

平成27年(ワ)第34010号

平成28年(ワ)第9404号

マイナンバー(個人番号)利用差止等請求事件

原告 関口博ほか40名

被告 国

準備書面(8)

2019年(令和元年)8月29日

東京地方裁判所民事第26部合議2係 御中

原告ら訴訟代理人 弁護士 水 永 誠 二

同 瀬 川 宏 貴

同 出 口 かおり

同 小 峰 将太郎

【目次】

はじめに

- 第1章 目的の重要性、手段の相当性に関する厳格審査基準による合憲性審査
 - 第1 合憲性審査基準—3頁
 - 第2 制度目的が公共の福祉を追求するものとはいえないことについて—4頁
 - 第3 目的達成手段としての個人番号の生成・指定・利用の必要性和合理性がないことについて—14頁
 - 第4 番号法上、法の目的と関連性のない個人番号の利用が許容されており、手段の必要性・合理性を欠くこと—19頁
 - 第5 個人番号カードの合憲性審査—28頁
- 第2章 住基ネット最高裁判決に基づく「構造審査」基準による合憲性審査
 - 第1 構造審査基準—36頁
 - 第2 マイナンバー制度の特質—36頁
 - 第3 システム技術上・法制度上の「不備」—37頁
 - 第4 被告がプライバシーや安全性を軽視し「不備」を生み出す根拠について—50頁
 - 第5 合憲性審査の結論—55頁
- 第3章 損害賠償について—55頁
- おわりに—55頁

【本準備書面においては、以下の用語例を用いる】

番号法 : 行政手続き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

個人番号 : マイナンバーともいう。

個人番号制度 : マイナンバー制度ともいう。

個人番号カード : マイナンバーカードともいう。

特定個人情報 : 個人番号とひも付けられた個人情報をいう。

平成20年住基ネット最高裁判決 : 平成20年3月6日最高裁第一小法廷判決（民集第62巻3号665頁）をいう。

はじめに

原告らが、その準備書面（7）で述べたように、現代社会におけるプライバシー侵害は、単にプライバシー情報を報道されたり、漏えいされたりする古典的な形での侵害だけではない。情報通信技術の高度な発展に伴い、それ自体は単純な個人情報であっても、それらが（特にデジタル化されたデータが）名寄せされてデータマッチングされれば、その人物の趣味や嗜好、人物像などを分析する＝プロファイリングする＝ことができるという形での侵害が重大で深刻な問題となっている。近時においては、A I（Artificial Intelligence 人工知能）の活用により、それらが容易に且つ大規模に、そして高い精度で行われうる社会を迎えているのである。

このような社会を迎えている現代においては、原告らのみならず、全国民・外国人住民のプライバシーを保障して行くために、個人情報を名寄せされない（されにくい）ようにすることを1つの柱として、その保障を十全にはかつてゆく必要がある。そうしなければ、プライバシー保障は、その基盤すら喪失するのである。一旦失われたプライバシーは元に戻すことはできない。さらに、そのような人物像がプロファイリングされてしまう社会では、「情報操作」などにより、民主主義社会の基盤すら掘り崩される結果となる。近年の米国大統領選挙がその危険性の一端を示している。

以上述べたような現代社会におけるプライバシー保障の重要性に鑑みるならば、その権利を制限・侵害する制度に関する合憲性は、少なくとも2つの審査基準により、厳格に判断されなければならない。

以下、第1章において、個人番号の「利用の目的の重要性、手段の相当性に関する厳格審査基準」による合憲性審査について、第2章において、平成20年3月6日住基ネット最高裁判決に基づく、いわゆる「構造審査」基準による合憲性審査について、それぞれ詳述する。

第1章 目的の重要性、手段の相当性に関する厳格審査基準による合憲性審査

第1 合憲性審査基準

1 マイナンバーシステムにおける個人番号の利用に関しては、第1に、個人番号とひ

も付けられた個人情報（特定個人情報）の取得や利用、保存、譲渡などの目的がそれぞれ公共の福祉を追求するものといえるかが厳格に審査されなければならない。その上で、第2に、仮にそのような目的が認められたとしても、目的達成のための具体的な手段（取得の手段や利用方法、保存形態など）が目的達成にとって必要かつ合理的なものといえるか、が厳格に問わ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 以下、第2において、目的の重要性・必要性が存しないこと（公共の福祉を追求するものとはいえないこと）について、第3において、（そもそも目的において重要な人権侵害を許容できるような重要性・必要性が存しない上に）目的達成の手段としての必要性・合理性が存しないことについて、第4において、番号法は、大幅な目的外利用を認めていることから、手段としての必要性・合理性を欠くことについて、第5において、マイナンバー制度の重要な柱として位置づけられている個人番号カードがプライバシー保護を第一に考えた制度設計となっていないため、原告らのプライバシーが侵害されていることについて、それぞれ詳述する。

第2 制度目的が公共の福祉を追求するものとはいえないことについて

プライバシーという重要な権利を侵害（制限）する場合は、その目的に公共の福祉を追求する上における重要性・必要性が存しなければならないことはいうまでもない。

1 個人番号の生成・指定と利用の目的の正当性について

被告は、「番号制度は、行政運営の効率化、公正な給付と負担の確保及び国民の利便性の向上を目的とする・・・（番号利用法1条）」ものであり、番号制度における個

人番号の利用及び特定個人情報の提供は、「法令又は条例の根拠に基づき」、「正当な行政目的の範囲内」であると主張する（第2準備書面、第2、2・7頁）。

この点、玉蟲教授は、「番号法」1条をあげて、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手続き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が目的であると指摘する（甲54）。

被告のあげる「行政運営の効率化」が甲54の①～③、「公正な給付と負担の確保」が甲54の④、「国民の利便性の向上」が甲54の⑤及び⑥に当たる。

そこで、以下、この3つの目的について、それぞれ検討するが、いずれも原告らの権利制限を正当化しうる正当な目的たりえない。

2 「国民の利便性の向上」（目的その1）について

「国民の利便性の向上」は、原告らの権利制限の理由たりえない

以下の理由による。

- (1) 第1に、原告らは、「利便性」よりもプライバシーの確保を求めている。「利便性」を求めている原告らに対して、その者に対する「利便性」を理由に権利制限を正当化することができないことは当たり前である。

玉蟲教授も、「⑤⑥のような国民の利益が国民のプライバシーに介入するための正当な目的といえるかはやや疑問が残る」と指摘している（甲54・18頁）。

- (2) 第2に、そもそも、令和元年6月25日に実施された原告原田の本人尋問により、本来の利用分野である社会保障分野でも、利用者に申請時の添付書類の省略等はほとんどなく、利便性は認められないことが明らかとなっている（以下、「原田調書〇頁」と表示する）。

具体的には、生活保護行政において、マイナンバー制度開始後も、保護を申請する住民は所得証明書や年金証書等の書類を挙証資料として提出する必要があるし（原田調書6頁）、電子申請でできるという保育園の入園申込についても、添付書類は別途郵送するか役所に出向いて提出する必要がある（同12頁）。待機児童が多い自治体では、必要とする住民が保育園に入所できるようにするために、1

件30分以上も時間をかけて面談して、各住民の実情を踏まえて保育園の入所希望を調整している（同13頁）。むしろ社会保障分野においては、手続の利便性より、必要な住民に必要な福祉サービスが行き渡ることのほうが重要なのであり、国民の利便性のためにマイナンバー制度を導入する意味はない。

- (3) 第3に、マイナンバー制度の、利用関係事務実施者に対して、過大な責務と費用、精神的な負担を義務付けている。マイナンバー制度は、民—民—官で個人番号とひも付けられた個人情報提供・流通する。そのため、個人番号を収集・保管し、官（行政）に提出することが義務づけられた税理士や雇用主などは、何らのメリットもないにもかかわらず、厳格な安全管理義務を負わされるなど、非常に過大な義務を負わされている。この点は、原告でもある医師や税理士の陳述により明らかである。

しかも、特定個人情報を不適正に取り扱った場合には、個人情報保護委員会から指導・助言や勧告・命令を受ける場合があるほか、正当な理由がないのに、個人の秘密が記録された特定個人情報ファイル（個人番号をその内容に含む個人情報ファイル）を提供した場合などには、重い刑罰の対象ともなりうるのである。

- (4) 第4に、国も、個人番号を提示しない利用者の場合は「情報連携しない」方針を出している。すなわち、平成29年11月8日付「情報連携の本格運用開始に関するQ&A」（内閣官房番号制度推進室・総務省大臣官房個人番号企画室作成）は、「問6 申請書類にマイナンバーを記載するよう求めてもなお、申請者が記載を拒否する場合、どう対応すべきか。」と設問し、「申請者がマイナンバーの提供を明示的に拒否する場合は、情報連携を行わず、申請者に添付書類の提出を求めることが適切です」と答えているのである（甲69）。

これは、「番号法第22条第2項による添付書類の省略は、原則として本人から各制度の個別法令において義務とされている個人番号の提供がなされ、情報連携を行った結果として実施されるものであることを踏まえ、当該義務を履行しない（個人番号を提供しない）者については情報連携を行わないことが適切であると整理している」ためであるとされているが、まさに上記(1)で述べたことを、国も実質的

に認めていると言わざるを得ない。

3 「行政運営の効率化」(目的その2) について

「行政運営の効率化」も原告らの権利制限の理由たりえない

(1) 第1に、そもそも、「行政運営の効率化」を理由として、国民の最重要の人権であるプライバシーを制限できるかという問題が存する。

玉蟲教授も、「行政機関にとっての利益である①～④を追求することについても、これらが純粹に行政機関の便宜のみを追求するものであるとするならば、それを国民のプライバシーへの介入を正当化する目的とみることはできない。かりにこれらが行政機関の便宜という観点のみから設定された目的である場合には、公共の福祉を追求するものとはいえず、端的に違憲であるというべきであろう。」と指摘している(甲54・18頁)。

(2) 第2に、原告原田本人尋問により、福祉の現場においては、「行政運営の効率化」も実現していないことが明らかとなっている。すなわち、生活保護行政において、申請者が個人番号記入は拒否しないものの番号がわからない場合は、行政職員が職権で住民票から番号を調べる手間が発生したり(原田調書2頁)、個人番号を記入した場合は必ず本人確認をしなければならない義務があり(同3頁)、番号確認と身元確認について、確認書類を作成しなければならず(同3～4頁)、従前の本人確認手続と異なり、番号法施行細則に従い、身元確認書類として認められた資料に基づき確認しなければならないという新たな義務を負担させられている(同4頁)。

さらに、従前、同一の自治体内において税情報や手当に関する情報をシステム上で確認できたにもかかわらず、マイナンバー制度導入後は、マイナンバー利用事務については新たに自治体で条例を制定しないと同一自治体内であっても情報を確認することができなくなってしまい、条例制定のためには個人情報保護評価を実施する必要が生じた(同7頁)。

結局、マイナンバー制度導入により生活保護行政において減った業務はなく、職員にとって行政運営の効率化は全く感じられず、むしろ上記の手間が増えたこ

とで仕事が増えたと感じてしまっている（同6頁）。生活保護認定までの期間も短縮されていない（同6～7頁）。

(3) 第3に、「費用対効果」の点からも正当化し得ない。

「行政運営の効率化」は、「費用削減効果」や「費用対効果」によって測られることが多い。被告も、ある制度を導入する際、その指標の一つとして用いる場合が多い。実際、平成20年住基ネット最高裁判決の対象となった事件においても、被告国は「費用対効果」について主張した。しかし、本件において、被告は、その点を具体的に主張立証すらしていない。

ア 被告は、わずかに、その第2準備書面、第2において、「職員数について単年度当たり7130人分の事務の削減が見込まれる」、「職員数について単年度当たり1910人分の事務の削減が見込まれる。また、仮に、税務職員等がそれらの作業の効率化により、人員を調査・徴収事務に当てた場合における税収は単年度当たり2400億円の増加が見込まれる」等と主張したのみである（傍点は原告ら代理人）。

そこで、原告らが、準備書面(5)において、「マイナンバー制度(納税者番号制度)が実施済みとなったこともあるので、それらの点について主張立証を行う予定が存するのかを求釈明したところ(9頁)、被告は、「原告らが述べる『結果(経費削減や効果等)』や『費用対効果の試算やその根拠』について、今後、被告において主張・立証を行う予定はない」(第4準備書面、第3、3・9頁)と釈明した。

すなわち、被告は、その主張する目的の正当性について、具体的な主張立証すらできなかったのである。

イ マイナンバー制度の創設・運用に要する費用は、膨大な金額に上っている。

被告は、

「平成25年度から平成31年度における制度導入に伴うシステム(付番システム、情報提供ネットワークシステム等の整備費や、行政機関等の既存システム)の改修費用等について、総額2840億円程度を見込んでいる。また、平成27年度から平成31年度における情報提供ネットワークシステ

ム、マイナポータル及び個人情報保護委員会システムの維持・運用等に係る費用については、通信回線等の保守運用経費も含め、総額590億円程度を見込んでいる」

と釈明した（被告第2準備書面、第4、5・23頁）。また、

「機構が運営する自治体中間サーバーを利用する地方公共団体が機構に対し、その運営にかかる費用を負担しており、平成29年度においては、全地方公共団体分の総額は約37億円」

であるとも釈明している（24頁）。

ウ また、マイナンバーカードに関する平成26年度当初予算から平成30年度当初予算までの総務省管轄の予算だけで、総計1562億4000万円が計上されている（平成30年度の当初予算だけで218億6000万円にも上っている）（国会図書館 調査と情報「マイナンバーカードに関する動向」末尾の一覧表参照 甲70）。

エ さらに、中小企業の会社員らが加入する『協会けんぽ』や大企業の『健康保険組合』などが、加入者やその家族のマイナンバーを使って所得確認などをするシステム利用料は、合計で年約100億円にのぼる。それゆえ、「ある健保組合の幹部は『マイナンバーで得られる情報はこれまで通り加入者にじかに求める方が簡単。システムはかえって手間がかかるので使わない』と話す。」などと報じられている（平成29年4月7日付朝日新聞記事・甲71）。

オ 被告は、2018年度（平成30年度）までの6年間で、100億円を超える整備費等をかけて、マイナポータルのサーバを整備したが、その利用率は想定件数の0.02%に留まった。しかも、6年を経過したため、サーバの使用期限が切れて、新たな整備費用をかけてシステムを更新し、来年度から利用しなければならなくなっている（令和元年7月27日付朝日新聞記事・甲72）。

会計検査院の官房審議官だった星野弁護士は、「サーバの利用想定はあまりに現実離れしており、個々のサービスの必要性や費用対効果を厳密に検討したとは思えない。過大な予算が投じられていないか、第三者による検証が必要だ。」と

コメントしている（同）。

カ 以上述べたように、マイナンバーシステムには莫大な税金や民間の資金が使われていることは明らかである。そして、第1、2、(2)、ウで述べたように、民間事業主の負担など、数字で上げられない負担も膨大である。これらに見合うだけの「効果」が具体的に主張立証されない限り、このシステムは、膨大な金喰い虫、いわば「IT箱物行政」といわざるを得ないのであり、「行政の効率化」に資しているなどとは、到底評価し得ない。

(4) 「公正な給付と負担の確保」（目的その3）について

「公正な給付と負担の確保」も原告らの権利制限の理由たりえない

ア 玉蟲教授は、「とりわけ④に示されるように、これらの目的が追求するのが社会権保障の適切な実現であるとするならば、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。」と述べる（甲54・18頁）

（「ただし、これらの目的が一応正当なものであるとしても、後に見るように、目的と手段との均衡という観点からすれば、目的の重要性がプライバシー侵害の程度との関係で否定される可能性があるし、これらの目的が『真に』正当な目的と断言するのはどうか（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」（同上）との限定付きではある）。

イ しかし、原告らが、その準備書面(3)の3頁以下で主張したように、マイナンバー制度を導入しても、「より正確な所得の捕捉」や「真に必要な社会保障の給付」は実現できない。番号制度があれば足りるという問題ではないのである。

そして、その点は、被告自身も、以下のように「非現実的」であるなどと認めているのである。

「(2) 番号制度の限界

一方、そのような制度改革と併せても、全てが完全に実現されるわけではない。例えば、全ての取引や所得を把握し不正申告や不正受給をゼロにする

ことなどは非現実的であり、また、『番号』を利用しても事業所得や海外資産・取引情報の把握には限界があることについて、国民の理解を得ていく必要がある。」(社会保障・税番号大綱―主権者たる国民の視点に立った番号制度の構築―)政府・与党社会保障改革検討本部 2011年6月30日・19頁)。

すなわち、①マイナンバーは国内の取引にのみ適用されるものであり、富裕層が利用することの多い海外での取引は対象外になっているため、マイナンバー制度は役に立たない(もちろん、海外資産も対象外である)。

そして、②マイナンバーでは資産を把握することはできない。平成30年から預貯金口座にマイナンバーの紐付けが開始されたが、それとて極めて低い割合に止まっていることは公知の事実であるし、それ以外の資産はマイナンバーと紐付けされていないものが多い。

さらに、③「事業所得」は、売上げから「経費」を除いたものとなるが、その「経費」に含まれるか否かは自己申告によらざるを得ない。「納税者番号制」を導入しただけでは、事業者の正確な所得捕捉は不可能である。

以上のように、番号制度は極めて限界があるものなのである。

むしろ、「公正な負担と給付の確保」を実現するためには、それ以外の問題の方が大きい。

たとえば、④国内取引に関して言えば、低率の分離課税がなされる取引(例えば、株式の譲渡利益に対する課税は20%)が存する。これは、所得を総合した累進課税になっていないために、「公正な負担」の理念に反する。実際に、年間の申告所得金額が一億円を超えると、急激に所得税の割合は減少しているし、その原因は株式譲渡益に対する低率分離課税が存することが指摘されている(原告ら準備書面(3)末尾添付の所得税負担率の表(甲73・2017年01月06日【政策解説】「民進党税制改革の基本構想」を決定より引用を参照)。

このような税制の重大な“抜け穴”が存するため、例えば、広大な不動産を有し、株の配当所得が数千万円も存するような人であっても、特定口座を利用して源泉分離課税を選択している場合は、申告所得がゼロということもあり得るのである。つ

まり、正確な所得の捕捉に基づく「公平な税負担の実現」は、税制自体の問題が大きいのであり、番号制の問題ではないのである。

⑤さらに、「公正な給付」という観点からは、何よりも、社会保障はつまるところ予算の問題であり、予算がなければ必要としている人に必要な社会保障給付はなされないという問題が存する。しかも、ホームレスで住民登録を抹消されているという、もっとも社会保障給付が必要な人にはマイナンバーがないため（マイナンバーは住民票が存することが前提となる）、それを利用した社会保障給付ができないという深刻な問題点も内包している（長年、生活保護に携わってきた原告原田の本人尋問（原田調書9頁）でもその点が指摘されている）。

また、そもそも、仮に住民票を有していても、日本においては、生活保護水準以下の所得しか無いにもかかわらず、生活保護の対象となっていないという「生活保護世帯の捕捉率」が極めて低いという厳然たる実態も存する（厚生労働省の推計でも研究者の推計でも、捕捉率は、所得だけで判定すると1～2割、資産を考慮しても2～3割にとどまっていると言われる）。

ウ 以上述べたことからだけでも、本マイナンバー制度が、プライバシーに多大な危険性を与えているにもかかわらず、そして、民―民―官の中間に位置する民（事業者等）に、メリット無しに安全管理義務等の極めて重い負担をかけているにもかかわらず（第1、2、②、ウ参照）、制度創設の本来の目的達成のために効果的な方法であるとは、評価し得ないものなのである。

本訴訟において、原告らは具体的に以上に挙げたようなマイナンバー制度の重大な「欠陥」について指摘してきた。しかし、被告はまったく反論できていない。この点は、原告ら準備書面(5)、8～9頁で既に指摘したところである。

エ 更に、原告原田の本人尋問により、福祉の場面においても、マイナンバー制度が上記の目的に役立っていないことが具体的に明らかとなっている。

まず、マイナンバー制度が生活保護の不正受給対策となるかについて、制度導入後から世田谷区福祉事務所で生活保護行政を担当してきた原告原田は、マイナンバーの活用により生活保護不正受給がわかった事案はないと明言する（原田調書9

頁)。

すなわち、福祉事務所では、不正受給対策として、従前から申請者の同意を得て、各銀行の本店や支店に照会書類を郵送して預金口座の照会（財産調査）を行っていた。マイナンバー制度が導入された後も、情報提供ネットワークシステムは各金融機関と自治体（福祉事務所）を接続するシステムではないため、たとえ銀行口座に任意にマイナンバーを付番する制度が始まったとしても、結局、従前通り、申請者の同意書及び照会書を各金融機関に郵送するしかないのである（同10頁）。

また、マイナンバー制度導入前から、戸籍照会の結果判明した旧姓や旧住所も併記して預金口座の照会を行っており、マイナンバーを付記して口座照会したからといって、調査できる範囲は従前とほとんど変わらないのである（同11頁）。

他方、マイナンバー制度により、生活保護の対象となるべき住民に対して保護を実施することができるようになったわけでもない。原告原田が知る限り、制度開始後、真に手を差し伸べるべき住民をマイナンバー制度によって見つけ出して保護を実施した例はない（同8頁）。そもそも生活保護は収入状況だけでその必要性を判断できるわけではなく、資産状況・親族の状況、稼働能力（病気や障害の状況を含む）等を総合的に考慮して判断しているが、マイナンバー制度ではその様な総合考慮ができない（プライバシー保護の観点からこれらの情報を全てネットワーク化することがあってはならないから）のである。

以上からすると、生活保護行政においてマイナンバー制度は無意味であると言わざるを得ない。

(5)小括

以上述べたように、本マイナンバー制度の目的とされる、①国民の利便性の向上、②行政運営の効率化、そして、③公正な給付と負担の確保は、いずれも合理性を欠き、したがって「公共の福祉」を追求するものとはいえない。

よって、目的に正当性は認められず、本マイナンバー制度は違憲であるといわざるを得ない。

第3 目的達成手段としての個人番号の生成・指定・利用の必要性と合理性がないことについて

第2で述べたことからして、本マイナンバー制度の目的自体に正当性がないため、それだけで本制度は違憲である。

以下、念のため、手段の必要性・合理性の点についても述べる。

1 必要性・合理性の要件

- (1) 人権を侵害（制約）する制度の憲法適合性を判断する場合、仮に目的に合理性や正当性が存したとしても、その目的達成の手段に必要性や合理性が存しない場合は、そのような制度は違憲となる。特に、本件のように人権の中でも中核ともいうべきプライバシー権・人格権を侵害する恐れのある場合には、手段の必要性・合理性は厳格に審査されなければならない。
- (2) この点、玉蟲教授も、「番号法によって追求される目的が一部において正当であるとしても、かかる目的の達成のために投入される具体的な手段に必要性・合理性が認められない場合には、個人番号の生成・指定・利用がプライバシー侵害となりうる」（甲54・19頁）と指摘する。

更に、原告ら準備書面(7)で索引情報(インデックス情報)の重要性について述べたように、「統一的な個人番号を用いなければならないかどうかという点で、例えば行政分野ごとに『分野別番号』を用いつつ、プライバシーコミッショナーを通じてそれらを結び付けるような手段では目的が達成できないことを国側が説得力を持って論証しなければならないことはいうまでもない。これが十分に行われぬ限り、個人番号の生成・指定に必要性・合理性が欠けることも考えられる」（同19頁）と、その合理性、すなわち人権制限が必要最小限のものといえるかについての審査の必要性についても指摘する。

2 「共通番号」である個人番号の利用・保存の必要性・合理性について

- (1) 第2で検討したように、個人番号制度の基本的な制度目的は、国民と外国人住民の全員に対し、いわゆる「納税者番号」として機能する個人番号（マイナンバー）

を割り振り、それに基づいて、より正確な所得捕捉をはかった上で、真に必要なとする人に必要な社会保障を提供するという点にある。また、「行政の効率化」という観点からは、マイナンバーとひも付けた個人情報をデータベース化し、中間サーバにそのデータのコピーを保存した上、情報提供ネットワークシステムを通じてそれらのデータを照会に応じて自動応答させて情報連携（データマッチング）できるようにして、それまで基本的に紙ベースで行われていた情報連携をネットワーク化・自動応答化することによる効率化を図ることにある。さらに、「国民の利便性」の観点からは、国民（住民）が各種申請を行う際に、所得証明書等の添付書類を提出しなくても良くなるなどの「利便性」を実現するという点にある。

- (2) 以上のうち、より正確な所得捕捉を図るという「目的」の限りにおいては、「納税者番号」の機能を有する個人番号を割り振り、利用することには、一定の合理性が存するよう見えなくはない(但し、前述のような重大な「抜け穴」があることは前提である)。

しかし、①この「目的」からするならば、「納税者番号」という分野別番号（税分野だけに限定して利用される個人識別番号）を用いれば良いのであり、分野をまたがって共通の個人識別番号を付する必要はない。

しかも、②所得の正確な捕捉に基づき、真に必要なとしている人に必要な社会保障を給付するという「情報連携」（データマッチング）目的を実現するために、マイナンバーシステムの中核ともいえる情報提供ネットワークシステムが作られたが、そこにおいては、（個人番号とひも付けられてはいるものの、）個人番号とは異なる事務ごとに別個の係用番号である「機関別符号」を用いて情報連携が行なわれているのだから、各行政庁において個人番号とひも付いたままの個人データを保有する必要性・合理性はない。

- (3) 原告らは、情報連携には「機関別符号」を用いるのであり、「共通番号」であるマイナンバーは不要である旨何度も主張し、求釈明した(例えば、準備書面(4)、第2、2及び3・5～9頁など)。

しかし、原告らの主張・求釈明にも拘わらず、被告は、その第3準備書面、第

3、3、(3) (17～19頁)等で、情報連携に必要なだから必要なのだ等と、答えて問題を解くかのような、かみ合わない主張を繰り返すのみで、何ら反論し得ていない。

原告ら準備書面(7)で詳述したように、分野を超えた共通の個人識別番号(共通番号)を用いることは、プライバシー情報の名寄せの危険性を飛躍的に高めるものであって、マイナンバー制度の最大の危険性である(この点は争いのない事実である)。

被告が、この核心とも言える点に関して、反論らしい反論を行えないことの一点だけから見ても、共通番号であるマイナンバーを用いた制度を利用する「手段の合理性」に関する合憲性は存しないものといわざるを得ない。

3 情報提供ネットワークシステムを用いて情報連携される事務範囲も、過度に広範に過ぎる

第3、2で述べたように、社会保障給付に際して、所得要件審査を行うという「目的」自体には一定程度の合理性が存するようにも考えられる。

しかし、社会保障の実際の現場においては、個人番号を割り振り、情報提供ネットワークシステムで情報連携をする必要性はない、少なくとも、これほど多額の税金と労力を投じてシステムを整備する必要はなかったと言わざるを得ない。

その点は、原告原田の本人尋問において具体的に明らかになっている(第2、3、(2))。なお、同尋問により、本制度の活用において、むしろ「不正受給対策」が前面に押し出されていること(甲61)は、その合憲性審査において留意されなければならない。

4 データマッチングという手段の必要性と合理性

(1) そもそも、本制度において、情報連携(データマッチング)される分野は、税、社会保障、災害対策の3分野だけといわれているが、税と社会保障分野だけでも十分に広範に過ぎる。この両分野の個人情報と共通番号をひも付けするだけでも、プライバシーに対する危険性は極めて高くなる。

すなわち、原告ら準備書面(7)で詳述したように、現代社会におけるプライバシー保障の一つの核心は、名寄せ・データマッチングの防止にある。したがって、

仮に社会保障給付のための所得審査などのためにデータマッチングが必要な場面があるとしても、それは最小限の範囲に止めるようにしなければならないし、ボタン一つで自動的にデータマッチングされるようなシステム構築は避けるようにしなければならない(後述第2章第4の、プライバシー・バイ・デザインを実現するためのプライバシー・インパクト・アセスメント(プライバシー影響評価)の必要性について参照)。

税や社会保障分野の個人情報、その一つ一つがきわめて機微性の高いものであるから、それを名寄せ・データマッチングがし易い共通番号付きのデータベース化し、データマッチングできるコンピュータ・ネットワークシステムを構築することに対しては、最低限、厳格なプライバシーへの影響評価と、影響を最小限にするための審査が必要となる。

- (2) この観点から、番号法別表第2で情報連携が認められている事務分野をしてみるならば、効率化の観点を優先して、共通番号をつけて情報連携できるものは、すべて情報連携しようという方針であり、プライバシー保障を軽視しているといわざるを得ない。これは、個人番号付きのデータベースが、過度に作られて過ぎていることを意味する。

このようなデータベースが構築され、ネットワーク化されたならば、原告らを含む国民のプライバシー情報(しかも、その一つ一つの内容がかなり機微なものである)を過度にデータマッチングすることを許容するものであって、原告らのプライバシー権、すなわち、情報主体である本人の同意が存しないところで収集・保存・利用(データマッチングを含む)・提供されない権利としての自己情報コントロール権を過度に侵害するものである。

この点について、玉蟲教授も、

「少なくとも別表第2を見る限り、データマッチングされる個人情報が『社会保障制度、税制、災害対策』の分野における行政運営の効率化・迅速化、公平な給付と負担の実現にとって必要不可欠な範囲に限定されているかは相当程度疑わしい。むしろ、これらの目的の実現にとってかかわりがあると思われる情報を広

く情報提供の対象として挙げているという印象を強く受ける」(20頁)。
と指摘しているところである。

5 安全性も確保されていない

原告らは、この間、違法な再委託問題等の具体例を挙げて、広範な事務に個人番号を利用することに伴って、そのデータ作成や発送事務等においてデータが、本来許された範囲外に「漏洩」している事実を指摘した。

また、個人番号と紐づけられた個人情報のデータベースが数多く構築されることに伴って、それらの情報の「のぞき見」や大量流出の危険性、そして、流出等した個人番号を用いた名寄せ・データマッチングの危険性が高まる結果となることも指摘した。年金事務分野などで利用が開始されれば、その恐れは極めて高くなると言わざるを得ない。

この観点からも、原告らを含む全国民・外国人住民のプライバシーへの危険性が高まるものである。

6 小括

以上より、個人番号付きデータベースが作られ過ぎていること、そして、分野別番号で情報連携できるならば、共通番号を利用したり、保存しなくても良いのに利用したりしていること等の点から、本マイナンバー制度はプライバシーに対する過度の侵害を内包するものであるから、本制度は、手段の点においても違憲と言わざるを得ない。

7 本来の3分野以外にも特定個人情報が提供等されていることについて

番号法19条14号は、税・社会保障・災害対策の3分野以外にも、「刑事事件の捜査のため」必要な場合や「その他政令で定める公益上の必要があるとき」には、個人番号の収集等を認める。

このような「例外」は、番号法における重大な欠陥であり、原告らを含む国民・外国人住民のプライバシーを侵害するものであるので、項を改めて、第4として別途詳細に論じる。

第4 番号法上、法の目的と関連性のない個人番号の利用が許容されており、手段の必要性・合理性を欠くこと

1 特定個人情報の利用（提供、収集、保管）に関する番号法の定め

番号法は、19条本文で特定個人情報の提供を原則禁止し、その例外を1号から16号まで列挙して提供可能な場合を限定している。

このように特定個人情報の提供が原則禁止されるのは、「特定個人情報は個人番号を含むものであり」「より厳格に第三者提供を制限しなければ、不正なデータマッチングが行われる蓋然性が高い」ためであるとされる（宇賀克也『番号法の逐条解説 [第2版]』（有斐閣、2016年）107頁）。

そして、番号法20条は、19条各号の場合を除いて特定個人情報の収集、保管を禁止し、収集・保管についても提供と同様の規律を定める。

しかし、番号法19条は以下に述べるように極めて広範な例外を定めており、番号法の目的とはおよそ関連性のない特定個人情報の利用（提供、収集、保管）を許容する定めとなっている。以下、①番号法19条14号の「刑事事件の捜査」における利用、②番号法19条14号の「その他政令で定める公益上の必要があるとき」における利用、③番号法19条16号の「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」における利用の順で論ずる。

2 番号法19条14号の「刑事事件の捜査」における利用

(1) 番号法の定め

ア 番号法19条14号は、以下の場合に特定個人情報の提供が許されるとする。

「各議院若しくは各議院の委員会若しくは参議院の調査会が国会法（昭和二十二年法律第七十九号）第百四条第一項（同法第五十四条の四第一項において準用する場合を含む。）若しくは議院における証人の宣誓及び証言等に関する法律（昭和二十二年法律第二百二十五号）第一条の規定により行う審査若しくは調査、訴訟手続その他の裁判所における手続、裁判の執行、刑事事件の捜査、租税に関する法律の規定に基づく犯則事件の調査又は会計検査院の検査（第三十六条において「各議院審査等」という。）が行われるとき、その他政令で定める

公益上の必要があるとき。」（下線引用者）

イ 番号法9条5項は次のように定め、同法19条14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。

「前各項に定めるもののほか、第十九条第十二号から第十六号までのいずれかに該当して特定個人情報の提供を受けた者は、その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ができる。」

ウ そして、番号法36条は、「前三条の規定（引用者注：個人情報保護委員会の監督権限を定めた規定）は、各議院審査等が行われる場合又は第十九条第十四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おける特定個人情報の提供及び提供を受け、又は取得した特定個人情報の取扱いについては、適用しない」と定め、刑事事件の捜査における特定個人情報の利用に個人情報保護委員会の監督が及ばないとする（下線引用者）。

エ また、19条14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、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（番号法23条）。

（2）被告の主張の変遷と現在の見解

原告ら準備書面（6）で詳述したように、刑事事件捜査における個人番号利用について、被告は当初の「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」（被告第2準備書面21～22頁）という見解を変遷させ、現在では、

「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)。(被告第3準備書面9～10頁)と主張する。

上記見解の括弧書きから明らかなように、被告の主張は、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。

(3) 刑事事件の捜査における利用と番号法の目的には関連性がなく、手段の必要性・合理性を欠いている

ア このように、番号法は「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」ことを許容するものであるが、このような個人番号の利用と、番号法の目的である「行政運営の効率化」「公正な給付と負担の確保」「国民の利便性の向上」との間に関連性を見出すことは困難であり、番号法の目的外の利用というべきである。「公正な給付と負担の確保」「国民の利便性の向上」は刑事事件の捜査とはおよそ関連性のないものであるし、「行政運営の効率化」についても準司法手続きである刑事事件捜査の効率化を行政運営の効率化と読み替えることは困難である。前記のように国の当初の主張は、刑事事件の捜査に「そもそも個人番号の利用ができない」というものであったが、この事実は番号法の目的と刑事事件における利用の関連性のなさを物語るものというべきであろう。

イ また、仮に何らかの関連性があるとしても、前記のように合憲性判断にあたっては、目的達成のための具体的な手段が目的達成にとって必要かつ合理的といえるかが厳格に問われる必要がある。刑事事件の捜査の効率化は様々な手段で図ることができるものである一方、上記の利用は捜査機関によるデータマッチングそのものであり(しかも前記のように番号法20条で収集、保管も可能となる)、プライバシーへの強い介入となるものであるから、上記の利用は目的達成にとって必要かつ合理的とはいえないというべきである。

なお、警察による個人情報のデータベース化に関し、山本龍彦教授は、「警察による個人情報の長期的かつ大規模な集積・統合、すなわちデータベース化を『強制処分』と捉え、これに法律上の根拠を“serious”に求めようとする前記見解は、きわめて妥当のように思われる。無論、こうした見解を前提とすると、法律に基づか

ない現状の指紋データベースやDNA型データベース等は、まさにこの点において違憲ということになる」と指摘しており（甲48・252頁）、個人番号を内容に含むデータベース化も、この観点から審査されなければならない。

（4）捜査機関による濫用を防ぐ手段がないこと

加えて、前記のように刑事事件の捜査における特定個人情報の利用には個人情報保護委員会の監督が及ばない（番号法36条）のであるから、捜査機関における濫用を防ぐ手段がない。さらに、前記のように刑事事件の捜査における提供は、情報提供記録を保管する必要はなく、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（番号法23条）ことから個人が自己の情報の違法な提供を知ることは極めて困難である。

この点、玉蟲教授も、「番号法19条14号『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る。」「同条同号（引用者注：19条14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・合理性を満たさず違憲である」と指摘している（甲54・24頁）。

（5）小括

以上のとおり、刑事事件の捜査における利用と番号法の目的には関連性がなく、手段の必要性・合理性を欠いており、番号法19条14号は憲法13条に反し違憲である。

3 番号法19条14号の「その他政令で定める公益上の必要があるとき」における利用

（1）番号法の定め

ア 前記のように番号法19条14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。

イ そして、番号法施行令26条は、「法第十九条第十四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（乙30・14頁）、同施行令別表は1から26までの場合に提供が認められるとしている（乙30・30～33頁）。

ウ また、前記のように、番号法9条5項は同法19条14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。

エ 番号法36条は、「第十九条第十四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。

オ これを受けて、番号法施行令34条は、同施行令別表1から26号までのうち、以下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（乙30・19頁）。

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23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24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）

カ また、19条14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、情報提供記録を保管する必要はなく、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（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) 番号法19条14号の規定は極めて広範に個人番号の利用を可能とするものである

前記のように番号法19条14号は「その他政令で定める公益上の必要があるとき」にも特定個人情報の利用（提供、収集、保管）を可能とする。このような抽象的な規定で、政令による特定個人情報の利用の原則禁止の例外を認めることは、行政機関に、番号法の目的と関連性のない極めて広範な個人番号の利用を認めることになる。

この点、玉蟲教授も、

「同様のこと（引用者注：番号法19条14号が違憲であること）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条及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」（甲54・24頁）と指摘している。

(3) 実際に番号法の目的と関連性のない極めて広範な個人番号の利用が政令によって定められており、かつその相当数の手続に個人情報保護委員会の監督が及ばないとされている

ア 前記のように、番号法施行令は、「政令で定める公益上の必要があるとき」に該当するものとして26の利用の例外を定めている。

それらを概観するだけでも、破壊活動防止法による処分の請求、審査、調査等（同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、国際捜査共助等に関する法律による共助等（同11号）といった外国の刑事事件への協力、少年法による調査（同7号）など多岐にわたる手続に個人番号を利用することができるかとされている。

イ 加えて、前記のように、番号法施行令34条により、同施行令で規定される26の手続のうち、13の手続について個人情報保護委員会の監督が及ばないとされている。

ウ 具体的にどのような手続に個人番号の利用が認められているかみていくと、例えば、番号法施行令別表9号では「破壊活動防止法」「27条による調査」の場合に個人番号の利用が許されるとしている。この「調査」とは公安調査官による調査のことであり、破壊活動防止法27条で「公安調査官は、この法律による規制に関し、第三条に規定する基準の範囲内において、必要な調査をすることができる」と定められている調査のことである。そして、この調査には個人情報保護委員会の監督は及ばない（番号法施行令34条）。番号法はこのような調査に個人番号を利用（提供、収集、保管）することを許容しているのである。

(4) 小括

番号法施行令26条が規定する26の手続のうち、少なくとも公安調査（番号法施行令別表9号、17号）、刑事事件捜査、外国犯罪の共助等（同別表（7号、11号、12号、13号、15号、16号、17号）といった手続に個人番号を利用することは番号法の目的と関連性がなく、目的外の利用というべきであ

る。また、仮に何らかの関連性があるとしても、刑事事件捜査と同様、このような手続に個人番号を利用することは、目的達成にとって必要かつ合理的とはいえないというべきである。

さらには、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、かつ前記のように多くの手続で個人情報保護委員会の監督も及ばないとされているのである。また、マイナポータルによって自己の個人番号（特定個人情報）の利用を確認できないことも刑事事件捜査と同様である。

以上より、政令によってこのように極めて広範に個人番号の利用を認める番号法19条14号の規定は、手段の必要性・合理性を欠いており、憲法13条に反し違憲である。

なお、實原教授の意見書（甲55・12頁以下）で述べられているように、番号法19条14号の「その他政令で定める公益上の必要があるとき」という規定は、白紙委任を認めたものであり、憲法41条にも違反するというべきである。

4 番号法19条16号の「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」における利用

(1) 極めて広範に個人番号の利用を可能とする

番号法19条16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14号と同様、番号法の目的と関連性のない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) 監視機関が利用範囲を策定するという問題

さらに、番号法19条16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33条以下）個人情報保護委員会が、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

以上より、個人情報保護委員会規則により、極めて広範に個人番号の利用を認める番号法19条16号の規定は、手段の必要性・合理性を欠いており、憲法13条に反し違憲である。

なお、番号法19条16条の規定も白紙委任を認めたものであり、憲法41条にも違反するというべきである。

5 小括～番号法19条14号、16号は法の欠陥である

以上のように、番号法は、同法19条20条は、特定個人情報の提供、収集、保管を原則禁止としながら、同法19条14号16号により、極めて広範な例外を許容している。これにより、「行政運営の効率化」「公正な給付と負担の確保」「国民の利便性の向上」という番号法の目的外の、あるいは著しく関連性の乏しい目的で個人番号を利用することが可能となっている。また利用の範囲の点でも、社会保障制度、税

制、災害対策といった分野と無関係に個人番号を利用することが可能となっている（番号法9条5項）。

しかも、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いない。具体的に述べると、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のである。そればかりか番号法19条14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、あえて規制を緩めているのである。このような番号法19条14号16号の規定は、法の欠陥というべきである。

第5 個人番号カードの合憲性審査

1 個人番号カードの特徴等

マイナンバー制度の重要な柱の一つに個人番号カード（「マイナンバーカード」）が存する。

同カードは、券面に、氏名、住所、生年月日、性別の4情報及び顔写真が記載され、裏面に個人番号が記載される。さらに、ICチップが搭載され、（ネットワークに接続したコンピュータ及びカードリーダーを用いれば）公的個人認証を利用できるようになっている。また、市区町村が対応していれば、コンビニにおける住民票の取得なども可能となる。

2 個人番号カードの事実上の所持強制施策

(1) 被告は、国民と外国人住民全員に個人番号カード（マイナンバーカード）を取得させ、常時携帯させることにより「利便性の高い社会」の実現を目指している。

マイナンバーカードを全国民・外国人住民に持たせ、カードを普及させるための多額の予算措置もとっている。

(2) 令和元年6月4日開催のデジタル・ガバメント閣僚会議において、「マイナンバーカードの普及とマイナンバーの利活用の促進に関する方針」（甲74）が決定された。

さらに、それに基づき、同月21日、「経済財政運営と改革の基本方針2019～『令和』新時代：『Society 5.0』への挑戦～」(いわゆる「骨太方針2019」)が、閣議決定された(甲75)。

後者の基本方針の中では、「第2章 Society5.0時代にふさわしい仕組みづくり」の柱の一つとして、「⑤ スマート公共サービス (i) マイナンバーカードを活用した新たな国民生活・経済政策インフラの構築」が挙げられており、「2022年度中にほとんどの住民がマイナンバーカードを保有していることを想定し、国は市町村ごとのマイナンバーカードの交付円滑化計画の策定の推進と定期的なフォローアップを行うとともに必要な支援を行うなど、マイナンバーカードの普及を強力に推進する。」との方針が掲げられている(12頁)。

(3) そして、国民全員が所持することを前提として、令和4年(2022年)度までのスケジュールとして、以下のような政策を進めようとしている(甲74、75)

ア 健康保険証との一体化による事実上の所持強制

被告は、令和3年(2021年)3月から、マイナンバーカードの公的個人認証機能を利用して、健康保険の被保険者資格の確認をインターネット経由のオンラインで行える仕組み(以下、「マイナンバーカードの健康保険証との一体化」という。)を進めている。

健康保険証は、医療機関で医療行為を受ける際、医療機関に示せば治療費の支払いが原則3割で済むものである。定期的な通院や急な事故によるけがなどのために、医療機関における治療に備えて、多くの国民は日常的に携帯している。

マイナンバーカードには、上記で挙げたように券面に機微性の高い情報が記載されているし、マイナポータル等での不正利用の恐れもある。紛失などの事故は、原告ら準備書面(4)で述べたように、今後も多発するおそれが高い。

付け加えるならば、被告は、全国の医療機関などが対応できるよう医療機関などの読み取り端末、システム等の早期整備を十分に支援するとしている。医療機関側にも健康保険証と一体化したマイナンバーカードの扱いを事実上強いられる

のである。大学病院など予算や設備が比較的十分な医療機関はともかくとして、規模の小さな診療所などにおいて、健康保険証と一体化したマイナンバーカードをどのように扱うのか、個人番号の漏洩などを防止する設備や体制を整備することが大きな負担となることは想像に難くない。

さらに、被告は、イで述べるようなポイント付与のメリットを、健康保険証としてマイナンバーカードを使えるようにした人に与えることを検討しており、年内に詰めるとしている（甲78・日経新聞の記事）。買い物の際のポイント付与などの特典というマイナンバーカード取得の動機付けを増やし、カード取得を促進しているのである。

イ 消費活性化策

被告は、令和2年度（2020年度）に実施するマイナンバーカードを利用した自治体ポイントによる消費活性化策について、利便性が高く将来のポイント利用の拡張性も担保したシステム基盤を目指し、マイナンバーカードの普及につなげることを計画している。

マイナンバーカードを携帯し、自治体においてポイントが付与され、消費活動の際に、ポイント利用をして、消費活動につなげることによるマイナンバーカードの普及が狙いと解釈できるが、これもプライバシー侵害のおそれが非常に高い。何故なら、一種のポイントカードとしてマイナンバーカードを利用することになれば、消費者は常にポイントカードたるマイナンバーカードを携帯することにならざるを得ず、紛失等の危険性が高まるからである。

ウ デジタルキャンパスの推進

被告は、デジタルキャンパス推進による大学におけるデジタル化の推進、マイナンバーカードの教員免許管理等への活用、をマイナンバーカード普及施策として挙げている。デジタル化として、まず第一に挙げられるのが、学生証とマイナンバーカードを一体化させることである

大学の学生にとって、身分証たる学生証は常に携帯するものである。いくつかの商業施設、飲食店などにおいて学生割引などの実施もしており、大学生は学生

証を常時携帯している。しかし、学生証の紛失の事例はあらゆる大学で発生しており、常時携帯させれば、マイナンバーカードの紛失等の危険性も高まらざるを得ない。

エ 公務員等においては、すでにマイナンバーカードの取得の促進が図られているが、被告は、地方公務員等のマイナンバーカードの一斉取得推進として、地方公務員の共済組合員についてマイナンバー取得を要請する方針を打ち出している。

本来マイナンバーカードの取得は任意であり、取得するか否かは個人の自由であったにも拘わらず、公務員という身分関係を利用することにより、反対の声を出しづらくするなどして、事実上、政府により所持を強制されるかのような方針が出されている。

現在、各公務員に対し、マイナンバーカードをすでに申請したか、申請していないのであれば、すぐに申請するようというアンケートの実施などもされており、公務員においては事実上の所持強制が行われていると言わざるを得ない。

また、共済組合から公務員に対し、マイナンバーカード申請書の配布や回収、取得状況の調査をし、事実上公務員がマイナンバーカードの申請を拒否できないような状況を作り上げている（甲77・東京新聞）。

オ 各種カード、手帳等との一体化

上記のほかに、被告は、お薬手帳とマイナンバーカードの一体化、ハローワークカード、ジョブカード、教員免状、運転経歴証明書、障害者手帳などとのマイナンバーカードとの一体化を方針として挙げている。

上記の各種カード、手帳も、携帯するものであるから紛失などにつながり、それによるプライバシー侵害の危険は高まると言わざるを得ない。

(4) 小括

上述したように、被告は、マイナンバーカードの普及を図り、そのために、あらゆる場面でマイナンバーカードを携帯していなければ、一定のサービスが受けら

れないということが生じてくるような施策を進めている。また、事業所や大学からマイナンバーカードと一体化した健康保険証や学生証を交付されることとなり、事実上拒否することが難しい状況に陥らせられている。さらに、お薬手帳や障害者手帳など、比較的安全管理能力に欠ける人々が携行する機会が多い手帳をカードと一体化する施策を推進することにより、マイナンバーカードの紛失や不正利用、マイナンバーの流出等の危険度が高まっている。

このような施策は、プライバシー侵害の恐れが非常に高い行為を事実上強いるものであり、国家による国民の権利侵害と言わざるを得ない。

3 目的達成手段に必要性・相当性が存しないことについて

(1) 被告は、前述の3つの目的達成を図るために個人番号カードがあり、また、このカード一枚で個人番号の確認と本人確認ができる、上述のコンビニにおける住民票の取得なども可能となるなどの利便性を享受できると主張する。そして、そのために2で挙げたような諸施策を強力に押し進めている。

しかし、まさにこのカード一枚で色々なことができるということ、そして、所持の事実上の強制が、かえって原告ら国民・外国人住民のカード利用者のプライバシーを侵害するものとなっているのである。

(2) 番号確認と本人確認を1枚のカードで行う必要はない(理由1)

個人番号は秘密にしておくべき情報である(番号法12条、15条等)。秘密にしておくべき個人番号をカードの券面に記載し、しかも、それを常時携帯することを事実上強制することは、2で述べたように、カードの紛失や個人番号の覗き見等のリスクが高まり、極めて危険である。

安全性を考えるなら、印鑑登録カードのように氏名・住所等すら記載されていない、カードを特定する番号だけが記載されたカードにICチップを入れたりする対策が考えられる。カードを安全に管理できない人やカード紛失のリスクが存することを前提に制度設計するならば、このような安全策を採ることが必要である。その上で、利便性を追求する人が便利に使えるように、スマートフォンのICチップの活用等を図るべきなのであって、全ての人にこの一種類のカードを持た

せること、そして日常的に携帯しなければ不便になるようにして、日常的な携帯を事実上強制するような施策は、紛失や一時的な盗用、個人番号の盗み見等の危険性を極大化させるものであって、プライバシーに対する重大な侵害である。

しかも、被告は個人番号カードのＩＣチップに搭載された公的個人認証の利活用をはかっているが、すべて公的個人認証を活用したアプリケーションにする必要はない。公的個人認証を活用して、厳格な個人認証を行う必要がある場面もあるであろうが、ＩＤとパスワードだけで済むような場面にまで公的個人認証を用いるのは、同制度の利用料を考えると無駄である上に、後述のように、公的個人認証の利用履歴がＪ－ＬＩＳ（地方公共団体情報システム機構・住民基本台帳ネットワークシステムや情報提供ネットワークシステム、公的個人認証等の全国センター）に一元的に管理される問題もあるからである。

少なくとも、カードの券面に個人番号が記載されている必要はないのであって、例えばパスワードつきでＩＣチップに記録するなどの対策をとれば、少なくとも、カードを見ただけで個人番号を盗み見されるリスクは解消できるのであり、そのような対策すらとっていない個人番号カードの制度設計は極めて安全性軽視であると言わなければならない。

(3) カード券面に「性別」記載の必要はなく、むしろ記載すべきではない（理由 2）

ア 被告は、「求釈明に対する回答書（2）」（平成29年1月24日付）の第4、3において、「第180回通常国会に提出した法律案においては、性別は個人番号カードの券面記載事項とされていなかったが、・・・身元を確認するために基本的には4情報（氏名、出生の年月日、男女の別及び住所）の記載が必要であることから、性別についても個人番号カードの券面記載事項として現行の番号利用法に規定したものである。なお、個人番号カードは、健康保険証としても利用することを検討しているが、医療の現場等においては、性別の確認を行う場面もあることから、その意味でも性別を個人番号カードの券面に記載する必要があるものと考えられる」と釈明する（25頁）。

イ しかし、不必要である。

何故なら、①現在最も確実な本人確認書類として利用されている運転免許証には性別記載はない。本人の外見からは性別は不明の場合もあるから、外見から推定できる性別とカード券面に記載された「性別」との不一致により、かえって本人確認ができなくなる恐れすら存する。

また、②保険証としての利用は、公的個人認証により、インターネット経由で、被保険者の資格確認を行うものであり、そこにおいて「戸籍上の性別」を確認するようにすることも可能である。

番号法の制定当時、既に「性同一性障害」の問題が広く知られていたにもかかわらず、それゆえに上記第180回通常国会に提出された法案では「性別」記載が除かれていたにもかかわらず、あえて「性別」を券面記載事項にしたことの人権侵害性は明らかである。

ウ 原告の性同一性障害者にとって、性別の記載が、その平穏な生活を送る上で様々な心配を引き起こすなど、その精神的苦痛は計り知れない。

その点は、甲46の陳述書によって、具体的に明らかにされている。

(4) なりすましの危険性を増大させる（理由3）

(1) で述べたように、国民・外国人住民の中にはカードの安全管理を行う能力がない人が一定割合存する。また、その能力がある人でも、一定割合で紛失、遺失等の危険性が存する。その場合、カードが拾得されたり、一時借用されたりした上、マイナポータル等でなりすましをされる危険性がある。マイナポータルでは、カード所持者の各種情報を見ることができただけでなく、各種の手続き等を行うことができる（今後ますますできるようになる範囲は広げられることが予定されている）。

したがって、カードを拾得した者や、高齢者などからカードを一時的に預かる等した者が、パスワードさえ分かれば、そのカード名義人になりすまして、各種個人情報の覗き見や各種手続きを行ってしまう可能性がある。自治体ポイント等のポイントを使われてしまうという被害にあう可能性も存する。ネットワーク上のなりすましの場合は、現実社会におけるなりすましに比べて、なりすましを見

破り、被害を防止することは非常に困難である。

被告の主張する“一枚で全て行える”という「利便性」が存するという事は、それを悪用される場合の危険性も、一枚で全て行われてしまうというものになってしまうわけであり、安全管理思想に反する。

個人番号カードのなりすまし対策は極めて不十分である。

(5) 公的個人認証の利用による J-Lis の情報一元管理（理由 4）

ア 原告ら準備書面（4）、第2、「8 J-LISへの情報集中という「不備」」で述べたように、J-LIS（地方公共団体情報システム機構）は、全国民及び外国人住民の本人確認情報や個人番号カードの情報（顔写真情報を含む）などのデータベースを保有している上に、公的個人認証の認証事務も行っているから、公的個人認証の利用履歴（少なくとも、いつ、どこで、公的個人認証を使ったかの情報）が蓄積されることになる。

イ 全国民と外国人住民の、公的な（＝自己申告ではない、住民票上の）本人確認情報と個人番号と住民票コードを、それらの変更履歴と共に、漏れなく保有していること、さらに、事実上所持が強制される個人番号カードの情報である「顔写真」情報も保有することになることから、J-LISはかつて存在したことの無い巨大な本人確認情報データベースを一元管理する機関となっている。

そのデータベースを保有する上に、公的個人認証の利用履歴情報まで保有することになるのである。

ウ 個人情報を一つの機関が管理すること（一元管理）は、プライバシーの保障上避けるべきである。この点は、被告も、安全対策として、マイナンバー制度における個人情報は「一元管理ではなく、分散管理されている」旨主張していることから、争いのない事実である。

その観点から考えると、上記のような J-LIS の保有する個人情報のデータベースは、それだけでもあまりに巨大なものであり、かつ、極めて価値の高いものである。同機構は、個人番号カード発行システムの不具合を引き起こすなど、そのシステム管理能力において、問題を起こした組織でもあり、このような機構に上述

の個人情報が一元的に管理されている状況は、原告らを含む全国民・外国人住民のプライバシーに高い危険性をもたらすものといわざるを得ない。

4 小括

以上指摘してきた点から、個人番号カードの制度設計、及び、同カードを事実上日常的に携帯することを強制する被告の施策は、原告らを含む全国民・外国人住民のプライバシーと、性同一性障害者の人格権（や平穏に暮らす権利）を著しく侵害するものであって、違憲といわざるを得ない。

第2章 住基ネット最高裁判決に基づく「構造審査」基準による合憲性審査

第1 構造審査基準

原告ら準備書面（7）で述べたように、マイナンバー制度に「システム技術上または法制度上の不備があり、そのために特定個人情報が法令上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、収集・保管・利用または第三者に開示または公表される具体的な危険が生じている」場合には、憲法13条で保障されたプライバシー権や人格権が侵害され、違憲となるというべきである。

これは、平成20年住基ネット最高裁判決が「構造審査」を採用していることに基づき、マイナンバー制度の合憲性審査にも「構造審査基準」が妥当することを主張するものである。具体的には、「システム技術上または法制度上の不備」につき、①システムの安全性が確保されているか、②罰則等による違法行為の厳格な禁止が実効的になされているか、③監督機関の設置等により、実効的に監視監督がなされているか、という観点から審査がされるべきである。

第2 マイナンバー制度の特質

システム技術上または法制度上の不備を個別に論ずる前に、今一度、マイナンバー制度が有する次のような特質を改めて確認する必要がある。

第1に、マイナンバーが共通番号であるという点である。事務分野を超えて同一の個人識別番号を用いる「共通番号」は、容易・確実に個人情報の名寄せ突合（データ

マッチング)を可能とする。この特性により、共通番号のついた個人情報、①複数分野にまたがるデータの効率的な処理(例えば、ビッグデータの処理)が可能となるから、厳格な統制の下にデータの利活用を進めないと、本人も気が付いていない個人の傾向や特性があぶりだされたり、類型化されたり、本人の同意なく個人像が作られたりする(プロファイリング)などのプライバシーや人格的自律に重大な影響を与えかねないデータ処理が行われる可能性が高い。また、②共通番号付の個人データは利用価値が高いため、不正入手のインセンティブが高く、したがって漏洩の危険性が高い上に、③一旦データが漏洩等した場合の被害に関しても、複数の漏洩データの名寄せ突合が容易確実にできるから、その被害も「分野別番号制」における漏洩よりもはるかに深刻なものとなる。このような共通番号の危険性は、被告も平成28年10月4日付け求釈明に対する回答書において、「飽くまで抽象的な一般論として」と限定をつけながらであるが認めるところである。

第2に、マイナンバーは、民間部門での利用も前提としたものであるという点である。そのため上記「不備」を審査するにあたっては、個人番号の利用範囲全体における危険性を検討しなければならない。この点について、番号法では、違反者に対する罰則こそ規定されているものの、全ての事業者が個人情報の管理について高いリテラシーや資源を有しているわけではないことはいままでもないし、今日、大企業においてさえ個人情報の流出は枚挙に暇がなく、また、事業者から流出した顧客名簿の売買が現実に行われていることも、周知の事実である。

以下、これを前提にシステム技術上の不備、法制度上の不備について論ずる。

第3 システム技術上・法制度上の不備

1 情報提供ネットワークシステムにおける情報連携にマイナンバーを用いないとしながら共通番号制を採るという「不備」

(1) 情報提供ネットワークシステムとは

番号法上、情報連携を行うに際し、情報照会者及び情報提供者は、直接に情報提供のやりとりを行うのではなく、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)。同システムで情報連携可能な事務は1800以上あ

り、同システムは、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には個人番号は使われない

マイナンバー制度では共通番号が採られていることから、各省庁等のデータベースには、個人情報と共通番号たるマイナンバーと一緒に保存されている（個人情報とマイナンバーのひも付け）。

ところが、情報提供ネットワークシステムにおける情報連携には、マイナンバーは使われず、機関別符号が使われる（乙1・8頁の図）。この機関別符号（情報提供用個人識別符号）の生成には、マイナンバーは使用されない（番号法施行令20条6項、2016（平成28）年11月15日付け求積明書参考資料2の1-1、平成29年1月24日付け求積明に対する回答書（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マイナンバーは不要ということになる。

(3) 小括

そうすると、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マイナンバーを保存せずに情報連携を行うという、プライバシー権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。したがって、個人情報と一緒にマイナンバーを保存するという手段を採ることが「システム技術上または法制度上の不備」にあたることは明白であるというべきである。

2 民間も含め漏洩等の事故が発生する前提での安全性の構築がされていないという「不備」

- (1) 前記のように、マイナンバー制度は、民一民一官でマイナンバーの利用が大規模に行われる制度（システム）である。民からすれば、マイナンバーの利用を強制される制度(システム)である。よって、マイナンバーを利用・管理する民間を含めたシステム全体について、欠陥（不備）がないかを調査し、対策しなければならない。

- (2) ところが、前述のとおり、民－民－官の中間の民（雇用主など）にとっては、全くのメリットがないのに重い安全管理義務が課されている。マイナンバー制度の「メリット」があるのは官のみである。これでは、民間、特にセキュリティ対策に資金と人材を投入する余裕のない中小零細企業などにおいて、セキュリティを高めるインセンティブはなく、セキュリティレベルが高位で平準化されることが困難という、当然の問題が発生する。
- (3) そうであるならば、民にこのような義務を課す以上、国には、容易かつ安価にセキュリティを高めやすい制度的・システム的な工夫をする義務、仮に情報が漏洩したとしても被害がなるべく少なくなるようにする制度的・システム的な工夫をしておく義務があるというべきである。

この点、国自身が既に「事故前提社会」として安全対策をとらなければならないという姿勢に転換している。

すなわち、日本の情報セキュリティの総元締めである内閣サイバーセキュリティセンター（NISC）の前身である内閣官房情報セキュリティセンターは、2009年（平成21年）に、情報セキュリティに関して、「事故前提社会」、すなわち、情報流出などの事故は必ず起きるものであることを前提に安全対策をとらなければならない、という考え方を採用しなければならないと強調するようになっているのである（「第2次情報セキュリティ基本計画」（同年2月3日付））。

- (4) にもかかわらず、マイナンバー制度は、そのような発想で制度設計されていない。そのことは、例えば、原告が住民税の特別徴収通知の誤配送の事実を指摘したのに対し、被告が「仮に特別徴収税額通知を送付することにより情報漏洩の危険などの問題が生じるとしても、それは番号制度そのものとは別次元の人為的ミスなどを原因とするものであり、仮に同通知の送付について問題があるとしても、それによって必然的に番号制度自体が問題のあるものとはいえない」などと主張している（被告第2準備書面18頁）ことから裏付けられる。

(5) 以上より、このような事故前提の安全対策をとっていないという基本的な「不備」がマイナンバー制度（システム）には存する。なお、実際に特別徴収通知の誤配送や特定個人情報漏洩等が生じていることは原告ら準備書面（3）（4）で述べたとおりである。

3 番号法19条14号、16号により番号法の目的と関連性のない極めて広範な利用が許容されている「不備」

この不備は、前記第1章、第4で主張したとおり、極めて大きな法の欠陥である。

4 プロファイリング（データマッチング）の防止措置がない「不備」

前記のように、共通番号制度の最大の問題は、データマッチングとプロファイリングである。

いったんマイナンバーとひも付けされたデータベースが作られたら、将来それを用いたプロファイリングをされる危険性が高いにもかかわらず、日本においてはそれを防止する憲法的な原則や、それを規制する法的規制等が存しないという「不備」が存する。

前記のように、番号法19条14号16号によって、政令等により極めて広範な分野で特定個人情報の提供、収集、保管が許容されており、現に政令等によって極めて広範な利用がすでに可能とされている。加えて、政府の戦略によりその利活用が促進されているから、今後もデータベースはどしどし作られてゆくことが想定される。現在の国家戦略からするならば、将来的には、健診データ、レセプトデータ、カルテデータ、はてはゲノムデータとの（医療等IDを媒介にした）ひも付けも想定されるのである。

したがって、よほど十分かつ慎重な議論をして、倫理面も含めて十分なコンセンサスを得た原則や基準を作ったうえで進めないと、取り返しのつかない事態を招来する危険性が高い。なお、国家安全保障的にも重大な危険性があり、もしも、「情報テロ」などにより大量に奪取された場合には、その一部として原告らの個人データ(特定個人情報)も奪取される危険性が存する。エドワード・スノーデン

氏の暴露で明らかになったように、NSAに所属したハッカー程度の能力があれば、特定個人情報の大量奪取は可能である。

マイナンバー制度には、このようなデータマッチング・プロファイリングに対する規制等がないという「不備」がある。

5 個人番号カードの券面にマイナンバー及び性別等の記載をし、そのカードの利活用を図って、持ち歩かせるようにしている「不備」

この不備は、前記第1章、第5で主張したとおり、マイナンバーの漏えいの危険性を高くし、性同一性障害者の人格権（や平穩に暮らす権利）を著しく侵害し、また、なりすましの危険性も高くするものであるなど、大きな制度的「不備」である。

6 行政のシステムにおいて、既存住基システムからマイナンバーシステムまで全部（物理的には）ネットワークでつながっているという不備

(1) マイナンバーのシステムは、「マイナンバー制度関連システム全体概要図」（甲17）からも明らかのように、市区町村、国の関係省庁（ただし、国税庁は除く）、住基ネット、地方公共団体情報システム機構（J-LIS）がすべてネットワークでつながっている。この間は、ファイアーウォール（以下、「FW」ともいう。）で「論理的に」切断されているだけである。

(2) 現在、行政窓口（例えばハローワーク）などではタブレット端末の利用が急速に進められている。このタブレット端末はセキュリティ的には従前の有線のコンピュータ端末よりも脆弱である。したがって、この端末が乗っ取られた場合、侵入者は、行政窓口職員になりすまして、少なくとも、当該行政機関の対応するデータベースまではアクセスすることができることになる。ここではFWは通過が前提となる。

そこから、更に乗っ取りを繰り返せば、さらにその先のデータベースまで不正アクセスすることも可能となる危険性が存する。

(3) 不正アクセスを防止するためには、FWを含む各機器について、日々発見される脆弱性の穴をふさぐ修正プログラムの適用（パッチあて）を行う必要が存す

る。しかし、FWから内側のセグメント（区画）に設置されている機器（サーバ、端末、FWなど）に対するパッチあては、パッチの提供があっても、直ちには行われぬ。何故なら、そのパッチをあててもシステムに不具合が出ないかどうかをチェックした後でないと適用できないからである。そのため、パッチあてを完了するまでにどうしてもタイムラグが生じる。住基ネットの場合は、数か月以上も遅れた例やあてていない例が存した。

そうすると、プログラムの脆弱性を突いた機器の乗っ取りの危険性は、通常のパソコンなどに比して高くならざるを得ないという危険性が存する。被告は、第3準備書面において、この「不備」について具体的な反論を行っていない。

7 J-LISへの情報集中という「不備」

第1章、第5、3、(4)で述べた通り、地方公共団体情報システム機構（J-LIS）は、本人確認4情報、住民票コード、マイナンバーとそれらの変更履歴、個人番号カードの顔写真等までを一括管理している機関である。そして、全国民と外国人住民に関するこれらの個人情報を一括管理する機関が従前は存しなかったことも事実である。

前述した被告の方針からすると、将来的にはほとんどの国民と外国人住民が個人番号カードを保有することが目指されている。そうすると、同機構は、ほとんどの国民と外国人住民の顔写真付きの本人確認情報を一括管理することになる。これだけでも相当な情報量であり、かつ、価値は高い。

同機構は、個人番号カード発行システムの不具合を引き起こすなど、そのシステム管理能力において、問題を起こした組織である。

したがって、この組織において、安全に管理される保証がないまま、同機構において一括管理される個人情報が積みあがっていつているという「不備」が存する。

被告は、J-LISにおいて「様々な個人情報を一括集中管理しているという事実はない」と釈明するのみで、上述の不備（危険性）について、何ら具体的な反論を行っていない。

8 個人情報保護委員会の体制が不十分であり、機能不全であるという「不備」

個人情報保護委員会（以下「委員会」という。）は、制度上の保護措置として機能していない。その点は原告ら準備書面（6）でも述べたが、その後に証拠提出した資料等に基づき詳述する。

(1) 個人情報保護委員会の意義・権限

ア 個人情報保護委員会の意義

(ア) 個人情報保護委員会は、もともと番号法により、2014年1月1日に特定個人情報保護委員会として設置された。この際には、いわば番号法の監督機関として開始をしていた（甲60・24頁）。

(イ) しかし、2015年9月の個人情報保護法改正により、個人情報保護法をも所管する機関として、特定個人情報保護委員会が個人情報保護委員会に改組された。これにより、個人情報保護委員会は、特定個人情報保護委員会として担当していた特定個人情報の適正な取り扱いの確保を図る任務に加え、個人情報保護法の全般についての独立した監督機関としての業務等を任務とすることになった。

(ウ) これは民間事業者に対する監督であり、従来主務大臣が分野ごとに行っていたものをすべて委員会が一元的に行うことになったのである（同24頁）。

(エ) 以上のように個人情報保護委員会は、特定個人情報の適正な取り扱いの確保を図る任務に加え、個人情報保護法の全般についての独立した監督機関として広範な業務を取り扱うようになり、かつ個人情報の利活用の促進という役割もあったことから下記で述べるように十分に機能することができていない（甲58・34頁）。

イ 個人情報保護委員会の権限

個人情報保護委員会は主に以下の権限を有している。

(ア) 番号法に関する権限

a 個人情報保護委員会が行使し得る権限として、個人番号利用事務等実施者に対し、必要な指導及び助言をすることができる（番号法33条）。

b また個人情報保護委員会は、特定個人情報の取扱いに関して法令の規定に違反する行為が行われた場合、当該違反者に対して、勧告及び命令することができる（同法34条）。

なお、同命令に違反した者には、2年以下の懲役又は50万円以下の罰金が科される（同法53条）。

- c このほか個人情報保護委員会が行使し得る権限として、特定個人情報を取り扱う者等に対し、必要な報告若しくは資料の提出を求め、または職員に立入検査させることができる（同法35条）。

同条の規定による報告若しくは資料の提出をせず、若しくは虚偽の報告をし、若しくは虚偽の資料を提出し、又は当該職員の質問に対して答弁をせず、若しくは虚偽の答弁をし、若しくは検査を拒み、妨げ、若しくは忌避した者には、1年以下の懲役又は50万円以下の罰金が科される（同法54条）。

- d さらに、個人情報保護委員会は、措置の要求をすることができる（同法37条）ほか、内閣総理大臣に対し、その所掌事務の遂行を通じて得られた特定個人情報の保護に関する施策の改善についての意見を述べるることができる（同法38条）。

(イ) 個人情報保護法に関する権限

- a 個人情報保護委員会は、必要な限度で、個人情報取扱事業者等に対し、個人情報等の取り扱いに対し、必要な報告若しくは資料の提出を求め、又はその職員に立ち入り検査させることができる（個人情報保護法40条）。
- b また、個人情報保護委員会は、必要な限度で、個人情報取扱事業者等に対し、個人情報等の取扱いに関し、必要な指導及び助言をすることができる（同法41条）。
- c さらに、個人情報保護委員会は、個人情報取扱事業者が、法令の規定に違反した場合において、個人の権利利益を保護するため必要があると認めるときは、当該個人情報取扱事業者に対し、勧告及び命令をすることができる（同法42条）。
- d 個人情報取扱事業者における個人情報の取り扱い等に関する苦情の申出についての必要なあっせん及びその処理を行う事業者への協力に関する事務を行う（同法61条）。

(ウ) さらに、2016年5月の行政機関個人情報保護法の改正により、国の機関の行政機関非識別加工情報の運用に当たっての規則制定等の権限が付与されるに至っ

ている（行政機関個人情報保護法第4章の2）。もっとも、それ以外の情報について、行政機関及び独立行政法人については監督等の権限は有していない。

(2) 個人情報保護委員会の体制が不十分であること

ア 上記のように個人情報保護委員会は重要な意義及び権限を有し、その取り扱う業務は多岐にわたるが（甲49参照）、その扱い業務量に比して、体制が不十分である。

イ 個人情報保護委員会の組織は委員長1名、委員8名の合計9名にすぎない（委員長を除き、常勤が4名であとの4名は非常勤である。甲59の2、50頁）。

上記非常勤についても、そもそも欠席が多い（甲60、23頁～24頁。甲59の1、7～8頁）。具体的には、3年間（2016年から2018年）で3割以上欠席が3名、2018年にいたっては、半分以上欠席という人が2名もいるような状況である。

つまり、実情としては、9名よりも少ない体制なのである。

ウ 人口推計によれば、2016年12月1日現在の日本の総人口（概算値）は1億2692万人、2017年12月1日は1億2670万人、2018年12月1日は1億2643万人であり、これら国民の個人情報は天文学的数字になる。上記のような委員9人の個人情報保護委員会において、全国民の個人情報が適切に取り扱われているかどうかを監視・監督するのが不可能であることは明らかである。

エ 被告は、第4準備書面7頁以下において、委員会の平成30年8月1日現在の職員数は141名であり、その所管する事務を適切に行なっており、番号制度における制度上の保護措置として機能していると主張する。

しかし、そもそも、職員は補助業務を行うのであり、判断は委員会の合議による。職員の調べた内容について、すべての委員が報告を受け、必要があれば追加調査を指示する等したうえで、委員が委員会において結論を出すことが想定されているはずである。仮に委員会の業務が職員任せになっているとすれば、まさしく委員会が機能していないことの証左である。

オ 他方、そもそも職員の内訳、配置が明らかにされていないという問題もある（甲 59-1・21頁以下）。

職員数の内訳（他省庁からの出向者の数、出身省庁、民間からは何人か。）や専門性（技術系が何人かなど。また例えば、委員会の命令違反は犯罪になるのだから（番号法84条）、命令及びその前提となる勧告（同法42条）を発するに当たってはそれが犯罪の構成要件として成り立つかというチェックが必要であるが、それに適した人員（検察庁あるいは裁判所からの出向者、弁護士の採用などが考えられる。）はいるのかなど。）を明らかにすべきであるがそれもなされていない。

個人情報保護委員会事務局組織令、同規則が公表されているが、これらをもみても組織の実態は不明である。委員会の所管する各事務に対応して、具体的にどのような部門が設けられているのかを示し、その上で、各部門にどのような出自の職員が何人配置されているのかを明らかにすべきであるがそれもなされていない。

つまり、本来明らかにされるべき職員の内訳、配置が明らかにされていないという問題もあり、この点から個人情報保護委員会の体制には疑問が生じざるを得ない。

カ 小括

番号法制定時の附則6条3項では、政府は委員会の行う監視又は監督について、「これを実効的に行うために必要な人的体制の整備、財源の確保その他の措置の状況を勘案し、適時にその改善について検討を加え、必要があると認めるときはその結果に基づいて所要の措置を講ずるものとする」とわざわざ規定しており、参議院内閣委員会の附帯決議でも（当時の）特定個人情報保護委員会の事務局機能の充実が要請されている。

さらに、2015年9月改正時の番号法及び個人情報保護法は、いずれも附則12条2項で、「政府はこの法律の施行後3年を目途として、個人情報の保護に関する基本方針の策定及び推進その他の個人情報保護委員会の所掌事務について、これを実効的に行うために必要な人的体制の整備、財源の確保その他の措置の状況を勘案し、その改善について検討を加え、必要があると認めるときはその結果

に基づいて所要の措置を講ずるものとする。」と規定している。

このように個人情報保護委員会については、法制定当初から、大きな期待が持たれているとともに十分に機能を果たしうるか不安視されていたところであるが、これまで述べたとおり、人的体制等が極めて十分な状況にあり、このような状況では、個人情報保護委員会の権限を行使して個人情報保護を図るという事も困難である。

(3) 会計検査院の指摘などから個人情報保護委員会の機能不全が現実に明らかになったこと

ア 市民団体「共通番号いらないネット」では、2018年1月30日に特別税額通知書の誤送付等による漏えいの発生や情報連携システムに対する会計検査院の指摘、日本年金機構の不正再委託の問題について、個人情報保護委員会に質問書を提出した（甲58・15頁）。

イ しかし、同年4月4日、個人情報保護委員会から「個別の事案に関する質問なので回答しない」と拒否された（同頁、甲56・32～33頁）。

ウ その後8月29日に、証人原田は、参議院内閣委員会の田村委員の仲介で、個人情報保護委員会へのヒアリングがあり、これらの問題と年金機構の不正再委託問題への対応について、説明を受けた。

しかし、説明を求めた特別税額通知の誤送付の実態や、年金機構の不正再委託でマイナンバーも提供されていた事例の内容、委員会の行った調査や指導の内容など、具体的な事柄は、「個別の内容はお答えできない」との回答に終始した（同15～16頁、甲56・33頁）。

エ また、住民税の特別徴収税額通知を送付した自治体や送付された事業者の安全管理措置、会計検査院に指摘を受けた情報連携の機関などについて、委員会として調査を行っていないことが明らかになった（甲56・12～15頁）。

さらに、特別徴収税額通知へのマイナンバーの記載を市町村に迫り漏えいの原因を作った総務省に対しては、「制度官庁の制度設計に対する指導監督は想定していない」と回答している（甲56・33頁）。

オ 立ち入り検査について、年に27件程度の定期的な立入検査を行うことしかできず（甲57・資料16「平成29年度年次報告」18頁）、それで違反を把握することは困難である。

カ 個人情報保護委員会は、苦情あっせん相談窓口に寄せられた情報により必要な指導助言を行っていると説明しているが（同27～28頁）、この窓口は、相手方への苦情の内容の伝達あっせん、他の相談窓口の紹介、監督部門への取次ぎなどを行うだけで、通報者にその後の処理の報告もされず、委員会がどのように責任をもって苦情を処理するのか、その処理基準や対応の仕方も明らかにされていない。

キ 以上の通り、個人情報保護委員会は、その意義を果たすことはなく、特別税額通知書の誤送付等による漏えいの発生や情報連携システムに対する会計検査院の指摘、日本年金機構の不正再委託といった重要な問題について市民に対して何らの説明も行うことをせず、委員会としての調査や指導などの実態もなく、また立ち入り検査及び苦情あっせんも十分ではないことから、その機能不全は明らかである。

(4) 違法再委託問題においても個人情報保護委員会の機能不全は明らかであること

ア 個人情報保護委員会に認められた権限

前述の通り、個人情報保護委員会では、個人番号利用事務等実施者に対する必要な指導、助言、法令違反行為に対する勧告及び命令及び立ち入り検査などの権限を有する。

イ 違法再委託問題で行った委員会の権限行使

(ア) 年金機構の違法再委託問題で行った権限行使

しかし、実際に行われた指導は「責任をもって請け負うという緊張感を持ち、危機管理に関する意識改革を引き続き行う」「特定個人情報等の適正な取扱いに向けた取組を継続的に実施すること」（乙48）というごく抽象的で、わずか数行で終わる簡潔なものが記載された書面を交付したにすぎない。この点について、個人情報保護委員会の権限に詳しい森田明弁護士も「各機関に任せてしまっていて、委員会が主導的に対応しているというふうには受け取れない」（甲60・35頁）と明確に述べて、その指導の不十分性を指摘している。

(イ) 国税庁・地方自治体の違法再委託問題で行われた権限行使

違法再委託の問題に関して、個人情報保護委員会はどのような権限を行使したのか、明らかにしていない。

実際に、同委員会は、ホームページ等に違法再委託の問題に対する対応を記載することもなく（甲58・32頁）、重大な法令違反の問題が生じているのに、一般市民は同委員会の対応を知ることができない状態にあった。

そのため、市民団体は、同委員会に対し、違法再委託の問題について、質問書を提出した。それにもかかわらず、同委員会は個別の案件のため答えることができないという極めて不誠実な対応をしたのである（同30～32頁）。

結局のところ、同委員会がどのような権限行使をしたのか明らかにならない以上、同委員会は、ほとんど権限行使をしていないと言わざるを得ない。

ウ 勧告・命令等の権限行使がされていないこと

番号法では特定個人情報の重要性に鑑みて、重い刑罰を科することが定められている。

しかし、その前提となる勧告・命令が行われない限り刑罰は適用されることはないのだから、結局は重い刑罰を法令上定めていたとしても何ら役に立たないものになってしまう。

本件でも、既に詳述したように、大量の特定個人情報が流出・不正利用の具体的危険にさらされているにもかかわらず、個人情報保護委員会による簡単な指導があるのみで、勧告・命令はなされていない。そのため、重い刑罰を科す前提が欠けているのである。

結局、違法再委託の問題のように極めて重大な問題が生じながら、個人情報保護委員会は、勧告・命令をしていないことを自認しているとしか言いようがない。

そもそも委託元の許諾なく業務が再委託されれば、その業務の監督が全くできないことが問題であるのに、十分な調査さえなされていない（甲60・12頁参照）のは、与えられた権限を放棄しているに等しい。

エ 番号制度の保護措置として意味がないこと

(ア) 保護措置として期待された役割を全く果たせていないこと

番号法10条1項では委託元の許諾を得れば再委託をすることができることとなっており、同法11条による監督を及ぼした上、問題が生じた場合には第3、1で述べた個人情報保護委員会の適切な権限行使を行うことで特定個人情報を保護することが求められている。

しかし、問題が生じた場合に権限行使が全くと言っていいほど行われていないことは前述のとおりであり、番号制度の保護措置として全く機能していない。また、番号法で再委託を禁止していない、あるいは再委託をする場合でもその方法についての条件を付けていないことは制度的な欠陥である。

(イ) 権限行使の状況が明らかにならなかったこと

委託元の許諾なく違法な再委託がされ、特定個人情報の流出・不正利用の危険性が生じたとしても、漏洩された本人はそのことを知るができない。

機構の違法再委託の問題についていえば、前述のとおり、市民団体による質問に対して、機構は説明を全くせず、後に指導を行ったことが分かったという状況であった(甲58・30～31頁)。また、システムズデザイン社及びAGS株式会社による委託元の許諾なき再委託についても、市民団体による質問書に対して個別の案件のため答えることができないとの回答があった(同32頁)。

オ 小括

以上述べたとおり、個人情報保護委員会は、組織上、実務上の限界もあって与えられた権限行使すら行えていない。個人情報保護委員会の体制が不十分であり、制度上の保護措置として機能していないことは明らかである。

第4 被告がプライバシーや安全性を軽視し「不備」を生み出す根拠について

1 プライバシー・バイ・デザイン等の軽視

被告の個人番号制度や個人番号カードの制度設計が、上述のように「利便性」優先、プライバシーや安全性の軽視となっている理由は、被告が、今や国際的な安全性に関するスタンダードな考え方であるプライバシー・バイ・デザイン(デザイン(=設

計)段階から組み込むプライバシー保護)や、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(プライバシー影響評価～環境影響評価のプライバシー版)を軽視し、行なっていないことに大きな原因が存する(原告ら準備書面(2)、第1、第2部分参照)。

2 被告も認めるプライバシー・バイ・デザイン

(1) 原告らは、プライバシー・バイ・デザインが今や世界のプライバシー保護機関(データ保護・プライバシー・コミッショナー国際会議)のスタンダードの考え方となっており、日本の個人情報保護委員会の委員長(当時)である堀部政男名誉教授も「プライバシー・バイ・デザインが今や新しいグローバル・スタンダードになってきている」と紹介していると主張した(準備書面(2)、4～8頁等)。

これに対して、被告は、「原告らが主張の根拠とする番号制度における個人情報保護方策の設計については、番号制度導入前の平成23年度に、政府・与党社会保障改革検討本部が同年1月31日に決定した『社会保障・税に関わる番号制度についての基本方針』(乙第25号証)に基づき設置された『個人情報保護ワーキンググループ』において検討が重ねられ、『プライバシー・バイ・デザイン』(ITシステムや業務慣行において、最初からプライバシー保護策を組み込み、侵害発生後の対応ではなく、事前にプライバシー保護策を組み込み、侵害発生後の対応ではなく、事前にプライバシー対策を講じておくようにするという概念)や、PETs(システムの機能を損なうことなく個人のプライバシーについて保護性を高める技術)といった国際的な考え方にも対応した措置を講ずることとされている(乙第26号証2ページ)。」と主張した(第2準備書面、第3、3(2)ア・11頁)。

この主張は、被告もプライバシー・バイ・デザインが世界的な考え方であり、その考え方に基づく対応を行う必要性は認めていることを示すものである。

(2) EU一般データ保護規則と同等の保護レベルを確保する義務

日本とEU間の相互の円滑な個人データ移転を図る枠組みが、平成31年1月23日に発効した。個人情報保護委員会と欧州委員会による、お互いの個人データの保護レベルが同等だとする決定が採択されており、日本とEUは、「プライバシーに関

する価値観の共有及び高いレベルの個人データの保護に基づく世界標準の形成に向けた協力の強化へのコミットメントを再確認」したとされている（個人情報保護委員会のHP・平成31年1月23日「日EU間の相互の円滑な個人データ移転を図る枠組みが発効しました。」参照）。

つまり、日本も、EUと同等の個人データ保護レベルを図る義務が生じたのである。

ところで、EU一般データ保護規則は、その25条で「データ保護バイデザインと初期設定によるデータ保護」義務を規定している。「管理者は、技術水準や運用費用等を考慮し、処理の段階においてデータ処理最小限化や仮名化の措置等の適切な技術的・組織的措置を講ずるものとする」、「管理者は初期設定において利用目的を超えて個人データが処理されないように適切な技術的・組織的措置を講じるものとする」（宮下紘中央大学准教授著『EU一般データ保護規則』154頁）とされる。

よって、日本においても、いわゆるプライバシー・バイ・デザインは、今や義務の内容となっている。

(3) にもかかわらず、出来上がったマイナンバーのシステム・制度は、「利便性」優先で、プライバシー保障に対する配慮は二の次となっている。

3 プライバシー・バイ・デザインに基づく制度設計

- (1) 被告も認めるプライバシー・バイ・デザインの考え方、すなわち、「ITシステムや業務慣行において、最初からプライバシー保護策を組み込み、侵害発生後の対応ではなく、事前にプライバシー保護策を組み込み、侵害発生後の対応ではなく、事前にプライバシー対策を講じておくようにするという概念」からするならば、①国や行政が権限を濫用して、特定個人情報を名寄せする危険性をあらかじめ防止する保護策を組み込むことが必要であるし、②国や行政が、法律の改正をするなどして“形式上合法的に”、過度な特定個人情報を名寄せする危険性をあらかじめ防止する保護策を組み込むことも必要である。
- (2) そのための方策としては、容易に名寄せできないように、分野別番号制にしておくことが最も基本的なものとなる。また、情報連携する必要性が高い場合は、その分野

別番号を、暗号技術を用いて紐づけることが、世界の趨勢となっている（例えば、オーストリアの制度）。さらに、個人情報の過度な名寄せがなされた場合は、行政から独立したプライバシー保護のための第三者機関が直ちにそれをチェックできるような体制をとっておくことが必要となる。

- (3) 具体的にこのような体制を整備するためには、プライバシー・バイ・デザインに基づく制度設計を実現するために、プライバシー・インパクト・アセスメント(プライバシー影響評価)を行うことが必要である。これにより、このような制度設計をすると、プライバシーにどのような悪影響が生じるかということが制度設計の初期段階で評価され、より悪影響のない制度設計が可能となるからである（副次的に、制度が出来てからの制度・システムの作り直しという事態を避けうることにより、膨大な税金の無駄が発生することの防止ともなる）。

4 プライバシー・バイ・デザインに反する現マイナンバー制度の設計

- (1) ところが、現マイナンバー制度は、到底上記プライバシー・バイ・デザインに基づく制度設計とはなっていない。
- (2) 本訴訟において、被告は、共通番号であるマイナンバーと機微な個人情報とをひも付けても、“漏れないようにすればよい”、“そのために、行政に対しても、民間に対しても、漏らさないように厳重な管理義務を法定している”という基本的発想に基づいて応訴している。そのことは、例えば、原告らが一定割合で必ず発生することが自明であるところの住民税の特別徴収通知の誤配送の事実を指摘したことに対し、被告が「仮に特別徴収税額通知を送付することにより情報漏洩の危険などの問題が生じるとしても、それは番号制度そのものとは別次元の人為的ミスなどを原因とするものであり、仮に同通知の送付について問題があるとしても、それによって必然的に番号制度自体が問題のあるものとはいえない」などと主張している（被告第2準備書面18頁）ことに端的である。

マイナンバーは「共通番号」であるゆえに、それを取得した民間人でも、マイナンバーにひも付いた個人情報を、マイナンバーをマスターキーとして名寄せすることが可能なことが大きな問題点である。かつ、現代社会におけるセキュリティは「事故前

提社会」として安全対策を講じなければならない（原告ら準備書面(1)、第2、4(2)・17頁や準備書面(4)、第2、4(5)・11頁）。

にもかかわらず、被告がこのような応訴態度をとっているということは、プライバシー・バイ・デザイン思想に基づいていないことを端的に表しているものといわざるを得ない（なお、原告らが、平成29年4月18日付「求釈明申立書」等で、繰り返し「プライバシー影響評価を行ったのか」などの点について釈明を求めたが、被告は頑なに釈明を拒否し続けた）。

- (3) その他にも、①マイナンバーシステムで行われている「特定個人情報保護評価」は、本来の、すなわち制度設計段階におけるプライバシー影響評価ではないという点にも、そのことは示されている。現在行われている特定個人情報保護評価は、個人番号と個人情報をひも付けて保存等することは前提として、個別事務のシステムにおいてプライバシー情報の漏洩等をなるべく少なくしようとするものでしかない。

しかも、②特定個人情報保護評価は、自己評価するものに過ぎない。かつ、③その評価の仕方が複雑であるので、特に小規模自治体の各現場では他の同種機関の特定個人情報保護評価をコピーアンドペーストして提出するというずさんな評価が続出している（この点は被告も認める）。これらの点に、プライバシー・バイ・デザインの考え方に沿わない制度設計と運用の思想が表れていると言わなければならない。

- (4) このような制度設計を行ったことにより、極めて膨大な労力と税金を投入して、機関別符号を用いた情報連携ネットワークシステムを整備したにもかかわらず、そして、そのような情報連携ネットワークシステムを作るのであれば、例えば、オーストリアの制度のように、分野別番号制を使いながら、プライバシーコミッショナーを通じた分野別番号同士の紐付けを可能とすることにより情報連携を可能とするような、「共通番号」を使わないで、その目的とした「情報連携」が行える仕組みも構築可能であったにもかかわらず、実現できなかったのである。

改めて、情報連携等がさらに拡大する前に、本制度・システムの見直しをすることが、是非とも必要であることを指摘する。

第5 合憲性審査の結論

以上指摘してきたように、いわゆる「構造審査」基準によっても、その不備の程度は著しい。

よって、原告らを含む全国民・外国人住民のプライバシーや人格権は具体的な危険にさらされており、第1章、第2章で検討したいずれの違憲審査基準に照らしてみても、本マイナンバー制度は違憲であると言わなければならない。

第3章 損害賠償について

以上指摘してきた点から、原告らのプライバシー権、人格権に対する危険性は明らかであるから、損害賠償請求も認められるべきである。

おわりに

- 1 本訴訟では、まず、自己情報コントロール権としてのプライバシー権（但し、本件では、訂正請求等の積極的な権利内容は直接問題にならず、自由権的な権利内容である）が認められるかが争われた。

この点に関連して、中央大学の宮下紘准教授が2015年に『プライバシー権の復権—自由と尊厳の衝突—』という著書を出されているが、その「まえがき」での一節を紹介したい（甲79）。

宮下准教授は次のように述べられている。

「本書の主題を設定するにあたっては、一つのきっかけがある。それは、2008年3月6日最高裁判所において下された、いわゆる住基ネット判決である。当時、筆者は個人情報保護法を所管していた内閣府個人情報保護推進室に勤務をしていたため、判決の結論を聞いてほっとしたのを覚えている。しかし、判決文を読むと、違和感のようなものを抱いた。判決にはプライバシー権を正面から認めた形跡はなく、むしろプライバシー権という言葉を避けているような印象を受けたからである。事実、調査官による解説では、自己情報コントロール権が憲法上保障された人権と認められるか否かについては正面から判断していないことが記されている。本

判決が下される前、2007年9月にカナダのモントリオールで開催されたデータ保護プライバシー・コミッショナー国際会議の場では、外国のコミッショナーや研究者たちからも日本の住基ネットについて最高裁がどのようなプライバシー権の判断を下すかについて注目されており、議論になった。後に各国のコミッショナー、研究者、さらには司法関係者に住基ネット判決を紹介した際、『日本は先進国であり、民主主義国家であるが、明確な形で自己情報コントロール権が人権として保障されていないのか』という指摘を、幾度となく受けた。」

ここからも読み取れるように、住基ネットがプライバシー権を侵害するとして争われた違憲訴訟は世界から関心を集めていたのであり、それは日本が自己情報コントロール権を正面から認めなかったからであった。

住基ネット最高裁判決から12年近くが経過した現在、住基ネットよりはるかに明確に番号制とデータマッチングが問題となる本マイナンバー制を問う裁判において、自己情報コントロール権が認められず、あいまいな判断が下されれば、日本は世界からどのようにみられるかということを裁判所には考えて判断いただきたい。

2 その際に、12年前とは様変わりしたと言ってよい、現代のプライバシーが置かれている状況を前提として勘案することが必要であることを改めて強調したい。

現代社会におけるプライバシー侵害は、情報通信技術の高度な発展に伴い、個人情報（特にデジタル化されたデータ）が名寄せされてデータマッチングされ、さらにその人物の趣味や嗜好、人物像などが分析される＝プロファイリングされる＝形での侵害が重大な問題となっているのである。近時においては、AI（Artificial Intelligence 人工知能）の活用により、それらが容易に且つ大規模に、そして高い精度で行われるようになってきている。このような社会を迎えている現代においては、原告らのみならず、全国民・外国人住民のプライバシーを保障して行くためには、名寄せされない（されにくい）ようにすることを1つの柱として、その保障を十全にはかつてゆく必要がある。そうしなければ、プライバシー保障は、その基盤すら喪失するのである。一旦失われたプライバシーは元に戻すことはできない。さらに、そのような人物像がプロファイリングされてしまう社会では、「情報操作」などにより、民主主義

社会の基盤すら掘り崩される結果となる。近年の米国大統領選挙は、その一端を示した。

- 3 そのような前提を措いた上で、本マイナンバー制度の合憲性を考えるならば、本制度は、その目的において公共の福祉を実現する上で重要性がないものである。そして、その手段の点においても欠くべからざる制度・システムであるとは言えない。少なくとも、分野別番号制を前提とした、よりプライバシー権や人格権に影響の少ない制度・システムをとりえたことが、原告らの主張立証によって明らかとなった。すなわち、本制度は、その目的においても、手段においても、プライバシーや人格権という最も価値の高い人権、しかも傷つきやすく・一旦傷つけられたら回復が事実上不可能な人権を侵害するものとして、憲法第13条に違反し、違憲といわざるを得ない。
- 4 被告は、このような重大な人権にかかわる問題であるにもかかわらず、一貫してその説明責任を果たさず、また、真摯な応訴態度をとってこなかったと言わざるを得ない。現代民主主義社会においては、「民は由らしむべし、知らしむべからず」（江戸時代には、法律を出した理由など人民に教える必要はない、一方的に法律（施政方針）を守らせればよいという意味に解されて、これが政治の原理の一つとなった・ブリタニカ国際大百科事典）ということは通用しない。また、被告の考え方の根底には、効率性を優先し、個人の人格を形成し、保障してゆくうえで最も重要なプライバシー権・自己情報コントロール権に対する保障を重視していないという姿勢が存すると言わざるを得ない。

裁判所におかれては、現在及び近い将来の原告を含む全国民・外国人住民のプライバシーや人格権、ひいては、民主主義を制度的に保障してゆくために、事実に基づき、知性と理性を発揮した判断を行うことを切に求めるものである。

以上