令和２年（ネ）第１０９号マイナンバー離脱等請求控訴事件

控訴人　　坊真彦　外

被控訴人　国

控訴審第１準備書面

２０２１年8月２５日

名古屋高等裁判所金沢支部　御中

控訴人ら訴訟代理人

弁護士　岩　淵　正　明

第１　はじめに

本準備書面は，玉蟲由樹教授（甲５０）の意見書に基づく主張書面であり，主として控訴理由書５頁「第２　憲法１３条で保障される自由に関する判断の誤り」の内容に関連するものである。

以下，プライバシー権保障の実体的内容を明らかにした上で，マイナンバー法の目的の正当性，個人番号の生成・指定・利用の必要性・合理性，データマッチングの手段としての相当性，さらにマイナンバー法が濫用・漏洩の危険を秘めていることについて論ずる。

第２　プライバシー権保障の実体的内容

１　自己情報コントロール権の重要性

（１）憲法１３条により保障されるプライバシー権の中でも，中核的意味合いを持つのが，「自分の私的な情報について，それをいつ，いかなる範囲で他者に対して明らかにするのかを自分自身で決定するという個人情報に関する自己決定権（以下，「自己情報コントロール権」という。）」である。そして，この自己情報コントロール権は，公権力による個人情報の取得から保存・蓄積，利用，第三者への譲渡（提供）へと進行しうる情報処理のプロセス全体について，情報主体によるコントロールを認めるものである。

また，一旦デジタルデータ化されネットワークの中に取り込まれた個人情報は，ネットワークの内外で際限なくコピーされ，いつまでも消えずに残り，情報

主体の思わぬところで情報同士が結びつけられ利用される危険性がある。そこで，個人情報が公開・暴露されるという「実害」が生じていなくとも，個人の知らないところで個人情報がやり取りされ，情報が結びつけられ，利用されるという「危険」を生じているという状況こそがプライバシー侵害的であると考える必要がある。

それゆえ，情報処理技術の進展は，必然的に自己情報コントロール権の重要性を高める結果となるのである。

（２）裁判所においても，京都府学連事件や指紋押捺拒否事件などで問題となった「取得」段階，京都市前科照会事件や住基ネット訴訟などで問題となった「利用・開示」段階など，さまざまな段階でプライバシー権を保障する方向での判断が示されている。

こうした裁判例からも，憲法上のプライバシー保護の要請及び自己情報コントロール権の理解は，裁判所においても原則として共有されているものと言える。

２　原判決の誤り

しかしながら，原判決においては，こうした自己情報コントロール権について十分な理解がなされていない。

（１）原判決は，「憲法１３条は，国民の私生活上の自由が公権力の行使に対しても保護されるべきことを規定しているところ，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又は公表されない自由を有するものと解される」とした上で，この自由は「行政機関等が個人情報を収集，保有，利用，提供等する過程においても認められる」という。しかし，その一方で，原告らが主張する自己情報コントロール権については，その憲法上の保障を否定している（原判決４１，４２頁）。

すなわち，原判決は「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」は憲法上保障されるものの，これを越えた範囲における「個人情報について包括的にコントロールする権利」までは憲法上保障されていないと見て

いるのである。

（２）また，原判決は，憲法１３条からは「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」のみが保障され，「みだり」なものに該当しない限りは，公権力による個人情報の第三者開示・公表といった行為があっても憲法上の問題を生じないと理解しているようである。つまり，公権力による「みだり」な個人情報の開示等があった場合には憲法１３条によって保護された自由が対抗し調整が図られる一方，「みだり」なものに至らない場合には個人には憲法上の権利が承認されていないのである。

しかし，このような理解は，最高法規である憲法によって人権を保障し，あらゆる公権力行為を拘束するものとして人権を理解する憲法上の人権解釈論において許容されるものではない。

むしろ，憲法１３条のもとでは，人は原理的に自由な存在として承認されており，個人情報についても原理的に当該個人に処分権限があると解される。

もちろん，こうした原則的な処分権限も，必要かつ合理的な制約には服しうる。しかし，だからと言って，「みだり」なものでない限り公権力は自由に際限なく個人の情報を収集等してよいというわけではない。そうでなければ，最高裁判例等が，個人情報の収集等に関して，正当な目的や必要性・合理性を満たす手段を要求してきたことの説明がつかない。

憲法上の権利・自由は，公権力の行使が「みだり」なものである場合にのみ個人の側に認められるものではない。まずは個人に原理的な自由が保障され，それに対する正当な目的や必要性・合理性を満たす手段での介入のみが憲法上正当化されるにとどまる。正当な目的を持たず，あるいは正当な目的を有していてもその手段が必要性・合理性を満たさない場合に，介入が「みだり」なものとなるのである。

これに対して，原判決は，自己情報コントロール権を基礎として，それを実現するために結果的に「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」が保障されるという人権保障の当然の経緯を無視して結果のみをつ

まみ食いすることで，基本的人権に関する明らかに誤った見解に依拠している。

（3）さらに原判決は，「多種多様な個人情報が収集，保存，利用，提供される各場面において，一律に本人に事前の同意の機会を与えることまで憲法１３条が保障していると解することは困難」（原判決４２頁）とする。

しかし，自己情報コントロール権が個人情報の取扱いに関する基礎となるという観点からすれば，個人には原則として自己情報コントロール権，ひいては「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」があり，ただ正当な目的の下での必要かつ合理的な手段によってのみこれが制約されるにとどまる，と考えるべきである。

以上のように，原判決は憲法上の人権の保護領域（保障範囲）の問題とそれに対する制約可能性の問題とを混同しており，到底受け入れられない。

3　個人識別性・特定性の高い情報の保護の必要性

（1）自己情報コントロール権が高度情報化社会において特別な意味合いを持つことは，個人番号制度との関係で特に意識すべき事柄である。

個人番号が情報提供ネットワークシステムを通じた分野横断的なデータマッチングのための検索キーとなることはマイナンバー法からも明らかであり，かかる視点からの検討は本件においては不可欠である。また，現在の電子的情報処理技術の下で，どのような個人情報の処理が行われているかを正確に認識することは，自己情報コントロール権の実体的内容を理解し，その保障を具体的に展開する上で重要な作業である。

（2）電子的情報処理技術の進展には，プラスの面がある一方で多くのマイナス面が指摘される。中でも，自己情報コントロール権を考える上でとりわけ重要なのは，それ自体ではとりたてて害のない個人情報であっても，それが他の情報と結びつくこと（データマッチング，名寄せ等）により包括的な人格像を描きうるという点である。

電子的情報処理技術の下では，個人に関する情報はほぼ無限定に集積・結合できるのであり，これによって個人の人格すら「ガラス張りの」ものとなる可能性

がある。

（３）以上を考慮すれば，プライバシー保護の観点において，個人情報の「内容」に着目して保護のあり方を議論する判例のアプローチには問題がある。

たしかに，思想，信条といった極めてセンシティブな情報に公権力が介入できるとすることは当然許されず，情報の「内容」に従った保護も必要である。しかし，現代社会においては，秘匿性が高くないとされる個人情報についても保護の程度を低く見積もることは適切ではなく，情報の集積・結合による「質の変化」に着目した保護が必要であり，だからこそ「重要ではない個人情報はない」と考えなければならない。

４　原判決における情報の秘匿性の程度の判断について

（１）上記３の点についても，原判決の理解は不十分である。

原判決は，「番号制度及び情報提供ネットワークシステムにおいて取り扱われる情報自体は，従前から行政機関等によって取り扱われてきた情報であ」ると述べ（原判決４２頁），結論として憲法１３条に違反しないとする。

しかし，本件において問題となっているのは，個人番号をインデックスとして，これまで各個に存在していた個人情報が結合され，それによってより人格プロフィールに近い新たな情報が作り出されることの問題性である。各個に存在する個人情報のそれぞれが持つ意味や価値がいくら小さかろうとも，そしてそれを収集・保有することにいくら正当性があろうとも，情報結合によって作り出される情報の価値が低いことにはならない。

むしろ，情報結合によって作り出される情報の価値は，それまでの各個に存在していた情報に比べて，はるかにセンシティブな情報となる可能性が高いのである。また，かかる情報結合は質的に「新たな」自己情報コントロール権に対する介入である。

（２）このような情報結合が憲法１３条によって保護される私生活上の自由を侵害するか否かは，改めてそれによって作り出される情報の意義を精査して論じるべきものである。そこで作り出される情報が，人格プロフィールを包括的に映し

出すものであれば，自ずと情報の秘匿性の程度は上昇する。

したがって，原判決の前述のような説示は，個人番号制度によって作り出される情報の秘匿性の高低を判定するための根拠とはなりえない。

（3）さらに，個人番号が情報結合にあたってインデックスとして機能するという見地からすれば，「個人番号それ自体」のプライバシー情報該当性のみを論じることには意味がない。このことは，マイナンバー法２条８項が「個人番号・・・をその内容に含む個人情報」を「特定個人情報」と定義していることにも矛盾している。

個人番号制度において問題となるのは，情報結合によって作り出される包括的な個人情報のプライバシー該当性である。個人番号のみを取り出してその質的な意味でのプライバシー該当性を否定するのは，番号制度の趣旨を見誤った解釈である。

5　自己情報コントロール権の社会的・民主制的意義

（1）以上のような，包括的な人格プロフィールの構築可能性は，それだけで憲法上のプライバシー保護の要請に反するものである。

言うまでもなく，個人は，私的な存在にとどまることも常に公的な存在であり続けることもない。それゆえ，憲法が「人間の尊厳」を保障し，人を「個人として尊重」する場合，そこには個人の公的生活と分離されたものとして私的生活を保護することが含まれている。

したがって，公権力が「人間を強制的にその全人格において記録し，カタログ化する」ような事態は，個人の私的生活の存在意義を認めないことに等しく，人間の尊厳や個人の尊重に明らかに反することとなる。

まさにここに憲法上のプライバシー保障の核心的意義がある。

すなわち，プライバシーの保護は，人間の尊厳や個人の尊重から直接に要求される事柄なのである。

（2）とかくプライバシーという概念については，その個人的な側面・意義が強調され，全体的な利益との衡量においてその価値が低く見積もられがちという問題

がある。

しかし，プライバシー保障には社会的・民主制的な側面・意義も同時に存在している。

デモや政治集会に参加することで，顔写真等の情報から個人の氏名等が特定され，そこでの活動がデータベースに記録され，そしてその情報がどのように利用されるのかを見通せない個人にとっては，行為を差し控える十分な理由となろう。誰が，自分について何を知り，それをどのように利用しようとしているのかが分からない状態で，人は真に自由な自己決定はできず，社会への参加そのものが阻害される。自己情報についてのコントロールがまるで効かない社会は，もはや民主主義社会の前提を失っている。

自己情報コントロール権の社会的・民主制的な意義は，プライバシーについて，全体的な利益との衡量においてその価値が低く見積もられるという一面的な衡量を見直す上でも，十分に意識されるべき事柄である。

6　個人情報の処理プロセスと段階ごとの審査の必要性

（1）憲法上のプライバシー保障が人間の尊厳や個人の尊重に直接関わる問題であり，社会全体，さらには民主制に関わる利益でもあることからすれば，自己情報コントロール権の制約については慎重な憲法上の正当化審査が要求されるべきである。

さらに，かかる正当化審査は，個人情報の取得だけでなく，蓄積，利用，譲渡・開示等の各段階において行われるべきものであると言える。

（2）公権力による個人情報の取扱いを全体的なプロセスの中で把握するならば，最初の段階として認識されるべきは収集・取得段階である。

公権力は，様々な目的から個人に関する情報を収集・取得するが，その取得方法が不適切であったり，正当な目的の範囲を逸脱して情報が取得される場合には，憲法上の問題が発生する。

そして，この段階の後には，情報の利用や記録・保存といった段階があるところ，その目的は取得目的と別々に設定されることもありうる。そのため，取得の

合法性（合憲性）はそのまま利用・保存の合法性（合憲性）を意味するとは限らない。さらに，保存されたデータの（再）利用や譲渡等の段階でも，取得や利用・保存とは異なる目的が存在しうるため，これらは異なる段階として理解される必要がある。

したがって，たとえ取得・収集の段階では適法であったとしても，それをデータベースに記録したりデータマッチングしたり，さらには保存後のある時点で改めて利用することには，連続性がなく，各段階での処理の適法性・合憲性が検討されなくてはならない。

（３）公権力による個人情報の取り扱いの正当化審査に当たっては，プライバシー保護の重要性から，比較的厳格度の高い審査が求められる。

具体的には，個人情報の取得や利用，保存，譲渡等の目的がそれぞれ公共の福祉を追求するものと言えるか，言えるとしても目的達成のための具体的な手段（取得の手段や利用方法，保存形態等）が目的達成にとって必要かつ合理的なものといえるかが厳格に問われるべきである。

７　原判決における情報処理の段階の理解について

（１）原判決は，「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は，行政機関が個人情報を収集，保有，利用，提供する過程においても認められる」と述べ（原判決４２頁），情報処理の段階に言及する。

しかし，ここで中心になっているのは，収集，保有，利用，提供の過程でみだりに第三者への開示・公表が行われてはならないということであり，各過程そのものの問題が意識されているとは言い難い。情報処理の段階的理解が徹底していないのである。

むしろ，問題とすべきは各段階それぞれの権利侵害性である。

（２）個人情報の処理の各段階はそれぞれ別の介入として構成されるべきである。たとえ個人情報の収集が適法に行われたものであったとしても，それが以後の利用や開示・公表を自動的に正当化するものではない。

したがって，利用及び開示・公表についてはそれぞれについての独自の正当化

が要求されるのである。

とりわけ，情報の利用段階は，情報社会において特別な意味を持つ。この段階においては，様々な情報が結合され新たな意味を付与されることによって全く異なるレベルの価値を生じうるから，正当な公権力による介入を越えて，「みだり」な処理が行われる可能性が高いのである。

それゆえ，この段階での自己情報コントロール権への介入は他の段階と切り離して，それ自体の問題として精査すべきものであると共に，収集段階とは異なるより慎重な考慮を必要とする。つまり，この段階での介入については，より厳格な審査基準を用いて，介入目的の重要性及び介入手段の必要性・合理性が審査されるべきである。

（3）原判決の「番号制度が取り扱う情報自体は，・・・従前から行政機関等が取得していた情報であって，番号制度の導入により行政機関等が新たに個人のプライバシーに係る情報を収集，保有するものではない。」（原判決４３頁）という認定は上述の問題を十分に理解していない。

まず，原判決に従えば，番号制度に基づいて管理や提供が行われることになる個人情報は，個人番号制度で利用されることを予定せずに収集された情報であり，収集段階においてこのような利用についての個人の承諾はなかったものと言える。したがって，新たに個人番号制度によってこれらの情報を利用するにあたっては，憲法上の権利に基づく適正な取扱いが強く要請されることになる。

また，収集済みの個人情報であればいかなる利用も可能になるということはあり得ない。すでに情報が行政機関によって管理されている状況から，情報の利用について個人の承諾を要求することが困難であるとしても，行政機関による管理を前提としつつ，自己情報コントロール権の実現が図られる必要がある。

収集済みの個人情報の利用段階での憲法上の保障は，行政機関に対して個人情報の適正な取扱いを求める権利として理解することができる。この場合，とりわけ重視すべきは，客観的な規範による個人情報の適正な取扱いの徹底である。収集済みの個人情報であっても，その利用について行政機関の恣意を排除し，適

正な取扱いルールを構築することによって個人情報の保護を行うべきことは，憲法１３条からの直接の要請だと言える。

（４）原判決はこの点につき，「番号制度による特定個人情報の収集等が原告らの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を侵害するものであるかは，①番号制度において取り扱われる個人情報の秘匿性の程度，②番号制度による個人情報の収集等が法令等の根拠に基づき正当な目的の範囲内で行われているか，③番号制度自体に法制度又はシステム技術上の不備があり，そのために法令等の根拠に基づかずに又は正当な目的の範囲を逸脱して個人情報が第三者に開示又は公表される具体的危険の有無，態様，程度等に照らし，番号制度の運用自体によって，原告らの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る具体的な危険が生じているといえるかによって判断することが相当」だとするが（原判決４３，４４頁），収集，保有，利用，提供等の過程での危険が第三者開示・公表の危険に限定されている限り，情報処理の各段階の固有の問題性は捨象されてしまっている。第三者開示・公表の危険があるかどうかとは別に，収集，保有，利用等がそれ自体みだりなものとなっていないかが厳格に問われるべきである。

とりわけ，利用段階についてはその特殊性を考慮し，より厳格かつ慎重な審査がなされる必要がある。しかし，原審は，個人情報がすでに行政機関によって収集済みであること等を理由として緩やかな審査で足りるとし，情報処理の段階という現代のプライバシー保障にとって重要な問題を軽視しており，明らかに本末転倒である。

また，原判決は上述の判断枠組みにおいて，個人のプライバシーに対する危険の有無を「番号制度自体に法制度又はシステム技術上の不備があり，そのために法令等の根拠に基づかずに又は正当な目的の範囲を逸脱して個人情報が第三者に開示又は公表される具体的危険の有無，態様，程度等に照らし，番号制度の運用自体によって，原告らの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る具体的な危険が生じているといえるか」によって判断しようとするにと

どまる。しかし，前述の観点からは，「法制度上又はシステム技術上の不備」があるか否かに関わらず，個人番号制度による個人情報の利用そのものが，人格プロフィールの構築という新たな「具体的危険」を生じていることを問題とすべきである。

また，原判決は，法制度又はシステム技術上の不備によって生じる具体的危険のみを評価の対象とすることで，個人番号制度のもつ問題性を著しく矮小化している。この点については，情報処理の段階的理解を徹底することによって，判断を正しい方向に向けなおす必要がある。

第３　マイナンバー法の合憲性に関する検討

１　以下では，これまで述べてきた憲法上のプライバシー保障及び自己情報コントロール権の観点から，マイナンバー法による個人番号の生成・指定及びその利用について検討する。

２　個人番号の個人情報性

まず，マイナンバー法に基づいて個人に指定される個人番号が，憲法上プライバシーに係る情報として保護されるかどうかについて検討する。

（１）個人番号は，１２桁の数字の羅列である。それ自体は個人の私的生活に関する事柄を内容として含むものではないし，これらの数字から即座に人の人格プロフィールの一部ないし全部が推知できるようなものでもない。

しかし，個人番号はこれによって特定の個人を識別することが予定され（１条６項），その性質上悉皆性，唯一無二性を持つため，個人番号が付番された特定の個人について高度の識別機能を有するものである。

したがって，それ自体の情報内容がセンシティブでないとしても，個人識別性・特定性の高い索引情報として，機能的アプローチの観点から，センシティブ情報と同様の保護を受ける必要のある個人情報だと言える。

（２）しかしながら，原判決は「個人番号は，住民票コードを変換して得られる番号であって，・・・それ自体に個人のプライバシーに係る情報を含むものではない」（原判決４４頁）として，憲法上の保護を否定する。

これは，指紋押なつ拒否事件で最高裁が指摘した，個人識別性・特定性の高さから「利用方法次第では個人の私生活あるいはプライバシーが侵害される危険性がある」情報としての性質を無視ないし軽視した説示である。このような個人番号の「機能」の軽視は，判決の論理構造そのものを大きく歪める原因ともなるものである。

3　プライバシー介入行為としての個人番号の利用とデータマッチング

次に，マイナンバー法に基づく個人番号の指定と運用が個人情報の処理プロセスのどの段階に関わる問題であるのかについて検討する。

（1）個人番号は，指紋情報や氏名などとは異なり，個人識別情報でありながら個人にもともと備わっていた固有の情報ではない。

また，指紋情報等の固有情報は，公権力の側に帰属する情報ではないため，公権力がこれを知るためには「取得」という段階を踏む必要がある。しかし，個人番号は公権力が一方的に生成・指定するものであるため，公権力側は「取得」の必要がない。それゆえ，個人情報の取得段階での憲法的コントロールは，個人番号については性質上不可能であるといってよい。

（2）しかし，個人番号を公権力が最初から知っており，取得という段階がないということが，利用や保存についても憲法上の問題を生じないということを当然に意味するわけではない。

マイナンバー法は1条において「個人番号・・・の有する特定の個人・・・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」することを予定している。したがって，ここでは個人番号を検索キーとした，異なる分野に属する個人情報のデータマッチングが行われることとなる。これが個人番号の利用に関する最も特徴的な点であると共に，プライバシー保護の観点からも重要なポイントである。

データマッチングが個人のプライバシー及び自己情報コントロール権　に対する介入であることは疑いがない。個人番号を検索キーとして異なる分野に属する個人情報が集積・結合されることは，自ずと個人の人格プロフィールへの到

達可能性を高めるものである。

それゆえ，データマッチングの範囲や規模によっては，それ自体で人間の尊厳や個人の尊重に抵触する可能性がある。

また，データマッチングの範囲・規模がそこまで大きなものでなくても，情報主体が予測不可能な形で個人情報が集積・結合される場合には，自己情報コントロール権に対する侵害を構成しうる。

（3）行政機関の各分野において個別に異なった目的から取得・保存されていた個人情報が分野横断的にデータマッチングされることは，これまでの行政実務では行われなかった新たな形態でのプライバシーへの介入である。

実際，住基ネット訴訟最高裁判決では，データマッチングの危険性の有無が判断において重要な要素となっていた。この判決で最高裁はデータマッチングによりプライバシー情報が「本人の予期しないときに予期しない範囲で行政機関に保有され，利用される具体的な危険が生じている」とした控訴審判決を破棄し，データマッチングの具体的危険は存在していないとの理由を挙げつつ，住基ネットは「自己のプライバシーに関わる情報の取扱いについて自己決定する権利ないし利益」を違法に侵害するものではないと判示した。

ただし，このことは，データマッチングそのものがかかる権利への介入であることまでも否定したわけではない。最高裁は，少なくとも住基ネットにおいてはデータマッチングの具体的危険が排除されていることを示したにとどまる。データマッチングが現実に行われる場合に，プライバシー保障及び自己情報コントロール権との関係でどのような評価をなすべきかは別途検討されるべき事柄である。

（4）マイナンバー法では，個人番号の指定がそのままこれを検索キーとする　データマッチングへとつながるものである。したがって，データマッチングによる個人のプライバシー及び自己情報コントロール権への介入が憲法上許容された範囲内にとどまっているかどうかが大きな問題となる。この際，データマッチングがこれまで行われてこなかった領域に踏み込む，従来よりも強度な個人のプラ

イバシーへの介入であるという認識が前提として共有されねばならない。

以上のように，個人番号とプライバシー保障の関係を考える上では，利用の段階でのプライバシー保障を中心に考える必要がある。そして，個人番号の利用によって，場合によっては人間の尊厳・個人の尊重に抵触することもありうるデータマッチングが具体的に行われるということが重視されるべきである（これが個人番号制度による「具体的な危険」である)。

（５）この点でも，原判決の理解は不十分である。

まず，原判決は，氏名等の「基本４情報は，番号制度の導入前から各行政機関等において収集，保有，管理，利用等がなされていた情報であり，個人の内面に関わるような秘匿性の高いもので」はないという（原判決４４頁)。しかし，この説示は，データマッチング前の段階での個々の情報の秘匿性の高さを述べたものにすぎない。

すでに述べたように，個人番号制度で問題となるのは，個人番号という個人識別性の高い索引情報と，単体ではそれほど重要ではない情報とが結合されて，もとの情報をはるかに超える質や価値をもった「新たな情報」が創出されることである。個々の情報の質に拘泥しているだけでは，個人番号制度を正当に評価したことにはならない。問題とすべきは，データマッチングによって得られる情報の全体についての秘匿性の高さである。

４　個人番号の生成・指定と利用の目的の正当性

次に，マイナンバー法における個人番号の生成・指定と利用が，公共の福祉の目的を追求するものといえるのかを検討する。

マイナンバー法１条では，情報提供ネットワークシステムを用いることで，①効率的な情報の管理及び利用，②行政機関内部での迅速な情報の授受，③行政運営の効率化，④公正な給付と負担の確保，⑤手続の簡素化による国民負担の軽減，⑥本人確認等における利便性の向上といった目的を実現することが想定されている。このうち，①～④は主として行政機関にとっての利益であり，⑤・⑥が国民にとっての利益と解される。

しかし，⑤・⑥のような国民の利益が，プライバシーに介入するための正当な目的といえるかは疑問が残る。本人利益を根拠として公権力によるプライバシーへの介入が正当化されるというのは，本末転倒だからである。

プライバシー保障を原則として考える限り，負担を受け入れあるいは利便性の向上を諦めることで自己のプライバシーの保障を重視する決定を個人がすることもまた自己決定の範囲内にあるというべきである。

5　個人番号の生成・指定・利用の必要性と合理性

マイナンバー法によって追及される目的が正当であるとしても，かかる目的の達成のために投入される具体的な手段に必要性・合理性が認められない場合には，個人番号の生成・指定・利用がプライバシー侵害となりうることは既述した。次はこの点について検討する。

（1）まず，個人番号の生成・指定が前記の①～④を達成する上で必要性・合理性を満たすかが問題となる。

この点，租税の適正な賦課・徴収やきめ細かい社会保障の実現を目指す上では，個人に関する情報の正確な把握が必要であり，その意味で個人識別性・特定性の高い情報の有用性はかなり大きいものといえる。

これに対して，個人番号の生成・指定の先に予定されているデータマッチングは，個人のプライバシーに対する新たなかつ強度な介入であるため，とりわけ慎重な判断が必要となる。具体的には，行政機関によるデータマッチングが，目的の範囲内にとどまるものとして法令上明確に限定されているかを厳格に審査すべきである。

この点，個人番号を用いた情報提供ネットワークシステムの利用は，将来的にはその他の行政分野での利用も予定されており，これに基づき１９条７号は別表第２に定められた範囲に限定して情報提供ネットワークシステムでの情報提供及びデータマッチングが行われることを定めている。

しかし，別表第２では極めて多様な情報が提供されることとなっている。したがって，マイナンバー法の下では，住基ネットでやり取りされるいわゆる「４情

報」とは比べものにならない量と範囲の実体情報が個人番号に紐づけされることになる。

（2）さらに問題なのは，マイナンバー法１９条１６号が「その他これらに準ずるものとして個人情報保護委員会規則で定めるとき」にも提供を可能としていることである。この規定は，個人情報保護委員会規則による追加的な情報提供範囲の拡大を予定したものと考えられる。

しかし，「特定個人情報の適正な取扱いを確保」するために設置された監視機関にすぎない個人情報保護委員会が，情報提供範囲の拡大について権限を持つということになれば，個人のプライバシーへの介入が行政機関の自律的判断によって可能になることとなり，憲法が要求する「法律」による権利の制限（憲法４１条，１３条）という前提を逸脱する。

したがって，同条同号により行われる，マイナンバー法所定の範囲を越える情報提供行為は違憲と評価すべきであるし，同条同号そのものが憲法上の要請に反し違憲とされるべきである。

6　データマッチングの手段としての相当性

（1）以上に加えて，設定された目的とデータマッチングのプライバシー介入の強度との均衡が欠けている場合も，かかる手段には必要性・合理性が欠けるものと考えるべきである。

個人のプライバシーの保護の要請は憲法１３条前段の「個人の尊重」から直接に導かれる要請であると共に，自己情報コントロール権は１３条後段によって根拠づけられる憲法上の権利である。これらは，公権力による情報活動が個人の人格プロフィールへの到達可能性を高く持つほどに，それに対抗する権利として重要性を獲得する。

この点，マイナンバー法が予定するデータマッチングで集積・結合される個人情報の中には，性質上かなりセンシティブな情報も含まれうる。また，一般には秘匿性が高くない情報であっても，個人番号に紐づけて集積・結合されることで，重要な情報へと質の変化を生じることもある。

こうして，多種多様な個人情報が，個人番号を検索キーとして集積・結合されることは，個人のプライバシーにとってきわめて重大な介入となりうる。したがって，個人番号の利用及びそれに基づくデータマッチングは，人格プロフィールへの到達可能性を高めるという点において，プライバシー保障及び自己情報コントロール権に対する強度な介入である。

このことから，個人番号の利用及びデータマッチングの目的は，かかる強度な介入を正当化しうるほどに重要なものであることを要求する。

なお，原判決においては，この点に関する理解がとりわけ欠けている。

（2）以上の観点からマイナンバー法の目的を改めて検討すると，上記①ないし⑥のうち，⑤・⑥がプライバシー保障及び自己情報コントロール権に対する強度な介入を正当化できないことはもちろんのこと，①～③の目的もそれだけでデータマッチングを正当化できるようなものではない。

また，④はデータマッチングを正当化できる重要な目的と言える。しかし，データマッチングが目的に必要な範囲に限定されているかは不明瞭であり，かつこれにより秘匿性の高い情報が構築されうることにも鑑みれば，やはり手段としての相当性を欠くというべきである。

マイナンバー法の目的は，領域特定が十分でなく内容自体が不明確で重要性を持つとは言えないがゆえに，個人のプライバシーに対する強度な介入を正当化できず，違憲である。

（3）原判決はマイナンバー法の立法目的をⅰ行政運営の効率化，ⅱより公正な給付と負担の確保，ⅲ国民の負担の軽減・利便性向上に求めた上で，これらを「いずれも正当なもの」と簡単に認定している。

しかし，個人番号の利用及びそれに基づくデータマッチングは，プライバシー保障及び自己情報コントロール権に対する強度な介入であるから，その目的が重要なものであることを要求することは，既述の通りである。

この観点からマイナンバー法の目的を改めて検討すると，上記ⅲがプライバシー保障及び自己情報コントロール権に対する強度な介入を正当化できないの

はもちろんのこと，ｉの目的もそれだけで人格プロフィールへの到達可能性の高いデータマッチングを正当化できるようなものではない。かろうじてⅱだけは重要な目的といえるが，この目的に真に必要な範囲にデータマッチングが限定されているかが不明瞭であり，かつデータマッチングにより秘匿性の高い情報が構築されうるという点にも鑑みれば，やはり目的と手段との間の均衡を失しており，合理性を欠く。

7　個人番号の濫用・漏洩の危険性

（1）マイナンバー法上の制度設計では，各分野で保有される個人情報の管理については分散管理方式が採用されており，個人情報が個人番号によって常に集積・結合されている状態にあるわけではない。

しかし，そうだとしても，個人番号がいつでもこれらの個人情報を集積・結合できる情報であることは否定できない。このことからすれば，センシティブ情報に匹敵する重要情報である個人番号については，濫用の危険性やサイバー攻撃その他の手段による漏洩の危険性に対する予防措置が十分に定められている必要がある。

（2）この点，マイナンバー法の法文上は，こうした濫用・漏洩に対する予防措置がそれなりにとられている（２０条，３３条以下等)。

しかし，それでもなお十分な措置が定められているとは言い難い。

たとえば，「刑事事件の捜査」のための情報提供（１９条１４号）は，提供される個人情報の範囲が限定できず，包括的な人格プロフィールが開示される可能性が否定できないため，個人番号を濫用するものであり，必要性・合理性を満たさず違憲である。

（3）また，漏洩の危険性についても予防措置が実効的であるかは問題である。

情報提供ネットワークシステムに関わる個人番号利用事務には，官民含め多くの実施者が関わっている。それぞれの事務実施者のレベルで十分な漏洩防止策が講じられていなければ，いくら情報提供ネットワークシステムを強固なものとしようとも個人情報の不正な取得・利用は避けられない。

個人番号が漏洩するということは，実害が出たかどうかという問題とは関わりなく，個人番号が他者に知られたというだけでプライバシーに対する危険を否応なく生じるものである。実際，すでに日本年金機構，国税庁，市町村のマイナンバー事務において，データ入力業務等を委託された事業者が委託元の許諾なしに他の事業者に業務を再委託していた事例が報告されている。このことだけでも予防措置の脆弱性がうかがい知れる。

（4）憲法上のプライバシー保護の要請は，個人のプライバシーが他者によって知られてしまうかもしれないという危殆化状況そのものを排除しようとするものであり，こうした考えは「プライバシー・バイ・デザイン」という言葉で世界的に重視されつつある。

データ保護に関する現在の世界水準ともいうべき EU 一般データ保護規則（GDPR）でも，制度設計の段階から個人のデータ保護措置を組み込んでおかなければならないことが規定されている。もはや，ここではプライバシー保護の必要性は当然の前提とされ，これを保護するためには何をすべきかが示されているといってよい。個人番号制度においては，データの必要最小限度性の遵守や匿名化などの措置が明らかに不十分であり，こうした要請に応えられない内容となっている。

（5）また，住基ネット訴訟最高裁判決は「住基ネットにシステム技術上又は法制度上の不備があり，そのために本人確認情報が法令等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な危険が生じているということもできない」として違憲主張を退けているが，このことは個人情報を取り扱うネットワークシステムに「システム技術上又は法制度上の不備」があり，漏洩等の具体的危険がある場合には違憲となりうるとの前提理解を示したものと解されている。これもまた，プライバシーの危殆化状況そのものを権利侵害として構成したものと言える。

したがって，予防措置の実効性も含めて，漏洩の危険性が否定できない状況においては，マイナンバー法がプライバシー侵害的なものであることもまた否定

できない。

第４　結論

以上のように，プライバシー権保障の中核である自己情報コントロール権は，現在の高度情報化社会において特にその重要性を高めている。それゆえ，自己情報コントロール権への介入の適法性・合憲性は，公権力による個人情報の取得から第三者への譲渡に亘る各過程において厳格に審査されなくてはならない。また，データマッチングにより統合された情報が，新たな自己情報コントロール権に対する介入となることも念頭に置く必要がある。しかし，原判決はこれらに関し十分な理解をしていない。

さらに，マイナンバー法に基づく個人番号の生成・指定及びこれを利用したデータマッチングは，個人のプライバシーへの強度な介入を正当化できるような重要な目的を追求するものといえず，違憲の疑いが強い。また，同法１９条１４号・１６号は明確に違憲であると言うべきである。

控訴審においては，個人番号を用いたデータマッチングが従来にはなかった新たな，そしてこれまで以上に強度なプライバシー介入行為であることを前提に，慎重かつ厳格な審査が行われなくてはならない。

以上