

平成18年11月15日

杉並区長 山田 宏 様

杉並区住民基本台帳ネットワークシステム調査会議

委員 田 島 泰 彦

委員 稲 垣 隆 一

委員 佐々木 俊 尚

## 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

杉並区住民基本台帳ネットワークシステム調査会議（以下「調査会議」という。）は、住民基本台帳ネットワークシステム（以下「住基ネット」という。）の構築に伴う諸問題について調査・検討を行い、杉並区長に報告することを課題に、平成14年7月に設置され、これまでに、同年8月1日、8月28日、平成15年5月29日の3回、報告をまとめてきたところである。

この度、当調査会議は、平成18年9月15日、18杉並第58888号により、現時点において、住基ネットについて、制度面、技術面及び運用面などあらゆる面で、総合的な安全性を確認することができるかについて、杉並区長から諮問を受けた。

本日、当調査会議は、

- I 住基ネットとプライバシー
- II 住基ネットとセキュリティ
- III 住基ネットと監視社会
- IV 住基ネットと横浜市・審議会の答申

の各項目のもとに住基ネットの安全性について総合的な検証と考察を加えた結果、住基ネットの総合的な安全性を確認するには至らなかったとの結論に達したので、報告する。その理由、根拠等の詳細は以下報告するとおりである。



# 杉並区住民基本台帳ネットワークシステム調査会議報告書

(第四回・平成18年11月)

## 目 次

I	住基ネットとプライバシー	1
1	住基ネットの制度と経緯	1
2	個人情報保護法の未制定と住基ネット	1
3	個人情報保護法の制定と課題	3
4	住基ネットとプライバシー	4
	(1) 住基ネットとプライバシー侵害の危険性	4
	(2) 求められるプライバシー保護のあり方	5
II	住基ネットとセキュリティ	6
1	住基ネットの物理的セキュリティは安全なのか	6
2	物理的セキュリティ以外の住基ネットの脆弱性について	11
3	住基データが漏洩した場合、どのような危険性が存在するのか	22
III	住基ネットと監視社会	24
1	個人情報保護と住基ネット	24
	(1) 現代社会における個人情報保護のあり方	24
	(2) 住基ネット上の本人確認情報の意義	26
2	監視社会と住基ネット	26
	(1) 監視社会の状況と進展	27
	(2) 監視社会における住基ネットの意義と役割	29
3	終わりに	30
IV	住基ネットと横浜市・審議会の答申	30
1	答申の概要	30
2	答申の問題点	32
	(1) 個人情報保護法制度の不備は解消されたか	32
	(2) 名寄せ等による情報の一元管理の懸念は解消されているか	33
	(3) 個人情報保護法制度以外の問題点は解消されたか	33
	(4) その他の問題点	34
3	答申の結論は妥当か	35
	別紙1	36
	別紙2	37
	別紙3	39

## I 住基ネットとプライバシー

### 1 住基ネットの制度と経緯

2002年8月5日、住基ネットがスタートした。これは、1999年の住民基本台帳法（以下「住基法」という。）の改正によって導入された仕組みで、国民一人一人に番号（住民票コード）を振り、氏名・生年月日・性別・住所などの基本情報とそれらの変更情報（本人確認情報）をコンピュータネットワークで全国的、一元的に管理しようとするものである。2003年8月には、希望者にICチップ内蔵のカード（住基カード）も交付され、本格稼働（第二次稼働）がなされた。

このシステムは、一連の行政上の申請などに際し、住民票の添付が省略されるなどの便利さをもたらす一方、国民総背番号制などと批判されるような個人情報の国家による過剰な管理・統制や、大規模大量の情報漏洩などプライバシーやセキュリティへの懸念を呼び起こしたため、その対応策として、個人情報保護の法整備を改正法の附則で定めた経緯があった。

ところが、2002年の国会でも、個人情報保護に関する主要な二つの法案（主として民間を対象とする個人情報保護法案と行政機関個人情報保護法案）が未成立のまま住基ネットが見切り発車的にスタートするという事態を前に、個人情報保護法制と住基ネットとの関係が改めて問われることになったのである。

そこで、個人情報保護法制の未整備などを理由に、東京都杉並区、国立市、中野区、国分寺市、福島県矢祭町などの自治体はネットワークに参加せず、また横浜市はネットワークへの参加を個々の住民の選択に委ねる方式を採用した。

2003年5月、継続審議を繰り返してきた、個人情報保護法案と行政機関個人情報保護法案を中心とする個人情報保護関連五法案が衆参両院を通過し、可決成立した。また、同年8月、住基カードの発行を含む、第二次稼働（本格稼働）がスタートした。これらを受けて、従来離脱をしてきた自治体の中でも見直しが進められ、中野区、国分寺市は参加へと態度変更をした。また、杉並区は選択制へと方針を変更した。さらに、長野県の田中知事（当時）は、第二次稼働前の8月15日、現行のシステムから離脱し、県独自システム構築を目指す方針を明らかにした。

個人情報保護法の制定と住基ネットの関係をめぐる問題は、おおよそ以上のような経緯をたどってきたのであるが、本節では、住基ネットの問題性を個人情報保護法制との関わりを中心に考察したい。具体的には、その論点を法律制定前の問題（後述2）と制定後の課題（後述3）に分けて検討し、最後にプライバシーの観点から住基ネットの問題点を総括的に明らかにしたい（後述4）。

### 2 個人情報保護法の未制定と住基ネット

前述したように、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、当時の小淵首相も、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（1999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）、個人情報保護法制の整備でこれに応えようとした経緯があった。

ここから考えると、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の整備であることは確かであるので、住基ネットが稼働した2002年8月から、個人情報関連法が可決成立した2003年5月までは、必要とされた法律が制定されていなかったのであるから、住基ネット稼働の前提を欠いており、その下での稼働は違法と断ぜざるを得ない。

附則1条2項の趣旨につき、総務省は、「個人情報の保護に関する法律の整備について言えば、政府は、立法機関ではなく、自ら法律を制定することはできないものであるため、『所要の措置』とは、法律案の検討、作成、国会への提出を意味し、政府としては、平成13年3月に個人情報保護法案を国会に提出したことにより、『所要の措置』を講じたことになると考えています」と説明しているが（総務省のホームページ掲載の「住民基本台帳ネットワークシステム/個人情報保護法案について」）、法律は制定されていなくとも、法案を提出しさえすれば政府の責任は果たされたとする論理は驚くべき詭弁であり、とてつもなく無責任な態度である。附則は個人情報保護の法律の制定を明確に要請していると解するべきである。

また、改正住基法で目的外利用の禁止や守秘義務違反への重罰など、十分な保護措置を施してあるとの主張もみられたが、附則規定や小淵答弁は、住基法上の規定に加えて一層の保護措置を求めた趣旨としか理解できず、これらの説明には説得力がない。いずれにせよ、以上のような説明では、保護法制未整備のままの住基ネットの見切り発車を正当化するのは困難である。

そこで、前述したように、こうした事態を前にして、杉並区などいくつかの自治体は住基ネットに参加せず、また横浜市は住基ネットへの参加を個々の住民の選択に委ねるとの方針を決めた。住基ネットへの強制を拒否し、批判する抵抗の拠りどころとして、自治体が改正住基法附則の規定や小淵首相の国会答弁に着目し、それを援用するのは、住民の個人情報の保護に責任を負っている自治体の立場としては、けだし当然であり、少なくとも、住基ネットの実施に密接に関わる個人情報保護法制が整備されない限り、住基ネットの稼働は違法の疑いが濃く、自治体の住基ネットへの参加は見合わされて然るべきなのである。政府は不参加自治体の対応を違法と非難したが、個人情報保護法未制定の段階での自治体の不参加は合法であり、むしろ参加することのほうが違法と評価されるべきである。

### 3 個人情報保護法の制定と課題

個人情報保護の関連法案が2003年の通常国会で可決成立したことは先に記したが、それではこれにより附則の要件は充足されたと言えるのであろうか。結論から先には、例えば、今回の法律制定によりこの要件が満たされたと考えるのは困難である。

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、小淵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。

#### 4 住基ネットとプライバシー

##### (1) 住基ネットとプライバシー侵害の危険性

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。

## (2) 求められるプライバシー保護のあり方

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。

## II 住基ネットとセキュリティ

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、財団法人地方自治情報センター（以下「LASDEC」という。）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。以下、それらセキュリティ脆弱性がどのようなものなのかという点についてと、加えて住基データが流出した場合にどのような危険性があるかということについて詳述する。

### 1 住基ネットの物理的セキュリティは安全なのか

そもそも、脆弱性のまったく存在しないというネットワークは、論理的には存在しない。セキュリティ業界では「100パーセント完璧なセキュリティは存在せず、その脆弱性が既知のものか未知のものかにかかわらず、どのようなネットワークでも必ず脆弱性は存在する」という受け止め方が、事実上の標準である。

では住基ネットには、いかなる脆弱性が存在しているのか。

住基ネットに関しては技術情報のほとんどが公開されておらず、多くは推測に頼るしかない。だがこれまでマスメディアや専門家のレポートなどで公開された情報から、ある程度は推し量ることができる。

2004年11月11～12日、東京都内でセキュリティ関連イベント「PacSec.jp/Core04」が開かれ、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）氏が参加した。

Nuwere氏はこのイベントで講演する予定だったが、講演内容の一部に総務省が難色を示し、Nuwere氏の当初の意向に沿う形での発表が難しくなったため、最終的に同氏の判断で講演は見送られることになった。この件についてNuwere氏は11月12日、自身のブログ（注1）で次のように書いた（注2）。

「日本政府が私の講演を禁止

[住基ネットは日本の国民IDシステムである。私は一年前、長野県のためにこのシステムのセキュリティ監査を行った。]

長い一日だった。総務省、すなわち住基ネットを維持する日本政府が、PacSecセキュリティカンファレンスでの私の今日の発表を差し止めた。総務省は、今現在政府から契約を得ようと努めている日本のイベントを脅して、私が話せないようにしたのだ。

日本政府は私に二つの選択肢を与えた。

- 1) 話すな。
- 2) 彼らの求める通りのことを言うように、抜本的にスライドを変更しろ。



スライドを一切使わずに、私自身の意見を言うのではどうかと申し出たところ、彼らは私に\*一切何も\*話すことは許されざるべしと告げた。私にとって明らかなのは、彼らが私のスライドやプレゼンを問題にしているわけではないということだ。彼らは、私が住基ネットの問題に注意を引くのを恐れていたのだ。総務省は問題から逃れられると思っている。彼らは、人々がその問題について話すのを禁止しておけば、問題はどこかへ消えてしまうと考えているのだ。私は、そのような日本政府の圧力から免れると思っていたが、そうした圧力をかける総務省の能力について、過小評価していた。

私に話すのを禁ずるにあたって、総務省の言い分はこうだ。「我々はこのカンファレンスを後援しているのだから、君の講演を止めろと言う権利が当然ある。」もしそうなら、日本政府は、気に入らない\*いかなる\*イベントであろうとも、単に協賛や後援をしておくだけで、その組織に内容変更を強制できてしまう。もしそうなら、日本は今後決して、より安全な環境へ向けて進歩することは無くなるだろう。

私が一番いらいらする点は、私は日本政府を\*非難するつもりはなかった\*という事実なのだ。私の話は、両方の側から挙げられた問題について、非常に公平でバランスのとれた扱いをするはずだったのだ。実際、総務省がかかえているかもしれない問題について、私と直接会って話せるように、彼らを招待もした。私はこのことを彼らに、電話でも、Eメールでも話した。しかし彼らは、カンファレンスの代表者達に圧力をかける方を選んだ。彼らは私と直接話すよう試みもしなかった。これはどういうことなんだ？

私が言うかも知れないことで、もしも彼らに何か問題があるというなら、どうして私にそう言わなかったのだ？政府との契約に頼っている会社に、どうして圧力をかけるのか？これがフェアと言えようか？私の話の目的は、住基ネットセキュリティシステムの両面について述べることだった。私には、それが失敗しようと成功しようと、何らの既得権益があるわけでもない。私はただ、それをもっと安全にするにはどうするのが一番か、システムを改良するにはどうするのが一番か、忠告をしたかっただけなのだ。しかし総務省は、セキュリティをいかに改善するかという私の忠告それだけで、住基ネットには問題があるという意味なのだろうと思い込み、この内容を認めることを拒絶したのである。こう言うのは残念だが、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！もし日本政府が、問題を指摘する誰かに耳を傾けようとしなければ、一体どうしてシステムが安全になるというのか。

今日は日本にとっては悲しむべき日であり、私にとってはフラストレーション

を引き起こす日だった。」

上記のブログで、Nuwere氏は「住基ネットにはセキュリティ上の問題がいくつかあるのだ。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、この発言には以下の二点の重要性がある。

- ① 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。
- ② 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。

また『ASAHI パソコン』（朝日新聞社刊）は、2004年3月1日号で、『長野県の住基ネット実験で、総務省が徹底反論 「侵入に使用した脆弱性は MS03-026」 修正プログラムの適用とチェックが焦点に』という記事を掲載した（注3）。以下のような内容である。

「本誌は2月1日号（1月6日発売）News&Viewsで、住基ネットの安全性について長野県が行った実験の中間報告を速報した。記事の執筆・取材の時点（2003年12月中旬）で、事実関係が不明確だったり、確認困難な部分があったりしたため、全体像をはっきりさせることができなかつた面がある。今回、関係者への再取材によって、最も基本のデータである脆弱性の種類も、具体的に明らかになった。こうした事実関係などを含め、実験の内容を再検証する。

まず、実験の内容をまとめてみよう。長野県は同県本人確認情報保護審議会メンバーの吉田柳太郎氏に委託して、昨年9～10月と11月の2回、県内の3町村と協力し、住基ネットの安全性確認実験を行った。同県の発表によれば、内容は以下の通りだ。

この実験では、長野県と総務省の間の情報交換はかなり乏しいようだ。「長野県に詳しい情報の提供を求めても、なかなかこたえてもらえない」と、同省市町村課の上仮屋尚・本人確認情報保護専門官はいう。実験の概要を把握した後、総務省は次のような見解を明らかにした。

- 【1】 施錠された重要機能室に鍵を借りて入り、侵入用端末を設置するなど、「侵入実験」として適切ではない。CSサーバーや端末のOSの管理者権限を奪取しても、住基ネットのデータに不正アクセスすることはシステム上、不可能だ。
- 【2】 FWを通過するポート番号がわかっても、対応する脆弱性がシステム上になければ侵入はできない。