

現在のページ：[ホーム](#) > [くらしの情報](#) > [証明・登録](#) > [住基ネットワークシステムについて](#) > [住民基本台帳ネットワークシステム](#) > [住民基本台帳ネットワークシステムについて](#) > [住基ネット調査研究事業](#) > [事業概要](#)

事業概要

更新日 平成22年7月27日

国立市住民基本台帳ネットワークシステム調査研究事業概要

平成15年7月

- 事業の目的

法律面及び情報システム面の専門家各1名に調査研究を依頼し、住民基本台帳ネットワークシステム再稼働に当たっての、条件整備の方針を明らかにすることを目的とする。

- 調査研究項目

1. 個人情報の保護に関する法律(平成15年法律第57号)及び行政機関の保有する個人情報の保護に関する法律(平成15年法律第58号)により、住民基本台帳ネットワークシステムに係る個人情報の保護は保障されたか。
2. 住民の自己情報コントロール権が保障されているか。
3. 国立市の住民情報コントロール権が保障されているか。
4. 情報漏えい等のリスクと住民基本台帳ネットワークシステムの稼働によるメリットとの比較衡量
5. ストーカー、DV(ドメスティック・バイオレンス)の被害者を支援する目的で制定・施行した「国立市ストーカー行為等の被害者支援に関する住民基本台帳事務取扱要綱」に沿った、被害者支援に障害とならない制度・運用が保障されているか。
6. 本人確認情報を利用する国の機関等の個人情報保護が十分措置されているか。
7. 個人情報の漏えいを防止するセキュリティ対策が十分措置されているか。
8. 公的個人認証制度における個人情報の保護及びセキュリティ対策が十分措置されているか。
9. その他必要な事項

用語解説：[住民基本台帳ネットワークシステム](#) [ストーカー行為](#) [本人確認](#) [住民基本台帳](#) [ストーカー](#)

※「用語解説」内のリンクは、ウェブリオが運営する辞書サイトの解説ページ(別ウィンドウ)に移動します。

総務部 市民課 市民係

電話:042-576-2111(内線 131,132) ファクス:042-576-0264

[メールでのお問い合わせは専用フォームをご利用ください。](#)

現在のページ：[ホーム](#) > [くらしの情報](#) > [証明・登録](#) > [住基ネットワークシステムについて](#) > [住民基本台帳ネットワークシステム](#) > [住民基本台帳ネットワークシステムについて](#) > 住基ネット調査研究事業

住基ネット調査研究事業

国立市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。)について、個人情報の保護および情報漏えい等システムのセキュリティに関する安全性が確認できないとの理由から、平成14年12月26日に回線を切断しました。

一方、全国的には平成15年8月25日から住基ネットの二次稼働が始まり、住民票の広域交付や、住民基本台帳カードによる転入転出の特例サービスが開始されています。市では、どのような条件整備をすれば再稼働が可能なかを明らかにすることを目的に、平成15年7月から住基ネットの調査研究に着手しました。法律面については弁護士の稲垣隆一氏に、情報システム面についてはアイ・ビー・エムビジネスコンサルティングサービス株式会社技術理事の大木栄二郎氏に依頼し、平成15年12月26日に報告書がまとまりました。市では、この報告書に基づき、ただちに改善が必要なものについては、すでにその整備を終えました。今後は、この結果を慎重に検討した上で、住基ネットの再稼働に向けてより一層の条件整備に努めていきます。市民の皆様のご理解とご協力をお願いします。

[事業概要](#)

[法律面](#)

[情報システム面](#)

[研究者の紹介](#)

現在のページ : [ホーム](#) > [くらしの情報](#) > [証明・登録](#) > [住基ネットワークシステムについて](#) > [住民基本台帳ネットワークシステム](#) > [住民基本台帳ネットワークシステムについて](#) > [住基ネット調査研究事業](#) > [法律面](#)

法律面

更新日 平成22年7月27日

記調査項目に関し、以下のとおり報告する。

記

1. 個人情報の保護に関する法律(平成15年法律第57号)及び行政機関の保有する個人情報の保護に関する法律(平成15年法律第58号)により、住民基本台帳ネットワークシステムに係る個人情報の保護は保障されたか。
2. 住民の自己情報コントロール権が保障されているか。
3. 国立市の住民情報コントロール権が保障されているか。
4. 情報漏えい等のリスクと住民基本台帳ネットワークシステムの稼働によるメリットとの比較衡量
5. ストーカー、DV(ドメスティック・バイオレンス)の被害者を支援する目的で制定・施行した「国立市ストーカー行為等の被害者支援に関する住民基本台帳事務取扱要綱」に沿った、被害者支援に障害とならない制度・運用が保障されているか。
6. 本人確認情報を利用する国の機関等の個人情報保護が十分措置されているか。
7. 個人情報の漏えいを防止するセキュリティ対策が十分措置されているか。
8. 公的個人認証制度における個人情報の保護及びセキュリティ対策が十分措置されているか。
9. その他必要な事項

調査事項1について

住民基本台帳ネットワークシステム(以下「住基ネットシステム」という。)に係る個人情報の保護は、個人情報の保護に関する法律(以下「個人情報保護法」という。)及び行政機関の保有する個人情報の保護に関する法律(以下「行政機関個人情報保護法」という。)が制定されても、少なくとも住民基本台帳法(以下「住基法」という。)を改正した第145回国会が想定した程度には至っていない。

1. 調査事項1の回答の前提として、住基法附則第1条第2項の「所要の措置」の意味を明らかにし、個人情報保護法及び行政機関個人情報保護法の制定によって附則第1条2項の「所要の措置」が行われたと言えるかを検討する必要がある。
2. 改正住基法附則第1条第2項の「所要の措置」は、第145回国会における住基法改正審議にあたり内閣提出法案への修正として議員提案されたものであり、提案者側は、その内容を「第1に、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、第2に、第1のシステムの整備状況をふまえ、住民基本台帳法におけるさらなる個人情報保護措置を講ずるため、所要の法改正等を図ること、第3に、地方公共団体が適切に住民基本台帳ネットワークシステムを運用することができるよう、自治省(当時)として個人情報保護に係る指導を十分に行うことなど」の三点だと説明し注1、政府も同様の認識を有することを明らかにしている注2。従って、小淵総理のいう「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」とは、上記の3つを意味するものと解される注3。
3. 「所要の措置」第1と法の制定

個人情報保護法等の制定の経緯

このような状況下で、政府は、住基法改正審議の最中の平成11年7月14日、高度情報通信社会推進本部に個人情報保護検討部会を設置して「所要の措置」第1の「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」の検討を開始し注4、この成果注5は、その後の個人情報保護法制化専門委員会の検討結果注6を経て、第154回国会への「個人情報の保護に関する法律案」、第155回国会への「行政機関の保有する個人情報の保護に関する法律案」、「独立行政法人等の保有する個人情報の保護に関する法律案」、「情報公開・個人情報保護審査会設置法案」及び「行政機関の保有する個人情報の保護に関する法律等の施行に伴う関係法律の整備等に関する法律案」として結実し注7、これら個人情報保護関連五法案は、第

156回国会で成立した。

個人情報保護法等の制定と「所要の措置」第1

成立した「個人情報の保護に関する法律」は、官民を通じた我が国における個人情報保護の基本法部分と民間部門における個人情報保護法の一般法、「行政機関の保有する個人情報の保護に関する法律」、「独立行政法人等の保有する個人情報の保護に関する法律」は、行政機関・独立行政法人における個人情報保護法の一般法、「情報公開・個人情報保護審査会設置法」は、これらによる情報公開に関する法制を整備したもの、「行政機関の保有する個人情報の保護に関する法律等の施行に伴う関係法律の整備等に関する法律」は、行政機関個人情報保護法等の施行に伴う関係法律の整備を行うものであり、「所要の措置」第1の「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」の一内容として制定されたものであるといえることができる。

「所要の措置」第1の実質的要件

もっとも、法が制定されても、その法が「求められる水準」を満たされない限り「所要の措置」第1の実質的要件は満たされていないとする指摘注8があり正当である。

1) 「求められる水準」の意義

この「求められる水準」とは、「第145回国会での改正住基法案の審議にあたり論じられた個人情報保護に関する主要な論点について少なくとも改正住基法を超える水準」を指すと解される注9。

その理由は以下の三点にまとめられる。

1. 第145回国会は、住基ネットシステムが実施された場合、住基法案では、同国会で論じられた個人情報保護に係る主要な論点に対応するには不備だとの認識に立っていたものと解され、小淵総理も同様の認識を答弁注10していること。
2. しかしながら、第145回国会においては、修正提案者側の説明、小淵総理及び野田毅自治大臣(当時)の答弁以上に「所要の措置」の具体的内容は示されず、その内容を具体化する決議もなされていないこと。
3. 従って、第145回国会は、「所要の措置」第1が有すべき水準として、改正住基法案の審議にあたり論じられた個人情報保護に関する主要な論点について、少なくとも改正住基法を超える水準を想定していたとはいえるものの、それ以上の具体的内容まで想定しているとは認められないこと。

2) 「求められる水準」の要件

「求められる水準」の要件を構成する「第145回国会での改正住基法案の審議にあたり論じられた個人情報保護に関する主要な論点」とは、個人を番号で一元的に管理することそれ自体の当否、個人情報保護法の整備に先立って住基ネットシステムを導入することの当否を別とすれば、以下のとおりである。

1. 十分なプライバシー保護、情報主体による個人情報の利用中止請求権を認めること。
2. 個人情報の一元的な収集管理を行わないこと、データマッチング、内部データベースの構築の危険への対処、名寄せの危険への対処、情報収集や犯罪捜査などの本人照会等に使われるという懸念が払拭されること。
3. 目的外利用の刑罰規定を設けること、特に公務員の違反時には即効性ある直罰とともに、その上司、責任者への処罰を定めるべきこと。
4. 行政機関が蓄積したデータベースの保持期間、消去を適切にすること、取扱者の記録を保存すること。

個人情報保護法・行政機関個人情報保護法は「求められる水準」にあるか

以下に述べるとおり、個人情報保護法及び行政機関個人情報保護法は、法制度としては、「求められる水準」の要件の1ないし3の論点について、改正住基法の水準を超える内容であると評価できる。

● 十分なプライバシー保護、情報主体による個人情報の利用中止請求権

1. 個人情報と憲法第13条の接合

ア 改正住基法は、本人確認情報を含む住民基本台帳記載の個人情報について、憲法上の人権との接合を明らかにしていない。

イ これに対し、個人情報保護法及び行政機関個人情報保護法第1条は、個人の権利利益の保護を定め、個人情報保護法第3条は、個人情報が「個人の人格尊重の理念の下に慎重に取り扱われるべきものであること」を定めて、個人情報が憲法第13条と接点を有することを明確にしている注11。行政機関個人情報保護法には、個人情報保護と憲法の関係を直接示す規定はないが、個人情報保護法第1条及び第3条は、個人情報保

護の基本法として行政機関にも適用される。

2. OECD8原則の具体化

ア 改正住基法は、都道府県知事及び指定情報処理機関以外に対する本人確認情報の開示請求を認めていない。また、都道府県及び指定情報処理機関が訂正、追加又は削除(以下「訂正等」という)の申出に対応して直接に訂正等を行う規定は設けていない。

イ これに対し、個人情報保護法第15条ないし第27条及び第31条並びに行政機関個人情報保護法第3条以下は、OECD8原則を具体化し、以下のとおり、本人が適切な範囲で個人情報に関与する仕組み注12を設けている。

- (ア) 保有個人データに関する事項の公表等は、個人情報保護法第24条と行政機関個人情報保護法第11条
- (イ) 保有個人データの開示は、個人情報保護法第25条と行政機関個人情報保護法第12条ないし第26条
- (ウ) 訂正等は個人情報保護法第26条と行政機関個人情報保護法第27条ないし第35条
- (エ) 利用停止、消去請求(以下「利用停止等」という)は、個人情報保護法第27条、行政機関個人情報保護法第36条ないし41条
- (オ) これらの例外措置を講じるときの理由説明義務は、個人情報保護法第28条
- (カ) 苦情処理は個人情報保護法第31条、行政機関個人情報保護法第42条

3. 自己情報コントロール権の実質的な保障

ア 改正住基法は、上記(2)記載のとおり、都道府県知事及び指定情報処理機関以外に対する本人確認情報の開示請求を認めず、また、都道府県及び指定情報処理機関が訂正、追加又は削除(以下「訂正等」という)の申出に対応して直接に訂正等を行う規定は設けていないことから、自己情報コントロール権を実質的に保障する明文の規定は認められない。

イ これに対し、個人情報保護法及び行政機関個人情報保護法については、堀部政男中央大学教授は、平成15年4月21日、第156回国会での個人情報保護法案の審議を行っていた参議院個人情報の保護に関する特別委員会に参考人として出席し、「自己情報コントロール権は、「本人の情報を取得する、収集する段階で目的を明確にする・・・目的外に利用しないとか、さまざまなものによって、・・・実質的に保護される・・・わけでありまして、特に、自分の情報を自分で開示請求しそれを見ることができ、誤っていれば訂正を求めることができる、それに応じない場合に異議を申し立てる等々の権利、これらをすべて含めて、むしろ自己情報コントロール権というふうに理解すべきであると私は考えております。それは、この法案におきましても実質的には保障されているものというふうに理解しております。それを政府案では、「権利利益を保護」ということで規定しております。」と述べており注13、第1条で「権利利益を保護」の文言を規定する個人情報保護法及び行政機関個人情報保護法はいずれも自己情報コントロール権を実質的に保障するものと評価され、改正住基法の水準を超えるものと評価できる。

- 個人情報の一元的な収集管理を行わないこと、データマッチング、内部データベースの構築の危険への対処、名寄せの危険への対処、情報収集や犯罪捜査などの本人照会等に使われるという懸念の払拭
1. 改正住基法は、データマッチング、内部データベースの構築、名寄せそれ自体は規制せず、目的拘束を厳格に定め、目的外利用を禁じている。
 2. 行政機関個人情報保護法も、例えば、恩給と年金の支給調整、不法出入国管理のための出入国管理と旅券のデータマッチングなど、行政目的達成のために一定のデータマッチングを必要とする場合もあることなどに鑑み、データマッチングそれ自体を禁じず、その弊害を、個人情報の保有、利用及び提供にあたっての厳格な目的拘束で防止する手法をとっている。

すなわち、行政機関個人情報保護法は、個人情報の保有を、所掌事務を遂行するため必要な場合に限り、利用目的をできる限り特定した上、目的達成に必要な範囲を超えて個人情報保護を保有、利用及び提供することを禁じている(第3条、第8条)。

しかし、これを担保するため、行政機関の長が個人情報ファイル簿を保有しようとするときは、一定の例外を除き、予め総務大臣に対して利用目的、記録項目、記録範囲及び記録情報の収集方法、経常的な提供先その他を通知させ(第10条)、個人情報ファイル簿を公表し(第11条)、目的外利用、提供に対する利用停止請求(第36条ないし第44条及び第47条)、施行状況調査結果による目的外利用や提供状況の公表等(第49条ないし第51条)等によってこれを担保し、更に一定のものについては、第55条が罰則を科す方法で規制している。

これらには広範な例外と行政機関の裁量が認められ、国会審議においても烈しく論じられた結果、付帯決議(第156回国会内閣法第72号)注14がなされるに至ったが、担保規定の内容に照らせば、改正住基法の水準を超えるものと評価できる。

なお、個人情報保護法は、利用目的の特定(第15条)、取扱いの目的制限(第16条)、取得時の利用目的の通知・公表又は明示、保有個人データに係る利用目的の公表、通知(第24条)、開示(第25条)、訂正等(第26条)及び利用停止等の請求(第27条)等を通じて上記弊害を防止する構造をとっている。
- 目的外利用の刑罰規定、公務員の違反時には即効性ある直罰規定、その上司、責任者への処罰の定め
1. 改正住基法は、都道府県知事、指定情報処理機関、本人確認情報の提供を受けた市町村長その他の市町村の執行機関若しくは都道府県知事を除く都道府県の執行機関又は別表第一の上欄に掲げる国の機関若しくは法人及び事務の受託者の、本人確認情報の利用制限(住基法第30条の30、32及び34)に反する行為に対する罰則を設けていない。
 2. しかし、行政機関個人情報保護法第53条ないし第55条は、上司、責任者の連座、両罰規定は設けてはいないものの、これらに反した本人確認情報の収集、盗用、提供のうち一定の態様のものについて罰則を科しており、改正住基法の内容を超える水準にある。

なお、個人情報保護法も、間接罰規定ではあるが、個人の重大な権利利益の侵害が切迫していると認められるに至れば、罰則を科しうる方法を講じている。
- 「行政機関が蓄積したデータベースの保持期間、消去を適切にすること、取扱者の記録を保存すること」について

- 改正住基法は、本人確認情報については、都道府県知事又は指定情報処理機関、本人確認情報の提供を受けた市町村長その他の市町村の執行機関若しくは都道府県知事その他の都道府県の執行機関又は別表第一の上欄に掲げる国の機関若しくは法人及びこれらから本人確認情報を受領して委託を受けて電子計算機処理等を行う者に対し、その漏えい、滅失及びき損の防止その他の当該本人確認情報の適切な管理のために必要な措置を講じなければならないことを定めている(第30条の29第1項、第30条の33)。また、住民票又は戸籍の附票に記載されている事項については、市町村長及び市町村長から住民基本台帳又は戸籍の附票に関する事務の処理の委託を受けた者に対し、住民票又は戸籍の附票に記載されている事項の漏えい、滅失及びき損の防止その他の住民票又は戸籍の附票に記載されている事項の適切な管理のために必要な措置を講じなければならないことを規定している(第36条の2)。

「行政機関が蓄積したデータベースの保持期間、消去を適切にすること、取扱者の記録を保存すること」は、この「適切な管理のために必要な措置」として行われるべきものと解されるが、明文の規定はない。

- 行政機関個人情報保護法第6条第1項は、個人情報の漏えい、滅失又はき損の防止その他の個人情報の適切な管理のために必要な措置を講じることが定められているが、改正住基法同様、上記保持期間、消去、取扱者の記録の保存を規定する明文はない。
なお、個人情報保護法第20条ないし第22条は、これに加えて従業員及び外部委託先への必要な監督を明文で義務づけており、法文の体裁上は、改正住基法を超える内容を規定している。しかし、改正住基法同様、保持期間、消去、取扱者の記録の保存を規定する明文はない。

- 改正住基法及び行政機関個人情報保護法の「適正な管理のために必要な措置」個人情報保護法の「安全管理のために必要かつ適切な措置」の具体的な規範内容はいずれも法定されていない。

個人情報保護法においては、「プライバシーポリシーの策定や研修の実施、安全管理者の設置等の監督・責任体制の整備といった人的な措置」注15すなわち「個人情報の取扱いに関する内部規程、マニュアル等の整備、安全管理者の設置、安全確保のための組織の整備、システムの安全セキュリティ監査の実施、個人情報保護意識の向上、安全性・正確性の確保のための研修の実施、外部委託に際しての再委託先への監督契約などの組織的保護措置、ネットワークコンピュータのファイアウォールの適切な設定、情報システム上のセキュリティ機器の整備や暗号化、アクセス制限の設定といった技術的な措置」を指すとされており、各事業分野における標準的な措置が示されることが期待されているとされ注16、改正住基法も行政機関個人情報保護法も解釈上記措置を含むセキュリティ対策が含まれると解される。

その実現の枠組としては、既にJISQ15001への準拠やその認証制度としてのプライバシーマークの取得、製品等の調達条件として用いられるべきISO15408及びST制度、情報セキュリティマネジメントの国際規格による枠組としてBS7799-1:1999、ISO/IEC17799:2000、JISX5080:2002、その認証制度としてBS7799-2:2002、ISMSVer.2.0による適合性評価制度の利用があり、監査制度としては主として内部監査人による助言型監査を想定したシステム監査の他に第三者による保証型監査をも利用できる情報セキュリティ監査制度が存在する。上記内容の、保持期間の特定、収集目的の終了による取得情報の削除、取扱者のログの保存は、JISQ15001への準拠(特に安全対策(4.4.4.2))、JISX5080への準拠にあたり他に合理的理由が存在しない限り原則として行うべき管理策であって、改正住基法第30条の29第1項、第30条の33及び第36条の2、個人情報保護法第20条及び行政機関個人情報保護法第5条の各措置の当然の内容となっているものと解される。

以上の検討によれば、個人情報保護法及び行政機関個人情報保護法は、法制度としては、上記(1)ないし(3)の論点について、改正住基法の水準を超える内容であると評価でき、「所要の措置」第1の実質的要件を満たすものと考えられる。

「所要の措置」第2について

- 「所要の措置」第2は、第1のシステムの整備状況をふまえ、住基法におけるさらなる個人情報保護措置を講ずるため、所要の法改正等が行われることである。
- 住基法の改正は、住基ネットシステムの利用を決定した平成11年8月18日法律第133号の後、「所要の措置」の形式的要件が満たされた平成15年5月23日から現時点(平成15年12月25日)までの間に、既施行分として、平成11年12月22日法律第160号、平成13年7月4日法律第101号、平成14年6月12日法律第65号があり、未施行分として平成14年12月6日法律第138号、平成14年12月13日法律第153号、平成14年12月13日法律第170号、平成14年12月20日法律第192号、平成15年5月30日法律第54号、平成15年6月11日法律第69号、平成15年6月18日法律第96号、平成15年7月4日法律第103号がある。
- しかし、これらのうち、「所要の措置」第1のシステムの整備状況をふまえ、上記法律第133号に「さらなる個人情報保護措置」を講ずることを内容とするものは認められない。
- 従って、「所要の措置」第2は認められない。

「所要の措置」第3について

- 「所要の措置」第3は、地方公共団体が適切に住民基本台帳ネットワークシステムを運用することができるよう、総務省として個人情報保護に係る指導を十分に行うことである。
- 総務省は、大臣官房政策統括官、自治行政局市町村課、住民基本台帳ネットワークシステム調査委員会、財団法人地方自治情報センター、住基ネットシステム推進協議会その他の組織の活動及びチャンネルを通じて膨大な指導を行っているものと見られる。その状況は、総務省ホームページからも一部を見て取ることができる(以下重複あり)。
 - 体制の整備
 - 平成14年2月地方公共団体における情報セキュリティ対策に関する調査研究会設置

- (2) 平成14年8月2日総務省住基ネットシステム緊急対策本部設置
 - (3) 平成14年8月30日住基ネットシステム調査委員会設置
- 個人情報保護条例の制定の促進
- 平成15年6月16日総務省政策統括官通知「地方公共団体における個人情報保護対策について」
- 情報セキュリティポリシー、技術基準、コンティンジェンシープランの策定と改正
- (1) 平成12年3月31日行政情報システム各省庁連絡会議幹事会了承「国の行政機関における情報システム関係業務の外注実施ガイドライン」
 - (2) 平成13年3月30日総務省自治行政局地域情報政策室「情報セキュリティポリシーガイドライン」制定
 - (3) 平成13年6月総務省自治行政局地域情報政策室「地方公共団体における情報セキュリティポリシーの例示」
 - (4) 平成14年6月10日総務省告示第334号「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」(「住基ネットセキュリティ基準」)制定
 - (5) 同日住基ネットシステム推進協議会決定「住基ネットのセキュリティ対策に関する指針」
 - (6) 平成14年8月2日発表総務省住基ネットシステム緊急対策本部「住基ネットシステム緊急時の対応の概要」
 - (7) 平成15年2月26日総務省政策統括官「情報セキュリティポリシーの早期策定等情報セキュリティ対策の徹底について」
 - (8) 平成15年3月18日「情報セキュリティポリシーガイドライン」一部改訂
- 情報セキュリティ対策の実施支援
- (1) 市区町村における庁内LAN上のデータ送信における高度なセキュリティレベルの維持を図るための技術面、運用面での方策を検討し、実行に移す。
 - (2) 市区町村における庁内LAN－インターネット間のファイアウォールについて、希望する市区町村に対し、遠隔でセキュリティ診断を実施する。
 - (3) セキュリティパッチについて、動作確認の迅速実施、引き続き早期の適用に努める。
 - (4) 住基ネットに対するペネトレーションテストの継続的实施
- セキュリティ研修
- (1) 平成15年5月13日の都道府県・政令指定都市住民基本台帳ネットワークシステム担当課長会議をふまえ、都道府県は市区町村に対して必要な技術指導を行うよう要請
 - (2) 平成15年8月8日発表 特に重点7項目は各都道府県、総務省及び指定情報処理機関において、徹底した技術的助言、指導を実施
 - (3) 地方公共団体職員に対するセキュリティ研修の実施
- 情報セキュリティに関する監査の促進
- (1) 平成14年7月29日発表 全地方公共団体を対象に監査法人等による外部監査を実施(稼働後できるだけ早期に、全団体に対して、運営面でのチェックリストを配布し、その回答状況を点検するとともに、監査法人等により個別に監査を行う方法を検討)
 - (2) 平成14年11月7日財団法人地方自治情報センター「チェックリスト、システム監査について」
 - (3) 平成15年1月、2月 住基ネットシステム及びそれに接続している既設ネットワークに関する調査
 - (4) 住基ネットシステムセキュリティチェックシート(第3回住基ネット調査委員会資料)
 - (5) 平成15年5月12日「住基ネットシステム及びそれに接続している既設ネットワークに関する調査票による点検結果」(第4回住基ネット調査委員会資料)
 - (6) 住基ネットシステムに関するチェックリストによる自己点検、セキュリティ監査の実施(第5回住基ネット調査委員会資料)
 - (7) 外部監査によるシステム運営監査
 - (8) 市区町村における庁内LANに関するチェックリストによる自己点検、セキュリティ監査の実施に対する積極的支援
 - (9) 監査ガイドライン、監査体制の整備
- 自治体等の要望への対応
- 平成15年9月29日「住基ネットセキュリティ基準」(総務省告示)改正による本人確認情報提供状況の開示、市町村調査権の法制面における位置づけを明文化
- 事故情報の通知と警告の発出
- (1) 平成14年11月7日財団法人地方自治情報センター「11月1日発生の全国センターサーバの障害について」
 - (2) 平成15年1月6日総務省自治行政局市町村課長「住民基本台帳における個人情報の保護対策について」
 - (3) 平成15年3月14日総務省自治行政局地域情報政策室長「個人情報の管理に係る外部委託契約の内容及び履行状況の緊急点検について(依頼)」長野県が実施した「市町村ネットワークの安全性調査」を受けての対応
 - (4) 平成15年5月29日総務省自治行政局市町村課長「長野県本人確認情報保護審議会の第一次報告について」
 - (5) 平成15年12月26日 長野県が実施した「市町村ネットワークの安全性調査」を受けての対応措置
- セキュリティ対策に関する地方財政措置
- 平成16年度地方財政重点施策注においても、電子自治体の推進施策として「住基ネットシステムの円滑な運用」、「電子自治体における安心と信頼の確保」が掲げられ、住基ネットシステムにおける個人情報保護のための、技術・運用面での対策の一層の充実、信頼性の高い

電子自治体を構築するため、すべての地方公共団体において住民の意識の高まりに対応した個人情報保護条例の制定及び情報セキュリティポリシーの策定を強力な推進、電子自治体を支える職員の教育・研修の推進、情報セキュリティ対策の中核を担う人材の研修強化が掲げられ、今後も、適切な住基ネットシステムの運用に向け、個人情報保護に係る指導を十分に行うことが理解される。

3. しかしながら、平成15年10月1日現在注21、セキュリティポリシーは、都道府県の6・4%、市町村の50・4%が策定していない。また、各自治体のセキュリティレベルを認識するのに不可欠である情報セキュリティ監査は、都道府県の23・4%が未実施(検討中を未実施に加えると76・6%)、市町村では、53・6%(同91・1%)が実施していない注22。

このような環境のもとで、個人情報保護に関する条例の制定状況は、全3260団体中の74・0%にあたる2413団体である注23。(なお、平成15年10月1日段階では全3204団体中の76・7%にあたる2458団体に増加注24している。)なお、定められた条例のうち、民間部門の事業者の責務を定めるものは54・2%、指針策定の助言や指針等による事業者に対する規制を行うものは18・5%、地方公共団体の民間事業者に対する監視体制を定めるものは、23・2%である。

4. 住基ネットシステムは、後に述べるとおり、電子国家、電子自治体の実現のインフラであり、全国の地方公共団体がその憲法上の地位、状況に応じて、その責務を適切に果たすべきものである。特に、個人情報保護法、行政機関個人情報保護法の成立した現在、個人情報保護条例の制定、個人情報保護を支える情報セキュリティ対策の出発点である情報セキュリティポリシーの策定、セキュリティレベルを認識し適切な情報セキュリティ対策を構築するための情報セキュリティ監査は不可欠というべきである。従って、上記の状況は早急に改善される必要がある。

個人情報保護条例、情報セキュリティポリシーの策定、情報セキュリティ監査の実施は、本来各自治体の意思によって行われるべきものであり、この状況が総務省が行う指導の不足に由来するものか否かは判断できないが、結果として、総務省の指導は奏功していないと評せざるを得ない。

調査事項1について

以上の検討結果に照らし、「所要の措置」第1は、個人情報保護法及び行政機関の保有する個人情報保護法によって満たされたといえることができるが、「所要の措置」第2の、「住基法改正によるさらなる個人情報の保護」は未だ行われていない。また、「所要の措置」第3の指導は更に充実される必要がある。よって、全体として附則第1条2項の「所要の措置」が講じられているとは認められない。

従って、個人情報保護法及び行政機関個人情報保護法による個人情報の保護は、少なくとも住基法を改正した第145回国会が想定した程度に至っていない。

調査事項2について

個人情報保護法及び行政機関個人情報保護法は、自己情報コントロール権を実質的に保障するものと評価できる。しかし、地方公共団体の中には、本人確認情報の開示、訂正、追加、削除、利用停止請求、本人確認情報の提供、利用状況の開示請求に係る条例・規則を制定していないものがある。従って、地方公共団体に対しても個人情報保護法、行政機関個人情報保護法同様の水準で自己情報コントロール権が実質的に保障されたとは認められない。それゆえ、住民の自己情報コントロール権が保障されているとは言い難い。

1. 上記第1、個人情報保護法・行政機関個人情報保護法は「求められる水準」にあるか、の(3)記載のとおり、個人情報保護法及び行政機関個人情報保護法は、自己情報コントロール権を実質的に保障するものと評価できる。
2. なお、住基ネットシステムに係る住民の自己情報コントロール権の保障に関して問題になるのは、住民の
 - (1) 本人確認情報を保有する機関及びその他官民を含む全ての本人確認情報保有者(以下「本人確認情報保有者」という。)に対する、本人確認情報の開示、訂正、追加、削除、利用停止請求
 - (2) 本人確認情報を提供する都道府県知事、指定情報処理機関、提供を受けた機関等本人確認情報保有者に対する、本人確認情報の提供及び利用状況の開示請求である。
3. 前項(1)「本人確認情報保有者に対する、本人確認情報の開示、訂正、追加、削除、利用停止請求」について
 - (1) 本人確認情報の開示請求手続は
 - 1) 都道府県知事、指定情報処理機関に対するものは住基法第30条の37第2項が規定している。
 - 2) 国の行政機関等に対するものについては、行政機関個人情報保護法第12条ないし26条、行政機関の保有する情報の公開に関する法律(情報公開法)が規定している。
 - 3) 地方公共団体に対するものについては、条例・規則により規定されるが、その規定状況は、平成15年4月1日現在、2480団体(全制定団体数:都道府県及び市区町村2828団体に占める割合97・4%)である。
 - 4) 民間に対するものについては、個人情報保護法第25条に規定されている。
 - (2) 本人確認情報の訂正、追加又は削除請求等の手続について
 - 1) 住基法第30条の40に都道府県知事、指定情報処理機関に対する申出手続が規定されているだけで、都道府県知事、指定情報処理機関が直接これに応じる権限は住基法上規定されていない。しかし、訂正、追加又は削除の申出があったときは、その旨が関係市町村に通知され、通知を受けた市町村は住民票の記載の訂正の要否等を遅滞なく調査して、一定の場合には訂正、追加又は削除を行うことが適当であるとされている(「住民基本台帳事務処理要領について」第6-5-(2)イ、オ)。市町村長は、住民基本台帳の正確性を維持すべき義務を負っており、指定情報処理機関が誤りの記載を知ったときは、委任都道府県知事に通報し(住基法第30条の11第5項)、都道府県知事は市町村長に通報し(住基法第12条の3)、市町村長は、届出、職権により訂正、追加又は削除を行う手順が備えられている。
 - 2) 国の行政機関等に対するものについては、行政機関個人情報保護法第27条ないし35条、利用停止請求については同法第36条ないし41条に規定されている。

3) 地方公共団体に対するものについては、地方公共団体の条例に規定されるが、平成15年4月1日現在、訂正の請求等を規定しているのは2453団体(全制定団体数に占める割合96.3%)、削除の請求等を規定しているのは2276団体(同89.4%)、利用中止の請求等を定めているのは1383団体(同54.3%)である注25。4) 民間に対する訂正、追加、削除及び利用停止請求については、個人情報保護法第26条ないし第27条に規定されている。

4. 上記2(2)「本人確認情報を提供する都道府県知事、指定情報処理機関及び市区町村並びに提供を受けた機関等本人確認情報保有者団体、民間に対する、本人確認情報の提供及び利用状況の開示請求」について

(1) 都道府県知事に対しては、本人確認情報の提供又は利用の状況に係る情報(提供先、検索元、提供年月日、利用目的等)の開示請求を行うことができる注26。都道府県知事は、これに備えるため、国の機関等、区域内の市町村の執行機関等若しくは当該都道府県の執行機関(都道府県知事を除く)に対し本人確認情報の提供を行った場合又は本人確認情報を利用した場合は、個人ごとの本人確認情報の提供又は利用の状況に係る情報を必要な期間保存する。

指定情報処理機関に住基法にもとづく事務を委任した都道府県知事は、指定情報処理機関に対し、指定情報処理機関が国の機関等又は区域内の市町村の執行機関等に対し本人確認情報の提供を行った場合における個人ごとの本人確認情報の提供の状況について報告を求め、当該提供の状況に係る情報を保存しており、指定情報処理機関の提供状況についての開示請求に応じる。

(2) 国の行政機関、地方公共団体、民間に対するものは、上記3(1)2)から4)までの記載と同様である。

5. 以上の検討に照らし、個人情報保護法及び行政機関個人情報保護法は、自己情報コントロール権を実質的に保障するものと評価できる。しかし、地方公共団体については、未だ本人確認情報の開示、訂正、追加、削除、利用停止請求、本人確認情報の提供、利用状況の開示請求に係る条例・規則を制定していない地方公共団体が存在する。従って、地方公共団体に対しても個人情報保護法、行政機関個人情報保護法同様の水準で自己情報コントロール権が実質的に保障されたとは認められない。

6 それゆえ、住民の自己情報コントロール権が保障されているとは言い難い。

調査事項3

国立市は、住基法にもとづき通知・提供した国立市民の個人情報に対して、開示、訂正、削除及び利用停止を求める権限を有しない。また、国立市が、住基ネットで拡散する個人情報が、どこでどのように取得、管理、消去されるのかを具体的に把握することは困難であって、そのような意味において国立市の住民情報コントロール権が保障されているとは言い難い。

1. 国立市の住民情報コントロール権とは、国立市が住基法にもとづき通知・提供した国立市民の個人情報に対して、開示、訂正、削除及び利用停止を求める権限、また、国立市が、住基ネットで拡散する個人情報が、どこでどのように取得、管理、消去されるのかを具体的に把握できる権限であると解される。
2. 国立市が住基法にもとづき通知・提供した国立市民の個人情報について、国立市が、直接その開示、訂正、削除及び利用停止を求める法律及び条例・規則は存在しない。
3. また、国立市が、住民の個人情報の管理者として、住基法にもとづいて通知・提供された個人情報が、どこでどのように取得、管理、消去されるのかを、直接、具体的に把握することを可能とする明文の定めを置く法律はなく、総務省告示に委ねられている。

すなわち、国立市長は、国の機関等及びその都道府県の執行機関、東京都内の市区町村の執行機関等に対しては都道府県知事(指定情報処理機関が本人確認情報の提供を行った場合は、都道府県知事及び指定情報処理機関)を経由して、道府県知事、都外の市区町村の執行機関に対しては直接、提供された国立市住民の本人確認情報の適切な管理のための措置の実施状況について報告を求め、本人確認情報の適切な管理のための措置の実施について要請を行うことができる注27。

しかし、告示によってこのような制度が設けられても、報告、要請の相手方が、個人情報保護に関する条例等のルールを持ち、適切な運用設計にもとづく規則・規程等によって実際の運用がなされ、かつ、その運用の現実を監査によって把握していなければ、的確な報告はもちろん、要請を受けてもこれを実現することは困難であって、制度はその目的を発揮できない。

ところで、調査事項1で検討したとおり、現時点においては、附則第1条第2項の「所要の措置」はその全てが取られているとはいえ、第145回国会が想定した住基ネットシステムの実施の前提としての個人情報保護の体制は整備されていない。平成15年10月1日現在、個人情報保護に関する条例を制定しているのは、上記のとおり全3204団体中2458団体(全団体の76.7%)。4月1日現在では、規則・規程等により個人情報保護対策を講じている団体を併せても2828団体(全団体の86.7%)である。個人情報保護を支える情報セキュリティ対策の基本となる情報セキュリティポリシーの制定団体は、都道府県では93.6パーセントに至っているが、市町村は、49.6%である注28。また、個人情報保護のためのセキュリティ対策の運用状況を認識するために不可欠のセキュリティ監査の実施状況を見ると、上記のとおり、平成15年4月1日時点で、内部監査によるものも含め、11都道府県(全都道府県の15%)、284市町村(全市町村の9%)である。

このような状況のもとにおいては、国立市が、上記告示による権限を行使して、住基ネットで拡散する個人情報が、どこでどのように取得、管理、消去されるのかを具体的に把握することは困難である。

4. 従って、国立市の住民情報のコントロール権が保障されているとは認められない。

調査事項4について

比較衡量は不可能であり調査事項4には回答できない。

1. 住基ネットシステムが既に稼働している現在、調査事項4の比較衡量を行うには、その基準が明確化され、かつ、メリット、デメリットが比較衡量を可能とする共通要素に分解されて把握できなければならない注29。
しかし、住基ネットシステムは、LGWAN、霞ヶ関WAN、住基カード、公的個人認証制度を利用した電子国家、電子自治体を実現する共通インフラとして位置づけられており、その実現によるメリットは極めて多様であり、現時点では比較衡量が可能な形で把握できない。
他方、住基ネットシステムのデメリットとしてあげられる事項も極めて多様である。仮に、個人情報保護やセキュリティ経費に限っても現時点では評価できない。附則第1条第2項の「所要の措置」は未だ実現されておらず、第145回国会が想定した個人情報保護の施策は今後委ねられている。統一的な基準にもとづく住基ネットシステム及びこれに接続される全国の市町村の庁内システム、既存住基、個人情報の提供される別表の機関・団体のシステムなどを含めた全体的なリスクアセスメントは行われていない。従って、国立市が、住基ネットシステム及びこれに接続されたネットワーク、上記各機関及び団体にあるリスクを把握することは困難である。
今後国立市が構築すべき個人情報保護、住基ネットシステム及び既存住基システム、庁内LANを含むシステムについて採用すべきリスクレベルも確定されていない。このような状況では対策経費も積算できない。
このようなもとは、両者のメリット、デメリットを比較衡量可能な形で把握できず、調査事項4の比較衡量を行うべき基準も定立できない。
2. 従って、比較衡量は不可能であり、調査事項4には回答できない。

調査事項5について

ストーカー、ドメスティックバイオレンスの被害者を支援する目的で制定・施行した「国立市ストーカー行為等の被害者支援に関する住民基本台帳事務取扱要綱」に沿った被害者支援に障害とならない制度・運用が確保されているとは言い難い。

1. そもそも、住民基本台帳、戸籍の附票の閲覧、交付請求は自由になしうるのが住基法の原則である。すなわち、
 - (1) 何人でも市町村長に対し、住民基本台帳の一部の写しの閲覧を請求し(住基法第11条第1項)、自己又は自己と同一の世帯に属する者以外のものであって当該市町村が備える住民基本台帳に記録されている者に係る住民票の写しで住基法第7条第13号に掲げる事項の記載を省略したもの又は住民票記載事項証明書で同条第1号から第12号まで及び第14号に掲げる事項に関するものの交付を請求し(住基法第12条第2項)、当該市町村が備える戸籍の附票の写しの交付を請求することができる(住基法第20条第1項)。
 - (2) また、住民基本台帳に記録されている者は、その者が記録されている住民基本台帳を備える市町村の市町村長に対し、自己又は自己と同一の世帯に属する者に係る住民票の写し又は住民票記載事項証明書の交付を(住基法第12条第1項)、その者が記録されている住民基本台帳を備える市町村以外の市町村長に対し、自己又は自己と同一の世帯に属する者に係る住民票の写しで住基法第7条第5号、第9号から第12号まで及び第14号に掲げる事項の記載を省略したものの交付を請求することができる(住基法第12条の2第1項)のものであって、市町村長は、住民基本台帳の一部の写しの閲覧請求に対しては「不当な目的によることが明らかなき又は住民基本台帳の一部の写しの閲覧により知り得た事項を不当な目的に使用されるおそれがあることその他の当該請求を拒むに足りる相当な理由があると認めるとき」(住基法第11条第3項)、その他の請求に対しては、「不当な目的によることが明らかなき」に限り、これを拒むことができるというのが住基法の原則である(住基法第12条第5項、第12条の2第6項、第20条第2項)。
2. 実務では、具体的な救済の必要なケースに対応して様々な努力が積み重ねられており、「国立市ストーカー行為等の被害者支援に関する住民基本台帳事務取扱要綱」においては、国立市長が、「ストーカー行為等の規制等に関する法律」に規定するストーカー行為等の被害者及び、「配偶者からの暴力の防止及び被害者の保護に関する法律」に規定する被害者から申出を受けたときは直ちに下記支援項目の(1)の措置を取り、次に、警視総監若しくは道府県警察本部長又は警察署長にストーカー行為等の被害者に関する照会書により照会する等の調査を講じた上、支援の開始の要件が満たされたときに、被害者、被害者と同一世帯に属する者及び市内居住の被害者の親族等のうち被害者の指定する者を「支援対象者」として以下の3項目の支援を行うものである。
 - (1) 支援対象者の住民票の写し等若しくは戸籍の附票の交付請求又は住民基本台帳の一部の写し(以下「閲覧リスト」という。)の閲覧請求について、請求者の本人確認を行うとともに、請求事由を明らかにする関係文書等の提示を求め、厳格な審査を行うこと。
 - (2) 加害者又は前号による請求者の本人確認ができない者若しくは正当な請求事由が明らかでない者からの住民票の写し等若しくは戸籍の附票の交付請求又は閲覧リストの閲覧請求については、その請求に応じないこと。
 - (3) 閲覧リストから支援対象者に係る記載事項の削除を行うこと。
3. 国立市の要綱制定は、ストーカーやドメスティックバイオレンスの被害が生命、身体の危険という重大なものであること、加害者に閲覧リストに記載された個人情報を了知されるだけで危険が及ぶ可能性があること、被害者の脅威は、加害者による住基法、個人情報保護法、行政機関個人情報保護法の違反行為その他不正アクセス禁止法、刑法犯を含む違法行為によってもたらされる可能性があることなどに鑑み、被害者保護の目的達成には、住基法の原則公開の原則を逆転させ、閲覧リストから支援対象者に係る記載事項を削除して、加害者による情報取得の手段を遮断させるまでの手段を講じることが不可欠であるとの認識にもとづいている。
4. 住基ネットシステムの実施によって、自己又は自己と同一の世帯に属する者に係る住民票の写しで住基法第7条第5号、第9号から第12条まで及び第14号に掲げる事項の記載を省略したものの交付を請求することが容易となり、本人確認情報は広範囲に流通する。このこと自体によって具体的な脅威が増大する事例を想定することは困難であるが、住基ネットシステムの運用面においては、例えば住民票コードの世帯単位での送付によって、世帯主である加害者に住民票コードを知られたり、加害者と別居して身の安全を図っていたドメスティックバイオレンスの被害者が加害者との接触を余儀なくされた事例が報じられている。
ストーカー・ドメスティックバイオレンスから被害者を保護するには、住基法第11条第3項、第12条第5項、第12条の2第6項、第20条第2項の運用に特段の措置を講じる必要があり、第156回国会においても片山総務大臣(当時)は検討の必要があることを答弁注30し、総務省も加害者を含む第三者による閲覧や写しの交付を市区町村が制限するための基準を盛り込んだ指針の検討を開始した旨が報じられている注31。また、

複数の自治体において住基ネットシステムの第二次稼働に伴い、閲覧用台帳から支援対象者の情報を削除するなどの対策が講じられている注32。

5. そこで、国立市長は、住基ネットシステムの実施にあっても、

- (1) 住基ネットの制度・運用について、送信情報からストーカー等被害者の本人確認情報を除外すること。
- (2) 上記の外、ストーカー等被害者と同一世帯に属する者及び同一市区町村内に住民登録を有する親族のうち被害者の指定する者も除外すること。

が必要であると認識している注33。6 しかしながら、住基ネットシステム実施後、上記要綱に匹敵する措置は講じられていない。また、国立市長の主張する上記2つの措置は未だ講じられておらず、上記総務省における検討結果も明らかにされていない。従って、ストーカー・ドメスティックバイオレンスの被害者を支援する目的で制定・施行した「国立市ストーカー行為等の被害者支援に関する住民基本台帳事務取扱要綱」に沿った被害者支援に障害とならない制度・運用が確保されているとは言い難い。

調査事項6、7及び8について

住基ネットシステムを利用する国の機関等及び公的個人認証制度における個人情報の保護の水準は、個人情報保護法及び行政機関個人情報保護法によって第145回国会の想定した水準に至っている。

個人情報の漏えいを防止するセキュリティ対策及び公的個人認証制度における個人情報の保護及びセキュリティ対策は、法律上規定されているが、セキュリティ対策を必要とするという基本的な思想を示すに止まり、セキュリティ対策が十分措置されているとは言い難い。

1. 住基ネットシステムを利用する国の機関等及び公的個人認証制度における個人情報の保護の水準は、個人情報保護法及び行政機関個人情報保護法によって第145回国会の想定した水準に至っていることについては、既に第1で論じた。

2. そこで、住基ネットシステム及び公的個人認証制度におけるセキュリティ対策について検討する。

(1) 住基ネットシステム及び公的個人認証は、行政手続のオンライン化を可能とする基礎的インフラである。住基ネットシステムと公的個人認証は、行政手続等における情報通信の技術の利用に関する法律(以下「行政手続オンライン化法」という)、「行政手続等における情報通信の技術の利用に関する法律の施行に伴う関係法律の整備等に関する法律」(以下「整備法」という)とともに機能することによって、行政手続の大規模なオンライン化を実現するものである。

(2) このオンライン化は、霞ヶ関WAN、LGWANで結ばれた行政機関と、国民の間をインターネットで結び、住基ネットシステムによる居住関係の確認、公的個人認証局による本人確認によって、約52000の行政手続をオンライン化するものであって、これにより、例えば事業所における雇用保険被保険者取得・喪失届(年間約1000万件)、パスポートの交付申請(年間約580万件)、戸籍謄抄本の交付申請(年間約3600万件)だけでも、合計約5180万件の手続がオンライン化されることになる。

(3) その結果、論理的には、対象とされる全ての行政手続の安全と信頼及び法的、経済的、政治的リスクが、霞ヶ関WAN、LGWAN、住基ネットシステム、インターネットのセキュリティ対策に依存することになる。

(4) これに対するセキュリティ対策の規定は以下のとおりである。

住基ネットシステムのセキュリティについては、住基法第30条の29は、当該都道府県知事又は指定情報処理機関が本人確認情報の電子計算機処理等を行うにあたり、また、本人確認情報の電子計算機処理等の委託を受けた者が受託した業務を行う場合に「本人確認情報の漏えい、滅失及びき損の防止その他の当該本人確認情報の適切な管理のために必要な措置を講じなければならない。」と規定している。

公的個人認証のセキュリティについては、電子署名に係る地方公共団体の認証業務に関する法律(以下「公的個人認証法」という)第20条が、都道府県知事及び受託事業者に対し、発行記録、失効情報及び失効情報ファイル(以下「認証業務情報」という)の電子計算機処理等の事務を行うにあたり「当該認証業務情報の漏えい、滅失及びき損の防止その他の当該認証業務情報の適切な管理のために必要な措置」を講じることを義務づけている。

また、個人情報のセキュリティについては、民間部門については、個人情報保護法第20条が個人情報取扱事業者に「個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置」を、国の行政機関等については、行政機関個人情報保護法第6条が行政機関の長に「漏えい、滅失又はき損の防止その他の個人情報の適切な管理のために必要な措置」を講じることを義務づけている。

なお、人による秘密の漏えい等については、国家公務員法、地方公務員法をはじめとする住基法その他の守秘義務規定が対応している。また、外部からの不正アクセスへの対処については、不正アクセス対策法が、ウイルスなどの不正プログラムの利用などについては、不正プログラムの作成、保管等を処罰する刑法改正が予定されており、コンピュータへの不正な働きかけによる実害の発生については、刑法が対応している。

(5) しかしながら、このような法体制が、上記の行政手続のオンライン化に適応したものと考えることは困難である。

特に、上記ネットワークは、住基ネットシステムだけをとりあっても約3300の自治体、指定情報処理機関、国等の機関と複数の責任主体が存在し、これにインターネットを経由する個人、法人という責任主体が存在することになる。この無数ともいべき独立した責任主体が、それぞれのマネジメントによって、上記ネットワークに加わりながら、ネットワーク全体の安全性、信頼性、効率性を確保するには、上記各法の安全対策を運用するための全体を統一したセキュリティポリシーが必要である。特に国家規模のネットワークのセキュリティ対策は、OECDセキュリティ新ガイドラインが主張するとおり、セキュリティが文化と呼べるまでに成熟した共通認識として全てのネットワーク参加者に把握され、これらが、統一的な方針にもとづいて、常に化する脅威、ぜい弱性及びリスクを的確に把握して特定のリスクレベルを実現する計画をたて、これを実際に実現し、状況の把握と評価のためのセキュリティ監査が行われ、監査結果をふまえた新たな計画、実施、監査、計画といういわゆるPDCAサイクルが現実に展開されることが必要であり、その担い手としての人の教育、人、金、物、技術の供給が現実に行われることが必要である。従って、セキュリティ法制は、これらの全てにわたる具体的なものであり、かつ、統一的な責任と思想のもとで全体を包括する対策が講じられる必要がある注34。

しかしながら、現時点では、対応する法律は、高度情報通信ネットワーク社会形成基本法(以下「IT基本法」という)第22条の「高度情報通信ネットワーク社会の形成に関する施策の策定にあたっては、高度情報通信ネットワークの安全性及び信頼性の確保、個人情報の保護その他国民が高度情報通信ネットワークを安心して利用することができるようにするために必要な措置が講じられなければならない。」との規定があるに止まる。

内閣官房の情報セキュリティ対策推進室は、平成12年7月情報セキュリティポリシーに関するガイドラインを発表し、平成13年10月には電子政府の情報セキュリティ確保のためのアクションプランを決定して電子国家実現に向け、地方自治体との連携をも配慮しつつ各種の施策をとりまとめ

ているが、調整機能が中心で、自身の施策としてこれらを推進する陣容としては不十分である。

また、普遍性をもって合理的なセキュリティ対策を実現するISMSによるセキュリティマネジメントの取り組みや調達の水準を確保するISO15408、ST、広く情報資産のセキュリティマネジメントの現実を認識・評価・改善するための情報セキュリティ監査制度は、いずれも官民の全体に採用されつつあるが、未だ十分ではない。

3. 「安全対策」の内容を示さず、運用の法制も枠組みも体制もなく、これを行うことを義務づけるだけの上記の法制は、セキュリティ対策を必要とするという基本的な思想を示すに止まり、セキュリティ対策が十分措置されているとは言いがたい。

以上

脚注

注1 第145回国会衆議院地方行政委員会1999年6月8日において、共同提案者を代表した宮路和明委員(自由民主党)は、共同提案にかかる附則第1条第2項の「所要の措置」の内容を以下のとおり説明している(同委員会議事録)。

「次に、この「速やかに、所要の措置を講ずるものとする。」という「所要の措置」であります。これは、私ども、政府にいわばそういう義務を課してあるという規定を盛り込ませていただいたということでもありますから、政府にこれからどういったことをやっていただくかということは今後の政府の検討にまたなければならぬわけでありまして、我々、議員修正を提案する者として期待しておりますことはどうということかということと申し上げさせていただきます。…一つは、やはり政府においても昨年、高度情報通信社会推進に向けた基本方針というのを総理が本部長をしておられるところで決定をして、これからいろいろなことをやっていくんだ、プライバシーの保護の問題、こういうことも既にこの中で決めておられるわけですね。そういうぐあいに、プライバシー保護についての法制を整備していかなきゃならないというのは喫緊の課題になりつつあるということは、我々も、この場における論議を踏まえてもよく理解できることであるわけでありまして、そうしたプライバシー保護に関する法制をやはり整備していくということが一つ。それから、それにあわせて、今の住民基本台帳法それ自体といえども、例えばカードの問題なんかについてもいろいろな議論がありました。そういうところにおいて、これからさらに高いプライバシー保護のための手だてを将来講じていくとするならば、この住民基本台帳法自体の世界においても、それにやはり準拠した、よりレベルの高い個人情報保護のシステムというものもあってしかるべきではないかというふうに思われるわけでありまして、そこところもやはり一つはやっていただきたい。それからまた、これは条例でもって市町村あるいは都道府県が、このネットワークシステム、運営をしていく主体になるわけでありまして、そこで、そうした地方自治体においてちゃんと、プライバシーの保護に十分配慮した措置をものも講じていってもらわなきゃならない。システムにおいてもそうですし、あるいはまた条例を定める場合によってもそうだというふうに思うわけでありまして、そういったところも具体的に検討して、そして自治省の方でしっかりと地方自治体に指導していってもらいたい。こういったものもろものが頭の中にごさいます、そして所要の措置というふうに規定させていただくことにした、こういうこととございます。」

注2 野田毅自治大臣は、平成11年6月10日、第145回国会衆議院地方行政委員会議員修正を提案した公明党・改革クラブ富田重之委員の「自治省として、所要の措置について現在どのような認識でいらっしゃるか」との質問に対して、「附則第一条第二項の「所要の措置」とは、第一に、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、第二に、第一のシステムの整備状況を踏まえ、住民基本台帳法におけるさらなる個人情報保護措置を講ずるため、所要の法改正等を図ること、第三に、地方公共団体が適切に住民基本台帳ネットワークシステムを運用することができるよう、自治省として個人情報保護に係る指導を十分に行うことなどを示すものと認識しております。」と答弁して、自治省としても個人情報保護法の制定、個人情報保護のための住民基本台帳法のさらなる改正、地方公共団体に対する適切な指導の三点を行う認識であることを明らかにしている(同委員会議事録)。

注3 「所要の措置」については、平成11年6月10日の衆議委員地方行政委員会における小淵総理の「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」との表現から、官民を対象とする個人情報保護法の制定に注目が集まっている。しかし、同日の委員会では、野田毅自治大臣が、「所要の措置」は何かとの質問に対し、本文の三つの施策であることを明確に答弁しており、同委員会において同席していた小淵総理もこれを否定していないから、小淵総理の言う「法整備を含むシステム」とは、「所要の措置」第1とは同じ表現であっても、野田国務大臣の答弁した三つの内容を指すものであることに留意する必要がある。

注4 もともと同部会の設置は、高度情報通信社会推進に向けた基本方針(平成10年11月9日本部決定)のアクション・プラン(平成11年4月16日本部決定)で予定されていたが、同会議第一回においては、特に「政府としても資料8の小淵総理の国会答弁にございますように、「民間部門をも対象とした個人情報保護に関する法整備を含めたシステムを速やかに整えること」としてあります。その際は、先程の3党の合意も念頭に置いて取り組んでまいりたいと考えております。委員の皆様方におかれましてこの点を御理解いただき、御協力をお願いします。」との説明がなされ、同部会では、第145回国会における三党派合意、小淵総理の答弁を踏まえ、「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」を検討することが求められた。

注5 平成11年11月高度情報通信社会推進本部個人情報保護検討部会「我が国における個人情報保護システムの在り方について(中間報告)」

注6 情報通信技術(IT)戦略本部個人情報保護法制化専門委員会「個人情報保護基本法制に関する大綱」(平成12年10月11日)

注7 提出時の法律案及び審議の経過は、衆議院のホームページ「議案」第154回国会、第155回国会の内閣法(内閣提出法律案)の項にある。

注8 田島泰彦・三宅弘編「解説&批判個人情報保護法・プライバシーと表現の自由を守るために」(明石書店)41頁以下。

注9 なお、田島教授は、「所要の措置」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」であるとし、その具体的な内容を「官に対しては民間に対するより厳格な規制がなされるべきこと、市民による自己情報のコントロール権を徹底した仕組みが構築されるべきこと、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・分野での厳格な規制、官に対して厳格な規制を及ぼしうることなどが必要である」とする(田島泰彦・三宅弘編「解説&批判個人情報保護法・プライバシーと表現の自由を守るために」(明石書店)42頁)。しかし、本文に述べる理由に照らし「所要の措置」について第145回国会がそのような具体的内容まで想定していたと認めることは困難である。附則1条2項の「所要の措置」がそのような内容を有するとの解釈が正当性を獲得するには、立法者意思に匹敵する正統性によって支えられる必要がある。

注10 小淵総理は、平成11年6月10日、衆議院地方行政委員会において、住民基本台帳ネットワークシステムの導入に当たり、個人情報保護方策としてはもともと住基法の改正で足りると考えていたが、改正住基法の修正審議にあたり、この認識を改め、住基法を含む当時の個人情報保護を上回る個人情報保護法制の整備を含むシステムが必要であると考えに至ったとし、その経緯を以下のとおり説明している。「今回の改正法案におきましては、民間部門を本人確認情報の提供先とせず、本人確認情報の厳重な保護措置を講じ、さらに住民票コードの民間利用を禁止していることから、住民基本台帳ネットワークシステムを導入する前提として包括的な個人情報保護法の制定を要するものでないとの認識を持っており、その旨、去る四月十三日の本会議で述べたところであります。が、しかしながら、改正法案の審議の中で、担当大臣等により、現時点で可能な限り個人情報保護措置を講ずるなどの説明を繰り返し行ったものの、なおプライバシーの保護に対する漠然とした不安、懸念は残っているとの指摘があったと承知をいたしております。一方、急速な情報化社会の進展の中で、民間部門を含めた個人情報保護法などの整備が必要であるとの御議論もあったところでございます。こうした状況の中で、住民基本台帳ネットワークシステムの実施に当たりましては、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の認識に至ったところでございまして、先ほど申し上げておりますように、個人の情報保護法というものになりますか、これから政府といたしましては、個人の情報保護というものにつきましては十分認識をして対処していきたいと考えております。」(同委員会議事録)

注11 園部逸夫編「個人情報保護法の解説」(株式会社ぎょうせい)66頁

注12 園部逸夫編「個人情報保護法の解説」(株式会社ぎょうせい)44頁

注13 第156回国会衆議院個人情報の保護に関する特別委員会平成15年4月21日における堀部政男参考人の意見(同委員会議事録)

注14 付帯決議の内容は以下のとおりである。

1. 個人情報ファイルの保有等に関する事前通知並びに個人情報ファイル簿の作成及び公用に係る義務規定の適用除外の解釈にあたっては、個人の権利利益の保護の観点から十分に配慮すること。
2. 保有個人情報の目的外利用及び提供が所定の要件に該当するか否かの判断は慎重かつ客観的に行うこと。
3. 利用目的が異なる2以上の個人情報ファイルを電子計算機を用いて照合し、又は結合する場合には、個人の権利利益を侵害しないよう十分留意すること。
4. センシティブ情報の取得又は保有にあたっては利用目的を厳密に特定するとともに、可能な限り法律その他の法令等によって取得根拠を明確にし、その利用、提供及び安全確保に特段の配慮を加えること。
5. 個人情報の取得にあたっては、防衛庁リスト問題等の教訓を踏まえ、適法かつ適正な方法により行うこと。

注15 長谷川博章「個人情報の保護に関する法律の概要」法律のひろば56巻9号7頁

注16 園部逸夫編「個人情報保護法の解説」(株式会社ぎょうせい)130頁

注21 総務省報道資料平成15年11月7日「地方公共団体における情報セキュリティポリシー(情報セキュリティ対策に関する基本方針)等の策定状況」
総務省自治行政局地域情報政策室

注22 総務省自治行政局地域情報政策室「地方自治情報管理概要」11頁(平成15年10月)

注23 総務省自治行政局地域情報政策室「地方自治情報管理概要」29頁(平成15年10月)

注24 総務省報道資料平成15年11月7日「地方公共団体における情報セキュリティポリシー(情報セキュリティ対策に関する基本方針)等の策定状況」
総務省自治行政局地域情報政策室

注25 総務省自治行政局地域情報政策室「地方自治情報管理概要」29頁(平成15年10月)

注26 総務省告示第334号「電気通信回線を通じた送信また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」(平成14年6月10日、同改正平成15年9月29日総務省告示第601号)

注27 総務省告示第334号「電気通信回線を通じた送信また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」(平成14年6月10日、同改正平成15年9月29日総務省告示第601号)第6、8(1)エ、同(2)イ、同(3)及び同(4)イ。

注28 総務省報道資料平成15年11月7日「地方公共団体における情報セキュリティポリシー(情報セキュリティ対策に関する基本方針)等の策定状況」
総務省自治行政局地域情報政策室

注29 住民基本台帳ネットワークシステム本格稼働前の平成13年11月から12月、日本弁護士連合会が実施した「住民基本台帳ネットワークシステムに関する地方自治体アンケート」によると、「住基ネットの出費は費用対効果の観点から合理的ですか」という問に対して、回答をよせた1490自治体の回答割合は、「合理的」が7%であるのに対して、36%の自治体が「不合理」、「どちらともいえない」51%、その他・無回答が5.9%であって、当時の、回答を寄せた自治体職員の認識の上では、デメリットが上回っている。

注30 第156回国会個人情報の保護に関する特別委員会議事録第4号(平成15年5月14日)

注31 平成15年9月1日付読売新聞

注32 国立市のみならず、江戸川区、大田区、桶川市、小金井市、国分寺市、新宿区、杉並区、調布市、練馬区、八王子市、羽村市、三鷹市、大和市ほか。

注33 国立市長の内閣総理大臣及び総務大臣宛平成15年9月19日付「ストーカー行為等及び家庭内暴力(DV)の被害者支援に係る住民基本台帳ネットワークシステムの制度・運用について(要望)」(国市民発第106号)

注34 日弁連はこの視点からセキュリティ基本法案を提示している。また、経済産業省の情報セキュリティ総合戦略は、同様の考え方に立ち、強化された内閣機能によって、高信頼性社会の実現を目指すとしている。

用語解説: [行政手続オンライン化法](#) [情報公開・個人情報保護審査会設置法](#) [IT基本法](#) [公的個人認
証法](#) [行政機関個人情報保護法](#)

※「用語解説」内のリンクは、ウェブリオが運営する辞書サイトの解説ページ(別ウィンドウ)に移動します。

総務部 市民課 市民係

電話:042-576-2111(内線 131,132) ファクス:042-576-0264

[メールでのお問い合わせは専用フォームをご利用ください。](#)

現在のページ: [ホーム](#) > [くらしの情報](#) > [証明・登録](#) > [住基ネットワークシステムについて](#) > [住民基本台帳ネットワークシステム](#) > [住民基本台帳ネットワークシステムについて](#) > [住基ネット調査研究事業](#) > [情報システム面](#)

情報システム面

更新日 平成22年7月29日

平成15年12月26日

大木 栄二郎

国立市住民基本台帳ネットワークシステム情報セキュリティ調査 報告書

調査の目的

国立市の住民基本台帳ネットワークシステム(以下「住基ネットシステム」という。)にかかわる情報セキュリティの現状を明らかにし、住基ネットシステムの再稼働に向けて、情報セキュリティ面に対処すべき項目とその対応の方向を明らかにする。

調査方法

関連の資料調査と関係者のインタビューをもとに調査する。ペネトレーションテスト等のシステムやネットワークの技術的な検証は行わない。

採用する枠組み

情報セキュリティマネジメントのベストプラクティスや、地方公共団体における情報セキュリティマネジメントに関する下記のガイド等を調査の基本枠組みとする。

- JIS-X-5080 情報セキュリティマネジメントの実践のための規範
- 地方公共団体における情報セキュリティポリシーに関するガイドライン
- 総務省告示第三百三十四号 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
- 住基ネットシステム及びそれに接続している既設ネットワークに関する調査票による点検結果
これらの規範やガイド類の内容を、(1)体制・規程の整備、(2)物理的対策、(3)技術的対策、(4)運用面の対策の四つに分類し、調査結果をこの四つの分類ごとに整理する。

調査対象と調査方法

調査対象を三つに分類し、それぞれの情報セキュリティマネジメントの現状を基本の枠組みに基づいて調査し評価する。

- 調査対象1: 国立市住民基本台帳システム(以下「住基システム」という。)
庁内LAN
関連資料調査、関係者インタビュー、実地調査で調べる
- 調査対象2: 国立市住基ネットシステム
関連資料調査、関係者インタビュー、実地調査で調べる
- 調査対象3.: 住基ネットシステム市外部分
公表資料からまとめる。下記を資料として用いる。
「住民基本台帳ネットワークシステム及びそれに接続している既設ネットワークに関する調査票による点検結果(平成15年5月12日)」

報告内容 現状の課題 調査対象1について

体制・規程の整備

- 情報セキュリティ管理規程が策定されておらず、誰がどんな責任を持っているのかが明確でない。職員は国立市個人情報保護条例などでセキュリティの必要性は認識しているが、具体的にどの情報についてはどのような手段でどの程度までのセキュリティを確保するかについて知識に乏しく共通の理解がない。
- 住民基本台帳情報(以下「住基情報」という。)のセキュリティ対策について、実現すべき管理レベルを定める責任者が明確でない。したがって、現状の住基システムのセキュリティ機能や運用が十分であるかを判断する基準がなく、運用担当者が守るべき手順やルールも明確ではない。
- 情報の重要度による区分がされておらず、機密性の高い住民情報が危険な状態に置かれている。

物理的対策

- マシンルームやコンソール卓の設置場所などの重要機能設置場所が容易に識別されるなど、物理的対策が適切でない。
- 重要機能設置場所に、いつ誰が入室したかをさかのぼって検証できる状態になっていない。
- 住基情報のバックアップテープが、万一の場合に復元に利用できない可能性が高い。早急にバックアップテープの遠隔地保管を検討する必要がある。

技術的対策

- 住基システムが持つべきセキュリティ機能の要件が明確にされていない。
- ベンダーのパッケージをカスタマイズして使用しているが、そのパッケージのセキュリティ機能が十分であるのか評価できていない。
- 住基システムの根幹にある行政基本システムにおける利用者の識別・認証は機能として不十分である。

運用面の対策

- ホストコンピュータのセキュリティにかかわる運用マニュアルや、情報機器及び記憶媒体の管理手順、ネットワークのセキュリティ運用手順などが策定されておらず、住基情報の安全確保が検証される手順が運用に組み込まれていない。
- 磁気テープなどの記憶媒体のどれに何が入っているかが台帳を用いて正確に把握・記録する運用にはなっていない。担当者の記憶に頼った運用になっており、何か起きた場合の対応が計画されていない。
- ネットワークの接続機器の設定が正しいかどうかの検証結果が残されておらず、セキュリティ上の問題がないかどうか把握できていない。
- ファイアウォール等の重要機器の運用状況を確認するプロセスが組み込まれていない。
- 既存住基システムと住基ネットシステムとはベースとなるネットワーク基盤を共有しているが、この部分の運用管理の基準が定められておらずドキュメントも十分ではない。
- 市民課の窓口の住基システムにアクセスする現場では、個人の識別と認証がほとんど形骸化しており、問題が起きた場合に誰がやったのかを追跡することは難しい。

報告内容 現状の課題 調査対象2について

体制・規程の整備

- 住基ネットシステムのセキュリティポリシー「国立市住民基本台帳ネットワークシステムセキュリティ管理規程」は策定されており、責任体制も明確に規定されている。
- しかし、国立市住基システムそのものにかかわるセキュリティ管理規程は策定されておらず、本人確認情報の部分についてだけセキュリティポリシーが存在する状態である。
- にもかかわらず、住基ネットシステムの一部を構成するゲートウェイサーバには、本人確認情報にとどまらず既存住基システムのほとんどの住基情

報が含まれている。すなわち、規程の定める範囲と、実際の住基ネットシステムの範囲とが一致していない。

- 住基ネットのセキュリティポリシーに記載された責任体制では、情報セキュリティの確保に必要な専門的知識の支援が十分ではなく、実務的に的確なリスク対応が図れるかどうか疑問が残る。実際的にはシステムの設計・開発の多くの部分が外部ベンダー依存になっているが、委託内容の検収時の検証がほとんどできていない。

物理的対策

- 事務スペースに設置され施錠管理されたキャビネットへの住基ネットシステムの収納は、それ自体は許容リスク範囲であると解釈できる。
- しかし、バックアップメディアの保管管理、さらにはメンテナンス時のベンダーの作業管理、執務時間外に及ぶメンテナンス時の監視などに多くの課題を抱えている。
- これらの運用に管理面での対策を加えなければ、物理的なセキュリティが確保できていないといえない。

技術的対策

- 住基ネットシステムの技術的なセキュリティ対策は、要求仕様が明確に定義されている。
- その要求仕様に基づいてベンダーに発注し設計開発されているため、技術的なセキュリティ機能の組み込みはなされていると考えられるが、検収時にこれらのセキュリティ機能を検証した記録は残されていない。
- 既存住基システムと住基ネットシステムの接続部分にあるゲートウェイサーバは、その取り扱い情報の種類から分類すると既存住基システムと同等である。しかしシステム構成では住基ネットシステムの一部として位置づけられ、管理責任も物理的な収納も住基ネットシステムとして取り扱われている。

運用面の対策

- 住民基本台帳ネットワークシステム基本設計概要書に定められた運用管理規程が策定されておらず、運用面からのセキュリティ対策が実施されているかどうかを検証できない。
- 個人情報格納された記憶媒体の管理規程がなく、どこにどれだけの個人情報が格納された媒体があるかも把握されていない。紛失してもわからない可能性が高い。
- 情報機器管理台帳はPCベースで作成されているが、情報機器管理規程は策定されておらず、セキュリティの確保には役立っていない。

報告内容 現状の課題 調査対象3について

体制・規程の整備

- 住基ネットのセキュリティ体制・規程等については概ね整いつつあるが、一割程度の団体が未整備の状況である。
- 国立市にはない「アクセス管理規程」「情報資産管理規程」「委託管理規程」などの具体的な規程を作成しすでに運用している団体が半数以上にのぼる。国立市も早急にこの面での規程類を整備していく必要がある。

物理的対策

- 重要機能室を設置している団体が9割程度にのぼり、重要機能室を設置していない団体についても概ね適切な管理がなされている。
- 端末機等を設置する事務室の不在時の施錠や入退室管理が約半数の団体で職員に周知され運用されている。

技術的対策

- 住基ネットシステムの技術的なセキュリティ対策は、要求仕様が明確に定義されている。

- 「担当職員がセキュリティ設定の内容を把握している」、及び「委託業者が行ったセキュリティに関する設定内容が適切か職員が確認している」につき、半数以上の自治体で周知され運用されている。

運用面の対策

- バックアップを定期的に行っている団体が8割以上、バックアップ媒体の別の場所への保存も6割以上の団体で実施されている。
- 既設ネットワークとコミュニケーションサーバ間のファイアウォール及び既設ネットワークとインターネットとの接続については、概ね適切な管理がなされているが、2割程度の団体でアクセスログ管理体制の整備が必要と指摘されている。

これらの調査結果から見ると、国立市既存住基システムのセキュリティレベルに比較して、住基ネットシステムのセキュリティレベルが低いという根拠はない。むしろ、国立市の既存住基システムのほうが住基ネットに比べてはるかに脆弱であるといわざるを得ない。住基ネットが全国の自治体と接続されるという点で脅威が大きくなることを考慮しても、既存住基システムに含まれる情報は住基ネットシステムよりも格段と機微な情報が含まれており、結果として国立市民の個人情報漏洩するリスクは、むしろ国立市内の既存住基システムのほうが大きいと思われる。

すなわち、国立市民の個人情報の漏洩等のリスクの視点からいえば、住基ネットに接続することにより国立市民の個人情報のリスクが大きくなるとする合理的な根拠はないと考える。むしろ、国立市庁舎内の住民基本台帳のほうがリスクが高く、早急に対策を講じるべき部分が多い。

報告内容 今後とるべき施策

体制・規程の整備

- 国立市の情報セキュリティポリシーを策定し、住基情報やその他の情報資産全体の管理体系を確立すべきである。現状の「国立市住民基本台帳ネットワークシステムセキュリティ管理規程」はその中に組み込むか、あるいはセキュリティポリシーの下位規程と位置付けるのが望ましい。
- 情報セキュリティポリシーには、情報資産ごとの管理責任の明確化やリスク分析にもとづく情報セキュリティマネジメントの考え方を盛り込む必要がある。
- 情報セキュリティポリシーには、国立市で取り扱う住民基本台帳を中心とする情報とそれらの情報を格納し処理する情報システムとを明確に区別し、情報管理責任とシステム管理責任とを分離してそれぞれに規程や手順を定めることが望ましい。システム管理の部分は外部の専門家に委託するなどセキュリティを高めることは可能であるが、情報管理責任はまさしく国立市の基幹業務であり、研修などを通じて職員の情報管理能力の向上を計らなければならない。
- 情報セキュリティポリシーの内容は、国立市の所有する情報を取り扱うすべての職員等に理解させ周知徹底する必要がある。そのためには、情報セキュリティを中心的に支える核となる職員の養成が不可欠である。
- 当面の情報セキュリティの確保のために、特に技術的な専門知識を必要とする部分については外部の専門家を招聘するなどにより、情報セキュリティ管理体制の充実を図ることが望ましい。

物理的対策

- 情報の重要度に応じて適用できる重要機能設置場所等の物理的なセキュリティの基準を明確に定めるべきである。
- 短期的には、ホストコンピュータを格納するマシンルームやコンソール卓の設置場所、住基ネットシステムを格納するキャビネットなどの施錠管理、鍵の管理、それらの設置場所への入退室管理などを厳格に行い、物理的な隔離の不十分な部分を運用で補う必要がある。
- 長期的には、マシンルームをより強固な環境に移設し、住基システムやその他の重要システム、ネットワーク機器類などを統合して収容し、特定の許可された人物以外の立ち入りを制限するなどにより物理的な安全性を更に確保することが望ましい。
- 住基情報など重要情報のバックアップテープを暗号化するなどの安全対策を施した上で遠隔地保管を早急を実施する必要がある。
- 磁気テープや取り外し可能磁気ディスクなど、記憶媒体の管理と厳重な保管管理を徹底する必要がある。

技術的対策

- 現住基システムを使用する市民課の窓口業務における担当者ごとのログインを徹底するべきである。
- 新たに作成する情報セキュリティポリシー、及びそれに基づいて策定することになる住基関連情報の管理要件に基づいて、住基システムが持つべきセキュリティ機能要件を明確にし、現状システムの実装とのギャップ分析を実施する必要がある。
- その結果に基づいて住基システムのセキュリティ機能を強化する必要がある。特に、行政基本システムにおける利用者の識別・認証は、より厳格な方法に改める必要がある。ギャップ分析の結果が大幅なシステム改訂の必要性を示す場合は、行政基本システムの基本構造を現状のパッケージのカスタマイズという形式から新たな構造に切り替えることも視野に入れなければならない。
- 住基ネットシステムの再稼動にあたっては、要求仕様に定義されているセキュリティ機能が的確に組み込まれているかを再点検する必要がある。

運用面の対策

- 情報セキュリティポリシーに記載されるであろう方針に基づいてホストコンピュータのセキュリティにかかわる運用マニュアルや、情報機器及び記憶媒体の管理手順、ネットワークのセキュリティ運用手順などを策定する必要がある。
- 磁気テープなどの記憶媒体の管理台帳、管理手順を整備し確実な管理を徹底する必要がある。
- ネットワーク基盤の運用管理手順を定め、ファイアウォール等の重要機器の運用状況を確認するプロセスを運用管理手順に組み込む必要がある。
- 住基ネットの再稼動にあたっては、「住民基本台帳ネットワークシステム基本設計概要書」に定められた運用管理規程類を策定し、関係する職員に遵守を徹底する必要がある。

このページは平成15年12月26日付で作成されたページです。

用語解説: [住基ネット](#) [運用マニュアル](#) [個人情報保護条例](#) [セキュリティポリシー](#) [磁気テープ](#)

※「用語解説」内のリンクは、ウェブリオが運営する辞書サイトの解説ページ(別ウィンドウ)に移動します。

総務部 市民課 市民係

電話:042-576-2111(内線 131,132) ファクス:042-576-0264

[メールでのお問い合わせは専用フォームをご利用ください。](#)

現在のページ：[ホーム](#) > [くらしの情報](#) > [証明・登録](#) > [住基ネットワークシステムについて](#) > [住民基本台帳ネットワークシステム](#) > [住民基本台帳ネットワークシステムについて](#) > [住基ネット調査研究事業](#) > [研究者の紹介](#)

研究者の紹介

更新日 平成22年7月27日

1. 法律面

稲垣隆一 氏

稲垣隆一法律事務所 弁護士 ISMS主任審査員

2. 情報システム面

大木 栄二郎 氏

アイ・ビー・エム ビジネスコンサルティング サービス 株式会社 技術理事

用語解説：[ISMS](#)

※「用語解説」内のリンクは、ウェブリオが運営する辞書サイトの解説ページ(別ウィンドウ)に移動します。

総務部 市民課 市民係

電話:042-576-2111(内線 131,132) ファクス:042-576-0264

[メールでのお問い合わせは専用フォームをご利用ください。](#)