個人情報保護とがん登録

Protection of personal information and cancer registry

安冨　潔*

1. はじめに

がん登録は個人情報保護法の適用から除外されており、その点で法律レベルではがん登録と個人情報保護の問題は一応整理されている。しかし逆に、がん登録と個人情報保護とに関する状況は悩ましくなったのではないかとさえ思われる。

というのは、がん登録の主体が様々であり、提供する側の医師の立場も様々であることから、個人情報の取り扱いをめぐる法的な仕組みが輻輳している。その中で、がん登録に当たって個人情報をどのように扱っていくかという問題について、法律レベルで一義的に整理されていないために、色々なレベルで検討していかなければいけないという状況にある。

本論では、個人情報とは何か、そして個人情報保護法の仕組みについて整理した上で、がん登録との関係で私見を述べるものである。

2. 個人情報と個人情報保護

まず、個人情報とは何かということについて考えたい。個人情報保護法では、生者の個人識別あるいは識別可能情報を個人情報として扱うという考え方をとっている。しかし、個人情報について、もっと広くとらえる考え方もある。たとえば死者も含めて個人識別可能情報ととらえるもので、1980 年の OECD 理事会勧告や我が国の JISQ15001 などは、そのように考えている。情報という広い概念の中で、個人情報というものも、生者と死者の両方を含む意味での個人識別可能情報があるが、我が国の個人情報保護法は生者に限った形での個人識別情報ととらえている。要約すると、特定の個人を識別する情報を個人識別情報と言う。他の情報と照合することによって特定の個人を識別できる情報を個人識別可能情報と言う。これらを総称して個人情報ととらえるのが一般的な理解であろう。

個人情報の保護に関する法律は、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、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いうように、個人情報を定義している。ここでは死者の情報は個人情報保護法からは外れることになる。もっとも死者の情報であっても、生者の情報でもある場合がある。例えば相続に関わる情報は、死者の情報である一方、相続という点では生きているご遺族等の情報でもある。このような場合は生者である相続人等の情報であるという観点から死者の情報を取り扱う仕組みとなっている。

条例での扱い方は様々であるが、生者に限るという絞りをかけたものは必ずしも多くない。宮城県の条例や仙台市の条例では、生者に限るという規定はない。他の自治体でも生者のみというとらえ方をしない条例も多い。

個人情報保護に関するコンプライアンス・プログラムの要求事項（JISQ15001）では、個人

*慶応義塾大学大学院法務研究科・法学部 教授
〒108-8345　東京都港区三田 2-15-45

情報を定義するに当たって、「個人に関する情報であって、当該記述に含まれる氏名、生年月日その他の記述または個人に別に付された番号、記号その他の符号、画像もしくは音声によって当該個人を識別できるものをいう」としている。

個人情報とは、大きく 2 つに分けられる。一つは、基本情報と言われるものであり、氏名、住所、電話番号、性別、生年月日、職業、などが該当する。もう一つはセンシティブ情報、機微な個人情報などと言われるものである。ただ、個人情報保護法はこの区別をしていない。広くただ個人情報というだけである。

一般に性別は基本情報とされるが、昨今若干難しい問題となりうるのは、いわゆる性同一性障害のケースにおいて、性別というものを基本情報としてとらえていいかどうかという問題である。この点は消極的に考えるべきだろうと思われる。基本情報としての性別は、いわゆる戸籍簿に載っている情報という意味でとらえるべきではないかと思われる。性同一性障害の場合の性別に関する情報は、センシティブ情報そのものである。したがって基本情報といってもその取り扱いに慎重を期さざるを得ない場合もある。

センシティブ情報は、具体的には思想信条及び宗教に関する事項、人種、民族、門地、本籍地、身体や精神障害、犯罪歴その他社会的差別の原因となる事項、勤労者の団結権や団体交渉及びその他団体行動の行為に関する事項、集団示威行為（いわゆるデモ）への参加、請願権の行使及びその他の政治的権利の行使に関する事項、保健医療及び性生活などがある。

ここで、個人情報とプライバシーとの違いについて整理したい。プライバシーとは、法的な仕組みで言うと、憲法 13 条の権利ととらえられるというのが一般的な理解である。プライバシーに関する古典的な概念とは、いわゆる「一人で放っておいてもらう」権利である。これは 1890 年、ハーバードロー・レビューにウォーレンとブランダイスが書いた論文で唱えられたものである（Warren & Brandeis, The Right to Privacy, Harv. L. Rev. 195:1890）。いわば他人から干渉を受けないというところに、人格権としてのプライバシーをとらえるという考えである。これは、新聞等のジャーナリズムで名誉棄損に当たるようなことが報道されるなかで、自分の領域に勝手に踏み込むなということから、プライバシーという考え方が登場した。しかし、1960 年代になって、情報というものは自分でコントロールするべきだという考え方が登場した。プライバシーも、その観点からとらえ直せるのではないかという考え方へ移行したのである。

古典的なプライバシーとは一人にしておいてもらう権利という考え方であり、我が国でも東京地裁で、私生活をみだりに公開されない法的保障ないし権利というものがあるという判例が出されている（東京地判 39.9.28 判例時報 385 号 12 頁）。その後、自分に関する情報はみずからコントロールできるものだとプライバシーのとらえ方が移ってきている。もっとも、両者は性格の違うものである。したがって、古典的な概念が排斥されて、新しい概念に移り変わったということではない。むしろ今は両方併存する状況にある。

個人情報保護とプライバシー保護という点では、前述のように個人情報とプライバシーとは必ずしも同じものではない。ただ、古典的な意味でのプライバシー、一人にしておいてもらう権利というとらえ方からすると、個人情報のうちの氏名等の基本情報は、プライバシーに含まず、個人情報よりもプライバシーの範囲の方が狭くなる。一方、新しい概念、自己情報コントロール権から見ていくと、氏名等もプライバシーに属する事項と考えられるので、保護される範囲は同じと考えられる。その意味では、新しい概念から見れば、個人情報とプライバシーは同じ法の範囲にあると言ってよい。必ずしも両者を一義的にとらえられないという点で、個

人情報とプライバシーは必ずしも同じものではないという理解が一般にされている。

また、権利の救済あるいは権利の保護の仕方についてもプライバシーと個人情報とでは違いがある。プライバシーの場合、とくに古典的な意味でのプライバシーという場合には、権利侵害があった場合、これを不法行為という民法上の権利侵害として、それに対する救済措置が想定される。刑事的に言えば、プライバシーの侵害ということであれば名誉棄損罪という犯罪に当たることがある。しかし、新しい概念として積極的に自己情報コントロール権というとらえ方をすると、上記の側面よりも自己情報の開示、訂正、削除請求ができるという、行政法上の規制になじむとらえ方になる。プライバシーをどう守るか、侵害されたときにどのように救済するかということは、以上のように整理できる。一方、個人情報の保護では、むしろ予防的な措置というか、事前の保護策というか、そのための仕組みとして個人情報保護制度ができ上がっている。

さて、個人情報保護の歴史的背景について述べる。1960 年代後半頃からヨーロッパで個人情報保護の必要性がうたわれるようになった。当初は行政機関が個人情報をどのように使用できるかということが問題となった。具体的に言うと、行政が持っている情報を警察が犯罪捜査に役立ててもよいかという問題が取り上げられた。それに対して、行政の情報をきちんと守る仕組みをつくるべきではないかという議論が盛んとなった。1970 年になると、アメリカで公正信用報告法という法律ができ、また旧西ドイツ・エッセン州でデータ保護法が制定された。それを契機として、1973 年のスウェーデンのデータ保護法、1974 年には有名なアメリカのプライバシー法ができ、個人情報保護の制度が各国で徐々に整備されるようになっていった。

個人情報保護の制度は、三つに大別される（表 1）。ヨーロッパではオムニバス方式と言って、公的な部門と民間部門ともに一つの法律で個人情報保護を行っている。これに対して、アメリカはセクトラル方式で、たとえば医療や電気通信など対象分野を一つ一つ区切って、個別に規制を行うやり方をとっている。中間に当たるのが、個人情報保護法ができるまでの我が国の方式である。行政と民間のそれぞれについて個別に規制するもので、セグメント方式と呼ばれている。

表 1. 個人情報保護のあり方

個人情報保護の方式	行政分野	民間分野	国
オムニバス方式	行政・民間について包括的な法律で規制		EU諸国
セグメント方式	法律で規制	自主規制	これまでの日本
セクトラル方式	法律で規制	自主規制＋個別法	アメリカ合衆国

今度の個人情報保護法では、行政も民間も基本法の部分と一般法の部分が個人情報保護法の中に取り込まれている。その意味ではオムニバスのようであり、セグメントのようであり、複雑な方式をとっている。アメリカではセクトラル方式で、行政は法律で包括的に規制して、民間部門は自主規制つまりガイドラインと個別法といった対応をしてきたわけである。

個人情報を守るときに、オプトインというやり方とオプトアウトというやり方がある。オプトインとは、事前に情報収集に当たって個人に拒否権を認めるものである。オプトアウトとは個人情報の第三者への提供の際に拒否権を認めるものである。基本はオプトインであり、第三者に個人情報が提供される前に、その情報主体に提供するかどうか同意を求めておいて、拒否されたら提供しないというのが一般的であると思われる。一方、あらかじめ第三者への個人情報の提供があるということを周知した上で、個別に事後的に提供の拒否を認めるというオプトアウトという方法も考えられる。

個人情報保護に関する最も基礎になる考え方が、1980 年の OECD（経済協力開発機構）

の理事会勧告で示された。プライバシー保護と　　範囲内で正確、完全、最新に保たれなければな

表 2. OECD 8 **原則と個人情報取扱事業者の義務規定の対応**

OECD８原則	個人情報取扱事業者の義務
○目的明確化の原則 収集目的を明確にし、データ利用は収集目的に合致するべき ○利用制限の原則 データ主体の同意がある場合、法律の規定による場合以外は目的以外に利用使用してはならない	○利用目的をできる限り特定しなければならない（第15条） ○利用目的の達成に必要な範囲を超えて取り扱ってはならない（第16条） ○本人の同意を得ずに第三者に提供してはならない（第23条）
○収集制限の原則 適法・公正な手段により、かつ情報主体に通知又は同意を得て収集されるべき	○偽りその他不正の手段により取得してはならない（第17条）
○データ内容の原則 利用目的に沿ったもので、かつ、正確、完全、最新であるべき	○正確かつ最新の内容に保つよう努めなければならない（第19条）
○安全保護の原則 合理的安全保護措置により、損失・破壊・使用・修正・開示等から保護するべき	○安全管理のために必要な措置を講じなければならない（第20条） ○従事者・委託先に対し必要な監督を行わなければならない（第21、22条）
○公開の原則 データ収集の実施方針等を公開し、データの存在、利用目的、管理者等を明示するべき ○個人参加の原則 自己に関するデータの所在及び内容を確認させ、又は意義申立を保証するべき	○取得したときは利用目的を通知又は公表しなければならない（第18条） ○利用目的等を本人の知り得る状態に置かなければならない（第24条） ○本人の求めに応じて保有個人データを開示しなければならない（第25条） ○本人の求めに応じて訂正等を行わなければならない（第26条） ○本人の求めに応じて利用停止等を行わなければならない（第27条）
○責任の原則 管理者は諸原則実施の責任を有する	○苦情の適切かつ迅速な処理に努めなければならない（第31条）

*各義務規定には適宜除外事由あり

個人データの国際流通に関するガイドラインである。これはガイドラインであるため、加盟国に対して法的な拘束力を持つものではなく、やわらかな指導内容となっている。このOECD のガイドラインには 8 つのルール（8 原則）がある。OECD 8 原則と個人情報保護法との対応関係を表 2 に示す。ガイドラインの項目によると、収集制限の原則、データ正確性の原則、目的明確化の原則、利用制限の原則、安全保護の原則、公開の原則、個人参加の原則、責任の原則という 8 原則がうたわれている（表 2）。

収集制限の原則とは、個人データの収集は適法かつ公正な手段によるべきであり、かつ適当な場合にはデータ主体に通知または同意を得て行うべきであるということ。データ正確性の原則とは、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らないということ。目的明確化の原則とは、個人データの収集目的は収集時より遅くない時期に明確化されなければならず、その後の利用は収集目的と両立し、かつ明確化されたものに限定されなければならないということ。利用制限の原則とは、個人データは明確化された目的以外に使用されるべきではないということ。安全保護の原則とは、個人データは紛失、不正アクセス、破壊、使用、修正、開示の危険に対し、合理的で安全な保護措置により保護されなければならないということ。公開の原則とは、個人データに係る開発、運用、政策は一般的に公開されなければならない。データ管理者を明示して容易にアクセスできるようにしなければならない。個人参加の原則とは、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確認し得ること、自己のデータをわかりやすい形で知り得ること、自己に関するデータについて

異議の申し立てができ、異議が認められた場合にはデータの消去、修正、完全化、補正ができるということ。責任の原則とは、データ管理者はこれらの諸原則を実施するための措置に従う責任を有するということである。

その後、1990 年に EU（欧州連合）指令、つまりガイドラインより拘束力を持つものとして加盟国に立法化を義務づけるものが出された。90 年に案が提案され、95 年になって、個人データ処理に係る個人情報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指令として採択された。これによって EU 諸国は、この EU 指令に従った法律の制定しなければならなくなった。EU 指令は加盟国に直接その指令内容を適用するものではないが、しかし、その内容は加盟国を拘束して、その国々が 1998 年 10 月までに個人情報保護に関する法律を制定または改正することになる。各国はこの指令に従って法律をつくるという状況になっている。

EU 指令は、個人データの適切な保護措置を設けることにより、個人データの流通の促進を図ること、EU 域内での個人データの自由な動きを保障すること、いわば個人情報の利活用を図ることを目的としている。利活用を図るためには、逆に情報を保護しないといけない。OECD ガイドラインは、保護という面から 8 原則を提案した。これに対して、EU 指令は、むしろ利活用に視点を置いており、効果的な利活用を図るためには個人情報を守らなければいけないという観点から個人情報保護を唱えている。

この EU 指令の中には、第三国条項と言われるものがあり、第三国（日本やアメリカなど）にも EU と同じレベルの個人情報保護の制度を作るように要求している。このことが様々な問題を引き起こすことになった。

この第三国条項は、EU 内から第三国へ個人データの移転をする場合には、その第三国が適切なレベルの保護措置を確保していることを条件とするという内容である。つまり、EU から見て EU と同じレベルの個人情報保護の制度を持っていれば、その国には個人情報を移してよい。しかし、そうでない国には個人情報は移さないというものである。よく挙げられる例を言うと、例えば航空機に乗る際に、健康上の理由や宗教上の理由で、こういうものは食べられないということをあらかじめ航空会社に言っておくと、特別な食事を用意してくれる場合がある。しかし、これは、ある意味では病気や宗教といったセンシティブな個人情報を含むものである。このような個人情報を EU 域内の航空会社同士なら移転できるが、それ以外には提供しないということである。これは利用者にとってみると大変不便であり、また具合の悪いことである。

そこで適切なレベルの保護措置は何かということが問題となる。しかし、EU 指令では個々に適切な保護措置のレベルや形態は問わない。どういう判断をするかと言うと、実効性が確保されているかどうかを問題としている。OECD ガイドラインのような、目的制限や適正管理などに関わるものが十分に第三国でとられているかどうか、また、実効性確保のためには、規則遵守のための良好なシステムがあるか、規則が遵守されない場合に救済措置があるか、個人情報保護のための適切なサポートが受けられるか、といったことが要求された。

そこで、アメリカの商務省はセーフハーバー原則（safeharbor）を作った。それは、告知、選択、データ移転、アクセス安全性、データの完全性、そして実効性の確保という 7 つの原則である。これらを遵守することを宣言した企業については、EU と同水準の個人情報保護がなされているものとみなすという約束を EU と取りつけたのである。

日本は、まだこのような原則を EU とは結んでいない。したがって、場合によっては適切な情報が日本に流れてこないことも起こり得る。例えばがん登録に関する様々な情報で言えば、

日本の個人情報保護は適切なレベルに達していないと EU が考えた場合、がん登録に関するデータを日本に流さないということも起こり得るのである。

個人情報保護法が制定されたが、がん登録は適用除外になっている以上、何らかの規定あるいは実効性の確保というレベルでのガイドラインや法律を作っておかないと、ヨーロッパとの情報の流通に支障を来す懸念もないわけではない。

3. 個人情報保護法と個人情報保護条例

個人情報保護法が制定されるにいたった直接の契機は、住民基本台帳のネットワーク化に伴う個人情報保護への懸念から政府として個人情報保護に関する法整備を検討すると小渕内閣総理大臣が答弁したことにある。しかし、個人情報漏洩やプライバシー保護への関心が IT 社会の進展とともに広く意識されるようになったことも法律制定のきっかけとなっている。

我が国の個人情報保護制度を整理すると、憲法 13 条があり、その下に法律がある。そして各自治体における条例があるという仕組みになっている。

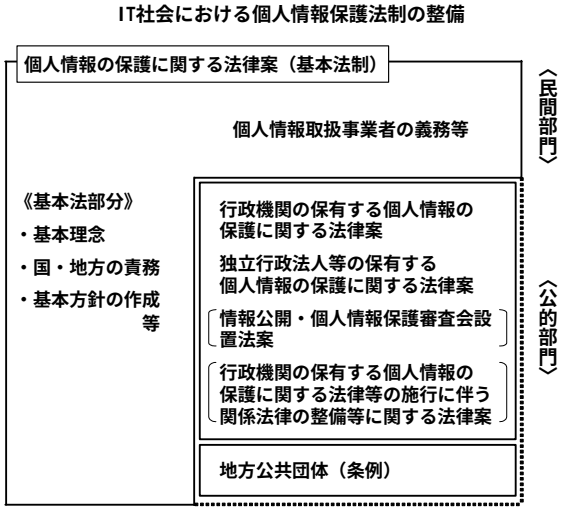
個人情報保護に関する我が国の歴史は、1981 年のプライバシー保護研究会の開催に始まる。そして、1988 年に民間行政部門の個人情報保護ガイドラインが作られた。法律としては行政機関について、行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律が制定された。その後、1994 年に高度情報通信社会推進本部が設置され、2000 年に個人情報保護基本法制の大綱ができた。そして 2003 年に個人情報の保護に関する法律が制定されたのを受けて、具体的な運用について 2004 年に個人情報の保護に関する基本方針が出されたのである。従前は個人情報保護について、（旧）通産省や郵政省等の分野でのガイドラインが存在した。また、1998 年に当時の通産省の外郭団体である日本情報処理開発協会がプライバシーマーク制度（P マーク）を設け、プライバシーをきちんと守っているかどうかのいわばお墨付きを与えるといった制度も存在していた。しかし、それはあくまでもガイドラインであり、法律よりも下のレベルであった。そこで法律のレベルで個人情報保護が必要ではないかという認識のもと、個人情報保護法へと向かっていった。国民が安心して IT 社会の便益が受けられるように、個人情報の適正な取り扱いのルールを定め、国民の権利利益の侵害を未然に防止しようという考え方で、個人情報保護法制定へ向かったのである。

その背景には、情報通信技術の発達によるコンピューターネットワークを利用した多量の個人情報が処理される中で、個人情報の漏洩などに対する社会的な不安が拡大している。個人情報の適正な取り扱いのルールを定め、国民の権利利益の侵害を未然に防ぐ必要があるという考えがあった。

具体的な立法の経緯を見ると、2001 年に個人情報保護に関する法律案が提出されたが、メディアからの反対で廃案に追い込まれた。その後行政機関等を含めた 5 法が提案され、色々な議論を経て継続審議となり、2003 年再提出され、5 月 23 日、第 156 国会で成立した。

個人情報保護法の仕組みは、民間部門と公的部門とに共通する形で、基本法となる基本理念

表 3. 個人情報保護法制の仕組み



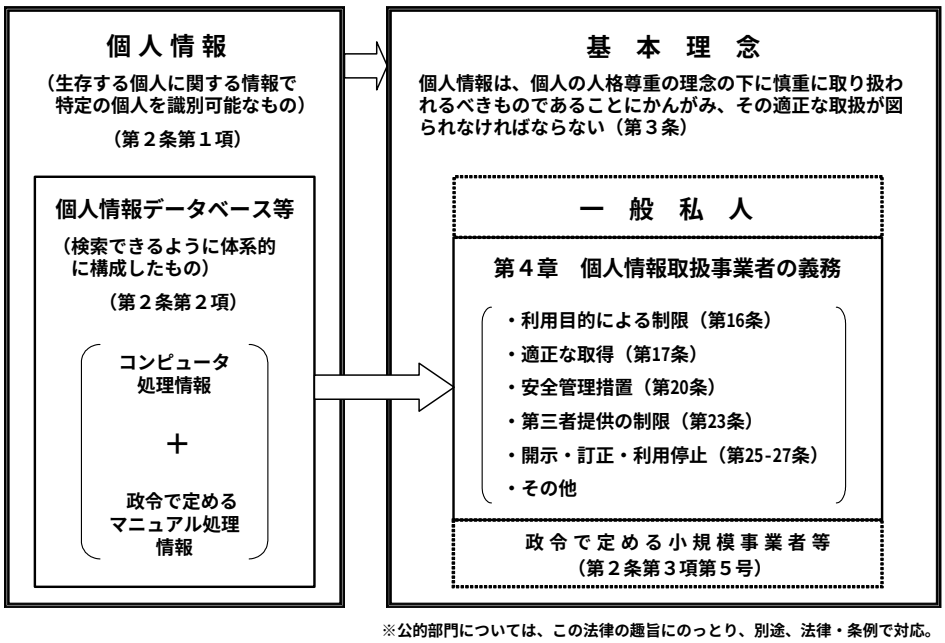
がある（表 3)。国や地方の責務あるいは基本方針の策定等が、基本法となるものである。そして、民間部門については個人情報保護法の中のいわば一般法的なものとして、個人情報取扱事業者の義務を定めている。公的部門には、それぞれの法律を定めた。前述の 5 法のうち、個人情報保護法を除く 4 法がそれに該当する。そして、地方公共団体は条例を定める。これが基本的な枠組みなのである。

個人情報保護法は第 1 条で、「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することに鑑み、個人情報の適正な取り扱いに関し基本となる事項を定め、国及び地方公共団体の責務等を明らかにするとともに、個人情報を取り扱う事業者の遵守すべき義務等を定めることにより、個人情報の有益性に配慮しつつ、個人の権利利益を保護することを目的とする」という目的規定を置いた。第 2 条で定義規定を置いて、様々な概念の整理が行われている（表 4)。法律では個人情報というものを広くとらえている。コンピューターで処理される情報に限らず、マニュアル情報でもきちんと体系的に検索できる扱い方になっているものも個人情報データベースと称することにした。そして、個人情報データベースで取り扱われている個人情報を個人データと定義した。さらに、その個人データのうち、個人情報取扱業者の義務として開示や訂正などに応じなければならない性質のデータのことを保有個人データと定義した。

すなわち、個人情報とは、データベース化されていない雑然としたものを広く言う。そして、それを検索できる（コンピューター情報でもマニュアル情報でも）ようにしたものを個人情報データベースとする。そこに載っているものが個人データである。そして、その開示・訂正・追加・削除に関する義務を事業者が負わされるものを保有個人データとした。個人情報保護の観点から言うと、個人情報取扱事業者として、国、地方公共団体、独立行政法人、その他に政令で 5,000 件以下となっているが、これを除くものを個人情報取扱事業者とするわけである。

個人情報保護法は、個人情報データベースに対して個人情報の取扱事業者の責務を定めて、守らせるという仕組みとなっている。個人情報は、個人の人格尊重の理念のもとに慎重に取り扱われるべきものであり、適正な取り扱いを図らなければならないということが基本理念で

表 4. 対象となる個人情報、事業者の範囲等



※公的部門については、この法律の趣旨にのっとり、別途、法律・条例で対応。

ある。これを受けて最初の法律案では、OECDの原則に沿うように、基本原則をうたっていた。しかし、これは個人情報取扱事業者の義務のところで整理できるだろうという考え方で、削除された。

個人情報取扱事業者が何をしなければいけないのかについて外部からの脅威との関係で整理をしてみる（表 4)。安全管理義務、従業者への監督義務、委託者への監督義務という義務がある。従業者などがその媒体等を持ち出したりすることの脅威に対して、監督義務を負っている。さらには、委託業者への監督する義務も負っている。情報の漏洩には、外部からの攻撃だけでなく、従業者や委託先等から漏れていくことの方が多いので、それに対する監督義務等を定めたのである。

本協議会との関係で言えば、第三者提供等の制限についての考え方は、（がん登録が本法から除外されるにしても）ご理解いただきたいところである。第三者提供の制限とは本人同意が原則であるということである。個人情報取扱事業者は、本人同意を原則として第三者へ提供しなければならない。ただし、例外として法令による場合、人の生命、身体、財産の保護、公衆衛生等に特に必要な場合、がん登録の場合、例外として第三者提供が認められると整理されている。自己情報をコントロールする権利という考え方からすれば、第三者提供における本人同意の原則が出てくるのは言うまでもないところである。その仕組みとして、オプトアウト方式を取り、外部提供をやめてくれと言えば、止められるという仕組みを置いた。なお、第三者提供といっても、何が第三者かということが問題である。例えば委託先への提供、合併等に伴う提供、あるいはグループでの共同利用といった場合は、第三者に当たらないということになっている。公衆衛生の向上のために特に必要がある場合、本人の同意を得ることが困難であるというときに、本人の同意なしに第三者提供が認められるということが第 23 条の第 3 号で規定されているが、これは疾病の予防や治療に関する研究等の場合には、社会全体でネットワークを形成する必要性があるという考えのもとで、例外とされたのである。

法律をつくる際の基本的な議論の中で、適用除外とされたものとして報道、著述、学術研究、宗教、政治がある。がん登録それ自体は事業であるので、学術研究という範疇で取り扱われることにはならないのかもしれない。しかし、医学の研究つまり学術研究の目的であるという側面から考えると、これは第 50 条の規定で適用除外とされているのである。

各自治体では個人情報保護条例あるいは情報セキュリティーポリシーを設けて、個人情報保護に取り組んでいる。すべての都道府県で個人情報保護条例を制定している。情報セキュリティーポリシーについても、1 団体を除く 46 都道府県が持っている。市区町村でも 3,199 団体のうち 2,521 団体（78.8%）が個人情報保護条例を制定し、1,802 団体（56.3%）が情報セキュリティーポリシーを定めている。

これは 2004 年の 1 月の状況であり、現時点ではさらに増えている可能性がある。自治体においてもかなりの所では条例を制定して、個人情報保護に努めていると言えよう。

4. 地域がん登録と個人情報保護

がん登録で扱われる情報はセンシティブな個人情報である。センシティブな個人情報をどう取り扱うべきかについて考えたい。国の法律、すなわち個人情報保護法ではセンシティブ情報とそうでない情報と仕分けしていない。しかし、条例によっては、センシティブ情報の収集に制限をかけているものがある。東京、大阪や宮城県の条例などがそうである。また、センシティブ情報の収集は原則不可であるけれども、審議会の承認を得て収集を認めるところもある。大阪府や宮城県などがそうである。その際は、個人情報保護審議会で、例えば、ある事業をやるに当たって、こういう情報を集めていい

か、提供していいかという議論をしていただく必要が生じる。がん登録に関しては、兵庫県でこれを認めないとする審議会の議論があり、がん登録事業ができなくなっていることは、周知の通りである。

ここでの問題点としては、審議会の委員の中に医師が入っている場合がほとんどないということが挙げられる。一般市民と学識経験者、あるいはマスコミらが審議会委員の構成となっていることが多い。がん登録事業というものを正確に理解している人が、審議会の委員の中に一体何人いるのだろうかということが問題である。ましてや一般の市民にとって、がん登録の意義は分からないだろうと思われる。その点では、がん登録関係の方々には、色々な機会にがん登録とはどのようなもので、なぜ必要なのか、どういう効果があるかということについて、いわば広報活動を進めていただきたいと思う。自治体の個人情報保護条例の審議会で、がん登録事業の審議が行われるときに、健康福祉課などの行政の担当者が説明をする場合が多い。しかし、行政の担当者が必ずしもがん登録事業をきちんと分かっているとは限らない。その意味では、審議会で熱心な議論ができるための情報提供すらされてない場合もあるのではなかろうか。その意味では、今後、がん登録事業の意義というものが広く周知されることが重要ではないかと思われる。

もう一つの問題として、がん登録に協力する医療機関の設立主体が様々であることが挙げられる。そのため適用される法的な根拠が統一されていない。独立行政法人等の医療機関では独立行政法人等の保有する個人情報保護法が、公立の医療機関では都道府県の条例が適用される。民間の病院では個人情報保護法が適用される。つまり、がん登録事業を進めていく上での法的な仕組みが必ずしも一つでないために、混乱した状況にあると言わざるをない。2004 年 1 月に厚生労働省の健康局長通知により、地域がん登録事業に関する個人情報保護法との関係が整理された。すなわち、利用及び提供の制限における本人同意の原則も適用除外であるという通知である。その意味では法律との関係は一応整理されたと言っていいわけであるが、しかし条例などとの関わりで残された問題は多いと思われる。

翻って考えると、事業の必要性や有効性ということもさることながら、やはり一般の市民にとっては、何をやっているのかよく分からないのであり、個人情報漏洩に対する不安が強い。これが個人情報保護の必要性を支える根拠でもある。昨今個人情報の漏洩に関する事例は相当数にのぼっている。社会保険庁からの情報漏洩が最近の新聞に報道されていた。2004 年 1 月、ある大手通信事業体から多くの情報が流れて、1 人 500 円の金券とおわび状を出して、その結果かかった費用は 40 億円であったと言われている。数年前に京都の宇治市で検診情報のシステムづくりを実施していた再委託の下請のアルバイト学生が、市の住民基本台帳の中から得た約 20 万人のデータを名簿屋に売ったという事件があった。これに対して 3 人の市会議員が損害賠償請求を起こし、最高裁において 1 人 1 万円の損害賠償が認められた。5,000 円の弁護士費用を加えて 15,000 円掛ける 3 ということで宇治市は45,000円払わされた。しかし、これが住民全員からの提訴であれば市の負担は膨大なものになる。経済的な損失だけではなく、情報が漏洩することのリスクは非常に大きい。やはり社会的な信用そのものが失われる。さらに言えば、ある事業をやったときに情報が漏れてしまえば、その事業ができなくなってしまうことすらあり得る。その意味では非常に怖い問題を含んでいる。

また、情報漏洩が簡単に行われてしまうという状況は、単にその事業ができなくなるとか、あるいは損害賠償請求を負わされるといったことだけではなく、社会そのものがプライバシーや個人情報に対する関心度が低い、不安な社会であるということを意味する。その意味で個

人情報の適正な取り扱いは、言うまでもなく必要であり、そのシステムづくりが不可欠なのである。個人情報の漏洩は情報主体への不利益、企業の不利益、社会の不利益など、様々な不利益をもたらす。個人情報の適正な管理のためには、個人情報保護に関する内部規定の整備、情報管理者の配置、個人情報へのアクセス環境の改善、職員への教育の徹底、監査体制の強化改善、業務委託の見直しと改善などが図られなければならない。職場に誰がいるか把握できているか、コンピューター室への入退室は適切か、データへのアクセス管理は適切か、委託業者への管理は適切か、これらのチェックが必要なのである。

個人情報はただ保護すればいいというものではなく、その適正な利用との兼ね合いが重要である。がん登録との関係においても、がん登録の有用性は否定しがたいものである。なお今後一層、がん登録事業が発展されるべきだと思う。その実施に当たっては、情報セキュリティーすなわち情報漏洩の防止という観点から、適切な個人情報保護をいかに図るかということが重要となる。

全くの私見として申し上げるならば、以上のような錯綜している法状況にあって、やはりがん登録事業そのものを法的に認める、いわばがん登録事業法とでもいうべき法律を作って、統一した形でがん登録事業が成功するような基盤づくりがなされることが必要ではないかと考える。このことは、多くの先生方のお考えの中にもあると伺っているが、まさにこれからは一つの事業として法律をつくり、その中で個人情報を守りながら、がん登録が今後一層充実したものになっていくことを願ってやまない。

Summary

The Law for Protection of Personal Information was enacted by the Japanese Diet in 2003. In this Lecture, I summarized several important concepts regarding the protection of personal information; definition and classification of personal information, distinction between personal information and privacy, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980 and European Union (EU) Detectives on the Protection of Individuals with Regard to the Processing of Personal Data and Privacy in 1990, and contents of the Law for Protection of Personal Information in Japan. The Japanese government declared that this Law was inapplicable to cancer registry because of its importance to public health and academic research. It is needless to say, however, that cancer registry should have every necessary measure to protect the cancer patients and contribute to the public health. I would propose that the Law for Cancer Registry be enacted in Japan.