甲第30 号証

住民基本台帳法の一部を改正する法律案

についての意見書

１９９８年3月１９日

日　本　弁　護　士　連　合　会

住民基本台帳法の一部を改正する法律案についての意見書

１．意見の趣旨

住民基本台帳ネットワークシステム構築を目的とした住民基本台帳法の一部改正案は、住民基本台帳を基礎に、全国民にもれなく十桁の統一番号を付し、この統一番号（住民票コード）を氏名、住所、性別、生年月日の４情報とともに、当該市町村だけでなく都道府県単位、さらに全国単位のセンターのコンピューターに同時登録されるよう各市町村のコンピューターを専用回線で結んだ全国ネットワークのコンピューターシステムで管理し、この統一番号（住民票コード）を各省庁共通の個人識別番号として使用し、様々な行政分野において利用し、効率のよい行政サービスを受けられるようにしようとするものであると自治省は説明している。

しかしながらこの改正は、住民基本台帳法の趣旨を潜脱し国民総背番号制につながるものであり、現行法体制のもとでは国民のプライバシーを侵害するものである。これは国家による国民の個人情報の集中管理であり、管理社会、監視国家を招来する危険性が強いので、今回の住民基本台帳法の改正に強く反対する。

２，理由

序

政府は第１４２回通常国会に住民基本台帳法の一部を改正する法案を提案し、住民基本台帳ネットワークシステムを構築する準備をしている。この法案は、１９９６年３月発表の『「住民記録システムのネットワークの構築等に関する研究会」報告書』（以下、報告書という）、同年１２月発表の『「住民基本台帳ネットワークシステム懇談会」意見』、１９９７年６月発表の自治省の「住民基本台帳ネットワークシステムの構築について（住民基本台帳法の一部改正試案）」（以下、「試案」という。）をベースとするものである。

当連合会は「納税者番号制の導入に関する意見書」（１９９２年１０月）等において、納税者番号制、国民総背番号制について反対する旨の意見表明をしてきたところであるが、住民基本台帳法の一部改正法案についても以下に述べるとおり、基本的に同一の見地から反対の意見表明を行うものである。

目　　次

第１　住民基本台帳法からの逸脱と個人情報保護の不備（概要）

（１）住民基本台帳法第１条は、「この法律は、市町村（特別区を含む。以下同じ。）において、住民の居住関係の公証、選挙人名簿の登録その他住民に関する事務の処理の基礎とするとともに住民の住所に関する届出等の簡素化を図り、あわせて住民に関する記録を正確かつ統一的に行う住民基本台帳を定め、もって住民の利便を増進するとともに、国及び地方公共団体の行政の合理化に資することを目的とする。」と定めている。

今回の住民基本台帳法一部改正案が実現しようとしている住民基本台帳ネットワークシステムは、同条が「市町村において」、住民の居住関係を公証し、住民に関する記録を正確かつ統一的に行う住民基本台帳の制度を根幹から変更するものであり、国の行政機関等が「住民の居住関係の公証、選挙人名簿の登録その他住民に関する事務の処理の基礎」とするための住民基本台帳を他の目的に使用することを認めている。このような住民基本台帳ネットワークシステムは、住民基本台帳法の目的と明らかに抵触するものであり、少なくとも同法の改正のみによっては実現不可能である。

（２）試案は、２１世紀の高度情報化社会における公的部門の基礎的インフラとして、住民の居住地域を越えた全国単位での「本人確認を行う」ことと「他の行政機関等へ本人確認情報を提供する」ことが「住民サービスの向上」に不可欠であるとし、住民基本台帳制度を基礎としてシステムを構築することが、「情報の正確性や導入コストの面」から最適であるとする。

しかし、現行住民基本台帳制度は全国単位で本人確認を行うことなど全く予定していない。住民基本台帳を作成するための住民票（同法第６条１項）及び磁気ディスク（同条３項）を含めて、住民基本台帳法では個人情報に対する法的な保護措置が欠けており、「何人も、住民基本台帳の閲覧、…（中略）…により知り得た事項を使用するに当たって、個人の基本的人権を尊重するよう努めなければならない。」（同法第３条４項）と規定されているにすぎない。このように個人情報の保護に関して全く無防備な現行住民基本台帳制度に、全く異質な住民基本台帳ネットワークシステムを、単に「情報の正確性や導入コストの面」から最適として導入しようとしている点に、様々な問題の根本的な原因がある。法案が個人情報保護の法的システム面でも不十分なことは後述のとおりである。

（３）法案では、本人確認情報（氏名、住所、性別、生年月日、住民票コード）は国の一元管理でなく、「市町村」が住民台帳を「管理」し、「ネットワークの部分」を「都道府県」及び「全国センター機能を果たす指定情報処理機関」が担当するとしている。報告書では、コンピューターを「各市町村に新たに設置し」、都道府県及び指定情報機関のコンピューターとを「専用回線」で結び、「外部からのアクセス」は不可能とする。しかし技術的にセキュリティが不備であることは後に詳述するとおりである。

ネットワーク化された個人情報の漏洩又は盗用があった場合、それが住民基本台帳を管理する市町村側で行われたのか、それともネットワークの部分を担当する都道府県ないし指定情報処理機関側で行われたのかも判然としない。

（４）指定情報処理機関の法的な性格も後述のとおり不明確である。報告書は４個の機能を掲げ、システム内の連絡調整、他の行政機関への情報提供の窓口、技術的なチェック、システムのバックアップを挙げている。これらの機能はネットワークシステムの保守管理を行う民間企業の業務とほとんど変わらない。

しかし、指定情報処理機関の任務はそれだけでない。住民からの「苦情」の処理を行い（３０条の４１）、住民からの開示請求（３０条の３７）、訂正請求（３０条の４０）にも対応するものとし、ＯＥＣＤ８原則の個人参加の原則を実現するものと位置づけている。住民からの個人情報に関する申入れを受理し処理する重要な権限を、ネットワークシステムの保守管理を主たる業務とする指定情報処理機関に付与しても、その組織に対して個人情報の保護など期待することはできない。

（５）都道府県・指定情報処理機関の保有情報は最低限必要な情報に限定し、氏名、生年月日、男女の別、住所及び住民票コード（と変更確認情報）に限るとしている。

住民基本台帳を作成する住民票に掲げる項目は、氏名、生年月日、男女の別、住所など全部で１４項目ある。住民基本台帳の電算化率は団体割合が９３．８パーセント、人口割合が９９．２パーセント（１９９７年４月１日現在）とされている。この１４項目のうちの４項目と住民票コードを本人確認情報の対象にするとしているが、磁気ディスクに収納された全情報とネットワークシステムに接続される本人確認情報の間でも個人情報の保護は等しく図られなければならない。もし、これを看過すればネットワークを通じて本人確認情報以外のすべて個人情報が侵害の危険にさらされる。ネットワーク分を切り離し人の手で処理するなら、両者の間に齟齬が生じる可能性がある。

（６）試案は個人情報保護措置を徹底し、「ＯＥＣＤ８原則等」を踏まえた保護措置規定を整備し、「技術上も万全」の保護措置を講ずるとしている。しかし、その保護措置は「法律で禁止する」とか「違反者に罰則を課する」というだけで到底実効性があるとは言えない。

試案の保護措置は内容において実効性に欠けるだけでなく、後述のとおり本人確認情報の提供先における保護措置が欠落している。国の行政機関等が本人確認情報の提供を受けた場合、当該行政機関も亦、その情報をＯＥＣＤ８原則に準拠して取り扱わなければならないこと多言を要しない。ところが現行の個人情報保護法制は後に詳述するとおり極めて不完全なものにすぎない。

本人確認情報の利用目的は、所定の事務を遂行する際の本人確認のためと限定されているのであるから、本人確認が済み次第、直ちにその情報を廃棄すべきである。廃棄しないで他の目的のために保存し、保管することなど許されるはずもない。ところが法案

には提供を受けた本人確認情報消去の規定はない。従って、国の行政機関等の事務を規定したそれぞれの法令において、上記の取り扱いを明記すべきであり、そのためには関連する法令のすべてを改正すべきである。

（7）住民の申請により市町村が「全国共通様式」の住民基本台帳カードを交付するとしている。このカードには住民票コードが書込まれており、それを読み出したり書き換える技術がある以上、住民票コードの盗用などを防ぐことは不可能である。まして、そのコードは所持者に固有の番号であり、不正に所持するものが本人になりすました場合、本人の救済手段を講じなければならない。法案にはこのような配慮が全く欠けている。またカードには余白利用が認められ、民間での利用に途を開いているといえる。

カードの問題は後に詳述する。

（8）本システムはすべての国民に住民票コードを付けて、これを広く行政機関・法人に提供するものであり、納税者番号制や国民総背番号制につながるものである。報告書はすでにその方向を示している。

第２　プライバシー権という側面からみた住民基本台帳ネットワークシステムの問題点

（１）国民総背番号制の議論

住民基本台帳ネットワークシステム（以下「本システム」という。）は、１９６８年に「政府におけるコンピューター利用の高度化」の閣議決定をうけ、１９７０年に行政管理庁を中心とする７省会議において提唱された「事務処理統一個人コード」の制度化が行われようとした際の、いわゆる「国民総背番号制」についての議論を想起させる。

われわれ人間には、本来ひとりで放っておいてもらう権利があり、他人ことに権力機関からみだりに干渉されることなく自由に振る舞う権利がある。これが犯されれば、人間の本来もっているはずの尊厳とか自律性が奪われたことになる。各行政機関が特定の目的のために個人から提供を受けた個人情報をコンピュータによって集中管理し、あらゆる目的のために即時に利用するというのが国民総背番号であり、そのような目的のために個人に番号をつけるのは、国民のプライバシーを侵害するおそれがある。個人が番号化されることによりその人格的利益を害し、国家による国民に対する管理体制がより強化されるのではないかなどと議論された。

今回、本システムの導入を提唱した報告書では、上記の議論の中で問題とされたところを意識的に改善しようとしていることが見受けられるものの、やはり問題点の中心は国民のプライバシーに関してであり、１９７０年ころの議論と本質的に変わるところはない。

（２）プライバシー権

そこで、本システムが、国民が有するプライバシー権あるいはプライバシーの利益を侵害するものであるか否かを考察する。

プライバシーの権利については、古典的には、「ひとりでほっておいてもらう権利」であるとか、「私生活をみだりに公開されない法的保障ないし権利」であるとされた。近時のプライバシー権の本質に関する学問的成果によれば、プライバシー権は、「自己に関する情報をコントロールする権利」であると定義されるようになっている。憲法１３条を根拠とする個人の尊厳を守るための権利概念であることに変わりはない。個人情報に関していえば、これに対してどのような脅威があればプライバシー侵害になるのかについては、１９８０年９月、ＯＥＣＤ（経済協力開発機構）が示した８原則のガイドラインを参酌しなければならない。

（３）どのような状況であればプライバシー侵害となるのか

実際に、ある特定の個人のプライバシー、つまり自己情報コントロール権が侵害され、それが財産的にせよ精神的にせよ実害を生じさせたときには、まさにプライバシーの侵害という不法行為の問題に発展する。例えば、個人情報が漏れ、これが悪用されて詐欺や恐喝の被害、あるいはダイレクトメールや勧誘電話の攻勢にあうといった被害が生じ

た場合などである。

さらに、あるシステムの導入が、そのような具体的な被害を生じかねない蓋然性があるならば、言い換えると、そのような脆弱性のあるシステムを創ることは、たとえ具体的な実害を生じていなくとも、国民の間に、大きな不安感や危惧感を抱かせることになる。その不安感、危惧感が一定程度を超えた場合には、国民一般との関係において、プライバシーの権利ないし利益の侵害状態が生じているというべきである。

プライバシー権は、人格権であり個人の精神的自由を支えるものであるゆえに、そのような危険な状態自体がプライバシーの権利ないし利益を損ねている状況と把握すべきでだからである。もちろん、およそ実害が発生する可能性が皆無ではないというだけでは、あくまで抽象的な危険があるだけであって、にわかに違法状態であるとはいえないかもしれない。しかし、少なくとも、システム自体に欠陥があると評価される場合で、そのようなシステムを設定することについて、特に優越すべき具体的な国民の利益、便益が認められない場合には、そのシステムの設定は、全国民に対する関係において、違法であるといわなければならない。プライバシーの権利が憲法１３条から導き出される権利ないし利益であり、本システムが、国、地方自治体によって構築されるものである以上、直接の憲法違反の疑いがあるということになる。

もっとも、ここでは、厳密な意味での違憲性や違法性が問題なのではない。国民にとって、その利益を害する危険性の高いシステムが構築されるのであれば、それを排除しなければならいというのは至極当然の議論なのである。

ともあれ、本システムが国民のプライバシーに対してもたらす脅威の程度を検証する必要がある。

（４）データの安全性について

ＯＥＣＤの８原則の一つとして「安全保護の原則」が謳われている。報告書によれば、ネットワークシステムへの違法なアクセスを防止するため、適切な技術上の保護措置をとるとしている。その例としては、専用回線の利用、通信データの暗号化、パスワード等による端末操作者の認証チェック、ネットワークシステムへのアクセス監視があげられている。

しかし、端末はそれこそ全国の津々浦々まで配置されるのであり（そうでないと、報告書がいうところの住民サービスや行政の効率化がはかれるはずがない）、端末のすべてにわたってセキュリティが保たれる保障があるのだろうか。公衆が利用するネットワークに繋がっていないから漏れないといえる保障はない。専用回線にいわゆる盗聴器をしかけてデータを盗むという技術はそれほど高度なものではなく、対象に価値があると認められれば、悪意者の介入によりいつでも為され得ることと考えるべきである。

また、法案は、データの漏洩を防ぐ万全の処置をとるといいながら、他方では電子計算機処理業務等を外部に委託することができるとする（３０条の１７、３０条の３３）。

この外部委託の際には安全保護の原則を守るために、守秘義務を課している。

しかし、せっかく専用回線を利用することにより、インターネットやパソコン通信において頻繁に行われているところのネットワークへの不正アクセスを封じることができても、外部に委託することにより、データ処理の根本の部分から個人情報が関係者によって持ち出されるという危険が大きくなる。同様の事件は、過去に頻繁に起こっているのであり、再び起こらないという保障はどこにもない。このような脆弱性を否定できないうえに、万一、その情報が漏洩されたときの混乱は尋常ではないものと推測される。単にデータがその時漏れたというだけのことではなく、そのデータを入手した者は、当該データの対象者の一生涯、これを悪用をする機会を有しているといえるのである。

個人情報保護の技術的措置の不完全性、非安全性については第６の部分で詳述することとする。

（５）データ結合の禁止が守られるのか

報告書においては、「データーの提供を受けた行政機関は、当該データーベースを基礎として構築するデーターベースと他のデーターベースを電子計算機処理により結合してはならない」としている。住民基本台帳をもとに国民全員に番号を付け、それをもとに行政が国民の管理を行えば、それぞれの行政分野において、効率的にデータベースが構築されるであろう。さらにデータベース間において結合が行われれば、さらに効率的に行政が運営できるということになるはずであるが、他方、本来であればあちこちに分散していたはずの個人情報がつなぎあわされ、各人のプライバシーは丸裸となる危険きわまりないことである。ＯＥＣＤの８原則では、データ結合の禁止は謳われていないと主張する向きもあるが、データの目的外利用を禁じていることはいうまでもない（「利用制限の原則」）。本来結合してはならない異なるデータどうしを結合することは、目的外利用にほかならない。このデータ結合の禁止は、国民のプライバシーを保護するために必要不可欠なものである。しかし、はたしてこれが厳格に守られるといえるであろうか。法案は、本人確認情報の提供を受けた者に対し、単に目的外利用をしてはならない旨規定するのみで（３０条の３４）、データベースの構築を禁止せず、使用済みの本人確認情報の消去も規定せず、提供目的違反に対して刑罰の定めもないし、国民の側からの中止請求権も認めていない。

そもそも、本システムの構想が打ち出されたのは、共通の番号を使うことにより、様々な行政分野から一元的に管理された効率のよい行政サービスを受けることにある。法令上明確な根拠がある場合には、４情報及びコードを他の行政機関に提供できるようにするとの構想であり、報告書は、将来、納税者番号制度への活用も可能であると示唆しているところでもある。納税者番号制度ということになればデータ結合は不可避である。

むしろ、報告書は、地方自治体が制定している個人情報保護条例の「オンライン禁止条項」（データの結合を禁止する条項）を廃止ないし規制の緩和をするように求めてい

るくらいである。その理由付においては、「オンライン結合に対する社会的な考え方も徐々に変わってきているところである」としている。これに対しては、問題意識の高まりによって、むしろ、データ結合が問題視される方向にあると見るのが正しいと思われるところであるが、報告書は、将来、効率的な行政の運営のために様々な行政分野で４情報及びコードを利用するのがよいと考えつつ、現時点における国民のプライバシーに対する意識がこれを許さないであろうと予測し、当面の批判をかわすべく、上記の異なるデータベースどおしの結合の禁止を謳ったという疑いが拭いきれない。

政府の税制調査会も、住民票コードを利用し、納税者番号制度への活用を示唆しているところである。

もし、将来の結合など全く考えていないというのならば、それほど効率的でないシステムの構築にこれほどまでの費用（初期投資→約４００億円、年間経費→約２００億円）をかける意味はどこにあるというのであろうか。

（６）自己情報のコントロールが可能か

本人確認情報は情報主体たる国民の知らないところで知らない間に通信回線を通じて市町村から他の市町村、都道府県、国、法人へと提供され、いつ、どこへ提供されたのか開示されることはない。しかもその提供先の用途は法案の別表に掲載された特定の事務に限らず、「条例で定める事務」、国の行政機関の「所掌事務」というように無限定なものとなっている（３０条の６、３０条の７、３０条の８、３７条）。従前、個別具体的な必要性を認識しつつ住民票の写しをとって自主的に交付していたのとは全く様相を異にする。このような本人確認情報の利用の仕方は自己情報コントロール権を侵害するものといえる。

（７）まとめ

以上にみたように、本システムを構築することは、ごく近い将来において、きわめて高い蓋然性で国民のプライバシーに対する実害を生じさせる危険を有するものである。他方、報告書が、このシステムの導入により行政活動が効率的になり、国民による利便性が高まるとＰＲしている程度のことは、全国統一的な付番をすることなく実現できることではないかと思われる。

結局、本システムは具体的な問題状況が生じる具体的危険性が相当程度高いというべきであり、そうである以上、その状態がプライバシー権の侵害であるといっても過言ではない。国民のプライバシーを保護するための万全の体制を整えずして、拙速にこのようなシステムを導入すべきではないものと考える。

第３　住民基本台帳ネットワークシステムにおける結合の問題（憲法上の位置付け）

１．オンライン結合などによるデータマッチングとプライバシー侵害

（１）本システムは、市町村、都道府県、国などの間で、本人確認情報を流通させるもので、それぞれの行政機関をオンライン結合させるものである。オンライン結合とは、「当該行政機関が管理する電算機と実施機関以外の者が管理する電算機その他の機器とを通信回線を用いて結合し、当該実施機関が保有する個人情報を実施機関以外の者が随時入手し得る状態にする方法」（神奈川県個人情報保護条例第１０条１項）と定義されている。利用者はこの結合が行なわれるときは、実施機関が保有する個人情報をいつでも必要に応じて入手できる状態にあるから非常に効率的かつ便利である。

行政機関が収集し、利用している個人情報は犯罪情報、税務情報、医療情報、教育情報、年金・福祉情報、家族情報、国勢調査など多種多様であり、これらの個人情報をオンラインで結合させることなどによるデータマッチングは国民の個人情報を瞬時に把握することにつながるものである。行政機関が個人情報を収集し、利用することは各行政機関が法令の目的の範囲内で行なうものであり、他への行政機関の利用を前提とするものでなく、その意味で限定されている。この目的及び範囲をこえて、国民の個人情報を瞬時に把握する行政上の目的、必要性は存在しない。

国民のあらゆる個人情報をすべて掌握できるようなシステムは行政上の目的をこえるものであり、各行政機関が個別に保有する個人情報を随時かつ瞬時に把握されることになれば、そのことだけで国民のプライバシーが丸裸にされることになる。これは個人の尊厳を著しく侵害するものである。憲法１３条（個人の尊厳、幸福追求権）に違反するおそれがあり、又、監視国家に導くものである。日本国憲法はこのようなシステムを許容していないと解される。

地方自治体の個人情報保護条例がオンラインの「結合禁止」を規定しているのは同様の趣旨である。ドイツ（１９８５年当時西ドイツ）の憲法裁判所が「個人を全人格的に管理することにつながる住民基本台帳番号制度は、憲法が保障する人格権を侵害し、国民総背番号制度を憲法違反」としたのも、同じような理由である。又、オーストラリアで国民総背番号制についてプライバシー保護庁の設置を前提としても国民がＮＯの意思表示を行ない、納税者番号制のみ導入したことも監視国家への危険性を考えてのことである。

（２）本システムは、住民票コードを各省庁共通の個人認識番号として使用することにより、将来すべての行政機関をオンラインで結ぶことなどによるデータマッチングの危険性を内包している。

法案は行政機関等は受領した本人確認情報（住民票コードを含む）を法律で認められ

た当該事務以外の目的に利用してはならないと規定している（３０条の３４）が、法律で規定すればデータマッチングも可能となっており、違反については罰則もなく、国民に中止請求権を与えるシステムともなっていない。政府はもともと行政情報推進基本計画を持っており、ネットワークを駆使した電子政府の実現を目指しているところである。

各行政機関は、それぞれの行政目的に応じて番号を付し、これをコンピューターで管理するようになってきている。すなわち、各市町村は独自に番号を付しており、国家機関も年金番号や納税管理番号などを付したりしている。ところが、現在すでに付されている番号は、各行政機関が独自に付しているものであり、これらの番号を統合する統一番号は未だ設けられていない。しかし、今回の住民基本台帳法の改正により、出生と同時に単一の番号が付され、これが基本的にはその者が全国どこに住所を移転しても、あるいは姓を変更しても変わらない番号となると、各行政機関はこの番号に統一化もしくは併用することは十分考えられる。そして、また、この番号により他の行政機関の保有する情報にアクセスし、更に情報を結合することも生じうるのである。この意味で、住民票コードは全ての行政機関の保有する情報にアクセスするためのマスターキーであり、かつ、これらの情報を結合するマスターキーの役割をはたすこととなる。

結合が許容される範囲は公益上の理由がある場合に、その毎行われるものに限定するべきであり、例えば個人情報を最も必要とする捜査目的であっても、その必要性があるときに限ってその毎、法令に基づいて利用できるようにすべきである。常時かつ瞬時に個人情報を把握できるシステムは捜査機関といえども許されるものではない。行政の効率性が個人の尊厳に優先するべき合理的理由はない。ましてやプライバシー保護対策が不十分な我国においては現時点での国民総背番号制は到底導入できるような状況にはない。民間における利用も当面は禁止されているが納税者番号制を導入すれば、当然民間が利用することになり、民間の利用を禁止することはできなくなる。民間の、例えば消費者信用情報機関が収集している情報に政府機関がアクセスすることになれば、国民の借金情報や破産・延滞などの事故情報も国家が掌握することになる。民間の医療機関が保有する医療情報や私立学校が保有する教育情報などへのアクセスも許されることになれば、国家による国民の全人格的把握を招来することにつながっていく。

２．オンライン結合、マッチング規制

すべての行政機関がこのシステムをいつでも利用できるようにすることは法律で規定したとしても憲法違反になることはすでに述べた通りである。プライバシー侵害を最小限にして行政の目的、効率化を実現させるためには公正な独立機関を設置し、オンラインを結合させるときは個別・具体的に事前にその承認を求めることが少なくとも必要である（個人情報保護条例も審議会の意見を聞くなどの方法をとっている）。本システムを、このような保護対策を施すことなく実施することはとうてい許されないものと理解すべきである。

行政機関の保有する電子計算機処理に係わる個人情報保護に関する法律は目的外利用は原則禁止としながらも（同法９条１項）、「前項の規定にかかわらず、保有機関の長は、次の各号のいずれかに該当すると認めるときは、ファイル保有目的以外の目的のために処理情報を利用し、又は提供することができる。ただし、処理情報をファイル保有目的以外の目的のために利用し、又は提供することによって、処理情報の本人又は第三者の権利利益を不当に侵害するおそれがあると認められるときはこの限りでない。」（同法９条２項）として、行政機関の判断で広範な目的外利用を可能としているのであって、結合を可能としている。これは、先進的な自治体の個人情報保護条例が目的外利用の禁止の規定以外にオンライン結合禁止を明確にしているのとは大きく異なる（神奈川県個人情報保護条例第１０条）。ちなみにアメリカにおいては１９８８年にデータマッチングの危険性に鑑み、コンピューターマッチング・プライバシー保護法が制定されるに至っている。この法律ではデータマッチングを行なうに際してはマッチングプログラムについて、その実施を公示すること、提供機関と受領機関との間で書面による取り決めを行ないかつ議会へ報告し、国民の閲覧に供すること、監督・調整のための各行政機関にデータ保護委員会を設けることなどチェックのための種々な規定をおいているが、それでも国民データバンクの創設の危険性が指摘されているのである。法案ではこのような保護手続さえなされていないのであって、導入の時期では到底ない。

第４　住民基本台帳カード発行に関する問題点

１．住民基本台帳カードとは

報告書と法案によれば、住民基本台帳カード（以下「カード」という。）は、住民がネットワークシステムを利用して、より積極的な行政サービスを受けることができるようにすることを目的として、住民基本台帳コードの設定主体である市町村が全国共通様式の住民基本台帳カードを発行し、発行対象としては、自らカードの発行を申請した者のみとすることが想定されている（３０条の４４）。

また、カードの記憶媒体はＩＣ（集積回路）を利用し、ＩＣには、氏名・住所・性別・生年月日の基本的４情報及びコードを記憶させるものとしているが、カードのＩＣの記憶容量は８、０００文字程度あることから、残余の記憶領域については、市町村が条例の定めるところによって独自の活用をする余地を認め（３０条の４４）、各種申請手続の申請書記載の省略や本人確認の用に供するほか、更には、本人の選択によりカード表面に基本的４情報、写真、コードを記載した場合には、ＩＤ（身分証明書）として活用することなども可能とされている。

２．カード発行に関する問題点

このように、カードの発行は、あくまで本人の任意の申請との位置付けがなされている。

しかしながら、カードの活用は、市町村の条例等及び本人の選択とされてはいるものの、既にＩＤカードやその他の活用も想定されていることからすれば、カードを所持する者とカードを所持しない者との間に、事務手続き上の取り扱いに差異が生じ、その結果、制度上カードの発行は本人の任意の申請とされてはいても、事実上カードの発行申請を義務づけられるのと同じ結果になりはしないか、また、ひいては行政サービスの享受自体に差別が生じないかという問題が生ずる。

そもそも、カードの発行が本人の任意の申請によるものとされる以上、カードの有無によって住民が受ける行政サービスに差異があってはならない筈である。ところが、実際の窓口業務においては、カードがあれば読取機により直ちに本人確認が可能となり、事務手続が円滑に処理され得ることから、カードを所持する者が行政サービスの上において優先され、カードを所持しない者は、カード所持者に劣後して扱われる結果となることは想像に難くない。その結果、住民の心理としては、行政サービスを迅速に受ける手段として、勢いカードの発行を申請することが予想される。しかしながら、これは、カードを所持するものと比較して、カードを所持しないことによって事実上受ける不利益を回避するために、カードの発行申請が義務付けられるのと同一と言うべきであって、真に住民の任意による申請とは言い難い。

また、行政側からしても、行政事務の簡素化・迅速化の観点から、住民に対して、行政

サービスを受けるにあたってカードの発行申請をするように事実上求めたり、極端な場合には、カードを所持しない者が、いつまでも行政サービスが受けられないという結果が生ずることさえも予想されないではない。

さらに、カードの発行が本人の任意の申請とされているとしても、カードの発行対象が成年者に限られているわけではなく、幼児も含めた全ての住民に対するカードの発行が想定されるのであるから、自らカードの発行を申請するか否かの意思決定ができない行為無能力者については、事実上は、親権者あるいは保護者の意思ということになり、当の本人が気がついたときには、既に自分のためにカードが発行されているということが当然起こり得る。

よって、カードの発行申請に関する本人の任意性が担保される保障はないばかりか、カードの所持の有無によって、事実上行政サービスの享受の仕方や内容自体に差別が生ずる危険性は高いものと言わざるを得ない。

3．カードの活用に関する問題点

次に、カードには、基本的４情報及びコードが記載され、単に住民基本台帳事務そのもの（転入・転出事務の簡素化・合理化、広域的な住民票の写し等の交付、行政手続における住民票の写し等の添付の省略、転出後短期間のうちに当該市町村へ再び転入してきた者（再転入者）の正確な把握、災害時等における住民基本台帳電算システムの補完）に限らず、カードを活用することにより、他の行政機関等における本人確認事務（選挙の際の本人確認、災害時・緊急時等の本人確認、旅券の交付の際の本人確認、公共サービスの広域的な利用の際の本人確認等）への利用から進んで更には納税者番号制度への活用、更には、ＩＣの記憶領域を利用して市町村独自の活用が想定されていることから、カードにどのような情報が記録されることとなるのかという問題がある。

すなわち、自治体の独自の活用範囲については明確な規定がないため、健康診断の記録や血液型、生活保護や介護サービスの受給関係、更には図書館の貸出記録といった個人のあらゆる情報も、条例で定めさえすれば記録されることも可能となり、カードを所持者する本人でさえも、カードにどのような情報が記録されているかが分からないという事態も生じ得ることとなる。

しかも、自治体の独自の活用とは言っても、健康診断の記録や血液型等の情報を例にすれば、一自治体での利用だけでは無意味であるとして、当然、他の自治体においても利用可能なものとされるべきだとの議論が生ずるであろうし、従って、全国共通様式となることが予想されるだけでなく、更には民間病院での利用も要請されることになるであろう。

しかし、このことは、自治体の独自の活用の名の下に、全国統一カードやカードの民間利用につながるものであり、個人情報にとって無限定な危険性と裏腹の関係にある。

４．カードの保護措置、管理に関する問題点

更に、カード発行については、カードの保護措置あるいはカード管理に関する問題がある。

カードに、個人に関する大量な情報が記録されることとなれば、技術的な偽造防止や盗用防止等の措置が十分に講じられなければならないことは当然のことである。

しかしながら、カードの偽造や盗用等を完全に防止することが技術的に可能かどうかには疑問があり、また、カードの偽造や盗用等による被害は、罰則をもってしても回復し難いところである。

また、カードは自ら申請した者にのみ発行されるため、その管理の負担は、カードの所持者本人に負わされることになる。そうであれば、カードの盗難・紛失による悪用の危険性は避けられず、更には、私法上の取引などにおいて、債務者を心理的に拘束して弁済を強制する手段として、カード自体の交付が事実上要求されたり、その他カードの交付を不当に要求されるなど危険性も全く考えられないではない。

法案は住民票コードの告知要求を禁止しているが、その抑止策としては、繰り返し告知請求をするケースについて知事が中止勧告をし、勧告に従わないときは勧告に従うよう命じ、その命令に違反するときに刑罰を課するというもので実効性が疑わしい（３０条の４３）。

５．まとめ

以上のごとく、カードの発行には制度上・事実上・技術上の難点があり、これらの難点を無視してまで、カードを発行すべき必要性・相当性があるとは考え難く、カードの発行には反対である。

第５　わが国の個人情報保護制度の不備

１．公的部門における個人情報保護制度の不備

（１）行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律（以下、現行法という。）は公的部門における個人情報保護法として、昭和６３年１２月に制定され、平成元年１０月に施行された。しかし現行法は、目的規定（第１条）が示すとおり、行政の適切かつ円滑な運営をはかることを重要な柱とし、むしろ個人情報の流通に重きがおかれており、基本的人権としての個人のプライバシー保護の観点が欠落している。このことが、以下のとおり具体的な規定におけるさまざまな問題点となって現れてきている。本人確認情報の提供先の個人情報保護システムが整備されているかどうかは、本システムの安全性を左右するものである。

本システムとの関連で問題となる要点を指摘することとする。

①「利用および提供」の制限の不備

現行法は９条において、原則として個人情報の目的外利用及び外部提供を禁じているが、ここでも広い例外規定がおかれている。すなわち、保有機関の内部で利用する場合、他の行政機関、地方公共団体、特殊法人に提供する場合には実質的には無制限に近い利用・提供が認められているのである。また、提供を受けた機関に対して、個人の権利利益の保護の観点から使用目的・使用方法等を制限する旨の規定がないため、提供を受けた機関は個人情報をどのようにも利用できることとなり、問題がある。

②個人情報の外部委託の問題

現行法は、実施機関が外部に個人情報の処理を委託できることを原則的に認め、ただ第１１条で安全確保措置の努力義務を課し、第１２条で、委託を受けた者に対し「業務に関し知りうる個人情報の内容をみだりに他人知らせ、又は不当な目的に使用してはならない」と規定しているだけである。しかしこのような抽象的な規定の仕方では、実施機関以外の機関ないし民間の業者から個人情報が漏洩する危険が大きいことは明らかである。

③個人情報の開示、訂正請求権の不十分さ

現行法は処理情報の開示請求権を認め、開示請求があれば処理情報を原則として書面で開示することを義務づけ（１３条）、その開示期限を３０日以内と定めている（１５条１項）。しかし、同時に開示請求の対象外の事項（１３条１項但書）と不開示事項（１４条）を広く認め、実質的に自己情報の開示請求権を形骸化させている。

また、不開示事項の規定は包括的かつ抽象的であり、実質的に開示請求権が実効あるものになっているとは言い難い。

個人情報の訂正については現行法は１７条で規定しているが、あくまでも訂正の申出および再調査の申出ができるというにとどまり、法律上の訂正又は削除の請求権を

認めるものではない。その結果、その申出に基づいて訂正するかどうか、どのように訂正するのかは保有機関の判断に一切委ねられているのである。

④「安全確保対策」の不完全さ

収集した個人データは正確かつ最新のものとして管理されるべきであり、紛失、破壊、改ざん、不当な流通等の危険に対して安全性確保のための措置をとる必要がある。現行法は法５条において「個人情報の安全確保等」として規定しているが「必要な措置を講ずるよう務めなければならない」と抽象的に規定するにとどまっており、具体的な基準、義務について何ら規定していない。

⑤救済手段の不備

現行法には個人情報の開示請求権を確保するための救済手段について「苦情処理」の規定をおいているのみであり（２０条）、制度としての救済手続の規定が欠落している。

⑥法人・地方公共団体などが規制の対象外

現行法は規制の対象を国の行政機関に限定し、民間はもちろん、特殊法人や地方公共団体を対象から除いている。

特殊法人は、国の政策と密接な事業を行っているものであり、その数も多く、これらを規制の対象から外すのでは実効性がない。

地方公共団体の内、個人情報保護条例が制定されているのは全体の約６割にとどまっているのであり、残りの４割は何らの規制もしていないのである。

（２）以上のとおり、公的部門においては、個人情報保護のための立法的手当ては一応なされているものの、その内容は極めてお粗末であり、実質的な法的整備はなされていないといっても過言ではなかろう。このような状況の中で本システムが導入されれば、国民のプライバシーが侵害される危険性は極めて大きいものと思われる。

２．民間部門における個人情報保護

法案は民間での住民票コード告知要求を禁止し、住民票コードの記載されたデータベースの構築を禁止しているが（３０条の４３）、任意ないし任意を装った住民票コードの告知は抑止されないし、事実上の民間でのカード利用の可能性があることは前記のとおりである。データベース構築禁止も他に提供することを予定したデータベースの禁止のみで自社用のそれは禁止されていない。民間での個人情報保護を論ずる必要性はここにある。

（１）ところで、我が国の民間部門における個人情報保護については公的部門と異なり、全く立法がなされていない。

ただ、ＯＥＣＤの「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」（１９８０年）を受けて、１９８６年３月４日通産省産業政策局長通達「消費者信用情報機関等における消費者信用情報の管理等について」、同日大

蔵省銀行局長通達「金融機関等が信用情報機関を設置又は利用する場合の信用情報の取扱について」が出され、その後、１９８７年には財団法人金融情報システムセンター（ＦＩＳＣ）が「金融機関等における個人データ保護のための取扱指針」を、１９８８年には財団法人日本情報処理開発協会（ＪＩＰＤＥＣ）が「民間部門における個人情報保護のためのガイドライン」をそれぞれ策定するなどし、さらに、通産省は機械情報産業局長の懇談会の「民間部門における電子計算機処理に係る個人情報保護について（指針）」（１９８９年４月）に基づいて１９８９年６月ガイドラインの策定を行うよう関係事業者団体に対する通達を出し、同年９月には大臣告示により「電子計算機処理に係る個人情報保護のための措置等についての登録簿に関する規則」を定め、「個人情報保護措置登録制度」を創設し、１９９１年９月郵政省電気通信局長「電気通信事業における個人情報保護に関するガイドライン」を策定するなどしてきているだけである。

このように、わが国では、民間部門における個人情報保護は法的規制によるのではなく、自主規制による方向で進められ、法律上の規制としては、わずかに割販法４２条の４や貸金業規制法３０条（いずれも努力義務として情報の適正使用と正確情報の提供を定める）があるに過ぎず、しかもこれらも訓示規定に過ぎない。

（２）ところが、このような対応しかとられてこなかったこの１０年間に、これらの自主規制では不十分であり、個人情報保護のためには無力であることを明らかにする事件が次のように多数発生している。勿論、事柄の性格上このように明るみにでたものは実態の極めてごく一部のものであることに留意することが必要である。

１９８７年　２月	東洋信託銀行顧客情報が積水ハウスへ流出。
１９８８年　４月	久留米市妊娠届出書リスト市会議員を通じ訪販会社へ流出発覚。
同年１１月	枚方市で献血者名簿が自治会長らに流出判明。
１９８９年１２月	警察庁が管理する犯罪歴などの個人情報が香川県警、大阪府警のＯＢから大手信販会社に流出。
１９９０年　６月	旧三菱、旧三井両銀行から個人預金者のリストが東京都内の名簿業者に流出していたことが判明。
１９９２年　３月	三銀クレジットの「三越」会員登録データ約１３０００人分が名簿業者流出していたことが判明。
同年　９月	都税未納者データが名簿業者へ流出。
１９９３年　１月	横浜銀行久里浜支店の顧客データ約４００人分が流出。
同年　４月	消費者金融会社武富士の元支店長が顧客リスト４０００人分を同業者に横流し。
同年　４月	松山市の１２才少女リスト流出。

１０月	東海銀行東逗子支店からの顧客データ２６４人分流出。
１９９４年１２月	東京都江戸川区民の定期健康診断データ約８万人分が名簿業者に流出。
１９９５年　５月	消費者金融会社プロミスの顧客データ約２０万人分が流出。
１９９６年　８月	全国信用情報センター連合会から複数の消費者金融業者を装った者が約５年間で８０万件以上の個人情報を引き出す。
１９９７年　２月	Ｃ．Ｉ．Ｃから約４年間にわたり約１０００件の個人情報が債権回収業者に流出。
５月	日本生命外交員員、第一生命の保険契約者１５名の情報不正入手判明。
１９９８年　１月	さくら銀行の顧客データ約２万人分が流出。
１月	大阪の美術品販売会社から約５３万人分の顧客リストが流出
１月	関東のインターネットプロバイダーの保有する加入者450名のパスワード・住所がインターネット上に流出発覚。
１月	人材派遣会社テンプスタッフから登録社員９万人のリストが流出。インターネットで売買。
１月	兵庫県警生田署から捜査写真１８０枚が流出、週刊誌が掲載。
２月	高島屋百貨店の顧客データ約５０万人分が１９９５年に流出したことが判明。
２月	富士通子会社からＩＤ、パスワード情報がハッカーに盗まれたことが判明。

これらをみると、個人情報流出は年を追うにしたがって、次第に増加し、かつ大量の個人情報が流出するようになってきていることが明らかである。

また、上記表には掲記しなかったが、この外、携帯電話の番号、住所や氏名、取引銀行名等の情報が流出したり、「和牛オーナーシステム」の申込み名簿が名簿業者に売り込まれたり、神奈川県では女子高生の名簿を購入し、テレクラ広告を郵送するなどの事件が発生したりしている。

このように、近時大量の個人情報が流出するようになったのは、情報の商業的価値が認識され、企業などのビジネス戦略に組み込まれるようになってきたことや、大容量の記憶装置が開発され、瞬時に大量のデータを複写することができるようになったことにその原因の一があろう。

このような事態に鑑みると、もはや業者の自主規制などのガイドラインなどだけによる規制では対応しきれない事態となっているのは明らかである。

（３）また、海外では、従来からの国内法等によるＯＥＣＤ８原則が盛り込まれている
ＯＥＣＤガイドラインの策定にとどまらず、特にＥＵにおいて、１９９５年１０月「個人データ処理に係る個人情報の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令」（ＥＵ指令）が採択され、情報の内容についても規制されるようになった。これによると、域内各国は当該指令に適合するように３年以内に法制化を含めた検討を行うこととされており、個人情報の第三国への移転について、第三国が十分なレベルの保護措置を講じていない場合には、その移転が禁止されるほか、第三国が十分なレベルの保護措置を講じていないとＥＵ委員会が認定した場合には、第三国と交渉できることとなっており、「個人情報の十分なレベルの保護」を世界に広げることを意図したものとなっている。

これに対し、我が国では、またもや立法的規制によるのではなく、自主規制路線を踏襲し、通産省は１９９７年１月「民間部門における電子計算機処理に係わる個人情報の保護に関するガイドライン」を策定するに止まっている。このガイドラインそのものは、内容的には１９８９年４月の旧ガイドラインより優れたものとなっているが、行政指導という不透明な手法であるため、「自主的対応の限界」や指導対象の限界、個人情報保護侵害に対して「罰則」がなく、実効性確保の点から「個人情報の十分なレベルの保護」とはいえない。特にＥＵ指定において規定されているデータ処理へのアクセス権、データ処理者への勧告権、司法手続実施権等の強大な権限を有する「監視機関」制度についてはいまだ検討中であり、これを欠く我が国においては「十分なレベルの保護」がなされていないことは明白である。

（４）しかも、１９９７年１月のガイドラインから約１年後の今日、続々と個人情報流出事件が発覚してきた現状及びマスコミをはじめとし、立法による個人情報保護が強く主張されるようになってきている状況からすると、民間部門ににおける個人情報保護のために、もはやこのような機関などをも設けた立法による規制が急務であることは明らかである。自治省も今般の法案提出にあたり、民間を含めた包括的な個人情報保護法の必要性を認めざるをえない状況にある。

（５）民間利用禁止について、今回の法案では、住民票コードの提供を求めることを禁じ、民間利用を禁止することととしているが、これに違反し、提供を求めたり、住民票コードの記録されたデータベースの構成をしても、直ちに処罰されることはなく、都道府県知事の中止勧告があった後、これに従わないときに初めて処罰することにしているに過ぎない。しかも、その罰則は、１年以下の懲役又は５０万円以下の罰金と軽いものである。ちなみに、住民票コードを付せられる日本人の数を１億人とすると、このコード全体を違法に利用しても、罰金であれば１人あたり２，０００分の１円以下のペナルティがあるに過ぎないこととなる。しかも、任意提供の禁止、任意提供を受けた者に対する制裁までは設けておらず、結局、任意提供があったとして住民票コードが利用さ

れるおそれが極めて大きい。しかも、現に住民票コードが民間利用されているか否かについて、これを現実に調査することは極めて難しく、不可能といえよう。したがって、民間利用を禁止するためには、任意提供を禁止するとともに、任意提供を受けた者に対しての制裁規定も必要である。

（6）したがって、民間での個人情報保護法を欠いたまま民間部門でのカードの活用等の見込まれる本システムを導入することは、国民のプライバシーの侵害を容認することとなるものと思われ、到底容認することができない。

第６　個人情報保護の技術的措置について

（１）コンピューター、通信の技術発展、格段の利便性、低価格化等のスピードはその産業に関わる者の想像力をも凌駕しているといわれている。これにともない、不正なデータアクセスをする者にとっても不正アクセスを行う可能性はますます増大している。

コンピューターに入力された厖大な個人情報へ不正なアクセスがなされると、不正者が一般のパソコンを使っていた場合でも一瞬のうちに１００万人単位の個人情報がコピーされ、また一瞬のうちに他へちょうどウイルスのように伝搬されるという。しかも、困ったことに、不正アクセスが行われたことやコピーがなされたことなどに情報管理者や情報主体が気づくのは往々にして大量のデータが流出し他のデータベースへマッチングされた事後のことが多いのである。さらに重大なことは、その結果を誰がどのように引き起こしたものか、何回どこまでコピーされたかなどを追跡調査することが困難であるということである。

最高級の技術とセキュリティを誇る米国国防省やＮＡＳＡ、我が国の大手電算機メーカーへすら不正アクセスは起こったし、今後決して起こらないとの保証はないのである。

試案は、ＯＥＣＤ理事会勧告８原則に則った個人情報保護措置を法律で講ずるとし、個人情報の適切な管理のために万全な技術的保護措置を講ずるとして、専用回線の利用・通信データの暗号化・パスワード等による末端操作者の認証チェック、ネットワークシステムへのアクセスの監視などをあげる。

しかし、以下にのべるような措置が講じられておらず、試案の想定する技術的措置のみでは電算機化された住民基本台帳上の個人データを電気通信回線に接続して利用することの不安を解消することはできない。

「合理的な安全措置」（ＯＥＣＤ８原則－安全保護の原則）を図るというのであれば、セキュリティの詳細な方法および本ネットワークシステムの具体的な内容を公開し、本当に不正アクセスが行われる余地のない万全なセキュリティがはかられているのか否かについて、国民とくにコンピューター技術者からの批判を広く仰ぐべきである。

（２）前述のように最新のかつ最強のセキュリティシステムをとっているといわれる米国国防省やＮＡＳＡへも不正アクセスなどはおきるし、いかなるパスワードや暗号化をもってしてもいずれは破られるといわれている。したがって、ネットワーク、通信の基本的な安全性の要点は、極力回線上にデータを流さないこと、およびデータベースの保存箇所を極力減らすことに尽きるはずである。不正なアクセスを排除するためにも、同一のデータベースを複数個異なった場所に置かず、データのあるところを一つにし、そこへアクセスさせることが望まれる。また、バックアップについても、同一管理組織内の異なった場所（地震、雷、火事等を考慮する）で行うのが管理上安全と思われる。

ところが、試案は、回線上にデータを流すうえ、データベースを市町村のほか、都道

府県及び指定情報処理機関の３カ所に置くことを前提にしている。市町村レベルに限ってみても、回線上のデータに触れることのできる者は全国でかなり多くいるのではなかろうか。端末機は全国でどれほど多く設置されるのであろうか。このようなシステムでは、不正アクセスの機会を多くするだけではないかと思われる。

本人確認４情報についてもそれぞれの市町村のみがデータを保存するという原則を変えるべきではない。かりに、将来、不正アクセス排除の技術が確立したときでも、この原則は維持されるべきであろう。

（３）試案は、専用回線を使用することを安全性の根拠にすえる。しかし、これとても、デジタル化された信号を電話会社の電算機へ経由させるものに変わらず不正アクセスの危険性は常にあるのではないか。インターネット回線だから危険で、専用回線だから無条件で安全という単純なものではないはずである。

（４）電算機におけるセキュリティも人間が作り出す以上、矛を強くすれば盾が強くなる、盾が強くなれば矛が強くなるという関係のように、不正アクセス、不正複写の方法も必ずや作りだすことができ、この相互関係のなかでセキュリティが確保されるものである。ところが、試案はシステムが絶対に不正使用されないことを前提にしているため、かえって不正使用を最小限にするための技術的措置についてはなんら触れるところがない。

（５）さらに、これらのシステムを不正に利用するときの障壁として、データベースそのもののコピーを防止するために、単一の端末からの連続データアクセス（複数のデータを一度に大量にコピーしようとするとき）が発生したときは管理者に警告するシステムを設置したり、一定の連続したデータをアクセスすることやアクセスできる個人情報の件数を制限する措置が必要ではないか。

法案によると、都道府県と指定情報処理機関において磁気ディスクに記録するとあるが、これらのデータを一般のパソコンで使用するＭＯ（光磁気ディスク）等で不正にコピーすると簡単にすべてを１枚のＭＯに保存できてしまうのではないか。ちなみにＭＯでは１００万人以上の本人確認情報を１枚のディスクで保存できるという。先に報道されたさくら銀行の顧客データの違法な持ち出しは光ディスクプロッピーに保存された約２万人分の個人情報であり、大阪の美術品販売会社の顧客情報５３万人分も１枚の光磁気ディスクにコピーされたものであった。多くの場合は誰がどのように行い、どこに渡したかを追跡調査することは困難であろうといわれている。内部でも問題が発生する可能性を否定できない以上、外部委託はどのようにしてその安全性を確保しようとするのか。法案によれば、指定情報処理機関も国や地方自治体等も本人確認情報の処理の下請をすることを前提としている（３０条の１７、３０条の３３）。単に罰則を設ければ足るものではなく、肝要なことは、①不正なアクセスがおこらない技術的な措置、及び②おこってもデータベースそのもののコピーを防止する技術などの確立にあるのに試案や

法案ではこれらの点になんら触れない。

（6）さらには、試案はこのデータベースを利用した機関名と目的が、アクセス・ログ（データベース等へのアクセス履歴、記録）として保存され、それを定期的にチェックする機能を設置するとするが、加えて国民に対しログの開示請求権を保障し、かつ健康保険組合が組合員に定期的に診療歴と医療費を通知するように情報主体へのアクセス歴の通知をも制度化することにより、不正アクセスの監視を行うべきである。なぜならば、不正にアクセスが行われたか否かを一番知るのは情報主体であるからである。そしてこのことが情報主体のコントロール権を保障することになる。

（7）また、法令に基づくアクセスがあった場合に法令の定めるデータ利用目的の範囲内のアクセスか否かをどのように判定し、その範囲を超えるアクセスがあったときにどのように処理するのか、法案はなんら記述しない。個人情報を必要とする個別具体的かつ公益上の理由がない限りアクセスを認めないという内容の法制は不可欠である。同時に、たとえパスワードを持っている者からのアクセスであっても「公安上必要である」というような抽象的な理由によってデータベースそのものをコピーしようとしたときは、電算機自体がアクセスを受け付けないようにするセキュリティシステムの構築が必要である。しかし、報告書から本法案に至るまでの自治省側の説明には、このような技術的な裏付けがあるのか否かについて触れたものはなかった。

第７　指定情報処理機関と権利保護規定の問題点

１．指定情報処理機関について

改正法案第３０条の１０から３０条の２８までは、指定情報処理機関についての規定である。指定情報処理機関は、「都道府県単位センターおよび全国単位センター」と言われてきたものであるが、法案によってはじめてその具体的内容が明らかになった。すなわち、都道府県知事は、指定情報処理機関に、住民票コードの指定及び市町村長への通知、本人確認情報の提供等の事務を行わせることができる。自治大臣は、地方公共団体が基本財産の全部または一部を拠出している等の指定基準に適合している場合にのみ、指定情報処理機関として指定することができる。指定情報処理機関には、本人確認情報保護委員会を置く。また、指定情報処理機関は、人事、事業計画、本人情報管理規程について自治大臣の認可を受け、報告を求められたり調査を受ける、さらには指定を取り消されることもあるなど、自治大臣の監督下におかれる。

このように、指定情報処理機関は、住民基本台帳ネットワークシステムの実務の中心的役割を果たすものと位置付けられているようである。しかし、その性格は不明確であり、疑問が多い。

まず、一体どのような機関が指定情報処理機関になるのか。住民票コードの付番や本人確認情報の取扱などプライバシーの核心に関わる業務を行うという公的性格からすれば、それ自体を目的とした公益法人を独自に設立する趣旨のようにも解される。しかし、事務処理を依頼するか否かは個々の都道府県知事に委ねられるし、指定の取消しもありうるということからすれば、地方公共団体が出資していて情報処理を扱う既存の民間機関を指定することもありうるのだろうか。その場合、指定情報処理機関におかれる本人確認情報保護委員会はどのような性格の機関になるのか。指定情報処理機関の代表者に意見を述べるに過ぎない委員会（３０条の１５）に第三者機関としての独立したチェック機能を期待することはできない。

従来いわれてきた、「都道府県単位センター」と「全国単位センター」の関係も不明確である。同一機関が両方を兼ねるのかも明らかではない。実際上全国に一つだけなのか複数の機関が存在することになるのかも不明である。さまざまな指定情報処理機関が全国に多数存在して、住民基本台帳ネットワークシステムを運用することは混乱を生じる恐れがあるし、プライバシー保護の点からも疑問である。かといって、事実上全国で一つの機関にすべての都道府県が委託するとなると、個人情報が高度に集中管理されることとなり、このシステムにおける都道府県の主体性はなくなり、「分権」は形骸化する。

指定情報処理機関については、従来の議論の中では言葉としては登場していたが、具体的な構想は示されておらず、法案となってようやく、これまでにあまり例のない、理解しにくい制度であることがわかった。従って、今後、国会審議以前に、国民に対して十分な

説明がされる必要があり、かつ、そのような機関を置くことの是非について議論を尽くす必要がある。

2．権利保障及び救済手続きの不備

改正法案では、都道府県知事又は指定情報処理機関に対する本人開示請求権を規定している（３０条の３７）。しかし、訂正等の請求については請求権として規定せず、「申し出」にとどめ、調査を行って結果を通知する義務を置くにとどめた（３０条の４０）。

また、本人確認情報は、市町村から他の市町村へ、都道府県又は指定情報処理機関から管轄内・管轄外の市町村、庁内及び他の都道府県、国又は法人へと幅広く通信回線を通じて提供されることになっており、提供の基準は別表に掲げる特定の事務に限らず、「条例で定める事務」、国の行政機関の「所掌事務」等、広範囲に及んでいるが（３０条の６、３０条の７、３０条の８、３７条）こうした目的外利用、外部提供についても情報主体たる国民に通知されることはなく、違法な本人確認情報流出をチェックする方法もない。

そして利用制限違反（３０条の３０、３０条の３２、３０条の３４、３０条の３６）等個人情報の違法な取扱の中止請求権等の不服申立の手段は規定せず、苦情処理の規程を置くに過ぎない（３０条の４１）。都道府県審議会も単に知事に建議をするのみ（３０条の９）で、是正命令権もなく救済機関としての役割を果たしえない。

さらに、都道府県知事又は指定情報処理機関が開示、訂正等に応じない場合の救済手続きや利用済の本人確認情報消去も全く規定されておらず、総じて制度の運用に伴う個人の権利の侵害を防止する手続きは不十分と言わざるを得ない。