個人情報保護における国際的枠組みの改正動向調査

報告書

平成 26 年 3 月 28 日

消費者庁

目次

はじめに

昨年度（平成 24 年度）の「アジア太平洋地域等における個人情報保護制度の実態調査」に引き続いて、本年度は、「個人情報保護における国際的枠組みの改正動向調査」を行った。

昨年度も述べたが、個人情報保護法制は、技術の進展を追い、経済の要請とのバランスをとりつつ、しかも、個々の国の文化を踏まえて、現下のグローバル化に対応しなければならないという極めて難しい課題を負っている。昨年度の APEC 構成エコノミーを中心とした個人情報保護法制の実態調査もそのような問題意識に出るものであった。

本年度は、問題意識はほぼ共通であるものの、具体的にどのような国際的取組みがなされているかに焦点を当てて調査を行った。すなわち、個人情報保護法制の一つの国際的な標準モデルとなることを意図している EU データ保護規則案の現状、国際的にみて唯一の法的拘束力ある枠組みと評価されている欧州評議会１０８号条約の現代化の動き、わが国においてもっとも馴染のある国際的文書であり、また、実際にわが国の現行法制に大きな影響を及ぼしている OECD ガイドラインの改正の動向を取り上げた。と同時に、EU とは別の方向から個人情報保護の問題を扱っていると評価できる米国の最新の動きも追っている。プライバシー権利章典をめぐる議論がそれである。そして、EU と米国の個人情報保護に対する異なるアプローチを架橋するものとしてのセーフハーバー協定についても最新の状況を調査した。さらに、わが国の関心事でもある EU からのデータ移転のための第三国としての十分性の審査を受けた経験があるという観点から、オーストラリアの審査後の状況についても検討を加えた。

上記の国々等に対する調査は、わが国でも個別に行われているところであるが、個人情報保護法制をめぐる国際的動きが激しい今日、常に最新の状況を、実態を踏まえて把握しておく必要があると思われる。本調査はそのような意図に出たものである。また、正確な動向調査は、わが国の立法作業の基礎としても有益と思料する。そのような意味で、この種の調査は、今後も定期的に継続されることが望ましいと考えるものである。

最後に、本調査に際して御助力を得た各国の個人情報保護当局関係者、制約のある期間内に現地調査を行っていただいた板倉、河井、宮下の各委員、資料の収集等、委員会の運営を支えてくださった消費者庁消費者制度課個人情報保護推進室の前田恵美氏に心より御礼申し上げる。

委員長　中央大学法科大学院教授　藤原静雄

個人情報保護における国際的枠組みの改正動向調査検討委員会

委員名簿・執筆分担

○	藤原　靜雄	中央大学教授 はじめに、あとがき執筆、全体につき査読
	板倉　陽一郎	ひかり総合法律事務所　弁護士 OECD 改正ガイドライン、オーストラリアにつき執筆
	河井　理穂子	埼玉工業大学専任講師 米国につき執筆
	宮下　紘	中央大学准教授 EU データ保護規則案、欧州評議会 108 号条約につき執筆

（○は委員長）

各項目の概要

Ⅰ 国際的取組みの動向

1 EU データ保護改革

EU では、1995 年のデータ保護指令に代わり、「個人データ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」（データ保護規則提案）が示され、加えて「犯罪又は刑事罰の執行における予防、捜査、捜索又は起訴を目的とする主務機関による個人データ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提案」 （刑事データ保護指令提案）という枠組みが示されている。2014 年 3 月現在これらは、委員会による提案を受け、議会が修正案を議決したものの、理事会においては修正案を内部で審議中の状況にあり、第一読会における三者対話を待っている状況にある。新しい規則提案においては、個人情報の範囲、適用範囲、データ主体の権利、事業者の義務、越境データ移転、および監督機関といった点の取り扱いが、データ保護指令と異なっており、重要な論点とされている。

2 欧州評議会条約第 108 号と現代化提案

1981 年署名の「個人データの自動処理に係る個人の保護に関する条約」（欧州評議会条約第 108 号）について、欧州評議会は、デジタル分野におけるプライバシー保護の強化と条約のフォローアップの仕組みを強力なものにすることを目的として、2011 年以降、条約の現代化の検討を行ってきた。2012 年 11 月に開催された第 29 回総会において諮問委員会による「現代化の提案」が採択されている。現代化にあたっては、主に、適用範囲と適用除外・制限、保護されるデータの範囲、センシティブ・データの処理、データ主体の権利、安全管理措置等の義務の内容、監督機関、越境データ移転、批准国間の相互援助および条約への加入について見直しが行われている。

3 OECD 改正ガイドライン

2013 年 7 月、「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」の 33 年ぶりの改正が OECD 理事会で承認され、「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」に新たな規定が加えられた。改正にあたり新たに、国家的なプライバシー戦略、プライバシーマネジメントプログラム、データセキュリティ侵害通知、説明責任を果たす組織および強化されたプライバシー執行といった概念が導入された。

II 国際的流れにおける各国の動き

1 米国のプライバシー保護法制の最新動向

2012 年 2 月、オバマ政権は「ネットワークの世界における消費者プライバシー：プライバシーの保護とグローバルデジタル経済の革新を促進するフレームワーク」を発表した。フレームワークの中心に位置づけられているのが「消費者プライバシー権利章典」であり、その実現に向けて、プライバシーに関する公的機関を対象とする連邦法（1974 年）及び民間の特定セクターを対象とした連邦法のどの適用も受けていない民間のセクターに適用される法の成立を促すとともに、マルチステークホルダープロセスによる執行可能な行動規範（codes of conduct）の整備を行うとしている。

また、EU 加盟国の個人データの移転に関するセーフハーバー協定については、プリズム問題を契機として、協定見直しの要請を EU 側より受け、より高い透明性、効果的な法執行、およびデータ移転におけるプライバシー保護の強化といった観点で、2014 年夏までに協定を強化するとされた。

2 オーストラリアにおける個人情報保護に関する国際的枠組みへの対応状況

国際的枠組みへの対応については、オーストラリアでは、各枠組みの刷新につき直ちに対応する必要性は特段認められていないようであり、政府の国際的枠組みへの対応は積極的とは見られない。欧州とのデータ移転につき経済界から強い要望が出ているような状況にもなく、現時点では優先順位が高い事項と考えられているとは言い難い。

一方でオーストラリアにおいては、2014 年 3 月 12 日に、2012 年プライバシー改正（プライバシー保護強化）法が施行された。改正法により、それまで公的部門に適用されていた情報プライバシー原則と民間事業者に適用されていた国家プライバシー原則は、新たに 13 のオーストラリアプライバシー原則（Australian Privacy Principles，APPs）に移行した他、連邦情報コミッショナー）の権限強化などが行われている。

I　国際的取組みの動向

1　EU データ保護改革

宮下紘（中央大学）※

「*プライバシーは人間の尊厳と個人の自由にとって不可分である。…*

データ保護改革は日本からウルグアイ、そしてその間にある世界中で議論されている。」[1]

—Viviane Reding（Vice-President European Commission）

はじめに—データ保護改革の現状

2012 年 1 月 25 日、ベルギー・ブリュッセルにて、欧州委員会副委員長 Viviane Reding は、「データ保護改革」を公表した。この改革案では、1995 年に採択された「個人データの処理及び当該データの自由な流通に係る個人の保護に関する指令」（1995 年 10 月 24 日採択，1998 年 10 月 24 日発行）（以下「EU データ保護指令」又は「指令」という。）に代わる「21 世紀に向けたヨーロッパのデータ保護枠組み」[2]が示された。この枠組みには、次の 2 つが含まれる。

・　「個人データ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（一般データ保護規則）提案」（以下、「データ保護規則提案」又は「規則

※ 本稿の執筆にあたり、2014 年 3 月に欧州委員会、欧州議会、欧州理事会、欧州司法裁判所、欧州データ保護監督機関、欧州消費者団体、ベルギー経済省、ナミュール大学、カトリックルーバン大学、Wilson Sonsini Goodrich & Rosati 法律事務所の方々からヒアリング調査を実施させていただいた。調査に際し、欧州連合日本政府代表部の岡野武司書記官にお世話になった。また、上記のヒアリング以外にも、2012 年 1 月にデータ保護改革が公表されて以降、2012 年 1 月～5 月のベルギーでのデータ保護改革の調査研究やその他国際会議の場などを通じて様々な方々から貴重なご意見を頂戴した。特に 2013 年 9 月に開催されたヨーロッパデータ保護国際会議後には、データ保護改革を推進してきた Viviane Reding 欧州委員会副委員長と Jan Philipp Albrecht 欧州議会議員から貴重なご意見を頂戴することができた。ここに記した方々に改めて謝意を記す。なお、EU データ保護指令の和訳は、堀部政男研究室「欧州連合（EU）個人情報保護指令の経緯・仮訳」新聞研究 578 号（1999）17 頁、に依拠させていただいた。

[1] Viviane Reding, Speech: *EU Data Protection Rules: Better for Business, Better for Citizens*, March 26, 2013. Available at http://europa.eu/rapid/press-release_SPEECH-13-269_en.htm (last visited March 27, 2014)

[2] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions; Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century*, COM(2012)9/3 (Jan. 25, 2012).

提案」という。）[3]

・ 「犯罪又は刑事罰の執行における予防、捜査、捜索又は起訴を目的とする主務機関による個人データ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提案」[4]（以下「刑事データ保護指令提案」又は「指令提案」という。）

EU には、連合の機能に関する条約第 16 条 1 項及び EU 基本権憲章第 8 条 1 項において「すべての者は、それぞれ自らに関する個人データの保護の権利を有する」とデータ保護が基本権であることが明確に記されている。ここで加盟国への「潜在的に直接効果を有する」[5]基本権を論じるにあたり、合衆国憲法のように憲法上の権利はあくまで政府の行為に対して行使しうるというという前提が EU にはなく、憲法以外の立法からも、「人間の尊厳」（EU 基本権憲章第 1 条）に立脚し普遍的な人権の保障が及ぶという思考が採られてきた、と言われる[6]。そして、これらの規定に基づき、データ保護という基本権を保障する目的で、EU の成長戦略及びデジタル・アジェンダとも整合する形で、「現代的で、強力で、一貫性あり、そして包括的なデータ保護の枠組み」としての規則提案と指令提案が委員会によって示された[7]。

---

[3] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM(2012)11 final (Jan. 25, 2012). 一般データ保護規則提案の邦語による紹介として、消費者庁「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」（堀部政男「国際的水準の意義」、宮下紘「EU データ保護改革と国際的水準への影響」）（2012 年 3 月）、新保史生「EU の個人情報保護制度」ジュリスト（2014）34 頁以下、藤原静雄「EU データ保護一般規則提案等の概要」NBL975 号（2013）4 頁、石井夏生利「EU データ保護規則提案と消費者プライバシー権利章典」Nextcom10 号（2012）、参照。

[4] European Commission, *Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data*, COM(2012) 10 final (Jan. 25, 2012).

[5] 庄司克宏「EU 基本権憲章の適用に関する議定書の解釈をめぐる序論的考察」慶應法学 19 号（2011）318 頁。また、EU 基本権憲章とデータ保護法制については、消費者庁『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』（庄司克宏「リスボン条約後の EU 個人データ保護法制における基本権保護と域外適用」）17 頁以下、参照。

[6] *See* Frank Michleman, *The Protective Function of the State in the United States and Europe: the Constitutional Question*, in EUROPEAN AND US CONSTITUTIONALISM 156 (Georg Nolte ed. 2005); Paul De Hert & Serge Gutwirth, *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action*, in REINVEINTING DATA PROTECTION? 3 (Serge Gutwirth et. al. eds., 2009); Stefano Rodotà, *Data Protection as a Fundamental Righ*t, *id.* at 77.

[7] *See* Viviane Reding, *The European Data Protection Framework for the Twenty-First Century*, 2 INT'L DATA PRIVACY L., 119, 128 (2012).

2014 年 3 月現在、EU データ保護改革は、委員会による提案を受け、議会が修正案を議決したものの、理事会においては修正案を内部で審議中の状況にあり、第一読会における三者対話を待っている状況にある（本稿の理事会修正はすべて 2014 年 3 月時点のものであり、今後変更の可能性がある）。これまでの主な経過は次のとおりである。

2012 年 1 月 25 日	委員会	EU データ保護改革（規則提案と刑事司法指令提案）公表
2012 年 2 月 27 日	議会	データ保護改革に関するプレゼンテーション
2012 年 12 月 7 日	理事会	加盟国閣僚会合による審議が本格的に開始
2013 年 1 月 16 日	議会	市民的自由・司法・内務委員会の修正案報告書公表（合計 3,999 か所にのぼる修正案が提示）
2013 年 10 月 21 日	議会	市民的自由・司法・内務委員会で採決可決（規則提案：賛成 51 票、反対 1 票、棄権 3 票、指令提案：47 票、反対 4 票、棄権 1 票）
2013 年 10 月 25 日	欧州理事会	加盟国首脳による「時宜を得た」規則提案の採択の必要性を確認
2014 年 3 月 12 日	議会	本会議で市民的自由・司法・内務委員会の修正案を可決・採択（規則提案：賛成 621 票、反対 10 票、棄権 22 票、指令提案：賛成 371 票、反対 276 票、棄権 30 票）
2014 年 3 月 12 日	議会	本会議で NSA 監視プログラムに関する決議が可決・採択（賛成 544 票、反対 78 票、棄権 60 票）
2014 年 3 月 20 日	理事会	Albrecht 議員による議会修正案の報告

2014 年 3 月現在のデータ保護改革に関する委員会、議会、理事会の反応はヒアリング調査を含め次のようなものであった。

委員会

議会での修正案の可決を受け、委員会は議会からの強力な支持を受けたものと捉えている[8]。議会の修正案のポイントとして、①一つの大陸に一つの法を実現するため規則という法形式と効果的な制裁、②欧州の市場での運用を行う EU 以外の企業への EU データ保護法の適用、③忘れられる権利と削除権、④企業と市民ための one-stop-shop の 4 点を挙げている。なお、委員会は 2014 年 6 月までにギリシャの議長国の下で理事会修正案の採択を求

[8] European Commission, *Memo: Progress on EU Data Protection Reform Now Irreversible Following European Parliament Vote*, 12 March 2014.

めており、委員会司法総局でのヒアリングにおいても同様の回答があった[9]。

議会

市民的自由・司法・内務委員会でこれまで審議された単一の提案で最多となる 3,999 の修正案が提出された[10]。この修正案をほぼ独力でとりまとめたのが、Jan Philipp Albrecht 議員（ドイツ緑の党）である[11]。委員会での正式な審議の時間は 30 時間、非公式な審議時間は 250 時間に及んでいる。EU 議会の選挙が 2014 年 5 月に予定されているが、この選挙により議会の議員の構成が変わっても、本会議での修正案可決の結果は変わらない。ヒアリング結果でも、圧倒的多数で可決した以上、選挙後に改めて 3,999 の修正案を再度審議し始める可能性はないとのことである。

理事会

理事会では年 4 回の加盟国の閣僚級（総務・内務大臣や法務大臣）会合のほか、データ保護専門家と加盟国政府関係者から構成される作業部会による審議が行われてきた。議会に比べて合意に至るまでの時間を要した理由は、one-stop-shop の構造への加盟国間の見解の不一致が最大の原因である（one-stop-shop の箇所を参照）。理事会におけるヒアリングによれば、理事会の修正が取りまとめられるのがどんなに早くても 2014 年 12 月であり、そこから 2015 年初旬に委員会と議会による三者対話の交渉に入るとのことである。

下記のとおり、2014 年 3 月現在、理事会は、三者対話（下記の図を参照）のテーブルにつくことができておらず、理事会内部での審議が継続されている。もっとも、2014 年 1 月と 3 月には、議会で修正案を取りまとめた Jan Philipp Albrecht 欧州議会議員を理事会に招き、議会での修正案の審議について意見交換が行われている。Albrecht 議員によれば、理事会閣僚級会合では、イギリス、デンマーク、ハンガリー、オーストリア、ドイツの各政府から規則提案の根本への憂慮が示されている一方で、スペイン、ポーランド、オーストリア、アイルランドの各政府からの早期採択の姿勢が示されている[12]。

---

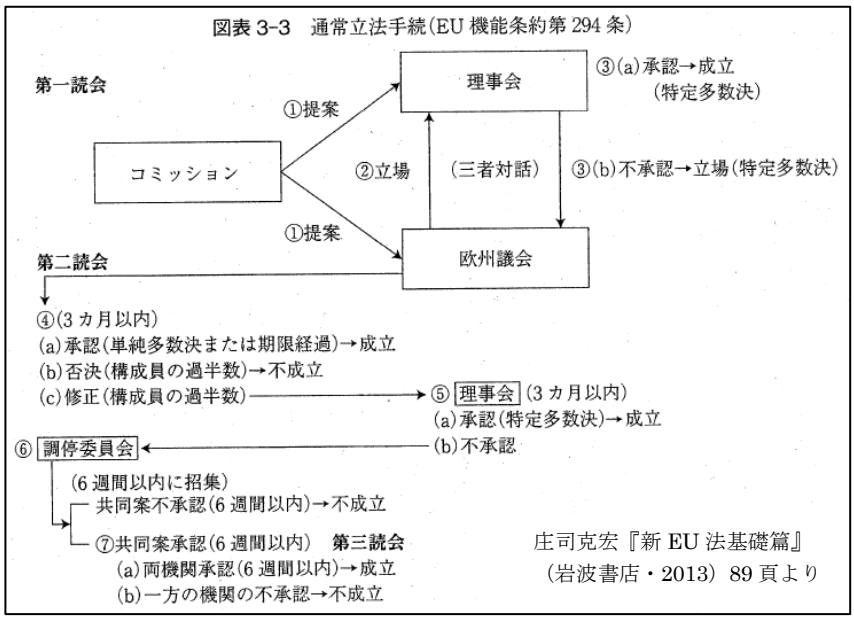
[9] Viviane Reding, *Speech: Making the EU Data Protection Reform Irreversible*, 11 March 2014.

[10] 市民的自由・司法・内務委員会が 3,133、産業委員会が 417、域内市場委員会が 226、雇用委員会が 27、法務委員会が 196 それぞれ修正案を提示し、合計で 3,999 の修正案となっている。*See* European Parliament, *Q &A on EU Data Protection Reform*, 4 March 2014.

[11] Albrecht 議員の政策秘書 Ralf Bendrath 氏によれば、2014 年中に Albrecht 議員が”Finger weg von unseren Daten!”を出版し、英語版にも翻訳される予定である。

[12] Jan Philipp Albrecht, *Uniform Protection by the EU: The EU Data Protection Regulation Salvages Informational Self-Determination*, in DATA PROTECTION ANNO 2014: HOW TO RESTORE TRUST? 125 (Hielke Hijmans & Herke Kranenborg eds., 2014). なお、ドイツのデータ保護機関は規則提案の強力な支持者であるのに対し、ドイツ政府が反対の表明を示しているのは、規則提案が公表される直前に、ドイツ憲法裁判所の裁判官

いずれにしても、理事会における審議には依然として時間を要するため、2014 年中の規則提案と指令提案の採択の見込みはなくなった。EU 関係者のヒアリングからは、2015 年の早い段階で三者対話に持ち込まれる、というのが現実的なシナリオとなっている。



また、EU データ保護改革をめぐっては、加盟国の首脳からも様々な思惑があると言われる。たとえば、2013 年 10 月 24 日から 25 日にかけて開催された欧州理事会では、イギリスのキャメロン首相がデータ保護改革の採択期限を 2015 年とすること自体に反対していたが、フランス、イタリア、ポーランドの意向により 2015 年までの採択という形に妥協されたと言われる[13]。さらに、2013 年 6 月に明らかになった米国 NSA による大量の個人情報の収集問題によって、EU 市民の個人データを保護するためデータ保護改革の必要性にも迫られてきた[14]。さらに、議会で 3999 もの修正案の背景には米国の IT 企業が中心となるロビー活動が盛んであったことも指摘しておく必要がある[15]。

が、ドイツ憲法で保障されてきたデータ保護の枠組みが失われることの悲嘆を論文で公表したことで、規則提案の正統性がドイツ国内で揺らいだ、と Albrecht 議員は指摘する。

[13] *See Victory for Tech Giants on EU Data Laws*, FT TIMES ONLINE, October 25, 2013 7:57 pm. Available at http://www.ft.com/intl/cms/s/0/5ad18e46-3d8c-11e3-9928-00144feab7de.html#axzz317dsq7yb (last visited 27 March 2014).

[14] *See e.g., EU demands legal redress from US in fallout from Snowden leaks: Data-sharing deals at risk as Europe drafts new rules,* THE GUARDIAN, 27 November 2013 at 18; *As It Denounces U.S. Spying, Europe Delays Privacy Protection at Home*, N.Y. TIMES, 30 October 2013 at A4.

[15] *See e.g., Data protection in the EU: the certainty of uncertainty*, THE GUARDIAN ONLINE, 5 June 2013. Available at

このように、データ保護改革は、様々な利害関係の中、政治的なアジェンダの中で審議・交渉が進められてきた。

以下、EU データ保護改革の重要な論点である①個人情報の範囲、②適用範囲、③データ主体の権利、④事業者の義務、⑤越境データ移転、⑥監督機関についてそれぞれ解説する。

---

http://www.theguardian.com/technology/blog/2013/jun/05/data-protection-eu-anonymous (last visited 27 March 2014).

Ⅰ．個人情報の範囲

１．個人データについて

（１）EU データ保護指令

・個人データとは、識別された又は識別することができる自然人に関するすべての情報を意味する。

・識別することができる個人とは、特に個人識別番号、又は肉体的、生理的、精神的、経済的、文化的若しくは社会的アイデンティティに特有な 1 つ又は 2 つ以上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することができる者をいう

（２）EU データ保護規則提案

委員会	・データ主体に関するすべての情報（第 4 条 2 号)。 ・遺伝データとは、出生前の遺伝継承又は取得された個人の特徴に関するあらゆる類型のデータを意味する（第 4 条 10 号)。 ・生体データとは、顔の画像や指紋認証等の特別の識別を可能とする身体的、生理的、又は行動の特徴に関するすべてのデータを意味する（第 4 条 11 号)。 ・健康に関するデータとは、個人の身体的もしくは精神的な健康、又は健康サービスに関するすべての情報を意味する（第 4 条 12 号)。
議会	・識別された又は識別することができる自然人に関するすべての情報を意味し、識別することができる個人とは、特に氏名、識別番号、位置データ、特有の識別子、又は肉体的、生理的、遺伝的、精神的、経済的、文化的若しくは社会的アイデンティティに特有若しくは性別の1 つ又は2 つ以上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することができる者をいう（第 4 条 2 号)。 ・追加情報の利用なしに特定のデータ主体に属しない個人データとしての仮名化データ（第 4 条 2a 号） ・アクセス権限がないいかなる者にも解読できない技術保護措置を通じた個人データとしての暗号化データが追加された（第 4 条 2b 号)。 ・一定の個人の性質を評価又は個人職務能力、経済状況、位置、健康、選好・信頼性・行為を分析若しくは予測することを目的とした自動処理の形態としてのプロファイリングが追加された（第 4 条 3a 号)。
理事会	・識別された又は識別することができる自然人に関するすべての情報を意味し、識別することができる個人とは、特に氏名、識別番号、位置データ、特有の識

	別子、又は肉体的、生理的、遺伝的、精神的、経済的、文化的若しくは社会的アイデンティティに特有若しくは性別の1 つ又は2 つ以上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することができる者をいう、という定義が検討されている（第 4 条 2 号）。 ・仮名化データの追加について検討されている（第 4 条 2a 号）。 ・遺伝データについて、生物学的なサンプルの分析から生じた、という文言の追加が検討されている（第 4 条 10 号）。 ・プロファイリングの定義の追加が検討されている（第 4 条 12a 号）。

（3）個人データの判断基準

第 29 条作業部会は、個人データの概念に関する意見[16]を公表しており、委員会のヒアリングによれば、EU データ保護規則提案において示された個人データの概念についてもこの意見を基にしている。EU 関係者からのヒアリングにおいても、匿名化に絶対的な基準はなく、個人データは日々変化するものであり、個人データの概念は広くとられていることを前提とすべきであるとの指摘があった。また、議会では、新たにプロファイリングの条項が設けられ、仮に識別（identify）できなくても single out できれば、データ保護の義務規定がかかることに注意を要するとの見解が示された。いずれにせよ、目的に掲げられた個人データの権利及び自由の保護という観点を踏まえ検討することが重要である。

また、2014 年 3 月 21 日に開催された OECD プライバシー専門家ラウンドテーブルにおいて、個人情報の範囲や類型論それ自体は実務において意味をなさないという EU 関係者のみならず米国の実務家からも指摘があった。もっとも、リスク分析の観点から個人情報の識別性概念等を有機的に議論することの有用性はあるという指摘もあった[17]。

EU データ指令（第 2 条）における「個人データとは、識別された又は識別することができる自然人に関するすべての情報を意味する。識別することができる個人とは、特に個人識別番号、又は肉体的、生理的、精神的、経済的、文化的若しくは社会的アイデンティティに特有な 1 つ又は 2 つ以上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することができる者をいう」。以下では、①「すべての情報」、②「に関する」、③「識別された又は識別することができる」、④「自然人」に分けてそれぞれ解説する。

16 Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, adopted on 20th June, 2007.

17 OECD, *Expert Roundtable Discussion: Protecting Privacy in a Data-Driven Economy: Taking Stock of Current Thinking*, 21 March 2014 (Session Ⅰ Personal Data Taxonomies and Governance). OECD については、本報告書・板倉論文を参照。

①「すべての情報（any information）」

「すべての情報」には情報の性質、内容、及び形態のそれぞれから判断しうる。情報の性質には「客観的な」情報（血液型など）のみならず、意見や評価など「主観的な」情報も含む（たとえば、「Titius は信頼できる借入人である」）。個人データに該当する情報とは、それが真実であり、証明されていることを必要としない。情報の内容の観点からは、個人データの概念には、いかなる種類の情報もデータに含む。すなわち、センシティブ・データは当然それに含まれるが、個人の地位や能力にかかわらず、個人に関する情報を含む。情報の形態には、アルファベット、数字、図、写真、音といったいかなる形態の情報も個人データの概念に含む。

例：医薬品の処方情報

医薬品の処方情報（たとえば、医薬品認証番号、医薬品名、医薬品含量、製造者、価格、再調剤、使用の理由、代用できない利用、処方者の氏名、電話番号等）は、たとえ患者が匿名化されていたとしても、個別処方薬の形態であろうと複数の処方薬から識別されたパターンの形態であろうと、その薬を処方する患者に関する個人データとみなしうる。したがって、識別された、または識別されうる医者によって記載された処方箋に関する情報を医薬品の製造者に提供することは、EU 指令における個人データの第三者提供に当たる。

例：テレフォン・バンキング

テレフォン・バンキングにおいて、銀行の指示に対する顧客の音声がテープに録音されれば、これらの録音された音声は個人データとしてみなされるべきである。

例：ビデオ監視

ビデオ監視システムによって撮影された個人の映像は個人が認識しうる限りにおいて個人データとなりうる。

例：子どもが描いた絵

親権に関する裁判手続において、少女への神経精神医学のテストの結果、彼女の家族を表した絵が提出された。その絵は、彼女の心情と彼女の家族の個々の構成員に対する心理に関する情報が示されていた。この場合、絵それ自体が個人データであるとみなされうる。その絵が実際に児童に関する情報を明らかにしており、たとえば、父親や母親の態度に関する情報が現されている。その結果、両親はこの子供が描いた絵という情報へのアクセス

権利を行使できる。

②「に関する（relating to）」

情報が特定の個人について（about）のものであるとき、その情報は個人「に関する」とみなされうる。個人「に関する」データであると考えられるためには、「内容」の要素、「目的」の要素、「結果」の要素が必要である。これらの 3 つはいずれか 1 つが条件となる。

―「内容」（contents）：個人に関する情報があらゆる状況に照らして評価されなければならないこと

―「目的」（purpose）：データが個人の地位や行動を評価したり、一定のかたちで扱ったり、影響を及ぼす目的を持って利用されること

―「結果」（result）：個人に関するデータを利用することで特定の人の権利及び利益に対する効果（impact）を有すること

例　家の価値

特定の家の価値は物についての情報である。この情報が特定の地域における不動産価格の水準を示すだけであれば、データ保護の規定が必ずしも適用されるわけではない。しかし、一定の場合にこのような情報も個人データとしてみなすこととなる。現実に、家は所有者の資産であり、たとえば一定の税金を支払う義務の範囲を決定するために利用される場合で、このような情報が個人データとしてみなさることに異論はない。

例　自動車サービス記録

自動車のサービス登録は、整備士が保有する自動車、走行距離、検査日、技術的問題、その他の状況に関する情報が含まれる。この情報はプレート番号やエンジン番号の記録と連結することができ、所有者と関連付けることができる。料金支払いの目的で整備士が自動車と所有者の関連性を作り上げれば、情報は所有者または運転者「に関する」ものとなる。

例　電話の通話記録（call log）

会社内部の通話記録は特定の通信に接続された電話から生じた通話に関する情報が提供された場合、この情報は異なる主体との関係を明るみに出すこととなりうる。会社がその通話の支払い義務を負い、電話機は勤務中の特定の労働者の支配に置かれ、通話はその労働者によって行われるものとされている。この場合でも、すべての発信・受信の通話に労働者の私生活、社会的関係、および通信に関する情報が含まれる限りにおいて、個人デー

タの概念がこれらの通信のいずれにも及ぶものといわなければならない。

例　タクシーの位置情報の監視

タクシー会社によって確立した衛星位置情報の体制によって、リアルタイムで利用できるタクシーの位置を決定することが可能となった。位置情報の処理の目的は、顧客の最も近い位置にいるタクシーを割り当てることで、よいサービス提供とガソリンの節約にあった。厳密に言えば、この制度に必要なのは運転手についてのものではなく、自動車に関するデータである。しかし、この制度はタクシー運転手の仕事を評価するものではないが、仕事を監視し、スピード制限を遵守しているか、適切な道のりを選んでいるかどうかなどチェックすることができる。それゆえ、この制度はこれらの個人に関する重大な効果をもたらし、そのようなデータは自然人に関するものとみなされる。この位置情報の処理はデータ保護規則に服することとなる。

③「識別された又は識別することができる（an identified or identifiable）」

自然人が集団の他の構成員と「区別される」（distinguished）ことで、その者は「識別された」（identified）とみなしうる。そのため、自然人が識識別することが可能でありさえすれば、その者が「識別されうる」こととなる。

識別は、通常、「識別されうる個人」の一定の情報、また特定の個人から特別の許可を与えられた者や特別の関係を有する者が保持する情報を通じて行われる。具体例としては、身長、髪の色、衣服等のただちに判別されないような人の外見がある。

EU 指令における「識別されうる個人」（identifier）とは、「特に個人識別番号、又は肉体的、生理的、精神的、経済的、文化的若しくは社会的アイデンティティに特有な 1 つ又は 2 つ以上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うる者という」。

・直接的または間接的に識別される方法について

直接的：氏名による識別

識別を確認するためには、氏名は、その者と同名人物との間の混乱を回避するため、他の情報（生年月日、患者の氏名、住所、顔写真）と結合されなければならない。Titius が借り入れた金額の合計の情報は氏名と結合することで識別された個人に関するとみなされうる。氏名は、他者を区別するための文字と音の組み合わせ情報を用いることで特定の個人を明らかにしている。また、氏名は、その者がどこに居住し、どこで見つかり、家族と多くの法的社会的関係におけるその者についての情報を与える。画像がその氏名と結合することでその者の外見を知ることさえできる。

間接的：電話番号、自動車登録番号、社会保障番号、パスポート番号、（年齢、職業、居所等）その者が属している集団を狭めていくことで識別しうる重要な属性の結合

「黒いスーツを着ている男性」といった副次的情報であっても、信号機で待っている通行人の中から識別することができる。そのため、問題は情報が関係している個人が識別されうるかどうかであって、特定の事案における状況に依拠しているのではない。

間接的な識別の類型は、小さなものであれ、大きなものであれ、「特有の結合」という現象に関係している。そのため、氏名を通じた識別は実際に多くの場合行われるが、氏名それ自体はすべての事案において個人を識別するために必要であるわけではない。

ウェブの閲覧監視（web traffic surveillance）ツールによって、ユーザーのウェブ上での行動も識別しやすくなった。ウェブ上での各人の決定に関する情報が集められてきた。このようなウェブ閲覧監視ツールは、個人の氏名や住所について尋ねることなく、この人物を社会経済的、心理的、哲学的あるいは他の基準に基づいて類型化することができるし、その人物の決定であるとすることができる。言い換えれば、個人を識別する可能性は、必ずしもその者の氏名を見つけ出す唯一の基準を意味するものではない。

欧州司法裁判所の判決[18]によれば、「インターネットのページにおいて、様々な人物を参照し、氏名や他の手段によって、たとえば労働条件や趣味に関するその者の電話番号や電話情報を与えることで、その者を識別することは、EU 指令が意味する個人データの処理を構成する」。

・識別方法について

指令前文 26 項は「識別できる」という用語に特に注意している。すなわち、「ある者が識別されうる根拠かどうかを決定するには、データ管理者または当該人物を識別するための他の人によって用いられるあらゆる可能な合理的手段（all the means likely reasonably to be）が採られるべきである」。

「データ管理者または当該人物を識別するための他の人によるあらゆる可能な合理的手段」という基準は、特に関係するすべての要因を考慮すべきである。識別を行うコストはひとつの要因であったとしても、唯一のものではない。意図された目的、処理が行われる方法、管理者による利点、個人の利益のみならず、組織的な機能障害のリスク（たとえば信頼義務違反）、技術的不可能性がすべて考慮に入れられるべきである。他方で、このテストは動

[18] CJEU, *Bodil Lindqvist*, C-101/01, 6 November 2003.

態的であり、処理されたときの技術の現状やデータが処理される機関の発達可能性を考慮すべきである。今日用いられたあらゆる可能な合理的手段で今日識別することはできない。もしもデータが1か月間のみ蓄積される予定であるなら、識別が情報の存在期間に可能であるとは予定されておらず、個人データとしてみなされるべきではない。しかし、10 年間の保存期間であれば、管理者は情報の 9 年目において生じる識別の可能性を考慮すべきである。この制度はこの後生じる発展に適応されていくべきであり、適切な技術的組織的措置を導入すべきである。

例　患者の名（ファースト・ネーム）とX線番号

女性の X 線番号が彼女のファースト・ネームとともに科学誌に公表された。その人物のファースト・ネームが、親族や知人が彼女が特定の病気にかかっていることを知っている事実と結合されれば、多数の者に対しその者を識別しうることとなり、X線番号が個人データとなりうる。

例　製薬研究のデータ

病院や個人医師患者の医療記録のデータを次の場合に医学研究の会社に移転する。患者の氏名は用いられていないが、異なる患者情報との間違いを避けるため、個々の臨床につきラムダムに番号が使われている。また、患者の氏名は守秘義務を課された個々の医者のみが所持しているおり、データには突合により患者の識別を可能とする追加情報が含まれていない。さらに、データ主体から識別された又は識別されうることが防止するためのその他すべての措置が講じられている。この状況下であれば、データ保護機関は、製薬会社によって行われる処理においてデータ主体を識別するために用いられるいかなる可能な合理的手段も存在していないとみなされる。

「用いられるあらゆる可能な合理的手段」を評価する関連要因は、データ処理におけるデータ管理者によって追求される目的（purpose）であり、次のような例が挙げられる。なお、データ主体の識別が処理の目的に含まれていない場合、識別をできない技術的な措置が非常に重要になってくる。この措置の法的義務は、結果ではなく、条件である。

例　ビデオ監視

ビデオ監視の文脈において特に関係してくる。データ管理者は収集された映像のごくわずかしか識別ができず、識別が行われる前に個人データは処理されていない。しかし、ビデオ監視の目的として、識別がデータ管理者によって必要である事案においてビデオの映

像に映った人を識別することは、たとえ現実に識別できない人が含まれていても、識別されうる個人についてデータを処理するものとして理解される。

例　可変的な（dynamic）IP アドレス＊[19]

第 29 条作業部会によれば､IP アドレスは識別されうる個人に関するデータであると考えられている。特にコンピュータの利用者を識別する目的で行われる IP アドレスを処理する場合（たとえば、著作者が知的財産権違反のコンピュータ利用者を告訴する目的)、裁判所に訴えるなどを通じて、管理者は特定の人物を識別するために「用いる合理的と思われる手段」が利用されること想定しており、それゆえその情報は個人データとしてみなされなければならない。

また、利用者の識別が要求されないインターネットカフェにおける個々のコンピュータに帰属する IP アドレスは、利用者の識別ができない。すなわち、コンピュータ X の利用中に収集されたデータが合理的な方法をもってしても利用者の識別ができず、したがって、個人データに該当しない。他方で、インターネット・サービス・プロバイダーは、問題となる IP アドレスが識別できるかどうかが分かることから、データが識別できない利用者であることを絶対的な確信をもって見分けることができない限り、安全な形ですべての IP 情報は個人データとして扱わなければならない。

例　落書きによる損害

自動車会社が経営する自動車が落書きによって繰り返し損害を受けた。損害の算定と加害者に対する法的主張を行うことを容易にするため、会社は損害の状況と落書きされた箇所やその画像、自動車のナンバープレート、落書きした者のサインを記録しておいた。記録の時点では誰が落書きしたかは分からないし、決して知ることができないかもしれない。しかし、いつか個人を識別することができる手段がある「合理的で可能な」ものとしてデータ管理者は期待しているのであれば、この処理は意味をなす。そのため、この画像に含まれる情報は「識別しうる」個人に関するものとしてみなすべきであり、記録された情報は「個人データ」としてみなされるべきである。

④「自然人（natural person)」

EU 指令の規則によって与えられた保護は自然人、すなわち人間（human beings）に適

[19] IP アドレスが EU データ保護指令における「個人データ」に該当するという意見は Article 29 Data Protection Working Party, *Privacy on the Internet - An integrated EU Approach to On-Line Data Protection*, adopted on 21 November 2000 においてすでに示されている。

用される。その意味で個人データの保護の権利は、特定の国における国籍や居所に制限されない普遍的なものである。EU 指令の前文２項は「データ処理の仕組みは人の用に供する」ことから、その仕組みは「自然人のいかなる国籍または居住地であっても、基本的な権利と自由を尊重しなければならない」と述べ、この点を明らかにしている。

このように個人データは、原則として、識別されたまたは識別されうる生存する個人（living individuals）に関するデータである。

そこで、死者に関する情報は、民事法上もはや自然人ではないことから、原則として EU 指令における個人データの主体としてみなすことはできない。しかし、死者のデータはいまだに間接的に特定の場合において一定の保護を受けることがある。

①データ管理者は、データに関係するある人が生存しているか、死亡しているか必ずしも確かめることができない。仮に特定ができたとしても、データ管理者は区別なく生存する個人と同じ仕組みで情報を処理している。データ管理者は死者のデータを処理する場合にも、生存する個人と死者とを区別するよりも、データ保護規則の義務に課されると同様に処理するほうがおそらく容易であろう。

②たとえば、血友病にかかり死亡した Gaia の情報は、X 染色体に含まれる遺伝子と関連しているため、彼の息子である Titius が同じ病気にかかる可能性が示される。このように死者に関するデータが生存する個人にも同時に関係することがあり、EU 指令における個人データになることから、死者の個人データも間接的にデータ保護規則の保護が及ぶこととなる。

③死者の情報は、データ保護法以外の規則によって格別の保護に服する可能性がある。医療関係者の秘密保持義務は患者の死亡とともに終わるわけではない。肖像や名誉に関する権利の国内法は死者の記憶の保護を認めるものとなる。

④加盟国が国内立法の範囲を拡張するのになんら妨げはないため、正当な利益がある場合、死者のデータ処理の国内データ保護法の規定を拡大することは可能である。

なお、欧州司法裁判所の判決により、法人であっても EU 基本権憲章の私生活の保護とデータ保護の権利が及ぶと解されている[20]。

（３）仮名化データ（pseudonymised data）等

仮名化されたデータとはアイデンティティを偽る過程を経たデータである。その目的は本人のアイデンティティを知ることなく同一人物に関する追加のデータを収集することである。これは研究や統計の文脈において特に関係してくる。

---

[20] *Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen*, 9 November 2010, C-92/09 & C-93/09.

さかのぼって追跡可能な仮名化されたデータは間接的に識別することができる個人に関する情報とみなしうる。そのため、議会により新たに追加された仮名化データは個人識別データの一つである、というのが委員会の解釈である[21]。

このほかに、第 29 条作業部会の意見では、符号化データと匿名化データがそれぞれ開設されている。符号化データ（key-coded data）は、匿名化の古典的な例である。情報は符号により記号化されている個人に関係しているが、その符号と識別されうる個人の一致をさせる鍵は別々に保管されなければならない。この種のデータは医療に関する臨床実験で広く用いられている。

これに対し、匿名化データ（anonymous data）とは、データ管理者または他のいかなる者によって用いられるあらゆる可能な合理的手段を考慮して、データ管理者からも他のいかなる者からもその者が識別することができない自然人に関するすべての情報として定義される。前文 26 項によれば、「データ主体がもはや識別できない方法で匿名化されたデータに保護の原則は適用されない」と解されている。前文 26 項に示されているように、識別に用いられるあらゆる可能な合理的手段の程度を特に参照してケース・バイ・ケースで行われるべきである。なお、欧州データ保護監督機関におけるヒアリングによれば、2014 年 2 月の第 29 条作業部会技術作業グループにおいて匿名化技術の利用に関する意見草案の審議が行われた。このグループで技術者が検討してきた結果によれば、匿名化に単一の基準はなく、ケース・バイ・ケースによる判断が必要であり、また完全な匿名化というのは存在しない、とのことである。

例　統計のための集計化されていないデータ[22]

国の統計機関によって個人情報が処理される場合、一定の段階では、情報は集計化されない形態で、特定の個人と関係して保存されるが、名前の変わりに符号（たとえば、X1234 と符号化された個人が週 3 日以上ワインを飲んでいる）を用いている。この機関はこれらの符号と解読の鍵は別々に保管している。しかし、この鍵は、統計機関によって「用いられる可能な合理的」なものとみなされうるため、それゆえ一連の個人に関する情報は個人データとしてみなされうる。

---

[21] Viviane Reding, Speech: *EU Data Protection Rules: Better for Business, Better for Citizens*, 26 March 2013.

[22] ドイツの国勢調査判決において、保有している個人情報を知らないでいることが人格の発展を妨げ、ひいては自己決定権を基盤とした民主的な秩序に対する重大な危機であるとして「情報自己決定」権が認められた。本判決の紹介として、鈴木庸夫・藤原静雄「西ドイツ連邦憲法裁判所の国勢調査判決（上）（下）」ジュリスト 817 号 64 頁、818 号 76 頁（1994）参照。

例　統計調査と部分情報の結合

データ保護規則の尊重義務とは別に、統計調査の匿名化を確保するため、統計調査官は職務上の特別の守秘義務が課せられ、匿名化されていないデータを公表することが禁じられている。これにより、識別可能な個人に帰属できない集計統計データを公表する義務がある。どれほど大量であっても、人のある類型において一定の基準から識別が可能となるような場合（たとえば、6000 人の住民の町に医者が一人しかいない)、この「差別化された」基準は用いられるべきではなく、あるいは一定の者に関する結果を「薄める」基準が追加されなければならない。

・オーストリアにおける仮名化データの利用について[23]

Albrecht 議員からのヒアリングによれば、規則提案に仮名化を新たに導入した背景にはオーストリアにおける間接的個人データの概念と仮名化データの利用があり、オーストリアの法制度を参考にしたそうである。

オーストリアのデータ保護法第 4 条 1 項では「間接的個人データ（indirectly personal data)」という概念があり、通常の個人データとは区別された類型がある。この「間接的個人データ」は、データ管理者からは識別ができるものの、仮名化措置等を施すことによって、受領者側から識別ができないデータを意味する。たとえば、病院において特定の個人を識別することができるデータであっても暗号を破ることができない（unbreakable）仮名化措置を施し、研究機関に仮名化データを提供する場合が、「間接的個人データ」の提供であり、この場合データ移転の規制に服しないこととなる。この「間接的個人データ」の利用は研究分野において利用されてきており、2000 年に施行されていて以降、オーストリア国内では深刻な違反例は一件もない、とのことである。

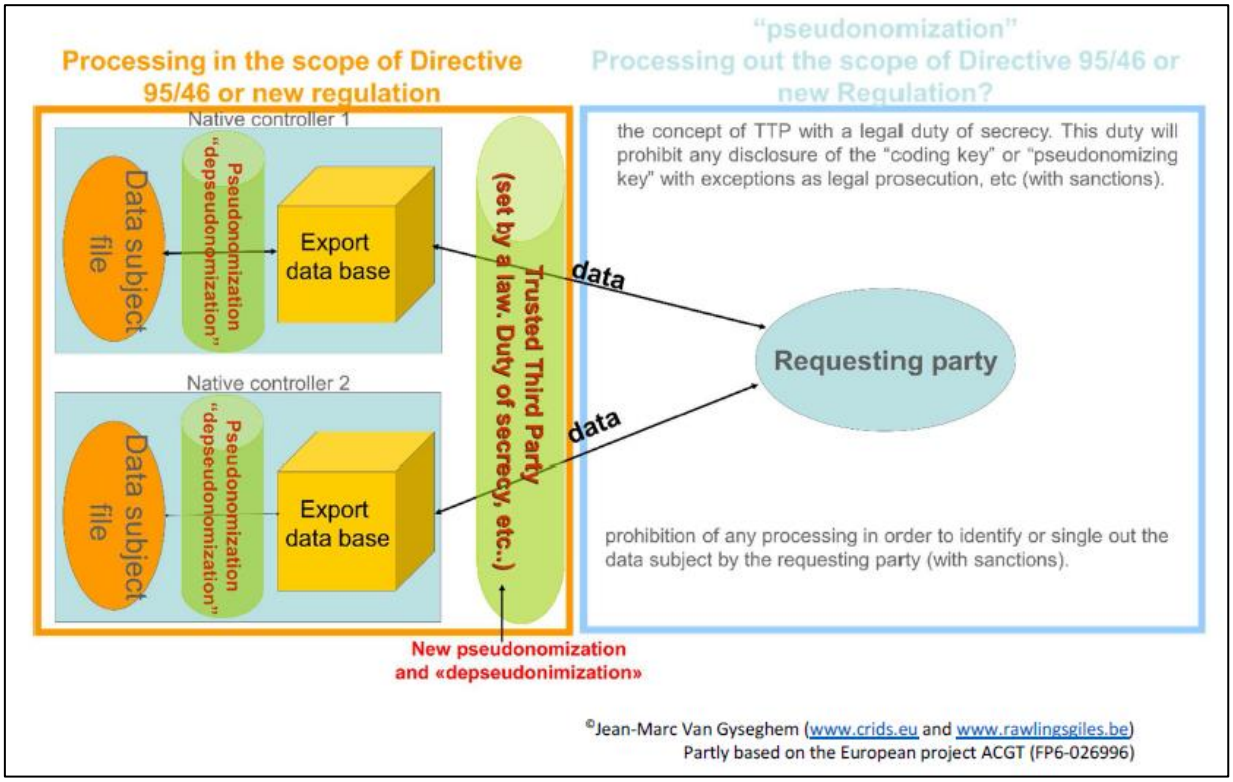
オーストリアの電子政府では電子的に個人を識別できる情報を用いる場合、指定の方法でデータを仮名化して、データ保護監督機関の監視の下、一方通行の暗号法（one-way cryptography）を用い、不可逆的にデータの識別ができない形で仮名化データを利用する。また、異なる省庁で異なる特定の電子識別情報（“sector specific e-identities”）を用いているので、再識別化が困難な状況にある。追加的措置として、仮名化されたデータは蓄積されておらず、その都度電子的に仮名化データが作られ、利用されている。民間分野では銀行においても一部仮名化データの利用例が見られる。

---

[23] オーストリア・元プライバシー・コミッショナーWaltraut Kotschy 博士の御厚意により、オーストリア電子政府における仮名化データの利用に関する資料等をいただいた。

・ベルギーにおける仮名化データの利用計画について[24]

ベルギーでは特に電子医療の分野において仮名化の需要が高く、その具体的利用方法について不可逆的に識別できないよう措置を施す第三者機関（Trusted Third Party）の設置が検討されてきた。各病院が保有するデータベースから医療分野の守秘義務が課せられた第三者機関が仮名化・暗号化措置を施し、仮名化・暗号化されたデータを研究機関等に対し不可逆的に識別することができないような形で提供する、という仕組みである。提供を受けた研究機関等においても再識別化が禁止される。この第三者機関はデータの性質や規模等にかんがみて、再識別化のリスク等の判断も併せて行うこととされ、設置には法的根拠を置く予定である。



（4）遺伝データ・生体データ・健康に関するデータ

規則提案には新たに遺伝データ、生体データ、健康に関するデータが定義に追加された。委員会におけるヒアリングによれば、これらのデータは特に取扱いに注意を要するデータの類型として列挙したものである。これらは EU 市民の統計結果を反映しているものと考えられる。たとえば、遺伝データは 88%の EU 市民が健康、性生活、民族出自等に関する

[24] ナミュール大学法・情報・社会研究所 Jean-Marc Van Gyseghem 研究員の御厚意により、ベルギーにおいて仮名化データ利用計画に関する資料等をいただいた。

データと同様にセンシティブであると回答している[25]。

生体データは、生物測定学上の財産、生理的特徴、生存している形跡または反復活動として定義される。大きく分けて 2 つの類型があり、指紋、光彩、網膜、顔認証、手相、声紋認証、静脈、DNA 配列等により身体的特徴に基づく技術と、署名、キーストローク、歩調等の行動的特徴に基づく技術がある[26]。特に DNA 配列は健康に関するデータ又は人種・民族の出自に関するデータとしてセンシティブ・データであるとみなされている。第 29 条作業部会は生体データの処理については、特に利用目的、利用目的に必要な限りでの比例原則、データの正確性、収集の最小限化、データ利用期間の限定、データ処理の法的根拠（同意の取得等）という点に留意が必要であることを示している[27]。また、新たな生体データの処理に際してはデータ保護監督機関への事前認可を受けることが奨励されている。さらに、プライバシー強化技術の利用による、データ保護に優しい方法で生体データ・システムの設計も推奨されている。

センシティブ・データとみなされる健康に関するデータについては、第 29 条作業部会が次の諸原則を遵守するよう電子医療を実施する医療機関等に呼びかけている[28]。すなわち、①患者の自己決定の尊重、②患者及び医療専門家の正確な認証、③電子医療記録へのアクセス、④電子医療記録の他の目的利用の原則禁止、⑤電子医療記録システムの組織的構造（分散型・集中型）、⑥蓄積されたデータの類型、⑦医療記録の国際移転（匿名化・仮名化の措置の必要性）、⑧プライバシー強化技術を用いた安全管理措置、⑨透明性、⑩責任の所在、⑪効果的なコントロールの構造（紛争解決・監査等）である。

２．センシティブ・データ

（１）EU データ保護指令

・加盟国は、人種又は民族、政治的見解、宗教的又は思想的信条、労働組合への加入を明らかにする個人データの処理、及び健康又は性生活に関するデータの処理を禁止なければならない（第 8 条 1 項）。

---

[25] European Commission, *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*, June 2011 at 148

[26] Article 29 Data Protection Working Party, *Working Document on Biometrics*, (WP80) adopted on 1 August 2003 at 3.

[27] Article 29 Data Protection Working Party, *Opinion on Developments in Biometric Technologies*, (WP193) 27 April 2012.

[28] Article 29 Data Protection Working Party, *Working Document on the Processing of Personal Data relating to Health in Electronic Health Records (EHR)*, (WP131), adopted on 15 February 2007.

・ただし、次に掲げる場合はこの限りではない。

a) 明示の同意が与えられた場合

b) 雇用分野での管理者の義務の履行及び特定の権利行使の目的に必要な場合

c) 同意を与えることができず、データ主体又はその他の者の重大な利益保護に必要な場合

d) 政治、思想、宗教又は労働組合を目的とした組織における正当な活動に必要な場合

e) 明白に公にされたデータの処理をする場合、又は法的請求の確定、行使、防御のために必要な場合

（2）EU データ保護規則提案

委員会	・人種・民族の出自、政治的見解、宗教、信仰、労働組合員、遺伝データ、健康、性生活、前科又は関連する安全措置に関するデータの処理は禁止する（第 9 条 1 項)。 ・ただし、次の場合はデータの処理の規定が適用されない。 a) データ主体の同意がある場合 b) 雇用分野での管理者の義務の履行及び特定の権利行使の目的に必要な場合 c) 同意を与えることができず、データ主体又はその他の者の重大な利益保護に必要な場合 d) 政治、思想、宗教又は労働組合を目的とした組織における正当な活動に必要な場合 e) 明白に公にされたデータの処理をする場合 f) 法的請求の確定、行使、防御のために必要な場合 g) EU 法に基づく公的利益のための職務遂行に必要な場合 h) 健康目的で必要な条件と安全措置がある場合 i) 歴史的・統計的・科学的研究に必要な場合 j) 公的機関による監督があり、EU 法又は加盟国法による十分な措置がある前科又は安全措置の処理をする場合（第 9 条 2 項)。
議会	・データ処理が禁止される類型について、性的志向、性アイデンティティ、行政罰、判決、被疑事実が新たに追加された（第 9 条 1 項)。 ・データ処理の禁止の例外として、契約締結に必要な場合（1aa 号)、アーカイブス・サービスに必要な場合（1ia 号）が新たに追加された。
理事会	・データ処理が禁止される類型について、哲学的信仰という文言の追加が検討

	されている（第 9 条 1 項）。

（3）センシティブ・データの取扱いについて

指令に比べ、規則提案には、センシティブ・データに遺伝データと前科又は関連する安全措置という項目が追加された。

第 29 条作業部会によれば、センシティブ・データの判断基準については、次の 3 つの方法がある[29]。第 1 に、特定のデータの類型をリストとして列挙し、それを禁止する現在のデータの類型に基づくアプローチである。第 2 に、一定の類型をデータの類型を列挙するが、新たなセンシティブ・データの類型を認めるため、加盟国の文化的法的違いを考慮する経緯に基づくアプローチである。第 3 に、条約第 108 号第 6 条のように、一定のセンシティブ・データの類型の処理を禁止はしないが、追加的安全管理措置を要求する予防原則に基づくアプローチである。指令は、第 1 の現在の特定の類型の禁止を採用している。

Ⅱ．適用範囲

１．法の適用範囲

（1）EU データ保護指令

・全部又は一部が自動的な手段による個人データの処理、及びファイリングシステムの一部、又はファイリングシステムの一部にすることが意図されたの個人データの自動的な手段以外の処理に適用される（第 3 条 1 項）。

・ただし、共同体法の適用範囲外の活動中に行われるもの並びに公の安全、防衛、安全保障又は刑事法の分野における加盟国の活動に関するすべての処理、及び自然人による純粋な個人的又は家庭的な活動には適用されない（第 3 条 2 項）。

（2）EU データ保護規則提案

委員会	・全部又は一部が自動的な手段による個人データの処理、及びファイリングシステムの一部、又はファイリングシステムの一部にすることが意図されたの個人データの自動的な手段以外の処理に適用される（第 2 条 1 項）。 ・ただし、次に掲げる場合には適用されない。

[29] Article 29 Data Protection Working Party, *Advice Paper on Special Categories of Data ("Sensitive Data")*, 20 April 2011.

	a) EU 法の適用外の活動における個人データ処理 b) EU 諸機関による個人データ処理 c) EU 条約第 2 章の活動を実施する加盟国による個人データの処理 d) もっぱら個人的又は家庭的活動のための個人データ処理 e) 犯罪防止、捜査、起訴等のための機関が行う個人データ処理（第 2 条 2 項）。
議会	・例外項目について、EU 諸機関による個人データの処理が削除された（第 2 条 2 項 b 号）
理事会	・例外項目について、EU 諸機関による個人データの処理が削除された（第 2 条 2 項 b 号）

（3）官民共通の包括的適用

指令も規則提案も官民に共通する法規範である。公的部門と民間部門を明確に分ける規定は存在しない。

しかし、ヒアリングによれば、理事会では、公的部門と民間部門における適用がそれぞれ全く同じとならない規定（たとえば、データポータビリティ権）があるとの指摘があった。現在提案されている規則提案についても、官民の領域に共通に各規定が適用されるという前提には留保が必要であるという指摘がある[30]。すなわち、公的部門においては、データ処理について民主的で説明責任を果たすべきあるのに対し、民間部門には行政手続の法理が適用されず、民間企業がデータ処理をする前提に民主的な政治過程の原理があるわけではない。そのため、民間部門においては特にデータ処理に関する改革が必要であり、特に EU 域内の企業によるデータ保護分野の調和と統一性の必要性が指摘される。

もっとも、本来データ保護の権利は公的機関による恣意的な私生活の干渉を排除することが、合衆国憲法の法理において見られるのと同様に、EU 基本権憲章においても前提とされている。欧州司法裁判所の法務官らによれば、民間部門におけるデータ処理が拡大しており、基本的権利保護の水平効果が生じる場合があるが、EU データ保護法も国家の干渉から私的当事者の活動を保護することを主たる目的として基本的人権を保障している[31]。

---

[30] Peter Blume & Christian Wiese Svanberg, *The Proposed Data Protection Regulation: The Illusion of Harmonisation, the Private/ Public sector Divide and the Bureaucratic Apparatus*, in THE CAMBRIDGE YEARBOOK OF EUROPEAN LEGAL STUDIES, volume 15, 2012-13, 27 (Catherine Barnard et. al. eds, 2013).

[31] *See* Juliane Kokott & Chtistoph Sobotta, *The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the ECtHR*, 3 INT'L DATA PRIVACY L., 222, 226 (2013).

（2）EU 刑事データ保護指令提案

欧州委員会は 2012 年 1 月規則提案と共に、刑事データ保護指令提案を公表した。この指令提案は、犯罪の防止、捜査、探知、もしくは起訴又は刑事罰の執行を目的とした機関による個人データ処理に関する個人の保護を目的としている。

２．域外適用

（1）EU データ保護指令

・各加盟国は、この指令に従って採択する国内規定を次に掲げる場合の個人データ処理に適用しなければならない。

(a) 処理が加盟国の域内に設置された管理者の活動に関連して行われる場合。同一の管理者が複数の構成国域内に設置されたときは、当該管理者は、これらの設置のそれぞれが適用される国内法により定められた義務を遵守することを確保するために必要な措置を講じなければならない。

(b) 管理者が加盟国の域内には設置されていないが、国際公法によって当該加盟国の国内法が適用される地域に設置されている場合。

(c) 管理者が共同体の域内に設置されていないが、個人データの処理を目的として当該加盟国の域内に設置された自動又はその他の設備を利用する場合。ただし、共同体の域内を通過する目的のためにのみ当該設備を利用する場合は、この限りではない。（第 4 条 1 項）

・管理者は、第一項（c）に定められた場合において、その加盟国の域内に設置された代理人を指定しなければならない。ただし、管理者自身に対して提起される訴訟は妨げない。

（2）EU データ保護規則提案（下線イタリックが修正案）

委員会	・本規則は、EU 域内を管理者又は処理者が設置された活動状況における個人データの処理に適用される（第 3 条 1 項）。 ・本規則は、連合域内に居住するデータ主体の個人データ処理に対し、連合に設置されていない管理者に適用される。ただし、当該処理活動は次に関係する場合とする。 (a) 連合域内の当該データ主体への商品又はサービスの提供 (b) 当該主体の行動の監視　（第 3 条 2 項） ・本規則は、EU 域内に設置されていないが、国際公法によって当該加盟国の

	国内法が適用される地域に設置されている管理者による個人データの処理に適用される。
議会	・本規則は、*連合域内で処理されていてもいなくても、*連合域内を管理者又は処理者が設置された活動状況における個人データの処理に適用される。（第 3 条 1 項） ・本規則は、連合域内*のに居住する*データ主体の個人データ処理に対し、連合に設置されていない管理者*又は処理者*に適用される。ただし、当該処理活動は次に関係する場合とする。 (a) 連合域内の当該データ主体*への支払いが要求されるかどうかにかかわらず、*当該データ主体への商品又はサービスの提供 (b) 当該主体*の行動*の監視（第 3 条 2 項）
理事会	・本規則は、連合域内に居住するデータ主体の個人データ処理に対し、連合に設置されていない管理者に適用される。ただし、当該処理活動は次に関係する場合とする。 (a) 連合域内の当該データ主体*への支払いが要求されるかどうかにかかわらず、*当該データ主体への商品又はサービスの提供 (b) *当該主体の行動が欧州連合域内で行われている限りにおいて、*当該主体の行動の監視　（第 3 条 2 項）

（3）EU データ保護指令における適用範囲

指令が適用される場合には、①一つ又は複数の加盟国において管理者が設置されている場合（第 4 条 1 項 a 号)、②国際公法によって加盟国の国内法が適用される地域に管理者が設置されている場合（第 4 条 1 項 b 号)、③管理者が共同体の域内に設置されていないが、加盟国内の設備を利用してデータが処理されている場合（第 4 条 1 項 c 号）が規定されている。

以下、それぞれの場合について第 29 条作業部会が示している具体的な事例を基に説明する[32]。それぞれの場合の適用の有無については、場合分けの図を参照。

a）一つ又は複数の加盟国において管理者が設置されている場合

管理者の設置とは「安定的な配置を通じて効果的かつ真の活動実施」（前文 19 項）を意味する。

[32] *See generally* Article 29 Data Protection Working Party, *Opinion 8/2010 on Applicable Law*, adopted on 16 December 2010.

例）インターネット・サービス・プロバイダ

日本に本社のあるインターネット・サービス・プロバイダである管理者が EU 加盟国で様々な活動を行っている場合（ハンガリーではデータセンターでの技術メインテナンス、アイルランドで個人データの処理を実施）

⇒（適用可能性あり）

アイルランドにおける事業活動が EU データ保護法の適用をもたらすことになる。アイルランドとハンガリーの国内法の適用の可能性もある。仮にアイルランドでの事業活動が個人データの処理を伴わなくても、EU 域内における設備の利用をしている場合、適用が及ぶ可能性がある。

（適用可能性なし）

もしも加盟国内の他の事務所での活動が個人データの処理を伴わないユーザーをターゲットとした広告活動のみであれば、EU 法は適用されない。

なお、2013 年 2 月 14 日、ドイツ行政裁判所はアイルランド・ダブリンにある Facebook においてドイツ人向けのデータ処理が行われていると認定し、ドイツのデータ保護法が適用されないとの判断を下した[33]。この問題は、現在規則提案で審議されている「主要拠点（main establishment）」の議論と関連する（one-stop-shop の箇所、参照）。

b) 国際公法によって加盟国の国内法が適用される地域に管理者が設置されている場合

例）外国の大使館

カナダにおける EU 加盟国の大使館は、当該加盟国の国内のデータ保護法が適用され、カナダのデータ保護法は適用されない。また、オランダ域内にあるいかなる国の大使館もオランダのデータ保護法が適用されない。ただし、非政府組織については、この例外が国際的合意などを除き原則として適用されない。

c) 管理者が共同体の域内に設置されていないが、加盟国内の設備を利用してデータが処理されている場合

設備（equipment）とは特定の目的を持って組み立てられたツールまたは装置と定義される。具体的には、クッキー、Java Script、バーナー等の類似のアプリケーションである[34]。

---

[33] Carlo Piltz, *Facebook Ireland Ltd. / Facebook Inc. v Indepdent Data Protection Authority of Schleswig-Holstein, Gemany-Facebook is not subject to German Data Protection Law*, 3 INT'L DATA PRIVACY L. 210 (2013).

[34] *See* Article 29 Data Protection Working Party, *Working Document on Determining the International Application of EU Data Protection Law to Personal Data Processing on the Internet by Non-EU Based Web Sites*, adopted on 30 May 2002 at 9-12.

たとえば、元ドイツ連邦憲法裁判所の裁判官によれば、ドイツでは、ドイツの領土にある設備を利用する限りにおいて、たとえ第三国からの通信傍受であってもドイツ憲法やデータ保護法制が適用されるとのことである[35]。

例）位置情報サービス

ニュージーランドに拠点のある会社が位置情報サービスを提供するため Wi-Fi のアクセスポイントに関する情報を収集するため EU 域内で自動車を利用している。この活動には多くの場合個人データの処理が伴っている。

適用の可能性は二通りある。一つは、道路の巡回をしながら自動車による Wi-Fi 情報の収集が第 4 条 1 項(c)における設備の利用とみなされる。いま一つ個人のモバイルデバイスを利用して個人に位置情報を提供しているため、同じく設備の利用と理解される。いずれの位置情報サービスも指令の規定を遵守しなければならない。

例）クラウドコンピューティング

管理者が誰であるか、またどのレベルでどのような活動が行われているかについて認定が必要となる。

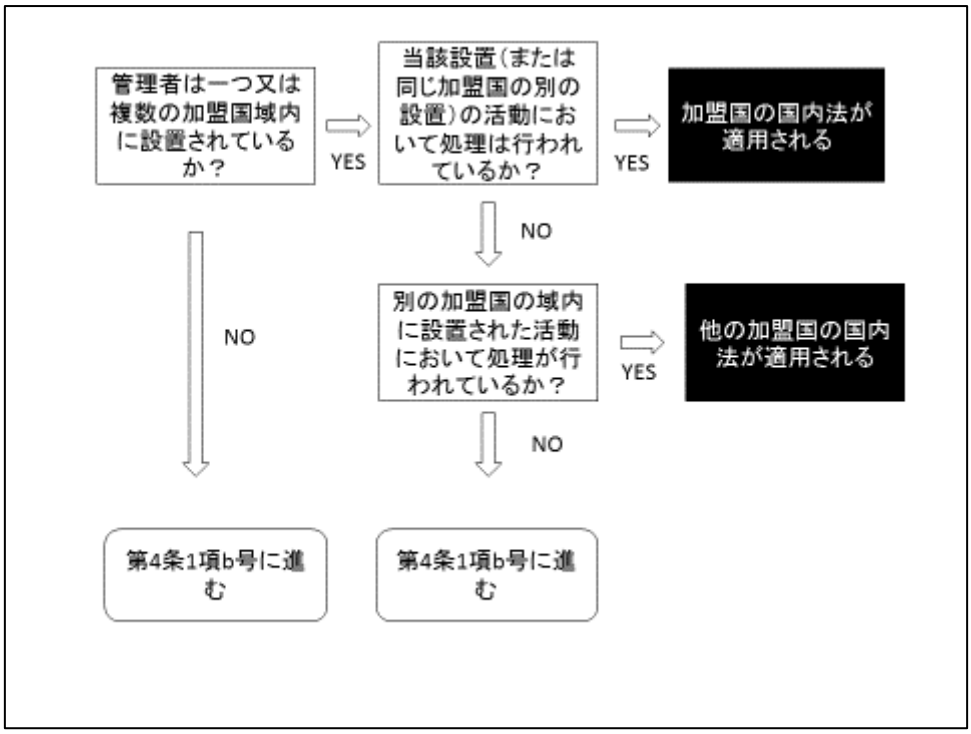
たとえば、クラウドサービスのユーザーである企業がクライアントとの会議のためオンライン上の予定表サービスを通じてデータ処理をすれば、EU 域内で設置された活動においてサービスを利用しているということができる（第 4 条 1 項(a)）。また、クラウドサービスプロバイダ自身も会議の当事者の個人的な面会や連絡先に関する同期サービスなどを提供していれば管理者とみなされる。また、クッキーをインストールするなどの設備の利用をする場合も第 4 条 1 項(c)により指令が適用される。

図

第 4 条 1 項 a 号：一つ又は複数の加盟国において管理者が設置されている場合

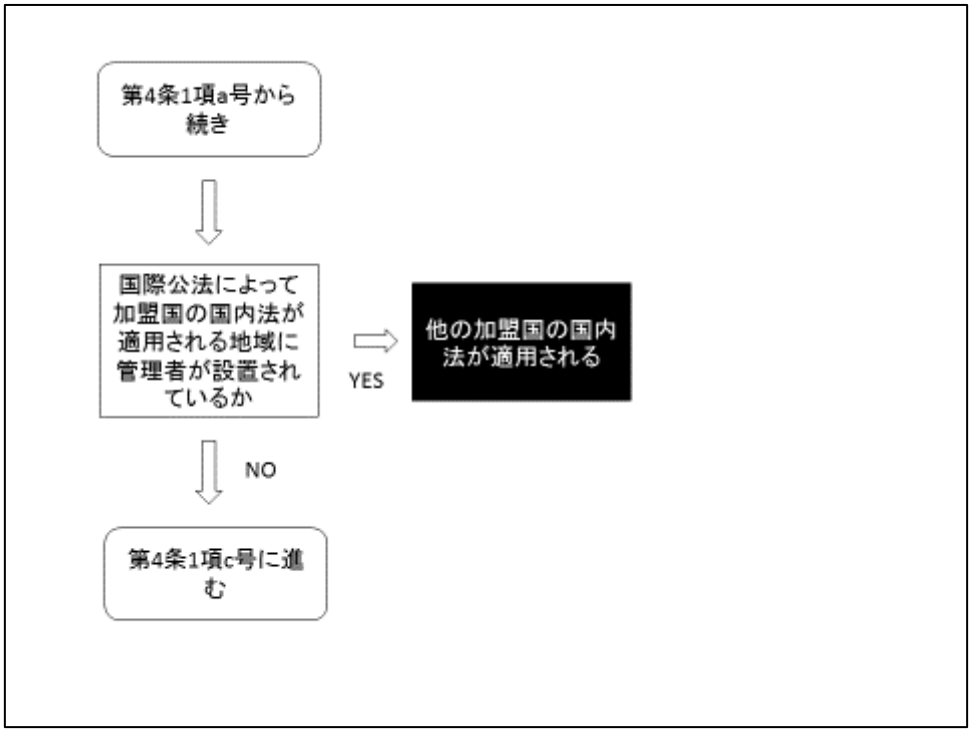
⇒規則提案第 3 条 1 項

[35] Wolfgang Hoffmann-Riem, Remark, Panel Democracy, Surveillance and Intelligence Agencies, 7th International Conference of Computers, Privacy and Data Protection, 24 Janaury 2014.



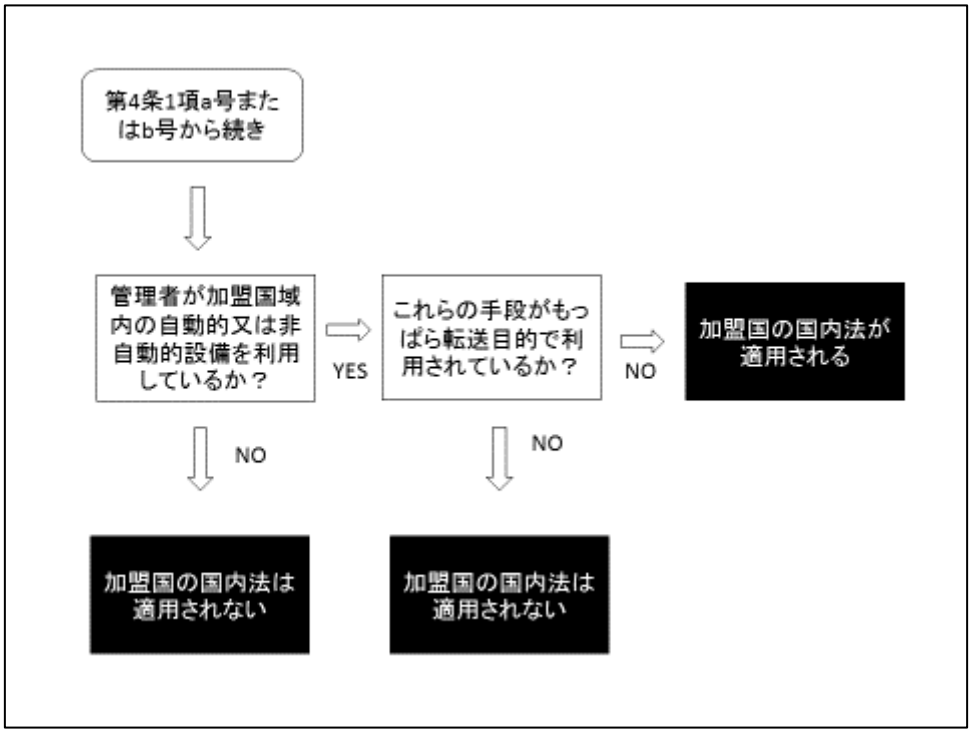
第 4 条 1 項 b 号：国際公法によって加盟国の国内法が適用される地域に管理者が設置されている場合

⇒規則提案 3 条 3 項



第 4 条 1 項 c 号：管理者が共同体の域内に設置されていないが、加盟国内の設備を利用してデータが処理されている場合

⇒規則提案 3 条 2 項



（4）域外適用とデータ保護監督機関の協力

各データ保護監督機関は、どの国の国内法が適用されうるかにかかわらず、加盟国の領域内においては、その権限を行使する資格を有している（第 28 条 6 項）。そこで、域外適用が問題となった場合、各データ保護監督機関はどのような場合に協力義務が発生するかが問題となる。

例）ソーシャル・ネットワーキング・サービス（第三国に本社があり、EU 域内に設置）

第三国に本社を持つソーシャルネットワークのプラットフォーム会社が EU 域内にも設置しており、EU 市民をターゲットに活動している場合、第 4 条 1 項 a 号に該当する。また、一つの設置でデータが処理されている以上、他の加盟国域にある設備の利用の有無は関係してこない。もっとも、各加盟国のデータ保護監督機関は、市民からの要請や苦情への対処のため他の加盟国の機関との協力の義務を負っている。

例）電子医療プラットフォーム

患者のデータの越境処理を促進するプラットフォームについて、たとえばベルギー市民がポルトガルを旅行中に急な治療が必要になった場合、その患者のデータはポルトガルに移転され、ポルトガルのデータ保護法の下でデータ処理されることとなる。その患者がベ

ルギーに戻った場合、ベルギーのデータ保護監督機関にまず苦情を申し出て、ベルギーの機関がポルトガルの機関と協力してポルトガル法に基づき違反があったかどうか調査することになる。

（５）EU データ保護規則提案の動向

欧州委員会の提案には、たとえ管理者が EU 域内に設置されていなくても、当該管理者が① 連合域内の当該データ主体への商品又はサービスの提供、② 当該主体の行動の監視を行っている場合、規則提案が適用されること（いわゆる「域外適用」）[36]を明確にした。これにより、指令第 4 条 1 項 c 号の設備の利用という基準が廃止されたが、新たに設けられた 2 つの基準は指令以上に EU 域外の管理者への適用の範囲が拡大することが予想される[37]。

議会と理事会は委員会の文言に修正案を示しているが、域外適用の枠組み自体は維持している。なお、議会の修正案では、データ処理者にも適用が及ぶとする点で委員会よりも広い適用範囲を想定している。2 つの基準について、それぞれ文言修正の案が示されており、今後、委員会の提案との交渉が行われることとなる。

a) 連合域内のデータ主体への商品又はサービスの提供

商品又はサービスの提供が行われたかどうかについては、支払いがされているかどうかに関わらず、管理者が一つ又は複数の加盟国に居住するデータ主体にサービスの提供を想定していることが明白でなければならない（前文 20 項・議会修正案）。

b) 連合域内のデータ主体の行動の監視を行っている場合

監視とは、個人が追跡され、又は個人に関する自動決定を行い、個人の選好、行動及び態度が分析、予測されることを目的にプロファイルされることを意味する（前文 21 項）。

（６）域外適用をめぐる法的課題

---

36 「域外管轄（extraterritorial jurisdiction）」とは、「国際法に基づく規制がない中国家の利益に影響を及ぼす個人の行為、財産、又は行動を国内の立法、司法又は執行による手段で国境を越える規制しようとする試み」と定義される。*See* International Law Commission of the United Nations, *ILC Report on the Work of its Fifty-Eighth Session, UN Doc A/61/10*, Annex E.

37 Christopher Kuner, *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law, Privacy & Security Law Report*, vol. 11, 1, 3 (2012).

いわゆる EU 法の域外適用については、消費者法[38]や競争法の分野などの指令や欧州司法裁判所の判例においてすでにみられる[39]。なお、域外適用とデータ移転の規制に関する第 4 条と第 25 条・第 26 条の複合的解釈の性格を有することに注意を要する[40]。

・欧州司法裁判所の判例

欧州司法裁判所の判決においても EU 域外に設置された事業者の「活動状況が共同体と密接に結びついている」[41]ことを理由に共同体法が適用されることを明らかにしている。また、欧州司法裁判所の活動の国際的性質に着目し、取引者の「活動を指図する（directing activities）」[42]場合に EU 法が適用される。規則提案における「商品又はサービスの提供」と「行為の監視」という 2 つの要件は「活動を指図する」という判例を具体化したものであると理解されている[43]。

・インターネット検索エンジンに関する法務官による意見（2013 年 6 月 25 日）

インターネット検索エンジンにより、プライバシー侵害を主張するスペインの原告らが提訴した事案において、本判決を前に、欧州司法裁判所の法務官（advocate general）による予備意見では、指令の適用範囲に関する論点について次のとおり示されている[44]。

a）適用範囲：インターネット・サービス・プロバイダの EU 域内の設置について

EU 人権憲章第 8 条（データ保護の権利）については、指令第 4 条 1 項で用いられている概念の解釈を考慮に入れなければならないが、全く新奇な基準であってはならない。プロバイダがどの程度の範囲で、どこで EU 在住のデータ主体の個人データを処理しているかについては不明確なところがあり、第 4 条 1 項の文言はあまり有益ではない。

---

38 Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts - Statement by the Council and the Parliament re Article 6 (1).

39 EU 法の他の領域とデータ保護分野の域外適用に関する論点については、消費者庁『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』17 頁以下（庄司克宏執筆）、参照。

40 Marie-Helene Boulanger & Cécile de Terwangne, *Internet et le Respect de la vie Privée*, 12 Internet face au droit, Collection Cahiers du Centre de Recherches Informatique et Droit, 189, 203 (1997).

41 *Ingmar GB Ltd v Eaton Leonard Technologies Inc.*, C-381/98, 9 November 2000.

42 *Peter Pammer v Reederei Karl Schlüter GmbH & Co KG*, C-585/08; *Hotel Alpenhof GesmbH v. Oliver Heller*, C-144/09, 7 December 2010. 規則提案の文言については、「監視（monitoring）」という管轄ではあまり用いられない文言よりも、本来の判例で用いられてきた「指図する（directing）」という文言を利用した方が適当である、という指摘がある。*See* Paul M. Schwartz, *EU Privacy and the Cloud: Consent and Jurisdiction Under the Proposed Regulation*, 12 PRIVACY AND SECURITY LAW REPORT 718, 720 (2013).

43 *See* Kuner, *supra* note 37, at 4.

44 Advocate General's Opinion on *Google Spain SL/ Google Inc. v. Agencia Española de Protección de Datos*, C-131/12, 25 June 2013.

もっとも、プロバイダのビジネスモデルに着目すると、加盟国内のデータ主体を対象として検索による広告収入を得ていること、EU 域内に子会社を置いていること、さらに各加盟国のウェブドメインを提供していることから EU 域内への管理者の設置が認定される。

b) 管理者：インターネット・サービス・プロバイダの管理者該当性について

→「管理者」・「処理者」の箇所を参照

c) 削除権（いわゆる忘れられる権利）：不完全・不正確な情報以外の個人データの削除について

→「削除権」・「忘れられる権利」の箇所を参照。

EU においては、データ保護法制の調和という観点から、OECD や欧州評議会では合意に至ることができなかった適用法の枠組みを示してきた[45]。しかし、実際にデータ処理や管理をする者にとっては重要な論点であるにもかかわらず、これまでのところプライバシーをめぐる訴訟において管轄や適用法に関する国際的合意は存在していない[46]。たしかに、欧州司法裁判所の判決[47]においてもあらゆるインターネットの問題に指令が適用されることを示したわけではない。インターネットの文脈においてもプライバシーの諸原則が適用されるかについては規則提案においても「開かれた問題」であるため、裁判所による解決が待たれている[48]。

この点、域外適用をめぐる問題は経済法分野において、属地主義の観点から客観的属地主義アプローチや効果論アプローチが議論されてきた[49]。すなわち、EU 域内で生じる行為の遂行や手段の使用に基づき、客観的属地主義を採っていると解することができる。他方で、第 4 条 1 項 c 号は手段の利用に着目し、EU 域外でのデータ処理により EU 域内の発生

---

[45] Lee A. Bygrave, *Determining Applicable Law pursuant to European Data Protection Legislation*, Computer Law & Security Report, vol. 16, p. 252 (2000). なお、いわゆる電子プライバシー指令には域外適用に関する条項はおかれていない。

[46] 特定の領域を想定せずに、裁判所やデータ保護監督機関の執行権限が及ぶ「管轄（jurisdiction）」の問題と、当事者の行為の合法・違法性を決定する「適用法（applicable law）」とは異なる次元の問題であることを認識する必要がある。*See* Eduardo Ustaran, *The Scope of Application of EU Data Protection Law and Its Extraterritorial Reach*, in BEYOND DATA PROTECTION 136 (Noriswadi Ismail & Edwin Lee Young Cieh eds., 2013). この点、米国では「適用法」の問題ではなく、「管轄」の観点からインターネット上のプライバシー問題を議論するのが一般的である。*See e.g.*, JONATHAN L. ZITTRAIN, JURISDICTION (2005).

[47] CJEU, *Bodil Lindqvist*, C-101/01, para 69.

[48] Christopher Kuner, *Foreign Nationals and Data Protection Law: A Transatlantic Analysis*, in DATA PROTECTION ANNO 2014: HOW TO RESTORE TRUST? 222 (Hielke Hijmans & Herke Kranenborg eds., 2014).

[49] 庄司・前掲注 39、25 頁、参照。

する効果に着目するとみなされれば、効果理論の立場と理解される。しかし、第 4 条 1 項 c 号の手段の使用という一般的抽象的な文言を用いることで、域外適用が拡大する「過剰規制」の問題点が指摘されてきた[50]。なお、規則提案の下では、「過剰規制」の問題を克服するため、標的基準のアプローチを採られているという指摘があるが[51]、既存の属地主義の客観的属主義や効果論のアプローチと標的基準のアプローチを複層的に用いた形での検討の必要性が指摘されている[52]。

Ⅲ．データ主体の権利

１．同意

（１）EU データ保護指令

・データ主体の同意とは、データ主体が自己に関する個人データが処理されることへの同意を表明することによって、自由になされた特定的でかつ十分に情報を提供された上での意思表示を意味する（第 2 条 h 号)。

（２）EU データ保護規則提案

委員会	・データ主体の同意とは、データ主体が自由に与えられた特定的で情報を受けた上での、明確な意思表示を意味する。そして、データが処理されることに同意する表明又は明確な積極的行動によるものとする。(第 4 条 8 号)。 ・管理者はデータ主体からの同意を得たことの立証責任を負う（第 7 条 1 項)。 ・データ主体はいつでも同意を撤回する権利を有する（第 7 条 3 項)。
議会	・同意の撤回について、同意は与える場合と撤回する場合と同様に容易な方法とする（第 7 条 3 項)。
理事会	・管理者の同意の立証責任について、管理者が同意を証明することができる、という表現の検討がされている（第 7 条 1 項)。

（３）同意の概念

同意は自己情報コントロールの基盤を成す概念である。第 29 条作業部会の意見において

---

[50] Bygrave, *supra* note 45, at 255.
[51] 庄司・前掲注 39、27 頁、参照。
[52] Dan Jerker B. Svantesson, *A "Layered Approach" to the Extraterritoriality of Data Privacy Law*, 3 INT'L DATA PRIVACY LAW 278, 286 (2013).

示されているとおり、同意はドイツで発展した情報自己決定の概念とも結びついている[53]。同意の概念の重要要素には、次の事項が含まれることとされている。

①「意思表示」…意思表示の形態は特定されていないが、書面による同意等の現実の行為が必要となる。

②「自由になされた」…詐欺、強制、その他消極的帰結の危険がある場合の同意は自由になされたものとみなされず、データ主体の自発的決定ないし真正な選択ができることが前提とされる。たとえば、空港におけるボディスキャナは、それを拒否すれば怪しまれるため、実質的に自由な同意とは言えない（選択を認める立法措置が必要）。

③「特定的」…利用目的が限定されない包括同意（blanket consent）は認められない。同意は処理の目的に関連する合理的かつ必要な範囲を対象として与えられなければならないが、必ずしも単一の事業につき同一の目的内の新サービス提供ごとに同意が必須というわけではない[54]。もっとも、特にソーシャル・ネットワーキング・サービスにおいても、個々のサービスについて異なる利用目的があれば、目的ごとに同意を得ることが奨励される。

④「明確」…同意についてデータ主体の意図について曖昧さを残さないことが明確な同意である。そのため、個人の意図に疑問が残る場合は、明確な同意とは言えない。たとえば、オンライン上でホテルからのロイヤリティ・プログラムを受けようとする場合、そのプログラムのために個人データが利用されることをチェックするボックスが必要となる。

⑤「明示」…センシティブ・データの処理には明示の同意が必要となる。たとえば、疫学研究のためのデータ利用については、データ主体からの異議申立があるまでデータ提供することは明示の同意の要件を満たしていない。そのため、いわゆるオプト・アウトは、明示による同意とはみなされず、異議申立権の行使の一環として位置づけられている[55]。

⑥「情報を受けた」…情報を受けた同意には、分かりやすい形での情報提供があること、そして、その情報に直接アクセス・認識できることが条件となる。犯罪マップを公開する場合、仮に特定の被害者との結合が可能な場合、情報が公開されることについての被害者からの同意が必要となる。

また、規則提案では、同意の撤回と管理者による同意の立証責任など新たな要件が加え

---

53 Article 29 Data Protection Working Party, *Opinion on the Definition of Consent*, (WP187) adopted on 13 July 2011.

54 CJEU, *Deutsche Telekom AG*, Case C-543/09, 5 May 2011.

55 ELENI KOSTA, CONSENT IN EUROPEAN DATA PROTECTION LAW 125 (2013).

られた点は注目すべきである。

（4）クッキーのための同意取得

EU 市民はインターネット上のサービスを受ける際に、54%が利用に関する条件等について事前に情報を受けていると回答しているが、28%が同意の手続がとられていないと回答している[56]。

インターネットのウェブ・オペレーターは同意を得る際に、第 29 条作業部会の作業文書によれば特に次の点について留意が必要である[57]。すなわち、同意が真正なものであるというためには、①クッキーが設定されることに関する具体的で特定された情報が提供されていること、②クッキーが設定される前の事前のタイミングの同意、③ユーザーの積極的な行為又は能動的な振る舞いによる同意、④自由な選択という 4 つの要件が必要である。

なお、インターネット上のサービスについて、ある国における同意が別の国における処理の根拠となりうるかどうかなどの論点について国ごとに異なる対応が採られてきた、という問題点が指摘されてきた[58]。

２．忘れられる権利及び削除権

（1）EU データ保護指令

・データの不完全または不正確な性質については、データ主体が修正、消去又はブロックの権利が保障されなければならない（第 12 条）。

（2）EU データ保護規則提案

委員会	・データ主体は、次に掲げる場合、管理者に対して自らに関する個人データの削除及び拡散を停止させる権利を有する。 a) 収集・処理の目的との関係でデータがもはや必要でなくなった場合 b) データ主体が同意を撤回した場合、データ保有期間を過ぎた場合、データ処理の法的根拠がない場合 c) データ主体が異議申立権を行使した場合

[56] European Commission, *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*, June 2011 at 121.

[57] Article 29 Data Protection Working Party, *Working Document Providing Guidance on Obtaining Consent for Cookies,* (WP208) adopted on 2 October 2013.

[58] European Commission, *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the light of Technological Developments; Working Paper No.2 Data Protection Laws in the EU*, 20 January 2010 at 8 (Douwe Korff).

	d) 本規則提案を遵守していないデータ処理が行われた場合（第 17 条 1 項） ・管理者は、個人データの複製・複写へのすべてのリンクを削除するよう第三者に通知し、管理者が責任を有するデータの公開に関してあらゆる合理的手段を採らなければならない（第 17 条 2 項）。 ・管理者は、次の場合を除き、個人データを遅滞なく削除しなければならない。 a) 表現の自由を行使するため b) 公衆衛生の分野で公的利益のため c) 歴史的・統計的・科学的な研究目的のため d) EU 法・加盟国法により個人データの保全の法的義務の履行のため e) その他処理の制限をされている場合（第 17 条 3 項）
議会	・条文の名称から忘れられる権利が削除された。 ・データを削除できる場合について、裁判所又はデータ保護監督機関により削除が終局的で最終的に確定された場合が追加された（第 17 条 1 項 ca 号）。 ・データの削除について、データ主体の本人であることが管理者によって証明できることを前提とする条項が追加された（第 17 条 1a 項）。 ・データ削除のための管理者の責任について、個人データの複製・複写へのすべてのリンクを削除するよう第三者に通知等の具体的方法が削除された（第 17 条 2 項）。
理事会	・忘れられる権利及び削除権について、管理者の義務として遅滞なく個人データを削除が検討されている（第 17 条 1 項）。 ・忘れられる権利を行使できる場合として、データ主体が異議申立権を行使した場合にそれを上回る正当な法的根拠という表現の追加と、不法な処理が行われた場合の追加が検討されている（第 17 条 1 項 c 号・d 号）。 ・管理者が削除する義務として、利用可能な技術とその実施の費用を考慮しつつ、という表現の追加が検討されている（第 17 条 2 項）。 ・管理者が削除すべき場合として、雇用分野における社会的な保護の目的のため、という条項の追加が検討されていれている（第 17 条 3 項 ca 号）。

（3）忘れられる権利の導入背景[59]

[59] 忘れられる権利の性格については、宮下紘「忘れられる権利をめぐる攻防」比較法雑誌 47 巻 4 号（2013）29 頁以下、杉谷眞「忘れてもらう権利」Law & Practice7 号（2013）153 頁以下、伊藤英一「ヨーロッパ『記憶する義務』から『忘れられる権利』の時代へ」新聞学研究所紀要 5 号（2012）230 頁以下、参照。

「忘れられる権利」は、2010 年から Reding 副委員長が提唱してきた権利である。2010 年 11 月 4 日、欧州委員会は、個人データの新たな包括的法的枠組みを公表し、その中で、「収集された目的にとってもはや必要でなくなった際にはデータを完全に消去してもらう」権利としての「忘れられる権利」が掲げられることとなった[60]。そして、Reding 副委員長は「神は許しを与え忘れるが、ウェブは決してそうではない。だから私にとって『忘れられる権利』は極めて重要である」[61]と主張し、「忘れられる権利」の導入に意欲を見せた。実際、EU 市民の 75%がいつでもインターネット上の自らの個人データの削除を希望している[62]。また、もともと、忘れられる権利はオンライン上でのソーシャル・ネットワーキング・サービスにおける児童の権利擁護を一つの目的としていたが、成人に対してもこの権利が及ぶことを明確にするため、議会修正案ではこのことを反映した[63]。

忘れられる権利の導入を唱道してきたフランスでは、フランス人権宣言第 2 条が、自由、所有、安全及び圧政への抵抗としての自然権の保障を謳い、プライバシーの尊重（respect de la vie privée）の保障が導かれている[64]。人間が人間らしく存在するために、あるいは人間だからこそ、「忘れる」ことが自由、所有、安全及び圧政への抵抗のその構成要素として尊重されなければならない。このモチーフを基に、ヨーロッパの中でいち早く「忘れられる権利」の必要性を唱道したのはフランスであった。2009 年 11 月 6 日フランス上院において、デジタル世界におけるプライバシーの権利の保障強化に関する法案が提出された[65]。実際、フランスでは 2012 年 CNIL に寄せられた申立の 1050 件（合計 6017 件）が「忘れら

---

60 European Commission, *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions; A Comprehensive Approach on Personal Data Protection in the European Union*, 4 November 2010, at 8. なお、Reding 欧州委員会副委員長は、すでに 2010 年 6 月 22 日の米国商工会議所での会議において、すでに「忘れられる権利」の導入の必要性を説いていた。*See* Viviane Reding, *Building Trust in Europe's Online Single Market*, Speech at the American Chamber of Commerce to the EU Brussels, 22 June 2010.

61 Viviane Reding, *Why the EU Needs New Personal Data Protection Rules, The European Data Protection and Privacy Conference*, 30 November 2010.

62 European Commission, *Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union*, June 2011 at 158.

63 *See* Rachele Ciavarella & Cécile De Terwangne, *Online SocialNetworks and Young People's Privacy Protection: The Role of the Right to be Forgotten*, in MINDING MINORS WANDERING THE WEB: REGULATING ONLINE CHILD SAFETY 157 (2014).

64 *See* Décision n° 99-416 DC du 23 juillet 1999. フランスのデータ保護法制としては、消費者庁『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』(2011) 34 頁以下、参照。

65 Proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique (n° 93 (2009-2010) de M. Yves DÉTRAIGNE et Mme Anne-Marie ESCOFFIER, déposé au Sénat le 6 novembre 2009).

れる権利」に関連するものであり、その現実的需要をうかがうことができる[66]。

他方で、欧州データ保護監督機官 Peter Hustinx はフランスの”le droit á l'oubli”が英語に「誤訳」され、「削除」・「消去」ではなく「忘却」のプロセスが誇張されすぎていると指摘する[67]。

議会でのヒアリングによれば、議会の採決直前に、Albrecht 議員が「忘れられる権利」という名称の維持をどうすべきか委員会の議員に聞いたところ、「削除権」にしておいた方がよい、という意見が多数を占め、名称変更に至った、というものである[68]。ただし、この名称変更は委員会が提唱した「忘れられる権利」の基本的性格それ自体の大きく変えるものではないことに注意が必要である。事実、委員会は議会が採択した後も、議会が依然として「忘れられる権利」を擁護したという理解を示してきた。2014 年 3 月時点でも、理事会の審議では「忘れられる権利」の名称は維持されており、「忘れられる権利」が規定されるかどうかは今後の三者対話での交渉にかかっている。

（4）執行可能性―ネットワーク情報セキュリティ庁報告書

「忘れられる権利」については、現実の執行に疑問が投げかけられることがある。たとえば、検索サイト等のデータ管理者が、直接関係のない無数に存在する掲示板における個人データに対して消去のために通知をすることが果たして可能であるか、ソーシャル・ネットワーキング・サービスにおいて共通の写真に掲載されている複数の個人の間で、ある個人が削除を求め、別の個人がその削除を求めない場合、どのように対応すべきか、あるいはインターネット上のサーバーにおけるデータを消去するためにどのような技術的措置を講ずべきか、といった様々な問題がすぐに提起される[69]。また、現在の個人情報の流通は、インターネット上複雑な過程を経て、収集、追跡、さらには再識別化が行われており、どの段階の個人情報を削除すべきかについても明確に定まらない[70]。

この点について、欧州ネットワーク情報セキュリティ機関による調査報告書（2012 年 11

---

66 Commission Nationale de l'Informatique et des Libertés, *Rapport d'Activité* 2012.
67 Peter Hustinx, *Speech: The Right to be Forgotten and Beyond: Data Protection and Freedom of Expression in the Age of Web 2.0*, Oxford Privacy Information Law and Society Conference, June 12, 2012.
68 忘れられる権利の名称変更を求める修正案として、欧州議会市民的自由・司法・内務委員会における European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Amendment 1380 (Alexander Alvaro), Amendment 1381 (Axel Voss), Amendment 1382 (Sylvie Guillaume, Françoise Castex), Amendment 1383 (Adina-Ioana Vălean, Jens Rohde)がある。
69 *See* Luiz Costa & Yves Poullet, *Privacy and the regulation of 2012*, 28 COMPUTER LAW & SECURITY REVIEW 254 (2012).
70 *See e.g.*, *They Know What You're Shopping For*, WALL ST. J., December 8, 2012 at C1.

月公表）では、「忘れる」ことの法的性格に関して 3 つの解釈が示されている[71]。

a) 最も厳格な解釈として、データの複製が問題とされているあらゆるインターネット上の拠点から消去・削除され、いかなる技術的な手段を用いてもその回復が不可能とするものである。

b) 不正な第三者によって解読されない限り、暗号化されたデータ複製の維持が認められるというものである。

c) 公開されたインデックスや検索エンジンの結果に表示されない限り、データの複製が認められるという最も緩やかで実践的な解釈である。

「忘れられる権利」の執行実務という観点からは、公開されたインターネットにおいてこの権利を執行することは「一般論として不可能（generally impossible）」であるものの、プラグマティックな実践方法として、検索エンジンのオペレーター等に対して忘れられるべき情報への参照にフィルターをかけるよう要請し、この権利を支えることが適当であると考えられている[72]。しかし、残された最大の問題は、何が忘れられるべき情報に該当するか、という「情報の内容」の審査であろう。

（５）欧州司法裁判所による審理

このような中、2012 年 3 月 9 日には、スペイン裁判所に係争されていた Google の検索結果（たとえば、検索結果において、家庭内暴力により離婚した被害者の住所が分かった件）から自らのデータの削除を求めた約 90 名による訴訟が、欧州司法裁判所に付託された[73]。本件では、現行の EU データ保護指令に基づき判断されることとなるが、次の 3 点が審理されることとなっている。第 1 に、EU データ保護指令の適用範囲の問題である。すなわち、米国に拠点を置く Google が「構成国内に設置されたデータ管理者」（4 条 a 項）といえるかどうか、あるいは域内の設置が認められない場合、「個人データの処理を目的として構成国の域内に設置された…設備を利用」しているかどうか、である。この点に関して、第 29 条データ保護作業部会の意見では、EU 域外の情報通信を取り扱う事業者に対して、EU 域内のミラーサイトを通じてデータの収集が行われる場合、そのようなクッキーなどを用いたデータの処理にも EU データ保護指令が適用されることを示している[74]。

---

71 European Network and Information Security Agency, *The Right to be Forgotten - Between Expectations and Practice* (November 2012) at 7.
72 *Id.* at 14.
73 CJEU, Case C131/12, *Google Spain, S.L., Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González*.
74 Article 29 Working Party, *Working Document on Determining the International Application of EU Data Protection Law to Personal Data Processing on the Internet by non-EU Based Websites* (WP56, adopted on May 2002) at 10.

第 2 に、データ処理者及び管理者の該当性である。Google はインターネットの検索エンジンによるインデックス情報を一時的に蓄積しているだけであり、データを処理し（2 条 b 項）、管理している（2 条 d 項）とみなすことができるかどうかである。第 29 条データ保護作業部会は、IP アドレス自体を個人データに該当するとみており、そのため IP アドレスやクッキーを処理すれば、データ管理者を構成するものと解している[75]。この点について、特定の言葉の検索結果として単に表示・羅列する場合、検索サイトは何らのデータ処理を行っていないようにも思われる。他方で、特定の言葉とともに、一定の関連する言葉を自動表示する場合（いわゆるサジェスト機能を用いた場合）、それはデータの編集・加工を行っていることからデータ管理者とみなすことができるかどうか慎重な審理が必要となろう。仮に検索サイトによるデータの編集・加工が認められれば、Google による表現内容の編集・加工によるプライバシー侵害に加担していると考えることができよう。

第 3 に、検索サイトから公表された自らの情報について、データ主体が削除及びブロックする権利（12 条）、そして異議申立の権利（14 条）が認められるかどうかという問題がある。この点、現行の 12 条は、規則提案 17 条のように、「忘れられる権利」を明言しているわけではないが、「データの修正、消去又はブロック」を定めている[76]。

2013 年 6 月 25 日、欧州司法裁判所による判決を前に、法務官（advocate general）による予備意見が公表された[77]。第 1 の争点、EU データ保護指令の適用範囲について、予備意見では、たとえスペイン国内で個人データの処理が行われていなくても、インターネット検索エンジンというビジネス・モデルに着眼して、スペイン在住の者をターゲットに広告配信などしていることから EU 域内に管理者を設置したものとみなし、指令の適用を受けることとなる。つまり、スペインのユーザーが被害を受けるおそれがある以上、個人データの物理的な所在それ自体は決定的な要素となりえないことを示している（域外適用の箇所参照）。

第 2 に、インターネット検索エンジンが個人データの処理を行っているとしても、第三

---

[75] Article 29 Working Party, *Opinion 1/2008 on Data Protection Issues related to Search Engines* (WP148, adopted on 4 April, 2008) at 9. 「ネットの世界では管理権限の所在の特定は難しい」のみならず、「この権利をネット情報の権利とするためには、ヨーロッパの外の国々がこの提案を受け入れる必要がある」（藤原靜男「国家による個人の把握と行政法理論」公法研究 75 号（2013）39 頁）。

[76] Google が提供するサービスについては、特に本人の同意の観点からその不十分さが指摘され、「忘れられる権利」の基盤となる同意の在り方との関係で問題となる。*See* Bart van der Sloot & Frederik Zuiderveen Borgesius, *Google and Personal Data Protection* in GOOGLE AND THE LAW 109 (Aurelio Lopez-Tarruella ed., 2012).

[77] CJEU, Case C131/12, *Google Spain, S.L., Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González*. Opinion of Advocate General JÄÄSKINEN, June 25, 2013.

者が運用するウェブページ上の個人データをコントロールしているわけではないため、データ管理者を構成するものではない。つまり、検索エンジンは表示されてくるウェブページの内容とは何の関係も有せず、そのウェブページ上の情報を変える手段を有していない。そのため、Google は EU データ保護指令が課している義務規定を法律上も事実上も履行することができず、またデータ保護機関が検索結果から情報の撤回を要請することができない。

第 3 に、最も実質的な争点である削除の権利については、表現の自由との調整も必要となり、現行の EU データ保護指令には「忘れられる権利」それ自体が規定されていないことから、既存の削除権や異議申立権を根拠に検索サイトからの情報の削除を一般的な権利として容認することはできないとされた。

Google は、名誉毀損やプライバシー・セキュリティ等を理由として、たとえば 2012 年 7 月～12 月において政府や裁判所から 24,179 のコンテンツを対象に 2,285 件の削除要請を受けており、その 45%に応じてきている[78]。いずれにせよ、欧州司法裁判所による本件審理は、法務官の予備意見でも再三言及され意識されていた「忘れられる権利」の今後の展開の試金石となろう[79]。

（6）データ保全指令

EU においては、テロリスト対策の一環として 2006 年にデータ保全指令[80]を発効した。これにより加盟国は通信履歴を 6 か月以上 2 年以下の期限を設け、保全しなければならないこととなった。この保全された通信履歴については、一定の要件の下、警察安全保障機関が IP アドレスや電話履歴等にアクセスすることが認められている。

欧州データ保護監督官によれば、データ保全指令は、「影響を受ける人々の規模と数の観点から EU がこれまで採択した中で最大のプライバシー侵害となる文書である」[81]と批判されてきた。そのような中、2013 年 12 月 12 日、欧州司法裁判所法務官による意見（2014 年 3 月現在係争中）によれば、データ保全指令は、EU 基本権憲章の第 7 条と基本権制約の

---

[78] Google 透明性レポート（2012 年 7 月～12 月）。
http://www.google.com/transparencyreport/removals/government/?metric=items (last visited on November 1, 2013)

[79] *See* Muge Fazlioglu, *Forget Me Not: The Clash of the Right To Be Forgotten and Freedom of Expression on the Internet*, 3 INT'L DATA PRIVACY L. 149, 153 (2013).

[80] 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.

[81] Peter Hustinx, *Speech: The "Moment of Truth" for the Data Retention Directive: EDPS Demands Clear Evidence of Necessity*, 3 December 2010.

ための必要性と比例原則を定める 52 条に違反し、無効であるとの判断を示した[82]。この意見に法的拘束力はないが、データ保全を定めた指令を違反とした論理が、忘れられる権利なるものへの接近とみることができる。

「…人間は、一定の期間を経て自らの存在を全うしている。…異論のないことと思われることとは、現在という時の認識と過去という時の認識の間の区別の可能性である。いずれの認識においても、各人は、『記録された』生として自らの生、特に『私生活』を意識することが一定の役割を果たす。」

そして、法務官は、『現在という時』のみならず、『過去という時』を一定の「時」を国家が保全することを必要かつ比例原則に照らして判断すると、『過去という時』への国家による干渉の正当化理由を見いだせない、と指摘した。

４．プロファイリングされない権利

（1）EU データ保護規則提案

委員会	・すべての自然人は、職務能力、経済状況、位置、健康、個人の選好、信頼性、行動を分析又は予測するための自動処理にのみよって法的効果がもたらされ又は影響を及ぼされる基準に服さない権利を有する（第 20 条 1 項）。
議会	・プロファイリングとは、一定の個人の特性を評価し、又は自然人の職務能力、経済状況、位置、健康、個人の選好、信頼性、行動を分析もしくは予測することを意図した個人データの自動処理のいかなる形態を意味する（第 4 条 3a 項）。 ・すべての自然人は、プロファイリングに異議申立の権利を有するという、表現に変更された（第 20 条 1 項）。
理事会	・プロファイリングの定期の追加が検討されている（第 4 条 12a 号）。 ・すべてのデータ主体はプロファイリングのみに基づく決定をされない権利を有する、という表現で検討されている（第 20 条 1 項）。

（2）プロファイリング

一定の個人の特性を評価又は個人職務能力、経済状況、位置、健康、選好・信頼性・行為を分析若しくは予測することを目的とした自動処理の形態としてのプロファイリングの定義が議会の修正案に追加された（第 4 条 3a 号）。第 29 条作業部会は議会が提案したプロファイリングの規定を支持し、データ主体に対する透明性とコントロールの確保の重要性

[82] CJEU, Opinion of Advocate General Cruz Villalón, *Digital Rights Ireland Ltd v. The Minister for Communications*, C-594/12, 12 December 2013.

を指摘している[83]。

欧州司法裁判所判決 Huber v. Germany[84]においても、ドイツに 3 か月以上居住する外国人を登録したデータベースが国籍に基づく差別的な個人データの蓄積として認められないことが明らかにされた。判決では、利用目的の制限の必要性とデータの質に関する比例原則のいずれからも認められないことを示した。このようなデータベースによる運用が結局は差別をもたらすプロファイリングを助長すると認められた[85]。

また、プロファイリングについては、2013 年 9 月に開催された第 35 回データ保護プライバシー・コミッショナー国際会議においてもプロファイリングに関する決議[86]が採択されていること、また欧州評議会条約第 108 号においてもプロファイリング決議が 2010 年に採択されていることなどから、特にビッグデータ・ビジネスを背景としたプロファイリング規制は国際的な潮流である。

Ⅳ．事業者の義務

１．基本概念

（１）EU データ保護指令

・管理者（controller）とは、単独または他と共同して、個人データ処理の目的及び手続を決定する自然人、法人、公的機関等をいう。（第 2 条 d 号）

・処理者（processor）とは、管理者のために個人データ処理を行う自然人、法人、公的機関等をいう。（第 2 条 e 号）

・取得者（recipient）とは、第三者であるか否かにかかわらず、データ開示を受ける自然人、法人、公的機関等をいう。（第 2 条 g 号）

（２）EU データ保護規則提案

---

83 Article 29 Data Protection Working Party, *Advice Paper on Essential Elements of a Definition and a Provision on Profiling within the EU General Data Protection Regulation*, adopted on 13 May 2013.

84 CJEU, *Huber v Federal Republic of Germany*, C-524/06, 16 December 2008.

85 Gellert Raphaël, De Vries Ekaterina, De Hert Paul & Gutwirth Serge, *A comparative analysis of anti-discrimination and data protection legislations*, in DISCRIMINATION AND PRIVACY IN THE INFORMATION SOCIETY 77 (Bart Custers et. al. eds., 2012).

86 35th International Conference of Data Protection and Privacy Commissioners, *Resolution on Profiling*, 25 September 2013. Available at https://privacyconference2013.org/web/pageFiles/kcfinder/files/2.%20Profiling%20resolution%20EN%281%29.pdf (last visited 27 March 2014).

規則提案において、「管理者」、「処理者」、「取得者」に関する定義に大きな変更はない。ただし、管理者および処理者は「データ保護担当者（data protection officer)」の指名が要件とされた（第 35 条)。この要件の一つには、中小企業の免除要件について審議が行われてきた。

委員会	・管理者及び処理者は、次の場合、データ保護担当者を指名しなければならない。 a) 処理が公的機関等によって行われる場合 b) 処理が従業員 250 名以上の企業によって行われる場合 c) 管理者又は処理者の中心的な業務が、その性質、適用範囲、目的によってデータ主体の定期的かつ体系的に監視を必要とする処理の実施の場合（第 35 条 1 項）
議会	・データ保護担当者の要件について、従業員 250 名という要件に代わり、法人による処理の場合、過去 12 か月間において 5000 件以上のデータ主体に関する処理を行っているかどうかという要件に変更された。（第 35 条 1 項 b 号） ・データ保護担当者の要件について、新たに、大規模なファイリングシステムにおいてセンシティブ・データ、位置データ、児童又は労働者に関するデータを成す管理者又は処理者の中心的活動、という要件が追加された（第 35 条 1 項 d 号)。
理事会	・EU 法又は加盟国の法に基づきデータ保護担当者を指名する、という表現で検討がされている（第 35 条 1 項)。

（3）検索エンジンと処理者・管理者の関係

2013 年 6 月 25 日欧州司法裁判所法務官の予備意見によれば、検索エンジンは第三者が運用するウェブページ上の個人データをコントロールしていないため、管理者ではない。検索エンジンは表示されてくるウェブページの内容とは何の関係も有せず、そのウェブページ上の情報を変える手段を有していない。そのため、Google は EU データ保護指令が課している義務規定を法律上も事実上も履行することができず、またデータ保護機関が検索結果から情報の撤回を要請することができない。

（4）中小企業の免除基準

データ保護担当者の指名の要件の一つに、中小企業免除がある。しかし、中小企業の免除基準について、委員会は 250 人の従業員という基準を示し、議会は過去 12 か月において

5000 件以上のデータ主体の処理という基準を修正案を示している。委員会のヒアリングによれば、従業員 250 人は EU の公式基準であり、より客観的で容易に測定できる基準が望ましいとのことである。他方で、議会は、特にクラウド・コンピューティングを念頭において、従業員数よりもデータ主体の処理の数を対象とすべきであるとの指摘があった。理事会では、今後、委員会と議会との交渉を進める予定とのことであった。

２．処理の合法性の原則

（１）EU 基本権憲章

・個人データは本人同意又は法律に定められたその他の正当な根拠に基づき処理されなければならない（第 8 条 2 項)。

・憲章によって承認される権利及び自由の行使に対するいかなる制約も、法律によって定められたものでなければならない。制限は、比例原則に従い、それが必要であり、かつ EU が承認する一般的利益の目的又は他者の権利及び自由を保護する必要性を満たした場合のみ許される（第 52 条 1 項)。

（２）EU データ保護指令

・公正かつ適法に処理されることを加盟国は定めなければならない（第 6 条 1 項 a 号）

・加盟国は次に掲げる条件を満たす場合にのみ、個人データが処理されるよう定めなければならない（第 7 条）

a) データ主体が明確に同意を与えた場合
b) データ主体が当事者となっている契約の履行のために処理が必要な場合、又はデータ主体による請求により、契約締結前に処理が必要な場合
c) 管理者が法的義務を遵守するために処理が必要な場合
d) データ主体の重大な利益を保護するために処理が必要な場合
e) 公共の利益又は公的権限の行使他のために行われる義務の遂行に処理が必要な場合
f) 正当な利益のために処理が必要な場合

（３）EU データ保護規則提案

委員会	・処理の根拠に、歴史的、統計的又は科学的研究に必要な場合が追加された（第 6 条 2 項)。
議会	・処理の合法性について、本規則の範囲内で、加盟国は詳細を定めることとす

	る、という規定が追加された（第 6 条 3 項)。
理事会	・追加の処理について、管理者は、当初の目的との関係、データ収集の経緯、個人デーの性質、追加の処理の帰結、適切な安全管理措置を考慮に入れなければならないことが検討されている（第 6 条 3a 項)。

３．データ侵害の通知義務

（1）EU データ保護規則提案

委員会	・個人データへの侵害が生じた場合、管理者は事実を知ってから、遅滞なく、また可能であれば 24 時間以内に監督機関に通知しなければならない。もしも 24 時間以内の通知ができない場合は、合理的な理由を示す必要がある（第 31 条 1 項)。 ・通知の内容には、少なくとも、個人データの侵害の性質（被害者数、データの類型・数)、データ保護管理者の連絡先、影響を小さくするための対策、侵害による結果、管理者による対策を含むこととする（第 31 条 3 項)。 ・委員会は標準的な書式、手続、文書の様式を指定することができる（第 31 条 6 項)。 ・データ保護又はデータ主体のプライバシーに悪影響を及ぼし得る侵害については、管理者がデータ主体と連絡をとらなければならない（第 32 条 1 項)。 ・管理者が監督機関への技術措置に関する報告が十分なものである場合のみデータ主体への連絡は必要ない（第 32 条 3 項)。
議会	・通知の時間について、24 時間以内という文言が削除された（第 31 条 1 項)。もっとも、前文において 72 時間以内の通知が要求されている（前文第 67 項)。 ・委員会による書式等の指定については削除が検討されている（第 31 条 6 項)。
理事会	・通知の対象について、データ主体の権利及び自由への深刻な影響を及ぼす侵害、という文言の追加が検討されている。また、通知の時間については、72 時間以内で検討されている（第 31 条 1 項)。 ・委員会による書式等の指定については削除が検討されている（第 31 条 6 項)。

（2）第 29 条作業部会による意見

第 29 条作業部会はデータ侵害通知義務について意見を公表し、データ主体にとっての悪

影響に関して、いくつかの事例から具体的な通知の有無など解説している[87]。

事例①：児童病院から 4 台のラップトップが紛失した事例（パソコンの中には医療・福祉に関するセンシティブ・データが含まれ、他の 2050 人の児童の個人データが含まれる）

この事例においては、紛失によって、医療機密、児童の治療への継続性の妨げ、さらに児童の医療記録による治療の妨げといった悪影響が予想される。データ主体の年齢や成長度を考慮に入れる必要があるが、データの通知が必要である。同時に保護者や代理人に対しての通知をすることも適当と言える。

事例②：生命保険会社の顧客データが、ウェブ・アプリの脆弱性による不当にアクセスされた事例（アクセスされた 700 人の顧客データには氏名、住所、医療に関する質問項目が含まれる）

この事例においては、データ主体の質問項目から職探し（妊娠中など）や家庭環境に悪影響を及ぼすことが予想される。技術の脆弱性の継続的な監視とともに、データ主体にも通知が必要である。

事例③：社員が第三者に全世界の顧客情報にアクセスできるログインとパスワードを教え、顧客情報がアクセスされた事例（100,000 人の顧客の氏名、住所、メールアドレス、電話番号、支払いデータを含む）

この事例においては、顧客の財産的な悪影響のみならず、データベースから顧客情報の修正や削除が行われる可能性がある。影響を受けた顧客への通知が必要である。

これらの事例で紹介がされているものの、個人データ侵害の通知義務の有無は事案ごとに判断すべきであると示されている。また、通知義務が発生しない場合として、最新のアルゴリズムを用いて安全に暗号化されており、権限のない者によるアクセスが不可能な場合やデータが安全にハッシュ・ソルトされており、権限のない者によるアクセスが不可能な場合には通知の必要がないとされている。

（3）加盟国の例

イギリスでは、「セキュリティ侵害管理に関するガイダンス」[88]を公表し、個人データへの侵害の事案が発生した場合の通知の仕方などを解説している。このガイダンスに基づく通知は法的に強制力がなく、任意である。しかし、医療・福祉の及び情報通信の二分野についてはそれぞれ別途ガイドが公表されており、いずれの分野もセキュリティ侵害の事案

---

[87] Article 29 Data Protection Working Party, *Opinion on Personal Data Breach Notification* (WP213, 25 March 2014). なお、EU ネットワーク情報セキュリティ庁では加盟国のデータ保護監督機関と協力して、データ侵害通知の実態についても調査している。*See* ENISA, *Data Breach Notifications in the EU* (2011).

[88] ICO, *Guidance on Data Security Breach Management, version 2.1* (2012).

が発生した場合、情報コミッショナー・オフィスや関係省庁への通知が義務付けられている[89]。特に情報通信分野（インターネット・サービス・プロバイダを含む）については、セキュリティ侵害の事案を知ってから 24 時間以内に最低限の情報を情報コミッショナー・オフィスに通知しなければならない。この通知を怠った場合、1000 ポンドの制裁金が科されることとなる。

セキュリティ侵害が発生した場合に情報コミッショナー・オフィスに提出すべき内容には、次の項目を記載することになっている。

①組織の詳細…名称、管理者の登録番号、連絡先

②データ保護侵害の詳細…事案の詳細、いつ、どのように、通知遅滞の場合はその理由、侵害防止のとっていた対策、関連する方針や手続等

③危険状態にある個人データ…個人データの性質、個人の数、個人の事実把握の有無、個人への予想される帰結と悪影響、苦情の有無、

④被害拡大防止と回復…被害の最小限・軽減策、回復の有無、再発防止策

⑤研修…データ保護法に基づく研修、全社員への研修義務、社員用のガイダンス

⑥ICO との過去の連絡…過去 2 年間の通知の有無（ある場合の詳細）

⑦その他…外国の監督機関への通知、警察への通知、他の規制機関への通知、報道の有無

フランスでは、情報処理、情報ファイル及び自由に関する法律第 34 条 bis の追加により、電気通信事業分野におけるデータ侵害事案のオンラインによる通知が義務化された[90]。データ侵害の事案が発生した場合、その事案を知ってから 24 時間に最低限の情報をデータ保護監督機関（CNIL）へのウェブサイトからのオンライン通知を義務付け、仮に必要な情報をすべて通知できない場合は 72 時間以内に通知しなければならない。仮に通知を怠った場合は、€300,000 及び 5 年以内の禁固の罰則が科されうる。①個人データを処理していること、②データ侵害があること（破壊、紛失、改ざん、漏えい、不正アクセス、偶発的又は不法なアクセスを含む）、③電気通信分野における事業者であること、が通知の前提となっている。

なお、個人データへの侵害発生を知ってから 24 時間以内の監督機関への通知という時間については、弁護士によるヒアリング結果からは実務において困難であるという指摘があ

---

[89] Department of Health, *Checklist Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation* (version 2.0), 1 June 2013; ICO, *Notification of PECR security breaches Privacy and Electronic Communications Regulations* (version 2.1), 26 September 2013.

[90] オンライン通知は、CNIL, *Notification de violation de données personnelles*; http://www.cnil.fr/vos-obligations/notification-de-violations/ (last visited 27 March 2014) からすることができる。

った。他方で、24 時間以内の通知を第一段階として、セキュリティの侵害があった事実のみの通知とし､その後二段階目として 72 時間以内の再通知というフランスの制度であれば、一定の形で機能し得るものと考えられる。

４．認証と行動規範

（１）EU データ保護指令

・加盟国が国内規定の適切な実施に役立てるために、行動規範の策定を促進しなければならない（第 27 条 1 項)。

（２）EU データ保護規則提案

委員会	・加盟国、監督機関及び委員会は、次の項目を考慮し、行動規範の策定を促進しなければならない。a）公正かつ透明なデータ処理、b）データ収集、c)市民及びデータ主体に関する情報､d）権利行使の要請､e）児童の情報と保護､f）第三国又は国際機関へのデータ移転、g）行動規範遵守のための監視及び確保の体制、h）裁判外紛争解決の手続（第 38 条 1 項)。 ・加盟国及び委員会は、欧州全域におけるデータ保護を認証する仕組みを構築するよう奨励する（第 39 条 1 項)。
議会	・行動規範の考慮事項について、消費者の権利の尊重という項目が追加された（第 38 条 1 項 aa 号)。 ・認証体制については、管理者又は処理者がデータ保護監督機関に対し、合理的な手数料の支払いにより認証を受ける、という形に変更された（第 39 条 1a 項)。 ・認証の名称については、標準的なデータ保護マークとして「欧州データ保護シール」とされた（第 39 条 1e 項)。 ・認証の有効期間については、最大で 5 年間とされた（第 39 条 1g 項)。
理事会	・行動規範の考慮事項について、正当な利益、仮名化データの利用、安全管理措置確保の対策及び手続、個人データ侵害の通知、が新たに追加項目として検討されている（第 38 条 1 項)。 ･行動規範については､その監視体制に関する条項が新たに検討されている（第 38a 条)。 ・認証の体制について、データ保護機関が認定する別個の機関が認証機関として認証及び定期検査を行うことが検討されている（第 39a 条)。

（3）自主規制と行動規範

EU においては、データ保護にとって法執行は不可欠で、自主規制は「神話」であるという前提がある[91]。そのため、各企業内が示した行動規範をデータ保護機関に提出し、その内容をチェックしてもらい、行動規範の遵守をデータ保護機関に対し証明するなどの対応が求められるよう検討が行われている。

（4）認証の比較

加盟国の中で認証制度を公式に設けているのはドイツ・シュレスヴィッヒ・ホルシュタイン州[92]とフランスである。EU 関係者からのヒアリングによれば、そもそも認証に関する議論はほとんど行われていないが、いずれの機関も日本の認証制度の普及を知っていた。ただし、日本の制度が法的強制力を有する監督機関に裏付けされていない制度であるため、他国の制度同様、EU においては日本とは異なる制度設計が行われている、との回答があった。委員会、議会、理事会によれば、EU では監督機関による制裁権限の行使が及ばない認証制度は有効ではない。また、欧州消費者団体によれば、消費者に選択肢を与えるという意味では認証が重要であるものの、プライバシー以外にもインターネットに関する認証があるため、認証の乱立はかえって消費者に混乱をもたらしてしまう、という危惧がある。以下、欧米における認証制度の比較一覧表をまとめておいた[93]。

	TRUSTe	BBBOnLine	ESPB Privacy Online	EuroPriSe	WebTrust	CNIL
認証機関とその性格	TRUSTe	民間企業	非営利団体	ドイツ・シュレスヴィッヒ・ホルシュタイン州	米国・カナダ会計士協会	データ保護監督機関
認証国	米国	米国	米国	ヨーロッパ	米国・カナダ	フランス
開始年	1997 年	1999 年	1999 年	2007 年	1998 年	2011 年
有効期間	1 年	—	—	2 年間	1 年間、90 日間の猶予	3 年間
認証数	4000 以上	145,700	400	22	—	—
基準	TRUSTe プライバシープログラム	BBB トラスト基準	ESPB プライバシー・オンライン・プ	EuroPriSe 基準	WebTrust 原則及び基準	CNIL の基準

91 Yves Poullet, *The Directive 95/46/EC: Ten Years after*, 22 COMPUTER LAW & SECURITY REPORT 206, 210 (2006).

92 藤原静雄「ドイツ・シュレスヴィッヒ・ホルシュタイン州のマーク制度」季報情報公開個人情報保護 25 号（2007）11 頁以下、参照。

93 一覧表は、
Rowena Rodrigues, David Wright & Kush Wadhwa, *Developing a Privacy Seal Scheme (that Works)*, 3 INT'L DATA PRIVACY L. 100, 102-103 (2013) に基づく。

			ログラム			
認証の類型	ウェブ・シール、モバイル・シール	ビジネス・プログラム	ESRB プライバシー・オンライン認証シール	ヨーロッパ・プライバシー・シール	WebTrust オンライン・プライバシー、消費者保護、認証	監査手続及び研修
費用	企業の規模による	330 ～ 7000 ドル	年会費と審査費	専門家費用等	基準履行による	―
認証取消	プログラム違反	プライバシー・ポリシー違反	苦情やプライバシー・オンライン基準に対する適切な措置の不履行等	原則と基準違反	サービス原則と基準違反	―
遵守・監視	自主的 継続中	自主的 継続中	自主的 Sentinel プログラム	自主的 専門家	自主的 専門家による定期的	法的強制 継続中
オンライン認証	○	○	○	×	○	○

５．データ保護バイ・デザインとデータ保護影響評価[94]

（１）EU データ保護規則提案

委員会	・管理者は個人データを必要以上に収集・保有しないよう初期設定により確保できる体制を確立しなければならない（第 23 条 2 項）。 ・処理の運用がデータ主体の権利及び自由に特定のリスクをもたらす場合、管理者又は処理者等は個人データの保護に対して想定される処理の運用の影響評価を実施しなければならない（第 33 条 1 項）。 ・特定のリスクをもたらす処理運用には次のものが含まれる。 a) 自然人に関する個人の性格の体系的かつ広範囲の評価 b) センシティブ情報のデータ処理 c) ビデオ監視等の公の場における監視 d) 児童、遺伝データ、生体データに関する個人データ（第 33 条 2 項）。
議会	・データ保護バイ・デザインについて、包括的な手続的安全管理措置に焦点を当てた個人データの収集から削除に至るまでの全体のライフサイクル管理であることが追記された（第 23 条 1 項）。

94 データ保護バイデザインやデータ保護影響評価等の基本概念については、英米法圏において発展してきたが、アン・カブキアン著・堀部政男ほか編『プライバシー・バイ・デザイン』（日経 BP 社・2012）、瀬戸洋一ほか『プライバシー影響評価 PIA と個人情報保護』（中央経済社・2010）、参照。

	・データ処理の影響のリスク分析に関する危険の尊重という新たな条項が追加された（第 32a 条 1 項）。 ・影響評価の実施対象について、リスク分析の条項で詳細な規定が追加された（第 32a 条 2 項）。
理事会	・データ保護影響評価の実施について、監督機関が実施すべきデータ処理のリストを決定し公表しなければならない、という規定の追加が検討されている（ダ 33 条 2a 項）。

（2）データ保護影響評価の導入背景

2009 年 5 月、欧州委員会が RFID におけるプライバシー及びデータ保護原則の実施に関する勧告を公表した[95]。同勧告に基づき、2010 年 7 月（2011 年 2 月改定）には第 29 条データ保護作業部会が RFID の適用におけるプライバシー・データ保護影響評価に関する意見[96]を公表するなどし、RFID におけるプライバシー・データ保護影響評価が確立していった。

また、欧米間でのプライバシー・データ保護をめぐる緊張が高まった旅客機の乗客データの記録の取扱いについて、2010 年 5 月には欧州議会がこの問題への新たな立法についてプライバシー影響評価の必要性を指摘した[97]。2010 年 7 月には欧州委員会副委員長兼司法総局コミッショナーが「データ保護担当者の任命、プライバシー影響評価の実施及び『プライバシー・バイ・デザイン』のアプローチの適用といった特定の構造」[98]を事業者及び公的機関に取り入れるよう呼びかけ、包括的なデータ保護影響評価への道が開かれていった。

---

95 European Commission, *Commission Recommendation of 12.5.2009 on the Implementation of Privacy and Data Protection Principles in Applications Supported by Radio-Frequency Identification*, 12 May 2009.

96 Article 29 Data Protection Working Party, *Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications*, WP175, 13 July 2010. なお、改訂版は 2011 年 2 月に公表されている。See Article 29 Data Protection Working Party, *Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications*, WP180, 11 February 2011.

97 European Parliament, *Resolution of 5 May 2010 on the Launch of Negotiations for Passenger Name Record (PNR) Agreement with the United States, Australia and Canada* (2011/C 81 E/12).

98 *See Viviane Reding Vice-President of the European Commission responsible for Justice, Fundamental Rights and Citizenship Towards a true Single Market of data protection Meeting of the Article 29 Working Party "Review of the Data protection legal framework", Brussels, 14 July 2010*. Available at http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/386 (last visited 27 March 2014)

また、エネルギー節約に関する指令（Directive on Energy End-Use Efficiency and Energy Services（2006/32/EC））において、加盟国はエネルギーの正確な消費を消費者に対してメーターで周知しなければならないことが定められている（第 13 条）。第 29 条作業部会は、同指令に基づき、スマート・メータリングに関するデータ保護の諸問題について 2011 年 4 月 4 日[99]、2013 年 4 月 12 日[100]そして同年 4 月 22 日[101]にそれぞれ意見を公表した。この意見の中では、スマート・グリッド専門化作業部会における研究を参照としつつ、プライバシー・バイ・デザイン、プライバシー強化技術、プライバシー影響評価といった概念が含まれている。

さらに、2013 年 6 月には、無人航空機システム（Remotely Piloted Aircraft System）の利用に関するプライバシー・バイ・デザインの導入とビデオ監視がもたらすプライバシー及びデータ保護影響評価の必要性が欧州委員会によって示されている[102]。

（３）プライバシー影響評価との異同

データ保護影響評価は、「個人データに関して想定される処理作業の影響の評価」（規則提案 33 条 1 項）と表記されており、少なくとも次の評価を含むとされる。①想定される処理作業の記述、②データ主体の権利及び自由に対するリスクの評価、③リスクに対処するための想定される措置、保護措置、セキュリティ措置と構造である（第 33 条 3 項）。プライバシー影響評価とデータ保護影響評価の関係については、それがプライバシーとデータ保護のとの関係に遡ることができるであろうが、両者は「決して同一の性質を有するものではない」[103]と一般的に考えられている。すなわち、「データ保護影響評価は本来的にコンプラインス・チェックであり、したがって、プライバシー影響評価よりもいくらかその範

---

99 Article 29 Data Protection Working Party, *Opinion 12/2011 on Smart Metering* (WP183, adopted on 4 April, 2011).

100 Article 29 Data Protection Working Party, *Opinion 07/2013 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* (WP 209, 12 April 2013).

101 Article 29 Data Protection Working Party, *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*, (WP205, 22 April 2013).

102 European Commission, *Roadmap for the integration of civil Remotely-Piloted Aircraft Systems into the European Aviation System: Final report from the European RPAS Steering Group: ANNEX 3 A study on the societal impact of the integration of civil RPAS into the European Aviation System*, June 2013 at 27 & 40.

103 Paul De Hert, *A Human Rights Perspective on Privacy and Data Protection Impact Assessment*, in PRIVACY IMPACT ASSESSMENT 34 (David Wright & Paul De Hert eds., 2012).

囲が制限されているのである」[104]。

なお、このリスク評価形態として、「プライバシー・バイ・デザイン（privacy by design）」、「データ保護バイ・デザイン」あるいは「データ保護バイ・デフォルト（data protection by default）」（規則提案第 23 条、30 条 3 項）が、データ主体の権利を擁護するためデータ処理の手段の決定時及び処理時点において適切な技術的・組織的安全管理措置を講じるべきものとして注目されてきている。同時に、「プライバシー・リスク管理（privacy risk management）」、「プライバシー・リスク分析（privacy risk assessment）」、「意図されたデータ処理の潜在的影響のリスク評価（a risk analysis of the potential impact of the intended data processing）」、という言葉が用いられることがある。「プライバシー・リスク管理」については、フランスデータ保護機関 CNIL がプライバシー・リスク管理という表現を使用している[105]。

（4）データ保護影響評価の内容

EU においては、データ保護影響評価それ自体がまだ「建設中」であり、具体的な内容は規則提案以外に示されていない。もっとも、ブリュッセル自由大学の Paul De Hert 教授らが欧州委員会司法総局の依頼により公表した勧告において、次の 12 要素がデータ保護影響評価の核心をなすべきであると考えられている[106]。それぞれの評価項目については、今後検討されていくものと考えられる。

① PIA が必要であるかどうかの決定（しきい値分析）
② PIA チームの認定と参照用語の決定
③ 提案された企画の描写
④ 情報流通およびその他プライバシー影響の分析
⑤ 利害関係者との相談
⑥ リスク管理
⑦ 法令遵守の確認
⑧ 勧告の定式化
⑨ 報告書の準備及び公表
⑩ 勧告の履行

---

104 Introduction to Privacy Impact Assessment, in PRIVACY IMPACT ASSESSMENT 8 (David Wright & Paul De Hert eds., 2012).
105 *See* Commission nationale de l'informatique et des libertés, *Guides Gestion des risques vie privée" (Methodology for Privacy Risk Management)*, 04 juillet 2012.
106 David Wright & Paul De Hert, *Introduction to Privacy Impact Assessment*, in PRIVACY IMPACT ASSESSMENT 12 (David Wright & Paul De Hert eds., 2012).

⑪　外部審査及び（又は）監査

⑫　企画変更に伴う PIA の改訂

Ⅴ．データ移転

１．十分性認定

（１）EU データ保護指令

・個人データの第三国への移転は、当該第三国が十分な水準の保護措置を確保している場合に限って、行うことができることを定めなければならない（第 25 条 1 項)。

・十分性のレベルは、データ移転作業に関するあらゆる状況にかんがみて評価されなければならない。特に、データの性質、予定されている処理作業の目的及び期間、発信国及び最終の目的国、当該第三国において有効である一般的及び分野別の法規範、並びに当該第三国において遵守されている専門的規範及び安全管理措置が考慮されなければならない（第 25 条 2 項)。

・第 31 条 2 項に規定する手続に基づく委員会が、第三国の十分な水準の保護の補償に関する認定をすることができる。また、第三国が十分な水準の保護を保障していないと認定した場合、当該第三国へのデータ移転を阻止するために必要な措置を講じなければならない（第 25 条 4 項・6 項)。

（２）EU データ保護規則提案

委員会	・データの移転は、委員会が十分な保護の水準であると認定した第三国、第三国の地域もしくは処理の分野、又は国際機関に対し行うことができる（第 41 条 1 項)。 ・十分な水準の保護の評価については、次の要素を考慮しなければならない。 a) 第三国又は国際機関が準拠する公の安全、防衛、安全保障、刑事法、専門的規則及び治安対策に関連する法の支配と立法、さらに EU 居住のデータ主体に対する効果的な行政・司法上の救済を含む執行可能な権利。 b) 第三国又は国際機関におけるデータ保護規則の遵守を確保し、データ主体の権利行使を支援・助言し、EU の監督機関との協力に責任を有する独立した監督機関の存在と効果的機能 c) 第三国又は国際機関による国際的な関与（第 41 条 2 項）

	・第三国又は国際機関における立法が EU 居住のデータ主体に対する強制力ある権利を保障していない場合、十分な水準の保護を行っていないという認定をすることができる（第 41 条 5 項）。
議会	・十分な水準の保護の評価については、a）立法の施行と司法の先例、b)監督機関の十分な制裁権限、c)法的拘束力ある文書への国際的な関与という文言がそれぞれ追加された（第 41 条 1 項 a 号～c 号）。 ・十分性の認定について、委員会が欧州データ保護委員会に意見を要請しなければならないという条項が追加された（第 41 条 6a 項）。 ・十分性の認定の効力は 5 年間とすることが追加された（第 41 条 8 項）。 ・EU 法で認められない移転又は開示の禁止に関する条項として、国際協定を除き、第三国の司法による判決及び行政による決定により管理者又は処理者に個人データを開示することができない条文が設けられた（第 43a 条 1 項）。 ・第三国の司法による判決及び行政による決定により個人データの開示が要請された場合、当該管理者又は処理者は遅滞なく監督機関に通知し、データ移転のための事前認可を得なければならない（第 43a 条 2 項）。
理事会	・十分な水準の保護の評価については、a）人権及び基本的自由の尊重、第三国又は国際機関からのデータの再移転に関する規則、b）監督機関の十分な制裁権限などの追加が検討されている（第 41 条 1 項 a 号・b 号）。 ・十分性の認定について、委員会が欧州データ保護委員会に意見を要請しなければならないという文言の追加が検討されている（第 41 条 3 項）。

（3）移転

データが第三国へ「移転」するとはどのようなことか。欧州司法裁判所 Bodil Lindqvist 判決[107]において、不特定多数の者に公開するインターネット掲示板は移転に該当せず、特定の名宛人に対しデータを移転する場合のみが EU データ保護指令の規制に服することが明らかにされた。本件では、スウェーデンにおける小さな教会コミュニティがインターネット上に公開した個人データについて第三国の市民がそれにアクセスすることができるとしても、「加盟国における個人がインターネットのページに個人データを掲載した場合、EU 指令 95/46 第 25 条の意味における『第三国への[データの]移転』があるとはいえない」とされたのである。

もっとも、同判決に対しては、インターネット上のデータがたとえ第三国に公開されて

[107] *Bodil Lindqvist*, C-101/01, 6 November 2003.

いるとしてもデータ移転とみなさなかったため、十分性認定なしにデータ移転が行える抜け道となりかねないという批判がある[108]。したがって、同判決個人が個人利用の目的でインターネットにデータを掲載した場合に限定しているとみるべきであり、この判決を広く解釈することは適切でない。

また、データの移転のみならず、いわゆる「データ・ヘブン」あるいは「データ・ショッピング」と呼ばれるように、十分性認定を受けた国・地域の経由にデータ転送についても問題とされる[109]。すなわち、EU 域内からのデータ移転を行う場合、十分性の認定を受けて国・地域へデータを一時的に移転し、そこから十分性認定を受けていない国へのデータを転送する場合は、実質的に十分性の要件が空文化されてしまうことになる。そこで、このようなデータの十分な保護水準を確保している第三国経由のデータの転送についてもまた EU 一般データ保護規則提案第 40 条では留意する規定が置かれることとなった。

（4）十分性審査の手続

欧州委員会による十分性審査については、1998 年 7 月 24 日、第 29 条作業部会が公表した「第三国への個人データ移転（EU データ保護指令第 25 条及び第 26 条の適用）に関する作業文書」[110]に基づき審査が行われる。欧州委員会によるヒアリングによれば、この作業文書は現在も有効であり、規則提案が発効するまではこの文書で示された審査を行うこととなる。審査の基準として、データ保護に関する「内容の原則」と「手続・執行の構造」の二点がある。

①内容の原則について

a) 利用制限の原則…データは、特定の目的に処理され、利用されるべきである。（指令 13

---

108 Cécile de Terwangne, *C.J.C.E., 6 novembre 2003: Protection des Données à Caractère Personnel - Champs d'application de la Directive 95/46 - Internet - Transfert de Données vers des Pays Tiers - Liberté d'expression*, 19 REVUE DU DROIT DES TECHNOLOGIES DE L'INFORMATION, 67,80 (2004).

109 *See* Els De Busser, *The Adequacy of an EU-US Partnership*, in EUROPEAN DATA PROTECTION: IN GOOD HEALTH 193 (Serge Gutwirth et. al., 2012).

110 Article 29 Data Protection Working Party, *Working Document: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive*, (WP12 adopted on 24 July 1998). 消費者庁・前記報告書、参照。また、EU の十分性審査の観点から日本の法制度を考察するものとして、藤原静雄「個人情報保護法制とメディア」小早川光郎ほか編『行政法の発展と変革上巻』（2001）713 頁、新保史生「個人情報保護マネジメントシステム」法とコンピュータ 25 号（2007）73 頁、村上裕章「国境を越えるデータ流通と個人情報保護」川上宏二郎先生古稀記念論文集刊行委員会編『情報社会の公法学』（信山社・2002）118 頁、など参照。データ移転一般論については、鈴木正朝「他国への個人データ越境移転制限条項の検討」ジュリスト 1464 号（2014）59 頁、参照。

条）

b) データの質及び比例の原則…データは、正確かつ最新のものとすべきである。

c) 透明性の原則…各人に対し、データ処理の目的及びデータ管理者に関する情報を提供すべきである。（指令 11 条２項、同 13 条）

d) 安全の原則…技術的かつ組織的な安全管理措置が、データ管理者により施されるべきである。

e) アクセス・訂正・異議申立の権利…データの本人は、自らに関する全てのデータのコピーを取得し、不正確な場合には、訂正する権利を有すべきである。また、一定の場合は、データの処理に異議申立を行うことができるようにすべきである。

f) 移転の制限…データの移転に際しては、データの受取側が十分な保護の水準を確保している場合のみに行うべきである。

なお、（ｉ） センシティブ・データ（指令 8 条に列挙された人種、民族出自、政治的思想、宗教上・哲学上の信念、労働組合員、健康・性生活に関するデータ）、（ii）ダイレクト・マーケティング（オプト・アウトの要件）、（iii） 個人の決定（データ移転に関する本人の知る権利）、が補足的な原則として保護水準の十分性の判断に考慮されうる

②手続・執行の構造

a) 法令遵守（コンプライアンス）の十分な水準の確保…十分な体制は一般にデータ管理者の義務とデータ本人の権利と権利行使の手段に対する高い意識がある。

b) データの本人に対する支援と援助の提供…個人は法外な費用をかけることなく、迅速かつ効果的に自らの権利を執行することができなければならない。

c) 適切な救済の実施…独立した裁定又は仲裁により、法令違反をした当事者に対して損害賠償と罰則を科すことができる体制が関与しなければならない。

これら①内容の原則と②手続・執行の構造について、第三国・地域の審査を実施してきているが、その多くがベルギー・ナミュール大学（Université de Namur, Facultés universitaires Notre-Dame de la Paix）法・情報・社会研究所（Centre de Recherche Information, Droit et Société）に委託されて、調査が行われてきた。

（５）十分性認定を受けた国・地域

欧州委員会からの十分性審査については、いわゆるホワイト・リストとブラック・リストがある。すなわち、十分性審査の結果、データの移転　が認められる第三国のホワイト・リストと、データ移転が禁止される第三国のブラック・リストである。これまでのところ、

スイス[111]、カナダ[112]、アルゼンチン[113]、ガンジー島[114]、マン島[115]、ジャージ島[116]、フェロー諸島[117]、アンドラ[118]、イスラエル[119]、ウルグアイ[120]、ニュージーランド[121]の 11 の国・地域が通常審査によるホワイト・リストに掲載されている（2014 年 3 月時点）。これに対し、「ブラック・リストの国を明示的に列挙することは政治的に極めてセンシティブ」[122]であることから、ブラック・リストに正式に指定された国は存在していない。もっとも、後に紹介するとおり、議会の決議により、NSA の監視活動に協力を行ったニュージーランドとカナダの十分性認定については停止とともに再調査の必要性が示されている。

なお、セクトラル方式で法整備を進める米国においては、EU データ保護指令への準拠が困難であることから、2000 年 7 月 26 日付の欧州委員会の決定により「セーフハーバー原

111 European Commission, *Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland* (2000/518/EC).
112 European Commission, *Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act* (2002/2/EC).
113 European Commission, *Commission Decision of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina C (2003) 1731.*
114 European Commission, *Commission Decision of 21 November 2003 on the adequate protection of personal data in Guernsey* (2003/821/EC).
115 European Commission, *Commission Decision 2004/411/EC of 28.4.2004 on the adequate protection of personal data in the Isle of Man.*
116 European Commission, *Commission Decision of 8 May 2008 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Jersey* (2008/393/EC).
117 European Commission, *Commission Decision of 5 March 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection provided by the Faeroese Act on processing of personal data* (2010/146/EU).
118 European Commission, *Commission Decision of 19 October 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Andorra* (2010/625/EU).
119 European Commission, *Commission Decision 2011/61/EU of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data* (2011/61/EU).
120 European Commission, *Commission Implementing Decision of 21 August 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal data* (2012/484/EU).
121 European Commission, *Commission Implementing Decision of 19 December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand* (2013/65/EU).
122 Article 29 Data Protection Working Party, *Discussion Document on First Orientations on Transfers of Personal Data to Third Countries Possible Ways Forward in Assessing Adequacy*, (WP4, adopted on 26 June, 1997) at 4.

則（Safe Harbour Principles）」に基づく協定を締結した[123]。また、第 29 条作業部会の 2001 年 1 月 26 日の意見において、オーストラリアが一定の条件を満たさない限り、十分な保護措置を確保しているとは認められない、というネガティブな評価が下されている[124]。米国とオーストラリアはこのほかに旅客機の乗客データの移転について、欧州委員会と別途協定を締結している[125]。

（6）第三国の司法判決・行政決定による開示禁止―議会修正案第 43a 条

NSA 問題を受け、議会は新たに第三国の司法判決や行政機関の決定による場合であっても、原則として EU 域内の管理者又は処理者による個人データの開示を禁止する条項を設けた。この条項は米国 NSA 問題が念頭に置かれていることから、この点については、「米国との関係」、を参照。

２．拘束的企業準則

（1）EU データ保護指令

・明文規定なし。

（2）EU データ保護規則提案

委員会	・監督機関は、以下の要件を満たした場合、拘束的企業準則を承認する。 a）法的拘束力があり、管理者又は処理者のすべての従業員に適用される b）データ主体に対し執行可能な権利を付与している c）第 2 項の条件を満たしている（第 43 条 1 項）

123 *See* European Commission, *Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently questions issued by the US Department of Commerce* (2000/520/EC).

124 *See* Article 29 Data Protection Working Party, *Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000* (WP40, adopted on 26 Jan., 2001).

125 *See Agreement between the European Community and the United States of America on the processing and transfer of PNR data by air carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, Signed in Washington on 28.5.2004* （この協定は 2006 年と 2007 年に更新されている）；*Agreement between the European Union and Australia on the processing and transfer of European Union sourced passenger name record (PNR) data by air carriers to the Australian customs service; OJ L213 of 08/08/2008.* この点については、内閣府『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』（2009 年 3 月）265-7 頁、参照。

	・拘束的企業準則には次の事項が特定されていなければならない。 a) 事業の体制、連絡先、メンバー b) データ移転（個人データの類型、処理の種類と目的、データ主体の種別、第三国） c) 国内・国際的な法的拘束力の性質 d) データ保護の一般的原則（利用目的の制限、データの質、処理の法的根拠、センシティブ・データの処理、セキュリティ措置、再移転の要件） e) データ主体の権利とその行使方法 f) EU 以外における事業者による違反の場合の加盟国内に設置された管理者又は処理者による責任負担 g) d, e, f 号に関する情報がデータ主体に透明性をもって提供される方法 h) データ保護担当者の任務 i) 拘束的企業準則の遵守を検証する体制 j) 方針変更を監督機関に通知する体制 k) 事業グループの法令遵守を確保するための監督機関との協力体制（第 43 条 2 項）
議会	・雇用データについても拘束的企業準則に含まれることが追加された（第 43 条 1a 項）。 ・拘束的企業準則に含まれる事項について、データ最小限化、データ保存期間、データ保護バイ・デザインの原則が追加された（第 43 条 2 項 d 号）。
理事会	・拘束的企業準則に含まれる事項について、苦情申立の手続の追加が検討されている（第 43 条 2 項 hh 号）。

（3）拘束的企業準則の要件と手続

拘束的企業準則とは、国際データ移転に関する法的拘束力を有し、データ主体に対し執行可能な権利を付与している企業準則である[126]。EU では 2003 年以降、第 29 条作業部会の作業文書として拘束的企業準則によるデータ移転を充分な保護水準にあるものとして運用してきた。もっとも、従来の作業文書が指定する項目を各加盟国のデータ保護監督機関が審査し、認定するという手続であると、運用面のばらつきが生じうるため、規則提案において明文化された（第 43 条）。

126 拘束的企業準則については、消費者庁「国際移転における企業の個人データ保護措置調査」（2010 年 3 月）58 頁以下（「BCR の制度的概要」（石井夏生利執筆）参照。

（４）拘束的企業準則の運用

2014 年 3 月現在、48 社が拘束的企業準則の承認を受けた企業として一覧が掲載されている[127]。承認を付与した監督機関の加盟国別では、イギリス 17 社、フランス 17 社、オランダ 8 社をはじめ、ドイツ、ルクセンブルク、アイルランド、デンマークにおいても承認が行われている。

（５）APEC における越境プライバシー・ルールとの相互運用に向けた取組

第 29 条作業部会は 2014 年 2 月 27 日に、相互運用性（interoperability）の促進の観点から、EU における拘束的企業準則（BCR）と APEC における越境プライバシー・ルール（CBPR）の Accountability Agent の要件について比較考察を行った意見を公表した[128]。この意見によれば、BCR と CBPR には認証の要件において「重大な違い」がみられ、また目的、範囲、審査手続においても差異が認定された。結果として、BCR と CBPR の要件は完全には両立できない、と指摘されている。そのため、グローバル企業は EU で事業展開する際の要件と APEC 地域で展開する際に要求される要件をそれぞれ考慮に入れる必要がある。

EU 関係者からのヒアリングにおいても、依然として、EU と APEC の間の相互運用性が現実のものになるには相当な時間を要する、との指摘があった。また、APEC 会合に出席している欧州データ保護監督機関の国際担当者からも、経済・商業分野を所管する政府関係者が中心となる APEC の議論には人権という発想が欠けており、法務関係者から構成される EU における議論とは性格が異なることが指摘された。

４．米国との関係

（１）セーフハーバー決定（Safe Harbour decision）

セーフハーバー決定とは、米国商務省が示した「セーフハーバー・プライバシー原則」と「セーフハーバー・プライバシー原則に関するよくある Q&A」に基づくデータ移転について、十分な保護水準に該当する認定された欧州委員会による決定である。欧州委員会が

---

127 European Commission, *List of companies for which the EU BCR cooperation procedure is closed*. Available at http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm (last visited 27 March 2014).

128 Article 29 Data Protection Working Party, *Opinion on a "Referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents*, (WP212) adopted on 27 February 2014.

2000 年 7 月 26 日に決定し、2000 年 11 月 1 日に発効した[129]。これにより、米国商務省が申請した企業のセーフハーバー・プライバシー原則に適合しているか審査の上、認証を行い、その一覧（2013 年 9 月現在、3246 社が掲載）を公表している。セーフハーバーのプライバシー原則には、次の 7 原則が定められている[130]。

①通知…取得・利用の目的、連絡先、第三者の類型、個人に付与された選択と手段

②選択…オプト・アウトの機会の提供

③再移転…再移転のための通知及び選択

④セキュリティ…紛失、誤用、不正なアクセス・開示、改変・破壊からの保護

⑤データの完全性…目的の範囲内での利用、正確性・完全性・最新性のための措置

⑥アクセス…企業が保有する個人情報へのアクセス、訂正、修正、消去

⑦執行…a）苦情・紛争の調査、損害賠償、b）実施のフォローアップ、c）救済の義務

セーフハーバーのプライバシー原則に違反した場合、米国連邦取引委員会が不公正又は欺瞞的な行為又は慣行への執行権限を有しており、プライバシー原則の履行を担保することとされている（なお、連邦取引委員会以外にも、連邦運輸省が所管する分野においても同省の執行権限が認められる）[131]。また、EU 加盟国はプライバシー原則の履行をしていない企業とのデータ移転を停止する権限を行使することができる（セーフハーバー決定第 3 条 1 項）。

EU データ保護指令が加盟国において施行されようとしていた当時、米国では、インターネットの台頭を受け、「自主規制によるプライバシー体制」をクリントン政権が示したばかりであった[132]。対照的に、EU では包括的で法執行に担保されたデータ保護法制の施行を準備していたところであった。EU と米国のプライバシーをめぐる衝突は、具体的な法制度の違いという点においてこの当時に遡ることができる[133]。以下、欧州委員会によるセーフハ

---

129 European Commission, *Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce*, 26 July 2000.

130 *Id at Annex I: Safe Harbor Privacy Principles issued by the US Department of Commerce on 21 July 2000.*

131 *Id at Annex: List of U.S. Statutory Bodies Recognized by the European Union.*

132 The White House, *A Framework for Global Electronic Commerce*, July 1997. Available at http://clinton4.nara.gov/WH/New/Commerce/read.html (last visited 27 March 2014).

133 米国とヨーロッパの衝突について、法制度以外にも、米国の制限政府の伝統とヨーロッパの身分制社会やナチスによる個人情報管理を原因とする、自由と尊厳をめぐる文化的な側面の異同を論じたものとして、宮下紘「プライバシーをめぐる米国とヨーロッパの衝突―自由と尊厳の対立（１）」比較法文化 18 号（2010）131 頁以下、参照。また、日本の「個人情報保護法基本法制に関する大綱の策定作業も、諸外国の法制・立法動向と EU・米国間

ーバー決定に至るまでの交渉の経緯とその後の調査過程についてまとめておいた。

セーフハーバー決定に至るまでの経緯及び調査過程

1998 年 10 月 24 日	EU データ保護指令の加盟国における施行
1998 年 11 月 4 日	米国商務省が産業界にセーフハーバー案を提示
1999 年 1 月 26 日	EU 作業部会が米国商務省との交渉過程に関する意見公表
1999 年 5 月 3 日	EU 作業部会が米国提案のセーフハーバー原則の検討結果による不十分な点の公表（6 月 7 日にはよくある Q&A の検討の検討結果公表）
2000 年 3 月 14 日	米国商務省が欧州委員会域内市場局とセーフハーバーの仮合意に至ったことを公表
2000 年 5 月 31 日	EU 第 31 条委員会の決定によりセーフハーバー枠組みが決定
2000 年 7 月 5 日	欧州議会がセーフハーバー原則が十分性審査を満たすと認定されない決議を採択（賛成 279 票、反対 259 票、棄権 22 票）
2000 年 7 月 21 日	米国商務省がセーフハーバー・プライバシー原則等を公表
2000 年 7 月 26 日	欧州委員会によるセーフハーバー・プライバシー原則等を十分な保護水準にあると認定
2000 年 11 月 1 日	セーフハーバー枠組みの発効
2002 年 2 月 13 日	欧州委員会によるセーフハーバーの施行状況調査が公表（実態面における問題点が指摘）
2004 年 10 月 20 日	欧州委員会によるセーフハーバーの施行状況調査が公表（実態面における問題点が指摘）
2005 年 7 月 25 日	欧州委員会がよくある Q&A に関する追加説明を公表
2012 年 3 月 19 日	欧州委員会副委員長と米国商務長官による共同声明でセーフハーバーの継続を表明
2012 年 8 月	連邦取引委員会が 10 社の調査結果を公表（2009 年～2012 年）

EU と米国のセーフハーバーの交渉は約 2 年間にも及び、異なる法制度の間のデータ移転の枠組み構築の難しさが明らかになった。さらに、交渉を長期化させた要因として、「1998

の交渉を睨みながらのものであった」という指摘がある。藤原静雄「個人情報保護法と諸外国の個人情報保護法制」園部逸夫編『個人情報保護法の解説〔改訂版〕』（ぎょうせい・2005）306 頁、参照。

年の春の時点では、米国があらゆる分野において十分なプライバシー保護の欠如が見られるとの一般的認定を下す可能性は極めて低い。そのような無愛想な認定を行えば、深刻な政治問題をもたらし、貿易戦争を引き起こすことになろう」[134]との楽観的な見方が支配していたものと考えられる。結局、米国の戦略的な外交・ロビー活動とバーゲニング力を背景とした政治的な妥協によって生み出されたのがセーフハーバーである。そして、「セーフハーバーの最大の功績は大西洋における大きな貿易衝突を回避できたことである」[135]と言われる。

また、米国のグローバル企業が、国内では米国法基準、ヨーロッパでは EU 法基準という二重の基準を回避し、「one-stop-shop」を実現できるという意味において、さらには、米国では包括的なプライバシー法制が欠如する中、「スイス・チーズ」（固くて大きな穴だらけのチーズ）の穴を埋め合わせることができる意味において、セーフハーバーは米国にとって絶好の道具であった[136]。

このようなセーフハーバー決定について、欧州委員会は 2002 年 2 月（2001 年 12 月時点の 129 社が対象）と 2004 年 10 月（2003 年 11 月時点の 403 社が対象）にセーフハーバーの原則の遵守状況について調査結果を公表した[137]。なお、2004 年 10 月の委員会による公式な報告に際して、欧州委員会の依頼によりナミュール大学の研究者が米国の研究者と共同で具体的な調査結果を公表している[138]。これらの調査結果には、①セーフハーバー・プライバシー原則を遵守していること又はプライバシー・ポリシーが公表されていないこと、②仮にプライバシー・ポリシーが公表されていても、セーフハーバー原則を反映していないこと、③プライバシー原則がどのように適用されているかの透明性がないこと、④プライバシー原則違反の制裁を含む法執行による担保の例がみられないことなど、セーフハーバーの「欠陥」が指摘されている。また、裁判外紛争処理として、いくつかの機関（TRUSTe、

---

134 PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 44 (1998).

135 DOROTHEE HEISENBERG, NEGOTIATING PRIVACY: THE EUROPEAN UNION, THE UNITED STATES, AND PERSONAL DATA PROTECTION 96 (2005)

136 *Interview with FTC Commissioner Mozelle Thompson*, Antitrust, spring, 2002 at 25 (Comment by Commissioner Thompson).

137 *See* European Commission, *The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerc*e, 13 February 2002；European Commission, *Commission Staff Working Document: The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce*, 20 October 2004.

138 European Commission, Safe Harbour Decision Implementation Study 19 April 2004

Direct Marketing Association Safe Harbour Program 、 BBBOnline 、 American Arbitration Association）がプライバシー原則違反の恐れがある場合、EU 市民に対し仲裁手続を提供しているが、申立の時点で 200～250 ドルの費用を要し、さらに手続を進めると追加費用が必要となる。欧州消費者団体のヒアリングにおいても、EU 市民が抽象的なプライバシー原則の米国側による解釈の下、消費者に非好意的で高額な米国の仲裁に申し立てる例はないため、効果的な救済構造であるとはみなされていないとのことであった[139]。これまでセーフハーバーの法執行を怠ってきた米国連邦取引委員会は、2009 年から 2012 年の認証を受けた企業の中でプライバシー原則を履行していない企業 10 社を公表したが、そのうちの 7 社が認証更新を行ったことによる原則違反であった[140]。2013 年の調査によれば、認証を受けている企業のうち約 10%の 427 社が虚偽表示をしているという結果も報告されている[141]。議会のヒアリングにおいても、2000 年 7 月の委員会の決定直前に十分性を否定する決議を採択しており、セーフハーバーはその決定当初から現在に至るまで不信と不満があり、委員会がただちに停止すべきである、という厳しい態度であった。

他方で、米国側セーフハーバーの商務省担当官によれば、セーフハーバーは「米国国内におけるプライバシー法令遵守の水準の向上の観点においても、またプライバシーがグローバル市場での成功を収める不可欠な要因であることを米国の企業による認識の促進においても、目覚ましい成功であり続けてきた」[142]と指摘されている。また、EU とのセーフハーバー継続の交渉に際し、オバマ政権は欧州連合米国代表部の大使にプライバシー問題に精通している前連邦通信委員会委員長を任命し、大使はブリュッセルにてセーフハーバーの意義を「革新的で成功の枠組み」[143]と評価している。

（２）旅客機乗客データ

2001 年 9 月 11 日の米国における同時多発テロを受け、同年 11 月 19 日に成立した航空運輸安全保障法に基づき、米国運輸保安局と国土安全保障省がテロリスト容疑者の事前ス

---

139 *See* BEUC, *Posititon Paper on EU Cloud Compurting Strategy* (2013) at 10. *See also Position Paper on Data Protection: Proposal for a Regulation* (2012) at 30; Galexia, *The US Safe Harbor: Fact or Fiction?* (2008) at 13.

140 *See Federal Trade Commission Enforcement of Safe Harbor Commitments*. Available at http://export.gov/build/groups/public/@eg_main/@safeharbor/documents/webcontent/eg_main_052211.pdf (last visited 27 March 2014).

141 Galexia, *EU/US Safe Harbor: Effectiveness of the Framework in relation to National Security Surveillance* (2013) at 4.

142 Damon Greer, *Safe Harbor: A Framework that Works*, 1 INT'L DATA PRIVACY L. 143, 147 (2011).

143 *See e.g.*, William E. Kennedy, *Remarks*: Forum Europe's 3rd Annual European Data Protection and Privacy Conference, 4 December 2012.

クリーニングを実施する目的で、米国運輸保安局は米国を離発着する航空会社に対し航空機の乗客名簿の事前提出を義務付けることとなった[144]。乗客データには、氏名、生年月日等の情報のほかに支払情報（クレジットカード番号）や特別要求サービス情報（食事制限、車椅子の必要性）などの 19 項目の情報を含むものとされている[145]。同様の措置はカナダやオーストラリアでも採用された。

そこで、EU では欧州委員会が米国国土安全保障省との交渉にあたり、2003 年 12 月には欧州委員会が乗客データの移転に関する十分性認定を行うことを決定した[146]。もっとも、第 29 条作業部会のレベルでは、2002 年の意見においてすでに乗客データの収集が比例原則に照らして適切でないことなどから米国側との交渉の必要性を指摘し[147]、また 2004 年 1 月には航空機乗客データに関する協定が十分性認定の枠組みで議論すべきでないことを意見として表明した[148]。さらに、議会からも委員会の決定案を認めない決議[149]が採択されてしまい、EU 内部でも足並みのそろわない中、2004 年 5 月 17 日に理事会決定により乗客データの処理と移転に関する決定が下され、同年 5 月 28 日に米国との協定が署名された[150]。これに対し、議会は委員会及び理事会の決定の取り消しを求め、欧州司法裁判所での審理を求めた。2006 年 5 月 30 日に下された欧州司法裁判所の判決では、安全保障分野を除外している EU データ保護指令第 25 条に基づき協定を締結する権限がないため、委員会及び理事会の決定が無効であると判断を下した[151]。ただし、判決は、委員会と理事会の決定を

---

144 *Aviation and Transportation Security Act*, Pub. L. No.107-71, 115 Stat. 597 (2001).
145 Department of Homeland Security, U.S. Customs and Border Protection Passenger Name Record (PNR) Privacy Policy, June 21, 2013.
146 European Commission, *Communication from the Commission to the Council and the Parliament: Transfer of Air Passenger Name Record (PNR) Data: A Global EU Approach*, 16 December 2003 at 11
147 Article 29 Data Protection Working Party, *Opinion on transmission of Passenger Manifest Information and other data from Airlines to the United States* (WP66), adopted on 24 October 2002 at 8.
148 Article 29 Data Protection Working Party, *Opinion on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP)* (WP87), adopted on 29 January 2004 at 12.
149 European Parliament, *Resolution on the draft Commission decision noting the adequate level of protection provided for personal data contained in the Passenger Name Records (PNRs) transferred to the US Bureau of Customs and Border Protection*, 22 March 2004.
150 European Council, *Council Decision of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection*, 17 May 2004.
151 CJEU, *European Parliament v. Council of the European Union & Commission of the European Communities*, C-317/04 & C-318/04, 30 May 2006.

2006 年 9 月 30 日までは有効とした。

この欧州司法裁判所の判決によって、2006 年 9 月 30 日以降、EU 域内の航空会社は、乗客データを米国国土安全保障省に提供すれば、EU データ保護指令の基本原則違反に問われ、また、提供しなければ、米国空港での離発着を拒否されるという深刻な状況に置かれることになった。そこで、2006 年 10 月に EU と米国の間で暫定協定として、2007 年 7 月 31 日まで有効な協定を改めて締結した[152]。その後、EU と米国の間で継続的な交渉が行われ、2007 年に 7 年間継続の新たな協定[153]合意に至り、さらにリスボン条約の後、2011 年 12 月 14 日に継続協定[154]の合意に署名した。なお、規則提案には、十分性審査の基準に安全保障に関するデータ移転を含めていることから、規則提案が発効されることになると、改めて乗客データの移転が十分性審査の対象となりうるので留意が必要である。

米国側からは国土安全保障省が、2012 年 7 月から 2013 年 8 月の 1 年間では、乗客データのうち 0.002 %のみが更なる調査対象となっていたことや 27 件の乗客データに特化した情報公開請求があったことなど EU のプライバシー原則からみて大きな問題がないことなどを報告書にまとめている[155]。

なお、乗客データの移転の問題は、EU と米国の間でのみ問題となっているわけではなく、データ保護プライバシー・コミッショナー国際会議の非公開セッションにおいても重要な審議事項として位置づけられてきた[156]。

（3）SWIFT 及びテロリスト金融追跡プログラム

SWIFT （Society for Worldwide Interbank Financial Telecommunication（国際銀行間通信協会））とは、電信による送金サービス等を行うため、2014 年 2 月現在、毎日約 2150

---

[152] *Agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security*, 27 October 2006.

[153] *Agreement Between the United States of America and the European Union on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (DHS)*, July 23-26, 2007.

[154] *Agreement Between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security*, 14 December 2011.

[155] U.S. Department of Homeland Security, *A Report on the Use and Transfer of Passenger Name Records Between the European Union and the United States*, 3 July 2013.

[156] 29th International Conference of Data Protection and Privacy Commissioners, *Resolution on the urgent need for global standards for safeguarding passenger data to be used by governments for law enforcement and border security purposes*, 28 September 2007. Available at http://privacyconference2011.org/htmls/adoptedResolutions/2007_Montreal/2007_M3.pdf (last visited 27 March 2014).

万通の電信を処理し、世界中 10,000 以上の金融機関の通信を取り扱うネットワーク運営組織である[157]。このネットワーク・オペレーション・センターが米国にはワシントンと EU にはブリュッセルにそれぞれ存在するが、SWIFT はベルギーに拠点を置く協同組合であることから、データ移転に際しては EU データ保護指令の規制に服することになる。2006 年 6 月に中央情報局（CIA）のプログラムの一環で米国財務省外国資産管理室がテロリストへの金融送金防止の目的で電信データを監視していたことが報じられた[158]。

これを受け、EU では、2006 年 7 月に議会が米国財務省による EU データ保護指令に違反した行為を非難する決議[159]を採択し、委員会では第 29 条作業部会が中心となって本件調査を行った。ベルギーのデータ保護監督機関による調査も行われ、「個人データを米国及び米国財務省に移転する全体の過程を取り巻く不透明かつ十分でもなければ効果的でもない措置は、EU データ保護指令に照らし重大な違反となり」、「データ保護に関するヨーロッパの基本原則に違反する」[160]と認定した。2007 年 6 月以降、委員会と理事会が米国財務省との SWIFT 問題に対処するための交渉を開始した[161]。

その後、委員会の提案に議会が拒否するなど EU 内部での合意に至るまでに時間を要したが、2010 年 7 月に理事会の決定によりテロリスト金融追跡プログラムを目的とした欧州連合と米国の間の金融電信データの処理及び移転に関する協定が 2010 年 8 月 1 日発効された[162]。同協定には、ユーロポールによるデータ処理及び移転に関する比例原則が規定されており、必要最小限のデータが処理・移転されているかどうかユーロポールによるチェック機能が担保されている（第 4 条）。また、同協定に関する施行状況の報告書が公表される

---

157 Society for Worldwide Interbank Financial Telecommunication, *SWIFT in Figures*, February 2014. Available at http://www.swift.com/assets/swift_com/documents/about_swift/SIF_2014_02.pdf (last visited 27 March 2014).

158 *See e.g.*, *Bank Data Shifted in Secret by U.S. to Block Terror*, N.Y. TIMES, 23 June 2006 at A6; *Bank Records Secretly Tapped; Administration Began Using Global Database Shortly After 2001 Attacks*, WASH. POST, 23 June 2006 at A1; Treasury Tracks Financial Data in Search Effort, WSJ, 23 June 2006, at A1.

159 European Parliament, *Resolution of 6 July 2006 on the interception of bank transfer data from the SWIFT system by the US secret services*, 6 July 2006.

160 Article 29 Data Protection Working Party, *Opinion on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)* (WP128), adopted on 22 November 2006 at 26-27. *See also* Commission de la protection de la vie privée, *Decision on Control and recommendation procedure initiated with respect to the company SWIFT scrl*, 9 December 2008.

161 *See US Federal Register*, vol. 72 No. 204, 23 October 2007 at 60065-60066.

162 Council Decision 2010/412/EU of 13 July 2010 on Agreement between the European Union and the United States of America on the Processing and Transfer of Financial Messaging Data From the European Union to the United States for Purposes of the Terrorist Finance Tracking Program, 13 July 2010.

とともに、3 年後に再評価が要求されている。そのような 3 年後の再評価を前にして NSA 問題が明らかになり、2013 年 10 月 23 日、議会は同協定の停止を要求する決議が採択された[163]。

（4）NSA 問題

① 委員会と議会の対応

2013 年 6 月 6 日、米国国家安全保障局（National Security Agency）が秘密裏に電話会社から数百万人もの米国人の通話記録を収集していたことが明らかになった[164]。この事実は、電話会社からのメタデータの収集のみならず、EU を含む世界中のインターネットの通信履歴や各国の首脳や大使を対象とした盗聴までもが明らかになった。

このスキャンダルに強く非難したのが EU であった。Reding 欧州委員会副委員長は、ニューヨーク・タイムズ（オンライン版）において「またやりました。またプライバシーの基本的権利への違反です。また市民の抗議です。また個人データの安全の市民の信頼を棒に振りました。」[165]とただちに米国による EU 市民のプライバシー侵害を痛烈に批判した。

さらに、Reding 副委員長は、2013 年 6 月 10 日に米国 Eric Holder 司法長官宛ての書簡で PRISM 問題について質問を行い、また 6 月 13－14 日にかけてダブリンでの Reding 副委員長と Holder 司法長官との閣僚会合の場で PRISM スキャンダルの事実を直接問いただした[166]。また、PRISM 問題を調査するための作業部会を設け、PRISM 問題による信頼回復が EU と米国の貿易協定の協議の前提になることも示した。

欧州議会もまた 2013 年 7 月 4 日に NSA による監視プログラムを非難する決議を採択し

---

163 European Parliament, European Parliament resolution of 23 October 2013 on the suspension of the TFTP agreement as a result of US National Security Agency surveillance, 23 October 2013.

164 *See NSA Collecting Phone Records of Millions of Verizon Customers Daily*, 6 June 2013, The Guardian Online (Available at http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (last visited 27 March 2014)); *NSA slides explain the PRISM data-collection program*, Wash. Post Online, 6 June 2013 (Available at http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (last visited 27 March 2014)) . *See also US Admits Secret Surveillance of Phone Calls Has Gone on for Years*, THE GUARDIAN, 7 June 2013 at 1 & 4; *U.S. mines Internet Firms' Data, Documents Show*, WASH. POST, 7 June 2013 at A1 & A12-14.

165 Viviane Reding, *Protecting Europe's Privacy*, N.Y. Times Online, 17 June 2013. Available at http://www.nytimes.com/2013/06/18/opinion/global/viviane-reding-protecting-europes-privacy.html?_r=0&pagewanted=print (last visited 27 March 2014).

166 Viviane Reding, *Speech: PRISM Scandal: The Data Protection Rights of EU Citizens Are Non-Negotiable*, 14 June 2013.

た[167]。同決議には、PRISM 及びその他のプログラムへの深刻な憂慮と EU 外交官へのスパイ活動への強い非難が示されているとともに、委員会によるセーフハーバーの見直しの要求が記述されている。さらに、議会では当時規則提案の審議中であり、NSA 問題を受け、新たに第 43a 条という条項を設け、第三国の司法判決や行政機関の決定による場合であっても、原則として EU 域内の管理者又は処理者による個人データの開示を禁止した。

② 特別作業部会

EU－US データ保護特別作業部会が設置され、4 回の会合を経て、11 月の閣僚会合までに調査報告書を取りまとめた。EU 側からは、委員会及び理事会議長国のほか第 29 条作業部会議長及び 10 名の専門家などが、また米国側からは司法省、国家情報長官室、国務省、国土安全保障省の担当官がそれぞれ構成員となった。2013 年 11 月 27 日に公表された「EU－US データ保護に関する特別作業部会の EU 共同議長による認定に関する報告書」[168]によれば、特に外国人が対象となる外国諜報活動監視法第 702 条について次の点で EU 側から見てデータ保護に関する問題が指摘された。

第 1 に、米国と EU では個人データの「処理」の概念が異なる。すなわち、EU 法の下では、データの取得自体が個人データの「処理」の一形態であると解され、データ主体の開示等の権利が適用されるのに対し、米国法では人為的な介入による分析が行われた場合のみ「処理」と限定的に理解されている。

第 2 に、外国諜報活動監視裁判所は、個々の令状を発給するのではなく、司法長官と国家情報長官の要請に基づき、認証という形で監視を承認しているが、この認証の実態については明らかにされていない。

第 3 に、外国人の監視について、ターゲットとされた特定の手続に服することとなるが、この手続きの評価基準やデータ収集の最小限化について米国側から確たる回答が得られなかった。なお、米国側によれば 1.6%の全世界のインターネット・トラフィックが取得され、そのうちの 0.025%が審査の対象となっている。

第 4 に、データ保全の観点からは、データの保存期間が原則 5 年となっているが、データが消去されたかどうかを確認する手段がない。

第 5 に、データベースに蓄積されたデータへのアクセスは限定されているが、刑事事件の可能性がある場合は情報共有が行われるおそれがある。

---

167 European Parliament, *US NSA surveillance programme, surveillance bodies in various Member States and impact on EU citizens' privacy*, 4 July 2013.
168 European Commission & the Presidency of the Council, *Report on the Finding by the EU-US Co-chairs of the ad hoc EU-US Working Group on Data Protection*, 27 November 2013.

第 6 に、不当な監視に対して、米国人は合衆国憲法の適用が及ぶが、事後的に刑事事件とならない限り、EU 市民には及ばない。

第 7 に、監視について対象となる市民の数量的制限がない。

これらの問題点のほかにも、愛国者法第 215 条に基づく監視の問題点も列挙されており、異なるデータ保護の水準で異なる類型のデータが異なる段階で監視の対象となっていることが理解できる。なお、報告書には米国側の諜報活動への支障が出るおそれがあるため、いくつかの項目については回答がされていない。

この報告書が公表される 2 週間ほど前の 2013 年 11 月 18 日、Reding 副委員長と Holder 司法長官らがワシントンでの閣僚会合後に、法執行分野におけるデータ保護の包括的協定の促進することを確約した旨共同プレス声明を公表している[169]。

委員会と理事会議長国による報告書とは別に、議会は米国の監視活動を強く非難し、司法内務問題に関する米国との協力に関する決議を 2014 年 3 月 12 日に採択した（賛成 544 票、反対 78 票、棄権 60 票）[170]。その決議には、単に米国による監視活動を非難するだけでなく、以下で示すとおり加盟国がセーフハーバーの「即時停止する（immediately suspend）」ことを要求する内容が盛り込まれた。さらに注意すべき点として、米国の監視活動に協力を行ったニュージーランド、カナダ、オーストラリアが名指されて、委員会が十分性認定を行った信頼を大きく損ねる国々であり、十分性認定の停止と再調査を要求している。

なお、NSA 問題を受け、米国側はセーフハーバー維持のためにそれなりに危機感があったものと考えられる。たとえば、2013 年の EU と米国の司法分野の閣僚会合の前に、連邦取引委員会 Edith Ramirez 委員長がブリュッセルでの EU-US 消費者対話において「セーフハーバーが最優先の執行課題」であることを宣言し、執行のための調査を開始したことを明らかにしている[171]。さらに、2013 年 9 月に Reding 副委員長や Albrecht 議員が出席したヨーロッパ・データ保護会議において、連邦取引委員会 Julie Brill 委員は安全保障に関する NSA 問題と商業目的のセーフハーバーは異なるものであり、セーフハーバーは「正し

---

169 European Commission, *Memo: Joint Press Statement following the EU-US-Justice and Home Affairs Ministerial Meeting of 18 November 2012 in Washington*, 18 November 2013.

170 European Parliament, *Resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*, 12 March 2014. *See also MEPs want co-operation with the US to be suspended*, EUROPEAN VOICE, Vol. 20 No. 10 at 5

171 Edith Ramirez, *Keynote Address: Protecting Consumers and Competition in a New Era of Transatlantic Trade*, Trans Atlantic Consumer Dialogue, 29 October 2013.

いターゲット」ではないことを主張し、セーフハーバーを擁護した[172]。2012 年 3 月 19 日、EU 側レディング副委員長と米国側ブライソン商務長官との間で「合衆国と欧州連合は US-EU セーフハーバー・フレームワークへのそれぞれのコミットメントを再確認する」[173]ことが共同声明で決まった翌年のスキャンダルであった。そのため、米国としての信頼回復のため、セーフハーバー継続に向けた動きであったと見ることができる。

なお、米国では、NSA 問題を受け、2013 年 12 月オバマ大統領設置の諜報活動及び通信技術審査部会の報告書と勧告「変化する世界における自由及び安全」[174]が公表された。同報告書の中でも国家安全保障局による対象監視活動への EU からの批判が取り上げられている。また、2014 年 1 月には、プライバシー及び市民的自由監視委員会が公表した「合衆国愛国者法 215 条に基づく通話記録プログラム及び外国諜報活動監視裁判所の運用に関する報告書」[175]には EU からのパブリック・コメントが寄せられていることが明らかにされている。

（5）セーフハーバーの見直し

PRISM 問題の EU と米国の調査がひと段落し、閣僚会合を終え、2013 年 11 月 27 日、欧州委員会は EU と米国のデータ移転の信頼の再構築に向けた枠組みを示すため、セーフハーバーの運用状況に関する報告と見直しを公表した[176]。

2013 年 9 月 26 日時点では、3246 社の企業が商務省からの認証を受けており、中小企業

---

172 Julie Brill, *Keynote Address*, 17 September 2013. 筆者はこの会議に出席したが、ヨーロッパのデータ保護会議であるにもかかわらず、米国は連邦取引委員会、国務省、商務省からの高官、さらに欧州連合米国代表部外交官などが多数出席しており、セーフハーバー維持に対するそれなりの危機感の表れであったとみることができよう。なお、米国連邦取引委員会の委員や有識者は、米国とヨーロッパにはプライバシーの共通性が多くみられるという楽観的な姿勢を、少なくとも対 EU プライバシー政策において、繰り返し示してきている。*See e.g.*, Julie Brill, *Bridging the Divide: A Perspective on US-EU Commercial Privacy Issues and Transatlantic Enforcement Cooperation*, in DATA PROTECTION ANNO 2014: HOW TO RESTORE TRUST? 179 (Hielke Hijimans & Herke Kraneborg eds., 2014).

173 *EU-US joint statement on data protection by European Commission Vice-President Viviane Reding and U.S. Secretary of Commerce John Bryson*, 19 Mar. 2012.

174 *Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, Liberty and Security in a Changing World*, 12 December 2013. この部会の委員を務めた Peter Swire 教授によれば、46 の勧告のうち約 7 割はただちに合衆国関係行政機関が受け入れられた、とのことである。

175 Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*, January 23, 2014.

176 European Commission, *Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspectives of EU Citizens and Companies Established in the EU*, 27 November 2013.

（従業員 250 名以下）が 60%（1925 社）を占めている。その多くが、EU 域内市場にサービスを提供する企業であり、51%の企業が人事・雇用管理の目的でのヨーロッパの労働者のデータの処理を行っている。

2002 年と 2004 年の委員会の報告書において指摘されたセーフハーバーの欠陥のほか、NSA 問題の影響のため、EU と米国の間のデータ移転の信頼性は損なわれた状況であった。ドイツは米国の NSA 監視活動を受けて 2013 年 7 月にセーフハーバーの停止を表明した[177]。もっとも、このように加盟国ごとの判断によってセーフハーバーの停止又は廃止が行われると加盟国での一貫した対応がとれなくなってしまう。そこで、委員会は EU と米国の信頼再構築に向け、セーフハーバーについて、停止又は廃止ではなくセーフハーバーを強化・補強するという方向性の検討を示した[178]。そして、委員会は、セーフハーバー強化を目的として、次の 13 の勧告を示している。

＜透明性＞

①認証を受けた企業はプライバシー・ポリシーを公表すべきである。

②認証を受けた企業のプライバシー・ポリシーは、現在リストとして掲載されている商務省のセーフハーバー・ウェブサイトへのリンクを常に設けるべきである。

③認証を受けた企業は、クラウド・コンピューティング・サービス等の下請会社との契約のプライバシーの条件を公表すべきである。

④商務省のウェブサイト上で現在認証を受けていない企業を”Not Current”と明確に知らせるべきである。

＜救済＞

⑤プライバシー・ポリシーには裁判外紛争解決（ADR）機関と EU 側の担当部署のリンクを含めなければならない。

⑥ADR は容易に利用でき、低廉でなければならない。

⑦商務省は透明性及び情報へのアクセス可能性に関する ADR 機関を計画的に監視すべきである。

---

177 Die Landesbeauftragte für Datenschutzund Informationsfreiheit, *Press Release: Conference of data protection commissioners says that intelligence services constitute a massive threat to data traffic between Germany and countries outside Europe*, 24 July 2013. Available at http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/ErgaenzendeDokumente/PMDSK_SafeHarbor_Eng.pdf?__blob=publicationFile (last visited 27 March 2014).

178 European Commission, *Communication from the Commission to the European Parliament and the Council: Rebuilding Trust in EU-US Data Flows*, 27 November 2013.

＜執行＞

⑧認証又は再認証を受けた企業の一定の割合が職権によるプライバシー・ポリシー遵守の調査対象とすべきである。

⑨遵守違反の認定がされた場合、当該企業は 1 年後に特定の再調査の対象とすべきである。

⑩企業の法令遵守や苦情申立に疑義がある場合、商務省は EU データ保護監督機関に通知すべきである。

⑪セーフハーバーの虚偽の主張は調査継続とすべきである。

＜米国機関によるアクセス＞

⑫認証を受けた企業のプライバシー・ポリシーには、どの米国法で公的機関での移転されたデータを収集及び処理が認められるかに関する情報を含まなければならない。

⑬セーフハーバー決定の安全保障の例外は厳密に見て必要かつ比例している限りにおいて用いることができる。

Reding 副委員長が主張するとおり基本的に米国の自主規制の枠組みは EU の産業界や市民から批判の的となっており、今回の勧告ではセーフハーバーの認証制度や自主規制の改善が最重要項目として位置づけられている[179]。また、米国側も 2014 年 1 月 21 日には、セーフハーバーのプライバシー原則を遵守していない 12 社を指摘するなど、執行強化の姿勢を見せている[180]。

11 月 27 日の委員会によるセーフハーバー強化を意図するコミュニケーションに対し、議会の反応は厳しいものであった。2013 年 12 月 10 日、議会市民的自由・司法・内務委員会に提出された作業文書では「セーフハーバーの決定を停止するか廃止するか」[181]という措置を委員会に迫る内容であった。その理由は、そもそもセーフハーバーは当初から政治的論争の的となってきており、議会のこれまで 2 回の調査でも個人の権利の司法救済の欠如、企業の補償金支払いがないこと、米国の異なるデータ保護体制などから EU データ保護規

---

179 Viviane Reding, *Speech: Data Protection Reform: Restoring Trust and Building the Digital Single Market*, 17 September 2013 (4th Annual European Data Protection Conference).

180 Federal Trade Commission, *FTC Settles with Twelve Companies Falsely Claiming to Comply with International Safe Harbor Privacy Framework*, 21 January 2014. http://www.ftc.gov/news-events/press-releases/2014/01/ftc-settles-twelve-companies-falsely-claiming-comply (last visited 27 March 2014). 詳しくは本報告書・河井論文、参照。

181 European Parliament, Committee on Civil Liberties, Justice and Home Affairs, *Working Document on US Surveillance Activities with respect to EU Data and its Possible Legal Implications on Transatlantic Agreements and Cooperation*, 10 December 2013.

則の執行への潜在的な障害となってきたことにある。そのため、セーフハーバーを停止又は廃止し、データ移転契約締結か拘束的企業準則を代替すべきである。そして、「セーフハーバーはもはや『セーフ』ではない」と結論付けられたのである。

また、ヒアリングからも理事会でも「セーフハーバーが汚染されている」との認識を持っており、ヨーロッパ側からの委員会・議会・理事会においても、セーフハーバーの見直し、修正、あるいは即時停止を迫るものであった。

2014 年 3 月 26 日には、EU と米国の首脳会談がブリュッセルで行われ、共同声明の中においてもセーフハーバーの見直しが言及されている[182]。すなわち、「データが商業目的で移転された場合データ保護を確保し高い透明性と効果的な執行並びに法的明確性を通じて貿易を可能とするために、2014 年夏までに包括的な方法でセーフハーバーの枠組みを強化することに関与していく」ことが明らかにされた。

2014 年 3 月までの状況はここまでであるが、今後、2014 年夏までにセーフハーバーの欠点などがとりまとめられた報告書が提出され、それに基づき今後セーフハーバーの見直しが行われるものと考えられる。なお、EU と米国の貿易協定については、データ保護が基本的権利であり、商品取引とは異なり、交渉の余地のない概念である。Reding 副委員長によれば「データ保護はお役所仕事でも関税でもない。データ保護は基本権であって、交渉の余地のないものである」[183]。

いずれにせよ、これら一連の動向のとおり、セーフハーバーが未来のモデルになりえない、とヒアリングにおいて委員会が態度を明確に示したとおり、米国以外の国がセーフハーバーを締結することは極めて非現実的というほかない[184]。

（6）その他米国との緊張関係

上記以外に、EU はプライバシー保護をめぐり、米国と繰り返し衝突してきた。たとえば、電子ディスカバリ（e-discovery）の導入により、米国の民事訴訟において、パソコンの電子メールを含む部電子文書等への情報へのアクセスが認められるようになった。これに対し、EU からは十分な保護水準が確保できない米国司法への電子データの移転が認められるべきではない、という対応が採られてきた[185]。また、米国の公益通報者保護法

---

182 Council of the European Union, *EU-US Summit, Joint Statement*, 26 March 2014.
183 Viviane Reding, *Speech: Towards a more dynamic transatlantic area of growth and investment*, 29 October 2013.
184 実際、イスラエルが十分性審査を受ける際に、セーフハーバーが強大なバーゲニング力を有する米国以外の国が締結する余地はないという見識ある判断から十分性審査の道を選択している。消費者庁・前記報告書（宮下紘「イスラエル」）118 頁、参照。
185 Article 29 Data Protection Working Party, *Working Document 1/2009 on pre-trial discovery for cross border civil litigation* (WP158), adopted on 11 Feburary 2009.

（Sarbanes-Oxley Act、SOX 法）についても、EU データ保護規則の観点から問題視されてきた[186]。

米国とヨーロッパのプライバシーをめぐる衝突は単に法制度、法所管の部署、さらには法体系といった表面的な違いではなく、根源にあるプライバシー権の哲学、価値観、そして文化の相違を映し出しているものとみることができる。

Ⅵ．監督機関

１．監督機関の地位について

（１）EU 基本権憲章（第 8 条 3 項）

基本権憲章で定められた個人データの保護に関する規則の遵守については、独立機関による監督を受けるものとする。

（２）EU データ保護指令（第 28 条）

・加盟国は、一つ又は複数の公的機関が指令の規定の適用を監督する責任を負うことを定めなければならない。（第 1 項）

・監督機関は、職務を遂行する上で、完全に独立して活動しなければならない。（第 1 項）

・加盟国の個人データ保護に関する行政措置又は規則の制定には監督機関に諮問しなければならない。（第 2 項）

・監督機関の職員は、機密情報について職業上の守秘義務を負う。（第 7 項）

（３）EU データ保護規則提案

委員会	・監督機関は、職務権限を行使する際、完全に独立して行動しなければならない。監督機関の構成員は、誰にも誰からも指示を求めたり受けたりしない。人的・技術的、財政的資源、施設等が監督機関に提供されなければならない（第 47 条 1～3 項）。

[186] Article 29 Data Protection Working Party, *Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime*, (WP117) adopted on 1 Feburary 2006. *See also* Renzo Marchini, *Conflict of Laws: Anonymous Whistleblowing Hotlines Under Sarbanes-Oxley and European Data Protection Laws*, 2006 Privacy & Data Security L. J. 575 (2006). 邦語による紹介として、石田信平「米国 SOX 法の内部通報制度と EU 個人情報保護原則の衝突」比較法文化 18 号（2009）169 頁以下、参照。

	・監督機関の構成員は、加盟国の議会又は政府による任命とし、個人データ保護に関する必要な経験と資質を有する者から選出される（第 48 条 1～2 項）。 ・監督機関の設置規則については、地位、構成員の資格、任命手続、任期（4 年以上）、構成員に適用される規則、解職規則と手続の各項目を加盟国の法律で定めることとする（第 49 条）。 ・監督機関の構成員及び職員は、職務上の守秘義務を負う（第 50 条）。
議会	・独立性について、完全な独立性と公平性の維持という文言が追加された（第 47 条 2 項）。
理事会	・独立性について、直接又は間接にかかわらず、外部からの影響力を受けない、という追加文言が検討されている。（第 47 条 2 項） ・職務上の守秘義務については実効性の観点から削除が検討されている（第 50 条）。

（4）独立性の要件

データ保護監督機関は、職務権限を行使する際、完全に独立して行動しなければならないことは、指令においても規則提案のみならず、EU 基本権憲章においても明確な態度を示している。指令と規則提案の前文においても「完全な独立性を備え職務を遂行する、加盟国内の監督機関の設置は、個人データの処理に関する個人の保護の不可欠な要素を成している」（指令前文 62 項・規則提案 92 項）と謳っている。この監督機関の独立性の要件は EU のデータ保護において核心部分を成していると言ってよい[187]。

しかし、この独立性の要件は歴史的に見ても、また理論的に見ても必ずしも自明なことではない。歴史的に見れば、1981 年に欧州諸国が署名した欧州評議会条約第 108 号は「効果的な保護」を規定するにとどまり、独立した監督機関の設置を要求していなかった。また、理論的に見れば、公正な裁判を受ける権利を除き、他の基本権保障（表現の自由や結社の自由）において、同様の独立監督機関を設ける規定は見られない。

この点、ピーター・ハンスティンクス（Peter Hustinx）欧州データ保護監督官は、データ保護分野において独立した監督機関の必要性を次のように論じる[188]。まず、歴史的見れ

187 なお、このような独立した監督機関によるデータ保護法の執行については、プライバシー市民団体等からも支持を受けてきた 。*See e.g.*, The Public Voice, *Civil Society Madrid Declaration: Global Privacy Standards for a Global World*, 3 November 2009; The European Consumer Organisation, *Data Protection Proposal for a Regulation: BEUC Position Paper*, 27 July 2012.

188 Peter Hustinx, *The Role of Data Protection Authorities*, in REINVENTING DATA PROTECTION? 132- 134 (Serge Gutwirth et. al. eds, 2009). 第三者機関の独立性を含む論

ば、個々の事業分野における個人データ保護の規律が行われていたが、あらゆる分野における規制が必要となり、データ保護の権利保障のための包括的な構造支援が必要となった。さらに、理論的に考えれば、他の基本権分野では強力な制度基盤（表現の自由によるマスメディアや結社の自由による労働組合や政党）により基本権の複層的なチェック機能が働きやすいのに対し、データ保護の分野では裸の個人がプライバシーの危険にさらされている。また、データ保護の侵害はそれ自体可視化されにくいこと、また専門的・技術的知見がないと侵害それ自体に対処しにくいことが指摘できる。同時に既存の法制度を用いてもデータ保護の効果的な保障が及びにくいという点も考慮する必要がある。たとえば、通常の民事訴訟であれば、情報の非対称性から権利の主張者は不利な立場に置かれていること、侵害防止のためのデータ保護という新たな分野の法規範の形成には多大な時間を要すること、さらにそれぞれの事業分野ごとの規律ではデータ保護の権利の予測可能性を担保し得ないことが指摘される。このようなことから、特別の地位にあるデータ保護機関が独立して権限行使することが必要となる。

また、ルーバン大学でのヒアリングでは、監督機関の意義には、①司法よりも迅速な苦情処理への対応ができること、②データ保護に見識を有する専門的な判断に基づく対応ができること、があるとの指摘があった。

以上のような独立した監督機関の必要性は欧州司法裁判所の判決においても全面的に支持されている。2010 年 3 月 9 日 European Commission v. Federal Republic of Germany[189] 及び 2012 年 10 月 16 日 European Commission v. Republic of Austria[190]においてそれぞれ監督機関の独立性要件の重要性を示した（2014 年 3 月現在係争中の European Commission v. Hungary[191]もある）。いずれの判決においても、「完全な独立性」の要件について次のように説明している。「独立性」とは、「いかなる指示を受けることもなく、又は圧力の下に置かれることなく、完全に自由に行動できること」を意味する。そして、「完全に」とは、「監督機関に対する直接又は間接のいかなる影響からも分離した決定権限」を含意する。すなわち、「完全な独立性（complete independence）」とは、「監督対象の機関によって行使されるあらゆる影響のみならず、直接又は間接を問わず、私的な生活への権利の保護個

点については、宍戸常寿「パーソナルデータに関する『独立第三者機関』について」ジュリスト 1464 号（2014）18 頁以下、参照。

189 CJEU, C-518/07, *European Commission v. Federal Republic of Germany*, 9 March 2010. 本判決の邦訳については、消費者庁「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」（2013）69 頁以下（加藤隆之「ドイツ」）、参照。

190 CJEU, C-614/10, *European Commission v. Republic of Austria*, 16 October 2012

191 CJEU, C-288/12, *European Commission v. Hungary*. *See also* András Jóri, *The End of Independent Data Protection Supervision in Hungary – A Case Study*, in European Data Protection: Coming of Age 395 (Serge Gutwirth et. al. eds, 2013).

人データの自由な流通の公正な衡量を測るという監督機関による任務の遂行疑義が生じうるいかなる外部的影響を排除すること」を意味している[192]。

そこで、「完全な独立性」の要件をめぐり、監督機関が政府から独立しているかどうか、また監督機関の職員、建物等が独立しているかどうか、がそれぞれ欧州司法裁判所で争われた。European Commission v. Federal Republic of Germany において、ドイツでは公的部門以外の個人データ処理について州の監視を受けることとなっており、監督機関の独立性が損なわれていると判断された。すなわち、欧州司法裁判所の判決によれば、「完全な独立性」の要件に照らし、州政府の下で監督活動を行うことは、監督機関が個人データの処理に関する規定を解釈し適用する際に客観的に活動することを妨げていると判断された。

European Commission v. Republic of Austria においては、更に詳細に独立性の実質的要件について説示している。本件では、オーストリアの監督機関が、職員、建物、情報提供の点において連邦首相府からの独立性しているかどうかが問われた。第 1 に、オーストリア監督機関の職員について、監督機関が連邦職員を雇用していることは職務上連邦機関との関連性があり、同時に連邦職員の地位的優位から監督機関の職員の活動が監視されることを許容する事態を生み出している。これはいかなる直接的・間接的影響も受けないとする独立性の要件に反する。第 2 に、予算法の都合により、監督機関の建物や職員を連邦首相府の下の省庁と一体化することは監督機関の決定に影響を及ぼす危険性がある。よって、公平性に疑いをさしはさみ、独立性の要件に反する。第 3 に、連邦首相府はいつでも監督機関から情報を受ける権利を有しているが、監督機関に情報を提供する義務を無条件で負わせることは間接的な影響力が生じうる。したがって、連邦首相府が監督機関に情報提供を負わせることは独立性の要件に反する。この判決を受けて、ただちにオーストリアは 2014 年 1 月 1 日付で新たな職員の雇用や建物の移転、連邦首相府の情報受領の権利の制限などの措置を採り、新たなコミッショナーを設置した[193]。

以上のとおり、データ保護監督機関は、単に設置法上の政府機関からの形式的独立性を意味するのではなく、権限行使のみならず、監督機関の職員や建物といった実質的独立性の要件を満たさなければならない。

---

[192] CJEU, *European Commission v. Federal Republic of Germany*, para 19 & 30; CJEU, *European Commission v. Republic of Austria*, para 41.

[193] Datenschutzkommission, *Letter to European Commission et. al.*, 16 December 2013. Available at https://www.dsb.gv.at/DocView.axd?CobId=53401 (last visited 25 March 2014). *See also* Alexander Balthasar, *'Complete Independence' of National Data Protection Supervisory Authorities*, 9 UTRECHT L. REV. 26, 28 (2013).

２．監督機関の義務と権限について

（１）EU データ保護指令（第 28 条）

・監督機関の権限には、次のものが含まれる。これら監督機関の決定に不服がある場合、裁判所に対して訴訟を提起することができる。（第 3 項）

a）データにアクセスする権限と調査権限

b）仲裁権限（処理実施前の意見、データのブロック、消去又は破壊する権限等）

c）訴訟手続を開始する権限

・監督機関は、個人が申し立てた主張を聴取し、その結果の情報提供をしなければならない。（第 4 項）

・監督機関は定期的に活動に関する報告書を公表しなければならない。（第 5 項）

・監督機関は、他国の法が適用され得た場合でも、自国の領域内においては監督する権限を有する。（第 6 項）

（２）EU データ保護規則提案

委員会	・監督機関は、各加盟国の領土内において権限行使する（第 51 条 1 項）。 ・監督機関の義務には、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のほか広報啓発を含むものとする。義務の遂行は原則としてデータ主体に無償で行うこととする（第 52 条 1～2・5 項）。 ・監督機関の権限には、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、議会・政府等への通知を含むものとする。監督機関は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、制裁権限を有するものとする（第 53 条 1～4 項）。 ・監督機関は年次報告書を作成し、公表する（第 54 条）。
議会	・義務と権限に、管理者及び処理者の認証を行うこと、が追加された（第 52 条 1 項 ja 号、第 53 条 1 項 ia 号）。 ・権限に、本規則提案違反の報告奨励のための仕組み策定が追加された（第 53 条 1 項 ja 号）。
理事会	・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）。 ・権限について、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）

（３）執行権限

指令の下では、EU 加盟国間において執行のばらつきがあることがしばしば指摘された。そこで、規則提案では、各加盟国の執行権限について強制力ある制裁権限を付与することが狙いとなっている。

強制力ある権限には様々なものが想定されるが、たとえば、2013 年 7 月、イギリスの情報コミッショナー・オフィスは、道路上を通行するすべての自動車のナンバープレートを自動的に認証するカメラをハートフォードシャーの警察が 6 か所 7 台設置したことが、個人データ処理の合法的根拠がないことと過度な個人データの処理を行っていることから、欧州人権条約第 8 条の私生活尊重の権利への不当な干渉となるとの決定を下した[194]。これにより、ナンバープレート自動認証のデータ処理のプライバシー影響評価によるその必要性が示されるまでその処理の停止が命じられた[195]。以下、指令の下での調査権限の一覧をまとめておいた。

加盟国の調査権限の比較一覧（欧州基本権機関による）[196]

	情報・文書の要求	データ・バンクとファイリング・システムへのアクセス	令状なしの捜索・抑収	令状による捜索・抑収	監査
ブルガリア	●	●	●		●
ベルギー	●	●	●		●
チェコ	●	●	●		●
デンマーク	●	●	●		●

194 ICO, *Enforcement Notice to the Chief Constable of Hertfordshire Constabulary*, 15 July 2013. *See also* ICO, *CCTV Code of Practice* (Revised Edition, 2008).

195 *See* ICO Press Release: *Police use of 'Ring of Steel' is disproportionate and must be reviewed*, 24 July 2013. http://ico.org.uk/news/latest_news/2013/Police-use-of-Ring-of-Steel-is-disproportionate-and-must-be-reviewed-24072013 (last visited 25 March 2014).

196 European Union Agency for Fundamental Rights, *Data Protection in the European Union: the Role of National Data Protection Authorities* (2010) p.21

ドイツ	●	●	●	●	●
エストニア	●	●	●		●
ギリシャ	●	●	●		●
スペイン	●	●	●		●
フランス	●	●		●	●
アイルランド	●	●	●		●
イタリア	●	●	●	●	●
キプロス	●	●	●		●
ラトビア	●	●	●		●
リトアニア	●	●	●		●
ルクセンブルク	●	●	●		●
ハンガリー	●	●	●		●
マルタ	●	●		●	●
オランダ	●	●	●		●
オーストリア	●	●	●		●
ポーランド	●	●	●		●
ポルトガル	●	●	●		●
ルーマニア	●	●			●
スロベニア	●	●	●		●
スロバキア	●	●	●		●
フィンランド	●	●	●		●
スウェーデン	●	●	●		●
イギリス	●			●	●

＊調査はドイツの捜索・抑収は連邦レベル、イタリア同意があれば令状不要であるが、それ以外は令状が必要。イギリスの監査は管理者の要請がある場合にのみ実施可能。

３．監督機関による罰則と救済について

（１）EU データ保護指令

・すべての者が権利の侵害に対して司法的救済を受ける権利を有することを定めなければならない（第 22 条）

・加盟国は、本指令を実施するため、適合的な措置を講ずるとともに、違反に対する制裁について特に規定を設けなければならない（第 24 条）。

（２）EU データ保護規則提案

委員会	・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）。 ・監督機関は最大で 1,000,000 ユーロ又は全世界での年間売上高の最大 2%を上限として制裁金を科すことができる（第 79 条）。
議会	・データ主体、その他の団体による苦情申立の権利及び司法的救済を求める権利について、「一貫性ある体制」という文言を追加した。（第 73 条）

理事会	・集団訴訟について、データ主体の代理という条項を設け、加盟国の立法により構成された団体が個人に代わって苦情申立することができるよう検討されている（第 76 条 1 項)。 ・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)。

（3）罰則

指令では、違反に対する制裁について特に規定を設けなければならない、と表現されたにとどまっていたが、規則提案では具体的な制裁について条文が置かれた。委員会の提案によれば、制裁は a) 250,000 ユーロ又は全世界の年間売上高 0.5%を上限とする場合、b) 500,000 ユーロ又は全世界の年間売上高 1%を上限とする場合、c) 1,000,000 ユーロ又は全世界の年間売上高 2%を上限とする場合にそれぞれ違法の行為により金額が異なる。

レディング副委員長によれば、グーグルのプライバシー・ポリシー変更の違法性についてフランスデータ保護監督機関が科した制裁金 15 万ユーロ（約 2100 万円）を例にとり、「ポケット・マニー」にすぎないと言う[197]。すなわち、フランスが科した制裁金 15 万ユーロという金額は 2012 年のグーグルの全世界の売上高の 0.0003%にすぎないのであって、「ヨーロッパの人々はもっと真剣に受け止めるべきである」と主張する。委員会が提案した全世界売上高の総額 2%であれば、制裁金は 7 億 3100 万ユーロ（約 10 億 2300 万円）となる。このようにデータ主体の権利を意味ある形で法執行することは、プライバシー保護を競争力あるものにさせると言われる。

全世界の年間売上高総額 2%という上限を制裁金として提示した委員会に対し、ヒアリングによれば、企業からは制裁金の金額があまりに高すぎるという厳しい批判があった。しかし、議会はこのような批判にもかかわらず、修正案において全世界の年間売上高総額 2%から 5%にその上限を上げた。ヒアリングによれば、理事会においては、議会とは逆の方向で審議されており、上限は低くなると予想される。また、欧州消費者団体によれば、このような制裁金の額の提示は競争法分野における蓄積からすれば決して大きな額ではない。また、これまでの EU 法の審議から見て、中間の 3%あたりが落としどころになるのではないか、という指摘があった。従来の EU の姿勢は、規則提案においても変わらず、法執行による制裁があることがデータ保護の権利を尊重するうえで不可欠であるという認識は、どの EU の機関も共通していた。さらに、十分性の最大の要件がこの制裁権限と現実の執行例である、と回答した機関もあった。

197 Viviane Reding, Speech: *The EU Data Protection Reform: Helping Businesses Thrive in the Digital Economy*, 19 January 2014.

（4）救済

2014 年 1 月に公表された欧州基本権庁（European Union Agency for Fundamental Rights）の調査結果によれば、データ保護監督機関がデータ保護の権利を実効的に救済するには現実的に次の 4 つの課題（①時間、②費用、③代理人・弁護士、④証拠）がある[198]。

①時間…データ主体が救済を求めてからのどの程度の時間をかけるのが適切か、という点について加盟国間でも一致が見られない。たとえば、苦情申立からデータ保護監督機関の決定を下すまでの期間を法律で定める加盟国がほとんどであるが、30 日（ポーランド・ブルガリア）から事案によって 2 年を要した（ドイツ）という事例が報告されている。多くの加盟国では 6 か月以内に事案の処理を行っているが、時間的制約を設けることでかえって十分な調査を行えないという指摘もある。また、司法による判決を求めることとなれば、データ保護監督機関による決定以上に時間を要するため、効果的な救済という観点からはあまりに時間がかかりすぎているのではないか、という指摘がある。

②費用…データ漏えいの被害にあったデータ主体であっても、弁護士費用や訴訟費用がかさむと訴訟を控えてしまい、効果的な救済の弊害になっているという指摘がある。加盟国には制約があるものの無償で苦情申立を受領し、訴訟手続を代行するところもある。

③代理人・弁護士…弁護士やプライバシー保護の市民団体からの支援により救済を求める方途があるものの、多くの国でデータ保護の分野に精通した法律家が極めて少ないという指摘がある。データ保護分野の裁判官と弁護士の質の確保は、特に技術的な分野との連携を含め人材育成が重要な課題となっている。フランスやハンガリーではデータ保護機関が裁判官や弁護士の研修を行っている[199]。

④証拠…多くの事例において消費者による証拠保全と立証が救済の障害になっていることが指摘されている。他方で、管理者側に合法な処理を行っていたことを立証責任が負わされるイタリア、苦情申立に好意的な推定が働くポーランドという例が見られる。救済のための立証の在り方については加盟国でもバラつきがあり、一元化すべきではないか、という提案がなされてきた。

---

198 European Union Agency for Fundamental Rights, *Access to Data Protection Remedies in EU Member States* (2014).

199 EU データ保護の法律実務に精通している Christopher Kuner 弁護士は、自身の体験をもとに、データ保護分野の裁判官と弁護士の人材育成がいかに重要な課題であるかを自身の体験をもとに指摘された。Christopher Kuner, Remark: *EU Data Protection Reform: Fixing the Last Bugs*, 7th International Conference on Computers, Privacy & Data Protection 2014: Reforming Data Protection: The Global Perspective, January 22, 2014.

４．監督機関の相互支援について

（１）EU データ保護指令（第 28 条）

・各監督機関は相互に協力しなければならない。（第 6 項）

（２）EU データ保護規則提案

委員会	・本規則の統一的施行及び適用のため、監督機関は相互支援を行う。他の機関からの支援の請求に対し、1 か月以内に適切な措置を講じなければならない。管轄権を有さない場合か本規則に抵触する可能性がある場合を除き、支援の要請を拒んではならない（第 55 条）。 ・各加盟国は、一つ又は複数の公的機関が規則の適用を監視する責任を有するものとする。複数の機関がある場合は、一つをコンタクト・ポイントとして指定する（第 46 条 1～2 項）。 ・管理者又は処理者が二か国以上に拠点を持つ場合、主要拠点のある国の監督機関が全加盟国の管轄権を有する（第 51 条 2 項）。 ・欧州データ保護委員会を設置する。同委員会は各加盟国から選出された長と欧州データ保護監督官で構成される（第 64 条 1~2 項）。欧州データ保護委員会は独立して行動する（第 65 条）。 ・加盟国の監督機関が、データ処理が複数の加盟国に関わる場合、域内でのデータ流通に実質的影響を及ぼす場合、事前協議の対象となる処理を行う場合、標準データ保護条項の決定を行う場合、契約条項の認可を行う場合、拘束的企業準則の承認を行う場合、欧州データ保護委員会に通知しなければならない（第 58 条 1～2 項）。 ・欧州データ保護委員会の任務には、欧州委員会への助言、ガイドライン・勧告、ベスト・プラクティスの発出、統一的体制に関する意見公表、監督機関の協力促進、研修促進、世界中のデータ保護機関との情報交換の促進を含む（第 66 条 1 項）。
議会	・主要拠点のある国の監督機関は主導的監督機関として適切な措置を講ずることとする。欧州データ保護委員会は主導的監督機関の認定に関する意見を発出することができる。（第 54a 条 1～3 項）
理事会	・主要な拠点のある国の監督機関として主導的監督機関に関する新たな条項が

	検討されている（第 51a 条）。 ・主要な拠点のある国の監督機関の認定に関する新たな条項が検討されている（第 51b 条）。

（3）監督機関の相互支援―one-stop-shop との関係

指令においては、各監督機関における相互の協力をしなければならない、という単純な条文が置かれているのみであった（第 28 条 6 項）。しかし、規則提案では、2012 年 1 月 25 日のレディング氏のプレスリリースの時から監督機関の EU 域内の統一的な対応を企図すべく one-stop-shop の意義が強調されてきた。One-stop-shop という概念は、すでに上記のように加盟国間の監督機関の権限と運用にバラつきがあり、全く同一の問題であっても加盟国によって対応が割れてしまうというデメリットの克服をする目的ですでに規則提案が公表される以前から提案されてきた。すなわち、2010 年に欧州基本権庁が「複数の機関が混乱と不必要な複雑性をもたらしている」という難点を克服するため「効率的な one-stop shops としての国内のデータ保護機関」が必要であることを指摘していた[200]。さらに、域内市場におけるデータの流通と個人データの権利という基本権保障という観点からも各加盟国の監督機関の相互支援の意義が示されてきた[201]。

そこで、委員会は、複数の加盟国に拠点を持つ管理者や処理者の行為について、主要な拠点のある国の監督機関が全加盟国における処理活動を管轄することで one-stop-shop の構造を示した。そして、いかなる国の監督機関でも苦情申立を受理することで加盟国間のデータ主体の権利を統一的に保障することを狙いとしている。

議会の修正案は、基本的に委員会の提案に基づいているが、「主導的監督機関（lead authority）」という文言を挿入し、主要な拠点のある国の監督機関が主導的監督機関として苦情申立に対応に当たるが、他の監督機関との合意に至る努力義務を設けることや欧州データ保護委員会による主導的監督機関の認定の手続を考案し、one-stop-shop の考え方を「一貫性ある体制（consistency mechanism）」として強固なものにした。

しかし、理事会においては one-stop-shop をめぐり加盟国間の対立が明らかになった。実際、理事会のヒアリングにおいて、理事会が規則提案の審議に議会に比べ時間を要している最大の理由は one-stop-shop をめぐる対立である、という指摘があった。理事会においては、データ保護の専門家以外の政府（大臣クラス）がメインとなり審議するため、作業部

200 European Union Agency for Fundamental Rights, *supra* note 198, at 9.
201 *See* EU Network of Independent Experts in Fundamental Rights, *Report on the Situation of Fundamental Rights in the European Union and its Member States in 2002*.

会でのデータ保護専門家にとっては当然視されてきた監督機関の連携強化が、各加盟国政府の立場からは権限行使の在り方の観点から必ずしも好意的に受け止められなかったことに原因がある[202]。

仮に理念としての one-stop-shop が受け入れられたとしても、現実にいかなる場合にどのように各監督機関が協力を行っていくかは重要な問題となる。理事会では、特に複数の加盟国が単一の決定に至る手続と管轄が限られている「主要拠点（main establishment）」のある監督機関の権限行使について慎重な議論が行われてきた[203]。この点、Stefano Melloni v. Ministerio Fiscal[204]において、欧州司法裁判所は刑事手続の基本権の保障のため加盟国の憲法秩序に関わらず EU の法的規則を無視する限りにおいて「EU 法の優越性の原則」に反すると判断している。データ保護という基本権憲章で定められた権利は EU 法を履行することによって実現されうるのであり、特に越境問題と複数の加盟国間に影響を及ぼす問題において one-stop-shop の意義は発揮されるものと考えられる。

欧州委員会の支援による執行協力促進のプロジェクト（PHAEDRA）は、コミッショナー国際会議とも連携を図り、具体的な越境執行協力の取組例について情報共有を行ってきている[205]。PHAEDRA が報告書に掲載している EU 加盟国を含むデータ保護監督機関の執行協力に関する具体的事例として、次の 11 件が列挙されている[206]。

なお、EU 第 29 条作業部会における協力連携をはじめ、国際的な連携枠組みについては、図に示しておいた（PHAEDRA 報告書に基づき作成）[207]。

---

[202] *See e.g.*, Council of the European Union, Press Release: 3279th Council Meeting, 5-6 December 2013; Council of the European Union, Press Release: 3260th Council Meeting, 7-8 October 2013.

[203] 理事会においても、one-stop-shop がそもそもデータ保護監督機関の competence の問題ではなく、jurisdiction という形で議論すべきではないか、という根本的なところでの審議が行われてきている。*See e.g.*, Council of the European Union, Press Release: *Data Protection: Council Supports "one-stop-shop" Principle*, 7 October 2013.

[204] CJEU, *Stefano Melloni v. Ministerio Fiscal*, C-399/11, 26 February 2013. *See also* Jan Wouters, Katrien Meuwissen, & Ana Sofia de Barros, *The European Union and National Human Rights Institutions*, KU Leuven, Working Paper No.112, July 2013. 本判決及び本論文については、「EU 法の優越性の原則」とともに Kuner 弁護士にご教示いただいた。EU 法の優越性については、庄司克宏『新 EU 法基礎篇』（岩波書店・2013）228 頁、中西優美子『EU 法』（新世社・2012）参照。

[205] データ保護監督機関の間の実践的かつ有用な協力改善プロジェクト（PHAEDRA：Improving Practical and Helpful Cooperation between Data Protection Authorities）は第 35 回データ保護プライバシー・コミッショナー国際会議において共同ワークショップを開催した。*See* PHAEDRA, *A Compass toward Best Elements for Cooperation between Data Protection Authorities* (2014) (Authors: Paul De Hert & Gertjan Boulet).

[206] *See* PHAEDRA, *Co-ordination and Co-operation between Data Protection Authorities* (2014) (Authors: David Barnard-Wills & David Wright).

[207] 日本は、基本方針に基づき、OECD プライバシー越境執行協力に関する勧告を踏まえ、

①グーグル・バズ

2010 年 4 月 20 日、カナダ、スペイン、イスラエル等のデータ保護機関によるグーグル CEO 宛の共同の書簡でプライバシー保護の規則の尊重を要求した[208]。その後、米国連邦取引委員会による調査で欺瞞的な方法を用いていたことなどから 20 年間にわたる監査等が決定した[209]。

②グーグル・ストリート・ビュー

オーストラリア、オーストリア、ベルギー、カナダ、チェコ、フランス、ドイツ、ギリシャ、香港、アイルランド、イタリア、オランダ、ニュージーランド、スペイン、スイス、イギリス、米国等において自国の法に基づきそれぞれ調査が行われた。特に技術的な調査については、カナダ、ドイツ、フランス、スペイン、オランダの間で非公式な連絡がとられた。結果として、データ保護機関の間で異なる事実認定がされるなど、対応が割れてしまった。

③グーグル・プライバシー・ポリシー（フランスによる調査）

グーグルのプライバシー・ポリシーの改訂について、ユーザーのデータの結合を行ったり、オプトアウトの可能性がなかったなどの理由から、EU データ保護指令に基づき設置された第 29 条データ保護作業部会[210]を代表してフランスデータ保護機関が調査を実施した

「消費者庁は、各省庁と協力し、必要な対応・措置を検討する」とある。しかし、諸外国のデータ保護監督機関に対応する機関が存在しないため（番号制度における機関は分野限定のため諸外国からカウンターパートとはみなされていない）、これまで越境執行協力ができなかった。この点、越境執行力ができない、あるいは他国で違法とされたことが、日本では合法であるという判断が示されてきたが、「プライバシー・個人情報を法的に保護していない国は、人権意識が乏しいという受け止め方もされた」という堀部政男教授の指摘は謙虚に受け止める必要がある。堀部政男「プライバシー・個人情報保護の国際的整合性」堀部政男編『プライバシー・個人情報保護の新課題』（商事法務・2010）8-9 頁、参照。

208 Jennifer Stoddart et. al., *Letter to Mr. Eric Schmidt*, 19 April 2010. Available at https://www.priv.gc.ca/media/nr-c/2010/let_100420_e.pdf (last visited 27 March 2014).

209 Federal Trade Commission, *Google, Inc., In the Matter of*, 24 October, 2011. Available at http://www.ftc.gov/enforcement/cases-proceedings/102-3136/google-inc-matter (last visited 27 March 2014).

210 EU 加盟国のデータ保護機関、EU 諸機関と欧州委員会から構成され、データ保護機関の加盟国間の統一的な法適用の促進等を目的とした EU のデータ保護の専門家会合である。年 5 回程度の会合を開催し、データ保護分野の専門的な意見や勧告を公表している。2014 年 3 月現在議長はフランス Isabelle Falque-Pierrotin である。

[211]。この調査については、フランスがアジア太平洋プライバシー機関やカナダ、米国とも連携を図るなど、グローバルな形で対応が行われた[212]。なお、制裁金は€150.000（フランス）[213]や€900.000（スペイン）[214]など国によって異なった。

④ワッツアップ

ワッツアップ（WhatsApp）のインスタントメッセージのアプリのユーザーの連絡帳へのアクセス等についてオランダとカナダが覚書（2012 年 1 月 16 日発効）を結んだ上で共同調査を行った。共同調査をしたものの、それぞれの執行権限の違いなどから、オランダとカナダではそれぞれ別の調査報告書が公表された[215]。報告書に示された勧告の内容（データ保全の期間）についてもオランダとカナダでは異なっている。

⑤フェイスブック

フェイスブックの国際本部がダブリンにあることからアイルランドによるフェイスブッ

---

[211] Article 29 Data Protection Working Party, Press Release: *Google's privacy policy: European data protection authorities are coordinating their enforcement action*s, 27 February 2013. *See also* Article 29 Data Protection Working Party, *Letter to Mr. Page*, 16 October 2012. Available at http://www.cnil.fr/fileadmin/documents/en/20121016-letter_google-article_29-FINAL.pdf (last visited 27 March 2014).

[212] *See e.g.*, APPA, *Letter to Article 29 Data Protection Working Party*, 12 October 2012. Available at http://www.cnil.fr/fileadmin/documents/en/APPA_SUPPORT_LETTER-Article_29_Letter.pdf (last visited 27 March 2014).

[213] Commission nationale de l'informatique et des libertés, *Deliberation No. 2013-420 of the Sanctions Committee of CNIL imposing a financial penalty against Google Inc.*, 3 January 2014. Available at http://www.cnil.fr/fileadmin/documents/en/D2013-420_Google_Inc_EN.pdf (last visited 27 March 2014).

[214] Agencia Española de Protección de Datos, Press Release, *The AEPD sanctions Google for serious violation of the rights of the citizens*, 19 December 2013. Available at http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2013/notas_prensa/common/diciembre/131219_PR_AEPD_PRI_POL_GOOGLE.pdf (last visited 27 March 2014).

[215] *See* Office of the Privacy Commissioner of Canada, *Report of Findings Investigation into the personal information handling practices of WhatsApp Inc., PIPEDA Report of Findings #2013-001*, 15 January 2013, Available at https://www.priv.gc.ca/cf-dc/2013/2013_001_0115_e.asp (last visited 27 March 2014); Dutch Data Protection Authority, *Investigation into the processing of personal data for the 'whatsapp' mobile application by Whatsapp Inc., Z2011-00987, Report on the definitive findings*, 15 January 2013.

クの監査を実施した[216]。監査に際し、ノルウェーの消費者審議会からの苦情を受け付けている。また、カナダ、米国、ドイツ・ハンブルクにおいてもそれぞれ調査が行われた。調査過程で管轄の問題が明らかになったこと、また監査という調査形態が EU では批判的であったことがそれぞれ指摘された。

⑥ソニー・プレイステーション・ネットワーク

ソニー・プレイステーション・ネットワークのハッキングによるユーザー情報の漏えいについて、オーストラリア、香港、ニュージーランド、イギリス等においてそれぞれ調査が行われた。オーストラリアでは子会社が個人情報を保有していなかったため、違反の認定ができなかったと結論付けられたが[217]、イギリスではハッキングが防止できていたという結論が下され、£250,000 の制裁金が科された[218]。ソニーの複雑な企業体系から管轄や責任の所在を問う問題が明らかになった。

⑦SWIFT と米国のテロ対策金融追跡プログラム

国際銀行間通信協会（SWIFT）が米国財務省のテロ対策の監視プログラムに協力するため金融データの無断送信が明らかになった。通信センターが置かれているベルギーが調査し、2006 年の報告でベルギー法に違反していることが指摘された。実質的にはベルギーの調査であったが、第 29 条作業部会を通じたヨーロッパの機関の協力の例であり、同時に EU が米国との交渉を行い、SWIFT データの取扱いに関して EU と米国の間で国際協定が締結された[219]。

⑧通信データ保全

データ保全指令に基づく通信会社やインターネットプロバイダに対するデータ保全の仕方について、第 29 条作業部会の調査によれば国内法の執行の在り方にばらつきがあること

---

[216] *See* Data Protection Commissioner, *Facebook Ireland Ltd. Report of Audit*, 21 December 2011; *Facebook Ireland Ltd. Report of Re-Audit*, 21 September 2012.

[217] Office of the Australian Information Commissioner, Sony PlayStation Network / Qriocity: Own motion investigation report, 29 September 2011. Available at http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/sony-playstation-network-qriocity (last visited 27 March 2014).

[218] Information Commissioner, *Monetary Penalty Notice*, 14 January 2013. Available at http://ico.org.uk/news/latest_news/2013/~/media/documents/library/Data_Protection/Notices/sony_monetary_penalty_notice.ashx (last visited 27 March 2014).

[219] *International Agreements on the signing, on behalf of the Union, of the Agreement between the European Union and the United States of America on the processing and transfer of financial messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program*, 28 June 2010.

が報告された。そこで、第 29 条作業部会を通じて加盟国のデータ保護機関が立ち入り調査を含む執行協力の調査を行った。アイルランド最高裁判所とオーストリア憲法裁判所においても審理され、欧州司法裁判所に付託された。データ保全指令は、私生活尊重と個人データ保護の基本権への干渉の疑いがあることから、2014 年 3 月現在、欧州司法裁判所において審理されている[220]。

⑨世界反ドーピング機関の規程

世界反ドーピング機関は、反ドーピング規程として「プライバシーと個人情報保護に関する国際基準」[221]を 2009 年に制定し、薬物テスト実施のための選手の居場所やセンシティブ・データを含む情報の提供が義務付けられた。ベルギーの選手らが私生活尊重の権利の侵害であることを主張し、第 29 条作業部会が調査を実施し、情報収集の最小限化の原則の履行に関する 2 つの意見を公表した。反ドーピング機関がカナダに所在していることから、カナダとも連携を図り、反ドーピング機関との意見交換を行ってきた。また、スペインの裁判所では反ドーピング規程がスペインのデータ保護法に違反しないとの判決が下された。

⑩GPEN プライバシー・スウィープ

OECD プライバシー保護法の執行に係る越境協力に関する勧告[222]に基づき 2010 年に設置されたグローバル・プライバシー執行ネットワーク（Global Privacy Enforcement Network）が、カナダの主導により 2013 年 5 月 6 日～12 日に第 1 回「プライバシー・スウィープ（Privacy Sweep）」というプライバシーの広報啓発活動を行った[223]。第 1 回のテーマはプライバシー実務の透明性であり、プライバシー・ポリシーの公表等についても併せて調査が行われた。参加国・地域は、オーストラリア、カナダ、エストニア、フィンランド、フランス、ドイツ、香港、アイルランド、マカオ、マセドニア、ノルウェー、イギリス、米国である。

⑪グーグル・グラス

---

220 CJEU, *Digital Rights Ireland and Seitlinger and Others*, Joined Cases C-293/12 and C-594/12, 8 April 2014.
221 The World Anti-Doping Code, *International Standard for the Protection of Privacy and Personal Information*, 11 May 2009.
222 OECD, *Recommendation on Cross-Border Co-operation in the Enforcement of Privacy Laws*, 12 June 2007.
223 GPEN, Action Plan for the Global Privacy Enforcement Network, adopted 15 June 2012; Part E amended 22 January 2013. Available at https://www.privacyenforcement.net/public/activities (last visited 27 March 2014).

2013 年 6 月、カナダが主導して第 29 条作業部会、オーストラリア、ニュージーランド、メキシコ、イスラエル、スイス、カナダ・アルバータ州、ケベック州、ブリティッシュ・コロンビア州の連名によるグーグル COE 宛て書簡でグーグル・グラスがもたらすプライバシーに関する問題について質問を行った[224]。米国連邦議会においても同様の質問項目を含む書簡を宛てている。プライバシーに関する潜在的な問題についてコミッショナーで共同して新たな技術利用が始まる早い段階で調査した例である。

（４）欧州データ保護委員会

規則提案では、新たに欧州データ保護委員会が設置されることになった。この委員会は、既存の第 29 条作業部会の役割を担うものではないかと考えられている。

第 29 条作業部会[225]

・構成員：EU 加盟国及び欧州連合自体のデータ保護監督機関の長等

・役割： ｉ）データ保護の諸問題に関する各国の専門家の意見の欧州委員会への提出

ⅱ） データ保護執行機関の協力を経た全ての加盟国における EU 指令の統一的な適用の促進

ⅲ） データ保護及びプライバシーの処理に関する自然人の権利及び自由に影響を及ぼす共同体の措置の欧州委員会への忠告

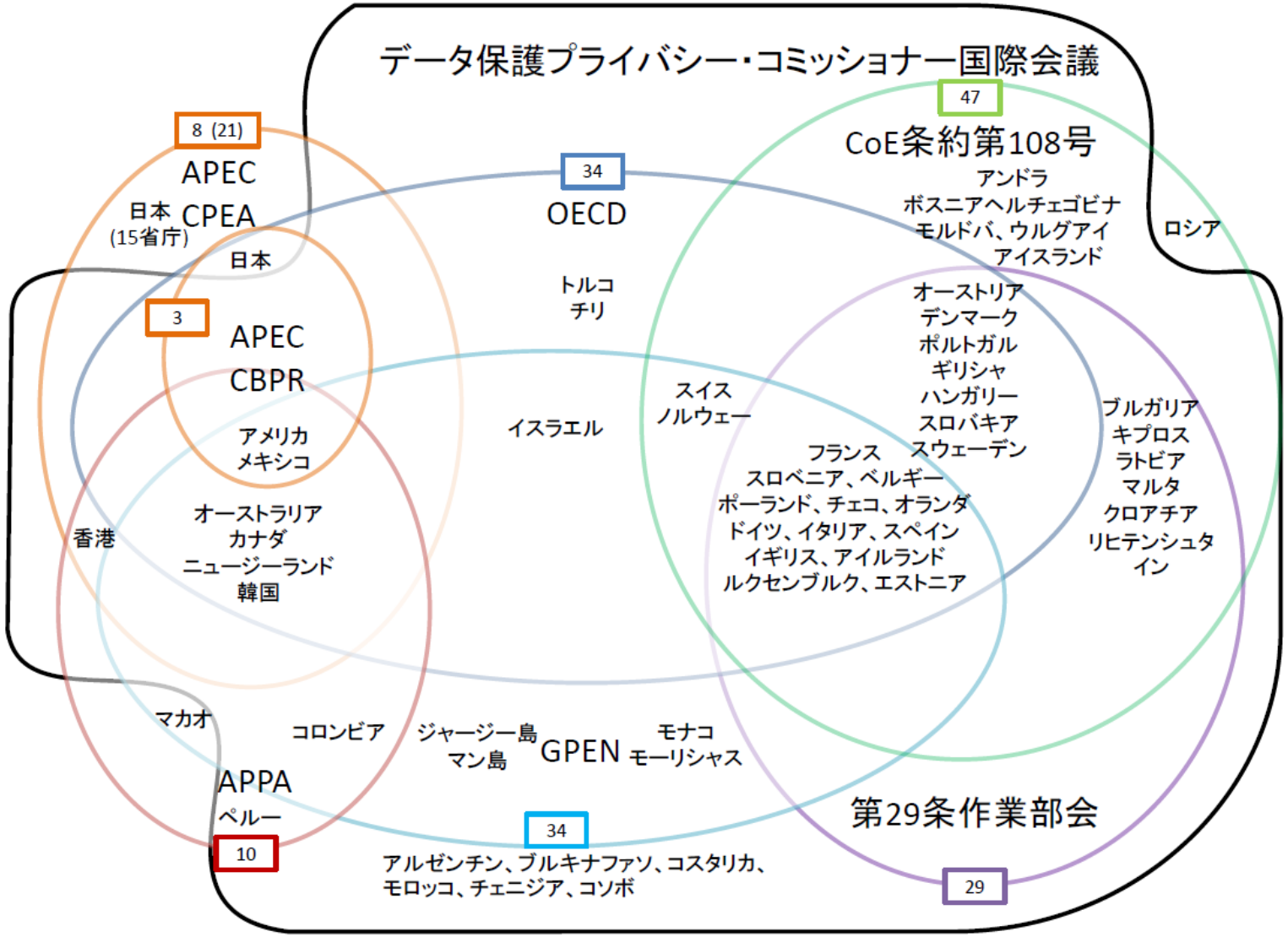
ⅳ） 欧州共同体におけるデータ保護及びプライバシーの処理に係る個人の保護に関する問題について市民全般、特に共同体に対する勧告

その他、定期的な会合を設け、各加盟国の執行状況や越境的な諸問題について検討を行っている。

---

224 Office of the Privacy Commissioner of Canada, “Data protection authorities urge Google to address Google Glass concerns”, News release, 18 June 2013. http://www.priv.gc.ca/media/nr-c/2013/nr-c_130618_e.asp (last visited 27 March 2014).

225 Yves Poullet & Sege Gutwirth, *The Contribution of the Article 29 Working Party to the Construction of a Harmonised European Data Protection System: an Illustration of ‘Reflective Governance’?*, in Défis du droit à la protection de la vie privée 570 (Verónica Perez Asinari & Pablo Palazzi eds., 2008).


データ保護プライバシー・コミッショナー国際会議
8 (21)
APEC
日本 CPEA
(15省庁)
日本
3
APEC
CBPR
アメリカ
メキシコ
香港
オーストラリア
カナダ
ニュージーランド
韓国
マカオ
コロンビア
APPA
ペルー
10
34
OECD
トルコ
チリ
イスラエル
ジャージー島
マン島
GPEN
モナコ
モーリシャス
34
アルゼンチン、ブルキナファソ、コスタリカ、
モロッコ、チェニジア、コソボ
47
CoE条約第108号
アンドラ
ボスニアヘルチェゴビナ
モルドバ、ウルグアイ
アイスランド
ロシア
スイス
ノルウェー
オーストリア
デンマーク
ポルトガル
ギリシャ
ハンガリー
スロバキア
スウェーデン
フランス
スロベニア、ベルギー
ポーランド、チェコ、オランダ
ドイツ、イタリア、スペイン
イギリス、アイルランド
ルクセンブルク、エストニア
ブルガリア
キプロス
ラトビア
マルタ
クロアチア
リヒテンシュタイン
第29条作業部会
29

2　欧州評議会条約第 108 号と現代化提案
（Council of Europe’s Convention 108 and its Modernisation Proposal）[226]

宮下紘（中央大学）

１．　欧州人権条約第 8 条―私生活尊重の権利

欧州人権条約（the European Convention on Human Rights）は、第二次世界大戦の後、欧州諸国の法の支配、民主主義、人権及び社会の発展の目的として、1950 年 11 月 4 日にローマで署名され、1953 年に発効された。同条約は、その管轄内のすべての者に対し、第 1 章で規定された権利及び自由を保障することが義務付けられている（第 1 条）。

締約国の義務の履行を確保するために、1959 年にフランス・ストラスブールに欧州人権裁判所（the European Court of Human Rights（ECtHR））が設置された。同裁判所は個人、集団、NGO、法人から同条約の違反の申立の審理を行い、締約国が条約の義務を履行するよう監督している。また、欧州評議会の一又は複数の加盟国が別の加盟国を提訴することも可能である。2014 年 2 月現在、47 の条約締約国があり、EU 加盟 28 か国はすべて締約している。

データ保護の権利は、欧州人権条約には明文規定がされていないものの、「すべての者が私生活、家庭生活及び通信の尊重の権利を有する」と規定する第 8 条にデータ保護の権利が含まれると解される。実際、欧州人権裁判所は、通信の侵害、様々な形態の監視、また公的機関による個人データの蓄積からの保護といったデータ保護の問題について審理してきている。欧州人権条約第 8 条については、国家からの私生活等の権利の侵害を保障しているのみならず、一定の状況下では私生活等の尊重を確保するために国家による積極的な義務を課していると解されている。

（１）法的保障の範囲

欧州人権条約第 8 条の私生活尊重の権利については、私生活・家庭生活のほかに、住居

[226] 本稿の執筆にあたり、2014 年 3 月に欧州評議会、欧州人権裁判所、ナミュール大学においてそれぞれヒアリング調査を実施させていただいた。ヒアリングに対応していただいた関係者にこの場を借りて謝意を記す。また、ヒアリングに際し、ストラスブール総領事館にお世話になり、併せて御礼申し上げる。

と通信を明示的に保障している[227]。また、通信傍受、監視、公的機関による個人データの蓄積からの保障等のデータ保護の問題が含まれると解されてきた[228]。

（２）法的性格

国家の積極的な義務の有無の判断については、統一的な判断基準がないため、状況、主題となっている問題、その背景を考慮に入れて判断することとなる[229]。第 8 条については、①締約国の共通の法的根拠・慣行が存在しているかどうか、②問題となる背景について特に子どもが関係するかどうか、といった判断要素を斟酌する必要がある[230]。

（参照条文）

欧州人権条約第 8 条 「私生活及び家庭生活への尊重の権利」

1. すべての者は、その私生活、家庭生活、住居及び通信への尊重を受ける権利を有する。

2. この権利の行使に対しては、法律に従い、かつ国土の安全、公共の安全もしくは国の経済的福利のため、混乱もしくは犯罪の防止のため、健康もしくは道徳の保護のため、または他者の権利及び自由の保護のため民主的社会において必要な場合以外、公的機関によるいかなる干渉があってはならない。

２．欧州評議会条約第 108 号

---

227 欧州人権条約第 8 条に関する解説としては、倉持孝司「プライヴァシーの権利と、私生活・私的生活の尊重―憲法学の視点から―」国際人権 17 号（2006）40 頁以下、谷口洋幸「プライバシーの権利と私生活・私的生活の尊重」国際人権 17 号（2006）45 頁以下、参照。

228 *See e.g.*, ECtHR, *Malone v. the United Kingdom*, No. 8691/79, 2 August, 1984（本判決の評釈は、倉持孝司「警察による電話盗聴および『メータリング』」戸波江二ほか編『ヨーロッパ人権裁判所の判例』（信山社・2008）342 頁、参照）;ECtHR, *Copland v. the United Kingdom*, No. 62617/00, 3 April 2007.

229 *See e.g.*, ECtHR, I v. Finland, No. 200511/03, 17, July 2008; ECtHR, K.U. V. Finland, No.2872/02, 2 December 2008; ECtHR, X and Y v. the Netherlands, 26 March 1985, § 23, Series A no. 91.
欧州人権条約第 8 条の積極的義務の解説については、ディートリッヒ・ムルスヴィーク・永田秀樹訳「ヨーロッパ人権条約による積極的義務」ノモス 22 号（2008）83 頁以下、渡辺豊「欧州人権裁判所による社会権の保障」一橋法学 7 巻 2 号（2008）459 頁以下、中井伊都子「私人による人権侵害への国家の義務の拡大（一）（二）・完」法学論叢 139 巻 3 号（1996）41 頁以下、法学論叢 141 巻 2 号（1997）34 頁以下、参照。

230 *See* URSULA KILKELLY, THE RIGHT TO RESPECT FOR PRIVATE AND FAMILY LIFE: A GUIDE TO THE IMPLEMENTATION OF ARTICLE 8 OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS 8 (2001).

（1）条約第 108 号の経緯

欧州評議会では 1970 年代に入り、閣僚委員会において欧州人権条約第 8 条を参照しつつ個人データの保護に関する決議を採択していった[231]。その後、1976 年 11 月から 1979 年 5 月までの間にデータ保護専門家委員会が 4 回会合を設け、データ保護に関する条約文書の作成が行われた。文書作成の過程では、OECD（経済開発協力機構）及びオブザーバーとしての 4 つの非加盟国（オーストラリア、カナダ、日本、米国）とも緊密に連携していった（説明書 15 項）。

そして、1981 年 1 月 28 日にいわゆる条約第 108 号（Convention 108）、「個人データの自動処理に係る個人の保護に関する条約（Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data）」の署名が行われた。そして、条約第 108 号は 1985 年 10 月 1 日に発効された。条約第 108 号はデータ保護分野において唯一拘束力ある国際的文書として存在してきた。すなわち、条約の自動執行力（self-executing）がなく、条約から直接個人の権利を導き出すものではないが、条約の批准国は、データ保護の各規定について国内法に導入することが義務付けられている（説明書 38 項）。国内法への導入方法は、当該国の憲法や法制度に基づき異なる形態で行われ、行動規範なども奨励されるが、拘束力ある方法での導入が前提とされている（説明書 39 項）。

条約第 108 号はリスボン条約に伴う 1999 年の改正が行われ[232]、2001 年には条約第 108 号の監督機関及び越境データ流通に関する追加議定書が採択された[233]。この追加議定書の採択により、いわゆる第三国である非加盟国への越境データ移転に関する規定と、データ保護の監督機関の国内の強制的設置に関する規定が導入された。ちなみに、条約第 108 号が署名された 1 月 28 日は「データ保護の日（Data Protection Day」として国際的なプライバシー保護のための日としてイベントが開催されてきた（2006 年 4 月 26 日欧州評議会閣僚委員会決定）。

2014 年 2 月現在、EU28 加盟国を含め 46 か国が条約第 108 号に批准している。また、欧州評議会の加盟国以外の国にも開かれており、加盟国以外のウルグアイは 2013 年 10 月

---

231 CoE, Committee of Ministers, *Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector*, 26 September 1973; CoE, Committee of Ministers, *Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector*, 20 September 1974.

232 CoE, *Amendments to the Convention for the protection of individuals with regard to automatic processing of Personal Data (ETS No. 108) allowing the European Communities to accede*, adopted by the Committee of Ministers, in Strasbourg, on 15 June 1999; Art. 23 (2) of the Convention 108 in its amended form.

233 CoE, *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, CETS No. 181*, 2001.

4 日に批准し、モロッコも批准のための交渉を行っている。また、第 30 回データ保護プライバシー・コミッショナー国際会議（2008 年 10 月・ストラスブール開催）において、欧州評議会の加盟国以外の国にも条約第 108 号の締結が推奨され、同条約が各国のデータ保護監督機関の協力促進となることが決議として採択された[234]。

現在の条約第 108 号は、7 章 27 条からなり、大きく分けて次の 3 部分から構成される。

① 基本原則に関する規定

② 越境データ移転に関する特別規則

③ 加盟国間における相互援助及び調査の仕組み

（２）条約第 108 号の現代化作業

欧州評議会は、デジタル分野におけるプライバシー保護の強化と条約のフォローアップの仕組みを強力なものとすることを目的として、2011 年以降条約第 108 号の現代化（modernisation）という改正の検討を行ってきた。2012 年 11 月 27～30 日に開催された第 29 回総会において諮問委員会による「現代化の提案」が採択されている[235]。

＜現代化作業の主な経緯＞

2010 年 10 月　プライバシーへの課題に対する欧州評議会の対応を公表（第 32 回データ保護プライバシー・コミッショナー国際会議（イスラエル・エルサレムにて））

2010 年 11 月　第 21 次総会において事務総局長が現代化への作業を表明

2011 年 3 月　第 23 次総会においてコンサルテーションによる結論報告

コンサルテーションはナミュール大学（Cécile de Terwangne & Jean-Philippe Moiny）が実施、報告書は 2011 年 6 月 21 日公表[236]

2011 年 10 月　第 25 次総会において「現代化提案」の公表[237]

2011 年 6 月～2012 年 11 月　「現代化提案」の草案審議

2012 年 11 月　第 29 次総会において「現代化提案」の採択

---

[234] 30th International Conference of Data Protection and Privacy Commissioners, *Resolution on the Urgent Need for Protecting Privacy in a Borderless World, and for Reaching a Joint Proposal for Setting International Standards on Privacy and Personal Data Protection*, 17 October 2008.

[235] CoE, *The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; Propositions of Modernisation*, 27-30, November 2012 (29th Plenary meeting).

[236] Cécile de Terwangne & Jean-Philippe Moiny, *Report on the consultation on the modernisation of Convention 108 for the protection of individuals with regard to automatic processing of personal data*, 21 June 2011.

[237] CoE, *The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; Modernisation of Convention 108: Proposals*, 15 November 2011.

2013 年 7 月　 データ保護特別委員会の設置

（３）データ保護特別委員会

2013 年 7 月 10 日に欧州評議会条約第 108 号現代化の最終文書を基に条約改正作業に入るため、データ保護特別委員会（Ad Hoc Committee）が設置された[238]。同委員会の任務は、2012 年 11 月に採択された条約第 108 号現代化提案（解説報告を含む）を閣僚委員会に提出するための最終準備を行うことである。特別委員会は、欧州評議会の加盟国、欧州評議会オブザーバーの地位にある国や欧州連合等の参加国（participants）（投票権なし）、オブザーバー（投票権なし）から構成される。

第 1 回会合（73 名が出席）は 2013 年 11 月 12 日～14 日に欧州評議会において開催された。第 1 回会合では、議長（Seamus Carroll：アイルランド）と副議長（Monique Cossali Sauvain：スイス）の選出のほか、条約の現代化提案についての意見交換が行われた。日本はストラスブール総領事がオブザーバーの地位にあることから、参加国として同総領事専門調査員と日本から消費者庁が出席した。日本のほかに、欧州連合、米国、メキシコも参加している。

今後、欧州評議会の閣僚委員会に提出する条約第 108 号の現代化の改正条約案の最終審議が行われ、閣僚委員会の審議を経て、条約の改正が行われる予定となっている。なお、第 2 回会議は 2014 年 4 月、第 3 回会議は 2014 年 9 月に開催される予定である。

３．欧州評議会条約第 108 号のデータ保護に関する基本原則と改正案[239]

（１） 目的

すべての個人に対し、自己に関する個人データの自動処理に関する権利と基本的自由の

---

238 欧州評議会規則及び閣僚委員会決議（Resolution CM/Res(2011)24 on intergovernmental committees and subordinate bodies, their terms of reference and working methods）に基づき設置された特別委員会である。

239 現在、条約第 108 号が改正作業中であることから、本報告書において「現代化による変更点」として示したのは、第 29 次総会（2012 年 11 月 27 日～30 日）で採択された"The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [ETS No.108]: *Propositions of Modernisation*"に基づき執筆している。また、説明書については、特別委員会において審議された 2013 年 12 月 18 日現在の草案 Council of Europe, Bureau of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data: *Draft Explanatory Report of the Modernised Version of Convention 108*, 18 December 2013.に基づき執筆している。本報告書が公表後、それぞれの文書が改正される可能性があることに注意を要する。

尊重、特にプライバシーの権利の尊重を保障することを目的としている。この保障は国籍や居所に関わらず、すべての個人に及ぶものと解される。データ保護の権利は、絶対的な権利ではなく、表現の自由や他の基本的権利及び自由との調整が必要な場合が生じるため、あらゆる利益の間の慎重な衡量が行われなければならない。

現代化提案には、前文に「人間の尊厳」、「個人データ及び当該データの処理をコントロールする権利」が明記され、また「グローバルな水準でのプライバシー及びデータ保護への尊重という基本的な価値の促進」が謳われている。

条約第 108 号	現代化による変更点
・自動処理される個人データの国境を越える流通の増大にかんがみ、すべての個人の権利及び基本的自由の保護措置、特にプライバシーの尊重の権利を拡大することが望ましい（前文）。 ・プライバシーの尊重及び情報の自由な流通の基本的価値を調和させる必要性を認識する（前文）。 ・すべての個人に対し、自己に関する個人データの自動処理に関する権利と基本的自由、特にプライバシー権を尊重されるための各加盟国の確保することを目的とする（第 1 条）。	・前文に「人間の尊厳及び特に個人データとその処理へのコントロールの権利を通じてすべての者の人権並びに基本的権利の保障を図ることを目的」という形で「人間の尊厳」と「個人データとその処理へのコントロールの権利」という文言が追記された。 ・前文に「グローバルな水準でのプライバシー及びデータ保護への尊重という基本的な価値の促進」という変更が行われている。 ・「処理がなされているときの個人データの保護」が追加された（1 条）。

○表現の自由との調整

データ保護の権利は、絶対的な権利ではない。表現の自由や他の基本的権利及び自由との調整が必要な場合が生じるため、データ保護の権利はあらゆる利益の間の慎重な衡量が行われなければならない（説明書（改訂中）9 項）。私生活保護の権利やデータ保護の権利については、欧州人権条約第 10 条が「すべてのものが表現の自由の権利を有している」と規定し、また「名誉又は他者の権利の保護」（第 10 条 2 項）という義務と責任を要求していることから、慎重な衡量が必要となる。

≪欧州人権裁判所の判例≫

Von Hannover v. Germany (No.2), ECtHR, Nos. 40660/08 and 60641/08, 7 February 2012

モナコ公国プリンセスのスキー休暇中の写真掲載の差止めが認められなかった事例

たとえ公的な文脈においても他者との交流関係の圏域が欧州人権条約第 8 条によって保障され、公的便実であっても写真の公表が私生活を侵害することがある（para95）。もっとも、私生活への保障の権利は表現の自由の権利と調整がされる必要がある（para106）。一般的な利害関心事であるかどうか、また写真が撮影された状況等を考慮すれば、国内裁判所の判断は適切であり第 8 条の違反は認められない（para126）。

なお、私生活の権利の侵害を容認したVon Hannover v. Germanyの第一次訴訟[240]において、個人データの蓄積と再生産を可能とする新たな通信技術に対処するため私生活の保護への高度の警戒が必要となりつつあることが指摘されている（para70）。

・Von Hannover v. Germany 第一次訴訟には、Boštjan Zupančič 裁判官による同意意見が付されている。Zupančič 裁判官は、「一定程度米国の影響の下で、裁判所がプレスの自由を盲目的に崇拝してきたと考えている」と述べ、「何が私的で隠匿されるものか、また何が公にされ保護されないかについての異なる種類の衡量へと振り子を戻すべき時にある」。（ヒアリング結果・欧州人権裁判所）

Axel Springer AG v. Germany, ECtHR, No. 39954/08, 7 February 2012

テレビに出演する有名人の薬物使用の逮捕有罪報道が私生活保護を侵害しないと事例

表現の自由には義務と責任が伴うものであり、私生活の尊重の権利との衡量が必要となる場合、次の 3 点について検討しなければならない（para89-95）。

① 公表された写真や記事が一般的な利害関係の討論へ寄与するものかどうか
② 対象となる人物が公的人物であるかどうか、また公的な関心事を話題とするものかどうか
③ 対象となる人物の行為が写真や記事よりも前に公表されているかどうか
④ 情報の入手方法はどのようなものか、またその情報は正確かどうか
⑤ 公表された写真や記事の内容、形態、帰結はどのようなものか
⑥ 刑罰はどの程度のものであったか

これらの事項を検討すると、表現の自由と私生活の保護との間の比例原則に合理的な関係があったとはいえず、表現の自由を侵害していた。

240 鈴木秀美「有名人のプライバシーと写真報道の自由」戸波江二ほか編『ヨーロッパ人権裁判所の判例』（信山社・2008）328 頁、参照。

Mosley v. the United Kingdom, ECtHR No. 48009/08, 10 May 2011

日曜発刊の新聞紙が F1 レーサーの性生活の写真と記事を報道したことに対し、イギリス国内で事前に本人に通知する義務に違反しているかどうかは私生活の保護と表現の自由に関する一般原則について検討しなければならない（para105）。本人への事前通知義務は私生活の保護をより効果的に保障するものであるが、ジャーナリズムへの制約についても検討しなければならない（para121）。

第 1 に、事前通知義務は公共の利益が認められる場合には萎縮効果をもたらし、本件ではレーサーの性生活がナチスのロールプレイであるという記事であり、公共の利益に該当する（para126-127）。第 2 に、事前通知義務は検閲の形態としての制約となっている（para129）。以上のことから、第 8 条は法的に拘束力ある事前の通知要件を要求していない（para132）。

Biriuk v. Lithuania, ECtHR No. 23372/03, 25 February 2009

ある村でエイズに感染しているという病院検査の事実を新聞紙で公表したことは、純粋に私的性質のものであり、第 8 条の保護の対象となる。また、近所に知られることとなり村での社会生活からの排除を受けることとなり、家族のプライバシー権を干渉することとなる（para42）。また、このような報道は社会への一般的な利益の討論にも寄与せず、正統な公共の利益を有するとは言えない（para43）。さらに、個人の健康状態に関する情報の秘密保持を保護する規範が国内法でも含まれており、個人がプライバシーを侵害された場合裁判所もそれに従うこととされている（para45）。

（２） 適用範囲と適用除外・制限

保護の対象は、官民に共通して自動処理された個人データファイル及び個人データの自動処理である。個別分野の保護については、警察・刑事司法、通信サービス 、雇用 、医療 、金融 、統計の各分野に勧告によって保護措置を定めている。

適用除外及び制限については、国土の安全、公共の安全、国家の財政上の利益の保護又は犯罪行為の抑止、データ主体又は他のデータ主体の権利及び自由の保護を理由として、保護の基本原則が制限されうる。また、統計又は学術研究の目的のために使用される場合、データ主体の権利行使の制限をする法律を定めることができる。

なお、現代化提案では、純粋に個人的又は家族活動を目的とする自然によるデータ処理には適用されないことが示されている。

条約第 108 号	現代化による変更点
【適用範囲】	
・公的部門及び民間部門における自動処理された個人データファイル及び個人データの自動処理について条約が適用される（第 3 条 1 項）。	・条約の管轄に服するデータ処理の主体に対して適用される、という修正が行われている。また、純粋に個人的又は家族の活動のための自然人によるデータ処理については適用されないことが明文化されている。 ・条約第 108 号では一定の個人データの類型が適用されない加盟国については欧州評議会事務総局長に通知する必要があったが、この規定が削除されることとなった。 ・前文において「グローバルなレベルでのプライバシー及び個人データの保護の尊重という基本的価値の促進が必要である」ということも新たに明記され、条約第 108 号がプライバシー及び個人データの保護に関する「グローバルなレベル」の問題を対象としている。
【適用除外と制限】	
・条約が定める基本的な権利及び義務については、本条の定めを除き、データの性質、特別の種類のデータ、追加的保護措置の規定の適用除外が認められない(第 9 条 1 項)。 ・次に掲げる民主主義社会に必要な措置に当たる場合にのみ制限することが認められる（第 9 条 2 項）。 a. 国土の安全、公共の安全、国家の財政上の利益の保護又は犯罪行為の抑止 b. データ主体又は他のデータ主体の権利及び自由の保護 ・統計又は学術研究目的のために使用される自動処理個人データファイルについて	・適用制限される項目について、経済・財政上の利益の保護、犯罪の防止が補足された（第 9 条 1 項 a 号）。 ・他のデータ主体の権利及び自由の保護として、表現の自由が明記された（第 9 条 1 項 b 号）。 ・越境データ移転の規制についても、法令の基づく場合や民主主義社会における必要な措置を構成する場合に適用制限が認められる（第 9 条 2 項）。

は、プライバシー侵害の危険がないことが明白であれば、データ主体の権利行使の制限を法律で定めることができる（第 9 条 3 項)。	

○警察・刑事司法におけるデータ保護

警察分野における個人データの利用を規制する勧告[241]において、警察のあらゆる活動における個人データの取扱いに関する規定を設けている。センシティブ・データの収集制限、データ主体のアクセス権等、データの保存期間といった原則が置かれている。

また、日本も批准しているサイバー犯罪に関する条約[242]においてデータ主体の権利に違反した行為を処罰する規定が設けられている。サイバー犯罪条約については、条約第 108 号とともに「人権・法の支配」課が所管している。

≪欧州人権裁判所の判例≫

S. and Marper v. the United Kingdom, ECtHR Nos. 30562/04, 4 December 2008[243]

無罪・不起訴となった被疑者の指紋と DNA の廃棄が認められた事例

強盗未遂とハラスメントで逮捕された 2 名の指紋と DNA が採取されたが、後にそれぞれ無罪と不起訴になり、指紋と DNA 試料の廃棄を求めた。DNA 情報は客観的で反証不可能であり、特定の個人や近親者との遺伝関係を識別手段として用いられる。このような情報を保全することは個人の私生活の権利の干渉になる(para75)。さらに、DNA は民族出自に関する情報を引き出す可能性があり、DNA の保全はセンシティブで私生活権利に影響を及ぼす（para76)。指紋の保全についても私生活尊重の権利の干渉を構成する（para86)。指紋等の個人情報の保全が比例原則に従い、公的な利益と私的な利益との公正な衡量を行っているかどうかについて、細胞サンプルの保全は特に侵害の度合いが強いため、保全は公的利益に比例しておらず、また民主社会に必要であるともみなさないため、第 8 条違反となる（para125)。

241 CoE, Committee of Ministers, *Recommendation No.R(87) 15 regulating the use of personal data in the police sector*,17 September 1987.

242 CoE, Committee of Ministers, *Convention on Cybercrime*, CRTS No.185, Budapest, 23 November 2001.

243 本判決の評釈として、江島晶子「犯罪予防における DNA 情報・指紋の利用と私生活の尊重を受ける権利--S およびマーパー対イギリス事件」国際人権 20 号（2009）120 頁、井上悠輔「被疑者段階で採取された試料・DNA 型データの保有継続をめぐって」医療・生命と倫理・社会 8 号（2009）74 頁、参照。

○個別分野のデータ保護

条約第 108 号には個別分野のデータ保護に関する規定はないものの、欧州評議会は特に留意が必要となる通信サービス[244]、雇用[245]、医療[246]、金融[247]、統計[248]の各分野について勧告を出し、各分野の特性に応じたデータ保護のあり方が示されている。

（3）保護の範囲

個人データとは、識別された又は識別することのできる個人に関するいかなる情報を意味する（現代化提案に変更なし）。記述、口頭によるコミュニケーション、監視カメラのフィルムを含む映像・画像、及び音声は個人データに含まれる。
識別の判断基準、匿名化・仮名化に関する明文規定はないが、勧告や説明書において示されている。

条約第 108 号	現代化による変更点
【個人データ】	
・「個人データ」とは識別された又は識別することのできる個人に関するいかなる情報（第 2 条 a 項）	変更なし
【自動処理】	
・「自動処理」とは、自動処理によって個人データに対して行われる作用、特にデータの蓄積、データの論理的・計算上の作用、変更、削除、回復、拡散（第 2 条 c 項）	・「自動処理」の定義から「データ処理」に名称変更がされた上で、特にデータの収集、蓄積、保存、変更、回復、開示、入手、削除、破壊又はデータに関する論理的・計算上の作用と詳細な記述になっている。

○映像・画像及び音声

---

[244] CoE, Committee of Ministers, *Recommendation No.R(95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services*, 7 February 1995.
[245] CoE, *Recommendation No.R(89) 2 on the protection of personal data used for employment purposes*, 18 January 1989.
[246] CoE, *Recommendation No.R(97) 5 on the protection of medical data*, 13 February 1997.
[247] CoE, *Recommendation No.R(90) 19 on the protection of personal data used for payment and other operations*, 13 September 1990.
[248] CoE, *Recommendation No.R(97) 18 on the protection of personal data collected and processed for statistical purposes*, 30 September 1997.

・識別された又は識別することのできる個人に関する情報には、欧州人権裁判所の判例によって、記述、口頭によるコミュニケーション[249]、監視カメラのフィルムを含む映像・画像[250]、及び音声[251]は個人データに含まれる。

≪欧州人権裁判所の判例≫

Amann v. Switzerland, ECtHR, No.27798/95, 16 February 2000

ビジネスの取引に関する電話を検察当局が傍受した事例

欧州人権条約 8 条にいう「私生活」は制限的に解されてはならず、「私生活」を広く解釈することは、条約第 108 号のすべての者の権利と基本的自由、特にプライバシー権（第 1 条）と個人データ（第 2 条）の保護の範囲とも一致するものである（para65）。

Bernh Larsen holding AS and Others v. Norway, ECtHR No.24117/08, 14 March 2013

共同利用のサーバー上のデータを検査のため税務当局に提出を認めた事例

欧州人権条約第 8 条にいう「家庭」には住宅内を含むが、一定の職務上あるいはビジネス上の建物内にもその保障が及ぶ（para104）。そのため、ビジネスで利用する建物内であっても電子データの捜索及び押収は家庭生活の尊重及び通信への干渉となると認定する（para106）。もっとも、税務当局によるデータの提出は第 8 条 2 項における合法性の要件に一致し、認められる（para134）。

Uzun v. Germany, ECtHR No.35623/05, 2 September 2010

GPS による監視が私生活の侵害となるが、比例原則から許容された事例

公道において爆破攻撃に関与した被疑者の行動を全地球測位システム（GPS）を用いて追跡することは、人の行動、意見又は感情に関する情報を開示することになるため、私生活尊重の権利への干渉の度合いが他の可視的な監視による場合に比べ大きなものとなる（para52）。もっとも、8 条 2 項の法令に基づく場合に該当すれば、私生活の侵害違反とみなされず、本件ではドイツ国内法により国内裁判所が比例原則に基づき審査を行っていることから、監視の乱用への十分な保護措置が施され私生活侵害の違反はないと結論付けられた（para69-74）[252]。

---

249 ECtHR, Kopp v. Switzerland, No.223224/94, 25 March 1998.
250 ECtHR, Peck v. the United Kingdom, No.44647/98, 28 January 2003.
251 ECtHR, P.G. and J.H. v. the United Kingdom, No.44787/98, September 2001.
252 なお、本件は監視のための事前通知の義務を放棄したものとは解されていない。*See* Paul De Hert & Franziska Boehm, *The Rights of Notification after Surveillance is Over: Ready for Recognition?*, in DIGITAL ENLIGHTENMENT YEARBOOK 2012, 35 (Jacques Bus et. al. eds., 2012).

○識別の判断基準

・一般的な識別の判断について記述はない。もっとも、欧州評議会は 1990 年の支払いデータに関する勧告[253]において「識別に不合理な量の時間、コスト、労力を要する場合は、個人が『識別でき』ないものとみなされる」（第 1 条 2 項）と記述されている。また、識別化や選り分けることができる場合にも識別は含まれる（説明書（改訂中）18 項)。ただし、非常に洗礼された方法による個人の識別は個人データには含まれないと解されている（説明書 28 項)。

・識別が不可能な場合は、管理者は本条約で規定される義務の履行のため追加的努力を行わなくてもよい（説明書（改訂中）19 項)。

○匿名化

・匿名化については、いかなる明白な識別データも伴わないが、関連する個人の識別を許す特定の場合に、データは匿名化されているように思われる。しかし、たとえば、物理的・生理的・遺伝的・精神的・経済的・文化的又は社会的に関するデータ単体又はその結合により、データ管理者又はある主体が、特定の個人を識別することが可能であることについては、当該データは匿名化されているとはみなされない（説明書（改訂中）20・21 項)。

・データの匿名性は技術の進展に伴い適宜再評価されなければならない（説明書（改訂中）22 項)。

○仮名化

・明文規定はないものの、説明書 42 項において、仮名化に関する記述がある。すなわち、目的に必要な時間を過ぎて氏名と結びつく形態のデータの蓄積する場合、その人の氏名から不可逆的に隔離することを意味するものではなく、データと識別子が連結可能でないことを意味する。仮名化は暗号解読による鍵を用いて再識別化ができる点で匿名化と異なると解されている。

・仮名化（pseudonym）については、ソーシャル・ネットワーキング・サービスに関する勧告[254]において、オンライン上のアイデンティティに関するユーザーの選択を助長するものとして、「仮名化を利用する権利は自由な言論と情報と思想を授受する権利の観点と私生

[253] CoE, Committee of Ministers, *Recommendation No. R Rec (90) 19 on the protection of personal data used for payment and other related operations*, 13 September 1990.
[254] CoE, Committee of Ministers, *Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services*, 4 April 2012.

活への権利の観点の両方から保障されるべきである」ことが指摘されている。

○非識別情報（non-identifying information）

・欧州人権裁判所では、児童が自らの出自と母親を知る請求をしても、匿名を希望する母親の非識別情報へのアクセスを認めないイタリア法が欧州人権条約第 8 条に違反すると判断したが、何が匿名化情報や非識別情報に該当するかについては判断していない[255]。

（4）センシティブ・データの処理

データの特別な類型として、人種、政治的見解、宗教上又はその他の信仰、健康又は性生活に関する個人データが具体的に列挙されている。

現代化提案では、センシティブ・データと明記され、適当な保護措置を施した場合にのみ処理が認められる。また、遺伝データや違反行為、犯罪に関するデータなどが新たに列挙された。データ主体の最も親密な圏域に影響を及ぼし、個人の尊厳に対する差別や危害の潜在的リスクがある場合に特に留意が必要である。

条約第 108 号	現代化による変更点
・人種、政治的見解、宗教上又はその他の信仰、健康又は性生活に関する個人データは適切な保護措置が国内法で規定されていない限り自動処理をしてはならない。有罪判決についても同様とする。（第 6 条）	・第 6 条の見出しの「データの特別類型」は「センシティブ・データの処理」と名称変更がなされた。 ・遺伝データ、違反行為、犯罪、関連する安全措置に関する個人データ、個人識別をする生体データの処理、人種の出自、政治的見解、労働組合員、宗教上又はその他の信仰、健康又は性生活に関する情報の個人データの処理については適切な保護措置が国内法で規定されている場合のみ自動処理ができると規定されている（第 6 条 1 項）。 ・適当な保護措置とは差別のリスクを減少させることを指す（第 6 条 2 項）。

○センシティブ・データの類型

255 Godelli v. Italy, ECtHR, No.33783/09, 25 September 2012 para 57.

・センシティブ・データについては、条約第 108 号で列挙されているすべてを記載すべきかどうかについては議論があるが、いかなる者もいかなる理由でも利用されるべきではない、という前提に立つべきである。（ヒアリング結果・欧州評議会）

○医療データの保護措置

・医療データは、公衆衛生、真に危険の防止及び特定犯罪の抑止、その他重要な公共の利益のために法律上認められた場合のみ収集と処理が認められる。また、疫学研究目的で医療データを利用する場合は、可能な場合は常に匿名化しなければならない。匿名化ができない場合、データ主体からの研究目的への同意、代理人等による同意、国内法が指定する機関での重要な公共の利益のための研究、又は法律上認められ公衆衛生に必要な研究な場合にのみ研究調査に医療データを利用することができる。また、データ移転についても、加盟国でない第三国に移転する場合、又は同等の保護原則がある場合にのみ、医療データの移転ができる[256]。

・また、医療データの保護は私生活尊重の権利を享受するために根本的な重要性を有しており、健康データの秘匿性の尊重は条約批准国の不可欠な原則をなしていること、そして患者のプライバシーの尊重のみならず医療専門家における信頼維持の観点からも重要であることが欧州人権裁判所においても確認されている[257]。

（５）データ主体の権利

何人もアクセス権・訂正権・消去権を有する。すなわち、自動処理個人データファイルの存在や管理者の身元を確認することができ、またデータ保護基本原則に違反してデータ処理が行われた場合、当該データを訂正・消去することができる。データ主体の権利は、民主社会に必要な措置のため他の権利や正当な利益との調整が必要な場合がある。

現代化提案では、新たに異議申立の権利が明記されている。これら一連の権利の集合は、「忘れられる権利」として知られる効果にプラグマテッィクな形で相当するものであると解されている。

条約第 108 号	現代化による変更点
【アクセス権】	

[256] CoE, *Recommendation No.R(97) 5 on the protection of medical data*, 13 February 1997.

[257] Z v. Finland, ECtHR, No.22009/93, 25 February 1997, para 95.

・何人も自動処理個人データファイルの存在や管理者の身元等を確認することができる。（第 8 条 a 項） ・合理的な期間で過度な支出を伴うことなく、自己のデータが処理されているかどうか通知を受けることができる。（第 8 条 b 項）	・データの出自に関するあらゆる情報とデータ処理の透明性の要件として示された情報が新たにアクセス権の対象となった（第 8 条 c 項）。 ・要請に対し、データ処理の理由とデータ主体に適用されたその帰結を知ることができる（第 8 条 d 項）
【訂正・消去権】	
・何人も基本原則に違反してデータ処理が行われた場合、当該データを訂正又は消去することができる。（第 8 条 c 項） ・訂正・消去等への応答がない場合、救済を求めることができる。（第 8 条 d 項）	・要求に応じ、（訂正又は消去することができる）という文言が追記された（第 8 条 e 項）。
【異議申立権】	
・明文規定なし	・管理者が処理の正当な根拠を示せない限り、個人データの処理に対し何時も異議申立することができるという条項が追加された。（第 8 条 b 項）
【救済の権利】	
・通知、訂正、消去の要求が遵守されないときは救済を受けることができる（第 8 条 d 項）。	・データ主体の居所に関わらず監督機関からの援助を受けることができることが明記された。（第 8 条 g 項）

○権利の行使

・データ主体の権利は他の権利や正当な利益との調整が図られなければならない。第 9 条に基づき、民主的社会に必要な措置を構成する場合にのみこれらの権利が制約されうるが、ケース・バイ・ケースの判断を必要とする（説明書（改訂中）73 項）。

○アクセス権

・アクセス権は原則として無償で実施すべきである。アクセス権の公正な公私を確保するため、分かりやすい形でコミュニケーションが標準的なデジタルな形態が適用されなければならない。

Gaskin v. the United Kingdom, ECtHR No.10454/83, 7 July 1989

自己の個人情報ファイルへのアクセス権が認められた事例[258]

幼少期に何人かの里親に育てられた記録が秘密として自治体に管理されていたため、その記録へのアクセスを求めた。自治体の公的記録の秘密保持があるものの、個人が自らの私生活・家庭生活に関する記録へのアクセスを求める利益が保障されなければならず、第8条に違反する（para49）。

○異議申立の権利

・大量のデータの自動処理によって個人像を浮き彫りにするプロファイリングについては、信用情報や勤務成績等について自動的な決定を行ってしまうことで、ときに不正確な結果や差別、偏見を生み出す可能性があり、自動的に個人に関する決定がされることに異議申立の権利が認められなければならない（説明書（改訂中）75項）。

・プロファイリングに関する勧告[259]において、プロファイリングを行う場合、データ管理者はデータ主体に対し、アクセス権・訂正権とともに異議申立の権利と苦情申立の権利の行使の条件に関する情報を付与することとされている。

Cemalettin Canli v. Turkey, ECtHR No.22427/04, 18 November 2008

過去の刑事事件の誤った記録提出が私生活尊重の権利を侵害するとされた事例

違法な組織の構成員として過去に2度刑事訴追されたが有罪とならなかった者の警察報告書が裁判所に提出されたが、その報告書中の有罪であった旨の不正確な情報は名誉を傷つけるものである（para35）。また、報告書には有罪とならなかった旨の記述が省略されており私生活尊重の権利に反する（para42）。

Ciubotaru v. Moldova, No.27138/04, 27 July 2010

民族出自の変更拒否が私生活尊重の積極的義務違反とされた事例

モルドバからルーマニアに民族出自の変更の求めを拒否された事案について、8条にはアイデンティティの詳細を確立する権利が含まれており、第8条に基づく自らの権利を主張するための効果的な手続枠組みが保障されなければならない（para49-51）。本件においては、自らの民族に関する主観的な認識以外にルーマニア民族集団との客観的に証明可能な関連性を有していることから私生活の効果的な尊重のための積極的な義務の履行を怠った（para58-59）。

---

258 本判決の評釈は、榊原秀訓「私生活の尊重と自己情報開示権」戸波江二ほか編『ヨーロッパ人権裁判所の判例』（信山社・2008）318頁、参照。

259 CoE, Committee of Ministers, *Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling*, 23 November 2010.

M.S. v. Sweden, ECtHR, No. 20837/92, 27 August 1997

本人の同意なしで医療データの社会保障局への提供が認められた事例

患者の同意なしに中絶を含む私的でセンシティブな医療データが開示されたことは私生活尊重への権利の干渉に関する問題となる（para35）。しかし、本件の医療データの社会保障局への提供は労働災害認定の目的であったことから、関連ある十分な根拠が認められ、その方法も正当な目的を実現するために不均衡であるとは言えない（para44）。

○消去権・「忘れられる権利」[260]

・現代化提案で審議されてきた利用目的の特定、処理の条件と正当性、訂正・消去の権利とともに異議申立の権利や同意の撤回の権利は、データ主体の保護の効果的な水準を示している。これら一連の権利の集合は、「忘れられる権利」として知られる効果にプラグマティックな形で相当するものであると解されている（説明書（改訂中）81 項）。

（６）義務の内容

既存の条約第 108 号には、義務の対象とファイル管理者としているが、現代化提案では「管理者」と「データ処理者」という分類が行われた。

個々の義務規定としては、合法なデータ処理、利用目的の特定と制限、データの正確性、安全管理措置、透明性という基本的な項目を列挙している。現代化提案では、データ保護違反の場合の通知義務が新たに導入された。

現代化提案では、新たに追加的措置として、原則と義務履行のための内部体制の構築、リスク分析の実施、デザイン段階からの個人データ保護の配慮、管理者のサイズ等に応じた措置の実施が明記された。

条約第 108 号	現代化による変更点
【データ管理者・データ処理者】	

[260] DELFI AS v. ESTONIA（no. 64569/09）が大法廷で係争中であり、インターネット上のニュース・ポータルサイト上の投稿の削除に関する許否が問われている旨、欧州人権裁判所 Zupančič 裁判官よりご紹介いただいた。

なお、条約第 108 号の現代化提案に「忘れられる権利」を明記すべきかどうかについては、あらゆる場面において必要性が認められたり、正当化できるかについて議論があった。*See* Sylvia Kierkergaard, Nigel Waters, Graham Greenleaf, Lee A. Bygrave, Ian Lloyd & Steve Saxby, 30 Years on- The Review of the Council of Europe Data Protection Convention 108, *Computer Law & Security Review*, vol. 27, p. 223, 227 (2011).

・「ファイル管理者」とは、国内法に従って、自動処理データファイルの目的、蓄積すべき個人データの種類及びデータに対し適用すべき操作を決定する権限を有する者（自人・法人等の団体）（第 2 条 d 項）	・「ファイル管理者」から「管理者」に名称変更 ・管理者の団体にデータ処理の決定権限を共同して行う者も含まれることになった。 ・「データ処理者」として、管理者に代わって個人データの処理を行う団体が新たに追加された（第 2 条 f 項）。
【合法なデータ処理】	
・自動処理される個人データは、公正かつ合法的に入手され、処理されなければならない（第 5 条 a 項）。	・第 5 条の見出しにデータ処理の正当性が明記された。 ・データ処理は正当な目的に関して比例しており、かつすべての段階であらゆる利益との公正な衡量を反映するものとされなければならない（第 5 条 1 項）。 ・データ処理の実施が、データ主体の自由な同意に基づくか又は法による正当な基盤を必要とする（第 5 条 2 項）。
【利用目的の特定と制限】	
・自動処理される個人データは、特定的でかつ正当な目的のため蓄積され、この目的に合致しない形で使用されてはならない（第 5 条 b 項）。 ・自動処理される個人データは、目的に照らして十分で、適切で、かつ過度なものであってはならない（第 5 条 c 項）。 ・自動処理される個人データは、蓄積された目的のために必要以上の長期間に特定できる形で保持されてはならない（第 5 条 e 項）。	・利用目的の要件に特定され正当な目的のほか、明示されたという要件が追加された（第 5 条 b 項）。
【データの正確性】	
・自動処理される個人データは、正確で、必要に応じ最新な状態に保たれていなけれ	・変更なし。

ばならない（第 5 条 d 項)。	
【安全管理措置】	
・偶発的もしくは権限のない破壊又は偶発的紛失並びにアクセス、改変又は伝播から個人データを保護するため、適切な安全管理措置をとらなければならない（第 7 条)。	・締約国は管理者、必要に応じ処理者に対する安全管理措置を講ずるものとする、という表現に変更された（第 7 条 1 項)。 ・データ主体の権利及び基本的自由を重大に干渉するデータ保護違反については、各締約国の監督機関に遅滞なく通知しなければならないとされた（第 7 条 2 項)。
【透明性】	
・明文規定なし	・管理者は、設置場所・居所、処理の目的、処理されるデータ、個人データの受領者、権利行使の方法、その他公正かつ合法的なデータ処理に関する情報をデータ主体に通知することで、データ処理の透明性を確保しなければならない（第 7 条 bis)。
【追加的措置】	
・なし	・管理者又は該当する場合処理者に条約の原則と義務の履行と内部体制の確立のためのあらゆる段階でのあらゆる適切な措置を講じるようしなければならない（第 8 条 1 項 bis)。 ・管理者と該当する場合処理者に予定されるデータ処理の権利と基本的自由への潜在的影響のリスク分析の実施を義務付けなければならない（第 8 条 2 項 bis)。 ・データ処理の製品及びサービスがデザインの段階からデータ保護の権利への配慮をしなければならない（第 8 条 3 項 bis)。 ・管理者のサイズ、処理されるデータの量と性格、リスクに照らし、本条の義務が適用されるものとする（第 8 条 4 項 bis)。

○管理者と処理者

・「管理者」とは、個人データの処理に関する意思決定権を有する主体を意味する。管理者はどこでデータが処理されていてもその処理に責任を有することになる（説明書（改訂中）24 項）。

・「処理者」とは、管理者の要請により処理を実行する管理者の代理として行動する別個の主体を意味する。管理者の労働者は処理者ではない。処理者が管理者の意思決定権を超えて処理を実施する場合、処理者は管理者とみなされる（説明書（改訂中）28 項）。

○処理の合法性

・人権条約第 8 条 2 項は、①法律に従い、かつ②国土の安全、公共の安全、犯罪の防止等のため、または②'民主的社会において必要な場合、を除き公的機関による私生活への干渉が認められないことを明らかにしている。データ処理にはこれら 2 つの合法性の条件を満たすことが必要とされる。

・合法性の基礎には、データ主体の不可欠な利益、実質的な公共の利益又は管理者の利益を上回る処理の利益の保護を目的とした必要な場合にのみ処理できるという考え方がある（説明書（改訂中 47 項）。たとえば、自然災害の状況では、緊急時という時間を限定することで、行方不明者の個人データの処理は公共の利益又はデータ主体の不可欠な利益に必要な場合である。（説明書（改訂中）49 項）。

・データ主体の同意に基づく処理については、同意が自由に与えられ、特定され、告知され、かつ明示的で明確なものでなければならない。そのため、沈黙や不作為は同意を構成するものではない（説明書（改訂中）44 項）。

・「法律に従い」（人権条約第 8 条 2 項）

Rotaru v. Romania, No.28341/95, 4 May 2000

ルーマニア法による安全保障上の情報の秘密ファイルの収集等が合法性違反とされた事例

ルーマニア諜報機関が共産主義体制の下で学生運動をしていた者の個人情報ファイルの保有と利用について、諜報機関が民主社会において正当な形で存在することを認めても、秘密の監視活動の権限は人権条約の下で許容される限度でなされなければならない（para47）。仮に第 8 条に違反することになれば、「法律に従い」という正当な目的への干渉があったこととなる（para48）。この「法律に従い」という文言は、当該疑いある措置が国内法に基づくことを要求されているだけでなく、さらに関係する人物がアクセスできるものであり、かつその効果の予見可能性がなければならない（para52）。ルーマニア法は諜

報活動を制約する規定がなく、情報保有の時間的制約もなく、また法の支配の要請として秘密監視の乱用に対する救済措置と監督手続が存在しない（para54-60）。したがって、法に基づかない私生活の情報の保有と利用は第 8 条の違反を構成する（para62）。

・正当な目的（国土の安全、公共の安全もしくは国の経済的福利のため、混乱もしくは犯罪の防止のため、健康もしくは道徳の保護）（人権条約第 8 条 2 項）

Peck v. the United Kingdom, No.44647/98, 28 January 2003

監視カメラの映像が本人の同意なしに公開されたことが違法とされた事例

自らの手を切り自殺を図ろうとした者が、公道の監視カメラに撮影され、その者の顔にぼかしを入れることなくナイフを持っている映像・画像が新聞紙等で公表された。公道であっても個人の行為を監視することは私生活の干渉を生じさせる（para59）。本件では公道での撮影自体が問題とされているわけではなく、その者が予見していない公表方法が私生活への干渉を生じさせている（para60）。本人の同意を得ずに、又はその者のアイデンティティにぼかしを入れることなしに映像を公表することは十分な根拠があったとは言えない。本件で映像を公表された者は国営・地方のメディアによるプライバシーへの深刻な干渉の被害者となってしまった（para85-86）。

・「民主社会に必要」（人権条約第 8 条 2 項）

Leander v. Sweden, No.9248/81, 26 March 1987

国土安全のための人物調査のための人事管理システムが合法とされた事例

海軍美術館の大工としての雇用について、人事管理システム上のリスクがあると判定され雇用拒否された者が、自らの情報が民主社会に必要であることを理由に登録が可能かどうか争われた。第 8 条 2 項における国土の安全の利益における民主社会に必要かどうかという基準については、社会の必要性とその正当な目的との比例性があるかが問題となる（para58）。本件では国土の安全の保護という目的のために必要とされているシステムであって、社会的必要性が認められる（para59）。そして、人事管理システムは、議会の委員会や議会のオンブズマン等によって監視されている（para65）。よって、第 8 条違反は認められない（para68）。

〇利用目的の特定と制限

・データが処理される目的との関係において過度なものであってはならないという要件は、比例原則を反映している（説明書（改訂中）54 項）。個人データの蓄積の時間制限に関する要件は、利用目的が実現されたらデータが消去されなければならないことを意味する（説

明書（改訂中）55 項)。

〇データの正確性

・データは正確であり、かつ必要に応じ、定期的に最新な状態にしておかなければならない（説明書（改訂中）53 項)。

〇安全管理措置

・技術的かつ組織な方法で個々の処理に対し特別な安全管理措置が講じられなければならない。個人データの性格、量、技術的な構造の脆弱性、データ・アクセスの制限、長期蓄積の要件等を考慮事項とする（説明書（改訂中）62 項)。

・個人への潜在的なリスクに対応する安全管理措置はデータ処理分野の現状のセキュリティの最高水準の方法と技術に基づかなければならない。コストは潜在的なリスクの深刻さと確率にふさわしいものとしなければならない（説明書（改訂中）63 項)。

≪欧州人権裁判所の判例≫

I v. Finland, ECtHR, No.20511/03, 17 July 2008.

病院の医療データ保護の安全管理措置を履行していなかったと認定された事例

ある女性が働く公立病院で自ら HIV に感染した記録が病院内の同僚に知られているのではないかと申し立てを行ったが、システム上過去にさかのぼって患者記録を明らかにできないため、不正なアクセスの立証ができなかった。しかし、女性側に立証責任を負わせ、病院の記録の欠陥を見落としている。アクセスログを維持するなどフィンランド国内法で定められた個人ファイル法の法的要件に従い医療ファイルの記録を保管しておらず、不法なアクセスに対して充分に管理がされていなかった（para44-46)。そのため、国家は私生活の尊重という積極的な義務を履行していなかった（para48)。

〇データ漏えい通知義務

・現代化提案には、新たにデータ漏えいが生じた場合、管理者は監督機関に事故とその対応の報告をしなければならないと定めている。また、必要に応じ、データ主体に対する通知も奨励されており、対応窓口などの情報も提供することが必要であるとされている（報告書（改訂中）65～66 項)。

・通知については、「遅滞なく」という要件が設けられているが、具体的な時間的制限は列

挙されていない[261]。

○ 透明性

・管理者は、公正な処理の確保とデータ主体の権利行使をできるようにするため、データ処理において透明性を要求される（説明書（改訂中 67 項））。

・管理者は最低限の情報をデータ主体に対し強制的に提供しなければならない。その最低限の情報には、管理者の氏名・住所、利用目的及び受取人は適切な形態で提供されるものとする。追加的情報として、個人データの保存期間、外国へのデータ移転に関する情報が提供されるものとする（報告書（改訂中）68 項）。

Harlambie v. Romania, No.21737/03, 27 October 2009

諜報機関に蓄積された情報開示を 5 年後とすることが違法とされた事例

公的機関によって保有された個人ファイルへのアクセスについては、効果的かつアクセス可能な手続でなければならない。ルーマニア諜報機関が保有するファイルの存在を告知してから 5 年後にしかアクセスができないとすることは、行政手続の時間が過度なものであり、アクセス手続が効果的でないと認定される（para92-96）。

○内部体制の構築：データ保護担当者

・管理者は、法令遵守を証明するために独立して任務を遂行するための「データ保護担当者」を配置することが想定される。データ保護担当者の設置は監督機関に通知されなければならない（説明書（改訂中）84 項）。

○リスク分析

・データ処理の前に、管理者はデータ主体の権利及び基本的自由への潜在的な影響の分析を実施しなければならない。その分析には、どの個人データがどのような目的で処理され、どのように収集され、利用され、流通され、開示されるか、また安全管理措置等の処理の全体像が考慮に入れられるべきである（説明書（改訂中）85 項）。

・リスク評価に関する枠組みのみを条約第 108 号現代化提案は示し、具体的なリスクの評価ツールは加盟国に委ねている。（ヒアリング結果・欧州評議会）

---

[261] この点、「遅滞なく」とは、複合的な要因を考慮する基準の下、少なくとも 7 日以内、という要件を設けるべきであるという見解がある。*See* Sylvia Kierkegaard, Niegel Waters, Graham Greenleaf, Elisabeth Thole, Willem Grosheide, Joseph V. Demaroco, Comments on the CoE Convention 108 Draft Proposal on Data Protection, *Computer Law & Security Review*, vol. 28 p.368, 374 (2012).

・認証制度に関する議論はこれまでのところない。（ヒアリング結果・欧州評議会）

〇デザイン段階での保護

・効果的な水準の保護を確保するために、できるだけ早い段階で、理想的にはシステムのデザイン段階においてデータ保護の要件が組み込まれなければならない。アプリやソフトウェア開発者は、デェフォルトの段階でのデータ最小限化の原則への注意を払うべきである（説明書（改訂中）86 項)。

（7）監督機関

条約第 108 号のオリジナルなテキストには監督機関に関する規定が整備されていなかった。2001 年の追加議定書第 1 条において、監督機関に関する条項が設けられた。

監督機関の要件としては、完全に独立して権限行使ができることであり、その権限には、調査・介入・訴訟手続を具備していることが要件とされている。

現代化提案では、監督機関の独立性要件をさらに強調し、いかなる者からの指示を受けたり求めたりしないことが明記されている。また、監督機関のデータ移転に関する役割、決定を下す権限及び制裁権限、そして広報啓発に関する責任が新たな権限として列挙された。

条約第 108 号	現代化による変更点
【監督機関の性格・要件】	
・条約の基本原則を履行する国内法の措置の履行を確保する責任を有する一又は複数の機関を設置しなければならない。(追加議定書第 1 条 1 項) ・監督機関は完全に独立して権限行使をしなければならない。(追加議定書第 1 条 3 項)。	・独立性の要件に、義務の履行と権限行使の際にいかなる者からも指示を受けたり求めたりしないことが定められた（第 12 条 bis4 項)。 ・監督機関の活動について報告書を公開し、透明性を高めることが記載された（第 12 条 bis5 項 bis)。
【監督機関の権限】	
・監督機関の権限には、調査、介入、訴訟手続を具備していているとともに、すべての者の個人データに関する権利及び基本的自由に関する申立を聴取しなければならな	・データ移転に関する役割、決定を下す権限及び制裁権限、そして広報啓発に関する責任が新たに監督機関の権限として追記された（第 12 条 bis2 項 b 項、c 項、e 項)。

い。（追加議定書第 1 条 2 項）	
【監督機関の協力】	
・監督機関は義務の履行に必要な限りにおいて互いに協力しなければならない（追加議定書 1 条 5 項）。	・監督機関の協力について、情報交換、調査等の調整、情報提供が明記された（第 12 条 7 項）。

○監督機関の形態

・監督機関は適切な制裁と救済を備え、自らの義務の実現のために真に独立していることが必要である。監督形態は、コミッショナー、コミッション、オンブズマン又は検査官が考えられる（説明書（改訂中）113 項）。連邦国家などの法制度の状況に対応するため複数の監督官が必要とされることがある。監督機関は、財政上・技術上・人事上（法律家・コンピューター専門家・IT 専門家）の必要なリソースを有しなければならない（説明書（改訂中）114 項）。

○監督機関の権限

・批准国は監督機関の設置に一定の裁量を有するが、少なくとも調査・介入の権限を有する機関でなければならない。監督機関はデータ保護に関して立法上・行政上の過程に関与する権限、データ移転に関する権限、個人の苦情に対応する権限、訴訟手続に関する権限を有していなければならない（説明書（改訂中）115 項）。また、監督機関の権限は、国内法に従い様々な形態があるとしても、管理者に対する強制的な差止やデータ処理の前に意見の発出の権限が含まれなければならない（説明書（改訂中）117 項）。

≪欧州人権裁判所の判例≫

K.U. v. Finland, ECtHR, No. 2872/02, 2 December 2008

インターネット投稿被害者救済のための国家の積極的義務が認められた事例

ある少年の写真や電話番号が勝手にインターネットの性的なデート・サイトに投稿されたため、動態的 IP アドレスから投稿者の特定を請求したが通信の秘密によりフィンランド裁判所で認められなかった。私生活または家庭生活の効果的な尊重には国家の積極的義務が内在しており、私人間の関係においてもこの義務を保証する措置が講じられなければな

らない（para42-43）。そして、投稿者の特定と訴追のための効果的な措置が少年の実践的かつ効果的な保護として要求されている。少年を救済するため、フィンランドの積極的義務を伴う表現の自由とプライバシーの衡量のための枠組みが立法府として当時提供されていなかったため、第８条に違反する（para49）。

Köpke v. Germany, ECtHR, No.420/07, 5 October 2010

国内機関による私生活尊重の権利と他の権利との衡量が適切と認められた事例

店内のレジでの現金盗難の調査のため事前の通知なしに職場でビデオ録画をして従業員を監視したことについて、家庭又は私的な場所以外の職場における活動にも私生活の概念は及ぶが、財産権や公共の利益の保護という利益との間の国内機関による公正な衡量が行われなかったわけではない。なお、国内機関は新たな洗礼された技術による私生活への侵入という対立利益についても今後重視しなければならない。

（８）越境データ移転

条約第 108 号は、発効当時越境データ移転については、原則として他の加盟国へのデータ移転の禁止をしてはならないという姿勢をとっていた。そして、同等の保護水準がなく、個人データの類型から特別の規制を要する場合や非加盟国への移転が行われる場合のみデータの移転の禁止が認められていた。

その後、EU データ保護指令の影響を受け、2001 年の追加議定書において「十分な保護措置の水準（an adequate level of protection)」という指令第 25 条で用いられている文言をそのまま導入した。データ移転先の国が加盟国でない場合でも、十分性の基準を満たせば「満足なデータ保護の体制（a satisfactory data protection regime)」とみなされ、データ移転が認められる。しかし、条約第 108 号では EU データ保護指令のように欧州委員会が行う十分性審査のための具体的な手続と要件は示されず、各加盟国又は組織が十分な保護措置の水準を満たしているかどうか判断することとされている（説明書 28 項)。そのため、EU とは異なり、欧州評議会が十分性審査をクリアしたホワイトリストとしての第三国や特定の組織を列挙するようなことはしなかった。そのため、EU データ保護指令における「十分性」と条約第 108 号における「十分性」は異なるものとして扱われてきた。

現代化の審議過程において、越境データ移転の規制が本格的に議論され、「適切な保護水準（an appropriate level of protection)」という文言が用いられ、その水準確保のための要件と例外が具体的に列挙されることとなった。もっとも、EU データ保護指令及び規則提案で示されている「十分性」との混同を避けるため、「現代化」提案の採択直前に「適切性」という要件に変更された。

十分性の基準については、「移転に関するあらゆる諸般の事情に照らして評価されなければならない」とされ、次の項目が審査対象となっている。

①データの類型

②移転されたデータの処理の目的と期間

③移転元の国と最終移転先

④移転に関連する国や組織に適用される一般・個別法の規則、専門的セキュリティの規則

なお、十分性審査は「ケース・バイ・ケース」に行われる（追加議定書説明報告書第 2 条 1 項）。

条約第 108 号	現代化による変更点
【データ移転の原則】	
・他の加盟国へのデータ移転は原則として禁止できないが、同等の保護水準がなく、個人データの類型から特別の規制を要する場合や非加盟国への移転が行われる場合はその限りではない。（第 12 条） ・移転先の国又は組織が十分な保護措置の水準を保障している場合には非加盟の国又は組織に移転することができる。（追加議定書第 2 条 1 項）	・データ移転の原則禁止の条件として、拘束力ある調和された地域の保護規則による規律の有無、及び適切な保護水準の確保の有無が明記された。 ・データ移転の受領者が非加盟国の国又は国際組織の管轄におかれている場合、個人データ保護の適切な水準が保障されている条件でのみデータは開示又は利用されることができる。 ・適切な保護水準は、①国並びに国際組織の法又は②特別に承認された拘束力ある文書が伴い移転に関連する者に実施しうる標準的保護措置のいずれかによって確保されうる。
【データ移転の例外措置】	
・ただし、データ主体の特別の利益になる場合や正当な支配的利益に必要な場合を国内法で定めていたり、管理者が移転に保護措置に責任を有し、監督機関から保護措置が十分であると認定された場合はこの限りではない。（追加議定書第 2 条 2 項）	・ただし、①リスクが通知された上でのデータ主体が自由かつ明確な同意を与えた場合、②データ主体の特別な利益に必要な場合、③法によって規定された、特に重要な公共の利益を含む正当な利益に必要な場合にはデータ移転が認められる。

	・監督機関は特別に承認された標準的保護措置、特別な利益、及び正当な利益に関する具体例を示すこととされている。 （第 12 条）

○適切な水準

・EU における十分な水準（adequate level）という言葉ではなく、欧州評議会では適切な水準（appropriate level）という文言を用いているが、その背景には両者の混乱を防止する目的がある。（ヒアリング結果・欧州評議会）

・EU のようなホワイトリストの列挙といった体制は検討していないが、適切な水準の保護措置を講じていることについて何らかのフォローアップの体制が必要であると考えている。まずは加盟国において適切な水準に関する評価を行うことが予定されている。（ヒアリング結果・欧州評議会）

○正当な支配的利益とデータ主体のための特別な利益

正当な支配的利益（a legitimate prevailing interest）がある場合、データの移転が認められる。ここで言う正当な支配的利益とは、欧州人権条約第 8 条 2 項、条約第 108 号 9 条 2 項、法的主張の公使又は防御、公的登録からのデータ抽出の文脈において特定された重要な利益の保護を指す。また、データ主体の特別な利益になる場合とは、データ主体との契約履行やデータ主体の重大な利益保護、又は同意を与えた場合を意味している（説明書第 31 項）。

○契約締結によるデータ移転

データ保護の十分な水準にない第三国へのデータの移転については、1992 年に欧州評議会は欧州共同体と商工会議所と連携してモデル契約によるデータ移転の調査を行ってきた。追加議定書採択以降は、監督機関により「十分な保護措置」が認定された場合、データ移転ができるが、ここで言う「十分な保護措置」には拘束力ある契約条項が含まれる（説明書第 32-33 項）。そこで、欧州評議会はいわゆるモデル契約を利用するための準備ガイドを公表し、そこで次の 14 の契約上履行すべき原則を示している[262]。

[262] CoE, Consultative Committee, *Guide to the preparation of contractual clauses governing data protection during the transfer of personal data to third parties not bound by an adequate level of data* (2002).
protection (2002)

１．一般的な規定―データ移転の合法性と契約履行の義務

２．データ主体への情報―移転前にデータ主体への通知のための適切な措置

３．移転の詳細―①移転元と移転先、②個人データの類型、③個人データの移転目的、④個人データが移転されるデータ主体の類型、⑤データの受取人、⑥移転されるデータに適用される保存制限

４．移転先の義務―公正かつ合法な処理と移転される目的制限

５．センシティブ・データ―センシティブ・データの移転に関する適切な追加措置

６．データの安全管理―適切な技術的・組織的安全管理措置

７．アクセス・訂正・削除・ブロックの権利－移転元と移転先におけるデータ主体の権利保障

８．第三者への利益供与―データ主体の権利行使を可能とする第三者への利益提供

９．責任補償―契約違反によるデータ主体が被害を被った場合の補償提供

10．適用法―契約関係を規律する法が移転元の法であることを確認、移転元の国内法でない場合は、条約第 108 号の加盟国の国内法であることを確認

11. 管轄と仲裁―移転元と移転先の運用に関するデータ主体に紛争定期の権利を付与（仲裁等）

12．データの開示―利用目的に応じた第三者へのデータ開示の制限と開示の場合の当初の契約で示された同等の水準のデータ保護を確保する条件

13．監督機関によるコントロールと協力―移転元による契約履行のチェックと移転先からの監督機関への情報提供と監督機関による意見の遵守

14．契約終了―移転元の国内法改正、監督機関による命令、倒産等による場合の契約終了

（９）相互援助

批准国は、条約の締結と共に相互援助に同意することとなる。相互援助をするための一又は複数の監督機関を事務総長に通知し、他国からの要求書を受領することとなる。

他国からの相互援助の要求に対し、監督機関の権限に適合しない場合、本条約の規定に従っていない場合、又は主権や安全保障及び公の秩序、さらに管轄内の者の権利や基本的自由を侵害する場合を除き、この要求を拒むことができない。現代化提案においては、国外に居住するデータ主体の権利行使の援助については削除された点を除き、大きな変更はない。

なお、条約第 108 号に基づく相互援助の実例は今のところ公表されていない。

条約第 108 号	現代化による変更点
【批准国相互間の協力】	
・批准国は、本条約を実施するために相互援助を行うことに同意する(第13条1項)。 ・批准国は、相互援助のため、一又は複数の機関を指定し、その名称及び所在地を事務総長宛てに通知する（第 13 条 2 項)。 ・指定された期間は、他の批准国により指定された機関の要請に応じ、情報を提供すること、及び国内法に従い適当な措置をとる（第 13 条 3 項)。 ・国外に居住するデータ主体に対し、自国の国内法により付与されている権利を行使することを援助する（第 14 条)。 ・相互援助の要求書を提出された指定機関は、次の場合を除き、その要求を拒むことができない。 a. 要求が機関の権限に適合しない場合 b. 要求が条約の規定に従っていない場合 c. 要求に応じることが、主権、安全保障及び公の秩序に適合しないか、又は管轄下にある者の権利及び基本的自由と適合しない場合 （第 16 条）	・指定された機関が、指定された監督機関と変更された。 ・第 14 条の国外に居住するデータ主体への援助が削除された。
【援助の費用及び手続】	
・批准国が相互に援助する場合、いかなる費用又は報酬の支払いも発生させるものではない。ただし、専門家及び通訳についてはこの限りではない（第 17 条)。	・特に変更なし。

(10) 条約の加入

条約の加入には、批准書、受諾書又は承認書を事務総長に寄託することとされている。

また、非加盟国であっても、閣僚委員会の過半数の決定と加盟国代表者の満場一致の議決があれば条約加入をすることができる。

現代化提案では、欧州連合と非加盟国に対しても条約批准の可能性がより明確にされた。

条約第 108 号	現代化による変更点
・本条約は欧州評議会加盟国による署名により開放される。条約は批准され、受諾され又は承認されなければならない。批准書、受諾書又は承認書は、事務総長に寄託する。（第 22 条 1 項） ・閣僚委員会は、評議会憲章 20 条 d 項に規定された過半数による決定及び同委員会に出席する資格のある加盟国代表者の満場一致の議決により、非加盟国に対し、この条約への加入を招請することができる。（第 23 条 1 項）	・評議会加盟国のほか、欧州連合、招請された評議会非加盟国が追加され、署名の対象となった。 ・議決の前に、条約委員会による意見に照らし、加盟国の満場一致の同意を得てから、非加盟国への招請をすることができるよう追加手続が入った。

○非加盟国の加入

・ウルグアイが 2013 年 10 月 4 日に批准し、モロッコも批准のための正式交渉を行っている。

（11）広報啓発：「データ保護の日」（Data Protection Day）

欧州評議会では、条約第 108 号が署名された 1 月 28 日をデータ保護の日として位置づけられた（2006 年 4 月 26 日閣僚委員会決定）。2007 年 1 月 28 日以降、毎年同日には市民への広報啓発活動向けのイベントを開催している[263]。

・第 8 回データ保護の日（2014 年 1 月 28 日）

「スノーデン後：監視に対抗するための法と技術の利用」

米国国家安全保障局による大量の個人データの監視、傍受、蓄積がプライバシーの人権を違反するものと言えるかどうか、また法の支配と民主主義にどのような帰結をもたらしたと言えるかについて専門家による討論が行われた。

263 米国議会においても 2014 年 1 月 28 日を「国民データプライバシーの日」として位置づける決議が採択された。113th U.S. Congress, S. Res. 337, Resolution expressing support for the designation of January 28, 2014 as “National Data Privacy Day”.

４．条約第 108 号と国際標準化の動向

（１）国際標準化

欧州評議会は、条約第 108 号の 30 周年を記念して、条約改正として現代化提案の作業を行ってきた。その作業の目的には、「グローバルなプライバシー基準としての条約第 108 号」[264]を掲げており、改正された条約第 108 号を一つの国際モデルとする狙いがあると考えられてきた。実際、2012 年にヨーロッパの国以外でウルグアイの批准を認め、ヨーロッパ以外の国にその条約第 108 号の価値を輸出することに成功した。これに追従するため、モロッコが条約批准に向けた正式交渉をはじめ、その他の国においても条約批准に向けた動きがある。さらに、欧州評議会の担当官からのヒアリングによれば、OECD、APEC、EU のそれぞれの国際文書と条約第 108 号は、説明書の中で記述されているとおり整合的で協調関係にあることが意識されている。このように、条約第 108 号の現代化は、様々な国際的文書の中でも唯一拘束力性格を活かし、国際標準化への道を拓く可能性を秘めている。

現在、現代化提案は「三匹のくま（Goldilocks Test）」[265]のテスト―女の子がクマの家で見つけたお粥は「熱すぎ」ても、「冷たすぎ」てもダメで、「ちょうどよい」ものでなければ飲まない―を受けていると言われる。すなわち、条約の基準があまりに高すぎてはその勢力の拡大に失敗するし、その基準が低すぎればデータ保護の原則は効果的に広まらない。したがって、国際的に見て「ちょうどよい（just right）」基準の作成に迫られている、というのである。条約第 108 号は EU を中心とする国から構成されていることから、「地域的な身分と偏見によってハンディキャップを負っている」ため、他の国際的文書よりは良いという「セカンドベスト」[266]の選択肢として捉えられてきた。他方で、欧州評議会は EU と全く同一の法律を形成してきているわけではないことにも留意が必要である[267]。結局のと

---

[264] Jörg Polakiewicz, Speech: Convention 108 as a Global Privacy Standard?, International Data Protection Conference, Budapest, 17 June 2011.

[265] Graham Greenleaf, 'Modernising' Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?, *Computer Law & Security Review*, vol. 29 No.4 p. 430, 436 (2013). なお、条約第 108 号は執行（特に適切な制裁と救済）の側面において具体的な基準を示していない点が問題視されている。*See* Graham Greenleaf, The Influence of European Data Privacy Standards outside Europe: Implications for Globalization of Convention 108, *International Data Privacy Law*, vol. 2 No.2 p. 68, 84 (2012).

[266] Lee A. Bygrave, *Data Privacy Law: An International Perspective*, Oxford University Press, 2014, p.206.

[267] *See generally* Paul De Hert & Serge Gutwirth, Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action, in *Reinventing Data Protection* (Serge Gutwirth, Yves Poullet, Paul De Hert, Cecile de Terwangne, Sjaak Nouw eds., Springer, 2009) p.3.

ころ、EU 以外の国から条約がどれだけ受け入れられるかが条約のグローバル化の鍵を握っていると考えられる。

この点、条約第 108 号と日本の法制度を比較検討すると、次の点で留意が必要であるように思われる。中には既存の個人情報保護法制度では対応できず、法律上新たに整備が必要な項目もあり、今後の検討課題となろう。

条約の各項目	日本の法制度との違い・留意点
目的	・「権利利益」の保護という記載のみで、人権や人間の尊厳といった明文条項がない。 ・私生活尊重のための国家の積極的義務の法理がない。
範囲	・官民に共通する点で条約との違いはない。ただし、適用除外規定（保有個人データや警察司法分野の適用除外）については検討が必要。
センシティブ・データ	・法律レベルでの明文規定なし。 ・条例において規定している自治体もある。
データ主体の権利	・民間部門では「求め」という表現になっている。 ・異議申立の権利がない。
義務規定	・管理者と処理者の区別がない。 ・小規模事業者への免除規定がある。 ・データ処理の合法性に関する規定がない。 ・データ保護漏えい通知義務が一部の分野でガイドラインで実施されているにとどまる。 ・追加的措置として、リスク分析やデザイン段階での保護に関する規定がない。
データ移転	・越境データ移転に特化した規定がない。
監督機関	・包括的な分野における独立した監督機関が存在しない。
相互援助	・基本方針において OECD と APEC の協力のみ明記されている。

（２）包括的範囲

欧州評議会の条約第 108 号はすべてのデータ保護分野に共通する包括的な性格を有している。これは、EU において議論されてきたデータ保護規則提案と警察司法分野に適用されるデータ保護指令提案のようにそれぞれ別分野を対象とするわけではなく、あらゆるデータ保護の問題に対応できるという点においてその射程は極めて広範である。

実際、欧州評議会は安全保障とプライバシーに関する問題についても積極的に取り組んできた。たとえば、2013 年 6 月に明らかになった PRISM 問題については、ヒアリング結果によれば、2013 年に閣僚委員会が個人データの人権を脅かす問題であるとして米国側に批判の書簡をあてた。さらに、PRISM 問題については、現代化提案の議論を促進したことは確かであり、大規模な監視への規制については議論にのぼった。また、欧州委員会がこの問題で米国と交渉をしており、この動向も注視している。欧州評議会では、PRISM 問題が発覚する前からもウェブ追跡に関する文書案を検討しており、PRISM 問題が明らかになった直後にその宣言[268]が採択された。さらに、欧州人権裁判所においては、イギリスにおける監視問題の訴訟について、特別の早期審理を開始したことが 2014 年 1 月に当事者に通知されている[269]。このような一連の警察・司法分野における個人データ保護の問題にも率先して取り組んでいる姿勢がうかがわれる。

[268] CoE, Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies, June 11, 2013.
[269] ECtHR, Letter on Big Brother Watch and Others v. the United Kingdom (AH/2265/001/LCA), 9 January 2014.

3　OECD 改正ガイドライン

板倉陽一郎（弁護士）

1. 概要

2013 年 7 月 11 日，Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data[270]（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）の 33 年ぶりの改正が OECD 理事会で承認され，Guidelines governing the protection of privacy and transborder flows of personal data（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，以下「OECD プライバシーガイドライン」又は「OECD ガイドライン」といい，特に改正後の OECD ガイドラインを「改正ガイドライン」，改正前の OECD ガイドラインを「1980 年ガイドライン」ということがある。）に新たな規定が加えられた[271]ほか，Supplementary explanatory memorandum to the revised recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data(2013)[272]（改正された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についての追加的説明覚書，以下「追加的説明覚書」という。）が解説文書として公表された。

OECD ガイドラインの改正作業は，「改正準備」も含めれば，1980 年ガイドライン 30 周年であった 2010 年から本格的に開始され，この時期は，EU データ保護指令の一般データ保護規則への改正提案の議論，欧州評議会第 108 条約の現代化提案の議論，米国における消費者プライバシー権利章典の議論の時期と重なる（本報告書においても，これらが取り上げられている）。これらの規範は互いに独立しているが，議論においては明示的・黙示的に相互参照されている。従って，OECD ガイドラインの改正を考察するにあたっても，これら他の規範の議論の影響について，考慮しなければならない。

本稿では，①改正の背景，②改正プロセス，③改正における論点を概説する。その際，必要な範囲で OECD ガイドラインの制定の経緯にも触れ，④履行状況，においては，我が

---

[270] *Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data* of 23 September 1980 [C(80)58/FINAL].

[271] *Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013)* [C(80)58/FINAL, as amended on 11 Jury 2013 by C(2013)79].

[272] *Supplementary explanatory memorandum to the revised recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data(2013).*

国以外の改正ガイドラインに対する反応をみた上で，改正ガイドラインが我が国個人情報保護法及び，その改正に関する議論に与える影響について概観する[273]。

2. 改正の背景

(1) 1980 年ガイドライン制定の経緯

OECD ガイドライン改正の背景を述べる前提として，1980 年ガイドライン制定の背景をみていく。

1980 年ガイドライン制定の経緯，特に日本からの視角については，WPISP 副議長を 12 年務められた堀部政男博士の文献に負うところが多い。堀部博士によれば，OECD がプライバシー問題を扱うに至ったのは，「欧米の利害調整を委ねられた結果」である。すなわち，欧州では，1970 年代から，プライバシー法，データ保護法の制定が相次いだ。これらの法律の中には，個人データの国外処理を制限する条項を設けているものがあった。いまでいう第三国移転条項である。第三国移転条項は，自国民のプライバシー保護には役立つが，諸国間の情報の自由な流れを妨げるという効果を持つことになり，仮に第三国移転条項がなくとも，プライバシー法やデータ保護法の存在そのものが，個人データの国外処理については規制として機能する。これに対し，情報産業で圧倒的な優位を占めていた米国は，プライバシー保護に関する法律の制定を米国の経済的利益に対する脅威と捉えた[274]。このような利害調整の場として，先進国の組織たる OECD が選ばれたわけである（**経済的対立**）。

OECD の，公的部門における越境データ移転に関する取組は，1969 年から始められ，専門家グループ（A Group of Experts）であるデータ・バンク・パネル（the Data Bank Panel）は，プライバシーの様々な側面についての分析及び研究を行い，1977 年にはウィーンでシンポジウムを行った[275]。ここでは，政府，産業界，国際的なデータ通信網の利用者，デー

---

[273] 本稿は，拙著「[招待講演] OECD プライバシーガイドライン改正と我が国個人情報保護制度への影響」電子情報通信学会技術研究報告 SITE2013-46―SITE2013-49，113 巻 274 号 19-24 頁（2013 年 10 月 29 日）を元に，私見を抑えた上で大幅に加筆・修正したものである。改正ガイドラインの解説としては，新保史生「OECD プライバシーガイドライン（2013 年改正）の解説」NBL1017 号 17-26 頁（2014 年）（以下，「新保 NBL」という。），新保史生「OECD プライバシー・ガイドライン 2013 年改正の概要」日本データ通信 195 号 20-23 頁（2014 年）（以下，「新保日本データ通信」という。）が存し，改正中の議論について触れたものとして，宮下紘「プライバシー・イヤー2012 ―ビッグ・データ時代におけるプライバシー・個人情報保護の国際動向と日本の課題―」Nextcom12 号 32-41 頁（2012 年）がある。また，改正ガイドラインの仮訳としては堀部政男・新保史生・JIPDEC（野村至）仮訳「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（2013）」（2014 年 3 月 28 日改訂版）が公表されており，新保 NBL23-26 頁にも掲載されている。本稿における改正ガイドラインの日本語表記も，原則として同仮訳に倣う。

[274] 堀部政男『プライバシーと高度情報化社会』（岩波書店，1988 年）65-76 頁。

[275] *Symposium on Transborder Data Flows and the Protections of Privacy*, Hpfburg,

タ処理サービス事業者等から意見や経験が述べられた。

OECD は，1978 年初頭に Expert Group on Transborder Data Barriers and the Protection of Privacy（国境を越えるデータの障壁とプライバシー保護に関する専門家グループ）をアド・ホックなグループとして設置した。このグループの議長はオーストラリアの裁判官であった Michael Kirby 卿が務めた。Kirby 卿の回顧録によれば，専門家グループの設置を導いたのは，データ移転への規制，プライバシーの保護に対する異なったアプローチである。欧州の OECD 加盟国にすれば，個人のプライバシーへの侵害は，「理論上の危険性」ではなかった。第二次世界大戦の間，治安官憲や軍部が個人データを「誤用」したのは，1978 年の段階では，生々しい記憶だったのである。一方，いくつかの非欧州諸国にとって，欧州の条約（欧州評議会第 108 条約）によるプライバシーの保護は，官僚的で，重圧となるやり方であり，潜在的に履行のコストが高く，越境データ移転の価値について十分に理解しておらず，データ保護の法的な壁に隠し，欧州の情報技術について，経済保護主義が背景にあるのであろうと，このような疑念の対象になった。他方，欧州諸国にとって，非欧州諸国は，現実的な，または実際的な効果を伴わないで合意しようとしている，「歯の抜けた虎」であるとみられた[276]（**理念的対立**）。

OECD プライバシーガイドラインの草案は同グループで議論され，1978 年及び 1979 年に数回の会議を開き，1979 年 9 月中旬には，ガイドラインの合意に達した案文と，説明覚書[277]（改正前の追加的説明覚書に相当するものであり，現在も効果を持つ[278]。以下，「説明覚書」という。）を作成した[279]。この間，欧州評議会（Council of Europe）や欧州共同体（European Community）とは緊密な協力が行われた[280]。

この専門家グループでの成果を元に OECD プライバシーガイドラインが 1980 年 9 月 23 日，OECD 理事会で採択された。なお，この専門家グループは，現在の WPISP（情報セキュリティ・プライバシー作業部会）の前身になったとされる。なお，ICCP（情報コンピュータ通信委員会）は 1981 年に設置されている。

このようにして成立した OECD プライバシーガイドラインは，経済的には，欧州と米国の利害調整をしつつ，理念的な対立も止揚し，データ保護の国際的水準を示すという役割を果たしたのである。

Vienna, September 1977.

276 Michael Kirby, The History, Achievement and Future of The 1980 OECD Guidelines on Privacy, *Round Table on the 30th Anniversary of the OECD Guidelines on Privacy*, Paris, 10 March 2010., p.4

277 *Original explanatory memorandum to the OECD Privacy Guidelines (1980).*

278 追加的説明覚書，"Process of the review"の項。

279 堀部政男『現代のプライバシー』（岩波書店，1980 年）103-106 頁。

280 説明覚書，1.。

⑵改正の背景

OECD プライバシーガイドラインは 1980 年の制定以降，データ保護の国際的水準を示すものとして長らく各国のデータ保護法制整備の指標となってきたが，情報通信技術やデータ分析技術の発展は猛烈なスピードで進み，1995 年の EU データ保護指令制定を始めとして，新たな情報通信技術の内容を視野に入れた立法も増加した。2014 年現在では，EU 加盟国すべてにデータ保護法が整備されているのみならず，北米，中南米，アジア（我が国を含む）にも相当の割合でデータ保護法が置かれている。近年では中東，アフリカ[281]にも制定国が現れてきている。

このような状況下で，OECD は 2008 年のインターネット経済の未来についてのソウル閣僚宣言において，「変化する技術，市場及び利用者の行動，そしてデジタル・アイデンティティの重要性の増加」の観点から，OECD プライバシーガイドラインをアセスすることとした。

3. 改正プロセス

(1) OECD プライバシーガイドライン 30 週年記念行事

OECD プライバシーガイドライン 30 周年となる 2010 年より，WPISP において改正作業が模索された。30 週年記念行事として, OECD は 3 つのイベントを開催した。それぞれ，①ガイドラインのインパクトガイドラインのインパクトに関するラウンドテーブル（30 Years After: The Impacat of the OECD Privacy Guidelines，2010 年 3 月 10 日，OECD 会議場），②「個人」の役割の増大に関するラウンドテーブル（The Evolving Role of the Individual in Privacy Protection: 30 Years after the OECD Privacy Guidelines，2010 年 10 月 25～26 日，イスラエル（エルサレム）国際会議場），③個人データ・プライバシーの経済学的側面に関するラウンドテーブル（The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines, 2010 年 12 月 1 日, OECD 会議場）として，ガイドライン改正に繋がる議論が行われた[282]。「改正作業の準備（preparations for work for the review）」とされている。また，30 周年記念レポートとして，”The Evolving Privacy

[281] 2014 年の国際データ保護・プライバシーコミッショナー会議の開催国はモーリシャスである。これは初のアフリカ開催である。
http://privacyconference2014.org/

[282] OECD (2013), "Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines", *OECD Digital Economy Papers*, No. 229, OECD Publishing.（以下，「専門家グループ報告書」という。）p.4
doi: 10.1787/5k3xz5zmj2mx-en

Landscape: 30 Years after the OECD Privacy Guidelines”と”Implementation of the OECD Recommendation on Privacy Law Enforcement Co-operation”の 2 つが公表された。

(2) 改正作業の本格化

改正作業の開始は，政府や利害関係者に質問票を配った時からとされている[283]。この利害関係者には，経済界，市民団体，インターネット技術コミュニティを含む。質問票は 2011 年 2 月に配布され，OECD 加盟国，BIAC[284]，CSISAC[285]及び ITAC[286]から，合計 19 の回答があった。また，欧州評議会第 108 条約諮問委員会[287]ビューロからも意見を受け取った[288]。

質問票への回答は，OECD のプライバシーの枠組みについて，より深い調査をすることで改正作業を継続する点に興味が示されていたが，強調点や手法は広い範囲に渡っていた[289]（この点は，OECD の公式文書であるので，婉曲的に表現されているが，欧州とそれ以外の加盟国の間での歩み寄りの困難さを述べているものと考えられる）。

(3) ToR の合意

2011 年には，”Terms on Reference for the Review of the OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data”（以下，「ToR」という。）の合意に至った。ToR は，合意の時点での改正作業の記録の意味を有し，専門家グループの議論に更なる方向性を与えることを意図している。ToR は現時点での問題や手法についての視点を共有するものであるが，改正結果についての余談を排除している[290]。

ToR は，①拡大するプライバシーの地平，②データ牽引社会のためのプライバシーについてのビジョンを練り上げること，③より効果的なプライバシーと越境データ移転へのア

---

283 Working Party on Information Security and Privacy, *Terms on Reference for the Review of the OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data*, DSTI/ICCP/REG(2011)4/FINAL

284 Business and Industry Advisory Committee to the OECD。OECD とは独立した経済団体であり，OECD の政策担当者に対して，経済界の観点から助言等を行っている。http://www.biac.org/index.htm

285 Civil Society Information Society Advisory Council。市民団体の集合体であり，ICCP（情報コンピュータ通信政策委員会）に対して助言等を行う。米国の EFF（電子フロンティア財団）や EPIC（電子プライバシー情報センター）などがメンバーに加わっている。http://csisac.org/

286 The Internet Technical Advisory Committee。インターネット関連技術団体の集合体であり，ICCP に対して助言等を行う。IEEE や ICANN などがメンバーに加わっている。http://www.internetac.org/

287 欧州評議会第 108 条約 18 条 1 項。

288 専門家グループ報告書 4 頁。

289 ToR，2 頁。

290 ToR，2 頁。

プローチを可能にする環境，④更なる考察のための論点，⑤形式面（今後の手続き）という 5 つの項目からなる。

①拡大するプライバシーの地平

ここでは，30 年前とのさまざまな状況の変化が述べられており，例として，

・収集，利用及び保管される個人データの***量***。

・個人及び団体の流行，移動，興味及び活動への示唆を得るために行われる，***分析の範囲***。

・新たな技術及び信頼できる個人データの利用がもたらす社会的経済的利益の***価値***。

・プライバシー***侵害***の増加。

・プライバシーを危険にさらす，又は保護する能力をもった***関係者の人数及び種類***。

・本人が理解し，処理されるであろうと期待する個人データを含む，***インタラクションの頻度及び複雑さ***。

・継続的かつ複数点間のデータ移転を可能とする通信ネットワーク及びプラットフォームにより維持されている，個人データの***国際的利用可能性***。

が挙げられている（強調及び斜体は原文に従っている）。いずれも，1980 年には想定し得なかった事態である。

②データ牽引社会（data-driven economy）のためのプライバシーについてのビジョンを練り上げること

国内外の経済的・社会的発展のためには個人情報の越境移転が絶対に必要である（critical）ことを考えて，「プライバシーリスクの分析」（an analysis of the privacy risks）を考慮に入れつつ，プライバシーの保護は，公開され，安全で，責任を持ち，効果的な移転を助けなければならない，とする。また，プライバシーの枠組みは表現の自由，報道の自由といった他の基本的権利についても考慮に入れなければならないとする。

極めて文意の取りづらい項目であるが，プライバシー保護が，他の利益等との調整の上でなされるべきことを述べているものと思われる。

③より効果的なプライバシーと越境データ移転へのアプローチを可能にする環境

現時点で，プライバシー保護の実効性を上げるために鍵となるいくつかの要素が特定されている，として，以下の項目を上げる。

・グローバルに相互運用可能（interoperable）なプライバシーの枠組み。

・政府内におけるプライバシー保護の重要度を，最大にまで上げる。その際，国家プライ

バシー戦略を策定することも考えられる。
・グローバルに活動するプライバシー執行機関のネットワークの発展を倍化する。
・特に個人データを大量に用いている企業について，プライバシー保護に関する注意を最高レベルにする。
・プライバシーリテラシーに関するイニシアチブを通じて，プライバシー文化を醸造する。
・特に個人データのハイリスクな利用をする事業者について，プライバシー・バイ・デザインを導入し，発展させることへのコミットメントを育むために，プライバシー影響評価，プライバシーマネジメントプロセス，プライバシー強化ツールなどの活用を図る。
・事業者に，簡単に利用できるプライバシーコントロールのデザイン及び導入を励行する。その際，実証的な研究に裏付けられ，オープンに発展した国際的な基準や実務にサポートされるべきである。
・データ本人の選択とコントロールをサポートするプライバシー制度を促進し，産業のベストプラクティスを励行する。
・技術的に無理がなく，文脈に機微なことを特徴とするプライバシー制度を通じ，創造的なビジネスモデルを認識する。

④更なる考察のための論点

WPISP がマルチステークホルダーの専門家による議論をホストするにあたり，更に考察が必要であるが，その際の共通理解として，以下の様な論点が挙げられた。

鍵となる関係者の役割と責任

・プライバシーをリスクに晒すことの可能な関係者の範囲の考察。プライバシー制度の適用範囲は拡大されるべきか？異なった関係者には異なった役割・責任が課せられるべきか？

・個人が，自らのプライバシーを保護するに際して，個人の意思決定の適切な役割は何か？個人が情報リスクをアセスしようとする場合，透明性の向上と事業者等からの通知の明確化でなし得るか？どのような場合に同意が非実用的（impractical）になるのか？「同意の撤回（withdrawal)」といった概念の役割はあるか？

・データ分析などの分野を含んだ技術革新によってもたらされる経済的・社会的便益の観点から，個人データの予期せぬ（unanticipated）利用によるリスクはどのように扱われるべきか？「個人の合理的期待」,「有益な再利用（beneficial reuse)」及び「データ保持期間」

などの概念の役割はあるか？

データ移転の地理的制限

・パーソナルデータの移転についての地理的制限のインパクトは何か？その分析は，Web ベースのサービス，クラウドコンピューティング，国際標準又は個人データ移転の保護について組織が自ら証明する，拘束力を有したアカウンタビリティの手法，これらの発達に影響を受けているか？どのようなアプローチが国際的にスケーラブルなプライバシーのルールや実務に貢献するものか？

積極的（proactive）な履行と執行

・個人データの安全な取扱いへの取組はどのようにしたら促進されるのか？個人データのセキュリティや，その他のプライバシー関係リスクのための政策的，技術的及び組織的な保護措置を履行させるための積極的なアプローチとして，どのようなインセンティブが必要か？「データ最小化」「データ管理人（stewardship）」「データポータビリティ」「情報の流れの透明化」「データ侵害通知」といった概念の役割はなにか？

⑤形式面（今後の手続き）

ToR に従い，WPISP はマルチステークホルダーによる専門家グループを組織した[291]。グループは，政府，プライバシー執行機関，学界，産業界，市民団体，そしてインターネット技術コミュニティからなるものである（Expert Group，以下「専門家グループ」という。筆者も当時から継続して加わっている）。専門家グループの議長は Jennifer Stoddart（カナダ連邦プライバシーコミッショナー，当時）であり，OECD 顧問である Omer Tene（イスラエル College of Management School of Law，当時）がラポータ（rapporteur）を務めた。

ToR は，専門家グループに，1 年以内（ToR の日付からであれば 2012 年 10 月まで）に勧告草案を WPISP に示すことを依頼した。

(4) 専門家グループ報告書

専門家グループが提示した勧告草案をベースとして，改正案が WPISP で議論され，WPISP の親会である情報コンピュータ通信政策委員会がこれを承認，2013 年 7 月 11 日に

[291] 正確には，専門家グループの枠組み自体は 2007 年越境執行勧告の元となった報告書（Report on the Cross-Border Enforcement of Privacy Laws, 2006）の際に”a volunteer group of experts”として存在しており，メンバー等についてメンテナンスを行ったものである。同様に，改正ガイドライン制定後も，専門家グループは枠組みとしては残存している。

OECD 理事会で採択されるに至ることとなる。

改正案は，プライバシーマネジメントプログラム，セキュリティ侵害通知，国家プライバシー戦略，教育及び啓発，国際的な相互運用性といった，新たな概念を導入しており，また，アカウンタビリティ，越境データ移転及びプライバシー法執行については拡大又はアップデートを行っている。他方で，いわゆる 8 原則や，「データ管理者」「個人データ」といった基本的な概念の定義については，現時点では変更すべき明確な方向性が見いだせなかったとして，これを維持している[292]。

専門家グループ報告書は，改正ガイドラインの採択後，2013 年 8 月 30 日に公表された[293]。その内容のうち ANNEX に記載されている「今後のあり得る研究のための論点」は改正ガイドラインに盛り込まれなかった論点をも含むものであるため，ここで概要を紹介する。

「同意」の役割[294]

多くの国内法において，同意の役割は強調されているが，事業者及びデータ本人の双方にとって負担となっている場合も見られる。雇用関係のように交渉力に差がある場合の同意は有効性に懸念があるし，他方で，医療研究のような場面での同意は極めて重要である。

そこで，以下の様な論点が考察に値しよう。

① 現在の枠組みにおける同意の役割は再評価されるべきか？同意の取得過程を改善し，又はデータ本人の更なるコントロールを及ぼすための方法はあるか？

② ある種の個人データの利用は，本人の選択の余地を最小化し，「社会的善（societal good）」であるとお墨付きを与えられるべきか？そのような場合，データ本人はオプトアウトの機会を与えられるべきか，それとも社会的規範は本人の選択に対する切り札（trump）となるのか？

③ 同意の適切な境界とはなにか？データ本人が，理解した上で同意したとしても，許されない，そのような種類のデータの利用方法はあるか？

「個人」の役割

伝統的には，個人データの収集者は政府，事業者及び研究機関が想定された。しかしながら，情報通信技術の発展により，個人が不特定多数と接触することは容易になり，個人が個人によってプライバシーへの脅威を与えられることもあり得るようになった。しかしながら，個人に対して，政府や事業者が課せられている制限と同様の制限を課すことは困

292 専門家グループ報告書 6 頁。
293 専門家グループ報告書 2 頁。
294 専門家グループ報告書 8 頁。

難であり，また，そのような制限は表現の自由や思想信条の自由と容易に抵触しうる。

そこで，以下の様な論点が考察に値しよう。

① 私的な個人がオンラインで個人データを利用し，頒布することについて，知らせるべき「グッドプラクティス」はあるか？個人間で個人データを「合理的に利用」するとはどういうことか？どこに境界があるのか？

② 個人間で個人データの利用をしてほしくない個人について，どのような救済が与えられるべきか？異なった種類のデータ管理者について，データ本人の権利はどのように取り扱われるか？

③ ある種の技術的手段によって，個人が選択を行えるように，より情報を与えられるようにすることは可能か？例えば，個人がある種の情報が共有される際にフィードバック（開示される聴衆の範囲を提示するなど）されるようにされるべきではないか？

目的特定及び利用制限の役割

目的特定及び目的外利用禁止の原則によれば，個人データは収集時の目的の範囲内で利用されなければならず，それを超えて利用する場合は本人の同意が必要である[295]。しかしながら，個人データのある種の二次的利用は，実質的に社会に便益をもたらすものである。例えば，医科学，エネルギーの効率的利用，漏えい防止など。目的外利用禁止の原則は，社会に有益な利用の負担になっているのみならず，多くの個人のデータが含まれる場合や，個人が特定できないデータが含まれている場合には，同意取得が現実的ではないという問題がある。他方で，個人には目的外利用を制限する正当な（legitimate）プライバシーの利益があり，あらゆる二次的利用が「社会に有益」とはいえない。

そこで，以下の様な論点が考察に値しよう。

① 目的特定及び目的外利用禁止の原則は，社会に有益な利用を過度に制限しているのか？イノベーションや価値創出との間で，バランスをとる必要はあるか？

② 個人データの再利用（re-use）には厳格な制限が課せられるべきか？それとも，「利益衡量」「公正さ」のようなよりフレキシブルな基準が適用されるべきか？特定の，受け入れられ得る再利用について，各国法で特定され，又は規制機関は「受け入れられる再利用原則」を描き出すべきか？

③ 個人のプライバシーの利益と政府又は事業者の再利用の利益の間のバランスを取るにあたり，匿名化や他のプライバシー強化技術は役立つか？

---

[295] 我が国個人情報保護法も全くこの定式に沿って立法されている。15 条及び 16 条。

個人データの定義

OECD ガイドラインは, 個人データを,「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。”“Personal data” means any information relating to an identified or identifiable individual (data subject).”」と定義する。しかしながら，匿名化や非識別化は頑健な技術ではないことが明らかになっており，これらの技術を用いるだけでプライバシーリスクを覆滅できるかどうかは，極めて疑わしい。データが個人的かどうかは，連続的（continuum）なものであり，二値（binary）ではないとの議論がなされている。

そこで，以下の様な論点が考察に値しよう。

① 非識別化によってもプライバシーリスクが残存するときに，匿名化や非識別化技術の役割は何であるか？プライバシーを保護する場合により効果的な他のアプローチは存在するか？

② 「識別されうる」と「識別され得ない」の二値的な差異は，識別度についての連続的なアプローチに代わられるべきであるか？その場合，識別度はどのように図られるか？

4. 改正における論点

(1) 二つのテーマ

改正プライバシーガイドラインには大きな二つのテーマが存在する[296]。一つはリスクマネジメントのアプローチに基づいたプライバシー保護の実践的な実施である。もう一つは，相互運用性（interoperability）を進展させることを通じて，プライバシーに対してグローバルな次元で取り組むべく，より一層の努力が必要であるということである。

このうち，リスクマネジメントの発想は，OECD 情報セキュリティガイドライン[297]に，相互運用性（interoperability）の発想は，EU-US セーフハーバー，欧州の拘束的企業準則（BCR），APEC-CBPRs（越境プライバシールールシステム）を巡る議論に[298]，それぞれ影響を受けている。前者は，プライバシーのみならずデータ保護も人権であると考える欧州とはベースラインが異なり，より現実的なアプローチを採っている。後者も，プライバシー，データ保護を巡る各国の法制，文化及び考え方等の多様性を認めた上で，収斂化（convergence）よりも現実的なアプローチを採用したと解することができる。

これらのアプローチは，1980 年から 33 年を経てもなお，OECD が「欧米の利害調整」

---

296 OECD, *The OECD Privacy Framework*, 2013, Foreword(p.4)

297 OECD, *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, 2002

298 追加的説明覚書，”International co-oparation and interoperability”の項。

の場であり続けていることを示している。欧州は，1995 年のデータ保護指令を中心として，e-プライバシー指令，欧州人権規約，リスボン条約など，プライバシー及びデータ保護の人権化，事業者から見れば規制強化の立場を強くしている。他方，米国は 2014 年に至ってもなお，データ保護に関する包括的立法は行っておらず，消費者保護の一環として，FTC（連邦取引委員会）が FTC 法 5 条の執行をしてプライバシー保護を進めており，オバマ大統領はプライバシー保護に意欲を見せるものの，事前規制的，拘束的なアプローチには慎重である。

さて，米国が「情報産業で圧倒的な優位」を占めている状況は変わらず，むしろ，強化されている。Google, Facebook, Amazon, Apple はインターネット上のサービス，トラフィックのかなりの部分を占めているほか，携帯電話の OS，音楽配信などを通じて，個人の検索語，メール，位置情報，趣味嗜好などを把握し，分析している。プライバシー，データ保護をめぐる「欧米の利害調整」はより困難な作業となっており，改正プライバシーガイドラインが特徴として挙げる点がいずれも現実的なアプローチであることも，道理がいく。

(2) 新たな概念の導入と OECD8 原則の維持

OECD が，新たに導入された主な概念として挙げているのが，①国家的なプライバシー戦略（19 条 a 項），②プライバシーマネジメントプログラム（15 条 a 項），③データセキュリティ侵害通知（15 条 c 項），④説明責任を果たす組織（15 条 b 項），そして⑤強化されたプライバシー執行（1 条 c 項及び d 項，19 条 b 項及び c 項）であり，これらは個別の項目で詳述する。⑥その他，表現の自由との関係（3 条 d 項），教育・普及啓発及びプライバシー保護技術の向上（19 条 g 項），データ管理者以外の者が果たすべき役割（19 条 h 項），国際的な相互運用・評価指標の開発（22 条）についても定められた[299]。

一方で，今回の改正にもかかわらず，専門家グループ報告書が述べたとおり，「基本原則」（OECD8 原則として著名である）は維持された。念のためこれらの原則を再掲すると，①収集制限の原則（7 条），②データ内容の原則（8 条），③目的明確化の原則（9 条），④利用制限の原則（10 条），⑤安全保護の原則（11 条），⑥公開の原則（12 条），⑦個人参加の原則（13 条），⑧責任の原則（14 条）である（条文後掲）。

この 33 年の間に，これらに並び立つような原則が全く現れてこなかったわけではない。例えば，「プライバシー・バイ・デザイン」は 1995 年ごろにカナダオンタリオ州情報・プライバシーコミッショナーである Ann Cavoukian 博士によって提唱され[300]，第 33 回国際

[299] 新保 NBL20 頁。
[300] Ann Cavoukian, *PRIVACY BY DESIGN…TAKE THE CHALLENGE*, Information and Privacy Commissioner of Ontario Canada, Ontario, 2009.

データ保護・プライバシーコミッショナー会議（イスラエル）の決議として採択され[301]，欧州一般データ保護規則提案の中でも「データ保護・バイ・デザイン」として条項に組み込まれているところである（本報告書 56 頁以下）。

しかしながら，「プライバシー・バイ・デザイン」といえども，我が国個人情報保護制度を含む，各国データ保護法制の基盤をなしている OECD8 原則に加えるものとしては，評価されなかったということである。結果的に，改正ガイドラインの中では，プライバシーマネジメントプログラムの内容の中で考慮されている[302]。

第 2 部 国内適用における基本原則 PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION 収集制限の原則 Collection Limitation Principle 7. 個人データの収集には制限を設け、いかなる個人データも、適法かつ公正な手段によって、及び必要に応じてデータ主体に通知し、又は同意を得た上で収集すべきである。 7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject. データ内容の原則 Data Quality Principle 8. 個人データは、利用目的の範囲内において利用し、かつ利用目的の達成に必要な範囲内で正確、完全及び最新の内容に保つべきである。 8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

[301] Resolution on Privacy by Design, http://www.justice.gov.il/NR/rdonlyres/F8A79347-170C-4EEF-A0AD-155554558A5F/26502/ResolutiononPrivacybyDesign.pdf

[302] 追加的説明覚書，”Privacy Management Programs”の項。

目的明確化の原則

Purpose Specification Principle

9. 個人データの収集目的は、データが収集された時点よりも前に特定し、当該利用目的の達成に必要な範囲内における事後的な利用又はその他の目的での利用は、その利用目的に矛盾しない方法で行い、利用目的を変更するにあたっては毎回その利用目的を特定すべきである。

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

利用制限の原則

Use Limitation Principle

10. 個人データは、第 9 項により特定された目的以外の目的のために開示すること、利用可能な状態に置くこと又はその他の方法で利用すべきではない。ただし、以下の場合はこの限りではない。

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) データ主体の同意がある場合、又は、

a) with the consent of the data subject; or

b) 法令に基づく場合。

b) by the authority of law.

安全保護措置の原則

Security Safeguards Principle

11. 個人データは、その滅失若しくは不正アクセス、き損、不正利用、改ざん又は漏えい等のリスクに対し、合理的な安全保護措置を講ずるべきである。

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

公開の原則

Openness Principle

12. 個人データの活用、取扱い、及びその方針については、公開された一般的な方針に基づくべきである。その方法は、個人データの存在及び性質に応じて、その主要な利用目的とともにデータ管理者の識別及び通常の所在地を認識できる方法によって示すべきである。

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

個人参加の原則

Individual Participation Principle

13. 個人は次の権利を有する。

13. Individuals should have the right:

a) データ管理者が自己に関するデータを保有しているか否かについて、データ管理者又はその他の者から確認を得ること。

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them;

b) 自己に関するデータを保有している者に対し、当該データを

b) to have communicated to them, data relating to them

i. 合理的な期間内に、

i. within a reasonable time;

ii. 必要がある場合は、過度にならない費用で、

ii. at a charge, if any, that is not excessive;

iii. 合理的な方法で、かつ、

iii. in a reasonable manner; and

iv. 本人が認識しやすい方法で、

iv. in a form that is readily intelligible to them;

自己に知らしめられること。

c) 上記（a）及び（b）の要求が拒否された場合には、その理由が説明されること及びそのような拒否に対して異議を申立てることができること。
c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
d) 自己に関するデータに対して異議を申し立てること及びその異議が認められた場合には、そのデータを消去、訂正、完全化、改めさせること。
d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.

責任の原則
Accountability Principle

14. データ管理者は、上記の諸原則を実施するための措置を遵守する責任を有する。
14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

(3) 国家的なプライバシー戦略

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。
19. In implementing these Guidelines, Member countries should:

a) 政府機関全体で調整を行った提案を反映した国内のプライバシー保護方針を発展させ、（なければならない）
a) develop national privacy strategies that reflect a co-ordinated approach across governmental bodies;

19 条 a 項は，「(加盟国は) 政府機関全体で調整を行った提案を反映した国内のプライバシー保護方針を発展させ、(なければならない)」と定める。条文だけでは必ずしも意義は明らかではないが，追加的説明覚書[303]によると，①民間事業者に対する規制という意味での，政府機関間の協調，②政府機関自身が保有する個人情報の保護に関する政府機関同士の協調，③国家サイバーセキュリティ戦略などの関連領域における政策策定との調和を図

303 追加的説明覚書，”National implementation”の項。

るための機能，などが求められている。

この点，我が国個人情報保護法は，政府に対し，「個人情報の保護に関する基本方針」（閣議決定，個人情報保護法 7 条）を定めることを義務付けている。①規制における政府機関間の協調については，現行の主務大臣制の下で相互緊密連絡協力義務が定められるなど（同法 36 条 3 項，なお 54 条）されているが，我が国が改正ガイドラインの内容を達成しようとした場合，なお以下の点に配慮すべきであると思われる。

まず，「個人情報の保護に関する基本方針」は，個人情報保護法制定後，大きく改正されたのは一度のみ（2009 年）である。プライバシー，データ保護の領域が情報通信技術や新たなビジネスモデルへの不断の対応を迫られることや，あえて法改正の手続を取らずに改正することが可能である立て付けになっている以上，19 条 a 項が，より頻度の多い改正（による新たな情報通信技術やビジネスモデルへの対応）なしに達せられるか，検討されなければならない。

内閣官房 IT 総合戦略本部や内閣官房情報セキュリティセンターの策定している情報通信技術戦略や情報セキュリティ戦略がほぼ年次で改訂されていることとの平仄も合わせられるべきである（③）。

②については，行政機関個人情報保護法に関する政府内部の文書というかたちでは現れているが，必ずしも，文書の策定に至る議論の内容等が公開されていない。公開の原則（12 条）との関係も含め，検討されなければならない。

また，今後，「個人情報の保護に関する基本方針」の性質が閣議決定であることが維持できるのかという問題がある。すなわち，後述するように，我が国においても現行の主務大臣制を超えて，プライバシー執行機関がいわゆる三条委員会として設置される方向性が存する。三条委員会（独立行政委員会）は政府からの一定の独立性をその特徴とするものであり，閣議決定により全面的に執行権限等が方向づけられるということになると，独立行政委員会としての性質と反することになる。他方で，プライバシー執行機関と主務大臣の権限が一部なりとも並立するということになれば，①政府機関間の協調の必要性は益々高まる。プライバシー執行機関が行政機関に対しても執行が可能になれば（この点も後述する），②政府機関が保有する個人情報についての政府機関同士の連携，についても重要性は増す。

我が国としては，今後，法的性質も勘案しつつ，国家プライバシー戦略のあり方を検討する必要が生じてくることとなる。

(4) プライバシーマネジメントプログラム

15. データ管理者は以下のことに責任を有する。
15. A data controller should:

a) 以下のプライバシーマネジメントプログラムを構築すること。
a) Have in place a privacy management programme that:
i. 管理下にあるすべての個人データに対するガイドラインを実施し、
i. gives effect to these Guidelines for all personal data under its control;
ii. 取扱いの体制、規模、量、センシティビティに応じて、
ii. is tailored to the structure, scale, volume and sensitivity of its operations;
iii. プライバシーリスク評価に基づく適切な保護措置を実施し、
iii. provides for appropriate safeguards based on privacy risk assessment;
iv. ガバナンス体制への組み入れと内部監査メカニズムを確立し、
iv. is integrated into its governance structure and establishes internal oversight mechanisms;
v. 問合せ及びインシデントへの対応計画を含め、
v. includes plans for responding to inquiries and incidents;
vi. 継続的なモニタリングと定期的評価を考慮した見直しを実施すること。
vi. is updated in light of ongoing monitoring and periodic assessment;

15 条 a 項は，データ管理者の義務として，プライバシーマネジメントプログラムの整備を求めており，その内容として，「i. 管理下にあるすべての個人データについて，ガイドラインが実施されるようになっている，ii. 取扱いの体制、規模、量、センシティビティに応じている，iii. プライバシーリスク評価に基づく適切な保護措置が実施されている，iv. ガバナンス体制へ組み入れられ，内部監査メカニズムが確立されている，v. 問合せ及びインシデントへの対応計画が含まれている，vi. 継続的なモニタリングと定期的評価を考慮した見直しが実施される，」ということを求めている。

「個人情報の保護に関する基本方針」6(1)③は個人情報取扱事業者に対して，「責任体制の確保」として一定程度プライバシーマネジメントプログラムに類似した責任体制を求めているが，実態として我が国で最も普及しているプライバシーマネジメントプログラムはプライバシーマーク制度である。プライバシーマークは日本工業規格「JIS Q 15001 個人情報保護マネジメントシステム―要求事項」に依拠し，2013 年 10 月時点で 1 万 3000 社以上

の付与事業者を数えている。他方，プライバシーマーク制度は国内工業規格である JIS Q に基づいているものであるから，そのままでは国際的に通用しない。

既存の（本格的な）事業者向けプライバシーマネジメントプログラムを巡っても上記のような論点が存するが，改正ガイドライン 15 条 a 項は「データ管理者」全て（官民問わず）に対する規範としてプライバシーマネジメントプログラムの整備を求めている。我が国における国内実施の方法としては，iv 号にならい，内部統制構築義務（会社法及び金融商品取引法）の関係で整備するということがあり得るが，「データ管理者」は会社であるとは限らず，不十分である。安全確保措置義務（行政機関等）又は安全管理措置義務（個人情報取扱事業者）における組織的保護措置の内容として読み込むことも考えられるが，セキュリティとプライバシーの保護を混同する嫌いもあり，現行法でカバーできない部分については国内実施のため，立法措置を含めた検討も排除されるべきではない。その際には会社法（団体法）的義務とするか，行政法的義務とするかの選択があり得る。

(5) データセキュリティ侵害通知

15. データ管理者は以下のことに責任を有する。 15. A data controller should: c) 個人データに影響を及ぼす重大なセキュリティ侵害があった場合、必要に応じてプライバシー執行機関又は他の関連機関に通知すること。当該セキュリティ侵害がデータ主体に不利益を及ぼすと思料される場合は、データ管理者は不利益を被るデータ主体に通知すべきである。 c) Provide notice, as appropriate, to privacy enforcement authorities or other relevant authorities where there has been a significant security breach affecting personal data. Where the breach is likely to adversely affect data subjects, a data controller should notify affected data subjects.

15 条 c 項は，データ管理者の義務として，「個人データに影響を及ぼす重大なセキュリティ侵害があった場合、必要に応じてプライバシー執行機関又は他の関連機関に通知すること。当該セキュリティ侵害がデータ主体に不利益を及ぼすと思料される場合は、データ管理者は不利益を被るデータ主体に通知すべきである。」と定めた。

我が国においては，特に対個人情報取扱事業者について，「個人情報の保護に関する基本

方針」6(1)②において「事業者において，個人情報の漏えい等の事案が発生した場合は，二次被害の防止，類似事案の発生回避等の観点から，可能な限り事実関係等を公表することが重要である。」とされているほか，各事業分野のガイドラインで，漏えい時の通知が定められている場合がある。例えば，経済産業省のガイドライン（「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」）では，「主務大臣等への報告」「影響を受ける可能性のある本人への連絡」のいずれをも漏えい時の「望ましい」措置として定めており（2-2-3-2.安全管理措置（法第 20 条関連））ガイドライン上の定めながら，15 条 c 項の前段及び後段に対応した運用がなされている。

もともと，侵害通知法が正当化されるのは，データ管理者には，セキュリティ侵害が発生した場合に，レピュテーションの低下のリスクがあり，侵害を公にするインセンティブが殆ど無い，ということに求められる[304]。米国ではほとんどの州で州法として定められており，欧州も一般データ保護規則提案でこれを導入しようとしている。

我が国個人情報取扱事業者は，ガイドライン上の措置であっても，比較的従順にこれを遵守する傾向にあるが，当初より個人情報，個人データを騙取するような目的で開発された悪意あるスマートフォンアプリの運用者等の悪質なものになると，ガイドライン上の措置では足りない。我が国においても，データセキュリティ侵害通知を法律上の義務とすることに関して，欧米と異なる特殊な状況にあるわけではないといえよう。

ただし，あまりにも瑣末な漏えい等で通知義務を負わせないようにとの配慮から，本項は「重大なセキュリティ侵害」であるとか「不利益を及ぼす」などの規範的概念を導入している[305]。国内法として実施する場合は，我が国事業者の性格等を勘案して，丁寧に導入される必要があるものと思われる。

(6) 説明責任を果たす組織

15. データ管理者は以下のことに責任を有する。 15. A data controller should:
b) 当該プライバシーマネジメントプログラムが適切に実施されていることを証明する準備を行い、特に、権限を有するプライバシー執行機関又は行動規範若しくは本ガイドラインに拘束力を与えるのと同等の取り決めの遵守を促進させる上で責任を有するその他の組織

304 追加的説明覚書，”Data security breach notification”の項。
305 追加的説明覚書，”Data security breach notification”の項。

からの求めに応じて対応すること。
b) Be prepared to demonstrate its privacy management programme as appropriate, in particular at the request of a competent privacy enforcement authority or another entity responsible for promoting adherence to a code of conduct or similar arrangement giving binding effect to these Guidelines; and

“Accountable Organisation”と呼称されている特徴であるが，具体的には，15 条 b 項において，データ管理者の義務として，「当該プライバシーマネジメントプログラムが適切に実施されていることを証明する準備を行い、特に、権限を有するプライバシー執行機関又は行動規範若しくは本ガイドラインに拘束力を与えるのと同等の取り決めの遵守を促進させる上で責任を有するその他の組織からの求めに応じて対応すること。」との定めがおかれた。これは，プライバシーマネジメントプログラムがプライバシー執行機関又はその代理機関によって監査されることを想定している[306]。

このような定め方は従来のデータ保護法では珍しく（同意取得義務又は表示義務が通常である），プライバシー執行機関に尋ねられたら回答するというのは，監査又は検査の発想である。プライバシー執行機関の権限によって，事業者の信用性を担保しようとするものであるので，プライバシー執行機関に適切な権限と，その遂行能力があることが前提になる（19 条 c 項とも整合的である。後述）。

(7) 強化されたプライバシー執行

1. 本ガイドラインにおいて、
1. For the purposes of these Guidelines:

c) 「プライバシーを保護する法」とは、国内の法律又は規則を意味し、当該法令の施行により、本ガイドラインと一貫性を有する個人データ保護の効果を有する。
c) “Laws protecting privacy” means national laws or regulations, the enforcement of which has the effect of protecting personal data consistent with these Guidelines.

d) 「プライバシー執行機関」とは、プライバシーを保護する法の執行に係る責任を有し、調査の実施又は執行手続きを遂行する権限を有する各加盟国が設置する公的機関を意味す

306 追加的説明覚書，”Privacy management programmes”の項。

る。
d) “Privacy enforcement authority” means any public body, as determined by each Member country, that is responsible for enforcing laws protecting privacy, and that has powers to conduct investigations or pursue enforcement proceedings.

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。
19. In implementing these Guidelines, Member countries should:

b) プライバシーを保護する法を整備し、
b) adopt laws protecting privacy;

c) プライバシー執行機関を設立して維持し、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、（る）
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;

改正ガイドラインは「プライバシー保護法」（1 条 c 項）及び「プライバシー執行機関」（1 条 d 項）の定義をおき，国内実施の内容として，プライバシー保護法の制定（19 条 b 項）と，プライバシー執行機関の設置及び，適切な（人的物的）資源並びに技術的専門性の確保等（19 条 c 項）を求めた。中でも，プライバシー執行機関は「プライバシーを保護する法の執行に係る責任を有し、調査の実施又は執行手続きを遂行する権限を有する各加盟国が設置する公的機関」とされている。

改正ガイドラインも公的部門及び民間部門を通じて適用されることに変更はない[307]。そうすると，我が国は，民間部門においては主務大臣が，公的部門においては総務大臣が，プライバシー執行機関の要件を満たしている必要がある。しかしながら，主務大臣が行える調査は報告の徴収（個人情報保護法 32 条）に限られており，立入調査権限は有していない。総務大臣が行政機関の保有する個人情報の保護に関する法律（平成 15 年法第 57 条，以下「行政機関個人情報保護法」という。）において有しているのは，行政機関の長に対す

307 ただし，民間部門について，ガイドラインの遵守に直接関係がある民間事業者や団体にとどまらず，すべてのステークホルダーが対象とされるべきとの明示がなされたという変更がある。新保 NBL18 頁。

る，「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」権限及び，「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」権限のみにほぼ限られる（行政機関個人情報保護法 49 条，50 条）。

もちろん，「調査」及び「執行手続」の意義に関しては加盟各国の法制が尊重されるものであるが，公的機関に関して総務大臣が有する権限が，我が国法の解釈においても，「調査」又は「執行手続」であると解釈され得るかどうかは更に検討が必要である。

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 年法第 27 号，以下「番号法」という。）において設置される特定個人情報保護委員会（いわゆる三条委員会である）は，個人番号を含む個人情報であるところの特定個人情報について，民間部門であるか公的部門であるかを問わずして，立入調査や勧告，命令を行う権限を有している（番号法 51 条，52 条）。番号法附則 6 条 2 項は特定個人情報保護委員会の所掌を特定個人情報のみならず通常の個人情報に広げる検討を要求しており[308]，「世界最先端 IT 国家創造宣言」（2013 年 6 月 14 日閣議決定）は「第三者機関の設置」に言及している。これを受けて IT 総合戦略本部に設置された「パーソナルデータに関する検討会」は，「パーソナルデータの利活用に関する制度見直し方針」（2013 年 12 月 20 日 IT 総合戦略本部決定）において「第三者機関（プライバシー・コミッショナー）の体制整備」の項目を掲げ，「パーソナルデータの保護と利活用をバランスよく推進する観点から、独立した第三者機関による、分野横断的な統一見解の提示、事前相談、苦情処理、立入検査、行政処分の実施等の対応を迅速かつ適切にできる体制を整備する。その際、実効的な執行かつ効率的な運用が確保されるよう、社会保障・税番号制度における「特定個人情報保護委員会」の機能・権限の拡張や現行の主務大臣制の機能を踏まえ、既存の組織、権限等との関係を整理する。」とされた。第三者機関の具体的設計についてはなお議論が続いているが[309]，これらは改正ガイドライン 1 条 d 項及び 19 条 c 項を踏まえて検討されるべきものといえる。

5. 履行状況

(1) 各国の履行状況

改正ガイドラインの成立からは 2014 年 3 月時点で半年しか経過しておらず，現時点で各国の履行状況のレポートは公表されていないが，改正ガイドライン成立時において既に

---

308 解説として宇賀克也『番号法の逐条解説』（有斐閣，2014 年）270 頁。

309 「第 6 回 パーソナルデータに関する検討会」（2014 年 3 月 27 日）では，事務局案とともに，宍戸常寿委員提出資料「第三者機関の体制整備に関する意見及び論点提起」が議論された。

OECD 加盟国全てにおいてデータ保護・プライバシー保護法制は整備されており[310]，①プライバシーの保護と情報の自由な流通に対し，政府内の最高レベルでリーダーシップを示し実行すること，②本勧告の附属文書に示され全体を構成するガイドラインを，すべての関係者（ステークホルダー）が関与するプロセスを通じて履行すること，③公的部門及び民間部門の双方に勧告を広く浸透させること，という要求事項[311]について加盟国として承認していることからは，各加盟国は，現状のデータ保護・プライバシー保護法制においてガイドラインの履行に支障があると考えているとは思われない。実際に，別章で解説されるように，毎年の法改正を進めているオーストラリアにおいては，政府において，改正ガイドラインのために法改正が必要であるとは認識されていない。もっとも，前節の各項目で，我が国におけるより望ましい履行について考察したように，履行しているかどうかというのは程度問題であって，今後，数年おきになされると思われる履行状況についての報告の中で[312]，ベスト・プラクティスが見出されてくるものとみえる。

他方で，改正ガイドラインの履行の法的性質はいかなるものであり，改正ガイドラインが直接的に裁判規範になるのか，という問題は別途存在する。すなわち，改正ガイドラインの要求事項からみて政府としてこれを履行していないとまではいえないものの，改正ガイドラインに直接的な裁判規範性が認められる場合には別途の規範として機能する場面，というのが想定しうるのかということである。

⑵　OECD ガイドラインの法的性質

OECD ガイドラインの法的性質及び直接的な裁判規範性については，数が少ないながら，これを判断した裁判例が存在する。いずれも下級審裁判例であるが，①東京高判平成 19 年 8 月 28 日判タ 1264 号 299 頁（TBC 流出事件控訴審），②東京地判平成 19 年 2 月 8 日判時 1964 号 113 頁・判タ 1262 号 270 頁（TBC 流出事件第一審），③東京地判平成 18 年 3 月 24 日判時 1938 号 37 頁・判タ 1274 号 103 頁（住基ネット東京訴訟），④東京高判平成 14 年 1 月 16 日判時 1772 号 17 頁・判タ 1083 号 295 頁（早稲田大学江沢民事件控訴審），⑤東京地判平成 13 年 4 月 11 日判時 1752 号 3 頁・判タ 1067 号 150 頁（早稲田大学江沢民事件第一審）が確認できるところである（後掲裁判例の下線は筆者）。

このうち，OECD ガイドラインの法的性質については，「そもそも OECD8 原則は，OECD

---

310 新保 NBL18 頁。

311 翻訳は新保 NBL18 頁によった。

312 改正ガイドラインの「指示事項」において，本勧告の履行状況の理事会への報告が定められている。新保 NBL18 頁。実務的には，WPISP より質問票が各加盟国に回送され，回答をまとめたレポート文書が WPISP，ICCP，理事会でそれぞれ承認されるというプロセスを経よう。

において 1980 年に採択された「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」の付属文書中に記載されたものであり，このような OECD の理事会勧告自体に，法的拘束力を認めることはできない」（③），「先進工業国を中心に組織され，経済に関する国際協力を目的とする国際機関である OECD は，1980 年 9 月，別紙「OECD ガイドライン」のとおり，個人情報の保護に関して八つの原則を掲げるなどの「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」を採択した。この勧告は，加盟各国に対する拘束力はないものの，加盟各国に対し，OECD ガイドラインに掲げている原則を国内法整備の指針として国内法の中で考慮することを求めている」（④），「この勧告は、加盟各国に拘束力のないものではあるが、加盟各国に対し、OECD ガイドラインに掲げている原則を、国内法整備の指針として国内法の中で考慮することを求めている。」（⑤）として，いずれも OECD 理事会勧告の法的拘束力は明確に否定している。ただし，③は，法的拘束力はないとした上で，住基ネットにおける個人情報保護関連各条文の，OECD8 原則（のうち，第 3 原則（目的明確化）と第 4 原則（利用制限））への当てはめを行っている。法的拘束力を否定する以上，この部分の判示は全くの蛇足であるといわざるを得ないが，OECD8 原則違反は否定されている。

他方，OECD ガイドラインの（プライバシー侵害を理由とする）不法行為請求の中での位置づけとしては，「OECD の加盟国は、OECD ガイドラインに掲げられている諸原則を国内法の中で考慮ずることを求められているのであり、そのことについて拘束力はないが、その諸原則は、普遍的なルールを志向しているという意味で参考にすべきであり、我が民法における不法行為の成否の基準となるものと解してよいであろう。すなわち、一定の行為が OECD ガイドラインに反することは、不法行為における権利侵害に当たることが多いと解すべきである。ただし、それ以上に、違法性を強める事情となると解することは理由がない。」とする⑤は，OECD ガイドライン違反を「権利侵害」の要件に位置づけているが，控訴審である④は「その諸原則は，各国の共通するルールとなることを志向しているという意味では参考となるものであり，民法における不法行為の成否を考える上での参考事情になると考えられるが，それ以上に，不法行為成立の十分条件となったり，違法性を強める事情となったりするものと解することはできない。」として，「参考事情になる」として，どの要件に位置づけられるかは明確にせず，トーンを落としている。

これらと別に，「これらのガイドライン（注：OECD ガイドラインを含む）は，直ちに不法行為における注意義務を構成するものではないが，そこで要請されている個人情報保護の必要性にかんがみると，本件情報流出事故が発生した平成 14 年ころにおいても，個人情報を取り扱う企業に対しては，その事業内容等に応じて，個人情報保護のために安全対策を講ずる法的義務が課せられていた」とする②は，注意義務の内容を構成しているかのよ

うな書きぶりであったが，控訴審である③においては，「原判決は，OECD のガイドラインや…が個人情報保護の必要性を要請していることを考慮したのであって，これをもって直接に注意義務の範囲や程度を確定したわけではなく…」として，やはり OECD ガイドラインの位置づけを曖昧にした。

このように，改正ガイドラインを含む OECD ガイドラインの不法行為請求上の位置づけは，現時点においては曖昧であり，仮に事業者が改正ガイドライン違反を引き起こしたとしても，それが不法行為請求でどのように位置づけられるかは，不明である[313]。

以上の裁判例の分析からは，改正ガイドラインの実施は，やはり国内法・国内制度化を待つ他なく，勧告のみでデータ本人に対して何らかの法的効果が得られることは期待すべきではないということになろう。立法府，行政府，事業者，事業者団体，更には今後設置される方向にある第三者機関における着実な実施が求められる。

①東京高判平成 19 年 8 月 28 日判タ 1264 号 299 頁（TBC 流出事件控訴審）

「…控訴人は，① OECD のガイドラインや民間部門における電子計算機処理に係る個人情報保護に関するガイドライン（平成 9 年 3 月 4 日通商産業省告示第 98 号）があることをもって，本件情報流出事故後の平成 17 年 4 月に施行された個人情報の保護に関する法律が要求するのと同等又はそれに近い水準の注意義務が控訴人に課せられていたというのであれば失当であるし，本件はインターネットの不正利用者が直接引き起こした事故であるから，控訴人の注意義務違反を認定するに当たってはこの点を十分に考慮すべきであり，また，控訴人がコントロールできない 2 次流出についてまでをも賠償の対象とすることはできない，…と主張する。…

…上記①について。原判決は，OECD のガイドラインや民間部門における電子計算機処理に係る個人情報保護に関するガイドライン（平成 9 年 3 月 4 日通商産業省告示第 98 号）が個人情報保護の必要性を要請していることを考慮したのであって，これをもって直接に注意義務の範囲や程度を確定したわけではなく，また，原判決は，事案の性質上，２次流出等又はそのおそれがあることによる精神的な苦痛があることを考慮したのであって，本件情報流出事故と相当因果関係のない損害についてまで範囲を広げて賠償の対象としたわけ

313 なお，不法行為請求においてどのように位置づけられるかが不明という点では，個人情報保護法違反も同様ではあるが，個人情報保護法違反の場合は，まだしも我が国の行政法規違反が民事請求にどのように影響するのか，という枠組みの中で議論できる。しかしながら，OECD ガイドライン，改正ガイドラインの場合は，法的拘束力がないことが前提となり，このような枠組みが設定されない。拙著「個人情報保護法違反を理由とする損害賠償請求に関する考察」情報ネットワーク・ローレビュー11 巻（商事法務，2012 年）1-12 頁参照。

ではない。…」

②東京地判平成 19 年 2 月 8 日判時 1964 号 113 頁・判タ 1262 号 270 頁（TBC 流出事件第一審）

「…現代社会においては，コンピュータによる情報処理技術が飛躍的に進展し，インターネットの拡大に代表されるようなオープンなコンピュータネットワークが拡大することなどによって，それらの技術を利用した事業活動の展開が容易になる一方で，それに伴う個人情報の不当な収集，利用，改ざん，開示や漏えい等の危険が高まり，個人情報の保護の強化が求められている。

そして，先進工業国諸国の国内的・対外的な経済政策を調整するための国際機関である OECD（経済協力開発機構）は，1980 年 9 月，「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」を採択し，その中で，国内適用における基本原則として，収集制限の原則，データ内容の原則，目的明確化の原則，利用制限の原則，安全保護の原則，公開の原則，個人参加の原則及び責任の原則といったいわゆる 8 原則を掲げた。このうち，安全の原則は，個人データは，その紛失又は不当なアクセス，破壊，使用，修正，開示等の危険に対し，合理的な安全保護措置により保護されなければならないというものである。この勧告は，加盟各国に対し，これらの原則を国内法整備の指針として国内法の中で考慮することを求めるものである。…

…前記認定のとおり，国際協力機関である OECD のガイドラインは，個人データについては，その紛失もしくは不当なアクセス，破壊，使用，修正，開示等の危険に対し，合理的な安全対策措置により保護されなければならないとし（安全保護の原則），我が国においても，民間部門における電子計算機処理に係る個人情報保護に関するガイドライン（平成 9 年 3 月 4 日通商産業省告示第 98 号）は，個人情報の利用の安全性の確保として，個人情報への不当なアクセス又は個人情報の紛失，破壊，改ざん，漏えい等の危険に対し，技術面及び組織面において合理的な安全対策を講ずるものとしており（17 条），個人情報を取り扱う関係業界団体や各企業等は，個人情報の保護のための具体的施策を実行することが求められていた。

これらのガイドラインは，直ちに不法行為における注意義務を構成するものではないが，そこで要請されている個人情報保護の必要性にかんがみると，本件情報流出事故が発生した平成 14 年ころにおいても，個人情報を取り扱う企業に対しては，その事業内容等に応じて，個人情報保護のために安全対策を講ずる法的義務が課せられていたものというべきで

ある。…」

③東京地判平成 18 年 3 月 24 日判時 1938 号 37 頁・判タ 1274 号 103 頁（住基ネット東京訴訟）

「…（1）　原告は，住基法 30 条の 5 に基づく市町村長から都道府県知事に対する本人確認情報の送信は，個人情報の目的外利用及び提供に当たり，このままでは，OECD8 原則のうちの目的明確化の原則（第 3 原則）及び利用制限の原則（第 4 原則）に違反するのであって，個人情報に係る本人の同意が必要である旨主張する。

（2）　しかし，そもそも OECD8 原則は，OECD において 1980 年に採択された「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」の付属文書中に記載されたものであり，このような OECD の理事会勧告自体に，法的拘束力を認めることはできないというべきである。

（3）　また，OECD8 原則のうちの目的明確化の原則（第 3 原則）との関係では，住基法は，その 1 条において，住民基本台帳及びその事務の目的を規定するとともに，その 30 条の 6 から 30 条の 8 までにおいて，本人確認情報の提供先と利用事務を明示し，かつ，これに限定しているのであるから，住基法の制度が，目的明確化の原則に違反するということはできないのである。

なお，住基法 1 条は，「この法律は，市町村（特別区を含む。以下同じ。）において，住民の居住関係の公証，選挙人名簿の登録その他の住民に関する事務の処理の基礎とするとともに住民の住所に関する届出等の簡素化を図り，あわせて住民に関する記録の適正な管理を図るため，住民に関する記録を正確かつ統一的に行う住民基本台帳の制度を定め，もつて住民の利便を増進するとともに，国及び地方公共団体の行政の合理化に資することを目的とする。」と定めている。したがって，住民基本台帳制度は，その目的として，当該住民の居住する市町村における事務処理の便宜等のみならず，「国及び地方公共団体の行政の合理化に資すること」も含むのであるから，住民基本台帳に記載された事項の全国的・広域的な行政利用をも予定していたものというべきである。

（4）ア　さらに，OECD8 原則のうちの利用制限の原則（第 4 原則）は，「個人データは，第 9 条（注：目的明確化の原則を定めている。）により明確化された目的以外の目的のために開示，利用，その他の使用に供されるべきではないが，次の場合はこの限りではない。（a）データ主体の同意がある場合，又は（b）法律の規定による場合」と定めている。そうすると，個人情報を収集目的の範囲内で利用，提供すること又は法律の規定による場合には，個人情報の利用等が許容されているというべきである。

イ　ところで，住基法は，その 30 条の 6 から 30 条の 8 までにおいて，本人確認情報の提供先と利用事務を明示し，かつ，これに限定しているのである。また，住基法 30 条の 30 及び 30 条の 34 は，本人確認情報の目的外利用を禁止しているのである。そうすると，住基法においては，本人確認情報を収集目的の範囲内で利用，提供することが，担保されているというべきである。

また，住基法 1 条の規定によると，住民基本台帳の制度における本人に係る情報の収集目的には，国及び地方公共団体の行政に用いることも含まれるというべきである。

そうすると，住基法に規定された都道府県知事や国の機関等が，居住関係の公証等の事務のために，住民基本台帳に記載された本人確認情報を用いることは，明確化された収集目的内の利用に当たるというべきである。また，市町村長が，このような目的のために，住基法 30 条の 5 に基づき，都道府県知事に対して，本人確認情報を送信することは，明確化された収集目的内の情報の提供に当たるというべきである。

ウ　さらに，そもそも，住基法に規定された国の機関等が，住基法に規定された事務のために本人確認情報を利用することや，住基法に規定された国の機関等に対して，住基法の規定に従って，本人確認情報を提供することは，いずれも，法律に基づく場合ということもできるのである。

したがって，住基法 30 条の 5 に基づく市町村長から都道府県知事への本人確認情報の提供は，法律に基づく場合であるということもできるのである。

なお，原告は，OECD8 原則のうちの利用制限の原則にいう「法律の規定による場合」の「法律」とは，すべての法律を指すものではなく，目的外利用・提供を合理的に認め得る実質的内容を伴った法律的根拠を意味する旨主張するが，そのように解すべき根拠は何もないのであって，この点についての原告の主張は，採用することができない。

エ　以上によれば，住基法 30 条の 5 に基づく市町村長から都道府県知事に対する本人確認情報の送信は，OECD8 原則のうちの目的明確化の原則（第 3 原則）及び利用制限の原則（第 4 原則）に適合するものであるということができる。

（5）　以上によると，原告の前記（1）の主張は，いずれにせよ採用することができない。…」

④東京高判平成 14 年 1 月 16 日判時 1772 号 17 頁・判タ 1083 号 295 頁（早稲田大学江沢民事件控訴審）

「…先進工業国を中心に組織され，経済に関する国際協力を目的とする国際機関である OECD は，1980 年 9 月，別紙「OECD ガイドライン」のとおり，個人情報の保護に関し

て八つの原則を掲げるなどの「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」を採択した。この勧告は，加盟各国に対する拘束力はないものの，加盟各国に対し，OECD ガイドラインに掲げている原則を国内法整備の指針として国内法の中で考慮することを求めている。これは，各国における個人情報保護を目的とした情報の流通に対する規制態様が区々に分かれ，情報の国際的な流通の障害となるおそれが生じたため，プライバシーの保護と情報の自由な流通という競合する価値を調和させるためのガイドラインを作成し，これに基づく各国の国内法の整備により，プライバシー保護を名目として情報の国際流通が妨げられることがないようにすることを目的としたものであった。…

…OECD ガイドラインは，前記（…）のとおり，個人情報を収集した者は，データ主体の同意がある場合又は法律の規定による場合以外，その収集の際に明確化された目的以外の目的のために個人情報を開示してはならない旨（利用制限の原則）を定めているが，本件名簿の提出は，本件講演会の参加申込者の同意がないまま個人情報を開示したものであって，これを開示することの法令上の根拠も存在しない以上，OECD ガイドラインの上記規定の趣旨に反するものということができる。しかし，OECD ガイドラインは，OECD の加盟国において，これに掲げられた諸原則を国内法の中で考慮することを求めているだけであって，法的な拘束力を有するものではない。ただ，その諸原則は，各国の共通するルールとなることを志向しているという意味では参考となるものであり，民法における不法行為の成否を考える上での参考事情になると考えられるが，それ以上に，不法行為成立の十分条件となったり，違法性を強める事情となったりするものと解することはできない。したがって，OECD ガイドラインの趣旨に反する行為が当然に不法行為を構成し，あるいは，これに違反することが不法行為の違法性を強めるとの控訴人らの主張は，採用することができない。…」

⑤東京地判平成 13 年 4 月 11 日判時 1752 号 3 頁・判タ 1067 号 150 頁（早稲田大学江沢民事件第一審）

「…先進工業国を中心とする経済に関する国際協力機関である OECD は、各国における個人情報保護を目的とした情報の流通に対する規制態様が区々に分かれ、情報の国際的な流通の障害となるおそれが生じたため、「プライバシーと個人の自由を保護し、かつプライバシーと情報の自由な流通という、基本的ではあるが競合する価値を調和させることに共通の利害を有すること」を前提として、「個人データの自動処理及び国際流通は、国家間の嘶しい形態を作り上げるとともに、相互に矛盾しない規則と運用の開発を要請すること、個

人データの国際流通は経済及び社会の発展に貢献すること」を確認し、「プライバシー保護と個人データの国際流通にかかる国内法は、そのような国際流通を妨げるおそれがあることを認識し、加盟各国間の情報の自由な流通を促進すること及び加盟各国間の経済的社会的関係の発展に対する不当な障害の創設を回避すること」を目的として、加盟各国に対して、個人情報保護に関する国内法整備の指針を示し、プライバシー保護を名目として情報の国際流通を妨げてはならないと勧告し、一九八〇年九月、「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」を採択した。

イ　この勧告は、加盟各国に拘束力のないものではあるが、加盟各国に対し、ＯＥＣＤガイドラインに掲げている原則を、国内法整備の指針として国内法の中で考慮することを求めている。

OECD ガイドラインは、個人情報の保護に関し、以下の八つの原則を掲げている。

（ア）個人データの収集には、制限を設けるべきであり、いかなる個人データも、適法かつ公正な手段によって、かつ適当な場合には、データ主体に知らしめ又は同意を得た上で、収集されるべきである（収集制限の原則）。

（イ）個人データは、その利用目的に沿ったものであるべきであり、かつ利用目的に必要な範囲内で正確、完全であり最新なものに保たれなければならない（データ内容の原則）。

（ウ）個人データの収集目的は、収集時よりも遅くない時点において明確化されなければならず、その後のデータの利用は、当該収集目的の達成又は当該収集目的に矛盾しないで、かつ、目的の変更毎に明確化された他の目的の達成に限定されるべきである（目的明確化の原則）。

（エ）個人データは、前条により明確化された目的以外の目的のために開示利用その他の使用に供されるべきではないが、１データ主体の同意がある場合、２法律の規定による場合はこの限りではない（利用制限の原則）。

（オ）　個人データは、その紛失若しくは不当なアクセス・破壊・使用・修正・開示等の危険に対し、合理的な安全保護措置により保護されなければならない（安全保護の原則）。

（カ）　個人データに係る開発、運用及び政策については、一般的に公開の政策がとられなければならない。個人データの存在、性質及びその主要な利用目的とともにデータ管理者の識別、通常の住所をはっきりさせるための手段が容易に利用できなければならない（公開の原則）。

（キ）　個人は、次の権利を有する（個人参加の原則）。

（１）データ管理者が自己に関するデータを有しているか否かについて、データ管理

者又はその他の者から確認を得ること。

（2）自己に関するデータを、a 合理的な期間内に、b もし必要なら過度にならない費用で、c 合理的な方法で、かつ、d 自己にわかり易い形で、自己に知らしめられること。

（3）上記（1）、（2）の要求が拒否された場合には、その理由が与えられること及びそのような拒否に対して異議申し立てができること。

（4）自己に関するデータに対して異議を申し立てることができること、及びその異議が認められた場合には、そのデータを消去、修正、完全化、補正させること。

（ク）データ管理者は、上記の諸原則を実施するための措置に従う責任を有する（責任の原則）。…

…OECD ガイドラインは、前述のとおり、個人情報の保護に関して、目的明確化の原則及び利用制限の原則を掲げ、「個人情報を収集した者は、データ主体の同意がある場合又は法律の規定による場合以外、その収集の際に明確化された目的以外の目的のために個人情報を開示してはならない」旨定めているところ、本件名簿の提出は、本件講演会の参加申込者に対して明示的に予告することなく、参加申込者の同意もなく、法律の明文の規定に基づかずに個人情報を開示したものであって、その限りで、OECD ガイドラインに反することになる。もっとも、前述のとおり、OECD の加盟国は、OECD ガイドラインに掲げられている諸原則を国内法の中で考慮ずることを求められているのであり、そのことについて拘束力はないが、その諸原則は、普遍的なルールを志向しているという意味で参考にすべきであり、我が民法における不法行為の成否の基準となるものと解してよいであろう。すなわち、一定の行為が OECD ガイドラインに反することは、不法行為における権利侵害に当たることが多いと解すべきである。ただし、それ以上に、違法性を強める事情となると解することは理由がないというべきである。…」

II　国際的流れにおける各国の動き

1　米国のプライバシー保護法制の最新動向

–消費者プライバシー権利章典と US-EU セーフハーバー協定をめぐる動き-

河井理穂子　（埼玉工業大学）

（1） 消費者プライバシー権利章典とその後

① 成立の経緯と概要

2012 年 2 月 23 日、オバマ大統領は、「ネットワークの世界における消費者プライバシー：プライバシーの保護とグローバルデジタル経済の革新を促進するフレームワーク」（Consumer Data Privacy in a Networked World: A framework for protecting privacy and promoting innovation in the global digital economy）という消費者プライバシーに関する大綱を発表した。この大綱では、情報社会における消費者プライバシー保護のあり方の青写真として「消費者プライバシー権利章典」（Consumer Privacy Bill of Rights）が提示されている[314]。

大綱の前文では、次のようなことが述べられている。豊富な情報、安価に大量の情報処理をする技術の向上、分析技術の目覚ましい発展は、ネットワーク社会にイノベーションを起こしており、ネットワークテクノロジーとそこから生まれるビジネスが米国と世界にもたらす利益は非常に大きい。そしてこのようなネットワークの世界では消費者からの信頼（trust）が必要であり、その信頼を守っていくためには、プラバシーの保護が非常に重要である。また、大綱の序論で、ほとんどのプライバシーに関する現行連邦法は、特定の分野（例えば、医療、教育、通信、金融サービス、インターネット上の子どもの個人情報など）に限られており、一般的なインターネット上における個人データ（personal data）は、包括的な連邦法の適用を受けていないことを指摘している。なお、ここでの個人データとは、特定の個人にリンクする（linkable to a specific individual[315]）

---

314 米国商務省の Internet Policy Task Force（IPTF）が 2010 年 12 月に提言をした「インターネット経済における商用データ、プライバシー及び技術革新：動的政策枠組み（消費者オンラインプライバシー保護に関するグリーンペーパー）」（Commercial Data Privacy and Innovation In the Internet Economy: A Dynamic Policy Framework (“Privacy and Innovation Green Paper”)）において、権利章典の策定が提言され、実質的にはこのグリーンペーペーをもとに、消費者プライバシー権利章典は策定されている。

315 この定義は、連邦政府の”personally identifiable information”に近い。これは、その個人本人を区別又は追跡することができる情報（その情報単体、又は特定の個人にリンクをした又はリンク可能な個人・本人に関する情報と組み合わせることによって）と定義され

データの集合すべてを指す。

米国のプライバシー保護法制は、基本的なプライバシー保護の原則を守り、柔軟かつ順応性のあるコモンローや消費者保護のための具体的な法律、Federal Trade Commission（FTC）による法執行、さまざまな利害関係者の意図を反映した政策形成を可能にしているプライバシー保護のフレームワークを基盤としており、すでにしっかりとプライバシーを保護していると大綱では前置きをしている。しかし、このフレームワークには、①（民間の）商業的な世界における基本的なプライバシー原則の明確な提示、②テクノロジーとビジネスモデルの発展に伴う消費者プライバシーに関する問題点についてのすべての利害関係者による持続的な取り組みの義務、という２点が欠けていると指摘をしている。この 2 点を補うために、本大綱が提案されているとしている。そしてこの大綱が提案するフレームワークは、消費者プライバシーの保護をしながら、イノベーションを促進させるものであるとしている。

提案されたレームワークの中心は、「消費者プライバシー権利章典」であり、それは、動的なインターネットの商業利用という環境に適応する基盤となるプライバシー保護原則と位置付けられている。大綱の中で政府は、議会に「消費者プライバシー権利章典」を実現するために、特に現在の特定分野に関するプライバシーに関する連邦法（例えば、医療や信用の分野）の適用を受けていない商業的な民間セクターに適用される法律の成立を促している。そして、政府は利害関係者（事業者[316]、プライバシーや消費者保護の団体、国際的なパートナー、州の訴訟務官、連邦刑事民事の執行機関そして学術界）間の話し合いをサポートして、「消費者プライバシー権利章典」の実行に必要なマルチステークホルダーのよる行動規範（Codes of conduct）の策定と採用を実現させるとしている。さらに、FTC の権限を拡大することによる効果的な法執行、そして他国のプライバシーフレームワークとの相互運用をより高める義務についても述べている。

以下が大綱の目次である。

ている。個人が本人であると明らかになるケースについてケースバイケースのリスクに対する評価が必要となるとしている。(Peter R. Orszag, Memorandum for the Heads of Executive Departments and Agencies, Guidance for Agency Use of Third-Party Websites and Applications, at 8 (Appendix), June 25, 2010)

[316] “company”と大綱では表現するが、この”company”とは、団体、法人、トラスト、合同事業、個人事業、法人格のない組合、営利ベンチャー、非営利法人など、連邦法のプライバシー関係法の適用を受けていないものも含まれる。本報告書では、「事業者」と訳している。

要旨

１章：序論　米国消費者プライバシー保護フレームワークの強化

２章：消費者プライバシー権利章典

３章：消費者プライバシー権利章典の実現に向けて：実効性のある行動規範の策定のためのマルチステークホルダープロセス

４章：FTC の法執行の強化

５章：プライバシー保護の国際的相互運用の促進

６章：消費者プライバシー権利章典の立法化

７章：個人プライバシー保護の改善における連邦政府のリーダーシップ

８章：結論

９章：付録 A　消費者プライバシー権利章典

10 章：付録 B　消費者プライバシー権利章典と The Fair Information Practice Principles (FIPPs)の比較

(A)　消費者プライバシー権利章典

巨大な企業や政府だけが個人情報を収集する時代は終わり、様々な事業者が大量のデータをあらゆる目的で収集し、消費者はオンラインソーシャルネットワークサービスや個人のブログなどで積極的に個人データをやり取りしている。現代では Fair Information Practice Principles（FIPPs）[317]が従来想定していた環境より、個人の情報に関する処理がより分散され、広く普及している。そして、この個人データの利活用はイノベーションを起こし、あらゆるビジネスに利益をもたらすといえる。このような環境のなかでイノベーションを維持しながら消費者プライバシーの保護を行っていくことが非常に重要となっている。そこで、消費者プライバシー権利章典は、FIPPs を 2 つの点で発展させている。

一つは、消費者が個人データを扱う事業者に何を望むべきであるのか、その権利について明らかにしている点である。また同時にネットワーク社会において消費者にも自己のプライバシーを守る責任があることを明記している。もう一つは FIPPs の個人データの収集・利用の際に背景情報（context）を重要視する部分を踏襲し、発展させている点である。消費者が、当該製品や当該サービスを利用するにあたって、通常期待する個人データの利用目的の範囲というのが背景情報であり、その範囲での利用に関しては、逐一消費者の同

317 公正な情報活動に関するデジタル時代のプライバシー保護原則。1970 年代に FTC によって提唱され、現代社会で国際的にもプライバシー保護の基盤の一つとなっている。

意を求める必要がないとするもので、事業者にとっては柔軟性があるものとなる。

消費者プライバシー権利章典では、消費者は個人データに関して以下の 7 つの権利を持つとされる。なお、消費者プライバシー権利章典は、商業的な個人データの利用に関するものであり公的機関による利用は含まない。

○個人のコントロール（Individual Control）

消費者は、自己のどのような個人データが収集され、どのような使われ方をされるのか知り、コントロールする権利を持っている。事業者は、消費者に対してその人の個人データをどのように他者と共有するのか、消費者が適切なコントロールができるようにしなければならない。また、事業者がどのように個人データを収集、利用、開示を行っているのかに関しても、同様に適切なコントロールを消費者が行えるようにしなければならないとする。このような消費者によるコントロールは、その個人データの規模、範囲、センシティブデータ[318]であるかなどを考慮することにより、消費者が容易に適切なコントロールを行うことができる方法によって提供されなければならない。そして、その方法は、個々のサービスやケースに即し、明確で簡潔な選択を行うことで達成され、事業者による個人データの収集、利用、開示について、自身にとって意味のある結論を消費者が出せるようなしくみでなければならない。さらに、個人データが収集されたときと同様に容易に行うことが出来る方法で、個人データ提供の同意の撤回や制限を行うことができるようにしなければならないとする。

特に第三者が個人データを直接収集するようなサービス（例えば、オンラインターゲッティング広告）を提供する事業者は、第三者事業者がどのように個人データを利用し、彼らが消費者に個人データの収集、利用、開示について適切な選択肢を提供しているかどうかについても十分に消費者の執事のように把握をして、消費者に適切な選択肢を提供する必要があるとする。もちろん、第三者事業者も、個人データの収集、利用、開示について消費者が明確で簡潔な選択を行うことできるしくみを持たなければならない[319]。

また、第三者事業者で、消費者との直接のやりとりを全く行うことができない事業者も

318 ここでは、就労、信用、保険などの情報を指す。

319 例えば、オンラインターゲッティング広告は、個人または個人のデバイスをトラッキングするが、このような場合事業者は、消費者に対して適切なコントロールのオプションを提供しなければならない。しかし大綱では一方で、テクノロジーの発展が消費者の個人データに対する個人のコントロールを可能にするともしている。例えば、”Do Not Track”のしくみでは、消費者は、第三者の事業者が自己の個人データをどう扱うか、または彼らがその個人データを受け取ることができるか否かについてもコントロールすることができ、いわゆるオプトアウト形式でオンラインターゲッティング広告の事業者に個人データを収集、利用させること拒否できるとしている。

いる。例えば、データブローカーなどが挙げられる。このような事業者は、個人にコントロールする方法を提供することは現実的でないので、消費者プライバシー権利章典が掲げる 7 つの項目のうち、個人データの商業利用において事業者がどのような役割を担っているか、明確な説明を公表することにより透明性（transparency）を高め、さらに、アクセスと正確性（Access and Accuracy）、説明責任（Accountability）の他の項目において消費者と直接やり取りできない部分を補う必要があるとしている。

また、消費者が自身の個人データのコントロールにおいて責任を負うことも述べられている。そのために事業者は、一度消費者が同意した個人データの収集等を撤回するしくみを、収集等の同意と同じしくみで持たなくてはならないとしている。

○透明性（Transparency）

事業者は、どのような個人データを収集し、なぜそのデータが必要なのか、いつそのデータを削除し、または非識別化（de-identified）するのか、そして第三者との個人データ共有があるのか、共有する場合はその目的などを常に明らかにしなければならない。このように透明性を高めることで消費者は、個人データの収集等におけるリスクのコントロールができる。また、青少年または子どもに関する個人データの収集においては、より一層の透明性が要求される。

○背景情報の尊重（Respect for Context）

消費者は、個人データを提供する際の背景情報（context）と矛盾しない、事業者による個人データの収集、利用、開示を望む権利を持つ。事業者は、背景情報と異なる目的で利用または開示をする場合は、提供時に消費者に対して目立つようにその他の目的を示し、消費者が容易に背景情報外目的利用について対応ができるようにしなければならない。また個人データ提供後に、背景情報と矛盾した目的で利用または開示を行う場合も同様に、その透明性を確保し、データ主体である消費者が対応をできるような選択肢を用意しなければならない。

この背景情報を重視した個人データ収集等については、事業者に柔軟性を与えるが、同時に事業者は、提供されるサービスや商品に基づいて、自己の個人データがどのように使われるのかを消費者がどのように認識して判断をするのか、また事業者の個人データ取り扱いにおける役割に関する説明をどのように理解するのか、いわゆる個人データ提供時の背景情報に基づいた消費者の理解をもとに検討する必要がある。

オンライン広告の事業者は、様々なビジネスモデルがありそれぞれ異なるプライバシーリスクを抱えている。それぞれについて事業者は、消費者との関係を重要視する必要があ

る。また、いわゆるセンシティブデータの収集や利用はオンライン広告の事業者は収集することを避けるべきであるとしている。

また、ソーシャルネットワーキングサービスおいて、消費者は積極的に個人データを掲載していく。事業者は、それらの個人データを例えばサービスの向上、新しいサービスの開発等に使用することができ、その度に消費者に同意を得る必要はない。しかし、例えばデータブローカーなどの第三者に個人データを移転する場合、その都度でなくてよいが明確に明示的に、第三者に個人データを開示してその他の目的で利用する可能性があることは掲示しなければならない。そして、その他の消費者プライバシー権利章典の項目と補完し合うことで、消費者にこれらの開示をさせない方法を提供することも重要である。

プライバシー研究者や技術者の間では、消費者プライバシーの保護は、従来の告知と同意のフレームワークから、利用と保存を重視することにシフトしていると指摘も多くなっている[320]。そして収集の際の背景情報を重視することの必要性が議論されはじめている。このことは、事業者による責任ある利用が重要視され、個人ではなく事業者に個人データ利用に関するより重い責任を課すこととなる。オバマ政権は、個人データの収集、利用等においてこの背景情報の尊重ということを基本としたい方針である。

○セキュリティ（Security）

事業者は、紛失、不正アクセス、破壊、変形、不正な開示などをさけるために、適切な予防措置をとり、さらに個人データの収集等に関わる業務に関し、評価を行わなければならない。セキュリティが守られていないと、消費者に困惑や経済的損失や物理的な害を及ぼすこととなる。これにより事業者は、消費者からの信頼だけではなく、ビジネスパートナーなどからの評判も落ちて、そのことによる経済的損失を負うこともあると考えられる。また、情報漏洩（Data Breach）の際には、消費者および法執行機関に直ちに報告をし、セキュリティ保護のための措置をとらなくてはならない。大綱では、情報漏洩に関する連邦法の必要性を特に指摘している。

○アクセスと正確性（Access and Accuracy）

事業者は、正確な個人データを保持する必要があり、消費者がそれらの個人データにアクセスをし、訂正、削除または利用の制限を行うことができる機会を与えなければならない。

現在、特定の分野（医療（The Health Insurance Portability and Accountability

320 Craig Mundie, "Privacy Pragmatism: Focus on Data Use, Not Data Collection," *Foreign Affairs*, March/April, 2014 http://www.foreignaffairs.com/articles/140741/craig-mundie/privacy-pragmatism

Act(HIPPA))、信用（the Fair Credit reporting Act）など）を除いて、消費者は自己の個人データにアクセスをして訂正をする法的な権利を持っていない。このような訂正、削除、利用の制限を行うために、消費者が容易に事業者の保持する個人データにアクセスを行うことができるようにすることは、イノベーションを助けるとしている[321]。

○焦点を絞った収集（Focused Collection）

事業者は、背景情報に沿った目的を達成するための最低限の個人データの収集におさえなければならない。また、必要のなくなったデータについては、消去または非識別化しなければならない。

○説明責任（Accountability）

事業者は、この７つの原則を守る責任を負っている。また、事業者はその従業員にこの原則を守るよう教育し、常に評価をしなければならない。また、これらの責任について監査報告書を出さなければならない。第三者にデータを移転する場合は、移転自体が重要なのではなく、その利用が消費者がデータを提供した背景情報と矛盾していないかどうかが重要となる。よって、第三者が契約上、７つの原則を守る責任を負い、また法的に追及できることを保障しなければならない。

(B)　マルチステークホルダープロセスによる執行可能な行動規範の策定

オバマ政権は、インターネットのようなユーザー主導のオープン分散環境であるプラットフォームのためのポリシーの策定には、マルチステークホルダーによる策定が最適であると考えている[322]。このようなオープンで透明性のあるマルチステークホルダープロセスは、柔軟で迅速なインターネットポリシーを可能にすると考えている。マルチステークホルダープロセスとは、ある分野に関係する様々な利害関係者の代表者すべてが一同に集まってその分野に係る方針等を議論し策定していくことで、それぞれの利害関係者の意見が

[321] オバマ政権は、21 世紀のスマートグリッドのフレームワークを提案しているが、インターネット上で消費者が自己の電気利用に関して閲覧可能な情報を提供できるしくみを支援することを述べている。（National Science and Technology Council, A Policy Framework for the 21st Century Grid: Enabling Our Secure Energy Future, at 41, 46, June 2011, http://www.whitehouse.gov/sites/default/files/microsites/ostp/nstc-smart-grid-june2011.pdf）

[322]例えば Digital Millennium Copyright Act（DMCA）の”Notice and Takedown System”の運用に関する例など、他多数。（http://www.uspto.gov/ip/global/copyrights/AGENDA_March-20_Multistakeholder_Forum-FINAL.pdf）

反映できるというものである。

インターネット上におけるプライバシー保護も同様で、マルチステークホルダープロセスによるルール作りが重要であるとする。マルチステークホルダープロセスでは、柔軟で迅速で分散環境に対応したルール作りが可能であり、また通常の規則（法律など）や条約と比べてただちにルールを変更することも可能である。大綱では、商務省の National Telecommunication and Information Administration（NTIA）が中心となって、このようなマルチステークホルダープロセスをサポートして、事業者が行動規範を策定する場を提供するとしている。事業者がこのマルチステークホルダープロセスに参加をして行動規範を策定し、採用するメリットは、消費者や他の事業者と直接プライバシーに関する課題を共有して議論をすることができること、そして行動規範を採用していることを FTC などの法執行機関が自身のプライバシーに関連する活動を好意的に解釈してくれることなどがあげられる。

マルチステークホルダープロセスは、1.熟慮（deliberation）、2.採用（adaption）、3.進化（evolution）の過程をたどる。1.熟慮の過程では、消費者プライバシーに関わる行動規範の採用をステークホルダーが行うことが可能な市場又は産業部門を選び、ステークホルダーの参加を募る。すべてのステークホルダーは、この行動規範の熟慮の過程に参加することが出来る。そしてそこで出来上がった行動規範は、全てのステークホルダーの同意が得られており、事業者が採用することが可能となる。事業者がこの行動規範を採用すると、他の自主規制などのプライバシーポリシーと同様に FTC は不公正又は欺瞞的な行為又は慣行に対する法執行（FTC 法第 5 条）が可能となる。その後、技術や市場の変化に応じてステークホルダーは、行動規範を迅速に修正していくことが可能である。NTIA が主導をして、ステークホルダーを招集して行動規範の修正を行ってもらうこともあるだろうし、ステークホルダー自身が自主的に集まって修正を行っていくことも可能である。さらに、議会がこの行動規範の修正期間を規定して修正を促すことができる。

現在検討中の行動規範については、その現状を後述する。

(C)　FTC の執行力の強化

行動規範の執行においては、FTC が重要な役割を果たす。FTC は、プライバシーポリシー等の順守を怠ったことについて、不公正又は欺瞞的な行為又は慣行（FTC 法第 5 条）として法執行を行うことが可能である。さらに、FTC は、消費者のプライバシー保護について、適切な措置を行っていない事業者に対して主張を訴状として発行し（bring cases）、同意審決（consent agreement）や審判手続き（Administrative Trials）を行うこととなる。このようにマルチステークホルダープロセスで策定された行動規範を採用する事業者に対

しては、FTC が既存の法律に基づいて法執行機関として機能することとなる。

FTC は、行動規範の策定に際して、支援とアドヴァイスを行うべきであり、マルチステークホルダープロセスにも参加をするべきであり、これらの行動規範を採用して順守しようとする事業者に対しては、好意的に対応するべきであるとされると大綱には述べられている。

(D)　国際連携の改善

インターネットは、国と国の境界をなくし、事業者が扱うプライバシー情報は国を超えて移動をする。異なる国のプライバシーに関する法をそれぞれ順守することは非常に複雑であり、またそのデータの移転の種類も様々である。特にクラウドコンピューティングの激増は、消費者に安くさまざまなサービスを届けることが出来る一方、消費者や事業者があらゆる個人データをネット上に蓄積させたり、使用することを可能にしている。

このような中でプライバシー保護のフレームワークは、重要性を増しており、柔軟なマルチステークホルダープロセスがお互い異なるプライバシーレジーム間での運用を可能にすると考える。そこで、国際的な他のプライバシーレジームとの相互運用を高めるために、相互承認、マルチステークホルダープロセスによる行動規範の展開、国際執行協力が重要であると考えている。

○相互承認

商業的なプライバシー保護のフレームワークの相互承認とは、効果的なグローバルなデータ保護の実現をすることである。それには、効果的な法執行と事業者が説明責任を明示することができるしくみが必要である。効果的な法執行は、相互運用には極めて重要となってくる。米国は、FTC がケースバイケースで法執行をするというアプローチを取っており、これらが民間事業者のプライバシーの保護に関する標準となってきている。事業者が自己のプライバシーポリシー遵守とプライバシーに関する手続きを明示することができることが、説明責任となる。これには、自己点検、評価、監督が含まれる。

複数国家間の相互承認の例として、Asia Pacific Economic Cooperation (APEC)の Cross Border Privacy Roles (CBPR)を挙げている。これは、APEC プライバシーフレームワークに基づいており、CBPR に参加の際には、メンバーエコノミー[323]は CBPR プログラム[324]の

[323] APEC には、多種多様な国と地域が参加しているため、APEC メンバーの国・地域を指す場合にはエコノミーと呼んでいる。

[324]企業等の越境個人情報保護に係る取組に関し、APEC プライバシー原則への適合性を認証する制度。申請企業等は、自社の越境個人情報保護に関するルール、体制等に関し自己

要件を満たしてなければならない。また、この要件については、メンバーエコノミー内において法執行が行われなければならない。CBPR が成功すれば、参加事業者は、説明責任を果たし、厳しいグローバルな標準を満たした個人データの保護を行っているということを消費者に示すことができ、自由に個人データの移転を APEC の国々の間ですることができるようになる。

また、ヨーロッパのデータ保護指令（EU Directive 95/46/EC）の 27 条では、データ保護指令を国内法に反映させるために行動規範を策定することを奨励している。米国の目指す行動規範は特定の業界内の規範であり、EU のそれは保護指令という一般原則を反映させるための規範である点は異なるが、行動規範に関しても EU と共通の認識を持っているとしている。米国は、EU レベル、またさらにそのメンバーステートレベルでも相互承認の基盤として行動規範を策定していくつもりである。

グローバルなデータの移転についての相互運用の成功している一例としては、US-EU セーフハーバーフレームワークや US-Switzerland セーフハーバーフレームワークがある。これらのフレームワークは、プライバシー保護を行いつつ、事業者が個人データをグローバルに事業を分断されることなく、大西洋をまたぐ個人データの移転を可能にした（詳細は後述）。このようにセーフハーバーフレームワークは、国際的な個人データの移動において障壁をなくし、貿易と経済的な成長を支援しているといえる[325]。

○国を超えたマルチステークホルダープロセスによる行動規範の展開

迅速で柔軟性のある分散環境でマルチステークホルダープロセスによって形成された行動規範は、特にグローバルな環境でイノベーションを促進して、消費者を保護するためには、伝統的な政府による規則より明らかに優れている。国を超えてマルチステークホルダープロセスによって策定された行動規範と既存の相互承認のプログラムを組み合わせることにより、事業者のコンプライアンス遵守の負担を軽減することができると考えられる。セーフハーバーフレームワークは、FTC が管轄権のない金融サービス、情報通信キャリア、保険などには適用されない。このような分野における大西洋をまたぐ個人データの移転については検討が必要である。

オバマ政権は、商務省などと協力することにより、他の国々と協力して行動規範を策定

審査を行い、その内容についてあらかじめ認定された中立的な認証機関（アカウンタビリティ・エージェント:民間団体又は政府機関）から認証審査を受ける。（「ＡＰＥＣ越境プライバシールールシステムについて」（経済産業省商務情報政策局国際室　2013 年 5 月）http://www.caa.go.jp/planning/kojin/pdf/20130531renrakukai1.pdf）

325 このように米国の EU-US セーフハーバーフレームワークに対する評価は高く、一方で後述のように EU 側は様々な問題点があることを指摘している。

するなど新たなメカニズムを提案するつもりであり、既存のセーフハーバーフレームワークを補完するものになると考えている。

○国際執行協力

個人データの保護についてグローバルな相互運用を実現させるために、強固な法執行の協力が重要である。FTC は、Global Privacy Enforcement Network（GPEN）の形成に貢献をした[326]。GPEN は、プライバシーに関する法執行の重要性を高めるために、共同で法執行を行うことなどを可能にするものである。米国は、OECD、APEC、Asia-Pacific Privacy Authorities Forum、The International Conference of Data Protection and Privacy Commissioners などの他の国際連携機関に加盟をしており、GPEN の活動はプライバシーに関する調査と法執行において連携を行うために役立っている。

（E） 消費者プライバシー保護立法

オバマ政権は、消費者プライバシー権利章典を法律として規定していくことを議会に強く要求している。FTC と州の訴務官に、消費者プライバシー権利章典に規定されている権利を守ることのできる直接の権限を付与する法律を規定する必要があるとし、また、事業者の負う法的な義務についてもこの権利章典より詳細に細かく規定しなければならないとしている。この権利章典は、オバマ政権と議会が法律を策定するために共同で動くためのガイドであると考えている。

また FTC に行動規範をレビューする権限を与える必要もあるとする。そして、行動規範を遵守している事業者については、その範囲において既存の法律の条項の適用を受けないことを保証することが必要である。

技術とビジネスにおいて、変化が多い分野においては、政府機関のガイドライン、司法解釈、業界の慣習などを組み合わせることによって、いわゆる一般法に事業者の活動が遵守をしているかどうかの判断を容易にしている。プライバシーに関する分野においても、同様のしくみを持つことが重要である。基本となるいわゆる包括的な一般法をおき、マルチステークホルダープロセスによって策定された行動規範と法執行におけるセーフハーバー（EU-US セーフハーバーを指すのではない、後述）によって、法を遵守しているかについて確信を持つことができる。

FTC が行動規範を採用する事業者に対して、確信をもってプライバシー保護を行うことが出来るようにする必要がある。それには、２つの法によるしくみが必要である。一つは、FTC に行動規範が消費者プライバシー権利章典に反しないかどうかレビューする明示的な

326 法律により他の法執行機関との連携をする権限が与えられた。

権限を規定することである。例えば行動規範が FTC に提出されてから半年ほどで、FTC はその行動規範についてパブリックコメントを求め、マルチステークホルダープロセスに参加をした参加者のコンセンサスを反映しているかどうか審査をし、もし反映していなければ、修正を求めることができるようにする。これらを可能にするため、本大綱では Administrative Procedure Act（5 U.S.C §552 et seq.）で、FTC に上記のような権限を付与することを提言している。二つ目は、FTC に行動規範を採用している事業者にセーフハーバーを与える権限を付与することである。これは、FTC の審査を通った行動規範については、その範囲においては一般法の適用を受けないというものである。

消費者プライバシー権利章典を実現するために規定される法は、プライバシーに関する既存の連邦法が適用されない分野に対して、プライバシーに関する統一の基準を与えるものとなる。国の統一のプライバシーに関する法律は必然であり、州法より優先される旨の規定も法律に組み込む必要があるとしている。そして州の訴務官は、行動規範を執行する権限を持つとする。

また、既存の法と矛盾しないようにし、二重に法が存在をすることを避けなければならない。既存の法は、データの機微性とその特定の分野での利用にそれぞれ対応したものになっている[327]。これらの法が適用される部分については、本大綱が提案する統一法の適用を受けない。

最後に、本大綱では特定の種類の個人データについては、漏洩に関して消費者に告知をする義務を課す統一基準を規定する。Security breach notification（SBN）は、機微データの保護を効果的に促進する。消費者は、自己の情報の漏洩について告知を受けることにより、ID 窃盗（identity theft）などを予防することができ、事業者側にとっては、さらなるデータセキュリティに関する手段を講じるインセンティブとなる。現在州法では、SBN を規定しているものが多い[328]が、それぞれ異なる規定であり、このようなパッチワーク状態が事業者にとって負担となっている。大綱では、統一的な SBN に関する法の必要性を主張している

② 消費者プライバシー権利章典の現状と今後の動向

（A）現状

1. マルチステークホルダープロセスによる行動規範の策定

---

[327] 例えば、医療保険の相互運用性及び説明責任に関する法律（HIPPA）や公正信用報告法（FCRA）

[328] 47 の州と the District of Columbia（ワシントン DC）、US territories がこのような法を備える。

商務省の National Telecommunication and Information Administration（NTIA）は、マルチステークホルダープロセスによる行動規範の策定を進めるため、ステークホルダーを集めて議論する場を開催している[329]。NTIA の役割は、様々なステークホルダーに議論する場を提供して、様々なステークホルダーの同意のもとに行動規範が作成されることを助けることである。行動規範は、一つの業界団体などが規範を決めるのではなく、様々な分野の関係者が集まって議論すること、またある一定のサービスや技術などに特化するものではないなど、米国のプライバシー保護において一定の役割を果たしているいわゆる自主規制とは異なる。

現在、行動規範は、携帯アプリ、顔認証、スマートグリッド（これは、環境省（Department of Energy）が担当をしている）の３分野[330]において検討されている。

マルチステークホルダープロセスによる最初の「携帯アプリにおけるデータの収集・共有に関する通知」に関する行動規範が策定され、事業者において採用され検証されている段階である[331]。この行動規範が策定されるまでは、約１年を要し、15 回の議論の場がもたれた。この通知の目的は、消費者に個人データの収集・共有について透明性を高めることである。事業者は、もちろんこの通知の他にも既存の法を遵守しなければならず、例えば California's Online Privacy Protection Act やその他の法は、それぞれのプライバシーポリシーを別に表示することを要求している。この通知では、どのような形態のデータを収集するのか、事業者のプライバシーポリシーへのリンク、第三者とデータを共有する場合はどのような第三者なのか、携帯アプリの提供者の素性を明確にすることが必要である。どのような形態のデータなのか、どのような第三者なのかについては、それぞれカテゴリーを提供しており、事業者は、それぞれどのカテゴリーにあてはまるのか、行動規範が提供するカテゴリーを選択して表示しなければならない。また、行動規範では、この通知のデザインについても推奨デザインを記述しており、それはちょうど食品表示のラベルのようなものである。

既にいくつかの事業者がこの通知に関する行動規範を採用して、事業者側の感触としては良好であるようである[332]。しかし、この行動規範については、その議論の場の運営方法

---

329 例えば、
http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency

330 2014 年 3 月 21 日に NTIA で行われた John Verdi 氏へのインタビュー（以下、「Verdi 氏インタビュー」という）。

331 Short Form Notice Code of Conduct To Promote Transparency In Mobile App Practices http://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf

332 例えば、AVG Technologies(http://www.avg.co.jp/)

から策定された行動規範の内容に至るまで、様々な批判[333]があるのも現状である。例えば、Center for Digital Democracy は、行動規範がユーザーによるテストをされていないこと、定義があいまいな部分があること、抜け穴がある可能性がある、マルチステークホルダープロセスの運営方法が事業者よりであったなどを指摘している。

現在 NTIA では、顔認証に関する行動規範を策定中であり、議論の場がもたれている。

現在策定中または策定済の行動規範の適用は全くの自主的なものであり、何か法的な責任において免除されるなどということはない。今後、大綱に記述されたように FTC にレビューの権限を与えるなどの立法がなされれば、行動規範の普及も広がると考えられる。

2. 立法化について

現在米国議会は、113th 議会の会期中（2013-2014）であり、以下のようなプライバシーに関連する法案が審議中である。

【上院】

＜包括的な個人データの保護とデータ漏洩に関する法案＞

包括的な個人データの保護とデータ漏洩に関する法案については、現在複数の法案が提出されている。本大綱で取り組むべき重要な事項として取り上げているため、１つの法案に絞り込んで成立を目指す可能性も高くなっている。

- Personal Data Privacy and Security Act of 2014 (S.1897)　提案議員 : Leahy (D-VT) 他 4 名

  １万人以上の個人データを扱う事業者は、セキュリティ措置についてその効果と脆弱性に関して監査を行わなければならない。また、データ漏洩があった場合は、ただちに（60 日）消費者に通知をしなくてはならず、5000 人以上の個人データが漏洩した場合は、連邦の法執行機関に報告をしなければならない。またデータ漏洩に関しては民事罰、刑事罰どちらも規定している。司法委員会（Committee on Judiciary）に提出された。

- Data Security and Breach Notification Act of 2014（S. 1976）　提案議員 : Rockefeller (D- WV)他 3 名

  S.1897 と類似する点が多いが、セキュリティ措置についての監査は、どの事業者も行うことが義務づけられたり、漏洩についての消費者への告知について 30 日以内と

333 例えば、Consumer Federation of America の反対声明。
http://www.consumerfed.org/news/693

規定をしたりと、やや S.1897 より厳しいものとなっている。通商・科学・交通委員会 （Committee on Commerce, Science, and Transportation）に提出された。

- Personal Data Protection and Breach Accountability Act of 2014（S.1995）提案議員：Blumenthal (D-CT) 他 1 名

  S.1897 と S.1976 と異なる点は、個人データの漏洩に対して、民事罰、刑事罰に加えて、消費者自身が救済を直接求めることができることを規定している（a private right of action）。

- Data Security Act of 2014（S.1927）提案議員：Blunt (R-MO) and Thomas Carper (D-DE)他 3 名

  超党派の議員による法案で、上記 3 つの法案より、包括的でなく厳しくはない。甚大な被害（substantial harm）を引きこす可能性がある場合のみ、個人データ漏洩を消費者へ通知する必要があるとする。そして、セキュリティ措置に関する事項は具体的には述べられておらず、さらに上記 3 つの法案では、FTC が中心となって法執行を行うのに対して、本法案では、各業界を監督するそれぞれの政府機関が法執行を行うこととしている。また刑事罰も規定しない。

＜その他＞

- Electronic Communications Privacy Act (ECPA) Amendments Act of 2013 (S. 607) 提案議員：Leahy (D-VT) 他 4 名

  この法案は、30 年前に成立した ECPA を改正するもので、法執行機関や政府機関は、もし法が成立すれば、個人の e メールについて令状なしでアクセスすることができなくなる。プリズム問題との関係で世論が注目をしており、成立する可能性も出てきている。

- Do Not Track Kids Act of 2013（S.1700）提案議員：Markey (D-MA) 他 2 名
- Cybersecurity and American Cyber Competitiveness Act of 2013（S.21）提案議員：Rockefeller (D- WV) 他 7 名
- Do-Not-Track Online Act of 2013（S.418）提案議員：Rockefeller (D- WV) 他 1 名
- Geolocational Privacy and Surveillance Act (GPS Act) （S. 639）提案議員：Wyden (D-OR) 他 1 名
- Data Security and Breach Notification Act of 2013（S. 1193）提案議員：Toomey (R-PA) 他 7 名
- FISA Accountability and Privacy Protection Act of 2013（S.1215）提案議員：Leahy（D-VT）他 10 名

【下院】

- Cyber Privacy Fortification Act of 2013（H.R. 1121）提案議員：Conyers (D- MI/13) 他 2 名
- Geolocational Privacy and Surveillance Act (GPS Act)（H.R.1312）提案議員：Chaffetz (R-UT/3)他 16 名
- Strengthening and Enhancing Cybersecurity by Using Research, Education, Information and Technology Act of 2013 (SECURE IT)（H.R. 1468）提案議員：Blackburn (R- TN/7)
- Application Privacy, Protection, and Security Act of 2013 (APPS Act)（H.R. 1913）提案議員：Johnson (D-GA/4)　他 6 名
- Do Not Track Kids Act of 2013（H.R. 3481）提案議員：Barton (R-TX/6)　他 12 名
- Personal Data Privacy and Security Act of 2014, （H.R. 3990）　提案議員：Shea-Porter (D-NH)（S.1897 と同様の内容）

その他、Cyber Intelligence Sharing and Protection Act (CISPA)　提案議員：Michael Rogers (R-MI) 他 11 名が下院を通過し、上院の対応を待っている状況にある。これは、インターネット上のトラフィックなどを政府が民間会社と共有することができるようにし、サイバー犯罪を捜査するのを助けるためのものである。特に NSA のプリズム問題[334]後、この法案に関しては批判も多いため、上院での通過は難しいと考えられている。

包括的な個人データの保護とデータ漏洩に関する法案の 4 つは、どれも民主党の議員によって提出された法案であり、大綱の実現へ向けての一貫といっても良い。しかし、共和党議員は、包括的な個人データ保護とデータ漏洩に関する法に関しては、後ろ向き傾向があり（今まで通りの業界ごとのセクトラルなしくみで十分であり、わざわざ立法の必要はない)、なかなか法案が通らない状況が続いている。また、包括的な個人データの保護とデータ漏洩に関する 4 つの法案も大綱の消費者プライバシー権利章典のほんの一部分の実現をもたらすものであり、今後の立法も険しい道のりであると考えられる。プライバシー保護団体が、連名でオバマ大統領にプライバシーに関する立法化を強く求める旨の文書を提

[334] 2013 年 6 月、米国政府が米国市民、非米国市民のあらゆる情報を民間企業を通じて得ているということが、元米国 NSA（National Security Agency）のエドワード・スノーデン氏によって暴露された問題。

出している[335]ことからも、立法化がなかなか難しい状況にあることがわかる。

(B) 今後

商務省の NTIA が中心となり、マルチステークホルダープロセスによるさらなる行動規範の策定が進められると考えられる。また、携帯アプリに関する行動規範を採用してからその後、どのようにさらに修正、発展していくのか、マルチステークホルダープロセスが本当にプライバシー保護の分野で機能するのかなど、課題は多い。また、事業者が行動規範採用のインセンティブを持ち、さらに消費者のプライバシー保護が行われるためには、大綱の求める FTC の権限の強化、機能の追加などが不可欠であり、これらの立法が待たれるところである。

上記で述べた包括的な個人データの保護とデータ漏洩に関する法案は、どれもまだ大綱を実現できているものとは到底言いがたい。しかし、最近の小売業における大規模な個人データの漏洩が相次ぐ[336]状況の中で、個人データ漏洩に関する通知についての連邦レベルでの立法化は、世論の後押しもあるかもしれない。

一方で、今後包括的な法が生み出されるかもしれないし、そうではないかもしれないが、FTC が包括的なプライバシーに関する法をある意味創造する機関として今後も機能していくことは間違いないという意見もある[337]。George Washington 大学ロースクールの Daniel Solove 教授は、FTC は消費者に対するプライバシー侵害に対して、不公正又は欺瞞的な行為を取り締まってきたことにより、プライバシー保護規定自身を生み出し発展させており、これは伝統的なコモンローのパターンをたどっていると言う[338]。

（２） US-EU セーフハーバー協定の概要と見直しの可能性

① 概要

米国は、民間部門におけるプライバシー保護法制は自主規制が基本で、特に機密性が高い情報を扱う分野でのみ個別法を制定するセクトラル方式を取っている。そのため、オム

---

335 The Electronic Privacy Information Center, the ACLU, the American Library Association, the Center for Digital Democracy and Public Knowledge などが消費者プライバシー権利章典の２周年（2014.2.24）に際して、オバマ大統領宛に、迅速な権利章典の立法化を要求した。http://epic.org/privacy/Obama-CPBR.pdf

336 例えば、2013 年 11 月 27 日から 12 月 15 日までの間、全米の Target の店舗で使用された、クレジットカード、デビッドカードの個人情報が 4000 万件あまり流出した事件。

337 2014 年 3 月 20 日に George Washington University Law School で行われた Danile Solove 教授へのインタビュー。

338 Daniel J. Solove and Woodrow Hartzog, “The FTC and the New Common Law of Privacy”, Columbia Law Review, 2014 [Vol.114:583]

ニバス方式による EU のプライバシー保護のフレームワークとは異なる形態を採用している。1995 年に採択された EU データ保護指令[339]では、十分なレベルの保護措置を確保していない第三国への EU 加盟国の個人データの移転は認められていない[340]。米国が十分なレベルの保護措置が確保されていないとみなされると、EU と取引を行う米国企業に甚大な経済的損失がもたらされると考え、米国商務省は EU に対してセーフハーバー協定を提案した。形式的には、EU データ保護指令第 25 条第 6 項に基づく欧州委員会の十分性の認定作業である[341]。十分性の評価は、実質的には EU データ保護指令第 29 条に基づいて設置された「個人データの処理に係る個人の保護に関する作業部会[342]」（以下作業部会）が行う。セーフハーバー協定について第 29 条作業部会において米国側とのやり取りを含め様々な検討がなされ、米国商務省との合意案に至った。正式なセーフハーバー協定は、米国では 2000 年 7 月 24 日と 9 月 19 日の連邦公示録で公示され、欧州委員会では、2000 年 7 月 28 日に公表された。欧州議会は、2000 年 6 月 22 日、欧州委員会の決定案に関する決議という形で、①セーフハーバーが FTC と商務省の所管の企業にのみ関係すること、②公に利用可能なデータは例外とされていること、③セーフハーバー違反に対して損害賠償が得られることが確実には結論づけられていないことなどを指摘している[343]。EU 側は不満を残しながらも、セーフハーバー協定を受け入れた。これは、米国との通商関係や情報流通の現状を無視することが出来なかったからであるといわれ、米国の強大な通商力と外交力によるものであるということができる[344]。

セーフハーバー原則（the Principles）は、7 つのセーフハーバープライバシー原則を示し

---

339 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

340 EU データ保護指令第 25 条第 1 項　「構成国は、処理されている又は移転後に処理が予定されている個人データの第三国への移転は、この指令に従って採択された国内規定の遵守を損なうことなく、当該第三国が十分なレベルの保護措置を確保している場合に限って、行うことができることを定めなければならない」（訳は、堀部政男研究室仮訳）

341 EU データ保護指令第 25 条第 6 項　「委員会は、第 31 条第 2 項に定める手続きに基づいて、第三国が私生活、個人の基本的な自由及び権利を保護するための当該第三国の国内法、又は特に本条第 5 項に規定された交渉の結果に基づいて締結した国際公約を理由として、第 2 項の規定の意味における十分なレベルの保護を保障していると認定することができる」（訳は、堀部政男研究室仮訳）

342 Working Party on the Protection of Individuals with regard to the Processing of Personal Data

343 藤原静雄・個人情報保護法制研究会『個人情報保護法の解説（改訂版）』（2005 年）pp305-306

344 岡村久道・新保史生、「電子ネットワークと個人情報保護：オンラインプライバシー法入門」（経済産業調査会、2002 年）pp121-122

た文書と 15 の FAQ からなる。組織[345]は、このセーフハーバー原則を遵守し、毎年自己認証（self-certification）に関する報告を商務省に提出してこのセーフハーバーフレームワークに参加をすることで、EU データ保護指令の第 25 条 2 の 2 項の十分性を満たしているとみなされる。そして、EU 諸国のデータを移転する際は事前に EU 諸国に許可を得る必要がない、または許可を得ているとみなされることなる。商務省は、セーフハーバーフレームワークに参加をしている組織に関するリストを所持し、公表をしている。

なお、セーフハーバーに参加をした組織がセーフハーバー原則に違反をした場合は、虚偽及び欺瞞的な商取引における行為（FTC 法第第５条）の禁止に基づき、FTC から訴状（complaint）が発せられる。受け取った組織がその内容に同意をする場合は、同意審決（consent agreement）を結ぶことができる。同意しない場合は、審判手続き（administrative trials）に入り、審判官は、措置命令の開始又は訴状棄却を推奨する審判を行う。最終的には、委員会（commission）がその審判を受けて最終的な決定と命令を行う。さらに、FTC はこれらの同意審決や命令に違反した場合には、組織に対して民事罰を課すよう、連邦裁判所に求めることができる。

以下にセーフハーバー原則（セーフハーバープライバシー原則と FAQ）について記載をする。

○ セーフハーバープライバシー原則（Safe Harbor Privacy Principles）[346]

以下の 7 つの原則から構成される。なお、ここでいう個人データ又は個人情報は、本人を識別できる又は識別可能なものをいい、米国の組織に EU の国々から移転され、あらゆる形態で保存されているものを指す。

1. 通知

   組織は、データを収集する際に、収集と利用の目的、個人が質問又は苦情を申し出る際の組織への連絡方法、情報を提供する第三者の種類、その情報の利用及び提供を制限するために組織が個人に付与する選択及び手段について、個人に告知をしなければならない。

2. 選択

   組織は、個人データが第三者に対して提供されるか否か又は、はじめの収集時に個人が承認をした目的又は事後的に承認した目的と矛盾する目的のために利用されるか否か

345 原文では、”organization”

346 US-EU Safe Harbor Framework Guide to Self-certification March 2009, Department of Justice, http://trade.gov/publications/pdfs/safeharbor-selfcert2009.pdf

について、選択する権利を与えなければならない（オプアウト）。さらに、このような場合について、センシティブデータ（医療又は健康状態、人種又は部族的な出自、政治思想、宗教又は哲学的信条、労働組合のへの加入事実、又は個人の性生活を特定する情報などの機微情報）関しては、積極的又は明示的（オプトイン）な選択があたえなければならない。

3. 再移転（第三者へのデータの移転）

   第三者へ情報を移転することに関して、組織は通知の原則を適用しなければならない。組織は、代理人として活動する第三者（その組織のためにその組織の指示に従って活動する）に対してデータを移転することができる。ただし、その第三者について、第三者がセーフハーバーの諸原則について同意し、もしくは EU データ保護指令又は他の十分性の基準をみたしていることを確認する必要がある。代替手段として、少なくとも関連する諸原則によって求められるものと同等のプライバシー保護レベルを提供することを要求する文書による合意を第三者と交わすこともできる。これらの条件に従っている場合、組織は第三者の違反行為があっても、その事実を認識し又は認識すべきであった場合、及び、合理的な予防措置を講じていなかった場合を除き、責任を免れることができる。

4. セキュリティ

   滅失、誤用及び権限のないアクセス、提供、改変及び破損から個人情報を保護するために、組織は合理的な予防措置を講じなければならない。

5. データの完全性

   個人情報は、その利用目的に関連するものでなければならない。組織は、目的に必要な範囲で、データが利用目的の範囲であり、正確であり、完全で最新なものであることを確実にするために、合理的な措置を講じなくてはならない。

6. アクセス

   個人は、組織が持つ自分自身の個人データにアクセスをすることができ、また訂正、修正又は削除をすることができる。ただし、個人のプライバシーへの危険よりも、当該情報への個人のアクセスを提供することが不相応な負担もしくは費用を必要とする場合、又は、当該個人以外の者の権利が侵害される場合はこの限りではない。

7. 執行

   セーフハーバー原則を遵守するために、以下のことが行わなければならない。a) 個人の苦情又は紛争が解決され、法律などによって損害が賠償されるしくみがすぐに提供できる状態にあること、b)セーフハーバー原則の遵守に関して実証をする手続きがあること、c)セーフハーバー原則の遵守違反によって引き起こされる問題に関して、法的救済

を行う義務を果たすこと。組織によるセーフハーバー原則遵守を確実にするため、制裁は著しく厳しくするべきである。組織が毎年の自己認証に関する報告書の提出を怠った場合は、セーフハーバーの参加組織リストから削除され、セーフハーバーに参加する利益を得ることができなくなる。

○ FAQ 1～15

以下の 15 の FAQ のセクションにおいて、セーフハーバー原則を遵守するためには組織が何をすれば良いのか、より具体的に詳細に説明をしている。

1. センシティブデータ
2.報道関係の適用除外
3.二次的責任
4.投資銀行及び会計監査
5.データ保護機関の役割
6.自己認証
7.証明
8.アクセス
9.人事
10.第 17 条の契約
11.紛争解決と執行
12.選択　オプトアウトの時期
13.旅行情報
14.医薬品と医療品
15.公の記録及び一般に入手可能な情報

② セーフハーバー協定の現状

セーフハーバーフレームワークには、現在 3518 の企業（2014 年 3 月 31 日現在）が参加[347]をしており、その数は増えてきている。

FTC における法執行は、2014 年に入り急激に増えている。2014 年だけで 13 のケース、トータルで 23 のケースがある[348]。2000 年のセーフハーバー協定の成立以来、2009 年まで 1 つもケースがなかったのに対し、2014 年だけで 13 ものケースが執行されている。FTC のセーフハーバーフレームワークに関する法執行は、セーフハーバー協定の成立当初は、EU 諸国からの照会に基づいて法執行を行っていた。このような照会ははじめの 10 年は 1 つもなく、その後も数件ほどしかなかった[349]。そこで、FTC スタッフが自主的に（proactive）法執行に取り組み始めた。その結果、2014 年は 14 ものケースが執行された。また、この自主的な取り組みにおいて、Google、Facebook、Myaspace などのセーフハーバー原則違反に関するケースが執行されている。これらのケースでは企業に、新しい製品とサービスに関するリスクに取り組み、プライバシーと個人情報の秘密を守る包括的なプライバシープログラムを実施しなければならないことを FTC は命令している。そして、そのプログラムでは、企業は予見ができるリスクを明らかにしてコントロールしなければならない。これらの企業は、そのプログラムに関して継続して独立したアセスメントを FTC に定期的に提出しなければならない。また、プライバシーに関わる取り組みとセーフハーバーフレームワークへの参加について、不正確な説明をすることを禁止している。これらの命令に違反をした場合、FTC は民事罰を求めることができる[350]。

また、FTC はセーフハーバーの登録に関する不正に関しても厳しく対処をしており、これまでに 7 件のケースがある。

以下に現在までの FTC セーフハーバーフレームワークに関して行った法執行のリストを記載する[351]。

1. Fantage.com, Inc.　February 10, 2014
2. DDC Laboratories, Inc., d/b/a DNA Diagnostics Center January 21, 2014
3. Level 3 Communications, LLC January 21, 2014
4. Reynolds Consumer Products, Inc. January 21, 2014
5. Receivable Management Services Corporation January 21, 2014
6. Apperian, Inc. January 21, 2014
7. Baker Tilly Virchow Krause, LLP January 21, 2014
8. BitTorrent, Inc. January 21, 2014
9. Atlanta Falcons Football Club, LLC January 21, 2014
10. PDB Sports, Ltd., d/b/a Denver Broncos Football Club January 21, 2014
11. Tennessee Football, Inc. January 21, 2014
12. Charles River Laboratories International, Inc. January 21, 2014

---

347 現時点で自己認証が行われている組織だけの数であり、自今認証が行われていない（多くの場合は、自己認証の更新（1 年ごとの）を忘れている場合）組織も含めると、4583 である。U.S.-EU SAFE HARBOR LIST　http://safeharbor.export.gov/list.aspx

348 2014 年 3 月 23 日に FTC で行われた Hugh G. Stevenson 氏へのインタビュー。この時点で、さらにもう 1 つが調査中であるということであった。

349 Privacy Enforcement and Safe Harbor: Comments of FTC Staff to European Commission Review of the U.S.-EU Safe Harbor Framework (November 12, 2013)
http://www.ftc.gov/sites/default/files/documents/public_statements/privacy-enforcement-safe-harbor-comments-ftc-staff-european-commission-review-u.s.eu-safe-harbor-framework/131112europeancommissionsafeharbor.pdf

350 例えば、Google は、2012 年に 2250 万ドルを支払った。

351 http://business.ftc.gov/legal-resources/2840/35

13. DataMotion, Inc. January 21, 2014
14. Myspace LLC May 8, 2012
15. Facebook, Inc. December 5, 2011
16. Google Inc. October 24, 2011
17. Karnani, Javian and Balls of Kryptonite LLC June 9, 2011
18. Collectify LLC January 19, 2010
19. Progressive Gaitways LLC January 19, 2010
20. Directors Desk LLC January 19, 2010
21. Onyx Graphics, Inc. January 19, 2010
22. ExpatEdge Partners, LLC October 6, 2009
23. World Innovators, Inc. October 6, 2009

③ EU との関係を受けた協定改定の動向

EU はセーフハーバー協定についてそもそも不満を持っていたようであるが、いわゆるプリズム問題を発端として、セーフハーバー協定の見直しをせまる声がさまざまな方面からあがっている。

まず、欧州委員会から欧州議会と欧州評議会に向けたセーフハーバー協定に関する 2 つの報告書（Communication）[352][353]が 2013 年 11 月に示された。一つは、セーフハーバー協定の現状分析、もう一つはその分析をもとに今後どのような見直しが必要となるかを示したものである。

現状分析では、セーフハーバーフレームワークに参加をしている組織のプライバシーポリシーを公に公表するべきであること、組織がきちんとセーフハーバーフレームワークメンバーであるために自己認証を更新しているかどうか確かめられるよう、商務省のセーフハーバーに関する Web ページへリンクをおくこと、代理人として活動する第三者（その組織のためにその組織の指示に従って活動する）に対してデータを移転する場合、その第三者がセーフハーバー原則を遵守するよう確認し契約を結ぶことが必要であり、さらにその場合商務省に申し出る必要があることなど、個人データ主体に対する透明性の点で問題がある点をまず報告書は指摘している。また補償に関して、組織の Web サイトにあるプライバシーポリシーから裁判外紛争解決手続（ADR）を提供する機関へのリンクを表示することにより、EU 諸国の人々が何かプライバシーに関する問題があったときに直接コンタクトができるようにすることを要求している[354]。また、米国のセーフハーバーフレームワークの中の ADR は費用が 200 ドルから 250 ドルかかる点も問題視している[355]。また、ADR に関して手続きや苦情主に対するフォローアップなどに関する透明性、アクセスの容易性などについて商務省が積極的に計画的に監視するべきであるとする。さらに、セーフハーバーフレームワークにおいて自己認証をしている一定の数の組織に対して、セーフハーバー原則遵守に関して米国当局が職権の調査を行う必要がある。苦情処理又は調査でセーフハーバー原則遵守違反が見つかった場合は、その 1 年後に再度フォローアップ調査を行うべきである。また、遵守違反の疑いがあった場合は、EU のデータ保護機関へ通知をしなければならない。さらに、セーフハーバー原則の遵守に関する不正は、引き続

---

352 “Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbor form the Perspective of EU Citizens and Campanies Established in the EU”
http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf

353 “Communication from the Commission to the European Parliament and the Council Rebuilding Trust in EU-US Data Flows”
http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf

354 これは、2013 年 3 月に米国商務省がはじめているが、このプロセスを強化しなければならないという主張である。

355 対照的に、EU における Data Protection Panel による苦情の解決は、無料である。

き調査されなくてはならない。Web サイトなどには、セーフハーバー原則を遵守しているとうたっていても、商務省のセーフハーバーフレームワーク参加組織一覧では、自己認証に関する更新がされておらず（not current という状態）、参加組織として認められない場合があるということは、セーフハーバー協定自体の信頼を大きく揺るがせることとなるとする。最後に、プライバシーポリシーには、組織が、EU から移転された情報を、米国法上国のセキュリティ等のために政府が収集、処理することが許される場合があることを明示しなければならないとしている。

一方、見直しに関する報告書では、1.自己認証においてセーフハーバーフレームワークに参加をしている組織のセーフハーバー原則遵守について、米国当局がより監督、監視を強める必要性、2.セーフハーバー原則において、米国のセキュリティのために個人のプライバシー情報に米国政府がアクセスできるという例外規定について厳しくて適用していく必要性があることを指摘している。また、直接はセーフハーバー原則とは関係ないが関係する事項として、3.現在米国と EU が交渉中の、刑事事件における警察・司法の協力に関する個人データ移転における包括的な保護のアンブレラ条項を実現させることで、移転される個人データの保護をより強化すること、4.民間組織が保有する個人データについて、正式な処理を踏まないで米国政府機関がアクセスすることがないようにすること、などの見直しの検討が必要であると指摘をしている。さらに、5. 米国内に居住していない EU 諸国市民に対して、プライバシー保護における司法上の救済を与えるしくみを米国において備えることも必要である旨を主張している。

2014 年 3 月 12 日、欧州議会はセーフハーバー協定を停止し、EU と米国の自由な情報の移動を停止する決議を行った。これは、プリズム問題を受けて議会の委員会が行った調査をもとに、議会が行った決議である。欧州議会には、セーフハーバー協定を停止する権限はないものの、米国側に見直しのプレッシャーとなっているとは考えられる。

以上のような EU からのセーフハーバー協定及び米国と EU 間における個人データ移転に関する見直しの強いメッセージを受けて、2014 年 3 月 26 日の米 EU 首脳会談声明[356]では、2014 年夏までに、より透明性があり、効果的な法執行が行うことができるようにし、個人データの移転におけるプライバシー保護が保障されるように、セーフハーバー協定を強化するという文章が組み込まれた。また、いわゆるアンブレラ条項に関する交渉も速度をあげていく旨も明示されている。

④ セーフハーバー協定の課題

米国と EU の現在のビジネスなどの状況を踏まえると、甚大な損害を招くこととなるため、実際問題としてはセーフハーバー協定の廃止や停止というものは考えられない。事実、2014 年 3 月 26 日の米-EU の首脳会談の声明においても、今後のセーフハーバー協定を強化するという趣旨が明記されている。米国側は、今後も必ずセーフハーバー協定を発展させていき、米国と EU 間の情報移動に関する重要な役割を果たすという積極的認識である。消費者プライバシー権利章典において明記されている行動規範でセーフハーバー協定を補完していきたい意向である。一方、EU 側は、実質的には EU 企業に損害を及ぼすことが明白であるため、セーフハーバー協定を存続せざるを得ないが、成立当初から不満を抱えている。そのため、プリズム問題を契機としてなんとか少しでも EU 諸国と EU 市民の主張を反映した協定となるよう、前述した欧州委員会の報告書にあるような問題を解決できる規定に見直しを進めたい考えである。

元々米国と EU のプライバシー保護フレームワークは、根本的に異なるしくみであり、両者の間で個人データを移転するにあたって、様々な課題が存在するのは当たり前である。2000 年のセーフハーバー協定成立当初は、セーフハーバーは米国の強大な通商力と外交力によるものと言われてきており、EU 側には不満が残るものであった。プリズム問題を契機に、EU が外交的なある種の切り札を持ったことにより、セーフハーバー協定に何らかの変化が及ぼされるこ

356 EU-US Summit: Joint Statement　http://www.whitehouse.gov/the-press-office/2014/03/26/eu-us-summit-joint-statement

とになるかもしれない。

2　オーストラリアにおける個人情報保護に関する国際的枠組みへの対応状況

板倉陽一郎（弁護士）

1　はじめに

本章では，オーストラリアにおける個人情報保護に関する国際的枠組み（以下，単に「国際的枠組み」という。）への対応状況について報告する。第 2 節では，国際的枠組みへの対応状況として，①オーストラリアの，国際的枠組みへの参加状況を概観し，②これら国際的枠組みの刷新に対する現下のオーストラリアの対応状況につき，インタビューを中心に述べる。第 3 節では，2012 年プライバシー改正（プライバシー保護強化）法の内容を概観する。これは，第 2 節でも解説するように必ずしも国際的枠組みへの対応のための法改正ではないが，クラウド・コンピューティング，ビッグデータの時代を迎え，個人情報が必然的に国境を超えて移転する以上，随所に，国際的枠組みとの接合点が見えるものである。

2　国際的枠組みへの対応状況

(1)　オーストラリアの国際的枠組みへの参加状況

オーストラリアにおける国際的枠組みへの参加状況を，①OECD 及び APEC，②欧州委員会及び欧州評議会，③自由貿易協定，④データ保護機関間会合の順に述べる。

①　OECD 及び APEC

OECD（経済開発協力機構，1961 年設立）については，オーストラリアは 1971 年以来の加盟国である[357]。OECD プライバシーガイドラインの制定においては，オーストラリアの Michael Kirby 判事（卿）の貢献が知られている。Kirby 判事は，OECD プライバシーガイドライン制定の際の ad hoc Group of Experts on Transborder Data Barriers and Privacy Protection（越境データ障壁及びプライバシー保護のための特別専門家グループ，1978 年設置）において議長を務め，同グループのプライバシーガイドライン起草作業を取りまとめた。このグループは，後の情報・コンピュータ・通信政策委員会（ICCP）情報セキュリティ・プライバシー作業部会（WPISP）の母体となり，WPISP では，その後，セキュリティガイドライン，暗号ガイドラインの制定や，近年では，2013 年 OECD プライバシーガイドライン改正など，重要な議論が行われてきている。

APEC（アジア太平洋経済協力，1989 年開始）については，第一回会合以来の参加エコノミーであり，第一回の APEC 会合はオーストラリアのキャンベラにアジア太平洋地域 12 カ国の外務大臣・貿易大臣が集まったことで始まっている[358]。

APEC における個人情報保護の議論は，電子商取引推進グループ（E-Commerce Steering Group, ECSG）の中のデータ・プライバシー・サブグループ（Data Privacy Subgroup, DPS）でなされてきたが，そもそも，APEC で個人情報保護の議論がなされるに至ったのは，後述する，オーストラリアに対する欧州委員会第 29 条作業部会の十分性認定についての意見がきっかけであったといわれている[359]。

---

357 Department of Foreign Affairs and Trade, “Australia and the OECD”, https://www.dfat.gov.au/oecd/

358 服部崇『APEC の素顔　アジア太平洋最前線』（幻冬舎ルネッサンス，2009 年）22 頁。

359 堀部政男「プライバシー・個人情報保護の国際的整合性」堀部政男編著『プライバシー・個人情報保護の新課題』（商事法務，2010 年）1-59 頁，11 頁。

APECにおける個人情報保護の取り組みについて,詳細は過去の消費者庁の調査に譲るが[360],その成果として，現在，越境プライバシー執行取決め（Cross-border Privacy Enforcement Arrangement, CPEA）と，越境プライバシールールシステム（Cross-Border Privacy Rules, CBPRs）が実施されている。オーストラリアに関していえば，CPEAには，連邦プライバシーコミッショナー事務局（現在は連邦情報コミッショナー事務局）が立ち上げ当初である2010年6月より参加し，共同管理者（Joint Administrator）の役割を果たしている[361]。他方，CBPRsへの参加は2014年3月現在，なされていない[362]。

また，今回のヒアリング先でもあるColin Minihan氏（オーストラリア連邦Attorney General's Office）は長年DPSの議長を務め（2007年～2011年），CPEA及びCBPRsの実施及び運営に多大な貢献を果たしている。

② 欧州委員会及び欧州評議会

欧州委員会との関係では，2001年に出された，第29条作業部会による十分性審査に関する意見が重要である。これは，第29条作業部会の意見のなかで，唯一十分性を認めるとしなかった意見であり（2014年3月現在),「オーストラリア政府にとっては大きなショックであった」とされている[363]。その内容については既に堀部政男博士（現・特定個人情報保護委員会委員長）による紹介がなされているが[364]，ここではより詳細にみることとする。

なお，この意見を経てのち，2014年3月現在，オーストラリアから欧州委員会に対して再度審査を求めたとか，又は欧州委員会からオーストラリアに対して審査を行うことにしたなどの情報は得られていない。

A 結論及び意見の対象

欧州委員会第29条作業部会によるオーストラリアの個人情報保護制度についての十分性審査に関する意見（Article29 Data Protection Working Party, Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000, Adopted on 26th January 2001 (5095/00/EN WP40 final)）の結論は，「上記で示唆された懸念点についての適切な保護措置が導入された場合にのみ十分であるとみなされる」というものである[365]。

また，意見の対象は，文書の題名にも現れているとおり，2000年プライバシー改正（民間部門）法（のみ）である。この点は，例えば，ニュージーランドがその十分性審査において，基本権法や人権法なども参照されていた点とは差異がある[366]。

以下では，「示唆された懸念点」の各項目につき，概要を記す。なお，これらの記載は2000

---

360 消費者庁『アジア太平洋地域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25年3月）。

361 APEC Cross-border Privacy Enforcement Arrangement (CPEA), http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx

362 CROSS BORDER PRIVACY RULES SYSTEM, http://www.cbprs.org/default.aspx

363 前掲堀部編著（堀部執筆）11頁。

364 前掲堀部編著（堀部執筆）49-51頁。

365 Article29 Data Protection Working Party, *Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000*, Adopted on 26th January 2001 (5095/00/EN WP40 final)（以下，「WP29意見」という。）この意見は13頁からなるものであるが，7頁程度はNPPを転載しており，冒頭の2頁はいわば前置きであるため，実質的に十分性審査についての意見は4頁程度しか書かれていない。オーストラリアの個人情報保護制度に与えたであろう衝撃に比して，あまりに簡潔なものである。

366 WP29意見の中でも，Telecommunications Act 1997等の，特定分野における個人情報保護に関する法規範について言及がある（2頁，注2)。

年プライバシー改正法段階での連邦プライバシー法及び，後述する国家プライバシー原則を前提としており，その後の法改正で変更された点も多々あるので注意しなければならない。

B　適用除外されている部門及び活動

作業部会は，適用除外されている部門及び活動が存在していることを懸念しており，特に，小企業[367]（small business）及び，被用者データ（employee data）の適用除外を挙げている[368]。小企業に関しては，オーストラリアの事業者に対するあらゆるデータ移転が，潜在的には，法の適用外にある小企業に移転されてしまうことを危惧している。被用者データに関しては適用除外となっているが，被用者データはセンシティブデータをしばしば含むがゆえに，少なくとも国家プライバシー原則[369]（National Privacy Principles，以下，「NPP」又は「NPPs」といい，使い分けは WP29 意見の原文による。）10（センシティブ情報）からは適用除外とされるべきではないと指摘され，退職者の情報について収集，第三者への開示が本人への通知なしに行われうることも懸念している[370]。

C　例外規定

NPP2.1(g)は，利用又は第三者への開示が「法律による場合」には許されるとしているが，あらゆる法律による例外を許すのは，法的不確実性に繋がりかねず，目的外利用禁止の原理からしても，広きに過ぎる例外規定ではないかと指摘されている[371]。

D　公開されており利用可能なデータ

公開されており利用可能なデータについては，収集についての規定（NPPs1）は適用されるものの，他のプライバシー原則が適用されない。二次的利用まで自由ということになると，EU データ保護指令の線引きからは外れ，1980 年 OECD プライバシーガイドラインでもそのような例外は定めていない，ということが指摘されている[372]。

E　データ主体への透明性

事業者に対して，事前又は同時での通知が「実務的（practicable）でない場合」収集後にデータ主体への通知を行うことを認めているが，これは 1980 年 OECD プライバシーガイドラインの第 9 原則に反すると指摘されている[373]。

F　ダイレクトマーケティングに関する収集及び利用

NPPs1 及び 2 は，目的外利用禁止原則をカバーしているが，利用及び開示の制限は二次的利用にしか及んでおらず，一時的目的のための収集及び合理的に期待し得る関連する目的についての利用については，本人への通知のみで許されている（同意が要求されていない）。実務的には，ダイレクトマーケティングについて，本人の同意が不要であるということになる。作業部

---

367 年間の総売上が 300 万オーストラリアドル以下の事業者である（法 6D 条）。

368 WP29 意見 3 頁。

369 民間事業者を対象とする個人情報保護原則であり，いわゆる義務規定に対応するものである。後述するように，2012 年プライバシー改正法で，公的部門を対象とする情報プライバシー原則（Information Privacy Principles，IPP）と統合され，オーストラリアプライバシー原則（Australian Privacy Principles，APP）が成立している。そのため，本稿では，NPP や IPP の個別の規定についての詳細には立ち入らない。

370 WP29 意見 4 頁。下線は WP29 意見の中で下線が引かれている部分に倣う。以下同じ。

371 WP29 意見 4 頁。

372 WP29 意見 4 頁。

373 WP29 意見 5 頁。

会は，WP12[374]において，オプトアウト手段なしに個人データをダイレクトマーケティングに利用することは，十分であるとは認められないとしている[375]。

G　センシティブデータ

NPP10（機微情報）は，収集についてしか制限を課していないもので，利用又は開示には特段の規制がない。他方，EU データ保護指令では，特定の除外事項に該当しない限り，「処理」を禁ずるため，ここには収集のみならず，利用及び開示も含まれる[376]。

H　EU 市民の収集されない権利の欠如

法 41 条(4)項は，NPP6 又は 7 の下での活動又は実務について，プライバシーコミッショナーが調査することを認めているが，オーストラリア市民又は永住者のプライバシーの侵害がある場合のみである。その結果，オーストラリアの永住者でない EU 市民のデータが EU からオーストラリアに移転された場合，当該市民はアクセス権又は収集にかかる権利を行使できない[377]。

I　オーストラリアから第三国への Onward Transfer（越境再移転）

NPP9 は，六つの要件のどれかに該当しない限り，事業者が国外に個人情報を輸出（export）することを禁じている（当該事業者の関連会社を除く）。

NPP9(a)については，どの第三国が実質的にオーストラリアと同等の制度を備えているといえるか，プライバシーコミッショナーが提示し，補助すべきである。

NPP9(f)については，法 5 条の域外適用が，オーストラリア人にしか及ばず，NPP9 が，非オーストラリア人について拡張されないことを指摘する。これは，実質的には，オーストラリアの企業が，欧州市民のデータを輸入（import）し，オーストラリア法の適用を受けることなく輸出できることを意味し，オーストラリアが十分性認定を受けた場合，EU データ保護指令の迂回（circumvent）を可能にしてしまう[378]。

欧州評議会との関係では，オーストラリアは参加国ではなく，欧州評議会第 108 条約についても加盟していないが，欧州評議会の所管するサイバー犯罪条約については 2013 年 1 月 3 日に加盟している[379][380]。なお，サイバー犯罪条約への加盟に先立っては，連邦プライバシーコミッショナーである Timothy Pilgrim から，同条約への加盟にあたっての個人情報・プライバシー保護に関する懸念点を含む Attorney-General's Department に向けた提案（Submission）が公表されている（2011 年 3 月）[381]。

---

374 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(DG XV D/5025/98 WP 12).

375 WP29 意見 5 頁。

376 WP29 意見 5 頁。

377 WP29 意見 5 頁。

378 WP29 意見 6 頁。

379 Council of Europe, "CYBERCRIME", http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp

380 Council of Europe, "Convention on Cybercrime CETS No.:185", http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG

381 Timothy Pilgrim, Australian Privacy Commissioner, Submission to Attorney-General's Department, March 2011, http://www.oaic.gov.au/news-and-events/submissions/privacy-submissions/proposed-accessi

なお，我が国からは，欧州評議会における第一回データ保護特別委員会[382]（AD HOC COMMITTEE ON DATA PROTECTION (CAHDATA)）（2013 年 11 月）に消費者庁がオブザーバ参加しているが，オーストラリアからは参加はなかった。

③　自由貿易協定

オーストラリアが締結している自由貿易協定のうち，既に発効しているものとして，ASEAN・豪新自由貿易協定（ASEAN-Australia-New Zealand FTA），豪智自由貿易協定（Australia-Chile FTA），豪新経済緊密化協定（Australia-New Zealand Closer Economic Relations），豪米自由貿易協定（Australia-United States FTA），馬豪自由貿易協定（Malaysia-Australia FTA），星豪自由貿易協定（Singapore-Australia FTA），泰豪自由貿易協定（Thailand-Australia FTA）が存在し，締結されているが発効していないものとして，韓豪自由貿易協定（Korea-Australia FTA）がある[383]。ここでは，電子商取引章の中に見られる個人情報保護に関係する条項を中心に検討する[384]。

なお，日豪経済協力協定（Japan-Australia Economic Partnership Agreement）は 2014 年 3 月時点では「大筋合意する方向で最終調整に入った」との報道がなされているが[385]，具体的な条項は明らかではない。

A　ASEAN・豪新自由貿易協定（ASEAN-Australia-New Zealand FTA），豪新経済緊密化協定（Australia-New Zealand Closer Economic Relations）

ASEAN・豪新 FTA は 2009 年発効。電子商取引章（第 10 章）に，オンラインデータ保護（第 7 条[386]）があるほか，協力条項に，データ保護及びプライバシーに関する情報・経験共有が含

---

on-to-the-council-of-europe-convention-on-cybercrime

382 AD HOC COMMITTEE ON DATA PROTECTION (CAHDATA) 1st meeting, Strasbourg, 12-14 November 2013, CAHDATA (2013) RAP01Abr, http://www.coe.int/t/dghl/standardsetting/dataprotection/CAHDATA/CAHDATA%282013%29RAP01Abr_En.pdf

383 Department of Foreign Affairs and Trade, “Australia’s Trade Agreements”, http://www.dfat.gov.au/fta/

384 電子商取引章の他に，電気通信に関する章や，金融に関する章においても個人情報又は個人データ保護に関する条項がおかれることがある。なお，FTA/EPA において電子商取引章がおかれるようになったのは，比較的最近であり，例えば，渡邊頼純監修・外務省経済局 EPA 交渉チーム『解説　FTA・EPA 交渉』（日本経済評論社，2007 年）で解説されているところの，日本が 2007 年までに締結した EPA（シンガポール，メキシコ，マレーシア及びフィリピン）では電子商取引章は設けられておらず，同書においても言及はない。他方，TPP においては電子商取引について交渉が行われているとされており，東條吉純「TPP 協定交渉におけるサービス貿易の自由化」ジュリスト 1443 号 42-47 頁（2012 年），45 頁は TPP における電子商取引章について触れている。

385 産経ニュース「日豪 EPA、4 月大筋筋合意へ　牛肉関税は協議継続」（2014 年 3 月 26 日），http://sankei.jp.msn.com/economy/news/140326/fnc14032618190009-n1.htm

386 “Article 7 Online Data Protection
1. Subject to Paragraph 2, each Party shall, in a manner it considers appropriate, protect the personal data of the users of electronic commerce.
2. A Party shall not be obliged to apply Paragraph 1 before the date on which that Party enacts domestic laws or regulations to protect the personal data of electronic commerce users.
3. In the development of data protection standards, each Party shall consider the international standards and criteria of relevant international organisations.”

まれている（第 9 条第 1 項 c[387]）。オーストラリア及びニュージーランドの他，必ずしも個人情報保護制度が整備されているとはいえない ASEAN を含む自由貿易協定であるためか，具体的な義務を課すような文言にはなっていない。

豪新経済緊密化協定は 1983 年発効であり，電子商取引章自体が見られないようである[388]。

B　豪智自由貿易協定（Australia-Chile FTA）

2009 年発効。電子商取引章（第 16 章）に，「個人データ」の定義（16.1 条(d)[389]）があり，オンライン個人データ保護（16.8 条[390]），個人データを含むコンサルテーションの条項（16.10 条第 1 項[391]）が存在する。「個人データ」の定義も内容的には「識別された又は識別され得る」本人を含むように定められた，オーソドックスなものであり，個人データ保護の条項も，双方の国内の施策を最大限尊重するものとなっている。

C　豪米自由貿易協定（Australia-United States FTA）

2005 年発効。豪米 FTA には，電子商取引章（16 章）があるにもかかわらず，データ保護やプライバシーに関する条項はみられない。これは，比較的早い時期に締結された FTA であるという点も関係していると思われるが，オーストラリアと米国の間における個人情報保護制度へのギャップも無関係ではないようにみえる。①米国の執行制度（FTC 法 5 条による不公正・欺瞞的な行為又は慣行（unfair or deceptive acts or practices）への包括的な執行））に親和的な CBPRs について，オーストラリアが加入するためには「多くの障壁」があるとされ，CPEA にはプライバシー執行機関（連邦プライバシーコミッショナー）が当初から加入したにもかかわらず，未だ，加入の目処が立っていないこと，②TPP における個人データ保護に関する条項を巡り，オーストラリア・ニュージーランドと米国の間に対立が存することが指摘されていること[392]などが，このギャップを裏付けている。

---

387 “sharing information and experiences and identifying best practices in relation to domestic legal and policy frameworks in the sphere of electronic commerce, including those related to data protection, privacy, consumer confidence, cyber-security, unsolicited electronic mail, electronic signatures, intellectual property rights, and electronic government;”

388 協定の内容の，ダンピング防止措置についての解説として，川島富士雄「地域経済統合におけるダンピング防止措置の適用に関する規律－横断的比較を通じた規律導入の条件に関する考察－」RIETI Discussion Paper Series 06-J-053，12 頁。

389 “personal data means information about an individual whose identity is apparent, or can reasonably be ascertained, from the information;”

390 “Article 16.8: Online Personal Data Protection
Each Party shall adopt or maintain a domestic legal framework which ensures the protection of the personal data of the users of electronic commerce. In the development of personal data protection standards, each Party shall take into account the international standards and criteria of relevant international bodies.”

391 “The Parties will consult on electronic commerce matters arising under this Chapter including in relation to electronic signatures, data protection, online consumer protection and any other matters agreed by the Parties.”

392 Jeffrey J. Schott at el., *Understanding the Trans-Pacific Partnership*, Policy Analyses in International Economics 99, January 2013.邦語文献では，前掲東條が「…米国は，既存 PTA にはない新規の提案も行っている。詳細は明らかでないが，データ・情報の国境を越える自由流通，及び，サービス提供者・顧客によるデータ・情報への自由なアクセスを目的として，締約国による越境データ流通の遮断行為を禁止する規定や，サービス提供の条件としての，自国領域内へのデータ・サーバー施設等の設置要求を禁止する規定を含む提案であるとされる。同時に，プライバシー保護に対する締約国の利益とのバランスにも配慮した仕組みも組み込まれ

D　馬豪自由貿易協定（Malaysia-Australia FTA）

2012 年発効。馬豪 FTA には，電子商取引章（第 15 章）が存在するが，オンライン個人データ保護に関する条項（15.8 条[393]）がおかれているに留まっている。発効当時（2012 年），マレーシアには個人情報保護法制も，プライバシー執行機関も整備されていなかったことからか，簡素な規定があるのみである。

E　星豪自由貿易協定（Singapore-Australia FTA）

2003 年発効。星豪 FTA には，電子商取引章（第 14 章）が存在するが，オンライン個人データ保護に関する条項（第 7 条[394]）があるにとどまっている。マレーシア同様，発効当時（2003 年），シンガポールには個人情報保護法制も，プライバシー執行機関も整備されていなかったことからか，簡素な規定があるのみである。

F　泰豪自由貿易協定（Thailand-Australia FTA）

2005 年発効。電子商取引章（第 11 章）が存在するが，具体的な条項はオンライン個人データ保護に関する 1106 条[395]のみにとどまっており，マレーシアやシンガポールの FTA と同様である。マレーシアやシンガポールは，オーストラリアとの FTA 締結後に，個人情報保護法制の整備やプライバシー執行機関の設置がなされたが，タイでは特段の動きは見られない。

G　韓豪自由貿易協定（Korea-Australia FTA）

2014 年締結，未発効。電子商取引章（第 15 章）が存在し，オンラインデータ保護に関する 15.8 条[396]の他，個人データについての定義が設けられている（15.10 条[397]）。

⑤　データ保護機関間会合

ている」（45 頁）と指摘する。

393 “Article 15.8 Online Personal Data Protection
1. Each Party shall establish or maintain legislation or regulations that protect the personal data of the users of electronic commerce.
2. In the development of personal data protection standards, each Party shall take into account the international standards and criteria of relevant international organisations.”

394 “ARTICLE 7 Online Personal Data Protection
1. Notwithstanding the differences in existing systems for personal data protection in the territories of the Parties, each Party shall take such measures as it considers appropriate and necessary to protect the personal data of users of electronic commerce.
2. In the development of data protection standards, each Party shall take into account the international standards and criteria of relevant international organisations.”

395 “Article 1106 Online Personal Data Protection
1. Notwithstanding the differences in existing systems for personal data protection in the territories of the Parties, each Party shall take such measures as it considers appropriate and necessary to protect the personal data of users of electronic commerce.
2. In the development of data protection standards, each Party shall, to the extent possible, take into account international standards and the criteria of relevant international organisations.”

396 “ARTICLE 15.8: ONLINE PERSONAL DATA PROTECTION
Each Party shall adopt or maintain measures which ensure the protection of the personal data of the users of electronic commerce. In the development of personal data protection standards, each Party shall take into account the international standards, guidelines and recommendations of relevant international organisations.”

397 “personal data means any information about an identified or identifiable individual;”

データ保護・プライバシーコミッショナー会議については，連邦プライバシーコミッショナー事務局， ニューサウスウェールズ州プライバシーコミッショナー、北部地域情報コミッショナー、ビクトリア州プライバシーコミッショナーが参加機関となっている(2014 年 3 月現在)。第 25 回会合（2003 年）はシドニーで開催されたほか，第 35 回会合（2013 年，ワルシャワ）開催時の執行委員会（5 ヶ国から構成）には連邦プライバシーコミッショナーである Timothy Pilgrim が名を連ねている。執行委員会にはホスト国と前回ホスト国が委員として加わることが慣例であり，そうするとオーストラリアの委員は 3 ヶ国のうちの一人として選ばれていることになる。その他，情報コミッショナー又は連邦プライバシーコミッショナーのオープンカンファレンスへの登壇，クローズドセッションではときに決議案の提案国となるなど，存在感を持って参加している。

APPA（アジア太平洋プライバシー機関会合）については，連邦情報コミッショナー事務局，ニューサウスウェールズ州情報プライバシー委員会，北部地域情報コミッショナー事務局，クイーンズランド州情報コミッショナー事務局及びビクトリア州プライバシーコミッショナー事務局が参加機関となっている[398]（2014 年 3 月現在）ほか，APPA 事務局を連邦情報コミッショナー事務局が引き受けている。直近でも，第 40 回（2013 年 11 月）がシドニーで，第 36 回（2011 年 12 月）がメルボルンで，第 33 回（2010 年 6 月）がダーウィンで開催されるなど，積極的な活動が見られる。

GPEN（グローバルプライバシー執行ネットワーク）についても，連邦情報コミッショナー事務局，ニューサウスウェールズ州情報プライバシー委員会，北部地域情報コミッショナー事務局，クイーンズランド州情報コミッショナー事務局及びビクトリア州プライバシーコミッショナー事務局が参加機関となっている[399]（2014 年 3 月現在)。

(2)　オーストラリアの国際的枠組みへの対応状況

ア　2013 年改正 OECD プライバシーガイドライン

2013 年に改正された OECD プライバシーガイドラインへの対応については，政府において，ALRC[400]の意見書に沿った一連の改正以外に別途改正が必要であるとは認識していないとのことである[401]。また，NSW 州プライバシーコミッショナー事務局においても，州法に直接的に適用されないことは確認した上で，改正 OECD プライバシーガイドラインの概念及び理念は，オーストラリアの制度と整合的であると認識している[402]。

有識者からは，改正 OECD プライバシーガイドラインの条項の中では，アカウンタビリティに関連する内容がもっとも重要であるとの見解が示された。また，2012 年プライバシー改正法は，ALRC における報告書が 2008 年，政府の対応が 2010 年，議会を通過したのが 2012 年であったため，内容的には古くなっている（また，その時系列からも，改正 OECD プライバシーガイドラインを踏まえたものではない）との指摘があり，他方，2012 年プライバシー改正法で導入された APP[403]1.2 は改正 OECD プライバシーガイドラインにおけるプライバシーマネジメ

398 http://www.appaforum.org/members/。
399 https://www.privacyenforcement.net/。
400 後述する。
401 2014 年 3 月 18 日に Attorney-General's Department で行われた Colin Minihan 氏へのインタビュー（以下，「Minihan 氏インタビュー」という)。
402 2014 年 3 月 17 日に New South Wales 州情報及びプライバシー委員会事務局で行われた Meredith Claremont 女史及び Sean McLaughlan 氏へのインタビュー（以下，「NSW 事務局インタビュー」という。）
403 後述する。

ントプログラムに類似したものであるとされた[404]。
いずれにせよ，オーストラリアにおいて，改正 OECD プライバシーガイドラインのための特段の法改正等は予定されていないようである。

イ　欧州評議会第 108 条約現代化
前述のとおり，オーストラリアは欧州評議会への参加は見られず，政府においては，2012 年プライバシー改正法に注力してきたため，現時点では，加盟による利益を見定めている段階にある[405]。有識者からは，オーストラリアとしては欧州評議会第 108 条約に加盟する計画も，そのモチベーションもないとの見解が示されている[406]。
このように，欧州評議会第 108 条約現代化については，オーストラリアにおいて直近の対応は予定されていない。

ウ　欧州委員会十分性認定
オーストラリアが第 29 条作業部会の意見によって十分性認定に留保が付された点は前述した。しかしながら，その後，欧州委員会と十分性認定を巡って外交交渉が進められているかというと，そのような状況にはないようである。有識者からは，ニュージーランドが十分性認定に関して 14 年の年月を費やした点の指摘とともに，オーストラリア政府において（そこまでの労力に見合った）利益を見出していないのではないかとの指摘があった[407]。

エ　APEC-CBPRs 等の認証制度
前述のとおり，Colin Minihan 氏は DPS 議長として APEC-CPEA 及び CBPRs の成立に多大な貢献をしたが，政府としての CBPRs への加入については，まずは 2012 年プライバシー改正法とのギャップ分析が必要であり，また，制度導入の利益を分析することも必要であるとされる。認証制度（トラストマーク）の導入についての需要を図るため，オーストラリアの経済界との対話も重要であるとする[408]。有識者からは，認証制度の導入には「多くの障壁」があるとされている[409]。CBPRs への加入については，認証機関となるアカウンタビリティ・エージェントが用意される必要があり，米国の加入にあたっては TRUSTe がこの役割を担っており，メキシコの加入にあたっては La Asociación Mexicana de Internet (AMIPCI)[410]が想定されているとされる[411]。しかしながら，オーストラリアにおいては，アカウンタビリティ・エージェントとして想定される団体について，今のところ名前が上がっていない状況である。
このように，連邦プライバシーコミッショナー（当時）は APEC-CPEA について立ち上げ時から加入しているものの，オーストラリア政府の CBPRs への加入については，なお，現行法とのギャップについて分析を必要としている段階である。また，アカウンタビリティ・エージェントの選定についても目処が立っているようには思われない。

オ　越境データ移転
これまで見てきたとおり，オーストラリアは欧州からの十分性認定を得られておらず，また，

---

404 2014 年 3 月 17 日に Information Integrity Solutions 社で行われた Malcolm Crompton 氏（同社 Managing Director，元豪州連邦プライバシーコミッショナー）及び同社 Annelies Moens 女史（同社販売管理部長）へのインタビュー（以下，「IIS インタビュー」という。）
405 Minihan 氏インタビュー。
406 IIS インタビュー。
407 IIS インタビュー。
408 Minihan 氏インタビュー。
409 IIS インタビュー。
410 La Asociación Mexicana de Internet (AMIPCI), http://www.amipci.org.mx/。
411 Malcolm Crompton, “Interoperability effort between APEC CBPR and EU BCR”

必ずしも十分性認定に向けた外交交渉を行っているわけでもない状況にあるため，欧州からの越境データ移転のためには，①本人の同意，②標準契約約款（Standard Contractual Clauses，SCC），③拘束的企業準則（Binding Corporate Rules，BCR）など，例外規定の利用が必要なはずである。

この点，政府においては，SCC 又は同意による移転が通常であると把握しているようである[412]。有識者においては，ほとんどの移転は契約（同意）により行われており，どれくらい SCC が使われているかはわからない，との認識である[413]。経済界から，十分性認定を得るべく交渉して欲しいとの要望も，特段聞かれない[414]。同様に，EU-US セーフハーバーのようなセーフハーバーについても，これについての要望はないとのことである。

他方，オーストラリアと最もつながりが深い外国であるニュージーランドについては，欧州委員会によって十分性が認定されている[415]。そうすると，理論上は，ニュージーランドは十分性認定を得るために，Onward Transfer（越境再移転）を規制しなければならないはずであり[416]，オーストラリアとの間の越境移転について，問題になっているのではないかという懸念も生ずるが，実務的には問題が表面化しているという様子は見られない。

(3) まとめ

このように，オーストラリアからは，OECD，APEC などの議論に人材が輩出されてきたが，オーストラリア政府の国際的枠組みへの対応は，積極的とは言い難い状況にあり，各枠組みの刷新に対する特段の対応の必要性も認められていないようである。経済連携協定にみえる電子商取引章にかかる個人情報保護の条項も，特色のあるものではない。欧州とのデータ移転につき経済界から強い要望が出ているような状況にもなく，現時点では優先順位が高い事項と考えられているとは言い難い。実際に，現在のオーストラリア政府は，規制緩和に大変力を入れており[417]，後述する 2012 年プライバシー改正法については，規制緩和という方向性とは逆行するからか，全く周知啓発活動を行っていないという[418]。

2001 年の第 29 条作業部会の意見書は，間違いなく，オーストラリアの個人情報保護制度に冷水を浴びせたが，欧州においても越境移転制限についての法執行は極めて低調であること[419]，ニュージーランドが 14 年を掛けて十分性認定を得たにもかかわらず，少なくとも経済的には目に見えるメリットがないことは，現時点でのオーストラリア政府や経済界の対応に影響を与

412 Minihan 氏インタビュー。
413 IIS インタビュー。
414 Minihan 氏インタビュー。
415 COMMISSION IMPLEMENTING DECISION of 19 December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand (notified under document C(2012) 9557) (Text with EEA relevance) (2013/65/EU)
416 詳細については，消費者庁『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）158 頁以下（加藤隆之執筆）。
417 規制緩和室（Office of Deregulation）は，2013 年 11 月以降，大統領・内閣省に設置されている。以前は，財政・規制緩和省として財政省の所掌であった。
http://www.dpmc.gov.au/deregulation/index.cfm
418 IIS インタビュー。なお，後述するように，連邦情報コミッショナー事務局においては施行に備えた解説資料をふんだんに用意している。
419 違法な越境データ移転について，”there is little or no sign of enforcement action by the supervisory authorities”とするものとして，Kuner, C. (2011), “Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future”, *OECD Digital Economy Papers*, No. 187, OECD Publishing.
http://dx.doi.org/10.1787/5kg0s2fk315f-en.

えているものと思われる。
他方で，データ保護機関（プライバシー執行機関）である連邦情報コミッショナー，同事務局及び連邦プライバシーコミッショナーは，データ保護機関間会合には積極的に参加しており，データ保護の世界では信頼を得ているといえる。
「プライバシー外交[420]」が，政府とデータ保護機関で二元的になることから，確かにこのような，政府の姿勢とデータ保護機関の姿勢が全く異なる状況は生じ得るが，一般的には，政府の力の入れ具合とデータ保護機関の積極的活動は比例するのであり[421]，オーストラリアには，世界的に見ても，奇妙な状況が生じているといってよいであろう。

3　2012 年プライバシー改正（プライバシー保護強化）法の概説

ここでは，2014 年 3 月 12 日に施行された，2012 年プライバシー改正（プライバシー保護強化）法について概説する。オーストラリアの個人情報保護法制については既に消費者庁（及び前身たる内閣府国民生活局）の調査で相当程度の紹介がなされており，詳細はそれらを参照されたいが[422]，2012 年プライバシー改正法の説明に必要な範囲で，オーストラリアの個人情報保護法制そのものにも触れる。

(1)　プライバシーの保護に関する憲法上，私法上の根拠

オーストラリアの個人情報保護法制についての理解の前提として，オーストラリアにおけるプライバシーの保護に関する憲法上，私法上の根拠についての議論を確認する。

ア　プライバシーの保護に関する憲法上の根拠

オーストラリアの憲法上，プライバシー権に関する条項は存在しない。そもそも，1901 年 1 月 1 日に成立したオーストラリア連邦憲法には、「権利章典」が存在せず，人権保障に関する条項もほとんどみられないとされる[423]。1973 年には，国際人権規約（B 規約）を国内法化するための人権法案（Human Rights Bill 1973 (Cth)）が連邦議会に提出された。この法案には個人のプライバシーの権利を保障する内容が含まれており，私人間の権利侵害をも規制するものであったが，議会での強い反対で廃案となった[424]。このような状況に関して，オーストラリアの著名な人権弁護士である Geoffrey Robertson 氏は，「オーストラリアは，基本的人権が法的に保護されずにいる，世界で唯一の民主的国家」であるとまで述べる[425]。このように，オーストラリアにおいて，プライバシーの保護については，国内憲法上の基礎を持たないといってよい。

イ　プライバシーの保護に関する私法上の根拠

法律レベルでも，オーストラリア法上は，プライバシーの一般的権利は認められておらず，

---

420 前掲堀部編著（堀部執筆）10 頁。

421 例えば，ウルグアイは，2012 年にデータ保護機関を中心に第 34 回国際データ保護・プライバシーコミッショナー会議を開催した後，欧州委員会からの十分性認定を得て，欧州評議会第 108 条約にも加盟している。

422 2009 年 3 月段階の状況として，新保史生「オーストラリア」内閣府『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 21 年 3 月）（以下，「2009 年調査」という。）190-222 頁。2011 年 3 月段階の状況として，六川浩明「オーストラリア」消費者庁『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）（以下，「2011 年調査」という。）146-164 頁。

423 山田邦夫「オーストラリアの憲法事情」国立国会図書館調査及び立法考査局『諸外国の憲法事情　オーストラリア』（2003 年 12 月）85-133 頁，115 頁。

424 前掲山田，120 頁。

425 Geoffrey Robertson, *The Statute of Liberty*, Vintage Books (2009). 但し，Robertson の見解に対する批判も同書第 7 章で検討されている。

不法行為法の観点からも，プライバシーそれ自体を保護するものはない[426]，とされ，個人情報に関するプライバシーは，連邦法，州及び地域法，信頼違反（breach of confidence[427]），契約法の「ミックス」によって保護されているとされる[428]。不法行為としては，他の不法行為を拡張することで，派生的類型（derivative manner）として保護されているとされる[429]。プライバシーの保護に関する私法上の根拠は，必ずしも一義的ではない。

(2) プライバシー保護制度の概要

ア 根拠法

① 連邦法

オーストラリアの連邦法レベルでのプライバシー保護制度は，連邦政府が 1987 年に National ID Card を導入しようとした際に，国民のプライバシー保護に懸念が生じたことを直接の契機として，1988 年に連邦プライバシー法（Privacy Act 1988）が成立したことからはじまるとされる[430]。つまり，オーストラリアのプライバシー保護制度，その嚆矢である 1988 年プライバシー法は，プライバシーの保護に関する憲法上の，又は私法上の必要性から生まれ出たものとは理解されていない。しかしながら，その成り立ちからして，公的部門を対象とする法律として制定されたのであり，情報プライバシー原則（IPP）は公的機関のみを対象としていた。IPP は，1980 年 OECD プライバシーガイドラインを基礎とした。1988 年プライバシー法は 1990 年に改正され，信用状況報告（credit reporting）に関する規制をⅢA 編に加えるに至った。

その後，2000 年プライバシー改正（民間部門）法が成立し，2001 年 12 月 1 日より，民間事業者（organisations）を対象とする国家プライバシー原則（NPP）が導入された[431]。政府はこれにより欧州連合との取引が促進されることを期待したが[432]，この改正法（により改正された 1988 年プライバシー法）が，欧州委員会第 29 条作業部会より，十分とはいえないとの意見の対象となった点は前述のとおりである。この改正を経て，1988 年プライバシー法の適用対象は，連邦政府機関，オーストラリア首都特別地域の政府機関，民間事業者（ただし小企業を除く）及び，健康情報を扱う民間事業者ということになった。

プライバシー法の改正は 2000 年と 2005 年に，上院の委員会により掲げられ，現在の技術の文脈に合わせ，法を十分で効果的なものにするための改正が必要とされた。これにより，連邦政府は 2006 年に，連邦法改正委員会（Australian Law Reform Commission, ALRC）に対し，1988 年プライバシー法改正のための諮問を行った。ALRC の最終報告書（For Your Information: Australian Privacy Law and Practice）は，2008 年 8 月に公表された。これは

---

426 Mirko Bagaric at.el., *Australian Human Rights Law*, CCH Australia Ltd. (2011), ¶.17-202.

427 英国法における信頼違反たる不法行為については，ジョン・ミドルトン「イギリスの 1998 年人権法とプライバシーの保護」一橋法学 4 巻 2 号 373-410 頁（2005 年），394 頁以下。

428 Brian Fitzgerald at el., *Internet and E-commerce Law, Business and Policy*, Thomason Reuters (Professional) Australia Ltd. (2011), p.911.

429 Australian Broad Casting Corporation v. Lenah Game Meats Pty Ltd. (2001) 208 CLR 199; [2001] HCA 63 (ABC v. Lenah).

430 2009 年調査 146 頁。この際，National ID Card についての法案（Australia Card Bill）は不成立となったが，税番号の利用目的として，収入に関する名寄せをするという拡張は成立したため，そのセーフガードとして，1988 年プライバシー法は成立した。前掲 Fitzgerald 他 921 頁。

431 2009 年調査 190 頁，2011 年調査 146 頁。IPP 及び NPP の具体的な内容については 2009 年調査 190-191 頁，2011 年調査 149-150 頁。

432 前掲 Fitzgerald 他 922 頁。

2600 頁に及ぶものであり，連邦プライバシー法改正のための 295 の提言が含まれている[433]。連邦政府は 2009 年 10 月に，295 の提言のうち，197 に応答し，141 の提言を受け入れ，34 は条件付きで受け入れ，20 は拒絶した[434]（第 1 ステージ）。この応答の具体化が，2012 年プライバシー改正（プライバシー保護強化）法（後述）である。なお，第 1 ステージで対応された 197 の提言の残余（98 の提言）については，第 2 ステージで対応される[435]。

なお, 連邦プライバシー法以外に, プライバシー又はデータ保護に関する法令としては, 1905 年センサス及び統計法（the Census and Statistics Act 1905(Cth)），1918 年連邦選挙法（the Commonwealth Electoral Act 1918(Cth)），1958 年移民法（the Migration Act 1958(Cth)），2005 年オーストラリアパスポート法（the Australian Passport Act 2005(Cth)），1953 年国家健康法（the National Health Act 1953(Cth)），1914 年犯罪法（the Crimes Act 1914(Cth)），2001 年会社法（the Corporations Act 2001(Cth)），1990 年データマッチングプログラム（手当及び税）法（the Data Matching Program (Assistance and Tax) Act 1990(Cth)），1982 年情報公開法 (the Freedom of Information Act 1982(Cth))，2010 年健康識別子法 (the Healthcare Indentifiers Act 2010(Cth)) などが挙げられる[436]。

②州及び地域法

1988 年プライバシー法は州及び地域の政府機関には適用がなく，これらにおける個人情報の取扱いはそれぞれの州及び地域法によって規律されている。西オーストラリア州及び南オーストラリア州にはこのための特別の立法が存せず，オーストラリア首都特別地域は 1988 年プライバシー法の直接の適用対象であるが，ニューサウスウェールズ（NSW 州）（1998 年プライバシー及び個人情報保護法)，ビクトリア州 (2000 年情報プライバシー法)，タスマニア州 (2004 年個人情報保護法)，北部地域（2002 年情報法)，クイーンズランド州（2009 年情報プライバシー法）はそれぞれ，州及び地域の政府機関の個人情報の取扱いを規律している。また，州又は地域によっては，健康情報の規律に関して独自の州法をおいているところもある[437][438]。

イ　監督機関

①　連邦法[439]

1988 年プライバシー法の執行・運用は連邦情報コミッショナー事務局内の連邦プライバシーコミッショナーによりなされている。

かつては，2000 年プライバシー改正（連邦プライバシーコミッショナー事務局）法（the Privacy Amendment (Office of the Privacy Commissioner) Act 2000(Cth)）により，連邦プライバシーコミッショナー事務局が 1988 年プライバシー法の監督・執行機関としておかれていたが, 2010 年 11 月 1 日以降, 2010 年連邦情報コミッショナー法 (the Australian Information Commissioner Act 2010(Cth)) により，新たに連邦情報コミッショナー事務局が設置され，長として連邦情報コミッショナーが置かれた。（初代連邦情報コミッショナーは John McMillan 教授が務めている。）連邦情報コミッショナーを補助するものとして，連邦プライバシーコミッショナーと，連邦情報公開コミッショナーが置かれている。連邦プライバシーコミッショナーは，引き続き Timothy Pilgrim が務めている (2010 年から連邦プライバシーコミッショナー，それ以前は 1998 年から連邦副（deputy）プライバシーコミッショナー)。

---

433 2011 年調査 148 頁。

434 前掲 Fitzgerald 他 924 頁。2011 年調査 149 頁。

435 2011 年調査 149 頁。

436 前掲 Fitzgerald 他 915 頁。

437 Office of the Australian Information Commissioner, “State and territory privacy law”, http://www.oaic.gov.au/privacy/other-privacy-jurisdictions/state-and-territory-privacy-law

438 前掲 Fitzgerald 他 916-921 頁。

439 前掲 Fitzgerald 他 924-925 頁。

連邦情報コミッショナーと連邦プライバシーコミッショナーの権限分配等についての詳細は，以前の消費者庁調査に譲る[440]。

② 州及び地域法[441]

前述のとおり，1988 年プライバシー法は州及び地域の政府機関には適用がなく，これらにおける個人情報の取扱いの監督機関も，それぞれの州及び地域法によって設置されている。NSW 州においては情報及びプライバシー委員会（長は情報コミッショナー），ビクトリア州においてはビクトリアプライバシーコミッショナー，タスマニア州においてはタスマニアオンブズマン，北部地域においては情報コミッショナー，クイーンズランド州においてはプライバシーコミッショナーがそれぞれ設置されている。独自の州法を持たない西オーストラリア州では監督機関が設置されておらず，南オーストラリア州では行政規制としてのプライバシー原則を所管するプライバシー委員会が存在する。オーストラリア首都特別地域の監督は連邦情報コミッショナー，連邦プライバシーコミッショナーによってなされる。

(3) 2012 年プライバシー改正（プライバシー保護強化）法

法改正への対応は 2012 年から 2013 年にかけて，連邦情報コミッショナー事務局の業務を引き続き独占しており，プライバシー法の 25 年の歴史の中で最も抜本的な改正である 2012 年プライバシー改正法は，2012 年 5 月 23 日に議会に提出され，2012 年 11 月 29 日に議会を通過した。連邦情報コミッショナー事務局は，施行日とされた 2014 年 3 月 12 日までに政府機関や民間事業者が施行準備をする際に必要となる，約 50 のガイダンス資料を作成した[442]。政府は広報啓発活動をほとんど行っていないとされているが，データ保護機関においては，施行準備のための地道なドラフティングが行われていたのである。

現時点で，2012 年プライバシー改正法への反応は，得てして良好である[443]。但し，ドラフトアクションポリシー[444]については，異議を予想している。特に，監査権限がどのように行使されるのかについては，経済界から感心が寄せられている。なお，2012 年プライバシー改正法の影響は，民間部門よりは，公的部門の方が，より大きいとされる[445]。

ア オーストラリアプライバシー原則（Australian Privacy Principles，APP 又は APPs）

① 概要[446]

2012 年プライバシー改正法により，公的部門に適用されていた情報プライバシー原則と民間事業者に適用されていた国家プライバシー原則は，新たに 13 のオーストラリアプライバシー原則（Australian Privacy Principles，APP 又は APPs）に移行した。これは，公的部門及び民間部門に共通して適用される原則である。APP の対象となる政府機関及び民間事業者はあわせ

---

440 2011 年調査 146-156 頁。

441 前掲 Fitzgerald 他 916-921 頁。

442 Office of the Australian Information Commissioner, *Annual Report 2012-2013*（以下，「2012 年年次報告書」という。）, p.6, p.48.

443 2014 年 3 月 17 日に連邦情報コミッショナー事務局で行われた Andorew Solomon 課長と Sarah Croxall 女史へのインタビュー（以下，「OAIC インタビュー」という）。

444 Office of the Australian Information Commissioner, *Office of the Australian Information Commissioner's privacy regulatory action policy*, (draft) March 2014.

445 OAIC インタビュー。

446 APPs の解説は主として Office of the Australian Information Commissioner, *Privacy law reform for APP entities (organisations) protecting information rights-advancing information policy* による。条文上は，2012 年プライバシー改正法後の 1988 年プライバシー法附則 1 条に該当し，これを抜き出した資料として，Office of the Australian Information Commissioner, *Privacy fact sheet17 Australian Privacy Principles*, January 2014.

て「APP 対象者（APP entities）（以下，「APP 対象者」又は単に「対象者」という。）」と称されることになった。APP は，収集，利用及び開示，正確性及びセキュリティ，開示及び訂正という，情報のライフサイクルを反映している。また，適用除外される場面として，「一般的許可状況（permitted general situation，7 種類。16A 条）」「医療健康許可状況（permitted health situation，5 種類。16B 条）」という概念が導入された。

② APP1　オープンで透明性の高い個人情報のマネジメント

対象者は，明確に表示され，更新されるプライバシーポリシー（APP プライバシーポリシー）を備えなければならず（APP1.3），APPs を遵守するためのプロセスを導入するための合理的な措置（reasonable steps）を採らなければならない（APP1.2）。

APP1 は，NPP5 が要求している公開性の原則より，プライバシーポリシーに関して，更に全体的な要件を導入している。また，APPs や，承認された APP コードの遵守についての，実務，手続及びシステムの導入，苦情や不服申立ての処理について可能にすることなどを求めている。有識者からは，APP1.2 と，改正 OECD プライバシーガイドラインにおけるプライバシーマネジメントプログラムの規定との類似性が指摘されている[447]。ただし，改正 OECD プライバシーガイドラインの成立は契機ではない。

③ APP2　匿名性と仮名性

データ本人に，対象者について，識別（identify）しないように求めることや，仮名を用いることを許す（APP2.1）が，個人を識別せずに，又は仮名で取り扱うことが実務的ではない（impracticable）場合等が，例外事由として定められている（APP2.2）。

データの本人に，匿名性や仮名性を確保するオプションを与える条項であるが，「実務的ではない」という広範な例外事由もまた定められている点が特徴である。APP2 は表題を「匿名性と仮名性」としているが，匿名データ又は仮名データを作り，別の規律を施すという，欧州一般データ保護規則提案[448]や，我が国の制度見直しの方向性[449]とは，別のアプローチである。

④ APP3　個人情報と機微情報の収集

個人情報は，当該情報が対象者の機能又は活動について，合理的に必要な場合（政府機関又は事業者。APP3.2）又は，直接的に関連する場合（政府機関。APP3.1）にのみ，収集することができる。収集は適法で公正な方法で行われなければならず（APP3.5），原則として，本人から収集しなければならない（APP3.6）。

機微情報の取得には，個人情報に掛かる要件に加え，本人の同意が必要である（APP3.3(a)）。機微情報とは，個人情報のサブセットであり，人種，出自，政治的言論，宗教的信念，性的傾

---

447 IIS インタビュー。

448 European Parliament, *European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Ordinary legislative procedure: first reading)*, P7_TA-PROV(2014)0212, http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN&ring=A7-2013-0402

449 『パーソナルデータの利活用に関する制度見直し方針』（平成 25 年 12 月 20 日高度情報ネットワーク社会推進戦略本部決定）は，「個人情報及びプライバシーの保護に配慮したパーソナルデータの利用・流通を促進するため、個人データを加工して個人が特定される可能性を低減したデータに関し、個人情報及びプライバシーの保護への影響並びに本人同意原則に留意しつつ、第三者提供における本人の同意を要しない類型、当該類型に属するデータを取り扱う事業者（提供者及び受領者）が負うべき義務等について、所要の法的措置を講ずる。」とする（3 頁）。

向，健康情報及び遺伝的情報等を含むような情報をいう（6 条）。機微情報の定義は 2012 年プライバシー改正法で広げられ，自動生体評価又は生体認証の目的に用いられる生体情報（biometric information）（6 条(d)）や，生体テンプレート（biometric templates）（6 条(e)）が含まれるとされた[450]。

⑤ APP4 望まぬ個人情報の取扱い

望まぬ個人情報（unsolicited personal information）の取扱いについての新たな原則である。対象者が，要求していないにもかかわらず個人情報を受け取ってしまった場合，対象者は，受領から合理的な期間内に，APP3 に従った収集であったかを検討しなければならない（APP4.1）。適法な収集でなかった場合，合法かつ合理的である場合にのみ，実務的な時間間隔でただちに，当該情報を破棄し，又は非識別化（de-identify）しなければならない。

⑥ APP5 収集通知

対象者は，個人情報を収集する前に，又は，収集後，実務的な時間感覚でただちに，対象者の素性及び詳細な連絡先（APP5.2(a)）等を通知しなければならない（APP5.1）。通知事項は多岐にわたるが，収集目的（APP5.2(d)），第三者から受領した事実（APP5.2(b)(i)），不服申立ての手続（APP5.2(h)）の他，海外の第三者に個人情報を開示するかどうか（APP5.2(i)），当該第三者の所在国（APP5.2(j)）が含まれていることが特徴である。

⑦ APP6 利用又は開示

APP6 は NPP2 を承継しており，個人情報は特定の目的（一次的目的）にしか用いることは出来ず，その他の目的（二次的目的）には利用できないのが原則である。APP6 は，NPP2.1 が定めていた例外事由を拡大している。例えば，行方不明者捜索の援助，法的紛争のための利用，秘密の保持された ADR のための利用などが含まれるとされる（APP6.2(c)の解釈か）。

⑧ APP7 ダイレクトマーケティング

APP7 は，ダイレクトマーケティング目的の個人情報の利用及び開示について規制している。一般的に，ダイレクトマーケティング目的に個人情報を利用するためには，本人の同意が必要であり，オプトアウトの仕組みが採用されていなければならない（APP7.3）。

2003 年スパム法（Spam Act 2003）や 2006 年架電拒否登録法（Do Not Call Register Act 2006）の適用がある場合には，本条の適用はない。

⑨ APP8 越境開示

APP8 及び新 16C 条は，越境開示[451]にアカウンタビリティの手法を導入している。この手法は，NPP9 における越境データ移転の手法とは異なる。

対象者は，海外の第三者に個人情報を開示する前に，当該情報について，海外の第三者が APP（但し APP1 を除く）に違反しないように，合理的な措置を採らなければならない APP8.1）。例外事由が複数定められており，同意があれば APP8 が適用されないことを明示した上でなされた本人の同意がある場合（APP8.2(b)）や，越境開示がオーストラリア法又は裁判所等の命令で要求され，又は承認されている場合（APP8.2(c)）などが挙げられる。

この改正の内容は，欧州委員会第 29 条作業部会に指摘された事項にそのまま従ったものとはいえず，オーストラリアの改正の方向性が，必ずしも欧州の十分性認定を第一義としていな

---

[450] この点，生体情報は生体テンプレート（いわゆる特徴点情報等）よりも当然に情報量が多いのであり，生体テンプレートが目的にかかわらず機微情報に含まれ，生体情報に目的による制限があるのは，直感には反するように思われる。

[451] 開示（Disclose）には，単なる国外のクラウド上でのデータの取り扱いを含まない（OAIC インタビュー）。

いことの証左であるようにも思われる[452]。

⑩　APP9　政府関連識別子の採用，利用又は開示

APP9 は，民間事業者に対し，原則として，政府関連識別子（6 条）を自らの識別子として採用し，利用し又は開示してはならないとしている。

これは，我が国のマイナンバー法（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）がマイナンバー（個人番号）の利用を厳格に法定し（マイナンバー法 9 条），民間事業者の事業への利用を禁止していることと同様の配慮によるものと考えられる。

⑪　APP10　正確性

APP10 は，対象者に対して，収集，利用又は開示する（利用又は開示する場合は目的に照らし）個人情報が正確，最新，かつ完全なものであるように，合理的な措置を踏むことを義務付けている（APP10.1 及び 10.2）。APP10.2 は NPP3 からの変更がみられる。

⑫　APP11　安全管理

APP11 は，対象者に対し，個人情報の誤用，障害及び消失（APP11.1(a)）又は不正アクセス，不正変更，不正開示（APP11.1(b)）を防ぐべく，状況に応じ，合理的な措置を採ることを義務付けている。「障害」は新たに導入された概念である。

また，破棄又は非識別化（de-identify）についても，一定の場合にこれを義務付けている（APP11.2）。

⑬　APP12　開示

対象者は，本人の個人情報を保有している場合，請求に応じて，情報を本人に開示しなければならない（APP12.1）。公的機関は 30 日以内に，民間事業者は合理的な期間内に，対応しなければならず（APP12.4(a)），個人からの請求に対して開示することが合理的で実務的である場合には，情報を開示しなければならない（APP12.4(b)）。開示を拒絶する場合，書面による理由の通知が必要であり，当該通知には不服申立ての手続が記載されなければならない（APP12.9）。公的機関は開示手数料を徴収してはならず，民間事業者が徴収する場合も，過剰であってはならない。また，開示の手数料でなければならず，開示請求の手数料であってはならない（APP12.7 及び 12.8）。

⑭　APP13　訂正

APP13 は，NPP6 が，「情報が不正確，不完全，又は最新でなく，訂正されるべきこと」を要件としていたことを改め，保有目的との関係で，正確で，最新で，完全で，関連し，誤解を招かないように，個人情報が訂正されるための合理的な措置を備えなければならないとした。そして，そのための要件として，保有している情報が，保有目的との関係で，不正確等，問題がある場合か，又は，本人から情報の訂正請求があった場合が定められた（APP13.1）。

イ　執行力の強化

2012 年プライバシー改正法は，コミッショナー（連邦情報コミッショナー）の権限を大幅に強化した。強化された権限の内容としては，①履行評価，②行動規範制定権限，③自主判断調査への判断としての裁決，④執行可能な約束，⑤民事罰命令などが挙げられる。

①　履行評価（performance assessments）

---

[452] 他にも，小企業の除外規定は十分性認定のための問題であることは政府において理解されているが，現時点では，これを適用除外規定から外す予定はないとされていることなども挙げられる。Minihan 氏インタビュー，OAIC インタビュー。

コミッショナーは，個人情報の取扱が，APPs，新たな信用情報に関する条項及びその他の規則又は行動規範に従っているかどうか，APP 対象者について履行評価（performance assessments）を行えるようになった（33C 条）。以前は，連邦行政機関，税ファイルナンバーの受領者，信用情報機関及びクレジットプロバイダーにのみ監査を行うことが出来たが，この権現をあらゆる行政機関と民間事業者に広げたものである。

この監査権限は民間事業者の反響が大きいようだが，今回の権限強化にともなって，連邦情報コミッショナー事務局の人員的増強はなされておらず，80 人程度の人員で広大なオーストラリア全土をカバーすることを考えると，実務的には限界がある[453]。

② 行動規範制定権限

コミッショナーは，より強化された，行動規範制定権限（ⅢB 編 26A 条～26W 条）が与えられた。これは，民間事業者において作り上げた行動規範を，承認・登録して，執行可能なものとするという権限である。行動規範の制度については後述。

③ 自主判断調査への判断としての裁決

コミッショナーが自主判断調査（Own Motion Investigation，”OMI”，40 条(2)）を行った結果，必要があれば，裁定（determination[454]）が行えるようになった（52 条(1A)）。

④ 執行可能な約束（undertakings）

対象者が，コミッショナーに対して約束（undertakings）を提出し，これをコミッショナーが承認した場合，その約束は執行可能（enforceable）とすることができる（33E，33F 条）。コミッショナーは undertakings の執行のために裁判所での手続を行うことが出来，その場合，裁判所は約束の遵守命令その他の適当な命令を出すことができる（33F 条(2)）。この約束は，監査の結果として提出されることをも意図されているようであり，月に 1 件の監査が行われ，その結果，2 件に 1 件が約束に至るとすれば，年間 6 件程度，という見解も示されている[455]。

オーストラリアでは，連邦証券投資委員会（Australian Securities & Investments Commission）にも，執行可能な約束（undertakings）を受け付ける制度が存在し，既に 100 以上の undertakings が登録されている[456]（2014 年 3 月現在）。

⑤ 民事罰命令

コミッショナーは連邦裁判所又は連邦巡回控訴裁判所に対し，民事罰命令（civil penalty order）を求めることができる（民事罰命令につきⅥB 編 80U 条～80ZC 条）。この命令による民事罰の上限は，対象が個人の場合は 34 万豪ドル（1 豪ドル＝95 円換算で 3,230 万円），対象が法人の場合は 170 万豪ドル（同，1 億 6,150 万円）である。

ウ 信用情報法の改正

信用状況報告に関する新たな規制が加わっている。より包括的な信用状況報告が導入され，単純化されたが，強化された収集及び異議申立ての手続きが加わった。また，一部の信用状況

---

453 OAIC インタビュー。

454 これにより侵害行為を行ってはならない等の宣言（declaration）を出すことができるが，determination 自身には法的拘束力がなく，強制的な履行にはなお裁判上の手続を行う必要がある（2011 年調査 154 頁）。

455 OAIC インタビュー。

456 Australian Securities & Investments Commission, “About the enforceable undertakings register”, https://www.asic.gov.au/asic/asic.nsf/byheadline/Enforceable+Undertakings+Register?openDocument

報告に関する条項違反には，民事罰が導入された。クレジットプロバイダーは外部の紛争解決枠組への参加が義務付けられ，更に，オーストラリア消費者クレジット協会（Australian Retail Credit Association）によって制定された信用状況報告に関する行動規範（CR コード）の遵守も求められる。CR コードは後述する執行可能な行動規範の一種であり，2014 年 3 月 12 日付で行動規範として連邦情報コミッショナー事務局の行動規範登録を受けている。

エ　行動規範（Codes）

2012 年プライバシー改正法は，情報プライバシーに関する行動規範（APP コード,26A 条～26K 条）及び信用状況報告に関する行動規範（CR コード，26L 条～26T 条）について，公共の利害に関するような場合には，行動規範登録を受け付け，拘束力を持たせることが可能とした。事業者団体等において行動規範を制定するためのガイドライン[457]も公表している。行動規範は，APPs に取って代わるものではないが，ある産業，領域又はある技術につき，どのように APPs が適用されるかについてより具体的に定めたものである[458]。

なお，約束（undertakings）と行動規範については，いずれも，登録された後，執行可能になるという点で共通する点が見いだせるが，約束が，個別の事業者等により登録されるものであるのに対し，行動規範は，事業者団体等によって登録されるものであるという違いがある。

(5)　2013 年プライバシー改正（プライバシー警告）法案[459]

2013 年 5 月 29 日，2013 年プライバシー改正（プライバシー警告）法案（the Privacy Amendment (Privacy Alerts) Bill 2013[460]）が，連邦下院に提出され，2013 年 6 月 18 日には，連邦上院が法務憲法問題委員会に調査と報告を求めた。この法案は，規制対象者に対して，深刻なデータ侵害が発生した場合に，連邦情報コミッショナー及び，データの本人に対する通知を義務付けるものである。

連邦情報コミッショナー事務局は，調査に対して，データ侵害通知の義務化に対して強くこれを支持する旨のコメントをし，現在の任意ベースでの侵害通知では報告は低調であり，義務付けた場合の利益を述べた。この利益には，データの本人における潜在的な被害の減少とともに，被害を引き起こした対象者の公的な信頼の再構築の助けになること，データ侵害に要するコストの減少が含まれる。連邦上院法務憲法問題委員会は，上院に対して，本法案を採択相当としている。

(6)　医療の電子化（eHealth）[461]

連邦政府は，2010 年 5 月に，個人がコントロール可能な電子医療記録（eHealth）システムに対する財政的支援を導入した。このシステムは，登録した消費者と，登録した医療関係事業者の間で，医療情報の安全な共有を可能にする予定である。消費者は，誰が eHealth 記録にアクセスするかを，コントロールすることができる。

2012-13 会計年度は，2012 年個人コントロール電子医療記録法（the Personally Controlled Electronic Health Records Act 2012(PCEHR Act)）が運用を開始した最初の年であり，年度終わりまでに，40 万人が eHealth 記録のための登録を行った。医療情報の特別なセンシティブさから，PCEHR 法及び，2010 年医療識別子法（the Health Identifiers Act 2010(HI Act)）にお

---

457 Office of Australian Information Commissioner, *Guidelines for developing codes Issued under Part IIIB of the Privacy Act 1988*

458 2012 年年次報告書 49 頁。

459 2012 年年次報告書 50 頁。

460 Perliament of Australia, “Privacy Amendment (Privacy Alerts) Bill 2013”, http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r5059

461 2012 年年次報告書 49 頁。

いては，個人医療情報の収集，利用及び開示について，保護及び規制する条項を備えている。連邦情報コミッショナー事務局はこれらの条項の遵守状況につき監督し，eHealth システムのプライバシーの側面について独立して規制している。連邦情報コミッショナー事務局の eHealth に関する活動は，健康高齢化省（the Department of Health and Ageing）との間の覚書（Memorandum of Understanding, MOU）に基いて行われているが，現在の覚書の有効期限は 2014 年 6 月 30 日である。この覚書により，連邦情報コミッショナー事務局は，監視活動に関して，健康高齢化省より，517,925 豪ドル（医療識別子の監視）及び 1,305,653 豪ドル（eHealth システムの監視）をそれぞれ受領している[462]。

以上

[462] 2012 年年次報告書 197 頁。このような監視業務の対価としての金銭の受領は，他の行政機関（オーストラリア首都特別地域法務地域安全省，Centerlink，連邦税関，人事省，産業・イノベーション・気候変動・科学・研究・第三期教育省，財務・規制緩和省）との間にも行われている。同 196-197 頁。

あとがき

本稿は、「はじめに」で示したように、今日、わが国として常に最新の情報を得ておくべき個人情報保護の枠組みに関する国際的な取組み等について、EU データ保護改革、欧州評議会条約第 108 号及びその現代化提案、OECD 改正ガイドライン、国際的な動きに対する対応例としての米国のプライバシー保護法制の最新動向及びオーストラリアにおける状況、を対象とする調査研究の成果を取りまとめたものである。各章の記述は、できる限り最新の情報を取り込む、具体的かつ客観的な分析を心がけるという方向で統一されている。

今回の調査の概要はこれまた冒頭で要約したところであるので、以下、各章について簡単にではあるがわが国として承知しておくべき背景事情などを補充して本報告書のまとめとしておきたい。なお、本報告書では、今後の議論の基礎的情報を提供することを目的として、EU データ保護規則案、欧州評議会条約第 108 号及び欧州評議会追加議定書、米国プライバシー権利章典の邦訳を掲げてあることも付記しておきたい。

EU では、1995 年のデータ保護指令に代わり、2012 年冒頭、一般データ保護規則提案が示され、新たな枠組策定も大詰めを迎えているところであるが、これについては以下のような点に留意する必要があると思われる。第一に、指令（構成各国で国内法化する）から規則（構成国に直接適用される）へという動きは、これまでの各国における法の実効性、執行の不統一性に対する問題意識の反映であり、EU は個人情報保護の分野における法の実効性をこれまで以上に重視するであろうということである。第二に、95 年指令からの主な変更点（個人情報の範囲、適用範囲、データ主体の権利、事業者の義務、越境データ移転、監督機関）は、構成各国の利害関係の調整の産物（理論的に割り切れたものであるとは限らないということ）である（また、米国の働きかけとの妥協がないわけではない）。しかしながら、個人情報保護の問題は人権レベルの問題であるという基軸があり、利害対立を超えて妥協がなされるという点に注目すべきである。第三に、治安に係る個人情報保護の問題について、刑事データ保護指令提案が示されている（こちらは指令である）という点にも、その内容とともに注目しておく必要があろう。

1981 年の「個人データの自動処理に係る個人の保護に関する条約」（欧州評議会条約第 108 号）については、デジタル分野におけるプライバシー保護を念頭において、条約の現代化作業がなされている。指摘すべきは、第一に、この条約の枠組みは法的拘束力あるもので、この法的拘束性が他の国際文書とは違った可能性を秘めているという点である。わが国としても EU との関係を考えるに際し念頭におくべき点であろう。第二に、この条約には EU 構成国以外の国も多く加盟しているという事実がある。第一及び第二との関連で、第三に、1995 年の EU データ保護指令は EU 法の世界法化（世界標準化）の文脈で語られることがあるが、この条約も EU 法の世界法化と関連付けて語ることができるように思われる（グローバルなプライバシー基準としての条約第 108 号）。第四に、その場合、この条約は個人情報保護において OECD ガイドラインよりも厳しい枠組みであるという点―それゆえにこそ EU 諸国がこれまでこの条約を OECD(ガイドラインよりも重視してきた―に注意する必要がある。

1980 年の OECD ガイドラインについて言えば、2013 年に 33 年ぶりの改正が OECD 理事会で承認されている（国家的なプライバシー戦略、プライバシーマネジメントプログラム、データセキュリティ侵害通知、説明責任を果たす組織及び強化されたプライバシー執行等が新規）。このガイドラインは、周知のように、わが国の個人情報保護法制の歴史の一頁となっているものであり、わが国では、EU 諸国以上に、大変に著名なものである。OECD ガイドラインを語る場合には、情報の自由な流通を考慮することが当初からの目的であること、流通を阻害する障害を早期に除くこと課題としていること、そして自主規制による緩やかな規律を旨とするも

のであることを確認しておく必要があろう。

なお，以上の EU データ保護指令から一般データ保護規則への改正提案，欧州評議会第 108 条約の現代化提案，OECD ガイドラインの改正などは、次に触れる米国における消費者プライバシー権利章典の議論とともに、経済のグローバル化、急速な ICT 技術の進展の中で、お互いの作業を睨みつつ、ある場合には連携して検討作業が進められている点も特記すべき点であろう。

さて、米国の動向であるが、第一に、プライバシー権利章典に関しては、ICT 社会における消費者保護問題についての、オバマ政権による EU への一定の回答であるということが許されよう。利用者（事業者）の責任をより厳しく問う枠組みになっているが、米国の最新の動向として収集、利用、保存という各プロセスを重視する方向がみられ、それは EU 的なアプローチへの接近とも解釈できるという点が興味深いと言える。第二に、EU・米国間の個人データの移転に関するセーフハーバー協定については、プリズム問題を契機として EU 議会などからその廃止を含む強硬な意見が出て、その見直しがなされる予定と報じられているが、この協定は EU と米国の間での「経済交渉」としての側面を有しているという点を看過してはならないと思われる。第三に、米国には EU のような個人情報保護の監督機関はなく、主に FTC が一定の枠内で問題を処理しており、今後 FTC の権限を強化することが提案されている（業界の自主ルールを審査する権限の付与など）。この点については、FTC は、もともと情報の流通を促すという目的で個人情報を保護する施策を考える組織であるという点にも留意が必要であろう。

オーストラリアは、EU（29 条作業部会）から EU 指令 25 条との関係で個人情報保護のレベルに十分性を欠くという烙印を押された国であり、2012 年にはその後の対応であるプライバシー保護法の改正も実現させている。しかし、国際的取組みの動向については、過敏にあるいは過剰に反応する必要はないという立ち位置をとっているようである。

以上に見てきたように、国際的な取組みとそれに対する反応は実に様々である。現在、わが国でも個人情報保護法制の改正作業が行われているところであるが、徒に法解釈の技術的な側面からのみ法制を考えるのではなく、利害調整を経て守るべきものは何か、EU・米国・アジア諸国との制度的調和をどのレベルで求めるか、実際に実務が動くか、一般法（オールジャパンの法）と個別法の切り分けは不可能か、という観点から議論することが肝要であろう。

資料 1：EU データ保護規則案（和訳）

欧州議会市民的自由・司法・内務委員会採決版[463]
2013 年 10 月 22 日

個人データ処理に関す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欧州理事会規則（一般データ保護規則）

（欧州経済地域と関連性のある文面）

欧州議会及び欧州連合理事会は、

欧州連合の機能に関する条約並びにとりわけその第 16 条(2)及び第 114 条(1)に関して、

欧州委員会からの提案に関して、立法機関制定法の草案を各国議会に伝達後に、

かつ欧州経済社会評議会の意見に関して、欧州データ保護監視官局への諮問後に、

通常の立法手続きに基づく行為により、

本規則を採択した。

第 1 章
一般条項

第 1 条　目的

1. 本規則は、個人データ処理に関する個人の保護に関連したルール及び個人データの自由な移動に関連したルールを定めたものである。

2. 本規則は、自然人の基本的人権と自由、とりわけ自然人の個人データ保護の権利を保護するものである。

3. 連合内における個人データの自由な移動は、個人データ処理に関する個人の保護と関係する理由により制約も禁止もされないものとする。

第 2 条　範囲

1. 本規則は、処理方法に関わりなく自動化手段による個人データの全部又は一部の処理、並びにファイリングシステムの一部を形成するか、ファイリングシステムの一部を形成するこ

463 本報告書で和訳された欧州議会市民的自由・司法・内務委員会採決版は、2014 年 3 月 12 日に欧州議会本会議において可決されている。

とを意図している個人データの自動化手段以外による処理に適用される。

2. 本規則は、以下の個人データ処理には適用されない。

(a) 連合法の範囲外である活動の過程におけるもの。

(b) （削除）

(c) 欧州連合条約第 5 編第 2 章の範囲内である活動の遂行時において、加盟国によるもの。

(d) 専ら個人的又は世帯の活動の過程において、自然人によるもの。この適用除外は、限定数の者のみによるアクセスを合理的に予想しうる個人データの公表にも適用されるものとする。

(e) 刑事犯罪の防止、調査、発見、若しくは起訴、又は刑事処分の執行の目的において、所轄公官庁によるもの。

3. 本規則は、2000/31/EC 指令、とりわけ当該指令第 12 条から第 15 条にある仲介業者の法的責任ルールの適用を損なわないものとする。

第3 条 地理的範囲

1. 本規則は、処理を行うのが連合内であるか連合外であるかを問わず、連合におけるコントローラ又はプロセッサの拠点による活動との関連で個人データ処理に適用される。

2. 本規則は、処理活動が以下と関連する場合、連合内に設置されないコントローラ又はプロセッサによる連合におけるデータ主体の個人データ処理に適用される。

(a) データ主体に支払いを要するか否かに関わりなく、連合における当該データ主体への物品又は役務の提供。

(b) 当該データ主体の監視。

3. 本規則は、連合内に設置されないが国際公法に基づき加盟国の国内法が適用される場所に設置されたコントローラによる個人データ処理に適用される。

*第4条　**定義***

本規則の目的上、

(1)　　（削除）

(2)　　「個人データ」とは、識別済み又は識別可能な自然人と関連したあらゆる情報（「データ主体」）を意味し、識別可能な者とは、直接又は間接的に識別できる者、とりわけ、名称、識別番号、所在地データ、一意の識別名といった識別手段への参照、或いは当該者の身体的、生理学的、遺伝学的、精神的、経済的、文化的、若しくは社会的な識別又は性別認識に固有の1つ以上の要素の参照により識別できる者のことをいう。

(2a)　「仮名データ」とは、追加の情報を別個に保持し、かつ非帰属性を確保するための技術的及び組織上の措置を前提としている限り、当該追加の情報を使用しなければ特定のデータ主体に帰属しえない個人データを意味する。

(2b)　「暗号化データ」とは、技術的な保護措置を通じてそのアクセス許可のないいかなる者にとっても理解不能となった個人データを意味する。

(3)　　「処理」とは、収集、記録、組織化、構造化、保存、適応若しくは修正、検索、参照、使用、伝送による公表、伝達若しくは別途利用提供、整列若しくは結合、削除又は破壊など、自動化手段によるか否かを問わず、個人データ又は一連の個人データに対して遂行する業務又は一連の業務を意味する。

(3a)　「プロファイリング」とは、自然人と関連した一定の個人的側面の審査、又はとりわけ当該自然人の職場実績、経済的状況、所在地、健康、個人的嗜好、信頼性、若しくは行動の分析又は予測を意図したあらゆる形態による個人データの自動化処理を意味する。

(4)　　「ファイリングシステム」とは、機能別又は地理別に一元化、分散化、又は分布化してあるか否かを問わず、特定の基準に基づきアクセス可能である構造化された一連の個人データを意味する。

(5)　　「コントローラ」とは、単独又は他者との共同により個人データ処理の目的と手段を決定する自然人若しくは法人、公的機関、政府機関、又はその他の団体を意味し、連合法又は加盟国法で処理の目的と手段を決定する場合、コントローラ又はコントローラ任命の特定の基準を連合法又は加盟国法で指定できる。

(6)　「プロセッサ」とは、コントローラに代わって個人データを処理する自然人若しくは法人、公的機関、政府機関、又はその他の団体を意味する。

(7)　「受領者」とは、個人データの公表先となる自然人若しくは法人、公的機関、政府機関、又はその他の団体を意味する。

(7a)　「第三者」とは、データ主体、コントローラ、プロセッサ、及びコントローラ若しくはプロセッサの直接的権限の下でデータの処理を許可された者以外の自然人若しくは法人、公的機関、政府機関、又はその他の団体を意味する。

(8)　「データ主体の同意」とは、具体的、明示的、及び通知されたその者の自由に行った意思表示を意味し、データ主体はこの意思表示により、当該データ主体と関連した個人データの処理に同意したことを発言又は明白な肯定的行動によって相手に伝える。

(9)　「個人データ侵害」とは、伝送、保存、又は別途処理された個人データの偶発的又は不法な破壊、喪失、修正、不正公表、又はアクセスを意味する。

(10)　「遺伝子データ」とは、対象となる個人からの生体試料の分析結果、とりわけ染色体、デオキシリボ核酸（DNA）、若しくはリボ核酸（RNA）の分析により、又は同等の情報の入手を可能にするその他の要素の分析により、継承したか取得したと判明したかかる個人の遺伝的特性と関連した全ての個人データを意味する。

(11)　「生体データ」とは、顔画像といった個人の一意の識別を可能にする当該個人の身体的、生理学的、又は行動学的な特性と関連したあらゆる個人データ、又は指紋鑑定データを意味する。

(12)　「健康に関するデータ」とは、個人の身体的又は精神的な健康と関連したあらゆる個人データ、又は当該個人への医療役務の提供を意味する。

(13)　「主たる拠点」とは、コントローラであるかプロセッサであるかを問わず、連合における事業又は事業グループの拠点がある場所を意味し、個人データ処理の目的、状況、及び手段について主要な意思決定を行う場所のことをいう。数ある中で次の客観的基準を検討しうる。コントローラ又はプロセッサの本部所在地、事業グループの構成事業体のうち、マネジメント機能と事務管理責任の面で本規則に定めるルールへの対処と執行に最も適しているものの所在地、効果的かつ実質的なマネジメント活動の行使により、安定的な取り決めを通じてデータ処理を決定する所在地。

(14)　「代表者」とは、コントローラにより明示的に指名され、かつ本規則の下でコントローラの義務に関してコントローラを代表する、連合内に設置された自然人又は法人を意味する。

(15)　「企業」とは、その法的形式を問わず、経済的活動に従事する事業体を意味し、それゆえに、とりわけ経済的活動に定期的に従事する自然人及び法人、共同経営会社、又は協会も含まれる。

(16)　「事業グループ」とは、支配権を有する事業及びその支配下にある事業を意味する。

(17)　「拘束的企業準則」とは、個人データを 1 つ以上の第三国における事業グループ内のコントローラ又はプロセッサに移転するか、一連の移転を行うことを目的に、連合加盟国の領域に設置されたコントローラ又はプロセッサが遵守する個人データ保護ポリシーを意味する。

(18)　「子ども」とは、年齢 18 歳未満のあらゆる人を意味する。

(19)　「監督機関」とは、第 46 条に基づき加盟国の設置した公的機関を意味する。

第 2 章
原則

第5 条　個人データ処理に関する原則

個人データは、以下に従うものとする。

(a)　データ主体との関連で適法、公正、かつ透明な方法により処理する（適法性、公正性、及び透明性）。

(b)　特定的、明確、かつ正当な目的のために収集し、これらの目的に合致しない方法により追加の処理をしない（目的の限定）。

(c)　処理を行う目的との関連で十分かつ関連性があり、必要最小限に限定するとともに、個人データを伴わない情報の処理により目的を果たせない場合にのみ、かつそうである限りにおいてのみ、処理を行うものとする（データの最小化）。

(d)　正確であり、かつ必要な場合に最新に更新して保持するとともに、処理を行う目的に関して不正確な個人データを遅滞なく削除又は訂正するよう、合理的な全ての手段を講じなければならない（正確性）。

(e)　個人データの処理を行う目的に必要な期間を超えずに、データ主体の直接又は間接的な識別を可能にする形態により保存するとともに、専ら歴史上、統計上、若しくは科学的研究のために、又は第 83 条及び第 83 条 a のルール及び条件に基づく公文書保管目的のためにデータを処理する限りにおいて、保存を継続する必要性を査定するために定期的な見直しを遂行し、かつデータのアクセスをこれらの目的に制限するための適切な技術的及び組織上の措置を確立している場合に、より長期間にわたり個人データを保存できる（保存の最小化）。

(ea)　　データ主体による自己の権利の行使を実質的に可能にする方法により処理する（実効性）。

(eb)　　適切な技術的及び組織上の措置を講じたうえ、不正又は不法な処理、及び偶発的な喪失、破壊、若しくは損傷から保護する方法により処理する（完全性）。

(f)　　コントローラの責任と法的責任の下で処理し、コントローラは本規則条文の順守を確保し、かつ順守を証明できるものとする（説明責任）。

第6条　処理の適法性

1.　　個人データの処理は以下の少なくとも1つに該当する場合にのみ、かつその範囲内においてのみ、適法であるものとする。

(a)　　データ主体は1つ以上の特定の目的のために自己の個人データの処理に同意している。

(b)　　データ主体が当事者となっている契約の履行に処理を必要とするか、契約の締結前にデータ主体の要請とともに手段を講じるために処理を必要とする。

(c)　　コントローラが対象となる法的義務の順守に処理を必要とする。

(d)　　データ主体の重大利益を保護するために処理を必要とする。

(e)　　公共の利益のために遂行する業務の履行に処理を必要とするか、コントローラに与えられた職権の行使に処理を必要とする。

(f)　　コントローラの追求する正当な利益の目的上、処理を必要とするか、公表を行う場合に、データの公表先となる第三者による処理を必要とし、コントローラとの関係に基づきデータ主体の合理的な期待を満たしている。但し、個人データの保護を要するデータ主体の利害又は基本的人権と自由が当該利益に優先する場合を除く。これは公的機関がその業務遂行において行う処理には適用されないものとする。

2.　　歴史上、統計上、若しくは科学的研究目的のために必要な個人データの処理は第 83 条で言及された条件とセーフガードを前提に適法であるものとする。

3.　　第 1 項の(c)号及び(e)号で言及された処理の根拠は、以下のいずれかにおいて提供されなければならない。

(a)　　連合法。

(b)　　コントローラが対象となる加盟国の法律。

加盟国法は、公共の利益の目的を満たすか、或いは他人の権利と自由の保護及び個人データ保護権の本質の尊重に必要であり、かつ追求する妥当な目的と均衡が取れていなければならない。本規則の許す限りにおいて、加盟国法は処理の適法性の詳細、とりわけデータコントローラに関するもの、処理の目的及び目的の限定、データの性質及びデータ主体、処理の手段及び手続き、受領者、並びに保存の継続期間を定めることができる。

4.　　（削除）

5.　　（削除）

第7条　同意の条件

1.　　処理が同意に基づく場合、コントローラは特定の目的に向けたデータ主体の個人データ処理に対するデータ主体の同意について立証責任を負うものとする。

2.　　データ主体の同意を別件とも関係する書面による宣言により得る場合、同意付与の要件をその外見上、当該別件から明確に区別できるように提示しなければならない。データ主体の同意に関する条文のうち、本規則に部分的に違反するものは完全に無効である。

3.　　処理のその他の法的根拠にかかわらず、データ主体は自らの同意をいつでも撤回する権利を有するものとする。同意の撤回は、撤回前の同意に基づく処理の適法性に影響しないものとする。同意の撤回は、同意の付与と同等に容易であるものとする。同意の撤回が提供役務の終了又はコントローラとの関係の終了に帰結しうる場合、データ主体はコントローラから通知を受けるものとする。

4.　　同意は目的限定とし、目的がもはや存在しないときに、又は個人データを当初収集した目的の遂行に個人データの処理がもはや必要でなくなり次第、その有効性を失うものとする。契約の締結又は役務の提供は、第 6 条(1)の(b)号に従い、契約の締結又は役務の提供に必要でないデータの処理への同意を条件としないものとする。

第8条　子どもの個人データ処理

1.　本規則の目的上、子どもへの直接の物品又は役務提供との関連で、年齢 13 歳未満の子どもの個人データ処理は子どもの親又は法的保護者が同意するか許可する場合にのみ、かつその範囲内においてのみ、適法であるものとする。コントローラは利用可能な技術を考慮に入れつつ、その他の不必要な個人データ処理を招くことなく、当該同意を確認するために合理的な努力を払うものとする。

1a.　同意の表明のために子ども、親、及び法的保護者に提供する情報は、コントローラによる個人データの収集と使用に関するものも含め、意図された対象者に適した明確な言葉により提供すべきである。

2.　第 1 項は、子どもと関連した契約の有効性、形成、又は効力に関するルールといった加盟国の一般契約法に影響を及ぼさないものとする。

3.　欧州データ保護役員会は第 66 条に従い、第 1 項で言及された同意を確認する方法の指針、勧告、及びベストプラクティスを発行する業務を付託されるものとする。

4.　（削除）

第9条　データの特殊分類

1.　人種若しくは種族的出身、政治的見解、宗教若しくは哲学的信念、性的指向若しくは性別認識、労働組合の加入及び活動を判明させる個人データの処理、並びに遺伝子データ若しくは生体データ又は健康若しくは性生活、行政的制裁、裁判判決、刑事犯罪若しくは犯罪容疑、有罪判決、或いは関連セキュリティ措置に関するデータの処理は禁止されるものとする。

2.　第1項は、以下のいずれかに該当する場合に適用されないものとする。

(a)　データ主体は、第7条及び第8条に定められた条件を前提に、1つ以上の特定の目的による個人データの処理に同意している。但し、第1項で言及された禁止事項をデータ主体が解禁できないことを連合法又は加盟国法で定めている場合を除く。

(aa)　データ主体が当事者となっている契約の履行又は締結に処理を必要とするか、契約の締結前にデータ主体の要請とともに手段を講じるために処理を必要とする。

(b)　差別を受けない権利といったデータ主体の基本的人権及び利害について十分なセーフガードを定めた連合法若しくは加盟国法又は団体協約により認められる限りにおいて、第82条で言及された条件とセーフガードを前提に、労働法の分野におけるコントローラによる義務の遂行と特定の権利の行使を目的に処理を必要とする。

(c)　データ主体が同意を付与するための身体的能力又は法的能力を有しない場合に、データ主体又は別の者の重大利益を保護するために処理を必要とする。

(d)　政治的、哲学的、宗教的、又は労働組合の狙いを持つ財団、協会、又はその他の非営利団体が、専ら当該大体の構成員若しくは元構成員又は当該団体の目的との関係で当該団体と定期的な連絡のある者と関連した処理であることを条件に、かつデータ主体の同意を得ずに当該団体外にデータを公表しないことを条件に、適切なセーフガードを伴いながらその適法な活動の過程において処理を遂行する。

(e)　データ主体が明白に開示した個人データと関連した処理である。

(f)　法的な主張の立証、行使、又は防御に処理を必要とする。

(g)　　連合法又は加盟国法に基づいて、国民の高い関心事であることを理由に遂行する業務の履行に処理を必要とし、追求する目的と均衡が取れており、データ保護権の本質を尊重し、データ主体の基本的人権と利害を保護するのに適切な措置を提供している。

(h)　　健康の目的上、かつ第 81 条で言及された条件及びセーフガードを前提に、健康に関するデータ処理を必要とする。

(i)　　第 83 条で言及された条件とセーフガードを前提に、歴史上、統計上、若しくは科学的研究目的のために処理を必要とする。

(ia)　　第 83 条 a で言及された条件とセーフガードを前提に、公文書保管役務に処理を必要とする。

(j)　　公的機関の制御下で、又はコントローラが対象となる法的義務若しくは規制上の義務の順守に処理を必要とするときに、或いは重要な公共の利益を理由に遂行する業務の履行にあたって、データ主体の基本的人権及び利害について十分なセーフガードを定めた連合法又は加盟国法により認められる限りにおいて、行政的制裁、裁判判決、刑事犯罪、有罪判決、又は関連セキュリティ措置と関連したデータ処理を遂行する。刑事犯罪の前科は公的機関の制御下においてのみ保持するものとする。

3.　　欧州データ保護役員会は第 66 条に従い、第 1 項で言及された特殊分類個人データを処理するための指針、勧告、及びベストプラクティス、並びに第 2 項に定める適用除外を発行する業務を付託されるものとする。

第 10 条　識別を認めない処理

1.　　コントローラの処理するデータがコントローラ又はプロセッサによる自然人の直接又は間接的な識別を認めないか、仮名データからのみ構成される場合、コントローラは専ら本規則のいずれかの条文の順守を目的にデータ主体を識別するための追加の情報を処理又は取得しないものとする。

2.　　データコントローラが第 1 項を理由に本規則条文を順守できない場合、コントローラは本規則の当該特定の条文について順守義務を負わないものとする。それによりデータコントローラがデータ主体の要請に応じられない場合、その旨をデータ主体に通知するものとする。

第 3 章
データ主体の権利

第 1 節
透明性及び様式

第 10 条 a　データ主体の権利に関する一般原則

1.　　データ保護の基本は、データ主体の明瞭かつ明白な権利であり、これをデータコントローラーは尊重するものとする。本規則の諸条文の狙いは、これらの権利の強化、明確化、保証、及び適切である場合、その成文化にある。

2.　　当該権利にはとりわけ、各人の個人データ処理に関する明確かつ理解しやすい情報の提供、自己のデータをアクセス、訂正、削除する権利、データを取得する権利、プロファイリングに異議を呈する権利、所轄データ保護機関に苦情を呈し、法的手続きを起こす権利、並びに不法な処理業務に起因して補償と損害賠償を受ける権利が含まれる。当該権利は一般に、無償で行使するものとする。データコントローラは、データ主体からの要請に合理的な期間内に対応するものとする。

第 11 条　透明性ある情報及びコミュニケーション

1.　　コントローラは個人データの処理に関して、かつデータ主体の権利行使のために、簡潔、透明、明確、かつ容易にアクセス可能なポリシーを確立するものとする。

2.　　コントローラは個人データの処理と関連したあらゆる情報及びあらゆるコミュニケーション、とりわけ子どもを特定的に対象としたあらゆる情報について、明確かつ平易な言葉を用いた理解可能な形態によりデータ主体に提供するものとする。

第 12 条　データ主体の権利行使のための手続き及び仕組み

1.　　個人データを自動化手段により処理する場合、コントローラは可能であれば電子的に要請を行う手段をも提供するものとする。

2. コントローラは第13条及び第15条から第19条に従い何らかの行動が講じられたか否かを、不当な遅滞なく、かつ要請の受領から遅くとも 40 暦日以内に、データ主体に通知するものとし、要請のあった情報を提供するものとする。複数のデータ主体がその権利を行使し、コントローラ側で不必要かつ不相応な努力を払うことを防止するために、当該データ主体による合理的な水準の協力を必要とする場合、この期間を更に1ヶ月間延長できる。当該情報は書面により付与するものとし、可能であれば、データコントローラは、データ主体の個人データへの直接アクセスをデータ主体に提供する安全なシステムへの遠隔アクセスを提供できる。データ主体が電子的形態により要請を行った場合、データ主体から別段の要請がない限り、可能であれば電子的形態により情報を提供するものとする。

3. コントローラがデータ主体の要請に基づき行動を講じない場合、コントローラは行動を講じない理由と、監督機関に苦情を呈し、司法的救済を求める可能性について、データ主体に通知するものとする。

4. 第1項で言及された要請に基づく情報と行動は無償とする。要請が明らかに過剰である場合、とりわけその反復的な特徴から明らかに過剰である場合、コントローラは情報提供又は要請に基づく行動の事務管理費用を考慮に入れつつ、合理的な手数料を課すことができる。この場合、コントローラは、要請の明らかに過剰な特徴の立証責任を負うものとする。

5. （削除）

6. （削除）

第13条　訂正及び削除の場合の通知要件

コントローラは、第16条及び第17条に従い遂行したあらゆる訂正又は削除について、その伝達が結果的に不可能でない限り、又は不相応の努力を伴わない限り、データ移転先の各受領者に伝達するものとする。データ主体から要請があった場合、コントローラは当該受領者についてデータ主体に通知するものとする。

第13条a　標準化された情報ポリシー

1. データ主体と関連した個人データを収集する場合、コントローラは、第 14 条に従い情報を提供する前に、以下の詳細をデータ主体に提供するものとする。

(a) 個々の特定の処理目的に必要な最小限度を超えて個人データを収集するのかの有無。

(b) 個々の特定の処理目的に必要な最小限度を超えて個人データを留保するのかの有無。

(c) 収集目的とは異なる目的に個人データを処理するのかの有無。

(d) 商業第三者に個人データを配布するのかの有無。

(e) 個人データを売却又は賃貸するのかの有無。

(f) 個人データを暗号化形式により留保するのかの有無。

2. 第 1 項で言及された詳細は、別添 X に従い、以下の 3 つの欄に文字列と記号を用いた整列表形式により、提示するものとする。

(a) 第 1 欄に当該詳細を象徴する図形を表示する。

(b) 第 2 欄に当該詳細を説明した不可欠情報を含める。

(c) 第 3 欄に特定の詳細を満たしたか否かを示す図形を表示する。

3. 第 1 項及び第 2 項で言及された情報は、見やすく明確に判読可能な方法により提示するものとし、情報の提供先となる加盟国の消費者が理解しやすい言葉で表示するものとする。詳細を電子的に提示する場合、機械可読であるものとする。

4. 追加の詳細は提供しないものとする。第 1 項で言及された詳細に関する詳細な説明又は追加の備考は、第 14 条に従いその他の情報要件とともに提供できる。

5. 欧州委員会は欧州データ保護役員会の意見を要請後、第 1 項で言及された詳細と第 2 項及び別添 1 で言及されたその提示を更に具体化させることを目的に、第 86 条に基づき委任法令を採択する権限を与えられるものとする。

第 2 節
データについての情報及びそのアクセス

第 14 条　データ主体に対する情報

1.　　データ主体と関連した個人情報を収集する場合、コントローラは第 13 条 a に基づく詳細を提供後に、少なくとも以下の情報をデータ主体に提供するものとする。

(a)　　コントローラの身元情報と連絡先詳細、及び該当する場合にはコントローラの代表者とデータ保護官の身元情報と連絡先詳細。

(b)　　個人データの意図された処理目的、及び個人データ処理のセキュリティに関する情報。第 6 条(1)の(b)号に基づく処理の場合には契約条件と一般的条件も含まれ、該当する場合、第 6 条(1)の(f)号にある要件の実施方法と充足方法に関する情報も含まれる。

(c)　　個人データの保存を行う期間、又はこれが可能でない場合、当該期間の決定に用いる基準。

(d)　　コントローラにデータ主体に関する個人データのアクセス及び訂正又は削除を要請する権利、当該個人データの処理に異議を呈する権利、又はデータを取得する権利の存在。

(e)　　監督機関に苦情を呈する権利、及び監督機関の連絡先詳細。

(f)　　個人データの受領者又は受領者の属性。

(g)　　該当する場合、データを第三国又は国際機関に移転するコントローラの意向、並びに欧州委員会による十分性認定が存在するか不在である場合、或いは第 42 条、第 43 条、又は第 44 条(1)の(h)号で言及された移転の場合、適切なセーフガードとその複製物を取得する手段への言及。

(ga)　　該当する場合、プロファイリングの存在、プロファイリングに基づく措置、及びデータ主体に対するプロファイリングから想定される効果についての情報。

(gb)　　自動化処理に伴う論理についての有意義な情報。

(h)　個人データの収集又は処理における特定の状況、とりわけ個人データの影響評価から高リスクの存在の可能性が示唆される一定の処理活動と業務の存在を考慮のうえ、データ主体に関して公正な処理を保証するのに必要な更なる情報。

(ha)　該当する場合、連続する過去 12 ヶ月間に個人データを公的機関に提供したか否かの情報。

2.　個人データをデータ主体から収集する場合、コントローラは第 1 項で言及された情報に加え、個人データの提供が必須であるか任意であるかの有無、及び当該データの不提供から考えうる帰結をデータ主体に通知するものとする。

2a.　1(h)の下で、公正な処理に必要な追加の情報を決定するにあたって、コントローラは第 38 条の下でのあらゆる関係指針を考慮するものとする。

3.　個人データをデータ主体から収集していない場合、コントローラは第 1 項で言及された情報に加え、特定の個人データの出所をデータ主体に通知するものとする。個人データの出所が公的に入手可能な情報源である場合、一般表示を行うことができる。

4.　コントローラは以下のいずれかに従い、第 1 項、第 2 項、及び第 3 項で言及された情報を提供するものとする。
(a)　データ主体からの個人データの入手時、又は上記を実行可能でない場合には不当な遅滞なく、提供する。

(aa)　第 73 条で言及された団体、組織、又は協会からの要請時に提供する。

(b)　個人データをデータ主体から収集していない場合、データ収集又は別途処理の特定の状況を考慮のうえ、記録時又は収集後の合理的な期間内に提供するか、別の受領者への移転を想定している場合、遅くとも最初の移転時に提供する、或いはデータを関係データ主体との伝達に使用する場合、遅くとも当該データ主体への最初の伝達時に提供する。

(bb)　専ら付随的活動として個人データを処理している小企業又は零細企業がデータを処理する場合、その要請があったときに限って提供する。

5.　第 1 項から第 4 項は、以下のいずれかに該当する場合には適用されない。

(a)　データ主体は第 1 項、第 2 項、及び第 3 項で言及された情報を既に入手している。

(b)　第 81 条及び第 83 条で言及された条件とセーフガードを前提に、歴史上、統計上、若しくは科学的研究目的のためにデータを処理し、データ主体から収集を行わず、当該情報の提供が結果的に不可能であるか不相応の努力を伴い、コントローラは誰でも検索できるように当該情報を公表している。

(c)　データをデータ主体から収集せず、その記録又は公表についてコントローラが対象となる法律に明記され、かつデータ主体の正当な利益を保護するための適切な措置を当該法律で定めており、処理によるリスクと個人データの性質を考慮に入れている。

(d)　　データをデータ主体から収集せず、第 21 条に従い、連合法又は加盟国法に定義された他の自然人の権利と自由を当該情報の提供が損なう。

(da)　　データをデータ主体から直接収集する場合を除き、連合法又は加盟国法で規定している職務上の守秘義務又は法定守秘義務の対象者による職務遂行にあたってデータを処理するか、当該対象者に知らせるためにデータを委託する。

6.　　第 5 項の(b)号で言及している場合において、コントローラはデータ主体の権利又は正当な利益を保護するための適切な措置を提供するものとする。

7.　　（削除）

8.　　（削除）

第 15 条　データ主体のデータアクセス権及びデータ取得権

1.　　第 12 条(4)を前提として、データ主体は要請とともに、データ主体と関連した個人データの処理の有無につき、コントローラからいつでも、明確かつ平易な言葉により以下の情報の確認を得る権利を有するものとする。

(a)　　個人データの各分類の処理目的。

(b)　　関係個人データの属性。

(c)　　第三国における受領者も含め、個人データの公表を予定しているかその公表先となった受領者。

(d)　　個人データの保存を行う期間、又はこれが可能でない場合、当該期間の決定に用いる基準。

(e)　　データ主体に関する個人データの訂正又は削除をコントローラに要請する権利、又は当該個人データの処理に異議を呈する権利の存在。

(f)　　監督機関に苦情を呈する権利、及び監督機関の連絡先詳細。

(g)　　（削除）

(h)　　当該処理の重要性と想定される帰結。

(ha)　　自動化処理に伴う論理についての有意義な情報。

(hb)　　第 21 条を損なうことなく、公的機関による要請の結果として個人データを公的機関に公表した場合、当該要請が行われたことの事実確認。

2.　　データ主体はコントローラから、処理中である個人データについてのコミュニケーションを入手する権利を有するものとする。データ主体が電子的形態により要請を行った場合、データ主体から別段の要請がない限り、電子形式かつ構造化形式により情報を提供するものとする。第 10 条を損なうことなく、コントローラはデータのアクセスを要請している者がデータ主体であることを確認するために全て合理的な手段を講じるものとする。

2a.　　個人データを電子的手段により処理する個人データをデータ主体が提供した場合、データ主体はコントローラから、一般的に用いられ、かつ個人データの回収先となるコントローラから妨害を受けずにデータ主体による更なる使用を可能にする電子形式かつ相互運用可能な形式による提供個人データの複製物を入手する権利を有するものとする。技術的に実行可能かつ利用可能である場合、データ主体の要請とともに、データをコントローラ間で直接移転するものとする。

2b.　　本条は、第 5 条(1)(e)の下でもはや必要でなくなったときに、データの削除義務を損なわないものとする。

2c.　　第 14 条(5)(da)の意味の範囲内に入るデータと関係するとき、データ主体に対象となる守秘義務を解く権限が与えられ、それに応じて行動を講じた場合を除き、第 1 項及び第 2 項に従い、アクセス権はないものとする。

3.　　（削除）

4. （削除）

第 3 節
訂正及び削除

第 16 条　訂正権

データ主体は、コントローラから当該データ主体と関連した不正確な個人データの訂正を得る権利を有するものとする。データ主体は、補足の提供による場合も含め、不完全な個人データの完成を得る権利を有するものとする。

第 17 条　削除権

1. 以下の根拠のいずれかに該当する場合、データ主体はコントローラから当該データ主体と関連した個人データの削除及び当該データの更なる配布の自制を得る権利、並びに第三者から当該データへのリンク削除又は当該データの複製若しくは再現を得る権利を有するものとする。

(a) 収集目的又は別途処理目的との関連でデータをもはや必要としない。

(b) データ主体が第 6 条(1)の(a)号に基づく処理への同意を撤回したか、同意した保存期間が満了し、データを処理するその他の法的根拠がない場合。

(c) データ主体は、第 19 条に従い個人データの処理に異議を呈した。

(ca) 連合を拠点とする裁判所又は規制機関が関係データを削除しなければならないという最終かつ絶対的な裁定を下した。

(d) データを不法に処理した。

1a. 第 1 項の適用は、削除を要請する者がデータ主体であるとのデータコントローラの確認能力に依存するものとする。

2. 第 1 項で言及されたコントローラが第 6 条(1)に基づき正当化されない理由により個人データを公にした場合、第 77 条を損なうことなく、コントローラは全て合理的な手段を講じてデータを削除するものとし、これには第三者による削除も含まれる。コントローラは可能であれば、関係第三者の講じた行動についてデータ主体に通知するものとする。

3. コントローラ、及び該当する場合には第三者は、以下のために個人データの留保を必要とする範囲内を除き、削除を遅滞なく遂行するものとする。

(a) 第 80 条に従った表現の自由の権利行使。

(b) 第 81 条に従った公衆衛生の分野における公共の利益の理由。

(c) 第 83 条に従った歴史上、統計上、及び科学的研究目的。

(d) コントローラが対象となる連合法又は加盟国法に基づく個人データを留保する法的義務の順守。加盟国法は公共の利益の目的を満たし、個人データ保護権を尊重し、追求する妥当な目的と均衡が取れているものとする。

(e) 第 4 項で言及されたものに該当する場合。

4. 以下に該当する場合、コントローラは削除の代わりに、通常のデータアクセス及び処理業務の対象とはならず、かつもはや変更できない方法により、個人データの処理を制限するものとする。

(a) その正確性についてデータ主体が異議を呈し、その最中、コントローラによるデータの正確性検証を可能にした。

(b) コントローラは、その業務達成のために個人データをもはや必要としないが、証拠目的にそれを維持しなければならない。

(c) 処理が不法であり、データ主体はその削除への異議とそれに代わる使用制限を要請した。

(ca) 連合を拠点とする裁判所又は規制機関が関係データを制限しなければならないという最終かつ絶対的な裁定を下した。

(d) 第 15 条の第 2a 項に従い、データ主体は個人データを別の自動化処理システムに伝送することを要請した。

(da) 特定種類の保存技術は削除を可能とせず、本規則の発効前にインストールされたものである。

5. 第 4 項で言及された個人データは、保存を除き、証拠目的かデータ主体の同意により、又は別の自然人若しくは法人の権利保護のために、或いは公共の利益の目的のためにのみ処理できる。

6. 個人データの処理が第 4 項に従い制限される場合、コントローラは処理制限の解除前にデータ主体に通知を行うものとする。

7. （削除）

8. 削除を遂行する場合、コントローラは当該個人データを別途処理しないものとする。

8a. コントローラは個人データの削除に設けた期限又はデータ保存の必要性の定期的な見直しに設けた期限を確実に遵守するための仕組みを実施するものとする。

9. 欧州委員会は欧州データ保護役員会の意見を要請後に、以下を更に具体化させることを目的に、第 86 条に基づき委任法令を採択する権限を与えられるものとする。

(a) 特定の部門と特定データ処理を対象とした第 1 項の適用基準及び要件。

(b) 第 2 項で言及された公的に入手可能な通信役務から個人データのリンク、複製物、又は再現物を削除するための条件。

(c) 第 4 項で言及された個人データの処理を制限するための基準及び条件。

第 4 節
拒否権及びプロファイリング

第 19 条 拒否権

1. データ主体の利害又は基本的人権及び自由に優先する処理について説得力ある法的根拠をコントローラが証明しない限り、データ主体は第 6 条(1)の(d)号及び(e)号に基づく個人データの処理をいつでも拒否する権利を有するものとする。

2. 個人データの処理が第 6 条(1)の(f)号に基づく場合、データ主体はいつでも、かつ更なる正当化を要せずに、無償により、全般的に又は特定目的のために、その個人データの処理を拒否する権利を有するものとする。

2a. 第 2 項で言及された権利は、とりわけ子どもを特定的に対象とした場合に、明確かつ平易な言葉を用いた理解可能な方法と形態によりデータ主体に明示的に与えられるものとし、その他の情報から明確に区別できるものとする。

2b. 情報社会役務の使用との関連で、かつ 2002/58/EC 指令にかかわらず、拒否権は、データ主体による自らの明確な意思表示を可能にする技術規格を用いた、自動化手段により行使できる。

3. 第 1 項及び第 2 項に従い拒否を支持した場合、コントローラは拒否決定の目的のために関係個人データをもはや使用又は別途処理しないものとする。

第20 条　プロファイリング

1. 第 6 条の条文を損なうことなく、あらゆる自然人は第 19 条に従いプロファイリングを拒否する権利を有するものとする。データ主体はプロファイリングへの拒否権について、高度に可視的な方法により通知を受けるものとする。

2. 本規則のその他条文を前提に、処理が以下のいずれかに該当する場合に限り、いずれの者も、データ主体に関して法的効果を生む措置に繋がるプロファイリング、又は同様に多大な影響を関係データ主体の利害、権利、若しくは自由に及ぼすプロファイリングの対象となりうる。

(a) データ主体の提出した契約締結又は履行の要請が満たされた場合に、契約の締結又は履行に必要となる。但し、データ主体の正当な利益を守るために適切な措置を提示した場合に限る。

(b) データ主体の正当な利益を守るための適切な措置をも定めている連合法又は加盟国法により明示的に認められる。

(c) 第 7 条に定める条件と適切なセーフガードを前提に、データ主体の同意に基づいている。

3. 人種若しくは種族的出身、政治的見解、宗教若しくは信念、労働組合加入、性的指向若しくは性別認識に基づき個人を差別する効果のあるプロファイリング、又は同様の効果を有する措置に帰結するプロファイリングは禁止されるものとする。コントローラはプロファイリングの結果として考えうる差別に対する効果的な保護を実施するものとする。プロファイリングは第 9 条で言及された特殊分類個人データのみに基づかないものとする。

4. （削除）

5. データ主体に関して法的効果を生む措置に繋がるプロファイリング、又は同様に多大な影響を関係データ主体の利害、権利、若しくは自由に及ぼすプロファイリングは、自動化処理のみに基づかず、かつその大部分が自動化処理に基づかないものとし、人的評価とその評価後に至った意思決定の説明をも含めるものとする。第 2 項で言及されたデータ主体の正当な利益を守るための適切な措置には、人的評価とその評価後に至った意思決定の説明を入手する権利も含まれるものとする。

5a. 欧州データ保護役員会は、第 66 条(1)項(b)に従い、第 2 項に基づくプロファイリングの基準及び条件を更に具体化させるための指針、勧告、及びベストプラクティスを発行する業務を付託されるものとする。

第 5 節
規制

*第 21 条 **規制***

1. 連合法又は加盟国法は、規制が、明確に定義された公共の利益の目的を満たし、個人データ保護権の本質を尊重し、追求する妥当な目的と均衡が取れており、データ主体の基本的人権と利害を尊重し、民主社会において以下を守るために必要かつ均衡の取れた措置であるときに、立法措置の方法により、第 11 条から第 19 条及び第 32 条にある義務及び権利の範囲を規制できる。

(a) 公共の安全。

(b) 刑事犯罪の防止、調査、発見、及び起訴。

(c) 税務。

(d) 規制対象職業倫理の違反の防止、調査、発見、及び起訴。

(e)　　(a)、(b)、(c)、及び(d)で言及されたものに該当する場合、所轄公的機関による行使の枠組みにおける監視上、検査上、又は規制上の機能。

(f)　　データ主体の保護又はその他の者の権利と自由の保護。

2.　　とりわけ、第 1 項で言及された立法措置はいずれも、民主社会において必要かつ均衡の取れたものでなければならず、少なくとも以下について特定の条文を含めるものとする。

(a)　　処理により追求する目的。

(b)　　コントローラの決定。

(c)　　処理の特定の目的と手段。

(d)　　悪用又は不法アクセス若しくは移転を防止するためのセーフガード。

(e)　　規制について通知を受けるデータ主体の権利。

2a.　　第 1 項で言及された立法措置は、当初の目的に厳密に必要とするものに追加してデータを留保することを民間コントローラに許可も義務化もしないものとする。

第 4 章
コントローラ及びプロセッサ

第 1 節
一般的義務

第 22 条　コントローラの責任及び説明責任

1.　　コントローラは、最新技術、個人データ処理の性質、処理の事情、範囲、及び目的、データ主体の権利と自由へのリスク、並びに組織の種類を考慮のうえ、個人データの処理が本規則を順守しつつ遂行されることを確実にし、かつ透明な方法によりそれを証明できるために、処理手段の決定時と処理自体の時期の両方に、適切なポリシーを採択のうえ、適切かつ証明可能な技術的及び組織上の措置を実施するものとする。

1a. コントローラは最新技術と実施費用を考慮のうえ、データ主体の自主的な選択を一貫して尊重する法令順守ポリシー及び手続きを実施するために、全て合理的な手段を講じるものとする。当該法令順守ポリシーは少なくとも 2 年毎に見直しを行い、必要に応じて更新するものとする。

2. （削除）

3. コントローラは、第 1 項及び第 2 項で言及された措置の十分性と有効性を証明できるものとする。公開企業による義務的な報告など、コントローラの活動に関する定期的な一般報告は、第 1 項で言及されたポリシーと措置の概要を含めるものとする。

3a. コントローラは連合内において、事業グループの関係事業分野間で正当な内部事務管理を目的に処理を必要とし、かつデータ保護の十分な水準とデータ主体の利害を内部データ保護規定又はそれに相当する第 38 条で言及された行動原則により守る場合に、コントローラがその一部を構成する事業グループ内で個人データを伝送する権利を有するものとする。

4. （削除）

第 23 条　設計及び初期設定によるデータ保護

1. 最新技術、現行の技術的知識、国際ベストプラクティス、及びデータ処理によるリスクを考慮のうえ、コントローラと該当する場合にはプロセッサは処理手段の決定時と処理自体の時期の両方に、処理が本規則の要件を満たし、かつデータ主体の権利保護、とりわけ第 5 条に定める原則に関するものを確実にする方法により、適切かつ均衡の取れた技術的及び組織上の措置と手続きを実施するものとする。設計によるデータ保護は、収集、処理から削除に至るまで、個人データの正確性、機密性、完全性、物的セキュリティ、及び削除に関する包括的な手続き上のセーフガードに体系的に焦点を当てつつ、個人データの全ライフサイクル管理をとりわけ考慮に入れるものとする。コントローラが第 33 条に従いデータ保護影響評価を遂行するとき、当該措置と手続きの策定時にその結果を考慮に入れるものとする。

1a. 異なる経済部門における設計によるデータ保護の広範な実施を促進するため、公共調達に関する欧州議会及び理事会指令に従い、かつ水道、エネルギー、運輸、郵便サービス分野における機関の調達に関する欧州議会及び理事会指令（公益事業指令）に従い、設計によるデータ保護は公共調達入札の必須条件とする。

2. コントローラは初期設定により、個々の特定の処理目的に必要であり、かつデータ量とその保存時間の双方の面でとりわけ当該目的を必要とする最小限度を超えて収集、留保、又は配布を行わない個人データのみを処理することを確実にするものとする。とりわけ、その仕組みは初期設定により、個人データを無制限数の個人にアクセス可能とせず、かつデータ主体がその個人データの頒布を制御できることを確実にするものとする。

3. （削除）

4. （削除）

第24条　共同コントローラ

複数のコントローラが共同して個人データ処理の目的と手段を決定する場合、共同コントローラは相互の取り決めという手段により、本規則の下での義務を順守する各自の責任、とりわけデータ主体の権利行使の手続きと仕組みに関するものを決定するものとする。取り決めは、データ主体を相手にした共同コントローラの各自の効果的な役割と関係を正当に反映するものとし、取り決めの本質をデータ主体に利用可能にするものとする。責任が不明瞭である場合、コントローラは連帯責任を負うものとする。

第25条　連合内に設置されないコントローラの代表者

1.　第3条(2)で言及された状況において、コントローラは連合における代表者を指名するものとする。

2.　当該義務は、以下のいずれかに該当する場合には適用されないものとする。

(a)　第41条に従い、十分な水準の保護を保証していると欧州委員会が認定した第三国に設置されたコントローラである場合。

(b)　連続するいずれかの12ヶ月間に5,000未満のデータ主体と関連する個人データを処理し、かつ第9条(1)で言及された特殊分類個人データ、所在地データ、又は大規模ファイリングシステムの子ども若しくは従業員に関するデータを処理しないコントローラである場合。

(c)　公的機関又は団体である場合。

(d)　コントローラがごく稀に、物品又は役務を連合におけるデータ主体に提供する場合。但し、個人データの処理が第 9 条(1)で言及された特殊分類個人データ、所在地データ、又は大規模ファイリングシステムの子ども若しくは従業員に関するデータと関係する場合を除く。

3.　データ主体への物品又は役務の提供、又はその監視を行う加盟国のいずれか 1 つに代表者を設置するものとする。

4.　コントローラによる代表者の指名は、コントローラ自身に対して発動されうる法的措置を損なわないものとする。

第 26 条　プロセッサ

1.　コントローラに代わって処理を遂行する場合、処理が本規則の要件を満たし、かつデータ主体の権利保護、とりわけ処理の遂行を準拠させる技術的セキュリティ措置及び組織上の措置に関するものを確実にする方法により、適切な技術的及び組織上の措置と手続きの実施につき十分な保証を提供するプロセッサをコントローラは選定するものとし、コントローラは当該措置の順守を確保するものとする。

2.　プロセッサによる処理の遂行は、プロセッサをコントローラに拘束する契約又はその他の法的行為に準拠するものとする。コントローラとプロセッサは、本規則の要件に関する各自の役割と業務を自由に決定するものとし、プロセッサについて以下を定めるものとする。

(a)　連合法又は加盟国法により別段の義務を課している場合を除き、専らコントローラからの指示を以って個人データを処理する。

(b)　守秘を約束した職員又は法定守秘義務を課された職員のみを雇用する。

(c)　第 30 条に従い、全ての必要な措置を講じる。

(d)　別段の決定を行う場合を除き、コントローラによる事前許可を前提として、別のプロセッサの参加条件を決定する。

(e)　処理の性質を鑑みて可能である限りにおいて、第 3 章に定めるデータ主体の権利行使要請に対応する、コントローラの義務を履行するための適切かつ関連性のある、技術的及び組織上の要件につき、コントローラとの間で合意を形成する。

(f)　処理の性質とプロセッサの利用可能な情報を考慮のうえ、第 30 条から第 34 条に基づく義務の順守を確保するためにコントローラを支援する。

(g)　データの保存を連合法又は加盟国法で義務づけている場合を除き、処理の終了後に全ての結果をコントローラに返却し、個人データを別途処理せず、既存の複製物を削除する。

(h)　本条に定める義務の順守を証明するために必要な全ての情報をコントローラに対して利用可能にし、現場検査を認める。

3. コントローラとプロセッサは、第 2 項で言及されたコントローラの指示とプロセッサの義務を書面により文書化するものとする。

3a. 第 1 項で言及された十分な保証は本規則第 38 条又は第 39 条に従った行動原則の遵守又は認証の仕組みにより証明できる。

4. プロセッサがコントローラの指示したもの以外の個人データを処理したか、データ処理の目的及び手段との関連で決定当事者となった場合、プロセッサは当該処理に関してコントローラであるとみなすものとし、第 24 条に定める共同コントローラに関するルールの対象となるものとする。

5. （削除）

第 27 条　コントローラ及びプロセッサの権限下での処理

プロセッサ、及びコントローラ又はプロセッサの権限の下で行為し、かつ個人データにアクセスできるあらゆる者は、コントローラの指示による場合を除き、当該個人データを処理しないものとする。但し、連合法又は加盟国法により処理を義務づけられる場合を除く。

第 28 条　文書化

1. コントローラとプロセッサは各自、本規則に定める要件の充足に必要な定期更新の文書を管理するものとする。

2. 更に、コントローラとプロセッサは各自、以下の情報に関する文書を管理するものとする。

(a) コントローラ、又は共同コントローラ若しくはプロセッサ、及び該当する場合には代表者の名称と連絡先詳細。

(b) 該当する場合、データ保護官の名称と連絡先詳細。

(ba) 該当する場合、個人データの公表先となるコントローラの名称と連絡先詳細。

(c) （削除）

(d) （削除）

(e) （削除）

(f) （削除）

(g) （削除）

(h) （削除）

3. （削除）

4. （削除）

5. （削除）

6. （削除）

*第29条 **監督機関との協力***

1. コントローラ、及び該当する場合にはプロセッサ、並びに該当する場合にはコントローラの代表者は、要請とともに、とりわけ第53条(2)の(a)号で言及された情報を提供することにより、かつ同項の(b)号に定めるアクセスを与えることにより、その義務の履行において監督機関と協力するものとする。

2. 第53条(2)の下での監督機関の権限行使に対して、コントローラとプロセッサは、監督機関の指定する合理的な期間内に監督機関に返答するものとする。当該返答は、監督機関の備考に対して講じた措置の説明と達成した結果を含めるものとする。

第 2 節
データセキュリティ

第 31 条　監督機関への個人データ侵害の通知

1.　個人データの侵害が発生した場合、コントローラは、その個人データの侵害を不当な遅滞なく監督機関に通知するものとする。

2.　プロセッサは、個人データの侵害の確証後、不当な遅滞なくコントローラに警告し、通知するものとする。

3.　第 1 項で言及された通知は、少なくとも以下に従わなければならない。

(a)　関係データ主体の分類と数、及び関係データ記録の分類と数も含め、個人データ侵害の性質を説明する。

(b)　データ保護官の身元情報と連絡先詳細、又は追加の情報を得られるその他の連絡窓口を伝達する。

(c)　個人データの侵害により考えうる悪影響を緩和するための措置を勧告する。

(d)　個人データ侵害の帰結を説明する。

(e)　個人データの侵害とその影響の緩和に対処するためにコントローラが提案したか、講じた措置を説明する。

必要であれば情報を段階的に提供できる。

4.　コントローラは、あらゆる個人データの侵害を文書化し、侵害を巡る事実関係、その影響、及び講じた是正行動を含めるものとする。当該文書は、本条及び第 30 条の順守を監督機関が確認できるようにする十分なものでなければならない。文書には、この目的のために必要な情報のみを含めるものとする。

4a. 監督機関は、通知を受けた侵害の種類について公的台帳を保持するものとする。

5. 欧州データ保護役員会は、第 66 条 1 項(b)に従い、第 1 項及び第 2 項で言及されたデータ侵害の確証と不当な遅滞の判定、並びにコントローラとプロセッサによる個人データ侵害通知を要する特定の状況に関する指針、勧告、及びベストプラクティスを発行する業務を付託されるものとする。

6. （削除）

第32 条　データ主体への個人データ侵害の報告

1. 個人データの侵害がデータ主体の個人データ、プライバシー、権利又は正当な利益の保護に悪影響を及ぼす可能性が高いとき、コントローラは、第 31 条で言及された通知の後、個人データの侵害を不当な遅滞なくデータ主体に報告するものとする。

2. 第 1 項で言及されたデータ主体への報告は、包括的及び明確かつ平易な言葉を用いるものとする。その中で個人データの侵害の性質を説明し、少なくとも第 31 条(3)の(b)号、(c)号、及び(d)号に定める情報と勧告、及び救済などデータ主体の権利についての情報を含めるものとする。

3. データ主体への個人データ侵害の報告は、コントローラが適切な技術的保護措置を実施のうえ、当該措置を個人データの侵害による関係データに適用したことを、監督機関を満足させるように証明した場合には不要であるものとする。当該技術的保護措置は、データのアクセスを許可されないあらゆる者に対して、当該データを理解不能なものとする。

4. 個人データの侵害をデータ主体に報告するコントローラの義務を損なうことなく、コントローラが個人データの侵害を既にデータ主体に報告していない場合、監督機関は、侵害により考えられる悪影響を考慮のうえ、コントローラに報告を義務づけることができる。

5. 欧州データ保護役員会は、第 66 条 1 項(b)に従い、個人データの侵害が第 1 項で言及されたデータ主体の個人データ又はプライバシー、権利又は正当な利益に悪影響を及ぼす可能性が高い状況について、指針、勧告、及びベストプラクティスを発行する業務を付託されるものとする。

6. （削除）

第 3 節
データ保護マネジメント

第32 条a　リスクの配慮

1.　　コントローラ、又は該当する場合にはプロセッサは、意図するデータ処理がデータ主体の権利と自由に及ぼす潜在的な影響のリスク分析を遂行し、その処理業務が特定のリスクをもたらす可能性が高いか否かを評価するものとする。

2.　　以下の処理業務は、特定のリスクをもたらす可能性が高い。

(a)　　連続するいずれかの 12 ヶ月間に 5,000 超のデータ主体と関連する個人データの処理。

(b)　　第 9 条(1)で言及された特殊分類個人データ、所在地データ、又は大規模ファイリングシステムの子ども若しくは従業員に関するデータの処理。

(c)　　個人に関して法的効果を生む措置の依拠となるプロファイリング、又は同様に多大な影響を個人に及ぼすプロファイリング。

(d)　　特定の個人に関して措置を講じるか意思決定を下すためにデータを処理する場合における、医療の提供、疫学的研究、又は精神疾患若しくは感染症調査のための個人データの大規模な処理。

(e)　　公的にアクセス可能な領域の大規模な自動化監視。

(f)　　第 34 条(2)の(b)号に従い、データ保護官又は監督機関との協議を要するその他の処理業務。

(g)　　個人データの侵害がデータ主体の個人データ、プライバシー、権利又は正当な利益の保護に悪影響を及ぼす可能性が高い場合。

(h)　コントローラ又はプロセッサの中核的活動を処理業務が占め、その性質、その範囲又はその目的を理由に、データ主体の定期的かつ体系的な監視を要する。

(i)　限定数になると合理的に予想できない複数の者に個人データをアクセス可能にする場合。

3.　リスク分析の結果に基づき、以下に従うものとする。

(a)　第 2 項(a)又は(b)で言及された処理業務のいずれかが存在する場合、連合内に設置されないコントローラは、第 25 条に定める要件と適用除外に沿って連合において代表者を指名するものとする。

(b)　第 2 項(a)、(b)、又は(h)で言及された処理業務のいずれかが存在する場合、コントローラは、第 35 条に定める要件と適用除外に沿ってデータ保護官を指名するものとする。

(c)　第 2 項(a)、(b)、(c)、(d)、(e)、(f)、(g)、又は(h)で言及された処理業務のいずれかが存在する場合、コントローラ、又はコントローラに代わって行為するプロセッサは、第 33 条に基づきデータ保護影響評価を遂行するものとする。

(d)　第 2 項(f)で言及された処理業務が存在する場合、コントローラは、データ保護官と協議するか、データ保護官を任命していない場合には第 34 条に従い監督機関と協議するものとする。

4.　リスク分析は、遅くとも 1 年後に見直しを行うか、或いはデータ処理業務の性質、範囲、又は目的に大幅な変更があった場合には直ちに見直しを行うものとする。第 3 項(c)に従い、コントローラがデータ保護影響評価の遂行を義務づけられない場合、リスク分析を文書化するものとする。

*第 33 条　**データ保護影響評価***

1.　第 32 条 a(3)の c 号に従いそれを要する場合、コントローラ、又はコントローラに代わって行為するプロセッサは、想定される処理業務がデータ主体の権利と自由、とりわけその個人データ保護権に及ぼす影響の評価を遂行するものとする。1 回の評価により、類似のリスクをもたらす類似の一連の処理業務に対処するのに十分であるものとする。

2.　（削除、第 32 条 a(2)に移行）

3.　　評価は、収集、処理から削除に至るまで、個人データの全ライフサイクル管理を考慮に入れるものとする。少なくとも以下を含めるものとする。

(a)　　想定される処理業務の体系的な説明、処理の目的、及び該当する場合にはコントローラの追求する正当な利益。

(b)　　目的との関連で、処理業務の必要性と均衡性に関する評価。

(c)　　業務により差別が取り込まれるか強化されるリスクも含め、データ主体の権利と自由に及ぼすリスクの評価。

(d)　　リスクに対処し、かつ個人データの処理量を最小化するにあたって想定される措置の説明。

(e)　　データ主体及びその他の関係者の権利と正当な利益を考慮に入れつつ、仮名化など個人データの保護を確実にし、かつ本規則の順守を証明するためのセーフガード、セキュリティ措置、及び仕組みの一覧。

(f)　　異なるデータ分類の削除期限の一般表示。

(h)　　第 23 条に従い、どの設計及び初期設定によるデータ保護の慣行を実施したのかの説明。

(i)　　個人データの受領者又は受領者属性の一覧。

(j)　　該当する場合、第三国又は国際機関の識別も含め、当該第三国又は国際機関への意図するデータ移転の一覧。第 44 条(1)の(h)号で言及された移転の場合、適切なセーフガードに関する文書。

(k)　　データ処理の内容に関する評価。

3a.　　コントローラ又はプロセッサがデータ保護官を指名した場合、当該データ保護官は、影響評価の手続きに関与するものとする。

3b.　　評価は文書化のうえ、第 33 条 a の(1)に従い、定期的なデータ保護順守審査に関する通常日程を組むものとする。第 33 条 a で言及されたデータ保護順守審査の結果が順守の一貫性欠如を示している場合、評価を不当な遅滞なく更新するものとする。

コントローラとプロセッサ、及び該当する場合にはコントローラの代表者は、評価を要請とともに監督機関に対し、利用可能にするものとする。

第33条a　データ保護順守審査

1.　第33条(1)に従い影響評価を遂行してから遅くとも2年後に、コントローラ、又はコントローラに代わって行為するプロセッサは、順守審査を遂行するものとする。当該順守審査は、データ保護影響評価を順守しつつ個人データの処理を遂行したことを証明するものとする。

2.　順守審査は少なくとも2年毎に定期的に遂行するか、或いは処理業務のもたらす特定のリスクに変更があったときには直ちに遂行するものとする。

3.　順守審査の結果が順守の一貫性欠如を示している場合、完全な順守の達成方法に関する勧告を順守審査に含めるものとする。

4.　順守審査とその勧告は文書化するものとする。コントローラとプロセッサ、及び該当する場合にはコントローラの代表者は、順守審査を要請とともに監督機関に対し、利用可能にするものとする。

5.　コントローラ又はプロセッサがデータ保護官を指名した場合、当該データ保護官は、順守審査の手続きに関与するものとする。

第34条　事前協議

1.　（削除）

2.　以下のいずれかに該当する場合、意図した処理の本規則順守を確保するため、とりわけデータ主体が晒されるリスクを緩和するため、個人データの処理前に、コントローラ、又はコントローラに代わって行為するプロセッサは、データ保護官と協議し、或いはデータ保護官を任命していない場合には監督機関と協議するものとする。

(a)　処理業務がその性質、その範囲、又はその目的を理由に、特定の高リスクをもたらす可能性が高いことを、第33条に定めるデータ保護影響評価で示している。

(b)　データ保護官又は監督機関は、第4項に従い指定された、データ主体の権利と自由に特定のリスクをもたらす可能性の高い処理業務に関して、その性質、その範囲又はその目的を理由に、事前協議の実施を必要とみなしている。

3. 意図した処理は、本規則を順守したものでなく、とりわけリスクの特定又は緩和が不十分である場合に本規則を順守したものでないと、所轄監督機関がその権限において決定した場合、当該所轄監督機関は当該意図した処理を禁止のうえ、不順守を是正するための適切な提案を行うものとする。

4. 欧州データ保護役員会は、第 2 項に従い事前協議の対象となる処理業務の一覧を策定のうえ、開示するものとする。

6. コントローラ又はプロセッサは、第 33 条に基づくデータ保護影響評価を要請とともに監督機関に提供するとともに、処理について監督機関による順守の評価を可能にし、とりわけデータ主体の個人データ保護にとってのリスクの評価と関連セーフガードの評価を可能にするその他の情報を要請とともに監督機関に提供するものとする。

7. 加盟国は、処理の性質を定義した国内議会の採択する立法措置又は当該立法措置に基づく措置の準備にあたって、意図した処理の本規則順守を確保するため、とりわけデータ主体が晒されるリスクを緩和するため、監督機関と協議するものとする。

第 4 節
データ保護官

第35 条　データ保護官の指名

1. 以下のいずれかに該当する場合、コントローラ及びプロセッサは、データ保護官を指名するものとする。

(a) 処理を公的機関又は公共団体が遂行する。

(b) 処理を法人が遂行し、かつ連続する 12 ヶ月間に 5000 超のデータ主体と関連する。

(c) コントローラ又はプロセッサの中核的活動を処理業務が占め、その性質、その範囲又はその目的を理由に、データ主体の定期的かつ体系的な監視を要する。

(d)　コントローラ又はプロセッサの中核的活動を、第 9 条(1)に基づく特殊分類データ、所在地データ、又は大規模ファイリングシステムの子ども若しくは従業員に関するデータの処理が占める。

2.　事業グループは、各拠点からのデータ保護官への容易な連絡を確実にすることを前提として、主任データ保護官を任命できる。

5.　コントローラ又はプロセッサが公的機関又は公共団体である場合、当該公的機関又は公共団体の組織構造を考慮に入れつつ、その複数の機関のためにデータ保護官を指名できる。

4.　第 1 項で言及されたもの以外の場合、コントローラ若しくはプロセッサ、又はコントローラ若しくはプロセッサの分類に入る協会及びその他団体は、データ保護官を指名できる。

5.　コントローラ又はプロセッサは、職務上の資質に加え、とりわけデータ保護法及び慣行の専門知識と第 37 条で言及された業務の履行能力を基にデータ保護官を指名するものとする。専門知識の必要水準は、とりわけ遂行するデータ処理と、コントローラ又はプロセッサの処理する個人データに要する保護に基づいて決定するものとする。

6.　コントローラ又はプロセッサは、データ保護官のその他の職務がデータ保護官としての本人の業務と義務に一致し、かつ利害相反に帰結しないことを確実にするものとする。

7.　コントローラ又はプロセッサは、データ保護官を、従業員の場合は少なくとも 2 年間を 4 期にわたり、或いは外部の役務請負業者の場合は、2 年間にわたり、指名するものとする。データ保護官は更なる任期にあたり再任できる。データ保護官がもはやその義務の履行に要する条件を充足しない場合でなければデータ保護官を任期中に解任できない。

8.　役務提供契約を基づき、コントローラ又はプロセッサは、データ保護官を雇用するか業務履行を行わせることができる。

9.　コントローラ又はプロセッサは、データ保護官の氏名と連絡先詳細を監督機関と一般大衆に伝達するものとする。

10.　データ主体は、データ主体のデータの処理と関連した全ての問題についてデータ保護官と連絡を取る権利、及び本規則の下での権利を行使する要請を行う権利を有するものとする。

11.　（削除）

第36条　データ保護官の地位

1.　　コントローラ又はプロセッサは、データ保護官が適正かつ適時に、個人データの保護と関連する全ての問題に関与することを確実にするものとする。

2.　　コントローラ又はプロセッサは、データ保護官が義務と業務を独立して遂行し、かつ職務機能の行使に関していかなる指示をも受けないことを確実にするものとする。データ保護官は、コントローラ又はプロセッサの幹部層に直接報告を行うものとする。コントローラ又はプロセッサは、この目的のために、本規則条文の順守につき責任を負う幹部を指名するものとする。

3.　　コントローラ又はプロセッサは、データ保護官による業務遂行を支援するものとし、職員、施設、設備、及びその他の資源も含め、第 37 条で言及された義務と業務の遂行に必要な全ての手段、及びデータ保護官の職務上の知識を維持するのに必要な全ての手段を提供するものとする。

4.　　データ保護官は、データ主体の識別に関して、かつデータ主体の識別を可能にする状況に関して、守秘義務に拘束されるものとする。但し、データ主体がその義務から解放した場合を除く。

第 5 節
行動規範及び認証

第38条　行動規範

1.　　加盟国、監督機関、及び欧州委員会は、様々なデータ処理部門の特定の特徴、とりわけ以下と関連した特定の特徴を考慮に入れつつ、本規則の適正な適用への寄与を意図した行動規範の策定又は監督機関の策定した行動規範の採択を奨励するものとする。

(a)　　データ処理の公正性と透明性。

(aa)　　消費者の権利の尊重。

(b)　　データの収集。

(c)　　一般大衆とデータ主体の情報。

(d)　　データ主体による権利行使の要請。

(e)　　子どもの情報と保護。

(f)　　第三国又は国際機関へのデータ移転。

(g)　　コントローラが行動規範を遵守するよう監視し、それを確保するための仕組み。

(h)　　第 73 条及び第 75 条に基づくデータ主体の権利を損なうことなく、個人データの処理に関して、コントローラとデータ主体間の紛争を解決するための裁判外手続き及びその他の紛争解決手続き。

2.　　ある加盟国においてコントローラ又はプロセッサの分類に入る協会及びその他団体が、行動規範の策定又は既存の行動規範の修正若しくは拡張を意図している場合、当該加盟国の監督機関に意見を仰ぐことができる。監督機関は、不当な遅滞なく、行動規範の草案又はその修正版の下での処理が本規則を順守しているのか否かの意見を提供するものとする。監督機関は、当該草案に関するデータ主体又はその代表者の見解を求めるものとする。

3.　　複数の加盟国においてコントローラ又はプロセッサの分類に入る協会及びその他団体は、行動規範の草案及び既存の行動規範の修正若しくは拡張版を欧州委員会に提出できる。

4.　　欧州委員会は、欧州データ保護役員会の意見を要請後に、第 3 項に従い提出を受けた行動規範及び既存の行動規範の修正若しくは拡張版が本規則に沿い、かつ連合内において一般的な有効性を有することを決定するために、第 86 条に基づき委任法令を採択する権限を与えられるものとする。当該委任法令は、データ主体に執行可能な権利を与えるものとする。

5.　　欧州委員会は、第 4 項に基づき一般的な有効性を有するとの決定が下された行動規範については、適切な公開が行われることを確実にするものとする。

*第 39 条　**認証***

1.　　（削除）

1a.　　いずれのコントローラ又はプロセッサも、事務管理費用を考慮に入れた合理的な手数料により、本規則、とりわけ第 5 条、第 23 条、及び第 30 条に定める原則、コントローラとプロセッサの義務、並びにデータ主体の権利を順守して個人データの処理を遂行しているとの認証を連合内のいずれの監督機関にも要請できる。

1b.　　認証は、任意、低費用、かつ不当な負担をかけない透明性ある手順を通じて利用可能であるものとする。

1c.　　監督機関と欧州データ保護役員会は、第 57 条に基づく一貫性の仕組みの下で協力し、連合内における手数料の調和も含め、調和の取れたデータ保護認証の仕組みを保証するものとする。

1d.　　監督機関は、認証手続きの最中に、コントローラ又はプロセッサを代行して監査を遂

行する専門の第三者監査人を公認できる。第三者監査人は、十分に適任の職員を擁し、公平であり、その義務に関していかなる利害相反もないものとする。監査人は、その義務を正確に履行しないと信じるに足りる理由がある場合、監督機関は、公認を取消すものとする。最終的な認証は、監督機関が行うものとする。

1e. 監督機関は、監査に基づき、本規則を順守して個人データを処理しているとの認証を受けたコントローラとプロセッサに対し、「欧州データ保護シール」と名づけられた標準データ保護マークを付与するものとする。

1f. 「欧州データ保護シール」は、認証を受けたコントローラ又はプロセッサのデータ処理業務が本規則の完全な順守を継続する限り、有効であるものとする。

1g. 1f にかかわらず、認証は最大で 5 年間有効であるものとする。

1h. 欧州データ保護役員会は、加盟国において発行済みである有効及び無効の全証明書を一般大衆が閲覧できる公的な電子台帳を確立するものとする。

2. （削除）

2a. 欧州データ保護役員会は自発的に、本規則を順守したデータ保護向上技術基準の認証を行える。

3. 欧州委員会は、欧州データ保護役員会の意見を要請後、かつ利害関係者、とりわけ産業及び非政府組織の利害関係者との協議後に、監査人の公認要件、付与と撤回の条件、及び連合内と第三国における認知要件も含め、第 1 項から第 1h 項で言及されたデータ保護認証の仕組みの基準と要件を更に具体化させることを目的に、第 86 条に基づき委任法令を採択する権限を与えられるものとする。当該委任法令は、データ主体に執行可能な権利を与えるものとする。

第 5 章
第三国又は国際機関への個人データの移転

第 40 条　移転の一般原則

個人データを処理してから第三国又は国際機関へ移転することや、移転後に処理を意図している個人データを移転することは、本規則のその他条文を前提に、第三国又は国際機関から別の第三国又は別の国際機関への個人データの移転条件も含め、本章に定める条件をコントローラとプロセッサが順守した場合にのみ行える。

第 41 条　十分性認定のある移転

1.　　第三国又は当該第三国内の領域若しくは処理部門、或いは対象となる国際機関は、十分な水準の保護を確保していると欧州委員会が認定した場合、移転を行える。当該移転は何ら特定の許可をも要しないものとする。

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とする。

(a)　　法の支配に加え、公共安全法、国防法、国家安全保障法、刑法、及び本法令実施に関するものも含めた発効済みの一般的及び部門別の関係法令、当該第三国において順守するか当該国際機関の順守する職務規定とセキュリティ措置、法哲学的先例、並びにデータ主体向けの効果的な行政的救済若しくは司法的救済も含めた効果的かつ執行可能な権利、特に個人データの移転元となる連合内に居住するデータ主体向けのもの。

(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。

(c)　　対象となる第三国又は国際機関が締結した国際公約、とりわけ個人データ保護に関して法的拘束力を有するあらゆる協定又は法律文書。

3.　　欧州委員会は、第三国又は当該第三国内の領域若しくは処理部門、或いは国際機関は、第 2 項の意味の範囲内で十分な水準の保護を確保していると認定するにあたって、第 86 条に基づき委任法令を採択する権限を与えられるものとする。当該委任法令は、処理部門と関係する場合に時限条項を定めるものとし、本規則に基づく十分な水準の保護をもはや確保できなくなり次第、第 5 項に従い取消とするものとする。

4.　　委任法令は、その適用領域と適用部門を特定し、該当する場合には第 2 項の(b)号で言及された監督機関を特定するものとする。

4a.　　第 3 項に基づき委任法令を採択した場合、欧州委員会は第 2 項に列挙した要素に影響を及ぼしうる第三国と国際機関の動向を継続的に監視するものとする。

5.　　欧州委員会は、第三国又は当該第三国内の領域若しくは処理部門、或いは国際機関は、本条第 2 項の意味の範囲内で十分な水準の保護を確保していないか、もはや確保していないと認定するにあたって、とりわけ当該第三国又は国際機関において発効済みである一般的及び部門別の関係法令が、データ主体向けの効果的な行政的救済若しくは司法的救済も含めた効果的かつ執行可能な権利、特に個人データの移転元となる連合内に居住するデータ主体向けのものを保証しない場合に、第 86 条に基づき委任法令を採択する権限を与えられるものとする。

6.　　第 42 条から第 44 条を損なうことなく、第三国又は当該第三国内の領域若しくは処理部門、或いは対象となる国際機関への個人データの移転を禁止すると、欧州委員会が第 5 項に基づき決定した場合。欧州委員会は、適切な時期に、本条第 5 項に基づく決定から帰結した状況の是正を視野に入れつつ、当該第三国又は国際機関と協議を行うものとする。

6a.　　第 3 項及び第 5 項に基づく委任法令の採択前に、欧州委員会は欧州データ保護役員会に保護水準の十分性に関する意見提供を要請するものとする。欧州委員会はこれに関し、第三国又は当該第三国内の領域若しくは処理部門の政府、或いは国際機関との通信物も含めた全て必要な文書を欧州データ保護役員会に提供するものとする。

7. 欧州委員会は欧州連合官報とそのウェブサイト上に、十分な水準の保護を確保しているか、確保していないと認定した第三国、第三国内の領域と処理部門、及び国際機関の一覧を公表するものとする。

8. 95/46/EC 指令の第 25 条(6)又は第 26 条(4)を基に欧州委員会の採択した決定は本規則の発効後 5 年間にわたり、当該期間の終了前に欧州委員会により修正、置換、又は撤回とならない限り、効力を有するものとする。

第 42 条　適切なセーフガードを介した移転

1. 欧州委員会が第 41 条に基づく認定を下さないか、第三国又は当該第三国内の領域若しくは処理部門、或いは国際機関は、第 41 条(5)に従い十分な水準の保護を確保していないと認定した場合、法的拘束力を有する法律文書の中で個人データ保護に関してコントローラ又はプロセッサで適切なセーフガードを提示していない限り、コントローラ又はプロセッサは、第三国、領域、又は国際機関に個人データを移転できない。

2. 第 1 項で言及された適切なセーフガードは、とりわけ以下のいずれかにより提供するものとする。

(a) 第 43 条に従った拘束的企業準則。

(aa) 第 39 条の第 1e 項に従い、コントローラと受領者向けの有効な「欧州データ保護シール」。

(b) （削除）

(c) 欧州委員会が第 62 条(1)の(b)号に従い一般的に有効であると宣言した場合、第 57 条で言及された一貫性体制に従い、監督機関の採択したデータ保護標準条項。

(d) 第 4 項に従い、監督機関により許可されたコントローラ又はプロセッサとデータの受領者との間の契約条項。

3. 第 2 項の(a)号、(aa)号、又は(c)号で言及されたデータ保護標準条項、「欧州データ保護シール」、又は拘束的企業準則に基づく移転は何ら特定の許可をも要しないものとする。

4. 本条第 2 項の(d)号で言及された契約条項に基づく移転の場合、コントローラ又はプロセッサは、契約条項について監督機関から事前許可を取得するものとする。別の加盟国内又はその他加盟国内のデータ主体に関する処理活動と関連した移転の場合、或いは連合内における個人データの自由な移動に多大な影響を及ぼす場合、監督機関は、第 57 条で言及された一貫性体制を適用するものとする。

5. 95/46/EC 指令の第 26 条(2)に基づいた監督機関による許可は、本規則の発効後 2 年間にわたり、当該期間の終了前に当該監督機関により修正、置換、又は撤回とならない限り、効力を有するものとする。

第 43 条　拘束的企業準則（BCR）による移転

1. 監督機関は、第 58 条に定める一貫性体制に従い、以下の場合に限り拘束的企業準則を承認するものとする。

(a) 法的拘束力を有し、コントローラの事業グループの全構成員と拘束的企業準則の網羅範囲内である外部下請け業者に、その従業員も含めて適用され、かつコントローラの事業グループの全構成員と拘束的企業準則の網羅範囲内である外部下請け業者により、その従業員も含めて執行される場合。

(b) データ主体に執行可能な権利を明示的に与える場合。

(c) 第 2 項に定める要件を充足する場合。

1a. 雇用データに関しては、第 43 条に基づく拘束的企業準則の策定につき、従業員の代表者に通知を行い、かつ連合又は加盟国の法律と慣行に従い、従業員の代表者が関与するものとする。

2. 拘束的企業準則は、少なくとも以下を明記するものとする。

(a) 事業グループとその構成員、及び拘束的企業準則の網羅範囲内である外部下請け業者の構造と連絡先詳細。

(b) 個人データの分類、処理の種類とその目的、影響を受けるデータ主体の種類、及び対象となる第三国又は諸国の識別も含め、データ移転又は一連のデータ移転。

(c) 内外におけるその法的拘束力の性質。

(d)　　データ保護一般原則、とりわけ目的の限定、データの最小化、保存期間の限定、データ品質、設計によるデータ保護及び初期設定によるデータ保護、処理の法的根拠、機微な個人データの処理、データセキュリティの確保措置、ポリシーに拘束されない組織への移転要件。

(e)　　第 20 条によるプロファイリングに基づく措置の対象外となる権利、第 75 条に従い加盟国の所轄監督機関と管轄裁判所に苦情を呈する権利、救済を得る権利、並びに該当する場合には拘束的企業準則の違反により補償を受ける権利も含め、データ主体の権利とその権利行使手段。

(f)　　連合内に設置されない事業グループのいずれかの構成員による拘束的企業準則違反の法的責任を加盟国の領域に設置されたコントローラが受諾すること。損害を引き起こした事態は、当該構成員の責任でないことをコントローラ又はプロセッサが証明した場合にのみ、コントローラ又はプロセッサの当該法的責任をその全部又は一部について免除できる。

(g)　　拘束的企業準則に関する情報、とりわけ本項(d)号、(e)号、及び(f)号で言及された条文に関する情報を第 11 条に従いデータ主体に提供する方法。

(h)　　事業グループ内の拘束的企業準則の順守監視と訓練及び苦情処理の監視も含め、第 35 条に従い指名したデータ保護官の業務。

(i)　　拘束的企業準則の順守確認の確保を狙いとした事業グループ内の仕組み。

(j)　　ポリシーへの変更を報告及び記録し、当該変更を監督機関に報告するための仕組み。

(k)　　事業グループの構成員による順守を確保するための監督機関との協力体制、とりわけ本項の(i)号で言及された措置の確認結果を監督機関に利用可能にすることによる協力体制。

3.　　欧州委員会は、本項の意味の範囲内で拘束的企業準則の形態、手続き、基準、及び要件を、とりわけその承認基準に関して、データ主体への透明性、プロセッサの遵守する拘束的企業準則に対する第 2 項の(b)号、(d)号、(e)号、及び(f)号の適用、及び関係データ主体の個人データ保護を確保するための更に必要な要件も含め、更に具体化させることを目的に、第 86 条に基づき委任法令を採択する権限を与えられるものとする。

4.　　（削除）

第 43 条 a　連合法によって認められていない移転又は公表

1.　　個人データの公表をコントローラ又はプロセッサに義務づける第三国の裁判所判決若しくは裁決、並びに行政機関の決定は、要請側第三国と連合又は加盟国との間で発効している刑事共助条約又は国際協定を損なうことなく、いかなる方法によっても認めず、或いは執行可能でないものとする。

2.　　第三国の裁判所判決若しくは裁決又は行政機関の決定により、個人データの公表をコントローラ又はプロセッサに要請する場合、コントローラ又はプロセッサ、並びに該当する場合にはコントローラの代表者は、不当な遅滞なく当該要請を監督機関に通知するものとし、移転又は公表の事前許可を監督機関から取得しなければならない。

3. 監督機関は、要請のある公表の本規則順守を、とりわけ公表が第 44 条(1)の(d)及び(e)、並びに(5)に基づき必要かつ法的に義務づけられるのか否かにつき、評価を行うものとする。その他加盟国からのデータ主体が影響を受ける場合、監督機関は、第 57 条で言及された一貫性体制を適用するものとする。

4. 監督機関は、要請について所轄国家機関に通知するものとする。第 21 条を損なうことなく、コントローラ又はプロセッサも、当該要請と、監督機関による許可についてデータ主体に通知し、該当する場合には、第 14 条(1)の(ha)号に従い連続する過去 12 ヶ月間に個人データを公的機関に提供したか否かについてデータ主体に通知するものとする。

5. （削除）

第 44 条 逸脱

1. 第 41 条に基づく十分性認定又は第 42 条に基づく適切なセーフガードが不在である場合、個人データの第三国又は国際機関への移転又は一連の移転は、専ら以下のいずれかを条件に行える。

(a) 十分性認定及び適切なセーフガードの不在に起因する当該移転のリスクについて通知を受けた後、データ主体が移転の提案に同意している。

(b) データ主体とコントローラの間の契約履行に、又はデータ主体の要請により講じる契約前の措置実施に、移転を必要とする。

(c) データ主体の利益のためにコントローラと別の自然人又は法人との間で交わす契約の締結又は履行に移転を必要とする。

(d) 公共の利益の重要な根拠のために移転を必要とする。

(e) 法的な主張の確立、行使、又は防御のために移転を必要とする。

(f) データ主体が同意を付与するための身体的能力又は法的能力を有しない場合に、データ主体又は別の者の重大利益を保護するために移転を必要とする。

(g) 連合法又は加盟国法に従い、一般大衆への情報提供を意図し、かつ一般大衆又は正当な利益を証明できるいずれかの者による参照に開放した台帳から、連合法又は加盟国法に定める参照条件をその特定の場合に満たしている範囲内において、移転を行う。

(h) （削除）

2. 第 1 項の(g)号に従った移転は、台帳に収納された個人データの全部又は分類別個人データの全部を含まないものとする。正当な利益のある者による参照を意図した台帳の場合、当該者から要請があったか当該者が受領者となる場合に限り、移転を行うものとする。

3. （削除）

4. 第 1 項の(b)号及び(c)号は、公的機関がその公権の行使にあたって遂行する活動には適

用されないものとする。

5. 第 1 項の(d)号で言及された公共の利益は、連合法又はコントローラが対象となる加盟国の法律の中で認めなければならない。

7. 欧州データ保護役員会は第 66 条 1 項(b)に従い、第 1 項を基にデータ移転の基準と要件を拡大することを目的に、指針、勧告、及びベストプラクティスを発行する業務を付託されるものとする。

第 45 条　個人データ保護のための国際協力

1. 第三国及び国際機関との関連で、欧州委員会及び監督機関は以下に向けた適切な措置を講じるものとする。

(a) 個人データ保護に向けた法令執行を確保するための効果的な国際協力の仕組み立案。

(b) 個人データ及びその他の基本的人権と自由の保護に向けた適切なセーフガードを前提に、通知、苦情申立、調査支援、及び情報交換を通じたものも含め、個人データ保護に向けた法令執行における国際相互協力の提供。

(c) 個人データ保護に向けた法令執行における国際協力の促進を狙いとした議論と活動に際する、関連性のある利害関係者への関与。

(d) 個人データ保護法令及び慣行の共有と文書化の促進。

(da) 第三国との法哲学的紛争に関する明確化と協議。

2. 第 41 条(3)の意味の範囲内で十分な水準の保護を確保していると欧州委員会が認定した場合、第 1 項の目的上、欧州委員会は第三国又は国際機関、とりわけ第三国又は国際機関の監督機関との関係を向上させるための適切な手段を講じるものとする。

第 45 条 a　欧州委員会による報告

欧州委員会は、遅くとも第 91 条(1)で言及された日付の 4 年後より定期的に、第 40 条から第 45 条の適用に関する報告を欧州議会及び理事会に提出するものとする。この目的上、欧州委員会は加盟国及び監督機関から情報を要請できるとともに、当該情報を不当な遅滞なく提供するものとする。当該報告は開示されるものとする。

第 6 章
独立監督機関

第 1 節
独立の状態

第 46 条　監督機関

1. 個人データ保護との関連で自然人の基本的人権と自由を保護するために、かつ連合内における個人データの自由な流通に資するために、加盟国は各自、本規則の適用の監視と連合全体におけるその一貫性ある適用への寄与につき 1 つ以上の公的機関が責任を負うことを定めるものとする。これらの目的上、監督機関は相互に、及び欧州委員会と協力するものとする。

2. 加盟国に 2 つ以上の監督機関を設置した場合、当該加盟国は欧州データ保護役員会への当該諸機関による効果的な参加のために、単独の連絡窓口として機能する監督機関を指定するものとし、第 57 条で言及された一貫性体制と関連したルールに対するその他の機関の順守を確保するための仕組みを策定するものとする。

3. 加盟国は各自、本章に従い採択する自国法の条文を遅くとも第 91 条(2)に明記された日付までに、かつこれに影響を及ぼすその後のあらゆる修正を遅滞なく、欧州委員会に通知するものとする。

第 47 条
独立性

1. 本規則第 7 章に従った協力及び一貫性の取り決めにかかわらず、監督機関は、付託された義務と権限の行使にあたって完全な独立性を以って行為するものとする。

2. 監督機関の構成員は、その義務の履行にあたって誰からも指示を求めず、かつ指示を受けず、完全な独立性と公平性を維持するものとする。

3. 監督機関の構成員は、その義務と適反するあらゆる行動を慎むものとし、その任期中に、有利であるか否かを問わず、その義務に反する職務に従事しないものとする。

4. 監督機関の構成員は、任期終了後に、就任の受諾や便益の受領に関して誠意ある慎重な行動をするものとする。

5. 加盟国は各自、相互協力、協力、及び欧州データ保護役員会への参加との関連で遂行するものも含めた監督機関の義務と権限の効果的な履行に必要となる十分な人的、技術的、及び財務資源、施設、インフラストラクチャーを監督機関に提供することを確実にするものとする。

6. 加盟国は各自、監督機関の長により任命され、かつ監督機関の長の指示対象となる独自の職員を監督機関が擁することを確実にするものとする。

7. 加盟国は、監督機関がその独立性に影響を与えない財務統制の対象となることを確実にするものとする。加盟国は、監督機関が別個の年次予算を有することを確実にするものとする。予算は開示するものとする。

7a. 加盟国は各自、予算制御を理由に国内議会に対して監督機関に説明責任があることを確実にするものとする。

第 48 条　監督機関の構成員についての一般的条件

1. 加盟国は、監督機関の構成員を関係加盟国の議会又は政府が任命しなければならないことを定めるものとする。

2. 構成員は、その独立性に疑いの余地がなく、特に個人データ保護の分野におけるその義務の履行に要する経験と技能が証明済みである者の中から選定するものとする。

3. 構成員の義務は、第 5 項に基づく任期満了、辞任、又は定年退職の場合に終了するものとする。

4. 構成員がその義務の履行に要する条件をもはや充足しないか、重大な違法行為で有罪となった場合に、管轄国内裁判所により、当該構成員を解任できるか、年金又はそれに代わるその他の給付に対する権利を剥奪できる。

5. 構成員の任期満了又は辞任の場合、当該構成員は、新規構成員の任命まで引き続き義務を行使するものとする。

第 49 条　監督機関の設立に関するルール

加盟国は各自、本規則の制限範囲内において、以下を法律により定めるものとする。

(a)　監督機関の設立と地位。

(b)　監督機関の構成員による義務の履行に要する資格、経験、及び技能。

(c)　監督機関の構成員を任命するためのルールと手続き、並びに職務に反する行動又は職務に関するルール。

(d)　監督機関の構成員の任期。本規則発効後の最初の任命を除き、4 年以上とし、監督機関の独立性を守るのに必要である場合には、その手続きを早めることにより、4 年より短くすることもできる。

(e)　監督機関の構成員に再任を認めるか否か。

(f)　監督機関の構成員と職員の義務を準拠させる規則と一般条件。

(g)　構成員がその義務の履行に要する条件をもはや充足しないか重大な違法行為で有罪となった場合も含め、監督機関の構成員の義務終了に関するルールと手続き。

第 2 節
義務及び権限

第51条　管轄

1.　監督機関は各自、第 73 条及び第 74 条を損なうことなく、所属加盟国の領域に対して、本規則に基づき与えられた義務の履行能力と権限の行使能力を有するものとする。公的機関によるデータ処理は専ら当該加盟国の監督機関が監督を行うものとする。

2.　（削除）

3.　監督機関は、裁判所がその司法権力において行う処理業務について監督能力を有しないものとする。

第52条　義務

1.　監督機関は以下を行うものとする。

(a)　本規則の適用を監視し、かつそれを確実にする。

(b)　第 73 条に基づきデータ主体又は協会の呈した苦情に対応し、当該事項を適切な範囲内において調査のうえ、とりわけ更なる調査又は別の監督機関との協調を必要とする場合に、苦情の進展と結果を合理的な期間内にデータ主体又は協会に通知する。

(c)　その他の監督機関と情報を共有し、かつその他の監督機関に相互協力を提供のうえ、本規則の適用と執行の一貫性を確保する。

(d)　調査は、自発的に、又は苦情を基に、若しくは不法な処理嫌疑について受領した特定かつ文書化された情報を基に、又は別の監督機関の要請とともに、実施のうえ、データ主体が当該監督機関に苦情を申し立てた場合に、調査の結果を合理的な期間内に関係データ主体に通知する。

(e)　個人データの保護に影響を及ぼす限りにおいて、とりわけ情報及び通信技術の開発と商業上の慣行につき、関係動向を監視する。

(f)　個人データ処理に関する個人の権利と自由の保護と関連する立法措置と行政措置について、加盟国機関及び団体の諮問を受ける。

(g)　第 34 条で言及された処理業務を授権し、それに関して諮問を受ける。

(h)　第 38 条(2)に従い、行動原則草案に関する意見を表明する。

(i)　第 43 条に従い、拘束的企業準則を承認する。

(j)　欧州データ保護役員会の活動に参加する。

(ja)　　第 39 条に従い、コントローラとプロセッサを認証する。

2.　　監督機関は各自、個人データ処理と関連したリスク、ルール、セーフガード、及び権利に関して、並びに個人データ保護に向けた適切な措置に関して、一般大衆の認知を促進するものとする。子どもを特定的に対象とした活動については、特に注意を払うものとする。

2a.　　監督機関は各自、欧州データ保護役員会と一緒に、個人データ処理と関連したリスク、ルール、セーフガード、及び権利に関して、コントローラとプロセッサの認知を促進するものとする。これには制裁と違反に関する台帳の保持も含まれる。台帳には、あらゆる警告と制裁の双方を可能な限り詳細に、並びに違反の解決を登録すべきである。監督機関は各自、本規則に基づく責任と義務に関する一般情報を要請とともに零細及び中小企業コントローラとプロセッサに提供するものとする。

3.　　監督機関は要請とともに、本規則の下での権利行使にあたっていずれのデータ主体にも助言を行い、適切であれば、これに関してその他の加盟国の監督機関と協力するものとする。

4.　　第 1 項の(b)号で言及された苦情については、監督機関は、電子形式により苦情申し立ての様式を提供するが、それ以外の通信手段も排除しないものとする。

5.　　監督機関の義務の履行は、データ主体にとって無償であるものとする。

6.　　要請が明らかに過剰である場合、とりわけその反復的な特徴から明らかに過剰である場合、監督機関は合理的な手数料を課すか、データ主体の要請した行動を講じないことができる。当該手数料は、要請のあった行動を講じるための費用を超過しないものとする。監督機関は、要請の明らかに過剰な特徴の立証責任を負うものとする。

*第53条　**権限***

1.　　監督機関は各自、本規則に沿って以下の権限を有するものとする。

(a)　　個人データ処理の準拠条文の違反嫌疑につき、コントローラ又はプロセッサに通知する権限、並びに適切であれば、データ主体の保護改善に向けて特定の方法による当該違反の是正をコントローラ又はプロセッサに命じる権限、又はデータ主体への個人データ侵害の伝達をコントローラに命じる権限。

(b)　　本規則により定める権利の行使に向けたデータ主体の要請の順守をコントローラ又はプロセッサに命じる権限。

(c)　　義務の履行と関連性のあるあらゆる情報の提供をコントローラとプロセッサ、並びに該当する場合には代表者に命じる権限。

(d)　　事前許可及び第 34 条で言及された事前協議の順守を確保する権限。

(e)　　コントローラ又はプロセッサに警告又は忠告を行う権限。

(f)　本規則条文に違反して処理を行った全データの訂正、削除、又は破壊を命じる権限、並びにそのデータが開示された第三者に当該行動を通知させることを命じる権限。

(g)　暫定的又は最終的な処理禁止を課す権限。

(h)　第三国の受領者又は国際機関へのデータの移動を保留する権限。

(i)　個人データ保護と関連したあらゆる事項に関して意見を表明する権限。

(ia)　第 39 条に従い、コントローラとプロセッサを認証する権限。

(j)　個人データ保護と関連したあらゆる事項に関して、国内議会、政府、又はその他の政治機関のほか、一般大衆に知らせる権限。

(ja)　第 66 条(4b)に従い欧州データ保護役員会の発行した指針を考慮に入れつつ、本規則の違反に関する内密の報告を奨励する効果的な仕組みを確立する権限。

2.　監督機関は各自、コントローラ又はプロセッサから事前通知なく以下を取得する調査権限を有するものとする。

(a)　その義務の履行に必要となる全ての個人データ並びに全文書及び情報へのアクセス。

(b)　データ処理設備及び手段へのアクセスも含め、その全ての施設へのアクセス。

(b)号で言及された権限は、連合法及び加盟国法を遵守しながら行使するものとする。

3.　監督機関は各自、とりわけ第 74 条(4)及び第 75 条(2)に従い、本規則の違反を司法機関に注意喚起し、かつ法的手続きを開始する権限を有するものとする。

4.　監督機関は各自、第 79 条に基づき、行政違反に制裁を課す権限を有するものとする。当該権限は、効果的かつ均衡の取れた制止的な方法により行使するものとする。

第 7 章
協力及び一貫性

第 1 節
協力

第 54 条 a　主たる機関

1.　個人データの処理が連合内のコントローラ又はプロセッサの拠点活動との関連で行われ、かつ 2 つ以上の加盟国にコントローラ又はプロセッサが設置されている場合、或いは複数加盟国の居住者につきその個人データを処理する場合、コントローラ又はプロセッサの主たる拠点の監督機関は、本規則第 7 章の条文に基づき、全加盟国におけるコントローラ又はプロセッサの処理活動に監督責任を負う主たる機関として行為するものとする。

2. 主たる監督機関は、責任を負うコントローラ又はプロセッサの処理活動につき、意見の一致を見る試みとして、第 51 条 1 項の意味の範囲内に入るその他全ての所轄監督機関と協議してから初めて、適切な監督措置を講じるものとする。主たる監督機関は、この目的のために、コントローラ又はプロセッサに関して法的効果を生むことを意図した措置を採択する前に、とりわけあらゆる関係情報を提出のうえ、第 51 条 1 項の意味の範囲内に入るその他の機関に相談するものとする。主たる機関は、関与機関の意見を最大限に考慮に入れるものとする。主たる機関は、責任を負うコントローラ又はプロセッサの処理活動に関して法的効果を生むことを意図した措置の決定権を与えられた唯一の機関であるものとする。

3. 欧州データ保護役員会は、所轄監督機関の要請とともに、以下のいずれかに該当する場合、コントローラ又はプロセッサにつき責任を負う主たる機関の識別に関する意見を表明するものとする。

(a) 各事案の事実関係から、コントローラ又はプロセッサの主たる拠点の所在地が明確でない場合。

(b) どの監督機関が主たる機関として行為するのかについて、所轄官庁の意見が一致しない場合。

(c) コントローラは、連合内に設置されておらず、かつ本規則の範囲内に入る処理業務により異なる加盟国の居住者が影響を受ける場合。

3a. コントローラがプロセッサとしての活動をも行使する場合、コントローラの主たる拠点の監督機関は、処理活動の監督につき主たる機関として行為する。

4. 欧州データ保護役員会は、主たる機関の識別を決定できる。

第55 条 相互支援

1. 監督機関は、本規則の一貫した方法による実施と適用のために、関係情報と相互支援を相互に提供するものとし、相互の効果的な協力に向けた措置を確立するものとする。相互支援はとりわけ、事前許可と協議、検査、及び調査の遂行要請、コントローラ又はプロセッサが複数加盟国に拠点を有する場合或いは複数の加盟国のデータ主体が処理業務により影響を受ける可能性が高い場合における事案の調査開始とその後の動向に関する速やかな情報提供など、情報要請と監督措置を網羅するものとする。第 54 条 a に定義された主たる機関は、関与監督機関との協調を確実にするものとし、コントローラ又はプロセッサの唯一の連絡窓口として行為するものとする。

2. 監督機関は各自、別の監督機関の要請に対し、遅滞なく返信する上で必要な全ての適切な措置を講じるものとし、その期間は 1 ヶ月を超えないものとする。当該措置にはとりわけ、調査過程に関する関係情報の送信、又は本規則に反する処理業務の停止若しくは禁止に向けた強制措置も含まれることがある。

3. 支援の要請は、要請目的と要請理由も含め、必要な情報の全てを包含するものとする。取り交わされた情報は、要請のあった事項に関してのみ使用するものとする。

4. 支援の要請先である監督機関は、以下のいずれかに該当しない限り、その順守を拒否できない。

(a) 要請について管轄権を有さない。

(b) 要請の順守が本規則の条文に抵触する可能性がある。

5. 要請を受けた監督機関は、要請元監督機関の要請を満たすために講じた結果を、又は場合に応じてその進展若しくは措置を、要請元監督機関に通知するものとする。

6. 監督機関は、その他の監督機関から要請された情報を電子的手段により、かつ可能な限り最短の期間内に、標準書式を用いて提供するものとする。

7. 相互支援の要請に従い講じたいかなる行動についても、要請元監督機関に手数料を課さないものとする。

8. 監督機関が別の監督機関の要請から 1 ヶ月以内に行動を講じない場合、要請元監督機関は、第 51 条(1)に基づき、所属加盟国の領域において予備的な措置を講じる能力を有するものとし、第 57 条で言及された手続きに基づき、当該事項を欧州データ保護役員会に付託するものとする。支援を完遂していないことを理由に、最終的な措置がまだ可能でない場合、要請元監督機関は、第 53 条の下での経過措置を所属加盟国の領域において講じることができる。

9. 監督機関は、当該予備的な措置の有効期間を指定するものとする。当該期間は、3 ヶ月間を超過しないものとする。監督機関は、第 57 条で言及された手続きに基づき、理由を十分に説明のうえ、当該措置を遅滞なく欧州データ保護役員会と欧州委員会に伝達するものとする。

10. 欧州データ保護役員会は、本条で言及された相互支援のための書式と手続き、並びに監督機関間及び監督機関と欧州データ保護役員会との電子的手段による情報交換の取り決め、とりわけ第 6 項で言及された標準書式を指定できる。

第56条　監督機関の共同作業

1. 協力と相互支援を強化するために、監督機関は調査業務、共同執行措置、及びその他の共同作業を遂行し、他の加盟国の監督機関からの指定構成員又は職員を関与させるものとする。

2. コントローラ又はプロセッサが複数加盟国に拠点を有する場合、或いは複数の加盟国のデータ主体が処理業務により影響を受ける可能性が高い場合、当該各加盟国の監督機関は、必要に応じて共同調査業務又は共同作業に参加する権利を有するものとする。第 54 条 a に定義された主たる機関は、関係共同調査業務又は共同作業に当該各加盟国の監督機関を関与させ、監督機関の業務参加要請に遅滞なく対応するものとする。主たる機関は、コントローラ又はプロセッサの唯一の連絡窓口として行為するものとする。

3. 監督機関は、各自、自国の法律を順守しつつ、かつ副監督機関の許可を得たうえ、主監督機関として調査業務も含めた執行権を共同作業に関与する副監督機関の構成員又は職員に与えるか、或いは主監督機関の法律により許される限りにおいて、副監督機関の法律に基づ

き副監督機関の構成員又は職員にその執行権の行使を認めることができる。当該執行権は、主監督機関からの構成員又は職員の指導下、かつ原則として主監督機関からの構成員又は職員の立会いの下においてのみ行使できる。副監督機関の構成員又は職員は、主監督機関の国内法の対象となるものとする。その行動について主監督機関が責任を引き受けるものとする。

4. 監督機関は、特定の協力活動の履行について定めるものとする。

5. 監督機関が 1 ヶ月以内に第 2 項に定める義務を順守しない場合、その他の監督機関は、第 51 条(1)に基づき、所属加盟国の領域において予備的な措置を講じる能力を有するものとする。

6. 監督機関は、第 5 項で言及された予備的な措置の有効期間を指定するものとする。当該期間は、3 ヶ月間を超えないものとする。監督機関は、理由を十分に説明のうえ、当該措置を遅滞なく欧州データ保護役員会と欧州委員会に伝達するものとし、当該事項を第 57 条で言及された体制に付託するものとする。

第 2 節
一貫性

第57 条　一貫性体制

第 46 条(1)に定める目的上、一般的範囲と個別事案の双方の事項について、本節の条文に基づき、監督機関は一貫性体制を通じて、欧州委員会と相互に協力するものとする。

第58 条 a　個別事案における一貫性

1. 第 54 条 a の意味の範囲内で法的効果を生むことを意図した措置を講じる前に、主たる機関は関係情報の全てをその他全ての所轄官庁と共有のうえ、措置草案をその他全ての所轄官庁に提出するものとする。いずれかの所轄官庁が 3 週間以内に、措置に重大な異議があることを表明した場合、主たる機関は措置を採択しないものとする。

2. 所轄官庁が主たる機関の措置草案に重大な異議があることを表明した場合、或いは主たる機関が第 1 項で言及された措置草案を提出しないか、第 55 条に基づく相互支援又は 56 条に基づく共同作業の義務を順守しない場合、この問題を欧州データ保護役員会が検討するものとする。

3. 主たる機関又はその他の関与所轄官庁と欧州委員会は、場合に応じて事実関係の要約、措置草案、当該措置の発動を必要とする根拠、提起された異議、及びその他の関係監督機関の見解も含めた関係情報を、欧州データ保護役員会に不当な遅滞なく、標準書式を用いて電子的に伝達するものとする。

4. 欧州データ保護役員会は、主たる機関の措置草案がデータ主体の基本的人権と自由に

及ぼす影響を考慮に入れつつ、問題を検討するものとし、当該問題について意見を発行するか否かを、その構成員の単純過半数票により、第 3 項に従い関係情報を提供してから 2 週間以内に決定するものとする。

5. 欧州データ保護役員会が意見の表明を決定した場合、6 週間以内に表明し、当該意見を開示するものとする。

6. 主たる機関は、欧州データ保護役員会の意見を最大限に考慮に入れるものとし、欧州データ保護役員会の委員長から意見に関する情報を入手後 2 週間以内に、措置草案と場合によっては措置草案の修正案を維持するのか修正するのかを、欧州データ保護役員会の委員長と欧州委員会に標準書式を用いて電子的に伝達するものとする。主たる機関に、欧州データ保護役員会の意見に従わない意向がある場合、それを正当化する妥当な理由を提供するものとする。

7. 欧州データ保護役員会がそれでもなお、監督機関の措置に第 5 項で言及された異議を呈する場合、1 ヶ月以内に、3 分の 2 の多数決により、監督機関を拘束する措置を採択できる。

第59条
（削除）

第60条
（削除）

第60条a　議会及び理事会への通知

欧州委員会は、欧州データ保護役員会の委員長からの報告を基に、少なくとも2年毎に定期的に、一貫性の手続きの下で対処した事項を理事会及び欧州議会に通知し、本規則の一貫性ある実施と適用の確保を視野に欧州委員会と欧州データ保護役員会の至った結論をその中に定めるものとする。

第63条　執行

1.　本規則の目的上、1 加盟国の監督機関による法的に執行可能な措置は、関係加盟国の全てにおいて執行されるものとする。

2.　監督機関が第58条(1)及び(2)に違反して措置草案を一貫性体制に付託しないか、第58条 a(1)に従った重大な異議の表明にもかかわらず措置を採択した場合、監督機関の措置は法的に効果的でなく、かつ執行可能でないものとする。

第2節
欧州データ保護役員会

第64条　欧州データ保護役員会

1.　本規則によって、欧州データ保護役員会を設立する。

2.　欧州データ保護役員会は、各加盟国の1監督機関の長と欧州データ保護監視官で構成されるものとする。

3.　ある加盟国において2つ以上の監督機関が本規則に基づく条文の適用の監視につき責任を負う場合、当該監督機関のいずれか一方の長を共同代表者に任命するものとする。

4.　欧州委員会は、欧州データ保護役員会の活動と会合に参加する権利を有するものとし、代表者を指名するものとする。欧州データ保護役員会の委員長は、欧州データ保護役員会のあらゆる活動について欧州委員会に遅滞なく通知するものとする。

第65条　独立性

1.　欧州データ保護役員会は、第66条及び第67条に従って、その業務の行使時には、独立して行為するものとする。

2.　第66条1項の(b)号及び第2項で言及された欧州委員会による要請を損なうことなく、欧州データ保護役員会はその業務の遂行にあたって誰からも指示を求めず、かつ指示を受けないものとする。

第8章
救済措置、法的責任及び制裁

第73条　監督機関に対する苦情を呈する権利

1.　その他全ての行政的救済又は司法的救済、並びに一貫性体制を損なうことなく、全てのデータ主体は、自己と関連した個人データの処理が本規則を順守していないとみなした場合に、いずれの加盟国においても監督機関に対する苦情を呈する権利を有するものとする。

2.　公共の利益のために行為し、かつ加盟国の法律に基づき適正に設立された団体、組織、又は協会は、いずれかのデータ主体の本規則の下での権利が個人データ処理の結果として侵害されたとみなした場合に、1つ以上のデータ主体に代わって、いずれの加盟国においても監督機関に対する苦情を呈する権利を有するものとする。

3.　データ主体の苦情とは別に、第2項で言及された団体、組織、又は協会は、本規則の違反が発生したとみなした場合に、いずれの加盟国においても監督機関に対する苦情を呈する権利を有するものとする。

第74条　監督機関に対して司法的救済を求める権利

1.　その他全ての行政的救済又は非司法的救済を損なうことなく、自然人又は法人は各自、自己と関係する監督機関の決定に対する司法的救済を求める権利を有するものとする。

2.　その他全ての行政的救済又は非司法的救済を損なうことなく、データ主体は各自、自己の権利保護に必要な決定がなされたいか、或いは第52条(1)の(b)号に基づき監督機関が苦情の進捗状況又は結果をデータ主体に3ヶ月以内に通知しない場合に、苦情について行動を講じることを監督機関に義務づける司法的救済を求める権利を有するものとする。

3.　監督機関に対する訴訟は、監督機関が設置された加盟国の裁判所に申し立てるものとする。

4.　一貫性体制を損なうことなく、データ主体の常居所がある加盟国とは別の加盟国の監督機関による決定と関係のあるデータ主体は、その常居所がある加盟国の監督機関に、自己に代わって他方の加盟国の所轄監督機関を相手に訴訟を申し立てることを要請できる。

5. 加盟国は、本条で言及された裁判所による最終決定を執行するものとする。

第 75 条　コントローラ又はプロセッサに対して司法的救済を求める権利

1. 第 73 条で言及された監督機関に対する苦情を呈する権利も含めた利用可能なあらゆる行政的救済を損なうことなく、自然人又は法人は各自、本規則を順守しないその個人データ処理の結果として、本規則の下でのその権利が侵害されたとみなした場合に、司法的救済を求める権利を有するものとする。

2. コントローラ又はプロセッサに対する訴訟は、コントローラ又はプロセッサが拠点を有する加盟国の裁判所に申し立てるものとする。これとは別に、コントローラがその公権の行使行為を行っている連合又は加盟国の公的機関でない限り、データ主体の常居所がある加盟国の裁判所に当該訴訟を申し立てることもできる。

3. 同一の措置、決定、又は慣行に関する訴訟が第 58 条で言及された一貫性体制において係属中である場合、データ主体の権利保護の上で、一貫性体制における手続きの結果を待つことができないほど緊急の場合を除き、裁判所は申立を受けた訴訟を保留できる。

4. 加盟国は、本条で言及された裁判所による最終決定を執行するものとする。

第 76 条　裁判手続きの共通規則

1. 第 73 条(2)で言及された団体、組織、又は協会は、1 つ以上のデータ主体により義務づけられた場合、第 74 条、第 75 条、及び第 77 条で言及された権利を行使する権利を有するものとする。

2. 監督機関は各自、本規則の条文を執行するか連合内における個人データ保護の一貫性を確保するために、法的手続きを起こし裁判所に訴訟を申し立てる権利を有するものとする。

3. 加盟国の管轄裁判所が他の加盟国において並行訴訟が提起されていると確信する合理的な根拠がある場合、当該加盟国の管轄裁判所に連絡を取り、当該並行訴訟の存在を確認するものとする。

4. 他の加盟国における当該並行訴訟が同一の措置、決定、又は慣行と関係する場合、裁判所は訴訟を保留できる。

5. 加盟国は、侵害嫌疑を解消し、関係利害への更なる損害を防止するために、暫定措置を含む措置の迅速な採択が、国内法の下で可能な訴訟によって確実に行われるようにする。

第 77 条　賠償を受ける権利及び法的責任

1. 不法な処理業務又は本規則に適合しない行動の結果として、非金銭的損害等の損害を被ったいかなる者も、受けた損害につき、コントローラ又はプロセッサに賠償を請求する権利を有するものとする。

2. 当該処理に 2 人以上のコントローラ又はプロセッサが関与する場合、第 24 条に従い責任の所在を決定した適切な書面による合意がない限り、当該コントローラ又はプロセッサは各自、損害の全額につき、連帯責任を負うものとする。

3. 損害を生じた事態につき責任を負わないことをコントローラ又はプロセッサが証明した場合、コントローラ又はプロセッサの当該法的責任をその全部又は一部につき免除できる。

第 78 条　ペナルティ

1. 加盟国は、本規則条文の違反に適用されるペナルティに関するルールを定めるものとし、コントローラが代表者の指名義務を順守しない場合も含め、その実施を確保するために必要なあらゆる措置を講じるものとする。定めたペナルティは効果的かつ均衡の取れた制止的なものでなければならない。

2. コントローラが代表者を設置している場合、コントローラに対して課しうるペナルティを損なうことなく、ペナルティを代表者に適用するものとする。

3. 加盟国は各自、第 1 項に従い採択する自国法の条文を遅くとも第 91 条(2)に明記された日付までに、かつこれに影響を及ぼすその後のあらゆる修正を遅滞なく、欧州委員会に通知するものとする。

第 79 条　行政的制裁

1. 監督機関は各自、本条に基づき行政的制裁を課す権限を与えられるものとする。監督機関は、連合内における調和的な制裁水準を保証するために、第 46 条及び第 57 条に基づき相互に協力するものとする。

2. 行政的制裁は、個別事案の都度、効果的かつ均衡の取れた制止的なものとする。

2a. 本規則に定める義務を順守しない全ての者に、監督機関は以下の制裁のうち少なくとも 1 つを課すものとする。

(a) 初回かつ故意でない非順守の場合、書面による警告。

(b) 定期的なデータ保護通常監査。

(c) 企業の場合、最大 1 億ユーロの罰金又は全世界年間収益の最大 5%の罰金のうち、いずれか多い方。

2b. コントローラ又はプロセッサが第 39 条に従い有効な「欧州データ保護シール」を所持している場合、故意又は過失による不順守の場合にのみ、第 2a 項(c)に従い罰金を課すものとする。

2c. 行政的制裁は、以下の要因を考慮に入れるものとする。

(a) 不順守の性質、重大性、及び継続期間。

(b) 違反の故意性又は過失性。

(c) 自然人又は法人の責任の程度、及び当該者による過去の違反における責任の程度。

(d) 違反の反復性。

(e) 違反の是正と違反による考えうる悪影響の緩和に向けた監督機関との協力の程度。

(f) 違反により影響を受ける特別分類個人データ。

(fa) データ主体の被った非金銭的損害も含めた損害の水準。

(fb) データ主体の被った損害を緩和するためにコントローラ又はプロセッサの講じた行動。

(fc) 違反から直接又は間接的に、意図したか得た金銭的利益、又は回避した損失。

(g) 以下に従い実施した技術的及び組織上の措置と手続きの程度。

(i) 第 23 条―設計及び初期設定によるデータ保護。

(ii) 第 30 条―処理のセキュリティ。

(iii) 第 33 条―データ保護影響評価。

(iv) 第 33 条 a―データ保護順守審査。

(v) 第 35 条―データ保護官の指名。

(ga) 第 53 条に従い監督機関の遂行する検査、監査、及び内部統制の協力拒否と妨害。

(gb) 事案の状況に適用しうるその他の悪化要因又は緩和要因。

3. （削除）

4. （削除）

5. （削除）

6. （削除）

7. 欧州委員会は、第 2 項及び第 2c 項で言及された基準と要因を考慮に入れつつ、第 2a 項で言及された行政上の罰金の絶対額を更新することを目的に、第 86 条に基づき委任法令を採択する権限を与えられるものとする。

第 9 章
特定処理データの状況に関する条文

第 80 条　個人データ処理及び表現の自由

1.　　加盟国は、欧州連合基本権憲章に基づき個人データ保護権を表現の自由の準拠ルールと調整するために必要とする場合にはいつでも、第 2 章の原則に関して、第 3 章のデータ主体の権利に関して、第 4 章のコントローラ及びプロセッサに関して、第 5 章の第三国又は国際機関への個人データの移転に関して、第 6 章の独立監督機関に関して、第 7 章の協力及び一貫性に関して、並びに第 9 章の特定処理データに関して、条文からの適用除外又は適用制限を定めるものとする。

2.　　加盟国は各自、第 1 項に従い採択した自国法の条文を遅くとも第 91 条(2)に明記された日付までに、かつこれに影響を及ぼすその後のあらゆる改正法又は修正を遅滞なく、欧州委員会に通知するものとする。

第 81 条　健康に関する個人データの処理

1.　　本規則に定めるルール、とりわけ第 9 条(2)の(h)号に基づき、健康に関する個人データの処理は、連合法又は加盟国法に基づき、その中で、データ主体の利害と基本的人権を守るために、必要かつ均衡の取れた範囲内において、かつデータ主体が以下のいずれかについて効果を予測しうる、適切かつ一貫性のある特定の措置を定めるものでなければならない。

(a)　　予防医学若しくは職業病医学、医療診断、看護若しくは治療提供、又は医療役務管理の目的により、当該データを、職務上の守秘義務を前提に健康の職業的専門家が、又は加盟国法若しくは国内管轄機関の確立したルールの下での相当の守秘義務をも前提に別の者が、その処理を行う場合。

(b)　　健康への深刻な国境間脅威からの保護、又は高水準の品質及び安全基準の確保、とりわけ医薬品若しくは医療機器向けのものなど、公衆衛生分野における公共の利益の理由により、守秘義務に拘束される者が処理を遂行する場合。

(c)　　とりわけ健康保険制度における給付又は役務の請求の手順及び医療役務の提供に用いる手続きの品質と費用対効果を確保するための、社会的保護といった分野における公共の利益のその他理由。公共の利益を理由とした健康に関する当該個人データ処理は、データ主体の同意を得ない限り、又は連合法若しくは加盟国法に基づかない限り、その他の目的によるデータ処理に帰結しないものとする。

1a.　　第 1 項の(a)から(c)号で言及された目的を個人データの使用なく達成できる場合、データ主体の同意又は加盟国法に基づく場合を除き、当該データをこれらの目的のために使用しないものとする。

1b.　　専ら科学的研究の公衆衛生目的による医療データ処理にデータ主体の同意を要する場合、1 つ以上の特定かつ類似の研究に同意を付与することができる。但し、データ主体はいつでも同意を撤回できる。

1c.　　臨床試験における科学的研究活動への参加に同意を付与するという目的については、

2001/20/EC 指令の関係条文が適用されるものとする。

2. 歴史上、統計上、若しくは科学的研究目的に必要とする健康に関する個人データの処理は、データ主体の同意を得た場合にのみ認められるものとし、第 83 条で言及された条件とセーフガードを前提とする。

2a. 国民の高い関心事に仕する研究に関しては、当該研究を別途遂行しえない場合に、第 2 項で言及された研究への同意要件の例外を加盟国法で定めることができる。対象となるデータは匿名化するか、研究目的のためにそれが可能でない場合には最高水準の技術基準の下で仮名化するものとし、データ主体の不当な再識別を防止するために全て必要な措置を講じるものとする。但し、データ主体は第 19 条に基づきいつでも拒否権を有するものとする。

3. 欧州委員会は、欧州データ保護役員会の意見を要請後に、第 1 項の(b)号で言及された公衆衛生分野における公共の利益及び第 2a 項で言及された研究分野における国民の高い関心事を更に具体化させることを目的に、第 86 条に基づき委任法令を採択する権限を与えられるものとする。

3a. 加盟国は各自、第 1 項に従い採択する自国法の条文を遅くとも第 91 条(2)に明記された日付までに、かつこれに影響を及ぼすその後のあらゆる修正を遅滞なく、欧州委員会に通知するものとする。

第 82 条 雇用におけるデータ処理の最低基準

1. 加盟国は、本規則に定めるルールに基づき、かつ均衡性の原則を考慮に入れつつ、とりわけ事業グループ内の人材採用と求職申し込みという目的、法律と団体協約により定める義務の国内法及び慣行に基づく免責も含めた雇用契約履行という目的、就業、健康、及び職場の安全に関する管理、企画、及び組織という目的も含まれるがこれらに限定されない目的のために、及び雇用と関連した権利と恩典の個別若しくは包括的な行使と享受の目的のために、並びに雇用関係解除の目的のために、雇用における従業員の個人データ処理を規制する特定のルールを法規定により採択できる。加盟国は本条に定める条文の団体協約による更なる具体化を認めることができる。

1a. 当該データの処理目的は、その収集理由と結びつけたうえ、雇用関係の範囲内でなければならない。二次的な目的のためのプロファイリング又は使用は、認められないものとする。

1b. 従業員の同意は、自由に同意を付与していないときに、雇用主によるデータ処理の法的根拠を提供しないものとする。

1c. 本規則のその他の条文にかかわらず、第 1 項で言及された加盟国の法規定には少なくとも以下の最低基準を含めるものとする。

(a) 従業員の知識のない従業員データの処理は認められないものとする。第 1 文にかかわらず、加盟国は法律により、データ削除の適切な期限を設けることによって当該慣行の許容性を定めることができる。但し、文書化しなければならない事実による裏づけを基に、従業員が犯罪を犯したか雇用において深刻な義務放棄を犯したとの疑いがあり、かつ事態の究明にデータの収集を必要とし、更には当該データ収集の性質と範囲

がその意図された目的に必要かつ均衡の取れたものである場合に限る。従業員のプライバシーと私生活をいつでも保護するものとする。調査は所轄官庁が遂行するものとする。

(b) 一般大衆にアクセス可能でなく、主に従業員がとりわけ浴室、更衣室、休憩室、及び寝室において私的な活動に使用する事業の一角についての光電子的又は音響電子的な公開監視は禁止されるものとする。秘密の監視はあらゆる状況下において許容されないものとする。

(c) 事業又は当局が診療又は適性検査において個人データを収集し処理する場合、当該データの使用目的を事前に申込者又は従業員に説明のうえ、その後に当該データを結果とともに申込者又は従業員に提供すること、並びにその意義について申込者又は従業員が要請とともに説明を受けることを確実にしなければならない。遺伝子検査及び分析の目的によるデータ収集は、原則として禁止されるものとする。

(d) 電話、電子メール、インターネット、及びその他の電気通信役務の使用を個人利用に認めるのか否かの有無とその範囲を団体協約により規制することができる。団体協約による規制がない場合、雇用主は、当該事項に関して従業員と直接合意に至るものとする。個人利用を認める限りにおいて、蓄積された通信データの処理は、とりわけデータセキュリティの確保、電気通信ネットワークと電気通信役務の適正な運用の確保、及び料金請求の目的のために認められるものとする。第 3 文にかかわらず、加盟国は法律により、データ削除の適切な期限を設けることによって当該慣行の許容性を定めることができる。但し、文書化しなければならない事実による裏づけを基に、従業員が犯罪を犯したか雇用において深刻な義務放棄を犯したとの疑いがあり、かつ事態の究明にデータの収集を必要とし、更には当該データ収集の性質と範囲がその意図された目的に必要かつ均衡の取れたものである場合に限る。従業員のプライバシーと私生活をいつでも保護するものとする。調査は所轄官庁が遂行するものとする。

(e) 労働者の個人データ、とりわけ政治的志向及び労働組合の加入と活動といった機微なデータは、いかなる状況下においても、労働者をいわゆる「要注意人物一覧」に載せるか、将来的な雇用についてそれを精査又は禁止するために使用できない。従業員の要注意人物一覧の処理、その雇用における使用、その作成、及びその回覧、又はその他の形態による差別は禁止されるものとする。加盟国は、検査を実施のうえ、本号の効果的な実施を確実にするために第 79 条(6)に基づき十分な制裁を採択するものとする。

1d. 事業グループ内の法的に独立した事業と法務助言及び税務助言を提供する職業的専門家との間の従業員個人データの送信と処理は認められる。但し、企業の業務と関連性があり、特定の業務又は事務管理手続きの実施に使用し、かつ保護に値する関係者の利害と基本的人権に反しない場合に限る。従業員データを第三国又は国際機関に送信する場合、第 5 章が適用されるものとする。

2. 加盟国は各自、第 1 項及び第 1b 項に従い採択する自国法の条文を遅くとも第 91 条(2)に明記された日付までに、かつこれに影響を及ぼすその後のあらゆる修正を遅滞なく、欧州委員会に通知するものとする。

3. 欧州委員会は、欧州データ保護役員会の意見を要請後に、第 1 項で言及された目的による個人データ処理のためにセーフガードの基準と要件を更に具体化させることを目的に、第 86 条に基づき委任法令を採択する権限を与えられるものとする。

第82条a　社会保障における処理

1.　　加盟国は、本規則に定めるルールに基づき、公共の利益において遂行する場合に、自国の公的機関及び省庁と民間機関及び部署による社会保障における個人データ処理の条件を詳述した特定の立法ルールを採択できる。

2.　　加盟国は各自、第1項に従い採択する条文を遅くとも第91条(2)に明記された日付までに、かつこれに影響を及ぼすその後のあらゆる修正を遅滞なく、欧州委員会に通知するものとする。

第83条　歴史上、統計上及び科学的研究目的の処理

1.　　本規則に定めるルールに基づき、以下に該当する場合、個人データを専ら歴史上、統計上、若しくは科学的研究目的に処理できる。

(a)　　データ主体の識別を認めないか、もはやこれ以上その識別を認めないデータの処理なくしてこれらの目的を達成できない。

(b)　　識別されたデータ主体又は識別可能なデータ主体の情報の帰属が可能なデータを、最高水準の技術基準の下でその他の情報とは別個に保管し、かつデータ主体の不当な再識別を防止するために全て必要な措置を講じている。

2.　　（削除）

3.　　（削除）

第84条　守秘義務

1.　　本規則に定めるルールに基づき、加盟国は国内法の下で又は国内所轄機関の確立したルールの下で、職務上の守秘義務又はその他の相当の守秘義務の対象となるコントローラ又はプロセッサに関して、それが個人データ保護権と守秘義務の調和が必要かつ均衡の取れたものである場合に、第53条に定める監督機関による権限を定めた特定のルールを確立していることを確実にするものとする。当該ルールは、コントローラ又はプロセッサが当該守秘義務の網羅する活動により受領したか、取得した個人データに関してのみ、適用されるものとする。

2.　　加盟国は各自、第1項に従い採択したルールを遅くとも第91条(2)に明記された日付までに、かつこれに影響を及ぼすその後のあらゆる修正を遅滞なく、欧州委員会に通知するものとする。

第85条a　基本的人権の尊重

本規則は、欧州連合条約の第6条に法制化された基本的人権と基本的な法原則を尊重する義務

を変更する効果を有しないものとする。

第 10 章

委任法令及び実施法令

第 85 条 b　標準形式

欧州委員会は、様々な部門とデータ処理状況の特徴と必要性を考慮に入れつつ、以下についての標準形式を定めることができる。

(a)　第 8 条(1)で言及された確認可能な同意を得るための特定の方法。

(b)　電子的形態も含め、第 12 条(2)で言及された伝達。

(c)　第 14 条 1 項から 3 項で言及された情報の提供。

(d)　データ主体への個人データ伝達向けも含め、第 15 条(1)で言及された情報へのアクセスの要請と付与。

(e)　第 28 条 1 項で言及された文書。

(f)　監督機関への第 31 条に従った侵害通知及び第 31 条(4)で言及された文書。

(g)　第 34 条で言及された事前協議及び第 34 条(6)に従った監督機関への通知。

2.　欧州委員会は上記にあたって、零細及び中小企業向けの適切な措置を講じるものとする。

3.　実施法令は、第 87 条(2)で言及された審査手続きに基づき採択するものとする。

第 86 条　委任の実施

1.　委任法令を採択する権限は、本条に定める条件を前提に欧州委員会に与えられる。

2.　[XXX 条]で言及された権限の委任は、本規則の発効日から不確定の期間にわたり欧州委員会に与えられるものとする。

3.　[XXX 条]で言及された権限の委任を、欧州議会又は理事会はいつでも取消とすることができる。取消の決定は、当該決定の中に明記された権限の委任を終了させるものとする。当該決定は、欧州連合官報に公表した翌日、又はその中に明記されたその後の日付に発効するものとする。当該決定は、既に発効している委任法令の有効性に影響を及ぼさないものとする。

4.　欧州委員会は、委任法令を採択次第、それを欧州議会と理事会に同時に通知するものとする。

5. [XXX 条]に従い採択した委任法令は、欧州議会及び理事会への当該法令の通知から 6 ヶ月以内に欧州議会と理事会の両方が異議を表明しない場合にのみ、或いは当該期間の満了前に欧州議会と理事会がいずれも、異議を呈しないことを欧州委員会に通知した場合に、発効するものとする。欧州議会又は理事会は自発的に、当該期間を 6 ヶ月間延長するものとする。

第 11 章
最終規定

第 91 条
発効及び適用

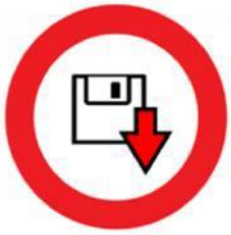
1. 本規則は、欧州連合官報にそれを公表後、20 日目に発効するものとする。

2. 本規則は[第 1 項で言及された日付の 2 年後]より適用されるものとする。

本規則は、全加盟国において全面的に拘束力を有し、かつ全加盟国において直接的に適用されるものとする。

別添1—第13条a で言及された詳細の提示

1. 第6項で言及された寸法に関しては、その詳細を以下の通りとする。

アイコン	不可欠情報	充足の有無
	個々の特定の処理目的に必要な最小限度を超えて個人データを**収集**しない	
	個々の特定の処理目的に必要な最小限度を超えて個人データを**留保**しない	
	収集目的とは異なる目的に個人データを**処理**しない	
	商業第三者に個人データを**配布**しない	
	個人データを**売却又は賃貸**しない	
	個人データを**未暗号化**形式より留保しない	

欧州連合の法律により、第 1 欄から第 3 欄の順守を要する。

2.　　第1号の表で「不可欠情報」と題した第2欄の各行にある以下の用語は太字形式とする。

(a)　　第2欄の第1行にある「収集」という用語。

(b)　　第2欄の第2行にある「留保」という用語。

(c)　　第2欄の第3行にある「処理」という用語。

(d)　　第2欄の第5行にある「売却又は賃貸」という用語。

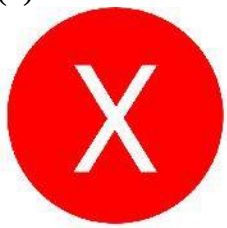
(e)　　第2欄の第4行にある「配布」という用語。

(f)　　第2欄の第6行にある「未暗号化」という用語。

3.　　第6項で言及された寸法に関し、第1号の表で「充足の有無」と題した第3欄の各行は、第4号の下で定める条件に基づき、以下の2つの図形のいずれかにより完成させるものとする。

(a)

(b)



4.

(a)　　個々の特定の処理目的に必要な最小限度を超えて個人データを収集しない場合、第1号の表における第3欄の第1行に3aで参照された図形を付すものとする。

(b)　　個々の特定の処理目的に必要な最小限度を超えて個人データを収集する場合、第 1 号の表における第 3 欄の第 1 行に 3b で参照された図形を付すものとする。

(c)　　個々の特定の処理目的に必要な最小限度を超えて個人データを留保しない場合、第 1 号の表における第 3 欄の第 2 行に 3a で参照された図形を付すものとする。

(d)　　個々の特定の処理目的に必要な最小限度を超えて個人データを留保する場合、第 1 号の表における第 3 欄の第 2 行に 3b で参照された図形を付すものとする。

(e)　　収集目的とは異なる目的に個人データを処理しない場合、第 1 号の表における第 3 欄の第 3 行に 3a で参照された図形を付すものとする。

(f)　　収集目的とは異なる目的に個人データを処理する場合、第 1 号の表における第 3 欄の第 3 行に 3b で参照された図形を付すものとする。

(g)　　商業第三者に個人データを配布しない場合、第 1 号の表における第 3 欄の第 4 行に 3a で参照された図形を付すものとする。

(h)　　商業第三者に個人データを配布する場合、第 1 号の表における第 3 欄の第 4 行に 3b で参照された図形を付すものとする。

(i)　　個人データを売却又は賃貸しない場合、第 1 号の表における第 3 欄の第 5 行に 3a で参照された図形を付すものとする。

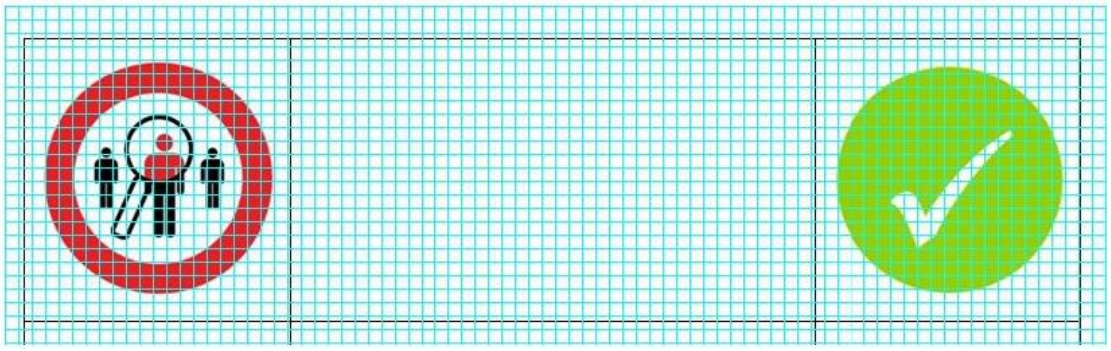
(j)　　個人データを売却又は賃貸する場合、第 1 号の表における第 3 欄の第 5 行に 3b で参照された図形を付すものとする。

(k)　　個人データを未暗号化形式により留保しない場合、第 1 号の表における第 3 欄の第 6 行に 3a で参照された図形を付すものとする。

(l)　　個人データを未暗号化形式により留保する場合、第 1 号の表における第 3 欄の第 6 行に 3b で参照された図形を付すものとする。

5.　　第 1 号にある図形のパントーン色見本は、パントーン黒 No 7547 及びパントーン赤 No 485 である。3a にある図形のパントーン色見本は、パントーン緑 No 370 である。3b にある図形のパントーン色見本は、パントーン赤 No 485 である。

6.　　以下の目盛り図による寸法については、表を縮小又は拡大した場合でも尊重するものとする。



なお規則案中、次の箇所は翻訳を割愛させていただいた。

第 18 条（削除）、第 30 条 処理のセキュリティ、第 37 条 データ保護官の業務、第 50 条 職務上の守秘義務、第 54 条 活動報告、第 58 条 包括的適用事項に関する一貫性、第 61 条 緊急措置、第 62 条 実施法令、第 66 条 欧州データ保護役員会の業務、第 67 条 報告、第 68 条 手続き、第 69 条 議長、第 70 条 議長の業務、第 71 条 事務局、第 72 条 機密性、第 80 条 a　文書へのアクセス、第 83 条 a　公文書保管に関する個人データ処理、第 85 条 教会及び宗教団体の既存のデータ保護ルール、第 87 条 委員会手続き、第 88 条 95/46/EC 指令の撤回、第 89 条 2002/58/EC 指令との関係及び修正、第 89 条 a　2001/45 規則との関係及び修正、第 90 条 審査

資料 2：欧州評議会条約 108 号条約（和訳）
出典　第一法規

個人データの自動処理に関する個人の保護のための条約（ヨーロッパ条約 108 号）
【仮訳】（1980 年 9 月）

前文

この条約の署名者である欧州評議会の加盟国は、欧州評議会の目的が、特に法の支配の尊重並びに人権及び基本的自由の尊重を基礎として、加盟国間のより大きな統合を達成することにあることを考慮し、自動処理される個人データの国境を越える流通の増大に鑑み、すべての個人の権利及び基本的自由の保護措置、特にプライバシーの尊重の権利を拡大することが望ましいことを考慮し、同時に国境のいかんを問わない情報の自由に対する加盟国の誓約を再確認し、プライバシーの尊重及び諸国民間の情報の自由な流通の基本的価値を調和させる必要性を認識して、次のとおり協定した。

第1章　総則

（目的）

第1条　この条約は、各締約国の領域において、その国籍又は居住地のいかんを問わず、すべての個人に対し、自己に関する個人データの自動処理に関する権利及び基本的自由の尊重、特にプライバシーの権利の尊重を保障すること（「データ保護」）を目的とする。

（定義）

第2条　この条約の適用上、

a　「個人データ」とは、特定された、又は特定されうる個人（「データ主体」）に関する全ての情報をいう。

b　「自動処理データファイル」とは、自動処理される一連のデータをいう。

c　「自動処理」には、自動処理手段により全部又は一部が処理される場合の操作であるデータの蓄積、当該データへの論理的又は数理的操作、当該データの改変、消去、検索又は伝播を含む。

d　「ファイル管理者」とは、国内法に従って、自動処理データファイルの目的、蓄積すべき個人データの種類及びそれらのデータに対して適用すべき操作を決定する権限を有する自然人又は法人、官庁、機関その他の全ての団体をいう。

（適用範囲）

第3条

1. 締約国は、公共部門及び民間部門における自動処理個人データファイル及び個人データの自動処理に対し、この条約を適用する。
2. いかなる国も、この条約に署名する際に、又は批准書、受託書、承認書、若しくは加入書を寄託する際に、又はその後において、欧州評議会事務総長にあてた宣言より、次のことを通知することができる。
   a　そのリストを寄託する一定の種類の自動処理個人データファイルに対してはこの条約を適用しないこと。ただし、このリストには、その国内法でデータ保護規定の適用を受ける種類の自動処理データファイルは含められない。
   したがって、国内法でデータ保護規定の適用を受ける自動処理個人データファイルの種類が追加されたときは、いつでも新たな宣言によりこのリストを補正する。
   b　法人格を有するか否かを問わず、人の集団、社団、財団、会社、法人及び直接的又は間接的に個人により構成されるその他の全ての団体にこの条約を適用すること。
   c　自動処理されない個人データファイルに対してもこの条約を適用すること。
3. ２の（b）又は（c）に定める宣言により、この条約の適用範囲を拡大した締約国は、当該拡大が一定の種類の個人データファイルのみに適用されるものであることを当該宣言において通知することができる。そのリストは寄託される。
4. ２の（a）に定める宣言により、一定の種類の自動処理個人データファイルを除外した締約国に対し、当該種類のものにこの条約を適用することを要求することはできない。
5. 同様に、２の（b）及び（c）に定める拡大のいずれかを行っていない締約国は、その拡大を行っている締約国に対し、その点についてこの条約の適用を要求することはできない。
6. ２に定める宣言は、この条約に署名する際、又は批准書、受諾書、承認書若しくは加入書を寄託する際に既に宣言を行っている国についてはこの条約が発効する時に、宣言をその後に行った国については欧州評議会事務総長が当該宣言を受領した後３ヶ月で効力を生ずる。これらの宣言は、欧州評議会事務総長あての通告を行うことにより、その全部又は一部を撤回することができる。撤回は、当該通告の受領の日の後３ヶ月で効力を生ずる。

第2章　データ保護に関する基本原則

（締約国の義務）

第4条

1. 各締約国は、この章に定めるデータ保護に関する基本原則を実施するため、その国

内法において必要な措置をとる。

2. この措置は遅くとも当該締約国に関し、この条約が発効するまでにとる。

（データの性質）

第5条 自動処理される個人データは、

a 公正かつ合法的に入手され、処理される。

b 明確化されたかつ正当な目的のために蓄積され、かつこれらの目的に合致しない形で使用されない。

c 蓄積する目的に照らして十分であり、適切であり、かつ、過剰にわたるものでない。

d 正確であり、必要な場合には最新なものに保たれる。

e 当該データが蓄積された目的のために必要とされる期間より長く、データ主体を特定できる形で保持されない。

（特別の種類のデータ）

第6条 人種、政治的意見又は宗教その他の信条を明らかにする個人データ及び健康又は性生活に関する個人データは、国内法により適当な保護措置がとられていない限り、自動処理することはできない。刑事有罪判決に関する個人データについても同様とする。

（データの安全保護）

第7条 偶発的若しくは権限のない破壊又は偶発的紛失並びに権限のないアクセス、改変又は伝播から自動処理データファイルに蓄積されている個人データを保護するため、適切な安全保護措置をとる。

（データ主体のための追加的保護措置）

第8条 何人も、

a 自動処理個人データファイルの存在、その主たる目的、及びファイル管理者の身元、現住所、又は主たる事務所を確認することができる。

b 合理的な期間でかつ過度な遅滞又は支出を伴うことなく、自己に関する個人データが自動処理データファイルに蓄積されているか否かを確認し、また、わかり易い形で当該データについて通知を受けることができる。

c この条約の第５条及び第６条に定める基本原則を実施する国内法の規定に違反してデータ処理が行なわれた場合には、それぞれの場合に応じて当該データを訂正、又は消去することができる。

d この条の（b）及び（c）にいう確認要求又はそれぞれの場合における通知、訂正若しくは消去の要求が遵守されないときは、救済を受けることができる。

（適用除外及び制限）

第9条

1. この条約の第５条、第６条及び第８条の規定に関しては、この条に定めるものを除き、いかなる適用除外も認められない。
2. この条約の第５条、第６条及び第８条の規定の制限は、締約国の国内法の規定する当該制限が次に掲げる民主主義社会に必要な措置に当たる場合に認められる。
   a　国家の安全、公共の安全、国家の財政上の利益の保護又は犯罪行為の抑止
   b　当該データ主体又は他のデータ主体の権利及び自由の保護
3. 統計又は学術研究の目的のために使用される自動処理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を侵害する危険がないことが明白である場合には、第８条の（b)、(c）及び（d）に定める権利の行使の制限を法律で定めることができる。

（制裁及び救済）

第10条 各締約国は、この章に定めるデータ保護に関する基本原則を実施するための国内法の規定に違反する行為に対する適当な制裁及び救済を措置する。

（保護の拡大）

第11条 この章のいずれの規定も、締約国が、この条約に明記されたもの以上に広範な保護措置をデータ主体に与える可能性を制限するもの、あるいはそれに影響を及ぼすものとは解釈されない。

第3章　越境データ流通

（個人データの越境流通と国内法）

第12条

1. この規定は、自動処理される個人データ又は自動処理される目的で収集された個人データが媒体の如何を問わず国境を越えて移転される場合に適用する。
2. 締約国は、プライバシー保護の目的のみを理由として、他の締約国の領域への個人データの越境流通を禁じ又は特別の許可に付してはならない。
3. しかしながら、各締約国は、次の場合、第２項の規定を制限する権利を有する。
   a　ある特定の種類の個人データ又は自動処理個人データファイルに対し、当該データ又は当該ファイルの性質を理由として、その国内法が特別の規定を含んでいる場合。ただし、相手側締約国の規定が同等の保護を定めている場合を除く。
   b　締約国の領域から他の締約国の領域の仲介を経て非締約国の領域へ移転される場合において、当該移転が移転する締約国の法令の適用を回避することになることを防ぐため。

第4章　相互援助

（締約国相互間の協力）

第13条

1. 締約国は、本条約を実施するために相互援助を行なうことに同意する。
2. そのために、
   a　各締約国は、１又は２以上の機関を指定し、そのおのおのの名称と所在地を欧州評議会事務総長あてに通報する。
   b　２以上の機関を指定した各締約国は、前号の通報を行なう際に、おのおのの機関の権限を記載する。
3. １の締約国によって指定された機関は、他の締約国により指定された機関の要請に応じ、
   a　自国のデータ保護の分野における法律及び行政慣行についての情報を提供する。
   b　プライバシー保護の目的のためにのみ、その領域内で行われる特定の自動処理に関する事実に基づく情報を提供するため、その国内法に従って全ての適当な措置をとる。ただし、処理中の個人データについては、この限りでない。

（国外に居住するデータ主体に対する援助）

第14条

1. 各締約国は、国外に居住する個人が、この条約の第８条に定める原則を実施するための自国の国内法により付与されている権利を行使することを援助する。
2. 当該個人が、他の締約国の領域内に居住しているときは、その個人は、自己の要求書を、当該締約国により指定された機関の仲介を経て提出することを選択することができる。
3. 援助の要求書の内容には、特に次のことに関する全ての必要事項を含む。
   a　氏名、住所及び要求を行う個人の身元を確認する他の関連事項
   b　要求に係る自動処理個人データファイル、又はその管理者
   c　要求の目的

（指定された機関より与えられた援助に関する保護措置）

第15条

1. １の締約国により指定された機関が他の締約国により指定された機関から情報を受け取った場合は、援助の要求に伴うものであろうと自らの援助要求に対する回答であろうと、当該情報をその援助の要求書の中に記載されている以外の目的に使用してはならない。
2. 各締約国は、指定された機関に属するか又はその代表として活動する者が当該情報に関する秘密あるいは機密についての適当な制限に拘束される様取り計らう。
3. いかなる場合においても指定された機関が第１４条第２項にいう国外に居住するデータ主体に代り、自発的に、かつ、当該個人の明示の同意なしに、援助の要求を行うことは認められない。

（援助の要求の拒否）

第16条 この条約の第１３条又は第１４条に基づき援助の要求書を提出された指定された機関は、次の場合を除き、それに応ずることを拒むことができない。

a　その要求が、回答の責任を有する機関のデータ保護分野での権限に適合しない場合。

b　その要求がこの条約の規定に従っていない場合。

c　その要求に応ずることが当該機関を指定した締約国の国家主権、安全保障及び公の秩序に適合しないか、又は当該締約国の司法的管轄下にある者の権利及び基本的自由と適合しない場合。

（援助の費用及び手続）

第17条

１．締約国が第１３条に基づき相互に供与する相互援助並びに締約国が第１４条に基づき国外にいるデータ主体に供与する援助は、いかなる費用又は報酬の支払をも発生させるものではない。ただし、専門家及び通訳に関し発生するものはこのかぎりでなく、当該費用又は報酬は、援助要請を行う機関を指定した締約国が負担する。

２．データ主体は、相手の締約国の居住者が法律上支払うこととされているものを除き、当該締約国の領域内で自己の為にとられた措置に関してのいかなる費用又は報酬の支払も求められない。

３．特に、方式、手続及び使用言語に関する援助についてのその他の細目は、直接、関係両締約国間で定めるものとする。

第5章　諮問委員会

（委員会の構成）

第18条

１．諮問委員会は、この条約の効力発生後設置される。

２．各締約国は、委員会への代表者１名及び同代理１名を指定するものとする。この条約の締約国でない欧州評議会の加盟国は、全て、オブザーバを委員会に出席させる権利を有する。

３．諮問委員会は、全会一致の決定により、そのいずれの会合にもこの条約の締約国でない欧州評議会の非加盟国をオブザーバとして出席するよう招請することができる。

（委員会の任務）

第19条 諮問委員会は、

a　この条約の適用の促進又は改善に関し、提案を行うことができる。

b　第２１条に従ってこの条約の改正を提案することができる。

c　第２１条第３項に従い、委員会に付託されたこの条約の改正提案に対し委員会としての公式見解を表明する。

d　この条約の適用に関する問題に関して、締約国の要請に基づき意見を表明することができる。

（手続）

第20条

1．諮問委員会は、欧州評議会事務総長により招集される。
その最初の会合は、この条約の効力発生の後１２ヶ月以内に開催される。その後は少なくとも２年に１回、及び締約国の代表者の３分の１が招集を要請した場合に、開催される。

2．締約国の代表者の過半数をもって諮問委員会の会合の定足数とする。

3．諮問委員会は、各会合の後、欧州評議会閣僚委員会に対し、その活動状況及びこの条約の運用に関する報告書を提出する。

4．この条約の規定に従い、諮問委員会は、その手続規則を作成する。

第6章　改正

（改正）

第２１条

1．この条約の改正は、締約国、欧州評議会閣僚委員会又は諮問委員会がそれぞれ提案できる。

2．いかなる改正提案も、欧州評議会事務総長によって、欧州評議会加盟国、及び第２３条の規定に従いこの条約に加入した又は加入を招請された全ての欧州評議会非加盟国に通報される。

3．さらに、締約国又は閣僚委員会による改正提案は、諮問委員会に対しても通報され、諮問委員会は、当該改正提案に関する意見書を閣僚委員会に提出する。

4．閣僚委員会は、改正提案及び諮問委員会により提出された意見を考慮し、その改正を承認することができる。

5．本条第４項に基づき閣僚委員会が承認した改正条文は、受諾を求めるため、締約国に送付される。

6．本条第４項に基づき承認された改正は、全ての締約国が事務総長あてに当該改正の受諾を通知した後３０日目に効力を生ずる。

第7章　最終条項

（効力発生）

第２２条

1．この条約は、欧州評議会加盟国による署名のために開放される。この条約は、批准

され受諾され又は承認されなければならない。批准書、受諾書又は承認書は、欧州評議会事務総長に寄託する。

２．この条約は、欧州評議会の５の加盟国が、前項の規定に基づきこの条約に拘束されることへの同意を表明した日の後３ヶ月の期間が満了した日の属する月の翌月の第１日に効力を発生する。

３．その後にこの条約に拘束されることへの同意を表明する加盟国に関しては、この条約は、批准書、受諾書又は承認書の寄託された日の後３ヶ月の期間が満了した日の属する月の翌月の第１日に効力を発生する。

（非加盟国の加入）

第２３条

１．この条約の発効後、欧州評議会閣僚委員会は、欧州評議会憲章第２０条（d）に規定された過半数による決定及び同委員会に出席する資格のある加盟国代表者の満場一致の議決により、欧州評議会非加盟国に対し、この条約への加入を招請することができる。

２．加入する国に対しては、この条約は、欧州評議会事務総長へ加入書が寄託された日の後３ヶ月の期間を満了した日の属する月の翌月の第１日に効力を発生する。

（領土条項）

第２４条

１．いかなる国も、署名の際に、又は批准書、受諾書、承認書若しくは加入書を寄託する際に、この条約の適用される自国領域を記載することができる。

２．いかなる国も、後日、欧州評議会事務総長にあてた宣言により、この条約の適用を当該宣言の中で特定した他の自国領域にも拡張できる。当該領域に関しては、この条約は、事務総長が当該宣言を受領した日の後３ヶ月の期間を満了した日の属する月の翌月の第１日に効力を発生する。

３．第２項に基づいてなされたいかなる宣言も、その中で特定した領域に関しては、事務総長に対する通告によりこれを撤回することができる。撤回は、事務総長が通告を受領した日の後６ヶ月の期間を満了した日の属する月の翌月の第１日に効力を生ずる。

（留保）

第２５条　　この条約の規定に関しては、いかなる留保も付することはできない。

（廃棄）

第２６条

１．締約国は、いつでも欧州評議会事務総長に対する通告を行うことにより、この条約を廃棄することができる。

２．廃棄は、事務総長が通告を受領した日の後６ヶ月の期間を満了した日の属する月の翌月の第１日に効力を生ずる。

（通告）

第２７条

１．欧州評議会事務総長は、欧州評議会加盟国及びこの条約の加入国に対して、次の事項を通告する。

a　署名

b　批准書、受諾書、承認書又は加入書の寄託

c　第２２条、第２３条及び第２４条に基づくこの条約の効力発生日

d　この条約に関連する他の全ての行為、通告又は通報

以上の証拠として、下名は正当に委任を受けてこの条約に署名した。１９８１年１月２８日にストラスブルグにおいて、ひとしく正文である英語及び仏語により本書１通を作成した。

この本書は、欧州評議会の文書保管所に寄託しておく。欧州評議会の事務総長は、欧州評議会の各加盟国及びこの条約に加入するよう招請された国全てに対して、その認証謄本を送付する。

資料３：欧州評議会追加議定書（和訳）

監督機関及び越境データ移転について個人データの自動処理に関する個人保護のための条約の追加議定書

2009 年 12 月１日発効の欧州連合条約及び欧州共同体設立条約を修正するリスボン条約。結果として、当該日付以降、欧州共同体に関する全ての言及は欧州連合として読むべきである。

前文

本個人データの自動処理に関する個人保護のための条約の追加議定書の締結国は、1981 年１月 28 日ストラスブールにおいて署名のための公開をした（以下、「条約」という。）

完全なる独立性をもって職務を執行する監督機関は、個人データの処理について個人の効果的な保護の重要な要素であることを確信する。

人々の情報の流通の重要性に考慮し、
国境を越えた個人データのやり取りの増大に伴い、人権及び基本的自由、特に個人データのやり取りに関するプライバシー権の効果的な保護を保障するのは必要であることを考慮し、以下のとおり合意した。

第１条 監督機関

１．各当事国は、条約第２章及び第３章及びこの追加議定書で言及されている原則を実施する国内法の措置の遵守を保障することについて義務を負う一つ又はそれ以上の機関を備えなければならない。

２．A　この限りにおいて、前述の機関は、本追加議定書１条１項で述べられた原則に効果をもたらせる国内法の規定の違反行為について、法的手続きを進め又は関連の司法機関に通報する権限だけでなく、特に、調査及び立入権を持たなければならない。

B　各監督機関は、個人データの処理に関し権限の範囲内でなされた自らの権利及び基本的自由に関し提出された請求を聞かなければならない。

３．監督機関は、完全なる独立性をもって自らの権限を執行しなければならない。

４．苦情を生じさせる監督機関の決定は、裁判所を通して申し立てることができる。

５．第４章の規定に従い、条約１３条の規定を損なうことなく、監督機関は義務を果たすのに必要な限りにおいて、特に全ての有用な情報をやり取りすることによって互いに

協力しなければならない。

第２条 条約の締結国の管轄下にない受領者への個人データの越境流通

１．各当事国は、条約の当事国でない国又は機関の管轄下にある受領者への個人データの移転は、その国又は機関が対象となるデータ移転について十分な保護レベルを保障する場合に限り、与えなければならない。

２．本議定書第２条１項を適用除外して、各当事国は、下記の場合に個人データの移転を許可することができる。

A　国内法で下記の理由により規定される場合

－　データ主体の特別の利益、

－　適法な社会的利益、特に重要な公的利益

B　特に契約の条項に基づく安全措置が、移転について責任を持ち、関連機関に国内法に基づき十分であると認められた管理者によって提供されている場合

第３条 最終規定

１．本議定書の第１条及び第２条は、当事国について、条約の追加的規定として解されるべきであり、条約の全ての規定は適用されなければならない。

２．本議定書は、条約の国家署名をもって署名のため公開されなければならない。条約に続いて、欧州共同体は本議定書に署名することができる。本議定書は、批准、受諾又は承認の対象となる。本議定書への署名は、事前又は同時に条約を批准、受諾又は承認もしくは条約に加盟しない限り、議定書の批准、受諾又は承認を意味しない。

３．A　本議定書は、５つの署名により第３条第２項の規定に従って議定書に従うことに同意することが表明された日の３カ月経過後の月の１日目に効力を持つ。

B　議定書に従うことへの同意を引き続き表明する本議定書への署名に関して、議定書は批准、受諾又は承認の書面の提出の日の後３カ月経過後の月の１日目に効力を持つ。

４．A　本議定書の効力発生以降、条約に加盟した全ての国は議定書にも加盟することができる。

B　欧州評議会事務総局への加盟書の提出によって加盟は効力を持ち、提出日から３カ月経過時点に続く月の１日目に効力を持つ。

５．A　全ての当事国は、欧州評議会事務総局に対する通知という手段により、いつでも本議定書を非難することができる

B　上記の避難は事務総局による通知の受領の日から３カ月経過時点に続く月の１日目に効力を持つ。

６．欧州評議会の事務総局は、欧州評議会の加盟国、欧州共同体及び本議定書に加盟したその他の国に以下のものを通知しなければならない。

A　全ての署名

B　批准、受諾又は承諾の書面の提出
C　第３条に従った本議定書の効力発生日
D　本議定書に関する法令、告知又は通知
適法に権限を持つ署名者の証として、本議定書に署名したものである。

ストラスブールで終了し、2001 年 11 月８日、英語及びフランス語で、両文書が同等に真正なものであり、一通は欧州評議会の記録保管所に提出されなければならない。欧州評議会事務総局は、認証等本を欧州評議会の加盟国、欧州共同体及び条約への加盟に招請された全ての国を伝達しなければならない。

資料４：消費者プライバシー権利章典（和訳）

消費者プライバシー権利章典は、個人データ、すなわち、データの集約を含む、特定の個人と連結可能なあらゆるデータに適用される。個人データは特定のコンピューター又はその他のデバイスと連結可能なデータを含みうる。政府は消費者プライバシー権利章典の原則を採用する連邦法を支持する。たとえ法律がなくとも、連邦取引委員会によって執行可能な行動原則のテンプレートとして、これらの権利を用いるマルチステークホルダープロセスを政府は開催する。消費者プライバシー権利章典、行動規範、及び強力な執行といったこれらの要素は、米国の消費者データプライバシーの枠組み及び国際的なパートナー間の相互運用を増強させるものとなる。

１　**個人によるコントロール：消費者は、事業者が収集する個人データ及びその利用方法についてコントロールする権利を有する。**事業者は、消費者が他者と共有する**個人データ**及び事業者が個人データを収集、利用又は開示する方法についての適切なコントロールする権利を消費者に対し提供しなければならない。事業者は、収集、利用又は開示する**個人データ**の規模、範囲、及び機微性と同様に、**個人データ**利用の機微性を反映し、利用が容易、かつアクセス可能な措置を消費者に提供することにより、これらの選択を可能としなければならない。事業者は、消費者が**個人データ**の収集、利用及び開示について有意義な決断ができるような時機及び方法によって、明確かつシンプルな選択を消費者に提供しなければならない。事業者は、消費者に対し、同意を初めに与えるのと同じ程度に利用可能かつ容易に利用できる形で、同意を撤回又は制限する方法を提供しなければならない。

２　**透明性：消費者は、プライバシー及びセキュリティの運用に関する情報を容易に理解し、その情報にアクセスできる権利を有する。**プライバシーリスク及び個人による統制を実行できるかどうかの十分な理解を得ることを消費者にとって可能にするのに最も有用な時と場所においては、事業者は、どのような**個人データ**を収集するのか、そのデータが何故必要なのか、それをどのように扱うのか、いつデータを消去又は消費者から非識別化するのか、及び第三者と**個人データ**を共有する目的について明確な記述を提供しなければならない。

３　**背景情報の尊重：消費者には、事業者が個人データを提供した提供目的と合致する方法で個人データを収集、利用及び提供することを期待する権利がある。**事業者は、法律によってそうでないと要求されていない限り、消費者との関係及び消費者がデータを最初に開示した提供目的と合致する目的に**個人データ**の利用及び開示を制限しなければならない。もし事業者が他の目的で**個人データ**を利用又は開示するのであれば、データ収集の時点において消費者にとって顕著かつ容易に実行可能な方法で他の目的を開示することによって、より高度の透明性及び個人による統制を提供しなければならない。もし収集の後に、デー

タが提供された提供目的とは異なる目的で**個人データ**を利用又は提供することを事業者が決定する場合には、高度の透明性及び個人による統制を提供しなければならない。最後に、事業者と関与する消費者の年齢及び技術の熟知度は、提供目的の重要な要素である。事業者は消費者の年齢及び洗練度に適切な方法で、この原則の義務を遵守しなければならない。特に、プライバシー権利章典の原則は、成人より子ども及び 10 代の若者から得られた**個人データ**についてより強い保護を要求することがある。

４　**セキュリティ：消費者は個人データの安全で責任ある取扱いを受ける権利がある。**事業者は、プライバシー及びセキュリティのリスクを**個人データ**の運用と関連づけて評価しなければならず、損失、すなわち権限のないアクセス、利用、破壊又は修正、及び不適切な開示などのリスクを統制するための合理的な安全措置を維持しなければならない。

５　**アクセス及び正確性：消費者は、利用可能な書式で、データの機微性及びデータが不正確であった場合に消費者に生じる逆の結果のリスクについて適切な方法で個人データにアクセスし、訂正する権利を有する。**事業者は、正確な**個人データ**を維持していることを保障するため合理的な措置を取らなければならない。事業者はまた、消費者に収集及び保有する**個人データ**への合理的なアクセスとともに、不正確なデータを訂正又は削除又は利用制限を要求する適切な方法及び機会を提供しなければならない。**個人データ**を扱う事業者は、表現の自由及び取材の自由と矛盾しない方法でこの原則を解釈しなければならない。事業者が消費者に対し、正確性を維持し、アクセス、訂正、削除又は制限権を提供するために利用できる方法を決定するにあたっては、事業者は、収集及び維持する**個人データ**の規模、範囲及び機微性及び**個人データ**の利用により消費者が経済的、身体的、その他物質的な損害に晒される可能性を考慮に入れなければならない。

６　**焦点を当てた収集：消費者は、事業者が収集及び保持する個人データにつき合理的な範囲で制限を加える権利を有する。**事業者は、利用目的尊重原則の下において特定された目的を達成するために必要な範囲に限って**個人データ**を収集すべきである。事業者は、一度**個人データ**が不要になれば、法的義務がない限り、安全に**個人データ**を開示又は非識別化しなければならない。

７　**説明責任：消費者は、事業者がプライバシー権利章典を守ることを保障するための適切な措置により個人情報を取り扱われる権利を有する。**事業者は、これらの原則の遵守について、執行機関及び消費者に対し説明責任を負わなければならない。事業者はまた、これらの原則の遵守について、従業員にも責任を負わせるべきである。この目的を達成するため、事業者は従業員を必要に応じて**個人データ**をこれらの原則と一貫した取扱をし、かつ、この観点から従業員の業績を定期的に評価するよう教育しなければならない。必要な場合には、事業者は全面監査を行わなければならない。**個人データ**を第三者に開示する事業者は、法令により除外されていない限り、最低限、この原則を守るための執行可能な契約上の義務が受領者に課されることを保障しなければならない。

以上