

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

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	(株)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・事故も起き続け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）」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、L G W A N 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じることなどが提言されている。

しかしながら、地方自治体の現場実態として、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は、そうしたセキュリティ対策がおろそかとなりがちで、机上の空論とまではいかないものの、より実態に即した評価を踏まえた対策を検討することが求められている。

そこで本研究では、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の実態を把握し、全国の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提言するものである。

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位置づけ

個人番号等を含む個人情報である特定個人情報は、「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」（以下「番号法」という）の個人番号利用事務実施者等の責務である「個人番号の漏えい、滅失または毀損の防止その他の個人番号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（番号法第 12 条および第 31 条）」との規定に基づくことになる。そしてこれは、前述した個人情報保護委員会が示した「ガイドライン」を踏まえ、保有する特定個人情報の適正な取り扱いを確保するために必要な安全管理措置を地方自治体として行う必要がある。

すでに地方自治体では、個人情報の保護に関する条例等で、各種の個人情報に関する保護措置が定められていることから、ガイドラインでは、番号法において特定個人情報の適正な取り扱いを確保するために必要な措置を講ずるもの（番号法第 4 条および第 5 条）とし、行政機関等および地方自治体に対して、特定個人情報に限定した適正な取り扱いを確保するため、主体的に特定個人情報の保護のための取り組みを行うための具体的な指針を定めたものと位置付けられる。一般的に法律は条例に対して優先して適用されることから、特定個人情報に関する番号法の特例規定は、地方自治体の個人情報の保護に関する条例等の規定に対して優先して適用される。

一方、特定個人情報に関し番号法に特段の規定がない事項については、地方自治体の個人情報の保護に関する条例等の規定が適用される。ただし、地方自治体等が保有する特定個人情報の適正な取り扱いを確保し、また地方自治体等が保有する特定個人情報の開示、訂正、利用の停止、消去および提供の停止を実施するため、必要な措置を講ずるもの（番号法第 31 条）としていることから、これらに対応するため、地方自治体の個人情報の保護に関する条例等の改正が必要となる。

また、地方自治体等では、個人のプライバシーの権利利益に影響を与え得る特定個人情報の漏えいその他の事態を発生させるリスクを軽減するための措置として特定個人情報保護評価書に記載した全ての措置を講ずることが求められる。

なお、番号法では、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られており、具体的には「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」および「特定個人情報の提供制限等」の三つに大別された保護措置が示されている。また、安全管理措置としては、組織的、人的、物理的、技術的といった四つの観点から成る安全管理措置が求められている。

2-2 特定個人情報に対する安全管理措置の概要

(1) 個人番号の原則的な取り扱い

個人番号を含む特定個人情報は、番号法が予め限定的に定めた事務の範囲の中から、具体的な利用目的を特定した上で、利用するのが原則である。従って、たとえ本人同意があったとしても、次の例外として認められる場合を除き、番号法が予め限定的に定めた事務の範囲以外で、個人番号および特定個人情報を利用することができないものと考えられる。

【例外として認められる場合】

- ①金融機関に該当する独立行政法人等が激甚災害時等に金銭の支払を行う場合（番号法第 9 条第 4 項、第 29 条第 2 項により読み替えて適用される独立行政法人等個人情報保護法第 9 条第 1 項、番号法施行

令第10条)

- ②人の生命、身体または財産の保護のために必要がある場合であって、本人の同意があり、または本人の同意を得ることが困難である場合（番号法第29条第1項または第2項により読み替えて適用される行政機関個人情報保護法第8条第2項第1号または独立行政法人等個人情報保護法第9条第2項第1号）

従って、番号法が予め限定的に定めた事務の範囲として個人番号利用事務等を特定し、さらに、その特定された事務等に対して使用される個人番号および個人番号と関連付けて管理される氏名、生年月日等の個人情報を含む特定個人情報等の対象範囲を明確にする必要がある。

（2）組織体制の整備

特定個人情報等の取り扱いは組織体制を整備する必要がある。具体的には、総括責任者および監査責任者を定めて、各部署の個人番号等の特定個人情報を取り扱う保護責任者および事務取扱担当者を特定し、特定個人情報等の取り扱いに対する責任の所在を明確にすることが必要である。なお、総括責任者は、保護責任者に対して、部署内における特定個人情報等の適正な管理のために必要な教育研修を行うことが求められる。

【組織体制の構成例】

①保護責任者（各部署の所属長）

特定個人情報等の取り扱いが適正に行われるよう、事務取扱担当者に対して必要かつ適切な監督を行うことが求められる。

そのため、事務取扱担当者に対して特定個人情報等の適正な取り扱いに関する理解を深めるための必要な教育研修を行うことが必要である（教育研修への参加機会の提供）。

②事務取扱担当者（現場担当者）

特定個人情報等の適正な取り扱いに関する理解を深めるための教育研修を受講することが求められる。また、予め事務取扱担当者が取り扱う特定個人情報等の範囲を明確にする必要がある。

なお、特定個人情報等を複数の課で取り扱う場合には、各課の任務分担および責任の範囲を明確にする必要がある。また、事務取扱担当者等が特定個人情報の適正な取り扱いに違反している事実や違反している予兆を把握した場合、および個人番号の漏えい、滅失または毀損等の事案が発生または発生する予兆を把握した場合には、事務取扱担当者を含めた地方自治体職員から保護責任者等に対して、速やかに報告等の連絡を行う体制を整えることも必要となる。法令または内部規定等に違反した地方自治体職員に対しては、法令または内部規定等に基づき厳正に対処することが求められる。

（3）特定個人情報ファイルの取り扱い状況を確認する手段の整備

個人番号をその内容に含む個人情報ファイルである特定個人情報ファイルの取り扱い状況を確認する手段を整備するため、次の項目を参考にしつつ特定個人情報ファイルの届け出等を求め、「特定個人情報ファイル簿」といった形の帳簿として整備することが求められる。ただし、取り扱い状況を確認するための記録等において、具体的な特定個人情報等の内容を記載することは認められない。

【特定個人情報ファイルの届け出等の項目例】

(ア) 特定個人情報ファイルの名称

(イ) 特定個人情報ファイルが利用に供される事務を取り扱う組織の名称

(ウ) 特定個人情報ファイルの利用目的

(エ) 特定個人情報ファイルに記録される項目および本人として特定個人情報ファイルに記録される個人の範囲（市民の対象範囲）

(オ) 特定個人情報ファイルに記録される特定個人情報等の収集方法

(カ) 特定個人情報ファイルに記録される特定個人情報等の保管・管理方法

(キ) 特定個人情報ファイルに記録される特定個人情報等の削除・廃棄方法

なお、多くの地方自治体では、個人情報の保護に関する条例等に基づき、地方自治体が保有する個人情報を含む情報の集合体であって、一定の事務の目的を達成するために特定の保有個人情報を容易に検索できる

ように体系的に構成した個人情報ファイルに対して、ファイル名称やファイル利用目的、担当の組織、記録項目、情報の収集方法、提供先（提供先がある場合）等を記載した帳簿として「個人情報ファイル簿」を整備し、一般の閲覧に供するとともに、インターネット等を通じて公表している。このため、多くの地方自治体がすでに整備している「個人情報ファイル簿」との整合性を確保する必要がある。

（４）危機管理等に向けた体制の整備

情報漏えい等の事案の発生または発生する予兆を把握した場合に備えて、適切かつ迅速に対応するための体制および手順等を整備することが必要である。特に、情報漏えい等の事案が発生した場合には、二次被害の防止、類似事案の発生防止等の観点から、事実関係および再発防止策等を早急に公表することが重要となる。

具体的には、情報漏えい等の事案の発生時には、違反の事案または番号法違反の恐れのある事案が発覚した場合の対応について委員会が定めた「独立行政法人等及び地方公共団体等における特定個人情報の漏えい事案等が発生した場合の対応について（2015年特定個人情報保護委員会告示第1号）」を踏まえ、次のような対応を行うことを念頭に、体制および手順等を整備することが求められる。特に、不正アクセス、ウイルス感染の事案に加え、標的型攻撃等の被害を受けた場合の対応について、関係者において定期的な確認または訓練等を実施することが必要である。

【情報漏えい等の事案の発生時の対応例】

- (ア) 情報漏えい等の事案が発覚した際の報告・連絡等
- (イ) 事実関係の調査および原因の究明
- (ウ) 影響を受ける可能性のある本人への連絡
- (エ) 委員会（第三者機関）および主務大臣等への報告
- (オ) 再発防止策の検討および決定
- (カ) 事実関係および再発防止策等の公表
- (キ) 特定個人情報保護評価（PIA）の見直し

特に重大事態に該当する事案またはその恐れのある事案が発覚した時点で、直ちにその旨を委員会に報告することや、事案の内容等に応じて、二次被害の防止、類似事案の発生回避等の観点から、事実関係および再発防止策等について、速やかに公表することが重要となる。さらに、二次被害の防止、類似事案の発生回避等の観点から、事実関係等について、速やかに、本人へ連絡し、または本人が容易に知り得る状態に置くことも考慮することが求められる。

（５）監査および安全管理措置等の見直し措置

監査責任者は、特定個人情報の管理の状況について、定期および必要に応じ随時に点検または内部・外部監査等の監査を行い、その結果を総括責任者に報告することが必要である。その際、総括責任者は、点検または監査の結果等を踏まえ、必要があると認めるときは、特定個人情報の安全管理措置等の見直し措置を行うことが求められる。

なお、監査の前提条件として、地方自治体職員が特定個人情報の取り扱いや持ち出しといった状況を記録し、その記録を一定の期間保存し、定期にまたは随時に分析することや、記録の改ざん、窃取または不正な削除の防止等の必要な措置を行うなど、運用状況を可視化し、庁内で把握しておくことが重要である。

（６）特定個人情報の安全管理措置と各種規定との整合性の確保

特定個人情報等の適正な取り扱いの確保については、組織全体として取り組む必要があるため、ガイドラインでは、特定個人情報等の安全管理に関する基本方針を策定するのが重要であることが示されている。その上で、地方自治体の個人情報の保護に関する条例等に基づく規定等を見直しを図り、特定個人情報等を取り扱う体制の整備および情報システムの改修等を行う必要があることが示されている。

ただし、番号法、行政機関個人情報保護法および地方自治体の個人情報の保護に関する条例等関係法令、ガイドライン、「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（2004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（同年9月14日総管情第85号総務省行政管理局長通知）」および「地方公共団体における個人情報保護対策について（2003年6月16日総行情第91号総務省政策統括官通知）」とい

った指針等および政府機関の情報セキュリティ対策のための統一基準や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等に準拠した地方自治体におけるセキュリティポリシー等を順守することが前提となる。また地方自治体では、特定個人情報保護評価を実施した事務については、その内容を順守する必要がある。また、個人番号利用事務の実施に当たり、接続する情報提供ネットワークシステム等の接続規定が示す安全管理措置を順守することも前提となる。

このため、地方自治体では、個人番号を含む特定個人情報に関する取得、利用・提供、保存・管理、削除・廃棄を行う各段階の事務処理の流れを整理し、具体的な取り扱いを定めるため、前述した前提を踏まえた取り扱い規定について、全庁的な考え方やルールとして新たに事務処理方針等を策定するか、既存の地方自治体におけるセキュリティポリシーまたは地方自治体の個人情報の保護に関する条例等の規定を見直すといった方法が考えられる。

特に、新たに事務処理方針等を策定している事例としては、神奈川県厚木市の「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(2)」や、埼玉県白岡市の「特定個人情報の適正な取扱いに関する事務処理方針(3)」等が挙げられる。ただし、全庁的な考え方やルールとして新たに事務処理方針等を策定した場合には、既存の地方自治体におけるセキュリティポリシーまたは地方自治体の個人情報の保護に関する条例等に基づく規定との整合性を考慮することが求められる。例えば、白岡市の「特定個人情報の適正な取扱いに関する事務処理方針」では、対象となる事務処理を、特定個人情報に関するものと限定した上で、当該事務処理を除く個人情報等の事務処理の安全管理措置については、セキュリティポリシーに定めることが示されている。特に技術的安全管理措置については、特定個人情報に関するものであっても、セキュリティポリシーに準拠して行われることが求められている。

このことは、例えば特定個人情報等の複製および送信、特定個人情報等が保存されている電子媒体等の外部への送付および持ち出し等については、責任者の指示に従い行うと定めること等が重要となる。ただし、こうした取り扱いについても、セキュリティポリシーまたは地方自治体の個人情報の保護に関する条例等に基づく規定とは異なる取り扱いを定めることは、かえって地方自治体職員に負荷を課すことになり、さらに混乱を招きかねない。

また、例えばセキュリティポリシーに準拠して行われる監査と特定個人情報の安全管理措置に伴う監査を別々に行うことは、業務負荷を強いることにもなり、地方自治体経営の観点から現実的でもないため、整合性を保った上で、整理・統合した形で安全管理措置を実施することが求められる。このため、庁内における個人番号が含まれる特定個人情報の扱い方の統一化を図りつつ、既存のセキュリティに関する各種規法定との整合を図る必要がある。

2-3 番号法と個人情報保護条例との関係

(1) 特定個人情報に対する個人情報保護条例の位置づけ

番号法は、一般法の特例を規定した特別法であることから、個人番号を含む特定個人情報の取り扱いに関する番号法の規定は、一般法の規定に優先して適用される。一方、特定個人情報に関して番号法に特段の規定がない事項については、一般法の規定が適用される。また、一般に法律は条例に優先して適用されることから、特定個人情報に関する番号法の特例規定は、地方自治体の個人情報保護条例の規定に優先して適用される。一方、特定個人情報に関して番号法に特段の規定がない事項については、地方自治体の個人情報保護条例の規定が適用される。

さらに、番号法により行政機関個人情報保護法および独立行政法人等個人情報保護法の規定を読み替えて適用することとされている部分があること等を踏まえ、番号法では「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、個人情報保護法及びこの法律の規定により講ずることとされている措置の趣旨を踏まえ、保有する特定個人情報の適正な取扱いが確保され、並びに当該地方公共団体が保有する特定個人情報の開示、訂正、利用の停止、消去及び提供の停止を実施するために必要な措置を講ずるものとする(第31条)」と規定されていることから、これらに対応するため、地方自治体では個人情報保護条例の改正等が必要となる場合がある。

また、番号法における特定個人情報の保護に関する規定は、地方自治体に対しても適用されることとなるが、「行政機関個人情報保護法等の特例(第29条)」および「情報提供等記録についての特例(第30条)」の規定に対しても、行政機関個人情報保護法や個人情報保護法等の読み替えとして規定されているものについて地方自治体の個人情報保護条例に適用されるものではないため、その趣旨に沿って個人情報保護条例の改正等の対応が必要となる場合もある。

なお、地方自治体の個人情報保護条例の改正等については、次のような対応が考えられるが、実際に特定個人情報を保有する 2015 年 10 月までに条例を整備する必要があり、すでに多くの地方自治体では個人情報保護条例の改正等が行われている。

- ① 現行の個人情報保護条例に特定個人情報の保護に関する規定を新規に追加する改正を行う（既存条例の改正方式）。
- ② 現行の個人情報保護条例の規定に読み替え規定を置き、特定個人情報の保護に関する規定を追加する改正を行う（既存条例の読み替え方式）。
- ③ 「特定個人情報の保護に関する条例」を新規に制定する（新設条例方式）。

上記のうち、多くの地方自治体では、①または②の方式を採用し、特定個人情報の保護に関する規定を追加する既存条例の一部改正等を行うことで対応している。一方、③の方式を採用している地方自治体は、東京都である(1)。東京都では、個人番号および特定個人情報は、個人情報保護条例における一般的な個人情報とは取り扱いが大きく異なることや個人情報保護条例における個人情報の定義は、番号制度における個人情報の定義よりも範囲が広いことから、既存の個人情報保護制度に混乱を生じさせるような現行条例の大幅な改正による対応は、必ずしも適切ではないと判断した。そこで、個人情報保護条例の特例を設けることとし、その特例について明らかにする必要があることから、特定個人情報の保護に係る新たな条例等を制定するとともに、現行の東京都の個人情報保護条例等についても、必要に応じて関係する規定を改正する等により番号制度に係る条例等の整備を行っている。

（２）改正等すべき個人情報保護の具体的な規定

番号法（第 31 条）の規定に基づき、行政機関等と同様の適用となるよう、地方自治体の個人情報保護条例の改正等すべき具体的な規定は、以下の通りである。

ア．「特定個人情報」の定義等の追加による条例改正等

地方自治体の個人情報保護条例における「個人情報」の定義は、「事業を営む個人の当該事業に関する情報、法人その他の団体に関する情報に含まれる当該法人その他の団体の役員に関する情報を除く」等の除外規定を設けている場合がある。従って、特定個人情報については、当該除外部分を含めて保護の対象となるよう、番号法（第 2 条第 8 項）に規定する「特定個人情報」の定義を追加する等が必要になる。

イ．番号法第 29 条、第 30 条に対応した条例改正等

番号法第 29 条、第 30 条に対応すると、次の事項について追加する等が必要になる。

① 利用目的以外の目的での利用に関する規定

特定個人情報は、利用目的以外の目的での利用について、通常の個人情報よりもさらに厳格に利用が許容される例外事由を限定する必要がある。また、情報提供等記録については、利用目的以外の目的での利用が想定されないため、利用目的以外の目的での利用を禁止する必要がある。

② 提供の制限に関する規定

番号法において特定個人情報を提供することができる場合は、番号法（第 19 条各号）に掲げられた場合に限定されているため、個人情報保護条例上も特定個人情報を提供できる場合を同条各号に掲げられた場合に制限する必要がある。また、オンライン結合を制限する規定が条例上置かれている場合、番号法（第 19 条各号）に掲げられた場合には、オンライン結合を可能とすることが必要な場合がある。

③ 開示・訂正・利用停止に関する規定

特定個人情報についてはその性格から、本人の関与についてより一層の保護が必要であると考えられることから、本人および法定代理人に加え任意代理人に対しても開示請求および訂正請求を行うことを認める必要がある。

④ 利用停止の請求の条件に関する規定

番号法では、特定個人情報について、番号法に違反する行為のうち特に不適切なものが行われた場合にも利用停止請求を認めているため、個人情報保護条例においても同様の措置を講ずる必要がある。なお、情報提供等記録については、システム上、自動保存されるものであり、利用制限等に違反する取り扱いが想定されないため、利用停止請求を認めないことを規定する必要がある。

⑤ 開示手数料の減免に関する規定

経済的な理由等によらずに、各個人が特定個人情報を容易に確認できるようにするため、開示手数料の減額または免除の措置を講ずる必要がある。

⑥他の条例による開示実施との調整に関する規定

他の条例等により同一の方法の開示が定められている場合に調整規定を設ける場合があるが、情報提供等記録開示システム（マイナポータル）による情報開示の方が、より市民の利便性が高い場合も想定されることから、他の法令等により同一の方法の開示が定められている場合でも、重ねて番号法に基づくマイナポータルを通じた開示を可能とする必要がある。

⑦開示・訂正時の移送に関する規定

情報提供等記録については、他機関で開示等の決定をする場合が想定されないため、移送に関する手続きを適用除外とする必要がある。

⑧訂正の通知先に関する規定

情報提供等記録は情報の照会者、提供者および情報提供ネットワークシステムを管理する総務大臣において記録・保管されるものであり、訂正した際にもこれらの主体に通知することとする必要がある。

⑨その他の規定

地方自治体の個人情報保護条例の実態に即して、特定個人情報および情報提供等記録の定義等必要な条項を追加する必要がある。また、特定個人情報は、番号法（第 19 条各号）により明確に提供できる場合が制限されるため、措置要求については適用除外とする必要がある。

ウ．特定個人情報の適正な取り扱いの確保を行うための条例改正等

安全管理措置として、個人番号利用事務等実施者は、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）の漏えい、滅失または毀損の防止その他の個人番号の適切な管理のために必要な措置を講ずることや、保有する個人情報である特定個人情報の漏えい、滅失または毀損（ルビ：きそん）の防止その他の保有個人情報の適切な管理のために必要な措置を講ずることを追加する等が必要になる。この他、利用目的の特定、保有の制限、利用目的の変更、利用目的の明示、保有する個人情報の正確性の確保等について、番号法（第 31 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。

（3）その他、地方自治体の条例改正または新たな制定が求められる事項

番号法では、これまで解説してきた個人情報保護条例等の改正または新たな制定の他、地方自治体では、次のような特定個人情報の利活用のための条例の改正等を行うことが必要となる場合がある。

ア．利用事務（番号法第 9 条第 2 項）

- ・番号法別表第 1 に規定されていない地方自治体の独自事務に利用する場合
- ・同一地方自治体の同一機関内における複数の事務間で特定個人情報を移転する場合
- ・当該独自事務の根拠となる条例において書面の提出を義務付けている場合に、上記の特定個人情報の移転により、当該特定個人情報と同一の内容の情報を含む書面の提出を不要とする場合

イ．提供制限（番号法第 19 条第 9 号）

- ・同一地方自治体内における他の機関に特定個人情報を提供する場合
- ・独自事務に個人番号を利用し、当該独自事務の根拠となる条例において書面の提出を義務付けている場合に、上記の同一地方自治体内における特定個人情報の提供を受けることにより、当該特定個人情報と同一の内容の情報を含む書面の提出を不要とする場合

ウ．個人番号カードの利用（番号法第 18 条）

- ・地方自治体が市民の利便性の向上に資するものとして条例で定める事務で利用する場合

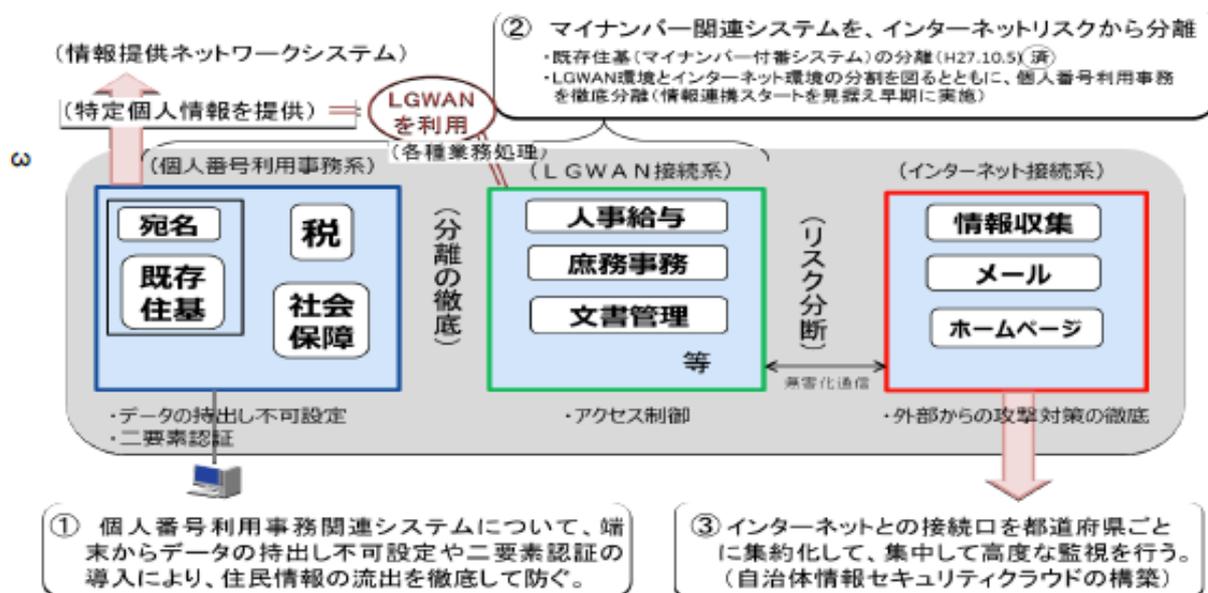
2-4 地方自治体における情報セキュリティ対策の抜本的強化

個人情報保護委員会のガイドラインとは別に、総務省においても、地方自治体の情報セキュリティに係る抜本的な対策を検討するため、「地方自治体情報セキュリティ対策検討チーム」（座長：佐々木東京電機大学教授）を設置し、平成 27 年 11 月 24 日に、以下の三層からなる対策を講じることにより、早急に各地方自治体の情報セキュリティ対策の抜本的強化を図ることが必要であるとの報告を行っている（4）。

- ① マイナンバー利用事務系では、端末からの情報持ち出し不可設定等を図り、住民情報流出を徹底して防止すること
- ② マイナンバーによる情報連携に活用される LGWAN 環境のセキュリティ確保に資するため、LGWAN 接続系とインターネット接続系を分割すること
- ③ 都道府県と市区町村が協力して、地方自治体情報セキュリティクラウドを構築し、高度な情報セキュリティ対策を講じること

そのため、総務省では、各地方自治体に対して、上記の三層からなる対策を講じるため、平成 27 年度補正予算案（平成 27 年 12 月 18 日閣議決定）において、「地方自治体情報セキュリティ強化対策事業」を計上するなど、各地方自治体の情報セキュリティに係る取組みに対する支援を実施している（図表 1 参照）。

図表 1 自治体情報セキュリティ強化対策事業



(出典：総務省「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）」平成 27 年 12 月 25 日)

3 郵送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「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た(図表2参照)

図表2 郵送アンケートの概要

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	郵送アンケート調査
調査対象	1,788 団体自治体 内訳 都道府県：47 団体、指定都市：20 団体、市：771 団体、特別区：23 団体、町：744 団体、村：183 団体
実施期間	平成 29 年 2 月
回収数	222 団体 (回収率：12.4%)
主な調査項目	問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 問1-1【基本方針等の整備】 問1-2【基本方針等の内容】 問1-3【個人情報保護条例の改正】 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【安全管理措置の取組】 問2-2【安全管理措置の取組課題】 問2-3【今後必要な安全管理措置の取組】

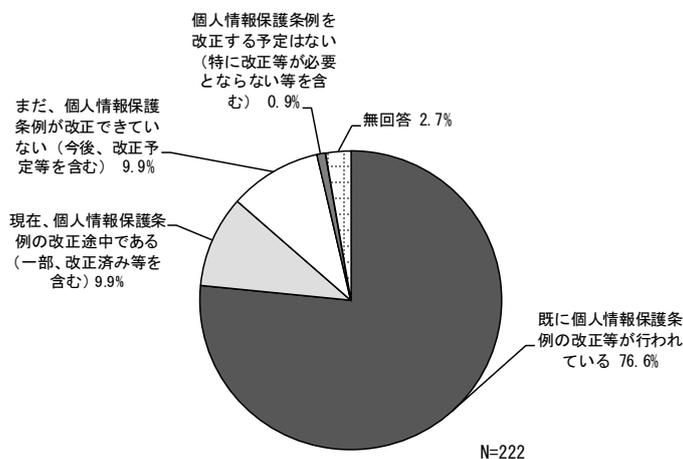
なお、地方自治体の通常の郵送アンケート調査では、3割程度となるが、番号制度の情報連携に向けた取り組みの最中であることや、番号制度の特定個人情報に関する安全管理措置に関して、公開できない項目が複数あるため、回答を控えたいとの返信があった地方自治体もあった。そのため、かなり低い回収率となったが、番号制度の特定個人情報に関する安全管理措置に対する地方自治体の実態としては、十分に明らかとなったものと思われる。

3-2 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

(1) 基本方針等の整備

特定個人情報（個人番号を含む個人情報）の適正な取扱いを確保するための具体的な指針となる個人情報保護委員会から示された「ガイドライン」に基づく、安全管理措置に関する基本方針等が整備され、それに伴う取り組みが行われているかについて尋ねると、次のとおりとなった(図表3参照)。

図表3 基本方針等の整備（単一選択）

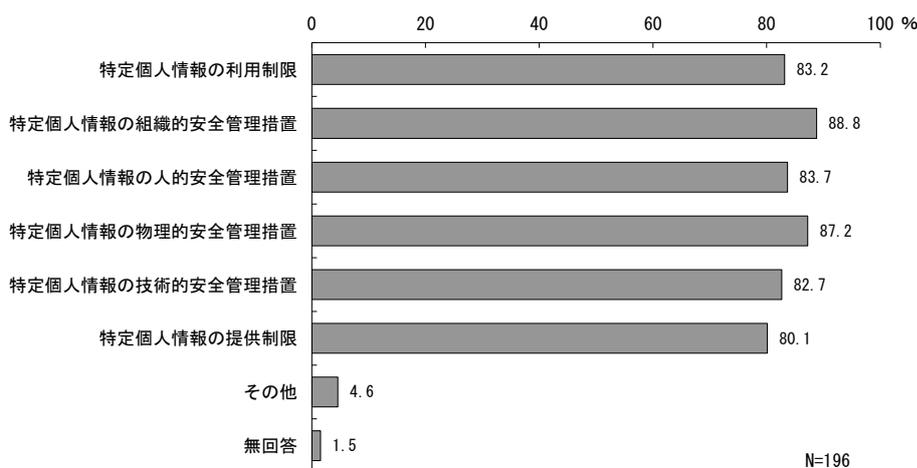


この結果、「既に基本方針等を整備し、それに伴う特定個人情報等を取り扱う体制の整備及び情報システムの改修等が実施されている」との回答が57.2%と6割近くあった。しかしながら、「現在、基本方針等が整備途中である（一部、整備済み等を含む）」が、7.7%、「まだ、基本方針等が整備できていない（今後、整備予定等を含む）」9.9%と、2割弱の地方自治体では、基本方針等の整備ができていない実態が明らかとなった。安全管理対策に関する基本方針等が十分ではない地方自治体が一定数存在している実態が明らかとなった。

(2) 基本方針等の内容

図表3で示した回答のうち、基本方針等を整備に関する内容について尋ねると、次のとおりとなった(図表4参照)。

図表4 基本方針等の内容（複数選択）

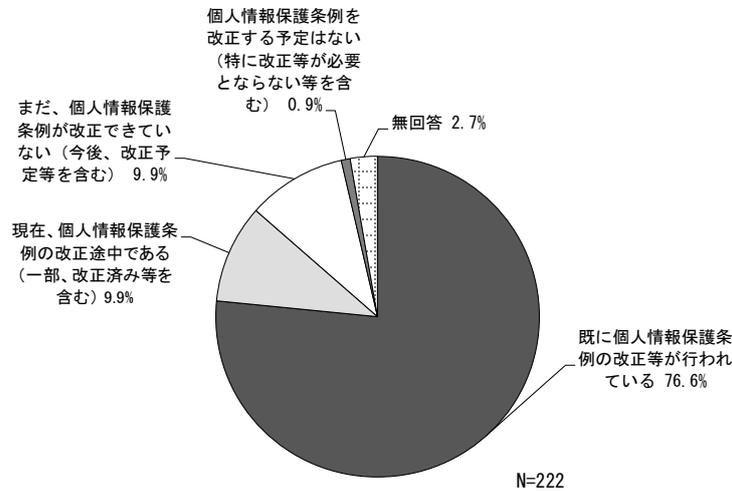


この結果、全ての対応について8割以上の回答となっていたが、組織的及び物理的な安全管理措置に対して、特定個人情報の提供制限の取組の割合が少なくなっており、若干ながらバラつきがあることが明らかとなった。

(3) 個人情報保護条例の改正

番号法第 32 条の規定に基づき、特定個人情報の取扱いとして必要な個人情報保護条例を改正等が行われているかを尋ねると、次のとおりとなった(図表 5 参照)。

図表 5 個人情報保護条例の改正 (単一選択)



その結果、「既に個人情報保護条例の改正等が行われている」と回答が 76.6%と、8 割弱の地方自治体において、すでに条例等の改正が行われているものの、「まだ、個人情報保護条例が改正できていない(今後、改正予定等を含む)」と回答する地方自治体が 9.9%、「個人情報保護条例を改正する予定はない(特に改正等が必要とならない等を含む)」と回答する地方自治体が 0.9%と、1 割近くの地方自治体において、改正等の対応ができていない実態が明らかとなった。

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ガイドラインに従って、以下の項目に対する 39 項目の設問に対する実施状況を把握することにした。なお、廃棄や見直し、対処等、まだ実例がない場合は、その予定でルール化されていることも実施に含めることにした。

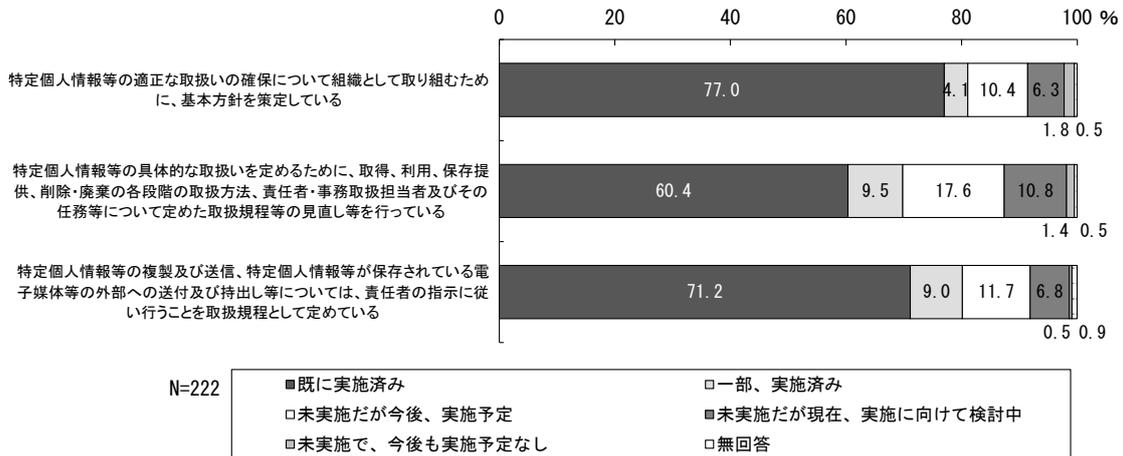
- A 基本方針の策定
- B 取扱規程等の見直し等
- C 組織的安全管理措置
 - a 組織体制の整備
 - b 取扱規程等に基づく運用
 - c 取扱状況を確認する手段の整備
 - d 情報漏えい等事案に対応する体制等の整備
- D 人的安全管理措置
 - a 事務取扱担当者の監督
 - b 事務取扱担当者等の教育
 - c 法令・内部規程違反等に対する厳正な対処
- E 物理的安全管理措置
 - a 特定個人情報等を取り扱う区域の管理
 - b 機器及び電子媒体等の盗難等の防止
 - c 電子媒体等の取扱いにおける漏えい等の防止
 - d 個人番号の削除、機器及び電子媒体等の廃棄
- F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

(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 6 参照)。

図表 6 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割弱の自治体で、「既に実施済み」との回答があったが、「B 取扱規程等の見直し等」の実施状況については、特に「取扱規程等の見直し等」について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た。

(2) 安全管理措置の取組（組織的安全管理措置）

次に、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 7 参照)。

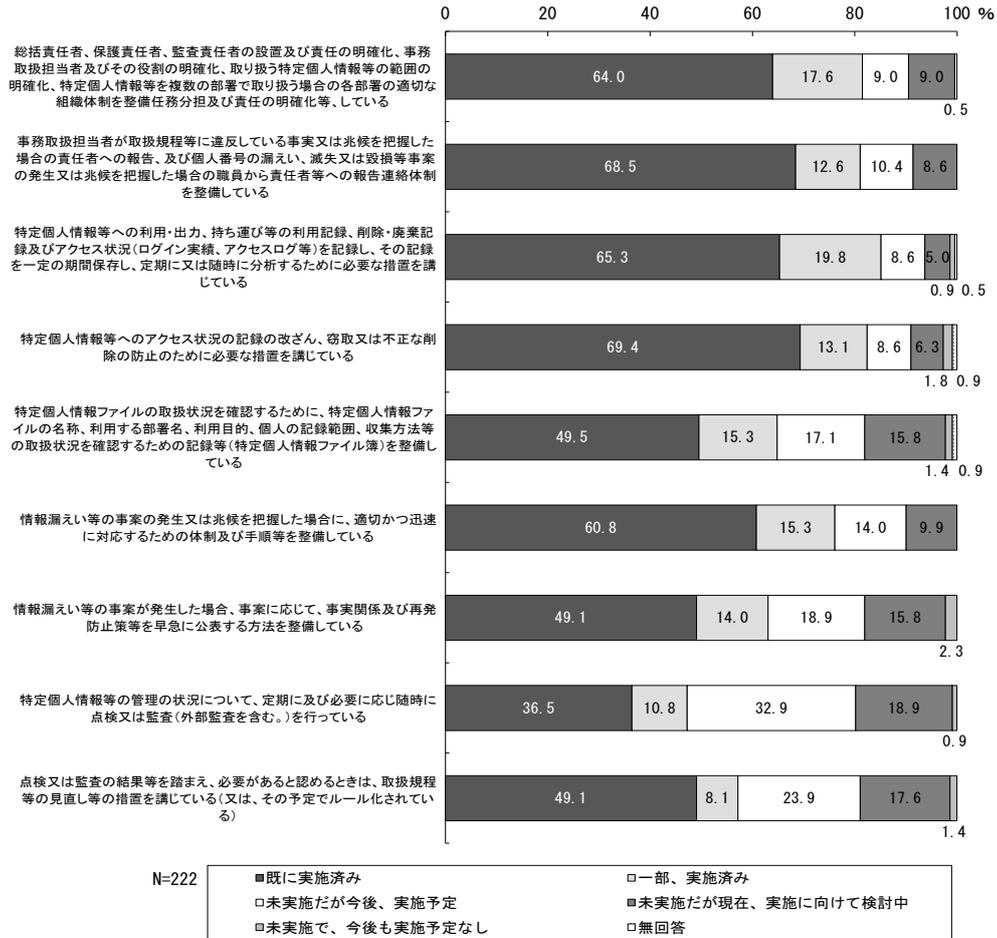
その結果、具体的な取り組みの実施状況にバラつきがあり、特に「特定個人情報ファイルの取扱状況を確認するための記録等（特定個人情報ファイル簿）の整備」の実施済みが 50.0%に留まっており、さらに「情報漏えい等の事案が発生した場合、事案に応じて、事実関係及び再発防止策等を早急に公表する方法の整備」の実施済みが 49.1%、「特定個人情報等の管理の状況について、定期に及び必要に応じ随時に点検又は監査（外部監査を含む。）」の実施済みが 36.5%に留まっていた。このことは、組織的安全管理措置の対応が不十分な地方自治体が多いことが明らかとなった。

(3) 安全管理措置の取組（人的安全管理措置）

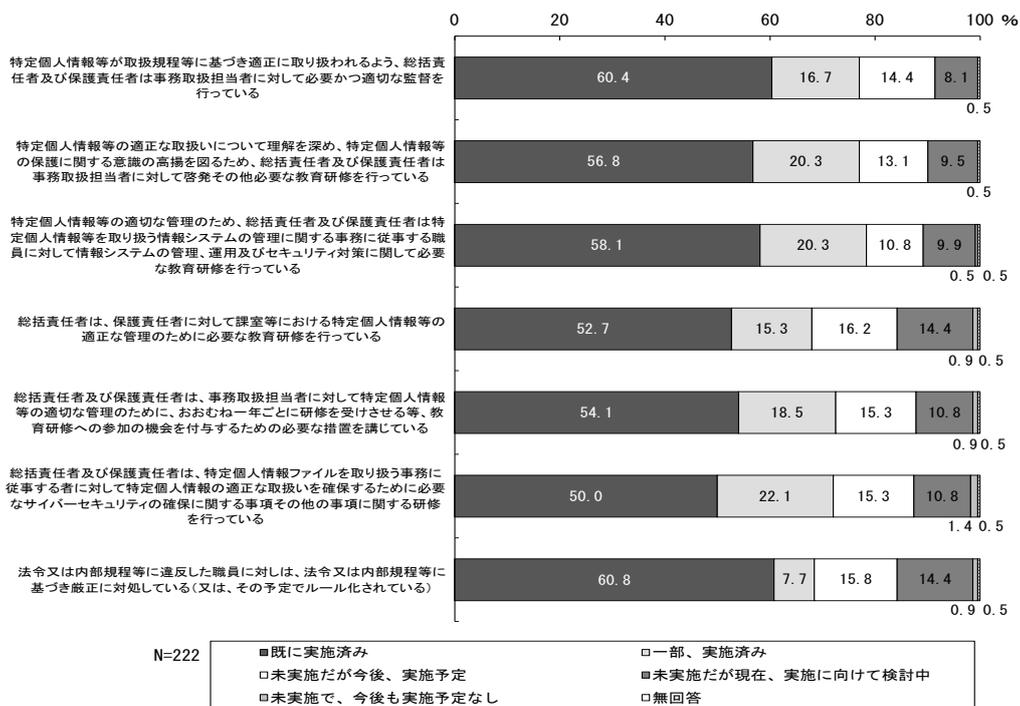
次に、特定個人情報の適正な取扱いを確保するための安全管理措置のうち、「D 人的安全管理措置」の実施状況について尋ねると、次のとおりとなった(図表 8 参照)。

その結果、具体的な取り組みの実施状況にバラつきがあるものの、おおそ各項目で6割程度の割合で実施済みとの回答であった。その中で「保護責任者に対して課室等における特定個人情報等の適正な管理のために必要な教育研修」の実施済みが 52.9%、「サイバーセキュリティの確保に関する事項その他の事項に関する研修」の実施済みが 50.2%に留まるなど、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ことが明らかとなった。

図表7 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）



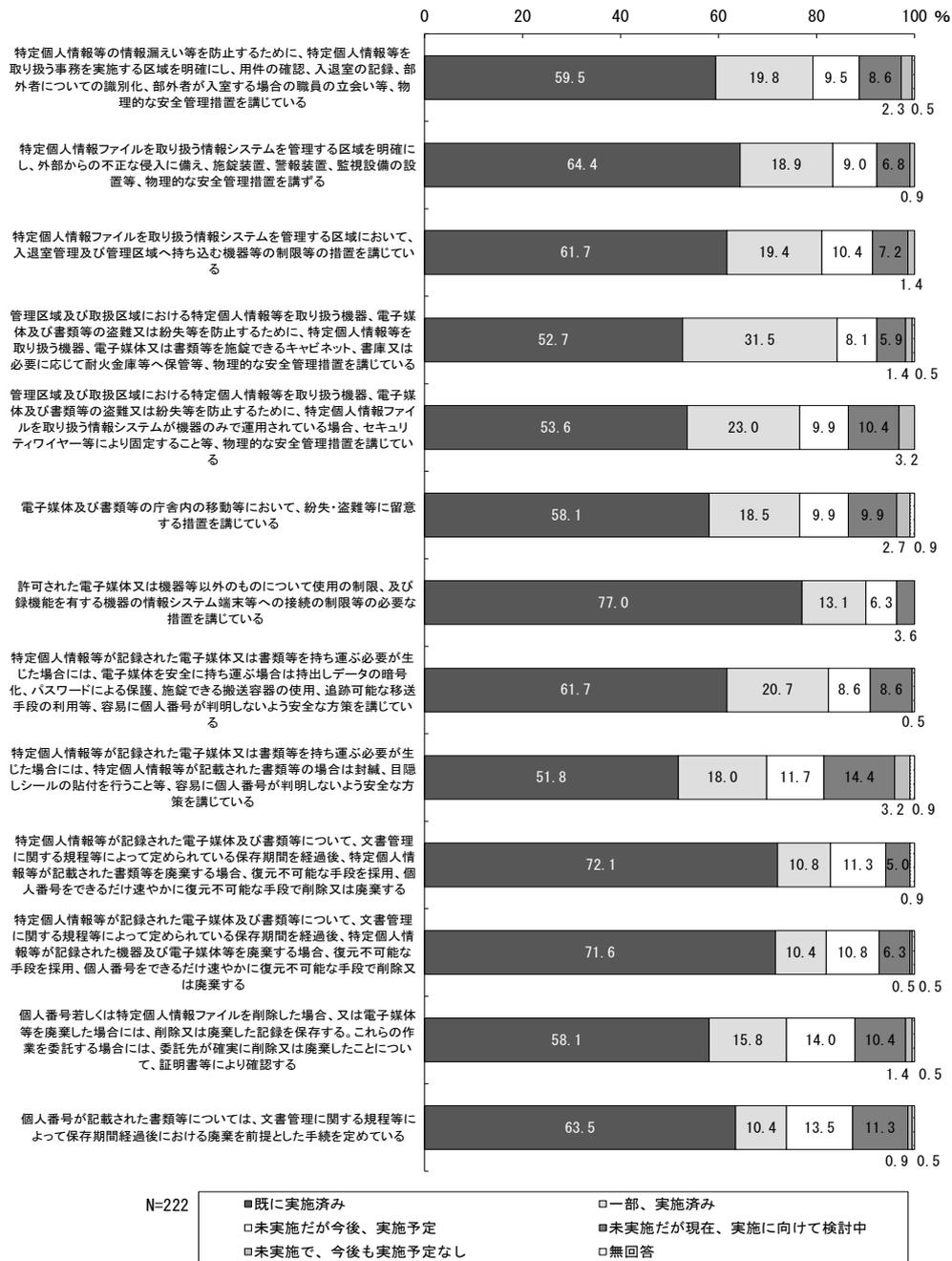
図表8 安全管理措置の取組（人的安全管理措置）（各項目に対して単一選択）



(4) 安全管理措置の取組 (物理的安全管理措置)

次に、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9参照)。

図表9 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)

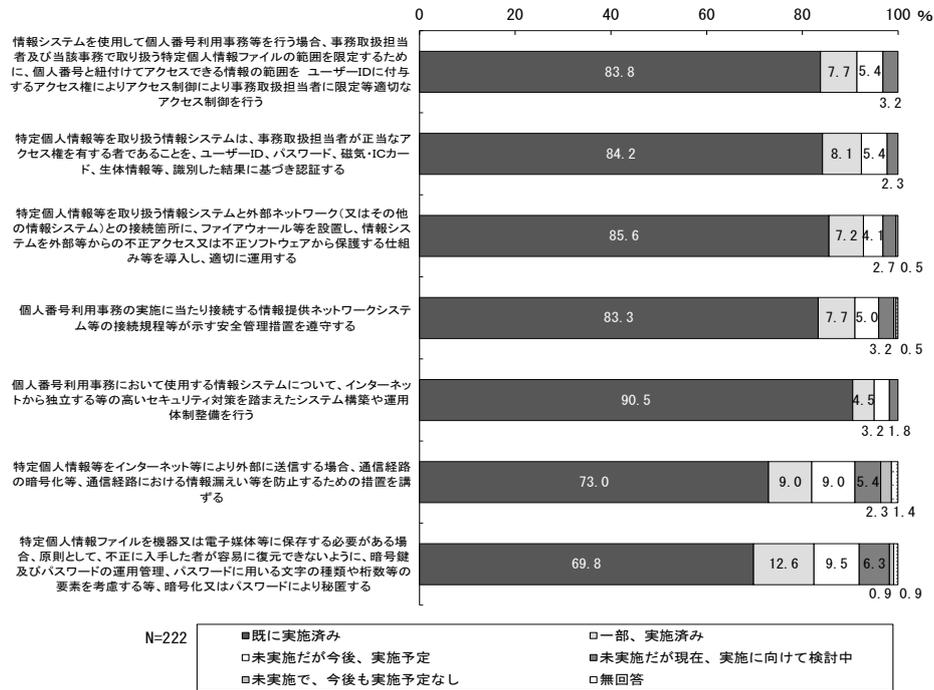


その結果、具体的な取り組みの実施状況にバラつきがあるものの、おおそ各項目で6割程度の割合で実施済みとの回答であった。その中で「特定個人情報等を取り扱う機器、電子媒体又は書類等を施錠できるキャビネット、書庫又は必要に応じて耐火金庫等へ保管等、物理的安全管理措置」の実施済みが52.9%、「特定個人情報ファイルを取り扱う情報システムが機器のみで運用されている場合、セキュリティワイヤー等により固定すること等、物理的安全管理措置」の実施済みが53.6%、「特定個人情報等が記載された書類等の場合は封緘、目隠しシールの貼付を行うこと等、容易に個人番号が判明しないよう安全な方策」の実施済みが51.8%に留まるなど、具体的な物理的安全管理措置の取り組みが不十分な地方自治体が多い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）

次に、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 10 参照)。

図表 10 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）



その結果、他の安全管理措置に比べて、具体的な取り組みの実施状況について7割から8割以上の割合で実施済みとの回答であった。その中で一番少ない割合の項目でも「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た。

3-4 安全管理措置の取組課題と今後必要な安全管理措置の取組について

(1) 安全管理措置の取組課題

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を行うに当たっての課題について尋ねると、次のとおりとなった(図表 11 参照)。

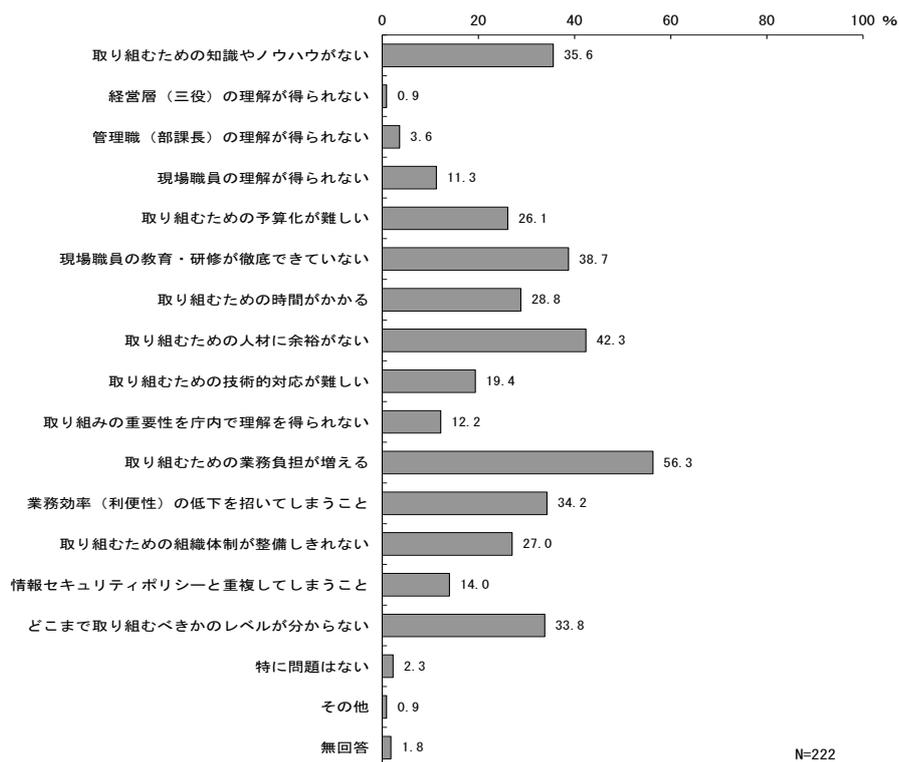
その結果、「取り組むための業務負担が増える」との回答が56.3%、次いで「取り組むための人材に余裕がない」との回答が42.3%、「現場職員の教育・研修が徹底できていない」との回答が38.7%、「取り組むための知識やノウハウがない」との回答が35.6%など、業務負荷や人材不足、さらに現場職員への教育研修の不徹底といった課題が明らかとなった。

(2) 今後必要な安全管理措置の取組

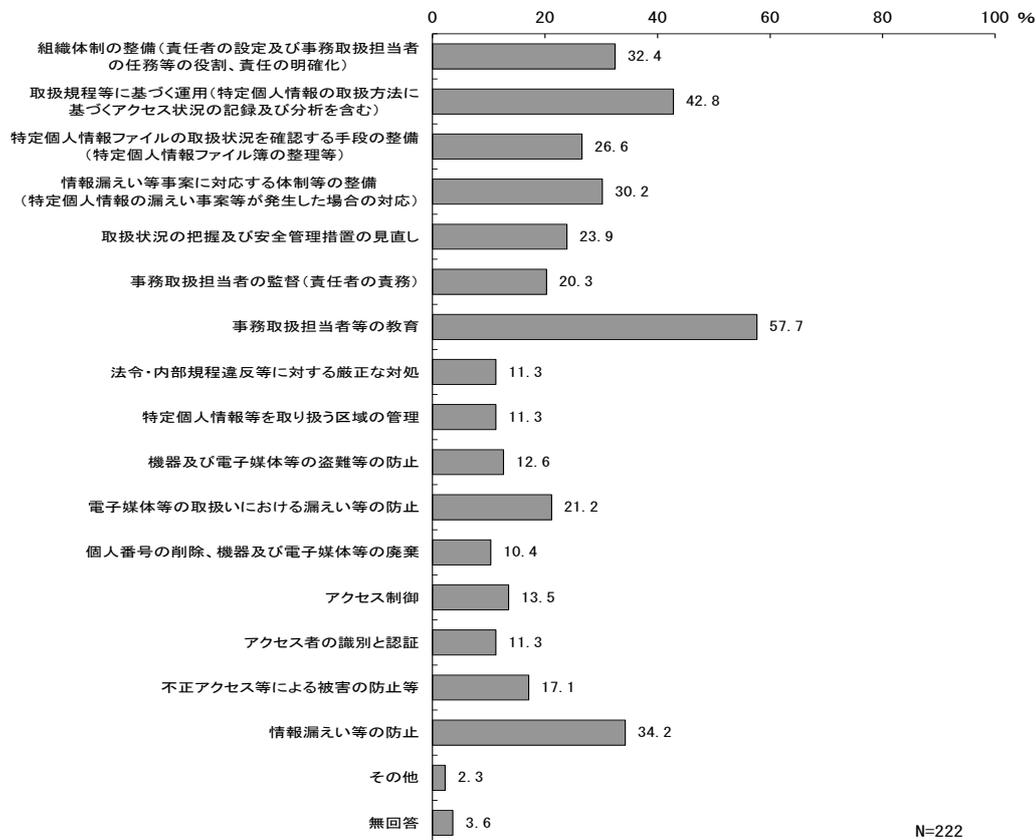
特定個人情報の適正な取扱いを確保するための安全管理措置として、今後、必要となる対策について尋ねると、次のとおりとなった(図表 12 参照)。

その結果、「事務取扱担当者等の教育」との回答が57.7%、次いで「取扱規程等に基づく運用(特定個人情報の取扱方法に基づくアクセス状況の記録及び分析を含む)」との回答が42.8%、「情報漏えい等の防止」との回答が34.2%、「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32.4%など、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た。

図表 11 安全管理措置の取組課題（複数選択）



図表 12 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) 番号制度導入後の地方自治体のセキュリティ対策のあり方に対する対応策

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、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「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。

この結果、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。このため、一定の割合ではあるものの、基本方針等の整備や個人情報保護条例の改正等の対応に取り組み切れていない地方自治体が存在している。総務省では、個人情報保護法、行政機関個人情報保護法等の改正を踏まえた個人情報保護条例の見直しに向けた検討が円滑に行われるよう設置された「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」において、個人情報保護条例の見直しの方向性を検討し、今後の課題として「将来的には、地方公共団体共通の提案受付窓口や地方公共団体が共同して非識別加工情報の作成を委託等できる仕組みを検討していくことも考えられる。」ことが提言されている(5)。こうした提言を踏まえ、円滑な条例等に取り組めるよう、地方自治体に対する支援策が求められる。

次いで、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明らかとなった。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ことが明らかとなった。

(2) 今後の展望に向けて

今回の全国自治体のアンケート調査の結果では、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が明らかとなった。そのため、番号制度導入後の地方自治体のセキュリティ対策として、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する対応にも軸足を移し、対策を実施する必要がある。ただ、今回の調査結果において、「安全管理措置の取組課題」として「どこまで取り組むべきかのレベルが分からない」と回答した地方自治体が33.8%と3割近くも存在しており、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する軸足の置き方を検討することも必要となると考えられる。その際、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が必要となる。

そこで、今後の研究では、今年度の研究で実施した自治体のアンケート調査に対して、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具体的な対応策について探求していくことで、番号制度の円滑な実施に寄与することに取り組むこととしたい。

【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)
- 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】」

【注】

- (1) <http://www.kojinjoho.metro.tokyo.jp/tokuteikojinjoho/index.htm>
- (2) <http://www.city.atsugi.kanagawa.jp/shiminbenri/totokezei/todokede/bangoseido/d033191.html>
- (3) <http://www.city.shiraoka.lg.jp/secure/12346/tokuteikojinn.pdf>
- (4) http://www.soumu.go.jp/main_content/000387560.pdf
- (5) http://www.soumu.go.jp/main_content/000485969.pdf

」〈発表資料〉

題名	掲載誌・学会名等	発表年月
瀧口樹良 「迷走する番号制度」	時事通信出版局	2017 年 4 月
湯浅塾道 「個人情報保護法と専門図書館」	専門図書館 279 号、27-32 頁	2016 年 9 月
湯浅塾道 「地方公共団体における個人情報の管理の統制-個人情報保護条例の実態」	韓国地方自治法学会「地方自治法研究」17 卷 1 号、97-129 頁	2017 年
湯浅塾道 「特別地方公共団体の個人情報保護の現状と課題」	情報法制研究 1 号、100-108 頁。	2017 年