令和２年（ネ）第１３４９号 マイナンバー（個人番号）利用差止等請求控訴事件

控　訴　人　　関口　博　ほか２６名

被　控　訴　人　　国

準　備　書　面　（1）

２０２１年(令和３年)　７月３０日

東京高等裁判所第１１民事部　御中

控訴人ら代理人　弁護士　水　　永　　誠　　二

同　　瀬　　川　　宏　　貴

同　　出　　口　　か お り

目次

はじめに

被控訴人の答弁書における反論は、控訴人らの控訴理由にかみ合わせようとしていないものである。そして、答えるのが困難な点については答弁を回避しているものである。

繰り返し指摘しているように、個人番号制度は、これからの国の情報システムの根幹をなす、非常に重大なインフラであり、それ故、全国民及び全外国人住民のプライバシー権をはじめとする人権に重大な影響を及ぼすものである。それゆえ、ＰＩＡ（Privacy Impact Assessment・プライバシー影響評価）の制度趣旨、すなわち、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という趣旨に鑑みるならば、その制度の創設前にその「影響評価」は行わなければならなかったものである。そうすることによって、①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」を両立させることが可能となるし、また、②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のである（訴状 15 頁、原審準備書面（1）の 18 頁、同（2）の 8～12 頁。なお、この趣旨、目的等については当事者間で争いがない。）。

しかるに、本来の意味におけるＰＩＡが行われていない現状に鑑みるならば、比較的制度創設初期といえる今の段階において、控訴人らの指摘する諸問題点について、国が真摯な説明責任を果たすことにより、（仮に個人番号制度を進めるとしても）よりプライバシーが保護された制度にすることが可能となる。

被控訴人は、「控訴人ら独自の見解に基づいて原判決を批判する」ものであると言いなすが、プライバシーに関する自由（権利）の内実、その自由（権利）に関する危険性（リスク）のとらえ方、さらにはＰＩＡやＰｂＤ（プライバシー・バイ・デザイン）など、いずれもスタンダードな考え方・とらえ方であり、そのような批判は当たらない。

以上のような観点から、被控訴人は誠実に控訴人らの主張にかみ合った説明責任を果たすべきであるし、司法府は国家理性を発揮して、丁寧な司法審査を行うべき

である。

以下、玉蟲教授の意見書（甲96・以下、本準備書面においては単に「意見書」という。）も踏まえて、ポイントを絞って再反論する。

第１　保障されるべきプライバシー権の内容とその保障の程度・基準について

１　原判決が認めた「自由」と被控訴人の主張する「自由」の相違について

(1)　被控訴人は、「憲法１３条は「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」を保障したものであると解されると主張しつつ、原判決は「従前の最高裁判決に沿うものである」と評価する（８頁）。

(2)　しかし、原判決は、（その理由を述べていない点はあるとして）「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、個人に関する情報をみだりに収集若しくは利用され、又は第三者に開示若しくは公表されない自由を保障するものと解される」と判示しており、平成２０年住基ネット最高裁判決よりも広い範囲での「自由」が保障されていると判断している。

この点は、後述するように、プライバシーに関する情報を含む個人情報の流通過程に即して権利ないし自由を保障しようとするものであると考えられるから、その方向性は正しいものである。

２　自己情報コントロール権を認めた「法令」の存在について

(1)　被控訴人は、「自己情報コントロール権を実体法上の権利として明示的に定めた法令は存在しない。」と主張する。

(2)　しかし、国際的にはＥＵのＧＤＰＲ（一般データ保護規則）をはじめとして、「自己情報コントロール権」（自己情報決定権）はスタンダードな権利となっている。５で後述するように、国は、日本もそれと同等の保障をすることをＥＵに対して宣明してもいる。

そして、国内的にも、少なくとも条例レベルでは、例えば以下のように「自己情報コントロール権」を保障しているものも多い。

ア　神奈川県

「県民の権利（開示、訂正及び利用停止の請求権）

県民等に対し、自己情報をコントロールする権利を保障するため、神奈川県個人情報保護条例（以下「条例」という。）では、自己情報の開示、訂正及び利用停止の請求権について規定しており、その概要は、次のとおりです。」

http://www.pref.kanagawa.jp/docs/h3e/cnt/f162/p753030.htm

イ　東京都

「３　東京都個人情報保護条例の特徴

本条例は、個人情報保護についての国際的なガイドラインといわれる、ＯＥＣＤ（経済協力開発機構 Organization for Economic Cooperation and Development）理事会勧告の８原則（８原則の内容についてはⅢ 資料 19 参照）を踏まえるとともに、プライバシーの権利を自己情報コントロール権（自己の情報の流れを自ら管理する権利）を含むものとして把握する現代のプライバシー理論をも考慮したものである。」

https://www.kojinjoho.metro.tokyo.lg.jp/tebiki/pdf/t00.pdf

ウ　千葉県野田市

野田市個人情報保護条例の解釈及び運用の手引

「（自己情報コントロール権の保障）

第５条の２　実施機関は、個人情報を第９条第１項第５号に掲げる事由により個人情報を取り扱う事務の目的以外の目的のために実施機関以外のものに提供しようとするときは、当該提供の対象となる者（以下この条において「対象者」という。）に対し、あらかじめ、提供の趣旨及び内容、異議がある場合の申出の方法その他対象者の自己情報コントロール権を保障するために必要な事項を野田市報及び野田市のホームページへの掲載の方法により周知しなければならない。

２　実施機関は、前項に規定する申出があったときは、原則として、その者の個人情報の提供をしてはならない。」

https://www.city.noda.chiba.jp/_res/projects/default_project/_page_/001/000/76

1/kaisyakuunyou.pdf

3　自己情報コントロール権の概念（内実）について

(1)　被控訴人は、「自己情報コントロール権を論ずるに当たっては,『自己に関する情報』とは何か,『コントロール』とはどのような行為 かなど，同権利の外延及び内容（誰に対して何を請求できる権利か）を明確にする必要があるところ,これらの点について統一した見解は見られない（増森珠美・最高裁判所判例解説民事篇〔平成２ ０年度〕153 ページ参照）のであって，その概念はいまだ不明確である。

このように，自己情報コントロール権は,その概念自体がいまだ不明確であり，統一的な理解が得られていないものであるから,名誉権などのようなそれのみで排他性を有する人格権とは異なり，差止請求及び削除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。

(2)　しかし、①甲 87（山本達彦教授のシンポジウムレジュメ）にあるように、「自己情報コントロール権」は、「結局、自己情報の開示・非開示、そして開示する場合はその内容について、相手に応じて自分が決定できることにその核心部分があり、それは自己情報のコントロールという定義のなかに吸収できる」ものであるから、その概念が不明確とはいえない。

また、②「名誉権などのようなそれのみで排他性を有する人格権」というが、「名誉権」概念の「それのみで排他性を有する人格権」といわれるその明確性が、プライバシー権とどのくらい質的に異なるのかの点すら、実は不明確であると言わなければならない。

さらに、③国自身が「自分の情報を・・・コントロールできるようにする」ということを「基本原則」として掲げていることを指摘しなければならない。すなわち、令和２年１２月２５日にデジタル・ガバメント閣僚会議で、「デジタル社会の実現に向けた改革の基本方針」が決定されたが、その中において、「Ⅱ　デジタル社会の将来像」の「２　デジタル社会を形成するための基本原則」の２番目で、「公平・倫理」があげられている。そこでは「データのバイアス等による不公平な取扱いを起こさないこと、個人が自分の情報を主体的に

コントロールできるようにすること等により、公平で倫理的なデジタル社会を目指す」と宣言しているのである（甲９８・２頁）。

被控訴人は、この「原則」を踏まえた答弁を行うべきである。

(3)　原判決も被控訴人の答弁書も、「プライバシー権」（プライバシーにかかる「自由」）の内実・外延、少なくとも、現代の高度にネットワーク化された社会が到来している中で、本件に関して、どのような「自由」が認められなければならないのか、その具体的内容と、保障されるべき理由が述べられていない。

①５０年以上前の京都府学連事件最高裁判決や、１０年以上前の住基ネット最高裁判決をあげるだけでは, 何ら本件に即した理由を述べたことにはならない。また、②平成２０年住基ネット最高裁判決が前提とした「住基ネットシステム」と個人番号制度とは、（ｉ）後者が重要な個人情報と結びつけられた「特定個人情報」として保管・利用等されていることや、（ⅱ）データマッチング（システム）を前提とした制度・システムであることなどにより、重要な点で判断の前提が異なることから、両者を同一に考えることができないことは当然である。

原判決（も答弁書）も、これらの「相違」を前提とした理由を述べていないのであって、説得力のある判示とはいえない。

４　意見書を踏まえた原判決の評価について～評価すべき点と誤っている点

(1)「収集若しくは利用」の点にも着目している点は、方向性としては正しい

ア　原判決は、「憲法１３条は・・・個人の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収集若しくは利用され, 又は第三者に開示若しくは公表されない自由を保障するものと解される」と判断した。

イ　上述したように、この点は、情報の流通過程を踏まえた判断であると評価でき、方向性としては正しいものである。

意見書も、（自己情報コントロール権を前提にした記述であるとはいえ）、「公権力による個人情報の取得にはじまり、その保存・蓄積や、一時的ないし恒常的な利用、さらには第三者への譲渡（提供）へと進行しうる情報処理のプロセス全体について」その保護を考えないといけないとしている（３頁）が、

その点を正当に捉えている。

ただし、同判決は、上記情報処理プロセスの「各段階はプライバシー保護との関係でそれぞれ異なった意味合いをもちうるため、段階ごとに分離された理解を必要とするものである」（同）という点について、配慮を払っておらず、その点で不十分である。

(2)　対象となる情報の「多種多様」性等を理由にあげる点の誤り

ア　原判決は、①番号制度の対象となる情報は「多種多様」であることや、②「従前も行政機関等において取り扱われてきた情報」であって、その際に情報主体の同意によるコントロールが必須のものとして取り扱われていたとは認められないことを理由として「コントロール」や「自己決定」の権利の対象として認めるべき情報が何であるかが明確に定まっているとは認めがたいと判断した。

イ　しかし、これらを理由とすることはいずれも誤っている。

まず、②の「従前も行政機関等において取り扱われてきた情報」であるとの点は、特定個人情報としての「利用」という新たな・これまでとは質的に異なる「利用」が問題になっているのであるから、これについて新たに権利（自由）侵害性を検討しなければならないことは当然であり（意見書 17～20 頁）、誤っている。

ウ　次に、①の「多種多様」であるとの点については、現代の高度にネットワークで情報化された社会では、もはや重要でない個人情報など存在しないと言わなければならないから、やはり誤っている。以下詳述する。

（ア）高度な情報処理技術の進展とプライバシー保障

現代社会におけるプライバシーの保障は、高度な情報処理技術の進展との関係で考える必要がある。すなわち、「いったんデジタルデータ化され、ネットワークのなか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、また情報主体の思わぬところで情報同士が結びつけられ，利用される危険性を秘め」るようになってきている。「このような状況が進展すればするほど，個人のプライバシーは大きなダメージを受

け」るようになってきているのである。

このことから、「個人が秘匿したいと考える私的な事項が公にされてしまうこと」だけを想定することでは足りなくなっているのである（意見書３頁）。

（イ）「公開」よりも「収集」・「利用」の危険性を考える必要性

そして、「むしろ、現代社会でのデータ処理の現実を考えるならば、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とりされ、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。いまやプライバシーは公開・暴露されて初めて問題となるものではなく、それが他者によって本人のあずかり知らぬところで収集され、利用されることで問題を生じる」と考えなければならないのである（同）。

（ウ）名寄せのマスターキーとしての「機能的アプローチ」の重要性

個人情報を収集、利用する際に重要なのが名寄せのマスターキーとなる共通番号（個人番号）である。この共通番号の持つ機能について、「機能的アプローチ」をすることが重要である（同８頁以降）。

個人番号が特定個人情報（個人番号ないしそれに代わる番号とひも付いた個人情報）を分野横断的にデータマッチングするための検索キーとなることが本制度の特質であり、この観点からの検討が本訴訟においては欠かせない。

「電子的情報処理技術の進展には、たしかに一方で情報処理の場面での人間の手による可謬性を排除し，処理の効率化・迅速化に貢献し、また処理のコスト削減などを実現したというプラスの側面もある」が、他方、「データ交換の簡便化、データの利用範囲の予測不能な拡大、データの相互関連付けによる質的に新たなデータの創出、あるいは、逆に全体的な関連付けから切り離されたデータの孤立による偏った認識の可能性といった、人格ないしは個人性の侵害の危険性」をもたらすからである（同８頁）。

「質的に新たなデータの創出」の例としては、断片的な買物履歴やネットの閲覧履歴をデータマッチングし、プロファイリングすることによって、本人も自覚していないような本人像が分析されてしまうこと（後述）、反対に、

「偏った認識の可能性」の例としては、例えば、薬物事犯の刑事事件に関わる裁判官や弁護人が、薬物の入手ルートに関する一般的な実情を知ろうとネット検索をしたような場合に、「薬物事件に関わる裁判官・弁護人」という情報と切り離されて、薬物の入手ルートの検索履歴関係の情報だけが名寄せされ、マッチングされた場合に、その人物は「薬物入手に関心があり、薬物の入手を図っている人物」というような誤った人物像が作られてしまう可能性などが想定される。

（エ）もはや重要でない個人情報など存在し得ない

このようなデータマッチングによる「質的に新たなデータの創出」（プロファイリング）の危険性を考えるならば、それ自体では取り立てて重要性のない個人情報であっても、それが他の情報とデータマッチングされ、分析（プロファイリング）されることにより、その個人の包括的な人格像を作り出されてしまうということが最大のリスクであるといわなければならない。

「たしかに、それぞれ独立した個人情報を相互に容易に結びつけることできるということは、電子的情報処理の特徴であるといえるし、また、その利用価値の大きなポイントである。しかし、この作業により、本来はそれほど個人の人格に深く関わらない諸データが集積され、個人の人格をより詳細に、あるいは全体的に把握することのできるデータへと作り替えられることもありうる。現代の電子的情報処理技術の下では、個人に関する情報は技術的にみれば、ほぼ無限定に集積・結合できるのであり、このこと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（住基ネット訴訟における金沢地判平成１７・５・３０はこれを『住民個々人が行政機関の前で丸裸にされるが如き状態』と表現する）。どんな些細なデータであっても、個人の人格把握にとって重要なデータへと作り替えられうるというこの状況からすれば、少なくとも電子的情報処理技術の場面では『重要でない』個人情報などもはや存在しないこととなろう」（同９頁）という指摘は重要である。

すでに民間部門では、例えば、アメリカの小売業者であるターゲット社が、大量の顧客データ（ビッグデータ）を解析して、特定の年齢層に含まれる女

性で無香料性のスキンローション、特定のサプリメント、大きめのバッグなどの商品を同時期に購入した者は、妊娠している可能性が高いという「パターン」を抽出し、自社の顧客データベースに当てはめ、その中から妊娠している顧客を予測し、彼女たちに対してのみベビー用品のクーポン券を配布するなどの活用を行っている（『恐ろしいビッグデータ　超類型化 vsＡＩ社会のリスク』朝日新書　山本達彦著・20 頁、26 頁）。

よって、「少なくとも電子的情報処理技術の場面では、『重要でない』個人情報などもはや存在しない」といわなければならず、原判決のように、収集等されない「自由」の対象を、情報の内容の重要性を基準とするような考え方は、もはやとり続けることができない。「個人識別情報」を対象としなければ、プライバシーは保障され得ない状況に立ち至っているのである。

(3)「みだりに」の解釈についての誤り

ア　原判決の判示

原判決は、「憲法１３条は、・・・個人の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収集若しくは利用され，又は第三者に開示若しくは公表されない自由を保障するものと解される」としながらも、原告（控訴人）らが主張する自己情報コントロール権については、「個人に関する情報を、一律に情報主体の同意によるコントロール及び自己決定を行う権利を憲法１３条が保障しているとは言い難い」と述べて、その憲法上の保障を否定している。すなわち、憲法１３条で保障されるのは「個人情報をみだりに収集等されない自由」だけであり、それを超えて「個人情報について包括的にコントロールする権利」が保障されているわけではないという判示を行っているように考えられる（意見書 5 頁以降）。

イ　憲法の権利保障の原理に反する考え方であること

しかし、このような考え方は、以下のように、明らかに憲法の権利保障の原理に反する（意見書 6～8 頁）

（ア）「みだり」に至らない収集等は公権力の自由であるのか

「憲法上，個人に関する情報を公権力が『みだりに』収集・・・することだけ

が禁止され，『みだり』なものに至らない収集・・・は許容されていると解する場合，そこでは原則として公権力の側に個人情報の自由な処理権限が承認されていることになる。通常であれば，公権力は個人の情報を当該個人の承諾などを必要とせずに，任意で収集したり，利用したりすることができるが，これが行き過ぎて『みだり』な収集などが行われる場合にのみ，これが違憲ないし違法となるというのが裁判所が前提とする図式であろう。この図式は，例えて言うならば，立法府・行政府に一定の裁量が認められる事項について，裁量権の行使が違法となるのは，それが逸脱・濫用にあたるような場合に限られるとされるのに近い。しかし，このような図式の下で個人に認められるのは，公権力が規制を及ぼさない限りで生じる『残余としての自由』に過ぎないことになる。ここで問題となっているのは，個人の自由とは無関係に，あくまで公権力の権力行使が不当なものであるか否かに過ぎないからである。『みだり』なものに至らない限り個人情報の取扱いが公権力の任意に委ねられているとすれば，そこでは個人の原理的な自由は存在しない。」ことになるからである。

（イ）「残余としての自由」は許されない

「このような『残余としての自由』は，伝統的に人権保障が憲法によって行われてこなかったイギリスにおいて，公権力の権力不行使の結果として認められてきたものである。すなわち，個人が原理的に自由であるわけではなく，制定法や判例法によって規制されていない限りにおいて市民の自由が認められるとするのがその特徴である。しかし，このような自由理解は，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日本国憲法上の人権解釈論においては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（『個人として尊重』，『生命，自由及び幸福追求に対する国民の権利については，…国政上最大の尊重を必要とする』），人の固有の情報である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まったく無制限に保障されているというわけではなく，公権力による正当な目的から生じる必要かつ合理的な制約には服しうる。しかし，

だからといって，『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するなどしてよいというわけではない。そうでなければ，これまでの最高裁判例などが，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。」

（ウ）個人に原理的な自由が保障されなければならない

よって、「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。介入として正当な目的をもたず，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，そのような介入が『みだり』なものとなるのである。『個人に関する情報をみだりに収集若しくは利用され、又は第三者に開示若しくは公表されない自由』はそのように解さなければ，憲法上の権利・自由としての意味をなさない。

これに対して，原審判決は，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収集若しくは利用され、又は第三者に開示若しく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。」と言わなければならない。

ウ　小括～正当な目的と必要性・合理性を満たす手段であることが必要である

以上より、上述の「よって」以下にあるように、「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」というのが、憲法の人権保障に即した考え方である。そして、この考え方に基づいて、「介入として正当な目的」を持たない場合はそもそも「みだり」な自由への介入となる。また、仮に「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」も、そのような介入は、「みだり」なものと判断されなければならないのである。

５　ＧＤＰＲ（ＥＵ一般データ保護規則）と同等の保障の必要性について

(1)　原判決と被控訴人の主張

この点について、原判決は判断していない。

被控訴人は、答弁書において、欧州委員会への書簡では、「『日本国憲法第１３条及び判例にて，憲法上の権利としてのプライバシー権を認めている。』と記載された後，『この観点から，最高裁判所は,みだりに個人が他人に個人情報を知らせたくないことは自然であり,この期待は保護されるべきであると判断した。』と記載され，脚注において早稲田大学名簿訴訟最高裁判決が引用されている。これらに照らせば，同指摘部分の記載は，同最高裁判決が認めた限度，すなわち，氏名，住所等の個人識別情報をみだりに第三者に『開示』されないことを法的保護の対象とするという限度でプライバシーにかかる権利が憲法上の権利として保障されていることを述べているにすぎず,控訴人らが主張する情報コントロール権が憲法１３条によって保障されていることを認めたものでないことが明らかである」と主張する（答弁書９～１０頁）。

(2)　被控訴人の主張のごまかし

控訴人は、①ＥＵのＧＤＰＲは「自己情報コントロール権」（自己情報決定権）を保障していること、そして、②そうであるならば、日本国がＥＵに対して、それと同等の保障を約束したのであれば、日本国内においてもＥＵと同等の自己情報コントロール権（自己情報決定権）を保障しないといけなくなるという論理関係になるのではないか、という主張を行った。

したがって、被控訴人が「かみ合った」認否反論をするのであれば、まさに上述の①、②の点に関する正面からの認否反論を行うべきである。

さらに、被控訴人は、ＥＵに対して、「情報コントロール権が憲法１３条によって保障されていることを認めたものでないことが明らかである」というのであれば、ＥＵに対して、追加審査に対してその旨明確に回答すべきである。

第２　判断枠組みについて

はじめに

控訴人らは、プライバシー上の危険性、セキュリティ上の危険性について具体的に主張した。しかし、被控訴人は変わらず諸々の制度や仕組みが存することをあげるのみであり、それらにより、どのようにそれらの危険性について防止されており、それゆえ「法制度上またはシステム技術上の不備」がないと評価できるのかについて、かみ合った反論を行わない。原判決の判示も同様である。

被控訴人が、プライバシーやセキュリティ上のリスク評価についての知見を持ち合わせていないとは考えられないので、このような答弁は、自己に都合の悪い点については、あえてかみ合った答弁を行っていないものと考えられる。

しかし、冒頭にも述べたとおり、個人番号制度・システムは、これからの国の情報システムの根幹をなす、非常に重大なインフラであり、そのリスクは全国民・全外国民住民のリスクとなるものであるから、以下、改めて、「リスク評価」の体系に合わせて、被控訴人（及び原判決）のリスク評価の判断が誤っていることについて述べる。

１「個人の人格的生存ないしその尊厳が脅かされるような態様」での危険性を必要とする誤り

(1)　原判決は、「個人の人格的生存ないしその尊厳が脅かされるような態様で開示等が行われた否か、又はその具体的な危険性があるか否かという観点から判断されるべきものと考えられる」と判示する（11 頁）。被控訴人も同様である（11 頁）

(2)　しかし、第１に指摘しなければならない点は、原判決も引用する昭和４５年京都府学連事件判決の「肖像権」侵害の場合も、その当時は、「人格的生存ないしその尊厳が脅かされるような態様」と評価できるような高度の「危険性」と捉えられていたわけではないということである。本人に無断で写真を撮ったとしても、有形力の行使ではないから違法ではないと考えられていた当時の状況のなかで、「何人も、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を有する」と判断したのが当時の最高裁大法廷であった。

つまり、技術の進歩に伴う新たな自由（権利）侵害に対して、それに見合った自由(権利）保障を考えなければならないのであって、そうしなければ、個人の自由（権利）の保障は実質のないものに後退してしまうのである。

本件においては、情報通信技術及び情報処理技術の飛躍的発展という状況の下、データマッチングによるプロファイリングという新たな自由（権利）侵害が問題となっている。この新たな侵害行為に対して、どのような保障が必要となるのかが判断される必要があるのである。

第２に指摘しなければならないのは、原判決は、「具体的な危険性」が必要としており、あたかも「具体的な危険性」と「抽象的な危険性」とを分けられるかのように捉えている点の誤りである（このような「二分論」を採ることは、被控訴人も同様である）。

この点は、「リスク評価」とも絡むので、以下項を改めて述べる。

２　原判決及び被控訴人の、情報関係におけるリスク評価の仕方の誤り

(1)　リスク評価とは

リスク評価とは，リスクアセスメントを構成する３つのプロセスの内の一つとされる。３つのプロセスとは、

リスク特定（リスクの洗い出し）、

リスク分析（リスクの大きさの算定）、そして

リスク評価（リスク分析にて得られたリスクの大きさを基に、対応の必要性や優先性の判断材料を提供する）を指す（甲９９の１）。

ア　リスク特定

個人番号のシステムにおいて、どこに、どのようなリスクが存するかを洗い出すことが第一段階である（甲９９の２）。

（ア）各セクション毎に流通過程に即したリスクの洗い出しの必要があること

市役所を例にとるならば、各セクション（例えば福祉課）において、個人番号とひも付いた個人情報（特定個人情報）の収集ー保存ー利用ー提供の各過程のどこに、どのような不正利用や漏洩等のリスクがあるかを洗い出すことになる。このようなリスク洗い出し作業は、他の市民課や市民税課などの全セクシ

ョンで行われなければならない。

（イ）民－民－官のそれぞれの過程でリスクの洗い出しの必要があること

個人番号（特定個人情報）は、民一民一官で利用され流通するのが通常であるから、個人番号通知を受ける個人（「民」）、その個人から個人番号を含む情報を受け取る事業主や会社（「民」）、さらにそれらの「民」から特定個人情報を受け取る市役所や税務署など（「官」）のそれぞれが（更に言えば、その「官」からさらに特定個人情報を受け取る国の機関等の「官」も）、それぞれの管轄内において、リスクの洗い出しを行う必要があることになる。

（ウ）洗い出すべきリスク

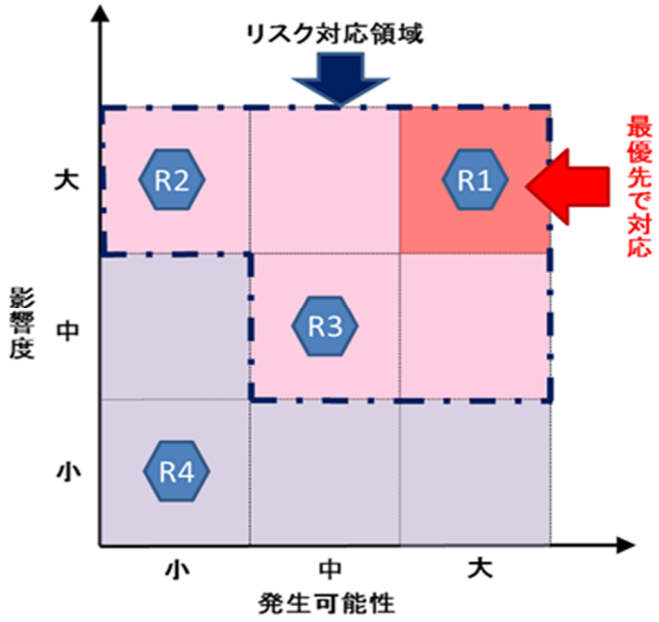
洗い出すべき「リスク」とは、いわゆるセキュリティ上のリスクととして、例えば、外部からの物理的な侵入・盗取のリスク（窓口で集めた個人番号入りの申請書類をまとめた簿冊の盗取など）や、ネットワーク経由の不正アクセス（市のデータベースへの不正アクセスによるデータの盗み出しなど）だけではなく、故意による内部犯行（市の担当者による簿冊の不正持ち出しや、データベースへのアクセスによるデータの不正持ち出し、目的外利用など）や過失による誤送信などの漏洩等も含まれる。

また、プライバシー上のリスクとして、例えば、利用目的からみて過度に広範囲の者に閲覧が許されていたり、過度に広範囲の個人情報に個人番号がひも付けされたりすることなどが挙げられる。

イ　リスク分析

「リスク分析」とは、リスクの特性を理解し、数あるリスクの中から，組織として「本当に対応が必要なものはどれか」、「より優先的に対応すべきものはどれか」を判断する為に、すなわち、リスク対応に優先順位をつけるための判断材料を得るための行為である。そのために、一般的には，リスクがひとたび顕在化した場合の「影響度」（影響の大きさ）と、それが起きる「発生可能性」（発生確率）を掛け合わせて評価される（甲９９の３）。

ウ　リスク評価



例えば、洗い出したセキュリティ上のリスクとして、（Ｒ１）市の特定個人情報のデータベースにアクセスできる市職員が、職務規律に違反してデータを大量に盗み出すリスク、（Ｒ２）市の福祉課窓口で集めた個人番号付き申請書簿冊の盗難のリスク、（Ｒ３）個人番号通知書の誤送付のリスク、等々があり、それぞれの「影響度」及び「発生可能性」の大小が上記表のように分析されたとする（例えば、（Ｒ１）のリスクについて、多数の市職員がデータベースにアクセスでき、アクセスログもとっていないような場合、その「発生可能性」は大であり、その「影響度」も大であると評価されたとする。また、（Ｒ２）の簿冊は課長が管理する鍵付きロッカーに保管されているから、「影響度」は大であるが、「発生可能性」は小と評価されたとする。）。

そうすると、この両者を掛け合わせた数値が一番大きいのは（Ｒ１）のリスクであり、最優先で対応をとる必要があると「リスク評価」されることとなる。

(2)　原判決及び被控訴人の主張の誤り

ア　リスク特定について

以上の観点からするならば、例えば、令和２年６月頃以降、国が積極的に「マイナンバーは漏れても大丈夫」などと宣伝していること（甲９１）は、個人や事

業主等に対して、「マイナンバーの漏洩」をリスクから除外するよう教育しているようなものであり、そもそも根本的に誤っていることは明らかである。

イ　リスク分析について

次に、リスク分析として、①「影響度」の分析として、特定個人情報を一体として評価せず、「個人番号」と「氏名、住所」等の本人確認情報とに分けて、個別に、「個人番号それ自体は・・・それ自体に何らかの個人のプライバシーに属する情報を含むものではない」であるとか、「氏名等の情報は、人が社会生活を営む上で一定の範囲の他者には当然開示されることが予定されている個人情報であって、個人の内面に関わるような秘匿性の高い情報とはいえない」（原判決58頁）と分析する誤りを犯している。また、②「発生可能性」に関しては、民間部門では一般に、漏洩や不正持ち出し等の発生可能性が高いといえるのであり、「影響度」と「発生可能性」を掛け合わせるならば、「官」以上にリスク評価が高い可能性もあるにもかかわらず、原判決も被控訴人も、民間のリスクについて看過している誤りを犯している。これではオーソドックスな分析とはいえない。

以上より、上記（Ｒ３）の個人番号通知書の誤送付のリスクや、違法再委託等について、その具体的な発生原因を分析することなく、簡単に「人的ミス」であって、「法制度上の仕組みまたはシステム技術上の措置に不備があったことにより生じたものとは認めがたい」とすることもまた誤りである。まず、「人的ミス」によるものであっても「リスク」として分析することが必要であるし、その発生の機序を分析して、そこに「不備」がないと評価されることによって、初めてこのような結論を導き出すことができるからである。

上記（Ｒ１）も人的なリスクであるが、罰則や懲戒制度があるというだけでなく、適切なアクセス制限がなされていたか、アクセスのチェック（アクセスログの記録とログ監査体制が十分であったかどうか等）が検討されなければならない。

違法再委託問題についても、単に禁止されているかどうかだけでなく、それを担保するための監視体制が十分かどうか等が検討されなければならない。

さらにプライバシー上のリスクに対しては、法律上、条例上、特定個人情報にアクセスが許されているかだけではなく、それが正当な目的のために、適正な範囲の関係者に限定されているか（「プライバシー保護基準」の策定）、その限定が具体的に履行されているか（「プライバシー保護手順書」の策定とその遵守状況）等の点が検討されなければならない。

これらの点を具体的に検討して初めて「不備がない」と評価されるのである。

ウ　「具体的な危険」について～たとえ僅かな可能性でも具体的危険である

ところで、情報関係のリスク評価においては、たとえ当該形態での「漏洩事故」の発生可能性が極めて僅かしかなくても、「現実的な危険」はある＝「具体的危険」はあると考えなければならない。その上で、上述したように、その発生可能性と、それによる影響度を掛け合わせて、そのリスク分析と評価が行われなければならない。

したがって、この考え方からするならば「具体的危険性」と「抽象的危険性」の二分論は、全く合理性がない。

そして、そのリスクを許容範囲内に収めることを目標として、どのような防止対策をとるのか、その対策の費用対効果はどうかを検討し、費用対効果が合わなければ、そのような情報システムを作ること自体をやめるということも選択肢とする。それが、情報関係のリスク評価である。

（例えば、仮に２０年か３０年にわずか一度の発生可能性しかない「事故」のリスクであっても、それにより国民の個人番号と本人確認情報のすべてが漏洩するというような甚大な損害が発生する場合は、そのリクス評価は極めて高いものであり、優先的に対応する必要があるものとならざるを得ない。なお、プライバシー影響評価は、これらをシステム構築の前に行うという作業であるといってよい。）

そして、「許容範囲内に収める」というのは、いくら対策をとっても、リスクを０にすることはできないということを前提とする（これを「事故前提」の考え方といい、日本のセキュリティ対策の「元締め」である内閣官房セキュリティセンターも、すでに平成２１年にこの考え方に立っている（原審原告ら準備書面

(1)、17 頁）。その意味で、「万全の（事前）対策」などというものは存在しない。

そこで、「事故前提」の対策として必要となるのが、全国民の個人情報が一度に流出しないように「一元管理」せずに「分散管理」するとか、管理する必要のない個人情報（データ）を保管しないようにして（＝データ最小化）保管する個人情報の数を１０個から５個に減らすとか、（減らせない場合は）５個と５個に分散管理するとか等の対策をとって、多種類の個人情報が一度に漏洩しないようにするなどの事前対策をとって、事故発生時のリスクを許容範囲に収められるようにする対策をとるのである。（被控訴人が「分散管理」を強調する意味はここに存するといわなければならない。従って、仮に物理的にサーバーが分散管理されていたとしても、その中のデータがネットワーク経由で一度に全部アクセスできる様な状態であれば、それは「一元管理」と評価すべきものとなる）。

以上述べたように、より、単に抽象的に「このような対策が講じられている」というだけでは、本当のリスク分析はできていないのであって、「具体的な危険」がないとは評価できないのである。

エ　「対策」ができていると主張されているのは「官」の管轄内だけである

ウで述べた点の「あてはめ」について更に述べる。

（ア）被控訴人は、システム技術上の対策について縷々述べる（17 頁以降）。

原判決も、６６頁以下で「個人番号制度に法制度上またはシステム技術上の不備があり、そのために個人に関する情報が法令若しくは条例の根拠に基づかずに又は正当な目的の範囲を逸脱して収集若しくは利用され、又は第三者への開示若しくは公表される具体的な危険が生じていないかどうかについて検討する」として縷々述べている。

（イ）しかし、①特に「（イ）システム技術上の措置について」であげている各措置は、民ー民ー官の特定個人情報の流通の中で、「官」に関する部分の、しかも、「情報提供ネットワークシステム」に関する部分だけであり、その他の部分に関する「措置」については全く検討されていない。また、②「（ア）法制度上の仕組みについて」においては、法律上の義務づけがなされていることが

ほとんどであり、かつ、その義務づけが実効性あるものであるのかについては全く検討されていない。

例えば、ａ）民－民－官の最初の民（個人）段階において、「漏えい」リスクとしては、個人番号カードの提示時における個人番号の「盗み見」等が想定できるが、「盗み見」を禁止するだけではほとんど実効性がない。「事故前提」の対策とすれば、カードの券面から個人番号の記載をなくすことによって、そもそも「盗み見」をされないようにすることや、個人番号を各分野共通の個人識別番号とするのではなく、「分野別番号」にすることによって、仮に「盗み見」され不正利用されたとしても、多くの分野の個人情報が芋づる式に検索等できないようにすることなどが、容易かつ実効的なリスク対策となることは明らかである。しかし、このような対策が講じられていない点において、重大な「不備」が存すると評価されなければならない。

また、ｂ）被控訴人は、「法制度上の対策」として、「人格プロフィールを作成することができないような仕組みが設けられている」とも主張している（19 頁）が、民間においては、「義務を課せば防止できる」という話しではない。しかも、外国でプロファイリングが行われることを防止することは事実上不可能である。安全保障の観点からみれば、一定の外国勢力はこのようなプロファイリング等を意図的に追求しているリスクは当然の前提としなければならないのであって、それこそ抽象的な仕組みがあるだけではリスクは高い＝現実的危険がある、といわなければならない。

オ　「業務一般に抽象的に存在する危険」と評価する誤り

被控訴人は、控訴人らがあげる事故例について、「上記のような事故が発生する恐れがあることは、情報を記した書面等を保管する業務一般に抽象的に存在する危険にすぎない」として、「不備又は欠陥により生じたものではない」と結論している（20 頁）。しかし、これではかみ合った反論になっていない。個人番号が漏れた場合の被害=損害は、一般の漏洩事件とは比べものにならない。しかも、個人番号だけが漏洩するという事故は想定できず、他の社会保障や税関係の重要な個人情報とセットで漏えいすることが多いことを看過して

いる。よって、このような比較は失当である。

カ　「刑事事件の捜査」、「白紙委任」の危険性

「刑事事件の捜査」の解釈運用上のリスクについては項を改めて主張し、また、いわゆる「白紙委任」に関するリスクについては、實原教授の意見書（甲９７）を基に、追って主張する。

キ　デジタル改革関連法成立に伴う危険性の増大

デジタル改革関連法の成立により、今後ますます個人番号の利用範囲は広がってゆき、個人番号カードの利用・提示の場面も増えて行く。そして、それらの利活用の拡大に関しても、ＰＩＡは行われていない。また、不正利用等を監視する機関である個人情報保護委員会は、同関連法によりさらに所管の範囲が広がったが、それに見合った予算や体制の拡充整備はどう考えても十分ではない。これらの点については、追って主張する。

ク　小括

以上述べてきたように、リスク評価の点から見るならば、被控訴人の主張立証は、特に民ー民の管轄内に関して全く足りていないし、それを受けた原判決の判断も穴だらけの状態で全く不十分であると言わなければならない。

被控訴人は、安全対策の重大な欠陥であるという控訴人らの主張に対して、かみ合った理由を示しえておらず、これは被控訴人の主張が失当であることを示しているといわなければならない。

３　番号法１９条１４号の「刑事事件の捜査」における特定個人情報の利用について

(1)　控訴人らの主張（控訴理由書３６頁以下）

番号法は、「刑事事件の捜査」における個人番号（特定個人情報）の利用に関し、提供（１９条）、収集、保管（２０条）を可能とし、特定個人情報ファイルの作成制限（２９条）もなく、個人情報保護委員会の監督も及ばない（３６条）としている。

したがって、警察等の捜査機関は、自己が刑事事件の捜査に必要であると判断

すれば、個人番号を利用して特定個人情報の提供を受け、収集保管し、特定個人情報ファイルを作成し、将来にわたって利用することが可能である。このような収集、保管、利用は捜査の端緒となる嫌疑の程度や犯罪の軽重などに関わりなく行うことが可能であり、それら捜査機関等の判断を第三者が監督する仕組みもない。

すなわち、原審で被控訴人が主張している番号法上の「制度上の保護措置」は、一切、刑事事件捜査利用には及ばず、捜査機関による濫用を防ぐ制度上の担保はない。

控訴人らが違憲であると主張するのは端的にいえばこの点であり、控訴理由書において「番号法は、『刑事事件の捜査』における個人番号の利用に関して、制限なく、フリーハンドで利用することを可能としてしまっている」と述べた（控訴理由書３９頁）のはこの意味である。

(2) 被控訴人の主張（答弁書１６頁）

これに対し、被控訴人は、答弁書において、「捜査機関が刑事事件の捜査のためであれば無限定に特定個人情報を収集できるものではないのは当然であり，捜査機関に対する個人情報の提供が，刑事訴訟法等の法令の定める手続（刑事訴訟法１８９条２項，１９１条１項等）に従って行われることを要するところ，番号利用法１９条１４号の『刑事事件の捜査』は，このような捜査を前提とするのであって，番号利用法上，刑事事件の捜査が行われる場合であればどのような場合でも必ず特定個人情報の提供が認められるものではない。」（１６頁）と主張する。

(3) 上記被控訴人の主張は、控訴人らの主張に対するかみ合った反論となっていない

前記のように、控訴人らは、刑事事件の捜査に特定個人情報を利用するかを判断するのが捜査機関であり、その判断を第三者が監督する仕組みがないことを問題としているが、上記被控訴人の主張はこの点には何ら反論していない。

その上で、上記の「フリーハンドで利用することを可能」という言葉尻をとらえたと思われるが、控訴人らの主張を「捜査機関が刑事事件の捜査のためであれ

ば無限定に特定個人情報を収集できる」（答弁書１６頁）と曲解し、無制限ではなく、刑事訴訟法の規制を受けている、と被控訴人は主張している。

(4)　刑事訴訟法の規定は濫用を防ぐ担保にならない

このように、被控訴人の主張は、刑事事件の捜査に特定個人情報を利用するかを判断するのが捜査機関であることを自認しつつ、刑事訴訟法規制から濫用のおそれはない、というものと解される。

しかし、控訴理由書でも述べたように（４１頁以下）、刑事訴訟法の規定は、捜査機関による濫用を防止する担保になるものではない。このことは被控訴人が上記主張で挙げる次の刑事訴訟法の条項を見ても明らかである。

「刑事訴訟法１８９条２項

司法警察職員は、犯罪あると思料するときは、犯人及び証拠を捜査するものとする。

刑事訴訟法１９１条１項

検察官は、必要と認めるときは、自ら犯罪を捜査することができる。」

要するに、これらの規定は、捜査機関である警察や検察が、犯罪があると考えれば、捜査をすることを定めているに過ぎず、何ら捜査機関による濫用を規制するものではない。

刑事訴訟法にもとづく捜査でも、令状によるものであれば、裁判所の審査が及ぶ。しかし、任意捜査の場合には、裁判所の審査が及ぶとは限らない。例えば刑事訴訟法１９７条２項にもとづき、個人番号を用いて個人の特定個人情報を照会して入手する場合、事前には裁判所の審査は及ばない。捜査の結果、公訴が提起され、しかも当該証拠が提出され、さらにその証拠能力が争われてはじめて、裁判所の審査が及ぶにすぎない。したがって、捜査機関による特定個人情報の利用について、刑事訴訟法の規制が及ぶのは当然であるが、ほとんどの場合、その適否を判断するのは捜査機関自身であり、濫用を防ぐ制度的保障はない。控訴人らが主張するのはこの点である。

(5)「目的」による規制も第三者による監督がなければ実効性がない

また、被控訴人は、番号法９条５項により、「捜査機関は，提供を受けた目的

を達成するために必要な限度で個人番号を利用できるにすぎない」と主張している（答弁書１６頁）。しかし、この点も、「提供を受けた目的を達成するために必要な限度」か否かを判断するのは捜査機関自身であり、第三者機関による監督が及ばない以上、この判断の適性を図る制度的保障はない。

前記のように、番号法２９条は、「個人番号利用事務等を処理するために必要な範囲を超えて特定個人情報ファイルを作成してはならない」と定めるところ、番号法１９条１４号による利用にはこの規定が及ばないとされている（番号法２９条本文）。したがって、捜査機関は、自ら「提供を受けた目的を達成するために必要」と判断すれば、収集した特定個人情報をファイル化し、将来にわたって利用することが可能となる。現に警察が１３０万件ものＤＮＡデータベースを作成して捜査に利用していることは控訴理由書４２頁で述べたとおりである。

(6)　刑事事件の捜査と裁判の執行等を同列に扱うべきではない

また、被控訴人は、番号法３６条が番号法１９条１４号に規定する手続を個人情報保護委員会の監督から除外する理由につき、刑事事件の捜査は、裁判の執行等と同様準司法手続である上、密行性が要求され、一方で刑事訴訟法等において、各種の保護措置や裁判所による救済措置等が講じられていると主張する（答弁書１６頁）。

しかし、濫用の危険性という点からみれば、刑事事件の捜査を裁判の執行等と同様に準司法手続と扱ってよいかそもそも疑問であり、刑事訴訟法による規制が濫用を防止するという点で意味をなさないことは前記のとおりである。また、裁判所による救済措置も前記のように極めて限定された場合にしか講じられない。

また、刑事事件の捜査に密行性が要求されることは一定認められるとしても、それが要求されるのは、通常特定個人を「収集」する一場面にしか過ぎない。一方で番号法は、捜査機関による特定個人情報の「収集」「保管」「利用」につき一切個人情報保護委員会の監督等の保護措置が及ばないとしているのである。密行性はこのような例外を認める合理的な理由とはいえない。

(7)　小括

以上のとおり、番号法上、捜査機関による濫用を防ぐ制度的な担保がないこと

は被控訴人も争いようがない。その上で刑事訴訟法の規制を持ち出す被控訴人の主張は、捜査機関が濫用するはずがないので濫用の危険はないと述べるのと大差ないものである。

控訴理由書４２頁以下で述べたとおり、住基ネット最高裁が判決が本人確認情報の適切な取扱いを監督する第三者機関のあることを合憲の理由としていることに鑑みれば、濫用を防止する制度的担保がないこと自体が制度上重大な不備であり、違憲の理由となるというべきである。

第３　被控訴人に対する「デジタル改革関連法」にかかる追加資料の要求

１　令和３（２０２１）年５月１２日、政府が提出したデジタル改革関連の６法案が、参議院本会議で採決され、自民・公明の与党のほか日本維新の会などの賛成多数で可決、成立した。

成立したのは次の６法であり、その内容は以下のように報道されている。

①　デジタル社会形成基本法（令和３（２０２１）年９月１日施行）

デジタル社会の形成に関し、基本理念および施策の基本方針、国、地方公共団体および事業者の責務、デジタル庁の設置並びに重点計画の策定について規定（IT基本法は廃止）

②　デジタル庁設置法（令和３（２０２１）年９月１日施行）

デジタル社会の形成に関する司令塔として、国の情報システム、地方共通のデジタル基盤、マイナンバー、データ利活用等の業務を強力に推進するデジタル庁を設置

③　デジタル社会の形成を図るための関係法律の整備に関する法律（令和３（２０２１）年９月１日より順次施行）

個人情報関係の3法を統合、国家資格に関する事務へのマイナンバーの利用の範囲を拡大、押印・書面手続の見直し、転入地への転出届に関する情報の事前通知

④　公的給付の支給等の迅速かつ確実な実施のための預貯金口座の登録等に関する法律（公布日から２年以内に施行）

緊急時の給付金や児童手当などの公金給付に、登録した口座の利用を可能とする

⑤　預貯金者の意思に基づく個人番号の利用による預貯金口座の管理等に関する法律（公布日から３年以内に施行）

相続時や災害時に、預貯金口座の所在を国民が確認できる仕組を創設

⑥　地方公共団体情報システムの標準化に関する法律（令和３（２０２１）年９月１日施行）

地方公共団体の基幹系情報システムについて、国が基準を策定し、基準に適合したシステムの利用を求める法的枠組みを構築

２　これらの法律の成立・施行により、これまでの主張立証(及び原判決)で前提としていた条文関係自体も大きく変わっており、また、その範囲も広範囲である。しかも、「束ね法案」であったこともあり、非常にその変更点を把握するだけも困難を伴う。

そこで、

(1)　被控訴人において、同関連法成立によって変更された条文関係等を、整理して提出することを求める。

(2)　併せて、同関連法において新設または修正されることになったところの、（これまで本訴訟において問題とされてきた）番号法関係の制度・システムについて、プライバシー影響評価（ＰＩＡ）を行ったのか否か、行ったとすれば、その結果について、明らかにするように求める。

以上