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（４）

２０１８年（平成３０年）２月２０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

第１　原告らのこれまでの主張の骨子

原告らは、マイナンバー制度・システムの危険性を論じるにあたり、これまで原告らが主張してきた被侵害権利利益等の骨子を、改めて以下のようにまとめて主張する。

１　被侵害権利利益について

(1)　自己情報コントロール権

原告らは、訴状において、侵害される権利について、「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、それによって、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」と主張した（訴状 15 頁以下・なお、準備書面(1)で自己情報コントロール権の根拠と内容等について主張した）。

(2)　自由権

原告らは、準備書面(3)において、私生活上の自由の一つとして、個人に関する情報をみだりに第三者に開示または公表されない自由はもとより、みだりに収集・保管・利用されない自由が保障されていると主張した（17 頁等）。

(3)　本件において、原告らの主張する被侵害権利利益は、「自己情報コントロール権」であるが、その中核的な内容において、(2)に述べた自由権が含まれるものである。すなわち、「みだりに」とは、原則として、その個人情報(プライバシーにかかわる情報)を収集等される際に、本人の同意（もしくは同意に真に代わりうるもの）によって、それらをコントロールして、自己のプライバシーを保護できる権利を中核とするものである。住基ネットに関する平成２０年３月６日最高裁判決が引用する昭和４４年１２月２４日最高裁大法廷判決（京都府学連事件判決）が、「個人の私生活上の自由」の一つとして、「その承諾なしにみだりにその姿態・容ぼうを撮影されない自由」と判示しているのは、その趣旨を含むものと解するべきである。

２　侵害態様について

(1)　原告らは、訴状 16 頁以下において、以下のａ～ｄの侵害態様について主張した。

ａ：原告らの同意なき収集・利用等による侵害

ｂ：漏洩による直接侵害の危険性

①漏洩

②データマッチング

③なりすまし

ｃ：プライバシー権侵害だけにとどまらない人格権自律権等の侵害

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

ｄ：性同一性障害者らの人格権侵害　性同一性障害者、ＤＶ被害者ら

(2)　このうち、ｂについて、訴状では「漏洩による」としているが、「漏洩」の場合にとどまらず、準備書面(3)の 8 頁で主張したように、②に関しては、利用事務の拡大や、そのような利活用を制限する原則的な基準が存しないこと、法律が改正されれば、これらのすべての情報が一元的にデータマッチングされてしまう危険性が存すること（例えばテロ対策の名目で）なども含むものである。

また、同じく準備書面(3)の 24 頁以下で主張したように、現代的プロファイリングの危険性についても主張するものである。「マイナンバー(制度)はまさに、現代的プロファイリングのインフラであり、マイナンバーを活用した場合の現代的プロファイリングによる個人の権利侵害の危険性は極めて高い」とも主張するものである。

３　違憲性判断基準

原告らは、平成２０年の住基ネット事件最高裁判決の基準を基に、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ると主張するものである。

このような事態に至れば、「個人の尊厳ないし人格的自律の存在が脅かされるような態様で個人情報が取り扱われ、又はその具体的な危険性がある場合」にあたる（準備書面(3)の 19 頁）。

第２　制度（システム）の危険性（「不備」）について

以下、(1)マイナンバー制度のどの範囲における「不備」が問題になるのか、そして、(2)どこに、どのような「不備」が存するのか、等について主張する。

１　制度（システム）の不備は、どの範囲で認められるか

準備書面(3)の２・１頁等で主張したように、マイナンバー制度（システム）の危険性を考える場合、情報提供ネットワークシステム（以下、「情報提供ｎｗｓ」ともいう。）だけを対象と考えるのは誤りである。何故なら、この制度（システム）は、住基ネット制度（システム）における住民票コードとは異なり、マイナンバーが、民－民－官で利用されるなど、民間部門での利用も前提としたものであるからである。したがって、マイナンバー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。

２　根本的な構造的「不備」である「共通番号」制度

(1)　マイナンバー制度（システム）の危険性を考えるに当たって、第１に問題となるのは、この制度が「共通番号制度」である点である。

事務分野毎に別の個人識別番号を用いる「分野別番号制」であれば、仮に複数の分野の個人データを名寄せ突合（以下、「データマッチング」ともいう。）しようとしても、氏名・住所・生年月日・性別等で行わなければならず、手間暇がかかる上に、正確に行うことができない。何故なら、氏名、住所（場合によっては性別）は変更がありうる上、氏名等に変更がなくとも、「斎藤」と「斉藤」など、漢字の同一性を確保することができないから、これらによる確実な名寄せ突合は困難であるからである。これに対し、事務分野を超えて同一の個人識別番号を用いる「共通番号制」の場合は、番号だけで、容易・確実に名寄せ突合ができる。

(2)　この特性により、共通番号のついた個人データは、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。現にマーケッティング分野ではビッグデータの処理による消費者のプロファイリングが盛んに行われている。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。

(3)　このような共通番号であるマイナンバーの危険性については被告も認めるところである。

すなわち、被告は、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も、

「番号制度において想定し得る客観的な危険性としては、

①　個人番号を用いた個人情報の追跡・名寄せ・突合が行われ、集積・集約された個人方法が外部に漏えいし得る危険性、

②　個人番号の不正利用（例：他人の個人番号を用いた成りすまし）等により財産その他の被害が発生し得る危険性、

③　国家により個人の様々な個人情報が個人番号をキーに名寄せ・突合されて一元管理され得る危険性のほか、集積・集約された個人情報によって本人が意図しない形の個人像が構築されたり、特定の個人が選別されて差別的に取り扱われ得る危険性」

があることは認めている。

以上を前提として、以下、マイナンバー制度の「不備」ないし欠陥を指摘する。

３　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

番号法は、その１条で法の目的を、①「行政運営の効率化」、②「行政分野におけるより公正な給付と負担の確保」、③「国民」の「利便性の向上」であるとし、その目的の実現を、「個人番号及び法人番号の有する特定の個人及び法人その他の団体を識別する機能を活用し、並びに当該機能によって異なる分野に属する情報を照合してこれらが同一の者に係るものであるかどうかを確認することができるものとして整備された情報システムを運用」することで図るとしている。

情報提供 nws（番号法２１条）はこの「情報システム」に該当するものである。同システムで情報連携可能な事務は１８００以上あり、情報連携を行うに際し、情報照会者及び情報提供者は、直接に情報提供の求めを行うのではなく、情報提供 nws を介することを原則とする(番号法２１条２項)。このように、情報提供 nws 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 nws における情報連携にはマイナンバーは使われない

上記のように、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が一緒に保存されている（個人情報とマイナンバーの紐付け）。

ところが、制度の最大の「売り」である情報提供 nws 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）。

そうであるとすると、当然、次の疑問が出て来る。

情報連携に共通番号であるマイナンバーを使わないのであれば、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する合理的理由はないのではないか、という疑問である。

(3)　原告の求釈明と被告の回答

この点について、原告は次のように求釈明を行った（２０１６（平成２８）

年１１月１５日付け求釈明書５～６頁）。

「情報提供ｎｗｓの目的は、分野を超えて、個人データを容易確実に連携させることにあると考えられるが、乙１、8 頁の図（マイナンバー制度における情報連携の概要）にあるように、同システムにおいて、省庁を越えた情報連携には「機関別符号」（と機関別符号同士をひも付ける情報連携用符号）を用いている。そうすると、個人番号がなくても情報連携自体は出来ると考えられる。また、特定個人情報の保護の観点からは、各省庁に個人番号を保存しておかない方が良いと考えられる（折角、情報提供ｎｗｓにおいて分野別＝機関別番号制にした意味が没却されて、いわば「頭隠して尻隠さず」状態となり、各省庁からの個人番号付きの個人データが大量漏洩する等の危険性が生じる）。

そこで、各省庁のデータベースでマイナンバーを保存しておく理由について明らかにするよう求める。」

これに対し、被告の回答の以下のものであった（平成２９年１月２４日付け求釈明に対する回答書（２）１４頁）。

「社会保障・税分野において情報提供ネットワークシステムによる情報連携を行うためには、個人を悉皆性（住民票を有する全員に付番）を有する番号によって特定するため各情報提供者のシステム等において個人番号を保有し、情報照会又は情報提供を行うことを可能としておくことが必要である」。

この被告の回答は、「情報連携に必要だから保有するのだ」と言っているに過ぎない。「情報連携に使わないのであれば何故保有するのか」という原告の質問の回答になっていない。

(4)　「使われない共通番号」という根本的な「不備」

しかし、この問題は、制度の根本的な不備というべき問題であり、このような回答でやり過ごせる問題ではない。

マイナンバーは、その共通番号たる性質の故、プライバシー権に対する重大な脅威となり得る制度であり、前記のようにその危険性は被告自身も認めるところである。したがって、マイナンバー制度は、個人のプライバシー権を制約

するものであり、違憲審査に服さなければならない。

すなわち、仮に①「行政運営の効率化」、②「行政分野におけるより公正な給付と負担の確保」、③「国民」の「利便性の向上」（番号法１条）といった目的に正当な理由があるとしても（なお、その正当性についても疑問があることはすでに指摘したとおりである（訴状１８頁等））、目的の達成ために、より制限的でない他の選びうる手段がある場合は、前記の「システム技術上または法制度上の不備」にあたり、違憲となるというべきである。

前記のように、情報提供 nws においては、情報連携に機関別符号（情報提供用個人識別符号（番号法施行令２０条））を用いることになっており、マイナンバーは使われない。

そして、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日付け求釈明書参考資料２の１－１、平成２９年１月２４日付け求釈明に対する回答書（２）８頁）。したがって、情報提供 nws 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。

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、より制限的でない方法（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。

別の言い方をすれば、制度の中核的なシステムである情報連携 nws においてマイナンバーは「使われない共通番号」なのであり、先に述べた共通番号の危険性に鑑みれば、マイナンバー制度には、「システム技術上または法制度上の不備」があるというべきである。

４　民間も含めたセキュリティを高度に保つことは困難であるという「不備」

(1)　準備書面(3)の１１頁～１３頁において、その一部を既に主張しているとこ

ろであるが、マイナンバー制度は、民ー民ー官を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）であるから、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。

ところが、民ー民ー官の中間の民（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。

(2) 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、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。

しかるに、国は、上述したように危険性の高い「共通番号」であるマイナンバーの利用を法で強制している。

(3) 被告は、「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」などと主張する（第２準備書面１８頁）が、後述のように、人為的ミスは必ず起きるものであり、それをも想定したセキュリティ対策を取っておく必要があるものである。そのような対策がとられていないことは、番号制度自体の制度的不備の問題である。

(4) 本訴訟の原告の中には、個人事業者や税理士など、上記中間の「民」として他人のマイナンバーの「安全管理」をする義務を課せられた者もおり、それらの原告は、自己のプライバシーを侵害される危険性にさらされている他、他人のマイナンバーを管理させられることにより、現に従前とは質を異にする義務

を課せられるという精神的侵害を被り、かつ、将来的には、仮に漏洩事故等を発生させた場合などには業務が成り立たなくなったり、損害賠償を受けたりするという財産権に対する侵害の危険性にもさらされているのである。

(5)　原告ら準備書面(1)の 17 頁で摘示したように、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（「第２次情報セキュリティ基本計画」（同年２月３日付）。

このような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。

(6)　なお、マイナンバー制度（システム）において、このような安全対策がとられていない背景には、既に主張したように、プライバシー・バイ・デザイン（ＰｂＤ）の思想（設計段階から、デフォルトでプライバシーが保障されるようにすることなど）に基づいた設計が行われていないことがある。

そして、制度構築の前に、この制度を創ることにより、プライバシーにどのような影響を与えるかという、本来の意味におけるプライバシー影響評価（プライバシー・インパクト・アセスメント・ＰＩＡ）が行われていないことも存するといわなければならない。環境影響評価が、工場等を建築する前に環境に対する影響を評価することと対比して考えるならば、被告の主張する「特定個人情報保護評価」は本来の意味におけるプライバシー影響評価ではない。

(7)　具体的な事故事例については、11 で後述する。

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」

(1)　マイナンバーは秘密にしておくべき情報である。この点は、番号法でその

入手等を厳しく規制し、罰則を設けていることから、争いのない事実である。

(2)　性別も、性同一性障害者にとっては重大なプライバシー情報である。さらに、住所も、ストーカーやＤＶ被害者にとっては、生命にもかかわる重大な個人情報として保護されるべき情報である。この点も、今や争いはないであろう。

(3)　このマイナンバーや性別、住所を券面に記載しておきながら、そのカードを日常的に持ち歩き、利用させようとしている制度と施策は、マイナンバー等の情報漏洩を推奨しているようなものであり、明らかに構造的な欠陥、「不備」であるといわなければならない。

(4)　被告国は、個人番号カードの利活用促進政策をとっている。従前から主張しているように、例えば、健康保険証との一体化、身分証明書との一体化、印鑑登録カードとの一体化、「市民カード」との一体化、「ポイントカード」としての利用等々である（甲１６）。

(5)　一枚のカードで、本人確認と番号確認ができる上、健康保険証やポイントカードなどの機能も持たせることができるならば、利便性を追求する人にとっては利便性が向上する面は確かに存するであろう。

　しかし、「利便性」はそのまま危険性に直結する。特に、高齢者や障がい者などに多い安全管理ができない人にとっては、情報の漏洩や不正利用の危険性が高くなるのであり、そのような人たちの利用を想定しない個人番号カードの安全対策である場合は、制度的な不備が存するといわなければならない。

(6)　この点を検討するならば、例えば以下の点があげられる。

ア　通常の印鑑登録カードは、もともと通常持ち歩かないものである上に、券面に氏名や住所等が記載されておらず、それが安全対策となっているが、個人番号カードでは、このような安全対策がなくなることになる。

イ　健康保険証との一体化が実現すれば、患者は受診時にパスワードを打ち込むことが必要となる。そうするとパスワードまで漏れてしまう可能性が

高くなってしまう。また、高齢者など、パスワードを適切に管理することが困難な人も多く、利用者の利便性の向上も図られない。

ウ　被告は、「性同一性障害者」に対する対策としては、性別の部分などをカードカバーで隠すという「対策」がとられていると主張するが、簡単にのぞき見されてしまうものであり、このような対策では不十分である。

また、被告は、健康保険証との一本化としての利用の際に「性別」は必要である旨反論するが、ネットワーク経由で被保険者資格を確認するシステムにするならば、その際に「性別」を確認することができるようにするなどの対策をとれば済む話である。

エ　本人確認の際には、「性別」まで必要ないことは、その目的で最も利用されている運転免許証に「性別」記載がないことからも明らかである。

オ　マイナンバーの確認が必要な場面など、年に1回あるかどうかであるから、本人確認とマイナンバー確認が1枚のカードでできるという「利便性」など、その危険性に比べれば全くないと評価できる。また、かつての住基カードの場合は、免許証等の顔写真付き身分証明書を有しない人が身分証明書代わりに取得した例が相当数存したが、券面に住民票コードの記載がなかったため、その点については安全であった。これに対し、個人番号カードの場合、仮に番号制度自体が必要との立場に立っても、利便性と安全性のバランスを考えるならば、本人確認と番号確認は2枚のカードに分けるなどの対策をとることができたにもかかわらず、そのような対策をとっていない。個人番号カードを取得する人の中にも身分証明書として取得する高齢者などが相当の割合で存すると考えられるのであり、被告は、それらの人たちが安全に持ち運び、利用できるカードを設計する必要があったのである。にもかかわらず、健康保険証やポイントカードなどと一体化してしまったならば、マイナンバーから本人確認4情報、顔写真までのすべての情報が券面に記載されたカードを日常的に持ち歩くことを事実上強制される結果となる。

その意味で、この個人番号カードの制度設計は、利便性に偏りすぎて、

安全性をないがしろにしているという重大な「不備」があるといわなければならない。

６　行政のシステムにおける「不備」

(1)　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

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）からも明らかなように、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)　ところで、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ー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)　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）に対する修正プログラムの適用（パッチあて）は、パッチの提供があっても、直ちには行われない。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。

【求釈明】

１　被告は、日本年金機構の全国の年金事務所、事務センター等に配置され、

年金機構職員等が基幹系業務等（年金記録の照会や届書等の入力処理等）に用いる端末は、平成２８年１０月時点で２万５４３８台である旨釈明しているが、この端末と、同機構における情報提供ｎｗｓによる情報連携が開始した場合の特定個人情報についての照会が可能となる端末とは同一であるのか。

仮に異なる場合は、照会が可能となる端末は何台位配置され、どのように上記端末と連携する予定か。

２　日本年金機構に限らず、マイナンバーシステムの機器に対するパッチあての状況について、明らかにされたい。

(4)　「のぞき見」の危険性を防止できない不備

前述したように、例えば、日本年金機構には２万５千台余の端末がある。

そして、過去には、著名人の個人情報の覗き見事件等が発生している。

業務の効率性を考えると、大量の日常業務の中に少数の「のぞき見」を紛れ込まされた場合に、その不正を発見することは非常に困難である。

【求釈明】

３　のぞき見防止のための、システム的な対策はどのようなものが存するのか。

７　警察によるマイナンバーを利用した個人情報収集に制約がない「不備」

(1)　マイナンバーによって個人情報を正確にマッチングできるということは、警察が、捜査活動及び情報収集活動において、対象とする個人の情報を、マイナンバーを鍵として、正確に収集できることにつながる。

次に述べるように、警察は、捜査活動もさることながら、警察法２条１項に基づく活動と主張して犯罪性のない市民活動に携わる個人情報を秘密裡に収集し、データベース化している。このような警察の活動について、法律や条例による制限はほとんど存しない。また、司法もこのような情報収集活動及びデータベース化を違法としていない。個人情報保護の観点から警察が保有する個人情報全般（捜査及び情報収集活動によるものを含む）を監督する独立した第三者機関も存しない。

このような状況で、国家戦略としてマイナンバーの利用範囲が拡大され（甲

１７）、各種行政手続のみならず、銀行口座情報や医療・健康情報、さらに将来的にはクレジットカード利用情報等と結びつくようになると、警察は、マイナンバーを鍵として、より正確かつ容易に、対象とする個人の情報を収集し、データベース化出来ることになり、実質上無制約の個人情報収集活動がますます肥大化する。

独立した監督機関による監督も法律による有効な制限もないままに、警察によるかかる活動が肥大化することは、憲法１３条が個人のプライバシーを保障したことを無効化するものであって、憲法上許容されないというべきである。

(2)　警察の個人情報収集活動

現在でも、警察による、犯罪と関係の無い市民の個人情報収集活動が秘密裡に行われており、何らかのきっかけでこの活動が発覚して初めて市民が知るという実態がある。

ア　ムスリム情報収集事件

（ア）警察が、テロ対策名目で、主に日本国内にいるイスラム教徒（ムスリム）の個人情報を調べ上げ、かつ、データベース化していたことが、インターネット上に流出した資料から明らかになった。

流出資料から、名簿を作成されたムスリムは、東京都内だけでも１万３０００人近くに上る。これは、東京都内在住のムスリムの約９割にあたる人数で、警察による、無差別・大規模な監視活動であることがわかった。警察は、ムスリム各人の経営する自動車販売店、食料品店、飲食店ほかあらゆる事業所を調べ上げ、取引先と顧客の動向を掴み、 関連する銀行口座の取引履歴まで「任意に」入手していた。「入国在留関係」に関する情報として、入国管理局等の公的機関に回答を求めないとわからないはずの情報（上陸年月日、旅券番号、旅券発行年月日、在留資格、本国住所、在留期間、登録年月日など）も記載され、日本における住所歴や通学・通勤先歴も、「住所歴学歴職歴」として記載されていた。個人情報を調べた結果、ムスリムではあるがおよそ犯罪とは無縁の人物であっても、データベースから削除されることはなかった。

東京地方裁判所は、平成２６年１月１５日判決において、このような警察の情報収集活動を適法と判断し、この判断は東京高等裁判所・最高裁判所によって追認された。

すなわち、警察が、ムスリム全員を対象に個人情報を収集してデータベース化し、犯罪と関係がないと判明しても情報を廃棄することなく保有し続けたことを、裁判所は、テロ対策目的であれば適法であると認めたのである。

（イ）「テロ対策」目的で、警察による情報収集活動が適法化される場合はあり得るとしても、イスラム教徒であることに着目した程度で、ムスリムほぼ全員の個人情報を公権力たる警察が収集していることが明らかとなった。しかも、公的機関や民間人を含め、大多数が警察の情報収集活動に「任意に」協力した結果、調査対象とされたムスリム各個人について、履歴書のような詳しいデータベースが作成されていたのである。

（ウ）このようなことが認められるならば、当然、監視・情報収集の対象となるムスリムの交友関係等も情報収集され、データベース化されることになる。上述したように、そこで収集される情報には制限がないのであるから、原告ら国民全員（当然、裁判官も含まれる）、外国人住民全員が対象となりうる。そして、その結果、プライバシーが侵害されるだけでなく、当然、「監視対象とならないよう」ムスリムと交際することは自粛しよう、ムスリム寺院等へ近寄ることは自粛しようという「萎縮効果」が発生する危険性は明らかである。

イ　大垣警察署警備課による市民監視

（ア）中部電力の子会社が、岐阜県大垣市内に風力発電施設を建設することを計画していることを自治会の配付資料で知った住民が、地域で風力発電事業の勉強会を企画して複数回開催し、また、同子会社主催の現地説明会にも参加した。

このような住民の動きについて、大垣警察署警備課は、わざわざ同子会社を呼び出して、勉強会に参加した住民の一部が、過去に別の自然保護運動を行ったことがあることや、勉強会に参加していない運動家の市民の氏名、地

元の法律事務所の名前等を挙げて、「大々的な市民運動へ展開すると御社の事業も進まないことになりかねない。」「身に危険を感じた場合はすぐに１１０番してください。」などと、同子会社に「アドバイス」した。

（イ）大垣署と同子会社との情報交換の内容を入手した新聞社がこれを報じたことから、大垣署が、何ら犯罪性のない住民の勉強会について、一私企業の新規事業に反対運動を起こすかもしれないと想像して、活動に加わりそうな個人の学歴・病歴等の個人情報を収集し、秘密裡に当該私企業に提供していたことが明らかになった。

（ウ）岐阜県警は、住民らの問い合わせに対して、このような活動も、警察法２条１項に基づく情報収集活動として適法であると回答した。岐阜県警のこのような主張からすれば、警察は、およそ犯罪性の認められない市民活動であっても、これに参加する者の個人情報を収集することができ、収集した情報を何ら制約なく保存・利用・提供できると考えて運用していることになる。

（エ）このようなことが認められるならば、住民のプライバシーが侵害されるだけでなく、住民運動等への参加に対する萎縮効果が発生することは必然である。

(3)　法律及び条例による制限が実効的ではないことについて

以上のように、警察は、犯罪捜査のみならず、上記各事案のような犯罪性のない個人の情報収集活動を秘密裡に行い、警察法２条１項で正当化している。同法は権限法ではなく組織法に過ぎず、同条項で情報収集・保管・利用の範囲を画しているわけでもないから、事実上、警察による個人情報収集活動は法律及び条例による制限はないに等しい。

すなわち、法律による制限として、警察庁に適用される行政機関個人情報保護法があるが、捜査活動等により収集された個人情報については総務大臣の監督を受けず（同法１０条２項１号、２号）、「犯罪の予防、鎮圧又は捜査、公訴の維持、刑の執行その他の公共の安全と秩序の維持に支障を及ぼすおそれがある」情報については、自己情報開示請求の対象とはならず（同法１４条５号）、警察庁が保有する自己情報の存在及び内容を個人が確認することもできない。

また、各都道府県の個人情報保護条例は、一応、警察にも適用され、東京都でも、個人情報の保護に関する条例は警視庁も対象となるが、個人情報の収集制限に関する規定（４条２項・３項）は「犯罪の予防、鎮圧又は捜査、被疑者の逮捕､交通の取締りその他の公共の安全と秩序の維持に係る事務については、適用しない」（４条４項）とされていることから、「公共の安全と秩序に係る事務」の一環として行われるであろう上記各事案のような情報収集活動には、同条例は適用されない。また、このような情報活動で得た情報については、自己情報開示請求の対象にもならず（１６条４号）、警視庁が保有する自己情報の存在及び内容を確認することもできない。

結局、日本には、警察の情報収集活動を規制する法律や条例は事実上存在せず、また、独立性を有する国の第三者機関として、個人情報保護委員会が設置されたが、同委員会の監督権限も、刑事事件に関する警察の利用等には及んでいない（番号法１９条１４号、３６条）。

このように、警察が行う個人情報の収集については、実効的な制限や監督がないまま、恣意的な情報収集活動が是正されることもなく、放置されている状況にある。

(4)　ところで、原告が「例えば、警察において、被疑事件の捜査のため、捜査関係事項照会で『これこれの個人番号の甲野太郎の税金関係情報を照会する」というような使い方はできないということであるのか。」と求釈明をしたことに対して、被告は、第２準備書面において、刑事事件の捜査は個人番号利用事務ではないため、そもそも個人番号の利用ができないから、原告らのいうような照会を行うことはできないと回答する（２１頁～２２頁）。

しかし、福島みずほ参議院議員の「番号法、個人情報保護法に関する質問主意書」（第１８９回国会(常会)質問主意書質問第１３６号(平成 27 年 5 月 22 日)に対する答弁書第１３６号（平成 27 年 6 月 2 日））（甲１８）において、

「捜査関係事項照会の際に、個人番号により照会することが認められるか、政府の見解を示されたい。」という質問に対して、政府は、「お尋ねの『捜査関係事項照会の際に、個人番号により照会すること』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（平成二十五年法律第二十七号。以下「法」という。）第十九条第十二号に該当する適法な特定個人情報の提供になり得る。」と答弁されている。

（注：現在の 14 号は、当時 12 号であった）

この２つの回答の間には重大な齟齬があるといわなければならない。

上記のとおり、刑事事件の捜査名目であれば番号法による明文の制限はなく、また、個人情報保護条例等の適用も除外されることからすれば、マイナンバーを捜査や情報収集活動に利用する危険性が高い。

今後、マイナンバーの利活用が進められて、個人の様々な情報がマイナンバーと紐付けられる事態になったときに、例えば、対象者の戸籍情報や住所等の住民票記載情報、預金口座情報・職歴情報・健康保険に関する情報は、マイナンバーを鍵として収集することで、正確かつ迅速に集められる。そうなると、ムスリム情報収集事件のように、対象者ごとの個人情報データベースの作成もより容易になる一方、かかる警察の情報収集活動について実効的な法律上の制限及び監督機関はない。

これは重大な不備である。

【求釈明】

４　例えば、ある民間会社から、12 桁の番号付きの個人データが大量に押収され、番号法５１条違反の疑いが持たれた場合、警察としては、発見された個人の個人番号は何かを照会して、その個人番号と発見された 12 桁の番号との同一性や、相関関係に法則性が存しないかを捜査しなければならなくなるはずであるが、このような捜査関係事項照会も番号法で許されないというのか、明らかにされたい。

（注：「特定個人情報」には、個人番号に対応し、当該個人番号に代わって用いられる番号等をその内容に含む個人情報も含まれている・番号法２条８号）

８　Ｊ－ＬＩＳへの情報集中という「不備」

(1)　被告は、地方公共団体情報システム機構（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。

しかし、同機構は、本人確認４情報とそれらの変更履歴、住民票コード、マイナンバー、個人番号カードの顔写真等までを一括管理していることは間違いない。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。

(2)　個人番号カードの発行枚数は、平成２９年１２月１日時点で約１３００万枚であるが、国の方針からすると、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。

さらに、後述するように、公的個人認証の利用履歴に関する情報も保有することになる。

(3)　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っているという「不備」が存する。

(4)　また、被告は、Ｊ－ＬＩＳが公的個人認証サービス関係で保有する個人情報種類・内容については、「氏名（外国人にあって住民票に通称が記載されれているときは当該通称を含む。）、出生の年月日、男女の別、住所、住民票コード及び電子証明書の発行の番号」であると釈明するが、同機構が保有する個人情報はそれだけにはとどまらない。

すなわち、個人番号カードに入った公的個人認証を利用するたびに、Ｊ－ＬＩＳに対して認証を求めることになるので、少なくとも、どこで公的個人認証を利用したのかの記録はＪ－ＬＩＳに残ると考えられるからである。

これにより、同機構は、公的個人認証を、いつ、どこで利用したのかという情報をも保有することになる。

９　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」

(1)　共通番号制度の最大の問題は、これまで主張してきたようにデータマッチン

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。

すなわち、日本においては、マイナンバーとひも付けられたデータベースの作成自体は、番号法等で規定しさえすれば何ら制限されていない上に、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。

すでに何度も主張しているように、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。

(2)　プロファイリングに関する「不備」として、第１に、現在の番号法上、「刑事事件の捜査」（番号法１９条１４号）の場合は、プロファイリングのための特定個人情報の収集について、明文で禁止されていない点がある。この点は、７で前述したとおりである。

今後、例えば、「テロ捜査」などの名目で、疑わしい人物を洗い出すために、マイナンバーを利用して収集した情報からスクリーニングを行うなどの利用が行われてしまう等の危険性が存する。

第２に、同じく「政令で定める公益上の必要があるとき」（１９条１４号）

は、特定個人情報の提供を受けることができるとされ、そこには明文の制限が存しないから、政府の意思によりその範囲が恣意的に広げられる危険性が存する。

第３に、現在の個人情報保護委員会の監督権限は、これらの利用については及ばないことになっている（番号法１９条１４号、３６条）。

したがって、明文の制限がない上に、実際にこのような利用が行われた場合に、それをチェックすることも非常に困難である。

これらの点も重大な「不備」である。

(3)　ＥＵ等では、これらについて、明文の制限と監督機関が存する。

ア　例えば、訴状や準備書面(1)で適示したように、ドイツにおいては、憲法上保障された「自己情報決定権」に基づき、１９８３年１２月１５日連邦憲法裁判所判決のような違憲判決が何件も出されている。

イ　また、例えば、ＥＵ一般データ保護規則（本年５月に施行）では、以下のようなプロファイリング規制やプライバシー・バイ・デザインに関する規定が存する。

（以下、『法と情報雑誌』第１巻第３号（２０１６年９月）１１０頁・夏井高人明治大学法学部教授訳による）

「第２２条　自動化された個人の判定、プロファイリングを含む

１．　データ主体は、自動化された処理のみに基づいて、プロファイリングを含め、彼もしくは彼女に関する法的効果を発生させ、または、彼もしくは彼女に対して同様に重大な悪影響を及ぼすような判定の対象とされない権利を有する。

２．　第１項は、以下に該当する判定には、適用されない。

(a)データ主体とデータ管理者との間での契約の締結またはその履行のために必要となる場合；

(b)管理者が服する欧州連合または構成国の法律により権限を与えられたものであり、かつ、データ主体の権利および自由並びに正当な利益を保護するための適切が定められている場合；または

(c)データ主体の明示明治の同意に基づく場合。

３．第２項の(a)および(c)に示す場合においては、データ管理者は、データ主体の権利及び自由並びに正当な利益、少なくとも、管理者の側での人間の関与を得る権利、彼または彼女の見解を表現する権利及び判定を争う権利を保護するための適切な

措置を実装するものでなければならない。

４．第２項に示す判定は、第９条第１項に示す特別類型の個人データに基づくことができない。ただし、第９条第２項の(a)または(g)が適用され、かつ、データ主体の権利及び自由並びに正当な利益を保護するための適切な措置がなされている場合を除く。」

Cf.　第９条　特別類型の個人データの処理

１．民族的もしくは社会的な出自、政治的意見、宗教上もしくは思想上の信条または労働組合への加入を明らかにする個人データの処理、並びに、遺伝子データ、自然人をユニークに識別することを目的とする生体データ、及び、自然人の健康又は性生活もしくは性的傾向性に関するデータの処理は、禁止される。

２．第１項は、以下の場合には適用されない。

(a) １以上の特定された目的のためのその個人データの処理について、データ主体が明確な同意を与えた場合。ただし、第１項に示す禁止をデータ主体が解除することはできないと欧州連合または構成国の法律が規定している場合を除く；

(b)雇用保険及び社会保障並びに社会保障法の分野において、管理者またはデータ主体の義務を履行する目的のため、または、それらの者の特別の権利を行使する目的のために処理が必要となる場合。（以下略）

第２５条　バイデザイン及びバイデフォルトによるデータ保護

１．技能の水準、実装の費用、処理の性質、範囲、処理過程及び目的並びに処理によって示される自然人の権利及び自由に対する様々な発生確率と深刻度のリスクを考慮に入れた上で、管理者は、この規則の要件に適合するものとし、かつ、データ主体の権利及び自由を保護するために、処理の方法を決定した時点及び処理それ自体の時点の両時点において、データのミニマム化といったようなデータ保護の基本原則を実装するために設計された仮名化や効果的な方法で、その処理の中に必要な安全性確保措置を統合するための適切な技術上及び組織上の措置を講じなければならない。

２．管理者は、処理の個々の特定の目的のために必要な個人データのみが処理されることをデフォルトで確保するための適切な技術上及び組織上の措置を実装しなければならない。この義務は、収集される個人データの分量、その処理の範囲、その記録保存の期間及びアクセス可能性について適用される。

３．第４２条により承認された認証方法は、本条の第１項及び第２項に定める要件の充足を説明するための要素として、これを用いることができる。

ウ　また、例えば、ドイツのデータコミッショナー（日本の個人情報保護委員

会にあたる組織）は、警察のデータベースを検査する権限も与えられている。

エ　以上は、法制度の異なるＥＵ等の例であるが、プライバシーを取り巻く環境はＥＵも日本も同様であること、個人情報の国際的流通の観点から、ＥＵの規制が直ちに日本の企業活動等へも影響している現実が存すること、昨年、日本の個人情報保護委員会もデータ保護・プライバシー･コミッショナー国際会議の正式メンバーになったことなどに鑑みるならば、日本においても同等以上の保護措置が必要である。

(4)　被告主張の誤り

ア　被告は、マイナンバーシステムは、分散管理のシステムであり、個人データは一元管理されない旨主張する。

この主張は、α：情報の一元的管理がなされないという点と、β：一挙に全部のデータに対して不正アクセスがなされたり、漏洩したりしないという２つの点を意味していると考えられるが、いずれも誤りないし不正確である。

イ　αの点に関する誤り

一カ所のデータベースで個人データを管理していなくても、ネットワークでつながっていれば、一カ所のデータベースで管理されている場合と機能的には変わりはなく、「一元的管理」となる。その点は、紙媒体で情報を管理していた時代とは全く異なる。この点、確かに情報提供ｎｗｓだけを取り出してみるならば、照会目的の絞り等が存するため、何の制限もなくすべてのデータにアクセスできるわけではないと思われるが、将来どのようなシステム設計になるかは不明である。また、現在においても、情報提供ｎｗｓを使わないプロファイリング等が明文で禁止されていない点は上述したとおりである。

【求釈明】

５　情報提供ｎｗｓ上、システム的に個別照会しかできないのか。

個別照会しかできないとする場合、一個の事務について、多数人について照会する必要がある場合は、事務が煩雑になるとも考えられるが、その照会事務はどのように行っているのか。

６　各省庁のデータベースにおける４情報（氏名、住所、生年月日、性別）や個人番号は常時アップデートされているのか。

ウ　βの点に関する誤り

地方自治体の中間サーバが２カ所に集中している問題を例にとれば、第１に、中間サーバへのアクセス権限を乗っ取られれば、ネットワーク経由で不正アクセスが可能となる。特に、中間サーバの管理者権限やシステムのメンテナンスを行う権限を持つ者が権限を濫用した場合や、その権限を乗っ取られた場合には、中間サーバに存するすべてのデータに不正アクセスされたり、漏洩したりする危険性が存する。第２に、中間サーバに物理的な攻撃がなされた場合は、一挙に中間サーバに存するすべてのデータが奪取される危険性が存する。あとは、暗号化等の防御が破られるかどうかの問題となるが、データを元に戻すためのパスワードまで漏れていた場合には、いくら高度な暗号化を行っていても、セキュリティ的には無力である。

10　なりすましの危険性が高いという「不備」

個人番号カードと暗証番号が盗まれたりしたら、マイナポータルにおけるなりすましが容易になし得る。前述したように、高齢者、障がい者等に多い情報弱者の場合、なりすまされても、本人は気がつきにくいという危険性が存する。

11　漏洩等の事故事例

(1)　はじめに

本項では、マイナンバー制度開始前の２０１５年１０月から現在にいたるまでマイナンバーをめぐる事故が多発し、その結果、原告らのプライバシー情報が日々侵害される具体的危険性が生じていることを明らかにする。

なお、地方税特別徴収通知誤配事件については、原告準備書面（３）２２頁以下で述べた通りであるが、これも原告らのプライバシー情報が日々侵害にされる具体的危険性が生じていることを基礎づける事件である。さらに言うと、この特別徴収通知の誤配事件を受けて、国（総務省）は、平成２９年１２月に総務省令を改正し（甲１９、２０）、同通知への個人番号の記載を「当分の間」行わないとした。原告準備書面（２）１５頁以下で詳述したように、国（総務

省）は、繰り返し通知・Ｑ＆Ａを出すなどして個人番号の記載を市区町村に強要していたのにかかわらず、今回の省令改正で個人番号を記載しないとしたのである。朝令暮改の典型というべきだろう。

そして、本項で述べることは、まさにマイナンバー制度に技術上又は法制度上の「不備」があることに他ならないのであり、特定個人情報が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ことになる。それゆえ、被告が第１準備書面の第３．４の「システム技術上又は法制度上の不備があり、そのために個人番号及び特定個人情報が法令又は条例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第三者に開示又は公表される具体的危険が生じている事実はない」という主張への反論となる。

(2)　マイナンバー制度に関する事故事例の紹介

ア　行政部門からの特定個人情報の漏えい

（ア）住民票へマイナンバーを記載した事故事例

①　２０１５年１０月１３日、茨城県取手市は、マイナンバー制度が始まる同月５日から、住民票を発行する自動交付機のシステムが切り替わるように、市の委託業者が同月３日に設定作業を行った。しかし、マイナンバーを記載しないようにする設定を怠ったため、誤ってマイナンバーを記載した住民票６９人分が発行された。同様のミスは福島県福島市、北海道札幌市でも発生した（甲２１号証の１～３）。

②　２０１６年２月１日、北海道帯広市の戸籍住民課の男性職員が、北海道外の企業が業務目的で請求した市民の住民票をプリンターで印刷した。そして、他の職員もほぼ同時に別の市民の住民票を印刷していて、同男性職員が取り違えたことから、同市は請求されたものとは別の市民のマイナンバーが記載された住民票を誤って郵送してしまった（甲２２）。

また、２０１７年９月１３日、岡山県倉敷市の水島支所で、誤って漢字が一文字違う人物へマイナンバーが記載された住民票の写しを交付してしまった（甲２３）。

③　まとめ

上記の事故事例は、住民票にマイナンバー、すなわち、個人番号を記載して発行してしまったというものである。以下の通知カードと同様に、住民票には氏名、住所、生年月日、性別等が記載されているのだから、住民票に個人番号が記載されたものが他者の手に渡れば、どの人物にどの番号が割り振られたか等、個人情報と個人番号が同時に漏えいすることによって、個人の識別は容易に可能となってしまうのである。そして、個人番号が記載された住民票が他者の手にわたるということは、故意にせよ、過失にせよ、個人番号を他者に対して提供したことと同じ結果になってしまうのである。そうだとすれば、法令上正当な目的の範囲を超えた個人番号の利用や特定個人情報の提供をしてしまったのと同じ状態が出現してしまっているのである。

（イ）マイナンバー通知カードの作成・発行における事故事例

マイナンバー通知カード（以下、「通知カード」という。）の作成・発行の場面においては、既に以下のような事故例が発生している。

① ２０１５年１２月４日、高市早苗総務大臣は、東京都葛飾区白鳥地区の約５０００世帯分の通知カードがミスで作成されていなかったことを明らかにした（甲２４）。

② ２０１５年１２月、滋賀、静岡、秋田の３県５市町で１８４人分の通知カードの印刷漏れが新たに判明した。内容は滋賀県日野町１５６人分、同県多賀町８人分、静岡県熱海市１２人分、秋田県潟上市４人分である（甲２５）。

③ ２０１５年１２月１６日、大阪市は、マイナンバーを記載した通知カードにつき、天王寺区に住む１９７７人分が作成漏れとなり、未送付になっていたと発表した（甲２６）。

④ ２０１６年２月２３日、香川県坂出市と長野県長野市の２人の男性に同一の個人番号が割り振られていたことが判明した（甲２７）。

⑤ まとめ

上記の各事故例は通知カードの作成漏れや２人に同一の個人番号を割り

振ってしまったとているという内容のものである。

上記の事故例は、作成されるはずの通知カードが作成されていなかったり、本来割り振られるはずのない同一の番号を２人に割り振ってしまったりしたものであるから、一人一人に唯一無二の個人番号が通知されて利用されるという前提が崩れ、マイナンバー制度の根幹を揺るがしかねないものである。制度設計、制度運用のあやうさ・脆弱さを体現してしまっている事故例といえる（なお、①については未だに原因が公表されていない）。

また、上記事故例は正確に確認作業をしていれば防止することができたヒューマンエラーといえ、マイナンバー制度の制度設計、制度運用に携わる者の確認作業がいい加減なものかを端的に表しているといわざるを得ない。マイナンバーのような全国的で、制度開始、制度運用においては膨大な作業を要し、携わる人の数もとりわけ多い制度においては、このようなヒューマンエラーは不可避的に生じ、事務負担から自ら招きかねないのは明らかである。そのため、被告の主張する厳格な本人確認なるものは、多くのヒューマンエラーを生じ、機能しないことは容易に想像できることである。

（ウ）通知カードの配達・交付における事故例

① ２０１５年１０月３０日、高知県の安芸郵便局が通知カードを誤配達した。同月３１日には、千葉県の流山郵便局が通知カードを誤配達した。これらは、郵便局やコールセンターに問い合わせ・指摘があって発覚した（甲２８）。

② 被告は当初、２０１５年１１月待つまでに通知カードの配布を終えるという計画を立てていた。

しかし、同月１１日時点で通知カードの配達が完了したのは、５９５万通であった。これは、全国約５６００万世帯の約１割に過ぎない。

そのため、日本郵便は同月１２日、通知カードを同月末までに全世帯に配達するのは難しい状況との認識を示した（甲２９）。

なお、同月１１日までに誤配達や窓口での誤送付等の事故は合計６８件

あった。

③　２０１５年１１月１７日、青森県の八戸郵便局が通知カード１通を別人に誤配達した。同月１日には、八戸西郵便局で誤配達があったばかりであった（甲３０）。

④　２０１６年1月２８日、大阪市鶴見区は親族の通知カードを受け取るために交付窓口に訪れた男性に、誤って別人の通知カードを交付した（甲３１）。

⑤　２０１６年2月２８日、三重県菰野町は同町に住む男性２人を取り違えてマイナンバーカードを発送していたことが判明した（甲３２）。

⑥　まとめ

上記事故例は､いずれも通知カードの誤配達についての事故事例である。上述した住民票と同じように、通知カードには、個人番号のみならず、住所、氏名、生年月日、性別等が記載されており、個人情報と個人番号が他人に漏れている結果になっている。すなわち、前述した他人に個人番号を提供したことと同一の結果が生じており、個人番号の漏えい問題が生じている。

イ　民間部門からの特定個人情報漏えい

（ア）民間事業所による特定個人情報漏えい

①　マイナンバーについて､身分証明書として使わないよう内閣府や総務省が通知を出していたにも関わらず､TSUTAYA がマイナンバーを本人確認に使用できるようにして２０１６年1月までホームページなどで公表していた（甲３３）。

②　２０１５年１１月頃、大阪の焼き肉店において、「マイナンバー・ラッキーくじ」なるキャンペーンをして、個人番号の下４桁が、店が選んだ数字と一致すると、特定のメニューを無料で進呈するなどのサービスを行おうとしていた。なお、この焼き肉店は、本サービスを実施する際に、内閣官房に事前に確認をとっていたところ、内閣官房が「良いとも悪いとも言えない」と回答していたために実施したということである（甲３

４）。

③　上記は、民間で起きた事故例であり、被告は個人番号について民間にも周知徹底をしているという。また、漏えいによる罰則も設け、民間による流出に関して、徹底した予防措置が取られているかのように主張する。しかし、実際には、民間における個人番号の取り扱いについての周知は徹底されていないのであり、上記のような事故例が生じている。

（イ）個人番号カードの持ち歩きの推奨と漏えいの危険について

下記①及び②は、直接の漏えいの事故例ではないが、漏えいの危険を助長する事柄であるため、事故例の一つとして主張する（③は事故例）。

①　２０１７年４月の消費税率１０パーセントの引き上げを進める中で、飲食品の購入の際にマイナンバーカードを持ち歩けば、購入した食品の消費税について一部還付を受けられるとの政策を財務省は検討していた。なお、これに対して、麻生太郎財務大臣は「カードを持ちたくなければ、持って行かないでいい。その代わり、その分の減税はないだけだ」と答えていた（甲３５）。

②　２０１７年１月初めに、２０１８年度からマイナンバーカードを保険証の代わりに使えるようにするという方針を出している。医療機関でこれを見せれば、健康保険の利用ができるとする（甲３６）。

③　個人番号カードを発行して以降、個人番号カードの紛失事故が相次いでいる。群馬県警が２０１６年に受け付けた個人番号カードの遺失届は合計２８６３にのぼり、３５４枚が落し物として届けられた。

④　まとめ

前述したように、マイナンバーカードには、その券面にマイナンバーが記載されている。マイナンバーカードを日常的に持ち歩くことは、必然的に盗み見などによる個人番号の漏えいの危険が常に伴う。マイナンバーは本来、秘密にしておくべき情報である。このマイナンバーを券面に記載しておきながら、そのカードを日常的に持ち歩き、利用させようとしている。そのことにより、③で挙げたように、紛失事故が数多く発

生している。このような制度と施策は、マイナンバーの漏えいを推奨しているようなものであり、明らかに構造的な欠陥、「不備」であるといわなければならない。

（ウ）民間企業の管理のずさんさ

JAL（日本航空株式会社）は、平成２９年１２月２０日、偽の請求書メールに騙され、約３億８０００万円の被害にあったと公表した（甲３７）。

JALという、従業員を１万人以上抱え、資本金も３０００億円以上もの、大企業でさえ、サイバー攻撃に対して、十分な防御が整っていない。

被告は民間企業のセキュリティが十分である旨述べるが、上記事故事例もマイナンバーと直接関連するものではないが、民間のセキュリティの甘さを基礎づける事故事例と言える。

ウ　まとめ

上記であげた事故例は氷山の一角であり、報道された事故例の中の一部に過ぎない。

また、事故があったが、検出されず報道されなかったものも含めれば、個人番号の漏えいの事故は数えきれないほど生じている。

それらには、ヒューマンエラーもあるが、そもそもそのようなマンパワーが明らかに足りないにも関わらず、複雑でプライバシー侵害のリスクの高い導入している制度設計自体の欠陥であるといえる。漏えいの危険性がこれだけあり、漏えいした際のプライバシーリスクの拡大を防ぐような制度が全くないことも、制度の欠陥、「不備」であると言える。また、本来秘密にしておくべき情報であるマイナンバーが記載されているマイナンバーカードを常備させるように推進していることは、漏えいのリスクを高める施策を国が推奨していることになり、明らかな構造的な欠陥「不備」である。

以上を踏まえれば、被告が主張するように、システム技術上又は法制度上の不備があり、そのために個人番号及び特定個人情報が法令又は条例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第三者に開示又は公表される具体的危険が生じている事実はない、とはとても言えず、特定個人情

報が開示又は公表される具体的危険が生じているといえる。

12　結語～マイナンバー制度（システム）は多数の根本的かつ重大な「不備」が存する違憲の制度である

以上述べてきたように、マイナンバー制度（システム）には根本的かつ重大な「不備」（欠陥）が存する。

第１に、同制度は、現在の「ビッグデータ」時代において、ＡＩによるデータ処理技術が驚異的進展を遂げる中で、プロファイリング等に対するプライバシー保護の原則や保護策がないまま構築が進められている。第２に、その根本は、この制度が「共通番号」制度を採用していることがある。３で述べたように、必要もないのにプライバシーにとって危険性の高い「共通番号」制を採用していることが根本的「不備」（欠陥）である。第３に、その上で、その「共通番号」であるマイナンバーとひも付けたデータベースの作成を推進し、また、官民でマイナンバー等を券面に記載した個人番号カードの利活用を進めて、事実上同カードを日常持ち歩かないと生活できないような制度・システムづくりの施策を推進していることである。

被告国は、ＩＴ弱者なども含めた国民と外国人住民の全員が、安心して利便性を追求できる制度・システムを構築する責務が存する。逆に言えば、ある程度の不便があっても安全性を追求する自由を保障しなければならない。全員が、事実上この制度・システムを利用しなければ生活できないようなものを構築することは、国民等の自由を侵害するものである。

このような制度・システムが完成してしまったならば、マイナンバーを含むプライバシー情報の漏洩流出という直接的侵害だけにとどまらず、「個人の尊厳ないし人格的自律」を保持していくことが著しく困難な社会を招来することは必然であり、憲法１３条に違反するといわなければならない。

そのような巨大なシステムが完成してしまう前に、プライバシー権、人格

権を将来にわたって保障してゆくために、厳格な司法審査を及ぼすことが求められているといわなければならない。

以上