平成１８年（行コ）第１１９号　住基ネット受信義務確認等控訴事件

控　訴　人　　杉　並　区

被控訴人　　東　京　都　外１名

準備書面（４）

平成１９年７月２７日

東京高等裁判所第１０民事部　御中

控訴人訴訟代理人

弁護士　吉　川　基　道

同　藤　田　康　幸

同　市　川　和　明

控訴人は，以下のとおり，被控訴人ら準備書面（３）に対し，必要と認める範囲で反論し，併せて，従前の主張を補充する。

第１章　プライバシー権（自己情報コントロール権）と本人確認情報について

第１　プライバシー（自己情報コントロール権）の権利性について

１　被控訴人の主張（被控訴人準備書面（３）１０頁以下）は，要するに，第１に，自己情報コントロール権には実定法上の明確な根拠がないこと，第２に，自己情報コントロール権の内容や外延が不明確であることからして，大阪高裁判決が不当であるとするものである（なお，「差止請求権の根拠たり得る実体法上の権利」という記述になっているが，本件においては，「差止請求権の根拠たり得る」か否かは直接的な問題ではない。また，「実体法」は「手続法」に対する概念であろうから，「実体法」とあるのは「実定法」の意味と思われる。）。

２　しかし，そもそも，そのような非難は，プライバシー権についても該当しそうである。プライバシーを保護することを明示した実定法は存在しないし，プライバシー権の内容や外延も実は必ずしも明確とは言い難い。

例えば，被控訴人が引用している杉原則彦最高裁調査官の解説（『最高裁判所判例解説民事篇　平成１５年度（下）（７月～１２月分）』）（以下，「杉原解説」という。）においても，「プライバシーとして保護される対象や，いかなる侵害が違法になるかといった点については，なお検討を要する点が多い。」「プライバシー侵害として論じられる事案は，その保護利益の性質も侵害行為の態様も多種多様である。」（４８５頁）としているとおりである。

それにもかかわらず，多くの下級審裁判例が具体的事案においてプライバシー権を保護し，最高裁判例も，最高裁平成７年９月５日判決（裁判集民事１７６号５６３頁），最高裁平成７年１２月１５日判決（刑集４９巻１０号８４２頁），最高裁平成１４年９月２４日判決（裁判集民事２０７号２４３頁），最

高裁平成１５年３月１４日判決（民集５７巻３号２２９頁），最高裁平成１５年９月１２日判決（民集５７巻８号９７３頁）（以下，「江沢民主席講演会事件上告審判決」という。）においてプライバシーが法的に保護されることを認めているのである。

被控訴人の主張は，権利ないし法的に保護される利益について，その名称が法文に記載されていなければ一切保護されないとし，また，権利ないし法的に保護される利益が予め一義的に明確に決まっていない限り保護されないとして，具体的な事案の積み重ねによる判例の形成を否定するものであり，度が過ぎた法実証主義的思想と言わざるをえない。

3　また，被控訴人の主張は，プライバシー権と自己情報コントロール権を全く別個のものと理解しているように見えるが，プライバシーと総称されるものの中で，情報化社会においては自己情報をコントロールする法的利益の重要性が高まってきたことを踏まえて，その法的利益が自己情報コントロール権と呼ばれているというのが実際である。

このことは，被控訴人が引用する杉原解説においても，多数の下級審裁判例を紹介した後で，「これらの裁判例をみると，プライバシーの権利の概念については，「私生活をみだりに公開されない権利」だけではなく，「自己情報コントロール権」に近い内容のものも加わってきているといえよう。この背景には，プライバシーの権利の侵害について，夫婦生活とか異性関係等のセンシティブな情報だけでなく，電話番号等の私生活上の情報が問題となる事案も出てきたこと，また，プライバシーの権利の侵害行為についても，表現行為だけでなく，第三者が保有する情報の提供が問題となり始めたことを指摘することができよう。」（４８６頁）としているとおりである。

この点については，２００７年５月１８日付中島徹教授の鑑定意見書（甲８４）が，「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」（５頁）と説明しているように，もともとプライバシーの中に含まれていた情報の自己決定権が高度情報化社会の中でより強く意識され問題となるようになったというのが正しい理解である。

4　また，杉原解説は，「プライバシーの保護によって守られるべき法的利益は私生活の平穏であるから，損害賠償の対象となるのは，私生活上の不安，嫌悪感，不快感といった精神被害である。また，前述のとおり，自己に関する情報を管理する権利こそが被侵害（要保護）利益と考えられるべきであるという見解も有力になってきている。そうすると，プライバシーの権利とは，「私的領域への介入を拒絶し，自己に関する情報を自ら管理する権利」ということになる。高度情報化社会では，様々な情報へのアクセスが容易になったことによって．一度漏えいした私的情報は直ちに他者からのアクセスにもさらされることになる。そこで，ある情報漏えいが直ちに私生活の平穏を具体的に害するものでないとしても，情報の漏えいは意に反する他者への公開の危険（私生活の平穏を侵害する抽象的危険）を包含することになる。自己に関する情報を管理する権利は，必ずしも内容の明確な権利とはいい難いが，このような社会背景を前提に理解されるべきものであろう。本判決が情報の開示について本人の「同意」を重要な要件としているのも，このような自己に関する情報を管理する権利の考え方と親和的なものとみることができよう。」（４８８頁）としており，最高裁調査官によっても，江沢民主席講演会事件上告審判決は自己情報コントロール権の考え方と親和的な判示をしているとされているのである。

5　被控訴人は，行政機関個人情報保護法に自己情報コントロール権が明記されていないことを論拠として主張しているところ，自己情報コントロール権が明記されていないこと自体は事実であるとしても，そのことゆえに自己情報コントロール権と内容を同じくするものが行政機関個人情報保護法に含まれていないと解釈すべきであると主張しているとすれば，論理の飛躍にほかならない。

つまり，被控訴人は，衆議院会議録を引用し，「法案に明記することは適切ではないとの答弁がされた」と主張しているが，自己情報コントロール権という用語が法案に明記されなかったとしても，憲法及び他の法令を含め総合的に解釈されて，具体的事案において自己情報をコントロールする法的利益を裁判所が認めることが妨げられるわけではない。

また，被控訴人は，総務省行政管理局監修『行政機関等個人情報保護法の解説』を引用しているところ，同書の第１条についての解説末尾の「参考」においては，同「法は『プライバシー権』や『自己情報コントロール権』という文言を用いず，あくまで個人情報の取扱いに伴い生ずるおそれのある個人の人格的，財産的な権利利益に対する侵害を未然に防止することを目的として，個人情報の取扱いに関する規律と本人関与の仕組みを具体的に規定するものである」（９～１０頁）としているにとどまる。

すなわち，「自己情報コントロール権」という文言を用いなかったことが，「自己情報コントロール権」を保障してはいけないという趣旨を含むとは言えないし，「個人情報の取扱いに伴い生ずるおそれのある個人の人格的，財産的な権利利益に対する侵害を未然に防止することを目的として，個人情報の取扱いに関する規律と本人関与の仕組みを具体的に規定する」ことは，一定の場合に自己情報をコントロールする必要性と正当性を認めているからこそである。なお，被控訴人も「行政機関個人情報保護法は，開示請求権，訂正請求権及び利用停止請求権を明文で定めており（同法１２条，２７条及び３６条），これらの権利は，その内容において，大阪高裁判決の判示する自己情報コントロー

ル権と共通するものを含んでいる。」としているように，行政機関個人情報保護法の規定する内容は自己情報コントロール権の内容と極めて親和的である。

ところで，上記解説は，プライバシー権も自己情報コントロール権も共に，一義的に明確でないとして，それらの文言を用いなかったとしているのであるが，裁判例の積み重ねにより認められてきたプライバシー権の裁判的保護を否定する趣旨でないことは明らかであろう。

6　住基ネットに関する裁判例では，大阪高裁判決以外にも，以下に述べるとおり，多くの裁判例が明示的又は実質的に自己情報コントロール権の保障を認めており，この点につき判例は確立していると言ってよい。なお，以下のうち「◎」印のものは明示的に認めているもの，「○」印のものは実質的に認めているものである。

◎　金沢地裁平成１７年５月３０日判決（判時１９３４号３頁，判タ１１９９号８７頁，http://www.courts.go.jp/）

「このような社会状況に鑑みれば，私生活の平穏や個人の人格的自律を守るためには，もはや，プライバシーの権利を，私事の公開や私生活への侵入を拒絶する権利と捉えるだけでは充分でなく，自己に関する情報の他者への開示の可否及び利用，提供の可否を自分で決める権利，すなわち自己情報をコントロールする権利を認める必要があり，プライバシーの権利には，この自己情報コントロール権が重要な一内容として含まれると解するべきである。」（判時１９３４号２３頁第２段）

○　名古屋地裁平成１７年５月３１日判決（乙１６）（判時１９３４号３頁，判タ１１９４号１０８頁，http://www.courts.go.jp/）

「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，本人確認情報や氏名の読み方等についても，これをみだりに収集，開示されたくないと考えることは自然なことであり，そのことへの期待は保護されるべきであるから，これをみだりに収集，開示されないという限度で

の法的利益は認められる。」（２１頁，判時１９３４号３９頁第４段）

○　福岡地裁平成１７年１０月１４日判決（乙１７）（判時１９１６号９１頁）

「自己情報コントロール権と称する権利が憲法１３条によって保障されるプライバシー権の一内容であるか否かは別としても，本人確認情報は，これをみだりに収集，開示されたくないと考えるのは自然なことであり，そのことへの期待は保護されるべきであるから，これをみだりに収集，開示されないという限度での人格的利益は認められる。」（２４頁，判時１９１６号９９頁第１段）

◎　大阪地裁平成１８年２月９日判決（判時１９５２号１２７頁，判タ１２０７号９１頁，http://www.courts.go.jp/）

「現代の情報社会において，個人の私生活上の自由や人格的自律を保障するためには，個人に関する情報について，行政機関等から不当に収集されたり，利用されたり，他に提供されたりしないように保護することにとどまらず，行政機関等が不当に個人情報を保有，利用しているような場合には，その情報が他の行政機関等へ提供されることを差し止めたり，その情報の抹消を求めたりする権利も保障される必要がある。」「保護の対象として中心となるのは，人格の生存や発展に不可欠な情報であり，それに直接かかわらない，外的事項に関する個人情報については，行政機関等が正当な目的で，正当な方法により収集，利用，他への提供しても，プライバシー権の侵害とはならないと解される。自己情報コントロール権は，このような内容の権利として憲法上保障されているというべきである」（判時１９５２号１４０頁第３段）

○　千葉地裁平成１８年３月２０日判決（乙１８）（http://www.courts.go.jp/）

「情報処理技術の発展に伴い，多くの分野において大量の個人情報が収集等されている状況下においては，個人情報が不当な目的のために収集されたり，想定された本来の目的以外に使用されるなどすると，著しく私生活の平穏を害するなど不都合な結果を招くおそれがあるのであって，かかる不都合を防止するためには，みだりに個人情報を収集・管理・利用されない利益を法的にも保護

に値する個人の利益として認めるのが相当である。そこで，自己に関する一定の情報について，みだりに収集等されない権利は，人格権の一内容として憲法１３条により保護される権利と解するのが相当である。」（３６頁）

○　東京地裁平成１８年４月７日判決（乙１５）

「憲法１３条は，個人の私生活上の自由の１つとして，個人の同意なく，みだりに個人情報を利用提供されない自由を保障しているというべきであり，国家機関が正当な理由もなく，個人の同意なく，みだりに個人情報を利用提供することは同条に反して許されないというべきである。」（２６頁）

○　和歌山地裁平成１８年４月１１日判決（未公刊）

「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，プライバシーの権利の一態様として，個人に関する情報につき，単に，行政機関等から不当に収集，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，他の行政機関等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保障される必要があるというべきである。」（３８頁）

◎　東京地裁平成１８年７月２６日判決（乙２５）

「このような社会状況においては，情報提供の相手方，利用方法等に関する本人の合理的な期待が保護されるべきであり，前記アのプライバシーに係る利益にも，個人情報を本人の合理的な期待に反して開示提供されない利益が含まれると解すべきである。」「したがって，本人確認情報が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利益は，法的な保護に値するものというべきである（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）。原告らの主張する自己情報コントロール権も，基本的には，同様の趣旨をいうものと理解され，その限度において理由があるというべきである。」（６８～６９頁）

◎　横浜地裁平成１８年１０月２６日判決（甲７５）

「憲法１３条は，すべての国民が個人として尊重されることを保障しているが，個人として尊重されるためには，私生活上の自由を保障することが不可欠であるから，『私生活をみだりに干渉されない権利』としてのプライバシー権は，憲法１３条により保障されているというべきである。さらに，高度に情報化された現代社会においては，インターネット等を通じた個人情報の収集，利用，提供により個人の尊厳が脅かされるおそれがある。そうすると，個人の尊厳を保障するためには，プライバシー権を単に『私生活をみだりに干渉されない権利』と解するだけでは足りず，『みだりに自己の情報を収集，利用，提供されない権利』（自己情報コントロール権）をも含む権利であると解するのが相当であり，このような自己情報コントロール権は，憲法１３条により保障されているものというべきである。」（３５頁）

◎　名古屋高裁金沢支部平成１８年１２月１１日判決（甲７４，乙２７）

「住基ネット上の本人確認情報に関して上記のような違憲状態が生じた場合において，その原因が上記アの観点からの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，人格権としてのプライバシー権に基づく妨害排除請求権又は妨害予防請求権によりその差止め等の救済（憲法１３条が国民に対して保障している人格権としてのプライバシー権に基づき，公権力による個人情報の提供を禁止し，公権力が保有する個人情報の削除を求めること）を求めることができるものというべきである。被控訴人ら主張のプライバシー権（自己情報コントロール権）は，上記の趣旨と範囲において，これを肯定することができる。」（３７頁）

７　被控訴人は，阪本教授や松井教授の論文を論拠として引用しているが，いずれも，極めて古い時期の論文であり，個人情報が広く保護されるようになった時代には不適切である。

つまり，坂本昌成「『人格権』に基づく自己情報の訂正請求権」が掲載されているジュリスト８２９号は１９８５年２月１日号であり，この論文は２０年

以上前のものである。また，阪本昌成「プライバシーと自己決定の自由」が掲載されている樋口陽一編『講座憲法学３』は，１９９４年６月の発行であり，これも，１３年も前の論文である。

さらに，松井茂記「プライヴァシーの権利について」が掲載されている法律のひろば４１巻３号は１９８８年３月号であり，これも約２０年前のものである。

8　そのほか，被控訴人は長谷部教授の見解を引用しているが，それは，「自己情報コントロール権として把握されるプライバシーには本質的な限界がある」というものであるところ，それはプライバシーに限界があることを述べているものである。憲法上のいかなる権利にも何らかの限界が存することは控訴人も大阪高裁判決も否定しないところであり，被控訴人の批判は的を射ていないと言わざるをえない。

第２　本人確認情報の要保護性

1　被控訴人は，江沢民主席講演会事件上告審判決につき，同事件についての杉原解説を援用しつつ，「氏名，学籍番号，住所及び電話番号」という「単純な情報」それ自体について，プライバシーに係る情報としての法的保護の対象とすべき旨を判示したものでない」とし，「講演会の参加申込者であるという，公開することが当然視できない情報が，氏名等のこれらの「単純な情報」と結びつくことによって，誰が講演会に参加したかが明らかになることから，この情報全体について，プライバシーに係る情報としての法的保護の対象となることを認めたものである」と主張している（被控訴人準備書面（３）１４頁以下）。

2　しかしながら，被控訴人の主張は，杉原解説を正しく理解したものではない。

杉原解説は，「本件個人情報は，Ｘらの氏名・学籍番号，住所及び電話番号並びにＸらが本件講演会の参加申込者であることであって，前４者の情報は基本的には個人の識別などのための単純な情報であるが，このような本来一定範

囲の他者には当然開示すべき単純な個人情報であっても，自己が欲しない他者にはこれを開示されたくないと考えることは自然なことであろう。そして，本件講演会が一定の思想，信条，し好を示すものでなく，本件講演会への参加申込者であることは大学の学生として教育活動への参加を希望したことを意味する情報にすぎないとしても，そのことも公開されることが当然とされる情報ではない。そして，本件個人情報は周知されていたものではない。そうすると，本件個人情報は全体としてプライバシーに当たる情報であると考えられる。判決要旨１は，この趣旨を明らかにしたものである。」（４８９～４９０頁）というものであり，上記「単純な情報」についても「自己が欲しない他者にはこれを開示されたくないと考えることは自然なことであろう」としているのである。

また，「本件講演会への参加申込者であること」「も公開されることが当然とされる情報ではない」としているのであり，「本件講演会への参加申込者であること」との結びつきを必須のものとはしていないのである。日中国交回復の前であれば中国の国家主席の講演会に参加申込みをしたことがセンシティブな情報に該当するかも知れないが，国交が回復され，政府が日中友好を促進している状況で，国賓として来日する中国の国家主席の講演会に参加申込みをすることは，あまりセンシティブな情報とは言い難いであろう。

3　大阪高裁判決（甲７２）は，「人は素性を知らない他人に対して然るべき理由もないのに自己の氏名や住所を明かすことはないといえるし，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思われる。」（４８頁）としており，この認識は江沢民主席講演会事件上告審判決及び杉原解説とほぼ共通の認識である。

そして，中島徹鑑定意見書（甲８４）が指摘しているように，この認識の点において，大阪高裁判決は，名古屋高裁判決（甲８３）・名古屋高裁金沢支部判決（甲７４）と異なっているわけである（１９頁）。要するに，３つの高裁判決の中で，大阪高裁判決の判示こそが，江沢民主席講演会事件上告審判決の判示に近いものと言うことができよう。

４　さらに，中島徹鑑定意見書（甲８４）が，「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・・・。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，・・・，極めて形式的な思考といわなければなりません。」（６頁）と述べているように，「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「形式的」な思考であって妥当ではないのであり，江沢民主席講演会事件上告審判決も「本件個人情報は全体としてプライバシーに当たる情報である」と「実質的」に判断しているのである。

そして，中島徹鑑定意見書が「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」（２１頁以下）につき，「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。」（２２頁）と述べているように，大

阪高裁判決が，名古屋高裁判決・名古屋高裁金沢支部判決と異なっているのは，形式的判断に陥らなかった点にあるわけである。

5　そのほか，被控訴人は「変更情報は身分関係の変動等を端的に推知させる情報ではない」と主張しているが，そもそも，要保護性の判断にあたって，身分関係の変動等を「端的」に推知させることは不可欠ではない。「端的」でなくても，推知させるものであれば，要保護性は高くなるのである。

被控訴人は，「例えば，婚姻により姓が変わった場合であれば，修正を行ったという単なる外形的事実を示す「住民票の記載の修正を行った旨」の記載に加え，「職権修正等」，「事由が生じた年月日」のみが「変更履歴」として記載され，これが都道府県知事に通知，提供されるにすぎず，婚姻，離婚等の具体的事由が通知されることはない」と主張しているが，まず第１に，「住民票の記載の修正を行った旨」・「職権修正等」の記載が行われている住民票は，住民票全体の中で少数であり，したがって，注意を惹きやすいものである。

第２に，「住民票の記載の修正を行った旨」・「職権修正等」の記載は，転居の記載などと異なり，身分関係の変動を推知させるものである。

第３に，身分関係の変動としては，婚姻，離婚，養子縁組，養子離縁及び認知などがあるところ，その中で圧倒的に数が多いものが婚姻・離婚であるから，「住民票の記載の修正を行った旨」・「職権修正等」の記載は，婚姻・離婚が行われた蓋然性が高いことを示すものである。

さらに言えば，「住民票の記載の修正を行った旨」・「職権修正等」・「事由が生じた年月日」の記載は，住民票記載の情報以外の他の情報と結びついて身分関係の変動を推知させることがあるし，また，「住民票の記載の修正を行った旨」・「職権修正等」・「事由が生じた年月日」の記載を端緒として他の情報を入手することにより身分関係の変動を推知できるようになることもある。

したがって，「住民票の記載の修正を行った旨」・「職権修正等」・「事由が生じた年月日」についての情報の要保護性を軽視するのは誤りである。

第２章　住基ネットの運用によるプライバシー権（自己情報コントロール権）の侵害について

第１　住基法と行政機関個人情報保護法の関係について

１　被控訴人らの主張

被控訴人らは，住基法３０条の３４は，法の定める目的の範囲内の利用等に当たらないデータマッチングを禁止しており，これに違反すれば懲戒処分の対象となるところ，行政機関個人情報保護法３条３項及び８条２項と，住基法３０条の３４等の本人確認情報の保護規定は，一般法と特別法の関係に立ち，住基法の規定が優先して適用されるから，大阪高裁判決の解釈，すなわち，行政機関個人情報保護法３条３項について，８条３項のような調整規定が置かれていないことを理由にして，住基法の適用を排除する解釈は誤りであり，行政機関個人情報保護法の趣旨に反すると主張している（被控訴人ら準備書面（３）１９～２２頁［(１）～（３）ア］）。

２　目的外利用・目的変更の危険性

（１）たしかに，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るが，これはしかし，受領した本人確認情報をそのまま目的外に利用することの禁止にとどまる。たとえば，行政機関が，法令に定められた事務処理の遂行のために，本人確認情報を受領し，すでに保有していた個人情報と結合した場合，その結合後の情報は，受領した本人確認情報そのものではない。そしてその結合後の個人情報は，結合前の当該個人情報が事務遂行の必要に応じて加工されてきたのと同様に，必要に応じて加工されることになろう。あるいは，結合前の当該個人情報と同じように，目的外利用や目的変更もあり得よう。その場合に適用されるのは，行政機関個人情報保護法であって，住基法ではない。あくまで住基法の規制は，受領した本人確認情報をそのまま利用・提供する段階

において，目的外の利用・提供を禁ずるにとどまっている。少なくとも，住基法には,行政機関保有の個人情報と結合された後の情報の取扱いについて,何らの定めがおかれていない以上，一般法である行政機関個人情報保護法が適用されることになるのである。したがって，本人確認情報を受領した段階での利用が目的外利用等に該当しなければ，それ以降，当該行政機関が本人確認情報と結合した個人情報は，行政機関個人情報保護法の適用対象情報となるから，同法３条３項の利用目的の変更も可能となるのである。

（２）実際に，行政機関による本人確認情報を含めた個人情報の取扱いで，最も懸念されることは，目的外利用・目的変更について，行政機関に大幅な裁量判断が認められている上に，後述するように，それが違法に及ぶことを監視し規制する第三者機関が不在であるという点である。この事実が，次のような結果に結びつくことは，容易に想定できることである。

（３）すなわち，もともと行政機関個人情報保護法の規定による限り，同法８条の目的外利用禁止の例外については，その３項が特別法による規制を予定していることは明らかである。では，同法３条３項の目的変更についてはどうか。同様に，特別法による規制を予定していたのであれば，８条３項に相当する規定が置かれてしかるべきであるが，そのような明文の規定はない。一方，総務省行政局監修の「行政機関等個人情報保護法の解説」は，行政機関個人情報保護法３条３項について，「新たな行政サービスの展開に対応する必要性等から，利用目的を変更せざるを得ない場合が生じることは一般に想定しうるところであり，行政の適正な運営を図りつつ，個人の権利利益を保護するという本法の目的に照らせば，利用目的に一定の柔軟性を持たせることが適当である。」（２６頁）としており，目的変更について，行政機関個人情報保護法８条３項に相当する規定がおかれていないということから，一般法である行政機関個人情報保護法が適用される余地があるかのように読みとれる。

その結果，上記のような第三者監視機関不在のもとでは，少なくとも実務上は，行政機関にとって利便性を有する解釈として，そのような解釈採用の可能性が高いといわなければならない。

（４）前述した結合後の個人情報について，仮にそれが本人確認情報を内包していると判断される限りにおいて，住基法３０条の３４の規制が及ぶと解釈するとしても，当該情報が，事務処理の範囲内で種々の加工を加えられていく過程で，住基ネットから情報提供を受けた本人確認情報であるかどうか不明確になっていく可能性が十分に考えられる。後述するように（４４頁），当初，本人確認情報を利用して結合前の個人情報の氏名・住所・性別又は生年月日（以下「氏名等」という。）の正確性が確認できれば，その後は，行政機関の保有する個人情報について，住民票コードを使用しなくても，個人が特定できる氏名等のいずれかの組み合わせにより名寄せすることが可能である。

いずれにしても，住基法の規制対象であるかどうかが不明確な状態の個人情報については，行政事務の効率化の観点から，他の個人情報と同様に行政機関個人情報保護法のみの適用対象と位置づけられて，利用範囲が拡大していく可能性は少なからずある。

その場合，上記のような第三者機関が存在しない以上，事実として，行政機関の判断のみが通用していくことになる。行政機関担当者にしてみれば，違反のおそれを申し出るか指摘すれば，自らの仕事が停滞するだけであるから，当該業務に関与する人々にはそれを申し出あるいは指摘するメリットは全くなく，それへの動機付けはどこにもない。それ故，違法行為は，情報管理がずさんで漏えいするような事態にいたって初めて判明するということとなり，事実上違法行為が摘発される可能性はほとんどないという事態になる。懲戒処分や罰則をいくら強化しても違法行為の防止に対する実効性がなく，全く無意味というべきである。

第２　住民による本人確認情報の利用状況の把握について

１　被控訴人らは，利用事務は，法律又は条例において明確に定められ，その規定の仕方も，住基法や条例上も別表において限定列挙され，一覧性があり，国の機関等への提供の状況については，官報において公示していることなどからしても，住民は，本人確認情報を利用できる事務を十分把握し得ると主張している（被控訴人ら準備書面（３）２９～３０頁）。

しかしながら，被控訴人らの主張は，単に形式的にそういえるだけのことであって，一般市民が事前に利用対象を把握することは実際には極めて困難であり，不当な利用を未然に防止することは不可能に近い。官報において公示されるのは対象事務と提供の仕方と件数だけで，自分の情報が提供されたかどうかは確認できない。これは，前記のとおり，本人確認情報が情報漏えいやデータマッチングが瞬時に起きるコンピュータ・ネットワークで利用されることを考えると，プライバシー権にとって極めて深刻な状態にあると言わなければならない。

２　また，被控訴人らは，「都道府県知事は，自己に係る本人確認情報の提供又は利用の状況に関する情報の開示請求に適切に対応するため，個人ごとの本人確認情報の提供又は利用の状況に係る情報を必要な期間保存することとされており（セキュリティ基準第６－８－（５）・乙第３２号証），住民は，住基法３０条の３７に基づき，都道府県サーバ及び全国サーバに保存されている自己に係る本人確認情報の開示を請求することができる。その上，住民は，個人情報保護条例に基づき，①本人確認情報を提供した住民の住民票コード，②本人確認情報を提供した住民の氏名，生年月日，性別及び住所，③提供先及び検索元，④提供年月日，⑤利用目的について開示請求を行うことができる（住民基本台帳事務処理要領第６－５－（３）・乙第３４号証）。」とする。

しかしながら，上記住民基本台帳事務処理要領第６－５－（３）には，「個

人情報保護条例に基づき開示を行うことが適当である」と記載されているに過ぎず，上記①～⑤のような具体的な開示事項については，特に記載がない。それ故，いかなる事項が開示されるかについては法令上の根拠が何もないのである。

また，情報の開示請求は，都道府県知事に対し，住基法３０条の３７で，「自己に係る本人確認情報について」開示を請求できるとしているに過ぎず，「提供又は利用の状況」については，法文上何ら規定がない。セキュリティ基準や住民基本台帳事務処理要領といった法令によらないあいまいな根拠に基づいて，しかも個人情報保護条例において開示制度が整備されることを前提として，ようやく開示がなされるに過ぎない。

さらに，条例の定め方如何によって，かろうじて事後的にいかなる国の行政機関等に提供されたかを知りうる可能性はあるが，膨大な利用事務の全てを事前に把握することはやはり事実上不可能であることに変わりはない。データマッチングや名寄せがされてしまってからでは手遅れなのである。

第３　本人確認情報の民間利用禁止の実効性について

被控訴人らは，「第三者が他人の住民票コードを知ることは極めて困難であり，住民は，仮にこれが第三者に知られてしまったとしても，その変更が可能である上，違反行為に対する罰則も設けられ，厳格な利用規制が行われているのであるから，住民票コードが本人の予期しない範囲で民間業者に保有され，利用される具体的危険があるとは到底いえないことは明らかである。」とする（被控訴人ら準備書面（３）３０～３２頁）。

しかしながら，納税者番号制度（甲７６）や社会保障番号制度（甲８５）への住基ネットの利用が検討されており，かかる制度が導入されてしまえば，もはや住民票コードの利用禁止は制度として廃止されたに等しく，手遅れであろう。それは米国において，社会保障番号がコンピュータ・ネットワーク社会の

中でなりすましなどに悪用され，現実の被害が生じていることで実証済みである。

また，第三者が住民票コードを知ることは不可能ではない。すなわち，平成１９年５月に愛媛県愛南町において，住民票コードを含む住基情報が大量に流出した（甲８６）。今回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件であり，このような過失による個人情報の漏洩が多発しており，第三者に住民票コードを知られてしまう可能性が現実にあるのである。

このほか，現時点でも，将来の利用を見越して，住民票コードの情報収集が行われていないとも限らない。大阪高裁判決が指摘するように「法の規制にかかわらず，個人情報そのものが商品価値を持ち，大量の個人情報の収集や流出が少なからず行われている社会の現状を考えると，違法な利用がたまたま発覚することを期待する以外に，実際に上記の禁止を担保する制度は存在しないと言わざるを得ず，その意味では，民間利用禁止の実効性は，現実には非常に疑わしい。」のであって，被控訴人らのような主張は現実社会での個人情報の価値を見誤ったものである。

第４　自衛官の募集に関する事案等の漏洩事例について

被控訴人らは，「過去の自衛官募集に関する事案を持ち出して，現在において，住基ネットの本人確認情報が国の機関等によって集積，結合され，利用される危険性が具体的に存在することの根拠とすることはできない。」と主張する（被控訴人ら準備書面（３）３２～３３頁）。

しかしながら，自衛官募集に関する事案は，行政機関の個人情報の収集や取扱いの具体例として，現実に実施されていた事実であり，それらがコンピュータ管理されている現状を考えると，本人確認情報を利用して，データマッチングや名寄せがされていく具体的危険性を基礎づける一要素となることは否定できない。つまり，この事例がそうであるように，行政機関によっては，個人情

報を際限なく集積・結合できれば，それが職務遂行上の便宜につながるとして，住基ネットの本人確認情報を利用して，その方向を希求することは十分あり得るのである。

また，前記のように過失による個人情報の漏えいが多発している現状があり，本人確認情報についても，愛媛県愛南町において，住民票コードを含む住基情報が大量に流出しているのである（甲８６）。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あるが，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ない。住基ネットは，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・システムなのである。今回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件であり，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らない（甲８４　３６頁）。

第５　住基カードの利用による名寄せの危険性について

１　被控訴人らは，「住基カードは，その内部構造及びそのセキュリティ対策上住基カード内に記録された情報が行政機関のコンピュータに残るようなシステムとはなっていないのであり（住基カードに関する技術的基準第２の２），このことは証拠（乙第２６，第３９号証）から明らかである。」（被控訴人ら準備書面（３）３３頁）とするが，引用する証拠のいかなる部分から明らかなのか不明である。

２　また，被控訴人らは，住基カードの内部構造は住民票コードが格納された「住基ネットのエリア」と「独自利用のエリア」に分かれており，住民票コードにアクセスするには，認証を経ることが必要であるが，市町村の独自利用による

サービスを提供する機関は，当該認証権限を付与されていないため，サービス提供機関は，独自利用のエリアを利用してサービスを提供するにとどまり，住民票コードが残るということはないから，名寄せされる危険性はないと主張している（被控訴人ら準備書面（３）３３～３４頁）。

しかしながら，法令上，独自利用において住民票コードの利用を禁止する根拠はどこにもなく，住基法１条の行政事務の合理化のため，市町村は，独自利用において住民票コードを利用することができるのであって，住基法３０条の６，３０条の７第６項２号により，条例で定める事務の処理に関して求めがあれば，提供することもできる。

3　被控訴人らは，「住民票コードの利用拡大は，住民基本台帳法の３０条の４２，３０条の４３等において厳しく抑制されており，上記告示はこうした住基法の趣旨を踏まえて定められたものである（住基法３０条４４第４項，住基法施行規則４６条参照）。したがって，住基カードの独自利用領域において住民票コードの利用を可能にすることは，この住基法の趣旨に明らかに反するものであり，法律の趣旨に適合する告示が法律に反するものに改正されることはおよそ考え難い。」「なお，住基カードの仕組みからしても，告示の改正がされない限り，市町村の独自利用サービスを受けた記録に住民票コードが付加される可能性は全くない（乙第２６，第３９号証）。」と主張する（被控訴人ら準備書面（３）３５頁）。

しかしながら，被控訴人らは，住基法の趣旨のうち行政事務の効率化を強調する立場から議論を展開して，本人確認情報の秘匿の必要性は必ずしも高くないという主張をしていたが（答弁書１８～１９頁），住基カードについては，（被控訴人らの主張では単なる便宜的数字であるはずの）住民票コードの利用拡大，つまり，独自利用領域での利用は，住基法３０条の４２等で厳しく抑制されている趣旨に反するというのである。行政事務の効率化を強調していた被控訴人らの立場からすれば，告示を改正して，利用拡大を進める可能性が高い

と言わざるを得ず，被控訴人らの主張はご都合主義的であって，説得力に欠ける。

また，市町村長は，条例の定めるところにより，条例に規定する目的のために住基カードを利用することができるのであるから（住基法３０条の４４条８項），告示が改正されない限り，独自利用に住民票コードが利用されないという保証はどこにもない。

第６　長谷部意見書及び堀部意見書について

１　長谷部意見書の誤り

被控訴人は，自己の主張を裏付けるものとして，長谷部意見書及び堀部意見書を引用している（３５～３６頁）が，いずれも当を得ないものである。

まず，長谷部意見書は，「現行法制度を前提とする限り，住民基本台帳ネットワークの運用を通じて，行政機関により住民票コードをマスターキーとするデータマッチングが行われ，住民のプライバシーが侵害される具体的な危険が生じているとはいいがたく，回復不可能な重大な損害の発生を抑止するためにシステムの差止を考慮すべき理由があるとはいいがたいと思われる。」（５～６頁）と述べている。

しかしながら，長谷部意見書は，形式的に条文を羅列しただけのことであり，実質的な検討は何もされていないので，大阪高裁判決への反論となり得ていない。なお，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あるが，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ある。この場合，対表現の自由とは異なり，公権力行使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ない。しかし，長谷部意見書は，公権力の側に個人情報の収集･利用権限があることを前提として，当該権限の抑制には具体的危

険性が必要であると説いている。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らない。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ある。たしかに，法律の文言上は，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る。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，大阪高裁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分かる（甲８４　４０～４１頁参照）。それ故，具体的危険の発生を回避する制度として，後述する第三者機関が必要であり，長谷部意見書の根拠は薄弱である。

2　堀部意見書の誤り

次に，堀部意見書は，「平成１１年住民基本台帳法改正法においては，個人情報保護の観点から現行の法制度の枠内で可能な限りの対応策が盛り込まれた。同法の立案に当たっては，国際的な水準に対応した個人情報保護対策を内包するシステムを構築すべく，十分な検討が行われたところである。（中略）以上見てきたように，住民基本台帳ネットワークシステムについては，住民基本台帳法に基づき，国際的なスタンダードに対応した個人情報保護措置が講じられていると評価することができる。」（１，７頁）としている。

しかしながら，堀部意見書もまた，形式的にＯＥＣＤ８原則と住基法の条文の対応関係を述べただけで，その実質的な内容に踏み込んだ検討は何らしておらず，住基法の規定や行政機関個人情報保護法の規定が同８原則を充たしていないことは明らかである（甲５７　４０～４５，甲８４　２４～２９頁参照）。それ故，同意見書は，あくまでも国際的なスタンダードに形式的に「対応」した個人情報保護措置が講じられていると言っているだけで，その実質的な内容が国際水準を満たしているかどうかは語っていないと言わざるを得ない。

第７　住基ネットの本質について

１　被控訴人ら主張の誤り

被控訴人らは，「住基ネットは，市町村が住民基本台帳制度を運営するという制度の基本的枠組みを変更することなく，全国的に市町村の区域を越えた本人確認ができるような仕組みを付加するものであり，①それぞれの機関が保有している個人情報は，従前どおり分散管理することを予定した地方公共団体共同のシステムであって，国等が個人情報を一元的に管理するシステムではないこと，②住基ネットのサーバ上に保有される情報は，本人確認のための氏名，生年月日，男女の別及び住所の４情報，住民票コード及び付随情報（変更情報）のみであること」などを指摘している（被控訴人ら準備書面（３）１８頁）。

しかしながら，被控訴人らの主張は，本人確認情報を収集・保有し利用するだけのシステムであると形式的に制度を説明するものであるが，かかる説明をするに止まっていることは，以下に述べるように，潜在的に住民の個人情報を包括的に取り扱う能力を秘めているシステムであるという住基ネットの本質を見落としている点で失当である。

２　住基ネットの本質

（１）個人情報の共同利用が可能であること

まず，大阪高裁判決も指摘するように，住基ネットの導入によって，「そのデータベース内における検索が極めて容易になり，また，行政機関が収集・保存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ということができる。」（甲７２　７４頁）のである。

（２）個人情報漏洩の不可逆性

しかも，個人情報は，一旦漏洩すれば，元の状態に戻すことができないと

いう性格を有しており（不可逆性），次に述べるように，コンピュータ・ネットワーク上で，情報漏洩やデータマッチングがあってからでは，手遅れであり，漏洩した情報，データマッチングされた情報を全て抹消することはほぼ不可能に近いのである（甲３０　２０頁参照）。

（３）コンピュータ・ネットワークであること

また，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，それがコンピュータ・ネットワークであるという点である。コンピュータ･ネットワークでは，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。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る。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という可能性を有している。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る（甲８４　１３頁，１７頁）。

ちなみに，ドイツ連邦憲法裁判所が，１９８３年の国勢調査判決（BverfGE６５,１）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」（下線は控訴人代理人）ものであるとして，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（上記下線部），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る（甲８４　４１～４２頁）。

（４）公的システムであること

さらに，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

のシステムであるが，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・システムでもある。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る。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託先における誤用・濫用による具体的危険が発生し，それが現実化した場合，それによるプライバシー権侵害は極めて深刻である。そのことを端的に示したのが，前述のごとく平成１９年５月に愛媛県愛南町において発生した住基情報の大量流出である。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あろう。しかし，住基ネットという仕組みにおいては，上述したように，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する。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ということができる（甲８４　１７～１８頁）。

（５）参加・離脱の自由がない制度であること

これに対し，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があり得る。しかしそれは，有効な反論とはいえない。第１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る。第２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る。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あろう。とはいえ，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，依然として残さ

れている。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ある（甲８４　１８頁）。

（６）小括

以上のように，住基ネットの本質の一つは，コンピュータ・ネットワークであることから，情報処理の速さゆえに，情報漏洩やデータマッチングが瞬時に起きる，つまり，抽象的危険が瞬時に具体的危険に転化するという点にある。

もう一つは，住基ネットが，民間とは比較にならない，行政機関の保有する膨大な個人情報に接続し，それらの情報の結合を可能にすることのできるコンピュータ・ネットワークであるということである。

すなわち，住基ネットは，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あるが，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・システムであるが故に，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システムなのである。

それ故に，住基ネットにおいては，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，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の本質であり，問題の核心なのである（甲８４　３２頁）。被控訴人らのように，住基ネットを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，正鵠を射ているとはいえない（甲８４　２１頁）。

第８　第三者機関の必要性について

１　情報漏洩やデータマッチングの未然防止（制度的担保）の必要性

（１）前記のとおり，個人情報が漏洩・データマッチングされてからでは，手遅れである以上，それを未然に防止する必要がある。また，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ある。なぜなら，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かもしれないが，コンピュータ・ネットワークにおいては瞬時に変わるため，人間が遮断することはほとんど不可能だからである。

それ故，潜在的危険が現実化すること（つまり具体的危険の発生）を回避するための制度の存在は，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（甲８４　４４頁）。

（２）また，総務省の行ったセキュリティ対策は，それ相応のものでなければ，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あり，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であるが，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ある。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ない。このような見地からも，セキュリティが損なわれる事態を想定して，情報漏洩やデータマッチングを防止する法制度による補完が必要なのである（甲８４　３１～３２頁）。

それ故，大阪高裁判決が判示するように「個人情報の取得について，本人に対しあらかじめ「利用目的を明示」することを要求し（同法４条），目的外の利用，提供の禁止の例外として「本人の同意」（同法８条２項１号）を定めている同法の制度趣旨にかんがみ，目的外利用禁止の例外については，「本人同意」とみなすことができるような相応の制度的担保が必要であると解される」（甲７２　８１頁）のである。

２　本人同意と同視できる制度的担保

（１）第三者機関設置の要請

上述したような住基ネットの本質に鑑みれば，未然に情報漏洩やデータマッチングなどの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ある。

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，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か，それらが適切な存在であるといった被控訴人らの主張は，行政機関に司法機関としての役割を兼務させる，あるいは，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いるのと同じであって，無意味である（甲８４　４３）。

それ故，法令上の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，つまり住基法上の業務と全く無関係の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後述するような第三者機関の設置が要請されるのである（甲７９）。

（２）本人による情報コントロールが不可能であること

また，以下のような観点からも第三者機関によるチェックが必要である。

前述したように，市民は，気がつかない間に利用範囲が拡大されることによって，現実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）となっている。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，現実を見ない形式論といわなければならない。

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のである（甲８４　３０頁）。

（３）被控訴人らの主張の誤り（その１）

ア　被控訴人らは，「そもそも住基法は，法で定める目的の範囲外の利用を厳格に禁止し，その違反に対しては，懲戒処分や刑事罰を科し得る法制度となっているのであるから，目的外利用禁止の例外にどのような制度的担保を要するかは本来論じる必要のない事柄である」（被控訴人ら準備書面（３）２２）という。

被控訴人らは，罰則等により目的外利用が禁止されており，その例外が許容されていない以上，禁止の例外についての制度的担保を論じる必要がないと主張しているものと思われる。

イ　しかしながら，大阪高裁判決は，法解釈上，目的外利用が可能であり，しかも，法文の抽象的な規定の仕方からすれば，「行政機関が住基ネット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が高い」と論じているのである。それ故に，「個人情報の取得について，本人に対しあらかじめ「利用目的を明示」することを要求し（同法４条），目的外の利用，提供の禁止の例外として「本人の同意」（同法８条２項１号）を定めている同法（行政機関個人情報保護法；控訴人代理人註）の制度趣旨にかんがみ，目的外利用禁止の例外については，「本人同意」とみなすことができるような相応の制度的担保が必要であると解される」（甲７２　８１頁）のである。では現行法制度上，目的外利用禁止のための制度的担保は十分かといえば，後述するように，罰則等の規制を考慮しても，十分とはいい難いのである。

被控訴人らは，罰則等で現行法制上，目的外利用が絶対的に禁止され，目的外利用の可能性が全くあり得ないという前提で議論しているが，その前提自体が形式的思考に基づく誤ったものであり，全く反論になっていない。

（４）被控訴人らの主張の誤り（その２）

ア　さらに被控訴人らは，①公共領域に属する個人情報は個人の承諾なくし

て利用できるという法制度が採用されていること，②この点は平成１１年の住基法改正の前後で変わりがなく，個人の承諾なくして利用しても人格的利益の侵害とはならないこと，③ＯＥＣＤ８原則が本人の同意を要求するのは本来の目的以外のために個人データの利用等を行う場合であり，住基法別表の事務のための提供は本来の目的の範囲内での利用であることなどから，「本人の同意」又はこれと同視できる制度的担保は不要であると主張している（被控訴人ら準備書面（３）２３頁）。

イ　しかしながら，被控訴人らの主張は，目的外利用が絶対的に存在しないという前提の下で，「本人確認情報を住基法別表に掲げられた国の機関等に対して別表に掲げられた事務のために提供すること」だけを形式的に取り上げて，本来の目的の範囲内であると結論づけたものに過ぎない。つまり，これは，本人確認情報の提供を受けた行政機関において，その後いかに本人確認情報が利用・提供されるかについての議論をあえて無視した形式的思考によるものであり，実質的な議論をしている大阪高裁判決の判断への反論になっていない。

ウ　また，以下のとおり，上記①～③の議論それ自体にも誤りがある。

（ア）すなわち，①のような認識では，公的機関が行う活動との関係で市民がおよそプライバシーを持ち得ないこととなりかねず，かかる認識自体が，問題とされなければならない。元来，「公共領域」においてこそ権力行使の限界が厳しく問われなければならず，憲法の視点を抜きにしてはそこでの問題を論じることはできないはずである。にもかかわらず，そうした視点が欠落している点で誤りであることは，２００６年９月２５日付中島徹教授の鑑定意見書において明らかにされているところである（甲５７　２０～２３頁）。問題は，個人「情報を個人の承諾を要することなく利用できるという法制度が採用されている」ことの憲法適合性なのであるから，被控訴人らの議論はそれ自体的はず

れである。

（イ）②の点については，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はあるが，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るわけではなかった。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である。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，容易に理解できる。それ故，被控訴人らの認識は明らかに誤りである（甲８４　１３～１４頁）。

（ウ）さらに，③の点については，被控訴人らのいう本来の目的とは，住基法１条に定められた「行政の合理化」（堀部意見書６～７頁）のことであると思われる。しかしながら，住基法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あるから，実際上いかなる内容でも含めることが可能である。そもそも，これでＯＥＣＤ８原則の「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るが，それは適切ではない。なぜなら，被控訴人らの解釈は，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いうに等しく，それでは，「目的の明確化」という日本語の日常的な用法

とはいえないし，「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になってしまうからである。被控訴人らも堀部意見書も，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おり，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していないのであるから，ほとんど無意味な説明である（甲８４　２７～２８頁）。

３　第三者機関のあり方

（１）ＥＵ指令における監視機関の定め

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る。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するが，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」（ＥＵ指令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る。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ある。

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る。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る。

この監視機関は，次のような権限を有する機関とされている。

（Ａ）処理対象のデータにアクセスする権限

（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

（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

このような監視機関は，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る。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る。

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る。

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る。

しかしながら，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ない。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である。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ある。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ないが，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のである。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のである（甲８４　４４～４６頁）。

（２）個人情報保護委員会（日弁連意見書）

ア　この点，２００３年１月３１日付日本弁護士連合会の「行政機関の保有する個人情報の保護に関する法律案の修正案に対する意見書」（甲７９の１）は，「各行政機関内における個人情報の統一的な管理体制の構築を図るためには，スウェーデンのデータ検査院など，公正な第三者機関を設置し，かかる第三者機関に行政機関の保有する個人情報保護の管理監督を委ねるのが」上記ＥＵ指令の要求であるとしている。

そして，今後の電子政府の到来（被控訴人ら準備書面（１）２５頁参照）に鑑みれば，第三者機関の設置は必須であるとし，内閣府に個人情報保護委員会を設置することを提案している。これは，公正取引委員会や電気通信事業紛争処理委員会などの独立行政委員会が現に存在していることからしても，そのような第三者機関としての個人情報保護委員会の設置は現実に可能であると指摘している（甲７９の２参照）。

さらに，第三者機関であるためには，「単なる行政機関の諮問機関では不十分であり，」上記ＥＵ指令の水準を満たしていない旨指摘し，行政機関を監視する職務を果たすために，少なくとも以下の権限を付与されるべきであるとしている。

すなわち，

「１．立ち入り調査権限

1.　「個人情報保護委員会」は，関連行政機関その他個人情報の処理が行われている場所に対し，立ち入り調査を行うことができること。

2. 立ち入り調査先には，地方自治情報センターも含むこと。

3. 地方自治情報センターから，地方自治情報センターが行政機関へ提供した住基ネットデータの具体的な提供内容の報告を受けられること。

4. 地方自治情報センターから，住基ネットデータに対するアクセスログの提供を受けられること。

2．利用停止命令

1. 「個人情報保護委員会」は，個人情報が違法な方法で処理されている場合あるいはそのおそれがある場合，個人データの利用停止命令等適当な措置を発動する事ができること。

3．データマッチング規制

1. データマッチング申請書を受理した場合，かかる申請書面を，申請と同時に官報および「個人情報保護委員会」のインターネット・ホームページに掲載すること。

2. データマッチングの同意を求める申請書面を検討して，法の定めるマッチング要件を充足しているか審査し，充足していると判断した場合は，申請に同意するとともに，「個人情報保護委員会」のインターネット・ホームページに掲載すること。

3. 「個人情報保護委員会」は，関連行政機関に対し，データマッチング実施方法の変更又はデータマッチングの中止を勧告する権限を持つこと。

4．センシティブ情報収集制限

1. センシティブ情報収集の同意を求める申請書を受理した場合，かかる申請書面を，申請と同時に官報および「個人情報保護委員会」のインターネット・ホームページに掲載すること。

2. センシティブ情報収集申請書面を検討して，法の定める収集要件

を充足しているか審査し，充足していると判断した場合は，申請に同意するとともに，「個人情報保護委員会」のインターネット・ホームページに掲載すること。

3. 「個人情報保護委員会」は，関連行政機関に対し，センシティブ情報収集の実施方法の変更又はセンシティブ情報収集の中止を勧告する権限を持つこと。

5．目的外利用の制限

1. 目的外利用の同意を求める申請書を受理した場合，かかる申請書面を，申請と同時に官報および「個人情報保護委員会」のインターネット・ホームページに掲載すること。

2. 目的外利用の同意を求める申請書面を検討して，法の定める目的外利用の要件を充足しているか審査し，充足していると判断した場合は，申請に同意するとともに，「個人情報保護委員会」のインターネット・ホームページに掲載すること。

3. 「個人情報保護委員会」は，関連行政機関に対し，目的外利用の実施方法の変更又は目的外利用の中止を勧告する権限を持つこと。

6．提供の制限

1. 他の行政機関等に対する個人情報の提供に関する同意を求める申請書を受理した場合，かかる申請書面を，申請と同時に官報および「個人情報保護委員会」のインターネット・ホームページに掲載すること。

2. 他の行政機関等に対する個人情報の提供に関する同意を求める申請書面を検討して，法の定める提供の要件を充足しているか審査し，充足していると判断した場合は，申請に同意するとともに，「個人情報保護委員会」のインターネット・ホームページに掲載すること。

3. 「個人情報保護委員会」は，関連行政機関に対し，他の行政機関

等に対する個人情報の提供の実施方法の変更又は他の行政機関等に対する個人情報の提供の中止を勧告する権限を持つこと。」（なお，各表題の括弧書き部分は省略した）

イ　以上に述べた諸点からしても，データマッチングや名寄せあるいは情報漏洩を防止して個人情報を保護するために，十分な監視権限の与えられた第三者機関の設置は必須なのである。しかしながら，現行法上，以上のような第三者機関と呼べる第三者による監視機関は存在しないと言わざるを得ないのである。それは，具体的「危険」認定の重要な一要素として働くものと言わなければならない。

（３）被控訴人らの主張の誤り（その１）

ア　被控訴人らは，①法律上，行政機関の保有する個人情報の透明性は確保されていること，②住基法３０条の９第１項の審議会は，本人確認情報の取扱い等について調査審議を行うことができる機関であり，管理及び運営面において，住民の本人確認情報を保護する役割を果たしていること，③指定情報処理機関に置かれる本人確認情報保護委員会が上記審議会と同様，管理及び運営面において，住民の本人確認情報を保護する役割を果たしていること，④セキュリティ基準で，都道府県知事は（市町村長も，都道府県知事を経由して），本人確認情報の提供先である国の機関等における本人確認情報の管理状況について報告等を要請することができる点でも，国の機関等が本人確認情報を不適切に扱うことを防止する制度的な担保が設けられていることなどを根拠として，大阪高裁判決は，住基ネットでは，本人確認情報を必要な範囲を超えて利用することのないよう二重，三重に本人確認情報保護措置が講じられていることを看過したものであると主張する（被控訴人ら準備書面（３）２５～２７頁）。

イ　しかしながら，被控訴人らは，制度を単に羅列したに過ぎない。どうしてそれらの制度が，実効性のある本人確認情報保護の措置として機能する

のかについて，全く触れられておらず，反論になっていない。大阪高裁判決は，行政から独立した第三者機関（外部機関）であることや，中立的立場から監視する第三者機関であって初めて適切な監視機能を期待することができるとしており，審議会が部内機関であることや，「国の行政機関等」による本人確認情報の利用については調査権限がないことを指摘しているところ，被控訴人らは，これらに対して全く反論できていない。

ウ　また，①～④それぞれについても次のような問題がある。

（ア）まず，①については，大阪高裁判決が指摘するように，行政機関「個人情報保護法では，その存在さえ知られない個人情報ファイルが多数予定されている（同法１０条２項，１１条１項（控訴人代理人註：２項の誤りと思われる））」（甲７２　７９頁）ことからすれば，透明性が確保されているとは到底いえない現状にある。前記第２の２（１９～２０頁）で述べたように，行政機関の保有する個人情報は膨大であって，正しく開示されているかどうかのチェックは国民個人が物理的に把握しうるところではないから，事実上無意味な指摘である。被控訴人の反論にもかかわらず，大阪高裁判決の次の指摘は，依然として正当であるといわなければならない。「個人情報については，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，利用目的を明確にし，本人がそれを知ることができるようにし，本人において個人情報保護の救済手段がとれるようにすべきことが要請されていると解されるが（個人情報保護法４条，３０条の３７，３６条ないし４１条参照），行政機関が保有する本人確認情報を利用できる国の事務は，当初は９３事務であったものが現在では２７５事務にまで拡大され，それは今後さらに拡大することが予想される。加えて，条例で定めれば，自治体が独自に他の機関に本人確認情報を提供することも可能である。もちろん住民は，法令上の拡大を知ろうと思えば知ることはできるであろうが，上記のように拡大して

くれば，実際上利用対象事務を把握することは困難であり，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ないに等しいといえる。また，本人確認情報についての開示請求権（住基法３０条の３７第１項）は，自己に関してどのような情報が収集管理されているかを確認し，必要に応じて訂正請求を行うために極めて重要な意味を有するが，開示対象は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といえる。」（甲７２　７９～８０頁）

（イ）②③については，上記のとおり，国の行政機関等への調査権限はないので，監視機能を果たし得ないのである。審議会で議論されているのは被控訴人ら自身が認めるように非公開とされるセキュリティ面の議論にとどまるのである。セキュリティ基準は，あくまでセキュリティ対策のための措置に関するものであって，データマッチングへの規制としては機能しない。

（ウ）④については，単に要請しうるだけで，法令上の義務ではないし，市町村長については間接的であり，都道府県知事においても立入権限も調査権限も認められている訳でもないことからすれば，行政機関内部での不正利用があっても，その把握は不可能である。それ故，具体的にいかなる意味で本人確認情報保護の措置となりうるのか不明であり，何ら実効性がなく，監視機能を果たし得ないことは明らかである。

エ　以上のとおり，現行法制上，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取扱い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ある。こうした理由から，大阪高裁判決は，「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，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ある。これは，正当な認識といわなければならない（甲８４　３９頁）。

（４）被控訴人らの主張の誤り（その２）

ア　被控訴人らは，東京都が住基法３０条の９に基づいて設置する審議会において，単に担当職員からの往基ネットの運用状況や住基ネットをめぐる裁判の動向等についての報告しか行われていないかのような控訴人の主張は事実誤認であり，失当であるとか，加藤真代委員（主婦連合会参与）の発言は，前提が現状と全く異なっており，加藤委員の発言を殊更過大に捉え，これを根拠に住基ネットの危険性を論じる控訴人の主張もまた失当であるとする（被控訴人ら準備書面（３）２７～２９頁）。

イ　しかしながら，控訴人が指摘しているのは，他の立法を待つまでもなく，住基法自体で，審議会の権限・位置付けは確定しているはずであるにもかかわらず，当の審議会委員が「第三者監視機関」の構成員としての認識を持ち合わせていないという事実である。それ故，「前提」の違いは関係がない。問題の核心は，そのような報告や発言にあるのではなく，次のような点にある。第一に，上記審議会では，本人確認情報の利用や提供への監視が，権限としても定められておらず，それを遂行しうる体制にもなっていないということであり，第二に，データマッチング規制という点で，都道府県審議会ということから来る当然の帰結ではあるが，国の行政機関の本人確認情報の利用等については，何ら調査権限がないということである。非公開の討論をいくら重ねたところで，行政から独立した監視機関としての機能が果たされことには全くならない。いずれにしても，被控訴人らの反論はポイントがずれている。

第９　住基ネットの違憲性について

１　個人情報の集積・利用の具体的危険性について

これまでに述べた諸点（特に第三者機関の不存在）を考慮すれば，大阪高裁判決の次のような指摘は，まことに正当といわなければならない。

「住基ネット制度には個人情報保護対策の点で無視できない欠陥があるといわざるを得ず，行政機関において，住民個々人の個人情報が住民票コードを付されて集積され，それがデータマッチングや名寄せされ，住民個々人の多くのプライバシー情報が，本人の予期しない時に予期しない範囲で行政機関に保有され，利用される危険が相当あるものと認められる。そして，その危険を生じさせている原因は，主として住基ネット制度自体の欠陥にあるものということができ，そうである以上，上記の危険は，抽象的な域を超えて具体的な域に達しているものと評価することができ，住民がそのような事態が生ずる具体的な危険があるとの懸念を抱くことも無理もない状況が生じているというべきである。したがって，住基ネットは，その行政目的実現手段として合理性を有しないものといわざるを得ず，その運用に同意しない控訴人らに対して住基ネットの運用をすることは，その控訴人らの人格的自律を著しく脅かすものであり，住基ネットの行政目的の正当性やその必要性が認められることを考慮しても，控訴人らのプライバシー権（自己情報コントロール権）を著しく侵害するものというべきである。」（甲７２　８４頁）。

本人確認情報を受領した行政機関において，データマッチングや名寄せに及ぶ可能性が法制上も実態上も存在することは，すでに述べたとおりである（第２章，第１）。さらに，前述したように，少なくとも，対象行政事務において本人確認情報を利用することにより，氏名等の正確性が確認できることから，行政機関の保有する個人情報について，住民票コードを使用しなくても，個人が特定できる氏名等のいずれかの組み合わせにより名寄せすることが可能となる。この場合，氏名等は，当該行政事務に関し，申請書類に書かせるなどして，

住基ネットとは無関係に別途行政機関が収集・保有していたものがあるはずである。それ故，かかる氏名等は，本人確認情報の一部ではないとされ，個人情報の集積・利用は，実質的に可能であるし，その具体的危険性は十分にある。

2　被控訴人ら主張の誤り

（1）被控訴人らは，「大阪高裁判決のいうような「少数の行政機関によって，行政機関全体が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」事態が生じるのは，個々の国の機関等が住基法別表の事務処理を行うために管理している個人情報について，これらを扱う公務員が，法令上の根拠もないのにあえてこれを他の国の機関等に提供し，当該機関等がこれを集約管理した上で，同法３０条の３４等に違反して本人確認情報を利用して名寄せやデータマッチングを行うような場合に限られるのである。」と主張している（被控訴人ら準備書面（３）２４頁）。

しかしながら，被控訴人らの主張は，目的外利用等が絶対的に禁止されており，例外はありえないことを前提とした議論であり，その前提となる法解釈や実態認識において誤りをおかしていることはすでに述べたとおりである。

（2）また，被控訴人らは，将来の利用目的の拡大をもって，名寄せやデータマッチングの具体的危険性が認められることにはならないと主張している（被控訴人ら準備書面（３）２５頁）。

しかしながら，本人確認情報の利用範囲については，住基法では「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ある。それ故，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ある。実際，住基法制定以来，利用対象は拡大され続け（平成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，さらには年金記録の管理にも利用することが議論されている。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あ

ろう。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ある。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得ない（甲８４　２８頁）。既に事実上，利用対象を把握することが困難となっており，個人のプライバシー権にとって，重大な脅威が生じている上，さらにそれが拡大していく危険性があるといえるのである。

３　住基ネットからの離脱の選択権

以上に述べたように，プライバシー侵害の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。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（甲８４　４４頁）。

第１０　結語

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から，控訴人が，被控訴人東京都に対し，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は，憲法に適合しており，適法である。それ故，住基法３０条の５は，かかる取扱いを許容しているものと解される。

よって，被控訴人東京都は，これを受信すべき義務を負っており，受信しないことは，住基法３０条の５に反し，違法である。

以　上