

2003年7月8日

東京都知事 石原 慎太郎 様

審査請求人 柳田由紀子外494名
上記総代 柳田 由紀子

同 若林京子

同 神島 由紀子

反 論 書

事件の表示

処分庁西東京市長が行なった住基ネット接続及び住民票コード付定に対し、行政不服審査法に基づき、審査請求人らが2003年3月24日付で行なった審査請求

反論の趣旨

処分庁の5月16日付弁明書につき、審査請求人らは以下の項目について反論する。

(1) 弁明書5(1)について

別紙2記載者は、法定期間を過ぎて審査請求を行なったものであることは認めるが、住基ネット接続及び住民票コード付定を不服とする考えにおいては他の申請人と何ら変わるところはない。

(2) 弁論書5(3)について

住民基本台帳法(以下「住基法」という)30条の5の規定は認めるが、その余については反論する。

(3) 弁論書5(4)について

処分庁の主張には疑義があるため反論する。

(4) 弁明書5(5)について

住民票コードの記載が、住基法7条13号に基づくものであることは認めるが、その余については反論と求釈明を行なう。

(5) 弁明書5(6)について

法制定の事実や規定内容については認めるが、住基ネット接続が必要不可欠である

こと、西東京市において本人確認情報の安全確保に必要な措置が講じられていること、よってプライバシーの権利や自己情報のコントロール権を侵害しないという主張については反論する。

(6) 弁明書5(7)について

政府が「個人情報の保護に関する法律案」を国会に提出したことをもって個人情報の保護に万全を期するための「所要の措置」を講じたとして住基ネット施行期日を変更せず実施したので、処分庁の住基ネット稼働は違法・不当ではないとする主張について反論と求釈明を行なう。

(7) 弁明書5(8)について

住基法36条の2に規定されている住民票に記載されている事項の安全確保について、西東京市として講じている措置が列挙されたが、ガイドラインを示しただけであり、実効性について反論と求釈明を行なう。

(8) 弁明書5(9)について

住基ネット接続により、本人確認情報を東京都に通知したことは、個人情報を外部提供した西東京市個人情報保護条例10条第2項第2号に該当するとする主張について反論する。

(9) 弁明書5(10)について

住基ネット接続と住民票コード付定は違憲であるとの審査請求人らの主張に対する、処分庁は改正住基法の合憲性について判断するところではないとの主張について反論する。

反論

1 弁明書5(1)について

弁明書別紙2記載者は、処分庁に異議申し立てをせずに東京都知事に審査請求を行なった者で、法定期間経過後の請求であることは認めるが、住基ネット接続と住民票コード付定を不服とする意思表示として審査請求を行なったものである。

処分庁は、本件処分について、2002年8月5日時点で、本件行為が「処分」であることを西東京市民に公表せず、また、住民票コード通知書にもその旨記載しなかったため、通知を受けた西東京市民全員が審査請求期間の教示をされていない。不服に思っているにもかかわらず、法的に不服申し立てを行なえるということを知りえた市民は多くはない。

8月5日以前も以後も、西東京市は住基ネットについての説明会を開催せず、説明責任を果たしているとはいえない環境で、市民はそもそも本件行為が行政処分であるということすら周知されていない。よって、異議申し立てに対する処分庁の決定を知ったことで、本件行為が処分であると知った別紙2記載者が審査請求期間を過ぎて審査請求を行なったのはやむを得ないものである。

なお、審査請求期間を定めた行政不服審査法 14 条には、但し書として審査請求期間を過ぎてもやむを得ない理由がある場合はこの限りではないとある。

2 弁明書 5 (3) について

住基法 30 条の 5 の規定に基づき、処分庁は本人確認情報を東京都に通知したものであり、取消しを求める審査請求は不合法であること、また、都知事や指定情報処理機関が保有する本人確認情報を回復したり削除する権限はないとの処分庁の主張について以下のとおり反論する。

そもそも住基法 3 条第 1 項では、市町村長は、住民基本台帳に記載された住民に関する記録について適正に管理が行なわれるように必要な措置を講ずるよう努める責務があるとされている。

そして、住基ネットが構築された際、36 条の 2 が制定され、「市町村長は、住民基本台帳（中略）の事務の処理に当たっては、（中略）記載されている事項の漏洩、滅失及び毀損の防止その他の住民票（中略）に記載されている事項の適切な管理のために必要な措置を講じなければならない。」とされ、市町村長は、個人情報の安全確保のために具体的な方策を講ずる義務を果たさなければならなくなった。

都知事に通知した本人確認情報は、住基法 7 条に定められた住民票情報の一部であるから、同法 36 条の 2 の規定により、この情報が送信先でも漏洩、滅失及び毀損しないように防止する責任がある。ところが処分庁は住民の意思を確認することなく本人確認情報を東京都に通知しながら、通知後の本人確認情報の扱いについては口出しする権限がないという。ということは、とりもなおさず東京都に通知した本人確認情報が煮て食われようと焼いて食われようと知らないよと言うが如きものである。

東京都に送られた本人確認情報はどうなるか。そこから指定情報処理機関である地方自治情報センターに送られ、本人確認情報の提供が認められている 264 事務に利用されることになっている。国の省庁等の行政事務や民間事務等利用する側には住民票コードにより個人情報のデータが蓄積されていくし、既に行政機関等で構築してきた個人情報データベースもあるため、住民票コードは一人一人を識別する番号であるからこの番号をカギにして各種データを検索し必要なデータを結合することが可能となる。利用が進めば進むほど個人情報としての価値が高まる。利用価値が高まればいくら罰則規定を設けても漏洩の危険性が増す。

末端で利用業務に携わる人間は常に入れ替わるから、データに触れる人間つまり秘密を知り得る人間は増加する。また、「秘密よ」「秘密よ」と言い合って秘密が広がりついには皆が知っていたということもよくあることだ。住基ネットはコンピュータの技術的要因の他に、こうした人的要因で個人情報が漏洩する恐れがある。市町村長は通知後の本人確認

情報の扱いについては口出しする権限がないということは、このような危険性を自らチェックできないということでもある。

情報は民主主義を発展させる上で欠くことのできない社会的資産であるから、情報資産管理の公正性・公平性が担保されなければならない。情報資産管理の公正性・公平性を担保するのは、自己情報コントロール権の確立以外にない。情報コントロールに関して、住基ネットは情報の送信側と受信側でお互いの同意のもとに情報を共有できない点で公正性・公平性に欠ける。処分庁が東京都に送信した本人確認情報は一方通行でさらに東京都から地方自治情報センターに送られ、送信先のセンターでどのように情報提供されるのか制御できない状態におかれるわけであるから、これは処分庁の情報コントロール権がないことを意味する。

このような状況を処分庁が理解するならば、処分庁は審査請求人らの本人確認情報の安全性を確保するために、東京都へ送信した審査請求人らの個人情報の削除を要求すべきである。送信情報の削除権限がなくとも削除要求はできるはずだ。

審査請求人らは、処分庁により二重に権利が侵害された状況に置かれている。まず処分庁によって自らの個人情報を本人の同意なしに一方的に東京都に送信されたことでプライバシーと自己情報コントロール権を侵害され、さらに処分庁が、市町村長には通知した本人確認情報をコントロールできないということを知りながら、すなわち個人情報が漏洩する恐れに対してチェックもできず、個人情報をなすすべもなく危険な状態に晒すのを承知で住基ネットに接続したことで、プライバシーと自己情報コントロール権を侵害された。

これらの処分庁の行為は住基法3条及び住民票に記載されている事項の安全確保義務を定めた住基法36条の2に違反するものである。

ちなみに国立市は、2002年12月26日に住基ネットを切断したが、その理由のひとつに、「住民基本台帳事務を処理する国立市の住民情報のコントロール権が確立されていないこと」を挙げている。上原国立市長は、市報「くにたち」の中でこのことを「住民から届けられた個人情報の管理者として、住基ネットで拡散する個人情報が、どこでどのように取得、管理、消去されるのかを具体的に把握できず、かつその安全性を確認できない。」と説明している（資料1）。

市町村長のコントロール権が確立されていないのならば国立市のように住基ネットを「切断」する方法もある。

3 弁明書5(4)について

処分庁は、改正住基法附則3条の「市町村長は、施行日に、この法律の施行の際現に住民台帳に記録されている者に係る住民票に新法第30条の7第1項の規定により都道府県知事から指定された新法第7条13号に規定する住民票コードのうちから選択するいず

れかの住民票コードを記載するものとする」との規定により審査請求人を処分したものであり、住基法30条の2の規定に基づく処分ではないと主張するが、以下のとおり誤りである。

まず、住基法7条は、住民票に記載する事項について定めたもので、13号が住民票コードとなっている。この住民票コードは、住民一人一人に付ける番号であって重複を避けるためにこの住民票コードをどのように付けるか付け方を定める必要があり、都道府県知事で番号の調整を行い（住基法30条の7の第2項）、そこで分けた番号を市町村長に指定した（住基法30条の7の第1項）ものである。市町村長は、住民票コードの記載に関する経過措置を定めた附則3条に基づき、都道府県知事から指定された番号で、当該市町村住民に仮の住民票コードを割り振った。

住基ネットは2001年12月から2002年3月まで総合運用テストを行いその後、7月22日に仮運用が始まった。ここで用いられた住民票コードは、附則3条による住民票コードであることは言うまでもない。

住基法30条の2は、「市町村長は、住民票の記載をする場合には、当該記載に係る者につき直近に住民票の記載をした市町村長が当該住民票に直近に記載した住民票コードを記載するものとする」と規定しているとおり、2002年8月5日施行日に、市町村長は、附則3条の規定により記載された住民票コードを、この30条の2の規定により、直近に記載した住民票コードとして記載したものである。

よって、住基法附則3条と30条の2の規定に基づき住民票コード付定がなされたものであるから、審査請求人らがこれらの規定に基づく処分の取消しを求めて審査請求を行なうことは正当である。

4 弁明書5(5)について

住民票コードの記載は、住基法7条13号の規定に基づき義務付けられていることは認めるが、共通番号の付番によって成り立つ住基ネットは、処分庁が主張するように単に地方公共団体共同のシステムという性格のものではなく、国家が国民の一元的管理を図るシステムであるから以下のとおり反論する。

処分庁は「住基ネットは、地方公共団体共同のシステムである」と主張する。なるほど情報を取り扱う組織に国は入っていない。住民に対して住民票コードの付番を直接行うのは市町村長であり、市町村長は本人確認情報を都道府県知事に送信し、都道府県知事はそれを地方自治情報センターに送信する流れになっているからだ。国が直接関与し、管理するシステムではない。しかし、実態はどうであろうか。

国立市長は住基ネットを離脱する前に、運用実態について繰り返し総務省に質問書を送付したが、その第3回質問書に対する総務大臣の回答には、「住基ネットは、行政機関が本

人確認のために利用するものであり、一般の住民の方が閲覧等を行うことができる制度ではありません。」(総行市第376号平成14年12月19日:「住民基本台帳ネットワークシステムに関する3度目の質問書(回答)」の8)と記されており、ここに書かれた利用主体である「行政機関」は、現実には本人確認情報利用のための法整備がなされている国の機関である。自治体事務において住基ネット利用を必須とするものは住基ネット自体を通じた本人確認情報の通知以外、現状では存在しない。また、形式上はともかく、全体としてみれば自治体としての利用メリットをふまえて自治体が自発的・積極的に住基ネット構築を進めてきたわけではないことは、周知の事実である。

つまり、住基ネットは、「国の機関」の電子ネットワーク化(電子政府)のために必要とされ、主として国の機関の利用のために、国法である住民基本台帳法を改正することによって構築が進められたものであることを、まず初めに指摘しておく。

次に、住基ネットの成り立ちと仕組みについて概括する。

1994年に旧自治省において私的諮問機関「住民記録システムのネットワークの構築等に関する研究会」が発足し、1996年3月に同研究会が「住民基本台帳番号制度」導入の提言をしたことで住基ネットはその制度的基礎が固まった。1998年3月住基法改正案が閣議決定され、国会に提出された。1999年8月改正住基法が成立すると、同年10月には都道府県を構成団体とする「住民基本台帳ネットワークシステム推進協議会」が発足した。

同年11月には総務大臣が指定情報処理機関として財団法人「地方自治情報センター」を指定した。指定されたのは「地方自治情報センター」ただ一つであった。地方自治情報センター」はコンピュータの普及に伴い、自治体のコンピュータ化を推進・指導するために1970年に設立された機関である。指定情報処理機関は、住基法30条の12に規定された指定基準を満たす必要があり、同条第1項3号には「地方公共団体が基本財産たる財産の全部又は一部を拠出しているものであること」という基準が設けられているため、基準にみ合う機関は事実上「地方自治情報センター」しかなかったからである。

「地方自治情報センター」は、47都道府県、12政令指定都市、23特別区、601市、1061町、176村等約2200団体が会員となり、これらの団体から納入された会費等で運営されているためこの基準を満たしたものである。

ちなみに同センター理事長職は旧自治省の事務次官の天下り先ポストと化していることや、常勤理事等は総務省からの出向という旧自治省の外郭団体であることから、国の意向を強く受けた機関である。

このように指定情報処理機関は「地方自治情報センター」一つしかないため、住基法30条の10第1項の規定により、都道府県は2000年3月までにすべてが「地方自治情報センター」への委任手続きを終えた。この「地方自治情報センター」に「全国サーバー」が置かれすべての本人確認情報が収集・管理されることになった。

都道府県は法的には住基ネットの運用主体であるが、実際は、市町村から送信された本人確認情報を、実質的には国の出先機関（国の利用利便のために、本人確認情報を一括して受け取り、これを管理運用する機関）として機能するよう設計・構築されている全国センター（地方自治情報センター）へ送信するだけであり、住基ネットに係る実際の仕事すなわちシステム管理・業務プログラム等の配信・コールセンター・ジョブスケジュールの管理実行等の運用管理は「地方自治情報センター」が独占的に実施し、その結果、本人確認情報の利用利益は国が独占する体制が作られている。

以上のとおり、住基ネットの成り立ちと情報管理の仕組みをみれば、実態として、住基ネットは地方公共団体の要請で構築された制度ではなく、国が導入を図り整えてきた制度に地方公共団体が組み込まれていったものであり、その中で「地方自治情報センター」がすべてを仕切る構造になっているのは明らかである。国（総務省）お墨付きの独占機関である「地方自治情報センター」が、住民の意思にかかわらず集約した本人確認情報を一元的に管理する体制は、実質的に国の住民管理強化を図る仕組みに他ならない。

処分行は、4つの理由を挙げて、住基ネットは国家が一元的に管理するシステムではないとしているので、これに対して個別に反論する。

第1の理由、保有される情報は本人確認のための氏名、住所、性別、生年月日の4情報であると主張されていることについて反論する。

住基ネットの各サーバーに保有される情報の内容については、上記4情報と変更履歴及び住民票コードそのものを含む6情報（住基法で規定される「本人確認情報」）である。弁明書のこの記述には明らかな誤認があることをまず指摘しておく。

4情報については住基法11条第1項の規定によりこれまでも閲覧請求が可能な公開情報であるが、同条第3項の規定により、市町村長は、請求が不当な目的によることが明らかなきときは請求を拒んだり、不当な目的に使用されるおそれがあること等の場合は請求を拒むことができるとの歯止めがなされている。

たとえばドメスティックバイオレンスの場合は、住基法のこの条文により、住民票公開を拒否することができた。住民票を公開するか否かは当該市町村長の責任で行なうことができたので、窓口の対応で処理できた。しかし住基ネットの場合は、市町村の窓口で対応ができない。つまり、住基ネット上の個人情報は、国の機関等の請求によって自動的に提供されるようにシステムの構造と機能が構築されていて、ここでは市町村長の判断による請求拒否の権限執行は不可能となっている（これは住基ネット自体の重大な欠陥のひとつであるといわざるを得ない）。そのため、市町村が都道府県に送信し、地方自治情報センターに送った本人確認情報のデータについて、市町村長は住民を守る責任が果たせない。

また、本人確認情報（6情報）の問題として考えると、たった6情報というわけにはい

かない。住民票コードは住民識別番号であるから、これをカギにして、さまざまな個人情報を収集し結合できる可能性がある。住民票コードは、個人情報の一元的管理を実現する個人識別コード（いわゆる国民IDコード）としての特性を、すべて備えているものである。

このことは、国（総務省）も十分承知しており、現在の住基法への改正を審議した1999年の国会審議においても、例えば春名衆院議員（共産党）の質問（4月20日）に対して、当時の鈴木自治省行政局長は「住民票コード自体は数字の羅列であり、それだけではプライバシーではないが、住民票コードと4情報が結びつくとプライバシーとなり、秘密情報となる」という主旨の答弁をしている。

従って、弁明書において「保有されているのは4情報」としたのは住基事務を取り扱っている自治体としてはきわめて不見識といわざるを得ず、このような自治体に「個人情報」の取り扱いをゆだねることに不安を覚える。

国や自治体が持つ多様な個人情報を結合（データマッチング）する上で、高い精度と効率を実現できる「住民票コード」（一人一人の個人を識別するIDコード）が国の行政機関等に提供される本人確認情報に含まれていることは、「国家が国民の一元的管理を図る」ためのシステム構築の基礎とすることができるものであり、従って、住基ネットによって保有される情報は4情報（正しくは6情報）であるとする処分庁の弁明は、住基ネットが国家による国民の管理強化であるとする審査請求人らの主張をなんら否定し得ない。

第2の理由、国の機関等への情報提供は、居住関係の確認のための求めがあったときに限定することについて反論する。

地方自治情報センターでの情報提供が限定されても、提供した情報がどう管理されるか処分庁は把握できないし、個人情報が漏洩しても、調査ひとつ頼めない。市町村長は地方自治情報センターと何ら法律関係がないためである。

また、地方自治情報センターと直接契約関係を持つ都道府県を通じて調査を依頼したとしても、市町村は信頼性のある調査結果が得られると期待することはできない。なぜなら、国の電子政府構想が想定している国の機関等の本人確認情報利用システムは、住基ネットから提供を受けた本人確認情報の取り扱いについて、本人確認情報の参照・移動・提供、コピーの作成・提供・参照・保存、およびオリジナルの本人確認情報とそのコピーの削除等最終処分の過程について高い確度でトレースできる機能をシステムとして実装していると考え根拠はまったく開示されていないためである。また、将来において構築されるシステムにおけるこうした機能の実装についても、明示的な方針が国の機関などにおいて確立・制度化されてはいないためである。

さらに、全国サーバーから国の機関等への本人確認情報の提供の方法には、ネットワークを通じた照会に対する個別の本人確認情報の提供とは別に、一括提供方式が想定されており、これは磁気媒体に記録された大量の本人確認情報を一括して国の機関などに提供す

るものであるといわれている。この一括提供方式によって住基コードを含む本人確認情報の提供を受けた場合、2003年8月中に住基システムが実装するとされている「アクセスログ」には、一括提供のためにコピーが作成された旨は記録されると考えられるが、その後の参照は住基ネットの本体システムとは直接接続されていないシステムによって参照されるため、個別の照会にもとづく提供時のようなアクセスログは作成されず、開示請求によって本人開示される情報も「一括提供」の記録にとどまるものと考えられる。

当然のことながら、一括提供された本人確認情報を参照利用するシステムにも、上記した本人確認情報の取り扱いを高い確度でトレースできる機能が実装されていると期待する根拠は存在せず、市町村が信頼性のある調査結果を入手できると期待することができないことは、個別照会による提供方式と何ら変わらない。むしろ、一括提供された本人確認情報の個別参照アクセスログは住基ネットの側に記録されないため、一括提供方式は目的外利用がより容易であり、目的外利用が行なわれた場合その実態を調査することはより困難であるといわざるを得ない。

住基法30条の7第3項で定めた居住関係の確認のために国又は法人が住基ネットを利用できる事務は264もあり、その約6割が国の所管事務とされている。また、今後の電子政府構築の進展にともない、この数は拡大するものと予想されている。この結果、国の機関等には、住民票コードで管理された個人情報のデータベースを構築することがきわめて容易になる。

確かに、国は「提供された本人確認情報は、参照の目的が果たされれば直ちに削除する」旨を表明しているが、これは制度的にもシステムに実装された機能としても、なんら担保されていない。また、「データマッチングは行なわない」旨も国はしばしば言明しているが、先日成立した個人情報保護関連法には、多くの自治体の個人情報保護条例に記載されるような「個人情報の電子的結合の禁止」規定は注意深く排除され、存在しない。従って、本人確認情報の提供を受けた行政機関等の内部で目的外利用の必要が生じたと認識された場合、これを有効に抑止しあるいは阻止する方策は講じられていないといえることができる。

以上から、国の機関等への情報提供は住民の居住関係の確認のための求めがあったときに限定されるとの処分庁の弁明理由は、住基ネットが国家による国民の管理強化になるとの審査請求人らの主張を否定し得ないことは明白である。

処分庁はむしろ、前述したように住基ネットによって提供された住民票コードを含む本人確認情報の利活用環境が、処分庁の責任に基づく調査の依頼等に誠実に答えるための制度・機能において未整備であること、合法・非合法を問わず本人確認情報なにかんずく住民票コードの目的外利用を容易に行ないうる環境であること、また住民票コードが目的外利用された場合には直ちに国による国民の管理を強化拡大する結果に繋がることに注目し、こうした環境に住民の個人情報を提供することが安全であるかどうかを慎重に検討して責任ある判断を下す必要があった。

付記するなら、住基法上では、国の機関等が本人確認情報の提供を求める場合の目的は「居住関係の確認」に限定されておらず、別表に定められた住基ネットの利用事務が現状では居住関係の確認の範囲であることに基づいた言明と理解できる。従って、別表に掲げられる利用目的を「居住関係の確認」の範囲を超えて改訂することは、同法1条の「国及び地方公共団体の行政の合理化に資すること」を根拠として、常に可能であるとも考えられ、その点で処分庁の弁明は継続的な妥当性に欠けていることも指摘しておく。

第3の理由、個々の目的ごとに法律上の根拠が必要であることについて反論する。

都道府県知事と指定情報機関の本人確認情報の利用及び提供については、住基法30条の30に規定されており、国又は法人については上記のとおり30条の7の第3項に規定されているが、当初対象事務は93であったものが264に増えた経緯からすれば、電子政府構築の進展にともない、今後更に増えることは确实と考えられる。

法律で定めれば本人確認情報の利用範囲は拡大でき、あるいは、利用事務が法的に規定されていても、利用目的が「居住関係の確認」でありさえすれば特段の規制を受けていないのであるから、個々の照会がどのような最終的目的をもって「居住関係の確認」を行なっているかについては、都道府県も処分庁も信頼性のあるチェックができないことは前述したとおりである。

以上から、たとえ法律上の根拠にのみ基づく本人確認情報の利用が行なわれていたとしても、現状において、また将来にわたって、住基ネットが国民に対する管理強化に繋がるものではないことを担保することはできていない。従って、処分庁の「個々の目的ごとに法律または条例上の根拠が必要」とする弁明が、住基ネットが国家による国民の管理強化であるとする審査請求人の主張を否定しえないことは明らかである。

第4の理由、目的外利用の禁止および一元的収集管理の否認について反論する。

目的外利用については、昨年の防衛庁リスト問題で明らかのように、目的外利用がたとえ禁止されていても、行政側はいつでもある意図をもって個人情報を集め、データ化することができる立場にあるし、利用目的に関連づければ何も問題にならない。また、そもそも役所内では、目的外利用とかの意識なく個人情報にアクセスすることが日常茶飯行なわれている可能性を否定できない。例えば、2002年6月、三重県四日市市において、複数の市職員が納税記録等のデータにアクセスし、他人の情報を照会していた事実が明るみにでた。発覚しなければ不正行為は続いていたのだから、他の自治体や省庁内部でもあり得ないことではない。

住基ネット利用対象事務に携わる人間は時間とともに増加するわけだからいくら秘密保持を定めても、秘密を知る人間は増える。利用対象事務で知りえた住民票コードをカギとして、他の省庁の個人情報データベースを検索・照合・結合することが可能になり、そうした行為が秘密裏に行われても、処分庁はチェックすることができない。

以上については、すでに第 1 の理由ないし第 3 の理由に対する反論の中で言及してきたことである。あえて指摘するなら、国の機関等における個人情報の目的外利用が禁止されたのは、2003 年になって成立した行政機関個人情報保護法などによるものであり、住基ネットが稼働した 2002 年 8 月 5 日の時点では、まだ国の機関による個人情報の目的外利用は法的に禁止されていなかったといえる。

なお、この行政機関個人情報保護法には目的外利用を禁止することが明記されたが、これには多くの例外規定が設けられており、その中には「相当な理由があるとき」には他の行政機関などに個人情報を提供することができること、行政機関内部での利用においても「相当な理由があるとき」は目的外利用が可能となることが規定されている。

次に、一元的に収集・管理することを認めていないとの弁明についてであるが、意味内容があいまいである。

収集管理の対象を本人確認情報と理解するなら、住民の本人確認情報は、住基ネットの全国センターに置かれたいわゆる全国サーバー上に一元的に収集され管理されているので妥当ではない。また、国の機関等が運用する個々の行政システム上の個人情報についての言及であると理解するのであれば、こうした個々のシステムが保有する個人情報の一元的な収集（データマッチング：個人情報ファイルの結合）やその管理利用については、住基ネット稼働開始時点でもまた現在でも、これを禁止する法規程等は存在していない。また、個人情報の結合が目的外利用にあたりとされても、行政機関個人情報保護法には前述したように「相当な理由があるとき」には目的外利用を可能とする例外規定があり、これを適用したデータマッチングは可能であると考えられる。

以上から、処分庁の「目的外利用の禁止」および「一元的な収集・管理を認めていない」との弁明には法的根拠がなく、住基ネットが国家による国民の管理強化であるとする審査請求人の主張を否定し得ない。

なお、処分庁が「目的外利用をも禁止し、一元的に収集・管理することを認めていない」とした根拠及びその意味するところを明らかにするよう釈明を求める。

以上のとおり、住基ネットは法的にも実態的にも、住民の個人情報について市町村長のコントロールが及ばない制度であり、国が国民を一元的に管理支配する手段として有効的に機能するシステムである。よって、処分庁が審査請求人ら本人の意思を問うことなく一方的に住民票コードを付番し、一方的に本人確認情報として住基ネットにのせたことは、間接的であるにせよ実質的には国のコントロール下に個人情報を無防備に晒したものであるから、地方自治の本旨及び住基法 3 条、同 36 条の 2 に違反する。

5 弁明書5(6)について

処分庁は、住基ネット接続は必要不可欠であり、住基法には本人確認情報の保護措置が規定されており、西東京市では、西東京市個人情報保護条例及び西東京市情報セキュリティポリシーにより、本人確認情報の安全確保に必要な措置を講じているから、接続はプライバシーの権利や自己情報コントロール権を侵害しないと主張する。これらにつき以下のとおり反論する。

住基法で本人確認情報の保護措置が規定されていることと実効性のある保護措置が講じられていることは別である。また、住基法の保護措置の規定だけでは不十分であるため、住基法改正時に、所謂附則1条第2項が付け加えられたのである。だから、住基法に保護措置の規定があるだけでは、本人確認情報の安全確保ができないのは自明である。

また、西東京市においては、西東京市個人情報保護条例及び西東京市情報セキュリティポリシーとしていくつかの規則等が定められているが、これらの規則もガイドラインとしての限界を強く持ち、実効性が確保される内容には到底なり得ていないため、本人確認情報の安全性が確保されているとはいえない。西東京市個人情報保護条例については後述する。ここでは、西東京市情報セキュリティポリシーではセキュリティが確保できないことを指摘する。

1) 防御対策

現在の情報通信技術においては、完璧なセキュリティを確保することはできないというのが技術自体が持つ基本認識であることを、処分庁は理解すべきである。セキュリティ上の100%の安全性を確保しようとするところみは、それ自体、経験的にもまた理論的にも限りなく安全対策を積み重ねていくことが必要とされる。従って膨大な経費の投入を招く結果となる。

現在の情報通信技術におけるセキュリティ対策は、こうした事実をふまえ「完璧なセキュリティは存在しない」ことを前提に防御策を構築するものである。まず未然に事故を防ぐために一定レベルの防御対策を施し、万一事故が起きた場合は被害を最小限に抑える手立てをあらかじめ講じておくというのが、取り得る対策とされている。すなわち事前の備えとしての事故防止対策と有事の際の危機管理対策である。

実施するセキュリティ事故防御対策の内容・レベルは、そのシステムやシステムが取り扱う情報資産の特性などによってシステム所有者・運用者の責任で判断されることになる。しかしながら住基ネットのような分散開放型ネットワークシステムでは、市町村、都道府県、および本人確認情報の主要な利用者である国の機関等多数にのぼるサブシステムがシステムに参加(接続)するため、このことから生じるセキュリティ確保の難しさも十分考慮してセキュリティ対策をとる必要があるとされている。

つまり、住基ネット上で提供される個人情報(本人確認情報)の安全は、処分庁が運用

する西東京市のシステムのセキュリティレベルによって決定されるだけでなく、全国の自治体及び本人確認情報の提供を受けるすべての国の機関等のサブシステムのセキュリティレベルによっても決定されるものであり、処分庁の運用するサブシステムのセキュリティレベルをどのように強化したとしても、それだけでは西東京市住民の個人情報の安全は確保できない。しかしながら、処分庁の弁明は、他の自治体、国の機関等のセキュリティレベルについて言及していない。

とくに現実の住基ネットでは、システムの運用主体は都道府県とされ、しかし実際の運用は地方自治情報センターに委託されており、その関係の中では、少なくとも処分庁を含む市町村には、住基ネット全体のセキュリティについて安全レベルを評価したり、安全レベルを強化する対策を直接実施することはできないようになっている。つまり、処分庁には、住基ネットに接続する3000以上のサブシステムのひとつとして、自己の運用するサブシステムのセキュリティレベルを確保することは可能であり、確保すべき責任を負っているが、他のサブシステムのセキュリティレベルを評価し対策を実施したり実施するよう要求する権限はない。

この問題は、住基ネットが多数のサブシステム（ノード）の参加する分散開放型ネットワークシステムであるにもかかわらず、分散開放型ネットワークシステムの技術が必要としている相互信頼にもとづくセキュリティ確保の条件を満たしていないことを意味しており、住基ネットが現に持っているセキュリティ上の重大な欠陥であるといわざるを得ない。またこの欠陥は、セキュリティ事故防御対策だけでなく、危機管理対策においても同じと考えられる。

以上の事実からだけでも、処分庁の「西東京市個人情報保護条例及び西東京市情報セキュリティポリシーにより、本人確認情報の安全確保に必要な措置を講じているから、接続はプライバシーの権利や自己情報コントロール権を侵害しない」とする弁明は根拠を持たないことが明らかである。

以下、2003年5月28日に公表された「長野県本人確認情報保護審議会第1次報告」の一つ、3『住基ネットのセキュリティ確保について - コストと効果 -』（吉田審議委員）（資料2、16頁以下参照）の添付資料[ITセキュリティ保護のコストについて]（資料3）に基づいて具体的な反論を行なう。

本資料は、「事前の備え」の具体策としては

強固なセキュリティシステム

24時間365日の不正侵入監視（IDS・Firewall）

セキュリティ専門技術者によるアナライズとレポートを挙げ、

「危機管理」の具体策としては

コンサルティングによって定める対応フォーマーション

有事の際の対応フロー策定

証拠保全のオペレーション

被害を最小限に抑える対応

を挙げている。前者については、ある程度コストをかければ一定程度の安全性は確保できるが、後者については、多額の経費がかかるという。不正侵入検知システム（IDS）は単に設置すれば事足れりというものではないからだ。きちんと運用できなければ意味がない。

上記報告は、IDS運用上の問題点をいくつか指摘している。一例を挙げれば、NIDS（ネットワーク型IDS）で攻撃の警告＝アラートがあった場合、直ちにその警告の真偽を判断し、本当の攻撃の場合は関係する周辺機器を絞り込み、ログの解析を行い、攻撃が成功しているかどうか判断しなければならないがそれには相当熟練した技術が必要だという。

地方自治情報センターのサーバーには全住民票コードが集約されているので、攻撃を受けるリスクも大きい。また、地方自治情報センターのNIDSでは検知されない攻撃の例（市町村から都道府県に対する攻撃 市町村から市町村に対する攻撃）地方自治情報センターのNIDSには検出されるが、大量のアラートを出すことで実質的にIDSを無効化する例（3通り）も指摘されており、こうした攻撃に対して住基ネットではどのように防御対策を実施しているのか、大きな不安を持たざるを得ない。

総務省は「長野県個人情報保護審議会第1次報告」に反論する文書「長野県個人情報保護審議会第1次報告についての考え方」を公表したが、セキュリティ対策については「IDS（侵入検知装置）を設置し、同様に常時監視」とだけ記され、NIDSでは検知されない、またはIDSを無効化する攻撃に対する防御対策については何ら言及されておらず、住基ネットにおけるこの種のセキュリティホールは存在は否定されていない。

以上から、処分庁の「西東京市個人情報保護条例及び西東京市情報セキュリティポリシー」により、本人確認情報の安全確保に必要な措置を講じているから、接続はプライバシーの権利や自己情報コントロール権を侵害しない」とする弁明は、この種の規定や実施手続きに関するセキュリティ対策（人的要素に係わるセキュリティ対策）と相互補完すべき技術的対策に大きな問題が指摘されるような状況では、根拠を持たないことは明らかである。

次に、処分庁の具体的な対策に即して反論する。

「西東京市情報セキュリティポリシー」として一括される規定においては、「西東京市情報セキュリティ基本方針」、「西東京市住民台帳ネットワークシステムセキュリティ対策基準」（以下「市住基ネットセキュリティ対策基準」という）、「西東京市情報セキュリティ対策基準」（以下「市情報セキュリティ対策基準」という）及び「セキュリティ実施基準」が

定められており、セキュリティ事故に対する基本的な防御体制・対応体制は、形式としては一定のレベルで整えられているものとも見える。しかしこれらは多くの場合、実施すべきセキュリティ対策の項目名を多数列挙した「セキュリティ確保のガイドライン」ではない。従って、こうした規定を設けることと、実際の運用面で実効性ある対策が実施されているかどうかは別である。

たとえば、「市住基ネットセキュリティ対策基準」では、住基ネットセキュリティ管理者（市民生活部長）、住基ネット運用責任者（市民生活部市民課長）等を置き、それらの責任で住基ネットセキュリティ対策を行なうことが定められているが、役職名が指定されているためこれら責任者が対策の個々の内容に精通していることを期待することはできない。また、住基ネット業務の外部委託ができるようになっているので、実際は委託業者に業務を丸投げしている場合、実効性あるセキュリティ対策がとられているかどうか、責任者が的確に判断することを期待する根拠をこれらの規定の中に見いだすことは困難である。実質的な責任はどうなるのか。また、監査について言えば「市情報セキュリティ対策基準」には規定があるが、「市住基ネットセキュリティ対策基準」自体には第三者による監査の定めがなく、検証が客観的に担保されていない。

「市情報セキュリティ対策基準」について見ると、これは、一般的な電子情報のセキュリティ対策の項目を定めたものであるから、これらの規定の中で具体的に住基ネットに係るセキュリティ対策がどれだけ立てられているのか不明である。

たとえば、総則、管理体制の整備、規定の整備の後に人事、教育、訓練の項があり、同基準第18に、「情報セキュリティ教育責任者は、情報システムのセキュリティ対策、運用管理に係る教育、訓練に関する計画及び実施の体制を確立し、関係職員に対して教育、訓練を実施する。」とあるが、実際にどのような計画がたてられ実施されているのか明らかでない。

監査についても、同基準第19に自主診断体制の確立、同基準第20に第三者による監査体制の確立、同基準第21に自主診断又は監査の実施、同基準第22に自主診断又は監査に基づく改善がそれぞれ定められているが、それらの体制の構成メンバーも明示されておらず、実際に機能しているのかどうか明らかでない。なお、住基ネットのサブシステムを含む処分庁が運用する情報システムに対して、実際にどのような自主診断・監査が実施されているのか、あるいは計画されているのか、市民に対して情報が積極的に開示されていない。この問題に代表されるように、「情報公開」にもとづく信頼関係の構築を旨とする「セキュリティポリシー」としては、「西東京市セキュリティポリシー」の諸規定は機能していないことを指摘しておく。

同基準の危機管理計画については、第23～24に計画の策定、確認が定められているが、システム管理者として危機に対応しうる高度な技術職員を確保できているのか不明である。

同基準第25に、障害発生に対する備えとして情報システム保険に加入することが定められているが、何をどこまでカバーする保険に加入するのか不明である。

以下第172までセキュリティ対策が定められているが、最後に第173から第179まで外部委託管理の項目が定められている。業務委託の場合、前述した長野県本人確認情報保護審査会の報告が指摘するような問題に対処できる高度な技術者を24時間体制で確保する旨の規定はない。

少なくとも、以上で指摘してきた問題点について、実効性のある具体的な対策がとられていることが処分庁から示されなければ、セキュリティについて「本人確認情報の安全確保に必要な措置を講じている」とは到底いえない。

さらに、前述したように住基ネットのような分散開放型ネットワークシステムにおけるセキュリティ確保については、市町村段階、都道府県段階、地方自治情報センター及び国の機関等の段階の各段階において、実効的な安全確保対策が講じられ機能していることが明示されていなければならない。自分のところだけは大丈夫では済まないのが住基ネットである。各段階で実施できているのだろうか。前掲した長野県本人確認情報保護審議会の報告を読む限り、少なくとも長野県では不十分であることがわかる。

2) 接続環境

防御対策以前の問題として住基ネットの接続環境の問題もある。

前記長野県本人確認情報保護審議会の報告2『住基ネットの現状と市町村LAN環境について』(佐藤審議委員)(資料2、8頁以下)には、調査した市町村におけるネットワークの接続状況について、住基ネットとインターネットが何らかの装置を介して繋がっている事例が複数存在していたことが記されている。

安全性の高いネットワーク接続形態は、住基ネットに繋がる基幹系ネット(既存住基システム)とインターネットに繋がる情報系ネット(庁内イントラネット)が物理的に分離していなければならないが、同報告では、住基ネット端末などがインターネットなど外部システムと接続され危険性が高いと考えられるネットワーク接続事例が6つも紹介されている。

こうした事例をみれば、西東京市の住基ネット端末はインターネットや外部システムと接続していないから安全だとは決して言えないことが分かる。3千余の自治体すべてが安全性の高い接続形態になっていることが担保されていなければ、外部からの侵入に対して信頼できる防御対策が実施されているとは言えないのである。

長野県では住基ネット稼働後に一部現地調査を含む信頼性の高い実態調査をしたので、このような危険性の高い接続形態の存在が具体的な形で判明したが、他の都道府県につい

ては、総務省による包括的なセキュリティ対策に関するアンケート調査の結果（後述する）があるだけで、信頼性の高い実態調査の結果は存在していない。

長野県で複数の自治体が危険性のある接続形態であったということは、住基ネット稼働以来当該自治体が是正するまで、他の住基ネット接続自治体においては、本人確認情報の安全性が脅かされているということである。審査請求人らの本人確認情報も当然含まれている。幸い被害は発生していないが、被害が発生するおそれは十分ある。

処分庁が、住基ネット運用開始時において住基法 36 条の 2 の住民票記載事項の安全確保義務を果たしていれば、このような危険な状態に本人確認情報を晒すことはなかったのであるから、住基ネットに接続した処分庁の行為は住基法 36 条の 2 に違反する。

なお、住基ネットの運営主体である都道府県によって構成される住民基本台帳ネットワークシステム推進協議会（以下住基ネット推進協という）は、このような問題が発生する可能性に気づいていたものとも思われ、住基ネットの構築段階における主要文書のひとつである「住民基本台帳ネットワークシステムセキュリティ基本方針書」において、「住基ネットの統一性及び均質性等を保持する」ことによってシステム全体のセキュリティレベルを確保する方針を採用している。

しかし、住基ネット推進協を「指導」する立場にある総務省の発表によれば、住基ネットの端末が何らかの形でインターネットに接続されていてセキュリティ上の大きな問題があるとされた自治体の数は、

- 1) 2002年7月31日の総務省発表：約200自治体（毎日新聞8月8日報道から）
- 2) 2003年2月13日衆議院予算委員会における片山総務大臣の答弁：30位
（衆議院予算委員会会議録2月13日第10号 河村議員の質問に対する答弁から）
- 3) 2003年6月5日総務省自治行政局市町村課の文書：全国の市町村の1割強
（「長野県個人情報保護審議会第1次報告についての考え方」より）

となっている。2)において大幅に減少したにもかかわらず、3)においては昨年7月の発表よりもさらに大きな数字となっている。このことは、総務省あるいは住基ネット推進協が統一的・均質的なセキュリティ構築に必須と考えられる全市町村の実態把握にすら失敗していることを示している。

上記3)の根拠となった、総務省の2003年1月から2月実施になるアンケート調査の結果（「住民基本台帳ネットワークシステム及びそれに接続している既設ネットワークに関する調査票による点検結果（平成15年5月12日）」）を具体的に参照してみると、調査票の設問は「インターネットへの接続を行っていない」となっており、長野県の報告書にある「加入電話網を通じて、出先機関または保守作業委託先事業者と接続している事例」および「持ち込みPCを容易に、住基ネット端末が接続されているLANのHUBに接続可能な事例」については調査対象とはなっていない。また回答集計を見ると、

- ・回答3 運用している
(定められた手続きが関係する職員に周知され、適切に運用されている): 60.7%
- ・回答2 整備している
(質問項目を実現する手続きが文書等で定められている): 13.2%
- ・回答1 整備していない
(規程等を常備していない。質問項目について文書等で定められていない): 12.1%

というもので、必ずしも「1割強」がインターネット接続をしているとはいえ、また、あえて「回答2」を選択した市町村の実態が「接続していない」とも言いがたい。従って、この調査結果から信頼性の高い市町村の実態をイメージすることは困難であり、総務省及びその指導を受ける住基ネット推進協は、市町村における住基ネット端末のインターネット接続の実態を現在の時点でも信頼できる精度で把握できてはいないこと、従って住基ネットのセキュリティが統一的・均質的に構築されたとする根拠を総務省並びに住基ネット推進協は持っていないと言える。

以上の事実と長野県本人確認情報保護審議会第1次報告書における精度の高い市町村の実態調査結果を合わせて考えるなら、住基ネット推進協の統一的・均質的なセキュリティ構築という方針が破綻していることは明らかで、住基ネットの全体としてのセキュリティレベルは、処分庁が希望的に想定した安全のレベルには到底達していないものと評価せざるを得ない。

よって、処分庁の「西東京市個人情報保護条例及び西東京市情報セキュリティポリシーにより、本人確認情報の安全確保に必要な措置を講じているから、接続はプライバシーの権利や自己情報コントロール権を侵害しない」とする弁明は根拠を持たないことは明らかである。

6 弁明書5(7)について

改正住基法施行についての大きな問題は、附則1条第2項に規定された、「この法律の施行に当たっては、政府は、個人情報の保護に万全を期するため、速やかに、所要の措置を講ずるものとする。」という約束が反故にされたことである。「所要の措置」について、政府は個人情報保護法案を国会に提出したことをもって「所要の措置は講じた」としたが、処分庁は、この政府見解をそのまま引き写し、施行日が変更されずに実施されたから住基ネット稼働は違法ではないと主張する。これについて以下のとおり反論と求釈明を行なう。

まず第1に、政府の言い訳は法治国家の理念に反するもので到底認められない。附則1条2項が付け加えられたことは、住基法30条の29から43に定められている「本人確認

情報の保護」規定では、個人情報保護をすることができないという判断が基になっていることを意味している。このままの状態では施行日を迎えたなら、個人情報は危険にさらされるのでそれを防ぐための手立てを講じておかなければならないということであった。所要の措置を講じる時期については「この法律の施行に当たっては」との文言に示されているように、施行日前に講じておかなければならないということである。

しかるに、2002年8月5日までに、何の法的措置もとられなかった。個人情報保護関連法案は提出されたが成立しなかった。法案は成立して法律にならなければ無意味・無価値である。個人情報保護法案を提出しただけで個人情報が保護される環境になったとは誰も認めない。そんなことが認められたら法治国家ではない。法的環境は変わらず個人情報の保護を保障できないまま住基ネットは稼働されたのであるから附則1条第2項の要件をみたしておらず違法な稼働である。

第2に、政府が提出した個人情報保護関連法案（主要には「個人情報保護法案」「行政機関個人情報保護法案」）の中身で、住民の個人情報が守れるのかという問題もある。個人情報保護関連法案は一部修正の上再提出され、2003年5月23日に関連5法案が可決・成立したが、多くの疑問が出されている。

例えば、行政機関個人情報保護法では、公務員の不正利用に対する罰則規定が設けられたが、先般起きた「防衛庁による自衛官募集に際しての情報収集問題」等のような職務上の行為については規制できない。個人情報の利用目的の変更や目的外利用、他の行政機関への提供について本人の同意は不要であるため、個人情報がどのように使われているか分からない。自治体の個人情報保護条例ではほとんどで設けられているセンシティブ情報（思想、信条、宗教、社会的差別の原因となる事項等）の収集を原則禁止する規定がない。行政保有の電子情報について、個人情報データを検索・照合・結合を原則禁止する規定がない。

以上のとおり、当該処分があった2002年8月5日時点で、何ら個人情報を保護する法的措置はとられなかったし、現在成立した個人情報保護関連法も、住民の個人情報を保護する万全なものになっていない。

弁明書によれば処分庁は、このような状態について何ら検討・判断することなく、また政府見解が十分に本人確認情報の保護の視点から実効性を持つものであるとする根拠を示すことなく、単に「改正住民基本台帳法にもとづき」住基ネットに接続したとしている。これは、住基法36条の2に規定された市町村長の責務を放棄した行為であり、違法・不当な処分である。従って処分庁のこの弁明は、何ら審査請求人の主張を否定するものとなり得ていない。

処分庁の弁明の主旨にはあいまいな部分が多いため、審査請求人らは処分庁に対して、次の求釈明を行なう。

第1に、個人情報保護法案を国会に提出したことをもって「所要の措置は講じた」というのは政府の弁明であるが、住基法は自治事務であるから、市町村長は、事務を遂行するにあたっては自らの責任で判断し、運用していかなければならない。処分庁としては政府の処置のどの点を適切なものだと判断したのか。

第2に、処分庁は個人情報保護法案が成立しない状態をどう考えていたのか。

第3に、個人情報保護法案の内容についてはどのような判断をもっていたのか。個人情報保護法案で個人情報の保護が万全になると考えたのかどうか。

7 弁明書5(8)について

改正住基法36条の2の安全確保義務について、制度面、システム面、運用面で適切な保護措置を講じているので安全確保義務違反はないとの処分庁の主張に以下のとおり反論と求釈明を行なう。

1) 制度面について

制度面で講じている適切な処置として次の4項目が挙げられている。

本人確認情報の提出先や利用目的を法律により具体的に限定。

関係職員に対する「安全確保措置」及び「秘密保持」の義務付け。

提出先が本人確認情報を目的外利用することの禁止。

民間部門の住民票コードの利用の禁止。

これらは単に改正住基法第4節「本人確認情報の保護」のうち、30条の30、30条の31～36、30条の43の内容を紹介しただけである。これらの条文は本人確認情報保護の基本的な取り決めにすぎない。繰り返して言うが、個人情報保護については、改正住基法のこれらの保護規定だけでは不十分であるから附則1条2項の「個人情報の保護に万全を期するため」「所要の措置を講ずるものとする」という条文がつけられたのである。

ところが、住基法36条の2は、市町村長がとるべき措置についての規定であるから、改正住基法の規定があるから制度面で適切な処置をとったとはいえない。

2) システム面について

システム面では次の5項目が挙げられている。

ICカードや暗証番号によるコンピュータ操作者の確認。

蓄積されているデータへの接続制限。

操作者の履歴管理。

通信相手となるコンピュータとの相互認証。

専用回線上の本人確認情報の暗号化。

これらは、西東京市住民基本台帳ネットワークシステムセキュリティ対策基準及び西東京市情報セキュリティ基準等に定められているセキュリティ対策であるが、既に指摘したとおり、これらはガイドラインに過ぎず、セキュリティを確保する上での実効性ある処置としては不十分である。

3) 運用面について

運用面では次の3項目が挙げられている。

情報保護管理者の設置。

安全確保のための対策会議の開催。

監査等の管理体制に関する措置

すでに指摘したように、これらの体制は形式的に整っていたとしても、有効に機能するかどうかは分からない。担う人材が情報技術に精通しているかどうか、適切な判断が下せるのかどうか検証する有効な手立てが講じられていない。

ここで重要なのは監査である。審査請求人らは、システムの監査については、住基ネットが分散開放型ネットワークシステムであることをふまえ、最新の分散開放型ネットワークの技術とセキュリティ確保・プライバシー保障について十分な知識と経験を持つ第三者機関が実施する必要があると考えている。

西東京市における監査の実施及び実施体制については、明確にされていない。西東京市の場合はどうなっているか処分庁に釈明を求める。

いずれにしても、上記のような一般的概括的内容を提示しただけでは、とても改正住基法36条の2の安全確保義務を処分庁が果たしたとは言えず、処分庁の弁明には根拠がない。

8 弁明書5(9)について

住基ネット接続は、西東京市個人情報保護条例においては、法令の定めがある個人情報の外部提供に当たるから同条例に違反しないとの処分庁の主張について以下のとおり反論する。

西東京市個人情報保護条例(以下、条例という)は1条において、この条例が「個人情報の適正な取扱いについての必要な事項を定め、個人情報を保護するとともに、自己に関する個人情報の開示請求等の権利を保護することにより、市民の基本的人権を擁護することを目的とする。」ことを定めている。さらに同3条では実施機関(市)は、「個人情報の

保管等をするときは、市民の基本的人権を尊重するとともに、個人情報の保護を図るために必要な措置を講じなければならない」として市に対する義務を課している。

個人情報はいくまで当該本人のみに帰属するものであり、市は事業活動の実施に当たってその保管を任されているにすぎない。個人情報の保管に際して条例5条は、市に対し「個人情報の重要性を認識し、個人情報に係わる市民の基本的人権の侵害を防止するための措置を講ずるように努め」ることを義務づけている。

こうした条例規定にかかわらず、特段の措置を講ずることなく住基ネットに接続し、本人の同意なしに個人情報を外部に提供することは、条例の規定に反し、個人情報の自己コントロール権を否定する暴挙といわざるをえない。

住基ネットによる外部機関への情報提供によって、可能性としての個人情報の漏洩や不正利用の危険性が增大することは明らかである。現実に複数の自治体がこうした危惧を理由に、住基ネットへの接続を拒否、あるいは中止、さらには本人による選択を認めるなどの措置を講じている。このような環境で、危険性が十分予測されうるにもかかわらず住基ネットによる外部提供を行うことは、条例の理念、精神をふみにじる重大な違反行為であると考えられる。逆にこうした現状では、市が住基ネットに接続しない（あるいは本人の判断による接続拒否を認める）ことこそが、住基法36条の2に規定する「漏洩、滅失及び毀損の防止その他～に必要な措置」に該当し、合法であるということができる。

確かに市が主張するとおり、条例10条第2項は「法令の定めのあるとき」は個人情報を外部提供することができる定められている。しかし同条第4項の規定を、市は故意に無視しようとしているのではないか。10条第4項の条文は以下のとおりである。

「実施機関は、第2項の規定により外部提供するときには、個人情報の使用目的若しくは使用方法の制限その他の必要な条件を付し、又はその適正な取扱いについて必要な措置を講ずることを求めなければならない」

つまり条例は「法令の定めがあるとき」であっても無条件に外部提供を認めているわけではなく、10条第4項に定められた条件を満たすことを課している。10条第2項の規定に基づいて外部提供する場合でも、それは10条第4項にしたがった処理をしなければならないことが、条例によって明示的に定められているのである。

ところが市はすでに、審査請求人の一人による質問書への回答 2002年9月3日付「住民基本台帳ネットワークシステムについての質問書に対する回答」において、外部提供にあたり何ら条件を付していないことを明言している（資料4）。さらに市は審査請求人らによる情報公開請求に対しても、接続にあたって条件を付したり必要な措置を講ずることを求めたことを記した文書は存在しないことを回答した（資料5）。これは明らかに条例に定められた必要な義務を怠ったものといわなければならない。

条例全体を読むならば10条第2項の規定は10条第4項の制約下にあるものと当然み

なされるべきであり、市弁明書に見られるような、「条例10条第2項第2号に該当する外部提供」であるから条例に違反していないという主張はただちには成り立たないことがわかる。

東村山市監査委員会は、2002年10月4日付の監査請求結果通知で住基ネット接続は同市の個人情報保護条例違反であるとの見解を示した。同市の条例では、西東京当市と同様に「法令の特別の定めのある場合」は外部提供の制限の例外となることが定められているが、個人情報の保護、適正な維持管理といった条例で定められた実施機関（市）の責務を満たしていない場合、住基ネット接続は同市条例に違反するとの判断を示した。西東京市の条例においても、3条、5条、6条、10条第4項などによって同様の責務が市に課せられているのである。

西東京市議会や市広報等において、市は個人情報保護、住基ネットについて個人の権利・利益の保護には万全の対応を講じていると主張している。しかし住基ネットはその性質上、一自治体の努力のみによっては十全な安全性を保証しえないものであり、このことは市議会2002年度9月定例会における市総務部長や情報推進課長の答弁も認めているところである。

一方、市長は国に対して個人情報保護のための早期の法整備を要請する全国市長会の「緊急要望」に同意しており、市長は、国の責務において個人情報保護の課題が未解決であると認識していながら住基ネット接続を行ったと指摘せざるをえない。

以上のとおり、処分庁は住基ネット接続の問題点がある程度は認識していたが、その上で特段の措置を講ずることもなく住基ネットに参加を決定した。これは市が、市民の個人情報を保護し市民の基本的な人権を擁護するという条例によって市に課せられている責任を果たしていないということであり、条例10条第2項の規定のみをもってただちに住基ネットへの接続が条例に違反していないという市の主張には根拠がないことは明白である。

9 弁明書5(10)について

住基ネット接続と住民票コード付定は違憲であるとの審査請求人らの主張に対する、処分庁は改正住基法の合憲性について判断するところではないとの主張について、以下のとおり反論する。

住基ネットへの接続や住民票コード付番は、憲法に保障された平和的生存権（憲法前文）、基本的人権（同11条）、個人の尊重と幸福追求権（同13条）を侵害するとの審査請求人らの主張に対して、処分庁は「国会が制定した法律に基づいて事務を執行する処分庁としては」「住民基本台帳法の合憲性について判断するところではない」と弁明する。これは

処分庁が合憲違憲の判断を避けたまま、ただ「適法」であるとの見解を示したものである。

国会で制定された法律は一般的に合憲であるとの合理的な推測が成り立ち、行政機関が国の法規についていちいち合憲性を判断する義務はないという主張と解されるが、審査請求人らは法律一般について合憲性の判断を市に求めているわけではない。

住民基本台帳事務は市の自治事務であり、住基ネットへの接続は市の責任において執行されているのであるから、当然、市は自らの責任においてなんらかの政策判断を行った上でそれを行っているとはみなくてはならない。処分庁の弁明に従うなら、西東京市は自らの行為が合憲であるとの判断もなしに、思考停止の状態で総務省のいわれるがままに事務を執行していることになってしまう。これはおそるべき責任放棄である。

日本国憲法92条は、「地方公共団体の組織及び運営に関する事項は、地方自治の本旨に基づいて、法律でこれを定める」と規定している。ここでいう「地方自治の本旨」については、住民自治と団体自治の二つの要素があるとされ、住民自治とは、地方自治が住民の意思に基づいて行われるという民主主義的要素であり、団体自治とは、地方自治が国から独立した団体に委ねられ、団体自らの意思と責任の下でなされるという自由主義的・地方分権的要素であると説明されている（芦部信喜『憲法新版補訂版』岩波書店、1999年、329頁）。

そして、地方自治団体はそれぞれ法人格を持っており、独立した存在である。国や県には市町村に対して指導や調整を行う役割がある（地方自治法2条第6項）ものの、法的には市町村は国や県と対等・協力関係にあると定められている。

つまり地方自治体が自らの意思と責任によって自治体を運営し、住民の権利や安全を保護していくことは憲法上法律上、自治体が当然負うべき義務である。というよりもむしろ、そのためにこそ自治体は住民から行政を付託されているのである。よって処分庁の主張は無責任極まりない。

いうまでもなく行政機関の執行する行為はすべて法に基づいて行われなければならない、法の正当性の根拠は憲法を措いてほかにはない。自らの行政が憲法に合致した適正なものであるかを不断に検証することは、およそ法を執行する国・自治体等の行政機関に課せられた責務である。かつて沖縄県が米軍基地使用に関する特別措置法に関してその違憲性を国に提起したことがあった。東京都の場合も銀行に対する外形標準課税の適法性について、国とは異なる判断を示した結果、行政訴訟となるに及んでいる。

自治体は場合によっては、住民の利益を擁護する立場で国とは違う法の解釈をすることもありうるし、また国に対して法律の違憲性について訴える主体ともなりうるのであるから、国の制定した法律の合憲性について自主的な解釈権をあらかじめ放棄するような処分庁の主張は、自治体の責務を忘れた軽率なものだ。

処分庁が自らの責任において行った自治事務により、住民の憲法上の権利が侵害され重大な損失をこうむった場合には何らかの損害賠償請求が行われる可能性もある。むしろそうした場合に法的に責任をとる主体は、法律（この場合は住民基本台帳法）を制定し施行

した国ではなく、あくまでも執行者である市であることはいうまでもない。処分庁がその点を十分認識しているか、疑問とせざるを得ないのである。

住基ネット接続が違憲であるとしてその差し止めを求める民事訴訟は、すでに全国の10地裁で、164人の原告によって提訴されるにいたっている。私たち審査請求人らも、審査請求書に記したとおり、処分庁西東京市の住基ネットへの接続と住民票コードの付番が憲法に違反すると考えるものである。処分庁に対しては自らの行政を真摯に検証し、真に憲法に恥じない行為であるかをいま一度振りかえって熟考されることを望む。

10 まとめ

前記1から9までの反論で示したとおり、審査請求人らに住民票コード付番を行い、審査請求人らの本人確認情報を東京都に通知し、法的にもシステマ的にも個人情報の安全性が確保されない状態で住基ネットに接続した処分庁の行為は、住基法36条の2の規定を遵守せずに行なった違法な処分であり、西東京市個人情報保護条例及び憲法にも違反するものであるから、これら処分の取消しを求める審査請求人らの主張は正当であり、これらの棄却を求める処分庁の弁明は失当である。

以下、住基ネット事務は「自治事務」であることを確認し、処分庁の責務について確認しておく。

改正地方自治法により、憲法92条に定められた地方自治の本旨に基づいて、国と地方公共団体の関係が明確にされた。すなわち、地方公共団体の役割は、1条の2の第1項で「住民の福祉の増進を図ることを基本として、地域における行政を自主的かつ総合的に実施する役割を広く担うものとする。」とされ、国の役割は同条第2項で「前項の規定を達成するため、国においては国際社会における国家としての存立にかかわる事務（中略）その他国が本来果たすべき役割を重点的に担い、住民に身近な行政はできる限り地方公共団体にゆだねることを基本として、地方公共団体との間で適切に役割分担するとともに、地方公共団体に関する制度の策定及び実施に当たって、地方公共団体の自主性及び自立性が十分発揮されるようにしなければならない。」とされた。そして、地方公共団体が処理する事務を「自治事務」＝「法定受託事務」以外のもの（地方自治法2条第8項）とし、国が処理する事務を「法定受託事務」とすることが明確化した。

そして住基法は「法定受託事務」に入っておらず「自治事務」である。

その住基法は、1条で住民基本台帳制度が市町村における事務であることを定めており、3条第1項では市町村長に住民基本台帳の整備と適正管理義務があることを定めていることから、住民基本台帳事務は市町村長の責任と判断で運用する制度であること、そして住基ネットはこの住民基本台帳事務の一つであるからまさしく市町村長の責任と判断で運用する「自治事務」であることを確認しておく。

よって、処分庁は住基ネット事務に関しては、市として主体的に判断し適切に運用する責務が課せられていることを再確認しなければならない。

一方国は、「自治事務」に関しては地方公共団体に対して、「是正の要求」(地方自治法245条の5)ができるだけであり、「是正の指示」(同法245条の7)、「代執行」(同法245条の8)はできず、是正要求に従わないことを理由に不利益な取り扱いをしてはいけない(同法247条第3項)とされているから、住基ネット事務の運用について国は市町村の自主的な判断に対して命令できる立場にないことも付記しておく(「長野県本人確認情報保護審議会第1次報告」4『住基ネットの法的問題について』(清水審議委員)資料2、24頁参照)。

終わりに、日弁連が2002年12月20日に発表した「自治体が住基ネットから離脱することに関する日弁連意見」の要旨を以下に示し、処分庁の再考を促したい。

この意見書は、十分に実効性のある個人情報保護法制の整備がなされていない現状において、市町村が住基ネットから離脱することは合法であるとしたもので、処分庁の住基ネット接続は住基法36条の2の規定を遵守しておらず違法であるとの審査請求人らの主張と軌を一にする。

日弁連の「住基ネット離脱は合法」とする理由の要旨は

1. これまでの経緯

2002年8月5日に住基ネットが稼働したが、住基法上、住基ネット稼働の前提条件2つを満たしていない。

住基法附則1条2項の定める、政府が行なうべき個人情報の保護に万全を期するための「所要の措置」

住基法36条の2の定める、市町村長が行なうべき住民基本台帳事務処理に際しての、住民票に記載されている事項の漏洩、滅失及び毀損の防止その他「適切な管理のために必要な措置」

2. 政府がとるべき措置

「所要の措置」とは十分実効性のある個人情報保護法制の確立を意味する。

住基法の本人確認情報の保護規定や行政機関の現行の個人情報保護法の規定では不十分であり、個人情報保護法案も欠陥がある。個人情報保護法案は最低限以下の6項目の規定が必要だ。

センシティブ情報の収集制限

本来の業務処理に必要な範囲を超えた名寄せの制限

名寄せ結果の漏洩の禁止

複数の行政機関相互間のデータマッチングの制限

第三者機関による電子政府の監督及び監視

罰則による担保

3. 政府の対応

民間対象の個人情報保護法案も行政機関個人情報保護法案も未成立で、住基法上の附則に違反し義務を尽くしていない。このような状況下での住基ネット稼働は、住民の個人情報が侵害されるおそれが高く危険だ。

法案も先の条件を満たしていない。政府、自治体にセキュリティ対策基本法制定が必要だ。

4. 市町村の住基法上の義務

住基法3条第1項では市町村として住民の個人情報を適正管理する仕組みを制定する義務を定め、市町村としてできる範囲の処置を想定している。住基ネットの構築で更に36条の2が制定され、市町村長は住民票記載事項の適切な管理のために必要な措置を講じなければならないとされた。これを受けて総務省告示で、市町村長は個人情報の漏洩のおそれがある場合には住基ネットの全部又は一部を停止できることを前提として、停止の基準の策定を求めている。

そこで、住基法第3条が定める「住民に関する記録の管理が適正に行なわれるような必要な措置」及び同法36条の2の定める「適切な管理のために必要な措置」とは、市町村において住基ネットの稼働による個人情報の「漏洩、滅失及び毀損の防止」を最低限含む住基ネットの安全確保のための個人情報保護法制の確立及び情報セキュリティ確保のための具体的方策を意味し、到達目的としては、(一)住基ネットとの接続により、接続した当該市町村の住民データが住基ネットを経由して外部に漏洩、滅失及び毀損されないこと、及び(二)住基ネットと接続した当該市町村から全国民の個人情報が漏洩、滅失および毀損されないことが要請される。

市町村がこうした住基法上の義務を履行するには、専門職員の配置でセキュリティ確保を図ること、実効性ある個人情報保護条例の制定、危険発生時の切断等具体的処置の法的義務づけなどが含まれると考えられる。

5. 市町村の現状

地方公共団体の3分の1は個人情報保護条例がなく、これらは住基法3条、同36条の2に違反している。

6. 接続義務と適切管理義務との衝突

法が未整備な上に、条例未整備の市町村があるため、住基ネット接続により個人情報が漏洩したり民間利用される危険性があるとともに、個人情報保護条例がない市町村から全国民のデータが漏洩する危険性がある。

以上の理由により、各市町村にとっては、現状で住基ネットと接続することは、住民の個人情報の重大な侵害につながると判断することも充分理解でき、住基法36条の2に基づき、各市町村は住民の個人情報に関する「漏洩、滅失及び毀損の防止その他

…適切な管理のために必要な措置」を講ずる義務を負担しているのだから、住民のプライバシーの侵害を防ぐため、敢えて住基ネットと接続しない処置も、住基法36条の2に定める「適切な管理のために必要な処置」に該当すると解されるので、日弁連は市町村が住基ネットから離脱することは合法と考える。

上記にみたとおり、個人情報漏洩の危険性があるため、住基ネットに接続しない自治体の処置は個人情報安全確保のために必要な措置に該当し合法であるとの日弁連の意見を処分は深く受け止めた上で、審査請求人らの反論と求釈明に対して再弁明と回答を行なうことを求める。

以上