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　(1)

２０１６（平成２８）年9月２１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

第１　自己情報コントロール権の根拠と内容

第２　現代社会における自己情報コントロール権の重要性

第３　被告には、更に具体的に制度の安全性に関する主張を行う義務が存する

第１　自己情報コントロール権の根拠と内容

はじめに

被告は、その第１準備書面において、「原告らのいう自己情報コントロール権は、実定法上の根拠も不明確である上、その外延及び内容も不明確であり、差止請求の根拠たり得る実体法上の権利とは認められない」と主張する。

しかし、以下で述べるとおり、「自己情報コントロール権」の実定法上の根拠は憲法１３条であって明確であり、内容についてもその本質部分については明確

である。

１　自己情報コントロール権は憲法１３条で保障されている人権であること

（１）憲法１３条の理念

憲法１３条前段は「すべて国民は、個人として尊重される。」と規定し、同条後段は「生命、自由及び幸福追求に対する国民の権利については、公共の福祉に反しない限り、立法その他の国政の上で、最大の尊重を必要とする。」と規定している。

ここに「個人として尊重」とは、単に国民は誰でも皆個人であるというような自明の事実を確認する意味ではなく、ドイツ憲法（ボン基本法）第１条1 項に規定されている「人間の尊厳」のような実質（主体性）を備えた個人としての尊重、すなわち、個人の人格的自律権の不可侵性の尊重を定めたものである。人格的自律権とは、個人が自分の生き方について、国や他人の価値観にとらわれることなく主体的に自己決定する権利（道徳的自律）のことであり、個人がそのような自律的存在になるためには、各個人の固有の価値観に基づく幸福追求権の保障が不可欠である。そして、この個人の人格的自律権が保障されることにより、国民は単なる自己実現の自由のみならず、民主主義社会における自己責任による行動の自由（自己統治の利益）をも享受することが可能となるのである。すなわち、憲法１３条はこうした自由民主主義（立憲民主主義）の基盤としての人権尊重主義という究極の憲法理念を謳った条文である。

（２）包括的人権規定

以上のような観点からは、人権が憲法１４条以下に規定されているいわゆる「人権カタログ」と呼ばれるものに限られる必要がないことは明らかである。人権カタログ中には明示されていない権利利益であっても、人格的自律権の尊重にとって重要な利益、いわゆる「人格的生存に不可欠な利益」は、当然に人権として認められることとなる。すなわち、憲法１３条は、このように人権カタログにない新しい人権の実定法上の根拠となる包括的人権規定なのである。

（３）プライバシー権の実定法上の根拠

他者に知られたくない個々人の私生活上の情報がみだりに他者に開示されたり、他者が私事に属する領域に侵入してくる場合には、個人の私生活における平穏が侵害されるのみならず、自己の意思決定過程に他者の介入を許すことになることから、自らの生き方のルールを自らが決定するという人格的自律（自己統治）の利益も脅かされることとなる。私事の公開、私生活への侵入からの自由としてのプライバシー権は、このように人格的自律を保護するという意味において、「人格的生存にとって不可欠な権利」であり、「個人の尊重」を実現する上での要となる権利の一つである。

したがって、プライバシー権は、不法行為法上の被侵害利益であるに止まらず、人格権の一内容として憲法１３条によって保障される人権であり、差止請求の法的根拠ともなり得る。

（４）自己情報コントロール権の実定法上の根拠

以上で述べたように、上記内容のプライバシー権が人権であるのは、それが国民の個人としての人格的自律権、すなわち、個人の人格的生存にとって不可欠な権利利益の保護のために不可欠であるからである。

このような個人の人格的自律権を守るためには、情報の流通が紙媒体中心であったころの社会においては、上記（３）の内容のプライバシー権を人権として保障するだけでも十分であったかもしれない。しかし、高度情報ネットワーク社会の進展は、上記内容のプライバシー権を保障するだけでは、人格的自律権の保護としては不十分な状況を生み出した。自己情報コントロール権は、このような社会状況の変化に対応して人格的自律を保護するものであり、その意味において「人格的生存にとって不可欠な権利」として憲法１３条によって保障される。

したがって、自己情報コントロール権は憲法１３条により保障される人権であり、その実定法上の根拠は明確である。

２ 自己情報コントロール権の内容

（１）自己情報コントロール権の内容は明確である

自己情報コントロール権とは何かについては、確かに論者によって表現やニュアンスの強調点において若干の差異が認められる。しかし、それは本質

的な差異ではなく、そのような差異があることは自己情報コントロール権の内容が曖昧であるということを意味するものではない。なぜなら、自己情報コントロール権の内容の明確性は、言葉や表現の統一性や類似性によってではなく、その解釈根拠の明確性・一貫性によってこそ担保されるものであるからである。

すなわち、自己情報コントロール権の実定法上の根拠は前述のとおり憲法１３条であるから、その解釈根拠もまた憲法１３条に基づく「個人の尊重」の理念以外にはありえない。そして、憲法１３条の理念は、個人の人格的自律、自由な自己決定、自己統治の利益である以上、同条により保障される自己情報コントロール権の内容も個人の人格的自律、自由な自己決定、自己統治の利益といった要素で構成されなければならないという点においてすでに明確なのである。

したがって、自己情報コントロール権の内容は明確であり、論者によって認められる若干の表現や強調するニュアンスの差異は権利内容の明確性を否定する根拠にはなり得ない。以上のような観点から、若干の裁判例や学説について以下で考察する。

（２）金沢地裁平成１７年５月３０日判決（判時１９３４号３頁）

住基ネットに関する標記判決（以下、「金沢地裁判決」という。）は以下のように述べている（下線部は引用者、以下同じ。）。

「　……　近年、ＩＴ（情報技術）の急速な発達により、コンピュータによる膨大な量の情報の収集、蓄積、編集、伝達が可能となり、またインターネット等によって多数のコンピュータのネットワーク化が可能となった。公権力や一般企業においては、これらを利用して広範な分野にわたる個人情報が収集、蓄積、利用、伝達されているところ、このようなデジタル情報は、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は判らないこと等の特性があり、一般の住民の間には、自己の個人情報が自己の知らぬ間に収集、利用される

ことについては、これが漏洩等によって拡散し、悪用され、自己の私生活の平穏が侵害されることへの不安が高まっており、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おり、住民の間に強い不安をもたらしている。このような社会状況に鑑みれば、私生活の平穏や個人の人格的自律を守るためには、もはや、プライバシーの権利を、私事の公開や私生活への侵入を拒絶する権利と捉えるだけでは充分でなく、自己に関する情報の他者への開示の可否及び利用、提供の可否を自分で決める権利、すなわち自己情報をコントロールする権利を認める必要があり、プライバシーの権利には、この自己情報コントロール権が重要な一内容として含まれると解するべきである。」

前記２で述べたのと同様、金沢地裁判決も、自己情報コントロール権の人権性を、高度情報ネットワーク社会における私生活の平穏と人格的自律の保護により根拠づけている。そして、自己情報コントロール権の内容についても「自己に関する情報の他者への開示の可否及び利用、提供の可否を自分で決める権利」と判示しているとおり明確である。

（３）大阪高裁平成１８年１１月３０日判決（民集６２巻３号７７７頁、判時１９６２号１１頁）

同じく住基ネットに関する標記判決（以下、「大阪高裁判決」という。）は以下のように述べている。

「　……　他方、社会の変化に伴い個人情報の取り扱われ方は変化していく。とりわけ、情報通信技術が急速に進歩し、情報化社会が進展している今日においては、コンピュータによる膨大な量の情報収集、保存、加工、伝達が可能となり、また、インターネット等によって多数のコンピュータのネットワーク化が可能となり、人は自己の個人情報が他者によってどのように収集、利用等されるかについて予見、認識することがきわめて困難となっている。このような社会においては、プライバシーの権利の保障、それによる人格的自律と私生活上の平穏の確保を実効的なものとするためには、自己のプライバシーに属する情報の取り扱い方を自分自身で決定するということが極めて重要になってきており、その必要性は社会において広く認識されてきて

いるといえる。今日の社会にあって、自己のプライバシー情報の取扱いについて自己決定する利益（自己情報コントロール権）は、憲法上保障されているプライバシーの権利の重要な一内容となっているものと解することが相当である。」

大阪高裁判決は、自己情報コントロール権の人権性の根拠として、先に引用した金沢地裁判決と同様、高度情報ネットワーク社会における私生活の平穏と人格的自律の保護を指摘するだけではなく、その必要性が社会において広く認識されてきているとの事実も指摘している。

そして、自己情報コントロール権の内容については、「自己のプライバシー情報の取扱いについて自己決定する利益」と判示している。これは先の金沢地裁判決の定義である「自己に関する情報の他者への開示の可否及び利用、提供の可否を自分で決める権利」を若干抽象化した程度の表現であるが、これを導くための根拠には前述のとおり人格的自律の保護が要素として含まれており、その限りで導かれる自己情報コントロール権の内容について本質的な差異が認められないということも明らかである。したがって、自己情報コントロール権の内容は明確である。

（４）ドイツ連邦憲法裁判所１９８３年１２月１５日判決

国勢調査に関する標記判決（以下、「ドイツ国勢調査判決」という。）は以下のように述べている。

「基本法秩序の中心は、自由社会の構成員として自由な自己決定を行う個人の価値と尊厳にあるといえるが、その保護に役立つのが、基本法一条一項と相俟って同法二条一項において保障されている一般的人格権（Allgemeines Persönlichkeitsrecht）である。そして、人格権は、自己決定権の思想により、個人の生活状況が、いつ、いかなる範囲で開示されるかを、原則として自らが決定するという権能を含むものである。かかる権能は、今日及び将来の自動化されたデータ処理の状況下では、特別に保護を必要とする。とりわけこの権能は、今日では以下のような理由で危機にさらされている。すなわち、自動化されたデータ処理によって、特定の又は特定しうる個人の人的状況及び物的状況に関する事項（以下、個人に関連するデータという）を、技術上

無制限に蓄積することができ、且いつでも距離に関係なく瞬時に引き出しうるということによってである。のみならず、自動化されたデータ処理は、複合的な情報システムが出来上がった場合には特に、他のデータ集積と結びつくことにより、一方的に市民の個人像を作り上げることを可能としてしまう。そしてその場合、当事者はこの個人像の正確性やその利用について十分なコントロールを行うことができないのである。それゆえ、従来からは知られていない方法で個人の行動を監視し、これに影響を与える可能性が増大しているといえる。それは、当局が関心を持つという心理的な圧迫を加えることで、各人の行動に影響を及ぼすことができるものなのである。したがって、人格権の自由な発達は、現代のデータ処理の諸状況の下では、自己の個人的データの無制限な調査、蓄積、使用、提供から各人を保護することを前提とする。それゆえ、この保護は、基本法一条一項と相俟った同法二条一項の基本権に含まれるものである。その限りで、この基本権は、各人に自己の個人的データの開示、使用について原則として自ら決定する権能を保障するものといえる。」（鈴木康夫・藤原静雄「西ドイツ連邦憲法裁判所の国勢調査判決［上］」『ジュリスト』８１７号・１９８４年7月１日付・６４頁）

ドイツ国勢調査判決は、前記日本の裁判例の考え方よりも端的に、自己情報コントロール権を、自己決定権（人格的自律）の思想により、人間の尊厳（ドイツ憲法（ボン基本法）第１条）に基づく人格権そのものの権能として肯定している。「人間の尊厳」に基づく人格権の本質とは、自分の生き方のルールを自分で決めるという自律のことであるから、自己情報コントロール権は自律的意思決定の要素として、人間である以上当然に認められなければならない権利であるとされ、したがってこれが侵害されると個人の行動の自由と人格の自由な発達が害され、その結果、自由な自己決定をなしうる構成員の存在を不可欠とする基本法秩序（立憲民主主義）自体が害されるとされている。

そして、ドイツ国勢調査判決における自己情報コントロール権の定義は、「自己の個人的データの開示、使用について原則として自ら決定する権能」であり、これもすでに紹介した日本の裁判例における定義と若干異なる表現であるとはいえ、上記判決は「　……基本法一条一項と相俟った同法二条一

項の基本権に含まれるものである。その限りで　……」と明確に述べられているように、「人間の尊厳の不可侵性を規定した基本法１条１項に基づく人格権に基づく限りで」との明確な解釈基準が示されており、したがって、その本質的内容は明確である。

ちなみに、ドイツ国勢調査判決のさらなる意義をここで指摘しておくと、それは自己情報コントロール権が人格的自律という人間の主体性確保のための不可欠な利益であることから、その侵害は国民が国家の客体的な道具や素材にされてしまうことを意味し、その結果は自由な自己決定をなしうる構成員の存在を不可欠とする基本法秩序（立憲民主主義）自体の存立をも危機に陥れることになるというロジックを明言することにより、自己情報コントロール権は、その侵害が最終的には立憲民主主義の破壊にまでつながるほどの重要な人権であるということを強調した点にある。したがって、自己情報コントロール権の不可侵性は最大限に尊重されるべきなのである。

（５）佐藤幸治名誉教授の「自己情報コントロール権」

佐藤幸治名誉教授は、プライバシー権について、以下のように論じている。「プライバシーの権利は、 個人が道徳的自律の存在として、自ら善であると判断する目的を追求して、他者とコミュニケートし、自己の存在にかかわる情報を開示する範囲を選択できる権利として理解すべきものと思われる。このような意味でのプライバシーの権利は、人間にとって最も基本的な、愛、友情および信頼の関係にとって不可欠の生活環境の充足という意味で（フリード）、まさしく「幸福追求権」の一部を構成するにふさわしいものといえる。」（『日本国憲法論』（成文堂 2011 年 4 月）182 頁）。

自己情報コントロール権は、これまで紹介してきた日本及びドイツの裁判例においてはどちらかといえば立憲民主主義を支える国民個人の自由な自己決定と自己統治の利益の場面を中心に語られていた。これに対し、上記佐藤幸治名誉教授の主張においては、「他者とのコミュニケート」の場面において現れる「愛」、「友情」及び「信頼」といった契機が強調されており、自己情報コントロール権を、「自律的な個人による自律的な他者関係の実現あるいは構築基盤」として位置づけようとされているように思われる。すなわ

ち、佐藤幸治名誉教授によれば、ある他者に対する自己のプライバシー情報の開示は、その他者に対し愛や友情や信頼を求め、あるいは与えるとの意思表明あるいは自己決定であり、逆にその不開示は、その他者に対し私が無関心であること、あるいは私に対して無関心であって欲しいとの意思表明あるいは自己決定ということであろう。これは自律的個人による自己実現が、このように自己情報をコントロールすることに基づいて他者との適切な距離の取り方を主体的に自己決定することにより、自己固有の道徳あるいは幸福観に基づいた他者関係を構築する点にあるという事実に着目し、自己情報コントロール権をこのような個人の幸福追求にとって不可欠な要素として基礎づけようと試みる考え方ではないかと思料される。

そうすると、佐藤幸治名誉教授も、個人を「道徳的自律の存在」と把握することによって、その人格的自律を充足ないしは要素とするものとして自己情報コントロール権を肯定していると解される。したがって、強調されるニュアンスが若干異なるとしても、自己情報コントロール権の内容を明確に限定する根拠はやはり個人の人格的自律権であり、その内容については他の裁判例等の考え方と本質的差異はないのである。

３　自己情報コントロール権の外延

（１）以上述べてきたように、自己情報コントロール権の実定法上の根拠は明確であり、したがって、その解釈根拠たる理念も明確である。だからこそ、その内容についても、論者によって多少の表現やニュアンス上の違いはあるとしても、本質的な部分については一致するのである。

要するに、自己情報コントロール権の根拠は憲法１３条の解釈根拠である個人の人格的自律であるから、その内容についても、個人の人格的自律権を害するかどうかという基準に従って判断することにより、明確な結論を導くことが可能となるのである。

以上のような観点からすれば、先に引用した金沢地裁判決も述べていることであるが、自己情報コントロール権が認められる場合に対象となる情報の典型としては、思想、信条、宗教、健康等にかかわるいわゆるセンシティブな情報を挙げることができる。

もっとも、たしかにその外延については明らかではなく、にわかには分類が困難であるような限界事例もあろう。しかし、外延部分に曖昧さが認められることは、自己情報コントロール権の人権性を否定すべき理由にはならない。こうした外延についての曖昧さは、表現の自由をはじめあらゆる典型的な人権についてもある程度までは認められるものである。したがって、外延部分に曖昧さがあることは自己情報コントロール権の人権性を否定する理由にはならない。外延部分の曖昧さを理由に典型事例における自己情報コントロール権の人権侵害性を否定することは本末転倒である。

（２）個人番号（マイナンバー）制度は、個人番号が様々な個人情報の名寄せのためのマスターキーとしての役割を果たすことになり、また個人番号の民間流通が広く前提とされる以上、それによる影響は自己情報コントロール権の外延部分のみににとどまると解する余地は全くない。すなわち、現代高度情報ネットワーク社会において個人番号制度が現在の制度設計のままで本格的に運用されるようになれば、国民は、まず税と社会保障関係の情報（これ自体センシティブ性の高いものである）、そして更に将来的には、思想、信条、宗教等に関わる（それらを推知しうる）センシティブ情報についても国家や他人によって集積される状況が生じる具体的危険性が認められるのであり、それ故、個人は監視されていると感じ、萎縮効果により、その自律的意思決定や行動の自由に対する悪影響も極めて大きくなる。この点に関する主張は追って詳論する。

４ 小括

以上述べてきたように、自己情報コントロール権の実定法上の根拠は明確であり、それは差止請求・削除請求の法的根拠となりえる憲法１３条が保障している人格的自律権に基づくものであるということである。

そして、自己情報コントロール権の内容もその根拠条文である憲法１３条の理念（趣旨）から導くべきであるという点で明確である。

確かに外延部分については不明確な部分があるかもしれないが、そのことは自己情報コントロール権の憲法上の人権性を否定する根拠にはならず、しかも本件訴訟で問題とされている個人番号制度においては、自己情報コントロール

権の中核部分の侵害が問題になるのであるから、その外延部分の不明確性を問題とする必要はない。

したがって、現行制度設計に基づく個人番号制度が憲法上の人権である自己情報コントロール権の中核部分を侵害する制度であることは明らかなのであるから、被告である国がこの制度が違憲ではないと主張するのであれば、国はその人権制限の合理的根拠について厳格な主張立証を行うべきなのである。

第2 現代社会における自己情報コントロール権の重要性

はじめに

第1で述べたように、そして、そこで摘示した判決理由の中でも指摘されていたように、自己情報コントロール権の人権性を顕在化させる原因となった社会状況の変化は、現代における高度情報ネットワーク社会の急激な発展である。それは、従来においてはあまり重要視されてはこなかったプライバシー情報の収集・集積・保管・利用による人権侵害の危機を劇的に高めることになった。

以下では、こうした社会状況の変化が、いかにして自己情報コントロール権の重要性を高める結果になったかについて具体的に詳論する。

1 紙媒体時代と異なる現代のプライバシー情報を取り巻く状況

現代のプライバシー情報は、コンピュータによりデジタル情報として管理され、また、日々大量に収集保存利用等されている。そして、それらのコンピュータはネットワーク化されている。すなわち、ネットワーク化された高度情報化社会となっている。これにより、かつてのように、紙媒体により個人情報が保存されたり、新聞等の紙媒体により私生活が暴かれたり、といった時代のプライバシーの保障とは、質的に全く異なる時代に突入している。

本件では、この点の理解なしには問題の本質に迫ることができないものであるので、以下、その特質の要点をまとめるならば、以下のとおりである。

①「高度情報化社会」においては、個々人の様々な個人情報が、大量に収集・保存・利用等されており、それらの個人情報が、コンピュータによって、デジタル情報（個人データ）として処理されている。

② デジタル化された情報は、瞬時かつ容易に複製を作成でき、しかも複

製による情報の劣化は生じない。

③　デジタル化された情報は、ネットワークにより、瞬時・大量・広範囲に伝達・伝播することが可能であり、いったん伝播された情報を回収することは、事実上不可能である。

④　さらに、人間の能力では不可能であったデータ処理、例えば、ネットワーク上にある無限大ともいえる膨大な情報の中から、コンピュータによって、ある個人の、一定条件の情報を、検索・名寄せして、データマッチングすることが可能となっているし、「ビッグデータの活用」の名の下に、そのようなデータの活用が重要性を持つに至っている。そして、それにより、当該個人の人物像を作成すること、言い換えるならば、当該個人のプライバシーを丸裸にすることも可能になっている。また、データの集積の仕方によっては、歪んだ個人像を造り出すことも出来るようになっている。その集積されたデータの中に誤ったデータが混入するならば、誤った個人像が作り上げられる危険性もある。

⑤　現実世界における、対面による成りすましだけでなく、ネットワーク上でＩＤとパスワードを冒用するなどして、成りすましをすることも可能となっている。

以上のように、プライバシーを取り巻く状況は、紙媒体時代とは、情報の収集、保管・管理、利用、開示・提供のすべての場面で、量的にも、質的にも大きく変化している。

２　現代社会におけるプライバシー情報に対する危険性

以上に述べた特質を基に、現代のプライバシー情報に対する危険性をまとめるならば、以下のとおりとなる。

ア　大量漏えい・改ざん等の危険性

a　上述の①②③の特質から、現代コンピュータ・ネットワーク社会においては、まず、大量漏えいや改ざんのおそれが大きくなっている。この点は、紙媒体で個人情報が管理されていた時代には考えられなかった、数十万件、数百万件単位の個人情報漏えい事件が頻発していることから、公知の事実である。

b　さらに、インターネット利用の拡大により、ネットワーク経由の情報漏洩事件（サイバーアタック）が頻発するようになっている。

紙媒体で個人情報を管理していた時代には、その紙媒体を保管していた場所を物理的に防御していれば漏洩等は防ぎ得た。また、コンピュータ（大型サーバ）で個人情報を管理・処理するようになってからも、それらのコンピュータがネットワークで接続されるようになるまでは、そのコンピュータの設置された部屋を物理的に防御することで漏洩等は防ぎ得た。

ところが、インターネット利用の時代に入ったことにより、ネットワーク経由の攻撃が可能となった。当該コンピュータが置かれた部屋を物理的に防御するだけでは漏洩等を防止することは不可能となったのである。この点は、近時大きく問題となっている電子メールを利用した「標的型攻撃」などに端的であるし、きわめて深刻な危険性である。

c　付け加えるならば、デジタル情報の特質として、情報が盗み出されたり、漏えいしたり、また、改ざんされたりしても、その痕跡が残りにくいという危険性がある。

d　紙媒体時代から、プライバシーは一旦知られてしまえば回復不可能なものであったが、漏洩した個人情報がインターネット上に流出した場合には、その回収は事実上不可能となる上、永久にネット上から消えることがなくなる危険性も発生している（「忘れられる権利」などが問題になるゆえんである）。

以上のことから、現代の高度情報ネットワーク社会におけるプライバシー情報に対する危険性は、紙媒体の時代とは質的に異なり、飛躍的に高まっているのである。

イ　データマッチングの危険性

より深刻なのが、データマッチングによるプライバシー侵害である。

上述④で指摘したように、紙媒体時代のデータマッチングは、人が手作業で、それらの情報を検索し、名寄せした上で、突き合わせてマッチングするしかなかったため、その作業は人間の肉体的能力の限界から処理能力に大きな限界があった。しかし、コンピュータによる情報処理技術の飛躍的進展によって、仮に数十億、数百億といった膨大なデータであっても、それらを処理することが可能な時代を迎えている。

したがって、この情報処理技術の質的転換に応じて、データマッチング(個人情報を名寄せし結合することによって、その者の趣味嗜好や生活スタイルなどの人物像を作り出すこと・プロファイリング)の危険性が飛躍的に高くなっている。

ウ　萎縮効果（チリング・イフェクト）

情報主体（本人）の同意なき情報収集や提供等がなされるような状況におかれたならば、もしくはイで述べたようなデータマッチングがなされるような状況におかれたならば、否、そのような「データマッチングが行われるかもしれない」という危惧感を抱かせるような状況が作られたならば、ひとびとに萎縮をもたらす。たとえば、様々な個人情報がマッチングされて、自分に関して、“マイノリティ"グループに関係している人物像、“反政府”的傾向を有する特定の集会に参加しているという人物像、特定の意見を表明しているという人物像が作られた、もしくは作られるかもしれないということを怖れて、「参加しないでおこう」、「意見を表明しないでおこう」という自由な活動に対する「萎縮効果」が発生する可能性が高いからである。

なお、データマッチングと萎縮効果の問題について、前述のドイツ国勢調査判決は、１９８３年段階において、既に明確にその危険性を指摘している。

インターネットが一般化する前である１９８３年段階において、このような明快かつ本質に踏み込んだ判断がなされている点において、この判決は非常に注目されるべきものである。

エ　単純な個人情報に関するデータマッチングの危険性

ところで、このような「データマッチング」の対象となる個人情報は、思想信条や病気に関する情報などのように、内容的に誰の目にも「プライバシー」と評価される情報（センシティブ情報）に限らない。すなわち、たとえば、「Ａという個人が、ある時点で、特定の場所を通過した」という情報は、それ自体を単独で取り上げれば「プライバシー」と評価できないような個人情報であることが多いであろう（しかも、個々の「通過情報」は公衆の目に触れている）。しかし、このような情報でも、一定数集積すれば、「Ａという特定人の行動および行動パターン、立ち寄り先」という、意味のある情報となるのであり、国家機関が勝手に収集してはいけない情報であることは明

らかである（このことは、たとえば、警察官が、被疑者でもない人物を、追尾して、その行動を監視することのプライバシー侵害性、違法性を考えれば明らかである）。

そして、さらにこのような「行動情報」と「Aに関するその他の情報」などを「データマッチング」すれば、Aの思想・信条や消費傾向などを推知できる情報までもが明らかとなる可能性が高いのである。また、現代のコンピュータ・ネットワーク技術を駆使すれば、そのような膨大な“単純情報”のマッチングと、そこからセンシティブな情報を抽出することは容易に可能となっているのである。

3　データマッチングのキーとなる「共通番号」の危険性

以上述べたように、データマッチングがプライバシーに及ぼす危険性は極めて深刻であるところ、そのような「データマッチング」の強力な武器となるのが「共通番号」である。

（1）「共通番号」と「限定番号」

共通番号は、分野毎に別々に付された番号（限定番号）と異なり、分野を超えてある個人を特定し識別する番号であるから、その番号をキーとして分野を超えた個人情報の名寄せが可能となる。しかも、国民と外国人住民の全員に対して、漏れなく（＝悉皆性）、重複しない（唯一無二性）個人識別番号を「共通番号」として割り振るならば、その機能は最大限に発揮される。

すなわち、例えば、運転免許証番号は運転免許行政上の個人情報の整理にしか使われていない「限定番号」であるから、この番号をもって正確に名寄せ出来るのは、運転免許行政分野の情報に過ぎない。ところが、「A」という個人に対し運転免許行政分野、税金の分野、社会保障の分野などいろいろな分野に共通の個人識別番号（例えば「12345」という共通番号）を割り振っておけば、Aに関する情報を氏名や住所、生年月日、性別の 4 情報で名寄せ・突合する面倒な手間は必要なく、いろいろな分野のデータベースや情報の集積の中から、当該番号だけを「マスターキー」として、Aに関する個人情報を、もれなく、かつ、他者のデータと間違うことなく、

容易かつ正確に名寄せすることが可能となるのである。

（２）共通番号がない場合の名寄せ（同一人性確認）の方法

共通番号がついていない場合は、氏名等の４情報で名寄せせざるを得ない。しかし、そのような名寄せにおいては、漢字の異体字（「齋藤」と「斎藤」と「斉藤」など）で表記してある場合や、氏名住所が変更になっている場合などは、Ａに関する情報であるにもかかわらず、Ａではない者の情報と認識されて、それらを漏れなく名寄せすることは不可能である。反対に、同姓同名の他人の情報が間違って名寄せされる可能性もある。これを４情報だけで正確に名寄せしようとするならば、市町村がバラバラに管理しているＡの住民票や戸籍をたどって、その同一人性を確認する必要があるのである。

（３）利便性と裏腹の危険性

以上述べたように、共通番号はデータマッチングに関して強力な武器となるものである。これは、データ処理の効率性という観点から見ればきわめて利便性の高いものである。しかし、プライバシー権（自己情報コントロール権）の保障という観点から見るならば、それを脅かす強力な武器となる。

例えば、複数のデータベースから個人情報が流出したとして、流出個人情報に共通番号がついておらず、名寄せのキーが氏名、住所等の４情報しかなかった場合と、共通番号が付いていた場合を対比してみるならば、それを悪用してデータマッチングを行おうとする者にとってどちらが便利かは明白であり、そのプライバシー侵害の危険性が後者の方が圧倒的に高いことは一目瞭然である。

プライバシーや人格的自律を守るために、データマッチングをしたり共通番号を付すことが許されない、という趣旨は、以上の点から明らかである。

４　高度情報ネットワーク社会においてプライバシーを守るための条件

以上述べてきたことを前提として、現代の高度情報ネットワーク社会においてこのような危険性からプライバシーを保護するためには、自己情報コントロー

ル権をプライバシー権として保障してゆくことが大前提であるが、更に、以下のような制度的な保護策をとることが必要となっていると言わざるを得ない。

以下、プライバシーを守るための条件（原則）について、簡潔に述べる。

（１）共通番号の利用禁止原則

上述した共通番号制の危険性からプライバシーを守るためには、共通番号の利用を原則禁止することが必要である。

確かに共通番号を利用すればデータマッチングを容易になしうる。しかし、共通番号を使うというのは、いわばアナログ時代の名寄せの技術なのであって、情報通信技術が発達した現代社会においては、分野別の「限定番号」を使いながら、暗号技術などを用いて必要な名寄せ・照合を行なうことが可能となっているし、それが趨勢になっている。また、上述のようにプライバシー侵害の大規模化、深刻化に対するプライバシー保護の要請が高まってきていることから、「共通番号」から「分野別番号（限定番号）」へというのが世界の趨勢になっている。例えば、世界有数の電子政府を構築しているオーストリアでは、分野別番号制と暗号技術などを用いたデータの突合を行うシステムを構築しているし、アメリカや韓国などでは、共通番号制の深刻な弊害を緩和するため分野別番号制へ移行しようと多大な努力を行っている最中である（これらについては追って詳述する）。

（２）「事故前提社会」という前提で制度構築をする必要性

現代社会においては「情報が漏れることを前提の安全対策」をとらなければならない。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た（「第２次情報セキュリティ基本計画」（同年２月３日付）。

情報流出事故を前提とするならば、仮に漏洩事故が起きた場合でも被害が極力小さくなるように、不必要な情報は収集・保管しないこと、情報の分散管理をすること、及び、漏洩した情報が名寄せがされにくい「分野別番号（限

定番号）制」を基本におくべきことは当然であり、その観点からも、世界の趨勢である分野別番号制を採用することが原則となるのは当然である。

（３）独立した専門的第三者機関の必要性

膨大な個人情報が流通している現代社会においては、自己のプライバシーを守るだけの知識も能力も有しない個人に代わって、行政から独立してその手続き違反等のプライバシー侵害がないことを監視監督する「独立の第三者機関」システムを作っておくことが必要である。

ＥＵ等では当然の制度となっている制度であり、例えばオーストリアなどでは、第三者機関がデータ突合の要のシステムを管理するなどして監督機能を果たしている。

このような組織がなければプライバシーの保護を全うすることは出来ない時代になっているのである。

日本の個人情報保護委員会の不十分性については訴状で指摘したとおりであるが、追って更に主張する予定である。

（４）ＰＩＡ実施によるプライバシー侵害最小化の必要性

プライバシー影響評価（Privacy Impact Assessment、略称：PIA）を実施して、制度設計・構築段階から、「プライバシー・バイ・デザイン」（設計段階からデフォルト状態でのプライバシー保護措置を組み込むことなどを求める考え方）の思想にのっとって、プライバシーに対する侵害度を最小化する取り組みも必要である。

訴状でも指摘したとおり、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。」ものであり、「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。」ことを目的としているものである（この定義には原被告間で争いがない）。

環境影響評価制度のように、事前にプライバシーに対する影響をチェック

させなければ、傷つきやすいプライバシー優先は実現出来ない。

このようなプロセスを経なければ、いったん作られた情報システム、特にインフラとして構築される情報システムは拡張する一方であるのが常であるから、プライバシーに対する深刻な影響を与えるといわざるを得ない。

今回の制度創設にあたって導入された特定個人情報保護評価制度、日本版プライバシー・インパクト・アセスメント（ＰＩＡ）といわれるものの不十分性についても、追ってさらに主張する予定である。

第３　被告には、更に具体的に制度の安全性に関する主張を行う義務が存する

１　被告も釈明で認めた現代における共通番号制の危険性

被告は、「求釈明に対する回答書」（平成２８年１０月４日付）において、「飽くまで抽象的な一般論として」という限定付きではあるが、「番号制度において想定し得る客観的な危険としては、

（ⅰ）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・集約された個人情報が外部に漏洩し得る危険性、

（ⅱ）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、

（ⅲ）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、

（ⅳ）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、

（ⅴ）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等が考えられる。」ことは認めた（平成２８年１０月４日付「求釈明に対する回答書」。但し、（ⅰ）から（ⅴ）は引用者が挿入）。

これらは、原告らが指摘してきた本番号制度（共通番号制度）の危険性を被告も一応は前提としていると評価出来る。

２　被告には原告らのプライバシーの安全を確保する責務があり、番号制度の安全性について具体的に説明すべき義務がある

（１）被告のプライバシーの安全を確保する責務

被告は、法律等により強制的に収集した原告らの個人情報に個人番号を付して、個人番号のシステムの中で保管、利用、提供等しようとしている。これにより、上述したように、原告らのプライバシーに対する危険性は従前より著しく高まっているのである。

したがって、被告には、当然、その安全性を確保する責務が存するし、安全であることを具体的に説明する義務がある。

（２）被告の説明は概括的なものに止まっている

ところで、被告は、答弁書や第１準備書面において、制度の安全性について主張しているものの、それらは制度の概括的な説明に止まっており、制度、システムの具体的内容や現場の運用の具体性に即した安全性に関する主張は未だなされていない。

特に、制度の柱となる情報提供ネットワークシステムは、平成２９年から稼働開始予定であり、その具体的制度内容、運用方法、現在行われていると思われる運用テストの結果や今後の利用拡大の中身等、原告らのプライバシーの安全に関わる情報は未だにほとんど明らかにされていない。

また、本制度のもう一つの柱となる個人番号カード（マイナンバーカード）についても、その利活用拡大の検討が急速に具体化されているところであるが、その具体的中身と安全対策について、ほとんど説明がなされていない。

（３）個人番号カード管理システムの障害事件等の発生

平成２８年１月１３日以降、個人番号カードの管理システムの障害が継続した。しかし、同システムを管理する地方公共団体情報システム機構（Ｊ－ＬＩＳ）が、その障害の「根本的な発生原因が判明」し、同年４月１５日及び２２日に「根本的な発生原因を取り除くための対応策を実施」したと公表したのは、最初の障害発生から３ヶ月以上も経過した同年４月２７日であった（「カード管理システムの障害に対するお詫びとご説明」地方公共団体情報システム機構理事長西尾勝作成）。

同年６月２２日付の「システム障害の総括を踏まえた対応について」（地方公共団体情報システム機構代表者会議議長飯泉嘉門作成）によると、今回の障害の原因は「事業者における設計不備、適合性評価の不足に起因するものであった」とされ、また「コンソーシアムを構成する事業者間の連携不足

により原因特定に時間がかかった」とされている。

以上の障害事件１つを見ても、情報提供ネットワークシステムを含む個人番号のシステムの具体的な安全性に対する信頼をおくことは出来ない。

また、消費税率を１０パーセントにアップした際、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が検討されたことに対し、「個人番号カードを買い物のたびに商店に渡すようなやり方では、個人番号を盗み見られたり、カードを紛失したりして、個人番号の漏洩の危険が高くなる」という批判が出ていた。現在検討されている個人番号カードの利活用促進は、要するに個人番号カードを多目的に利用することを目指すものであって、日頃からカードを持ち歩き、利用の際に相手方にカードを渡したり示したりすることになるのであって、上記と同じ問題が発生する。しかし、これらの危険性に対する根本的な安全対策についての説明はなされていない。

（４）被告は、現場に即した具体的安全対策を説明すべき義務がある

以上述べたように、被告は、原告らのプライバシー情報の安全確保策について具体的に説明する義務が存するにもかかわらず、未だその説明を行っていない。すみやかに具体的な安全対策について説明を行うべきである。

仮に被告においてこれを行わないというのであれば、原告らにおいて不明な点について求釈明を行うなどした後に、プライバシーやセキュリティ上の問題点について更に主張を行ってゆく予定である。

以上