L-018

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

新山　剛司†　　北　寿郎‡
Takeshi　Niiyama　　Toshiro　Kita

１．はじめに

共通番号（マイナンバー）法は、2013年5月24日に参院本会議で可決、成立し、2016年1月施行予定である。個人に12ケタの番号を付与した1枚のカードを配布し、健康保険番号、介護保険番号、年金番号などを共通番号化することで、より利便性の高い住民サービスを国民に提供することを目的としている。一方で、個人情報であるマイナンバーを詐称されることに起因した情報漏洩事故の発生が施行前から最大の懸念事項として関心を集めている。

マイナンバーの前身である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。）は住民の利便性の向上と国及び地方公共団体の行政の合理化のため、居住関係を公証する住民基本台帳をネットワーク化し、全国共通の本人確認ができるシステムとして構築された。同様に住基ネット稼働以前から今回のマイナンバーのような個人情報の漏洩が危惧されていた。

内閣官房と内閣府による「マイナンバー社会保証・税番号制度　概要資料」[1]では、「諸外国の問題点を踏まえた制度」により安心・安全を確保することが記載されている。その中では2大措置として「制度上の保護措置」と「システム上の安全措置」が挙げられており、一見万全なセキュリティ対策が行われているかのように見える。

総務省をオブザーバーとした「個人情報保護ワーキンググループ」及び「情報連携基盤技術ワーキンググループ[2]」で対策方法や運用について議論されている。

付録表1に個人情報保護ワーキンググループの構成員を示す。この表からは12名中11名（92%）が法律分野の権威であることが示されている。このワーキンググループによりマイナンバーがどのような情報資産であり、どのように運用されるべきか、またその資産を侵害した場合にどのような罰則が与えられるかなどの考え方が提示されている。

付録表2に情報連携基盤技術ワーキンググループの構成員を示す。この表からは11名中9名（82%）は情報セキュリティ分野の権威であることが示されている。このワーキンググループにより情報資産であるマイナンバーが流通するシステムをどのような方針でセキュアに構築するかについての考え方が提示されている。これは概要設計、基本設計、詳細設計でいうところの概要設計に該当する。

マイナンバーに関する情報システムの調達の指針においても同様に厳しいセキュリティ基準が設けられている。総務省の「マイナンバー付番システム等の構築に係る情報提供依頼（RFI）について」[3]の中で比較検討が行われている。

当該システムはセキュリティを重視した設計方針をとっており、行政機関を結ぶネットワークの間では、個人情報は「符号」を用いられ完全に匿名化されている。情報連携が始まると、この「符号」が各システムの入り口まで流通する。各システムに格納されている所得情報や年金の給付状況などの個人情報は従来どおり行政ネットワーク内に閉じた形で利用される。符号には、これらは個人番号や氏名、住所など個人を特定できる情報は一切含まないため、セキュリティに配慮した高度なセキュリティシステムだと位置付けされている。

しかしマイナンバーの民間利用では、公的個人認証法の民間拡大[4]について、医療機関、金融機関、ショッピングサイトへの利用などが明記されており、民間事業者が流通するマイナンバー関連情報のセキュリティ対策を講じることが必要性であるが、諸外国の情報漏洩事故が示す通り、情報漏洩が発生する箇所が公共サービスを利用したシステムから民間サービスを利用するシステムが拡がることから情報漏洩の可能性が更に高くなる可能性がある。

実際に従来研究からは、ITによる技術を活用した新たな試みによりシステムやセキュリティの専門家が想像もしないアプローチから情報漏洩事故が発生する可能性が明らかになった。更に先行調査では既にマイナンバーと同様の公共サービスを提供している諸外国において情報漏洩が発生していることを明らかとした。

これらの情報からマイナンバー利用時、特に民間サービス利用時には情報漏洩事故が発生する可能性が高いことは明白であり、民間サービス利用時に考えられるサービスフローやシステム構成のシミュレーションモデルを構築し、そのモデルについてリスク評価を行うことが重要と考えた。モデルに基づきリスク評価を実施し、必要なセキュリティ対策についてまとめた。

残された課題として、より現実に則したリスク評価の実施が求められる。継続研究として、それを解決するために米国において最も情報漏洩事故の発生確立が高い場所であった大学を選定し、実際の国内大学におけるマイナンバー利用のシミュレーションモデルを構築し、そのリスク評価を行うこととする。

最終的にこれらの研究に関する考察から得られた知見を基に現実にマイナンバー制度を運用する住民、民間企業、中央省庁や地方自治体に対して、予見される情報漏洩事故について実践的な提言を試みる予定である。

2．従来研究と研究の目的

マイナンバーのセキュリティに関する従来研究は2つの観点で行われてきた。1つは「個人情報漏洩とプライバシーに関する研究」であり「制度上の保護措置」に関連するものである。もう1つは「情報システムセキュリティに関する研究」であり「システム上の安全措置」に関連するものである。それぞれ事項以降に従来研究について調査した結果を示す。

† 同志社大学大学院総合政策科学研究科
‡ 同志社大学ビジネススクール

2.1 個人情報漏洩とプライバシーに関する研究について

マイナンバーの前身でもある住基ネットの2002年稼働以前より、政府主導の住民サービスにおける情報漏洩に対するリスクの懸念が指摘されてきた。豊福(2004)はサービスを受ける側の住民となる全国20歳から60歳までの2000名に対して2003年10月24日から27日にかけてオンラインのウェブアンケートを実施し、住基ネットカードの利用についての意識調査について最終報告として2085の有効回答の結果を報告している。調査対象者の10%が個人情報漏洩事故に直接遭遇しており、29%が疑わしい自体に遭遇したと回答している。計約4割が個人情報漏洩事故に遭遇している状態であったことから住民が住基ネットの利用について漠然とした不安を抱えていることが伺われる。また性別では女性が、年代別では20歳代の若年層が住基ネットの利用について懸念している。プライバシー保護の観点では本来、性別や年代別などのセグメンテーションに基づきしっかりとしたケアが必要であることが本データより推察される。

上原(2004)は、自治体が抱える情報セキュリティ上の課題と対策について総括している。個人情報保護を中心としたプライバシーの問題、システム自体のセキュリ対策、特に住民サービスが従来から長い年月をかけて業務種別毎のシステムを開発し連携させてきたためにシステム構成が非常に複雑で統率が困難であるなどのガバナンスの問題点を指摘している。また早急な電子自治体化が進められる中で、自治体が抱える財政面や、それに起因した人材確保の困難性がある。またそれらの解決策として外部のITベンダーへの外注が考えられるが、新たな問題として、ガバナンス体制やセキュリティ対策の体制構築が挙げられており、多角的な観点からの包括的なセキュリティ対策の必要性が必要となる。

マイナンバーにおいても同様に情報漏洩に関するプライバシーの問題について「個人情報保護ワーキンググループ」で対策が検討されている。

「個人情報保護ワーキンググループ」の構成員である石井 (2012)は、セキュリティの一般概念であるCIA（Confidentiality（機密性）、Integrity（完全性）、Availability（可用性））という三要素を用いてマイナンバー法に関するセキュリティの考え方について考察し、マイナンバー法自体は個人情報保護法などの日本特有の事情に大きく影響され、Confidentiality（機密性）を重視した法案であり、それに違反した場合の法定刑も厳格であることなどを報告している。このことは単にシステムの安全性の観点だけでなく、法制度の観点からも情報漏洩に対する厳格な対応について言及している為、犯罪抑止力となることが期待されている。

2.2 情報システムセキュリティに関する研究について

北 (2004)は、「住基ネットにおけるセキュアな本人確認情報の流通に関する研究」の中でマイナンバーの前身でもある住基ネットにおいて住基ネットの稼働開始から 2004 年 11 月までにシステム上の脆弱性に起因する情報漏洩が起こっていないことから住基ネットのシステムとしての安全性はほぼ安心できるレベルにあると判断しても良いであろうと言及している。同様にマイナンバーにおいても総務省を中心に政府機関の為の統一管理基準に基づいたセキュリティが担保されることを考えるとマイナンバーに関連したシステム設計についても安心できるレベルになるであろうと推測できる。

実際に、住基ネットのシステムセキュリティについて懸念した長野県による「住基ネットに係る市町村ネットワークの脆弱性調査最終結果概要」[5] では侵入可能とあるが侵入は庁内 LAN のみで住基ネットのシステムには侵入することはできなかったと報告されている。

マイナンバーに関するところでは「情報連携基盤技術ワーキンググループ」の構成員である山口 (2002) を始め IT セキュリティの第一人者らが、セキュアなマイナンバーシステムの構築についての指針策定に大きく貢献している。

一方でワーキンググループの方針としても示され、情報漏洩対策として大きな位置付けを担う「符号」について、高木 (2013) らは「プライバシー保護の観点からも、情報セキュリティ技術の観点からも、無用なものであることが示された。」と明言していることからセキュリティに対する取り組みについて全ての懸念事項が払拭されたとは言い難い。

また海外の研究に目を向けると、既にマイナンバーと同様の公共サービスを提供している諸外国の中でも先行してソーシャルセキュリティナンバー（以下 SSN）を導入した米国においては技術的に高度で、かつユニークな情報漏洩の危険性が報告されている。2012 年に開催された Black Hat2012 においてカーネギーメロン大学の行動経済学者、Alessandro (2012) のチームによる報告ではフェースブックにアップされた大量のプロフィール写真を集め、顔認証技術を用いて本人を特定することが可能であるだけでなく、さらにはそこから個人の SSN まで割り出すことが可能だという実験結果を示し世界に衝撃を与えた。

本論ではマイナンバーに関連した情報漏洩事故について体系的に整理するために、このリスクは番号そのものを推測できる脆弱性、そしてフェースブックなどのソーシャルネットワークで誕生日や出身地など容易にSSN等の個人情報を入手できる脆弱性の存在を示唆するものとして位置付けることとした。この報告から、予測困難な情報漏洩事故の可能性を技術的に高度な手法で予見しており、幅広い知見に基づいた対策を講じる必要性を示唆している。

従来研究では、実際に起こっている住基ネットやSSN等に関連した情報漏洩事故の調査について網羅性及び詳細性が十分であるとは言い難く、情報漏洩事故が発生する可能性について更なる分析が重要であると考えた。新山 (2014) は、実際にマイナンバーと類似のサービスを既に展開している米国、韓国と、日本国内の住基ネットにおいて実際に発生した情報漏洩事故を分析した。日米韓における情報漏洩事故についての先行調査ではマイナンバー利用時、特に民間サービス利用時には情報漏洩事故が発生する可能性が公共サービスを利用している場合のみよりも高くなることが推測される。従って民間サービス利用時に考えられるサービスフローやシステム構成のシミュレーションモデルを構築し、そのモデルについてリスク評価を行うことが重要である。リスク評価の際には、ソーシャルネットネットワーク、ビッグデータ、クラウド、モバイルと言った加速するIT環境の主要因についても考慮し、従来存在しなかったようなセキュリティリスクを評価することも考慮した。

また、リスク評価から得られた結果から情報漏洩対策に

必要なセキュリティ対策を検討することも研究の目的とする。

3. 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

3. 1 民間サービス利用のシミュレーションモデル構築

民間サービス利用時に考えられる全てのサービスを網羅してリスク評価を行う必要があることから、人が生まれてから亡くなるまでどのような形でマイナンバーと関わるのかについてライフサイクルを基準にシミュレーションモデルを構築したイメージを図 1 に示す。そのイメージシミュレーションの中で起こり得る情報漏洩事故を予想し、そのリスク評価を行うこととする。

まずはライフサイクルの中で考えられる全てのサービス例をリストアップした。

図 1 ライフサイクルにおけるマイナンバーとの関わりとそのリスク評価のイメージ概要

福井県勝山市のホームページ上に掲載されている「ライフサイクルインデックス」[6]では人の誕生から亡くなるまでライフサイクルに応じた全てのサービスが記載されているため、シミュレーションモデル構築の際にサービス項目として列挙した。公共サービスに関連した形で民間サービスが活用されることが想定されるため関連した公共サービスを理解しておくことは事項以降のシミュレーション構築に有効であった。

別表1に諸外国におけるマイナンバー類似サービス例を調査しまとめた。

日本政府が民間利用サービスとして検討している金融サービス、医療サービス、e－コマースなどが含まれており、民間利用のシミュレーションモデル構築時の一例として列挙する際に有効であった。

諸外国の中でも特にシンガポールは、eCitizen[7]と呼ばれる独自のサービスを展開しており、マイナンバー利用時の参考として大いに役立つことから個別に詳細に調査した。

eCitizenは1999にシンガポール政府により初めて開始された国民の要望に応じた情報とサービスを提供するワンストップのポータルで、国民中心に様々なサービスを1つのトランザクションで処理することができる。財務省によって主導され、シンガポール情報通信開発庁に管理されている。このサービスは「シンガポール人が世界中どこからでも利用できる統合電子サービス提供計画」に基づき構築された、公的サービスの窓口である。省庁別サービスではなく「ライフ・イベント」で構成される。従ってライフサイクルに応じたシミュレーション構築とリスク評価の参考となると考えた。eCitizenのサービスは65組織で計451個のサービスを提供しており、1999年のサービス開始時108個から大幅に増加している。付録表3にeCitizenのサービスの例をに示した。

eCitizenの特徴としてスマートフォンとタブレット向けのアプリケーションがAndroidOS用とiOS 用にリリースされている。Android用は全組織の46% （65組織中30） がリリースしており、iOS 用は51% （65組織中33） がリリースしている。今後はスマートフォンとタブレット向けアプリケーションの利用増加が予想される。日本のマイナンバーにおいても同様にスマートフォンとタブレット向けのアプリケーションがリリースされる可能性が高い。スマートフォンやタブレット向けアプリケーションと端末自身が紛失することなどが予想され、セキュリティホールになることが想定される。

これまでの福井県勝山市「ライフサイクルインデックス」のサービス例、諸外国における民間サービス利用例、そしてシンガポールの例e-Citizenの3種類のサービス例を基に考えられる全ての公共サービスを列挙した後に重複を省いた結果を別表2に示した。

図10に考えられるマイナンバー利用時のサービスイメージを示す。マイポータル利用時に考えられるシミュレーションモデルとして様々な利用シーンが想定されるが、マイナンバーがシステムの共通IDとなり、政府が準備したシステムと民間企業のシステム間を流通する場合、マイポータルがワンストップサービスの窓口としての役割を担い、全てのサービス利用時にマイポータルを経由することと想定される。

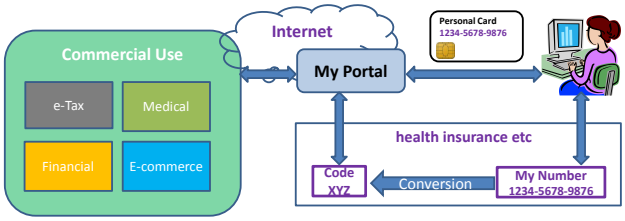

図2 マイナンバーを利用した民間サービスイメージ（筆者作）

例えば、転居の際に民間の引越しサービスを利用するケースと民間の英会話学校に申し込むケースを考えてみる。利用シーンは両サービスともに、マイナンバーをIDとしてマイポータル、企業ポータルにログインする。サービス申し込みはワンストップで進む。つまりサービス種別に依存せず、ITサービスとして共通のスキームで進行する。従って全てのサービスは同様の利用形態となり、シミュレーションすべき利用シーンが限定されることが想定される。同様に情報連携基盤技術ワーキンググループの坂本泰久構成員より提出された「マイ・ポータル等における民間連携・民間活用の実現に向けた方針（案）」[8]の中でもマイポータルを活用した5つのワンストップサービスの活用モデルが述

べられている。表1にその5つのモデルについて今村圭氏が「マイナンバーを活用した官民連携の今後」[9]の中で具体的な活用イメージとして整理している内容について抜粋し示した

表1　マイナンバーを活用した官民連携の今後

活用モデル	概　要	活用イメージ
1．バックオフィス連携	利用者本人から事前に同意を得た上で、民間事業者が必要に応じて市町村等から本人の情報を確認する。	●終身年金保険における保険者の生存情報の確認（住民票等の取得） ●激甚災害時における保険金受取人や相続人等の確認（戸籍情報等の取得）
2．公的個人認証サービスの民間拡大	個人番号カード内の本人情報（氏名、住所、生年月日、性別）を用いて、利用者本人の操作によりオンラインで利用者の本人確認を行う。	●オンラインでの銀行口座等開設時における（法令に基づく）本人確認 ●年齢や性別の確認が必要な物品・サービス（酒類等）のオンライン購入時の資格確認
3．マイ・ポータルからの自己情報の提供	利用者本人の操作により、個人番号カード内に無い自己情報をオンラインで民間事業者へ提供する。	●勤務先や健康保険組合において、被扶養者を認定するための世帯情報 ●住宅ローン等の審査に必要な所得情報の提出
4．民間事業者からの通知	民間事業者から利用者（契約者等）のマイ・ポータルへ各種情報の通知を行う。	●電気、ガス、水道等の検針情報、請求書情報等の通知 ●生命保険等の契約内容や保険料支払証明書等の通知
5．Webサイト間連携	民間事業者のWebサイトにおいて、マイ・ポータル関連サービスを提供する。	●検索ポータルの個人用ページの一部でマイ・ポータルの情報を提供

出所：今村圭氏（株式会社三菱総合研究所）「マイナンバーを活用した官民連携の今後」[9]

パターンは5つあるが、全てにおいてマイナンバーが「符号」として流通することを考えた場合、マイナンバーはPCやタブレットなどの利用者設備を通じて、マイポータルに流通し、その後行政が準備した設備や民間企業の設備を流通することとなるが、利用される設備項目はその3ヶ所となる。セキュリティ対処箇所は「利用者設備」「民間事業者設備」「行政機関設備（マイポータル含む）」の3か所に限定されるため3か所に焦点を絞りリスク分析を実施する。

3.2　シミュレーションモデルのリスク評価

リスク評価基準として一般的に認知されている Information Security Management System（以下 ISMS[10]）（JIS Q 27001（ISO/IEC 27001））を利用した。ISMS は一般財団法人日本情報経済社会推進協会（JIPDEC）が管理する ISMS 適合性評価制度であり、ISO(国際標準化機構)とJIS（日本工業規格）の両方で制定された唯一のリスク評価基準である。また情報処理推進機構（IPA）や JPCERT（Japan Computer Emergency Response Team Coordination Center）などの情報セキュリティ組織として著名な団体も運用ガイドを案内するなどデファクトスタンダードとして位置づけられている。

ISMSとは組織（企業、部、課など）における情報セキュリティを管理するための仕組みのことで、各組織の情報資産に対する様々なリスクについてリスクごとの技術的な対策を定めるだけではなく、組織によるリスク評価に基づいて必要なセキュリティ対策を講じ、システムを運用することを定める基準となるものである。

リスク値の算出についてはJIS Q 27001（ISO/IEC 27001)において以下の算出式を用いると案内されている[11]。

リスク値＝「資産の価値」×「脅威」×「脆弱性」

「資産の価値」について、今回はマイナンバーそのものである。本来は各個人ごとにマイナンバー自体の価値が異なるがリスク評価をシンプルにするためにリスク評価の前提条件として全てにおいてマイナンバーの資産価値として定数の1とする。

「脅威」について事故の発生頻度で比較。「高」「中」「低」でそれぞれスコア「3」「2」「1」とする

「脆弱性」について技術的難易度「高」「中」「低」をそれぞれスコア「1」「2」「3」とする。図11にリスク値の早見表例を示す。

リスク値早見表例

	脅威								
	1			2			3		
	ぜい弱性								
資産の価値	1	2	3	1	2	3	1	2	3
1	1	2	3	2	4	6	3	6	9
2	2	4	6	4	8	12	6	12	18
3	3	6	9	6	12	18	9	18	27
4	4	8	12	8	16	24	12	24	36

図2　出所：ISMSユーザーズガイド[25]

例えば、「脅威」が「ID詐称」の場合では事故の発生頻度が「高」となるため、スコア「3」とする。「脆弱性」が「付箋紙にマイナンバーを記載」とすると技術的難易度をが「低」であるためスコアは「3」となる。「資産の価値」は上述の条件を適用し「1」とすろと、以下の算出に従ってリスク値は「9」となる。

リスク値＝「1」×「3」×「3」＝「9」

表9に脅威スコア基準について日米韓の情報漏洩事故の頻度より推定した結果を示す。

表2　脅威スコア基準

	脅威種別（Threat Type）					
	ハッキング	盗難	ID偽称	対策不備	内部犯	Total
米国	6	5	3	2	0	16

韓国	3	0	2	0	2	7
日本	0	1	30	1	2	34
Total	9	6	35	3	4	57
割合	16%	11%	61%	5%	7%	100%
頻度	中	中	高	低	低	—
スコア	2	2	3	1	1	—

この結果から、脅威種別として「ID詐称」について発生する割合が61%と高かったことから脅威頻度「高」でスコア3とした。同様に発生頻度として発生する割合10%以上の「ハッキング」と「盗難」２を発生頻度「中」でスコア2とした。それ以下の「対策不備」「内部犯」をスコア1とした。

表3に脆弱性スコア基準について日米韓の情報漏洩事故の頻度より推定した結果示す。

表3　脆弱性スコア基準

技術的難易度	説明	スコア
高	ハッキングや APT （Advanced Persistent Threat）と呼ばれる標的型攻撃などの高度な攻撃手法が用いられる場合	1
中	ID 詐称（なりすまし）に起因した事故であるが計画的に内部に侵入した場合や他での盗難による情報を活用するなど計画性が高い場合や、犯罪組織の関与している場合	2
低	ID 詐称によるなりすまし、音声の模倣、WEB 上で情報が一般の人間でもアクセスできる状態である場合。盗難（パソコン、ハードディスク、USB などの各種記憶媒体）や単なる対策不備の場合	3

この結果から技術的難易度の高い「ハッキング」等を技術難易度「高」でスコア1とした。同様に「ID詐称」でも内部犯が関連するなどの場合は技術難易度「中」でスコア2とした。単なる「ID詐称」の場合は技術難易度「低」でスコア3とした。

別表3に、表9と10で示した基準に基づき行ったリスク評価の結果示す。

この評価では、利用者の視点ではID詐称によるリスク評価スコアが9と最も高かった。ID詐称という脅威についての脆弱性は情報漏洩事故の過去の例やISMS監査の経験等から個人番号が目につき易い所にあるということなどが考えられた。セキュリティ対策としては付箋紙をPCや机に張らないことが挙げられる。同様に紛失という脅威に対する対策としては路上に落としたり電車等に忘れたりすることが無いように配慮することが必要となる。

個人番号カードの観点では他人になりすますという脅威についての脆弱性を軽減するために保管場所をセキュアにすることや、管理徹底が挙げられる。

使用する端末や、端末のOSの観点では、過去の一般的な情報漏洩事故の事例を考えると、マルウェア感染やハッキングや盗難などの脅威についての脆弱性対策としてOSやソフトウェアのパッチ適用やバージョンアップ実施などの基本的な項目が挙げられる。

民間企業の視点では、他で入手した個人番号で従業員がアクセスする脅威についての脆弱性対策として、入退室などのアクセス制限やシステムに対するアクセス制限の実施が必要である。同様にスコアは4であるが、個人情報リスト、パソコン、磁気テープなどの盗難という脅威に対するセキュリティ対策として保管場所をセキュアにし、キーロックを実施する必要性がある。

自治体の視点では、職員の自宅PCのマルウェア感染やハッキングという脅威に対してOSやソフトウェアのパッチ適用やバージョンアップ実施などが必要となる。

情報漏洩対策としては既知の脅威に対するセキュリティ対策と技術革新に対する準備の2点が重要である。既知の脅威を知るための足がかりとして実際に発生した情報漏洩事故の調査分析を行ったが氷山の一角に過ぎない。情報が無いということは事故そのものについて攻撃者以外誰も気づいていないという可能性は否定出来ない。従って常に情報収集を継続することが必要である。

また近年のIT技術革新は目覚ましいものがあり、既存のセキュリティ対策を凌駕する攻撃が矢継ぎ早に行われる。従って常に最新のITの技術動向に対して情報収集を怠ってはならない。今後も継続したリスク評価を実施していく必要がある。

４．本研究の結論と今後の研究計画について

内閣官房と内閣府による「マイナンバー社会保証・税番号制度　概要資料」では、「諸外国の問題点を踏まえた制度」により安心・安全を確保することが記載されている。その中では2大措置として「制度上の保護措置」と「システム上の安全措置」が挙げられており、一見万全なセキュリティ対策が行われているかのように見える。

マイナンバーのセキュリティに関する従来研究は2つの観点で行われてきた。1つは「個人情報漏洩とプライバシーに関する研究」であり「制度上の保護措置」に関連するものである。もう1つは「情報システムセキュリティに関する研究」であり「システム上の安全措置」に関連するものである。

制度上の保護措置として「個人情報保護ワーキンググループ」はマイナンバー法に違反した場合の法定刑が厳格になることを報告しており、このことが犯罪抑止力として期待されている。

システム上の安全措置として「情報連携基盤技術ワーキンググループ」は「符号」を用いた安全なシステム設計の計画について報告している。

しかし高木（2013）からは「符号」方式の効果について疑問を呈した研究内容が報告されている。また海外の研究者らは、予測困難な情報漏洩事故の可能性を技術的に高度な手法で予見しており、このことから幅広い知見に基づいた対策を講じる必要性が示唆された。

これらの報告は「システム上の安全措置」に関する政府

側の報告とは異なるためシステムの安全については不安が残るものとなった。従って「情報連携基盤技術ワーキンググループ」で未だ議論が継続されている「システム上の安全措置」に焦点を絞り研究を進めていくこととした。

従来研究では、実際に起こっている住基ネットやSSN等に関連した情報漏洩事故の調査について網羅性及び詳細性が十分であるとは言い難く、情報漏洩事故が発生する可能性について更なる分析が重要であると考えた。先行調査として実際にマイナンバーと類似のサービスを既に展開している米国、韓国と、日本国内の住基ネットにおいて実際に発生した情報漏洩事故を分析した。

日米韓の情報漏洩事故を比較した結果、日本では事故発生場所が全て自治体であるが、民間利用をしている米国と韓国では発生場所が大学や企業と広がりを見せていた。この結果から、特に民間サービス利用時には情報漏洩事故が発生する可能性が公共サービスを利用している場合に限定した場合よりも高くなることが容易に推測された。従って民間サービス利用時に考えられるサービスフローやシステム構成のシミュレーションモデルを構築しそのモデルについてリスク評価を行うことが重要であると考えた。

シミュレーションモデル構築の参考情報として「福井県勝山市のライフサイクルインデックス」、「諸外国における民間サービス利用例」、「シンガポールのe-Citizen」の3種類のサービス例を用いた。これらの参考情報から考えられる全ての公共サービスと民間サービスを列挙し、シミュレーションモデル構築を試みた。その結果、ワンストップポータルやモバイルなど様々なツールを活用した利用モデルが導き出された。それをマイナンバーのケースに適用するとマイナンバーがシステムの共通IDとなり、政府が準備したシステムと民間企業のシステム間を流通する場合、マイポータルがワンストップサービスの窓口としての役割を担い、全てのサービス利用時にマイポータルを経由することが予想された。マイポータルを経由して全ての利用シーンおいてマイナンバーが流通することを考えるとセキュリティの防御対処場所は「利用者設備」「民間事業者設備」「行政機関設備（マイポータル含む）」の3か所に限定されるため、3か所に焦点を絞ってシミュレーションモデルを構築し、リスク分析を実施した。その結果、ID詐称によるリスク評価スコアが9と最も高かった。同様にスコアの高い各項目における「脅威」と「脆弱性」の内容を分析した結果、利用者の視点、個人番号カードの観点、民間企業の視点、自治体の視点からそれぞれのセキュリティ対策が明確となった。

このように個別の情報漏洩事故について詳細に分析し、事故の傾向から将来マイナンバーの民間サービス利用時に予測されるリスク評価を行った例は従来研究には無く、初めての取り組みとなった。また分析結果を基に「マイナンバーを付箋紙に記載して机に貼らない」などの具体的なセキュリティ対策を明確にしたことで実運用面からも有益なものとなった。

今後の研究計画は、より現実性の高いリスク評価を実施することが重要であるとことから、米国においてSSNの情報漏洩事故の発生確立が最も高い場所であった大学を対象とし、実際の国内大学におけるマイナンバー利用時のリスク評価を行う予定である。

参考文献

＜和文＞

豊福晋平　住民基本台帳ネットワーク・カードについてのオンライン意識調査に関する考察
情報処理学会研究報告　2004-05-08　43 号
21-26

上原哲太郎　自治体が抱える情報セキュリティ上の課題とその対策
電子情報通信学会技術研究報告. SITE, 技術と社会・倫理 104(392), 1-6, 2004-10-22

石井夏生利　マイナンバー法と情報セキュリティ
情報セキュリティ総合科学 第 4 号 2012 年 11 月

北寿郎　e-Japan 計画：住基ネットに見える課題
情報科学技術レターズ,情報処理学会 2004
347-350

新山剛司　共通番号(マイナンバー)制度における情報セキュリティー民間利用におけるリスク評価ー,ITEC（同志社大学）,2014 年 6 月号

山口英　ブロードバンド時代のインターネットセキュリティ　岩波書店　2002

高木浩光　国家による個人識別番号とその利用システムのあり方　～ プライバシーの観点から ～
情報処理学会研 究報告, Vol.2013-CSEC-61, No.29, pp.1-8」

＜英文＞

Alessandro Acquisti (2012)
Faces of FaceBook(Privacy in the Age of Augmented Reality)
: Based on a presentation at BlackHat USA, 2012

Alessandro Acquisti (2009)
Predicting Social Security numbers from public data : PNAS (Predicting Social Security numbers from public data)

Takeshi Niiyama (2007)
Thwarting information security threats in modern anonymous P2P software

＜ホームページ：2014 年 11 月 1 日閲覧まで＞

1. 平成26年度10月版　内閣官房　社会保証改革担当室　内閣府　大臣官房　番号制度担当室　マイナンバー　社会保障・税番号制度　概要資料　スライド16
http://www.cas.go.jp/jp/seisaku/bangoseido/pdf/gaiyou_siryou.pdf
2. 内閣官房　個人情報保護ワーキンググループ及び情報連携基盤技術ワーキンググループ
http://www.cas.go.jp/jp/seisaku/jouhouwg/index.html
3. 総務省の「マイナンバー付番システム等の構築に係る情報提供依頼（RFI）
http://www.soumu.go.jp/main_sosiki/jichi_gyousei/daityo/mynumber_rfi.html
4. 平成26年　総務省　公的個人認証サービスの民間拡大について

http://www.kantei.go.jp/jp/singi/it2/senmon_bunka/number/.../siryou1.pdf
5. 長野県「住基ネットに係る市町村ネットワークの脆弱性調査最終結果概要」
http://www.pref.nagano.lg.jp/shichoson/kensei/soshiki/shingikai/ichiran/j-net/kekka.html
6. 福井県勝山市「ライフサイクルインデックス」
http://www.city.katsuyama.fukui.jp/docs/uploads/data/9189_data_lib_data_130613112950.pdf
7. eCitizen
http://www.ecitizen.gov.sg/Pages/default.aspx
8. 「情報連携基盤技術ワーキンググループ」坂本泰久構成員（日本電信電話（株）情報流通ﾌﾟﾗｯﾄﾌｫｰﾑ研究所）「マイ・ポータル等における民間連携・民間活用の実現に向けた方針（案）」
http://www.kantei.go.jp/jp/singi/it2/denshigyousei/dai25/siryou2_1_1.pdf
9. 今村圭氏（株式会社三菱総合研究所）により報告された「マイナンバーを活用した官民連携の今後」
http://www.mri.co.jp/opinion/column/localweb/001346.html
10. ISMS
http://ja.wikipedia.org/wiki/%E6%83%85%E5%A0%B1%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E3%83%9E%E3%83%8D%E3%82%B8%E3%83%A1%E3%83%B3%E3%83%88%E3%82%B7%E3%82%B9%E3%83%86%E3%83%A0
11. ISMSユーザーズガイド　P33
http://www.isms.jipdec.or.jp/doc/JIP-ISMS113-21.pdf

別表1.諸外国におけるマイナンバー類似サービス例

アメリカ	銀行、信用金庫	口座開設、ローン、カード発行、過去の破産申請の履歴を調べることにより、利用者の支払能力の有無を確認
	証券会社	
	クレジットカード会社	
	運転免許の発行	本人確認
	教育	学生番号
	企業	従業員番号
	ビデオレンタル会社	本人確認
	WEB サービス（Google, PayPal, VeriSign,）	ｲﾝﾀｰﾈｯﾄｻｰﾋﾞｽ提供
	兵役（認識票）	本人確認、各種サービス提供

韓国	銀行	本人確認
	医療	カルテ、処方箋
	教育	学生番号
	企業	在籍証明書、履歴書
	不動産	賃貸契約の証明書
	通信	契約時、wifi 利用時の本人確認
	ｲﾝﾀｰﾈｯﾄｶﾌｪ	本人確認
	ゲーム	青少年利用制限実施の為の年齢証明
	実名制	（インターネット等の書き込みの際に本人証明が必要）
	テロ対策	個人管理

スウェーデン	銀行	口座開設、ｲﾝﾀｰﾈｯﾄﾊﾞﾝｷﾝｸﾞ
	医療	ヘルスケア予約サービス、診療・介護デリバリー請求、処方箋の発行、診断書・傷病証明書の発行、HER／PHR（カルテに類似）
	福祉	高齢者向けケアサービス
	企業	起業・開業登録、支払、住所移転

デンマーク	銀行	口座開設、ｲﾝﾀｰﾈｯﾄﾊﾞﾝｷﾝｸﾞ
	不動産	土地の売買等契約時に利用
	携帯電話	契約時に利用
	新聞	契約時に利用
	企業	求職、就職時

フランス 注）一部地域での試験運用	教育	出欠確認
	交通	支払
	レストラン	予約・支払
	レジャー施設	予約・支払
	駐車	支払

ドイツ	銀行	口座開設
	不動産	登記

オーストリア	医療	患者の既往歴データ蓄積（カルテに類似）
	企業	求職、就職時

オランダ	医療	詳細不明

	教育	詳細不明
	金融	詳細不明

エストニア	金融	口座開設、ｲﾝﾀｰﾈｯﾄﾊﾞﾝｷﾝｸﾞ
	医療	医療保険情報
	教育	高等学校の受験時に国民 ID 利用
	交通	乗車券（1 週間の定期券など）
	不動産	詳細不明
	運転免許の発行	
	パスポートの代替	
	駐車	支払
	犯罪歴	詳細不明

タイ	金融	口座開設、ｲﾝﾀｰﾈｯﾄﾊﾞﾝｷﾝｸﾞ
	教育	小学校等の教育
	運転免許の発行	

マレーシア	金融	ATM 利用、電子マネー
	医療	健康情報（カルテに類似）
	交通	有料道路や公共交通機関等の交通料金の精算
	運転免許の発行	
	食糧の配布	詳細不明

スリランカ	金融	口座開設、ｲﾝﾀｰﾈｯﾄﾊﾞﾝｷﾝｸﾞ
	運転免許の発行	

インド	金融	口座開設、ｲﾝﾀｰﾈｯﾄﾊﾞﾝｷﾝｸﾞ
	不動産	取引
	電話	契約
	自動車	購入
	貧困層の身分証明	本人確認
	不法移民とテロの脅威への対処	詳細不明

別表2. マイナンバーを利用したサービス例

ライフサイクル	住民サービス	民間サービス
誕生	出生届 マイナンバー申請交付 母子健康事業（手帳配布、健康診査） 国民健康保険（加入手続き、出産育児一時金）	
育児	子ども福祉（医療費、児童手当、保育園、支援） 予防接種	
教育	幼稚園 小・中学校・高校・大学 児童、学童クラブ 教育相談	

		英会話などのサブカルチャー等　（申し込みや支払）
成人	国民健康保険（加入手続き、出産育児一時金） 国民年金 選挙 税金（市民・県民税、固定資産税、自動車税） 生活環境（ごみ、上下水道） 転入、転出、転居 住民票請求、印鑑登録・証明 福祉（母子、父子家庭、難病患者支援） 各種健診 すまい（市営住宅入居、住宅に関する助成制度） ペット（愛犬の登録、狂犬病予防注射） スポーツ施設利用 運転免許センター（国土交通省） 船舶免許、航空免許　（国土交通省） パスポート発行　（外務省） 公共レジャー施設利用	引越し会社（公共の転入転出情報と関連し手配可能） ケアセンター 民間レジャー施設利用（予約・支払） 金融機関　（銀行、証券、クレジットカード）（口座開設、インターネットバンキング、ローン、カード発行、ATM 利用、電子マネー） 保険会社 医療　（カルテ、処方箋、予約、診療・介護デリバリー請求、診断書・傷病証明書の発行、デイケアサービス、医師の登録） 企業　（個人向け）従業員番号、在籍証明書、履歴書、求職、就職時 企業　（企業向け）起業、開業登録、支払、住所移転、求人 インターネットサービス（Yahoo, Google, Equifax, PayPal, VeriSign, Wave Sys, Verizon, Wi-fi などの ID 管理）（ショッピング、検索、支払） 不動産　（登記、賃貸契約の証明書） 固定電話、携帯電話会社　（契約時の本人確認、サービス申請や支払） 電気、ガス　（契約時の本人確認、サービス申請や支払） 新聞会社　（契約時の本人確認、サービス申請や支払） 交通機関　（有料道路や公共交通機関等の交通料金の精算） レストラン　（予約・支払） 駐車場（管理会社）　（支払） 建築会社　（建築プランのオンライン申請や費用の e-Payment（電子ペイメント）） 医療機器会社、薬局（店舗の情報等提供） 弁護士会　（弁護士の登録） 旅行会社　（旅行申し込みや支払）
老後	各種健診	

	後期高齢者医療制度 国民年金 高齢者福祉 介護保険	
死亡	死亡届	葬儀場（埋葬、火葬、墓地等に関する申請やサービス）
緊急時	防犯、防災	

別表3.マイナンバーを利用したサービス例

場所	対象	脅威	スコア	脆弱性	スコア	リスク評価
利用者	利用者	ID 詐称	3	個人番号が目につき易い所にある。 例）付箋紙を PC や机に張る等	3	9
		操作ミス	1	知識不足など	3	3
	個人番号カード	ID 詐称（なりすまし）	3	・紛失 例）路上に落とす。電車等に忘れる	3	9
		盗難（カード自体、鞄や財布などに入れていた場合など）	2	・保管場所がセキュアでない。 ・不用意な管理	3	6
		他人のカードを利用したなりすまし	3	・保管場所がセキュアでない。 ・不用意な管理	3	9
		アングラサイト等での個人番号購入	1	信頼できないサイト等への容易な個人番号情報提供	2	2
		FB 等の SNS からの情報漏洩	1	不用意な情報アップロード	2	2
	電子証明書パスワード	ソーシャルエンジニアリング（ゴミ箱拾うなど）	1	付箋紙等に書いたパスワードを安易にゴミ箱に捨てる	3	3
		パスワードクラック	1	推測容易（誕生日など）なパスワード設定	2	2
	アクセスする端末（PC,ﾀﾌﾞﾚｯﾄ,ｽﾏｰﾄﾌｫﾝ）	マルウェア感染ハッキング	2	OS やソフトウェアのパッチ未適用 バージョンアップ未実施 脆弱性対策未実施	2	4
		盗難	2	・保管場所がセキュアでない。 ・不用意な管理	2	4
	ソフトウェア（PC,ﾀﾌﾞﾚｯﾄ,ｽﾏｰﾄﾌｫﾝ用）	マルウェア感染ハッキング	2	OS やソフトウェアのパッチ未適用 バージョンアップ未実施 脆弱性対策未実施	2	4
		盗難	2	・保管場所がセキュアでない。 ・不用意な管理	2	4
民間会社	民間会社従業員	内部犯	2	・入社時の人物評価の精度（道徳や倫理観） ・入退室などのアクセス制限 ・システムに対するアクセス制限	1	2
	マイ・ポータルとのインターフェースの	マルウェア感染不正侵入（ハッキング）	2	OS やソフトウェアのパッチ未適用 バージョンアップ未実施 脆弱性対策未実施	1	2
		他で入手した個人番号で従業員がアクセ	2	・入退室などのアクセス制限 ・システムに対するアクセス制限	2	4

	システム	ス				
		対策不備（DB が容易にアクセスできる状態など）	1	・セキュリティ監査の精度	3	3
		盗難（リスト、パソコン、磁気テープなど）	2	・保管場所がセキュアでない。（キーロックなどが未実施）	2	4
		紛失	2	・持ち運びや保管方法の徹底	2	4
		ID 詐称	3	・偽物のサイトの存在	2	6
自治体 情報保有機関（市町村）・住基ネット	職員	内部犯	1	・入社時の人物評価の精度（道徳や倫理観） ・入退室などのアクセス制限 ・システムに対するアクセス制限	1	1
	自宅 PC	マルウェア感染ハッキング	2	OS やソフトウェアのパッチ未適用 バージョンアップ未実施 脆弱性対策未実施	2	4
	住基ネット **LGWAN** マイポータル	住基ネットで省庁及び自治体が構築したシステム及びネットワークでは情報漏洩事故が発生しなかったことから今回も安全と仮定する。 注）事故が 100%発生しないということではない。				—