

主 文

本件訴えをいずれも却下する。
訴訟費用は原告らの負担とする。

事実及び理由

第1 当事者の求めた裁判

1 原告らの請求の趣旨

被告が、原告らに対し、2002年（平成14年）8月5日付けで行った、住民基本台帳法に基づく11桁の番号を付与した行為（処分）を取り消す。

2 被告の答弁

(1) 本案前の申立て

主文同旨。

(2) 請求の趣旨に対する答弁

原告らの請求を棄却する。

第2 事案の概要

1 本件は、原告らが、被告に対し、被告が住民基本台帳法に基づき原告らに11桁の番号（以下「住民票コード」という。）を付与した行為（以下「本件行為」という。）は、憲法13条で保障されている原告らのプライバシー権を侵害する違法な行政処分であると主張して、本件行為の取消しを求めた事案である。

2 争いのない事実等

(1) 原告らは、富山市の住民である。

(2) 被告は、平成14年8月5日、原告らに対し、本件行為をした。

(3) 本件行為は、住民各人につき、それぞれ異なる住民票コードを住民票へ記載するものである。住民票コードは、市町村長から都道府県知事へ、氏名、生年月日、性別、住所及び住民票コードを含むこれらの変更情報（以上の6情報を「本人確認情報」という。住民基本台帳法30条の5第1項）とともに通知され、これらが、都道府県知事から指定情報処理機関（現在は「財団法人地方自治情報センター」（以下「地方自治情報センター」という。）のみである。）へ通知される。

(4) 平成14年8月5日に始まった第一次稼働によって、市町村で集められた本人確認情報は、コンピュータネットワーク（住基ネット）によって都道府県に送られ、更に地方自治情報センターに送付された。国の行政機関等は、地方自治情報センターのコンピュータにアクセスできるようになっており、本人確認情報を利用できるようになった。平成15年8月25日に始まった第二次稼働では、全国どこの市町村からでも地方自治情報センターにアクセスして、全国どこに住んでいる人の本人確認情報でも確認できるようになった。富山市も、第二次稼働への参加を表明している。

3 争点

(1) 本件行為が「行政庁の処分その他公権力の行使に当たる行為」（行政事件訴訟法3条2項、以下「行政処分」という。）に当たるか（本案前の申立てについて）。

（被告の主張）

行政処分とは、行政庁の法令に基づく行為のすべてを意味するものではなく、公権力の主体たる国又は公共団体が行う行為のうち、その行為によって、直接国民の権利義務を形成し又はその範囲を確定することが法律上認められているものをいう。本件行為は、住民票の情報を表現するための記号を付したもので、あるいは検索のための番号を付したものにすぎないから、本件行為によって原告らの住民としての地位に変更が生じるものではなく、また、その地位に影響を与えるものでもない。したがって、本件行為は、「直接国民の権利義務を形成しまたその範囲を確定することが法律上認められているもの」ではなく、行政処分に該当しない。

（原告らの主張）

本件行為により、原告らの本人確認情報というプライバシーが全国の市町村端末によって、また、一定の事務を扱う中央省庁において検索及び閲覧可能となる。このことは、原告らのプライバシー権が直接制限され又はその範囲が確定されることに他ならない。

なお、本件行為の性質は附番の通知であるが、観念の通知を含む通知にも行政処分性は認められる。

(2) 本件行為の違法性

（原告らの主張）

ア プライバシー権の保障及び内容

原告らには、憲法13条によりプライバシー権が保障されている。その内容は、当事者が自己に関する情報をコントロールする権利（自己情報コントロール権）であると解される。自己情報コントロール権とは、自分に関する情報を他者に開示する・しない及び利用・提供の可否を自分で決める権利である。

イ 国の行政機関による利用の不承認

本件行為により、国の行政機関は、原告らの住民票コードを本人確認の手段として使用することができるようになり、このことによって、国の各種行政機関が蓄積、保有している原告らの個人情報、きわめて容易に抽出、検索できるようになる。これらを統合、分析することによって、各種行政機関が様々な目的をもって収集、蓄積した原告らの個人情報を、その目的、範囲を超えて把握することが可能となる。原告らは、国の行政機関によって収集、蓄積された原告らの個人情報が、当初の目的の範囲を超えて、また、収集、蓄積した行政機関以外において把握されることを承認しない。本件行為は、原告らの承諾なく、原告らの個人情報を国の行政機関に利用可能な状態にするものであるから、原告らのプライバシー権（自己情報コントロール権）を侵害している。

ウ 情報漏えいの危険性

プライバシーは、いったん侵害されると被害の回復が極めて困難である。また、インターネットの発達した今日では、いったん漏えいした個人情報がインターネット網を通じて世界のどこに流れるかわからない。このような特徴を持つプライバシーを保護するためには、個人情報を流通させる場合には絶対に漏えいしないような保障が必要である。これがない場合には、現実に情報漏えいの事態が起らなくとも、プライバシーを危険にさらしたという点で、プライバシー権を侵害したと評価すべきである。そして、次の(ア)ないし(ウ)の点からすると、原告らのプライバシーが侵害される危険性が高く、被告の本件行為は原告らのプライバシー権を侵害している。

(ア) 自治体のシステム不備による情報漏えいの危険性

第二次稼働後は、全国どこの市町村からでも、地方自治情報センターにアクセスして本人確認情報を利用することができる。富山市もこれに参加しているため、原告らの個人情報が全国の自治体に流通し、又はアクセス可能な状態となる。しかし、全国の少なくない自治体において、システム不備による情報漏えいの危険性がある。

すなわち、全国ほとんどの自治体においては、①住民票を管理する住民台帳システムなど基幹系ネットワーク、②行政庁内で発生する様々な情報を管理・交換するための省内イントラネットなどの情報ネットワーク、③行政情報を住民に知らせるためにインターネットから直接アクセスが可能な公開系ネットワーク、④全国の住基ネットに接続するための住基コミュニティーサーバー（以下「住基CS」という。）を収容する住基ネットワークを有している。上記③は何人からも接続可能であるから、ネットワークシステムとして①及び④を③から独立させておかなければ情報漏えいの危険がある。ところが、長野県下27の自治体においては、③と①及び④とが直接ルーターやハブで接続されていた。③と①及び④との間にはファイアウォールが設置されているはずであるが、住基ネットに用いているコンピュータの基本OSに、次々とセキュリティーホールが発見されていて、住基ネットへの侵入の可能性のあるセキュリティー上の脆弱性が認められる現状においては、情報漏えいの危険性が高い。

長野県が平成15年9月から11月に同県内3自治体で実施した侵入実験（以下「長野県における侵入実験」という。）では、ファイアウォールは通過されたが、住基CSは当該自治体において完璧にパッチが当てられていたため侵入できなかった。しかし、住基ネットに用いているコンピュータのOSについて、住基CSを含むコンピュータネットワーク上のサーバーのOSが既知の脆弱性を含んだまま運用されていること等が明らかになった。上記のとおり、住基ネットに用いられているコンピュータの基本OSには次々にセキュリティーホールが発見されているから、そのたびにパッチが当てられなければ侵入の危険性がある。また、セキュリティーホールが発見されてから、これに対処するためのパッチが配付されるまでの間も常に侵入の危険性がある。

その他にも、庁内LANにおいて上記①と②の区別がなされていないケース、出先機関との間で上記①がダイヤルアップで接続されていて発信元電話番号でチェックされていないケース、委託業者側からダイヤルアップ又は専用線接続で庁内LAN

に常時接続可能なケースなどがある。
なお、総務庁が実施した侵入実験では侵入に失敗しているが、このことは、実施担当者の技術・能力が低かったことを示すだけであって、この実験がネットの安全性を示していると評価することはできない。
被告は、市区町村、都道府県、指定情報処理機関及び本人確認情報の提供を受けた行政機関に対するセキュリティー基準の義務づけなどの運用面の措置を講じていると主張するが、そのような措置は行っていない。また、被告は、専用回線も使用していない。被告の主張する本人確認情報の暗号化やファイアウォールの設置が、十分な侵入防御の能力を持っているとはいえない。

(イ) セキュリティーポリシーの欠陥

上記ネットワークシステム以外にも、保守業務、バックアップデータ等外部委託業者による漏えいの危険性、庁内での無権限者によるアクセス、その他情報漏えいのあらゆる可能性を想定したセキュリティーポリシーが、住基ネットに参加するすべての自治体において確立されていなければならない。しかし、平成15年1月から2月の段階では、全国の1割程度の自治体でセキュリティー体制が未整備であり、2割程度の市町村団体ではコミュニケーションサーバーのアクセスログの管理体制すら未整備である。また、全国73の自治体は、セキュリティー対策の自己点検について報告すらできない状態である。

被告は、セキュリティー対策として一定の措置がとられていることを主張する。しかし、コンピュータのネットの安全性を主張するためには、想定できる危険性を全てあげ、それぞれに対する対策の有無及び内容を吟味・評価するセキュリティーポリシーの策定が不可欠であり、これを欠く安全対策は著しく効力が低い。住基ネットでは全国の市町村端末から原告らの情報の照会が可能となるから、全国すべての市町村においてセキュリティー上万全の対策がとられていなければ不安がないとはいえない。

(ウ) 行政機関内部における乱用防止措置の欠如

プライバシー侵害の危険性をなくすためには、全国すべての市町村において、行政機関の職員による個人情報漏えいを防止する措置が必要である。

長野県における侵入実験により、自治体の職員は、本来接続に必要なIDカードやパスワードがなくても住基CSを支配できる状態に入れることが明らかになった。また、現行システムでは、職員が、目指す相手の詳しい情報を持たなくても、相手の本人確認情報にたどり着くことができる。

そうすると、プライバシー侵害の危険性をなくすためには、こうした盗み見行為に対する規制が必要である。しかし、全国の自治体において、また、被告においても、職員が不正な操作を行った場合に処分する体制が整っていない。

すなわち、原告らは、平成10年6月29日及び同月30日に、富山市役所において、同市職員から、富山市個人情報保護条例に違反し、目的外で個人・世帯内容の検索を受けてプライバシーを侵害された。原告らは、平成14年12月18日、被告に対し、同条例に基づいて苦情申立てを行い、違法行為を行った職員の処分等を求めたが、被告は、職員又はその管理責任者に対する処分を行わなかった。このように、被告においても不正が生じているのであるから、他の自治体においても、同様の事態が生じないという保障は全くない。

また、全国の自治体において、職員が市民の個人情報を目的外使用した場合に、職員に対し何らかの不利益を課する旨の条例を置いていないところがほとんどである。個人情報保護法においても、国の行政機関の職員について、情報を漏えいした場合に処罰する規定はあるが、目的外使用した場合に処罰する規定は欠いている。

したがって、行政機関内部における乱用防止措置は極めて不十分である。

エ 住民基本台帳法及びそれに基づく住民ネットの構築と、個人情報保護との関係
住民票コードを利用すると、単一の番号の下に電算化された個人情報を蓄積することが容易となる。これは、個人データファイル(特定の基準に基づき自動化された手続によって利用できる個人データの集合体)を作成することにほかならない。個別情報が一か所に集中管理されると、情報の流用や目的外利用が発生しやすくなるので、これを阻止するため、全国の多くの自治体の個人情報保護条例において、外部提供の禁止原則や、電子計算組織の結合禁止原則が定められている。条例が定めるこれらの原則は、憲法上保障された自己情報コントロール権の具体化又は制度的な担保であるから、たとえ法令の定めがあつたとしても、当然に外部提供され、又は電子計算組織の結合禁止が解除されるわけではなく、外部提供や電子計算組織の結合禁止を解除するためには、これらを正当化するに足る個人情報の保護措置が

とられていなければならない。しかし、住民基本台帳法、個人情報保護に関する法律（以下「個人情報保護法」という。）及び行政機関の保有する個人情報の保護に関する法律（以下「行政機関個人情報保護法」という。）における個人情報の保護措置は、自己情報コントロール権の保障という観点から多くの問題点を残している。そうすると、市区町村自治体が、現在の個人情報保護法制においては、平成11年法律第133号（住民基本台帳法の一部を改正する法律、以下「法133号」という。）附則1条2項にいう「所要の措置」が満たされていないと解して、その地域自治として住基ネットに参加しないという選択をすることは合法であり、また、住民個人が自分の本人確認情報に限り住基ネットに接続しないように求めることは、自己情報コントロール権の本質的部分に属するので、最低限の保障として認められるべきである。

(ア) 住民票コードと住基ネットの基本的性格
氏名、住所、生年月日及び性別の基本4情報は、それ自体がプライバシー保護の対象であり得るが、住民票コードが付されると、事実上いわゆる個人データファイルが成立する。住基ネットの利用事務の拡大が予想され、対象とする基本情報についても住民基本台帳法上限定する歯止めがない状況のもとで、電算化された各種個人情報が住民票コードにより一括管理されれば、収集当初は市区町村や都道府県、国の機関に分散していた個人情報であっても、それらを結合することが極めて容易となる。住民票コードは全住民を対象とし、利用事務の範囲も法令の改正により将来的には無制限であるから、単一の番号の下に個人情報を蓄積することが可能となる。このことは、個人データファイルを作成することにほかならない。

(イ) 外部提供の禁止及び電子計算組織結合禁止の原則が持つ意義
特定の目的のために個人の同意に基づいて集められた個別情報が、行政機関相互の間で交換され、あるいは一か所に集中管理されると、情報の流用や目的外利用が発生しやすくなる。多くの自治体の個人情報保護条例において、外部提供の禁止原則や、電子計算組織の結合禁止原則が定められているのは、こうした状況が生じることを阻止するためである。

条例は、本人の同意を得ないで外部提供をすることができる場合として、「法令の定めがあるとき」と定めており、住民基本台帳法がそれに該当するので、本人確認情報の都道府県への送信が事務の適正な執行であるとの主張も考えられる。しかし、外部提供禁止の原則は、憲法上保障された自己情報コントロール権を具体化したものであるから、住民基本台帳法によってもこの原則を自在に解除できるわけではない。また、法文上も、法令の定めがあるとき外部提供することが「できる」と規定されているだけで、外部提供が義務づけられているわけではない。法令の定めがあれば当然に外部提供すべきものではなく、住民の個人情報を十分に保護するために、外部提供を拒否できる場合もあると考えるべきである。

電子計算組織の結合禁止原則も、自己情報コントロール権の保障を制度的に担保する重要な原則である。したがって、やはり、法令の定めがあれば当然に禁止が解除されるわけではなく、法令上、禁止解除を正当化するに足る個人情報の保護措置がとられていなければならない。それらの条件を充足することなく、法令で一方的に外部接続禁止を解除できるとすれば、憲法上の自己情報コントロール権、それを具体化した個人情報保護条例上の権利保障は極めて不安定となる。

そうすると、住民基本台帳法、行政機関個人情報保護法及び個人情報保護法における個人情報保護措置が、これらの禁止解除を正当化するに足るものであるかどうか問題となるが、次のとおり、これらの法律による個人情報保護措置には多くの問題点がある。

a 住民基本台帳法上の本人確認情報の保護措置は、OECD 8原則（①安全保護の原則、②責任の原則、③目的明確化の原則、④利用制限の原則、⑤収集制限の原則、⑥データの品質維持の原則、⑦公開の原則、⑧個人参加の原則。以下「8原則」という。）を充足していない。

住民基本台帳法30条の29第1項、2項は、都道府県知事、指定情報機関及びそれらから本人確認情報の電子計算機処理等の委託を受けた者は、本人確認情報が漏えい、滅失、き損しないよう適切な管理を行うために必要な措置を講じなければならないと規定し、同法36条の2は、市町村長とその受託者は、本人確認情報に限らず、住民票記載事項全てに同様の義務を負うと定める。これは8原則①及び②に対応するかに見える。しかし、「適切な管理のために必要な措置」の具体的内容が示されていない。そもそも、従来から、住所、氏名、生年月日、性別の基本4情報が、何人でも閲覧請求できるとされている以上、安全確保は名目的なレベルにとど

まる。

同法30条の30第1項、2項は、本人確認情報の利用及び提供の制限を規定する。これは8原則の③及び④に照応するかに見える。しかし、8原則の本来の趣旨は、個人情報を利用されている本人が、情報取扱者の使用目的や使用の実態を知ることができるように目的を明確化すべきこと、更に、本人に対して使用目的を知らせるべきことを求める点にある。しかし、同条項は「法律で定められた目的以外のために本人確認情報を利用又は提供してはならない」と規定するだけであるから、法律の定めだけで、利用・提供の範囲を拡大することができる。

同法30条の42は、住民票コードの不必要な収集禁止を定める。これは8原則の⑤に対応するかに見える。しかし、ここでいう「不必要な」場合とは、同法上の事務ないし同法に基づき本人確認情報の提供を求めることができる事務の遂行に必要な場合以外を指しているから、前同様に、法律や条例によって、利用できる事務の範囲を将来的に無制限に拡大できる。また、同法30条の43第1項から3項までは、民間における住民票コードの利用を禁止しているが、民間利用規制の実効性は疑わしい。

同法30条の37及び30条の40は、本人確認情報の開示請求権等を定めるが、8原則⑥から⑧までとは、似て非なるものである。開示対象が本人確認情報の記録された磁気ディスクに限定されており、本人確認情報がいかなる機関に提供されたのか、それ以外の情報を都道府県や国、指定情報機関が保有していないかどうかという自己情報コントロール権の核心をなす点が欠落している。また、仮に、本人確認情報に誤りがあっても、それを訂正する権利が認められていない。8原則⑥から⑧は、それぞれ、⑥個人データは正確で完全、最新のものであること、⑦個人データをめぐる情報政策の公開原則（いかなる個人データを誰が保有しているかを容易に知りうること）、⑧自己情報開示請求権と開示が拒否された場合の異議申立権の保障、申立てが認められた場合の削除ないし訂正等の請求権保障を内容としているが、住民基本台帳法上、これらの保障はなされていない。

同法30条の41及び36条の3に定める苦情処理は、8原則⑧に関連するが、これらは、単に本人確認情報の取扱いに関する苦情の適切かつ迅速な処理に努めるべきことがうたわれているだけであり、権利保障の視点が欠けている。住民基本台帳法上、市町村長の処分については都道府県知事に対して審査請求をすることができる（同法31条の4）。しかし、指定情報機関及び国に対しては、処分性の不存在等を理由として、行政不服審査法上の異議申立てが認められる可能性が低く、個人情報が送信された先における利用状況のコントロールは極めて困難である。

b 個人情報保護法及び行政機関個人情報保護法における個人情報の保護措置
行政機関個人情報保護法では、適正取得のルールが課されていないこと、思想・信条などに関わるセンシティブ情報の収集禁止原則が定められていないこと、本人情報の開示・訂正権などの例外が広く認められていること、利用目的の変更や目的外の利用・提供が広範に認められていること、同法が当面施行に至っていない（平成17年4月1日施行）ことなど、規制内容が個人情報保護法よりも緩和されている。

行政機関個人情報保護法2条3項は、「保有個人情報」を「行政機関の職員が職務上作成し、又は取得した個人情報」と定義するが、各自治体の外部接続により形成されたネットワークを通じて、国の行政機関が、当該情報を「参照」するだけであると解せば、「保有個人情報」には該当せず、国に対する開示等の請求はできないこととなる。

同法では、収集制限が明記されていない。同法3条1項は保有の制限を定めるのみであり、個人情報の保護に十分であるとはいえない。

同法3条3項は、利用目的の変更を「変更前の利用目的と相当の関連性を有すると合理的に認められる範囲」で認め、本人の同意を得ることを要件としていない。この場合、「相当の関連性」の有無を判断するのは当該行政機関であるから、判断が厳格になされる制度的な担保は存在しない。同法4条に定める利用目的の明示も形骸化する。

同法4条の利用目的の明示についても、同条1号から4号における利用目的を明示しない場合の定めは、漠然かつ広範にすぎ、例外規定としての役割を果たしていない。

同法8条は、利用及び提供の制限を定めるが、同条2項2号、3号は職務の遂行上必要があれば、個人情報の目的外利用を認めている。「必要な限度」、「相当の理由」等の要件が課されているが、その有無は行政機関が自ら判断するので、実際に

は利用制限の歯止めとはならない。仮に目的外利用を認めるとしても、本人に対し、事前に新たな利用目的と利用する行政機関を通知し、あわせて利用停止請求権（同法36条以下）を行使する機会を保障すべきであるが、このような制度は同法上存在しない。

個人情報保護法においては、行政機関に対しては、行政機関個人情報保護法よりも一層緩やかな義務規定が存在するのみである。個人情報保護法は、法133号附則1条2項にいう「所要の措置」と呼ぶにふさわしい内容を充分備えていない。

(ウ) 住民基本台帳法と個人情報保護条例との関係

住民基本台帳法及びそれに基づく住基ネットは、法文上各自治体の定める外部接続禁止等の解除を命じているように見える。しかし、個人情報保護条例の諸規定は、憲法の人権保障と一体化し、それを具体化した規定としての意味を持っているから、住民基本台帳法が当然に先占できるわけではない。市区町村が、現在の個人情報保護法制においては、法133号附則1条2項にいう「所要の措置」が満たされていないと解し、住基ネットに参加しないという選択をすることは合法である。また、住民個人が自己の本人確認情報に限って住基ネットに接続しないように求めることは、憲法13条に基づく自己情報コントロール権の本質的部分に属するから、自治体の政策決定いかにかわらず、認められるべきである。

オ まとめ

本件行為は、原告らの承諾がないのに、また、個人情報保護のための措置が十分でないためプライバシー侵害の危険性が大きい状態であるのに、原告らに住民票コードを付し、全国ネット（住基ネット）に接続したものである。これによって、他の自治体又は国の行政機関が原告らのプライバシーを侵害する危険が生じたものであり、このことについては番号を付与した被告が責任を負うべきものである。よって、本件行為は、憲法13条に反し原告らのプライバシー権を侵害するものであるから、その取消しを求める。

(被告の主張)

被告は、法133号附則3条の規定により本件行為をしたのであるから、本件行為は適法である。

本件行為は、住民票の情報を表現するための記号を付したものにすぎないから、原告らのプライバシーを侵害することはない。

被告は、本人確認情報の提供先の限定や目的外利用の禁止など制度面の措置、市区町村、都道府県、指定情報処理機関及び本人確認情報の提供を受けた行政機関に対するセキュリティ基準の義務づけなど運用面の措置、専用回線上の本人確認情報の暗号化やファイアウォールの設置の各措置をとって個人情報を保護している。既存住民基本台帳等のシステムを含む市内LANがインターネットと接続しているとしても、住基CSはファイアウォールの設定により既存住民基本台帳のシステムと遮断されていること、住基CS及び同端末でのインターネット及び電子メールの使用は基本的に禁止されていることなどからすれば、セキュリティ上危険であるとはいえない。

住基ネットでは、次の措置を講じており、同システムは極めて安全である。仮に市区町村の市内LANのセキュリティ装置が十分でないためウイルス等が侵入したとしても、住基ネットに入り込み、他の市区町村の住基CS、都道府県サーバーや指定情報処理機関サーバーに到達するおそれはない。

ア 指定情報処理機関のネットワーク監視室が監視するファイアウォールを、住基CSネットワーク方向、都道府県サーバー及び指定情報処理機関サーバーの全方向に設置し、不正な通信がないか24時間常時監視している。

イ IDS（侵入検知装置）を設置し、同様に常時監視している。

ウ 通信は、専用回線と専用交換装置からなるネットワークを介して実施している。通信の際は、公開鍵方式により正しい通信相手への接続を相互に認証している。公開鍵方式の秘密鍵は第三者による読出しや変更ができないようになっている。この相互通信の過程で暗号通信を実施している。

エ 通信は、独自の住基ネットアプリケーションによって行っており、インターネットで用いられる汎用的なプロトコルを使用していない。住基ネットアプリケーションは、操作者用ICカード認証を行って初めて起動する設計となっている。

また、住民基本台帳法上、次の措置が講じられている。

ア 住基ネットにおける本人確認情報の利用は、公的部門における住民の居住関係の確認のための利用に限定している（同法30条の7第3項ないし6項）。

イ 住民票コードを含む国の機関等へのデータ提供には、個別の目的ごとに法律上

の根拠が必要であり、また、目的外利用の禁止を定めている（同法30条の30、30条の34）。

そもそも、市区町村長は、住民基本台帳法により、住民票の記載等を行った場合には、全住民の本人確認情報を電気通信回線により都道府県知事に通知するものとされており（同法30条の5）、本人確認情報の通知等に関する事務は、市区町村長に義務づけられたものである。

第3 当裁判所の判断

1 本件行為が行政処分に当たるか否かについて判断する。

取消訴訟の対象となる行政処分とは、公権力の主体たる国又は公共団体が行う行為のうち、その行為によって、直接国民の権利義務を形成し、又はその範囲を確定することが法律上認められているものをいう。

本件行為は、市町村長が住民基本台帳法7条に基づき住民票に住民票コードを記載するものである。ところで、市町村長が住民票に同条各号に掲げる事項を記載する行為は、いわゆる公証行為であるから、その性質上国民の権利義務に直接的な影響を及ぼすものではなく、ただ、その行為が他の何らかの法的効果と結びつけられている場合に限って行政処分性が認められるものと解される。本件行為は、氏名、住所等の文字情報によって本人確認をする場合よりも、取り扱うデータの量を減少させて迅速な検索を可能にし、かつ、確実な本人確認を実現する目的で〈証拠略〉、住民票に11けたの数字を記載したものであるから、住民票コードは、既に記載されている住民票の内容を表現するものにすぎない。そうすると、本件行為は、基本的にはもともと市町村長が実施していた公証行為の延長線上にあるというべきであるから、その性質上、当該行為そのものによって直接新たに国民の権利義務を形成し、又はその範囲を確定するものとはいえない。また、住民票コードの付与が、例えば、当該市町村の選挙人名簿に登録されるか否かを決定付ける特定の住民の氏名等を住民票に記載する行為のように、何らかの法的効果と結びついていると解すべき根拠もない。

原告らは、原告らの本人確認情報というプライバシーが全国の市町村端末によって、また、一定の事務を扱う中央省庁において検索及び閲覧可能となることによって、原告らのプライバシー権が直接制限され又はその範囲が確定される旨主張する。しかし、原告らの主張は、住民票コードが原告らに付与されることに伴って、間接的あるいは抽象的に生じうる不利益をいうものにすぎず、採用できない。

2 以上によれば、本件行為は取消訴訟の対象となる行政処分とは解されないから、本件訴えはその余の点について判断するまでもなくいずれも不適法である。

よって、本件訴えをいずれも却下することとし、主文のとおり判決する。

富山地方裁判所民事部

裁判長裁判官 永野圧彦

裁判官 剣持淳子

裁判官 三輪篤志