甲第71号証

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　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）が未成立のままで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（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、附則規定や小渕答弁は、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で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渕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。結論から先に言えば、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。

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。

(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いなら、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った面がある。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。

【３】市町村の庁内ＬＡＮ部分に対する侵入は、住基ネットには直接関係しない。だが住民票データなどが改竄された場合、誤った情報が住基ネットを流れる危険性はある。また、住基ネットとは関係ないが、庁内ＬＡＮのサーバーには、税や国保など重要な個人情報が収納されているので、市町村に一層のセキュリティー対策を呼びかける必要がある。

また、ＣＳサーバーの管理者権限を奪っても、LASDEC側から通報がなかったことを長野県は問題視しているが、LASDECが２４時間監視しているのはファイアウォールまでで、そこから先は市町村の責任領域としている。いずれにせよ問題は、住基ネットのデータに不正アクセスできるかどうかだ。

従来、総務省は「住基ネットはＩＣカードとパスワードがなければ動かないシステム」と説明してきているが、長野県側がカードなしでＯＳを乗っ取り、カード認証の有効性に疑問を抱かせた。この点について、前出・上仮屋専門官は以下のように説明する。

「住基ネットのデータは、ＣＳ端末に組み込まれた専用のアプリケーションからしか検索・閲覧できない。このアプリは、ＩＣカードとパスワードの認証がなければ起動・操作できません」

つまり端末―サーバー間のＯＳレベルのやりとりのほかに、アプリケーションレベルでの認証が必要なシステムになっているということだ。ＩＣカードとパスワードがアプリケーションレベルの認証に使われているという事実はこれまであまり明らかにされておらず、長野県の発表でも触れられていなかった。

同省市町村課の高原剛・住民台帳企画官は「パスワード設定などに一部甘さがあったことは反省点」としつつ、「データ漏洩は、住基ネットを停止しなければならないほどの事態。今回の実験でそんな事態が起きるとは考えていない」と見解を語る。

本誌の取材に対して、吉田氏は「実験に使用したセキュリティーホールはMS03-026」と明かした。ほかに、MS03-039とMS03-046も、修正プログラムが当たっておらず、利用可能だったという。MS03-026は昨年７月１７日に公開された。大流行したウイルス「MSブラスト」にも悪用された点で記憶に新しい。

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。先ほど吉田氏が挙げた３つの脆弱性は、その時期のものであるため、ＣＳサーバーに関しては、両者の主張する事実関係はそれなりにかみ合う。

だがＣＳ端末については、当時の最新の脆弱性であるMS03-049（１１月１２日発見）以外はすべて、実験の行われた１１月２５日より前に修正プログラムの適

用を市町村に要請していたという。

「ＣＳサーバーはＦＷで保護された位置にあり、脆弱性の影響を直ちには受けないが、ＣＳ端末はＦＷ外にある場合が多く、短期間の動作確認テスト後、できるだけ早く適用を要請している」と、LASDEC住民基本台帳ネットワークシステム全国センターの戸田夏生担当部長はいう。この要請通りに処理されていれば、ＣＳ端末の MS03-026 や 039、046 などは解消されていたはずであり、これらの脆弱性を突いてＯＳを乗っ取ることはできない。

この点が長野県側と国側の主張の最大の食い違いであり、今後の検証の重要なポイントだ。本誌では、端末の乗っ取りの詳細や、実際に市町村レベルで修正プログラムがどう適用されていたかなど、引き続き関係者に具体的な確認を求めているが、ＣＳ端末の乗っ取りが成功したということは、修正プログラムの適用やチェックの態勢に大きな課題を残したと言えるだろう。(後略)」

この記事で『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、「MS03-026」だったことを突き止めている。この「MS03-026」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「MS03-026」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。

住基ネットは、LASDECが管理する部分と、市町村が管理する部分とに分かれている（別紙１、注４）。その境界に当たるファイアウォール（ＦＷ③）から右側は、LASDECが不正アクセスを２４時間監視している。左側の市町村管理部分では、ＣＳサーバーなど重要な機器は「重要機能室」と呼ばれる施錠した部屋に保管されている。住基ネットのデータ検索などはＣＳ端末から行うが、ＣＳ端末は重要機能室に置かれている場合もあれば、庁内に置かれている場合もある。

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「MS03-041」「MS03-042」「MS03-043」「MS03-044」「MS03-045」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。

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

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できるのだろうか。

そうではない。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。

横浜市本人確認情報等保護審議会は２００６年４月、「住民基本台帳ネットワークシステムの総合的な安全性について」という答申において、次のように述べている。

「4　結論

(1)　住基ネットの総合的な安全性について

住基ネットの安全性を判断するに当たり、制度面、技術面及び運用面の３つの側面から、考察していく。

ア　制度面について

横浜方式導入の最も大きな理由である個人情報保護法制度の不備については、個人情報保護法等が施行され適正に運用されていること、地方自治体における個人情報保護条例及びセキュリティポリシーの制定状況等を見ると着実に整備されてきていると判断できる。

また、他自治体への調査請求やアクセスログ開示請求の仕組みなど、その他、横浜市が懸念した問題点についても、様々な個人情報保護に対しての制度化が進んでおり、制度面からみた問題点は、解消されていると見ることが出来る。

なお、住基ネットに関し、「名寄せなどにより情報が一元管理されるのでは」「プライバシーの侵害では」との懸念の声もあるが、これらについては住民基本台帳法で「本人確認情報の利用及び提供の制限」や「住民票コードの告知要求制限」、「住民票コードの利用制限」などの規定があること、また、住民票コードについても、自らの申請で何度でも変更が可能な制度となっており、自己情報コントロール権が保障されているともいえることから、これらの懸念に対しては、制度面で一定の措置が取られているといえる。

イ　技術面について

稼働当初から専用回線の利用のほか、通信を行う際の相互認証及びデータの暗号化、ファイアウォール及び侵入検知装置の設置とこれらの２４時間常時監視を行うなど、外部からの不正侵入に対し、適正な防止策が採られている。このことは、品川区におけるペネトレーションテスト等でも実証されている。

また、ＩＣカード及びパスワードにより操作者の限定を行うとともに、操作履歴及びアクセスログの取得・解析等により、いつ、誰が、住基ネットを使用したのか追跡調査が可能となっている。これらのように外部からの不正侵入への防止策のほか、内部の不正使用に対する防止策も講じられていることから、技術面でも充分な個人情報保護対策がなされているといえる。

ウ　運用面について

国等の研修や指定情報処理機関等の技術支援による各地方自治体のセキュリティに対する意識・技術の向上はもちろん、不測の事態発生を想

定した訓練等、個人情報保護に向けた運用面の取り組みは、充分なレベルに達していると考えられる。

このように、横浜市が当初懸念していた事項は、国及び横浜市等の対応により解消されている。これは、横浜市が取り組んだ成果として評価に値するが、審議会としては、単に住基ネットのセキュリティ向上にとどまらず、住基ネットや住民票の閲覧制度について、横浜市が警鐘を鳴らしたことで、住基ネットだけでなく、国の個人情報保護に対する考え方自体を変えることができたものではないかと考えている。

したがって、横浜方式の導入の理由である個人情報保護法制度の不備も解消され、セキュリティ強化に向けた指摘事項についても一定の対応がなされたこと、並びに今後もセキュリティ向上に向けた対応がなされていくと推測されることなどを踏まえると、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。」

また２００３年６月に開かれたイベント「RSA Conference 2003 Japan」で、東京工業大学フロンティア創造共同研究センターの大山永昭教授が「政府調達の現場と情報セキュリティ」というセッションの中で、「住民基本台帳ネットワークとＩＣカードのセキュリティ」と題して講演した。大山教授はスマートカードの第一人者であり、政府のＩＴ戦略会議・ＩＴ戦略本部合同会議で委員を務めるなど、住基ネットのキーパーソンの一人である。

大山教授は、講演の中で以下のような趣旨のことを述べている（注６）。

「安全性に関して、技術的側面ではネットワークの専用回線化、データの暗号化、ファイアウォールの設置、データの改変やソフトの追加ができないようにコンテンツサーバーの専用化、１人１枚の端末操作用カード、ログの記録、ネットワークのモニタリングが行われている。運用面では、管理・運用規定の制定、職員の研修、システム安全性の第三者評価を実施。」

横浜市・審議会の答申、住基ネットキーパーソンである大山教授のいずれも、

（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。

以下、その点について記す。

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。

以下は、同年３月２９日に同町が配布した追加の報道発表資料である（注８)。

「業務資料の流出に関する追加説明

昨日、業務資料のネットワーク上への流出について、内容を説明し、町民をはじめとする関係者に対し、お詫びを申し上げたところでありますが、説明に当たって、住基ネットに関して説明が不足しておりましたので、改めて説明をさせていただきたいと思います。

まず、住基ネット情報の内容でありますが、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、及び、全国自治情報センターから送付された通知文が流出したものでありますが、まず、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。

今回、流出したパスワードは平成１５年当時のもので、現在使用されていないものであります。

また、住基システムに関連する「セキュリティーホールの対策について」という通知文書でありますが、平成１６年に全国自治情報センターから送付されたオペレーションシステム上の脆弱性に関するもので、これについても、すでに処理が終わっているもので、今回の流出によって現システムに影響があるとは考えていなかったところであります。

従いまして、これらの情報の流出によって、住基ネットシステムに外部から侵入できるという認識には立っていなかったことから、特に説明をしなかったものであります。

しかし、いささかでも疑念があれば、特に住基ネットについては社会的にも関心の高いものでありますから、昨日の会見で報告をすべきであったと、反省しているところであります。従いまして、斜里町の情報管理の不適切であったことについて、改めてお詫びをし、再発防止に全力を挙げることを申し上げて、追加の説明とさせていただきます。」

では、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だったのだろうか。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。

また、「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、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。以下は、当時の日本経済新聞の記事である。

「住基ネット用　データ盗まれる　バックアップ向け　福島・岩代町９６００人分

福島県岩代町（大内正男町長）が住民基本台帳ネットワーク（住基ネット）に記載した全住民約九千六百人分の個人情報などを収めたデジタルテープが、町が管理を委託したコンピューター処理会社の社有車から盗まれていたことが二十八日までに分かった。

町によると、盗まれたテープは震災などに備えたバックアップ用のデータで、住基ネットに利用される氏名、住所、生年月日、性別、住民票コードと変更履歴の六情報が入っている。内容は暗号化され、専用の機器や十分な知識がないと解読は難しいうえ、住民番号なども入力している住基ネットの保管用テープそのものではないという。

大内町長は「住民に不安を与えぬよう早急に対応策を検討する」と述べた。

福島署などによると、二十六日午後六時二十分ごろ、町から情報の管理を委託された同県郡山市のコンピューター処理会社「エフコム」の福島市中町の駐車場で、社員が社有車から離れた数分の間に、後部座席の窓ガラスが割られてテープを入れたジュラルミンケース（長さ約四十センチ、幅約十センチ、高さ約十五センチ）がなくなっていた。車には鍵がかかっていた。福島署が窃盗事件として捜査している。

町によると、エフコムには一九九七年から財務処理を委託し、今年八月の住基ネット稼働時からテープの管理を任せていたという。

総務省の井上源三市町村課長によると、盗まれたデータは住基ネットのサーバーに登載する情報の基になったものとみられ、町民の個人情報などが含まれているが、データは暗号処理されているという。（２００２年１２月２８日、日

本経済新聞夕刊１１面)」

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。

同様の事件は、内部犯行によっても起こりうる。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。

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を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。

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。同県は公式ホームページで、以下のように説明している（注１１）。

「住基ネットは、制度面、技術面及び運用面から様々なセキュリティ対策が講じられており、平成１４年８月の稼動以来大きなトラブルや事故は発生していませんが、今後とも個人情報の保護を徹底し、県民の安心の確保を図ることが重要です。

このため、県が管理する住基ネットシステムの情報セキュリティ対策が、一定の水準を満たし、組織的かつ継続的に取り組みが行われていることを客観的に説明できるように、第三者評価の認証を取得しています。（平成１７年３月２５日）

この認証を維持するためには、年１回の継続審査を受ける必要があるため、平成１８年３月にその継続審査が実施され、認証の継続が認められました。

なお、当初取得したISMS審査基準（ISMS認証基準（Ver.2.0）（国内規格）及びBS7799-2：2002（英国規格））は、平成１７年１０月から国際規格であるISO/IEC 27001：2005 に移行したため、今回の継続審査においては、移行後の基準であるISO/IEC 27001：2005 に対する認証を取得しました。」

以下、ISMSについて、WIKIPEDIA日本語版での記述を記す。

「情報セキュリティマネジメントシステム（じょうほう － 、ISMS：Information Security Management System）は、情報に関するセキュリティを管理するための仕組。以降では特に記載の無い限り、日本での状況を記載する。

情報処理サービス業に対し、コンピュータシステムの安全対策が十分かどうかを認定する制度として、旧通産省の「情報システム安全対策実施事業所認定制度」

（以下、安対制度という）があった。安対制度では主に施設・設備等の物理的な対策に重点がおかれ、対象業種としてはデータセンターを持った情報処理業が対象となっていた。平成１２年７月に通商産業省から公表された「情報セキュリティ管理に関する国際的なスタンダードの導入および情報処理サービス業情報システム安全対策実施事業所認定制度の改革」に基づき、（財）日本情報処理開発協会（JIPDEC）にてスタートさせた民間主導による第三者認証制度である。

以下の様な理由により、安対制度はISMSへと発展的解消されている。

- 情報処理の発展に伴い、情報処理に関するセキュリティは情報処理業のみではなく、あらゆる業種が対象となる
- 国の制度から民間の制度へ（規制緩和）
- 情報セキュリティ管理に関する国際的な標準の導入

BSI（英国規格協会）によって規定された、BS 7799 がベースとなって標準化が進んでいる。BS 7799 は Part１と Part２の２部構成になっている。Part１は情報セキュリティ管理の実施基準が、Part２にはその仕様が書かれている。

ISMS認証基準はPart２を基準に策定されているが、Part１の内容も取り入れた形になっている。

また、ISO化も進められており、BS 7799-1 については、ISO/IEC 17799 として策定されており、BS 7799-2 についても、ISO/IEC 27001 として策定されている。

JIS化も行われており、ISO/IEC 27001 は JIS Q 27001 として、ISO/IEC 17799 は JIS Q 27002 として、策定がされている。

ISMSでは、情報資産を特定し、リスクを洗い出し、リスク軽減を行う形で、セキュリティを高める。

情報資産は、以下の切り口で洗い出しを行う。

- 情報資産：データベース、データファイル、手順書、監査証跡など
- ソフトウェア資産：業務用ソフトウェア、システムソフトウェア、開発用ツールなど
- 物理的資産：コンピュータ装置、通信装置、記録媒体など
- サービス資産：ユーティリティ（空調、電源、照明）など
- 人的資産：資格、技能、経験など
- 無形資産：組織の評判、イメージなど

これらの情報資産に対して価値、影響度、蓋然性を基準として評価し、機密性、完全性、可用性の観点から、リスク対策を実施する。

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。

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

住基データが漏洩した場合、その危険性はどこにあるのかを、以下述べる。

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。

（注１）http://www.ejovi.net/archives/2004/11/japanese_govern.html[ejovi.net]
（注２）翻訳はスラッシュドットジャパンに掲載されたものによる。
（注３）http://www.asahi.com/tech/apc/040226.html
（注４）この図は日経BP社『ITPro』編集部による。
（注５）「住基ネットに対するペネトレーションテスト結果報告」（総務省、平成一五年十月十七日）

（注６）「【レポート】RSA Conference - 住基ネットと住基カードのセキュリティ」
(http://journal.mycom.co.jp/news/2003/06/03/22.html)
（注７）WIKIPEDIA (http://ja.wikipedia.org/wiki/)
（注８）自治体情報政策研究所ホームページ
(http://www.jj-souko.com/elocalgov/contents/c1096.html) より。
（注９）JCA-NET　北海道斜里町から流出したとみられる「住基ネット」関連ファイル
(zip圧縮) (http://www.jca.apc.org/e-GovSec/etc/anotherAndLink.html)
（注１０）http://www005.upp.so-net.ne.jp/jukisosho/news/news20_4.htm
（注１１）埼玉県公式ホームページ「住基ネットシステムにおけるISMS認証の継続について」
(http://www.pref.saitama.lg.jp/A02/B000/juki-net/keizoku_isms.html)

Ⅲ　住基ネットと監視社会

1　個人情報保護と住基ネット

(1)　現代社会における個人情報保護のあり方

ア　１９６０年代以降、個人の情報をはじめ、さまざまな情報を大量かつ迅速に、収集・管理・利用することを可能とするコンピュータが官民を問わず急速に普及する状況を迎え、またこのようなコンピュータのネットワークがインターネットの出現・普及により急速に進展し、プライバシーの保護は新たな段階に入った。ここでは、自分が知らないうちに、他者により自分に関する情報が勝手に集められたり、利用されたり、自分について間違っていたり不正確な情報が保有され、それに基づいて一定の判断や措置が行われる、さまざまな形で利用される危険が顕在化していった。

こうした事態を前に、従来主張されてきた、単に一人でほおっておいてもらう消極的な権利では、そのような危険に十分対処し、人間の尊厳は守りきれないと考え、自己情報の開示・訂正請求権を含め、自分についての情報は自分がコントロールする権利としてプライバシーの権利を積極的に捉える見解が提唱されるようになった。

イ　コンピュータやインターネットの発展など情報化社会におけるプライバシーへの脅威を考えると、自己情報のコントロール権としてプライバシーの権利を積極的に構成することは支持されてしかるべきだと考える。

そして、このコントロール権の対象に含まれる自己情報には、個人の私的領域

に属する情報、すなわち狭い意味でのプライバシーとして捉えられる情報だけではなく、それ以外の領域に属する個人情報をも広く含めて考える余地がある。プライバシー権に基礎付けられた自己情報のコントロール権の制度化として、個人情報保護制度を捉える考え方である。

ウ　他方で、個人情報の保護制度は、憲法の表現の自由などの原則と十分調整される必要がある。なぜならば、“個人情報”保護という概念は、従来、メディアの取材・報道などとの調整概念として裁判所により探求・提示されてきた“プライバシー”保護の観念が、表現の自由や報道の自由を踏まえた限定的な概念である（たとえば、私事性の要件や免責の法理など）のと異なり、そうした限定性を欠き、「個人が識別可能な」一切の情報を、公私の区別なく対象とし、管理の局面も含め広く規制し、市民に開示・訂正等の積極的な請求権を付与し、相手方にそれに応じる重い負担を義務づけるなど、はるかに広範で強力な規制を要請しているからである。

エ　こうした点を考えると、自己情報のコントロール権に裏付けられた個人情報保護制度は、政府など公的機関への規制の枠組みとして理解されるべきであり、こうした官への厳格な規制は表現やメディアを含む民間の領域にストレートかつ一律に及ぼされるべきではない。

まず何よりも確保されなければならない課題は、統治に関わって、また統治の一環として政府や自治体などの公的機関が保有する国民や住民の個人情報の取り扱いへの規制であり、それに対する市民のアクセスとコントロールの拡充強化である。

今日、政府・自治体は、私たちの生活に関わる膨大で重要な個人情報を広く収集・管理・利用しており、公権力による個人情報の誤用・濫用や個人情報の過剰な管理と監視社会体制の構築を許さず、人間の尊厳や自由と自律を確保するためには、何よりも国家からのプライバシーや個人情報の保護が不可欠だからである。この種の個人情報の公共的性格は、個人情報保護制度が自己情報のコントロール権の一環として憲法上の保障を受ける根拠をもち、それへの厳格な規制を要請し、開示や訂正などの請求権の行使も十分に正当化されると考えられる。

オ　他方で、政府・自治体など公的機関だけでなく、今日、膨大な個人情報を収集・管理・利用し、時に濫用してきた民間部門へも一定の規制強化が求められているのは確かであるが、この点では、個人情報の自由な流通の確保などへの配慮が欠かせない。というのは、民間においては、憲法の表現の自由とそれに由来する情報の自由な流通、学問の自由、そして私法の一般原則である私的自治の原則や憲法上の営業活動の自由などが妥当し、市民の原則自由な活動が保証されて然るべきであり、個人情報保護のための規制には、その目的において官への規制に準じた根拠が求められるとともに、目的にふさわしい規制の程度・態様が選択される

必要があるからである。民間には多種多様な活動主体と活動内容が見られるので、その規制のあり方も一律ではなく、柔軟で多様なあり方が求められるべきである。

(2) 住基ネット上の本人確認情報の意義

ア 公権力が管理・利用する個人情報に対して自己情報のコントロール権としてのプライバシーの保護が広く及ぶべきだとすれば、住基ネット訴訟金沢地裁判決（２００５年５月３０日）が判示するように、住基ネット上の氏名、住所、生年月日、性別の本人確認情報もその保護範囲と考えることは当然である。

この点では、金沢地裁判決が引用しているように、早稲田大学名簿提供事件最高裁判決（第二小法廷。２００３年９月１２日民集57巻8号973頁）が既に、氏名、住所等の「個人情報についても、本人が、自己が欲しない他者にはみだりに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り、そのことへの期待は保護されるべきものである」ので、「プライバシーに係る情報として法的保護の対象となる」との判断を示していた。前記金沢地裁判決は、「住基ネットシステムにおける市町村長、都道府県知事及び被告地自センターによる本人確認情報の通知、保存、提供は、本人確認情報の新たな、しかも甚だしい拡散であるし、そもそも現代社会に於けるプライバシーの権利の重要性に鑑みると、住基法による上記閲覧及び写し等の交付を定めた規定自体の相当性を再検討すべきものと考えられる」と判示した。

イ 住基ネット上の本人確認情報は、全国的、一元的にコンピュータ管理される点で住基法上の本人確認情報と性格が同じとは言えない。すなわち、前者はコンピュータ化されること自体で本人確認情報の「はなはだしい拡散」に他ならない上、その住民票コードとあいまって、他の膨大な個人情報との照合・結合にさらされる危険を飛躍的に高めるからである。しかも、原則公開とされていた住民基本台帳を事実上原則非公開に転換する法改正が先の国会で行われた。

これらを考えると、住基法上の本人確認情報はプライバシーとして要保護性が低いとは言えず、これも射程に含むプライバシーに対して安易な制約が許されるべきではなく、自己情報のコントロール権の重要な対象として厳格に保護される必要がある。

2 監視社会と住基ネット

(1) 監視社会の状況と進展

ア 住基ネットの意義や役割を理解するためには、日本の監視社会の進展という大きな流れとの関わりで検討を加えることが欠かせないと思われる。ここで「監視社会」とは、「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」とでも差し当たり定義しておく。

イ　住基ネットの成立はこうした監視社会の重要な要素を構成し、言論統制や軍事化に関わる一連の事態もその不可欠の局面を織り成しているのだが、ここでは監視の直接的な装置と基盤にまず簡単に触れておく。

監視社会の典型的、代表的装置として各種の監視カメラがある。

これには、盗難車両や容疑車両の捕捉などのため、警察庁により全国の高速道路や主要国道に約７００箇所設置され、通過する車両をことごとく撮影し、その記録をコンピュータに保存するＮシステムと称される監視カメラや、「防犯」用に街頭、駅、コンビニ、集合住宅などに設置されている各種監視カメラなどが含まれる。後者の「防犯」カメラとしては、警視庁により歌舞伎町に５０台設置された監視カメラや、新宿や池袋など主要駅とその周辺に設置された数百台のカメラ群、コンビニに備え付けられた監視カメラなどがあり、名古屋市では警察の監視カメラが運び込まれ、警察と電話回線で結ばれるコンビニさえ現れている。いずれにしても、私たちは日々膨大なカメラに囲まれ、姿態や行動が写され、記録されていることになる。

ウ　このような監視カメラは急速に増加しつつあるだけでなく、成田空港や関西空港で既に導入されたバイオメトリックスの一種である顔認証装置と連動すれば、特定の個人をたやすく照合・識別し、その行動を追跡・捕捉できることになる。この５月には地下鉄の霞ヶ関駅で監視カメラと連動した顔認証システムの実験も行われた。

日本の監視カメラでもっとも問題なのは、この問題が個人の肖像権やプライバシーという重要な人権に関わる事柄にもかかわらず、明確な法的根拠に基くことなく、また濫用防止などの実効的な歯止め措置も用意することもなしに増殖を続けていることである。

エ　こうした「防犯」カメラの増殖を後押しし、地域ぐるみの監視体制を推し進めるのが、生活安全警察に支えられ、全国の自治体で制定が進められてきた生活安全条例である。たとえば、２００３年に制定された東京都の「安全・安心まちづくり条例」は、犯罪への対処を民間や地域にも責務として課し、警察の指導のもと、民間も巻き込んで、住民に防犯のための活動をさせる仕組みが定められ、公的機関にも、民間の事業者にも、各種建築物や施設の造築に際し、「犯罪の防止に配慮した構造、設備等を有する」ものの普及に努めることが、その責務として規定されている（１４条以下）。これは、戦時下の「隣組」制度さえ想起させる、官民一体となった、地域ぐるみの相互監視体制の構築、監視社会の組織的基盤づくりに他ならない。

オ　こうした日本の監視社会への道は近年ますます強化される傾向が顕著である。そのいくつかを次に列記しておくが、テロ対策や外国人対策および行政情報の統

合化・「最適化」などを名目にしているものが多い。

前者に関係したものとしては、前述した地下鉄駅での顔認証システムの導入実験のほか、昨年１月から開始された事前旅客情報システム（APIS）の導入、入管難民法改正による生体情報の提供義務化やデータベース化、外国人情報の一元管理化などが含まれる。

顔認証システムは、予めコンピュータに記録した要注意人物のデータと撮影した監視カメラの映像を瞬時に照合・特定し、追跡・捕捉等のアクションを可能にする仕組みだが、要注意人物を誰がどういう基準で判定するのかなど、重大な問題が少なくない。

APISとは、外国から日本に到着する航空機につき、法務省、警察庁、財務省が、航空会社から、ネットワークで、旅客・乗員に関する情報の提供を受け、それぞれが保有している個人情報と自動的に照合し、テロリストや犯罪人、不法入国者等「好ましくない者」を特定し、入管審査や税関検査、警察の取り締まりを強化しようとする措置である。官民や官庁間、日本と外国の間がネットワークで結ばれ、日々情報交換が繰り返され、日本人と外国人旅行者についての膨大なデータベースが航空会社や省庁で構築されることになる。

第１６４回国会で成立した改正入管難民法により、特別永住者などを除く１６歳以上の来日外国人に顔写真と指紋のデジタル情報の提供が義務付けられ、国際指名手配情報や過去の強制退去者資料等と照合され、テロ被疑者の強制退去等に活用するだけでなく、それらをデータベース化し、犯罪捜査等にも利用していくことになった。これにより従来の入管、外国人登録などのデータベースに加え、膨大な来日外国人情報のデータベースが新たに構築されることになる。

また、来年の秋には、予め任意に入管で指紋登録を済ました日本人や特別永住者に対して迅速に手続きが進む「自動化ゲート」の制度も始まり、これらの人たちのデータベースも新たにつくられることになる。なお、先のAPIS制度は本改正により義務化されることになった。

さらに、以上のようなさまざまな出入国管理等に関わる情報管理は、将来、インテリジェンスシステムとして一元的に統合化する方向が示されている。

カ　後者の行政情報の統合化としては、「納税者番号制」の導入、「社会保障個人会計制度」の導入、各省庁で進む業務、システム等の「最適化計画」の推進などが含まれる。「納税者番号制」は、政府の税制調査会の小委員会で検討が進められている構想で、住基ネットの住民票コードの利用や突合せが重要な論点となる。「社会保障個人会計制度」は、社会保障番号を付して、社会保障の給付・負担に関する情報を一元管理する構想で、これも住民票コードとの突合せが大きな問題となる。

各省庁が進めている「最適化計画」とは、省庁内でのネットワークの構築（一

省庁一ネットワーク化）や省庁を超えたネットワーク化の計画で、これにより行政情報の統合化を進めようとしている。

キ　以上のように、市民を監視する技術と制度はいろいろな形で「整備」され、その情報を管理するシステムも統合・強化されつつあり、こうした過剰な管理と監視のもと、行政の前で市民が丸裸にされる事態が既に現実のものとなりつつあるのである。

(2)　監視社会における住基ネットの意義と役割

ア　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。

イ　先に見たように、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。

ウ　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。

3　おわりに

住基ネットが行政の効率化や住民の利便性に資する側面があるとしても、監視社会のなかでそれが果たす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考えると、このような制度が合憲的に維持できるかどうか疑わしい。仮に、住基ネットの仕組みを前提とするにしても、自己情報コントロール権としてのプライバシー権の最低限の要請を満たす必要がある。

この権利は人間の尊厳に由来する重要な人権であるから、行政の効率化や住民の利便性などの価値と対等に秤にかけて考量されるべきものではない。この観点から考えると、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が欠かせない。にもかかわらず、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本質的に侵害し、憲法が定める個人の尊重と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。

Ⅳ　住基ネットと横浜市・審議会の答申

２００６年５月、中田宏・横浜市長は、横浜市本人確認情報等保護審議会が「住基ネットの安全性は総合的に見て問題はない」旨の答申を出した（２００６年４月２５日）ことを受けて、今後、従来の「市民選択方式」（いわゆる横浜方式）から「全員参加方式」に転換すると発表した。横浜方式の転換の根拠となった同審議会の答申は、住基ネットをめぐる重要な論点を内包しており、住基ネットの現状を吟味する上で一つの素材となると考えられるので、最後にこれを取り上げ、検討を加えることにしたい。

1　答申の概要

答申は、大きく「1　住基ネット稼働当初の問題点」、「2　現在の状況」、「3　今後見込まれる状況」、「4　結論」から成っている。

このうち、1では、２００２年８月、横浜市が緊急避難的な措置として市民選択制を内容とする横浜方式を採用した理由として、(1) 改正住基法の附則規定にもかかわらず、個人情報保護法が制定されないまま住基ネットが実施されること、(2) それ以

外の問題点として、ア 住基ネットに対する国の責任の明確化、イ 自治体からの調査要求等、ウ アクセスログの開示請求の仕組み、エ 不正使用に対する罰則規定、オ 住基ネット将来像の明示、もあったことが示されている。

２では、住基ネットのセキュリティに関する運用状況と住基ネットの各種サービスの提供状況がまとめられた後、１で指摘された稼働当初の問題点が現状に照らして検証されている。まず、個人情報保護関連５法の成立、施行により個人情報が保護されないという問題は発生していないとし、さらにア～オの問題点も、いずれもクリアーされている旨が示されている。

すなわち、アについては、２００３年５月の総務省作成資料により国の責任が明確に述べられ、また国はセキュリティ確保の各種取り組みを行っている。イについては、２００３年９月の総務省告示「電気通信回線を通じた送信又は磁気ディスクの送付の方法並びに磁気ディスクへの記録及びその保存の方法に関する技術的基準」によって国又は関係自治体等に報告・調査等を求めることが可能になった。ウについては、同「技術的基準」により、都道府県知事が市民の本人確認情報等の提供状況について、市民からの開示請求に対応するための情報を生成し、保存することになったし、市町村についても２００４年４月から市町村長の判断によりその機能を装備することが可能となり、横浜市でも同年４月から開始した。エについては、行政機関個人情報保護法、独立行政法人等個人情報保護法で盗用等の不正使用につき罰則が定められ、自治体の条例等も強化され、横浜市も国に先駆け個人情報保護条例で不正使用に関する罰則規定を盛り込んだ。オについては、利用事務の変更等の法律案の検討に際しては第三者機関である住民基本台帳ネットワークシステム調査委員会の審議を経て行うことになっているし、地方自治体への意見照会も行われている。

続いて、各地で提起されている住基ネット訴訟も取り上げられ、いずれも住基ネットのセキュリティについては具体的危険のあるシステムではない旨の判決が示されたと総括されている。

３では、住基ネットの利用事務の拡大が進む状況の中、年金等の現況確認事務では、膨大な件数処理の必要から、住基ネット情報を一括して取り込み現存確認行うため、非通知者は死亡した人などと同様現存していないと判断され、年金の支給が停止される可能性があり、これを避けるため横浜市の本人確認情報は通知者を含め全て利用できないという不都合が生じていることが指摘されるとともに、原則非公開への住基法の改正や横浜市を含む地方自治体での閲覧制限など個人情報保護の取り組みが強化されている動向が記されている。

以上を受けて４では、住基ネットの安全性についてこれまでの考察が制度面、技術面、運用面に即して要約されるとともに、特に名寄せによる情報の一元管理の危惧についても、住基法に定める利用・提供制限等の諸規定があり、住民票コードも変更可能な制度となっていて自己情報コントロール権が保障されているなど、一定の措置が

取られていると述べている。これを踏まえ、先のいずれの面でも「横浜市が当初懸念していた事項は、国及び横浜市等の対応により解消されている」だけでなく、「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」と結論付けている。

2　答申の問題点

やや詳しく答申の内容を紹介してきたが、このような答申の結論とそれを導く議論には疑問を感じる点が少なくない。既に本報告書のⅠ～Ⅲの中で実質的に指摘してきたことと重なる点もあるが、ここでその主要な問題点を列記しておくことにする。

(1)　個人情報保護法制度の不備は解消されたか

第一に、答申の２や４で展開している、横浜市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。

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。

(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

以上との関連で、前述したように、答申は、住基法上の規制規定や住民票コードの変更可能性などを根拠に、名寄せ等による情報の一元管理やプライバシー侵害の懸念を退けているが、これについても重大な疑問がある。これについては、Ⅰおよび特にⅢで既に詳しく指摘したところだが、ここでは必要な範囲で改めて触れておくことにする。

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。

(3)　個人情報保護法制度以外の問題点は解消されたか

次に、個人情報保護の法制度以外に当初横浜市が指摘していた論点（ア～オ）については、横浜市の審議会が言うように問題点は解消されたと考えられるか。結論を先に記すと、この点でも同意するのは困難だと言わざるを得ない。

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。

(4)　その他の問題点

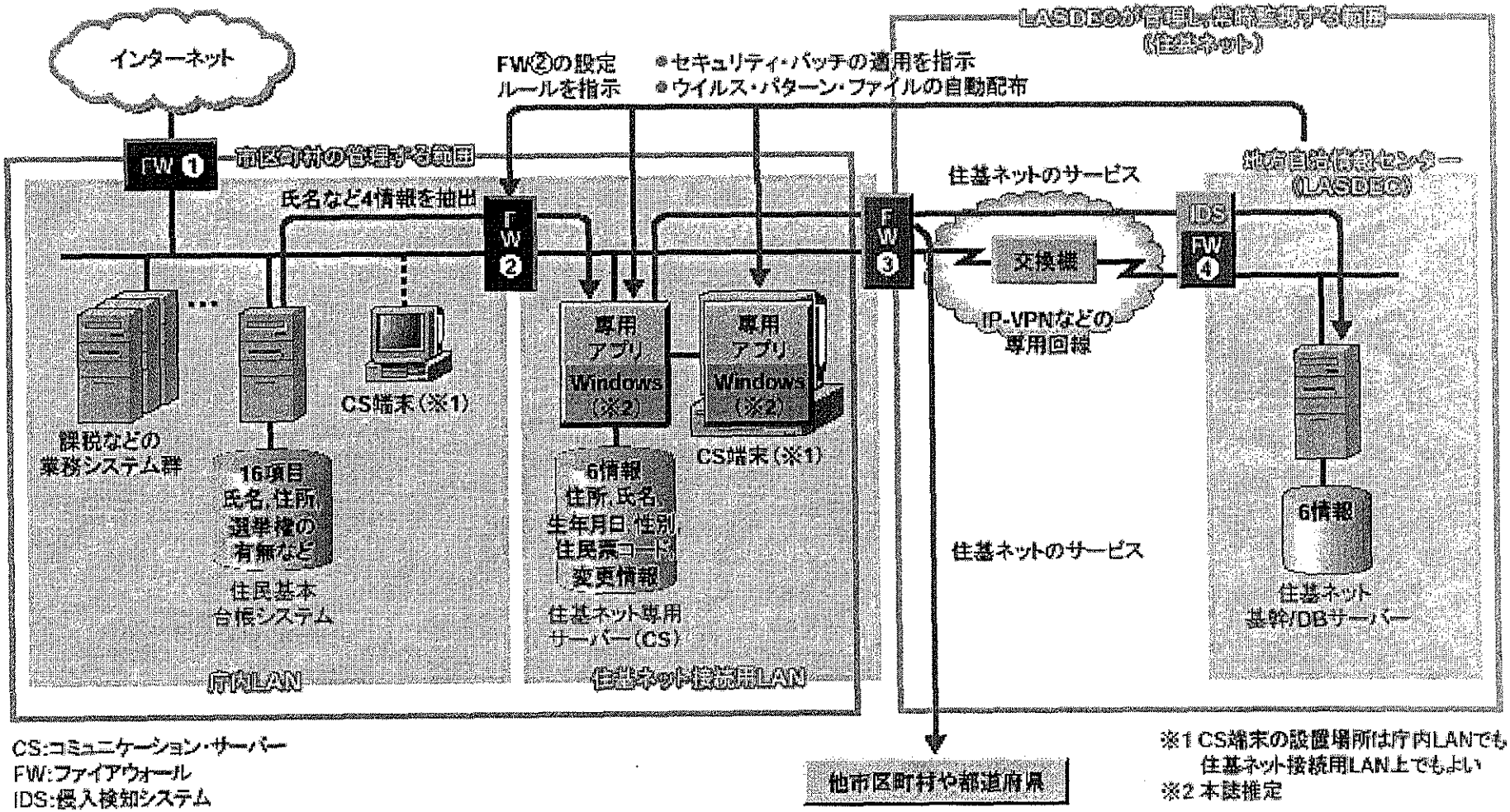
以上のほか、二点について付しておく。一つは、選択制を維持すると一部の事務では通知者の本人確認情報も利用できないと述べている箇所についてであるが、こうした議論は、横浜地裁での住基ネット訴訟において原告側証人として証言した花園勝・横浜市市民局区政支援部窓口サービス課システム担当課長（当時）が、国側の主張に対して、横浜市は、通知者の情報は利用できるはずであり、利用してほしい旨要請をしているとかつて発言したことと相反し、年金現況報告の住基ネット利用について、横浜方式を続ければ市民全員が対象外になるとの総務省による横浜市への説明に対し、社会保険庁が「そんなことは言っていない」と報じられている（朝

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。

3　答申の結論は妥当か

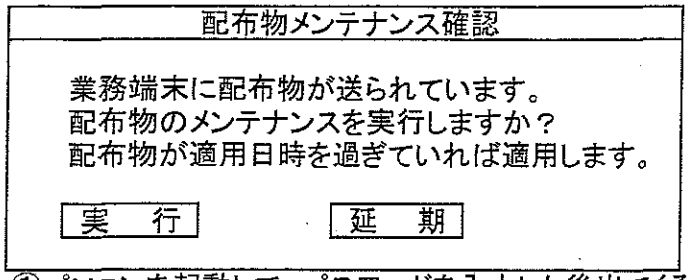
以上のように見てくると、また本報告書のⅠ～Ⅲで示してきたものを踏まえて考えるといっそう、今回の答申のように、選択制を導入した際横浜市が抱いた住基ネットの安全性への疑問がその後解消され、「現時点において総合的に見て問題はない」との結論を導く論拠が希薄であり、結論の妥当性を支えることは困難だと断ぜざるを得ない。



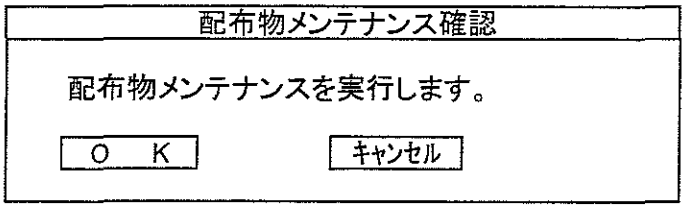
CS:コミュニケーション・サーバー
FW:ファイアウォール
IDS:侵入検知システム

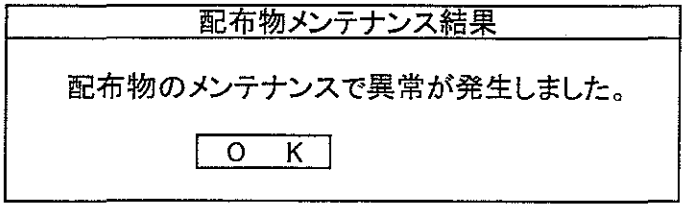
※1 CS端末の設置場所は庁内LANでも
住基ネット接続用LAN上でもよい
※2 本誌推定

別紙1



①パソコンを起動して、パスワードを入力した後出てくる画面





■■不在時操作マニュアル

朝9:00過ぎたら

手 順

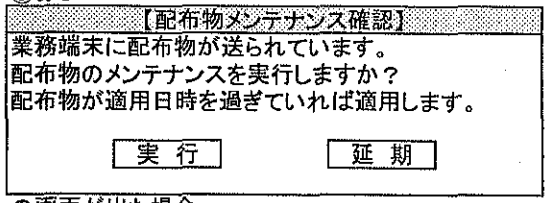
①電源on
②パスワード入力画面が出る。　→　shiretokoと入力する。

以下のとおり、3つのパターンになる。

↓↓↓
③の1
青い画面になる。
何も変化がない。
終了してよい。

↓↓↓
③の2
青い画面になる。
左下のタスクバーに【資源配布クライアント】という文字が点滅している。
（通常約10分～30分で消える。）
点滅が終わって気づいた時点で、終了してよい。

↓↓↓
③の3



の画面が出た場合。
戸籍住民係　■■係長に電話して
「CS電源立ち上げましたら、配布物メンテナンス画面の実行と延期がでましたが、どちらを選べばいいですか？」と聞いてください。
言われたほうをクリックしてください。
そしてOK、OKで進んでください。
その後、③の1か③の2になります。

↓↓↓
終了（③の1～3まで共通）
スタート　→　シャットダウン　→　OK、キャンセル、ヘルプがあるのでOK　→　少し待ったら画面消える　→　終わり

7月15日システム設定、テスト

1 作業内容

① システム構築手引書　導入手引書　(カード発行環境編)　[第1．0版]　[平成15年2月]
スキャナ設定、確認
9．1　統一文字フォント再インストール時のレジストリ再設定について

② 住民基本台帳ネットワークシステム　二次テスト手引書　二次テスト仕様書例　第1．0版　平成15年2月

8 カード交付申請内容登録／カードレイアウト編集
12 カード交付
13 カードパスワード
14 カードパスワード初期化
15 カード一時停止
16 カード一時停止解除
17 手入力によりカード廃止する場合のカード廃止・回収(他とほぼ同様の手順のためこのテストはしていない。)
18 連動してカード廃止される場合のカード廃止・回収(他とほぼ同様の手順のためこのテストはしていない。)
23 広域交付(交付地市町村)　7月17日
24 広域交付(住所地市町村)　7月17日
26 転入(付記転入)　　相手市町村、既存住基システムとのやりとりがある。今回は、していない。
31 連携市町村におけるカード回収　　相手市町村とのやりとりがある。今回は、していない。
33 本人確認

手順　8→33→12→33→13→33→14→33→15→33→16→33

7月17日広域交付住民票交付cs操作

広域交付住民票申請書を受理した後

準　備

1 CS電源ON
2 カードリーダライタ電源ON
3 プリンタ電源ON　オンライン点灯確認
4 用紙確認(印鑑証明書用紙)
5 業務管理者用カード

手　順　手引書の23. 広域交付(交付地市町村)のとおりだが下記に詳細を示す

初期状態(青い画面)から

NO.	手引書	画面状態	操作
1		青い画面	CSシステム起動をダブルクリックする
2		業務メニュー	カードをクリックする
3		カードを挿入してください	業務管理者用カードを職員用のリーダライタに挿入する
4		パスワード入力	shiretokoを入力する
5	23－5	業務メニュー画面	「広域交付依頼入力」をクリックする
6	23－6	本人確認情報照合	①住基カードによる本人確認 ②住基コードの手入力による本人確認 ③4情報の手入力による本人確認　の方法がある。
①の場合は、カードをクリックする　②③の場合は、入力して検索をクリックすると、23－10に行く			
7	23－7	住基カードを挿入してください	請求者の住基カードを挿入する
8	23－8	テンキーパッド～してください	4桁数字パスワードを入力し、確定(請求者本人)　注:3回誤りで使用不可能
9	23－9	パスワード確認しました	OKをクリックする
10	23－10	本人確認情報照合	対象者確認し、確定をクリックする
11	23－11	広域交付依頼入力	依頼先市町村名等を指定して確定をクリックする
12	23－12	広域交付を依頼しますか？	はいをクリックする
13	23－13	広域交付依頼を完了しました	OKをクリックする
14	23－14	業務メニュー	
このまま約5分待つ			住所地役場承認作業中
15	23－15	画面最下部に「●広域交付受信あり」が点灯	「広域交付依頼依頼」をクリックする
16	23－16	広域交付依頼結果一覧	対象者をクリックしてから、住民票をクリックする
17	23－17	住民票情報表示(交付地)	NO.11で依頼した内容を確認する
18	23－18	住民票情報表示(交付地)	印刷をクリックする
19	23－19	広域交付住民票を印刷しますか？	はいをクリックする
20	23－20	住民票情報表示(交付地)	印刷された広域交付住民票を確認する
21	23－21	住民票情報表示(交付地)	戻るをクリックする
22	23－22	広域交付依頼結果一覧	戻るをクリックする
23	23－23	業務メニュー	この後、使用しなければ業務終了をクリックする。カードが出てくるので抜き取る。

「広域交付作業」　住民票の写しの広域交付について清里町とやりとりしながら行った。

(1)交付地市町村の場合　※清里町交付斜里町承認

①清里町で広域交付の受付(申請事由を聴取:cs入力時必要)
②清里町で本人確認処理
　(カード有:カード読込)
　(カード無:免許証等で本人確認。)
　(免許証等無く、住所も忘れた:4情報から本人確認情報の検索。入力は、全部いれなくてもよい)
③清里町から斜里町に「広域交付住民票の依頼」
④斜里町は必要な情報を受信し、CS画面の下部タスクバーに「広域交付承認」欄がオレンジ色になり、ポーンと音が鳴る
⑤斜里町は、CS画面に気づき「広域交付承認」する。(広域交付住民票印刷可能)
⑥清里町は、斜里町からの承認を受信し(タスクバーオレンジ色)、「広域交付依頼結果」から広域交付住民票を印刷し交付する。

(2)住所地市町村の場合　※斜里町交付清里町承認
①清里町は必要な情報を受信し、CS画面の下部タスクバーに「広域交付承認」欄がオレンジ色になり、ポーンと音が鳴る
②清里町は、CS画面に気づき「広域交付承認」する。(広域交付住民票印刷可能)
※要は、(1)の④⑤の部分の作業

メモ
1 広域交付住民票は、住基カードが無くても取れる。
2 オフコンは使用しない。
3 CS業務メニューの
広域交付依頼入力
広域交付依頼結果
広域交付承認

のみ使用する。
4 広域交付住民票用紙は、印鑑証明書の用紙を使う予定

「付記転出転入作業」　清里町とやりとりしながら行った。詳細別紙付記転入転出のとおり。