

■ Topics | トピックス

## 「製薬協メディアフォーラム」を開催

テーマは「個人情報保護法改正の動向と医療情報の立法政策のあり方」

2020年2月5日、日本橋ライフサイエンスハブ(東京都中央区)にて、「製薬協メディアフォーラム」を開催しました。今回は「個人情報保護法改正の動向と医療情報の立法政策のあり方」をテーマに、新潟大学大学院現代社会文化研究科・法学部教授の鈴木正朝氏より講演がありました。当日は20名の記者が参加しました。以下は鈴木氏の講演内容の採録です。



講演の様子

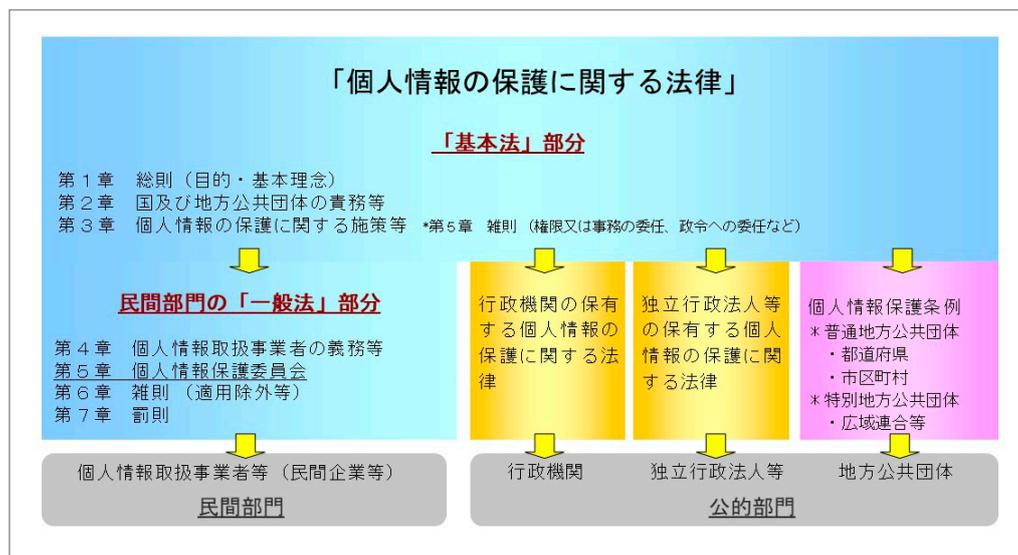
### 個人情報保護法制の全体構造と成り立ち

我が国の個人情報保護法の全体構造は、民間部門では個人情報取扱事業者等の民間企業を対象とする「個人情報の保護に関する法律」(以下、個人情報保護法)が、公的部門では中央官庁等を対象とする「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)、国立大学・国立大学病院等を対象とする「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)、都道府県・市町村・広域連合等の地方自治体を対象とする「個人情報保護条例」があり、これら全体を個人情報保護法の第1章～第3章からなるいわゆる「基本法」部分が全体を規律する建付けになっています(図1)。



新潟大学 大学院現代社会文化研究科・法学部 教授 鈴木正朝氏

図1 個人情報保護法制の全体構造



もともと個人情報保護法制については、国が立法政策に関与しない時期に、先進的な自治体が海外の立法例を調査し、有識者を招いて条例を作ってきた歴史がありました。我が国の個人情報保護法制は、自治体が作り上げてきたと言えると思います。

その後、汎用機の普及とともに、大手企業、自治体、国等が汎用機を使ってデータベースを運用してきたことに伴い、1988年に初めて「電子計算機に係る個人情報の保護に関する法律」を作りました。日本の個人情報保護法制の黎明期は自治体が、次に国が行政機関だけを縛る1988年法を制定し、この法律の後継が現在の行政機関個人情報保護法となります。当初は電子計算機の処理情報に限定した法律でした。

民間では、業界団体ごとに省庁の指導を受けながら、業界のガイドラインで個人情報を取り扱ってきた経緯がありました。長らく自主規制の時代が続きます。ところが、1999年に住民基本台帳ネットワークシステム（以下、住基ネット）導入を目指した住民基本台帳法の改正法案を国会に提出するにあたり、当時の自民党、公明党、自由党の連立与党の3党合意で個人情報保護法を作ることが決まりました。国民からの批判に対応する必要があったからでした。当時の霞が関は、包括的な一般法では、利活用において過剰反応が問題になるということで、ガイドライン行政で十分であるという立場でした。私も当時は業界団体におりましたので、自主規制で十分だという意見を述べておりました。住基ネットを入れるという政治決定の前に霞が関と業界の意見は退けられたかたちになり、1999年改正住民基本台帳法とともに個人情報保護法も通過させるべく急ぎ法案が起草されることになります。

しかし、その後は、メディア規制法であると新聞協会やペンクラブ等から大きな批判が沸き起こり、2度も継続審議となり、3度目にはとうとう廃案となったため、報道機関の適用除外条項を入れ基本原則を除く等意見をとり入れた法案を新たに提出し直して、2003年に、現在に続く民間部門を規律する個人情報保護法が初めてできあがりました。

その後、マイナンバーを導入するにあたり、同じく共通番号制度である住基ネット訴訟の最高裁合憲判決の理由中に示された趣旨を踏まえて、第三者機関を設置すべきということになり、番号法の中で独立行政委員会として「特定個人情報保護委員会」ができました。それが2015（平成27）年改正で、従来の主務大臣制を改めて、民間部門の個人情報保護法を個人情報保護委員会の所管とするように権限を拡大し今日に至ります。現在、総務省が所管している行政機関個人情報保護法と独立行政法人等個人情報保護法の公的部門の権限も個人情報保護委員会に統合し、ルールも整合させようということが検討されています。どうやら統合の方針にあるようです。自治体の個人情報保護条例も法律でひきとるべきかどうかについては現在自治体のヒアリングをしている段階で結論は出ていません。

## 個人情報保護法制2000個問題

従来は主務大臣制といって、経済産業分野は経済産業大臣、総務省所管範囲は総務大臣、医療系は厚生労働大臣が、個人情報保護法の監督・執行をすることになっていました。それが、縦割り行政のまま個人情報保護法を解釈した結果、実は個人情報該当性の判断基準が異なっておりました。厚生労働省だけ特別な解釈をしていたのです。提供先基準を採用し、「連結可能匿名化」という特殊な解釈をして医療現場のニーズに添っていたわけです。しかし、これは通常あり得ないことです。政府解釈においては、1つの法律1つの解釈でないといけません。この問題は、2015(平成27)年改正で、個人情報保護委員会に権限が一元化されることで解消されました。

残るは10年前から私が主張している「個人情報保護法制2000個問題」(以下、「2000個問題」)です。「2000個問題」はなにかと言うと、ルールが2000個、権限が200個に分立しているということによる弊害のことを言っております。これは日本の個人情報保護法制が福岡県春日市にはじまる地方自治体の取り組みの中で育まれてきたという歴史的経緯を踏まえて、個人情報保護法5条が、自治体ごとに区域の特性に応じて取り扱うことを認めているように、言うなれば基本仕様がそうになっている、制度設計上そのようになっているということの帰結です。これが、広域災害対応の中で、またデータ社会に移行していく過程でその弊害が顕著に現れてきたというわけです。

2000個の数え方ですが、まず「個人情報保護法」「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3つの法律があります。次に、普通地方公共団体の「個人情報保護条例」が、2010年現在で1912個(都道府県47、市町村1727、特別区23)あります。加えて、特別地方公共団体(広域連合、一部事務組合)の「個人情報保護条例」が100近くあり、これらをすべて足し合わせるとゆうに2000を超えます(図2)。よく「行政機関個人情報保護法」を真似ているから、大方同じだと言う人がいますが、かなりばらつきがあります。個人情報の定義も10種類以上あると思います。ゲノム情報が個人情報になる自治体もあれば、ならない自治体もあります。病院の9割5分は民間病院ですから、「個人情報保護法」が90数%適用されているので問題ないと言う人もいるかもしれませんが、希少疾患や難病は基本的には国公立大学病院や自治体立病院が診ていまずので、単純に数や割合だけで論じることはできません。病院間の適用法バラバラ問題は結構深刻だろうと思いますし、厚生省等の指針等の弥縫策で逃げてると手戻りの連続だろうと思います。明らかに今後の情報化の障害として立ちはだかり続けると思います。

図2 医療分野における個人情報保護法：法律・条例の適用例

個人情報の取扱い主体	適用法	所管省庁等	個人情報の取扱い主体	適用法	所管省庁等
厚生労働省	行政機関個人情報保護法	総務省	XX広域連立□□病院	XX広域連合個人情報保護条例	XX広域連合
独立行政法人国立病院機構岩手病院	独立行政法人等個人情報保護法	総務省	一部事務組合立△△病院	一部事務組合△△病院個人情報保護条例	一部事務組合△△
岩手県立病院	岩手県個人情報保護条例	岩手県	●●市立凸凹病院	【指定管理者募集要項や条例に規定されている場合】 →●●市個人情報保護条例	●●市
地方独立行政法人宮城県立病院機構	宮城県個人情報保護条例	宮城県	指定管理者：民間事業者(医療福祉法人凸凹会)	【指定管理者募集要項や条例に規定されていない場合】 →個人情報保護法(?)	個人情報保護委員会(?)
気仙沼市立病院	気仙沼市個人情報保護条例	気仙沼市	◇◇衛生組合立	適用法(法規制)なし	なし(◇◇衛生組合の自主規制)
日本赤十字盛岡病院	個人情報保護法	個人情報保護委員会	○○地区休日急患診療所	<法の空白地帯>	
財団医療法人○○会病院	個人情報保護法	同委員会			
個人医院	個人情報保護法	同委員会			

病院を見ていくと「2000個問題」の現実が見えてきます。個人情報の取り扱い主体によって適用される法律や所管省庁等が異なっていて、カルテやレセプト情報のデータベースの連携や緊急対応等を阻害する原因の一つになっています。つまり、患者さんが病院に担ぎ込まれた緊急事態への対応に、医療情報の取扱いやメディア対応に戸惑う病院に迅速に指導、通達等行うべき役所がバラバラになるのは、個人情報保護法制におけるこうした縦割り行政の弊害による結果です。これは、自治体をまたぐ広域災害でも問題になります。

立命館大学情報理工学部の上原哲太郎教授が、「2000個問題」を調査しました。まずは、47都道府県、20政令指定都市の67個に限定しても、個人情報の定義がこれだけ違うことがわかります(図3、4)。

図3 「個人情報」の定義の違い(47都道府県)

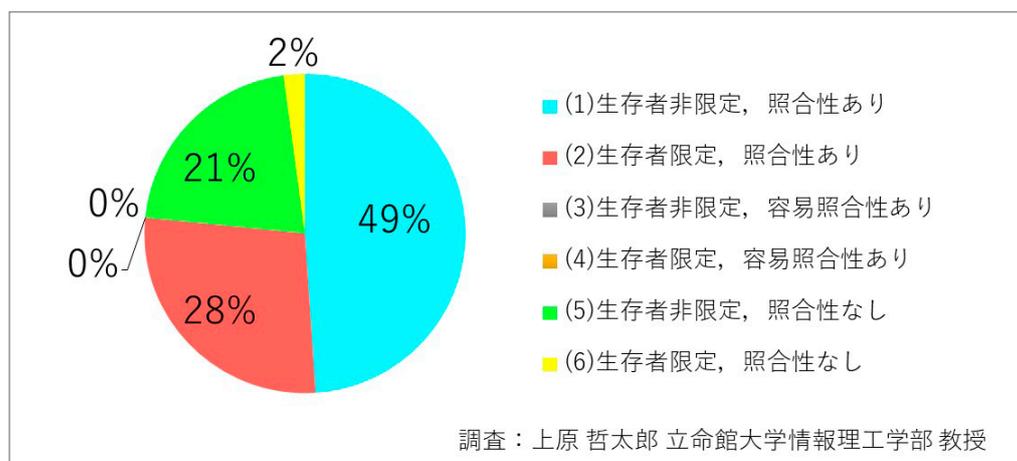
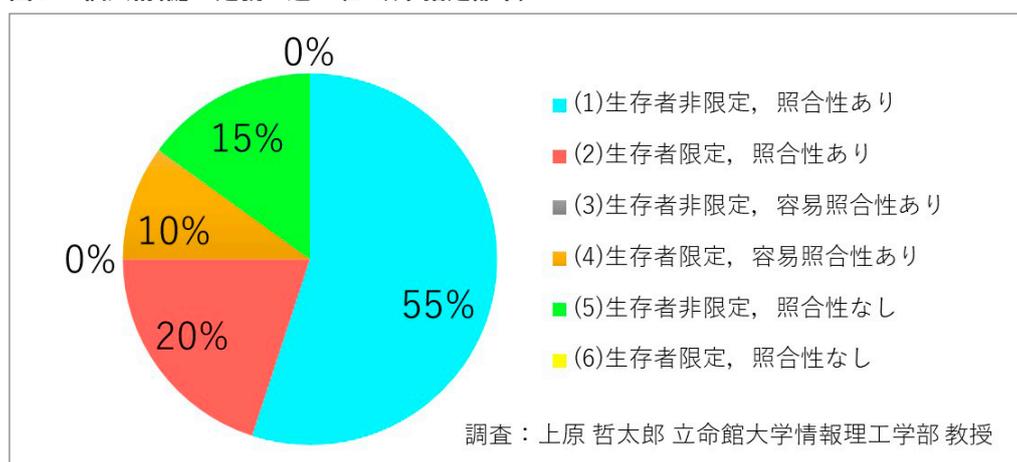


図4 「個人情報」の定義の違い(20政令指定都市)



定義の条文の文言の違い、加えて個人情報該当性判断基準等解釈の違いにより、たとえば、私立病院では個人情報保護法に従い、一定のゲノム情報単体を個人情報に該当するとしているのに対して、個人情報に該当しない公立病院が出てきたりするわけです。こういったことが、今まであまり問題にならなかったのは、厚労省等のガイドライン、ガイダンス、指針等告示や通達において、条例をいわば上書きして病院関係者が条例をみずらに告示中心で運用してきたところが多かったからだと思います。下位ルールが上位ルールを破るわけです。とても法治国家とは言えない中で、なんとかしのいできていたということです。ただ、法務機能が充実している組織ほどに問題に直面していたということはありません。

ここにEUの一般データ保護規制(General Data Protection Regulation : GDPR)が登場します。希少疾患やゲノム含めて、医療データや創薬データをグローバルに流通させることに取り組まねばならない時代に、明らかにEU並の保護水準に達していない日本の国内法制とその運用実態にあつては、EUの求める十分性を満たすことはできずデータ交換は常に停止されかねない法的リスクに直面していたと言えます。先般、悲願の十分性の相互認定になんとか温情でこぎ着けましたが、それとてその対象は民間部門だけのことです。行政機関個人情報保護法、独法等個人情報保護法や個人情報保護条例で規律される公的部門はEUとのデータ交換に大きな不安を残しています。国立がん研究センター、国立大学病院や公立大学病院やその他の自治体立病院は蚊帳の外のまま放置されています。私立病院や市立大学とその付属病院は民間部門ですので問題はありませぬ。同じ研究機関、同じ病院なのにこの違いです。

研究機関や製薬業界が、世界中からゲノムデータを集めゲノム創薬の研究開発をする、そしてグローバルに事業展開するに際しても、このような状況ではなかなか前に進めません。研究開発拠点のEU移転も検討課題とならざるを得ないところ

があります。

現在の条例の大多数が、オンライン結合禁止条項をもっています。日本は電子政府化を標榜しマイナンバー制度を導入しましたが、それは国だけの話であり、条例の基本思想は、電算機の外部との接続、ネットワーク化を危険視したままにあります。共通番号も忌み嫌っているわけです。確かにスタンドアローンで運用し、電算センターの入退館等、安全対策基準を厳格に守り、データベースごとに独立した識別子とし共通番号制度を忌避した方が安全にリスク少なく運用できるかもしれません。

しかし、こうした思想に立脚した個人情報保護条例が2000も分立している限り、電子政府化含むデータ社会への移行はなかなか進まないのも当然です。

それから例外条項の内容もバラバラです(図5、6)。ルールがバラバラなだけでなく、あの3.11にあっても、例外条項を適用し個人情報を国に提供したのはたった2件だけでした。岩手県と福島県南相馬市だけです。災害時の大混乱の時期にあっては、例外条項があってもそれにあてはめて判断することができなかったということでしょう。ルールを法律で統一し、権限を個人情報保護委員会に統合し、その政府解釈を適時に通達していくことの方が合理的ではないかと思います。

図5 電子計算機処理・オンライン処理の制限(47都道府県)

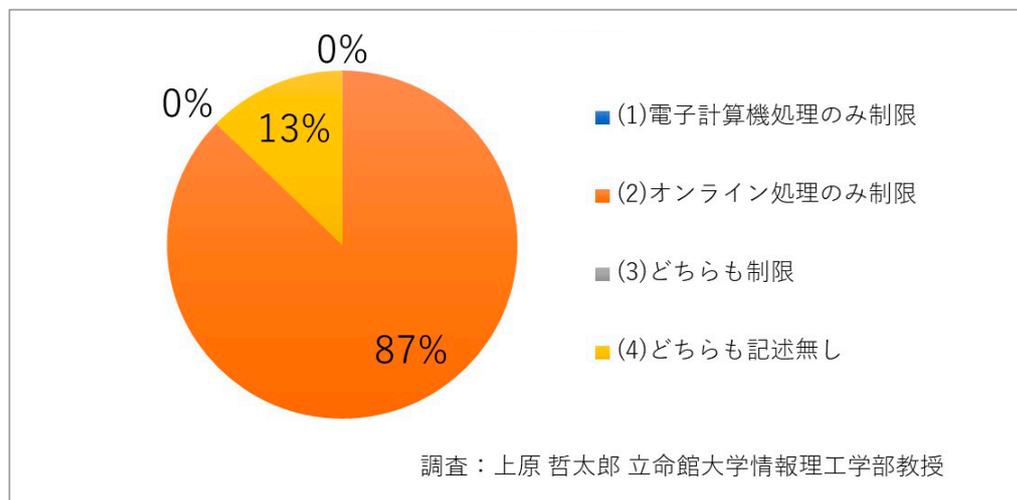
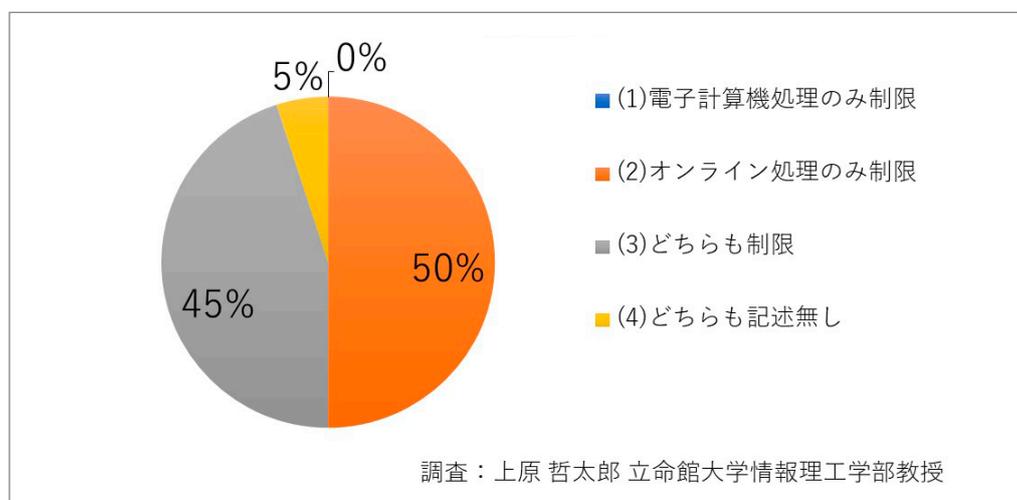


図6 電子計算機処理・オンライン処理の制限(20政令指定都市)



実は個人情報保護法の適用除外には、報道目的のほかにも、学術研究目的と政治目的と宗教目的があります。医療創薬においては、学術研究目的の適用除外条項は非常に重要です。学術研究に限定された利用目的の範囲内であれば、本人

の同意なく、個人情報保護取扱事業者等の義務規定の適用なしに、自組織の倫理委員会の意見等を基礎にした各組織の長の判断のもとで、自主規制によって個人情報を取り扱うことができることになっています。しかし、先に述べた「2000個問題」としてルールと権限が2000に分かれているため、学術研究目的の適用除外を定めていない都道府県が13も存在します。「2000個問題」を放置しているため、病院同様に国立大学、公立大学、私立大学間の個人情報の取扱いルールが異なり日本の学術研究の発展の障害となっていました。

### 「医療ビッグデータ政策」から「医療クオリティデータ政策」へ

さて、35年後の2055年には、日本の総人口は8800万人になると推計されています。現在の生活水準を維持していきなければ、より高付加価値の次世代産業を立ち上げなくてはなりません。そのときに、製薬業界はなにをやっていけば良いのかを考えてみます。

従来推進してきたのは「医療ビッグデータ政策」です。これは、大量の「匿名加工情報」を医療分野および関連分野を横断的に収集・分析して、主に相関関係の知見を得るのが狙いです。対象情報は、公私の医療等情報および関連情報で、それらの相関関係を探っていきます。手法は非個人情報化(Anonymisation)による本人保護と利活用推進策です。これを行うためには、先ほどの「2000個問題」の解消が必要です。ここが解決しない限り、医療ビッグデータ政策は花開きません。

次に推進すべきなのが、「医療クオリティデータ政策」です。これは正確な「医療仮名加工情報」を医療分野内で収集・分析し、主に因果関係の知見を得ることを目的とします。因果関係的知見を得るためには、正確な情報を取得する必要があります。ただし、対象情報は公私の医療情報に限定すべきだと考えます。手法は医療仮名加工情報(Pseudonymisation)による本人の保護と利活用の推進です。日米欧の法体系は異なりますが、対象情報の概念整理は法体系の違いを乗り越えて整合することが可能ですので、日本法においても、匿名と仮名の概念を整理し、EU・米国と同じ概念でやりとりをできるようにして、日米欧のData Free Flow with Trust (DFFT)の基盤を作り、希少疾患等のデータ含めて日米欧のデータベースの連携を図っていくべきです。対象は医療情報に限定するので、特別法の制定ができます。これをたとえば「医療仮名加工情報法」として制定するよう提言していきたいと思っています(図7)。

図7 医療ビッグデータ政策から医療クオリティデータ政策へ

医療ビッグデータ政策から医療クオリティデータ政策へ	
医療ビッグデータ政策 →	医療クオリティデータ政策
ねらい：大量に匿名加工情報を医療分野及び関連分野横断的に収集・分析し、主に相関関係的知見を得る。	ねらい：正確な医療仮名化情報を医療分野内で収集・分析し、主に因果関係的知見を得る。
対象情報：公私の医療等情報及び関連情報(ヘルスケア等)	対象情報：公私の医療情報
手法：非個人情報化(Anonymization)による本人保護と利活用推進策	手法：(医療)仮名化(Pseudonymization)による本人保護と利活用推進策
GDPRとの対応：前文26項(anonymous information)	GDPRとの対応：第4条第5号(pseudonymization)
対策：「一般法」の改正 2000個問題の解消	対策：「特別法」の制定 例) 医療仮名データ法(仮)

「医療クオリティデータ政策」が必要な理由は、医療個人情報は「匿名加工情報」等の非個人情報化での利活用には限界があるからです。たとえば、脳のスキャンデータ、レントゲン、臓器写真等の画像情報は本人と1対1の関係にあるという意

味で氏名等を削っても仮名加工情報であり個人情報に該当します。なお、厳密に言うなら、この影像情報の個人情報該当性の評価は自治体ごとに変わる場所はあるでしょう。こうした影像情報を匿名加工情報とするために、たとえばかかる影像にモザイク処理をすることになりますが、医学的にまったく無意味な情報になってしまいます。そこで、こうした影像情報等を本人同意なく第三者提供したり、学会等で公表したりできるように従来採用してきたのが「連結可能匿名化」という考え方です。これにはそもそも矛盾があります。連結可能であるなら匿名化したとは言えず、それは個人情報にほかならないからです。

医療IDを導入したら、医療ID自体が個人情報になります。ひもづく医療情報はすべて個人情報と評価されることとなります。医療等分野に限定した仮名加工情報に関する特別法を作り、仮名加工情報(個人データ)を利用できる道を開く必要があります。医療データのトレーサビリティやポータビリティ、また消去権を確保するためには特定個人が識別できる必要がありますから個人データでなければなりません。そのため、医療データは常に個人データとして検索可能なように体系的に構成されているべきです。

では、具体的にどのような法律を作るべきでしょうか。

主体は認証制度とし、資格者として医師と指定研究者に限定します。対象は法律によって厚労省が指定する特定医療データベースに限定します。なんでも良いのではなく主体と対象を限定するのです。対象情報は「医療仮名化情報」にします。2020年の改正で仮名化情報の概念が入りますので、その医療版の特別法を作れば良いのです。

次に、利用目的は法定利用目的に特定します。現在の個人情報保護法は、利用者が自由に利用目的を特定できますが、特別法では、利用目的を法律で(1)学術研究・公衆衛生、(2)本人治療、(3)創薬に限定します。データ移送は、個人情報保護委員会が指定する暗号化措置を取り、処理施設は厚労省が指定する特定安全対策事業所を指定します。個票(医療仮名化情報)は、学術的な検証可能性を担保した後に消去します。個人情報保護委員会の指定団体による監査も入れます。

措置としては、違反した場合には医師免許の停止、取消、本処理の資格停止を行います。罰則は医師法に準じる直罰(懲役)です。効果としては、医療仮名加工による本人の同意なく第三者提供できる、データの収集と分析ができるということなのです。

つまり、ルールを厳格に縛ったうえで、一人ひとりの正確なデータを本人の権利利益を害することなく仮名加工情報として大量に取り扱うことができるようにすべきという意見です。これが実現できれば、AIによる画像診断の精度を飛躍的に向上させ、また、病気の早期発見、早期治療につなげ、医療費総額の上昇を抑えることにも寄与するだろうと思います。

## 記名式Suica履歴データ無断提供事件

「記名式Suica履歴データ無断提供事件」(以下、「Suica事件」)を理解することによって、2020(令和2)年の個人情報保護法の改正のポイントの一つが見えてくると思いますので、ここで振り返っておきたいと思います。

結論を先に言うなら、これは、今回の改正案にある仮名加工情報を理解するうえで格好の事例ということができます。要するに個人情報とは何か、非個人情報化の一つである「匿名加工情報」はいわば個人情報の概念を裏から問いかけるものでした。いわばその中間に位置づけられるような仮名とはなにかを教えにやってきたのがこの事件でした。残念ながら7年前の事件当時私どもの問題提起に対しては、情報法を扱う少なからぬ弁護士さんやIT企業等法務部門の方々、財界からもビッグデータビジネスを阻害し、個人情報の有用性への配慮を欠くプライバシー原理主義的な意見であると大きく指弾されました。メディアも法的な問題としてではなく消費者の不安に応えなかった問題だという理解での報道が大半でした。要するに日本には仮名という概念がなかったということを意味しています。要するに個人情報の概念の明確化をなしえずにいたということでもあります。

この事件の事実の概要は、次の通りです。JR東日本が日立製作所(以下、日立)にSuicaのデータを加工して提供し、日立はそのデータを分析し、駅利用状況分析レポートという統計情報にして販売するというものでした。しかし、JR東日本が、今日でいうところの仮名加工情報のままSuicaデータを引き渡していたことが後に判明し社会問題となったという事件でした。

JR東日本は、社内に情報ビジネスセンターを作り、社内に障壁を立てて、彼らの考えるところの匿名処理をしたうえで、非個人情報化したという理解のもとで、本人の同意またはオプトアウト手続きを不要と解して通常のデータとして日立に売却しました。

ここで問題になっているのは、利用者氏名、フリガナ、電話番号、性別を記録している定期のSuicaですが「記名式Suica」と言っています。この記名式Suicaをそれなりに加工したもののこれがまだ個人データのままであったことが問題でした。記

名式Suicaデータベースには、Suica ID、利用者氏名(フリガナ)、電話番号、生年月日、性別コード、乗降履歴データが記録されています。乗降履歴には入札情報と出札情報(それぞれ駅番号、ゲート番号、年月日時分秒)、鉄道利用金額が記録されています。またキヨスク等での購買履歴(物販情報)もデータベースに記録されます。

このSuicaデータベースを社内のビジネスセンターに提供するときには、氏名、フリガナ、電話番号は消去し、生年月日の日を削除する処理をしていました。さらに、それをビジネスセンターから日立に販売提供するときには、Suica IDが原データ(提供元のデータベース)と照合できないように、ハッシュ関数を用いて不可逆的に生成した別番号と置換しており、かつ提供の都度それを変更しておりました。物販情報も削除していました。JR東日本は、これだけの処理をしているので、日立においては特定個人を識別することはできないと原データと容易に照合することもできないデータになっていると考えました。

しかし、これは未だ個人データのままであると主張しました。なぜなら、JR東日本において原データと当該提供用のデータを照合すれば、容易に個人が識別されてしまうからです。つまり、提供用データには、生年月のほかに、乗降履歴があります。乗降駅の駅番号、ゲート番号があり、秒単位でゲートを通過した時間が記録されているわけですから個性ある唯一無二のデータになってしまいます。提供元データベースにも同じ履歴データがあるわけですから、この履歴部分を照会すれば、容易に照合可能です。当然に原データに記載の内容を見て、誰のデータであるかがわかってしまうことになります。

要するに頭の部分のSuica IDだけ匿名化して、体の部分の履歴データをそのまま生データとして出しているのです。同種のデータベースは多数あると思いますが、一般的には履歴データが積み重なるほどに個性が出てきてやがて一意になっていくものが多いのではないかと思います。氏名等が削除されても履歴データ自体に識別性が形成されてしまうことになります。

実在する本人と当該データまたはレコードとの間に1対1の関係性があること、これが個人情報であることの大前提であり、個人情報性を決める原理的なポイントになります。

「医療仮名加工情報」の導入の提言において、厳しい規制案を提案しているのは、「医療仮名加工情報」が個人情報のままだからにほかなりません。匿名加工情報より本人にたどり着くという点でも、データを丸める必要がないので正確性も維持できるという点でも、有用性が高く、またその反面、本人に不利益な影響を与える可能性もまた高いデータだからです。

## リクナビ事件

「リクナビ事件」の概要は次の通りです。採用活動を行うB社(34社のリクナビ契約企業)が学生から集めた情報を、氏名・住所等は削除してCookieやIDにしてA社(リクルート)に渡します。A社がそのCookieで閲覧履歴等を分析して、前年度の内定辞退の実績を学習データとして内定辞退予測スコアリングを行い、その結果を本人のIDに付けてB社に渡します。B社はそもそもIDの氏名・住所をもっていますから、容易に両者のデータを照合することができるわけです。

A社においてCookieは個人情報に該当しないと当初A社は説明していましたが、B社はその内定辞退予測スコアを面前の就活生の評価としてしっかり照合できていたということです。

A社が当初個人情報ではないと言い張ったのは、A社とB社は別事業者であり、両者はそれぞれ独立して個人情報該当性を考えることができるからでした。A社ではCookieと照合し得る就活生の氏名等の情報をもっていないので、A社としては個人情報には該当しないはずだという潜脱的な解釈を行っていたわけです。実際は両者一体となって内定辞退予測スコアを推測しているわけで、本来なら採用活動をしている企業(B社)が当該業務全体の責任を負う管理事業者(Controller)となり、リクルートを委託先の処理事業者(Processor)として構成すべき内容でした。

テクニカルにA社もB社もControllerであると構成したことが問題でした。本来はB社がControllerとしてA社も含めて一体的に個人情報該当性の有無を評価し、その利用目的を特定し就活生に明示すべきでした。

実際は、A社は利用目的Aを、B社は利用目的Bを就活生に明示していましたが、就活生においては、ばらばらに利用目的を見せられても、両者一体となってサイト閲覧履歴等を評価対象とされながら内定辞退率予測スコアリングをする、そのスコアを採用活動のために利用される可能性があるという全貌を理解することはできない構造になっていました。部分的な利用目的を見せられても、サイト閲覧履歴で内定辞退予測をされていることなど本人はわかりようがありません。個人情報保護法に違反するという評価は避けられないところだったというべきです。

(広報委員会 コミュニケーション推進部会 角田 伊久子)