平成２７年（ワ）第１６３２号，平成２８年（ワ）第３６４号

マイナンバー(個人番号)利用差止等請求事件

原 告　三戸部尚一　外８名

被 告　国

準　備　書　面（２）

（現代社会における自己情報コントロール権とマイナンバー制度）

２０１６（平成２８）年１２月１日

仙台地方裁判所第１民事部合Ａ係　御中

原告ら訴訟代理人弁護士　野　呂　　圭

同　弁護士　草　場　裕　之

同　弁護士　齋　藤　信　一

同　弁護士　十　河　　弘

同　弁護士　田　村　智　明

同　弁護士　宇　部　雄　介

外

（目次）

第１　現代社会における自己情報コントロール権の重要性

１　はじめに

原告準備書面（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。

２　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。

３　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」などが問題になる所以である）。

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置かれたならば，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置かれたならば，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，人々に萎縮をもたらす。例えば，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，原告準備書面（１）６頁で照会した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，例えば，「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，例えば，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。

４　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できるのは，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，漏れなく，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

共通番号が付いていない場合は，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付いておらず，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は，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。

５　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い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である。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，前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（平成２１）年２月３日付け「第２次情報セキュリティ基本計画」において，情報セキュリティに関して，「事故前提社会」への対応力強化，すなわち，情報漏えい，情報システムのサービス機能低下・停止などの情報セキュリティ上の問題・事故が生じ得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（基本計画２７頁参照)。

情報漏えい（流出）事故を前提とするならば，仮に漏えい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，漏えい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）の思想に則って，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（被告第１準備書面１３頁も，この内容を認めている。）。

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できない。

そして，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，ＰＩＡのプロセスを経なければ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２　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とマイナンバー制度

１　住基ネット訴訟最高裁判決が認めたこと

（１）住基ネット訴訟最高裁判決は次のように判示している。

「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ものであり，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（最高裁昭和４０年（あ）第１１８７号同４４年１２月２４日大法廷判決・刑集２３巻１２号１６２５頁参照)。」

そこで，以下，他の最高裁判決も踏まえて，住基ネット訴訟最高裁判決が，憲法１３条により保護されるとした「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」の内容につき述べる。

（２）最高裁はこれまで次のとおり，憲法１３条は，「個人の私生活上の自由」が国家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旨判示してきた。

ｉ）京都府学連事件判決

住基ネット訴訟最高裁判決が引用している最高裁大法廷昭和４４年１２月２４日判決（京都府学連事件／刑集２３巻１２号１６２５頁）は，警察官がデモ参加者の容貌を写真撮影した行為が問題となった事案である。

同判決は，「・・・憲法１３条は，『すべて国民は，個人として尊重される。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，立法その他の国勢の上で，最大の尊重を必要とする。』と規定しているのであって，これは，国民の私生活上の自由が，警察権等の

国家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ものということができる。そして，個人の私生活上の自由の一つとして，何人も，その承諾なしに，みだりにその容ぼう，姿態（以下「容ぼう等」という。）を撮影されない自由を有するものというべきである。・・・少なくとも，警察官が，正当な理由もないのに，個人の容ぼう等を撮影することは，憲法１３条の趣旨に反し，許されないものといわなければならない。」と判示し，「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容ぼう・姿態を撮影されない自由」が，憲法１３条により，国家権力の行使に対しても保護されるべきことを認めていた。

ⅱ）指紋押捺事件判決

最高裁はまた，最高裁第三小法廷平成７年１２月１５日判決（指紋押捺事件／刑集４９巻１０号８４２頁）でも，次のように判示している。

すなわち，「憲法１３条は，国民の私生活上の自由が国家権力の行使に対して保護されるべきことを規定していると解されるので，個人の私生活上の自由の一つとして，何人もみだりに指紋の押なつを強制されない自由を有するものというべきであり，国家機関が正当な理由もなく指紋の押なつを強制することは，同条の趣旨に反して許されず・・・」として，「みだりに指紋の押捺を強制されない自由」が憲法１３条により，国家権力の行使に対して保護されることを認めていた。

ⅲ）以上のとおり，最高裁は，憲法１３条が，「個人の私生活上の自由」が国家権力の行使に対して保護されるべきことを規定していることを前提に，「みだりにその容ぼう・姿態を撮影されない自由」や「みだりに指紋の押なつを強制されない自由」が，「個人の私生活上の自由」の一つとして憲法１３条により保護されるべきことを従来から認めていた。

（３）最高裁はまた，以下の判例において，個人に関する情報をみだりに開示・公表されない利益が，法的に保護される旨判示してきた。

ⅰ）前科照会事件判決

最高裁第三小法廷昭和５６年４月１４日判決（中京区役所前科照会事件／民集３５巻３号６２０頁）は，中京区長が弁護士法２３条の２に基づく照会に対して，前科等を回答したことが問題とされた事案であるが，次の

とおり判示している。

「前科及び犯罪経歴（以下「前科等」という。）は人の名誉，信用に直接かかわる事項であり，前科等のある者もこれをみだりに公開されないという法律上の保護に値する利益を有するのであって，市区町村長が，本来選挙し各の調査のために作成保管する犯罪人名簿に記載されている前科等をみだりに漏えいしてはならないことはいうまでもないところである。」

すなわち,「前科等をみだりに公開されない利益」が法律上保護に値することを認めている。

ⅱ）ノンフィクション「逆転」事件判決

最高裁第三小法廷平成６年２月８日判決（ノンフィクション「逆転」事件／民集４８巻２号１４９頁）でも,「ある者が刑事事件につき被疑者とされ，さらには被告人として公訴を提起されて判決を受け，とりわけ有罪判決を受け，服役したという事実は，その者の名誉あるいは信用に直接にかかわる事項であるから，その者は，みだりに右の前科等にかかわる事実を公表されないことにつき，法的保護に値する利益を有するものというべきである。この理は，右の前科等にかかわる事実の公表が公的機関によるものであっても，私人又は私的団体によるものであっても変わるものではない。」と判示されており，みだりに前科等を公表されない法的利益があることを認めている。

ⅲ）早稲田大学名簿事件判決

さらに，最高裁第二小法廷廷平成１５年９月１２日判決（早稲田大学名簿事件／民集５７巻８号９７３頁）は，次のように判示している。

「本件個人情報は，Ｄ大学が重要な外国国賓講演会への出席希望者をあらかじめ把握するため,学生に提供を求めたものであるところ,学籍番号,氏名，住所及び電話番号は，Ｄ大学が個人識別等を行うための単純な情報であって，その限りにおいては，秘匿されるべき必要性が必ずしも高いものではない。また，本件講演会に参加を申し込んだ学生であることも同断である。しかし，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開示されたくないと考えることは自然なことであり，そのことへの期待は保護されるべきものであるから，本件個人情報は，プ

ライバシーに係る情報として法的保護の対象となるというべきである」

すなわち，前科等のように秘匿性の高い情報だけでなく，必ずしも秘匿性の高くない個人情報であっても，みだりに他者に開示されないという利益が法的保護に値する旨判示しているのである。

ⅳ）法廷イラスト事件

最高裁第一小法廷平成１７年１１月１０日判決（民集５９巻９号２４２８頁）は，「人は，みだりに自己の容ぼう等を撮影されないということについて法律上保護されるべき人格的利益を有する。」とした上，さらに「また，人は，自己の容ぼう等を撮影された写真をみだりに公表されない人格的利益も有すると解するのが相当」と，「人は，自己の容ぼう等を描写したイラスト画についても，これをみだりに公表されない人格的利益を有すると解するのが相当である」などとした。

ⅴ）以上のように最高裁は，容ぼう・姿態については，みだりに撮影されない利益だけでなく，みだりに公表されない利益も法的保護に値するとし，また，前科前歴等のように秘匿性の高い情報だけでなく，氏名等のような，必ずしも秘匿性の高くない情報であっても，みだりに開示・公表されない利益が法的保護に値することを認めてきたのである。

（４）「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」の内容

ア　以上のような最高裁判決を踏まえると，住基ネット訴訟最高裁判決は，「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」が法的保護に値する利益であることを前提に，これが憲法１３条に基づくものとして，公権力の行使に対しても保護されるべきことを明言したものというべきである。

イ　そして，上記判示では，「開示又は公表されない自由」とされているものの，最高裁が，個人情報の「開示・公表だけ」を問題にしていると解すべきではない。

なぜなら，住基ネット訴訟最高裁判決が引用する京都府学連事件で問題になったのは，写真撮影行為である。容貌・姿態といった個人情報の「収集」過程が問題となった事案に関するものであった。

指紋押捺事件で問題になったのも，指紋という個人情報の「収集」過程であったし，法廷イラスト事件では，写真撮影行為という「収集」行為と，その「公表」とが同列に問題にされている。

これらの最高裁判決を踏まえると,「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，厳密な意味での「開示・公表」だけを問題にしているとは考えられない。

ウ　さらに，住基ネット訴訟最高裁判決は，上記判示に続けて,「住基ネットが被上告人らの上記の自由を侵害するものであるか否かについて検討する・・・」として，①本人確認情報の秘匿性の程度が高くないこと，②本人確認情報の管理・利用等が法令上の根拠に基づき，正当な行政目的の範囲内で行われること，③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も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旨判示し，さらに，原判決の指摘するデータマッチング等の危険性についても検討を加えている。

漏えいの可能性は，個人情報の「管理」のあり方の問題であり，データマッチング等の目的外利用の危険性は個人情報の「利用」のあり方の問題であって，厳密には「開示・公表」と区別することもできるが，住基ネット訴訟最高裁判決は，これらを含めて,「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」を侵害するか否かの問題として論じているのである。

エ　そうすると，住基ネット訴訟最高裁判決が，憲法１３条により保護されるとする「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，収集，管理・利用，開示・公表といった個人情報の取扱いの全般について,「みだりに」取り扱われないことを，公権力との関係でも保障している，と解されることになる。

（５）「みだりに」の判断基準

住基ネット最高裁判決は，どのような場合に「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」が侵害されたことになるのか，一般的な基準を提示してはいない。

この点，憲法１３条は，前段で「個人の尊厳」原理を定め，これを受けて後段で，人格的自律の存在として自己を主張し，そのような存在であり続ける上で重要な権利・自由を包括的に保障する権利（幸福追求権）を定めたものと解されている（佐藤浩治「日本国憲法論」１７５頁）ことを踏まえると，「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という以上は，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」が侵害されることになると言える。

（６）差止も認められるべきである

「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条により保護されているという以上，かかる自由を侵害する態様で個人情報が現に取り扱われ，又は取り扱われる具体的な危険性がある場合には，事後的な救済だけでなく，事前の差止が認められるべきことは当然である。

最高裁第三小法廷平成１４年９月２４日判決（「石に泳ぐ魚」事件／判時１８０２号６０頁）は，「公共の利益にかかわらない被上告人のプライバシーにわたる事項を表現内容に含む本件小説の公表により公的立場にない被上告人の名誉，プライバシー，名誉感情が侵害されたものであって，本件小説の出版等により被上告人に重大で回復困難な損害を被らせるおそれがあるというべきである」と判示して，本件小説の出版等の差止請求を認めた原判決を維持しているところである。

２　マイナンバー制度による「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」の侵害

（１）被告も釈明で認めた現代におけるマイナンバー制度の危険性

被告は「求釈明に対する回答書」（平成２８年９月３０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以下の点を認めた。

（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。

これらは，原告らが指摘してきたマイナンバー制度（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できる。

（２）「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」の侵害性

もっとも，被告の主張（第２準備書面，求釈明に対する回答書）では，番号制度においては，制度上の保護措置及びシステム上の保護措置を講じているから，これらの危険性は具体的な危険性ではない，とされている。

しかし，仮に，被告の主張する保護措置が不十分であって，上記した危険性が具体的な危険性と評価できるとすれば，それはまさに，「個人の尊厳ないし人格的自立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」として，「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」が侵害されている状態というべきである。

（３）保護措置の不十分さ

保護措置が不十分であることは改めて詳論する予定であるが，本準備書面では以下の点を指摘する。

ア　システム障害等の事故の多発

原告準備書面（３）で述べるマイナンバー制度に関連する事故例を踏まえると，マイナンバー制度の保護措置は十分であるとは認められない。

例えば，２０１６（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，その障害の根本原因を特定し，同年４月１５日及び２２日にそ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【甲４の４３】。

同年６月２２日にＪ－ＬＩＳが発表した「カード管理システムの中継サーバに生じた障害等について」【甲４の４４】によると，上記障害発生の原因及び原因の特定に長時間を要した要因は以下のとおりであった。

（障害発生の原因・背景）

①不具合を作りこんだ原因（設計不備・過信）

・中継サーバを担当した事業者の事前の適合性評価が不足していたこと（中継サーバの機器構成は，住基ネットの市町村ＣＳにおいて安定稼働実績（過信）があったことから，バージョン・設定相違等があったにもかかわらず，事前の適合性評価（相性問題の事前検証）が不足していた。）。

・ＯＳ仕様の理解不足から，システムの処理中になんらかの異常が発生した場合の対応（例外処理）について，中継サーバを担当した事業者の検討が不足していたこと。

②事前に検知できなかった原因（適合性評価，単体テスト不足・過信）

・中継サーバを担当した事業者の事前の適合性評価，単体テストが不足していた。

（原因の特定に長時間を要した要因）

・ログを取得するよう改修する必要があったこと。（安定稼働実績のある装置であったことから，検証に必要なログを取得する設定になっていなかった。）

・本番環境と異なる設定で試験した結果，再現環境で不具合が再現せず，原因特定に時間を要したこと。

・中継サーバを担当した事業者が原因究明への主導的な対応を行わなかったこと。（調査全体を取りまとめる立場の５社コンソーシアムの代表事業者と中継サーバを担当した事業者間での連携が不足していた。）

以上の障害事故１つを見ても，カード管理システムの管理態勢が杜撰であったことが認められ，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到底できない。

イ　個人番号漏えいの危険に対する対策の欠如

また，消費税率を１０％に上げた際，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。

ウ　個人情報の一元管理による危険性を除去していない

被告は，抽象的な一般論としてではあるが，マイナンバー制度には「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」を認めている（平成２８年９月３０日付け求釈明に対する回答書３頁)。

ここにいう「一元管理」とは，個人番号をキー（起点）として他の個人情報に繋ぐことによって個人情報を収集・集積することを意味すると解される。

ところで，被告は,「分散管理」について,「各機関がそれぞれ個人情報を保有し，必要に応じて情報提供ネットワークシステムを使用して情報を照会･提供を行う」方法であると説明している(被告第１準備書面４１頁)。つまり，例えば，行政機関Ａは個人番号と紐付けされる情報提供用個人識別符号（番号利用法施行令２０条）を用いて，情報提供ネットワークシステムにより他の行政機関の保有する個人情報を取得できるということである。

そうすると，被告の主張する「分散管理」は，実質的には上記の「一元管理」と異ならないこととなる。なぜなら，いずれも個人番号を起点にして個人情報を収集・集積する点で変わりはないからである。

したがって，被告が保護措置の一つとして主張する「分散管理」（被告第１準備書面４１頁，被告第２準備書面２３頁）は,「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」のある方法であることを被告自身が認めていることになる。そして，被告はこのような「一元管理」による危険性の除去を制度上もシステム上も講じていない。

なお，被告は，システム上の保護措置として，「ア　個人情報の分散管理」，「イ　アクセス制御」，「ウ　符号による紐付け」，「エ　通信の暗号化」を挙げているが（被告第１準備書面４１～４２頁），これらのシステム上の保護措置の法的根拠が不明である（被告は乙第５号証９頁を摘示しているが，これは内閣官房社会保障改革担当室が作成した案内文書に過ぎず，法的根拠ではない。）。

以　上