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

はじめに

1　個人情報保護制度における国際的水準の検討

個人情報保護の取組を推進するにあたっては、OECDをはじめとして、APEC、EUなど様々な場で進められている取組を踏まえ国際的な協調を図っていくとともに、わが国の法制度についても国際的な理解を求めていくことが重要であるとされている。(「個人情報の保護に関する基本方針（平成16年4月閣議決定、平成20年4月25日一部変更、平成21年9月1日一部変更)」)

EUデータ保護指令25条は、各国が国内法を整備するに際し、「十分なレベルの保護（adequate level of protection)」(以下「十分性」(adequacy）という。）を確保している場合に限り、個人データの第三国への移転を認めるように規定しなければならないことを定めている。EUにより「十分性」を認定された国・地域は9つに上る(2012年3月現在)が、日本はまだ「十分性」の認定を得ていない。「十分性」概念は、EUデータ保護指令にとどまらず、韓EU・FTAでも個人情報保護制度の水準を表すものとして取り入れられており、自由貿易協定等の国際交渉の場面でも重要な意味を持つ可能性がある。

また、OECDにおいてもプライバシーガイドラインの改正の動きがあり、データ保護・プライバシーコミッショナー会議は2009年に国際標準草案を採択し、翌2010年には同会議の参加の要件を緩和するなど、個人情報保護制度について国際社会が求める水準につき、議論が活発化している状況が存在する。

我が国でも、消費者委員会に設けられた個人情報保護専門調査会の報告書で「我が国の法制度に対する国際社会の理解を求めていくとともに、国外で活動する事業者等のニーズも踏まえつつ、協調の在り方を検討する必要がある。」とされている（平成23年7月26日)。また、内閣官房に設置された社会保障・税番号制度の個人情報保護ワーキンググループの報告書でも、EUデータ保護指令の十分性の要件に配慮した記述が存在する（「個人情報保護ワーキンググループ報告書（平成23年6月23日)」)。

個人情報保護制度における国際的水準については、平成21年度に行った調査（「国際移転における企業の個人データ保護措置調査　報告書」平成22年3月）において国際標準草案の検討が含まれていたが、上記のように、特にEUデータ保護指令の「十分性」概念の重要性が増しており、多面的に議論されている状況に鑑みると、「十分性」概念を含む個人情報の保護水準をめぐる国際的な議論についてより詳細に把握しておく必要がある。

そこで、本調査では、個人情報保護制度の国際的水準について、個人情報保護制度に関する有識者による委員会を設置し、文献調査のみならず、可能な限り、関係者や現地の研究者などから調査を行うことによって、特にEUデータ保護指令の「十分性」審査について分析し、今後の制度検討・政策決定に資することを目的とした。

2　個人情報保護をめぐる議論の活発化

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で検討を開始した後、個人情報保護をめぐる議論は、これまでよりも更に活発化してきた。

2012年に入ってからの主な動きを見ると、次のようになる。

ア 2012年1月25日　欧州連合、個人データの取扱いに係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の規則（一般データ保護規則）提案（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)公表

イ 2012年2月14日　日本政府、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案閣議決定、国会提出

ウ 2012年2月23日　アメリカ合衆国ホワイトハウス、ネットワーク世界における消費者データ・プライバシー：グローバルなデジタル経済におけるプライバシー保護及びイノベーション促進のための枠組み（COSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY）公表

エ 2012年3月19日　欧州委員会ビビアン・レディング副委員長及び合衆国ジョン・ブライソン商務長官による欧州連合・合衆国データ保護共同声明（EU-U.S. joint statement on data protection by European Commission Vice-President Viviane Reding and U.S. Secretary of Commerce John Bryson）公表

オ 2012年3月26日　アメリカ合衆国連邦取引委員会（Federal Trade Commission)、急激な変化の時代における消費者のプライバシー保護：ビジネス及び政策立案者への勧告（Protecting Consumer Privacy in an Era of Rapid Change：Recommendations For Businesses and Policymakers）公表

これらのいくつかについては、それぞれ関連したところで取り上げられるので、参照されたい。

3　検討委員会の構成

◎堀部政男　　一橋大学名誉教授　情報法
庄司克宏　　慶應義塾大学教授　EU法
國見真理子　　田園調布学園大学専任講師　国際経済法
加藤隆之　　亜細亜大学准教授　憲法
宮下紘　　駿河台大学准教授　憲法・英米法
高谷知佐子　　森・濱田松本法律事務所　弁護士

河井理穂子　　埼玉工業大学専任講師／国立情報学研究所特任助教　情報法・知的財産権法

◎は委員長

オブザーバ　小山洋平　森・濱田松本法律事務所　弁護士

消費者庁消費者制度課個人情報保護推進室政策企画専門官・弁護士の板倉陽一郎氏は、全体の企画、調査、調整など全体にわたって大きな役割を果たしたことを特記したい。

4　本報告書の構成

本報告書は、次のような構成になっている。

はじめに

堀部委員長

1　個人情報保護制度における国際的水準の理論面

(1) EUデータ保護指令における「十分性」審査についての概要

事務局

(2) 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

庄司委員

(3) 国際経済法の観点からみたEUデータ保護指令に関する検討

國見委員

2　個人情報保護制度における国際的水準の実践面

(1) 欧州委員会

・国際的水準の意義

堀部委員長

・EUデータ保護改革と国際的水準への影響

宮下委員

(2) イスラエル

宮下委員

(3) ウルグアイ

河井委員

(4) ニュージーランド

加藤委員

(5) インド

高谷委員・小山オブザーバ

あとがき

堀部委員長

資料　EUデータ保護指令仮訳

5　本報告書の特徴

個人情報保護制度における国際的水準については、これまでにも様々な議論が展開されてきた。

国際的には、前述のように、特にEUデータ保護指令の「十分性」概念の重要性が増しており、「十分性」概念を含む個人情報の保護水準をめぐる国際的な議論についてより詳細に把握しておく必要があることから、文献調査ばかりでなく、可能な限り、関係者や現地の研究者などから調査を行うことによって、EUデータ保護指令の「十分性」審査について分析し、今後の制度検討・政策決定に資することを目的とした。

本報告書は、まず第一に、「十分性」の問題を正面から分析したものであるという特徴を持っている。「EUデータ保護指令における『十分性』審査についての概要」（事務局）をはじめ、各委員の議論は、様々な検討をしつつ、「十分性」に論及している。

第二に、国際的水準について、EU法・国際経済法の観点から論じているところに大きな特徴がある。「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」（庄司克宏）は、EU法の観点から個人データ保護法制について検討している。2007年12月13日リスボン条約が署名され、2009 年12月1日発効したリスボン条約の後のEUデータ保護法制における基本権保護はもとより、「十分性」について規定しているEUデータ保護指令やそのいくつかの条項がEU法体系の中でどのように位置づけられているかを明らかにしている。また、「国際経済法の観点からみたEUデータ保護指令に関する検討」（國見真理子）は、世界貿易機関（World Trade Organization）（WTO）という1995年に設立された国際機関との関係でEUの個人データ保護の国際移転の規制を検討し、EU側はこの規制を専ら人権問題と考えるため、EUの規制がWTOの問題になり得るかについては疑問が残るとしながらも、十分性認定を得ていない国としては、国内での個人情報保護の取組と並行して、WTOの二国間協議の場でEU 側と話し合う機会を持つことも選択肢から排除すべきではないとしている。

第三に、関係者や現地の研究者などからの聞き取り調査を踏まえて関係法令について検討しているところに特徴がある。欧州委員会関係では、「国際的水準の意義」（堀部政男）、「EUデータ保護改革と国際的水準への影響」（宮下紘）が、欧州委員会司法総局をはじめ、研究者・弁護士等からの聞き取り調査を含めてまとめている。また、2011年1月31日欧州委員会決定で十分性を認められたイスラエル（宮下紘）、2012年3月現在では、欧州委員会の決定は出ていないが、2010年10月12日第29条作業部会で十分性を認められたウルグアイ（河井理穂子）及び同じく欧州委員会の決定は出ていないが、2011年4月4日第29条作業部会で十分性を認められたニュージーランド（加藤隆之）は現地調査を踏まえた取りまとめである。さらに、欧州委員会と非公式な議論を行っているインド（高谷知佐子・小山洋平）は、IT関係で注目を集めている国のIT法や2011年個人情報保護規則等について現地調査も交えてまとめている。

6　表記について

本報告書は、上記のように、委員会の各委員が外国の法令・文献等、聞き取り調査等を基に執筆したものからなっている。基本的な表記については「統一訳語表」を作成し、統一した。しかし、それら以外については、各執筆者の表記を尊重した。そのため、必ずしも統一されていない場合があることをお断りしたい。

7　謝辞

最後になったが、今回の調査でお世話になった方々に感謝を申し上げたい。

ヒアリングでは、欧州委員会司法総局、ベルギー・ナミュール大学Cécile de Terwangne教授、ベルギー・ブリュッセル自由大学Paul De Hert教授、ベルギー・リンクレーターズ法律事務所Tanguy Van Overstraeten弁護士、イスラエル法・情報・技術機関長Yoram Hacohen氏、同法務課長Amit Ashkenazi 氏、イスラエル・College of Management School of Law、Omer Tene准教授、URCDP（ウルグアイ個人情報保護法担当監督機関）Mag. Federico Monteerde氏、ウルグアイ・Citizen's Officeの Dra. Esc. Beatriz Rodriquez Acost氏及びDra.esc. Prof. Maria Jose Viega Rodriguez 氏、ウルグアイ・リパブリカ大学Dra. Ana Brian Nougreres教授、ニュージーランド・プライバシーコミッショナー事務局Blair Stewart准コミッショナー、ニュージーランド・Law Commission のJohn Burrows委員長（教授）、ニュージーランド・オークランド大学Gehan Gunasekara准教授、ニュージーランド・オタゴ大学Paul Roth教授、インド・Ministry of Communication & IT のDr.Gulshan Rai氏、インド・Data Security Council of India のDr. Kamlesh Bajaj氏、その他多くの方々にご協力を頂いた。ヒアリング先各国の大使館、特に欧州連合日本政府代表部の井上淳書記官、阪口理司書記官、田中信彦書記官には現地調査の円滑な実施にご配慮を頂いた。また、検討委員会における議論には総務省、外務省、経済産業省からのオブザーバの参加を得、有益な意見交換を行うことができた。

平成24 年（2012年）3月

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委員長

堀部　政男

目次

1　個人情報保護制度における国際的水準の理論面

＜1＞　EU データ保護指令における「十分性」審査について

事務局[1]

1　EU データ保護指令第 25 条とは

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 1995 年 10 月 24 日の欧州議会及び理事会の 95/46/EC 指令（1995 年 10 月 24 日採択、1998 年 10 月 24 日発効。以下「EU データ保護指令」又は単に「指令」という。）において、個人データの第三国への移転は、原則として「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」（指令 25 条 1 項）と定められている。

2012 年 3 月現在、日本は EU から「十分なレベルの保護措置」を確保している国であるか否かの判断がされていない。

「十分なレベルの保護措置」に該当するかどうかの判断については、第 29 条作業部会*による“*Working Document: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive* (*24 July 1998*)”（以下「WD」という。）に基づき、以下のとおり解説が示されている。

（参考）

*欧州委員会司法総局・第 29 条作業部会（以下「第 29 条作業部会」という。）

・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。

1　本稿は宮下紘委員の全面的な協力を得つつ、板倉陽一郎（消費者庁消費者制度課個人情報保護推進室政策企画専門官・弁護士）において整理したものである（第 1 回検討委員会資料として配布された）。なお本稿のうち意見に渡る部分は、板倉の個人的見解であり、所属する組織の見解ではない。（他の執筆部分の取扱いも同様である）

2　欧州委員会に十分性を認定された国・地域

2000年7月26日	スイス
2001年12月20日	カナダ
2003年6月30日	アルゼンチン
2003年11月21日	ガーンジー島
2004年4月28日	マン島
2008年3月8日	ジャージー島
2010年3月5日	フェロー諸島
2010年10月19日	アンドラ
2011年1月31日	イスラエル

（2012年3月現在）

上記の国・地域のほか、第29条作業部会の意見において十分な保護水準を確保していると認められた国・地域は、ウルグアイ（2010年）、ニュージーランド（2011年）がある。

3 「十分なレベルの保護措置」の審査基準

WDによれば、EU指令に基づく特定国の「十分な保護水準」の審査には、次の原則と手続・執行の構造が検討事項とされている。

（ｉ）内容の原則（content principles）：

① 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条）

② 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。

③ 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）

④ 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。

⑤ 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。

⑥ 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。

（ii）手続・執行の構造：（procedural/enforcement mechanisms）

独立した機関の形態をなす「外部監督」の制度*が、データ保護の法令遵守の制度として必要である。データ保護の制度の目的は、以下の３点である。

① 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。

② 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。

③ 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課すことができる体制が関与しなければならない。

*外部監督の制度

指令28条により、データ保護に関しては職権行使にあたって「完全に独立して活動」する機関（いわゆる、プライバシー・コミッショナー）が監督することが要求されている（ただし28条はEUの構成国に対して適用される条文であり、十分性認定における外部監督の制度において「完全な独立性」までが求められているかどうかは、明らかではない)。この機関には、データへのアクセス権限、調査権限、違反に対する法的措置の権限等が付与されなければならない。主要国の監督機関の運用実態については、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』(2011年3月）参照。

4　主な国・地域の審査結果

前述のとおり、2012年3月現在、欧州委員会の決定として十分な保護水準を確保していると認められた国・地域は、スイス（2000年）、カナダ（2001年）、アルゼンチン（2003年）、ガーンジー島（2003年）、マン島（2004年）、ジャージー島（2008年）、フェロー諸島（2010年）、アンドラ（2010年）、イスラエル（2011年）の9つである。また、上記の国・地域のほか、第29 条作業部会の意見において十分な保護水準を確保していると認められた国・地域は、ウルグアイ（2010 年）、ニュージーランド（2011年）がある。

このうち、カナダは、2001年1月に「個人情報保護及び電子文書法」（PIPEDA）を施行。2004年までに3段階に分けて民間事業者の対象範囲を広げ、2004年1月に全面施行となった。2001年12月20日の欧州委員会決定で、適切な保護水準の国と認められる。セグメント方式では、初めてEUデータ保護指令に準拠した事例。連邦政府部門対象の「連邦プライバシー法」、民間部門対象のPIPEDA、州政府対象の州法等、複数の法律を組み合わせることにより、ほぼ全ての機関を対象とした法的枠組みを形成した。

また、アメリカ、オーストラリアのEUデータ保護指令への対応状況は以下のとおりである。

（1）アメリカ：

民間の自主規制を尊重し、またセクトラル方式で法整備を進めるアメリカにおいては、法制によるEUデータ保護指令への準拠は困難である。このため、特定の認証基準を設け、その認証を受けた企業ごとに十分性を付与する「セーフハーバー原則」のための交渉を1998年より実施し、2000年に協定を締結している。アメリカ企業がセーフハーバーに参加することは任意であるが、参加可能な企業は連邦取引委員会（FTC：Federal Trade Commission）及びアメリカ運輸省の管轄にある企業に限られており、連邦準備理事会（FRB）管轄の金融機関や、コモンキャリア、航空会社、貨物及び倉庫会社は含まれていない。2004年末のEU委員会の監査においては問題点が多く指摘され、①原則遵守の意思表明の必要性、②連邦政府（商務省）の強力な指導とモニタリングの必要性、③違反者に対する強力な影響力の行使の必要性などが連邦政府に要請された。

欧州委員会委員であるヴィヴィアン・レディングは2011年12月6日のスピーチの中で「米国の自主規制はEUと米国の完全な相互通用性を満足させるものとは考えていない」と述べているが[2]、2012年3月19日の米国商務長官ジョン・ブライソンとの共同声明では、「米国・欧州連合間のセーフハーバーの枠組みを尊重することを再確認」するとしている[3]。

2　Viviane Reding Vice-President of the European Commission, EU Justice Commissioner The future of data protection and transatlantic cooperation Speech at the 2nd Annual European Data Protection and Privacy Conference Brussels, 6 December 2011 (http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/851&forma t=HTML&aged=0&language=EN&guiLanguage=en)

3　EU-U.S. joint statement on data protection by European Commission Vice-President Viviane Reding and U.S. Secretary of Commerce John Bryson (http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/192)

（2）オーストラリア：

1988年施行の「プライバシー法」の適用範囲を民間事業者にまで広げた「プライバシー修正法」を2000年に施行。これにより、法形式はセクトラル方式からオムニバス方式へと改変された。（ⅰ）年商300万豪ドル未満の小規模事業者及び被雇用者のデータが規制対象外とされたこと、（ⅱ）一般に利用可能な個人データが規制対象外とされたこと、（ⅲ）データ取得時の本人への通知が困難な場合には、事後に通知してもよいとされたこと、（ⅳ）ダイレクト・マーケティングが主目的のデータ利用について、オプトアウトが認められていないこと、（ⅴ）センシティブ・データの規制が収集のみで、利用や開示についての規制がないこと、（ⅵ）EU市民の個人データについて、本人の訂正請求権が認められていないこと、（ⅶ）EUから取得した個人データをオーストラリアから第三国へ移転することが規制されていないこと等を理由に、保護水準が不十分とされた。

2011年12月現在も、オーストラリアは法改正の作業中である。

5 「十分性」審査の留意点等

WDは、3で述べた内容のほか、十分性の運用面、またEUデータ保護指令25条2項における十分性がない場合における対処方法、さらに、26条1項の例外規定等、下記の点に留意することが記されている。

（1）欧州評議会条約第108号

欧州評議会条約第108号はデータ保護に関する唯一の拘束力ある国際文書であるが[4]、第三国移転に関する規制がないという弱点がある。もっとも、（ｉ）当該国に法令遵守を確保するための適切な体制が整備されていること、（ii）当該国が、データを中継地として移転されず、十分性の要件を満たさない国への移転をしないことを充足している場合、欧州評議会108協定によりデータ保護指令の25条1項のもとデータの第三国移転が許容される。

（2）事業者の自主規制

データ保護指令25条2項は「あらゆる状況」に照らして第三国による保護の水準を審査すると規定されており、事業者の自主規制が考慮されなければならない。特定の自主規制の規則又は文書については、以下の3点が考慮されなければならない。

① 十分な法令遵守の水準…規則の存在に対する高い意識、消費者に対する透明性確保、監査等による外部検証、法令違反に対する罰則の性質と執行が存在するかどうか。

② データ本人の支援と援助…データ本人からの苦情を調査する必要な権限を備えた中立かつ独立した制度が存在するかどうか。

③ 適切な救済…損害に対してデータ本人が利用できる救済方途が存在するかどうか。

以上のとおり、上記2「十分なレベルの保護措置」の審査において示された客観的かつ機能的アプローチを用いた自主規制の評価、個人データが移転された全ての構成員を拘束するものでなければならないこと、文書の透明性があり、核心となるデータ保護原則が含まれていること、一般的な法令遵守の十分な水準を確保している体制があること、データ本人からの苦情を処理し、規則違反に対する裁定する、容易にアクセスができ、中立で独立した機関が存在すること、法令違反に対する適切な救済が保証されていることが必要となる。

（3）契約条項の役割

データ保護指令26条2項の標準契約約款*により「不十分な」第三国へのデータの移転が認められる。契約締結という考え方は1992年に欧州評議会（Council of Europe）、国際商工会議所（the International Chamber of Commerce）、及び欧州委員会（the EuropeanCommission）が共同してこの問題に取り組んできたことに始まり、現実世界においてデータの移転に関する問題に対処してきた。

---

4 内容については堀部政男「EU における個人データの国際移転に関する実態」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・報告書』（2010 年3 月）9-57 頁参照。

契約は、データがEU域外に移転される際にデータ管理者によって十分な安全管理措置が施される手段である。そのため、契約の規定は、所与の状況において保護の不可欠な要素を含む十分な保護の一般レベルの欠如を埋め合わせるものでなければならない。

26条2項において用いられている「十分な保護措置」の意味を評価するには次の点に留意する必要がある。

① 実質的なデータ保護規則

第三国へのデータ移転の処理には、①目的利用制限の原則、②データの質・比例の原則、③透明性の原則、④安全の原則、⑤アクセス・訂正・消去の権利、⑥契約の非当事者へのデータ移転の制限といった基本原則が当てはまる。さらに、センシティブ・データやダイレクト・マーケティング、自動処理に関する原則が適用される状況もありうる。また、これらの原則はデータの受け手が遵守できるように詳細なものでなければならない。

② 実質的な規則の効果的実施

データ保護の体制の効果の水準については、その体制の能力として①法令遵守の良好な水準の調達、②個人のデータ主体への支援と援助の提供、③重要な要素である、損害を受けた当事者に対する適切な救済の提供である。

③ 法適用の問題

データ移転の受け手が当該国の法令によって警察、裁判所、税務署等の機関に対し個人情報を開示する可能性があるが、EUデータ保護指令16条によれば、法がそうすることを要求するものでない限り、データ管理者が個人情報を開示することが許されるものではない。しかし、このような開示はEUデータ保護指令13条1項における「公序（ordre public)」のひとつのために民主主義社会において必要な場合に限られるべきである。

④ 契約締結のための実務上の考慮事項

標準的な契約書式を作成することを排除するものではないが、個々の事情に適合するように個々の契約は作成されなければならない。なお、EU域外において処理が行われる契約の不履行の調査が困難であることが指摘される。そのため、契約による解決が適切な場合と契約が十分な保護を保証することができない場合もある。そこで、クレジットカード取引や航空券予約等に用いられるような大規模な国際ネットワークが公的な審査や規制に服するように参考となりうる。

*標準的契約約款（standard contractual clauses）

標準的契約約款について、欧州委員会は2001年、2004年、2010年にそれぞれ標準的な契約に関する決定を公表している。詳細については、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）92頁以下、参照。

（4）十分性要件の例外

26条1項は第三国移転のための「十分性」要件から免除される場合を規定している。

①データ主体本人の明確な同意がある場合

②データ主体と管理者との間の契約履行または契約締結前の措置に必要な場合

③ データ主体の利益のために管理者と第三者との間の契約締結または履行に必要な場合
④ 重要な公共の利益を根拠としてまたは国際的な訴訟ないし法的手続において必要ないし法的の要求される移転の場合
⑤ データ主体本人の重大な利益の保護のため必要な場合
⑥ 法令によって公衆に情報提供し、公衆または正当な利益を有する者による閲覧のために公開されている記録から移転される場合

（5）手続的問題

当作業部会は、次の類型の移転については特に注意を要するものと考えている。
① EUデータ保護指令8条に定義されるデータのセンシティブな類型を伴う移転
② 財政的な損失の危険のある移転
③ 個人の安全へのリスクをもたらす移転
④ 個人に重大な影響を及ぼす決定を目的としてなされた移転
⑤ 個人の名声への重大な悪影響を及ぼしたり低下させたりする危険のある移転
⑥ 個人の私生活への重大な侵入（迷惑な電話勧誘）をなす行為をもたらす移転
⑦ 大量データの反復移転
⑧ 新たな技術を用いたデータ収集を伴う移転

6　日本の法制度に対するEU調査の結果

2010年1月20日、欧州委員会は「特に科学技術の発展に照らしたプライバシーの新たな課題に対する異なるアプローチに関する比較研究」調査（*Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments*）を公表した。同調査では、日本を含む11か国（チェコ、デンマーク、フランス、ドイツ、ギリシャ、イギリス、アメリカ（連邦・カリフォルニア州・ニュージャージー州）、オーストラリア、香港、インド、日本）の個人情報保護法制の動向を紹介し、その分析を行っている。

日本については、ニュー・サウス・ウェールズ大学Graham Greenleaf教授が担当し、「日本の法律はまだ4年間しか執行されておらず、暫定的な評価は困難である。さらに、日本では、訴訟ではなくインフォーマルな紛争解決に関する法制度に依拠している。省庁が収集した資料、コンプライアンス、データ違反、救済に関する公表資料から、日本の法律が効果的であることの証拠がないと判断することは合理的であろう」と指摘されている。また、国際基準からした日本の位置づけについて、「日本のデータ保護制度はOECDガイドラインの基準を満たしている。また、APECプライバシー・フレームワークの基準を満たしていることも疑いはない。EU指令との関係になるとこのレポートの範囲を超えるもので、難しい判断となる」と述べられている。

（EUデータ保護指令参照条文）

Ⅳ章　第三国への個人データの移転

第25条　原則

1. 構成国は、取り扱われている又は移転後に取扱い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に実体的効果を持つことなく、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。
2. 第三国によって保障される保護のレベルの十分性は、一つのデータ移転作業又は一連のデータ移転作業に関するあらゆる状況に鑑みて評価されなければならない。特に、データの性質、予定されている取扱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、並びに当該第三国において遵守されている職業上の規則及び安全保護対策措置が考慮されなければならない。
3. 構成国及び委員会は、第三国が第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ないと考えられる事例について、相互に情報提供しなければならない。
4. 構成国は、第31条第２項に規定する手続に基づいて委員会が、第三国が本条第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ないと認定した場合には、当該第三国への同一タイプのデータの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。
5. 委員会は、適切な時期に、第４項に基づく認定によってもたらされる状況を改善することを目的とする交渉を開始しなければならない。
6. 委員会は、第31条第２項に規定する手続に基づいて、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。

　構成国は、委員会の決定を遵守するために必要な措置を講じなければならない。

第26条　例外

1. 構成国は、第25条の適用を制約するものとして、及び特別な場合を規律する国内法に別段の定めがある場合を除いて、第25条第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ない第三国に対する個人データの移転又は一連の移転は、次の条件を満たした場合に行うことができることを定めなければならない。

（ａ）データ主体が、予定されている移転に対して明確な同意を与えている場合。又は、

（ｂ）移転が、データ主体及び管理者間の契約の履行のために、又はデータ主体の請求により、契約締結前の措置の実施のために必要である場合。又は、

（ｃ）移転が、データ主体の利益のために、データ主体及び第三者間で結ばれる契約の締結又は履行のために必要である場合。又は、

（ｄ）移転が、重要な公共の利益を根拠として、又は法的請求の確定、行使若しくは防御のために必要である場合、又は法的に要求される場合。又は、

（ｅ）移転が、データ主体の重大な利益を保護するために必要である場合。又は、

（ｆ）法律又は規則に基づいて情報を一般に提供し、及び公衆一般又は正当な利益を証明する者のいずれかによる閲覧のために公開されている記録から、閲覧に関する法律に規定された条件が特定の事例において満たされる範囲内で、移転が行われる場合。

2. 構成国は、第1項の規定に実体的な効果を持つことなく、管理者が個人のプライバシー並びに基本的な権利及び自由の保護、並びにこれらに相当する権利の行使に関して、十分な保護措置を提示する場合には、第25条第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ない第三国への個人データの移転又は一連の移転を認めることができる。当該保護措置は、特に適切な契約条項から帰結することができる。

3. 構成国は、第2項によって付与された許可を、委員会及び他の構成国に通知しなければならない。

一つの構成国又は委員会が、個人のプライバシー並びに基本的な権利及び自由の保護を含む正当な理由に基づいて異議申立てを行った場合には、委員会は、第31条第2項に規定された手続に基づいて適切な措置を講じなければならない。

構成国は、委員会の決定を遵守するために必要な措置を講じなければならない。

4. 構成国は、第31条第2項に規定された手続に従って、一定の標準契約条項が本条第2項によって要求される十分な保護措置を提供していると決定する場合には、委員会の決定を遵守するために必要な措置を講じなければならない。

＜2＞　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

慶應義塾大学大学院法務研究科教授（ジャン・モネ・チェア）
庄司　克宏

1　リスボン条約と個人情報保護法制

（1）リスボン条約による改正前のEU

欧州連合（EU）条約すなわちマーストリヒト条約（1992年2月7日署名、93年11月1日発効）は、超国家的な性格を有する欧州共同体（EC）条約とは異質でありながら、ECと共通の制度的枠組みを有するEUを創設した。同条約第A条3段には、「連合は欧州共同体に基礎を置き、本条約により確立される政策及び協力形態により補完される」と規定されていた。

超国家的統合を基本とする「欧州共同体」は複数形（ECs）で表記され、ECのほか欧州石炭鉄鋼共同体（ECSC、2002年7月23日まで）及び欧州原子力共同体（Euratom）が含まれるが、一般的経済統合を目的とするEC が中心的存在であった。「〔EU〕条約により確立される政策及び協力形態」とは、EC諸機関を共有しつつも政府間協力を基本とする共通外交・安全保障政策（CFSP）および警察・刑事司法協力（PJCC、1997年10月2日署名、99年5月1日発効のアムステルダム条約により改正される前は司法内務協力JHA）を指す。

このような組織構造は「三本柱構造」と呼ばれた。欧州理事会の政治的指針の下、理事会、欧州議会及びコミッション（欧州委員会）は、3つの柱ごとに異なる権限を行使した。これらの諸機関は、別個の国際法人格を有するEC、Euratom、ECSC（2002年7月23日廃止）および狭義のEU（黙示的国際法人格）を運営した[1]。以上の点を法秩序の面から整理すると図表1のようになる。

この枠組みの下で、1995年10月24日付EUデータ保護指令95/46（〔1995〕OJ L 281/31）はEC法として制定される一方、警察・刑事司法協力の枠組みにおいて処理される個人データ保護に関する枠組決定2008/977（〔2008〕OJ L 350/60）はEU法（狭義）として制定された。

図表1

<table>
<tr><td colspan="3">EU法（広義）
（EU法（狭義）＋EC法）</td></tr>
<tr><td colspan="2">EU法（狭義）
（EU条約＋実施措置など）</td><td>EC法＊
（EC条約＋派生法など）</td></tr>
<tr><td colspan="2">政府間協力（国際法）</td><td>超国家的法秩序</td></tr>
<tr><td>共通外交・安保政策
（CFSP）</td><td>警察・刑事司法協力
（PJCC）</td><td>域内市場</td></tr>
</table>

＊ EC法は、広義にはEC、Euratom、ECSCの各条約および派生法等を含む概念である。

（庄司克宏著『EU法　基礎篇』岩波書店、2003年、5頁）

（2）リスボン条約による改正後のEU

欧州憲法条約（2004年10月29日署名）の批准失敗を経て、2007年12月13日リスボン条約が署名され、2009年12月1日発効した。同条約により三本柱構造が廃止され、「連合は欧州共同体に取って代わり、

1　庄司克宏著『EU法　基礎篇』岩波書店、2003年、17頁、同『EU法　政策篇』岩波書店、2003年、145、146頁。

かつ、それを承継する」(EU条約第1条3段）ことにより、また、EUとして単一の法人格（EU条約第47条）を付与されることにより（Euratomは別個の法人格を維持)、以前は法的性格を異にしたEUとECが並存する法体系が結合されて、単一の法秩序が創出されている。このような単一の法秩序を成すEUにおいて、(ECから引き継がれた）超国家性が支配的である。ただし、これは政府間主義が廃止されて、すべての事項が「共同体化」されることにより超国家的な性格を帯びるというわけではない。とくに共通外交・安全保障政策（CFSP）との関係でEUは事実上の二本柱構造となっている[2]。この点につき、図表2を参照されたい。

リスボン条約による改正後、EU基本条約の正式名称は、EU条約およびEU機能条約となった。EU基本権憲章[3]は、それらの条約と同等の法的拘束力を付与されている（EU機能条約第6条1項)。なお、イギリス、ポーランド及びチェコには、EU基本権憲章の適用に関する議定書[4](第30号)が適用されるが、個人情報保護に関して影響を及ぼすものではない。

EU機能条約第16条には次のように規定されている。

「１．何人も自己に関する個人データの保護に対する権利を有する。

２．欧州議会及び理事会は、通常立法手続きに従い、連合の諸機関、団体、事務所及び庁並びに連合法の範囲内に当たる活動を行うときの加盟国による個人データの処理に関わる個人の保護についての規則［rules]、並びに、かかるデータの自由移動についての規則［rules］を定める。これらの規則［rules］の遵守は、独立の機関のコントロールに服する。本条に基づき採択される規則[rules]は、欧州連合条約第39条[5]に定める特別の規則［rules］を害するものではない。」

EU機能条約第16条に基づき、コミッションが提案している一般的データ保護規則（General Data Protection Regulation）提案に全面改正される予定である（EU諸機関及び補助機関に適用されるデータ保護規則45/2001は維持される)。また、枠組決定2008/977は「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」に全面改正される予定である。

図表２

<table>
<tr><th colspan="3">EU法</th></tr>
<tr><th>政府間協力</th><th colspan="2">超国家的法秩序</th></tr>
<tr><th>共通外交・安保政策
(CFSP)</th><th>自由・安全・司法領域
(警察・刑事司法協力を含む)</th><th>域内市場</th></tr>
</table>

（庄司克宏『欧州連合　統治の論理とゆくえ』岩波新書、2007年、2010年第4刷、巻末表1）

2　庄司克宏「リスボン条約（EU）の概要と評価」『慶應法学』第10号、2008年（195－272）201頁。

3　庄司克宏「EU基本権憲章（草案）に関する序論的考察」『横浜国際経済法学』第9巻2号、2000年（1－23頁)。

4　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』第19号、2011年（317－330頁)。

5　共通外交・安全保障政策（CFSP）に関して、EU条約第39条は次のように規定する。「欧州連合条約第16条に従い、かつ、同条2項の適用除外により、理事会は本章［CFSP］の範囲内に当たる活動を行うときの加盟国による個人データの処理に関わる個人の保護についての規則［rules］並びにかかる自由移動についての規則［rules］を定める決定を採択する。これらの規則［rules］の遵守は、独立の機関のコントロールに服する。」なお、EU条約第31条1項によれば、CFSPにおける決定は原則として全会一致による。

（3）規則、指令、枠組決定と直接効果

① 直接適用可能性と直接効果

EU機能条約第288条〔旧EC条約第249条〕2段には次のように規定されている。

「規則は一般的適用性を有する。規則はそのすべての要素について義務的であり、かつ、すべての加盟国において直接適用可能［directly applicable］である。」

他方、警察・刑事司法協力に関する旧EU条約第34条2項（リスボン条約により削除）は、次のように規定する。

「･･･理事会は、･･･加盟国の法律及び規則の接近のため枠組決定を採択することができる。枠組決定は、達成すべき結果について名宛人たるすべての加盟国を拘束するが、形式及び手段についての権限は国内機関に委ねる。それは、直接効果［direct effect］を伴わない。」

以上の2つの条文を比較すると、「直接適用可能」と「直接効果」という文言は意味を異にすることがわかる。直接適用可能とは、国内立法への変形や受容なしに国内法秩序でそのまま適用できることを意味する。他方、直接効果とは、「共同体法が加盟国の領域において法源となり、共同体諸機関及び加盟国だけでなく共同体市民にも権利を付与し及び義務を課し、並びに、特に国内裁判官の前において共同体法から権利を引き出しかつ同法に適合しないすべての国内法規定を排除させるために共同体市民により援用されることができる能力をいう」[6]。個人は、国家が直接効果を有するEU法規定を遵守していない結果として自己の権利を侵害される場合、国内裁判所でその規定に依拠して自己の権利の救済を得ることができる。なお、「直接効果」という語で意味されるものが、しばしば「直接適用可能性」という用語で表現される場合があるので注意を要する[7]。

EU法規定が直接効果を発生するのは、「無条件かつ十分に明確」という要件を充足している場合である。EU法規定が「無条件」であるとは「それがいかなる条件による制限も受けず、又は、その実施若しくは効果において共同体諸機関若しくは加盟国によるいかなる措置の採択にも服しない義務を定めている場合」を指し、また、EU法規定が「個人が依拠し、国内裁判所が適用しうるほど十分に明確」であるとは、「それが一義的な文言で義務を定めている場合」をいう[8]。例えば、当該規定が裁量の余地を残しており、あるいは、一般的な目的又は政策を定めるのみでそれを達成すべき特定の手段を定めていない場合には「無条件かつ十分に明確」であるとはみなされない[9]。規則であっても「無条件かつ十分に明確」ではない規定は、直接効果を有しない。

---

6 Marianne Dony, *Droit de la Communaute et de l'Union européenne, troisième édition, Editions de l'Université de Bruxelles,* p. 264.

7 庄司克宏著『EU法　基礎篇』前掲、120、121頁。

8 Cases C-246/94, C-247/94, C-248/94 and C-249/94 *Cooperativa Agricola Zootecnica S. Antonio and Others v. Amministrazione delle finanze dello Stato*［1996］ECR I-4373, para. 18.

9 庄司克宏著『EU法　基礎篇』前掲、122頁。

② 指令の直接効果

EU機能条約第288条〔旧EC条約第249条〕3段によれば、「指令は、達成すべき結果について名宛人たるすべての加盟国を拘束するが、形式及び手段についての権限は国内機関に委ねる。」

この規定の文言からすると、指令は「無条件かつ十分に明確」という直接効果の要件を充たしていないように見える。しかし、EU司法裁判所はケース・バイ・ケースで判断することとし、指令の国内実施期限が遵守されていない場合または国内実施されたが不的確な実施の場合であって、当該指令の規定が「無条件かつ十分に明確」である場合には、直接効果（ただし、対国家（地方自治体や国有企業などの「国家の派生物」を含む）との関係における直接効果に限定される）を発生することが判例法上確立されている[10]。

③ EUデータ保護指令95/46の直接効果

EUデータ保護指令95/46の第7条には次のように規定されている。

「加盟国は、以下の場合に限り、個人データを処理することができることを規定しなければならない。

・・・

(f) 管理者又は当該データが開示される一若しくは複数の第三者により追求される正当な利益のために処理が必要であること。ただし、かかる利益よりも、第1条1項に基づく保護を要求するデータ主体の基本的権利及び自由にとっての利益の方が上回る場合は、この限りでない。」

この規定についてEU司法裁判所は、以下のように述べている。

「当裁判所の確立された判例法によれば、指令の規定は、その主題に関する限りにおいて無条件かつ十分に明確である場合常に、国家が指定された期間の終了までに当該指令を国内法において実施しなかったとき又は国家が当該指令を的確に実施しなかったとき、当該国家に対し個人により国内裁判所において援用されることができる。

指令95/46の第7条（f）は、個人により依拠され、かつ、国内裁判所により適用されるために十分明確な規定である。さらに、当該指令は疑いなくその規定のいくつかの実施において加盟国に多かれ少なかれ裁量権を付与しているが、第7条（f）については無条件の義務を示している。[11]」

その結果、指令95/46の第7条（f）は直接効果を有するとされた[12]。すなわち、指令であっても、上述の要件を充たす規定は直接効果を有し、国内裁判所において援用可能である。

---

10 同上、134－139頁。

11 Cases C-468/10 and C-469/10 - *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF)* (C-468/10), *Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) v. Administración del Estado* (judgement of 24 November2011), not yet reported, paras. 51, 52.

12 *Ibid*., para. 55.

2．基本権としての個人情報保護

（1）EU条約第6条とEU司法裁判所判例法

EUにおける基本権保護について定めるEU条約第6条は、3つの手段を規定する。第1に「EUは基本権憲章に定められた権利、自由及び原則を承認する」（第1項）としている。なお、先述したように、基本権憲章はEU基本条約（EU条約及びEU機能条約）と「同一の法的価値」を有する（第1項）。第2に、EUは欧州人権条約に加入することを義務づけられている（第2項）。これによりEU法は、欧州人権条約に基づき、欧州人権裁判所の監督を受けることとなるが、現在交渉中であり、まだ実現には至っていない。第3に「〔欧州人権条約〕により保障され、かつ、加盟国に共通の憲法的伝統に由来する基本権は、EU法の一般原則を構成する」（第3項）。これは判例法を条文化したものであり[13]、EU司法裁判所は次のように判示している。

「基本権は、加盟国に共通の憲法的伝統及び加盟国が協力して作成し又は署名国となっている国際条約に従って、当裁判所が遵守を確保する法の一般原則の不可欠の一部であるということを当裁判所は一貫して判示してきた。その点で〔欧州人権条約〕はとくに重要である。[14]」

（2）欧州人権条約との関係 ― 欧州人権裁判所から見たEU法

EU自体は欧州人権条約の締約当事者ではない。しかし、EU加盟国が欧州人権条約の締約国としてEUの行為に責任を負う。すなわち、EUは間接的に欧州人権条約上の責任を負うことになる。他方、欧州人権条約と「同等の保護」がEUに存在するとの推定が与えられている。ただし、「明白な瑕疵」がある場合、その推定は破られる[15]。欧州人権裁判所は、以下のように判示している。

「当裁判所の見解では、〔EU規則に基づく〕法的義務に従ってとられた国家の行動は、〔EU〕が提供する実体的保障及びその遵守を監督する仕組みの双方に関して、欧州人権条約が規定するのと少なくとも同等とみなされうる仕方で基本権を保護しているとみなされる限り、正当化される。当裁判所では、「同等（equivalent）」とは「類似（comparable）」を意味する。当該組織の保護が「同一（identical）」でなければならないとの要件は、遂行される国際協力の利益に反するものとなろう。しかし、同等性についてのいかなるそのような認定も最終的なものではなく、基本権保護における関連する変化に照らして審査に服する。[16]」

このように、基本権の実体的及び手続的保障の両面で欧州人権条約が付与するのと同等の保護がEUに存在するとされる場合、「国家は当該組織への加盟から生じる法的義務を単に実施しているにすぎないとき、欧州人権条約の要求から逸脱していないという推定が存在する[17]」。しかし、「同等の保護」の

---

13 庄司克宏著『EU法　基礎篇』前掲、161－166頁。

14 Cases 46/87 and 227/88 *Hoechst* [1989] ECR 2859, para. 13.

15 庄司克宏「欧州人権裁判所の「同等の保護」理論とEU法」『慶應法学』第6号、2006年（285－302）290－294頁。

16 Application No. 45036/98, *Bosphorus Hava Yolları Turizm ve Ticaret Anonim Şirketi v. Ireland* (Grand Chamber), 30 June 2005, (2006) 42 E.H.R.R. 1, para. 155.

17 *Ibid*., para. 156.

推定が破られる場合があることも示されている。すなわち、「特定の事件の状況により欧州人権条約上の権利の保護に明白な瑕疵がある（manifestly deficient）と考えられる場合、いかなるそのような推定も破られる[18]」。

以上の結果、個人情報保護においても、EUは欧州人権条約の水準と（少なくとも）同等の保護を確保する必要がある。それが達成されないようなことがあれば、欧州人権裁判所により加盟国の責任が問われ、間接的にEUの欧州人権条約違反が認定されることになる。

（3）EU基本権憲章第8条（個人データの保護）

① EU基本権憲章第8条とその背景

EU基本権憲章第8条は、個人データの保護について次のように規定する。

「１．何人も自己に関する個人データの保護に対する権利を有する。

２．かかるデータは、特定された目的のために、かつ、当該者の同意又は法律に定める他の正当な根拠に基づき、公正に処理されなければならない。

３．これらの規則の遵守は、独立の機関によるコントロールに服する。」

第8条の起草過程として、欧州人権条約を補完する条項として、個人データの使用を決定する権利が追加されなければならないことが示されていた[19]。また、「基本権憲章に関する説明文書」（［2007］OJ C 303/17）によれば、第8条が制定された背景として、次のように説明されている。

「本条は、EC条約第286条及び指令95/46並びに欧州人権条約第8条及び1981年欧州審議会条約に依拠している。EC条約第286条は、今ではEU機能条約第16条及びEU条約第39条に変更されている。共同体諸機関及び補助機関に関する規則45/2001も参照されている。上述の指令及び規則は、個人データ保護に対する権利の行使のための条件及び制限を含んでいる。」

このように基本権憲章第8条は、欧州人権条約第8条を背景とし、それを補完するものとして制定された。

② 欧州人権条約との関係

EU基本権憲章は欧州人権条約との関係について第52条3項で規定している。

「本憲章が［欧州人権条約］により保障される権利に合致する権利を含む限りにおいて、当該権利の意味及び範囲は欧州人権条約に定められたものと同一でなければならない。本規定は連合法がより広範な保護を与えることを妨げない。」

---

18 *Ibid.*

19 “Affirming Fundamental Rights in the European Union. Time to Act”, *Report of the Expert Group on Fundamental Rights* (European Commission) Brussels, February 1999, p. 16.

この規定に関して、前掲「基本権憲章に関する説明文書」は、以下のように述べている。

「保障される権利の意味及び範囲は〔議定書を含む欧州人権条約〕文書のテキストだけでなく、欧州人権裁判所及び欧州連合司法裁判所の判例法によっても決定される。・・・いずれにせよ、憲章により与えられる保護の水準は〔欧州人権条約〕により保障されるより低くなることは決してできない。」

その結果、EU司法裁判所は、基本権憲章の規定が争点となる事件において、欧州人権条約および欧州人権裁判所の判例法を参照して考慮に入れる必要がある。

③ EU基本権憲章第8条に関するEU司法裁判所判例

EU規則が農業補助金の受益者に関するデータ（氏名、金額等）のウェブサイトによる公開を義務づけていたところ、そのEU規則の当該規定は個人データ保護に対する基本権に反して無効か否かが争われた。本件において、EU司法裁判所は、まず、基本権憲章第8条及び第7条（私生活の尊重)、第52条1項（基本権の行使に対する制限)、第52条3項及び第53条（ECHRに相応する判断）に照らして判断するとした。次いで、上記公開は、基本権憲章第7章の意味における私生活への干渉であること、また、それは同第8条2項に当たる個人データの処理であることを指摘し、同第52条1項に照らして正当化されるか検討する必要があるとした。その結果、EU規則の当該規定による情報公開は、期間、頻度、性格等による区別がないため、比例性原則に反するとされ、その限りにおいて無効であると判示された[20]。

3．EUデータ保護指令の域外適用

（1）域外適用の定義

一般に、国家管轄権は3つに分類される。第1に立法管轄権、第2に執行管轄権、第3に司法管轄権である。立法管轄権とは「国家が対外的要素を伴う事件に自国法を適用する権限」、執行管轄権とは「国家が他国の領域において行為を行う権限」、また、司法管轄権とは「一国家の裁判所が対外的要素を伴う事件を審理する権限」を意味する[21]。

「域外管轄」（extraterritorial jurisdiction）とは、国際法委員会によれば、「国際法の下で規制がない場合に、国境を越えて国家の利益に影響を及ぼす人、財産又は行為の処分を国内の立法、判決又は執行により規制する」[22]ことを意味する。本稿では「域外適用」（extraterritorial application）という用語をこの意味内容で使用することとする。

---

20 Case C-92/09 and C-93/09 - *Volker und Markus Schecke GbR* (C-92/09), *Hartmut Eifert* (C-93/09) *v. Land Hessen* (judgement of 9 November 2010), paras. 43-89.

21 Michael Akehurst, “Jurisdiction in International Law”, *British Yearbook of International Law*, Vol. 46, 1972-1973, pp. 145-257 at 145.

22 International Law Commission (ILC), “Report on the Work of its Fifty-Eighth Session” (1 May-9 June and 3 July-11 August 2006) UN Doc A/61/10, Annex E, para. 2.

また、国際法委員会によれば、「国家が自然人又は法人、財産又は状況に対する管轄を有効に主張するため、そのような人、財産又は状況に対する何らかの連結（connection）を有しなければならない、ということは一般的に受け入れられている[23]」とされている。「域外管轄の行使のための十分な基礎を構成しうる種類の連結」に関する国際法の一般原則として存在するとされているのは、第1に属地主義（territoriality principle）として、客観的属地主義（objective territoriality principle）及び効果理論（effects doctrine）、第2に属人主義として（nationality principle）、積極的（能動的）属人主義（active nationality principle）及び消極的（受動的）属人主義（passive personality principle）、第3に保護主義（protective principle）、第4に普遍主義（universality principle）である[24]。

第1の属地主義（領域主義）とは、管轄権が当該国家の領域内で行われた行為に基づく場合をいう[25]。また、客観的属地主義とは、「国家がその領域外における人、財産又は行為に関して行使する管轄権であって、規制の対象となる当該行動の構成要素が国家の領域内で発生する場合をいう[26]」。さらに、効果理論とは、「自国領域内で実質的効果を受ける国家の領域外で発生する外国人の行動に関して主張される管轄」を指す場合であり、「当該行動の要素が規制を行う国家において生じることを必要としない」[27]。

第2の属人主義（国籍主義）とは、通常、積極的（能動的）属人主義を意味し、「国家が自国民の外国における活動に関して行使することができる管轄」[28]を指す。また、消極的（受動的）属人主義とは、「国家が自国民に損害を与える外国での行動に関して行使することができる管轄」[29]をいう。

第3の保護主義とは、「国家が、国家安全保障に対する対外的脅威のような国家の基本的国益に対する脅威を構成する外国の人、財産又は行為に関して行使することができる管轄」[30]を指す。また、第4の普遍主義とは、「いかなる国家も国際社会の利益のために国際法上の一定の犯罪に関して行使することができる管轄」[31]である。

本稿では、EU法の域外適用に関わるものとして、とくに客観的属地主義と効果理論に限定して取り上げる。

---

23 *Ibid.*, para. 42.

24 *Ibid.*, paras. 10, 42.

25 Christopher Kuner, “Data Protection Law and International Jurisdiction on the Internet(Part 1)”, *International Journal of Law and Information Technology*, Vol. 18 No.2, 2010, pp. 176-193 at 188.

26 International Law Commission (ILC), *op. cit.*, para. 11.

27 *Ibid.*, para. 12.

28 *Ibid.*, para. 14.

29 *Ibid.*, para. 15.

30 *Ibid.*, para. 13.

31 *Ibid.*, para. 16.

（2）EU 競争法の域外適用

EU 司法裁判所の最上級審である司法裁判所によれば、EU 競争法（EU 機能条約第 101 条：カルテル等の禁止）の違反には、協定等の形成及びその実行という 2 つの要素があり、決定的な要素はそれが実行される場所である[32]。すなわち、客観的属地主義の立場をとっている。

これに対して、EU 司法裁判所の下級審である総合裁判所（旧第一審裁判所）は、合併規則に関して、域外で実施された合併であっても、EU 内において「直接的かつ実質的効果」を有することが「予見可能」な場合、EU が規制を及ぼすことは、国際公法上正当化されるとした[33]。このように、総合裁判所は（少なくとも、関係事業者の全世界での売上高の合計を含む基準で規制対象を判断する合併事案については）効果理論の立場を表明している。

なお、EU の競争当局であるコミッションは、合併事案にとどまらず、EU 競争法一般において一貫して効果理論の立場をとっている。

（3）EU データ保護指令の域外適用―第 4 条 1 項（c）

EU データ保護指令の規定のうち、域外適用の可能性があるのは、第 4 条 1 項（c）である。

「各加盟国は、本指令に従って採択する国内規定を、以下の場合の個人データの処理に対して適用しなければならない。･･･

（c）管理者が共同体領域に開業していないが、個人データを処理する目的で、自動化の有無にかかわらず、当該加盟国の領域に所在する手段(equipment; des moyens)を使用すること。ただし、かかる手段が共同体領域を単に通過する目的で使用される場合はこの限りでない。」

この規定は、EU 域内で生じる行為の遂行（手段の使用）に基づいているため、客観的属地主義に基づいているように思われる[34]。一方、第 4 条 1 項（c）は、手段の使用それ自体ではなく、個人データ管理者が EU 域外に移動することにより EU ルールを回避するのを防ぐことに焦点を当てるものであり、EU 域外でのデータ処理により EU 域内で発生する効果に着目しているとみなすならば、効果理論の立場に基づいていると考えることもできる[35]。第 29 条作業部会は、「欧州連合の外に開業するが･･･EU 内の手段を使用するウェブサイトが個人データ処理、特に収集のための保障、及び、欧州レベルで承認され、かつ、欧州連合内で開業するすべてのウェブサイトにいずれにせよ適用可能な個人の権利を尊重

32 Case 89, ...129/85 *Woodpulp* [1988] ECR 5193, paras. 16-18.

33 Case T-102/96 *Gencor Ltd v. Commission* [1999] ECR II-753, paras. 90-101.

34 Christopher Kuner, *op. cit.*, p. 188.

35 *Ibid.*, p. 190; Christopher Kuner, “Data Protection Law and International Jurisdiction on the Internet(Part 2)”, *International Journal of Law and Information Technology*, Vol. 18 No. 3, 2010, pp. 227-247 at 239.

する場合にはじめて、個人の高度の保護が確保され得る」[36]としている。

ここで問題となるのは、「手段」という用語で意味されているものの範囲である。とくにcookies, JavaScript, ad banners などの使用が含まれるか否かである[37]。第29条作業部会は、これを肯定している[38]。ただし、そのように考える場合、第4条1項（c）の「手段」の使用の範囲が広範になり、その基準が十分な管轄上の連結として機能するには不明確であるという批判が加えられている[39]。

また、指令95/46の第28条6項は「各監督機関は、当該処理に適用可能な国内法が何であれ、自己の加盟国領域において、第3項に従って自己に付与された権限を行使する管轄権を有する」と規定し、属地主義を定めているため、各国データ保護機関の権限は自国領域でなされるデータ処理に対して行使される[40]。他方、第4条2項によれば、上記第4条1項（c）に該当する場合、管理者は当該加盟国領域に開業する代表（a representative）を指名しなければならない。「管理者自身に対して起こされうる法的訴訟を害するものではない」とされているので、域外の管理者が指令に反した場合、管理者が指名した代表が責任を負うことが念頭にあると思われる。しかし、これだけでは、たとえばEU内に資産を有しないデータ管理者がEU市民のデータを処理するために自らのウェブサイト上でcookiesを使用することに対して、EU法上の管轄権を行使しうる現実的な見込みはほとんどないとされている[41]。

（4）一般的データ保護規則案における域外適用

コミッションが提出している一般データ保護規則提案の第3条2項には、現行指令の第4条1項（c）に対する批判を踏まえて、次のように規定されている。

「本規則は、処理活動が以下に関連する場合、連合内に開業していない管理者により、連合内に居住するデータ主体の個人データ処理に適用される。

（a）連合内のかかるデータ主体への物又はサービスの提供、又は

（b）彼らの行動の監視」

---

36 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 web sites”, WP 56, 30 May 2002, p. 15.

37 Christopher Kuner, Part 2, *op. cit.*, p. 229.

38 Article 29 Working Party, “"Privacy on the Internet" - An integrated EU Approach to On-line Data Protection”, WP 37, 21 November 2000, p. 28; Article 29 Working Party, WP 56, *op. cit.*, p. 11, 12.

39 Christopher Kuner, Part 2, o*p. cit.*, p. 239, 242.

40 Christopher Kuner, Part 1, *op. cit.*, p. 191.

41 Christopher Kuner, Part 2, *op. cit.*, p. 234, 235.

この規定は、「標的基準」（targeting criteria）を採用し、域外のデータ管理者が域内の個人を標的とする何らかの行動をとった場合に、EUの個人情報保護法制の適用を限定するものである。

この基準については、いつオンライン活動が特定国を「標的」とするのかを決定することが難しいという指摘がある[42]。それに関しては、3つの要因に焦点を当てるべきとする見解がある。第1に、当事者はいずれの法が規律すべきかを決定するために契約取りきめを行ったか否かである。第2に特定の管轄を標的にするか又は回避するためのテクノロジーの使用、及び、第3に当事者がオンライン活動の地理的ロケーションについて有していたか又は有しているべきであった知識である[43]。

標的基準と域外適用の関係については、引き続き検討を要する課題である。

（5）その他の問題 ― セーフ・ハーバーからの第三国移転

他の域外適用の事例として、アメリカのセーフ・ハーバー制度とそれに基づく個人データ保護の十分性に関連して、EU内からアメリカのセーフ・ハーバーのメンバーに個人データが移転された後、それからさらに第三国に移転される場合に、EUデータ保護指令（に基づく加盟国法）は適用可能かという問題が存在する。EUのコミッション及び数カ国の個人データ保護機関は、EUの個人情報保護法制がそのような場合にも引き続き適用されるという立場をとっている[44]。これについても、問題の指摘にとどめ、今後の検討課題としたい。

---

42 *Ibid*., p. 240.

43 *Ibid*; Michael A. Geist, “Is There a There There? Toward Greater Certainty for Internet Jurisdiction”, *Berkeley Technology Law Journal*, Vol. 16, No. 3, 2001, pp. 1345-1406 at 1384-1404.
By †

44 Christopher Kuner, Part 2, *op. cit*., p. 231, 240, 241.

＜３＞　国際経済法の観点からみたEUデータ保護指令に関する検討[1]

田園調布学園大学専任講師　國見　真理子

＜＜目次＞＞

1　本調査研究報告書執筆においては、委員会の座長である堀部政男先生をはじめメンバーの諸先生方、そして、オブザーバーの方々から有益なご意見を賜り、大変勉強になりました。とりわけ消費者庁消費者制度課個人情報保護推進室政策企画専門官の板倉陽一郎弁護士には、色々お世話になりました。ここでお世話になった皆様に厚く御礼申し上げます。尚、ここでの見解はあくまでも個人的なものであり、政府の公式見解ではありません。

1　はじめに

（1）WTO 概説

＜WTO とは＞

WTO とは、世界貿易機関（World Trade Organization）という 1995 年に設立された国際機関である。これは、GATT から改組・発展した国際貿易に関する専門機関であり、現在、加盟国数は 153（独立の関税地域を含む）である。

＜WTO の主な機関＞

WTO の主な機関として、以下のようなものがある。

● 閣僚会議（Ministerial Conference）

これは、WTO の最高意思決定機関である。すべて WTO 加盟国の代表によって構成され、少なくとも２年に１回の頻度で開催されることになっている（WTO 設立協定第４条1）。

● 一般理事会（General Council）

これは、WTO のすべて加盟国の代表によって構成される組織である。閣僚会議と並列して存在する実務組織である（WTO 設立協定第４条2）。

一般理事会の下には各種組織が存在する。この中で重要な関連組織の一つとして、WTO 協定に関する紛争処理を行う組織（DSB）が挙げられる。

◆ 紛争解決機関（Dispute Settlement Body ＝ DSB）

これは、「紛争解決委員会」とも呼ばれる。WTO 設立協定第４条３によれば、「一般理事会は、紛争解決了解に定める紛争解決機関としての任務を遂行するため、適当な場合に会合する」と規定されている。そのため、厳密には一般理事会の下部組織ではなく、一般理事会自体が DSB としての機能を果たすこととなっている。

WTO 設立協定附属書２（紛争解決に係る規則及び手続に関する了解）によれば、紛争解決機関として、具体的には以下の２つの機関の設置を定めている。

・小委員会（Panel）

紛争事件についての実質的な判断を行う第一審の役割を果たす。ただし、条約上は、勧告又は裁定は DSB 自体が行うとされている。これは、通称「パネル」と呼ばれている（第６条）。

・上級委員会（Appellate Body）

小委員会（パネル）の上級審にあたる存在である（第 17 条）。

＜WTO 設立協定＞

WTO諸協定とは、WTO設立協定と４つの付属文書から構成される。WTO設立について定めた国際条約は正式名称を「世界貿易機関を設立するマラケシュ協定」という。通常は、WTO設立協定またはWTO協定と呼ばれている。

WTO設立協定は本体および附属書に含まれる各種協定からなる。

附属書は1から４までである。附属書1 ～ 3はWTO設立協定と一括受諾の対象とされており、WTO加盟国となるためには附属書1 ～ 3のすべてを受諾しなければならない。附属書４は一括受諾の対象ではなく、受諾国間でのみ効力を有する。

1995年のWTO設立と同時に、1994年GATT（1947年GATTが発展・強化したもの）以下のWTO諸協定も同時に効力を生じることになった**【図表１】**。

【図表１　WTO 協定】

附属書１
附属書1A：物品の貿易に関する多角的協定
(A)　1994年の関税及び貿易に関する一般協定（1994GATT）
(B)　農業に関する協定
(C)　衛生植物検疫措置の適用に関する協定（通称 SPS 協定）
(D)　繊維及び繊維製品（衣類を含む）に関する協定（繊維協定、2004年末に終了）
(E)　貿易の技術的障害に関する協定（通称 TBT協定）
(F)　貿易に関連する投資措置に関する協定（通称 TRIMs 協定）
(G)　1994年の関税及び貿易に関する一般協定第６条の実施に関する協定（アンチダンピング協定）
(H)　1994年の関税及び貿易に関する一般協定第７条の実施に関する協定（関税評価協定）
(I)　船積み前検査に関する協定
(J)　原産地規則に関する協定
(K)　輸入許可手続に関する協定
(L)　補助金及び相殺措置に関する協定
(M)　セーフガードに関する協定
附属書1B　サービスの貿易に関する一般協定（GATS）
附属書1C　知的所有権の貿易関連の側面に関する協定（TRIPS協定）

附属書２　紛争解決に係る規則及び手続に関する了解（紛争解決了解）
附属書３　貿易政策審査制度
附属書４　複数国間貿易協定
(A)　民間航空機貿易に関する協定

(B)　政府調達に関する協定
(C)　国際酪農品協定（1997年末に終了）
(D)　国際牛肉協定（1997年末に終了）

（注）下線は、付属書の内、本調査研究との関係が深いものを指す。

（2）GATT/GATS 概説

＜GATT について＞

GATTとは、関税及び貿易に関する一般協定（General Agreement on Tariffs and Trade）のことである。これは、1994年に作成された世界貿易機関を設立するマラケシュ協定（WTO設立協定）の一部(附属書1A)を成すモノの貿易に関する条約である。もともとは1948年に発足したGATTであるが、ウルグアイラウンド交渉の結果、1995年からはWTO設立協定の一部という位置づけになっている。

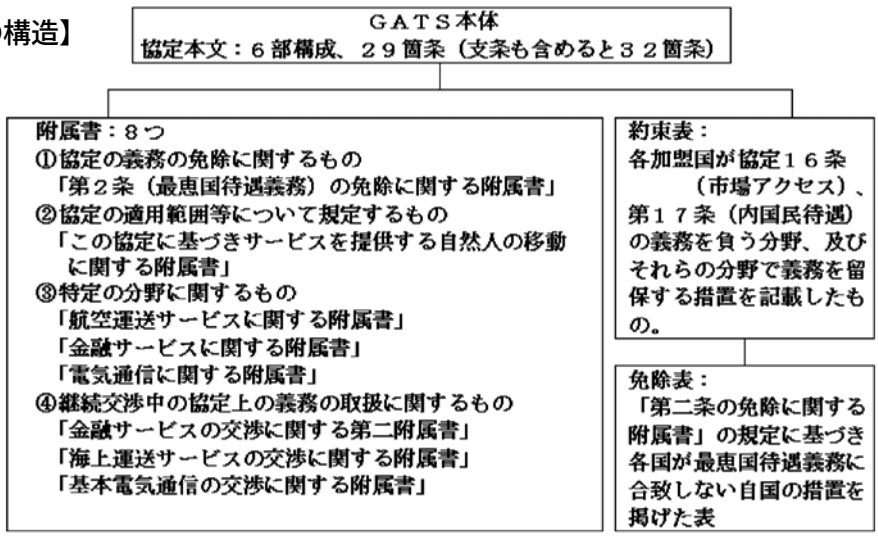
GATTの目的は、できるだけ自由かつ平等な基礎に立って国際貿易の伸展を図るため、関税及び輸出入制限、その他もろもろの貿易上の障壁の軽減・除去しようとすることにある。

＜GATSについて＞

GATSとは、サービスの貿易に関する一般協定（General Agreement on Trade in Services）のことである。これは、1994年に作成された世界貿易機関を設立するマラケシュ協定（WTO設立協定）の一部（附属書1B）を成すサービス貿易に関する条約である。

GATSは、サービス貿易への政府規制についての初めての多国間条約であり、条約本文、8つの附属書、及び、各国の約束表からなる**【図表２】**。

【図表２ GATSの構造】



出典：外務省資料

http://www.mofa.go.jp/mofaj/gaiko/wto/service/gats_1.html#1-4

GATSは、すべての分野の民間のサービス（政府の権限の行使として提供されるサービス以外のサービス）を対象とする。サービス貿易を以下４つのモードに分類し、それぞれについて各国が約束表において自由化を約束するという構成を採っている**【図表３】**。

【図表３　サービス貿易４つのモード】

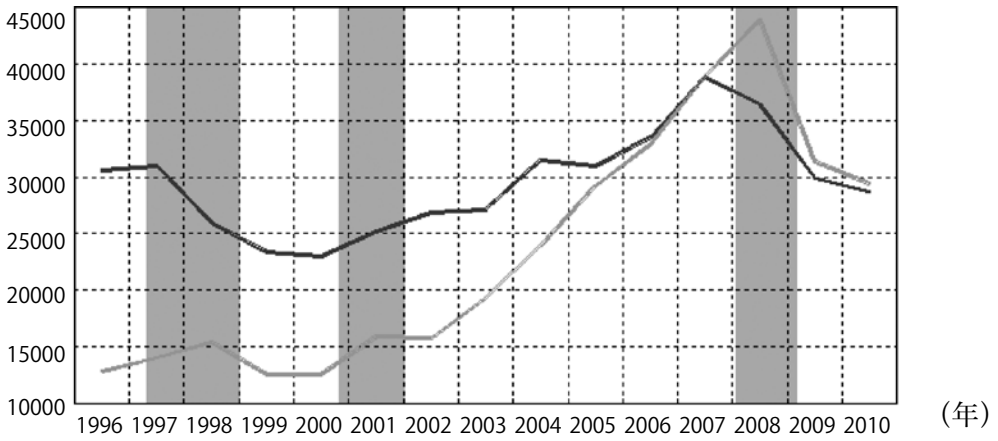
・第１ モード：国境を超える取引
・第２ モード：海外における消費
・第３ モード：業務上の拠点を通じてのサービス提供
・第４ モード：自然人の移動によるサービス提供

ところで、日本・EU間のサービス貿易の規模とはいったいどれぐらいなのだろうか。
日本銀行の国際収支統計によれば、日本・EU間のサービス貿易は輸出入ともに最近は３兆～４兆円規模で推移している**【図表４】**。日本の一般会計の歳入が40兆円レベルであることに鑑みると、日本・EU間でのサービス貿易はその約１割に相当する程の規模である[2]。

このように、WTO発足以来、日本とEU間でのサービス貿易はその重要性を高めてきた状況にある。

【図表４　日本・EU 間のサービス貿易統計 1996 年～ 2010 年】

（億円）



出典：日本銀行国際収支統計。

■：サービス収支/日本からEUへの支払額

■：サービス収支/日本へのEUからの受取額

2　財務省資料「平成23 年度 平成24 年1 月分 国庫歳入歳出状況」
http://www.mof.go.jp/budget/report/revenue_and_expenditure/fy2011/2401a.htm

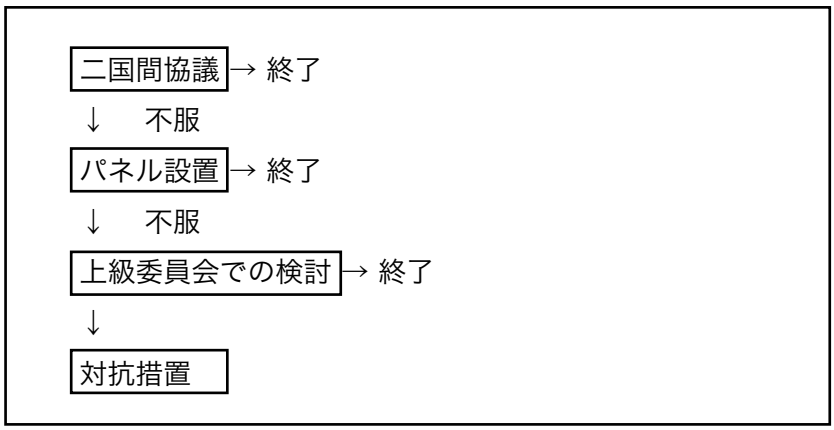
（3）WTOの紛争処理

世界経済のグローバル化の進展とともに、各国の措置を巡って、WTO協定との関係が問題となる場面が増えている。実際、WTO諸協定の条文解釈に関する加盟国間の紛争が絶えない状況にあり、WTOの紛争解決手続は大いに活用されている。

そこで、WTOの紛争解決の流れについて概説する。

WTOの紛争処理は、大まかには以下のような流れである**【図表5】**。まず、WTO加盟国内の紛争当事国同士の二国間協議が行われる。次に、協議に不服のある場合には小委員会（パネル）設置を行う。そこで紛争解決に至らない場合には、更に上級委員会で検討を行う。その結果、場合によっては、損害を受けた国に対して相手国への対抗措置の発動が認められる。

【図表5　WTO紛争解決の主な流れ】



WTOで生じた約400件の紛争処理事例のうち、その大半はGATTのケースであり、GATSに関するケースは約20件程度である[3]。

次に、EU指令の下でEUが行っている個人データの国際移転の規制を巡り、どのような点がWTOとの関係で問題となるのかについて検討を行う。

2　論点の検討

（1）個人データの国際移転はGATTかGATS、どちらの問題か

GATTとGATSの条文を見る限りでは、個人データの国際移転の問題に関してどちらにも該当する可能性があると考えられる。そこで、以下で、その具体的な検討を行う。

3　2012年3月13日現在、WTOから紛争処理報告書が出ているのは全434件である。その中でGATSのケースは22件である。
http://www.wto.org/english/tratop_e/dispu_e/dispu_status_e.htm

そもそも個人データという情報そのものについては、電気通信技術を通じて国境を越えて国際移転できる。これは、無形物であるデータの越境送信として、GATSが規律するサービス貿易に該当する可能性がある。

また、個人データは、顧客名簿や電話帳そして個人データを取り込んだCD-ROM といった有体物に化体される場合がある。このようなモノが国境を越えて国際移転する場合については、GATTが規律するモノの貿易に該当する可能性がある。争いあるものの、日本政府としては、たとえ個人データが無形物としてのデジタルコンテンツであっても、モノに関するGATTの規制範疇に入るものと考えている[4]。

さらに、1998年にWTO事務局の発表したレポートでは、電子商取引はモノ、サービス、又はそれと異なる類型のどれかにあたりうると指摘されている[5]。例えば、インターネットを通じた電子ブックは、規格品としてモノやサービスに該当しうる。他方、個人データが非規格品である限りは、その移転はGATSにあたるがGATTにはあたらないとする。もちろん、GATTとGATSはそれぞれ独立の協定であるが、両者が相互に関連性を有するときには、ある特定の措置がGATTとGATS双方の問題に該当する場合がある[6]。

以上より、個人データの国際移転の問題はGATSとGATT双方に該当可能性があるといえる。ただし、GATSにはGATTと異なり個人データの保護に関する例外条項が明文上に存在するなど、個人データに関する配慮がなされている**【図表６】**。

そこで、まずは、GATSマターの該当可能性について、掘り下げて検討する。

【図表６　GATT/GATS 該当可能性の比較】

	GATS の問題とする場合	GATT の問題とする場合
メリット	・データ通信や電子商取引の問題に対処するにはモノに関する GATT だけでは不十分。 ・(GATT には存在しない）市場アクセス、国内規制に関する規制の該当可能性がある。	・「個人データ」保護に関する例外規定の例示なし（例外に該当しないことで、GATT 違反認定の可能性が高まる。） ・GATT の条文解釈に関するパネルケース過去の蓄積がある（ので予見可能性が GATS のケースより高い場合もある。
デメリット	・「個人データ」保護に関する明示の例外規定あり（例外に該当すると、GATS 違反にならない)。 ・デジタルコンテンツが GATS の対象となるのか争いあり。 ・GATS の条文解釈に関するパネルケースの蓄積が少ない。	・デジタルコンテンツが GATT の対象となるか争いがある上、データ通信や電子商取引の問題が GATT だけですべてフォローすることは不可能。 ・市場アクセス、国内規制に関する規制条文が存在しない。

4　交渉当時の我が国の立場として、例えば、デジタルコンテンツがキャリアメディアに記録されて越境取引される場合にGATTの規律対象になるケースにおいては、同様のデジタルコンテンツが仮にインターネットを通じて配信される場合にも、GATTの規律対象とされるべきであり、従って、MFN及び内国民待遇、数量制限の一律禁止が無条件で認められるべきであるというものである。
http://www.meti.go.jp/policy/trade_policy/wto/html/proposal_e_commerce_j.html#tyu_07

5　Gregory Shaffer, Globalization and Social Protection: *The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards,* 25 Yale J. Int'lL 1 2000, at 48.

6　John H. Jackson Et Al., Legal Problems of International Economic Relations 159 (5th ed. 2008).

＜GATS の該当可能性についての検討＞

そもそも、個人データの国際移転そのものが、GATSの規制対象である「サービス」に該当するのかが争いになる。

WTO協定に関しては、条文自体が抽象的で曖昧な部分が多い。そのため、条文解釈については、GATT/WTOの紛争処理の場でケース・バイ・ケースの判断がなされてきたこれまでの慣行や事務局の解釈ノート等によって蓄積がなされてきた。

では、GATS協定においては、どのように条文解釈されてきたのだろうか。そこで、過去の紛争処理事例を見てみる。

本件の争点に関係するGATS協定の紛争処理事例として、「メキシコの電気通信サービスに関する措置」の問題（WT/DS204/R）が挙げられる[7]。

本パネル報告書では、パネルでは本件がGATSの問題になるかを検討するために、GATS協定上の越境取引にあたる「サービス」の定義を検討した。

その際、被提訴国のメキシコは、「A国からB国への顧客データ送信のためにサービス提供者はただそれだけを送信するのであって、GATS上の越境取引にはあたらない」と主張した(para.7.27)。

しかし、パネルは、GATT事務局の解釈ノートを用いて、「(提訴国の）アメリカのサービス提供者が、(被提訴国）メキシコの提供者とネットワークを通じて国境でつながることによって越境でサービスが供給されているといえ、これはGATS1条2の越境取引に該当する」と判断した(para.7.45)。

以上のパネルの判断を見る限り、顧客データのような個人データを国際移転することは、GATS上のサービスに該当する可能性が高いといえる。個人データの国際移転については、そのすべてがGATSの規律する「サービス」に該当するとまでは断定できないものの、WTOの過去の紛争処理事例に鑑みると、GATSの対象である「サービス」に該当する可能性は十分あるだろう。

1986年〜1994年のGATTウルグアイラウンドにおいてGATS策定が議論されていた時分に比べて、今日では国際的なデータ通信とその関連事業は世界経済を左右するほどの規模になっている。更に、世界中に情報通信網が張り巡らされている高度情報化社会においては、情報通信ネットワークを用いて個人データの国際移転をする機会が多くなっている。ここでは、個人データ送信は、瞬時にかつ世界中に、モノの貿易のように国境の通関などないまま直接伝達される。これは、従来のGATTが想定しているような通関業務が必要な有体物の貿易とは根本の性質が異なっている。

7　本ケースのパネルでは、メキシコが電気通信サービス分野において反競争的で差別的規制維持したことは自由化約束違反、また、越境基本電気通信サービスの供給をコストに見合う合理的なレートで認めてこなかったことも約束違反と判断した。以上については、経済産業省編『2011年版不公正貿易白書』資料編p28を参照。
http://www.meti.go.jp/committee/summary/0004532/2011_04_03.pdf

したがって、個人データの国際移転を巡っては、GATTよりもGATS協定の方が検討の中心となるものと考える[8]。

そこで、本調査研究においては、個人データの国際移転の問題については、主としてGATSの側面からみたWTO違反該当性の検討を行う。ただし、国際経済法上で問題となりそうなものを網羅的に検討する必要性があることから、GATTとの関係についての検討も適宜行うこととする。

（2）EUの「十分性」審査システムは非関税障壁の問題といえるか

EUデータ保護指令には、他国の個人データ保護法制が十分かどうか審査する規定がある（指令25条）。この「十分性」審査システムによって、他国の個人データ保護の法体系が不十分とEU側が判断した場合、EUからその国への個人データの国際移転は原則として禁止される。

そのため、EUの「十分性」審査システムの運用方法によっては、自由な個人データの国際移転そのものが阻害される恐れがある。

したがって、EUの審査システムは、WTO協定の規定するモノやサービス等の自由貿易に反する措置となる可能性がある。

そこで、国際経済法の観点からみて、EUデータ保護指令について、以下のような手順で検討を行うことにする。まず、個人データの国際移転がGATS上のどのようなサービスにあたるのかという問題についてみてみる。その上で、サービス貿易に及ぼす影響や具体的なGATS条文該当可能性について検討を行う。それらを踏まえて、最後に考察を行うこととする。

そもそも、個人データの国際移転とGATS協定との関係について検討するにあたり、EUデータ保護指令下の審査システムはGATS協定違反の措置にあたるのだろうか。

審査システムとは、EUデータ保護指令25条で規定されるように外国の個人データ保護法制がEUのレベルからみて十分であるといえるかどうかをEUが審査する制度のことを指す。ただし、EUがどういう法体系を置くかについては主権の範疇にある。

そこで、GATS関係の検討対象としては、EU指令上で規定される「十分性」審査システムそのものではなく、審査システムの運用・執行方法というEU指令下で行われている措置がGATS違反にあたるかについてであると考える。

8　先行研究を調査した限りにおいても、EUデータ保護指令に関しては、WTO協定との関係ではGATSとの整合性について検討したものに集中しており、GATTの問題を中心的に論じた論文は調査時点段階では見当たらなかった。

（3）GATS 違反該当可能性の検討

① 当該措置はGATS1条2の「サービス貿易」にあたるか

「サービス」貿易に関する直接的な定義はGATS上存在しない。しかし、GATS1条3（b）の規定によれば、「政府の権限の行使として提供されるサービスを除くすべてのサービス分野が協定の対象となる」とされる[9]。

本問題は、GATS1条2で規定するサービスの4モードのどれに該当するのだろうか。そこで、最初に4つのモードについて概説する。その上で、個人データの国際移転がサービスのどのモードにあたるのかについて検討を行う。

＜サービス貿易の4モード＞

4つのモードの概要としては、第1と第2モードについてはモノの貿易同様の越境取引に関するものである。第3モードは対外直接投資に類似したものである。第4モードは外国人労働者の受入れ・送出しに関係するものである。

4つのモードの具体的内容は、以下の通りである**【図表7】**。

第1モード（国境を越える取引）とは、いずれかのWTO加盟国から他の加盟国の領域へのサービスの提供のことを指す。例えば、アメリカのネット書店Amazon.com から日本の消費者がインターネットを通じて洋書を購入することなどが挙げられる。

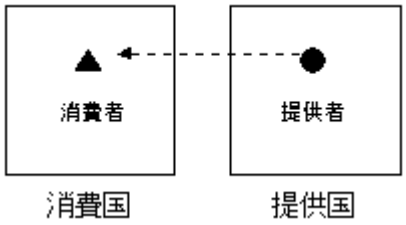
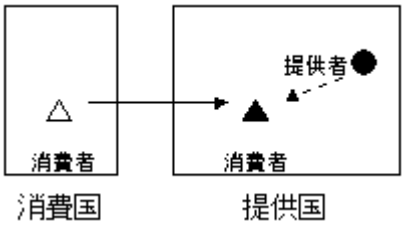
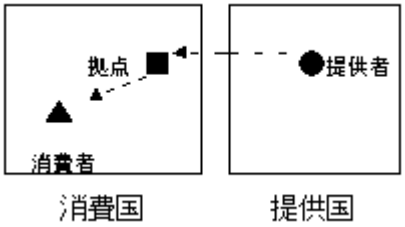
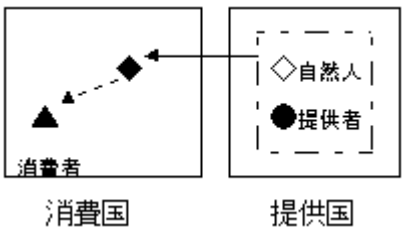
第2モード（海外における消費）とは、いずれかの加盟国の領域内におけるサービスの提供であって、他の加盟国のサービス消費者に対して行われるものを指す。例えば、日本の航空会社であるJALがアメリカのボーイング社に自社所有の飛行機の修繕を依頼することなどが挙げられる。

第3モード（業務上の拠点を通じてのサービス提供）は、いずれか加盟国のサービス提供者によるサービスの提供であって、他の加盟国の領域内の業務上の拠点を通じて行われるものを指す。例えば、みずほ銀行のNY支店から日本へ海外送金サービスを行うことが挙げられる。

第4モード（自然人の移動によるサービス提供）とは、いずれかの加盟国のサービス提供者によるサービスの提供であって他の加盟国の領域内の加盟国の自然人の存在を通じて行われるものを指す。例えば、アメリカの人気シンガーであるシンディ―・ローパーさんを招いて、東日本大震災復興チャリティコンサートを東京で開催するといったものが挙げられる。

9　宮家邦彦『解説 WTOサービス貿易一般協定（GATS）』（外務省経済局、第1版、1996）24頁。

【図表７　GATS上のサービス貿易の４態様】

態様	内容	典型例	典型例のイメージ図
1. 国境を超える取引 （第１モード）	いずれかの加盟国の領域から他の加盟国の領域へのサービス提供	○スカイプを利用して、外国のコンサルタントを利用する場合 ○ネットサイトを利用して外国の通信販売を利用する場	
2. 海外における消費 （第２モード）	いずれかの加盟国の領域内におけるサービスの提供であって、他の加盟国のサービス消費者に対して行われるもの	○外国の会議施設を使って国際会議を行う場合 ○外国で船舶の修理をする場合	
3. 業務上の拠点を通じてのサービス提供 （第３モード）	いずれかの加盟国のサービス提供者によるサービスの提供であって他の加盟国の領域内の業務上の拠点を通じて行われるもの	○海外支店を通じた金融サービス ○海外現地法人が提供する流通・運輸サービス	
4. 自然人の移動によるサービス提供 （第４モード）	いずれかの加盟国のサービス提供者によるサービスの提供であって他の加盟国の領域内の加盟国の自然人の存在を通じて行われるもの	○招聘外国人アーティストによるパフォーマンス ○日本で研修中の外国人看護師による看護サービス	

注）イメージ図の記号　●:サービス提供者、▲:サービス消費者、■:業務上の拠点、◆:自然人、
○△□◇:移動前、◀- - -:サービス提供、◀——:移動、◀– —:拠点の設置

出典：外務省HPを基に著者作成

（http://www.mofa.go.jp/mofaj/gaiko/wto/service/gats_5.html）

では、４つのモードの内、個人データの国際移転が関係するのはどのモードなのだろうか。

個人データの国際移転については、電気通信網を利用した電子商取引かデータ送信が主な用途と思われる。しかし、個人データの国際移転といっても色々な事象があるので、ひとくくりに考えるのは難しい。

そこで、以下でもう少し掘り下げて考えてみることにしたい。

まず、電子商取引が電気通信サービスを通して電子商取引が行われる際は、先述のメキシコの電気通信サービスを巡るWTOの紛争処理パネル（WT/DS204/R）で問題になったように、顧客の住所や信用情報といった個人データについての越境送信取引が行われることになるので、モード1が主に問題になるものと考えられる。

また、グローバル展開をしている多国籍企業において、海外支店の現地採用の人事情報を本社に送信する場合には、モード3が主に問題になるものと考えられる。

更に、電子商取引の場合、海外における消費のために個人データを送る必要がある場合もあるので、モード2も問題になりうる。海外のアーティスト招聘のためにビザを発給する関係で個人データをやりとりする場合、モード4との関係も問題になりうる。

このように、個人データの国際移転については、GATS上のサービスの4モードのすべてに該当する可能性があるといえるものの、主としてモード1とモード3が問題になるものと考えられる[10]。

したがって、個人データの国際移転については、GATS1条2の規定するサービス貿易に該当するものと言える。

② GATS1条1のサービス貿易に「影響をあたえる」措置といえるか

個人データの国際移転がGATS1条2のサービスに該当するとすれば、次にそれはGATS1条1の意味におけるサービス貿易に「影響をあたえる」措置といえるだろうか。

まず、加盟国の「措置」とは、法律、規則、行政上の行為、準則手続、決定その他の方式であるかを問わないとされる(GATS28条(a))。

そして、サービス貿易に「影響を与える」とは、GATS28条（c）で例示しているように、

（ⅰ）サービスの購入、支払又は利用に係る措置

（ⅱ）サービスの提供に関連して加盟国が公衆一般に提供されることを要求しているサービスへのアクセス及び当該サービスの利用に係る措置

（ⅲ）加盟国の領域内におけるサービスの提供のための他の加盟国の者の存在（業務上の拠点を含む）に係る措置

などが挙げられる。

---

10 Carla L. Reyes, *WTO-Complaint Protection of Fundamental Rights: Lessons From The EU Privacy Directive*,12 Melb. J. Int'l L. 141 2011, at 149. See also, Maria Veronica Perez Asinari, *The WTO and the Protection of Personal Data. Do EU Measures Fall within GATS Exception? Which Future for Data Protection within the WTO e-commerce Context?*,18th BILETA Conference Controlling Information in the Online Environment, April 2003, at 2.

つまり、「影響を与える」とは、モノの貿易に関するGATTの先例に倣って、同種のサービスまたはサービス提供者との間に存在する競争関係や競争条件（結果としての貿易量ではない）に影響を及ぼすような措置のことといえる[11]。

また、過去の紛争処理事例を見た場合、上級委員会の審理は、サービス影響に「影響を与える(affecting)」とは、単なる「規制(regulating and governing)」という意味よりも、むしろなんらかの「効果（an effect on)」がある措置であると示唆している[12]。

ということから、この「影響を与える」という概念とは、単なる法規上の規制のみならず、なんらかの効果を与える広範な意味での政府等による措置を包含するものと考えることができる[13]。

更に、個人データの国際移転は国際貿易の拡大とともに益々必要性が高まっているために、データの国際移転を禁止・制限するEUデータ保護指令そのものがWTOの自由貿易原理と適合しない可能性も指摘されている[14]。

---

11 前掲注9、30頁、同42頁。この先例は、GATT3条の解釈に関するものである。

12 例えば、カナダのオートパクト（自動車関連措置）事件のパネル報告（WTO/DS139/AB/R)

13 Reyes, supra note 10 at 150.

14 Ibid, at 150-151. See also, Eric Shapiro, *All is Not Fair In the Privacy Trade: The Safe Harbor Agreement and the World Trade Organization,* 71 Fordham L. Rev. 2781, 2002-2003 at 2781.

③ 具体的該当条文の検討

個人データの国際移転を規制するEU指令は、具体的にはGATS上のどの条項の問題にあたるのだろうか。

GATS上の関係としては、主に最恵国待遇（2条)、国内規制（6条)、市場アクセス（16条）の該当可能性が考えられるので、以下で、それぞれの条文問題について検討する。

A：最恵国待遇（2 条）との関係

【関連規定】

● 最恵国待遇（MFN：Most-Favoured-Nation Treatment）･･･GATS 第 2 条

1　加盟国のサービス及びサービス提供者に対し、他の加盟国の同種のサービス及びサービス提供者に与える待遇よりも不利でない待遇を与えなければならない。(＝与えられた最も有利な待遇をすべての加盟国のサービス提供者に与えなければならない。)

2　加盟国は、1の規定に合致しない措置であっても、「第二条の免除に関する附属書」に掲げられ、かつ、同附属書に定める要件を満たす場合においては、当該措置を維持することができる。

3　この協定の規定は、特定の地域で生産され、かつ、消費されるサービスを国境に隣接する地域に限定して交換することを容易にするため、加盟国が隣接国に対して有利な待遇を与えることを妨げるものと解してはならない。

最恵国待遇とは、通商条約等に基づいて加盟国の一方が他の第三国に対して与えているか又は将来与えることのある最も有利な待遇を他の加盟国に対して与えることをいう。すなわち、WTOに加盟している諸外国の間では平等の扱う側面を有しており、これは無差別待遇とも呼ばれている。

本条は、GATSの基本原則である最恵国待遇原則を規定する。本条の下、WTO加盟国は、相互に即時かつ無条件の最恵国待遇を同種のサービス及びサービス提供者に対して与える義務を負う（本条1)。

他方、加盟国は、一定の要件を満たす場合においては、第2条の義務に合致しない措置であっても維持することができるとされ、限定的に最恵国待遇の義務からの「免除」を認められる(本条2及び第2条の免除に関する付属書)。

また、GATT第24条3(a)の規定に倣い、国境隣接区域に限定されるサービスの交換は最恵国待遇義務の例外とされる（本条3)。

GATSでは、各加盟国の一般的義務として、即時かつ無条件の最恵国待遇を付与しなければならないのが原則である。これは、GATS1条及び28条で定義される各態様の下で提供されるサービスの競争条件に影響を及ぼす「すべての加盟国政府等の措置」を意味する(GATS1条)[15]。ただし、GATS16条のように約束表に記載される自由化約束の対象措置に限られない[16]。

そして、2条2の存在は、ウルグアイラウンド交渉時に、無条件・無制限の最恵国待遇の付与は途上国等の「ただ乗り」を許容することになるという懸念が表明されて以来、各国の見解が対立した結果の妥協の産物といえる。GATSでは協定発効時において、特定の約束に係る自由化交渉とあわせて交渉を行った上で、これを当該国の第2条の免除に係る表（免除表）として、「第2条の免除に関する付属書」に掲げることにより、この義務に関して原則10年間の「免除」が認められることになったからである。

このように、本条は「一般的義務」としての性格と、その「免除」を一定期間認めるという一時的・例外的な性格とを組み合わせることにより、二国間の自由化交渉の成果を最終的に多数国間の枠組みの中で均霑し、サービス貿易の漸進的な自由化を図るという機能が付与されたということができる[17]。

最恵国待遇原則の違反可能性の例としては、EU-アメリカ間で構築されたセーフ・ハーバー枠組みについてアメリカに対して付与している待遇と、「十分性」審査を経ていない他国に付与している待遇との差別が挙げられる。

EUデータ保護指令によれば、EUの十分性審査で「十分性」要件を満たしていない国に対しては、EUからの個人データの国際移転が原則禁止される（25条)。

アメリカは法制度全体についてはEUの要求する「十分性」認定を受けていないものの、セーフ・ハーバー枠組みに従い、商務省に登録された一定のアメリカ企業に対しては、EUから域外のアメリカへの個人データの国際移転が認められている（形式的にはセーフ・ハーバー枠組みについて「十分性」を認めた形)。

これに対し、「十分性」審査を終えていない日本、第29条作業部会の審査においては、「十分性」が認められなかったオーストラリアといった国においては、企業がBCRなどを利用しない場合にはEUから域外への個人データの国際移転は原則として禁止される。

この点、ECのバナナ輸入制限事件における上級委員会報告（WT/DS27/AB/R）によれば、WTOにおける「無差別の」義務とは、法律上形式上の差別のみならず、事実上の差別に対しても適用されるものである[18]。

---

15 外務省経済局国際経済機関第一課『解説WTO協定』(財団法人日本国際問題研究所、初版、1996）483頁。

16 前掲注9、53 頁。

17 前掲注9、52 頁。

18 Jackson, supra note 6 at 964.

したがって、個人データ国際移転に関してEUの行っている措置は、国毎に差別的な待遇差を与えているといえる。これは、「貿易に影響を与える」措置として、最恵国待遇原則に反する可能性があるものと考えられる。尚、アメリカ以外に、セーフ・ハーバー枠組みによる移転をEUに許されている国はこれまで皆無である。

B:国内規制（6条）との関係

【関連規定】

●国内規制（Domestic Regulation）･･･GATS第6条

1　加盟国は、特定の約束を行った分野において、一般に適用されるすべての措置であってサービスの貿易に影響を及ぼすものが合理的、客観的かつ公平な態様で実施されることを確保する。

2　(a)加盟国は、影響を受けたサービス提供者の要請に応じサービスの貿易に影響を及ぼす行政上の決定について速やかに審査し及び正当とされる場合には適当な救済を与える司法裁判所、仲裁裁判所若しくは行政裁判所又はそれらの訴訟手続を維持し、又は実行可能な限り速やかに設定する。加盟国は、当該訴訟手続が当該行政上の決定を行う機関から独立していない場合には、当該訴訟手続が客観的かつ公平な審査を実際に認めるものであることを確保する。

(b)(a)の規定は、加盟国に対し、その憲法上の構造又は法制の性質に反するような裁判所又は訴訟手続の設定を要求するものと解してはならない。

3　特定の約束が行われたサービスの提供のために許可が必要な場合には、加盟国の権限のある当局は、国内法令に基づき完全であると認められる申請が提出された後、合理的な期間内に当該申請に関する決定を申請者に通知する。加盟国の権限のある当局は、申請者の要請に応じ、当該申請の処理状況に関する情報を不当に遅滞することなく提供する。

4　サービスの貿易に関する理事会は、資格要件、資格の審査に係る手続、技術上の基準及び免許要件に関連する措置がサービスの貿易に対する不必要な障害とならないことを確保するため、同理事会が設置する適当な機関を通じて必要な規律を作成する。当該規律は、これらの要件、手続及び基準が特に次の基準に適合することを確保することを目的とする。

(a)客観的な、かつ、透明性を有する基準(例えば、サービスを提供する能力)に基づくこと。

(b)サービスの質を確保するために必要である以上に大きな負担とならないこと。

(c)免許の手続については、それ自体がサービスの提供に対する制限とならないこと。

5　(a)加盟国は、特定の約束を行った分野において、当該分野に関し4の規定に従って作成される規律が効力を生ずるまでの間、次のいずれかの態様により当該特定の約束を無効にし、又は侵害する免許要件、資格要件及び技術上の基準を適用してはならない。

(i) 4の(a)、(b)又は(c)に規定する基準に適合しない態様

(ii) 当該分野において特定の約束が行われた時に、当該加盟国について合理的に予想され得なかった態様

(b) 加盟国が(a)に基づく義務を遵守しているかいないかを決定するに当たり、当該加盟国が適用する関係国際機関の国際的基準を考慮する。

6　加盟国は、自由職業サービスに関して特定の約束を行った分野において、他の加盟国の自由職業家の能力を確認するための適当な手続を定める。

本条は、加盟国が「特定の約束」を行った分野において、一般に適用される加盟国の措置のうち、サービス貿易に影響を及ぼす国内措置が合理的、客観的かつ公平な態様で実施されることを確保することを加盟国に対して求める一般総則的な規定である。

本来の趣旨は、もともとは保健衛生、安全の保護、財政の安定化等の公共的・防衛的な目的のための貿易制限である。しかし、個々の措置が分野毎に大きく異なるため、国際的に受入可能な規制とそうでないものとの間に一般的な境界線を引くことが非常に困難であった。

そこで、ウルグアイラウンドでは、サービス提供者を規制する各国の主権的権能を是認した上で、国内規制がサービス供給の権限・能力等の合理的、客観的かつ公平な基準と態様に基づき、貿易制限的や差別的なものであってはならない旨の条件を付すこととなった[19]。例えば、免許・資格要件、技術基準については、客観的かつ透明性のある基準で、サービスの質を確保するために必要以上に大きな負担とならないことや免許手続自体がサービスの提供に対する制限とならないように確保されなければならない。

本条項のWTO違反該当可能性としては、GATS6条1、3、6との関係の問題が考えられる。

6条1項は一般に適用されるすべての措置に適用されるので、サービス貿易に影響を及ぼす個人データの国際移転に関するあらゆる措置に対して適用可能である。例えば、EUはデータプロセッシング分野について特に例外を置かずに自由化約束をしている。EUの「十分性」審査の運用次第によっては、これは客観性に欠ける不公平な貿易制限措置になりうる。

更に、サービスのモード1と2に関する海外事業者や消費者の越境取引に関する制限措置としては、6条3と6が問題となる可能性があるだろう。

19 前掲注9、87頁。

C：市場アクセス（16条）との関係

【関連規定】

●市場アクセス（Market Access）･･･GATS第16条

1　加盟国は、第一条に規定するサービスの提供の態様による市場アクセスに関し、他の加盟国のサービス及びサービス提供者に対し、自国の約束表において合意し、特定した制限及び条件に基づく待遇よりも不利でない待遇を与える。

2　加盟国は、市場アクセスに係る約束を行った分野において、自国の約束表において別段の定めをしない限り、小地域を単位とするか自国の全領域を単位とするかを問わず次の措置を維持し又はとってはならない。

(a) サービス提供者の数の制限(数量割当て、経済上の需要を考慮するとの要件、独占又は排他的なサービス提供者のいずれによるものであるかを問わない。)

(b) サービスの取引総額又は資産総額の制限(数量割当てによるもの又は経済上の需要を考慮するとの要件によるもの)

(c) サービスの事業の総数又は指定された数量単位によって表示されたサービスの総産出量の制限(数量割当てによるもの又は経済上の需要を考慮するとの要件によるもの)

(d) 特定のサービスの分野において雇用され又はサービス提供者が雇用する自然人であって､特定のサービスの提供に必要であり､かつ､その提供に直接関係するものの総数の制限(数量割当てによるもの又は経済上の需要を考慮するとの要件によるもの)

(e) サービスが合弁企業等の法定の事業体を通じサービス提供者によって提供される場合において、当該法定の事業体について特定の形態を制限し又は要求する措置

(f) 外国資本の参加の制限(外国の株式保有比率又は個別の若しくは全体の外国投資の総額の比率の上限を定めるもの)

市場アクセスは、加盟国が自国の約束表に掲げたサービス分野についてのみ適用される。加盟国にはそれぞれの国内事情により､「市場アクセス」や「内国民待遇」の義務を約束することができないサービス分野につき、これを自国の約束表に掲げないことが認められている。

本条では、サービス貿易を規制する各種規制の中で、主に経済的要因から課されている規制の類型を特定し､「市場アクセス」という特別の概念の下で、市場参入の際の数量制限、形態制限、外資制限を原則として撤廃すべき制限的措置として限定的に明示している。

そのため､「市場アクセス」に関する約束を行っている加盟国において他の加盟国のサービス提供者がサービスの提供を行う際は、その加盟国が自国の約束表において､「市場アクセスに係る制限」の欄を別段に定め､（留保）をしない限り、当該他の加盟国のサービス提供者は本条２に列挙されているような制限措置の適用を受けることなく市場に参入できることが法的に保証されている。

他方、各国は市場アクセスに関して約束を行った分野について、自国の約束表で別段の定めをしない限り、以下の措置をとってはならない。

(a) サービス提供者の数の制限

(b) サービスの取引総額又は取引資産の制限

(c) サービスの事業の総数又は指定された数量単位によって表示されたサービスの総産出量の制限

(d) サービス提供に必要であり、かつサービス提供に直接関係する自然人の総数の制限

(e) サービスを提供する事業体の形態の制限

(f) 外国資本の参加の制限

市場アクセス規定の違反該当可能例として、以下のようなものが考えられる。

電気通信サービスを巡っては、EUはデータプロセッシングサービスの自由化約束を行っている。このことから、EUはEUデータ保護指令によって、個人データ国際移転サービス自体を禁止すること自体が市場アクセスの内でサービスの総産出量の制限違反に該当する可能性がある[20] (GATS16 条2(c))。

以上のように、GATSに関しては、主に3つの条項違反の該当可能性が具体例として挙げることができる。

そこで、次にこれらの条項に該当する場合に、個人データ保護がGATSの規定する一般的例外に該当する可能性があるのかについて検討を行うことにする。

④一般的例外規定(14 条)該当性の検討

A：GATS14 条の個別条項該当性

本件では、GATS14条の一般的例外規定の内で同条（c）（ii）が問題となるので、以下でその該当可能性を検討することとする。

【関連規定】

●一般的例外…GATS 第14 条

この協定のいかなる規定も加盟国が次のいずれかの措置を採用すること又は実施することを妨げるものと解してはならない。

ただし、それらの措置を、同様の条件の下にある国の間において恣意的若しくは不当な差別の手段となるような態様で又はサービスの貿易に対する偽装した制限となるような態様で適用しないことを条件とする。

・・・(中略)・・・

(c) この協定の規定に反しない法令の遵守を確保するために必要な措置。この措置には、次の事項に関する措置を含む。

（ii）個人の情報を処理し及び公表することに関連する私生活の保護又は個人の記録及び勘定の秘密の保護

20 Reyes, supra note 10 at 162.

本条制定の経緯として、GATTの一般的例外規定には「個人の情報」に関する明示の規定は存在しないのに対し、GATSでは交渉時に個人データを例外規定に入れるべきか、その取扱い自体が大きな争点となった[21]。

EU側を中心に、人権保護の観点から、個人データ保護についてのGATS協定の例外規定該当性が強く主張された。

これに対し、EUデータ保護指令を例外扱いすることは特定国の国内基準の域外強制執行(extra-territorial enforcement)を認めることとなり、サービス産業の事業機会を奪うおそれがあるという主張がなされた。

GATS交渉でこのように見解が対立する中、個人データと当時のGATS14 条(c)の「国内法令の遵守」を確保するための措置として記載されていたプライバシー保護等の措置との整合性が問題とされたこともあって、最終的にはGATSでは個人データの処理・公表に関連する私生活の保護と個人の記録・勘定の秘密の保護を一括して無限定な一般的例外から外して、「国内法令の遵守の確保に必要な措置」の中に個人データを限定的に含めることとなった。

＜GATS14条（c）（ii）における「必要性」要件の検討＞

「必要性」要件とは、法令遵守確保のために当該措置が必要な措置といえるかということである。GATSの一般的例外規定は厳格に適用されるべきものであり、あくまでも貿易制限的でないことが条件である[22]。

「必要性」要件の判断に関するリーディングケースとして、以下のような２つの判断基準がWTOの実務慣行上存在するとされる[23]。

・より制限的でない措置のテスト
・比較衡量テスト

WTOのパネルケースの過去事例に鑑みると、現在は、GATS14条の個別条項を巡る解釈慣行としては、後者の「比較衡量テスト」による判断が主流となっている[24]。これは、GATSの一般的例外規定を初めて上級委員会として検討した米国・越境賭博サービス事件の上級委員会報告書（WT/DS285/AB/R）で採用された方法である。

---

21 前掲注９、133 頁。

22 Shaffer, supra note 5 at 51.

23 より制限的でない措置のテストの例としては、米国関税法337条事件において、GATT20（ｄ）の一般的例外に関する解釈として用いられている。また、比較衡量テスト（weighing and balancing test)の例としては、米国の越境賭博サービス事件において、GATS14条の一般的例外に関する判断として用いられている。

24 Reyes, supra note 10 at 174.

ここでは、EUの個人データ保護の合法的な公共政策目的がGATS14 条の一般的例外に該当するか否かが重要である[25]。本件での比較衡量の対象としては、EUデータ保護指令による個人のプライバシー保護法益とデータの越境取引の自由との重要性が挙げられる。

ところが、GATS14条における「必要性」テストは、その要件自体が非常に曖昧なために、予見可能性に乏しい。そのため、「必要性」要件の判断はフレキシブルに行わざるをえない。特に、WTOの審査機関には条文解釈の広範な裁量が与えられているからである[26]。

更に、WTOの慣行として、貿易とプライバシーとの間の微妙なバランスをとることに対して、パネルはとても慎重な立場を取っている。パネルでは、貿易競争の利益とプライバシーの利益との緻密な比較衡量は避けて、EUが外国のプライバシー保護を考慮に入れたかどうかという過程審査に力点を置いているとされる[27]。

このことから、本件の比較衡量テストにおいては、越境取引の自由貿易とプライバシーという2つの利益衡量だけで問題の結論を出すことは困難である。むしろ、EUの指令（や新規則）による「十分性」審査のプロセスについて、GATS上問題があるのかを検討すべきである。

他方、EUによる「十分性」の事実審査の場面では、第三国の法制度の評価が対等又は適切に行われないことはありうるが、このような法令でない単なる事実審査はGATSの判断対象外であるという指摘もある[28]。

しかし、WTOの判断対象となる「措置」とは、法律、規則、行政上の行為、準則手続、決定その他の方式であるかを問わない(GATS28条 (a))。つまり、サービス貿易に「影響を与える」とは、単なる法規上の規制のみならず、なんらかの事実上の効果を与える広範な意味での政府等による措置を包含するものと考えられる。

とすれば、EU指令に基づく事実審査も政府等による「措置」に該当する以上、GATSの対象外であるとの主張には賛成することはできない。

以上のことから、「十分性」の審査方法そのものがGATS14条の個別要件を満たして判断対象となる可能性は十分あるものと考える。

---

25 Shaffer, supra note 5 at 51.

26 See, Reyes, supra note 10 at 164.

27 Shaffer, supra note 5 at 51.

28 Asinari, supra note 10 at 6.

B：GATS14 条柱書要件の検討

本件措置がGATS14（c）（ii）の「必要性」要件のテストを満たす場合、次に、同条柱書に戻って、要件を満たすかを検討する必要がある。ここでは、本件措置が，同条柱書が規定するサービス貿易制限となる恣意的・不当な差別的手段にあたるかを検討することになる。

まず、WTOの性質上、GATSの一般的例外の要件が個人データ保護に対して明確にあてはまるかどうかは予見不能である。実際に人権保護目的でのデータ移転保護規制の問題がWTOで検討されたことがない上、紛争処理機関に広い裁量があるため、どう判断されるか予測が難しいからである。

その上、たとえWTOで争うことにした場合でも、EU側からは、「十分性」を認定していない国の事業者に対しても個人データの国際移転を個別に認める代替措置（指令26条など）を講じている以上、本件指令が恣意的・不当な差別的手段にあたるとは言えないと主張してくることが見込まれる。

しかし、これを争う国としては、EUの指令26条は十分性審査を経ていない国の企業にとっては個別申請が必要で、煩雑で使いにくく負担のかかる制度である上、EU指令とは別建てでUSにのみ認めているセーフ・ハーバー枠組みによってUSに与えている待遇と「十分性」認定を受けていない国に与えている待遇の違いは恣意的で差別的なものであることから、EUの措置はWTO違反に該当するとの反論は十分可能であろう。このような待遇差を設けているEUの個人データ国際移転を巡る「措置」は恣意的・不当な差別的手段に該当し、GATS14条柱書の但書要件を満たしているとは言い難い。

よって、EUが行っている個人データの国際移転に対する保護措置は、GATS14条の一般的例外に該当せず、WTO協定違反該当可能性があるものと考える。

（4）GATT 違反該当可能性の検討

先述のように個人データの国際移転の問題はGATSマターかGATTマターかという論点については、どちらの協定にも該当可能性がある。特に、WTOの電子商取引に関する議論の場では、EUはGATSであると主張するのに対し、日米などはどちらかといえばGATTであるという立場を取っている。そこで、以下ではGATTとの関係性について検討を行うこととする。

EU指令を巡ってGATTとの関係で問題となりうるものとして、最恵国待遇（GATT1条)、数量制限禁止(GATT11条)が主として考えられる。その上で、一般的例外規定（GATT20条）との関係が問題になる。

① 最恵国待遇（１条）との関係

【関連規定】

● 最恵国待遇…GATT 第１条

1　いずれかの種類の関税及び課徴金で、輸入若しくは輸出について若しくはそれらに関連して課され、又は輸入若しくは輸出のための支払手段の国際的移転について課せられるものに関し、それらの関税及び課徴金の徴収の方法に関し、輸入及び輸出に関連するすべての規則及び手続に関し、並びに第三条2及び4に掲げるすべての事項に関しては、いずれかの締約国が他国の原産の産品又は他国に仕向けられる産品に対して許与する利益、特典、特権又は免除は、他のすべての締約国の領域の原産の同種の産品又はそれらの領域に仕向けられる同種の産品に対して、即時かつ無条件に許与しなければならない。

本条はGATTの基本原則である最恵国待遇原則を定めた規定である。これは､GATTの志向する自由・無差別原則に基づいて世界貿易を発展させる目的を達成するための大きな柱となっている[29]。最恵国待遇原則の確保には、関税や輸出入制限についてだけこれを遵守するのでは不十分である。

例えば、手続や運用面で特定の相手国との貿易に特別の負担をかけるならば、その相手国は貿易上他の国と比べて不利な立場に置かれることになり、関税や輸出入制限によって無差別待遇が与えられてもその効果は著しく減殺されることになる。

そこで、GATTでは、以下に挙げる広範囲な事項について、他の国の産品及び他の国に仕向けられる産品に対して即時かつ無条件に最恵国待遇を与えることを義務付け、貿易条件を平等にすることを図っている。

（ⅰ）輸出入関税、輸出入課徴金、輸出入に対する支払の国際的振替に対する課徴金
（ⅱ）関税及び課徴金の徴収方法
（ⅲ）輸出入に関連する規則及び手続
（ⅳ）輸入品に対して、直接又は間接に課される内国税及び内国課徴金
（ⅴ）輸入品の国内における売買、輸送、分配又は使用に関する法令及び要件

最恵国待遇違反の可能性の例としては、GATSと同様に、EU-アメリカ間で構築されたセーフ・ハーバー枠組みによってアメリカに対して付与している待遇と、「十分性」審査を経ていない他国に付与している待遇との差別が挙げられる。

特に電子商取引におけるデジタルコンテンツは、その市場規模も年々拡大しており、現在のような差別的措置をEUが継続することは大いに問題があるだろう。

---

29 津久井茂充『ガットの全貌』(日本関税協会、初版、1993）19頁。

②数量制限禁止(11 条）との関係

【関連規定】

●数量制限禁止…GATT 第11 条

1　締約国は、他の締約国の領域の産品の輸入について、又は他の締約国の領域に仕向けられる産品の輸出若しくは輸出のための販売について、割当によると、輸入又は輸出の許可によると、その他の措置によるとを問わず、関税その他の課徴金以外のいかなる禁止又は制限も新設し、又は維持してはならない。

2　前項の規定は、次のものには適用しない。

(a) 輸出の禁止又は制限で、食糧その他輸出締約国にとつて不可欠の産品の危機的な不足を防止し、又は緩和するために一時的に課するもの

(b) 輸入及び輸出の禁止又は制限で、国際貿易における産品の分類、格付又は販売に関する基準又は規則の適用のために必要なもの

(c) 農業又は漁業の産品に対して輸入の形式のいかんを問わず課せられる輸入制限で、次のことを目的とする政府の措置の実施のために必要なもの

(i) 販売若しくは生産を許された同種の国内産品の数量又は、同種の産品の実質的な国内生産がないときは、当該輸入産品をもつて直接に代替することができる国内産品の数量を制限すること。

(ii) 同種の国内産品の一時的な過剰又は、同種の産品の実質的な国内生産がないときは、当該輸入産品をもつて直接に代替することができる国内産品の一時的な過剰を、無償で又は現行の市場価格より低い価格で一定の国内消費者の集団に提供することにより、除去すること。

(iii) 生産の全部又は大部分を輸入産品に直接に依存する動物産品について、当該輸入産品の国内生産が比較的にわずかなものである場合に、その生産許可量を制限すること。この(c) の規定に従って産品の輸入について制限を課している締約国は、将来の特定の期間中に輸入することを許可する産品の総数量又は総価額及びその数量又は価額の変更を公表しなければならない。さらに、(i) の規定に基いて課せられる制限は、輸入の総計と国内生産の総計との割合を、その制限がない場合に両者の間に成立すると合理的に期待される割合より小さくするものであってはならない。締約国は、この割合を決定するに当り、過去の代表的な期間に存在していた割合について、及び当該産品の取引に影響を及ぼしたか又は影響を及ぼしている特別の要因について、妥当な考慮を払わなければならない。

本条は、数量制限の禁止を明記している。国内産業保護のために考えられる手段のうち、輸入数量制限の場合、輸出国がある国に対して商品を輸出するためのいかなる努力を行っても、その定められた数量以上には輸出することができず、GATTが掲げている自由貿易の拡大という目的が著しく妨げられることになる。

関税の場合は、商品の質、価格の面での努力いかんでは、ある程度の関税が課されても、この関税の障壁を乗り越えて、輸入することができる。また、関税は各国の税率が明らで公平な適用を受けることが容易だが、輸入数量制限は内容が行政当局の自由裁量によって決定されることが多く、差別的・恣意的な扱いを受ける可能性もあり、きわめて不透明な措置となるおそれがある。

国際貿易に対する障壁の中で、数量制限は貿易を阻害する効果としてはより直接的かつ強力なものであり、世界の経済活動に対して著しい抑圧を強いるものである[30]。そのため、GATTに数量制限の一般的禁止が盛り込まれた。

本条の違反該当可能性として、次のような数量割当制限の問題が考えられる。例えば、「十分性」を認めない国の企業に対しては、原則として一切のコンテンツ配信、海外移転は行うことを認めない。他方、「十分性」を認めた国には自由にそれを行うことを認めている。これは、国際移転の全面禁止＝割当量がないという数量割当規制にあたりうる。よって、EUの措置は、GATT11条の要件を満たす数量制限として問題になるだろう。

③一般的例外規定(20条)該当性の検討

【関連規定】

●一般的例外…GATT第20条

この協定の規定は、締約国が次のいずれかの措置を採用すること又は実施することを妨げるものと解してはならない。ただし、それらの措置を、同様の条件の下にある諸国の間において任意の若しくは正当と認められない差別待遇の手段となるような方法で、又は国際貿易の偽装された制限となるような方法で、適用しないことを条件とする。

(d) この協定の規定に反しない法令(税関行政に関する法令、第二条4及び第十七条の規定に基いて運営される独占の実施に関する法令、特許権、商標権及び著作権の保護に関する法令並びに詐欺的慣行の防止に関する法令を含む。)の遵守を確保するために必要な措置

本条は、GATTにおける各種の一般的例外を規定している。近年では、特に各国のとる環境規制との関係で議論になることも多くなっている。本条は、GATSの一般的例外規定と同様に、柱書と対象範囲を明示した個別条項の2部構成からなる。

ここで問題になるのは、同条（d）の法令遵守のために必要な措置である。GATSのところで述べたのと同様に、必要性テストを満たすかどうかがここでは重要である。

まず、GATSの場合と異なり、個人情報に関する明文上の規定がないので、EUの個人データ保護に関する規制が（d）の範疇にあたるかどうかが争いになるだろう。仮に（d）の範囲内であるとしても、次に柱書の差別的な制限のところが問題となる。ここでも、GATSの場合と同様に、アメリカに対してだけセーフ・ハーバー枠組みで特別に個人データの国際移転を認めるような差別的な措置を継続している限り、EUの柱書要件の該当可能性は低いと考えられる。

30 Ibid, at 25.

3　考察

国際経済法（WTO）の観点からEUの個人データ保護の国際移転の規制を検討してきたが、EU側はこの規制を専ら人権問題と考えるため、果たしてEUの規制がWTOの問題になりうるのかについては疑問が残る。

そこで、この疑問に答えるには、個人データ保護の法規制を巡る国際的動向やその背景を理解する必要がある。

最近の動向として、EUは従来の指令から規則レベルへの格上げを予定しており、超国家的な規制を強める傾向にある。このため、EUの規制強化によって、一般データ保護規則提案における各国の国内規制に対するEU規制の域外適用のために、貿易制限効果の発生が予想される[31]。

他方、アメリカでも規制強化の流れがある。ただし、アメリカの規制はあくまでも分野ごとであり、民間の自主規制をベースに行うというスタンスである。また、ビジネスの現場をみると、アメリカは、最近何かと話題になるfacebookのようにITを利用したビジネスがEUより活発で進んでいる。そして、通商法の世界では、アメリカはlevel playing fieldの発想の下、世界中で同一レベルの競争条件の下、自由で公正な競争を促進することを希求している[32]。WTOという貿易専門の国際機関ができたのは、その象徴ともいえる。

このように、自由なビジネスを希求するアメリカの要求が、EUによる個人データ保護の問題に対する国際経済法の観点からみた問題提起の背景にあるように思われる。

更に、EUの個人データ保護を巡る国際移転の規制は、広範な意味での貿易制限措置の対象となりうるので、これに反対する動きが益々高まる可能性があるだろう。

特に、EUにおける個人情報におけるプライバシー保護規制は基本的人権の保護の側面が強いとされるが、今回の規則提案を見る限りでは、越境取引規制という経済的側面をより一層重視した規定になってきている。

EUの規制強化によってグローバル経済活動への規制が強まると、貿易制限効果が高まることが予想されるので、より一層バランスのとれた適切な個人データ規制のあり方が重要になる[33]。

そこで、「十分性」認定を得ていない国の立ち回り方を検討するに、EUの規制はWTO協定に反する貿易制限的な措置であるとして、WTOの紛争処理の場で話し合いの機会を持つ必要性が生じてくる。

確かに、個人データ保護の掲げる人権保護という公共目的からみれば、EUの規制はWTOのGATSやGATTの一般的例外規定に該当し、WTO上違反とならないのかもしれない。

しかし、既に検討したように，EUが行っている個人データ保護を巡る規制の方法、特にセーフ・ハー

---

31 Shaffer, supra note 5 at 46.

32 See, John H. Jackson, The World Trading System - Law and Policy of International Economic Relations 17 (1st ed. 1992).

33 See, Lucas Bergkamp, *EU Data Protection Policy, The Privacy Fallacy: Adverse effects of Europe's Data Protection Policy in An Information-Driven Economy,* 18 Computer L. and Sec. Rep. 31 ,39 (2002).

バー枠組みでアメリカに対してのみ認めている措置の存続は最恵国待遇原則違反にあたる可能性が高いと思われる。これは、GATSやGATTの規定する一般的例外規定にある必要性要件を満たさず、恣意的で差別的な運用としてWTO協定違反になるおそれがある。

その上、EUの規制強化で域外適用のリスクが高まることは、WTOの掲げる自由貿易制度に対する大きな抜け穴となる危険性も指摘されている[34]。要するに、これは政治力のある大国が自国の見解（環境、社会、その他の国内基準）を他国に押し付ける問題ともいえる。そして、これらの見解の押し付けが、各種の保護主義の手段や一国主義的な社会厚生問題の言い訳として利用されることを避けるために、注意深く適切な境界線を設定することを求めていくべきである。

したがって、「十分性」認定を得ていない国としては、国内での個人情報保護の取組みと並行して、WTOの二国間協議の場でEU側と話し合う機会をもつことも選択肢から排除すべきではない。

仮にそのような機会に接したとして、当該国家が主張すべき2つのシナリオとして、
①EU側がセーフ・ハーバーに対する「十分性」認定を撤回すること
又は
②アメリカ以外の国にもセーフ・ハーバーを無差別に認めること
が考えられる。

①については、EU側にも潜在的需要はあるかもしれない。セーフ・ハーバー自体がWTO違反該当可能性がある上、アメリカ以外の国からセーフ・ハーバーに対するクレームがくることを恐れることがあり得るからである。

しかし、セーフ・ハーバーの廃止にはアメリカ側の反発が強そうである。

そこで、廃止を求める場合には、それと同時に、BCRなどの既存制度を利用者である外国企業にとって、より使い勝手や透明性を高めたものにしてもらうことを強く要求するべきである。当該国企業のグローバル展開に悪影響を与えることになれば、当該国から海外への企業の流出傾向を強める点で深刻な問題である。

②については、「十分性」審査で十分性が認められない、若しくは認められなさそうな共通利害を有する他国と協力して交渉することが求められる。また、EUとの間のサービス貿易の規模が大きい場合には、EUに対して貿易相手としての重要性を意識させるような形で、WTO協定違反可能性もちらつかせつつ交渉を有利に進めようとすることも必要かもしれない。

近年のGATSを巡るWTOの紛争処理事例をみると、中国関連で電子商取引がらみの案件（例えば、外国事業者の情報発信サービスの配信制限、電子支払サービスの制限措置など）がWTOの紛争処理の場に次々と上がってきている。

そのため、電子商取引とも関連の深いEUの規制を巡る本問題は、WTOの紛争処理の場での協議対象として検討可能なものであると考える。

---

34 Stefannie Zleptnig, Non-Economic Objectives in WTO Law: Justification Provisions of Gatt, Gats, Sps and Tbt Agreements, 318 (2010).

2　個人情報保護制度における国際的水準の実践面

＜1-1＞　欧州委員会
国際的水準の意義

一橋大学名誉教授　堀部　政男

1　はじめに

プライバシー・個人情報を保護しながら、その流通・利活用を図るという考え方は、その保護策が議論されるようになった当初から認識されていたといえる。その系譜についてはこれまでにも論じられてきた[1]。

今回の調査では、1995年10月24日に採択されたEUデータ保護指令（EU Data Protection Directive）の第三国への個人データの移転に関する規定が具体的にどのように適用されてきているかなどが主たる対象となっているが、個人データの国際流通は、1970年代に入って、一国の個人データが他国で処理されるような事例が出てきたことから、プライバシー・個人情報保護について国際的議論が必要になってきたことなども理解しなければならない。

2　国際的水準志向の国際的文書

国際的水準志向の国際的文書として挙げることができるものは、多数にのぼる。ここでは、そのいくつかの名称を掲げることにする。

（1）OECDプライバシー・ガイドライン（1980年）

後述する。

（2）CoE個人情報保護条約（1981年）

後述する。

（3）EUデータ保護指令（1995年）

後述する。

（4）APECプライバシー・フレームワーク（2004年）

本稿では割愛するが、概要については宮下紘「OECD・APEC・EU等の個人情報保護の国際的な取組」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（2009 年）3月、石井夏生利『個人情報保護法の理念と現代的課題』（勁草書房、2008年）340-342頁、同「OECD、APEC、EU等国際動向と日本への影響」情報ネットワーク法学会個人情報保護研究会「日本のプライバシー・個人情報保護とマネージメントシステムの国際標準化シンポジウム第1回」（2012年2月18日）資料等を参照。

（5）国際個人データ・プライバシー保護基準（2009年）

後述する。

（6）EU一般データ保護規則提案（2012年1月25日）

本報告書「EUデータ保護改革と国際的水準への影響」参照。

1　例えば、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報告書」、平成22年（2010年）3月参照。

3　OECDのプライバシー・ガイドラインと個人データの国際流通

（1）個人データ保護と国際流通の障害

経済協力開発機構（Organisation for Economic Co-operation and Development: OECD）では、1960年代末ころからデータ保護について議論が始まった。欧州では、1970年代に個人情報保護法制定国が現れた。それらの国の中には、個人データの海外移転・国際移転についてデータ保護機関（Data Protection Authority, DPA）と総称されることのある独立性の強い機関の承認を要するものもあった。一方、データ処理に長けている国は、そのようなプライバシー保護（protection of privacy）傾向に対抗するために情報の自由な流れ（free flow of information）を主張するようになった。

この利害対立の調整をゆだねられたのが、OECDであった。 OECDは、1978年初めに、「国際データ障害とプライバシー保護専門家グループ」(Expert Group on Transborder Data Barriers and Privacy Protection）という新しいアド・ホックのグループを設置し、個人データの国際流通と個人データ及びプライバシーの保護についての基本的ルールに関するガイドラインを作成するように指示した。

（2）OECDプライバシー・ガイドラインの採択

OECDは、この専門家グループの作業を基に、1980年9月23日に「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」(Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data)を採択した。この理事会勧告は、プライバシー保護の国際水準を示したものとして注目に値するとともに、日本においては、プライバシーをどのようにして保護するかを国レベルで検討する契機の一つになった。これは、最近では、OECDプライバシー・ガイドライン（ OECD Privacy Guidelines）と呼ばれている[2]。

このガイドラインには「解説メモランダム」(Explanatory Memorandum）が付されている。それをも見るならば、個人データの国際流通と各国のプライバシー・個人情報保護法の関係に関する議論がどのようなものであったかを知ることができる。それは、現代の問題を考えるに当たっても参考になる。

2　OECDプライバシー・ガイドラインなどについては、
http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html
で閲覧できる。邦訳は行政管理庁行政管理局の仮訳によるが、一部改訳したところもある。
日本の文献では、とりあえず、堀部政男『現代のプライバシー』(岩波書店、1980年)、同『プライバシーと高度情報化社会』(岩波書店、1988年)、行政管理庁行政管理局監修・財団法人行政管理研究センサー編集『改訂世界のプライバシー法』(ぎょうせい、1982年)（この改訂版には加藤一郎東京大学法学部教授と堀部政男一橋大学法学部教授［いずれも当時］の「推薦のことば」が掲載されている)、石井夏生利『個人情報保護法の理念と現代的課題―プライバシー権の歴史と国際的視点』（勁草書房、2008年）等参照。

（3）OECDプライバシー・ガイドラインの背景

解説メモランダムは、ガイドラインの一般的背景について次のように述べている。

「1970年代は、個人データの収集及び使用についてのプライバシーの保護に関する調査検討及び立法活動が活発化した時代と言えるであろう。数多くの公式の報告書で指摘していることは、問題が政治レベルで真剣に取り上げられているが、同時に、相反する利害を調整するという作業は、デリケートであり、かつ、一度限りではなかなか解決し難い、ということである。一般の関心は、個人データのコンピュータ処理に伴うリスク及びそのかかわりあいに集中する傾向があり、いくつかの国では、コンピュータ及びコンピュータ支持の活動のみに限定した法律を制定する選択をしている。他の国では、特定のデータ処理技術に関係なく、むしろプライバシー保護問題に対するより一般的なアプローチを採用している。」

解説メモランダムは、当時における加盟国の立法化などを明らかにした後、データ保護と情報の自由な流通について次のように記している。

「いくつかの理由により、個人データの取扱いについて、個人の保護措置を講ずる問題は、一国のレベルのみでは完全には解決し得ない。国境を越えるデータ流通の飛躍的な増加と国際的なデータ・バンク（検索その他の目的のためのデータの収集）の形成は、国家間の協調的行動の必要性を高めてきていると同時に、データの保護及びその収集、処理、流布の制限への要請とに対し、適当なバランスが取られなければならないという情報の自由な流通を擁護する議論を支持するものとなっている。」

このような背景を踏まえてOECD理事会勧告はまとめられた。そのことが理事会勧告の中に要約されている。

（4）理事会勧告の認識

まず、OECD理事会は、次のような認識を明らかにしている。

「1960年12月14日のOECD条約第1（c）、3（a）及び5（b）の各項に留意し、加盟国は、国内法及び国内政策の相違にもかかわらず、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、個人データの自動処理及び国際流通は、国家間の関係に新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、プライバシー保護と個人データの国際流通に係る国内法は、そのような国際流通を妨げるおそれがあること。」

（5）勧告の内容

理事会は、このような認識に基づき「加盟国間の情報の自由な流通を促進すること及び加盟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決意し」､勧告した。この中で「加盟国間の情報の自由な流通を促進すること」と「加盟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」が重要視されていることは、現代においても注目される必要がある。その具体的な勧告内容は、次のとおりである。

1　加盟国は、本勧告の主要部分である勧告付属文書のガイドラインに掲げているプライバシーと個人の自由の保護に係る原則を、その国内法の中で考慮すること。

2　加盟国は、プライバシー保護の名目で個人データの国際流通に対する不当な障害を創設することを除去し又は回避することに努めること。

3　加盟国は、勧告付属文書に掲げられているガイドラインの履行について協力すること。

4　加盟国は、このガイドラインを適用するために、特別の協議・協力の手続についてできるだけ速やかに同意すること。

これらのうち、特に「2　加盟国は、プライバシー保護の名目で個人データの国際流通に対する不当な障害を創設することを除去し又は回避することに努めること」が国際流通の面では重要である。

しかも、1980年段階では、「1　加盟国は、本勧告の主要部分である勧告付属文書のガイドラインに掲げているプライバシーと個人の自由の保護に係る原則を、その国内法の中で考慮すること」ということで、加盟国でこのガイドラインに準拠した国内法が整備されるであろうという期待と見通しがあったと見ることができる。これは、加盟国でプライバシー・個人情報保護法が制定されるならば、それらの国の間では、自由な情報流通を確保して行こうとする考え方に基づいている。

しかし、加盟国の中でも経済大国である日本の立法化は、1988年に「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律」は制定されたものの、民間部門を対象とする個人情報保護法が2003年に制定されたことに見られるように、大幅に遅れた。

立法化が進んだ欧州からすると、自国民の権利を保護するために、第三国が後述のような「十分性」の基準を確保している場合に限って、移転を認めるという発想になってきた。

（6）勧告付属文書の構成

ここに出てくる勧告付属文書「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」は、第１部・総則、第２部・国内適用における基本原則、第３部・国際適用における基本原則 ―自由な流通と合法的制限、第４部・国内実施、及び第５部・国際協力からなっている。それらのうち、第２部の「国内適用における基本原則」が、日本におけるプライバシー保護を考える上でとりわけ重要な役割を果たしてきている。その８原則は、上掲の第２部「国内適用における基本原則」に示されているが、日本ではあまりにも有名であるので、説明は省略し、原則のみを掲げることにする。それらは、次のようになっている。

① 収集制限の原則 (Collection Limitation Principle)

② データ内容の原則 (Data Quality Principle)
③ 目的明確化の原則(Purpose Specification Principle)
④ 利用制限の原則(Use Limitation Principle)
⑤ 安全保護の原則(Security Safeguards Principle)
⑥ 公開の原則(Openness Principle)
⑦ 個人参加の原則(Individual Participation Principle)
⑧ 責任の原則(Accountability Principle)

（7）国際適用における基本原則―自由な流通と合法的制限

第3部の国際適用における基本原則―自由な流通と合法的制限は、次のようになっている。

「15 加盟国は、個人データの国内における処理及びその再移出が、他の加盟国に及ぼす影響について配慮すべきである。

16 加盟国は、単なる通過も含めた個人データの国際流通が阻害されず、安全であることを確保するために、あらゆる合理的かつ適当な手段を講ずべきである。

17 加盟国は、自国と他の加盟国との間における個人データの国際流通を制限することを控えるべきであるが、後者が未だガイドラインを実質的に遵守していない場合、又はかかるデータの再移出がその国のプライバシー保護規制を免れようとする場合は、この限りでない。

加盟国は、また、自国のプライバシー法制が、その性格からして特別の規制をしており、かつ他の加盟国が、自国と同等の保護を課していないある種の個人データに関しては、その流通を制限することができる。

18 加盟国は、プライバシーと個人の自由の保護という名目で、これらの保護に必要とする程度を超え、かつ、個人データの国際流通に対して障害を創設することになるような法律及び政策並びに運用を差し控えるべきである。」

これまでの叙述やこれらからの基本原則からも明らかなように、一方では、同等な個人データ保護法の制定を勧告しながら、他方では、それが個人データの国際流通の妨げにならないように勧告している。

（8）OECDのプライバシー保護法執行越境協力

プライバシー・個人情報が瞬時にして国境を越えて地球を駆け巡る状況に対応することも踏まえ、OECDでは、2005年からプライバシー保護法の執行に関する国際協力について検討してきた。これに直接かかわってきたが、2007年6月12日に「プライバシー保護法の執行における越境協力に関するOECD 理事会勧告」(Recommendation of the OECD Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy）を採択した（これについては、拙稿「ユビキタス社会と法的課題―OECDのインターネット経済政策による補完」、ジュリスト2008年8月1・15日号を参照されたい。）

4　CoE 個人情報保護条約の締結

（1）CoE と個人情報保護条約

OECD と協力し、歩調を合わせながら、データ保護について検討してきた欧州評議会（Council of Europe, CoE）は、OECD プライバシー・ガイドラインとほぼ同じ時期に個人情報保護条約を策定した。

ちなみに、この CoE は、欧州統合の推進を目的として第二次大戦後の 1949 年に設立された国際機関で、日本の外務省の資料によると、現在の加盟国は 47 か国（EU 全加盟国、南東欧諸国、ロシア、トルコ、NIS 諸国の一部）である。その CoE の閣僚委員会は、1980 年 9 月 17 日、「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）（条約第 108 号（Convention 108））を採択した[3]（当時の加盟国は 21 か国であった）。そして、この条約は、翌 1981 年 1 月 28 日[4]、各国の署名に付され、1985 年に、5 か国目の西ドイツが批准をしたので、同年 10 月 1 日に、発効した。この条約に具体化されている個人データ保護の原則は、内容的には OECD 理事会勧告のそれとほぼ同じであるが、形式的には異なった方法で定められている。それらは、欧州諸国を基準とした、個人情報の国際水準を示している。

（2）CoE 個人情報保護条約の概要

7 章 27 か条からなる条約のうち、第 2 章がデータ保護に関する基本原則と題されていて、第 4 条から第 11 条に及んでいる。それらのうち、主要なものと考えられる第 5 条（データ内容）、第 6 条（特別の種類のデータ）、第 7 条（データの安全保護）及び第 8 条（データ主体のための追加的保護措置）を紹介するにとどめることにする。

・データ内容等

まず、データ内容（Quality of data）に関する第 5 条は、次のようになっている。

「自動処理を受ける個人データは、

a 公正かつ適法に収集され、処理される。

b 明確化されたかつ正当な目的のため蓄積され、かつこれらの目的に合致しない形で利用されない。

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。」

3　CoE 条約については、
http://conventions.coe.int/treaty/en/treaties/html/108.htm
で閲覧できる。邦訳は行政管理庁行政管理局の仮訳によるが、一部改訳したところもある。日本の文献では、とりあえず、堀部政男『現代のプライバシー』（岩波書店、1980 年）、同『プライバシーと高度情報化社会』（岩波書店、1988 年）、行政管理庁行政管理局監修・財団法人行政管理研究センサー編集『改訂世界のプライバシー法』（ぎょうせい、1982 年）、石井夏生利『個人情報保護法の理念と現代的課題―プライバシー権の歴史と国際的視点』（勁草書房、2008 年）等参照。

4　1 月 28 日は記念すべき日となっており、Data Protection Day として各種の行事が行われている。

これは、OECDガイドラインの収集制限の原則、データ内容の原則、目的明確化の原則及び利用制限の原則に対応している。

次に、特別の種類のデータ（Special categories of data）に関する第6条は、「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。罪科に関する個人データについても同様とする」と定めている。

欧州諸国のデータ保護法には、センシティブなデータについて特別の保護措置がとられている場合があるので、このような条項が設けられたとみてよいであろう。

・データの安全保護等

また、データの安全保護（Data security）についての第7条は、「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当な安全保護措置をとる」としている。

これは、OECDガイドラインの安全保護の原則に相当する。

さらに、データ主体のための追加的保護措置（Additional safeguards for the data subject）にかかわる第8条は、次のように規定している。

「何人も、

a　自動処理個人データフアイルの存在、その主たる目的、及びフアイル管理者の身元、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アイルに蓄積されているか否かを確認し、又、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　この条約の第五条及び第六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われる場合には、それぞれの場合に応じて当該データを修正、又は消去することができる。

d　この条の（b）及び（c）にいう確認請求、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。」

このデータ主体のための追加的保護措置は、OECDガイドラインの公開の原則及び個人参加の原則に対応する。

（3）非加盟国の加入

日本は、CoEの加盟国ではないが（1996年以降、日本はオブザーバー）、このCoE条約は、非加盟国の加入（Accession by non-member States）についても条項を設けている。これに関する第23条は、次のように定めている。

「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の3か月の期間を満了した日の属する月の翌月の第一日に効力を発生する。」

前述のように、このCoE条約は、1985年10月1日に発効したので、条約上は、欧州評議会閣僚委員会が、日本に対して、CoE条約への加入を招請することができる。1980年代後半にこのような議論もあった。

（4）追加議定書

2001年11月8日に、「個人データの自動処理に係る個人の保護に関する条約への監督機関及び越境データ流通についての追加議定書」（Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and trasborder data flows）が各国の署名に付された。

これは、3か条からなるもので、各条の条文見出しは、次のようになっている。

第1条　監督機関（Supervisory authorities）

第2条　本条約の締約国の管轄に服さない受領者への個人データの越境流通（Transborder flows of personal data to a recipient which is not subject to the jurisdiction of a Party to the Convention）

第3条　最終条項（Final provisions）

5　EUデータ保護指令

（1）モデルとなったCoE条約

日本では、上掲のOECDプライバシー・ガイドラインは有名であるのに対して、CoE条約についてはこれまでにも紹介してきているけれども、意外に知られていない。

ところが、欧州においては、CoE条約が大きな役割を担ってきている。CoE条約は、欧州では、データ保護基本権（fundamental right to protection of personal data）に関する最初の法的枠組みであると考えられているものであって、後述するEUデータ保護指令のモデルであるということができる。

（2）データ保護指令提案の採択

ア　最初のデータ保護指令提案[5]

当時の欧州共同体（European Communities, EC）理事会（Council）は、1990年7月27日に、①「個人データ取扱いに係る個人の保護に関する理事会指令提案」（Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data）及び②「公衆デジタル通信網特にISDN及び公衆デジタル移動体通信網における個人データ及びプライバシー保護

5　EUデータ保護指令については、1990年7月27日に公表された直後から論じ始めた。とりあえず、堀部政男「情報化とプライバシー」、ジュリスト1000号（1992年5月1日-15日号）（新世紀の日本法：GLOBAL時代の針路）参照。

に関する理事会指令提案」(Proposal for a Council Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks, in particular the integrated services digital networks (ISDN) and public digital mobile networks）を採択した。

この段階で、①のデータ保護指令提案は、日本のようにEC構成国（当時）でない第三国への個人データの移転についても規定していた（第24条)。その第1項は、次のようになっていた。

「構成国は、取扱い過程にある個人データ又は取扱いを目的として収集された個人データの第三国への移転は一時的又は恒久的であるかを問わずその国が十分なレベルの保護（adequate level of protection）を確保している場合に限って行うことができるということをその法に規定しなければならない。」

また、その第3項は「委員会は、構成国によって提供された情報に基づき又はその他の情報に基づき第三国が十分なレベルの保護をしていないと認定し、また、その結果として生ずる状況が委員会又は構成国の利益を害するおそれがあると認定する場合には、その状況を矯正する目的で交渉に入ることができる」と日本を含む第三国と交渉することがあり得ることを明らかにしていた。

ここに出てくる指令（Directive）というのは、当時においては、EEC条約において、「達成すべき結果について、これを受領するすべての構成国を拘束するが、方式及び手段については構成国の機関の権限に任せる」(同条約第189条）ものである（これに対し、最も拘束力の強い規則（Regulation）は、「一般的な効力を有し、そのすべての要素について義務的であり、すべての構成国において直接適用することができる」というものである)。換言すれば、指令は、規則のように直接適用するものではないが、構成国を拘束することに注意する必要がある。こうすることによって、構成国間において個人データ保護法の調和・統一を図ろうとする方向が出てきている。

イ　改正提案と採択

この最初のデータ保護指令提案をめぐって各方面で多彩な議論が展開された。それらの議論を踏まえて、EC委員会は、1992年10月15日、「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理事会指令の改正提案」(Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data）を明らかにした。

最初の提案の第24条は、改正提案では第26条となり、ただし書が追加された。それは、次に掲げる場合には、十分な保護を講じていない第三国に対しても移転を行うことができるとするものである。

―……データ主体が契約締結に先立って手段を講じるために提案された移転に同意した場合

―データ主体が十分な保護を講じていない第三国にデータを移転することが提案され又は
提案されることがあり得るという事実について情報を与えられていることを条件として、
その移転がデータ主体と管理者との間の契約の履行のために必要である場合

―移転が重要な公益上の理由で必要な場合

―移転がデータ主体のきわめて重大な利益を保護するために必要である場合

ちなみに、1991年12月にオランダのマーストリヒトで開催された理事会で「欧州連合条約」(Treaty on European Union)(一般に「マーストリヒト条約」と呼ばれている。)の締結について合意され、1992年2月にこの条約が調印された。マーストリヒト条約は、1993年11月1日に発効し、欧州連合(European Union, EU)が発足した。

その後、欧州議会及び理事会は、1995年2月20日に「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・・・指令を採択するために1995年2月20日に理事会によって採択された・・・共通の立場」(Common Position...adopted by the Council on 20 February 1995 with a view to adopting Directive...of the European Parliament and of the Council of...on the protection of individuals with regard to the processing of personal data and on the free movement of such data)を明らかにした。

これは、「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1995年10月24日の欧州議会及び理事会の95／46／EC指令」(Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data)として採択された[6]。これがEUデータ保護指令(EU Data Protection Directive)、指令95/46/EC(Directive 95/46/EC)などと略称されているものである。

このEUデータ保護指令は、3年後の1998年10月24日に発効した。

また、前掲の②の「公衆デジタル通信網特にISDN及び公衆デジタル移動体通信網における個人データ及びプライバシー保護に関する理事会指令提案」は、これまでに見てきたデータ保護指令よりもかなり遅れて、1997年12月15日に「電気通信分野における個人情報取扱い及びプライバシー保護に関する1997年12月15日の欧州議会及び理事会の指令97/66/EC」(Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector)として採択された。この1997年の電気通信分野の指令は、2002年7月12日に「電子通信分野における個人情報取扱い及びプライバシー保護に関する2002年7月12日の欧州議会及び理事会の指令2002/58/EC(プライバシー及び電気通信に関する指令)」(Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)によって全面的に修正された。

6　EUデータ保護指令については、
http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf
で閲覧できる。この邦訳については、堀部政男研究室仮訳「EUデータ保護指令」参照。本報告書の資料として掲載する。また、例えば、堀部政男「EU個人情報保護指令と日本」、『変革期のメディア』(ジュリスト増刊号(1997年6月))358頁以下、同「EU(欧州連合)個人情報保護指令の経緯とその仮訳」、新聞研究1999年9月号17頁参照。

ウ　EUデータ保護指令前文の第三国移転言及

EUデータ保護指令の全体的構成など明らかにしなければならない課題は多いが、ここでは、第三国への個人データの移転について見るので、その点に限定して検討するにとどめることにする。

EUデータ保護指令は、本文34ヶ条の前にリサイタル（recitals）という72の条項がある。前文といえるものであるが、そのうち、個人データの第三国移転については、第56項から第60項までの5項にわたって、この直ぐ後で検討する本文第25条及び第26条の導入部ともいうべき説明がなされている。最初の第56項及び第57項は、次のようになっている（「…ので」という表現になっているが、これはこの種の文書の書出しのwhereas の訳である）。

「（56）個人データの越境流通は国際取引の拡大にとって必要であるので；本指令によって欧州連合で保障されている個人の保護は十分なレベルの保護を確保している第三国への個人データの移転の妨げとはならないので；第三国によって提供される保護レベルの十分性は移転活動又は一連の移転活動を取り巻くすべての状況に照らして評価されなければならないので；
（57）他方、十分なレベルの保護を確保していない第三国への個人データの移転は禁止されなければならないので；」

エ　第三国への個人データの移転―第25条[7]

第三国へのデータの移転については、「諸原則」（Principles）に関する第25条で最初のデータ保護指令提案の第24条の「諸原則」とは少し異なる規定が設けられている（「共通の立場」の段階で修正）。その第1項は、次のようになった。

「構成国は、取扱い過程にある個人データ又は移転後取り扱うことを目的とする個人データの第三国への移転は、この指令の他の規定に従って採択されたその国の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（adequate level of protection）を確保している場合に限って行うことができるということを規定しなければならない。」

この十分性の評価がどのようになされるかについては、第25条第2項に規定されている。
その第25条第2項は、次のようになっている。

「第三国によって保障される保護レベルの十分性は、一つのデータ移転の運用又は一連のデータ移転の運用に関するあらゆる状況にかんがみ評価されなければならない。特に、データの性格、予定されている取扱いの運用の目的及び期間、発出国及び最終目的国、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（the rules of law, both general and sectoral, in force in the third country in question）、並びに当該国において遵守されている専門的規範（professional rules）及び安全保護対策措置（security measures）が考慮されなければならない。」

7　消費者庁、前掲注1参照。また、堀部政男「プライバシー・個人情報保護の国際的整合性」、
同編著『プライバシー・個人情報保護の新課題』（商事法務、2010年）29頁以下参照。

第25条の第3項以下の規定は、次のようになっている。

「3. 構成国及び委員会は、第三国が第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ないと考えられる事例について、相互に情報提供しなければならない。

4. 構成国は、第31条第2項に規定する手続に基づいて委員会が、第三国が本条第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ないと認定した場合には、当該第三国への同一タイプのデータの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。

5. 委員会は、適切な時期に、第4項に基づく認定によってもたらされる状況を改善することを目的とする交渉を開始しなければならない。

6. 委員会は、第31条第2項に規定する手続に基づいて、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。

構成国は、委員会の決定を遵守するために必要な措置を講じなければならない。」

オ 第26条 例外

第25条につづく「第26条 例外」は、次のように規定している。

「1. 構成国は、第25条の適用を制約するものとして、及び特別な場合を規律する国内法に別段の定めがある場合を除いて、第25条第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ない第三国に対する個人データの移転又は一連の移転は、次の条件を満たした場合に行うことができることを定めなければならない。

（a）データ主体が、予定されている移転に対して明確な同意を与えている場合。又は、

（b）移転が、データ主体及び管理者間の契約の履行のために、又はデータ主体の請求により、契約締結前の措置の実施のために必要である場合。又は、

（c）移転が、データ主体の利益のために、データ主体及び第三者間で結ばれる契約の締結又は履行のために必要である場合。又は、

（d）移転が、重要な公共の利益を根拠として、又は法的請求の確定、行使若しくは防御のために必要である場合、又は法的に要求される場合。又は、

（e）移転が、データ主体の重大な利益を保護するために必要である場合。又は、

（f）法律又は規則に基づいて情報を一般に提供し、及び公衆一般又は正当な利益を証明する者のいずれかによる閲覧のために公開されている記録から、閲覧に関する法律に規定された条件が特定の事例において満たされる範囲内で、移転が行われる場合。

2. 構成国は、第1項の規定に実体的な効果を持つことなく、管理者が個人のプライバシー並びに基本的な権利及び自由の保護、並びにこれらに相当する権利の行使に関して、十分な保護措置を提示する場合には、第25条第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ない第三国への個人データの移転又は一連の移転を認めることができる。保護措置は、特に適切な契約条項から帰結することができる。

3. 構成国は、第2項によって付与された許可を、委員会及び他の構成国に通知しなければならない。

一つの構成国又は委員会が、個人のプライバシー並びに基本的な権利及び自由の保護を含む正当な理由に基づいて異議申立てを行った場合には、委員会は、第31条第2項に規定された手続に基づいて適切な措置を講じなければならない。

構成国は、委員会の決定を遵守するために必要な措置を講じなければならない。

4. 構成国は、第31条第2項に規定された手続に従って、一定の標準契約条項が本条第2項によって要求される十分な保護措置を提供していると決定する場合には、委員会の決定を遵守するために必要な措置を講じなければならない。」

（3）十分性認定基準

ア　第29条作業部会の「作業文書」

今回の調査にとって特に重要であるのは、「十分性」の認定基準である。

EUデータ保護指令に定められている第29条作業部会（Article 29 Working Party）は、EUデータ保護指令の「十分性」基準（データ保護指令第25条及び第26条）に基づいて評価を行うが、具体的には、「個人データの第三国移転：EUデータ保護指令第25条及び第26条の適用」(WP 12 5025/98)(Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive（WP 12 5025/98)(adopted by the Working Party on 24 July 1998)（以下「WP 12」という。）という文書[8]によっている。

WP 12は、次のような章などからなっている。

8　欧州委員会の十分性認定の基準は、2012年1月25日公表のEU一般データ保護規則提案が採択されるまでは、現行のEUデータ保護指令に規定されているところであり、その解釈は、このWP 12によることになる。2012年2月に欧州委員会司法総局のデータ保護担当者に対して、WP 12の改定の予定を尋ねたところ、それはないとのことであったので、当分の間はこれを参照する必要がある。

これらのうち、第1章（Chapter 1）の「何が『十分な保護』を構成するか」には、具体的な基準が示されている。その一部を紹介すると、次のようになる。

（ｉ）実体原則（Content Principles ）

基本原則は、次のとおりである。

1）目的限定原則（purpose limitation principle）

2）データ内容・比例原則（data quality and proportionality principle）

3）透明性原則（transparency principle）

4）セキュリティ原則（security principle）

5）アクセス、訂正及び異議申立ての権利（rights of access, rectification and opposition）

6）再移転制限（restrictions on onward transfers）

追加的原則の例

1）センシティブ・データ（sensitive data）

2）ダイレクト・マーケティング（direct marketing）

3）自動処理による個人に関する決定（automated individual decision）

（ii）手続／執行メカニズム（Procedural/ Enforcement Mechanisms）

データ保護システムの目的は、基本的には次の3要素を満たすことである。

1）ルールの善良なレベルのコンプライアンス（a good level of compliance）を果たすこと。

2）データ主体がその権利を行使するに当たって個々のデータ主体に支援と援助（support and help to individual data subjects）を提供すること。

3）ルールが遵守されなかった場合に被害者に適切な救済策（appropriate redress）を提供すること。

（4）十分性認定手続

EUデータ保護指令の十分性の要件については、前掲の第25条の規定から明らかであるが、その第25条第6項の規定、すなわち、「6．委員会は、第31条第2項に規定する手続に基づいて、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」という規定は、理事会及び欧州議会が欧州委員会に対して、十分性の認定をする権限を付与したものである。その認定手続は、通常、次のようになっている[9]。

① 欧州委員会の提案

② 構成国のデータ保護コミッショナーのグループである第29条作業部会（Article 29 working party）の意見

9　後掲の日白協会（Belgium-Japan Association）主催のデータ保護会議（BJA-Conference on Data Protection）におけるハナ・ペチャコバ（Hana Pechackova）女史のプレゼンテーションによる。

③ 構成国の多数決による第31条専門委員会の意見
④ 欧州委員会がその執行権限を適正に行使したかをチェックするための欧州議会による30日間の調査
⑤ 欧州委員会委員合議体（College of Commissioners）による決定の採決

（5）オーストラリアに関する評価[10]

十分性が認定されている諸国等については、別稿で扱われるが、ここでは、オーストラリアに関する評価を見ることにする。

オーストラリアの2000年プライバシー修正（民間部門）法（Privacy Amendment (Private Sector) Act 2000）について、第29条作業部会は、「オーストラリアへのデータ移転は、上述の懸念に見合う適切な保護措置が導入された場合にのみ十分であると見ることができると考える」という結論を出した[11]。

その意見（OPINION）として掲げられている項目の概要は、次のようになっている（ここでは、要約している場合があり、また、番号も適宜付した）。

(1) 適用除外されるセクター及び活動（Sectors and activities excluded）

作業部会は、いくつかのセクター及び活動が法の保護から除外されることを懸念する。

特に、

・小規模ビジネス（small business）（法第6D条は、年間の総売上高が300万オーストラリアドル（1ドル75円として、2億2,500万円）以下のビジネスと規定している）が適用除外であること。

・被用者データ（employee data）が適用除外であること。

(2) 除外（Exceptions）

全国プライバシー原則2.1(g)（National Privacy Principle NPP 2.1(g)）が、情報の利用又は開示が法により要求され又は授権される場合には、二次的目的のために利用され又は開示されることを認めていること。

(3) 一般に利用可能なデータ（Publicly available data）

一般に利用可能な公刊物に掲載することを目的とするデータの収集は、NPPs　1（収集）の範囲内に入るが、一度、情報が一般に利用可能な公刊物の定義に該当するようなフォーマットで編集されるならば、他のプライバシー原則が適用されなくなること（これは、アクセス及び訂正のような個人の権利を排除することになる）。

---

10 堀部、前掲注7　49頁以下参照。

11 Article 29 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.

(4) データ主体への透明性（Transparency to data subjects ）

NPP1.3（収集）は、組織が収集前又は収集時の個人に通知することを認めているが、しかし、これが現実的でないならば、その後において可及的速やかに通知してもよいと付け加えている。収集が行われた後に組織が個人に通知することを認めることは、OECDガイドラインの目的明確化の原則（個人データの収集は、収集時より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、目的の変更ごと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）に反する。

(5) 特にダイレクト・マーケティングに関するデータの収集及び利用（Collection and use of data in particular with regard to direct marketing）

NPP 1（収集）及び2（利用及び開示）は、個人情報の収集はその必要性、公正かつ適法な手段によることを要求することにより、また、利用及び開示に限定及び条件を課すことにより、目的明確化の原則をカバーしている。しかし、ダイレクト・マーケティング用に個人データを利用するためには、個人の同意を得ることを必ずしも必要としていない。

(6) センシティブ・データ（Sensitive data）

NPP10（センシティブ・データ）は、センシティブ・データの収集のみに制限を課しているにすぎない。NPP2にいくつかの規定がある健康データ以外のセンシティブ・データの利用又は開示に対して特別な制限又は条件はない。

(7) EU市民の訂正権の欠如（Lack of correction rights for EU citizens）

第41条第（4）項は、NPP6又は7に基づき、オーストラリア市民又は永住者のプライバシーに対する干渉がある場合にのみその行為又は実態をプライバシー・コミッショナーが調査することを認めている。その結果、永住権を持たないEU市民は、アクセス権及び訂正権を行使できない。

(8) オーストラリアから第三国への再移転（Onward transfers from Australia to other third countries）

オーストラリアから第三国への再移転を禁止していない。

（6）日本に関する評価

ア　ブリュッセルのデータ保護会議の開催（2009年4月23日）とアジェンダ

ベルギーの首都ブリュッセルにおいて、2009年4月23日、日白協会（Belgium-Japan Association）主催のデータ保護会議[12]（BJA-Conference on Data Protection）が開催された。この会議は、BJA副理事長であるタンギー・バン・オーバーストラテン（Tanguy Van Overstraeten）弁護士（リンクレーターズ法律事務所（Linklaters LLP）のパートナー）が中心になって企画された。

---

12 堀部、前掲注7 52頁以下参照。今回の調査で十分性認定手続について情報提供を要請したが、政治的な面があるということや内部的なものであるということで具体的なまとまった情報を得ることができなかった。この会議の模様は、貴重である。

2009年4月23日の「EUと日本におけるプライバシー・個人情報保護」(Privacy and Personal Data Protection between EU and Japan) 会議と称することができるデータ保護会議のアジェンダは、次のようになった。

○ 序論（Introduction）リンクレーターズ法律事務所 タンギー・バン・オーバーストラテン
○ 日本におけるプライバシー・個人情報保護（Privacy and personal information protection in Japan） 一橋大学名誉教授　堀部政男
○ 欧州連合におけるデータ保護―EUから第三国への個人データ移転（Data Protection in the European Union - Personal Data Transfers from the EU to third countries）
タンギー・バン・オーバーストラテン
○ 十分性認定手続（Adequacy finding procedure） 欧州委員会・司法自由安全総局[13]
（European Commission Directorate-General-Justice, Freedom and Security）法務政策部（Legal Affairs and Policy）ユニットD5・データ保護（Unit D5 -Data Protection）事務官（Desk Officer）ハナ・ペチャコバ[14]（Hana Pechackova）
○ 日本におけるデータ保護―2006年第一段階のCRIDによる調査結果（Data Protection in Japan: Findings by CRID in FIRST STEP report of 2006）［CRIDは Centre de recherche informatique et droit（情報法研究センター）の略[15]］ナミュール大学教授（Prof. at the University of Namur）イブ・プレ（Yves Poullet）→当日、プレ教授が病気のため出席できなかったので、フランク・デュモルチィエ（Franck Dumortier）氏が出席して講演
○ ケース・スタディ：EUにおけるAGCのデータ保護ルールの取扱い（Case study: AGC dealing with data protection rules in the EU）AGC Europe［AGC は、Asahi Glass Corporation］租税・監査・リスク・マネージメント・デレクター（Tax, Audit & Risk Management Director）
エマニュエル・ハザール（Emmanuel Hazard）
○ 閉会の辞（Closing remarks） タンギー・バン・オーバーストラテン

イ　ブリュッセルのデータ保護会議の意義

このデータ保護会議は、大変有益であったといえる。内容面についてはいうまでもないが、これまでは非公開の場で知り得ていたことの一端が公の場で議論されたことが極めて重要な意味を持っているからである。OECDのWPISP（Working Party on Information Security and Privacy, 情報セキュリティ・プライバシー作業部会）副議長としてOECDの会議に出席する機会は、1996年から2008年までの12年間続いた。また、政府の仕事でブリュッセルを訪ねることもしばしばあった。これらの機会に欧州委員会関係者等と意見交換した回数は、数え切れないほどであった。そのような機会に知り得たことを公開することは国益に反する場合があることも考慮してこれまで発言することを差し控えてきた。

---

13 現在は、司法総局（Directorate-General for Justice）である。

14 昨年、他の総局に異動した。

15 現在は、crids（Centre de Recherche Information, Droit et Société）である。

ところが、2009年4月、公開の場で欧州委員会関係者等と意見交換することができたことは、個人情報保護をめぐる日本とEUの議論を一定程度まで公開することを可能にしたと理解している[16]。

データ保護会議におけるスピーカーのプレゼンテーションは、それぞれ極めて重要であった。

しかし、そのすべてを紹介することは不可能であるので、ここでは、会議開催の趣旨、欧州委員会による日本個人情報保護法の評価手法、また、日本個人情報保護法に関する分析について少し述べるにとどめることにする。

ウ　欧州委員会の「十分性認定手続」―ペチャコバ女史のプレゼンテーション

このデータ保護会議では、前述のように、欧州委員会・司法内務総局のハナ・ペチャコバ女史が、「十分性認定手続」というプレゼンテーションを行った。すでに知り得ていたものもあるけれども、今回、公の場で初めて明らかになったものもあり、極めて重要な意味を持っている。2012年2月に欧州委員会司法総局の個人データ保護担当者は、十分性認定手続には政治的は面もあり、また、それは内部的なものでもあるということで明確は回答を避けたといえるので、女史のプレゼンテーションは、十分性認定手続、特に日本との関係を取り上げていることから、これを見ることにする。そのプレゼンテーションは、次のような構成と概要になっていた（番号は、本稿で説明する便宜上付けた）。

(1) プレゼンテーションの目的（Goal of the presentation）
- 基本的データ保護原則を含むEEA（欧州経済地域）における現行のデータ保護・プライバシー立法の概要
- 十分性認定手続とは何か及び欧州委員会は日本への対応はどのようなところにあるかについて説明
- 次の段階

(2) ECの法的枠組み（EC legal framework）

(3) 指令95/46/ECの適用範囲（Scope of Directive 95/46/EC）

(4) 諸原則（Principles）

(5) データ取扱いは合法でなければならない（Data processing must be legitimate）

(6) データ保護機関（Data Protection Authorities）
- 独立性の機関
- 国内法の執行権限

(7) 第29条作業部会（Article 29 Working Party）

(8) 十分性：一般的論点（Adequacy—general issues）

(9) 十分性：法的手順（Adequacy—legal steps）
- 前述

(10) 十分性（Adequacy）

---

16 堀部政男「グローバル社会と日本のプライバシー・個人情報保護―OECD情報セキュリティ・プライバシーWP副議長12年の経験」、NBL912号（2009年9月1日）参照。

（11）「十分な保護」の第三国（“Adequate”3rd countries）

（12）十分性：結論（Adequacy-conclusions）

これらのうち、ここでは日本との関係で注目すべきいくつかの点について見ることにする。

ペチャコバ女史は、プレゼンテーションの目的の中でデータ保護・プライバシーの分野における欧州委員会の作業についてばかりでなく、十分性認定手続とは何か、欧州委員会は日本との関係でどのようなところにあるかについても説明するとした。

また、十分性の法的手順について述べたところをEUデータ保護指令との関係で、簡単にコメントを加えて見ることにする。

欧州委員会が、第三国が十分なレベルの保護を確保しているかどうかを決定する権限を与えられていることを述べた。

これは、EUデータ保護指令第25条第6項を指している。繰り返しになるが、第25条第6項は、次のように規定している。

「委員会は、第31条第2項に規定する手続に基づいて、第三国が個人の私生活並びに基本的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。」

これは、欧州委員会の認定権限に関する規定である。第6項の前の同条第4項は、「構成国は、第31条第2項に規定する手続に基づいて委員会が、第三国が本条第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ないと認定した場合には、当該第三国への同一タイプのデータの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」とし、同条第5項は、「委員会は、適切な時期に、第4項に基づく認定によってもたらされる状況を改善することを目的とする交渉を開始しなければならない」と規定している。

欧州委員会関係者によると、これらの規定に基づき委員会が「十分性」評価を行い、その評価が得られない場合には、交渉に入るということであった[17]。しかし、必ずしもそうではないと話も聞いていた。

ペチャコバ女史が、公の会議で「十分性認定手続を開始するためには、第三国の代表による公式な要請が欧州委員会に提出されなければならない」と述べたことは、EUデータ保護指令の解釈の変更であるようにも受け取れる。

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

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

・このような決定の効果は、個人データが27のEU構成国及び3つの欧州経済領域（European Economic Area, EEA）（ノルウェー、リヒテンシュタイン及びアイスランド）からその第三国へ、

17 今回の調査でベルギーのナミュール（Namur）大学を訪れ、データ保護について海外調査なども行っている前掲注15 のcrids で意見交換をした。その席で、セシル・ドゥ・テェルワンニィ（Cécile de Terwangne）教授は「評価の開始には2つの方法がある。欧州委員会が調査を開始する場合と、第三国がドアを叩いてくる、すなわち、要請してくる場合である」と語っていた。前掲のオーストラリアは前者の場合であるかと質問すると、そのとおりであるとのことであり、欧州から見ると、オーストラリアはコモンウェルス（英連邦）の一員であり、近い存在であるとのことであった。

追加的な安全保護措置を必要としないで、流通することができることである。

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

・したがって、EU構成国から日本へのデータの移転は、EU構成国各国のデータ保護機関による事前の情報／権限付与（prior information/authorization）を意味する指令95/46/EC第26条に従って行われなければならない。

（EUデータ保護指令第26条は、前掲のとおりであるので、ここでは繰り返さないことにする。）

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

また、前述の「(12) 十分性：結論」として、女史は、次のようなことを明らかにした。

・委員会は、日本のやり方の評価を開始する予備的段階に入った。

・日本におけるデータ保護・プライバシー立法に関する分析を準備している。

・EU-日本ビジネス・ダイアログ・ラウンドテーブルは、2008年7月3日・4日、東京で「データ保護レジーム」について議論した。

・ビジネス・ダイアログ・ラウンドテーブルは、EUと日本の機関が両者の間で、国際的な平等、透明及びセキュアなデータ保護レジームを確保するために協働すべきであると勧告した。

・委員会は、ビジネス・ダイアログ・ラウンドテーブルのために経過報告を準備している。

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

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

・とはいえ、この構想も日本側によって支持されなければならない。

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

以上が「(12) 十分性：結論」部分である。

日本が今後どのように対応するか検討が必要である。

6　国際個人データ・プライバシー保護基準

（1）2009年マドリード会議の決議

これまでの叙述からも明らかなように、国際的水準は、主として国際的な機関において議論されてきた。そのような中で、国際機関ではない、データ保護・プライバシー・コミッショナー国際会議（International Conference of Data Protection and Privacy Commissioners）という会議体が国際的水準を策定したので、取り上げることにする[18]。それは、「国際個人データ・プライバシー保護基準」(International Standards on the Protection of Personal Data and Privacy）というものである。

（2）データ保護・プライバシー・コミッショナー国際会議とマドリード決議

「国際個人データ・プライバシー保護基準」は、「マドリード決議」（Madrid Resolution）とされている。さらに詳しくは、「データの取扱いに係るプライバシー保護に関する国際基準草案の共同提案」（Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data）となっている。これは、もう少し短縮して、「国際プライバシー基準」（International Standards of Privacy 又は International Privacy Standards）と呼ばれることがある。

この文書の最初で、スペイン・データ保護庁長官（DIRECTOR OF THE SPANISH DATA PROTECTION AGENCY）のアルテミ・ラロ・ロンバルテ（ARTEMI RALLO LOMBARTE）は、次のように述べている。

「データの取扱いに係るプライバシー保護に関する国際基準草案の共同提案を提示することは私にとって光栄である。この共同提案は、2009年11月5日にマドリードで開催されたデータ保護・プライバシー・コミッショナー国際会議において歓迎された。スペインデータ保護庁がコーディネーターを務め、50か国のプライバシー保護機関が共同して努力した結果、5つの大陸における立法を統合することにより、この権利の保護が許容する多くのアプローチを反映するようにしたテキストを作成することができた。この合意文書は、当該権利の基礎にある諸原則及び保障のユニバーサルな性格を強調することにより、また、情報の越境流通で特徴づけられるグローバル化した世界における個人の権利と自由のよりよい保護に貢献することにより、新たな価値を付加している。

今や、われわれ監督監視機関は、市民にそのプライバシーと個人データのよりよい保護を与えることに強くコミットすることから、その普及と促進という大きな仕事を引き受けることになる。」

この中に共同提案の趣旨が明確に出ている。

データ保護・プライバシー・コミッショナー国際会議の際には、その前日などに他のプライバシーやデータ保護関係の会議が開催されることが多い。2009年11月にもいくつかの会議が開かれた。その一つである市民的団体を中心とした会議において、マドリード・プライバシー宣言（Madrid Privacy Declaration）が11月3日に採択された。これは、プライバシーが世界人権宣言（Universal Declaration of Human Rights）などで提示された基本的人権（fundamental human right）であることを高らかに謳い、10項目にわたって、確認や要請を行っている。この宣言は、ここでは割愛する。

---

18 堀部政男「『国際プライバシー基準』（International Standards of Privacy）という新たな基準論議―2009年マドリード会議の決議」、日本データ通信172号（2010年3月）1頁以下、藤原静雄「『個人データの処理に係るプライバシー保護の国際標準草案のための共同提案』について」、消費者庁、前掲注1 報告書125頁以下など参照。

（3）国際プライバシー基準の構成

国際プライバシー基準は、6部25条からなっている。それぞれの部と各条の見出しを日本語訳すると、次のようになる。

第Ⅰ部：総則（Part I: General Provisions）

1　目的（Purpose）

2　定義（Definitions）

3　適用範囲（Scope of application）

4　追加的措置（Additional measures）

5　制限（Restrictions）

第Ⅱ部：基本原則（Part II: Basic Principles）

6　適法性及び公平性（Principle of lawfulness and fairness）

7　目的明確化の原則（Purpose specification principle）

8　均衡原則（Proportionality principle）

9　データ質原則（Data quality principle）

10　公開原則（Openness principle）

11　責任原則（Accountability principle）

第Ⅲ部：取扱いの適正性（Part III: Legitimacy of processing）

12　適正性の一般原則（General principle of legitimacy）

13　センシティブ・データ（Sensitive data）

14　データ取扱いサービスの提供（Provision of processing services）

15　国際移転（International transfers）

第Ⅳ部：データ主体の権利（Part IV: Rights of the Data Subject）

16　アクセス権（Right of access）

17　訂正・削除権（Rights to rectify and to delete）

18　異議申立権（Right to object）

19　これらの権利の行使（Exercise of these rights）

第Ⅴ部：セキュリティ（Part V: Security）

20　セキュリティ措置（Security measures）

21　守秘義務（Duty of confidentiality）

第Ⅵ部：コンプライアンス及び監視（Part VI: Compliance and Monitoring）

22　事前措置（Proactive measures）

23　監視（Monitoring）

24　協力及び協調（Cooperation and coordination）

25　責任（Liability）

（4）国際プライバシー基準と日本の個人情報保護法

国際プライバシー基準と日本の個人情報保護法を比較してみると、日本の法律の位置づけの一端が明らかになる。ここでは、前者にあって、後者にそれに該当するものがないか又は類似のものはあるが異なるものをいくつか指摘することにとどめることにする。

第1に、前者には、「13　センシティブ・データ」に関する規定があるのに対して、後者にはない。日本でも地方公共団体の条例では規定しているものもある。前者では、第1項で、抽象的に、「a. データ主体の最も機微な領域に影響するデータ、又はb. 悪用の場合にⅰ．違法な若しくは恣意的な差別、又はii．データ主体に対する重大な危険を引き起すおそれのあるデータ」を挙げて、第2 項で、EUデータ保護指令などで規定されているセンター・データに言及している。

第2に、前者には、「15　国際移転」に関する規定があるのに対して、後者にはない[19]。

第3に、前者には、「第Ⅳ部　データ主体の権利」に関する規定があるのに対して、後者には個人情報取扱事業者の「義務」という形の規定があるにすぎない（開示（第25条）、訂正等（第26条）、及び利用停止等（第27 条））が、「権利」という観点からは規定していない。前者は、「16　アクセス権」、「17　訂正・削除権」、「18　異議申立権」及び「19　これらの権利の行使」について規定している。前者で「権利」として構成しているのは諸外国の通常の規定の仕方の反映であろう。

第4に、前者の「23　監視」で規定している要件を備えた監視機関に相当するものは、後者にはないといわなければならない。後者では、事業所管大臣が監視の役割を担っている（第32条～第36条）のに対し、前者でいう監視機関（supervisory authorities）は公平で、かつ、独立していなければならないとされている。

第5に、前者には、「24　協力及び協調」の国際協力に関する規定があるのに対し、後者には、「国及び地方公共団体の協力」に関する規定（第14条）があるにすぎず、国際協力はない。

（5）国際的水準の継続的検討の重要性

日本国内でも、プライバシー・個人情報保護についてかなり議論されているが、グローバル化している現代社会においては、その議論の中で国際的水準との比較をすることが求められる。そのため、国際的水準について継続的に検討することは極めて重要である。

---

19 これについても論じたいことが多々あるが、とりあえず、堀部政男「クラウドコンピューティング社会の進展とプライバシー・個人情報保護の論点」、月報司法書士2010年2月号（日本司法書士会連合会）を参照されたい。

＜1-2＞　欧州委員会
EU データ保護改革と国際的水準への影響[1]

駿河台大学法学部准教授　宮下　紘

人は「忘れる」生き物である。人は「忘れる（forget）」ことを常とし、「覚える（remember）」ことを例外とする。しかし、現代の情報通信技術の進展に伴い、人の記憶から「忘れられる」ことがデジタルの世界では「覚えられている」。人は忘れても、デジタルの世界は忘れない。もはや「忘れる」ことが例外ではなくなったのである。そこで、「忘れられる権利（the right to be forgotten）」という新たな権利を掲げ、プライバシー・データ保護の権利が新たな世代を迎えることとなった[2]。

1　EU データ保護改革の概要

2012年1月25日正午（ベルギー時間）、欧州委員会副委員長兼司法総局コミッショナーのViviane Reding 氏が「データ保護改革（Data Protection Reform）」を公表した。17年前にEUデータ保護指令が採択された当時、インターネットを利用していたヨーロッパ市民は約1％にすぎなかったが、現在、欧州には2億5000万人のインターネット・ユーザーがおり、個人データの大量かつ瞬時にして容易に流通する環境において、強固で一貫性のある欧州の法的枠組みが必要となった。Reding氏はプレス・カンファレンス[3]の中で、オーストリアの学生がFacebook における自身の個人情報の削除を求めた例を挙げた。彼がオーストリアに在住であり、アイルランドに拠点があるFacebookに削除を求めるにはアイルランドのデータ保護機関に苦情の申立てをしなければならなかった。しかし、将来この学生は自国のオーストリアのデータ保護機関に申立てをすれば、オーストリアの機関からアイルランドの機関に照会・付託し、欧州域内のどこにおいても同一の規則が適用され、すなわち本人の個人データを消去する権利が担保されるべきであるとReding氏は指摘した。

1　本稿を執筆するにあたり、2012年1月25日～27日にブリュッセルで開催されたComputers, Privacy & Data Protection 会議への出席並びに関係者からのヒアリング、及び同年2月14日～17日にかけて堀部政男委員長とともに欧州委員会、ナミュール大学、ブリュッセル自由大学、ブリュッセル・リンクレターズ法律事務所においてそれぞれヒアリングを実施した。ヒアリングを快諾してくださった関係者及び欧州連合日本政府代表部の井上淳書記官、阪口理司書記官、田中信彦書記官にはこの場を借りて謝意を記す。また、第3回検討委員会における堀部政男委員長の説明資料「EUの新データ保護提案の概要」（2012年2月29日）を参考にさせていただいた。堀部委員長からは本稿の執筆にあたり大変貴重な御指摘を頂戴した。ここに記して堀部委員長の御厚意に感謝する。

2　“the right to be forgotten”については、*See* Jeffrey Rosen, *The Right to be Forgotten,* 64 Stan. L. Rev. *88 (2012);* Ivan Szekely, *The Right to Forget, the Right to be Forgotten*, in European Data Protection: In Good Health? 347 (Serge Gutwirth et. al. eds., 2012). なお、忘れられる権利それ自体は、フランスで発達した“droit à l'oubli”に由来する。*See* Alex Türk, La vie Privée en Peril: Des Citoyens Sous Contrôle 157-8 (2011). 1978年フランス情報と自由法が制定された当初、利用期間を制限する義務（obliger）であったが、実在する人がインターネット上の無形の人格（intangible identité）とも切り離されないための法規範が必要となった。邦語による紹介として、宮下紘「忘れられる権利－プライバシー権の未来」時の法令1906号（2012）43頁以下、参照。

3　Available at http://ec.europa.eu/avservices/video/player.cfm?ref=82655&sitelang=en

このような「単一のデジタル市場」を作り、データ保護がヨーロッパ市民の基本的権利であることを再確認しつつ、行政の負担軽減（年間約23億ユーロの負担軽減と想定）と共に消費者にも企業にも分かりやすいデータ保護の原則を示す重要性が示されたのである。

（1）EU データ保護指令の改正案

2012年1月25日、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」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」[4]が示された。すなわち、既存のEUデータ保護指令に代わり、新たに次の2つの枠組みが示され、欧州議会及び欧州理事会に提案された。

- 「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（Proposal for a Regulation on the Protection of Individuals with regards to the Processing of Personal Data and on the Free Movement of Such Data）」（以下（一般データ保護規則）提案という。）[5]
- 「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（Proposal for a Directive 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）（以下「刑事データ保護指令提案」という。）[6]

前者は、一般データ保護規則（General Data Protection Regulation）と呼ばれ、後者は、警察司法分野のみに適用される指令である。いずれの前文（recital）1項も個人データの保護が「すべての者は、自らに関する個人データの保護の権利を有する」と規定する欧州連合基本権憲章第8条1項[7]及び欧州

---

4 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).

5 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).

6 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).

7 The Charter of Fundamental Rights of the European Union Art. 8(1).

連合の機能に関する条約第16条1項[8]に基づき「基本的権利」であることを宣言することから始まっており、今回の新たな提案が人権保障のための法であることを明確にしている。既存のEUデータ保護指令は、一般データ保護規則提案へと全面改正されることとなる。なお、今回の欧州委員会の提案に基づき、欧州議会及び欧州理事会においてそれぞれ審議され、提案後から1年半～2年後を目途にEU一般データ保護規則提案及び刑事データ保護指令提案が採択される見込みとなっている[9]。

【ヒアリング結果】

・今後の過程としては、一般データ保護規則提案が17か国語に翻訳され、欧州議会や欧州理事会での審議がなされることとなっている。文書の性格からしても、審議・検討に時間を要し、2014年前に採択される見込みはないであろう。（リンクレターズ）

（2）EUデータ保護指令改正の背景

現行のEUデータ保護指令の目的と原則に関する限り良いと考えられるが、個人データ保護に関する執行が欧州連合の中でバラつきがあること、また法の曖昧な部分やオンライン活動に関するリスクがあるという市民の認識が存在している。そこで、①更に強力で一貫した欧州連合におけるデータ保護の枠組み構築、②デジタル・エコノミーが加盟国の産業促進となるような強力な執行による裏付け、③経済界と公的機関に対する法的及び実務上の確実性の補強という観点から、EUデータ保護の枠組みの改革の必要性が生じた[10]。

そして、今回の改革を提案するに当たり、各種の会議・ワークショップ等のほか、①「個人データの保護の基本的権利に向けた法的枠組みのコンサルテーション」[11]（2009年7月9日～同年12月31日、168通の意見を受理）と②「欧州連合における個人データ保護に関する欧州委員会の包括的アプローチのコンサルテーション」[12]（2010年11月4日～2011年1月15日、305通の意見を受理）を実施した。

---

8 The Treaty on the Functioning of the European Union Art.16 (1).

9 なお、現行のEUデータ保護指令は、1990年7月27日に提案がなされた後、1992年10月15日の改正提案が提出され、1995年10月24日に採択されている。

また、今回のEUデータ保護改革の提案は当初の予定では2011年内に公表される予定であったが（*See* Viviane Reding, *The Upcoming Data Protection Reform for the European Union*, 1 INT'L DATA PRIVACY L. 3, 5 (2011).）、意見集約に時間を要したと考えられる。2012年3月時点では、欧州議会の主要な4党を含む「非常に好意的な」反応が多く寄せられており、今回の提案は2013年夏までに合意に至ることを目標としている、とReding氏は指摘する。*See Five Minutes with Viviane Reding, Vice-President of European Commission*, Mar. 2, 2012. Available at http://eprints.lse.ac.uk/43044/1/blogs.lse.ac.uk-Five_minutes_with_Viviane_Reding_VicePresident_of_the_European_Commission_A_single_set_of_dataprotect.pdf

10 Proposed Regulation, *supra* note 5. at 2.

11 Consultation on the legal framework for the fundamental right to the protection of personal data. Available at http://ec.europa.eu/justice/newsroom/data-protection/opinion/090709_en.htm

12 Consultation on the Commission's comprehensive approach on personal data protection in the European Union. Available at http://ec.europa.eu/justice/newsroom/data-protection/opinion/101104_en.htm

②のコンサルテーションの過程において、多くの利害関係者から既存の原則が現状のままでよいものの、新たな技術（特にオンライン）及びグローバリゼーションの進展に伴う課題に更にうまく対処していくために既存の枠組みの適合化の必要性が指摘された。同時に、経済的利害関係者からは、法的確実性の強化やデータ保護の原則の調和に関する要求も提出された。

（3）EU一般データ保護規則提案の形式的変更

①「指令」から「規則」への法形式の変更

EUデータ保護「指令」からEUデータ保護「規則」という法形式が変更された。「指令（directive）」は加盟国を拘束するものの、形式及び手段に関する権限は加盟国の国内機関に委ねられているが、「規則（regulation）」は、その制定により自動的に各国の国内法制度の一部となり、国内立法を必要とせず直接適用される。

②「規則」の条文数の増加

EUデータ保護指令は前文（recital）42項目及び本文34条からなるのに対し、一般データ保護規則提案は前文解説139項目及び本文91条から構成されており、前文及び条文の数が増えている。

（4）EU一般データ保護規則提案の構成

第Ⅰ章　総則（第1条～第4条）
目的、適用対象、適用範囲、定義等を定めている。

第Ⅱ章　諸原則（第5条～第10条）
データ処理の原則、同意、児童の個人データ処理、特定分野の個人データ処理等の規定がある。

第Ⅲ章　データ主体の権利（第11条～第21条）
透明性、データへのアクセス、訂正及び消去、異議申立等のデータ主体の権利が列挙されている。

第Ⅳ章　データ管理者及びデータ処理者（第22条～第39条）
一般的な義務、データ・セキュリティ、データ保護影響評価、事前承認、行動規範及び認証について義務規定がある。

第Ⅴ章　個人データの第三国又は国際機関への移転（第40条～第45条）
個人データの移転の一般原則、十分性決定、十分性決定がない場合の移転、拘束的企業準則、国際協力等を定めている。

第Ⅵ章　独立監督機関（第46条～第54条）
独立した地位、義務と権限について規定している。

第Ⅶ章　協力及び一貫性（第55条～第72条）
監督機関の協力、一貫性ある法適用、欧州データ保護委員会に関する条文がある。

第Ⅷ章　救済、責任及び制裁（第73条～第79条）
苦情申立、司法救済、補償・責任、加盟国及び監督機関の罰則・制裁の義務を定める。

第IX章　特定のデータ取扱状況（第80条～第85条）
表現の自由との調整、医療目的の情報、雇用管理の情報及び歴史・統計・科学研究目的の情報の取扱い等について規定する。
第X章　委任立法及び実施法（第86条～第87条）
第XI章　終章（第88条～第91条）

（5）EU一般データ保護規則提案の特徴

①目的

「個人データの処理に係る個人の保護に関する規則及び個人データの自由な流通に関する規則」（第1条1項）を定め、「自然人の基本的権利及び自由、特にその個人データの保護の権利を保護する」（第1条2項）ことを目的としている。

現行のEUデータ保護指令とほぼ同様であるものの、現行の指令にある「プライバシーの権利」（第1条1項）という言葉が削除され、欧州連合基本権憲章及び欧州連合の機能に関する条約で示された「個人データの保護の権利」に統一されている。なお、EU一般データ保護規則提案には、第30条（プライバシー・バイ・デザイン）及び第32条（個人のデータ又はプライバシーの保護）において「プライバシー」という言葉が用いられている。

②適用範囲

（ⅰ）EUにおけるデータ管理者及びデータ処理者の設置による活動において個人データを処理する場合、（ⅱ）EU域外における管理者がEU在住のデータ主体の個人データを処理し、欧州連合におけるかかるデータ主体に対して商品若しくはサービスを提供する場合又はかかるデータ主体をモニタリングする場合、（ⅲ）EU域外における管理者が国際公法によって加盟国の国内法が適用される所で個人データを処理する場合にはEU一般データ保護規則提案が適用されることになる。（第3条1項～3項）

この規定は、自動処理の方法及びファイリングシステムによる個人データの処理に適用されると定めている現行のEUデータ保護指令（第3条1項）から大きく改正された。特に（ⅱ）の域外適用については、たとえばデータ管理を日本で行っている事業者に対してもEU在住のデータ主体に対して商品若しくはサービスを提供する場合又はかかるデータ主体の活動をモニタリングする場合には適用可能性があることを示唆している点は注意を要する。前文21項において、「活動をモニタリングする」こととは、データ主体に関する決定を下し、又は個人の選好、行動及び態度を分析若しくは予測する目的で個人を「プロファイル」するデータ処理技術を用いてインターネット上で個人を追跡することを指していると解説されている[13]。

---

13 なお、EU域外の情報通信を取り扱う事業者に対しては、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unique indentifer（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と解されている。*See* 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*, (WP 56, adopted on 30 May 2002). また、このことは欧州委員会司法総局データ保護課長（2012年3月現在）がかつて執筆した共著論文において示されていた。*See* 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).

なお、第29条作業部会の意見において、現行のEUデータ保護指令の下でも、EU域内で技術のメインテナンスを行っている場合や支店を置いている場合の日本のインターネット・サービス提供者に対するEUデータ保護指令の適用の可能性の例が出されている[14]。

③本人の権利

（ｉ）本人の同意について

本人の同意に関する新たな条文が設けられた（第７条)。管理者がデータ主体の同意があったことを立証する責任を負うほか（第７条１項)、データ主体は自らの同意を撤回することができる（第７条３項)。すなわち、個人が真正かつ自由な選択をできず、また事後的に同意を撤回することができない場合は、同意が法的に有効であったとはみなされないのである（前文33 項)。

なお、同意については、自らの希望を特定して表明できる「曖昧なものであってはならない(unambiguous)」ことが第29 条作業部会の意見において示されている[15]。

（ii）忘れられる権利

EUデータ保護指令で定められていたデータの修正、消去、ブロック（第12条）とは別に、「忘れられる権利（the right to be forgotten)」が新たに設けられた（第17条)。欧州委員会の調査（2010 年11月～ 12月実施）によれば、75％のEU市民が何時であっても自らのデータを消去できることを希望している[16]。（ｉ）データの利用目的が必要でなくなったとき、（ii）データ主体が同意を撤回し、同意されたデータ保有期間が経過し、若しくはデータ処理の法的根拠がないとき、（iii）データ主体が個人データの処理に異議申立を行ったとき、又は（iv）その他の理由によりデータ処理が一般データ保護規則提案に違反したときには、データ主体が管理者から個人データを消去する権利及びかかるデータの更なる流通を回避する権利を有している（第17条１項)。そして、管理者が個人データを公表している場合、管理者がその公表に責任を負っているデータに関して、データ主体が当該個人データへのリンク、又はその複製若しくは複写を消去するよう要請していることを当該データを処理する第三者に対して通知するために技術的措置を含むあらゆる合理的な措置を講じなければならない(第17条２項)。なお、表現の自由、公共の利益、歴史・統計・科学の研究目的等の理由を除いて、管理者は遅滞なく個人データを消去しなければならない（第17条3項)。

なお、忘れられる権利については、実効性に疑問が残るとされているが、2012年3月スペインの裁判所から欧州司法裁判所に検索サイトにおける個人データの消去に関する事案の意見照会が行われ、その判断が待たれるところである[17]。

---

14 Article 29 Data Protection Working Party, *Opinion 8/2010 on applicable law*, (WP179, adopted on 16 Dec. 2010) at 16-7.

15 *See* Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent* (WP187, adopted on 13 July 2011).

16 European Commission, *Special Eurobarometer 359: Attitude on Data Protection and Electronic Identity in the European Union* (June 2011) at 158. 消去を希望しないと回答したEU市民は4％にすぎない。

17 ECJ, Case C-131/12.

（iii）データ・ポータビリティの権利

データ主体は、電子的な方法で個人データが処理されている場合は、管理者に対してデータの複写を得る権利を有する（第18条1項）。

④事業者の義務

（ｉ）プライバシー・バイ・デザイン（privacy by design）[18]、データ保護バイ・デフォルト（data protection by default）

管理者は、データ主体の権利の保護を履行するために技術的かつ組織的措置を講じなければならない（第23条1項）。同時に、管理者は、初期設定で（by fault）利用目的に必要な限りで個人データが処理され、また目的に必要な必要最小限の範囲で収集又は保有される体制を実施しなければならない（第23条2項）。さらに、管理者及び処理者が個人データの処理に際して適切なセキュリティ水準を維持できるよう、欧州委員会はプライバシー・バイ・デザイン（データ保護バイ・デザイン（第23条3 項））及びデータ保護バイ・デフォルトに向けた技術及び解決策の進展を考慮しつつ、技術的及び組織的措置の基準及び条件を具体化していくこととなっている（第30条3 項）。

（ii）データ保護責任者（data protection officer）及び代理人（representative）

EU域外のデータ管理者で第3条2項（EU域内のデータ主体に対して商品若しくはサービスを提供する場合又は活動をモニタリングする場合）に該当する管理者はEU域内に代理人を配置しなければならない（第25条1項）。ただし、（ｉ）十分な保護措置を確保していると認められている国における管理者、（ii）250人以下の従業員の企業、（iii）公的機関、又は（iv）EU在住のデータ主体に対してごく稀に商品ないしサービスを提供するにすぎない管理者はこの限りではない（第25条2項）。また、管理者及び処理者が、（ｉ）公的機関によって処理が行われる場合、（ii）250人以上の従業員によってデータが処理される場合、又は（iii）管理者若しくは処理者の中心的活動がデータ主体を規則的かつ体系的にモニタリングを必要とする処理運用からなる場合、データ保護責任者を配置しなければならない（第35条1項）。また、管理者又は処理者はデータ保護法の専門知識を有する専門的資質に基づきデータ保護責任者を任命することとし、その任期は少なくとも2年としなければならない（第35条5項・7項）。

（iii）データ保護違反の通知義務（data breach notification）

個人データの侵害の事案においては、管理者は遅滞なく、かつその事案を知り得たときから24時間以内に監督機関に対して当該個人データ侵害を通知しなければならない。24時間以内に通知がされない場合は、合理的な正当化事由をもって監督機関に対して通知をしなければならない（第31条1項）。ここにいう、「侵害」とは、個人データ又はプライバシーに不利な影響を及ぼすことを指し、具体的に

18「プライバシー・バイ・デザイン」はカナダ・オンタリオ州コミッショナーであるアン・カブキアン博士によって提唱され、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において「プライバシー・バイ・デザインに関する決議」が採択された。この点については、堀部政男「プライバシー・バイ・デザイン」ビジネス・ロー・ジャーナル（2011）参照。

はID盗難・詐欺、物理的被害、名誉に対する重大な屈辱又は損害を言う（前文67項）。通知の内容については、少なくとも（ｉ）データ主体の類型や数等を含む個人データ侵害の性質、（ii）データ保護責任者の連絡先、（iii）個人データの侵害を和らげるための措置、（iv）個人データ侵害の結果、（ｖ）管理者が講じた措置を参照することとされている（第31条3項）。

なお、データ保護違反の通知義務は、2012年3月時点でアメリカの40州以上において各州の制定法が整備されている[19]。

（iv）認証（certification）

EU加盟国及び欧州委員会は、データ保護の認証及びデータ保護のシールならびにマークの仕組みを確立することとなっている（第39条1項）[20]。

【ヒアリング結果】

- 今回の一般データ保護規則提案では説明責任の原則が強化され、これはAPECにおける取組から教訓を得ているものと考えられる。日本にはプライバシーマークがあるのであれば、十分性審査の際に欧州委員会に対してもその点を強調していくとよいであろう。欧州委員会は、現状で知識はないものの、認証制度に興味があり、日本の認証制度はひとつの参考となりうる。（ブリュッセル自由大学）
- 認証については、自主規制の枠組みを好むアメリカの主張と整合的であり、セーフ・ハーバーの延長上にあると考えることができる。（リンクレターズ）

⑤データ移転

（ｉ）十分性審査

２．において記述。

なお、十分性の決定がない場合、①拘束的企業準則、②欧州委員会が採択した標準データ保護条項、③管理者ないし処理者とデータ受領者との契約、又は④標準契約条項、若しくはその他の適当かつ比例した方法によってデータの移転を行うことが認められる（前文83項、第42条第2項）。

---

19 *See generally* JOHN P. HUTCHINS ET.AL., US. DATA BREACH NOTIFICATION LAW: STATE BY STATE (2007).

20 欧州レベルにおける認証制度のいち早い取組として、ドイツにおけるシュレスヴィッヒ・ホルシュタイン州のマーク制度がある。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、参照。

（ii）拘束的企業準則（binding corporate rules）

拘束的企業準則とは、主に多国籍企業を対象として、データの取扱い・移転に関して法的に執行可能な拘束力を有した企業ルールをEU加盟国の各データ保護監督機関による審査を経て承認された場合に、当該企業のデータ移転が認められる制度である[21]。十分性審査の例外規定である現行のEUデータ保護指令第26条2項に基づき十分な安全保護措置を施しているものとして運用面において認められてきた。2012年3月2日現在、15社が各データ保護監督機関から拘束的企業準則の承認を受けている（イギリス8社、フランス6社、ルクセンブルク1社）[22]。しかし、EU一般データ保護規則提案においては、第43条において明示的に認められることとなった。

【ヒアリング結果】

・ データ移転についてはBCRが明文化されたため、今後促進されることになるであろう。（リンクレターズ）

⑥監督機関（supervisory authority）

監督機関は、付与された義務及び権限を行使するに際し、完全に独立してこれを行うこととされている（第47条1項）。その義務としては、（i）一般データ保護規則提案の適用の監視、（ii）データ主体からの苦情受付、（iii）他の監督機関との情報共有、（iv）調査、（v）個人データ保護への影響の監視、（vi）EU 加盟国の諸機関からの相談受付、（vii）一定のデータ処理の事前認証、（viii）行動規範草案への意見提出、（ix）拘束的企業準則の承認、（x）欧州データ保護委員会の活動への参加が掲げられている（第52 条1項）。また、その権限としては、（i）管理者又は処理者に対する違反通知、（ii）管理者又は処理者に対する一般データ保護規則提案遵守の命令、（iii）管理者又は処理者に対する情報提供の命令、（iv）一定のデータ処理の事前認証、（v）管理者又は処理者に対する警告又は忠告、（vi）訂正・消去又はデータ破壊の命令、（vii）処理の一時的又は終局的な禁止命令、（viii）第三国等へのデータ移転の中止、（ix）個人データ保護に関する意見の提出、（x）個人データ保護に関する国の議会等への通知が含まれている。

---

21 *See* Article 29 Working Party, *Working Document on Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers* (WP74, adopted on June 3, 2003).
また、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報告書」（2010年3月）58 頁以下、参照。

22 *See* European Commission, *List of companies for which the EU BCR cooperation procedure is closed* (Mar. 2, 2012).
http://ec.europa.eu/justice/policies/privacy/binding_rules/bcr_cooperation_en.htm

なお、EU一般データ保護規則提案が公表される直前の2012年1月17日、ハンガリーの憲法改正に伴うデータ保護機関のコミッショナーの任期途中の地位の喪失について、データ保護機関の独立性の要件を満たしていないおそれがあるとして、欧州委員会がハンガリー政府に対し調査手続を開始した[23]。

【ヒアリング結果】

・ ヨーロッパでは独立性のある機関の重要性を誇張しすぎているが、今回の一般データ保護規則提案にもあるように「効果的な救済（effective remedy）」が担保されているかどうかが重要である。さらに、透明性のある機関であるかどうか、そして政策決定に対する一定の影響力を有しているかどうか、機関のスタッフの数や任命過程といった要素がヨーロッパの主張する独立機関の判断基準となりうる。（ブリュッセル自由大学）

⑦罰則

いかなる監督機関も行政罰を課す権限を有している（第79条1項）。罰則の金額については、違反の類型に応じて、（ｉ）250,000ユーロ又は全世界の1年の企業売上の0.5％以下（第79条4項）、（ii）500,000ユーロ又は全世界の1年の企業売上の1％以下（第79条5項）、（iii）1,000,000 ユーロ又は全世界の1 年の企業売上の2％以下（第79 条6 項）と3 段階の定めがある。

---

23 *See* European Commission, press release: *European Commission launches accelerated infringement proceedings against Hungary over the independence of its central bank and data protection authorities as well as over measures affecting the judiciary* (Jan. 17, 2012). また、データ保護監督機関の運用実態等については、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」（2011年3月）、参照。

2　EU データ保護指令及び一般データ保護規則提案における「十分性」審査について

（1）十分性審査の対象

EUにおいては、すでに1980年代から「国境を越えるデータ流通の問題に対する十分な応答（adequate responses）を見出す必要性の認識が高まっていた」[24]。そして、「個人データの越境流通が関連するデータ主体のプライバシーの十分な保護を保障できてない」[25]ことが指摘され、EUデータ保護指令はEU加盟27か国及び欧州経済領域におけるデータ管理者の個人データの移転を制限する「十分な保護の水準（adequate level of protection）」という要件を設けるに至った。

EUデータ保護指令第25条及び一般データ保護規則提案41条に基づく個人データの第三国への移転については、しばしばその対象が問題となる。特にインターネットのように開かれたネットワークでは、特定の個人データをインターネット上にアップロードした時点で第三国のユーザーがそれを閲覧できれば個人データの第三国移転に該当してしまう可能性がある[26]。そこで、欧州司法裁判所は2003年11月6日の判決において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」[27]という判断を下している。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[28]。したがって、同判決は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。近年では、クラウド・コンピューティングについては、そもそもどこでデータが処理・蓄積されているか、という複雑な問題を提起するが、クラウド・サービスのユーザーや場合によってはサービス提供者を含めデータ管理者がEU域内で設置されている場合、EUデータ保護指令が適用されることとなる[29]。したがって、クラウド・コンピューティング・サービス提供者との契約を締結していないEU 域外の国・地域については、十分性の評価がケース・バイ・ケースになるとしても、十分な保護水準を確保していない第三国へのデータ移転はクラウド・コンピュ

---

24 Cees J. Hamelink, Transnational Data Flows in the Information Age 94 (1984).

25 A.C.M. Nugter, Transborder Flow of Personal Data within Ec 294 (1991). この当時は、越境データ移転の枠組みが人権保障というよりはむしろ商取引の帰結であったと指摘される。*Id.* at 295.

26 EUデータ保護指令第25条のデータ移転に伴う問題点として、当初から指摘されていた。

See Cécile de Terwangne & Sophie Louveaux, *Data Protection and Online Networks*, 13 Computer L. & Security Rev. 234, 244 (1997).

27 Judgment of the Court of 6 November 2003 in Case C-101/01: *Bodil Lindqvist*.

28 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).

29 Article 29 Data Protection Working Party, *Opinion 8/2010 on applicable law*, (WP179,adopted on 16 Dec. 2010) at 21-2.

ーティング・サービスについても禁止されることになると解されている[30]。

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[31]。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。

さらに、データの移転に際しては、標準契約条項等を除き、EUデータ保護指令第26条が例外を明文で認めているとおり、①データ主体が移転について同意を与えている場合（第26条1項(a)）、②移転が契約履行又は契約締結前の措置に必要である場合（第26条1項(b)）、③データ主体のために、データ主体及び第三者との間の契約締結・履行に必要な場合（第26条1項(c)）、④重要な公共の利益を理由とした法的請求に基づく場合（第26条(d)）、⑤データ主体の重大な利益を保護するために必要な場合（第26条(e)）、⑥法令に基づき閲覧目的で公開されている情報を移転する場合（第26条(f)）については、十分性の要件を必要としない。なお、EU一般データ保護規則提案第44 条1 項は若干の変更（重要な変更点として、データ主体の同意に基づく移転については十分性認定がないことに伴うリスクを通知することが追記された（第44条1項(a)））があるが同様の規定を置き、同条1項 (h) には移転の頻度が低く、小規模なものに限り、適切な安全管理措置を施し、正当な利益のための必要な場合、という条項が追加された。

（2）十分性審査の手続

欧州委員会からの十分性の決定が下されるまでの手続は明文の定めがあるわけではない。

これまでの例からすると、①欧州委員会による事前調査、②第29条作業部会による意見、③第31条作業部会による審議、④欧州委員会による決定という流れになっている。欧州委員会の調査報告書では、「『十分性』認定の過程は長期間で、遠回りである（long and tortuous）」であるとも指摘されており[32]、第29条作業部会の意見が公表されるまでに審査には通常1年半から2年を要し、その後、欧州委員会の決定への手続に進む。

---

30 *See* Yves Poullet, Jean-Marc Van Gyseghem, Jean-Philippe Moiny & Jacques Gérard, Claire Gayrel, *Data Protection in the Clouds* in COMPUTERS, PRIVACY, AND DATA PROTECTION: AN ELEMENT OF CHOICE 399 (Serge Gutwirth et al., 2011). また、クラウド・コンピューティングEUデータ保護指令を含む国際動向については、新保史生「諸外国の機関とEUの動向」岡村久道編『クラウド・コンピューティングの法律』（民事法研究会・2012）399 頁以下、参照。

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

32 *See* European Commission, *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the light of Technological Developments, Working Paper 2: Data Protection Laws in the EU* (by Douwe Kroff) (20 Jan. 2010) at 66.

法制度の詳細な調査は、①の欧州委員会による事前調査であり、その多くがベルギーのナミュール大学（Université de Namur, Facultés universitaires Notre-Dame de la Paix）の法・情報・社会研究所（Centre de Recherche Information, Droit et Société）に委託されて行われている。同研究所には欧州を代表するプライバシー・データ保護関係の教授及び研究員（2012年3月時点で47名）がおり、欧州委員会のデータ保護の諸施策のみならず、欧州評議会条約第108号の改正案にも様々な提言を行ってきている。そして、日本の法制度の十分性に係る第1次審査（非公表）を行ってきたのもナミュール大学である[33]。

この事前調査をもとに、第29条作業部会（working party）における審議（近年は1年に5回開催、議長はオランダデータ保護機関のJacob Kohnstamm）を経て、意見が公表される。同作業部会は、データ保護の監督機関又は各加盟国が指名した機関の代表者等によって構成され（EUデータ保護指令第29条2項）、第三国における保護の水準に関する意見を欧州委員会に提出することがその権限として認められている（EUデータ保護指令第30条第1項(b)）。データ保護に関する専門的知見を有する第29条作業部会の意見が、実質的に欧州委員会の最終的な決定に影響を及ぼすものと考えられている。実際、第29条作業部会はEUデータ保護指令が発効される直前の1998年7月24日「第三国への個人データの移転：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部会文書」（以下、「WP12」という。）[34]を公表し、十分性審査について次の要件を示している。すなわち、第1に内容原則であり、①利用目的の制限に関する原則、②データの内容に関する原則及び比例原則、③透明性の原則、④セキュリティに関する原則、⑤アクセス・訂正・異議申立の権利、⑥海外移転に関する制限が示されている。補足的な原則として、①センシティブ・データ、②ダイレクト・マーケティング、③自動的な個人決定が掲げられている。そして、第2に、手続・実体の構造として、①法令遵守の優れた水準、②個々のデータ主体に対する支援と援助、③適切な救済が十分性審査の要素とされている。このWP12に基づく第29条作業部会の意見が出され、その上で、EUデータ保護指令第31条に基づく委員会（committee）に対して欧州委員会の草案に対する意見を聴いたうえで、最終的な決定が下されることとなっている(EUデータ保護指令第31条2項)。

しかし、上記のような手続がEUデータ保護指令にも一般データ保護規則提案にも示されていないため、どのような手続を経て十分性審査が認定されるかについては依然として不透明な部分がある。この点、欧州委員会の十分性の決定がない場合、イギリスの情報コミッショナー・オフィスは「データ管理者自身が評価することができる」[35]ことを示しており、またオランダデータ保護機関は「データ管

33 Cécile de Terwangne, Florence de Villenfagne, Franck Dumortier, Virginie Fossoul, Yves Poullet, Masao Horibe, *First analysis of the personal data protection law in Japan in order to determinate whether a second step has to be undertaken* (unpublished, 2006).

34 Article 29 Data Protection Working Party, *Working Document: Transfers of personal data to third countries: Applying Article 25 and 26 of the EU data protection directive* (WP12, adopted on 24 July 1998).

35 Information Commissioner's Office, *Sending Personal Data outside the European Economic Area (Principle8)*. Available at http://www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_8.aspx

理者は[オランダの]法務大臣の許可を経ることに基づき十分な保護措置を提示する措置を講じている」[36]とも指摘している。このようにEUデータ保護指令第25条の十分性に基づくデータ移転については、「加盟国間における指令の実施状況は様々であり、国際データ移転に対する国内の法的アプローチはかなり異なる結果となっている」[37]ことが報告されている。このようなことから、「現状の十分性の基準は明らかに不十分である」[38]と言われてきた。そこで、十分性手続に要する財政上及び人的資源の増強、十分性手続に関する第三国との対話の促進、ベスト・プラクティスを共有し手続の一元化、部分的・分野別の十分性審査の利用が提案されてきた[39]。さらに、このような硬直的な十分性審査に代わって、2007年以降APECにおいて越境プライバシー・ルールにおいて議論されてきた、個々の組織を認定する仕組みの「説明責任（accountability）」プロジェクトが拘束的企業準則との相互運用性（interoperability）を視野に入れつつ注目されつつある[40]。もっとも、「説明責任」の原則それ自体はOECDプライバシー・ガイドラインの基本原則にも含まれているとおり、それ自体はひとつの重要な原則であり、ただちに十分性認定と同一視しうるような性格のものと理解すべきではないと考えられる[41]。

さらに、個人データの移転の問題はこれまで世界貿易機関（World Trade Organization）の枠組みでは検討されてこなかった。しかし、WTOが人権問題を取り上げることのできる機関であるかどうかという疑義が付きまとうこととなるが、十分性認定に伴うデータ移転が制限されることになれば「遅かれ早かれWTOにおいてこの問題が直面することは真実であろう」[42]とも考えられている。もっとも、一例をあげるならば、日本が2011年に署名した模倣品・海賊版拡散防止条約のEUとの交渉において、このような貿易協定であっても、それが「個人の基本的権利、特にプライバシー及びデータ「保護の

---

36 Dutch Data Protection Authority, *Policy Paper on Transfers of Personal Data to Third Countries in the Framework of the Dutch Data Protection Act (WBP)*, Feb. 2003.

37 Christopher Kuner, OECD Digital Economy Papers No187, *Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present, and Future* (8 Dec., 2011) at 20.

38 Christopher Kuner, *Developing an Adequate Legal Framework for International Data Transfers*, in Reinventing Data Protection? (Serge Gutwirth et. al. eds., 2009) at 272.

39 *Id*. at 268.

40 この点、日本はAPEC越境プライバシー執行のための協力取決めの実施に参画することが2011年11月に15省庁が正式に承認された。なお、この承認前の第6回個人情報保護関係省庁連絡会議資料（http://www.caa.go.jp/seikatsu/kojin/renraku.html）を参照）。

41 *See* Colin Bennett, *International Privacy Standards: Can Accountability be Adequate?*, 16 Privacy Laws & Business 13, 14 (2010).

42 María Veroníca Pérez Asinari & Yves Poullet, Privacy, *Personal Data Protection and the Safe Harbour Decision: From Euphoria to Policy, From Policy to Regulation?,* in In the Future of Transatlantic Economic Relations 132 (David M. Andrews & Robert Schuman Centre eds., 2005). *See also Yves Poullet, Transborder Data Flow and Extraterritoriality: The European Position,* 2 J. Int'l Commercial L. & Technology 141 (2007). WTOがプライバシー紛争の権威ある解決策となりうる旨のアメリカ側からの主張として、*See* Peter P. Swire & Robert E. Laitan, None of Your Business: World Data Flows, Electronic Commerce, And the European Privacy Directive 194 (1998).

権利」に関連するものである以上、EU データ保護の水準を確保すべき必要性が指摘されている点に注意を要する[43]。

なお、上記の十分性審査の手続のほかに、欧州委員会は各国の法制度の調査及びデータ移転に関するワークショップ[44]等の開催を行ってきている。

【ヒアリング結果】

- 十分性審査のプロセスは、①事前調査を行い、②第29条作業部会による意見、③第31条委員会に基づき欧州委員会の決定という長期間のプロセスである。通常2年程度の時間を要する。（欧州委員会）
- 欧州委員会が十分性審査をする場合には、①当該国からの申請があった場合と、②EU にとって重要であるとの認識から十分性審査を始める場合がある。（ナミュール大学）

（3）十分性審査の意義

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[45]、カナダ[46]、アルゼンチ

---

43 *See* European Data Protection Supervisor, *Opinion on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA)* (2010/C 147/01). Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:147:0001:0013:EN:PDF.

44 2008年10月21日、欧州委員会主催の"Workshop on International Transfers of Personal Data"（ベルギー・ブリュッセル）において、EU加盟国以外に、日本のほか、カナダ、イスラエル、メキシコ、アメリカにおけるデータの移転状況に関するセッション（Regional Approaches to Data Protection and Transfers of Personal Data at International Level）が設けられ、筆者はこのセッションのモデレーターを引き受けた。

45 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).

46 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).

ン[47]、ガンジー島[48]、マン島[49]、ジャージ島[50]、フェロー諸島[51]、アンドラ[52]、イスラエル[53]の9 の国・地域がホワイト・リストに掲載されている（2012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」[54]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、セクトラル方式で法整備を進めるアメリカにおいては、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・ハーバー原則（Safe Harbour Principles）」に基づく協定を締結した[55]。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[56]。アメリカ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[57]。

---

47 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.*

48 European Commission, *Commission Decision of 21 November 2003 on the adequate protection of personal data in Guernsey* (2003/821/EC).

49 European Commission, *Commission Decision 2004/411/EC of 28.4.2004 on the adequate protection of personal data in the Isle of Man.*

50 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).

51 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).

52 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).

53 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).

54 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.

55 *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).

56 *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).

57 *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。

また、欧州委員会からの十分性が認定されても、それはあくまで「条件付き」であり、また「暫定的」であることに留意が必要である[58]。これまでの十分性認定の決定には、各国・地域の決定には次の点が付記されている。第1に、十分性が認定された国へのデータの移転については、現行EUデータ保護指令第25条以外の規定に従って採用された加盟国内の規定の履行を保証するための措置を講じることができ、また当該第三国へのデータ移転を中止する権限を行使しうる。第2に、欧州委員会は当該決定の運用を監視するとともに現行EUデータ保護指令に基づく第31条委員会に対して関係事実を報告することとなっている。また、十分性を認定された国・地域の法改正に伴い欧州委員会の十分性認定の決定を修正しうることなどが記されることがある。

さらに、第29条作業部会の意見では、十分性の「肯定的な認定については、包括的な（horizontal）データ保護法を有する国に限定されず、当該国の特定の分野についても及ぶ」[59]とされている。実際、カナダについては、欧州委員会の決定において公的部門を規律するプライバシー法（Privacy Act）に関する言及がされているにもかかわらず、民間部門を規律する個人情報及び電子文書法（Personal Information Protection and Electronic Documents Act）についてのみ十分性が認定されている[60]。

EUデータ保護指令が発効された17年間でこれまで9つの国と地域のみが十分性認定を受けたにすぎず、欧州委員会の2010年1月に公表された報告書では「その手続が望まれていたよりも小さなインパクトしかなかった。そのため、EU及び欧州経済領域以外の国における強力なデータ保護法の進展が結果として実際よりも強力に推進されてこなかった」[61]と指摘されている。他方で、同報告書では、アメリカとのセーフ・ハーバーがヨーロッパからの「信頼性（credibility）」を獲得できなかった点に言及し、「特にアジア太平洋の国々において、各国の法がヨーロッパの十分性の水準を確保すべきであるという命題は、それが貿易において恩恵的な効果をもたらすと感じられてきている点において当初から重要であった」[62]ことも記されており、近時、欧州委員会が日本を含むアジア太平洋地域における国々を十分性審査の戦略的地域として捉えていることがうかがえる。いずれにせよ、十分性審査は、「ヨーロッパ帝国主義（impérialisme européen）」の名の下にEUのデータ保護の価値観を他国に押し付けるのではなく、諸事情を考慮に入れケース・バイ・ケースの判断に基づくプラグマティックな手法で行われてきている[63]。

---

58 Douwe Korff, Data Protection Laws in the European Union 186 (2005).

59 *See* Article 29 Data Protection Working Party, *Working Document: Transfers of personal data to third countries: Applying Article 25 and 26 of the EU data protectiondirective* (WP165, adopted on 1 Dec. 2009) at 27.

60 *See* 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) Art.1.

61 European Commission, *Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the light of Technological Developments, Final Report* (20 Jan. 2010) at 16.

62 *Id.* at 42.

63 Yves Poullet, *Comment appliquer les règles de protection des données aux transferts de données personnelles dans une société à la fois globale mais également multi-économique et multiculturelle?*, 12 Lex Electronica 9 (2007).

【ヒアリング結果】

・欧州委員会は近年十分性審査を地理的に拡大している。また、EUとの取引等の経済的影響を考慮しながら十分性審査を進めてきている。（ナミュール大学）

・十分性審査は、外交・政治問題である。総論としては、各国の制度に大きな違いはないが、個別の論点でヨーロッパとそれ以外の国ではいくつかの緊張関係がある。（ブリュッセル自由大学）

（4）EU一般データ保護規則提案第41条

EUデータ保護指令において、個人データの第三国への移転は、原則として「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」（第25条1項）と定められている。この規定はEU一般データ保護規則提案において改正されたものの、十分性審査の枠組みそれ自体に大きな変更点はない（新旧条文比較表は103頁～104頁を参照）。

EU一般データ保護規則提案第41条には、「欧州委員会が、第三国、当該第三国における領土若しくは処理される分野、又は問題とされている国際機関が十分な保護措置を確保している場合に移転は行うことができる」という規定が置かれている。また前文78項では「第三国への移転は本規則の完全な履行の下に行われることができる」ことが明らかにされている。

現行の指令と一般データ保護規則提案は、基本的な枠組みは同一であるものの次の点で異なっている。

① 個人データの移転が第三国のみならず、第三国における領土、処理される分野、国際機関が明記されることとなった。

② EU 域内からデータを受領した国から別の国の転送についても一般データ保護規則提案を履行することが求められる。

③ 十分性の決定は欧州委員会が行うことが明記された。

④ 十分性を評価するにあたっての基準が詳細なものになった。

以上の変更点の中でも、④の十分性を評価するにあたっての3要素は重要である。（ⅰ）公共の安全、防衛、国土の安全及び刑事法を含む有効な関連立法である一般的及び分野別の法規範、（ⅱ）当該国又は当該国際機関によって履行される専門的な規則並びに安全措置、及び（ⅲ）データ本人に対する効果的な行政法上ならびに司法上の救済を含む効果的かつ執行可能な権利という要素が掲げられている。いずれもEUデータ保護指令には列挙されていなかった項目であり、十分性を申請する国等がこれらの要素を立証する責任が求められることとなる。

第2に、第三国ないし国際機関における一つ又は複数の「独立した監督機関の存在及び効果的な機能」の存在が挙げられている。独立性については、EU一般データ保護規則提案においても「いかなる者からも指示を求められたり受けたりしない」「完全な独立性（complete independence）」（第47条1項・2項）が要求されるものと考えられる。また、これらの機関は、「データ本人の権利行使のため本人を支援し、助言し、かつ欧州連合並びに加盟国の監督機関との協力する目的でデータ保護規則の履行を確保する責任を負う」こととされている。すなわち、監督機関は、第29条作業部会WP12が示し

た「法令遵守の優れた水準、個々のデータ主体に対する支援と援助、そして適切な救済」[64]の要件と共に、EU加盟国の監督機関との協力を行うことが求められている。

第3に、「国際的な責任（the international commitments）」が十分性審査の要素となった。ここにいう「国際的な責任」とは、一般的に拘束力のある国際的な文書を指していると解されている。そのため、最も歴史が古く拘束力ある国際的な文書である「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）」（いわゆる、欧州評議会条約第108号）の重要性が増すと予想されている[65]。第29条作業部会WP12においても、「欧州評議会条約第108号を採択した国がEU指令第25条の意味における十分な保護水準を与えているとみなしうることは単なる学問的興味以上のものである」[66]と述べられている。実際、アンドラが十分性を認定された際、第29条作業部会の意見において欧州評議会条約第108号へ締結されたことが個々の内容原則の観点から好意的に評価されている[67]。同時に、データ保護の分野で大きな影響力を有するデータ保護プライバシー・コミッショナー国際会議における決議への参画もまた重要な「国際的なコミットメント」であると考えられる[68]。日本がこれまで法制度の基盤として参照してきた「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OECD理事会勧告（Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data）」（1980年9月23日採択）、日本が加盟エコノミーとして

---

64 *See* Article 29 Data Protection Working Party, *Working Document: Transfers of personal data to third countries: Applying Article 25 and 26 of the EU data protection directive* (WP12, adopted on 24 July 1998) at 7.

65 *See* Christopher Kuner, *The European Commission's Proposed Data Protection Regulation*, PRIVACY AND SECURITY LAW REPORT, Feb. 6, 2012 at 9.

66 *See* Article 29 Data Protection Working Party, *Working Document: Transfers of personal data to third countries: Applying Article 25 and 26 of the EU data protection directive* (WP12, adopted on 24 July 1998) at 8. もっとも、欧州評議会条約第108号それ自体が改正作業の段階にあり、改正案（2012年3月5日時点）第12条にはデータ移転に関して「十分な保護水準」という要件が入っていることには注意を要する。*See* The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *Modernisation of Convention 108: New Proposals* (Mar. 5, 2012). Available at http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD-BUR_2012_01Rev_en.pdf

67 *See* Article 29 Data Protection Working Party, *Opinion 7/2009 on the level of protection of personal data in the Principality of Andorra* (WP166, adopted on 1 Dec. 2009) at 5.

68 実際、第29条作業部会の意見では、イスラエルが2010年に開催された第32回データ保護プライバシー・コミッショナー国際会議の主催国であったことを評価している。*See* Article 29 Data Protection Working Party, *Opinion 6/2009 on the level of protection of personal data in Israel* (WP165, adopted on 1 Dec. 2009) at 15.
この点、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以降、プライバシーの国際基準の要請が特に高まり、第31回会議において2009年11月5日に採択されたいわゆるマドリッド・プライバシー・宣言（International Standards on the Protection of Personal Data and Privacy, available at http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf）がひとつの重要な指針となりうる。堀部政男「『国際プライバシー基準』（International Standards of Privacy）という新たな基準論議―2009年マドリード会議の決議」日本データ通信172号（2010）1頁、藤原静雄「第3国への個人データ移転と『個人データの処理にかかるプライバシー保護の国際標準草案のための共同提案』」季報情報公開個人情報保護37号（2010）3頁、参照。

参考にしてきた「APECプライバシー・フレームワーク（APEC Privacy Framework）」（2004年10月29日採択）、あるいは国際連合「電子計算処理に係る個人データファイルの規制に関するガイドライン（Guidelines for the Regulation of Computerized Personal Data Files）」（1990年12月14日採択）はいずれも重要な国際的な文書であることに疑いはないものの、拘束力がない点で注意を要する[69]。

【ヒアリング結果】

- 一般データ保護規則提案では、これまでの第29条作業部会による意見をもとに欧州委員会が決定を下していたが、同作業部会による意見が廃止され、欧州委員会による決定に一元化された。また、一般データ保護規則提案には、十分性審査にテロ対策等を含む公共の安全という項目が追加され、データ保護の体制を考慮しうることになった点は注意を要する。（ナミュール大学）
- 現行の指令第25条と一般データ保護規則提案第41条の間に大きな構造の変化はない。
  一般データ保護規則提案第41条2項c節における「国際的なコミットメント」とは、拘束力ある文書を指している。（欧州委員会）

（5）EU一般データ保護規則提案第41条に対する関係機関の反応

（ｉ）第29条作業部会[70]

EU一般データ保護規則提案は個人データが保護された状態にあることを保証するためデータ管理者の説明責任を適切に強調している、という評価をしている。その上で、第41条6項の「第42条から第44条の規定を除き」という解釈について、十分性認定を受けていない国・地域・国際機関が、それでもなおこれらの規定に基づき第三国へのデータ移転が可能であるかどうかについて明確にすべきであるという意見を述べている。また、新たに設置される欧州データ保護委員会（European Data Protection Board）が十分性の決定について欧州委員会からの相談を受ける義務が含まれることを強く提案する旨意見表明している。

また、第29条作業部会は、EU一般データ保護規則提案の審議過程において現行の十分性審査の手続の再設計（redesign）を主張しており、WP12及びプライバシー保護に関する国際基準の共同提案に照らした十分性審査の基準の精緻化と更に多くの十分性の決定を下さすための審査手続の合理化を規則提案公表前から指摘していた[71]。

---

69 この点、欧州委員会は、カナダの個人情報及び電子文書法の十分性認定について、OECDプライバシー・ガイドラインと国連の個人データファイル・ガイドラインに依拠していることに言及している。*See* 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) at recital 8. 同様に、第29条作業部会はニュージーランドについても、OECDプライバシー・ガイドラインに準拠していることが再三指摘されている。*See* Article 29 Data Protection Working Party, *Opinion 11/2011 on the level of protection of personal data in New Zealand* (WP182, adopted on 4 April 2011).

70 Article 29 Data Protection Working Party, *Opinion 01/2012 on the data protection reform proposals* (WP191, adopted on 23 March 2012).

71 Article 29 Data Protection Working Party, *The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for fundamental right to protection of personal data* (WP168, adopted on 1 Dec. 2009) at 10-1.

（ii）欧州データ保護監督機関[72]

第三国移転の条項は非常に進展がみられ、かつ特定されていると指摘し、特に第41条2項が法規範及び、自主規制の役割がひとつの選択肢であるものの、効果的な救済体制ならびに独立した監督機関の存在をさらに明確にしている点を取り上げている。そして、前文79項において一般データ保護規則提案が欧州連合と第三国との間において完結した国際合意には効力を有しないとしている点について、既存の国際合意のみに適用すべきであることを推奨している。同時に、一般データ保護規則提案の発効後2年以内の国際合意であるとの経過規定を置くことも付言している。さらに、前文82項と第41条6項の解釈について、十分性認定を受けていない場合、「第42条から第44条の規定を除き」データ移転が可能かどうかについて、前文と本文との解釈の整合性が不明確であるという意見が述べられている。

また、欧州データ保護監督機関は、EUデータ保護改革案が公表される過程において、欧州委員会による十分性審査の決定が加盟国の間で異なった形で解釈されたり、実施されている批判を取り上げ、十分性の決定に関する加盟国におけるデータ保護機関の誠実な協調を要求していた[73]。

なお、何がデータ移転に該当し、該当しないかについても一般データ保護規則提案の中で明確にされるべきであることが指摘されている。そして、欧州データ保護監督機関は、欧州司法裁判所の判決の解釈も不明確であることから、特定の受取人に対してデータが送られる目的があるかどうか、データが無料で公開されているかどうか、さらに現実に外国の受取人に移転が行われたかどうかを考慮して決定すべきであると主張している[74]。

（iii）アメリカ商務省

2012年2月23日、アメリカホワイトハウスは、「ネットワーク化された世界における消費者データ・プライバシー」を公表した[75]。この消費者データ・プライバシーの枠組みにおいて、①消費者プライバシーの権利章典（Consumer Privacy Bill of Rights）、②執行可能な行動規範の策定に向けた多様な利害関係者との協議の促進、③連邦取引委員会の執行強化、④グローバルな相互運用（interoperability）の進展について記載され、オバマ大統領が早期に議会での法案提出・審議を求める内容となっている。

---

72 European Data Protection Supervisor, O*pinion of the European Data Protection Supervisor on the data protection reform package,* 7 Mar. 2012.

73 European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Region* (18 Jan., 2011) at 14, 30.

74 *Id.* at 19.

75 The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 23, 2012). Available at http://www.whitehouse.gov/sites/default/files/privacy-final.pdf. なお、消費者プライバシーの権利章典については、欧州委員会司法総局長が指摘するとおり、「消費者」のデータに限定されている点が批判されうる。司法総局は、消費者保護を人権問題として所掌しているが、消費者保護とは別の課がデータ保護を担当している。EU Conference: Privacy and Protection of Personal Data, March 19, 2012 (Francoise Le Bail欧州委員会司法総局長発言).

このアメリカの提案を受け、2012年3月19日に開催された欧州委員会主催の会議において、欧州委員会副委員長Reding 氏とアメリカ商務長官John Bryson氏によるデータ保護に関する共同声明が発表された[76]。共同声明において、「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」ことが指摘されている。アメリカとEUとの貿易額は2010年で約5600 億ドルにのぼり[77]、アメリカとEUのデータ移転の必要性は極めて大きい。セーフハーバー・フレームワークは2000年以降、3000社を超える企業がこれまでアメリカ商務省から認証を受けてきた。しかし、欧州委員会によって認められている参加可能なアメリカ企業が連邦取引委員会及びアメリカ運輸省の管轄にある企業に限られていること[78]や、①セーフ・ハーバー原則への遵守の意思表明の必要性（参加企業にプライバシー・ポリシーの公表がされていない例がみられた)、②商務省の強力な指導とモニタリングの必要性、③違反者に対する連邦取引委員会の強力な影響力の行使の必要性などが欧州委員会から合衆国政府に要請されていた[79]。また、Viviane Reding 欧州委員会副委員長兼司法総局コミッショナーは2012年3月19日の会議において、セーフ・ハーバー原則の履行に努力がみられるものの、技術・法律の専門家による対話の継続を必要としており、セーフ・ハーバー協定の改善に向け、「更なる改善がなされるべきである(more needs to be done)」[80]と指摘している。今回、アメリカは十分性審査を受けるという形ではなく、改めて「US-EUセーフ・ハーバーの継続的な緊密連携」を実施することを公表している。

---

76 *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. Available at http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/192&format=HTML&aged=0&language=EN&guiLanguage=en.

77 *See* Safe Harbour Workbook, available at http://export.gov/safeharbor/eu/eg_main_018474.asp.

78 連邦取引委員会が連邦取引委員会法第5 条に基づく権限行使をできる場合（不公正又は欺瞞的な慣行に対する救済を行える場合）と、運輸省が米国法典第49編第41712条に基づく権限行使をできる場合（不履行に対する個人への救済が与えられる場合）に限られている。*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, Annex* (2000/520/EC).

79 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*, Oct. 20, 2004 at 13-14. 欧州委員会の作業文書の前に欧州委員会からの要請でナミュール大学が作成した報告書には基本的な原則が履行されていないばかりでなく、法執行が担保されていないなど多くの「欠陥」が詳細に指摘されている。*See* Jan Dhont, María Verónica Pérez Asinari, & Yves Poullet, *Safe Harbour Implementation Study* (19 April, 2004). Available at http://ec.europa.eu/justice/policies/privacy/docs/studies/safe-harbour-2004_en.pdf
このように、アメリカのセーフ・ハーバーの枠組みは自主規制を前提としており、規制効果が希薄であること、また救済の欠如などから「自主規制は神話」であると批判されてきた。*See* Yves Poullet, *The Directive 95/46/EC: Ten Years after*, 22 Computer Law & Security Report 206, 210 (2006).

80 *See* Viviane Reding, *Towards a New "Gold Standard" in Data Protection?*, EU Conference: Privacy and Protection of Personal Data, March 19, 2012. Available at http://ec.europa.eu/commission_2010-2014/reding/pdf/speeches/20120319speech-data-gold-standard_en.pdf

なお、プライバシー団体等のNGOから欧州委員会、ホワイトハウス等に宛てた意見には、アメリカの法案が早く議会を通過できるようにすることと同時に、このような立法の欠如によって、アメリカはEU に対し個人データ保護の十分な保護措置を保証できないことが記されている[81]。

【ヒアリング結果】

・アメリカとのセーフ・ハーバーは機能しておらず、欧州委員会が不満を持っていると思われる。（ブリュッセル自由大学）

（6）日本の法制度に対する評価

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

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

主要な点については次のとおり報告されている。

○インターネット

日本法はインターネットに関して2つの点において対処できていない。第1に、個人情報保護法は取扱事業者にしか適用されないため、個人の行為については及ばない。第2に、仮に事業者がインターネットからの情報を入手しても、その事業者が小規模取扱事業者であれば、個人情報保護法が適用されない。

○越境データの移転

データ移転をする日本の事業者も外国の受領者もどちらも規制されていない。

○個人の権利救済

東京地裁の判決では、個人の開示請求権が否定された[83]。他の事案では民法709条により個人情報の漏えい事案について、損害賠償が容認されたことがあるが、その額は客観的に見て極めて低額である。民法その他の立法によりデータ保護違反があった場合、これらの法令を用いることができるが、裁判所が個人の権利を執行するための十分な代替措置となりうるかは疑問である。

---

81 *See NGO Letter on Privacy and Data Protection* (Mar. 19, 2012). Available at http://epic.org/privacy/intl/NGO-Letter-on-EU-US-Privacyfinal.pdf.

82 *See* European Commission, *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, B-5: Japan*, (by Graham Greenleaf) Jan. 20, 2010. Available at http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_B5_japan.pdf

83 東京地判平成19年6月27日判時1978号27頁。この点、「もし、わが国の個人情報保護法が、開示・訂正・利用停止の求めについて、司法救済を与えないものであるということになれば、EU個人情報保護指令12条、22条の求めるレベルに達していないということになり、わが国は、個人情報保護措置の不十分な国として、EU加盟国から個人データの移転を禁止されるおそれがある」という指摘がある。宇賀克也『個人情報保護の理論と実務』（有斐閣・2009）95頁、参照。

○監督機関

日本には独立の監督機関が存在しない。主務大臣制による執行が行われている。また、データ漏えいの通知制度や事業者の登録制度も存在しない。

国民生活センターおよび地方公共団体が処理する苦情について、各省庁が調査しているようには思われず、これらの苦情から強制的な処罰が行われているかは明らかになっていない。

さらに、主務大臣制の監督は応答的規制の制度を十分に果たしているとは思われない。

日本ではデータ漏えいによって名声を傷つけてしまうことが問題とされてきた。日本のデータ・コンプライアンスが他の国に比べて徹底しているという証拠はない。

○自主規制と行動規範

認定個人情報保護団体の取組の強化が取りまとめにおいて示されているが、この取組の効果については国民生活審議会から示されていない。

○日本のトラストマーク

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

そして、結論として、次のように述べられている。

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

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

（国際基準から見た日本の位置づけについて）日本のデータ保護制度はOECDガイドラインの基準を満たしている。また、APECプライバシー・フレームワークの基準を満たしていることも疑いはない。EU 指令との関係になるとこのレポートの範囲を超えるもので、難しい判断となる」[84]。

---

84 本調査報告書を執筆したGreenleaf教授は、別の論文の中で、アフリカ、ラテンアメリカ、アジア、オーストラリア、カリブ諸国の33の国・地域の法制度を比較分析し、その中で4カ国のみが例外的に「ヨーロッパ的な」諸要素（'European' elements）を備えていないとして日本、バハマ、ベトナム、チリを列挙する。また、同論文の中では、コロンビア、メキシコ、ペルー、韓国、インド、台湾が十分性審査を申請又は申請準備している可能性があることが記されている。*See* Graham Greenleaf, *The Influence of European Data Privacy Standards outside Europe: Implications for Globalization of Convention* 108, 2 INT'L DATA PRIVACY L. 68 (2012). また、Greenleaf 教授は、日本にはデータ保護監督機関が欠如していることが最大の要因となって、「日本はアジアの中で最も貧弱なデータ・プライバシー法を有する国の1つである」と指摘する。*See* Graham Greenleaf, *Independence of Data Privacy Authorities (Part II): Asia Pacific Experience*, 28 COMPUTER LAW & SECURITY 121, 126 (2012).

なお、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。

また、これまでも日本を含め多くの国・地域の十分性審査に関する欧州委員会からの事前調査に関わってきているナミュール大学法・情報・社会研究所のCécile de Terwangne教授は、「グローバルなデータ保護規制モデルは可能か」[85]と題する論文の中で、普遍的なデータ保護の基準として次の点を指摘しており、傾聴に値する。①利用目的制限の原則、②データの質の原則、利用目的の特定および制限の原則、④センシティブ・データ、⑤安全管理の原則、⑥公開性の原則、⑦個人参加の原則、⑧責任・説明責任の原則、⑨越境移転における適切な保護水準（proper level of protection）をデータ保護の内容として示し、同時に、①独立した監督機関、②法的な制裁及び救済を掲げている。さらに、追加的な原則として、①収集最小限の原則、②比例原則、③データ処理の知る権利を記している。これらの普遍的な原則は第29 条作業部会が十分性審査の基準として示した作業部会の文書（WP12）とほぼ同様の内容である。これらの普遍的な原則からみた日本の法制度の分析については本報告書の趣旨を超えるものであるが、日本の個人情報保護法制にセンシティブ・データ、越境移転における適切な保護水準、独立した監督機関、データ処理の知る権利について少なくとも明文規定が存在していないことを指摘するにここでは留めておく。

最後に、長年世界のプライバシー・個人情報保護法制度の研究を重ねるとともに、各国の関係者との意見交換を行ってきた堀部政男教授は「プライバシー外交」の推進を提唱する。この外交交渉において「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」[86]という指摘を「忘れない」こととしたい。

---

85 Cécile de Terwangne, *Is a Global Data Protection Regulatory Model Possible?*, in REINVENTING DATA PROTECTION 185-187 (Serge Gutwirth et. al. eds., 2009).

86 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。

現行 EU データ保護指令	EU 一般データ保護規則提案
第４章　第三国への個人データの移転	第５章　第三国又は国際機関に対する個人データの移転
	第 40 条　移転に対する一般原則 　処理されている又は第三国ないし国際機関への移転後に処理が予定されている個人データのいかなる移転も、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転送に対する場合を含め、本規則の他の規定に従い、本章で示された条件が管理者及び処理者によって履行される場合に限ってのみ行うことができる。
第 25 条　原則 １．構成国は、取り扱われている又は移転後に取扱い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に実体的効果を持つことなく、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。	第 41 条　十分性の決定に伴う移転 １．欧州委員会が、第三国、当該第三国における領土若しくは処理される分野、又は問題とされている国際機関が十分な保護措置を確保している場合に移転は行うことができる。かかる移転にはいかなる追加的許可も必要としない。
２．第三国によって保障される保護のレベルの十分性は、一つのデータ移転作業又は一連のデータ移転作業に関するあらゆる状況に鑑みて評価されなければならない。特に、データの性質、予定されている取扱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職業上の規則及び安全保護対策措置が考慮されなければならない。	２．保護措置の十分性を評価するにあたり、欧州委員会は次の点に考慮しなければならない。 (a) 公共の安全、防衛、国土の安全及び刑事法を含む有効な関連立法である一般的及び分野別の法規範、当該国又は当該国際機関によって順守される専門的な規則並びに安全措置、同時に、データ本人、特に個人データが移転された欧州連合に在住するデータ本人に対する効果的な行政法上ならびに司法上の救済を含む効果的かつ執行可能な権利 (b) データ本人の権利行使のため本人を支援し、助言し、かつ欧州連合並びに加盟国の監督機関との協力する目的でデータ保護規則の履行を確保する責任を負う当該第三国ないし当該国際機関における一つ又は複数の独立した監督機関の存在及び効果的な機能 (c) 当該第三国又は国際機関が従事する国際的な責任 ３．欧州委員会は、第三国、当該第三国における領土若しくは処理される分野又は国際機関が第 2 項の意味における十分な保護措置を確保していることを決定することができる。これらの決定行為は第 87 条第 2 項を参照して所定の審査手続に従い採択されなければならない。 ４．前項の決定行為は地理的かつ分野別の適用を特定しなければならず、かかる適用がある場合、第 2 項 (b) において示された監督機関を認定しなければならない。
３．構成国及び委員会は、第三国が第 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ないと考えられる事例について、相互に情報提供しなければならない。	５．欧州委員会は第三国、当該第三国における領土ないし処理された分野又は国際機関が、具体的には、当該第三国又は国際機関において一般ならびに個別の効力ある関連する立法がデータ本人、特に個人データが移転された欧州連合に在住するデータ本人に対して効果的な行政法上ならびに司法上の救済を含む効果的かつ執行可能な権利を保障していない場合には、本条第 2 項の意味における十分な保護措置を確保していないと決定することができる。これらの決定行為は第 87 条第 2 項を参照して所定の審査手続、そうでなければ、個人データ保護の権利に関する個人に対する極度に急を要する場合に第 87 条第 3 項を参照して手続に従い採択しなければならない。

4．構成国は、第 31 条第 2 項に規定する手続に基づいて委員会が、第三国が本条第 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ないと認定した場合には、当該第三国への同一タイプのデータの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。	6．前項に従い欧州委員会が決定した場合、第 42 条から第 44 条の規定を除き、当該第三国、当該第三国における領土ないし処理される分野又は問題とされている国際機関への個人データのいかなる移転も禁止されなければならない。欧州委員会は、本条第 5 項に基づきなされた決定から生じた状況を改善する観点から適当な時期に当該団三国又は国際機関と協議に入らなければならない。
5．委員会は、適切な時期に、第 4 項に基づく認定によってもたらされる状況を改善することを目的とする交渉を開始しなければならない。	
6．委員会は、第 31 条第 2 項に規定する手続に基づいて、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。構成国は、委員会の決定を遵守するために必要な措置を講じなければならない。	
	7．欧州委員会は欧州連合の公式刊行物において十分な保護措置が確保されていること又はされていないことを決定した場合、第三国及び国際機関におけるこれらの第三国、領土及び処理される分野の一覧を公表しなければならない。
	8．指令 95/46/EC の第 25 条第 6 項又は第 26 条第 4 項に基づき欧州委員会によって採択された決定は、同委員会による訂正、更新、又は取消があるまで引き続き効力を有するものとする。

＊EUデータ保護指令の訳については、付録の堀部政男研究室仮訳を参考にした。
(参考)
前文78項
　個人データの越境流通は国際取引及び国際協力の拡大にとって必要である。これらの流通の増大が個人データの保護に関する新たな課題と憂慮をもたらした。しかし、個人データが欧州連合から第三国又は国際機関に移転される場合、本規則によって欧州連合が保障する個人の保護の水準がないがしろにされるべきではない。いずれにせよ、第三国への移転は本規則の完全な履行の下に行われることができる。
前文79項
　本規則は欧州連合とデータ主体への適切な保護措置を含む個人データの移転を規制する第三国との間において完結した国際合意を損なわない。
前文81項
　欧州連合が確立した基本的価値、特に基本的人権の保障に即して、欧州委員会は、第三国の審査に際し、当該第三国が法規範、司法へのアクセス及び国際人権の規範並びに基準をどのように尊重しているかを考慮すべきである。
前文82項
　欧州委員会は第三国、第三国における領土若しくはデータ処理の分野又は国際機関がデータ保護の十分な水準を確保していないことを同じく認定する。その結果として、当該第三国への個人データの移転は禁止されるべきである。その場合、欧州委員会と当該第三国又は国際機関との間での相談を行うことが条件とされるべきである。
前文83項
　十分性の決定が存在しない場合、管理者又は処理者はデータ本人の適切な保護措置により第三国における個人データの不足を補填する措置を講じなければならない。かかる適切な措置は、拘束的企業準則、欧州委員会が採択した標準データ保護条項、監督機関が採択した標準的なデータ保護条項若しくは監督機関が認可した契約条項、又はデータ移転の運用若しくはデータ移転の一連の運用を取り巻く状況及び監督機関からの認可というあらゆる事情に照らし正当化された他の適当かつ比例した方法から構成される。

＜2＞　イスラエル[1]

駿河台大学法学部准教授　宮下　紘

はじめに

1890年「プライバシーの権利」という言葉が生誕した。ルイス・ブランダイスとサミュエル・ウォーレンによる共著論文「プライバシーの権利（the right to privacy）」においてである[2]。同論文は、「いまや生活への権利は、生を享受する権利を意味するようになった。すなわち、それは独りにしておいてもらう権利（the right to be let alone）なのである」とプライバシーの権利の内実を語っていた。

その後、ルイス・ブランダイスは、合衆国最高裁判所の裁判官に就任し、1928年、盗聴が憲法で禁止されている捜索にあたるかどうかが問われたOlmstead v. United States[3]において、「独りにしておいてもらう権利」を反対意見として提示した。ブランダイス裁判官は次のよう述べた。「憲法の起草者は、政府に対し、独りにしておいてもらう権利を付与した。すなわち、それは最も包括的な権利であり、文明化された人類によって最も価値ある権利である」[4]。ブランダイスが弁護士のときに執筆した「プライバシーの権利」の論文とOlmstead 判決の反対意見は、1967年Katz v. Untied States[5]の法廷意見として認められ、以後、プライバシーの権利がアメリカの法制度及び判例において確立した。

ブランダイスは、弁護士でもあり、裁判官でもあったが、彼はユダヤ教徒でもあった。ブランダイスの一連のプライバシーの権利論はユダヤの”tikkun olam”―人は自らの壊れた世界観を隠匿するという教え―を体現しているものと理解される[6]。また、ユダヤ教の箴言には他者との信頼関係構築のために秘密を保持する重要性が説かれている[7]。

「ユダヤ人民の発祥の地」[8]としてのイスラエルにおけるプライバシーの権利を取り巻く環境・制度を紐解くことは、プライバシーの権利を理解する一助となりうる。

1　本稿の執筆に際して、2012年1月に実施されたヒアリング調査において対応してくださったイスラエル法務省の法・情報・技術機関長Yoram Hacohen ならびに法務課長Amit Ashkenazi、及びCollege of Management School of Law、Omer Tene准教授の御厚意につき、この場を借りて御礼申し上げる。

2　Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

3　277 U.S. 438 (1928).

4　*Id*. at 478 (Brandeis, J., dissenting).

5　389 U.S. 347 (1967).

6　Erwin Chemerinsky, *Rediscovering Brandies's the Right to Privacy*, 45 Brandies L. J. 643 (2007).

7　Fred Rosner, Contemporary Biomedical Ethical Issues and Jewish Law 59 (2006).

8　The Declaration of the Establishment of the State of Israel, May 14, 1948.

１．イスラエルの個人情報保護法制

（１）イスラエル国の基本情報[9]

面積：2.2万平方キロメートル（日本の四国程度）

人口：約770万人

首都：エルサレム

民族：ユダヤ人（約75.4％）、アラブ人その他（約24.9％）

政体：共和制　元首：シモン・ペレス　首相：ビンヤミン・ネタニヤフ

議会は一院制（120名）（全国1区の完全比例代表選挙制度）

貿易相手国：輸出 北米（31％）、欧州（26％）、アジア（23％）

輸入 欧州（35％）、アジア（23％）、北米（11％）

経済協力：主要援助国は米。（建国以来、多額の有償無償経済援助を実施）

（２）基本法

イスラエルは、コモン・ローを採用し、成文憲法が存在しない。イスラエルの法制度はイギリス化（Anglicization）を経て、1980年代以降ユダヤ法（halkha）の影響を受けてきた[10]。

憲法典に代わる「基本法（Basic Law）」[11]が1958年に最初に制定され、実質的憲法としての機能を果たしてきた。つまり、他の法律との矛盾衝突が生じた場合、基本法が優先され、イスラエル最高裁判所によって当該法律は違憲無効とされる。本稿でも紹介するが、イスラエルのプライバシー保護は、比較法的に見ても活発な最高裁判所の判例によっても支えられている[12]。

プライバシーの権利については、1992年3月17日成立の「基本法：人間の尊厳と自由（Basic Law: Human Dignity and Liberty）」において明記されることとなった。同法の目的は、ユダヤ教の民主的国家としてのイスラエル国家の価値を確立する目的で人間の尊厳と自由を保障することとされている。同法7条は次のとおりプライバシーの権利を保障している。

第7条（プライバシー）

(a) すべての人がプライバシーと親密の権利を有している。

(b) 許可なく人の私有地への立ち入りをしてはならない。

(c) 人の私有地、身体及び所有物の捜索をしてはならない。

(d) 人の通信、信書及び記録の秘密を侵してはならない。

9　外務省HP参照。http://www.mofa.go.jp/mofaj/area/israel/data.html

10 *See* Menachem Mautner, Law and Culture Of Israel 35-6 (2011).

11 The Knesset, *Basic Laws*: *Introduction*. Available at http://www.knesset.gov.il/description/eng/eng_mimshal_yesod.htm

12 *See* Mautner, *supra* note 10, at 54.

もっとも、第8条（権利の侵害）により、①イスラエル国の価値に寄与する場合、②適切な目的がある場合、③必要以上に権利が侵害されない場合（いわゆる比例原則）については、プライバシーの権利が制限されうる。

この1992年基本法で掲げられたプライバシーの権利は、欧州人権条約（European Convention on Human Rights）第8条が保障する私生活の保護やEU加盟国のデータ保護法との間を反映していると理解されている[13]。

（3）プライバシー保護法

1981年の段階においてイスラエルのプライバシー保護法（Protection of Privacy Law: 5471-1981）[14]が制定されていた。その後、9回の法改正を行っている。

プライバシー保護法は全5章（第1章：プライバシー侵害、第2章：データベースにおけるプライバシー保護、第3章：弁護（プライバシー侵害をした場合の弁護手段)、第4章：公的機関による情報・データ提供、第5章：雑則）37条からなっている。

① プライバシー侵害について

同法第2条では、プライバシー侵害の例を次のとおり列挙している。

第2条（プライバシー侵害の例）

プライバシー侵害とは次のことをいう。

（1）本人を嫌がらせるような方法で又はその他の嫌がる方法で人を詮索又は追跡すること

（2）法で禁止されている盗聴をすること

（3）私的領域において人を撮影すること

（4）人を侮辱し又は軽蔑する可能性がある人の写真を公表すること

（5）受信者又は記者から許可なく、記述されたものが歴史的な価値を有するか、あるいは記述したときから15年が経過しない限り、公表を意図しない手紙又はその他記述したものの内容を複写又は使用すること（電子署名法において定義された電子メッセージを含む）

（6）人の氏名、名称、映像又は音声を営利目的で使用すること

（7）人の私生活に関して法で定められた守秘義務に違反すること

（8）人の私生活に関して明示又は目次の合意によって定められた守秘義務に違反すること

---

13 *See* The Israeli Law, Information and Technology Authority, *A Guide to Data Protection in Israel* (Jan. 2010) (by Ian Bourne). Available at http://www.justice.gov.il/NR/rdonlyres/C7DE27A2-4CC2-4C5E-9047-C86CC70BD50B/18333/AguidetodataprotectioninIsrael1.pdf.

14 Available at http://www.justice.gov.il/NR/rdonlyres/217BB43B-ED56-4F9B-A51F-074C3D29AE1D/18334/ProtectionofPrivacyLaw57411981unofficialtranslatio.pdf.

（9）定められた目的以外で人の私生活に関する情報を利用すること又は他者に伝えること
（10）（1）、（7）又は（9）の下でのプライバシー侵害の方法で得られた物を公表又は提供すること
（11）人の性的履歴、健康状態ないし私的領域における行為を含む人の親密な生活に関する事柄を公表すること

この第2条に列挙されたプライバシー侵害については、データベースにおけるデータの取扱いに限らず、あらゆる人のプライバシー侵害を含むものとされている。

② プライバシー保護の基本原則

イスラエルのプライバシー保護の適用範囲と基本原則について、第29条作業部会が示した作業文書（WP12）[15]の基本原則の項目（①利用目的の制限の原則、②データの質に関する原則及び比例原則、③透明性の原則、④セキュリティの原則、⑤アクセス・訂正・異議申立の権利、⑥国外移転の制限、追加項目として、⑦センシティブ・データ、⑧ダイレクト・マーケティング、⑨自動的な個人の決定）にしたがってみていく。

（i）適用範囲

・保護の対象

プライバシー侵害の保護の対象は「人（person）」に限られ､法人は含まれない（第3条）。情報とは、人格、身分、親密な関係、健康状態、経済的地位、職業・資格、人の意見・信念と定義される（第7条）。また、イスラエルの最高裁判所は「情報という言葉は…個人の氏名によって検索されないデータベースから引き出されるデータを含むべきである」（Israel v. Bank Ha'Po'alim）と解し、保護の対象を広く理解している。さらに、下級審の判断ではあるもののIPアドレスについて「同意なく本人のIPアドレスを公開することによってオンラインユーザーを特定することは、プライバシーの侵害という不法行為を構成することがある」（Rani Mor v. Ynet）という結論を下している。

・義務の対象

義務の対象であるデータベースとは、磁気を帯びた又は光学式の方法によって保存され、コンピュータ処理を目的としたデータの集積をいう。ただし、個人利用の目的の収集、またそれ自体で当該人物のプライバシーを侵害しない氏名、住所等のみを含む情報は除かれる（第7条）。なお、第2章のデータベースに関する義務規定は、情報が自動処理された場合にのみ適用されることとなり、マニュアル処理等の場合は第2 条によって保護することとなる。

---

15 Article 29 Data Protection Working Party, *Transfers of personal data to third countries: Applying Article 25 and 26 of the EU data protection* (WP12, adopted on 24 July, 1998).

（ii）目的制限の原則

第2章には個別の規定はない。しかし、一般的なプライバシー侵害を定めた2条（9）の規定（定められた目的以外で人の私生活に関する情報を利用すること又は他者に伝えること）は、事業者に対しても及ぶこととなっている。また、このことは、第8条(b)の規定により、データベースが設置された目的を除いて、データベースの利用を禁止する旨の利用制限によっても裏付けされている。さらに、第9条(b)(2)はデータベースの利用のための登録について、その申請はデータベースが設置された目的及び情報が意図とされている目的について明らかにしなければならないことを定めている。金融データの利用を利用目的の観点から制限したイスラエル最高裁判所の判決（Database Registrar v. Ventura）においてもこれらの規定のことが示されている。

（iii）データの質に関する原則及び比例原則

データの質に関する原則について特定の条文は列挙されていない。もっとも、第14条(a)において、自らの情報を検査した者がその情報について正しくない、不完全である、あるいは最新でないことを知った者はデータベースの所有者又は所有者が国外の場合は処理者に対して当該情報の訂正又は消去を要請することができる、と規定されている。これを担保するため、同条(b)ではデータベースの所有者が訂正又は消去に同意した場合、所有者は当該情報について必要な変更を加えなければならないとされている。これを拒否された場合、データ主体は裁判所に対して異議申立をすることができる（第15条)。

比例原則についてもまた、プライバシー保護法には列挙されていない。しかし、職場におけるビデオカメラによる監視を制限した判決や企業間での情報の交換を認めていた条項を無効と判断したエルサレムの標準契約裁判所の判決など比例原則に関する法理がある（Eisner v Richmond / Bank of Israel v. First International Bank of Israel)。

（iv）透明性の原則

データベースにおける個人に関する情報を保存及び利用する場合、本人からの要請に応じて、当該人物の情報が適法に利用されること、その利用目的、そして情報の提供先とその提供目的を通知しなければならない（第11条)。また、データベースの所有者がデータ処理者と異なる場所でデータを保管している場合、所有者は処理者に対して検査の要請に応じるよう書面で命じることができる（第13条A(1))。

（v）セキュリティの原則

情報セキュリティとは、合法な許可なく公開、利用、又は複写からの情報の統合の保護又は情報の保護することを意味している（第7条)。そして、いかなる者も法の定め又は裁判所の命令なくして自らの職務として得た情報を開示してはならず、これに違反した場合は5年以下の禁固に処せられる（第16条)。また、データベースの所有者、処理者又は管理者はデータベースの情報セキュリティに責任を負うこととされている（第17条A)。また、公的機関、銀行、保険会社、クレジット関連会社は情報セキュ

リティに関する適切な資質を有する者（security supervisor）を任命することとなっている（第17条B(a)）。

なお、2010年に「データベースにおけるセキュリティに関する規則案」が草案されており、情報セキュリティの責任者の設置義務、定期点検の実施、アウトソーシングの契約に関する規則等を含むセキュリティ強化の内容になっている[16]。

（vi）アクセス・訂正・異議申立の権利

すべての者が、自分自身、書面による代理人又は親権者によって、データベースにおいて保存された自らに関するいかなる情報も検査する権限を有している（第13条(a)）。また、情報の検査については、ヘブライ語、アラビア語、英語で行うこととされている（第13条(b)）。また、本人の身体又は健康状態に関する情報の検査の場合、当該人物に極めて悪影響を及ぼすと考えられる場合、本人に代わって専門家に当該人物の情報を提供することができる（第13条(c)）。そして、検査の要請に係る費用としては、20シュケル（約400円）支払うこととされている（第13条(d)）。また、検査を行った結果、情報が正しくない場合等、本人は必要な修正を要請することができる（第14条(a)）。本人の検査及び修正を拒否した場合については、本人が裁判所に申し立てることができる（第15条）とともに、刑事罰の対象となっている（第31条）。なお、異議申立の権利については明確な規定がないものの、利用目的の制限及びデータ主体への通知の規定から、これらの規定に違反した場合は、第2条9項に基づきデータ主体が異議申立をすることができるものと解されている。判例においても、警察が保有するファイルについて、自らの情報を知る権利があることを認めている（Fischler v. Chief of Police）。

（vii）国外移転の制限

個人データの第三国移転について、プライバシー保護法第36条2項は「イスラエル国の境界の外部への又は外部からのデータベースの情報送信に関する条件」について法務省がその執行に責任を負うことと規定している。そこで、法務省は2001年6月17日、データの海外移転に関する規則（Protection of Privacy (Transfer of Data Abroad) Regulations, 5761-2001）を制定した[17]。同規則はデータの移転に関する制限及び条件等を内容としている（全5条）。第1条は、データの移転の制限について次のように規定されている。すなわち、いかなる者も、移転されるデータの保護水準がイスラエル法によっ

16 Draft on Information Security Database, 5770-2010. Available at http://www.justice.gov.il/NR/rdonlyres/450A9F18-F22A-4D47-A408-47221D88BE24/18541/ProtectionofPrivacyRegulationsDraft25110.pdf

17 Available at http://www.justice.gov.il/NR/rdonlyres/6A5EC09A-BDBC-419F-8007-5FD6A6B8E0A5/18342/PrivacyProtectionTransferofDataabroadRegulationsun.pdf　なお、イスラエルにおいては、EUの十分性要件を課すのではなく、説明責任（accountability）の原則をもとにデータ移転を行うことが現実的である、という指摘がある。*See* Omer Tene, *Israel's Data Protection Reform*, 10 Privacy & Data Protection 13, 14 (2009).

て提供されるデータ保護の水準よりも低くならない場合を除き、イスラエルのデータベースからデータを国外に移転してはならないし、またすることができない。そして、具体的な保護の原則として、①データが合法かつ公正な方法で収集・処理されること、②データを受領したときの目的のみによって利用されること、③収集されたデータが正確かつ最新でること、④データ主体に検査の権利が認められること、⑤データベースにおける十分なセキュリティ措置を講じていることが要件として列挙されている。もっとも、第2条は、次のとおりデータ移転の例外を認めている。

① データ主体の同意がある場合
② 個人の健康を保護するデータためにデータの移転が不可欠な場合
③ 自国のデータベースの所有者の外国にある企業へ移転し、かつデータ保護が保証されている場合
④ データ受取人がデータ保護の義務を履行できる場合
⑤ 法令によってデータが公にされている場合
⑥ 公共の安全秩序の保護に不可欠な場合
⑦ イスラエルの法によって移転が必要とされている場合

また、第3条によって、移転されたデータの受取人はデータベースの所有者に対して書面で十分な保護措置を講じる旨確約しなければならない。このように、EUデータ保護指令第25条が定める十分性の要件と類似の規定が整備されている。

（viii）センシティブ・データ

センシティブ情報は第7 条で定義される「情報」（人格、身分、親密な関係、健康状態、経済的地位、職業・資格、人の意見・信念）のほかに、憲法、国会法及び司法委員会の承認を伴い、法務省が命令によって決定した情報が含まれる。

（ix）ダイレクト・マーケティング

ダイレクトメール（direct mailing）はデータベースに氏名が含まれる人物の1つ又は複数の特徴によって決定された集団の属性に基づきある人物に個人的にコンタクトを取ること、と定義される（第17条C)。そして、内容物がダイレクトメールであることを明示すること、受取者がデータベースのコンタクトリストから削除する権利があることを通知すること、さらにデータベースの所有者の氏名及び住所を明らかにしなければならない (第17条F)。そして、すべての者が書面によってダイレクトメールに用いられた当該人物の情報を消去してもらう要請をすることができる（第17条F(c)）。

（x）自動的な個人の決定

特定の明文規定はない。

（xi）その他

・賠償責任及び罰則

第1章のプライバシー侵害及び第2章におけるデータベースに関する規定に違反した場合、権利が侵害された個人は50,000シュケル（約100万円）を上限として民事上の損害賠償の訴訟を提起できる（第29条A)。また、消費者及び労働者に関する違反については、集団訴訟（class action）を提起することができる[18]。また、罰金の額は258,000シュケル（約516万円）が上限（となっており、裁判所の判断の下5年以下の禁固刑の規定（第16条）がある。

・登録制度

事業者は、10万人以上の情報を含むデータベース、センシティブ情報を含むデータベース、代理又は同意によって自身によって提供されていない情報が含まれるデータベース、公的機関に属するデータベース、勧誘サービスのために用いられるデータベースについて、利用の登録が必要である（第8条(c)）。

・データ保護違反通知義務

個人情報の漏えい等規則に違反した場合、金融分野についてのみ、データ保護違反の通知義務が生じることになる。

【ヒアリング結果】

1980年OECDプライバシー・ガイドラインが成立する前にすでにプライバシー保護法案は議会での審議が進んでいたため、イスラエルのプライバシー保護法は必ずしもOECDプライバシー・ガイドラインに依拠したものではない。また、実際の十分性審査については、第29条作業部会等に対してイスラエルの法制度が十分な保護水準であることを立証することになり、不文憲法、判例法、プライバシー保護法の3本から丁寧に説明を行った。

なお、イスラエルのプライバシー保護法と日本の個人情報保護法の異動について、下記のとおり表としてまとめておいた。

18 携帯電話会社が利用者のテキストメッセージを必要と定められている期間を超えて保有していたため、集団訴訟が提起された例Sudri v. Pelephone Communications Ltd., 21185-07-09(Central District Court).がある。*See* Omer Tene, *Reforming the Law from the Ground Up: Recent Developments in Israel's Privacy Regulation*, 9 PRIVACY & SECURITY LAW REPORT 1341 (2010).

	イスラエル	日本
法の仕組み	オムニバス方式（第4章に公的機関を対象とした規定）	セクトラル方式（基本法部分は、官民共通）
保護の対象	プライバシーそのものが保護の対象情報とは、「人格、人の地位、親密な関係、健康状態、経済的地位、職業・資格、人の意見・信念」と定義（7条）センシティブ情報、IPアドレスも含む	個人情報「生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの」格別の措置（6条）
事業者の義務	データベースの利用登録（8条）、情報セキュリティ（17条）等 ダイレクトメール（17条） 外国へのデータ移転（2001年規則）	OECDガイドライン8原則に基づく （15条以下）
本人の権利	開示（13条）、訂正（14条）、開示・訂正義務違反の訴訟（15条）	開示（25条）、訂正（26条）、利用停止（27条）
執行機関	法・情報・技術機関（7条） 文書提出、立ち入り検査、登録抹消（10条）	主務大臣制（36条）
罰則	民事：5000シュケル以下（約10万円）の賠償（29条） 刑事：1年の懲役（31条）	6月以下の懲役又は30万円以下の罰金（56条）

（4）イスラエル法・情報・技術機関

プライバシー保護法はデータベースの登録官（Registrar）の設置を規定し、裁判所の裁判官としての資質を有する者であり、官報（Reshumot）の公示により政府に任命されることとなっている（第7条）。

この登録官の設置のため、イスラエル法・情報・技術機関（The Israeli Law, Information and Technology Authority（以下、「ILITA」という。））は、2006年9月にイスラエル政府の決定（Israel's Government decision no. 4660 (19.01.2006)）に基づき司法省によってイスラエルのデータ保護機関として設立された。法務省の一機関ではあるものの、ILITAの長（Yoram Hacohen）は独立性をもって活動することができるとされている[19]。また、ILITAは法務部門、執行及び捜査部門、登録及び監督

19 ILITAが法務省の一機関として活動をしており、行政法上は法務大臣、また実質的には検事総長の影響をそれぞれ受ける可能性があり、EUデータ保護指令第28条にいう「完全な独立性」の要件を満たしているかどうか疑義が生じるという指摘がある。*See* Omer Tene, *Israeli Data Protection Law: Constitutional, Statutory and Regulatory Reform*, 8 Privacy and Data Protection 6, 10 (2007).

部門の3部の部署から構成され、30名程度で活動を行っている。

ILITAは、①プライバシー法に基づくデータベース登録、②クレジットデータサービス法に基づくクレジットデータサービス登録、③電子署名法に基づく認証登録という3つの既存の法規制の機能を統合している。その任務は、①個人データ保護の強化、②電子署名の使用の規制、③プライバシー及び情報技術違反の執行強化である。同時に、電子政府等の技術に関連する立法や政府の情報技術の企画に向けた政府内部の中心的な知識の拠点として活動している。

ILITAの権限としては、①データ登録者の検査、②苦情処理、③刑事事件の捜査、④行政罰、⑤クレジットデータサービスの認可、⑥データベースの登録、⑦データ登録者向けのガイドラインと標準規範、⑧情報プライバシー権の広報啓発が掲げられている。実際の執行については、ILITAが監督部署を設置し、検査官を任命することとなっている。そして、検査官は、データベースに関するデータ主体の情報及び書類を本人に提出するよう要求することができ、またデータベースの運用がされているという合理的な信念のもとその場への立ち入り、捜索、違法な行為をしていた場合の押収をすることができる（第10条(e1)）。実際の執行例としては、たとえば、近年、内務省が管理していた住民基本台帳のデータベースから約920万人の個人情報が不正アクセスにより公開され、ILITAの捜査により6名の容疑者が逮捕された事例[20]、住民基本台帳の不正コピーに基づきデータベースの売却を行った事業者に対して258,000シュケル（約516万円）の罰金を課した事例[21]、またマーケティング目的で不正に入手した個人データを利用した事業者に対して177,000シュケル（約354万円）の罰金を課した事例[22]がみられる。また、2009年の施行状況報告によれば、データベースへの登録は新たに408件の申請があり、その内の13%が申請を却下されている。また、2009年には107件の苦情処理を受理している[23]。

また、ILITAは国際協力を促進するため、データ保護プライバシー・コミッショナー国際会議、OECD 情報セキュリティ・プライバシー作業部会へのイスラエル代表としての出席、十分性審査への対応、スペインデータ保護機関の共同プロジェクトへの関与を行ってきている。

【ヒアリング結果】

ILITAは2007年から実質的な活動を始めている。ILITAは確かに法務省の一機関であるが、独立して刑事手続に基づく権限執行をできることや独立した予算が確保されていることなどが評価されたと考えられている。

---

20 http://www.justice.gov.il/MOJEng/ILITA/News/crackedcase.htm.

21 http://www.justice.gov.il/MOJEng/ILITA/News/fines220610.htm.

22 http://www.justice.gov.il/MOJEng/ILITA/News/administrative+fines.htm.

23 ILITA, *Annual Report on Action of Law, Information and Technology in 2009* at 24-32. http://www.justice.gov.il/NR/rdonlyres/A9CC34D5-9A75-47F7-98A9-D65FCA1EED7E/0/ILITAreport2009.pdf（ヘブライ語のみ）

（5）国際協力

イスラエルは、プライバシー保護に関する国際協力に力を入れている。第1 に、プライバシー関連の国際会議を開催してきている。中でも、2010年10月25日から29日にエルサレムにて開催されたOECDプライバシー・ガイドライン30周年記念国際会議（以下、「OECD会議」という。）及び第32回データ保護プライバシー・コミッショナー国際会議（以下、「コミッショナー会議」という。）には日本を含む世界中から約600名のプライバシー・コミッショナー、公的機関の担当官、研究者、実務家等が参加した。OECD会議は、「プライバシー保護における個人の進化する役割：OECDプライバシー・ガイドラインから30年（The Evolving Role of the Individual in Privacy Protection: 30 Years after the OECD Privacy Guidelines)」というテーマの下、イスラエルの首相であるビンヤミン・ネタニヤフ氏が挨拶を行った[24]。ネタニヤフ首相は「我々は自由な情報を持つ他の自由な社会を振る舞うことができ誇りに思う。しかし、この自由は我々のプライバシーとセキュリティに対する大きな脅威を伴うこととなる。…これは、単に顧客や市民としての個人にとっての問題ではない。それは国にとっての問題でもあり、同時に国際レベルにおける問題でもある」[25]と指摘した。また、コミッショナー会議では、「プライバシー：新世代（Privacy: New Generations)」というテーマの下、ILITAの主導によって20のセッションにおいてプライバシーを取り巻く最新問題が議論されるとともに、非公開セッションにおいては3つの決議が採択された[26]。このほかに、ILITA は、EUからの有識者等を招聘してEUからの十分性認定を受けたことに伴うビジネス界への影響に関する会議（The Business Potential of the EU Recognition of Israel's Data Protection Regime, July 7, 2011）を開催するなど定期的に会議等を開催している。

---

24 OECD Conference: *The Evolving Role of the Individual in Privacy Protection: 30 Years after the OECD Privacy Guidelines (Oct. 25-26, 2010).* Available at
http://www.oecd.org/document/44/0,3343,en_2649_34255_45780844_1_1_1_1,00.html
筆者は、同会議の結論のセッション（Implications for Policy Making）にパネリストとして参加させていただいた。
http://www.oecd.org/document/44/0,3746,en_2649_34255_45780844_1_1_1_1,00.html

25 Israel Ministry of Foreign Affairs, *PM Netanyahu addresses OECD conference in Jerusalem* (Oct 25, 2010). Available at
http://www.mfa.gov.il/MFA/Government/Speeches+by+Israeli+leaders/2010/PM_Netanyahu_addresses+OECD_Conference_Jerusalem_25-Oct-2010.htm

26 32nd International Conference of Data Protection and Privacy Commissioners.
Available at http://www.justice.gov.il/PrivacyGenerations/ 筆者は、「医学研究における新たな傾向：個別化医療（Emerging Trends in Medical Research: Personalized Medicine)」のセッションの議長を務めさせていただいた。

第2に、イスラエルは各国のプライバシー・コミッショナーと協働してプライバシー保護に関する執行に関与してきている。たとえば、2010年4月19日付のグーグル社宛ての手紙でILITAはカナダ、フランス、ドイツ、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、イギリスのプライバシー・コミッショナーと共同でGoogle社のサービスに対する抗議を行っている[27]。同書簡は、Google Buzz やストリート・ビューなどの「Google 者の新たな技術適用を開始することで世界の市民のプライバシー権が忘れられようとしている」と指摘し、Google 社のプライバシー及びデータ保護について問題点を明らかにしている。

第3に、ILITA はデータ保護を強化する目的で2009年6月から18か月の”Twinning Project”というものを実施した[28]。このプロジェクトは、欧州委員会からの資金（1,000,000ユーロ）でスペインのデータ保護機関と共同で国際基準に基づくイスラエル・プライバシー保護法の執行の強化をすることとイスラエルの行政機関、データ処理者及び市民におけるデータ保護の認識向上が目的とされている。この期間中にはスペインのデータ保護機関と共同して国際データ移転及びアウトソーシングに関する会議､ウェブサイトにおけるプライバシーの会議など2011年1月までに8 回の会議を開催してきている。

（6）プライバシー保護法の見直し動向

2007年1月、法第2章（データベース）を見直す目的で、次長検事（Deputy Attorney General）ら14名の有識者からなる委員会の報告書（Report: Committee for the Examination of legislation Relating to Database）（全135頁）（以下、当時次長検事で座長を務めたYehoshua Schoffmanにちなんで『Schoffman 報告書』という。）が公表され[29]。

同報告書には、①法の適用範囲、②情報の定義、③データ登録者の義務、④データ登録者の権限、⑤プライバシー保護審議会、⑥データベース運用の義務、⑦開示及び訂正の権利、⑧例外規定、⑨ダイレクト・マーケティング、⑩データの国外移転について、それぞれ委員の多数意見・少数意見が記されるとともに、EU、カナダ、アメリカ、アイルランドとの比較法的分析も含まれており、既存の法律に対する勧告が示されている。「同委員会は、ヨーロッパのデータ保護の水準と『十分性』の問題について明白に留意していた」[30]という指摘があるとおり、同報告書には随所にEUとの比較分析が含まれている。

---

27 Letter to Google Inc. Chief Executive Officer (April 19, 2010). Available at http://www.priv.gc.ca/media/nr-c/2010/let_100420_e.pdf See also http://www.justice.gov.il/MOJEng/ILITA/News/regulatorswarn.htm

28 ILITA, Twinning Project IS/2007/ENPAP/JH/01: Strengthening Data Protection in Israel. Available at http://www.justice.gov.il/MOJEng/ILITA/TwinningProject/

29 http://www.justice.gov.il/NR/rdonlyres/B11D19EE-7FC0-42ED-B2F5-2B4FDEE66BD4/18343/SchoffmanReport1.pdf

30 ILITA, *A Guide to Data Protection in Israel.*

まず、EUデータ保護指令については、「経済の成長と進展を窒息させる」、「先制的、官僚的、裁量的な体制を作り出している」といった批判的な意見と「消費者に対するより多くの情報と選択を企業が提供することを要求しているに過ぎない」といった「楽観的な意見」が掲載されている[31]。

また、同報告書には、セーフ・ハーバーについて、「他の国が同様の規定に依拠することができる見込みはないであろう。なぜなら、自主規制と政府の監督の組み合わせのセーフ・ハーバーの規定はアメリカ法に限定的に適合されており、さらに現実的には、アメリカがEU法の遵守というよりはむしろアメリカのバーゲニングの力を反映しているためである」と記載されている[32]。

このほかに、情報の定義を個人情報への変換、プライバシー侵害に対する集団訴訟に関する法改正、セキュリティ違反のデータベースの所有者からデータ本人への通知義務の導入、国外移転に関する罰則の整備などが示されている[33]。なお、イスラエル側から十分性審査の事前調査にもかかわり、またSchoffman報告書の委員会の委員でもあったMichael D. Brinhack 教授は報告書について次のとおり指摘している。すなわち、「委員会はイスラエルがアメリカの立場ではなくプライバシーに関するヨーロッパの理解を選択したことを再確認したのである」[34]。

【ヒアリング結果】

Schoffman 報告書は欧州委員会への十分性認定を申請する直接の契機になったわけではないが、同報告書においてEUの動向を調査した経緯があることは事実である。

（7）プライバシー保護に関する世論調査

イスラエルでは、2009年9月にプライバシー保護に係る意識に関する調査（18歳以上の男女529名から電話面談による有効回答）が実施された[35]。主な結果は次のとおりである。

- 個人データが適切に保護されていないと感じると回答　70%
- 異なる機関同士での個人データの移転についてイスラエルの既存の立法では対処しきれないと回答　58%（対処できると回答した者は34%）、
- データ保護に関する市民の意識が低いと考えていると回答　79%
- 個人データの利用に際して同意が必要であると考えていると回答　81%
- プライバシー保護法が適切な補償のための権利を付与していると考えていると回答　76%
- インターネットで個人データを用いることを心配していると回答　69%（安心であると回答22%）

---

31 *Schoffman Report*, at 129-130.

32 *Id*. at 126.

33 *Id*. at 91-4.

34 Michael D. Birnhack, *The EU Data Protection Directive: An Engine of a Global Regime*, 24 Computer Law & Security Report 508, 516 (2008).

35 ILITA, *Results of the data protection opinion poll conducted by ILITA*. Available at http://www.justice.gov.il/MOJEng/ILITA/TwinningProject/Publications/Results+of+the+data+protection+opinion+poll.htm

・ウェブ上でのプライバシー・ポリシーを常に確認すると回答　8%（たいてい確認すると回答 18%、ほとんど確認しないと回答　20%、1 度も確認したことがないと回答　42%）

2．イスラエルに対する十分性審査の手続

（1）イスラエルからの申請の背景

2007年7月12日	イスラエル代表部から欧州委員会にEUデータ保護指令25条の十分性審査の要請を受け、審査を開始した。イスラエルの十分性の審査を実施するに際して、欧州委員会はナミュール大学情報・法研究所に対して詳細な報告書を作成するよう依頼した。
2009 年3月18日	ナミュール大学情報・法研究所の報告書を基にセーフ・ハーバー作業部会（Safe Harbour Subgroup）で議論され、同作業部会はイスラエルの機関に対して、更なる明確化を要求した。
2009 年9月2日	ILITA からの回答がある。
2009 年9月16日	作業部会の際にILITAの長に対し明確化を要求し、議論を継続した。
2009 年10月12日～ 13日	作業部会から第29条作業部会に結果報告があり、意見を採択することとなった。

（2）事前調査

イスラエル側からの十分性評価の申請を受け、欧州委員会はナミュール大学情報・法研究所（現在は、情報・法・社会研究所Centre de Recherche Information, Droit et Société）に対し、イスラエルの規制制度が第29条作業部会WP12に基づき個人データ保護の規制に関する運用状況について分析を依頼した。なお、この報告書（Franck Dumortier, Cécile de Terwangne,Florence de Vilenfagne, Yves Poullet, Michael D. Birnhack, *Assessment of the personal data protection regime in Israel to determinate whether provides adequate protection : final report*（2008年）、Cécile de Terwangne,Florence de Vilenfagne, Laurence Dumortier, Yves Poullet, Michael D. Birnhack, *First analysis of the personal data protection law in Israel in order to determinate whether a second step has to be undertaken*（2006年））は公表されていない。

【ヒアリング結果】

第29条作業部会に対するイスラエルの法制度に関する説明については、ILITAの長及び法務課長、また1名の有識者とともにこれを行った。

３．イスラエルに対する十分性審査の結果概要

（１）第29条データ保護作業部会の意見

第29条データ保護作業部会は、2009年12月１日付の意見において、「当作業部会は、イスラエルが指令95/46/EC 第25条第６項にしたがい十分な保護水準を保証しているものと信ずる」[36]との結論を下した。

この意見（全18頁）は、①背景、②イスラエルにおけるデータ保護に関する法、③個人データの十分な保護を提供するものとしてのイスラエルのデータ保護法の評価、④評価の結果、という構成になっている。すでに１と２においてそれぞれ、イスラエルの十分性審査の背景及び法制度については紹介したため、以下、第29条作業部会の評価について紹介する。

（ｉ）保護の対象

第７条の「人格、身分、親密な関係、健康状態、経済的地位、職業・資格、人の意見・信念」という情報の定義は、EUデータ保護指令第２条「識別された又は識別され得る自然人に関するすべての情報」という定義とは異なっている。そこで、イスラエルのプライバシー保護法は、①特定のデータの類型のみを対象としているのではないか、また②識別し得る情報が保護の対象になっているかの疑問が生じる。しかし、イスラエルの担当官からの説明を受け、法律とそれを補完する裁判所の先例によって保護の枠組みが構成され、それはEUデータ保護指令の定義と一致するものと作業部会は信じている。

（ii）保護される処理の制度

第７条では「磁気又は光学式方法によって保存され、コンピュータ処理を意図されたデータの収集」をデータベースとして定義している。イスラエルの担当官の説明によれば、自動処理されないデータについても、法で定められた秘匿性と同意という基本原則によって保護されうるとのことであることを明記する。しかし、当作業部会は、データ処理の全体性の観点から処理されるデータを保護することを明確にすることを要望する。

なお、Schoffman報告書では、マニュアル個人情報ファイルについても、法の義務が及ぶようにすべきことが指摘されている[37]。

（iii）目的制限の原則

作業部会は、プライバシー保護法第２条９項、第８条(b)、第９ 条(b)(2)の規定及びイスラエルの最高裁判所の判例から目的制限の原則を尊重しているものと信じている。

---

36 Article 29 Data Protection Working Party, *Opinion 6/2009 on the level of protection of personal data in Israel* (WP165, Dec. 1, 2009).

37 *Schoffman Report*, at 23.

（iv）データの質に関する原則と比例原則

データの質に関する原則について独立した規定がないものの、訂正権を認めた14条、訂正を拒否した場合のデータベース所有者の義務を定めた15条から、データを最新の状態に保つ義務があると認められる。

また、比例原則もプライバシー保護法には特定的に列挙されていないものの、作業部会は、イスラエルの担当官から最高裁判所の判決における比例原則に関する憲法の適用に関する説明を受け、この明確な説明から比例原則を満たすものと考えている。

（v）公開の原則

データの本人に対する情報提供を義務づけている第11条また、データベースの所有者が処理者に対してデータ本人に対する検査を要請に応じるよう命令すること定めた第13条A(1)の規定からEUデータ保護指令を十分に履行していると考えられる。

（vi）セキュリティの原則

第7条における情報セキュリティの定義をはじめ、第16条、第17条、第17条A、第17条B の規定からこの原則は守られていると考えられる。

（vii）アクセス・訂正・異議申立の権利

自らのデータを検査する権利（第13条)、訂正権（第14条）とともにこれに違反した場合の罰則（第31条）の規定がある。異議申立の権利については、ダイレクトメールに関してそのような権利が認められている（第17条F)。しかし、一般的な条項の下で異議申立の権利が確立されていないように思われるが、利用目的の権利（第8条(b)、第2条9項）及びデータ主体への情報提供の観点から、利用目的を超え過剰な処理が行われた場合、プライバシー侵害の一般原則である第2条9項に違反し、罰則の対象となる。さらに、データの主体が自らの情報について知る権利を認めた最高裁判所の判決を積極的に評価することもできる。このようなことから、イスラエルの立法がデータ本人のアクセス・訂正・異議申立の権利を十分に保障していると理解される。

（viii）データ移転に関する制限

2001年プライバシー保護規則によってデータベースの移転に関する制限が行われているが、作業部会は第三国への転送についても制限が及び、イスラエルにおいてデータが処理されるEU市民の権利が十分に尊重されることを可能とするものであると信じている。

なお、国際的なデータ移転については、その例外規定がプライバシー保護規則第2条に設けられているものの、その解釈指針については、第29条作業部会が示した解釈（WP114）[38]を参考にすべきであることが同作業部会から指摘されている。

---

38 Article 29 Data Protection Working Party, *Working Document on a Common Interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995* (WP114, adopted on 25 Nov. 2005).

このほかに、補足的な原則として、次のようなものがあり、自動決定に関する点を除き、いずれもEU指令の基本原理に合致する。

（ix）センシティブ・データ

第7条は、EUデータ保護指令第8条が列挙するすべてのデータの類型（人種または民族、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）が掲げられていないものの、類似するものとみることができる。作業部会としては、イスラエル担当官に対して、特に意見と信念とはEUデータ保護指令が規定する内容が含まれ、また親密な関係には特に民族出自又は性生活に関連するデータを指しているものと主張する。さらに、センシティブ・データの収集に伴う事前の同意については、明確な規定がないものの透明性の原則を参照することによってデータ主体に対して情報が明確に与えられるものとなっていると信じている。このようなことから、EUデータ保護指令とは同様の規則があるわけではないが、イスラエルの立法は十分にセンシティブ・データの原則を充足しているものと考えられる。

（x）ダイレクト・マーケティング

作業部会は、イスラエルの立法においてダイレクト・マーケティングについて明確に規制が行われていることを十分に確認することができる（第17条F)。

（xi）自動的決定

自動的決定に関する原則について明文化されていないものの、ナミュール大学の報告書及びイスラエルの担当官からの説明において、データの主体が自動的決定に対する異議申立をすることができる。しかし、作業部会はEUデータ保護指令15条に基づく同様の原則を補足することを奨励する。

○手続・運用の体制

（i）規則を順守する優れた水準の確保

ILITAは、第7条に基づき設置された機関であり、データベースの登録とともにデータ処理の検査の権限を有している。ILITAの長の任命及び解任に関するイスラエル政府の近時の修正によって、EUデータ保護指令における監督権限の設置される目的に十分な独立性が認められる。ILITA及びその長は公務員（civil servant）としての身分を享受し、いかなる命令的・政治的側面にも従属するものではない。独立した委員会の事前評価を受け、イスラエル政府が決定した高官（a high rank official）としてILITAの長が任命され、6年間の任期を有する。ILITAの長の職務を停止するには、特別な事情の下、特別公務員委員会（special Civil Service Commission）による場合でなければこれを停止することができず、独立性を有する反トラスト委員会の体制と類似する。ILITAの財政についても、データベースの登録料がILITAに直接還元されるなど、その独立性を維持するだけの割当てが行われてきている。加えて、検察庁、内務省、運輸省、防衛省、司法省を含む公的機関に対する立ち入り検査を実施する権限が付与されているというILITAの回答からも独立性が保障されている。

また、32回データ保護プライバシー・コミッショナー国際会議を招聘するなど、個人データ保護の

努力がみられる。このようなことから、作業部会はイスラエルにデータ保護に関する監督機関が存在するものと結論づけることができる。

さらに、ILITAはプライバシーの侵害について、裁判所の刑事手続に従い捜査する権限が認められるとともに、行政罰を課すことができる。

以上のことから、作業部会はイスラエルの立法が規則を順守する優れた水準の確保しているものと信じている。

（ii）個々のデータ主体に対する支援と援助

登録官（ILITA）は監督するための部署の設置及び検査官の任命により、ILITAの検査官がデータ主体の情報及び文書を本人に届けるよう要求すること、建物への立ち入り、捜索及び押収が認められている（第10条(e)）。この規定により、個人データへの主体に対する支援と援助が十分保障されていると考えられる。

（iii）適切な救済

作業部会は、行政罰及び刑事罰を含む制裁の措置からプライバシーの権利及び個人データの違法な処理の結果生じる財産に対する損害を補償する権利が十分に担保されていると信じている。

④評価の結論

第29条作業部会は、イスラエルが十分な保護水準を確保していると結論付けた。もっとも、イスラエルに対する将来的な立法措置として次のことが提案された。

・マニュアル・データベースへの法の義務の適用
・民間部門における情報収集原則の明確化
・国際的なデータ移転の例外規定に関する解釈

（2）欧州委員会の決定

2011年1月31日、欧州委員会は「個人データの自動処理に関するイスラエル国による個人データの十分な保護」に関する決定を下した[39]。本来であれば、第31条委員会による審議を経て、本決定を下すべきであるが、同委員会の議長が期日までに意見を提示していなかった（前文16 項）。

全7条からなる意見となっている。第1条1項は「指令95/46/EC 第25条2項の趣旨から、イスラエル国は、欧州連合から個人データの自動的な国際移転に関して、又は自動的に移転されない場合、イスラエル国は、欧州連合から個人データの自動的な国際移転に関して、又は自動的に移転されない場合、

39 European Commission, *Commission Decision 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). もっとも、イスラエルが十分な（adequate）水準の保護措置を確保していることは、それがEUの基準と同一（identical）であることを意味するものではないと、ナミュール大学との事前調査に加わったBirnhack教授はある共著論文の脚注において指摘している。*See* Michael Birnhack & Niva Elkin-Koren, *Does Law Matter Online?: Empirical Evidence on Privacy Law Compliance*, 17 Mich. Telecomm. Tech. L. Rev. 337, 356 n112 (2011).

イスラエル国において更なる自動処理を受けることとし、欧州連合から移転される個人データの保護の十分な水準を確保しているものとみなす」と十分性認定を行っている。前文9項においても、イスラエルのデータ保護の法的水準は、データベースにおける自動処理される個人データに関して自然人の保護の十分な水準のために必要なすべての基本原則を満たしていることが記載されている。

もっとも、第29条作業部会の意見及び第1条においても指摘されているとおり、この十分性認定は自動処理されたデータの移転のみを対象としており、「自動処理化されていない方法は本決定には含まれるべきではない」（前文12項）となっている点は注意を要する。

その他、第29条作業部会でのマニュアル処理への適用、比例原則、データ移転の例外規定の留意点もまた指摘されている（前文15項）。

また、1条2項はイスラエルにおける監督機関がILITAであることを示している。その対象は、東エルサレムを含む国際法上認められているイスラエル国の領土について適用される（第2条2項）。

そして、EUデータ保護指令の他の規定で定められた措置を講じるため加盟国が条件又は制限を課すことは認められており（第2条1項）、イスラエルにおける受取人へのデータの移転を停止する権限を行使することができる（第3条1項）。

最後に、この決定を下した2011年1月31日から3カ月以内に加盟国は決定を履行するための必要な講じることが定められている（第6条）。

4．イスラエルに対する十分性審査から学ぶべきこと

（1）欧州評議会条約第108号という選択肢

イスラエルの「プライバシー外交」[40]には明確に2 つの選択肢があったように考えられる。ひとつは、EUデータ保護指令第25条に基づく十分性の認定を受ける方法である。いまひとつは、欧州評議会条約第108号（個人データの自動処理に係る個人の保護に関する条約）を締結することで、これにより実質的に十分な保護水準を確保している国であるとみなされる方法である。第29条作業部会WP12 においても、「欧州評議会条約第108号を採択した国がEU指令第25条の意味における十分な保護水準を与えているとみなしうることは単なる学問的興味以上のものである」[41]と述べられており、欧州評議会条約第108号の締結は実質的に十分性認定と類似の効果を持ちうるのである。ILITAからのヒアリングにおいてもこのことは指摘された点である。また、Schoffman 報告書においても十分性審査に関する委員会の一般的な合意として次のような記載がある。

---

40 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）59頁。

41 *See* Article 29 Data Protection Working Party, *Working Document: Transfers of personal data to third countries: Applying Article 25 and 26 of the EU data protection directive* (adopted on 1 Dec. 2009, WP165) at 15. もっとも、欧州評議会108条約それ自体が改正作業の段階にあり、改正案（2012年3月5日時点）第12条にはデータ移転に関して「十分な保護水準」という要件が入っていることには注意を要する。*See* The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *Modernisation of Convention 108:New Proposals*. Available at http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD-BUR_2012_01Rev_en.pdf

「当委員会の委員は欧州連合が[EUデータ保護]指令の要件に整合的に保護水準を確保している国としてイスラエルを受け入れるかどうかの問題について審議をすべきであるということに一致していた。当委員会の委員は[欧州評議会]条約に入るよりも指令第25条2項に従う認定の方が好意的であると考えている。その第1次的な理由は、指令の枠組みにおいて、すでに多くの国がヨーロッパの基準を順守していると認定されてきているが、他方で欧州評議会以外の国で条約に応じた国は1つもない。そのため、当委員会は指令の規定に基づく認定の試みに十分な優先度を置き、もし成功するのであれば、他の国が認められてきたのと同様に我々も情報の送信を認められることとになるであろう。指令は欧州連合のすべての加盟国によって義務的に履行していることに伴い現在は特に重要である。それに対し、条約は指令によって対処されていない分野において基本的に重要である(国土の安全、法執行など)。当委員会の勧告に従い、法務省は外務省を通じ欧州委員会にこの問題を書面で伝えたことを指摘しておく。イスラエルは指令の基準を満たす国として認定されるべきイスラエル側の要請に関してその見解を決定するため現在欧州連合と連絡をとっているところである。[2007年1月公表時点]」[42]

このように、個人情報保護の国際的水準を検討にするにあたり、イスラエルはEU データ保護指令と欧州評議会条約第108号の2つの選択肢を分析し、その結果、前者への申請に踏み切ったものと理解される。

(2) ILITAの独立性

ILITAについては、法務省の一機関であることから、その独立性については疑問視されていた。Schoffman 報告書においてもILITAの権限強化(特に刑事手続法のもとでの捜査権限)が指摘されていた[43]。もっとも、実際の十分性審査においては、第29条作業部会の意見にも示されているとおり、ILITAの長の任命、解任並びに任期の手続及びILITAの予算が保障されていること、またILITAは自らが属する法務省を含め公的機関に対しても立ち入り検査をできる点などから独立性の要件を満たしていると評価されている。このように、十分性審査については、機関それ自体の法的性格というよりも、その機関が効果的に法を執行できる位置にあるという「実質的要件(substantive criteria)」を立証することが重要であり、ILITAが独立性を認められたことは他の十分性を申請する国にとっても新たな道を開いたことになる[44]。

---

42 *Schoffman Report*, at 89.

43 *Schoffman Report*, at 43.

44 *See* Tene, *supra* note 18, at 1342.

（3）国際協力の重要性

イスラエルは、プライバシー保護における国際協力に非常に熱心に取り組んでいる。本稿で紹介したとおり、他のデータ保護機関との協働、国際会議の開催などの取り組みはEU加盟国とも協調し得る可能性を十分に示していると思われる。実際に、「ILITAは他のデータ保護機関の経験から学ぶことに極めて熱心である。そして、ILITAは格別に開かれ、受容性のある組織である」[45]という指摘のとおり、ILITA は今回のヒアリング対応も含め他の国の機関との国際協調性を非常に重んじているように思われた。2012年1月25日に公表されたEUデータ保護規則案第41条2 項(c)には新たに「国際的な責任（the international commitments）」が十分性審査の要素として掲げられている。国際的に影響力のあるデータ保護プライバシー・コミッショナー国際会議を開催するなどILITAが従事してきた「国際的な責任」は日本にとってもひとつの教訓となりうると思われる。

45 ILITA, *A Guide to Data Protection in Israel.*

＜3＞　ウルグアイ

埼玉工業大学専任講師／国立情報学研究所特任助教
河井　理穂子

１．個人情報保護制度の概要

1.1　個人情報保護関係法令の概要

（１）ウルグアイ東方連邦共和国[1]

ウルグアイ東方共和国（以下、ウルグアイ）は、南アメリカ大陸の南東に位置し、北はブラジル、西はアルゼンチンに接している。南側にはラプラタ川が流れ、東側は大西洋である。気候は、平均気温16℃で1年を通して適度に雨が降る。人口は、338万人ほど（2010年の統計、欧州系90%、欧州系と先住民の混血8%、黒人系2%)、面積は17.6万平方メートルの小国である。首都は、モンテビデオ、公用語はスペイン語である。そのGNI（国民総所得）は、355億米ドルで、2010年の経済成長率は、8.5%にもなる。農牧業（牛肉、羊毛、米等)、食品加工業、製造業（羊毛製品、皮革加工品等）が主要産業であるが、サービス産業、ソフトウェア産業も近年重要な産業になりつつある[2]。現在の主要貿易相手国は、輸出入ともに、ブラジル、アルゼンチン、中国が上位を占めている。

政治制度は、立憲共和制であり、行政、司法、立法の三権分立が確立している。

（２）個人情報保護制度の意義

情報社会の中で、日々個人の情報が蓄積され、処理され、流通している現状に鑑み、ウルグアイの個人情報保護制度においては、個人情報に関する権利が人権として定義されている。The Agency for the Development of electronic Government and Knowledge Based Society（AGESIC）のもとに、個人情報保護担当機関（監督機関）(the Personal Data Control and Regulatory Unit, URCDP）が新設され、同様にAGESIC のもとに存在するCitizen’s Right Officeが個人情報保護法制の執行実務を担っていることからも、個人情報に関する権利は人権である、という捉え方が強いことが伺える。

一方で、ウルグアイ政府は、個人情報保護制度を整備することは、ウルグアイの国際的競争地位を高める事につながると考えている[3]。EU諸国が、EUデータ保護指令（Directive 95/46/EC of the European Parliament and the Council, of 24 October 1995）に従って十分性を満たさない国々への個人情報の移動を制限していることをあげ、このことがウルグアイ企業の海外マーケットへの進出の障害になり、さらにウルグアイへの海外からの投資の障害になる可能性があることへの危機感が強い。後述するように、ウルグアイ政府がかなりのスピードで個人情報保護法制を整備したことの背景には、このような経済的な政策方針が存在すると考えられる。

1　外務省HPより http://www.mofa.go.jp/mofaj/area/uruguay/data.html

2　URCDP（ウルグアイ個人情報保護法担当監督機関）のMag. Federico Monteerde 氏へのインタビュー（2012 年3月5日）

3　Unidat reguladora y De control de Datos Personales, Annual Report 2009 (Unidad Reguladora y De Control De Datos Personales), p1

（3）憲法上のプライバシーの権利と個人情報に関する権利

現行憲法は、1967年に制定されたものであり、プライバシーの権利及び個人情報に関する権利について明文では規定されていない。しかし、憲法第72条においては、「この憲法が定める権利、義務、保障は、人間が生まれながら持つもの、また共和国政府から得たものを排除するものではない」と規定されており，さらに、憲法第332条は、「憲法が承認する個人の権利、付与されている権利、国家権力に課せられた義務は、関連の法令の欠如によって妨げられない。むしろ、これらは、現行の類似の法律、法の原理原則、一般原則によって代用されることにより、保護されなければならない」と定めている。

このように、憲法第72条、第332条により、憲法に明文として書かれていなくとも個人の根本的な権利は承認されており、これをもとにウルグアイの個人情報保護法（The Protection of Personal Data and “Habeas Data” Action (Law No.18331, LDPD)）が、2008年8月6日に制定されている。

（4）個人情報保護法制概要

(a) The Protection of Personal Data and Habeas Data Action（LDPD, Law No.18331）（個人情報保護法）

ウルグアイの個人情報保護法の主たる部分を構成しているのがThe Protection of Personal Data and “Habeas Data” Action（Law No.18133、以下 LDPD）である。この法律は、2008年8月11日に公布され、公共機関、民間機関のすべてに適用される、いわゆるオムニバス方式を採用している。

まず、第１条で、個人情報に関する権利を人が生まれ持った権利として規定し、この権利は憲法第72条に含まれているとされている。そして一般条項である第2条は「この法律は、どのような媒体に記録された個人情報にも適用され、公共、民間問わずその個人情報のその後の利用に適用される」としている。

(b) The Regulating Decree No.414/009 (DPDP)（行政規則）

LDPDが成立した後、2009 年8月31日にウルグアイ政府は、The Regulating Decree No.414/009 (以下、DPDP) という行政規則を制定した。この規則は、LDPD に関してその適用範囲、定義、同意、セキュリティ、情報へのアクセス権、個人情報データベースの登録方法、監督機関、委員会、諮問委員会の機能、様々な手続方法などについて規定をしている。また、この行政規則の前文では、この個人情報保護に関する全国的な法制度は、EU データ保護指令（Directive95/46/EC of the European Parliament and the Council, of 24 October 1995）の定めるレジームに適合させることが適当であると明確に書かれている。

(c) Regulatory degree No.664/008（個人情報データベースの登録に関する規則）

本規則は、LDPDに規定されている個人情報データベースの登録に関する手続について規定するものである。LDPD以前には、信用情報分野のみに適用される個人情報保護法（Law No. 17838、2004年に成立）が存在していたが、LDPD成立後は効力を失い、Law No.17838のもとで登録された個人情報データベースはそのままLDPD上の個人情報データベースに移行された。

なお、LDPDで規定される個人情報データベースとは、「処理、取り扱うことができる状態に整理されたすべての個人情報で、それが電子的であるかそうでないかは問わない」(LDPD 第4 条 (A))。また、

LDPD では、Chapter V において公共機関のデータベースについて、Chapter VI において民間機関のデータベースについて、それぞれ登録する義務がある旨規定されている[4]。

（5）The Protection of Personal Data and Habeas Data Action（LDPD, Law No.18331）（個人情報保護法）と The Regulating Decree No.414/009 (DPDP)（行政規則）

（a）適用範囲

LDPD と DPDP は、DPDP 第3条に定められた2つの場合に適用される。1つは、ウルグアイにおいて設立された個人情報データベース、データベース管理者によって個人情報が取り扱われている場合、もう1つは、ウルグアイの個人情報データベース、データベース管理者によって個人データが取り扱われている訳ではないが、データの処理にウルグアイ国内に設置されているメディアを使用される場合である。後者の場合には、例外規定が置かれており、データの移転（transfer）のみがウルグアイ国内のメディアを通して行われる場合は、国外の個人情報データベース、データベース管理者が国内にその代理人を指名し、法的義務を果たしている限りは、適用除外になるとされている（DPDP 第3条)。

また、個人情報データベースが、個人的に家庭内での利用に限られている場合（E メール、個人的な日記など)、公共のセキュリティ、防衛、国家の安全保障、刑事的な犯罪に関わる場合は、この法律は適用されない（DPDP 第2条)。

（b）個人情報収集の目的と事前同意

個人情報を収集する場合、当該情報の利用目的、データベース管理者による情報の取り扱われ方に関して、原則として情報主体の同意を得なければならない（LDPD　第9条、DPDP　第9条)。個人情報を収集する際には，如何なる目的で利用され、その情報を取り扱うのが誰であるのか，などを明確に伝えることが必要とされ、特にセンシティブデータ[5]の収集については、必ず同意が必要とされる。また、10営業日以内に同意が得られない場合は、同意が得られなかったとみなす（DPDP 第6条）など、同意に関する細かい規定がDPDPで規定されている。また、形態は問わないが、同意の証拠について保存しておく義務が、データベース管理者にあることも規定されている（DPDP　第6条)。LDPD 第11条では、自然人又は法人が法的に情報を入手した場合、秘密性を保持し、ビジネスや事業の収集時に定めた目的のみに使用することとし、第三者への配布を禁止している。

4　ある民間企業に対するインタビュー（2012年3月6日、8日）では、登録手続が大変煩雑かつ政府からの登録やLDPDに関する情報が少ないことから、登録が義務であるにもかかわらず、特に中小企業が登録まで至っていない例もみられた。また、登録を怠ったこと自体に対する法的な罰則は存在しない。

5　センシティブデータとは、人種、政治観、倫理や健康、性生活に関する情報（LDPD4条（E））をいい、特に健康に関するデータについては、DPDP 第4条（D)で、EU裁判所によって導かれた、過去、現在、未来の身体的、健康的健康状態であると定義をしている。遺伝情報なども含まれる。

例外として事前同意が必要ではない場合についても、LDPD 第9条（A）～（E）に列挙されている。公共にオープンになっている情報源から得られたデータ（たとえば記録や出版物、マスコミなどからの情報)、行政機能上必要な情報、法的な義務によって集められるデータ、情報の収集が契約によって定められている場合や就業上必要である情報、個人的な利用のために収集される情報などについては、同意が必要でないとされる。特に（C）では、自然人の氏名、ID card番号、国籍、住所、誕生などの個人データの収集の場合、事前の同意は必要ないとする。法人の場合は、会社名、ブランド名、税番号、住所、電話、責任者名については、事前の同意が必要ないとされている点に特徴がある。

（c）データの真実性“ veracity principle”

LDPD 第7条では、集められた個人情報は、真実かつ適切で，偏り、欠缺があってはならず、また収集の目的に照らし、必要以上に多く集められたものであってはならないとされる。また収集においては、フェアで不正ではなく、侮辱的であってはならず、その他すべてのこの法律に反するものであってはいけないとされる。

さらに､個人情報は正確で､最新のものでなくてはならないとする（LDPD 第7条)。そして､個人データが不正確又は間違っている場合は、データベース管理者は、いつでもそのことに気づいたら速やかにデータを削除し、正確な情報に書き換えなければならない。また、この法律に従って、期限の切れたデータも削除される必要がある（LDPD 第7条)。

LDPD 第8条では、収集された個人情報はその収集目的以外の利用については禁止され、収集の目的と照らし合わせて個人情報の削除が必要又は適当な場合は、いつでも個人情報は削除されなければならないとしている。

（d）透明性の原則

情報主体の権利として､個人情報を収集される際､その目的などを伝えられることが認められている。LDPD 第13条において、データを収集する者は、そのデータを取得するときに、事前に、明確に、はっきり、曖昧性なく、情報主体に対して以下の点を伝える義務があることが規定されている。

☆　データの取扱目的、そのデータを取得する者が誰であるか

☆　そのデータが保管される電子的又はその他のデータベースの存在、管理者が誰であるのか、管理者の住所

☆　センシティブデータの場合、同意なしに個人データの収集が強制されることはないこと

☆　データを提供することにより起こりうる結果とデータ提供を拒むことによる結果、又はその結果の不明確性

☆　情報主体は、自己の個人情報にアクセスする権利があり、修正、削除をする権利があること

収集に際して同意が必要な個人情報かそうではないかに関わらず、情報収集の際には以上の事柄を情報主体に伝えなければならない。

（e）アクセス、訂正、異議に関する権利

IDカードやその他の方法で身元が確認されれば、すべての情報主体は公共又は民間のデータベースの自己に関する情報にアクセスする権利を有する。またこの権利は、6ヶ月に1回であれば無償で行使

することができる（LDPD 第14条)。要請された情報は明確に、コーディングなしに、説明が必要ならこれを付して、一般人が理解できるような表現で提示されなければならない。さらに、要請のあった情報について、データベース管理者は5営業日以内に提供をしなければならず、この要請への応答が拒否された場合又は要請自体に反応がない場合、情報主体は後述するHabeas Data Action を取ることができる。

また、情報主体は自己の個人情報が正しくない場合はこれを訂正することを求めることができる。さらに、状況に応じて、自己のデータの処理に反対することもできる。

個人の権利に関連して、LDPD第15条は、自然人、法人は誰でも、自己の個人情報について、エラー、間違い、抜け落ち等が存在する場合、修正、更新、追加、削除を依頼することができるとする。

また、情報主体からのデータの要求が、ある側面だけを参照するものであっても、提供する個人情報は､総合的でありすべてのその人に関することを含んでいなければならないとする。手書き､電話､図､など情報主体の望む適切な形態で提供される必要がある。さらに、その情報主体と関わりがあるものであっても、第三者へ個人情報を提供してはならない（LDPD第14条)。

(f) データセキュリティ

LDPDは、第5条（E）においてデータセキュリティ原則を規定しており、第10条ではその原則を発展させ、データベース管理者又はデータベースの取扱者は、情報のセキュリティ、信用性（機密性）を脅かすことのないよう、必要な措置を講じなければならないとする。この措置は、データの変更、紛失、無許可の処理が行われることのないよう、そして、故意的か故意的ではないかを問わず、さらに人的か技術的かを問わず、情報の取り扱われ方に問題がある場合はそれを検知することが必要であるとする。そして、このような完全なセキュリティに関する措置が行われない場合は、個人情報に関するデータベースの保持を認めない。

また、個人データの漏えいについては、情報主体への報告義務がある（DPDP 第8条)。

(g) 個人情報保護担当機関（監督機関）

個人情報保護担当機関についての詳細は後述するが、LDPDに関する監督機関として、Unit for the Regulatory and Control of Personal Data（以下、URCDP）を置く事が規定されている（LDPD 第31条)。URCDP は、Agency for the Development of Electronic Management Government and Information and Knowledge Society（以下、AGESIC）に属する独立した機関である。URCDPは、AGESIC の下にありながら､独立性を持つという特徴を持ち､URCDPは､行政に対して報告義務がなく、業務に対して完全なる独立性を保っている。

URCDPは、侵害行為に対する処罰の執行権限を有する他、大きく分けて8つに分けられる業務を遂行する義務を負う。詳細については、後述（1.2）する。

(h) 処罰

侵害行為に対する処罰については、LDPD 第35条に規定されており、いずれもURCDPがその執行権限を持つ。1）警告、2）500000index units（500万円以下)、3）データベースの停止の3つが挙げられている。3）データベースの停止については、侵害行為が行われてから6ヶ月以内に、URCDPが裁判所に対して命令を求めることにより、裁判所よりデータベースの停止命令が下される。

(i) 個人データの第三国移転に関する規則

DPDP第4条の(E)と(F)では、個人情報の輸出入者につき定義されている。個人情報の輸出者とは、自然人、公共、民間を問わず、ウルグアイ領に存在し、第三国へ個人情報を移転する者である。また、個人情報の輸入者とは、第三国のデータベース管理者、取扱者から（第三者の場合を含む）個人情報を受けとる者のことである。

LDPD第23条は、すべての個人情報に関して、第三国又は他の国際機関のうち、個人情報の保護について十分なレベル（国際的、又はその地域において）に達しない国又は機関への移転を禁止している。また、URCDPは、十分なレベルに達していない第三国への個人情報の移転について、管理者が十分なセーフガードを設けているのかに関する監視を行うことができるとされている。

LDPD 第23条に設けられている例外は、以下の場合などであり、この場合は、第三国の個人情報保護のレベルに関わらず移転が可能である。

☆ 情報主体が個人情報の移転につき明確に同意している場合

☆ その移動が、情報主体とデータベース管理者の間の契約の執行に必要な場合又は契約の前提であった場合、若しくはその移動が、公共の福祉、又は裁判上必要であった場合

☆ 人命に関わる場合

☆ 個人情報の提供を受けるための法的要件を満たした場合

(j) Habeas Data Action

Habeas Data Action は、ラテンアメリカの国々特有の法制度で、情報主体が自己の情報についてデータベースにアクセスすることが出来、相手方が公共機関であるか、民間事業者であるかに関わりなく、その情報が間違っている場合又は古くなった場合に、修正、更新、消去を要求できるというものである。Habeas Data Actionが憲法によって定められている国、法律によって定められている国など、国ごとに異なるが、上記の要求が認められない場合は、裁判所に権利の実現と補償を求めることできるとする点が共通する。

ウルグアイでは、どのような法主体（自然人、法人、公的機関、民間事業者関わらず）であっても、憲法によって認められている人が持つすべての権利に関する侵害行為（公的権限を有する機関の不作為や民間事業者による侵害行為を含む）について裁判所に救済を求めることが出来るという法律、Amparo Law No.16011（Ley de amparo）が1988年に成立した[6]。この法律は、他の法令において権利侵害に対する救済が与えられておらず，かつ行政による救済がない場合のみ適用される[7]。この救済の特徴は、その早さである。判決が出るまで1審で30日、2審で60日であるという点である[8]。

---

6 Allan R. Brewer-Carías, Constitutional Protection of Human Rights in Latin America: A Comparative Study of Amparo Proceedings, Cambridge University Press (2008), p117

7 前掲6,p118

8 Dra. Ana Brian Nougreres 教授（リパブリカ大学）へのインタビュー

LDPDでは、Chapter VII（第37 条〜）において、Habeas Data Protection Action を規定し、手続については、このAmparo Lawの文言をそのまま用いている（第40条〜第45条)。LDPDにおけるHabeas Data Actionでは、情報主体は、データベースに登録されている自己の情報を参照したいとリクエストをしたが拒否をされた場合、期限以内に回答をもらえなかった場合、また、情報主体がデータベースの自己の個人情報について、修正、更新消去する、追加、削除することをデータベース管理者に尋ねたが、リクエストに応えない、十分に理由を述べずに期限以内に回答しない場合について、裁判所に対して救済を求めることが出来る。

個人情報に関する権利に対する侵害の場合、証拠収集が難しいという問題点がある。公共、民間問わず、個人情報が保管されているデータベースは組織内部に存在し、情報を得ることは難しい。そのため、個人情報に関する権利が侵害されたと考える者は、はじめからHabeas Data Actionによって裁判所に起こすのではなく、まずURCDPに苦情を申し入れ、調査をしてもらう。この際、様々な事柄に対してURCDPは開示を求めることが出来るため、被害者側に有利に働く場合が多いという[9]。侵害行為に対する救済について、URCDPにおける行政からのアプローチと被害者が直接行うHabeas Data Actionによる裁判所へのアプローチの２種類を平行して行うことは可能であるが、今までに前例はない[10]。

(k) センシティブデータ

LPDP 第4条（E）では、人種、人種のルーツ、政治観、倫理、労働組合等の所属状況、又は健康や性生活に関する情報をセンシティブデータとしている。特に、健康に関するデータについては，DPDP4d)で、EU裁判所によって導かれた定義である、「過去、現在、未来の身体的、精神的健康状態」として定めている。ここには、遺伝情報なども含まれる。

LPDP 第18条では、何人も強制的にセンシティブデータを収集されないとし、情報主体の同意の上でのみこれらの情報は収集できる。ただし健康情報については､公共又は民間の健康に関連する機関は、患者又はそこでケアを受けている者の身体的、精神的な個人情報の機密性を守り、特定の規定と条項を遵守することにより、収集できる（LPDP 19条)。さらに、LPDP 第17条（C）では、健康情報の流通について規定をする。公共の健康、公衆衛生、緊急、疫学上の利用について、データと個人が結びつかない状態で特定できない状態であれば、事前の同意は必ずしも必要ないとしている。

(l) ダイレクトマーケティングなど

情報主体は、ダイレクトマーケティングに個人情報が使われることをいつでも拒むことができる。LDPD 第21条では、家の住所、広告や手紙を送付することなど、営業、広告などに使える、又は消費者の趣味趣向を出すことができる情報については、その情報が公共にアクセス可能であるか、個人から同意を得て得られたものであるときのみ、利用することができる。また、この場合も情報主体はいつでもそれらの情報を削除することができる。

9　前掲8

10 前掲8

また、自動処理であるかないかによらず、個人情報を処理することによって得られる、就業状況や信用関係などについて自己に重大な影響を及ぼす事柄については、LDPD 第16条において、人はそれらの情報によって判断をされない権利を有しているとする。さらに、このような情報によって影響を受けた情報主体は、データベース管理者にこれらの情報が得られた元の情報、そして処理方法について追求することが出来る。

1.2 個人情報保護担当機関（執行機関）

（1）Unit for the Regulatory and Control of Personal Data（URCDP）

LDPD 第31条により、LDPD 及びDPDP の監督執行機関として、The Unit for the Regulatory and Control of Personal Data（以下、URCDP）が設立された。URCDP は、The Agency for the Development of electronic Government and Knowledge Based Society（以下、AGESIC）の下におかれているが、独立性を保っている[11]。AGESICは、大統領の下に存在する政府機関である。

(a) URCDP の構成

URCDP の執行委員会は、3人の委員で運営される（1人は、AGESICのエグゼクティブディレクター、あとの2人は、独立した判断、能力、客観性、公平さを保つために、経歴、実務経験、知識などをもとに行政から指名される。選任は大統領にゆだねられ、その手続は法律によって決められている。エンジニア、弁護士などのさまざま職業の委員が選出される[12]。執行委員会のメンバーのAGESICのエグゼクティブディレクター以外は、任期4年で再任が可能である。不適格、不作為、犯罪行為においてのみ法的手続によってのみ解任させることができ、大統領や行政部はそれ以外の理由で解任することが出来ない。執行委員会のメンバーは、命令、指示などはどこからも受けることなく、またどこへの報告義務もないとLDPD 第31条に明記されている。執行委員会の行政行為は、独立して公平性をもって、法に基づいて、非公開で行われる。DPDP 第23条において、URCDPの委員長は、毎年3人のメンバーが持回りで交代するとされる。委員長に欠員が出た場合は、AGESIC のエグゼクティブディレクターが担当する。執行委員会の議決は、多数決で決定されるが、同数の場合は、委員長の票を2票と数える（DPDP 第24条）。委員長は、緊急の際に特別措置を行うことを決めることができ、それは議決にも反映される。また、執行委員会は、諮問機関を持つ。諮問機関は、5人で構成され、それぞれ議会から指名される人権問題に明るい人（議員である必要はない）、司法からの代表、行政の代表、学者からの代表、民間からの代表の5名である。

---

11 URCDPの他に、the Unit for Access to public Information（UAIP）という独立性のある機関がAGESICには存在する。

12 2012年3月現在の委員は、エンジニア1人に、弁護士2人という構成である（URCDPの執行委員の1人であるFederico Monteverde 氏に対するインタビューによる）。

（b）URCDPの役割とCitizen's Office

LDPD 第34条に明記されている、URCDPの役割は以下である。

☆　必要とする人への法的な総合的な支援とアドヴァイス

☆　法律でカバーされている事項の実現のための規則などの制定

☆　データベース管理者の登録、調査及び常に登録されていることを保持すること[13]

☆　データベース管理者がどの程度まで個人データの完全性、正確性、セキュリティに関する規則を遵守しているかをモニターし、必要に応じ立入調査を実施すること

☆　背景情報、関係書類、プログラムなどデータの取り扱いに必要な情報すべてを、政府、民間のデータベース保持者に要請すること（URCDPは、情報が安全、秘密に扱われることを保証しなければならない）

☆　政府機関から依頼のあった場合に、法違反に対する行政罰、その他個人情報の取り扱いに関する法に関する規則、決定に関する意見書を起案すること

☆　必要に応じて個人情報に関する法案について、行政府に対してアドヴァイスを与えること

☆　情報主体に対して、無償で、個人情報データベースの存在、その目的、データベース管理者の素性を教えること

さらに、LPDPは、取調べ、立入調査、処罰に際してURCDPが従うべき手続と規則を定める。特に、データベース登録手続と国際データ移転に関しては、DPDPに規則が定められている。

上記の役割と後述する行政罰執行の実務は、実際はAGESICの中にあるCitizen's Officeの職員によって行われている。Citizen's Officeは、LDPDに定められている業務以外にも、広く人権に関わる問題に関する業務についても担当をしている。Citizen's Officeは、15人のメンバーで構成され、その大半が弁護士である[14]。

---

13 データベースの登録数は、2009年度はデータベース数：5733、データベース管理者数：3365 であったが、2010年度は、新規追加についてデータベース数：3934、データベース管理者数：2185 となり、合計で、データベース数：10693、データベース管理者数:6047 となった。（2011年度については、2012年3月現在まだ年次報告書が出来ていない）

14 Citizen's Office のDra. Esc. Beatriz Rodriquez Acost とDra.esc. Prof. Maria Jose viega Rodriguezに対するインタビュー（2012年3月7日）

（2）行政罰執行のしくみと状況

(a) 行政罰執行のしくみ

LDPD 第12条は、データベース管理者はこの条項の違反に関して責任があるとし、LDPD 第35 条において、URCDPは以下の行政罰を執行することができるとされている。

データベース管理者、取扱者がこの法に違反した場合は、

☆　警告

☆　500000index units（約500万円）までの罰金を課す

☆　データベースの停止

AGESIC は、データベースの停止に際しては、情報流出又は違法行為が証明されてから6日以内に管轄権のある裁判所に対して、停止の命令を求めなければならない。

URCDPの権限に関しては、DPDP 第31条において以下のように規定されている。

☆　執行委員会が法的根拠のある決定を行った場合、どのような立入調査も行うことができる。

☆　執行委員会が法的根拠のある決定を行えば、証拠隠滅の可能性がある場合、裁判所に対し必要な措置を講じるための要請をすることができる。

☆　すべての上記の措置に関して、データベース管理者、取扱者と対話をし、10日以内の猶予を与える。10日の期間経過後は、執行委員会での決定が30日以内に行われ、執行が行われる。

(b) 執行状況

2010年度のURCDPに対する電話での問い合わせは2640件で、このうち手紙によるものが227 件であった。電話の問い合わせの86%がデータベース登録の手続に関するものであった。手紙による問い合わせでは、LDPDに関する疑問が141件、データベース登録に関する問い合わせが76件などであった[15]。このうち、苦情は11件であった。

また、2010年度は2389件の決定と25件の意見を公開した。この2389件の決定の大半はデータベースの登録手続に関しての回答であった。

さらに、行政罰執行については、2010年度は5件の警告が行われ、罰金も1件課された。2011年度にはじめてデータベースの停止を巡るケースが起こり、現在裁判所の命令待ちの状態である[16]。

---

15 Unidat reguladora y De control de Datos Personales, Memoria annual 2010,p30

16 2010 年4 月現在（前掲14）

（3）情報主体への支援とサポート

LDPD 第34条（A）では前述のように、URCDPは必要とする人への法的な総合的な支援とアドヴァイスを行うと規定する。さらに、(H）で、URCDPの役割として, 無償で、個人情報データベースの存在、その目的、管理者の素性を教えることなどを規定している。それ以外にも、たとえば、DPDP 第25条では、URCDPが意見を公表する際には、Webに掲載しなければならないとされるなど、情報主体への様々なサポートが提供されている。

2　十分性審査の交渉過程

2.1　十分性審査の準備

ウルグアイでは、個人情報保護に関する初めての法律（Law No.17838）が2004年に成立したが、法的に保護されていたのは一部の個人情報に関してだけであった。すなわち、法の適用範囲は信用情報に関わる情報だけに限定され、総合的なものではなかったのである。

ウルグアイ政府は、Law No.17383の適用範囲を広げ、すべての個人情報に総合的に適用する必要性に鑑み、新しい法律の制定を検討した。この際、同時にEUデータ保護指令上の十分性を満たすことを視野に入れた。

ウルグアイの個人情報保護制度がEUデータ保護指令条の十分性を満たすことの最大のメリットは、ヨーロッパの資本を呼び込むことができることである。ヨーロッパ資本がウルグアイ国内に流れ込むことにより、産業や雇用を伸ばそうという狙いがある。ウルグアイはソフトウェア産業においてかなりの飛躍を遂げており、現在南米で第1位のソフトウェア輸出国である[17]。また、IT関係の教育にも力を入れており、小学生1人に1台のノートパソコンを配布することに成功し、すべての小学校に無線LANが設置されている[18]。ウルグアイ政府は、ヨーロッパ資本のうち、特にコールセンターやソフトウェアなどの特に個人情報に関わる可能性の高い産業を念頭においており、個人情報保護法の整備は必須であるという政策を打ち出している[19]。

上記のような理由から2008年にEUデータ保護指令上の十分性を満たすことを視野に入れた形の新しい個人情報保護法（LDPD）が制定される運びとなった。

成立過程の詳細は、2.3にて後述する。

---

17 RCDP の執行委員の1 人であるFederico Monteverde 氏に対するインタビュー（2012 年3 月5 日）

18 前掲17

19 前掲17

2.2　十分性審査の過程

（1）経過

2008年10月20日、ウルグアイは、欧州委員会（European Commission）に対して、データ保護指令の25条6項の十分性を満たしているかどうかについて、手続を開始するよう要請をした。

欧州委員会は、ナミュール大学情報・法研究センター（the Centre de recherches Informatique et Droit(CRID) of the Universit of Namur, 当時）に対して、ウルグアイの個人情報保護制度が、1998年7月24日に29条作業部会によって承認された「第三国への個人データ移転・EU データ保護指令25条及び26条の適用」（Transfers of personal data to third countries: Applying articles 25 and 26 of the EU Data Protection Directives）という作業文書（WP）に示された要件を満たしているかどうかの分析を依頼し、その後、同センターにより報告書が提出された。この報告書作成には、アルゼンチン人のPablo Palazzi 弁護士[20]が携わった[21]。2010年2月11日、ウルグアイ政府は、URCDPを通してこの報告書の指摘した事項（問題）について回答を行った。

29条作業部会の下に、サブグループが設立され、ウルグアイ政府の上記報告書への回答も考慮にいれ、ウルグアイ個人情報保護法がEUデータ保護指令の示す十分性を満たしているかについて評価を行った。サブグループは、ウルグアイにおける個人情報保護のレジーム（Law No.18331, of 11 August, the Protection of Personal Data and ”Habeas Data” Action（LPDP）と the Regulating Decree of 31 August 2009, dictated on its development（DPDP））に対する前向きな評価を下したものの、さらにいくつかの事柄を明確にする回答を求める手紙をウルグアイ政府に送った。

ウルグアイ政府は、2010年6月23日、29条作業部会に対して、要請に対して相当な長さの回答を送り、URCDP 年次報告書（2009年）と2009年5月31日までのURCDPの活動についての資料も添付をした。このウルグアイの回答は、2010年9月にサブグループへ送られ、特に回答を求めた項目を中心に分析が行われ、サブグループは作業部会に分析の結果を回送した。作業部会は、これを受け、ウルグアイの個人情報保護制度がEUデータ保護指令上の十分性を満たすかにつき、Opinion 6/2010 on the level of protection of personal data in the Eastern Republic of Uruguay（2010年10月12日発行）において審査結果を公表した。

ウルグアイ政府（URCDP）は、2回の正式な回答文書の送付の他に、電話やメールなどで数々の質問をサブグループのメンバーとやり取りをしている。また、この回答の過程においては、スペイン語が母国語であるという利点を生かし、スペインのプライバシーコミッショナーと密な連携がなされていた[22]。

---

20 http://www.habeasdata.org/ を主催しており、個人情報保護法の分野で幅広く活躍をしている。

21 前掲14

22 前掲17

（2）審査

作業部会の審査結果が記載されたOpinion 6/2010 on the level of protection of personal data in the Eastern Republic of Uruguay では、基本原則として、1）目的限定の原則、2）データの質に関する原則及び比例原則、3）透明性に関する原則、4）セキュリティに関する原則、5）アクセス、訂正及び異議申立に関する権利、6）第三国への移転に関する制限に関して、付加的原則として、1）センシティブデータ、2）ダイレクトマーケティング、3）自動的な個人決定、そして、手続と執行メカニズム（個人情報保護担当機関）について、それぞれEUデータ保護指令で規定されている内容と比較しながらひとつひとつ検討を行っている。

以下では、作業部会が作業文書で特に問題にした点、又は強調をしている点について示す。

(a) URCDP（個人情報保護担当機関）の独立性について

ウルグアイ政府によると、29条委員会を説得することに苦労した点は、URCDPの独立性についてであった[23]。

URCDP が大統領の下に属するThe Agency for the Development of electronic Government and Knowledge Based Society（AGESIC）に属しており、執行委員会は、AGESIC のエグゼクティブディレクター、大統領から指名された2人の委員から構成されているため、行政機関から独立していないのではないかという懸念を作業部会はもった。これに対して、ウルグアイ政府は、URCDPはどの権力にも属さず、またURCDPはどの機関又は人に対しても報告義務を持たず、法に規定されている事項以外で解任されないと説明をした。

また、DPDPに定められているように、執行委員会の3人のメンバーが1年ごとに持回りで委員長を務めることにより、委員会の決定がより公平に行われ、AGESICのエグゼクティブディレクターの権限を制限し、委員会の独立性を強めていると作業部会は考えた。さらに、2009年度と2010年の途中までのURCDPの活動の結果などを総合的に考慮して、29条作業部会はURCDPの独立性について認めた。

(b) データの質に関する原則及び比例原則について

(個人情報収集において事前の同意が必要でない場合（LDPD 第9条（c））)

LDPD 第9条（c）では、自然人の氏名、ID card 番号、国籍、住所、誕生日のリストの場合、また法人の場合は、会社名、ブランド名、税番号、住所、電話、責任者名については、個人情報収集において事前の同意は必要ないと規定されている。これに対して、作業部会は個人情報の目的外利用の可能性について懸念を示した。ウルグアイ政府は、どのような場合においても、この法律の原則である目的の制限に関する原則を超えるものではなく、よって、同意が必ずしも必要でないとしても、データベース管理者は、明示的に法的な範囲内のデータの処理だけが認められおり、データの適当、適切、そして制限を超えない範囲での取得に限られていると説明をする。これにより、作業部会は、データの質に関する原則及び比例原則を満たしていると認めた。

---

23 前掲14

(c) 透明性原則について

LDPD 第9条では個人情報の収集に事前に同意が必要な場合について、LDPD第13条では事前の同意が必要な場合とそうではない場合についても両方、その個人情報収集の目的やデータベース管理者の情報等を、情報主体に対して収集の際に伝える必要があるとしている。これらの条文は、同意がある場合、又は自発的に情報主体から情報が提供される場合にのみ適用されるようにも読めると、29条作業部会は疑問をもった。これに対して、ウルグアイ政府は、これはすべての場合、無条件にすべての法的条件に基づいて処理される情報に適用されると説明をした。たとえば、データコミュニケーションの結果、第三者を通じて収集された情報についても、情報主体はこれらの情報の転送について事前にLDPD 第13条に基づいて知らされなければならないとしている。これによって、透明性原則の十分性は満たされていると作業部会は判断をした。

(d) データの第三国への移転について

EUデータ保護指令では、自国から第三国へ個人情報を移転した場合、さらなる国への個人情報移転は、その次のさらなる国がEUデータ保護指令上の十分性を満たした法制度を有している場合に限るとしている（例外は、EUデータ保護指令第26条に規定されている場合のみである)。

LDPD は、EUデータ保護指令と類似の国際情報移転に関するコンセプトを持つ。しかし、LDPD 第23条は、このコンセプトが適用されない２つの種類（２つのリスト）の例外を規定する。このうち２つ目のリストは、EUデータ保護指令の第26条2項で規定するものと同等であると考える。一方、1 つ目のリスト（以下に掲載）は、EUデータ保護指令の第26条1項と文言上一致するものではないものを含むと作業部会は考えた。このリストにあてはまる場合では、第三国への個人情報移転に関して、LDPD が適用されないこととなり、すなわち十分なレベルの個人情報保護が行われていない国への個人情報移転も認められるのではないかとの懸念を作業部会は抱いた。

＜１つ目のリスト＞

A) 適切な協定や条約に基づいた国際的な司法協力

B) 公共医療、衛生のための医療情報の移動

C) 法に適合した銀行におけるお金の移動に伴うもの

D) ウルグアイがメンバーである国際協定の合意

E) 組織犯罪やテロ、麻薬流通に撲滅のための諜報機関間の国際協力

特に、B)、C)、D)は、EUデータ保護指令の第26条1項より、広い範囲で例外を認めているように読むことができると、作業部会は考えた。

これに対し、ウルグアイ政府によって、EUデータ保護指令の第26 条1 項より広くはないと解釈することができるとされた。すなわち、C）は、個人と輸出者の契約における関係に基づく例外規定であると解釈でき、また、B)とD)は、常に重要な公共の福祉、ウルグアイが加盟している重要な国際合意か、又は一般的な重大な公共の福祉が存在する場合のみに適用されると解釈されるとした。これらのことを前提に、作業部会は第三国への情報移転に関して、十分性を満たすと判断するが、上記のウルグアイ政府の回答のような解釈を可能にする規定の導入を推奨するとした。

（e）Habeas Data Action の重要性

前述の通り、LDPD 第38条では、情報主体が、データベースに登録されている自己の情報を参照したいとリクエストをして拒否をされた場合、情報主体が修正、更新、消去する、追加、削除することを管理者にたずね、リクエストに応えない、十分な理由を述べずに期限以内に回答をしない場合に、情報主体は、Habeas data actionを裁判所に起こすことができるとする。また、裁判所の決定、判決に対して、データベース管理者など個人情報を保持する側は、15日以内にその決定、判決に従わなければならない。

作業部会は、このHabeas Data Actionの存在が、ウルグアイの個人情報保護法制において、特に情報主体に対する補償という点で優れているといえると考えている。法的に保護されていても、権利を実現する手段が整備されていなければ意味がない。この点、ウルグアイの個人情報保護法は、URCDPによる監督執行の他に、通常の民事訴訟より迅速に結論が出されるHabeas Data Actionによる保護を備えている点で、侵害行為に対して十分な補償を与えることができると考えられるとされる。

2.3　十分性審査に対応するための法改正等

前述の通り、ウルグアイ政府は2004年に初めて成立した、信用情報分野のみに適用される個人情報保護法（No. 17838）を置き換える法律（LDPD）を2008年に成立させた。これにより、ウルグアイの個人情報保護法は、特定の一分野のみに適用される法からすべての分野に適用される総合的な法となった。政府関係者は、EUデータ保護指令上の十分性を満たすことだけがLDPD 成立の目的ではないとするが、ウルグアイ政府にとって大きなインセンティブであったことは間違いない。

2008年のLaw No.18331（LDPD）の成立には、政府の法案提出から1 年もかからなかった。2007年9月16日に、政府が議会へ法案を提出し、同9月27日に上院へ提出された。そして2008 年5月15日に上院において可決し、2008年７月16日に下院において可決された。その後、2008年8月6日にLaw No.18331（LDPD）は成立した。

この法律は、ウルグアイの法システムの中にEUデータ保護指令の十分性を満たすような個人情報保護法を成立させるような内容となっており、ウルグアイ政府が法案を作成した際には、数々の国際経験豊富な弁護士などが関わった。ウルグアイ特有の法システムの上に、EUデータ保護指令上の十分性を満たす法を新しく作ると云う事で、EUとの制度上の違いなどもあり苦労する点も多かった。たとえば、憲法上、行政機関から独立した機関を作ることは難しく、個人情報保護法の執行において独立性を保つ機関を設立することに苦労したようである。さらに、法律を成立させるため、上下院の議員にこの法律の内容、必要性、重要性について説明することも必要であり、これにも相当な時間な時間がかけられた[24]。

---

24 前掲8

3. 十分性審査の結果

2008年10月20日にウルグアイ政府が欧州委員会に対して、EUデータ保護指令上の十分性審査の依頼をしてから、2010年10月12日に29条作業部会がその十分性についての審査結果について報告書を発行するまで、2年が経過をした。29条作業部会は、ナミュール大学情報・法研究センター（当時）の報告書、作業部会からウルグアイ政府への質問に対する回答、ウルグアイ政府によって提出された資料類を総合的に判断し、EUデータ保護指令上の十分性を満たしていると判断をした。

ただし、この作業部会の判断は、欧州委員会への単なる「意見」に過ぎず、EUデータ保護指令上の十分性をウルグアイの個人情報保護法制度が満たしているかどうかの最終判断は、今後欧州委員会によってなされることとなる。ウルグアイ政府から十分性審査以来から、4年弱が経過しており、作業部会の審査結果の発行からも既に約2年が経過をしている。ウルグアイのEUデータ保護指令上の十分性審査についての欧州委員会の判断がいつなされるか、ウルグアイ政府関係者は気をもんでいるようであった[25]。

2012年秋には、34th International Privacy Commissioner Conference（プライバシーコミッショナー会議）が、ウルグアイのプンタ・デル・エステで開催される予定であり、今年こそは欧州委員会のウルグアイに対する十分性審査の判断がなされるのではないかと、ウルグアイ政府関係者は期待をよせている。

4　十分性審査の影響

4.1　十分性審査の経済的影響

前述の通り、ウルグアイのEUデータ保護指令上の十分性審査に関しては、作業部会の文書が発表されたのみであり、欧州委員会からの正式な審査結果の発表がないため、特に目立った経済的影響はまだウルグアイ国内では出ていない[26]。

しかし、ウルグアイ政府は、ヨーロッパ資本をよびこむこと、特にコールセンターやソフトウェア産業のウルグアイ国内での振興を政策として打ち出しており、The Agency for the Development of electronic Government and Knowledge Based Society（AGESIC）などの政府機関は、国内のITインフラや国民のITリテラシーの向上、個人情報に関する権利に関する理解とその重要性を国民に対して教育をするなどの活動を進めている。

また、個人情報保護法に関する意識やデータベースの登録などの現状に関するインタビューを地元の複数の中小企業に実施したが、登録を行っていない中小企業も見られた。データベースの登録を行っていない企業も、法律上は登録義務があり（罰則はない）、登録が必要であることは認識しているが、登録の手続の煩雑さや理解できない部分などが多すぎて登録までに至っていないようであった。また、登録を行った中小企業の多くは弁護士を雇い、弁護士に作業を委任している形を取っている。中小企業にとっては負担の大きいものとなっている。

---

25 前掲14

26 前掲17

これに対して、AGESIC にあるCitizen’s Office では、登録に関する様々な質問を国民から受け、説明をしている。データベース登録については、前述の通り2009年度はデータベース数：5733、データベース管理者数：3365であったが、2010年度は、新規追加についてデータベース数：3934、データベース管理者数：2185となり、合計で、データベース数：10693、データベース管理者数:6047となった。この数字をみる限り、毎年着実に登録数は増えていることは分かる。

一定のデータベース登録作業をあと1、2 年で終わらせたいところであるとウルグアイ政府はしている[27]。

4.2 十分性審査の法的影響

2008年の法改正以後、データベース登録に関する問い合わせ、苦情等が相次ぎ、それらに関してURCDPは、決定（resolution）か意見（opinion）を発行している。さらに、初のデータベースの停止に関する要請が裁判所に出され、現在その決定待ちである[28]。さらに、Habeas Data Action が裁判所に何件が起こされており、LDPD成立3年が経ち、法の執行について環境が整いつつあるものの、まだまだ整備が足りない部分も目立っている。

27 前掲17

28 前掲14

＜4＞　ニュージーランドにおける個人情報保護制度と EUデータ保護指令の十分性審査

亜細亜大学法学部准教授　加藤　隆之

＜＜構成＞＞

Ⅰ　個人情報保護制度の概要

(1) 個人情報保護制度の概要

ニュージーランドの個人情報保護制度の中心は、1993年5月17日に制定され、その大部分が同年7月1日から施行された、プライバシー法（Privacy Act 1993）と一般にいわれているものである。同法の正式名称は非常に長いため、同法の第1条（短い名称と施行日、Short Title and commencement）では、the Privacy Act 1993として引用できるということが示されている。

なお、同法の正式名称は、「プライバシーの保護と個人データの越境的流通についてのガイドラインに関するOECD理事会勧告（the Recommendation of the Council of the Organisation for Economic Co-operation and Development Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data）に全般的に従い、個人のプライバシーを促進かつ保護すること、とりわけ、

(a) 以下のことに関して、確固たる原則を確立すること
　(ⅰ) 個人に関する情報の、公的又は私的部門の機関による収集、利用又は開示、及び
　(ⅱ) 自己に関する情報であり、かつ、公的又は私的部門の機関によって保有されている情報に対する個人によるアクセス
(b) 個人のプライバシーの侵害に関する苦情を調査するプライバシー・コミッショナーの指名について定めること、及び、
(c) これらの事項に付随する事柄について定めること

を目的とした法律というものである。

このように、ニュージーランドのプライバシー法は、1980年に策定されたいわゆるOECDプライバシー・ガイドラインに依拠していることを、その正式名称において明示している。なお、ニュージーランドは、1973年からOECDの加盟国となっている。

このプライバシー法では、第2条から第133条までの規定が12の章に分けられて配置されており、さらに、8附則が定められている。それぞれの章と附則の内容は次の通りである。

第1章　通則（Preliminary provisions）（第2条ないし第5条）
第2章　情報プライバシー原則（Information privacy principles）（第6条ないし第11条）
第3章　プライバシー・コミッショナー（Privacy Commissioner）（第12条ないし第26条）
第4章　個人情報へのアクセスを拒絶する十分な理由（Good reasons for refusing access to personal information）（第27条ないし第32条）
第5章　個人情報へのアクセス及び収集に関する手続規定（Procedural provisions relating to access to and correction of personal information）（第33条ないし第45条）
第6章　行為規範及び情報プライバシー原則の適用除外（Codes of practice and exemptions from information privacy principles）（第46条ないし第57条）

第7章　個人情報の公的登録（Public register personal information）（第58条ないし第65条）
第8章　苦情（Complaints）（第66条ないし第89条）
第9章　コミッショナーの手続（Proceedings of Commissioner）（第90条ないし第96条）
第10章　情報照合（Information matching）（第97条ないし第109条）
第11章　法執行情報（Law enforcement information）（第110条ないし第114条）
第11A章　ニュージーランド域外への個人情報の移転（Transfer of personal information outside New Zealand）（第114A条ないし第114H条）
第12章　雑則（Miscellaneous provisions）（第115条ないし第133条）

第1附則　コミッショナーに対して適用される規定（Provisions applying in respect of Commissioner）
第2附則　公的登録（Public registers）
第3附則　情報照合規定（Information matching provisions）
第4附則　情報照合規範（Information matching rules）
第5附則　法執行情報（Law enforcement information）
第5A附則　OECDガイドライン第2章で示された国内適用に関する基本原則（Basic principles of national application set out in Part Two of the OECD Guidelines）
第6附則　改正された規定（Enactments amended）
第7附則　削除された規定（Enactments repealed）
第8附則　削除された命令（Orders revoked）

このうち、第11A章は、2010年プライバシー（越境情報、Cross-border Information）改正法（Privacy Amendment Act 2010）によって追加された。この改正は、主として、EU諸国から移転された個人データを保護することを目的として、その越境的再移転を原則的に禁止することなどが盛り込まれており、ニュージーランドが、後にみるEUの十分性審査をパスするためになされたものである。

このプライバシー法の他にも、個別法などによって、ニュージーランドのデータ保護が図られているが、それについては、後にみる29条作業部会の意見書に記されているので、そちらをご参照願いたい。

（2）個人情報保護執行機関の概要

（a）コミッショナー制度

ニュージーランドの個人情報保護執行の制度は、いわゆるコミッショナー制を採用している。この制度については、プライバシー法12条から26条及び第1附則で定められているが、第1附則の多くの定めは、現在では削除されており、わずかに、第1附則4の「恩給又は退職金」及び同附則12の「所得税の免除」に関する規定が残されているに過ぎない。そこで、プライバシー法12条から26条の規定のうち、主要なものをみてみることにする。

プライバシー・コミッショナーは、独人性の機関（a corporation sole）であり（12条(2)(a)）、2004年クラウン・エンティティズ法(Crown Entities Act 2004)7条の目的のためのクラウン・エンティティである（12条(2)(b)）。クラウン・エンティティ（Crown entity）とは、2004年クラウン・エンティティズ法に基づいて設置されるニュージーランドの政府機関であり、特殊な統治下に置かれ、特別な責任と権限を有する地位にある。その特徴は、機関の統治と運営とが分離されている点にある。

このクラウン・エンティティにはいくつかの種類があるが、プライバシー・コミッショナーは、独立（Independent）クラウン・エンティティであり、政府の政策から独立してその職務権限を行使しなければならない（13条(1A)）。また、クラウン・エンティティズ法では、責任のある（responsible）大臣が、クラウン・エンティティにおける国家利益を監視及び管理することを求められているところ（27条及び88条)、プライバシー・コミッショナーについては、法務大臣がこれを担当している。

現在のプライバシー・コミッショナーは、マリエ・シロフ（Marie Shroff）である。彼女は、2003年に5年の任期で選任され、その後、2008年に5年の任期で再任された。さらに、プライバシー法15条では、副コミッショナー（Deputy Commissioner）に関する定めがあり、その法的地位の保障や権限行使の範囲が、基本的にコミッショナーと同一であることが規定されている（15条(2)(3)）。なお、この副コミッショナーの存在は、必要的に求められているものではない（15条(1)）。

さらに、現在、オークランド（Auckland)、法と政策（Legal and Policy)、調査（Investigations）を担当するものとして、3名の准コミッショナー(Assistant Commissioner)がおかれている。このうち、国際問題などを担当しているのが（Auckland担当)、コミッショナー・オフィスが設置された1993年からこの地位にあるブレア・スチュワート（Blair Stewart）氏である。データ保護に関するほとんどの国際会議には、彼が出席している。

（b）コミッショナーの権限

プライバシー・コミッショナーの主な役割・権限として、21の事項が13条で列挙されているが、促進する（promote)、調査する（examine)、相談する（consult)、示唆する（make suggestions)、助言する（provide advice)、報告する（report）などという動詞が使われており、同条の権限は強制力を伴わないものである。

もっとも、コミッショナーは、プライバシー法の他の規定又は他の立法で与えられた権限についても行使することができる（13条(1)(u)）。だが、それらの多くの規定も、コミッショナーに強力な権限

を付与するものとはいえない。たとえば、コミッショナーは、個人のプライバシーが侵害されたと思われる事件について、その苦情を受けて又は自らのイニシャティヴで（69条(2)）、その調査をすることができ、それを解決するため、仲裁者として行動することはできるが（69条(1)）、当事者になすべき行為を命じることはできない。

また、プライバシー・コミッショナーは、1908年宣言的判決法（the Declaratory Judgments Act 1908）に従って、高等裁判所（the High Court）の判決を得たほうが望ましいと考えた場合、その事件を手続コミッショナー（Proceedings Commissioner）に付託することができるが、それを提訴するか否かの判断は、同コミッショナーに委ねられている（20条(1)）。

同様に、プライバシー・コミッショナーが、私人の苦情を受けて調査した結果、人権手続長（Director of Human Rights Proceedings）に対してその事件を付託できるが（77条(2)）、人権裁判所に提訴するか否かの判断は、その長が行うことになっている（77条(3)）。

コミッショナーが、唯一、実質的な権限を有する場合、つまり、強制的に決定できる場合とは、個人情報の開示を私人が求めた際、その相手方が公的機関であれば、原則としてこれに無料で応じることになっているが（35条(1)、36条）、私的機関であれば、合理的な費用を徴収しても良いことになっているところ、その場合の費用が不合理であるため、相当額を裁定するというときである。かつて1度だけ、コミッショナーがこの権限を行使したことがある。

Ⅱ　EUデータ保護指令にもとづく十分性審査

（1）十分性審査の交渉過程

EU諸国では、「個人データの取扱いにかかる個人の保護及び当該データの自由な移動に関する1995年10月24日の欧州議会及び理事会の95/46/EC指令」（Directive 95/46/EC of the European Parliament and of the Council, of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data、以下、「EU データ保護指令」又は単に「EU 指令」という。）25条にもとづいて、個人情報の十分な保護水準（adequate level of protection、以下、十分性などという）を充足していない国々への個人データの移転を禁止している。

そこで、EU諸国からのデータ移転が許される国か否か、すなわち、その国がデータ保護について十分な制度を有しているか否かに関する判断を欧州委員会が行うことになっている。この審査は、まず、EUデータ保護指令29条を根拠として設置される「個人データの取扱いに係る個人の保護に関する作業部会」（一般に、29条作業部会といわれている）においてなされ、そこで形成された意見が欧州委員会で検討されるというプロセスを経ている。

この29 条作業部会では、各国のデータ保護法の具体的な調査について、ナミュール大学（University of Namur）情報・法研究所（Centre de Recherches Informatique et Droit, CRID）（現在の法・情報・社会研究所（Centre de Recherche Information, Droit et Société），以下こちらの表記を用いる）に協力を依頼している。29条作業部会の意見書でもふれられているように、ニュージーランドの十分性審査については、オタゴ大学（University of Otago）法学部のポール・ロス（Paul Roth）教授を中心として書かれた報告書に依拠しているが、ロス教授への依頼は、このナミュール大学の研究所から直接になされた。もっとも、その当時、この法・情報・社会研究所の関係者とロス教授は面識がなかった。

ロス教授の推測によれば、同センターと関係のあったオーストラリアのニューサウスウェールズ大学のグレアム・グリーンリーフ（Graham Greenleaf）教授が、ロス教授を紹介したのではないかということである。ロス教授は、以前、グリーンリーフ教授と共に仕事をしたことがあり、グリーンリーフ教授は、以前にこのセンターから仕事の依頼をされたことがあったため、同センターとつながりがあったという。

そして、ニュージーランドに関する報告書の作成は、このグリーンリーフ教授と、もうひとり、ノルウェーのオスロ大学のリー・ビグレイブ（Lee Bygrave）准教授と共に行うという形であったが、実質的には、ロス教授が1 人で作成したようである。なお、この報告書には、ロス教授の名前のほか、上記2人の教授が共同で（with the collaboration）、ナミュール大学の法・情報・社会研究所が監修し（under the supervision of）、作成したということが記されている。

この報告書の作成にあたって、ロス教授は、ナミュール大学の法・情報・社会研究所とやり取りを行った。その理由は、主に、同研究所が、ロス教授の作成した報告書の内容について、不明瞭な点などの説明を求めたからであるという。なお、ロス教授によれば、29条作業部会や欧州委員会のメンバーと直接やり取りしたことはないという。

こうした欧州委員会によるニュージーランドの個人データ保護制度の実質的な十分性審査は、同国の2010年のプライバシー法改正前後あたりから始められたようであり、ロス教授によれば、4ヶ月程度の期限を与えられ、報告書を作成したという。また、同教授によれば、中立的な専門家の意見のほうが望ましいと考えられているため、大学の教員である自分に依頼がきたのではないかという。

もっとも、重要なことは、この報告書の作成をひとつの判断資料として、29条作業部会が意見を形成し、それを欧州委員会に提出し、また、それをひとつの判断資料として、欧州委員会が最終的な結論を出すというプロセスになっているということである。それゆえ、29条作業部会の意見書にも書かれているように、その意見書を作成する経緯で、同作業部会は、ニュージーランドのプライバシー・コミッショナーや法務省に対しても説明や意見を求めたという。また、ロス教授の報告書はもちろんのこと、29条作業部会の意見も欧州委員会を拘束するものではない。

なお、この十分性審査が開始されるための、正式な申込みというものは存在しないが、非公式には、ニュージーランドの准プライバシー・コミッショナーであるブレア・スチュワート氏が、欧州委員会のデータ保護部署の担当者に十分性の審査をして欲しいという旨を伝えていたという事実は存在する。また、ブレア氏が、様々な国際会議に出席した際に、この担当者に対して、ニュージーランドのプライバシー保護法制を説明し、理解を求めていたという経緯があり、今回のニュージーランドに対する十分性の審査は、同氏の尽力によるところが大きいということは、ニュージーランド国内の専門家からも一般的に認められている。

（2）十分性審査の結果

ニュージーランドのプライバシー保護法制が十分な保護水準を満たしているか否かについて、2011年4月4日、29条作業部会の意見が出された。この意見では、十分性審査の基準からすると、同国の法制度にはいくつかの問題点があることを認めつつも、十分な保護水準を有していると判断している。その概要は、以下のとおりである。

1. 序論及び背景

- 29条作業部会は、2009年に、ニュージーランドのデータ保護立法の十分性について検討するよう要請されたところ、2009年12月の全体会合において、これに関連するサブグループがこの任務を与えられた。
- 欧州委員会は、求めていたニュージーランドの個人データの保護の十分性に関する報告書を提供されたが、それは、ダニーデン（Dunedin）にあるオタゴ大学法学部のロス教授によって書かれたものである。また、その報告書は、ナミュール大学法・情報・社会研究所の監修のもと書かれたものである。
- 本報告書では、1998年7月24日に29条作業部会によって承認された「第三国への個人データ移転・EUデータ保護指令25条及び26条の適用」（Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU Data Protection Directive）と題した作業文書（WP 12）に示された要件に照らして、ニュージーランド法制度の十分性の程度について分析を加えている。

・ また、本報告書では、法規とはいえないルール（non-legal rules）、運用実態、プライバシーに関連して存在する一般的な行政や企業の体質（culture）についても言及している。
・ 当サブグループでは、本報告書のほか、本報告書に関するニュージーランドのデータ保護執行機関及び法務省のコメント、さらに、2010年のプライバシー改正法に関する法務省の文書についても検討対象とした。また、当サブグループは、より詳細な情報の取得や内容の明確化のため、ニュージーランドのコミッショナーに対しても質問した。その結果、当サブグループでは、2010年9月7日に施行されたプライバシー改正法の適用に関するプライバシー・コミッショナーの指針（guidance）などの情報についても検討した。
・ 本意見は、ロス教授の報告書に相当程度依拠しているが、右教授の報告書は、WP12で示された要件にニュージーランドの制度が適合するか否かという観点から、明快に記載されている。

2. ニュージーランドのデータ保護に関する立法

・ ニュージーランドには、成文憲法が存在せず、議会制民主主義をとっている。もっとも、憲法としての意味を有し、より高位の法（higher law）として考えられている規定も多く存在する。こうした規定の中には、1990年ニュージーランド権利章典法（the New Zealand Bill of Rights Act 1990）や1993年人権法（the Human Rights Act 1993）がある。その他にも、プライバシー違反や秘密保持違反に対する判例法上の不法行為の承認を含む、データ保護に関する判例法上の原理やルールが多く存在する。
・ ニュージーランドにおける中心的なデータ保護立法は、1993年のプライバシー法であり、同法は、1980年9月23日の「プライバシー保護と個人データの越境的流通に関するOECDガイドライン」（OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data）に強く影響されている。
・ プライバシー法の46条のもと制定された3つの完全なプライバシーの行為規範（privacy codes of practice）では、とりわけ、健康情報、通信情報、信用報告情報に対して、より厳格な基準が適用されている。また、情報の自由、スパム、一定のプライバシー違反に対する刑罰、刑の消滅、監視カメラ、健康情報の保持、公的記録、差別禁止法などのような領域に関連する法律も存在する。さらに、投票者のプライバシーを保護する1993年選挙法（the Electoral Act 1993）における秘密規定のように、プライバシーに関連する規定がおかれているものがある。
・ プライバシー法は、プライバシー・コミッショナー・オフィスを独立した機関として設立している。プライバシー・コミッショナーは、組織や個人の権利・義務を明確にするために、特定の苦情に関する匿名化された事案を含む、様々なガイドライン、概況報告書、その他の情報を公表している。このことによって、プライバシー原則の実際的な適用に関する指針が提供されている。さらに、人権に関する判例法が、プライバシー法の指針や解釈を提供している。
・ ニュージーランドは、プライバシーの規定を含む情報の自由に関する2つの立法も有している。政府情報法（Official Information Act）は、中央政府及び公的機関が対象であり、1987年の地方公

共団体情報及び会合法（Local Government Official Information and Meetings Act）は、地方政府が対象である。政府情報の公開を求めることができる要件、及び、個人に影響する政府決定がなされた場合にその理由を求める権利について、プライバシー規定が存在する。

- ニュージーランドは独立した司法機関を有し、プライバシー法に関する紛争について、人権審査裁判所（the Human Rights Review Tribunal）に提訴することができる。地方裁判所（the District Court）は、コモン・ロー上と刑事法上の紛争を審理する。これらの双方の裁判所からの上訴審は、高等裁判所（the High Court）である。更なる上訴審は、上訴裁判所（Court of Appeal）、そして、最高裁（Supreme Court）である。
- 名誉毀損、ニューサンス、ハラスメント、悪意による欺もう、侵害、陰謀、故意に害悪を加えること、ネグリジェンス、詐称通用などプライバシーに関する民事的救済が存在する。さらに、刑事法では、権限のない個人情報の利用や開示などのプライバシー違反に関する様々な規定が存在する。
- ニュージーランドは、人口430万人の小国であり、本専門家の報告書では、公正な情報の取扱いが優れたビジネスであると考えられていることが明らかとされている。企業は、このような小さな市場を無視することはできず、問題のあるような取扱いのニュースはすぐに広まる。このことが、ビジネスの遂行にあたって重大な影響を与えている。

3. ニュージーランドの立法によるデータ保護の十分性水準に関する評価

- 当作業部会は、ニュージーランドにおけるデータ保護法の十分性審査の評価が1993年のプライバシー法に焦点をあてている。
- プライバシー法の規定及び個人データの保護に関する判例法は、当作業部会のWP12意見を考慮に入れつつ、本指令の主要な規定と比較される。WP12意見では、データ保護の「内容」（content）に関する原則及び「手続上又は執行上」（procedural/enforcement）の要件の中核となる多くの原則を列挙している。これらを遵守することが、保護が十分であると認められるための最低限の要件と考えられている。

3.1. 立法の適用範囲

- プライバシー法は、いかなる形態の個人情報にも適用される。また、同法は、民主主義社会では一般的である、特定の公共の利益に関するわずかな適用除外があるほか、あらゆる公的団体や私的団体にも適用される。
- 同法は、個人情報を「個人を識別できる情報」（information about an identifiable individual）と定義し、かつ、その個人が生存している場合と定めているが、公式な死亡の記録についても含むものとしている。
- 識別可能性については、個人を識別できる情報そのもののみで判断するのではない。裁判所は、Proceedings Commissioner v. Commissioner of Police [2000] NZAR 277において、「一般人の数名にとって識別しうる」（had the capacity to identify to some members of the public）情報である限り、同法の目的にかなった個人情報であると判示した。

・ プライバシー法は、特定の例外を除いて、あらゆるニュージーランドの機関（agency）に適用される。この機関とは、「法人であるか否か、公的部門であるか私的部門であるか否かにかかわらず、あらゆる自然人や団体であると定義されており、また、疑義を避けるため、省も含む」（any person or body of persons, whether corporate or unincorporate, and whether in the public sector or the private sector; and for the avoidance of doubt, includes a Department）と定義されている。
・ いかなる個人もプライバシー・コミッショナーに苦情を申立てることができ、プライバシー改正法の制定後は、いかなる個人もニュージーランドの機関に対して、情報主体アクセス要請（subject access request）を提出することができるようになった。
・ 適用除外については、特定的に法で明記されている。その中心的なものは、政治上、憲法上、司法上の根拠を有するものである。報道機関は、その報道活動に関連する範囲で、同法の適用を免れる（EU指令第9条と類似している）。
・ よって、本作業部会は、プライバシー法の適用範囲がEU指令に定めたものと類似していると解する。

3.2. 内容に関する原則

・ プライバシー法は、12の情報プライバシー原則を有している。これらの原則は、公的部門の機関が保有する情報へのアクセス権を除いて、裁判所によって直接執行されるものではないが、プライバシー侵害がある場合には、プライバシー・コミッショナーに対して苦情の申立てができる。
・ プライバシー侵害は、これらの原則違反によって、個人に対して害悪（harm）や損失（loss）をもたらした場合に生じるものである。この害悪を基礎としたアプローチについて、プライバシー・コミッショナーは、それが法において広く明確にされており、損失、不利益（detriment）、損害、権利侵害（injury）、また、権利、利益、特権、義務に対する否定的な影響を含むものであることを確認している。
・ 最も重要なことは、プライバシー法が明示的に定める分野では、重大な侮辱、尊厳の重大な低下、感情への重大な損害という形態での精神的損害を含んでいるということである。というのも、プライバシー侵害であるというためには、情報主体のアクセスや訂正原則との関連で害悪や損失を証明する必要がないからである。

基本原則

① **目的適合原則（The purpose limitation principle）**「データは、特定の目的のために処理されなければならず、それゆえ、移転の目的と両立する範囲においてのみ、利用又は更なる流通がなされなければならない。このルールの唯一の許される例外は、本指令第13条に定められている根拠のひとつに基づき、民主的な社会において必要とされるものでなければならない。」

・ 第29条作業部会は、ニュージーランドが、情報プライバシー原則の第1原則（個人情報の収集目的）、第10原則（個人情報の利用に関する制限）、第11原則（個人情報の開示に関する制限）によって、この原則について規定していると考える。

・ 第1原則は、機関が個人情報を収集する際に、その収集目的が合法的なものであり、その機関の機能や活動と関連性があり、その目的にとって必要でなければならないと定めている。第10及び11原則では、個人情報の利用又は開示は、その収集目的又は直接関係する目的に合致しなければならない。
・ 第10原則は、2次的目的に関する例外について定めている。第10(e)原則では、機関が、合理的な根拠に基づき、当該情報が利用される目的が情報収集時の目的と直接関連すると確信する場合、他の目的のためにその情報を利用できると定めている。また、第11(a)原則では、機関が、合理的な根拠に基づき、情報の開示がその取得目的と関連する目的のひとつである又は取得目的と直接関連すると確信する場合、その情報の開示ができると定めている。
・ 個人情報の利用や開示に対する「直接関連した目的」という2次的な根拠は、個人情報が、「移転の目的と両立する範囲においてのみ、利用又は更なる流通がなされなければならない」という目的に適合的である。
・ 第10原則における他の例外のほとんどは、本指令の13条に定める例外に適合的である。本指令が反映されていないものは、処理における正当な目的に関する第7条の規定である。さらに、プライバシー・コミッショナーの処理の承認権限を定める規定がある。これは、予期せぬ状況又はプライバシー法では定めがおかれていない状況に対応するためのものであるが、これらの承認行為の詳細については、プライバシー・コミッショナーの年次報告書に記載されている。
・ よって、本作業部会は、ニュージーランドの制度がこの原則に適合的であると考える。

② **データの質に関する原則及び比例原則 (The data quality and proportionality principle)**「データは、正確でなければならず、必要な場合には、最新のものに更新されなければならない。データは、それが移転又は処理される目的との関係で、適合的であり、関連性があり、それを超えるものであってはならない。」

・ 本作業部会は、データの質に関する原則が、情報プライバシー原則の第7原則（個人情報の収集)、第8原則（利用前に確認すべき個人情報の正確性など)、第9原則（機関による必要以上の個人情報保持の禁止）によって、また、比例原則が第1原則（個人情報の収集目的）によって規定されていると考える。
・ 第8原則では、個人情報を保有する機関は、その情報が利用される予定の目的に照らして、それが正確であり、最新であり、完全であり、関連性を有し、かつ、ミスリーディングなものではないと確認するような（仮に存在するのであれば）合理的な措置をとらずに、その情報を利用してはならないと定めている。
・ 第7(2)原則のもと、機関は、情報が正確であり、最新であり、完全であり、ミスリーディングなものではないことを確保するために、自発的に又は私人からの求めに従い、情報収集を行う義務がある。仮に、私人が求めた訂正に対し、当該機関がそれを躊躇する場合であっても、当該私人は、

訂正の申立てがあったことを既存の情報に付加することを求めることができる。

・ 保持については、第9原則で定められており、そこでは、個人情報を保有する機関は、当該情報が合法的に利用される目的のため必要な機関を超えてその情報を保持してはならないと定めている。
・ 比例性については、第1(a)原則で定められており、そこでは、収集された情報は、その機関の機能や活動に関連していなければならないと定めている。第1(b)原則では、情報収集は、収集目的にとって必要なものでなければならないと定めている。プライバシー・コミッショナーのケースや人権審査裁判所の判例の中には、この関連性の範囲を超えないこと（non-excessive）と必要性の基準に関する解釈について検討したものが存在する。

③ **透明性に関する原則（Principle of transparency）**「データ主体は、そのデータが処理される目的、第三国における処理管理者（controller）の身元（identity）及び公正な処理を確保するために必要なその他の情報に関する情報を提供されなければならない。許される唯一の例外は、本指令11条(2)及び13条に示されている。」

・ 本作業部会は、透明性の要求が、情報プライバシー原則の第2原則（個人情報の情報源）、第3原則（情報主体からの情報収集）、第4原則（個人情報の収集方法）によって規定されていると考える。
・ 第2(1)原則では、機関が個人情報を収集する場合、当該機関は、当該個人から直接情報を収集しなければならないと定めている。第3(1)原則では、データ主体から直接個人情報を収集した場合、その機関は、そのデータ主体がそれを認識することを確保すべく合理的な措置をとらなければならないと定め、次に、当該個人に提供されるべき情報が列挙されている。この列挙事由は、本指令10条に定める要素を含んでおり、かつ、それを超えるものである。
・ プライバシー法では、当該個人以外の情報源から個人情報を収集した場合、本人に対する通知（notification）に関する定めがない。なぜなら、いくつかの例外が存在するものの、同法における原則は、データ主体以外のものから個人情報を収集してはならないというものだからである。
・ 第4原則は、違法な手段又は不公正若しくは当該個人の個人的事柄について不合理な範囲で侵入するという形で、機関が個人情報を収集してはならないと定めており、公正について規定している。
・ この透明性の原則に対するいくつかの例外は、本指令の11条(2)及び13条のそれに合致するが、合致しないものも存在するため、以下検討する。

i）機関が、合理的な根拠に基づき、データ主体から承認があったと確信しているとき

・ 本法は、情報提供に基づく同意（インフォームド・コンセント）ではなく、承認（authorization）という文言を使用している。しかしながら、プライバシー・コミッショナー及び裁判所は、同文言を積極的かつ故意的な形態での明示的同意であると解釈している。あるプライバシー・コミッショナーのケースでは、承認とは明確な行為を求めており（authorisation requires a positive act）、反対しなかったというのは承認ではないと宣言したものがある。

ii）機関が、合理的な根拠に基づき、同原則に従わないことによってデータ主体の利益を侵害しないと確信しているとき

・ この例外は、ニュージーランドで採用されている害悪ベース・アプローチに由来するものであり、本指令7f条で要求されているバランシング・テストに関する精神と似ている。もっとも、ニュージーランドでは、このテストが組織の行為によってもたらされた害悪や損失に関連したものである。注意すべきことは、組織は、当該個人に通知し、その活動に対する承認を得ることを選択するのが当然であるということである。このことは、本法が会話、噂話、内心にある情報を含めたあらゆる個人情報を対象としているニュージーランドでとられているアプローチにと論理的に適合する。このような枠組みのもとでは、本法が実際に機能するためにある程度の柔軟性が必要とされるのであり、害悪ベース・アプローチは、それを達成するためのひとつの手段である。これはヨーロッパのアプローチとは異なるものであるが、個人の権利や自由を侵害することになる可能性は低い。この例外のもとにある個人情報は、依然として、他の情報プライバシー原則のもとにある。

iii）機関が、合理的な根拠に基づき、同原則に従うことが収集目的に反すると確信しているとき

・ 本指令では、これに正確に相応する例外規定はないが、この例外は、13(a)条から(f)条に定める例外規定を反映しており、とりわけ雇用や法執行分野における監視活動に関連して利用される可能性が高い。

iv）プライバシー・コミッショナーによって特別な権限が付与されたとき

・ この例外は、個人データを処理することが望ましい又は必要である場合に、本法でカバーされない予期せぬ状況をカバーするために定められている。コミッショナーは、この権限の付与の結果、個人にもたらされる害悪よりも公共の利益が「相当程度、優越する」(outweighs, to a substantial degree）場合、又は、個人にもたらされる害悪に優越する当該個人にもたらされる明白な利益が存在する場合に限り、この権限を付与する。プライバシー・コミッショナーは、当該個人が個人情報の収集、利用又は開示に関する承認を拒否した場合、権限を付与することはできない。つまり、機関は、まず当該個人の同意を得ようとしなければならない。仮に、個人が同意を拒否した場合、コミッショナーは、権限を付与することはできない。
・ このニュージーランドのアプローチは、ヨーロッパのそれと異なるところがあるが、29条作業部会は、本法が透明性の原則に適合的であると考える。なぜなら、本法の基本原則は、個人情報が、常に、当該個人から直接収集されなければならず、その収集時に目的などを本人に通知しなければならないこととなっているからである。他の情報源から情報収集することや収集時に要求されている通知を行わないことは、この原則の例外と解されている。

④ **セキュリティに関する原則**「情報管理者は、情報処理によって生じる危険に対処するため、適切な

技術的及び組織的措置をとらなければならない。処理の責任者を含む、情報管理者の権限のもとで行動するいかなる者も、その情報管理者の指示に基づかずにデータ処理をしてはならない。」

・ 本作業部会は、第5原則（個人情報の保管及びセキュリティ）がセキュリティ原則で求められる側面をカバーしていると解する。この原則はOECDのセキュリティ安全措置に基づいており、その文言は、本指令の17(1)(2)条に似ている。機関は、情報が処理者に渡される場合、権限なきアクセスや開示を防止するための合理的なあらゆる措置をとらなければならない。情報管理者の指示を超えて情報を利用する処理者は、本法の原則に違反する。プライバシー・コミッショナーの事例ノートでは、とりわけ（銀行情報のような）センシティブな又は私的な情報は、厳格なセキュリティ措置によって保護されなければならないことが示されている。この原則は、データ管理者及びデータ処理者の双方を拘束する。
・ よって、当作業部会は、ニュージーランドの法がセキュリティ原則を遵守していると解する。

⑤ **アクセス、訂正、異議に関する権利**「個人は、自己に関するあらゆるデータを複写し、不正確なデータを訂正する権利を与えられなければならない。一定の場合、当該個人は、自己のデータの処理に反対することができなければならない。これらの権利に対する唯一の例外は、本指令13条に合致していなければならない。」

・ 29条作業部会は、第6原則（個人情報へのアクセス）及び第7原則（個人情報の訂正）において、アクセス権及び訂正権について定められていると解する。かつて、アクセス権及び訂正権は、ニュージーランド市民又は住民、つまり、物理的にニュージーランドに居住する者に限られていた。しかし、2010年プライバシー改正法は、いかなる個人も「情報プライバシー請求」（information privacy requests）ができるようになった。この請求には、機関が個人情報を取得しているか否かの確認の請求、アクセスの請求、訂正の請求が含まれている。公的部門の機関に関しては、アクセス権は直接的な法的権利であり、プライバシー・コミッショナーを経ずに、その権利行使のため裁判所に訴えることができる。
・ アクセス権の例外のほとんどは、本指令13条の規定と合致している。国家安全保障や防衛について定め、本指令で明示されていない諸外国や国際組織との国際関係についても定めている。しかし、本作業部会は、このことが十分性の水準に影響を与えるとは考えていない。

・ 13(g)条に相当する様々な例外規定のほか、本法には、本指令に定めのない管理上の例外規定も存在する。これらについては以下検討する。
・ 請求が取るに足らない若しくは濫用的なもの、または、請求された情報が瑣末なものである（the request is frivolous or vexatious, or the information requested is trivial）場合には、アクセスを拒否することができる。この規定は、アクセス権の濫用を防止する目的のものであり、欧州の情

報の自由に関する制定法で認められる規定と似ている。

・ 情報が容易に抽出できない（not readily retrievable）場合、情報が存在しない若しくは発見できない（does not exist or cannot be found）場合、又は、情報が他の機関によって保有されている若しくは他の機関の機能や活動により密接に関係していると考える根拠が存在しないが、その情報が当該機関によって保有されていない場合という3つの実際的な管理上の例外が存在する。第3番目の例では、機関がアクセスの請求を他の関連する機関へ移転する義務を負う。

・ 情報処理に反対する権利に関しては、ニュージーランドで直接的な規定はない。しかし、第3原則（情報主体からの情報収集）では、個人がその通知をされた際に処理に反対することができる。第3(1)(e)(f)原則では、個人が以下の通知を受けることになっている。

(e) 法によって若しくはそのもとで、情報収集が承認若しくは要求されていた場合
（ｉ） 特定の法によって若しくはそのもとで、情報収集が承認若しくは要求されていること
（ii） その個人による情報提供が自発的なものか義務的なものであるのかについて
(f) 仮に要求されている情報の全部又は一部が提供されなかった場合、（仮にあるとすれば）その個人にもたらされる結果

・ プライバシー・コミッショナーが、個人の異議申立の機会が否定された場合に関する苦情を調査した2つの事件が報告されている。
・ WP12では、一定の状況においてのみ、個人は異議申立の権利を有するべきであり、その権利はニュージーランドへ移転する前にEUにあるEUデータのために存在しなければならないと記されている。
・ よって、本作業部会は、ニュージーランドの法が、アクセス、訂正、異議申立の権利に関する原則に合致するものと解する。

⑥ **第三国への移転に関する制限**「第三国から他国への個人データの継続的な移転は、後者も十分な保護水準（adequate level of protection）を確保している場合に限り許容される。これに対する唯一の例外は、本指令26条第1文に定められている。」

・ ニュージーランドの法律はOECDガイドラインを基礎としているため、個人データが第三国へ移転された場合の保護に関する特定の規定をおいていない。本法10条は、ニュージーランドの機関が第三国で情報を保管している場合にも適用され、このことによってニュージーランド域外に存在する情報に対しても本法の原則が適用される。この規定は、ニュージーランドの機関のために行動する第三国に存在する情報処理者によって保有されている情報にも適用される。
・ 第11原則の開示制限は、第三国に存在する機関に対する場合も含まれている。この規定の例外は、

本指令26条の修正規定と概ね一致する。情報が第三国にある場合でさえ、ニュージーランドの機関は、その第三国で行われた利用や開示から生じる害悪や損失に対して依然として責任を負う。それゆえ、その危険を最小化し、適切な安全策をとることは、それら機関の利益となる。

・ 2010年のプライバシー改正法は、越境移転に関する苦情を関係機関に付託し、例外的な場合には、海外から移転された個人情報の更なる移転を禁止する権限をプライバシー・コミッショナーに付与する制度を導入した。プライバシー・コミッショナーは、この規定がいかに機能し、そのオフィスがこの新しい権限をいかに行使する意向であるのかについてガイドラインを作成している。コミッショナーは、移転禁止通知（transfer prohibition notice）を発布することができ、その違反行為に対しては、10,000ドル以下の罰金を伴う刑事訴追が可能である。

・ 通知の発布には、コミッショナーが、以下の点を認めなければならない。

(a) 当該個人情報が他の国家から受領したものであり、その情報がプライバシー法と同等の安全措置を定める法が制定されていない第三国へ移転されること

(b) 当該移転が、OECDガイドラインに定められている、国内適用に関する基本原則の違反となる可能性の高いこと

・ コミッショナーは、移転を禁止する裁量権限を行使する際、次の点を考慮しなければならない。

(a) 114条で定められている事項（人権やプライバシーに匹敵する他の社会的利益、ニュージーランドが負う国際的な義務、情報プライバシー原則、公的記録プライバシー原則）

(b) 予定されている個人情報の移転が、個人へ影響を与える又は与える可能性が高いか否か

(c) ニュージーランドと他の国々との情報の自由な流通を促進することが望ましいか否か

(d) 越境的データ流通に関連する国際的なガイドラインの存在や発展（OECDガイドライン及びEU指令を含む）

・ 実効的な越境執行に関して、制定法及びコミッショナーのガイドラインは、欧州のデータ保護執行機関が移転について、プライバシー・コミッショナーへ注意を促した場合、コミッショナーはその事案を優先的に扱い、必要な場合、禁止通知を発布することができるということを明示している。また、コミッショナーは、移転禁止権限行使を正当化できる可能性のある移転措置を、事前に発見するための調査権限を有している。

・ データ保護執行機関を通じて以外の方法によって、コミッショナーが、ニュージーランド域外への移転を認識する方法が明らかとされていないため、本作業部会は、これらの規定の実際的な実効性に関して多少の疑念を有している。しかしながら、法における変化やコミッショナーの指針は、更なる移転に関する十分性確保の必要性について、移転禁止命令という罰則と共に、産業界に注意を喚起している。現実には、ニュージーランドは欧州から地理的にも遠いこと、経済の規模やその性質に鑑みると、ニュージーランドの機関が、EUを源とする相当量のデータを第三国へ移転すると

いう経済的利益を有している可能性は低い。
・ 本作業部会は、ニュージーランドの法律が第三国移転の原則に完全に合致しているとはいえないものの、大きな欠点があり、十分性の認定の妨げになるとは考えない。

付加的原則

・ WP12文書では、特定の情報類型の処理に適用されるべき一定の原則に言及しており、とりわけ次のようなものがある。

① **センシティブ情報**「センシティブな（sensitive）データ類型（これらは本指令8条に列挙されている）の場合には、データ処理に際して個人からの明示的な同意を要求するなど、付加的な安全措置がとられなければならない。

・ プライバシー法は、本指令と同様の形でセンシティブ・データと非センシティブ・データとを区別していない。本法は、あらゆるデータを潜在的にセンシティブであり、同一水準の保護下にあると解している。本指令8条に列挙されたデータ類型は、1993年人権法によってカバーされている。ニュージーランドのデータ保護法制は、EU指令に先駆けたものであり、OECDガイドラインで示されたアプローチに従ったものである。とりわけ、このことは、目的ベースのアプローチであることを意味している。というのも、情報が収集された目的が、第10原則及び11原則のもと、その利用及び開示の情報を決定するからである。さらに、本法の第11章及び第5附則が、公的部門の機関による法執行情報へのアクセスを詳細に規制している。
・ また、ニュージーランドは、特に注意が求められる一定の情報類型を別に扱う（earmarking）ことによって、OECDガイドラインに従っている。このことは、特定の拘束的実務規範を通じてなされている。健康情報は、プライバシー法よりも厳格な規定を含む1994年健康情報プライバシー規範（Health Information Privacy Code 1994）によって定められている。その他の規範として、2003年電子通信情報プライバシー規範（Telecommunications Information Privacy Code 2003）及び2004年クレジット報告プライバシー規範（Credit Reporting Privacy Code 2004）がある。後者は、クレジットの報告者が、クレジット報告の目的でクレジット情報以外の個人情報を収集してはならないと定めている。
・ 個人が、重大な侮辱を受けた、尊厳を失わされた又は感情を傷つけられた場合、プライバシー法ではその救済措置がある。精神的損害は、その違反行為によって、架空の合理的な人間ではなく、当該個人が実際にいかに傷ついたかということに依拠して判断される。
・ 人権法に含まれる差別規制の規定に加えて、他の立法においても、一定のデータ類型に対する保護について定めている。たとえば、1961年刑法（Crimes Act 1961）では、通信傍受（interception）の禁止を含む、個人のプライバシーに反する行為を犯罪としている。また、1974年興信所及び安

全措置法（Private Investigators and Security Guards Act 1974）では、民間の調査員が個人の事前の同意なく写真撮影又は映像として記録することを禁止し、そのような証拠が民事訴訟で許容されないことを定めている。いくつかの欧州諸国のように、情報の自由に関する立法は、他人の事柄の開示を含み、優越する公共の利益がない場合の開示を防止する規定を含んでいる。本指令8条に明記された範囲を超えたデータ類型の違法な取扱いによる権利侵害が認められたという情報が、プライバシー法の下で多く存在する。

・ よって、本作業部会は、ニュージーランドがセンシティブ・データ原則に合致していると解する。

② **ダイレクト・マーケティング**「ダイレクト・マーケティング目的でデータ移転がなされる場合、個人は、いつでも、その目的での自己データの利用を拒否することができるべきである。」

・ この原則を検討するにあたって、本作業部会は、ニュージーランドが小国であり、ダイレクト・マーケティング行為が他の国ほど発達していないという点を認める。プライバシー法では、ダイレクト・マーケティングに関する特定の規定をおいていないが、情報プライバシー原則は、この分野にも同様に適用される。このことは、個人情報が当該個人から直接取得されなければならないという一般原則を含むものである。よって、EUからニュージーランドへ個人情報が移転され、ニュージーランドでダイレクト・マーケティングのために利用されるということは、あったとしても稀であろう。
・ さらに、電子通信情報プライバシー規範は、収集できる情報の種類及びその利用に制限を加えている。この規範は、ネットワーク管理者、電子通信サービス・プロバイダー、住所録出版者、尋問機関（enquiry agencies)、インターネット・サービス・プロバイダー、契約に基づいて他の機関へのコール・センター・サービスを行うコール・センター、携帯電話小売業者に適用される。また、この規範は、ダイレクト・マーケティングのための電子通信情報の利用を個人の同意のある場合に限り許容している。
・ 2007年迷惑メール防止法（Unsolicited Electronic Messages Act 2007）は、スパムに対処し、営利的な性質を有するEメール、インスタント・メッセージ、SMS、MMSについて定めている。同法は、メッセージが同意ある者にのみに送られ、送信停止の装置を含まなければならないという点で、2002/58/EC指令と同様の機能を有している。
・ コミッショナーは、ダイレクト・マーケティングに関する多くの苦情に対処し、成功を収めている。
・ 自主規制に関しては、ニュージーランド・マーケティング協会（New Zealand Marketing Association）及び広告基準団体（Advertizing Standards Authority）が、個人のプライバシーを保護するようその会員を積極的に教育している。両者とも行動規範を作成し、市場におけるすべての取引者がその原則に従うよう求めている。また、無料の苦情処理サービスも行っている。
・ さらに、ニュージーランド・マーケティング協会は、迷惑電話やメールに関する無料のメール禁止・電話禁止サービス（Do Not Mail and Do Not Call Service）を運営している。もっとも、そのリ

ストの最新版のコピーは、その会員にのみ送付されている。

・ ニュージーランドにおけるダイレクト・マーケティングの取扱いの枠組みは、欧州のそれと異なるが、実際には、個人がオプト・アウトする方法がいくつか存在する。法的にオプト・アウトする権利がない場合であっても、個人はプライバシー・コミッショナーへ苦情を申立てることができ、同コミッショナーは、この分野における法の強化の必要性を認識している。現実には、EUに在住している個人が、ニュージーランドからダイレクト・マーケティングを送られる可能性は相当低い。それゆえ、本作業部会は、ニュージーランドの法律がダイレクト・マーケティング原則を完全に満たしていないものの、大きな欠点があり、十分性の認定の妨げになるとは考えない。

③ **自働個人決定（Automatic individual decision）**「移転目的が、本指令15条の意味における自働決定である場合、当事者は、この決定の背後にある理由を知る権利を有しなければならない。また、その者の正当な利益を保護するためのその他の措置がとられなければならない。」

・ 専門家の報告書では、ニュージーランドにおいて、自働決定が一般的ではなくこの慣行を妨げる様々なルールのあることを明らかにしている。政府情報の照合プログラムが自働決定を許している場合もあるが、プライバシー法の第10章（情報照合）及び第4附則（情報照合ルール）によって規制されている。コミッショナーは、これらのプログラムの監視機能を有している。このルールでは、自働決定の結果の妥当性に対する個人の調査やその個人に対する潜在的な行為に関する情報提供を含む、個人への安全措置が求められている。
・ 個人は、原則として、個人情報が収集される際にその目的を知らされる必要がある（第3原則）。個人情報の正確性は、その利用以前に確保される必要がある（第8原則）。個人情報は、原則として、収集目的を超えて利用されてはならない（第10原則）。自働決定をなす機関は、その行為が個人に損害を与えた場合、法的責任を負う危険性がある。
・ 公的部門に関しては、政府情報法又は地方公共団体情報及び会合法のもとで、すべての個人が、その個人に影響を与える決定の理由へアクセスする制定法上の権利を有することになっている。もっとも、この規定は、ニュージーランド市民又は住民、つまり、物理的にニュージーランドに居住する者に限り適用される。
・ よって、本作業部会は、ニュージーランドの法が自働個人決定の原則に十分合致していると解する。

3.3. 手続的又は執行上の仕組み

WP12では、データ保護の手続的制度の基本的な目的を確認し、これを基礎として、第三国において利用されている様々な司法及び非司法の手続上の仕組みを判断することを求めている。

この点に関するデータ保護制度の目的は、以下のとおりである。

— ルールに対する十分な水準の遵守に資すること

— データ主体が権利行使する際の援助を提供すること

— ルールが遵守されなかったことに伴い侵害された当事者に対する適切な救済を提供すること

a）ルールの遵守について良好な水準を確保すること「優れた制度とは、データ管理者が自らの義務について、また、データ主体が自らの権利やその行使方法について、高程度で認識していることと一般的に特徴づけられる。

効果的かつ抑止的な（dissuasive）制裁の存在は、公権力、検閲者、独立したデータ保護機関の役人による直接的な認証の制度がそうであるように、そのルールの尊重を確保するうえで重要な役割を果たす。」

データ管理者及び個人における認識

- プライバシー法は、1993年から施行され、あらゆる公的部門又は私的部門の機関が、少なくとも1人のプライバシー官（privacy officer）をおくことが求められている。彼らは、たとえば、アクセス請求を処理すること、調査に際してプライバシー・コミッショナーと活動すること、その他、彼らの機関がプライバシー法を遵守するよう確保することなど、情報プライバシー原則を彼らの機関が遵守するよう奨励する責務を負う。国内では、プライバシー官ネットワークがいくつか存在し、会合を開いている。
- プライバシー・コミッショナー・オフィスでは、そのウェブサイト上に、選別された調査に関する匿名の事例ノートを含む、広範囲の情報を載せており、4半期にニュース・レターを発行している。また、このオフィスでは、プライバシー官などに対して、通常の研修やワーク・ショップを国内各地で行っており、毎年開催されているアジア太平洋プライバシー認知週間（Asia-Pacific Privacy Awareness week）にも関与している。さらに、このオフィスでは、数年に1回、コミッショナーの効果及び認知度を測るための調査を行っている。

プライバシー・コミッショナー・オフィス

- プライバシー・コミッショナーは、クラウン・エンティティ（Crown entity）であり、その役割、義務、権限において、独立して活動することが求められている。プライバシー・コミッショナーは、責任のある大臣（responsible minister）、すなわち法務大臣の推薦に基づいて、総督（Governor-General、ニュージーランドの国家代表）によって指名される。総督による指名は、ごく少数の重要な制定法上の指名のためのとりわけ高い水準の手続である。コミッショナーとしてその指名を推薦するため

には、その者が適切な知識、技術及び経験をもつという意見を責任ある大臣が有しなければならない。

- プライバシー法13条(1A)は、コミッショナーが定められた役割や義務を果たし、権限を行使する際に、これを独立して行わなければならないことを定めている。
- プライバシー・コミッショナー・オフィスは、その年に行われた承認されている（authorized）公権力の情報照合プログラム及びその法令遵守の評価などの内容について、毎年、議会に報告することが求められている。
- プライバシー・コミッショナーは、苦情を調査し、これを解決しようと試み、自発的に調査を実施するなど、オンブズマンとしての役割を果たす。また、同コミッショナーは、教育、法令遵守の監視、政策的助言の付与、質問回答、首相への報告など、本法で定められた役割を有する。本法第9章では、プライバシー・コミッショナーに対して、宣誓による証人を尋問し、その証人に対して、平日20日以内に情報及び書類を提供するよう求める権限を付与している。
- コミッショナーは、プライバシー法以外の法律のもとでも、権限、役割、義務を有している（たとえば、健康法（Health Act)、社会保障法（Social Security Act)、家庭内暴力法（Domestic Violence Act)、旅券法（Passport Act）などにおいて)。
- プライバシー・コミッショナー・オフィスは、データ保護及びプライバシー・コミッショナーの国際会議（International Conference of Data Protection and Privacy Commissioners)、APEC越境プライバシー執行協定（APEC Cross-border Privacy Enforcement Arrangement)、及び、国際プライバシー執行ネットワークのメンバーとして認められている。

執行手段及び制裁

- 本法の第9章（コミッショナーの手続）では、プライバシー・コミッショナーの調査手続及びその権限が定められている。この調査に協力しない又は妨害した場合には、2,000ドル以下の罰金に処せられる。
- プライバシー・コミッショナーによって紛争が解決されず、その紛争の申立人又は人権手続長(Director of Human Rights Proceedings）が更なる審理を求めた場合、その紛争を人権審査裁判所に付託することができる。紛争の申立人は、コミッショナーが拒否した場合であっても、その手続長に対して、人権審理裁判所への付託を求めることができる。この裁判所では、損害賠償、禁止的又は命令的な差止めの性質を有する性質の命令を含む、あらゆる救済方法が用意されている。メディアは、このような決定を報道する傾向にあり、小国であるニュージーランドでは、否定的な報道が抑止的な効果を有する。
- 手続長が申立人を代理しないと決定し、また、よくあるように、申立人に代理人がついていないにもかかわらず、プライバシー法における重要な原則が争われている場合、コミッショナーが、通常その訴訟を代理する。人権手続長は、出廷又は意見を述べる権限を有しているが、この権限を行使しなかった場合、コミッショナーがそのような権限を有すると定められている。人権手続長は、複

数の個人のために集団訴訟を提起する権限も有するが、これまでのところ、この権限が行使されたことはない。

- 既に指摘したように、2010年プライバシー（越境情報）改正法では、ニュージーランドから十分性の水準を充足しない第三国への移転に関連し、移転禁止通知を発出できる権限をコミッショナーに対して付与した。
- このようなことに鑑みると、本作業部会は、ニュージーランド法制が、データ保護に関するルールの遵守において良好な水準を確保するための必要な要素を有していると解する。

b）データ主体の権利行使に対して援助を提供すること「個人は、迅速かつ効果的に、また、法外な費用がかからずに、自己の権利を行使できなければならない。そのために、苦情を独立して調査することを認める、何らかの制度的な仕組みがなければならない。」

- 既に指摘したように、プライバシー・コミッショナーは、そのオフィスの役割、義務、権限との関係で、独立して行動することが求められている。このオフィスでは、ここ数年間、苦情をより効果的に処理し、未処理件数を減らすための仕組みをおいている。コミッショナーは、苦情処理の際、事実関係を確認し、紛争当事者の合意を導く目的で、強制的に当事者を召喚することができる。オフィスは、紛争解決のため、独立した内部の仲裁手続をとることがある。機関は、プライバシー法で特に定められていない救済手段を内容とする、合意に基づく取決めをすることができる。
- 個人が、コミッショナーや裁判でその代理人となっている人権手続長に対する不服を申立てる際に、費用はかからない。不服申立人は、無料かつ代理人なしで、人権審査裁判所へ出訴することができる。しかし、その不服申立人が敗訴した場合、勝訴した当事者の現実的かつ合理的な訴訟費用を負担しなければならない。
- 本作業部会は、ニュージーランド法制が個人を支援するための十分な仕組みを有すると解する。

c）ルールが遵守されなかったことに伴い侵害を受けた当事者に対する適切な救済措置を提供すること「これは、支払われるべき損害賠償を認め、妥当な場合には制裁を課すことのできる独立した司法機関又は仲裁機関の制度を含まねばならないという点で重要な要素である。」

- プライバシーに関するほとんどの苦情は、コミッショナーによって解決されてしまうか又は調査後の手続へと進まない。人権審理裁判所へ出訴される事件は、1年に20件ほどあり、その数は一定している。
- 人権審理裁判所は、確認判決（declarations）、差止命令（restraining orders）を出す権限や事件の細部を排除又は個別の審理の一部若しくは全部を有効と扱う権限を有する。また、右裁判所は、最高200,000ドルまでの損害賠償を認めることができる。プライバシー法下における現在までの最高額は、侮辱、尊厳の喪失及び被害者の感情を害したということに対する40,000ドルの支払いで

ある。損害賠償の請求額が200,000ドルを超えている場合には、右裁判所は、損害賠償額を裁定するため、その事件を高等裁判所へ付託できる。

- 人権審理裁判所は、アクセスの要請が拒否された場合に情報を開示するというような、機関によって求められる行為を明らかにするための命令を出すことができる。また、右裁判所は、本法で定められていないその他の救済措置の命令を出すこともできる。
- 仮に事実認定に関して問題がある場合、高等裁判所へ上訴できる。また、高等裁判所の判決は、法律問題に限り上訴裁判所へ上訴できる。高等裁判所が上訴の許可を与えなかった場合、上訴裁判所が、右裁判所にとって法律の争点を議論する価値が十分にあると判断すれば、この許可を与えることができる。同様の手続が最高裁判所への上訴でも履践されている。
- よって、本作業部会は、ニュージーランド法が適切な救済措置を提供していると解する。

4. 評価結果

- ニュージーランドのデータ保護及びプライバシー法は、EU指令より先んじて制定され、概ねOECDガイドラインに従ったものであるが、EUからの個人データの移転についての十分性に関する懸念に対処するため、近年いくつかの改正を行っている。いくつかの懸念が依然として存在するが、本作業部会は、十分性が本指令と同等ということを意味しないということを想起すべきであると考える。それゆえ、本作業部会は、ニュージーランドが十分な保護水準を確保していると解する。
- しかしながら、本作業部会は、ニュージーランドが現行法制度における弱点に対処するため、必要な措置をとることを勧める。とりわけ、本作業部会は、プライバシー・コミッショナーがダイレクト・マーケティングの分野で法を強化することを引き続き求めること、及び、ニュージーランドから十分性評価を受けていない第三国への移転の効果的監視を確保することを勧める。また、本作業部会は、プライバシー・コミッショナーが移転禁止通知を発出するか否かを決定する際に、OECDガイドラインとEU指令のほか、関連する欧州委員会の決定及び29条作業部会の指針をも考慮に入れるよう求める。
- また、本作業部会は、本委員会でなされるあらゆる決定の一部として、ニュージーランドにおけるデータ保護の進展、および、WP12文書や本文書で言及されているデータ保護原則のプライバシー・コミッショナー・オフィスによる適用方法を詳細に追跡していくことを強調しておきたい。

ブリュッセルに於いて、2011年4月4日

本作業部会長を代表して

部会座長

ヤコブ・コーンスタン

（Jacob KOHNSTAMM）

Ⅲ　ロー・コミッション報告書

(1)　プライバシーの法制度に関する報告書

この欧州委員会のニュージーランドの法制度に対する十分性審査と、時期的には平行して、同国の国内では、ロー・コミッションによるプライバシーの法制度全般に対する調査・検討が行われていた。ロー・コミッションは、プライバシー・コミッショナーと同様に、独立クラウン・エンティティであるが、独任性ではなく、合議制の機関である。現在、5名のロー・コミッショナーが任命されている。このうち、プライバシー制度に関する報告書作成を先導したのが、コミッショナーのひとりであるジョン・バロウ教授（Professor John Burrows）である。

ロー・コミッションでは、2008年1月に第1段階（stage 1）の報告書として、「プライバシー：概念と問題点」と題した調査報告書をまとめた。そこでは、概念的な枠組みに関するプライバシーの問題点を概観し、他の段階の報告書におけるより詳細な検討のための問題点を確認するのに役立つものであったが、具体的な勧告は示されていない。

第2段階（stage 2）の報告書では、「公的登録」について検討されており、これは、2008年2月に議会へ提出されたが、そこでは、1993年の公的記録に関する規定は検討対象とされていない。また、2010年2月に公にした第3段階（stage 3）の報告書では、「プライバシー、処罰及び救済」と題して、プライバシー侵害における民事法、刑事法などの妥当性について検討されているが、プライバシー法に焦点をあてたものではなかった。

そこで、このプロジェクトの最終段階である第4段階（stage 4）の報告書では、個人情報の収集、セキュリティ、利用、及び、プライバシー・コミッショナーの設置に関する1993年プライバシー法に焦点をあてて検討を行い、これを2011年6月30日に発表した。

ロー・コミッションでは、これら第2段階から第4段階での報告書において、プライバシー制度の改正すべき点や新たに導入すべき制度について、具体的な勧告を示している。そして、政府側として法務省は、これらの勧告に対して、それに従うか否かについての回答をしなければならないことになっており、2010年8月には、第3段階に対する予備的回答がなされたが、ほとんどの勧告に対する回答については、第4段階の報告書が出るまで延期している。また、この回答がなされるまでの期間は、通常6ヶ月とされているが、第4段階の報告書を含めたこれら一連の報告書の勧告内容が膨大であることから、法務省は1年くらいの期間が必要であるとしており、未だ回答がなされていない。

とはいえ、近い将来、遅くとも今年の9月までには、第2段階から第4段階の報告書で示されているロー・コミッションの勧告のすべてに関して、それに従うのか否かについて回答がなされるものと考えられている。なお、政府に回答義務はあるが、ロー・コミッションの勧告に従うべき義務はない。

（2）1993年プライバシー法に関する勧告の概要

① 報告書の概要

ロー・コミッションがなした勧告のうち、第3段階の報告書におけるそれも、私的な個人による監視装置の利用に関する法律の大きな改正に関するものであり、重要であるが、とりわけ、重要な勧告は、プライバシー法全般において改正すべき点を検討している第4段階で示されているものであるため、これについてみてみることにする。

この第4段階の報告書における各章の項目は、次の通りである。

(本章)

- 第1章　はじめに
- 第2章　範囲、アプローチ、重要概念
- 第3章　プライバシー原則
- 第4章　例外と適用除外
- 第5章　プライバシー・コミッショナーの役割、機能及び権限
- 第6章　苦情、執行及び救済
- 第7章　データ保護違反通知
- 第8章　他の法律との交錯
- 第9章　法執行
- 第10章　科学技術
- 第11章　個人情報の越境的移転
- 第12章　その他の問題点

(補遺)

- 補遺1　情報共有
- 補遺2　情報照合
- 補遺3　情報プライバシー原則
- 補遺4　意見提出者のリスト

既に指摘したように、ニュージーランドでは、主に欧州委員会から十分性審査において、十分な保護レベルを有するとの判断を得るため、2010年にプライバシー法の改正をしたばかりであるが、その本体である1993年プライバシー法は、既にロー・コミッションの報告書発表の段階では、18年を経過しており、プライバシーのような進化・進展の早い領域では、同法の改正が必要な段階に来ていると解されている。

② 勧告内容

ロー・コミッションでは、プライバシー法が改正されるべき点について、136もの勧告を出している。これらの勧告内容は、29条作業部会がニュージーランドのプライバシー法制度に対する十分性の審査

の際に指摘した問題点と重複している部分もあるが、その多くは、ロー・コミッションが独自に、法制度として改正すべきと考えているものである。ここでは、ロー・コミッションが出した勧告のうち、その主な内容について、同コミッションが行った2011年8月2日の報道発表をもとに、以下詳述することにする。

プライバシー・コミッショナーのための新しい権限 (New tools for the Privacy Commissioner)

現在、プライバシー法の執行は、苦情が申立てられたことを契機として行われている。個人はプライバシー・コミッショナーに苦情を申立てることができるが、コミッショナーが行使できる権限は限られている。コミッショナーが、イニシャティヴをとり、効果的にプライバシー法の遵守を確保できるようにするため、次の2つの重要な権限をコミッショナーに与えるよう勧告する。

- コミッショナーは、プライバシー法違反の機関に対して、その法を遵守する措置を執るよう命じる通知を出すことができる。その機関は、人権審査裁判所に上訴する権利を有する。このような権限付与は、多くの海外のコミッショナー権限と歩調を合わせるものである。
- コミッショナーは、十分な理由がある場合、個人情報の処理に関する機関の実務や制度の監査（audit）を求めることができる。

データ保護違反通知（Data breach notification）

データ保護違反通知によって、重大な害悪の危険を減少させる措置を人々がとりうる場合、又は、データ保護違反が重大な場合には、この通知を義務的とする（mandatory）ことを勧告する。

苦情処理手続の簡素化（Streamlining the complaints process）

プライバシー法の苦情処理手続は、不必要に複雑であるように思われる。現在のところ、プライバシー・コミッショナーは、苦情に対して、何ら拘束のある決定を出す権限はない。人権審査裁判所（the Human Rights Review Tribunal）のみが、これをなしうる。和解によって解決できないプライバシーの苦情に対して、以下の改正をすべきことを勧告する。

- プライバシー・コミッショナーが、人権審査裁判所で訴訟を追行できるか否かについて決定できるべきである。現在のところ、この決定は、人権手続長（the Director of Human Rights Proceedings）によってなされており、手続が複雑化している。
- 「アクセス」に関する苦情については、コミッショナーが拘束力ある決定をなすことができるべきである。個人が機関のアクセス拒否をコミッショナーに申立てた場合、コミッショナーは、その機関がその情報を開示すべきか否かについて決定できるようにすべきである。なお、その機関は、上訴する権利を有する。

さらに、代理による苦情申立てに関する規定をより明確にするよう勧告する。代理による苦情申立ては、たとえば、より匿名性を保持できること、多くの人々に影響する制度上の欠陥に対して、より効果的に対処できることなど、個人による苦情申立てよりも数多くの利点を有している。

情報共有（Information Sharing）

政府機関相互の情報共有は、より効果的なサービスの提供や違法行為の発見などの観点から望ましいことも多いが、プライバシー法がその障害となっている場合もある。それゆえ、これを認める新たなメカニズムが必要である。

政府間の情報共有が認められるためには、プライバシー・コミッショナーを含めた議論を重ね、最終的には、プライバシー法で明記された基準を遵守すべきことを定め、内閣によって承認されるべきである。すべての共有プログラムは、その機関のウェブサイト及びプライバシー法の附則で列記すべきである。また、議会及びプライバシー・コミッショナーによる審査に服するべきであろう。

越境的に移転される個人情報のより良い保護 (Better protection for personal information sent overseas)

ニュージーランドの機関が、その機関のために保管又は処理してもらうことを目的として、越境的に個人情報を移転する場合、その機関がその情報に対する全面的な責任を依然として負担すべきである。他方、機関が、その機関のために保管又は処理してもらうことを目的としてではなく、越境的に個人情報を開示する場合、その機関は、その情報が受け入れられるプライバシー基準に服するよう合理的な措置をとらなければならない。また、プライバシー法において、コミッショナーに対して諸外国のプライバシー保護執行機関と協力する権限を付与すべきである。

不快感を与えるオンライン上の情報に対するより良い保護 (Better protection against offensive online publication)

インターネットの力は、他人の私的な情報をオンライン上に載せることで濫用されうる。プライバシー法は、オンライン情報にも適用されるが、いくつかの広範な例外が現在存在する。だが、その情報がとりわけ不快感を与える場合には、その例外規定が適用されるべきではない。

たとえば、以前の恋人の裸の写真をその同意なしにネット上に載せるというケースがある。現在のところ、その者は、個人の私的又は家庭内での事柄と関連して収集又は保有している者であり、プライバシー法が適用されないと主張することが可能である。しかし、情報の収集、利用又は開示が「高度に不快感を与える」場合には、この適用除外規定は適用されるべきではない。さらに、このような情報は、「公に入手可能な情報」であるが、その更なる利用や開示を禁止するよう改正されるべきである。

健康と安全（Health and safety）

現行法では、機関が、健康や安全に対する「深刻かつ差し迫った脅威を防止又は軽減させる」ため

に個人情報を利用又は開示することを認めているが、差し迫ったという文言を削除すべきである。脅威が深刻であっても、差し迫っていないという理由で、機関が情報を開示できないという場合が現実に存在している。また、新たに、健康や安全を理由として、本人以外からの情報収集を認める例外規定をおくべきである。そして、本人がその情報へのアクセスを求めた場合、機関は、健康又は安全にとって深刻な危険が存在することを理由としてその情報開示を拒むことができるようにすべきである。

電話禁止登録とダイレクト・マーケティング (Do Not Call register and direct marketing)

現在、マーケティング協会によって行われている電話禁止登録については、立法的な根拠を与え、業者はすべからく人々の意向を尊重すべきよう義務付けるべきであるが、これは、プライバシー法というよりは、むしろ、消費者法を通じてなされるべきである。もっとも、オプト・アウトの規定をプライバシー法におく必要が将来的に生じる可能性があるだろう。また、オンライン・マーケティングに関するプライバシー問題やこれに対する諸外国の反応にも注視し、この分野における更なる措置の必要性を注視していくべきである。さらに、産業界は、自働決定に対するマーケティングに関する現行のプライバシー保護規範の妥当性について検討すべきである。

(3) 個人情報の越境的移転に関する勧告の概要

このように、ロー・コミッションは、プライバシー法の全般に渡り、勧告を行ったが、次に、個人情報の越境的移転に関する部分の勧告について詳しくみてみることにする。なぜなら、仮に今後、日本が欧州委員会の十分性審査を受ける事態となった場合には、この点が新たな立法をせざるを得ない事項のうちのひとつとなると考えられるからである。

ニュージーランドにおける2010年のプライバシー法の改正は、とりわけ、欧州委員会の十分性審査にパスすることを目的として、個人情報の越境的移転の法規制を厳格にする方向で行われたが、ロー・コミッションは、この改正法に対して、一定の評価をしつつも、更なる法改正が必要であると指摘している。

つまり、欧州委員会の審査をパスするため、EU諸国の人々の個人情報を保護する制度を導入している点は評価するが、ニュージーランド在住の自国民の個人情報を保護する制度としては不十分であるとロー・コミッションでは考えている。

確かに、2010年の改正法では、個人情報の処理などのため、諸外国からニュージーランドの機関へその情報が委託された場合に、それを越境的に移転して再委託することを原則として禁止している。そのため、もともとニュージーランド国内にある個人情報については、この規定の保護が及ばないのである。

とはいえ、この点は、EU諸国及びその国民の保護のために行動する欧州委員会による審査においては影響がない点であり、それゆえ、2010年の改正法が、29条作業部会の十分性審査において、肯定的

に受け止められ、このような改正法も十分なレベルの保護を有していると判断されたのではないかと考えられる。

ロー・コミッションによる個人情報の越境的移転に関する勧告の概要については、次の通りである。

問題の本質

2010年のプライバシー法の改正は、ニュージーランドが海外から個人情報の移転を受け、それを更に不十分なプライバシー保護水準の諸外国へ移転する場合に、プライバシー・コミッショナーが介入できる権限を与えている。この改正の主要な利点は、EUの審査における十分性の地位を獲得したことである。このことによって、データ処理、クラウド・コンピューティング、金融、コール・センターなどの分野において、新たな取引の機会が生じるものと考えられる。

だが、プライバシーの観点からすると、この改正は、ニュージーランドの取引先である諸外国の市民の利益に資するものであるが、ニュージーランドを起源とし、不十分なプライバシー水準の場所への越境的データ移転の懸念に対処しようとするものではない。

改正へのアプローチ

この問題について、5人の意見提出者（submitters）は、現状のままで良いとしているが、9人の意見提出者は、より一層の保護が必要であると解している。国税庁（Inland Revenue)、社会発展省（the Ministry of Social Development)、関税局（the Customs Service）の3つの政府機関は、一定の状況下で越境的情報共有を認める定めをおいている。

2010年6月21日～22日にウェリントンで開催された、インターネット・ニュージーランド主催によるフォーラムでは、プライバシー法10(3)条の射程範囲が広範に及ぶ可能性があることについて懸念が示された。同規定では、外国法（アメリカの愛国者法(USA PATRIOT Act)のような）の要求に従って個人情報が開示される場合、アカウンタビリティの適用が除外されることについて定められている。

そこで、ロー・コミッションでは次のように考える。機関の越境的個人情報の移転は、「個人情報が処理や保管のため、ニュージーランドの委託者の機関として働き、その委託に関連する目的以外の目的で個人情報を利用することを禁止されている海外の機関へ、個人情報を委託する場合」と「海外の機関自身の利用のため、個人情報を開示する場合」とに分けられる。

委託(outsourcing)から開示(disclosure)まで様々な取引の類型を考慮することは､我々の分析にとって極めて重要な要素である。結論的には、機関が、越境的個人情報の移転に関する責任を負うべきであるが、アカウンタビリティのレベルは、移転の類型によって異なると解する。

まず、個人情報を海外へ委託する機関のアカウンタビリティの水準は、相対的に高いと解すべきである。個人情報を委託すると決定した機関は、その個人情報の取扱いに対して、依然として完全に責任を負うと解することが適切である。個人情報を信用して組織に預けた人々が、委託されるという決定によって、不利益を被ることがあってはならないからである。このことは、委託の取決めにおいて、個人情報がニュージーランドのプライバシー法と同レベルのプライバシー水準に服することが確保さ

れていなければならないということを意味する。このようなアカウンタビリティの水準が、プライバシー法によっても企図されていると思うが、現行法によってこの点が明確化されるべきだと考える。

次に、海外の機関への開示に関しては、アカウンタビリティの水準は異なり、やや限定的となると解する。開示する機関は、プライバシー原則を遵守すべき責任を負う。第11原則に従わない開示は、違法である。さらに、機関は、海外で開示された情報が、受け入れられるプライバシー水準に服するように合理的な措置をとるように求められるべきである。このような規定を新たにプライバシー法へ導入すべきである。われわれが好ましいと考えるモデルは、アカウンタビリティと越境的データ移転統制との両輪モデルであり、かつ、それが情報の自由な越境的流通を不当に妨げない程度であるというものである。

我々は、新しいアカウンタビリティの原則を本法に導入するという手法について、プライバシー・コミッショナー・オフィスから賛同を得たものの、意見書からは、明示的な賛同が得られなかった。このことから､新しい原則に対して十分な支持が得られていないと考えている。そこで､アカウンタビリティを強化するため、本法に対してなされ得るその他の改正点について検討した。

現行プライバシー法は、ニュージーランド域外に移転される個人情報を保護し、機関が責任を負うような方向へ向けられているが、それらの規定は、散在している。我々は、それらの規定を最新のものとし、明瞭化し、本法のひとつの章にまとめることが必要であると考えている。本法を越境的データ移転に適用するためには、機関は3(4)条、10条、第5(b)原則、第10原則、第11原則及び新しい11A章を参照しなければならず、これは極めて複雑である。

また、我々は、これらの規定によっても、現在よりアカウンタビリティを促進できると考えている。そこで、指摘した2つの区別に従って、以下検討する。

海外への個人情報の委託

機関が、自らのために個人情報の処理を行うため、海外の機関にその処理を委託する場合、仮に、その個人情報が、他の機関によって海外へ移転されたとしても、プライバシー法は、その委託機関が、依然としてその個人情報を保有している（それゆえ､それに対する責任を有している）と解している（プライバシー法3(4)条、10(1)(2)条)。

現行法は、クラウドコンピューティングの契約上の取決めや委託取決めの越境的な側面の複雑性や洗練化（sophistication）を予期していなかった。ひとつの問題として、3(4)条は、委託された個人情報に対する機関の責任について定めているが（その個人情報が依然として委託機関によって保有されていると解することによって)、それと同時に、アカウンタビリティからサービス提供者を免責するという機能も有しているということがあげられる。この免責の条件は、サービス提供者が、自身の目的のために、その情報を利用又は開示しないというものである。だが、この規定の解釈が意味するところは、サービス提供者によるこの条件の不遵守が、その個人情報がもはや委託機関によって保有されていないという結果となり、それゆえ、その機関のアカウンタビリティの水準が下落するということである。我々の見解では、3(4)条におけるこれら2側面の機能は、別々に扱われるべきである。この

条件は、委託業者のアカウンタビリティを制限するのではなく、アカウンタビリティからサービス提供者を免責することのみに作用すべきである。

3(4)条の解釈は、国内の文脈において取り立てて困難を生じさせない。なぜなら、委託業者もサービス提供者もニュージーランドのプライバシー法に服するからである。しかし、サービス提供者が国外の機関である場合には、その法の適用に問題が生じる。それゆえ、越境的委託においては、委託機関がその取決めによって個人情報の取扱いに対する責任を依然として負うと解することについて、合理的な根拠を強化すべきである。

我々は、2000年カナダ個人情報法保護及び電子文書に関する法（the Canadian Personal Information Protection and Electronic Document Act 2000 (PIPEDA)）の規定に沿った、委託目的での移転に関して、より広範囲に及ぶアカウンタビリティの規定を導入することを勧める。

「機関は、処理のために第三者に移転した情報を含む、その保有又は管理（custody）する個人情報に対して責任を負う。」

この新しい規定は、安全な管理や処理など、3(4)条の射程に現在含まれている機関の機能を捕捉すべきである。

この種の規定の採用は、プライバシー法3(4)条の現在のアプローチを簡潔化及び明瞭化するものである。この規定は、機関が、委託取決め下におけるサービス提供者のいかなるプライバシー違反に対しても責任を負うということを意味している。

この種の厳格なアカウンタビリティの要求は、機関の自己保身のためには、個人データの海外委託の前に、危険評価（risk assessment）を行い、その回避のために必要な措置をとる必要があることを意味している。PIPEDAでは、第三者によって情報処理がなされる場合には契約上又は他の手段を利用することとし、そのことを制定法で明示している。だが、我々は、ニュージーランドのプライバシー法の枠組みでは、この種の要求は、制定法上の要求というよりは、指針の問題とする方が適切であると解する。

プライバシー・コミッショナーは、委託されたデータに対して、プライバシー法と同等の水準の保護を確保するために、契約又は他の手段を利用して委託機関がいかに自らを保護できるかに関する指針を提供すべきである。

このような指針の一部として、プライバシー・コミッショナーは、そのオフィスがニュージーランドのプライバシー法と同等のプライバシー水準を有する法域のリストを保有することが機関にとって役立つか否かについて検討することができる。このことによって、特定の委託取決めが承認されるものではないが、機関が委託目的で法域を選択する際に、何らかの確信を提供するであろう。ある法域が、このプライバシー・コミッショナーのリストに含まれていない場合には、契約規定のような更なる措置が必要であるということを示唆しているだろう。

我々は、諸外国の法で要求された行為について免責する、10(3)条で定められている例外については、プライバシー保護が減じられる可能性があるものの、これを削除することは困難であると解する。

外国法の要求に関する重大な懸念がある場合には、それは、プライバシー・コミッショナーが発言

する又は指針を出すことのできる問題である。このような指針は、一般国民や機関に対して、その要求の存在がプライバシー保護に影響を与える可能性のあることを知らせることができるだろう。また、個人データを収集する際に外国法の要求を通知することは、その影響に関する懸念を減少させることに役立つだろう。

このアカウンタビリティの形態は、越境的委託取決めにのみ関するものであり、その他の個人情報の越境的移転に関するものではない。個人情報の海外への開示については、異なるアカウンタビリティの水準を勧める。

越境的移転に関するすべての規定は、プライバシー法のひとつの章としておかれることが望ましいと考える。国内における委託取決めに関するアカウンタビリティについて定めをおくことも、検討する必要があるだろう（現在は3(4)条である）。我々は、このことは、越境的委託取決めに対するアカウンタビリティの定めとパラレルに、国内的取決めに適用される規定を定めることによって、それと整合的になすことを勧める。

（勧告）

R107 「プライバシー法は、越境的委託に関する取決めに関する完全なアカウンタビリティの明示的な規定を含むべきである。それは、以下のような趣旨の、2000年カナダ個人情報保護及び電子文書に関する法律の規定の前半部分に依拠すべきである。」

・機関は、保管、管理、処理のために第三者に移転した情報を含む、その保有する個人情報に対して責任を負う。

R108 「プライバシー・コミッショナーは、機関が個人情報を海外へ委託する前に行う危険評価の実施に関する指針を、その機関のために定めるべきである。」

R109 「プライバシー法は、R107で勧告した規定とパラレルの規定として、国内における委託の取決めに関する完全なアカウンタビリティについて、明示的な規定を含むべきである。」

他の海外への開示

ニュージーランドの機関が、その保有する個人情報を海外の機関自身の利用やその更なる開示のために、その機関へ開示する場合、プライバシー法は、その最初の開示は第11原則を遵守することを求めているが、その情報が海外へ移転された後、それが十分な保護を受けるかについて考慮することをその開示する機関に求めていない。

我々は、海外に個人情報を開示する際に、その開示機関が、受け入れられる（acceptable）プライバシー水準にその情報が服することを確保するのに必要な合理的措置をとるという明文を定めることを勧める。

この要求される合理的措置を確認するため、機関は、開示前にその移転先でいかなる法制度が適用されるか検討することを通じて、危険評価をしなければならない。さもなければ、その機関は（契約上の取決めなどを通じて)、プライバシー保護を確保するため、必要な措置を採らなければならない。

「受け入れられるプライバシー水準」とは、ニュージーランドのプライバシー法と必ずしも同一である必要はない。それは、OECDの国内適法に関する基本原則、EU指令、APECプライバシー・フレームワーク原則のような承認された国際的措置を基礎とするものを含む。プライバシー・コミッショナーは、国際的なプライバシーの枠組みが受け入れられるものであることを承認する権限を与えられるべきである。

プライバシー・コミッショナーは、機関が海外へ個人情報を開示する前の危険評価の実施及び契約その他の手段の利用について、指針を提供すべきである。このような指針の一部として、プライバシー・コミッショナーは、承認された国際的プライバシーの枠組みのいずれかに基づいて、受け入れられるプライバシーの水準を有している法域のリストをそのオフィスが保持することが、機関にとって役に立つのかについて検討しうる。

このアカウンタビリティ規定に対する例外は、以下に対する開示を含むべきである。

- 当該情報主体に対する場合
- 法の遵守への違反を回避する必要のある場合
- 公衆の健康や公共の安全、個人の生命や健康に対する重大な危険を回避する必要のある場合

また、外国法によって求められた場合の開示に関する10(3)条の例外は、そのまま適用されるべきである。さらに、7条は、特別法によって、特定の機関による個人情報の海外への開示に関する追加的例外を定めうることを認めていると解されよう。

これに加えて、本、雑誌、新聞、公的な登録などのように、「公に入手可能な刊行物」（publicly available publication）においてなされている情報の開示は、適用除外とする必要がある。なぜなら、新しいアカウンタビリティ規定の目的は、広く世界への開示を制限するものではなく、機関相互における個人情報に焦点をあてた（targeted）開示を保護するものだからである。

海外への開示に関する個人の同意を例外とすることについては、これを勧めない。個人にとって容易に理解可能で、かつ、機関にとって効率的であり対費用効果の優れた形で、意味のある同意を獲得することは困難であろうと考えられるからである。同意は、依然として、第11(d)原則のもと開示禁止の例外であろうが、機関は、その情報開示後も、受け入れられるプライバシー水準の適用を確保するアカウンタビリティの遵守が求められる。

海外への開示に関する推奨するアプローチは､アカウンタビリティ・モデル（個人情報を送る機関に、適切な措置をとる義務を課す）に依拠しているが、それはデータ移転統制モデル（同等なデータ保護水準を有しない国へのデータ移転を禁止する）をも含むものである。この両モデルを採用することによって、それぞれの純粋型の利点と欠点の間のバランスをとることができると考える。

第1に、情報の自由な流通に望ましくない制限となる可能性があるため、情報受領者によるプライバシー違反に対して、海外へ個人情報を開示した機関に対して、厳格責任を課さないような規定をおくべきである。

第2に、ニュージーランド・プライバシー原則の最低限度の基準としてのデータ移転統制モデルは、過度に負担が大きく、不当に制限的なものとなりかねない。このアプローチが海外への開示の一般的な条件として正当化されるとは考えられない。とはいえ、ニュージーランドからの情報移転について、プライバシー保護のために、何らかの最低基準は必要である。それゆえ、ニュージーランドのプライバシー原則と同一ではないが、国際的に受け入れられたプライバシー価値に基づくいかなるプライバシーの枠組みであっても、個人情報の海外への開示の目的にとって受け入れられるものと考えられるべきである。柔軟な基準を設定する利点は、国際的な措置に従い、プライバシー法を施行している国々への越境的データ移転に関する障壁を課すことを避けることにある。

一般的なプライバシーの枠組みが存在しない場合であっても、機関同士が契約による適切な枠組みを設定していればその開示は可能である。また、以下で議論するように、越境的プライバシー・ルールを通して、海外への開示を促進することも可能である。

アカウンタビリティとデータ移転統制モデルを両用しており、提案されている越境的開示のアカウンタビリティに関するオーストラリアのアプローチについて検討した。しかし、このアカウンタビリティ措置には多くの例外が定められている点が批判されており、我々も、そうではなく、より照準を定めた（targeted）規定をおくことが望ましいと考えている。

R110 「海外における個人情報の開示について、新たなアカウンタビリティの措置が導入されなければならない（委託取決めの場合を除く）。開示を行う機関は、開示される情報が、受け入れられるプライバシー水準に服していることを確保するために、合理的に必要と思われる手続をとることが求められる。」

R111 「この新たな措置に対する例外は、次の開示を含むべきである。」

- 当該個人に対する場合
- 法の不遵守を回避するために必要な場合
- 公衆衛生や安全、又は、個人の生命や健康に対する重大な侵害を回避するために必要な場合
- 一般に入手可能な刊行物においてなされる場合

「7条及び10(3)条（又はこれらの条文の代替条文）は、この新たな措置に対して適用されるべきである。」

R112 「プライバシー・コミッショナーは、特定の海外のプライバシー制度が受け入れられるプライバシー水準を定めたものであると承認する権限を有するべきである。プライバシー・コミッショナー・オフィスは、このような制度のリストをウェブサイト上で開示すべきである。」

R113 「プライバシー・コミッショナーは、ニュージーランドの機関のために、個人情報を海外で開示する前の危険評価の実施、および、受け入れられるプライバシー水準の適用を確保するための契約その他の手段の利用に関する指針を定めるべきである。」

データ移転禁止権限

2010年プライバシー（越境情報）改正法は、プライバシー・コミッショナーに個人情報の移転を阻止又はそれに条件を課す権限を付与した。しかし、この権限は、他の国からニュージーランドへ個人情報が送られ、さらに第三国へ送られる場合にのみ行使される。

もともとニュージーランドに存在する情報の越境的移転の場合には、アカウンタビリティ・モデルが現段階では最善である。この場合、機関は、海外の情報受領者が適切なプライバシー水準を遵守するよう確保する義務を負うが、それに従わない場合やその水準が保たれていない地域へ移転される場合もある。

こうした場合に、プライバシー・コミッショナーのデータ移転禁止権限が行使できるように2010年の改正法を拡大できないかとも考えられる。一見すると、それは論理的にみえる。だが、その必要はないと考える。第6章において、コミッショナーが、コンプライアンス通知（compliance notice）を出す一般的な権限を有するべきことを勧告した。仮に、第11原則に反して若しくは我々が提案する相当の注意を払うべき（due diligence）義務に違反して、情報が海外へ送られる予定である若しくはまさに送られようとしている場合、当該機関は、プライバシー法の要求を遵守していないことになるだろう。その場合、コミッショナーがコンプライアンス通知を出すことが妥当である。2010年に導入された規定に対して改正が必要であるということを示唆しているのではない。もっとも、コンプライアンス通知に関する我々の勧告が受け入れられないのであれば、コミッショナーのデータ禁止通知権限の拡大に関する検討がなされるべきである。

越境的執行協力

プライバシー・コミッショナー・オフィスで特に優先順位の高い事項は、プライバシー執行機関相互の協力体制を創設し、それを促進することである。そのオフィスでは、以下の2つのイニシャティヴで重要な役割を担っているという。

- プライバシー法の執行における国際協力の枠組みを確立することを目的とするAPEC越境プライバシー執行協定取決め（the APEC Cross-border Privacy Enforcement Arrangement）
- OECD作業部会の協力で設立されたグローバル・プライバシー執行ネットワーク（the Global Privacy Enforcement Network（GPEN））

2010年のプライバシー改正法72C条では、プライバシー・コミッショナーが、特定の紛争について海外のプライバシー執行機関と相談、または、その紛争を適切なそれらの機関に付託することを認めている。

争点報告書（issues paper）で示したように、プライバシー・コミッショナーが、次のような更なる執行協力の措置が採れるよう新たな規定を定めるべきである。

- プライバシー法違反の可能性のある行為に関して、諸外国のプライバシー執行機関と関連する情報を共有すること
- 諸外国のプライバシー法違反の可能性のある行為に関して、諸外国のプライバシー執行機関へ援助

を提供すること
- コミッショナーと諸外国のカウンターパートとの間で、援助を求めること及びこれを与えること
- 他の公権力や利害関係者と共に援助を提供すること
- 越境的プライバシーに関する紛争を処理するため、司法手続権限を付与すること

カナダでは、近年、プライバシー・コミッショナーに対して、その海外のカウンターパートやプライバシー違反に責任のある個人又は組織と情報を共有することを認める新たな規定を最近PIPEDAに追加した。このような情報は、諸外国のプライバシー違反に関する調査と関連している限り、共有し得るものとなっているのである。

R114 「プライバシー法は、以下のように改正されるべきである。」
- プライバシー・コミッショナーが、プライバシー法に反する可能性のある行為に関して、諸外国のプライバシー執行機関と関連情報を共有できるようにすること
- プライバシー・コミッショナーが、諸外国のプライバシー法に反する可能性のある行為に関して、諸外国の執行機関に援助を提供できるようにすること
- プライバシー・コミッショナーと諸外国のカウンターパートとの間で援助を求めること及びこれを与えることに関する定めをおくこと
- 越境的プライバシー紛争を処理するため、訴訟権限を付与すること

プライバシー・コミッショナー・オフィスは、APECの越境的プライバシー・ルール（cross-border privacy rules, CBPR）の制度に対して、現時点で確固たる判断を加えることが難しいと考えているようである。そこで、プライバシー・コミッショナーは、越境プライバシールールの承認を許容するようにプライバシー法を改正することが、最も柔軟なアプローチであると考えている。というのも、中期的には、このイニシャティヴがより大きな重要性を帯びてくる可能性があるからである。

この規定は、ニュージーランドがCBPR制度の採用へコミットするように求めるものではないが、その制度が有益であると判断されれば、将来的にその制度への加入する機会を創造することになる。

プライバシー・コミッショナーは、CBPR制度への参加又はアカウンタビリティ機関の設立に関する将来的な権限を与えられるべきである。

R115 「プライバシー法は、ニュージーランドにおける越境的プライバシー・ルールの将来的採用を許容する規定を含むべきである。この規定は、議会における命令（Order in Council）によって決定されたときから施行される。」

＜5＞　インド[1]

森・濱田松本法律事務所　弁護士　高谷　知佐子・小山　洋平

一　個人情報保護制度の概要

Ⅰ　個人情報保護関係法令

1　概要

インドにおける個人情報の保護に関する法令は、Information Technology Act, 2000（以下「IT法」という。）第43A条、及び、同条に基づき、インド通信情報技術省情報技術局[2]が制定した、Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011（以下「2011年個人情報保護規則」という。）である。これらの法令により保護される個人情報は、後述するとおり、コンピュータに保管されているものに限られ、2012年4月1日現在、文書等に記録されたものを含む個人情報全般を保護の対象とした法令は、存在しない。

2　IT法第43A条

IT法には、当初、個人情報の保護に関する規定は設けられていなかった。同法は、所定の要件を満たす電磁的記録に書面と同等の効力を認める規定（同法第4条)、電子署名に法的効力を認める規定（同第5条)、電子署名を認証する機関に関する規定（同第21条以下)、サイバー犯罪に関する規定（第43条及び第65条以下）等を内容とするものであり、日常社会において様々な情報が広く電磁的記録により作成・保存されるようになっている現状に対応することを目的としたものと考えられる。

その後、IT法改正法（Information Technology (Amendment) Act, 2008）により、新たに第43A条が規定され、個人情報の保護に関する規定が新設された。同条[3]は、センシティブ個人情報（“sensitive

---

1　本報告書の内容は、以下の機関に対するインタビュー及び任意に訪問した現地法律事務所の弁護士との議論並びにEuropean Commission のウェブサイト(http://ec.europa.eu/index_en.htm）において公表されている情報に依拠するものであり、その真実性についての検証は逐一行っていない。

* Data Security Council of India

* Government of India, Ministry of Communication & IT, Department of Information Technology

2　Department of Electronics and Information Technology, Ministry of Communications and Information Technology

3　Section 43A: “Where a body corporate, possessing, dealing or handling any sensitive personal information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected. ”

personal data or information”）をコンピュータ内において保管し又は取り扱う法人等（“body corporate”）[4]が、合理的安全措置（“reasonable security practices and procedures”）を実行・維持（“implementing and maintaining”）することを怠ったことにより他人に損害等を与えた場合における、当該他人に対する補償義務を規定したものである。これらの要素のうち、「センシティブ個人情報」や「合理的安全措置」の具体的内容は、政府が別途規定する規則に委ねられていたが、それに相当する規則が制定されていなかったため、IT法第43A条の規定にもかかわらず、必ずしも多くの法人等が合理的安全措置を講じるには至っていなかった。

3　2011年個人情報保護規則の概要

IT法第43A条の規定に基づき[5]、インド通信情報技術省情報技術局は、2011年個人情報保護規則を制定し、同規則は、2011年4月11日から効力を生じた。同規則は、全部で8条からなる規則で、具体的には、表題（第1条）、定義（第2条）、センシティブ個人情報の定義（第3条）、プライバシーポリシーの作成・公表義務（第4条）、センシティブ個人情報を取得する際の本人からの同意取得義務（第5条）、センシティブ個人情報の第三者への開示についての本人からの同意取得義務（第6条）、センシティブ個人情報を移転する場合の移転先における保護体制及び移転の必要性の条件（第7条）、合理的安全措置の内容（第8条）をその内容とする。

4　2011年8月通達

2011年個人情報保護規則は、当初から、その適用範囲や文言が曖昧であるとして、明確化を求める声が強かった。特に、センシティブ個人情報を取得する際や第三者に開示する際の本人からの同意取得義務（同規則第5条及び第6条）が、当該情報を本人から直接取得する法人等に限らず、インドでBPO事業などアウトソーシング事業を営む法人等にも適用される可能性が存したため、NASSCOM[6]などを中心とする業界団体から、業務に著しい支障を与えるとして強い反発が提起されていた。

そこで、2011年8月、かかる点も含む同規則の内容を明確化するための通達（Press Note）（以下「2011年8月通達」という。）が公表された。

4　原文では、“body corporate means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities”と定義される。

5　2011年個人情報保護規則の柱書きでは、“In exercise of the powers conferred by clause (ob) of subsection (2) of section 87 read with section 43A of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules”と記載されている。

6　National Association of Software and Services Companies(http://www.nasscom.org/)。インドのIT業界及びBPO業界を代表する団体。

Ⅱ　2011 年個人情報保護規則の適用範囲

1　保護の対象となる個人情報の種類

IT法第43A条は、前述のとおり、センシティブ個人情報をコンピュータ内において保管し又は取り扱う法人等の責任を規定している。同条において、センシティブ個人情報の具体的内容は下位規則に委ねられたものの、文言上は、センシティブ個人情報をその保護対象としている。

これに対して、2011年個人情報保護規則は、個人情報（“personal information”）の定義（同規則第2条(1)項(i)号）とセンシティブ個人情報（同第3条）の定義を区別している。そのうえで、文言上は、プライバシーポリシーの作成・公表義務（同第4条）は、センシティブ個人情報を含む個人情報を保有する法人等に適用されると解される一方で、情報の取得及び第三者への開示の際に本人からの同意取得を義務付ける規定（同第5条及び第6条）は、センシティブ個人情報のみに適用されるように読める。

この点、理屈上は、IT法第43A条がセンシティブ個人情報のみを対象としたものであり、2011年個人情報保護規則は同条に依拠するものである以上、同規則が規定すべき対象はセンシティブ個人情報のみに限定されるべきであり、同規則の全ての規定はセンシティブ個人情報のみに適用されると解する余地もある。

しかしながら、2011年個人情報保護規則が本来規定すべき範囲を超えている可能性がありつつも、一般的には、同規則の文言上、センシティブ個人情報に該当しない個人情報にも適用されると解される条文（第4条）については、センシティブ個人情報に限らず適用されると解されているようである。

2　義務の対象となる法人等

2011年8月通達は、2011年個人情報保護規則が適用される法人等の範囲に関して、“These rules are … applicable to the body corporate or any person located within India.”と規定する。かかる文言のうち、“body corporate within India”の内容は比較的明確であるが、“any person located within India”については、当該“person”が個人情報を収集する側を指すのか、個人情報を提供する側を指すのか必ずしも明らかではなく、仮に後者に解すると、理屈上は、インドに所在する個人の情報を保有する海外の法人等にも同規則が適用されることになる。

3　その他

IT法第43A条は、センシティブ個人情報をコンピュータに保管等する者に適用される旨規定するので、同法に基づき規定された2011年個人情報保護規則もコンピュータに個人情報を保管等する法人等を適用対象とし、例えば、紙媒体によってのみ個人情報を保管する法人等には適用されないと解されている。他方で、同規則上、適用対象を一定数以上の個人情報を保有する法人等に限定していないため、

理屈上は、コンピュータ内に1 つでも個人情報を保有している場合は、2011 年個人情報保護規則の適用を免れないことになる[7]。

Ⅲ　2011 年個人情報保護規則の内容

1　個人情報とセンシティブ個人情報

個人情報とは、自然人に関する情報であって、直接又は間接に、法人等にとって入手可能か又は入手可能性のある情報と相まって、当該個人を特定できる情報をいう（2011 年個人情報保護規則第２条(l)項(i)号）。

センシティブ個人情報は、同規則第３条に列挙されており、具体的には以下の情報を指す。

① パスワード
② 銀行口座、クレジットカード、デビットカードその他の支払方法の詳細などの金融情報
③ 肉体的状態、生理的状態、精神衛生状態
④ 性的指向
⑤ 診療記録・診療履歴
⑥ 生体情報
⑦ サービス提供のため、法人等に対して提供された上記各項目に関する詳細情報
⑧ 法人等が加工目的で取得した上記各項目に掲げる情報で、適法な契約等に基づいて保管又は加工されたもの

2　プライバシーポリシーの作成・公表義務

センシティブ個人情報を含む個人情報を収集、受領、保有、保管、又は取扱う法人等は、以下の内容を含むプライバシーポリシーを作成の上、個人情報の提供者に分かるようにし、かつ、当該法人等のウェブサイトに掲載しなければならない（同規則第４条）。

① 明確かつ参照容易な、個人情報の取扱い及び方針に関する記述
② 個人情報及び第３条に基づき収集されるセンシティブ個人情報の類型
③ 当該情報の収集及び使用の目的
④ 第６条に規定するセンシティブ個人情報を含む情報の開示に関する事項
⑤ 第８条に規定する合理的安全措置に関する事項

なお、第４条のプライバシーポリシーの作成・公表義務は、BPO 事業などアウトソーシング事業を営む業者にも適用されると解されている。

7　例えば、会社等が保有する従業員の個人情報についても、2011 年個人情報保護規則上の個人情報の定義からは除外されていないため、理屈上は、かなり広い範囲の法人等に同規則が適用されることになる。

3　個人情報を取得する際の義務

（1）取得時の本人からの使用目的に関する同意

法人等がセンシティブ個人情報を取得する場合、かかる取得に先立ち、当該情報の提供者から使用目的について同意を得なければならない。かかる同意を得る手段として、2011年個人情報保護規則においては、書面、ファクシミリ又は電子メールによるべき旨が規定されているが（同規則第5条1項)、2011年8月通達により、電気通信（“electronic communication”）の方法が含まれることが明らかにされた。その具体的な内容は不明であるが、例えば、インターネットの画面上で同意を取得する態様が想定されると思われる。

（2）取得の制限

法人等は、本人から使用目的についての同意を取得すれば無限定にセンシティブ個人情報を取得できるわけではなく、①当該情報が当該法人等の機能又は活動に関連する適法な目的のために取得され、かつ、②当該目的のために当該情報の取得が必要と考えられる場合にのみ、取得できるとされている（同条第2項)。

（3）取得の際に講じるべき措置

個人からセンシティブ個人情報を取得する法人等は、取得に際して、当該個人に以下の事項を認識させるために、状況に応じた合理的措置を講じる義務を負う（同条第3項)。

① 当該情報が取得されている事実
② 当該情報の取得目的
③ 当該情報の受領予定者
④ 当該情報を収集する機関及び当該情報を保有する機関の名称及び住所

（4）保持期間の制限

センシティブ個人情報を保有する法人等は、当該情報の適法な使用目的に必要な期間その他法律上要求される期間を超えて保持してはならない（同条第4項)。

（5）目的の制限

取得された情報は、当該情報が取得された目的のためにのみ使用することができる（同条第5項)。

（6）取得した情報の正確性の確保

法人等は、情報提供者の要求に応じて、提供した情報の内容を検討する機会を提供すると共に、個人情報及びセンシティブ個人情報が正確でないか又は不完全であることが判明した場合、実現可能な

範囲で、訂正又は修正しなければならない（同条第6項）。但し、法人等は、提供された個人情報又はセンシティブ個人情報の真実性について責任を負うものではない旨、明記されている（同項）。

（7）情報提供者による同意を撤回する権利

法人等は、センシティブ個人情報を含む情報を取得するに先立ち、情報提供者に対して、当該情報を提供しない選択肢を与える必要がある。また、情報提供者は、サービスを利用する過程において、既に行った同意を書面により撤回する権利を有する（同条第7項）。なお、情報提供者からの同意が得られない場合や同意が撤回された場合、法人等は、関連する商品やサービスの提供を行わないことができるとされている（同項）。

（8）苦情担当役員の設置等

法人等は、個人情報[8]の処理に関して個人情報の提供者が有する不満に早急に対処しなければならない（同条第9 項）。かかる目的のため、法人等は、苦情担当役員（“Grievance Officer”）を配置し、その氏名及び連絡先をウェブサイトに公表しなければならない。苦情担当役員は、当該苦情を迅速に（但し、苦情を受けてから1 ヶ月以内に）対処しなければならない（同項）。

4　センシティブ個人情報の第三者への開示についての本人からの同意取得義務

法人等がセンシティブ個人情報を第三者に開示（“disclose”）する場合、当該開示が予め当該情報の提供者との間で合意されている場合や法律上の義務に基づく場合を除き、提供者から事前の同意を得る必要がある（同規則第6条1項）。かかる規定によりセンシティブ個人情報を受領した第三者は、さらにそれを第三者に開示してはならない（同条第4項）。

センシティブ個人情報の公表は、一切禁止されている（同条第3項）。

5　法人等へのサービス提供者に対する第5条及び第6条の適用関係

前述のとおり、センシティブ個人情報を取得する際や第三者に開示する際の本人からの同意取得義務等を規定する2011年個人情報保護規則第5条及び第6条の規定が、インドでBPO事業やコールセンター事業などのアウトソーシング事業を営む法人等（以下「アウトソーシング事業者」という。）にも適用されるか否かについては、必ずしも明確ではなかった。仮に適用される場合、アウトソーシング事業者は、個人情報の提供者と直接の契約関係等を有するわけではないため、同意の取得に困難が予想され、業務に支障を及ぼすとして、業界団体から強い反発が寄せられた。

8　2011年個人情報保護規則第5条9項は、単に「情報（“information”）」の提供者が有する不満に早急に対処すべき義務を規定するのみで、センシティブ個人情報に限定していないため、センシティブ個人情報でない個人情報も含むと考えられる。実務上は、かかる苦情担当役員も含めたプライバシーポリシーを作成することが想定される。

この点、2011年8月通達により、第5条及び第6条の規定は、アウトソーシング事業者には適用されないこととされ[9]、かかる義務を負うのは、個人情報の提供者に対して契約に基づき直接サービスを提供する法人等に限定される旨が明確化された。

通常、アウトソーシング事業者に業務を委託する法人等が、個人情報の提供者に対して第5条及び第6条の義務を負うことになるため、かかる義務に違反しないために必要となる事項をアウトソーシング事業者との間の契約に規定し、アウトソーシング事業者は、かかる契約上の義務を負うことになる。もっとも、かかる契約において、いかなる内容を規定すべきかについては、2011年個人情報保護規則上、特に規定されていない。

6　センシティブ個人情報を第三者へ移転する場合の第三者における保護体制及び開示の必要性の条件

法人等は、センシティブ個人情報を、2011年個人情報保護規則の規定に従って当該法人等が講じるのと同程度の保護を講じるインド又は他の国に所在する法人等に移転（“transfer”）[10]することができる（第7条）。かかるセンシティブ個人情報の移転は、当該法人等と情報提供者との間の適法な契約の履行に必要な場合又は当該情報提供者が情報の移転について同意した場合に限り、行うことができる。

7　合理的安全措置の内容（第8条）

（1）IT法第43A条の内容

IT法第43A条において、合理的安全措置（“reasonable security practices and procedures”）とは、対象情報を、不当なアクセス、損害、使用、改変、開示、毀損から守るための安全措置であって、①当事者間の合意、②法律、又は③かかる合意若しくは法律が存在しない場合は政府が規定する合理的安全措置を意味するとされている。このうち、②に相当する法律は現在のところ存在せず、③に相当するものとして、政府は2011年個人情報保護規則において、合理的安全措置に関する規定（第8条）を置いた。

前述のとおり、IT法第43A条により、合理的安全措置を実行・維持（“implementing and maintaining”）している場合には他人に与えた損害等の補償義務を免れることになる。同条の上記文言を前提とする限り、当事者間で合理的安全措置を合意すれば、2011年個人情報保護規則第8条に規定する合理的安全措置を講じなくても、IT法第43A条が適用されることになる。

9　“Any such body corporate providing services relating to collection, storage, dealing or handling of sensitive personal data or information under contractual obligation with any legal entity located within or outside India is not subject to the requirement of Rules 5&6. ”

10　第6条に規定される「開示（“disclose”）」と区別される概念で、「移転（“transfer”）」は当該個人情報の保有者が追加又は変更される場合が予定されている。

なお、IT法第43A条及び2011年個人情報保護規則上は、当事者間で合意する場合における合理的安全措置の内容について特段の規定は設けられていないが、実務上は、かかる合意内容は、2011年個人情報保護規則に準じたものである必要があると解されているようである。

（2）2011年個人情報保護規則が定める合理的安全措置の内容

法人等は、当該法人等が行う事業の性質上保護されるべき情報資産に相応しい管理的、技術的、機能的かつ物理的な安全管理措置を備えた「安全措置基準」を講じており、包括的かつ文書化された情報保護プログラム及び情報保護方針を有する場合は、合理的安全措置を講じているとみなされる（同規則第8条1項）。個人情報の保護義務に違反した場合、法人等は、法律により権限付与された機関の要求に応じて、当該法人等が文書化された情報保護プログラム及び情報保護方針により安全管理措置を講じていたことを立証しなければならない（同項）。

（3）安全措置基準の具体例

2011年個人情報保護規則において、いかなる場合に、同規則第8条1項に規定する「安全措置基準」を講じているとされるかの具体的内容は必ずしも明らかではないが、法人等が、①情報セキュリティ・マネジメント・システムの国際規格であるIS/ISO/IEC 27001（同条第2項）や、②産業協会又はそれによって設立された団体が定めるIS/ISO/IEC指針以外のデータ保護の最善運用指針（当該指針は政府の適正な認証・通知を受ける必要がある。同条第3項）に従っている場合は、後述(4)に記載の認証又は監査を行うことを条件に、「安全措置基準」を講じているとされる（同条第4項）。

（4）安全措置基準の監査

前述のIS/ISO/IEC 27001又は産業協会等が定めるデータ保護の指針を講じた法人等が、これらの基準又は最善運用指針について、独立性を有する監査官を通じて、政府が正式に承認した団体による定期的な認証又は監査[11]を受けている場合、当該法人等は、合理的安全措置を講じているとみなされる。

なお、2011年個人情報保護規則が施行されてからほぼ1年が経過するが、政府が正式に承認した団体は未だ存在しないようであり、法人等がかかる監査等を行うとしても、現状は、自主的な監査に留まっているようである。

---

11 かかる認証又は監査は、少なくとも年1回及び法人等が情報処理やコンピュータの重要なアップグレードを行う度に行われる必要があるとされる（2011年個人情報保護規則第8条4項）。

二　欧州委員会による事前調査の状況

EUデータ保護指令（“EU Data Protection Directive”）に基づく個人情報保護に関する十分性審査について、欧州委員会（“European Commission(EC)”）によるインドの個人情報保護法制に関する調査として、これまでに、2005年6月に“First Analysis of the Personal Data protection Law in India – Final Report”（以下「2005年レポート」という。）を、2010年1月に“Comparative Study on Different Approaches to New Privacy Challenges, In Particular In the Light of Technological Development”（以下「2010年レポート」という。）を発表している。

2005年レポートは、ECからの委託に基づきベルギーのナミュール大学（University of Namur）が取りまとめたものであり、その主たる目的として、ECがインドの個人情報保護制度についてEUデータ保護指令上の十分性審査を行うかどうかの決定を行うための資料としてインドにおける個人情報保護法制を調査することが挙げられている。2005年レポートにおいては、（調査当時における）IT法は、個人情報保護よりはむしろ電子商取引やサイバー犯罪の規制を対象としたものであり、インドは個人情報の保護に関して十分な法令上の手当てがなされていない、との結論が下されている。なお、当該調査の時点においては、前述の2008年IT法改正や2011年個人情報保護規則の制定はまだ行われておらず、現在のインドにおける個人情報保護法制とは前提が異なる点に注意が必要である。

また、2010年レポートは、ECによる各国の個人情報保護法制に関する調査として、LRDP Kantor Ltd が中心となって取りまとめられたものである。2010年レポートにおいては、インドの個人情報保護法制に関して、EUデータ保護指令上の十分性を充たすと明確に断定しうる側面は見受けられない、インドは個人情報保護に関しては極めて初期段階にあると結論づけている。ただし、同レポートにおいては、2011年個人情報保護規則が未制定であり、2008年IT法改正法において新設された第43A条の解釈が未だ明確に示されていない状態での調査が基礎とされており、こちらについても、インドにおける現状とはそもそも前提が異なっている点に注意する必要がある。

三　十分性審査の交渉過程

Ⅰ　十分性審査の対応状況

本件ヒアリング調査を行った2012年3月時点において、インド政府は、EUデータ保護指令に基づく個人情報保護に関する十分性審査について、ECに対する審査開始の申請は行っていない。但し、ECとの間で個人情報保護体制に関する議論の場を設け、ECにインドにおける個人情報保護体制が十分なものであると理解させることにより、インド企業とEU各国企業との間での取引における個人情報の取扱いが簡素化されることが期待できるとの目論見に基づき、2011年9月以降の約6ヶ月間、インド政府側の担当機関である商工省[12]は、ECとの間で、断続的に議論の機会を持ってきている。これまでに直接会談が2回、電話会議（テレビ会議）も複数回にかけて行われてきている。このような議論を行ってきていることについて、インド政府としては、ECとの間での正式な議論の場として位置づけておらず、非公式に内部的な議論を行っているものと整理しているとのことである。なお、十分性審査について、ECに対して正式申請を行うか否か、また行うとしてどの時期に行うか、といった点について具体的な計画はこれまでのところ特に有していないとのことである。

Ⅱ　ECとの議論の状況

2011年9月以降行われてきたインド政府とECとの間での個人情報保護に関する議論においては、インド政府側では商工省及びインド通信情報技術省情報技術局が窓口となり、2回の直接会談（場所：ベルギーとインド）及び数回に亘る電話会議（テレビ会議）の場が設けられた。個人情報保護に関するインドの非営利団体であるData Security Council of Indiaからも2名が参加している。

ECとの議論の過程において、インド政府側からは、個人情報保護に関する法令についての情報として、IT法及び2008年のIT法改正法、並びに同法の施行規則として2011年4月に公表された2011年個人情報保護規則をEC側へ提供している。インド政府側から提供されたこれらの情報に対し、EC側からは、質問や照会の連絡は来るものの、具体的な問題点の指摘等はなく、その他特段のコメントはなされていない。

上述のとおり、2012年3月時点においては、インド政府において十分性審査の正式申請に関する具体的な計画はないことから、ECとの間において引き続き非公式な議論が行われるものと見込まれている。

---

12 Ministry of Commerce and Industry

Ⅲ　個人情報保護関係法令に関する改正状況等

インドにおける個人情報保護関係法令であるIT法及びその施行規則の制定及び改正の経緯については前述のとおりである。すなわち、IT法については2000年に当初制定された後、2008年に改正が行われた。当該改正により新設された第43A条及び第72A条により、インド国内のあらゆる法人等(“body corporate”）に対して、合理的な個人情報保護に関する措置を実施すべき旨が義務付けられることとなった。また、インド政府はIT法第43A条関する施行規則として2011年個人情報保護規則を2011年4月に制定、公表した。2008年のIT法の改正及び2011年個人情報保護規則の制定に際しては、事前に改正案及び規則案がパブリックコメントの手続に付されたうえで、最終的な決定がなされたものである。

インド政府は、個人情報保護に関する国際的な取組みに関して、これまでアメリカ商務省[13]との協議や、データ保護・プライバシー・コミッショナー会議[14]への参加を通じて国際的な議論に参加してきた実績を有するものの、過去、経済提携協定や自由貿易協定を含む国際的な取り決めに基づいて、ECを含む他国より、個人情報保護関係法令の規制について改正等の対応を求められたことはない。上記IT 法の改正及び2011年個人情報保護規則の制定についても、他国からの要請やEUとの非公式な議論に基づいて行われたものではない。

インド政府においては、これらの法令に規定するところにより、インド国内における個人情報保護に関する規制のレベルはEUデータ保護指令において要求されている水準とほぼ等しいものとなっているものと考えており、現時点において、IT法第43A条及び2011年個人情報保護規則について、更に改正する具体的な予定は有してない。

なお、個人情報保護に関する当局の体制については、IT法の当初より特段の変更は行っておらず、十分性審査に対応するための規制部門の新設等は実施していない。

---

13 Department of Commerce

14 International Conference of Data Protection and Privacy Commissioners

四　十分性審査の途中経過

前述のとおり、インド政府は十分性審査に関し、ECに対して申請を行っておらず、当該審査が正式に開始した状況にはなく、個人情報保護体制に関するECとの非公式な議論を行っているというのが現状である。

五　十分性審査に関する議論の影響

Ⅰ　十分性審査に関する議論の経済的影響

インドにおける個人情報保護関係法令の状況に関する十分性審査は未開始ではあるが、インド政府としては、インドにおける個人情報保護体制が十分性を満たすレベルのものであるとECに理解させることにより、EU加盟国とインドとの間での個人情報の移転に関する障壁を低減させることができると考えているようである。また、インドが将来的に十分性審査の申請をし、当該審査が行われた結果、EUデータ保護指令上の十分性が認められるとの判断が正式に下された場合には、EU加盟国とインドとの間での個人情報の移転に関する障壁がないことが明確となる。このため、インド国内の産業界は、EU加盟国とインドとの間での商業取引に関する障壁の低減や手続の簡素化、ひいてはこれによる通商関係の振興につながるものとして、個人情報保護体制に関しECとの議論が行われていることについて、基本的に歓迎のスタンスを取っているものと考えられる。

Ⅱ　十分性審査に関する議論の法的影響

前述のとおり、IT法に関しては2008年に改正が行われ、2011年個人情報保護規則が2011年4月に制定、公表されている。2011年9月以降、ECとの議論が断続的に行われてきているが、その中で、個人情報保護関係法令に関する更なる改正といった特段の要請はEC側からなされていない。インド側としても、現在の個人情報保護関係法令は、EUデータ保護指令において求められている水準の規制となっていると考えており、現時点において今後更なる法改正等を行うことは予定していない。したがって、インド政府としては、少なくとも現時点においては、ECとの議論の過程における何らかの法的影響は認められないし、仮に将来的に十分性審査の申請を行い、当該審査が開始された場合においても特定の法的影響が及ぶ可能性は低いものと考えているようである。

以 上

あとがき

21世紀に入ってから10年を経過した今日、プライバシー・個人情報保護をめぐる議論は、テクノロジーの飛躍的な発展との関係で、ますます熱を帯びてきている。

プライバシー・個人情報保護について半世紀（50年）以上にわたり研究するとともに、実践してきた経験を持つ者にとっては、その議論の展開はある程度予測されたところである。

30年以上も前になるが、1980年に著した『現代のプライバシー』（岩波書店）の「あとがき」で次のように書いた。

「今回、本書をまとめるにあたり、プライバシーについて、広範囲にわたり検討を行なった。検討すればするほど、無限の拡がりと奥行きのある問題であることがわかってきた。このような形でまとめてみたものの、新たな課題がつぎからつぎへと脳裡を去来している。」

当時においては、国際的な議論は始まったばかりであったといえる。『現代のプライバシー』は1980年8月20日に刊行された。この本の執筆段階では、今日では広く知られている、経済協力開発機構（Organisation for Economic Co-operation and Development, OECD）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」（Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data）、すなわち、プライバシー・ガイドライン（Privacy Guidelines）は、議論の過程にあった。そのドラフトを分析し、紹介した。プライバシー・ガイドラインは、1980年9月23日に理事会で採択された。

日本は、1961年に設立されたOECDに1964年に加盟が承認された。加盟国としての日本では、このプライバシー・ガイドラインの採択を機に政府レベルでプライバシーに関する検討が始まった。それは、行政管理庁（当時）のプライバシー保護研究会においてであった。私は、そのメンバーとして外国政府との意見交換などに当たった。この研究会の報告書は、1982年7月にまとまり、立法化の方向性を示した。

また、1988年にまとめた『プライバシーと高度情報化社会』（岩波書店）では、先に引用した文章を再掲し、それにつづけて、次のようにその後の状況を描写してみた。

「その後の発展をつぶさに観察してみると、約七年半前に記したことがますます真実味を帯びてきたように思えてならない。しかも、問題は、情報化社会の高度化に伴って以前にも増して多様化・複雑化してきている。本書では、プライバシー保護・個人情報保護の重要性・緊急性を一人でも多くの方に知っていただくために、それらの問題のうち、今日の時点で取り上げておかなければならないと考えられるものについて検討を加えた。

しかし、残された課題が多いうえに、高度情報化社会の進展につれてさらに種々様々な問題が起こってくるであろう。前著でも情報化社会との関連で現代的プライバシー権を論じたが、そこでいう情報化社会は主としてコンピュータ社会を意味していた。だが、1980年代に入り、今日では、情報化社会という概念でとらえようとしている情報化はコンピュータと電気通信とが結合されて広く社会に影響

を与える現象として認識されているということができる。換言すれば、現代から近未来にかけての情報化は、スタンドアローン（独立）のコンピュータといういわば「点」が通信回線という「線」と結合して「面」へと拡大し（ネットワーク化の進展)、加速度的に社会のあらゆる分野、特に家庭生活にまで波及する傾向を示していると把握できる。そのため、今日いう情報化は、ちょうど産業革命がそうであったように、既存の制度に計り知れないインパクトを与える必然性を具備している。」

それに関する研究は、「無限の拡がりと奥行きのある問題」という、いわば“奥儀”を探究するようなものである。

私自身、その奥儀をきわめるべく、様々な方法で様々な研究と実践を試みてきた。ときには充実感のあるリアクションがあるかと思えば、ときには徒労感の残る反応に遭遇したこともある。

しかし、日本では、プライバシー・個人情報保護問題に対する反応は一般的には鈍く、議論の国際的展開のキャッチアップも不十分であったといわざるを得ない。キャッチアップの重要性は、改めていうまでもないところである。

今回、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で、EUデータ保護指令が求める「十分性」（adequacy）について総合的に調査することができた。その意義は、どのように強調してもし過ぎることはない。

本調査報告書が、世界の個人情報保護制度の一定部分がEUデータ保護指令などとの関係でどのように捉えられているかについて広く認識される機会になることを期待する。

一橋大学名誉教授
堀部　政男

資料　EUデータ保護指令仮訳

「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１９９５年１０月２４日の欧州議会及び理事会の９５／４６／ＥＣ指令」(Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data)

堀部政男研究室仮訳

前文［７２項］(省略)

第Ⅰ章 総則

第1条 指令の目的

1. 構成国は、この指令に従って、個人データの取扱いに関して、自然人の基本的な権利及び自由、特にそのプライバシーの権利を保護しなければならない。
2. 構成国は、第1項に基づいて与えられる保護を理由として、構成国の間の個人データの自由な流通を制限し、又は禁止してはならない。

第2条 定義

この指令の目的に関して、

(a)「個人データ」とは、識別された又は識別され得る自然人（以下「データ主体」という。）に関するすべての情報をいう。識別され得る個人とは、特に個人識別番号、又は肉体的、生理的、精神的、経済的、文化的並びに社会的アイデンティティに特有な一つの又はそれ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得る者をいう。

(b)「個人データの取扱い」(以下「取扱い」という。）とは、自動的な手段であるか否かにかかわらず、個人データに対して行われる作業又は一連の作業をいう。この作業とは、収集、記録、編集、蓄積、修正又は変更、復旧、参照、利用、移転による開示、周知又はその他周知を可能なものとすること、整列又は結合、ブロック、消去又は破壊することをいう。

(c)「個人データ・ファイリングシステム」(以下「ファイリングシステム」という。）とは、集約型であるか、非集約型であるか、又は機能的若しくは地理的に分散されたものであるか否かにかかわらず、特定の基準に基づいてアクセスすることができる構築された一連の個人データをいう。

(d)「管理者」とは、単独で又は他と共同して、個人データの取扱いの目的及び手段を決定する自然人、法人、公的機関、機関又はその他の団体をいう。取扱いの目的及び手段が国内の若しくは共同体の法律又は規則によって決定される場合には、管理者又はその指定に関する特定の基準は、国内法又は共同体法でもって定めることができる。

(e)「取扱者」とは、管理者のために個人データの取扱いを行う自然人、法人、公的機関、機関又はそ

の他の団体をいう。

(ｆ)「第三者」とは、データ主体、管理者、取扱者及び管理者又は取扱者の直接の職権の下でデータを取り扱う権限を与えられている者以外の自然人、法人、公的機関、機関又はその他の団体をいう。

(ｇ)「取得者」とは、第三者であるか否かにかかわらず、データの開示を受ける自然人、法人、公的機関、機関又はその他の団体をいう。ただし、特定の調査の枠内でデータを取得する機関は、取得者とみなされない。

(ｈ)「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取り扱わ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のかつ十分に情報を提供された上での意思表示をいう。

第３条 適用範囲

1. この指令は、全部又は一部が自動的な手段による個人データの取扱い、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とすることが意図されている個人データの自動的な手段以外の取扱いに適用される。
2. この指令は、次の個人データの取扱いには適用してはならない。
   ―欧州連合条約第Ｖ章及び第VI章に規定されている共同体法の適用範囲外の活動中に行われるもの、及び公安、防衛、国家安全保障（取扱作業が国家安全保障問題にかかる場合には国家の経済的安定を含む。）又は刑法の分野における国家の活動に関するすべての取扱作業
   ―自然人によって、純粋に個人的な又は家庭内での活動中に行われるもの。

第４条 適用される国内法

1. 各構成国は、この指令に従って採択した国内規定を次の場合の個人データ取扱いに適用しなければならない。

(ａ) 取扱いが構成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) 管理者が構成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構成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、個人データの取扱いを目的として当該構成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。

2. 管理者は、第１項（ｃ）に定められた場合において、その構成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。

第Ⅱ章 個人データの取扱いの適法性に関する一般準則

第５条

構成国は、本章の規定の制限の範囲内において、個人データの取扱いが適法となる条件をより正確に定めなければならない。

第Ⅰ節 データ内容に関する原則

第６条

１．構成国は、個人データが次の条件を満たすように定めなければならない。

(ａ)公正かつ適法に取り扱われること。

(ｂ)特定された明示的かつ適法な目的のために収集され、それに続いてこれらの目的と相容れない方法で取り扱われないこと。ただし、歴史的、統計的又は科学的な目的のために引き続き行われる取扱いは、構成国が適切な保護措置を定めている場合には、これとあいいれないものとはみなされない。

(ｃ)データが収集され、及び／又はそれに続いて取り扱われる目的に照らして、適切であり、関連性があり、かつ過度でないこと。

(ｄ)正確であり、かつ必要な場合にはデータを最新のものに保つこと。データが収集され、又はそれに続いて取り扱われる目的に照らして、不正確又は不完全なデータが消去又は修正されるのを確保するために、あらゆる合理的な手段が講じられなければならない。

(ｅ)データが収集される、又はそれに続いて取り扱われる目的に照らして必要とされる期間内に限り、データ主体の識別が可能な形態で保存されること。構成国は、歴史的、統計的又は科学的な利用のために長期間保存される個人データに関して適切な保護措置を定めなければならない。

2.　管理者は、第１項の遵守を確保しなければならない。

第Ⅱ節 データ取扱いの正当性の基準

第７条

構成国は、次の条件を満たす場合にのみ、個人データが取り扱われるように定めなければならない。

(ａ)データ主体が明確に同意を与えた場合、又は、

(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取扱いが必要な場合、又はデータ主体の請求により、契約の締結前に、その段階を踏むために取扱いが必要な場合、
又は、

(ｃ)管理者が従うべき法的義務を遵守するために取扱いが必要な場合、又は、

(ｄ) データ主体の重大な利益を保護するために取扱いが必要な場合、又は、

(ｅ)公共の利益のために、又は管理者若しくはデータの開示を受ける第三者に与えられた公的権限の

行使のために行われる業務の遂行上取扱いが必要な場合。又は、

(ｆ)管理者又はデータの開示を受ける第三者若しくは当事者の正当な利益のために取扱いが必要な場合。ただし、これらの利益より、第1条第1項の規定に基づいて保護が必要とされるデータ主体の基本的な権利及び自由に関する利益が優先する場合には、この限りではない。

第Ⅲ節 特別な種類の取扱い

第8条 特別な種類のデータの取扱い

1. 構成国は、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取扱い、及び健康又は性生活に関するデータの取扱いを禁止しなければならない。
2. 第1項は、次の場合には適用されない。

(ａ)データ主体が前項に定められたデータの取扱いに対して明示の同意を与えた場合。ただし、構成国の法律がデータ主体の同意によっても第1項の禁止を解除し得ないことを規定している場合は、この限りではない。又は、

(ｂ)取扱いが、雇用法の分野において管理者の義務の履行、及び特定の権利の行使の目的のために必要な場合。ただし、十分な保護措置を定めている国内法により、権限を与えられている場合に限る。又は、

(ｃ)取扱いが、データ主体が物理的に又は法的に同意を与えることができない場合に、データ主体又はその他の者の重大な利益を保護するために必要な場合。又は、

(ｄ)取扱いが、政治、思想、宗教又は労働組合の目的を有した財団、協会又はその他の非営利団体による、適切な保障の下での正当な活動の過程において行われる場合。ただし、その取扱いが当該団体の構成員又は団体の目的に関して団体と定期的に接触している者のみに関係していること、及び当該データがデータ主体の同意を得ないで第三者に開示されないことを条件とする。又は、

(ｅ)取扱いが、データ主体により明白に公にされたデータに関する場合、又は法的な請求の確定、行使又は防御のために必要な場合

3. 第1項の規定は、データ取扱いが予防的医療、医療診断、看護若しくは治療の提供の目的のため又は健康管理サービスの運営のために必要な場合、並びに国内法又は国の管轄機関が定めた規則により、職業上の守秘義務を負う医療専門家によって、又は同様の守秘義務を負うその他の者によってデータが取り扱われる場合には、適用されない。
4. 構成国は、適合的な保護措置を定める場合に、重要な公共の利益を理由として、国内法又は監督機関の決定により、第2項の規定に加えて、適用除外を規定することができる。
5. 犯罪、刑事事件の有罪判決又は安全保障に関するデータの取扱いは、公的機関の管理の下でのみ行わせることができる。また、国内法に適合的な特定の保護措置が定められている場合には、その措置を定めた国内規定に基づいて、構成国により認められる例外に従って取り扱うことができる。ただし、有罪判決の完全な記録は、公的機関の管理の下でのみ保存され得る。

構成国は、行政制裁又は民事事件の判決に関するデータににについても、公的機関の下で取り扱われなければならないことを定めることができる。

6. 第4項及び第5項に規定されている第1項の例外は、委員会に通知されなければならない。

7. 構成国は、国内の個人識別番号又はその他一般的に適用されている識別子の取扱いに関する条件を定めなければならない。

第9条 個人データの取扱いと表現の自由

構成国は、プライバシー権と表現の自由に関する準則を調和させる必要がある場合に限り、ジャーナリズム目的又は芸術上、文学上の表現目的のためにのみ行われる個人データの取扱いについて、本章、第Ⅳ章及び第Ⅵ章の規定の適用除外及び例外を定めなければならない。

第Ⅳ節 データ主体に提供されなければならない情報

第10条 データ主体からデータを収集する場合の情報

構成国は、管理者又はその代理人が、その者自身に関するデータが収集されるデータ主体に対して、少なくとも次の情報を提供しなければならないことを定めなければならない。

ただし、データ主体が既にその情報を得ている場合はこの限りではない。

(a) 管理者及びその代理人がいる場合はその身元

(b) そのデータが予定されている取扱いの目的

(c) 次に示すようなその他の追加情報

—データの取得者又は取得者の所属

—質問に対する回答が義務的なものであるか任意的なものであるか、及び回答しなかった場合にもたらされるであろう結果

—データ主体に関するデータにアクセスする権利、及びそれを修正する権利があること。これらの追加情報は、データが収集される特定の状況を考慮して、データ主体に関して公正な取扱いを担保するために必要な場合に限る。

第11条 データがデータ主体から収集されなかった場合の情報

1. 構成国は、データがデータ主体から収集されなかった場合、管理者又はその代理人が個人データの記録を始めたとき、又は第三者に開示されるであろう場合には遅くとも最初に開示されるときまでに、データ主体に対して少なくとも次の情報を提供しなければならないことを定めなければならない。ただし、データ主体が既にその情報を得ている場合はこの限りではない。

(a) 管理者及びその代理人がいる場合はその者の身元

(b) 取扱いの目的

(c) 次に示すようなその他の追加情報

——関係するデータの種類

——データの取得者又は取得者の所属

——データ主体に関するデータにアクセスする権利、及びそれを修正する権利があること。

これらの追加情報は、データが取り扱われる特定の状況を考慮して、データ主体に関して公正な取扱いを担保するために必要な場合に限る。

2. 第1項の規定は、特に統計目的又は歴史的、科学的調査の目的の取扱いのためのものであり、当該情報の提供が不可能であり若しくは過度の困難を伴う場合、又は記録、開示が法律により明示的に規定されている場合には、適用されない。構成国は、このような場合に、適切な保護措置を定めなければならない。

第Ⅴ節 データ主体のデータへのアクセス権

第12条 アクセス権

構成国は、すべてのデータ主体に対して、管理者から次に定めるものを取得する権利を保障しなければならない。

(a) 合理的な期間内に制約なく、及び過度の遅れ又は費用を伴うことなく、

—データ主体に関するデータが取り扱われているか否かの確認、及び少なくとも取扱いの目的、関係するデータの種類、開示されたデータの取得者又は取得者の所属に関する情報

—取り扱われているデータ及びその情報源に関する入手可能な情報の理解可能な形式でのデータ主体への連絡

—少なくとも第15条第1項に規定された自動的な決定の場合には、データ主体に関するデータの自動処理に係る論理についての知識

(b) 適切な場合には、特にデータの不完全又は不正確な性質のために、この指令の規定に従わないで取り扱われたデータの修正、消去又はブロック

(c) データが既に開示されている第三者に対する（b）に従って行われた修正、消去又はブロックの通知。ただし、これが不可能であり又は過度の困難を伴う場合はこの限りではない。

第Ⅵ節 適用除外及び制限

第13条 適用除外及び制限

1. 構成国は、次の事項を保護するために必要な場合には、第6条第1項、第10条、第11条第1項、第12条及び第21条に規定された義務及び権利の範囲を制限する法的措置を採択することができる。

(a) 国家安全保障

(b) 防衛

（c）公共の安全
（d）刑事的犯罪又は規制されている職業に対する倫理違反の予防、取調べ、捜査及び起訴
（e）通貨、予算及び課税に関する事項を含む構成国又は欧州連合の重要な経済的又は財政的利益
（f）（c）（d）及び（e）の場合に、たとえ一時的なものであっても、公的権限の行使に関する監視、捜査又は規制職務
（g）データ主体の保護、又はその他の者の権利及び自由の保護

2. 構成国は、特にデータが特定の個人に関する措置又は決定のために利用されるのではない場合に、十分な法的保護措置に従って、明らかにデータ主体のプライバシーを侵害するおそれがない限りにおいて、立法措置により、第12 条に規定された権利を制限することができる。これには、データが科学的調査目的のためにのみ取り扱われる場合、又は統計を作成する目的のためにのみ、必要な期間を超えないで、個人的な形式で保存されている場合がある。

第Ⅶ節 データ主体の異議申立権

第14条 データ主体の異議申立権

構成国は、データ主体に次の権利を与えなければならない。

（a）少なくとも第7条（e）及び（f）に規定された場合には､国内法に別段の規定がある場合を除き、いつでも自己に関するデータの取扱いに対して、自己の特定の状況に関連するやむにやまれない正当な理由を根拠として、異議申立てを行うことができること。適法な異議申立てがあった場合には、管理者によって始められた取扱いに、当該データを含むことはできない。

（b）管理者がダイレクト・マーケティング目的のために取り扱うことを予定している自己に関する個人データの取扱いに対して、請求にもとづき無料で異議申立てを行うことができること、又は個人データが最初に第三者に開示される前に、若しくは第三者のダイレクト・マーケティング目的のために利用される前に十分な情報の提供を受け、かつ開示又は利用に対して無料で異議申立てを行う権利を明示的に与えられること。

構成国は、データ主体が（b）前段に規定された権利の存在を確認できるために必要な措置を講じなければならない。

第15条 自動処理による個人に関する決定

1. 構成国は、すべての者に対して、その者に関する法的効果を生じさせる、又は重大な影響を与える判断であって、かつそれが業績、信用度、信頼性、行為等、その者に関する個人的な側面を評価することを意図したデータの自動処理にのみ基づくものである場合に、その判断の対象とならない権利を与えなければならない。
2. 構成国は、次の場合に、この指令の他の条項に従って、個人が第1項に関する種類の判断の対象となり得ることを定めなければならない。

（a）判断が契約の締結又は履行の過程において行われる場合。ただし、データ主体が行った契約の締

結又は履行のための要求が満たされた場合、又はデータ主体の見解を認める協定のように、データ主体の正当な利益を保護する適切な措置が存在することを条件とする。又は、

（b）データ主体の正当な利益を保護する措置が、同時に規定された法律により、認められた場合。

第Ⅷ節 取扱いの機密性及び安全性

第16条 取扱いの機密性

取扱者自身も含む、個人データにアクセスを有している、管理者又は取扱者の下に従事している者は、管理者からの指示に基づく場合を除き、個人データを取り扱ってはならない。ただし、法律の規定により取り扱うよう命じられている場合は、この限りではない。

第17条 取扱いの安全性

1. 構成国は、特に取扱いがネットワーク上のデータの伝送を伴う場合及びその他のあらゆる不法な取扱形式に対して、偶発的な又は違法な破壊、偶発的な損失、変更、無権限の開示又はアクセスから個人データを保護するために、管理者は、適切な技術的及び組織的措置を実施しなければならないことを定めなければならない。

   この措置は、技術水準及びその導入に伴う費用を考慮して、取扱いによって生じ得る危険及び保護すべきデータの性質に応じた適切な水準の保護を保証できるものでなければならない。
2. 構成国は、管理者が自己の利益のために取扱いを行う場合には、実施される取扱いに関する技術的安全措置及び組織的措置において、相応の保証を提供する取扱者を選定し、及びこの措置の遵守を確保しなければならない。
3. 取扱者による取扱いの実施は、取扱者を管理者に拘束させる、特に次の規定を含む契約又は法律行為に準拠しなければならない。

   ―取扱者は管理者の指示にのみ基づいて行動しなければならないこと。

   ―取扱者が設置されている構成国の法律によって定義される第1項に規定された義務は、既存の取扱者にも課せられなければならないこと。
4. 証拠を保全するために、データの保護に関する契約又は法律行為、及び第1項に規定された措置に関する要件の一部は、書面又はその他の同等の形式によらなければならない。

第Ⅸ節 通知

第18条 監督機関への通知義務

1. 構成国は、管理者又は代表者がいる場合はその者が、一つの目的又は複数の関係する目的を達成することを意図した全部又は一部の自動処理作業及び一連の作業を実施する前に、第28 条に規定された監督機関に通知しなければならないことを定めなければならない。
2. 構成国は、次の場合に、かつ次の条件に基づいてのみ、通知の簡略化又は適用除外を定めることができる。

―取り扱われるデータを考慮しつつ、データ主体の権利及び自由に制約的な影響を与えるおそれが低い種類の取扱作業に関して、管理者又はその代理人が取扱いの目的、取り扱われるデータ又はデータの種類、データ主体の所属、データの開示を受ける取得者又は取得者の所属、及びデータが保存される期間を特定した場合、及び／又は、

―管理者が、管理者を規律する国内法に従って、特に次の事項に関して責任を有する個人データ保護担当役員を任命した場合

―この指令に基づいて制定された国内法の規定を、それぞれの方法でもって、内部的適用を行うことを確保すること。

―第21条第2項に定められた情報に関する事項を含む管理者が行う取扱作業の記録を保管すること。

これによって、取扱作業がデータ主体の権利及び自由に制約的な影響を与えるおそれがないよう保証すること。

3. 構成国は、法律又は規則に従って、情報を公衆に提供することが予定されている、及び公衆一般又は正当な利益を証明する者のいずれかによる閲覧のために公開されている記録の保管を唯一の目的としている取扱いには、第1項を適用しないことを定めることができる。
4. 構成国は、第8条第2項（d）に規定された取扱作業の場合に、通知義務の適用除外又は通知の簡略化を定めることができる。
5. 構成国は、個人データを含む一定の又はすべての非自動的処理作業が通知されなければならないこ とを明記し、又はこれらの取扱作業には簡略化された通知が必要であることを定めることができる。

第19条 通知の内容

1. 構成国は、通知に含まれるべき情報を特定しなければならない。これには、少なくとも次の事項が含まれなければならない。

(a) 管理者及びその代理人がいる場合には代理人の名称及び住所

(b) 取扱いの一つ又は複数の目的

(c) データ主体の一つ又は複数の所属、及びデータ主体に関するデータ又はデータの種類に関する記述。

(d) データの開示を受け得る取得者又は取得者の所属

(e) 第三国へのデータの移転の予定

(f) 取扱いの安全性を確保するために、第17条に従って講じられる措置の適切性に関する予備的評価を認める一般的記述

2. 構成国は、第1項に規定された情報に影響を与える変更が監督機関に通知されなければならない旨の手続を特定しなければならない。

第20 条 事前の調査

1. データ主体に特定の危険をもたらすおそれのある取扱作業を指定し、その取扱作業がその作業開始前に検査を受けていることを調査しなければならない。
2. この事前の調査は、管理者からの通知の受領を受けて監督機関が、又は疑いのある場合には監督機関に意見を求めなければならない個人データ保護担当役員が実施しなければならない。
3. 構成国はまた、国の立法機関による措置、又はその立法措置に基づいて取扱いの性質を定義し、適切な保護措置を定めた措置のいずれかの準備段階において、この調査を実施することができる。

第21 条 取扱作業の公開

1. 構成国は、取扱作業が公開されることを確保する措置を講じなければならない。
2. 構成国は、第18条に従って通知された取扱作業の記録が監督機関によって保管されなければならないことを定めなければならない。
   この記録は、少なくとも第19条第1項（a）から（e）までに掲げられた情報を含むものでなければならない。
   この記録は、何人も閲覧することができる。
3. 構成国は、通知義務のない取扱作業に関して、管理者又は構成国が任命する他の機関が、少なくとも第19 条第1 項（a）から（e）までに規定された情報を、請求があったすべての者に対して適切な形式で提供できる状態にしておくことを定めなければならない。
   構成国は、取扱いの唯一の目的が、法律又は規則に従って情報を公衆に提供し、及び公衆一般又は正当な利益を証明できるすべての者のいずれかに対する閲覧を意図している記録の保管である取扱いには適用しないことを定めることができる。

第Ⅲ章 司法的救済、責任及び制裁

第22 条 救済

構成国は、とりわけ第28条に規定された監督機関によって、司法機関への付託に先立って、なされる行政的救済に実体的効果を持つことなく、すべての者が、かかるデータ取扱いに適用される国内法によって保障される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23 条 責任

1. 構成国は、違法な取扱作業、又はこの指令に従って規定された国内規定とあいいれない行為の結果として生じた損害を被ったすべての者が、被った損害に対する金銭賠償を管理者から受けることができることを定めなければならない。
2. 管理者は、損害の原因となった結果に対して責任がないことを証明した場合には、全部又は一部の賠償責任を免除され得る。

第24 条 制裁

構成国は、この指令の規定を完全に実施することを担保するために適合的な措置を講じ、及びこの指令に従って定められた規定に対する違反がある場合に課せられる制裁について特に規定しなければならない。

第Ⅳ章 第三国への個人データの移転

第25条 原則

1. 構成国は、取り扱われている又は移転後に取扱い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に実体的効果を持つことなく、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。
2. 第三国によって保障される保護のレベルの十分性は、一つのデータ移転作業又は一連のデータ移転作業に関するあらゆる状況に鑑みて評価されなければならない。特に、データの性質、予定されている取扱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、並びに当該第三国において遵守されている職業上の規則及び安全保護対策措置が考慮されなければならない。
3. 構成国及び委員会は、第三国が第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ないと考えられる事例について、相互に情報提供しなければならない。
4. 構成国は、第31条第2項に規定する手続に基づいて委員会が、第三国が本条第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ないと認定した場合には、当該第三国への同一タイプのデータの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。
5. 委員会は、適切な時期に、第4項に基づく認定によってもたらされる状況を改善することを目的とする交渉を開始しなければならない。
6. 委員会は、第31条第2項に規定する手続に基づいて、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。

   構成国は、委員会の決定を遵守するために必要な措置を講じなければならない。

第26条 例外

1. 構成国は、第25条の適用を制約するものとして、及び特別な場合を規律する国内法に別段の定めがある場合を除いて、第25条第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ない第三国に対する個人データの移転又は一連の移転は、次の条件を満たした場合に行うことができることを定めなければならない。

（a）データ主体が、予定されている移転に対して明確な同意を与えている場合。又は、
（b）移転が、データ主体及び管理者間の契約の履行のために、又はデータ主体の請求により、契約締結前の措置の実施のために必要である場合。又は、
（c）移転が、データ主体の利益のために、データ主体及び第三者間で結ばれる契約の締結又は履行のために必要である場合。又は、
（d）移転が、重要な公共の利益を根拠として、又は法的請求の確定、行使若しくは防御のために必要である場合、又は法的に要求される場合。又は、
（e）移転が、データ主体の重大な利益を保護するために必要である場合。又は、
（f）法律又は規則に基づいて情報を一般に提供し、及び公衆一般又は正当な利益を証明する者のいずれかによる閲覧のために公開されている記録から、閲覧に関する法律に規定された条件が特定の事例において満たされる範囲内で、移転が行われる場合。

2. 構成国は、第1項の規定に実体的な効果を持つことなく、管理者が個人のプライバシー並びに基本的な権利及び自由の保護、並びにこれらに相当する権利の行使に関して、十分な保護措置を提示する場合には、第25条第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ない第三国への個人データの移転又は一連の移転を認めることができる。当該保護措置は、特に適切な契約条項から帰結することができる。
3. 構成国は、第2 項によって付与された許可を、委員会及び他の構成国に通知しなければならない。一つの構成国又は委員会が、個人のプライバシー並びに基本的な権利及び自由の保護を含む正当な理由に基づいて異議申立てを行った場合には、委員会は、第31条第2項に規定された手続に基づいて適切な措置を講じなければならない。
   構成国は、委員会の決定を遵守するために必要な措置を講じなければならない。
4. 構成国は、第31条第2 項に規定された手続に従って、一定の標準契約条項が本条第2項によって要求される十分な保護措置を提供していると決定する場合には、委員会の決定を遵守するために必要な措置を講じなければならない。

第Ⅴ章 行動規準

第27条

1. 構成国及び委員会は、構成国がこの指令に従って採択した国内規定の適切な実施に役立てるために、様々な分野の特色を考慮しつつ、行動規準の策定を促進しなければならない。
2. 構成国は、国内の規準の草案を策定し、又は既存の国内の規準を修正又は拡充しようとしている業界団体及びその他の管理者の業界の代表機関が、これを国家機関の意見を聞くために付託できるように定めなければならない。
   構成国は、当該国家機関が、とりわけ付託された草案がこの指令に従って採択された国内規定に従ったものであるか否かを確認するよう定めなければならない。適合するとみえる場合には、国家機関はデータ主体又はその代理人に意見を求めなければならない。

3. 共同体の規準草案及び既存の共同体規準の修正又は拡充は、第29条に規定された作業部会に付託することができる。この作業部会は、とりわけ付託された草案が、この指令に従って採択された国内規定に従っているものであるか否かを決定しなければならない。適合するとみえる場合には、国家機関は、データ主体又はその代理人に意見を求めなければならない。委員会は、作業部会によって承認された規準の適切な公開を保障することができる。

第VI章 監督機関及び個人データの取扱いに係る個人の保護に関する作業部会

第28条 監督機関

1. 各構成国は、一つ又はそれ以上の公的機関が、この指令に従って構成国が採択した規定の範囲内で、その適用を監視する責任を負うことを定めなければならない。
   この機関は、委任された職権を遂行する上で、完全に独立して活動しなければならない。
2. 各構成国は、個人データの取扱いに係る個人の権利及び自由の保護に関する行政措置又は規則を制定する際に、監督機関に諮ることを定めなければならない。
3. 各監督機関は、特に次の権限を与えられなければならない。
   ―取扱作業の対象を構成するデータにアクセスする権限、及び監督職務の遂行に必要なすべての情報を収集する権限等の調査権限
   ―例えば、第20条の規定に従って取扱作業の実施前に意見を述べ、及びこの意見の適切な公開を保障する権限、データのブロック、消去又は破壊を命じる権限、取扱いの一時的又は確定的な禁止を課す権限、管理者を警告又は懲戒する権限、中央議会又はその他の政治機関に問題点を照会する権限等の仲裁権限
   ―この指令に従って採択された国内規定への違反があった場合に法的手続を開始する権限、又はこの違反を司法機関に通知する権限
   監督機関の決定に不服がある場合は、裁判所に対して訴訟を提起することができる。
4. 各監督機関は、個人データの取扱いに係る個人の権利及び自由の保護に関して、すべての者及びそれを代表する協会からなされる主張を聴取しなければならない。このような者は、主張の結果についての情報を提供されなければならない。
5. 各監督機関は、定期的に活動報告書を作成しなければならない。この報告書は、公開されなければならない。
6. 各監督機関は、当該取扱いに関してどの国の国内法が適用され得るかにかかわらず、当該構成国の領域内においては、本条第3項の規定に従って付与された権限を行使する資格を有する。各監督機関は、他の構成国からこの権限を行使することを要請される場合がある。
   監督機関は、特にすべての有益な情報を交換する等、職務の遂行に必要な範囲内で、相互に協力しなければならない。

7. 構成国は、監督機関の構成員及び職員が、退職後であっても、アクセスした機密情報に関して職業上の守秘義務を負うことを定めなければならない。

第29条 個人データの取扱いに係る個人の保護に関する作業部会

1. 個人データの取扱いに係る個人の保護に関する作業部会（以下「作業部会」という。）が、ここに設置される。

この作業部会は、助言機関であり、独立して活動しなければならない。

2. 作業部会は、監督機関の又は各構成国が指名した機関の代表者、共同体の機構及び団体のために設立された一つの又は複数の機関の代表者、及び委員会の代表者によって構成されなければならない。

作業部会の各構成員は、各人が代表している機構又は機関により指名されなければならない。構成国が一を超える監督機関を指名した場合は、それらの機関は、共同代表を指定しなければならない。これと同一の規定が、共同体の機構及び機関のために設立された監督機関の場合にも適用されなければならない。

3. 作業部会は、監督機関の代表者の単純多数決によって決定を行わなければならない。
4. 作業部会は、その議長を選出しなければならない。議長の任期は2 年とし、再任を妨げないものとしなければならない。
5. 作業部会の事務局は、委員会によって設置されなければならない。
6. 作業部会は、その手続に関する独自の準則を定めなければならない。
7. 作業部会は、議長独自の判断又は監督機関の代表者の要請若しくは委員会の要請のいずれかに基づいて、議長によって会議目録にあげられた議題について検討しなければならない。

第30条

1. 作業部会は、次の事項を行わなければならない。

(a) この指令に従って採択された国内措置の統一的な適用に資するために、当該措置の適用を含むあらゆる問題点について検討すること。

(b) 共同体域内及び第三国における保護のレベルに関する意見を委員会に提出すること。

(c) この指令の修正の提案、個人データの取扱いに係る自然人の権利及び自由を保護するための追加的な又は特別な措置、並びにこの権利及び自由に影響を与える共同体の措置についてのその他の提案に関して、委員会に助言を与えること。

(d) 共同体レベルで策定された行動規準に関して意見を提出すること。

2. 作業部会が、共同体域内において個人データの取扱いに係る個人の保護が同等であることに影響を与えると思われる相違が、構成国の法律及び慣行の間に生じていると認定した場合には、状況に応じて、このことを委員会に通知しなければならない。
3. 作業部会は、共同体域内の個人データの取扱いに係る個人の保護に関連するあらゆる事案に関し

て、独自の判断に基づき、勧告を行うことができる。

4. 作業部会の意見及び勧告は、委員会及び第31条に規定された専門委員会に送付されなければならない。

5. 委員会は、作業部会の意見及び勧告に応じて委員会がとった行動について、作業部会に通知しなければならない。この通知は、欧州議会及び理事会に対しても送付される報告書において行わなければならない。この報告書は、公開されなければならない。

6. 作業部会は、共同体域内及び第三国における個人データの取扱いに係る自然人の保護に関する状況について年次報告書を作成し、これを委員会、欧州議会及び理事会に提出しなければならない。この報告書は、公開されなければならない。

第Ⅶ章 共同体の実施措置

第31条 専門委員会

1. 委員会は、構成国の代表者によって構成され、委員会の代表者が議長を務める専門委員会の支援を受けなければならない。

2. 委員会の代表者は、講じられるべき措置の草案を専門委員会に対して提出しなければならない。専門委員会は、事案の緊急性に応じて議長が設定した期間内に、草案に対する意見を述べなければならない。

この意見は、条約第148条第2項に規定された多数決によって述べられなければならない。専門委員会内における構成国の代表者による投票は、当該条項に規定された加重多数決によらなければならない。議長は、投票してはならない。

委員会は、即時に適用されなければならない措置を採択しなければならない。ただし、この措置が専門委員会の意見と合致しない場合は、委員会が、直ちに理事会に対して当該措置について連絡しなければならない。これは、次によるものとする。

―委員会は、連絡を受けた日から三ヶ月間、決定された措置の適用を延期しなければならない。

―理事会は、有効な多数決によって、前号に規定された期限内に異なった決定を行うことができる。

最終条項

第32条

1. 構成国は、この指令の採択の日から少なくとも3年以内に、この指令を遵守するために必要な法律、規則及び行政規定を発効させなければならない。

構成国がこうした措置を採択する際には、これらの措置は、この指令への参照を含んでいなければならず、又は公布する際には、その参照部分を添付しなければならない。当該参照方法は、構成国によって定められなければならない。

2. 構成国は、この指令に従って採択された国内規定が発効する日に既に実施されている取扱いが、その日から3年以内にこれらの規定に合致させられることを確保しなければならない。

構成国は、前段からの例外として、この指令の実施のために採択された国内規定が発効する日に既にマニュアルのファイリングシステムにより実施されているデータ取扱いが、この指令の採択の日から12年以内にこの指令の第6条、第7 条及び第8条に合致させられなければならないことを定めることができる。ただし、構成国は、データ主体に対して、その請求により、及び特にデータ主体がアクセス権を行使する際に、不完全な、不正確な又は管理者によってなされる正当な目的とあいいれない方法により蓄積されたデータの修正、消去及びブロックを行う権利を保障しなければならない。

3. 構成国は、第2 項からの例外として、適切な保護措置に基づいて、歴史的調査の目的のためにのみ保存されるデータについては、この指令の第6条、第7条及び第8条の規定に合致させる必要がないことを定めることができる。

4. 構成国は、この指令の適用を受ける分野において採択された国内法の規定の文書を委員会に連絡しなければならない。

第33条

委員会は、第32条第1項に規定された日から少なくとも3年以内に、この指令の実施に関して、必要であれば、適切な修正案を添付して、理事会及び欧州議会に対して定期的に報告しなければならない。

委員会は、特に自然人に係る音声及び画像データの取扱いに関するこの指令の適用について調査し、情報通信技術の発展及び情報社会の進展状況に照らして必要であると考えられる適切な提案を提出しなければならない。

第34条

この指令は、構成国に発出される。

1995年10月24日 ルクセンブルグ

欧州議会議長

理事会議長