平成２７年（ワ）第１６３２号，平成２８年（ワ）第３６４号
マイナンバー（個人番号）利用差止等請求事件
原　　告　三戸部尚一　外８名
被　　告　国

準　備　書　面（４）

（特定個人情報保護評価制度の不十分性）

２０１７（平成２９）年9月１５日

仙台地方裁判所第１民事部合Ａ係　御中

原告ら訴訟代理人弁護士　野　呂　　圭

同　　　　　　弁護士　齋　藤　信　一

同　　　　　　弁護士　十　河　　弘

同　　　　　　弁護士　宇　部　雄　介

外

（目次）

第１　はじめに

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。

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。なぜなら，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）現在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，個人情報が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（２）２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（もっとも，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２　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ように説明している。

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（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，②プライバシー保護は初期設定で有効化されること，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，④全機能的であること。ゼロサムでなくポジティブサム，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，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，⑦利用者のプライバシーを最大限に尊重すること。後記２(2)参照。）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５・『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（FIP ｓ：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５・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，２０１０（平成２２）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５・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)③ｂ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５・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様に，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，２０１３（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。

(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５・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５・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５・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（ＰＥＴｓ)』**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)　ＰＩＡの実施対象

ＰＩＡ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ＰＩＡ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。ＰｂＤにおいてもＰＩＡ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。

ＰＩＡ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。ＰｂＤ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（ＰＥＴｓ）とは

プライバシー保護強化技術（Privacy Enhancing Technologies，ＰＥＴｓ）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，匿名による決裁システム，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）がなされていなければ「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３　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

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かかわらず，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などが挙げられる。

被告国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は到底確保できない。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)　被告国は，情報提供ｎｗｓの運営に係る特定個人情報保護評価を行っているとか，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（原告求釈明申立書（２）添付の被告から別紙２の回答書（２）の２０頁など)。

(2)　しかし，本来のＰＩＡは，上述したことからも明らかなように，独立の専門的第三者機関が，システム構築に先だって，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ＰＩＡ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，２０１６（平成２８）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１１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２０１７（平成２９）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６）。

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)　東京地裁原告らが，“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，被告国は，「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」（原告求釈明申立書（２）添付の被告から別紙２の回答書（２）の１４頁）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２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ざるを得ない。

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)　東京地裁原告らは，“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，被告国は，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」をはかっていない旨の回答を行った（原告求釈明申立書（２）添付の被告から別紙２の回答書（２）の２４頁)。

(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言わざるを得ない。

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)　東京地裁原告らは，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，被告国は，「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』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，被告国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ｎｗｓ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)　被告国は，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」（原告求釈明申立書（２）添付の被告から別紙２の回答書（２）の１７頁）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。

以　上