

番号制度の導入後におけるセキュリティ対策に対する実態的評価に関する実証的研究（継続）

| | | |
|-------|--------|----------------------------|
| 代表研究者 | 瀧口 樹 良 | 情報セキュリティ大学院大学客員研究員 |
| 共同研究者 | 湯浅 壘 道 | 情報セキュリティ大学院大学情報セキュリティ研究科教授 |
| 共同研究者 | 豊田 充 | ㈱浜銀総合研究所地域戦略研究部副主任研究員 |

1 はじめに

本研究は、行政の情報化施策の一環として、電子政府・電子自治体を促進させる観点から、地方自治体の現場実態に合わせたセキュリティ評価の指標設定等を通じて、「社会保障・税番号制度（以降、「番号制度」という）」の導入後におけるセキュリティ対策について実証研究を行うものである。

地方自治体の取り巻く環境は、番号制度の導入と合わせて、近年のクラウド技術等の ICT の進展や高度化するサイバー攻撃など、取り巻く状況の変化に適時適切に対応し、安心・安全な行政サービスを住民に提供するため、更なる情報セキュリティ対策の向上に努めることが求められている。

このため、総務省は、「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」及び「地方公共団体における情報セキュリティ監査ガイドライン」（以下「ガイドライン」という）の改定を行い、地方公共団体における情報セキュリティ対策の向上に取り組んでいる。

また、番号制度の導入に当たっては、セキュリティやプライバシーといった側面などから、様々な不安や懸念が指摘されているため、番号制度の導入に当たっては、企業や地方自治体等で安全管理措置の整備・運用や、特定個人情報保護評価の実施等、様々な対応が求められている。そのため、個人番号その他の特定個人情報に対する適正な取扱いを確保するために必要な措置を講ずることを任務とする内閣府外局の第三者機関である個人情報保護委員会から行政機関等・地方公共団体等編として、「特定個人情報の適正な取扱いに関するガイドライン」が提示され、その安全管理対策としてのセキュリティ対策が求められている。

特に、2001年からの政府による「e-Japan 戦略」以降、政府および全国の地方自治体において情報化に積極的に取り組まれており、それに対するセキュリティ対策も実施しているものの、セキュリティに関する事件・事故も起きているのが実態である。番号制度の導入に当たっては、住民の個人番号等の特定個人情報が外部に漏れることによる個人情報漏洩、なりすまし等による番号の不正利用、番号に紐付けされた情報が一元管理されるのではないかと不安に対し、罰則の強化やシステム上の安全措置、情報の分散管理など対策を施しているものの、実際に特定個人情報を取り扱う情報保有機関である地方自治体では、今まで以上に個人情報保護対策が求められることになる。この個人情報保護対策の具体的な安全管理措置が情報セキュリティ対策と重なるため、地方自治体においては、より一層の情報セキュリティ対策が求められる。特に、職員だけでなく委託先も含めた特定個人情報を取り扱う関係者全体の人的対策を行う必要がある。

こうしたセキュリティ対策の基本となるものが、先に述べた個人情報保護委員会が提示する「特定個人情報の適正な取扱いに関するガイドライン（行政機関・地方公共団体等編、以下「本ガイドライン」という）」である。このガイドラインでは、組織として個人番号および特定個人情報を適正に取り扱うための基本方針や取扱規程などのルールを策定する必要があります。さらに、ルールを徹底するための職員研修や、技術的なセキュリティ対策を取るなど、必要かつ適切な安全管理措置を講ずることが求められている。

さらに平成 27 年 6 月 1 日に日本年金機構から公表された個人情報流出事件は、職員の端末が外部からのウイルスメールによる不正アクセスを受け、大量の個人情報が流出するといった、重要な個人情報を取り扱う行政機関等に対する信頼性を揺るがしかねないものであった。そのため、番号法の法案改正審議にも影響する事態を巻き起こした。

こうした事態を踏まえ、総務省では地方公共団体における情報セキュリティに係る抜本的な対策を検討するため、自治体情報セキュリティ対策検討チームを開催し、新たな地方自治体の情報セキュリティ対策の抜本的強化に向けて、番号制度に関わりがある住基、税、社会保障などのシステムにおいては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への二要素認証の導入等を図ることにより、住民の個人情報の流出を徹底して防ぐことや、LGWAN 環境のセキュリティ確保に資するため、財務会計など LGWAN を活用する業務用システムと Web 閲覧やインターネットメールなどのシステムとの通信経路を分割すること。さらに、インターネット接続系においては、都道府県と市区町村が協

力してインターネット接続口を集約した上で、地方自治体の情報セキュリティクラウドを構築し、高度なセキュリティ対策を講ずることなどが提言されている。

そこで、本研究では、番号制度におけるセキュリティ対策の基本となるものとして個人情報保護委員会が提示する「特定個人情報の適正な取扱いに関するガイドライン（行政機関・地方公共団体等編）」に基づき、組織として個人番号および特定個人情報を適正に取り扱うための利用、提供、収集・保管の制限や講ずべき安全管理措置の内容を分析することとした。併せて、番号法、行政機関個人情報保護条例等関係法令、「行政機関の保有する個人情報の適切な管理のための措置に関する指針について（平成16年9月14日総管情第84号総務省行政管理局長通知）」、「独立行政法人等の保有する個人情報の適切な管理のための措置に関する指針について（平成16年9月14日総管情第85号総務省行政管理局長通知）」及び「地方公共団体における個人情報保護対策について（平成15年6月16日総行情第91号総務省政策統括官通知）」等の指針、政府機関の情報セキュリティ対策のための統一基準等に準拠した各府省庁等における情報セキュリティポリシー、及び接続する情報提供ネットワークシステム等の接続規程等が示す安全管理措置等の規定を踏まえ、技術的対策に着目されがちであった点を踏まえ、組織面や実態面、及び人的側面にも着目し、セキュリティ対策として実現可能な有効な対策として、特定個人情報の利用・提供、保管・管理、削除・廃棄の各方法に関する安全管理措置の基準について分析を行うこととした。

そこで、平成27年度においては、番号制度の導入を前提に、個人番号その他の特定個人情報に対する適正な取扱いとしての情報セキュリティ対策として、本ガイドラインで示された安全管理対策の取り組み評価が可能な指標化を行い、地方自治体に対するアンケート調査に基づき、番号制度導入後の地方自治体のセキュリティ対策のあり方を検討するため、番号制度の特定個人情報に関する安全管理措置の取扱いの実態を把握するため、個人情報保護委員会の本ガイドラインに示された情報セキュリティ対策を含めた「（別添）特定個人情報に関する安全管理措置（行政機関等・地方公共団体等編）」に基づく取り組みの実態や課題等に関する地方自治体を把握するため、全国の地方自治体（都道府県及び市町村区）を対象に、郵送アンケート調査を実施し、特定個人情報に関する安全管理措置の実態や取組課題や今後必要な取組について考察することとした。

その結果、2割弱の地方自治体では、基本方針等の整備ができていない実態や、1割近くの地方自治体において、個人情報保護条例の改正等の対応ができていない実態が明らかとなった。さらに、特定個人情報に関する安全管理措置については、技術的安全管理措置に比べて、組織的安全管理措置、人的安全管理措置、物理的安全管理措置に対して具体的な取り組みの実施状況にバラつきがあった。そのため、今後必要な安全管理措置の取り組みとして、取扱担当者等の教育や取扱規程等に基づく運用、さらに情報漏えい等の防止、組織体制の整備といった対策が必要となっている実態が明らかとなった。また、安全管理措置の取組課題としても、業務負荷や人材不足、さらに現場職員への教育研修の不徹底といった課題が浮き彫りとなった。このため、今後、取扱担当者等の教育を浸透させるとともに、取扱規程等に基づく運用といったセキュリティ対策としてのPDCAサイクルを回す仕組みづくりが求められている。

そこで、平成28年度は、こうして明らかとなった地方自治体のセキュリティ対策の実態に対して、その地域の住民意識として、どのように捉えるのかといった利用者としての視点を踏まえた比較分析を試みることで、より住民の理解が得られるセキュリティ対策を検討することが可能となるものと考えられる。特に、特に財政力や専門的な担当者の確保が困難と思われる地方自治体において、どこに重点を置いたセキュリティ対策が住民から求められているかについて、具体的に検討することとした。

具体的には、平成27年度に実施した自治体のアンケート調査の調査項目に準じて、番号制度を利用する可能性の高い国内ネット利用者（ネットを利用する住民）を対象にWEBアンケート調査を実施する。このWEBアンケート調査で行うことで、住民として求められるセキュリティ対策の要件や優先度による比較分析を試みることで、より地方自治体の現実的なセキュリティ対策の取り組みに対する提言を行うものである。

2 番号制度の導入後におけるセキュリティ対策としての安全管理措置

2-1 特定個人情報に対する安全管理措置の具体的な指針とされるガイドラインの位置づけ

番号法に基づく番号制度は、社会保障、税及び災害対策の分野における行政運営の効率化を図り、国民にとって利便性の高い、公平・公正な社会を実現するための社会基盤として導入されるものとされている。

一方で、番号制度の導入に伴い、国家による個人情報の一元管理、特定個人情報の不正追跡・突合、財産その他の被害等への懸念が示されてきた。個人情報の適正な取扱いという観点からは、個人情報の保護に関する一般法として、個人情報保護法、行政機関個人情報保護法、及び独立行政法人等個人情報保護法

の3つの法律があり、また、地方自治体では個人情報保護条例において各種保護措置が定められている。

但し、番号法においては、一般法に定められる措置の特例として、個人番号をその内容に含む個人情報（以下「特定個人情報」という）の利用範囲を限定する等、より厳格な保護措置を定めるとともに、国が設置・管理する情報提供ネットワークシステムの使用を始めシステム上の安全管理措置を講ずることとしている。そこで、番号法（第4条）及び個人情報保護法（第60条）に基づき、行政機関等及び地方公共団体等が特定個人情報の適正な取扱いを確保するための具体的な指針を定めものとされ、個人情報保護委員会において、番号法の適用を受ける者のうち行政機関等及び地方公共団体等を対象とする具体的な指針として本ガイドラインが策定されることとなった。

なお、本ガイドラインは、特定個人情報の適正な取扱いについての具体的な指針を定めているため、特定個人情報に関し、番号法に特段の規定がなく一般法又は個人情報保護条例が適用される部分については、一般法を基に定められている指針等（「行政機関の保有する個人情報の適切な管理のための措置に関する指針について」（平成16年9月14日総管情第84号総務省行政管理局長通知）、「独立行政法人等の保有する個人情報の適切な管理のための措置に関する指針について」（平成16年9月14日総管情第85号総務省行政管理局長通知）及び「地方公共団体における個人情報保護対策について」（平成15年6月16日総行情第91号総務省政策統括官通知）等をいい、以下「指針等」という。）を遵守することを前提としている。

2-2 番号法の特定個人情報に関する保護措置の概要

個人番号は、社会保障、税及び災害対策の分野において、個人情報を複数の機関の間で紐付けるものとして、住民票を有する全ての者に一人一番号で重複のないように、住民票コードを変換して得られる番号とされている。そのため、個人番号が悪用され、又は漏えいした場合、個人情報の不正な追跡・突合が行われ、個人の権利利益の侵害を招きかねない危険性をはらんでいる。

そのため、番号法においては、特定個人情報について、一般法よりも厳格な各種の保護措置を設けている。この保護措置は、「特定個人情報の利用制限」、「特定個人情報の安全管理措置等」及び「特定個人情報の提供制限等」の3つに大別されている。

（1）特定個人情報の利用制限

番号法においては、個人番号を利用することができる範囲について、社会保障、税及び災害対策に関する特定の事務に限定している（番号法第9条及び別表第1）。また、行政機関個人情報保護法及び独立行政法人等個人情報保護法の読替え又は適用除外の規定を置き（同法第30条第1項及び第2項）、本来の利用目的以外の目的で例外的に特定個人情報を利用することができる範囲について、行政機関個人情報保護法及び独立行政法人等個人情報保護法における個人情報の利用の場合よりも限定的に定められている。

地方自治体においては、番号法第32条の規定に基づき、行政機関等と同様の適用となるよう、個人情報保護条例の改正等が必要となる場合がある。さらに、個人番号利用事務等実施者に対し、必要な範囲を超えた特定個人情報ファイルの作成を禁止している（同法第29条）。

（2）特定個人情報の安全管理措置等

行政機関等については、行政機関個人情報保護法及び独立行政法人等個人情報保護法に基づき、保有個人情報の安全管理措置を講じなければならない、個人情報の取扱いの委託を受けた者にも同様の義務が課されている（行政機関個人情報保護法第6条、独立行政法人等個人情報保護法第7条）。また、行政機関等の職員又は受託業務に従事している者は、個人情報を漏えいし又は不当な目的に利用することが禁止されている（行政機関個人情報保護法第7条、独立行政法人等個人情報保護法第8条）。なお、地方自治体等については、個人情報保護条例に基づくこととされている。

一方、番号法においては、これらに加え、個人番号（生存する個人のものだけでなく死者のものも含む。）について安全管理措置を講ずることとされている（番号法第12条）。また、個人番号利用事務等を再委託する場合には委託者による再委託の許諾を要件とする（同法第10条）とともに、委託者の委託先に対する監督義務を課している（同法第11条）。さらに、委託を受けた者及び再委託を受けた者は、個人番号利用事務等実施者になることを明確にし（同法第2条第12項及び第13項）、これらの者も番号法における個人番号の安全管理措置を講じなければならないこととされている（同法第12条）。

（3）特定個人情報の提供制限等

行政機関個人情報保護法及び独立行政法人等個人情報保護法は、保有個人情報について、法令の規定に基

づく場合等を除くほか、本人の同意を得ないで、第三者に提供することを認めていない（行政機関個人情報保護法第8条、独立行政法人等個人情報保護法第9条）。また、地方自治体等については、個人情報保護条例の定めに基づくこととなる。

一方、番号法においては、特定個人情報の提供について、個人番号の利用制限と同様に、一般法における個人情報の提供の場合よりも限定的に定めている（番号法第19条）。また、何人も、特定個人情報の提供を受けることが認められている場合を除き、他人（自己と同一の世帯に属する者以外の者をいう。同法第20条において同じ。）に対し、個人番号の提供を求めてはならない（同法第15条）こととなる。さらに、特定個人情報の収集又は保管についても同様の制限を定められている（同法第20条）。なお、本人から個人番号の提供を受ける場合には、本人確認を義務付けられている（同法第16条）。

（4）特定個人情報保護のための主体的な取組

行政機関等及び地方自治体等は、番号法等関係法令並びに本ガイドライン及び指針等に従い、特定個人情報の適正な取扱いを確保するための具体的な方策について検討し、実践するとともに、国民・住民等の意見、事務の実態、技術の進歩等を踏まえ、点検・見直しを継続的に行う体制を主体的に構築することが求められている。

なお、本ガイドラインについても、社会情勢の変化、国民意識の変化等諸環境の変化に加え、個人情報の保護に関する技術の進歩及び国際動向も踏まえつつ、必要に応じ見直しを行うものとされている。

2-3 個人情報保護委員会に対する報告徴収・立入検査等

個人情報保護委員会は、特定個人情報の取扱いに関する監視・監督並びに苦情の申出についての必要なあっせん及びその処理を行う事業者への協力を求めることができる（番号法第29条の3、第29条の4、第35条）。

具体的には、個人情報保護委員会は、特定個人情報を取り扱う者その他の関係者に対し、特定個人情報の取扱いに関し、必要な報告若しくは資料の提出を求め、又はその職員に、当該特定個人情報を取り扱う者その他の関係者の事務所その他必要な場所に立ち入らせ、特定個人情報の取扱いに関し質問させ、若しくは帳簿書類その他の物件を検査させることができることとなっている。

（1）漏えい事案等に関する報告の受付状況等

個人情報保護委員会が公表した「年次報告（平成29年度）」によると、平成29年度において、特定個人情報の漏えい事案その他のマイナンバー法違反の事案又はそのおそれのある事案について、374件の報告を受けた。このうち、「重大な事態」については、地方公共団体から1件、事業者から4件の報告を受けている（番号法第29条の4、図表1）。

なお、漏えい事案等の報告の多くは、地方自治体におけるマイナンバーを含んだ書類の誤送付・誤交付であった。また、重大な事態については、マイナンバーが記載された書類が滅失した事案等であり、いずれもマイナンバーが悪用されたとの報告は受けていない。そのため、漏えい事案等の報告を受けて、再発防止策等の確認を行うとともに、同種の事態が起きないように指導等を行っている。

（2）立入検査等の実施状況

個人情報保護委員会が公表した「年次報告（平成29年度）」によると、個人情報保護委員会の立入検査を行うに当たり、平成29年度検査計画を策定し、検査の実施方針として、行政機関等に対する定期的な検査を行うとともに、地方自治体等に対しては、規模、特性及び事務の内容等を勘案の上、選択的に実施することなどを定めている。平成29年度においては、法令及び本ガイドライン等の遵守状況、特定個人情報保護評価書に記載された事項の実施状況等を实地に確認するため、行政機関等6件、地方自治体18件、事業者3件の立入検査を実施し、指摘した事項について改善を求めている（番号法第35条及び第29条の3第1項）。

また、地方自治体等のシステムセキュリティ面に重点を置く实地調査を4件実施し、特定個人情報の適正な取扱いに関して改善を求めた。なお、地方自治体等に対しては、これらの調査結果等を踏まえ、システムセキュリティ面に限らず、広く特定個人情報の取扱状況を实地に確認することが重要であるとの観点から、試行的に検査項目を絞った立入検査も13件実施している。

（3）地方自治体等の特定個人情報の取扱いに関する定期的な報告の状況

個人情報保護委員会が公表した「年次報告（平成29年度）」によると、特定個人情報ファイルを保有する

地方自治体及び地方独立行政法人は、毎年度、前年度においてマイナンバーの漏えい、滅失又は毀損の防止その他のマイナンバーの適切な管理のために講じた措置に関する事項その他当該特定個人情報ファイルに記録された特定個人情報の取扱いに係る事項を報告することとされている（番号法第29条の3第2項）。

平成29年度においては、平成28年度における全項目評価書又は重点項目評価書に記載されたリスク対策の措置状況等、立入検査等で把握した課題等を踏まえて個人情報保護委員会が設定した項目に係る特定個人情報の取扱い状況について、2,242機関から報告を受けている。こうした結果を踏まえて、地方自治体等における特定個人情報の適正な取扱いに向けた改善を促すため、33団体に対して特定個人情報安全管理措置セミナーを開催している。

さらに、地方公共団体から参加希望を募り、40団体に対して、マイナンバー漏えい事案等が発生したとの想定で初動対応の訓練を実施し、さらに訓練を通じて得られた知見について地方自治体等に対して周知等を行っている。

図表1 特定個人情報の取扱いに関する監視・監督に係る処理状況

（期間：平成29年4月1日～平成30年3月31日）

| 対応事項 | 件数等 |
|---------------------|---|
| 特定個人情報の漏えい事案等の報告の受付 | 286機関・374件 （うち「重大な事態」（※1）に該当：5件） （内訳） 行政機関等：4機関、11件 地方公共団体：220機関、270件 （うち「重大な事態」に該当：1件） 事業者：62機関、93件 （うち「重大な事態」に該当：4件） |
| うち「重大な事態」の内容 | ①地方公共団体において、約250人分のマイナンバーが記載された書類を紛失した事案 ②事業者において、プログラミングミスにより約800人分のマイナンバーカード等の本人確認書類の画像データを削除した事案 ③事業者において、火災により約260人分のマイナンバーが記載された書類を滅失した事案 ④事業者において、誤って約440人分のマイナンバーが記載された書類を廃棄した事案 ⑤事業者において、盗難により約110人分のマイナンバーカードの写しなどの書類が持ち去られた事案 |
| 立入検査の実施 | 27件（※2） （内訳）行政機関等6件、地方公共団体18件、事業者3件 |
| 指導・助言 | 173件 |

※1 「重大な事態」とは、「特定個人情報の漏えいその他の特定個人情報の安全の確保に係る重大な事態の報告に関する規則」第2条各号に掲げる事態である。

※2 立入検査の実施件数は、立入検査開始日を基準として計上している。

（出典：個人情報保護委員会「平成29年度 年次報告」）

2-4 特定個人情報に関する安全管理措置

個人情報保護委員会が提示している本ガイドラインでは、講ずべき安全管理措置として「（別添）特定個人情報に関する安全管理措置（行政機関等・地方公共団体等編）」として、以下の安全管理措置の項目を定めている（図表2）。

なお、本ガイドラインに示す安全管理措置の項目以外にも、保有する特定個人情報等の性質、情報漏えい・滅失・毀損等による影響等の検討の結果に基づき、情報漏えい等事案の未然防止及び検知並びに事案発生時の拡大防止等の観点から、適切に判断する必要がある。

図表2 本ガイドラインに示す安全管理措置の項目

| |
|-----------|
| A 基本方針の策定 |
|-----------|

- B 取扱規程等の見直し等
- C 組織的安全管理措置
 - a 組織体制の整備
 - b 取扱規程等に基づく運用
 - c 取扱状況を確認する手段の整備
 - d 情報漏えい等事案に対応する体制等の整備
- D 人的安全管理措置
 - a 事務取扱担当者の監督
 - b 事務取扱担当者等の教育
 - c 法令・内部規程違反等に対する厳正な対処
- E 物理的安全管理措置
 - a 特定個人情報等を取り扱う区域の管理
 - b 機器及び電子媒体等の盗難等の防止
 - c 電子媒体等の取扱いにおける漏えい等の防止
 - d 個人番号の削除、機器及び電子媒体等の廃棄
- F 技術的安全管理措置
 - a アクセス制御
 - b アクセス者の識別と認証
 - c 不正アクセス等による被害の防止等
 - d 情報漏えい等の防止

(出典：個人情報保護委員会「特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）」平成 26 年 12 月 18 日（平成 29 年 5 月 30 日最終改正）

本研究では、セキュリティ対策として実現可能な有効な対策として、特定個人情報の利用・提供、保管・管理、削除・廃棄の各方法に関する安全管理措置の基準となる本ガイドラインで示された安全管理対策の取り組み評価が可能な指標化として、図表 2 で示されている項目を 39 項目として整理することとした。

なお、この 39 項目は、平成 27 年度において実施した全国の地方自治体（都道府県及び市町村区）を対象とした郵送アンケート調査（以下「地方自治体アンケート」という）の指標にも採用している。

3 WEB アンケート調査による自治体の安全管理対策の実態把握

3-1 郵送アンケート調査の実施概要

前述した問題意識を踏まえ、番号制度の特定個人情報に関する安全管理措置の取り扱いの実態を把握するため、個人情報保護委員会の本ガイドラインに示された情報セキュリティ対策を含めた「(別添) 特定個人情報に関する安全管理措置(行政機関等・地方公共団体等編)」の内容に基づく取り組みの実態や課題等に対して、番号制度を利用する可能性の高い国内ネット利用者(ネットを利用する住民)を対象にWEBアンケート調査を実施した(図表3)。

図表3 WEB アンケート調査の概要

| 項目 | 概要 |
|--------|---|
| 目的 | ①特定個人情報の適正な取扱いを確保するための具体的な指針について ②特定個人情報に関する安全管理措置について ③安全管理措置の取組課題や今後必要な安全管理措置の取組について |
| 実施手法 | WEB アンケート調査(ネットアンケート調査会社経由で、対象者にメールで回答を依頼し、WEB サイト経由で回答を回収) |
| 調査対象 | 1,200 人 ✓ 国内に在住するインターネットを利用するユーザ(18 歳以上の男女)の中から、10 地区(北海道、東北、関東、北陸、甲信越、東海、近畿、中国、四国、九州・沖縄)に均等割り付けにて送付し、回収。 |
| 実施期間 | 平成 30 年 2 月 |
| 信頼性の確保 | 所要時間が短い回答や、極端に同じ箇所にチェックしてある回答、また特定の規則性がみられる回答などは、有効回答とはみなさず除外。 |
| 主な調査項目 | 問 1 番号制度の認知度等について 問 1-1 【認知度の有無】 問 1-2 【不安感の有無】 問 2 特定個人情報に関する安全管理措置について 問 2-1 【必要な安全管理措置】 問 2-2 【安全管理対策の優先度】 問 2-3 【今後必要な安全管理措置の取組】 問 3 回答者自身について |

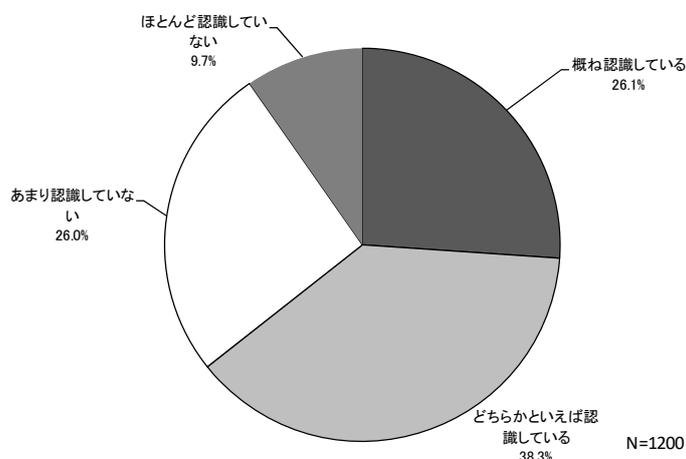
なお、ネットアンケート調査には、調査対象がインターネットユーザに限定されるという偏りがあるものの、番号制度においてマイナポータルの活用など、インターネットを通じたマイナンバーの活用が積極的に行われることが想定されていることから、そうした関心のあるユーザに対して意識調査を行うことで、課題を浮き彫りにできるものと判断した。また、10 地区の均等割り付けにて送付した理由は、地域差による意見の相違を予め防ぐためである。

3-2 番号制度の認知度等について

(1) 認知度の有無

番号制度の内容に対する認識の有無について尋ねると、次のとおりとなった(図表4)。

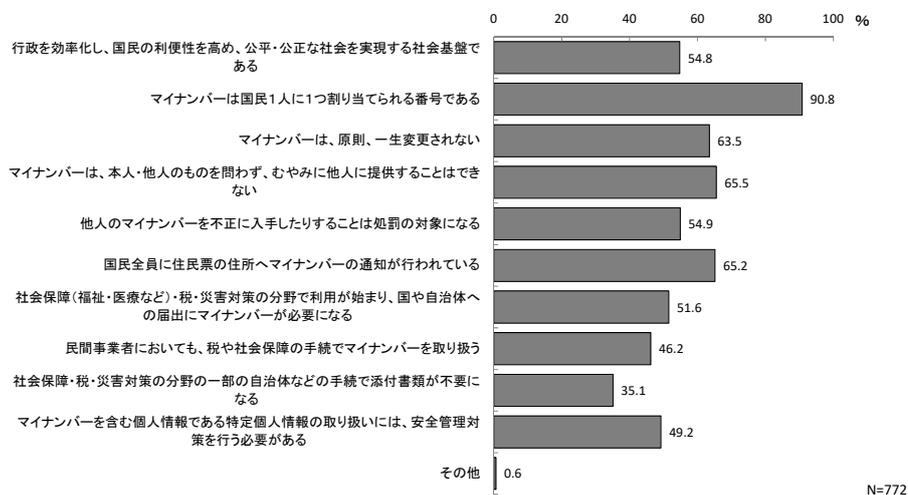
図表4 認知度の有無(単一選択)



この結果、「概ね認識している」との回答が26.1%、「どちらかといえば認識している」との回答が38.3%と、認識している割合が64.3%と6割を超える回答であった。一方、「あまり認識していない」との回答が26.0%、「ほとんど認識していない」との回答が9.7%と、認識していない割合が35.7%と3割を超える回答があり、未だ十分にネットユーザに認識ができていない割合が一定数存在している実態が明らかとなった。

なお、図表4において認識している割合(64.3%)のネットユーザに対して、番号制度で認識している内容について尋ねると、次のとおりとなった(図表5)。

図表5 番号制度の認識内容(複数選択)

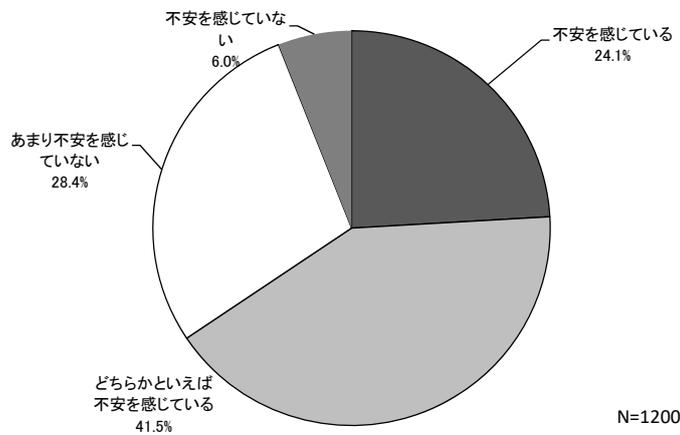


この結果、上位の認識として、「マイナンバーは国民1人に1つ割り当てられる番号である」との回答が90.8%、「マイナンバーは、本人・他人のものを問わず、むやみに他人に提供することはできない」との回答が65.5%、「国民全員に住民票の住所へマイナンバーの通知が行われている」との回答が65.2%、「マイナンバーは、原則、一生変更されない」との回答が63.5%との順となっており、番号制度の仕組みに対する認識が多くを占められていた。他方、番号制度の効果として国が示している「社会保障・税・災害対策の分野の一部の自治体などの手続で添付書類が不要になる」との回答が35.1%となっており、あまり認識が進んでいないことが明らかとなった。

(2) 不安感の有無

番号制度について、情報漏えい等の不安感を感じるかの有無について尋ねると、次のとおりとなった(図表6)。

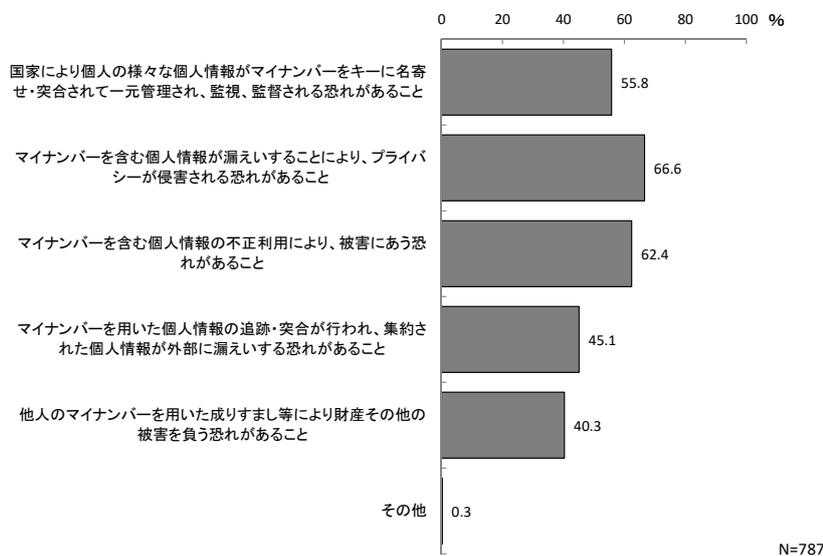
図表6 基本方針等の内容(単一選択)



この結果、「不安を感じている」との回答が24.1%、「どちらかといえば不安を感じている」との41.5%と、番号制度に対して不安を感じている割合が65.6%と6割を超えるネットユーザが不安を感じていた。

そこで、図表6において認識している割合(65.6%)のネットユーザに対して、どのような不安を感じているかを尋ねると、次のとおりとなった(図表7)。

図表7 番号制度に対する不安感の内容(複数選択)



この結果、「マイナンバーを含む個人情報が漏えいすることにより、プライバシーが侵害される恐れがあること」との回答が66.6%、「マイナンバーを含む個人情報の不正利用により、被害にあう恐れがあること」との回答が62.4%と、プライバシーの侵害や不正利用に対する被害に対して不安を感じているネットユーザが多いことが明らかとなった。

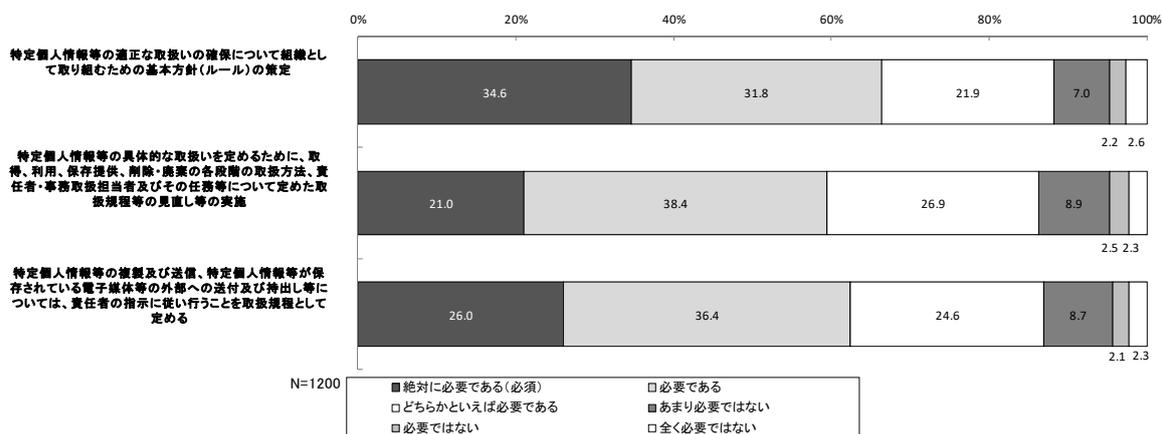
3-3 特定個人情報に関する安全管理措置の必要性について

特定個人情報の適正な取扱いを確保するための安全管理措置の対策として、個人情報保護委員会が示す本ガイドラインに従って、前述の通り以下の項目に対する39項目の設定問に対して、「絶対に必要である(必須)」から「全く必要ではない」までの必要性を6段階にネットユーザに評価してもらうこととした。

(1) 安全管理措置の取組(基本方針の策定および取扱規程等の見直し)

特定個人情報の適正な取扱いを確保するための安全管理措置のうち、「A 基本方針の策定」および「B 取扱規程等の見直し等」の実施状況について尋ねると、次のとおりとなった(図表8)。

図表8 安全管理措置の取組(基本方針の策定および取扱規程等の見直し)(各項目に対して単一選択)



この結果、「A 基本方針の策定」については8割以上のネットユーザが、必要との回答があり、「B 取扱規程等の見直し等」の実施状況についても同様に8割以上のネットユーザが、必要との回答があった。

但し、平成27年度に実施した地方自治体アンケートでは、「取扱規程等の見直し等」について実施した自治体が6割に留まるなど、具体的な取扱規程等にまで落とし込んで規定しきれていない実態が明らかとなっており、ネットユーザとの差が生じていることが明らかとなった。

(2) 安全管理措置の取組(組織的安全管理措置)

特定個人情報の適正な取扱いを確保するための安全管理措置のうち、「C 組織的安全管理措置」の実施状況について尋ねると、次のとおりとなった(図表9)。

この結果、「絶対に必要である(必須)」との回答が多かった項目として、「特定個人情報等へのアクセス状況の記録の改ざん、窃取又は不正な削除の防止のために必要な措置」が30.3%、「情報漏えい等の事案の発生又は兆候を把握した場合に、適切かつ迅速に対応するための体制及び手順等の整備」が27.6%、「情報漏えい等の事案が発生した場合、事案に応じて、事実関係及び再発防止策等を早急に公表する方法」が26.2%となっていた。

そのため、組織的安全管理措置の対応として、改ざん防止や情報漏えいに対する対策がネットユーザから求められている。

(3) 安全管理措置の取組(人的安全管理措置)

特定個人情報の適正な取扱いを確保するための安全管理措置のうち、「D 人的安全管理措置」の実施状況について尋ねると、次のとおりとなった(図表10)。

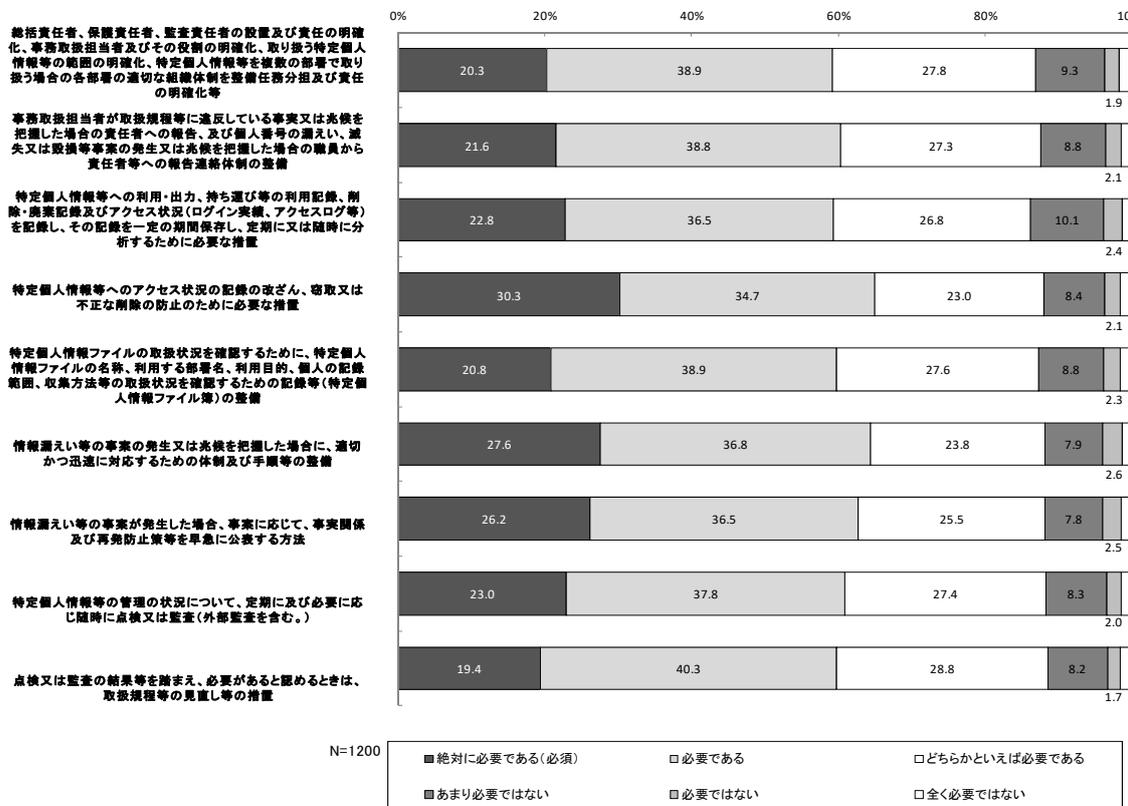
この結果、「絶対に必要である(必須)」との回答が多かった項目として、「法令又は内部規程等に違反した職員に対しては、法令又は内部規程等に基づき厳正な対処」が30.3%、「特定個人情報等が取扱規程等に基づき適正に取り扱われるよう、総括責任者及び保護責任者は事務取扱担当者に対して必要かつ適切な監督」が21.2%、「特定個人情報等の適切な管理のため、総括責任者及び保護責任者は特定個人情報等を取り扱う情報システムの管理に関する事務に従事する職員に対して情報システムの管理、運用及びセキュリティ対策に関して必要な教育研修」が21.1%となっていた。

そのため、人的安全管理措置の対応として、厳正な対処や適切な監督、さらに必要な教育研修が求められ

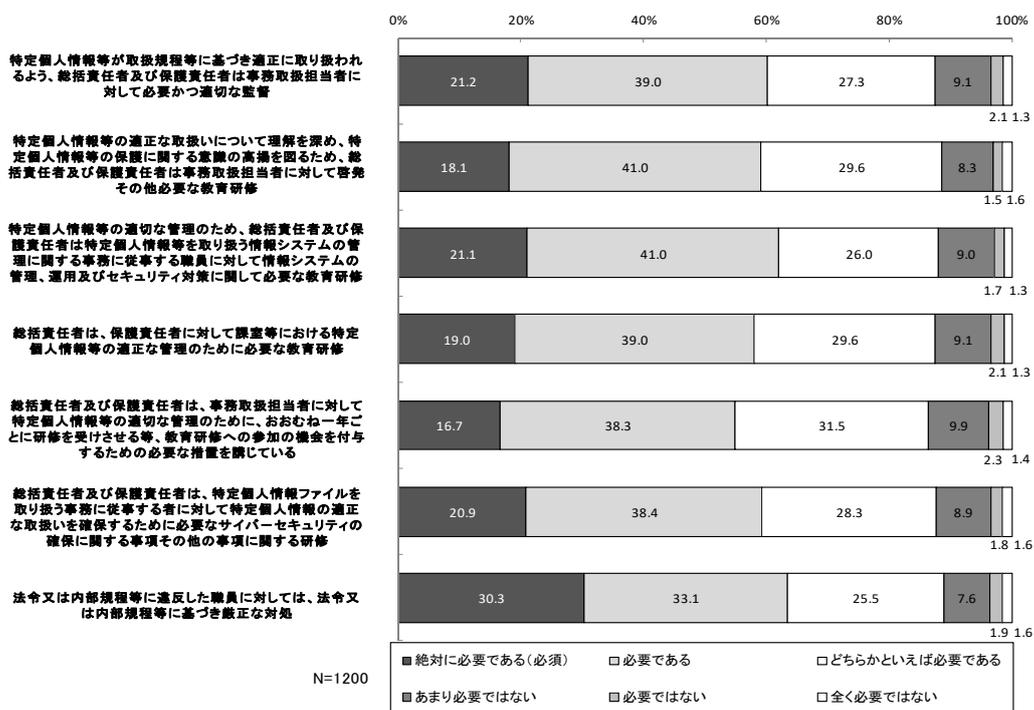
ていることが明らかとなった。

但し、平成 27 年度に実施した地方自治体アンケートでは、具体的な各課の担当者に対する研修等が不十分な地方自治体が多い実態が明らかとなっており、ネットユーザとの差が生じていることが明らかとなった。

図表 9 安全管理措置の取組（組織的安全管理措置）（各項目に対して単一選択）



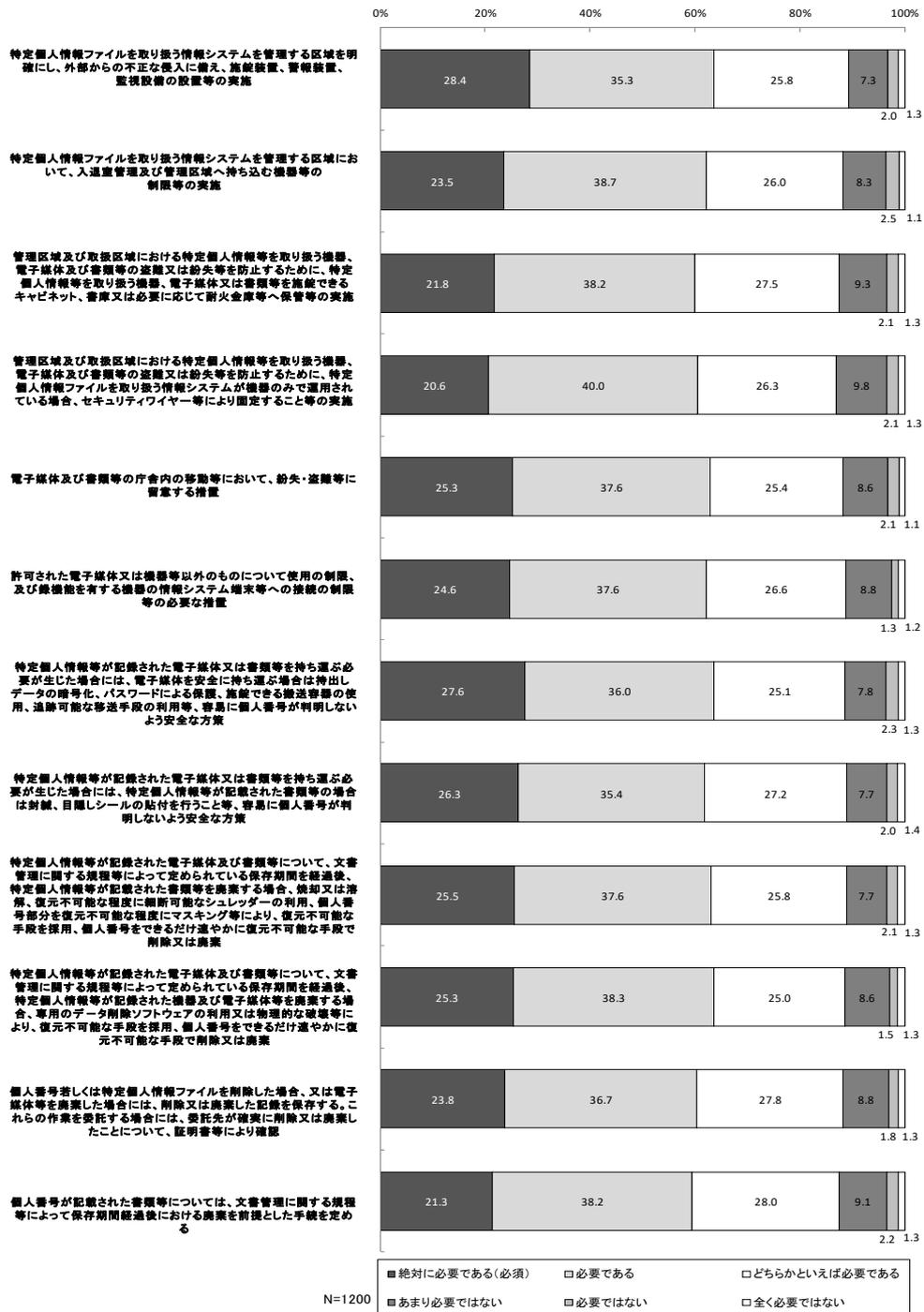
図表 10 安全管理措置の取組（人的安全管理措置）（各項目に対して単一選択）



(4) 安全管理措置の取組（物理的安全管理措置）

特定個人情報の適正な取扱いを確保するための安全管理措置のうち、「E 物理的安全管理措置」の実施状況について尋ねると、次のとおりとなった(図表 11)。

図表 11 安全管理措置の取組（物理的安全管理措置）（各項目に対して単一選択）



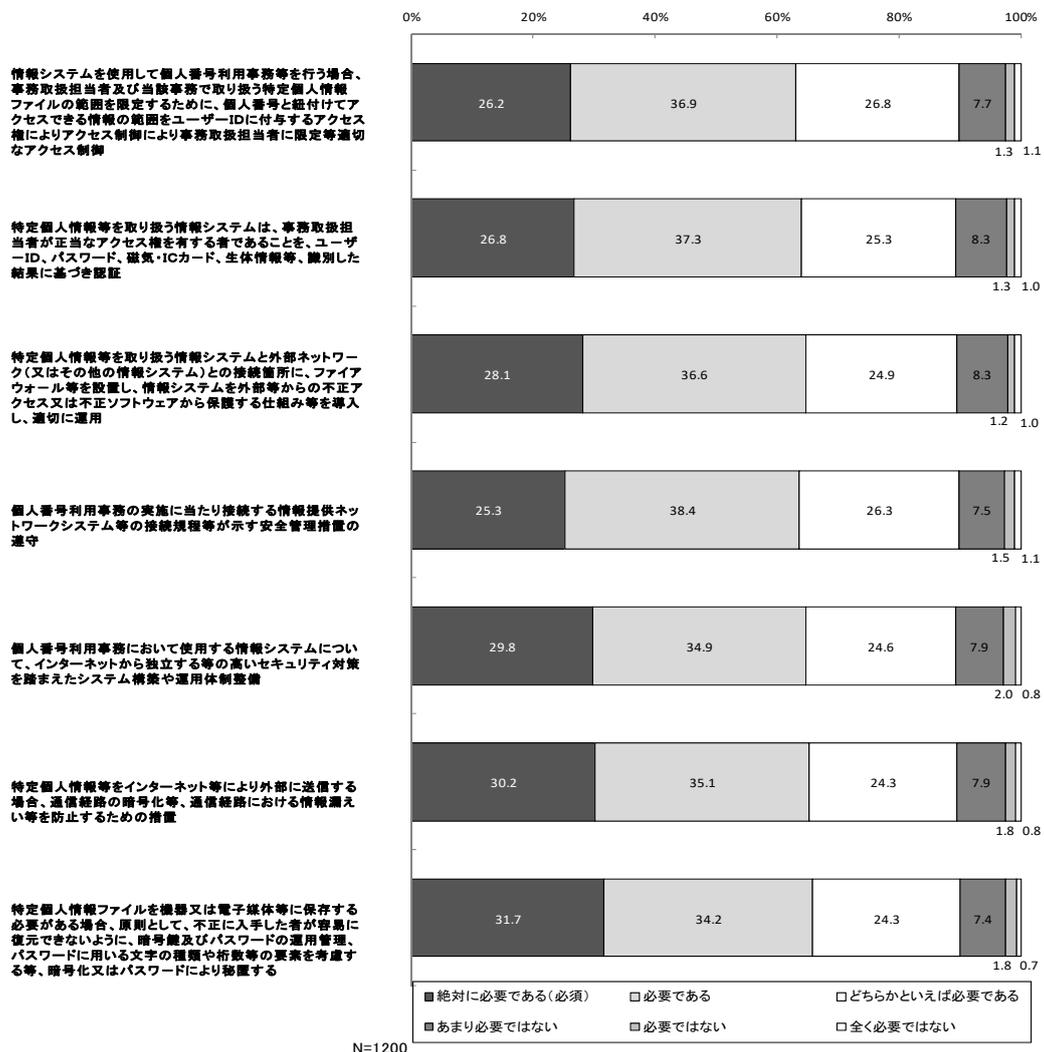
この結果、「絶対に必要である(必須)」との回答が多かった項目として、「特定個人情報ファイルを取り扱う情報システムを管理する区域を明確にし、外部からの不正な侵入に備え、施錠装置、警報装置、監視設備の設置等の実施」が 28.4%、「特定個人情報等が記録された電子媒体又は書類等を持ち運ぶ必要が生じた場合には、電子媒体を安全に持ち運ぶ場合は持出しデータの暗号化、パスワードによる保護、施錠できる搬送

容器の使用、追跡可能な移送手段の利用等、容易に個人番号が判明しないよう安全な方策」が 27.6%、「特定個人情報等が記録された電子媒体又は書類等を持ち運ぶ必要が生じた場合には、特定個人情報等が記載された書類等の場合は封緘、目隠しシールの貼付を行うこと等、容易に個人番号が判明しないよう安全な方策」が 26.3%となっていた。そのため、外部からの不正な侵入の防止や特定個人情報の持ち運びに対する対応などが求められていることが明らかとなった。但し、平成 27 年度に実施した地方自治体アンケートでは、「容易に個人番号が判明しないよう安全な方策」の実施済みが 51.8%に留まるなど、具体的な物理的な安全管理措置の取り組みが不十分な地方自治体が多い実態が明らかとなっており、ネットユーザとの差が生じていることが明らかとなった。

(5) 安全管理措置の取組（技術的安全管理措置）

特定個人情報の適正な取扱いを確保するための安全管理措置のうち、「F 技術的安全管理措置」の実施状況について尋ねると、次のとおりとなった(図表 12)。

図表 12 安全管理措置の取組（技術的安全管理措置）（各項目に対して単一選択）



この結果、「絶対に必要である(必須)」との回答が多かった項目として、「特定個人情報ファイルを機器又は電子媒体等に保存する必要がある場合、原則として、不正に入手した者が容易に復元できないように、暗号鍵及びパスワードの運用管理、パスワードに用いる文字の種類や桁数等の要素を考慮する等、暗号化又はパスワードにより秘匿する」が 31.7%、「特定個人情報等をインターネット等により外部に送信する場合、通信経路の暗号化等、通信経路における情報漏えい等を防止するための措置」が 30.2%、「個人番号利用事務において使用する情報システムについて、インターネットから独立する等の高いセキュリティ対策を踏ま

えたシステム構築や運用体制整備」が29.8%となっていた。そのため、暗号化又はパスワードによる秘匿化や通信経路における情報漏えい等を防止するための措置、高いセキュリティ対策を踏まえたシステム構築や運用体制整備などの対応が求められていることが明らかとなった。

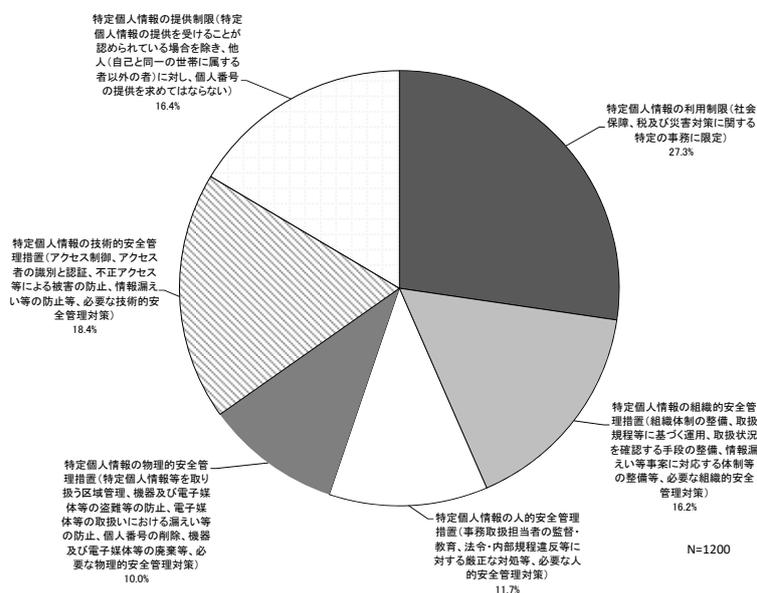
なお、平成27年度に実施した地方自治体アンケートでは、「特定個人情報ファイルを機器又は電子媒体等に保存する必要がある場合に暗号化又はパスワードにより秘匿する」の実施済みで69.8%など、多くの地方自治体で十分な取り組みとなっている実態が明らかとなっており、ネットユーザとの差が生じていないことが明らかとなった。

3-4 安全管理措置の優先度と今後必要な安全管理措置の取組について

(1) 安全管理対策の優先度

地方自治体などの行政機関において、番号制度における特定個人情報の適正な取扱いを確保するための安全管理措置として、最も重要な対応策について尋ねると、次のとおりとなった(図表13)。

図表13 安全管理対策の優先度(単一選択)



この結果、「特定個人情報の利用制限(社会保障、税及び災害対策に関する特定の事務に限定)」との回答が27.3%、「特定個人情報の技術的の安全管理措置(アクセス制御、アクセス者の識別と認証、不正アクセス等による被害の防止、情報漏えい等の防止等、必要な技術的の安全管理対策)」との回答が18.4%ということで、特定の事務への限定や必要な技術的の安全管理対策が求められていることが明らかとなった。

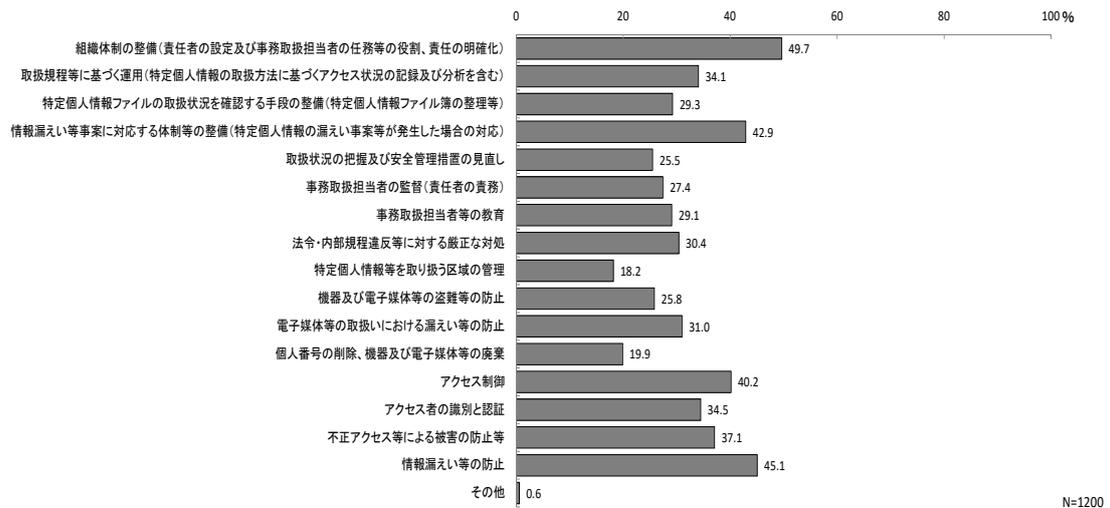
(2) 今後必要な安全管理措置の取組

地方自治体などの行政機関において、特定個人情報の適正な取扱いを確保するための安全管理措置として、今後、どのような対策が重要について尋ねると、次のとおりとなった(図表14)。

この結果、「組織体制の整備(責任者の設定及び事務取扱担当者の任務等の役割、責任の明確化)」との回答が49.7%、「情報漏えい等の防止」との回答が45.1%、「情報漏えい等事案に対応する体制等の整備(特定個人情報の漏えい事案等が発生した場合の対応)」との回答が42.9%、「アクセス制御」との回答が40.2%となっていた。このことから、ネットユーザにおいては「組織的の安全管理措置」や「技術的の安全管理措置」に対する対応が求められていることが明らかとなった。

なお、平成27年度に実施した地方自治体アンケートでは、事務取扱担当者等の教育や取扱規程等に基づく運用、さらに情報漏えい等の防止、組織体制の整備といった対策が必要となっている実態が明らかとなっており、地方自治体においてもネットユーザにおいても、ほぼ同様の対策の必要性を感じていることが明らかとなった。

図表 14 今後必要な安全管理措置の取組（複数選択）



4 まとめと提言

(1) 番号制度の導入後におけるセキュリティ対策に対する実態的評価

本研究では、番号制度の導入を前提に、個人番号その他の特定個人情報に対する適正な取扱いとしての情報セキュリティ対策として、「特定個人情報の適正な取扱いに関するガイドライン」で示された安全管理対策の取り組み評価が可能な指標化を行い、平成 27 年度に実施した地方自治体アンケートにも採用した図表 2 で示されている項目を 39 項目に対して 6 段階評価を行うこととした。そのうえで、番号制度を利用する可能性の高い国内ネット利用者（ネットを利用する住民）を対象に WEB アンケート調査を実施し、特定個人情報に関する安全管理措置の実態や取組課題や今後必要な取組について考察することとした。

その結果、番号制度を認識している割合が 6 割を超える一方で、番号制度に対してプライバシーの侵害や不正利用に対する被害といった不安を感じている割合も 6 割を超えていたことが明らかとなった。このため、更なる番号制度に対する不安の解消に努める必要がある。

また、特定個人情報に関する安全管理措置として、技術的安全管理措置における暗号化又はパスワードにより秘匿などはネットユーザからの必要性も高く地方自治体における対応も進んでいることから、その差が見られることがなかったものの、人的安全管理措置における各課の担当者に対する研修や物理的な安全管理措置における容易に個人番号が判明しないよう安全な方策に対するネットユーザからの必要性に対して、具体的な等が不十分な地方自治体が多い実態が明らかとなっており、ネットユーザとの差が生じていることが明らかとなった。

(2) 今後の展望に向けて

平成 28 年度に実施した WEB アンケート調査では、今後必要な安全管理措置として、ネットユーザにおいて「特定個人情報の利用制限」を前提とした「組織的安全管理措置」や「技術的安全管理措置」に対する必要性が求められていることが明らかとなった。一方、平成 27 年度に実施した地方自治体アンケートでも、今後必要な安全管理措置の取り組みとして、取扱担当者等の教育や取扱規程等に基づく運用、さらに情報漏えい等の防止、組織体制の整備といった対策が挙げられており、すでに多くの地方自治体では十分な取り組みとなっている実態があることから、特に組織的安全管理措置の重要性を指摘することができる。そのため、今後、取扱担当者等の教育を浸透させるとともに、責任者の設定及び事務取扱担当者の任務等の役割、責任の明確化といった組織体制の整備が求められていることが明らかとなった。

そのため、こうした地方自治体の技術的な対策のみならず、組織体制の整備といった取り組みを行うことこそが、住民の理解が得られるセキュリティ対策を検討することが可能となるものと考えられる。そこで、今後の研究としては、こうした取り組みの実効性のある地方自治体に対する支援策などについて探求していくことで、番号制度の円滑な実施と安全管理対策の取り組みに寄与していきたい。

【参考文献】

宇賀克也(2009)『個人情報保護の理論と実務』有斐閣

宇賀克也、水町雅子、梅田健史(2013)『完全対応 自治体職員のための番号法解説』第一法規

宇賀克也、水町雅子、梅田健史(2014)『施行令完全対応 自治体職員のための番号法解説【制度編】』第一法規、年
大山水帆(2015)『どうなるどうする自治体マイナンバー対応』ぎょうせい

神奈川県厚木市(平成 27 年 11 月)「厚木市社会保障・税番号制度を適正に運用するための指針」

黒田充(2016)『マイナンバーはこんなに恐い! 国民総背番号制が招く“超”監視社会』日本機関紙出版センター

個人情報保護委員会(2014 年 12 月 18 日)『特定個人情報の適正な取扱いに関するガイドライン(行政機関等・地方公共団体等編)(本文及び(別添)特定個人情報に関する安全管理措置)』(2016 年 4 月 1 日一部改正)

個人情報保護委員会「平成 29 年度 年次報告」2017 年

埼玉県白岡市(平成 27 年 12 月)「特定個人情報の適正な取扱いに関する事務処理方針」

総務省(2013 年 8 月)「地方公共団体における番号制度の導入ガイドライン」(地方公共団体における番号制度の活用に関する研究会)

総務省(平成 27 年 12 月 25 日)「新たな自治体情報セキュリティ対策の抜本的強化について(総行情第 77 号)」

総務省(平成 29 年 5 月 19 日)「地方公共団体が保有するパーソナルデータに関する検討会報告書」

内閣官房社会保障改革担当室「社会保障・税番号制度」(<http://www.cas.go.jp/jp/seisaku/bangoseIDo/>)
内閣官房社会保障改革担当室・内閣府大官房番号制度担当室「マイナンバー概要資料」2016年8月版
内閣府大臣官房番号制度担当室(2014年5月12日)「行政手続における特定の個人を識別するための番号の利用等に関する法律(番号法)【逐条解説】」
瀧口樹良「迷走する番号制度」時事通信出版局、2017年4月

〈発 表 資 料〉

| 題 名 | 掲載誌・学会名等 | 発表年月 |
|---|----------------|----------|
| 湯浅塾道「地方公共団体における官民データ活用の法的課題」 | 情報法制研究(第2号)有斐閣 | 2017年11月 |
| 瀧口樹良「番号制度の導入を踏まえた地方自治体の個人データの利用と保護対策のあり方」 | 時事通信出版局 | 2018年6月 |