平成１９年（ネ）第5840号　損害賠償請求控訴事件

控 訴 人　小崎令子 外39名

被控訴人　西東京市

準 備 書 面（2）

平成２０年5月7日

東京高等裁判所　第14民事部　ロC係　御中

控訴人ら訴訟代理人

弁護士　清　水　勉

弁護士　増　田　利　昭

弁護士　鈴　木　雅　人

弁護士　佐　渡　島　啓

弁護士　冨　田　千　鶴

弁護士　関　口　正　人

弁護士　結　城　大　輔

第１　はじめに

１　共通している問題意識

被控訴人は，その主張の正当性を裏付ける書証として，控訴審において，東京高裁平成１９年１０月１７日判決（以下「東京高裁判決」という。）（乙３７）及び大阪高裁平成２０年２月２７日判決（以下「大阪高裁判決」という。）（乙４５）を提出した。

判決の主文が当該訴訟の原告ら（控訴人ら）の請求を棄却しているという点では，本件の被控訴人の求める内容になっている。しかし，その判決理由をみるならば，決して被控訴人の主張を全面的に採用しているわけではなく，むしろ，本人確認情報のプライバシーとしての保護の必要性や住基ネットのセキュリティ上の問題点などについては当該訴訟の原告ら（控訴人ら）の主張と共通する部分が多い。それが結論において原告ら（控訴人ら）の主張と異なる原因は，後に説明するとおり，いわば当てはめの段階での事実認識や評価の誤りということができるのである。

なお，東京高裁判決（乙３７）は，最高裁第一小法廷平成２０年３月６日判決（乙４０）によって維持されている。

２　争点のちがい

東京高裁判決及び大阪高裁判決では住基法改正により制度化された住基ネットに限定しての，プライバシー侵害性やセキュリティなどが争点となっていた。

これに対して，控訴人らが本件で問題にしていることは，国民総背番号制ともいうべき本人確認情報（とくに住民票コード）という制度が個人のプライバシー保護の観点からきわめて問題があるというものであって，住基法の改正によって作られた住基ネットの仕組み内のセキュリティだけを問題にしているのではない。既存住基システム内にある本人確認情報が不正に利用されることは，

住基ネット自体のセキュリティがいくら完璧だと言ってみても，被害者である住民にとっては何の救いにもならないのである。

したがって，本件で問題とすべきプライバシー保護は住基ネット内だけでなく，住基ネットと直結している既存住基システムについても同等に確保されなければならないのである。

以下，それぞれの判決について検討することにする。

第２　東京高裁判決（乙３７）について

１　東京高裁判決（乙３７）についての理解

⑴　被控訴人の主張

被控訴人は，東京高裁判決（乙３７）について，一審原告の上告および上告受理申立が棄却ないし不受理決定されたことをもって，控訴人らの主張が明らかに失当であるとする（答弁書５頁）。

そもそも東京高裁判決（乙３７）は，住民らの本人確認情報を住基ネットの磁気ディスクから削除せよという請求であることからも明らかなように（乙３７・１～２頁「当事者の求めた裁判」２⑷，３⑵），あくまでも住基ネットそのものを問題とする裁判である。これに対して，本件訴訟では，住民票コードを付番（既存住基）・通知（住基ネット）したことを違法行為としているものであり，住基ネットのプライバシー侵害性は住基ネットに直結している市町村の既存住基システムの安全性をも問題としているものである。その意味で，東京高裁判決（乙３７）は本件の事案にそのままあてはめられるものではない。

また，東京高裁判決（乙３７）は，およそ住基ネットという制度・仕組みにより住民の本人確認情報を管理，利用等することそのものが憲法１３条に違反しないと判断しているわけではない。当該事件の主張立証内容に基づいて事実認定（あてはめ）を行ったところ，憲法違反の事実が認定できなかっ

たとするだけにすぎない。したがって，東京高裁判決（乙３７）をもって，被控訴人らの主張が明らかに失当であるとすることはできない。以下，詳論する。

⑵　東京高裁判決（乙３７）の判断内容

ア　プライバシー性

東京高裁判決（乙３７）では，プライバシー性について，「他人に知られたくないと感じる個人の私生活上の情報（プライバシー）を自己の欲しない他者にみだりに開示され，利用されないという期待は，憲法１３条によって保障される人格権の一内容として，法的保護を受ける利益に当たるというべきである。」と判示している（乙３７・３０頁）。

このようなプライバシーについての理解を前提に，本人確認情報のプライバシー性について，次のように判断している。

① 氏名，出生の年月日，男女の別及び住所（４情報）は，個人の思想，信条など人格的自律に深く関わる情報などと比べると，秘匿されるべき必要性は必ずしも高くない。しかし，現在の社会情勢の変化及びそれを踏まえて国民意識の変化等に照らすと，このような情報であっても，自己が欲しない他者にこれを開示されたり，みだりに利用されたくないと考えるのは自然なことと考えられ，そのことへの期待は法的に保護されてしかるべきである。すなわち，４情報についても，プライバシー性を認めるものである。

② 変更情報は，転入，転出，氏名の変更等に係る情報であるから，これも，自己が欲しない他者には知られたくないと感じる私生活上の情報に含まれるとして，プライバシー性を認めている。

③ 住民票コードは，特定個人に付されたもので，特定個人と結びついて認識される（Ａという特定個人の住民票コード番号であるとい

う認識がされる）限りにおいて私生活上の事実ないし情報という面があることから，プライバシー性を認めている。

以上のような本人確認情報のプライバシー性についての東京高裁判決（乙３７）の理解は，決して，控訴人のこれまでの主張と異なるものではない。これに対して，被控訴人が「住民票コード自体は，無作為な１１桁の数字にすぎず，・・・(中略)・・・，住民票コードの流出が，直ちに住民らのプライバシーが侵害される現実的，具体的危険を生じさせるものではない。」〔答弁書８頁〕として，あたかも住民票コードはプライバシー情報ではないかの如き主張をしていることからすると，本人確認情報のプライバシー性に関する被控訴人の主張は東京高裁判決（乙３７）と異なっていることは明らかである。

イ　判断基準

東京高裁判決（乙３７）では，プライバシー侵害に基づく差止請求の判断に当たり，次のような判断基準を示している。

① 自分以外の第三者が自分の知られたくない私生活上の情報（プライバシー）を取得し，保有しているが，その情報を保有し，一定範囲でそれを利用すること自体をとらえて違法とはいえないような場合であっても，その情報の保有管理の仕方ないし仕組みからして，自分のプライバシーに係る情報が他者にみだりに開示される，あるいは当該情報が法で許容されないような形態でみだりに利用されるなどして，当該個人の私生活の平穏，人格的自律が脅かされ，重大な損害が生ずる現実的，具体的危険があると認められる場合には，その情報を保有するものに対して，人格権に基づき，そのような危険が生じないよう予防を請求することができるとする余地が生じる

と言うべきである（ただし，人格権に基づく妨害排除請求である以上，当該人格権の主体が，妨害予防を請求するに足るほど，プライバシー侵害の現実的，具体的な危険にさらされているといえることが前提となるものである)。（乙３７・３０頁２２行目～３１頁１２行目）

② ①のような危険が，住基ネットのような公的な制度によって生じるという場合には，当該制度の持つ公共性ないし公益上の必要性との対比において，それが受忍限度を超え，違法なものかどうかを更に検討する必要が生じる（乙３７・３１頁１２～１５行目)。

③ 本人確認情報が国民のプライバシーに属する情報という面があることから，その保管管理の制度的仕組みが適切さを欠き，制度的に個々の国民のプライバシーの侵害を引き起こす現実的，具体的危険が大きいとすると，これは，プライバシーに属する情報の保管管理についての国民の合理的な期待を裏切るものであって，そのような保管管理の仕組みを定めた制度（住基ネット）自体が，個々の国民のプライバシーを侵害の危険にさらすものとして，違憲違法と評価され，人格権に基づき，その侵害の予防を請求することができると解する余地が生じてくるといえる（なお，このように制度自体が違憲違法と評価される場合には，制度（住基ネット）の公共性，公益性との比較における受忍限度の検討は不要となると考えられる)。（乙３７・３５頁１６行目～３６頁４行目）

④ 住基ネットの制度それ自体が違憲違法とまではいえないとしても，その現実の運用状況からすると，控訴人らの本件確認情報が漏洩するなどしてそのプライバシー侵害が引き起こされる現実的，具体的危険があるという場合にも，侵害の予防を求めることができると解する余地が生じる。（乙３７・３６頁４～８行目）

上記②の基準は，住基ネットのように当該自治体の判断で参加が強制される制度においては，公的な制度であるというだけで，（プライバシー侵害の危険性があっても）住民に受忍を求めるということになりかねず，妥当性を欠いている。

もっとも，東京高裁判決は，②の基準によってあてはめを行っているものではなく，本人確認情報がプライバシー情報であることから，受忍限度の検討を不要とするとして，その後のあてはめは③，④の基準で行っている。したがって，そのような判断の仕方自体は，控訴人らの主張とも懸け離れているものではない。

⑶　東京高裁判決（乙３７）の事実認定の問題点

東京高裁判決（乙３７）は，住基ネットについて，（ｉ）本人確認情報の保管管理の制度的仕組みが適切さを欠き，制度的に個々の国民のプライバシーの侵害を引き起こす現実的，具体的危険が大きいか否か（制度面。上記③の基準），（ii）制度の現実の運用状況からして，本人確認情報が漏洩するなどしてそのプラバシー侵害が引き起こされる現実的，具体的危険があるかいなか（運用面。上記④の基準）の２つの側面から，事実認定を行っている。

ア　制度面の検討の問題点

まず，東京高裁判決（乙３７）の事実認定における根本的な問題は，「住基ネット」を，ＣＳ（市町村のＣＳと住基ネットのＣＳを含む。以下，同様），都道府県サーバ，全国サーバとそれらを繋ぐネットワークの仕組みの内側だけに限定し，ＣＳへの入口ともいえる市町村の既存住基システムやその他「住基ネット」外側の仕組み，人員等に関しては，あたかも「住基ネット」のセキュリティとは無関係であるとすることにある。確かに，本人確認情報が上記の「住基ネット」という制度・仕組みの内側（ここで言う「内側」は，上記のように，ＣＳ，都道府県サーバ，全国サーバとそれらを繋ぐネットワークの仕組みの内側という意味である。以下，同様）

だけで処理され，流通するものであって，外側に内側の情報を一切出さないような制度・仕組みであれば，東京高裁判決（乙３７）のような観点から事実認定を行うことも，人が関与することの問題性を除けば，あながち不合理とはいえない。しかし，本人確認情報は，そもそも「住基ネット」の外側（東京高裁判決の見方による。控訴人らとしては，外側とは認識していないし，そのような分類自体，責任逃れの弁解だと理解している。）である既存住基システムにおいて記録・作成され，ＣＳを通して，「住基ネット」に送信される。そして，「住基ネット」に接続している国の行政機関や都道府県，市町村により「住基ネット」を通して本人確認情報が照会され，流通・利用される。とすれば，「住基ネット」という制度・仕組みにおける本人確認情報の漏えい等の侵害の危険性の現実性，具体性の判断にあたっては，「住基ネット」の内側のみに着目し，内側から漏洩しなければ漏洩の危険がないとするのでは，当該危険性を「現実的，具体的」に検討したことにはならない。この意味で，東京高裁判決（乙３７）の事実認定は，制度面にしろ，運用面にしろ，制度・仕組みの現実に具体的に即して判断されたものとは言えず，プライバシー保護の観点から，極めて不十分である。

次に，制度面の現実的，具体的危険性の有無については，住基法等の法令の定めやセキュリティ基準，住基カードセキュリティ基準の規定を挙げて，「住基ネットの制度的仕組みが適切さを欠き，制度的に，控訴人らの本人確認情報が外部に漏えいする現実的，具体的危険があるとはいえないというべきである。また，制度的に，本人確認情報が法の許容する以外のことに利用されるなどして，個人の私生活の平穏や人格的自律を脅かす事態が引き起こされる現実的，具体的な危険があるともいえないというべきである」と結論づけている（乙３７・４８頁１１～１６頁）。しかし，その部分に引き続いて「従来，基本的には市町村だけが保有することにな

っていた本人確認情報が，住基ネットによりネットワーク上で共有されるという制度的仕組みが採られるようになったため，情報漏洩の危険性が高くなったということがいえないことはない」と指摘している（乙３７・１６～２０行目）。まさにこの点こそ市町村でいくらでも起こりうる問題なのである。にも関わらず，同判決では，「上記のように詳細にセキュリティ対策を施した制度的な仕組みからすると，制度上危険が増大したとはいえない」と結論づけてしまっており，問題に気づきながら「ない」ことにしてしまっている。これは明らかに矛盾している。ネットワーク上で共有するという制度的仕組みから情報漏洩の危険性が生じているということは，決して，一般的，抽象的な危険性ではなく，制度的仕組みそのものに内在しているという点で，つねに現実的，具体的な危険性である。

イ　運用面の問題点（その１）

まず，東京高裁判決は，「従来，基本的には市町村だけが保有することとなっていた本人確認情報が，住基ネットによりネットワーク上で共有されるという制度的仕組みが採られるようになったため，情報漏洩の危険性が高くなったということがいえないことはない」（乙３７・４８頁）とし，住基ネットの制度的仕組みそのものの問題点を指摘している。そして，市町村の現場における実際の運用の実態については，「もっとも，市町村の中には，上記のセキュリティ基準等を完全には遵守せず，未だ住基ネットの管理がずさんなところも相当数あることがうかがわれる（パスワードの管理が不十分，重要機能室への入退室管理が不十分，アクセスログの管理が不十分，あるいは，住基ネットとネットワーク接続されている庁内ＬＡＮからインターネット接続ができるにもかかわらず，庁内ＬＡＮの監視が不十分等）。」（乙３７・５３頁）と明確に指摘している。

また，東京高裁判決は，北海道斜里町，帯広市，福島県塙町での本人確認情報の流出事故について，「運用関係者の過誤又は故意による違法な

行為により，本人確認情報が外部に漏洩するということがこれまでにもいくつか生じたし，またこれからも生ずる可能性があることは否定できない」とする（乙３７・６５頁)。

さらに，社会保険庁において，住民票コードを閲覧できる端末が社会保険事務所等に設置されており，その数は全国で９４３１か所に上ること，社会保険庁の最適化計画実現後は端末の１人１台化が実現することになっており，将来の年金業務の業務系・支援系システムでは，被保険者・受給権者情報のなかに住民票コードも登録されることとされていること（乙３７・６２頁）をあげて，「それだけ職員等による不正閲覧等の危険が高まっているということもあながち否定できない」とする（乙３７・６５頁)。

以上のような東京高裁判決の運用面における問題点の指摘は，正にそのとおりであろう。本人確認情報を住基ネットというネットワーク上で共有することで，本人確認情報の情報漏洩の危険性が制度的に高くなっているにもかかわらず，実際の運用面においては，住基ネットの管理をセキュリティ基準に則って厳密に行っている市町村もあれば，そうでなく杜撰な管理しかしていない市町村もあるのであり，住基ネットそのものからの流出ではなくても，その周辺部分から本人確認情報が流出した事件が現に起きており，これからも生じる可能性があることは否定できないものであり，社会保険庁の現場の業務では容易に住民票コードが見られることから，職員等による不正閲覧等の危険性も高まっている状況にある。

そうであるならば，東京高裁が自ら立てた運用違憲の判断基準（上記③の基準。乙３７・３６頁４～８行目）に上記の認定事実を当てはめれば，住基ネットの現実の運用状況からして，本人確認情報が漏洩するなどしてそのプライバシー侵害が引き起こされる現実的，具体的危険があるということになるはずである。

ところが，東京高裁は，現実の運用に上記の指摘事実のような問題点

があるにもかかわらず，「多くの市町村では概ねセキュリティ基準が遵守されている状況にある」こと，北海道斜里町等の事故を契機として，総務省から「住基ネットのセキュリティに関する文書等を厳重に管理」すること等を「関係職員に周知徹底することが通知されている」（乙３７・６６頁）こと，社会保険庁等による不正閲覧については刑事罰が科されていることによって，プライバシー侵害の現実的，具体的危険がないとして（乙３７・６６頁），現実と正反対の結論に至ってしまっている。

これは極めておかしな結論である。「多くの市町村では概ねセキュリティ基準が遵守されている状況にある」という事実が厳密に確認できているわけではないし，「概ね」が具体的に何を指しているのか定かでないし，「遵守」が自己点検の結果とすればほとんど意味がない。その他の相当数の市町村では杜撰な管理しかしていないことは東京高裁自ら認定しているところである（乙３７・５３頁）。従来のような市町村毎に管理運営するシステムであれば，適正管理している市町村からは情報漏洩の危険性は少ないものであるし，そうでない市町村があっても，情報漏洩するのは基本的には当該市町村の住民や当該市町村と関わりのある範囲の者の情報に限られていたであろう。しかし，東京高裁が指摘しているように，問題は，住基ネットでは，ネットワーク上で本人確認情報を共有することにある。すなわち，ある市町村が鉄壁のセキュリティ管理をしていたとしても，住基ネットを通じて，当該市町村の住民の本人確認情報が，杜撰なセキュリティ管理の市町村や行政機関等に提供されれば，そこから情報漏洩してしまう危険性は格段に高いものとなるのである。したがって，「多くの市町村では概ねセキュリティ基準が遵守されている状況にある」ということは，裏返せば，（そして東京高裁自ら事実認定しているように）それ以外の市町村は杜撰な管理しかしていないということであるから，決して，情報漏洩の危険性が低いという結論にはならないものである。斜里町事故等

に関しては，総務省から通知したというだけであり，住基ネットのセキュリティ情報の管理が市町村の現場で周知徹底されたという認定にはならない。むしろ，東京高裁自身は，「運用関係者の過誤又は故意による違法な行為により，本人確認情報が外部に漏洩するということがこれまでにもいくつか生じたし，またこれからも生ずる可能性があることは否定できない」（乙６５頁）としているのであるから，当該通知だけで，将来についてはもちろんのこと，現在についても，情報漏洩が生じる可能性が何ら否定できるようになるわけがない。社会保険庁の不正閲覧については，そもそも社会保険庁の職員は公務員であるから，従来から刑罰をもって守秘義務を厳重に課していたはずである。にもかかわらず，不正閲覧はいとも簡単に生じたものであるし，それによって不正閲覧した職員が逮捕されたり，刑事裁判で実刑を受けたということもない。そのような現実からすれば，当の公務員らが，本人確認情報を不正に閲覧したくらいでは刑罰は受けないだろうと高をくくっていたとしても，何ら不思議はない。そうであれば，刑罰規定を設ければ，興味本位の，またはある特定の目的や意図による不正閲覧を抑止することができるなどとはとても期待できない。

いずれにしろ，東京高裁判決は，住基ネットにおけるプライバシー侵害による差止請求の可否に関する判断基準を正しく定立し，かつ，住基ネットにおけるプライバシー情報の直面している漏洩の危険性を十分に認識しながら，なぜか，プライバシー侵害の現実的，具体的危険がないと結論づけてしまっており，事実の当てはめ作業において重大な間違いを犯してしまっているものである。

ウ　運用面の問題点（その２）

東京高裁判決は，住基ネットの下では，住民票コードが付された本人確認情報を鍵（キー）として利用すれば，様々な箇所に保有されている個人情報を名寄せして結合して保管するということも技術的には容易にな

ったことを認識しながらも（乙３７・６７頁），法令の規定や刑罰，そして特定の行政機関によって住民個人のプライバシー情報が，本人確認情報を鍵（キー）にして集められ，結合されてデータベース化されるという危険が，現実的，具体的なものになったとまでは認められないとする（乙３７・６９頁）。

しかし，そもそも名寄せが技術的に容易になったということは，やろうと思えば容易にできるということに他ならない。これは名寄せの「現実的，具体的危険性」に他ならない。現に，東京高裁判決が事実認定しているように「出入国管理業務・システム最適化計画」や政府の諮問機関などで国民総背番号制についての議論がされ，税制調査会などで納税者番号への住民票コードの利用を検討していることからすれば，名寄せは現実に行われていないとしても，その危険性は現実的，具体的になっていることは明らかである。

また，東京高裁判決では，「特定の行政機関」による名寄せのみを問題としているようであるが，個人のプライバシー侵害という観点からすれば，「特定の行政機関」などによる組織的な名寄せだけではなく，個人レベルでの名寄せの問題には何ら言及しておらず，明らかに片手落ちである。組織的に大々的に名寄せを行おうとする場合は，法律との抵触や住民からの批判等にさらされることになるから，より慎重に進められることになろう。しかし，行政機関内部において，取扱業務を異にする者が２～３人の少数でも，示し合わせて協力すれば，特定の目的をもって，特定の個人に関する情報を，住民票コードを鍵（キー）として収集することは，住基ネット導入以前に比べて，はるかに容易になったものである。この点からしても，特定の行政機関が名寄せを現に行っていないから，名寄せの現実的，具体的危険性はないと結論づけることは間違いである。

２　費用対効果について

大阪高裁判決（乙４５）では，控訴人らの，住基ネット導入に伴う行政事務の効率化の程度がわずかなものであるのに対し，導入に伴うコストが膨大であって費用対効果の点において均衡を失っているという主張・立証に対しては，控訴人ら提出の証拠（鳥取県知事の記者会見内容，地方公共団体に対するアンケート結果と裁判所からの嘱託に対する回答等）では不十分であるとする。

しかし，平成２０年３月７日付けの新聞記事（甲９１）からも明らかなように，千葉県においては，平成１９年末で県内の住基カードの交付枚数は計１０万６０００枚で，交付率はわずかに１．７４％にとどまっている。交付率が県内最高の市川市ですら，交付率は６．１４％と１割にも満たない状況であり，続く浦安市が２．５９％，習志野市でも２．１１％に過ぎない。

このような住基カード交付率の低さは全国的なものであることからすれば，立法府・行政府の広範な裁量権を前提としても，裁量権を逸脱していると言えるほどに費用対効果のバランスを大きく欠いていることは明らかである。

第３　大阪高裁判決（乙４５）について

１　プライバシーと本人確認情報

⑴　プライバシー保護の必要性

大阪高裁判決は，以下にみるとおり，憲法１３条を根拠とするプライバシー権を認めていないものの，プライバシーの利益の保護の必要性については認めている。

すなわち，「プライバシー権という権利は，いまだこれが認められる外延も内包も不明確であり，不確定な要素が多く，その内容としての個人情報の保有及び収集等を制限するように求める権利を憲法１３条から直ちに認めることはできない」（４１頁）としつつも，続けて，「しかしながら，プライバシーの利益は法的保護に値するものということができるから，行政機関が，

正当な理由もないのに，個人の同意を得ないまま，その私生活上の事実又は情報を収集することは上記のプライバシーの利益を侵害するものとして，許されないというべきである。」（４１～４２頁）としている。

そして，さらに続けて，「近年，巨大データバンクやコンピュータなどの情報処理技術の発達に伴い，行政機関のみならず民間部門においても多量の個人情報が収集，蓄積，管理，利用，提供され，また，このようなデジタルデータは，半永久的に劣化しないで保存することができ，かつ，簡単に複製が可能であり，さらに，インターネット等を通じて，情報を瞬時かつ大量に流通させ，伝達することが可能になっている。」（４２頁）という実態を正確に直視した上で「このような状況下の現代社会においては，個人の私生活上の平穏，人格的自律を保障するためには，プライバシーの利益保護の一態様として，個人に関する情報につき，単に行政機関等により同意のないまま収集，利用されたり，そのような情報が他に提供されたりしないように保護される必要があるにとどまらず，侵害の程度，態様等によっては，個人情報が他に提供されることを差し止めたり，不当に蓄積，保存されている個人情報の抹消を求める権利も認められる場合がある」（同頁）として，現代のコンピュータ社会におけるプライバシー権保護の必要性を認めている。

⑵ 本人確認情報の要保護性

本人確認情報の要保護性については，基本４情報はいずれもそれ単独では秘匿性が認められない（あるいは秘匿性が低い）としつつも，「それらが統合されて存在する場合には，それぞれの情報が単独で存在する場合に比較して，当該個人の特定の精度が格段に高くなり，当該個人に関するその他の情報を集積するための鍵として利用されたり，当該個人をねらい打ちにして私生活の平穏が害されるような事態に至る可能性は高まるものといえる。」（４４頁）として，本人確認情報が個人特定の鍵として利用されることの問題性を的確に理解している。

⑶ 住民票コード

住民票コードについては，「重複のない１１桁のコードであって，全ての国民の住民票に対して個別に割り当てられて記載されている結果，当該住民票の対象とされている住民個人の氏名，住所，生年月日，性別を住基ネットのシステムを利用して取得するためのキーとなるだけでなく，当該住民個人を一意的に識別することが可能なコード番号として機能し得ることにもなる。また，住民票コードには表記のぶれや重複がない上，氏名，住所等の変更があっても住民票コードはそれに伴って変更されることがないため，その前後の同一性を確認することが可能であって，単なる個人識別情報を組み合わせたものと比較すれば，氏名や住所の表記のぶれに左右されず，また，同姓同名・同一生年月日・同性の者についても同一性を識別することが可能であるという点で，高い精度で個人のプライバシー情報の集積や統合，分析が可能となるという特徴を有する。」（４５頁）と，住民票コードの特性を的確に理解している。

⑷ 本人確認情報

本人確認情報に関しては次のように指摘している。

「情報処理技術の発達に伴い，行政機関のみならず民間部門においても多量の個人情報が収集，蓄積，管理，利用，提供され，また，このようなデジタルデータは，半永久的に劣化しないで保存することができ，かつ，簡単に複製が可能であり，さらに，インターネット等を通じて，情報を瞬時かつ大量に流通させ，伝達することが可能になっている状況にあること，そして，住民票コードが高度の個人識別機能を有することもすでに説示したところであり，そうすると住民票コードを主キーとして住民個々人に関する各種の情報が連結されて公権力による住民に対する情報管理がなされたり，上記のような情報の流通，伝達の危険性が現実化するおそれがないとはいい切れない。これらの点をふまえると，本人確認情報は，プライバシーの中核をなすとこ

ろの思想，信条，宗教等個人の自己同一性や人格的自律に関わる情報に関するものではないとはいえ，これに密接に関連するものとして，法的保護に値するものであるということができる。」（４６頁）としている。

そして，続けて差止請求権との関連ではあるが，次のように指摘している。「上記の正当な方法によって本人確認情報が収集，利用，提供されているか否かの判断に当たっては，本人確認情報が上記の危険性にさらされていないかに十分留意してこれを判断，検討しなければならない。すなわち，住基ネット規定の欠陥ないし不備故に，本人確認情報がプライバシーを暴いたり私生活の平穏を害する意図などの害意を有する者が容易に利用できる状態に置かれている場合や，個別に収集されたプライバシーに関する情報を相互に結合するために本人確認情報が公権力によって利用され，あるいはそのような目的の下に利用が容易な状態に置かれている場合には，当該個人のプライバシーの利益が現実に害され又は害される具体的な危険があるということができるから，たとい立法目的は正当であっても，立法目的達成の手段において合理性がないといえるもので，そのために，住基ネット規定そのものが，結果として，プライバシーの法的利益を侵害するものとして，その規定に基づく事務の処理に対する差止めが許されることがあり得るということができる。」（４６頁）

⑸　小括

このように大阪高裁判決は，本人確認情報についてプライバシー保護の必要性があることを認めている。その上で，差止が認められるべき制度的欠陥や実情が存在するか否かを検討することとしている。

２　収集目的の正当性と方法の正当性

⑴　目的の正当性

本人確認情報を前記のように位置づける以上，裁判所としては，当然，本

人確認情報ないし住基ネットの目的の正当性について，慎重に検討すべきである。

ところが，大阪高裁判決は，昭和４２年に住民基本台帳制度が始まったこと（４７～４８頁），その後，民間部門と並行して，「行政部門においても，住民サービスの向上や行政事務の効率化のために，情報通信技術を有効に活用する必要性に迫られていた。」と抽象的に述べ（４８頁），住基ネットができたことを説明し（４８～４９頁），「その結果」として，「これまではそれぞれの事務ごとに住民に義務づけられていた，申請，届出，住民票の写しの添付等の住民側の負担が解消される一方，行政側においても，事務の効率や事務処理の正確性が向上しており」（４９頁）という事実を認定し，「今後も，各種の事務につき，上記のような住基ネットの効用の拡大が期待されている。」（同頁）と抱負を述べている。そして，「以上のように，住基ネットは，高度に情報化された現代社会において，社会からの要請に基づき，・・・導入されたものであり，・・・立法目的は・・・正当なものであると認められる。」（同頁）とまとめている。

しかし，「社会からの要請」などという抽象的な「要請」で個人のプライバシーが制約されてよいはずがない。それまでの住民のどのような負担がどのように解消されたのか，また行政のどのような事務がどの程度効率化され，事務処理の正確性がどれほど上がるのか，具体的な検討を全くしていない。

上記のプライバシーと本人確認情報との関係について緻密に検討し判示した部分と比べると，まるで別人が書いたのではないかと思われるほど，緻密な検討を一切しない，一面的な積極的評価（どんな悪い制度であっても探せばどこかにメリットと言える部分はある。）になってしまっている。住民がほとんど負担に感じていない手間（１年間に１度も住民票の取得を必要としない人達が無数にいる。）や手数料（数百円）を「解消」したところで，住民は負担から解放されたという実感を抱かない。行政側においても，局所

的にみれば，「事務の効率や事務処理の正確性が向上」したとしても，限られた人材・予算の中で投入しなければならない人的・時間的・経済的負担増を併せて考えれば，積極的評価は簡単にはできないはずである。

控訴人らが原告準備書面(13)３頁や控訴理由書２３頁以下などで繰り返し主張しているとおり，改正住基法の目的には重大な疑義があるのであるから，この点は慎重な判断が必要である。

⑵　方法の正当性

大阪高裁判決は，目的の正当性について具体的な検討をまったくしないで認めてしまっているので，必然的に，方法の正当性は認められることになる。

方法の正当性を考えるとき，費用対効果の観点は欠かせない。なぜなら，住基ネットは市町村の自治事務として運用されている制度であるから，事務効率にあまりないしほとんど役立たないならば高額の予算を組むことができない。費用対効果の原則からして当然である。各市町村が住基ネットにどれだけの人材と公費をかけることができるかが，本人確認情報流出防止に直結しているのである。

この点に関して，大阪高裁判決は，当該原告ら（控訴人ら）の提出した書証が当該被告ら（被控訴人ら）に関するものではなかったことから，他の自治体に関する実情をいくら示したところで，「控訴人らの上記主張」（「住基ネット導入に伴う行政事務の効率化の程度がわずかなものであるのに対し，導入に伴うコストが膨大であって費用対効果の点において均衡を失している」）「が証明されたものとはいい難い」（５０頁）と認定している。しかし，この点はむしろ住基ネットを管理運用している自治体の側から積極的に主張立証すべきであり，これをしていない以上，費用対効果については主張立証がないとみるべきである。

大阪高裁判決は，続けて，「立法政策又は行政上の施策の当否の問題として，立法府又は行政府が広範な裁量権を有する事項である」（５０頁）と述

べるが，費用対効果は単純な効率性の問題ではない。自治体がどこまで本人確認情報に手間隙をかけられるかという，本人確認情報の現実的な保護のあり方に直結する問題であるから，立法府等の広範な裁量権を有する事項として判断放棄をしてしまってよいことではない。

３　住基ネットのセキュリティについて

⑴　侵入実験

大阪高裁判決は，長野県内の３町村で行われた侵入実験と，ほぼ同時期に都内品川区で行われた侵入実験について検討しているが，これらはいずれも事前に住基ネットの管理者に告知して行われたものであるから，管理者としては侵入実験開始前に急遽万全の態勢を組むことができる条件下にあった。とくに当時はたまたまブラスターが世界的に猛威を振るった直後ということでコンピュータネットワークのセキュリティに対する関心が急速に高まった時期であるから，この時期のこのような侵入実験をもって住基ネットのセキュリティが確保されているという結論を導くのは誤りである。

そもそも侵入実験は安心するために行うものではなく，脆弱性を探し出しその対策を講じることを目的とするものである。長野県内の３町村の侵入実験にしても品川区の侵入実験にしてもその結果を安心材料として読むことが誤りである。

長野県内の３町村の侵入実験で明らかになった共通の脆弱性は，被控訴人が言うところの「住基ネット外」の庁内ＬＡＮである。既存住基の管理は住基ネットと無関係だと考えるのであれば，住基ネットの脆弱性ではないとして放置しておけばよい。しかし，既存住基内で管理されている本人確認情報は，住基ネットＣＳ内で管理されている本人確認情報と同等に保護されるべきだと考えるのであれば，重要な指摘であり，改善されなければならない。

品川区の侵入実験については，長野県の３町村の場合と異なり，報告書（甲

９２）をみても，侵入実験の手法や過程，その結果の詳細が明らかにされていないから，およそ必要十分なものだったかどうかの判断はできない。すなわち，公表されている実験の概要としては「(財) 地方自治情報センター（実際にはクロウ社)」が「平成１５年１０月１０日，１１日，１２日」に「品川区の協力を得て」，①「住基ネットーＣＳ間のファイアーウォール」，②「ＣＳー庁内ＬＡＮ間のファイアーウォール」，③「庁内ＬＡＮ上のＣＳ端末」に対する「ペネトレーションテストを実施した」ことだけであるし，その結果も，①については「ＣＳセグメントから３時間」「ファイアーウォール攻略のあらゆる手段を試みたが，成功しなかった，脆弱性も見いだせなかった」，②については「庁内ＬＡＮセグメントから６時間」「ファイアーウォール攻略のあらゆる手段を試みたが，成功しなかった。脆弱性も見いだせなかった。」，③については「庁内ＬＡＮセグメントから６時間」「ＣＳ端末の権限奪取のためあらゆる攻撃を行ったが，成功しなかった。不正侵入を許すような弱点も見いだせなかった」（甲９２）というに過ぎない。長野県の実験の報告と比較しても，品川区の実験内容がいかに明らかにされていないかは明らかで，この結果報告だけの安全性が確認などできない。

なお，クロウ社も「住基ネットの範囲内ではないが，庁内ＬＡＮに対してもチェックリストによる自己点検やセキュリティ監査を行うべきである」と助言している。これは，本人確認情報が漏洩する危険性を住基ネットシステムに限定せず，既存住基からの漏えいも危惧する控訴人らの立場と共通している。

⑵ チェックリストによる自己点検

チェックリストによる自己点検については，自分で点検するという点で果たして正直に行われているかどうかが第三者にはわからないし，自己点検する当該職員の専門性もまったく保障されていない。例えば，本人確認情報が漏洩した愛南町の自己点検結果はどうであったのか。西東京市のチェックリ

ストの結果がどのようなもので，それが客観的にも正しいかどうかは，全く不明である。

⑶　情報漏えいの危険性の程度（５６頁）

大阪高裁判決が，「a　セキュリティの評価について」（５６頁）で述べている考え方は，１つの自治体内で完結しているコンピュータネットワークについてのものとしてであれば，このように言えないことはない。しかし，１つの自治体内で完結していない他の都道府県や市町村と直結しているコンピュータネットワークでは１自治体だけのセキュリティについて「十分高度なもの」と評価できたとしてもほとんど意味がない。すべての自治体が「十分高度なもの」になっている必要がある。

大阪高裁判決は，①「庁内ＬＡＮの既存住基サーバの管理者権限を奪取するとともに，庁内ＬＡＮとＣＳセグメントとを仕切るＦＷを無効化するなどの手順を踏むことによって，正規のユーザがＣＳクライアントにおいて実行できるデータの検索などの操作が可能となる」，②「物理的にＣＳセグメントに接続可能であるならば，容易にＣＳセグメントに攻撃用端末を接続して，ＣＳの管理者権限を奪取することが可能」と認めるものの，①については上記品川区の実験から「一応適切な設定が行われ，安全性が検証されている」とし，②については「ＣＳセグメントを構成する部分の大半は施錠された重要機能室内に存していて，部外者が物理的に接続することは極めて困難」などとして現実の危険性は否定する。

しかし，①品川区の実験だけで安全性が検証されたということなど出来ないことは上記の通りであるし，②「大半」と大阪高裁が述べている時点で，危険性の高い自治体があることを物語っているし，少なくとも全ての自治体で現実の危険性がないとは言えない。

何より，この大阪高裁判決の原告住民らはあくまで住基ネットからの情報漏えいを問題としていたが，本件の控訴人らは，既存住基等も含めて本人確

認情報の漏えいの危険性を争っているのであって，この大阪高裁判決の認定を援用するだけでセキュリティに関する被控訴人らの反論が足りていることにはならない。この点に関して大阪高裁判決が「いまだ控訴人らの情報が住基ネットを通じて漏洩するという具体的で現実的な危険性を裏付けるものではない」（６３頁）と限定を付しているのも，既存住基を除いて考えていることがはっきり読み取れる。

また，大阪高裁は，セキュリティパッチの運用が適切に行われていないとまでは認めることは出来ないというが，ブラスター問題では，１ヶ月前にウィンドウズ社から配布されていたセキュリティパッチを多くの自治体が適用せず，それによってブラスターウィルスに感染してしまったことが明らかになっている。

大阪高裁判決は，地方自治情報センターが阿智村においてケーブルが５回抜き差しされたことを検知し，直ちに総務省に報告したことなどを挙げて，「指定情報処理機関監視ＦＷを攻撃して無効化し，他の市町村のＣＳサーバや庁内ＬＡＮなどへ侵入することは，現実的にはほとんど考えられない。」（５９頁）としているが，同判決によれば，地方自治情報センターは１回の抜き差しには何の反応もせず，午後１０時０４分５５秒から午後１０時３４分２０秒までの約３０分間もの間，何もしないでいたということである。約３０分間という時間があれば不正侵入をしようとすればできたかもしれないと考えるのがセキュリティに真摯に取り組む姿勢である。大阪高裁判決の判断は却ってセキュリティへの取り組みをルーズにさせる危険がある。

４　法的保護措置（６０頁）

⑴　ＯＥＣＤ８原則との関係

大阪高裁判決は，「法は，・・・いわゆるＯＥＣＤ８原則を踏まえたと思われる多角的な保護措置を講じている。」（６０頁）と述べているが，これでは

住基ネットの根拠法ともいうべき改正住基法が成立した平成１１年８月当時の国際基準からすると，個人データ保護として不十分なのである。

１９９５年（平成７年）１０月，ＥＵでは，「個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令」が出され，その２５条では，加盟国は，個人データの第三国への移転は，当該第三国が十分なレベルの保護措置を確保している場合に限って行うことができると規定している。ここにいう「保護措置」とは第三者による監視機関である。この要請を充たしているかどうかこそがＥＵ指令に応じているかどうかの判断基準となる。

⑵　住基法による保護措置について

大阪高裁判決は，本人確認情報の利用及び提供先の制限等，役職員等に知亜汁秘密保持義務等，安全確保義務，監督命令等並びに報告及び立入検査，自己の本人確認情報の開示・訂正等の制度があることを挙げて，「住基ネットの運用によって個人のプライバシーの利益に対する侵害の現実の危険が存するものと認めることはできない。」（６３頁）としている。

そして，続けて，「斜里町等事件は，住基ネットからデータが漏洩するような抽象的危険性があることを裏付けるものにとどまり，いまだ控訴人らの情報が住基ネットを通じて漏洩するという具体的で現実的な危険性を裏付けるものではないと認められる。」（６３頁）とし，住基ネットから漏洩するのでないかぎり問題はないという考え方に立っている。そして，斜里町事件も帯広市事件も塙町事件も愛南町事件も「住基ネット自体から情報が漏洩した事件ではなく・・・いまだ控訴人らの情報が住基ネットを通じて漏洩するという具体的で現実的な危険性を裏付けるものではない。」（同頁）と結論づけている。

このような説明が，本人確認情報が不正利用されることを危惧する住民に対して説得力を持つはずがない。

５　行政機関等によるプライバシー情報統合の具体的危険性（６４頁）

⑴　個人データの連結の危険性

大阪高裁判決は，住民票コードによる個人データの連結の危険性を指摘している。

「住民票コードが種々の行政目的に利用されるに際しては，当該行政目的に関して，当該個人が行政機関に申告した情報や，当該個人と行政機関との相互関係に関する履歴，行政機関が独自に収集した情報などが結び付けて保存されることが考えられる。」（６４頁）とした上で，「このようにして収集，集積された当該個人に関する情報が，住民票コードを主キーとして連結されれば，当該個人の社会生活全般にわたる情報となり，思想や良心などの内心を推知することが可能となる事態にも至りかねず，公権力主体による国民の管理統制につながる危険性を有するものであることは否定できない。」（同頁）としている。

そして，続けて，「このように，行政機関等により，住民票コードが個別に集積されたプライバシーに関する情報を結合するために利用され，あるいはそのような利用が容易な状態に置かれている場合には，当該個人のプライバシーの利益が害される危険性があるものということができるのであって，かような場合には，住基ネット規定は，立法目的を達成する手段としての合理性がないし正当性を欠く疑いがあるものといえる。」（同頁）としている。

このような考え方は，控訴人らの考え方に共通するものがある。

⑵　データマッチングについて

ところが，大阪高裁判決は，本人確認情報に関する守秘義務やその違反に対する刑罰などの規定があることを挙げて，「住民票コードを利用して国民のプライバシー情報を集約することによって，プライバシーの利益が現実に侵害され，あるいは侵害が生じる危険が現実化しているとはいえない」（６６頁）と結論付けている。

しかし，このような理由については，控訴人が準備書面(6)２１頁以下，同(7)８頁以下などで繰り返し述べたように，実効性に乏しいと言わざるを得ない。

また，大阪高裁判決は，「住民票コードを使用したデータマッチングは，住基ネットに関与する都道府県知事，国の機関あるいはその職員がこれらの法律の定めを遵守する限りは実現しないものであり，これらのものが法律の定めに違反する行為を組織的にすることを前提として，データマッチングの現実的危険があるとすることは当を得ない」（６６頁）という。

しかし，この点については東京高裁判決での検討のとおり，行政機関内部において，取扱い業務を異にする者が数名の少数でも示し合わせて協力すれば，特定の個人に関する情報を住民票コードを鍵として収集することが極めて容易にできるようになったことは疑いの余地がない。不正利用される個人の側からすれば，不正行為を行う者が行政組織かどうかはどうでもよいことである。「組織的」なデータマッチングしか問題にしないという大阪高裁判決の姿勢こそが問題である。

また，大阪高裁判決は「将来，住基ネットにおける本人確認情報の提供先，利用目的の拡大等がなされるとしてもそれは法律の改正によるものであって，主権者たる国民の意思を離れて無制限に拡大するものではないから，本人確認情報の提供先，利用目的の変更等があり得ることは，控訴人らが主張するところの住民票コードを使用したデータマッチングによるプライバシーの利益の侵害を理由づけるものとなり得ない」（同頁）ともいう。

しかし，これは抽象的な法律論（理屈）であって，現実的なデータマッチングの危険を回避する手段としては実効性を持たない。本人確認情報を利用できる国の行政事務がわずかな数から２６４事務に拡大した法改正のときに一体幾人の国民がこの改正内容を事前に知っていたか。国会議員でさえもがほとんど知らなかった内容である。住基法の本人確認情報についていえば，

国民は，自分の情報がどこに提供されているのか，住基ネット稼働当初から現在までどの程度の提供先が増加したのか，大凡でも認識しているとはおよそ思われない。国民のプライバシー侵害が具体的に問題となっている場面で，このような空虚な議論で現実から逃避することは許されない。

第４　その他の乙号証について

１　乙第４１号証ないし第４４号証の意味

被控訴人は，自らの主張を裏付ける書証として前記東京高裁判決，大阪高裁判決以外に乙第４１号証ないし第４４号証を提出しているが，これらは，都道府県，市町村の情報セキュリティが運用のみならず，運用の前提となる条例や契約条項が，これまで不十分であったことを認めているものである。しかも，これらの通知等によって問題がすべて解決するわけでもない。

被控訴人も，当然，このようなことを自覚しているはずである。

２　各乙号証について

⑴　乙第４１号証

平成 19 年 5 月 25 日付け文書『外部委託に伴う個人情報漏えい防止対策の徹底について』は，総務省大臣官房総括審議官から，都道府県知事（個人情報保護対策担当課・市区町村担当課扱い），指定都市市長（個人情報保護対策担当課扱い）あてに発せられた，情報セキュリティに関する措置を求めたものである。住基ネット内の本人確認情報を守るだけでは本人確認情報（既存住基内にある）を守ることはできないということをはっきり意識した通知である。

総務省がこのような考え方に立脚している以上，被控訴人も同様の問題意識に立っているはずである。それはまさに控訴人らの問題意識と同じである。

ただ，最高裁判決の考え方からすれば住基ネットには関係ない指摘である。

⑵　乙第４２号証

平成 19 年 5 月 25 日付け文書『個人情報の取扱いに係る外部委託契約の内容及び遵守状況の緊急点検について（依頼)』は，総務省自治行政局地域情報政策室長から，各都道府県情報セキュリティ対策担当部長，各都道府県市区町村行政担当部長あてに発せられた，情報セキュリティに関する自己点検を求めたものである。

そこで問題にされていることは，①業務の委託先事業者による無断での再委託，②従業員によるデータの無断持ち出し，③委託業務終了後のデータの返還・廃棄の不徹底である。これも住基ネット内のセキュリティの問題ではない。

乙第４２号証の自己点検の結果がどうなったかを明らかにされたい。

最高裁判決の考え方からすれば，これも住基ネットには関係のない要求だということになる。

⑶　乙第４３号証

平成 19 年 5 月 25 日付け文書『住民基本台帳における個人情報保護の対策について』は，総務省自治行政局市町村課長から，各都道府県住民基本台帳担当部長あてに発せられた，情報セキュリティに関する措置を求めたものである。

総務省は，住基法３６条の２を引用して，「住民票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」ことを強調している。

総務省は「自己の住民票コードについては，住民基本台帳法第３０条の３に基づき，何人でも記載の変更を請求することができるところであり，当該制度について住民へ周知徹底を図られたいこと。」としているが，これが他人による住民票コードの不正利用を考慮したものであることは明らかであ

り，住民への周知徹底を求めているのは法の規定が本人からの変更請求がないかぎり住民票コードを変更できないという制度上の欠陥があるからである。

末尾のまとめとして，「今回の事案は，各市区町村が個別に整備したシステムから個人情報が流出したものであり，住民基本台帳ネットワークシステム自体からの個人情報の流出ではないが，・・・住民基本台帳ネットワークシステムにおける個人情報保護についても，重ねて万全を期するよう対応されたいこと。」「なお，都道府県においても，市区町村同様，住民基本台帳ネットワークシステムにおける個人情報保護について，万全を期するよう対応されたいこと。」と明記している。

この通知では冒頭の文章中に「各市区町村においては，個人情報保護に万全を期する必要があるため」と書いているように，住基ネット内のセキュリティだけを強調しても実務的には意味がないことを十分に自覚している。

⑷ 乙第４４号証

平成 19 年 6 月 1 日付け文書『外部委託に伴う個人情報情報漏えい防止対策に関する対応及び留意事項』は，総務省自治行政局地域情報政策室長から，各都道府県情報セキュリティ対策担当部長，各都道府県市区町村行政担当部長あてに発せられた，情報セキュリティに関する措置を求めたものである。

この通知によると，総務省はこれまでもガイドライン等で対策をお願いしてきたが，それでも全住民の個人情報が漏えいするという事件が起こってしまったという現実を認めている。当該自治体でも当然，委託契約上は再委託禁止等の規定を設けていたはずであるのに，無断再委託先での漏えいという事態を招いたのであり，ガイドライン等を設けただけでは実効性を確保できないことが明らかになった。

だからこそ，総務省は「今回の事案を踏まえて」，「外部委託に伴う個人情

報の漏えい防止対策として必要と考えられる対応及び留意事項を別添のとおり取りまとめましたので，各地方公共団体におかれましては，・・・お願いします。」と言わざるを得なかったのである。

個人情報の外部への漏えい事案の多くは委託先からのものである。なぜ自治体は外部委託するのか。専門職員がいないこと，専門職員を雇うだけの財政上の余裕がないことが原因である。このような事態はほとんどの自治体で今後も変わらない。外部委託対策は必要不可欠である。

最高裁判決は，住基法の規定などを根拠に「十分」としているが，総務省の調査（乙４４添付）によれば，平成 18 年 4 月 1 日現在の時点で，個人情報保護条例に委託業者等の責務規定を設けていない自治体が 8.6%ある。個人情報保護条例に契約等によるデータ保護の確保措置を設けていない自治体が 23.1%ある。このような実情を踏まえて，総務省では，「個人情報保護条例にこれらの規定を設けていない地方公共団体においては，早急に規定を設けることが望まれる。」として，ネットワーク全体としてのセキュリティに問題があることを自覚して，改善を求めている。

また，総務省は，外部委託に関する留意事項で，「外部委託に際して取るべき情報セキュリティ対策は，取り扱う情報の重要性とリスクの大きさを勘案して適切な水準のものとする必要がある」としている。最高裁は，被控訴人の主張を採用して，本人確認情報はプライバシー情報としてさほど重要なものではないと評価しているが，総務省は「厳格な情報セキュリティ対策を講じる必要がある。」としており，被控訴人と見解を異にしている。

以上