

I プライバシー・個人情報保護の国際的整合性— 特に独立個人情報保護機関設置の提唱

II プライバシー・個人情報保護の国際的整合性 と沖縄個人情報保護特区化法（仮称）の提案

一橋大学名誉教授 堀部 政男

I と II 共通

はじめに一連続シンポジウムについて

- 共通番号制と国民 ID 時代に向けたプライバシー・個人情報保護法制のあり方<課題と提言>
- 第1回シンポジウム（2010年8月21日（土）、東京大学情報学環福武ホール）
- 第2回シンポジウム（2010年10月9日（土）、一橋記念講堂）
- 第3回シンポジウム（2010年12月19日（日）、学術総合センター会議室）

プライバシー・個人情報論議の世界的展開の時期区分

- 第1期 プライバシー権の歴史的展開期
- 第2期 個人情報保護法議論期(1960年代)
- 第3期 個人情報保護法制定萌芽期(1970年代)
- 第4期 国際機関基準確立・個人情報保護法制定発展期(1980年代)
- 第5期 国際機関基準確立・個人情報保護法制定展開期(1990年代)
- 第6期 個人情報保護法制定拡大期(2000年代)
- 第7期 プライバシー・個人情報論議の展望

第4期 国際機関基準確立・個人情報保護法制定発展期(1980年代)

第5期 国際機関基準確立・個人情報保護法制定展開期(1990年代)

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）の堀部政男「Ⅱ EUデータ保護指令と個人データの国際移転」から

（1）EUデータ保護指令提案の背景

1) OECD プライバシー・ガイドラインの採択

ア プライバシー保護と情報の自由な流れ

EUデータ保護指令 (EU Data Protection Directive) として知られている EU (European Union, 欧州連合) の指令は、個人情報保護法の早期制定国、特に欧州におけるデータ保護法の考え方を反映したものであるといえる。

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である。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およ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。

イ OECD 理事会勧告 (1980年)

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¹。

¹ OECD プライバシー・ガイドラインなどについては、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)、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。

ウ 勧告の内容

OECD 理事会は、次のような認識を明らかにしている（邦訳は総務庁行政管理局（当時）の仮訳によるが、一部改訳したところもある）。

「1960年12月14日のOECD条約第一(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。」

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」、次のように勧告した。

- 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。

エ 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。

オ 8原則

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8原則は、日本でも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)

2) CoE 個人情報保護条約の締結

ア CoE と個人情報保護条約

日本が加盟国であるためか、OECD のプライバシー・ガイドラインについてはかなりよく知られているが、ほぼ同じ時期に採択された、欧州評議会(Council of Europe, 以下「CoE」という。)の個人情報保護条約はほとんど知られていない。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 개국 (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 (当時の加盟国は 21 개국であった)。そして、この条約は、翌 1981 年 1 月 28 日、各国の署名に付され、1985 年に、5 개국目の西ドイツ (当時) 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、ヨーロッパ諸国を基準とした、個人情報の国際水準を示しているもので、中身を見ておくことにする²。

イ 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 of 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 (邦訳は総務庁行政管理局 (当時) の仮訳によるが、一部改訳したところがある)。

² CoE についても、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)、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。

・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。」

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、目的明確化の原則および利用制限の原則に対応している。

次に、特別の種類 of 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採られていない限り、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。

ヨーロッパ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採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見てよいであろう。

・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採る」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ァイルの存在、その主たる目的、及びファイル管理者の身元、現住所、又は主たる事務所を確認することができる。
- b 合理的な期間でかつ過度な遅滞又は支出を伴うことなく、自己に関する個人データが自動処理データファイルに蓄積されているか否かを確認し、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。

ウ 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。

エ 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 transborder 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)

(2) EU データ保護指令提案

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えることができる。³

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

当時の欧州共同体 (European Communities, EC) 理事会 (Council) は、1990 年 7 月に、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、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

³ EU データ保護指令などについては、堀部政男「プライバシー・個人情報保護の国際的整合性」、堀部政男編著『プライバシー・個人情報保護の新課題』(商事法務、2010 年) 所収などを参照。

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。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。

ウ 第三国への個人データの移転—第 25 条

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り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。」

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。

エ 第 26 条 例外

第 25 条に続く「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。このような保護措置は、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) 充分性認定基準

ア 第 29 条作業部会の「作業文書」

日本にとって特に重要であるのは、「充分性」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「充分性」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。) という文書によっている。

WP 12 は、次のような章などからなっている。

序説 (Introduction)	p. 3
第1章 (Chapter 1) 「何が『十分な保護』を構成するか」 (What constitutes “adequate protection”?)	p. 5
第2章 (Chapter 2) 条約第108号を批准した諸国へアプローチの適用 (Applying the approach to countries that have ratified Convention 108)	p. 9
第3章 (Chapter 3) 産業界の自主規制へのアプローチの適用 (Applying the approach to industry self-regulation)	p. 11
第4章 (Chapter 4) 契約条項の役割 (The role of contractual provisions)	p. 16
第5章 (Chapter 5) 充分性要件の例外 (Exemptions from the adequacy requirement)	p. 26
第6章 (Chapter 6) 手続的論点 (Procedural issues)	p. 28
資料 (Annex 1) 例示 (Examples)	
資料 (Annex 2) [データ保護指令] 第25条及び第26条 (Articles 25 and 26)	

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。

ここで紹介したのは、WP 12 のほんの一部である。

イ 第 29 条作業部会の「十分性」評価と欧州委員会による認定国等

欧州委員会は、第 29 条作業部会が第一段階として WP 12 により評価したところに基づいて最終的に判断してきているが、これまでに、スイス (Switzerland)、カナダ (Canada)、アルゼンチン (Argentina)、アメリカ合衆国セーフハーバー・スキーム (the United States “safe harbor” scheme)、ガーンジー (Guernsey)、マン島 (Isle of Man)、ジャージー (Jersey)、フェロー諸島 (Faeroe Islands) について「十分性」の認定を行った。また、第 29 条作業部会は、2009 年 12 月 1 日に、イスラエル (Israel) 及びアンドラ (Andorra) について十分性を認める意見を採択した。

ウ オーストラリアに関する評価

これらに対し、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。（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）

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、一たび、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）。

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

NPP 1.3（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ない、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、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、個人情報収集の必要性、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。

4) 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 (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。

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 (European Commission Directorate-General-Justice, Freedom and Security) 法務政策部 (Legal Affairs and Policy) ユニットD5・データ保護 (Unit D5 -Data Protection) 事

務官 (Desk Officer) ハナ・ペチャコバ (Hana Pechackova)

- 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] ナミュール大学教授 (Prof. At the University of Namur) イブ・プレ (Yves Poulet) →当日、プレ教授が病気のため出席できなかったため、フランク・デュモルチエ (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・ディレクター (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

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。

女史のプレゼンテーションは、次のような構成になっていた (番号は、本稿で説明する便宜上ふった)。

- (1) プレゼンテーションの目的 (Goal of the presentation)
- (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)
- (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)
- (10) 十分性 (Adequacy)
- (11) 「十分な保護」の第三国 (“Adequate” 3rd countries)
- (12) 十分性: 結論 (Adequacy-conclusions)

これらのうちには、既に別稿で検討しているものも多いので、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、充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、充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「充分性」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。しかし、必ずしもそうではないと話も聞いていた。

このようなことを認識している私にとって、ペチャコバ女史が、公の会議で「充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。というのは、欧州委員会は、EUデータ保護指令に基づき、当初、自ら充分性認定手続を開始するとしていたからである。

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

- ・委員会は、第三国が十分なレベルの保護を確保していると認定することができる。
- ・このような決定の効果は、個人データが27のEU構成国及び3つの欧州経済領域(European Economic Area, EEA)(ノルウェイ、リヒテンシュタイン及びアイスランド)からその第三国へ、追加的な安全保護措置を必要としないで、流通することができることである。

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

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

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

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

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。

国民生活審議会「個人情報保護に関する取りまとめ（意見）」（2007年6月29日）からの抜粋

VII 国際的な整合性

(1) 現状

ア 個人情報保護における国際的な取組としては、1980年の「OECDプライバシー保護と個人データの国際流通についてのガイドライン」（以下「OECDガイドライン」という。）において示されている、いわゆる8原則が、以降の国際的な取組や各国における取組の基本となっている。我が国の個人情報保護制度もこのガイドラインに即したのものとなっている。

イ 国際連合では、「電子計算機処理に係る個人データ・ファイルに関するガイドライン」を1990年に採択している。

ウ OECDでは、OECDガイドラインに沿った取組を推進しており、最近では、プライバシー法執行の越境的な課題の検討を行っている。

エ 欧州連合（EU）では、「個人データ処理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」を採択している。この指令において、構成国は、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ことを定めなければならないとされている。

オ アジア太平洋経済協力（APEC）では、APECプライバシーフレームワークを2005年11月に策定し、越境的なプライバシー規則の構築等、EUとは異なる検討を行っている。

(2) 課題

個人情報保護には世界共通のインフラが必要であることから、国際的な枠組み等のグローバルな視点も重要である。

我が国の法律では、国際的な情報の移転に関する規律自体は明確に定められていないことについて、どのように考えるかとの指摘がある。

(3) 今後の検討方向

ア OECDでは、プライバシー法執行の越境的な課題が検討されており、APECでは、越境的なプライバシー規則の構築や、情報共有や調査・執行の越境協力の課題が検討されている等、国際的な取組が進められている。

イ OECD, APEC, EU等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、併せて我が国の個人情報保護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。

ウ 今後の我が国における個人情報保護制度を考えるに当たっては、我が国の制度や実態に加え、これらの国際的動向を十分に踏まえる必要がある。

VIII 第三者機関の意義

(1) 現状

ア 個人情報保護法において、第4章の個人情報取扱事業者の義務は、事業の用に供している個人情報が対象とされていることから、各事業等を所管する大臣が、主務大臣として、当該事業における個人情報の適正な取扱いについて、行政責任と権限を有するものとされている。

イ 平成19年5月31日現在、事業等を所管する各省庁により、22分野について35のガイドラインが策定され、主務大臣制の下、事業者等に対する指導・監督が実施されてきている。

ウ 平成19年5月31日現在、個人情報保護法第37条の規定に基づき、主務大臣が認定個人情報保護団体として認定した団体は、計34団体である。

(2) 課題

諸外国には、中立的な第三者機関が個人情報保護法を執行している例も多い。

(3) 今後の検討方向

我が国では、個人情報の取扱いは民間事業者の事業活動の一環として行われ、当該事業活動と不可分なものであるとともに、業種・業態に応じた様々な特性を有していることから、個人情報の適正な取扱いを十分に確保するためには、事業ごとのきめ細かい判断が不可欠であり、また、当該事業活動に関する事務と一体的に遂行することが合理的かつ実効的であると考えられる。

こうしたこと等から、当面、主務大臣制を維持することが妥当であると考えられ、第三者機関の設置については、国際的な整合性も踏まえ、中長期的課題として検討することが必要である。

(参考) 国際的には、第三者機関として、次の要件を充足することを求める例がある^注。

自主性・独立性や、適切な範囲の機能及びその実施の法的な権限による担保の観点から、我が国の機関がこの要件を充足することは困難であると考えられる。

- ① 適切な法的根拠に基づいて設置された公的機関であること。
- ② 所掌事務の遂行のために適切な水準の自主性・独立性が保証されていること。
自主性については、第三者機関が、法的・実務的に、第三者の許可を得ずに適切な措置を講じる権限を付与されていることが求められる。独立性については、第三者機関が政治的・行政的干渉を受けずに活動し、既得権益の影響に耐えることができるために重要である。
- ③ 所掌事務を定めている法律が、データ保護やプライバシーに関する国際的な枠組みに準拠していること。
- ④ 適切な範囲の機能を有しており、その実施が法的な権限により担保されていること。

データ保護の第三者機関は、法令順守、監督、調査、救済、指導及び公教育等の分野について、一連の機能を有する。第三者機関は、助言的な機能を有するだけでなく、法的・行政的な結果を伴う監督権限を有さなければならない。

注： 「資格に関する委員会の基準及び規則並びに認定の原則」(2001年9月25日データ保護コミッショナー国際会議採択(2002年9月9日データ保護プライバシーコミッショナー国際会議改定))による。

I プライバシー・個人情報保護の国際的整合性—特に独立個人情報保護機関設置の提唱

EU データ保護指令の主要な規定と日本の個人情報保護法との対比

(堀部政男編著『プライバシー・個人情報保護の新課題』(商事法務、2010年)から)

1 データ保護指令検討の必要性

欧州の関係者は当然のことながら EU データ保護指令ないしそれに準拠して制定された各国法を基準に照会・問合せ・質問等をするので、その指令については、日本でもより広く検討されなければならない。指令もかなり知られるようになったが、全体がどのようなになっているか、その中で、いくつか注目に値する規定がどのようなものかを見ることにする。それとともに、日本の個人情報保護法との対比も簡単に試みることにする。このような対比はほとんど行われていない。

全体の構成がどのようなになっているかについては前述したので、ここでは、いくつかの規定を見ながら対比をすることにしたい。

2 総則

ア EU データ保護指令

第 I 章総則の前に前文 [72 項にわたっている] があるが、これについては省略することにする。「第 I 章 総則」は、「第 1 条 指令の目的」、「第 2 条 定義」、「第 3 条 適用範囲」、

及び「第4条 適用される国内法」からなっている。

イ 個人情報保護法

個人情報保護法の「第1章 総則」は、「第1条 目的」、「第2条 定義」及び「第3条 基本理念」からなっている。

ウ 対比

EU データ保護指令にも個人情報保護法にも「総則」があり、「第1条 目的」と「第2条 定義」は形式的には共通にあるが、その構成は、異なる。

3 目的

ア EU データ保護指令の「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。

イ 個人情報保護法の「第1条 目的」の要旨

高度情報通信社会の進展に伴い個人情報の利用が著しく拡大していることにかんがみ、個人情報の適正な取扱いに関し、一定の規定を設けることにより、個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的としている。

ウ 対比

EU データ保護指令の名宛人は、構成国であるので、構成国に一定の義務付けをしている。その第1項は、「・・・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権を保護しなければならない」と「個人データの取扱い」との関係で、「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」(fundamental rights and freedoms of natural persons, and in particular their right to privacy) を保護することを義務付けている。

個人情報保護法の「個人の権利利益」の保護よりも、具体的であり、また、プライバシー権を明示しているところに違いがある。

日本の政府レベルでプライバシーについて総合的に検討した最初の研究会である、行政管理庁（当時）のプライバシー保護研究会は、1982年7月にまとめた報告書を「個人データの取扱いに伴うプライバシー保護対策」と題した。私は、この研究会の最年少のメンバーとして、当時、世界のプライバシー保護に関する動向などについて研究したが、報告書のタイトルの「個人データの取扱い」は、EU データ保護指令の「個人データの取扱い」(processing of personal data) と同じである。EU データ保護指令と同様にとらえ方をしたことがあることに注目されたい。

個人情報保護法は、「個人情報の有用性」と「個人の権利利益の保護」とのバランスをとることを目的としている。EU データ保護指令は、EU 構成国に適用されるので、第2項は

「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、構成国の中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」と、「構成国の中の個人データの自由な流通」の制限又は禁止をしないように義務付けている。この考え方は、OECD プライバシー・ガイドラインと同じである。

4 定義

ア EU データ保護指令の「第 2 条 定義」

この指令の目的に関して、

(a) 「個人データ」(personal data) 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。)(processing of personal data(“processing”))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、整理又は結合、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。)(personal data filing system(“filing system”))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」(controller)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」(processor)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」(third party)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」(recipient)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」(data subject’s consent)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

つ十分に情報を提供された上での意思表示をいう。

イ 個人情報保護法の「第2条 定義」の要旨

- ・「個人情報」—生存する個人に関する情報（識別可能情報）

個人情報保護法では、この「個人情報」と後掲の「個人データ」、「保有個人データ」と区別している。それぞれで適用規定が異なる。

第4章の個人情報取扱事業者の義務等の規定のうち、「個人情報」は、次の規定に出てくる。

第15条（利用目的の特定）、第16条（利用目的による制限）、第17条（適正な取得）、第18条（取得に際しての利用目的の通知等）、第31条（苦情の処理）

- ・「個人情報データベース等」—個人情報を含む情報の集合物（検索が可能なもの。一定のマニュアル処理情報を含む。）

・「個人情報取扱事業者」—個人情報データベース等を事業の用に供している者（国、地方公共団体等のほか、取り扱う個人情報が少ない等の一定の者（特定の個人数が過去6ヶ月以内のいずれの日においても5,000人を超えない者）を除く。）

- ・「個人データ」—個人情報データベース等を構成する個人情報

第4章の個人情報取扱事業者の義務等の規定のうち、「個人データ」は、次の規定に出てくる。

第19条（データ内容の正確性の確保）、第20条（安全管理措置）、第21条（従業員の監督）、第22条（委託先の監督）、第23条（第三者提供の制限）

- ・「保有個人データ」—個人情報取扱事業者が開示、訂正等の権限を有する個人データ

第4章の個人情報取扱事業者の義務等の規定のうち、「保有個人データ」は、次の規定と関連している。

第24条（保有個人データに関する事項の公表等）、第25条（開示）、第26条（訂正等）、第27条（利用停止等）、第28条（理由の説明）、第29条（開示等の求めに応じる手続）、第30条（手数料）

- ・「本人」—個人情報によって識別される特定の個人

ウ 対比

定義規定を見ると、その法律で使われている主要な概念が明らかになる。一つ一つを対比することはしないが、EUデータ保護指令では、「個人データ」（personal data）及び「個人データ・ファイリングシステム」（personal data filing system）という概念を使っているのに対し、個人情報保護法では、「個人情報」、「個人データ」、及び「保有個人データ」を区別している。

また、EUデータ保護指令では、「管理者」（controller）については、前述のように、「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」となっている。これに相当するのは、個人情報保護法では、「個人情報取扱事業者」であり、その範囲は、かなり狭い。

5 特別な種類の取扱い

ア EU データ保護指令

(ア) 特別な種類のデータの取扱い

EU データ保護指令は、「第Ⅱ章 個人データの取扱いの適法性に関する一般準則」で、「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 5 条）として、「第Ⅰ節 データ内容に関する原則」、「第Ⅱ節 データ取扱いの正当性の基準」及び「第Ⅲ節 特別な種類の取扱い」の各節の 1 つで、「特別な種類のデータの取扱い」に関する第 8 条 が、次のように規定している。

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。

(イ) 表現の自由

「個人データの取扱いと表現の自由」に関する第 9 条は、次のように規定している。

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、ジャーナリスティックな目的又は芸術上、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。

イ 個人情報保護法

個人情報保護法には、「特別な種類のデータの取扱い」に該当する規定はない。しかし、「表現の自由」にかかわる規定は、「第 4 章 個人情報取扱事業者の義務等」の適用を除外する形で、「第 5 章 雑則」の中の第 50 条が、次のような趣旨の規定となっている。

・報道、著述、学術研究、宗教活動、政治活動の用に供する目的で個人情報を取り扱う報道機関、著述を業として行う者、学術研究機関等、宗教団体、政治団体については、第 4 章の適用を除外（第 50 条第 1 項）

・これらの主体は、安全管理、苦情処理等のために必要な措置を自ら講じ、その内容を公表するよう努力（第 50 条第 3 項）

ウ 対比

EU データ保護指令で規定されているものが個人情報保護法では規定されていない場合がいくつかあるが、この「特別な種類のデータの取扱い」もその 1 つである。しかし、表現の自由との関係は、個人情報保護法にも規定されている。もともと、個人情報保護法は、報道機関ばかりでなく、著述を業として行う者、学術研究機関等、宗教団体、政治団体については、第 4 章の適用を除外している。

個人情報保護法ではないが、日本でも、JIS Q 15001 : 1999、それにとって代わった JIS

Q 15001 : 2006 において、「機微な個人情報」について規定している。

6 第三国への個人データの移転

ア EU データ保護指令の「第三国への個人データの移転」

(ア) 第 25 条 原則

EU データ保護指令は、章立ての 1 つとして、「第 IV 章 第三国への個人データの移転」を掲げ、「第 25 条 原則」及び「第 26 条 例外」について規定している。

「第 25 条 原則」は、次のように規定している。

1. 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。
2. 第三国によって保障される保護のレベルの充分性は、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、発信国及び最終目的国、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、並びに当該国において遵守されている専門的規範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。

(イ) 第 26 条 例外

「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。このような保護措置は、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。

イ 個人情報保護法

個人情報保護法は、第三国への移転については規定していない。

ウ 十分性評価基準

(ア) EU データ保護指令による評価

第三国へのデータの移転に関する規定は、日本にとっても重要な意味を有するので、これを再掲することにする。

「諸原則」(Principles)に関する第 25 条は、最初の指令提案の第 24 条の「諸原則」とは少し異なっている(「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。」

ここでは、日本の状況を念頭において、分析してみることにする。

(1) 「あらゆる状況にかんがみ評価されなければならない」ということで、個人情報保護法のみが評価の対象になるわけではない。

(2) 考慮されるものとして、法規範を中心に見るならば、「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）」が対象になる。

① 「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）は、日本という第三国で有効である一般的法規範である個人情報保護法、また、分野別を行政分野・独立行政法人分野、地方公共団体分野などと解釈すると、行政分野の行政機関個人情報保護法、独立行政法人分野の独立行政法人等個人情報保護法、地方公共団体の個人情報保護条例などをあげることができる。さらに、分野を限定するならば、住民基本台帳関係情報、戸籍関係情報はそれぞれ住民基本台帳法及び戸籍法ということになる。ここでは、日本について見ているが、EU データ保護指令が主として意識しているのは、アメリカの状況であるといえる。そのため、現在の日本の状況に当てはめるのは容易ではない。

② 「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）」は、法が適用されない分野を意味しているように解釈することもできる。例えば、報道機関の専門的規範（professional rules）は、これに当たると見ることができる。個人情報保護法制定以前は、事業分野別のガイドラインなどもこれに相当するということできたが、個人情報保護法制定後の関係省庁ガイドラインは個人情報保護法に根拠があるので、この範疇に入らないと見るべきであろう。

プライバシーマーク制度については、どのように見るか。安全保護対策措置（security measures）も含めて、この範疇に属するといえるであろう。

ここでも、日本について見ているが、EU データ保護指令が主として意識しているのは、

アメリカの状況であるといえる。そのため、現在の日本の状況に当てはめるのは容易ではない。

③問題は、内容面である。ここにあげたものが、EU データ保護指令に照らして内容的に十分性を有するかどうかである。これについては、特に個人情報保護法の内容を EU データ保護指令と詳細に比較検討しなければならない。それについては、別途、検討することにした。

(イ) 第 29 条作業部会の「作業文書」による「十分なレベルの保護」の評価基準

EU データ保護指令第 29 条については後述するが、第 29 条は、「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」(Working Party on the Protection of Individuals with regard to the Processing of Personal Data) について規定している。その作業部会が 1998 年 7 月 24 日に採択した「個人データの第三国への移転：EU データ保護指令第 25 条及び第 26 条の適用」(Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive) と題する「作業文書」(Working Document) (WP12) というものがある。意外に知られていないが、「十分なレベルの保護」の評価基準を示したものとして重要である。これについては、後述する。

7 監督機関

ア EU データ保護指令の監督機関

EU データ保護指令は、「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」において、「第 28 条 監督機関」、「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」及び「第 30 条 【作業部会の所掌事項】」について規定している。そのうち、監督機関に関する第 28 条は、次のようになっている。

1. 各構成国は、一つ又は二つ以上の公的機関が、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。

—取扱い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い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。

イ 個人情報保護法の監督機関—主務大臣に関する規定の要旨

個人情報保護法では、監督機関という概念ではとらえていないが、EU データ保護指令の監督機関に当たるのは、主務大臣である。それに関する規定の要旨は、次のようになっている。

(ア) 主務大臣の関与 (第 32 条～第 35 条)

- ・この節の規定の施行に必要な限度における報告の徴収、必要な助言
- ・個人情報取扱事業者が義務規定(努力義務を除く)に違反し、個人の権利利益保護のため必要がある場合における勧告、勧告に従わない一定の場合の命令等
- ・主務大臣の権限の行使の制限(表現、学問、信教、政治活動の自由)

(イ) 主務大臣 (第 36 条)

- ・個人情報取扱事業者が行う事業等の所管大臣、規定の円滑な実施のために必要があるときは、内閣総理大臣が指定

ウ 対比

EU データ保護指令に規定されている監督機関は、上掲の第 28 条から分かるように、独立性の強いものであって、個人情報保護法における行政機関の長としての主務大臣とは基本的に異なる。これは、公的部門をも監督する権限を有することとも関連している。日本では、行政機関個人情報保護法にも、独立行政法人等個人情報保護法にも、監督機関がなく、その点も異なる。

前述の「一般的な法規範」に相当する個人情報保護法が規定する主務大臣制は、EU データ保護指令でいう監督機関を有しないということから内容的に充分性の要件に欠けると判断されるおそれがある。また、「分野別の法規範」である行政機関個人情報保護法、独立行

政法人等個人情報保護法には監督機関の規定もなく、個人情報保護法と同様に判断されることになるであろう。

8 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

ア EU データ保護指令の「第 29 条作業部会」(注)

EU データ保護指令第 29 条は、前述のように、「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」について、次のように規定している。

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。

イ EU データ保護指令の作業部会の「作業部会の所掌事項」

EU データ保護指令第 30 条には条文見出しはないが、前述のように【作業部会の所掌事項】と名付けることができる。それは、次のようになっている。

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。

ウ 個人情報保護法

個人情報保護法には、EU データ保護指令の作業部会に相当する機関はない。

エ 対比

EU データ保護指令と個人情報保護法とは、基本的な発想が異なるので、対比することが困難な面もあるが、この作業部会もその一つである。EU データ保護指令第 30 条第 1 項にあるように、この作業部会が、「(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」になる。

II プライバシー・個人情報保護の国際的整合性と沖縄個人情報保護特区化法（仮称）の提案

EU データ保護指令及び e-プライバシー指令について（再掲）

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）の堀部政男「II EU データ保護指令と個人データの国際移転」から

「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。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。これは、e-プライバシー指令(e-Privacy Directive)と呼ばれることがある。

EU指令を参照した日本の個人情報保護ガイドラインの例

EU データ保護指令

・通商産業省「民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン」(1997年3月4日通商産業省告示第98号)【1989年通産省ガイドラインの改正】

e-プライバシー指令(電気通信指令)

・郵政省「電気通信事業における個人情報保護に関するガイドライン」(1998年12月2日郵政省告示第570号)【1991年郵政省「電気通信事業における個人情報保護に関するガイドライン」(9月)の改正】

これらの経験から、当面、次のようなことが考えられる。

- ・EU データ保護指令のレベルを満たす「沖縄個人情報保護特区化法(仮称)」の検討
- ・同様の「沖縄県個人情報保護特区化法(仮称)」の制定
- ・体制整備、特に個人情報保護独立監視機関の設置
- ・EU に審査要請
- ・クラウドコンピューティング時代の適合的なデータセンターの振興
- ・個人情報保護特区の沖縄の情報産業の高度化→情報産業の発展

別添参考資料

・堀部政男 「『個人情報保護』先進国への必須条件 独立監視機関設置に期待」 ビジネス法務 2009年10月号。

第6期 個人情報保護法制定拡大期(2000年代)

別添参考資料

・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 2010年3月号。

第7期 プライバシー・個人情報論議の展望

OECD プライバシー・ガイドラインの検討

EU データ保護指令の検討、2010年11月ころにはその結果公表予定