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　理　由　書

２０２１（令和３）年４月１５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

【　目　次　】

第１　はじめに……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……５頁

１　原判決の内容……５頁

２　原判決の誤り……６頁

(1)　自己情報コントロール権が保障されるべきこと……６頁

(2)　他の地裁判決では自己情報コントロール権が認められていること……８頁

(3)　情報管理システムに接続されない自由が保障されるべきこと……８頁

第３　判断基準の誤り……１０頁

１　原判決の内容……１０頁

２　厳格な判断基準が求められていること……１０頁

(1)　原判決の誤り……１０頁

(2)　厳格な判断基準が求められること……１１頁

第４　個人情報による人権侵害の危険性に関する誤り……１１頁

１　個人の人権を侵害する危険性を過小評価していること……１１頁

２　個人番号と結びついた特定個人情報の検索・収集等の可能性は，「抽象的な可能

性」（原判決４４頁）ではなく具体的な可能性として想定できること……１２頁
３　「番号制度が取り扱う情報が漏えい又は目的外使用等された場合に，個人の私生活上の自由が侵害される危険性は…（中略）…高くなることがあり得る」（原判決４５頁）との認定は，ＡＩ（人口知能）の発達した現代社会では，妥当ではないこと……１３頁
４　小括……１４頁
第５　番号制度による個人情報の収集等は法令の根拠に基づくものでないこと……１４頁
１　はじめに……１４頁
２　番号利用法１９条１６号が政令及び規則へ白紙委任をしていること……１４頁
３　番号利用法施行令別表７号ないし９号及び１１号等が番号利用法１９条１４号又は同法全体の委任の趣旨を超えるものであること……１６頁
⑴　原判決の判断……１６頁
⑵　番号利用法施行令別表８号について……１６頁
⑶　番号利用法施行令別表７号，同１１号，同２４号について……１８頁
⑷　番号利用法施行令別表９号，同１７号について……１９頁
⑸　小括……２１頁
第６　番号制度は個人情報の利用提供等を正当な目的の範囲内で行う制度となっていないこと……２１頁
１　原判決の判断……２１頁
２　原判決の誤り……２１頁
⑴　行政運営の効率化について……２１頁
⑵　行政分野におけるより公正な給付と負担の確保について……２２頁
⑶　手続の簡素化による国民の負担の軽減，本人確認の簡易な手段その他の利便性の向上について……２３頁
３　結語……２４頁

第７　法制度上又はシステム技術上の不備による情報漏えい，目的外利用される具体的危険性の有無，程度等に関する誤り……２４頁
１　法制度上の不備の有無……２４頁
⑴　原判決の判示……２４頁
⑵　控訴人らの主張……２５頁
２　システム技術上の不備の有無……３０頁
⑴　分散管理の採用……３０頁
⑵　情報提供ネットワークシステムの保護措置……３０頁
３　事故事例の判断について……３３頁
第８　他の地裁判決の存在……３９頁
１　名古屋地方裁判所令和元年１２月２７日判決（事件番号：平成２８年（ワ）第１２９４号，同第２５２３号）……３９頁
⑴　憲法１３条で保障される自由の内容（同判決２８頁）……３９頁
⑵　個人情報の秘匿性の程度（同判決３０頁）……４０頁
２　東京地方裁判所令和２年２月２５日判決（事件番号：平成２７年（ワ）第３４０１０号，平成２８年（ワ）第９４０４号）……４０頁
⑴　憲法１３条で保障される自由の内容（同判決５６頁）……４０頁
⑵　判断基準について（同判決５９～６０頁）……４０頁
３　仙台地方裁判所令和２年６月３０日判決（事件番号：平成２７年（ワ）第１６３２号，平成２８年（ワ）第３６４号）……４１頁
⑴　行政機関等相互の情報連携の問題点（同判決２４頁）……４１頁
⑵　憲法１３条が保障する自由の内容（同判決２４頁）……４２頁
⑶　マイナンバー制度で扱われる個人情報について（同判決２５頁）……４２頁
⑷　個人番号自体の重要性（同判決２５～２６頁）……４２頁
４　大阪地方裁判所令和３年２月２４日判決（事件番号：平成２７年（ワ）第１１９９６号，平成２８年（ワ）第２０２３号，同第２８９５号）……４３頁

⑴　憲法１３条で保障される自由の内容（同判決４４頁）……４３頁
⑵　違憲審査基準について（同判決４５～４６頁）……４４頁
５　裁判例のまとめ……４４頁
第９　さいごに……４６頁

第１　はじめに

原判決は，憲法１３条で保障される人権・自由について，今日に至っても未だ自己情報コントロール権すら認めないという時代錯誤な判断をした。また，マイナンバー制度が個人の人格的自律の前提となる自分像の形成に重大な影響を与えることを無視し，その合憲性の判断基準について，厳格な目的・手段審査を行うことなく，形式的な審査にとどめるという過ちを犯している。

そして，個人情報がもたらす人権侵害の危険性を極めて過小評価したうえ，マイナンバー制度の根拠となる番号利用法が政令及び規則に白紙委任していることや，番号利用法施行令が番号利用法の委任の趣旨を逸脱している点を見過ごすという過ちも犯している。

さらに，マイナンバー制度の目的についても，具体的な立法・制度内容との関連性が認められず（又は極めて弱いものであり），自己情報コントロール権の制限の重大性に見合わない目的となっており，到底正当なものとは言えない点も見落としている。

加えて，法制度上又はシステム技術上の不備による情報漏えい，目的外利用の具体的な危険性があり，実際に漏えいや成りすましなどの事故事例が生じているにも関わらず，これらの事実を無視し，形式的な制度の存在だけをもって問題なしとする過ちも犯している。

なお，マイナンバー制度の違憲性を争う裁判は全国の複数の裁判所に提訴されており，各地方裁判所にて判決が出ている。控訴人らとしては，これら他の地方裁判所の判決内容にも到底承服できないものの，原判決はこれらの判決にも反するものであって，この点からも，原判決は直ちに破棄されなければならない。

以下，詳述する。

第２　憲法１３条で保障される自由に関する判断の過り

１　原判決の内容（同書第３の２(1)，４１～４３頁）

(1)　原判決は，最高裁平成２０年３月６日第一小法廷判決（以下「住基ネット最

判」という。）を引用したうえで，憲法１３条に基づき，「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，行政機関等が個人情報を収集，保有，利用，提供等（以下「個人情報の収集等」ともいう。）する過程においても認められるものと解される。」と判示した。

(2) そのうえで，「個人に関する情報は…多種多様なものがあり，個人の人格的生存との関係での要保護性の程度も一様とはいえない」ことや，「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り，その取扱いの都度当該個人の同意が必須のものとして運用されてきたものでない」ことを指摘したうえで，「現時点においては，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である。」として，控訴人らの主張する自己情報コントロール権が憲法１３条で保障されていないと判示した。

(3) また，情報管理システムに接続されない自由についても，「（自己情報コントロール権に基づく：引用者注）事前の同意権が保障されることを前提とした主張であって，その前提を欠く」うえに，「情報管理システム自体の目的，内容，仕組み，接続によって生ずる利益，弊害等を検討することなく，一律に情報管理システムに接続されない自由を認めることもできない」として，これを否定した。

2 原判決の誤り

(1) 自己情報コントロール権が保障されるべきこと（上記1(1)及び(2)）

ア 原判決は，憲法１３条で保障されるプライバシーに関する自由について，「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」に限定して認めているが，このような理解は，もはや許されない。

すでに原審の原告ら準備書面１や準備書面１１，１２にて述べたとおり，学説及び複数の裁判例などに照らして，自己に関する情報を自分でコントロ

ールする権利としての自己情報コントロール権が憲法１３条によって保障されることは，今日においてはもはや確立した見解といえる。そして，その具体的な内容については，自己の個人情報を「開示又は公表」される場面だけでなく，収集，保有，利用等を含む，情報の流れ全体について，自らコントロールする権利が認められなければならない。

イ　また，原判決は，「現時点においては，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である。」とするが，これも誤っている。

これもすでに原審の原告ら準備書面１１などで主張したところであるが，現代の高度に発達した情報処理技術の前では，それ自体では個人の人格に深く関わらない情報であっても，それらが大量に集積・統合されることで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極めて要保護性の高い情報へとつながりうるのであって，もはや重要ではない情報など存在しない。したがって，原則として，個人に関する情報はその全てが自己情報コントロール権による保障の対象とされなければならない。

ウ　その一方で，控訴人らは，自己情報コントロール権が制約される場面について，原判決がいうような「一律に本人の事前同意」のある場合に限定しているわけではない。

憲法１３条により，自己の情報を収集，保有，利用，管理，開示・公表するといった情報の流れの各場面において自ら決定する権利が保障されるものの，公共の福祉に基づく制約を受けることは否定していない（ただし，自己情報コントロール権が，個人の人格的自律にとって最も根源的な権利であることから，その制約の合憲性は厳格に判断されることになる。）。

したがって，いかなる場合でも本人同意がない限り制約が認められないとの意味で自己情報コントロール権を捉えている点でも，原判決は誤っている。

(2) 他の地裁判決では自己情報コントロール権が認められていること

なお，後述するとおり，マイナンバー制度の合憲性を争う訴訟は全国各地で提起されており，いくつもの地裁判決が出されている。その判決の内容も，原判決のように，個人の情報について「開示又は公表」段階に限って，その自由を認めるものは，少数である。

そして，多くの裁判所は，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にとどまらず，個人に関する情報をみだりに収集，保有，管理又は利用されない自由をも保障していると判示している。

すなわち，現在の裁判実務においても，憲法１３条は個人に関する情報の流れ全体（収集，保有，管理，利用，開示・公表等）を自ら決定し，コントロールする権利を保障していることが認められているのであって，これに反する原判決は誤っている。

(3) 情報管理システムに接続されない自由が保障されるべきこと（上記1(3)）

ア 原判決は，情報管理システムに接続されない自由について，「(自己情報コントロール権に基づく：引用者注) 事前の同意権が保障されることを前提とした主張であって，その前提を欠く」として否定する。しかし，すでに述べたとおり，控訴人らが主張する自己情報コントロール権は，事前の同意権を絶対の前提としているわけではないのであって，原判決の認定は，そもそもの前提が誤っている。

イ さらに，原判決は，「情報管理システム自体の目的，内容，仕組み，接続によって生ずる利益，弊害等を検討することなく，一律に情報管理システムに接続されない自由を認めることもできない」とするが，これは裏を返せば，場合によっては情報管理システムに接続されない自由が認められる余地が存在することを認めているとも読める。

また，それは置くとしても，情報管理システムに接続された場合，個人は自ら直接に個人情報を提供した相手以外の主体にも，当該情報管理システム

を通じて，個人情報が開示・公表されることになる。これは，原判決も認める「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」を侵害する事態を招くことになる。

したがって，原判決の判断に沿ったとしても，少なくとも，「個人に関する情報をみだらに情報管理システムに接続されない自由」が認められなければならない。これに反する判断をしている点でも，原判決は誤っている。

ウ　なお，マイナンバー制度との関係で，「情報管理システムに接続されない自由」が認められなければならない点については，すでに原審の原告ら準備書面１（該当箇所は同書１８～４０頁）にて詳細に論じたとおりである。ここで再度，簡潔に説明するならば，次のとおりである。

（ア）マイナンバー制度には，①個人情報の大量漏えい・改ざんの危険，②チリング・エフェクト（萎縮効果）の危険，③他人による自己情報の集積・統合（自分像の作成）などの危険がある。

（イ）そして，行政各分野で構築されている情報管理システムが共通番号に紐づけされることにより，各分野に分散して管理されていた膨大な個人情報が，即座に，正確かつ網羅的に収集・統合される結果，①大量漏えい・改ざんの危険が増大し，②チリング・エフェクト（萎縮効果）の危険や③他人による自己情報の集積・統合（自分像の作成）の危険なども現実化することになる。

このような広範囲にわたる情報の紐づけが可能となるのは，各個人にデータマッチングのキーとなる万人不同性及び終生不変性を有する共通番号が付番され，マイナンバー制度という膨大な個人情報がほとんど自動的にやり取りされる情報管理システム内に取り込まれているからである。このような情報管理システムに取り込まれてしまうと，もはや個人では自己に関する情報がどの範囲で流通し，自己に関する情報がどこまで結合されて自己の統合された自分像がどのように組み立てられているかを

把握し，コントロールすることは不可能となる。

（ウ）このような個人がマイナンバー制度による危険から逃れるためには，最終的には，共通番号を付番されないようにし，その結果としてマイナンバー制度という情報管理システム自体に取り込まれないようにする以外に方法はない。これができない時には，個人の人格的自律にとって重大な侵害が生じることになるのである。

したがって，マイナンバー制度から個人の人格的自律を守るためには，個人に「情報管理システムに接続されない自由」が認められなければならず，これがマイナンバー制度における自己情報コントロール権の具体的内容なのである。

（エ）これに反し，「情報管理システムに接続されない自由」を否定する原判決は誤っている。

第３　判断基準に関する誤り

１　原判決の内容（原判決４３～４４頁）

原判決は，マイナンバー制度の合憲性を判断する基準として，「①番号制度において取り扱われてい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上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または公表される具体的危険性有無，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らに第三者に開示又は公表す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である。」と判示した。

２　厳格な判断基準が求められること

(1)　原判決の誤り

原判決の定める判断基準は，マイナンバー制度の目的の正当性や重要性に関する検討が不十分である一方，原判決の挙げる上記①ないし③の認定について

は形式的な認定でも許される基準であり，侵害される権利の重大さに照らして緩やかに過ぎることから，誤っている。

(2) 厳格な判断基準が求められること

すでに，原審の原告らの準備書面９などで主張したとおり，マイナンバー制度の合憲性を判断するための基準としては，制約される人権が人格権に基づく重要な権利である自己情報コントロール権及び情報管理システムに接続されない自由であることから，厳格な基準が求められる。

すなわち，マイナンバー制度により制限される自己情報コントロール権や情報管理システムに接続されない自由は，憲法の基本原理である個人の尊重の中核部分である自分像の形成を確保するために極めて重要な権利である。経済的自由の問題ではなく，精神的自由の問題，より正確には精神的自由のさらに前提となる個人の尊重原理に関わる重要な人権である。そして，これが侵害される場合には，個人の自由な言動に重大な萎縮効果をもたらし（このことは，現在の中華人民共和国における監視社会の状況を見れば明らかである。），民主的過程での修正も不可能である。

したがって，これを制約する制度の合憲性を判断するためには，必要不可欠な目的に基づくものか否か（目的審査），またその手段が目的との実質的関連性を有するものであって，侵害の程度が必要最小限度のものであるか否か（手段審査）について，厳格に審査されなければならない。

原判決は，このような必要な合憲性判断を行っていない以上，直ちに破棄されなければならない。

第４　個人情報による人権侵害の危険性に関する誤り

１　個人の人権を侵害する危険性を過小評価していること

原判決は，基本４情報（氏名，性別，生年月日，住所）は秘匿性の高いものではないとし，特定個人情報として個人番号と結びついて保有，管理されている各情報は秘匿性の高い情報であるものの，個人番号の漏洩又は目的外使用等により

これらの情報を検索，収集等される可能性は「抽象的な可能性」に留まるとする。しかも，これらの情報が漏洩又は目的外使用等された場合に，個人の私生活上の自由が侵害される危険性は，従来から各行政機関において収集，保有，管理，利用等していた情報の場合に比して「高くなることがあり得る」とする（原判決４４～４５頁）。

しかし，原判決のこの事実評価は，侵害の危険性の程度を過小に評価しており不当である。とりわけ，個人の人権を侵害する危険性が高ければ高いほど，個人に番号制度からの離脱の自由を認める必要性が高まる点で，侵害の危険性の程度の評価は番号制度の制度設計そのものに直結する問題であり，この点の過小評価は原判決の最も不当な点のひとつである。

２　個人番号と結びついた特定個人情報の検索・収集等の可能性は，「抽象的な可能性」（原判決４４頁）ではなく具体的な可能性として想定できること

原判決は，基本４情報が秘匿性の高い情報ではないこと，個人番号そのものは住民票コードを変換して得られる情報でそれ自体が個人のプライバシーを含むものではないことを指摘する。

しかし，原判決は個人番号の機能を考慮せずに危険性評価をしており，個人情報を含むさまざまな情報がコンピュータ・ネットワークを通じて容易に結びつきうる現代社会の実態を無視したものである。

すなわち，現代の情報ネットワーク社会において，個人番号は，基本４情報のみならず秘匿性の高い特定個人情報をも紐づけるキーとして機能するものであり，キーとなる個人番号から行政機関が取得・保有してはいるものの他の情報との連結がなされずにいる特定個人情報を含むさまざまな個人情報を検索あるいは名寄せすることが，可能となっている。また，このような検索あるいは名寄せが可能とならなければ，国が予定している番号制度はおよそその掲げる目的を達成できない。つまり，番号制度そのものが，キーとなる個人番号をもとにさまざまな個人情報を検索あるいは名寄せすることを制度的に予定しているのである。

特定個人情報を含む個人情報の検索あるいは名寄せが制度的に予定されている以上，個人番号の漏洩又は目的外使用等により特定個人情報を収集・検索等される可能性は，具体的に存在するというべきである。

3　「番号制度が取り扱う情報が漏えい又は目的外使用等された場合に，個人の私生活上の自由が侵害される危険性は・・・（中略）・・・高くなることがあり得る」（原判決４５頁）との認定は，ＡＩ（人工知能）の発達した現代社会では，妥当ではないこと

番号制度が取り扱う情報は，個人の診療記録や税務情報など私生活上の秘匿性の高い情報が多数含まれている。また，番号制度の下では，個人番号をキーとして，私生活上の秘匿性の高い情報を含むさまざまな個人情報の検索あるいは名寄せが容易に行える。

そして，ＡＩ（人工知能）の発達した現代社会では複数の個人情報から当該個人をプロファイリングすることが可能となっている。プロファイリングの意味内容，その可能性及び危険性等については，原審での原告ら第８準備書面で詳述した。

番号制度の下で，プロファイリングが行われることで，個人の私生活上の自由が侵害される危険性としては，以下のものが考えられる。

１つは，プロファイリングにより，本人の同意なく秘匿性の高い個人情報が事実上収集可能となる点である。例えば，いわゆるアウティング（ゲイ，レズビアン，トランスジェンダー等のＬＧＢＴの人について，当人の同意を得ずに公にしていな個人の性的指向や性同一性等を暴露すること）と同様の状態がプロファイリングにより可能となる。

２つ目は，行政機関が保有する個人の情報は，高い正確性を有することが通常であり，そのような情報の検索あるいは名寄せが個人番号をキーとして容易に行えることからすると，思想信条のような個人の内心についてもより高い制度でのプロファイリングが可能性となる。内心の自由は憲法が保障した侵すことのでき

ない絶対的な基本的人権であるにもかかわらず，個人番号により紐づけられた精度の高いさまざまな個人情報にもとづいてプロファイリングすることにより，内心の自由までが侵害されうる。

原判決は，「高くなることがあり得る」と可能性の一つとしか認定していないが，これはＡＩ（人工知能）によるプロファイリングが現実的に多く行われている現代社会の実態を無視した推論であり，「番号制度が取り扱う情報が漏えい又は目的外使用等された場合に，個人の私生活上の自由が侵害される危険性は」確実に高まる。

4　小括

以上より，原判決は，番号制度により個人の私生活上の自由が侵害される危険性を過小評価しているというべきである。

第５　番号制度による個人情報の収集等は法令の根拠に基づくものでないこと

1　はじめに

番号利用法１９条１６号が政令及び規則へ白紙委任をしていること，そして，番号利用法施行令別表７号ないし９号及び１１号等が番号利用法１９条１４号又は同法全体の委任の趣旨を超えるものであることから，番号制度による個人情報の収集等は法令の根拠に基づくものとはいえない。以下，詳述する。

2　番号利用法１９条１６号が政令及び規則へ白紙委任をしていること

(1)　原判決は，同条１６号が，同条１号ないし１５号に「準ずるものとして」個人情報保護委員会規則に定める場合に特定個人情報の提供を認めるものであるところ，①同条１号ないし１５号は特定個人情報の提供が認められる場合を個別具体的に規定していること，②特定個人情報の提供が認められる具体的な場合について，あらかじめ全てを予想して規定することは困難であり，政府から独立した個人情報保護員会に対し規則で定めることを委任する合理的必要性もあることから，同条１６号が政令及び規則への白紙委任を認めるものではないと判断した。

⑵　しかし，法１９条１６号による委任の範囲は，抽象的で広汎であり，そこに，「指導又は制約すべき目標，基準，考慮すべき要素等」（猿払事件（最大判昭和４９年１１月６日刑集２８巻９号３９３頁）の大隅裁判官ら反対意見参照）はなく，同号により規定された規則は，法律の具体的な授権に基づいて制定された規定とはいえない。

⑶　すなわち，法１９条１６号は，先に述べたとおり，「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。」と規定するだけである。確かに，「これらに準ずるもの」という基準はあるものの，法１９条は，その１号から１５号まで特定個人情報の提供が認められる例を広汎に規定しており，また，同１５号の「人の生命，身体又は財産の保護のために必要がある場合において，本人の同意があり，又は本人の同意を得ることが困難であるとき」のように抽象度が高い。マイナンバー法においてやり取りされる情報が税や社会保障に関する比較的センシティブな，秘匿性の高い情報であることから憲法上も特に保護すべき情報であることに鑑みれば，「これらに準ずるもの」という基準のみでは，具体的な基準，考慮すべき要素等が提示されているとはいえない。

この点，個人情報保護委員会規則に委任する他の規定として，個人情報保護法２４条（外国にある第三者への提供の制限を定める規定）では，「個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国として個人情報保護委員会規則で定めるもの…」とか，「個人データの取扱いについてこの節の規定により個人情報取扱事業者が講ずべきこととされている措置に相当する措置を継続的に講ずるために必要なものとして個人情報保護委員会規則で定める基準…」のように，規則制定の際に考慮すべき要素が一応明示されているところ，これらに比しても，法１９条１６号の規定は，具体的な基準や考慮すべき要素等を提示していないものであるといえ，不十分な規定であると言わざるをえない。

確かに，個人情報保護委員会は，行政機関や事業者等，特定個人情報の取扱

者に対して，必要な指導・助言や報告徴収・立入検査を行い，法令違反があった場合には勧告・命令等を行う専門性の高い機関である。

しかし，そうであるからといって，行政機関が個人番号を利用し，特定個人情報を収集，保管することについて，広範な裁量による規則制定を認めてよいことにはならない。なぜなら，「委員会は，あくまで法律で定められた範囲どおりに番号制度が運用されていることを担保する監視機関であって，その範囲を決定する機関ではない。委員会は，情報技術に関する豊富な専門知識を有するが，これは技術面にかかわる「立法」（指針等の策定）を行う正当性を与えるものであっても，情報経路の決定・拡張する「立法」を行う正当性を与えるものではない。したがって，委員会規則のみに基づいてなされる個人情報の提供は，形式的根拠を欠くものとして違憲と解すべきであろう。」（甲２１（山本龍彦「番号制度の憲法問題―住基ネット判決から考える」同『プライバシーの権利を考える』２２４頁））と山本龍彦教授が述べるとおり，同委員会は国会による民主的コントロールは受けておらず，同委員会の判断であっても，「法律」と同視することは許されないからである。

⑷　以上より，番号利用法１９条１６号による委任の範囲は，抽象的で広汎であり，政令及び規則へ白紙委任をしていることは明らかである。

３　番号利用法施行令別表７号ないし９号及び１１号等が番号利用法１９条１４号又は同法全体の委任の趣旨を超えるものであること

⑴　原判決の判断

原判決は，番号利用法施行令別表７号ないし９号及び１１号は，番号利用法１９条１４号に具体的に列挙された調査等と同様の公益上の必要のあるものに含まれると解するのが相当であり，番号利用法１９条１４号又は同法全体の委任の趣旨を超えるものと認めることはできないと判断した。

⑵　番号利用法施行令別表８号について

ア　しかし，以下のとおり，番号利用法施行令別表８号（「租税に関する法律

又はこれに基づく条例の規定による質問，検査，提示若しくは提出の求め又は協力の要請が行われるとき。」）については，番号利用法１９条１４号又は同法全体の委任の趣旨を超える内容であることが明らかである。

イ　マイナンバー法１９条１４号は，犯則調査のための特定個人情報の提供を認めている。そして，同号の規定する「その他政令で定める公益上の必要があるとき」の一つとして，施行令別表８号は，租税に関する法律等による質問，検査，提示もしくは提出の求めまたは協力の要請が行われるときを挙げている。内閣府の説明では，同８号は「租税に関する法律の規定による質問，検査等を行う際に，納税者等が保有している個人番号が記載された税務関係書類など（特定個人情報）の確認等を行う場合があることから」設けられたものとされている。

確かに，両者を比較してみると，一見，マイナンバー法の挙げる犯則調査と施行令の挙げる税務調査は，租税が関係しているという点で関連性の強いもののようにも見える。

しかし，①犯則事件の調査においては，裁判所の発行する許可状により臨検等を行うことができる場合があり（国税通則法１３２条），必要があるときには警察官の援助を求めることもできる（国税通則法１４１条）が，税務調査では，当該職員の質問に対して答弁をしなかった場合に刑罰が予定されているにすぎず（国税通則法１２８条など），調査自体の強制までは認められていないことからすれば，裁判所の判断に基づいて行われることがある犯則調査だけを特定個人情報の提供が認められる場面として挙げたことは，より強制力が弱く，裁判所の関与もないままに行われることを特質とする税務調査の場面では特定個人情報の提供を認めないというのがマイナンバー法１９条１４号の趣旨であること，②犯則調査と税務調査の間には，それらが行われる頻度という点で大きな違いがあり（具体的には，国税庁が平成２９年（２０１７年）度に査察調査に着手した件数は１７４件であるのに対して，

同年度において行った税務調査の件数は６２万３０００件であったとされる。），租税分野での調査において圧倒的な割合を占める税務調査において特定個人情報の提供を認めるかはマイナンバー制度においてきわめて重要な判断であり，この場合にも特定個人情報が提供されると想定されていたのであれば，それを法律の明文で定めていたはずであること，③松山地判平成１３年１１月２２日（判タ１１２１号２６４頁），名古屋高判昭和５０年８月２８日（税資９３号１１９８頁）などの裁判例でも，犯則調査と税務調査は異なる性格をもつことが確認されていることからすれば，立法者は特定個人情報を提供できる場面から税務調査を意図的に除外したと考えるのが合理的である。

なお，施行令（案）に対するパブリックコメントにおいても既に指摘されているように，平成２４年（２０１２年）の第１８０回国会に提出された旧法案では，特定個人情報の提供禁止の例外の一つとして「租税に関する法律の規定に基づく犯則事件の調査若しくは租税に関する調査」を挙げていた（当時の１７条１１号）。しかし，この法案が廃案になったのち，現在の法律には，旧法案にはあった「若しくは租税に関する調査」の部分が削除されている。

ウ　以上より，番号利用法施行令別表８号は，番号利用法１９条１４号に具体的に列挙された調査等とは，明らかに性格を異にしており，立法者は特定個人情報を提供できる場面から税務調査を意図的に除外したといえるから，同号は，番号利用法１９条１４号又は同法全体の委任の趣旨を超える内容であることが明らかである。

(3)　番号利用法施行令別表７号，同１１号，同２４号について

ア　また，以下のとおり，番号利用法施行令別表７号（「少年法第六条の二第一項又は第三項の規定による調査が行われるとき。」），同１１号（「国際捜査共助等に関する法律第一条第一号に規定する共助（同条第四号に規定する受

刑者証人移送を除く。）又は同法第十八条第一項の協力が行われるとき。」），同２４号（「国際刑事裁判所に対する協力等に関する法律第二条第四号に規定する証拠の提供，同条第十号に規定する執行協力又は同法第五十二条第一項に規定する管轄刑事事件の捜査に関する措置が行われるとき。」）についても，番号利用法１９条１４号又は同法全体の委任の趣旨を超える内容であることが明らかである。

イ　この点，①番号利用法１９条は，不正な特定個人情報の提供によるプライバシー権侵害を防止するため，特定個人情報の提供を原則禁止し，かかる禁止が解除される例外事由を各号で規定することとされていること，②番号制度が，「個人番号及び法人番号の利用に関する施策の推進は，個人情報の保護に十分配慮しつつ，行政運営の効率化を通じた国民の利便性の向上に資することを旨として，社会保障制度，税制及び災害対策に関する分野における利用の促進を図るとともに，他の行政分野及び行政分野以外の国民の利便性の向上に資する分野における利用の可能性を考慮して行われなければならない。」（番号利用法３条２項）ことからすれば，当該番号性の趣旨・目的に反する特定個人情報の提供は許されないことは明らかである。

ウ　しかし，別表７号，同１１号，同２４号のいずれにおいても，国民の利便性の向上や，社会保障制度，税制及び災害対策に関する分野における利用の促進との関係が明らかではなく，番号利用法１９条１４号又は同法全体の委任の趣旨を超える内容であることが明らかである。

⑷　番号利用法施行令別表９号，同１７号について

ア　さらに，以下のとおり，番号利用法施行令別表９号（「破壊活動防止法第十一条の規定による処分の請求，同法第二十二条第一項の規定による審査，同法第二十七条の規定による調査又は同法第二十八条第一項（無差別大量殺人行為を行った団体の規制に関する法律第三十条において準用する場合を含む。）の規定による書類及び証拠物の閲覧の求めが行われるとき。」），番号利

用法施行令別表１７号（無差別大量殺人行為を行った団体の規制に関する法律第七条第一項，第十四条第一項若しくは第二十九条の規定による調査，同法第七条第二項若しくは第十四条第二項の規定による立入検査又は同法第十二条第一項の規定による処分の請求が行われるとき。）についても，番号利用法１９条１４号又は同法全体の委任の趣旨を超える内容であることが明らかである。

イ　すなわち，別表７号，同１１号，同２４号のところで述べたところと同様，いずれにおいても，国民の利便性の向上や，社会保障制度，税制及び災害対策に関する分野における利用の促進との関係が明らかではなく，番号利用法１９条１４号又は同法全体の委任の趣旨を超える内容である。

ウ　さらに，特定個人情報が提供されてよい場面として公安目的の調査を挙げておらず，刑事事件の捜査を挙げるにとどまっていることとの関係が問題となる。

この点，刑事事件の捜査を通じた情報収集から考えると，それは具体的な事件との関係で，その事件に関係する人物・団体を調べるために行われるものである。それに対して，公安目的での資料の収集は，特定の人や団体に着目するものである。そのため，刑事事件での捜査と比べて，公安目的での資料の収集は，個人や団体に対する偏見に基づいてなされる危険性を内包している。

こうした場面で特定個人情報が提供されるのであれば，個々人に対して，自身を標的にして情報収集がなされているとの印象を生み，それは，調査対象者でなくても，人々に「政府によって監視されている」との意識を生む。さらに，そうした意識が，憲法で認められているはずの行為も控えようとする心理的効果を生むことも懸念される。

このように，公安目的での情報収集は，個々人の憲法上の権利の行使を抑圧する心理的な効果ももちうる。それゆえ，公安上の措置に際しての特定個

人情報の提供は，刑事事件の捜査時の提供との均衡性・同質性を欠くものであり，マイナンバー法１９条１４号による委任の範囲を逸脱しており，違法，違憲である。

⑸　小括

以上より，番号利用法施行令別表７号ないし９号及び１１号等は，番号利用法１９条１４号又は同法全体の委任の趣旨を超えるものであり，憲法１３条，同４１条との関係で，違憲無効である。

第６　番号制度は個人情報の利用提供等を正当な目的の範囲内で行う制度となっていないこと

１　原判決の判断

原判決は，番号制度の目的は，行政機関等が，個人番号を活用し，情報システムを運用して，効率的な情報の管理及び利用並びに他の行政事務を処理する者との間における迅速な情報の授受を行うことができるようにすることで，①行政運営の効率化，②行政分野におけるより公正な給付と負担の確保，③手続の簡素化による国民の負担の軽減，本人確認の簡易な手段その他の利便性の向上を図ることにあるとし，いずれも正当なものであると判断した。

２　原判決の誤り

しかし，以下のとおり，いずれの目的も，具体的な立法・制度との関連性がほとんどないか，または弱いものであり，自己情報コントロール権の制限の重大性に見合わない目的であるから，正当なものとは到底いえない。たとえれば，性的文書の頒布・販売を制限する立法の「目的」として，他人の生命の保護という事由を揚げるようなもので，「目的」自体は，確かに，重要で正当であろうが，規制対象と目的との間に関連性は見いだせない（門田孝「違憲審査における「目的審査の検討」（一）参照」）。

⑴　行政運営の効率化について

ア　原判決は，番号制度の導入による行政運営の効率化や経済効果等について

は，種々の試算がなされているところ，現時点でこれらの試算が誤りであると認めるに足りる証拠はなく，そして，当該目的が果たされることにより，限りある国家予算，人的資源等を効率的に運用することに繋がるものであって，公益の増進に資するから，当該目的は正当であると認められるなどとした。

イ　しかし，番号法が施行されて既に５年以上経過しているが，試算が出されたきり，具体的に，過誤や無駄がなくなったとか，経費削減の効果があったということは示されていない。むしろ，例えば，厚労省職業安定局が個人番号制度とハローワークの事業をつなぐ中間サーバーを約８０億円かけて整備しながら，その利用率で最大で想定の０．１％にとどまっていたというような明らかに費用対効果が認められない実態が浮き彫りになっている。

すなわち，現在までに番号制度による行政運営の効率化を示す結果は得られておらず，立法時に詳細な検討がされていなかったことが強く推認されるから，当該目的は正当とは認められず，便宜上設定された目的であると言わざるをえない。

(2)　行政分野におけるより公正な給付と負担の確保について

ア　また，原判決は，当該目的が果たされることは，公平，公正な社会の実現及び社会保障がよりきめ細やかに的確に行われる社会の実現に繋がるものであって，公益の増進に資するから，当該目的は正当であるなどとするが，以下のとおり，番号制度により性格な所得把握等は期待できない。

イ　政府・与党社会保障改革検討本部が作成した２０１１年６月３０日付社会保障・税番号大綱 (https://www.soumu.go.jp/main_content/000141660.pdf) では，「全ての取引や所得を把握し，不正申告や不正受給をゼロにすることなどは非現実的であり，また，『番号』を利用しても事業所得や海外資産・取引情報の把握には限界があることについて，国民の理解を得ていく必要がある」（１９頁）として，正確な所得把握が困難であることが示されている。

このように，個人番号制度は，制度設計当初から正確な所得把握ができないことが明らかであったのであり，それに加えて資産の把握もできない以上，真に救済が必要な者への社会保障給付も不可能である。

公正な給付と負担の確保それ自体は正当ではあるが，個人番号制度はそれを実現するものとは言えない以上，そもそもそれを個人番号制度の目的とすること自体が誤りである。

(3) 手続の簡素化による国民の負担の軽減，本人確認の簡易な手段その他の利便性の向上について

ア さらに，原判決は，当該目的が果たされることにより，例えば，申請や届出手続が複雑あるは煩雑であることにより当該申請や届出を躊躇せざるを得ない国民を減らすことが可能になり，ひいては国民全体に対する利益をもたらし得るものといえ，公益の増進に資するから，当該目的は正当であるなどとするが，以下のとおり，当該目的は，自己情報コントロール権への介入を正当化するほどの行政目的たり得ない。

イ しかし，番号制度がない場合には，申請や届出手続が複雑あるは煩雑であることにより躊躇せざるをえないが，番号制度がある場合にはそのようにはならない具体的な申請や届出手続などは明らかにされておらず，根拠のない妄想の類に過ぎない。

また，玉蟲由樹教授が，「国民の利益が国民の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やや疑問が残る。本人利益を根拠として，公権力による個人の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の感が否めないからである。プライバシー保障を原則として考える限りにおいて，負担を受け入れ，あるいは，利便性の向上をあきらめることで，自己のプライバシー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ろう。したがって，国民の利益を根拠としてプライバシーへの介入を行うことは目的の面においてそもそも正当化可能なものと

はいいがたい。」等と指摘しているとおり（甲３４，１８頁），そもそも国民全体の些細な便益が，一個人の憲法上の人権を制約する目的として正当化されるはずがない。

3　結語

以上より，いずれの目的も，具体的な立法・制度との関連性がほとんどないか，または弱いものであり，自己情報コントロール権の制限の重大性に見合わない目的であるから，正当なものとは到底いえない。番号制度は，個人情報の利用提供等を正当な目的の範囲内で行う制度となっていないことは明らかである。

第７　法制度上又はシステム技術上の不備による情報漏えい，目的外利用される具体的危険性の有無，程度等に関する誤り

1　法制度上の不備の有無

(1)　原判決の判示

原判決は，番号利用法は，個人番号や特定個人情報が漏えいし，目的外利用されることを防ぐための種々の法制度上の措置を講じており，これに不備があるとまでは認められないとする。

そして，その理由として，番号利用法及び番号制度においては，①個人番号の利用や特定個人情報の提供が可能な場合は限定列挙されており，行政機関等や個人番号利用事務等実施者には，個人番号及び特定個人情報の収集，利用等をする各場面において様々な義務が課され，これに違反すれば刑罰の対象にもなること，②行政機関等が本人から個人番号の提供を受ける場面においては，成りすまし等を防止するために，本人確認措置をとることが義務付けられていること，③情報ネットワークシステムを用いた情報連携が行われた場合には，その記録を一定期間保管することが義務付けられ，個人情報保護法に基づく開示請求等によって本人がその情報を確認することができる仕組みが整っていること，④行政機関等が特定個人情報ファイルを保有するに先立って，特定個人情報保護評価を実施して個人情報保護委員会の承認を受ける仕組みが設け

られ，⑤個人情報保護委員会は，特定個人情報の取扱いに対する指導，助言，命令，立入検査等の権限を有し，独立性が強く保護された立場から個人情報の取扱いの監視，監護を実施する仕組みが整っていることを挙げる（原判決５２頁）。

(2) 控訴人らの主張

ア　たしかに，①に関し，番号利用法１９条は特定個人情報の提供を原則的に禁止し，例外的に許容される範囲を同条１号から１５号までに列挙している。

しかし，同条１６号は，個人情報保護委員会が番号制度の運用を監視・監督する機関に過ぎず，その範囲を決定する機関ではないにもかかわらず，「個人情報保護委員会規則で定め」た場合に，特定個人情報の提供を許容する旨規定している。

また，同条１４号は「その他政令で定める公益上の必要があるとき」に特定個人情報の提供を許容しているが，この規定は，結局のところ特定個人情報の提供の範囲をすべて政令に委ねてしまっていることになる。

このように「規則」や「政令」による例外が無限定に認められていることからすると，特定個人情報の提供には，重大な抜け穴があると言わざるをえない。すなわち，１９条は，情報漏えいや目的外利用の具体的危険性を防止しうるほどの「限定列挙」とはなっていないのである。

さらに，罰則につき，番号利用法は不正行為の罰則を従来よりは強化しているが，罰金刑や比較的短期の懲役刑に過ぎず，個人番号の取得により大きな経済的利益に結びつく場合があることからすれば，抑止力として十分とはいいがたい。その上，番号ないし特定個人情報の利用制限，提供制限，収集制限に対する通常の違反については罰則の対象になっていない。罰則が欠如している部分を個人情報保護委員会の適切な権限行使によりカバーしているといった実態も存しない。また，罰則適用の前提となる個人情報保護委員会の勧告・命令についても，後述するとおり，同委員会の機能不全によって，

大量の違法再委託がなされてもまともな指導・勧告さえ行われていないのであって，罰則適用の前提を欠くものとなっている。

したがって，罰則によって情報漏えい等が抑止されており，その危険がないなどということは到底できないのである。

イ　次に，④特定個人情報保護評価については，以下のような問題がある。

まず，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（甲３８・１９，２０頁）。

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（番号利用法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，わ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３７の２・３４頁）。

そして，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。

なお，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。

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。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のである（甲３９・１３頁）。

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。同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。

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。

要するに，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。

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（甲３８・２１，２２頁参照）。

さらには，特定個人情報保護評価の仕組みの問題点として，特定個人情報保護評価書がそもそも難解であることが挙げられる。これについては，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（甲３６・２０～２３頁，甲３７の１・１８～２１頁）

次に，意見募集が形骸化しているという問題点もある。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にはならないことに加え，評価実施者としては意見がない方が進めやすいことから，積極的に意見を掘り起こそうとするインセンティブの乏しいことが，意見募集の形骸化に拍車をかけている。このように意見募集の手続は形骸化しており，ほとんど機能していないのである。

そのほか，再委託問題における特定個人情報保護評価制度の機能不全も問題点として挙げることができる。

本来なら，特定個人保護評価制度があり機能しているはずであるところ，年金機構・国税庁・地方自治体それぞれで「評価書」で禁止されていた再委託がされていたことが発覚したのである（甲３６・１１，１２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端的に示している。

以上のように，特定個人情報保護評価制度は，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と言わざるを得ない。

ウ　さらに，⑤個人情報保護委員会自体の問題として，体制の不十分性を指摘することができる。

すなわち，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）ところ，非常勤については，そもそも欠席が多い（甲３６・２３，２４頁。甲３

７の４・７，８頁)。具体的には，２０１６年から２０１８年の３年間で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。

このように少人数体制であるにもかかわらず，その業務量は莫大で，２０１８年１年間の特定個人情報保護評価書は１万０７５８件に上る。これだけの業務を実情９名より少ない体制でこなすことは到底不可能である。

加えて，個人情報保護委員会は，その意義を果たすことはなく，特別税額通知書の誤送付等による漏えいの発生や情報連携システムに対する会計検査院の指摘，日本年金機構の不正再委託といった重要な問題について市民に対して何らの説明も行うことをせず，委員会としての調査や指導などの実態もなく，立ち入り検査及び苦情あっせんも十分ではないことから，その機能不全は明らかである（甲３８・１６～１９頁)。

また，先に挙げた日本年金機構の不正再委託に関しても，個人情報保護委員会の権限に詳しい森田明証人が「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３６・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。このように，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のである。

以上のように，個人情報保護委員会には体制の不備があり，個人番号や特定個人情報が漏えいし，目的外利用されることを防ぐための法制度上の措置として不十分でないことは明らかである。

エ　その他，原判決が指摘する②の本人確認措置や③の情報提供の記録と開示については，単にこのような制度や仕組みがあると言っているだけで，これらが実際に機能しているかについての検証は全くない。

そもそも，原判決は，情報漏洩等を防ぐために「種々の法制度上の措置」

が講じられているとして，措置を羅列しているだけで，その措置が実際に機能しているかどうかを検証する姿勢に欠けている。

2　システム技術上の不備の有無

(1)　分散管理の採用

原判決は，番号制度においては「分割管理」の方法により個人番号及び特定個人情報の管理を行っていることから，「一元管理の方法に比して，不正アクセス等があった場合における情報の大量流出の危険性を相当程度減らす効果が期待できる」と判示する（原判決５４頁）。

しかし，番号制度において採用されている「分散管理」が，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」そのものであることについては，原告第４準備書面で述べた通りである。

すなわち，控訴人らが原審において指摘したとおり，どのようなシステムであろうとも不備は生じ得，そこから情報漏えいや目的外利用等は生じ得るのである。分散管理されていようと，アクセス制限されていようと，マイナンバーという個人情報を紐付けるキーとしての共通番号が存在する以上，それを介した個人情報の不正取得の可能性は常に生じる。

ましてや，分散管理については，ハードウェア的には，全国２箇所に設置された自治体中間サーバー・プラットフォームのそれぞれに，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しているのであるから，いくらパーティション等で自治体ごとに区分されていようとも，１台のサーバーに全ての情報が蓄積されているという意味で一元管理と呼ぶほかないものである。このような危険な状態で，番号制度のシステムは構築されているのである。

(2)　情報提供ネットワークシステムの保護措置

原判決は，情報提供ネットワークシステム及びこれを用いた情報連携が，インターネットから隔離されていることを理由に外部からの不正アクセスのリスクは低いとするが（原判決５４，５５頁）これは極めて皮相で浅薄な認識で

ある。

番号制度における情報連携は，情報提供ネットワークシステム（コアシステム）を介して行われ，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ている。そして，このような仕組みを構築することによって「仮に一つの地方公共団体の自治体中間サーバーに不正アクセス等があったと視点も芋づる式に他の地方公共団体の自治体中間サーバーに保存された情報を引き出せるものではない」（被告第３準備書面１５頁）とされている。

しかし，情報提供ネットワークシステムは，国（総務大臣）の管理の下に置かれている（番号利用法２条１４項，２１条１項）。このことがこのシステムの本質的な問題点である。

国のいうように，情報提供ネットワークシステムにおいて，「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れば，情報管理者である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しまっているのである。

ここでは，現実に内部の情報流用が起きたかどうかということが問題ではな

い。情報管理者である国が，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。

これに対し，我が国の番号制度とよく似た仕組みを持ち，番号制度に先行して２００１年から運用が始められたオーストリアの情報連携制度は，情報連携を行うネットワークシステムについての管理を，州代表，労働組合の代表，連邦政府の代表，裁判所の代表などで構成される「データ保護委員会」という第三者委員会が行うことになっている。これは行政内部からの不正アクセスや名寄せを防止するためである。

GDPR（EU におけるデータ保護規則）においては，情報の管理主体（データ管理者）に対し，様々な規制をおいているが，これがなければビッグデータの管理者が自ら保有する個人データにアクセスし，自由にプロファイリング等ができてしまうからであり，これを放置すれば重大なプライバシー侵害を招くからである。本件番号制度は，国（行政機関）がすべての国民のあらゆる個人情報を番号に紐づけて管理し，情報提供ネットワークシステムを利用して合法的に情報連携を行う制度であるから，情報の管理主体による内部からの不正アクセスやプロファイリングを防止するための厳しい規制が求められるのは言うまでもない。そして，その最も端的な方法は，ネットワークシステムの管理主体を国（行政機関）から切り離すことであり，先行するオーストリアではこれを実現している。しかし，本件番号制度ではネットワークシステムの管理主体を国にしてしまっているので，これではシステム上内部からの不正アクセスを防止することはできない。内部の不正アクセスに対し，罰則や懲戒規定があるといっても，故意に不正アクセスを行う犯罪者の前では，これらはまったく無力である。

我が国の番号制度がオーストリア方式を採用せず，敢えてシステムを国の管

理下に置いたのは，まさに制度上の欠陥，しかも致命的な欠陥といえるのである。

3　事故事例の判断について

(1)　原判決は，「事故事例は，いずれも専ら人為的なミスや故意の不正行為に起因するものであり，番号制度自体の不備によるものとは認め難い。」とする。

ア　しかし，そもそも人為的ミスと故意の不正行為を同列に論ずることは明らかな誤りである。けだし故意の不正行為の場合は，その目的いかんによっては，例えば個人情報取得の目的による防御システムの突破などによる番号制度自体の悪用もありうるのであるからである。

故意の不正行為の最近の実例としては，三菱電機が２０２０年１１月２０日，第三者による不正アクセスによって，代金の支払先になっている金融機関８６３５口座の情報や取引先の名称や代表者，電話番号などが流出したと発表している。

三菱電機では２０１９年6月にもサイバー攻撃を受けたが，この際には機密性の高い防衛や鉄道や電力関連などの取引先の情報が流出したおそれがあり，当時の調査では，国内外のパソコンやサーバーなど１３２台でウィルス感染の疑いが確認されていた。その後三菱電機ではネットワークへのアクセス制限を強化し，マイクロソフト３６５の利用に必要なＩＤとパスワード認証に加え，社内ネットワーク内での本人認証システムをパスしなければ利用できない「２段階認証」を採り入れていた。ところがハッカーは，認証システムが発行する「電子チケット」を入手し，やすやすと侵入し，被害の再発を防げなかったのである。（甲４３）

又，２０２０年１１月にインターネット上で公開された情報によると，テレワークや遠隔操作に使われる情報機器の欠陥が悪用され，少なくとも６０７の国内企業や行政機関などがサイバー攻撃を受け，警察庁や日本政府観光局，岐阜県庁，リクルート，札幌大などでの被害が判明した。警察庁は，２

２０１９年８月から４６件の不正アクセスがあったと公表し，文部科学省では，大学など２１機関に対して不正アクセス被害を受けた恐れがあるとして注意喚起した。多くがＩＤ，パスワードなどの認証情報を盗まれており，盗まれたＩＤ，パスワードを使ってシステム内部に侵入されると機密情報を盗み出すのが容易になり，被害が拡大する恐れがある。（甲４４）

このような故意の不正アクセスが現に存在する以上，個人情報取得の目的による防御システムの突破による番号制度自体の悪用もありうるとみるべきである。

イ　更に，どのようなシステムであろうとも，それを利用し運用するのは人であるから，人もシステムの一部である。人為的ミスや故意の不正行為も，そのシステムの運用の中で生じている。とりわけ，個人番号の利用範囲が拡大していけばいくほど，そこに関わる機関や人の範囲は，民間も含めて拡大してくから，人為的なミスによる漏えいや不正行為の危険性も増大することになる。しかも，人為的ミスによるものであろうがなかろうが，一旦漏えいした場合の被害の質や大きさに何ら変わりはない。人為的ミスによる漏えいを，番号制度に基づく漏えいではないと断言する原判決が不当であることは明らかである。

従って，番号制度の技術上の不備を検討する際には，人為的ミスも含めて検討されなければならない。そして，現実に漏えい事故が多数発生している以上，番号制度において情報漏えいや目的外利用等が発生する危険性は，すでに十分に具体的危険だというべきである。

ウ　また，人為的ミスが避けられないものだとするなら，番号制度は，仮にミスや不正行為が発生しても，情報漏えい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はずである。しかし，番号制度には，そのような仕組みは全く考慮されていない。この点でも，システム技術上の不備があると言わざるを得ない。

(2) 原判決は「個人番号のみが流出する場合には個人のプライバシーに係る情報は含まれない上，流出した個人番号の不正利用を防止するため請求又は職権により新たな個人番号を取得することもできる。」とする。

しかし，各事故事例は，個人番号とともに，氏名，住所，収入に関する情報，税情報等の個人情報が漏えいしているのであって，個人番号だけが漏えいしたものは皆無である。つまり，番号制度の下で発生している漏えい事故は，常に個人番号と住所，氏名などの個人識別のための情報，及び個人に関する情報の３つがセットになって漏れているのであり，そこに記載されている番号が誰のものであるのかが直ちに判明してしまっているのである。

現に，２０２０年2月１２日，福井家庭裁判所武生支部は，家事審判の書類に記載された個人番号をマスキングしないまま，閲覧・謄写の許可がなされ，特定個人情報が外部に漏えいする事故が発生したことを明らかにした。

これは，同審判事件において，申立人の男性が，２０１９年１１月に相手方が提出した書類を同支部の許可を得て謄写したところ，３人分の個人番号を記載した税関係の書類２枚が含まれていたものであり，２０２０年１月に同支部職員が書類の内容を確認中に判明した。（甲４５）

そして，本事故事例においても，個人番号とともに，税関係の情報が漏えいしたのであり，個人番号だけが漏えいしたのではない。

裁判所から特定個人情報が漏えいする事故事例が発生したことで，個人番号だけが漏えいするということはありえないことが改めて明白になったといえる。

裁判所は，個人番号の記載のない書類の提出を求めるなど，個人番号について慎重な取扱いをしている。

そのような慎重な取扱いをしている裁判所であっても，特定個人情報の漏えいが発生したのであるから，他の公的機関や民間企業からの特定個人情報の漏えいは必然であるというほかなく，実際に漏えい事件が後を絶たない。このような現状から，特定個人情報の漏えいは人為的な過誤にとどまるものではなく，

現行の番号制度は特定個人情報の漏えいを防ぐことができる仕組みにはなっておらず，番号制度に不備があることは明らかであるといえる。

従って，個人番号自体にプライバシーに関する情報が含まれていないことは何らの安心材料にはならず，むしろ個人番号をキー（鍵）とする名寄せ・突合のリスクは，番号制度以前の漏えいとは比べ物にならないほど増大しているのである。

(3) さらに，原判決は「当該個人番号が流出した者について，流出した個人番号を用いて他の特定個人情報が流出したとか，データマッチングが行われたとの事実を認めるに足りる証拠もない。このことからも，成りすまし防止のための本人確認措置や罰則，分散管理や符号による紐づけなど，個人番号を用いた他の特定個人情報の流出やデータマッチングをできる限り防ぐための各種制度は，一定程度機能していることがうかがわれる。」とする。

ア 原判決指摘の，「データマッチング」「罰則」「分散管理」「符号」については，前項エ項で反論しているところであるので，本項では，「成りすまし防止」について反論する。

イ すなわち「成りすまし防止」について言えば，令和２年５月に発覚した石川県能登町での詐欺事件では，被疑者はマイナンバーカードを利用して成りすましを行ったものであるが，原判決指摘の「成りすまし防止のための本人確認措置」が機能しなかったために，成りすましによる詐欺が実行されたのであるから，原判決の判断は事実をもって否定されているのである。（甲４６）

ウ 結果として原判決は，流出に対する予防措置が「一定程度機能していることがうかがわれる」とする。

しかし，流出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かかわる個人番号利用事務には，官民含め，多くの実施者がかかわっている。それぞれの事務実施者のレベルで十分な漏えい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・利用を避けようがない。個人番号が流出するということは，流出した個人番号を利用して実際に不正な情報の取得・利用などが行われ，実害が出たかどうかという問題とはかかわりなく，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。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。

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，漏えい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いえる。したがって，予防措置の実効性も含めて，流出の危険性が否定できない状況においては，番号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。

⑷ 加えて原判決は，「違法な再委託に対しては，個人情報保護委員会が，指導や，立入検査を実施し，立入検査を踏まえた改善事項を指摘するとともに，改善状況について報告を求めるなど，再発防止に努めている。」とする。

ア 番号法１０条１項は，個人番号利用事務又は個人番号関係事務（以下「個人番号利用事務等」という。）を委託した者の許諾を得た場合に限り，その全部又は一部の再委託をすることができると規定している。

これは，再委託先が特定個人情報を保護するための十分な措置を講じているか，過去に個人情報の漏えい事故を起こしている場合には十分な改善

策を講じているかを委託元に慎重に検討させる趣旨であり，特定個人情報の安全対策上，極めて重要なものである。

しかし，委託元の許諾を得ない個人番号利用事務等の違法再委託は，本来は渡ってはならない再委託先に特定個人情報が渡ってしまったもので，その実質は特定個人情報の漏えいであるとともに，特定個人情報が本来管理すべき各地方自治体，行政機関等のコントロールから全く逸脱した形で無制限に流通することとなってしまい，国民の特定個人情報につき，誰がどのように利用しているかが全く把握できない状態となってしまう。

このように，違法再委託の問題の本質は，特定個人情報の安全性確保に極めて重大な脅威をもたらすという点にあり，法制度上の不備，制度上の欠陥が顕在化したものである。

イ　上記の決して看過されてはならない重大問題を内包する特定個人情報の再委託は，まず次の地方自治体，行政機関において続発した。

東京都では，墨田区，台東区，豊島区，江戸川区において違法再委託が発生した。

神奈川県では，川崎市において違法再委託が発生した。

埼玉県内では，さいたま市，東松山市，幸手市，和光市，深谷市，本庄市，羽生市において違法再委託が発生した。（甲４７）

そして，２０１９年５月２９日，熊本市は，個人番号を含む課税資料のデータ入力業務を委託した業者が，熊本市の許諾を得ることなく無断で他の業者に当該業務の一部を再委託していた事実を発表した。この違法再委託により漏えいした特定個人情報の本人の数は２万９１６０人とされている。（甲４８）

さらに，詳細は不明であるが，地方公共団体において２０１９年４月１日から同年９月３０日までの間に，違法再委託が４件発生し，約４８万５５００人，約２万９２００人，推計約３５万人，約４８万９００人の特定

個人情報が漏えいしたとされている。（甲４９）

このように，特定個人情報の違法再委託の問題は，多数の地方自治体，行政機関等において発生しており，違法再委託により漏えいした特定個人情報の数は，約３６７万件を超えたことになる。

(5) 原判決は結果として「これらの事故事例の存在をもって，直ちに番号制度自体に法制度上又はシステム技術上の不備があり，そのために原告らの特定個人情報が流出し又は不正な名寄せ，突合（データマッチング）がなされるなどの具体的な危険が生じていると認めることもできない。」とするが，これが誤りであることは前項までの指摘で明らかである。

すなわち，番号制度で利用される情報ネットワークシステムには，システム技術上の不備があり，また，人為的ミスによる漏えい等やデータマッチングによる危険も考慮した場合，情報ネットワークシステムは，これらに対する対処を全く行っていないに等しい状況にあると言える。従って，システム技術上も，十分に具体的危険のレベルに達しているというべきであり，原判決の認定・判断は誤りである。

第８　他の地裁判決の存在

マイナンバー制度については，全国各地の裁判所において，その合憲性を争う訴訟が複数提起されている。そのうち，本控訴審において，少なくとも参照すべき点について，以下に紹介する。

１　名古屋地方裁判所令和元年１２月２７日判決（事件番号：平成２８年（ワ）第１２９４号，同第２５２３号）

(1) 憲法１３条で保障される自由の内容（同判決２８頁）

同判決は，情報通信技術の急速な進歩と，膨大な量の情報の収集，保管，加工，伝達等が可能となっている現状を前提に，憲法１３条が保障する自由の内容について，「何人も，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，保管，開示又は公表されない自由又は法的利益を有する」と

判示した。

⑵　個人情報の秘匿性の程度（同判決３０頁）

また，同判決は，マイナンバー制度で取り扱われる個人情報の秘匿性について，「番号制度において特定個人情報として個人番号とひも付けられて利用等される個人情報は，利用分野が税，社会保障，災害対策の３分野に限られている現時点においても，所得情報や社会保障の受給歴といった秘匿性の高い情報を含むものであり，その量も多い。そして，これらの情報がそれぞれひも付けられている個人番号については，これを基にして様々な情報を集約，検索等できる論理的な可能性を否定できず，これらが漏えいしたり目的外利用されたりした場合には個人の私生活又はプライバシーが侵害される危険性がある。」として，マイナンバー制度で取り扱われる情報の秘匿性が高いことを明確に認定した。

そのうえで，合憲性の判断について，「検討に当たっては，番号制度が，全体として，以上のような性質を有する個人に関する情報の利用等について，必要かつ合理的な範囲にとどまることが担保されている仕組みになっているか否かについて，慎重に吟味する必要がある。」として，厳格に判断する必要があることを認めている。

２　東京地方裁判所令和２年２月２５日判決（事件番号：平成２７年（ワ）第３４０１０号，平成２８年（ワ）第９４０４号）

⑴　憲法１３条で保障される自由の内容（同判決５６頁）

同判決は，憲法１３条が，「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」と判示している。

ここでは，何らの理由を示すことなく当然の前提として，個人に関する情報の開示・公表だけではなく，その収集・利用といった情報の流れ全体に対して憲法１３条の保障が及ぶことが明示されている。

⑵　判断基準について（同判決５９～６０頁）

また，同判決は，マイナンバー制度で取り扱われる個人情報について，「直ちに個人の内面に関わるような秘匿性の高い情報とまではいえないものの，みだりに第三者に開示されたくないと考えることが一般的であって，取扱方法によっては個人の人格的な権利利益を損なうおそれがある個人に関する情報も含まれていると認めることができる。」として，その秘匿性が高いことを認めている。

さらに，「個人番号制度によって，上記のような個人に関する情報が個人番号と結び付けられ，情報提供ネットワークシステムによる情報連携の対象となったことにより，複数の行政機関等が保有する個人に関する情報の同一性の確認が，個人番号制度の導入前と比較して，格段に正確かつ迅速に行うことが可能になったと認められる。」としたえで，「個人番号制度では，その取り扱う情報として，個人識別情報以上に慎重に取り扱われるべき個人に関する情報が含まれるものと認められる。」として，マイナンバー制度自体により，個人の権利利益に対する侵害の危険が高まっていることを認めている。

そして，法律や条例の根拠の有無，制度目的の正当性，目的との適合性，及び法制度・システム技術上の不備について，「それぞれを慎重に審理判断する必要がある」として，厳格な審理判断が必要であることを認めている。

3　仙台地方裁判所令和２年６月３０日判決（事件番号：平成２７年（ワ）第１６３２号，平成２８年（ワ）第３６４号）

(1)　行政機関等相互の情報連携の問題点（同判決２４頁）

同判決は，「ある行政機関が保有している個人情報を他の行政機関に提供することは，「個人に関する情報」を「第三者」に「開示」することに当たると解されるから（最高裁住基ネット判決も，このような解釈を前提にしていると解される。），行政機関等相互における個人情報の提供は，「個人に関する情報」を「第三者に開示又は公表する」ことに当たる」と判示している。

これは，マイナンバー制度で取り扱われる情報が，従前いずれかの行政機関等において取り扱われていたとしても，マイナンバー制度における情報連携に

よってこれまで取り扱えなかった行政機関が取り扱えるようになることは，個人の情報に対する新たなプライバシー侵害の契機となることを，明確に認定したものである。

⑵　憲法１３条が保障する自由の内容（同判決２４頁）

また，同判決は，「プライバシーの侵害は，開示又は公表の場面だけで問題となるのではなく，収集，保存，利用の各場面でも問題となりうるから，公権力の行使から国民の私生活上の自由を保護するためには，「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」が保障されるだけでは足りず，「個人に関する情報をみだりに収集，保存，利用されない自由」も保障される必要があると解するのが相当である。よって，憲法１３条は，「個人に関する情報をみだりに収集，保存，利用されない自由」も保障していると解するのが相当である。」と判示する。

⑶　マイナンバー制度で扱われる個人情報について（同判決２５頁）

マイナンバー制度で取り扱われる個人情報についても，同判決は，「人がみだりに他者に開示されたくないと考えることが一般的といえる情報（例えば，生活保護法２４条１項の保護の開始の申請の受理に関する事務の処理において利用される，保護の開始を申請する者の資産および収入の状況に関する情報（番号利用法９条，同法別表第１の１５の項，番号利用法別表第一の主務省令で定める事務を定める命令１５条２号，生活保護法２４条１項４号），地方税法による地方税の課税標準の決定に関する事務の処理において利用される，前年の所得について算定した総所得金額（番号利用法９条，同法別表第１の１６の項，番号利用法別表第一の主務省令で定める事務を定める命令１６条，地方税法３２条等）等）まで，多種多様なものがある。」として，秘匿性の高い情報が含まれることを明確に認めている。

⑷　個人番号自体の重要性（同判決２５～２６頁）

さらに，同判決は，個人番号自体の重要性についても，「個人番号は個人情報

と紐づけられるものであり，個人番号をキーに個人情報の追跡・名寄せ・突合が行われ，集積・集約された個人情報によって本人が意図しない形で個人像が構築されたり，特定の個人が選別されて差別的に取り扱われたりする一般的・抽象的な危険があるから…，個人番号自体が，当該個人番号に紐づけられた個人情報がみだりに他者に開示されたり，名寄せ・突合等されたりすることを防止するため，適切に管理，利用等されるべき情報ということができる。」と判示している。

すなわち，個人番号自体が個人のプライバシー保護のために重要であり，個人番号に紐づけられた情報ではなく，個人番号自体を「みだりに収集，保存，利用されない自由」が憲法１３条により保護されると認めている。

4　大阪地方裁判所令和３年２月２４日判決（事件番号：平成２７年（ワ）第１１９９６号，平成２８年（ワ）第２０２３号，同第２８９５号）

(1)　憲法１３条で保障される自由の内容（同判決４４頁）

同判決は，高度情報化社会がデータベースに強く依存し，様々な情報が集積統合されてデータベースが構築されている現状を認めたうえで，「個人に関する情報が，一旦適法に公表又は開示された場合に，その情報について他者により自由に収集，保有，管理，利用等されるとすれば，本人が予期しない形で，データベース化されるなどして様々な個人情報が集積・統合されることにより，部分的又は完全な人物像が作り上げられ，場合によっては誤った人物像が形成されるおそれが生じ，人々の社会的活動に対する萎縮効果などの個人の人格的自律に多大な影響が生じうる。」と認定した。

そのうえで，憲法１３条が保障する自由について，「憲法１３条が公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個人の私生活上の自由には，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があるにとどまらず，個人に関する情報をみだりに収集，保有，管理又は利用されない自由をもその内容に含むものと解するべきである。」と判示した。

⑵　違憲審査基準について（同判決４５～４６頁）

また，同判決は，違憲審査基準に関する部分において，「個人情報が漏えいした場合に，漏えいした特定個人情報の名寄せにより，本人の関与しないところで，その意に反した個人像が勝手に作られるというプロファイリングの危険性や，プロファイリングによって，他人がその本人に成りすますことが容易になり，本人の関与しないところで歪んだ個人像が作られるという危険性が生じる可能性が存在することが認められるところ，このような個人情報の漏えいによる影響が重大であることは否定できない」として，マイナンバー制度によるプロファイリングの危険性について，明確に認定している。

そのうえで，法律や条例の根拠の有無，制度目的の正当性，目的との適合性，及び法制度・システム技術上の不備について，「慎重に判断して決するべきである」として，厳格な審査基準が必要であることを認めている。

５　裁判例のまとめ

控訴人らは，上記のいずれの判決についても，その判断枠組みや事実認定，結論について，これに賛成するものではない。しかし，これらの判決において認定された，次の①ないし⑤は，最低限考慮されなければならない。

①　憲法１３条が保障する自由の内容

憲法１３条は，個人に関する情報について，開示・公表にとどまらず，収集，保管，利用等を含む，情報の流れ全てを保障している。そして，個人は，これをみだりに収集，保管，利用，開示又は公表されない自由又は法的利益を有している。

②　マイナンバー制度で扱われる個人番号・個人情報の秘匿性

マイナンバー制度で取り扱われる個人情報には，秘匿性の高い情報が多く含まれている。

また，個人番号も，これをキーとして個人情報の追跡・名寄せ・突合が行われ，集積・集約された個人情報によって本人が意図しない形で個人像が構

築されたり，特定の個人が選別されて差別的に取り扱われたりする一般的・抽象的な危険がある。

したがって，いずれの情報も，漏えいや目的外利用により個人の私生活又はプライバシーが侵害される危険性がある。

③　行政機関等における情報連携について

ある行政機関が保有している個人情報を他の行政機関に提供すること自体が「個人に関する情報」を「第三者」に「開示」することに該当することから，マイナンバー制度で取り扱われる情報が，従前いずれかの行政機関等において取り扱われていたとしても，マイナンバー制度における情報連携によってこれまで取り扱えなかった行政機関が取り扱えるようになることは，個人の情報に対する新たなプライバシー侵害の契機となる。

④　プロファイリングの危険性

現在の高度情報化社会においては，様々な情報が集積統合されてデータベースが構築されており，個人に関する情報が公表，開示又は漏えいした場合には，本人が予期しない形でデータベース化されるなどして様々な個人情報が集積・統合されることにより，部分的又は完全な人物像が作り上げられる可能性がある。そして，場合によっては，本人の意に反した又は誤った人物像が形成されたり，他人がその本人に成りすますことで歪んだ個人像が作られる危険性があり，人々の社会的活動に対する萎縮効果などの個人の人格的自律に多大な影響が生じうる。

⑤　判断基準

マイナンバー制度で取り扱われる情報の秘匿性やプロファイリングの危険性などに照らし，マイナンバー制度の憲法適合性を判断するに際には，法律や条例の根拠の有無，制度目的の正当性，目的との適合性，及び法制度・システム技術上の不備について，厳格に判断する必要がある。

そして，原判決は，上記①ないし⑤をいずれも満たしておらず，これは原判決

の結論にも影響を及ぼしていることから，この点からも，原判決は直ちに破棄されなければならない。

第９　さいごに

以上のとおり，原判決の判示するプライバシーに関する権利・自由の内容は，もはや時代遅れであり，直ちに取り消されなければならない。また，現在の高度情報化社会においてデータベースの構築が果たす役割，個人の人格的自律に与える重大な影響はもはや無視できないのであって，この点を軽視し，極めて緩やかな基準による司法審査に終始することは許されない。

また，現在，無秩序に，際限なくマイナンバーの利用範囲が拡大され，または拡大が提唱されているおり，このような状況は，番号利用法が施工された当初，国民にとっては全く予見できないものであった。これらの利用範囲の拡大は，番号利用法が違憲な白紙委任を許すものであり，また委任立法の範囲を逸脱したものであることも明らかである。

さらに，利用範囲の拡大に伴い，もはや当初の制度目的も形骸化しており，マイナンバー制度の目的には，自己情報コントロール権という重大な人権を制約することを正当化できる目的など存在しないと言わざるをえない。

本控訴審においては，国家が運営する巨大データベースであるマイナンバー制度が個人の自己情報コントロール権及び情報管理システムに接続されない自由を侵害するものであることを正面から認め，多数の漏えい事故等が生じていることや監視体制の実情といった事実に基づき，その危険性及び制度の合理性を判断することを求める。そして，事実に基づいて審理するならば，マイナンバー制度が個人の人格的自律を侵害する違憲な制度であることは明らかである。

以上