

平成27年（ワ）第570号 マイナンバー離脱等請求事件

原告 坊 真彦 外49名

被告 国

第3 準備書面

平成29年3月7日

金沢地方裁判所民事部合議A係 御中

原告ら訴訟代理人弁護士 岩 淵 正 明

第1 はじめに

本書面では、マイナンバー制度開始前の2015年10月頃から現在に至るまで、マイナンバーを巡る事故が多発しており、原告らのプライバシー情報が侵害される具体的危険性が生じていることを主張する。

これは、被告の「システム技術上又は法制度上の不備があり、そのために個人番号及び特定個人情報が…第三者に開示又は公表される具体的危険性が生じている事実はない」との主張に対する反論及び訴状で主張した「マイナンバー制度の本質的危険性」の裏付けとなる。

第2 マイナンバー制度に関して実際に発生している事故例

マイナンバー制度開始前の2015年10月頃から現在に至るまで、報道されただけでも、以下の通り、多くの情報漏洩及びその危険があった。ただし、

これらは、あくまで報道から得られる情報のみによるものであり、報道されていないもの、発覚していないものも存在すると考えられる。それらを含めれば、マイナンバー制度に関する事故例はさらに増える。

なお、地方公共団体情報システム機構（以下「機構」という。）とは、番号法8条1項の市町村長からの求めに応じて、電子情報処理組織を使用して、同条2項に掲げる要件に該当する個人番号を生成し、当該市町村長に対し、通知する機関である。

また、以下では、マイナンバーカードについて、「個人番号カード」という（もともと、第2の1(3)ケのような例外的な記載もある）。

1 行政部門からの特定個人情報漏洩

(1) 住民票へマイナンバーを記載した事故例

ア 2015年10月13日、茨城県取手市は、住民票を発行する自動交付機の設定ミスにより誤ってマイナンバーを記載した住民票69人分を発行したことを明らかにした。取手市によれば、マイナンバー制度が始まる同月5日から住民票を発行する自動交付機のシステムが切り替わるように、市の委託業者が同月3日に設定作業を行ったが、マイナンバーを記載しないようにする設定を怠っていたとのことである。同様のミスは、福島県福島市、北海道札幌市でも発生した（甲3の1～3）。

イ 2016年2月12日、北海道帯広市が請求されたものとは別の市民のマイナンバーが記載された住民票を誤って郵送していたことが判明した。帯広市によれば、同月1日、戸籍住民課の男性職員が、北海道外の企業が業務目的で請求した市民の住民票をプリンターで印刷した。他の職員もほぼ同時に別の市民の住民票を印刷しており、取り違えたとのことである（甲3の4）。

ウ まとめ

上記の事故例は、住民票にマイナンバー、すなわち個人番号を記載して発行してしまったというものである。以下の通知カードと同様に、住民票には氏名、住所、生年月日、性別等が記載されており、上記第2の1(1)イの事故例のように、住民票に個人番号が記載されたものが発行され他者の手に渡れば、どの人物にどの番号が割り振られたか等、個人情報と個人番号が同時に漏洩することにより個人の識別は容易に可能となってしまう。

また、上記第2の1(1)イの事例のように、個人番号が記載された住民票が他者の手に渡ることは、故意にせよ過失にせよ、他者に対して、個人番号を提供したことと同じ結果になってしまう。そうだとすれば、法令上の正当な目的の範囲を超えた個人番号の利用や特定個人情報の提供をしてしまったのと同じ状態が出現してしまっているのである。

(2) マイナンバー通知カードの作成・発行における事故例

マイナンバー通知カード（以下「通知カード」という。）の作成・発行の場面においては、以下のような事故が発生している。

ア 2015年12月4日、高市早苗総務相は、東京都葛飾区白鳥地区の約5000世帯分の通知カードがミスで作成されていなかったことを明らかにした（甲3の5）。葛飾区役所が機構に提出した住民データが、何らかの理由で国立印刷局での印刷工程に送られていなかったことが原因と考えられる。

イ 2015年12月、滋賀、静岡、秋田3県の5市町村で184人分の通知カードの印刷漏れが新たに判明した（甲3の6）。内訳は、滋賀県日野町156人分、同県多賀町8人分、同県愛荘町4人分、静岡県熱海市12人分、秋田県潟上市4人分である。原因は自治体側の事務処理ミスである。このうち日野、愛荘両町では印刷に必要な住民情報の管理に不備があった。

ウ 2015年12月16日、大阪市は、マイナンバーを記載した通知カー

ドにつき、天王寺区に住む1977人分が作成漏れとなり、未送付になっていたと発表した（甲3の7）。

データ作成はNTTデータ関西に委託されており、通知カードは世帯ごとに発送するため、データも世帯別に作成する。そして、住民基本台帳で世帯主が空欄になっている児童福祉施設の入所児童については抜き出してデータを作る作業が必要だが、NTTデータ関西が抽出ソフトの設定を誤ったため、世帯主が空欄でない1967人と入所児童10人の情報がデータに反映されていなかったことが原因である。

エ 2016年2月23日、香川県坂出市と長野県長野市の2人の男性に同一の個人番号が割り振られていたことが判明した（甲3の8）。

2人の男性は、氏名の読み方と生年月日が同じで、氏名の漢字は1文字違いであった。長野市の男性が2010年頃に同市に転入した際、前住所地の住民票が何らかの理由で1998年に削除されていた。前住所地を不明として転入を受け付けたが、長野市職員が住民基本台帳ネットワークで男性を確認する際に、氏名の読み方と生年月日が同一であった坂出市の男性が転入してきたものと誤認し、2人の男性の住民票コードが同一になった。

オ まとめ

上記の各事故例は、通知カードの作成漏れや2人に同一の個人番号を割り振ってしまったというものである。

上記の各事故例は、作成されるはずの通知カードが作成されていなかったり、本来割り振られるはずのない同一の番号を2人に割りふってしまったものであるから、一人一人に唯一無二の個人番号を振るという前提が崩れ、マイナンバー制度の根幹を揺るがしかねないものである。付番というマイナンバー制度の基本中の基本の部分ですら、制度設計・制度運用の危うさ・脆弱さを体現してしまっている事故例といえる。

また、上記事故例は、正確に確認作業をしていれば防止することができたヒューマンエラーともいえる。マイナンバー制度の制度設計・制度運用に携わる者の確認作業がいかにかいい加減なものかを端的に表しているといわざるを得ない。マイナンバーのような全国的で、制度開始・運用においては膨大な作業を要し、携わる人の数もとりわけ多い制度においては、このようなヒューマンエラーは不可避免的に生じ、事務負担から自ら招きかねないのは明らかである。そのため、被告の主張する厳格な本人確認なるものは、多くのヒューマンエラーが生じ、機能しないことは容易に想像できる。

(3) 通知カードの配達・交付における事故例

ア 2015年10月30日、高知県の安芸郵便局が通知カードを誤配達した。同月31日には、千葉県流山郵便局が通知カードを誤配達した。これらは、郵便局やコールセンターに問い合わせ・指摘があつて発覚した（甲3の9）。

イ また、2015年10月31日、青森県の五所川原郵便局では局員が配達途中に2通の通知カードを紛失し、警察に落し物として届けられたため、同年11月1日に日本郵便が回収した（甲3の9）。

ウ 被告は当初、2015年11月末までに通知カードの配布を終えるという計画を立てていた。

しかし、同月11日時点で通知カードの配達完了したのは595万通であった。これは全国約5600万世帯の約1割に過ぎない。

そのため、日本郵便は、同月12日、通知カードを同月末までに全世帯に配達するのは難しい状況との認識を示した。

このような結果になった原因の一つは、国立印刷局から日本郵便に持ち込まれた通知カードが同月11日までで2393万通であり、全体の42パーセントにとどまっていることであつた。

なお、同月11日までに誤配達や窓口での誤交付等の事故は合計68件あった（甲3の10）。

エ 2015年11月17日、青森県の八戸郵便局が通知カード1通を別人に誤配達した。同月1日に八戸西郵便局で誤配達があったばかりであった。

原因は、配達員が局内で再配達の手紙に貼る伝票を間違えた上、配達時に郵便物と伝票を照合する作業を怠ったことにある（甲3の11）。

オ 浜松市では、2015年11月から12月上旬、袖ヶ浦市では同年12月、高岡市では2016年1月、機構が送付した封書に通知カードが同封されていなかったとの住民からの報告があった。各市が機構に事実関係を確認すると、機構はシステム上発送時に通知カードが同封されていることを確認している旨回答した。結局、各市は住民の希望に応じて個人番号を変更した通知カードの作成を機構に要請することとなった（甲3の12）。

カ 2015年12月27日時点で、通知カードについては全体の9割に当たる5126万2000通の受け取りが完了した。しかし、1割の558万通が不在等で受け取られず、市区町村に保管先が移った。また、大阪市では381人分につき、未作成であることが判明し、2016年1月1日に制度運用が開始した後に配達されることになった（甲3の13）。

キ 2016年1月19日、総務省の集計により、通知カードのうち、全体の6.2パーセントに当たる362万通が本人に受け取られず、市区町村に保管されていることが判明した（甲3の14）。

ク 2016年1月28日、大阪市鶴見区は、親族の通知カードを受け取るために交付窓口を訪れた男性に対し誤って別人の通知カードを交付した。

窓口の職員は、住所や氏名を確認しないまま通知カードを渡していた。同区は誤送付した通知カードを回収し、通知カードの番号を変更した。なお、同月、大阪市では都島区や生野区でも同様の事案が発生した（甲3の15）。

ケ 2016年2月28日、三重県菰野町に住む男性2人を取り違えてマイナンバーカードを発送していたことが判明した。別の男性住人のカードを受け取った男性が郵便局に連絡して判明した。町は誤配に気づいた男性に本人のカードを渡し、別の男性住人の個人番号は変更した（甲3の16）。なお、報道によれば、「マイナンバーカード」、すなわち個人番号カードが発送されたとなっているが、個人番号カードは、交付の際に本人確認をすることとなっており、本人が受領することになるので、個人番号カードは発送されるものではないと考えられる。そのため、上記マイナンバーカードというのは通知カードのことであると考えられる。

コ 2016年2月26日、各自治体に残る通知カードは240万通、全体の4.1パーセントとなった。そして、希望すれば交付される個人番号カードの申請数は同年3月2日時点で890万枚であり、このうち581万枚が自治体に発送済みで、91万枚は住民に交付された。

この点について、個人番号カードの交付数が申請数の約1割にとどまるのは、下記の第2の1(4)で述べるような機構のシステム障害が発生したことが大きな要因である。

機構のシステム障害のためにパスワード設定等、交付のために必要な自治体側の作業ができず、住民への交付作業が遅れがちになるのである（甲3の17）。

サ 佐賀市では、2016年3月、通知カードが不在等の「不達」で市役所に約3000通が戻ってきている（甲3の18）。

シ 2016年3月18日時点で、通知カードのうち、本人と連絡が取れないことなどが理由で全国の市区町村の窓口に戻されたものが約218万通となっていた（甲3の19）。

ス 総務省は、複数の通知カードの誤配達を受け、2015年11月2日に日本郵便に対して指導を行った。しかし、その後も誤配達等の問題が判明

したため、同省は日本郵便に対して嚴重注意を行うほどだった（甲3の20）。

セ まとめ

上記の各事故例は、通知カードの誤配達、通知カードの未受領等に関する事故例である。

第2の1(3)ア、イ、エ、ク、ケ、スのように、通知カードが誤配達されると、通知カードには、氏名、住所、生年月日、性別等が記載されているため、第2の1(1)の事故事例の場合と同じように、通知カードが誤配達されて、他者の手に渡れば、どの人物にどの番号が割り振られたか等、個人情報と個人番号を照らし合わせて個人の識別は容易に可能となってしまう。

このように、すでに必要な範囲・正当な行政目的の範囲を逸脱して個人番号が提供・漏洩されることと同じ結果をもたらす通知カードの誤配達という事故事例が発生しており、法令の規定や被告の主張する対策をもってしても事故を防ぐためには不十分であることが明らかになっている。このような巨大なシステムでは、莫大な事務処理が必要となり、その中でシステムエラーの他にヒューマンエラーも不可避免的に生じることは(2)オでも言及したとおりである。

一方で、第2の1(3)ウ、オ、カ、キ、コ、サ、シのように、一人一人の国民に配達されるはずの通知カードが配達されずに、市区町村に保管される、窓口に戻ってくる等の状態にあるというのは、マイナンバー制度に反対していて、通知カードの受領も拒否する者、マイナンバー制度への不安を持つ者が多数存在することを意味する。

そして、このような通知カードの配達についての滞りは、全国民に通知カードを送り、受け取ってもらわなければならないというマイナンバー制度の設計にそもそも無理があることを端的に示している。

(4) 機構におけるシステム障害

ア 2016年1月21日及び22日に、機構と一部の自治体との間で、個人番号カード交付時に必要な情報のやり取りができない状態となる障害が10分から20分程度生じた。

また、同月25日にも同様の障害が生じた。サーバーの再起動により約40分後に復旧したが、70市町に影響が出た。

個人番号カードを管理するシステムのトラブルは、同様のものが同月13日、18日、19日にも発生しており、短期間で6回発生した（甲3の21）。

イ 2016年1月30日、機構は原因不明のシステム障害を起こしたサーバー2台の欠陥を知りながら、障害発生時に不完全なサーバーでも複数用意すればデータ処理を補えると判断した。そして、同月25日と28日に同型サーバー2機を情報通信会社に設置させてサーバーの運用を始めた（甲3の22）。

ウ 2016年2月22日、機構と多くの地方自治体との間で個人番号カード交付に必要な情報がやり取りできない状態となる障害が午後1時頃より約3時間半にわたって生じた。このとき、自治体からシステムにつながらず、（個人番号カードを）交付できない等の連絡が約200件あり、自治体の個人番号カード交付業務に影響が出た。

個人番号カードを管理するシステムのトラブルは、アと合わせて合計7回となる（甲3の23）。

エ 上記システム障害により、個人番号カードが地方自治体の窓口で受け取れない事例が全国各地で相次いだ。そのため、東京都や都内の区市町村は機構に対し、システムの改修や迅速な情報提供を求める要望書を提出した（甲3の24）。

オ まとめ

上記の各事故例は、個人番号カード交付の遅滞をもたらしたシステム障害についての事故例である。約1か月の間に、合計7回もシステム障害が発生するようなサーバーを運用していたというのは、まさにシステム技術上の不備にほかならない。個人番号カードの交付は、単純な作業に関するものである。このような基本的な事務についてすら、上記の通りの事故が生じるのであるから、マイナンバーが本格的に運用され、多種多様な情報が取り扱われる複雑な事務処理になれば、一層、事故が発生する可能性は高いと言え、個人番号および特定個人情報の漏洩のおそれは必然といえるほど高くなるといえる。

また、当初のシステム障害から約1か月間、合計7回もシステム障害が発生しながら、情報通信会社とともに、迅速に原因究明することなく、不完全なサーバーでも複数用意することでデータ処理を補えると判断する等、機構のシステム障害への対応は個人番号と特定個人情報を扱う機関としての適格がないと評価されてもやむをえないものである。

そのため、上記の各事故例は、機構がマイナンバー制度で重要な位置を占めているにもかかわらず、制度運用から間もない現時点で多く問題を生じさせており、マイナンバー制度の設計・運用の危うさ・脆弱さを体現してしまっているものである。

(5) 個人番号カードの交付における事故例

ア 平成28年2月時点で、静岡県浜松市では、市に到着しながら交付が滞っている個人番号カードが約2万6400枚に上る。なお、個人番号カードの到着数は約3万6700枚であり、交付数は約1万300枚である。この原因については、機構のシステム障害の影響が大きい上、個人番号カード到着後も本人確認等、自治体側の事務処理作業が機構側のトラブルで滞り、未交付が増えていることにある（甲3の25）。

なお、静岡市も、同年2月末時点で約2万5000枚の個人番号カードの交付が滞り、同月末時点で、個人番号カードの到着数は3万715枚、交付数は5252枚だった。

イ 2016年3月4日、栃木県塩谷町は個人番号カードを誤って別人に交付したことを明らかにした。町は個人番号カードを回収し、本来の申請者に手渡したが、その際、個人番号カードが他人に渡ったと伝えていなかったことも判明した。

同年2月29日、役場窓口で個人番号カードを交付する際、町内の男性と名字が1文字違いの別人の個人番号カードを職員が本人確認を十分せず、誤って手渡したことが原因とされる。同日中に男性から連絡を受けて回収し、翌3月1日、そのまま本来の申請者に交付していた（甲3の26）。

ウ 2016年4月4日、個人番号カード交付については、上記システム障害により、2015年度までに希望者（1019万人の個人番号カード申請）のわずか2割程度の227万枚しか発行できなかったことが判明した。この時点に至っても、上記システム障害の原因は不明という状態であった（甲3の27）。

なお、このような事態にもかかわらず、一旦は関係者の処分は見送られ、その後も2016年6月22日に西尾理事長らが報酬を返納するにとどまった（甲3の28）。また、住民サービスの低下を危惧した京都府の自治体でつくる府戸籍住民登録事務協議会は、同年2月、機構に改善を要請した。さらに、千葉や福岡等の政令指定都市で構成する指定都市市長会も、同年4月6日当時、機構を所管する総務省にトラブルの説明を求める方針であった（甲3の29）。

エ 2016年8月29日、埼玉県熊谷市の夫婦が同年2月22日頃、親族名義の個人番号カード申請書を不正に入手した上で、妻が、夫の顔写真を貼って交付を申し込み、同年4月22日に市の行政出張所で個人番号カー

ドをだまし取ったとして、夫婦ともに逮捕された（甲3の30）。

なお、この件について、熊谷市の市民課長は「親族の住所と夫の自宅が同じで、見た目の年齢も似ていたことなどから、親族と同一人物と信じてカードを交付してしまった」と説明している。

オ まとめ

上記の各事故例は、個人番号カードの交付についての事故例である。

第2の1(5)ア、ウのように、上記システム障害と相まって、個人番号カードの交付が遅滞して希望者数と比べて圧倒的に少数の者にしか個人番号カードを交付できなかったというのは、まさにシステム技術上の不備である。そのため、やはりこのような不備がある運用をしていれば個人番号および特定個人情報漏洩する危険性があり、「個人番号及び特定個人情報が法令または条例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危険が生じている事実はない」等と考えることは無理がある。これも、やはりマイナンバー制度という制度設計・制度運用の危うさ・脆弱さを体現してしまっている事故例と言わざるをえない。

次に、第2の1(5)イ、エの事故例は重大である。被告によれば、個人番号カードの交付の際には、原則として、市町村窓口に来庁を求め、本人確認書類の提示による確認を行うなど、厳格な本人確認を行うとされている。また、偽りその他不正の手段により通知カード又は個人番号カードの交付を受けたものは、6月以下の懲役又は50万円以下の罰金に処することとされ、これは罰則を強化したものの一つとされている。これらは、被告が安全対策として強調するものである。

しかし、第2の1(5)イの事故例はまさに個人番号カード交付の際に、本人確認を十分していなかったことが原因となっているのであって、被告の強調する安全対策が奏効していないことが早くも露呈してしまったのであ

る。

また、第2の1(5)オの事故例も、罰則を強化したところで、偽りその他不正の手段により個人番号カードの交付を受ける者が存在すること、そして偽りその他不正の手段により個人番号カードの交付を受けることを防ぎきれないことが露呈した事故例である。

さらに、被告は上記の厳格な本人確認や個人番号カードの偽造防止対策、罰則強化により、個人番号カードを不正取得又は偽造される具体的危険が生じているとは言えないと主張していた。しかし、実際にオの事故例において、個人番号カードの不正取得が行われてしまったのである。

したがって、被告の安全対策が奏効していないことは火を見るより明らかである。

(6) 行政手続上のミスによる個人番号の大量漏洩

2017年2月16日、静岡県湖西市は、2016年に同市にふるさと納税をした1992人について、別人のマイナンバーを記載して寄付者が住む自治体に通知していたと発表した。国の個人情報保護委員会によると、一度に大量のマイナンバーが本人以外の第三者に漏洩したのは、2015年10月のマイナンバー制度開始以来最大規模で、番号法で定められた「重大な事態」にあたるとのことである（甲3の31）。

確定申告が不要になる「ワンストップ特例制度」でふるさと納税の寄付を受けた自治体は、寄付者が住む市区町村に寄付分の税を控除するよう通知する。湖西市は、2017年1月27日に5853人分の通知を発送したが、同月30日に送付先の自治体から「他人のマイナンバーが記載されている」という連絡を受け、調査の結果、8都道県の174市区町に通知した計1992人のマイナンバーが別人のものだった。

同市の総務部長は「今年から通知にマイナンバーを記載しなければならなくなり、事務作業が増えたため」と釈明した。

(7) その他の事故例

ア 2016年4月5日、総務省は地方自治体が個人番号カードを交付する作業で、内蔵のICチップが使用不能となるトラブルが相次いでいることを明らかにした。トラブルは少なくとも17政令指定都市のほか、金沢市と佐賀市でも確認されていた。政令指定都市での発生件数は、堺市が同年3月28日までに33件、熊本市が同月末で6件である、新潟市は2件であり、大阪市は同年2月22日時点で151件である。

そして、その後もトラブルが多数起きていた。また、札幌、さいたま、千葉、横浜、相模原、静岡、浜松、名古屋、京都、神戸、広島、福岡、北九州の13市は、トラブルは確認しているが件数を集計していない。

トラブルは、個人番号カード交付時の暗証番号設定等の手続きで発生し、政令市の区役所等にある交付窓口の端末から自治体サーバーにアクセスが集中し、負荷がかかって一部で処理できなくなった。エラーが出るとICチップが使えなくなり、市区町村で再設定もできないため、個人番号カードを作り直す必要がある（甲3の32）。

イ マイナンバー制度の個人向けサイトである「マイナポータル」は当初、2017年1月に運用を開始する予定であった。

しかし、サイバー攻撃を受けた日本年金機構のセキュリティー強化に時間がかかることが判明したこと、国の機関同士の情報連携に関するシステムの開発にも2、3か月の遅れが出ていることなどから、「マイナポータル」の本格運用開始が2017年7月となった（甲3の33）。

ウ まとめ

これらの事故例は、個人番号カード内蔵のICチップが使用不可能になる、「マイナポータル」の運用開始が半年も遅れるというものである。そして、これらもまさにシステム技術上の不備に他ならない。また、被告は、マイナポータルが個人情報の利用の確認の機関として利用できるとの話を

しているが、今後もこのようにサイトが停止したり、ハッキングの標的になったりすることによって、個人情報の利用確認ができなくなったり、同サイトから個人情報が漏洩したりするという危険性があると言わざるをえない。

なお、被告は、日本年金機構からの個人情報漏洩事件は番号制度と関連性が認められないと主張しているが、「マイナポータル」の本格運用開始が遅れる理由にサイバー攻撃を受けた日本年金機構のセキュリティー強化に時間がかかることが判明したことが挙げられているのであり、これは同事件と番号制度とは関連性が認められることに他ならないのである。

2 民間部門からの特定個人情報漏洩

(1) 民間事業者による特定個人情報漏洩

民間事業者はマイナンバー運用以降、税務申告などをまだ終えていないため、今も収集・利用開始段階にあると思われる。しかし、すでに多くの事故が発生しているところである。

例えば、身分証明書として使わないよう内閣府や総務省が通知を出していたにもかかわらず、ツタヤがマイナンバーを本人確認に使用できるようにして、2016年1月までホームページなどで公表していた（甲3の34）。

被告は、新聞広告やチラシ・ポスター作成・配布、説明会への講師派遣、ホームページ上での広報資料や質疑応答、説明会の動画掲載等をしているから、十分に周知・研修を図っている旨主張する。しかし、個人情報という取扱いに特に慎重さが求められるものについては、その取扱者が実際に適切かつ安全に個人情報を取り扱うことができるかが問われているのであって、被告のように、単に周知・広報を図れば事足りるというものではないのである。そのため、被告がそのような主張をしているということ自体が、いかに被告が個人情報の漏洩の危険についていい加減に捉えているかということを物語

ると言わざるをえない。

そして、実際に上記事故例が生じているということが、いかに民間へ正しい使用方法の周知をすることが難しいかを示しているのである。

(2) その他の個人による特定個人情報漏洩

ア 2015年11月30日、兵庫県伊丹市において、60代の女性宅に2人組の女性が現れて通知カードを求めた。60代の女性は夫と子供3人を含む一家5人分のカードを封筒ごと渡した（甲3の35）。

イ 2016年1月26日、横浜市立新吉田小学校の20代女性事務職員が教職員38人とその家族16人の計54人分のマイナンバーが書かれた書類を紛失した。同女性職員は、東急横浜駅で下車する際、マイナンバーのほか、教職員や配偶者と扶養親族の氏名が記入された書類を入れたかばんをなくしたことに気づいた（甲3の36）。

ウ 静岡県警察の発表（2016年2月頃と考えられる）によれば、直近1年間に受理した遺失届のうち、通知カードの遺失届は123件であった。そのうち16件はその後自分で発見し、9件が持ち主に戻った。しかし、98件はその当ても発見されず「調査中」のままであった。静岡中央署では18件を受理し、「家の中でなくした」「ゴミと一緒に捨ててしまった」というものが多かった。

なお、静岡県警会計課は「悪用の恐れもあるので、気をつけてほしい」と呼びかけていた（甲3の37）。

エ 石川県では、2016年2月6日までに、県内全12警察署のうち11署で計50人分の通知カードの落とし物の届け出があった。具体的には、金沢中署で11人分、金沢東署・津幡署各9人分、白山署7人分、輪島署5人分、他6署では1から2人分の届け出があった。

なお、石川県警では、当時では悪用例は確認されていないものの、個人情報流出につながりかねないため注意を呼びかけていたほか、県警幹部も

「個人情報他人に見られると犯罪に悪用されるおそれがある」と注意を促していた（甲3の38）。

オ 2016年2月、新潟県警会計課は2015年の拾得物・遺失物の取り扱い状況につき発表した。そして、落とし物として届け出があった拾得物のうち、通知カードが50件あった（甲3の39）。

通知カードの落とし物は、コンビニエンスストアのコピー機に置き忘れられたケース等で、新潟市など都市部で多かった。

カ 2016年3月21日、居酒屋チェーン「鳥貴族」のフランチャイズ加盟店を運営するダנקの従業員が大阪市内のコンビニエンスストアで車上荒らしに遭い、従業員430人のマイナンバーを含む個人情報が記載されていた扶養控除申告書が持ち去られた（甲3の40）。

ダנקは同年4月5日に鳥貴族や個人情報保護委員会へ報告し、対象となる従業員には直接説明と謝罪を行った。

キ 遅くとも2016年3月4日には、インターネット上で「マイナンバー占い」と称して、マイナンバーを入力させようとするサイトが確認されており、神奈川県川崎市中原区や茨城県取手市等では、ホームページで注意喚起している（甲3の41）。

ク 2015年11月頃、大阪の焼肉店が個人番号に「1129（いいにく）」、「4129（よいいにく）」等が含まれていたら、焼肉を無料で食べることができるというサービスを提供しようとした。しかし、内閣官房は、法令違反（番号法15条）にあたる可能性があり、問題がないとは言いきれない、また、個人番号を提示するときに、個人情報を収集してしまうことを危惧しているとして、上記サービスの自粛を要請した（甲3の42）。

ケ まとめ

第2の2(2)イ、ウ、エ、オ、カの事故例は、個人番号の紛失・盗難についての事故例である。これら事故例は、通知カードの誤配達事故例と同じように、氏名、住所、生年月日、性別等とともに個人番号を紛失・盗難されたものといえ、どの人物にどの番号が割り振られたか等、個人番号による個人の識別は容易に可能となってしまうだけでなく、他者に対して、個人番号を提供したことと同じ結果になってしまうのである。

次に第2の2(2)アの事故例は重大である。被告は、通知カードの不正取得も厳重な刑罰により禁止されており、通知カードを不正取得又は偽装される具体的危険が生じているとも言えないと主張している。

しかし、第2の2(2)アの事故例ですでに通知カードの不正取得が行われてしまった。やはり厳重な刑罰により禁止されていても通知カードを不正取得することも防ぎきれず、被告の主張する安全対策が奏効していないことがまたもや露呈してしまったのである。

また、第2の2(2)キの事故例であるが、「マイナンバー占い」で興味を引く等様々な形で巧妙に個人番号を不正取得しようとする行為が実際に行われている。不正取得の仕方によっては、氏名・住所などの基本的な個人情報以外にも、個人番号カード発行に必要なパスワードなどの重要な情報を合わせて取得することも考えられ、これを被告の主張する安全管理措置を講じるだけで防ぐことは不可能である。悪意を持って個人番号を不正取得しようとする者を止めることはできず、情報が集約するデータベースを国が提供することは情報漏洩したときのリスクを増大させるだけである。

最後に、第2の2(2)クの事故例は、悪意はないとしても、個人番号を用いた飲食店のサービス等を提供・利用することで、自己の意図しないところで個人番号や特定個人情報が流通してしまうおそれや法令違反を犯してしまうおそれがあることを示す好例である。また、被告は、個人番号は単なる個人識別情報にすぎず、これのみからは、他の何らの個人情報を得る

ことも不可能であると主張するが、それならばなぜ自肅を要請する必要があったのか、疑問を抱かざるをえない。

3 自治体職員による個人情報の不正取得

- (1) 2017年1月11日、東京都中野区の元臨時職員が、区個人情報保護条例違反で逮捕された（甲3の43）。同人は、2014年10月から2016年3月に3回、中野区の行政情報オンラインシステムで同区の20代女性の名前や住所を閲覧しており、同人所有のパソコンには女性50人分の個人情報が記録されていた。上記事件では、氏名、住所が問題とされたが、同人は、マイナンバーカードに関する業務を担当しており、個人情報を閲覧するためにIDとパスワードを与えられていたとのことであるから、氏名、住所と併せてマイナンバーも不正取得される可能性は多分にあった事案である。しかも、中野区は、個人情報の取り扱いに関する研修会を開いていたが、臨時職員は対象外とされており、同人はかかる研修を受けていなかった。すなわち、中野区は、同研修を受けていない臨時職員にマイナンバーを取り扱う業務を担当させ、そのためのIDとパスワードも与えていたことになる。

仮にシステムのセキュリティーが完璧であったとしても、マイナンバーを扱う職員の情報に対する規範意識が低ければ、情報は容易に漏れてしまう。しかも、上述の例は、元臨時職員のみならず、中野区自体の情報保護に対する意識が相当に低いことを示している。

- (2) 自治体において公務員が個人情報を不正入手する事件は、上述のものだけではない。

2015年6月には、東京都大田区の職員が知人女性の住所や生年月日を2000回以上閲覧し、区個人情報保護条例違反容疑で逮捕された。

また、2016年1月には、岐阜県職員が人事給与システムにアクセスし、女性職員ら約1万人の生年月日などの個人情報を収集、不正利用し、県個人

情報保護条例違反容疑で逮捕された。

このように同種の事件は、様々な自治体で発生しているのである。

(3) まとめ

氏名、住所、生年月日などの公務員による不正取得の事件が多数発生しているという現実を踏まえれば、たとえ刑罰強化が図られているとしても、個人番号や特定個人情報漏洩しないなどとは断言できないはずである。かかる事件が発生する限り、特定個人情報は常に漏洩の危険性に曝されているというほかない。

4 行政機関及び民間企業からの個人情報の大量紛失・漏洩

- (1) サイバー攻撃被害を2016年に公表した国内の企業や行政機関の93組織から流出、または流出した恐れがある個人情報などが、少なくとも1260万件に上ることが判明した（甲3の44）。内訳は、民間企業の関連が65件、行政機関が17件、学校が11件であった。漏洩した情報が最も多かったのは、JTBが2016年6月に発表した約679万件であった。攻撃手法では、ハッカーにセキュリティ上の欠陥をつかれたのが43組織と最も多く、パスワードを解析されたのが22組織、メールでウイルスを送りつけられるメール攻撃は19組織、不明・未公表が9組織であった。
- (2) 2017年2月17日、全国健康保険協会広島支部は、最大19万人分の氏名や診療内容など個人情報を記録したフロッピーディスクとCD計535枚を紛失したと発表した（甲3の45～46）。同支部によると、診療報酬の再審査請求を行うためにCDなどに情報を記録し、535枚に2012年9月から2015年3月のデータが入っていた。段ボール箱に梱包し、事務室内の保管庫に施錠して保管していたが、昨年12月21日に紛失に気付いた。建物内を探しても見つからなかったという。
- (3) 2017年3月3日、神奈川県内の医療従事者などが加入する健康保険組

合が、1000人以上のマイナンバーなどが入ったCD-Rを紛失していたことが判明した（甲3の47）。同組合は、誤ってゴミとして焼却処分されたとみられるなどと説明している。

第3 結語

- 1 本書面でも取り上げた各事故例は、番号制度が抱える制度上の欠陥、システム技術上の不備や脆弱さ、刑罰強化による不正・犯罪の抑止力の弱さ等、番号制度の問題点を次々に明らかにしたものである。
- 2 その中でも、特に重大で看過することができない事故例は、個人番号カード交付の際の不十分な本人確認による誤交付、個人番号カードの不正取得、個人番号の不正取得を企図したサイトの存在、通知カードの不正取得、公務員による個人情報の不正取得・利用の事故・事件例である。

被告は、個人番号カード交付の際の厳格な本人確認や厳重な刑罰により、同カードや通知カードを不正取得される具体的危険性はない、「システム技術上または法制度上の不備があり、そのために個人番号および特定個人情報が…第三者に開示または公表される具体的危険性が生じている事実はないなどと主張している。

しかし、上記事故例により、個人番号カード交付の際には杜撰な本人確認もなされていること、意図せずとも膨大な事務処理と制度に関係する人が官民合わせて非常に多い為ヒューマンエラーが不可避免的に生じること、個人番号カードや通知カードを実際に不正に取得することができること、悪意を持って個人番号を不正取得しようとする者を止めることができないことが明るみとなったのである。しかも、個人情報を不正取得しようとする者は、特定個人情報へのアクセス権限を有する公務員にも存在しているのである。すなわち、厳格な本人確認や厳重な刑罰などという安全対策は実際には奏効していないことが明らかとなったのである。

3 そして、上記事故例に加えて、システム技術上の不備・脆弱さに基づく事故例等、番号制度という制度設計・制度運用の危うさ・脆弱さを体現する各事故例も生じている。このように番号制度の運用は当初から危うかったのであるから、今後、情報連携が始まれば情報漏洩のおそれは飛躍的に高まっていくことになるのである。

本書面でも取り上げた事故例でも、個人番号だけでなく、同時に氏名・住所等が流出しているものが多数で、同時に個人情報が出ていけばそれだけで情報漏洩した時の個人のプライバシーの侵害される程度は大きくなる。氏名・住所のような基本的な情報だけでなく、個人番号カード発行に必要なパスワードなどの重要な情報を合わせて取得することも考えられ、重要な情報が漏れるだけ、個人のプライバシーへの侵害は大きくなる。

悪意を持った者が、情報が確実に価値の高い闇のデータベースを完成させることもでき、これによる二次被害も甚大なものとなってくる。

また、このデータベースと地方公共団体等のマイナンバー管理者が通謀することで、その機関に認められる限りでの情報がさらに流出していくこととなる。そして、マイナンバーが生涯不変であることから、マイナンバーに関連する情報も、国民の気づかぬ間に生涯を通じて永続的に流出することとなる。

被告がというような、マイナンバーが単なる番号で、個人情報ではないという単純な話では全くなく、原告らの個人情報に生じている危険性は現に差し迫った極めて具体的なものといえる。

4 したがって、「システム技術上又は法制度上の不備があり、そのために個人番号および特定個人情報が（省略）第三者に開示又は公表される具体的危険」はすでに生じている。又、原告らのプライバシー情報が日々侵害される具体的危険性も生じている。

以 上