甲第84号証

２００７年5月１８日

東京高等裁判所第１０民事部　御中

鑑　定　意　見　書

杉並区と東京都･国との間における住民基本台帳ネットワークに関する訴訟につき、控訴人代理人からの質問に答える形で、以下のとおり意見を述べます。

早稲田大学法務研究科教授
中　　島　　徹

目　次

個人情報保護の評価基準としてのＯＥＣＤ８原則については、名古屋高裁判決及び本件原審判決が判示し、堀部政男意見書（乙１０）も提出されています。それらの問題点につき、ご指摘下さい。併せて、ＥＵ指令の位置づけ・内容についても、お聞かせ下さい。

住基法・行政機関個人情報保護法の規定の評価・解釈をめぐって、３高裁判決の間で違いがあり、それがデータマッチング・名寄せの具体的危険性を認めるか否かの差になって表れているように思われますが、３高裁判決の上記規定の評価・解釈の当否についてのご見解をお聞かせ下さい。

データマッチング・名寄せの具体的危険性を認めるか否かの差は、第三者監視機関の有無・必要性（名古屋高裁金沢支部判決・大阪高裁判決）、監視措置・是正制度の有無（名古屋高裁判決）についての理解の違いからも来ているようですが、このあたりについてはどのように考えるべきでしょうか。

本件訴訟では、控訴人杉並区が、被控訴人都に対し、住基ネットを通じて杉並区民の本人確認情報を送信するにあたって、通知を希望しない住民の本人確認情報については送信せず、通知希望者の本人確認情報のみを送信すること、それを被控訴人都が受信しないことが適法か否かが問われています。この点について、これまでに述べられたことを踏まえてのご見解をお聞かせ下さい。

これから名古屋高裁平成１９年２月１日判決（以下「名古屋高裁判決」又は「①判決」といいます。甲８３）、名古屋高裁金沢支部平成１８年１２月１１日判決（以下「名古屋高裁金沢支部判決」又は「②判決」といいます。甲７４）及び大阪高裁平成１８年１１月３０日判決（以下「大阪高裁判決」又は「③判決」といいます。甲７２）（以下、これら３つの判決を「３高裁判決」といいます）についてのご見解を中心にお尋ねします。

１　まず最初に、これら３高裁判決を評価する視点を明らかにする意味で、「プライバシー権」、「自己情報コントロール権」、「個人情報保護」は、それぞれ、相互にどのような関係にあって、どのような内容を含意しているのかにつき、住基ネットに即しながら、ご見解をお聞かせ下さい。

まず、「プライバシー権」と「自己情報コントロール権」の関係について述べ、次に、それらと「個人情報保護」との関係について論じることとします。

（１）「プライバシー権」と「自己情報コントロール権」の関係について

周知のように、Privacy は当初「一人で放っておいてもらう権利」と定義されました（Olmstead v. United States, ２７７ U.S.４３８（１９２８）におけるブランダイス裁判官の反対意見）。これに対しては、今日のような情報伝達技術が発達した社会では、「一人で放っておいてもらう」だけでは十分とはいえないとの批判があります。しかし、この定義の中には、日本でプライバシーという語を理解する際に鍵となる考え方が直接・間接に含まれていました。

Olmstead 事件で問題となったのは、屋外にある電話線に盗聴器を設置することが、アメリカ合衆国憲法修正４条の禁じる「不当な捜索・押収」に該当するかどうかでした。法廷意見は、盗聴器は屋外に設置されているから、物理的な意味での「捜索・押収」には該当しないと述べて、合憲と判断しまし

た。これに対しブランダイス裁判官は、たとえ家屋の外にある設備であっても、実質的に「私的領域」を侵犯する以上、プライバシー権の侵害となると論じたのです。

これは家を個人の聖域と観念し、その中で行われる生活、例えば誰と生活を共にし、子供を作るかどうかといった個人生活の形成からそれに関わる情報に至るまで、政府による干渉を禁じるという考え方です。このような意味で、ブランダイス裁判官の「一人で放っておいてもらう権利」という定義には、情報の秘匿と自己決定という二つの側面がもともと内在していました。これがのちに、私生活上の秘密を暴露されないといった面に重点を置くいわゆる「情報プライバシー権」と、自分の人生を自分で決める「自己決定権」、そしてその二つの面を併せ持った「情報の自己決定」という意味での「自己情報コントロール権」という観念を生み出すもととなったのです。

もっとも、このように述べたからといって、「一人で放っておいてもらう権利」という定義を今日でも維持すべきであると主張しているわけではありません。肝心なことは、The Right to Privacy という語の理解に、情報の秘匿権と自己決定権という両面が本来的に具わっていたという点です。日本では、しばしばプライバシー権の定義について「一人で放っておいてもらう権利から自己情報コントロール権へ」と変化したと説明されます。これはしかし、プライバシー権の理解が質的に変化したということを意味しているのではありません。すでに見てきたように、もともと「一人で放っておいてもらう」ということに含まれていた自己決定の側面が、自分に関する情報についても意識されるようになったということにすぎないのです（ただし、日本では自己決定権と情報プライバシー権を分けて考える傾向があります。それはしかし、たまたまプライバシーを情報とだけ関連づけて理解してきたという日本社会に固有の事情によるもので、本質的な問題ではありません）。

（2）「プライバシー権」及び「自己情報コントロール権」と「個人情報保護」

の関係について

では、以上の点と個人情報保護はいかなる関係にあるでしょうか。住基ネットにおける個人情報は、氏名、生年月日、性別、住所の本人確認情報と住民票コードおよび変更情報ですが、いずれも個人識別情報に該当することについては争いがありません。これらは、いわゆる索引情報として、プライバシー保護が要請される度合いは低いという指摘もあります。しかし、それ自体は「索引」であっても、それがネットワーク上でさまざまな情報と結合されれば、センシティブ情報への入り口となりうるわけですから、基本４情報の性格だけを独立に論じることは、必ずしも適切ではありません。最高裁も、学生の氏名や学籍番号等の索引情報について「プライバシーに係る情報として法的保護の対象となる」ことを認めています（最判２００３（平１５）年９月１２日民集５７巻８号９７３頁）。これは、氏名や学籍番号などが講演会参加者を特定する情報であることを考慮に入れた実質的な判断です。逆にいえば、本人確認情報の性質だけを切り離して要保護性を論じることは、以下に述べるように、極めて形式的な思考といわなければなりません。

氏名や住所等に多少でも要保護性を認めるのであれば（被控訴人もその点は認めています）、問題の焦点は、本人確認情報の「法的保護」の「程度」（質問事項２および３で再度言及します）と「方法」（同じく質問事項７で再度検討します）です。一見すると、住基ネットにおけるプライバシー問題と直接に関係がなさそうにみえるOlmstead判決に言及したのは、その点にかかわります。法廷意見は、盗聴器が家の外にあるという極めて形式的な理由で、プライバシー権の侵害を否定しました。しかし今日では、プライバシー権侵害を肯定するブランダイス反対意見の正当性を疑う法律家はいないでしょう。けれども、ブランダイス裁判官の反対意見がKatz v. United States, ３８９ U.S.３４７（１９６７）で法廷意見となるまでには、約４０年の歳月を必要としました。Olmstead で法廷意見に与した裁判官たちが、ブランダイス裁判官のように実

質的な思考をしていれば、このような無駄は省けたに違いありません。

Olmstead 判決にみられるような形式論は、姿形こそ異なるものの、住基ネットの正当化に際してもしばしば登場します。一例をあげれば、個人情報の目的外利用には原則として本人の同意が必要とされるべきであるにもかかわらず、政府や一部の判決が、法律で定めれば本人同意は不要と論じていることなどがそれです。

たしかに、法律の制定により形式的には国民の同意があったといえそうです。しかしそれでは、ブランダイス裁判官が論じたような対政府との関係におけるプライバシー権は保障されていないも同然です。釈迦に説法でしょうが、憲法は、多数決（に基づく法律）によっても奪われない権利を保障しているからです。質問事項２以下では、住基ネットを正当化する際に用いられる数々の形式論が、いかに憲法上のプライバシー権保障を実質的に損ねているかについて、具体的に検討してみたいと思います。

２　３高裁判決は、内容に違いはあるものの、それぞれ、憲法１３条からプライバシー権あるいは自己情報コントロール権の保障を導いていますが、各判決の当該部分の判示について、どのように評価すべきでしょうか。

プライバシー権あるいは自己情報コントロール権に対する３高裁判決の態度は、いずれも憲法１３条に基づく人格権の一内容と理解している点で、一見すると大差がないようにみえます。しかし、以下にみるとおり、実際にはニュアンスの差以上の違いがあります。

（１）名古屋高裁２００７（平１９）年２月１日判決（①判決）は、プライバシーを「個人の私生活上の情報」と同定し、「憲法１３条によって保障される人格権の一内容として、法的保護を受けることができる利益」であると解して、

「国家機関が、正当な理由もないのに、個人の同意を得ず、みだりに個人の私生活上の情報を収集、開示することは、同条に反して許されない」（２８頁）と述べています。他方、「自己情報をコントロールする権利がプライバシー権として認められるか否かは別としても」と述べて、事実上、自己情報コントロール権としての側面をプライバシー権の理解から除外しました。

この判決の特徴は、プライバシー権の保障を、もっぱら国家機関の権力行使の限界という観点から論じている点にあります。もちろん、そのこと自体は人権保障にとって不可欠な視点ではあります。しかし、自己情報コントロール権の保障に消極的であることに示されるように、情報の取扱いについて個人の主体性を認めず、国家機関が「個人の私生活上の情報を収集・開示」できる限界を論じているにとどまっています。「収集・開示」自体は、自明の前提とされているのです。そのために、せっかく総論としてプライバシー権の保障を強調しておきながら、実際には権利の限界を帰結しやすい議論となっています。

そのことをはっきりと示しているのが、「正当な理由もないのに、個人の同意を得ず、みだりに」という一文です。これは、逆にいうと、正当な理由があれば、個人の同意を得なくても「情報を収集・開示」できる（「みだりに」には該当しない）ことを意味します。この場合、何をもって「正当な理由」と考えるかが重要なポイントとなります。というのも、その理解いかんによっては、前記 Olmstead 判決における盗聴器の設置も、犯罪捜査という「正当な理由」があるので、個人の同意なしに情報を収集・開示できるということになりかねないからです。なお、この点は質問事項３と密接に関わるので、そこで改めて検討することにしたいと思います。

（２）名古屋高裁金沢支部判決２００６（平１８）年１２月１１日判決（②判決）も、プライバシー権に関して①判決と同様の視点を採用しています。②判決は、プライバシー権を「個人の私生活上の自由及び平穏に関する利益で、個

人の人格的自律ないし人格的生存に必要不可欠な利益（個別規定で保障されている基本権と同等の憲法的価値を有する人格的利益）」と敷衍します。ここでのプライバシー権は「人格的生存に必要不可欠な利益」とされていますから、制限が容易には認められない権利と解されるのでなければ、権利論として一貫しません。

ところが、実際には「国家機関等の公権力といえども、正当な理由がなく、社会生活上当然に受忍すべき限度を超えて……個人の私生活上の情報を収集し、管理し、利用（他者への開示を含む）することは、憲法１３条が保障するプライバシー権を侵害するものとして許されない」（以上、３３頁）と述べることで、権力行使の限界は緩和されています。というのも、ここでいわれる「正当な理由」には①判決と同様の問題があることに加え、受忍限度論を導入することで、プライバシー権の保障がさらに相対化されているからです。

（３）以上の２判決に対し、大阪高裁２００６（平１８）年１１月３０日判決（③判決）は、対照的なプライバシー権理解を示しています。同判決も、プライバシーの権利を「他人からみだりに自己の私的な事柄についての情報を取得されたり……第三者に公表されたり利用されたりしない私生活上の自由」と定義する点で、一般論としては前記２判決と大差ありません。

③判決が、①・②判決と決定的に異なるのは、以下の点においてです。すなわち、情報通信技術が急速に進歩した情報化社会においては、「プライバシーの権利の保障……を実効的なものにするためには、自己のプライバシーに属する情報の取扱い方を自分自身で決定するということが極めて重要になってきており、その必要性は社会において広く認識されてきている」と述べて、「自己のプライバシー情報の取扱いについて自己決定する利益（自己情報コントロール権）は、憲法上保障されているプライバシーの権利の重要な一内容となっている」（４７～４８頁）との認識を示しているのです。このよ

うな「自己情報コントロール権」への積極的な言及は、①・②判決には見られません。

もちろん③判決も、自己情報コントロール権の無限定な保障を説いているわけではありません。むしろ、住基ネットにおける本人確認情報の収集、保有、利用等については、「①それを行う正当な行政目的があり、それらが当該行政目的実現のために必要であり、かつ、②その実現手段として合理的なものである場合には、本人確認情報の性質に基づく自己情報コントロール権の内在的制約により（もしくは、公共の福祉による制約により）、原則として自己情報コントロール権を侵害するものではない」（５０頁）と述べています。

しかし、ご存知のように①・②判決と③判決とでは、プライバシー権侵害の有無をめぐる最終的な結論が全く異なりました。その分岐点は、質問事項１への回答で言及したブランダイス裁判官の定義のもつ意味や、「私生活上の自由」の観念に本来的に含まれていた自己決定の要素に着目するかどうかにあります。①・②判決も、「私生活上の自由」を起点にプライバシー権の保障を語ってはいるのですが、「一人で放っておいて」もらえない場合があることを指摘するだけで、今日の社会状況の下で「一人で放っておいて」もらうために、個人がいかなる権利を保障されるべきかという視点が欠けているのです。

その結果、プライバシー権が法的保護の対象であることは認めつつも、その制限が比較的容易に認められることとなりました。プライバシー権が憲法１３条で保障される憲法上の権利であると解しても、その内実の理解いかんで、このように法的保護の「程度」は大幅に異なってしまうのです。私は、権利制限を容易に認める①・②判決の論理が、「人格的生存に不可欠」というプライバシー権への評価と一貫していないのではないかと考えますが、この点はさらに質問事項３、６および７で敷衍します。

3　３高裁判決は、それぞれ、プライバシー権あるいは自己情報コントロール権との関係で、本人確認情報が法的保護の対象となることは認めていますが、法的保護の程度については、各判決の間で大きな差が見られます。なぜこのような差が生じたのでしょうか。お考えをお聞かせ下さい。

結論から申しますと、ア）本人確認情報の性格をどのように理解するか、イ）プライバシー権問題を論じる際に住基ネットという特殊なシステムの性格と、そこで本人確認情報を利用することの意味をどこまで考慮に入れるかという２点への対応の違いによって、法的保護の程度が異なる内容の判断となったと私は考えています。ちなみに、ア）とイ）は密接に関連していますが、以下では、便宜上、判決ごとにア）とイ）を分けて考察します。

（１）①判決における本人確認情報の位置づけと問題点

ア）本人確認情報の法的性格について

①判決は、いわゆる基本４情報について、「社会生活上一定の範囲では必然的に開示され、利用されている情報」で「個人の思想、信条等に関する情報と比較すると、平均的な一般人がその開示に苦痛を感じる程度は相対的に低い」、住民票コードは「個人を識別するために技術的に用いられる１１桁の便宜的な数字」で「個人の人格的自律に直接かかわるものではない」、変更情報は「身分上の変動事由は記載されないから、他人に知られたくない個人情報が開示されるとはいえない」し、仮に「身分上の変動事由が推測可能であるとしても、……純粋に私生活上の情報とは言い難」く、「秘匿する必要性が高いということはできない」との認識を示しています。

もっとも、「予定された開示対象及び利用範囲を逸脱してみだりに開示されないという限度では個人の期待は法的保護に値する」（以上、２９頁）と述べ

ていますが、質問事項２への回答で述べたように、これは、「逸脱してみだりに」でなければ、つまり「正当な理由があれば」法的保護の対象ではなくなる（制限される）ということですから、「いずれも秘匿する必要性が高いということはできない」という前段の認識を反映して、保護の程度は極めて低いものとなっています。①判決の場合、前述のように（質問事項２への回答参照）個人の人格的自律に係るプライバシー権ですら「正当な理由」があればそれだけで制限されるわけですから、ましていわんや、本人確認情報のような要保護性の低い情報について、保護の程度が低いものとなることは当然の帰結でしょう。

しかし私は、①判決のこのような理解を、質問事項１への回答で言及したOlmstead 判決法廷意見の形式論に類似する不適切なものであると考えています。たしかに、氏名等々の本人確認情報は、抽象的にそれだけを取り出して考えれば、社会生活を営む上で一切開示しないですむ情報ではありません。けれども、私たちは通常の日常生活においてすら、誰に氏名等を告げるかについてそれなりの考慮を払います。この点、住基ネットは、公的システムであるからそうした考慮の余地はないという反論があるかもしれません。しかし、住基ネットは、後述するように（本鑑定意見書２８頁）、法令の改正によって本人確認情報の利用目的の拡大や変更が随時可能です。普通の市民にとって、そもそも法令改正の有無を知ること自体が必ずしも容易なことではありません。ましていわんや、本人確認情報の利用目的が拡大ないし変更されたことを知ることとなると、制度に精通した専門家でなければ絶望的でしょう。その意味で、住基ネットは、自分の情報が誰に開示され利用されているかを把握することが現実には非常に難しいシステムなのです。そしてその点が、市民の不信感を醸成する一因となっているのです。これに対して、単に「正当な目的」があるとか、不信感には根拠がない、氏名の秘匿度は高くない等々と説くだけでは、法的議論として説得力に欠けるといわなければな

りません。

この場合、住基ネットが技術的に安全なものでなければならないことは当然の前提です。しかし１００パーセント安全な技術は存在しないのですから、その上に二重三重に安全を確保する法的仕組みが、住基ネットを支える制度に具わっていなければなりません（この点は、質問事項６および７でさらに検討します）。プライバシー情報は、いったん漏洩すれば元の状態に戻すことができない（不可逆性）のですから、市民が開示や利用に慎重になることには相応の理由があるのです。ちなみに、この点は、次のイ）と関わります。

イ）住基ネットにおいて本人確認情報を利用することがもつ意味

住基ネットをめぐるプライバシー問題を検討する際に忘れてはならないことは、それが情報の大量かつ迅速な処理が可能なコンピュータ・ネットワークであるという点です。この点について、①判決は、「４情報については、行政目的に使用される場合には、旧住基法当時から、国や他の自治体に対して開示されていたものというべきであり、住基ネットの運用開始に……よって、４情報の開示対象又は利用範囲に質的な変化があったということまではできない」（３０頁）と述べています。

ここにも、住基ネットという制度をひとつひとつの要素に分解して、それぞれを形式的に理解する①判決の特徴をみることができます。なるほど、本人確認情報のうち、いわゆる基本４情報は、住基ネット運用以前の旧住基法でも「国や他の自治体に対して開示されていた」ものですが、その処理は国や各自治体の保有する個別のコンピュータ内で（電子化以前には紙媒体で）独自になされるだけで、全国的なネットワークにおいて行われているわけではありませんでした。旧住基法における本人確認情報の処理と住基ネットでのそれは、全国規模で統一的に処理されるかどうかという点で、質的に全く異なるものなのです。そのことは、インターネット成立以前に家庭で使用さ

れていたいわば孤立したコンピュータと、インターネットに接続された現在のコンピュータとでは、同じコンピュータでも果たすことができる機能が全然違うことを想起すれば、おわかりいただけるでしょう。

また、本人確認情報も、それ自体としては単なる個人識別情報にすぎないとしても、コンピュータ･ネットワークを介してセンシティブ情報への入り口となりうる情報です。その点で、本人確認情報を本人確認情報としてだけ把握することは、適切ではありません。インターネット成立以前と成立後の本人確認情報では、それが果たすことのできる役割も大いに異なっているのです。それにもかかわらず、旧住基法でも基本４情報は利用されていたとか、一般社会で氏名を開示しないで生活することはできないと論じることは、盗聴器が屋外に設置されているから「不当な捜索・押収」に該当しないという形式論を採用したOlmstead判決と同様の思考といわなければなりません。

（２）②判決における本人確認情報の位置づけと問題点

ア）本人確認情報の法的性格について

②判決も、本人確認情報（基本４情報とその変更情報）を「それ自体では個人の人格、思想、信条、良心等の内心に関する情報とはいえないし、表現、集会等の私生活上の行動に関する情報ともいえない」と捉えました。また、住民票コードとその変更情報も「特定の個人についての迅速な検索処理を可能とし、かつ、確実な本人確認を可能とする目的で、無作為に作成された１０桁の数字及び１桁の検査数字からなる１１桁の数字にすぎない」ので、いずれも「個人の人格的自律ないし人格的生存の維持や発展」（以上、３４～３５頁）に関する情報ではないと解する点で、①判決と共通の認識に立脚しています。

もっとも、本人確認情報とその変更情報は、「その一体的な取扱いにより、特定の個人を極めて容易に検索することができる」し、住民票コードとその

変更情報は、「その高度な個人識別性の故に、他の本人確認情報以上に、その取扱い次第では同様の危険があ」るので、「国家機関等の公権力が住基ネットにおいて本人確認情報を取り扱うことは、憲法１３条が国民に対して保障している、個人の人格的自律ないし人格的生存に必要不可欠な利益としての私生活上の自由及び平穏と密接な関連をも」ち、「その管理又は利用に関する法制度とこれに関連する同法制度の運用の実情のいかんによっては、憲法１３条により保障されているプライバシーに関する権利を害し、あるいは、これを害する具体的なおそれがあるため、憲法１３条に違反する状態にあるものと評価されるに至ることもあり得ないではない」（以上、３５～３６頁）と述べてもいます。この点で、本人確認情報をもっぱら要保護性の低い情報と解する①判決と比べると、若干ニュアンスを異にする判断であるといえなくもありません。

それにもかかわらず、結果的に、②判決も「本人確認情報は、そのものとして」「個人の私生活上の自由及び平穏に関する利益（憲法の個別規定で保障されている基本権と同等の憲法的価値を有する人格的利益）に直接に関わるものではない」から、「その行政事務の処理の必要等の正当な理由がある限り、相当な方法で、これを収集し、管理し、利用することは、その本人確認情報に係る住民の同意がなくとも、憲法１３条に違反するものではなく、これにより、当該本人確認情報に係る個人の私生活上の自由及び平穏が一定の範囲で制限されることがあったとしても、憲法１３条にいう『公共の福祉』による制限として、許される」（以上、３７～３８頁）と述べて、①判決と異ならない判断を示しました。

このように、②判決はせっかく本人確認情報と他の情報の「一体的利用」という問題に言及しながら、最終的には本人確認情報の性格だけを論じることで結論を導いています。そのような立場をとる限り、本人確認情報がもつ一般的性格に注目するだけですから、①判決と同様の結論にたどり着くこと

は当然でしょう。しかし、そのような議論の進め方には、①判決における旧住基法との対比論（本鑑定意見書１３頁）と同様に、住基ネットというコンピュータ･ネットワークにおいて本人確認情報を収集し利用することの意味を無視しているという問題点があります。以下では、②判決におけるこの面からの問題について、やや詳しく述べます。

イ）住基ネットにおいて本人確認情報を利用することがもつ意味

①判決は、本人確認情報が旧住基法時代から用いられ、住基ネット運用後も、本人確認情報の利用について質的変化はないという認識を前提にしていましたから、その認識の当否を別にすれば､論理的には一貫していました。これに対し、②判決は本人確認情報の利用について、「違憲状態が生じた場合において、その原因が･･････住基ネット規定によるものであるときには、同規定は憲法１３条により無効となり、本人確認情報に係る住民は･･････差止め等の救済･･････を求めることができる」（３７頁）と論じていますから、旧住基法と住基ネットの下での本人確認情報の利用は質的に異なっているとの認識を有していると解する余地があります。その点で、①と②の両判決には違いがあるといえなくもないわけです。

ただし、②判決では、救済を求めることができる場合に、違憲状態が「住基ネット規定によるものであるとき」という条件が付されています。判決によれば、これは「住基ネットに使用されるシステムの安全に関する規定や住基ネットの管理運営に関してプライバシーの保護を担保する規定を欠くなどのために、使用されているシステムについて安全上無視し得ない欠陥があって、容易に外部からの侵入を許すものであったり、住基ネットの管理及び運営が著しく杜撰になされ、住基ネットの管理運営に従事する者が不正に本人確認情報にアクセスするなどして、本人確認情報が簡単に漏えいし、あるいは流出する具体的な危険があるという場合」（３４頁）を意味するものとされ

ています。このように解すると、本人確認情報の利用が、それを望まない者との関係で違憲とされる場合は、国が顕著な欠陥のあるシステムを作った場合や、現場での不正行為を前提とした管理運営がおこなわれているという、いわば異常事態に限定されることになります。

もちろん、そうした事態が許されないことはいうまでもありません。しかしながら、コンピュータ・ネットワークの特質のひとつは、コンピュータに蓄積された大量の情報をネットワーク経由で迅速に処理することができる点にあります。これは、裏を返せば情報漏えいやデータマッチングが瞬時に起きることを意味しています。つい先ほどまで、プライバシー権を侵害することなく稼動していたシステムが、次の瞬間にはプライバシー権を侵害する可能性があるわけです。その意味で、コンピュータ・ネットワーク・システムというものは、常に具体的危険を惹起する可能性を秘めているということができます。そういう特質を有するシステムであるにもかかわらず、②判決の指摘するような例外的場合にのみ「救済を求めることができる」というのでは、救済の実効性に乏しいといわなければなりません。

住基ネットは、それ自体としては本人確認情報等を保有するだけのシステムですが、同時にそれは、本人確認情報により各行政機関が保有するコンピュータと接続できるネットワーク・システムでもあります。そして、各行政機関が保有するコンピュータには、民間の保有する個人情報とは比較にならない質と量の情報が蓄積されています。このような全体としてのネットワーク・システムにおいて、外部からの侵入、あるいは、行政機関内部やその委任先における誤用・濫用による具体的危険が発生した場合、それによるプライバシー権侵害は極めて深刻です。そのことを端的に示したのが、質問事項６で言及する本年（２００７（平１９）年）５月に判明した愛媛県愛南町における住基情報の大量流出です。もちろん、危険が現実化していない通常の稼動状況においては、危険は抽象的危険にとどまっているといえるでしょう。しか

し、住基ネットという仕組みにおいては、すぐ上で述べたように、各行政機関の保有する個人情報を結合するコンピュータ・ネットワークというシステムの特質と、情報処理の速さゆえに、抽象的危険は瞬時に具体的危険に転化します。その意味で、住基ネットにおいては、具体的危険と抽象的危険は常に連続する関係にあるのです。

この点に関し、それはコンピュータ・ネットワークに付随する危険性であり、住基ネットに固有なものではないという反論（①判決は、内部者による情報漏えいについて「コンピュータ社会の有する一般的な危険の範疇に属する」と述べています）があります。しかしそれは、有効な反論とはいえません。第一に、それは前述のように、住基ネットが各行政機関の保有する情報に接続することのできるネットワーク・システムであるという点を看過しています。第二に、民間のコンピュータ・ネットワーク・システムの場合、それを利用するかどうかは、個人の選択に委ねられています。現代社会では、コンピュータ・ネットワークで情報が管理されるクレジット・カードを所持しないことは、現実問題として、日常生活にさまざまな不便をもたらすでしょう。しかし、コンピュータ・ネットワークの信頼性に疑問をもち、クレジット会社と契約をしないという選択の余地は、依然として私たちに残されています。しかし、住基ネットでは、現行制度上そのような参加および離脱の自由が認められていないのです。

盗聴装置と住基ネットを同視するつもりはありませんが、「正当な目的」があって、みだりに開示されない限り情報の収集・利用は許されるというのであれば、Olmstead 判決は今日でも有効であり、盗聴装置の設置は一般的に合法であるはずです。しかし今日では、アメリカ合衆国でも日本でも、盗聴は一定の条件の下で例外的に認められるにすぎません（その是非については、ここでは論じません）。そうでなければ、プライバシー権を侵害する違憲な国家行為となるからです。

いうまでもないことですが、盗聴装置は、機能上、個人識別情報しか収集しえないものではありません。それにもかかわらず法制度上、個人識別情報を収集するだけと規定されていれば設置は一般的に認められるなどという議論をすれば、およそ説得力に欠ける法的議論と評価されるでしょう。

住基ネットにおいても、住民票コードにより各行政機関が保有している情報を結合することで、本人確認情報は「個人の人格的自律ないし人格的生存の維持や発展に関わるような情報」（②判決３５頁）と一体化する場合があるのです。私は、②判決がこのような認識を有していたにもかかわらず、本人確認情報「それ自体」の性格を強調することで、コンピュータ・ネットワーク一般が有する上記の危険性と、個人識別情報の取扱いについて個人選択を認めない住基ネット・システムに固有の問題点のいずれをも無視してしまったと考えています。

（３）③判決における本人確認情報の位置づけと問題点

ア）本人確認情報の法的性格について

③判決も、本人確認情報について、「人が他者との関わりを持つ社会生活の基礎となる個人識別情報であって、個人の私的情報ではあるが、同時に公共領域に属する個人情報であるといえるものであり、もともと秘匿性の高いものとはいえない」と述べる点で、①・②判決と共通の認識に立脚しています。前二者と異なるのは、「今日の社会においては、一般的に秘匿性の低い個人情報であっても、人によってはある私的生活場面では秘密にしておきたいと思う（秘匿性の高い）事柄があり、そのような個人情報の取扱い方についての本人の自己決定を承認する社会的意識が形成されていると認めて差し支えない」という認識でしょう。同様に、住民票コードについても、「それ自体数字の羅列にすぎない技術的な個人識別情報であるが、住民票コードが記載されたデータベースが作られた場合には、検索、名寄せのマスタ

ーキーとして利用できるものであるから、その秘匿の必要性は高度である」という認識を示しています。

その上で、個人識別情報は「その取扱い方によっては、情報主体たる個人の合理的期待に反してその私生活上の自由を脅かす危険が生ずることがあるから、本人確認情報は、いずれもプライバシーに係る情報として、法的保護の対象となり（最高裁判所平成１５年９月１２日第二小法廷判決・民集５７巻８号９７３頁参照）、自己情報コントロール権の対象となるというべきである」（４９～５０頁）と述べて、本人確認情報の保護に必ずしも積極的ではなかった①・②判決と異なり、③判決はそれを自己情報コントロール権の対象であると位置づけたのです。

もっとも、ここで肝心なことは、そうした一般論にではなく、権利の保障をどのように実質的に図るか（質問事項６および７で検討する法的保護の「程度」）という点にあることを、私は繰り返し指摘してきました。というのも、③判決もまた、「本人確認情報は、公権力との関係でみれば、他の地方公共団体や行政機関において行政目的実現のために必要な範囲で個人識別情報として収集、保有、利用等する必要のある場合がある」ことから、前記の①正当な行政目的と必要性及び②実現手段としての合理性といった例外条件（本鑑定意見書１０頁の③判決引用部分参照）を定めている点で、①・②判決と認識を共通にしているからです。

確かに、一見したところ上記②の要件は、①・②判決には欠けているようにも思えますが、「本人確認情報の漏えいや目的外利用などによる、住民のプライバシーないし私生活上の平穏が侵害される具体的危険がある場合には、上記②の実現手段として合理性がないものと」なると述べているので、実質的には②判決の具体的危険の有無を問う考え方と同じであるといえます。このようにみてきますと、①・②・③判決の間には、一般論レベルでは、個人識別（本人確認）情報の要保護性についての社会的承認を前提にした自己情

報コントロール権への言及の有無を除くと、大きな違いはないともいえます。

その上で、「住基ネットの行政目的の正当性及び必要性は、これを肯認することができる」（５９頁）とし、技術面および人的側面においても、セキュリティが不備で本人確認情報が漏えいする「具体的危険性が存在するとまで認めることはできない」と判断している点も、①・②判決と同様です。しかしながら、前述のように、①・②判決と③判決では住基ネットの憲法適合性について全く異なる判断が下されました。その理由について、私は次のイ）で述べるように考えています。

イ）住基ネットにおいて本人確認情報を利用することがもつ意味

③判決の基本的特徴は、住基ネットが既存のコンピュータ・ネットワークとは質的に異なるシステムであることを踏まえ、そこにおけるプライバシー保護について、単に法制度が整えられているかどうかを形式面で判断するだけでなく、予測される運用も視野に入れて具体的に検討した点にあります。すでに指摘したように、住基ネットは公的システムですから、住民票コードを入力することで本人確認情報と結合される各行政機関の保有する個人情報の質及び量は、民間のネットワークとは比べ物にならないものです。住基ネットを、各行政機関のコンピュータに蓄積された情報を結合することが可能なネットワーク・システムと把握せず、本人確認情報等のみを保有するシステムとだけみることは、正鵠を得ているとはいえません。

③判決は、そのことを「行政機関が保有している膨大な個人情報をデータマッチングし,住民票コードをいわばマスターキーのように使って名寄せすることにより、個人情報を共同利用することを可能とするインフラが、住基ネットにより整備された」（７４頁）と表現しています。

こうした理解とは異なり、住基ネットを形式的にみれば、そこで直接に用いられている情報は、氏名等の基本４情報と住民票コードならびにそれらの

変更情報だけですから、住基ネットは③判決の指摘するようなインフラではありえないということになります。実際、質問事項６でやや詳しく検討するように、①判決は「行政機関が保有する個人情報を一元的に管理する主体は存在しない」「指定情報処理機関が住民に関するデータベースを作成、保有することはないし、国の機関からデータベースの提供を受けることもないから、指定情報処理機関が……データマッチングをする可能性はない」と断言しています。

なるほど、法的にはこのようなデータマッチングは禁じられています。しかし、技術的には十分に可能ですから、「データマッチングをする可能性はない」とはいえません。繰り返しの比喩になりますが、Olmstead において問題となった盗聴装置は、物理的には屋外にありましたが、技術的には屋内の会話を聞くことを可能にする装置です。それゆえ、実質的には「不当な捜索･押収」に該当すると考えるべきものなのです。もちろん、設置はしたけれど実際に盗聴が行われるまでは具体的危険がないという理由で、プライバシー侵害を否定する余地もありません。ブランダイス裁判官が指摘していたように、設置しただけで「違法な捜索･押収」に該当すると考えなければ、盗聴が実行できるからです（違法収集証拠の排除法則では、プライバシー侵害は回復できません）。

こうした制度や技術の一体性を念頭に置いた実質的思考（③判決）と、法制度や技術を個別に捉え、その枠内で完結させて論じる形式的思考（①・②判決）の違いが、①・②判決と③判決の間における結論の違いを導いたのです。ちなみに、住基法上の本人確認情報の保護措置や技術的安全性についての各判決の理解とその評価については、質問事項６および７で具体的に述べさせていただきます。

４　本件原審判決の自己情報コントロール権・プライバシー権論あるいは本人確認

情報の位置づけについては、３高裁判決との対比で、どのように評価されますか。

本件原審判決は、自己情報コントロール権について「内容が不明確であり、それ自体憲法１３条によって保障されるか疑問があるというべきである。原告が主張するような個人情報の憲法上の保護としては、……プライバシー権の問題として検討されるべきである」と判示しています。ここでは、自己情報コントロール権とプライバシー権は異質な権利として把握されているようです。

より具体的に申しますと、本件原審判決は自己情報コントロール権の権利性を事実上否定し、市民が情報の主体であることを認めていません。他方、本人確認情報に関しては、「個人的な情報をみだりに収集、開示されないという利益については、その限度で、法的保護が認められるべきである」と述べて、「プライバシー権の問題」として論じています。しかし、「氏名、生年月日、性別及び住所については、従前から、原則として、何人も、閲覧や交付を求めることが可能であった……こともあり、これらの情報については、完全に秘匿される必要性が高いものであるとまでいうことはできない」「住民票コードは、住民票の記載事項であるにすぎず……私生活上重要であり、完全に秘匿される必要性が高いものであるとまではいえない」と述べて、本人確認情報の要保護性を実質的には認めていません。

他方、住基ネットについては、行政「事務の効率化や正確性の向上に資するもので」、「住民の利便性の増進を図ることも可能になる」ので、「正当な目的を有する」と評価しています。その上で、正当な目的を有する以上、「住基ネットの導入によって、個人情報について、みだりに収集、開示が行われているということはできない」（以上、８０～８２頁）と結論づけています。

以上の要約から明らかなように、本件原審判決は、３高裁判決の中では①判決に最も近い判断となっています（むしろ①判決の原型というべきかもしれません）。それゆえ、本件原審判決に対しては、質問事項２および３への回答で①

判決について述べたことがそのまま妥当すると考えています（本鑑定意見書８～１０頁参照）。

また、住基ネットの特質に関しても、③判決と対照的に、「住基ネットは、それぞれの機関が受領した本人確認情報を分散して管理することを制度として予定していることから、これらの機関が分散管理している情報を統一的に収集し得る主体もシステムも存在しない」ので、「住基ネットの導入により、目的の範囲内の利用を越えて行政機関が持っている個人情報がデータマッチングされ、住民票コードをいわばマスターキーのように使って名寄せされる具体的な危険性があるとは認めがたいというべきである」（９０頁）と述べています。

こうした認定を支えているのが、住基法「改正……の経緯、趣旨及び目的」を重視し、「行政事務の効率化を図ろうとした改正法の趣旨及び目的を没却させる……ような方向で住基法の文理解釈を修正することは許容されない」（６１頁）という本件原審判決の基本的態度です。もちろん制定された法律を尊重すべきことは当然ですが、法律が制定されれば、その規定が憲法にとって代わるわけでないことはいうまでもありません。しかし、本件原審判決は、頑なまでに改正住基法の定めに忠実であることを求め、同法の規定自体に存在するかもしれない問題点をプライバシー権保障の観点から検証してみようとはしません。その点では、①判決以上に形式的な思考をしているといってもよいでしょう。なお、以上の点に関しては質問事項５、６および７で、それぞれ具体的に検討したいと思います。

５　個人情報保護の評価基準としてのＯＥＣＤ８原則については、名古屋高裁判決及び本件原審判決が判示し、堀部政男意見書（乙１０）も提出されています。それらの問題点につき、ご指摘下さい。併せて、ＥＵ指令の位置づけ・内容についても、お聞かせ下さい。

①判決がＯＥＣＤ８原則（以下、「８原則」といいます。なお、８原則の内容は①判決や本件原審判決に言及があるので、ここでは繰り返しません）に言及しているのは判決書５２頁から５４頁ですが、そこでは８原則と住基法の規定の各文言を対応させるだけで「ＯＥＣＤ８原則に沿った内容となっているものと認められる」と認定しています。しかし、なぜ「認められる」のかについては一切説明がなされていません。その意味で、単なるあてはめにとどまっています。こうした態度は、本件原審判決や堀部意見書にも共通する姿勢ですが、ここでは、そうした形式的判断で「８原則に沿っている」と認定することの問題点をはっきりと示している本件原審判決と堀部意見書を検討対象としたいと思います。

（１）ＯＥＣＤ８原則の法的拘束力

本件原審判決は、そもそも８原則について、「法的拘束力を認めることはできない」という立場をとっています。なるほど、８原則は、ＯＥＣＤ理事会の勧告にすぎませんから、その点で法的拘束力がないともいえます。しかし、８原則は、日本政府も遵守義務を負っている「市民及び政治的権利に関する国際規約」（いわゆるＢ規約）１７条を具体化したもので、情報の国際的流通を前提に、それを促進するために必要な個人情報保護の「最低基準」を示したものですから（８原則に付されたAnnex to the Recommendation ６による説明）、日本も加盟しているＯＥＣＤの設立目的に適合的であろうとするならば、政府は８原則を充たす法制度を整えなければなりません。それは、厳密な意味で日本国内における裁判規範ではないかもしれませんが、政府はこれを無視できないという意味で、政府にとって国際人権Ｂ規約と同様の拘束力があるのです。

また、ＥＵ個人データ保護指令（以下、「ＥＵ指令」といいます）は、その水準を充たさない第三国に対して、ＥＵ市民の個人情報を移転することを認めません。それゆえ、日本がＥＵとの経済的・社会的関係を継続しようとする限り、政

府はＥＵ指令に示された個人情報保護の水準を充たす法制度を設けなければならないのです。

もちろんこれは、他国との経済的・社会的関係を考慮しつつ政府が負う責務であって、８原則やＥＵ指令が市民に権利を保障する人権規範であることを当然には意味しません。しかし、例えば８原則は、個人情報を国際的に流通させることを可能にする「最低基準」として、個人に対し保障されるべき権利や措置を具体的に提示していますので、政府が８原則に対応する国内的保障策を講じない場合には、他国との関係継続を望む以上、保障できない理由をＯＥＣＤと日本国民に説明する必要があります。

また、ＥＵは、ＥＵ指令の求める水準の個人情報保護制度を設けない限り経済的･社会的関係を継続しない旨を宣言しています。したがって、個人情報保護制度の具体化は、関係継続を望む日本国民にとっても無関心でいられる事柄ではありません。この点で、日本国政府は、ＥＵの求める水準の個人情報保護制度を設けないことの説明責任を国の内外に果たす必要があるのです。以上のことからわかるように、ＥＵ指令は日本国内で法的拘束力を有する裁判規範とはいえません。しかしながら、それが個人情報保護の基準のひとつであることまで否定する理由もないでしょう。裁判規範としての法的拘束力がないからといって、その内容までが無意味なものになるわけではありません。むしろ、あるべき個人情報保護の水準を明らかにするための有力なてがかりのひとつであるはずです。

他方、政府がこれらの国際的準則を充たした法制度が国内に存在すると主張しても、その内容に合理的な疑問が提起された場合には、上に述べたのと同様の説明責任を負っているといわなければなりません。私は、次に述べるように、本件原審判決や堀部意見書が、政府に代わって納得のいく説明を果たしたとはいえないと考えています。なお、ＥＵ指令は８原則をさらに精緻化したものですから、仮に８原則が充足されていないのであれば、ＥＵ指令が充足されているかどうかについて論じる意味はありません。

（2）ＯＥＣＤ８原則をめぐる本件原審判決と堀部意見書の問題点

すでに論じた本件原審判決の特徴である形式的思考は、８原則との関係においても見出すことができます。例えば、住基法１条は住民基本台帳およびその事務の目的を規定し、同３０条の６から３０条の８までにおいて本人確認情報の提供先と利用事務を明示しているので、８原則の定める「目的明確化の原則」（第３原則）に反しないと本件原審判決は述べます。

しかし、１条には「住民に関する事務の処理」、「住民の利便の増進」、「国及び地方公共団体の行政の合理化」等の一般的抽象的な目的が掲げられているだけですので、実際上いかなる内容でも含めることが可能です。これで「目的明確化の原則」や、目的に適合する限りで個人情報の利用を認める「利用制限の原則」が充足されているというのであれば、それらの原則は、元来が無内容な原則であったか、あるいは充足という言葉の意味を薄めて理解する必要があります。

具体例をあげると、本件原審判決は、１条の目的には「国及び地方公共団体の行政の合理化に資すること」も含まれるので、「住民基本台帳に記載された事項の全国的・広域的な行政利用も予定していたものというべき」（７７頁）であると指摘しています。また、利用制限の原則との関係では、「３０条の６から３０条の８までにおいて本人確認情報の提供先と利用事務を明示し」（７８頁）ていると述べていますが、利用事務は、現在ではかなり大部になった有斐閣版小六法にすら掲載されていない別表に委ねられており、内容の確認が容易ではありません。また、提供先も国内の全地方公共団体におよんでおり、それを逐一確認することは、現実問題として不可能に近いでしょう。

ちなみに、堀部意見書も、「目的明確化の原則は、住民基本台帳法第１条の目的規定に加え、第３０条の６ないし第３０条の８及び別表において本人確認情報の提供先と利用事務を明示し、これに限定していることが挙げられる」「利用制限の原則は、第３０条の６ないし第３０条の８及び別表において本人確認情報の

提供先と利用事務を行政機関等に限定していることのほか、第３０条の３０の『本人確認情報の利用及び提供の制限』、第３０条の３４の『受領者の本人確認情報の利用及び提供の制限』などが対応している」（５～６頁）と述べて、本件原審判決と同様の立場をとっています。

以上の例でわかるように、本件原審判決や堀部意見書は、たとえ一般的抽象的な文言でも、とにかく「目的」を語っていれば、利用目的を特定したことになると考えているようです。しかしそれでは、「目的の明確化」という日本語の日常的な用法とはいえません。「行政の合理化」という「目的」に含まれないのは、行政と無関係のものくらいです。

また、利用制限の原則との関係でも、住基法は「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してはならない」と規定しているだけですから、法律で定めさえすれば、利用・提供の対象を拡大することは容易に可能です。実際、住基法制定以来、利用対象は拡大され続け（２００６（平１８）年５月１５日現在で２９３事務）、今では税金やＮＨＫ受信料の徴収にも利用することが議論されています。

もちろん、市民は法令上の利用拡大を知ろうと思えば知ることはできるでしょう。しかし、一般市民が利用対象を把握することは実際には極めて困難であり、本人の同意や利用をめぐる異議申立ての機会は保障されていないも同然です。これでは、利用目的の明確化や利用制限の原則のみならず、目的の告知は本人が理解できるように行うことを求める８原則における個人参加の原則も実現されていないといわざるをえません。

このように、本件原審判決ならびに堀部意見書は、単に形式的に住基法と８原則の対応関係を説明するだけにとどまっています。住基法の規定が８原則に適合するように目的を明確化しているか、それらが利用・提供の制限といえるだけの具体的内容を有しているか等については、何らの具体的説明も行われていません。私は、ここにもOlmstead判決と同様の形式的思考（「屋外に設置されているから」）

を見出すことができると考えています。

6　住基法・行政機関個人情報保護法の規定の評価・解釈をめぐって、３高裁判決の間で違いがあり、それがデータマッチング・名寄せの具体的危険性を認めるか否かの差になって表れているように思われますが、３高裁判決の上記規定の評価・解釈の当否についてのご見解をお聞かせ下さい。

私は、これまでと同様、ここでも形式的思考と実質的思考の違いが３判決の間に住基法や行政機関個人情報保護法の評価や解釈に違いを生じさせたと考えています。以下では、判決文に即して検討してみましょう。

（１）①判決における規定の評価・解釈について

①判決は、「住基ネットにおいては、住基法によって本人確認情報の保護のための禁止規定やこれに違反した場合の罰則が設けられているほか、住基ネットや住基カードについてセキュリティ対策が講じられており、これらによって、運用関係者による漏えいの危険や外部の第三者の侵入による本人確認情報の漏えいや改ざんを防止するための合理的な措置が講じられているものと認めるのが相当である」（４８頁）と述べて、本人確認情報保護のためにとられている法的ならびに技術的措置が十分なものであると評価しています。

しかしながら、法的措置については、質問事項５での議論における８原則の評価と同様、単に関係する条文を列挙して十分であると評価しているにとどまります（３１～３５頁）。具体的にそこで取り上げられているのは、ａ総務大臣や都道府県知事、都道府県審議会の各種権限（監督命令等）、ｂ本人確認情報の安全を確保するための措置を講じる義務、ｃ都道府県知事ないし指定情報処理機関に対する利用又は提供の制限、ｄ市町村、都道府県及び指定情報処理機関、電算処理受託者ならびにその役員、職員等に対する罰則を伴う

秘密保持義務等、ｅ住民票コードの告知に関する制限の５点ですが、いずれも条文が列挙されているだけで、そこで採用されている措置が具体的に検討されているわけではありません。

例えば、ｃの利用又は提供の制限は、住基法の定める場合以外には本人確認情報を利用又は提供してはならないという当然の事柄を規定しているにすぎません。これでは、住基法で定めれば、いかなる利用･提供も行うことができることになってしまいます。かくして、質問事項５でも指摘したように、気がつかない間に利用範囲が拡大されることによって、市民は実際には自分の本人確認情報の利用状況や提供先を確認することが極めて困難（事実上不可能）となります。自分に関する情報がどのように利用され、あるいはそれを誰が保有しているのかを知ることが現実には困難な状況でも、法律上は知ることができる仕組みになっているからプライバシー権が侵害されているとはいえないという説明は、Olmstead 判決と同様の、現実を見ない形式論といわなければなりません。

それにもかかわらず、このように制度のたてまえ論を貫くのであれば、個人が自分で自分に関する情報の流れを実質的にチェックできない以上、住基法に基づいて本人確認情報を取り扱う機関とは別の、独立・公平な第三者機関が情報の流れをチェックするなどの制度が最低限必要となるでしょう。この点は、質問事項７で検討します。

このように、住基ネットをめぐる訴訟において問われていることは、現在の法制度が憲法上のプライバシー権を保障するものとなりえているかどうかです。そうした検討を行わないまま、単に条文を列挙するだけで保護に欠ける点はないと論じるだけは、説明として不十分であるとのそしりをまぬかれないでしょう。

同様の問題点は、総務大臣等の監督権限についてもあてはまります。住基法で定めればいかなる利用・提供でも行うことができるという前提を不問に

付したまま、監督権限に関する条文を列挙しても、それはいわゆる自己言及的正当化論にすぎません。制度の運営主体ないしそれに関連する機関が自らを常にチェックしているから安心であると主張しても、その説明で納得する人はほとんどいないはずです。このことは、住基法に基づき本人確認情報を取り扱う機関相互の間でのチェックにおいても同様にあてはまります。このような場面では、住基法上の業務と全く無関係の公平・独立な第三者機関の設置が必要であることは、上に述べた通りです。しかし、住基法上、そのような機関は存在していません。

また、本人確認情報の安全確保についても、「本人確認情報の適切な管理のために必要な措置」（住基法３０条の２９）の内容こそが問われているのに、「必要な措置」を講じることが規定されていると引用しているだけですから、同様に肝心の問題点は解消されていないのです。さらに、住民票コードの告知制限や秘密保持義務も、それ自体としては当然のことを規定しているにすぎません。肝心なことは、そうした制限や義務の履行が確保されていると市民が信頼できるようなチェック体制、つまり独立・公平な第三者機関を作ることであるにもかかわらず、そのような機関は設けられていないのです。

プライバシーのような不可逆性を特質とする権利を侵害する可能性を有する制度を設ける場合には、侵害行為が生じないようにチェックする機関は不可欠です。現在の法制度がそれにふさわしい機関であるかどうかを不問に付したまま、現行法上の制度を引用して、十分な措置が講じられていると評価するだけでは、説得力はありません。①判決が形式的思考を特徴としていると指摘する所以です。

さらにまた、住基ネットのセキュリティ対策に関する３５頁以下の評価についても同じことが指摘できます。なるほど、総務省の行ったセキュリティ対策は、それ相応のものでしょう。そうでなければ、住基ネットという公的システムを構築することは、そもそも許されないはずです。その意味で、技

術的に可能な限り万全な対策がとられるべきことは当然のことにすぎません。しかし、コンピュータ開発の歴史において、セキュリティ技術の確立と破壊が繰り返されてきたことは周知のとおりです。少なくとも、現時点では１００パーセント確実で安全な技術は存在しません。そこで、セキュリティが損なわれる事態を想定して、公平・独立な第三者機関によるチェック等の法制度によるバックアップが必要となるのです。

住基ネットにおいて、このようにセキュリティを確保するための法的制度や厳重な技術的対策の必要性が強調されるのは、前述のように、住基ネットが各行政機関の保有する情報の結合を可能にするネットワーク・システムだからです。住基ネットは、潜在的に住民の個人情報を包括的に取扱う能力を秘めているからこそ（制度上は、本人確認情報を収集・保有し利用するだけのシステムですが）、人格権保障の観点からさまざまな疑問が提起されてきたのであり、その点こそが住基ネット問題の核心なのです。この点は、データマッチングの問題と深く関わります。

①判決は、データマッチングに関連して、（ア）「国の機関等は、……住民票コードを要素とするデータベースを作成し、保有しているものと認められる。……住民票コードはデータマッチングのキーとして容易に使用できるものである」と述べます。しかしながら、（イ）「行政機関が保有する個人情報を一元的に管理する主体は存在しない」（ウ）「指定情報処理機関が住民に関するデータベースを作成、保有することはないし、国の機関からデータベースの提供を受けることもないから、指定情報処理機関が、控訴人らの指摘するようなデータマッチングをする可能性はない」（エ）「本人確認情報の受領者は、……住基法所定の範囲内に限り、本人確認情報とその保有する個人情報とを、比較、検索、結合することができるものであり、当該事務に属さない事務のために他の事務に関するデータベースと結合することは禁止されている」（オ）「国の機関等が、他の国の機関等が保有する

住民票データを含むデータベースの提供を受けることは、住基法３０条の４２により禁止されているから、他の国の機関等が保有するデータベースと結合を行うことはできない」（カ）都道府県知事や指定情報処理機関は、本人確認情報の提供状況について、「報告書を作成して、公表すること」（キ）「都道府県知事は、国の機関等に対して、提供した情報の適切な管理のための措置の実施状況につき報告を求め、適切な措置の実施を要請を行う」等の不正な利用に対する監視措置が講じられていることを理由に、「データマッチングの危険にさらされているということはできない」（以上、５０～５２頁）と結論づけました。

この判旨には、次元の異なる事柄が同列に論じられている点で、理論的混乱があります。（ア）では、データベースの作成が技術的に可能であることを認めておきながら、（イ）以下で、データベースの作成は法律上禁じられているからできないと論じている点がそれです。例えば（オ）で、「住基法３０条の４２により禁止されているから……データベースと結合を行うことはできない」と論じている部分がその具体例といえるでしょう。これでは、盗聴装置を屋外に設置しても、法律で屋内での会話の盗聴は禁じられているから盗聴はできないといっているのと同じです。物理的には可能だけれど、法律で禁じているから行われることはないという説明は、データマッチングの危険を否定する論拠として説得的であるとはいえません。物理的に可能であれば、法律に違反する行為がなされないようにチェックすることは常識に属します。そして、住基ネットにおいては、行政機関相互のコンピュータ・ネットワークを通じて扱われる個人情報の質と量を考慮すると、チェック機関は、本人確認情報の取扱いを業務とする機関以外の独立・公平な第三者機関であることが制度への信頼感と透明性の確保のためには不可欠なのです。

また、①判決は、行政機関個人情報保護法に言及して、「同法においても、

個人情報を保有するに当たっては、行政機関は、法令に定める事務を遂行するために必要な場合に限り、かつ、その利用の目的をできる限り特定しなければならないこと、利用目的の達成に必要な範囲を超えて、個人情報を保有してはならないこと（行政機関個人情報保護法３条）、利用目的以外の目的のために保有個人情報を自ら利用し、又は提供してはならないこと（同法８条）が定められて」（５１頁）いることなどを、データマッチングの危険を否定する論拠にあげています。

法律で禁じられているからという論拠の問題点は、上に述べたとおりですので繰り返しません。また、利用目的の限定という法制度上のたてまえも、「目的の達成に必要な範囲を超えて」「利用目的以外の目的のために」といった、それ自体としては当然の限定が、実際には限定として機能しない（住基法における目的概念の漠然性と法改正による目的変更の容易性）ことも、すでに述べました（本鑑定意見書２７～２８頁）。

もっとも①判決は、この点について、「住基ネットにおける本人確認情報の提供先、利用目的の変更等は法律の改正によるべきものであって、国民の意思を離れて無制限に拡大する性質のものではないから、将来法律の改正によって提供先及び利用目的の変更がありうるからといって、住基ネットが名寄せ、データマッチングの可能性を持ち、プライバシー保護の見地から危険な制度であるということはできない」（５２頁）と反論しています。

ここには、本人確認情報の提供先や利用目的の変更について法律で改正すれば国民の同意があったとみる考え方が前提とされています。しかしこれはあまりに形式的な擬制であり、提供先や目的変更を容易には知りえない住基ネットにおいては採用できない考え方であることは、すでに指摘しました（本鑑定意見書７頁、２８～３０頁）。

また、①判決は、「控訴人らの主張は、将来における名寄せ、データマッチングの抽象的な危険性を指摘するものであって、現時点での住基ネットに具

体的な危険性があることを主張するものとは認められない」といいます。この点についても、本鑑定意見書１７～１８頁で論じたように、住基ネットにおいては抽象的危険と具体的危険は連続した関係にあり、具体的危険が現実のものとなってからでは手遅れであることを忘れるべきではありません。そして、抽象的危険が具体的危険へと転換しないようにするためには、それを監視する仕組みが必要になります。この点は、さらに質問事項７で検討します。

（２）②判決における解釈・評価について

②判決も住基法については、「本人確認情報を含む個人情報保護を目的とする多数の規定を置いている」として、①判決とほぼ同じ評価を行っています。すなわち、（ア）都道府県知事及び指定情報処理機関が住基ネットに関して保有する情報は本人確認情報のみに制限される、（イ）本人確認情報を利用し、提供できる場合及び提供の相手は住基法により限定される、（ウ）その提供を受けた国の機関（受領者）が受領した本人確認情報の利用及び提供も住基法により制限されている、（エ）関係者の秘密保持義務と違反に対しては刑事罰が課される、（オ）本人確認情報の漏えい等の防止のために必要な安全措置を講ずる義務が規定されている、（カ）都道府県知事及び指定情報処理機関には本人確認情報の保護に関する事項を調査審議するための第三者機関の設置規定が存在することなどを理由に、「住基法は、本人確認情報を含む個人情報保護に相応の配慮をし、その保護のための施策を講じているものということができる」と結論づけたのです。

以上の指摘に関しては、①判決について論じたことがそのままあてはまりますので繰り返しません。②判決の特徴は、「本人確認情報を使用したデータマッチングは、住基ネットに関係する都道府県知事、国の機関等あるいはその職員がこれら法律の定めを遵守する限りは実現しないのであり、これらの者がこれら法律の定めに違反することを当然の前提として、上記データマッ

チングの具体的な危険があるとすることは、当を得たものということはできない」と述べている点にあります。

なるほど、住基法の規定に反して故意に違法行為を行う職員はそう多くはないでしょう。しかし、個人情報に経済的価値が認められ、あるいは個人情報に個人的な関心を持つ者が皆無とはいえない社会状況を念頭に置くと、そうした職員が全く存在しないと想定することも楽観的にすぎるかもしれません。

また、過失による個人情報の漏えいは、さらに深刻です。質問事項３で言及した愛媛県愛南町における住民票コードを含む住基情報の大量流出は、各自治体から業務を請け負った情報処理会社の元社員のパソコンから、ファイル交換ソフト「ウイニー」を通じて発生したものです。これを、委託先の元社員が行ったことで、住基ネット自体に固有の危険があることを意味しないと言い逃れることはできません。住基ネットは、いかなる原因であれ、そこに蓄積されたデータが漏えいすれば、個人に深刻な影響を与える可能性を有するネットワーク・システムなのです。実際、新聞報道（２００７年（平１９）５月１８日読売新聞夕刊）によれば、愛媛県愛南町で流出した個人情報は、住民票コードや国民年金口座など約１４万３０００件であるということです。たとえ、現時点でこれらの情報が悪用されたという報告はなくても、この種の情報は時を経て次第に悪用されることはしばしばあることですし、何よりも、悪用される可能性があること自体が問題とされなければなりません。

さらにいえば、データマッチングが組織的に行われないという保証もどこにもありません。のちに質問事項７で紹介するドイツ連邦憲法裁判所の国勢調査判決は、電子データの蓄積には以上のような問題点があるという認識に立脚して、国勢調査に基づくデータの利用について個人の権利を保障するために必要と思われる条件を、憲法から導き出しました。そこで注目されたのは、コンピュータ・ネットワークの具体的危険ではなく抽象的危険であった

ことは、わが国の住基ネット問題を考える上でも示唆的です。そして、このように抽象的危険に着目する以上、質問事項７で検討するような第三者監視機関の要否は、決定的に重要な問題となるのです。

（３）③判決における解釈・評価について

③判決は、①・②判決が指摘していたような「法規制からすれば……住基ネットの運用によって控訴人らが主張するようなデータマッチングや名寄せが行われることは考え難いといえなくもない」と述べます。しかしながら、各行政機関の個人情報の取扱いを規律する行政機関個人情報保護法は、３条３項で利用目的の変更を認めていますが、それには同法８条３項のような他の法令の適用がある旨の規定が存在しません。したがって、受領者の本人確認情報の利用及び提供の制限を定める住基法３０条の３４の適用がなく、目的外利用が可能となるという問題点が存在していることを指摘しています。

この点、利用目的変更後の目的は、行政機関個人情報保護法３条１項にいう「利用目的」に該当するので、行政機関個人情報保護法８条１項・３項の適用を受け、住基法３０条の３４が適用されるとの反論があるかもしれません。しかし、行政機関個人情報保護法３条１項の役割は、行政機関が個人情報を保有する際に目的を「特定」して示すこと、つまり収集目的を明確化することにあります。ところが、同３項でいかに「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」に限定されていても、「合理的に認められる範囲」は行政機関の裁量判断に委ねられていますから、収集時点で特定された利用目的の変更は依然として可能です。もとより、この段階では、住基法３０条の３４を適用する余地はありません。このように利用目的が変更されたあとで、変更後の利用目的も行政機関個人情報保護法３条１項の「利用目的」に該当するので同法８条１項・３項の適用があり、住基法３０条の３４が適用されると論じても、それは形式的な条文操作にすぎず、有効な反論

とはいえないのです。

もっとも、本人確認情報の受領者である行政機関等については、住基法３０条の３４で本人確認情報の目的外利用が禁じられています。これはしかし、本人確認情報を目的外に利用することの禁止であって、本人確認情報を利用して入手した個人情報の利用目的を変更することの禁止ではありません。個人情報を収集した時点で本人確認情報の利用が目的外利用に該当しなければ、それ以降、受領者が入手した情報は、行政機関個人情報保護法の適用対象情報となりますから、同法３条３項の利用目的の変更も可能となります。

本人確認情報の利用目的と、行政機関個人情報保護法における個人情報の利用目的は、「利用目的」という用語において同一でも、どの情報に関してのものであるかは当然には同じでないことを忘れるべきではありません。後者には、本人確認情報を利用して入手した本人確認情報以外の個人情報も含まれているのです。それゆえ、行政機関個人情報保護法と住基法を一般法と特別法の関係にあるとして、常に必ず特別法である住基法が適用されると論じることは誤りであるといわなければなりません。

また、仮に本人確認情報を利用して入手した個人情報についても住基法３０条の３４の適用を受けるので、当該個人情報の利用目的も変更できないと解するとしましょう。しかし、その禁止を担保する制度は現行法には存在しません。法律で禁止されているからというだけでは、永続的かつ実効的に禁止違反をチェックすることはできないでしょう。

目的の変更に関する法制度をこのように解すると、目的の変更は制度上あるいは事実上、行政の裁量に委ねられることになります。③判決は、それをチェックする適切な監視機関が制度上存在しない点を指摘して、データマッチングの危険があることを指摘したわけです。この点、①・②判決は、都道府県審議会や指定情報処理機関における本人確認情報保護委員会があるので第三者監視機関は存在すると指摘していますが、これらは住基法上の内部機関

ですから、国の行政機関等の本人確認情報の利用について調査権限があるわけではありません。

つまり、本人確認情報を利用する各行政機関においては、収集された個人情報の利用目的を変更することについて、それが適正に行われることを確保する制度的担保が実質的に存在しないのです。こうした理由から、「利用目的変更の適切な運用が厳格になされる制度的担保は存在しないといわざるを得ず、住基法の利用目的明示の原則（同法４条）が形骸化する危険性は高い」（以上、７８～７９頁）と指摘して、③判決は制度内在的にデータマッチングの危険があることを明らかにしているのです。これは、正当な認識といわなければなりません。

その他、（ア）住民が利用対象事務を把握することは困難であること、（イ）本人確認情報の開示請求権（住基法３０条の３７第１項）の対象は磁気ディスクに限定されているため、「本人確認情報がいかなる機関に提供されたか、それ以外の情報を都道府県や国、指定情報処理機関が保有していないかどうかといった重要な点について、本人において確認することが事実上不可能な状態にある」こと、（ウ）住民票コードの「民間利用禁止の実効性は、現実には非常に疑わしい」こと、（エ）行政機関個人情報保護法は、利用・提供制限の例外として、「行政機関が法令の定める所掌事務の『遂行に必要な限度で』保有個人情報を内部で利用する場合であって、当該個人情報を利用することについて『相当な理由があるとき』（同法８条２項２号）……は、本人の同意がなくとも、利用目的以外の目的のために保有個人情報を利用し又は提供することができる……と定める」が、「上記の『必要な限度』、『相当な理由』等の要件の有無は、行政機関が自ら判断するのであるから、実施には、実効性の有る利用制限の歯止めになり得ず、行政機関が住基ネット上における本人確認情報の利用を事実上自由に行いうることになってしまう危険性」などをあげて、「現在の住基ネットのシステム上では一元化の主体機関は存在しな

いことから、個人情報の完全な一元化までの具体的危険があるとはいえないにしても、行政機関が個別に保有する多くの部分の重要な個人情報が結合・集積され、利用されていく可能性は決して小さくない」（以上、８０～８２頁）ことも指摘しています。

③判決も指摘するように、これらは伝統的用語法における意味での具体的危険の存在を示すものではないかもしれません。しかしながら、同判決の分析が示すように、制度上、必ずしも名目どおりに個人情報の保護が図られる仕組みになっているわけではないことを考慮すれば、住基ネットにおいては、具体的危険が抽象的危険と常に隣り合わせにあるということが、決して思い込みや偏見でないことは、おわかりいただけるだろうと思います。

③判決は、以上のようなさまざまな考慮を経由して「危険は、抽象的な域を超えて具体的な域に達している」との結論に到達しましたが、実をいうと私自身は、住基ネットにおける肝心の問題は、プライバシー権を侵害する具体的危険性があるかどうかではないと考えています。事案が出版の差止めであれば、現に目の前にある出版物にプライバシー権侵害の具体的危険性があるかどうかを問うことは当然でしょう。しかし、住基ネットで問われているのは、プライバシー権保障における公権力行使のあり方です。この場合、対表現の自由とは異なり、公権力の抑制を大胆に行っても、原則として（公権力の行使が憲法上義務づけられていない限り）憲法に違反することはありません。しかし現実には、公権力の側に個人情報の収集･利用権限があることが前提とされて、当該権限の抑制には具体的危険性が必要であると説かれています。これは、権利の保障論として倒錯しているといわなければなりません。

住基ネットのようなコンピュータ・システムにおいては、情報処理の速度が速いので、具体的危険が発生してからでは被害の発生を回避することは困難です。たしかに、法律の文言上は、①・②判決のいうように、住基法も行

政機関個人情報保護法も、個人情報の収集目的を明確化し、利用制限を行政機関に課しているようにみえます。しかし、制度の仕組みを多少なりと分析してみると、現在の住基法や行政機関個人情報保護法の制度では、③判決が指摘するように、具体的危険の発生を回避する仕組みとして適切でないことがわかります。そこで、次の質問事項では、具体的危険の発生を回避する制度について、検討してみたいと思います。

7　データマッチング・名寄せの具体的危険性を認めるか否かの差は、第三者監視機関の有無・必要性（名古屋高裁金沢支部判決・大阪高裁判決）、監視措置・是正制度の有無（名古屋高裁判決）についての理解の違いからも来ているようですが、このあたりについてはどのように考えるべきでしょうか。

（１）住基ネットにおける具体的危険の回避

プライバシー権侵害について、具体的危険性が存在することを要件とする考え方は、質問事項２で検討したプライバシー概念と密接に関連しています。例えば、①判決における「国家機関が、正当な理由もないのに、個人の同意を得ず、みだりに個人の私生活上の情報を収集、開示することは、同条に反して許されない」という説示が、「正当な理由」があれば、個人の同意なしに私生活上の情報を収集,開示できることを意味するものであることは、すでに指摘しました。住基ネットがプライバシー権を侵害するというためには、それに具体的危険が伴っていることの立証が必要であるという考え方は、公的機関による本人確認情報の収集･利用権限を自明の前提とするからこそでてくるものです。

しかし、この収集･利用権限は、コンピュータ･ネットワークを前提にした場合、自明のものではありません。質問事項６への回答で言及（３６頁）したドイツ連邦憲法裁判所は、１９８３年の国勢調査判決（BverfGE　６５,１）

で「人格の自由な発展は、データ処理に関わる現在の条件の下では、個人情報の無制約な収集、蓄積、利用及び流布に対して各人が保護されることを前提とする。この保護は、基本法１条１項と結びついた２条１項に含まれる。基本権は、その限りで、個人情報の放棄及び利用について原則として自ら決定する各人の権限を保障する」と述べて、自己情報コントロール権を憲法上の具体的権利であるとの明快な判断を示していました。これは、コンピュータ・ネットワークが個人情報の保護にとって潜在的に危険性を有しているとの認識を前提にしての判断です。

さらに、１９９９年の通信監視判決（BverfGE　１００,３１３）では、「審査の基準となるのは基本法１０条であるが、国勢調査判決の諸規準は、基本法１０条にも妥当する。①侵害の目的が領域に特化したかたちで、かつ、詳細に規定されており、収集されたデータがこの目的のために適合的であり必要であること。また、取得されたデータの保存･利用は、閲覧を授権した法律が定めた目的に原則として拘束される。②基本権の要請は、……情報の他者への提供におよぶ。データの伝達は、通常、利用連関の変更を伴い、当事者に対して、当初の連関におけるよりも重大な結果をもたらしうる」と指摘しています。翻訳文はやや難解かもしれませんが、①は収集目的の明確化、②は目的外利用の禁止について述べているもので、それらを憲法の保障する基本権の一内容と認めたわけです。

これに対して日本では、①判決が典型的であるように、自己情報コントロール権の権利性にはいまだに疑問が呈され、収集目的の明確化や目的外利用の禁止を名目的なものにとどめて怪しむところがありません。８原則やＥＵ指令は、ドイツ連邦憲法裁判所が下したような判断を基礎づけ、また、そうした判断によって具体化されているわけですが、日本では、質問事項４で検討した本件原審判決や堀部意見書の見解が依然として主張され、③判決のような一部の例外を除いて、住基ネットの適法性と安全性は疑問の余地のない

ものと観念される傾向にあります。しかし、日本の「例外」は、ドイツでは憲法「原則」なのです。

このことが意味するのは、住基ネットを基軸とする行政機関のコンピュータ・ネットワークにおいて公的機関が本人確認情報を収集・利用する権限は自明のものではなく、また、具体的危険性がなければプライバシー権侵害は生じないと考えることにも疑問の余地があるということです。逆にいえば、住基ネットにおいては、具体的危険の発生を回避する何らかの制度が設けられていなければ制度を正当化することはできないのです。そうした制度を欠いている場合、③判決のように「危険は、……具体的な域に達している」と解するか、それともプライバシー権侵害は抽象的危険で足りると論じるかは、あえていえば言葉の問題にすぎません。

（2）プライバシー権侵害を回避する制度

結論を先にいえば、住基ネットにおいてプライバシー権侵害を回避するために最低限必要な制度は、公平な第三者によって構成される情報取扱いの監視機関です。①判決は、都道府県や指定情報処理機関のような住基法上の機関に監視機能を委ねることで足りると解し、②判決も、若干の疑問は呈するものの、結論としては大差ありません。しかし、住基ネットで収集・利用される情報の取扱いを監視する機関として、それらが適切な存在であると考えることは、行政機関に司法機関としての役割を兼務させるのと同じであるといわなければなりません。

逆に、第三者監視機関に関する各判決の立場の違いは、住基ネットにおけるデータマッチングや名寄せの危険性に対する各裁判所の評価を反映しています。具体的危険がない以上、プライバシー権の侵害もないと考える①・②判決は、住基法上の措置や機関で足りると考えるでしょうし、住基ネットは現に危険な域に達していると解する③判決は、第三者による監視機関が存在

しないことを「危険」認定の一要素としています。

質問事項６で言及した愛媛県愛南町における情報の大量流出を例に考えてみましょう。この事件において、個人情報が流出してはじめて具体的危険ありと考えることは、すでに指摘したプライバシー情報の不可逆性（本鑑定意見書１３頁）という観点からみて適切でないことはおわかりいただけるだろうと思います。しかし、①・②判決のように、個人情報が流出していない段階では抽象的危険にとどまるとして、住基ネットを正当化すれば、データの流出を阻止する具体的なタイミングは、実際には存在しないも同然です（観念的に考えれば、抽象的危険が具体的危険に変わる時点は存在するでしょうが、コンピュータ・ネットワークにおいては瞬時に変わりますから、人間が遮断することはほとんど不可能です）。それゆえにこそ、抽象的危険が具体的危険に変わらないようにチェックするための制度として、ネットワーク全体について公平かつ独立で実効的な監視権限をもつ第三者機関の設置が要請されるのです。それは、住基ネットを正当化するための必要最小限の条件であるといってもよいでしょう。

このように私は、コンピュータ・ネットワークを形成する基点としての住基ネットの性格を考えるとき、具体的危険の発生を回避するためには、各行政機関における個人情報の取扱いをチェックする独立かつ公平な第三者機関が是非とも必要であると考えます。そして、そうした制度が存在しない現状では、自分の情報を守るための最終手段として、住基ネットからの離脱を選択する自由が保障されるべきことが、憲法上のプライバシー権保障の帰結であると考えます。

第三者機関に関しては、ＥＵ指令における監視機関の定めが参考になります。ＥＵ指令は、ＥＵ域内のみならず日本のような第三国にも、８原則以上に厳格な個人情報保護を要求しますが、個人情報保護を達成するための形式や方法について各国の裁量にゆだねました。しかし、個人情報保護が達成されたかどうかについては、ヨーロッパ委員会が加盟国の代表者からなる「専門委

員会」（３１条）の支援を受けて、最終的に「十分なレベルの保護」について判断することとされています。そして現在でも、ヨーロッパ委員会は、日本を「十分なレベルの保護」を行っている国であると公式には認めていないようです。

その理由のひとつとして、ＥＵ指令２８条に規定される監視機関が存在していないことを指摘することができます。同条は、ＥＵ指令を遵守すべく加盟国が制定した個人情報保護法制が実効的に適用されていることを監視する職務を遂行する「完全に独立した」監視機関の設置を求めています。この監視機関は、（A）処理対象のデータにアクセスする権限や（B）監視を遂行するために必要なあらゆる情報を収集する権限、具体的には（ア）データ対象者の権利や自由に危険を及ぼす可能性のあるデータ処理作業について、作業が実施される前に勧告を行う権限や、そうした勧告が適切に公開されることを確保する権限、（イ）データのブロック化や消去ないし破壊を命じる権限、（ウ）データの処理を一時的ないし確定的に禁止する権限、（エ）データ管理者に対する警告や懲戒権限、（オ）データ処理において問題となる点を議会等に照会する権限をはじめとする実効的な介入権限、さらには（C）個人情報保護法制に違反する措置に対して訴訟を提起し、あるいは違反を司法当局に通知する権限などを有する機関で、個人データの処理に対する個人の権利及び自由に関して、個人または個人を代表する機関からの請求を受理するものとされています。もちろん、関係する個人や機関は、請求の結果に関して通知を受ける権利を有しています。また、各監視機関は定期的にその活動について報告書を作成し、その報告書は公開されるものとされています。さらに、監視機関は、他の加盟国の監視機関によって、その権限の行使を求められることがあり、各監視機関の間では情報交換ならびに職務の遂行に必要な範囲での協力義務が課されています。

残念ながら、日本では、住基法や行政機関個人情報保護法いずれにおいても、このような権限を有する機関が存在していません。この一事をもってしても、ヨーロッパ委員会が日本を「十分なレベルの保護」を行っていない国であると評価

することは当然なのです。ＥＵ指令も８原則も、いずれも経済交易等の円滑化のために個人情報データの流通を促進することを前提に、データ処理における個人情報の保護を図るものです。それは、直接的に人権としての個人情報保護を打ち出すものではありませんが、データ処理に潜在する危険性が深刻に認識されているからこそ、監視機関にはこれだけの権限が付与されているわけです。繰り返しになりますが、ＥＵ指令が、住基法の憲法適合性に関する評価を左右する裁判規範性を有するわけではないとしても、愛媛県愛南町で発生した住基情報の流出のような事例を念頭におけば、住基法が定める制度の評価基準としては、重要な意義を有していると私は考えます。

８　本件訴訟では、控訴人杉並区が、被控訴人都に対し、住基ネットを通じて杉並区民の本人確認情報を送信するにあたって、通知を希望しない住民の本人確認情報については送信せず、通知希望者の本人確認情報のみを送信すること、それを被控訴人都が受信しないことが適法か否かが問われています。この点について、これまでに述べられたことを踏まえてのご見解をお聞かせ下さい。

質問事項８への回答は、これまで述べてきたことから自ずと明らかであると思います。情報の自己決定という観念は、仮に住基ネットがプライバシー権保障の観点からみて合理性を欠く制度であっても、それを利用する各人の自由を含みます。ですから、住基ネットに利便性を認め、それに参加する者の権利も保障する必要があります。他方、質問事項７で論じたように、制度にプライバシー権保障を期待できない現状がある場合、当該制度を利用しない自由が認められることが質問事項１以来論じてきた憲法上のプライバシー権保障の要請です。杉並区の対応は、こうした個々の住民の意思を尊重したものですから適法といえます。

そのような自由を認めれば、住基ネットと旧制度における事務等を並存させなければならず、事務作業の効率性に欠け、財政負担も生じて不合理であるとの

批判はあるでしょう。しかし、そのように効率性を追及するのであれば、第三者監視機関の設置等、容易に実現可能な制度を設けることで住基ネットの信頼性を高めればよいのです。また、地方自治体は住基法の定めに従う義務があるという反論もあるでしょうが、住基法といえども、憲法上のプライバシー権保障を無視することはできません。杉並区の行為は、区民の憲法上の権利を保障すべく、東京都に対し通知希望者の本人確認情報のみの受信を求めているわけですから、憲法に適合する適法なものです。

以　上