

平成27年(ワ)第34010号

平成28年(ワ)第9404号

マイナンバー(個人番号)利用差止等請求事件

原告 関口博ほか40名

被告 国

## 準備書面(2)

2017年(平成29年)3月31日

東京地方裁判所民事第26部合議2係 御中

原告ら訴訟代理人 弁護士 水 永 誠 二

同 瀬 川 宏 貴

同 出 口 かおり

同 小 峰 将太郎

## 【目次】

### はじめに

1	安全性が確保されていないことを示した被告の釈明内容	3頁
2	プライバシー保護の国際的水準である <b>Privacy by Design</b> に反する日本のシステム	3頁
第1	プライバシー・バイ・デザイン	4頁
1	プライバシー・バイ・デザインとは	4頁
2	国際的に採択・採用されているプライバシー・バイ・デザイン	5頁
3	プライバシー・バイ・デザインとプライバシー・インパクト・アセスメント(P I A) との関係	8頁
4	プライバシー保護強化技術(P E T s) とは	9頁
5	小括～プライバシー・バイ・デザインに基づいて制度構築を行う義務	9頁
第2	日本のマイナンバーシステムが、プライバシー・バイ・デザインに反し、基本的な安全性を欠いている典型例について	10頁
1	制度・システム全体についてプライバシー影響評価を行っていない点	11頁
2	機関別符号で情報連携するにも拘わらず、各省庁においてマイナンバーを保有している点	12頁
3	個人番号カードの券面に個人番号・性別を記載している点	12頁
4	地方公共団体情報システム機構(J-LIS)による「一元管理」の点	13頁
5	「一元管理」と「分散管理」についての理解を誤っている点	14頁
第3	住民税特別徴収税額決定通知書に個人番号を記載することの問題点	15頁
1	住民税特別徴収税額決定通知書とは	16頁
2	総務省による通知、Q&Aの送付	16頁
3	個人番号を記載した特別徴収税額通知書を送付する根拠、理由	17頁
4	個人番号を記載した特別徴収税額通知書を送付することの危険性	18頁
5	この問題から裏付けられる番号法の違憲性	21頁

## はじめに

### 1 安全性が確保されていないことを示した被告の釈明内容

被告は、「求釈明に対する回答書（２）」（平成２９年１月２４日付）を提出した。しかし、その内容は、肝腎な点についての釈明を回避するとともに、マイナンバー制度のシステムが基本的な安全性に欠けるものであることを示したものであった。

マイナンバー制度は、平成２９年３月１７日、情報連携ネットワークシステム（情報連携nws）やマイナポータルの本格運用開始予定が同年１０月以降にさらに遅れると発表されるなど、未だその安全性に関する前提事実関係が明らかにされていない点も数多く存するところであるが、以下、明らかに安全を欠く点について何点か明らかにする。すなわち、①そもそも、そのような制度にする必要性すら明らかにされていない点や、②そのような制度にする必要性が一定程度存したとしても、その必要性を実現するために、容易に対策することのできる安全性すら確保されていない設計となっていることについてである。

### 2 プライバシー保護の国際的水準である **Privacy by Design** に反する日本のシステム

原告らは、求釈明の前提として、その準備書面（１）の第３、２において、“被告国は、その行政目的実現のために必要であるとして、国民・外国人住民の同意なく、あえて危険な「共通番号」を附番し、利用を開始したのであるから、その利用を巡る安全確保の責務と説明責任が存する”と指摘した。

いまやその安全は、「国際水準」において保障されなければならない。何故なら、例えば、サイバー攻撃は全世界からなされるものであるし、（たとえ直接的に特定個人情報が国際的に流通するということはないとしても）、現時のグローバル経済の下においては、情報が国際的に流通することを前提として、その保護水準も国際水準において整備しなければならなくなっているからである。

その「国際水準」として、注目を集めているのが「プライバシー・バイ・デザイン」(Privacy by Design・以下「PbD」と表記することもある。)である。これは、個人情報コンピューターネットワークにより大量に収集・保存・利用される現代社会において(原告準備書面(1)11頁以下参照)、大量の情報漏えい等、事後に原状回復が困難な状況を招く前に、自己情報コントロール権等の個人の権利利益を保護するための取組みを事前に講じるための仕組みである。政府が、諸外国で採用されているプライバシー影響評価に相当するものとして情報保護評価(PIA)を導入したのも、この国際水準がプライバシー権等の個人の権利利益の保護のために必要不可欠であることを認めているからこそである(もともと、後述の通り、日本版PIAはマイナンバー制度の仕組みそのものではなく、この制度で運用される個別の事務だけを対象としており、甚だ不十分である。)

そこで、以下、まず、プライバシー・バイ・デザインについて簡単に説明を行った後に、マイナンバーシステムが基本的な安全性を欠いている代表的な例を幾つか挙げて指摘する。

## 第1 プライバシー・バイ・デザイン

### 1 プライバシー・バイ・デザインとは

- (1) プライバシー・バイ・デザインについて、その提唱者であるカナダ・オンタリオ州情報・プライバシー・コミッショナーであるアン・カブキアンは以下の様に説明している。

プライバシー・バイ・デザインは、大規模にネットワーク化された情報システムにおいて適切にプライバシー保護を実現していくための概念である。情報通信技術が広く浸透し、刻々と進歩する現在、もはやプライバシー情報の安全は単に規制の枠組みを順守するだけでは保障できない。組織の活動のあらゆる場面で、標準的に保障される必要がある。

プライバシー保護に関し、従来はプライバシー強化技術(PETs)を利用する

ことが解決策と考えられてきたが、今日では、もっと実質的なアプローチが必要だと認識されている。例えば PETs を採用することにより利便性が犠牲になる（二者択一型のゼロサムモデル）といったことのない、必要な条件を同時に満たせるポジティブサムモデルを目指すことである。それが PETs に代わる PETs プラスの基本的な考え方になる。

プライバシー・バイ・デザインの目的は、プライバシーを確保することと自己の情報に対する個人のコントロールを獲得すること、組織のために持続可能な競争的利点を獲得すること。そして、それは七つの基本原則を実践することで達成できる。これらの原則は、あらゆる種類の個人情報に適用され得る。特に、医療情報や財務データといった機微なデータには強力に適用されなければならない。（以上、甲 2・『プライバシー・バイ・デザイン プライバシー情報を守るための世界的新潮流』堀部政男一橋大学名誉教授、一般財団法人日本情報経済社会推進協会 (JIPDEC)、アン・カブキアン編著、p.90)

- (2) 新保史生慶應義塾大学教授は、プライバシー・バイ・デザインについて、「プライバシー保護を目的として利用される技術及び対策を、システム設計及びその構築段階から検討・実装し、ライフサイクル全般において体系的かつ継続的にプライバシー保護に取り組むことである。目標とするのは公正な情報の取り扱い（FIPs : Fair Information Practices）の達成である。プライバシー保護に向けた取り組みを計画し、それを実施する。その際の基礎となるのが七つの基本原則と六つのプロセスである。」と説明している（「プライバシー保護におけるプライバシー・バイ・デザインの意図 PbD、PIA、PETs の相互関係」・甲 2・p.45）。

## 2 国際的に採択・採用されているプライバシー・バイ・デザイン

- (1) このプライバシー・バイ・デザインに関しては、平成 22 年（2010 年）10 月に開催された第 32 回データ保護・プライバシー・コミッショナー国際会議において、プライバシー・バイ・デザインに関する決議が採択されている。決議の概要は、以下のとおりである。（甲 2・p.56～58）

- ① プライバシー・バイ・デザインを基本的なプライバシー保護の不可欠な構成要素であると認識する。
  - ② プライバシー・バイ・デザインの採用が組織の初期機能形態としてプライバシーを確立するように推奨する。
  - ③ データ保護・プライバシー・コミッショナー／機関が次のことを行うように要請する。
    - a 資料の配付、啓発及び個人的唱道を通じてできるだけ広くプライバシー・バイ・デザインを促進すること
    - b それぞれの法域内におけるプライバシーポリシー及び立法の立案においてプライバシー・バイ・デザインの基本原則を組み込むように助長すること（以下略）
- (2) そして、上記 1 (1)及び(2)の「七つの基本原則」、2 (1)③ bの「プライバシー・バイ・デザインの基本原則」とは、以下の 7 原則を指す。（甲 2 ・ p.58、p.91～92）
- ① 事後的でなく事前的、救済策的でなく予防的であること  
プライバシー・バイ・デザイン(PbD) のアプローチは、受け身ではなく先見的に対応することが特徴である。プライバシー侵害が発生する前に、それを予想し予防することを目的としている。このため、事後ではなく事前に作用する。
  - ② プライバシー保護は初期設定で有効化されること  
プライバシー保護の仕組みはシステムに最初から組み込まれる。個人データは、個人が何もしなくても、そのまま保護される。個別の措置は不要である。
  - ③ プライバシー保護の仕組みがシステムの構造に組み込まれること  
プライバシー保護の仕組みは、ITシステムおよびビジネス慣行のデザインおよび構造に組み込まれるものである。事後的に、付加機能として追加するものではない。つまり、プライバシー保護の仕組みは、ITシステ

ムおよびビジネス慣行に不可欠な、中心的な機能になる。

④ 全機能的であること。ゼロサムではなくポジティブサム

プライバシー・バイ・デザインでは、プライバシー保護の仕組みを設けることによって、利便性を損なうなどトレードオフの関係を作ってしまうゼロサムアプローチではなく、すべての正当な利益および目標を収めるポジティブサムアプローチを目指す。

⑤ データはライフサイクル全般にわたって保護されること

プライバシー情報は、生成される段階から、廃棄される段階まで、常に強固なセキュリティで守られなければならない。すべてのデータは、データライフサイクル管理の下に安全に保持され、プロセスの終了時には確実に破棄される。

⑥ プライバシー保護の仕組みと運用は可視化され透明性が確保されること

どのようなビジネス慣行または技術が関係しようとも、プライバシー保護の仕組みが機能することを、すべての関係者に保証する。この際、システムの構成および機能は、利用者および提供者に一樣に、可視化され、検証できるようにする。

⑦ 利用者のプライバシーを最大限に尊重すること

設計者および管理者に対し、プライバシー保護を実現するための強力かつ標準的な手段と、適切な通知および権限付与を簡単に実現できるオプション手段を提供し、利用者個人の利益を最大限に維持する。

(3) このプライバシー・バイ・デザインは、EUデータ保護規則等の中にも取り入れられている。

日本においても、平成25年6月に、総務省の下に設置された研究会がとりまとめた「パーソナルデータの利用・流通に関する研究会報告書～パーソナルデータの適正な利用・流通の促進に向けた方策」において、

「パーソナルデータの利活用の基本理念を具体化するものとして、次の7項目をパーソナルデータ利活用の原則として提示する。

- ・透明性の確保
- ・本人の関与の機会の確保
- ・取得の際の経緯（コンテキスト）の尊重
- ・必要最小限の取得
- ・適正な手段による取得
- ・適切な安全管理措置
- ・プライバシー・バイ・デザイン

などと、「基本理念を具体化する原則」として導入されているものである。

(4) 以上のような情勢を踏まえて、日本の個人情報保護委員会委員長でもある堀部政男一橋大名誉教授は、「プライバシー・バイ・デザインが今や新しいグローバル・スタンダードになってきている」と紹介しているのである（「新しいグローバル・スタンダードとしてのプライバシー・バイ・デザイン」甲2・p.56～）。

(5) なお、上記7原則の根底には**データ最小化 (data minimization)**の概念、すなわち、個人情報収集、利用、提供および保有は、どこでも可能な限り最小化されるべきだという考え方があるとも説明されている。（「プライバシー・バイ・リデザインへの進化」甲2・p.78）。

### 3 プライバシー・バイ・デザインとプライバシー・インパクト・アセスメント (PIA) との関係

新保史生慶應義塾大学教授は、以下の様に説明する。（甲2・p.48～）

(1) PIAとは

プライバシー・インパクト・アセスメントとは、情報システムにおけるプライバシー保護策についての評価手法である。この評価を通じて盲点を見つけ、改善することで、個人情報の適正な取り扱いを確保し、個人のプライバシーを保護するための方策を最適なものに近づけられる。

(2) PIAの構造

PIAを実施する意義は、個人のプライバシーへの影響を最低限にするた



めに取り得る『方策』（制度面での対応）だけでなく、プライバシー・個人情報保護のために実施可能な『対応（技術的な対応）』までを検討することにある。制度面について言えば、不適合の原因を明らかにして体制を整備するなどの対応が可能になる。一方、技術面については、後述の『**プライバシー保護強化技術（P E T s）**』を利用した情報セキュリティ対策の必要性の有無を検討する基礎になる」と説明されている（同 p.49）

### (3) P I Aの実施対象

P I Aがもともと対象としていたのは、行政情報システムであった。ただ P I Aの目的は、情報システムの構築に当たって事前にプライバシーへの影響を評価すること。P b DにおいてもP I Aの実施は重要な要素であり、その場合の実施対象は、当然ながら公的組織には限定されない。

P I Aの実施が必要とされる背景には、公的権力による個人情報の一元的管理に伴う問題がある。例えば、ジョージ・オーウェルの『1984年』において『ビッグ・ブラザー』への懸念という形で示され議論されてきた。しかし今や、ビッグ・ブラザーだけでなく民間事業者においても、個人情報を取り扱う大規模なデータベースが構築されるようになっている。民間企業による『リトル・ブラザー』における情報の取り扱いも、公的権力による取り扱いに匹敵する影響力を持つ。P b Dを考えるうえでは、そのような大規模なデータベースを保有する民間部門の事業者も対象にすべきだろう。（同 p 49～50）

## 4 プライバシー保護強化技術（P E T s）とは

プライバシー保護強化技術（Privacy Enhancing Technologies、P E T s）とは、プライバシー保護を向上させるために利用される技術の総称である。具体的には、匿名による決済システム、通信の秘密を保障する匿名化技術、リアルタイムでの通信内容及び通信した事実の保護、匿名認証などである。（同 p.51）

## 5 小括～プライバシー・バイ・デザインに基づいて制度構築を行う義務

以上述べてきたように、現時点において大規模情報システムを構築するに際

しては、事前にプライバシーに対する影響を評価し、プライバシー保護強化技術を活用するなどして、プライバシー保護を最大限にはかりつつ、利便性を損なうことがないようなシステム開発を行うことが、日本を含めた「グローバル・スタンダード」となっているのであり、被告国もそのような手続きを踏むことが義務づけられているのである。

日本における大規模情報システムであるマイナンバーシステムにおいてもプライバシー・バイ・デザインに基づいた制度設計（PIAの実施や、それに基づくPETsの導入等を含む）がなされていないならば「グローバル・スタンダード」の安全性は確保されていないといわざるを得ない。

以下、その観点をも踏まえて、マイナンバーシステムについて何点か指摘する。

## 第2 日本マイナンバーシステムが、プライバシー・バイ・デザインに反し、基本的な安全性を欠いている典型例について

上述した枠組みに沿ってマイナンバーシステムを検討してみるならば、事前的・予防的な状態で安全性が確保されていないと言わなければならない。必要性も示されていないにも拘わらず、プライバシー保護にとって危険性の高い「共通番号制度」を採用していること、その背景には、制度設計に先立ってマイナンバー制度の仕組み自体のプライバシー影響評価（PIA）を行っていないこと等があげられる。

被告が主張する安全対策は、いわば情報提供nwsの中だけの安全対策に過ぎず、それ以外の現場の端末部分や、情報提供nws以外の部分では、それらの管理者等により“安全を確保することになっている”という建前論だけである。これでは国民と外国人住民のプライバシーの安全など、到底確保できない。また、一旦事故等が発生した場合に、リスクを許容できる程度に抑えるという制度設計になっていないと言わなければならない。

以下、その点が端的に表れている何点かについて指摘する。

## 1 制度・システム全体についてプライバシー影響評価を行っていない点

(1) 被告は、情報提供 n w s の運営に係る特定個人情報保護評価は行っている（乙 1 6）とか、個別機関毎の特定個人情報保護評価において、他の評価書のコピペやベンダーへの丸投げという報道については承知しているが、「評価実施機関が、特定個人情報ファイルを取り扱う事務における当該ファイルの取り扱いやリスク対策等について、それぞれの事務の実情に応じて、自らの責任において主体的に評価するものである」などと回答している（「回答書（2）」の 2（8）、（9）など）。

(2) しかし、本来の P I A は、上述したことから明らかなように、独立の専門的第三者機関が、システム構築に先だつて、プライバシーに対する影響を最小化するために、行うものである。

したがって、特定個人情報保護評価のように、システム構築後に、それぞれの機関が、自主評価するものは P I A とは評価し得ないものである。

さらに、システム全体について、総合的にプライバシーに対する影響を評価しなければ、プライバシーに対する真の影響評価とはなり得ない。その点は、例えば「環境影響評価」において、それぞれの工場から排出する汚染物質の量が基準値以下であっても、その地域の工場群全体としての排出量やそれぞれが排出する汚染物質の複合作用等の影響を評価しなければ、環境に対する真の影響評価たり得ないことと対比して考えれば、明らかである。

(3) したがって、このような「特定個人情報保護評価」が行われても、プライバシーの安全性が確保されているとは到底評価し得ない。

なお、日本年金機構は、年金情報流出問題を受けて、平成 2 8 年 6 月から 7 月にかけて個人情報保護委員会及び内閣サイバーセキュリティセンターによる検査等を受け、同年 8 月末までに端末の従前の共有フォルダ内の年金個人情報の移行・削除を実施したと報告した。これを受けて、政府は同年 1 1 月 8 日、サイバーセキュリティ対策が強化されたとして、同機構のマイナンバー利用を平成 2 9 年 1 月から認める政令を閣議決定した。しかし、その

後、会計検査院の指摘により、少なくとも13都府県の19施設で計78ファイルの年金個人情報等が消去されていなかったことが判明している（甲3・日本年金機構作成の文書）。

このことに示されるように、自主点検は極めて杜撰なものであり、専門的な第三者機関による徹底した点検を行うことは最低限必要である。

## 2 機関別符号で情報連携するにも拘わらず、各省庁においてマイナンバーを保有している点

(1) 原告らが、“機関別符号で（政府の目的とする）情報連携ができるのであるから、個人番号を各機関で保有しておく必要はないのではないか？”と求釈明したことに対して、被告は、「情報連携を行うためには、個人を悉皆性（住民票を有する全員に付番）を有する番号によって特定するため各情報提供者のシステム等において個人番号を保有し、情報照会又は情報提供を行うことを可能としておくことが必要である」（2(1)）と回答している。

(2) しかし、このような回答では、そもそも各機関に個人番号を保有しておく必要性について、何ら釈明したことにはならない。必要性もないのに、プライバシーにとって危険性の高い共通番号である個人番号を保存しておくことは許されない。

第1でも述べたように、プライバシー保護の観点からは（仮に保存しておく必要性があった場合でも）「データ最小化」を行うことが原則なのであり、これを行っていないシステムはプライバシーに危険性をもたらすシステムであると言わなければならない。

## 3 個人番号カードの券面に個人番号・性別を記載している点

(1) 原告らは、“多目的利活用がはかられている個人番号カード（マイナンバーカード）は、日常的に持ち歩くことにならざるを得ず、そのカードの券面に個人番号を記載することは危険ではないか。プライバシー保護の観点からは、（仮に個人を特定するマイナンバー自体が必要であるとしても、）マイナンバーの確認をするための「通知カード」と、多目的利活用のための「個

人番号カード」とは別物とするのがプライバシー保護対策としては最低限必要であり、かつ、容易に取り得る対策ではないか？”という求釈明を行った。この求釈明の趣旨は、文面を読めば明らかである。

しかし、被告は、あえてその趣旨を「曲解」し、通知カードと個人番号カードの「ワンカード化」をはかっている旨の回答を行った（4(2)）。

(2) しかし、この点もまったく危険性に対する疑問に答えていない。

カードの券面に個人番号を記載することの危険性は自明であるので、あえてこの点に関する再求釈明は行わないが、個人番号カードの券面に、日常的には使う必要がなく、かつ、秘匿すべきものである個人番号を記載し、さらに本人確認のためには必ずしも必要のない「性別」を記載したうえで持ち歩き、提示することを推奨する（身分証明書や健康保険証との一体化が制度化されれば、持ち歩き、提示することが義務化されることになる）制度にすることは、明らかにプライバシー保護に反したものとわざわざを得ない。

#### 4 地方公共団体情報システム機構（J-LIS）による「一元管理」の点

(1) 原告らは、J-LIS が、全国民及び外国人住民の本人確認情報（氏名、住所、生年月日、性別、住民票コード、個人番号）及びそれらの変更履歴、個人番号カードの発行に関する情報（写真情報を含む）等を一括集中管理しているとして、その安全性に関する求釈明を行った。

これに対し、被告は、「機構が様々な個人情報を一括集中管理しているという事実はないのであって、『同機構は、外国人を含む全住民の本人確認情報（中略）等を一括集中管理している』（求釈明書 12 ページ）とする原告らの主張はそもそも誤りである」と回答する。

(2) しかし、J-LIS がこれらの個人情報を管理していることは紛れもない事実なのであって、被告の回答は誤っている。（なお、原告らは、J-LIS において、情報提供 n w s で提供される特定個人情報を「一元管理している」という主張を行っているわけではない）。

住民基本台帳ネットワークシステム（住基ネット）の構築以前は、本人確認

情報は各市区町村で、各市区町村住民の分が「分散管理」されていた。それが、住基ネットにより、J-LIS の前身である地方自治情報センターにおいて、全国民分（全市区町村民分）の本人確認情報が一元管理されるように変わっている（なお、各都道府県にも、各都道府県の全市区町村民分の本人確認情報が一元管理されるようになった）。J-LIS はそれを引き継いでいるのであるから、「本人確認情報の一括集中管理」を行っているのは明らかである（なお、さらに、J-LIS が集中管理するようになった情報は、求釈明であげたように、地方自治情報センターが管理していた情報を上回るものである）。

全国民及び全外国人住民の本人確認情報及びそれらの変更履歴は、現代社会においてはビッグデータ処理の基本として活用できるなど、極めて価値の高い情報となっているほか、例えば、それらの変更履歴は身分関係の異動を推知させる情報であるなど、機微にわたる情報という性質も有している。したがって、その安全確保は極めて重大な問題である。

J-LIS は、この間の個人番号カード発行を巡る障害問題を発生させた組織であり、そこで保管管理される原告らの個人情報の安全性は厳格に審査されなければならない。

## 5 「一元管理」と「分散管理」についての理解を誤っている点

- (1) 被告は、マイナンバー関係の情報は「一元管理」されておらず、「分散管理」されている旨主張し、今回の「回答書」においても、地方自治体の中間サーバについて、「『1箇所の中間サーバに地方自治体の情報が全て集中する』、『一箇所の中間サーバに対する攻撃で、全ての地方自治体の情報が奪われてしまうという危険性が生じることになる』（求釈明書7ページ）という事実はない」（第2、7、イ）などと主張する。
- (2) しかし、この釈明は、「一元管理」・「分散管理」の物理的な意味と論理的な意味を取り違えており、誤っている。

すなわち、まず、地方自治体の中間サーバは、物理的な意味では、一箇所（＝東西2箇所のデータセンターのそれぞれ）に設置された中間サーバに集

約されているのであり、同所の中間サーバに地方自治体の情報が全て集中することになる。したがって、このデータセンターに対する物理的な攻撃がなされれば、そこにあるデータは全て奪われてしまう危険性が発生しているのである。被告の主張は、ネットワークのアクセス権限は各自治体にあるから、例えば、一つの自治体の権限を乗っ取っても、他の自治体の中間サーバにアクセスすることができないということを主張しているに過ぎず、その意味でかみ合った釈明になっていない。（なお、遠隔地からネットワーク経由でデータセンターのサーバに対する攻撃がなされて、管理者的な権限（いわばオールマイティな権限）が奪われた場合は、遠隔地からの攻撃も可能となるという危険性も発生している。）

反対に、ある機関の個人データが仮に3箇所にあるサーバで（物理的に）「分散管理」されていたとしても、これら3箇所のサーバがネットワークでつながっているならば、1箇所のサーバで「一元管理」している場合と変わらず、この機関の個人データは「一元管理」されていると評価しうるのである。この場合の「分散管理」の安全対策上のメリットは、物理的にある1箇所のサーバが攻撃されたとしても、他の2箇所のサーバのデータは奪われたりせず、安全であるという点になる。

### 第3 住民税特別徴収税額決定通知書に個人番号を記載することの問題点

原告らが、住民税特別徴収税額決定通知書に個人番号を記載して郵送することの危険性を指摘したことに対し、被告は、「番号利用法12条に基づき、個人番号利用事務等実施者は、個人番号の漏えい、滅失又は毀損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じなければならず、市町村において適切に送付され、特別徴収義務者においても、適切な受領及び管理が行われることとなる」と回答した（「求釈明に対する回答書（2）第7、2」）。

しかし、このような回答は、現実を見ずに、法令や制度がある以上、関係者はそれに従った安全対策を講じるはずであるという観念的な“机上の空論”を述べるに過ぎないものであり、まったく誤っている。

以下、詳論する。

## 1 住民税特別徴収税額決定通知書とは

市区町村は、毎年5月に、会社等の各事業者に対し、事業者の従業員等の給与から徴収する住民税額を通知している（以下、この通知を「特別徴収税額通知」という。地方税法43条）。

この通知書の書式は、地方税法施行規則2条により同規則第3号様式によるものとされているが、平成27年10月29日の総務省令改正により（総務省令第90号）、同様式が変更され、個人番号が記載されるものとされた（甲4、甲5）。

特別徴収税額通知は、これまで普通郵便で送付されているが、国・総務省は個人番号が記載されるようになっても、従前通り普通郵便で送付することを認めている（甲7のQ7に対するA7）。

## 2 総務省による通知、Q&Aの送付

(1) 平成28年11月25日付け「平成29年度分以降の個人住民税に係る特別徴収税額決定通知書（特別徴収義務者用）の送付に関する留意事項について（通知）」

上記の様式の変更に関して、総務省は、平成28年11月25日、各都道府県市区町村担当課に対し、平成29年度分以降の特別徴収税額通知書には、個人番号が記載されることとなったとして、当該通知書の送付に関して、「技術的な助言」（地方税法245条の4）として、留意事項を通知している（甲6）。

(2) 平成29年3月6日付け「特別徴収税額通知（特別徴収義務者用）への個人番号記載に関するQ&Aの送付について」

上記の通知の送付後も、後述のように、特別徴収税額通知書に個人番号



を記載しないとする市区町村が出てきた。すると、国・総務省は、平成29年3月6日に、各都道府県市区町村担当課に対し、「特別徴収税額通知（特別徴収義務者用）への個人番号記載に関するQ&A」を送付した（甲7）。同Q&Aには、市区町村の判断で個人番号欄を設けない様式とすることはできないとの回答（Q3に対するA3）や、個人番号の記載を不記載や一部不記載（アスタリスク表示を含む）とすることは認められないとする回答（Q4に対するA4）がある。

### 3 個人番号を記載した特別徴収税額通知書を送付する根拠、理由

#### (1) 根拠

国・総務省の説明によれば、市区町村が各事業者に対し、従業員の個人番号を記載した特別徴収税額通知書を送付することができる根拠は、番号法19条1号の規定であるとする。

すなわち、特別徴収税額通知書の送付は、個人番号利用事務実施者である市区町村が、個人番号関係事務実施者である特別徴収義務者たる各事業者に対し、「個人番号利用事務を処理するために必要な限度で」、特定個人情報を提供する場合に該当すると説明している（甲7のQ1に対するA1。求釈明に対する回答書（2）第7・2でも同様に回答）。

なお、特別徴収義務者たる事業者は、「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」（番号法9条3項）ことから、特別徴収通知により従業員の個人番号を取得したとしても、これを地方税に関する事務以外の事務（例えば、所得税に関する事務）に利用することはできないとされる（甲6・1頁）。また、この提供により従業員の個人番号取得が免除されることはなく、まだ個人番号を取得していない従業員については引き続き取得に努める必要があるとされる（甲6・1頁）。

#### (2) 理由

国・総務省の説明によれば、市区町村が各事業者に対し、従業員の個人番号を記載した特別徴収税額通知書を送付する理由は、「特別徴収税額通知に

個人番号を記載することにより、特別徴収義務者と市区町村との間で、正確な個人番号が共有されることにより、個人住民税の税務手続を通じて、番号法が目的とする公平・公正な課税や事務の効率化につながることを期待されるため」とされる（甲7のQ2に対するA2）。

#### 4 個人番号を記載した特別徴収税額通知書を送付することの危険性

上記のように、国・総務省は、個人番号を記載した特別徴収税額通知書を各事業者に送付するよう市区町村に求めている。

しかしながら、このような措置には下記のような様々な問題があり、個人のプライバシーを危険にさらすものである。

##### (1) 情報漏洩の危険

ア 前記のように、個人番号が記載された特別徴収税額通知書は、普通郵便で送付してもよいとされる。したがって、誤配送による漏洩の危険を否定できない（なお、周知のように各市町村から各世帯に送付された通知カードは簡易書留郵便で送付されている）。

イ また、特別徴収税額通知書は、一律に会社等の事業者に送付されるため、個人番号を収集していない、安全管理措置を講じていない事業者にも送付されることになり、事業者から漏洩してしまう可能性がある。このようなことは倒産、休眠、移転等している事業者に対して送付されることにより十分生じ得ることである。

ウ さらに、国・総務省は、事業者に対し、個人番号を取り扱う部署や担当者をあらかじめ定めるよう指導しているところ、会社等宛に送付された特別徴収通知書を担当者以外の者が開封し、適切な管理がされない等の理由により漏洩してしまう可能性がある。

この担当者以外の開封の可能性については国・総務省も認めるところであり、その対策として、総務省の通知では、市区町村に対し、「通知書の送付にあたり、特別徴収義務者において定める個人番号を取り扱うこととされた部署や担当者に確実に到達するよう、正確な送付先（宛名

)の把握をお願いします」としている(甲6・2頁)。

しかし、現場の市区町村の担当者が、多いところでは数万件に上る通知先の担当部署、担当者を把握するというのは不可能を強いるものであり(この総務省の指導によれば、市区町村において担当者の異動を毎年把握せよということになることを想像すれば明らかであろう)、行政運営の効率化という番号法の趣旨に真っ向から反するものである。

エ ウで述べた担当者以外の者の開封という事態は、個人番号の管理を外部委託している事業者についても同様に生じ得る。

オ 上記で述べたような漏洩の危険性について、原告は2016年11月15日付け求積明書7(2)において、積明を求めたが、被告は、普通郵便での送付を認めているのかという原告の求積明に正面から答えず、市区町村は番号法上、「個人番号の漏えい、滅失又は毀損の防止その他の適切な管理のために必要な措置を講じなければならず」、事業者においても「適切な受領及び管理が行われることとなる」というものであった(平成29年1月24日付け求積明に対する回答書(2)第7・2)。

しかしながら、このような被告の回答は、現実を見ずに、法令、制度がある以上、現実がそれに合致しているはずという根拠のない想定に立っているものであり、危険がないという理由にはなっていない。

(2) 事業者個人番号を提供していない従業員等の個人番号を事業者提供  
する問題

前記のように、個人番号付きの特別徴収税額通知は、一律に送付されることになるため、事業者に対して個人番号を提供していない従業員等の個人番号も、市区町村から事業者提供されることになる。国・総務省はその提供について従業員等の同意は不要としている(甲7のQ5に対するA5。平成29年1月24日付け求積明に対する回答書(2)第7・2において被告も認めている)。

しかしながら、事業者が個人番号を提供していない従業員等の個人番号を事業者に送付することは、後述のようにプライバシー権・情報コントロール権の侵害するものというべきである。

### (3) 行政の負担の問題

ア 特別徴収税額通知の送付に関して、市区町村は、個人番号利用事務実施者として、「個人番号の漏えい、滅失又は毀損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じ」る義務を負っており、個人番号の漏洩等に関し責任を負う立場にある（番号法12条）。

イ そのため、漏洩のリスク等を考慮して、市区町村が、当該通知書を普通郵便でなく簡易書留で送付することが考えられるが、それには相当の財政的、人的負担を伴うことになる。

例えば、通知を簡易書留で送ろうとすると、1通あたり310円余計に送付費用がかかることになる。人口89万人の世田谷区は約8万通を発送しており、約2500万円の負担増になる。

ウ 自治体の対応

漏洩のリスクと行政の負担を考慮して、自治体の中には、特別徴収税額通知書に個人番号を記載しないこととした自治体もある。

甲8の調査によれば、中野区、世田谷区、足立区、葛飾区など都内62自治体のうち30の自治体が、「個人番号を記載しない」又は「一部のみ記載（一部をアスタリスクで抹消表示）」と回答している（平成29年2月21日現在）。

例えば、中野区は、①「情報漏えいのリスク」、②「簡易書留で郵送する場合」の「郵送料」の「大幅な増大」及び③「受取までに日数を要し」「徴収事務に支障を来たすおそれ」を理由に、特別徴収税額通知書に個人番号を記載しないとしている（甲9、甲10・4頁）。

また、東京23区の税務課長会は、総務省に対し、特別徴収税額通知書に個人番号の記載をやめるよう要望している（甲10・5頁）。

## エ 国・総務省の対応

これに対し、国・総務省の対応は、あくまで、特別徴収税額通知書に個人番号を記載せよというものである。前記のように、総務省は、平成28年11月25日に「平成29年度分以降の個人住民税に係る特別徴収税額決定通知書（特別徴収義務者用）の送付に関する留意事項について（通知）」を出した（甲6）が、それでも個人番号を記載しないとした自治体があることを憂慮したのか、さらに平成29年3月6日に「特別徴収税額通知（特別徴収義務者用）への個人番号記載に関するQ&A」を出している（甲7）。

平成28年11月25日付け通知では「技術的な助言」（地方税法245条の4）として留意事項を通知していたのに対し、平成29年3月6日付けのQ&Aでは、市区町村の判断で個人番号欄を設けない様式とすることはできない（Q3に対するA3）、個人番号の記載を不記載や一部不記載（アスタリスク表示を含む）とすることは認められない（Q4に対するA4）としており、市区町村に対する締め付けを強めていることが分かる。このような国・総務省の姿勢は、市区町村による漏洩等の危険を回避する措置を妨害し、事実上危険な方法を強制するものである。

## 5 この問題から裏付けられる番号法の違憲性

(1) 以上のとおり、個人番号を記載した特別徴収税額通知書を送付することには様々な問題がある。ここから言えることは、単に国・総務省の方針が不当であるというに留まらず、下記に述べるように番号法の違憲性を裏付けるものと言える。

### (2) 目的の不明確性

そもそも、国・総務省が、市区町村の反対にも関わらず個人番号を記載した特別徴収税額通知書を送付させようとする目的は、前記のように、「特別徴収税額通知に個人番号を記載することにより、特別徴収義務者と市区町村

との間で、正確な個人番号が共有されることにより、個人住民税の税務手続を通じて、番号法が目的とする公平・公正な課税や事務の効率化につながることを期待されるため」（甲7のQ2に対するA2）というものであった。

極めて抽象的かつ曖昧な説明であり、上記で述べたような漏洩等のリスクがあるにもかかわらず送付を行う理由となっていない。①「特別徴収義務者と市区町村との間で、正確な個人番号が共有されること」という原因と②「番号法が目的とする公平・公正な課税や事務の効率化につながることを期待される」という結果の因果関係が全く不明である。

### （3）目的とは反対の事務の負担を生むこと

むしろ具体的に見ていくと、行政にとっては「事務の効率化」とは反対の負担を負うことになることは前記のとおりであるし、事業者にとっても、特別徴収通知により提供された個人番号は、「地方税に関する事務以外の事務に利用することはでき」ず、「特別徴収税額通知書により、従業員の個人番号の提供を受けることをもって特別徴収義務者における個人番号の取得が免除される訳ではなく、個人番号を取得できていない従業員については、引き続き、個人番号の取得に努めていただく必要がある」（甲6・1頁）ことから、事務の効率化につながるとはいえず、却って、個人番号を別に保管・管理しなければならないことになり、事務の負担が増えることになる。

### （4）番号法の違憲性

したがって、このような目的で個人番号が記載された特別徴収税額通知書を送付することに、個人番号利用事務を処理するための必要性があるとは全く認められず、国・総務省が説明するように、番号法19条1号の「個人番号利用事務を処理するために必要な限度で」に該当するとは到底言えない。

もっとも、仮に国・総務省が述べるように、上記のような極めて抽象的かつ曖昧な目的で個人番号（特定個人情報）送付することが番号法19条1号により可能だとすると、次のことが言える。

すなわち、番号法は、上記のような極めて抽象的かつ曖昧な目的で、漏洩

等のリスクがあるにもかかわらず、個人番号（特定個人情報）を市区町村から事業者に対し、本人の同意なく、送付することを可能とする法律ということになる。そして、その扱いは、事業者に対し個人番号を提供しているか否かに関わらず可能ということになる。

したがって、このような個人番号（特定個人情報）の提供を可能とする番号法は、正当な目的無く、かつ目的との手段との関連性もなく、個人のプライバシー権・情報コントロール権を制約するものであり、憲法13条に反し違憲というべきである。

以上