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（２）

平成１８年１２月１４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

第１　受信拒否の適用違憲（中島意見書を踏まえた主張）

中島徹鑑定意見書（甲５７。以下，「中島意見書」という。）を踏まえて以下のとおり主張する。

１　一定の危険性への法的対処のあり方（中島意見書６～１３頁参照）

住基ネットを含むコンピュータ・ネットワークについては，セキュリティを確保することにつき，社会的コンセンサスがあり，安全性を全く欠いたシステムの存在が社会的に許容される余地はない。したがって，コンピュータ・ネットワークを構築する者は，少なくとも主観的には十分と思われるセキュリティ対策を講じる。また，コンピュータ・ネットワークへの現実の侵入が成功するかどうかは，侵入しようとする者の熱意・知識・技術等の条件に大きく依存している。

それゆえ，１００％安全なコンピュータ･ネットワークは存在しないし，他方，安全性が０％のコンピュータ･ネットワークも存在しないのが通常である。

したがって，住基ネットにおける個人情報の漏えい等についての危険性につき，抽象的危険とか具体的危険とか，あるいは安全性につき，相当の安全性と言ってみたところで，それらの違いは相対的なものにすぎず，厳密な線引きができるものではない。抽象的危険しかないと言ってみても，あるいは，相当の安全性があると言ってみても，そこには厳然として，情報漏えい等についての一定の危険は残るのである。

ここで問われるのは，そのような一定の危険が現実化した場合の損害につき，どのような負担の仕方を採用すべきかということである。

情報漏えい等についての一定の危険を「ないもの」と同視してコンピュータ･ネットワークを構築することを許すとすれば，個人情報の漏えい等があった場合に，情報主体としては，故意・過失等を立証できる場合にのみ一定の損害賠償を求めるという事後的方法(極めて少額の損害賠償となることが予想され，また，故意・過失等の立証に苦労することが予想されるので，実効性が乏しい

ことが予想される。）ぐらいしかないであろう。そして，情報の性質からして，漏えいがなかったという原状に回復することは不可能である。

このような結果は，１００％安全とは言えず，一定の危険が存在することについての法的扱いとして適切とは言いがたい。

個人情報を全く保護する必要がないという立場に立つのでなく，保護の根拠や範囲はともかくとしても一定の保護が与えられるという立場に立つ以上は，情報漏えい等についての一定の危険への法的対処が必要となる。

われわれの社会は，一定の危険が否定できないことへの法的対処の道具立てを既に持っている。例えば，医療におけるインフォームド・コンセントがその例である。人体の複雑性，そして，それが完全には解明されていないことから，医療行為は１００％安全とは言えず，一定の危険を常に伴っている。医療行為にはメリットとデメリットが伴うことを避けがたいから，それらの影響が及ぶ患者自身が十分な説明を受けた上で同意することが必要とされているわけである。また，それらのメリットとデメリットは，患者自身の生き方や生活の質に関わり，患者自身の価値観に基づいて考量するしかないからである。それゆえ，医療行為は，一定のメリットの評価とともに，一定の危険を甘受するという患者自身の決断によって行われることになる。

住基ネットに対する情報主体の利害状況も，医療行為に対する患者の利害状況と酷似しており，一定の便益を一定の危険よりも重視するか，一定の便益よりも一定の危険を重視するかは，便益や危険により直接影響を受ける情報主体自身の決断に委ねるのが適切である。

2　プライバシー権の多義性と権利性の関係（中島意見書１３～２３頁参照）

被告はプライバシー権が権利として認められるためには，それが「一義的明確性」を備えていることが必要であるというが，権利の性質上，元来が多義的であるプライバシー権にそれを求めることは背理である。

実定法なかんずく憲法上の権利規定は文言の抽象性を免れえないが，憲法の場合，むしろその点にこそ積極的意味がある，つまり，人権は憲法に書かれているものに限定されないというのが近代立憲主義の基本的前提であり，文言の抽象性によって制定当時想定できなかった権利を発展させる余地が生まれるからである。そうした憲法の特性を無視して，憲法で保障される権利に「一義的明確性」を要求することは，それが改めて法律で具体化されない限り権利としては保障されないという明治憲法流の「法律の留保論」と同質の議論であるが，それは，日本国憲法における人権保障の原則に反する。

ドイツ法において論じられてきた，排他性を有する物権的権利として認められるための要件としての「一義的明確性」という要件は，歴史的産物であり，プライバシー権を物権的請求権の文脈で理解することに必然性があるわけではない。

財産権の場合でも，そもそも何を財産権保障の対象とするかについても一義的に明確であるわけではない。そのことは，憲法２９条２項が「財産権の内容は，・・・法律でこれを定める」と規定していることに端的に示されている。それにもかかわらず，財産権については，一義的に明確とはいえないから権利性は否定されると論じる見解は存在しない。

これらの点を踏まえると，プライバシー権が権利として承認されるためには，権利内容が「一義的明確性」を備えていることを要求する被告の議論には理由がない。

3　個人情報の法的保護（中島意見書２３～２９頁参照）

セキュリティ対策によって保護されるべき権利・利益の性格が問題になるが，被告国はプライバシー概念の不明確性を理由に，そのような権利・利益は存在しないと主張してきた。

このような主張が正当であるとすると，極端にいえば，住基ネット（という

公的制度）においてセキュリティ対策を施す必要はないことになるが，実際には，「相応の」セキュリティ対策がなされている。これは，被告国がそこに含まれる情報をもっぱら国や自治体自身の財であると解しているのでない限り，何らかの意味で，個人情報が保護されるべき権利ないし利益であると認めていることを意味するはずである。住基法上の「所要の措置」として，個人情報保護法制が念頭に置かれていることも，この点を裏付けている。

医療行為におけるインフォームド・コンセントについてと同様に，住基ネットにおいても，具体的危険の程度は事前に確実に予測することはできないので，情報保護の不可逆性の観点からみて，情報主体の同意なく個人情報を蓄積し利用すれば，情報取扱の基本原則に反すると考えるべきである。これは，住基ネットの運用を除けば，通常のサイトにおいて，個人情報の利用に際しては必ず利用目的を明示して同意を求めることに示されるように，今日ではコンピュータ・ネットワークの運営上当然のことと考えられている。この点は，個人情報保護法の定めるところでもあるが，仮に個人情報保護法が存在しなくても当然のことである。少なくとも諸外国ではそのように解されてきた。その一例が，ＯＥＣＤ８原則等のガイドラインである。また，民間企業の情報収集・利用にはこうした同意を求めながら，行政機関の場合にそれを不要とするのは一貫性に欠ける。

住基ネットのセキュリティ対策によって保護が意図されている権利・利益の種類や性格からして，それを保護するために必要な最低限度の条件，言い換えれば住基ネットの管理運営主体が果たすべき「責任」の内容は，情報主体に対し情報収集・利用への「同意」の機会を保障することにある。これは，ちょうどインフォームド・コンセントがそうであるように，憲法その他の制定法がそれを命じる以前に，われわれの社会が個人情報の取扱について暗黙のうちに作り上げてきた自生的なルールである。しかし，住基法は，これを制度化していない。

ここでいう「同意」は，医療における個別の患者ごとの治療とは異なり，全住民を対象とする一般的制度である住基ネットにおいては，個々の住民に対して個別具体的に求める必要はなく，暗黙の同意（＝拒否権の保障）で足りるであろう。しかし，国会が審議し立法を行えば住民の「同意」があったとみなすことは擬制がすぎる。ここでも，インフォームド・コンセントと同様に，少なくとも個人にネットワーク上での情報の収集・利用を「拒否」する機会を具体的に保障するのでなければ，「同意」があったとはいえないと考えるべきである。そうでなければ，個人の権利であることから必要とされる「同意」要件は全く形骸化してしまうことになる。

4　**プライバシー権と個人情報の保護，自己情報コントロール権の関係**（中島意見書２９～４０頁参照）

原判決は，「自己情報コントロール権」につき内容が不明確であるとして，本件はプライバシー権の問題として論じるべきだという見解をとっているが，「自己情報コントロール権」は，具体的文脈の下では必ずしも権利内容が不明確であるわけではない。本件訴訟との関係では，制定法の有無に関わりなく，本人確認情報の収集・利用に関し，情報主体の同意を要件とすべきであるという結論を導くことができるばかりでなく，個人情報保護法は情報主体の同意をかなり厳格に求めており，実際には，制定法上も個人情報の収集･利用については，同意の契機が重視されている。このことからも，自己情報コントロール権の権利内容として「同意」を重視することは決して一方的な主張ではなく，むしろ当然のことである。

これに対し，原判決は，プライバシー権を「個人的な情報をみだりに収集，開示されないという利益」と言い換え（８１頁），それを「みだりに」の要件との関係で公共の利益との比較衡量に付して，権利侵害なしとの結論を導いているが，これは，個人情報の保護は大切だが，「みだりに」収集･開示するの

でなければよいといっているだけのことである。そもそも，この原判決の定義自体，特定個人のプライバシー侵害事例を想定して作られたものであり，住基ネットのような全住民を対象とする巨大なシステムを念頭においてはいないのであって，ここでは，比較の対象とならないものが比較されており，これでは，１９６０年代までの抽象的な「公共の福祉」論による人権の制約と径庭ないといわざるをえない。

このことに明らかなように，原判決の議論には，住基ネットのような「ひとりでほっておいてもらう」だけでは，プライバシー権を保障したことにならないシステムにおいて，情報主体の権利を保障するという制度的視点が全く欠けている。情報主体の権利・利益を保護するためには，住基ネットという１００％安全であるとはいえないシステムを前提にする限り，情報主体の「同意」を求めることが制度的に不可欠である。

住基ネットにおける本人確認情報保護の観点から導出されたこの「同意」の要件は，他方では「自己情報コントロール権」の核心をなす要件である。それと同時に，これは原判決のいうプライバシー権を保障する―みだりに収集，開示されない―ための制度的担保でもある。原判決のプライバシー権と自己情報コントロール権の分離にもかかわらず，住基ネットの文脈では，プライバシー権，自己情報コントロール権，個人（識別）情報保護のいずれもが，概念自体は相互に異なるものの，それを保護するためには，情報主体の同意を要件とするという一点に帰着するのである。この限りで，自己情報コントロール権もプライバシー権も内容が不明確であるとはいえないのである。

5　ＯＥＣＤ８原則ならびにＥＵ指令と住基法（中島意見書４０～４７頁参照）

原判決の特徴は，ＯＥＣＤ８原則の趣旨を極めて形式的に理解している点である。例えば，目的明確化の原則との関係で住基法１条をあげるが，１条は総則規定であり，「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併せ掲げられている。こうした文言には，実際上いかなる内容でも含めることが可能であることは常識に属する。これで「目的明確化の原則」や「利用制限の原則」が充足されているというのであれば，それらの原則は無内容な原則ということになるだろう。実際，原判決は１条には「国及び地方公共団体の行政の合理化に資すること」も含むので，「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」と指摘している。また，「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」ているというが，利用事務は別表に委ねられ，提供先も要するに国内の地方公共団体全てに及んでいるのである。単に条文との対応関係を指摘すれば，それでＯＥＣＤ８原則を充足したことになるわけではない。

ＯＥＣＤ８原則における目的明確化の原則および利用制限の原則の趣旨は，個人情報を利用されている本人が，情報取扱者の使用目的や使用の実態を知ることができるように，遅くとも収集時点で利用目的を明確にし，かつ本人に対して利用目的を知らせるべきことを求める点にある。原判決は，一般的抽象的な文言でも，「目的」を語ってさえいればそれで利用目的を特定したことになると考えるようであるが，それは「目的の明確化」という日本語の日常的な用法といえない。「行政の合理化」という「目的」に含まれない事柄は，行政と無関係のものだけであろう。

加えて，住民基本台帳法は「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あるから，法律で定めさえすれば，利用・提供の対象を拡大することができるようになっている。収集時点での目的明確化は，この点で有名無実化しているのである。実際，当初の９３であった利用事務は，現在までに２７５事務に拡大されている。そして，いわゆる電子政府構想の下では，１万６千件以上の事務に利用することが予定されているとも伝えられている。これに加えて，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だろう。しかし，一般市民向けの有斐閣版小六法では，利用事務を規定しているはずの別表は，「(略)」とされていて，その内容を確認できないのである。インターネット経由で別表を入手することはできるが，現に別表をみれば分かるように，一般市民が利用対象を把握することは極めて困難であり，実際上は本人の同意や利用をめぐる異議申立の機会は保障されていないに等しい。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，告知は本人が理解できるように行うことを求めるＯＥＣＤ８原則における個人参加の原則も無視されていることになるであろう。

ちなみに，法令上の規定に基づき情報の提供を受けた機関も同様の義務に服するが，これも裏を返せば，情報受領者は法律や条例で定める目的の範囲内であれば，提供を受けた情報をさらに他の機関に提供できるということである。その結果，利用･提供の対象は拡大されうる。これもまた，本人の同意なしに利用・提供を認める点で，前記原則の趣旨に反する。

以上の点からすると，原則が形骸化されていても，法律の文言にうたわれていればそれで充足されたという立場をとるのでない限り，住基法はＯＥＣＤ８原則の定める目的明確化の原則ならびに利用･提供制限の原則を充足していないと評価せざるを得ない。

なお，原判決はＯＥＣＤ８原則の法的拘束力を否定するので，そもそもＯＥＣＤ８原則との対応関係を論じる必要はないはずであるが，ＯＥＣＤ８原則の法的拘束力を否定するのも誤りである。なぜなら，ＯＥＣＤ８原則は１９６６年に国連総会で採択され，日本も１９７９年に批准した「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と位置づけられているからである。同条は，プライバシー権を一般的に保障した規定であるが，もちろん日本政府はその遵守義務を負っている。その具体化としての意味を持つＯＥＣＤ８原則の特徴は，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」(minimum standards)を示している点にある（これは，Annex to the Recommendation 6に明記されている)。このことは，ＯＥＣＤが経済の国際的な共存と発展を目的とする国際機関であることを考えれば，容易に理解できるであろう。ＯＥＣＤ加盟国である日本がそ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らないのである。

また，ＥＵ個人データ保護指令は，更に一歩進んで，ＥＵ指令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ない。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，政府は同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る必要がある。

以上の点から，ＯＥＣＤ８原則およびＥＵ個人データ保護指令は日本と無関係でありえず，政府はそれらが求める個人情報保護の水準を充足する法制度を設けなければならない立場にあるといえる。例えばＯＥＣＤ８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る。仮にそれらが「基本的人権」と観念できないとしても，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，その理由を説明する責任を国の内外に対して負うことは当然である。他方，政府が，これらの国際的準則を充たした国内法制度が存在すると主張する場合でも，その内容に合理的な疑問が提起された場合には，同様の説明責任を負っているといわなければならない。

ちなみに，ＥＵ指令は，ＯＥＣＤ８原則をさらに精緻化したものであり，住基法がＯＥＣＤ８原則を充たしていない以上，さしあたり，さらにＥＵ指令を充足しているかどうかを論じる必要はない。

6　憲法上のプライバシー権と住基ネット（中島意見書４７～５４頁参照）

憲法上，プライバシー権を保障することに否定的な立場をとる見解としては，

①説　そもそもプライバシー権は私法上の人格権に基づいて認められるもので，憲法上の権利ではない。

②説　憲法に明文規定がなく，一義的に明確な内容を有してもいないので，憲法上の権利としてプライバシー権を観念することはできない。

③説　憲法上保障されるプライバシー権は，私的領域にのみ認められ，公的領域においては原則として認められない。

④説　憲法上，プライバシー権は公的領域においても認められるが，公共の福祉の制限を受ける。

などが存在する。

①説は，プライバシー権侵害は私人間にしか生じないという立場である。一見すると，①説と③説は同一の見解であるようにも思えるが，③説は私的活動領域におけるプライバシー権侵害が国家によって行われる可能性があることを認める点で，①説と異なるプライバシー権の理解を採用している。ただし，私的活動領域における権利侵害しか認めない点では，両者は同一である。

プライバシー権は，①説が説くように，もともと私人間における「私的領域」の保護を念頭において，私法上の人格権の保障という観点から論じられてきたという歴史的経緯がある。しかし，これはプライバシー権論の歴史的沿革の問題にすぎず，国家が私人のプライバシー権を侵害することはありえないと考えることは事実に反する。一例をあげれば，電話盗聴がそれである。アメリカ憲法上の例でいえば，修正４条が禁じる不当な捜査・押収という刑事手続上のプライバシー問題がそれであるが，アメリカ合衆国においては，国家の私的領域への侵入との関係で，憲法上のプライバシー権が明確に観念されている。もっとも，日本では，この種の事案は憲法３１条以下の適正手続保障の文脈で論じられることが一般的である。刑事手続に適正さを求めることの背後にプライバシーの観念が存在する以上，アメリカ合衆国の判例法理は，日本にも妥当する。今日では，プライバシー権を私法上の人格権に限定して理解し，憲法上のプラ

イバシー権の存在を一般的に否定する理由はないといわなければならない。

なお，②説の明文規定の不存在と一義的明確性の欠如という否定論の論拠については，２項で述べたように権利性を否定する論拠とはならない。

また，住基ネットという個別具体的な文脈においては，情報主体の同意という観念が制定法以前に導出でき，それが住基ネットという国家の設営したシステムの下でのプライバシー権保障の核心をなすことも前述のとおりである。これを「人格権」に包摂するかどうか，あるいは「自己情報コントロール権」と呼ぶかどうかは言葉の問題でしかない。問題はしかし，これを憲法上の権利と位置づけることができるかどうかである。

③説は，憲法上のプライバシー権が保障されるのは私的領域のみであるとし，その典型例の一つは，刑事手続上のプライバシー権問題である。憲法は，国家が個人の私的領域に踏み込むことを原則として禁じるが，住基ネットのような公的領域においては，プライバシー権を保障していないというのである。この立場は，そのように論じる理由として「私的領域の限界が同時に公的領域の限界でもある以上，独自の線引きを許すならば，社会生活そのものが成り立たなくなるおそれがある」ことをあげる。

ここでの問題に密接に関わると思われる点に関連して，最高裁昭和５６年４月１４日判決（民集３５.３.６２０）（前科照会事件）は，前科は公的情報であり，私的領域の問題ではないにもかかわらず，名誉権，実質的には伊藤裁判官が指摘するようにプライバシー権の成立を認めている。これは，公的領域においても憲法上のプライバシー権が成立し得ることを認めた一例である。

ちなみに，③説の立場からも「具体的にどこまでを私的な生活領域の問題として保護すべきかは，社会の慣習や通念によって定まる部分が大きい」と指摘されており，前述したように，住基ネットのようなコンピュータ・ネットワークの場合，そうした観点から生活領域の問題と解する余地も充分にある。また仮に，国の主張するように住基ネット自体は公的領域に属するものだとしても，

１００%安全とはいえず，ＯＥＣＤ８原則等の国際的基準を充たしているかどうかも疑わしい制度について，およそプライバシー権の保障がありえないと論じることが「社会通念」に合致するかどうかは，大いに疑問の余地がある。

そもそも憲法問題は，多くの場合，公的領域において発生する。ここでいう「公的領域」は，日本国憲法の下では，民主主義の観念に合致するように制度化されていなければならないはずである。もちろん，「民主主義」もまた多義的観念であり，いかなる状態が民主主義に合致するかは必ずしも明らかであるわけではない。しかし，一般論としていえば，政府が個人の情報を自由に収集し利用することができる社会は，管理社会ないし監視社会と呼ばれることはあっても，民主主義社会と呼ばれてはこなかった。③説のように，行政目的での住民情報の収集･利用は公的領域に属する者であるから自由であると論じるとすれば，論理的にはこうした社会を許容することになってしまう。公的機関の情報収集能力が飛躍的に高まった今日の社会で，近代的な―かなりの程度に独自性の強い―公私二分論に基づいて，公的領域に関する憲法上のプライバシー権を否定することが憲法論として適切であるかどうかは，慎重に検討する必要がある。もっとも，これに対しては，そのように自由な収集･利用を住基ネットは認めていないという反論がなされるだろうが，前述のように，制度上，目的明確化の原則や目的外利用の禁止が極めて形式的にしか担保されていない点で，説得力に欠ける。

したがって，プライバシー権の出自が私的領域にあるからという理由だけで，私的領域にとどまっている者に，公的領域におけるプライバシー権を保障しないことの実質的理由は，国家の利益を偏重する「公共の福祉」論くらいしかないことがわかる。

④説は，住基ネットが公的領域に属することを「公共の利益」と等置する。もちろん，実際には行政の効率性論に代表される具体的な公益を挙げるだろうが，効率性だけで人権制限が正当化できるのであれば，憲法は無用の長物であ

る。行政コストの削減は，それ自体としては重要な公益目的ではあるが，人権保障にはコストがかかる場合があり，憲法はそのことを念頭に置きつつなお，さまざまな権利を保障しているのである（効率性だけを考えるなら，刑事手続の適正保障など必要ない）。加えて，住基ネットがコスト面も含めて効率的であるかどうかについては，自治体の負担や住基ネットの稼動に要している費用，住基カードの普及率の低さなど，多くの疑問が投げかけられていることは周知のとおりである。

また，現代においては，何が公益であるかを確定することが困難であるからこそ，ＯＥＣＤ８原則や，それに体現される「自己情報コントロール権」のような，それ自体としては手続的性格の強い権利の保障が求められていることも忘れるべきではない。さらにいえば，国家＝公益という図式は現代の民営化論や規制緩和論の下で自明のものといえなくなっており（従来，国家が担ってきた業務は「公務」と理解されてきたが，今日では「民にできることは民に」というスローガンの下で，民間企業に業務の遂行が委ねられることは少なくない），他の分野では政府自らがそのことを強調してやまない点である。それにもかかわらず，ことが住基ネットに関係すると，とたんに国家的利益を語って怪しまないというのは，一貫性に欠ける態度というべきである。こうした矛盾は，行政機関個人情報保護法と個人情報保護法とで，情報取扱者に課される義務の程度が異なることにも現れている。

４項において，住基ネットの文脈においては，プライバシー権保障の核心となる要件として，ＯＥＣＤ８原則やＥＵ指令を引き合いに出すまでもなく，情報主体の同意権の保障が導き出されることを述べたが，これは住基ネットにおける個人情報という人格的利益を保護するための最低条件であるから，単なる一般的公益性ではなく，やむにやまれぬ国家的利益の存在が証明されない限り制限できない権利ないし利益といえる。しかし，国は住基ネットについて，一般的公益性以上の正当化理由を示してきていない。一般的公益の存在だけで住

基ネットの運用を正当化できるのは，およそ憲法上のプライバシー権を論じる余地がない場合であるが，その点に関する国の主張に理由がない。

7　結論（中島意見書５４頁参照）

杉並区は，住基ネットへの参加および不参加を希望する住民の要望を踏まえて，参加を希望する者の本人確認情報だけを東京都に送信しようとした。杉並区の措置は，本人確認情報の収集･利用についての住民の同意を尊重する点で，憲法上のプライバシー権（自己情報コントロール権）保障を意図したものといえるが，東京都は住基法の定めに反することを理由に今日まで受信を拒否してきている。仮に東京都が杉並区の選択的送信を受信するならば，杉並区との関係において住基ネットの運用は合憲といえるが，東京都が受信を拒否するのであれば，憲法上の権利の保障を実現しようとする自治体の活動を阻む点で，その運用は違憲であるといわざるをえない。

第2　住基ネットの総合的な安全性の欠如

1　はじめに

横浜市本人確認情報等保護審議会（以下「横浜市・審議会」という。）は，平成１８年４月２５日付答申（乙２０）において，「住基ネットの安全性は，稼働当初と比較し格段に高まっており，現時点において総合的に見て問題はないと判断できる。」としているが，これに関し，杉並区長より杉並区住民基本台帳ネットワークシステム調査会議に対して，平成１８年９月１５日に諮問(甲７０）が出され，これを受けて，同調査会議は，同年１１月１５日に「住民基本台帳ネットワークシステム調査会議第四回報告書」(以下「調査会議報告書」という。甲７１）を提出した。以下のとおり，調査会議報告書が指摘するように，現時点においても，住基ネットの総合的な安全性を確認することはできないといわざるを得ない。

2　制度面

（1）個人情報保護法制上の不備

住基ネットの導入に際しては，個人情報やプライバシーへの懸念から，改正住基法の附則１条２項で，「この法律の施行に当たっては，政府は，個人情報の保護に万全を期するため，速やかに，所要の措置を講ずるものとする」と定め，当時の小渕首相も，住基ネットの実施に当たり，「民間部門をも対象とした個人情報保護に関する法整備を含めたシステムを速やかに整えることが前提であると認識いたしております」と答弁した（平成１１年６月１０日開催の第１４５通常国会衆院地方行政委員会での答弁）。

それ故，前記附則の「所要の措置」とは，事柄の性格上，行政機関を中心とした個人情報保護法制が整備されることである。

この点，個人情報保護の関連法案が平成１５年の通常国会で可決成立したが，これにより前記附則の要件が満たされたと考えるのは困難である。

調査会議報告書（甲７１）では，次のとおり指摘している（３～４頁）。

「まず留意が必要なことは，附則で求められている個人情報保護法制とは，何よりも住基ネットの実施に密接に関わる法制を意味し，その主要な対象は，住基法に定める個人情報保護措置の一般法としての性格をもつ行政機関個人情報保護法であると考えられることである。なお，主として民間を対象とする個人情報保護法は，小渕答弁にもかかわらず，理論的には住基ネットの制度と主要かつ直接的に関係するというものではなく，その意味で住基ネット稼働の条件としてこの法律の制定を求めることは妥当とは言えないが，本人確認情報の民間利用など，関わりをもつ局面もある。

第二に，附則が求めているのは，個人情報保護法という名前の法律が制定されさえすればその中身は問わないということでは断じてない。そこで求められている個人情報保護法制とは，個人のプライバシーと個人情報をきちん

と保護できる仕組みを備えた本来の保護法制でなければならない。

この点で，成立した関連法は，表現やメディアを含め民間に一律の法の網をかける一方で，官に対して厳格な規制を及ぼせないなどの重大な問題を種々抱えた欠陥法であって，附則の実質的要件を満たしていないといわざるを得ない。具体的には，成立した行政機関個人情報保護法は，本来行政機関に要請される，民間より厳格な規制が欠如し，民間規制法としての性格をもつ個人情報保護法よりも緩やかな規律しか課していないところさえある。

例えば，法律では，「相当の関連性」があれば個人情報の利用目的の変更が広く認められており（３条３項），「相当な理由」があれば目的外の利用と提供も広範に許容されている（８条２項）。また，国の安全や外交等に関する個人情報ファイルや犯罪捜査と公訴の提起・維持に関する個人情報ファイルを含め，個人情報ファイル簿の作成・公表に数多くの例外を認めているし（１１条２項），個人に関する情報，法人に関する情報，国の安全に関する情報，公共の安全に関する情報，国の機関の審議・検討に関する情報，国の機関の事務・事業に関する情報など，不開示情報の類型が設定され，本人情報の開示・訂正等の権利が及ばない例外を広範囲に列挙している（１４条）。さらに，民間にさえ課している適正取得のルールが定められておらず，当初の法案への修正で加えられた規律違反への罰則も，コンピュータ処理された個人情報ファイルの提供，不正目的での個人情報の提供・盗用，職権濫用による個人の秘密情報の収集など最小限にとどまるし（５３条～５５条），思想・信条等に関するセンシティブ情報の収集禁止規定も設けられていない。加えて，法の運用をチェックする第三者機関の設置も，訴訟が起こせる裁判所を広げる訴訟管轄の特例措置も，定められていない。

これでは行政機関を厳格に規制し，市民による自己情報のコントロールを徹底した仕組みとは程遠く，求められる個人情報保護法制の水準を満たしているとはとうてい言えない。なお，民間を対象とする個人情報保護法も，立

法事実の丁寧な精査，検証を経て，緊急度や重要性の高い特定領域・分野での個別法の制定ではなく，民間に一律の法規制を課すという方式がとられているため，官が立ち入ってはならない市民の表現やメディアの取材・報道に不当に介入するなど一方で過剰に民間の活動を規制するとともに，他方で政府に準じて厳格な規制が求められる通信，信用・金融，医療，教育などの領域・分野で過少な規制しか加えられず，本来の要件を満たす法制となっているとは言い難い。

このように見ると，個人情報保護の関連法は制定され，その意味で附則の形式的要件はクリアーされたといえるものの，その実質的要件はいまだ満たされたと評価することは困難である。したがって，住民の個人情報保護に責任を担う自治体は，真に個人情報の保護を果たせる確固とした法制が整備されていないことを理由にして，住基ネットに参加しない立場をとることは当然であり，もとより適法な選択である。」

（２）監視社会化の流れの中での位置付け（名寄せの危険性）

また，調査会議報告書（甲７１）は，住基ネットについて，次のとおり，名寄せの危険性のある制度であることを指摘している（２９～３０頁）。

「住基ネットのシステムは全国民の巨大なデータベースの構築を意味し，国家による市民管理の重要な基盤的制度としての役割を担うものである。

住民票コードをいわばマスターキーとして，他でデータベース化されている市民のさまざまな情報，たとえば税の捕捉に必要な所得や取引行為，社会保障の受給関係，教育歴，運転免許やパスポート，出入国情報や車の所有などから，果ては犯罪歴，病歴に至るまでのもろもろの個人情報が照合され，突合せられ，結合され，番号一つで市民の生活が文字通り丸裸にされるおそれが強いからである。

また，大量の情報を記憶できるＩＣチップ内蔵の住基カードはさまざまな目的で利用されることが可能で，現在は希望者だけに交付されるが，将来利

用が広がれば多くの住民がこれをもつことを事実上強いられかねないし，もっとも広汎な身分証明書として活用され，国民が携行を義務付けられる事態さえないとは言えない。」

「テロ対策や外国人対策などを名目にさまざまなデータベースが構築され，民間や外国も含めそうしたデータが交換され，もろもろの行政の利用が広げられ，さらにそうした情報の統合化の方向が確認できる。

そういうなかで住基ネットが各種データベースを繋ぎ，統合を促進する上で基盤的役割を担う可能性が高い。

にもかかわらず，こうした過剰な国民管理を防ぐ手立ては改正住基法にも行政機関個人情報保護法にも存在しないと言わなければならない。金沢地裁判決が示しているように，改正住基法は目的外の利用・提供を禁止しているが（３０条の３４），照合・突合せ・名寄せ・データマッチングがここでの利用・提供になるかどうか不明確だし，これへの違反に対する罰則も，第三者による監視の仕組みも欠如しているので，データマッチングへの有効な規制は法定されているとはとうてい言えない。また，行政機関個人情報保護法にはデータマッチングを明示的に禁止する規定も第三者によるチェックシステムもないだけでなく，利用目的の変更や目的外の利用・提供について行政の裁量を広く認めているので，実効的な規制を加えるのは困難である。」

「データマッチングについてはそれを行う主体が存在していない旨の議論もあるが，法で明確な禁止と歯止めがない以上，さまざまな行政機関がそれを行う主体となりうることこそが問題なのである。また，さまざまな行政上の統合にあわせ，必然的に統合的な管理主体が今後生まれていくことが示唆されているし，そうなるのは必定である。」

以上のような「市民がその行動や生活につき公権力等による監視・統制に系統的，日常的にさらされる社会」（甲７１　２６～２７頁）である監視社会における住基ネットの位置付けからすれば，名寄せによる過剰な住民管理

によるプライバシーと人間の尊厳の深刻な侵害をもたらす危険性が高いと言わざるを得ない。

（3）自己情報コントロール権の制度的保障の本質的欠如

さらに，調査会議報告書（甲７１）は，住基ネットでは自己情報コントロール権に対する制度的な保障が本質的に欠如していることについて，次のとおり指摘している（４～５頁）。

「全国民の個人情報をコンピュータで中央集権的，一元管理する住基ネットのシステムは，大量の個人情報が漏洩され，不正使用される危険を格段に高めるだけではなく，個人の情報が過度に官に管理され，乱用される危険も大きい。

何しろ一億数千万人分の国民すべての基本情報がコンピュータネットワークで繋がれ，全国的，一元的に管理され，運用されることになるので，もしこれが漏れたり，不正に使用されるとすればその被害の規模と程度は計り知れない。私たちの大量の個人情報が商売の道具として利用されたり，不正に悪用されたらと考えると，ぞっとせざるを得ない。現にアメリカでは，官民で広く利用されてきた社会保障番号について，他人の番号を盗用した犯罪が多発し，深刻な社会問題となっている事実が報告されている。

さらに住民票コードとして私たちに番号が付され，全国民の巨大なデータベースが構築されるということは，私たちの情報が官により過剰に管理され，監視される危険を格段に高める。将来，住民票コードをいわばマスターキーとして，他でデータベース化されている私たちのさまざまな情報，たとえば，税の捕捉に必要な所得や取引行為，社会保障の受給記録，教育歴，運転免許や車の所有などから果ては犯罪歴，病歴に至るまでの諸々の個人情報が結合され，番号一つで私たちの生活が丸裸にされるおそれがある。

また，大量の情報を記憶できるＩＣチップ内蔵の住基カードは，住民票の広域交付などのほか，福祉，公共施設利用，印鑑登録など，さまざまな目的

で利用できるとされている。これは建前上希望者だけに交付されることになっているが，利用できるサービスが広がれば，これをもっていないと不便この上ないということになり，多くの市民がこれをもつことを事実上強いられかねない。さらには，もっとも汎用的な身分証明書として活用され，果てはパスポートの国内版として国民がその携行を義務づけられる事態さえないとは言えない。」

「こうした住基ネットがはらむ深刻なプライバシー侵害への危険を考慮すると，たとえ十分な個人情報保護法制を用意したとしても，そもそもこうした仕組みがプライバシーや人間の尊厳，地方自治などの原則を含む日本国憲法に相応しい制度かどうか疑念が生ずる。もし何らかのネットワークが必要であるとしても，住基ネットのような中央集権的なシステムを強制すべきではなく，個人や地方の主体性を最大限尊重する緩やかな自治的，分散的なシステムを下から積み上げていく方式が本来望ましいだろう。

万が一住基ネットの仕組みを前提とするとしても，プライバシー権への十分な配慮が不可欠である。憲法はプライバシーの権利を人権として保障しており（１３条），この権利は，特に国や自治体など官に対しては，市民の自己情報のコントロール権として構成され，厳格な規制を官に加える法理として理解される必要がある。

住基ネットの実施については，個人情報に及ぼす深刻な危険にもかかわらず，その制度の意味や趣旨について市民は十分な説明を受けてこなかったし，制度上も，自分に番号を付され，その情報がコンピュータで全国的，一元的に管理され，行政事務の処理に際し広く共同利用されることつき同意を求められ，その意思を表明し，選択権を行使できるなどの仕組みを欠き，自己情報のコントロール権の制度的保障が本質的に欠如している。プライバシー権の充足という観点からは，住基ネットへの参加・不参加の選択権を個人に保障する制度を構築することが欠かせない。にもかかわらず，住基ネットへの

参加を個人に無理やり強制することは，プライバシー権を侵害し，個人の尊重と基本的人権の精神に根本的に背馳すると言わなければならない。

また，政府が主張するように住基ネットは国のシステムではなく，あくまでも自治体共同のネットワークであるとすれば，住民の個人情報の保護に責任を担う自治体は，自らの主体的判断で住基ネット参加の是非を判断できる機会を保障すべきである。この結果として自治体が不参加を決断したり，個々の住民の選択に委ねる方式を採用したとしても，これは憲法が保障する地方自治権（第八章）の正当な行使と言える。政府は，自治体の離脱や個人の選択制を違法と決め付けるが，それを保障しない住基ネットこそ違憲の疑いが強いと言わなければならない。」

3　技術面（物理的セキュリティについて）

住基ネットには，さまざまなセキュリティ上の脆弱性が現存しており，それらの脆弱性によって，地方自治情報センターのサーバーに保存されている全国民の住基データは外部に流出する可能性がある。

この点について，調査会議報告書（甲７１）が，次のとおり指摘している（８頁）。

すなわち，２００３年に長野県で行われた住基ネット侵入実験に実際に携わった米 SecurityLab の Ejovi　Nuwere（イジョビ・ヌーワー）氏は，「住基ネットにはセキュリティ上の問題がいくつか有るのだ。良いニュースは，技術上の問題は簡単に解決できるということだ。しかし住基ネットにおける最大の問題は，技術上にあるのではなく，問題が存在することすら認められない総務省にあるのだ」と述べている。具体的にどのような「セキュリティ上の問題」だったのかは開示されていないが，この発言には，第１に，実際に侵入実験に携わった専門家が，住基ネットにセキュリティ上の問題があったことを明確に認めている点，第２に，総務省はこうしたセキュリティ上の問題を公にすることを認め

ていない点で重要性があると指摘している。

また，脆弱性について，次のようにも指摘している（１０～１１頁)。

「『ASAHI パソコン』編集部は，長野県から侵入実験を委託された吉田柳太郎氏の証言から，同県の住基ネット侵入実験に使われた脆弱性は，「MS ０３-０２６」だったことを突き止めている。この「MS ０３-０２６」脆弱性は，実験が行われる以前の２００３年７月１７日にすでに公開されていたもので，実験当時は周知の脆弱性だった。マイクロソフトは実験当時にはすでに「MS ０３-０２６」脆弱性に対応する修正プログラムを配布していたのにも関わらず，住基ネットのＣＳサーバーには適用されていなかったのである。この点について記事は，「ＬＡＳＤＥＣによれば，ＣＳサーバーの修正プログラムは，いきなり適用すると誤作動する危険があるため，十分な動作確認後に導入することになっている。そのため，昨年７月ごろから後の修正プログラムは，実験時点では適用されていなかったものがかなりあるという」と指摘している。運用上の問題から，脆弱性がそのまま放置されているケースが少なからずあるということである。つまり住基ネットは現在も，他の脆弱性が放置されている可能性はゼロではない。またこうした脆弱性の適用情報について，総務省とＬＡＳＤＥＣは一切情報公開していない。」

「長野県の侵入実験の後，２００３年１０月１０～１２日に総務省が品川区の協力で実施した「住基ネットに対するペネトレーションテスト」では，ＦＷ②，ＦＷ③，庁内ＬＡＮ内のＣＳ端末の三カ所に対して，侵入実験が行われた。実際にテストを行ったのは，米クロウ社（Crowe Chizek and Company LLC）である。この実験では，三カ所のいずれも侵入に成功せず，脆弱性も見いだせなかったとされている（注５)。

だがこの直後，１０月１６日にはマイクロソフトから「MS ０３-０４１」「MS ０３-０４２」「MS ０３-０４３」「MS ０３-０４４」「MS ０３-０４５」という五種類の脆弱性が公表され，それぞれに対応した修正プログラムが公開されて

いる。これら脆弱性はほぼ毎月のように断続的に公表されており，侵入実験でこれらの脆弱性の存在がどの程度確認されたのかは，総務省の結果報告では明らかにされていない。

ＬＡＳＤＥＣのサーバーは一元管理され，こうした修正プログラムが適用されていたとしても，全国のすべての自治体に置かれているＣＳサーバーに関しては，これらの修正プログラムがどの程度適用されていたのかは，推測の域を出ることができない。だが前掲の『ASAHI パソコン』誌の記事から推測すれば，修正プログラムが全国のすべての自治体のＣＳサーバーに導入されていたとは考えがたい。最新の脆弱性を利用すれば，地方のＣＳ端末には侵入可能だった可能性は現実問題として，きわめて高いのである。」

4　運用面

（1）はじめに

仮にこれら「外部からの侵入」の危険性が完全に排除されたとして，それで住基ネットは安全であると断言することはできない。

この点について，調査会議報告書（甲７１）は，次のとおり指摘している（１１頁）。

「住基ネット情報の漏洩は，

① 外部の者による情報漏洩－１（インターネット経由でファイアウォールから侵入する不正アクセス）

② 外部の者による情報漏洩－２（外部のものが自分の身分を騙るなど，何らかの人的方法によって不正侵入したり，あるいは物理的な盗難によって情報が漏洩するケース）

③ 内部の者による情報漏洩（組織に恨みを持ったり，金銭的理由で行われる内部犯行）

④ 内部の者による情報漏洩（紛失，Ｗｉｎｎｙ利用などの誤って起こし

た事故)

の四つのルートが存在するからである。

したがって安全性を計測できるのは，侵入実験（ペネトレーションテスト）だけではない。ペネトレーションテストで計測できるのは，上記の四種類のうち，「①外部の者による情報漏洩－１（インターネット経由でファイアウォールから侵入する不正アクセス)」だけでしかないからである。

セキュリティは，他の②～④の可能性も含めて総合的に判断されなければならない。」

さらに，次のようにも指摘している（１３頁）

すなわち，横浜市の答申（乙２０）及び住基ネットキーパーソンである大山教授のいずれもが，

（A）　ＩＣカードとパスワードによって操作者の限定を行っている

（B）　操作履歴とアクセスログで，いつ誰が住基ネットを使用したのかがわかる

という二点を中心に不正アクセス以外の不正使用防止を可能にするとしている。だがそれらが絶対的に，前掲の②～④の不正使用を防止できるかどうかといえば，現実にはかなり限定的と言わざるを得ないという。

以下，詳述する。

（２）外部の者による情報漏洩－２（②）

ア　ソーシャル・エンジニアリング手法による漏えい

調査会議報告書（甲７１）は，「②　外部の者による情報漏洩－２（外部のものが自分の身分を騙るなど，何らかの人的方法によって不正侵入したり，あるいは物理的な盗難によって情報が漏洩するケース)」について，次のとおり指摘している（１４頁)。

「まず②の「外部の者による情報漏洩－２（外部のものが自分の身分を騙るなど，何らかの人的方法によって不正侵入したり，あるいは物理的な

盗難によって情報が漏洩するケース)」についてであるが，ひとつの手法に，ハッカーの世界で言う「ソーシャル・エンジニアリング（社会工学)」がある。インターネット上の百科事典である「ウィキペディア（ＷＩＫＩＰＥＤＩＡ）日本語版」は，ソーシャル・エンジニアリングの項目を以下のように説明している（注７）。

「ソーシャル・エンジニアリングは，人間の心理的な隙をついて個人が持つ秘密情報を聞き出す方法のこと。ソーシャル・ワークとも呼称される。

元来はコンピュータ用語で，コンピュータ本体に被害を加えることなく，パスワードを入手し不正に侵入（クラッキング）するのが目的。この意味で使用される場合はソーシャルハッキング，ソーシャルクラッキングとも言う。以下のような方法がよく用いられる。

- システム管理者などと身分を詐称してパスワードを聞きだす
- 本体を操作する人の後ろに立ち，パスワード入力の際のキーボード（もしくは画面）を凝視する。
- パスワードが書かれた紙を盗み見る。

現在はパスワードだけではなく，クレジットカードなどの番号を盗んだり，家族に詐称して金を振り込ませる（オレオレ詐欺）など詐欺の手口にも使われる。

キャッシュカードについて暗証番号を聞き出し，盗難カードや偽造カードで不正出金を行う手口にも用いられる。電話で連絡を取り，

- 警察を名乗り，逮捕した不審者が持っていたカードの確認を行うために暗証番号を聞き出す
- 信販会社を名乗り，手違いで余分に引き落とした決済金を口座に返金するために暗証番号を聞き出す

個人情報を聞き出す為にも用いられる。電話で連絡を取り，

・ 学校の同級生の親族を名乗り，本人や他の同級生の住所や電話番号を聞き出す

・ 宅配便を名乗り，住所が良く判らないという口実で正確な住所を聞き出す」

２００６年３月２８日，北海道斜里町で町役場の職員のパソコンから，業務資料が誤ってファイル交換ソフト「Ｗｉｎｎｙ」のネットワークに流出する事故が起きた。

この中には，住基ネットで使うＣＳ端末の古いパスワードや，操作マニュアルなどが含まれていた。」

また，平成１８年３月２９日に同町が配布した追加の報道発表資料によれば，「業務操作マニュアルの中にパスワードが記載されていたもの」が含まれていたという。

調査会議報告書（甲７１）は，この「業務操作マニュアルの中にパスワードが記載されていたもの」とはどのようなものであったかについて，次のとおり指摘している（１５～１７頁）。

「Ｗｉｎｎｙに流出した資料はほぼ永久に消滅しないため，現在もＷｉｎｎｙネットワーク上で収集することができる。ここでは，JCA-NET が実際に収集し，ホームページ上で公開している斜里町の漏洩情報の中から，業務操作マニュアルをプリントアウトしたものを（別紙２）（別紙３）に示す（注９）。

（別紙２）に表示されている「shiretoko」というパスワードは，斜里町の報道発表資料には「平成１５年当時のもので，現在使用されていないもの」とされている。だが重要なのはこのパスワードではない。重要なのは，電源を投入後，どのような画面が表示され，その表示に従ってどのような

手順を踏んで手続き（プロシージャ）を進行させれば良いのかということが，事細かに説明されている点である。これらのプロシージャは，ハッカーによるソーシャル・エンジニアリング手法の重要な手がかりとなる材料であって，ハッカーは前掲のＷＩＫＩＰＥＤＩＡの説明にあるように，あらゆる方法を採って「内部の人間」を騙り，内部の人間からパスワードなどさまざまな情報を得ようとする。

（別紙２）では，【配布物メンテナンス確認】という画面が出た場合，戸籍住民係係長（Ｗｉｎｎｙ上に流出したファイルでは実名が含まれているが，JCA-NET が公開した資料では実名の部分は黒塗りされている）に電話をして，「ＣＳ電源を立ち上げましたら，配布物メンテナンス画面の実行と延期が出ましたが，どちらを選べばいいですか？」と聞くという手順が詳細に書かれている。

これらの手順は，ソーシャル・エンジニアリング手法を駆使するハッカーに悪用される可能性がある。ＣＳ端末は全国の自治体に一律に導入されており，操作手順も全国で標準化されている。となると戸籍住民係の係長名を調べた上で，庁内の電話から架電して「ＣＳ電源を立ち上げましたら，配布物メンテナンス画面の実行と延期が出ましたが，どちらを選べばいいですか？」と伝えれば，相手係長は間違いなく架電者を役所内部の人間と信じるだろう。その上でさらに細かい操作手順などを聞いたりすれば，詳しい情報を入手することは可能なのである。

また斜里町の報道発表資料には，「住基システムは特定の端末機は指定された職員のみが使用できることになっており，このためにシステムを作動する端末ごとのパスワードと，操作者の識別カードが必要であります」と書かれている。横浜市・審議会の答申や大山教授のコメントでもＩＣカード（識別カード，端末操作用カード）が必須であり，このカードがなければアクセスは不可能であるため，仮にパスワードだけが漏れたとしても

不正アクセスされる心配はないとされている。

しかし従来，住基ネット以前から存在していた各区市町村の住民基本台帳システムでは，端末操作にＩＤとパスワードを使ってアクセス管理をしていたのにもかかわらず，事実上このシステムが形骸化していたことは，すでに各方面から指摘されている。

・　職員間でＩＤを共用していた

・　ＩＤ，パスワードを端末のモニタ上に紙に書いて貼り付け，運用していた

などのケースが多数報告されている。また住基ネットに関しても，同様の報告がなされている。２００４年１２月１７日に開かれた福岡地裁での住基ネット差し止め訴訟の裁判期日で，住基ネットの第一次運用開始の時に，北九州市八幡東区役所市民課に勤務し住基ネットの職員研修を受けた須崎和幸氏と，大阪府松原市役所に１７年間勤務した経験を持つ自治体情報政策研究所の黒田充氏が原告側証人として出廷した。このなかで，須崎氏は，セキュリティ・ポリシーの徹底などのセキュリティ対策の教育が現場ではほとんどなされていないことや，住基ネット端末を操作するのは正規職員よりも民間の派遣社員の方が頻度は高く，しかも操作にあたって必要なパスワードは，誰でもすぐに見えるところに置いてあるという実態を証言している（注１０）。

こうしたずさんな運用は一部のケースかも知れないが，しかし住基ネットは全国約１８００（平成１８年１１月現在）の自治体のＣＳサーバーがＬＡＳＤＥＣの中央サーバーに接続され，どの自治体からもＬＡＳＤＥＣのすべての住基データがダウンロードできるという仕組みである。となると，こうしたずさんな運用が行われている一部自治体から，全国の住基データがまとめて流出する危険性は，残念ながらきわめて具現的であると言わざるを得ない。」

イ　物理的盗難による情報漏洩

また，調査会議報告書（甲７１）は，「②　外部の者による情報漏洩－２（外部のものが自分の身分を騙るなど，何らかの人的方法によって不正侵入したり，あるいは物理的な盗難によって情報が漏洩するケース)」については，次のとおり指摘している（１７～１８頁)。

「上記のようなソーシャル・エンジニアリング手法による漏洩の危険性以外に，物理的盗難による情報漏洩もある。

２００２年１２月には，福島県岩代町で，住基ネットのデータを収めたデジタルテープが盗難される事件が起きている。」

「盗まれたデジタルテープ５本のうち３本は，事件発覚２日後の１２月３０日，福島市内の河川敷で発見された。３本のうち２本は住基ネットで使う１１けたの住民票コードなど１５項目の個人情報が入っていた。残る１本と未発見の２本には住基ネットを稼働させるためのシステムが収録されていた。この結果，町は町民の同意を得た上で，全員の住民票コードを変更するという前代未聞の事後策を取らざるを得なくなったのである。」

（３）内部の者による情報漏洩（③)

さらに，調査会議報告書（甲７１）は，同様の事件は，内部犯行によっても起こりうるものであり，先の情報漏洩の四ルート区分でいえば，「③内部の者による情報漏洩（組織に恨みを持ったり，金銭的理由で行われる内部犯行)」がそれに当たるとして，次のとおり指摘している（１８～２０頁)。

「この内部犯行によって自治体内部の住民情報が漏洩した事件としては，１９９９年の５月に発覚した京都府宇治市の事件がある。

この事件の発覚のきっかけとなったのは，兵庫県にある神戸新聞の記者が，大阪府堺市にある名簿業者のホームページを見ていて，「宇治市住民票　総数２１万７６１７」という名簿データが販売されているのを発見したことだった。神戸新聞は協力関係にある京都新聞編集局に連絡し，京都新聞の宇治

市担当記者らが取材に入った結果，５月２２日に京都新聞が報道して事件は公となった。

この名簿に含まれていたのは，住所・氏名・性別・年齢の基本４情報以外に加えて世帯主名や世帯主との続柄，それに宇治市固有の「住民番号」も漏洩した。住民番号というのは，宇治市が住民基本台帳のシステムを作り上げた際，住民一人一人に便宜上割り振られたナンバーである。

これは住基ネットのデータとは異なり，住基ネットが導入される以前から従来型の住民基本台帳システムで使われてきた番号だ。住民番号は内部管理用のもので，外部には公開されていない。この番号が名簿データに含まれていることで，データは市役所内部から何らかの形で流出したことは間違いないと認定された。

この従来型データは，庁舎一階にある市民課に置かれているパソコンと，地階のマシンルームの両方に保存されていた。市民課窓口の端末は一度に１世帯分のデータしか表示できない仕組みで，またマシンルームも厳重な入退室管理が行われていたとされていた。住基ネットのＣＳ端末，ＣＳサーバーと同様のセキュリティ管理が行われていたのである。

しかしそれにも関わらず，住民データは漏洩した。

漏洩ルートは，翌２０００年６月になって解明された。

宇治市は１９９８年，情報システムのメンテナンスを発注していたＡ社に，乳幼児検診システムの名簿データの作成を依頼。Ａ社はこの業務を，別の下請け会社Ｂ社に発注していた。この下請け会社のスタッフのひとりが，データを名簿業者に横流ししていたというのである。名簿業者も，宇治市に対して「名簿は１９９８年５月，Ｂ社のアルバイト男性（２３歳）から２５万８０００円で購入した」と証言。

この時，市はＢ社に事実関係を確認したが，Ｂ社の担当者は市に対して，「うちはやっていない」と否定したという。また横流ししたと見られるアル

バイト男性はこの時点ですでにＢ社を退社しており，市の問い合わせに対してＢ社を通じ，「名簿の横流しは行っていない」とこちらも否定した。

だが名簿業者側から売り渡しの書類が市に提出され，この書類に残された住所氏名がアルバイト男性と一致。筆跡も，男性がＢ社で作成した書類のそれと酷似していた。

このため市はこの事実を発表するとともに，宇治市個人情報保護条例違反の容疑で刑事告発することにしたのである。

しかしデジタル化された個人情報はいったん流出すれば，「コピーは本当に作られていなかったのか」「インターネット上に公開されるのではないか」という不安が残る。

このため宇治市は，名簿業者の持っていたデータを市職員が消去する場面をビデオカメラで撮影し，それを公開するという提案を行い，実際に公開をスタートさせた。

業者は宇治市の住民データ２１万７６１７件が含まれたデータを光磁気ディスク（ＭＯ）に保存しており，市側との合意後にこのＭＯを市職員に手渡している。この際，職員は現場でデータを消去し，その様子をカメラで録画したという。

録画したデータを公開すると市議会総務委員会で発表した市側に対し，市議会議員からは「データを持ち出した元大学院生に市が接触できていないのに，名簿業者の持っていたデータが唯一のコピーだと信じられるのか」「市が現時点で把握している情報をすべて公開してほしい」などと質問が出た。確かに，データを持ち出したと見られていた元大学院生が，名簿のコピーを別に作って自分で保管していたり，あるいは他の名簿業者などに売り渡していた可能性は否定できない。もし元大学院生が一方的に宇治市から非難されたことに怒り，市に損害を与えようとすれば，どんな行動でも取ることができた。

たとえば名簿のデータを，インターネットの匿名で開設できるウエブサイト上にアップロードするといった手口も可能である。そしてそのＵＲＬ（ウエブサイトのアドレス）を，「２ちゃんねる」などのインターネット匿名掲示板に書き込んだらどうなるだろうか。

２ちゃんねるは一日に延べ数百万人がアクセスするとされ，社会に対する影響力は計り知れないほどに大きくなっている。もしアクセスの多い「ニュース速報」板などにＵＲＬが書かれれば，数え切れないほどのユーザーが面白半分に名簿データをダウンロードし，別の匿名掲示板や匿名サイトなどに転載を繰り返すという結果になる。

過去，漏洩してはならないデータがネット上に出現するたび，何度も繰り返されてきたできごとである。そうなったら最後，インターネット上に無数に増殖してしまった名簿データをすべて回収するのは不可能に近い。なぜなら，インターネットは，コピーされたデータを自動的に追跡して削除するというような機能は持っていないからである。

これは住基ネットのデータが漏洩する事件ではなかったが，しかし同様の漏洩事件が住基ネットデータに関しても引き起こされる可能性は，ほぼ同等と考えられる。自治体内部の職員であれば，住基ネットにアクセスする権限を持ち，ＩＣカードとパスワードを保有しているからである。」

（４）内部の者による情報漏洩（④）

以上に続けて，調査会議報告書（甲７１）は，次のとおり指摘する（２０～２２頁）。

「そうであれば，「④内部の者による情報漏洩（紛失，Ｗｉｎｎｙ利用などの誤って起こした事故）」の可能性も同じ程度に高いことは明確である。北海道斜里町で住基ネットの古いパスワード，操作マニュアルが漏洩した事故は，この④のＷｉｎｎｙ利用で誤って起こしたものであり，今後，同種の事故が起きないという保証はまったく存在しない。

そんな中で，住民に対して少しでも住基ネットの安全性を高めるため，ＩＳＭＳ（情報セキュリティマネジメントシステム）規格の認証を取得する自治体も現れてきている。たとえば埼玉県は２００５年３月２５日にＩＳＭＳを取得した。」

「尚，ＩＳＭＳではリスクをゼロにする事は求めていない。リスク対策を行う事は，コストが掛かる為，組織として許容できる範囲のリスクかどうかの判断を経営陣が行う事を求めていて，許容範囲までのリスク軽減の対策を講じ，実行されている事を管理する事が求められている。

情報資産の洗い出しから始まって，リスクの洗い出し，対策の検討実施，効果の確認，見直しのＰＤＣＡサイクルを回す事がＩＳＭＳである。」

「埼玉県がＩＳＭＳを取得したことは評価されるべきだが，前出のように住基データは全国の自治体に設置されているＣＳサーバーのどこからでもアクセスが可能であり，すべてのデータを引き出すことが可能である。そうなると埼玉県だけがＩＳＭＳを取得し，セキュリティを高めたとしても，他にひとつでもセキュリティの甘い自治体があれば，そこから埼玉県を含めた全国の住基データが漏洩してしまう。

セキュリティには，Weakest Link（最も弱い部分）という言葉がある。システム全体のセキュリティ強度は，最も弱い部分（Weakest Link）によって決定されるという意味である。その意味で，ＩＳＭＳを取得した自治体が将来に全国の大半を占めたとしても，セキュリティの弱い自治体がごく一部にでも残っていれば，そこが Weakest Link になってしまい，セキュリティ全体の強度は下がってしまうことになる。」

（５）住基データが漏洩した場合の危険性について

調査会議報告書（甲７１）は，住基データが漏洩した場合の危険性はどこにあるのかについて，次のように述べている（２２～２３頁）。

現在，住基ネットで使われる住基カードは，主には住民票の発行と引っ越

しの際の転出・転入届に使えるだけとなっている。自分の住んでいる市町村とは別の役所で住民票を発行してもらったり，引っ越しの際に転出・転入の両方の届が一度に出せるというメリットがある。

これはしかし総務省の考える住基カードの利用方法の一部でしかなく，今後は電子認証のキーとして使われることになっている。政府の電子認証は公開鍵方式が使われることになっていて，この住基カードの中に秘密鍵と公開鍵が収められているというわけである。

つまりは住基カードに，「実印」と同じ役割を持たせようということになる。

今のところは住基カードを使おうと思ったら，役所に持って行ってカードリーダーに差し込み，４ケタの暗証番号をその場でテンキーパッドから入力しなければならない。しかもできるのは住民票と転出・転入届だけである。

しかし今後，このカードを自宅のパソコンにＵＳＢ接続したカードリーダーに挿入し，インターネット経由で自動車の登録やパスポートの申請，年金や社会保険の手続きなどさまざまな申請に使えるようになる。夢の将来としてずっと語られてきた電子政府の実現，ということになる。

この件について，佐々木委員がヒヤリングを行った政府のＩＴ施策に携わっている官僚は次のように指摘した。

「住基カードが普及しないのを，旗振り役の総務省はいちばん恐れている。せっかく巨費を投じ，多大な宣伝費をかけ，反対を押し切って実現したシステムが普及しないのでは，『ムダ使い』呼ばわりされかねない」

そこで住基カードが利用されるよう，総務省はさまざまな施策を進めようとしている。

そのひとつが，住基カードの利用の拡大なのである。現在でも，市町村などが住基ネットとは別のアプリケーションを使って独自の使い道を行うことは認められている。たとえば岩手県水沢市では，市役所や公民館に設置され

た端末を使い，公共施設の予約や市民病院の再診予約などに利用することができる。ほかにも図書館の利用カードにしたり，お年寄りのバス優待証代わりにしたりと，全国の役所ではさまざまに知恵を絞っているようだ。

さらに，総務省は民間での利用も一部解禁し，住基カードを商店街のポイントカード代わりにしたり，病院の診察券にも転用できるようにすることを想定している。

一枚のカードでいろんなサービスに使えるというのは，一見まことに便利な話に思える。しかしその場合のセキュリティの危険性はいっそう高まることになる。

住基カードに収められている情報は，住民票コードなどの個人情報▽公的個人認証のための情報▽図書館の貸し出しカード機能など各自治体が自由に使える部分，などが切り分けられ，それぞれにパスワードがかけられるようになっている。

しかしこのうち，住基カードを役所の窓口のカードリーダーに挿入して利用する際のパスワードは，わずか４ケタの数字でしかない。また役所によっては，物理的なセキュリティ対策が乏しい。つまりテンキーパッドを覆うカバーが小さく，横側からキーパッドの操作を覗けてしまうケースが少なからず存在している。いくらカード自体のセキュリティを高め，高度な暗号をかけたとしても，４ケタの暗証番号を見られてしまったのでは，何の意味もない。

アメリカでは，住基ネットで使われる１１桁のコードと似た「社会保障番号」（ソーシャル・セキュリティ・ナンバー）が幅広く使われている。そしてこの数字を盗まれて悪用され，勝手にクレジットカードを使われたり，カネを借りられたりといった「なりすまし」事件が後を絶たない。社会保障番号と名前，生年月日程度があればクレジットカードを作ることができてしまう社会の仕組みにも問題があるが，日本も住基カードがこうした犯罪に使わ

れるようにならないという保証は存在しない。」

5　横浜市答申（乙２０）への反論

（１）制度面

ア　個人情報保護法制度の不備について

横浜市・審議会答申は，個人情報保護法制度の不備については，着実に整備されてきており，制度面からみた問題点は，解消されているとする（乙２０　１０頁）。

しかしながら，調査会議報告書（甲７１）が述べるように，横浜市・審議会答申が当初懸念していた事項は解消されるに至ったとの認識には根本的に異を唱えざるを得ない。その理由は，以下に引用するとおりである（３２頁）。

「まず，横浜市の審議会が「横浜方式導入の最も大きな理由である」とする個人情報保護法制度の不備は本当に解消されたといえるのか。この点については，個人情報関連５法が２００３年５月に成立し，その後施行されるに至ったのは事実であるが，改正住基法の附則の趣旨はどんな内容であれ個人情報保護の名を掲げる法律が制定されさえすればいいというものではもとよりなく，個人情報を保護できる実質を備えるものであることが求められるのは当然である。

この点では，Ｉで詳論したように，住基ネットともっとも深い関連をもつ，全面改正された行政機関個人情報保護法を取り上げても，附則が要請する実質的要件を満たしていないと言わざるを得ない。すなわち，主として民間を規制する個人情報保護法にさえ定められている適正な取得・収集の規制規定も用意されておらず，利用目的の変更や目的外利用・提供を広く認め，名寄せやデータマッチングを明示的に禁止せず，個人情報ファイルの作成・公表や本人情報の開示・訂正に広範な例外を規定し，罰則規定

も最小限にとどめ，センシティブ情報の収集も禁止せず，法運用をチェックする第三者機関も設置されていないからである。

なお，住基法改正による基本４情報の原則非公開化が個人情報の保護を一定程度進めるものであることは確かであるが，これが行政機関個人情報保護法や後述する改正住基本法が定めるきわめて不十分な個人情報保護制度を補いきれるものでないことは言うまでもないし，そもそも住基ネットのシステムは片山総務相（当時）が繰り返し明言したように，本人確認情報はプライバシーとして要保護性に乏しいとの前提で構築され，運用されてきたものであり，これに基づく制度の設計自体が批判的に吟味しなおされなければならないはずである。」

イ　名寄せへの懸念について

なお，横浜市・審議会答申は，名寄せへの懸念についても，制度面で一定の措置が取られているとして，意に介していない（乙２０　１０頁）。

しかしながら，調査会議報告書が述べるように，これについても重大な疑問がある。その理由は，以下に引用するとおりである（３３頁）

「答申は，名寄せ等の懸念に対しては住基法上制度面で一定の措置が取られていると述べているが，Ⅲでも指摘した金沢地裁判決が疑問を提示しているように，目的外の利用・提供禁止規定（３０条の３４）が名寄せやデータマッチングを含むか不明確だし，この違反への罰則も，第三者による監視の仕組みも欠いているので名寄せやデータマッチングへの有効な規制を期待するのは困難であるし，前述したように，行政機関個人情報保護法もこれらを明示的に禁ずる規定がないばかりか，利用目的の変更や目的外の利用・提供について行政に大幅な裁量を委ねてさえいる。

こういう有効な規制が欠如するなか，Ⅲで詳しく見たように，さまざまな分野で行政情報の統合，共有化が進展しつつあり，行政機関に住民が開示した「情報に住民票コードが付され，データマッチングがなされ，住民

票コードをマスターキーとして名寄せがなされると，住民個々人の多面的な情報が瞬時に集められ，・・・住民個々人が行政機関の前で丸裸にされるが如き状態になる」との金沢地裁判決の危惧が現実のものとなりつつあるのである。

また，答申が名寄せ等への歯止め措置として，住民票コードは変更可能な制度なので自己情報コントロール権が保障されていると述べている点も看過できない。確かに住民票コードは変更可能であるが，その変更は履歴として記録され，辿られることが可能である。これが名寄せやデータマッチングの防止策としてどういう意味を持つのか，理解不能である。また，住民票コードの変更の制度をもって自己情報コントロール権の保障規定と考えるのは，自己情報コントロール権の矮小化に他ならない。この権利が本来の意味を発揮するのは，金沢地裁判決が示したように，この権利を行使して住基ネットへの参加・不参加の判断を市民に委ね，離脱の権利を承認することである。」

（２）技術面

横浜市・審議会答申は，住基ネットの技術面について，外部からの不正侵入に対する適切な防止策（品川区のペネトレーションテスト等で実証）や内部の不正使用に対する防止策が採られており，十分な個人情報保護対策がなされているとする（乙２０　１０頁）。

しかしながら，前記のとおり，長野県での侵入実験に携わった専門家がセキュリティ上の問題を指摘している。にもかかわらず，総務省はセキュリティ上の問題を一切情報開示していないため，十分な防止策が採られていることを全く説明していないに等しい。

さらに，前記のとおり，品川区の行った侵入実験の直後にも断続的に脆弱性が公表されており，同実験においてこれらの脆弱性の存在がどの程度確認できたかについても明らかにされていない。

そのような状況下で，何を根拠に適切な防止策が採られたとしているのか不明である。

（3）運用面

横浜市・審議会答申は，国等の研修などによる自治体のセキュリティに対する意識等の向上，不測の事態を想定した訓練等をもって，個人情報保護に向けた運用面の取り組みは十分なレベルに達しているとする（乙２０　１０頁）。

しかしながら，現に前記のような情報漏えいが頻発している状況にあり，運用面での問題が解消されているとはいえない。

（4）その他

ア　個人情報保護法制度以外の問題点

横浜市・審議会答申は，個人情報保護法制度以外の問題点を５つ指摘していたが（乙２０　１～２頁「ア」～「オ」），横浜市が当初懸念していた事項は，解消されているとする（乙２０　１０～１１頁）。

しかしながら，調査会議報告書（甲７１）が，次のとおり指摘しているように，かかる結論に同意するのは困難だと言わざるを得ない（３３～３４頁）。

「アの国の責任が不明確であるという点については，「総務省は，制度を所管する立場から，また，指定情報処理機関に対して監督を行う立場から責任を負う」との総務省文書が示され，都道府県に対してセキュリティ研修の実施などの取り組みを行ってきたのは確かだが，北海道の斜里町における住基ネット情報の流出事件や，札幌弁護士会のアンケート結果（２００５年６月の「札幌弁護士会会報」所掲），神奈川県の実態調査（２００３年８月の住基ネットに関する研究会による「住基ネットに関する神奈川県市町村実態調査についての報告」），住基ネット訴訟の大阪地裁判決（２００６年２月９日）などで示された地方自治体における個人情報保護

やセキュリティに関するずさんな運用などを見る限り，総務省が責任を持って監督しているとは言いがたい。

イの自治体からの調査要求の点では，これも総務省告示（前記「技術的基準」）により可能となったのは事実だが，実際には斜里町の住基情報の流出という重大な事態にもかかわらず，横浜市は国や斜里町に報告も求めていないし，横浜市民への説明も行っておらず，制度の実効性に疑問を持たざるを得ない。

ウのアクセスログの開示請求の仕組みについては上記「技術的基準」等により，一定の制度化が図られたとはいえ，一部の自治体では住基ネットの端末を操作する場合の操作者識別カードを複数の職員が使いまわしていることも判明しており（兵庫県），その場合にはアクセスログによって誰が操作したかはわからず，個人情報の保護に資するかどうか，疑問が残る。

エの不正使用に対する罰則規定については，前述したように，行政機関個人情報保護法では，データマッチングやセンシティブ情報の収集などへの罰則はないなど，その範囲は最小限にとどめられているので，十分な規制となっているか，きわめて疑問である。

オの住基ネットの将来像の明示の点では，利用事務の変更の法律案の検討に際しての第三者機関の審議等で十分な歯止めになるか疑問があるだけでなく，Ⅲでみたように，行政情報の統合化・共有化の進展の中に住基ネットを据えて考えると，住民票コードをマスターキーとしてさまざまな情報が名寄せされ，データマッチングが進み，国民の個人情報が一元的に管理される危険はますます強まりつつあると言わざるを得ない。」

イ　その他の問題点

その他の問題点として，調査会議報告書（甲７１）は，次のとおり，二点付言している（３４～３５頁）。

「一つは，選択制を維持すると一部の事務では通知者の本人確認情報も

利用できないと述べている箇所についてであるが，こうした議論は，横浜地裁での住基ネット訴訟において原告側証人として証言した花園勝・横浜市市民局区政支援部窓口サービス課システム担当課長（当時）が，国側の主張に対して，横浜市は，通知者の情報は利用できるはずであり，利用してほしい旨要請をしているとかつて発言したことと相反し，年金現況報告の住基ネット利用について，横浜方式を続ければ市民全員が対象外になるとの総務省による横浜市への説明に対し，社会保険庁が「そんなことは言っていない」と報じられている（朝日新聞２００６年５月３日付）ことなどを考えあわせると，そのまま受け取って然るべきかどうか，吟味が求められよう。

また，これまでの住基ネット訴訟の判決の評価にも問題を感じる。答申では，住基ネットの安全性について具体的危険のあるシステムではないと判断した点が一面的に強調されているが，これはフェアーな判決評価とは言えないのではないか。現に，金沢地裁判決がデータマッチングの危険を強く指摘していたことや大阪地裁判決が自治体の運用がセキュリティの点で多くの問題を抱えていることを認定していることなどには言及がされていないし，プライバシーの権利を自己情報コントロール権として積極的に承認し，本人確認情報もこれに含まれるとの司法判断が少なからず示されていることの意義も語られていない。住基ネットの安全性を盲目的に追認する司法判断だけが示されてきたわけでは決してないという事実を軽視してはなるまい。」

6　結論

調査会議報告書（甲７１）が，「以上のように見てくると，また本報告書のⅠ～Ⅲで示してきたものを踏まえて考えるといっそう，今回の答申のように，選択制を導入した際横浜市が抱いた住基ネットの安全性への疑問がその後解消

され，「現時点において総合的に見て問題はない」との結論を導く論拠が希薄であり，結論の妥当性を支えることは困難だと断ぜざるを得ない。」（３５頁）と述べているとおり，住基ネットの総合的な安全性は，未だ確認できていない。

以　上