副　本

平成１８年（行コ）第１１９号　住基ネット受信義務確認等請求控訴事件

控 訴 人　　杉並区

被控訴人　　国，東京都

準 備 書 面 (2)

平成１９年３月１日

東京高等裁判所第１０民事部　御中

控訴人の本件各訴えが「法律上の争訟」（裁判所法３条１項）に当たらず，不適法であることは，答弁書第３に述べたとおりである。したがって，控訴人の平成１８年１２月１４日付け準備書面(2)（以下「控訴人準備書面(2)」という。）における主張に対しては，本来反論の必要はないが，被控訴人らは，念のため，以下のとおり反論することとする。

なお，略語等は，本書面において新たに用いるもののほか，従前の例による。

第１　「第１　受信拒否の適用違憲（中島意見を踏まえた主張)」に対する反論

１　控訴人の主張

控訴人は，自己情報コントロール権（プライバシー権）が憲法上保障された権利であることを前提として，住基ネットに対する情報主体の利害状況は，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ゆだねるのが適切であること及びＯＥＣＤ８原則等から，情報主体である住民に自己の情報の利用・提供に関する「同意」の機会を保障すべきである旨主張する（控訴人準備書面(2)第１・３ないし１６ページ)。

２　住民の「同意」の機会を保障しなければならないわけではないこと

(1)　しかしながら，これまで答弁書第５の３(1)及び(2)（１５ないし２１ページ）等で繰り返し述べてきたとおり，自己情報コントロール権は，実定法上の根拠がない上，その実質的な内容，範囲，法的性格についても，様々な見解があり，権利としての成熟性が認められないものであるから，そもそも実体法上の権利とは認められない。また，プライバシーの概念は多義的で，その内容も流動的であることから，最高裁判所もこれを一義的な内容を持った権利として認めることになお慎重である。したがって，憲法上あるいは実定法上，住民各個人に対し，行政機関の収集・処理し得る個人情報の範囲をコ

ントロールし得る権利が，保障されているわけではないから，「住基ネットに対する情報主体の利害状況」が，医療行為に対する患者の利害状況と酷似しているということはできないというべきである。

(2) また，仮に，自己情報コントロール権を認める見解を前提とするとしても，最高裁判所が再三にわたって指摘しているように，プライバシーの権利ないし利益は，個人の「私生活上の自由」を保護するものであり，個人の公的活動領域をも含めて，当然に保護するものではないから，その本来の保護対象は，私的生活領域における自己情報にとどまるものである。すなわち，特定の個人を識別し得る情報を含む個人情報のすべてが，憲法上のプライバシーの権利として保護されるわけではないし，個人情報の保有やその収集・処理の制限一般を公権力に対して求める積極的な権利が，憲法１３条自体から直ちに導かれるわけでもない。また，私的生活領域にかかる自己情報についてさえ，情報主体たる個人がそのすべてについてコントロールすることは，事実上不可能であり，一般的社会通念としても，そうしたコントロールが期待されているとはいい難いのであって，「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ことに留意する必要がある。長谷部恭男東京大学大学院教授も，同趣旨の意見を述べている（乙第１１号証２ページ）。

(3) そもそも住基法は，その立法目的において，行政の合理化のため，都道府県や国の機関が個々の住民の承諾を得ずに住民票記載情報を利用することを当然に予定している。すなわち，住民票記載情報のように，人間の社会生活の基礎となる個人情報は，いわば公共領域に属する個人情報であるから，行政の合理化のため，これらの情報を個人の承諾を要することなく利用できるとの法制度が採られているのであり，この点は，平成１１年の住基法の改正前と後で何ら変わりないし（被告国ら準備書面(8)１３，１４ページ），住民票記載情報を住民の同意を得ることなく利用したからといって，これが自

己情報コントロール権の侵害に当たると解する余地はない。

この点について，名古屋高等裁判所金沢支部平成１８年１２月１１日判決（以下，「名古屋高裁金沢支部判決」という。乙第２７号証）も，「本人確認情報は，そのものとして，個人の人格的自律ないし人格的生存に必要不可欠な，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，本人確認情報のプライバシーとしての要保護性について，憲法１３条が，国家機関等の公権力との関係で，国民に対し，本人確認情報に係る住民の同意を得ることなくしては，国家機関等の公権力においてこれを収集し，管理し，利用することができないような強度なものとして保障しているものと解することはできないのであり，国家機関等の公権力において，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」い旨判示している（乙第２７号証３７ページ２１行目ないし３８ページ６行目）。

(4) 控訴人は，ＯＥＣＤ８原則によれば，当該個人情報の利用につき，本人の同意が必要であると主張する（控訴人準備書面(2)第１・１０ページ１０行目以下）が，同原則に照らして本人の同意が要件になるのは，本来の利用目的以外のために個人データの開示，利用等を行おうとする場合であって，個人情報の収集目的の範囲内又は法律の規定による場合については，あえて本人の同意を得ることまでは求められていない。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行政目的のために提供することは，住民基本台帳の本来の目的の範囲内での個人情報の利用であり，住基ネットを通じて本人確認情報を通知・提供することについて，ＯＥＣＤ８原則に照らして個別の住民の同意を得ることなどが求められているということはない。この点は，ＯＥＣＤの情報セキュリティ・プライバシー・ワーキ

ング・パーティの副議長を務めている堀部政男中央大学大学院教授も同趣旨の意見を述べている（乙第１０号証（以下，「堀部意見書」という。）６，７ページ)。

３　小括

以上のとおり，住基ネットにおいて住民の本人確認情報を利用するためには住民の承諾が必要であるとする控訴人の主張は，前提となる住基法の趣旨を全く理解せず，独自の見解によるものであり，失当である。住基ネットにおいて住民の同意を得ないで本人確認情報を利用することは，住民の権利・利益を何ら侵害するものではない。

以上の点については，名古屋高裁金沢支部判決においても，「本人確認情報事務処理は，いずれも住基法という法律の規定に基づく措置であるところ，住基法には，上記提供を含む住基法所定の本人確認情報処理事務に関し，本人確認情報に係る住民の同意又は住基ネットへの参加表明をその要件とし，あるいは，住基ネットへの不参加又は離脱を表明している者についての除外を定める規定はないから，住基法は，控訴人県の知事に対し，本人確認情報に係る住民の同意又は住基ネットへの参加意思の有無を問うことなく，一律に，その区域内の市町村長から通知を受けた住民（被控訴人らが含まれる。）に係る本人確認情報に関して住基法所定の本人確認情報処理をすることを命じているものであること（…（略）…）は明らかであり，住基ネットに関係する住基法の諸条項の文言に照らしても疑いを入れない。」と適切に判示されているところである（乙第２７号証３１ページ１行目以下)。

第２　「第２　住基ネットの総合的な安全性の欠如」に対する反論

１　「２　制度面」について

(1)　「(1) 個人情報保護法制上の不備」について

ア　控訴人は，改正住基法の附則１条２項の「『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。」とし，「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。」と主張する。

そして，その論拠として「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法であると考えられることである。」，「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。」などと主張する（控訴人準備書面(2)１７ないし１９ページ）。

イ　しかしながら，以下のとおり，控訴人の主張は失当である。

そもそも，改正住基法附則１条２項の規定は，平成１１年の改正法案の国会審議の過程において，住基ネットについては，同法によって，十分な個人情報保護措置が講じられているものの，なおプライバシー保護に対する漠然とした不安，懸念が残っていることを踏まえ，議員修正により規定されたものである。

そして，改正住基法附則１条２項にいう「所要の措置」とは，民間部門における個人情報保護に関する制度についての措置を指すものであるから，この点に関する控訴人の理解は誤りである。

すなわち，改正法成立当時，公的部門における個人情報保護制度としては「行政機関の保有する電子計算機処理にかかる個人情報の保護に関する法律」が存在する一方，民間部門における個人情報保護制度は存在しなかった。このような状況を受けて，政府は，住民基本台帳ネットワークのシステムの実施に当たり，「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」としたものである（上記

国会審議において，小渕恵三総理大臣から，「住民基本台帳ネットワークシステムの実施に当たり，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」との答弁がされている。乙第２８号証)。

そして，民間部門の個人情報保護制度を定めた「個人情報の保護に関する法律案」は，第１５１回国会において，平成１３年3月２７日に提出され，政府としては，上記の「所要の措置」を講じたものである。なお，同法案１１条１項には，「政府は，国の行政機関について，その保有する個人情報の性質，当該個人情報を保有する目的等を勘案し，その保有する個人情報の適正な取扱いが確保されるよう法制上の措置その他必要な措置を講ずるものとする。」との規定があり（乙第２９号証)，これを受けて，公的部門の個人情報保護制度について定めた行政機関個人情報保護法等の４法案が第１５４回国会において，平成１４年3月１５日に提出されている。

よって，「所要の措置」に関する控訴人の主張が誤りであることは明らかである。

なお，名古屋高裁金沢支部判決も，改正住基法附則１条２項にいう「所要の措置」が講じられていないということはできない旨適切に判示している（乙第２７号証４６ページ１６行目以下)。

(2)　「(2) 監視社会化の流れの中での位置付け（名寄せの危険性)」について

ア　控訴人は，「『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』(…（略）…）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。」などと主張する（控訴人準備書面(2)１９ないし２１ページ)。

イ　しかしながら，その根拠として控訴人が挙げる論拠はいずれも，将来の抽象的な危惧を述べるものか，誤った法の解釈に基づくものにすぎない。

以下，控訴人が論拠として挙げている順に従って，詳述する。

(ｱ)　住民票コードの利用を制限していること

まず，控訴人は，「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…（略）…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」と主張する（控訴人準備書面(2)１９ページ）。

しかしながら，住民票コードは，住基ネットというコンピューターネットワークを構築するに当たり，行政において，個人の確実な特定を可能にし，迅速かつ効率的な検索を実現するために不可欠であることから，設けたものであるところ，住基法は，以下のとおり，住民票コードの利用を厳しく制限することとしている。

a　住民票コードは無作為の番号で，住民の申請によりいつでも変更できる（住基法３０条の３）。

b　民間部門が住民票コードを利用することを禁止しており，特に，民間部門が契約に際し住民票コードの告知を要求したり，住民票コードの記録されたデータベースで他に提供されることが予定されているものを構成した場合，都道府県知事は中止勧告や中止命令を行うことができる。都道府県知事の中止命令に違反した者は，１年以下の懲役又は５０万円以下の罰金が科せられる（住基法３０条の４３，４４条）。

c　行政機関が住民票コードを利用する場合も，目的外利用の禁止，告知要求制限等の規定により利用が制限されており（住基法３０条の３４，３０条の４２），指定情報処理機関は国の機関等に対し，住民票コードを利用して住基法で定めるところにより本人確認情報の提供を行うことはできるが，国の機関等と他の国の機関等との間で住民票コ

ードを利用しデータマッチングをすることは禁止されている。

このように，住基法においては，住民票コードの利用が厳しく制限されており，控訴人の上記主張は失当である。

(ｲ) 住基カードの交付・携帯は希望者のみであること

また，控訴人は，「大量の情報を記憶できるＩＣチップ内蔵の住基カードは…（略）…現在は希望者にだけ交付されるが，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。」と主張する（控訴人準備書面(2)１９，２０ページ)。

しかしながら，住基カードは，市町村長が住民の申請により交付する（住基法３０条の４４第３項）ものである上，携帯が義務付けられているものではないから，控訴人の上記主張は，何ら根拠がない。

(ｳ) データマッチングが行われるおそれの不存在について

さらに，控訴人は，「住基ネットが各種データベースを繋ぎ，結合を促進する上で基盤的役割を担う可能性が高い。」と主張する（控訴人準備書面(2)２０ページ)。

しかし，住基法は目的範囲内の利用等に当たらないデータマッチングを絶対的に禁止している上，住基ネットの制度上の仕組みに照らしてみても，法の許容しないデータマッチングが行われる具体的危険は皆無であるから，控訴人の主張には理由がない。

a 住基法等が目的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いること

(a) 住基法３０条の３４

住基法３０条の３４は，住基法別表の事務を行うため本人確認情報を受領した者は，当該本人確認情報の提供を受けることが認めら

れた事務の処理以外の目的のために，受領した本人確認情報の利用又は提供をしてはならない旨を明確に規定し，目的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いる。

(b)　住基法と行政機関個人情報保護法との関係

住基法３０条の３４を始めとする住基法中の本人確認情報の保護規定は，個人情報の中でも，住基ネットというネットワークシステムで取り扱う本人確認情報について，その保護措置を講じるために特に設けられたものである。

これに対し，行政機関個人情報保護法は，行政機関における個人情報一般について，その取扱いに関する基本的事項を定めるもの（同法１条参照）である。

したがって，国の行政機関が住基ネットを通じて受領した本人確認情報を保有する場合において，行政機関個人情報保護法等が一般法であるのに対して，住基法中の本人確認情報の保護規定が特別法の関係にある。したがって，国の機関等が住基ネットを通じて受領した本人確認情報は，まずは住基法中の本人確認情報の保護規定の適用によって保護されるのであり，住基法中に規定がない場合に初めて一般法である行政機関個人情報保護法が適用されるのであって，両者が抵触する場合には，住基法中の本人確認情報の保護規定が優先して適用される（平成１５年４月１８日衆議院個人情報の保護に関する特別委員会会議録６号１７ページ（乙第３０号証），平成１５年４月２５日個人情報の保護に関する特別委員会会議録１１号４ページ（乙第３１号証），堀部意見書３ページ参照）。

行政機関個人情報保護法８条２項２，３号は，一定の要件の下で利用目的以外の目的のための保有個人情報の利用，提供を認める規定であり，また，同法３条３項は，一定の要件の下で利用目的の変

更を認める規定である。しかし，上記のとおり，住基法３０条の３４はこれらの規定の特別法に該当するのであるから，本人確認情報については，結局，住基法３０条の３４が優先して適用されることになる。したがって，目的の範囲内の利用等に当たらないデータマッチング，すなわち，受領者における同法所定の事務処理に必要とされる限度を超えた本人確認情報の利用，提供は，全面的に禁じられており，行政機関個人情報保護法の規定の適用により，その禁止が解除される余地は全くないのである。

b　違反行為に対する罰則等が規定されていること

目的範囲内の利用等に当たらないデータマッチングを行うことは，住基法３０条の３４所定の職務上の義務の違反に該当するため，懲戒処分の対象となる（国家公務員法８２条及び地方公務員法２９条）。

また，行政機関の職員が，目的範囲内の利用等に当たらないデータマッチングや名寄せを行うために，本人確認情報に関する秘密が記載された文書，図画又は電磁記録を収集した場合には，「その職権を濫用し，専らその職務以外の用に供する目的で」行ったものとして，１年以下の懲役又は５０万円以下の罰金に処せられることになる（行政機関個人情報保護法５５条）。

さらに，目的範囲内の利用等に当たらないデータマッチングや名寄せを行わせるために，指定情報処理機関の役員及び職員（住基法３０条の１７第３項），本人確認情報の提供を受けた国の機関等の職員が，その知り得た本人確認情報に関する秘密を他の国の機関等に漏らした場合には，公務員の守秘義務違反等に該当し，刑罰の対象となる（国家公務員法１０９条１２号，１００条１項，２項及び地方公務員法６０条２号，３４条１項，２項，行政機関個人情報保護法５３条，５４条，住基法４２条）。

c　第三者機関が規定されていること

住基法３０条の９第１項は，「都道府県に，第３０条の５第１項の規定による通知に係る本人確認情報の保護に関する審議会を置く」こととしている。この審議会は，「この法律の規定によりその権限に属させられた事項を調査審議するほか，都道府県知事の諮問に応じ当該都道府県における第３０条の５第１項の規定による通知に係る本人確認情報の保護に関する事項を調査審議し，及びこれらの事項に関して都道府県知事に建議することができる」ものとされている（同法３０条の９第２項)。したがって，この審議会は，当該都道府県における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のである。

また，同法３０条の１５第１項は，「指定情報処理機関には，本人確認情報保護委員会を置かなければならない」とし，この委員会は，「指定情報処理機関の代表者の諮問に応じ，第３０条の１１第１項の規定による通知に係る本人確認情報の保護に関する事項を調査審議し，及びこれに関し必要と認める意見を指定情報処理機関の代表者に述べることができる」ものとされ（同法３０条の１５第２項)，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。

さらに，セキュリティ基準第６－８(1)－ウ及びエ（乙第３２号証）は，都道府県知事は，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を求め，適切に管理するよう要請することができ，市町村長も，都道府県知事を経由して上記のような報告等を要請することができると定めており，この点においても，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

保がされている。

上記「本人確認情報の保護に関する審議会」及び「本人確認情報保護委員会」については，別件名古屋高等裁判所金沢支部判決１８年１２月１１日判決（平成１７年（ネ）第１５４号事件）においても，これらを設置する旨の規定があることを指摘して，「住基法が行政機関による個人情報の目的外利用禁止の制度的担保を設けていないということはできない」と正当に判示されているところである。

d　住基ネットの制度上の仕組みに照らしてみても，法の許容しないデータマッチングが行われる具体的危険が皆無であること

平成１８年５月１５日現在，本人確認情報の提供が認められている事務は２９３事務あるが，これらの国の機関等の保有する情報を一元的に管理する主体は存在しない。本人確認情報を記録，保有する指定情報処理機関は，住基法別表で定める国の機関等に対し，その求めに応じて本人確認情報を提供することは予定されているものの（同法３０条の１０），指定情報処理機関には，国の機関等からその保有する本人確認情報以外の住民に関する情報を収集し，これを管理することができる権限は付与されておらず，国の機関等にもそのような情報を指定情報処理機関に対し提供する権限や義務はなく，指定情報処理機関において，国の機関等が保有する情報を結合することは不可能である。そして，本人確認情報の提供について，その対象となる事務が法改正により追加されるとしても，目的外利用を禁止する諸規定が改正されたわけではないから，対象事務の拡大によって，データマッチングの具体的危険が増大することにはならない。

また，住基ネットは，それぞれの機関がそれぞれ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おり，実際上も，指定情報処理機関及び本人確認情報の提供を受けた国の機関等は，そ

れぞれ分散して情報を管理しており，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。そのため，控訴人が危惧する，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が生じるためには，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統一的に集約管理した上で，同法３０条の３４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か，あるいは，何者かが，不正アクセス防止法に違反して，多数の国の機関等から個人情報を盗取し，これを統一的に集約管理し，なおかつ，個人の多面的な情報が瞬時に集められる情報管理システムを構築することが必要になるが，このような事態はおよそ想定できるものではない。

(3)　「自己情報コントロール権の制度的保障の本質的欠如」について

控訴人は，「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問を生ずる。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。」などと主張する（控訴人準備書面(2)２２ページ７行目以下）が，かかる政策論は，訴訟における法的主張としては意味をなさない。

(4)　小括

以上のとおり，制度面において，住基ネットの総合的な安全性に何ら問題はなく，控訴人の主張は失当である。

2　「３　技術面（物理的セキュリティについて)」について

(1)　控訴人は，長野県で行われた住基ネット進入実験に実際に携わったイジョヴィ・ヌーワーが，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，総務省が，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ことを問題視したことを指摘し，住基ネットには，様々なセキュリティ上の脆弱性が現存していると主張する（控訴人準備書面(2)２３，２４ページ)。

しかしながら，控訴人も指摘するように，イジョヴィ・ヌーワーは具体的にどのような「セキュリティ上の問題」があったのかを全く示していない（控訴人準備書面(2)２３ページ）のであり，控訴人の主張はそもそも失当である。

(2)　また，控訴人は，「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。」，「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。」などと主張する（控訴人準備書面(2)２４，２５ページ)。

しかしながら，この点については被控訴人ら準備書面（1）の第３の２（2）ウ(ｲ)（２４ページ）において主張したとおり，住基ネットにおいては，権限のない者が容易にアクセスできないよう管理を行うとともに，市町村設置ファイアウォールを設置するなどしてＣＳを防御しているのであり，住基ネットの物理的セキュリティに問題があるとする控訴人の上記主張は失当である。

3　「４　運用面」について

(1)　「(2) 外部の者による情報漏えい－２（②)」について

控訴人は，ソーシャル・エンジニアリング手法や斜里町の事故などを摘示して，「こうしたずさんな運用は一部のケースかもしれないが，しかし住基

ネットは全国約１８００の自治体のＣＳサーバがＬＡＳＤＥＣの中央サーバに接続され，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。」などと主張する（控訴人準備書面(2)３０ページ)。

しかしながら，被控訴人ら準備書面(1)の第３の１(1)（１１ないし１３ページ）において既に主張したとおり，市町村のＣＳは，当該市町村の住民の本人確認情報を保有するのみであり，他の市町村の住民の本人確認情報を保有していないから，他の市町村の本人確認情報を閲覧，改ざんするためには他の市町村，都道府県及び指定情報処理機関が管理するファイアウォールを突破して地方公共団体の共同のネットワークである住帰ネット本体に侵入する必要があり，このような行為を実行することは極めて困難である。したがって，仮にある市町村におけるセキュリティ対策に不十分な点があるとしても，これが他の市町村の住民の本人確認情報のセキュリティに影響を与え，具体的危険を生じさせるわけではないことは，明らかであり，控訴人の主張は失当である。

(2)　「(3) 内部の者による情報漏洩（③)」について

控訴人は，控訴人準備書面(2)３１ないし３４ページにおいて，内部の者が故意に情報漏洩を行う危険性を摘示する。

しかしながら，内部の者に対する不正防止については，以下のような対策が採られているところであり，控訴人がるる指摘する点を踏まえても住基ネットのセキュリティに具体的な危険が生じているとはいえない。

ア　重い刑罰や監督による不正行為の防止

(ｱ)　改正法は，住基ネットに係る事務に従事する市町村，都道府県，指定情報処理機関及び本人確認情報の提供を受けた国の機関，地方公共団体

の機関等の職員に対し，本人確認情報処理事務等に関して知り得た本人確認情報に関する秘密又は本人確認情報の電子計算機処理等に関する秘密の保持義務を課し（住基法３０条の１７第１項，３０条の３１第１項，３０条の３５第１項及び２項），これに違反した者に，通常の公務員の守秘義務違反よりも重い刑罰を科している（例えば，国家公務員法１０９条１２号，１００条１項，２項及び地方公務員法６０条２号，３４条１項，２項は，１年以下の懲役又は３万円以下の罰金に処するとするが，住基法４２条は，２年以下の懲役又は１００万円以下の罰金に処するとする。）。また，住基法は，市町村，都道府県，指定情報処理機関及び本人確認情報の提供を受けた国の機関，地方公共団体の機関等の委託事業者に対しても，同様に，その事務に関して知り得た本人確認情報に関する秘密又は本人確認情報の電子計算機処理等に関する秘密の保持義務を課し（住基法３０条の１７第２項，３０条の３１第２項，３０条の３５第３項），これに違反した者に，２年以下の懲役又は１００万円以下の罰金を科している（住基法４２条）。

また，電気通信事業法１７９条２項により，住基ネットを運用する通信事業に従事する者が通信の秘密を侵した場合にも，重い刑罰が科される（３年以下の懲役又は２００万円以下の罰金）。

(イ) 行政機関個人情報保護法は，国の機関等の担当職員が正当な理由がなく個人情報を提供した場合や不正な利益を図る目的で個人情報の提供又は盗用を行ったり，職務の用以外の用に供する目的で職権を濫用して個人の秘密を収集した場合に重い刑罰を科している（同法５３条ないし５５条）。

(ウ) 指定情報処理機関に対する監督

上記(ア)の罰則のほかに，指定情報処理機関は，総務大臣による役員の選任等の認可，解任命令（住基法３０条の１６），本人確認情報管理

規程の認可（同法３０条の１８），事業計画の認可等（同法３０条の１９），監督命令（同法３０条の２２第１項），報告及び立入検査（同法３０条の２３第１項），指定の取消し（同法３０条の２５）等による監督に服するほか，委任都道府県知事による指示（同法３０条の２２第２項），報告及び立入検査（同法３０条の２３第２項）等の監督を受けるものとされている。また，指定情報処理機関は，本人確認情報の保護に関する事項等を調査審議するため，本人確認情報保護委員会を置くこととされており（同法３０条の１５），このような措置により適切な監督を受けている。

(ｴ) このように，住基ネットにおいては，住基法や関係法令は，関係者に重い刑罰を科したり，指定情報処理機関に対する監督を通じて，情報の漏洩や不正な目的での提供等が生じないような措置を講じている。

イ　照会条件の限定

本人確認情報の検索に際しては，①即時提供（端末機から照会条件を入力し，都道府県サーバ又は指定情報処理機関サーバから即時に本人確認情報の提供を受ける方式）の場合，「住民票コード」，「氏名＋住所」又は「氏名＋生年月日」を端末機に入力しないと本人確認情報の提供を受けられない仕組みとなっている。また，「氏名＋住所」又は「氏名＋生年月日」を入力する場合は，前方一致検索（文字列検索の手法の一つで，先頭の文字が一致する単語やフレーズを探す方法）が可能であるが，該当者が５０人を超えるときは本人確認情報の提供が受けられない。なお，前方一致検索は，少なくとも「氏名の先頭一文字＋住所全部」，「氏名全部＋住所の都道府県・市町村名を除いた先頭一文字」，「氏名の先頭一文字＋生年月日全部」の入力が必要である。

次に，②一括提供（本人確認情報照会対象者の情報をファイル化して都道府県サーバ又は指定情報処理機関サーバに照会し，これらのサーバから

照会結果ファイルを受け取る方式）の場合も，①と同様に，照会元から送られてきた「住民票コード」，「氏名＋住所」，「氏名＋生年月日」等のファイルに，都道府県サーバ又は指定情報処理機関サーバにおいて，本人確認情報を追記して照会元にファイルを返送するなどの措置が講じられている（照会条件について，セキュリティ基準第４－４－(7)参照・乙第３２号証）。

このように，担当者が当該個人情報を容易に検索できないような措置が講じられている。

ウ　操作者識別カード認証によるアクセス制御

本人確認情報は，ＣＳ，都道府県サーバ及び指定情報処理機関サーバ内に保存されており，端末機には存在しない。端末機からサーバにアクセスする際には，常に操作者識別カードと端末機との間で相互認証を行って初めて住基ネットアプリケーションが起動する設計とされており，アクセス権限のない職員等及び外部から本人確認情報データベースへアクセスすることはもちろん，住基ネットアプリケーションを起動することもできない。その上，操作者識別カードの種別により，システム操作者ごとに住基ネットが保有するデータ等へ接続できる範囲を限定している（セキュリティ基準第４－３－(1)，第４－４－(1)，(2)，(3)，(5)参照・乙第３２号証）。

このように，住基ネットにおいては，アクセス権限のない職員がアクセスできないような措置が講じられている。

エ　アクセスログの定期的解析と調査

指定情報処理機関は，運用管理規程に基づき，定期的に指定情報処理機関サーバのアクセスログの解析を行い，万一不正使用の兆候を検出した場合，緊急時対応計画等に基づき必要な連絡，対策等を実施する。

市町村は，都道府県に対し，あるいは，都道府県を経由して指定情報処理機関に対し，当該市町村の住民の本人確認情報に対するアクセスログの

解析要請を行うことができ，都道府県は，指定情報処理機関に対し，住民のアクセスログの解析要請を行うことができる（セキュリティ基準第４－４－(6)・乙第３２号証)。

このように，アクセスログの定期的なチェックにより，不正アクセス等を発見して適切な措置を講ずることができる。

オ　住民に対する本人確認情報提供状況の開示

住基ネットにおける本人確認情報の提供状況を開示するシステムについては，地方公共団体からの要望等を踏まえ，住基ネット推進協議会において検討が行われ，平成１５年２月７日，２次稼働をめどとして以下のようなシステムを開発することが決定された。

これは，都道府県サーバ及び指定情報処理機関サーバにおいて，本人確認情報提供状況の開示用データ（提供先／検索元，提供年月日，利用目的等）を生成する機能を装備し，都道府県は，都道府県サーバの開示用データ及び指定情報処理機関から送信される指定情報処理機関サーバの開示用データを保存し，それぞれの個人情報保護条例により住民から請求があった場合その開示を行うというものである。

そして，平成１５年１０月１日から本人確認情報提供状況の保存が開始され，同年１１月以降，準備が整った都道府県から順次，開示が開始されている（乙第３３号証の１，２。セキュリティ基準第６－８－(5)・乙第３２号証，住民基本台帳事務処理要領第６－５－(3)・乙第３４号証。)。

このように，当該個人に対しても，本人確認情報の提供状況を明らかにすることにより，当該個人に対して，不正使用の端緒が分かるようにしている。

カ　住民票の写しの広域交付における不正防止

住所地市町村において，交付地市町村の特定の操作者識別カード（操作者用ＩＣカード）から一定時間に一定数以上の住民票の写しの広域交付要

求があった場合は，不正な要求である可能性があることから，システム上，住民票の写しの広域交付を停止する措置が講じられている。

キ　担当職員に対する教育・研修

住基ネット関連のセキュリティ研修として，平成１４年度以降，４７都道府県において，市町村の住基ネット担当者を対象に，個人情報保護意識の向上，住基ネットの安全性の確保等を目的としたセキュリティ研修会が実施されているほか，総務省においても，地方公共団体職員や本人確認情報の提供を受ける国の機関等の担当職員に対する研修会を実施しているところである（乙第３５号証）。

ク　小括

以上のとおり，内部の者の故意による情報漏洩の危険に対し，住基法を始めとして，種々の方策が講じられているのであり，そのような危険をとらえて，住基ネットのセキュリティに具体的な危険性が生じているとみるのは相当ではない。

この点については，名古屋高裁金沢支部判決も，これらの対策により，「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。」と適切に判示しているところである（乙第２７号証３９ページ２０行目ないし４０ページ２０行目参照）。

(3)　「(4) 内部の者による情報漏洩（④）」について

控訴人は，「ＩＳＭＳ（情報セキュリティマネジメントシステム：引用者注）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。」などと主張する（控訴人準備書面(2) ３５ページ）。

しかしながら，上記(1)のとおり，ある特定の市町村におけるセキュリテ

ィ対策につき仮に不十分な点があるとしても，これが他の市町村の住民の本人確認情報のセキュリティに影響を与え，具体的危険を生じさせるわけではないから，控訴人の主張は失当である。

(4)　小括

以上のとおり，「運用面」においても，住基ネットのセキュリティに具体的な危険が生じているとはいえず，控訴人の主張は失当である。

4　「5　横浜市答申への反論」について

控訴人が，控訴人準備書面(2)３８ページ以下で主張する横浜市答申への反論については，その大部分が同準備書面第２の１ないし４において主張されたことであるか，従前の準備書面で主張されていたことの繰り返しであるため，新たな反論の要を認めない。

第３　結語

以上の次第で，控訴人の主張はいずれも失当であるか又は理由のないことが明らかである。本件訴えはいずれも却下されるべきであるが，仮にそうでないにしても，本件控訴はいずれも速やかに棄却されるべきである。また，当審において拡張された請求に係る訴えについても速やかに却下あるいは請求棄却の判断がされるべきである。