

平成27年(ワ)第11996号,平成28年(ワ)第2023号,平成28年(ワ)第2895号 個人番号利用差止等請求事件

原告 平野かおる ほか144名

被告 国

準備書面14

2019(令和元)年7月11日

大阪地方裁判所第24民事部合議2へ係 御中

原告ら訴訟代理人弁護士 大江 洋 一



同 辰 巳 創 史



第1 はじめに

本準備書面では、証拠提出した玉蟲由樹教授の意見書(甲30号証)を踏まえた、原告らの憲法上の主張である。したがって、本準備書面中の括弧内に記載された頁数は、すべて同意見書の頁数である。

第2 本準備書面の構成

本準備書面の構成(第3～第6)は以下のとおりである。

まず、第3では、本件で問題となるプライバシー権の中核が自己情報コントロール権であり、その本質は、すでに、判例においても実質的に認められていることについて明らかにする。

第4では、個人番号制度が生み出すプライバシー権侵害の特質を明らかにし、「機能的アプローチ」の重要性を指摘するとともに、被侵害法益の重大性を論じる。

第5では、国が本件においてプライバシー権等の制約理由としている目的の「重

要度が軽すぎる」(22頁)ことを明らかにする。したがって、番号法の違憲性はこの時点ですでに明らかとなる。

第6では、制約手段の相当性判断基準について、番号法に基づく個人情報処理プロセスの特質及び住基ネット判決(最判平成20・3・6)の先例性を踏まえながら論じるとともに、個人番号制度の濫用防止策を欠いているために明らかに違憲といわざるをえない条文が認められること、及び、個人番号の漏洩を防ぐことは現行制度の仕組上、不可能であることを明らかにする。

第3 プライバシー権の本質とその法的根拠

1 プライバシー権の人権性

個人のプライバシーは、憲法によって直接に保護される対象である。すなわち、個人のプライバシー保護は、憲法13条前段が定める「個人の尊重」理念の要請であり、したがって、プライバシー権は、憲法13条後段の幸福追求権の一環として保障される主観的権利(憲法上の人権)である。

この点については、いまや、日本の憲法学において、「広い見解の一致がある」(2頁)。

2 プライバシー権の中核としての自己情報コントロール権

プライバシー保護にとって中核的な意味合いをもつ権利は、「自分の私的な情報について、それをいつ、いかなる範囲で他者に対して明らかにするのかを自分自身で決定するという個人情報に関する自己決定権」であり、これが自己情報コントロール権と呼ばれる権利である(2頁)。

自己情報コントロール権は、その権利の本質からして、公権力による個人情報の取得にはじまり、その保存・蓄積、利用、さらには第三者への譲渡(提供)へと進行しうる情報処理のプロセス全体について、情報主体によるコントロールを認めることを内容とする人権であり、各段階は、プライバシー保護との関係でそれぞれ異なった意味合いをもちうるため、段階ごとに分離された理解を必要とする(3頁)。

3 裁判例が認めてきたプライバシー権

以上で述べたことについては、日本の憲法学において広い見解の一致があるだけでなく、最高裁判例を含む多くの裁判例も認めている(3頁～5頁)。

まず、「宴のあと」事件東京地裁判決(東京地判昭和39・9・28)は、「私事をみだりに公開されない」という私法上の人格権の一つとして理解されるもの

ではあるが、「個人の尊厳」の保護を根拠に「幸福の追求」の一環としてプライバシー権を承認している。

最高裁も、その後、京都府学連事件（最大判昭和44・12・24）では人の容ぼう・姿態情報の要保護性を、京都市前科照会事件（最判昭和56・4・14）では、前科および犯罪経歴情報の要保護性を、指紋押なつ拒否事件（最判平成7・12・15）では「みだりに指紋の押なつを強制されない自由」をそれぞれ認めている。また、先述した住基ネット訴訟においても、憲法13条が保障する「個人の私生活上の自由の一つとして、何人も、個人に関する情報をみだりに第三者に開示又は公表されない自由を有する」ことが確認されている。

これらの保障を個人情報の処理プロセスとの関係でみると、京都府学連事件および指紋押なつ拒否事件で問題となっていたのは個人情報の「取得」段階での問題であり、京都市前科照会事件や住基ネット事件で問題となったのは「利用」や「開示」の段階である。

すなわち、最高裁は、「自己情報コントロール権」という名称自体は使用していないが、これらの判決を通じて、公権力による個人情報の取得にはじまり、その保存・蓄積、利用、さらには第三者への譲渡（提供）へと進行しうる情報処理のプロセス全体に対する情報主体によるコントロール、つまり、自己情報コントロール権の本質的な内容につき、すでに実質的に、すべて認めているのである。したがって、自己情報コントロール権の人権性は、日本の憲法学のみならず、もはや裁判所においても広く共有されているといえる（5頁）。

4 自己情報コントロール権の端的な人権性が認められるべきである

以上のように、自己情報コントロール権の本質的な内容は、日本の憲法学だけではなく最高裁判所判例も認めている。また、以下で詳論するように、自己情報コントロール権の内実は、現代高度情報化社会において個人が尊重され、人間の尊厳が擁護されるために保障されるべき極めて重要な国民の権利利益である。そうであるなら、国民の自己情報コントロール権が端的に憲法上の人権として保障されていることは明確にされるべきである。したがって、裁判所は、単なる私法上の人格権の一つとしてではなく、自己情報コントロール権が憲法上保障される人権であることを、判決において、端的に正面から認めるべきである。

第4 番号法が生み出すプライバシー侵害の重大性

1 プライバシー権保障の趣旨

すでに述べたように、日本の憲法学においてすでに「広い見解の一致」をみているプライバシー権は、憲法の基本的人権尊重主義の根本理念である、個人の尊重及び人間の尊厳保障の要請として認められる人権である。玉蟲教授の言葉をお借りすれば、「自己情報コントロール権の主張は、決して一部の、何かしら「やましい」ところをもつ人々の、一般には受け入れがたい「わがままな」主張などではない。この主張は、人間の尊厳や個人の尊重、さらには民主的共同体の維持といった、重要かつ実質的な憲法価値との関連において理解されねばならないものである。」(11頁)

「個人の尊重」の趣旨は、公益や公の秩序と対立するわがままや私益の保障ではない。周知のとおり、個人の尊重概念は「人格的生存」と言い換えられることも多い。また、ドイツの人間の尊厳概念も、その源は、あのコペルニクスの転回を提唱し、実践理性を重視した哲学者のカントである。これらのことからわかることは、これらの理念の共通項あるいは中核が、個人の主体性（自己実現）と自己立法（自己統治）の価値であるということである。

人は、社会的存在として、国家の法に従う義務があるが、だからといって、私的領域における自己実現と自己統治がすべて否定されるべき存在ではない。人は、国家の道具や客体にされるために生まれてきたのではない。どんな人間も、個人として、自分らしい人生を主体的に生きるための権利が認められなければならない。そして、そのためには、国家の法が不可侵な私的領域、国家に干渉されずに自己決定することが可能な内的親密領域が強く保障されねばならない。これが、プライバシー権及び自己情報コントロール権保障の一般的根拠である。

では、本件個人番号制度は、具体的に、どのようなプライバシー侵害を惹起し、個人の尊重や人間の尊厳を侵害する危険があるのだろうか。

2 番号法が生み出すプライバシー侵害

(1) もはや重要でない情報はない

個人番号制度は、現代の高度に発達した情報処理技術を前提にすることによってはじめて成立する制度である。したがって、個人番号制度が生み出すプライバシー侵害を論じるにあたっては、以下に述べる、現代の高度情報処理技術下におけるプライバシー情報の変質を無視してはならない。

この点、従前であれば、プライバシー権保護に関して問題となる情報は、

特定の時間や場所における断片的なものがほとんどであった。だからこそ、プライバシー情報としての要保護性の判定にあたって、情報の内容、重要性、機微性等を問題にすることには合理性が認められた。

しかし、本来はそれほど個人の人格に深くかかわらない諸データであっても、それらが大量に集積され、結合されると、個人の人格をより詳細に、あるいは全体的に把握することのできるきわめて要保護性の高い情報へと質が変化するという個人情報の機能が看過されてはならない。現代の高度に発達した電子的情報処理技術の下では、個人に関する情報は技術的にみれば、ほぼ無限定に集積・結合できるのである。すると、現代では、個人情報が備えるこのような機能によってこそ、個人の人格が「ガラス張り」にされてしまう可能性が生じるのである。

以上のことを考慮すれば、個人番号制度のように、現代の高度情報処理技術を前提とした制度下におけるプライバシー保護を実践するにあたっては、情報処理過程にのせられる個人情報の「内容」に着目して保護のあり方を決めるという、これまで学説・判例において中心的に採用されてきたアプローチはもはやとるべきではない（6頁）。

たとえば、江沢民講演会事件最高裁判決（最判平成15・9・12）での「学籍番号、氏名、住所及び電話番号は、…個人識別等を行うための単純な情報であって、その限りにおいては、秘匿されるべき必要性が必ずしも高いものではない」という説示がその典型例である。しかし、先述した個人情報の機能を思い出すなら、たとえ「個人識別等を行うための単純な情報」にすぎないものであっても、それが特定の講演会出席という事実と結合されれば、個人の思想や人格プロフィールに関する重要情報へと質が変化することが理解されるであろう。

したがって、現代の電子的情報処理技術の下においては、プライバシーの保護の観点で重要ではない情報は存在しないことを前提とすべきであり、これまで重要ではないとされてきた情報に対する保護のあり方を以下に述べる機能的なアプローチによって補完することが肝要である（7頁）。

（2）機能的アプローチ

先述した個人情報の「機能」に着目すれば、とりわけ個人識別性・特定性の高い情報については、内容面での重要情報と同程度の保護が行われる必要がある（7頁）。

この点については、2006年のいわゆる「ラスター捜査決定」におけるドイツ連邦憲法裁判所の見解が参考になる（7頁～8頁）。同決定は、「情報自己決定権への介入の強度は、いかなる内容が介入によって把握されるのか、とくに当該情報がそれ自体や他の情報との結合においてどの程度の人格関連性を示し、いかなる方法によってこれらの内容が獲得されるのかに、とりわけ左右される」との一般論を述べている。注目すべき部分は、もちろん、獲得される個人情報の内容と並んで、「とくに」との言葉を添えて当該情報の他の情報との結合可能性が重視されている点である。すなわち、ドイツ連邦憲法裁判所はもはや情報の内容よりも、その機能に重点を置いた議論を展開しているのである。

以上より、情報テクノロジーの発達した現代社会の現実に鑑みれば、プライバシー保護を貫徹するためには、その情報がもちうる機能に着目した保障のあり方を模索しなければならない。個人識別性・特定性の高い情報はその機能の高さから、内容面での重要情報に匹敵する重要性をもつ情報である。したがって、他の情報との結合可能性が著しく高い、というよりも、他の情報を集積・結合することにその主たる目的がある情報——索引情報やインデックス情報——が問題となっていればいるほど、かかる情報の処理については、とりわけ強い憲法上の保護が及ぶと解すべきなのである（7頁～8頁）。

（3）索引情報またはインデックス情報としての個人番号

（2）で述べた結論は、実は、判例もすでに認めている。

たとえば指紋情報、DNA型情報、生体認証情報、SNS等のIDやパスワード、クレジットカードのカード番号といったものは、単体で見れば、「指先の紋様」や単なる数字やアルファベットの羅列にすぎず、「それ自体では個人の私生活や人格、思想、信条、良心等個人の内心に関する情報となるものではない」

（指紋押なつ拒否事件最高裁判決）。しかし、同判決は、これらは個人識別性・特定性の高さから「利用方法次第では個人の私生活あるいはプライバシーが侵害される危険性がある」情報であるとも指摘したのである（7頁）。

その場合の利用方法こそが、先述した個人識別性・特定性の高い情報の機能性の高さに着目した利用方法のことであり、具体的には、それらの個人識別性・特定性の高い情報を検索キーとして、ここに個人にかかわる様々な情報を結合させるという方法である。このようにして利用される個人識別性・

特定性の高い情報は、「索引情報」や「インデックス情報」と呼ばれる（7頁）。

単体としては意味のない数字の羅列である個人番号がこのような情報の典型であることはいうまでもない。個人番号は、索引情報あるいは検索キーとして用いられることで、個人の私生活あるいはプライバシーを侵害する大きな危険性を生み出すのである。

したがって、個人番号制度が生み出すプライバシー権及び自己情報コントロール権侵害は、現在の高度に発達した電子的情報処理技術の下で、個人番号が分野横断的なデータマッチングのための検索キーとなることを前提に、検討されなければならない。すると、同制度が生み出す最大の人権侵害は、国家による包括的人格プロフィールの構築可能性であることが明らかになる。

（5頁）

（4）包括的な人格プロフィールの構築可能性

電子的情報処理技術の進展は、個人情報処理に関し、プラス効果だけではなく、「多くのマイナス面」ももたらした。それは「とくに個人にかかわるデータとの関連で、データの物質化によるデータ交換の簡便化、データの利用範囲の予測不能な拡大、データの相互関連づけによる質的に新たなデータが創出される可能性（たとえば、個人の包括的な人格プロフィールの構築）あるいは逆に全体的な関連づけから切り離され、断片化されたデータによって本来の人格とは異なる誤った人格像が形成される可能性といった、人格ないしは個人性の侵害の危険性」である。「情報テクノロジーの発展は、情報やデータの取り扱いによる人格ないしは個人性の侵害の可能性をも増大させた」

（5頁）のである。

すなわち、現代の高度に発展した電子的情報処理技術に基づく個人番号制度とは、個人番号を検索キーとして、その個人に関する大量の情報を瞬時に関連づけることにより、個人の包括的な人格プロフィールの構築することが可能なシステムなのである。

現代の電子的情報処理技術の下では、個人に関する情報は技術的にみれば、ほぼ無限定に集積・結合できるのであり、このことによって個人の人格すら「ガラス張り」のものとなる可能性がある。住基ネット訴訟における金沢地判平成17・5・30はこれを「住民個々人が行政機関の前で丸裸にされるが如き状態」と表現している（6頁）。

（5）個人番号制度の人権侵害性の内実

包括的な人格プロフィールの構築可能性は、それだけで憲法上のプライバシー保護の要請に反する（8頁）。個人番号の利用範囲が拡大されれば、個人番号が検索キーとなって検索可能な個人情報がますます集積される。現代国家は、福祉国家・社会国家実現のために、これらのデータをますます必要とするようになる。こうして、包括的な人格プロフィールの構築可能性もますます高まることとなる。

ここで注意すべきは、このような包括的な人格プロフィールが実際に構築されなくとも、現代の高度に発達した電子的情報処理技術下においては、「構築可能性」が存在すれば、それだけで憲法上のプライバシー権侵害であるという点である。

現代の高度に発達した電子的情報処理技術の下で、いったんデジタルデータ化され、ネットワークのなかに取り込まれた個人情報は、玉蟲教授の言葉をお借りすれば、「ネットワークの内外で際限なく、劣化もなしに容易にコピーされ、世界的規模で一瞬にして拡散されうる。しかも、これらのデータは、いつまでも消えずに残り、また情報主体の思わぬところで情報同士が結びつけられ、利用される危険性さえも秘めている。」（3頁）のである。したがって、「プライバシーの侵害という、個人が秘匿したいと考える私的な事項が公にされてしまうことを想定しがちであるが、むしろ現代社会でのデータ処理の現実を考えるならば、個人情報が暴露されるという「実害」が生じていなくとも、個人の知らないところで個人情報がやり取りされ、上記のような「危険」を恒常的に生じているというその「状況」こそがプライバシー侵害的であると考えられる必要がある。それゆえ、情報処理技術の進展は、必然的に個人のプライバシー保護のために自己情報の処理を自らの意思にもとづいてコントロールすることの重要性を高める結果となる」（3頁）のである。

たしかに、現在の国や企業等が、包括的な人格プロフィールを作成する可能性は高いとまではいえないかもしれない。しかし、だからといって個人番号制度に人権侵害性がないとはまったくいえないのである。なぜなら、そのような包括的な人格プロフィールが作成されてしまっただけからでは、それらの情報は「ネットワークの内外で際限なく、劣化もなしに容易にコピーされ、世界的規模で一瞬にして拡散され」、「いつまでも消えずに残り、また情報主体の思わぬところで情報同士が結びつけられ、利用される」ことになってしまい、もはやプライバシー侵害による被害の回復は手遅れになるからである。

したがって、個人番号制度が、時の政府や企業が包括的な人格プロフィールを作成するために利用しようと思えばできるような制度であること自体が、自己情報コントロール権としてのプライバシー権の侵害なのである。

以上より、国が個人番号制度の合憲性を主張立証したいなら、単に、現時点において、包括的な人格プロフィール作成の目的や危険がないという事実だけではなく、将来のどんな政府も、あるいは将来の法改正によっても、同制度が包括的な人格プロフィール作成のために利用される可能性がない制度であるということ、すなわち、包括的人格プロフィールの構築可能性自体が存在しないということを主張立証すべきなのである。しかし、個人番号を検索キーとしたデータマッチングが行われることが前提である現行の個人番号制度において、そのような立証は不可能であろう。

3 個人番号制度がもたらす害悪

(1) 人間の尊厳あるいは個人の尊重の侵害

では、こうした包括的な人格プロフィールの構築可能性は、個人にどのような害悪をもたらすのであろうか。

この問題に関し、ドイツの連邦憲法裁判所は1969年のマイクロセンサス決定において、「国家が人間を強制的にその全人格において記録し、カタログ化する権利そのものを要求できる場合には、…このことは人間の尊厳と調和しない」と述べている（9頁）。すなわち、ドイツ基本法における「至上の価値」とされる「人間の尊厳」が害されるのである。国家に対し、国民の全人格の強制的な記録とカタログ化を認めることは、国民に対し、個人としての私的生活の存在意義を認めないことに等しく（9頁）、個人の内的な親密領域における自己実現及び自己統治を否定することであるから、まさに、人間の尊厳侵害あるいは個人の尊重の侵害であらう。

また、これは自己情報コントロール権侵害でもある。なぜなら、国家による全人格のカタログ化は、個人にとっては、「私が何であるか」を、自分ではなく、国家の都合によって決められることを意味するからである。「自らの人格やそれにまつわる情報についての主体的な決定権限を失えば、人はその範囲において公権力の行為の単なる客体にすぎなくなってしまう。」（10頁）それは、人間を国家の道具や客体として扱うことであり、明らかな人間の主体性侵害であるから、このような自己情報コントロール権侵害も、究極においては、個人の尊

重あるいは人間の尊厳の侵害である。

ドイツでは、その後、1983年の国勢調査判決において、個人には「いつ、いかなる限度で個人的な生活状況が明らかにされるのかを原則として自己で決定する」権限があることを明言した。これは、「情報自己決定権」と呼ばれ、現代および将来の自動的データ処理の諸条件の下では、「特別に保護を要する」とされた。その理由は、「自己の社会的状況に関する一定範囲の個人情報をも十分な確実性をもって見通すことができない者、コミュニケーションの相手方となりうる者の情報量をある程度も評価することができない者は、自己決定によって計画し、決定する自由を本質的に制限されている。自己について誰が、何を、いつ、いかなる機会に知るのかを市民がもはや知りえないような社会秩序やこれを可能ならしめる法秩序は情報自己決定権と合致するものではない」という点にある（10頁）。

（2）民主政の侵害

以上のことから、本件で問題とされるプライバシーの侵害は、個人の自己実現、自己統治、主体性及び情報自己決定権という、いずれも人格的生存の核心の侵害であり、究極において、憲法の人権尊重主義の根本理念である個人の尊重及び人間の尊厳の侵害であることが明らかになった。

すると、ここで忘れてはならないことは、上記のような利益が侵害されてしまうと、民主政の過程にも瑕疵が生じ、民主政が機能不全に陥ってしまうという点である。前掲のドイツ国勢調査判決も、「このことは、個人のそれぞれの発展の機会を妨げるだけでなく、公共の福祉をも害する。なぜなら、自己決定は、市民の行動および協働能力に基づく自由で民主的な共同体の基本的な機能条件であるからである」（10頁）と指摘しており、玉蟲教授も「個人の自律が民主的な共同体の形成にとっても不可欠の前提である」（11頁等）と述べられている。

民主主義が健全に機能するためには、自由かつ主体的に自己決定できる市民の存在が前提である。個人の主体性や自己決定権を奪うプライバシー侵害は、したがって、民主主義をも機能不全にしてしまう。

4 結論

以上より、番号法が生み出すプライバシー侵害の被侵害利益は極めて重大であることが明らかになった。とすれば、そのような重大な人権の制約が許され

る場合とは、きわめて高度に重要な目的が認められる場合でなければならず、仮に目的に正当性が認められる場合であっても、手段の相当性が厳しく審査されるべきであり、具体的には、「より制限的でない他の選ぶうる手段」がある場合には、それによるべきなのである。

第5 制約目的の重要度が「軽すぎる」

番号法1条では、情報提供ネットワークシステムを用いることで、①効率的な情報の管理及び利用、②行政機関内部での迅速な情報の授受、③行政運営の効率化、④公正な給付と負担の確保、⑤手続の簡素化による国民負担の軽減、⑥本人確認等における利便性の向上といった目的を実現することが想定されている。このうち、①～④は主として行政機関にとっての利益であり、⑤・⑥が国民にとっての利益と解される（17～18頁）。

まず、⑤・⑥のような本人利益を根拠として公権力による個人のプライバシーへの介入を正当化することは本末転倒である（18頁）。何が本人の利益であるかの決定は、まさに、本人の自己決定権に委ねられるべきものであり、国が自らの価値観によって勝手にそれを決め、個人に押しつけてよいものではないからである。したがって、国民の利益は、個人のプライバシーへの介入を正当化する目的とすることはできない。

ところで、「公共の福祉」とは、人権尊重主義を重視する立場によれば、一般に、他者人権との衝突の調整原理と解されている（内在的制約説）。つまり、憲法上認められている他の人権保障との調整が目的である場合にのみ、目的の正当性は肯定されるのである。

この観点からすれば、①～③については、ほとんど純粋に行政機関の便宜のみを追求するものであり、国民の利益につながる側面があるといっても、極めて間接的なものにすぎないといわざるをえないから、重大な人権であるプライバシー権、自己情報コントロール権、情報自己決定権の制約を正当化する目的とは到底認められない。

唯一、④に示されるように、これらの目的が追求するのが積極的な社会経済政策の実現であるとするならば、玉蟲教授も、「いささか間接的ではあるが、目的の正当性自体は承認しうる余地がある」と述べられている。「公正な給付と負担の確保」自体は、たしかに、現代社会における重要な人権にかかわる政策課題であることは否定できないからである（18頁）。

しかし、以上のような表現からしても、あくまでも、政府が上記目的と個人番号制度との関連性を具体的に立証できた場合に、「かろうじて」という意味である。

たとえば、法案段階から言われていたことであるが、現行の個人番号制度によっては国民の在外資産を把握することはできないし、生活保護の把握率を上昇させるといったような、公正な給付目的が促進されているわけでもない。したがって、④は、仮に国が、④が掲げる目的と現行の個人番号制度の関連性について具体的に立証した場合に限り、かろうじて正当性が認められる余地があるにすぎないのである。

だからこそ、玉蟲教授も、「(本当に「公正な給付と負担の確保」につながるのか)は、国による十分な論証を必要とする事柄であり、さらにそれを踏まえた立法事実の厳密な検証も含めて議論の余地があろう。」(18頁)と述べられており、結論的には、「番号法が掲げる目的は、いずれも強度なプライバシー介入行為である個人番号を用いたデータマッチングを正当化できるほどに重要なものとはいいがたい。憲法上のプライバシー保護の重要性や、番号法にもとづいて行われるプライバシーへの介入の重大性に対して、掲げられた目的の重要度が軽すぎるのである。」(22頁)と述べられている。

原告らの主張も、まさに同様であることを、ここで強調しておきたい。すなわち、番号法の違憲性はこの時点ですでに明らかなのである。個人番号制度の目的は、極めて重要な人権である自己情報コントロール権を制限するための目的としては、「重要度があまりに軽すぎる」のであり、その違憲性は、このことだけで、まったく明白なのである。したがって、番号法は、先述したように、被告である国が、④が掲げる目的と現行の個人番号制度の関連性について具体的に立証しない限り、本来、第7で論じる制約手段の相当性等を検討するまでもなく、番号法は違憲なのである。

第6 制約手段の相当性判断基準

1 はじめに

以上で述べたように、原告らとしては、個人番号制度の目的の重要性が、プライバシー権、自己情報コントロール権、ひいては個人の尊重、人間の尊厳の制約目的としてはあまりに軽すぎる点で、同制度が違憲であることはすでに明白であると考えるが、以下では、万一目的の正当性が肯定された場合に備え、

念のため、制約手段の相当性判断基準についても論じる。

2 番号法に基づく個人情報処理プロセスの特質

すでに述べたように、自己情報コントロール権に係る個人情報の処理プロセスは、公権力による個人情報の取得、その保存・蓄積、利用、さらには第三者への譲渡（提供）へと進行し、各段階は分離された理解を必要とする。しかし、番号法に基づく個人情報の処理プロセスには以下に述べるような特質が認められ、それが制約手段の相当性の判断基準にも影響する。

番号法によると、個人番号は、地方公共団体情報システム機構によって生成され、市町村長によって個人に対して指定される。したがって、個人番号は、指紋情報やDNA型情報のように個人にもともと備わる固有情報ではない。個人の固有情報ならば、公権力が知るためにはその「取得」という段階を踏む必要がある。すると、この段階で、自己情報コントロール権は、情報の内容的・機能的重要性に応じて一定のハードルを設けることとなる。しかし、個人番号の場合は、公権力が一方的に生成・指定するものであるがゆえに、最初から公権力側に帰属しており、「取得」の段階がないのである。すると、個人番号は、索引情報やインデックス情報になり得るきわめて重要な個人識別情報でありながら、国はそれを、何らのハードルを超えることなく、事実上の取得を完了できてしまうことになるのである。したがって、これは、「公権力によって一方的に付番された番号によって管理されたくない」という個人の要求をまったく無視する制度であり、個人の尊重及び幸福追求権の観点からは違憲の余地が十分に認められる（15頁）。

ともあれ、個人番号については国による情報の取得段階のハードルが存在しないのであるから、利用・保存の段階での違憲審査は一層厳しいものが要請されてしかるべきということになる。これが番号法の個人番号制度に認められる特有の問題である（15頁）。

3 個人番号の利用・保存段階の問題点

公権力による情報取得が適法に行われれば、その後の利用・保存等も自動的に適法になるわけではない。とりわけ、個人番号の利用等については、先述のとおり、その取得段階における国に対するハードルがないわけであるから、利用等がそれ自体で憲法上正当化されうるものかどうかは厳しく審査されなけれ

ばならない。

個人番号の利用に関して、番号法はその目的規定である1条において「個人番号…の有する特定の個人…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」することを予定している。つまり、番号法は、個人番号を検索キーとした、異なる分野に属する個人情報のデータマッチングが行われることを正面から肯定しているのである。データマッチングが行われるということが個人番号の利用に関する最も特徴的な点であるとともに、プライバシー保護の観点からも重要なポイントである。

データマッチングが個人のプライバシーおよび自己情報コントロール権に対する強度の介介入行為であることは疑いがない。個人番号を検索キーとして異なる分野に属する個人情報が集積・結合されることは、おのずと個人の人格プロフィールへの到達可能性を高めるからである。また、データマッチングの範囲・規模がそこまで大きなものでない場合であっても、情報主体が予測不可能なかたちで個人情報が集積・結合されるような場合には自己情報コントロール権侵害を構成しうる。

行政機関の各分野においてそれぞれ個別に、異なった目的から取得・保存されていた個人情報が情報提供ネットワークシステムを通じて分野横断的にデータマッチングされるというのは、これまでの我が国の行政実務では行われてこなかった新たな形態でのプライバシーへの介介入行為である(16頁)。

ここで忘れてはならないのは、住基ネット訴訟最高裁判決(最判平成20・3・6)である。同判決は、データマッチングによりプライバシー情報が「本人の予期しないときに予期しない範囲で行政機関に保有され、利用される具体的な危険が生じている」とした控訴審判決を破棄し、データマッチングの具体的な危険は存在していないとの理由を挙げつつ、住基ネットは「自己のプライバシーに関わる情報の取扱いについて自己決定する権利ないし利益」を違法に侵害するものではないと判示したのであった。

この判示は、どんなデータマッチングであっても、プライバシー保護の観点から問題がないというものではない。少なくとも住基ネットにおいては住民票コードと氏名・生年月日・性別・住所のいわゆる「4情報」の結合を超えるデータマッチングの具体的な危険が排除されていることを示したにとどまる(17頁)。かかる範囲を超えるデータマッチングが現実に行われる場合に、どのような評価をなすべきかについては何ら示されていない。

番号法が正面から認めているデータマッチングとは、住基ネット事件において具体的危険がないとされていたデータマッチングとは、明らかに、比較にならないくらいに強度なプライバシーへの介入である。国が、個人識別性の高い個人番号を、何のハードルもなく取得し、それが検索キーや索引情報となり、さまざまな個人情報が結合されることになるからである。しかも、番号法においては、個々のデータマッチングや情報提供には本人同意が原則不要とされている。本人同意なしに行政機関の判断のみによって個人情報が集積・結合されるということは、個人にとっては強制的な処分と何ら変わるところがない（17頁）。

したがって、すでに述べた比例原則（je-desto 原則）に従うなら、これほどの強度な介入が正当化されるためには、きわめて「高度な目的」が設定される必要があることになる。しかし、それが存在しないことについては、すでに述べたとおりである。

4 番号法 19 条 14 号・16 号は明確に違憲である

すでに述べたように、個人番号はデータマッチングの際の検索キーとして機能する索引情報である。すると、いかに番号法上の制度設計上では分散管理方式が採用されていたとしても、個人番号がいつでもさまざまな個人情報を集積・結合できる情報であることは否定できない。すると、個人番号はセンシティブ情報に匹敵する重要情報であり、濫用の危険性やサイバー攻撃その他の手段による漏洩の危険性に対する予防措置が十分に定められている必要がある。

以上の観点からすれば、番号法 19 条 14 号・16 号は明確に違憲である。

番号法 19 条 14 号は「刑事事件の捜査」のための情報提供を許容しているが、ここには本質的に濫用ないし過剰な情報収集の危険性が存在している。捜査の端緒となる嫌疑の程度や犯罪の軽重などを一切問わずに、捜査機関が個人番号に紐づけられた膨大な量の個人情報の提供を受けうるとすれば、それは明らかに過剰なプライバシーへの介入行為となろう。しかも、同条同号にもとづいて行われる捜査機関への情報提供については、同法 36 条により、個人情報保護委員会の権限が及ばないこととされており、濫用防止の措置がまったく不十分である。たとえ、刑事訴訟法および刑事訴訟規則によって捜査機関に各種の義務が定められているといっても、番号法上は際限なく個人情報を収集可能である点で、捜査機関による秘密裡での重要個人情報の収集・利用を結果的に承認す

るものとしてプライバシー保護の要請に反する。同条同号にもとづく刑事事件の捜査のための情報提供は、提供される個人情報の範囲が限定できず、包括的な人格プロフィールが開示される可能性が否定できないため、個人番号を濫用するものであり、必要性・合理性を満たさず明確に違憲である（24頁）。

同様のことは、番号法19条14号が「その他政令で定める公益上の必要があるとき」にも情報提供を認める点にもいえる。これについては、番号法施行令26条および別表がその範囲を定めているが、その範囲は行政機関が如何様にも拡大できるものである。「公益上の必要」は文言として不明確であるため、行政機関による範囲拡大を限界づける意味をもちえない。かかる規定も個人番号の濫用を引き起こす可能性があるものというべきであろう（24頁）。

また、漏洩の危険性についても予防措置が実効的であるかは問題である。被告である国は、一方において、情報提供ネットワークシステムについて安全性を強調し、個人番号制度は情報漏洩の危険がないとても安全な制度であると広報しておきながら、個人番号事務実施者に対しては、ガイドライン等で、個人番号はさまざまな機会に漏洩する危険を伴うものであるから、高度で厳格な安全管理措置を施し、取扱いにあたっては細心の注意を払うようにと強く求めている。

要するに、いかに安全性の高いインフラを構築したとしても、これにかかわる個人番号利用事務には、官だけではなく民を含め、きわめて多くの人間の実施者がかかわっているのである。すると、それぞれの事務実施者のレベルで十分な漏洩防止策が講じられていなければ、いくら情報提供ネットワークシステムを強固なものとしようとも個人情報の不正な取得・利用を避けようがないということになるであろう。しかし、健康保険証との一体化や、消費税増税対策のポイント還元などを名目とした個人番号カードの事実上の利用強制などが今後進むことになれば、他人の個人番号を目にする機会を持つ事務実施者の数は莫大な人数になる。そのような莫大な人数の多様な事務実施者に対し、十分な漏えい防止策を講じることが不可能であることは、現段階ですでに生じている事務実施者等の軽率な行為による個人番号漏えい事故の数からしても明らかなことであろう。

個人番号が漏洩するということは、漏洩した個人番号を利用して実際に不正な情報の取得・利用などが行われ、実害が出たかどうかという問題とはかかわりなく、さまざまな個人情報の索引情報である個人番号が他者に知られたとい

うだけでプライバシーに対する危険を生んでいるのであり、それは憲法上の人権であるプライバシー権を侵害しているのである。

第7 結論

まず、番号法が制約することとなる自己情報コントロール権は、憲法13条後段の幸福追求権の一環として憲法上端的に保障されている人権である。

番号法は、個人の自己実現と自己統治、さらには健全な民主政を支えている個人の尊重及び人間の尊厳の実現に直結する自己情報コントロール権の制約立法でありながら、その制約目的の重要度があまりに軽すぎる点で明白に違憲である。

また、個人番号の取得段階では、国に対するハードルがまったく存在せず、利用段階で行われるデータマッチングは住基ネットとは比べものにならないくらいに広範囲である。

さらに、濫用の危険がある番号法19条14号・16号は明白に違憲である。

また、いかに情報提供ネットワークシステムの安全性が堅固であるとしても、個人番号は、莫大に数々の人の眼に触れざるをえないものである以上、その漏えいを防ぐことはそもそも不可能である。

以上より、番号法の違憲性は明らかである。

以上