訴　　状

平成２７年１２月１日

金沢地方裁判所　御中

原告ら訴訟代理人弁護士　　岩　　淵　　正　　明

原　　告　　別紙原告目録記載のとおり
原告ら訴訟代理人　　別紙訴訟代理人目録記載のとおり

〒１００－００１３　東京都千代田区霞が関１丁目１番１号
被　　告　　国
上記法務大臣　　岩　　城　　光　　英

マイナンバー離脱等請求事件
訴訟物の価額　８０，０００，０００円
貼用印紙額　　２６０，０００円

目　　次

請 求 の 趣 旨

1　被告は、原告らにかかる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第２条第５項に定める個人番号を収集、保存、利用及び提供してはならない

2　被告は、保存している原告らの個人番号を削除せよ

3　被告は、原告らに対し、各１１万円及びこれに対する訴状送達の日の翌日から支払済みまで年５分の割合による金員を支払え

4　訴訟費用は被告の負担とする

との判決並びに仮執行宣言を求める。

請 求 の 原 因

第１　はじめに

本訴訟は、マイナンバー制度がもたらすプライバシーを中心とした人格権等の侵害について、その憲法適合性を問うものである。言い換えるならば、コンピュータ・ネットワークが発達し、「ビッグデータ」の利活用が急速に進められている現代の高度情報化社会におけるプライバシー権保護のあり方について問うものである。

番号制によるプライバシー権侵害の問題は、情報漏洩などの“目に見える”侵害に止まらず、情報の一元的管理とデータマッチングによる「萎縮効果」など“目に見えない”重大な危険を発生させるものであり、現代社会における人権保障の観点から慎重に検討・考察する必要がある。

しかるに、被告は、マイナンバー制度の法案審議の過程においても、法案成立後の制度利活用推進の過程においても、現代の高度情報化社会におけるプライバシー保護の特質と重要性についてほとんど検討を加えないまま、IT戦略と成長戦略の柱として、マイナンバー制度の利活用をスケジュールありきで推し進めている。

マイナンバー制度は、日本に住民票をおく全員の個人情報を扱う巨大インフラであり、一旦動き出してからではその修正は極めて困難である。米国、韓国のように、大量の情報漏洩やデータマッチング、成りすましなど、番号制の弊害が大きな社会問題となる前に、今のうちに差し止めて弊害が生じないようにプライバシー保障の観点からしっかりと見直すことが必要である。

裁判所には、現代の高度情報化社会におけるプライバシー保護の重要性に鑑み、諸外国の知見や弊害も踏まえて、慎重かつ本質に迫る審理を行うことを求める。

なお、以下用いる用語例は下記のとおりである。

① 番号法

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

② マイナンバー

番号法第２条第５項に定める個人番号

③ マイナンバー制度

番号法第２条第５項に定める個人番号、同第７項に規定する個人番号カード、同第１４項に定める情報提供ネットワークシステム等の番号制度全般

④ 特定個人情報

番号法第２条第８項に定めるマイナンバー付きの個人情報

⑤ データマッチング

様々な個人情報を名寄せ・突合すること。これによってある者の人物像をつくりだすことを「プロファイリング」という。

第２　当事者

１　原告ら

原告らは、別紙原告目録記載の市区町村に住民票をおいている者であり、番号法第２条第５項に定めるマイナンバーの付番を受けた。

2　被告

被告は、平成２８年１月以降、番号法で定めた税、社会保障、災害対策の各分野で、マイナンバーの収集、保存、利用、提供等を行おうとしているものである。また、被告は、その後も、マイナンバー、個人番号カード、情報提供ネットワークシステム等のマイナンバー制度の利活用を積極的に図っている。

第３　マイナンバー制度の概要等

被告は、マイナンバー制度の概要について「マイナンバー 社会保障・番号制度概要資料」（平成２７年８月版）（甲１）記載のとおり説明している。その制度の特徴は以下の点にまとめることができる。

1　国民と外国人住民の全員に対して、新たに「マイナンバー」と呼ばれる重複しない１２桁の「背番号」（個人識別番号）を付番したこと。

2　マイナンバーを、民間でも利用可能な広範な分野、まずは、税、社会保障、災害分野の共通番号として利用すること。

3　マイナンバーは原則生涯不変であること。

4　マイナンバー確認と本人確認のために、マイナンバー、氏名、住所、生年月日、性別等を記載し、顔写真のついたICチップ入りの「個人番号カード」を無料配布し、その利活用を図ろうとしていること。利活用の対象は、現在検討されているものだけでも、国家公務員の身分証明書、健康保険証、印鑑登録証など多数に上る。

5　各省庁等に収集、保存されている、特定個人情報の連携（＝データマッチング）をするためのシステムである情報提供ネットワークシステムを整備したこと。

6　平成２９年１月から、「マイナポータル」というインターネットポータルサイトを立ち上げ、個人番号カードを使えば、各種情報提供や手続きを行えるようにしたこと。

7　今後、積極的にマイナンバー制度の利活用を図ることが国家戦略として位置づけられており、広範な利活用案が急速に実現に移されようとしていること。

第４　マイナンバー制度（共通番号制度）の危険性

マイナンバー制度は、

①　分野毎に別々の番号が用いられる「分野別番号」制度ではなく、分野を超えて共通の個人識別番号を用いる「共通番号制度」であること

②　現在、番号法で定められた利用事務だけでも広範であり、かつ、これらの事務で収集、保存等される特定個人情報は、税や社会保障分野の機微性の高いものであり、情報の価値が高いこと

③　近い将来、さらに利用分野の拡大が予定されていること

という特徴を有するものであるから、情報漏洩等の危険性が高く、その被害も深刻となる。

さらに、政府は、平成２８年１月の運用開始以前から、その利用事務の拡大を急速に進めており、将来の危険性はさらに高くなる。したがって、以下述べるとおり、原告らのプライバシー等に対する危険性は非常に高いものとなっている。

１　マイナンバー制度の本質的危険性

⑴　漏洩の危険性

ア　官民で作られることになる膨大なデータベース

マイナンバーは“納税者番号”（税務分野で個人を識別する背番号）と“社会保障関係の番号”（社会保障分野で個人を識別する背番号）として、広く民間で収集、保存され、関係行政庁等へ提出する書類に記載される番号（民－民－官で利用される番号）となる。

したがって、行政機関のみならず、民間においても、いたるところにマイナンバー付きの個人情報データベースができることになる。総務省によ

ると、平成２４年２月１日現在で、全国で４１２万８２１５の企業が存在し、その従業員数は５５８３万７０００人とされており、民間だけでも、少なくともこの従業員数（及びその扶養家族数）に応じたマイナンバー付き個人情報データベースが全国で４１２万件以上作られることになる。

イ　民間部門からの個人情報漏洩の危険性

民間で膨大な数のデータベースが作られることから、民間部門での特定個人情報の漏洩の危険性が高まるのは必然である。特に、マイナンバー制度に関して、平成２８年１月からの運用開始を目前としている現在においても、いまだに制度に関する周知や研修が十分に行われていない。

また、マイナンバー制度のセキュリティ対策には、１社あたり平均約１０９万円もの費用がかかるとされている（平成２７年５月１９日付帝国データバンクの公表資料「マイナンバー制度に対する企業の意識調査」）。

そのため、制度の安全確実な運用にはほど遠い“準備不足”のまま運用開始を迫られた民間企業等においては、セキュリティ対策が不十分なところも多い。そのような中で、平成２７年１０月５日以降、各人に通知された従業員や取引先等の個人番号が収集、保存されている状況にある。

このような状況の中では、特定個人情報の安全は確保できず、その漏洩事件の発生は必然と言わざるをえない。

ウ　行政部門からの個人情報漏洩の危険性

行政部門からの特定個人情報漏洩の危険性も、また高くなる。

その危険性を端的に示したのが、平成２７年６月１日に公表された日本年金機構からの１２５万件にも上る基礎年金番号付き個人情報の漏洩事件である。

同機構は、番号法に基づく特定個人情報保護評価（訴状１３頁）において、「不正プログラム対策」及び「不正アクセス対策」を十分に行っているとして、「特定個人情報の漏洩やその他の事態を発生させるリスクを軽

減させるために十分な措置を講じている」と宣言していたにもかかわらず、前記漏洩を生じさせた。このような宣言をしたところにおいても、セキュリティの実態は極めて不十分なものであることが明らかとなったのである。

同機構が採用している基準は、特定個人情報を扱う他の行政機関と同じ「政府機関の情報セキュリティ対策のための統一基準群」である。したがって、他の行政機関からも同じように情報が漏洩する危険性がある。

なお、同時期に情報セキュリティに関しては相当の水準にあるはずの米国の人事局においても、サイバー攻撃により２０００万人を超える人事データが漏洩したことが明らかとなっている。

エ　情報漏洩の危険の現実性

このような最近の事例に鑑みると、前記の各所において、官民問わずに大量の個人情報漏洩が発生し、機微なプライバシー情報が違法に収集されたり、公開されたりする危険性があることは明らかである。特に、セキュリティ水準がまちまちである民間においては、漏洩の危険性はより高いと言わなければならない。

そして、情報がデジタル化され、ネットワークの発達した現代の高度情報化社会においては、このように一旦漏洩してしまった特定個人情報を抹消し、元の状態に回復することが事実上不可能であるから、その危険性は深刻である。

⑵　名寄せ・突合（データマッチング）の危険性

ア　漏洩した特定個人情報の名寄せ・突合の危険性

一旦漏れた特定個人情報は、名寄せのマスターキーである「マイナンバー」により、多くの分野の個人情報を、他人の個人情報と混同することなく、容易かつ確実に名寄せ・突合（＝データマッチング）することが可能となる。

しかも、このマイナンバーは、原則生涯不変であるから、一生涯を通じ

た個人情報が名寄せされかねない。

漏洩した個人情報の名寄せにより、本人の関与しないところで、その意に反した個人像が勝手に作られることになる（＝プロファイリング）。また、場合によっては、後述の成りすましにより、例えば多重債務者とされて、その旨の登録がなされてしまう危険性もある。

そして、このようにしてデータマッチングにより作られた個人像も、消去することが事実上不可能であるから、その被害も深刻である。

イ　国家・行政機関による情報の一元化の危険性（「監視国家化」の危険性）

さらに危険なのは、国により、情報提供ネットワークを用いた、あるいは、用いないでなされる個人情報の一元化である。

㈠　番号法に定められた行政機関等においては、平成２９年１月以降、情報提供ネットワークシステムを通じて、原告らを含む全国民・外国人住民の個人情報を名寄せ・突合できることになる。このシステムにおいては、番号法別表記載の事務に当てはまる要求を出しさえすれば、自動的に当該個人の情報取得が可能となる。

したがって、これらの行政機関等の担当者が、情報要求の目的を偽るなどして情報収集を行うという危険性が存する。そして、その危険性はマイナンバー制度の利活用の促進（番号法別表記載事務の拡大等）により、今後さらに高まる。

㈡　警察機関などは、「刑事事件の捜査」のためとすれば、情報提供ネットワークシステムを使わずに、特定個人情報を収集できる（番号法１９条第１２号）。

近時、警視庁外事課が「テロ対策」を口実に、まだ罪を犯してもいないムスリム住民の監視を行い、その住所、職業、預金口座等まで情報収集していたことが明らかとなった。このような活動でも「刑事事件の捜査」という名目をつけるならば、警察は官民の各所に対して特定個人情

報の収集要求を行うことができるようになるのである。

しかも、このような収集・利用等に関しては、第三者機関である個人情報保護委員会（平成２８年１月以降）のチェックを受けることもないのである（番号法第５３条、改正後の第３９条）。

㈢　以上のように、行政機関により、原告らを含む全国民・外国人住民の個人情報が一元的収集・管理の対象となる危険性、すなわち「監視国家化」の危険性は高いと言わなければならない。

⑶　成りすましの危険性

ア　現実世界の成りすまし

㈠　前述のように、特定個人情報が漏洩し、それが名寄せ・突合されればその対象者の個人像が明らかになる。したがって、その情報を利用すればその人に成りすますことが容易となる。

㈡　また、住基ネットの住民基本台帳カードについては、報道されたものだけでも不正取得事件が２０件以上も発生している。そのこともあり、例えば、ソフトバンク社では同カードを身分証明書として利用することを認めなかった。

この前例からみても、マイナンバー制度の施行に伴って交付される、通知カードや個人番号カードの不正取得、あるいは偽造等による成りすましの危険性も高いと言わなければならない。対面での成りすましの場合は、個人番号カードや免許証等によって本人確認を厳格に行うことが出来るが、例えば、個人番号カードのコピーを偽造する等して、郵送でクレジットカードを作るなどをされた場合は、容易に成りすましを行うことができる。

㈢　成りすましをされた場合、例えば、勝手に債務を作られるなど、本人の関与しないところで、誤った、もしくは歪んだ本人像が作られることになる。

しかも、この場合、成りすましをされたということを主張立証する責任は本人にあることになるから、その訂正は極めて困難である。この成りすましによる被害は、米国などでは極めて深刻な社会問題となっているところである。

イ　マイナポータルにおける成りすまし

現実世界だけでなく、インターネットの世界においては、より成りすましの危険性は高い。

すなわち、番号法により、平成２９年１月以降、マイナポータルというインターネットサイトが構築され、そこから自己の個人情報の閲覧や、各種行政等の手続きが相当広範囲にできるようになることが計画されている。

したがって、個人番号カードを不正取得したり、高齢者などの“IT弱者”の手助けをするように装って、パスワードを教えてもらい、もしくは何らかの手段で知ることが出来れば、マイナポータルにアクセスして、その人の個人情報を覗いたり、色々な手続きを勝手に行うことも可能となる。

便利さをうたうマイナポータルであるが、いったん成りすまされた場合には、現実世界の成りすましと異なり、対面によるチェックが働かない分その裏返しの危険性が高くなる。

２　マイナンバー制度利用拡大による危険性の増大

⑴　被告は、国家戦略、成長戦略の重要な柱として、マイナンバー制度の利活用の促進を図っている（世界最先端IT国家創造宣言など参照）。

また、被告は、番号法の附則上は施行３年後に見直すことになっているにもかかわらず、施工前から銀行預金等へのマイナンバー付番やメタボ健診等情報へのマイナンバー付番など、利用拡大法案を成立させている（平成２７年９月３日）。

⑵　その一環として、被告は、個人番号カードを、身分証明書、健康保険証、印鑑登録証などとワンカード化させることを促進して、同カードの普及を図

っている。国家公務員の一部については、平成２８年４月から身分証明書と個人番号カードの一体化が計画されている。

また、一時は、消費税率の１０％へのアップ時に、軽減税率導入の代わりに個人番号カードを利用した還付金制度すら検討されるに至った。

これらワンカード化などの施策が実行されれば、個人番号カードの所持は事実上強制されることになる。この個人番号カードの券面（裏面）には、秘密とされるべきマイナンバーが記載されており、同カードを身分証明書などとして日常的に持ち歩かなければならなくなれば、マイナンバーを第三者に知られる機会や個人番号カード自体を不正取得されてしまう機会は激増し、危険性が極めて高くなるといわなければならない。

⑶　さらに、被告は、マイナポータルについても「ワンストップサービス」の窓口として、その利活用の範囲を広げることを推進している。よって、この面においても、成りすまし等の危険性は高くなると言わざるを得ない。

３　性同一性障害者、ペンネーム使用者、ストーカー被害者等の危険性

性同一性障害者は、生活のために雇用先などに対し戸籍上の性を明らかにすることが強制される。性同一性障害者への差別や偏見は根強く、性同一性障害者は、戸籍上の性を明らかにすることによって耐えがたい精神的苦痛を受けることになる。

また、作家や芸能人などペンネーム・芸名を利用している者も、同様に戸籍上の氏名を告知することが強制される。作品や芸風のイメージに合わせたペンネーム・芸名を使用しているこれらの者にとっては、プライバシーの開示に留まらない人格の中核（アイデンティティ）にも関わる侵害ともなる。

その他、DV、ストーカー被害者は、住所を告知することを強制されることになる。これらの者にとっては、自宅住所を知られることにより、生命・身体への危険性が発生する。

なお、マイナンバー制度により特定個人の情報を検索、名寄せしやすくなっ

たことにより、例えば、政府要人、防衛産業技術者及び自衛隊関係者等の個人情報の不正取得等の危険性も高まる。これは、安全保障上の危険性にもつながるものである。

4　安全対策の不十分さ

被告は、第３の冒頭で述べた「概要資料」（甲１）に記載されているように以下のような制度面・システム面での安全対策を行っていると説明している。しかし、それらは全く不十分である。

⑴　制度面の安全対策の不十分さ

ア　被告の挙げる制度面での安全対策は、

①本人確認（個人番号の確認と身元確認）を厳格に行う

②特定個人情報の取得収集等を法律で制限する

③第三者機関（特定個人情報保護委員会）が監視機関として設置される

④個人情報保護法より罰則が強化（重罰化）されている

⑤マイナポータルで自分の特定個人情報が何に使われているか調べられるというものである（甲１・９頁）

イ　しかし、①については、本人確認のための個人番号カードに、個人番号も記載されていることから、同カードが普及することと比例して、個人番号を他人に知られる危険性や、同カードの不正取得の危険性が高まるという点を考慮していない。

③の第三者機関に関しては、その権限の不十分さやマンパワーの不足が指摘されている。

②や④については、故意や過失により、法に反して個人番号等の個人情報が収集され、それらが“闇のデータベース”化される危険性を無視しているなど不十分である。

そして、そもそも、政府当局者は、個人番号は住所のようなものでありそれが漏れたこと自体では危険性が発生しない旨の認識を示している。こ

のような認識では、個人番号の名寄せのマスターキーとしての危険性が等閑視されることは必然である。

⑵　システム面の安全対策の不十分さ

ア　被告の挙げるシステム面の安全対策は、①情報の分散管理、②情報提供ネットワークシステムで特定個人情報を照会・収集する場合は、マイナンバーで照会するのではなく別の符号を用いて行う、③アクセス制御を行っている、④通信の暗号化を行っている、というものである。

イ　しかし、これらはいずれも情報提供ネットワークシステム（及びそれと接続する行政機関のデータベース等）内だけの安全対策であり、上述のように漏洩等の危険性が高い民間部門における安全対策たり得ていない。ネットワーク内だけを守るのではまったく不十分である。

以上述べてきたように、政府の述べる安全対策は極めて不十分と言わざるを得ない。これは、基本的に名寄せのマスターキーとなる、分野を超えた共通番号であるマイナンバーを利用することに基本的欠陥があることを示している。

⑶　その他の安全対策の不十分さ

ア　被告は、日本版PIA（Privacy Impact Assessment）と称する、特定個人情報保護評価制度を導入したことも、プライバシー保護のための対策としてあげている。

イ　プライバシー影響評価（Privacy Impact Assessment、略称：PIA）とは「個人情報の収集を伴う情報システムの企画、構築、改修にあたり、情報提供者のプライバシーへの影響を『事前』に評価し、情報システムの構築・運用を適正に行うことを促す一連のプロセスをいう。」「設計段階からプライバシー保護策を織り込むことにより、『公共の利益』と『個人の権利』を両立させることを目的に実施される。また、PIAを実施することにより、情報システム稼働後のプライバシーリスクを最小限に抑えること

ができ、改修とそれに伴う追加費用の発生の予防にもなる。」「PIAは、国際標準化委員会ISO TC68（金融サービスの専門員会）において２００８年４月に、ISO22307（Financial Services Privacy impact assessment）として標準ドキュメントが発行された。」ものである。

ウ　しかし、日本版PIAは、マイナンバー制度全体、特に共通番号制度を採用したことによるプライバシー侵害性については評価の対象としておらず各個別機関の特定個人情報のシステムのプライバシーに対する影響を、第三者機関による評価ではなく自己評価するものでしかない。本来のPIAとはほど遠いものである。

第５　原告らの権利・利益侵害

１　プライバシー権及び人格的自律権の侵害

⑴　憲法第１３条で保障されたプライバシー権

第４で述べた各危険性により、原告らは憲法第１３条で保障されているプライバシー権を侵害される。

プライバシー権は、極めて高度な情報化社会を迎えた今日においては、「自己情報コントロール権」として保障されなければならない。すなわち、自己の個人情報が収集、保存、利用、提供される各場面において、事前にその目的を示され、その目的のための収集・利用等について、同意権を行使する（自己決定する）ことによって、自己のプライバシーを保護できる権利である。

そして、これによって、自己の対外的なイメージをコントロールすることもできるようになるのである。

プライバシー権は、人格権の中でもっとも中核的な権利であり、また、人格的自律権、ひいては民主主義の基盤ともなる重要な権利である。そして、プライバシーの権利が一旦侵害された場合、その回復は事実上不可能である

点でも、その保護の程度は極めて高いといわなければならない。

⑵　原告らの同意なき収集・利用等による侵害

被告は、番号法に基づいているとして、原告らの同意なく、原告らの特定個人情報を収集、保存し、さらに今後広く利用、提供等を行い利活用しようとしている。

しかし、番号法による個人番号付情報の収集、保存、利用等は、あまりにも広範である。かつ、その規定の仕方は複雑であり、その利用範囲を認識することは極めて困難である。したがって、その収集等は原告らの予想を超え到底同意しがたいものであるから、原告らの自己情報コントロール権を侵害するものであって、その収集、保存等は憲法１３条に違反している。

⑶　漏洩による直接侵害の危険性

前述のように、原告らは、本制度によってマイナンバーと共に税や社会保障などに関する機微な個人情報が漏洩する危険性にさらされる。

また、原告らは、このようにして漏洩した個人情報を名寄せ・突合（データマッチング）される危険性にもさらされる。

さらに、成りすましの危険性にもさらされる。

これらにより、原告らは、自己のプライバシー情報を他人に公開されたり自分が意図しない勝手な個人像が作られたり、さらには成りすましによって誤った、もしくは歪んだ個人像を作られることによって、プライバシーを侵害される危険性にさらされている。成りすましの場合には、債務を作られるなどの経済的被害も発生しうる。

そして、一旦このような危険性が現実化した場合は、それらの個人情報の回収や修正等は極めて困難であり、侵害の回復は事実上不可能であって、その被害は極めて深刻である。

⑷　プライバシー権侵害だけに止まらない人格的自律権等の侵害（萎縮効果）

マイナンバー制度は、単にプライバシー権を侵害するというだけに止まら

ない。人格的自律権、ひいては表現の自由をも侵害し、民主主義の基盤を破壊することにもなる。

被告が作成した平成２３年６月３０日付「社会保障・税番号大綱」においても以下のような指摘がされている。

> （番号制度により）個人情報の有用性が高まれば、扱い得る情報の種類や情報の流通量が増加し、情報の漏洩・濫用の危険性も同時に高まることから、情報活用の場面における不正は防がねばならない。もしこれを疎かにするならば、国民のプライバシーの侵害や、成りすましによる深刻な被害が発生する危険性がある。仮に、様々な個人情報が、本人の意思による取捨選択と無関係に名寄せされ、統合されると、本人の意図しないところで個人の全体像が勝手に形成されることになるため、個人の自由な自己決定に基づいて行動することが困難となり、ひいては表現の自由といった権利の行使についても抑制的にならざるを得ず（萎縮効果）、民主主義の危機をも招くおそれがあるとの意見があることも看過してはならない。

このような「萎縮効果」は、人身の自由のように直接目に見えるものではないが、もっとも根源的で、かつ、深刻な影響を与えるものである。この点、ドイツの憲法裁判所では、既に１９８３年１２月１５日の「国勢調査判決」において明確に指摘されているところでもある。

⑸　性同一性障害者らの人格権侵害

第４の３で述べたように、性同一性障害者やDV被害者らは、本制度によって、以上に止まらない人格的権利や生命身体の安全を強く侵害されている。

２　制度の必要性及び費用対効果の不存在

以上のとおり、マイナンバー制度は原告らのプライバシー権等に対する著しい侵害の危険性をもたらすものであり、当然に差し止められるべきである。

また、原告らに侵害を受忍させるような制度創設の必要性は存在せず、費用対効果も著しくバランスを失しており、強い違法性を有することも明らかである。

⑴　目的の不明確さとプライバシー権侵害を受忍させる理由の不存在

ア　目的の不明確さ

被告は、元々、①正確な所得の捕捉、②真に必要としている人に必要な社会保障の給付、ということを制度創設の目的としてあげていた。

しかし、マイナンバー制度を導入しても所得を正確に捕捉することは出来ない。そのことは、被告自身が「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」（平成２３年６月３０日付「社会保障・税番号大綱」１９頁）と認めている。

また、社会保障の給付についても、結局は予算の問題となるから、マイナンバー制度を導入しても、社会保障給付が充実するという効果は認められない。むしろ、現時の社会保障費抑制・削減の大きな政策の下では、かえって、社会保障の給付対象者の収入、資産等を、マイナンバー制度を活用して厳しく審査する方向での利用の危険性すら存在する。

イ　情報化社会のインフラ及び利便性の向上等に対する必要性の不存在

被告は、マイナンバー制度は情報化社会のインフラであるとも説明している。

しかし、マイナンバー制度のような「共通番号制」を使わなくても、情報化社会のインフラは整備できる。例えば、オーストリアにおいては、分野別の番号制を基礎として、世界有数の電子政府を構築しているのである。

また、国民の利便性に関しても、ICカードと公的個人認証等を用いればほとんど解決するものであり、マイナンバー制度が必然のインフラでは

ない。

結局、プライバシー権の侵害を受忍させる制度創設の必要性は存在しないと言わなければならない。

⑵　費用対効果の不存在

ア　マイナンバー制度を構築するためには、３０００億円程度の費用がかかると言われている。地方自治体などの関連費用も入れると、その額はもっと大きくなり、このシステムの安全対策費用も入れると膨大な構築費用が必要となる。

しかも、その運用にも毎年数百億円の費用がかかり、５～６年ごとに機器の更新費用も必要となる。

イ　このような膨大な費用がかかるというのに、被告は、法案審議の時はもちろん、現在に至るまで、その費用対効果について確たる試算を提示していない。

ウ　前述のとおり、プライバシー影響評価（PIA）は、プライバシー権保護と構築後の改修等のための莫大な費用投資を防止することにその目的がある。しかし、被告は後者の観点からのPIAを行っていない。

エ　以上のとおり、マイナンバー制度は費用対効果のバランスを著しく失していると言わざるを得ず、いわゆる“ITハコモノ行政”の危険性も高いと言わざるを得ない。

３　住基ネット差止請求事件最高裁判決との関係

被告は、平成２０年３月６日に出された住基ネット差止請求事件に関する最高裁判所の判決を前提として、マイナンバー制度はその合憲とされた要件を満たしていると説明している。

しかし、マイナンバー制度では、①同制度でマイナンバーとひも付けて扱われる個人情報は極めて機微性が高いものであること、②マイナンバーが券面に印字された個人番号カードの所持が事実上強制となり、その不正取得、漏洩等

の危険性が高いこと、③個人番号の民間での収集、保存、提供等が広く義務付けられているところ、特に民間部門ではセキュリティ対策が不十分であることそして、④そもそも本制度はデータマッチングを目的とした制度であること等の点で、同最高裁判決が合憲と判断した各要素について、前提が全く異なっている。

したがって、マイナンバー制度は、最高裁判所の示した「合憲」の要件を満たしているとは到底いえない。

4　小括～差止め等の必要性及び損害賠償～

以上述べてきたように、マイナンバー制度は原告らのプライバシー等に対する侵害の危険性が極めて高い。その危険性を除去するには、マイナンバーの収集、保存、利用、提供を差し止めるしかない。よって、憲法第１３条で保障されたプライバシー権に基づき、被告に対し、マイナンバーの収集等の差止めを請求する。

さらに、プライバシー権侵害に対する原状回復として、被告が保存しているマイナンバーの削除を請求する。

原告らは、それぞれ以上述べてきたような危険性にさらされている。その精神的苦痛は金銭をもって計ることは困難であるが、その慰謝料の額は原告一人あたり１０万円を下回ることはない。

原告らは、原告ら訴訟代理人弁護士に対して本件訴訟を委任し、その費用及び報酬を支払うことを約束した。その一部金として、原告一人当たり１万円を請求する。

第６　結語

以上述べてきたように、マイナンバー制度には、国民と外国人住民のプライバシー保障を根底から掘り崩す危険性がある。

にもかかわらず、その点に関する検討はほとんど行われないまま、マイナン

バー制度の利活用が国家戦略とされ、急速に制度の具体化と利用開始が始まろうとしている。

よって、原告らは、マイナンバー制度からの離脱及び損害賠償を求めて本訴に及んだ次第である。

以　上

証　拠　方　法

甲第１号証　　マイナンバー 社会保障・番号制度概要資料

添　付　書　類

1	甲号証写し	2通
2	訴訟委任状	50通