訴　　状

２０１６年3月２４日

横浜地方裁判所民事部　御中

原告ら訴訟代理人　弁護士　小　賀　坂　徹

同　大　野　美　樹

同　石　畑　晶　彦

外

当事者の表示

当事者　別紙当事者目録記載のとおり

原告ら訴訟代理人　別紙代理人目録記載のとおり

マイナンバー（個人番号）利用差止等請求事件

訴訟物の価額　金３２１，６００，０００円

貼用印紙額　金９８６，０００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（平成二十五年五月三十一日法律第二十七号）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本訴状送達の日の翌日から支払い済みに至るまで年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。

5　第３項につき仮執行宣言。

請　求　の　原　因

第１　はじめに

近年、情報処理技術の高度化と情報化の急速な進展により、私たちは無数の情報ネットワークシステムに取り囲まれて生活している。それは私たちの生活に豊かさと利便性をもたらした反面、自己に関する情報が予期しない形で流通し、利用されるという深刻な問題を生じさせている。ネットワークシステムの中のデジタル情報は，半永久的に劣化しないで保存できること，瞬時に複製，伝達できて，短時間に爆発的に増殖させることができること，複製されても，そのことが容易には判らず，伝達先を把握することはほとんど不可能であること，書き換えも容易であり，書き換えられていることが外観上直ちには判らないこと等の特性があり，このような中で個人情報が一旦漏洩し拡散してしまえば、その損害の回復をはかることは基本的に不可能である。実際に，個人情報の大量漏洩や個人データの不正な売買といった事案が相次いで社会問題化している。さらに深刻なのは、情報ネット

ワークシステムにおいては、個人の情報はほとんど自動的にやりとりされ、当該個人ですら、その時々において自己に関する情報が、どの範囲で流通し、自己に関する他の情報とどこまで結合されて自己の統合された像が構築されているかを捕捉することさえ不可能であることである。したがって、自己の情報をコントロールすることそのものが困難、ないし不可能となっているのであり、ネットワークシステムへのアクセスは、こうしたリスクと直面することが不可避なものとなっている。

このような中、私たちは、日常的に、情報ネットワークシステムのもたらす利便性と、私生活の平穏が害され、人格的自律が阻害されるリスクとを天秤にかけながら、基本的に個々人の意思に基づいて、どの情報ネットワークシステムにアクセスするのかを判断しているのである。

しかし、本年１月から運用が開始された「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」により、原告らは自らの意思と無関係にあらゆる情報に紐づけすることが可能な１２桁の個人番号（マイナンバー）を付番され、自らの意思と無関係にマイナンバー制度という巨大な情報ネットワークシステムに取り込まれてしまっている。後に述べるとおり、マイナンバー制度は個人情報の漏洩の危険を本質的に内包しているものであり、原告らはその危険に怯えながら生活せざるを得ない状況に追い込まれている。実際、本年１月に運用が開始されてまだ３ヶ月にも満たないが、事故や不具合は後を絶たず、そのことが連日のように報道されている。しかもこの危険（リスク）は、システムの正常な運用によってもたらされるものから、システム運用上の不具合によって意図せずもたらされるもの、システム運用に携わる公務員等の故意または過失によってもたらされるもの、システム外部からの違法な働きかけ等によってもたらされるも

のに至るまで、種々のものがありうる。どうして原告らは、自らの意思と無関係にこのような深刻な危険（リスク）を享受することを強いられなければならないのであろうか。まさに原告らのプライバシー権を中心とした人格権が侵されていると言わざるを得ない。

本訴訟は、マイナンバー制度がもたらす原告らの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、また「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の内容とその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”侵害のみに止まらず、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”重大な危険性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・考察する必要のある問題である。しかるに、国は、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は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るから、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的問題となる前である今のうちに差し止めて、それらの弊害が発生しないように、プライバシー保障の観点からしっかりと見直すことが是非とも必要である。

裁判所におかれては、現代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、諸外国の実情や弊害、知見をも踏まえて、慎重かつ事案の本質に迫る審理を行うことを求めるものである。

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（平成二十五年五月三十一日法律第二十七号）

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、当事者目録記載の住所欄記載の市区町村に住民票をおいている者である。原告らは、行政手続における特定の個人を識別するための番号の利用等に関する法律（平成二十五年五月三十一日法律第二十七号）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、２０１６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、個人番号を収集・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もいる。

第3　マイナンバー制度の概要とその特徴

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・税番号制度　概要資料」（２０１５年１１月版）（甲１）記載のとおりと説明している。

この制度の特徴は、以下の点である。

① 国民と外国人住民（および法人）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、災害対策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、本人確認のために、マイナンバーと、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、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 ２０１７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

第３で述べたように、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って、情報の価値が高いこと、

③　近い将来、更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は高く、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いるから、将来の危険性は更に高くなる。

したがって、原告らのプライバシー等に対する危険性は、以下に述べるように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

(1)　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

第３で述べたとおり、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、いたるところに特定個人情報データベースができることになる。総務省統計局によると、２０１２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５５８３万７０

００人とされるから、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)に応じた特定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　民間部門からの特定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、２０１６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、未だ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社当たり平均約１０９万円もの費用がかかるとされている（２０１５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、２０１５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・保管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得ない。

ウ　行政部門からの特定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、２０１５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。同機構では、番号法に基づく特定個人情報保護評価（後述）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、上記流出を生じさせ

た。また、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」であった。しかし、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。

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２０００万人分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　特定個人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ならば、上記の各所において、官民を問わずに、大量の特定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の存在は明らかである。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。

(2)　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、①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、②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。

漏洩した特定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、後述の成りすましをされることにより、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）

更に危険性が高いのは、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。

（ア）番号法に定められた行政機関等においては、２０１７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（別表記載事務の拡大等）により、今後更に高まる。

（イ）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（番号法第１９条第１２号）。近時、例えば、警視庁外事課が、「テロ対策」を口実に、現に犯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が、このような活動でも、「刑事事件の捜査」という名目を付けるならば、警察は、官民の各所に対して、特定個人情報の収集要求をすることができることになるのである。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（２０１６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）。

（ウ）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。

(3)　成りすましの危険性

ア　現実世界のなりすまし

（ア）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。従って、その情報を利用すれば、その人に成りすますことが容易になる。

（イ）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。そのこともあって、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。

この前例から見ても、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なりすましの危険性も高いとい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も出来るが、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いうることになる。

（ウ）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、２０１７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のぞき見たり、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、一旦成りすまされた場合は、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　マイナンバー制度の利用拡大による近い将来における危険性の増大

（１）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）。被告は、番号法の附則上は、施行３年後の見直しとなっているにもかかわらず、施行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、利用拡大法を成立させている（２０１５年９月３日）。

（２）その一環として、被告は、個人番号カードを、身分証明証、健康

保険証、印鑑登録証などとワンカード化することを促進して、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パーセントへのアップ時に、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いるのであり、同カードを身分証明証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、危険性は極めて高まると言わなければならない。

（３）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　その他、性同一性障害者、ペンネームの使用者、ストーカー被害者等の危険性

以上に述べた全員に対する危険性の他、性同一性障害者に関しては、生活してゆくために、雇用先などに対し、戸籍上の性を相手方に明らかにすることを強制される。そのため、精神的に耐えがたい苦痛を受けざるを得ない。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（住民票上の）氏名を告知することを強制される。これらの者にとっては、プライバシーの開示に止まらない、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、住民票上の住所を告知するこ

とを強制されことになるし、ＤＶ被害者等を支援する弁護士も、事務所住所ではなく、自宅住所を取引先等に告知することを強制される。これらの者にとっては、自宅住所を知られることにより、業務妨害の危険性に止まらず生命身体の危険性すら発生しうる。

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、政府要人や、防衛産業の技術者や自衛隊関係者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　安全対策の不十分性

被告は、第３で述べた「概要資料」にあるように、以下のような、(1) 制度面、(2) システム面での安全対策を図っていると主張している。しかし、それらは全く不十分である。

（１）制度面の安全対策

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を高めるという点を考慮していない。また、③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。

（２）システム面の安全対策

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いわざるを得ない。

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ものである。

(3)　その他の安全対策（日本版ＰＩＡ）

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委員会)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、人格的自律権の侵害

（１）憲法第１３条で保障されたプライバシー権

第４記載の各危険性により、原告らは、憲法第１３条で保障された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、学説上、または判例上「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とされてきた。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。

さらに冒頭述べた通り、現代の情報ネットワークシステムにおいては、個人の情報はほとんど自動的にやりとりされ、当該個人ですら、その時々において自己に関する情報が、どの範囲で流通し、自己に関する他の情報とどこまで結合されて自己の統合された像が構築されているかを捕捉することさえ不可能であり、したがって、自己の情報をコントロールすることそのものが困難、ないし不可能となっている。このような状況においては、どのようなネットワークシステムに接続するのか、接続されるのかということこそが重要な意味を持っている。この観点からすれば、現代におけるプライバシー権の内容は、「自己の意思に反して、個人に関する情報を情報ネットワークシステムに接続されない自由」までをも包含するものと考える必要がある。このように観点に立てば、原告らが自らの意思と無関係にあらゆる情報に紐づけすることが可能な個人番号（マイナンバー）を付番され、自らの意思と無関係に巨大な情報ネットワークシステムに取り込まれてしまったことそのものが、原告らのプライバシー権の重大な侵害だといえるのである。

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。

（２）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・保管し、さらに今後広く利用、提供等を行ない利活用しようとしている。

しかし、番号法の収集・保管、利用等は、あまりにも広範であ

り、かつ、その規定の仕方は複雑であるため、その利用範囲を認識することは極めて困難であり、そもそも原告らの同意を観念することができない。したがって、その収集等は原告らのプライバシー権を侵害するものであって、その収集・保管等は憲法第１３条に違反している。

（３）　漏洩による、直接侵害の危険性

ア　原告らは、前述のように、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。

イ　更に原告らは、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。

ウ　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。なお、成りすましの場合は、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。

（４）プライバシー権侵害だけに止まらない人格権自律権等の侵害（萎縮効果）

マイナンバー制度は、単にプライバシー権侵害というだけには止まらない、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、２０１１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、結合されると、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。

（５）性同一性障害者らの人格権侵害

第４、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性を強く侵害されている。

２　制度の必要性、費用対効果の不存在

以上のように、マイナンバー制度には、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るばかりでなく、制度創設の必要性等も存しないし、費用対効果も著しくバランスを失している。

(1)　目的の不明確性

ア　正確な所得捕捉と必要な人に対する社会保障給付

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を実現するということを、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、正確な所得の捕捉は出来ない。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」（２０１１年６月３０日付「社会保障・税番号大綱１９頁）と述べて、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、資産等について、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する。

イ　情報化社会のインフラ、利便性の向上等

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主張している。

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、制度創設の必要性は存しないと言わざるをえない。

(2) 費用対効果の不明確性

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れば、もっと増大するし、このシステムの安全対策費用等も入れるならば、膨大な構築費用を要する。しかも、その運用にも毎年数百億円の費用がかかる。５～６年ごとの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 前述のように、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。

被告は、後者の目的の観点からのＰＩＡを行ってもいない。

エ 以上より、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 ２００８年３月６日住基ネット差止最高裁判決との関係

（１）被告は、２００８年３月６日の住基ネット差止請求事件に関する最高裁判決を前提として、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旨主張している。

（２）しかし、マイナンバー制度は、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が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・保管、提供等が広く義務づ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性であること、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から、マイナンバー制度が「合憲」の要件を満たしているとは到底評価し得ない。

4　小括～差し止め等の必要性及び損害

(1)　以上述べてきたように、マイナンバー制度は、原告らに対するプライバシー等に対する侵害の危険性が極めて高く、また、制度の必要性等も存しない。それ故、その危険性を除去及び予防するには、原告らのマイナンバーの収集・保管・利用・提供を差し止めるしかない。

(2)　また、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が必要である。

(3)　さらに、原告らは、それぞれ以上述べてきたように自己の意思に反して巨大情報ネットワークシステムであるマイナンバー制度に組み込まれプライバシー権を侵害され、かつ個人情報の漏洩の危険にさらされてもいる。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、その金額は、少なくとも原告一人当たり金１０万円を下らない。

(4)　原告らは、原告ら代理人弁護士に対して、本件訴訟を委任し、その費用及び慰謝料額の１割相当額の報酬を支払うことを約した。

第６　結語

よって、原告らは被告に対し、

①　プライバシー権に基づく妨害排除・妨害予防請求として、マイナンバーの収集、保存、利用及び提供の差し止め、並びに被告が保存

している原告らのマイナンバーの削除を請求するとともに、

② 国家賠償法に基づく損害賠償請求として、金１１万円及びこれに対する本訴状送達の日の翌日から支払い済みまで年５分の割合による遅延損害金の支払いを求める。

以上

証　拠　方　法

甲第１号証　「マイナンバー　社会保障・税番号制度　概要資料」
（２０１５年１１月版）

添　付　書　類

１	甲号証（写し）	１通
２	訴訟委任状	２０１通