

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(1)

平成18年12月21日

東京高等裁判所第10民事部ハロ1係 御中

被控訴人兩名指定代理人

被控訴人国指定代理人

被控訴人東京都指定代理人

控訴人の平成18年9月26日付け準備書面(1) (以下「控訴人準備書面(1)」という。)における主張は、従前の主張の繰り返しや独自の見解に基づくものが多く、新たに反論を要するものではないが、なお念のため、被控訴人らは、必要と認める限度で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3章「『合憲的限定解釈論』に対する反論」に対する再反論」について

1 はじめに

控訴人は、「住基法30条の5第1項を憲法13条に適合するように合憲的限定解釈をすれば、行政との関係での利便性よりも、住基ネットからの本人確認情報の流出等の危険を重視しようとする住民の個人情報については、市町村長(…(略)…)は都道府県知事への通知義務を負わないと解すべきである」と主張する(控訴理由書53, 54ページ参照。以下「合憲的限定解釈論」ともいう。)。かかる主張は、住基ネットによる本人確認情報の流通・利用が、自己情報コントロール権を放棄しない住民との関係では、それらの住民の自己情報コントロール権を侵害するものであり、それらの住民の本人確認情報を住基ネットにより流通・利用することは違憲であるとの見解を前提とするものである。しかしながら、答弁書でも述べたとおり、自己情報コントロール権は、保護されるべき権利・利益の内容や範囲、法的性格が判然とせず、いまだ権利として成熟したものとはいえないものである。

この点をおくとしても、住基ネットにおいて利用又は提供される情報は、住民票の記載事項のうち、必ずしも秘匿される必要性が高いものであるということとはできない「本人確認情報」に限られている。加えて、住基ネットにおける「本人確認情報」の利用又は提供には、行政上の正当な目的や必要性があることが必要であり、かつ、その利用又は提供に厳格な限定がされているのであって、情報の漏えいや不正利用の具体的危険性も存在しないのであ

る。したがって、控訴人の主張する自己情報コントロール権を前提としてもこれを侵害するものではないことは明らかである。

このように控訴人の主張する「合憲的限定解釈論」はその前提を欠くものというほかないが、なお念のため、若干反論する。

2 第2「『第3 自己情報コントロール権と本人確認情報』に対する反論（答弁書17頁以下）について」に対する反論

- (1) 控訴人は、被控訴人らが「住民票コードが法律上禁止されるデータマッチングや名寄せに利用される具体的危険は認められず、住民票コードを秘匿する必要性は、高度であるなどということとはできない。」と主張したのに対し、「『住民票コードを秘匿する必要性』が高度であるからこそ、禁止規定を置いているのである。」と主張する（控訴人準備書面(1)21ページ）。

しかしながら、禁止規定を置いているからといって、ただちに「住民票コードを秘匿する必要性」が「高度である」と結論づけるのは論理の飛躍である。住民票コードを秘匿する必要性は高度であるなどということとはできないことについては、既に答弁書（17ないし19ページ）で述べたとおりである。

- (2) また、控訴人は、「『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』の記載は婚姻・離婚等を推知させうるものであるし、何もそれらの記載のみで『端的に推知させる』ものでなくても、他の情報と併せることにより推知させることが十分ありうるのである。」と主張する（控訴人準備書面(1)23ページ）。

しかしながら、「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」の記載のみによって、何故、婚姻・離婚等が生じたことが推知されることになるのか理解できない。また、控訴人のいう「他の情報」については、その情報が何であるのかを全く明らかでないから、根拠とはならない。

(3) さらに、控訴人は、「住民基本台帳に記載されている情報が『従来から公開情報とされていた』こと自体が不適切であったのであり、それゆえに住民基本台帳法が改正されたのである（平成18年6月15日、同年法律第74号）。」と主張する（控訴人準備書面(1)23ページ）。

しかしながら、今回の平成18年法律第74号による法改正では、閲覧制度がダイレクトメール等の民間の営業活動で利用されていることが、住基法1条の目的に照らして広すぎるのではないかといった点が考慮されたものであり、住民基本台帳に記載されている情報が従来から公開情報とされていたこと自体が不適切であったことを理由として行われたものではない。よって、控訴人の主張は失当である（乙第22号証、第23号証）。

3 第3「『第4 自己情報コントロール権と住基ネット』に対する反論（答弁書21頁以下）について」に対する反論

(1) 控訴人は、東京地裁平成18年4月判決において、『相応の安全性』という場合の安全性とは、それなりの安全性であり、十分な安全性ではないことを示しているわけである。なお、同判決としても『漏えい、改ざんについて（中略）若干の可能性が否定できない』として、危険を認めざるを得なかった点に留意すべきである。」と主張する（控訴人準備書面(1)24ページ）。

しかしながら、同判決は、「本人確認情報はその秘匿の必要性が必ずしも高くない上、住基ネットにおける本人確認情報の利用提供の態様は限定されたものであるということができること、住基ネットにおいて本人確認情報の漏えい、改ざんなどの具体的危険性があるとまではいえないことからすれば、住基ネットにおける本人確認情報の利用提供の態様は、一般的に許容される限度を超えない相当のものであるということができ。」（乙第15号証41ページ）と判示し、原告の請求を棄却しているのであり、住基ネットにおける情報漏えいや改ざんの具体的危険性を肯定するもので

はないことは明らかである。控訴人の主張は、判決の一部を殊更に強調して誤った解釈を導こうとするもので相当ではない。

- (2) また、控訴人は、「将来において法改正により堂々と『行政機関による大規模なデータマッチングや名寄せが行われる』ようになる危険が現時点において認められると言うべきである。」と主張する（控訴人準備書面(1) 24ページ）。

しかしながら、本件において問題とされているのは、飽くまでも現行の住基法であるから、現行の同法を前提として主張すべきことは当然である。控訴人の上記主張は、根拠もなく、将来においてデータマッチングや名寄せが行われる可能性を殊更強調するものであって、失当である。

なお、控訴人は、「公務員の法令遵守義務があれば足りるというのはいかにも単純すぎるのであり、公務員の違法行為や過失が全くありえないかのような前提は現実性を欠いていると言うべきである。」と主張する（控訴人準備書面(1) 25ページ）が、あえて公務員の違法な行為等を想定し、住基ネットの危険性を論じるのは適当でない。

- (3) さらに、控訴人は、「そもそも、住基カードの利用が極めて乏しいため、既に「住基法が予定する効果の達成は著しく困難」になっていると言うべき」などと主張する（控訴人準備書面(1) 27ページ）が、既に述べたとおり、住基ネットは、行政サービスの向上と行政事務の効率化を目的とするシステムであるだけでなく、我が国の国家戦略である電子政府・電子自治体の実現のために不可欠な基盤を成すものである。控訴人の主張はこのような住基ネットの意義を正しく理解しないものであって、失当である。

3 小括

以上のとおり、控訴人の主張は、現行の住基法に基づく住基ネットの運用を正しく理解せず、憶測を述べるにすぎないものである。したがって、控訴人の主張する自己情報コントロール権を前提とするとしても、住基ネットの

運用が何らこれを侵害するものではなく、控訴人の主張はその前提を欠くものであって、失当であることは明らかである。

第2 第4章「『住基法・地方自治法から導かれる区の裁量権論』に対する反論 に対する再反論」について

1 はじめに

控訴人は、「関連する法体系との整合的かつ合理的な解釈をすべきことは当然のことである」などとして「体系的解釈」について論じている（控訴人準備書面(1)29ページ）が、法令の解釈を行う際には、立法者の意思を表すものとして、その規定の文理を十分尊重すべきものであり、「体系的解釈」の名の下に、規定の文理を全く離れた恣意的な解釈をすることは許されない。本人確認情報の送信につき控訴人に裁量権が認められるべきである旨の控訴人の主張は、住基法30条の5第1項及び2項の規定の文理に明らかに反し、これを無視するものである。

控訴人は、改正法の趣旨及び目的や改正法を踏まえた関係法令の改正等について正解せず、専ら「地方自治法制との関連」や「個人情報保護法制との関連」から、本人確認情報の送信につき控訴人に裁量権が認められるべき旨を強弁するにすぎず、このような解釈方法が不相当であり、採用できないことは、答弁書（28ないし30ページ）において詳論したとおりである。

2 第1「住基法解釈のあり方について」に対する反論

- (1) 控訴人は、被控訴人らが「セキュリティ基準（乙第8号証）第4-9-(4)は、不正アクセスが判明した場合の対応について、「都道府県知事、市町村長及び指定情報処理機関は、不正アクセスが判明した場合、相互に連絡調整を行い、被害状況の把握、被害拡大を防止するための措置等必要な措置を講ずること」を定め、ファイアウォールで不正アクセスの徴候を発見したときなど本人確認情報に脅威を及ぼすおそれの高い事象が確認され、

本人確認情報の漏えい等の危険が具体的に発生した場合のように、緊急かつやむを得ないと客観的に認められる事情の存する場合に、応急的な措置として、市町村長又は都道府県知事が、一時的に住基ネットとの切断等の措置を講ずることを定めたものにすぎない。したがって、具体的な漏えい等の危険性が生じていないにもかかわらず、住基法36条の2を根拠として、一部の住民の本人確認情報を通知しないという取扱いを恒常的に行うことは許されない（乙第9号証）のであって、セキュリティ基準は、同法30条の5第1項及び2項の送信義務規定の適用範囲を限定するものなどではないことは明らかである（原判決75, 76ページ）。」と主張した（答弁書30, 31ページ）のに対し、「なぜ、緊急かつやむを得ないと客観的に認められる事情があれば、応急的な措置が認められるのであろうか。そのような措置を取ることができるという、住基法の明文規定があるであろうか。この点は、本人確認情報の保護というプライバシー権保護の見地から、条理上、住基法30条の5が予定していると解釈するほかない。」「結局、被控訴人自ら体系的条理解釈を認めており、原判決も緊急時にかかる措置を取ること自体は容認しており、同様である。住基法30条の5の解釈として、切断が認められること自体は争いがないのである。」などと主張する（控訴人準備書面(1)30, 31ページ）。

しかしながら、被控訴人らが、住基法30条の5の解釈として、一部の住民の本人確認情報の通知をしないという取扱いを恒常的に行うことを認めるものでないことは明らかである。

すなわち、被控訴人らは、住基法36条の2について、「法（引用者注：住基法）に定める事務を実施することを前提として住民票等に記載されている事項又は本人確認情報の適切な管理のために必要な措置を講ずべきことを規定したものであり、また、住基ネットについては、制度面、技術面及び運用面において個人情報保護のための措置が講じられていることを

考えあわせても、この規定を根拠として市町村長…（略）…の判断で、住基ネットを運用せず、法に定める本人確認情報の通知等の事務を行わないとすること（いわゆる住基ネットからの離脱又は不接続）はできない」（乙第8号証）と解することを前提として、上記のとおり、「具体的な漏えい等の危険性が生じていないにもかかわらず、住基法36条の2を根拠として、一部の住民の本人確認情報を通知しないという取扱いを恒常的に行うことは許されない（中略）のであって、セキュリティ基準は、同法30条の5第1項及び2項の送信義務規定の適用範囲を限定するものなどではない。」と主張しているのである。したがって、被控訴人らが、住基法30条の5の解釈として、一部の住民の本人確認情報の通知をしないという取扱いを恒常的に行うことを認めるものでないことは明らかであって、控訴人の上記主張は、被控訴人らの主張を曲解するものであり失当である。

- (2) また、控訴人は、「住基ネットの総合的な安全性が確認できるまでの段階的な参加を求めているのであり、未来永劫恒常的に切断し続けるというものではない。その意味では、あくまでも一時的であって恒常的な切断という批判は当たらない。」などと主張する（控訴人準備書面(1)31ページ）。しかし、セキュリティ基準第4-9-(4)にいう「一時的」な「住基ネットとの切断等の措置」は、住基法に定める事務を実施することを前提として、「緊急かつやむを得ないと客観的に認められる事情の存する場合」を指すのであって、住基ネットについては、制度面、技術面及び運用面において個人情報保護のための措置が講じられていることからすれば、控訴人が主張するように「住基ネットの総合的な安全性が確認できるまでの段階」を「一時的」なものと解する余地がないことは明らかであり、控訴人の主張は失当である。

3 第2「地方自治法制との関連について」について

控訴人は、「住基法と地方自治法は、単純に一般法・特別法の関係にたつ

わけではなく、『地方自治の本旨』の実現を目指す地方自治法制を無視した解釈をすることは許されない。特別法であることを理由として、地方分権の方向性を否定する被控訴人らの主張こそ不当である。」と主張する（控訴人準備書面(1)33ページ）。しかし、被控訴人らは、答弁書（32ページ）でも主張したように、「住基法は、(中略)地方自治法10条1項、及び(中略)同法13条の2に基づき制定された法律であり、地方自治法の特別法に位置付けられるべきものである」旨主張しているのであり、「『地方自治の本旨』の実現を目指す地方自治法制を無視」しているわけでも、「地方分権の方向性を否定」しているわけでもない。よって、控訴人の主張は失当である。

4 第3「個人情報保護法制との関連について」について

- (1) 控訴人は、「被控訴人らの主張では、およそいかなる利用方法でも、行政機関等が一定の行政目的を実現するためであれば、すべて行政の合理化に資するのであるから、本来の目的の範囲内に収まることになり、個人情報保護法制は行政機関等との関係では全く無意味化する。」と主張する（控訴人準備書面(1)33ページ）。

しかしながら、住基法30条の34は、受領者は、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ているのであるから、控訴人の主張は、住基法に関する誤った解釈に基づくものであり、失当である。

- (2) また、控訴人は、「立法政策の変更の可能性を無視して、現時点で問題がなければ、将来どうなるろうとも構わないというような解釈論は無責任であり、適切ではない。」と主張する（控訴人準備書面(1)35ページ）が、前記のとおり、本件においては現行法令の規定の解釈が争点となるべきものであり、いまだ不明である将来の立法政策の変更の可能性などは争点とはならない。なお、被控訴人らは、控訴人主張のような解釈論は採ってい

ない。

5 小括

以上のとおり、控訴人は、市町村長が住民基本台帳事務を処理する際には、住基法の規定の文理や目的・趣旨に即した解釈適用をするのが当然であるのに、これに反した恣意的な取扱いを正当化しようとするために「体系的解釈」の必要性を強弁するにすぎず、その主張は失当であるというほかない。

第3 第5章及び第6章「『住基ネットの危険性』についての補充的主張」に対する反論

1 「第5章 北海道斜里町、帯広市、福島県塙町への調査嘱託回答結果について」に対する反論

(1) はじめに

控訴人は、東京地方裁判所民事第50部が行った北海道斜里郡斜里町、北海道帯広市及び福島県東白川郡塙町（以下、順に「斜里町」、「帯広市」、「塙町」といい、三者を併せて「別件各市町」という。）に対する調査嘱託の結果（甲第58号証ないし60号証（各枝番を含む。）、以下「別件東京地裁50部調査嘱託の結果」という。）を踏まえ、斜里町で住基ネットに関する情報が流出した事実（以下「斜里町事案」という。）、帯広市の嘱託職員による住民基本台帳の業務外閲覧の事実（以下「帯広市事案」という。）及び塙町で住民票コードが記載された名簿が配布された事実（以下「塙町事案」といい、斜里町事案、帯広市事案と併せて、「別件各事案」という。）に基づいて、「住基ネットの危険性」について補充的に主張する（控訴人準備書面(1)35ないし61ページ）。

しかしながら、本件においては、控訴人が被控訴人東京都に対し、杉並区民のうちの通知希望者のみに係る本人確認情報の送信を行い、非通知希望者に係る本人確認情報の送信を行わないという取扱いが、住基法30条の5に

違反するか否かが問題とされるべきであるところ、控訴人の上記主張は、同条の解釈に何ら関係のないものであって、そもそも失当であるというほかない。

この点をおくとしても、住基ネットとは、各市町村、各都道府県及び指定情報処理機関において電子計算機を設置し、市町村長が都道府県知事に、委任都道府県知事が指定情報処理機関に本人確認情報をネットワークにより通知し、それぞれ各市町村、各都道府県及び委任都道府県の住民に係る本人確認情報を保存することとした地方公共団体の共同のシステムである。具体的には、①各市町村に、既に設置されている住民基本台帳事務のコンピュータ（既存住基システム）との橋渡しをするためのコンピュータ（CS（コミュニケーション・サーバ））を新たに設置し、②電気通信回線による送信又は磁気ディスクにより、既存住基システムからCSに、本人確認情報を渡して市町村の本人確認情報を保存し、③各市町村のCSを専用回線で結んでネットワーク化し、④都道府県レベルに47のサーバを、全国レベルに一つのサーバを設置し、⑤CSから各都道府県サーバに、各都道府県サーバから全国サーバに、最新の本人確認情報を通知し、それぞれ各都道府県の住民の本人確認情報、全国の住民の本人確認情報を保存しているものである。そして、既存住基システムと住基ネット（具体的にはCS）は、ファイアウォールを介して接続されているが、既存住基システムも高いセキュリティが確保されている上、CS及び既存住基システムは、インターネット等の外部のネットワークと接続している公開サーバ（情報系）等の機器とは分断されている。

したがって、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。すなわち、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、他の市町村の住民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基ネット本体に侵入する必要があるところ、かかる行為を実行することは極めて困難である。

また、このような住基ネットの構築状況を踏まえた上で、別件各事案をみるならば、別件各事案は、控訴人の区内に住む住民（取り分け、住基ネットからの離脱を求める住民）のプライバシーを侵害する現実的・具体的危険性を認める根拠になるようなものではなく、「住基ネットの危険性」についての控訴人の補充的主張は、理由のないものである。

むしろ、別件東京地裁50部調査嘱託の結果により、別件各事案は、現実に住基ネット自体から個人情報が出たものではなく、いずれも住基ネットのセキュリティ上は問題がないことが明らかになったというべきである。

念のため、若干補足する。

(2) 別件各事案は住基ネットのセキュリティ上問題とはならないこと

ア 斜里町事案について

(ア) 斜里町長作成の平成18年5月18日付け「調査嘱託について（回答）」

（甲第58号証の2。以下「斜里町回答」という。）によれば、斜里町事案は、斜里町役場の本庁舎及びウトロ支所に設置されている住基ネットのCS端末等から、本人確認情報が流出したものなどではなく、斜里町の総務環境部ウトロ支所係員で、住基ネット関連業務を含め、支所業務全般を担当していた職員が、その自宅に保管している「私物であり、公用として使用したことはない」個人用パソコン（斜里町回答2及び5③）から斜里町の保有する業務資料等が流出したものである。

(イ) 斜里町回答によれば、流出した情報のうち住基ネット関連の情報は、斜里町回答末尾添付の資料2であるところ（斜里町回答4③）、同資料2を

子細に検討しても、当該情報の中に、住民基本台帳に関する個人情報は一切含まれていない。また、流出したという住基ネットに関連するパスワードも「平成15年度当時の古いパスワードで現在は使われていない」ものである（斜里町回答4③）。さらに、資料2に含まれている全国センターから各市区町村住民基本台帳ネットワークシステム担当課長あてにされた「Windows2000のセキュリティホール（MS04-025）の対策について（通知）」と題する事務連絡文書についても、その1枚目に「平成16年7月31日にマイクロソフト株式会社より、緊急の対応を必要とするセキュリティ情報『Internet Explorer用の累積的なセキュリティ更新プログラム（867801）（MS04-025）』の発表がありましたので、お知らせします。」とあるように、平成16年当時のオペレーションシステム（OS）上の脆弱性に関する公開情報とその対応策を通知したものであり、通知内容に対する対策は既に完了している（乙第24号証の2）。

その余の流出した情報（斜里町回答添付の資料1（甲第58号証の2）参照）も、住基ネットのセキュリティを左右するものではないから、結局、斜里町事案は、住基ネットのセキュリティ上、何らかの問題を生じさせるものではないことが別件東京地裁50部調査囑託の結果明らかになったというべきである。

イ 帯広市事案について

帯広市長作成の平成18年5月15日付け「調査囑託書について（回答）」（甲第60号証の2。以下「帯広市回答」という。）によれば、平成15年8月21日から平成16年1月13日までの間にあった、いわゆる不正閲覧は、一般事務を担当する職員が「宛名管理システム（既存住基システムとの連携により宛名情報を提供するシステムで、住基ネットとは直接的に接続していないもの。）」（帯広市回答1③参照）を職務外で使用し、同システムにより表示された宛名情報を閲覧したというものであり、また、平成

17年6月18日から同年10月12日までの間にあった不正閲覧は、証明交付事務を行う嘱託職員が職務外で既存住基システムの端末で住基ネットとは直接的に接続していないものを使用し、上記既存住基システムの画面を閲覧したというものであった（帯広市回答1①③，2，3②③，4①ないし③）。このように、いずれの不正閲覧も、住基ネットのCS端末を不正に操作したのではなく、住基ネットそれ自体から情報が流出したのではないから、帯広市事案は、住基ネットそれ自体のセキュリティとは全く関係のないことが明らかになったというべきである。

ウ 埴町事案について

埴町長作成の平成18年5月17日付け「調査嘱託書について」（甲第59号証の2。以下「埴町回答」という。）によれば、埴町事案は、平成16年9月13日、行政区長を集めて実施した「平成16年度敬老会打合会議」の席上で、埴町役場の保健福祉課福祉係長が配布した75歳以上の招待者名簿に住民票コードが記載されていたというものであって（埴町回答1）、住民票コードの情報が、住基ネットシステムそのものから直接流出したのではないから、やはり、住基ネットそれ自体のセキュリティとは全く関係のないことが明らかになったというべきである。なお、上記名簿は、その場ですべて回収されている（埴町回答7〔3〕）。

(3) 別件各市町は住基ネットのセキュリティの確保に適切に努めていること

そもそも、特定の市区町村におけるセキュリティ対策を問題として、他の市区町村の住民の本人確認情報のセキュリティに対する具体的危険性を考えること自体が失当であるが、この点をおくとしても、以下に述べるとおり、別件東京地裁50部調査嘱託の結果によれば、回答した別件各市町のセキュリティ対策は適切にされていることが明らかになったというべきである。

ア 住基ネットシステムの設置状況について

(7) 斜里町について

斜里町においては、権限のない者が容易にCSにアクセスできないようにするため、施錠した部屋にCSを設置し、必要のない限り職員が立ち入れないようにし、その入退出については、入退出管理簿を備え付けて管理している上、CSと既存住基サーバとの間にファイアウォールを設置し、さらに、住基ネットに無線LAN及びダイヤルアップ接続を使用せず、CS端末からインターネットや外部の電子メールを利用できないようにするなどして（甲第58号証の2。斜里町回答6(1)）、CSを防御している。

(イ) 帯広市について

また、帯広市においても、権限のない者が容易にアクセスできないようにするため、パスワードやIDカードにより入退室管理ができる専用の部屋にCSを設置した上（甲第60号証の2。帯広市回答5(1)イ）、既存住基サーバとの間にファイアウォールを設置し（帯広市回答5(1)ウ）、さらに、住基ネットに無線LAN及びダイヤルアップ接続を使用せず、CS端末からインターネットや外部との電子メールを利用できないようにするなどして（帯広市回答5(1)）、CSを防御している。

(ウ) 埴町について

さらに、埴町においても、パスワードやIDカードにより入退室管理ができる専用の部屋にCSを設置した上（甲第59号証の2。埴町回答6(1)イ）、住基ネットにおいて無線LAN及びダイヤルアップ接続を使用しない（同エ及びカ）、住基ネットのサーバ及びCS端末からインターネットや外部との電子メールを利用できないようにするなどして（同オ）、CSを防御している（なお、埴町回答がファイアウォールに言及していないのは、調査事項に入っていないからであると考えられる。）。

(I) 小括

このように、いずれの別件各市町においても、住基ネットシステムの設

置状況をとらえて、本人確認情報の流出の危険があるなどといえないことは明らかである。

イ セキュリティポリシーの制定、外部監査の実施について

セキュリティポリシーや外部監査の実施は、住基ネットのセキュリティを保持するための必要条件でなく、一部の市町村がセキュリティポリシーを制定していなかったり、外部監査が実施されていないからといって、このことが直ちに住基ネットのセキュリティの低下をもたらすものではない。

この点をおくとしても、斜里町では、個人情報保護条例及びセキュリティポリシーを制定し、自己点検及び確認を毎年度実施している（甲第58号証の2。斜里町回答6(2)）。また、同町では、平成18年3月16日、全職員に対し、個人情報や業務資料等が記載されている媒体の外部持ち出しの禁止、私物パソコンを含め、「Winny」をはじめとするファイル交換ソフトの使用の禁止について指示を出し、再発防止に向け速やかに対応しているところである（斜里町回答2）。

また、帯広市では、個人情報保護条例及びセキュリティポリシーを制定した上、毎年度、内部監査委員による監査を実施しており（甲第60号証の2。帯広市回答5(2)ア）、現に住基ネットそれ自体から情報が流出した事実はない。

さらに、埴町では、同町事案が発生した当時は、個人情報保護条例は制定されておらず、セキュリティポリシーが制定されていたのみであったが、同事案発生後、平成16年11月から個人情報保護条例が施行され、また、内部監査も実施されるに至っており（甲第59号証の2。埴町回答6(2)）、現在まで住基ネットそれ自体から情報が流出した事実はない。

このように、別件各市町は、住基ネット及び既存住基システムのセキュリティの確保に努めており、別件各事案の発生を踏まえてもなお、住基ネット及び既存住基システムに関する市町村のセキュリティ対策は適切に確保

されているというべきである。

ウ 人的管理状況及びパッチ当て等について

控訴人は、「人的管理状況」、「セキュリティパッチ当て」等についても調査嘱託事項に挙げているが、この点については、別件東京地裁50部調査嘱託の結果を踏まえても、住基ネットから情報が流出する具体的危険性を認め得る事情を見いだすことはできない。

(4) 小括

以上のとおり、別件東京地裁50部調査嘱託の結果によれば、別件各事案はいずれも住基ネットのセキュリティ上問題となるものではない上、別件各市町は住基ネットのセキュリティの確保に適切に努めているというべきであるから、同調査嘱託の結果は、控訴人の区内に住む住民のプライバシーを侵害する具体的・現実的危険性を根拠付けるものとならないというべきである。

したがって、別件東京地裁50部調査嘱託の結果を踏まえても、控訴人の主張に理由がないことは明らかである。

この点、東京地裁民事50部は、平成18年7月26日に言い渡した判決（乙第25号証）において、住基ネットには、「外部者の侵入による本人確認情報の漏洩を防止するための、合理的なセキュリティ対策が講じられているというべきである。」（同判決82ページ）、「運用関係者による漏洩の危険に対しても、これを防止するための様々な措置が講じられているというべきである。」（同判決84ページ）との判断を示した上で、当該調査嘱託の結果を踏まえた上で、別件各事案は「いずれも、住基ネットからの情報漏洩の危険に関する判断を左右するものではない。」との判断を示している（同判決85ページ）。

2 「第6章 さいたま地裁における調査嘱託の結果について」に対する反論

(1) はじめに

控訴人は、さいたま地方裁判所第6民事部が行った埼玉県比企郡小川町

(以下「小川町」という。), 所沢市, さいたま市, 朝霞市及び狭山市 (以下, これらの市町を総称して「さいたま調査自治体」ともいう。) に対する調査嘱託の結果 (甲第61号証ないし65号証, 以下「別件さいたま調査嘱託の結果」という。) を踏まえ, 住基ネットの運用によって, 住基ネットへの侵入, 個人情報の流用・漏洩の危険がある旨主張する (控訴人準備書面(1)61ないし66ページ)。

しかしながら, 本件においては, 控訴人が被控訴人東京都に対し, 杉並区民のうちの通知希望者のみに係る本人確認情報の送信を行い, 非通知希望者に係る本人確認情報の送信を行わないという取扱いが, 住基法30条の5に違反するか否かが問題とされるべきであるところ, 控訴人の上記主張は, 同条の解釈に何ら関係のないものであって, そもそも失当であるというほかない。

この点をおくとしても, 前記1で述べた住基ネットの構築状況に照らせば, 住基ネットに対する外部からの直接的なアクセスや攻撃は想定することすらできないのであって, 住基ネットには十分なセキュリティが確保されているというべきである。また, 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, 直ちに他の市町村の住民の本人確認情報のセキュリティに具体的危険が生じるわけではないことも前述のとおりである (本書面12, 13ページ)。

念のため, 控訴人の主張に対し, 若干反論する。

(2) 「第1 セキュリティの問題について」について

ア 「1 CS端末等の設置台数が多数にのぼる点」について

(ア) 控訴人は, さいたま調査自治体では, CS端末, 特に既存住基サーバとネットワークで結ばれている端末は至る所に設置されており, これらの端末を通じて既存住基サーバが攻撃されて管理者権限を略奪される危険性が高く, 更に, 同サーバが拠点とされて住基ネットサーバ

が攻撃され、その管理者権限も略奪される危険性が高い旨主張する（控訴人準備書面(1) 6 2 ページ）。

(イ) しかしながら、CS、都道府県サーバ及び指定情報処理機関サーバ間の通信は、すべて専用回線及び専用交換装置で構成されたネットワークを介して行い、また、指定情報処理機関サーバと国の機関等サーバとの間は、専用回線又は磁気媒体でデータ交換を行う。したがって、これらのサーバ以外との通信を行うことはできない（セキュリティ基準第3-3）。また、サーバ間で相互認証・暗号通信を実施しており、仮に他のコンピュータをネットワークに接続できたとしても、通信を行うことはできない（乙第26号証5ページ）。そして、住基ネットの通信プロトコルは、独自の住基ネットアプリケーションによる独自プロトコルであり、インターネットで用いられる汎用的なプロトコルを使用していない。このため、その内容を解析して、当該通信を疑似した不正アクセスを行うことは不可能である。また、すべてのCSのネットワーク側、すべての都道府県サーバのネットワーク側及び指定情報処理機関サーバの全方向に指定情報処理機関監視ファイアウォールを設置して、インターネットで用いられるプロトコルの通過を遮断している（セキュリティ基準第4-3(2)）。さらに、住基ネット全体で徹底したコンピュータウイルス・セキュリティホール対策を実施している上、不正な通信の遮断をしている。このような点のみに照らしても、控訴人の主張は失当である。

(ウ) そもそも、上記(ア)の控訴人の主張するような危険性が生じるためには、①いずれかのCS端末から既存住基サーバが攻撃され、②管理者権限が奪取され、③それを拠点として住基ネットサーバが攻撃され、④住基ネットサーバの管理者権限も奪取されるという段階を経る必要があるところ、以下に述べるように、いずれの段階の想定もおよそ現

実的なものではない。

まず、上記①及び②については、CS端末のOS（コンピューターシステム全体を管理するソフトウェア。）権限を取得するだけでも、到底容易ではない。

次に、上記③は、既存住基サーバを拠点として住基ネットサーバが攻撃されるという主張であると解されるが、住基ネットシステムと既存住基システムを橋渡しするCSについては、指定情報処理機関監視ファイアウォールによって不正な通信を遮断しており、また、既存住基システムと接続し、端末機を設置するため、CSと既存庁内LANを接続する場合にも、市町村が厳格に管理するファイアウォールによって、既存住基システム・端末機側からの不正な通信を遮断している（なお、さらに、既存庁内LANが外部ネットワークと接続する一部の団体は、市町村管理のファイアウォールを設置し外部からの不正な通信を遮断している。）。

このように、CSセグメントと既存住基サーバセグメントとの間にはファイアウォールが設置されており、当該ファイアウォールを通過する通信は制限されている。そして、上記④についても、既存住基サーバから庁内LANを通じて市町村設置ファイアウォール越しにCSのOSの管理者権限が取得される具体的危険性が長野県侵入実験によってさえ実証されておらず、一般論としてその取得が不可能であることは、原審における被告ら準備書面(8)第7（25ないし28ページ）に述べたとおりである（なお、インターネットから庁内LANへ侵入される具体的危険性も実証されていないことは、同書面第3・10ないし14ページに述べたとおりである。）。

したがって、既存住基サーバに接続されている端末がそのまま住基ネットのセキュリティホールになるかのような控訴人の上記(ア)の主張

は、失当である。

イ 「2 セキュリティ対策の不十分性」について

(ア) 「リスクアセスメントの欠如」について

控訴人は、さいたま調査自治体が、いずれも「リスクアセスメント」を行っていないと論難する（控訴人準備書面(1)63ページ）。しかしながら、「リスクアセスメント」にも様々な手法があるのであって、埼玉県においては、さいたま調査自治体を含めた同県内の全自治体において、総務省によるチェックリストを利用した自己点検を実施しており、これもリスクアセスメントの一種といえることができるのであるから、むしろ、同県内の各自治体においては、リスクアセスメントが定期的に行われているというべきであり、控訴人の主張は失当である。

(イ) 「第三者監査の欠如」について

また、控訴人は、小川町やさいたま市を取り上げ、第三者監査を受けていないと論難する（控訴人準備書面(1)63ページ）が、外部監査の実施は住基ネットのセキュリティを確保するための必要条件ではなく、外部監査が実施されていないことが直ちに住基ネットのセキュリティの低下をもたらすものでないことはいうまでもない。

各市町村は、セキュリティ基準を遵守して住基ネット及び既存住基システムのセキュリティの確保に努めているところであるし、その取組状況については、上記チェックリストに基づく自己点検が実施されているのみならず、当該自己点検の結果を踏まえ、都道府県、総務省及び指定情報処理機関が必要な指導・助言を行っているのであるから、住基ネットについて情報漏洩等の具体的危険性は存在しない。

(ウ) 「担当職員のセキュリティ対応能力の欠如」について

控訴人は、専任職員を配置しなければ、直ちに情報漏洩等の具体的

危険が生じるとの認識を前提に、小川町、所沢市、朝霞市及び狭山市においては、住基ネットの運用に関して、専任職員が配置されていないと論難するようである（控訴人準備書面(1)64ページ）が、住基ネットの担当職員に対しては十分な研修等が行われており、専門的知識を要する事項については、各市町村の情報担当課からサポートを受けたり、総務省、都道府県又は指定情報処理機関から技術的な助言を受けたりして事務を行っている。控訴人の上記主張は、何ら具体的証拠に基づかずに、自治体の担当職員に資質がないなどと論難するものにすぎず、失当である。

なお、控訴人は、「狭山市では、住基ネット導入に伴う職員研修も行っていない。」と主張する（控訴人準備書面(1)64ページ）が、狭山市が主催する職員研修は行われていないものの、住基ネット導入時のほか、その後においても、総務省、LASDEC及び埼玉県による説明会や資料配付等が定期的に行われているから、上記主張は失当である。例えば、平成17年6月15日には、同県内全市町村の住基ネット担当者等を対象とする「住民基本台帳ネットワークシステム担当者研修会」が実施され、狭山市の担当者もこれに出席している上、同日、埼玉県主催で、組織的なセキュリティ対策についての啓発として「ISMSセミナー」が実施され、これについても狭山市の担当者が出席している。

ウ 「3 操作者識別カード、パスワード」について

(ア) 控訴人は、さいたま調査自治体においては、パスワードや操作者識別カードが割り当てられている職員の数が多く、その範囲も広い上、パスワードの変更頻度が少ない（なお、狭山市においてはパスワードを変更したことがない。）ことから、住基ネットのセキュリティが低下すると主張するようである（控訴人準備書面(1)64、65ページ）。

しかしながら、割り当てられている操作者識別カードの種類や数が多いのは、適切な管理を行うために、権限等をより細かく分けている結果であるし、操作者識別カードの数が少なければ、必然的に複数の職員で共用することになり、万一不適正な利用があった場合の責任追及等が困難になるという面もあるのである。してみると、上記控訴人の主張する事態が直ちに住基ネットのセキュリティを低下させるものとはいえないことは明らかである。

- (イ) また、控訴人は、パッチ当てが極めて迅速に行われなければ、直ちに不正侵入等の具体的危険が生じるとの認識を前提として、セキュリティパッチ当ての回数が不十分であり、かつ適用時期も遅いなどと論難する（控訴人準備書面(1)65ページ）が、かかる主張も失当である。すなわち、パッチが公開されてからパッチ当てが行われるまでの間にある程度の時間を要するものであることは、住基ネットを構成するCSのみならず、あらゆるコンピュータについていえることである。だからこそ、一般に、コンピュータネットワークにおいては、いわゆる物理的対策やファイアウォールを設置するなどの対策を講じる必要があるとされているのであり、パッチ当てにある程度の時間を要しているからといって、このことから直ちに住基ネットにおいて情報漏洩等の具体的危険が存在するなどということはない。そして、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。このCSの安全性が総合的に確認されていることは、長野県侵入実験においても、ファイアウォール越しにCSを攻撃することは全くできなかったことからしても明らかであり、これはパッチが公表されていないセキュリティホールであっても同様である。

エ 小括

以上のとおり、さいたま調査嘱託の結果を踏まえても、住基ネットへの侵入及び個人情報の流用・漏洩の具体的危険があるなどとは到底いえない。

(3) 「第2 行政の効率化に関して」について

ア 控訴人は、住基ネットの目的の正当性とは、「行政の効率化」であり、ここにいう「効率化」とは経費の削減であることを前提として、さいたま調査嘱託の結果を踏まえ、住基ネット関連費用が膨大であり、削減された経費がほとんどないなどとして、住基ネットには「行政の効率化」効果が存在しない旨主張する（控訴人準備書面(1)67, 68ページ）。

イ しかしながら、既に述べたとおり、住基ネットは、国及び地方公共団体を通じた行政の効率化・合理化を図るとともに、行政手続における住民の負担軽減、住民サービスの高度化等により住民の利便を増進するため、地方公共団体の共同のシステムとして、各種行政の基礎であり居住関係を公証する住民基本台帳のネットワーク化を図り、本人確認情報により全国共通の本人確認ができる仕組みを構築し、また、市町村の区域を越えた住民基本台帳に関する事務の処理を行うための体制を整備しようとするものであり、広範な行政事務において、住民負担の軽減と行政事務の効率化及び正確性の向上を実現し、また、行政手続のインターネット申請を可能にし（その基盤となるのが公的個人認証サービスである。）、さらに、市町村のネットワーク化による住民基本台帳事務の簡素化及び広域化を実現することを目的として導入されたものであり、電子政府・電子自治体の基盤となる不可欠なシステムである。

そして、一部の住民の離脱を認めることは、その都度非通知希望者であるかどうかを確認せざるを得ないことになり、対象となる事務の内容によっては、非通知希望者に関する事務のみならず、住基ネットの利用を全面的に見合わせざるを得なくなることも予想されること、住民の一

部にでも不参加があると、ネットワークが寸断され、ネットワークによらない事務処理を存置せざるを得ないなど、効率化が阻害されることになることから、離脱を認めることは住基ネットの行政目的を著しく害することになるのである。

したがって、住基ネットの立法目的の合理性及び必要性が認められること、住基ネットに多くの利便性が認められることは明らかであるから、控訴人の上記主張はその前提において失当である。

第5 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訴え却下あるいは請求棄却の判断がされるべきである。