月株式会社野村総合研究所

p.66-67（関係箇所のみ引用（下線は事務局にて記載））

（３）日本に関する評価

一橋大学名誉教授の堀部政男氏は、ブリュッセルのデータ保護会議で明らかにされた、日本の個人情報保護法に対するヨーロッパの見方について、次のように取り上げている。

（略）

③ 欧州委員会の「十分性認定手続」―ペチャコバ女史のプレゼンテーション

このデータ保護会議[1]では、前述のように、欧州委員会・司法内務総局のハナ・ペチャコバ女史[2]が、「十分性認定手続」というプレゼンテーションを行った。

（略）

ペチャコバ女史は、前掲の「(10)十分性」において、特に日本について、次のようなことを述べた。

・委員会は、第三国が十分なレベルの保護を確保していると認定することができる。

・このような決定の効果は、個人データが 27 の EU 構成国及び 3 つの欧州経済領域(European Economic Area, EEA)(ノルウェイ、リヒテンシュタイン及びアイスランド)からその第三国へ、追加的な安全保護措置を必要としないで、流通することができることである。

・日本は、個人の私生活にかかわる個人データ及び基本権に関して十分なレベルの保護を提供している国であるとは、EU によってまだ考えられていない。

・したがって、EU 構成国から日本へのデータの移転は、EU 構成国各国のデータ保護機関による事前の情報／権限付与(prior information/authorization)を意味する指令 95/46/EC 第 26 条に従って行われなければならない。(EU データ保護指令第 26 条は、前掲のとおりであるので、ここでは繰り返さないことにする。)

・移転がデータ主体の保護を確実なものとする適切な保障を提供することを証明するためには、特に特別の契約上の取決めによって、例えば、委員会によって承認された標準契約条項モデルの一つを使用することによって、行うことができる。

（略）

・委員会は、個人データの保護とデータ移転の領域における協力関係を改善し、最高度の国際的基準に従い EU と日本間における個人データの自由な移転に向けて作業を進めるつもりである。

・委員会は、日本のデータ保護法の全体像を把握し、十分性認定手続をおそらく開始するために、詳細な分析を行うことを考えている。

・とはいえ、この構想も日本側によって支持されなければならない。

・十分性認定手続を開始するためには、日本の代表部によってなされる公式の要請が欧州委員会に提出されなければならない。

---

[1] ベルギーの首都ブリュッセルにおいて、2009 年 4 月 23 日、日白協会(Belgium-Japan Association)主催のデータ保護会議(BJA-Conference on Data Protection)が開催された。

[2] (European Commission Directorate-General-Justice, Freedom and Security)法務政策部(Legal Affairs and Policy)ユニット D5・データ保護(Unit D5 -Data Protection)事務官(Desk Officer) ハナ・ペチャコバ(Hana Pechackova)

p.78（関係箇所のみ引用（下線は事務局にて記載））

③十分な保護レベルの有無

ブリュッセルのデータ保護会議におけるペチャコバ氏のプレゼンテーションによれば、十分性認定手続を開始するためには、日本の代表による公式な要請が欧州委員会に提出されなければならない。そして、日本は、個人の私生活にかかわる個人データ、及び、基本権に関して十分なレベルの保護を提供している国であるとは、EU によってまだ考えられていない状況である。

しかし、上記の検討結果を踏まえると、日本が十分性の認定を受けるためには、クリアしなければならない複数の課題が存在するといえる。一方で、**国内事業者を対象にしたヒアリング結果によれば、個人データ保護指令に至急対応しなければならないという声はあまり見られず、過剰な規制は望ましくないという趣旨の意見が多く寄せられている。**

２．個人情報保護制度における国際的水準に関する検討委員会・報告書（平成 24 年 3 月消費者庁）

p.101（関係箇所のみ引用（下線は事務局にて記載））

（６）日本の法制度に対する評価

2010 年 1 月 20 日、欧州委員会は、「特に科学技術の発展に照らしたプライバシーの新たな課題に対する異なるアプローチに関する比較研究」82 を公表した。日本を含む 11 か国の法制度の状況を調査する内容の報告書となっている。日本については、オーストラリア・ニュー・サウス・ウェールズ大学法学部の Graham Greenleaf 教授がその調査結果を公表した。

日本の状況については、33 頁の報告書の中で、①日本における情報プライバシーの背景、②立法、③要約と結論の構成からなり、特に立法内容について詳細な分析がなされている。

主要な点については次のとおり報告されている。

（略）

〇日本のトラストマーク

日本のトラストマークはプライバシーマークが用いられており、事業者はそれを取得する努力や漏えい後の報告をするなど行っており、同時に消費者にとってもこのマークを信頼できるものとなっている。

そして、結論として、次のように述べられている。

「重要な行政罰・刑事罰、および法令違反に伴う裁判所の判断が存在しないと言われる。日本の実務家によれば、事業者にとっては法令違反することによる多額の罰金を支払うことや団体訴訟というよりも社会的地位の低下の危険が指摘されている。…

日本の法律はまだ４年間しか執行されておらず、暫定的な評価は困難である。さらに、日本では、訴訟ではなくインフォーマルな紛争解決に関する法制度に依拠している。省庁が収集した資料、コンプライアンス、データ違反、救済に関する公表資料から、日本の法律が効果的であることの証拠がないと判断することは合理的であろう。

（国際基準から見た日本の位置づけについて）日本のデータ保護制度は OECD ガイドラインの基準を満たしている。また、APEC プライバシー・フレームワークの基準を満たしていることも疑いはない。EU 指令との関係になるとこのレポートの範囲を超えるもので、難しい判断となる」

３．パーソナルデータの教科書（2014 年日経ＢＰ社　小林慎太郎）

p.115（関係箇所のみ引用）

日本の個人情報保護制度では、第三者機関は設置せず、行政機関に対する保護は各府省の自主的な取り組みに任され、民間事業者へは、各分野の所管官庁が担当する「主務大臣制」と呼ばれる方式をとっている。この権限が分散化した日本の体制は、公的機関の監視や個人の権利利益の保護が不十分であるとＥＵから指摘されており、個人情報保護法を見直す論点の一つとなっている。

※　３は、前述１．の p.66、67 に記載されているペチャコバ事務官のコメントを基に記載しているとのこと。

資料２－参考５

未定稿

諸外国における公的部門が保有するパーソナルデータの監督機関

	関係法令	監督機関	性格、位置付け、任命、体制・組織形態
イギリス	【単独】 データ保護法	【単独】 情報コミッショナー	〈組織〉 ・独任制の機関（約 350 人） ・女王任命
			〈所掌〉 ・データ管理者の登録 ・諸規則の制定権 ・報告徴求権、立入検査権 ・データ保護法遵守に関する情報発信、相談対応、業界団体に向けた実務指針の配布 ・データ保護法に違反したデータ管理者の提訴
フランス	【単独】 情報処理、情報ファイル及び自由に関する法律	【単独】 情報処理及び自由に関する全国委員会（CNIL）	〈組織〉 ・合議制の独立行政機関（約 130 人） ・委員 17 名により構成（裁判官（破毀院総会選出）、国会議員（上院下院選出）、経済・社会評議会委員、ＩＴ専門家（上院下院議長任命）等）
			〈所掌〉 ・毎年、年次報告書を提出 ・届出された個人情報の自動処理及び許可した処理のリストを公表 ・不服申立処理 ・行政調査権（立入調査権、情報収集のための物件の入手） ・警告、処理中止の指示、指示に従わない情報処理責任者への制裁権限

ドイツ	【単独】 連邦データ保護法 ※ ただし、公的部門と民間部門を書き分け（対象個人情報の範囲（データベースか紙情報も含むか）、規律の内容等）	【複数】 国（連邦）：連邦データ保護・情報自由監察官 州、民間部門：州のデータ保護・情報自由監察官又は内務省の下の監督官庁	〈組織〉 ・独任制の機関（約 90 人） ・連邦議会選任、連邦大統領任命 ・連邦政府の法的監督の下、連邦内務省に置かれ、連邦内務省の職務監督を受ける 〈所掌〉 ・苦情処理 ・公的機関によって得られた信書等の内容等に関する個人データの監督 ・全ての執務室への立入権限 ・監督と関連したあらゆる資料及び書類、蓄積されたデータ等の閲覧 ・立法への意見表明
オーストリア	【単独】 個人データの保護に関する連邦法 ※ ただし、公的部門と民間部門を書き分け（対象個人情報の範囲（データベースか紙情報も含むか）、規律の内容等）	【単独】 「データ保護委員会」及び「データ保護審査会」	〈組織〉 〇データ保護委員会 ・独立行政機関（委員も独立） 〇データ保護審査会 ・連邦総理府に設置 ・各代表者により構成（第１党４人、第２党３人、その他政党各１人、労働組合１人、経済団体１人、各州２人、自治体１人（市長会、町村会各１人））、首相任命１人 〈所掌〉 〇データ保護委員会 ・正当な状態を確立するための勧告 〇データ保護審査会 ・データ保護の法政治的問題における要請について、連邦政府及び州政府に助言 ・データ保護のための基本的で重要な質問についての審議 ・公共部門データ管理者にする情報及び文書の報告徴求権 （・連邦政府と州政府に対するデータ保護の改善のための提案権（立法機関も同様））

カナダ	【複数】 公的部門：連邦プライバシー法 民間部門：個人情報保護及び電子文書法により規律	【単独】 カナダプライバシーコミッショナー	〈組織〉 ・独任制の機関 ・議会議決、総督任命 ・省庁の長官代理としての地位及びすべての権限を有する 〈所掌〉 ・調査及び検討に必要と認めた文書及び物品を提出させる権限 ・立入検査権限 ・自ら不服申立てを行う権限（自己付託） ・自ら当事者となって司法裁判所に救済を求める権限
米国	【複数】 公的部門:連邦プライバシー法 民間部門：セクトラル方式（分野ごとに規律）	【複数】 公的部門：行政管理予算庁（OMB） 官民共通：プライバシー保護調査委員会 民間部門：連邦取引委員会（FTC）を中心としつつ、多数の機関が存在	〈組織〉 〇行政管理予算庁 ・大統領府に置かれている執行機関であり、その一部門で行政機関のプライバシー等を所掌している。 〇プライバシー保護調査委員会 ・７名で構成（大統領選３人、上院選２人、下院選２人） 〈所掌〉 〇行政管理予算庁 ・各行政機関が規定を実施するに当たり使用するガイドライン及び規則の作成、一般国民からの意見を聞くための公示、制定 ・行政機関による規定の実施について継続的な援助及び監督 〇プライバシー保護調査委員会 ・個人情報の保護のために実施すべき基準及び手続を定めるためのデータバンク、情報システム等の調査（個人情報伝達システム、情報処理プログラム等の調査、検討、分析等を含む） ※　医療や電子的小切手処理における個人情報活動を対象に含む

			・連邦議会の方針を遂行するために必要な他の個人情報活動についての調査 ・特定種類の情報につき、その収集が個人のプライバシーの権利を侵害するものとして、行政機関による収集を法令で禁止すべきことを決定 ・所掌事務の遂行のための立入検査、個人特定可能データの受領等

〈法体系〉

・官民で共通の法律になっているのは、イギリス、フランス、オーストリア、ドイツ

・官民で法律が分かれているのは、カナダ、米国

（米国の民間部門においては事業分野別のセクトラル方式）

〈監督機関〉

・官民を通じて単一の監督機関になっているのは、イギリス、フランス、オーストリア、カナダ

・官民別の監督規制機関を有するのはドイツと米国

参考

EU データ保護指令と EU データ保護規則の比較（ＥＵ加盟国の機関が満たすべき基準）

	監督対象等	概要
EU データ保護指令（1998 年）	官民共通 ・一つ又は複数の公的機関、職務を遂行する上で、完全に独立して活動（28 条 1 項）	・行政措置又は規則の策定の際の諮問（28 条１項） ・データへのアクセス権限、調査権限（28 条３項） ・処理実施前の勧告、データのブロック、消去又は破壊、執行停止又は取消、管理者への警告又は懲戒、国会への照会等（28 条３項） ・違反の際の訴訟提起又は司法当局への通知（28 条３項） ・個人からの請求受付・処理、調査依頼受付・処理（28 条 4 項） ・報告書の作成・公表（28 条第 5 項）
EU データ保護規則案	官民共通 ・権限を行使する際、完全独立して行動。構成員は完全な独立と公平を維持。（第 47 条 1・2 項）。	【義務】 ・本規則適用の監視と確保、データ主体による苦情申立の聴取及び調査報告、他の監督機関との情報共有と相互扶助、調査、個人データ保護に影響を及ぼす動向の監視、立法・行政措置に関する協議、処理運用に関する認可、行動規範の草案、拘束的企業準則の承認、欧州データ保護委員会への参加、管理者及び処理者の認証、広報啓発（第 52 条 1～2 項）。 【権限】 ・違反通知、命令、事前認可・事前協議、警告・注意、データ修正・削除・破壊の命令、処理の禁止、データ移転の停止、意見表明、 管理者及び処理者の認証、議会・政府等への通知、本規則提案違反の報告奨励のための仕組み策定（第 53 条 1 項） ・データへのアクセスと立ち入り検査等の調査権限、訴訟手続を進める権限、制裁権限（第 53 条 2～4 項） ・年次報告書の作成公表（第 54 条）。 ＜欧州理事会による修正案＞ ・義務に、本規則提案のための管理者及び処理者への意識向上が追加されたが、立法・行政措置に関する協議、処理運用に関する認可、行動規範の草案、拘束的企業準則の承認、欧州データ保護委員会への参加の削除が検討されている（第 52 条 1 項 ac 号、f～i 号）。 ・権限に、国内の立法により、監視権限（monitoring powers）、調査権限（investigatory powers）、 是 正

		権限（corrective powers）、認可権限（authorisation powers）をそれぞれ規定することが検討されている（第 53 条 1 項～1c 項） 【罰則と救済】 ・データ主体、その他の団体はいかなる加盟国の監督機関に対し苦情申立する権利及び司法救済を求める権利を有する（第 73～74 条）。 ・監督機関は訴訟手続を進める権利を有する（第 76 条 2 項）。 ・監督機関は制裁金を科すことができる（第 79 条）。 ＜欧州理事会による修正案＞ ・訴訟手続について、他の加盟国ですでに同一事件の訴訟が進行している場合、その国の訴訟を停止することができることが検討されている（第 76a 条）。

資料２－参考６

行政機関等個人情報保護法の施行に関する総務大臣の権限・役割及び情報公開・個人情報保護審査会の所掌等

□　総務大臣の権限・役割

＜行政機関等個人情報保護法に規定されている権限等＞

行政機関等個人情報保護法は、個人情報の保有、管理等の主体である各行政機関等の長の義務、とるべき必要な措置等を規定している。その上で、各行政機関等における法運用の統一性、法適合性を確保するとともに、個人の権利利益を保護する等の観点から、個人情報の保有主体たる各行政機関の長等から離れた（各行政機関から独立的な）立場にある総務大臣の権限として、以下を規定している。

・個人情報ファイルの保有等に関する事前通知

第 10 条　行政機関（略）が個人情報ファイルを保有しようとするときは、当該行政機関の長は、あらかじめ、総務大臣に対し、次に掲げる事項を通知しなければならない。

法運用の統一性、法適合性を確保するための調整を行うという観点

・開示請求としようとする者に対する情報の提供等

第 47 条第２項　総務大臣は、この法律の円滑な運用を確保するため、総合的な案内所を整備するものとする。

政府全体として自己情報の開示請求権、訂正請求権、利用停止請求権制度やその手続等について教示、案内を行ったり、開示請求等をしようとする者が自己の情報がどの行政機関にどのように保有されているか等について参考となる情報を提供するなど、総合的な案内をする目的

・施行の状況の公表

第 49 条　総務大臣は、行政機関の長に対し、この法律の施行の状況について報告を求めることができる。
２　総務大臣は、毎年度、前項の報告を取りまとめ、その概要を公表するものとする。

本法の施行の状況を把握し、必要と認める場合には、その改善措置を適時適切に講ずる等の目的

・資料の提出及び説明の要求、意見の陳述

第 50 条　総務大臣は、前条第一項に定めるもののほか、この法律の目的を達成

するため必要があると認めるときは、行政機関の長に対し、行政機関における個人情報の取扱いに関する事務の実施状況について、資料の提出及び説明を求めることができる。

第 51 条　総務大臣は、この法律の目的を達成するため必要があると認めるときは、行政機関の長に対し、行政機関における個人情報の取扱いに関し意見を述べることができる。

各行政機関等における法運用の統一性、法適合性を確保する目的。例えば、個人情報ファイルの保有に関する事前通知、法施行状況の調査、国民からの苦情等により、本法の違反又は不適切な運用が疑われる場合、総務大臣は各行政機関の長へ資料の提出及び説明を求め、必要な場合、意見を述べ改善を図ることを規定するもの。

＜運用に関する取組＞

総務大臣は、各行政機関から離れた（独立的な）立場から、法施行の運用、円滑性を確保するため、以下の取組

① 行個法の施行、運用に当たっての各種指針等の策定、発出

- 行政機関の保有する個人情報の適切な管理のための措置に関する指針について（平成 16 年９月 14 日総務省行政管理局長通知）
- 独立行政法人等の保有する個人情報の適切な管理のための措置に関する指針について（平成 16 年９月 14 日総務省行政管理局長通知）

行個法第６条等に基づく正確性、安全確保、利用・提供の制限等に関する措置の徹底のため具体的な方針を提示

具体的には、管理体制、職員の責務、保有個人情報の取扱い（アクセス制限、複製等の制限、誤りの訂正、廃棄等）、情報システムにおける安全の確保等（アクセス制御、アクセス記録、不正アクセス防止等）、情報システム室等の安全管理、入退室記録、保有個人情報の提供及び業務の委託等、安全確保上の問題への対応（事案の報告及び再発防止措置、公表等）、監査及び点検の実施等に関する内容を規定

② 民間部門も含めた重大事案の発生に際して、随時の点検、必要な対応要請

- 行政機関等が保有する個人情報の適切な管理の徹底について（通知）（平成 26 年７月 24 日付け総管管第 60 号総務大臣通知）

③ 漏えい等の事案の発生に応じて随時注意喚起と再発防止等の観点から通知等を発出

・　保有個人情報の持出し等による漏えい等の防止について（平成 18 年３月８日事務連絡）
・　ＰＤＦファイルのホームページへの掲載に係る個人情報の取扱いについて（平成 20 年５月 30 日事務連絡）

④　毎年度、法施行状況調査を実施、取りまとめの公表

⇒漏えい等問題の発生状況等に応じて必要な改善等の要請

・　行政機関等個人情報保護法の適正な運用について（平成 25 年８月 30 日事務連絡）

⑤　法の適正・円滑な施行を図るため、定期的に連絡会議を開催

⑥　各府省の個人情報保護に関する研修の実施

□　情報公開・個人情報保護審査会の所掌、権限等

行政機関等が保有する個人情報について、自己情報の開示、訂正、利用停止請求等の本人関与の仕組みの運用の中立性、客観性を確保するため、合議制の機関として法律により設置されているもの

＜審査会の調査審議の手続＞（第三章）

審査会の調査権限

第九条　審査会は、必要があると認めるときは、諮問庁に対し、行政文書等又は保有個人情報の提示を求めることができる。この場合においては、何人も、審査会に対し、その提示された行政文書等又は保有個人情報の開示を求めることができない。

２　諮問庁は、審査会から前項の規定による求めがあったときは、これを拒んではならない。

３　審査会は、必要があると認めるときは、諮問庁に対し、行政文書等に記録されている情報又は保有個人情報に含まれている情報の内容を審査会の指定する方法により分類又は整理した資料を作成し、審査会に提出するよう求めることができる。

４　第一項及び前項に定めるもののほか、審査会は、不服申立てに係る事件に関し、不服申立人、参加人又は諮問庁（以下「不服申立人等」という。）に意見書又は資料の提出を求めること、適当と認める者にその知っている事実を陳述させ又は鑑定を求めることその他必要な調査をすることができる。

意見の陳述

第十条　審査会は、不服申立人等から申立てがあったときは、当該不服申立人等に口頭で意見を述べる機会を与えなければならない。ただし、審査会が、その必要がないと認めるときは、この限りでない。

２　前項本文の場合においては、不服申立人又は参加人は、審査会の許可を得て、補佐人とともに出頭することができる。

意見書等の提出

第十一条　不服申立人等は、審査会に対し、意見書又は資料を提出することができる。ただし、審査会が意見書又は資料を提出すべき相当の期間を定めたときは、その期間内にこれを提出しなければならない。

委員による調査手続

第十二条　審査会は、必要があると認めるときは、その指名する委員に、第九条第一項の規定により提示された行政文書等又は保有個人情報を閲覧させ、同条第四項の規定による調査をさせ、又は第十条第一項本文の規定による不服申立人等の意見の陳述を聴かせることができる。

提出資料の閲覧

第十三条　不服申立人等は、審査会に対し、審査会に提出された意見書又は資料の閲覧を求めることができる。この場合において、審査会は、第三者の利益を害するおそれがあると認めるとき、その他正当な理由があるときでなければ、その閲覧を拒むことができない。

２　審査会は、前項の規定による閲覧について、日時及び場所を指定することができる。

調査審議手続の非公開

第十四条　審査会の行う調査審議の手続は、公開しない。

不服申立ての制限

第十五条　この法律の規定により審査会又は委員がした処分については、行政不服審査法（昭和三十七年法律第百六十号）による不服申立てをすることができない。

答申書の送付等

第十六条　審査会は、諮問に対する答申をしたときは、答申書の写しを不服申立人及び参加人に送付するとともに、答申の内容を公表するものとする。

資料２－参考７

研究会での議論（国際的整合性、第三者機関）

＜パーソナルデータの利活用＞

国際的整合性

- **我が国の個人情報保護法制が前提としているOECDプライバシーガイドラインの改正や､EUデータ保護規則の提案､またドイツ等の諸国の例を参考にしてはどうか。**
- **国際的整合性も１つの論点だが、最終的には我が国として機能するような制度にする必要があるのではないか。**
- （質問に対し）国際的整合性について、グローバルなデータ流通の妨げにならないことは重要であるが､必ずしもＥＵ基準に合わせるよう主張するものではないし､十分性条件について意見の一致をみているわけでもない。（経団連）
- **諸外国の取組との比較の際は、実際に公的部門により行われているサービスと、公的部門が関わっていないサービスとを分けて考えた方がよいのではないか。例えば、我が国では信用情報機関であるＣＩＣ（割賦販売法・貸金業法指定信用情報機関）は公的部門でないし、また、反社会勢力への該当に関する情報は、警察の情報を利用するかどうかによって異なるということになるのではないか。**
- **現在の論点の中で、機微情報はEUに、個人特定性低減データは米国に由来するものであり、両者の関係について検討が必要である。一般的に低減データを導入して、それを更に機微情報とそれ以外に分けるという議論はこれまでなく、この研究会で初めて議論することになるのではないか。**

＜第三者機関の権限・機能等＞

第三者機関の体制・機能

- **「制度の国際的な調和」として、我が国の個人情報保護法制が前提としているOECDプライバシーガイドラインの改正やEUデータ保護規則の提案を参考にしてはどうか。【再掲】**
- 行政機関等によるプライバシー影響評価（PIA）については、番号法における特定個人情報保護評価の手法を活用するとともに、権利利益の侵害に関わるリスク評価のあり方も含めて、実効あるプライバシー影響評価の実施方法について評価・検証する必要があるのではないか。（経団連）
- 第三者機関は必要と思うが、十分な人材や財源が期待できるようになるまでは、実務は従来どおり主務大臣が行うべきではないか。第三者機関は、動きの鈍い省庁を会計検査院のようにチェックしたり、個人情報保護の専門家として各省庁の相談を受けたりする総合的な役割を果たすべきではないか。（日消協）
- （質問に対し）第三者機関は必要であり、例えば、自治体間の運用を合わせるため

のガイドラインのようなものを作る役割を担ってはどうか。また、第三者機関の機能は、消費者委員会のように、行政機関等の保有する個人情報についても縦割りの垣根を取り払って見ることが望ましいのではないか。（全相協）

・条例については、国の法令と自治体の条例を同じにするわけにはいかないし、国が自治体に対しこういう条例にしろと言うことも憲法違反でありできない。そこで、第三者機関が調整機関として役割を果たすという議論があり得るのではないか。

・第三者機関を作るメリットとして、主務大臣制であるとどの省庁に相談してよいか分からない場合に、統一的窓口としての役割を期待できる面があるのではないか。

・行政機関等における個人情報の取扱いについて監視・監督する独立した第三者機関を設立し、大幅に拡充された権限にふさわしい予算・人員を配置して、その任に当たらせるべきではないか。（日弁連）

総務大臣・各主務大臣と第三者機関の権限・機能等の整理

・第三者機関がEUデータ保護指令における十分性認定を受けられるように、総務大臣の権限を移管し、強い権限を与えるべく検討を行うべきではないか。

・（質問に対し）国際的整合性について、グローバルなデータ流通の妨げにならないことは重要であるが、必ずしもＥＵ基準に合わせるよう主張するものではないし、十分性条件について意見の一致をみているわけでもない。ただ、官民間の適正かつ円滑なデータ流通を図るために、個人情報の保護と利活用に関する行政機関が持っている権限等を第三者機関にできるだけ移行していく、場合によっては一元化することについても検討いただきたい。（経団連）

・第三者機関の権限について慎重な立場であり、保護色が強くなり過ぎると経済に悪影響を及ぼしかねないので、慎重に議論すべき。加えて、設置そのものについても慎重な考え方を持っているが、第三者機関を作るとするならば、個人情報を保護するための仕組みとしては、官民で同じであるべきではないか。（新経連）

・低減の程度や機微情報の選択について、制度改正大綱ではケースバイケースということになっており、第三者機関が認定等を行うとしても、少なくとも各省の大臣がある程度関与する仕組みを作る必要があるのではないか。

・行政機関が保有する個人情報の管理・監督について、医療情報については専門知識を有する所管省庁が管理・監督すべきであり、第三者機関がその役割を果たすのは困難ではないか。

・（質問に対し）医療データの管理・監督は、諸外国では専門家のアドバイスを受けてプライバシーコミッショナーが行っており、それは現在我が国で議論されている第三者機関とは異なるものである。（山本参考人）

・医療や教育など各分野の情報については、関係省庁が施策の一環として取扱いを検討し、必要があれば地方公共団体にも助言等を行うべきであって、国の第三者

機関が、行政機関の保有する各分野の個人情報について関与するのは極めて困難なのではないか。

・すべて第三者委員会に引き寄せるという立場から、全く逆の立場、そして個別法を通じて重なりがあるとする中間的な立場など、いろいろな選択肢があるのではないか。

・（質問に対し）第三者機関は、各省庁の個人情報の取扱いの問題が発生した際には、各省庁に徹底調査させたり、各省庁の個人情報の取扱いについて調査したりする権限が必要であり、各行政機関に直接権限行使できる関係が望ましいのではないか。（日弁連）

（注）明朝体で記載したものは、ヒアリング対象者など構成員以外の者の意見である。

パーソナルデータに関する検討会（高度情報通信ネットワーク社会推進戦略本部（ＩＴ総合戦略本部））における国際動向に係る議論

● パーソナルデータ検討会の方向性

・ 最低限、交渉テーブルに着いて、越境データ問題を解決しなければならないというミッションがあり、そこのテーブルに着くためのミニマムな事項は全部洗い出す。第三者機関は数年内に越境データ問題を解決して、産業振興の基盤整備に備えるということは必達の目標。
・ 特に米国、それからやがては欧州との執行協力体制の構築の必要性もやはり越境データ問題解決をして、外貨を稼いでいくという経済成長に向かうのであれば、そこら辺の整備の交渉等に第三者機関に働いてもらうという方向性も、多分、一致しているのではないか。

● アメリカ－日本－ＥＵの関係について

・ アメリカのプライバシー保護の考え方をＥＵにすり合わせて議論すべきではないかという学会の意向も強まっているだろうと私は見ている。（ＥＵ型）
・ 委員提出資料でもあったように、どちらかというとビジネス展開上の制約を強める方向のＥＵケースよりも、ＩＴ分野で経済成長を実現している米国ケースで実現していこうと御提案されており、（略）日本のほうがＥＵよりはビジネスとしては先進的な部分がかなりあるので、ビジネスとして後進なところに全てを合わせる必要はない。（それ以外）
・ ＥＵ・米国追随型ではなく、日本が提案していくというところの局面で、要はＥＵと交渉で頑張れるような交渉の土俵に乗ることを目指していくというのが大筋の考え方ではないか。（ＥＵ型）
・ 米国と協調してＯＥＣＤなどを活用して、日本の提言に基づく国際ルール化ということも模索してＥＵに対応していくことも検討すべき。（それ以外）
・ 機軸となるのは、日米間のビジネスが一番大きい。米国の消費者のデータも持ってこられるというところをベースにし、対ＥＵをどうするかという議論もしていく。そのための執行協力の機関として第三者機関があるということだろう。（ＥＵ型）
・ ＥＵの十分性をとるために日本の制度をどうするかという議論よりも、日本に適した良い制度を作って、その上で理解を求めていくべき。やはり日本としてしっかりとした制度をつくっていくということがより重要。（それ以外）

（注）意見の末尾に括弧書きを付したものは、事務局（総務省）において仮に次のとおり整理したものである。
・（ＥＵ型）は、ＥＵとの整合性を重視する意見。
・（それ以外）は、ＥＵ型ではない形で、我が国に適した個人情報保護の在り方を志向した意見

● セーフハーバーと十分性認定について

・ 国際的に見ても、オプトアウトの手続によって対応しているものは、例えば、米国の金融サービス近代化法を初めとして、一部の法令があるが、ＥＵからはやはりこの部分については、現在でもセーフ・ハーバーの観点からも十分性の基準は認められていないところである。

・ 今後、特定個人情報保護委員会の権限を拡充することによって、国際的な対応に当たっての意見を発信する、また交渉を行うということも可能になると、例えば米国のように、ＥＵとの間でセーフハーバーとして政府による交渉の結果、データの移転を可能にすることもできるのではないか。

● 十分性認定のための規律

・ ＥＵの十分性認定に適合しないのではないかと思われる点としては、センシティブデータの取扱いの規定がないこと、義務規定の適用除外事業者が存在すること、オプトインによる本人同意手続というものが必要。

・ 本人関与について、具体的に請求権の行使の根拠となり得るかどうかということについても、ＥＵの権利としてのプライバシーという観点からの点についても考慮が必要。

・ 機微情報の類型をつくらないとＥＵとの交渉のテーブルに着けないという政治的な問題がある。

● 第三者機関の対象、機能

・ 例えば、第三者機関が法規制によらないガイドラインレベルでの規制によって、一定の要件、または条件のもとに第三者提供の例外を設ける適用除外事由を、明確に示すということは当然あり得るかと思う。

・ オープンデータの活用を円滑に進めるためにも、第三者機関が公的部門を対象にすることは必要。

・ ＯＥＣＤガイドラインは、プライバシー執行機関を置くと定めているが、プライバシー執行機関というのは、国際的にも官民双方を対象にすることが一般的である[1]。

・ 第三者機関が地方公共団体に対しても、どのような法執行を行うのかについて検

---

1 一部の国では、用語「プライバシー執行機関」は、プライバシーを保護する法を共同で執行する機関のグループを指すこともある。たとえば、公共分野のデータ管理者の監督は、政府の異なる部門に属する複数の機関に関係することがあり、当該期間は、ガイドラインの策定や他のデータ利用要件を課す権限を有することがある。そのような場合、第 19 項（c）で要求されている「管理組織、リソース、技術的専門知識」を単一の組織に統合することはできないが、それらの機関全体として執行制度を備えているものとして認めることができる。（プライバシー保護と個人データの国債流通についてのガイドラインに関する理事会勧告改正の補足説明覚書（2013））

In some countries, the term “privacy enforcement authority” can also refer to a group of bodies that collectively enforce laws protecting privacy. For example, oversight of public sector data controllers may involve multiple bodies from different branches of government, who may also have the authority to issues guidelines or other data usage requirements. The “governance, resources, and technical expertise” called for in paragraph 19(c) may not, in such a case, be embodied in a single entity, but rather be found in the enforcement system as a whole.

討することが必要になってくる。

- 国際的に見ても主務大臣の権限との調整を図って第三者機関がそれなりの役割を果たすことができるようにしていく必要がある。
- 日本の場合、第三者機関がないこともあってグローバル・プライバシー・エンフォースメント・ネットワークのメンバーにはなっていない。そのため、外国から見ると日本のどこに協力を求めたらいいのかもわからない状況。
- 特に米国、それからやがては欧州との執行協力体制の構築の必要性もやはり越境データ問題解決をして、外貨を稼いでいくという経済成長に向かうのであれば、そこら辺の整備の交渉等に第三者機関に働いてもらうという方向性も、多分、一致しているのではないか。【再掲】
- プライバシーコミッショナーとして、日本の新しい第三者機関がせっかく国際社会に登場するのであるから、官民を通じた個人情報の適切な取り扱いを行っているという観点からも、この行政機関についての施行状況の公表、資料提出、説明要求、意見陳述は、新しい個人情報保護委員会に移してもいいのではないか。
- 強い政治的な中立性ないし行政機関に対するコントロール権限を、番号関連については既に特定個人情報保護委員会が持っていることからすると、むしろ行政機関個人情報保護法の先ほどのような権限は第三者機関に移すことを検討していただいていいのではないか。

● 越境移転について

- 日本はデータの第三国移転の規定がないので、結果的にデータロンダリングが可能である。そのため、日本を経由して第三国に移転されるということについては、逆に他の国に迷惑をかけるという状況にもなりかねないという状況がある。データのロンダリングという観点からの海外からの批判、国内の事業者が単に委託先の監督責任を果たすということで果たされている第三国へのデータ移転ということについては、何らかの対応が必要だろう。（略）ＥＵでは域外適用というところでかなり思い切った規定を置いているということも参考にすべきところはあるだろう。
- グローバル化を重視しながらも、他国へのデータ移転について、政府がチェックし得ない状況というのは、やはり問題ではないか。

● ＯＥＣＤ関係（プライバシー執行機関）

- 新しくプライバシー執行機関という用語が明記され、プライバシー保護のための法律を各国で整備をすることになっており、我が国もそれに対応しなければ、当然、国際的な標準に対応できないというところもあるかと思う。

注）本資料は、検討会における個々の委員の発言を基に作成したものである。