

2009 年度卒業論文

山田正雄ゼミナール

グローバルな視点から見た個人情報保護法

～国際的個人情報保護の基準に関する一考察～

日本大学法学部 政治経済学科 4年

学籍番号：0620290

齊藤 徹

はじめに

1990年代以降、インターネットの登場とその普及により、世界中でやり取りされる情報量とそのスピードは確実に増大し今なおそれは増え続けている。その中でも個人情報というものが官公庁、教育機関、企業組織などさまざまな場面で扱われおり、われわれの生活に深くかかわっている。そうした中でファイル共有ソフトの安易な利用や、個人情報を顧客から預かっている組織の不注意、悪意ある行為により個人情報が流失する事件が後を絶たない。日本では2005年に「個人情報保護に関する法律」(以下個人情報保護法)が制定された。これは「個人情報の有用性」と「個人の権利利益の保護」を目的として施行された法律である。しかし、個人情報のやり取りは日本国内だけでなく、他国の組織とICTを通して行われるケースがあり、増えてきている。

そして、日本における個人情報保護法には世界的視点から見て国際的基準が満たされていないのではないかとされており、他国と個人情報をやり取りするときに経済面など様々な障害が発生する可能性がある。

本論文では1988年に宣言されたOECDプライバシー・ガイドラインをはじめ、EUデータ保護法、モントルー宣言などの国際的ガイドライン・法律を検証し、個人情報に深くかかわるプライバシーの研究が進んでいるアメリカ、EU(特に独立した監督機関がいち早く導入したイギリス)の例を取り上げ、日本における個人情報保護法の国際的基準を満たすにはどのようにすれば良いか考察していきたいと思う。

はじめに

- 目次 -

1 日本における個人情報保護法

- 1.1 個人情報とは
- 1.2 個人情報保護法の形式
 - 1.2.1 セグメント方式
 - 1.2.2 旧行政機関法
 - 1.2.3 個人情報保護法
 - 1.2.4 行政機関個人情報保護法
 - 1.2.5 独立行政法人等個人情報保護法
 - 1.2.6 個人情報保護指令
- 1.3 個人情報保護の監督制度

2 国際的個人情報保護基準の歴史

- 2.1 OECD プライバシー・ガイドライン
 - 2.1.1 収集制限の原則
 - 2.1.2 データ内容の原則
 - 2.1.3 目的明確化の原則
 - 2.1.4 利用制限の原則
 - 2.1.5 安全保護の原則
 - 2.1.6 公開の原則
 - 2.1.7 個人参加の原則
 - 2.1.8 責任の原則
- 2.2 EU 個人保護指令
- 2.3 モントルー宣言

3 EUの個人情報保護法

- 3.1 個人情報保護法の形式
 - 3.1.1 オムニバス方式
- 3.2 イギリスの例
 - 3.2.1 1984年データ保護法
 - 3.2.2 1998年データ保護法
 - 3.2.3 個人情報保護法の監督制度

4 アメリカの個人情報保護法

- 4.1 個人情報保護法の形式
 - 4.1.1 セクトラル方式
- 4.2 公的部門のプライバシー保護法
- 4.3 民間部門のプライバシー保護法

4.4 個人情報保護法の監督制度

4.4.1 セーフ・ハーバー協定

4.4.2 セーフ・ハーバー原則

5 今後の展望～日本における独立した第三者機関の行方～

むすびにかえて

参考文献・URL

1 日本における個人情報保護法

1.1 個人情報とは

個人情報とは「個人情報の保護に関する法律」(以下個人情報保護法とする)第2条1項で「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できるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。)」と定義されている。

この定義を要約すると個人情報とは生存者の個人識別情報と言える。これを具体的に構成する要件は①生存する、②個人に関する情報であって、③特定の個人を識別できるもの(すなわち個人識別性のあるもの)という3要件を満たす必要がある。この3要件を満たす情報が個人情報に該当する。この情報がコンピュータ処理の対象となっているか(電算処理情報)、コンピュータ処理の対象外であるか(マニュアル処理情報)を問わない。たとえ顧客から受け取った名刺1枚でも個人情報となりうる。

先ほど述べた3要件について詳しく論ずる。

「①生存する」とは個人であっても死者や実在しない人物に関する情報は個人情報に該当しない。個人情報保護法は、開示の求めをはじめ本人関与を認める複数の規定を置いており、これらの規定は本人が生存する者であってはじめて可能になるものであることから、死者は除外される。架空の人物に関しても同じである。

次に「②個人に関する情報」とはまず「個人」とは自然人である。そして「個人」に関するものに限られるわけであるから、各都道府県が有する面積のような「個人」に関しない情報は個人情報保護法では含まれない。企業の本支店の所在地情報、他社との取引内容等の法人その他の団体それ自体に関する情報(団体情報)も個人情報に該当しない。しかし、ある情報の内容が団体情報に該当するときでも、団体の役員情報のように、その情報が同時に要件を満たす場合には当該部分の情報は個人情報に該当する可能性はある。本法は「個人」が日本国籍・国内住居者であることを要件にしない。

したがって、外国人の情報も含まれ、国外住居者の情報も含まれる。ただし、これらの個人情報は日本国内で取り扱われるに限りにおいて本法の対象になる。そして、「個人」に関する情報とは、個人の属性に関する情報の全てをいう。その情報の存在する形式は文字等に限定してはなく、例えば防犯カメラの映像や、音声録音されたメディアなども該当しうる。

そして「③特定の個人を識別できるもの(個人識別性)」について、すなわち個人識別性を有する情報は、ただ単に氏名だけの記述のみでは個人識別性に欠き、他の情報と照合することにより個人識別性が確立される。この他の情報の具体的例として生年月日、住所、電話番号、印影、口座番号、クレジットカード番号、職業、ICカードの番号、パスワード等、特定の個人の属性や所有物、関係事実等を表す情報である。^{注1}

1.2 個人情報保護法の形式

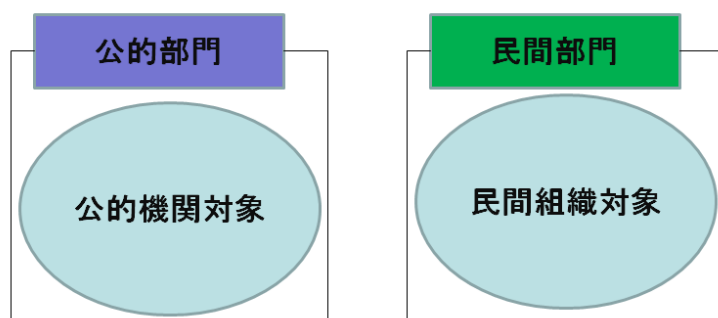
個人情報を保護する法律は世界各国で定められているが、その国々においてその形式は違ってくる。その形式は主にセグメント方式、オムニバス方式、セクトラル方式の3つが挙げられる。

日本はその中でもセグメント方式を採用している。この章ではその日本における個人情報保護法の種類とその形式、個人情報保護法が規定する領域について考察していく。

1.2.1 セグメント方式

セグメント方式とは個人情報を保護する法律の制定方式の1つで、公的部門と民間部門を別の法律で規律する形式である。これは後述する「行政機関の保有する電子計算機処理に係る個人情報保護に関する法律(以下「旧行政機関保護法」)」が制定されたときに見られた形式である。(図表.1)

セグメント方式



(図表.1)筆者作成

1.2.2 旧行政機関保護法

「行政機関の保有する電子計算機処理に係る個人情報保護に関する法律(以下「旧行政機関保護法」)」は1988年に制定された法律である。これは国レベルで初めて施行された個人情報の保護に関する法律である。地方公共団体レベルでは1973年6月に徳島市が「電子計算処理に係る個人情報の保護に関する条例」が施行されたがこれはコンピュータ処理に主眼を置いたものであった。そして1975年3月には国立市「電子計算組織の運営に関する条例」、1985年6月の川崎市「個人情報保護条例」と相次いで成立した。

都道府県レベルでは神奈川県が初めて1990年3月に「個人情報保護法条例」を公布した。その後次々と各地方自治体は個人情報保護条例を制定していき、2006年には47都道府県すべてが個人情報保護条例を制定している。

こうしたものの背景には1970年代以降、行政機関が保有する住民基本台帳等に見られる個人情報を電子化するという流れがある。当初の条例は電子計算処理に関する個人情報保護を内容としていたが、川崎市の条例以降、マニュアル処理情報を対象にする条例が現れるようになり、神奈川県条例では初めて民間部門をも規制対象とする傾向も見られた。

そうした中で1988年に「旧行政機関保護法」が制定された。

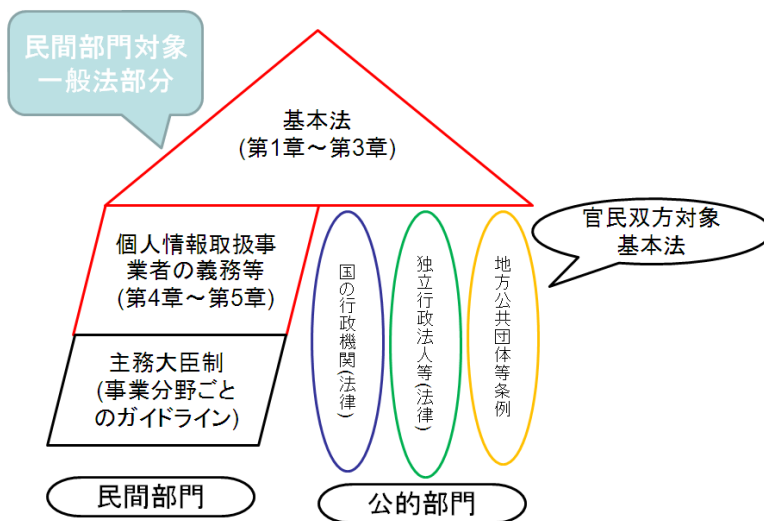
しかし、この法律はコンピュータ処理情報の「個人情報ファイル」^{注2}のみを対象としていること、思想・信条や医療情報などのセンシティブ・データの収集制限規定が存在しないこと、個人情報の訂正等は申出制度に過ぎず法的な訂正請求権は認められていないなど、個人情報保護の観点からは不十分な点が多く見られていた。また、後述するOECDプライバシー・ガイドラインでは民間部門を排除しているわけではないが、民間部門の規制は時期尚早と当時の政府は判断し、行政に対する国民の信頼確保の一方策として、行政機関法のみが制定された。

1.2.3 個人情報保護法

旧行政機関保護法が施行され、その後1990年代に入るとインターネットの普及による高度情報化社会へと進展、住民基本台帳法の改正による国民総背番号制への懸念、後述のEU個人保護指令の「十分なレベルの保護」の問題、国内における個人情報漏えい事件の多発といった状況を受けて2003年に「個人情報保護に関する法律(以下個人情報保護法)」が制定され、2005年に全面的に施行された。この法律「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。

個人情報保護法は全6章で構成されていて第1章から第3章は基本法、第4章以降は一般法となっている。個人情報保護法は旧行政機関法と違い公的部門だけでなく民間部門に関しても規制する。その点だけでなく、旧行政機関法で見られたセクトラル方式を採用せず、基本法では官民双方を規制する基本的な項目を作り、第4章以降の一般法で民間部門に関して個別に規定するという方式を取った。これは後述するEU諸国で見られるオムニバス方式、アメリカで見られるセグメント方式とは一線を画した方式である。(図表.2)

個人情報保護に関する法体系イメージ



(図表.2)『消費者庁・個人情報保護に関する法体系イメージ』を参考にし、筆者作成

第1章から第3章で構成されている基本法とは第1章総則(目的・定義・基本理念)、第2章国及び地方公共団体の責務等、第3章個人情報保護に関する施策等を定めている。

第1章総則の目的(第1条)では先にも述べたとおり、「個人情報の有用性」と「個人の権利利益の保護」を目的とするとしている。定義(第2条)ではその対象情報と対象者を定めている。対象情報は大まかに「個人情報」「個人データ」「保有個人データ」と区別している。最も基本となる定義は「個人情報」である(p4参照)。「個人データ」は、検索可能な個人情報の集合(個人情報データベース)を構成する情報であり、コンピュータ情報のみならず、マニュアル情報も含まれる。「保有個人データ」は、「個人データ」の中でも、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となる。また、その適用対象となる者すなわち対象者は個人情報取扱事業者である。この個人情報取扱事業者とは個人情報データベース等を事業の用に供している者であって、国、地方公共団体等のほか、取り扱う個人情報が少ない一定のもの(特定の個人の数が過去6ヶ月以内のいずれの日においても5000人を超えない者)を除いた者である。

第1章総則の第3条では「基本理念」を定めている。ここでは「個人情報は、個人の人格尊重の理念の下に慎重に取り扱われるべきものであることにかんがみ、その適正な取扱いが図られなければならない」とされている。これは、個人情報保護法の理念が、憲法第13条の個人の尊厳に由来することを謳っている。

第2章は、第4条から第6条で構成されている。第4条は「国の責務」、第5条は「地方公共団体の責務」、第6条は「法制上の措置等」を定めている。このうち、第6条は、第1項で旧行政機関法の改正、第2項で後述する独立行政法人等個人情報保護法の法制化を定めていたが、実現されたことから削除された。現在は「政府は、個人情報の性質及び利用方法をかんがみ、個人の権利利益の一層の保護を図るため特にその適正な取扱いの厳格な実施を確保する必要がある個人情報について、保護のため格別の措置が講じられるよう必要な法制上の措置その他の措置を講ずるものとする」という定めがあり、これは個別法の根拠規定である。この個別法とは医療や金融・信用、情報通信等のセンシティブ・データに対する分野別の法律であり、衆議院および参議院の各個人情報の保護に関する特別委員会で議論になっており早急な検討を謳っている。

第3章は第7条から第14条から構成されている。

第7条では「個人情報の保護に関する基本方針」について定められており、先ほども記したように個人情報保護法が憲法上の個人の尊厳に基づくことを明らかにしている。

第8条から第10条は「国の施策」について定めている。例えば地方公共団体への支援、苦情処理のための措置、個人情報の適正な取扱いを確保するための措置である。

第11条から第13条は「地方公共団体の施策」について定められており、地方公共団体等が保有する個人情報の保護、苦情処理のあっせんなどが定められている。

第14条は「国及び地方公共団体の協力」について定めている。これは「国及び地方公共団体は、個人情報の保護に関する施策を講ずるにつき、相協力するものとする」と定めてい

る。

以上が基本法と呼ばれる第1章から第3章の部分である。

次に4章以降で構成されている一般法と呼ばれる部分である。

この一般法部分では第4章個人情報取扱事業者の義務等、第5章雑則、第6章罰則を定めている。

第4章では後述するOECDプライバシー・ガイドラインを念頭に置き、個人情報の利用目的の特定や制限、個人情報を取得する際の適正な方法によるものとする定めや第三者提供に関する制限を設けている。また、公表等、開示、訂正等、利用停止等など、個人情報取扱事業者は取り扱う保有個人データを本人の知りえる状態に置かなければならず、開示を請求されればそれに応えなければならない義務を負う、保有個人データの内容が事実と異なり訂正を求められたら調査しその結果に基づき当該保有個人データの内容の訂正等を行うことを義務付けられている。そして個人情報取扱事業者は本人から当該本人が識別される保有個人データが本法16条(利用目的による制限)に違反して取り扱われるという理由または本法(適正な取得)に違反して取得されたものであるという理由によって、当該保有個人データの利用停止等を求められた場合に、その求めに理由があることが判明したときは、違反を是正するために必要な限度で遅滞なく当該保有個人データの利用停止等を行わなければならない。これを利用停止等の求めといい、利用停止等とは、利用の停止または消去を総称する用語である(本項かつこ書)。

また、民間団体による個人情報の保護の推進も定めており、認定個人情報保護団体^{注2}に関する所定の認定業務を規定している。

第5章では本法が目的とする「個人情報の有用性」と「個人の権利利益」を保護することの中で、個人情報の有用性を実現する規定である。憲法の保障を受ける報道の自由、表現の自由、学問の自由、信教の自由、政治活動の自由等を損なわないようにすることを趣旨としている。

第6章では罰則についてである。罰則は間接罰である。違反行為があった場合、まず自主的な是正が求められ、主務大臣から、助言、勧告、命令があり、個人情報取扱事業者が命令に従わないときに初めて罰則が適用される。具体的には、主務大臣の命令に違反した個人情報取扱事業者は、6月以下の懲役又は30万円以下の罰金に処せられる(第56条)。また、報告義務に違反した個人情報取扱事業者又は認定個人情報保護団体は、30万円以下の罰金に処せられる(第57条)。その他、両罰規定も設けられている。(第58条)。

1.2.4 行政機関個人情報保護法

正式名称は「行政機関の保有する個人情報の保護に関する法律(以下行政機関個人情報保護法)」である。これは2005年に施行され、前述の旧行政機関法を全面改正し、これを充実・強化したものである。本法は、「行政の適正かつ円滑な運営を図りつつ、個人の権利利益を保護することを目的」としている(本法第1条)。旧行政機関法のように電子計算機処理

情報に限定することなく、個人情報保護法と同様にマニュアル処理情報を含めて対象情報とした。これは個人情報保護法の基本法部分(個人情報保護法第1章から第3章)の下において、国のすべての行政機関を対象機関とする一般法として、行政機関における個人情報の取扱いに関する基本的事項を定める法律である。

1.2.5 独立行政法人等個人情報保護法

正式名称を「独立行政法人等の保有する個人情報の保護に関する法律(以下独立行政法人等個人情報保護法)」といい、2003年5月に国会で新法として可決成立し、2005年4月に施行された。本法は独立行政機関等を対象機関とする一般法としての役割を担っている。独立行政法人等が保有する個人情報の保護を図るために独立行政法人等における、保有する個人情報の取扱いに関するルールを明らかにする法律である。対象とする法人は政府の一部を構成するとみられる法人であり、独立行政法人等情報公開法の対象法人と同様である。

1.2.6 個人情報保護条例

地方公共団体における個人情報保護は、地方公共団体自ら制定する個人情報保護条例を中心に図られてきた。古くは1970年代前半からで、行政が個人情報を電子処理するのを推進してきたことにより個人情報保護に関する規制が注目されてきた。この地方公共団体の個人情報保護条例は個人情報保護法の基本法部分(第1章～第3章)が適用される。しかし、個人情報保護法の一般法部分(第4章～第6章)については、地方公共団体個人情報取扱事業者から明文で除外されているため(同法第2条2項3号)、第4章の義務の名宛人とならず、適用されない。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の対象ともならない。

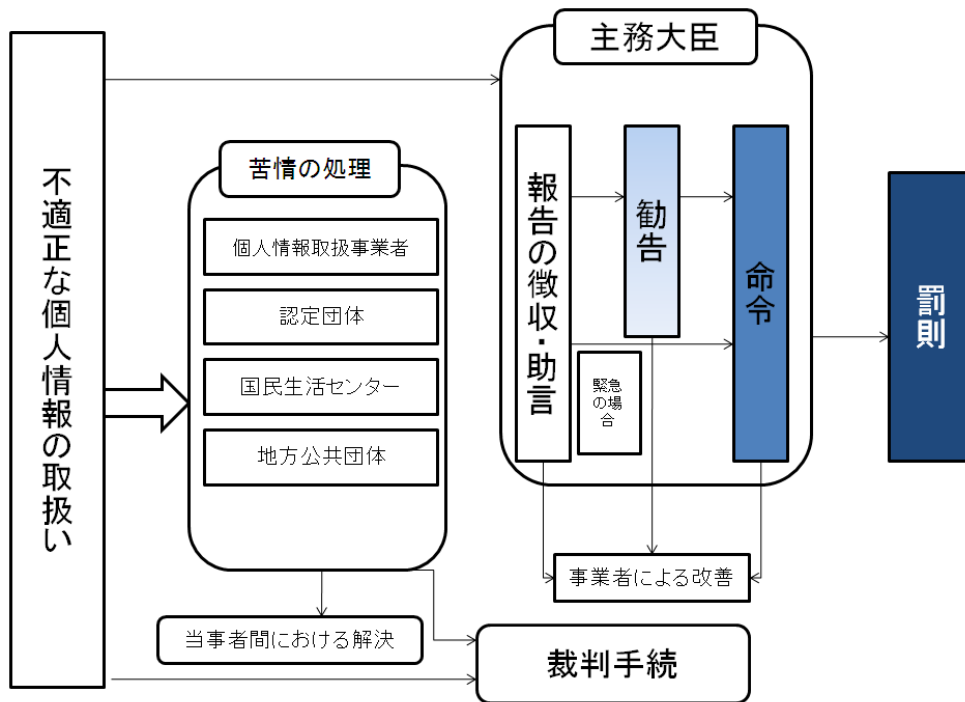
地方公共団体は、その保有する個人情報について、自ら制定する個人情報保護条例により規律を加えてきたが、同法11条1項に基づき、その保有する個人情報の性質、当該個人情報を保有する目的等を勘案し、その保有する個人情報の適正な取り扱いが確保されるよう必要な措置を講ずることに努めなければならないことから、地方公共団体は、個人情報保護法の基本法部分に即して、個人情報保護条例の整備等を行うべきこととなっている。

地方公共団体は自ら保有する個人情報の保護の推進を図る地位にあるだけでなく、その区域内の事業者および住人に関し施策を講じるべき地位にあると定められている(同法第12条)。また、業者と本人との間に生じた苦情が適切かつ迅速に処理されるようにするため、苦情の処理のあっせんその他必要な措置を講ずるよう努めなければならない(同法第13条)。

1.3 個人情報保護の監督制度

ここでは日本における個人情報の保護が適正かつ実効的な規制の実現を目指す第三者機関について論ずる。個人情報保護法では主務大臣を監督機関としての地位を置き、個人情

報取扱事業者に対し報告徴収・助言・勧告および命令を行うことができる(個人情報保護法第 32 条～第 36 条)。しかし立入検査は認められていない。(図表.3)



(図表.3)

『消費者庁ホームページの個人情報保護法の解説(実効性担保も仕組み)』を参考に筆者作成

主務大臣の監督機関としての主な機能として、もし不適正な個人情報の取扱いが行われた場合、まず個人情報取扱事業者に対して報告徴収および助言が行われる。報告徴収とは個人情報の取り扱いに関してこれを報告させることができ(同法第 32 条)、助言とはそれに対して必要な助言をすることを定めている(同法第 33 条)。これは、後述の勧告。命令とは異なり違反行為の存在を要件としておらず「施行に必要な限度」であれば行うことができる。「施行に必要な限度」とは本法第 4 章第 1 節に規定されている。本節が保護しようとする個人の権利利益を侵害するおそれが認められず、もしくは、そのおそれが少ないものと認められた場合には、「施行に必要な限度」という要件に該当せず、報告徴収・助言の対象外になりうる。

次に勧告とは、個人情報取扱事業者が義務規定(努力義務や個人情報取扱事業者の便宜を図った規定を除く)に違反し、個人の権利利益保護のために必要がある場合に、違反行為の中止等を個人情報取扱事業者に対してすることである(同法第 34 条第 1 項)。

また命令は、勧告を受けた個人情報取扱事業者が、正当な理由なく勧告に従わず、個人の重大な権利利益の侵害が切迫していると認められる場合に下すことができる(同法第 34 条第 2 項)。しかし、利用目的による制限(同法第 16 条)、適正な取得(第 17 条)、安全管理措置等(第 20 条ないし第 22 条)、第三者提供の制限(第 23 条第 1 項)の違反があった場合で、

緊急性が認められるときは、勧告を経ずに命令を下すことができる(第34条第3項)。もし命令に従わなかった場合、6カ月以下の懲役または30万円以下の罰金が科せられる(第56条)。

主務大臣が個人情報保護法に基づく勧告を下した初のケースは、みちのく銀行の事件である。当時の金融庁は、2005年5月20日、約130万件の顧客情報の入ったCD-ROMを紛失したみちのく銀行に対して、個人データの安全管理のための措置の実効性確保、個人データの安全管理を図るための従業者に対する監督の徹底を勧告した。

なお、命令を下したケースは2010年1月現在まではまだ存在していない

注釈

[1] このような具体的な個人情報(氏名、生年月日、口座番号など)だけでなく、インターネット上の行動様式を表すような情報、例えばAmazonなどにアクセスした際のアクセスログの記録や、消費者としての行動、購買履歴なども個人情報として扱われるケースもある。

[2] 主務大臣によって認定された個人情報取扱事業者の個人情報の適正な取扱いの確保を目的とし、認定業務を行う団体。

2 国際的個人情報保護基準の歴史

ICTの飛躍的な発達に伴って、個人情報の保護の必要性が注目され、世界各国では1970年代に入るとそれに対応するため法律整備をし始めた。その中で、特にヨーロッパの法律には、個人情報の国外処理を制限する条項を設けているものが多く存在した。そのような制限条項は、自国民のプライバシー保護、個人情報の保護には役に立つが、諸国間の情報の自由な流れを妨げるという効果を持っていた。

たとえ制限条項がなくとも個人情報の保護を目的とする法律はデータの国外処理の阻害要因になる可能性があった。

そのようなことから個人情報の適正な取り扱いに関するルールを定め、各国間で情報の自由な流れと個人情報の保護を調和させ、足並みをそろえる必要があった。また、それらの法的実効性を担保するための第三者機関についても言及された。

第2章では各国の個人情報の保護に関する法律を制定する際に大きな影響を受けたと思われる代表的な個人情報の保護を目的とした条約、宣言及び勧告などを取り上げる。

2.1 OECD プライバシー・ガイドライン

1970年代に入り、先述の通り各国間での個人情報の適正な取り扱いに関するルールと、個人情報の自由な流れの保護を調和させるのを委ねられたのが経済協力開発機構(Organisation for Economic Co-operation and Development,以下 OECD)^{注1}である。

OECDは1980年9月23日、「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勧告」(Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.以下

「OECD プライバシーガイドライン」とする。)を採択した。このOECD プライバシー・ガイドラインは世界各国の法制度の指導的な役割を担っており、日本でも個人情報保護対策を真剣に検討する契機になった。

このOECD プライバシー・ガイドラインは冒頭において認識内容^{注2}を示し、次のように勧告している。

- 「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、又はそのような障害の創設を回避することを努めること。
- 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・協力の手続きについてできるだけすみやかに同意すること。」^{注3}

このOECD プライバシー・ガイドラインは全5部で構成されており^{注4}、その中でも「第2部 国内適用における基本原則(Basic Principles of National Application)」で掲げた8原

則は日本における個人情報の保護を考える上で最も重要であり、個人情報保護法とも深く関連し、各国で制定されている個人情報の保護に関する法律はこれを参考又は考慮して制定されている。

個人データとは識別され又は、識別されうる個人に関するすべての情報をさす。ここでは各国が参考にしてしている OECD プライバシー・ガイドラインの 8 原則を考察していく。

2.1.1 収集制限の原則

収集制限の原則(Collection Limitation Principle)では、「個人データの収集には、制限を設けるべきであり、いかなる個人データも、適法かつ公正な手段によって、かつ適当な場合には、データ主体に知らしめ又は同意を得た上で、収集されるべきである。」とされた^{注5}。これは、データが処理されるべき方法、データの性質、データが利用されるべき状況又はその他の状況が、特別にセンシティブとみなされることを理由として、データ収集に制限を設けること、データ収集方法に関する要件を定めたものである。

2.1.2 データ内容の原則

データ内容の原則(Data Quality Principle)では、「個人データは、その利用目的に沿ったものであるべきであり、かつ利用目的に必要な範囲内で正確、完全であり最新なものに保たなければならない。」^{注6}

個人データはその利用目的に沿った内容であるべきであり、当該利用目的に必要な範囲において正確、完全であり最新のものに保たれるべきであるとされた。

2.1.3 目的明確化の原則

目的明確化の原則(Purpose Specification Principle)では、「個人データの収集目的は、収集時よりも遅くない時点において明確化されなければならない、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せず、かつ、目的の変更ごとに明確化された他の目的達成に限定されるべきである。」とされた^{注7}。

これは、データ収集より前の段階、また、いかなる場合でもデータ収集時より遅くない時点で、データの利用目的の特定が可能であるべきであること、及び、後の目的変更も同様であることを意味する。

2.1.4 利用制限の原則

利用制限の原則(Use Limitation Principle)では、「個人データは、第 9 条(目的明確化の原則)により明確化された目的以外の目的のために、提供、利用、その他の使用に供されるべきではないが、次に場合はその限りではない。(a)データ主体の同意がある場合、又は、(b)法律の規定による場合」とされている^{注8}。

個人データは、目的明確化の原則により明確化された目的以外の目的のために

開示、利用、その他のことに使用されるべきではないが、データの主体の同意がある場合
か法律の規定による場合のときは除かれる。

2.1.5 安全保護の原則

安全保護の原則(Security Safeguards Principle)では、「個人データは、その紛失又は無権
限のアクセス・破壊・使用・修正・提供等の危険に対し、適切な安全保護措置により保護
されなければならない。」とされている^{注9}。

2.1.6 公開の原則

公開の原則(Openness Principle)では、「個人データに係る発展、運用及び政策につい
ては、一般的な公開の政策が取られなければならない。個人データの存在、性質及びその主
要な利用目的とともにデータ管理者の識別、通常の住所をはっきりさせるための手段が容
易に利用できなければならない。」とされている^{注10}。

2.1.7 個人参加の原則

個人参加の原則(Individual Participation Principle)では以下のように勧告している。

「個人は次の権利を有する。

- (a) データ管理者が自己に関するデータを有しているか否かについて、データ管理者又はそ
の他の者から確認を得ること。
- (b) 自己に関するデータを、(I)適切な期間内に、(II)もし必要なら、過度にならない費用
で、(III)適切な方法で、かつ、(IV)自己に分かりやすい形で、自己に知らしめること。
- (c) 上記第(a)項及び第(b)項に基づく要求が拒否された場合には、その理由が与えられるこ
と、及び、そのような拒否に対して異議を申し立てることができること。かつ、
- (d) 自己に関するデータに対して異議を申し立てること、及び、その異議が認められた場合
には、そのデータを消去、修正、完全化、補正させること。」^{注11}

2.1.8 責任の原則

責任の原則(Accountability Principle)では、「データ管理者は、上記の諸原則を実施する
ための措置に従う責任を有する。」とされている^{注12}。

以上の8原則は、日本における個人情報保護法が制定されるにあたって重要視された原則
である。この原則は、個人情報の保護を目的とした法律が、国際的にその安全性が担保さ
れるレベルを満たしていくために重要な指標となっており、世界各国でも法律を制定する
にあたって重要視されている。

また、OECD プライバシー・ガイドラインでは第三者機関については特に言及はしてい
ないが同ガイドラインにおいて採るべき実効性の担保の仕組みは各国の法体系等によって

変わり得るので、監督機関としての第三者機関の設置は各国の判断に委ねられた。

2.2 EU 個人保護指令

個人データの保護に関しては、先述の OECD プライバシー・ガイドラインが存在していたが、欧州連合(European Union, 以下 EU)は、これらが個人データ保護をめぐるその後の状況に十分対応していないことや、EU 加盟国の制定した個人データ保護に関する法律の保護水準や内容の違いが、情報の自由な移動に対する障害となり、企業や個人の活動に余分な負担をかけていることを認識した。

そこで EU 加盟国の個人情報に関する国内立法の調和、統一を図ることを目的として、1995年10月24日、「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1995年10月24日の欧州議会及び理事会の95/46/EC指令(以下「EU 個人保護指令」)」が採択された。

この EU 個人保護指令の主な目的として EU は、基本的権利及び自由、特にプライバシー権の保護を重視しつつも、EU 加盟国の制定した国内法の保護水準の違いが情報の自由な移動に対する障害となったことを懸念し、そこで、プライバシー保護と情報の自由な流通を調整し、EU 加盟国の個人情報に関する国内立法の調和、統一を図ることを目的として、本指令が採択された。

この採択により、EU の非加盟国は、EU に加盟しない限り個人保護指令にいう第三国扱いとなるという指令の性質から、日本は、指令の直接的な影響を受けないものと解釈してきた。しかし、第三国への個人データ移転に関する定めを設け、個人データの保護について「十分なレベルの保護」を講じていない第三国に対しては、データの移転を禁じることが可能となった。このように、第三国に影響を与える規定を設けたために、それとの関係で世界的に注目されることとなった。

EU 個人保護指令が採択された1995年当時の日本においては、個人情報の保護を対象とする法律は旧行政機関法による行政部門に対するものしかなく、民間部門を対象とした個人情報保護法が制定されていなかったため、EU 加盟国諸国からのデータ移転が禁じられることを危惧し、「十分なレベルの保護」に適合するような対策を講じるため、民間部門を対象とした個人情報保護を目的とした法律の整備を行うため契機となった。

また、第三者機関についても規定を設けた。EU 個人保護指令では、各構成国は各国の規定の適用に関し完全に独立して監督する公的機関を定めなければならないとされた。監督機関としての機能は、調査・介入・法的手続きの開始、違反の司法機関への通知・個人の主張の聴取・定期的な活動報告書の作成とされた。

2.3 モントルー宣言

最近の第三者機関の規定の国際的動向の中においてデータ保護・プライバシー・コミッショナー国際会議がある。これは、各国、特にヨーロッパ諸国やカナダ、オーストラリア、ニュージーランドなどのデータ保護機関、すなわち各国の法令に基づく公的機関であり自主性・独立性を保証され、調査権等の権限を有する第三者機関から構成されるデータ保護及びプライバシー保護に関する国際会議である。そのデータ保護・プライバシー・コミッショナーの第27回国際会議の中で2005年に「モントルー宣言」がこの会議で承認された。

この宣言は、「グローバル化した世界における個人データ・プライバシーの保護：多様性を尊重するユニバーサルな権利」と題されている。そしてデータ保護・プライバシー・コミッショナーは個人データの取扱いに伴う個人の保護のためのユニバーサルな協定の発展を目指して、政府並びに国際的及び超国際的機関と協力することに合意するとした内容の宣言であり、この目的達成のため以下の3点を訴えた。

- ① 国際連合に対してデータ保護を詳細に明言した法的拘束力を持つ文書の立案
- ② 世界中の政府に対してデータ保護・プライバシーに関する法的文書の採択の促進
- ③ 非加盟国がその条約に加盟することの要請

また、この宣言の中で「独立監視及び法的制裁の原則」について言及されている。日本はデータ保護に関する違反に対する法的制裁として、主務大臣を通じて罰則を与える間接罰に留まっており、各国が採用しているような直接罰の制度を採用していないため「十分なレベルの保護」を満たしていない可能性があり、EU個人保護指令と同様に十分な個人情報の保護のレベルが達成されていない恐れがある。

注釈

[1] 2010年1月現在のOECD加盟国はオーストリア、スイス、ベルギー、トルコ、カナダ、イギリス、デンマーク、アメリカ、フランス、日本、ドイツ、フィンランド、ギリシャ、オーストラリア、アイスランド、ニュージーランド、アイルランド、メキシコ、イタリア、チェコ共和国、ルクセンブルク、ハンガリー、オランダ、ポーランド、ノルウェー、大韓民国、ポルトガル、スロバキア、スペイン、スウェーデンの30カ国

[2] OECD プライバシー・ガイドラインにおける認識内容

「加盟国は国内法及び国内政策の相違に関わらず、プライバシーを個人の自由を保護し、かつプライバシーと情報の自由を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」

「個人データの自動処理及び国際流通は国家間で相互に矛盾しない規則と運用の発展を要請」

「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」

「プライバシー保護と個人データの国際流通にかかる国内法は国際流通を妨げるおそれがある」

[3] 石井夏生利 『個人情報保護法の理念と現代的視点課題 プライバシー権の歴史と国際的視点』 勁草書房 2008年(以下「石井著」) 302～303頁

[4] 5部構成は「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-自由な流通と適法な制限」「第4部 国内実施」「第5部 国際協力」

[5] 石井著 304頁

[6] 石井著 305頁

[7] 石井著 305～306頁

[8] 石井著 306頁

[9] 石井著 306～307頁

[10] 石井著 307頁

[11] 石井著 308頁

[12] 石井著 309頁

3 EUの個人情報保護法

日本が個人情報の保護に関する法律の国際的基準を満たすために必要と思われるEUの個人情報保護法の形式について考察する。

EUは、個人情報の保護に関して歴史的に見てもとりわけ早い段階から意識しており、個人情報保護を法的に担保する独立した第三者機関・監督機関の導入をしている。そうした中で、日本の独立した第三者機関について考察するときに重要であるだろう。

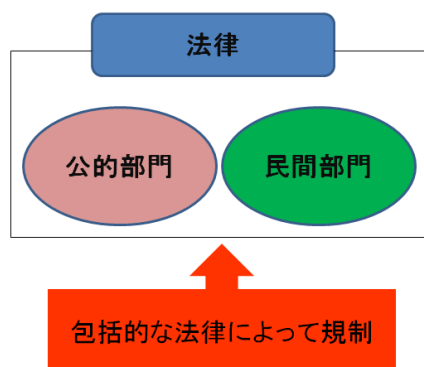
3.1 個人情報保護法の形式

3.1.1 オムニバス方式

EU諸国は個人情報保護法の形式として日本のセグメント方式と異なり、オムニバス方式を採用している。セグメント方式は公的部門を対象とする法律と、民間部門を対象とする法律をそれぞれ分けて制定する形式であるがオムニバス方式は公的部門と民間部門を包括的な法律によって規制する形式である。

この形式はEU個人保護指令以降、世界の趨勢となっている個人情報保護の法律の形式である。(図表.4)

・オムニバス方式



(図表.4) 筆者作成

3.2 イギリスの例

EUの代表的な個人情報保護に関する法律の例としてイギリスを取上げる。イギリスはOECDプライバシー・ガイドラインやEU個人保護指令などの影響を受けて独立した第三者機関の導入を早い段階に行った国である。

3.2.1 1984年データ保護法

1980年代に入るとOECDプライバシー・ガイドラインの採択により、個人情報の保護をめぐる国際情勢は大きな変化が見られるようになった。その潮流の中で、イギリスでは1984年に「個人に関する自動処理情報の利用及び当該情報に関するサービスの提供を規制する

ための法律(以下「1984年データ保護法」)」を制定した。この1984年データ保護法はオムニバス形式を採用している。

1984年データ保護法は以下の特徴が挙げられる。

- (1) 公的部門、民間部門を問わずにコンピュータ処理される個人データを対象とする。
- (2) 個人データを保有するデータ利用者又は他の者にデータデータに関するサービスを提供するコンピュータ・ビューロが一定の場合を除いてデータ保護登録官に登録しなければならない。
- (3) データ利用者が個人データの利用についてデータ保護登録官を通して公開しなければならない。また、情報の適正な取扱いを行う等の諸原則に従わなければならない。
- (4) その登録を扱い、データ保護についてオンブズマン的役割を果たすデータ保護登録官を置いたこと。
- (5) データ主体が自己に関する情報にアクセスし、その誤りの訂正を求めることができるようになった。
- (6) 不服申し立てを審理するデータ保護審判所を置いたこと。
- (7) 法律を段階的に施行したこと。

(2)に挙げたデータ保護登録官とは、イギリスにおける女王から独立した法執行機関である。保護登録官は女王によって任命され、データ利用及びコンピュータ・ビューロを営む者が、データ保護原則の遵守を促進することについて、1984年データ保護法に基づく権能を遂行することを義務としている。具体的には、登録申請の受理及び拒否を行い、執行通知、登録抹消通知、移転禁止通知の送達といった監督権限を行使する。また、本法に基づく権能行使に関する年次報告の提出等の義務を負う。

このデータ保護登録官は個人情報の有用性を保つ独立した第三者機関の役割として注目に値するが、1984年データ保護法があまり浸透しなかったことも影響してデータ保護登録官があまり活躍できなかった面があった。

3.2.2 1998年データ保護法

1984年データ保護法は1995年に採択されたEU個人保護指令を受けて1998年に全面的に改正され、「当該情報の取得、保有、利用又は提供を含む、個人に関する情報の取扱いの規制のために新たな規定を設けるための法律(以下「1998年データ保護法」)」が制定された。施行は2000年3月1日である。

日本における個人情報保護法の目的は第1条に掲げられているが、この法律はその正式名称そのものが目的となっている。

1984年データ保護法は、コンピュータ処理される個人データ、すなわち自動処理データのみが法律の適用対象となっていたが1998年データ保護法ではそれ以外に「関連するファ

ファイリングシステムの一部として記録される情報(以下「関連するファイリングシステム」))を対象としており、法律上では「個人データ」という概念を使用している。

また、1998年データ保護法の中では個人情報という大きな括りの中で「データ」、「個人データ」、「関連するファイリングシステム」を定義している。

それは以下の通りである。

(1) データ

「データ」とは、「(a)当該目的のために与えられる指示に応じて自動的に動作する装置によって処理される方法、(b)当該装置によって処理されるべきことを意図して記録される情報、(c)関連するファイリングシステムの一部として又は関連するファイリングシステムの一部を構成すべきことを意図して記録されている情報、又は(d)上記(a)、(b)又は(c)の各号には該当しないが68条によって定義されるアクセス可能な記録の一部を構成する情報」をいう

(2) 関連するファイリングシステム

「関連するファイリングシステム」とは、「情報が当該目的のために与えられる指示に応じて自動的に動作する装置によって処理されないにもかかわらず、個人への照会又は個人に関する基準への照会によって、特定個人に関する特別の情報が容易にアクセスできるような方法でその一連の情報が構成されている限度における、個人に関する一連の情報」をいう。

(3) 個人データ

「個人データ」とは、「(a)当該データから、又は(b)データ管理者^{注1}が保有し、又は保有することになる可能性のある当該データその他の情報から、識別できる生存する個人に関するデータであって、かつ、当該個人に関する意見の表明及び当該個人についてデータ管理者その他の者の意図の表示を含む」ものとされている。

「意図の表示」とは例えば、特定の者が「怠け者である」というのは、「当該個人に関する意見の表明」であり、「怠け者であるから解雇する」というのは「意図の表示」とされる。

以上をまとめると、「データ」とは先にも述べたように自動処理されるものの他に関連するファイリングシステムの一部として記録されるマニュアル処理情報を含み、当該データが生存する個人を識別する場合は、個人データに含まれることとなる。

関連するファイリングシステムは特定の個人の情報に容易にアクセスできる形で、一連の情報が構成されている場合を指すことから全てのマニュアル処理情報を含むわけではない。

また、本法は「センシティブな個人データ(以下「センシティブ・データ」)」に関しても触れている。「センシティブ・データ」は以下のようなものが挙げられる。

- ①人種又は民族的出自
- ②政治的信条
- ③宗教的信仰又は類似の性質を持つ他の信仰
- ④労働組合の加入
- ⑤身体又は精神の健康状態
- ⑥性生活
- ⑦犯罪の前科・容疑
- ⑧犯罪の容疑の手続き、処分、判決

この「センシティブ・データ」に関する定めは1998年データ保護法で新しく導入された項目である。これは、個人情報を取扱う上で重要視しなければならない。なぜならこれらのことが公になってしまうとその当該個人が社会生活を営む上で大きな被害を受ける可能性がある。

3.2.3 個人情報保護法の監督制度

本法では公的部門と民間部門の双方を独立して個人情報保護の色説的な監督する機関として「コミッショナー」が置かれた。コミッショナーは、1984年データ保護法の定めるデータ保護登録官を引き継ぎ、データ保護コミッショナーとしてスタートした。その後2000年情報自由法の運用にあたるようになったことから、2001年から「情報コミッショナー (Information Commissioner)」に名前を変更した。

この情報コミッショナーは政府から独立した法執行機関であり、その権能は51条が、「データ管理者による善良な実務の遂行を促進し、また、とりわけ、データ管理者による本法の義務の遵守を促進するように、本法に基づき自らの権能を行使することは、コミッショナーのぎむである。」と定めている。

また、情報コミッショナーの主な職務・職権は以下の3点が挙げられる。

(1) 法の遵守・監視

情報コミッショナーには違反したデータ管理者に対する執行通知、評価情報に基づく情報提出通知、また本法違反のデータ管理者の物件に対する立入検査権が認められている。さらに違反者に対する訴追権限が付与されている。

(2) データ管理者の監督・登録

データ管理者は、個人データを取扱うにあたって、通知事項(氏名、住所、代表者、個人データのカテゴリ、取扱目的、データの提供先、情報を欧州経済地域外へ移転させる場合の国名)、及び情報安全保護遵守のための措置を、情報コミッショナーに通知しなければならない。情報コミッショナーは通知を行った者の登録簿を保持しなければならない。

データ管理者は、情報コミッショナーの登録簿に記載されなければ個人データを取扱ってはならないとされている。

(3) 普及・啓発その他の活動

情報コミッショナーは国民に対する情報提供、善良な実務に関する指針のための実施基準の準備及び配布等、データ保護に関する啓発を行うものとされている。

また、情報コミッショナーはその職員、代理人等は原則として取得した情報の機密性を守らねばならず、故意または過失によりこれに違反して情報を提供した場合は、有罪となる。

以上のように EU の個人情報保護に関する法律は OECD プライバシー・ガイドラインや EU 個人保護指令などの国際的な指針を元にして作られている傾向がある。このような国際的な指針を満たすことにより他の国に対して個人情報の保護の安全性を示すことができる。特に EU 個人保護指令で EU 諸国以外の第三国に個人データを転送するときに、EU から十分な保護水準^{注2}に達していなかった場合、データ転送ができず、経済的にも大きく支障をきたす恐れがある。

注釈

[1] 個人、法人、権利能力なき社団を問わず公的部門民間部門をも問わない。

[2] 2010年1月現在、EU から保護水準を確保している国はスイス、カナダ、アルゼンチンガンジー島、マン島、ジャージー島があげられる。

4 アメリカの個人情報保護法

アメリカはICTの発展が世界に比べて顕著であるとともに、個人情報の保護に密接に関わるプライバシー権の研究も盛んである。そのような環境の中でアメリカはEU諸国や世界の趨勢である個人情報保護法の形式を取っておらず、独自の法律形式を取っている。

またアメリカはEU加盟国ではないのでEU個人保護指令による第三国に個人データを転送する際に十分な保護水準に達していない可能性があった。

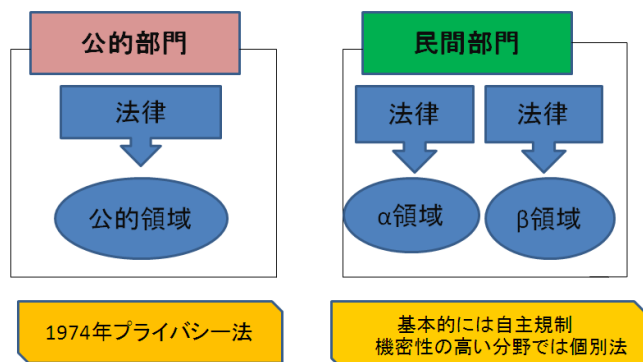
この章ではアメリカの個人情報保護法の形式と、EU加盟国以外の第三国の国際的な指針に対する対策を考察する。

4.1 個人情報保護法の形式

4.1.1 セクトラル方式

日本の旧行政機関法では公的部門と民間部門を別々の法律で規制するセグメント方式を、EU諸国の多くでは公的部門、民間部門を包括的に規制するオムニバス方式を採用している。一方アメリカは、公的部門では包括的な法律で規定し、民間部門は基本的には自主規制に委ね、重要度の高い領域に関しては個別の法律で規制するというセクトラル方式を採用している。(図表.5)

・セクトラル方式



(図表.5)筆者作成

この方式は特に保護が必要な領域には限定して規制することができるのがメリットではあるが、他方で、個別領域ごとに制定するため関連業界や利益団体、政治的状況の影響を受けやすいというデメリットがある。

アメリカはこのように民間部門は自主規制に委ねる一方で、重要な領域に関しては個別法を用いるという他の方式とは一線を画している傾向がある。

4.2 公的部門のプライバシー保護法

アメリカは1960年代から1970年代にかけて合衆国政府、行政機関の急速なコンピュータ化がされ、個人データの多くがコンピュータ処理をされるようになった。

そうしたアメリカにおいて公的部門の個人情報を保護するための法律は、「合衆国の記録の濫用から個人のプライバシーを保護し、個人が合衆国の行政機関の保有する自己に関する記録へアクセスを与えられること定め、プライバシー保護調査会を設置する等のため、第552条のaを追加して合衆国法律集第5編を改正するための法律(以下「1974年プライバシー法」)」である。

この「1974年プライバシー法」は主に以下の事項が定められている。

- (1) 連邦政府機関の記録の誤用から個人のプライバシーを保護
- (2) 連邦政府機関が保有する個人情報に対する本人によるアクセス
- (3) プライバシー保護調査委員会の設置

本法の規定する「個人」(Individual)とは、合衆国国民又は、適法に永住を認められた外国人である。

保護する情報として多く挙げられるのは「記録システム」である。「記録システム」(system of record)とは、行政機関の管理下に置かれる記録の集合であって、そこから、個人の氏名又は何らかの識別番号、記号、その他指紋、声紋、写真等、個人別に付された識別項目のことである。これはすなわち、個人の識別情報によって情報を検索できる記録の集合であり、検索可能な個人情報の集まりである。

アメリカは包括的な個人情報保護に関する法律が存在せず特定分野ごとに法律が制定されているため、個人情報保護に関する法律ごとに「個人情報」の定義がなされており、分野ごとに定義が異なる。

また、プライバシー保護調査委員会は、プライバシー法の基本となる8原則を以下のように掲げている。

- ①公開の原則
- ②個人アクセスの原則
- ③個人参加の原則
- ④収集制限の原則
- ⑤利用制限の原則
- ⑥提供制限の原則
- ⑦情報管理の原則
- ⑧責任の原則

各原則は1974年プライバシー法の1つ又は複数の規定の中で明らかにされており、適用に当たっては個人、組織及び社会の利益を衡量することが求められている。この8原則は法律で規定されているわけではないが、のちのOECDプライバシー・ガイドラインの元となる8原則であり、個人情報保護の国内的基準に関して重要な位置を占めている。

4.3 民間部門のプライバシー保護法

アメリカの個人情報保護に関する法律の形式はセクトラル方式を取っているため、民間部門のプライバシー保護法、すなわち、民間に対する個人情報保護に関しては基本的に自主規制に委ねており、特別に機密性の高い分野においては個別的な法律を制定している。それはアメリカの風土として、情報の自由な流通を重視しているという点もある。主な例として以下のものがあげられる。

※具体例

(1)信用・金融分野

「系列銀行、証券会社、保険会社、及び他の金融サービス業者に対して裁量的枠組みを提供することにより、金融サービス業界の競争を促進する等のための法律(以下1999年金融サービス近代化法)」はその代表例である。

この法律は、金融分野の規制緩和に伴い、銀行、保険、証券取引等の業務を行うための新たな金融機関の設立を認め、金融商品のワン・ストップ・サービスの実現などを目標にしたものである。金融機関は顧客の個人情報の提供や保護に関するプライバシー保護方針を明示するよう義務付けられた。

(2)情報通信分野

「子どもの保護:1998年子どもオンラインプライバシー保護法」は、1998年に成立した。本法はFTC^{注1}の勧告を受けて成立し、商業目的のウェブサイトやオンライン・サービスの管理者を対象として、13歳未満の子どもからインターネット上を通じて個人情報を収集する場合、事前に親の同意を得ることを義務付けるとともに、親に対して、子どもが提供した個人情報のアクセス権を認めた。

本法に関連してFTCにより児童オンラインプライバシー保護規則が定められており、ウェブサイト運営者等がプライバシーポリシーに含めるべき事項、保護者からの同意取得の時期・方法等について詳細に規定されている。

4.4 個人情報保護法の監督制度

アメリカにはイギリスの情報コミッショナーのような独立した個人情報の保護全般を統一的に監督する第三者機関は存在していなく、分野別に個人情報に関する第三者機関は各個別法の規定に委ねられている。

しかし、EU 個人保護指令において EU 加盟国は非加盟国である第三国に個人情報を移転する場合は国内の個人情報保護の法律の基準が十分な保護レベルに達していないと個人情報を移転できない可能性が出てきた。これはアメリカ、EU 諸国間での個人情報の往来が滞ることとなり経済的に大きな損害を被ることとなる。アメリカは EU 諸国の個人情報保護法の形式であるオムニバス方式とは違い、セクトラル方式を用いているため、その十分な保護レベルに達するよう示すためにアメリカ商務省は EU に対して「セーフ・ハーバー協定(Safe Harbor Agreement)」を提案し、その水準を保つことを目指した。

4.4.1 セーフ・ハーバー協定

1995年に採択された EU 個人保護指令第 25 条第 1 項によって EU 加盟国は個人情報を第三国に移転する場合、その第三国が EU 個人保護指令によって定められた国内着ての遵守を損なうことなく、当該第三国が十分な保護レベルを確保しなければならなかった。このような EU の動きにアメリカは自国内の事業者と EU 加盟国間における個人データの流通に障害を来す懸念し、対処しなくてはならない状況にあった。

その様な状況を受け、セーフ・ハーバー協定は 2000 年 5 月に締結された。

これは、アメリカ商務省が作成する「セーフ・ハーバー原則」を産業界が遵守していれば十分な個人情報の保護がされているとみなされ、EU 個人保護指令に違反にならないとした。

この協定によりアメリカのセーフ・ハーバー参加者は EU 側とアメリカ側の二重の個人情報の保護基準に悩む必要がなくなった。また、企業によってはプライバシーの侵害に対して予見可能性の面でメリットがある。

4.4.2 セーフ・ハーバー原則

セーフ・ハーバー原則とはアメリカ商務省が作成したセーフ・ハーバー協定に関する原則であり、遵守していれば EU 個人保護指令に違反にならないとされる。

セーフ・ハーバーの適用対象は EU からアメリカへ流通する個人情報であり、アナユアル・デジタル情報も含まれる。国民からデータを集め、そのデータをアメリカに持ち込むすべての企業が対象となり、セーフ・ハーバーに加入するか否かは完全に組織の判断に委ねられている。セーフ・ハーバーの資格を得ようとする組織は、自らセーフ・ハーバーを遵守していることを商務省に対して証明することが必要となる。

遵守を自主的に証明した日から組織はセーフ・ハーバーの利益の享受をすることができ、加入した組織は、セーフ・ハーバーによる利益の享受を確実にするために毎年、商務省に対して遵守事項に同意していることを証明しなくてはならない。

セーフ・ハーバーに加盟し、遵守事項に従う組織は十分な保護レベルの要件を満たしたものとされる。

商務省は、セーフ・ハーバー原則の要件を満たした組織の「セーフ・ハーバー・リスト」

を保有しこれをウェブサイトで公開している。

セーフ・ハーバー原則の内容は以下の通りである。

- ① 告知
取得した情報、利用目的等を個人に告知しなければならないとする。
- ② 選択
個人情報に目的外使用に関する選択、第三者への提供に関する選択(opt-out)の原則
センシティブ情報に関して積極的又は明示的な選択を与えなければならない
(opt-in)原則
- ③ アクセス
個人情報に関して、その本人は組織が保有する情報に誤りがある場合その情報に対して開示、訂正、変更、削除請求が認められている。
- ④ セキュリティ
個人情報を取扱う組織は不正行為に対する予防措置を講じなければならない。
- ⑤ 第三者への提供
個人情報を第三者へ提供する場合、当該本人に通知し、選択させる余地がなければならないとしている。
- ⑥ データの完全性
個人情報はその利用目的に関連するものではなく、個人情報を取扱う組織はデータの利用目的、正確性、完全性、最新性を確保しなくてはならないとしている。
- ⑦ 実施・施行
FTC、商務省が違反に対して告知、調査、停止命令などを下せる監督体制にすることとしている。

アメリカは EU と独自にセーフ・ハーバー協定を締結することによってセクトラル方式を維持しつつ個人情報の保護レベルの十分性を保つことに成功した。

これは、アメリカの外交力と経済力でなせた業であるだろう。

注釈

[1] アメリカの連邦取引委員会(Federal Trade Commission,FTC)

5 今後の展望～日本における独立した第三者機関の行方～

OECD プライバシー・ガイドラインや EU 個人保護指令、モントルー宣言などの国際的な個人情報の保護基準の取り決めを受けて、アメリカは独自の路線でセーフ・ハーバー協定を結ぶことにより EU に対して十分な保護レベルを保つことに成功し、基準を満たしたアメリカの組織は EU と個人情報のやり取りができる体制を整えた。

これは、EU 側がアメリカに対してセーフ・ハーバー協定のような特別な処置を下したのはアメリカとの通商関係や、情報の流通等の現状を無視することができず、アメリカの提示した枠組みに同意せざるを得なかった。この方法はアメリカ特有の解決手段であると考えられる。

一方日本は、政府から独立した監督機関は存在せず、個人情報保護法を違反しても緩やかな監督権限を持つ主務大臣による間接的な罰則のみを科し、民間部門は自主規制に委ねるという組み合わせである。また、行政機関に関しても行政のセルフチェックのみになっている。日本は国際的な個人情報の保護の基準を担うために、法律に基づく独立的・専門の機関を設置する必要がある。

監督機関は個人情報の有用性と流用性を保ち、イギリスのような個人情報保護法を的確に理解している法執行機関が望ましい。しかし、個人情報を保護する際には憲法上の表現の自由・営業活動の自由、そして行政の円滑な運営を損なわないようしなくてはならず、専門的な知識のある監督機関にしなくてはならないだろう。

おわりに

インターネットが登場して約 50 年近くが経った。そして ICT の発達も日進月歩であるなかで個人情報のやり取りも各場面で重要視される一方、氏名や住所、アドレスなどの個人情報の流出するケースが後を絶たない。

これらのケースは人為的ミスによる流出が多いが、また違う個人情報、例えば、Amazon での消費行動などの個人情報の当該者が把握しきれずに、サイトの運営者が自分の個人情報が知らずに利用されている場合もある。

旧来の憲法的な意味でのマスコミの過剰な報道からプライバシー権を守る概念である「ひとりで放っておいてもらう権利」から自分で自分の情報をコントロールするという「自己情報コントロール権」が ICT の情報の容易なコピーと伝達の早さによって限界がきているのかもしれない。

そうした中でやはり日本において、政府から独立した、専門的な監督機関の設置により個人情報の有用性と流用性を保つ必要があるだろう。そして、各国の法体系や慣習、プライバシー権の違いがあり、難しいところではあるが、国際会計基準のようなインターネット上における国際的な個人情報の保護を保つための明確な基準や、スポーツ仲裁裁判所のような独立した監督機関を設置が将来的に来るかもしれないが道のりは険しいだろう。

最後にこの論文を執筆するにあたり指導をしてくださった山田正雄教授をはじめ、助言をくれたゼミナールの仲間たちに感謝の意を述べて終わりにしたいと思う。

参考文献・URL

《書籍》

- * 岡村久道・新保史生 『電子ネットワークと個人情報保護法』 2002年 現代産業叢書
- * 堀部政男 『インターネットと法第2版』 2006年 新生社
- * 小向太郎 『情報法入門デジタルネットワークの法律』 2008年 NTT出版
- * 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』
2008年 勁草書房
- * 岡村久道 『個人情報保護法』 2009年 商事法務
- * 芦部信喜・高橋和之補訂 『憲法第四版』 2007年 岩波書店
- * 宮台真司・神保哲生・東浩紀・水越伸・西垣通・池田信夫
『ネット社会の未来像』 2006年 春秋社

《雑誌》

- * 堀部政男 「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の補完」
『実用法律雑誌ジュリスト』 No.1361 2008年
- * 『別冊ジュリスト メディア判例百選』 No.179 2005年

《URL》

- * OECD 東京センター <http://www.oecdtokyo.org/>
- * 消費者庁ホームページ <http://www.caa.go.jp/>
- * 消費者庁・個人情報の保護 <http://www.caa.go.jp/seikatsu/kojin/index.html>

《その他》

- * 『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』 2008年
- * 読売新聞 2007年3月13日
- * 読売新聞 2007年3月18日