令和２年（ネ）第１３４９号 マイナンバー（個人番号）利用差止等請求控訴事件

控　訴　人　　関口　博　ほか２６名

被　控　訴　人　　国

# 準　備　書　面　（５）

２０２２年(令和４年)８月２４日

東京高等裁判所第１１民事部　御中

控訴人ら代理人　弁護士　水　　永　　誠　　二

同　　瀬　　川　　宏　　貴

同　　出　　口　　か お り

【目　次】

## はじめに

原判決は、基本的に、平成 20 年 3 月 6 日の住基ネット最高裁判決（以下、単に「住基ネット最高裁判決」という。）の判断手法と基準を踏襲して、本件で問題となっている個人番号制度（以下、「マイナンバー制度」ともいう。）の合憲性を判断している。すなわち、①　保障されるべき人権（自由）の中身を設定し、②　そこで問題となる情報の性質や価値について判断し、③　設定された人権(自由)への危険性の有無・程度を判断するという枠組みである。

控訴審における審理により、この判断枠組みに沿った原判決の判断内容は、以下のように、その不十分性が明らかとなった。

①　保障されるべき人権（自由）の中身に関して

ａ）原判決は、憲法 13 条は、個人に関する情報をみだりに「収集若しくは利用され、又は第三者に開示若しくは公表されない自由」を保障するものと解されるとして、「開示」「公表」以外の個人情報の流通場面にまで、その保障を認めた。この点は、情報の取得・収集―保管―利用―開示・提供という情報の流通過程の全てにおいてその保障を認めたものであり、評価できる。

ｂ）しかし、「みだりに」の内容は極めて曖昧であり、また、緩やかな基準で判断されすぎているものであって、不十分である。

②　問題となる情報の性質や価値について

原判決は、「漏えい」の危険性を中心に評価しているため、個々の個人情報が「漏えい」した場合の価値（危険性）を、一つ一つ切り離して判断するという手法をとっている。しかし、これでは、極めて不十分である。すなわち、一つ一つを取りあげるならば、小さな価値しかない情報であっても、それらを名寄せ・突合（データマッチング）して、分析（プロファイリング）することで、新たな・重要な価値が創造されるようになるという、現代的な危険性を念頭において判断しなければならなくなっているからである。そして、そのデータマッチングの鍵である共通番号（マイナンバー）の機能的重要性に注目しなければならないことも明らかとなったのである。

③　情報への危険性の有無・程度を判断する基準等について

②で述べたように、ＡＩ(人工知能)を用いたビッグデータの利活用・分析（プロファイリング）の進展状況など、現代社会の、個人データ保護・プライバシー保護を巡る急激な状況の変化を踏まえるならば、個々の個人情報の価値を、一つ一つ切り離して判断するという手法、特にそれらの情報が「漏えい」した場合の危険性を中心において判断することでは、極めて不十分であることが明らかとなった。また、原判決の「具体的危険」に関する評価の仕方が不十分であることも明らかとなった。

以下、詳述する。

## 第１章　憲法 13 条で保障されるべき権利・自由と合憲性審査基準

### 第１　保障されるべき権利・自由について

#### １　原判決の判示中、評価されるべき点

(1)　原判決は、「憲法 13 条は、国民の私生活上の自由が公権力の行使に対しても保護されるべきことを規定しているものであり、個人の私生活上の自由の一つとして、個人に関する情報をみだりに収集若しくは利用され、又は第三者に開示若しくは公表されない自由を保障するものと解される（最高裁昭和 44 年 12 月 24 日大法廷判決・刑集 23 巻 12 号 1625 頁、最高裁平成 15 年 9 月 12 日第二小法廷判決・民集 57 巻 8 号 973 頁、最高裁平成 20 年 3 月 6 日第一小法廷判決・民集６２巻３号６６５頁等参照)」(56 頁)と判断した。

(2)　上記判示中、「収集若しくは利用され、又は第三者に開示若しくは公表されない自由」とした点は、個人情報（個人データ）流通の全過程における保護の必要性に着目したものであり、開示提供場面の問題だけとはしていない点で、正当である。

#### ２　原判決の判示中、自己情報コントロール権を否定する理由は不当である

(1)　原判決は、「個人に関する情報は、社会通念に照らした秘匿性や私事性の強弱、当該個人に関する情報を保有する目的、個人に関する情報を保有すること

により生ずる利益と弊害、当該個人が主観的に秘匿を求める程度の大小などに照らして、様々な類型のものが存在すると認められる。現状においては、上記のように様々な類型が存在する個人に関する情報のうち、情報主体の同意によるコントロール及び自己決定を行うことを権利として認めるべき情報が何であるかが明確に定まっているとは認めがたい。そうすると、これら個人に関する情報を、一律に情報主体の同意によるコントロール及び自己決定を行う権利を憲法１３条が保障しているとはいい難い」（56 頁）と判断した。

(2)　しかし、第１に、原判決及び平成 20 年の住基ネット最高裁判決が引用する京都府学連事件の最高裁判決も、「個人の私生活上の自由の一つとして、何人も、その承諾なしに、みだりにその容ぼう・姿態・・・を撮影されない自由を有する」と判示しており、本人の「承諾」すなわち「同意」を要件とした「自由」を認めているものである（原審原告準備書面(3)、15 頁参照)。単に「みだりに」という要件を示しただけではない点に注目すべきである。

第２に、後述するように、個人情報(データ)の利用が高度に進められている現代社会において、情報主体の同意によるコントロール（自己決定）を行う権利(自由)を保障しなければ、今やプライバシー保護対応ができない時代状況となっていることを看過してはならない。

第３に、「権利として認めるべき情報が何であるかが明確に定まっているとは認めがたい」という点も理由とならない。

山本龍彦教授は以下のように述べている。

「情報自己決定権なり自己情報コントロール権は、権利の内実についてのコンセンサスが形成されていないので、権利として未成熟と言われる。しかし、渋谷のように考えることは十分可能であり（※引用者注)、いま存在するもの以上のコンセンサスを求めるとすれば、例えば『表現の自由』も権利として存在し得ないことになる。→なぜなら、表現の自由も、その根拠・機能や具体的な保護範囲に関して厳格なコンセンサスが形成されているとは考えにくいからである。→自己情報決定権に関してのみ、学説間の『共通性』

ではなく『差異』に着目するのはフェアではない。」（甲 87・2020 年 6 月 23 日開催「第 4 回情報法制シンポジウム」 3 頁）。

※　渋谷秀樹（立教大学大学院法務研究科教授）

「結局、自己情報の開示・非開示、そして開示する場合はその内容について、相手に応じて自分が決定できることにその核心部分があり、それは自己情報のコントロールという定義の中に吸収できる」

さらに言うならば、個人に関する情報は、いまや個人が有する一種の「財産権」とも評価できるものであり、GDPR の個人データのポータビリティの権利は、そのことを前提としている（山本龍彦教授『AI vs.民主主義』NHK 出版新書 P180～183 など）

第 4 に、国民のプライバシーに関する権利意識も高まっている。個人情報保護法施行後 17 年以上が経過し、国民の個人情報保護・プライバシー保護に関する法意識も高度化し、自己の情報を収集したり、利用したりする場合は、本人の同意を得ることが原則であるとの法意識が定着していると言える。

以上より、現代社会におけるプライバシー権として、「自己情報コントロール権」ないし「自己情報決定権」は認められるべきである。

**３　原判決の「みだりに収集等されない自由」は「残余の自由」しか認めないものであり、憲法解釈として不当である**

仮に「自己情報コントロール権」の権利内容が、未だ不明確な部分が残っており、「権利」「自由」の内実が明確でない部分が残るとしても、そうであればなおさら、「みだりに」の内実を明確にしなければ、憲法解釈として不当である。

玉蟲由樹教授は、その意見書（甲 96・以下、「意見書（甲 96）」という。）において、原判決の「みだりに収集等されない自由」とすることは、「残余の自由」であり、憲法上の人権解釈論においては許容されないと述べている（6～8 頁）。

「憲法上，個人に関する情報を公権力が『みだりに』収集・・・することだけが禁止され，『みだり』なものに至らない収集・・・は許容されていると解する場合，そこでは原則として公権力の側に個人情報の自由な処理権限が承認されてい

ることになる。通常であれば，公権力は個人の情報を当該個人の承諾などを必要とせずに，任意で収集したり，利用したりすることができるが，これが行き過ぎて『みだり』な収集などが行われる場合にのみ，これが違憲ないし違法となるというのが裁判所が前提とする図式であろう。この図式は，例えて言うならば，立法府・行政府に一定の裁量が認められる事項について，裁量権の行使が違法となるのは，それが逸脱・濫用にあたるような場合に限られるとされるのに近い。しかし，このような図式の下で個人に認められるのは，公権力が規制を及ぼさない限りで生じる『残余としての自由』に過ぎないことになる。ここで問題となっているのは，個人の自由とは無関係に，あくまで公権力の権力行使が不当なものであるか否かに過ぎないからである。『みだり』なものに至らない限り個人情報の取扱いが公権力の任意に委ねられているとすれば，そこでは個人の原理的な自由は存在しない。」ことになるからである。

「このような『残余としての自由』は，伝統的に人権保障が憲法によって行われてこなかったイギリスにおいて，公権力の権力不行使の結果として認められてきたものである。すなわち，個人が原理的に自由であるわけではなく，制定法や判例法によって規制されていない限りにおいて市民の自由が認められるとするのがその特徴である。しかし，このような自由理解は，最高法規である憲法によって人権を保障し，あらゆる公権力行為を拘束するものとして人権を理解する日本国憲法上の人権解釈論においては許容されるものではない。むしろ，憲法 13 条のもとでは，人は原理的に自由な存在として承認されており（『個人として尊重』，『生命，自由及び幸福追求に対する国民の権利については，…国政上最大の尊重を必要とする』），人の固有の情報である個人情報についても，原理的に当該個人に処分権限があると解される。」

なお、同教授は、

「もちろん，こうした原則的な処分権限もまったく無制限に保障されているというわけではなく，公権力による正当な目的から生じる必要かつ合理的な制約には服しうる。しかし，だからといって，『みだり』なものでない限り，公権力は自

由に際限なく個人の情報を収集するなどしてよいというわけではない。そうでなければ，これまでの最高裁判例などが，個人情報の収集等に関して，正当な目的や必要性・合理性を満たす手段を要求してきたことの説明がつかない。」と述べている。

### ４　小括

(1)　以上より、現代社会においては、「自己情報コントロール権」ないし「自己情報決定権」が認められるべきである。

(2)　また、少なくとも、原判決の「みだりに収集等されない自由」の内実は、玉蟲教授が述べるように、以下のように、目的、手段の両面から、厳格に限定されなければならない。

「憲法上の権利・自由は，公権力の行使が『みだり』なものである場合にのみ個人の側に認められるものではない。まずは個人に原理的な自由が保障され，それに対する正当な目的や必要性・合理性を満たす手段での介入のみが憲法上正当化されるにとどまる。介入として正当な目的をもたず，あるいは正当な目的を有していても，その手段が必要性・合理性を満たさない場合に，そのような介入が『みだり』なものとなるのである。『個人に関する情報をみだりに収集若しくは利用され、又は第三者に開示若しくは公表されない自由』はそのように解さなければ，憲法上の権利・自由としての意味をなさない。」（7～8 頁）

## 第２　情報の性質・価値について

### １　個々の情報をバラバラに評価する原判決の誤り

(1)　原判決は、「個人番号制度において取り扱われることとなる情報が，原告らの前記の自由に対する具体的な危険を生じさせ得るものであるかどうか，まず検討する」（58 頁）として、「個人番号それ自体」、「氏名等の情報」と、一つ一つの情報をバラバラに評価して、「個人の内面に関わるような秘匿性の高い情報とはいえない」等と評価する。

また、「個人番号制度に基づいて管理や提供が行われることになる個人情報」についても、「いずれも個人番号制度の導入前から行政機関等において収集，利用等が行われていた個人情報であり，個人番号制度によって新たに収集，利用等が行われるようになった個人情報ではないものの，社会福祉に関する事務や納税に関する事務等における個人情報が含まれているものと認められる。これらの個人情報の中には，直ちに個人の内面に関わるような秘匿性の高い情報とまではいえないものの，みだりに第三者に開示されたくないと考えることが一般的であって，取扱方法によっては個人の人格的な権利利益を損なうおそれがある個人に関する情報も含まれていると認めることができる」（58～59 頁）と、それぞれの情報の価値について評価を行う。

(2)　しかし、①原判決は、データマッチングとプロファイリングにより、個々の情報の価値を超えた、新たで重要な、例えば「個人の内面に関わるような」価値すら生じることを看過している。そして、②「いずれも個人番号制度の導入前から行政機関等において収集，利用等が行われていた個人情報であり」としている点は、すでに保有している情報でも、データマッチング、プロファイリングという、新たな「利用方法」により、情報の質が劇的に変化することを看過している（意見書（甲 96）11～12 頁）。

**２　個人番号のインデックス機能の重要性を考えない原判決の誤り**

原判決は、③個人番号（マイナンバー）の価値についても、特定個人に関する、分野を超えて・バラバラに存在する様々な個人情報を、洩れなく・同姓同名の他人の情報と混同することなく・確実にデータマッチング(名寄せ・突合)するにあたって、インデックスとして機能するという、現代社会のデータ利活用における死活的重要性をもつことを看過している。

さらに、そもそも、番号法 2 条 8 項が「個人番号…をその内容に含む個人情報」を「特定個人情報」と定義しているのであって、「個人番号それ自体」を取り出して、そのプライバシー情報該当性のみを論じることには意味がないというべきである（意見書（甲 96）11～12 頁）。

### ３　情報の「漏えい」の危険性を前提に情報の価値を考えている原判決の誤り

しかも、原判決は、情報の「漏えい」の危険性を前提として、「漏えい」した場合の情報の価値を考えている点で不十分である。

原判決が、情報の「漏えい」の危険性を前提としている点は、原判決が、上記判示の前に、以下のように、繰り返し「漏えい」について指摘している点に見て取れる（57～58 頁）。

「現代の高度情報化社会において，個人に関する情報が一度漏えいすると，これがインターネット等を介して無限定に流通する危険性があり，インターネット等を介して流通するに至った当該個人に関する情報を完全に回収したり消去したりすることが事実上不可能であることは公知の事実である。すなわち，現代においては，ひとたび個人に関する情報の漏えいが生ずれば，当該個人の権利や利益が侵害される危険性の除去が困難であり，また，侵害が生じた場合の損害の程度も拡大しやすいということができる。そうすると，個人に関する情報を取り扱う制度においても，収集や利用ができる情報の範囲や情報を取り扱うことができる者の範囲について適切な限定がされていなかったり，情報の開示や公表に関し十分な制御がされていなかったりする場合には，個人に関する情報の漏えいを生ずるおそれがあり，また，漏えいする情報の質及び量の両面で高い危険性を生じさせるから，そのこと自体が個人の権利や利益を侵害するものとなり得る。

したがって，番号利用法及び同法に基づく個人番号制度により前記の自由に対する侵害があるかどうかについては，当該制度において，個人に関する情報をみだりに収集若しくは利用され，又は第三者に開示若しくは公表されることについて，具体的な危険が生じているかどうかの観点から審理判断すべきである。」

確かに、インターネットが極めて高度に発達した現代社会において、情報が「漏えい」した場合の危険性を十二分に踏まえて、その保護策を講じることは必要である。しかし、デーマッチングによるプロファイリングの危険性が問題となっている現代社会では、それだけでは十分ではないのである。

## 第３　データマッチング・プロファイリングの危険性と個人番号制度

### １　データマッチング・プロファイリングされる時代へ突入していること

(1)　控訴理由書の第 1 章、第 3 (22～25 頁)で述べたように、現代社会はＡＩを活用したビッグデータ解析（プロファイリング）の時代に入っている。そのことは、GAFA と呼ばれる民間のデジタルプラットフォーマーがプロファイリングにより圧倒的な地位を築いたため、その規制が全世界的な課題となっている点に端的に表れている。そして、その圧倒的な地位や力は、単に市民の消費生活を支配するだけではなく、市民の投票行動等、民主主義の過程そのものを誘導することさえ可能にしている。既に述べたように、2016 年アメリカ大統領選挙の結果を左右したと言われる、ケンブリッジ・アナリティカ事件にその危険性は端的に表れている。

(2)　このような世界的趨勢の中、日本も「デジタル改革」の名の下、「行政が最大のプラットフォーム」になることを目指して、データ連携とデータ利活用の施策を強力に推し進めている（控訴人ら準備書面（４）、(5) デジタル改革関連法関係、包括的データ戦略関係の主張参照)。

### ２　データマッチング・プロファイリングの鍵となる「共通番号制度」

(1)　このデータマッチングの鍵となる「技術」が「共通番号制度」である。これにより、様々な分野に散在する個人情報(データ)を、容易に、洩れなく・確実に名寄せ・突合（データマッチング）することが可能となるからである。

すなわち、通常、個人情報の名寄せ・突合は、氏名・住所・性別・生年月日の４情報を基になされる。しかし、氏名は、婚姻等を契機に変更される場合があるし、例えば、「斉藤」「斎藤」「齋藤」などと漢字表記が統一されていない場合もある。同姓同名の他人も存在する。住所も、引越のたびに変更される。性別すら変わる可能性がある。このような事情により、４情報によって、個人情報を、洩れなく、かつ、他人と間違うことなく、正確に名寄せ・突合することは事実上不可能であった。ところが、全国民に、漏れなく(悉皆性)・重複しない(唯一無二性)、個人識別番号を付番した場合、その番号と紐づけられた個人情報(デ

ータ)は、「番号」を「検索キー」として、漏れなく、他人の情報と紛れることなく、芋づる式に、正確な名寄せ・突合（データマッチング）をすることが可能となるのである。

(2)　各国において導入されている個人識別番号制度（国民番号制度）は、番号の活用範囲やプライバシー保護の仕組み等に着目して、概ね、①フラットモデル、②セパレートモデル、③セクトラルモデルの３類型に分類される（株式会社国際社会経済研究所「国家情報システム（国民 ID）に関する調査研究報告書」2011年３月 20 頁参照)。

フラットモデルは、各人に割り当てられた一つの個人識別番号を行政機関及び民間の様々な場面で共通して活用する方式であり、アメリカ、スウェーデン、韓国などの国で採用されている。

セパレートモデルは、個人識別番号の利用範囲を限定的に捉え、例えば医療分野と年金分野とで別個の番号を用いる分野別番号の制度である。例えば、ドイツの納税者番号制度はもっぱら税金分野のみに限定されている。

セクトラルモデルは、一つの個人識別番号が共通に用いられるが、各分野毎に異なる「分野別番号」（セキュリティーコード（sector specific Personal Identification Number)）が用いられる方式である。例えば、日本も参考にしたオーストリアでは、出生時に公開される番号たる国民登録番号を暗号処理してID（SourcePIN）を作成するが、この番号は非公開で eID カードのみに格納され、本人以外は知ることはできない。各分野では、この SourcePIN に一定の暗号処理をして得られた「分野別番号」（sector specific Personal Identification Number）という個人識別番号（国民ＩＤ）が生成され、使用される。各分野で共通の個人識別番号を使用するフラットモデルと異なり、①ある分野の担当者が、「分野別番号」を鍵として他の分野の個人情報の名寄せ・突合をすることはできず、また、②仮に情報漏えい事件が発生しても、被害は「分野別番号」に止まるから、同番号を鍵として、他の分野の個人情報を名寄せ・突合することもできないというメリットがある。反面、分野を超えた情報連携については、「分

野別番号」から、データコミッショナー(日本の個人情報保護委員会に相当)を通じてSourcePINを媒介に、他の「分野別番号」を知ることができるから、確実な情報連携ができるというメリットも享受できる。日本は、個人番号制度を作る前に、このような「セクトラルモデル」の仕組みを知っていたにもかかわらず、同様の仕組みは、情報提供ネットワークシステムの中だけの仕組み、すなわち「機関別符号」という一種の「分野別番号」を使って情報連携するという仕組みだけを作った。それ故、後述（第2章第6）するように、各省庁に、税・社会保障・防災分野共通の個人番号(マイナンバー)とひも付けて、各個人情報を保存されたままになっているのである。

(3)　以上述べてきたように、ビッグデータのデータマッチングとプロファイリングの時代に突入している現代社会においては、その危険性を防止するために、各分野共通の個人識別番号（共通番号）を使用することは避けて、分野別番号を用いること、そして、情報連携については、暗号技術を用いて、データマッチングを防止しつつ、厳格な要件と監視機関の監視の下に、確実な連携を行うことができるようにすることが、プライバシーを守りつつ、一定の利便性を追求する場合の、一つの到達点であると言える。

しかしながら、日本においては、個人番号（マイナンバー）と個人番号制度を徹底活用することが、方針として強調されているのである(控訴人ら準備書面(3)　7頁～8頁、本準備書面第2章第6)。また更に、個人番号の利用分野をこの3分野以外にも拡大するという施策を採ろうとしているのである(後述第2章、第6参照)。

### 3　「具体的危険性」の評価方法における原判決の誤り

(1)　原判決は、「番号利用法及び同法に基づく個人番号制度により前記の自由に対する侵害があるかどうかについては，当該制度において，個人に関する情報をみだりに収集若しくは利用され，又は第三者に開示若しくは公表されることについて，具体的な危険が生じているかどうかの観点から審理判断すべきである」（57～58頁）として、「具体的危険」を要件としている。しかも、その具体

的評価の仕方からみるならば、相当高度の・差し迫った「具体的危険」が存することを、差止め等の要件として求めていると考えられる。

(2)　しかし、そのような「具体的危険」の評価の仕方は誤りである。

情報に関するリスク評価おいて、「具体的危険」と「抽象的危険」を分けることができず、全てのリスクを「具体的危険」として評価しなければならないことは、控訴人ら準備書面(1)の第２、「２　原判決及び被控訴人の、情報関係におけるリスク評価の仕方の誤り」において述べたとおりである。

(3)　しかも、最近だけでも、重大な漏洩事故が立て続けに発生している。

例えば、①令和４（2022）年５月 26 日に公表された、岩手県釜石市の市職員２名が、7 年間にわたり、「数万人分」の住民基本台帳に記載された個人情報や約 600 名分の特定個人情報（個人番号付個人データ）などを、業務に関係なく送受信していたり、自宅の個人のパソコンに送信していたりした事件がある。当該職員は、令和３年の業務監査対象から自分の担当業務を外すことも行っていた（甲 121 の 1、2)。なお、市は、「関係省庁と協議を行ったところ、マイナンバーの変更が可能な要件は『マイナンバーが漏洩しただけではなく、不正に用いられるおそれがあると認められるとき』に限られるなどの見解が示され」たことなどから、「関係省庁の助言および見解を踏まえ、データが個人のパソコンから外部に流出した形跡がないこと、現時点において対象となられた方々への直接的な被害などは確認されていないことから、今般の事案がマイナンバーの変更が可能な要件には該当しないと判断し、マイナンバーの変更は行わないことといたしました」と広報している（甲 121 の 3)。

また、②同年６月 21 日には、兵庫県尼崎市において、再々委託業者の社員が、全市民（46 万 517 人分）の住民基本台帳情報や住民税に係る情報等をＵＳＢメモリーに入れたまま持ち出して、泥酔の上紛失してしまうという事件が発生した（甲 122 の 1、2)。

これらの事件は、①事件では、７年もの長期間にわたり不正を発見できなかったことや、マイナンバーの漏洩が確定できないのに「マイナンバーの変更を行わ

ない」という決定を行っていることなどの問題が指摘できるし、②事件では、「再委託原則禁止」原則があるにもかかわらず、それを守れる状況ではないことや、市が再々委託を把握できていなかったこと、実際の業務において、全住民情報が容易に持ち出されていたことなどの問題が指摘できる。同事件でマイナンバーが持ち出されなかったことは、全くの偶然と言わざるを得ず、極めて重大な事故である。

このような重大事故が発生していることに対し、「人為的ミス」であり「具体的危険」はない、と評価することは、リスク評価として完全に誤っているといわなければならない。

### ４「事故前提社会」の考えでリスク対策をとることの必要性

「事故前提社会」の考え方は、情報セキュリティは、事故が起こることは完全に防止することはできないから、事故が起こり得ることを前提として、事故時の対応力をより重視して行こうというものである。

このような考え方は、既に平成 21（2009）年 2 月に政府発表された「第 2 次情報セキュリティ基本計画」において、セキュリティ管理の新たなキーワードとして押し出されている（甲 123)。

この考え方からするならば、後述するように、そもそもマイナンバーのような「共通番号」ではなく分野別番号にするであるとか、結合したり保存したりするデータを「最小化」するといったことを原則化する必要が存する。

## 第４　審査基準

### １　考えられる２つの審査基準

以上述べてきたように、控訴審における主張立証により、原判決の判断は、情報の「漏えい」の危険を中心に考えているものであって、“ビッグデータとＡＩを活用したプロファイリング”が進められている現代社会においては不十分であることが明らかとなった。

したがって、本件で問題となっている個人番号制度の憲法適合性も、原判決よ

りも、より厳格な基準によって判断されなければならないことも明らかである。

**(1) 基準１－目的、手段の必要性・合理性を厳格に審査する基準**

上記第１、4 で述べたように、仮に「みだりに」という基準を採るとしても、その内実は、「個人に原理的な自由が保障され，それに対する正当な目的や必要性・合理性を満たす手段での介入のみが憲法上正当化されるにとどまる」のであって、「介入として正当な目的をもたず，あるいは正当な目的を有していても，その手段が必要性・合理性を満たさない場合に，そのような介入が『みだり』なものとなる」と判断されなければならない。

この点は、特定の目的のために憲法 13 条で保障される重要な・傷つきやすい人権・自由の制約が行われるのであるから、その目的・手段の両面において、厳格な審査を行う必要があるのは当然であることからも、求められる基準であると言わなければならない。

したがって、第 1 にその「目的」の必要性および正当性が、第 2 に、その「手段」の必要性・合理性が厳格に審査されなければならない。

とりわけ、目的達成手段については、取得、利用、保存等の対象となっている情報は、目的達成にとって真に必要な範囲内のものにとどまっているかを問題にすべきであるし、かつ、取得、利用、保存等の対象が個人の重要情報（センシティブ情報や索引情報など）である場合には、目的はそれを正当化できるほどに重要なものといえるか、人権侵害性が最小限のものとなっているか、が検討される必要があるものである（甲 54・玉蟲教授の意見書 13 頁等)。

**(2) 基準２―住基ネット最高裁判決で示された「構造審査基準」**

平成 20 年の住基ネット最高裁判決は、「住基ネットにシステム技術上又は法制度上の不備があり，そのために本人確認情報が法令等の根拠に基づかずに又は正当な行政目的の範囲を逸脱して第三者に開示又は公表される具体的な危険が生じているということもできない」と判示した。

これを受けて、原判決は、「個人番号制度が個人に関する情報をみだりに収集若しくは利用され，又は第三者に開示若しくは公表されない自由に対して具

体的な危険が生じているかどうかは，㋐個人番号制度が，法令又は条例の根拠に基づき正当な目的の範囲内において個人に関する情報を取り扱う制度となっていること，及び，㋑番号利用法が政令等に委任する部分についても前記㋐にいう正当な立法目的の範囲内にあると認められること」に加えて，「㋒個人番号制度に法制度上又はシステム技術上の不備があり，そのために個人に関する情報が法令若しくは条例の根拠に基づかずに又は正当な目的の範囲を逸脱して収集若しくは利用され，又は第三者に開示若しくは公表される具体的な危険が生じていないかどうかについて.それぞれを慎重に審理判断する必要があるというべきである」（59～60 頁）との判断基準を打ち立てている。

しかし、上述したことから、上記㋐㋑の要件は、当然備えるべき必要最小限のものと言わなければならない。そして、㋒は、その当然の必要最小限のものを、「法制度上又はシステム技術上の不備」という形で言い換えているに過ぎない。これらの要件が整っていない場合は、「具体的危険」が存するのは、情報セキュリティ上あまりにも当然である。

この審査基準の具体的内容として、プロファイリングの危険性防止等の不備がないことなどが組み込まれなければならない。

## ２　住基ネット制度と個人番号制度との相違と、より厳格な審査基準の必要性

### (1)　住基ネット制度と個人番号制度の共通性

住基ネット最高裁判決の判断対象である住基ネット制度と、本件の判断対象であるマイマンバー制度は、確かに、両制度ともに、住民票を有する国民と外国人全員に、重複しない、唯一無二の個人識別番号を付する点では同一性を有する。マイナンバー(個人番号)は、住基ネットで付された住民票コードを暗号変換して作られる番号であり、住民票コードと 1 対 1 の対応関係にあるからである。また、両番号は、住民票の記載事項でもある（マイナンバーは住民基本台帳法７条８の２号、住民票コードは同条１３号。）。

### (2)　住基ネット制度と個人番号制度の根本的に異なる点

しかし、両制度（両番号）は、以下のように重要な点で根本的に異なる。

ア　第１に、住民票コードは行政内部でしか利用しない番号であるのに対し、マイナンバーは広く民間でも収集保管された上、官に提供される番号（民・従業員など→民・事業者など→官・税務当局などで利用される番号）である。

両番号制度にこのような根本的な違いが生じるのは、その制度目的が大きく異なることによる。

住基ネット制度は、地方公共団体の共同のシステムとして、住民基本台帳のネットワーク化を図り、本人確認情報を各地方公共団体が共有することにより、全国的に特定の個人情報の確認ができる仕組みを構築し、市町村の区域を越えて住民基本台帳に関する事務処理を行おうとするものであるとされる。それゆえ、住民票コードは、行政内部での利用しか予定されていない。

これに対し、マイナンバー制度は、本来、「税と社会保障の一体改革」の為に、マイナンバーをいわゆる「納税者番号」として利用することにより「より正確な所得の捕捉」をすることを前提に、社会保障や税の給付と負担の公平化を図るとともに、「（所得に応じて）真に必要とする者に、必要な社会保障を給付する」ことを実現するための「社会保障番号」としても利用するものとして創設すると説明されていた(甲 1・『マイナンバー制度の導入趣旨』部分参照)。「納税者番号」としての利用であるから、民間部門で広く使われることが前提となる。すなわち、雇用や報酬支払い等の現場である民間事業者から給与や報酬等の支払いの金額を支払調書に記載して税務当局に提出する際に、「納税者番号」を記載してもらえば、たとえその者が多数箇所からの支払いを受けていても、（今までのように氏名、住所で名寄せするよりも）「番号」を基に、容易・確実に名寄せでき、その合計所得額を捕捉し易い。そして、この合計所得額が、本人からの申告と合致しているかをチェックし易い。よって、所得は正確に捕捉できるようになり、所得申告のゴマカシができにくくなる。このように説明されていたのである。

以上のような目的を実現するためには、すべての事業者等において、その支払先からマイナンバーを収集することが必要とされる。そのため、訴状 7

頁で指摘したように、全国で４百万以上というマイナンバー付きの給与等に関するデータベースが出来上がることになるのである。

イ　第２に、住民票コードはデータマッチングを目的としない番号であるとされるのに対し、マイナンバーはデータマッチングを目的とした番号である。

第１で述べたような方法により捕捉した「正確な所得」を基にして、税を公平に徴収したり、所得の少なさに応じて真に必要としている人に必要な社会保障給付を給付するために、それらの社会保障給付関係の個人情報を正確・確実に整理するための個人識別番号（いわゆる「社会保障番号」）としてもマイナンバーを利用し、税と社会保障という２つの分野の個人情報を正確にデータマッチングすることをも目的として、マイナンバー制度は創設されたとされる。その意味において、マイナンバーはそもそもデータマッチングを目的とした番号なのである。

ウ　第３に、住基ネット制度はデータマッチングのシステムを有しないのに対し、マイナンバー制度はデータマッチングを目的とした情報提供ネットワークシステムを有する。なお、上述したマイナンバー制度の目的からするならば、国税庁が情報提供ネットワークシステムに接続しないことは不思議であるが、国税庁が情報提供ネットワークシステムに接続することは当初から予定されていない。国民等の税情報（所得情報）は、地方自治体が保有する地方税情報を利用することとされているからのようである。

エ　第４に、以上述べた目的の違いから、住基ネット制度では、番号（住民票コード）と紐づけられた個人情報が、本人確認情報（氏名、住所、生年月日、性別及びそれらの変更情報）だけであるのに対し、マイナンバー制度においては、番号（マイナンバー）と紐付けられる情報が、勤務先やそこでの給与額、地方税額、扶養家族、障害の有無・内容、社会保障給付の有無・内容、預貯金額とその預け先金融機関名等、極めて秘匿性の高い情報に及んでいる（なお、将来的には、病名や診療内容が推知できるレセプト情報などとも紐づけられる）である。

オ　第５に、住民票コードは自由に変更できる番号であるのに対し、マイナンバーは原則生涯不変の番号である。

カ　第６に、利用されるＩＣカードの券面に住民票コードは記載されなかったのに対し、マイナンバーカードにおいては、券面(裏面)にマイナンバーが記載される（なお、顔写真の券面への掲載も選択制ではなく、必須とされている)。

(3)　小括

以上指摘した点より、個人番号(マイナンバー)制度は、その取り扱う情報の機微性が高いだけでなく、データマッチングを目的とした制度であることなどから、より人権(憲法で保障された自由)侵害性が高いものである。よって、その合憲性審査基準は、より高度なものとしなければならない。

**３　「デジタル改革」によるデータ利活用とマイナンバー制度の徹底活用が方針化されていることと、より厳格な審査基準の必要性**

(1)　控訴人ら準備書面（3）及び同（4）で「デジタル改革関連法」及び「包括的データ戦略」について述べたように、国は、行政自身が最大のプラットフォームとなり、データの利活用を推し進めてゆくこと、及び、マイナンバー制度の活用を中心的な政策としている。

すなわち、「重点計画」（甲 104）において、

「（３）マイナンバー制度の利活用の推進」を掲げ、【目指す姿】として、「個人の ID・認証基盤であるマイナンバー制度をデジタル社会における社会基盤として利用することにより、行政の効率化、国民の利便性の向上、公平・公正な社会を実現する」としている（甲 104・44 頁)。

また、「（４）マイナンバーカードの普及及び利用の推進」も掲げ、【目指す姿】として、「マイナンバーカードの IC チップには電子証明書などの機能を搭載しており、民間事業者を含め様々なサービスに活用することができる」、「マイナンバーカードの 徹底的な利用を推進する」との方針を掲げている(同・46 頁)。なお、令和４年度末（2023 年３月末）までに、個人番号カード

がほぼ全国民にいきわたることを目指すことを目指して、1．８兆円という膨大な税金を使って、ポイント付与キャンペーンまで行っている。

(2)　小括

個人情報（データ）の利活用が進められ、しかも、ＡＩを利用した、過去の経験からは想像もできないようなデータの利活用が可能となっているという現状や、そのことにより、「ケンブリッジ・アナリティカ事件」などのように、民主主義の基盤自体を掘り崩すことに利用することが可能となっているというということを踏まえて、そのようなデータ利活用の日本におけるインフラとして位置づけられている個人番号制度という観点からも、その合憲性審査基準は厳しくせざるを得ない。

**４　世界水準の高度化と、より厳格な審査基準の必要性―ＧＤＰＲ等における対応状況**

(1)　個人データの利活用は、全世界で進行している事態であり、民間においては、いわゆるＧＡＦＡなどのデジタルプラットフォーマーにおいて先行している。それに対してＥＵなどではＧＤＰＲ（ＥＵ一般データ保護規則）の制定等で対応している。

日本も、ＧＤＰＲの十分性認定を受けているのであるから、ＧＤＰＲと同等の保護水準を確保する必要が存する（控訴人ら準備書面(1)、第１、５参照）。

(2)　ＥＵにおける対応状況と保護基準等は、おおよそ以下の通りである。

**ア　プライバシーと個人データ保護を人権として保障**

ＥＵ基本権憲章８条には、基本権としての「personal data」（日本の個人情報保護法における「個人データ」とは意義が異なる）の保護が規定されており、これを受け、ＧＤＰＲが二次法として規定されている。

ＧＤＰＲ前文１項でも、「personal　date」の取扱いと関連する自然人の保護は、基本的な権利の一つである。ＥＵ基本権憲章８条１項・・・は、全ての者が自己に関する『personal data』の保護の権利を有すると定めている。」と規定している。このことから、ＧＤＰＲが、「personal data」という人権思

想を出発点とするものであることが示されている。「personal data」保護を基本権と位置付けるため、その制限は正当な理由がある場合に限り認められることになる（これは、日本における基本的人権の保障とその制限の正当化の判断手法～法律上の根拠と目的の正当性、手段の必要最小限度性～の考え方と共通するものである）。

ＥＵにおいては、プライバシー権として理解される「私生活尊重の権利」と「個人データ保護の権利」は一般的に区別されており、ＥＵ基本権憲章でもそれぞれ７条と８条という別の条項が設けられている。私生活尊重の権利は、私的事柄への過度な干渉防止の必要性から、そして「personal data」保護の権利は、自らに影響を及ぼす事柄への個人の十分なコントロールを保護する必要性から、それぞれの規定が設けられているとされるが、両者は重なり合う部分もあるとされる（甲 124・宮下紘「ＥＵ一般データ保護規則」23頁）。

**イ　「同意」意義の明確化**

ＧＤＰＲ４条 11 項は、

「(11) データ主体の「同意」とは、自由に与えられ、特定され、事前に説明を受けた上での、不明瞭ではない、データ主体の意思の表示を意味し、それによって、データ主体が、その陳述又は明確な積極的行為により、自身に関連する個人データの取扱いの同意を表明するものを意味する。」と規定する（個人情報保護委員会の仮訳による。ただし、「個人データ」は「personal data」を指す。）。

つまり、「同意」の内容としては、同意が①自由に与えられたもので、②範囲が特定され、③十分な説明を受けた上で、④明瞭であり、⑤積極的行為によって表明されたものでなければならないことになる。

**ウ　プロファイリングの禁止**

ＧＤＰＲ４条４項は、

「(4) 「プロファイリング」とは、自然人と関連する一定の個人的側面を評価

するための、特に、当該自然人の業務遂行能力、経済状態、健康、個人的嗜好、興味関心、信頼性、行動、位置及び移動に関する側面を分析又は予測するための、個人データの利用によって構成される、あらゆる形式の、個人データの自動的な取扱いを意味する。」（同）と定義した上で、

22 条 1 項で、

「1. データ主体は、当該データ主体に関する法的効果を発生させる、又は、当該データ主体に対して同様の重大な影響を及ぼすプロファイリングを含むもっぱら自動化された取扱いに基づいた決定の対象とされない権利を有する。」(同)と「プロファイリングされない権利」を

21 条 1 項で、

「1. データ主体は、自己の特別な状況と関連する根拠に基づき、第 6 条第 1 項(e)又は(f) に基づいて行われる自己と関係する個人データの取扱いに対し、それらの条項に基づくプロファイリングの場合を含め、いつでも、異議を述べる権利を有する。管理者は、データ主体の利益、権利及び自由よりも優先する取扱いについて、又は、訴えの提起及び攻撃防御について、やむをえない正当な根拠があることをその管理者が証明しない限り、以後、その個人データの取扱いをしない。」（同）と、「異議申立権」を保障している。

**エ　プライバシー・バイ・デフォルト（プライバシー・バイ・デザイン）**

GDPR25 条は、以下のように、プライバシーが、データ主体が特別な手続きをしない、初期状態で保障されるような措置（「データの最小化」や「仮名化」など）をとるよう「管理者」に義務づけている。

「1. 技術水準、実装費用、取扱いの性質、範囲、過程及び目的並びに取扱いによって引きおこされる自然人の権利及び自由に対する様々な蓋然性と深刻度のリスクを考慮に入れた上で、管理者は、本規則の要件に適合するものとし、かつ、データ主体の権利を保護するため、取扱いの方法を決定する時点及び取扱いそれ自体の時点の両時点において、データの最小化のようなデータ保護の基本原則を効果的な態様で実装し、その取扱いの中に必要な保

護措置を統合するために設計された、仮名化のような、適切な技術的措置及び組織的措置を実装する。

2. 管理者は、その取扱いの個々の特定の目的のために必要な個人データのみが取扱われることをデフォルトで確保するための適切な技術的措置及び組織的措置を実装する。この義務は、収集される個人データの分量、その取扱いの範囲、その記録保存期間及びアクセス可能性に適用される。とりわけ、そのような措置は、個人データが、その個人の関与なく、不特定の自然人からアクセス可能なものとされないことをデフォルトで確保する。」（同）

**オ　データ保護影響評価（Data protection impact assessment）**

GDPR35 条は、データ影響保護評価（プライバシー・インパクト・アセスメント）について、以下のように規定する。

「1. 取扱いの性質、範囲、過程及び目的を考慮に入れた上で、特に新たな技術を用いるような種類の取扱いが、自然人の権利及び自由に対する高いリスクを発生させるおそれがある場合、管理者は、その取扱いの開始前に、予定している取扱業務の個人データの保護に対する影響についての評価を行わなければならない。類似の高度のリスクを示す一連の類似する取扱業務は、単一の評価の対象とすることができる。

2. 管理者は、データ保護影響評価を行う場合、その指定をしているときは、データ保護オフィサーに対して助言を求めなければならない。

3. 第 1 項に規定するデータ保護影響評価は、とりわけ、以下の場合に求められる：

(a) プロファイリングを含め、自動的な取扱いに基づくものであり、かつ、それに基づく判断が自然人に関して法的効果を発生させ、又は、自然人に対して同様の重大な影響を及ぼす、自然人に関する人格的側面の体系的かつ広範囲な評価の場合；

(b) 第 9 条第 1 項に規定する特別な種類のデータ又は第 10 条に規定する有罪判決及び犯罪行為と関連する個人データの大規模な取扱いの場

合；又は

(c) 公衆がアクセス可能な場所の、システムによる監視が大規模に行われる場合。」(同)

**カ　独立の第三者監督機関**

ＥＵ基本権憲章において、個人データ保護に関する「規則の遵守は、独立の機関による統制に服する」(８条３項) と規定されている。これは、裁判所とは別に、個人データ保護を専門とした独立の機関を設けることにより、基本権としての個人データを保護することを目的としている。

ＧＤＰＲ51 条１項は、

「1. 各加盟国は、取扱いと関連する自然人の基本的な権利及び自由を保護し、かつ、EU 域内における個人データの自由な流れを促進するため、本規則の適用を監視する職責を負う 1 若しくは複数の独立の公的機関を定めなければならない（「監督機関」)」と規定する。

同 52 条は、監督機関の「完全な独立性」について定め、その職員についても、

「5. 各加盟国は、各監督機関が、関係する監督機関のメンバー又はメンバーたちの指示のみに従うその監督機関自身の職員を選任し、かつ、これを雇用することを確保しなければならない。」としている。

同 53 条 2 項は、そのメンバーの資格について定め、

「2. 個々のメンバーは、特に、個人データの保護の領域において、その職務を遂行し、かつ、その権限を行使するために求められる資格、経験及び技能を備えていなければならない。」などと、その独立性の要件やメンバーの資質等について細かく規定している。

**(3)　小括**

以上のように、いまやプライバシー保護、個人データ保護の世界水準は、上記のような具体的諸原則を定めるところまで来ている。

控訴人らがこの間述べてきたように、平成 31 (2019) 年 1 月 23 日に、日本

はＧＤＰＲと同等の水準の個人データ保護を約束し(甲 86)、それに応じてＥＵから「ＧＤＰＲの十分性認定」を受けているのであるから、ＧＤＰＲ並の個人情報保護水準を構築する義務が存する。

また、その点を措くとしても、個人データの高度な利用が進められる現代社会においては、同程度の保護措置がなければ、到底「プライバシー権」ないし「個人の私生活上の自由の一つとして、個人に関する情報をみだりに収集若しくは利用され、又は第三者に開示若しくは公表されない自由」は保障されないものである。

## 第２章　日本の個人番号制度の審査－合理性に欠け、重大な「不備」が存する

### 第１　２つの審査基準から評価した個人番号制度の結論

#### １　きわめて不十分な点や抜け穴の多い制度である

上述した観点、特にＧＤＰＲに示されている現代社会の保護水準を審査基準とするならば、日本の保護水準は、極めて不十分性や抜け穴が多いものであって、憲法で保障された“傷つきやすい“人権（自由）を守るに足りないものである。

すなわち、目的・手段の厳格な合理性審査基準からするならば、個人番号制度は、以下に述べるように、そもそもその目的において合理性を欠いていたり（後述の番号法 19 条 15 号による政令委任の利用目的が、税・社会保障・防災分野以外に広く認められている点など)、手段が合理性を欠いていたり（データ最小化原則に反するなど）するものである。

また、「構造審査基準」からするならば、それらの実態は、重大な「不備」が存すると評価されるものであって、原判決の「個人番号制度に法制度上又はシステム技術上の不備があり，そのために個人に関する情報が法令若しくは条例の根拠に基づかずに又は正当な目的の範囲を逸脱して収集若しくは利用され，又は第三者に開示若しくは公表される具体的な危険が生じている」という基準に従ったとしても、「具体的危険」が存すると言わざるを得ない。

控訴人らは、原審、控訴審を通して、個人番号制度について、数多くの問題点が

存することを指摘してきた。そのすべてについて本準備書面で再度指摘することはできないが、その主なものについて、以下、具体的に指摘する。

## ２　目的の合理性の欠如

(1)　原判決は、「原告らは，各行政機関や地方自治体において，個人番号制度の運用開始後も各種の申請届出等の場面において証明書等の提出を引き続き求めている一方，個人番号制度により生活保護の対象となる住民を発見できた事例は存在しないこと，行政運営の効率化のために多額の費用を支出することは本末転倒であることなどを指摘し，個人番号制度の導入と前記立法目的の実現との関連性を否定する主張をし，これに沿う証拠として原告原田の供述が存在するものの，これは，現時点においては個人番号制度の導入から年月が浅く，その制度が未だ過渡期的状況にあることを示すものといえ，個人番号制度の導入がおよそ行政運営の効率化等の上記立法目的に資さないものであるとは考えられず，前記 1 ないし 3 の目的が正当であることを否定するものとは評価できない」(63 頁)などと判示した。

(2) しかし、①「個人番号制度の導入から年月が浅く」なくなった控訴審段階においても、被控訴人は「行政運営の効率化」について、何ら主張立証できていない。しかも、②例えば、現在行われているマイナンバーカード普及のためのポイント付与事業のために 1．8 兆円もの予算措置が講じられる（有名人を使ったテレビコマーシャル費用や、これまでのポイント付与などを含めれば、優に 2 兆円を超えることになることは明白である）など、「手段の目的化」とも言うべき極めて不合理な施策が続いている。③原判決は、「個人番号制度による経済効果は 1 兆 1500 億円であるとか，3 兆円であるとかという試算(乙 19，　20）もあることからすれば，　これが正当な立法目的となり得ることは明らかである」(62 頁)と判示したが、これは「このような試算が存すること」を示すだけであり、実際にこのような経済効果があったことは全く立証されてもいない。その点を措くとしても、この「経済効果」として挙げられた数字と比較して、2 兆円を超すポイント付与関連予算の異常性は際立っている。④マイナンバーカードと保険証の一体化施策に

ついても、この保険証に対応した医療機関の方が、かえって医療費が高くなるという本末転倒の事態も発生している（控訴人ら準備書面（4）・13 頁）。これに対しては、流石に政府内部からも批判が巻き起こったため、急遽その診療報酬を変更するという事態まで起こっているが、やはり医療費が高くなること自体は変わりが無い（甲 125）。

## ３　手段の合理性の欠如―ＧＤＰＲで示された具体的基準の欠落

### (1)　番号法等では、上述した具体的基準のすべてが欠落している

日本における個人番号制度の実態は、ＥＵのＧＤＰＲで具体的に示された保護基準を措いて評価するならば、以下の通り極めて保護水準が低い。

これは、仮に同制度の目的の合理性が認められたとしても、その手段の合理性がない、もしくは、「重大な不備」が存すると言わざるを得ないものである。

すなわち、まず、上述アで述べた自己情報コントロール権、データ保護権が人権として認められていない。次に、イの「同意」権の保障も、ウの「プロファイリング」されない権利の保障も十分ではない。エの、「プライバシー・バイ・デザイン」はデジタル改革関連法をはじめ、個人情報保護法、番号法にも保障されておらず、オの、それを実現するための手続きである「プライバシー・インパクト・アセスメント」も保障されていない。なお、番号法関係で、「特定個人情報保護評価」は存するが、これはプライバシー・インパクト・アセスメントと評価するには足らない簡単な自己チェックに過ぎない。しかも、個人番号制度自体について、その制度・システムを構築する前に、評価がなされていない点で決定的に要件を欠いている。そして、最後の砦ともいえる、カの独立の第三者機関(個人情報保護委員会)による監視監督も極めて不十分である（この点は、別途後述する）。

なお、ＥＵにおいては、日本の個人番号のような「共通番号制」自体がそもそも損しない。ドイツは厳格な分野別番号制であるし、日本が制度を作る際参考としたオーストリアも、セクトラルモデル（分野別番号を前提として、暗号を用いた情報連携を行うモデル）であり、そもそも日本とは全くそのモデルが

異なる。

### (2) プライバシー・バイ・デザインの理念の欠落

これらの実態は、そもそも特定個人情報に対するリスクを最小化するという理念（プライバシー・バイ・デザインや、その一内容であるデータ最小化原則）も、その理念を実現するための手続き（プライバシー・インパクト・アセスメント）もないことを示している。もちろん、プロファイリング防止の原則も定められていない。

これでは、データの漏えい防止や「プロファイリング」防止等の人権（自由）に対する重大なリスク（「具体的危険性」）を防止することが構造的に担保されていないと言わざるを得ない。

### (3) 原判決が適示する各種「保護措置」の不十分性

ところで、原判決は、縷々制度的、システム的な措置がとられていることをあげている。

しかし、上述したように、それらの措置があることは最低限であり、それらがあることによって安全性が担保されているとは言えない。むしろ、控訴理由書の第２章第６（59 頁以下）で指摘したように、原判決の指摘するシステム的な安全措置は、情報提供ネットワーク内だけのものであって、その他の行政部門や民間部門の安全性は何ら担保されていないなど、おおきな穴のあるものである(それ故、大きな事故も発生しているのである)。

## 第２　刑事事件の捜査における特定個人情報の利用について濫用を防止する制度的保障がないこと

### １　控訴人らの主張

控訴人らは、一貫して、捜査機関によって刑事事件の捜査等の名目で特定個人情報が濫用的に収集、保管、利用されるおそれがあることを主張している。

すなわち、番号法は、「刑事事件の捜査」における特定個人情報の利用に関し、提供（１９条１５号)、収集、保管（２０条）を可能とし、特定個人情報ファイル

の作成制限（２９条）もなく、個人情報保護委員会の監督も及ばない（３６条）としている。さらに、刑事事件の捜査における特定個人情報の提供は情報提供ネットワークシステムを介さないものであるから、情報提供記録の保管の必要はなく、個人が自己の情報提供記録をマイナポータルで確認することもできない（２３条)。

したがって、捜査機関による濫用を防ぐ制度上の担保はなく、警察等の捜査機関は、自己が刑事事件の捜査に必要であると判断すれば、個人番号を利用して特定個人情報の提供を受け、収集保管し、特定個人情報ファイルを作成し、将来にわたって利用することが可能である。

**２　福島意見書（甲 120）に基づく濫用の危険性**

捜査機関による濫用の危険性について、福島至教授の意見書（甲 120）に基づき、具体的に述べる。

従来、「物理的な法益侵害を伴うことなく、人の動静を同時的に監視し、あるいは事後的に追跡する捜査手法」である監視捜査は、任意捜査と位置づけられてきた。しかし、現代情報通信技術の飛躍的発展に伴い、以前とは比べものにならないほどの包括的、網羅的な個人情報の収集ができるようになった（甲 120・2 頁)。

そのため、指紋やＤＮＡ型のような、特定人の同一性確認のために、同人について得た情報を照合する第１類型のほか、特定人の情報を統合、解析することによって、同人についてさらなる知見を得る第２類型、特定人を前提とせず、大量の情報の統合、解析を通じて、捜査対象者を浮かび上がらせる第３類型の監視捜査が可能になっている（同３頁)。

マイナンバーには、税や社会保障に関する情報が紐づけられており、さらにマイナンバーカードには、自治体サービス、ｅ－Ｔａｘなどの電子申請、各種民間のオンライン取引等（オンラインバンキングなど）の情報が紐づけられる（同５頁)。

捜査機関は、マイナンバーに紐づけられる膨大な情報の開示を受けることができれば、相当な程度（個人の宗教的信条や思想等を把握することができる程度）

の監視捜査を実現できる状況にある。マイナンバー情報を用いて行う監視捜査は、上記の第２類型での利用が多いと思われるが物品やサービス等の購入履歴や図書利用履歴のデータベースの利用可能性を考えるならば、第３類型の監視捜査にも利用できる（同６頁）。

マイナンバーに紐付けられる個人情報を捜査機関が取得する監視捜査は、「個人の情報を継続的、網羅的に把握する」ことをかなり可能にすると思われる。従って、情報量が相当量に上る情報取得時点において、この監視捜査は直ちに強制処分と評価されると考えられる。強制処分法定主義に基づき、あらかじめ刑事訴訟法によってその要件や手続を定めておかなければならない。その根拠は憲法３１条のみならず、憲法１３条が保障する情報プライバシー権の保障にある（同10頁）。

捜査機関が情報主体の承諾なくマイナンバーを利用して情報を取得する行為は、現行法の規定は法律による規律としては不十分であり、違憲、違法の疑いが濃い（同10頁）。

**３　刑事訴訟法の規定は濫用を防ぐ担保にならない**

これに対し、被控訴人は、捜査は刑事訴訟法に基づき行われるため捜査機関による濫用のおそれはないと主張するが、刑事訴訟法の規定は濫用を防ぐ担保にならない。刑事訴訟法１８９条２項、１９１条１項は、いずれも捜査機関である警察や検察が、犯罪があると考えれば、捜査をすることを定めているに過ぎず、何ら捜査機関による濫用を規制するものではない。

福島意見書で指摘されているように、監視捜査は任意捜査として実施されるため、令状の審査が及ばず、裁判所の審査が及ぶのは、捜査の結果、公訴が提起され、しかも当該証拠が提出され、さらにその証拠能力が争われるという極めて例外的な場合に過ぎない。また、事件が発生しなくても捜査を行う公安警察活動の場合は、そのような例外的な審査すら行われない。

捜査機関による特定個人情報の利用について、刑事訴訟法の規制が及ぶのは当然であるが、ほとんどの場合、その適否を判断するのは捜査機関自身であり、濫

用を防ぐ制度的保障はない。

住基ネット最高裁判決が本人確認情報の適切な取扱いを監督する第三者機関のあることを合憲の理由としていることに照らせば、番号法上、捜査機関の濫用を防止する制度的担保がないこと自体が制度上重大な不備というべきである。

**４　原判決の判示の誤りについて**

刑事事件の捜査に関する原判決の判示の誤りについては、控訴理由書３６頁以下で述べたとおりである。

すなわち、①原判決が「証拠となり得る書類等に個人番号が記載されていた場合において，当該個人番号の記載された書類等を用いて捜査等ができないことにもなりかねない」という限定された場面での弊害を理由に、刑事捜査の全体に目的の正当性を認めることは誤りであること、②原判決の番号法１９条１４号（現１９条１５号）の解釈（「個人番号を用いることができる場合を限定することと，捜査機関において少なくとも従前と同様の捜査手法を用いた犯罪捜査を行う必要とを調整するための規定」というもの）は、番号法の構造から誤りであること、③原判決には、目的の正当性のみ判断して、正当な目的の範囲内において個人に関する情報を取り扱う制度となっているかという自ら立てた基準について何ら判断をしていないという誤りがあること、という点である。

**５　被控訴人自身、個人番号を利用した特定個人情報の収集等を否定していない**

前記のとおり、原判決は、「証拠となり得る書類等に個人番号が記載されていた場合において，当該個人番号の記載された書類等を用いて捜査等ができないことにもなりかねない」という限定された場面を理由としているが、被控訴人自身は、そのような場面を超えて、広く特定個人情報を収集する場面があることを明言している。

すなわち、被控訴人は、原審において、当初、「刑事事件の捜査は個人番号利用事務ではない（番号利用法９条１項に該当しない）ため，そもそも個人番号の利用ができない」（原審被告第２準備書面２１～２２頁）と主張していたが、主張を変遷させ、次のように主張している。

「番号利用法１９条１４号については,・・・刑事訴訟法等の法令に反しない限りにおいて書類の提供を受け，提供を受けた目的を達成するために必要な限度で個人番号を利用すること（同法９条５項）ができるにすぎない（なお，仮に警察機関が個人番号を入手しても、その入手した目的である刑事事件の捜査に必要な限度を超えて個人番号を利用した名寄せ等を行うことは認められないし，当該個人番号を利用して，情報提供ネットワークシステムを介した特定個人情報の入手ができるわけでもない)。」（原審被告第３準備書面９～１０頁）

上記被控訴人主張の括弧書きから明らかなように、被控訴人の主張は、刑事事件の捜査に必要な範囲であれば、個人番号を利用した名寄せ等を行うことができるというものである。繰り返すが、この場合、「刑事事件の捜査に必要な限度」を超えているか否かを判断するのは捜査機関自身であり、番号法上、捜査機関の濫用を防止する制度的担保はない。

なお、この点に関する被控訴人の主張の変遷については、原審原告ら準備書面（６）で詳述している。

**６　小括**

以上のように、司法審査の及ばない任意捜査や公安警察活動により、特定個人情報が提供（番号法１９条１５号)、収集、保管（同２０条）される場合に、個人情報保護委員会の監督が及ばず（同３６条)、特定個人情報ファイルの作成制限（同２９条）もないことから、捜査機関により刑事事件の捜査等の名目で特定個人情報が濫用的に収集され、特定個人情報ファイルが作成され、将来にわたって利用されるおそれがある。このような番号法の規定は、人権を制約する手段の必要性・合理性を欠き、かつ、制度上の不備があるものであり、憲法１３条に違反するというべきである。

## 第３　番号法１９条１５号１７号が政令等に特定個人情報の利用を委任していることが憲法１３条に違反すること

### １　原判決は、控訴人らの憲法１３条違反の主張について判断をしていない

控訴人らは、番号法１９条１５号及び１７号が政令等に特定個人情報の利用を委任している点について、まず憲法１３条違反を主張し、加えて憲法４１条違反を主張している。

しかしながら、原判決は憲法４１条違反について判断するのみで、憲法１３条違反の主張について何ら判断をしていない。

そこで、以下憲法１３条違反の主張について、改めて述べる。

なお、法改正により番号法旧１９条１４号が１５号に、旧１６号が１７号に改正されたため、以下では新たな条項により主張を行う。

## ２　番号法１９条１５号について

### (1)　番号法の定め

番号法１９条１５号は、同号に列挙した場合に加え、「その他政令で定める公益上の必要があるとき」に特定個人情報の提供を認めている。

そして、番号法施行令２５条は、「法第十九条第十五号の政令で定める公益上の必要があるときは、別表に掲げる場合とする」とし、同施行令別表は１から２４までの場合に提供が認められるとしている。また、番号法９条５項は同法１９条１５号により特定個人情報の提供を受けた者は、個人番号の利用ができるとする。

さらに、番号法３６条は、「第十九条第十五号の政令で定める場合のうち各議院審査等に準ずるものとして政令で定める手続が行われる場合」には個人情報保護委員会の監督は及ばないとしている。

これを受けて、番号法施行令３４条は、同施行令別表１から２４号までの手続のうち、以下の１３の場合には個人情報保護委員会の監督は及ばないとしている。

別表１号（恩赦法による特赦等）

同　２号（独占禁止法の犯則調査）

同　３号（地方自治法による調査）

同　４号（金融商品取引法の犯則調査）

同　６号（検察審査会法による審査）

同　７号（少年法による調査）

同　９号（破壊活動防止法による処分の請求、審査、調査又は書類及び証拠物の閲覧の求め）

同１１号（国際捜査共助等に関する法律による共助又協力）

同１３号（国際的な協力の下に規制薬物に係る不正行為を助長する行為等の防止を図るための麻薬及び向精神薬取締法等の特例等に関する法律による共助）

同１６号（組織犯罪処罰法による共助）

同１７号(無差別大量殺人行為を行った団体の規制に関する法律による調査、検査、処分の請求）

同２１号（犯罪収益移転防止法による届出、通知、提供、閲覧、謄写若しくは写しの送付の求め）

同２２号（国際刑事裁判所に対する協力等に関する法律による証拠の提供、執行協力、管轄刑事事件の捜査に関する措置）

また、１９条１５号における提供は情報提供ネットワークシステムを介さないものであるから、個人が自己の情報提供記録をマイナポータルで確認することもできない（番号法２３条）ことは、刑事事件の捜査で述べたことと同様である。

**(2)　政令への委任は１９条本文の原則の大幅な例外となっていること**

このように、番号法は、政令の委任より極めて広範に特定個人情報の利用を可能としており、現に２４もの利用の例外を認めている。しかも、政令により個人情報保護委員会の監督を排除できるとしており（法３６条)、２４のうち１３の手続で監督が及ばないとされている。

番号法１９条本文が原則として特定個人情報の提供を禁止としながら、実際には、極めて広範に利用が認められているのであり、原則と例外が逆転している。番号法は、このような広範な利用を認めながら行政機関による個人番号の不正利用等を防止する措置を講じておらず、捜査機関や公安調査庁による個人番号の濫用のおそれに対しては、刑事訴訟法や破防法といった法の規制に委ねるのみで、番号法は何らの規定も置いていない。そればかりか番号法１９条１５号による利

用には個人情報保護委員会の監督が及ばないとして、あえて番号法の規制を緩めているのである。

### (3) 小括

このように政令により特定個人情報の広範な利用を可能とする番号法の規定は、人権を制約する手段の必要性・合理性を欠き、かつ、制度上の不備があるというべきである。

また、前記壊活動防止法による処分の調査等（番号法施行令別表９号）・無差別大量殺人行為を行った団体の規制に関する法律による調査等（同１７号）といった公安調査など、政令により個人情報保護委員会の保護が及ばないとされている手続については、刑事事件捜査と同様、もしくはそれ以上に行政機関による濫用の恐れも否定できないのであり、この意味でも人権を制約する手段の必要性・合理性を欠き、かつ、制度上の不備があるものであり、憲法１３条に反し違憲であるというべきである。

## ３　番号法１９条１７号について

### (1)　１９条本文の例外であること

番号法１９条１７号は、「その他これらに準ずるものとして個人情報保護委員会規則で定めるとき」にも特定個人情報の提供が許されるとしている。このような抽象的な規定で特定個人情報の利用の原則禁止の例外を認めることは、番号法１９条１５号と同様、極めて広範な個人番号の利用を可能とするものである。

### (2)　監視機関が提供範囲を定めるという背理

さらに、番号法１９条１７号が問題なのは、「特定個人情報の適正な取扱いを確保」するための監視機関に過ぎない（番号法３４条以下）個人情報保護委員会が、例外的に提供する場合を定めることができるとしている点である。

この点、山本龍彦教授は、「委員会（引用者注：個人情報保護委員会）は、あくまでも法律で定められた範囲どおりに番号制度が運用されていることを担保する監視機関であって，その範囲を決定する機関ではない。委員会は，情報技術に関する豊富な専門知識を有するが，これは技術面にかかわる『立法』(指針等の策定)

を行う正当性を与えるものであっても，情報経路を決定・拡張する『立法』を行う正当性を与えるものではない。したがって，委員会規則のみに基づいてなされる特定個人情報の提供は,形式的根拠を欠くものとして違憲と解すべきであろう」と述べられている（甲 48 の 3・224 頁)。

また、玉蟲教授も、「かかる監視機関が情報提供範囲の拡大について権限をもつということになれば，個人のプライバシーへの介入が行政機関の自律的判断によって可能となることになり，憲法が要求する『法律』による権利の制限（憲法４１条，１３条）という前提を逸脱することになる。」「同条同号（引用者注：番号法旧１９条１６号）により個人情報保護委員会規則を通じて行われる，番号法所定の範囲を越える情報提供行為は目的達成手段としては著しく合理性を欠き，違憲と評価するべきであるし，同条同号そのものが憲法上の要請に反するものとして違憲とされるべきである」と述べられている（甲５４・２０頁)。

**(3) 小括**

このように特定個人情報の広範な利用を可能とする点、及び監視機関である個人情報保護委員会が提供範囲を定めるとしている点で、人権を制約する手段の必要性・合理性を欠き、かつ、制度上の不備があるものであり、憲法１３条に反し違憲であるというべきである。

## 第４　番号法１９条１５号１７号が政令等に特定個人情報の利用を委任していることが憲法４１条に違反すること

この点は、控訴審で提出した準備書面（２）で述べたとおりであり、これを援用する。

## 第５　個人番号カードの電子証明書の発行番号が個人番号と同等の個人識別符号となり、これを利用した情報連携が行われること

この点は、控訴審で提出した準備書面（３）及び（４）で述べたとおりであり、これを引用する。

なお、上記準備書面（３）において、控訴人らは、電子証明書の申請日や民間事業者等の署名検証者がどこであるのかといった利用履歴が、Ｊ－ＬＩＳのデータベースに蓄積されていくのであれば、全住民をプロファイリングするのに可能な情報が国の共管する機関に蓄積されていくことを意味すると主張し、被控訴人に対しＪ－ＬＩＳのシステムについて求釈明を行ったところ、被控訴人は下記の回答を行った（令和４年５月１１日付け被控訴人第２準備書面４頁）。

「機構（引用者注：Ｊ－ＬＩＳ）のデータベースには、後者の方法（引用者注：利用者から提示された電子証明書の発行の番号について、都度機構に対し、失効しているか否かを照会するという方法）により電子証明書の発行の番号について発行の有無に係る照会があった場合にのみ、当該照会が行われたことに関する記録がされるだけであり、利用者が当該電子証明書を用いていかなるサービスを利用したのかといった利用履歴について記録、保存がされることはない。」（下線引用者）

この点、上記被控訴人の回答は、控訴人の上記の主張を否定しているようで、その実、Ｊ－ＬＩＳに「当該照会が行われたことに関する記録がされる」ことを認めているのであり、「当該照会が行われたことに関する記録」が何であるのか明らかにされなければ、上記控訴人らの主張を否定することはできないというべきである。

## 第６　情報提供ネットワークシステムにおける情報連携に個人番号を用いないとしながら個人番号を各行政庁で保管すること

### １　原判決にはこの点について何ら判断をしていない

控訴理由書でも述べたが、原審において、控訴人らは、個人番号制度の中核をなすシステムである情報提供ネットワークシステムにおいて、情報連携に個人番号が使用されず、機関別符号が使用されることから、各省庁に個人番号付きの個人データを保存する必要がないことを繰り返し指摘した。

しかし、原判決はこの主張に対し何ら判断を行っていない。

そこで、この点に関する主張を改めて述べる。

### ２　情報提供ネットワークシステムにおける情報連携には個人番号は使われない

### (1)　情報提供ネットワークシステムとは

番号法１条は、法の目的を①「行政運営の効率化」、②「行政分野におけるより公正な給付と負担の確保」、③「国民」の「利便性の向上」であるとし、その目的の実現を、「個人番号及び法人番号の有する特定の個人及び法人その他の団体を識別する機能を活用し、並びに当該機能によって異なる分野に属する情報を照合してこれらが同一の者に係るものであるかどうかを確認することができるものとして整備された情報システムを運用」することで図るとしている。

情報提供ネットワークシステム（番号法２１条）はこの「情報システム」に該当するものである。同システムで情報連携可能な事務は１８００以上あり、情報連携を行うに際し、情報照会者及び情報提供者は、直接に情報提供の求めを行うのではなく、情報提供ネットワークシステムを介することを原則とする(番号法２１条２項)。このように、情報提供ネットワークシステムはマイナンバー制度の中核をなすシステムであるということができる。

### (2)　情報提供ネットワークシステムにおける情報連携

マイナンバー制度は共通番号であることから、各省庁等のデータベースには、個人情報と共通番号たる個人番号が一緒に保存されている（個人情報と個人番号の紐付け)。

ところが、情報連携の根幹である情報提供ネットワークシステムにおける情報連携には、個人番号は使われず、機関別符号が使われる（乙１・８頁の図)。そして、この機関別符号（情報提供用個人識別符号）の生成には、個人番号は使用されない（番号法施行令２７条５項、原審における２０１６（平成２８）年１１月１５日付け求釈明書参考資料２の１－１、平成２９年1月２４日付け求釈明に対する回答書（２）８頁)。

したがって、情報提供ネットワークシステムにおける情報連携には個人番号は不要ということになる。

## ３　控訴人らの求釈明と被控訴人の回答

そうであるとすると、当然、次の疑問が出て来る。

情報連携に共通番号である個人番号を使わないのであれば、各省庁等のデータベースに個人情報と一緒に個人番号を保存する合理的理由はないのではないか、という疑問である。

この点について控訴人らが求釈明を行ったところ（２０１６（平成２８）年１１月１５日付け求釈明書５～６頁)、被控訴人は下記のとおり回答した（平成２９年１月２４日付け求釈明に対する回答書（２）１４頁)。

「社会保障・税分野において情報提供ネットワークシステムによる情報連携を行うためには、個人を悉皆性（住民票を有する全員に付番）を有する番号によって特定するため各情報提供者のシステム等において個人番号を保有し、情報照会又は情報提供を行うことを可能としておくことが必要である」。

この被控訴人の回答は、「情報連携に必要だから保有するのだ」と言っているに過ぎない。「情報連携に使わないのであれば何故保有するのか」という控訴人らの質問の回答になっていない。

### ４　使われない共通番号という根本的な不備

仮に番号法の目的が正当だとして、その目的達成のために情報連携が必要だとしても、各省庁等のデータベースに個人情報と一緒に個人番号を保存せずに情報連携を行うという、より制限的でない方法（プライバシーにとってより危険性の少ない方法）で目的を達成することができる。

にもかかわらず、特段の理由なく、個人情報と一緒に個人番号を保存するという手段を採ることは、人権を制約する手段の必要性・合理性を欠き、かつ、制度上の不備があるものであり、憲法１３条に反し違憲であるというべきである。

## 第７　プライバシー保護原則がないまま、データ利活用優先で個人番号の利用事務が拡大される点について

### １　我が国における個人番号制度の利用拡大

#### (1)　番号法制定当初の利用目的

我が国における個人番号制度は、平成 25（2013）年の番号法制定当初は、税、

社会保障、災害対策の 3 分野に限定されていた。この 3 分野にしか個人番号を用いてはならず、個人番号を他人に見られてもいけない、とされていた。

裁判所の各手続において、当事者が個人番号が記載された書類を書証等として提出する場合は、個人番号部分をマスキングするよう求められているのも、個人番号を他人に見られてはいけないとされていたからである。番号法制定当初の個人番号制度は、形式上は税・社会保障・災害対策分野に限定したセパレートモデルを採用していたと言える（税・社会保障分野だけでも極めて広範である、刑事事件の捜査などの広範な例外が存するといった批判が存することは別として)。これにより、フラットモデルを採用した米国におけるような、番号流出によってなりすまし被害が多発する弊害や、連邦機関における個人情報を対象としたコンピュータによるデータマッチング処理によるプライバシー侵害の危険もないとされていた。

**(2) 個人番号の利用分野の拡大**

しかし、政府はその後、個人番号を見られても悪用困難だから問題ない、との説明を行うようになり（甲 105 参照)、個人番号の利用分野についても、法改正により、金融分野、医療分野に拡充され、預貯金口座への付番、特定健診・保健指導に関する事務における利用、予防接種に関する事務における接種履歴などに拡大された。

加えて、平成 31（2019）年には、戸籍法の一部を改正する法律により、番号法に基づく情報連携の対象に戸籍に関する情報が追加され、令和 6（2024）年 3 月以降、戸籍情報と個人番号との情報連携が可能になるとされている。

さらに、令和 3（2021）年 1 月 25 日、政府は、新型コロナワクチンの接種状況を把握するためとして、個人番号と紐付けたシステムの構築に乗り出すと公表し、同年 4 月中旬頃からワクチン接種記録システム（ＶＲＳ：Vaccination Record System）の運用を開始した。ＶＲＳの危険性については、控訴人ら準備書面(3)で述べたとおりである。

令和 3（2021）年 5 月 19 日に公布されたデジタル改革関連法では、①医師免

許等の国家資格に関する事務への個人番号の利用、②公金受取口座を個人番号とともに登録する制度の創設、③預金口座への個人番号の付番等が定められた。

**(3) デジタル社会における社会基盤とされた個人番号**

令和４（2022）年６月７日に政府が閣議決定した「デジタル社会の実現に向けた重点計画」は、個人番号（マイナンバー）制度を個人のＩＤ・認証基盤と位置付け、個人番号制度をデジタル社会における社会基盤として利用することにより、「行政の効率化、国民の利便性の向上、公平・公正な社会を実現する」ことを目指すとして、「マイナンバーの利用の拡大を図るとともに、継続的な発展に向けて、マイナンバーカードによる認証を利用した行政サービスを民間が後押しするための仕掛け、つまりはライフイベントにおいて、行政サービスと民間事業者のビジネスの恩恵を、国民一人ひとりが官民システムの連携を通じて享受できる社会の実現を目指す」（甲１２６、６頁）としている。

ついに政府は、個人番号制度について、社会保障・税・災害の３分野に限定するとの方針を転換した。

「国民にとって利便性を感じてもらうこと」を第一に考えるべき（同 60 頁）との方針のもと、「令和４年（2022 年）から、デジタル庁を中心に、これらに関係する行政手続等の横串での精査を行い、上記の各制度を所管する関係府省庁においてマイナンバーの利用や情報連携を前提とした個々の制度等の業務の見直しを行いつつ、マイナンバー法の規定の在り方と併せて、マイナンバーの利活用の推進に向けた制度面の見直しを実施する。」（同頁）、

「従来のマイナンバー利用事務からの拡大を図り、利用者のアクセシビリティを確保しつつ、デジタル完結を図る。」（同頁）、

「その上で、国民の理解を得つつ、令和５年（2023 年）にマイナンバー法改正を含む必要な法案提出など法令の整備を実施し、令和６年（2024 年）以降にシステム等の整備を行い、令和７年度（2025 年度）までに新たな制度を施行することを目指す。」（同頁）

として、令和７（2025）年度までに、この３分野以外の手続にも個人番号を利用

できるようにすることを目指している。

### (4) 個人番号制度の在り方についての重大な方針転換

以上のように、当初、形式上とはいえセパレートモデルを採用していた個人番号制度は、国家施策としてのデジタル改革関連法の一つであるデジタル社会形成基本法３７条１項等に根拠を有する閣議決定「デジタル社会の実現に向けた重点計画」(2022 年６月７日)（甲１２６）により、利用分野を限定することなく、個人のＩＤ・認証基盤と位置付け、個人番号制度をデジタル社会における社会基盤として利用するというフラットモデルに向かうことを明らかにした。

今後、更に広範な分野で共通番号（統一番号）化した場合、個人番号をキーとして名寄せすれば、あらゆる個人情報が、漏れなく・確実に名寄せ・突合（データマッチング）できることになり、このことが悪用されると容易にプロファイリングできるようになる。米国における社会保障番号（ＳＳＮ）のように、幅広い行政分野及び民間分野で広く利用されることになった結果、ＳＳＮを用いた不正な名寄せや、名寄せされた個人情報の販売が行われ、社会問題となることが確実である。

不正な名寄せや名寄せされた個人情報の売買は、漏えいした情報をもとになされるが、すでに日本でも個人情報の漏えい・紛失事故は、上場企業とその子会社 120 社が 2021 年に公表した分に限っても、事故件数 137 件、漏えいした個人情報 574 万 9773 人分に達している。平成 20 (2012) 年から令和 3 (2021) 年までの累計事故件数は 925 件、漏えい・紛失した可能性のある個人情報は累計 1 億 1979 万人分と、ほぼ日本の人口に匹敵するという（甲１２７)。

個人番号の利用拡大により名寄せできる個人情報が増えると、個人のプライバシーや人格権を侵害するおそれが非常に高くなる。

## ２　電子証明書機能の利用拡大によるプライバシー侵害のおそれ

### (1) 電子証明書機能部分の利用に法規制がないこと

個人番号カードの電子証明書機能は、民間事業者でも利用可能なものであるが、電子証明書の利用を規制する条項は番号法になく、公的個人認証法６３条１項が

規定するのみであることは、控訴人ら準備書面(3)で述べた通りである。

政府は、個人番号カードの「利便性を高める」として、医療分野に限らず、個人番号カードの電子証明書機能の多目的利用を推進している。しかし、この多目的利用により、電子証明書の発行番号やマイキーＩＤ等の各種ＩＤと、様々な個人情報とがひも付けられることになる。発行番号や各種ＩＤは個人番号と同様に個人を確実に識別する機能を有するのであるから、個人番号と同様の「共通番号制」の危険性を有することになる。しかも、これらの発行番号やＩＤには、番号法による個人番号の利用制限のような法的規制は存しないから、その危険性は更に高い。

**(2) 国による電子証明書機能の利用拡大**

このように、個人番号カードの電子証明書機能についての法整備はなされていない状況であるにもかかわらず、国は、個人番号カードの電子証明書機能を利用して健康保険証として利用できるとするとともに、「生まれてから学校、職場など生涯にわたる個人の健康等情報を、マイナポータル等を用いて電子記録として本人や家族が正確に把握するための仕組み」としてＰＨＲ（personal health record）に取り組んでいる（「経済財政運営と改革の基本方針 2020～危機の克服、そして新しい未来へ～」16 頁脚注 32（令和 2（2020）年 7 月 17 日））。

厚生労働省のデータヘルス改革推進本部は、令和 3（2021）年 6 月 4 日「データヘルス改革に関する工程表」（甲１２８）を策定した。

この工程表の「自身の保健医療情報を閲覧できる仕組みの整備」の項目においては、健診・検診情報（乳幼児健診・妊婦健診、特定健診、事業主健診、自治体健診、学校検診、予防接種等）、レセプト・処方箋情報（薬剤情報、電子処方箋情報、医療機関名等、手術・透析情報等、医学管理等情報）、医療的ケア児等の医療情報、電子カルテ・介護情報等（検査結果情報・アレルギー情報、告知済傷病名、画像情報、介護情報）について、既にマイナポータルで閲覧可能なものに加え、今後閲覧が可能となる時期等が記載されている。

**(3) 最も機微性の高い個人情報の塊であるＰＨＲ**

ＰＨＲは、生まれてからの生涯にわたる健康・医療情報等が集められる仕組みであり、前記「データヘルス改革に関する工程表」では、集められる情報は、検診情報やレセプト・処方箋情報にとどまらず、電子カルテ等やゲノム解析結果までもが予定されている。それらの情報は、最も機微性が高いものであり、むやみな収集・結合自体がプライバシー侵害となり得る。万が一、情報が漏えいしたときの被害は甚大なものとなり、取り返しが付かない事態を招来する。

ＰＨＲは、一生涯にわたる情報の蓄積を前提としており、長年の情報の蓄積によって、個人の健康状態の全体像が分かってしまう極めて機微な個人情報の塊である。

国民のすべてが、自身の健康・医療情報等のデータが蓄積されていくことを、必ずしも積極的に認識するとも限らない。さらに、遺伝的素因が原因となる疾病においては、当該個人のみならず、その家族にも関わる情報であるといえるから、当該個人の同意のみによって情報が蓄積されてしまうと、家族等の情報コントロールが及ばない危険性もある。遺伝情報をはじめ、医療情報が企業により積極的に利活用されると、本来加入できたはずの保険契約から排除されるなどの不利益を生じるおそれが強い。

**(4)　遺伝情報・ゲノム情報に基づく差別禁止規定すらない我が国の法制度**

このように、極めて機微性の高い情報を蓄積していく制度を構築しようとしているにもかかわらず、法律面において、個人情報保護法による一般的な規制を除けば、遺伝情報に基づく差別等を具体的に禁止する法令がない。

令和４（2022）年４月６日、日本医学会及び日本医師会は、「我が国の社会環境の整備としては、個人情報の取得や第三者提供に本人同意の取得を求めるという個人情報保護法による対応のみに留まっており、不当な差別や社会的不利益の防止については、法律あるいは自主ルールのいずれの形でも定められていません。我が国では、国民皆保険の制度が整備され、公的健康保険の加入に際して、遺伝情報・ゲノム情報の提示を求められることはありません。しかし、いわゆるがん保険や死亡保険等の、民間保険の引受・支払実務における遺伝情報・ゲノム情報

の取り扱いに関するルールは不明瞭な状況にあり、業界の自主規制の検討状況を待っている状況にあります。」との共同声明を出して、警鐘を鳴らしている（甲１２９）。

医療に関する個人情報は、極めて高度のプライバシー情報であり、情報主体（患者）による自己情報のコントロールや情報の第三者利用についても一般的な個人情報とは格別の考慮を必要とするものであり、医療情報に関する個人情報保護の個別法を制定するしかない。ところが、政府は、次世代医療基盤法を制定したり、デジタル田園健康特区（仮称）を指定し、健康医療情報の自治体を超えたデータ連携を推進し、ＰＨＲを介して一元管理を図る医療版情報銀行制度を構築する構想など、医療情報の利活用を図る法整備等には積極的であるにもかかわらず、プライバシー保護についての検討はほとんどなされていない。

現在の法制度の下で、個人番号カードの電子証明書部分を利用したＰＨＲを推進することは、国民の自己情報コントロール権及びプライバシー権を明らかに侵害するものであって、違憲というべきである。

### ３　プロファイリング禁止規定の欠如

(1)　GDPR（General Data Protection Regulation: 一般データ保護規則）では、プロファイリングを「自然人と関連する一定の個人的側面を評価するための、特に当該自然人の業務遂行能力、経済状態、健康、個人的嗜好、興味関心、信頼性、行動、位置および移動に関する側面を分析または予測するための、個人データの利用により構成されるあらゆる形式の個人データの自動的な取扱い」と定義した上で（4 条 4 号）、異議申立権（21 条）、自動的処理のみによる意思決定に服さない権利（22 条）等を定めて一定の法的規律を行っている。しかし、我が国の個人情報保護法制には、プロファイリングについて定義した規定もなければ、これを直接的に規制する規定もない。

(2)　このような規制の存しない状況のまま、個人番号の利用拡大や個人番号カードの電子証明書機能の利用拡大により、個人データの収集範囲を拡大し、蓄積することになると、日本における最大のプラットフォーマーたる行政機関は、マイナ

ンバーや各種ＩＤに紐付けられた本人確認情報（氏名、住所等）、税・社会保障関係情報、医療関係情報、そしてデジタル改革関連法によって収集が拡大する個人情報を用いることで、民間を遙かに上回る精度で個人のプロファイリングをすることが技術的に可能となる（個人番号カードに関しては、政府は、近い将来において健康保険証との一体化を実現する方針であるから、国民皆保険のもと、国民は、その取得・所持が強制されることになる）。行政機関によるプロファイリングが禁止されないまま、行政機関が収集する個人情報が拡大の一途を辿り、情報が結合され、さらに進んで分析（プロファイリング）されてしまうと、プライバシー権や人格権に対する侵害は、単なる情報結合を超えた重大なものとなる。

デジタル改革関連法は、個人情報の結合制限やプロファイリングの禁止について何ら規定を設けていない点において、プライバシー権等を侵害するおそれが著しいものとして違憲の疑いが高いものといわなければならない。

## 第８　個人番号制度の監視監督機関である個人情報保護委員会の不十分性

### １　第三者機関が必要な理由

これまで述べてきたように、極めて急速に、日々発達してゆく情報化社会において、巨大なデジタルプラットフォーマーに対して、一個人が自己のプライバシーや個人データを守るための実効的な行動を取ることは、事実上困難である。国等の行政機関における膨大な自己の特定個人情報の処理（個人番号と結びついた各種ＩＤとひも付けられた個人情報の処理を含む）について、個人でチェックをした上で危険防止を求めることも、同様に困難となっている。そもそも、どのような特定個人情報が収集・保存されているのかが開示されていないような分野も存する。

特に、今後、行政が最大のプラットフォームになることが国の目標とされる「デジタル改革」が、国家の中心施策として推し進められていくならば、一層その困難性が増す。

このような状況の下にあって、個々人に代わって、個人データ保護、プライバ

シー保護のために、独立して、専門的能力のある第三者機関が活動することが必要となり、それが日本においては個人情報保護委員会である。

**２　住基ネット最高裁判決が合憲とした理由**

住基ネット最高裁判決も「第三者機関」の存在を、具体的危険が無いことの大きな理由にしている。

第４、３で述べたように、住基ネットシステムと個人番号システムの違いに鑑みるならば、さらにこの点は重要なポイントとなるし、第三者機関が十分に機能しない状況であれば、手段の合理性がない、ないし、重大な「不備」が存する（具体的危険性がある）と言わなければならない。

**３　第三者機関が備えるべき機能・要件等を欠いていること**

公正取引委員会の事務総局定員 （平成 30 年度末）は 834 人、会計検査院の事務総局職員数（平成 30 年１月現在定員）は 1244 人、国税担当の職員数が５万 6000 人である（甲 50)。これに比して、 個人情報保護委員会の定員は、令和２年度末 139 名から、令和３年度末 148 名（令和４年度末 195 名）と極めて少ない。

確かに、同委員会が、少ない人数にもかかわらず、一定の活動を行っていることは認められる。しかし、同委員会の極めて広大で重大な任務に比して、その人員は少なすぎると言わざるを得ない。「デジタル改革関連法」で、今後飛躍的に拡大された任務に比して、そもそも人員が少なすぎるし、その他にも、権限にも極めて重大な「不備」があるといわなければならない。

以下、その主な点を指摘する。

**(1)　委員会の任務に個人情報の利活用推進も含まれていること**

個人情報保護法 128 条は、個人情報保護委員会の任務として、以下のように定めて、個人情報の利活用に配慮することもその任務に含めている。

「委員会は、行政機関等の事務及び事業の適正かつ円滑な運営を図り、並びに個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の個人情報の

有用性に配慮しつつ、個人の権利利益を保護するため、個人情報の適正な取扱いの確保を図ること（個人番号利用事務等実施者（行政手続における特定の個人を識別するための番号の利用等に関する法律（平成二十五年法律第二十七号。以下「番号利用法」という。）第十二条に規定する個人番号利用事務等実施者をいう。）に対する指導及び助言その他の措置を講ずることを含む。）を任務とする。」

また、番号法 19 条 17 号は、「その他これらに準ずるものとして個人情報保護委員会規則で定めるとき」と定めて、個人情報保護委員会に、特定個人情報提供禁止の例外を定める権限も与えている。

① ＧＤＰＲにおいては、独立した監督機関の設置が義務づけられているところ、「取扱いと関連する自然人の基本的な権利及び自由を保障し」（GDPR51 条）と，明確にプライバシー保護のための第三者機関として機能が純化されている。日本の個人情報保護委員会は、基本権（人権）の保護を監督機関の目的としている GDPR と異なるといわなければならない。

② また、ＧＤＰＲで設置される機関には、個人データの利用範囲の拡大権限は一切存在しない（51 条～59 条、甲 83・宮下紘著「ＥＵ一般データ保護規則」（勁草書房））。ちなみに、1995 年に制定されたＥＵデータ保護指令においても、この構造は全く同様であったから、ＥＵでは、このようなデータ保護機関の役割の純化は 20 年以上の伝統を有する。

以上より、日本の個人情報保護委員会は、その任務が個人情報保護に純化されていないと言える。これは、たとえて言えば、原子力規制委員会の任務に、「原子力利用の有用性に配慮しつつ」その職務を行えと規定するに等しく、その意味で大きな「不備」が存する。この点は、(2) で述べるように、その委員の選任にも影響している。

**(2) 委員会の監督権限が及んでいない重要な分野が存すること**

個人情報保護委員会の監督権限が及んでいない重要な分野、例えば番号法 19 条 1 項 15 号の「刑事事件の捜査」分野があることは、前述したとおりである

（甲１３０・宮下紘「デジタル政策とプライバシー保護」・107 頁参照)。

人権侵害が想定される最たる分野である「刑事事件の捜査」に権限が及んでいない点は、極めて大きな不備であり、この一点だけでも違憲性があると言わざるを得ない。

**(3) 個人情報保護を専門とする常勤委員が存しないこと**

個人情報保護委員会は、委員長及び委員８人（常勤４名、非常勤４名）で構成される（個人情報保護法 131 条第１項)。

委員長及び委員には、①個人情報の保護及び適正かつ効果的な活用に関する学識経験のある者、②消費者の保護に関して十分な知識と経験を有する者、③情報処理技術に関する学識経験のある者、④行政分野に関する学識経験のある者、⑤民間企業の実務に関して十分な知識と経験を有する者並びに⑥連合組織・・・の推薦する者が含まれるものとされている（同法 131 条第４項)。」

しかし、プライバシー保護が専門である常勤委員が不存在という重大な「不備」が存する。プライバシー法の専門家であった堀部政男初代委員長の退任後、現在８人の委員のうち３人（うち、常勤委員は２人）が「民間企業の実務に関して十分な知識と経験を有する者」となっているとともに、専門委員５人のうち４人が「民間企業の実務に精通している者」が選任されている。前述第４、４(2)カで述べたＧＤＰＲの基準に照らすならば、委員会の役割から見て、著しく均衡を失した構成である。

これは、①「個人情報の保護及び適正かつ効果的な活用に関する学識経験のある者」という専門性の選出枠組みが不備であることに関係する。委員会の目的は、まず何よりも「個人情報保護」なのであるから、「個人情報の保護」に関する学識経験のある者という枠から常勤の委員を、複数選ぶ必要があるというべきである。

この「不備」に関しては、例えば、令和３年７月に、ＪＲ東日本が鉄道セキュリティ向上の取組みとして、個人情報保護委員会と相談の上、顔認識カメラを用いて不審者等の検知を行うことを公表した事件に端的にその結果が表れ

ていると言わなければならない。公表後の報道により、この顔認識カメラが駅や列車内で犯罪を犯して、刑務所に服役後の出所者等も対象としていたことが分かり、世論の批判を受けて、ＪＲ東は、出所者等を検知の対象から外したのである。

個人情報保護委員会は、相談を受けたにもかかわらず、このような個人情報の利活用等を規制しなかったのである（甲１３０・109 頁）。

なお、個人情報保護委員会の事務局員についても、

「ＥＵからの関心事でもあるが、特に日本の公的部門の監視にあたり事務局職員の他省庁からの出向は、そもそも出向元の省庁等が監視対象となりうることから、利益相反と見なされかねない点に留意が必要である」（甲１３０・108 頁）

**(4) 膨大な任務に比して委員会のマンパワーが不足していること**

控訴人ら準備書面（3）、第 2、5（26 頁以下）等で指摘してきた通り、個人情報保護委員会は、その監督・監視対象が、民間、国の行政機関、地方公共団体と大きく拡大してきており、その内容も極めて高度で専門的なものになった。個人情報保護委員会の責任範囲は格段に拡大し、監督すべき業務量は想像を絶する程増大している。

一方、上述したように、個人情報保護委員会の任務は、「行政機関等の事務及び事業の適正かつ円滑な運営を図り、並びに個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の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ため、個人情報の適正な取扱いの確保を図ること（個人番号利用事務等実施者に対する指導及び助言その他の措置を講ずることを含む。）を任務とする。」（個人情報保護法 131 条）と規定されており、本来的任務である「個人情報の保護」以外に、「個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の個人情報の有用性に配慮」することまでもが任務に含まれる。

そして、所掌事務として「個人情報の保護及び適正かつ効果的な活用についての広報及び啓発に関すること」（同法 132 条 6 号）が規定されている。

このため、個人情報保護委員会が本来果たすべき個人情報の保護についての取り組みが弱体化することは必然と言わなければならない。

同委員会の定員は、上述のように若干増加されているが、その総務や会計等の業務に携わる職員を除いた「実働部隊」の人員も、多種多様な業務のうち、個人情報保護や特定個人情報保護に当たる人員の数も明らかとされていない。

また、被控訴人は、「委員会が所掌事務を適切に行っていること」を立証するとして乙 60 の 1～5 を提出するが、これらは、委員会が存在し、一定の活動をしていることの立証にしかならない。上述したように、現代社会においては、個々人が自己の特定個人情報を含む個人情報の利用状況を適切に監視し、守ってゆくことは事実上不可能な状況にあるのであるから、委員会が適切な監視・監督を行っていることが証明されない限り、控訴人らの特定個人情報の安全性は担保されていないと言わざるを得ない。

また、証拠提出されていない部分も含めて「年次報告書」の全体を読むと、報告書上、実に多種多様で数多くの活動を行っていることが記載されている。

しかし、わずか 100 名強程度と考えられる人員でこれだけの活動を「十全に」行っていると考えることも、経験則上困難である。

さらに、監視・監督が一定水準で行われていると言うためには、会計検査院のように委員会が定期的に、少なくとも一定数の、実地「監査」活動を行うことが必要であると思われるところ、そのような活動を行っていることはうかがえない。実地「監査」を行わなければ、上述した事故のような「再々委託」の危険性や実際の現場の運営の杜撰さ（規定違反等）は発見することは困難である。人員不足から、各機関の自主チェック（それ自体もコピーアンドペーストが多いのではないかといわれている）結果の報告だけで済ませざるを得ないのが日本の現状である。

例えば、ドイツのデータ保護機関においては、秘密裏に行われている監視や

テロ対策データベースに対してすら、監視権限が及ぶ上に、これらは個人による監視ができないので、連邦データ保護コミッショナーによって、2年に1回のチェックが義務づけられている（日弁連2017年人権擁護大会第2分科会基調報告書資料編409頁参照)。

このような定期的な「監査」活動がなければ、事前の防止も兆候の把握も困難であり、安全性の担保ができていないと評価せざるを得ない。

## 第９　結語

以上述べてきたように、控訴審における主張立証により、原判決の不十分性は明らかとなった。被控訴人は、控訴人らの指摘する点に「木で鼻を括った」ような対応をするのではなく、日本の「デジタル政策」を持続的かつ健全に発展させるためにも、現代社会において憲法13条で保障された国民のプライバシーや自由を守り発展させるためにも、真摯に対応すべきである。

上述したように、すでに一定規模の「事故」は発生している。今後、大きな事故が発生しないうちに、また、引き返すことのできない利用状況まで至らない今のうちに、個人番号の利用を停止して、抜本的な見直しを行う必要があることを、控訴人らは求めるものである。

以上