



言渡	令和5年3月9日
交付	令和5年3月9日
裁判所書記官	

令和4年(才)第39号

判 決

当事者の表示 別紙当事者目録記載のとおり

上記当事者間の福岡高等裁判所令和2年(ネ)第457号マイナンバー(個人番号)利用差止等請求事件について、同裁判所が令和3年9月29日に言い渡した判決に対し、上告人らから上告があった。よって、当裁判所は、次のとおり判決する。

主 文

本件上告を棄却する。

上告費用は上告人らの負担とする。

理 由

上告代理人山本一行ほかの上告理由について

第1 事案の概要

1 本件は、行政手続における特定の個人を識別するための番号の利用等に関する法律(令和3年法律第36号による改正前のもの。以下「番号利用法」という。)により個人番号を付番された上告人らが、被上告人が番号利用法に基づき上告人らの特定個人情報(個人番号をその内容に含む個人情報)の収集、保管、利用又は提供(以下、併せて「利用、提供等」という。)をする行為は、憲法13条の保障する上告人らのプライバシー権を違法に侵害するものであると主張して、被上告人に対し、プライバシー権に基づく妨害予防請求又は妨害排除請求として、上告人らの個人番号の利用、提供等の差止め及び保存されている上告人らの個人番号の削除を求めるとともに、国家賠償法1条1項に基づき、慰謝料等の支払を求める事案である。

2 原審の適法に確定した事実関係の概要等は、次のとおりである。

(1) 番号利用法の目的

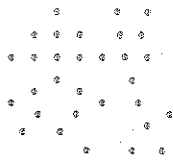


番号利用法は、①行政機関、地方公共団体その他の行政事務を処理する者（以下「行政機関等」という。）が、個人番号等の有する特定の個人等を識別する機能を活用し、及び当該機能によって異なる分野に属する情報を照合してこれらが同一の者に係るものであるかどうかを確認することができるものとして整備された情報システムを運用して、効率的な情報の管理及び利用並びに他の行政事務を処理する者との間における迅速な情報の授受を行うことができるようにするとともに、これにより、行政運営の効率化及び行政分野におけるより公正な給付と負担の確保を図り、かつ、行政機関等に対し申請を行うなどする国民が、手続の簡素化による負担の軽減、本人確認の簡易な手段その他の利便性の向上を得られるようにするために必要な事項を定めるほか、②特定個人情報の取扱いが安全かつ適正に行われるよう、行政機関の保有する個人情報の保護に関する法律、独立行政法人等の保有する個人情報の保護に関する法律及び個人情報の保護に関する法律（いずれも令和3年法律第37号により廃止又は改正される前のもの。以下同じ。また、以下、これらを併せて「一般法」という。）の特例を定めることを目的とするものである（番号利用法1条）。

(2) 個人番号及びその利用範囲

ア 個人番号とは、住民票コード（住民基本台帳法7条13号）を変換して得られる番号であって、当該住民票コードが記載された住民票に係る者を識別するために指定されるものをいい（番号利用法2条5項）、住民票コードを復元することのできる規則性を備えるものではなく、全国を通じて重複のない11桁の番号及び1桁の検査用数字によって構成されるところ、個人番号とすべき番号は、地方公共団体情報システム機構によって生成される（同法8条、同法施行令（令和3年政令第195号による改正前のもの。以下同じ。）8条）。

市町村長（特別区の区長を含む。以下同じ。）は、当該市町村（特別区を含む。以下同じ。）が備える住民基本台帳に記録されている者について、上記機構から通知された個人番号とすべき番号をその者の個人番号として指定し、その者に対し、



当該個人番号を通知しなければならず（同法7条1項、附則3条）、また、その者の申請により、その者に係る個人番号カード（氏名、住所、生年月日、性別、個人番号その他政令で定める事項が記載され、本人の写真が表示され、かつ、これらの事項その他総務省令で定める事項が電磁的方法により記録されたカードであって、権限を有する者以外の者による閲覧又は改変を防止するために総務省令で定める必要な措置が講じられたもの）を交付する（同法17条、同法施行令13条）。

市町村長は、当該市町村が備える住民基本台帳に記録されている者の個人番号が漏えいして不正に用いられるおそれがあると認められるときは、その者の請求又は職権により、その者の従前の個人番号に代えて、新たな個人番号を指定し、速やかに、その者に対し、当該個人番号を通知しなければならない（同法7条2項）。

イ 番号利用法は、行政機関等が、一定の事務の処理に関して保有する特定個人情報ファイル（個人番号をその内容に含む個人情報ファイル）において個人情報を効率的に検索し、及び管理するために必要な限度で個人番号を利用することができるとするほか（同法9条1項、2項。以下、これらの規定により上記限度で個人番号を利用して処理する事務を「個人番号利用事務」という。）、法令又は条例の規定により上記一定の事務の処理に関して必要とされる他人の個人番号を記載した書面の提出その他の他人の個人番号を利用した事務を行うものとされた者は、当該事務を行うために必要な限度で個人番号を利用することができるとしているが（同条3項。以下、同項の規定により個人番号利用事務に関して行われる他人の個人番号を必要な限度で利用して行う事務を「個人番号関係事務」という。）、上記一定の事務の範囲を、社会保障、税、災害対策及びこれらに類する分野の法令又は条例で定められた事務に限定することで、個人番号によって検索及び管理がされることになる個人情報を限定している。

また、一般法においても、個人情報について、あらかじめ特定された利用目的以外の目的のために利用すること（以下「目的外利用」という。）は原則として禁止されているところ（行政機関の保有する個人情報の保護に関する法律8条等）、番

号利用法は、人の生命、身体又は財産の保護のために必要である場合であっ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や、激甚災害発生時等であって一定の要件を満たす場合に限り、特定個人情報の目的外利用を認め、目的外利用が許容される例外事由を一般法よりも厳格に規定している（番号利用法9条4項、30条、32条）。

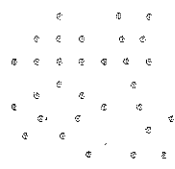
(3) 特定個人情報の提供に関する規制

番号利用法は、特定個人情報の提供を原則として禁止し（同法19条）、その禁止が解除される例外事由を同条各号で規定している。具体的には、同法に基づく制度上当然に特定個人情報の提供が予定されるときや、同法制定以前から同様の個人情報の提供を認めていた他の法律の規定により特定個人情報の提供がされるとき等に加え、7号及び8号において、行政機関等が同各号により限定された一定の事務を処理するために必要な一定の特定個人情報の提供を他の行政機関等から受ける必要があるときについても、特定個人情報の提供を認めるものとし、7号又は8号の規定による提供に際して、後記(4)のように情報提供ネットワークシステムの使用を義務付けている。

また、番号利用法は、不必要に特定個人情報が入手されること自体を防ぐため、同条各号のいずれかに該当する場合を除き、他人（自己と同一の世帯に属する者以外の者をいう。以下同じ。）に対して個人番号の提供を求めることや、特定個人情報（他人の個人番号を含むものに限る。）の収集又は保管をすることを禁止している（同法15条、20条）。

(4) 情報提供ネットワークシステムによる情報連携

ア 番号利用法の下でも、個人情報が共通のデータベース等により一元管理されるものではなく、各行政機関等が個人情報を分散管理している状況に変わりはないため、同法の目的を達成するためには、各行政機関等との間の情報連携が必要となる。そのため、同法は、情報提供ネットワークシステムによる特定個人情報の提供について、次のような規定を設けている。



イ 情報提供ネットワークシステムとは、行政機関の長等の使用に係る電子計算機を相互に電気通信回線で接続した電子情報処理組織であって、暗号その他その内容を容易に復元することができない通信の方法を用いて行われる番号利用法19条7号又は8号の規定による特定個人情報の提供を管理するために、同法21条1項の規定に基づき総務大臣が設置し、及び管理するものをいう（同法2条14項）。

上記システムによる情報連携は、番号利用法19条7号又は8号の規定により特定個人情報の提供を求める者（以下「情報照会者」という。）及びその提供をする者（以下「情報提供者」という。）が、情報提供用個人識別符号（同条7号又は8号の規定による特定個人情報の提供を管理し、及び当該特定個人情報を検索するために必要な限度で個人番号に代わって用いられる特定の個人を識別する符号）を用いて特定個人情報の授受をするというものであり、具体的には、情報照会者は、上記符号を上記システムの設置及び管理をする総務大臣から取得した上で、総務大臣に対して上記符号や照会する特定個人情報の項目等を送信し、総務大臣は、当該特定個人情報の提供が同法21条2項所定の要件（同法19条7号又は8号により適法にされたものであること並びに情報照会者及び情報提供者の保有する特定個人情報ファイルについて後記(5)イの特定個人情報保護評価が適正に実施されていること）を充足するものであることを確認した上で、情報提供者に対して特定個人情報の提供の求めがあった旨を通知し、同通知を受けた情報提供者は、情報照会者に対して当該特定個人情報を提供するものとされている（同法19条7号、8号、21条、21条の2、22条、26条）。

番号利用法は、情報照会者及び情報提供者並びに総務大臣に対し、同法19条7号又は8号の規定により特定個人情報の提供の求め又は提供があったときは、情報照会者及び情報提供者の名称、提供の求め及び提供の日時、特定個人情報の項目等を記録し、当該記録を一定期間保存することを義務付けており（同法23条、26条）、本人は、これらの記録の開示や訂正を求めることができる（同法31条、32条、行政機関の保有する個人情報の保護に関する法律12条、27条等）。

ウ 番号利用法は、総務大臣並びに情報照会者及び情報提供者に対し、同法19条7号又は8号の規定による特定個人情報の提供の求め又は提供に関する事務に関する秘密の漏えいの防止等のために、情報提供ネットワークシステム並びに情報照会者及び情報提供者が上記事務に使用する電子計算機の安全性及び信頼性を確保すること等を義務付けている（同法24条、26条）。これを受け、上記システムは、インターネットから切り離された行政専用の閉域ネットワークを使用し、特定の個人を識別するための符号として、個人番号を推知し得ず、かつ機関ごとに異なる情報提供用個人識別符号を用いるとともに、その通信が暗号化され、提供される特定個人情報自体も情報提供者により当該情報照会者しか復号できないように暗号化されている。

さらに、番号利用法は、上記事務又は上記システムの運営に関する事務に従事する者又は従事していた者に対し、その業務に関して知り得た当該事務に関する秘密の漏えい又は盗用を禁止している（同法25条、26条）。

(5) 特定個人情報の管理に関する規制

ア 番号利用法は、個人番号利用事務又は個人番号関係事務（以下、併せて「個人番号利用事務等」という。）を処理する者及びその委託を受けた者（以下、併せて「個人番号利用事務等実施者」という。）に対し、個人番号の漏えい等の防止その他の個人番号の適切な管理のために必要な措置を講ずることや、本人から個人番号の提供を受けるときに本人確認措置をとることを義務付ける（同法12条、16条）ほか、個人番号利用事務等の委託に関して、委託者の許諾を得た場合に限り再委託を認める（同法10条）とともに、委託者に対し、特定個人情報の安全管理が図られるよう、受託者に対する必要かつ適切な監督を行うことを義務付けている（同法11条）。

イ また、番号利用法は、個人番号利用事務等実施者等に対し、同法19条12号から16号までのいずれかに該当する場合を除き、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することを禁止する（同

法29条)とともに、行政機関の長等において、上記ファイルを保有し、又は保有しようとするときは、上記ファイルを取り扱う事務に従事する者に対して特定個人情報の適正な取扱いを確保するために必要なサイバーセキュリティの確保等に関する研修を行うものとしている(同法29条の2)。

そして、番号利用法は、上記ファイルを保有しようとする者が、事前に特定個人情報保護評価(特定個人情報の漏えいその他の事態の発生の危険性及び影響に関する評価)を自ら実施し、これらの事態の発生の抑止等をするための措置を講ずるものとしている(同法27条、28条)。同法28条による評価の実施が求められる場合、行政機関の長等は、特定個人情報ファイルを保有する前に、当該ファイルを取り扱う事務の概要及び同事務に従事する者の数、当該ファイルに記録されることとなる特定個人情報の量、当該ファイルを取り扱うために使用する電子情報処理組織の仕組み及び電子計算機処理等の方式、当該ファイルに記録された特定個人情報を保護するための措置等の各事項を評価した結果を記載した評価書を公示し、広く国民の意見を求め、得られた意見を十分考慮した上で評価書に必要な見直しを行った後に、当該評価書に記載された当該ファイルの取扱いについて個人情報保護委員会(内閣府設置法49条3項に基づき内閣府の外局として設置された第三者機関(個人情報の保護に関する法律59条)。以下「委員会」という。)の承認を受け、承認を受けたときは、速やかに当該評価書を公表するものとされ、評価書の公表を行っていない特定個人情報ファイルに記録された情報又は記録されることとなる情報については、番号利用法19条7号又は8号の規定による提供や提供の求めが禁止される(同法28条)。

(6) 規制の実効性を担保するための制度

ア 番号利用法は、上記の各規制の実効性を担保するため、個人の秘密に属する事項が記録された特定個人情報ファイルの不正提供(同法48条)、業務に関して知り得た個人番号の不正な利益を図る目的での提供又は盗用(同法49条)、職権を濫用して専ら職務の用以外の用に供する目的で行った個人の秘密に属する特定個

人情報が記録された文書等の収集（同法52条）等、上記の各規制に違反する行為のうち悪質なものについて、刑罰の対象とし、一般法における同様の罰則規定よりも法定刑を加重するなどしている（番号利用法第9章）。

イ また、番号利用法は、独立した第三者機関である委員会に種々の権限を付与した上で、特定個人情報の取扱いに関する監視、監督等を行わせることとしている。

すなわち、特定個人情報ファイルを保有する行政機関等は、当該ファイルに記録された特定個人情報の取扱いの状況について、定期的に、委員会による検査を受け、又は委員会に報告するものとし（同法29条の3）、個人番号利用事務等実施者は、特定個人情報ファイルに記録された特定個人情報の漏えい等の重大な事態が生じたときは、委員会に報告するものとされている（同法29条の4）。そして、委員会は、個人番号利用事務等実施者に対し、特定個人情報の取扱いに関し、必要な指導及び助言をすることができ（同法33条）、必要があると認めるときは、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をした者に対し、期限を定めて、当該違反行為の中止等を勧告した上で、又は緊急に措置をとる必要があると認めるときは勧告することなく、当該違反行為の中止等を命ずることができる（同法34条）。さらに、委員会は、特定個人情報を取り扱う者その他の関係者に対し、特定個人情報の取扱いに関し、必要な報告若しくは資料の提出を求め、又はその職員に当該関係者の事務所等に立ち入らせ、特定個人情報の取扱いに関し質問させ、若しくは帳簿書類等を検査させることができる（同法35条）。また、委員会は、情報提供ネットワークシステム等の構築及び維持管理に関し、合理化及び効率化を図った上でその機能の安全性及び信頼性を確保するよう、総務大臣その他の関係行政機関の長に対し、必要な措置の実施を求め、さらに、その措置の実施状況について報告を求めることができる（同法37条）。

第2 上告理由のうち憲法13条違反をいう部分について

1 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（最高裁平成19年（オ）第403号、同年（受）第454号同20年3月6日第一小法廷判決・民集62巻3号665頁）。

2(1) そこで、行政機関等が番号利用法に基づき特定個人情報の利用、提供等をする行為が上告人らの上記自由を侵害するものであるか否かを検討するに、前記第1の2(1)のとおり、同法は、個人番号等の有する対象者識別機能を活用して、情報の管理及び利用の効率化、情報連携の迅速化を実現することにより、行政運営の効率化、給付と負担の公正性の確保、国民の利便性向上を図ること等を目的とするものであり、正当な行政目的を有するものといえることができる。

(2) そして、前記第1の2(2)イのとおり、番号利用法は、個人番号の利用範囲について、社会保障、税、災害対策及びこれらに類する分野の法令又は条例で定められた事務に限定することで、個人番号によって検索及び管理がされることになる個人情報に限定するとともに、特定個人情報について目的外利用が許容される例外事由を一般法よりも厳格に規定している。

さらに、前記第1の2(3)及び(5)イのとおり、番号利用法は、特定個人情報の提供を原則として禁止し、制限列举した例外事由に該当する場合にのみ、その提供を認めるとともに、上記例外事由に該当する場合を除いて他人に対する個人番号の提供の求めや特定個人情報の収集又は保管を禁止するほか、必要な範囲を超えた特定個人情報ファイルの作成を禁止している。

以上によれば、番号利用法に基づく特定個人情報の利用、提供等は、上記の正当な行政目的の範囲内で行われているといえることができる。

なお、番号利用法19条14号及び16号は、上記の特定個人情報の提供の禁止が解除される例外事由の一部の定めを政令又は個人情報保護委員会規則に委任するが、特定個人情報の提供が許されるべき全ての場合を同法に規定することは困難であり、その一部を政令等に委任することには合理的必要性があるといえるべきである。そして、同条14号は、各議院が国会法104条1項により審査又は調査を行

うときなどといった具体的な場合を掲げた上で、「その他政令で定める公益上の必要があるとき」と定めるものであり、法令の規定に基づく審査や調査等が行われる場合であって、上記の具体的な場合に準ずる公益上の必要があるときに限定して政令に委任したものと解され、白紙委任を行うものとはいえないし、これを受けた番号利用法施行令25条及び別表各号の内容をみても、上記の委任の範囲を超えるものとは認められない。また、同法19条16号も、具体的かつ詳細な規定である同条1号から15号までに準ずる相当限られた場合に限定して個人情報保護委員会規則に委任したものであり、白紙委任を行うものとはいえず、これを受けた同規則の内容をみても、上記の委任の範囲を超えるものとは認められない。

3 もっとも、特定個人情報の中には、個人の所得や社会保障の受給歴等の秘匿性の高い情報が多数含まれることになるところ、理論上は、対象者識別機能を有する個人番号を利用してこれらの情報の集約や突合を行い、個人の分析をすることが可能であるため、具体的な法制度や実際に使用されるシステムの内容次第では、これらの情報が芽づる式に外部に流出することや、不当なデータマッチング、すなわち、行政機関等が番号利用法上許される範囲を超えて他の行政機関等から特定の個人に係る複数の特定個人情報の提供を受けるなどしてこれらを突合することにより、特定個人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得るものである。

しかし、番号利用法は、前記第1の2(2)イ及び(3)のとおり、個人番号の利用や特定個人情報の提供について厳格な規制を行うことに加えて、前記第1の2(5)及び(6)のとおり、特定個人情報の管理について、特定個人情報の漏えい等を防止し、特定個人情報を安全かつ適正に管理するための種々の規制を行うこととしており、以上の規制の実効性を担保するため、これらに違反する行為のうち悪質なものについて刑罰の対象とし、一般法における同種の罰則規定よりも法定刑を加重するなどととも、独立した第三者機関である委員会に種々の権限を付与した上で、特定個人情報の取扱いに関する監視、監督等を行わせることとしている。

また、番号利用法の下でも、個人情報が入通のデータベース等により一元管理されるものではなく、各行政機関等が個人情報を分散管理している状況に変わりはないところ、前記第1の2(4)のとおり、各行政機関等の中で情報提供ネットワークシステムによる情報連携が行われる場合には、総務大臣による同法21条2項所定の要件の充足性の確認を経ることとされており、情報の授受等に関する記録が一定期間保存されて、本人はその開示等を求めることができる。のみならず、上記の場合、システム技術上、インターネットから切り離された行政専用の閉域ネットワーク内で、個人番号を推知し得ない機関ごとに異なる情報提供用個人識別符号を用いて特定個人情報の授受がされることとなっており、その通信が暗号化され、提供される特定個人情報自体も暗号化されるものである。以上によれば、上記システムにおいて特定個人情報の漏えいや目的外利用等がされる危険性は極めて低いものということができる。

さらに、個人番号はそれ自体では意味のない数字であること、情報提供ネットワークシステムにおいても特定の個人を識別するための符号として個人番号が用いられていないこと等から、仮に個人番号が漏えいしたとしても、直ちに各行政機関等が分散管理している個人情報が外部に流出するおそれが生ずるものではないし、前記第1の2(2)アのとおり、個人番号が漏えいして不正に用いられるおそれがあるときは、本人の請求又は職権によりこれを変更するものとされている。

これらの諸点を総合すると、番号利用法に基づく特定個人情報の利用、提供等に関して法制度上又はシステム技術上の不備があり、そのために特定個人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。

4 そうすると、行政機関等が番号利用法に基づき特定個人情報の利用、提供等をする行為は、個人に関する情報をみだりに第三者に開示又は公表するものということとはできない。したがって、上記行為は、憲法13条の保障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を侵害するものではないと解する



のが相当である。また、以上に述べたところからすれば、被上告人が番号利用法に基づき上告人らの特定個人情報の利用、提供等をする行為は上告人らのプライバシー権を違法に侵害するものであるとする上告人らの主張にも理由がないものというべきである。

以上は、当裁判所大法廷判決（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）の趣旨に徴して明らかである。論旨は採用することができない。

第3 その余の上告理由について

論旨は、違憲をいうが、その前提を欠くものであって、民訴法312条1項及び2項に規定する事由のいずれにも該当しない。

よって、裁判官全員一致の意見で、主文のとおり判決する。

最高裁判所第一小法廷

裁判長裁判官	深	山	卓	也
裁判官	山	口		厚
裁判官	安	浪	亮	介
裁判官	岡		正	晶
裁判官	堺			徹

令和4年(才)第39号

令和3年(ネ才)第117号 上告提起事件

上告人 外10名

被上告人 国

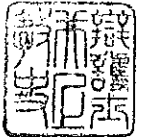


上告理由書

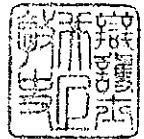
2021(令和3)年12月9日

最高裁判所 御中

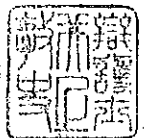
上告人ら訴訟代理人 弁護士 山本 一行 代



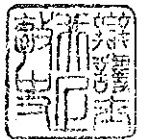
同 武藤 糾 明 代



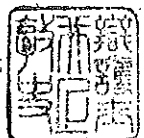
同 池 永 修 代



同 井 上 敦 史



同 梅 野 晃 平 代



同 馬 場 勝 代



第1	はじめに	4
1	1995年以降、2000年代までのデジタル社会の進展	4
2	2010年代以降のデジタル社会の進展	8
3	デジタル庁はどこへ向かうのか。	9
4	顔認証システムの活用	11
5	プライバシーを保護しても、デジタル社会は実現可能である。	15
第2	自己の個人情報についての権利・自由に関する憲法13条の解釈の誤り（民 訴法312条1項）	17
1	原判決の判示	17
2	原判決は現代社会における情報管理技術に全く対応しようとしていない。	17
(1)	コンピューターによる情報管理の特徴、危険性	17
(2)	プロファイリングの問題性	17
(3)	個人番号制度は民間利用、拡大が予定され、実施されていること	22
3	番号利用法における個人情報の収集等が具体的危険にさらされていること	22
(1)	法制度上の不備について	22
(2)	システム技術上の不備及び事故事例について	24
(3)	小括	26
4	小括	26
第3	違憲審査基準に関する憲法解釈の誤りについて	27
1	原判決の判示内容	27
2	プライバシー権にかかる違憲審査基準	28
3	本件で採用されるべき違憲審査基準	30

4	原判決の認識の誤りについて	32
5	原判決の違憲審査の具体的危険の判断の誤り	33
第4	平成20年最高裁判決の判断枠組みに照らせば個人番号制度の違憲性は明らかであること	36
1	一審判決及び原判決の判断	36
2	個人番号制度は住基ネット制度と根本的に異なること	37
(1)	根本的な相違点	37
(2)	両制度の根本的な相違点がもたらす危険性の飛躍的増大	40
(3)	小括	41
3	平成20年最高裁判決の考慮要素に照らした個人番号制度の評価	41
(1)	平成20年最高裁判決の概要と考慮要素	41
(2)	平成20年最高裁判決の考慮要素を比較検討すれば個人番号制度は違憲であること	43
第5	憲法41条に関する原判決の憲法解釈の誤り	45
1	総論	45
2	憲法41条の意義と委任立法	46
(1)	憲法41条の意義	46
(2)	委任立法とその限界	46
3	憲法適合性の判断基準	47
(1)	判例の概観	47
(2)	憲法適合性の判断基準	48
4	特定個人情報の意義と要保護性	48
5	他の国家機関への委任に合理的必要性がないこと	49
(1)	総論	49
(2)	個人番号制度における番号利用法19条の重要性	50
(3)	個人番号制度が採用する特定個人情報の取扱いについての基本姿勢	50

(4) 結論	51
6 番号利用法19条14号の規定が白紙委任であること	53
(1) 番号利用法19条14号の規定	53
(2) 「公益上の必要があるとき」が指導制約指針たりえないこと	53
(3) 同号の例示が指導制約指針たりえないこと	54
(4) 結論	54
7 番号利用法19条16号の規定が白紙委任であること	54
(1) 総論	54
(2) 個人情報保護委員会への委任に合理的必要性がないこと	55
8 番号利用法施行令25条・別表各号が委任の範囲を逸脱していること ...	56
(1) 総論	56
(2) 各論	57

第1 はじめに

1 1995年以降、2000年代までのデジタル社会の進展

私たちは、否応もなく、デジタル社会の中で生きている。現状を直視し、十分な認識がなければ、プライバシーの現代的な意義を正しく理解することは難しいと思われる。そのため、1995年のウィンドウズ革命後のデジタル社会の進展を論じた上で、現代におけるプライバシーの意義を冒頭に述べることにしたい。

代理人の1名である筆者は、1994年の司法試験に合格した。研修所に入る前に、同じ年に合格した受験仲間からパソコンを借り、ワープロ入力の練習を行った。この当時、ウィンドウズはバージョン3.1であり、簡単な英単語を入力してコマンドを行う形式だった。

研修所に入った1995年の秋、実務修習中に、ウィンドウズ95が発売さ

れた。素人でも簡単に操作ができるようになり、それまで日本で主流だったパソコン通信から、インターネットによる情報流通へと転換が起り始めた。1997年実施の研修所の卒業試験の小論文でも選択問題の一つとして「インターネット社会」という1行問題が出された。

2000年頃までは、日本のインターネット環境は牧歌的なもので、例えばヤフーでキーワード検索をかけてみても、その結果が2頁とか3頁しか表示されないと言うことも多かった。少し先進的な人が使用するメディアという感じで、逆に言うと、現在のように誰も彼もが写真や動画をアップロードするようなことはなかった。パソコンや、インターネットで取り扱うことのできる情報量は、年々飛躍的に伸びており、草創期は画素数を減らした静止画像を送信するだけでも相当な時間がかかっていたのである。

それでも、世界中の人と囲碁や将棋を楽しめたり、コミュニケーションをとれるようになったという点で画期的な変化が訪れた。文字媒体での情報発信は容易になり、ブログが世界中で開設され、それまで情報の受け手の立場に甘んじていた一般市民が情報の発信者となり得る状況となった。また、インターネットメールが主な通信手段の地位を築き始めた。情報の発信が自由になることの利便性は、名誉毀損やプライバシー侵害の深刻さという副作用も伴うものであった。2ちゃんねるという掲示板ができ、匿名による誹謗中傷などが横行したが、発信者が特定できずに削除請求も困難となり、泣き寝入りを強いられる事件が絶え間なく起こるようになり、プロバイダ責任制限法は制定され、改訂されたが、被害回復の困難さは現在まであまり軽減されていない。

プライバシーが、デジタル社会の文脈で真剣に検討されるようになったのは、2001年の9.11テロが起こった後である。通常は普通の市民として生活をしているのに、突然有事になるとテロ行為を行う「スリーパー」と呼ばれるテロリスト予備軍を、インターネット上で探し出す必要があるという、犯罪が起こる以前における「犯罪予防」の行政警察領域であった。例えば、爆弾の作

り方を教えるホームページが作成され、そこにアクセスしたものを割り出し、データベースを作成して監視対象とするなどの活動がなされるようになり、どのような条件であればどの程度許されるのかなどが議論になった。

ドイツでは、テロの恐れがあるものへの電話盗聴を認める予防的監視を認めたニーダーザクセン州警察法33a条は、予防的領域における具体的危険について予測可能性、統制可能性を担保できる「規範特定性・明白性」に欠けるとして、連邦憲法裁判所は、2005年7月27日、基本法10条に違反し違憲無効とする判決を出した。

また、「若い独身男性、アラブ圏出身、正規ビザを有する、技術系」など、実行犯に共通する要素と考えられたものについて、多様な機関に対して、例えば大学なら「氏名、誕生日、出生地、国籍、住所、宗教、専攻、閲覧した本、集会参加歴など」、クレジットカード会社や交通機関に関しては利用履歴などの情報収集を行うことができる「スクリーニング捜査」が各州警察法で定められた。令状による収集が要件とされていたノルトラインヴェストファーレン州では、人口1600万人のうち、実に450万人もの情報が収集された。連邦憲法裁判所は、連邦または州の存立もしくは安全、または個人の身体、生命もしくは自由に対しての具体的危険が存在する場合にしか認められないところ、危険が抽象的にとどまる段階で予防的に行うことは認められないとして、2006年4月4日、ノルトラインヴェストファーレン州警察法31条を違憲とする判決を出した。

これらの違憲判決の基礎にあるのは、国勢調査の際に国民に付された番号が、どの範囲での個人情報と結合するのかが限定されないまま施行されようとした国勢調査に対し、憲法異議が出され、これを違憲とした連邦憲法裁判所の1983年12月15日付け国勢調査事件判決である。同判決は、以下のように指摘し、情報自己決定権を憲法上の重要な人格権として保障した。

「逸脱した行動が、常に記録され、情報として永続的に蓄積され、利用され、

伝達されることに不安を抱くものは、そのような行動によって目立つことを控えようとするであろう。このことは、個人のそれぞれの発展の機会を妨げるだけではなく、公共の福祉を害する。なぜなら、自己決定は、市民の行動及び共同能力に基づく自由で民主的な国家共同体の基本的な機能条件であるからである。」(以上、2007年11月1日日弁連人権擁護大会シンポジウム第1分科会基調報告書「市民の自由と安全を考える—9.11以降の時代と監視社会—」より)

どこまでの自分の情報が結合させられるのかを確実に見通せないような自己情報の収集・利用・提供は憲法違反であるという明快な論理であり、これをプライバシー権と呼ぶか、自己情報コントロール権と呼ぶかはともかく、我が国においても憲法上保障されている重要な人格権である。

なお、2007年6月6日に、筆者らが連邦憲法裁判所に聞き取りに伺った際、スクリーニング捜査事件判決の主任であったホフマン＝リーム連邦憲法裁判所副長官がふらりと現れ、以下のコメントを残された。

「2001年9月11日以降のテロ対策を求める政治的な圧力が強い中で、法治国家という立場を保つことは大変難しいことだ。

憲法は長い期間にわたって使われるものであり、変更を安易にするものではない。解釈についても一時的な問題で変更を加えることは困難である。

通信に関する民間企業が保有する通信内容や、ソフトウェアを用いて知ることのできる商品の購入歴などのデータを国家に受け渡すような法律ができる可能性がある。このような法律ができることは、市民的自由に対する脅威となる。」

2008年2月27日、連邦憲法裁判所は、諜報機関である州憲法擁護庁に対し、インターネット経由で対象者の記録媒体に密かに侵入し、データを収集する監視手法を認めた州法を違憲無効とする判決を下した。この判決では、情報技術システムの機密性と不可侵性の保障に対する基本権（IT基本権）が一

般的人格権に含まれることを前提とし、これを秘密裏に侵すことができるのは、極めて重大な法益に対する具体的危険の現実的根拠が存在する場合だけであり、その場合も原則として裁判官の令状の留保のもとにおかれるべきであり、中核領域を守る予防措置が執られていなければならないなどとした。

2 2010年代以降のデジタル社会の進展

2010年代に入ると、我が国でもスマートフォンの普及が著しくなった。インターネットへのアクセスは、現在では、PCからよりスマートフォンからの方が多くなるなど、インターネット通信量の飛躍的な増大だけでなく、その手段も変化している。撮影した写真や動画をすぐにアップロードすることができ、スマートフォンと親和性の高いツイッター、フェイスブック、インスタグラムなどのSNSが飛躍的に普及したのも2010年代の際だった特徴である。

若い世代では、テレビ視聴よりユーチューブ等のインターネット動画視聴の時間が上回ると報道されている。企業が支出する宣伝広告費も、新聞やテレビに対するものより、インターネットに対するものの方が上回るようになった。端末利用者の検索キーワードやホームページ等の閲覧履歴に応じた、興味関心事項に連動して表示される行動ターゲティング広告の有効性が周知のものとなり、営業活動を行う企業側からすると、従来より3割程度少ないコストをデジタルプラットフォームに支払うだけで、従前と同様の売上が上がるようになってきている。

いまや私たちは、デジタル社会の中に組み込まれた生活をしている。

もちろん、デジタル社会は私たちの生活に大きな利便性をもたらしている。一度ユーチューブの動画を視聴すると、「この動画を見た人はこんな動画を見えています」と言って、関心のありそうな動画をおすすめしてくれる。あるいは、アマゾンで商品を購入すると、「この商品を購入した人は、こんな商品を購入しています」と言って、関心のありそうな商品をおすすめしてくれる。

しかし、他方で、デジタル社会の基盤を提供しているデジタルプラットフォームは私たちのプライバシー情報を大量かつ容易に収集・分析・利用するため、検索キーワード、閲覧した記事やユーチューブチャンネル、GPSをオンにしていることにより蓄積されていく移動履歴など、当の本人は到底覚えておくことの不可能な遙か以前から現在に至るまで、そして近い将来の行動予測まで、記録し活用し、収益を上げている。アメリカでは、フェイスブックにつけた「いいね」の選択を分析するだけで、高い確率で人種、宗教、支持政党を推測できると指摘されるようになった。分析対象となる「いいね」の数が増えると、同僚や友人、配偶者よりもその人の人格を正しく補足できるとされている。

利用者の利便性は、自分の好みの商品や動画・サービスなどをお勧めしてもらえらること、企業の利便性は、宣伝広告費を3割減らし、経費節減を果たしたことが主なものである。これらに対して、利用者である市民が失ったものは、その興味関心に基づく行動履歴、購入履歴、検索履歴、視聴履歴など、全人格的なプライバシー情報にまで及んでいる。そこに果たして利用者のプライバシーとの比例性が保たれ、同意原則が守られているといえるだろうか。

3 デジタル庁はどこへ向かうのか。

本年成立したデジタル改革関連法案に基づき、本年9月1日にデジタル庁が発足した。

官民を横断するデジタル社会の進展、データの利活用が図られようとしている。

しかしながら、前項で検討したとおり、2010年代以降に明らかになってきた、デジタルプラットフォームによる自由自在なプライバシー情報の利活用は、主権者の幸福に資するとは限らない。また、民間事業者によるプライバシー情報の利活用が、主権者のコントロールがきかないほどのプラットフォームの権力の肥大化につながったという問題点を考えると、公権力主導で同様の仕組みを目指す場合には、そもそもそのような進め方が妥当であるのかも含

め、さらに検討されるべき問題点は大きいものと思われる。

デジタル社会の実現に向けた重点計画（2021年6月15日、高度情報通信ネットワーク社会推進戦略本部、官民データ活用推進戦略会議）によれば、デジタル社会の形成に向けた基本的な施策の冒頭に「マイナンバーカードの普及、マイナンバーの利活用促進」が掲げられ、以下の項目が挙げられている。

① マイナンバーカードの普及

ア マイナンバーカードの健康保険証としての利用

イ 運転免許証との一体化

ウ 在留カードとの一体化

エ マイナンバーカードの国外継続利用

オ マイナンバーカードのマイナンバーカードの電子証明書の円滑な発行・更新等

カ 全業所管官庁等を通じた計画的な取組

② マイナンバーカードの利活用促進

ア マイナンバーを利用した情報連携

イ 公金受取口座の登録・利用及び預貯金付番の円滑化

ウ 各種免許・国家資格等のデジタル化

エ 養育費の支払い確保

また、「デジタル社会の形成に向けた基本的な施策」の2番手に掲げられている「徹底したUI・UXの改善と国民向けサービスの実現」には、冒頭に「マイナポータルの抜本的改善」との項目が掲げられており、やはりデジタル庁が目指すデジタル化の中心は、マイナンバーカードが根幹をになっているものと強く示唆される。

2015年に、「マイナンバー制度利活用推進ロードマップ（案）」が公表された。広く国民に周知されたとはいいがたいが、その中では以下の未来予想図が掲げられていた。

2017年から2019年にかけての目標として、マイナンバーカードについて、「ワンカード化の促進」の名の下に、「個人番号カードをデビットカード、クレジットカード、キャッシュカード、ポイントカード、診察券などとして利用⇒ワンカード化の促進⇒スマホ等のデバイスにダウンロードして代用できるよう研究・関係者との協議の上実現」、2018年の目標として、「番号制度見直し(利用範囲の拡大)」「戸籍制度見直し」「個人番号カードと運転免許証の一体化」「個人番号カードと医師免許との一体化」「個人番号カードと教員免許との一体化⇒教員資格の確認 更新忘れ対策が容易に」「学歴証明(卒業証明書)」「健康保険証オンライン資格確認(4月目途)⇒個人番号カードを健康保険証として利用」、2020年の目標として、「個人番号カードもスマホも持たずにあらかじめ本人確認の上登録した生体情報で代用も可能に!」「全国民が個人番号カードを保有できる⇒すべての国民が安心安全にネット環境を利用できる権利を有する世界最先端IT国家へ!」が掲げられている。

果たして、私たち主権者は、このような広範なプライバシー情報の名寄せを前提とするワンカード化を希望しているのだろうか。健康保険証や運転免許証との一体化、および既存の健康保険証の廃止(「将来的に保険証の発行を不要としてマイナンバーカードのみの運用への移行を目指していく」という厚労省・オンライン資格確認等システムに関する運用等の整理案(概要)令和元年6月版)という政府の強い政策誘導からは、医療機関を受診する可能性のある市民は、例外なく個人番号カードを保有する以外に選択の余地がなくなる恐れがある。しかもそれは2022年度中に実現することが目標とされている。

これは、私たち主権者が自ら選択したデジタル社会の第一歩だろうか。

また、その後に政府が想定している未来予想図は、私たち主権者が自ら望んでいる姿だろうか。事実上の強制に至る蓋然性が高いが、上告人らのように、望まない市民に対するプライバシー権侵害ではないのだろうか。

4. 顔認証システムの活用

また、個人番号カードには、指紋の1000倍と言われる高度な本人確認機能を有する顔認証データの収集・利用が不可分一体とされている問題点がある。健康保険証機能を活用する場合、医療機関に導入されたカードリーダーで、受診者の個人番号カードのICチップに埋め込まれた顔画像データから生成される顔認証データと、本人の顔画像とを、カードリーダー内蔵のカメラでチェックし、同一人であることを判断してから受診させるよう指導されている。

しかしながら、顔認証データが高度な本人確認機能を持つことから、GDPR（欧州一般データ保護規則）9条1項は、顔認証データを典型とする生体情報の原則収集禁止を掲げ、同2項及び3項の例外は、生命に関する利益を保護するために必要な場合やEU法または加盟国の内国法による定めが存在し、重要な公共の利益を理由とする取り扱いが必要な場合などに限定され、民間事業者の収集・利用には議会による法律制定が必要とされている。日本弁護士連合会も、2012年、2016年に加え、本年も顔認証システムの利用に対する制限立法を求める提言を繰り返しているが、今なお存在しない上、逆に全国民に対し、顔認証システムの利用が強制されかねない情勢となっている。

顔認証システムの導入は正確な個人の識別を可能とすることから、誤認可能性の著しい低下と導入コストの低下などにより利用者は急激に増えている。個人の住宅、マンション、企業内・行政機関内の一定区域などにとどまらず、大阪のUSJ、成田空港、新宿の書店、東京駅など公共性の高い場所での設置も広がっている。「安全・安心」「防犯」「利便性」など誰もが歓迎するような設置目的になっていることから、この流れは今後さらに加速するだろう。しかし、顔認証システムは、個人を識別するデータを記録しいつでも利用できるようにすることが可能であるが故に、設置の仕方、利用の仕方によっては誰の行動も記録し、リアルタイムで追跡し、過去に遡って確認することもできる。見ず知らずの者に自分の行動や生活状況を見張られ続ける状況が起りかねない。これは究極のプライバシー侵害であり、思想良心の自由、信教の自由、表現の自由

に対する侵害、総体としての人格権の否定、つまりあらゆる自由人権の否定につながりかねない。

中国では、6億台の顔認証機能付きの街頭監視カメラにもとづき、住民全員の個人情報データベースとの検索がなされている。街角で行った交通違反で減点され、直ちに罰金が科されたり、政治犯が逮捕されたりしている。海外メディアの実証実験によれば、場所を明らかにせずに公共空間に現れたターゲットを、当局が特定するまでに要した時間はわずか7分であったという（2021年9月18日福岡県弁護士会主催シンポジウム「デジタル社会と監視を考える」におけるジャーナリスト倉澤治雄氏の講演による）。人権に十分な配慮を行わないまま、顔認証システムが全面的に社会で実用化されることには計り知れない闇があるといわねばならないだろう。

このような重大な問題を孕んでいることが明らかであるにもかかわらず、我が国では未だに顔認証システムの利活用に関する法的規制がない。防犯カメラの設置規制の法律さえない。

デジタル改革関連法には、個人情報保護法制の大改正も含まれており、そこでは、国法である個人情報保護法より住民のプライバシーを保護するために先に成立し、センシティブ情報の収集制限など、前述したGDPR 9条にも関連する、手厚く住民のプライバシーを保護するための条文も含まれていた条例が、国法並みのプライバシー保護で足りるとして、保護水準が切り下げられる懸念がある。

もともと、住民基本台帳ネットワークシステムは、市区町村の基礎的地方自治体が保有している、正確で最新の住民の居住状況を国家行政事務が可能な限り自由に捕捉するための制度設計と、住民のプライバシー保護を図るため必要のない国家行政事務への提供を防止するための制度設計がせめぎ合ったシステムであった。

利便性や行政の効率化を優先するデジタル社会においては、主権者のプライ

プライバシー保護はたえず後方に退く危険がある。)自衛隊適齢者情報の提供に関する基礎自治体の慎重姿勢が次々と変化している昨今の情勢を考え合わせると、デジタル改革関連法は、全体として住民のプライバシー保護機能を有する中間団体であった地方自治体のバリアを破壊して、国家による住民情報の直接の捕捉につながる懸念も否定できない。

個人番号制度(原判決では「番号制度」と表記しているが、「番号制度」には納税者番号等、他の番号における制度も含むため、本書面では「個人番号制度」と表記する。)は、当初の税・社会保障制度のための手段という位置づけから、行政効率化が目標とされ、必ずしも税・社会保障と関連性のない国家行政事務にまで個人番号の利用が政令への委任により開かれている。また、直接個人番号を媒介として情報を連携するわけではないとしても、個人番号カードを通じた民間事業者におけるデータベースの作成には制限がない。

しかし、利便性・効率性というデジタル化の光の部分だけを強調し、その障害となり得るプライバシー保護の要請を後景に退かせる制度設計においては、情報主体である私たち主権者は、国家行政機関や民間事業者からデータを収集・分析・利活用されるただの客体に成り下がる恐れすら否定できない。それは、我が国ではアメリカほど発達しなかった強力な情報権力者であるデジタルプラットフォームを、あたかも公権力主導で一から立ち上げ、官民一体となつてのプライバシー情報の利活用一辺倒による経済発展のみを指向していくかのようである。このようなシステムの近い将来では、本来の主権者である1人1人の市民の自己決定や自己実現を萎縮させる恐れすらある。

利便性・効率性の優先ではなく、あらかじめ必要なプライバシー保護措置を事前に埋め込んだ制度設計によるデジタル社会の設計図がなければ、その後の世界は、プライバシー保護のない社会にならざるをえない。仕組みが動き出す前に、設計図にプライバシー保護のための必要な施策をすべて事前に埋め込まなければならない。

本件訴訟において、住基ネット訴訟最高裁判決をもとに審査を行う場合、このようなプライバシー保護措置が十全であるかという厳格な検討を個人番号制度全体に対して慎重に行う内容であるべきである。

それは、1995年以降、さらには2010年代以降の革命と呼ぶべきデジタル社会化、個々人の行動履歴、移動履歴等が民間事業者に過ぎないデジタルプラットフォームの手のひらの上で完全に把握されているという現実、同様の仕組みが我が国で官民一体として作り上げられかねないという現実を前提とした、実効性のあるものでなければならない。

ドイツ連邦憲法裁判所は、現実的要請から安易にプライバシー侵害的な政策がとられることに対し、決して妥協することなく、絶えず憲法の番人としての自らの使命を全うする判断を行い、市民のプライバシー権を毅然として保護し続けている。そのような姿勢が、市民から高く評価されている。

私たち市民も、このような最高裁判所の審査を求めている。

5 プライバシーを保護しても、デジタル社会は実現可能である。

世界的に技術導入に重点が置かれがちで、住民自治の観点が切り捨てられがちなかデジタル化の中で、バルセロナは2015年に「スマートシティのインフラを民主化する」というゴールを掲げ、市民が市政に参加するためのプラットフォーム「デシディム」(カタルーニャ語で「私たちが決める」の意味)づくりから始めた。市の予算の一部に市民が提案する政策に配分する「参加型予算」を設置し、市民の提案する政策に従い、市議会での議論を経て配分されるように変化した。その結果、市内のビルの屋上に農園を作る政策など約1500もの提案が市議会で採択されている。我が国でも兵庫県加古川市や横浜市の一部地域で同様の試みがなされている。

また、EUでは、デジタルプラットフォームへの対抗戦略として、2017年に欧州委員会がDECODE (Decentralized Citizens Owned Data Ecosystem: 脱中央集権・市民所有型データエコシステム) プロジェクトを始めた。これは、

オンライン上で生成される個人情報の蓄積・管理、運用に関して、市民自らが個人データの秘匿や共有をコントロールできるようにする仕組みである。例えば、自分の移動データについて、公共交通機関には開示するが、保険会社や広告会社には非開示にするというように自分の意思によって選択できる。その際の大原則は、「個人データは企業や政府のものではなく、それを持つ人自身のものである」という「データ主権」の思想であるとされる。バルセロナ市 CTO のブリア氏は、「テクノロジーの世界では、シリコンバレーの監視資本主義や、ディストピア的な中国のモデルとは異なる物語を提唱することが非常に重要です。私たちはヨーロッパをリードして、代替モデルを提唱したいのです」と語っている（以上につき、「人々による人々のためのデジタル社会へ」内田聖子、雑誌世界 2021年4月号）。

我が国のデジタル化は、すべて内閣官房が設計図を描き、市民はただその客体に過ぎないという前提で着々と進んでいる。もし、日本も民主主義国家であるのならば、例えば EU やバルセロナ市のように、主権者自身が自らの「情報主権」に目覚め、公権力や民間事業者に対しても、自らの移動履歴・行動履歴を誰には提供してもいいが、誰には提供したくない、という自己情報の提供に関する自己決定権を行使できるべきであり、その不可欠の前提として、まずその設計図の作成に主体的に参加できるべきではないだろうか。

私たち自身が自分たちの頭で考え、自分たちの最大の幸福に資するような、プライバシー権、自己情報コントロール権の観点からも望ましい主権者による情報主権が全うされた自律的なデジタル社会の実現を目指すべきではないだろうか。自由権に対する制限であるにもかかわらず、行政機関の広範な裁量での制限を任せることの可能な憲法上の根拠を見いだすことは困難ではなからうか。

民主主義国家においては、過度に人権を制約する内容の立法が行われても、それで終わりではなく、司法審査による是正が可能とされている。市民のプラ

プライバシー権を毅然として保護しうるのは司法の重要な機能である。憲法の番人として、プライバシー権を保護する機関にふさわしい審査を求める。

第2 自己の個人情報についての権利・自由に関する憲法13条の解釈の誤り（民訴法312条1項）

1 原判決の判示

原判決は、「憲法13条は、・・・何人も、個人に関する情報について、同条が保障する権利の内容は、それをみだりに第三者に開示又は公表されない自由と解するのが相当である」と判示する（原判決書14頁）。

2 原判決は現代社会における情報管理技術に全く対応しようとしていない。

しかし、このようにプライバシー権を狭く解するのは、コンピューターによる情報管理技術が進んだ現代社会には、全くそぐわない。

(1) コンピューターによる情報管理の特徴、危険性

コンピューターによるデジタル化された情報管理技術によっては、膨大な量の情報を管理することができるようになった。これらは半永久的に劣化することなく保存ができる。また瞬時に複製ができ、複製は無限に可能である。爆発的に増殖された情報は、いとも容易に伝達でき、爆発的に増殖させることができる。複製が行われたことは容易にはわからず、伝達先を把握することもほとんど不可能である。書き換えも容易であり、書き換えられたことはきわめてわかりにくい。

いったん情報が収集されると、拡散、漏えいを止めることはきわめて困難であり、拡散、漏えいされると、そのことによるプライバシーの侵害はきわめて深刻なものとなってしまふ。

現代社会においては、プライバシー権は上記のような危険が十分理解され、その危険が回避できるようなものとして構成されなければならない。

(2) プロファイリングの問題性

これら危険は、プロファイリングが可能になることによって増すことになる。

ア プロファイリングとは

GDPR（EU一般データ保護規則）は、プロファイリングを「自然人に関する特定の個人的側面を評価するために、特に、当該自然人の職務遂行能力、経済状況、健康、個人的選好、関心、信頼性、行動、位置もしくは動向を分析または予測するために、個人データを用いて行うあらゆる形式の自動化された個人データ処理」と定義している（甲98・257頁）。

イ 現代的なプロファイリングの特徴

プロファイリングという手法は、これまでもなかった訳ではない。しかし、現代的なプロファイリングはビッグデータを瞬時に機械的に分析して行うもので、それゆえアマゾンのような世界的マーケットを有する組織であっても、全世界の顧客に対して対処できているのである。そして、このような分析は、アマゾンに限らず、ビッグデータを保有する主体において日常的に行われている。そこで、まずはその現代的なプロファイリングの特徴をみておくこととする。

① データ量

プロファイリングに用いられるデータの量が、従前から存在した古典的なプロファイリングとは、桁違いに大きい。

② 自動性

従来は、複数のデータから、人間が、経験則や勘を頼りに対象者の個人的側面を予測していたが、現代的プロファイリングにおいては、コンピューター上で自動的に対象者の個人的側面を予測する。

③ 科学的信憑性

豊富なデータ量と人間の直感を排した自動的処理によって行われるため、一般に結果に対する科学的信憑性が高くなる。このため、対象者が、

プロファイリング結果を否定し、その評価を覆すことは困難になる。

④ 意外性（予見困難性）

世界的規模で収集され、プールされる大量のデータから、人間が想像できないような事物の相関関係が明らかになることがある。

例えば、アメリカの小売業者であるターゲット社は、無香料性ローションの購入履歴、特定サプリメントの購入履歴、大きめのバッグの購入履歴など、一見妊娠とは関連性が明らかでないデータによって、顧客の妊娠の有無をプロファイリングして、ベビー用品の広告を行っていた。

⑤ 項目の広範性・細目性

前述のターゲット社は、上記データ解析から、妊娠の有無だけでなく、出産予定日までも予測していた。現代的プロファイリングにおいては、大量のデータを自動的に高速処理できることから、対象項目が拡張し、相当に細かい個人的事項までも、予測・評価できるようになってきている。そして、それは妊娠や出産予定日といった極めてセンシティブな情報までもが対象とされているのであり、驚きを禁じ得ない。

ウ 現代的プロファイリングの利用場面

前述のアマゾンのレコメンド機能やターゲット社以外のケースでも、以下に示すような現代的プロファイリングの具体例は多数存在する。

① 警察による犯罪予防のための犯罪者予測

シカゴ警察では、例えば「殺人の犠牲者を知る者が自らも殺人に巻き込まれる可能性は通常の9倍である」というような経験的データから、暴力犯の実行者と犠牲者を予測するアルゴリズムを構築し、潜在的な暴力犯実行者等をリスト化して、警告や社会的サービスの告知等を行なっている。

近年は、潜在的な重罪犯罪者を「合理的な正確性」をもって予測するアルゴリズム、仮釈放中の者が殺人に関与するかどうかを予測する

アルゴリズム、児童虐待を行なう家族を予測するアルゴリズム等が構築されている。

② ネット配信のニュースの提供側からの取捨選択

ネットを通じて配信されるニュースは、プロファイリングにより予測された当該ユーザーの政治的信条や個人的選好等を前提に選択的に配信されていることが少なくない。

当該ユーザーの関心に合っていないと（確率的に）判断された情報はフィルタリングされ、その選好に合っていると（確率的に）判断された情報のみ自らが取込まれる状態が生じる。すなわち当該ユーザーの見たい景色（ニュース）だけが提供され、見たくない景色（ニュース）は提供されない。このようにことが続けば、ニュースの配信側はユーザーの思考をある程度コントロールできてしまうことになりかねないであろう。

③ 選挙運動での利用

プロファイリングによって、有権者本人に直接尋ねることなく、非政治的な個人データを含む多様な情報から迂回的に、一定の正確性をもって、信条や支持政党等に関する政治的プロファイルを構築し、選択的で効率的な選挙運動を行なうことができるようになっている。

④ アメリカの実験では、フェイスブックで何に「いいね」ボタンを押したかを集積・分析しただけで、そのユーザーが白人であるか黒人であるかを95%の確率で、男性であるか女性であるかを93%の確率で、民主党支持者であるか共和党支持者であるかを85%の確率で、キリスト教信者であるかイスラム教信者であるかを82%の確率で正しく分類できるとされている（甲99・146頁）。

エ 現代的プロファイリングとプライバシー保護

個人の私生活をのぞき見することは、古典的なプライバシー概念に照ら

しても、プライバシー権の侵害にあたることに争いはないであろう。

とすれば前述のように妊娠の有無のようなセンシティブな私的事項を、本人の同意なく、アルゴリズムによって自動的にプロファイリングすることは、プライバシー権を侵害するといっているのではないか。少なくともプライバシー権の保護との間に厳しい緊張状態をもたらしていることに疑問の余地はないであろう。

山本龍彦教授（慶應大学）は、このような事態をプライバシー権の侵害と捉え、かつセンシティブな事項を一定の精度で予測するプロファイリングは、少なくとも改正個人情報保護法17条2項のいう要配慮個人情報の「取得」に該当し、本人の事前同意がない限り、同条違反を構成すると考えるべきであるとしている（甲98・266頁）が、非常に説得的といえよう。一般的な非センシティブな個人情報等を集積してプロファイリングすることで、迂回的であれ、容易かつ瞬時に要配慮個人情報にアクセスできてしまうのであるから、ここに法的規制を及ぼそうという考えは、プライバシー権の保護の観点からは不可欠であるからである。

また、現代的プロファイリングが普通に行われている社会においては、情報の種類にもはや差異を設けることはできない。いかなる個人情報も、他の情報と併せることによってプロファイリングの材料になり得るのである。

それに加え、プライバシー権の保護のためには、膨大な個人情報を収集、管理する主体に対する法的規制の必要性を自覚的に意識する必要があるということである。というのも、一般的な非センシティブな個人情報等を集積してプロファイリングすることで、容易かつ瞬時にセンシティブな個人情報に到達することが可能なのは、ビッグデータを収集、管理する主体に限られるのであり、その主体が自由にデータマッチングや分析を行いうる状況を放置すれば、本人の同意のないままセンシティブな情報に到達し、

事実上私生活をのぞき見ることが可能となるからである。つまり、プライバシー権保護のための現代の課題は、もはや情報漏えいの危険の防止ということから、情報の管理、利用の方法をどのように規制し、データ管理者が情報主体の私生活をのぞき見することをどのように防止していくのかにシフトしているといえる。もちろん情報漏えいさせないことも、それはそれとして重要な課題ではあるが、それだけで必要十分ということではなくなっているということである。

GDPR（EU一般データ保護規則）は、このことを明確に意識し、プロファイリングの問題をビッグデータ社会における個人情報・プライバシー保護法制の中核に据えている。GDPRの試みは、現代社会におけるプライバシー権の保護の実効性の確保、ひいては我が国憲法13条のプライバシー権をどのように捉えなければならないかについて、重要な示唆を与えている。

(3) 個人番号制度は民間利用、拡大が予定され、実施されていること

この点については本書面の冒頭に述べたとおりである。

個人番号カードは保険証や運転免許証と一体化されるなどして、事実上強制されようとしている。また、個人番号カードが本人確認の手段とされ、それが種々の情報に紐付けられており、それが拡大されようとしている。顔認証システムとも連動され、ますますプライバシーにとって危険なものとなろうとしているのである。

3 番号利用法における個人情報の収集等が具体的危険にさらされていること

(1) 法制度上の不備について

ア 特定個人情報の提供等について（番号利用法19条14号及び16号）

番号利用法19条14号及び16号の規定が白紙委任であり、無限定に特定個人情報の提供が許容されることになることについては、後述のとおりである。

「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、行政が立法者の意図しない目的に特定個人情報を利用すること（目的外利用）が可能となっているものであり、個人番号及び特定個人情報の提供等が制限されておらず、法制度上の不備があるといわざるを得ない。

イ 特定個人情報保護評価制度

特定個人情報保護評価において明確に禁止されていたにもかかわらず、年金機構などで業務の再委託がなされていたことは、争いのない事実である。

ここで問題となるのは、禁止されていた業務の再委託がなされていたことであり、再委託の発覚後に個人情報保護委員会が監督権限を行使したか否かではない。

禁止していることを容易に実行できるような特定個人情報保護評価は、評価たり得ないのである。

したがって、かかる点においても法制度上の不備があるといわざるを得ない。

ウ 個人情報保護委員会による監視・監督等

個人情報保護委員会の所管事務と組織の実態に照らせば、到底有効な監視をなし得るとは考えられない。

また、個人情報保護委員会の権限は、番号利用法施行令34条に掲げる場合については適用除外とされていることから（番号利用法36条）、個人番号制度が目的とする税、社会保障、災害という3つの利用分野以外の分野における個人番号の取扱いに対して、個人情報保護委員会の権限が及ばないことになる。

したがって、かかる点においても法制度上の不備があるといわざるを得ない。

エ 罰則

確かに、罰則によって不正行為や違反行為の完全な抑止を期待することは困難である。

だからこそ、罰則によって、不正行為や違反行為の危険性をなくすことはできず、有効性が低いものである。

したがって、かかる点においても、個人番号の取得が大きな経済的利益に結び付き得ることも併せ鑑みると、法制度上の不備があるといわざるを得ない。

オ 個人番号カード

個人番号制度において個人番号カードの利用拡大が図られており、実際に現在利用範囲が拡大している最中である。

そして、個人番号カードの裏面には個人番号が記載されていることから、個人番号カードの利用が拡大されればされるほど、個人番号が漏えいする機会も増えていくこととなる。

このように個人番号制度の利用目的とは無関係の利用態様をあえて許容し、個人番号の漏えいの機会を増大させる個人番号制度は、個人番号の漏えいや不正利用を防ぐための法制度という方向性に完全に矛盾するものである。

したがって、かかる点においても法制度上の不備があるといわざるを得ない。

カ 小括

以上のように、番号利用法には法制度上の措置に不備が多々あることから具体的危険が既に存在しているうえに、今後個人番号の利用範囲が拡大していけばいくほど、関与する民間も含めた機関や人の範囲も拡大することから、法制度上の不備による具体的危険性はより高まっていくものである。

(2) システム技術上の不備及び事故事例について

ア 分散管理とはいえないこと

自治体中間サーバーが、地方公共団体ごとにアクセス権限が限定され、他の地方公共団体が保有する情報を引き出すことはできない仕組みとなっていたとしても、物理的に2か所に集約されていること自体には争いはない。

そして、個人番号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のであるから、物理的に2か所に集約されている状態は個人情報の不正取得という観点から極めて危険性の高いものである。

したがって、システム技術上の不備があるといわざるを得ない。

イ 人為的ミス

個人番号が記載された住民票等の誤送付等の人為的ミスが発生したこと自体に争いはない。

かかる人為的ミスが運用上の人為的な過誤であったとしても、制度を構築する際には、運用上の人為的な過誤が発生しないように検討されなければならない。

特に、個人情報の不正取得等の可能性がある個人番号制度においては、他の制度よりも一層検討される必要がある。

それにもかかわらず、人為的ミスが発生していることから、システム技術上の不備があるといわざるを得ない。

ウ プロファイリング

現代社会においては、データの管理主体が、いつでも容易にプロファイリングが可能な状態となっていること自体が、重大なプライバシー侵害となり得る。

この観点から、個人番号制度をみると、個人番号制度を構築するネットワークシステムが究極的には国の管理下に置かれていることは間違いなく、

情報管理者である国は、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、プロファイリングすることが可能な状態にある。現実には内部の情報流用が起きたかどうかは問題ではなく、プロファイリングを可能とする管理体制となっていること自体が問題なのである。

したがって、かかる点においてもシステム技術上の不備があるといわざるを得ない。

エ 小括

以上のように、番号利用法にはシステム技術上の不備が多々あることから具体的危険が既に存在しているものである。

(3) 小括

以上のように、番号利用法における個人情報の収集等は漏えい等の具体的危険にさらされている。

よって、このような具体的危険にさらされている個人情報の収集等については、プライバシー権（憲法第13条）によって保障されるべきである。

4 小括

以上のような現代社会における情報の性質を考えるならば、プライバシー権を原判決の言うような「みだりに第三者に開示又は公表されない自由」とのみするのでは、プライバシー権は全く保護されない。個人番号制度も、後記第3、および第4で（第4では住基ネットと比較しつつ）述べるように、以上と同様の危険性をもっているのである。

これら現代社会における個人情報の特質を考えるならば、プライバシーの権利の保障、それによる人格的自律と私生活上の平穩の確保を実効的なものにするためには、自己のプライバシーに属する情報の取扱い方を自分自身で決定するということが極めて重要になってきている。

その必要性は社会において広く認識されてきている。また、最高裁判例である京都府学連事件、京都市前科照会事件、指紋押なつ拒否事件等では、例えば

京都府学連事件及び指紋押なつ拒否事件では個人情報の「取得」の段階で保障を考えているなど、個人情報について、取得、利用及び開示といった個人情報処理の各プロセスにおける権利・自由を肯定してきているのである。

今日の社会にあつて、自己のプライバシー情報の取扱いについて自己決定する利益（自己情報コントロール権）は、憲法上保障されているプライバシーの権利の重要な一内容となっているものと解されるべきである。

これを狭く解した原判決は、憲法に違反していると言うほかない。

第3 違憲審査基準に関する憲法解釈の誤りについて

1 原判決の判示内容

本件における違憲審査基準について、一審判決は「憲法13条によって自己情報コントロール権が保障されている」旨の上告人らの主張を排斥したうえで、「番号利用法及び番号制度が個人に関する情報をみだりに第三者に開示又は公表されない自由を侵害するものであるか否かは、①番号制度において取り扱われる個人番号及び特定個人情報の秘匿性の程度、②行政機関等による情報の収集、保管、利用、提供等に関する法令等の根拠の有無及び行政目的の相当性、③法制度上又はシステム技術上の不備による情報漏えい又は目的外利用の具体的な危険の有無等の観点から、番号制度によって、みだりに個人に関する情報が収集、保管、利用、開示又は公表が行われる具体的な危険があるといえるかによって判断するのが相当である」として（一審判決38頁）、極めて緩やかな審査基準により判断した。

そして、原判決においても、上記一審判決を踏襲し、上告人らが主張する意味で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ていると解することはできないとしたうえで、「番号制度における特定個人情報の利用及び提供は、法令等の根拠に基づき、正当な行政目的の範囲内で行われているものと認められ、かつ、法制度上又はシステム技術上の不備に起因して特定

個人情報法が法令等の根拠に基づかずには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は認められない」として、上告人らの控訴を棄却した（原判決13頁）。

しかしながら、上記一審判決及び原判決は上告人らの侵害される権利の性質を過小評価することでその違憲審査基準の判断及び憲法13条の解釈を誤ったものである。

以下、詳述する。

2 プライバシー権にかかる違憲審査基準

(1) 憲法は、人間が生まれながらに有すると考えられる基本的人権を侵すことのできない永久の権利を絶対的に保障する考え方をとっている。もっとも、この基本的人権は無制限に保障されるものではなく、いわゆる公共の福祉による制約を受けることとなる。

そして、公共の福祉による制約が憲法上許されるか、すなわち合憲か違憲かを判断する基準が違憲審査基準である。この違憲審査基準は、制約を課される人権の性質によって大きく異なるものであるため、違憲審査基準を検討するにあたっては、上告人らの侵害される権利（プライバシー権）の性質を正確に理解する必要がある。

(2) この点について、芦部信喜教授はプライバシー権にかかる違憲審査基準について、「個人情報は、①だれが考えてもプライバシーであると思われるもの、②一般的にプライバシーと考えられるもの、③プライバシーに該当するかどうか判然としないもの、に大別できる。個人情報の収集・保有・利用ないし開示についてプライバシー権の侵害の有無が争われた場合、①は人の人格的生存の根源にかかわるので、最も厳格な審査基準（目的は必要不可欠なやむにやまれぬ利益で、手段はその目的を達成するための必要最小限度のものに限定される旨を要求する基準）によって、合憲性を判断しなければならない。」、「プライバシー権は人権尊重の原理を支

える人格不可侵の原則（人間の尊厳性）の核心にあるもの、とすることができる。個々人の人格ないし自律が最高度に尊重されてはじめて、人は真に自覚的な存在として自己を実現し、精神的自由の保障を全うすることが可能となる。したがって、結婚・出産・子供の養育などにかかわる個人の人格的ないし自律的存在にとって基本的と考えられるプライバシー権の侵害か否かが争われる場合には、精神的自由に準じて「厳格審査」が必要である（やむにやまれぬ利益の基準）。」としている。

(3) また、長谷部恭男教授もプライバシー権にかかる違憲審査基準について、「プライバシーが侵害されたか否かは、問題の情報が個人の私的な情報か否かと同時に、問題となった具体的状況で、本人がどの範囲での流通（あるいは非流通）を合理的に想定すべきかにも依存する。個人の私的情報の保護が個人の自律のために不可欠であることを考慮すると、信条、社会的身分、病歴、犯罪歴等、特に取扱いに配慮を要するセンシティブな情報を、政府が本人の同意なく収集・利用・伝達する措置は、厳格な違憲審査に服することになり、措置が正当化されるのは、それが必要不可欠な利益を達成するための必要最小限度の手段であることを政府が立証した場合に限定されるべきである。」としている。

(4) さらに、過去の最高裁判例でも、前科照会事件最高裁判決（昭和56年4月14日。民集35巻3号620頁）において、伊藤正己裁判官が「国または地方公共団体においては、行政上の要請など公益上の必要性から個人の情報を収集保管することがますます増大しているのであるが、それと同時に、収集された情報がみだりに公開されてプライバシーが侵害されたりすることのないように情報の管理を厳にする必要も高まっているといつてよい。近時、国または地方公共団体の保管する情報について、それを広く公開することに対する要求もつよまってきた。しかし、このことも個人のプライバシーの重要性を減退せしめるものではなく、個人の秘密に

属する情報を保管する機関には、プライバシーを侵害しないよう格別に慎重な配慮が求められるのである。本件で問題とされた前科等は、個人のプライバシーのうちでも最も他人に知られたいくないものの一つであり、それに関する情報への接近をきわめて困難のものとし、その秘密の保護がはかられているのもそのためである。もとより前科等も完全に秘匿されるものではなく、それを公開する必要の生ずることもありうるが、公開が許されるためには、裁判のために公開される場合であっても、その公開が公正な裁判の実現のために必須のものであり、他に代わるべき立証手段がないときなどのように、プライバシーに優越する利益が存在するのでなければならず、その場合でも必要最小限の範囲に限って公開しうるにとどまる。」との補足意見を述べており、これは「やむにやまれぬ利益」基準に当たる厳格な違憲審査基準を採用しているものであると考えられる。

- (5) 以上のことからすると、人格的生存の根源に関わる情報やセンシティブな情報等を収集・保管・利用等することによりプライバシー権を侵害している場合においては最も厳格な違憲審査基準が採用されるべきである。

3 本件で採用されるべき違憲審査基準

- (1) 以下に述べるように、本件においては最も厳格な違憲審査基準、具体的には「目的は必要不可欠なやむにやまれぬ利益で、手段はその目的を達成するための必要最小限度のものに限定される旨を要求する基準」で判断されなければならない。
- (2) そもそも、番号利用法19条は「何人も、次の各号のいずれかに該当する場合を除き、特定個人情報の提供をしてはならない。」と規定し、特定個人情報の提供に制限を課している。そのため、本人の情報であり、かつ本人の同意があったとしても、法に定められた目的以外で自己の特定個人情報を提供することは禁止されている。

このように、特定個人情報は従来の個人情報保護法や行政機関個人情報

保護法、独立行政法人等個人情報保護法などで取り扱われているものとは全く異なる取扱いをされているものであり、極めてセンシティブな情報であることが前提とされている。

- (3) 次に、個人番号制度の下では拡大利用やデータマッチングがなされており、個人番号制度によって収集・保管・利用されることになる特定個人情報は本人確認情報だけにとどまらず、勤務先や収入、税額、扶養家族、障害の有無・内容、社会保障給付の有無・内容、預貯金額とその預け先金融機関名、病名や診療内容が推知できるレセプト情報など、人格的生存の根源にかかわるものを当然に含む、極めてセンシティブなものとなっている。

さらに、個人番号制度は制度発足以降、順次その利用が拡大されてきており、これまで個人番号カードが国家公務員の身分証明書として利用されたほか、総務省がキャッシュレス業者と連携して個人番号カード保有者にポイント還元が行われたり、個人番号カードが健康保険証として利用されたりするようになった。そして、まもなく、個人番号カードの新規取得者に最大5000円分のポイントを付与し、健康保険証として登録すれば7500円、給付金などの受け取り用の預貯金口座の登録で7500円分のポイントがそれぞれ付与されることが予定されているなど、当初予定されていなかった分野にまで個人番号制度の利用拡大が図られてきており、個人番号制度によって収集・保管・利用されることになる特定個人情報の範囲も無限定に拡大されつつある。

つまり、個人番号制度の利用が拡大するにつれて、個人番号制度によって収集・保管・利用されることになる特定個人情報は本人確認情報だけにとどまらないものとなり、前述のように勤務先や収入、税額、扶養家族、障害の有無・内容、社会保障給付の有無・内容、預貯金額とその預け先金融機関名、病名や診療内容が推知できるレセプト情報など、人格的生存の根源にかかわる極めてセンシティブな情報も当然に収集・保管・利用されることとなり、

今後その範囲はますます拡大されていくこととなる。

- (4) 以上のように、個人番号制度によって侵害される上告人らの権利（プライバシー権）は、個人の人格的生存の根源に関わる極めてセンシティブなものとなる。

加えて、個人番号制度は監視監督機関が不十分であったりプライバシー影響評価が適切になされていないなどプライバシー侵害についての安全性が十分に確保されていないことや個人の極めてセンシティブな情報を個人が望まないにもかかわらず国が強制的に取得していく制度であることなどの事情も併せ鑑みると、個人番号制度にかかる違憲審査基準は最も厳格な違憲審査基準、すなわち目的は必要不可欠なやむにやまれぬ利益で、手段はその目的を達成するための必要最小限度のものに限定される旨を要求する基準で判断されなければならない。併せて、最も厳格な違憲審査基準においては、合憲性の推定が働かないため、国が個人番号制度の合憲性を積極的に主張・立証しなければならない。

しかしながら、一審判決及びそれを踏襲した原判決は、個人番号制度において侵害される上告人らの権利（プライバシー権）の性質を過小評価し、その違憲審査基準の判断及び憲法13条の解釈を誤っているため、速やかに破棄されなければならない。

4 原判決の認識の誤りについて

- (1) ところで、原判決は「番号制度が国民のプライバシーあるいは憲法13条によって保障される私生活上の自由を侵害するという前提に立つことはできない」との誤った認識を基に、前述の緩やかな審査基準にて憲法適合性を判断している（原判決17頁）。
- (2) しかし、国は個人番号制度制定当初より、個人番号制度に対する国民の懸念として、「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えいするのではないかといった懸念」や「個

人番号の不正利用等により財産その他の被害を負うのではないかといった懸念、「国家により個人の様々な個人情報個人番号をキーに名寄せ・突合されて一元管理されるのではないかといった懸念」を指摘したうえで、その対策として本人確認措置など制度面における保護措置や分散管理の実施などシステム面における保護措置を講じるものと説明を行っていた（乙1のスライド9）。

つまり、国としても個人番号制度によって国民のプライバシー権あるいは自己情報コントロール権などが一定程度制限を受けることは前提としており、しかしながら、それに対する各種保護措置を講じることによって前記権利を過度に侵害するものではないとの認識に立っていたにもかかわらず、原判決は「番号制度が国民のプライバシーあるいは憲法13条によって保障される私生活上の自由を侵害するという前提に立つことはできない」として、個人番号制度によって国民の権利は何ら侵害されていないと判示しているのであるから、原判決は明らかに個人番号制度に関する認識を誤っており、個人番号制度に関する当事者の主張も正解していないものである。

5 原判決の違憲審査の具体的危険の判断の誤り

原判決は、「番号制度における特定個人情報は、個人の識別性が高いことに加え、所得や社会保障の受給歴など秘匿性の比較的高い情報も含まれるから、」として、「番号制度自体に法制度上またはシステム技術上の不備があり、そのために法令等の根拠に基づかずにまたは正当な目的の範囲を逸脱して、特定個人情報が第三者に開示または公表される具体的な危険が生じている場合には、」「個人に関する情報をみだりに第三者に開示または公表されない自由を侵害するものといえる。」とした（原判決16頁）。

しかしながら、具体的な当てはめにおける、具体的な危険の存否に関する判断が明らかに不合理である。それは、個人番号のセンシティブ性を一顧だにしていなかったことである。

自分に付された番号であるのだから、個人情報保護法その他の法令における場合と同様、当然にその利用、提供が自由に処分されてしかるべきとも思われるのにもかかわらず、番号法19条は、全国民に対し、法の目的外での提供を一律に禁止しているのである。このような情報は、公務員など、特殊な身分に基づいて他人や団体の秘密を取り扱う場合の守秘義務の場合以外には類を見ないものを言わねばならない。情報主体（プライバシー権の帰属主体、あるいは主権者）ですら、自由に利用、提供が許されず、法令によって明示的に禁止されているほどのセンシティブ情報は、不要不急の行政事務によって勝手に利用されてはならないということは明らかであり、そのような事象が生じていないか、将来生じる蓋然性が高くないか、という警戒心が必要である。個人番号は、主権者が望んで取得した情報ではない。公権力が強いて付番したものである。しかも、主権者は自由に利用、提供できず、明文で禁止されている。にもかかわらず、不要不急の行政事務で広く利用が開かれていたり、厳に目的の曖昧なままで行政事務に提供されていたり、あるいは民間事業者の収益事業で広く利用可能であるとすると、番号法19条との矛盾は耐えがたいものとなる。

このような個人番号の本質からすると、その提供、利用が許される行政事務は厳格に制限されているべきであり、提供、利用が許されるための行政目的には、厳格な審査が必要不可欠なのである。

原判決は、この相関関係を全く理解していないため、たいした行政目的でなくとも、またその目的達成のための効果がたいして存在しなくても全く問題ないという判断に傾いている。いわく、「控訴人らは、行政の効率化や公正な給付と負担の確保という目的については、そのためにプライバシーへの介入が正当化されるのでは本末転倒であると主張する。しかしながら、行政機関等相互の情報連携を適切かつ円滑に行うことが、上記の3つの目的の達成に資するものであることは、現代社会における行政事務の性質及び態様に照らせ

ば明らかであるし、個人番号制度の運用のみによってそれらの目的が達成されるものではないことも明らかである。そして、こうした事柄の性質上、その効果や国民生活への影響を定量的に正確に予測することは困難と思われるが、そのことから制度自体が不要であると言うことにはならないのであって、目的の実現可能性について具体的な立証がないという控訴人らの主張は当たらない。」（原判決17頁）

行政効率化等に、関連はしている。個人番号制度によってその程度を計測することは不可能だが、なにも問題はない、要するにそういうことである（だとすれば、目的の実現可能性について具体的な立証がないという控訴人らの主張は正当であるというのが論理的帰結であり、そこも明確に自己矛盾をきたしている）。

このような違憲審査基準は、芦部教授によれば、経済的自由権のうち、積極的・政策的規制（積極目的規制）において採用されるべき「明白の原則」である（憲法第5版芦部信喜、高橋和之補訂218頁）。

すなわち、「当該規制措置が著しく不合理であることの明白である場合に限って違憲とする」方法である。立法府の広い裁量を認め、規制立法の「合理性」の有無の審査を緩やかに行うものである。しかしながら、プライバシー権は、公権力からの介入を拒む自由権であり、積極目的規制における経済的自由ほど緩やかに侵害しても構わないというのは、我が国の判例にも適合しないばかりか、デジタル社会におけるプライバシー確保のために主導的立場に立ちつつあるEUのGDPR（一般データ保護規則）の明文の到達点からみれば、人権の観念について50年くらい遅れている発展途上国の議論と司法を眺めているような残念な判断である（EUがアメリカとの間で個人情報の流通を認めたセーフハーバー協定は、2015年10月6日欧州司法裁判所判決で無効とされ、その後同趣旨で制定されたプライバシーシールドも、2020年7月17日欧州司法裁判所判決で無効とされた。いずれも、市民間の流通情報

が、行政機関によってアクセス可能であることを問題視してプライバシー権＝情報自己決定権侵害としている）。

原判決のように、ここまで、行政目的の正当性の曖昧さや、関連性の不明確さが事実として認定できるのであれば、端的に「具体的危険がある」と判断しても全く差し支えがない。番号法19条で厳格な利用禁止を定めている番号の利用の行政目的が曖昧であり、関連性が不明確である以上、「必要最小限度」規制であろうとすれば、それを逸脱していること、すなわち必要性の乏しい、あるいは関連性の不明確な個人番号の提供、利用が現になされている具体的危険が明白だからである。むしろ、そう判断するが妥当である。従って、原判決の違憲審査基準は不適切であるが、仮にその点をおいたとしても、行政目的の正当性や目的達成のための相当性がこれほど不明確であることを認定している以上、具体的危険ありと判断するのが素直なのであり、端的に違憲判断を下すべきであった。このような意味においても、原判決の判断は自己矛盾を来しており、破棄を免れない。

第4 平成20年最高裁判決の判断枠組みに照らせば個人番号制度の違憲性は明らかであること

1 一審判決及び原判決の判断

一審判決は、住民基本台帳ネットワークシステム（以下、「住基ネット」という。）に関する平成20年3月6日最高裁判決（以下、「平成20年最高裁判決」という。）を参照したうえで「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」と判示し、「番号利用法及び番号制度が上記自由を侵害するものであるか否かは、①番号制度において取り扱われる個人番号及び特定個人情報の秘匿性の程度、②行政機関等による情報の

収集、保管、利用、提供等に関する法令等の根拠の有無及び行政目的の相当性、③法制度上又はシステム技術上の不備による情報漏えい又は目的外利用の具体的な危険の有無等の観点から、番号制度によって、みだりに個人（原告ら）に関する情報が収集、保管、利用、開示又は公表が行われる具体的な危険があるといえるかによって判断するのが相当である」（以上につき一審判決・38～39頁）と判示したうえで結論においてその具体的な危険を否定した。

原判決は、このような一審判決を踏襲し、「番号制度における特定個人情報の利用及び提供は、法令等の根拠に基づき、正当な行政目的の範囲内で行われているものと認められ、かつ、法制度上又はシステム技術上の不備に起因して特定個人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される具体的な危険が生じているとは認められないから、控訴人らの権利を侵害するものとは認められない」と結論している（原判決・13頁）。

しかしながら、このような一審及び原審の判断は、平成20年最高裁判決が前提としていた住基ネットと個人番号制度との間に存する根本的な相違点を全く理解できていない。そもそも、平成20年最高裁判決当時と現在とでは、すでに個人情報を取り巻く環境が別次元といえるほどに劇的な変化を遂げていることに気付くことすらできていない。

以下に述べるとおり、個人番号制度は、平成20年最高裁判決の対象である住基ネット制度とは根本的に異なっており、平成20年最高裁判決で示された考慮要素を比較するならば個人番号制度が合憲であるなどとはおよそ評価できない。

2 個人番号制度は住基ネット制度と根本的に異なること

(1) 根本的な相違点

ア 平成20年最高裁判決の判断対象である住基ネット制度と本件の判断対象である個人番号制度は、確かに両制度ともに、住民票を有する国民と

外国人全員に、重複しない、唯一無二の個人識別番号を付する点では同一性を有する面がある。個人番号は住基ネットでは付された住民票コードを暗号変換して作られる番号であり、住民票コードと1対1の対応関係にあるからである。また、両番号は、住民票の記載事項でもある（個人番号は住民基本台帳法第7条 8の2号。住民票コードは同条13号。）。

イ しかし、両制度（両番号）は、以下のように重要な点で根本的に異なるものである。

- i まず、住民票コードは行政内部でしか利用しない番号であるのに対し、個人番号は広く民間でも収集保管された上、官に提供される番号（民・従業員など→民・事業者など→官・税務当局などで利用される番号）である。

両番号制度にこのような根本的な違いが生じるのは、その制度目的が大きく異なることによる。すなわち、住基ネット制度は、地方公共団体の共同のシステムとして、住民基本台帳のネットワーク化を図り、本人確認情報を各地方公共団体が共有することにより、全国的に特定の個人情報の確認ができる仕組みを構築し、市町村の区域を越えて住民基本台帳に関する事務処理を行おうとするものであるとされる。それゆえ、住民票コードは、行政内部での利用しか予定されていない。

これに対し、個人番号制度は、「税と社会保障の一体改革」の為に、個人番号をいわゆる「納税者番号」として利用することにより「より正確な所得の捕捉」をすることを前提に、社会保障や税の給付と負担の公平化を図るとともに、「(所得に応じて) 真に必要とする者に、必要な社会保障を給付する」ことを実現するための「社会保障番号」としても利用するものとして創設された制度である。「納税者番号」としての利用であるから、民間部門で広く使われることが当初から予定されている。

- ii 次に、住民票コードはデータマッチングを目的としない番号であると

されるのに対し、個人番号はデータマッチングを目的とした番号である

。上記 i で述べたような方法により捕捉した「正確な所得」を基にして、税を公平に徴収したり、所得の少なさに応じて真に必要な人に必要な社会保障を給付したりするために、それらの社会保障給付関係の個人情報をも正確・確実に整理するための個人識別番号（いわゆる「社会保障番号」）としても個人番号を利用し、税と社会保障という2つの分野の個人情報を正確にデータマッチングすることを目的として、個人番号制度は創設されたとされる。その意味において、個人番号はそもそもデータマッチングを目的とした番号なのである。そのため、個人番号制度はデータマッチングを目的とした情報提供ネットワークシステム（情報提供NWS）を有している。

- iii また、以上述べた目的の違いから、住基ネット制度では番号（住民票コード）と紐付けられた個人情報が本人確認情報（氏名、住所、生年月日、性別及びそれらの変更情報）だけであるのに対し、個人番号制度においては個人番号と紐付けられる情報が勤務先やそこでの給与額、地方税額、扶養家族、障害の有無・内容、社会保障給付の有無・内容、預貯金額とその預け先金融機関名等、極めて秘匿性の高い情報に及んでいる（なお、将来的には、病名や診療内容が推知できるレセプト情報なども紐付けられる）。
- iv さらに、住民票コードは自由に変更できる番号であるのに対し、個人番号は原則生涯不変の番号である。
- v 加えて、利用されるICカードの券面に住民票コードは記載されなかったのに対し、個人番号カードにおいては、券面（裏面）に個人番号が記載される（なお、顔写真の券面への掲載も選択制ではなく、必須とされている）。

ウ このように、個人番号制度は住基ネット制度とは根本的な相違点が存在していることが明確に認識される必要がある。

(2) 両制度の根本的な相違点をもたらす危険性の飛躍的増大

以上のように、個人番号制度は制度創設の目的を達成するには極めて不十分な制度であるにもかかわらず、上述のような目的の下、①個人番号に紐付けられる情報の秘匿性の高さ、②利用目的の合理性・的確性、③民間でも広く利用される点など、住基ネットとは根本的に異なる制度として作られたため、以下に述べるようなプライバシーに対する危険性の増大をもたらしている。

ア 漏えいの危険性が高いこと

個人番号は、民一民一官で利用する番号であるから、広く民間で収集・保存された上、官に提出される番号とならざるを得ない。住民票コードが官（行政）の中でしか利用されない番号であったのと比べると、個人番号が漏えいする危険性は飛躍的に高くなる。かつ、この個人番号は、民間にも保管されているセンシティブな個人情報をも名寄せするキーとなる番号であるから、その不正収集、不正利用（闇のデータベース作りなど）などのインセンティブも高い。

イ センシティブな個人情報のデータマッチングの危険性も飛躍的に高くなること

前述のように、個人番号と紐付けられる個人情報は、税関係情報や社会保障関係情報であり、誰がどこで働き、どのくらいの所得を得ているのか、扶養家族の有無、障害の有無、社会保障給付の内容などを推知しうる個人情報と結びついているから、それらがデータマッチングされる危険性も高まることになる。

ウ 利用事務の拡大が予定されていること

個人番号の利用事務は法律で定めないとはいけないとされているが、

そもそも既に税と社会保障分野の多数の事務で利用が開始されている。そして、その利活用を制限する原則的な基準は存しない。むしろ、その利活用の促進が国家戦略とされているから、今後益々いろいろな個人情報と紐付けられることが予想されるのであり、データマッチングされうるプライバシー情報は益々増加していくことにならざるを得ない。

エ 法律が改正されれば、これら全ての情報が一元的にデータマッチングされてしまう危険性が存すること

個人番号の利用事務には、それを制限する原則は存しない。例えば番号利用法第19条12号「その他政令で定める公益上の必要があるとき」には、条文上何らの限定が存しないことなどからすると、今後、例えば「テロ対策」などの名目で、疑わしい人物を洗い出すためにマイナンバーを利用して収集した情報をデータマッチングして、スクリーニングを行うなどの利用が許されてしまう等の危険性も存する。

また、現在の個人情報保護委員会の監督権限が、刑事事件に関する警察の利用などには及んでいないこと（番号利用法19条12号、37条）等に鑑みるならば、このような利用分野の場合、それをチェックすることも非常に困難である。

(3) 小括

以上より、住基ネット制度と個人番号制度との相違点は、個人情報に対する危険性を飛躍的に増大させるものである。

3 平成20年最高裁判決の考慮要素に照らした個人番号制度の評価

(1) 平成20年最高裁判決の概要と考慮要素

平成20年最高裁判決は、「憲法13条は国民の私生活上の自由が公権力の行使に対しても保護されるべきことを規定しているものであり、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」ことを認めた。その上で、住基ネット

さらに、

- ⑧ 住民票コードで個々の住民の個人情報が名寄せ可能となるデータマッチングについても、「データマッチングは本人確認情報の目的外利用に当たり、それ自体が懲戒処分の対象となるほか、データマッチングを行う目的で個人の秘密に属する個人情報を保有する事項が記録された文書等を収集する行為は刑罰の対象」となること、「現行法上、本人確認情報の提供が認められている行政事務において取り扱われる個人情報を一元的に管理することができる機関又は主体は存在しないこと」等から、住基ネットの運用によって具体的な危険が生じているということとはできないとした。

平成20年最高裁判決は、以上の8つの要素を考慮して、住基ネットは憲法13条により保障された上記自由を侵害するものではないと結論付けている。

- (2) 平成20年最高裁判決の考慮要素を比較検討すれば個人番号制度は違憲であること

上述した住基ネットと個人番号制度との違いを踏まえて、平成20年最高裁判決の考慮要素と個人番号制度の要素とを比較検討するならば、次のように、個人番号制度は、憲法13条により保障された上記自由を侵害しているといわなければならない。

ア 個人番号と紐付けられた個人情報の機微性、秘匿性の程度

- ① 個人番号と紐付けられて管理・利用等される個人情報は、上記の4情報や異動履歴情報に限らず、勤務先及び給与額、地方税額、扶養家族、障害の有無・内容、社会保障給付の有無・内容、預貯金額とその預け先金融機関名など、行政目的に限定することなく、民間利用を含めた極めて機微性・秘匿性の高い個人情報である（甲1「マイナンバーの利用範囲」参照）。さらに、将来的には、病名や診療内容が推知できるレセプト

情報なども紐付けられることが決まっている（甲14）。

- ② これらの個人情報、収入や社会保障に関する情報等、人が社会生活を行う上で他者への開示を予定していない情報であり、預貯金額やその入出金情報は個人の行動・生活状況を知りうるものであるから、個人の内面に関わる秘匿性の高い個人情報である。
- ③ これらの情報は、個人番号制度導入以前から、必ずしも法令に基づき必要に応じて他の行政機関等に提供され、その事務処理に利用されてきたものとはいえない。加えて、今後さらに新たな個人情報と紐付けすることも想定されている。
- ④ 個人番号は、民間部門でもひろく上記個人情報と紐付けされており、“悪用しやすい”番号であるため、その秘匿性の程度は本人確認情報と異なるものであるとは到底評価できない。

イ 侵害や危険性の有無・程度

- ⑤ 個人番号付き個人情報の管理、利用等は、形式的には法令等の根拠に基づいているとはいえ、その範囲は税と社会保障分野だけでも極めて広範であり、国民等にとって予想が付きにくい上、今後ますます利用範囲が広がることは確実である。
- ⑥ 個人番号制度のシステム上の欠陥等による漏えいの具体的危険は高い。
上述したように、民間企業等でも利用されることが予定されていることに加えて、住民票コードと異なり、個人番号は各個人から事業主等を介して行政機関に提供することを予定した民一民一官の制度であることや、民間企業等が各個人から提供された個人番号だけでなく、個人番号と関連づけられた個人情報を取得することも予定される制度であることからすれば、システム面においても、行政機関内のシステム（情報提供NWS）に欠陥等が見当たらなければ具体的危険がないということにはならない。個人番号を管理する民間を含めたシステム全体について欠陥

等がないかを調査し、対策する必要があるが、システム全体の調査・対策は到底不可能である以上、漏えいの具体的危険があると見るほかない。

- ⑦ 受領者による個人番号と紐付けされた個人情報（特定個人情報）の目的外利用又は漏えい等は、懲戒処分又は刑罰をもって禁止されているとはいえ、実効性が住基ネットの場合と比較して極めて低い。

行政機関のみにおける利用等を前提とした住基ネットと異なり、個人番号制度では、多種多様な民間企業の従業員等が個人番号やこれと紐付けられた個人情報の受領者・取扱者として関与することになるが、これらの民間企業の規模は様々で、統一したコンプライアンス体制を採用することもできず、研修が徹底できるとも考えられない。個人情報の目的外利用や漏えい等は秘密裡に行われ、目的外利用や漏えい等の瞬間に周囲が気付いてこれを取り締まることは不可能なのであって、漏えいからしばらく経って、漏えいした個人情報等を不正利用される被害が生じたときに初めて発覚することもしばしばある。したがって、たとえ、法律上、受領者による目的外利用や漏えい等を刑罰等で禁止したとしても、現実的な規制は不可能、少なくとも、住基ネット制度のように行政機関内だけの規制で足りる場合と比較して大幅に規制の程度は低下すると言わざるを得ない。

- ⑧ 個人番号制度は、住基ネット制度と異なり、そもそも個人情報のデータマッチングを目的とした制度であり、この点もまったく異なる。

以上のように、平成20年最高裁判決における考慮要素を比較検討するだけでも、個人番号制度は、私生活上の自由を侵害する具体的危険性の存しない制度であるとは到底評価し得ないのである。

第5 憲法41条に関する原判決の憲法解釈の誤り

1 総論

番号利用法19条14号及び16号（ただし現行法では15号及び17号）は憲法41条に反し違憲であるところ、原判決はこれを違憲としておらず、憲法解釈の誤りがある。

番号利用法施行令25条・別表各号は、番号利用法19条14号による委任の範囲を逸脱しており憲法41条に反し違憲であるところ、原判決はこれを違憲としておらず、憲法解釈の誤りがある。

2 憲法41条の意義と委任立法

(1) 憲法41条の意義

憲法41条は、「国会は、国権の最高機関であつて、国の唯一の立法機関である。」と定める。

ここにおいて、国会が「唯一の」立法機関であるとは、実質的意味の立法はもっぱら国会が定めなければならないことを意味し、そこには、

- | |
|---|
| <p>①国会による立法以外の実質的な意味の立法は、憲法の特別の定めがある場合（議員規則、最高裁判所規則）を除いて許されないこと（国会中心立法の原則）</p> <p>②国会による立法は、国会以外の機関の参与を必要としないで成立すること（国会単独立法の原則）</p> |
|---|

の2つの意味が含まれている（芦部信喜『憲法第7版』（岩波書店）307頁参照）。

このうちの国会中心立法の原則によれば、実質的意味の立法は、国会のみが行うことができ、行政がこれを行うことはできない。

(2) 委任立法とその限界

ア もっとも、今日の社会福祉国家においては、国家の任務が増大し、①専門的・技術的事項に関する立法や、②事情の変化に即応して機敏に適應することを要する事項に関する立法の要求が増加し、また、③地方的な特殊事情に関する立法や、④政治の力が大きく働く国会が全面的に処理するの

に不適切な、客観的公正のとくに望まれる立法の必要が増加した。

イ 委任立法は、このような実際上の必要から条理上認められると解されているが、基準なき広範な委任は、国家機関と権能に関する憲法上の取決めを破壊するものとなるため、個別・具体的でない委任、すなわち白紙委任は許されない。

ウ また、委任立法に関しては、委任を行う法律側の問題のほかに、委任を受けた命令側の問題、すなわち、委任に基づき定められた命令が、法律による委任の範囲を逸脱していないかとの問題も生じることとなる。

法律による委任の範囲を逸脱して命令を定めることは、当該法律に反し違法となるのみならず、行政が実質的な意味の立法を行うものとなり、憲法41条に反し違憲となる。

3 憲法適合性の判断基準

(1) 判例の概観

ア この白紙委任の問題に関し、個別・具体的な委任といえるかが争われた最も著名な例としては、公務員の政治的行為を制限する国家公務員法102条1項において、例示の定めこそあるものの、「人事院規則で定める政治的行為をしてはならない。」との形で、禁止される「政治的行為」が何かをほとんど規則に一任していることが問題となった、いわゆる猿払事件最高裁判決（最大判昭和49・11・6刑集28巻9号393頁）がある。

イ この猿払事件最高裁判決において、多数意見中に、白紙委任の有無の判断の前提となるような一般論は示されていないが、4名の裁判官による反対意見は、授權規定の憲法適合性に係る一般論として、「国会が、法律自体の中で、特定の事項に限定してこれに関する具体的な内容の規定を他の国家機関に委任することは、その合理的必要性があり、かつ、右の具体的な定めがほしいままにされることのないように当該機関を指導又は制約すべき目標、基準、考慮すべき要素等を指示してするものであるかぎり、必

ずしも憲法に違反するものということとはできず、また、右の指示も、委任を定める規定自体の中でこれを明示する必要はなく、当該法律の他の規定や法律全体を通じて合理的に導き出されるものであってもよいと解される。」としている。

この部分は、反対意見中に示されたものではあるが、昭和49年度最高裁判所判例解説刑事篇243頁（香城敏麿）は、「委任の限度に関する一般論及び公務員関係の規律の対象となる行為の規定の委任についての見解は、多数意見と異なるものではなく、むしろこれを補足するものとして十分に参考に値する内容をもっている。」として、反対意見が示した上記の一般論は多数意見の立場と異なるものではない旨の説明を行っている（判例タイムズ第1423号117頁参照）。

なお、上記判決において、最高裁は国家公務員法102条1項の規定を白紙委任とは認めなかったが、学説では、この委任はやはり白紙的だとみる見解が支配的である（芦部信喜『憲法第7版』（岩波書店）308頁）。

(2) 憲法適合性の判断基準

ア 以上からすれば、番号利用法19条14号及び16号による命令への委任の憲法適合性は、上記の判断基準、すなわち、他の国家機関に委任すべき合理的必要性があり、かつ、具体的な定めがほしいままにされないように当該機関を指導又は制約すべき目標、基準、考慮すべき要素等が指示されているか否かによって判断されるべきである。

イ なお、今日、委任立法の手法は広範に用いられているが、既にみたとおり、憲法41条の国会中心立法の原則の下では、委任立法はあくまでも例外であることは、上記の判断に際しあらためて意識されるべきである。

4 特定個人情報の意義と要保護性

(1) 特定個人情報は、番号利用法2条8項により「個人番号をその内容を含む個人情報」と定義されており、概括的にいえば、従来の個人情報に個人番号

を結合させたものである。

- (2) 個人情報、個人番号という原則終生不変・万人不同の情報と結合されることによって、その者の他の個人情報との名寄せがきわめて容易となる。

これは、公的機関における利用に限られず、民間においても、特定個人情報が流出した場合には、流出した特定個人情報相互間で、個人番号をタグとした名寄せが可能となる。

なお、個人番号は、同じく終生不変・万人不同とされる指紋等とも異なり、単なる数字の羅列であることから、専門的な知識がなくとも容易に識別可能であり、誰でもこれを用いた名寄せが可能である。

この点に関し、今日、個人情報は、社会において高い利用価値を有するものと捉えられており、かつ、情報のデジタル化により、一度流出した情報を完全に消去することは不可能となっていることからすれば、いわゆるダークウェブ等の非合法市場において、各所から流出した特定個人情報を名寄せしたデータベースが作成され、情報が累積されていくであろうことは想像に難くない。

- (3) このように、特定個人情報は、従来の個人情報に名寄せのタグとなる個人番号が付加・結合されたものとして、従来の個人情報よりもはるかに高い要保護性を備えている。

5 他の国家機関への委任に合理的必要性がないこと

(1) 総論

上記3でみたとおり、番号利用法19条14号及び16号による命令への委任の憲法適合性を判断するにあたっては、具体的な定めを他の国家機関に委任することの「合理的必要性」が前提となる。

しかしながら、個人番号制度における番号利用法19条の重要性及び個人番号制度が採用する特定個人情報の取扱いについての基本姿勢からすれば、特定個人情報の提供範囲については、法律自体によって明確に規定されるこ

とが必要なものであり、他の国家機関に委任することの合理的必要性を欠くものである。

(2) 個人番号制度における番号利用法19条の重要性

ここで、番号利用法19条の個人番号制度全体における位置づけを考えたとき、同条は、個人番号と個人情報の結合体である特定個人情報について、いかなる場合にその提供を許容し、いかなる場合に許容しないかを定めるものであり、個人番号制度の基本的性格（個人のプライバシーとの調和点をどこに求めるか等）を決定する根幹規定となるものである。

加えて、番号利用法は、従来から存在する制度や価値観を具体化するといったものではなく、「個人番号制度」という全く新しい制度（価値観）を創設するものであるため、その解釈にあたって既存の価値観をよりどころとすることにも限界がある。

つまるところ、番号利用法19条は、個人番号制度という全く新しい制度（価値観）の創設にあたり、その基本的性格を決定する根幹規定となるものであり、また、そこでは解釈にあたって既存の価値観をよりどころとすることにも限界があるから、立法者自身が、その内容を明確に規定することが強く要求されるものである。

(3) 個人番号制度が採用する特定個人情報の取扱いについての基本姿勢

ア 個人番号制度における特定個人情報の取扱い

i 特定個人情報の「提供」

番号利用法は、同法19条柱書で「何人も、次の各号のいずれかに該当する場合を除き、特定個人情報の提供をしてはならない。」と定め、特定個人情報の提供について、情報主体による提供さえ原則禁止としたうえで、同条1号ないし16号に該当する場合のみ例外的にその提供を認めている。

このように、特定個人情報の提供につき「原則禁止」との厳格な位置

づけがなされているのは、特定個人情報は個人番号を含むものであり、より厳格に第三者提供を制限しなければ、不正なデータマッチングが行われる蓋然性が高いためとされている（宇賀克也『番号法の逐条解説〔第2版〕』（有斐閣）107頁）。

ii 特定個人情報の「利用」

番号利用法9条5項は、「前各項に定めるもののほか、第19条第12号から第16号までのいずれかに該当して特定個人情報の提供を受けた者は、その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することができる。」と規定し、特定個人情報の利用可能範囲を定めている。

これによれば、番号利用法19条14号及び16号による特定個人情報の提供範囲及びその提供目的は、その利用可能範囲とも直結している。

イ 特定個人情報の取扱いについての厳格な姿勢

上記アのとおり、個人番号制度は、特定個人情報の提供及び利用可能範囲につき情報主体による提供を含めて原則禁止とするという、非常に厳格な姿勢を採用している。

そして、その範囲を超えた提供や利用は、違法となるとともに、個人のプライバシーという今日の情報社会においてきわめて重大な利益を脅かすものとなるのであるから、この点からも立法者自身がその内容を明確に規定することが強く要求されるものである。

(4) 結論

ア 以上のとおり、個人番号制度における番号利用法19条の重要性及び個人番号制度が採用する特定個人情報の取扱いについての基本姿勢からすれば、特定個人情報の提供範囲については、法律自体によって明確に規定されることが必要なものであり、他の国家機関に委任することの合理的必要性を欠くものである。

また、仮に、他の国会機関に委任することの合理的必要性が直ちに否定されなかったとしても、上記(2)及び(3)でみたような事情からすれば、他の国家機関を「指導又は制約すべき目標、基準、考慮すべき要素等」は、高度に具体的かつ明確であることを要するというべきである。

イ また、別の観点として、番号利用法19条14号には、特定個人情報の提供が認められる場合として「刑事事件の捜査」が含まれるところ、その主体たる警察機構は、歴史的に人権侵害の主体となってきたものである。

そうであるところ、既にみたとおり、同号は、特定個人情報の利用可能範囲とも直結しており、同号の解釈次第では警察機構による特定個人情報の収集・利用が無限定に拡大しうるところであり、かかる観点からも、規定の明確性が強く要求される。

この点に関しては、番号利用法19条14号が、公的機関が従来適法に収集してきた資料について、当該資料中にたまたま特定個人情報が含まれることによって資料収集が妨げられることがないよう、あくまで副次的に提供を認める趣旨ということであれば、捜査機関による利用可能範囲は相当程度限定されうるが、国は、この点に関する解釈を明確にしておらず、また、番号利用法19条14号に基づく特定個人情報の提供には個人情報保護委員会による監督等も及ばない(番号利用法36条)ことから、十分な監督等の及ばない環境下で捜査機関による特定個人情報の収集・利用が広範になされうる構造が存在している。

なお、被上告人は、「捜査機関が刑事事件の捜査のためであれば無制限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」から、その限界は不明確でないと主張する(被上告人第1準備書面「第

2. 2 (1)]]。

しかしながら、刑事訴訟法は、そもそも特定個人情報の存在を前提としては定められておらず、特定個人情報の保護の観点から十分なチェックが及ぶものとは考えがたい（例えば、令状審査に際し、差押対象物についていかなる特定個人情報を含むかを現場の裁判官が十分に考慮しているとは認めがたい。）。

6 番号利用法19条14号の規定が白紙委任であること

(1) 番号利用法19条14号の規定

以上をふまえて、番号利用法19条14号をみると、同号は、

- | |
|---|
| <p>①各議院もしくは各議院の委員会もしくは参議院の調査会が国会法第104条第1項もしくは議院における証人の宣誓及び証言等に関する法律第1条の規定により行う審査もしくは調査</p> <p>②訴訟手続その他の裁判所における手続</p> <p>③裁判の執行</p> <p>④刑事事件の捜査</p> <p>⑤租税に関する法律の規定に基づく犯則事件の調査</p> <p>⑥会計検査院の検査</p> <p>⑦その他政令で定める公益上の必要があるとき</p> |
|---|

として、数件の例示の後に「その他政令で定める公益上の必要があるとき」と定め、政令への委任を行っている。

(2) 「公益上の必要があるとき」が指導制約指針たりえないこと

ここで、「公益上の必要があるとき」との文言が、委任を受けた機関を指導又は制約すべき目標、基準、考慮すべき要素等を指示しているかを考えたとき、およそ国家の行為というものは、大なり小なり公益を目的としてなされるものであり、公益上の必要の存在を大前提に、競合する人権との調整を図る必要があるのであるから、「公益上の必要があるとき」との文言は、特定個

個人情報の提供の範囲、とくに限界を考えるにあたり、委任を受けた機関をなら指導・制約する意味を持ちえない。

(3) 同号の例示が指導制約指針たりえないこと

また、同号の例示からも、同号による特定個人情報の提供の限界を画すべき共通の指導・制約指針を見出すことは困難であり、委任を受けた機関を指導又は制約すべき目標、基準、考慮すべき要素等が指示されているとはいえない。

同号の規定について、上記「5(4)イ」でみたような副次的な提供の規定とみたとしても、既にみた特定個人情報の要保護性及び個人番号制度における取扱いに鑑みれば、公的機関による調査等であれば無限定に特定個人情報の提供が許されるものとは解し得ず、提供が許されるためには、当該調査等につき、特定個人情報の保護に優先すべき公益上の必要性が認められなければならないはずであるが、同号の規定が、いかなる調査等であれば特定個人情報の保護に優先すると解しているかは、同号の解釈によっても見出せない。

(4) 結論

そのため、番号利用法19条14号は憲法41条により禁止される白紙委任を行うものであって違憲であり、これを違憲としなかった原判決には憲法解釈の誤りがある。

7 番号利用法19条16号の規定が白紙委任であること

(1) 総論

番号利用法19条16号をみると、「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。」して、個人情報保護委員会規則に委任を行っている。

しかし、同規定については、既にみた14号ひとつをとっても限界を見出すことが困難な番号利用法19条各号の規定について、「これらに準ずる」との不明確な限定の下に広範な委任を行うものであって、14号による委任と

同様、白紙委任というべきものである。

ゆえに、番号利用法19条16号も憲法41条に反し違憲であり、これを違憲としなかった原判決には憲法解釈の誤りがある。

(2) 個人情報保護委員会への委任に合理的必要性がないこと

ア ところで、番号利用法19条16号は、原則禁止である特定個人情報の提供の例外を規定することを「個人情報保護委員会」に委ねている。

しかし、そもそも個人情報保護委員会は、その機関の設置された趣旨や使命から考えると、特定個人情報の提供範囲を拡大する方向に関与する機関としては全く不相当であり、具体的な内容の規定を個人情報保護委員会に委任することは、上記した憲法適合性の判断基準における「合理的必要性」を欠くものといわなければならない。

イ すなわち、番号利用法19条14号の「その他政令で定める公益上の必要があるとき」として、同法の主務官庁である内閣府が特定個人情報の提供範囲の拡大を担うことには、行政機関相互の所掌配分としては相当の合理性がある。

しかし、個人情報保護委員会は、個人情報保護法60条において、「委員会は、個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の個人情報の有用性に配慮しつつ、個人の権利利益を保護するため、個人情報の適正な取り扱いを図ることを任務とする。」と規定されているとおり、個人情報の有用性に配慮はしつつも、あくまで、個人の権利利益を保護することを終局目的として、個人情報の適正な取扱いが確保されているか否かについて、個人情報取扱事業者や個人番号利用事務実施者等の実施機関を監督する第三者機関である。

個人情報保護委員会は、このような役割から、独立性が保障され（個人情報保護法59条1項及び62条）、立入検査、勧告、命令、指導、助言等

(同法40条ないし42条)を行う強力な監督権限を付与されている。

したがって、特定個人情報の無限定な第三者提供を可及的に防止することによって個人のプライバシーを保護しようとする番号利用法及び同法19条の趣旨からは、番号の利用の拡大は内閣府の役割とし、個人情報保護委員会はこれらの機関に対する監督機関として純化することが、その職責を全うするために必要かつ相当であると考えられる。

EU一般データ保護規則においても、独立した監督機関の設置が義務づけられているが、当該機関には、プライバシーの利用範囲の拡大権限は一切存在しない(51条ないし59条)。

ちなみに、平成7年に制定されたEUデータ保護指令においても、この構造は全く同様であったから、EUでは、このようなデータ保護機関の役割の純化は20年以上の伝統を有する。

この点に関し、原判決は、「番号利用法19条16号の趣旨は…委員会に対して特定個人情報の提供範囲の拡大を推進させる役割を負わせる趣旨とは解されない。」(原判決18頁)と述べるが、同号が拡大を「推進させる役割」を負わせているかは重要な問題ではない。

番号利用法19条16号が、個人情報保護委員会に対し、特定個人情報の提供範囲を拡大する方向での権限を付与していること自体は事実であるところ、監督機関であるにもかかわらず、特定個人情報の提供範囲拡大を自ら許容した行政事務が存在した場合、当該行政事務に対する監督を中立かつ厳格になしうるかの疑問が生じるどころであり、少なくとも、監督業務の「公正らしさ」には多大な疑問が生じるどころである。

ウ したがって、監督機関に対し特定個人情報の提供範囲を拡大する方向での権限を付与すること自体が、判断基準における「合理的必要性」を欠くものである。

8 番号利用法施行令25条・別表各号が委任の範囲を逸脱していること

(1) 総論

上記6のとおり、番号利用法19条14号は、政令への白紙的な委任を行うものであるところ、委任側の法律が白紙的な委任しか行っていない場合において、受任側の政令が委任の趣旨に沿った適切な定めを行うことは不可能であり、番号利用法施行令25条・別表各号は、番号利用法19条14号の委任の範囲を逸脱し違憲というべきである。

(2) 各論

ア はじめに

上記(1)のとおり、番号利用法施行令25条・別表各号は全体が違法かつ違憲というべきであるが、念のため個別にもみていく。

イ 別表8号について

i 被上告人は、別表8号の税務調査につき、「徴税権の適正な運用を確保し、租税の公平確実な賦課徴収を図るという目的を実現するために不可欠であるから、特定個人情報の提供を認めるという視点からすると、同号で具体的に列挙された調査等と同様の公益上の必要性があると解される。」と主張する（被上告人第1準備書面「第2. 2 (2) ア」）。

ii かかる説明は、一見するともっともらしいが、公益上の必要をもって個人の自由・権利に対する制限・介入が許容されるかは、その目的のみが問題となるのではなく、対立する自由・権利の憲法上の重要性や、制限・介入に際しての手續保障の有無・程度等の総合衡量によって判断されるものである。

そのため、犯則調査について特定個人情報の提供が認められるからといって、同一の目的を有する税務調査についても提供が認められてよいとは当然にはならない。

iii また、被上告人がいう、税務調査も犯則調査も「徴税権の適正な運用を確保し、租税の公平確実な賦課徴収を図る」という目的達成のための

手段の1つであるとの説明も、実際には適切でない。

甲第114号証は、国税庁の研修機関である税務大学校が作成した、税法に関する講本の抜粋であるが、その139頁をみると、税務調査と犯則調査との関係については、

通則法第11章に規定する犯則事件の調査（犯則調査）と通則法第7章の2に規定する質問検査権に基づく調査（税務調査）とは、その目的、性格が著しく異なっている。

質問検査権に基づく調査は、各税法の定める国税の納付、賦課、徴収が適正に行われるよう、納税義務者などに対して、質問、検査を行うものであって、全くの行政手続である。

これに対して、犯則事件の調査は、国税についての犯則があると認められる場合に、通告処分又は告発を終局の目的として、犯則事件の証拠を発見、集取するために行うものであって、形式的には行政手続であるが、実質的には刑事手続に近い性質を持つものである。

とされており、また、同135頁においても、

【税務調査・目的】 適正な課税を行うために必要な資料を収集することを目的とする調査である。

【犯則調査・目的】 悪質な脱税者について検察官に告発し、刑事訴追を求めるために、脱税の実態（犯則事実及び犯則嫌疑者）を明らかにするとともに、十分証明できる証拠を収集することを目的とする調査である。

として、両者の目的及び性格が大きく異なることが説かれている。

また、同130頁をみると、国税犯則調査手続の趣旨として、

各税法に定める罰則は、全て刑罰を科するものであって、過料その

他の行政罰を科するものではない。したがって、租税犯については、特別の定めがない限り、刑訴法の規定に従って、捜査機関が捜査し、裁判所で審理裁判すべきものである。

しかし、国税に関する犯則事件は、①証拠関係においては、一般の刑事事件とは相当異なるものがあること、②証拠の収集にも、また証拠に対する価値判断にも、特別の経験と知識を必要とすること<中略>などから、特殊な犯罪である。そのため、日常国税の賦課事務に従事し、課税物件や納税義務者に接触している税務職員に、その調査と処分を行わせることが便宜であるばかりでなく、証拠隠滅を防ぎ、できるだけ敏速な調査と適正公平な処分を行うことを可能とすることから、国税に関する犯則事件の調査及び処分については、通則法第11章（旧国犯法）において刑訴法による通常の刑事手続とは異なる手続を定めたのである。

との説明がなされており、これによれば、犯則調査は、本来的には通常の刑事手続によるべきところ、対象犯罪の特殊性に鑑み、日常的に租税の賦課事務に従事し専門性を有する税務職員にこれを扱わせることとしたものであり、刑事手続から便宜的に切り出されたものとして、「刑事事件の捜査」又は「裁判の執行」に近接した性格を有していることが分かる。

また、同140頁をみると、犯則調査については、

調査手段である質問、検査、領置、照会、臨検、搜索、差押え及び記録命令付差押えは、いずれも国民の社会生活に重大な影響を及ぼすものであるため、通則法第11章においては、当該職員に対し、これらの権限の行使について種々の制限、条件、手続などを定めることにより人権の保障と調査の厳正を期することとしている。

とあり、その権限行使について人権保障のための種々の制限、条件及び

手続等が定められているとともに、

通則法第7章の2に規定する質問調査権を有する当該職員が、同時に国税犯則調査手続上の当該職員である場合もあるが、質問検査権の質問の権限と国税犯則調査手続上の質問の権限は、厳格に区別して行使されるべきである。

として(同141頁)、税務調査の権限とは厳格に区別して行使すべきものとされている。

- iv. 以上によれば、犯則調査は、税務調査とはその目的及び性格が著しく異なるものであり、両者が同一の目的達成のための手段であるとする説明は適切ではなく、また、犯則調査において人権保障のための種々の制限、条件及び手続等が定められていることからすれば、犯則調査に関して特定個人情報の提供が認められるからといって、税務調査に関しても当然にこれを認めるべきとはならない。
- v. この点に関しては、犯則調査について「徴税権の適正な運用を確保し、租税の公平確実な賦課徴収を図る」ことが主たる目的ではないにしても、そのことが目的の1つ、あるいは最終目的であることには相違ないのであるから、同一の目的を有する税務調査にも同様の公益上の必要性があるとの反論が考えられる。
- vi. しかしながら、国税庁が平成29年度に査察調査に着手した件数が174件であるのに対し、同年度に行った税務調査の件数は62万3000件であったとされるところ(甲83・16頁)、もし、番号利用法19条14号が、「徴税権の適正な運用を確保し、租税の公平確実な賦課徴収を図る」との点に着目して犯則調査を列举事由としたのであれば、犯則調査が列举される一方で、それよりも圧倒的に件数が多く、上記目的との関係でもより直接的な税務調査が列举されないことは、いかにも不自然である(この点に関して、税務調査は第180回国会に提出された旧

法案では列挙事由とされていたものの、現行法では削除されている。)

vii また、番号利用法19条14号の列挙事由は、

- | |
|--|
| <p>①各議院もしくは各議院の委員会もしくは参議院の調査会が国会法第104条第1項もしくは議院における証人の宣誓及び証言等に関する法律第1条の規定により行う審査もしくは調査</p> <p>②訴訟手続その他の裁判所における手続</p> <p>③裁判の執行</p> <p>④刑事事件の捜査</p> <p>⑤租税に関する法律の規定に基づく犯則事件の調査</p> <p>⑥会計検査院の検査</p> |
|--|

であるところ、上記①は立法、上記②ないし④は司法機能に関するものであり、上記⑥は、内閣に対して独立の地位を有する憲法上の機関である会計検査院の機能に関するものである。

そのうえで、上記⑤は、既にみたとおり、本来的には刑事手続によるべきものが、対象犯罪の特殊性に鑑み、便宜的に切り出されたものであることからすれば、上記②ないし④の司法機能に類するものといえる。

このようにして列挙事由をみると、純粋な行政機能に関するものは列挙事由には含まれていないのであり、そのような中、純粋な行政手続である税務調査が同号による特定個人情報の提供対象に加わることは自然とはいいがたいし、同号がこれを許容していると解すべき根拠もない。

viii 以上からすれば、別表8号の規定は、番号利用法19条14号による委任の範囲を逸脱するものというべきである。

ウ 別表7号について

別表7号の少年法6条の2の規定による調査について、被上告人は、列挙事由の「刑事事件の捜査」と同様のものと解するようであるが、被上告人自身が指摘するとおり、少年法6条の2の規定による調査の主体は、司

法警察職員たる警察官のほか、警察官ではない警察職員にまで拡大されており（少年法6条の2第3項）、捜査機関として刑事訴訟法等による規制が及ばない者にまで範囲が拡大されている。

エ 別表11号及び24号について

- i また、別表11号の国際捜査共助等に関する法律に規定する共助及び協力、別表24号の国際刑事裁判所に対する協力等に関する法律に規定する証拠の提供、執行協力及び管轄刑事事件の捜査に関する措置は、いずれも国際協力に関するものであり、そこでは、特定個人情報が国外に提供され、国外において利用されることが前提とされている。
- ii しかしながら、番号利用法19条14号の列挙事由はもちろん、同条の他の規定をみても、特定個人情報の国外提供につき定めるものはなく、特定個人情報の国外提供は、番号利用法施行令において、突如として出現している。
- iii この点について、わが国に住民票を有する者の個人番号と個人情報の結合体である特定個人情報について、国外への提供を認めるか否かはきわめて重要な問題であり、番号利用法19条14号が特定個人情報の国外提供を明確に認めていると解すべき指針がないにも関わらず、その国外提供を認めている別表11号及び24号は、番号利用法19条14号による委任の範囲を逸脱するものである。

オ 別表9号及び17号について

別表9号の破壊活動防止法の規定による調査等及び別表17号の無差別大量殺人行為を行った団体の規制に関する法律による調査等も、「刑事事件の捜査」と比較したとき、調査等の主体が司法警察権を持たない公安調査官に拡大されており、刑事訴訟法等による規制も及ばない（なお、これらの法律によって公安調査官に認められている調査権限はかなり抽象的かつ広範であり、特定個人情報の広範な取得・利用がなされる危険性が大きい。）。

カ 結論

以上のおおりにあり、個々の規定をみても、番号利用法施行令は、同法
19条14号による委任の範囲を逸脱するものである。

以上



これは正本である。

この正本は、理由書について契印を省略している。

令和5年3月9日

最高裁判所第一小法廷

裁判所書記官 長谷川 和 秀

