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１５

２０１９（令和元）年７月１１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

第１　はじめに－本書面の目的

被告国も認めるとおり、番号制度において、個人情報が制度目的を越えて漏洩するなどして、原告らのプライバシー権が侵害される具体的危険がある場合には、目的実現の手段として合理性がないことになる。

そのため、以下においては、①「システム上技術上又は法制度上の不備があり、そのために個人番号及び特定個人情報が法令又は条例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危険が生じている」という点、及び②個人番号及び特定個人情報の漏洩を防止するために必要な安全管理措置が講じられているとする被告国の主張に対する反論として委員会の勧告及び命令、立ち入り検査、刑罰などは機能していない、委員会の独立性なども疑問がある、個人のプライバシー等に与える影響を予測・評価し、かかる影響を軽減する

措置を講じるための特定個人情報保護評価も機能していないという点について論証する。

第２　個人情報漏洩の具体的な危険

１　はじめに（番号制度にシステム上の不備があることについて）

番号制度は、仮に不正行為やミスが発生しても、情報漏洩が最小限度にとどまる仕組みが選択されなければならないし、そのように設計されなければならない。

なぜなら、個人番号及びそれとともに管理される情報は、住基ネットの場合と比べても機微性があり格段に秘匿性が高い情報であるうえに、個人番号は原則的に生涯不変の番号であり、流出した時点で被害が甚大であるからである。

ところが、番号制度において、情報漏洩が最小限度にとどまる仕組みが選択されておらず、そのように設計もされていない。

情報漏洩の際のリスクを軽減するためには、番号を分野別にすることが考えられるし（番号を分野別にすれば、漏洩した番号が生涯不変の唯一の番号である個人番号となるリスクを軽減できるし、名寄せのリスクも軽減される）、番号の記載を最小限にとどめる必要もある。また、コアシステムの管理者を第三者機関とすれば、国による不正アクセスを防ぐこともできる。しかし、被告は、そのような制度設計にしていない。

２　コアシステムの問題点

（１）コアシステムの問題点（総務大臣による一元管理の問題点）について、原田証人は、以下のとおり証言している（甲３２の１，７～１１頁、甲３３の１，５～１２、１５～１６頁）。

情報提供ＮＷＣは、総務大臣が設置して一元的に管理しているシステムであるといえる。

番号制度は、符号で連携するもので、マイナンバーは使わないと説明されている。しかし、番号制度は、コアシステムの中のＩＤコードといわれるものを

変換して個人を識別していく仕組みであり、当然、システム全体で、ある特定の個人のものであるということは識別できるようになっていると考えられ、それが出来なければ、例えばマイナポータルで特定個人の情報提供の記録、その人が保有しているマイナンバーがついている個人情報の本人開示とか、そういうことも出来なくなるから、当然、ＩＤコードで本人の識別はできていると考えられる。したがって、システム上、個人の識別は可能であると考えられる。

情報提供ＮＷＣの仕組みは、外部から不正アクセスされた時に本人、いわゆる誰それさんの情報だと言うことはわかりにくいシステムになっていると思われるが、内部（国）からわかりにくいシステムになっているとは言えない。

システムの中で一番大事なのは情報連携が符号を生成して連携を仲介する、コアシステムと言われる部分であるが、オーストリアのシステムは、コアシステムの部分は、不正な名寄せを防止するために、データ保護委員会という第三者委員会が管理することになっている。

一方で、日本の場合にはここは総務大臣が管理することになっており、国が不正に名寄せする余地があるシステムであると考えられる。

現在、情報提供ＮＷＣでは、符号による連携が行われているが、これは政令で決められているので、政令を変えれば、マイナンバーを使って情報連携することも可能になる。

情報提供ＮＷＣが実際どういう設計になって、どういうふうに作られているのかは、全く公開されていない。したがって、国民はシステムの安全性を検証することもできない。

（２）コアシステムには以下の問題点が存すること

ア　番号制度における情報提供ネットワークシステムを介した情報連携について、行政機関相互の情報連携は個人番号を使って行うのでなく、コアシステムによって生成された「符合」を用いて行なわれると説明され（乙１、Ｐ８参照)、このような仕組みを構築することによって「万が一、情報提供ネット

ワークシステムによる情報連携の情報が第三者に傍受された場合であっても、いもづる式に特定個人情報が漏洩することを防止するシステムになっている」としている。

しかし、ここでの根本問題は、コアシステムが、国（総務大臣）の管理下にあるということである（番号法２条１４項、２１条１項)。

コアシステムによって生成された「符号」を用いて情報連携を行うことが、仮に外部からの不正アクセス対策になるとしても、そのシステムが国の管理下におかれているのであるから、国の側からはその気になりさえすればいつでもあらゆる個人情報にアクセスし、名寄せすることが可能となっていることを意味している。つまり、いかに複雑な「符合」を生成したとしても、システム管理者である国は、「符合」がどの個人に対応するのかを常に把握しうるし、そのシステムを用いてすべての個人のあらゆる情報を瞬時に取得できることになる。その結果「様々な個人情報が、本人の意思による取捨選択と無関係に名寄せされ、結合されると、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ことになるため、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。」（税制大綱）との懸念が現実化しているのである。

これは現実に内部の情報流用が起きたかどうかという問題ではない。国がシステム上、すべての個人情報にアクセスし、欲する情報を自由に名寄せできる仕組みとなっていることが「プライバシー上の懸念」）そのものであり、重大な萎縮効果をもたらし「民主主義の危機」を招来するものである。

この点が番号制度における情報提供ネットワークシステムの根元的問題であるといいうる。

イ　内部職員による情報流用は「懸念」でなく現実化している

２０１７年１月に、個人番号（マイナンバー）の業務を担当していた東京都中野区の職員が住民情報システムに接続し、複数の女性の個人情報を繰り返し盗み見ており、そこから得た情報をもとに一人暮らしの若い女性の部屋に侵入していたことで逮捕されていたことが明らかとなり、さらに同人の自宅からは女性約５０人の個人情報が発見され、その情報をもとに性犯罪を繰り返していた疑いもあることが報道された。

こうした事例は、中野区職員のものに限られず、行政職員が個人情報を不正入手した事例が多発している。

報道に現れたものだけでも、２００５年に旧社会保険庁の職員が芸能人らの年金の加入記録を閲覧していたケース、２００８年に長野県松本市の職員がストーカー目的で女性の戸籍謄本を入手したことで逮捕されたケース、２０１２年に千葉県船橋市の職員が住民の個人情報を探偵業者に漏らしたことで逮捕されたケース、２０１５年に東京都大田区の職員が区の端末で知人女性の住所を不正に閲覧して逮捕されたケース、同年に大阪府堺市の職員が有権者６８万人分の情報を持ち出していたことが発覚したケース、２０１６年に岐阜県職員が県庁のサーバーから女性職員の個人情報を入手して逮捕されたケースなどがある。

このような行政職員による多くの不正アクセスの事例は、住基ネット最高裁判決のいうように「罰則や懲戒処分」などでは防ぎようのないことを実証したものであり、改めて震撼とする事態であるといわざるを得ない。

行政職員による不正アクセスは、如何に外部からの侵入防止の方策を強化したとしても防げるものではない。しかも、番号制度における情報提供ネットワークシステムは、前述のとおり、国の側からはすべての個人のあらゆる情報にアクセス、名寄せが可能であり、これによる情報流用の量も質も番号制度以前のものを圧倒的に凌駕している。

これに対する対応策は、行政内部からの自由なアクセスを遮断する制度的

な「担保」を設けるしかない。しかし、前述のとおり、情報提供ネットワークシステムを国（総務大臣）が管理している仕組みには、こうした「担保」は存在していない。

ウ　内部からの情報流用・不正アクセス防止のために制度的担保の具体例（オーストリアのケース）

オーストリアにおいても個人番号と「符号」を用いた情報連携の仕組みが、我が国の番号制度発足前の２００１年から運用されている。

まず、それまで市町村ごとに管理していた住民登録データを連邦内務省が管理する中央住民登録簿（ＣＲＲ）に一元化し、全住民に中央住民登録番号（ＣＲＲ番号）をつける。これが我が国の個人番号（マイナンバー）に相当するものである。しかし、ＣＲＲ番号は後に述べる「ソースＰＩＮ」の生成のみに使用し、各行政分野での利用・保存はしないこと、ＣＲＲ番号は非公開とされていることが、我が国の個人番号とは大きく異なっている。

情報連携のためのシステム管理は、政府から独立したデータ保護委員会が行う。データ保護委員会は連邦大統領の任命による独立機関で、他の行政機関や議会等には所属していない。６名の委員で構成されており、内訳は「州の代表２名」「労働組合の代表１名」「連邦政府の代表１名」「裁判所の代表１名」とされている。

データ保護委員会は、ＣＲＲ番号からソースＰＩＮと呼ばれる個人別の秘匿番号を生成し、それをもとに各行政機関に対応する「ｓｓＰＩＮ」と呼ばれる個人識別符号を生成、発行し、これを用いて行政機関ごとの情報連携を行うことになっている。この「ｓｓＰＩＮ」が我が国の番号制度における機関別符号に相当するものといえよう。そして、このデータ保護委員会の機能が、まさに我が国の番号制度における情報提供ネットワークシステムに相当するものである。

このようにオーストリアにおいても、個人番号とは異なる機関別の符号を

用いて情報連携を行うという点では、我が国番号制度における情報連携の仕組みと共通している。しかし、決定的かつ本質的に異なっているのは、我が国ではコアシステムは直接国（総務大臣）が管理しているのに対し、オーストリアでは国から完全に独立した第三者機関がシステムの管理を行っていることである。

このような仕組みを採用することによって、国からの情報アクセスに制度的な歯止めを掛けており、国民のプラバシー保護を図っているのである。こうしたことが、内部からの情報流用・不正アクセス防止のために制度的担保に他ならない。

我が国の番号制度が、このような内部からの情報流用・不正アクセス防止のための制度的担保を設けることをせず、国（総務大臣）が情報提供ネットワークシステムを直接管理するという制度にしたことは、プライバシー保護の観点からは致命的な欠陥であるといえる。

エ　外部からの不正アクセス・情報漏洩の懸念も依然として存在すること

被告は、個人番号ではなく「符合」を用いて情報連携を行っていると説明し、このような仕組みを構築することによって「万が一、情報提供ネットワークシステムによる情報連携の情報が第三者に傍受された場合であっても、いもづる式に特定個人情報が漏洩することを防止するシステムになっている」としている。

この点、個人番号と「符合」との直接の対応関係は判然としないが、仮に個人番号と「符合」との直接の対応関係がないとしても、コアシステムによる機関別符号の「生成プログラム」が解明されれば、各行政機関で保有されている個人情報の同一性は明らかになるのであって、各行政機関ごとに独自の番号や符号を用いて管理していた時よりもリスクが高まるのは明白である。

ここでの危険性は、結局のところ、すべての行政機関が統一の番号で情報管理をしていることからくる当然の帰結であり、一見複雑な情報連携のシス

テムを構築したようにみえても、統一番号による情報管理という元々の実体が変わらない以上、リスクが軽減されることはない。

さらにつけ加えるならば、個人番号でなく「符合」によって情報連携するということは「技術的事項」とされ、番号法上何らの規定もないことの問題が挙げられる（番号法施行令２０条に定められているだけである)。このことにより、将来的に政令を変更し直接個人番号を用いて情報連携を行うようにしたとしても違法の問題を生じないのであり、個人番号を直接用いた情報連携に進む可能性も否定できないのである。もし、こうなればすべての行政機関の保有する個人情報は、直接個人番号で紐づけられるのであって、一層危険が増すことは明らかである。

3　中間サーバープラットホームの問題点

（1）中間サーバープラットホームについて、原田証人は、以下のとおり証言している（甲３２の１，６～７頁、甲３３の１，１７頁)。

中間サーバーは、情報連携のために新たに設けられたものであり、情報連携の対象になっている住民の最新の個人情報、当該自治体の中で当該住民を識別するための宛名番号、情報連携のために個人を識別するための機関別符号が保管されている。

元々、中間サーバーは自治体ごとに設置して情報連携の際に使用する想定だったが、２０１４年１月頃、国が中間サーバーを全国的に共同化、集約するという方針を示したことにより、中間サーバープラットホームが全国に２か所(東日本と西日本）に設置された。しかし、お互いにバックアップをし合っているので、実質的には全国１箇所に集約されているといえる。

（2）中間サーバープラットホームに以下の問題点が存すること

ア　地方公共団体の情報管理に関しては、番号法の施行後、新たに自治体中間サーバーが創設、整備された。自治体中間サーバーのソフトウェアは、地方公共団体において共通に整備することが必要となるので、国において一括開

発され、ハードウェアについては、クラウドを積極的に活用して共同化を図ることとし、これを自治体中間サーバー・プラットフォームとして全国２箇所に設置された（「東日本センター」と「西日本センター」）。そして、東日本センターと西日本センターは、相互バックアップにより業務継続性を強化するとされた（甲３４）。

この２箇所の自治体中間サーバー・プラットフォームに各自治体の情報管理システムがネットワークを通じてつなげられ、各自治体の管理する個人情報はここで一括して集約整備されることとなる。自治体中間サーバー・プラットフォームのデータベースには、特定個人情報の副本が保存されている。

自治体中間サーバー・プラットフォームのデータベースにおいて管理される個人情報についても、コアシステムによって生成された機関別符号がつけられ、その機関別符号に紐づけられて管理される。各自治体のデータは区分管理しアクセスは制御されていると説明されている（甲３４）。この地方公共団体に関する情報連携システムは、２０１７年（平成２９年）７月１８日に試行運用が開始された。

イ　自治体中間サーバー・プラットホームによる情報管理は「一元管理」そのものである

すでに述べたとおり自治体中間サーバー・プラットフォームは全国２箇所に設置され、これらは相互に連携しバックアップを取り合う関係となっているので、結局のところ、１つの中間サーバーに、全国すべての地方公共団体の保有する個人情報のすべてが集積することとなる。しかも、地方公共団体の保有する個人情報の中には、地方公共団体固有の情報に加え、他の行政機関の保有する個人情報も含まれる。例えば住民税を課税するためには、住民の所得に関する情報が不可欠で、地方公共団体は税務署等からその情報を入手し保有している（社会保障についても同様である）。こうした情報を直接的、間接的に包含した個人情報がネットワークシステムを通じて中間サーバー・

プラットフォームに集積されるのである。このように地方公共団体の保有する全国民の個人情報が事実上１箇所に集積していることは、驚愕すべき事態である。

前述のとおり、統一した個人番号であらゆる個人情報を管理すること自体が問題であるが、地方公共団体の保有する多様な個人情報は実質的に１つの中間サーバーに集積され、各行政機関はこの中間サーバーにアクセスすることによって個人情報を取得するのであるから、この中間サーバーが地方公共団体の保有する個人情報の「共通データベース」そのものに他ならず、ここには「分散管理」という実態はない。被告がいくら否定しようとも、少なくとも地方公共団体の保有する個人情報については、「一元管理」そのものである。

ウ　情報漏洩の影響は極めて甚大である

「全国民の個人情報が事実上１箇所に集積していることは、驚愕すべき事態である」と述べた意味は２つある。

ひとつは自治体中間サーバー・プラットフォームに何らかの不正アクセス、サイバー攻撃等があれば、すべての国民の多様な個人情報が一網打尽に漏洩してしまう恐れがあることである。

このことは、前述のとおり、被告も「特定の機関に個人情報を集約して単一のデータベースを構築する『一元管理』を行うことは、プライバシー上の懸念が大きい」「万が一そのデータベースから情報漏洩等が生じた場合の影響も甚大なものとなる」（被告第１準備書面Ｐ４２）と述べているとおりである。

自治体中間サーバー・プラットフォームに集積された個人情報には、基本４情報がなく、また個人番号と異なる符合によって束ねられていたとしても、そこにある多種多様の情報の内容から個人を識別することは容易である。現代の高度情報化社会においては、個人に関する微細な情報であっても、これ

を基にインターネット等を通じて当該個人の特定に至り得ることは周知の事実であり、上記のような不正な働きかけによって利用者が特定される可能性が抽象的なものにとどまるなどといえないことは明らかである。

自治体中間サーバー・プラットホームに不正アクセスがあった場合の、漏洩する個人情報の規模の大きさ、内容の多様さは計り知れず、その際に個人の被るであろう不利益は想像を絶するものである。

現代の高度に発達したネットワーク社会においては、年金情報の漏洩や企業の顧客情報の漏洩の例を持ち出すまでもなく、情報は漏洩、流出する可能性のあることを前提に管理方法が構築されなければならない。

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においても、２００９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ているのである(「第２次情報セキュリティ基本計画」（同年２月３日付)。

ところが、あらゆる個人情報を実質的に全国１つの中間サーバーに集積してしまう番号法における「情報ネットワークシステム」は、この観点に真っ向から逆行する管理方法であり、個人情報を不当に危険に陥れるものである。

自治体中間サーバーは全国２箇所に設置されて相互にバックアップを取り合う関係にもなっており（被告第４準備書面，５Ｐ)、アクセス制限が破られた場合や物理的な破壊・不正な持ち出し等について、物理的に同一の建物内か別々の建物内かは明らかに被害の程度が異なり、同じでないことは明らかである。

４　重複付番の問題点

（１）重複付番について、原田証人は、以下のとおり証言している（甲３２の１，１１～１２頁、甲３３の１，３～４頁)。

番号制度の目的は、正確に個人を識別する番号をつけることによって、迅速、正確に情報の交換、情報共有を行うことであると法律にも記載されている。

したがって、個人を正確に識別することが一番大事な点であり、例えば二人の人に共通の番号が付されたり、一人の人に別の番号が二つ付されることがあると、正確な識別ができなくなり、番号制度の根幹が崩れることになる。

ところが、２０１６年頃、住民票コードが重複付番されていたために、長野県と香川県で別の二人の男性に同じマイナンバーが付されていることが明らかになった。この件は、５年間発覚しなかったものであり、同様の事例が存在する可能性がある。

（２）重複付番号は重大な制度の欠陥であること

正確な付番は、番号制度の是非の議論以前の問題ともいえ、制度の根幹をなすものであって、当然に正確に付番がなされていなければならない。制度的に正確な付番がなされない仕組みは、重大な制度の欠陥であるといえる。

５　違法再委託問題等によって、現実に個人情報の大量漏洩が発生しており、これが制度の欠陥によるものであること

（１）新たに判明した個人番号利用事務等の違法な再委託

ア　神奈川県川崎市

神奈川県川崎市（以下「川崎市」という。）は、市民税と県民税の課税に必要な給与支払報告書の情報をデータ化するための入力業務をシステムズデザイン株式会社（以下「システムズデザイン社」という。）に２０１７年１２月１８日から２０１８年３月３１日までの間、約３９万件分委託していた。

しかし、システムズデザイン社は、川崎市に無断で別の業者に同業務のうちデータの入力作業及び納品物となる記録媒体の適正性の確認業務を再委託しており、上記約３９万件分の給与支払報告書のうち、約３５万件分については、個人番号等が記載されていた（甲３５）。

川崎市の特定個人情報保護評価書においては、市民税・県民税データ入力業務の普通徴収、特別徴収、国税連携いずれについても再委託しないことが明記されている（甲３６）。

なお、システムズデザイン社は、２０１８年３月に川崎市が行った聞き取り調査に対し、再委託を実施していない旨を報告していた。

イ　東京都墨田区

東京都墨田区（以下「墨田区」という。）は、平成２８年度及び平成２９年度課税分について、紙で受領した給与支払報告書等の課税資料のデータ入力業務をシステムズデザイン社に委託していた。

しかし、システムズデザイン社は、墨田区の承認を得ることなく、同業務を再委託していた（甲３７）。委託した課税資料件数は、平成２８年度課税分１６万４４７９件、平成２９年度課税分１５万７７９２件にものぼり、そのうち特定個人情報に該当するものは平成２９年度課税分中、約９万５０００件である。

墨田区の特定個人情報保護評価書においては、住民税の申告情報のデータ作成業務は再委託しないことが明記されている。また、「墨田区における特定個人情報等の安全管理に関する基本方針」（甲３８）においては、墨田区は、番号法等の法令遵守、再委託先を含む委託先において、番号法に基づき墨田区自らが果たすべき安全管理措置と同等の措置が講じられるよう必要かつ適切な監督を行うこと等が明記されている。

ウ　東京都台東区

東京都台東区（以下「台東区」という。）は、２０１７年１０月１９日から２０１８年３月３１日までの間、特定個人情報を含む給与支払報告書等、平成３０年度課税分の資料約１２万件のデータ入力業務をシステムズデザイン社に委託していた。

しかし、システムズデザイン社は、東京都台東区に無断で同業務を再委託

していた（甲３９）。

台東区の特定個人情報保護評価書においては、特別区民税・都民税の当初課税資料データファイルの作成業務は再委託しないことが明記されている（甲４０）。

エ　東京都豊島区

東京都豊島区（以下「豊島区」という。）は、２０１７年１１月１３日から２０１８年４月１２日までの間、平成２９年度及び平成３０年度特別区民税・都民税データエントリー業務をシステムズデザイン社に委託していた。

しかし、システムズデザイン社は、少なくとも同期間において７万件以上、豊島区の許諾を得ずに同業務を再委託していた（甲４１）。

豊島区の特定個人情報保護評価書においては、個人住民税の課税資料の電子データ化のためのパンチ作業は再委託するとされているものの、再委託の許諾方法は、「委託者から、あらかじめ再委託するものの名称、再委託の内容、再委託先において個人情報を取り扱う責任者及び担当者の氏名等の通知を受けて、再委託先に関する審査を行い、承認することにより再委託を行うことができる」とされている。

オ　東京都江戸川区

東京都江戸川区（以下「江戸川区」という。）は、２０１６年１２月２８日から２０１７年４月３０日までの間、平成２９年度当初賦課決定にあたり、給与支払報告書、特別区民税・都民税申告書等の課税資料の確認作業やスキャニング、データパンチ処理業務を株式会社プリマジェストに委託していた。そして、株式会社プリマジェストは、その課税資料のデータパンチ業務をシステムズデザイン社に再委託したところ、システムズデザイン社は、同業務を江戸川区の許諾を得ずに再々委託していた（甲４２）。しかも、その件数は約３２万件を超えるものであった。

江戸川区の特定個人情報の取扱いに関する管理規程（甲４３）においては、

江戸川区は、個人番号利用事務等の全部又は一部の委託をする際には、「委託を受けた者」において、区が果たすべき安全管理措置と同等の措置が講じられるよう必要かつ適切な監督を行うこと（甲４３，２１条３項）、個人番号利用事務等の全部又は一部の「委託を受けた者」が再委託（更に再委託する場合も含む。以下同じ。）をする際には、委託をする個人番号利用事務等において取り扱う特定個人情報の適切な安全管理が図られることを確認した上で再委託の諾否を判断する（甲４３，２１条５項）こと等が記載されている。

カ　埼玉県本庄市

埼玉県本庄市（以下「本庄市」という。）は、特定個人情報を取り扱う業務で、原票からのデータ入力を行う「データ入力業務」（平成２８年度・平成２９年度分）をＡＧＳ株式会社（以下「ＡＧＳ社」という。）に委託していた。しかし、ＡＧＳ社は、番号法１０条１項に違反して、委託元である本庄市の許諾を得ないで一部業務を外部事業者に再委託及び再々委託していた（甲４４）。

キ　埼玉県東松山市

埼玉県東松山市（以下「東松山市」という。）は、上記「データ入力業務」（平成２８年度・平成２９年度分）をＡＧＳ社に委託していた。しかし、ＡＧＳ社は、番号法１０条１項に違反して、委託元である東松山市の許諾を得ないで一部業務を外部事業者に再委託及び再々委託していた（甲４４）。

ク　埼玉県羽生市

埼玉県羽生市（以下「羽生市」という。）は、上記「データ入力業務」（平成２８年度・平成２９年度分）をＡＧＳ社に委託していた。しかし、ＡＧＳ社は、番号法１０条１項に違反して、委託元である羽生市の許諾を得ないで一部業務を外部事業者に再委託及び再々委託していた（甲４４）。

ケ　埼玉県深谷市

埼玉県深谷市（以下「深谷市」という。）は、上記「データ入力業務」（平

成２８年度・平成２９年度分）をＡＧＳ社に委託していた。しかし、ＡＧＳ社は、番号法１０条１項に違反して、委託元である深谷市の許諾を得ないで一部業務を外部事業者に再委託及び再々委託していた（甲４４）。

コ　埼玉県和光市

埼玉県和光市（以下「和光市」という。）は、上記「データ入力業務」（平成２８年度・平成２９年度分）をＡＧＳ社に委託していた。しかし、ＡＧＳ社は、番号法１０条１項に違反して、委託元である和光市の許諾を得ないで一部業務を外部事業者に再委託及び再々委託していた（甲４４）。

サ　埼玉県幸手市

埼玉県幸手市（以下「幸手市」という。）は、上記「データ入力業務」（平成２８年度・平成２９年度分）をＡＧＳ社に委託していた。また、幸手市は、特定個人情報を取り扱う業務で、原票の封入封緘を行う「封入封緘業務」（平成２９年度分）をＡＧＳ社に委託していた。しかし、ＡＧＳ社は、番号法１０条１項に違反して、委託元である幸手市の許諾を得ないで、それら業務のうち一部業務を外部事業者に再委託及び再々委託していた（甲４４）。

（２）多くの許諾なき再委託が頻発していること

違法再委託の問題は、日本年金機構（以下「機構」という。）から始まり、上記のように大阪・東京の両国税局や川崎市・さいたま市などの地方自治体からシステムズデザイン社へ委託された住民税のデータ入力業務、埼玉県内の上記市町村からＡＧＳ株式会社へ委託された給与支払報告書や個人住民税のデータ入力業務が、それぞれ委託元の許諾なく再委託されていたことも判明した。

このように頻発する違法再委託の問題について、被告国は、番号法３３条に基づく個人情報保護委員会の指導を行っている、同法３５条に基づく検査を実施している等と主張する（被告第６準備書面７頁）。しかし、その指導については、「責任をもって請け負うという緊張感を持ち、危機管理に関する意識改革を引き続き行う」「特定個人情報等の適正な取扱いに向けた取組を継続的に実施

すること」というごく抽象的で、わずか数行で終わる精神論に終始するものにすぎない。かかる指導が不十分なものであることは明らかであり、指導の名に値しないと断ぜられても致し方ない。

個人番号の適正な取扱いを監視・監督する個人情報保護委員会がそのような不十分な対応しかしていない現状においては、違法再委託の問題が頻発するのも当然の結果である。

（３）流出や不正利用の危険にさらされた特定個人情報

ア　年金機構、恵和ビジネスの問題

従前、原告らが主張したように、機構よりデータ入力を委託されていた株式会社ＳＡＹ企画は、法令、契約、特定個人情報保護評価書に違反して、中華人民共和国の業者へ許諾なくデータ入力を再委託していた（原告ら準備書面１０，２０頁)。そのときに、機構は、氏名とフリガナのみが提供されたと発表していた（甲３３の２、資料１４)。

しかし､実際には､「事務処理が終わってるということもあってログなども残ってないということで、最終的に提供された事業者のところに何が提供されたということは確認はできない」というのが事実である（甲３３の１，２９頁以下、甲３２の１，３０頁)。そうだとすれば、氏名とフリガナのみにとどまらず、年金情報に関する個人情報も流出・不正利用の危険にあったと言わざるを得ない。

また、下記でも述べる不十分な対応しかとられなかった結果、株式会社恵和ビジネスが委託元の機構の許諾なく業務の再委託をした際には、現に１６件、１０名分のマイナンバーのついた特定個人情報が提供されている（甲３３の２、資料１４。甲３２の１，３１頁)。この件では、実際にマイナンバーとその他の個人情報が流出しているのであり、特定個人情報流出の危険性は現実化しているのである。

イ　自治体等における問題

大阪・東京の両国税局や川崎市・さいたま市などの地方自治体からシステムズデザイン社へ委託された住民税のデータ入力業務では、国税局や地方自治体が持つ個人の収入等に関する個人情報がマイナンバーとともに委託されていた。特に、同社は上記地方自治体の立入調査の際に、業務の再委託はしていないとの虚偽の報告をして不正を行っていた。そのため、地方自治体の委託先企業の情報管理能力の審査が適正に行われていたのか疑問を抱かざるを得ない上、後述のように委託元からの委託業務の監督も十分に行われていないと言わざるを得ない。

埼玉県内の上記市町村からＡＧＳ株式会社へ委託された給与支払報告書や個人住民税のデータ入力業務でも同様に個人の収入等に関する個人情報がマイナンバーとともに委託されていた。

これは、本来、委託元の許諾がなければ業務の再委託がなされてはならず、許容されていない再委託先に特定個人情報が渡ってしまったのであり、特定個人情報の漏洩・流出にほかならないのである。

ウ　小括

以上のように立て続けに委託元の許諾なく違法な再委託が頻発しており、少なくとも約２３０万人分の特定個人情報の流出があったといえる。そして、流出した個人情報はマイナンバーに加え、年金という社会保障に関する重要な個人情報や、住民税といった個人の給与に関する機密性の高い情報であって、プライバシー侵害の度合いも大きい。

これらの情報が委託元の許諾なく再委託され、それが委託元の不十分な監督しかなされないままに、自由に取り扱われていたということになるのである。

（４）住基ネットとの違い

住基ネットでは、システムの保守管理を除き、入力業務などを外部に委託することは制度上許容されていなかった。

他方で、番号制度のもとでは制度上、委託元の許諾を得れば、業務の再委託が可能であるから、委託元の監督を前提とする再委託が予定されている。しかし、実際には、多くの委託元の許諾のない違法な再委託が横行し、住基ネットでは発生していなかった特定個人情報の流出が現実化し、不正利用のおそれも発生している（甲３２の１，２９頁)。このような大量漏洩があったにもかかわらず、具体的再発防止策がまったくとられていない。これは、現行の仕組みが違法な再委託を防止する有効な手立てを持っていないという点において、番号制度の本質的な欠陥であるといえる（甲３２の１，３３頁参照)。さらに付け加えるなら、現実に発生した違法な大量漏洩という事態を前にしても、何ら有効な再発防止策を講じられていないのは、今後も同様の事態が発生する現実的危険を有しているといわざるを得ない。

第３　個人情報保護委員会が機能していないこと

従前述べてきたようにマイナンバー法において，プライバシー権の侵害を生じさせないためには個人情報保護委員会が十全に機能しなければならない。住基ネットに関する最高裁判所第一小法廷平成２０年３月６日判決（民集６２巻３号６６５頁）は，「住基法は，都道府県に本人確認情報の保護に関する審議会を，指定情報処理機関に本人確認情報保護委員会を設置することとして，本人確認情報の適切な取扱いを担保するための制度的措置を講じていることなどに照らせば，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。」と判示している。

すなわち，本判決が，住基ネットによって「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」を侵害しているがどうかを判断するに際して重視したのは，住基ネットのシステムの構造であり，その重要な判断要素と

なった一つが，審議会や本人確認情報委員会のような監視機関が設置されていることである。マイナンバー法に引き直してみると，審議会や本人確認情報委員会に相当するものは，個人情報保護委員会である。

しかるに，以下述べるようにマイナンバーの合憲性を基礎づけるべき最も重要な個人情報保護委員会は機能しておらず，さらには特定個人情報保護評価も機能しておらず，マイナンバーは違憲である。以下詳述する。

1　個人情報保護委員会の意義・権限・取り扱う業務

（1）個人情報保護委員会の意義

ア　個人情報保護委員会は，もともと番号法により，２０１４年1月1日に特定個人情報保護委員会として設置された。この際には，いわば番号法の監督機関として開始をしていた（甲４９，２４頁）。

イ　しかし，２０１５年9月の個人情報保護法改正により，個人情報保護法をも所管する機関として，特定個人情報保護委員会が個人情報保護委員会に改組された。これにより，個人情報保護委員会は，特定個人情報保護委員会として担当していた特定個人情報の適正な取り扱いの確保を図る任務に加え，個人情報保護法の全般についての独立した監督機関としての業務等を任務とすることになった。

ウ　これは民間事業者に対する監督であり，従来主務大臣が分野ごとに行っていたものをすべて委員会が一元的に行うことになったのである（甲４９，２４頁）。

エ　以上のように，個人情報保護委員会は，特定個人情報の適正な取り扱いの確保を図る任務に加え，個人情報保護法の全般についての独立した監督機関として広範な業務を取り扱うようになり，かつ個人情報の利活用の促進という役割もあったことから下記で述べるように十分に機能することができていない（甲３２の１，３４頁）。

（2）個人情報保護委員会の権限

また，個人情報保護委員会は，主に以下のような権限を有している（甲４７，５０頁参照）。

ア　番号法に関する権限

（ア）個人情報保護委員会が行使し得る権限として，個人番号利用事務等実施者に対し，必要な指導及び助言をすることができる（番号法３３条）。

（イ）また個人情報保護委員会は，特定個人情報の取扱いに関して法令の規定に違反する行為が行われた場合，当該違反者に対して，勧告及び命令することができる（番号法３４条）。

なお，同命令に違反した者には，２年以下の懲役又は５０万円以下の罰金が科される（番号法５３条）。

（ウ）このほか個人情報保護委員会が行使し得る権限として，特定個人情報を取り扱う者等に対し，必要な報告若しくは資料の提出を求め，または職員に立入検査させることができる（番号法３５条）。

同条の規定による報告若しくは資料の提出をせず，若しくは虚偽の報告をし，若しくは虚偽の資料を提出し，又は当該職員の質問に対して答弁をせず，若しくは虚偽の答弁をし，若しくは検査を拒み，妨げ，若しくは忌避した者には，１年以下の懲役又は５０万円以下の罰金が科される（番号法５４条）。

（エ）さらに，個人情報保護委員会は，措置の要求をすることができる（番号法３７条）ほか，内閣総理大臣に対し，その所掌事務の遂行を通じて得られた特定個人情報の保護に関する施策の改善についての意見を述べることができる（番号法３８条）。

イ　個人情報保護法に関する権限

（ア）個人情報保護委員会は，必要な限度で，個人情報取扱事業者等に対し，個人情報等の取り扱いに対し，必要な報告若しくは資料の提出を求め，又はその職員に立ち入り検査させることができる（個人情報保護法４０

条）。

（イ）また，個人情報保護委員会は，必要な限度で，個人情報取扱事業者等に対し，個人情報等の取扱いに関し，必要な指導及び助言をすることができる（個人情報保護法４１条）。

（ウ）さらに，個人情報保護委員会は，個人情報取扱事業者が，法令の規定に違反した場合において，個人の権利利益を保護するため必要があると認めるときは，当該個人情報取扱事業者に対し，勧告及び命令をすることができる（個人情報保護法４２条）。

（エ）個人情報取扱事業者における個人情報の取り扱い等に関する苦情の申出についての必要なあっせん及びその処理を行う事業者への協力に関する事務を行う（個人情報保護法６１条）。

ウ　さらに，２０１６年５月の行政機関個人情報保護法の改正により，国の機関の行政機関非識別加工情報の運用に当たっての規則制定等の権限が付与されるに至っている（行政機関個人情報保護法第４章の２）。もっとも，それ以外の情報について，行政機関及び独立行政法人については監督等の権限は有していない。

（３）個人情報保護委員会の取り扱う業務

個人情報保護委員会が取り扱う業務内容は，①特定個人情報の監視・監督に関すること，②苦情あっせん等に関すること，③特定個人情報保護評価に関すること，④個人情報の保護に関する基本方針の策定・推進，⑤国際協力，⑥広報・啓発，⑦その他委員会の所掌事務の処理状況を示すための国会報告や必要な調査・研究等，多岐に亘る。さらに，上記以外にも，匿名加工情報の取扱いについて，官民を通じて個人情報保護委員会が一元的に所管することが予定されている（甲５０）。

２　個人情報保護委員会の体制が不十分（甲４９，２３～２４頁）

（１）既に繰り返し主張しているとおりであるが，上記のように個人情報保護委

員会は重要な意義及び権限を有し，その取り扱う業務は多岐にわたるが，その扱い業務の量に比して，体制が不十分であることが明らかとなっている。

（２）まず，個人情報保護委員会の組織は委員長１名，委員８名の合計９名にすぎない（委員長を除き，常勤が４名であとの４名は非常勤である）（甲５０）。

上記非常勤についても，そもそも欠席が多い（甲４９，２３頁～２４頁。甲４５の２，７～８頁）。具体的には，３年間（２０１６年から２０１８年）で３割以上欠席が３名，２０１８年にいたっては，半分以上欠席という人が２名もいるような状況である。

つまり，実情としては，９名よりも少ない体制なのである。

（３）業務量が莫大である例として，取り扱う業務内容の③特定個人情報保護評価書だけをとってみても，２０１６年１年間の特定個人情報保護評価書は１０００件を超えている。

特定個人情報の適正な取り扱いの確保を図る任務の一環である特定個人情報保護評価について，２０１７年１年間の特定個人情報保護評価書についてみると，１月が４３１件，２月が３９３件，３月が７６３件，４月が１２２４件，５月が１４５７件，６月が２３３４件，７月が２７９８件，８月が１１５７件，９月が４３６件，１０月が９１２件，１１月が７１６件，１２月が７２０件，合計１万３８４１件に上る。

加えて，２０１８年１年間では，１月が２４３件，２月が２２８件，３月が３５７件，４月が７５０件，５月が１３３５件，６月が２１６２件，７月が１８９１件，８月が１０７４件，９月が８４８件，１０月が８４３件，１１月が４５２件，１２月が５７５件，合計１万０７５８件に上る。

２０１７年と２０１８年を単純に比較すると，件数が減少しているようにも見えるが，実際には２０１７年において取り合っていた評価書の改定等により，引き続き２０１８年も取り扱うことも多く，件数が年度にわたって積み重なっていることからすれば，業務量は増大しているのである。

（４）人口推計によれば，２０１６年１２月１日現在の日本の総人口（概算値）は１億２６９２万人，２０１７年１２月１日は１億２６７０万人，２０１８年１２月１日は１億２６４３万人であり，これら国民の個人情報は天文学的数字になる。上記のような委員９人の個人情報保護委員会において，全国民の個人情報が適切に取り扱われているかどうかを監視・監督するのが不可能であることは明らかである。

（５）小括

番号法制定時の附則６条３項では，政府は委員会の行う監視又は監督について，「これを実効的に行うために必要な人的体制の整備，財源の確保その他の措置の状況を勘案し，適時にその改善について検討を加え，必要があると認めるときはその結果に基づいて所要の措置を講ずるものとする」とわざわざ規定しており，参議院内閣委員会の附帯決議でも（当時の）特定個人情報保護委員会の事務局機能の充実が要請されている。

さらに，２０１５年９月改正時の番号法及び個人情報保護法は，いずれも附則１２条２項で，「政府はこの法律の施行後3年を目途として，個人情報の保護に関する基本方針の策定及び推進その他の個人情報保護委員会の所掌事務について，これを実効的に行うために必要な人的体制の整備，財源の確保その他の措置の状況を勘案し，その改善について検討を加え，必要があると認めるときはその結果に基づいて所要の措置を講ずるものとする。」と規定している。

このように個人情報保護委員会については，法制定当初から，大きな期待が持たれているとともに十分に機能を果たしうるか不安視されていたところであるが，これまで述べたとおり，人的体制等が極めて十分な状況にあり，このような状況では，個人情報保護委員会の権限を行使して個人情報保護を図るという事も困難である。

３　違法再委託問題においても個人情報保護委員会の機能不全は明らかであるこ

と

（１）個人情報保護委員会に認められた権限

前述のとおり，個人情報保護委員会では，個人番号利用事務等実施者に対する必要な指導，助言，法令違反行為に対する勧告及び命令及び立ち入り検査などの権限を有する。

（２）違法再委託問題で行った委員会の権限行使

ア　年金機構の違法再委託問題で行った権限行使

年金機構の違法な再委託で問題となったＳＡＹ企画に係る事案について被告国は，形式的な指導を行ったのみである。被告国によって実際に行われた指導というのは「責任をもって請け負うという緊張感を持ち，危機管理に関する意識改革を引き続き行う」「特定個人情報等の適正な取扱いに向けた取組を継続的に実施すること」（乙４３の１）というごく抽象的で，わずか数行で終わる簡潔なものが記載された書面を交付したにすぎない。この点について，個人情報保護委員会の権限に詳しい森田証人も「各機関に任せてしまっていて，委員会が主導的に対応しているというふうには受け取れない」（甲４９，３５頁）と明確に証言し，その指導の不十分性を指摘している。

イ　国税庁・地方自治体の違法再委託問題で行われた権限行使

違法再委託の問題に関して，個人情報保護委員会はどのような権限を行使したのか，明らかになっていないどころか，同委員会はなぜか徹底的に秘密裏にしようとしている。

実際に，同委員会は，ホームページ等に違法再委託の問題に対する対応を記載することもなく（甲３２の１，３２頁），重大な法令違反の問題が生じているのに，一般市民は同委員会の対応を知ることができない状態にあった。

そのため，市民団体は，同委員会に対し，違法再委託の問題について，

質問書を提出した。それにもかかわらず，同委員会は個別の案件のため答えることができないという極めて不誠実な対応をしたのである（機構について甲３２の１，３０，３１頁。システムズデザイン社及びＡＧＳ株式会社について甲３２の１，３２頁）。

結局のところ，同委員会がどのような権限行使をしたのか明らかにならない以上，同委員会は，ほとんど権限行使をしていないと言わざるを得ない。

（３）勧告・命令等の権限行使がされていないこと

ア　権限行使の前提を欠くこと

番号法では特定個人情報の重要性に鑑みて，重い刑罰を科することが定められている。

しかし，その前提となる勧告・命令が行われない限り刑罰は適用されることはないのだから，結局は重い刑罰を法令上定めていたとしても何ら役に立たないものとなってしまうのである（原田尋問３４頁参照）。

本件でも，既に詳述したように，大量の特定個人情報が流出・不正利用の具体的危険にさらされているにもかかわらず，個人情報保護委員会による簡単な指導があるのみであり，勧告・命令はなされていない。そのため，重い刑罰を科す前提が欠けているのである。

イ　適切な権限行使がされていないこと

また，委託元の許諾なき違法な再委託について権限行使がほとんどなされていないことは上記のとおりであり，すでに報道で判明しているだけでも上記のように多くの委託元の許諾なき再委託がなされてしまっていて，再発を防げなかったことからすれば，いくら立入検査を実施しようが，指導及び助言を実施しようが全くもって不十分であることは明らかである。

また，違法再委託の問題のように極めて重大な問題が生じながら，個人情報保護委員会は，勧告・命令をしていない。

そもそも委託元の許諾なく業務が再委託されれば，その業務の監督が全くできないことが問題であるのに，十分な調査さえなされていない（甲４９，１２頁参照）のは与えられた権限を放棄しているに等しい。

（４）番号制度の保護措置として意味がないこと

ア　保護措置として期待された役割を全く果たせていないこと

番号法１０条１項では委託元の許諾を得れば再委託をすることができることとなっており，同法１１条による監督を及ぼした上，問題が生じた場合には第３，１で述べた個人情報保護委員会の適切な権限行使を行うことで特定個人情報を保護することが求められている。

しかし，問題が生じた場合に権限行使が全くと言っていいほど行われていないことは第３，２・３で述べたとおりであり，番号制度の保護措置として全く機能していない。また，番号法で再委託を禁止していない，あるいは再委託をする場合でもその方法についての条件を付けていないことは制度的な欠陥である（甲３２の１，３３頁参照）。

イ　権限行使の状況が明らかにならなかったこと

委託元の許諾なく違法な再委託がされ，特定個人情報の流出・不正利用の危険性が生じたとしても，漏洩された本人はそのことを知ることができない。

機構の違法再委託の問題についていえば，前述のとおり，市民団体による質問に対して，機構は説明を全くせず，後に指導を行ったことが分かったという状況であった（甲３２の１，３０～３１頁）。また，システムズデザイン社及びＡＧＳ株式会社による委託元の許諾なき再委託についても，市民団体による質問書に対して個別の案件のため答えることができないとの回答があった（甲３２の１，３２頁）。

（５）小括

したがって，個人情報保護委員会は，組織上，実務上の限界もあって再委

託問題において与えられた権限行使すら行えていない。再委託問題によって個人情報保護委員会が保護措置として意味がないことが明らかになった。

第４　特定個人情報保護評価も機能していないこと

１　特定個人情報保護評価の目的(甲３２の１，１９～２０頁参照)

特定個人情報保護評価は，番号制度に対する懸念（国家による個人情報の一元管理，特定個人情報の不正追跡・突合，財産その他の被害等）を踏まえた制度上の保護措置の一つであり，事前対応による個人のプライバシー等の権利利益の侵害の未然の防止及び国民・住民の信頼の確保を目的とする。

すなわち，特定個人情報保護評価は，個人情報保護委員会の定める指針に基づき実施される（番号法２８条１項）が，これは「個人番号を検索キーとした不正なデータマッチングが行われるおそれがあり，その適正な取扱いを確保する必要性が特に大きいため，我が国の法律では初めて，プライバシー影響評価制度として，」プライバシー侵害を事前に予防するために導入されることになったものである（甲４７，３４頁）。

２　システムの要件定義終了前に保護評価ができなかったこと（甲３２の１，２０～２１頁，甲３３の１，１３頁～）

（１）特定個人情報保護評価は，個人情報保護委員会が決めた「特定個人情報保護評価指針」において，システム構築の「要件定義→基本設計→詳細設計→プログラミング→テスト→システム運用開始」というプロセスのなかで，評価の実施時期をシステムの要件定義の終了までに実施することを原則としていた。

（２）この要件定義終了前までに行うことの重要性につき，会計検査院は，「情報システムが備えるべき機能・性能を具体的に定めて明確化する極めて重要な工程であり，明確な要件定義を行えない場合，計画の遅延や情報システムの機能・性能が要求水準に満たないものとなる事態等が発生するおそれが高

まる」と指摘していた（甲３３の１，１３頁）。

（３）しかし，実際には１３２機関１７１件の特定個人情報保護評価のうち１１６件は要件定義の終了までに実施されていなかった。

（４）そして，個人情報保護委員会は特定個人情報保護評価が，要件定義終了までに実施されていなかったことについて指導や監督等も行っていなかった。

３　個人情報保護委員会が運用の変更を行ったこと（甲３２の１，２１～２２頁）

（１）他方で，個人情報保護委員会は，２０１８年５月２１日に，規則や指針自体を変更して，特定個人情報保護評価の時期を要件定義の終了前からプログラミング開始前に変更した。

（２）個人情報保護委員会は上記の変更を行った理由として，個人情報保護評価はシステムの具体的な運用面を含めたリスク対策の評価を求めており，運用面はシステム設計中においても関係機関との調整が必要になってくる事実があったので，要件定義終了までに実施することが困難になったと説明している。

（３）しかし，会計検査院の報告によれば，個人情報保護委員会が説明するような「要件定義後の工程で評価書の記載項目をより詳細に検討する必要があった。」という理由で実施できなかったのはわずか２．５％しかなく，むしろ大半の理由は特定個人情報保護評価の理解不足が原因であった。

（４）本来は，個人情報保護委員会において，保護評価制度に関する適切な指導を行うべきであったのに十分な指導を行わなかった結果，このような事態が生じていたのである。

（５）以上のとおり，個人情報保護委員会は，十分な指導や監督をしないまま，特定個人情報保護評価の指針の変更を行った結果，要件定義前，つまり情報システムが備えるべき機能・性能を具体的に定めて明確化する前に評価するという意義を没却したのであり，自らの役割を放棄したに等しいのである。

４　特定個人情報保護評価の仕組みの問題点（甲４９，２０～２３頁，甲４５の

１，１８～２１頁）

（１）特定個人情報保護評価書がそもそも難解であること

そもそも特定個人情報保護評価書が極めて難解で読みづらく，作成すること自体が難しく，他の機関のものをそのまま記載したものや誤った記載なども少なくないことは否定できない事実である。

難解で読みづらいことについては，様式を改善し，第三者点検機関（地方公共団体の審議会）の委員が一生懸命に読み込み，審議回数を重ねて慣れることで，ある程度克服できるかもしれないが，作成する側が作成自体に苦労しているようでは，自己評価がきちんとされているか，評価の前提となるリスク対策が本当にされているのか，といった疑問を否定できないのである。

（２）意見募集が形骸化していること

ア　国民の意見を聴取することの意義については「評価実施者や個人情報保護委員会の委員長，委員以外の国民の中にも，情報システムについての優れた知見を有する者が少なくなく，重要な論点や事実が国民の意見聴取手続きを通じて提出されることはありうると思われる。また，何がプライバシーにあたるかは相対的な面があり，一般にプライバシー性が低いと考えられている住所がストーカー被害者にとっては生死にかかわる情報であることもあり，性同一性障害者にとっては性別が機微性のある情報でありうる。したがって，広く国民の意見を聴き，多様な意見を十分に考慮した上で評価書の見直しを行うこととしている。」と説明している（甲４５の１，１９頁）。

イ　しかし，評価書に対する意見募集の手続きについては形骸化しており，ほとんど機能していない。

上記の趣旨からすれば，意見募集は専門家だけを対象とするものではなく，一般の市民も対象とすべきではあるが，当該事務に関する情報の取扱いに格別の関心・利害関係があるような者も想定しているのであるから，

意見募集の趣旨すなわちどのような事務のためにどのような特定個人情報ファイルが設けられるのかについてまずわかりやすい説明がされ，そのうえで評価書を提示する必要がある。

ウ　もともと難解である評価書のみを示して意見を求めても到底実効性のあるものとは思えない。実際に比較的問題点が見えやすい神奈川県の「高等学校等就学支援金の支給に関する事務（公立学校）に係る個人情報保護評価書（重点項目評価）について」及び「同（私立高等学校等）に係る個人情報保護評価書（重点項目評価）について」に関しても，まったく意見は寄せられなかったのである。

エ　加えて，評価実施者としては意見がない方が進めやすいのであり，積極的に意見を掘り起こそうとするインセンティブは乏しいことが，意見募集の形骸化に拍車をかけている。

（3）自己評価の限界及び基礎項目評価に留まっていることの限界

ア　評価書には，「このようなシステムになっていて」，「このようなリスクが考えられるが」，「それはこのようにして防ぐことになっている」という点が記載されている。

イ　もっとも，これは重点項目評価や全項目評価の場合であって，基礎項目評価の場合は，形式的な事項に留まり，リスク評価は記載されない。

ウ　そして，リスクへの対応が書かれている場合でも，それはあくまで自己評価であり，対応は十分されていると常にかかれているが，その真偽は不明である。

エ　無論，自己評価としての評価書作成が正常に機能すれば，評価書作成過程で新たなリスクを発見したり，リスク対策が不備な点を補ったりできるが，実際に機能しているとは言い難い点からしても，実効性には疑問がある。

オ　そして大部分の場合，基礎項目評価にとどまっていることも限界と言わ

ざるを得ない。

（４）個人情報保護審議会が第三者点検をすることの問題点

ア　本来であれば，地方公共団体の特定個人情報保護評価書についても，委員会が直接審査し，承認すべきである。しかし，それは到底不可能のため，地方公共団体に設置される個人情報保護に関する審議会が「個人情報の保護に関する学識経験のある者を含む者で構成される合議制の機関」（特定個人情報保護評価に関する規則7条4項）として，その役割を果たすこととされている。

イ　しかし，地方公共団体の審議会がこうした業務を行うにふさわしいかは甚だ疑問である。審議会は，もともと個人情報保護条例の規定に基づく第三者提供等の例外の是非を審議したり，個人情報保護条例の改正等の制度面の議論をするなどしており，固有の業務が少なくない。また審議会機能だけでなく，審査会機能（不服申立て案件につき諮問を受けて判断を示す）を兼ねているところもある。審議会の中で特定個人情報保護評価に必要なシステムの知識がある人は限られている。このように能力的にも，時間的にも充実した第三者点検をすることは難しい。

ウ　加えて，基礎項目評価のみとなる場合も多く問題である。

つまり，それでも，リスク対策が具体的に記載される全項目評価書や重点項目評価書であれば，議論を重ねることで問題の所在が分かるようになってくることが期待できるが，基礎項目評価では，事務の概要と法令上の根拠，担当部署などの形式的事項としきい値評価程度の記載しかない。

エ　例えば，神奈川県の審議会で第４５回に新たに審議した5件の基礎項目評価書はいずれも４頁（実質２頁と言ってもよい）である。ちなみに第４４回で審議した２つの重点項目評価書はそれぞれ１８頁，１９頁ある。

要するに基礎項目評価書では特定個人情報保護評価の実を上げることは期待できないのである。

オ　そして，全項目評価か重点項目評価か基礎項目評価かは，対象となる人数により形式的に分かれてしまうので，プライバシー保護上重要な論点のある事務についても基礎項目評価で済まされてしまう。あるいは「高等学校等就」学支援金の支給に関する事務に係る個人情報保護評価」のような全国的な事務について，県ごとに取扱いが異なり，しかも大部分は基礎項目評価になっている。

（５）再委託問題における特定個人情報保護評価の機能不全

上述したとおり，特定個人情報保護評価は，番号制度に対する懸念（国家による個人情報の一元管理，特定個人情報の不正追跡・突合，財産その他の被害等）を踏まえた制度上の保護措置の一つであり，事前対応による個人のプライバシー等の権利利益の侵害の未然の防止及び国民・住民の信頼の確保を目的とする。

ア　年金機構・国税庁・地方自治体それぞれの個人情報保護評価書の記載

（ア）保護評価書で禁止されていたこと

違法再委託に関わる年金機構，国税庁，地方自治体は，それぞれ保護評価書のなかで再委託は行わない旨，明確に記していた。

機構についていえば，個人情報流出の事件がかつてあったことを踏まえ，再委託について個人情報保護委員会での審議も行われていたにも関わらず，本件のような違法な再委託が行われていたことになるのである（甲４９，１１頁から１２頁参照）。

プライバシー侵害を事前に予防するために導入された保護評価書に反して，委託元の許諾のない再委託が立て続けに発生してしまっていること自体，保護評価書が機能していないことを示している。

（イ）違反があったとしても措置が取られていないこと

被告国は，再委託があっても特定個人情報が流出しているか断定できないとしているが，個人情報を扱う業務では切り離して峻別するのでは

なく，一体として個人情報保護評価をすることとなっている（甲４９，１２頁・１３頁）。そうだとすれば，断定できないとしても再委託の問題が番号制度・番号法と関わりないことはあり得ないはずである。

しかし，本件では保護評価書への違反があったにも関わらず，業務停止などの具体的措置は取られていない。これでは保護評価書を置いた意味が失われている。

イ　番号制度の保護措置として意味がないこと

個人情報保護評価書はその性質としてあくまで「自己点検，自己評価の仕組み」であり，守られるかは事業主体如何となる上，委託・再委託となると受託した業者は評価手続には直接関わっていないために個人情報保護評価書の存在が意識されづらく，禁止されていても軽視される（甲４９，１７頁・１８頁）。

ところが，個人情報保護評価を定めた当の事業主体が自ら保護評価書に違反し，違反に対しての具体的措置が取られていないことはすでに述べたとおりである。また，番号制度によって，特定個人情報を取り扱う業務が急増したこともあり，業務をこなせないことによる委託・再委託も増加するのであって，そのなかで個人情報保護評価書がより形骸化する状況にある（甲４９，１８頁）。

さらに，番号制度には保護評価書に違反したとしても情報連携をしない等の措置は取られておらず，そのこともあって保護評価書が実効力ある保護措置とはなっていないのである（甲３２の１，３３頁から３４頁）。

以上からすれば，違反の場合の措置もなく，そのこともあって実際上も存在を軽視されるか形骸化しているため，個人情報保護のための保護措置としては全く機能していない。

以　上