[Ⓡ 研究論文]

マイナンバー制度がもたらすリスクに対するシステム監査の有用性について

Usability of the System Audit Against Risks Led by National Identification Number

吉田　博一
Hirokazu　Yoshida

兵庫県立大学大学院応用情報科学研究科社会応用情報科学研究センター
Information Science Research Center for Social Applications,
Graduate School of Applied Informatics, University of Hyogo

概　要

「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」により全国民にマイナンバーとよばれる個人番号が 2015 年 10 月より通知され、個人ごとの顔写真やマイナンバーが記載された IC カードであるマイナンバーカードの交付が 2016 年 1 月より開始されている。このマイナンバーを利用した制度について、国は法令で利用範囲が限定されている等の措置が講じられており、安心・安全な制度と説明している[1]。一方、マイナンバーカードに内蔵されている IC チップには、電子証明書や自治体独自のアプリケーションが格納されているが、利用範囲は限定されていない。また、地方自治体では、マイナンバーの利用に伴うセキュリティ対策が強化されている。

本研究では、このようなマイナンバーに関わる制度全般に関して主に情報システムの観点からリスク分析を行い、リスク対応におけるシステム監査の有用性を論ずる。

キーワード：マイナンバー制度　公的個人認証　リスク分析　システム監査

1　はじめに

「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（平成 25 年 5 月 31 日法律第 27 号）」(以下「マイナンバー法」という。) に基づく社会保障・税番号制度（以下「マイナンバー制度」という。）では、申請手続き時の添付書類の省略や行政機関から個人ごとに必要なお知らせを配信するプッシュ型サービス等住民の利便性が向上するとされている。

このマイナンバー制度が行政の効率化や住民の利便性の向上につながる国の基盤システムとして確立するには、リスクマネジメントを確実に行い、事故の発生を防ぎ、住民の不安の解消も必要である。

マイナンバー制度の運用に関わる組織は、行政機関（行政機関個人情報保護法第 2 条第 1 項に規定する行政機関をいう。）及び独立行政法人等（独立行政法人等個人情報保護法第 2 条第 1 項に規定する独立行政法人等をいう。）（以下「行政機関等」という。）並びに地方公共団体及び地方独立行政法人（「地方独立行政法人法」（平成 15 年法律第 118 号）第 2 条第 1 項に規定する地方独立行政法人をいう。）（以下「地方自治体等」という。）、マイナンバー法第 2 条第 7 項に規定される個人番号カード（以下「マイナンバーカード」という。）を利用する民間事業者である。

マイナンバー制度における添付書類の省略等利便性を実現するための主要なシステムの構成要素が、中間サーバー・プラットフォーム（以下「中間サーバ」という。）と呼ばれるデータベースである。この中間サーバには、行政機関等や地方自治体等が保有する特定個人情報（マイナンバーを含む個人情報を「特定個人情報」という。）を格納する。これまでは住民が添付書類を用意したが、これからは行政機関等や地方自治体等が中間サーバに情報照会を行う情報連携を行うことになる。

投稿受理日	2017 年 3 月 29 日
再投稿受理日	2017 年 9 月 21 日
再々投稿受理日	2017 年 12 月 8 日
査読完了日	2017 年 12 月 12 日

マイナンバーカードは顔写真付きの氏名・住所・性別・生年月日とマイナンバーが記載されたICカードで、マイナンバー法第17条に基づき個人の申請により交付されている。

マイナンバーカードのICチップには、「電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律（平成14年12月13日法律第153号）（以下「公的個人認証法」という。）」に基づき電子的に個人を認証する電子証明書の機能（以下「公的個人認証サービス」という。）が搭載されている。

マイナンバーの情報連携は、マイナンバー法で利用範囲が限定されているが、マイナンバーカードに搭載されている公的個人認証等アプリケーションの利用範囲は限定されていないため、リスクも大きいと考えられる。

このマイナンバーによる情報連携は、地方自治体等において情報セキュリティ対策の強化が必要となり、地方自治体等の情報システムやネットワークに影響を及ぼしている。

先行研究では、新山ら[2]はこれまでの情報漏えい事故からのマイナンバー制度のリスクを分析した。松田[3]はマイナンバー対応の情報システム導入時点で実施される特定個人情報保護評価（PIA:Privacy Impact Assessment、マイナンバー法第27条、第28条に規定するプライバシー影響評価）が監査の義務化につながると論じた。しかしながら、マイナンバー制度全般についての先行研究はない。

本研究では、マイナンバー制度全般について関連する情報システムを中心にリスクを分析し、システム監査の有用性について論ずる。

なお、リスクマネジメントの観点からは発生確率と影響度によるリスク評価が必要となるが、本研究ではマイナンバーカード制度全般の網羅的なリスクを分析等の対象とする。

2 マイナンバー制度の概要

2.1 マイナンバー法案国会上程当初の目的

マイナンバー制度は住民基本台帳法（昭和42年7月25日法律第81号）に基づく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。）などの国民総背番号制の導入とは異なり、次のような経緯がある。

マイナンバー制度の当初の法案は2012年2月に国会に上程された。この時点では給付付き税額控除等の施策を導入すると記載されていた。同年6月「社会保障と税の一体改革」についての民主、自民、公明の3党合意により「消費増税時の低所得者対策として、給付付き税額控除か複数税率（軽減税率）」実現の目的で、マイナンバー法の審議が開始された[4]。

しかし、その後の政権交代で、給付付き税額控除は導入しないことになり、マイナンバー法案の目的が国会上程当初と変わった。

2.2 マイナンバー法成立時における目的

マイナンバー法は、2013年に成立・公布された。マイナンバー法第1条では、目的として、「行政運営の効率化」及び「行政分野におけるより公正な給付と負担の確保」を図り、かつ、「国民が、手続の簡素化による負担の軽減、本人確認の簡易な手段その他の利便性の向上を得られるようにする」ほか、「特定個人情報の取扱いが安全かつ適正に行われる」こととしている。以降の条文及び施行令等に具体的対策が記載されている。

国民の利便性の向上としては、行政機関や地方自治体への申請手続きの際、これまで住民が自ら納税証明書等の添付書類を取得し添付しなければならなかったところを、行政機関等が情報連携を行うことで、添付書類を省略できることになる。

2.3 マイナンバーカードの利用拡大

前述のように、マイナンバーカードには、氏名、住所、生年月日、性別、マイナンバーと本人の写真が表示されている。

マイナンバー法第18条で、マイナンバーカードは本人確認の措置において利用するほか条例や政令で定めるところにより、公的個人認証サービス等のアプリケーション等が、ICチップに搭載されている。

公的個人認証サービスは、マイナンバー法に利用範囲が限定されていない。更に、このサービスはこれまで行政機関等や地方自治体等しか利用できなかったが、民間事業者の利用も可能となり、実際の利用も進んでいる。

このマイナンバーカードのICチップに搭載されたアプリケーション等の利用範囲の拡大によるメリットを国は強調している。

2.4 個人情報流出事案に伴う自治体情報セキュリティ対策

2015 年 5 月日本年金機構において約 125 万件という大量の個人情報流出事案が発生した。

この半年後にはマイナンバー制度の施行日の 2015 年 10 月が迫っており、総務省は、地方自治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学識経験者や国・地方自治体関係者による自治体情報セキュリティ対策検討チームを設置し、「新たな自治体情報セキュリティ対策の抜本的強化に向けて」報告をまとめた[5]。これを受け、地方自治体等はマイナンバー関連業務だけでなく、全庁の情報システムやネットワークの構成が見直されることになった。

2.5　マイナンバー制度の影響範囲

マイナンバー制度の影響範囲は、(1) マイナンバーによる情報連携、(2) マイナンバーカードの利用拡大、(3) 個人情報流出事案に伴う自治体情報セキュリティ対策と広がっている。本研究では、この 3 分野に分けて考察する。

3　マイナンバーによる情報連携等のリスク

3.1　マイナンバーの国民の懸念分野

マイナンバー制度は、住基ネットの導入過程等を踏まえ、プライバシーや情報漏洩に対する国民の懸念を想定した制度設計が行われた。その国民の懸念として次の (1) から (3) を想定している[1]。

(1) マイナンバーを用いた個人情報の追跡・名寄せ・突合が行われ、集積・集約された個人情報が外部に漏えいするのではないか（以下「個人情報漏洩リスク」という。）。

(2) マイナンバーの不正利用（例：他人のマイナンバーを用いた成りすまし）等により財産その他の被害を負うのではないか（以下「マイナンバー不正利用リスク」という。）。

(3) 国家により個人の様々な個人情報がマイナンバーをキーに名寄せ・突合されて一元管理されるのではないか（以下「マイナンバー一元管理リスク」という。）。

これらの懸念に加え、情報連携のデータの誤りにより間違った判断がされる場合のリスクを「誤データによる情報連携リスク」とし、4 つのリスクについて分析し、システム監査の有用性について、考察する。

なお、リスクの洗い出しにはステークホルダー別に行うことが必要[6]とされており、各リスクのステークホルダーを明確にする。

3.2　マイナンバーによる情報連携等のリスク分析とシステム監査の有用性

(1) 個人情報漏洩リスク

他人のマイナンバーを知ればその個人に関する行政機関等や地方自治体等で保有する個人情報が全て外部に漏えいするのではないかという住民からの危惧がある。

これに対し、システム面では、次の措置を講じている[1]。

①行政機関等や地方自治体等の業務ごとの情報システム（以下「業務システム」という。）が保有する情報を正本とし、連携に必要な情報のみを副本として中間サーバに保存し、情報の照会・提供は副本を用いることで、個人情報を一元管理ではなく、分散管理する。

②中間サーバ及び情報連携するネットワークは、マイナンバーを直接のキーとして用いず、住民票コードをもとにマイナンバーが推測できないように生成された機関別符号を連携のキーとして用い、安全性を確保している[1]。

行政機関等や地方自治体等の内部の業務システムとの間では、マイナンバーを用いず、団体内統合宛名番号という別の番号を用い、マイナンバーと情報連携する際に用いる符号等と紐づけて管理する団体内統合宛名システムを整備した[7]。

このように、個人情報の照会・提供には、マイナンバーを直接用いないので、情報のやりとりでは、誰の個人情報かわからない。

③アクセス制御により、アクセスできる人やファイルを制限し、認証やアクセスログ等を管理し、通信経路の暗号化を行う。

制度面では、次の措置が講じられている。

①個人情報の保護に関する法律（平成 15 年法律第 57 号）に基づき設置された個人情報保護委員会が行政機関等や地方自治体・事業者等への監視・監督を行う (マイナンバー法第 33 条～第 35 条)。

②マイナンバー法第 27 条、第 28 条に規定されている特定個人情報保護評価を行い、リスクを軽減するための措置を講ずる。特定個人情報保護評価は、行政機関等や地方自治体等が、特定個人情報を含むファイル（以下「特定個人情報ファイル」という。）を保有しようとするときは、保有する前に特定個人情報ファイ

ルを保有することで生じるリスクとそれに対する対策を、所定の様式に記入し、公表することを原則として義務付ける。

③マイナンバー法第48条～第57条に情報漏えいやマイナンバーの不正取得等に関する罰則を強化する。

④マイナンバー法附則第6条第3項に規定する「情報提供等記録開示システム」（以下、「マイナポータル」という。）により本人が自分自身の特定個人情報の内容や情報連携でやり取りされた履歴が確認できる[1]。

このようにシステム面や制度面からも情報漏えい対策が講じられているが、実際に個人情報等を取り扱うのは人間であり、故意または過失による運用の誤りが発生しても、個人情報が漏えいしないようシステム面や制度面の安全管理措置の厳格な運用が必要となる。

システム面や制度面の運用については、個人情報保護委員会によりガイドラインが示されている[8]が、ガイドラインはあくまでも指針であり、その趣旨に沿って正しく運用されているかを情報技術にも熟知している者が総合的に点検及び評価することが必要である。

従って、個人情報保護委員会によるガイドラインの趣旨に沿った運用について、行政機関等や地方自治体等に対するシステム監査の導入が有用となると考えられる。

なお、特定個人情報保護評価は、業務システム導入前に自己評価を行い、導入後も少なくとも1年に1度見直して、記載内容の変更が必要か否かを検討し、公表してから5年を経過する前に再実施するよう努めるものとされ、今後監査が義務付けされるという期待もあるが、特定個人情報保護評価はあくまでもマイナンバーに対応した業務システム等についての導入時の対応に位置づけされている。

また、マイナポータルを利用するためには、マイナンバーカードやICカードリーダライタを準備し、JAVAのインストール等煩雑な操作が必要となっていたが、短時間で簡単に利用者環境の設定ができるようにする等のシステムの改善が行われているところである[9]。

(2) マイナンバー不正利用リスク

他人のマイナンバーを知ればその個人になりすまして行政機関からの給付金等を盗んだりするという住民からの危惧がある。

これに対し、情報の照会・提供を行うことができるのは、マイナンバー法第9条により、社会保障・税・災害対策の分野のマイナンバー法「別表第二」で規定されている業務に限定されている。

また、マイナンバーを利用した申請に対しては、必ず厳格な本人確認措置を講ずる（マイナンバー法第16条）としている。

本人確認では、①正しい番号であることの確認（マイナンバー確認）と②手続きを行っている者が番号の正しい持ち主であることの確認（身元確認）を行う[10]ことになっており、マイナンバーだけでは申請が完結しない。

しかしながら、この本人確認の運用は人が行うものであり、厳格な運用が必要となり、情報技術にも熟知している者が総合的に点検及び評価することが必要となる。

従って、本人確認の厳格な運用について、行政機関等や地方自治体等に対するシステム監査の導入が有用となると考えられる。

(3) マイナンバー一元管理リスク

国家により個人の様々な個人情報がマイナンバーをキーに名寄せ・突合されて一元管理されるのではないかという住民からの危惧がある。この懸念は、国民総背番号制構想が持ち上がった時点でも同様のものがあったが、マイナンバー制度にあっては、これまで述べたように次の対策がとられている。

利用範囲が限定され、マイナンバーを利用する個人情報も限定されている。その個人情報は、既に業務システム等に保管されているものを、その形態を変えずに分散管理する。情報連携を行うために、個人情報の一部を副本として中間サーバに登録するが、中間サーバではマイナンバーで管理せず地方自治体ごとに異なる符号等で格納される。

このようにマイナンバーで一元管理できない仕組みとなっているが、このシステム間連携の仕組みが当初の想定通り稼働しているかどうかは、住民にとっては不安なところで、情報技術にも熟知している第3者が、総合的に点検及び評価する必要がある。

国全体での運用状況の適切性について、マイナンバー制度を所管する内閣府や総務省に対するシステム監査が有用と考えられる。

(4) 誤データによる情報連携リスク

申請手続きにおいてマイナンバーを用いて行政

機関等や地方自治体等の間で情報照会することで添付書類を省略できるようになる。

しかしながら、情報連携の際、中間サーバに格納されている照会・提供されるデータが誤っている場合や申請で必要とされる時点と異なる時点のデータを参照する場合（例えば、1月1日時点が必要とされるところを申請日時点のデータを参照する）、申請結果の判断が誤っているという住民からの危惧もある。

これに対して、3.2節(1)で述べたマイナポータルでは、自己情報表示機能により中間サーバに登録されている自己に関する特定個人情報を、情報提供等記録表示（やりとり履歴）機能により中間サーバにおける自己に関する特定個人情報がどの機関にて照会・提供されたか等の履歴を、確認することができる。

住民が自ら確認できるとはいえ、正しく情報連携できているかは、制度所管の国において動作保証をすべきである。また、マイナポータルは住民自らが情報連携の運用を確認できるサービスであり、その利便性の向上や利用の周知を図ることが必要である。

このためには、正確な情報連携、マイナポータルの利用状況等について内閣府や総務省等行政機関に対するシステム監査が有用であると考えられる。

4　マイナンバーカードの利用拡大におけるリスク

4.1　マイナンバーカードの利用範囲

マイナンバーカードの概要は2.3節で述べた。国では、次のようなメリットがあるとしている[10]。

①マイナンバーを証明する書類
②本人確認の際の公的な身分証明書
③付加サービスを搭載した多目的カード
④コンビニ等で行政上の各種証明書を取得
⑤各種行政手続のオンライン申請
⑥各種民間のオンライン取引／口座開設

このうち、①は図1のカード裏面の利用で、マイナンバー法により利用範囲が規定されている。②は図1のカード表面の利用で、マイナンバーは表示されておらず、広く身分証明書としての利用が可能である。

③から⑥に関しては、図1のICチップに搭載されたアプリケーションを利用する。

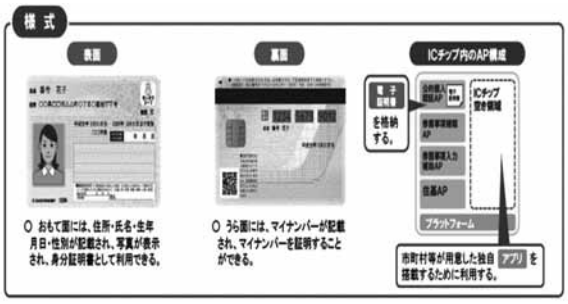

図1 マイナンバーカードについて[10]

4.2　公的個人認証サービスの利用拡大

4.2.1　サービス対象を民間事業者へ拡大

公的個人認証サービスは「住民基本台帳法(昭和42年7月25日法律第81号)」第30条の44第1項に基づき2003年度より交付が始まった住民基本台帳カード（以下「住基カード」という。）に電子証明書を格納し、国税電子申告・納税システム（e-Tax）[11]や地方税ポータルシステム（eLTAX）[12]、市区町村が発行する証明書（住民票の写し、印鑑登録証明書等）を全国のコンビニエンスストア等のマルチコピー機から取得するサービス（コンビニ交付）等が利用できるようにするものである。

マイナンバーカードの発行により、公的個人認証サービスは住基カードに代わりマイナンバーカードを利用することになった。

公的個人認証法第39条第1項の規定により地方公共団体情報システム機構が認証事務を実施している。

4.2.2　サービス対象を民間事業者へ拡大

これまで公的機関や地方自治体しか利用できなかったが、2016年1月からは、総務大臣の認定を受ければ、民間事業者も公的個人認証サービスを利用できるようになった[1]。現在認定事業者は次のサービスを提供している。

○ケーブルテレビに個人に最適な行政情報やオンラインショッピング、家庭に応じた最適な防災情報等の地域情報の配信基盤を提供
○マイナンバーカードを活用して、地域における母子保健、医療、福祉等住民が日常的に利用する情報を提供するシステム基盤を運営
○プラットフォーム事業

プラットフォーム事業とは、公的個人認証サービスを利用するために必要となる電子証明書の有効性確認のシステム基盤を整備し、

その機能をクラウドサービスとして各民間事業者に提供する事業である。

現在、携帯電話サービス契約締結時の本人確認を自動化する機能、新規証券口座開設時の本人確認のオンライン完結かつ即時取引開始機能、非対面での不動産取引時にオンライン上で本人確認する機能等が稼働している。

民間事業者が公的個人認証サービスを利用するには、システム、組織体制、運用規程等を整備し、不正アクセスの防止等の基準をクリアし、公的個人認証サービスを適切に利用できる民間事業者として認定を総務大臣から得なければならない[13]。

また、利用者の拡大やサイバー攻撃等に対して、サービス維持のための設備投資等の情報セキュリティ対策を講ずる必要がある。

4.3 携帯電話を用いた利用推進

公的個人認証サービス利用促進のため、携帯電話を用いた次の3方式を推進している[1]。

(1) 携帯電話をICカードリーダライタとして使用し、携帯電話とPCを連携させる
(2) 携帯電話がICカードリーダライタとPCの役割を担う
(3) 携帯電話に電子証明書を格納し活用する

(3)の場合、公的個人認証サービスを利用するためにマイナンバーカードを持ち歩く必要がなくなる

4.4 マイキープラットフォーム

マイナンバーカードの活用策として、総務省が推進しているのが、マイキープラットフォームである[14]。

マイキープラットフォームとは、住民が自らのマイナンバーカードのICチップにマイキーIDと呼ばれるIDを格納し、図書館等公共施設の利用者カードや商店街のポイントカードなどの各種IDと結び付ける共通基盤である。これを利用して住民の公益的活動の支援と地域の消費拡大につなげることを目的としている。

マイキーIDは、希望者が自分で作成し、マイナンバーカードに格納する。図書の貸出し履歴や物品の購入履歴等の情報はマイナンバーカードには格納しない。マイキーID利用の際は行政窓口の職員や商店街等の店員等にはマイナンバーカードを手渡さずに、住民自らがカードリーダを操作する。このような運用により、個人情報が流出しないとしている。

2017年9月25日からマイキープラットフォームが稼動し、実証事業として先行自治体による住民向けのサービス提供が始まった[15]。

4.5 子育てワンストップサービス

児童手当、保育、母子保健、ひとり親支援の手続きについて、これまで地方自治体窓口に出向いて手続きごとに申請する必要があったところを、3.2節(1)で述べたマイナポータルを使い、自宅等から市区町村の子育て関連手続を検索し、マイナンバーカードで電子署名を付して申請できる子育てワンストップサービスを総務省が推進している[1]。

総務省では、2016年12月に「アクションプログラム」[14]を公表し、全市区町村に参加を呼びかけ、2017年のマイナポータル本格運用開始に併せて、全市区町村で順次サービス提供を開始するとしていた。

マイナポータルは当初2017年7月より運用開始の予定であったが、同年11月13日からに延期された[16]。子育てワンストップサービスも一部の地方自治体で開始された。

4.6 マイナンバーカードの利用拡大におけるリスク対応とシステム監査の有用性

(1) マイナンバーカード紛失リスク

9cm×5cmのカードという物理的な形状により紛失しやすいという住民の危惧がある。

リスク回避としてカードを携行しないという対応もあるが、紛失・盗難時には、マイナンバーカードコールセンターに連絡すると、速やかに当該カードの失効情報が登録され、利用できなくなる[10]。

利用の都度失効情報を逐一照会する運用の場合は即時に利用不可となるが、失効情報リストの配信により有効性を確認する運用方式を採用している場合は、配信が1日1回となり、タイムラグが発生し、しばらくは利用できる可能性がある。

失効情報リストのタイムラグ等運用の支障発生状況や再発行の手続きにおける迅速性・厳密性については、行政機関等や地方自治体等に対するシステム監査という第3者の検証が有用と考えられる。

(2) 独自アプリケーションが利用されないリスク

地方自治体等が、独自に作成したアプリケー

ションをマイナンバーカードのICチップに搭載するには、オンラインでダウンロードはできず、地方自治体等の窓口に住民がマイナンバーカードを持参しなければアプリケーションの搭載ができない等利便性が悪く独自作成したアプリケーションが利用されないという地方自治体の危惧がある。

利用を促進するには、住民ニーズにあった魅力的なアプリケーションを作成し、住民に広報等の周知が必要になると思われる。

このため、導入効果の分析や利用状況を検証することが必要となり、情報システムの開発・普及動向に詳しい第３者による行政機関等や地方自治体等に対するシステム監査が有用と考えられる。

(3) 公的個人認証による個人情報流出リスク

公的個人認証サービスの民間事業者への拡大により、これまで運転免許証のコピーの送付等で住所・氏名等を確認していた手続きがオンラインで即時に確認できるなど、住民や民間事業者ともに利便性が向上する。

しかしながら、マイナンバーの情報連携に比べて、法律上に利用範囲の規定がなく、大臣認定を受ければ民間事業者でも利用できるなど利用にあたっての制約が低く、氏名、住所、生年月日、性別の個人情報が住民の同意なしに流出するという住民の危惧がある。

マイナンバー法による情報連携ではないので、マイナポータルでは公的個人認証サービスの利用履歴を確認できないが、住民が自ら確認できる仕組みが必要になると思われる。また、公的個人認証サービスの利用時には、必ず事前に個人情報取得に対する同意を住民から得るよう徹底することが望ましい。

このため、総務省やシステム運用主体の地方公共団体情報システム機構は、利用履歴の情報開示機能を提供すると共に、住民の同意取得状況等について民間事業者に対するシステム監査を導入して検証することが有用であると考えられる。

(4) 公的個人認証の大臣認定基準の適正運用リスク

民間事業者が公的個人認証サービスを利用する際に、4.2.2 節で述べた基準を満たし大臣認定を得る必要がある。

この基準を満たし、安定的に運用するため、適正な投資額やどのレベルの運用をすればよいかという事業者の危惧がある。

リスクアセスメントを行い、優先順位を付けた対策を行うことが必要となるが、自社でこのようなノウハウがない場合、大臣認定基準を満たした適切な運用を行っているかについて、専門的な知識を有する第３者が民間事業者に対しシステム監査を行うことが有用と考えられる。

(5) 公的個人認証の大臣認定基準の未達成リスク

プラットフォーム事業の場合は、サービス利用事業者は大臣認定の手続きをサービス提供事業者に代行させることが可能で、サービス利用事業者が基準を満たしたセキュリティ対策を実際に行っているかどうか不安であるという住民等利用者の危惧がある。

総務大臣の認定にあたっては、業務の手順、業務従事者の責任及び権限等について規定等により明確かつ適切に定め、かつ適切に実施することが認定基準の中に記載されており、当該業務の監査の実施も必要とされている。

プラットフォーム事業のサービス利用事業者が基準を満たした運用を行っているかは、認可官庁である総務省や運用主体である地方公共団体情報システム機構による検証が必要であるが、情報技術の専門知識を有する第３者によるシステム監査を行うと共に、その結果を公表することが有用と考える。

また、認定基準に沿った適切な運用状況についてプラットフォーム利用事業者も含めた認定事業者に対するシステム監査が有用と考えられる。

(6) 携帯電話紛失リスク

携帯電話をカードリーダライタ等として利用する場合は、携帯電話を紛失しても、携帯電話の中にはマイナンバーカードの情報は保有していないため、マイナンバーの情報流出のリスクはない。

携帯電話に電子証明書を格納した場合は、携帯電話の紛失はマイナンバーカード紛失リスクと同様の住民の危惧がある。

マイナンバーカードの場合は、必要時以外はカードを携行しないというリスク回避ができたが、携帯電話の場合は携行しないという対応は難しい。

マイナンバーカード紛失時の対応と同じく失効情報リストのタイムラグ等により運用の支障が発生していないか、再発行の手続きが速やかにかつ厳密に行っているか等について、行政機関等や地方自治体等に対するシステム監査が有用となる。

(7) マイキープラットフォーム利用混乱リスク

マイキープラットフォームを利用者が自分自身

で操作するのは、難しいと考えられ、実際の利用する場面では混乱するという住民のリスクが考えられる。

マイキープラットフォームを利用する住民や公共施設・商店街等の職員がわかりやすく操作ができるようテストや習熟等に十分に準備して進めることが必要で、マイキープラットフォームをサービス提供している総務省において適切な対策が必要となる。

マイキープラットフォームの適切な運用状況や公共施設・商店街等の利用状況については、導入を推進する総務省においてシステム監査を導入して検証することが有用と考えられる。

(8) 子育てワンストップサービス利用混乱リスク

子育てワンストップサービスを利用するにはマイナポータルの設定が必要であるが、3.2 節 (1) で述べたようにマイナポータルは利用方法が煩雑で現在システムの改善が進められているところである。

また、このサービスが地方自治体により提供の有無や範囲が異なることから利用にあたって混乱するという住民・地方自治体等のリスクが考えられる。

マイナポータルの改善は、サービスを提供している内閣府が行っているが、子育てワンストップサービスを使った手続きの対応やその周知は地方自治体の役割である。

マイナポータルの改善状況については、内閣府に対して、子育てワンストップサービスを利用する申請等の手続きの拡充やその広報・周知については、地方自治体等に対するシステム監査が有用であると考えられる。

5 自治体情報セキュリティ対策の抜本的強化が及ぼすリスク

5.1 自治体情報セキュリティ対策の抜本的強化とは

2.4 節で述べたように 2015 年 5 月日本年金機構の個人情報流出事案を受け、総務省の検討チームが出した「新たな自治体情報セキュリティ対策の抜本的強化に向けて」に基づき、全国の地方自治体でマイナンバーに関連する業務だけでなく庁内の全情報システムやネットワークの構成が見直されることになった。

その概要は次の図 2 のとおりとなる。

この対策を徹底するため、総務省は 2015 年度補正予算で、自治体情報セキュリティ強化対策事業 255.0 億円を措置した [17]。

内容としては、次の「以下の三層からなる対策で、情報セキュリティ対策の抜本的強化を図る自治体を支援」するものである。

①マイナンバー利用事務系（マイナンバーを利用する事務を扱う情報システムや端末を接続するネットワーク。個人番号利用事務系ともいう。）では、端末からの情報持出し不可設定等を図り、住民情報流出を徹底して防止

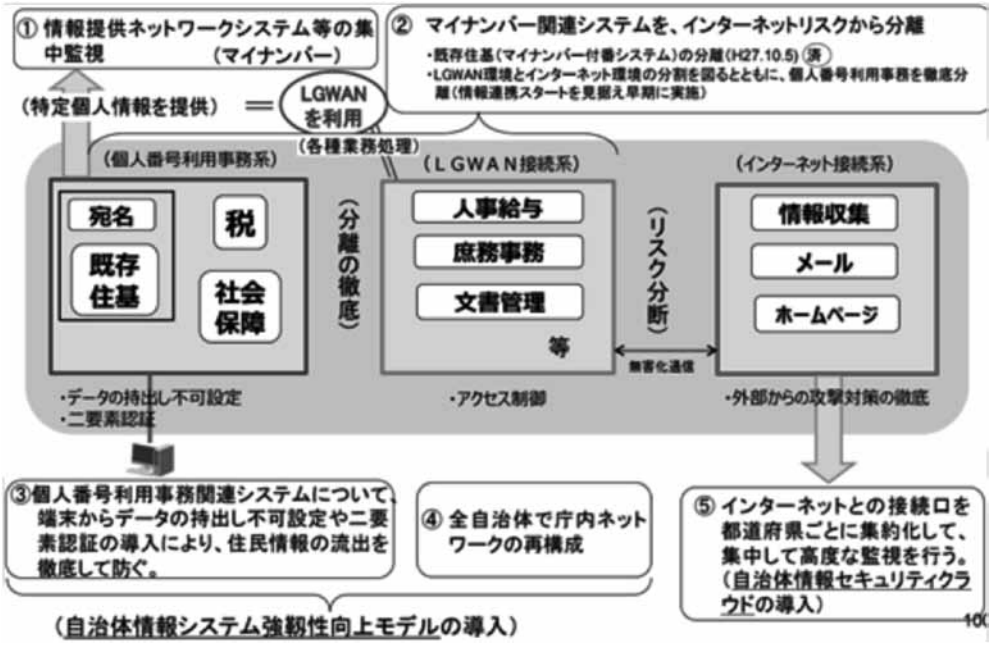

図 2 自治体情報セキュリティに係る攻撃リスク等の低減のための抜本的対策の概要 [5]

②マイナンバーによる情報連携に活用される総合行政ネットワーク（Local Government Wide Area Network）（以下「LGWAN」という。）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（無害化された通信は許容されており、分離ではなく分割と呼んでいる。）

③都道府県と市区町村が協力して、高度な情報セキュリティ対策を講じるため、自治体情報セキュリティクラウドを構築

5.2　抜本的強化の影響と業務上の影響

前節の方針により、地方自治体内のネットワークが、マイナンバー利用事務系、LGWAN 接続系、インターネット接続系の３つに分かれることになり、各々のネットワークに対策を講ずることが必要となる。しかしながら、一人の職員が、住民対象のマイナンバー利用事務も、財務関係等の LGWAN に接続された内部事務も、インターネットのメール対応やホームページの検索を行うことがあり、この場合１人３台の端末を利用することになる。

吉田[18]は、こういった複数ネットワークへの端末配備、ソフトウェアのアップデート、ネットワーク間でのメールやファイルの受渡しについての対応と課題について指摘した。

この対応と課題をもとに、リスク対応とシステム監査の有用性を論ずる。

5.2.1　複数ネットワークへの端末配備

個人番号利用事務系と LGWAN 接続系、インターネット接続系の各々の回線に接続して１人３台の端末を設置している団体もあるが、費用やスペース面で課題があり、次の対策を講じている団体が多い。しかしながら、その対策による課題も生じている。

（1）インターネット接続端末を業務上必要な箇所にのみ配置する

住民と接する窓口では、必ずしもインターネットに接続した端末を利用せず、業務システムのみを利用している部署もあるので、インターネット接続端末を各部署に１台というように設置台数を絞る。

（課題）Web 閲覧が行いにくい。常時見ているわけではないので、インターネットメールが届いてもすぐに確認できない。

（2）デスクトップ仮想化技術を用い、端末でネットワーク接続を切り替えて利用する

VDI（Virtual Desktop Infrastructure）や SBC（Server Based Computing）方式といったデスクトップ仮想化技術を用い、LGWAN 接続系とインターネット接続系の端末を１台の端末でネットワーク接続を切り替えて利用することにより物理的な端末台数を減らし、設置スペースを小さくする。

（課題）ライセンス料が必要で費用がかさむ。

5.2.2　ソフトウェアの更新プログラムの適用

従来、インターネット経由で無償ダウンロードしていたソフトウェアの更新プログラムは、個人番号利用事務系や LGWAN 接続系ではネットワーク分離のため、利用できなくなる。その対策と課題は次のとおりである。

（1）LGWAN-ASP サービスを利用する

LGWAN-ASP によるベンダーのソフトウェア更新サービスを利用する。

（課題）従来無償で利用していたものが、有償となる。

（2）媒体を用いて個別に適用する

ダウンロードした更新プログラムを媒体に格納し、各々のサーバや端末に個別適用する。

（課題）更新プログラム適用のたびに個別に作業が必要となる。

（3）都道府県単位で更新プログラムの配信サーバを構築する

既に都道府県と市町村とで LGWAN を共同利用している場合、LGWAN 用の更新プログラムの配信サーバを構築する。

（課題）配信サーバの構築費が必要となる。都道府県によっては、ネットワークを共同利用していない場合もある。

（4）総務省によるマイナンバー利用事務系や LGWAN 接続系の端末への更新プログラムの提供サービスを利用する

平成 29 年度総務省が整備する予定のマイナンバー利用事務系や LGWAN 接続系の端末へ更新プログラムの提供サービスを利用する。

（課題）全地方自治体等に対し一定の頻度で更新プログラムを配信することになり、配信時刻指定等個別の対応は難しい。

5.2.3　ネットワーク間でのメールやファイルの受け渡し

LGWAN 系とインターネット接続系が分割されているため、インターネットメールの添付ファイルを直接 LGWAN 系で受信することができず、ネットワーク間でのファイルのやり取りができなくなる。その対策と課題は次のとおりである。

(1) メール内容を画像またはテキスト化

メール内容を画像またはテキスト化して転送・閲覧し、添付ファイルは開かない。

（課題）添付ファイルが全く利用できない。メール本文中の URL がハイパーリンクされない。ファイルの２次利用ができないなど利便性の低下につながる。

(2) 無害化ツールを利用する

メールの添付ファイルや電子申請・媒体持込のファイルからマクロやスクリプト等危険因子を除去する無害化ツールを利用する。セキュリティクラウドや LGWAN-ASP、ファイル交換サーバにも無害化ツールを利用する。

（課題）無害化前後のファイルの同一性が確保できない。無害化ツールの利用に費用がかかる。ファイル種別により無害化ツールが対応できないものも存在し、この場合は (1) の画像化により受渡しすることになる。

(3) ウィルスチェックを行い媒体により受け渡しする

ウィルス対策ソフトやサンドボックス等によりウィルスチェックを行ったものを媒体により受け渡しする。

（課題）媒体の持ち運びや媒体からファイルの転送の手間がかかる。個人番号利用事務端末はデータの持出し不可設定を行っており原則媒体の利用はできない。

5.3 自治体情報セキュリティ対策の抜本的強化が及ぼすリスク対応とシステム監査の有用性

(1) 日々の脅威に対するリスク

日々新たな脅威に対する情報セキュリティ対策について、情報セキュリティ対策を怠るとサーバや端末が攻撃にさらされる地方自治体のリスクがある。

日々新たな脅威に対する情報セキュリティ対策について、地方自治体の場合は、内部に専門的な人材を抱えるのが難しい。情報セキュリティ対策の適切な運用をしているかについて、地方自治体等に対するシステム監査により検証することが有用と考えられる。

(2) メール送受信の遅れによるリスク

5.2.1 節で述べたように住民とのやりとりに利用されるインターネットメールをすぐに確認できる環境がないため、メールの確認・送受信に時間がかかり、住民との迅速な意思疎通できないという住民、地方自治体等のリスクが考えられる。

対応策としては、グループウェア等によりインターネットメールの到着通知を行う等のツールの利用が考えられる。いずれの方法が適切かについては、インターネットメールの利用頻度等を考慮した適切な運用をしているかについて、地方自治体等に対するシステム監査による検証が有用と考えられる。

(3) 更新プログラム適用の遅れによるウィルス感染等のリスク

5.2.2 節で述べた更新プログラムの配信サーバが利用できない場合、パターンファイルの更新が遅れ、ウィルス感染する等の地方自治体のリスクがある。

サーバや端末の設置環境・台数や費用・体制を考慮した適切な運用をしているかについて、地方自治体等に対するシステム監査による検証が有用と考えられる。

(4) ファイルの受渡し不可によるリスク

5.2.3 節で述べた住民とファイルの受渡しについて、データファイルでの受渡しができない、または、画像等イメージデータでしか受渡しができないことになり、前節と同じく、住民との迅速な意思疎通できないという住民、地方自治体等のリスクが考えられる。

住民の利用頻度等や地方自治体における費用・体制を考慮した適切な運用をしているかについて、地方自治体等に対するシステム監査による検証が有用と考えられる。

6 マイナンバー制度におけるシステム監査の有用性

これまで、マイナンバーの情報連携、マイナンバーカードの利用、自治体情報セキュリティ対策の抜本的強化の３つの観点からマイナンバー制度におけるリスク分析を行い、この対応において、情報技術にも熟知している者が、総合的に点検及び評価するシステム監査の導入が有用となるシステム監査の有用性を論じた。

これらのリスクを、ステークホルダー別にまとめ、システム監査対象の団体及び業務を要約した

のが、次の表１～３である。

ステークホルダー別にリスクとシステム監査対象の団体及び業務をまとめた結果から次の結論が導かれる。

・住民に対するリスクについては、行政機関等と地方自治体等に対するシステム監査が、網羅的なリスク対応につながり、効果的な対応となる。住民の不安を払しょくし、リスクを軽減するためには、システム監査を導入すべきであると考えられる。
・地方自治体等に対するリスクについては、様々な対応が必要となるが、その対応が当該地方自治体の規模や情報システムの環境、利用状況に合わせて適切であるかについて、システム監査が有用であると考えられる。
・公的個人認証サービスを利用する民間事業者に対するリスクに対しては、投資対効果や住民の同意を得た運用というコンプライアンスの確保の面から、システム監査が有用である。

7　おわりに

本研究では、マイナンバー制度全体を俯瞰してリスク分析を行い、リスク対応におけるシステム監査の有用性を考察した。全てのリスクに対し、システム監査の観点から有用であることがわかった。

このシステム監査の有用性を広く周知し、システム監査を実施することで、マイナンバー制度を発展させ、国の基盤となるよう進めるべきと考える。

今回の研究からは除外したが、マイナンバーは一般の民間企業でも事業主として従業員等のマイナンバーを管理し、税務署等へ報告する義務が生じ、この業務におけるリスクも生じている。業種・業態、事業所規模・従業員の構成等を考慮したリスクマネジメントが必要となるが、本研究では除外して考察した。

今後は、マイナンバー制度の普及状況や制度等の変更にも配慮し、更にリスク軽減となるようなシステム監査の実践的な研究を進めていきたい。

表１　住民に対するリスクとシステム監査の対象

リスク概要	監査対象			システム監査対象業務 【 】内は監査対象団体が特定される場合
	行政機関等	地方自治体等	民間事業者	
①個人情報漏洩リスク	○	○		個人情報保護委員会によるガイドラインの趣旨に沿った運用
②マイナンバー不正利用リスク	○	○		本人確認の厳格な運用
③マイナンバー一元管理リスク	○			国全体での適切な運用【内閣府、総務省】
④誤データによる情報連携リスク	○			正確な情報連携、マイナポータルの利用状況等【内閣府、総務省】
⑤マイナンバーカード紛失リスク	○	○		失効情報リストのタイムラグ等に運用の支障発生状況 再発行の手続きにおける迅速性・厳密性
⑦公的個人認証による個人情報流出リスク	○	○		利用履歴の情報開示や民間事業者への同意取得の徹底【総務省、地方公共団体情報システム機構等】
			○	住民からの情報取得の同意取得状況
⑨公的個人認証の大臣認定基準の未達成リスク	○	○		プラットフォーム利用事業者が適切な運用をしているか【総務省、地方公共団体情報システム機構】
			○	認定基準に沿った運用をしているか【民間事業者】
⑩携帯電話紛失リスク	○	○		マイナンバーカード紛失時の対応と同じく失効情報リストのタイムラグ等に運用の支障発生状況 再発行の手続きにおける迅速性・厳密性
⑪マイキープラットフォーム利用混乱リスク	○			マイキープラットフォームが適切に運用されていることや公共施設・商店街等の利用状況【総務省】
⑫子育てワンストップサービス利用混乱リスク	○			マイナポータルの改善状況【内閣府】
		○		子育てワンストップサービスを利用できるよう申請等の手続きの対応やその広報・周知
⑬日々脅威に対するリスク		○		情報セキュリティ対策の適切な運用
⑭メール送受信の遅れによるリスク		○		インターネットメールの利用頻度等から適切な運用
⑯ファイル受渡し負荷によるリスク		○		自治体側の体制や住民の利用頻度等から、費用・体制を考慮した適切な運用

表２　地方自治体等に対するリスクとシステム監査の対象

リスク概要	監査対象		システム監査対象業務 【 】内は被監査団体
	行政機関等	地方自治体等	
⑥独自アプリケーションが利用されないリスク		○	導入効果分析や利用状況
⑫子育てワンストップサービス利用混乱リスク	○		マイナポータルの改善状況【内閣府】
		○	子育てワンストップサービスを利用できるよう新政党の手続きの対応やその広報・周知
⑬日々脅威に対するリスク		○	情報セキュリティ対策の適切な運用
⑭メール送受信の遅れによるリスク		○	インターネットメールの利用頻度等から適切な運用
⑮更新プログラム適用の遅れによるウィルス感染等のリスク		○	サーバや端末の設置環境・台数費用・体制を考慮して適切な運用
⑯ファイル受渡し負荷によるリスク	○	○	地方自治体側の体制や住民の利用頻度等から、費用・体制を考慮した適切な運用

表３　民間事業者に対するリスクとシステム監査の対象

リスク概要	監査対象			システム監査対象業務 【 】内は被監査団体
	行政機関等	地方自治体等	民間事業者	
⑦公的個人認証による個人情報流出リスク	○	○		利用履歴の情報開示や民間事業者への同意取得の徹底【総務省、地方公共団体情報システム機構】
			○	住民からの情報取得の同意取得状況
⑧公的個人認証の大臣認定基準の適正運用リスク			○	大臣認定基準を満たした運用

参考文献：

1）内閣官房；「マイナンバー 社会保障・税番号制度概要資料 平成 29 年 7 月版」、http://www.cao.go.jp/bangouseido/pdf/seidogaiyou_2907.pdf、URL 参照日 :2017/9/14.

2）新山 剛司、北 寿郎；「共通番号 (マイナンバー) 制度の民間サービス利用時における個人情報漏洩のリスク評価に関する研究」、情報科学技術フォーラム講演論文集、14、4、213-224(2015).

3）松田貴典；「マイナンバー制度でのリスク対策と監査 : 自治体等における特定個人情報保護評価をモデルにして」、監査研究、41、10、7-21(2015).

4）首相官邸；「第百八十一回国会における野田内閣総理大臣所信表明演説」(2012 年 10 月 29 日)、http://www.kantei.go.jp/jp/noda/statement2/20121029syosin.html、URL 参照日 :2017/9/14.

5）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向けて」、http://www.soumu.go.jp/main_content/000387560.pdf、URL 参照日 :2017/9/14.

6）経済産業省；「先進企業から学ぶ事業リスクマネジメント実践テキスト」(2005)

7）総務省；「番号制度の導入に向けた情報システムの対応について」、月刊 J-LIS　H27. 1 月、pp.15-20、https://www.j-lis.go.jp/data/open/cnt/3/1282/1/H2701_03.pdf、URL 参照日 :2017/9/14

8）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）」、https://www.ppc.go.jp/files/pdf/my_

number_guideline_gyosei-chihou.pdf、URL 参照日 :2017/10/31.
9) 内閣府 ;「マイナポータル関連スケジュール (平成 29 年 10 月 5 日時点)」 http://www.cao.go.jp/bangouseido/pdf/portal01.pdf、URL 参照日 :2017/11/29
10) 総務省 ;「マイナンバーカードを活用したオンライン取引等の可能性について」(2017 年 10 月)、 http://www.soumu.go.jp/main_content/000511828.pdf、URL 参照日 :2017/11/27.
11) 国税庁 ;「国税電子申告・納税システム (e-Tax)」、 http://www.e-tax.nta.go.jp/、URL 参照日 :2017/9/14.
12) 一般社団法人地方税電子化協議会 ;「地方税ポータルシステム (eLTAX)」、 http://www.eltax.jp/、URL参照日 :2017/9/14.
13) 総務省 ;「公的個人認証サービス利用のための民間事業者向けガイドライン」(2015)、 http://www.soumu.go.jp/main_content/000400619.pdf、URL 参照日 :2017/9/14.
14) 総務省 ;「ワンストップ・カードプロジェクト アクションプログラム」、 http://www.soumu.go.jp/main_content/000455778.pdf、URL 参照日 :2017/9/14.
15) 総務省 ;「マイキープラットフォームの運用開始等」、http://www.soumu.go.jp/main_content/000508643.pdf、URL 参照日 :2017/11/24.
16) 総務省 ;「マイナンバー制度における「情報連携」及び「マイナポータル」の本格運用等開始」、 http://www.soumu.go.jp/menu_news/s-news/01kanbo07_02000001.html、URL 参照日 :2017/11/24.
17) 総務省 ;「平成２７年度総務省所管　補正予算（案）の概要」、 http://www.soumu.go.jp/main_content/000391075.pdf、 URL 参照日 :2017/9/14.
18) 吉田博一 ;「マイナンバー制度及びセキュリティ強靭化対策が及ぼす自治体情報システムの展望について」、経営情報学会 2017 年春季全国研究発表大会 .

吉田　博一　　兵庫県立大学大学院応用情報科学研究科社会応用情報科学センター研究員