平成２７年（ワ）第１１９９６号，平成２８年（ワ）第２０２３号，平成２８年（ワ）第２８９５号　個人番号利用差止等請求事件

原告　平野かおる　ほか１４４名

被告　国

準備書面１６

２０１９（令和元）年１０月１７日

大阪地方裁判所第２４民事部合議２へ係　御中

原告ら訴訟代理人弁護士　大　江　洋　一

同　辰　巳　創　史

甲第３１号証（實原教授作成の意見書）に基づき、原告らは、以下の通り主張する。

なお、本書面では、甲第３１号証の「１.」「２.」「４.」に基づいて主張し、「３.」及びこれに関連する部分については、準備書面１７にて主張する。

第１　「自己情報コントロール権」が認められること

１　「自己情報コントロール権」が憲法学において認められていること（甲３１「１.」「(2)」第１段落：２頁）

原告らが主張している自己情報コントロール権は、既にドイツで１９８３年の国勢調査判決において「情報自己決定権」として認められたものと同様のものである。

そして、日本の憲法学の大家である佐藤幸治教授において、「外的情報も悪用され又は集積されるとき、個人の道徳的自律の存在に影響を及ぼすものとして、プライヴァシーの権利の侵害の問題が生ずる」と指摘し、そうした問題の一例として“データ・バンク社会”の問題が挙げられている。佐藤教授は、このような場面において必要な権利として、「自己に関する情報をコントロールする権利」を提唱し、「その人についての情報の①取得収集、②保有および③利用・伝播、の各段階について問題となる」と指摘している。

この佐藤教授の見解は、原告らの主張する「自己情報コントロール権」と同じ内容のものであり、憲法学において一般的なものと評価されている。

2　最高裁も「自己情報コントロール権」を認めていること（甲３１「１.」「(2)」第２，３段落：２～３頁）

最高裁判例では、「自己情報コントロール権」との言葉自体は用いられていないものの、「みだりに第三者に開示・公表されない自由」などの言葉を用いて、実質的には、「自己情報コントロール権」が認められているといえる。

すなわち、最高裁は、プライバシー権に関する権利として、京都府学連事件において、「承諾なしに、みだりにその容ぼう・姿態を撮影されない自由」を認めた。早稲田大学江沢民講演事件においては、学籍番号や氏名、住所といった、必ずしもそれ自体では私生活の様子が分からない情報についても、「このような個人情報についても、本人が、自己が欲しない他者にはみだりにこれを開示されたくないと考えることは自然なこと」であるとして、個人情報が法的保護の対象になるとした。

加えて、住基ネット事件判決において、「個人の私生活上の自由の一つとして、何人も、個人に関する情報をみだりに第三者に開示または公表されない自由」があり、これが憲法１３条で保護されるとした。担当した調査官も、住基ネット最判が「従前の最高裁判例の延長」にあり、「『個人に関する情報をみだりに第三者に開示又は公表されない自由』が憲法１３条により保障されること」

を示したものと説明している。

以上のとおり、最高裁は、「自己情報コントロール権」という言葉は用いていないものの、佐藤教授が提唱し、原告らの主張する「自己情報コントロール権」を、各場面に応じて、実質的に認めている。

3　「自己情報コントロール権」が認められること（甲３１「１.」「(2)」第４段落：３頁）

「自己情報コントロール権」と呼ぶかは別としても、原告らが主張する、各種情報の「取得収集・保有・利用（伝播）の各段階で同意なしの取扱を拒む権利」は、学説においても、最高裁においても、実質的に認められている。そして、マイナンバー制度においては、プライバシー性が高い多くの情報がやり取りされることから、その合憲性を判断するには、「自己情報コントロール権」を認めたうえで、その制約の妥当性が検討されなければならない。

第２　マイナンバー制度の危険性

マイナンバー制度には、次の危険性が存在する。

１　情報漏洩の危険性（甲３１「１.」「(3)」「①」：３頁）

マイナンバー制度においては、行政機関のみならず、民間にも特定個人情報データベースが作成される。行政機関においてすらセキュリティの実態が極めて不十分であるところ、セキュリティ対策が事業者ごとに異なる民間部門が個人番号等を扱うことで、情報漏洩の危険性が高まっている。

さらに、一旦漏洩した場合、特定個人情報を抹消し、元の状態に回復することは事実上不可能であり、このことも情報漏洩の危険性を増大している。

２　データマッチングの危険性（甲３１「１.」「(3)」「②」：３～４頁）

個人番号を用いることで、他者の個人情報と混同することなく、容易かつ正確に「データマッチング」することが可能となっている。こうした「データマッチング」を通じて個人の様々な情報が次々と知られてしまう結果、本人の意

に反する個人像が、知らないうちに形成されうる。これは、マイナンバー制度を通じた情報の一元化と「監視国家」の誕生につながる不安を生じさせている。

3　住基ネットとの比較（甲３１「１.」「(3)」「③」：４～５頁）

(1)　取扱機関

住基ネットにおいては、行政機関だけが住民票コードを扱う。一方、マイナンバー制度においては、民間事業者も「個人番号関係事務実施者」として個人番号を扱っている。

(2)　利用目的

住基ネットでは、「住民基本台帳に記録された個人情報のうち、氏名、住所など特定の本人確認情報を市町村、都道府県及び国の機関等で共有してその確認ができる仕組み」であるのに対し、マイナンバー制度の目的は「効率的な情報の管理及び利用並びに他の行政事務を処理する者との間における迅速な情報の授受」へと広がっている。

(3)　提供場面

マイナンバー制度では個人番号の利用範囲や特定個人情報を提供できる場面が、税や社会保障、災害分野を中心に著しく広がっている。これに伴い、住基ネットと比較して、関係する行政機関の増大、利用目的の拡張、民間事業者も番号を扱うこと、利用範囲や情報提供が可能な場面の著しい広がりをもたらしている。

(4)　情報の内容

住基ネットでは、いわいる「基本四情報」を自治体・国が共有・確認するだけであった。これに対してマイナンバー制度は、「特定個人情報」を提供するためのものであり、そこでは、所得や支出など、一般的に他人に知られたくないプライバシー性の高い情報が多く提供されている。

(5)　情報環境の変化

住基ネット判決が出されてから現在までに、ＩＴ環境も大幅に変化し、行

政機関だけでも大量の情報を保有するようになった一方、ハッキングの技術は巧妙化している。

国際的には、ＥＵにおいて新たにデータ保護規則が施行されるなど、個人情報の保護強化の傾向が一層強まっている。日本国内でも、住基ネット判決時よりも、自己情報コントロール権の重要性が広く認識されるようになっており、被告自身も「本人の意図しないところで個人の全体像が勝手に形成」される危険性に言及し、「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」との認識を示している。

(6) 小括

以上のとおり、住基ネットと比較してマイナンバー制度は、個人番号を扱う主体だけでなく利用目的も拡張され、提供される情報のプライバシー性も飛躍的に強まっている。また、住基ネット判決以降、個人情報保護の状況も国内外において大きく変化し、「本人の意図しないところで個人の全体像が勝手に形成」される危険性を被告自身も認識するに至っている。

したがって、マイナンバー制度の合憲性審査に当たっては、住基ネットとの制度内容や時代背景の違いが、慎重に検討されなければならない。

第３　合憲性の判断枠組み

マイナンバー制度の合憲性を判断する際には、概ね、以下の点を考慮しなければならない。

１　「自己情報コントロール権」への制約の妥当性が判断対象であること（甲３１「１.」「(4)」「②」：５～６頁）

原告らの主張する「自己情報コントロール権」又は、「取得収集・保有・利用（伝播）の各段階で同意なしの取扱を拒む権利」、「みだりに第三者に開示ま

たは公表されない自由」が、憲法上の保護を受けることは、判例・学説において決着済みである。したがって、マイナンバー制度によるこれら権利・自由への制約が妥当であるかを、検討しなければならない。

2　住基ネット判決との関係（甲３１「１.」「(4)」「③」：６頁）

すでに述べたとおり、住基ネットに比較してマイナンバー制度では「個人の情報がみだりに第三者に開示・公表されない自由」が侵害される危険性が飛躍的に高まっている。したがって、住基ネット最判よりも厳格・慎重な審査が必要である。単に住基ネット判決をなぞるだけの理由付けでは、上訴審での破棄差戻しを免れない。

3　明確性の要請（甲３１「１.」「(4)」「④」第１段落：６頁）

個人情報の利用方法を予測するためにも、マイナンバー制度の基本的仕組みは、国会の決定により、容易に変更できないものとして、国民に明確に示される必要がある。具体的には、「マイナンバー制度において、どのような情報が、どのような機関によって、どのような場合に取得収集・保有・利用等されうるか」が、法律において明確に規定されているかが、慎重に検討されなければならない。

4　利用等の範囲の合理性（過度に広汎な規定の禁止）（甲３１「１.」「(4)」「④」第２段落：６頁）

マイナンバー法の規定自体が明確であったとしても、そこで認められる個人情報の利用等の範囲が、合理的な範囲を超えて広汎でないかも、慎重に検討されなければならない。これに反する場合には、個人情報の収集等が「みだり」に行われることになり、原告ら国民の利益を十分に保護できなくなる。

5　情報漏洩防止措置（甲３１「１.」「(4)」「④」第３段落：６頁）

マイナンバー法の採用する仕組みが、個人情報の違法な漏洩防止を実現できるかも、検討する必要がある。また、本人が自己の権利の救済を迅速に求めるための制度が整備されているかも、慎重に検討しなければならない。

６　萎縮効果の防止（甲３１「１.」「(4)」「④」第４段落：６頁）

法の規定が不明確な場合、法が頻繁に改正されて個人情報の提供場面が際限なく広がる、もしくは、そのおそれがある場合、さらには法の明文で認められている以上に広い範囲で個人情報が提供される場合などには、個人情報が知らないうちに収集等されている、もしくは、そのおそれがあることで、日常的な、合法的な行動も控えてしまう心理が生じかねない。したがって、萎縮効果とも関連付けて検討しなければならない。

第４　マイナンバー制度全体の憲法上の問題

１　情報漏洩防止制度の不備

(1)　罰則による予防の限界（甲３１「２.」「(1)」：７頁）

マイナンバー制度では、違法な行為を罰則の対象として規定している。しかし、違法な行為を処罰しても事後的な対応に過ぎず、ひとたび個人情報が漏洩したならば、そのこと自体の原状回復は不可能という限界がある。また、厳罰が予定されていても、諸事情から冷静な判断を欠くに至った者が違法な行為に及ぶことを防げるわけではない。したがって、罰則によって情報漏洩を確実に防げるわけではない。

(2)　個人情報保護委員会による監督制度の不備（甲３１「２.」「(2)」：７～８頁）

ア　マイナンバー制度では、個人情報保護委員会が設置されていることから、当該委員会による監督が十分といえるかが検討の対象となる。

イ　この点、個人情報保護法は、個人情報保護委員会の任務について、「個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の個人情報の有用性に配慮しつつ」、「個人の権利利益を保護するため、個人情報の適正な取扱いの確保を図ること」（注：下線部引用者）と規定する（個人情報保護法６０条）。

同条の「個人情報の適正かつ効果的な活用」とは個人情報を「国民」全体で利用することを意味すると考えられ、これは「みだりに第三者に開示・公表されない」という意味での「個人情報の適正な取扱いの確保」と相容れない。したがって、個人情報保護委員会の「個人情報の適正かつ効果的な活用」という目的自体、漏洩防止の限界として作用するおそれがある。

ウ　また、所掌事務が多岐に渡るにもかかわらず、個人情報保護委員会の常勤・非常勤委員の人数は少なく、マイナンバー制度における個人番号や特定個人情報の提供・利用等を十分に監督することは、現実的には不可能である。

エ　さらに、マイナンバー法３６条は、同法１９条１４号の委任に基づき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による監督等に関する規定（マイナンバー法３３－３５条）を適用しないとする。マイナンバー法施行令が別表で挙げるもののうち一部が「各議院審査等に準ずるもの」に該当するところ、別表７，９，１１号などがこれに含まれている。これにより、特定個人情報が警察官や公安調査官に提供される際には、個人情報保護委員会の監督等が及ばないことなる。

したがって、マイナンバー制度における特定個人情報の利用の重要な場面がその監督等の対象から除外されているといえ、個人情報保護委員会がマイナンバー制度の運用を十分に監督等できるかは、その権限の面からも疑わしいと言わざるを得ない。

オ　以上のとおり、個人情報保護委員会は、個人情報の保護のみを目的としておらず（それどころか、相反するはずの個人情報の利用促進をもその目的としている。）、所掌事務の多さに比して小規模組織にとどまっていることに加え、与えられた権限も限定されている。

したがって、個人情報保護委員会による監督は、マイナンバー制度における個人の権利保護の仕組みとして、不十分である。

2　利用目的の広汎性（甲３１「２.」「(3)」「①」：８～１０頁）

(1)　マイナンバー制度における個人番号の利用範囲や特定個人情報の提供場面は、あまりに広範であり、これを正確に認識することは困難である。

すなわち、マイナンバー法が認める個人番号の利用範囲や、情報提供ネットワークシステムを使った特定個人情報の提供場面が非常に広範なことに加え、膨大な量の主務省令にも目を通さないと、自己の情報が開示・公表される範囲の全体像を認識できなくなっている。これにより、思いもよらない形で自己の情報が利用されるおそれがある。

(2)　加えて、マイナンバー法は、法改正により、制度目的と関連性の薄いものにまで、個人番号の利用範囲や特定個人情報の情報提供場面を拡張している。例えば、特定検診、「ペイオフ」のための預貯金額の合算、予防接種の実施に関する情報などである。

このように、マイナンバー制度の目的（税や社会保障、災害）と関連性の薄い範囲・場面にまで個人情報の「開示・公表」が拡張される結果、個人の情報が「みだり」に収集等されることになり、今後もより一層広範囲に及ぶおそれがある。さらには、主務省令で規定する個人情報の利用範囲や特定個人情報の提供場面などを、法の規定が輪郭づけていると言えるのかも疑わしい。

(3)　また、個人番号の利用範囲や特定個人情報の提供場面が広範に拡張されるということは、マイナンバー制度のもと、「合法的」に「みだり」に個人情報の収集等が行われることになる。このように、「合法的」に利用・提供が可能になるということは、違法な情報漏洩を防止する仕組みである罰則や個人情報保護委員会による監督等が十分に機能しない事態を招くことにもなる。

⑷　以上のとおり、マイナンバー制度においてどのような収集等が適法・違法になるかを法の規定から読み取ることは容易ではなく、法改正による利用・提供範囲の拡張は、個人情報が「『合法的』に『みだり』に第三者に開示・公表される」危険性を増大させている。加えて、利用・提供の範囲の拡張は、個人情報の開示・公表の多くを適法とする結果、違法な情報漏洩を防ぐ仕組みである罰則や個人情報保護委員会による監督等に機能不全をもたらす。

したがって、マイナンバー制度は、その利用目的の広さという点で、憲法上重大な問題を含んでいる。

３　個人に与えられている救済制度の不備（甲３１「２.」「⑶」「②」：１０頁）

マイナンバー法３２条は、自己情報の開示等を実施するために必要な措置を講ずるように定めている。しかし、自己情報の開示・訂正・利用の停止・消去・提供停止請求権を明示する条例を定めていない地方自治体も多く、現時点では有効に機能していない。

加えて、情報提供ネットワークを使用しない情報提供が行われた場合、提供記録を記録する必要がなく、「マイナポータル」によっても自己情報の利用・提供状況を確認することができない。この場合、原告らは、事実上、情報提供の状況を知ることができない。情報提供の有無を知ることは、違法な提供による権利侵害に対する防御や回復を求める前提となるところ、これが事実上不可能ということは、不利益を救済する手段がないことと同義である。

したがって、マイナンバー制度は、本人に対する不利益の救済という点でも、憲法上の不備がある。

第５　結論（甲３１「４.」：２１～２２頁）

マイナンバー制度は、違法な情報漏洩を防ぐ仕組みとして刑罰規定があるが効果に限界があり、違法な情報提供を個人情報保護委員会の監督により未然に防止することも考え難いことから、憲法１３条に違反し、違憲である。

さらに、個人番号の利用範囲や特定個人情報の提供が極めて広く認められることにより「違法」な情報漏洩の範囲が狭まり、「違法」な情報漏洩を防ぐ仕組みである罰則や個人情報保護委員会による監督等が十分に機能しなくなる問題もあり、この点も憲法１３条との関係でマイナンバー制度の違憲性を導く。

次いで、情報提供ネットワークシステムによらずに特定個人情報を提供される場合には、自己の特定個人情報がどのように提供されているかをマイナポータルで確認することができないことから、事実上、情報提供の状況を知ることができず、違法な情報提供が行われたとしても、権利侵害の防御や回復が不可能となっている。したがって、情報提供ネットワークシステムによらない情報提供の記録をマイナポータルで確認できないことは、不利益の救済という点で、憲法上の不備であり、憲法１３条に反しており違憲である。

また、法改正により、個人番号の利用範囲と特定個人情報の提供場面が拡張され、マイナンバー法の目的である税・社会保障・災害の３分野に直接関連しない場面にまで及んでいる。すなわち、現行のマイナンバー制度の下では、利用範囲が際限なく拡張される可能性があり、さらに主務省令の規定次第では利用範囲の拡張に歯止めがかけられなくなるおそれがある。このような、個人情報の利用範囲や提供場面を本人の同意もなく際限なく拡張することは、まさに「みだりに第三者に開示・公表」することに外ならず、この点でも憲法１３条に反している。

以上