

# マイナンバー制度とプライバシー

～違憲訴訟で問題となったこと

報告の骨子  
はじめに

- 1 マイナンバーとマイナンバーカード
- 2 共通番号制の利便性とプライバシーへの危険性
- 3 裁判で問題になったこと
- 4 さいごに

2023年9月10日

弁護士 水 永 誠 二

# はじめに

## マイナンバー制度を巡り、さまざまな問題が噴出

- ・システム設計の誤り → コンビニの多目的端末で他人の住民票が出てきた
- ・マイナ保険証で、被保険者資格のひもづけ誤り → 他人の投薬履歴の閲覧
- ・保険資格が表示されなかった → 10割負担
- ・介護施設入居者や独居高齢者・障害者がマイナンバーカード（マイナ保険証）を取得できない。パスワードを管理できない → この人たちの医療をどうするか、など

## どういう問題か？

政府が、現場の実情を踏まえずに、上からの強引で・急速なマイナンバーカード普及促進。その背後には、プライバシー保護に重きを置かないまま、急速にデータ利活用（特に医療データ、教育データ）をはかるための「デジタル化」推進という**データ戦略**の存在

⇔ **誰一人取り残されないデジタル社会の実現**  
**プライバシーの保障**

## データの利活用とプライバシー保障の両立はなかなか難しい

ここでいう<プライバシーの保障>・・・漏洩問題は直接的だが従。  
一番深刻な問題は、個人情報（個人データ）が集められて、同一人の情報であると突合（データマッチング）され、個人像が分析されてしまう（プロファイリング）こと。  
これによる、国（行政）による個人情報の一元化による「監視社会」化の危険性。  
さらに、「萎縮効果」の発生の危険性 ⇒ 民主主義社会の前提を掘り崩すもの。

# 1 マイナンバーとマイナンバーカード（正式には「個人番号」「個人番号カード」）

（前提）2つは関連はするものの別物

マイナンバーは、12桁の個人識別番号(利用事務分野を越えた背番号 = 共通番号)

マイナンバーカードは a) 身分証明書(氏名、住所、生年月日、性別と顔写真が表面に記載) と、

b) マイナンバー証明書（裏面に記載）

+ c) 公的個人認証機能を搭載した多目的ICカード（ICチップ搭載で、電子証明書を格納（なお、電子証明書はマイナンバーと無関係）

- ・政府は「デジタル社会のパスポート」として多目的利用化を図ると同時に、全国民（外国人住民含む）に、2023年3月末までに取得させることを目標化。
- ・そのために、1兆8000億円もの予算を付け、高額のポイント付与なども実施。
- ・さらに、2024年秋には、「マイナ保険証の義務化」を表明 →それでも4人に3人止まり

（表面）

顔写真  
氏名  
住所  
生年月日  
性別



（裏面）

マイナンバー

ICチップ



総務省HPより

## 2 共通番号制の利便性と危険性

### 【2-1 共通番号（利用分野を越えた個人識別番号）の利便性・機能性】

a もともと、本人確認情報（氏名、住所等）は、住民基本台帳（住民票）の情報として、市区町村限りで保管

b 市区町村では、当該市区町村の住民に対して、独自の住民番号を付けて住民データを管理。（紙の簿冊時代から）

c 名寄せ・突合の必要性

→ex. 障害者に対する社会保障手当てを出す資格として、所得制限がある場合、障害者であるという住民データ（福祉課などで管理）と、その人の住民税データ（住民税課などで管理）とを、名寄せして突合（データマッチング）する必要がある。

d 名寄せ・突合の手段

→ <同一人の情報である> ことを確認するために通常使うのは、本人確認 4 情報（氏名、住所、生年月日、性別）

しかし、氏名は、婚姻等を契機に変更される。また、例えば、「斉藤」「斎藤」「齋藤」などと漢字表記が統一されていない。同姓同名の他人も存在する。住所も、引越のたびに変更される。性別すら変わる可能性がある。

**4 情報によって、個人情報をも、漏れなく、かつ、他人と間違ふことなく、正確に名寄せ・突合することは事実上不可能**



**全住民に、漏れなく・重複せずに付番された住民番号（個人識別番号）を割り振れば**、例えば、「1 2 3 4 番」は何人もいる「斎藤和雄」さんのうちの特定の一人と確実に特定できる。また、1 2 3 4 番という番号にひもづけられた個人情報（障害情報や地方税情報など）も、確実に名寄せ・突合できる。つまり、1 2 3 4 番にひもづけられた個人情報は、漏れなく・他人と間違ふことなく・正確に、名寄せ・突合（データマッチング）すること（その上でプロファイリングすること）が可能となる。

	氏名	住所	識別番号	各種個人情報
1	齋藤和雄	A市中町 1 - 2 - 3	1 2 3 4	健康診断情報
2	齋藤和雄	A市北町 2 - 2 - 3	3 4 5 6	地方税情報
3	齊藤和雄	A市南町 3 - 4 - 5	4 4 5 6	家族情報
4	齋藤和雄	A市北町 2 - 2 - 3	6 6 2 3	障害者情報
5	齊藤和雄	A市西町 2 - 3 - 4	1 2 3 4	破産者情報
6	坂本和雄	A市東町 1 - 3 - 4	1 2 3 4	地方税情報

(今回のマイナ保険証のひもづけ間違いは、この1 2 3 4番を、同姓同名、同一生年月日の、別の「齋藤和雄」にひもつけてしまったという問題。基本的にこの番号と特定の個人にかかる個人情報のひもづけ自体（ないしは、最終確認自体）は、人の力でやらざるを得ない。)

これを、日本全国的に行おうとしたのが、**住民票コード**（11桁の個人識別番号）

国内の全住民に対して、重複しない住民票コードという背番号を付けて管理すれば、データの管理も突合（データマッチング）も迅速・確実にできるようになる。

(※ この「住民票コード」を暗号変換して作ったのが、**マイナンバー**（12桁の個人識別番号）)

## 【2-2 共通番号（利用分野を越えた個人識別番号）の危険性】

### （1）ビッグデータの利活用の進展

- ・膨大なデータを統計学を利用して、意味のある事象の関連性を見つけ出す。

#### 有名な米国の例（商業利用）

スーパーマーケットなどを全国展開するA社は、大量の顧客データ（ビッグデータ）を解析して、（特定の年齢層に含まれる女性で、無香料性のスキンローション、特定のサプリメント、大きめのバッグなどの商品を同時期に購入した者は、妊娠している可能性が高い）という「パターン」を抽出・発見

- このような「パターン」を、自社の保有する巨大な顧客データベースに当てはめ、  
その中から妊娠している顧客を予測し、彼女たちに対してのみベビー用品のクーポン券を送付。

（『おそろしいビッグデータ 超類型化 A I 社会のリスク』（山本達彦著、朝日新書）

#### 有名な政治利用の例（ケンブリッジ・アナリティカ事件・2016年）

- ➡ターゲットをピンポイントで狙い、巧妙に情報を送れば、ある政策・候補者に投票するように誘導することも可能！  
（英国のEU離脱、米国大統領選挙で、フェイスブック利用情報を分析・利用して誘導）



国（行政）による個人情報の一元化による「監視社会」化の危険性。

さらに、「萎縮効果」の発生の危険性 ⇒民主主義社会の前提を掘り崩すもの。

データを握るものが権力を握る⇔「番号をつけられたものは番号にふさわしい扱いしか受けない。」（斎藤貴男氏）

## (2) 参考～プロファイリングが進んだ監視社会・中国

### 【監視社会】

**スマホ決済の進展** アリババの「アリペイ（支付宝）」とテンセントの「ウィーチャットペイ（微信支付）」で90%以上のシェア

- ・杭州の名刹には賽銭箱にQRコードが貼ってあり、スマホをそれにかざすだけで好きな額を納められる。
- ・クレジットより利用手数料が安い（クレジットの3～5%に対し、アリペイではわずか0.6%）

### アリババグループの信用情報機構 芝麻（ジーマ）信用 による格付け

「身分特質」「履約能力」「信用歴史」「人脈関係」「行為偏好」の5項目について個々人の点数を算出し、総合点で格付け。

（銀行の伝統的信用データではカバーしきれなかった信用カードのない者、学生、自由業者などの個人情報も網羅して評価）

700～950 極好

650～700 優秀 650点以上はシェアサイクルや電気自動車の保証金不要などの優遇

600～650 良好

550～600 中等

350～550 較差

### 【監視国家】（上記の情報も、当然、国が収集している）

全国で1億7000万台の監視カメラ 生体認証機能付き 警察官も生体認証機能付き眼鏡型カメラ

監視カメラに写れば、直ちに個人認証され、行動が監視される・・・『1984』を超える世界が現に到来している。

### ■プライバシーの丸裸化——それを利用した誘導

→自律した個人を前提とする民主主義の基盤の掘り崩し ← 自己情報コントロール権の確立

### 3 住基ネット裁判、マイナンバー裁判で問題になったこと

- 2002年 8月 住基ネット違憲訴訟開始
- 2005年 5月30日 金沢地裁判決 違憲判決
- 2006年11月30日 大阪高裁判決 違憲判決
- 2008年 3月6日 最初の住基ネット訴訟最高裁判決
- 2015年12月1日 マイナンバー違憲訴訟開始
- 2023年 3月 9日 最初のマイナンバー訴訟最高裁判決

#### 3-1 住基ネット裁判の論点

- 1 憲法13条で保障される権利は何か？ プライバシー権 = 自己情報コントロール権は保障されているか？
- 2 侵害態様について
  - a 「原告らの同意なき市区町村外への提供等による侵害」
  - b 特にデータマッチングはプライバシー侵害であることを強調した



### 3-2 住基ネット訴訟 金沢地裁判決のポイント (大阪高裁判決もほぼ同旨)

行政機関は、住民個々人について膨大な情報を持っているところ、これらは、住民個々人が、行政機関に届出、申請等をするに当たって、自ら開示した情報である。住民個々人は、その手続に必要な限度で使用されるとの認識のもとにこれらの情報を開示したのである。

ところが、これらの情報に住民票コードが付され、**データマッチング**がなされ、**住民票コードをマスターキーとして名寄せ**がなされると、住民個々人の多面的な情報が瞬時に集められ、**比喩的に言えば、住民個々人が行政機関の前で丸裸にされるが如き状態になる。**

これを国民総背番号制と呼ぶかどうかはともかくとして、そのような事態が生ずれば、あるいは、生じなくとも、住民においてそのような事態が生ずる具体的危険があると認識すれば、住民一人一人に**萎縮効果が働き**、個人の**人格的自律が脅かされる結果**となることは容易に推測できる。

そして、原告らが上記事態が生ずると具体的危険があると認識していることについては相当の根拠があるというべきである。

### 3-3 2008年3月6日 住基ネット最高裁第1小法廷判決のポイント

**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」（1969年京都府学連事件判決を引用）**・・・開示・公表のみ**

#### 最高裁判決が合憲の理由としてあげた要素

①「住基ネットによって管理、利用等される本人確認情報は・・・いずれも、個人の内面に关わるような秘匿性の高い情報とはいえない」、「住民票コードは、住基ネットによる本人確認情報の管理、利用等を目的として、都道府県知事が無作為に指定した数列の中から市町村長が一を選んで各人に割り当てたものであるから、上記目的に利用される限りにおいては、その秘匿性の程度は本人確認情報と異なるものではない」**・・・情報の性質**

② a 本人確認情報の管理、利用等は、法令の根拠に基づく b 住民サービスの向上及び行政事務の効率化という正当な行政目的の範囲で行われている c 外部から不当にアクセスされるなどして本人確認情報が容易に漏えいする具体的危険性がない d 懲戒処分又は刑罰をもって目的外利用や秘密の漏えい等が禁止されている、都道府県に本人確認情報の保護に関する審議会、指定情報処理機関に本人確認情報保護委員会を設置して、本人確認情報の適切な取扱いを担保するための制度的措置を講じている**・・・安全確保措置**

ことなどから、**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又は正当な行政目的の範囲を逸脱して第三者に開示や公表される具体的危険が生じているということもできない**

e 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しない

③「行政機関が住基ネットにより住民である被上告人らの本人確認情報を管理、利用等する行為は、**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はできず**、当該個人がこれに同意していないとしても、憲法13条により保障された上記の自由を侵害するものではないと解するのが相当である。」

### 3-4 住基ネット制度とマイナンバー制度の異同

	項 目	住基ネット制度	マイナンバー制度
1	全住民に、漏れなく、重複しない番号か	○	○
2	番号は変更可能か？	○（自由に変更可）	×（原則生涯不変）
3	使用場面	原則、行政内部	民－民－官で利用
4	データマッチングシステムの存否	×	○（情報提供ネットワークシステム）
5	ICカード（公的個人認証）	○（住基カード）	○（マイナンバーカード）
6	ICカードの多目的利用	△	○
7	マイナポータル（情報閲覧ポータル）	×	○

両者の基本は同一。マイナンバー制度の方が利活用重視。  
 住基ネット制度で、小さく産んで大きく育てようとして失敗したので、マイナンバー制度で民間利用も含めて実現しようとした。

## 3-5 マイナンバー違憲訴訟

全国8地裁 2015年12月1日（仙台、新潟、金沢、東京、大阪） 2016年3月24日（神奈川、愛知、九州）提訴  
2023年3月9日 九州、愛知、仙台訴訟について最高裁第1小法廷判決（合憲判断）

### 【論点】

#### 1 被侵害権利利益について（憲法13条で保障される権利）

a : 「自己情報コントロール権」と併せて、

b : 「自己に関する情報をみだりに収集・保管・利用ならびに第三者に開示または公表されない自由」

（2008年3月6日住基ネット最高裁判決を前提にしての主張）

#### 2 侵害態様について

a 「原告らの同意なき収集・利用等による侵害」

b 「①漏洩、②データマッチング、③なりすまし」

・・・テロ対策名目等による一元的データマッチング(プロファイリング) の危険性も含む

「マイナンバー（制度）はまさに、現代的プロファイリングのインフラであり、マイナンバーを活用した場合の現代的プロファイリングによる個人の権利侵害の危険性は極めて高い。

### 3 違憲性判断基準

#### A 目的の重要性、手段の相当性に関する厳格審査基準

#### B 住基ネット最高裁判決に基づく「構造審査」基準

マイナンバー制度に、①**システム技術上または法制度上の不備**があり、  
②そのために特定個人情報<sup>が</sup>法令上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、収集・保管・利用、または、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、憲法13条で保障されたプライバシー権や人格権が侵害されると主張  
・・・住基ネット事件最高裁判決の「基準」を基に、山本達彦慶応大学法科大学院教授の主張する「**構造審査**」

### 制度(システム)の危険性（「不備」）として主張した点

#### 0 前提：制度（システム）の「不備」は、どの範囲を対象に考えるか？

➔ マイナンバーが利用される、民－民－官 のすべての範囲。  
情報提供ネットワークシステムだけが対象ではない。  
(この点が、住基ネットとは全く異なる・・・「概念図」参照)

#### 1 根本的な構造的「不備」である「**共通番号**」制度 ↔ **分野別番号制度**

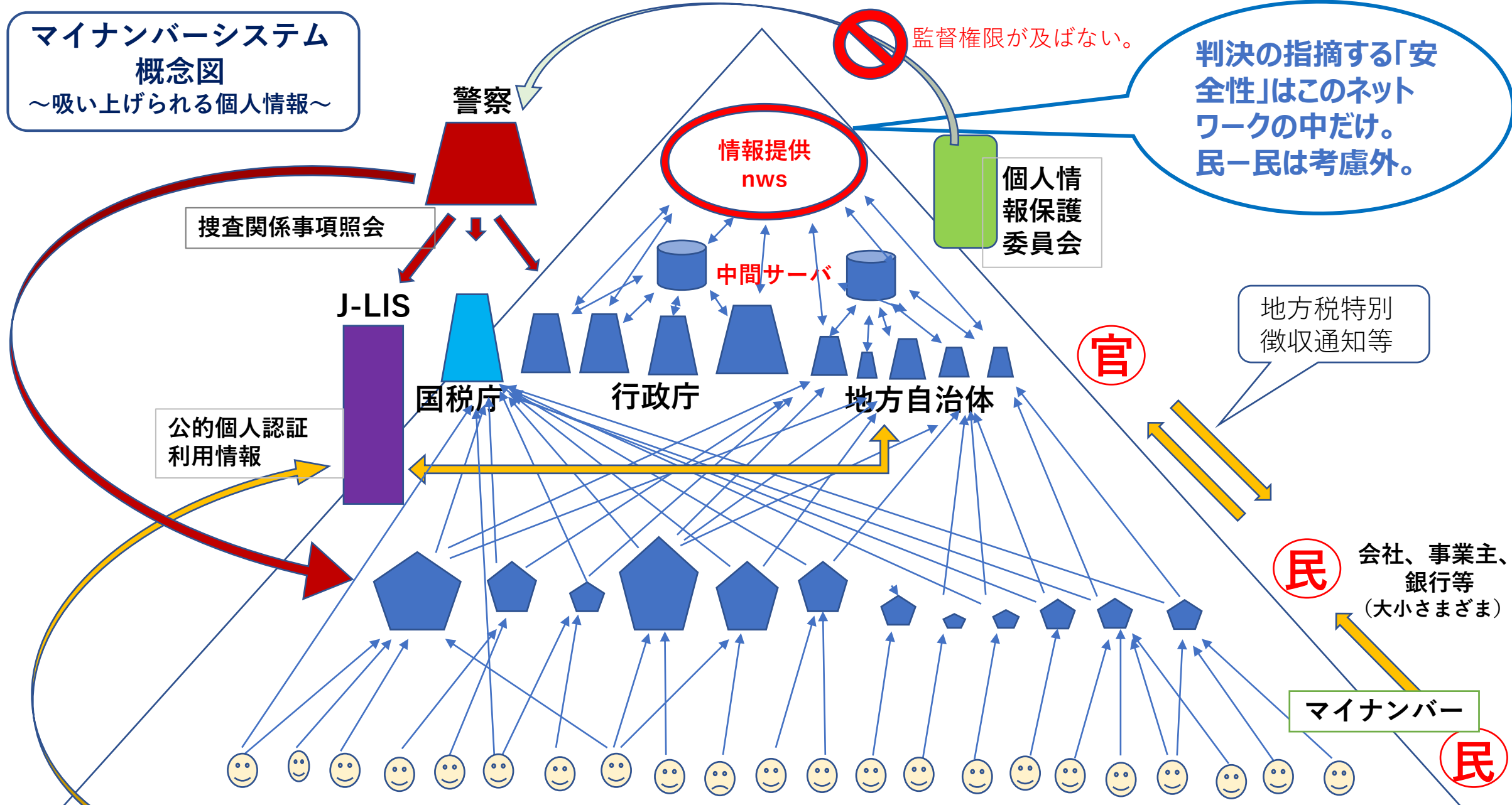
#### 2 **情報提供ネットワークシステム**における情報連携には「**機関別符号**」を用いる（＝マイナンバーを用いない）としながら、共通番号制を採るという「不備」（※オーストリアの制度参照）

#### 3 民間も含めた**セキュリティ**を高度に保つことは困難であるという「不備」

➔民－民－官のそれぞれの規模も財力もさまざまであり、セキュリティの高位平準化は無理。  
(概念図参照)

- 4 **個人番号カード**の券面にマイナンバー及び性別等の記載をし、そのカードの利活用を図って、持ち歩かせるようにしている「不備」
  - カードの利活用を図ることにより、危険性も著しく高度化  
**健康保険証との一体化による事実上の義務化**、印鑑登録カード、性別記載と性同一性障害の方 etc.
- 5 行政のシステムは**全部ネットワークでつながっている**ため危険性が高いという「不備」
  - 住基ネットの時代からさらにネット化が進んだ現場 (ex. タブレットの利用)
- 6 **警察**によるマイナンバーを利用した個人情報収集に制約がない「不備」
  - 番号法19条15号、36条 (適用除外・概念図参照)
- 7 **J-LIS (地方公共団体情報システム機構)** への**情報集中**という「不備」
  - 本人確認4情報、変更履歴、住民票コード、マイナンバー、個人番号カードの顔写真、公的個人認証等
- 8 プロファイリング (データマッチング) の**防止措置**がない「不備」
  - 自己情報コントロール権が確立していない+個人情報保護委員会の非力さ  
番号法19条15号「刑事事件の捜査」「政令で定める公益上の必要があるとき」 (P b d)  
「テロ捜査」名目をつけられたら・・・⇔cf. EUのデータ保護原則、プライバシーバイデザイン
- 9 **なりすまし**の危険性(マイナンバーカードとパスワード窃盗など)が高いという「不備」
  - マイナポータルが普及すればするほど、なりすまされ、情報が盗まれたり、何らかの手続きをされたりする危険性が高まる。

マイナンバーシステム  
概念図  
～吸い上げられる個人情報～



# オーストリアの情報連携システム

～分野別番号制でプライバシーに配慮しつつ、機能的な情報連携を実現

『国民ID 導入に向けた取り組み』（NTT出版）  
61頁の図を基に作成

非常に複雑そうに見えるが、実際には簡単なボタン操作で行われている。

中央住民登録簿  
CRR

③CRRは一致する「氏名」のCRR番号を回答。

②DSKは、送信された「氏名」のCRR番号を照会。

データ保護委員会  
DSK

④DSKは、人物XのCRR番号からソースPINを生成したうえで、ssPIN 2（機関Bの分野別番号）を計算

⑤DSKは、ssPIN 2 を機関Bの公開鍵で暗号化して、機関Aに通知

①機関Aは、データが欲しい人物Xに関する「氏名」「機関Aの分野別番号（ssPIN 1）」「機関Aの分野コード」を送信

⑥機関Aは、暗号化されたssPIN 2とともに、人物Xに関するデータを照会

行政機関B

住民データは分野別番号（ssPIN 2）で管理

行政機関A

住民データは分野別番号（ssPIN 1）で管理

⑦機関Bは、人物Xに関するデータを返送



## 3-6 住基ネット訴訟判決をなぞったマイナンバー違憲（九州）訴訟最高裁判決(1)

### (a) 憲法13条によって保障される権利（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  
住基ネット判決とまったく同じ（住基ネット訴訟最高裁判決を引用）  
★自己情報コントロール権（自己情報決定権）を認めないどころか、  
高度情報化社会になっている現代において、1960年代の人権論！

(b) 「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」として、以下の要素を挙げた。（★この順番も住基ネット判決と同じ）

#### ① 正当な行政目的を有するものということができる。

「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を限定するとともに、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、・・・番号利用法は、特定個人情報の提供を原則として禁止し、制限列挙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うことができる。」

※ これに続いて、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ことについて論及。

# 住基ネット訴訟判決をなぞったマイナンバー違憲（九州）訴訟最高裁判決(2)

## c) 住基ネット判決と違っているところはどこか（10頁の「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・・・のとおり・・・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・・・監視、監督等を行わせることとしている。」などとして、結局、「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。」として、

「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」と結論した。

# 住基ネット訴訟判決をなぞったマイナンバー違憲（九州） 訴訟最高裁判決(3)

- ★1 マイナンバー制度が秘匿性の高い情報のデータマッチングを目的とした制度であるので、どうしてもその危険性自体は一定言及せざるを得なかった。
- ★2 この危険性を認めながら、安全確保措置については、住基ネットと同様の、形式的な安全措置を羅列して、具体的な危険はないと結論。
  - ← あまりにも甘い認定ではあるものの、利用分野を3分野に限定しているなど、厳格な規制をしているから危険性はないのだ、という理由付けをせざるを得なかった。
    - ⇔ しかし、2023年6月のマイナンバー法改正で、3分野限定を撤廃「その他の行政分野」を入れる。（3条2項 社会保障制度、税制、災害対策その他の行政分野における利用の促進を図る）
- ★3 請求を認めないためのトリック
  - = 総論において、憲法13条で保障される「自由」に「利用」の場面を入れていない理由
  - 入れると、個人番号（共通番号）を付したことによる行政機関内部でのデータマッチングによるプロファイリングの危険性（ひと言で言うと「監視国家化」の危険性）、個人情報の利用における大きな質的变化（インデックス機能を利用したデータマッチング、プロファイリング）について問題とならざるを得ない（玉蟲由樹教授、山本龍彦教授等）。
    - 「提供」場面だけの保障にすれば、法令の認めない提供・漏えい等さえなければ良い、と持って行ける。

## 4 さいごに

マイナンバー制度・日本のデジタル化に欠けているものは？

～GDPR（EU一般データ保護規則）を参考に

0 そもそも、任意取得が原則のマイナンバーカードを保険証と一体化して、事実上の所持義務化にするなどの問題点

1 プライバシー（自己情報コントロール権）の確立が必要

EU基本権憲章8条では、基本権としてのpersonal dataの保護を規定

GDPRはそれを受けて制定されている。

日本では、基本的人権として確立していない。（それをサポートする個人情報保護委員会の強化も必要）

2 プライバシー・バイ・デザイン（PbD）の考え方の定着が必要

=設計(Design)段階から組み込むプライバシー保護

…カナダ、EUなど世界のプライバシーコミッショナー（日本では個人情報保護委員会）でスタンダードな考え方

GDPR25条 プライバシー・バイ・デフォルト

日本では、利活用に前のめり（AIの利活用を巡っても同様）

（そもそも、「マイナ保険証の事実上の義務化」で露になったように、「デジタル弱者」のことすら念頭に置かずに制度設計を行い、強引に進めようとしている。⇔「誰一人取り残されないデジタル社会の実現」）

3 PbD実現のためには、プライバシー影響評価の義務化も必要

=環境影響評価のプライバシー版…制度、システムを作るに先立って、プライバシーに対する影響を評価して、最小化する。

それにより、後で問題が発覚し、膨大な作り直し費用がかかることも防止できる。

…GDPR35条 データ保護影響評価

日本の「特定個人情報保護評価」は、自己評価に過ぎず、内容も薄い。