令和４年（ネオ）第４４７号　個人番号利用差止等請求上告提起事件

上 告 人　[redacted]

被上告人　　国

上　告　理　由　書

２０２３（令和５）年３月６日

最高裁判所　御中

上告人ら訴訟代理人弁護士　　大　　江　　洋　　一

同　　辰　　巳　　創　　史

外１９名

第１　はじめに－急速に進化するIT技術に配慮しない時代遅れの原判決

ＩＴ技術はすさまじい勢いで進化している。すでに控訴審でも詳述したように、顔認証の技術、ＤＮＡ解析などＩＴによる人物の特定の技術は日進月歩の勢いである。例えば中国においては、国中に巨大なカメラネットワークが張り巡らされており、同国の顔認識システムは国内のほぼすべての市民を記録していると言われている。報道によれば、１日あたりの記録件数は６８０万件を超え、ホテルや公園、観光スポット、モスクの周辺に設置されたカメラが人々を撮影し、詳細な情報を記録しているとされる。技術的にはそこまでの個人情報の把握が可能となっているのである。

このことは、個人のプライバシー侵害の危険も飛躍的に拡大していることを示している。そうであるなら、法的な規制・解釈も当然これに伴うことが要求される。

ところが、原判決は、このような発達したＩＴ技術に関する理解に欠けており、そのために切迫したプライバシーへの危機についてあまりに鈍感である。

例えれば、数百キロの射程距離があるミサイルを保有する「敵」（本件では国家権力）について、その技術認識を誤り「ピストルしか持っていないのだからここまで届くはずがない」と述べているようなものである。

民事訴訟の分野において率先してＩＴ化を進めようとする裁判所が、そのＩＴの理解においてこれほどまでに鈍感であることに驚き呆れるばかりである。

マイナンバー制度は、すべての国民に番号を振ることにより、個々人毎の情報の集約を図るという制度である。後述のとおり、政府は個人番号カードを民間事業者が活用することを推奨しているが、この個人番号は、地方公共団体情報システム機構を通じて、マイナンバーに紐付けることが可能であり、結局のところ、民間による個人情報の一元化も可能な立て付けとなっている。

さらに、近時（２０２３年１月）の報道によれば、政府は、現在は社会保障と税、災害対策の３分野に限定しているマイナンバーの利用範囲について、法改正を経ずに省令で定めることを可能とする法改正を行おうとしている。すなわち、国会の審議を経ずに行政の判断のみでマイナンバーの使途拡大が進む恐れや、個人情報漏えいのリスクがさらに拡大することとなる。

マイナンバー制度はこのように、潜在的に、甚大なプライバシー権の侵害を伴う制度であることからして、憲法上到底許容できるものではない。時代錯誤の理解を背景に、そのような危険性を否定した原判決は直ちに取り消されるべきである。

第２　本書面の構成

本書面においては、原判決における「付加説明」（３０頁以下）に対応して、第３において「プライバシーの権利（個人情報についての権利、自由）に関する憲法１

３条の解釈の誤り」、第４において「捜査機関による濫用のおそれについて」、第５において「法１９条１５号及び１７号の規定が白紙委任であって憲法４１条に反すること」、最後に第６において「マイキーＩＤ、電子証明書の発行番号によってプライバシー権侵害が生じること」について述べる。

第３　プライバシーの権利（個人情報についての権利、自由）に関する憲法１３条の解釈の誤り

１　原判決の判断

（１）原判決は、個人番号及び特定個人情報の収集等については、①法律上の根拠が存在し、②目的は正当であり、③番号制度がその正当な目的に適合すること、④目的に範囲を逸脱して、第三者又は行政機関に収集等される具体的危険性が生じているとはいえないとしている。そのうえで、個人に関する情報をみだりに収集、保有、管理若しくは利用され、又、第三者に開示若しくは公表されない自由を侵害するとはいえないとしている。

（２）しかし、原判決の「第三者又は行政機関に収集等される具体的危険性が生じているとはいえない」という解釈、適用は、自己情報コントロール権が提唱されだした高度情報化社会から更に一歩進んだ、コンピューターによる情報管理技術が進み、ビッグデータの時代である現代社会においては時代にそぐわない解釈、適用である。上告人らが主張しているプライバシーの権利（自己情報コントロール権）に関しては、時代の変遷とともに、その権利の内容が変容してきているものであり、その内容の変化に応じた憲法１３条、プライバシーの権利の解釈、そして適用をすべきである。

プライバシーの権利は、①個人に関する情報をみだりに収集されない権利から出発し、その後、②みだりに公開されない権利へと発展してきた。収集から公開の間には、原判決も指摘するように、保有、管理、利用の段階があり、ビッグデータ時代においてマイナンバーにより情報連携することにより、

プライバシーの権利は、収集→保有→管理→利用→管理のすべての段階で侵害が生じうる。そして、現在のビッグデータ時代においては、具体的危険性が生じている。

2　初期のプライバシーの権利（個人情報の収集の場面）

（1）プライバシーの権利の登場

プライバシーの権利は、最初、「ひとりで放っておいてもらう権利」、すなわち、個人の私的領域に他者を無断で立ち入らせないという自由権的、消極的なものとして理解され、発展してきた。かかるプライバシー権が生まれた背景として、１９世紀のアメリカでは、イエロージャーナリズムと呼ばれる扇情的な報道による私生活の暴露が問題となっていた。これに対抗する手段として「ひとりで放っておいてもらう権利」としてのプライバシーの権利が発展してきた。

（2）日本におけるプライバシーの権利の登場

その後、半世紀を経た後、１９６０年代の日本においても、１９６４年（昭和３９年)、「宴のあと」事件一審判決において「私生活をみだりに公開されない法的保障ないし権利」とする私法上の権利（人格権）は個人の尊厳を保ち幸福の追求を保障するうえにおいて必要不可欠なものであるとし、それが憲法に基礎づけられた権利であることを認められた。

私法上の権利として認められた、人格権の一つとしてのプライバシー権は、その後の京都府学連事件や前科照会事件の最高裁判決によって憲法上の権利として確立した。

（3）みだりに個人情報を収集されない権利

京都府学連事件（１９６９年（昭和４４年））においては「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・・・。これを肖像権と称するかどうかは別として、少なくとも、警察官が、正当な理由もないのに、個人の容ぼう等を撮

影することは、憲法１３条の趣旨に反し、許されない」とされた。

指紋押捺拒否事件での下級審判決において、私生活上の自由の一つとして、「承諾なしにみだりに指紋押捺を強制されない自由」があることを認めたが、同一人性を確認するために必要かつ合理的な手段として合憲とされた。最高裁は、指紋の押捺を強制されない自由を憲法１３条によって保護される「個人の私生活上の自由の一つ」としたが、押捺制度の立法目的には「十分な合理性があり、かつ、必要性も肯定できる」とし、手段も「一般的に許容される限度を超えない相当なものであった」とした。

その中で、指紋は「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が、性質上万人不同性、終生不変性をもつので、採取された指紋の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」り、「国家機関が正当な理由もなく指紋の押捺を強制することは、憲法１３条の趣旨に反して許されず・・・」としている。

（４）最近の個人に関する情報の収集についての最高裁判例

ＧＰＳ最高裁判決において、ＧＰＳ（全地球測位システム）端末を承諾なしに車両などに取り付けて行う捜査（ＧＰＳ捜査）につき、①「個人の行動を継続的、網羅的に把握することを必然的に伴うから、個人のプライバシーを侵害し得るものであり」、また、②そのような機器を個人の所持品に密かに装着する点で「公権力による私的領域への侵入を伴うもの」としたうえで、憲法３５条の保障対象には「住居、書類及び所持品」に限らずこれに準ずる私的領域に「侵入」されることのない権利が含まれており、ＧＰＳ捜査は「個人の意思を制圧して憲法の保障する重要な法的利益を侵害するもの」として、刑事訴訟法上特別の根拠規定がなければ許容されない強制の処分にあたると判示したものである。

（５）マイナンバーは、指紋と同様な個体識別情報といえる。

指紋押捺事件における指紋という情報の「万人不同性」、「終生不変性」は、マイナンバーにおける一人ひとりに１２ケタの番号を付番され、同じ番号の者は存在せず、その個人番号は原則生涯不変であるのと同じである。マイナンバーは、指紋やDNA情報などの先天的な情報とは異なり、国により付番される番号ではあるものの、後天的に付番された個人番号は、指紋やDNA情報と同様に個人の識別のための唯一無二の情報となる。

指紋押捺事件においては、最高裁は、採取された指紋の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」り、「国家機関が正当な理由もなく指紋の押捺を強制することは、憲法１３条の趣旨に反して許され」ないとしている。これとパラレルに考えるならば、マイナンバー制度においても、付番された個人番号の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」り、「国家機関が正当な理由もなく個人番号の付番を強制することは、憲法１３条の趣旨に反して許され」ないということになるはずである。

（6）マイナンバーによる情報連携は、継続的、網羅的に個人の行動を把握する

ＧＰＳ捜査の特徴である「個人の行動を継続的、網羅的に把握することを必然的に伴う」は、マイナンバーによる情報連携により社会保障、納税番号ほか、生まれてから亡くなるまでのあらゆるライフイベントの際に生じるあらゆる情報と結合されていき、個人の行動を継続的・網羅的に把握することを必然的に伴うという点では同じである。そうすると、マイナンバーの付番と情報の結合は公権力による私的領域への侵入を伴うものであるといえ、個人の意思を制圧して憲法の保障する重要な法的利益を侵害するものといえる。ここでいう法的利益については、プライバシーの権利にほかならない。

３　自己情報コントロール権

（１）プライバシーの権利の内容の変化

個人の私的領域に他者を無断で立ち入らせないという自由権的、消極的な

ものとして理解されてきたプライバシーの権利は、情報化社会の進展に伴い変化していく。１９６０年代の情報化の進展により、国家や私企業が個人に関する情報を大量に保有することが問題視されるようになった。個人の情報が国や私企業により収集、保有、蓄積されていく中で、保有する個人情報の開示を求め、訂正や削除を行わせる権利が主張されるようになった。

初期の段階で主張された、個人の私的領域に他者を無断で立ちいらせないという自由権的、消極的な従来のプライバシー権から、個人に関する情報（個人情報）が行政機関によって集中的に管理されているという現代社会においては、個人が自己に関する情報を自らコントロールし、自己の情報についての閲読、訂正ないし抹消請求を求めることが必要であると考えられるようになったのである。

そこで、情報化社会の進展にともない、プライバシー権は、自由権的側面のみならず、プライバシーの保護を公権力に対して積極的に請求していくという側面が重視されるようになった。表現の自由が、情報を発信する自由から、知る権利やアクセス権等の情報を取得する自由へと拡大されたのと同様に、プライバシー権もその内容は拡大されていったのである。

（２）自己情報コントロール権の登場

佐藤幸治教授は、書籍の中でプライバシーの権利を「個人が道徳的自律の存在として、自ら善であると判断する目的を追求して、他者とコミュニケートし、自己の存在に関わる情報を開示する範囲を選択できる権利として理解すべきもの」とした。そして、公権力が、個人の道徳的自律の存在に直接関わらない外的事項に関する個別的情報（仮にこれを「プライバシー外延情報」と呼ぶ）を、正当な政府目的のために、正当な方法を通じて取得・保有・利用しても、直ちにはプライバシーの権利の侵害とはいえないが、かかる外延情報も悪用されまたは集積されるとき、個人の道徳的自律の存在に影響を及ぼすものとして、プライバシーの権利の侵害の問題が生ずる。データ・バン

ク社会の問題は、まさにこれであると述べている。

マイナンバーは、個人に付番された１２桁の番号であり、それ自体は個人の道徳的自立の存在に直接関わらないものであるが、社会保障、納税情報を初めとして行政機関が保有している個人のあらゆる情報とデータマッチングされたり、集積されると、佐藤教授が指摘するように、個人の道徳的自立の存在に影響を及ぼすものとして、プライバシーの権利の侵害が生じうる。

自己情報コントロール権が提唱されたころ、個人情報保護法が成立、施行されているが（１９８８年、昭和６３年)、その背景として、１９７０年代以降の情報化社会の進展、具体的にはコンピュータによる情報処理の普及がある。個人情報のデータベースが構築されコンピュータで処理されるようになると、個人情報の利用が飛躍的に容易になってきたのである。

国が保有している課税関係や社会保障関係の個人情報を考えてみると、これがそれぞれデータベース化されれば、両者を結合して分析を行うことが容易となる。こうしたことは、従来の紙の書類による個人情報の保有の場合には非常に困難であった。データベースの結合、分析によって、税の過少申告や社会保障の不正受給といった不正行為の発見が容易となり、行政の効率化等に資する面もある。他方で、これまではそれぞれの行政分野で必要な個人情報が断片的に収集され、保有されていたに過ぎなかったのが、このような情報の突き合わせ（データマッチング）によって個人の姿が立体的に浮かび上がってくることになり、このことが新たな国による個人の管理につながるとして、プライバシー侵害であると捉えられるようになってきた。こうした状況は民間事業者との関係でも同様であり、民間事業者による個人情報のコンピュータ管理についても同じような脅威が語られた。

また、コンピュータによる個人情報の管理がなされ、さらにネットワーク化が進むと、大量の個人情報を容易に持ち出すことができることになり、個人情報の漏えいといったリスクも飛躍的に増大している。

（3）みだりに個人情報を公開されない権利

前科照会事件、（１９８１年、昭和５６年）において、最高裁は、地方公共団体が弁護士の照会に安易に応じた行為を違法とし、前科をみだりに公開されない自由をプライバシー権の一つとして認める趣旨とも解されるような見解も示している。「前科・犯罪経歴は人の名誉・信用にかかわり、これをみだりに公開されないのは法律上の保護に値する利益である」とした。

伊藤正巳裁判官の補足意見は、「前科等は、個人のプライバシーのうちでも最も他人に知られたくないものの一つであり、公開が許されるためには、裁判のために公開される場合であっても、その公開が公正な裁判の実現のために必須のものであり、他に代わるべき立証手段がないときなどのように、プライバシーに優越する利益が存在するのでなければならず、その場合でも必要最小限の範囲に限って公開しうるにとどまる。」と述べ、やむにやまれぬ利益基準に当たる厳格審査基準を適用した。

江沢民講演会参加者名簿提出事件、（２００３年、平成１５年）は、早稲田大学で中国の江沢民国家主席の講演会が開催された際に、警備に当たった警察の要請に応えて大学が、参加希望学生が氏名・学籍番号・住所・電話番号を記入した名簿の写しを学生に無断で警察に提出したことに対して、学生が大学に対してプライバシー侵害を理由に損害賠償を求めた事案である。最高裁は、「本人が、自己が欲しない他者にはみだりにこれを開示されたくないと考えることは自然なことであり、そのことへの期待は保護されるべきものであるから、本件個人情報は、上告人等のプライバシーに係る情報として法的保護の対象となる」とした。

住基ネット訴訟、（２００８年、平成２０年）において、最高裁は、「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ものと解される」とした。そのうえで、本人確認情報の目的外使用には住民基本台帳法上重い刑罰により禁止さ

れる等の制度的担保が組み込まれており、プライバシー侵害の具体的な危険が発生しているとは言えないと判示した。

情報化社会の進展に応じて、裁判所も、政府や私企業が取得した個人情報をみだりに公開されない（開示、公表されない）自由が保障されることを最高裁も認めるに至ったのである。

（4）個人情報の取り扱いの全過程が保障されていると考えるべき

個人に関する情報について保障される自由は、以下のように保障されるに至っている。

個人に関する情報の取得	宴のあと、京都府学連、
↓	指紋押捺拒否、GPS 捜査
保有	
↓	
管理、利用	
↓	
開示、公表	前科照会、江沢民講演会参加者名簿
	住基ネット

この点、保有、管理、利用に関する事例はない（若しくは少ない）ものの、入口の取得が保障されて、出口の公開が保障されるのであるから、その間の保有、管理、利用も当然保障されることになる。住基ネット判決や原判決も「みだりに収集、保有、管理若しくは利用され、又は第三者に開示若しくは公表されない自由」と述べており、保有、管理、利用も保障されることが前提となっている。

4　現在の状況（ビッグデータ時代）

（1）自己情報コントロール権が提唱されて以降の時代の変化

現代においては、①１９７０年代のインテル社によるマイクロプロセッサーの開発と、それによる計算能力の向上によって画される第一段階、②ネッ

トワーク化と、それによる連結能力の向上によって画される第二段階を経て、③「データ」と「予測能力」の向上によって画される第三段階に至っている。データバンク社会を超えるビッグデータ社会が到来している。

ビッグデータについては、明確な定義があるわけではないが、従来のデータベース管理システムなどでは記録や保管、解析が難しいような巨大なデータ群のことを指す。企業向け情報システムメーカーのマーケティング用語として多用されている。

多くの場合、ビッグデータとは単に量が多いだけでなく、様々な種類・形式が含まれる非構造化データ・非定型的データであり、さらに、日々膨大に生成・記録される時系列性・リアルタイム性のあるようなものを指すことが多い。今までは管理しきれないため見過ごされてきたそのようなデータ群を記録・保管して即座に解析することで、ビジネスや社会に有用な知見を得たり、これまでにないような新たな仕組みやシステムを産み出す可能性が高まるとされている。

また、大量のデータから知識、知見を掘り当てるデータマイニングも行われるようになった。これは、膨大なデータセット（ビッグデータ）のなかから統計的に有意なパターンないし関係性を抽出、発見するものである。情報システムに蓄積した巨大なデータの集合をコンピュータによって解析し、これまで知られていなかった規則性や傾向など、何らかの有用な知見を得ることができる。「マイニング」(mining)とは「採掘」の意味で、膨大なデータの集積を鉱山になぞらえ、そこから有用な知見を見出すことを鉱石を掘り出すことに例えた表現となっている。

２０１５年（平成２７年）に行われた個人情報保護法の改正の背景には、①スマートフォンをはじめとするモバイル機器の普及や情報通信技術の急速な進展により、パーソナルデータを含んだビッグデータの収集分析が可能となったこと、②特定の個人を識別できなくても、同一の人物であることを

識別可能な場合（それが誰か１人の情報であることは判明するが、その１人が誰であるかまでは判明しない場合）が情報通信技術の進展により増大し、それがビジネスに利活用される事例（ＩＰアドレスを利用した行動ターゲティング広告など）が増大するにつれ、特定の個人が識別されることを用件とする個人情報に着目した規制のみでは不十分ではないかという問題が認識されるようになったこと、③経済活動のグローバル化の進展に伴い、情報通信技術の面においても、クラウドサービスに代表されるような国境を越えた情報の流通が進展しており、パーソナルデータもその例外ではないため、日本国民のパーソナルデータも日本の主権の及ばない海外に蓄積し、海外で利活用される傾向が一層進展していくことが想定されるので、日本でも国際的調和に留意しつつ、諸外国からパーソナルデータが集積する事業環境を整備することが要請されていることがあった。個人情報保護法においては、時代の変化に応じた改正がなされている。そうすると、プライバシーの権利についても、時代の変化に応じて内容も変化させていくべきである。

（２）自己情報コントロール権において指摘されていたことが現実化している

１９８０年に出版された、堀部政男著「現代のプライバシー」（岩波新書）において、堀部は「情報収集技術の発達、その蓄積能力の巨大化、個別情報の集中可能性などをあげることができる。個人の情報は、その部分、部分のみを取り出しても、ある特定の個人の全体像を浮かびあがらせることは困難である。しかし、部分的な情報が個人に付された統一的な番号で進められ、組み合わせられるならば、バラバラでは意味ないが、多数の部分の合成によって意味を持つようになるモンタージュ写真のように、個人を識別することが可能になってくる。ところが、個別的な情報のなかに誤っている物がある場合には、本人の真の姿をとらえることができなくなる。それは、あたかもいびつな金魚ばちに入れられて、ゆがんでみえる金魚のようなものである。」と述べている。

ここでいう「統一的な番号」は、当時は納税者番号、社会保障番号、共通番号であったものが、現在ではマイナンバーのことを指している。社会保障に関する断片的な情報、税金に関する断片的な情報、その他行政機関が保有する断片的な情報が、統一的な番号（マイナンバー）によりデータマッチングされることにより、バラバラでは意味がなかった情報が、多数の部分の合成によって意味をもつようになり、個人を識別することが可能となってくる。

さらに現代では、プロファイリングの技術も変化、向上してきた。プロファイリングは、ある分野における能力を評価、予測するため、若しくは人々の分類の識別を支援するために、個人の精神的及び行動的特性を記録、分析することとか、自然人に関する一定の個人的側面を評価すること、又は、特に、当該自然人の職務上の成果、経済状況、位置、健康、個人的嗜好、信頼性若しくは行動を分析又は予測することを意図した、あらゆる形式の自動個人データ処理であると言われている。

プロファイリングは、対象とする個人が誰であるか分からなくても同一個人に紐付くデータを組み合わせることで、その個人の人物像を描くことができる一方で、そうしたデータに不正確なものも含まれていた場合、描かれた人物像も歪んでしまうリスクがある。また、データには誤りはなかったとしても、分析に用いるアルゴリズムによっては、本人に好ましくない人物像が描かれてしまうリスクがある。

同じく、堀部政男著「プライバシーと高度情報化社会」において、堀部は、「１９８０年代に入り、今日では、情報化社会という概念でとらえようとしている情報化はコンピュータと電気通信とが結合されて広く社会に影響を与える現象として認識されているということができる。換言すれば、現代から近未来にかけての情報化は、独立のコンピュータといういわば「点」が通信回線という「線」と結合して「面」へと拡大し（ネットワーク化の進展）、加速度的に社会のあらゆる分野、特に家庭生活にまで波及する傾向を示して

いると把握できる。」と述べている。１９８０年代に言われていたことが、現代（２０２０年代）に現実化してきているといえる。

山本龍彦教授は、その著書「プライバシーの権利を考える」の中で、ビッグデータ社会においては、情報の連結可能性、検索可能性、解析可能性を飛躍的に高め、個人のデジタル・バイオグラフィーまたはデジタル・ダブル（分身）の作成を可能にした現代の情報技術を前提とすると、情報システムやデータベースの存在それ自体が、我々を無力化し、脆弱化させうると述べている。そして、現代人の生活、さらに現代人のアイデンティティ形成は、情報システムやデータベースに強く依存しており、もはやそれなくしてはありえないとも述べている。

そのような高度にネットワーク化されたデータベースにおいて、自分の情報が、どこに、どの程度、いつまで保存されているのか、ネットワーク上をどのように飛び交い、誰に、どのように扱われるのか正確に知ることができない。データベースにおける情報の流通は、我々情報主体にとって基本的に不可視で、具体的に補足することができなくなっている。

マイナンバーは、複数の機関間において、それぞれの機関ごとに個人番号やそれ以外の番号を付して管理している同一人の情報を紐付けし、相互に活用することが可能となり、本人確認にも用いられる。番号法の規定によるものを除く、特定個人情報（個人番号をその内容に含む情報）の収集、保管、特定個人情報ファイルの作成の禁止をはじめ、個人情報保護委員会による監視、監督、「要配慮個人情報」に関する規定の整備等々の配慮は施されてはいるが、この制度に取り込まれる情報は「際限なく拡大していく」ことが予想され、個人の様々な個人情報がマイナンバーをキーにして名寄、突合されていくのではないかと不気味な危惧を一概に否定しきれない。

既に保有している断片的個人情報からは明らかにならなかった情報主体の私事を新たに知ろうとする行為が可能となっている。データ媒介的覗き見と

もいえ、これはプライバシーの権利が誕生した際の私生活の暴露が再び問題となっている

宴のあと事件判決が「一般の人が、・・・当該私人の私生活であると誤認しても不合理でない程度の真実らしく受け取られるものであれば、それはなおプライバシーの侵害としてとらえることができる」としているが、断片的な情報をデータマッチングすることにより、一定の制度が担保されたアルゴリズムによって導かれた結果は、「真実らしく受け取られる」情報であると解され、その限りにおいて、データ媒介的覗き見として、プライバシー権の侵害を構成する。

5　マイナンバーによるデータマッチングにより私事がみだりに収集される

マイナンバーは、一人ひとりに１２ケタの番号を付番し、その個人番号は原則生涯不変であり、同じ番号の者は存在しないのであるから、付番された個人番号は、指紋やＤＮＡ情報と同様に個人の識別のための唯一無二の情報となる。

各行政機関が保有する断片的な個人の情報は、その部分、部分のみを取り出しても、ある特定の個人の全体像を浮かびあがらせることは困難であるが、マイナンバーという個人に付番された統一的な番号で部分的な情報が組み合わせられるならば、バラバラでは意味ないが、多数の部分の合成によって意味を持つようになるモンタージュ写真のように、個人を識別することが可能になってくる。

今までは、断片的な個人情報からは明らかにならなかった情報主体（＝個人）の私事について、現在のプロファイリング技術の下では、取得できるようになってきている。アメリカのターゲット社という小売店が、商品購入者の購買履歴を、性、年齢などの属性やウェブの閲覧履歴をみ合わせて分析し、妊娠や慢性疾患の可能性といった顧客プロファイルを作成し、それに基づいて妊娠検査薬やサプリメントなどのダイレクトメールを送信することができた。妊娠という事実は、当人の父親はダイレクトメールが送られてくるまでは知らなかった

し、妊娠初期であれは当人ですら知らなかった妊娠という事実を、プロファイリング技術を駆使した小売店の方がいち早く把握するということも十分ありうる。データマッチングされた情報の利用方法次第では、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。

以上のように、番号利用法において、マイナンバーを共通の識別子として、各行政機関が保有する個人に関する情報がデータマッチングされることにより、国家が断片的な個人情報からは明らかにならなかった個人の私事が取得できるようになる。このような時代背景（ビックデータ社会におけるコンピューターのアルゴリズムによるプロファイリングが実現した社会）の下では、共通の識別子たるマイナンバーを起点として行政機関が保有する個人情報をデータマッチングさせることにより、みだりに個人に関する情報を取得される具体的危険性が生じているといえる。原判決は、この点を見過ごして、具体的危険性が生じているということはできないと解釈、適用しているのであり、プライバシーの権利の解釈を誤っている。

第４　捜査機関による濫用のおそれについて

１　個人番号は新しい犯罪捜査等に有益である

上告人らは繰り返し、警察等の捜査機関により、マイナンバー制度が濫用される危険性を指摘してきた（例えば、原審における２０２２年５月２日付準備書面２など）。

すなわち、急速な情報通信技術の進展により、大量の個人データを収集し、分析することにより、将来犯罪を犯す可能性の高い人物を特定し、警察等による監視対象としたり、裁判所における量刑に反映させたりすることが可能となっていること（アメリカでは現実に行なわれている）、日本でも警察がこうした新しい技術を犯罪捜査や治安維持活動に利用していることを指摘した。そしてこうしたデータ分析を行う上で、確実に個人を特定しうる識別子を使用できれ

ば、極めて有益であること、個人番号はまさにその条件に合致していることを述べた。

2　原判決は情報通信技術の進展を無視している

（1）これに対して原判決は、情報通信技術の進展による新しい捜査手法について何ら言及せず、従来の捜査手法を前提とした上で、しかも、個人番号は、捜査機関による情報の収集を効率化するだけの働きしかしないものと問題を矮小化してしまった。

すなわち、原判決は、「・・・捜査機関は、犯罪の疑いがあり、かつ捜査上の必要がある場合でなければ、公務所等に対して特定個人情報の提供を求めることはできないというべきところ、控訴人らが個人番号により紐付けられることを懸念する税金、年金、社会保障等の情報は、従前より、捜査機関において、捜査上の必要があれば捜査関係事項照会等の任意捜査の方法により取得しうるものである。」（３１、３２頁）として、あくまで従来からの捜査手法だけを念頭に置いている。

その上で、「これらの情報が個人番号により紐付けられることで、捜査機関による情報収集が効率化する可能性はあるが、そうであるからといって、番号利用法によって無限定な情報収集が許容されるようになったわけではないし、当然ながら、刑事事件の捜査のため提供を受けた特定個人情報は、提供を受けた目的を達成するために必要な限度で許されるにすぎない。」（３２頁）としている。

（2）以上のように、原判決は、情報通信技術の飛躍的な発展により、新しい捜査手法等が現実のものとなっており、これに個人番号が活用される危険性のあることを無視し、何らの判断も示していない。

しかも原判決は、「・・・刑事事件の捜査のため提供を受けた特定個人情報は、提供を受けた目的を達成するために必要な限度で許されるにすぎない」とするが、現実の警察によるデータの利用実態すら無視した判断を示してい

る。

警察が、個別の事件の捜査過程において取得した指紋やＤＮＡをデータベース化し、犯罪捜査等に活用していることは広く知られている。指紋やＤＮＡの取得は、あくまで個別の事件の捜査に必要であるから許容されているはずだが、これをデータベース化し、将来の犯罪捜査等にも利用しているのである。このような利用は法律に基づくものではない。

そうすると、警察は、具体的な事件の捜査のために取得した特定個人情報であっても、これをデータベース化し、将来の犯罪捜査等に利用するはずである。このような特定個人情報の利用は法律に基づくものではないし、個人情報保護委員会の監視も及ばない。原判決はこのような事態を許容するのであろうか。

第５　法１９条１５号及び１７号の規定が白紙委任であって、憲法４１条に反すること

１　原判決の判断

上告人らは、法１９条１５号及び１７号による委任が個別具体的なものではない白紙委任であること及び同１５号により制定された施行令別表３の内容は委任の範囲を超えたものであることから、憲法１３条、４１条に違反するものであると主張した。

これに対し、原判決は１５号については、「その他政令で定める公益上の必要があるとき」というのは同号の具体的列挙にかかる事由と同等、同様の公益上の必要性があるものに限定するものと認められるため白紙委任ではないとし、同号にもとづく施行令別表３の内容は、同号にいう公益とは税、社会保障及び災害分野の３分野に限定する理由はないとして委任の範囲を超えるものでないとした。

１７号については、「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」としているのは、同条１号から１６号で具体的に定める例外的場合に準ずる場合をいうことは明らかであるため白紙委任ではないとした。

２　１９条１５号の白紙委任性

そもそも法１９条は特定個人情報の提供を原則として禁止し、その例外を各号で列挙する形となっているが、１５号で「その他政令で定める公益上の必要があるとき」とのみ規定して政令に例外を委任している。「公益上の必要」というのはあまりにも曖昧不明確にすぎるものであり、さらに１５号の列挙事由と同等、同様のものと原判決が解したように捉えたとしても「同等」「同様」のものということでは何らの縛りになるはずもない。

さらに、原判決は、施行令別表３を憲法に違反しないものとする理由付けのために、公益の内容として、番号法の本来の目的である税、社会保障及び災害の３分野に限定しないものと解したのである。これでは、「公益上の必要があるとき」としたことが、特定個人情報提供が許容される例外事由を政令で定める際に何らの制限もないことになってしまう。

つまり、原判決は、「公益上の必要があるとき」というのを、番号法の立法趣旨からも逸脱して無限定に広く認めて構わないとしたものであるが、それこそ１５号が白紙委任を定めた条項であることを認めたのと同じである。

従って、法１９条１５号が白紙委任であるという上告人らの主張は正しく、法律の根拠なく上告人らの憲法上の権利を成約するものとして憲法４１条に違反し、上告人ら個人の情報をみだりに収集（提供）されるものとして憲法１３条に違反する。

３　１９条１７号の白紙委任性

原判決は、１７号は「その他これらに準ずるもの」という文言が同条１号から１６号で具体的に定める例外的場合であるから無制限の委任をしたものでないとする。

しかし、１９条各号の例外事由全てに準ずる場合というのはそれ自体で広範であり、個人情報保護委員会規則で例外事由を定めるにあたっては広く認められるということを指しているに他ならない。同条１号から１６号の例外事由を厳格に解釈するというのなら別であるが、原判決が前記２で述べたとおり１５号の政令委任に関して「公益上の必要」を法の所定の目的から逸脱して判断しても構わないと解したのだから、１７号で定める例外に関しての制限はほとんどないという他ない。

原判決は、１号から１６号に準ずる場合ということで委任の具体性が確保されているとするが、その内容について何らの説明もなく、むしろ上記のとおり１号から１６号の例外事由を広く解釈する姿勢を示していることからすると、個人情報保護法への規則委任は制限のない白紙委任と考えられる。

従って、法１９条１７号が白紙委任であるという上告人らの主張は正しく、１５号同様に憲法４１条及び憲法１３条に違反する。

第６　マイキーＩＤ、電子証明書の発行番号によってプライバシー権侵害が生じること

１　原判決は、「申請者の申請により個人番号カードに記録される電子証明書の発行番号は有効期限があり、有効期限の経過に伴い新たに発行されるたび異なる番号となるし、マイキーＩＤも、任意でマイキープラットフォームを利用することを選択した際に初めて作成されるもので、変更したり廃止することもできるものであるから、いずれも、全住民に付番され、原則として生涯不変の番号である個人番号とはその性質が異なり、個人番号と事実上同一の機能を有するとまではいえない」と判示する（３５頁）。

２　しかし、電子証明書の有効期限は５年間であって、それほど頻繁に更新が必要となる訳ではない上に、電子証明書を発行し、その失効情報を管理している地方公共団体情報システム機構（以下「機構」という）は当然ながら、その変

更履歴も管理している。そして、個人番号カードを民間事業者が活用することを推奨する観点から、機構は、民間事業者が今の発行番号で照会すれば、その前の発行番号を回答するサービスも提供している。したがって、機構の管理する発行番号の変更履歴を参照すれば、５年ごとに発行番号が変更されても、同一人に対して発行された電子証明書の発行番号をすべて特定することは可能である。

3　また、原判決は、電子証明書の発行番号は、番号利用法の規制が及ばないことは認めつつ、公的個人認証法において、他の機関の電子計算機システムや他の個人情報ファイルとの結合によって、特定の個人に係る個人情報を集積することができないよう必要な規制がかけられていると判示している（３５頁）。

しかし、原判決の適示する公的個人認証法６３条１項は、検証者等以外の者が、データベースを構成することを禁じているにすぎない。署名検証者等である行政機関や民間事業者は、当然ながら、電子証明書の発行番号が記録されたデータベースを構成することが許されている。また、同法５２条及び５３条は、検証者等に対し、機構から受領した失効情報等について、確認目的以外での利用・提供を禁止しているが、同条項で禁止されているのは、「機構から受領した」失効情報等である。個人番号カードを使ってオンラインで手続きを申請した際に、利用者が送信した電子証明書に含まれる発行番号について、確認目的以外の目的で利用することが禁止されているとは解されない。さらに、民間事業者が署名検証者等になるためには主務大臣の認定を受ける必要があり、当該認定に関し、総務省告示により電子証明書の発行番号の外部提供は禁止されているものの、当該規制は法律によるものではない上に、情報の漏えい防止等のための措置として定められており、名寄せやデータマッチングを制限するための規制ですらない。また、同法４５条において、機構が認証業務情報を利用・提供できる場合が限定されているが、例えば、捜査機関が、犯罪捜査のために必要として、刑事訴訟法１９７条２項に基づく捜査事項照会によって、認証業務情

報の提供を求めた場合に、公的個人認証法４５条各号に規定がないことから、機構がこれを提供できないとは到底解されない。これは機構以外についても言える。政府が推奨するように、個人番号カードの電子証明書の利用が広く普及すれば、官民問わず、電子証明書の発行番号と紐付けたデータベースが構成されることとなる。そしてこれらのデータベースに記録された情報について、捜査機関が、犯罪捜査のために必要として、刑事訴訟法に基づく照会をした場合には、公的個人認証法があるからといって、その提供が違法になるとは解されない。

以上のとおり、公的個人認証法は規制として不十分である。

4　また、マイキーＩＤも変更したり廃止したりできるとはいえ、度々変更したり廃止することは現実的でなく、電子証明書の発行番号と同様に情報の名寄せ、プロファイリングに利用される可能性がある上に、マイキーＩＤついては、番号法の規制も個人情報保護法の規制も及ばないのはもちろん、公的個人認証法の規制すら及ばない。

5　以上のとおり、個人番号カードの利用が事実上義務付けられる状況となっている現状においては、マイキーＩＤや電子証明書の発行番号を利用して、情報の名寄せ・プロファイリングが行われ、プライバシー権が侵害される具体的危険がある。

以上