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

同志社大学大学院総合政策科学研究科

技術・革新的経営専攻　博士課程（一貫性）

2011年度　　1003

目次

第１章　本研究の目的と本論文の構成

１　マイナンバー法とセキュリティ対策の概要

2016年1月施行予定の共通番号（マイナンバー）制度によって日本に居住する外国人を含む全住民に付与されるマイナンバーの漏洩防止は、個人情報の保護という点だけでなく今後の我が国の情報通信産業の競争力強化という観点からも重要な課題である。住民基本台帳ネットワークシステム（以下「住基ネット」）とマイナンバーで大きく異なる点は、住基ネットの利用範囲が住民サービスに限定されているのに対し、マイナンバーの利用範囲が民間利用にまで拡大されている点である。

全住民規模での個人番号付与とその民間利用という施策は、我が国にとってのチャレンジである。主管官庁である内閣官房や内閣府等は様々な観点からのマイナンバー制度における個人情報保護対策の検討を行っているが、より詳細で網羅性の高い研究が求められている。

マイナンバーの前身である住基ネット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。

総務省（2014）によると、マイナンバーは住基ネットを後継する形で、更に民間への利用まで検討されている。民間利用では、公的個人認証法の民間拡大について、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いる。

マイナンバーを民間利用する場合、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、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へと拡がることから情報漏洩の可能性が更に高くなると予想される。

内閣官房と内閣府（2014）による「マイナンバー社会保証・税番号制度　概要資料」に記載されているマイナンバーが流通する方法や民間システムとの連携について、その内容を図1に示す。

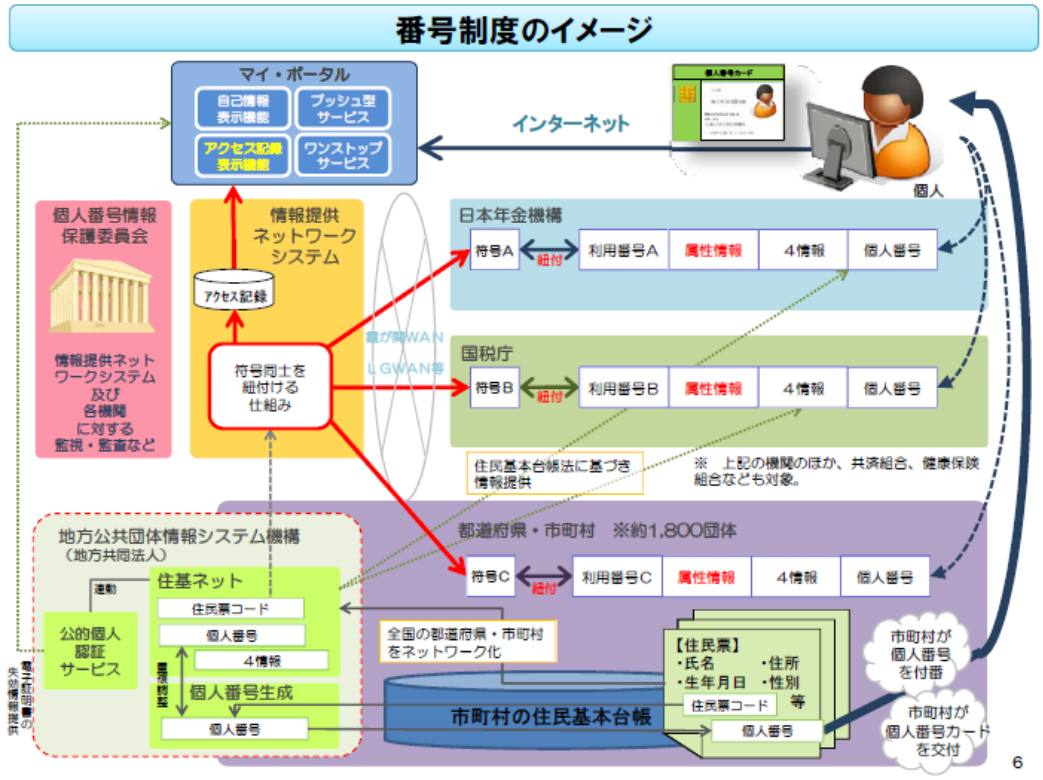

図1　番号制度のシステム連携イメージ

出所：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」

マイナンバーのセキュリティ対策については「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。2大措置として「制度上の保護措置（制度）」と「システム上の安全措置（技術）」が挙げられており、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」[1]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。12名中11名（92%）が法律分野の権威である。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。11名中9名（82%）は情報セキュリティ分野の権威である。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。これはシステム設計における概要設計、基本設計、詳細設計での概要設計に該当する。概要設計レベルでのセキュリティ対策となるため、システム構築における詳細設計レベルではセキュリティ対策が完全では無いことも懸念される。

（１）制度上の保護措置（制度）

「制度上の保護措置（制度）」について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」で個人情報保護に関する法整備について検討されている。

島田（2012）は、国民のマイナンバー制度に対する懸念で最も多かったのは個人情報漏洩事故とプライバシー侵害（40.5%）であるという内閣府の世論調査（2011）を受けて、制度上の保護措置として第三者機 関(いわゆる三条委員会)の設置による監視、法令上の規制等の措置(目的外利用の制限、閲覧・複写の制限、守秘義務等)、および罰則強化等で対応する予定だとしている。

政府主導の住民サービスにおける個人情報漏洩の懸念は、マイナンバーの前身である住基ネットの2002年稼働以前から指摘されてきた。

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歳までに対して2003年10月24日から27日まで住基ネットカードの利用に関する意識調査についてオンラインウェブアンケートを実施し、2085の有効回答の結果を報告している。結果によると調査対象者の10%が個人情報漏洩事故に直接遭遇しており、29%が疑わしい事態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を示している。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いた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。

「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る。

企業側もマイナンバーに関連した個人情報の取扱いについて積極的に取り組んでおり、日本ユニシスの寺田（2005）は、個人情報保護に関するガイドライン情報及び企業の個人情報保護対策の進め方を示した。

（２）システム上の安全措置（技術）

「システム上の安全措置（技術）」について、総務省をオブザーバーとした「情報連携基盤技術ワーキンググループ」で対策方法や運用について議論されている。

マイナンバーに関する情報システムの調達は総務省の「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」[2]の指針に基づき比較検討が行われ、厳しいセキュリティ基準が設けられている。

「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)らの IT セキュリティ第一人者が、国内ではインターネットにおけるセキュリティの啓蒙活動を続け、マイナンバーにおいてもセキュアな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。

その中身は図1に示すように政府が構築予定の「情報提供ネットワークシステム」と呼ばれる情報連携のための専用システムを意味する。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。情報連携ではこの「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。

マイナンバーの前身である住基ネットのシステムセキュリティについて振り返ると同様に研究者や自治体が報告を行っている。

北（2004)は、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、概ね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。

このことからマイナンバーの「情報提供ネットワークシステム」についても高度なセキュリティシステムが構築されることが予想される。

一方で長野県（2012）によると「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」のとおり、幾つかの脆弱性が報告されている。特に脆弱性としてリスクが高いものを下記に抜粋する。

- 既存住基サーバの管理者権限のユーザ名及びパスワード設定に問題があり、庁内 LAN に接続した調査用コンピュータにより管理者権限で正規のユーザになりすましてログオンが可能であった。更にこの際、データベースのユーザ名及びパスワード設定に問題があったので、データベースの内容を閲覧することが可能であった。

- 既存住基サーバで使用されている OS には既知の脆弱性が存在しており、庁内 LAN に接続した調査用コンピュータにより、この脆弱性を利用して管理者権限を奪うことが可能であった。

上記 2 つの脆弱性は運用上の課題である。厳しいセキュリティ基準でシステムが設計されたとしても使う側のセキュリティスキルや意識に問題があった場合は脆弱性が発生する。

更に、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、既に複数の研究者から技術面でのセキュリティ上の問題が指摘されている。

高木（2013)は、「符号」を活用してもシステムが連携した結果、「符号」と連動した個人情報が入手可能であることから「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。」と酷評している。

同様に李（2013）は、現状の符号を用いた情報連携の場合、同じ時間帯で複数の人を対象に同じサービス業務を実施した場合、情報連携元と連携先機関のログには、連携した機関名と情報の用途など、ログの内容の一部が複数に亘って同一に記録される可能性が高く、この様なケースでは、ログの記載順番から同一人の位置を突き止めるのが容易であるため、連携先でのログ記録の順番に工夫する必要があると報告している。

これらの報告からセキュリティに対する技術面での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。

（３）「体制（人と組織）」の整備

前節で「制度上の保護措置（制度）」と「システム上の安全措置（技術）」の2大措置について説明した。加えて措置を実行するための対策方法や運用を実際に行う「体制（人と組織）」の整備は2大措置と同等に非常に重要な課題である。

上原（2004）は、マイナンバーを導入する自治体のセキュリティ対策についても「個人情報保護を中心としたプライバシーの問題（制度）」、「システム自体のセキュリ対策不備（技術）」、「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（体制）」の３つの分野についてセキュリティ対策を講じる必要性があることを改めて論じている。

木村（2004）もプライバシー保護対策、情報インフラの整備、情報提供やアクセシビリティの向上、ワンストップサービス化など多くの課題を指摘しているが、CIOなどのIT人材育成、マネージメント改革や業務の見直しなどの課題も強く指摘している。

同様にKitamura（2006）は、兵庫県庁における情報セキュリティの取り組みについて報告する中で、情報セキュリティについて兵庫県の担当は業務をアウトソーシングしているが、マネージメントを行うための情報セキュリティに関する知識が不足している点を指摘している。セキュリティに関連するJ-SOX法などの新たな取り組みに対応できるのは一部の組織だけであり、相対的に対応が遅れていることを問題提起している。

手塚（2015）の報告によると、我が国では内閣官房内閣サイバーセキュリティセンター(National center of Incident readiness and StrategyforCybersecurity) がサイバーセキュリティ対策の中核を担っており、2014年11月6日にはサイバーセキュリティ基本法が

成立し、サイバーセキュリティ戦略案の策定、国の行政機関による施策実施の推進や評価、有事の際の対応や調査などを実行しているとしている。

サイバーセキュリティ戦略本部は内閣関連組織であるIT総合戦略本部や国家安全保障会議と連携し、立案したサイバー戦略を内閣に提示すると共に行政各部の指揮監督に関する意見具申を行っている。その役割の中では国際イベントである2020年東京オリンピックとパラリンピックに向けた対策の強化も担っている。

サイバーセキュリティの推進において最高情報セキュリティ責任者と称されるChief Information Security Officer (CISO)を中心とした体制の確立、セキュリティポリシーを中心とした情報セキュリティ関連規則や文書類の整理、情報セキュリティ教育、情報セキュティ監査などの整備が必要となると述べている

マイナンバーの情報漏洩対策に関連した体制の問題についても同様に自治体や民間企業においてCISOを中心として体制を確立する必要がある。その点についてHonda (2012) はマイナンバー制度導入の成功の鍵を握るのはリーダーの存在が不可欠であり政府CISOがそれを担うべきであると説いている。

しかし、独立行政法人情報処理推進機構（IPA）の報告（2013）では「CISOはいない」と答えた企業が1801社のうち57.7%に達し、現実の企業運営においてセキュリティ管理体制が構築されていないことが伺える。CISOには技術、経営、法務、組織を体系的に習得したリーダーとしての専門知識が必要である。

牧野（2007）は、実際の情報漏洩事故が発生した際の再発防止においても人的情報セキュリティ対策、即ち企業倫理の確立や法遵守の徹底を中心とした人間系の対策が最も重要であり、そのために必要な以下の10項目を示して結論付けている。

（1）行動基準の徹底（2）プロジェクト管理における情報セキュリティ対策の強化（3）技術的・システム的な情報セキュリティ対策強化（4）協力会社における情報セキュリティ管理体制の強化（5）オフィスセキュリティの強化（6）情報セキュリティ教育の充実・強化（7）セキュリティ事故関係者に対する処分（8）モニタリング活動の強化（9）予防法務機能の強化（10）組織体制等の強化

Chief Information Security Officer (CISO)が日本国内で不足していることは既に述べたとおりであるが、牧野（2007）の提唱する項目を実行するために現場で活躍すべきセキュリティ人材についても人材不足の問題がある。

独立行政法人情報処理推進機構（IPA）（2014）は日本における情報セキュリティ人材の需要、供給能力、キャリアパスに関する調査結果を報告している。報告によるとセキュリティ技術者は23万人存在するが業務を遂行するうえで十分なスキルを有する者は約9万人であり、現実的に必要な人材が8万人程度不足しているとしている。学術機関では大学院、大学、高等専門学校、専門学校で受講可能な学生が約2万人在籍しており、論文等を執筆している学生が約1000人程度であり、全体的に不足しているとも述べている。更にはセキュリティに従事する人材としてサイバー攻撃に精通しインシデント対応を行ったりシステムの脆弱性を発見したり、また欠陥の無いシステムを構築出来る人材が求められるが中長期的な育成や企業側における安定した雇用形態などが必要と報告している。

セキュリティ対策について人や組織の問題は現実の情報漏洩事故において大きな影響を及ぼすため、人材育成を実施し、セキュリティ人材を確保することが必要である。

２　本研究の目的

本研究では、マイナンバーを民間利用する場合のリスクを明らかにすることが最大の目的である。

着目すべき3つの分野の中で既に法整備されたマイナンバー法を除いた「技術」「体制」の2つの分野に着目し、安全措置の中で対策や実際の運用で不足している点を明らかにする。その結果、法整備の見直しが必要な内容が生じた場合は、見直しについても提言する。

マイナンバーに関する「技術」「体制」の2つのセキュリティ分野の従来研究の情報から以下の観点で問題点を明確にする。

- 従来研究から現在までの情報漏洩事故の取り組みについて調査し、最新の攻撃手法やその防御法について学び、それらの攻撃手法がマイナンバーの民間利用の際にどのような脅威となるか考察する。

- 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発生した情報漏洩事故を調査し、事故の発生場所、脅威種別、技術的難易度を明らかにする事によりマイナンバーを民間利用した際に情報漏洩が発生する可能性を明確にする。

- マイナンバーの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一般的なシミュレーションモデルを構築し、そのモデルについて独自に考案したリスク評価手法を用いて情報漏洩のリスク評価を行う。そのリスク評価結果に基づき必要なセキュリティ対策を立案する。

- より具体的なリスク評価の実施のため民間利用の例として大学を選定し、既に発生した個人情報漏洩事故を調査分析する。それぞれの事故において、誰（人物）が、どのような業務を行っている際に発生したのか、またその攻撃についてどのような脅威種別で、実現するためにどの程度の技術難易度が必要とされるのか、について明確にする。

- 実際の国内大学におけるマイナンバー利用の業務ごとのシミュレーションモデルを構築し、そのリスク評価を独自の手法で実施し、必要なセキュリティ対策を立案する。

人や組織に関連する「体制」について、第２章で後述する従来研究の調査結果から、情報漏洩事故においてヒューマンエラーに起因したものが多いため、その防止策が情報漏洩事故防止にとって非常に重要であることがわかった。従って以下の取り組みにより問題点を明確にし、その対策を立案することとした。

- ヒューマンエラーの分析手法は、特に人の命に関わる航空、鉄道、船舶、電力、ガス、原子力、医療などの各分野で研究が進んでいるが、ITセキュリティ業界では最適な分析手法が未だ確立されていない。従って、各分野で確立された代表的なヒューマンエラーの分析手法の調査比較を行い、最適な手法を選択する。

– 選択し、独自に改良したヒューマン分析手法を、実際に過去に発生したマイナンバー漏洩事故に適用実験し、情報セキュリティに最適な分析手法を評価する。またその評価結果を実運用に活用できるかどうかについて可能性を模索する。

本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セキュリティを高めるための提言を試みた。

3　本論文の構成

前述のとおり、本研究は、2016年1月施行予定の共通番号（マイナンバー）制度の利用範囲が民間利用にまで拡大された際の個人情報漏洩のリスク評価が目的である。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、既に情報漏洩事故が発生していることから、マイナンバーを民間利用した際には情報漏洩事故のリスクが存在するという仮説を立て、それを検証することが筆者の研究動機になっている。

前項の研究目的を説明するために、第１章以下を下記の構成とした。

「第１章　本研究の目的と本論文の構成」

マイナンバーの利用範囲が民間利用にまで拡大されている点から、情報漏洩のリスクが懸念されている。

マイナンバー法は既に法整備されたため「制度上の保護措置（制度）」を除いた「システム上の安全措置（技術）」と「体制（人と組織）」に着目し、安全措置の中で対策や実際の運用で不足している点を明らかにした。

「第２章　個人情報漏洩事故に関する従来研究」

日本で話題となった年金機構の個人情報漏洩事故や、海外の研究者らによる、遠隔からアクセスされ自動車の制御を奪われる脆弱性の報告を調査し、最新の攻撃手法やその防御法について学び、攻撃手法がマイナンバーの民間利用の際にどのような脅威となるか考察する。

情報漏洩事故は増加の傾向にあり、中でも事故原因の半数以上はヒューマンエラーに起因すると報告されていることからヒューマンエラー防止策の重要性を示す。

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から個人のソーシャルセキュリティーナンバー（SSN）まで割り出すことが可能だという実験結果などから、同様にマイナンバーの利用用途を拡大するとリスクも拡大することが示唆されたため、民間利用における情報漏洩のリスクを明確にする。

「第３章　諸外国におけるマイナンバー類似サービスの情報漏洩事故分析」

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米国、韓国において発生した情報漏洩事故を調査し、事故の発生場所、脅威種別、技術的難易度を明らかにする。調査結果に基づきマイナンバーを民間利用した際に情報漏洩が発生する可能性を明確にする。

「第４章　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」

マイナンバーの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一般的なシミュレーションモデルを構築し、そのモデルについて独自に考案したリスク評価手法を用いて情報漏洩のリスク評価を行う。またそのリスク評価結果に基づき必要なセキュリティ対策を立案する。

「第５章　大学におけるマイナンバー利用時の個人情報漏洩のリスク評価」

より具体的なリスク評価の実施のため民間利用の例として大学を選定し、既に発生した個人情報漏洩事故を調査分析する。それぞれの事故において、誰（人物）が、どのような業務を行っている際に発生したのか、またその攻撃についてどのような脅威種別で、実現するためにどの程度の技術難易度が必要とされるのか、について明確する。実際の国内大学におけるマイナンバー利用の業務ごとのシミュレーションモデルを構築し、そのリスク評価を独自の手法で実施し、必要なセキュリティ対策を立案する。

「第６章　ヒューマンエラーの防止策」

航空、鉄道、船舶、電力、ガス、原子力、医療などの各分野で既に確立された代表的なヒューマンエラー分析手法である「4M-5E」、「Medical SAFER」、「VTA」について、どの手法が情報漏洩事故の分析に最も適しているか実際に発生した漏洩事故を適用実験した。

その結果、4M-5EとVTAのフローチャートを併用したモデルが最適であることを詳細に説明する。

「第７章　4M-5EとVTAを組み合わせたヒューマンエラー分析のマインナンバー漏洩事故への適用実験」

VTAと4M-5Eの組み合わせ分析手法を茨城県取手市における個人番号（マイナンバー）を誤記載した住民票交付事件に適用実験した。その結果、VTAを用いて関連者や関連物を時系列で視覚化し、その関連性を明確にしたうえで4M-5Eを適用したところ、分析項目ごとに問題点を漏れ無く抽出できた。それに基づいて項目ごとにその背後要因の探索を容易に実施できた。最終的に対策案がマトリックスにおいて各項目の交差点上に容易に導き出されることを詳細に説明する。

「第８章　本研究のまとめとマイナンバーのセキュリティを高めるための提言」

本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セキュリティを高めるための提言を示す。事故が発生してしまった際には状況を正確にまとめ分析した結果を報告し、マイナンバーが漏洩するリスクと対策案を考える手法としてシミュレーションモデルを用いたリスク評価の活用について述べる。更に、発生した事故がヒューマンエラーに起因するものであった場合は、VTAと4M-5Eとを組み合わせた分析手法を活用する事について述べる。

第２章　個人情報漏洩事故に関する従来研究

１　システム上の安全措置（技術）に関する研究

2015年5月に発生した日本年金機構の個人情報漏洩事故は我々の記憶に新しいところである。本事故は、我が国における情報漏洩事故の中でも極めて規模が大きいだけでなく、国家が保有する情報システムに対する攻撃であることから国家の安全保障を揺るがす程の社会的大問題となった。これを受け政府与党は、2016年1月施行予定であったマイナンバ

ー制度と基礎年金番号との連結の開始時期を当初予定の来年１月から延期する調整に入った。

日本年金機構の報告（2015）によると、機構のシステムがサイバー攻撃を受け47都道府県すべてに渡って総計約125万人、年金受給者52万8795人の個人情報が流出した。個人情報は基礎年金番号、氏名、生年月日、住所の4種類であった。日本年金機構の職員が受信したメールは件名が「厚生年金基金制度の見直しについて（試案）に関する意見」というもので、メール末尾にあるURLをクリックしたところコンピューターウイルスに感染したとされている。日本年金機構が所有する全てのパソコンにはウイルス対策ソフトが導入されていたが、このウイルスは「新種」と呼ばれる未知のウイルスでウイルス対策ソフトの最新版の定義ファイルでも検知出来なかった。その後の調査で、このウイルスはパソコンの利用者IDを搾取し、更に送り込まれたウイルスを誘導し、最終的に感染したパソコンを乗っ取るものであった。感染端末は日本年金機構のネットワークからインターネット介して他のサーバーと通信を行っており、その不審な動きを内閣サイバーセキュリティセンター（NISC）が感知し、本事故がようやく発見された。

日本機構の職員は不審なメールを開かないように教育されていたとしている。しかし近年はサイバー攻撃の手法が、専門家でも危うく騙されてしまうほど巧妙化している。現に本事故においても件名も担当の関連業務であるかのように意図的に作成されている。

情報漏洩事故に繋がったその他の要因としては、インターネットから切り離されているCLOSED(閉鎖的な)ネットワークで利用されていた社会保険オンラインシステムから、記録媒体（CD-ROM）等を用いてインターネットに接続されたファイル共有サーバへ個人情報をコピーし、作業していた点も挙げられる。日本年金機構の内規では個人情報をファイル共有サーバへ保存することを原則禁止していたとしている。また日本年金機構の内規では、個人情報を保存する場合にはファイルに「人に推測されにくいパスワード」を設定することを義務付けていたにも拘らず、個人情報を保存する場合に、一部のファイルにしかパスワードが設定されていなかった。更には1回目のウイルス感染の発生後に全職員へ注意喚起が通知されたが、通知の不徹底から別の職員が再度標的型攻撃メールに添付されたファイルを開封し、2回目以降のウイルス感染が発生したとされている。

この事件からシステム上の安全措置（技術）について対策が必要な項目を以下に述べる。

- 「新種」のウイルスにも対応出来る対策を検討する。
- 個人情報をファイル共有サーバへ保存する際のアクセス制限を行う。

・　　個人情報を保存する場合にはファイルに「人に推測されにくいパスワード」を設定することをシステムで検知する仕組みを取り入れる。

今回は公共サービスにおける情報漏洩事故であったが、実際には一般市民に普及しているライフラインやエンターテイメントのサービスにも影響を及ぼすためサイバーセキュリティ対策は一般市民にとっても非常に重要な問題となっている。

MILLER（2014）らが報告した内容によると、自動車会社のクライスラー社のクライスラーの車内インターネット/エンターテインメントシステム「Uconnect」に脆弱性が発見された。脆弱性を利用された場合、遠隔からアクセスされ自動車の制御を奪われるため悪意のある第三者が利用した場合は最悪の場合、殺人カーを利用した殺人劇が繰り広げられることとなる[3]。

脆弱性を持つ対象の車種は 2013 から 2014 年にかけて生産されたダッジ・ラムとダッジ・バイパー、2014 年生産のジープ・チェロキー、グランドチェロキー、ダッジ・デュランゴであり、その数は合計 47 万 1000 台に達するとしている。興味深いのはその脆弱性の対処方法である。対処方法は車両識別番号(VIN)をもとに自分の車に脆弱性があるのかどうかを確認し、対象車種であれば修正プログラムを USB メモリにダウンロードし、Uconnect システムの USB ポートからアップデートを適用するというものである。自動車というオフラインの製品の修理について従来は、自動車整備工場などのオフラインで行われてきたが、製品の一部が IT 化され、問題が発生すると IT で修復するというような時代に様変わりしている。

英国の Pen Test Partners（2015）という民間会社の報告では、韓国 Samsung Electronics 社が提供しているスマート冷蔵庫（型番：RF28HMELBSR）に脆弱性があり、悪意のある第三者に利用されると Google サービスへのログイン情報が盗まれる恐れがあるとしている。Google サービスは様々なサービスと連携しているため悪用された場合の被害は膨大なものとなると予想される。このように生活に身近な存在である冷蔵庫がサイバー攻撃の対象となるような時代になった。

Google社による自動運転自動車や家庭内の家電遠隔操作が実用化され、様々な製品がインターネットを通じてつながるInternet of Things（IoT）の時代が到来しつつある現在、サービスやインフラなどの全ての産業がサイバーセキュリティ対策を講じる必要性がある。

手塚（2015）によるとサイバー攻撃手法は様々な目的で開発されている。理由として従来の爆弾を落とすなどの物理的な攻撃手法に比べてメリットが多いとされている。例えばサイバー攻撃はプログラムが中心であるため高価な部品を必要としない、それらの管理コストなども不要であるため全体期なコストパフォーマンスが高い、インターネット経由であるため攻撃者の特定が困難で時間がかかる、またインターネットに関連した技術革新が早く、攻撃手法が容易に発見されるのに比べて防御する側はその準備が間に合わない、などが理由として挙げられる。新たな攻撃手法に対する防御策について技術面から多面的に検討することが必要であることが改めて述べられている。

情報漏洩事故に関する技術面（システム上の安全措置（技術））の研究は、日本国内においても2006年に個人情報保護法が施行されて以来、情報漏洩事故の社会的関心の高まりを受けて、様々な手法で行われてきた。

荒井（2004）は、情報漏洩防止システムの提案の中で、機密情報を暗号化するだけでなく、強制アクセス制御により情報漏洩を防止する試みを発表している。この機能があれば日本年金機構の事故の際には仮に「新種」のウイルスに感染したとしても個人情報漏洩が防げたかもしれない。

榊原（2011）は、ログ分析による情報漏洩監視を提唱している。ファイルを追跡出来る様々なログを監視し機密情報が組織外へ持ち出されたか確認することが可能となるからである。この機能があれば日本年金機構の事故の際には個人情報漏洩事故発生後、いち早く事故に気づき、初動対応が更に迅速に行えたかもしれない。

Niiyama（2006）は、Winnyを利用した情報漏洩事故の防止を目的としてWinnyアラナイザーと呼ばれる分析ツールでWinnyネットワークを解析した。結果、漏洩したファイルがどのように拡散するかについて調査分析し、その対策を政策提言した。

従来から技術的なセキュリティ対策は行われてきたが、情報漏洩事故を根絶するに至るまでの技術は発明されてはいない。

舘（2006）は、企業におけるセキュリティ対策は いたちごっこの側面があり、完全なセキュリティ対策システムというものは存在せず、システムの運用を通して対策の見直しやフィードバックを繰り返していく必要があると述べている。加えて仮にインシデントが発生した際に、 素早く状況を把握し、対策立案・実施するためにはある程度組織だって動けるような体制の必要性を述べており、現実的な組織として企業や組織におけるセキュ

ティ活動専門組織として昨今各企業が社内に設置しているCSIRT(Computer Security Incident Response Team)の提唱や、各国レベルで公共的な活動を行うチームである米国のCERT/CCや日本のJPCERT/CCなどを紹介している。

次項から体制（人や組織）に着目した従来研究を紹介する。

２　体制（人や組織）に関する研究

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情報漏洩はまさに個人情報漏洩である。

米国大手通信会社ベライゾン（2014）のグローバルセキュリティレポートによると95カ国、63,000件以上のセキュリティ事故を調査対象とし、その中には1,367件の漏洩事故が含まれていたと報告している。

筆者も協会員を務めたことのある日本セキュリティ協会（2008）からも情報漏洩事故は増加の傾向にあると報告されているとおり依然として大きな社会問題となっている。中でも事故原因の半数以上はヒューマンエラーに起因すると報告している。報告によると2011年の情報漏洩事故の原因としてヒューマンエラーとして分類される「誤操作」が34.8%,「管理ミス」が32.0%,「紛失・置忘れ」が13.7%,であり、3項目の合計は 80.5%を占めた。

ヒューマンエラーとは、「意図しない結果を生じる人間の行為」と規定[4]されており、人為的過誤や失敗のことである。ヒューマンエラーを起こす場合には注意力の欠如、披露、錯覚などが原因と考えられている。

Reason（1994）はヒューマンエラーが、人の行動の、どの時点で発生したのかに着目し、以下の4つの体系で定義している。

・スリップ(錯誤):うっかりして意図せずに犯してしまうエラー
・ラプス（失念）:し忘れによるエラー(ど忘れ)
・ミステイク:正しく実行できたが、計画自体が間違っていたことによるエラー
・違反:意図して実施しない。手抜きをするエラー

これらの定義ごとに発生した情報漏洩事故について分析する必要がある。

また事故を起こした本人だけでなく組織全体や組織の管理者の意識、また周辺の環境などの要素を取り入れることも必要である。

ヒューマンエラーに起因した情報漏洩事故については、エラー発生の詳細な状況分析と対策立案の手法について具体的な方法が提示される必要がある。

日本国内では情報セキュリティ心理学とトラスト（Security Pasychology & Trust）[5]が2008年にヒューマンエラー防止フレームワークの研究グループとして発足した。情報セキュリティ心理学とトラストはセキュリティに関する研究を心理学、人間工学、安全工学等の面から進めており、ヒューマンエラー防止が最大の研究テーマとなっている。

江崎（2005）は、ヒューマンエラー対策には個人の問題を考えるだけでなく、個人が属する組織での継続的な運用が必要であるとしている。

ヒューマンエラーの分析手法は特に人の命に関わる航空、鉄道、船舶、電力、ガス、原子力、医療などの各分野で研究が進んでいる。

鈴木（2004）は、JR東日本の事故防止策検討の一環としてヒューマンエラーの分析ツールとして代表的な「4M-4E」を適用し、鉄道事故防止の観点から、事故調査の担当者のみならず、安全管理を行う社員と現場で活動する社員にも有用であるため、より一層の浸透を図りたいとしている。

伊藤（2004）は、船舶運航におけるヒューマンエラーの分析において代表的な「m-SHEL」を用いて事故を軽減する手法を紹介している。

高川（2004）は、海外の原子力発電所における事故事例の収集に基づきヒューマンエラー分析のための現場で理解されやすいヒューマンエラー事例シートを作成した。

各分野で確立されたヒューマンエラー分析の手法は各組織で導入されており、事故事例が収集分析され、人の教育などの組織的取り組み、エラー発生を未然に防ぐための作業環境改善に取り組んでいる。

上野（2011）は、ICT（Information Communication Technology）における障害分析にヒューマンエラー分析を導入する重要性を述べている。

サイバーセキュリティ分野においては、主に各分野で確立された手法をサイバーセキュリティ分野の情報漏洩事故に適用する形で多くの研究が進められている。

川越（2008）は、情報漏洩事故においてヒューマンエラーに起因した事故が多いことから人的要因が関係する情報セキュリティ事故については、従来から行われてきた技術対策では不十分であり、ヒューマンエラー防止策が大きな課題だと指摘し、その取組の必要性を論じている。中でもエラーを誘発する要因(PSF: Performance Shaping Factor)を分析したうえで評価するなどの組織的エラー管理が不可欠であると指摘している。

富樫（2009）は、ヒューマンエラーの分析ツールとして医療現場で用いられている「M^2 SAFER」を採用し、ヒューマンエラーに起因した情報漏洩事故の主たる原因であるメール誤送信に着目し、仮想事例に添って適用実験を行った。その結果、ヒューマンエラーの防止策として非常に有効であり、メール誤送信に限らずセキュリティ対策全般に活用できる分析手法であるとしている。

村上（2010）らは、ヒューマンエラーの分析ツールとして医療現場で用いられている「Medical SAFER」を採用し、対象事例として、実際に2003 年に発生した「大阪府庁内ネットワークのコンピュータウイルスによるネットワーク障害」を取り上げて適用を試みた結果、分析の一連の流れを確認し、原因の分析、対策案の立案やその評価について十分効果的に活用できたとしている。従ってMedical SAFER系列のヒューマンエラー分析ツールを活用し、サイバーセキュリティにおける情報漏洩事故のヒューマンエラー分析に有用であったと結論付けている。

しかし代表的な手法を実際に発生したサイバーセキュリティにおける情報漏洩事故のヒューマンエラー分析に適用し、分析した事例は未だ報告されておらず情報セキュリティ業界にとって最適なヒューマンエラー分析手法は一例（村上（2010））のみ試験されただけである。

またマイナンバーの配布が2015年10月からであり、そのため情報漏洩事故が発生したのが2015年10月以降であり、現時点（2015年10月末）ではヒューマンエラー分析ツールに適用し、その効果を測定した研究は行われていない。本研究では代表的なヒューマンエラー分析ツールを比較したうえで実際に発生したマイナンバー情報漏洩事故にそれぞれを適用し、その効果を測定するという新たな試みを行うこととした。

３　海外におけるマイナンバー類似サービスとそのセキュリティ対策

総務省（国際大学グローバル・コミュニケーション・センター）（2012）や財団法人自治体国際化協会（2006）によると諸外国では既にマイナンバーの類似サービスを活用した電子政府化が推進されている。その中でも特にシンガポールの「eCitizen」[6]については全ての公共サービスがワンポータルで提供されており、将来のマイナンバー利用時の参考となる。

安岡（2012）は、高税率国、社会保障の充実で知られてきたデンマークにおいて電子化ポータルによる市民、医療・保健、税務を中心に電子政府システムが効果的に稼働している点を高く評価しているが、今後の課題として個人情報保護の問題や電子署名などセキュリティに関する課題を挙げている。

既に諸外国では情報漏洩事故が発生しており、その対策が今後の大きな課題であることは明白である。

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、Acquisti(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。

報告によると、まずフェースブック、LinkedInなどのソーシャルネットワークにアップされた大量のプロフィール写真から、大学内等のオフィシャルな情報にアップされた個人を特定し、住所などの個人情報を特定する。Acquisti(2009)らは、この報告よりも以前にSSNを統計学的手法にて推測するDBを構築し、上述した個人情報と関連付けてSSNを推測するという新しい手法を提示しており、その研究内容を利用して今回の研究発表を行っている。

研究内容について、筆者独自の理解に基づき、図2-1を用いてそのメカニズムを解説した。

Acquistiらはデータベース1（以下DB1）とデータベース2（以下DB2）の情報を照会し、SSNを特定している。

ソーシャルネットワークなどインターネット上のオープンな情報より、人物に関する大量の画像データを入手する。学内などの学生情報等から、人物画像と個人に関する名前、住所、生年月日、性別などの4大項目情報を入手する。これら2つの情報源から画像と個人情報を関連付けたDB1を構築する。

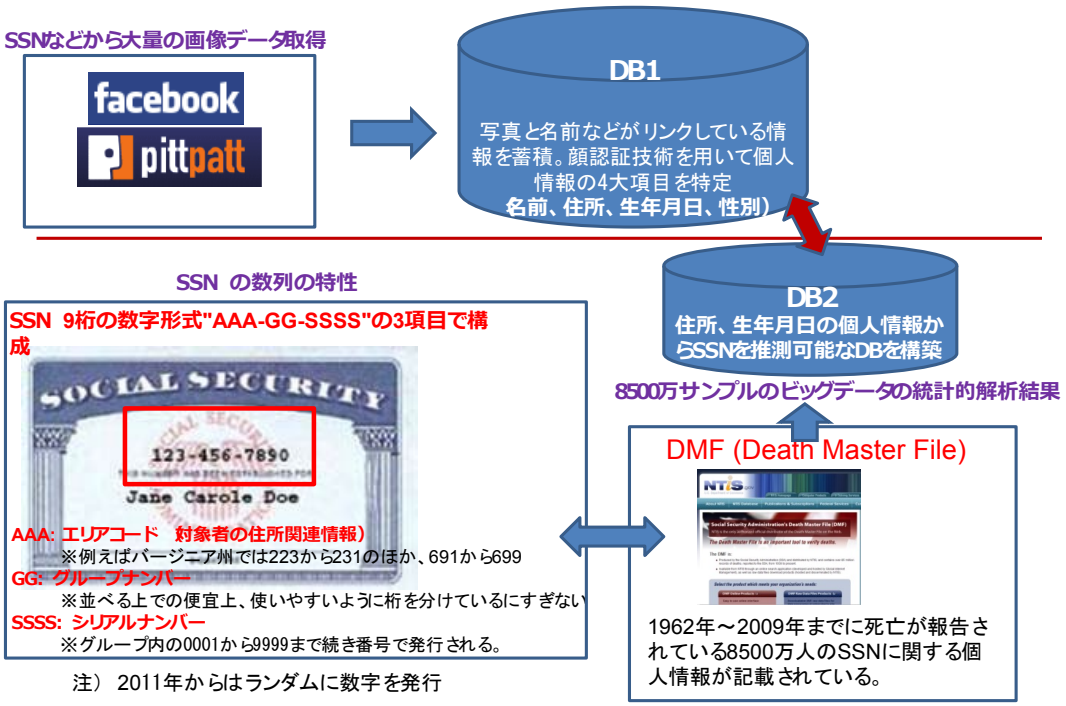

図2-1　Faces of FaceBookのメカニズム

次にDB2の構築方法について説明する。

Social Security Administration （米国社会保障局（以下SSA））は、1980年以来公表されているDeath Master File（以下DMF）[7]というDBの存在を明らかにしている。DMFには1962年～2009年までに死亡が報告されている8500万人のSSNに関する個人情報が記載されている。DMFは元々臨床実験等における死亡確認や、クレジットカード会社や公共サービスにおける身分詐称を防止するために用いることが目的とされていた。実際には、DMFを悪用した税金還付を求めた虚偽申告などが社会問題となっている。

DMFは容易に入手できるため、これらを標本母体とし、SSNの番号が割り振られた経緯などを参考に、統計学的手法を適用し、SSNを推測することが可能であるとAcquistiは指摘

している。SSNの番号割り振りの経緯[8]については以下のような情報により推測が可能である。

SSNは9桁の数字形式"AAA-GG-SSSS"の3項目で形成されており、最初の3桁がエリアコードと呼ばれ、発行された事務局の番号であったが、1973年にボルチモアの事務局で一括して発行されるようになり、それ以降は、送り先対象者の郵便番号となった。例えばバージニア州では223から231のほか、691から699のエリアナンバーが使われている。中間の2桁の番号はグループナンバーである。地理その他のデータ上の意味合いはなく、並べる上での便宜上使いやすいように桁を分けているにすぎない。

2011年7月25日から割り当て方針が変更され、エリアナンバーはランダムに割り当てられるようになったが、2013年時点で2年程しか経っておらず、生存するほぼ全ての米国人のSSNが統計学上推測可能であると推測される。

この研究からは、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が示唆されている。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が明らかとなった。

中川（2007）は、米国における個人情報保護の動向について、氏名と社会保障番号と生年月日の三つが揃えば、クレジットカード口座を作成したり、車のローンを組んだり、携帯電話を購入することができることから最も重要な個人情報と米国では位置づけられていると述べている。 2005年には、個人情報窃盗による被害者は約890万人、被害者一人当たりの被害額は6,383ドル、被害総額は566億ドルとされている。被害者が問題を解決するために費やした平均時間も、2002年の33時間から2005年の40時間と長くなっており、被害が深刻化していることがうかがわれる。下院行政改革委員会が、2003年1月以降の連邦行政機関における個人情報漏洩事故を調査した結果、調査対象とされた全19省庁において一度は情報漏洩事故がおきていたことや、 各省庁は、どのような個人情報が漏洩したかを把握していない場合が多いことが明らかとなった。個人情報窃盗の原因の多くは、消費者の不注意や、親族や近隣住民による窃盗である。具体的には、財布、小切手帳又はクレジットカードの亡失又は盗難が30％で、友人や近親者が個人情報を取得できた場合が15％である。対策として法制度の観点から、1899年構成信用報告法、1974年プラバシー法、1998年

個人情報窃盗対策法、1999年グラム・リーチ・プライリ法連邦取引委員会法第5条、などの法律が制定されている。

一方行政機関による取り組みとして連邦取引委員会Federal Trade Commissionが個人情報窃盗データ情報センター（Identity Theft Data Clearinghouse）を設立し、個人情報窃盗についての報告を提出した消費者から情報を収集している。FTCは、この情報を消費者監視データベース（Consumer Sentinel database）に提供しており、これが1,000を超える法執行機関により利用されている。また社会保障番号の利用制限なども検討されていることが報告されている。

このような米国の法制度について堀田（2009）は、個人識別情報の不正取得・不正使用に対する刑事訴追について説明している。1998年に制定されたのが「ID盗取・濫用防止法」ID盗取罪であり、個人を特定されるものとして定義されているのは「氏名、社会保障番号、生年月日、運転者免許番号、移民登録番号、旅券番号、雇用主/納税者番号、生体情報、電子上の識別番号・コード等、電気通信上の識別情報等である。また州毎の取り組みも行われており、1996年に国内初の明文によるIDEALLY盗取処罰規定をアリゾナ州が定めている。現在では全ての州において「身元確認情報」と総称した各種ID情報の不法取得やこれを用いた詐欺を処罰する処罰規定を置いていると記載している。

次に韓国の個人情報漏洩事故についての従来研究の調査を行った。

張（2012）は、個人情報保護に関する韓国の現在の法律としては、「公共機関の情報公開に関する法律（1994年制定）」および「情報通信網利用促進および情報保護に関する法律（1999年全面改正）」が代表的であると述べている。前者は対象が公共機関に限定され、後者は情報通信サービス提供者に限定される。韓国情報保護振興院の2007年の発表によると、総計9000件の個人情報流出事故のなかで、住民登録番号の盗用が78%でもっとも多いと報告している。現行個人情報保護の体制は予防的な機能が足りず、既に侵害された個人情報の事後的な救済手段も十分ではなく、民事的賠償に頼っている状況である。各個別事業者が、住民登録番号以外の手段で本人確認をできる ように住民登録番号の代替手段として、i-Pin（Inter-net Personal Identification Number）などが提案されたが、定着化には至っていないと述べている。

崔（2012）は、現在までに韓国で整理されている個人情報保護に関連した法律を説明している。韓国において多発する情報漏洩事故を防ぐための韓国政府の取り組みについて瀧

ロ（2014）は、釜山広域市の新たな義務措置「住民登録番号代替手段(I-PIN)の提供」を紹介している。インターネットホームページ会員加入のため本人確認が必要な場合に、必ず代替手段(I-PIN など)を提供することにより、万が一I-PINが漏洩しても住民登録番号の直接的な漏洩を防ぐのが目的であると述べており、マイナンバーの利用時にも活用できる可能性があると考えられる。

４　まとめ

システム上の安全措置（技術）に関する研究について日本年金機構の情報漏洩事故から必要な技術についてのヒントを見つけることが出来た。

例えば、「新種」のウイルスにも対応出来る対策を検討する、個人情報をファイル共有サーバへ保存する際のアクセス制限を行う、 個人情報を保存する場合にはファイルに「人に推測されにくいパスワード」を設定することをシステムで検知する仕組みを取り入れる、などである。一方最新の攻撃手法が開発されている。例えば遠隔からアクセスされ自動車の制御を奪われるリスク、スマート冷蔵庫の脆弱性があり、悪意のある第三者に利用されるとGoogleサービスへのログイン情報が盗まれるリスク、などである。

情報漏洩事故に関する技術面（システム上の安全措置（技術））の研究は、日本国内においても2006年に個人情報保護法が施行されて以来、情報漏洩事故の社会的関心の高まりを受けて、自治体、民間企業において行われてきた。代表的な情報漏洩対策手法を以下に示す。

・強制アクセス制御により情報漏洩を防止
・ログ分析による情報漏洩監視
・漏洩したファイルの追跡

企業におけるセキュリティ対策はいたちごっこの側面があり、完全なセキュリティ対策システムというものは存在しないため、システムの運用を通して対策の見直しやフィードバックを繰り返していく必要があり、加えて仮にインシデントが発生した際に、素早く状況を把握し、対策立案・実施するためのセキュティ活動専門組織が必要である。

体制（人や組織）に関する従来研究は、情報漏洩事故が増加の傾向にあり、事故原因のにおけるヒューマンエラーに起因する事故が全体の80.5%を占めることから、その重要性が指摘されている。

ヒューマンエラーに起因した情報漏洩事故については、エラー発生の詳細な状況分析と対策立案の手法について具体的な方法が提示される必要があるが、ITセキュリティ業界ではその標準化が始まって日が浅い。従ってサイバーセキュリティ分野においては、主に各分野で確立された手法をサイバーセキュリティ分野の情報漏洩事故に適用する形で多くの研究が進められている。代表的なヒューマンエラー分析手法である「4E-4M」、「Medical SAFER」、「VTA」等をITセキュリティの情報漏洩事故のにおけるヒューマンエラー分析に適用出来るかについて近年研究が行われてきた。

しかし従来研究から明らかになった課題を以下2点で述べる。

- 代表的な手法を「実際に発生した情報漏洩事故」のヒューマンエラー分析に適用し、分析した事例は未だ報告されておらず、情報セキュリティ業界にとって最適なヒューマンエラー分析手法は一例（村上（2010））のみ報告されただけである。
- マイナンバーの配布が2015年10月からであり、そのため情報漏洩事故が発生したのが2015年10月以降であり、現時点（2015年10月末）ではヒューマンエラー分析ツールに適用し、その効果を測定した研究は行われていない。

海外におけるマイナンバー類似サービスとそのセキュリティについての調査では、「シンガポールの「eCitizen」や「デンマークにおける電子化ポータルによる市民、医療・保健、税務を中心とした電子政府システム」などが既に稼働しており、参考となったが、反面、多くの国で既に情報漏洩事故が発生していることから、その情報漏洩事故が懸念される。

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、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た。

韓国政府は韓国において多発する情報漏洩事故を防ぐため、代替手段(I-PIN など)を提供することにより、万が一I-PINが漏洩しても住民登録番号の直接的な漏洩を防ぐなどの取り組みを行っていることが明らかになった。

従来研究では、実際に国内外で起こっている住基ネットやSSN等に関連した事故を詳細に分析した研究例が少ない。従って、多くの事故事例から攻撃場所、攻撃手法、頻度、攻撃の技術レベルなどを分析する必要がある。

そのため、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比較の結果を次章に示す。

第３章　諸外国におけるマイナンバー類似サービスの情報漏洩事故分析

１　調査対象国の選定と調査方法

OECD（2012）と国際大学グローバル・コミュニケーション・センター（2012）で紹介された諸外国における国民ID制度の紹介と利用例の中で以下の観点から調査対象国を選定した。

・国民ID制度が、その国民に浸透し、公共サービスと民間サービスで利用されている。

・公共サービスと民間サービスで国民IDの情報漏洩事故が社会問題となっている。

・日本と文化的に近く、情報漏洩事故の情報が入手し易い。

本章では、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、また日本国内においてもマイナンバーの前身である住基ネットにおいて実際に発生した情報漏洩事故を検索し、その情報漏洩事故について調査を実施した。

検索手法としてGoogleを使ったWeb検索を用いた。1ヶ国につき、10時間の検索の中で発見されたものを調査対象の情報漏洩事故とした。10時間は調査対象の抽出に要した時間であり、対象の情報漏洩事故について詳細に調査した時間は含まない。

調査対象の情報漏洩事故については、以下の項目について調査を実施した。調査項目については後述する予定のリスク評価に必要である内容とした。

- 事故発生年
- 内容（どのような情報漏洩事故であったか）
- 発生場所
- 脅威種別

– ハッキング：コンピュータシステムに侵入したり、プログラムを改造・改良したりすることにより発生した事故

– 盗難：PC、記憶装置などの物理的な物品の盗難事故

– ID 詐称：個人を特定する ID（身分証）を詐称（なりすまし）することに起因した事故

– 対策不備：ウイルス対策ソフト未導入や ID が記載されたファイルが簡単に閲覧できる状態など、セキュリティの対策を十分行ってない状態で発生した事故

– 内部犯：問題が発生した組織、もしくは下請け会社の内部関連者が犯人である事故

- 技術難易度 「高」「中」「低」のレベルで記載

– 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

– 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

– 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

２　米国における情報漏洩事故

1935年に社会保障法が成立して以降、ソーシャルセキュリティナンバー（以下SSN）が様々な公共サービスと民間サービスで利用されてきた。公共サービスの利活用の効率性のために様々なシーンで本人確認の手段として用いられてきたが、反面、本人偽称による不正送金や不正ローン取得など、様々な社会問題を引き起こした。

JETRO/IPA（渡辺）（2005）は、米国における個人情報漏洩の現状と対策についての報告書の中でソーシャルセキュリティナンバー（SSN）漏洩事故を幾つか紹介している。

上述の調査条件に基づき調査した情報漏洩事故を表3-1に示した。

表3-1　米国におけるSSNの情報漏洩事故一覧

No	年	内容	発生個所	脅威種別	技術難易度
1	2013/9	SSNDOB(Social Security Number + Date Of Birth)という個人情報売買を行うアングラサイトの情報源は、他企業のDBにマルウェア（ボット）を仕掛けて情報をハッキングして入手	企業DB（LexisNexis、Dun & Bradstreet、Kroll Background America	ハッキング	高
2	2012/6	Face Book上の動画から、ある女性の声を入手し音声を模倣することで友人になりすましSSNを入手	Face Book	ID詐称（音声模倣）	低
3	20011/11	2000年～2005年の間に数学のコースを受講した7093人のSSN等が蓄積されたDBに対し不正侵入	大学DB（パーデュー大学）	対策不備	低
4	20011/8	マルウェアを利用したハッキング被害により、75,000人の氏名とSSNが漏洩	大学DB（ウィスコンシン大学）	ハッキング	高
5	20011/8	関係者43,000人の氏名とSSNが、10カ月間Googleで誰でも検索できる状態	大学DB（エール大学）	対策不備（ﾃﾞｨﾚｸﾄﾘｰﾄﾗﾊﾞｰｻﾙ）	低
6	2005/10	犯人は他で盗難した情報を悪用して合法的に存在する企業になりすまして同社で約50 件の顧客口座を開設し、14万5000人分の個人情報を購入	企業DB（チョイスポイント）	ID 詐称	中
7	2005/3	保管する顧客3万人の住所氏名、SSNなど個人情報が盗難	企業DB（LexisNexis）	ID 詐称	低
8	2005/3	連邦政府職員120万人のSSNやクレジットカード番号を含むデータのバックアップ用テープが２月の移送中に紛失（盗難）	企業のデータバックアップ用テープ（Bank of America）	紛失/盗難	低

No	年	内容	発生個所	脅威種別	技術難易度
9	2005/2	学生や教授陣など３万人の氏名、写真、SSNなどの個人情報がハッキング被害に遭い不正詐称	大学DB（バージニア州のジョージ・メイソン大学）	ハッキング	中
10	2004/12	献血者情報を保存したノートブックが盗難に遭い、献血者10万人に氏名、生年月日、SSNといった個人情報漏洩の恐れがあることを通知	企業持ち出しPC（デルタ血液銀行）	盗難	低
11	2004/10	顧客情報を保存したパソコン４台が盗難	企業DB（金融サービス大手ウェルズファーゴ）	盗難	低
12	2004/10	州民140万人の個人情報がハッキングされ不正詐称	大学内DB（カリフォルニア大学バークレー校に設置されたカリフォルニア州政府のDB）	ハッキング	高
13	2004/6	献血者14万5000 人の情報を保存したノートブックが、施錠した車両から盗難	大学（カリフォルニア大学ロサンゼルス校）	盗難	低
14	2004/3	10 万人近くの卒業生、大学院生、過去の入学志願者の個人情報が記録されていたノートパソコン１台が盗難	大学（カリフォルニア大学バークレー校）	盗難	低
15	2003/後半	カリフォルニア州サンタ・アナ出身のコンピューター技術者ニコラス・リー・ジェイコブセンが７ヵ月間、ネットワークに不正に侵入し、顧客400人のSSNを不正詐称	企業DB（携帯電話大手T モバイル）	ハッキング	高
16	2002/4	職員26万5000人分の氏名、給与情報、SSNなどの個人情報が保存されていたコンピューターがハッキングされ不正詐称	自治体DB（カリフォルニア州）	ハッキング	高

1936年にはじめてSSNが発行されて以降、様々な漏洩事故が報告されており、上記検索条件では2002年の事故が最も古いものであった。

漏洩事故の発生場所としては、発行元の自治体である割合がわずか6%（1件）に対し、大学44%（7件）と企業44%（7件）で全体の88%を占めている。

脅威の種別としては、それぞれ、ハッキング38%（6件）、盗難31%（5件）、ID詐称19%（3件）、対策不備13%（2件）であった。中には最新のウイルス感染を用いて特定企業のDBを攻撃対象とするような、高度なハッキング技術も用いられており、常に最新の攻撃手法についての防御策を講じることの必要性も同様に示唆される。

事故の技術的な難易度は、それぞれ高31%（5件）、中13%（2件）、低56%(9件)であった。

既にSNS（Face Book）上でソーシャルセキュリティナンバー（SSN）の漏洩事故が発生しており、IT先進国を象徴するものであるが、個人情報がアップロードしていくようなタイプのサービスが台頭しており、新たなサービスが新たな脅威の原因となることが示唆されている。

浦川（2010）は、SNSなどのソーシャルメディアにおける情報漏洩防止手法についてWebフィルタリングの観点から、情報漏洩に関連したキーワードを検索するなどの新たな提案を行っている。しかしソーシャルメディアには文章、画像、映像など様々な媒体が混在しているため情報漏洩対策については一筋縄でいかないのが実情である。

一方でPCの盗難、対策不備などの技術的難易度では低レベルなものが全体の56%（9件）であることから、我が国のマイナンバーにおいても策定されるセキュリティポリシーに沿って関係者が運用レベルまで漏洩事故に対する備えを油断することなく実施することが求められる。

McAfeeの外部セキュリティコンサルタントであるSiciliano(2010)による調査結果によると、ソーシャルセキュリティナンバー（SSN）の漏洩の発生場所としてのランキングトップ10（Top Ten Most Dangerous Places to Leave Your Social Security Number）が報告されている。そのランキングを図3-1に示す。

図3-1　Top Ten Most Dangerous Places to Leave Your Social Security Number

出所：　Siciliano, Robert (McAfee)

Top Ten Most Dangerous Places to Leave Your Social Security Number

この報告によると、ソーシャルセキュリティナンバー（SSN）が情報漏洩し易い最も危険な場所の1位は大学で事件件数が108件、2位は銀行等金融機関で96件、3位は病院で71件、4位が地方自治体で44件、それ以降はアメリカ合衆国州政府で33件、医療ビジネスで27件、非営利団体（NPO）で23件、テクノロジー関係の企業で22件、医療保険会社で20件、医療関係企業で20件となっている。

またSiciliano（2009）は、レンタルビデオ、カーディーラーなどの窓口で安易にソーシャルセキュリティナンバー（SSN）を報告した結果、情報が漏洩した事例を報告している。

これらの報告から、マイナンバーが民間利用される際には情報漏洩事故が発生する可能性の箇所が公共サービスのシステム範囲だけでなく民間サービスのシステム範囲にまで拡大する可能性が示された。従って自治体と民間企業の連携により、広範囲なセキュリティ対策を講じることが求められる。

表3-1のNo.１に記載された、SSNDOB(Social Security Number + Date Of Birth)という個人情報売買を行うアングラサイトに関する情報漏洩事故と、No.2に記載されたFace Book上の動画から、ある女性の声を入手し音声を模倣することで友人になりすましソーシ

ャルセキュリティナンバー（SSN）を入手した情報漏洩事故は非常に興味深い事例であることから詳細な分析を行った。

Krebs, Brian氏(Washington Postの元記者)（2013）は、自身のブログ「Krebs on Security」で、米国の「SSNDOB（Date Of Birth）」という個人情報を売買する違法サービスについての問題を報告している。ブログに掲載された情報を基に筆者独自の理解でこの情報漏洩事故の問題を分析した内容を図3-2に示す。

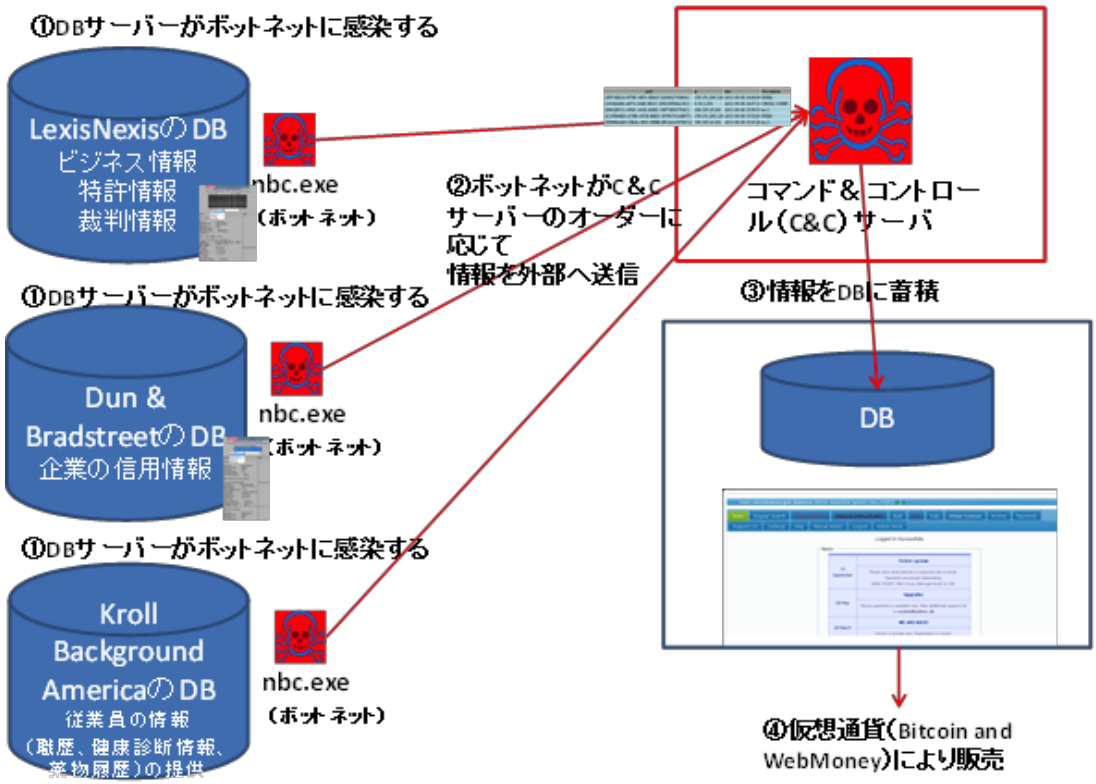

図3-2　SSNDOB問題のメカニズム　（出所：筆者作成）

SSNDOBは「Social Security Number」（SNS）と「Date Of Birth」（生年月日）を合わせた略称である。情報漏洩のメカニズムは以下のとおりである。

①LexisNexis、Dun & Bradstreet、Kroll Background Americaなど、米国の複数の大手データ仲介業者のDBサーバーがボットと呼ばれるコンピューターを悪用することを目的と

したプログラムに感染する。今回はnbc.exeというファイル名の実行ファイルが利用された。

②ボットネットがC&C（コマンド&コントロール）と呼ばれる命令をサーバーのオーダーに応じてソーシャルセキュリティナンバー（SSN）を外部へ送信する。C&Cというのはボットを遠隔操作するサーバー型のプログラムのことである。

③情報をDBに蓄積

④仮想通貨（BitcoinやWebMoney）により販売

Brian Krebs氏のブログによると、この違法サイトでは400万人以上の米国人に関するSNSと生年月日などを不正に入手し、その情報を販売していたとしている。当時FBI長官を務めていたロバート・ミューラー氏、CIA長官ジョンブレナン氏、ビヨンセ氏、カニエ・ウェスト氏、ジェイZ氏、ミシェル・オバマ氏ら、著名人のソーシャルセキュリティナンバー（SSN）を入手可能あることで大きな話題となった。

一般人の一般的なID情報の価格は1件あたり50セントから2.5ドルであるがクレジットカード情報や身元調査情報などの付加価値が付くと5ドルから15ドルであり、既に1,300万人のユーザにより取引されていた。

Krebsによると現在市場に出ているマルウェア（ウイルス等の悪質な不正プログラム）対策ツールの上位46製品は、今回用いられた不正プログラムを検出することが出来なかったと報告している。

この手法はhacktivist（ハクティビスト）と呼ばれる政治的ハッカー集団であるUGNaziが明らかにしたものである。

この事故では高度なハッキング技術が用いられていることから対策の難易度も高度なものが求められる。

またこの事故では漏洩した個人情報（ソーシャルセキュリティナンバー（SSN）を含む）が膨大で、かつ著名人の情報が多く含まれていた点、社会的信用度の高い会社のDBから漏洩していた点、最新のハッキング技術が用いられた点、Bitcoinなどの仮想通貨が用いら

れていた点、政治的ハッカー集団がその攻撃手法を明らかにした点など多くの注目する要素があり社会的な反響が大きかった。

さらに仮想通貨（BitcoinやWebMoney）により個人情報が売買されていたこともセンセーショナルであった。

Christin(2012)は、アメリカやヨーロッパを中心に、少なくとも十数か国にまたがるシルクロードと呼ばれるネット上の巨大闇市場が存在し、市場ではビットコインと呼ばれる仮想通貨が使用され、麻薬や違法商品など2万4,000点以上の違法取引が扱われているという事実を報告した。またMooreやChristin(2013)らはビットコインでの取引では45%の処理で以上が発生し、実在の通貨が搾取される危険性を証明している。

この事例から、マイナンバーに関するセキュリティについて考察すべきことは多い。以下に列挙する。

- アングラサイトも含め、かなり広範囲を網羅して情報漏洩について監視すべきであること、例えば著名人の個人情報の漏洩が無いかどうか調査することなどは一つの指標となる。

- 最新のセキュリティ技術（アンチウイルスソフトなども含め）を実装しても起こり得るリスクに対して予防策だけでなく、軽減策、回復策の3つの段階での対策について講じる必要があること

- ハッカー集団も含め、様々な組織の活動状況なども視野に入れる必要があること

- 最新のITサービス（今回は仮想通貨）に着目し、その利用範囲はマイナンバーとの相関関係を把握してリスクを予見すること

マイナンバーにおいても同様に情報漏洩事故が発生することが容易に予測される。必要なことはその事例から学んだ教訓をいかに早く対策として講じることができるかという点である。

表3-1のNo.2に記載されたFace Book上の動画から、ある女性の声を入手し音声を模倣することで友人になりすましソーシャルセキュリティナンバー（SSN）を入手した情報漏洩事故は、McAfeeの外部セキュリティコンサルタントでソーシャルセキュリティナンバー（SSN）漏洩事故に詳しいSiciliano, Robertとフェースブックからソーシャルセキュリティナンバー（SSN）を詐称する事例として米国のTVショウで有名なAnderson Hays Cooperの番組[9]でも紹介されたものであるが、この事故は、フェースブックにアップされた情報からソーシャルセキュリティナンバー（SSN）を聞き出す非常に簡単な手法として紹介されている。番組ではバーニーという悪役を演じる女性と、アガサとサンディーという仲の良い友人2名の計3名がデモを演じている。デモの手順は以下のとおりである。

- バーニーがアガサの友人情報等をフェースブックから入手する
- バーニーは、ビデオから音声を聞いてアガサの声を知り、それを模倣する
- バーニーはフェースブックから入手した電話番号を基にプログラミングで電話番号を詐称する
- アガサの声を真似てアガサのふりをしてサンディーに電話してソーシャルセキュリティナンバー（SSN）聞き出す

と言う簡単な手法である。この事例からはAcquistiらの研究と同様に、フェースブックなどのSNSで露出された個人情報から、簡単にソーシャルセキュリティナンバー（SSN）を入手できる脆弱性が示唆されている。

マイナンバーを米国同様に民間サービスに利用した場合は、米国と同様に情報漏洩事故が発生することが容易に予測される。事例から学んだ教訓をいかに早く対策として講じることができるが重要である。

３　韓国における情報漏洩事故

韓国において1962 年に制定された「住民登録法」の第7条（住民登録番号票などの作成）第3項によると、市長、群守（群の長）、区長（基礎地方自治体の首長）は住民に対して

個人別に固有な住民登録番号を付与することと規定しており、これが住民登録番号に該当する。施行以来、多数の改訂が繰り返され現在に至っているが、改定の中にはセキュリティ対策の一環で実施されたものがあり情報漏洩事故が韓国でも問題になっていることが明らかになっている。調査条件に基づき調査した情報漏洩事故を表3-2に示した。

表3-2　韓国におけるRRN情報漏洩事故一覧

No	年	内容	発生個所	脅威種別	技術難易度
1	2012	個人情報を盗むために偽装就職した自治体職員が自分の ID で市・郡・区住民管理システムにアクセスし、個人情報を詐称	自治体 DB	内部犯	中
2	2011	サーバーがハッキング被害に遭い、会員 1300 万人分の情報が流出	企業 DB オンラインゲームサイト （メープルストーリー）	ハッキング	高
3	2011	ネイトとサイワールドの会員数それぞれ 2500 万人と 3300 万人の情報がハッキングされ漏洩	企業 DB （ SK コミュニケーションズが運営するポータルサイト「ネイト（NATE）」と「サイワールド（Cyworld）」	ハッキング	高
4	2008	ウェブサイトがハッキングされ、1081 万人にのぼる同サイトメンバーの情報が漏洩。韓国人が企画し、中国人が実行	企業 DB オークションサイトサイト （オークション）	ハッキング	高
5	2008	代表取締役、副社長および社員、計 22 人が全国 1,000 カ所以上にあるテレマーケティング業者に対して、顧客に無断で提供	企業 DB （大手通信会社の Hanaro Telecom）	内部犯	低
6	2008	容疑者は大学が研究目的で構築した Web サイト内の「携帯情報照会」を通じ、携帯電話事業者の DB に接続できるアカウントやソースコードを入手。LGT 加入者の携帯電話番号を入力すれば、加入者の個人情報を確認できるブログを運営	企業 DB （携帯電話事業者の LG Telecom）	ID 詐称	高
7	2006	14 万人を超える大量の名義盗用事故が発生	企業 DB オンラインゲームサイト （リネージュ）	ID 詐称	低

発生場所はそれぞれ、企業86%（6件）、6件の内訳はオンラインゲーム2件、SNS1件、オークション1件、企業DB2件、自治体14%（1件）であった。米国で見られないようなオンラインでの事故が発生しており、特にオンラインゲームは没頭した学生の死亡事故が発生するなど、大きな社会現象となったこともあり、そのオンラインゲームでの情報漏洩事故は韓国におけるインターネット事情を反映した特徴的な事例である。

脅威の種別としてはハッキング43%（3件）、ID詐称29%（2件）、内部犯29%（2件）であった。オンライン事故が多いこともあり、ハッキング、ID詐称で全体の72%を占めている。

事故の技術的な難易度を分析したところ、それぞれ高57%（4件）、中14%（1件）、低29%（2件）であった。高の事故が最も多く、オンラインでの脅威の大きさが明確となっている。

代表的な情報漏洩事故の1つにMaplestoryという人気オンラインゲームサイトのサーバーがハッキング被害に遭い、会員1300万人分の情報が流出した事例がある[10]。図3-3にゲームのサービスイメージ[11]を示す。

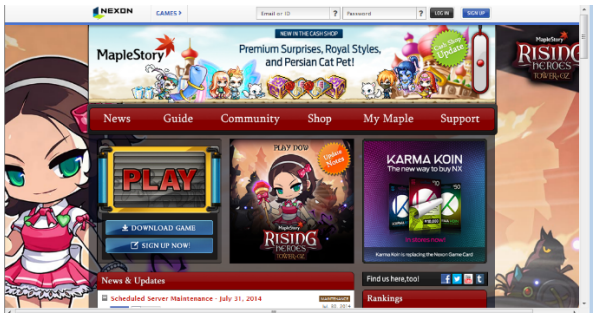

図3-3　事故が発生したMaplestoryのサービスイメージ

出所：Maplestory 公式HP[11]：

韓国インターネット振興院が運営する「住民登録番号クリーンセンター」のホームページをITジャーナリストの趙が紹介している。そのホームページのイメージ[12]を図3-4示す。

図3-4　「住民登録番号クリーンセンター」のホームページ

出所：趙（ITジャーナリスト）のコラム[12]

これによると自分の住民登録番号がどのWebサイトの会員登録に使われたのか、つまり個人情報が盗用されていないか確認できる。

利便性は向上されるが、このサイト自体がハッキングされる脅威は存在する。

また、自分の住民登録番号を検索サイト「コグル[13]」では、入力するとＳＮＳサイトのフェースブックが抽出され、家族の写真や血液型、趣味や住まいなど個人を特定できる情報が誰でも見ることができたという。コグルは現在サービス停止中である。

４　日本における情報漏洩事故

1999年8月18日改正住民基本台帳法が公布、住民票コードについて規定され、2002年8月5日住民基本台帳ネットワークシステムの稼働と同時に住民票コードの一斉割り当てが行われた。以降様々な情報漏洩事故が発生している。

調査条件に基づき調査した情報漏洩事故を表3-4に示した。

表3-4　日本における住民票コード情報漏洩事故一覧

No	年	内容	発生場所	脅威種別	技術難易度
1	2013	住民基本台帳システムの端末を目的外に使い市内に住む女性の個人情報を閲覧、知人に漏洩	自治体DB 千葉県船橋市	内部犯	低
2	2006	職員の自宅にある個人用パソコンがウイルスに感染し、パソコン内に保管されていた斜里町の保有する業務資料が、ファイル交換ソフト「Winny」のネットワーク上に流出	自宅PC （北海道斜里町）	ウイルス感染 (Winny)	低
3	2006	診察券とクレジットカードを使って兵庫県三田市在住の女性に成りすまし、大阪市内に勝手に転居させ住基カードを不正に取得。住基カードを使って女性名義の銀行口座を勝手に解約	自治体DB （大阪府大阪市天王寺区）	ID詐称	低
4	2006	東京都の中学3年の女子生徒（14歳）と無職少女（17歳）の2人がそれぞれ20歳と19歳の姉名義の健康保険証を使って姉になりすまし、住基カードを不正に取得。アダルトビデオへの出演に応募するのが目的	自治体DB （東京都）	ID詐称	低
5	2006	新潟県長岡市で男（47歳、2006年4月逮捕）が、東京都中野区が交付した他人名義の住基カードに自分の顔写真を張るなどして偽造し、これを身分証明書として使いアパートを契約	住基カード （東京都中野区）	ID詐称	低
6	2006	住基カードに記載された氏名、生年月日、住所などを架空のものに書き換え、携帯電話を購入	住基カード （愛知県名古屋市）	ID詐称	低
7	2006	住基カードに記載された氏名の一部を砂消しゴムで消して偽名のカードを偽造し、携帯電話とおまけの携帯音楽プレーヤー「iPod」各133台を同市内の携帯電話販売店28店から詐取	住基カード （北海道札幌市）	ID詐称	低
8	2005	失跡中の福岡県警の元警察官の男がインターネットで不正に売買されていた大阪市の無職男性の住民票や保険証を60万円で購入し、転居し、男性名義の住基カードを不正に取得	自治体DB （京都府京都市）	ID詐称	低
9	2005	他人になりすまし虚偽の転入届と養子縁組届提出し、住基カードを不正に取得	自治体DB （大阪府羽曳野市）	ID詐称	低
10	2005	知人から預かった国民健康保険証を悪用し住基カードを不正に取得	自治体DB （兵庫県神戸市）	ID詐称	低
11	2005	北九州市の男（29歳、2005年10月逮捕）が、他人になりすまし、虚偽の転居届を提出し住基カードを不正に取得	自治体DB （愛知県名古屋市）	ID詐称	低
12	2005	義弟になりすまし住基カードを不正に取得	自治体DB （大阪府大東市）	ID詐称	低

No	年	内容	発生場所	脅威 種別	技術 難易度
13	2005	同居していたホームレスの男の国民健康保険証を悪用し住基カードを不正に取得	自治体 DB （愛知県名古屋市）	ID 詐称	低
14	2005	他人になりすまし原町市に虚偽の転入届と婚姻届を提出し不正に住基カードを取得	自治体 DB （福島県郡山市）	ID 詐称	低
15	2005	親類になりすまし、住基カードを不正に取得し銀行等から借金	自治体 DB （福岡県北九州市）	ID 詐称	低
16	2005	盗んだ健康保険証を利用して他人になりすまし、住基カードを不正に取得し携帯電話を購入	自治体 DB （福岡県北九州市）	ID 詐称	低
17	2005	親類になりすまし住基カードを不正に取得し携帯電話を購入	自治体 DB （愛知県豊橋市）	ID 詐称	低
18	2005	不正に取得した郵貯カードを使って親類の女性に成りすまし、携帯電話を購入する目的で住基カードを不正に取得	自治体 DB （愛知県豊橋市）	ID 詐称	低
19	2005	顔見知りの男性から氏名と住所を聞き出し住基カードを不正に取得	自治体 DB （北海道釧路市）	ID 詐称	低
20	2005	福岡市で拾った健康保険証を元に渋谷区へ偽りの転入届をし、住基カードを不正に取得。成人女性になりすましてアダルトビデオに出演	自治体 DB （東京都渋谷区）	ID 詐称	低
21	2005	親類の女性に成りすまし住基カードを不正に取得し、消費者金融に出す身分証明書として使用	自治体 DB （山口県周南市）	ID 詐称	低
22	2005	虚偽の転入届と養子縁組届を提出し、住基カードを取得。このカードを使って、販売目的で携帯電話 10 台の購入契約をし、銀行口座を 2 つ開設	自治体 DB （東京都杉並区）	ID 詐称	低
23	2005	指定暴力団山口組系の組周辺者の男ら 3 名が、路上生活者の男性ら 2 名から保険証を借用し住基カードを不正に取得。住基カードでクレジットカードを作成し、高級外車などを購入。	自治体 DB （東京都足立区）	ID 詐称	低
24	2005	携帯電話契約の際に、偽造された住基カードを身分証明に使用	住基カード （東京都北区）	ID 詐称	低
25	2005	住基カードに記載された氏名の一部を爪で削って別人を装い携帯電話を購入	住基カード （愛知県名古屋市）	ID 詐称	低
26	2004	知人になりすまし、住基カードを不正に取得し金融機関で借金	自治体 DB （新潟県新潟市）	ID 詐称	低
27	2004	他人の国民健康保険証を悪用し虚偽の転居届を提出し、住基カードを不正に取得	自治体 DB （北海道札幌市）	ID 詐称	低
28	2004	女（31 歳、同）に男の妻になりすましをさせ不正に住基カードを取得	自治体 DB （埼玉県所沢市）	ID 詐称	低

No	年	内容	発生場所	脅威種別	技術難易度
29	2004	自分が雇っている男性になりすまし住基カードを不正に取得　（金融機関から借り入れ目的）	自治体DB（福島県相馬市）	ID詐称	低
30	2004	横浜市の男（当時56歳）は、再交付された住基カードの氏名と生年月日の記載を「何らかの方法」で不正に書き換えた。男は「東京・歌舞伎町の中国人に偽造させた」と供述	住基カード（東京都新宿区）	ID詐称	中
31	2004	住基カードに記載された氏名、住所、生年月日を何らかの方法で不正に書き換え携帯電話を購入	住基カード（佐賀県伊万里市）	ID詐称	低
32	2003	他人への成りすましにより、住基カードが不正に取得	自治体DB（佐賀県鳥栖市）	ID詐称	低
33	2002	町が独自に設置・運用している住民基本台帳処理システムのバックアップ業務を委託している富士通系の情報処理会社の社有車（ライトバン）が車上荒らしに遭遇	Digital Data Storage（バックアップ用）（福島県岩代町）	盗難	低
34	1999	再々委託先のアルバイト従業員が当該データを不正にコピーし名簿業者に販売し、さらに他へ転売	自治体DB（京都府宇治市）	内部犯（再々委託）	低

2002年8月の発行開始直後から既に漏洩事故が発生している。住民サービスに限定した利用のため発生場所は全て自治体DB関連（DBそのものではない）となっている。

脅威の種別としてはID詐称89%（30件）、内部犯6%（2件）、盗難3%（1件）、対策不備（ウイルス感染（Winnyを介するもの）3%（1件）となっている。なりすましによるID詐称が85%を占めているのが特徴的である。日本特有のWinnyを介する問題も発生している。

技術難易度については低97%（33件）、中3%（1件）となっており、ほとんどが技術的には低いレベルで事故が発生している。また住基ネットシステム自体がハッキングされた事例は現時点では確認されていない。

表3-4のNo.7は技術難易度が「低」で発生した情報漏洩事故の一例である。2006年に北海道札幌市で発生した情報漏洩事故の内容を図3-5に示す。

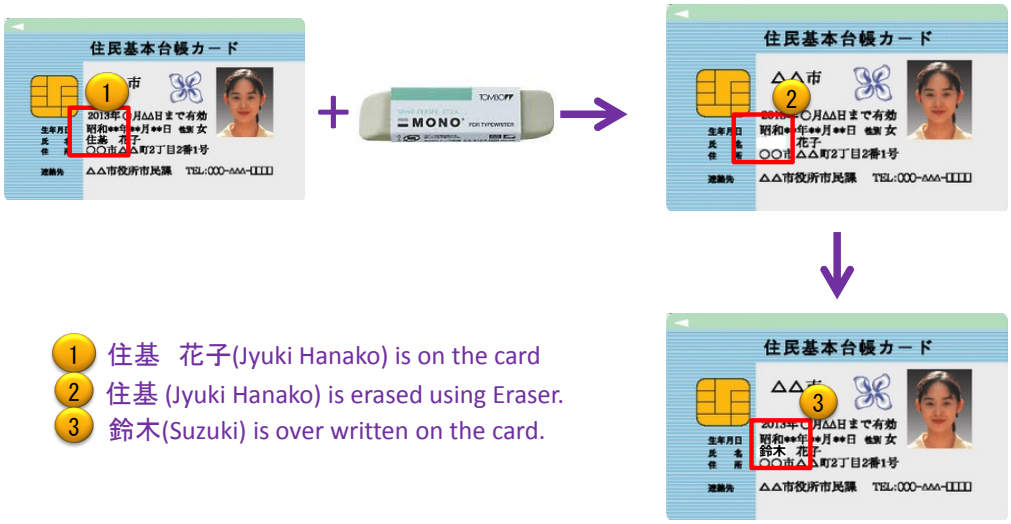

図3-5　消しゴムを使ったID詐称事故（出所：筆者作成）

住基カードに記載された氏名の一部を砂消しゴムで消して偽名のカードを偽造し、携帯電話とおまけの携帯音楽プレーヤー「iPod」各133台を同市内の携帯電話販売店28店から詐取したという内容である。技術難易度が低い場合でも十分事故が起こる可能性を示唆しており、運用も含め多角的な対策、事故発生後の軽減策、回復策という時系列に沿った3つの対策が必要である。

5　日米韓における情報漏洩事故比較

日米韓における情報漏洩事故について比較した結果を表3-5に示した。

表3-5　諸外国の情報漏洩事故比較一覧

国名	発生場所			脅威種別					技術難易度		
	自治体	大学	企業	ハッキング	盗難	ID詐称・偽称	対策不備	内部犯	高	中	低
米国（%）	6	44	50	38	31	19	13	0	31	13	56
韓国（%）	14	0	86	43	0	29	0	29	57	14	29
日本（%）	100	0	0	0	3	89	3	6	0	3	97

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、韓国では発生場所が大学、企業と広がりを見せている。

米国、韓国においては脅威種別としてハッキングが高い数値を示しているが日本では0件である。このことから自治体、特にセンター側の設備については、国家レベルで監視されており、比較的セキュアであることが伺える。

一方で民間利用が広がると対策すべき箇所も拡大し、セキュリティを担保することが困難となることが予測される。技術難易度に関して、日本は低レベルの管理不足が97%と多数を占めるが、米国、韓国では高レベルのハッキングによる被害などが発生している。

米国ではソーシャルセキュリティナンバー（SSN）が大学で既に利用されており、大学で情報漏洩事故が発生するなど情報漏洩事故の発生場所が公共サービスの場所から民間サービスの場所へ拡大している。このことから、我が国が今後マイナンバーの利用範囲を民間利用にまで拡張した際にリスクが拡がる可能性が高くなることが予想される。

また自治体のシステム自体がハッキングされた事例は米国においてわずか1件報告されているだけであり実際には単なる対策不備などの技術的に低いレベルのものが事故の大半であった。

６　まとめ

以下に日米韓の情報漏洩事故の比較を行った結果から得られた考察を述べる。

・　米国におけるソーシャルセキュリティナンバー（SSN）漏洩事故の発生箇所は発行元の自治体である割合がわずかであるのに対し、大学と企業で全体の9割近くを占めていた。またIT先進国を象徴するかのように既にソーシャルネットワークとして知られるフェースブック上で情報漏洩事故が発生している。攻撃手法も技術的に高度な割合が高かった。

・　米国におけるSSNDOB(SSN Data of Birth)問題と呼ばれたデータ仲介業者のハッキングによる情報漏洩事故では、最新のアングラサイトも含めかなり広範囲を網羅して情報漏洩について監視すべきであること、最新のセキュリティ技術（アンチウイルスソフトなども

含め）を実装しても起こり得るリスクに対して予防策だけでなく、軽減策、回復策の3つの段階での対策について講じる必要があること、ハッカー集団も含め様々な組織の活動状況を監視必要があること、最新のITサービス（今回は仮想通貨）に着目し、その利用範囲はマイナンバーとの相関関係を把握してリスクを予見すること、などの必要性が明らかとなった。

・ 韓国における漏洩事故の発生箇所は発行元の自治体で発生した割合に対して企業での発生割合が高かった。また文化的な背景を象徴してオンラインゲーム、オークション、ソーシャルネットワークに関連した大きな情報漏洩事故が発生している。脅威種別もハッキングが高い割合を占めており攻撃手法も技術的に高度な割合が高かった。

・ 日本における漏洩事故の発生箇所は、全て発行元の自治体であった。ID詐称で全体の9割近くを占めており攻撃手法も技術的に低度な割合が多かった。住基カードの名前を砂消しゴムで消して別名を記載するような技術的に難易度が低いID詐称も発生しており、運用面からの対策の必要性も示唆される。

情報漏洩がいったん発生してしまった場合には次の 4 点について課題がある。

- 法律の観点からは、いったん漏洩した電子データを回収するためにはプロバイダや警察関係者、弁護士などに相談しないと個人では容易にそれらの漏洩した電子データを追跡できない

- 技術の観点から、例えば漏洩した電子データが紙に印刷されたり、USB 等の外部媒体に保存されたりするため追跡に限界がある。

- 経済性の観点でも回収作業に必要とされる膨大なコストの問題がある。

- 組織行動学の観点からは、法律、技術、経済の問題を体系的に整理して対応できる有能な CISO (Chief Information Security Officer)が必ず必要であるが一般的に人材が不足している点と配下の組織整備などに問題がある点が挙げられる

法律、技術、経済、組織行動学の 4 つの観点から総合的に情報漏洩に相対する準備の必要性や時間軸の観点から、「防御策」、「被害軽減策」、「回復策（漏洩した情報を回収する）」についての対策が必要である。情報漏洩が起きた場合の回復策の困難性を考慮して、発生可能性がある情報漏洩事故について事前に予測し、その「防御策」を講じておくことは非常に重要であると考えられる。

日米韓における情報漏洩事故比較の結果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明らかとなった。

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。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する必要がある。

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重要である。

第４章　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

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 4-1 に示す。

図 4-1　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（出所：筆者作成）

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った。

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4-2に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」[14]を示す。このインデックス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。

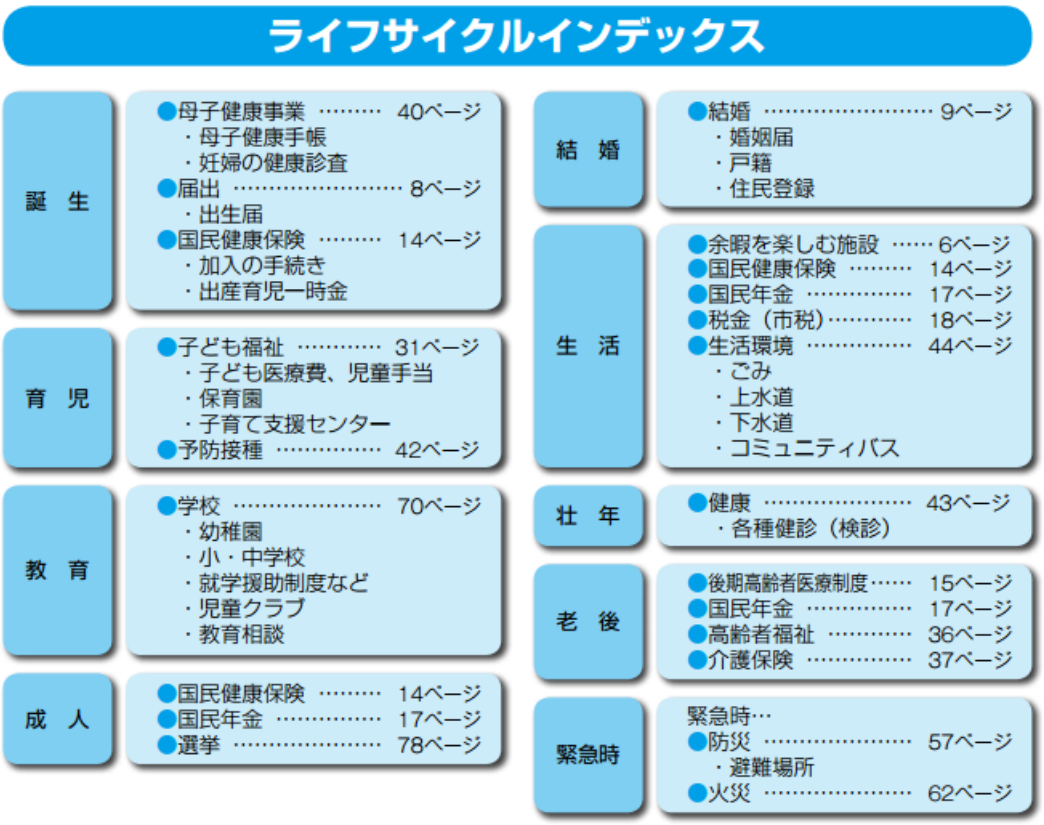

図4-2　福井県勝山市「ライフサイクルインデックス」[14]

出所：福井県勝山市「ライフサイクルインデックス」

諸外国におけるマイナンバー類似サービス例を調査した結果を表4-1に示す。

表4-1　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（Equifax, Google, PayPal, VeriSign, Wave Sys., Verizon）	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、デイケアサービス、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

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例として参考になった。

諸外国の中でも特にシンガポールは、eCitezen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。調査結果は付録表3に示した。

eCitezen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。

eCitezen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。

eCitezen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。

葛野（2011）は、Androidはアプリケーションに対する端末上の情報やデバイスへのアクセス制御をパーミッションの管理で制御するが、そのパーミッションの組み合わせによっては端末情報の外部送信、すなわち情報漏洩が発生する危険があることから、予め決めた情報フロールールによって制御された通信のみ許可する手法を提案した。

スマートフォン アプリケーション プライバシーポリシー 普及・検証推進タスクフォースは総務省（2014）がオブザーバーとなり、スマートフォン上のアプリケーションにプライバシー保護についての報告書が発出された。筆者も構成員を務めたが、内容は利用者情報を収集した広告会社やセキュリティ会社がどのように取扱っているかというものであり、それに基づき今後、利用者のプライバシーの保護についてアプリケーションでどのように制御するかの検証推進が行われてきた。

同様に筆者がワーキングメンバーを務めた日本ネットワークセキュリティ協会（Japan Network Security Association(JNSA)）からもスマートフォンの安全な利活用のガイドラインが報告された。従来PC向けとして開発されたOSがスマートフォンのOSとして採用された結果、PCに搭載されるOSの脆弱性が、スマートフォンにも影響を及ぼす状況が生じてい

る。また機器の開発サイクルの短縮化の結果、脆弱性が潜在したまま出荷され、これを悪用した情報漏洩事故がが発生していると述べている

マイナンバー関連のサービスもeCitizenのようにスマートフォンやタブレット向けアプリケーションを利用することが想定されており、アプリケーション経由や端末自身が紛失することによるでの情報漏洩が予想され、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網羅した後に重複を省いた結果を表4-2に示した。

表4-2　サービス例一覧

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	引越し会社（公共の転入転出情報と関連し手配可能）
	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）	ケアセンター
	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	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	

現時点で考えられるマイナンバー利用時のサービスイメージを図4-3に示す。

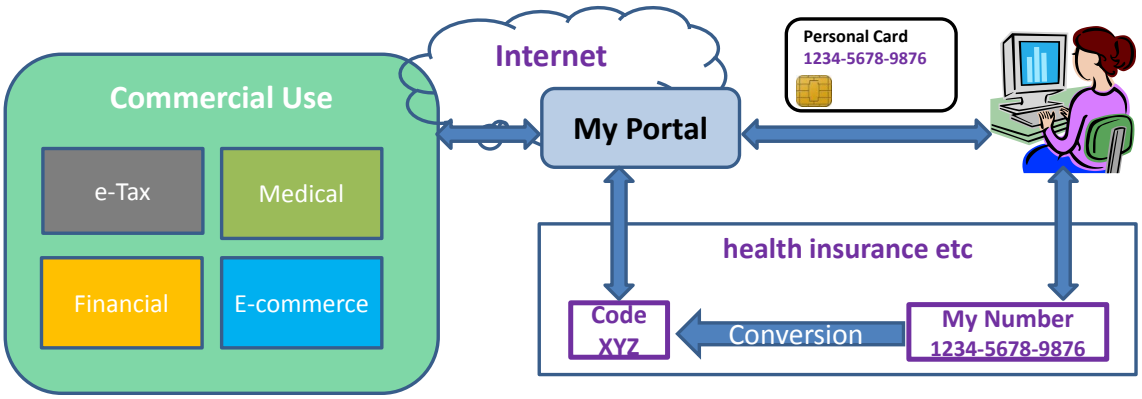

図4-3　マイナンバーを利用した民間サービスイメージ（筆者作）

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。

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処理される。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。

情報連携基盤技術ワーキンググループの構成員である坂本（2012）は「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）」の中で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について述べている。

同様に今村（2012）は、「マイナンバーを活用した官民連携の今後」の中で具体的な活用イメージとして5つのモデルについて整理しており、その内容について抜粋し表4-3に示した。

表4-3　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」

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。

2　シミュレーションモデルのリスク評価

前節では、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、「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か所が重大なセキュリティホールになる可能性があることを明らかにした。本節では、それぞれの設備に対するリスク評価を実施した。

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[15]）（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[16]。

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。リスク値の早見表例を図4-4に示す。

	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4-4　出所：ISMSユーザーズガイド[15]

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」

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表4-4示す。

表4-4　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。

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を4-5に示す。

表4-5　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。

表4-4と表4-5で示した基準に基づき行ったリスク評価の結果を4-6示す。

表4-6　リスク評価

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システム	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ス	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
		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。				—

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他の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。

３．まとめ

民間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およびリスク評価の指標を提案した。シミュレーションの結果、マイナンバーの民間サービス利用時には、「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か所が重大なセキュリティホールになる可能性があることを明らかにした。

それぞれの設備に対するリスク評価を実施したところ、以下リスクが明確になった。

- ID詐称
- マルウェア感染やハッキング
- 盗難

- 他で入手した個人番号で他の従業員がアクセス

それらへの対策として以下が必要である。

- 付箋紙をPCや机に張らない
- 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
- OSやソフトウェアのパッチ適用やバージョンアップを実施する
- 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を実施する
- 個人情報リスト、パソコン、磁気テープなどの保管場所をキーロックするなどでセキュアにする。

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がある。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。

第５章　大学におけるマイナンバー利用時の個人情報漏洩のリスク評価

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、米国においてソーシャルセキュリティナンバー（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った。

１．米国の大学における情報漏洩事故

Anderson(2009)は、なぜ大学においてソーシャルセキュリティナンバー（SSN）の情報漏洩が頻発するかについて報告している。報告によると大学内には多種多様な個人情報があるが、ステークホルダーのセキュリティ意識や対策が不十分であり、また限られた財源で増加したサイバー脅威への対策が求められるため対応が十分では無いことなどが理由であると結論付けている。

大学内にある機密情報として名前、アドレス、連絡先リスト、メールアドレス、ネットワークログイン情報、ソーシャルセキュリティナンバー、成績、財政援助、研究成果、ドナー情報、健康記録、アクセス情報、クレジットカード情報などがあり、これらが漏洩する主な原因として電子メールやボイスメールへのアクセス 、借入または貸与のコンピュータ上のデータへのアクセス、個人の机へのアクセス、ハッキング、フォーム上の社会保障番号の使用、給与の管理、個人の健康に関するお問い合わせ、休暇中のお問い合わせやストーキングなどが考えられるとしている。大学がサイバーアタックのターゲートとなる理由としては「USの大学の半分は学生IDとしてソーシャルセキュリティナンバー（SSN）を使用すること」「学生は、音楽やビデオをダウンロードするため様々なシステムとの連携が盛んであること」「大量の個人情報が登録されているデータベースのセキュリティ対策が不十分であること」「年中無休行政サービスやデジタルライブラリ･リソースへのアクセスは、潜在的な違法行為に利用されること」「攻撃手段として無線周波数識別子（RFIDの）及びIDカードの使用があること」などを挙げている。大学には保護者、学生、受験者、卒業生、職員、教員などの多様なステークスフォルダーが存在するが限られた財源で規制、社会の期待、記録へのアクセスの容易性、および増加したサイバー脅威への対策が求められる。効果的なプライバシー管理と情報セキュリティ対策が技術と組織の両面から必要となる。プライバシーを守るための提言として、１．調査活動、２．個人情報保護オフィサーの任命、３．プライバシー諮問委員会の設立、４．プライバシー擁護派の内部組織を確立する 、５．セキュリティとプライバシーキャンペーンの実行などが述べられている。

「第３章　表3-1　米国におけるSSNの情報漏洩事故一覧」の情報漏洩事故の中から大学内で発生した事故のみを抜粋し表4-1に示す。

表5-1　米国大学におけるSSNの情報漏洩事故一覧

No	年	内容	発生個所	脅威種別	技術難易度
1	20011/11	2000年～2005年の間に数学のコースを受講した7093人のSSN等が蓄積されたDBに対し不正侵入	パーデュー	対策不備	低
2	20011/8	マルウェアを利用したハッキング被害により75,000人の氏名とSSNが漏洩	ウィスコンシン	ハッキング	高
3	20011/8	関係者43,000人の氏名とSSNが、10カ月間Googleで誰でも検索できる状態	エール大学	対策不備（ﾃﾞｨﾚｸﾄﾘｰﾄﾗﾊﾞｰｻﾙ）	低
4	2005/2	学生や教授陣など3万人の氏名、写真、SSNなどの個人情報がハッキング被害に遭い不正詐称	バージニア州のジョージ・メイソン大学	ハッキング	中
5	2004/10	州民140万人の個人情報がハッキングされ不正詐称	カリフォルニア大学バークレー校に設置	ハッキング	高
6	2004/6	献血者14万5000人の情報を保存したノートブックが施錠した車両から盗難	カリフォルニア大学ロサンゼルス校	盗難	低
7	2004/3	10万人近くの卒業生、大学院生、過去の入学志願者の個人情報が記録されていたノートパソコン１台が盗難	カリフォルニア大学バークレー校	盗難	低

情報漏洩の43%(7件中3件)はハッキングであり、29%(7件中2件)は対策不備であったが共に個人情報が蓄積されたデータベースがターゲットとなっている。残りの29%(7件中2件)はノートパソコンの盗難であった。

ソーシャルセキュリティナンバー（SSN）を狙った意図的な攻撃である可能性も高い。大学内のセキュリティ対策が不十分ではなく、映像や音楽のダウンロードなど他システムとの連携が多く、攻撃口が多岐に渡るため防御出来てないことが原因と考えられる。

２　日本国内大学における情報漏洩事故と分析

上繁（2012）によると、長崎大学ではInformation Security Management System（ISMS）を構築し、その運用項目として学内関係者へのセキュリティ教育を実施した。学部一年次の全入学者1588名へのアンケートを行い、スマートフォンやタブレットなどトレンドのデバイスに関する理解は不十分であり、関連のセキュリティ専門用語の知識は欠如しているという結果を報告した。

上田（2011）は、徳島大学内においてISMSによるセキュリティ評価基準を導入した内容について報告している。

市川（2009）によると、山口大学でもISMSの構築と運用のプロセスを紹介し、組織として取り組む考え方を提示している。

田島（2014）は、学内IT環境に対する脆弱性診断の実施方法や診断システムの構築と運用について詳しく報告している。

成澤（2006）は、私立大学も「個人情報取扱事業者」の条件を満たすことや世論の影響からその対応が課題であると認識し、大学独自の個人情報保護規定の制定の必要性からその制定を実際に実施し報告している。

永井（2008）はセキュリティ対策をするためのコストについて、従来の国立大学では個別の作業毎に人件費などの事故コストを定量的に把握する習慣がないため，コスト定量化の仕組みを新たに策定することを提案している。このように一部の大学で積極的にセキュリティ対策に関する取組が行われているが、まだ一部の大学に過ぎない。例えばISMSを導入している大学は全大学のわずか1.8%（784校中14校）に留まっている。この数値はISMS認証取得組織検索[17]を用いて筆者が独自に算出した数値である。

その結果を反映するかのように日本国内の大学でも情報漏洩事故が多発している。

日本国内大学において発生した情報漏洩事故[18]30件（2013年9月から2015年1月）について発生箇所、脅威種別、技術難易度、どの業務過程で発生したか、業務に携わっていた人物の観点で整理した結果を表5-2に示した。

表5-2　日本国内大学における情報漏洩事故一覧

No	年	内容	発生個所	脅威種別	技術難易度	業務	人物
1	2015/1	教員が出張先のマレーシアにおいて学生 39 人分の個人情報を保存した USB メモリを紛失	大阪市立	紛失（USB）※海外	低	研究活動	教員
2	2015/1	2013 年春の健康診断時に撮影した学生 9336 人分の胸部レントゲンフィルムが所在不明。191 人分のフィルムについては氏名と学籍番号が特定できる状態	慶應義塾	紛失	低	保健管理	職員
3	2014/12	フィシングメールにより多くの本学ユーザの ID/PW が搾取	同志社大学	フィッシングメール	高	教務	学生
4	2014/12	教員採用選考の応募者情報が保存された USB メモリが所在不明。教員採用選考の応募者に関する氏名、住所、電話番号、生年月日など、17 人分の個人情報を保存	宮崎大学	紛失（USB）※海外	低	就職	職員
5	2014/12	行政文書の公開請求を受け 12 月 19 日に請求者に対し公開を行った文書内に個人情報が含まれているとの指摘を受けたため文書の公開を停止	新潟県立看護大学	対策不備	低	渉外	職員
6	2014/11	同大医学部保健学科の教員が利用していたネットワーク接続型のハードディスク（NAS）に個人情報が保存されていたが、パスワードを設定しておらず外部から閲覧可能	秋田大学	対策不備	低	教務	教員
7	2014/10	学内作業をアルバイトとして依頼した 105 名に事務連絡をする際に誤って 2634 名分の学生の氏名、住所、電話番号、メールアドレスを含んだメールを誤送信	龍谷大学	対策不備（メール誤送信）	低	教務	職員
8	2014/10	教員が出張先のスペインで学生のべ 277 人分の個人情報を保存したハードディスクが盗難	大阪市立	盗難　※海外	低	教務	教員
9	2014/9	教員が 2000 年から 2013 年の間に担当した 3 科目の受講者に関する氏名や成績などの情報が保存されていたパソコンが海外で盗難	上智	盗難　※海外	低	教務	教員
10	2014/9	システム情報科学研究院の教授が担当する 3 科目の講義を過去 3 年間に履修した学生、および卒業生約 400 人の氏名と点数、さらに国内外の大学、研究所、企業の研究者約 300 人の氏名と連絡先、送受信メールなどの個人情報が保存されていたパソコンがスウェーデンの国際会議中に盗難	九州大学	盗難　※海外	低	教務	教員
11	2014/6	職員が日本学生支援機構奨学金の申請者 181 人に対して、6 月から奨学金の支給が開始される 172 人分の学生の氏名や生年月日、学年、学籍番号、奨学生番号などが記載されていたメールを誤送信。	横浜市立	対策不備（メール誤送信）	低	奨学金	職員
12	2014/5	保健管理室へ相談に訪れた学生や教員など 58 人の氏名や性別、学部、学籍番号、相談区分などが記録されていた USB が紛失	広島市立	紛失（USB）	低	保健管理	職員
13	2014/4	同大教授が、大学からネットワーク接続に対応したハードディスクを自宅に持ち帰り、使用していたところ、セキュリティ設定に問題があり、インターネット経由で学生 4 万 7 千人の個人情報が検索サイトで閲覧可能	千葉大学	対策不備	低	教務	教員

No	年	内容	発生個所	脅威種別	技術難易度	業務	人物
14	2014/3	学生 1824 人に誤って学生 20 人分の休学・退学情報をメールに添付し送信	明治薬科大学	対策不備（メール誤送信）	低	教務	職員
15	2014/3	医学系研究科のサーバーのセキュリティ設定がデフォルトのままであり研究のため保有していた検査データ 356 人分の氏名、検査データ、患者 ID、性別、年齢、アルファベット表記による疾患名の略称と氏名や学生番号、性別、指導教員名、学内メールアドレスなどが閲覧可能	名古屋大学大学院	対策不備	低	教務	教員
16	2014/3	講義を履修した学生 40 人の氏名、学籍番号、提出物データ、成績集計に関するデータなどが保存されていた USB が紛失	大阪女子短期大学	紛失（USB）	低	教務	教員
17	2014/2	ネットワーク接続ストレージ（NAS）のアクセス制限が正しく設定されていなかったことが原因で学生や教職員など約 450 人の個人情報が流出し、検索サイトで閲覧可能	筑波	対策不備	低	教務	職員
18	2014/1	4 年生 77 人分の卒論途中評価を含むファイルを誤って同学科の全学生 277 人に誤送信	福岡大学	対策不備（メール誤送信）	低	教務	職員
19	2014/1	教員が車上荒らしの被害に遭い、同教員が 2009 年から 2013 年に担当した講義を受講した学生の氏名、学籍番号、成績データなど 2264 件の個人情報を保存したノート PC が盗難	兵庫医療大学	盗難（車上荒し）	低	教務	教員
20	2013/12	教員免許状の更新講習について申し込みを受け付けている教員免許更新支援センターのサーバーが不正アクセスを受け講習申込者の個人情報が流出した可能性	信州大学	ハッキング	高	就職	職員
21	2013/12	生物生産学部において、受験生から提出された一部入学志願関係書類を紛失	広島大学	紛失	低	入試	職員
22	2013/11	399 人分の氏名、学籍番号、成績などのほか、研究参加者 273 人分の研究データが保存されていた USB メモリを紛失	四天王寺大学	紛失（USB）	低	教務	教員
23	2013/11	13 人の氏名、受験番号、専攻系名、希望種別、推薦順位などが記載されていた「日本学生支援機構大学院奨学生申込者名簿」をキャンパス内に 30 分放置	東京大学	対策不備	低	奨学金	職員
24	2013/11	デジタル複合機 2 台内の他大学の学生 115 人の試験結果、医科学研究所職員の氏名が記載されたセミナー受講証 12 人分など個人情報が含まれるデータがインターネット上で閲覧可能な状態	東京大学	対策不備	低	教務	職員
25	2013/10	教員が、学生約 200 人の氏名、学籍番号、試験の点数などが記録された USB メモリを紛失	大正大学	紛失（USB）	低	教務	教員
26	2013/10	教員免許更新講習用のサーバーが不正アクセスを受け、サーバー内で管理されていた「教員免許更新講習の受講者の氏名、住所、電話番号、勤務先」が流出した可能性	清和大学	ハッキング	高	就職	職員
27	2013/10	医学部付属病院の医師が、氏名、患者番号、生年月日、年齢、性別など患者 12 人分の個人情報が含まれていた電子カルテを投影した資料を用いて学会発表を実施	東京医科歯科大学	対策不備	低	研究活動	教員

No	年	内容	発生個所	脅威種別	技術難易度	業務	人物
28	2013/10	メールの送信ミスが発生し、国際シンポジウムの参加申込者のメールアドレス 339 件とそのうち 10 名の氏名が流出	東京大学大学院教育学研究科	対策不備（メール誤送信）	低	教務	職員
29	2013/10	学生採用試験において、答案用紙 8 人分を紛失	航空保安大学校	対策不備	低	入試	職員
30	2013/9	法学部において学生 141 人に事務連絡メールを一斉送信した際、送信先アドレスを「TO」に設定して送信。そのため、宛先とした全員の氏名、学年、メールアドレスが表示	名古屋大学	対策不備（メール誤送信）	低	教務	職員

業務内容については情報漏洩事故が多いものから教務40%(30件中12件)、研究活動27%(30件中8件)、就職（教員免許）10%（30件中3件）、保健7%(30件中2件)、奨学金7%(30件中2件)、入試7%(30件中2件)、渉外3%(30件中1件)となっている。履修登録等の授業に関連した教務の割合が多いのは作業項目や作業量から予想できたが、教員による研究活動の割合が多かったことが新たに判明した。

情報漏洩に関連した人物別では職員が57%(30件中17件)、教員が40%（30件中12件)、学生がわずか3%(30件中1件)であった。先の米国大学における調査でも同様に学生が原因の情報漏洩事故は発生していない。日米両国の結果から学生が情報漏洩事故に起因していないということが判明した。従ってリスク評価においては教職員が重要な調査対象となる前提で考察を進めることとする。

更に脅威種別や技術難易度について表5-3に示した。

表5-3　日本国内大学における情報漏洩事故の脅威種別割合と技術難易度割合

	脅威種別					技術難易度		
	ハッキング	盗難・紛失	ID詐称・偽称	対策不備	内部犯	高	中	低
(%)	**10 (3)**	**40 (12)**	**0 (0)**	**50 (15)**	**0 (0)**	**10 (3)**	**0 (0)**	**90 (27)**
頻度	**中**	**高**	**低**	**高**	**低**			

技術難易度の高いハッキングが全体の10%（30件中3件）発生している。教員免許の更新の為の業務に使用されているハッキング事故が同時期に7%（30件中2件）発生していることから、今後は米国同様に個人情報をターゲットとしたハッキング事故が発生することが予想される為、効果的なハッキング対策が求められる。

一方で技術難易度の低いメールの誤送信やネットワーク接続型ハードディスクの設定不備などの対策不備が全体の50%（30件中15件）発生している。同様に技術難易度の低いUSB、PC等の盗難・紛失等が40%（30件中12件）発生している。この2つの事故の合計で事故全体の90%（30件中27件）を占めることから、関連者へのセキュリティ教育など現在の人的、設備的資源（リソース）で対応できることも多く、その結果、大学におけるセキュリティ対策の遅れが露見された結果となった。

３　日本国内大学におけるマイナンバーの利用シミュレーションとリスク評価

米国の大学では約半数近くの大学が学生IDの代替としてSSNを利用していることから、将来利用する大学が増えてくることが想定されるため、学生IDの代替としてマイナンバーを利用した場合を想定し、大学内での各作業におけるリスク評価を実施することとした。

３．１　リスク評価の方法

リスク値の算出については「第４章　２　シミュレーションモデルのリスク評価」と同様の手法を用いた。

リスク値　＝　「資産の価値」　×　「脅威」　×　「脆弱性」

「資産の価値」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。

「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」とし下表5-4に示す。

表5-4　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

大学でのリスク評価を行うにあたり、「第４章　２　シミュレーションモデルのリスク評価」について以下の三点を改善した。

一点目は、３か所のセキュリティホールへのリスク評価は一般的なものに限定されていた。例えば、「民間事業者設備」は金融や医療など様々な対象があるにも拘らず「民間事業者設備」という一項目としてリスク評価をしている為、対策も一般論に留まっている。今回は具体的なリスク評価対象の組織として「大学」を調査対象とし、より現実に則したリスク評価を行った。

二点目としてリスク評価に用いた算出基準の中でも、特に脅威の基準が日米韓の事故の件数から頻度を導いた点で改善が必要であった。つまり日本の事故が37件、米国の事故が16件、韓国の事故が7件であるが、それらの数値を使って頻度を求めているため事故が多かった日本における事故の種類がそのまま高い頻度として基準になっている事である。そ

の点については、国内大学で起きた事件３０件をサンプルの母体として均一化したことで改善した。

表5-2の情報漏洩事故30件から算出した頻度の「高」「中」「低」についてそれぞれスコア「3」「2」「1」で表現し脅威の基準として用いた。

その結果を表5-6に示す。

表5-6　脅威スコア基準

頻度	説明	スコア
高	盗難・紛失、対策不備など	3
中	ハッキング	2
低	ID 詐称、内部犯	1

三点目として大学内の登場人物が行う日常の作業に着目し、詳細にリスク評価を実施した。学生や教職員がどのような場面でマイナンバーを利用し、それがどのようにシステムに流通するかについて、同志社大学の「電算処理　業務システム一覧」[19]を参考に学生が入学試験を受験した時点から卒業生するまで行う作業についてシミュレーションを実施し、先のリスク評価基準を用いてリスク評価を行った。電算処理の業務システム一覧を示し、どのような作業工程があるか記載して表5-7にまとめた。

表5-7　電算処理　業務システム一覧

作業	詳細	説明	情報漏洩事故件数%(30) ※その他1件
学生情報	入試	合否判定、合格通知書作成、 統計資料作成（志願者・採点データ処理は外部委託）	7%(2)
	学費	学費請求、学費収納状況管理	0%(0)
	教務	学籍管理、科目登録、授業運営、成績管理 証明書データ作成、学修支援システム	40%(12)
	保健管理	健康診断データ管理、 再検査・精密検査データ管理、統計資料作成 証明書データ作成	7%(2)
	証明書発行	教務、保健管理関係の証明書発行	0%(0)
	就職	会社情報管理、学生就職情報管理、 統計資料作成、	10%(3)

		会社情報提供(WWW)	
	奨学金	奨学生選考、奨学生異動管理、 貸与奨学金返還管理、統計資料作成	7%(2)
教育・研究	授業情報	シラバス入稿、冊子CD-ROM用データ作 成、シラバス公開・検索、休講情報	0%(0)
	研究活動	学会への参加、研究論文投稿など	27%(8)
	研究者情報	研究者基本情報管理、業績検索(WWW)	0%(0)
	知的財産	特許情報管理、申請・統計資料作成	0%(0)
管理情報	渉外対応	他機関への対応、行政文書公開	3%(1)
	財務	予算管理、日次・月次処理、現預金残高管 理、物品等発注管理、備品管理、決算処理、 電話課金、財産目録管理	0%(0)
	科研費管理	受入、執行管理、報告書作成	0%(0)
	人事・給与	勤務管理、人事稟議、在籍・異動、研修、 アルバイト管理、給与計算、税額計算、 福利厚生業務、統計資料作成	0%(0)
学術情報	蔵書検索、学術情報検索、学術情報ポータル サイト、発注管理、貸出返却、予算管理、WEB サービス(購入希望、予約依頼、貸出更新 等)、学内紀要・貴重書電子化		0%(0)

３．２　入試に関連した作業におけるリスク評価

シミュレーションの前提条件としてマイナンバーは受験番号として用いられ、入学後もそのまま学籍番号（学生ID）として利用されると予想した。マイナンバーを利用した入試業務は以下の6つのプロセスで構成される。

①大学のWEBサイト、もしくは書類（郵送か大学構内）による募集要項の入手

②募集要項にマイナンバーを記載し郵送で応募

③受験費振込の際に振込者の先頭にマイナンバーを入力し金融機関の窓口業務担当者に提出

④受験票が大学側に到着しマイナンバーで受験者を管理

⑤受験会場でマイナンバーを答案用紙や小論文答案用紙等に記載

⑥合格発表（学内掲示板と郵送）大学側が受験者に対して合格発表を行う際に郵送の同梱物である合格証書にマイナンバーを記載

リスク値の算出方式に基づき、入試に関連した作業におけるリスク評価を実施した。その結果を表5-8に示す。

表5-8　入試に関連した作業におけるリスク評価

脅威	脅威スコア	脆弱性	脆弱性スコア	リスク評価
受験者が応募用紙にマイナンバーを記載する際に周辺に居る悪意ある第三者に漏洩	1	応募用紙のマイナンバーは閲覧が容易	2	2
受験応募用紙の郵送の際の郵送事故	1	郵便局での管理について内部者が悪意のある第三者である場合は防止困難	1	1
金融機関の窓口業務の担当者が悪意のある第三者でありマイナンバーが漏洩	1	金融機関での管理について内部者が悪意のある第三者である場合は防止困難	1	1
銀行の勘定系システムに対するハッキング	1	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	1
応募用紙を処理する大学側の担当者が悪意のある第三者でありマインナンバーが漏洩	1	大学機関での管理について内部者が悪意のある第三者である場合は防止困難	1	1
受験応募用紙の郵送の際の郵送事故	1	郵便局での管理について内部者が悪意のある第三者である場合は防止困難	1	1
受験会場の試験管が悪意のある第三者でありマインナンバーが漏洩	1	試験監督員が悪意のある第三者である場合は防止困難	1	1
答案用紙を郵送する際の郵送事故	1	郵便局での管理について内部者が悪意のある第三者である場合は防止困難	1	1
解答作業を行う大学の担当者もしくは作業を委託している業者の担当者が悪意のある第三者でありマイナンバーが漏洩	1	解答作業を行う機関での管理について内部者が悪意のある第三者である場合は防止困難	1	1
合格証書を郵送する際の郵送事故	1	郵便局での管理について内部者が悪意のある第三者である場合は防止困難	1	1

受験者が応募用紙にマイナンバーを記載する際に周辺に居る悪意ある第三者に漏洩するリスク値が2と最も高い。脅威（頻度）は低いためポイントは1となり、脆弱性（技術難易

度）は2であることからリスク値は2となる。その他の考えられるリスク項目についてリスク評価を行ったがリスク値は全て1でありリスクは低いことが明らかとなった。

応募用紙や回答用紙の紛失事故が2件発生しているが郵送事故に関しては2005年12月の朝日新聞に「04年度に郵政公社が把握している誤配と紛失は、普通郵便230億通のうち約35万通、配達証明郵便と書留は3億6,000万通のうち1,000通余り、小包で14億3,000万件のうち5,000件余り」と掲載されている。回答用紙は回収後、配達証明郵便で配送されていると推測されるため、紛失の確率は3億6,000万通のうち1,000通余りであることから事故発生率は低いと考えられる。

以上より入試関連時に郵便事故によるマイナンバーの漏洩リスクは極めて低いことが明らかになったが、各組織の担当者が悪意のある第三者であった場合の内部犯の防止は極めて困難であり、各組織での内部犯漏洩対策がセキュリティ対策上は重要である。

３．３　学費に関連した作業におけるリスク評価

学費に関連した作業は以下の3つのプロセスで構成されている。

①学費請求を入学予定者もしくは在校生へ郵送

②振込用紙を持参し金融機関窓口で納付

③学費収納状況を大学側で確認。未納の場合は催促状の郵送など収納管理

リスク値の算出方式に基づき、学費に関連した作業におけるリスク評価を実施した。

その結果を表5-9に示す。

表5-9　学費に関連した作業におけるリスク評価

脅威	脅威スコア	脆弱性	脆弱性スコア	リスク評価
郵送事故によりマイナンバーを記載した応募用紙が紛失や盗難	1	郵便局での管理について内部者が悪意のある第三者である場合は防止困難	1	1
受験費用の振込の際に振込者の先頭にマイナンバーを入力した場合に金融機関の窓口業務の担当者にマイナンバーが露出	1	金融機関での管理について内部者が悪意のある第三者である場合は防止困難	1	1
金融機関の勘定系システムに対するハッキング	1	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	1
大学側の担当者は大学の情報システムにログインして収納状況を確認する際に入学予定者や在校生のマイナンバーが漏洩	1	大学機関での管理について内部者が悪意のある第三者である場合は防止困難	1	1
催促状を郵送する場合も同様に郵便事故のリスク	1	郵便局での管理について内部者が悪意のある第三者である場合は防止困難	1	1

リスク値が全て1と低い点や、過去に情報漏洩事故が学費に関する作業時に発生していない点からマイナンバーの漏洩リスクは極めて低いと考えられる。

一方で各組織の担当者が悪意のある第三者であった場合の内部犯の防止は極めて困難であり、各組織での内部犯漏洩対策がセキュリティ対策上は重要なポイントとなる。

３．４　教務や研究活動に関連した作業におけるリスク評価

教務や研究活動による作業を考えた際には関連者として学生、教員、職員が挙げられる。それぞれの立場での作業についてリスク評価を行った。学生の立場から教務に関連した作業をリストアップすると学籍管理、科目登録、授業運営、成績管理 証明書データ作成、学修支援システム運用などが挙げられる。学生が行う教務の作業では入学時に配布される学生番号とそれが記載された学生カード[20]が重要な役割を担っている。学生番号は学籍を

管理するために用いられる管理番号であり、同志社大学の学生に対しては「同志社の個人情報保護の基本方針」[21]という運用ルールに基づき配布される。関連する具体的な内容を幾つか下に記す。

- 具体的な利用システムはセキュリティ情報となるため非開示である。
- 学生カードは身分証明書としての機能は勿論、接触ICチップ、非接触ICチップ、磁気ストライプ、マトリクスを利用して以下のような各種サービスを利用可能としている。

（教務）Webシングルサインオンサービス　…　接触ICチップ、マトリクス
（教務）情報教室・PCコーナー利用時の端末利用認証　…　接触ICチップ
（教務）入退室管理　…　非接触ICチップ、磁気ストライプ
（証明書発行）各種手数料等納入　…　非接触ICチップ
（学術情報）図書システム　…　非接触ICチップ、磁気ストライプ
（その他サービス）生協マネー　…　非接触ICチップ

- サービスを安全に利用するために、学校法人同志社としての基本方針と規定[22]に則って運営されている。

学籍管理、科目登録、授業運営、成績管理、証明書データ作成、学修支援システムについては既に現状の学内サービスもオンラインで統一されている。マイナンバーを利用した教務に関連した作業は以下の8つのプロセスで構成される。

①大学のWEBサイト（同志社の場合はWebシングルサインオンサービス）にユーザIDとパスワードでログイン実施。「ネットワーク利用資格認定試験」に合格した後、DUET(Doshisha Univ.Electronic Tutorial system))呼ばれる学修支援システムを通じて「履修手続き（履修科目登録、中止、チェック）」、「時間割表示」、「休講情報や試験情報」、「授業評価アンケート」「成績確認」などの各種サービスを利用

②メール利用（PCとスマホ）

③Webdisk

学生個人に割り振られたオンラインディスクサービスである。授業で使用する電子資料などをアップデートして保管

④e-class

教員は資料のアップデートや出欠管理や試験など担当授業に関わる作業を一括してWebインターフェースで実施

⑤Go Global

外国協定大学派遣留学制度へのエントリーやご学習習熟度などを管理

⑥e-career

進路希望の登録、企業情報の検索、求人情報の検索、セミナーやインターンシップの情報などを検索

⑦scholorship/school Fee（奨学金・学費延分納申請）

奨学金の申請や学費の分納申請が行えるポータルサイト

⑧e-learning（図書館講習会）

図書館の利用案内、図書の貸出や返却などが可能

リスク値の算出方式に基づき、学生、職員、教員それぞれの教務や研究活動に関連した作業におけるリスク評価を実施した。その結果を表5-10に示した。

表5-10　教務や研究活動に関連した作業におけるリスク評価

脅威	脅威スコア	脆弱性	脆弱性スコア	リスク評価
学生カードに学籍番号としてマイナンバーが印字される場合、教職員がその番号を知ることが可能	1	カードの両面は容易に閲覧が可能	3	3
マイナンバーが漏洩すると他の学生サービスにも容易にログインされ、その他の個人情報が漏洩するリスク	1	1つのIDパスワードでの管理であるがセキュアな保存が未実施（付箋紙に記載してPCや机に貼りっぱなしである）	2	2
教務の連絡事項を職員がメールサービスを行った際に誤送信等でマイナンバーが漏洩するリスク	3	メールの誤送信を防止するサービスが未導入。職員へのメール使用方法やセキュリティについての教育が不徹底	3	9
奨学金の作業に関してはID(マイナンバー)が漏洩すると悪意のある第三者がパスワードを類推した場合に振込先の金融機関に本人になりすましてログインし、口座の残高から金銭を搾取するリスク	2	大学機関での管理について内部者が悪意のある第三者である場合は防止困難	1	2
各種情報を印刷した場合に印刷機やキャンパス内に置き忘れたりする可能性	1	職員や教員のセキュリティ意識が低く重要な個人情報を有した資料を預かっているという認識の欠如	2	2
職員や教員がマイナンバーを保有した情報をUSB、PC、外付けハードディスクに保存し、紛失や盗難に遭う	3	職員や教員のセキュリティ意識が低く重要な個人情報を有した資料を預かっているという認識の欠如	3	9
ネットワーク接続ストレージ（NAS）のアクセス制限が正しく設定されておらずインターネットからマイナンバーが閲覧可能	2	職員や教員のセキュリティ意識と知識が低い	3	6

教務の連絡事項を職員がメールサービスを行った際に誤送信等でマイナンバーが漏洩するリスク値が9と極めて高い数値になっている。学内の連絡等にメールを使用するケースが多く、実際にメール誤送信などメールに関する情報漏洩事故の頻度は16%（30件中5件）と高い。

また技術的な難易度も容易であることからマイナンバー利用時にも同様に高いリスクとして考えられる。メールの誤送信を防止するサービスの導入や職員へのメール使用方法やセキュリティについての教育を徹底することが事故防止のために重要な事項となっている。

職員や教員がマイナンバーを保有した情報をUSB、PC、外付けハードディスクに保存し、紛失や盗難に遭うリスク値が同じ9であった。職員や教員のへのセキュリティ知識の醸成が求められる。

表5-2に基づいた情報漏洩事故分析では、特に海外の学会に参加した際の事故が多かったことから、国内以上に紛失や盗難に注意すべきである。

またシステム上もUSB、PC、外付けハードディスクに個人情報を保存させない点について学校側でセキュリティポリシーとして定め運用方法まで徹底して実施することが求められる。

ネットワーク接続ストレージ（NAS）のアクセス制限が正しく設定されておらずインターネットからマイナンバーが閲覧可能である点についてはリスク値が6と高い数字を示した。教職員へのセキュリティ教育や、そのような設備を容易に利用させないというセキュリティポリシーと徹底した運用が求められる。

３．５　保健管理に関連した作業におけるリスク評価

マイナンバーを利用した保険管理における作業は以下の4つのプロセスで構成される。

①健康診断や健診を実施し、データ管理

②再検査・精密検査データ管理

①の検査の結果、再検査や精密検査が必要になった場合はその検査や検査結果のデータ管理を行う必要がある。

③統計資料作成

各学生の情報から学年別、学部別などのデータを整理し、そのデータに基づいた資料を作成する。

④証明書データ作成

各学生の健康診断書などの証明書を作成する。

リスク値の算出方式に基づき、健康管理に関連した作業におけるリスク評価を実施した。その結果を表5-11に示した。

表5-11　健康管理に関連した作業におけるリスク評価

脅威	脅威スコア	脆弱性	脆弱性スコア	リスク評価
健康診断の際にレントゲンフィルムなど関連した個人情報が紛失	1	病院関係、学校側における個人情報を包含した資料の管理体制が問題	2	2
健康診断に関連した資料にマイナンバーが記載されており、それら資料を保有した情報をUSB、PC、外付けハードディスクに保存し、紛失や盗難に遭う	3	病院関係と大学関係職員のセキュリティ意識が低く重要な個人情報を有した資料を預かっているという認識の欠如	3	9

健康診断に関連した資料にマイナンバーが記載されており、それら資料を保有したUSB、PC、外付けハードディスクが紛失や盗難に遭うリスク値が9と極めて高い。対策としてはセキュリティ教育の徹底や、システム上もUSB、PC、外付けハードディスクに個人情報を保存させない点について学校側でセキュリティポリシーとして定め運用方法まで徹底して実施することが求められる。

健康診断の際にレントゲンフィルムなど関連した個人情報が紛失するリスクについては病院側と学校側における個人情報を包含した資料の管理体制に問題があるため、両組織においてマイナンバーを含めた個人情報の取扱についてセキュリティ教育を徹底する必要がある。

３．６　就職（教員免許取得）に関連した作業におけるリスク評価

マイナンバーを利用した就職（教員免許）における作業は以下の5つのプロセスで構成される。

①免許資格課程仮登録　（DUET経由）

②免許教科に登録し履修　単位取得　（DUET経由）

③教育実習等に参加

④教員免許取得

⑤教員免許更新

リスク値の算出方式に基づき、教員免許に関連した作業におけるリスク評価を実施した。その結果を表5-12に示す。

表5-12　教員免許取得に関連した作業におけるリスク評価

脅威	脅威スコア	脆弱性	脆弱性スコア	リスク評価
教員免許更新支援センターのサーバーが不正アクセスを受け講習申込者の個人情報が流出	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
マイナンバーを含んだ個人情報をUSB、PC、外付けハードディスクに保存し、紛失や盗難に遭う	3	大学関係職員のセキュリティ意識が低く重要な個人情報を有した資料を預かっているという認識の欠如	3	9

マイナンバーを含んだ個人情報をUSB、PC、外付けハードディスクに保存し紛失や盗難に遭うリスク値が9と極めて高い。対策としてはセキュリティ教育の徹底や、システム上もUSB、PC、外付けハードディスクに個人情報を保存させない点について学校側でセキュリティポリシーとして定め運用方法まで徹底して実施することが求められる。

教員免許更新支援センターのサーバーが不正アクセスを受け講習申込者の個人情報が流出するリスク値が4と中程度のリスクであるが、表5-1に基づいた米国の大学における漏洩事故分析結果からもハッカーが個人情報をターゲットにしたハッキングを行っているため日本国内でも今後は同様の事故が増加すると推測される。

従ってハッキング対策の徹底が求められることから最新のハッキング情報についても入手し対応を行うことやOSやソフトウェアのバージョンアップやパッチ適用を実施し、脆弱性対策を徹底する必要がある。

４　まとめ

Siciliano(Mcafee) (2010) の報告にあった、米国においてソーシャルセキュリティナンバー (SSN) の情報漏洩事故の発生確立が最も高い場所である大学について、実際に日本国内の大学での情報漏洩事故について分析した。

日本国内の大学では情報課を中心にセキュリティ事故防止に向けISMSの導入や個人情報漏保護のルール策定が行われてきたが一部の大学で従来導入されたものの、多くの大学ではまだ未導入である。そのような状況を反映して、大学における情報漏洩は2013年9月から2015年1月の間に判明しただけでも30件の情報漏洩事故が報告されている。

それら情報漏洩事故の内容を分析した結果、情報漏洩に関連した人物別では学生がわずか3%(30件中1件)であった。職員が57%(30件中17件)、教員が40% (30件中12件)であることからセキュリティ意識が低いと思われた学生ではなく、教職員がセキュリティホールとなっていることが判明した。従って教職員へのセキュリティ対策が今後は更に必要となることが判明した。それらの情報も参考にし、日本国内の大学においてマイナンバーが利用されることを想定したシミュレーションに基づきリスク評価を実施した結果を以下に示す。

- 業務内容については情報漏洩事故が多いものから教務40%(30件中12件)であり、次いで研究活動27%(30件中8件) であることが判明した。それらの情報に基づいた評価基準を策定し、登場人物である学生、教員、職員の日々の作業においてマイナンバーを利用すると仮定した上でのリスク評価を行った結果のまとめは以下のとおりである。

- 入試に関連した作業におけるリスク評価については、受験者が応募用紙にマイナンバーを記載する際に周辺に居る悪意ある第三者に漏洩するリスク値が2と最も高く、対策としてはマイナンバーを他人に知られないようにする意識の醸成などの運用が必要であることが判明した。全体を通してこの作業に関するリスク値は低いため大きなリスクとはなり得ないことが判明した。

- 学費に関連した作業におけるリスク評価については、リスク値が全て1と低い点や、この作業に関連した情報漏洩事故が発生していない点からマイナンバーの漏洩リスクは極めて低いと考えられる。

- 教務や研究活動に関連した作業におけるリスク評価については、職員によるメール誤送信、マイナンバーを保存したUSB、PC、外付けハードディスクを教職員が紛失や盗難に遭うリスクがリスク値9と高い。それぞれの対策としてシステムを活用した防御策や本人へのセキュリティ教育が重要である。

- 保健管理に関連した作業におけるリスク評価については、同様にUSB等の外部媒体を介したリスク値が9と高く、上述と同様の対策を講じる必要がある。また学外関係者についても同様のセキュリティ教育が必要である。

- 就職（教員免許取得）に関連した作業におけるリスク評価についても同様にUSB等の外部媒体を介したリスク値が9と高く、上述と同様の対策が求められる。教員免許更新支援センターのサーバーが不正アクセスを受けて講習申込者の個人情報が流出するリスクはリスク値が4と中程度のリスクであるが、今後はハッカーが個人情報をターゲットにしたハッキングを行う事故の発生が予想されるためハッキング対策が必要である。

リスク評価では職員によるメール誤送信、マイナンバーを保存したUSB、PC、外付けハードディスクを教職員が紛失や盗難に遭うリスクが非常に高かった。

日本国内大学における情報漏洩事故における調査では、メールの誤送信やネットワーク接続型ハードディスクの設定不備などの対策不備が全体の50%（30件中15件）、USB、PC等の盗難・紛失等が40%（30件中12件）発生している。この2つの事故の合計で事故全体の90%（30件中27件）をヒューマンエラーが占めることから、ヒューマンエラーの防止策の重要性が改めて示された。

次章では、これらの結果を受け、情報漏洩事故におけるヒューマンエラーの防止策について考察を進めた。

第６章　ヒューマンエラーの防止策

１　分析の考え方

ヒューマンエラーを防止するという観点から考えた場合に、事故を引き起こす最大の要因、すなわちリスクは人間である。過去に発生した情報漏洩事故の多くがヒューマンエラーに起因しているのは人間が機械やコンピューターと異なり完全では無いからである。本来それぞれの人間が持っている特性や個性、それら人間を取り巻く様々な環境下においてヒューマンエラーが発生した原因を探ることが最も重要な作業であり、それにより情報漏洩事故の再発防止の仕組みを構築することが可能となる。

２　代表的な分析手法の紹介

本章では、分析手法について例を挙げて説明し、それらの分析手法の特性を考慮して、サイバーセキュリティに最適なものを選択する。また既に発生したマイナンバーの情報漏洩事故におけるヒューマンエラーの分析手法として適用し、その効果を図ることが最終的な目的である。

航空、鉄道、船舶、電力、ガス、原子力、医療などの各分野で確立されたヒューマンエラー分析手法として代表的なものとして「4M-4E」、「Medical SAFER」、「VTA」等のモデルがある。

２．１　4M-4Eについて

「4M-4E」はアメリカ空軍が開発し、米国国家運輸安全委員会（National Transportation Safety Board （NTSB））の事故調査委員が採用した手法である。

千葉（2004）によると、その後1974年に国際民間航空機関（International Civil Aviation Organization （ICAO））が出版した「事故防止マニュアル」が広く普及し世界各国の航空業界が採用する事故防止のための標準的な手法としてデファクトスタンダードとなり既に産業界でも様々な分野で活用されている。

事故が発生した場合の事故調査においては「誰が犯人か（Who）」という責任者を追求する発想に基づいて行われるケースが多かったが、「なぜ発生したのか（Why）」という発想に転換し原因を究明する必要があるという考えに基づいている。事故原因究明のために重大事象（Safe Critical events）の内容に抽出し、時系列に並べて事故要因の連鎖関係（Sequence of events）を明らかにする必要がある。

4M とは以下4つのMを意味している。

- Man(人間)
- Machine(機械)
- Media(媒体)
- Management(管理)

4E とは以下4つを意味しており4M に対応する対策を意味している。

- Education(教育)
- Engineering(工学)
- Enforcement(強化・徹底)
- Example(模範・事例)

Environment(作業環境)を加えて5Eとする場合もあり、本研究では5Eを採用した。これらをマトリックスとして表に記載していくことにより、さまざまな視点からの分析を行う手法である。事象概要に基づき、ヒューマンエラーの要因を全て網羅している要因分類表から該当する要因をマトリックスに記載する。それら要因に対する該当する対策を対策分類表に基づきマトリックスに記載する。

（公財）原子力安全技術センター（2015）では「トラブル事象分析手法4M-5E」が紹介されている。

紹介文中の「利用にあたっての留意事項」にはその特徴として以下の2点について述べている

- 事象分析の専門家でなくても比較的利用が容易である
- 作業担当者レベルでも要因分析が出来る

一方で利用上の注意点として下記2点が該当する場合はヒューマンエラーの要因分析として最適ではないとしている。

- 要因が様々で複雑な事故
- 潜在的な要因があり、再発防止策などについて詳細に行う必要性がある場合

これらの特性や注意点を認識し活用することが必要である。

２．２　Medical SAFERについて

Medical SAFERは、「SHEL」モデルを改良したものである。

関岡（2005）によると、「Software、Hardware、Environment、Liveware（作業者と他者)」の 4つの観点から要因分析を行い評価するものであり、1972年に英国のエドワーズ（Edwards,E.）によって開発され、1984年にKLMオランダ航空の機長であったHawkins, F.H.が改良し完成させたとしている。これに1990年代後半に東京電力原子力研究所の河野（1999）が「Management」を加えたモデルとして「m-SHEL」モデルを提供し、交通やプラント等の事故分析に用いられている。「Pm-SHELL」モデルは、さらに「Patient(患者)」を加えた手法であり、主に医療分野において用いられている。

m-SHELは以下5つを意味している。

- m（management）（マネージメント）
- l（liveware）（人間）
- s（software）（ソフトウェア）
- h（hardware）（ハードウェア）

- E（environment）（環境）
- L（liveware）(他の人間)

m-SHELの中心はあくまでも人であり、中心の当事者である最初のL（liveware）(人間)に対して以下のとおりそれぞれの関連性を示している。

L-SはL（liveware）(人間)とS（software）（ソフトウェア）の関連性を示しており、コンピュータプログラムやマニュアルなどが該当する。
L-HはL（liveware）（人間)とH（hardware）（ハードウェア）の関連性を示しており、サーバーやネットワーク機器などが該当する。
L-EはL（liveware）（人間)とE（environment）（環境）の関連性を示しており、天候、温度、湿度、振動、天候など作業者の作業内容や効率に影響を及ぼす外的要因の事を意味する。
L-LはL（liveware）（人間)とL（liveware）（人間）の関連性を示しており、上司、同僚、部下などの協働者を意味する。

ヒューマンエラー分析の観点から、それぞれの関連性が正常に機能していない場合にエラーが発生する確立が高くなる。従って常にこれらの関連性に注視して分析し、問題が発生した場合には改善策を講じる流れとなる。M（management）（マネージメント）は他の要素とは独立した項目であり、全ての項目に影響を及ぼす監視的な役割を担っている。実際に事故（インシデント）が発生した場合にはそれぞれの関連性において正常に機能していない項目を要因として「要因分析と対応策」という表に記載する。
自治医科大学医学部医療安全学教授である河野（2014）は「Pm-SHELL」の考えに時系列で事象を整理することを加えたものを「Medical SAFER（Medical System by Analyzing Fault root in human ERror incident）」医療向けに開発した。
現場担当者が分析に関する専門知識を持たなくとも自分達の手で事故分析を行えるように作成されたものであることから、この分析手法は昨今よく利用されている。

２．３　VTA（Variation Tree Analysis）について

「VTA（Variation Tree Analysis）バリエーションツリー分析」はFTA（Fault Tree Analysis）の欠点を修正し作成された。フロー チャート式に追っていき事故要因を洗い出す手法が特徴的であり、人や物、組織などの主体ごとに時系列に沿って、事故につながる通常から逸脱した行為や操作、判断を探り、最終的に事故要因を洗い出す手法である。多くの事故に見られるエラーの連鎖をこの要因ごとに対策を講じることで断ち切るものである。

ヒューマンエラー分析手法で代表的な「4M-5E」、「Medical SAFER」、「VTA」の３種類を実際に発生した情報漏洩事故へ適用し、その効果を比較することで、どの手法がサイバーセキュリティに適しているか判断することとした。

３　情報漏洩事故に最適なヒューマンエラー分析手法の選択

３．１　実験手法と事故事例の選択

適用実験では前章で説明したヒューマンエラー分析手法で代表的な「4M-5E」、「Medical SAFER」、「VTA」の３種類を用いてその効果を比較検討した。

事故事例としてUSB、PC等の紛失を分析・対策立案の対象とした。理由として以下3点を挙げる。

- NPO 日本ネットワークセキュリティ協会（2008）によると、情報漏洩事故の種別は、PC等媒体の紛失・盗難、メールや FAX の誤送信、誤廃棄、不正アクセス、ウイルス感染に起因したものなど多様化している。報告によると2011年の情報漏洩事故の原因としてヒューマンエラーとして分類される「紛失・置忘れ」が13.7%であり高い割合を示していることから対象として最適であると考えた。

- 日本国内大学における情報漏洩事故分析においてもUSB、PC等の盗難・紛失等が40%（30件中12件）と高い割合で発生していることから事故事例の適用実験の題材として最適であると考えた。

- またITの利用頻度、利用容易性、持ち運びが簡単である点、大量のデータをやり取りが可能であり大規模な情報漏洩事故となる可能性が高いなどの理由からもUSB、PC等の紛失を分析・対策立案の対象とすることが最適であると考えた。

３．２　適用実験

選択した「4M-5E」、「Medical SAFER」、「VTA」について分析するために必要となる基礎情報として事故報告書を作成した。作成した事故報告書の情報に基づき「4M-5E」、「Medical SAFER」、「VTA」、それぞれの手順に従って適用実験を行った。

対象事故として表5-2「日本国内大学における情報漏洩事故分析」の１番の事例として紹介した2015年1月に発生した大阪市立大学教員の USBメモリ紛失による個人情報の漏洩事故を取り扱うこととした。理由として大阪市立大学の公式HP[23]上に事故の状況が細かく報告されており、分析に必要な情報が得られると考えたからである。

【事故報告書】

（以下）

タイトル：大阪市立大学教員のUSBメモリ紛失による個人情報の漏洩事故

施設名：大阪市立大学

発生日時：2015年1月

発生状況：教員の海外出張時

発生場所：クチン市（マレーシア）

発生設備及び機器：USBメモリ

事故の原因：布製ポーチの紛失。布製ポーチには、USBメモリ1 個、パスポート、航空機の搭乗券3枚が入っていた。

事故の種類：紛失

結果／影響：当該教員が2009年に担当した2つの授業を受講した39名分の学生の学籍番号、氏名、 成績データ（のべ62 件）の情報漏洩の可能性

法律区分：個人情報、プライバシー

[状況]

平成 27 年 1 月 27 日(火)、大阪市立大学教員が海外出張中、滞在先のマレーシアにおいて布製ポーチを紛失した。

布製ポーチには、USBメモリ1個、パスポート、航空機の搭乗券3枚が入っており、そのうちUSBメモリには本学学生及び卒業生の個人情報を含むデータファイルが保存されていた。当該教員は直ちに現地警察に遺失届を提出したが、 現時点ではまだ見つかっておらず、捜索を続けている。

今後の対応

- データ紛失対象者のうち、本学に在籍する学生に対し、2014年2月5日(木)より口頭及び文書にて、説明及びお詫びを実施。
- 卒業生に対しては、説明及びお詫びを文書にて送付。
- 本学ホームページにて2014年2月6日(金)より、学長名で本件の説明とお詫びを掲載。

事実経過

(1) 平成27年1月27日(火)午後9時30分ごろ［現地時間］理学研究科准教授(男性45歳)がクチン市(マレーシア)にて、公園内を通行中に、ズボンのポケットに布製ポーチを入れていた。

(2) 同日午後9時45分ごろ ズボンのポケットに入れていたはずのポーチが無くなっていることに気付く。付近を 捜すとともに、地元警察に遺失届を提出。

(3) 平成27年1月29日(木)日本領事事務所で帰国のための渡航書を受理。

(4) 平成27年2月4日(水)午前8時30分 帰国。

［紛失した個人情報］エクセルファイル(2個) ※パスワード保護有りに記載された
当該教員が2009年に担当した2つの授業を受講した39名分の学生の学籍番号、氏名、成績データ(のべ62件)

［原因］ USBメモリ紛失。所持品管理不徹底によるヒューマンエラー

［対策］

・クチン市(マレーシア) の地元警察に遺失届を提出。

・2月9日(月)の部局長等連絡会において、理事長より全学部・研究科長に対して、注意喚起を行い、個人情報の適正管理及び記憶媒体の持ち出しの際に内容確認を厳重に行うことを強く命じた。

[影響/被害]

本件に関し、情報流失等の被害報告は無し

(以上)

(1) 「4M-5E」の適用について

事故報告書に基づき「4M-4E」の手順に添ってヒューマンエラー分析を実施する。今回は、Environment(作業環境)を加えて5E とする。原子力安全技術センター (公団) (2015) が使用している分析手法マニュアルを参照し分析を行った。

[Man：作業者の心身的な要因、作業能力的な要因]

１．身体的要因

大学教員の身体的な要因、体格、作業姿勢等の要因について調査を行う項目である。

海外出張中の大学教員の身体的な要因は、大学からの報道発表には一切記載が無いことから要因分析が不可能である。また体格や作業姿勢等は今回の事故における身体的な要因とは関連性が低い。

２．心理生理的要因

大学教員の心理的、生理的な要因について調査を行う項目である。

大学教員の思い込み、推測などの主観的な要因と過度の緊張、焦り等の心理的なストレスの他、病気、睡眠不足等の生理的なストレスなどが含まれる。海外出張中の大学教員の心理生理的な要因は大学からの報道発表には一切記載が無いことから要因分析が不可能で

あるが、海外出張中ということでその前の準備で疲労が蓄積していた可能性や、その作業や時差の影響による睡眠不足の可能性は考えられる。

３．技量

大学教員の技量の不足について調査を行う項目である。

作業を行う上で十分な技能が無かったり、作業に不慣れであったりする場合が該当する。今回の情報漏洩事故が発生した原因は布製ポーチの紛失であり、個人情報が含まれていたUSBメモリの操作に関する技量については事故原因との直接的に関連している可能性は低い。

４．知識

大学教員の知識の不足、誤った理解等の要因について調査する項目である。

公園内で布製ポートを紛失し、現在も発見されていないことから盗難の可能性もある。海外での安全管理や持ち出し可能な電子媒体であるUSBメモリの安全な保管に対して知識が不足していた可能性がある。

５．不正

大学教員自らの意図又は指示を受け不正を認識したうえ行う行為等の要因について調査する項目である。

今回の事故については布製ポーチをクチン市(マレーシア)内の公園で紛失した事が大学教員自ら分かった時点でクチン市(マレーシア)内の地元警察に遺失届を提出していることや、紛失により大学教員に金銭面等、何らメリットが無いことを考えた場合にこの項目は情報漏洩事故の要因として関連性は無い。

６．作業実施

大学教員の作業実施のタイミング、作業対象、作業順序、整理整頓の実施などが事故の要因になっていないか調査を行う項目である。

今回の情報漏洩事故の要因とは関連性が無いと判断した。

[Machine：設備・機器・器具固有の要因]

１．機器

機器の故障や動作不良など、機器固有の問題が情報漏洩事故の要因となっていないか調査する項目である。

今回の情報漏洩事故発生時にUSBメモリの故障と布製ポーチの紛失に関連は無い。

２．設計・機能

設計、インターフェースに関する要因、設計ミス、人間工学上の配慮の欠如などトラブルに関与した機器及び他の同機種にも共通し得る要因について調査する項目である。

今回の情報漏洩事故について、大学からの報道発表にはUSBメモリの詳細な一切記載が無いことから推測すると、大学教員は一般的なUSBメモリを使用していたと推測される。一般的なUSBメモリの場合はどのPCでも利用できるため個人情報が搾取される可能性が高くなる。

３．品質

機器の品質や管理状態に関する要因について調査する項目である。設備や機器が老朽化しているなどの機器の固有の問題に関するものである。

今回の情報漏洩事故については事故とUSBメモリの品質に関連性は無い。

４．物理的・化学的挙動

設備や機器の作業の結果生じた現象により事故に影響を与えた要因について調査する項目である。

今回の情報漏洩事故については事故とUSBメモリの使用やそれを利用した作業とは特に関連が無い。

[Media：作業者（今回は大学教員）に影響を与えた物理的、人的な環境の要因]

１．作業環境

大学教員に影響を与えた環境に関する要因について調査する項目である。照明や空調などの人工的な環境と雷、風雨などの自然環境が含まれる。

今回の情報漏洩事故について、大学からの報道発表には大学教員に影響を与えた人工的な環境と自然環境についての記述が一切無かったことから、特殊な環境下に大学教員が置かれていた可能性は極めて低い。

２．コミュニケーション

大学教員への情報伝達の不足に起因する要因や、必要な情報伝達方法がありながらも十分に機能していないなどの要因について調査する項目である。

大学教員は情報漏洩事故発生当時に他の人間とコミュニケーションを取りながら実施する作業を行ってはいなかったため事故との関連性は無い。

３．作業条件

作業の特性や役割分担、作業時間など労働条件に関する要因について調査する項目である。

大学教員は情報漏洩事故発生当時に業務に関する作業を行っていなかった。クチン市(マレーシア)にて、公園内を通行していたに過ぎない。従って事故との関連性は無い。

４．職場状況

人間関係や職場の慣習、組織風土などに関する要因について調査する項目である。

大学教員は情報漏洩事故発生当時に業務に関する作業を行っていなかったためことから人間関係や職場の慣習、組織風土などは事故とは何ら関連が無い。

[Management：組織における管理状態に起因する要因]

１．組織

組織の管理、運営に関する要因について調査する項目である。予算や経営方針、責任体制の要因を含むとされている。

大阪市立大学では、その情報セキュリティポリシー[24]の中で全学管理体制は、CISO(情報セキュリティ統括責任者)が統括するものとしており、予算、大学の経営方針における個人情報を取り扱う方向性、責任者及び責任体制の要因については今回の事故に影響は無い。

２．規則

規則、規定、基準に関する要因について調査する項目である。大阪市立大学は公立大学法人として「大阪市立大学情報セキュリティポリシー」を2007年4月16日に制定している。大阪市立大学情報セキュリティポリシーⅡ、情報セキュリティ対策基準、7　情報セキュリティ対策、(7)　情報機器又は記憶媒体の管理・処分という条項には明確に「情報が記録されたCD、DVD、HDD、フラッシュメモリ等媒体は適切に保管されなければならない。」とされている。

しかし「適切」という表現は、人によりその方法や程度にの認識が異なるため、ヒューマンエラーを招く要因となる。今回の事故を振り返った時、以下の点がサイバーセキュリティ対策上に留意すべき点である。

- 個人情報をUSBメモリに保存する必要はなかった。

  保存された個人情報は報道発表によると「当該教員が2009年に担当した2つの授業を受講した39 名分の学生の学籍番号、氏名、成績データ(のべ62件)」と記載されている。大学教員が海外に出張に行く場合は、その殆どが海外における現地調査や研究、共同研究者との打合せ、国際学会参加などと想定される。その際に6年前に自らが担当した学生の成績データは不要ではなかったと思われる。USBメモリの利用形態を考えた場合は過去のデータを削除、もしくは然るべき必要な保存場所にデータを移し替える必要があったはずだがそれを行わなかったと推測できる。従ってそれら必要な作業までセキュリティポリシー、もしくは実施マニュアルに記載しておく事が「規則」の観点で必要であった。

３．作業計画

不適切な作業計画に関する要因について調査する項目である。

大学教員がクチン市(マレーシア)に出張中に、USBメモリを持ち運んでいる事に関する安全対策やリスク評価が不十分であった。セキュリティポリシーもしくは、その実施マニュアルにおいて、USBメモリに個人情報を保存している場合の安全な持ち運び方法や利用方法を明記しておく必要があった。

４．教育訓練

知識技能に関する教育、訓練に関する要因について調査する項目である。

大阪市立大学情報セキュリティポリシーⅡ、情報セキュリティ対策基準、7　情報セキュリティ対策に「情報基盤センターを含む部局等ごとに、物理的、技術的な情報セキュリティ対策手順を具体的に定め、実施しなければならない。また、人的な情報セキュリティ対策として、本ポリシー対象者に教育、研修、啓発等を行い、情報セキュリティの重要性を理解させなければならない。」と定めている。

しかし実際に事故が発生している事実から次の２つの項目が事故の要因として考えられる

・本ポリシー対象者（今回は大学教員）に教育、研修、啓発等を行ったが、指導員、教材、教育環境などが十分ではなく「教える側」に問題があった。

・本ポリシー対象者（今回は大学教員）に教育、研修、啓発等を行ったが十分ではなく本人「教えられる側」のセキュリティ知識や意識が不足していた。

５．不正

管理者が関与する不正行為についての調査項目である。

管理者による不正行為の指示、黙認、隠蔽などは今回の事故と関係性が無い。

６．確認

確認手順が検討していない、もしくは確認体制が機能しないなどについて調査する項目である。

この項目は（公団）原子力安全技術センターに関連する作業において、その作業内容を何度も確認するような状況下においては必要な項目であるが、大阪市立大学の大学教員の海外主張時の作業において適用の必要性はない。

７．変更措置

計画変更が事故に与えた要因について調査する項目である。

今回の海外出張時に当初の業務計画と大きく異なる点があったとは大学からの報道発表には一切記載が無いことから要因分析が不可能である。しかし計画変更が事故に影響した可能性は低い。

８．組織要因・風土

組織の文化、考え方、風土などが事故の要因となっているか調査する項目である。

具体的にはルール違反が日常化していたり、安全性よりもコストが重視されていたり、問題が発生した場合に隠蔽したり、などの不正行為が組織の中で行われているかどうかなどを調査する必要があるが、大学からの報道発表には一切記載が無いことから要因分析が不可能である。しかし今回の情報漏洩事故においてそのような事が行われていた可能性は低い。

[Education: 職務遂行のために必要な 能力、意識を向上させるための対策]

１．知識教育

業務を遂行するために必要となる知識の向上を図るための対策の事である。具体的な対策例は以下のとおりである。

・大阪市立大学情報セキュリティポリシーⅡ、情報セキュリティ対策基準、7　情報セキュリティ対策の改定

・「情報基盤センターを含む部局等ごとに、物理的、技術的な情報セキュリティ対策手順」を準備

２．意識教育

セキュリティポリシーやセキュリティ対策手順を順守する。また事故があった際に事故報告書を適正に提出させるための対策は以下のとおりである。

・人的な情報セキュリティ対策として、本ポリシー対象者に教育、研修、啓発等を実施

・情報セキュリティ意識啓発（ネットワークセキュリティに関する意識啓発及び教育）については、情報基盤センター教員が担当し、部局等情報資産管理責任者に対しネットワーク利用に際しての情報セキュリティ確保の重要性、基本的に守るべきルール等につき周知徹底を図る。講演・リーフレット・ホームページ等各種媒体を通じて情報セキュリティ意識啓発を行う。

３．実技

業務の遂行に必要な技量の向上を図るための対策。

対策例としてはOJT（On the Job Trainning）や実地訓練となる。USBメモリの使用方法は実地訓練というよりも、２．知識教育を実施することで習得可能である。。

[Engineering：安全性を向上させるための設備、方法の技術的な対策]

１．設備機器の改善

事故・トラブルの要因となった設備機器上の要因を改善するための対策。

今回の場合は、万が一情報漏洩事故が発生した場合でも、USBメモリに含まれた個人情報にアクセス出来ないというフェールセーフの考え方も必要である。フェールセーフとはエラーによる被害の拡大を防いだり、エラー前の状態に回復できるようにするエラー対処である。代表的な考え方の1つである。これは、故障や事故などの異常時に安全側に作動する仕組みのことである.。

情報漏洩対策を徹底しているNTT東日本やNTT西日本などの企業では業務で使用するUSBメモリを会社が提供する指紋認証によるアクセス制限機能付きUSBメモリに限定[25]している。

万が一情報漏洩事故が発生した場合でも、USBメモリが指紋認証によるアクセス制限機能をが有しているため、実際に個人情報が搾取される可能性は極めて低くなる。その結果悪用される可能性も極めて低くなる。

次に設計の改善を行う事である。例えばクラウドサービス（従来は利用者が手元のコンピュータで利用していたデータやソフトウェアを、ネットワーク経由で、サービスとして利用者に提供するもの）の利用により実データを大学教員が保有するPCやUSBメモリに保管しないなど、技術的な代替手段を利用する。

２．工程の改善

事故・トラブルの要因となった取扱方法など、ソフト面の改善を図るための対策。

今回の情報漏洩事故においては製造方法の改善を行ったり、検査方法の改善を行ったり、取扱方法の改善を行ったりする必要性は無い。

３．基準の見直し

機器の安全装置、警報の発報レベル等に関する各種設定値を改善する対策。

この項目は（公団）原子力安全技術センターに関連する作業において必要な項目であるが、大阪市立大学の大学教員の海外主張時の作業において適用は不要だと考えられる。

[Enfrocement: 業務を確実に実施するための強化・徹底に関する対策]

１．規定化

業務内容を定型化し業務の簡素化、手順の明確化のための対策。

大阪市立大学は情報セキュリティポリシーとその手順を既に制定している。今回の情報漏洩事故を受け、それらを必要に応じて改定する。

２．評価・指導

業務内容を適正化するとともに、事故の要因となりやすい作業に対するセキュリティ意識の向上を図るための対策。

作業内容の評価、指導及び注意喚起を行う。またセキュリティ監査の実施も対策案として検討する。「情報セキュリティポリシーⅡ、情報セキュリティ対策基準、10　点検・評価及び見直し」には部局等による定期的な情報セキュリティ点検業務が明記されている。「部局等情報資産管理責任者は、当該部局における情報システム、情報機器及びネットワークに対して、情報セキュリティポリシー実施手順に基づいた必要な情報セキュリティ対策が実際に実施されているかどうか、また、情報セキュリティポリシー実施手順に記載された情報セキュリティ対策に不足がないかどうかについて、定期的に点検を行わなければならない。外部事業者に業務委託等を行う場合、部局等情報資産管理責任者は、本ポリシーの遵守について定期的に点検を行わなければならない。」としている。また点検結果に基づき、必要な改善を行わなければならないとしており、更には点検結果について、本ポリシーの記載に疑義が生じたときは、CISOに直ちに報告しなければならない。とも述べている。

３．危険予知活動

業務における箇所の抽出や、危険を未然に防ぐ対策を講じるための対策。

危険予知活動の徹底や、大学教員の体調確認などが該当するが、今回の情報漏洩事故にはあまり関連性が無い。

[Example:　具体的な事例を示す対策]

１．模範事例

情報漏洩事故における危険箇所を認識し、事故を未然に防止するための認識向上を図るための対策。

・参考となる情報漏洩事故事例を収集する。

２．水平展開

・共通性のあるトラブル等の情報を共有するための対策。

・データベースによる情報の共有を実施する。

［Environment： 物理的な作業環境を改善する対策］

１．作業環境の改善

業務に対する注意力を図るための対策。

照明、騒音、温度、湿度等、適した作業環境を整えるというものであるが今回の情報漏洩事故には該当しない。

4M 分析で抽出・分類した要因に対して、5E対策分類に従って対策を導き出した結果を表6-1に示す。

表6-1. 4M-5Eマトリックスの結果

		4M			
		Man 作業者の心身的な要因、作業能力的な要因	**Machine** 設備・機器・器具固有の要因	**Media** 物理的、人的な環境の要因	**Management** 組織における管理状態に起因する要因
	脆弱性の具体的な要因を記載する。	・海外出張中の準備で疲労が蓄積していた可能性や、その作業や時差の影響による睡眠不足の可能性は考えられる。 ・海外での安全管理や持ち出し可能な電子媒体であるUSBの安全な保管に対して知識が不足していた可能性が考えられる。	・一般的なUSBの場合はどのPCでも利用できるため個人情報が搾取される可能性が高くなる。	－	・大阪市立大学情報セキュリティポリシーが制定されているが運用レベルでは十分ではなかった。 例） ・個人情報をUSBメモリーに保存する必要はなかった ・USBメモリーに個人情報を保存している場合の安全な持ち運び方法や利用方法を計画しておく必要があった ・本ポリシー対象者（今回は大学教員）に教育、研修、啓発等を行ったが、指導員、教材、教育環境などが十分ではなく「教える側」に問題があった。 ・本ポリシー対象者（今回は大学教員）に教育、研修、啓発等を行ったが十分ではなく本人「教えられる側」のセキュリティ知識や意識が不足していた。
5E	Education 職務遂行のために必要な 能力、意識を向上させる ための対策	・知識教育 物理的、技術的な情報セキュリティ対策手順の徹底 ・意識教育 講演・リーフレット・ホームページ等各種媒体を通じて情報セキュリティ意識啓発を行う ・OJTによりセキュリティ教育を受ける	－	－	情報基盤センター教員が情報セキュリティ意識啓発を実施
	Engineering 技術、工学的な対策	－	－	・万が一情報漏洩事故が発生した場合でも、指紋認証によるアクセス制限機能付きUSBメモリを使用することにより中に含まれていたExcelファイルにアクセス出来ないようにする。 ・クラウドサービスの利用により実データを大学教員が保有するPCやUSBメモリに保管させなくする。	－
	Enforcement 強化、徹底による対策	－	－	－	・今回の情報漏洩事故を受け、情報セキュリティポリシーとその手順を改定する。 ・作業内容の評価、指導及び注意喚起を行う。またセキュリティ監査を実施する。
	Example 模範、事例による対策	－	－	－	模範事例を」作成し水平展開する。
	Environment **物理的な作業環境を改善する対策**	－	－	－	－

手法の有効性について

・4M-5Eのそれぞれの項目をマトリックスにすることにより、「Man（人間）、Machine（機械）、Media（媒体）、Management（管理）」に対して対策すべき5E 「 Education

（教 育）、Engineering（工学）、Enforcement（強化・徹底）、Example（模範・事例）、Environment（作業環境）」のそれぞれの項目が非常に明確となり、分析の際に漏れが非常に少なくなると想定できる。また視覚的に捉え易く関係者で情報漏洩事故情報を共有するのに便利である。

・エラーの要因が明確となり、その対策が適切に検討出来る。

<u>改善すべき点</u>

・4M-5Eは、世界各国の航空業界が採用する事故防止のための標準的な手法としてデファクトスタンダード(基準)となっているが、4M-5Eの項目を情報セキュリティ業界に適用するための改善が必要である。例えば5Eの1つであるEnvironmentという項目があるが、「照明、騒音、温度、湿度等、適した作業環境を整える」については工事現場など、作業現場においては事故の大きな要因となることが考えられるが、情報セキュリティに関する情報漏洩事故では、そのような要因が事故の原因となったケースについての報告が無いため、この項目について分析そのものが必要であるか不明瞭である。

（２）「Medical SAFER」の適用について

Medical SAFERの手順については村上（2010）、富樫（2009）、新原（2013）の手順を参照し、以下の手順1から手順7に添ってヒューマンエラー分析を進めた。結果を手順1から順に以下に示す。

手順1：事象の整理

発生した事象を整理し、何がどうして起こったかという事実を把握する。

３．２　適用実験で既にまとめた【事故報告書】を活用する。

手順2：問題点の抽出

事象を分析し問題点を抽出する。

・USBメモリを紛失したという問題点を抽出した。

手順3：背後要因の探索

問題が発生した背後にある要因を探す。そのためにUSBメモリを紛失したという問題点についての疑問を列挙した。

・USBメモリを持ち運んだ点は運用上問題ではなかったのか？

・情報セキュリティポリシーの内容は適切であったか？

・２つのエクセルファイルにはパスワードが設定されていたが、USBのメモリにはアクセス制限（指紋認証やパスワード）は必要ではなかったのか？

・過去の在籍学生の成績は大学教員の出張に必要であったか？

・大学教員はセキュリティ教育を受けていたか？

手順4：考えられる対策案の列挙

問題点やその背後要因から対策を考える。

USBメモリを紛失したという問題点についての対策案として検討した結果を以下に示す。

・USBメモリを持ち運んだ点は運用上問題ではなかったのか？という疑問については必ずしもUSBメモリを持ち出す必要はなく、PC内への保存やクラウドサービスの利用でも良かったと思われる。

・２つのエクセルファイルにはパスワードが設定されていたがUSBのメモリーにはアクセス制限（指紋認証やパスワード）は必要ではなかったのか？という疑問に

ついてはあった方が良かったと考えられる。理由は万が一USBメモリを紛失してもデータへのアクセス制限が可能であったからである。

・過去の在籍学生の成績は大学教員の出張に必要であったか？という疑問については不要であったと考えられる。大学教員が海外に出張に行く場合はその殆どが海外における現地調査や研究、共同研究者との打合せ、国際学会と容易に想定される。その際に6年前に自らが担当した学生の成績データが必要だったとは考え難いからである。

・大学教員はセキュリティ教育を受けていたかという疑問について、大学側は人的な情報セキュリティ対策として、本ポリシー対象者に教育、研修、啓発等を実施すること、情報セキュリティ意識啓発（ネットワークセキュリティに関する意識啓発及び教育）については、情報基盤センター教員が担当し、部局等情報資産管理責任者に対しネットワーク利用に際しての情報セキュリティ確保の重要性、基本的に守るべきルール等につき周知徹底を図ること、講演・リーフレット・ホームページ等各種媒体を通じて情報セキュリティ意識啓発を行うこと、について情報セキュリティポリシーの中で明記している為、セキュリティ教育を受けていたと考えられる。しかし、過去に担当した学生の個人情報が含まれるUSBメモリを持ち運んだ点やUSBメモリそのものに対してのアクセス制限が施されていなかった点などを考えると、セキュリティ教育を受けてはいるが、十分な知識や意識を持ち合わせているとは言い難い状態であった。

・情報セキュリティポリシーの内容は適切であったか？という疑問については上述したが、USBメモリの持ち運びに関する運用ルールとして、例えばUSBメモリそのものに指紋認証機能を具備させてアクセス制限を実施する、もしくはUSBメモリの持ち出し自体を禁止していたなどのルールは無かったのだろうかといった疑問が残るため、適切だったと断言出来るレベルでは無い。従って情報セキュリティポリシーの改定は必要な対策である。

手順5：実施する対策の決定

実行可能性を基に対策案を評価し、実施する対策を選択する。「Medical SAFER」は「Medical SAFER」の手順5においては「SHEL」の発展版であるMSHELの評価マトリックスが利用されることが多いため、今回はそれを活用した。m-SHELのm（management）（マネージメント）、L（liveware）（人間）、S（software）（ソフトウェア）、H（hardware）（ハードウェア）、E（environment）（環境）、L（liveware）（他の人間）に対してその対策を以下の観点で評価するものである。

・やめる（なくす）
・できないようにする
・わかりやすくする
・やりやすくする
・知覚能力を持たせる
・認知、予測させる
・安全を優先させる
・できる能力を持たせる
・自分で気づかせる
・検出する
・備える

解決策に対する評価を実施した。m-SHELモデルの6項目と「エラー対策の思考手順」の11項目を掛け合わせた全66項目に対して対策の有無を確認することで情報漏洩対策の網羅性を検証した結果を表6-2にまとめた。

表6-2　Medical SAFERマトリックスの結果

		情報セキュリティ対策の思考手順										
		やめる（なくす）	できないようにする	わかりやすくする	やりやすくする	知覚能力を持たせる	認知、予測させる	安全を優先させる	できる能力を持たせる	自分で気づかせる	検出する	備える
MSHEL	m（management）（マネージメント）	・USBメモリの使用をやめさせる ・過去の在籍学生の成績をUSBメモリに保存させない								・セキュリティ教育、研修、勉強等を実施する。		・USBメモリーにアクセス制限（指紋認証やパスワード）を設ける ・情報セキュリティポリシーを改定する
	L（liveware）（人間）	・USBメモリの使用をやめる ・過去の在籍学生の成績をUSBメモリに保存しない								・セキュリティ教育、研修、勉強等を受講する。		USBメモリーにアクセス制限（指紋認証やパスワード）を設ける
	S（software）（ソフトウェア）	・USBメモリの使用をやめてクラウドサービスを利用する。										
	H（hardware）（ハードウェア）							USBメモリーにアクセス制限（指紋認証やパスワード）を設ける				
	E（environment）（環境）											
	L(liveware) (他の人間)									・セキュリティ教育、研修、勉強等を受講する。		・USBメモリ紛失に関する個人情報漏洩事故について関連者に共有 ・USBメモリーにアクセス制限（指紋認証やパスワード）を設ける事を関連者に共有

・「USBメモリを持ち出す必要はなく、PC内への保存やクラウドサービスの利用でも良かったと思われる」という解決策についてはm（management）（マネージメント）とL（liveware）（人間)との観点からは「やめる」という評価とした。

H（hardware）（ハードウェア）の観点からも同様に「やめる」という評価となり、代替案としてクラウドサービスの利用を検討するという評価とした。

L（liveware）（他の人間）についてはUSBメモリ紛失に関する個人情報漏洩事故について関連者に共有する必要が有るため「備える」という評価にした。

他の観点であるS（software）（ソフトウェア）、E（environment）（環境）については該当無しという評価とした。

・USBメモリにアクセス制限（指紋認証やパスワード）を設けるについては、m（management））（マネージメント）とL（liveware）（人間）との観点からは万が一情報漏洩事故が発生した場合を想定しての対策であることから「備える」という評価とした。

H（hardware）（ハードウェア）の観点からは新たな機能具備させることから利用方法が煩雑となるため煩わしい面もあるが「安全を優先させる」という評価の観点で必要とした。

他の観点であるS（software）（ソフトウェア）、E（environment）（環境）については該当無しという評価とした。

・過去の在籍学生の成績をUSBメモリに保存しないという対策についてはm（management）（マネージメント）、L（liveware）（人間）の観点から「やめる」という評価とした。
L（liveware）（他の人間）の観点は該当無しという評価とした。
L（liveware）（他の人間）についてはUSBメモリに過去の在籍学生の成績等の不必要な情報を保存しない点について関連者に共有する必要が有るため「備える」という評価にした。
S（software）（ソフトウェア）、E（environment）（環境）については該当無しという評価とした。

・大学側は人的な情報セキュリティ対策として、本ポリシー対象者に教育、研修、啓発等を実施することと、情報セキュリティ意識啓発（ネットワークセキュリティに関する意識啓発及び教育）を実施する対策についてm（management）（マネージメント）、L（liveware）（人間）、L（liveware）（他の人間）の観点から「自分で気付かせる」という評価とした。教育、研修、啓発等を受講することにより、必要な知識や意識を自ら習得し、気づく必要があるためである。
S（software）（ソフトウェア）、E（environment）（環境）については該当無しという評価とする。
・情報セキュリティポリシーの改定
m（management）の観点から「備える」という評価とした。
その他のL（liveware）（人間）、L（liveware）（他の人間）、（software）（ソフトウェア）、E（environment）（環境）については該当無しという評価とした。

手順6：対策の実施

誰が、いつまでに、どのように実施するか決め、的確に実施されたか確認する。タスクリストなどを作成し管理するのが望ましい。

手順7：実施した対策の効果の評価

実施した対策に効果があったのか、あるいは新たな問題点はないかなどを評価する。

具体的な方法として頻繁に発生する事故の場合は事故発生数の推移等を確認する、組織の社員や関連者へのアンケートを実施する、またセキュリティ監査などを活用してその効果を図るなどが挙げられる。

また1ヶ月後、3ヶ月後、6ヶ月後など定期的に期間を決めて継続実施することにより、改善策が適切に実施されているか、期待された効果が得られたか、新たに別の問題が発生していないか、などが明確となり、より一層の効果が得られる。

手法の有効性

「Medical SAFER」は医療分野で広く利用されており、サイバーセキュリティとは全く別分野で利用されているツールではあるが、m-SHEL モデルの6項目と「エラー対策の思考手順」の11項目を掛け合わせた全66項目に対して対策の有無を確認することで、情報漏洩対策の網羅性を検証出来き、また対策などについては非常に有効な結果が得られたと考える。

改善すべき点

m-SHEL モデルの 6項目の中で、S（software）（ソフトウェア）、E（environment）（環境）の2項目については今回のヒューマンエラー分析において該当が無かった。

分析項目が66項目と多く、網羅性が高い反面、効率化の観点で考えた場合に全ての分析項目が必要かどうかについては今後他の事故などに適用する過程で確かめる必要がある。

もしくは情報セキュリティ向けに修正する必要がある。従って「Medical SAFER」は医療分野で広く利用されているものであり、情報セキュリティ分野に活用できるが適用レベルに至るにはまだ改善の余地があると考えた。

また「エラー対策の思考手順」の11項目については例えば「やめる」と「できないようにする」という感覚的な言葉による判断のため、言葉の境界線が不明瞭であり、どの項目に対策案を記載すれば良いか表6-2を作成する過程で非常に困難であった。各人の主観に判断を委ねていると捉えることも出来るため、その精度については別の事故を活用し、検証する必要がある。

更には「分析の手順4：考えられる対策案の列挙」と「手順5：実施する対策の決定」の手順の順番についても作業過程で効率的とは考え難いものであった。手順3：背後要因の探索で問題が発生した背後にある要因を探し、結果として「USBメモリを紛失」したという問題について手順4：考えられる対策案の列挙をした。この作業過程では「USBメモリを紛失」したという事実に対して考えられる対策を挙げる必要がある。実際に以下の対策案を列挙した。

・USBメモリの使用をやめる

・過去の在籍学生の成績をUSBメモリに保存しない

・USBメモリの使用をやめてクラウドサービスを利用する

・USBメモリにアクセス制限（指紋認証やパスワード）を設ける

・セキュリティ教育、研修、啓発等を実施し、対象者は受講する

・USBメモリ紛失に関する個人情報漏洩事故について関連者に共有する

上記対策案の中で、例えば「USBメモリにアクセス制限（指紋認証やパスワード）を設ける」などについてはある程度情報セキュリティやITの知識が必要とされる。

村上（2010）は「「Medical SAFER」は分析に関する特殊な知識も不要であるため、現場の事故関係者が利用することで、より有効な分析が行えるのではないかと考える。」としているが、解決策の立案部分については担当者のスキルレベルにより、対策案の数や精度にバラつきが予想される。すなわち、その対策案に関して、m-SHELモデルの6項目と「エラー対策の思考手順」の11項目を掛け合わせた全66項目に対して対策の有無を確認することで、情報漏洩対策の網羅性を検証する為、対策案で列挙することが担当者のスキル不足により出来なかった対策案については網羅することが出来ないという問題が残る。

（３）VTA（Variation Tree Analysis）バリエーションツリー分析の適用について

富樫（2009）や危険物保安技術協会（2010）に記載された具体的な調査手法を参考に以下の手順に添って作業を進めた。

①事故に関与した当事者、関係者、関連事象などを「軸」として設定する

当事者は大学教員、大学関係者、学生（卒業生）、クチン市(マレーシア)現地警察、関連物としてUSBメモリ（エクセルファイル（2 個）※パスワード保護有り、に記載された当該教員が2009年に担当した2つの授業を受講した39 名分の学生の学籍番号、氏名、 成績データ（のべ 62 件））

②左端に時間軸を定め、時間の経過は下から上に進む

事実経過

(1) 2015年1月27日(火)午後9時30分ごろ［現地時間］理学研究科准教授（男性45 歳）がクチン市（マレーシア）にて、公園内を通行。ズボンのポケットに布製ポーチを入れていた。

(2) 同日午後9時45分ごろ ズボンのポケットに入れていたはずのポーチが無くなっていることに気づく。付近を捜すとともに、地元警察に遺失届を提出。

(3) 2015年1月29日（木）日本領事事務所で帰国のための渡航書を受理。

(4) 2015年年2月4日（水）午前8時30分 帰国

(5) 2015年年2月5日（木）大阪市立大学から在籍学生に口頭と文書で謝罪

(6) 2015年年2月5日（木）大阪市立大学から卒業生に説明及び謝罪の文書を送付

(7) 2015年年2月6日（金）大阪市立大学HPにて学長名で本件のお詫びを掲載

(8) 2015年年2月9日（月） 部局長等連絡会において、理事長より全学部・研究科長に対して、注意喚起を行い、個人情報の適正管理及び記憶媒体の持ち出しの際に内容確認を厳重に行うことを強く命じ、徹底することを指示

③変動要因や通常作業を四角枠で囲って示す（変動要因は太い枠にする）

④全般に影響していたと見られる要素は「前提条件」として、図の最下部に記述する。
本項目は特に記載事項無し。

⑤ノードは簡潔な言葉で表現し、説明が必要な場合には図の右脇に説明欄を設け、ノードに付けた番号の補足説明を記す。

⑥各ノードの関連（連鎖）を直線矢印で結ぶ。

⑦事故の直接的あるいは間接的な要因と考えられるものを「排除ノード」として点線枠とする。

⑧ノードの連鎖を断ち切ることによって事故を未然に防止できたと判断される個所（ブレーク）に水平線破線を引く。このようにして作成されたVTAを用いて排除ノードの裏側にあるヒューマンファクターを解析し、それに対する多重の再発防止策を検討する。

VTA手法による事故分析をまとめたフローチャートを図6-1に示す。

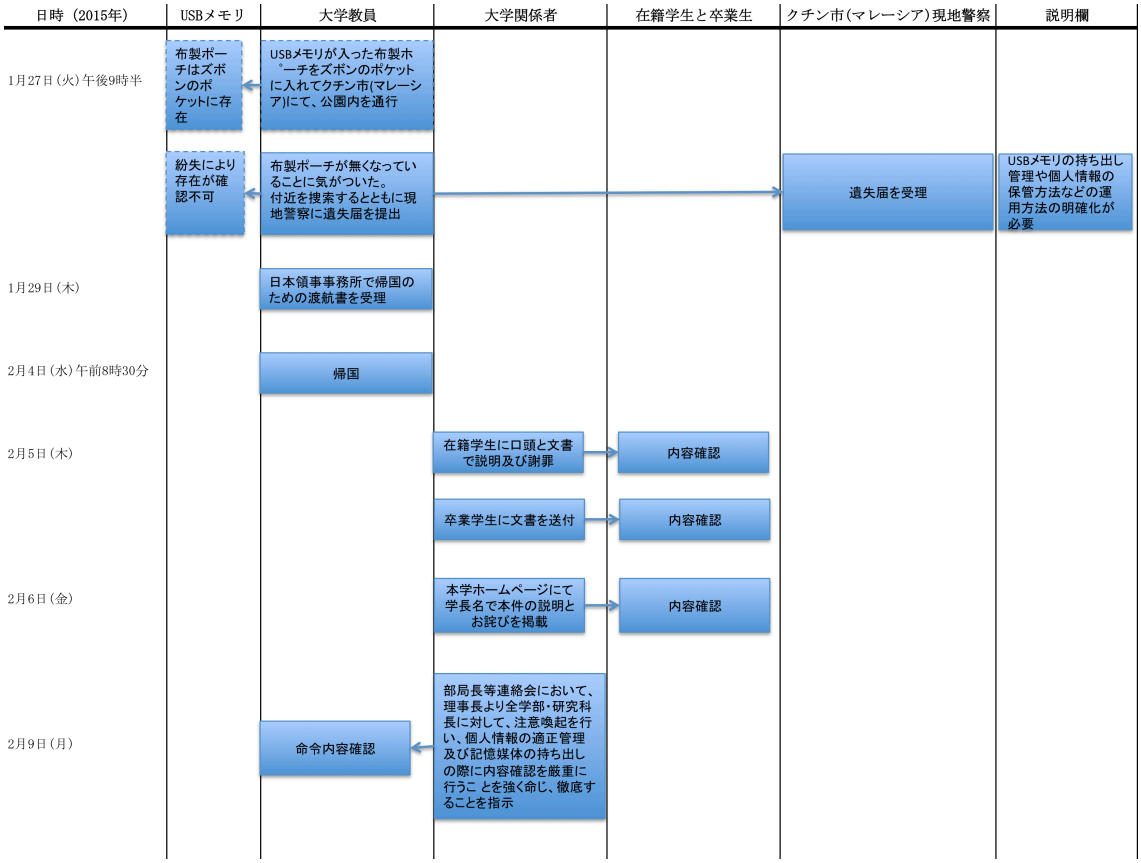

図6-1　VTA手法による事故分析をまとめたフローチャート（出所：筆者作成）

チャート中に情報漏洩事故が起こる要因となった部分を点線で囲んでいる。これを起点として情報漏洩事故につながる要因が全体的に把握でき、USBメモリと人や組織のかかわりが浮き彫りとなることにより、事故を未然に防ぐ対策を立案する。

点線で囲んだのは「USBメモリが入った布製ポーチをズボンのポケットに入れてクチン市(マレーシア)にて、公園内を通行中に、布製ポーチが無くなっていることに気がついた。」という項目である。布製ポーチがポケットから紛失しなければ事故が発生していなかったという結果から考えられる対策として以下の点をあげる。

・布製ポーチではなくチェーン付きの袋に入れる

・USBメモリを持ち歩かない

・USBメモリを暗号化するなどの追加機能を具備する

・USBメモリの使用に関するセキュリティポリシーの確認と必要に応じた改定を行う。

手法の有効性

時系列で事象をまとめるため、誰が何を行ったかなどの整理が可能である。情報漏洩事故の関連者や関連物が明確になり、責任者や当事者がフローチャートで目視化できる点は非常に有効なツールとして考えられる。

改善すべき点

情報漏洩事故の関係者や、情報漏洩事故が起こる要因となった部分を点線で囲むことにより、それらの関連性が明確には出来たが、その背後要因関連を明確にするのが困難である。具体的には、4M-5Eで説明したような「Man（人間）、Machine（機械）、Media（媒体）、Management（管理）」に対して対策すべき5E 「 Education（教育）、Engineering（工学）、Enforcement（強化・徹底）、Example（模範・事例）、Environment（作業環境）」が明確になっていないため具体的に詳細な原因分析やその分析に基づいた対策が導き難い点が改善点である。

また対策案の立案が考案者のスキルに依存する為、対策案にバラつきが生じる。今回はUSBメモリに起因した情報漏洩であったため、その分野に詳しいコンサルタントなどであれば過去の経験から容易に対策案を思いつくかもしれないが、そうで無い場合は、USBメモリから想像した表面的な対策案しか思いつかない可能性が高い。

３．３　最適な分析手法の選択

「4M-5E」、「Medical SAFER」、「VTA」、を実際の事故（大阪市立大学教員のUSBメモリ紛失による個人情報の漏洩事故）に適用し、手法の有効性を比較検討した結果を表6-3に示し、検討結果の詳細を以下で述べる。

表6-3　「4M-5E」、「Medical SAFER」、「VTA」手法の有効性比較表

	4M-5E	VTA	Medical

			SAFER
事象の整理の容易性	△	○	△
問題点の抽出の容易性	○	×	△
背後要因の探索の容易性	○	×	△
考えられる対策立案の容易性	○	×	△
分析者間の結果のバラつきの少なさ	○	△	△
実施する対策を決定する容易性	○	△	△
実施した対策の効果を評価する容易性	○	△	○

○要件を満たしており他の分析方法よりも優れている　△要件を満たす　×要件を満たさない

（1）事象の整理の容易性

どの手法も事故報告書のような事象を説明する工程があるため、事象の整理は同等に実施可能である。従って最低限の要件を満たしていると言えよう。

特にVTAはフローチャートにより、関連者や関連物が視覚化され、事故におけるそれぞれの相関関係の認識が容易となる点が他の分析手法よりも優れている。

（2）問題点の抽出の容易性

VTAのようにフローチャートで時系列に事象を整理する場合は、ヒューマンエラーの発生理由が分かり難いため、次工程における要因の探索が困難となる。

Medical SAFERは、事故報告書に基づき問題点を抽出するため、この時点での作業に作業者のスキルによるバラつきが見られる。スキルの高い人は経験に基づき多くの問題点を発見出来るが、スキルの低い人はあまり多くの問題点を発見出来ない。

4M-5Eについてはそれぞれの項目に基づき理路整然と問題点を抽出できるため他の手法と比較して優れている。

（3）背後要因の探索の容易性

VTAは前項で述べたとおり、ヒューマンエラーの発生理由が分かり難いため、そのヒューマンエラーの背後に隠れている背後要因を探索することは容易ではない。

Medical SAFERは問題点を全て網羅して列挙出来た場合は背後要因の探索を実施出来るが前述のとおりスキルの低い人があまり多くの問題点を発見出来なかった場合は関連して背後要因の探索は容易ではない。

4M-5Eについては項目毎に問題点を抽出できるため、項目毎にその背後要因の探索が容易に実施出来た。従って他の手法と比較して優れている。

（4）考えられる対策立案の容易性

それぞれの手法は前工程が後工程に影響を及ぼす。

VTAは前項で述べたとおりヒューマンエラーの発生理由が分かり難いため、その背後要因の探索が容易では無いことから、問題の本質を見抜くことが困難である。従って、問題に対する対策案の立案も容易ではない。

Medical SAFERは、問題点を全て網羅して列挙出来た場合は背後要因の探索を実行出来るため、対策立案が実行できる。前述のとおりスキルの低い人があまり多くの問題点を発見出来なかった場合は、関連して背後要因の探索は容易ではないため結果として対策立案は容易に実行出来ない。

4M-5Eについては項目毎に問題点を抽出できるため、そ項目毎にその背後要因の探索が容易に出来た。従って、結果として対策案が容易に導き出され、他の手法と比較して優れている。

（5）分析者間の結果のバラつきの少なさ

VTAは、フローチャートに時系列ごとの事象を記載していく手法であるため事故報告書に漏れが無いという前提の場合は関連者、関連物の記載漏れが無くなる。しかし対策案立案の場面では担当者のスキルにより対策案の数や質にバラつきが発生する。

Medical SAFERは問題点を全て網羅して列挙出来た場合は背後要因の探索を実行出来るため、対策立案が実行できる。前述のとおりスキルの低い人があまり多くの問題点を発見出来なかった場合は関連して背後要因の探索は容易ではないため結果として対策立案は容易に実行出来ない。

4M-5Eについてはそれぞれの項目に基づき理路整然と問題点を抽出できるため、それぞれの項目毎にその背後要因の探索も容易に実施出来る。従って分析者のスキルに依存しない結果が得られるため他の手法と比較して客観性が保たれる。

（6）実施する対策の決定の容易性

実施する対策は以下の基準で選定される。

・効果：対策によるエラー防止の効果

・即効性：対策実施後に効果が現れる早さ

・費用：対策にかかる費用

・労力：対策を実施するにあたって必要な人材確保

VTAは、前項で述べたとおり問題に対する対策案の立案も容易ではない。従って対策案の効果、即効性などが十分に得られない可能性がある。

Medical SAFERは、スキルの低い人があまり多くの問題点を発見出来なかった場合は関連して背後要因の探索は容易ではないため、結果として対策立案は容易に実行出来ない。従って即効性などが十分に得られない可能性がある。

4M-5Eについては項目毎に問題点を抽出できるため、項目毎にその背後要因の探索が容易に実施出来る。結果として対策案が容易に導き出されることから対策実施の効果、即効性が十分期待出来る。

（７）実施した対策の効果の評価の容易性

VTAは、分析基準となる項目を有していないため、実施した対策の効果を図ることは困難である。

「Medical SAFER」は、m-SHEL モデルの6項目と「エラー対策の思考手順」の11項目を掛け合わせた全66項目に対して対策の効果を網羅的に確認出来るため実施した対策の効果を図ることは容易である。

4M-5Eのそれぞれ「Man（人間）、Machine（機械）」、Media（媒体）、Management（管理）」に対して対策すべき5E 「 Education（教 育）、Engineering（工学）、Enforcement（強化・徹底）、Example（模範・事例）、Environment（作業環境）」が非常に明確となっているため対策の効果をそれぞれの項目毎に確認出来るため実施した対策の効果を図ることは容易である。

以上の比較検討より、ヒューマンエラー分析に4M-5Eが最適であるという結果を得られた。加えてVTAはフローチャートにより、関連者や関連物が時系列で視覚化される点、事故報告書と併用し、事故の事実関係を明確にする資料として利用すれば更に分析効果があがると考えた。

第７章　4M-5EとVTAを組み合わせたヒューマンエラー分析手法のマイナンバー漏洩事故への適用実験

１　マイナンバー漏洩事件

2015年10月からマイナンバーの全住民への通知が開始された。通知以前よりマイナンバー制度に便乗した不審電話が発生しており、2015年10月28日に独立行政法人国民生活センターより注意喚起[26]が出された。相談事例では怪しい者から電話がかかってきたというケースが報告されている。例えば、「行政機関を名乗りマイナンバー制度の手続きで至急に振込先の口座番号を教えてほしい。」、「マイナンバー制度の導入に伴い個人情報を調査中である。」、「知らない業者からマイナンバーを管理します。」などと言った内容である。

また別の事例としては「マイナンバー占い」[27]と呼ばれるという危険な占いサイトや占いアプリが出来ているとネット上で話題になっている。自分のマイナンバーと生年月日などを入力することにより、自分の未来などが占えるもののようであるが遊び半分で入力する人がいてもおかしくない。

法律上、マイナンバーを法律で定められたこと以外に使用すること自体が法律違反であり、例え本人の同意があったとしても、占いという本来マイナンバー制度で利用すべき目的と異なる内容で他人のマイナンバーを聞くことは犯罪であるが現実に全て防止できないのが現状である。このように技術的な実現難易度は低いがアイデアレベルで人を騙してマイナンバーを搾取する事故も今後多発すると考えられる

自治体職員やマイナンバー業務委託業者によるヒューマンエラーも既に発生している。

2015年10月5日から10月9日にかけて茨城県鳥取市[28]において、マイナンバーを記載した住民票を誤って69名に交付した事故が発生した。市内２箇所に設置された自動交付機で発行された住民票にマイナンバーを誤記載しており、10月9日14時頃に市民より指摘を受け問題が発覚した。取手市によると自動交付機の運営をしている同市が業務委託した茨城計算センターの設定ミスで本来マイナンバーを記載しないように設定すべきところを設定が

漏れていた事により事故が発生したとしている。職員が対象者へ訪問し、謝罪しているのに加えて茨城計算センターにより設定が修正された。

2015年10月6日、札幌市厚別区役所において60代の女性が「住民票コード」を記載した本人と夫の住民票の発行を請求した際に職員が端末の操作を誤ってマイナンバーを記載した住民票を交付した事故が発生した[29]。同区役所では市の担当職員約200名に対して、住民からの請求がないに場合に誤ってマイナンバーを記載した住民票を交付しないよう、注意を呼びかけた。また住民票の交付システムの改修も検討している。

2015年10月26日、横浜鶴見区では職員がマイナンバーと個人情報を転載した転出証明書を申請者とは別の住民に誤って交付した事故が発生した。横浜市の報告によると同日16時頃に戸籍課において転出証明書を交付した際に申請者とは別人に誤って交付した。後ほど申請者が転出証明書を受け取っていないと深刻が有り事故が発覚した。転出証明書にはマイナンバー、１世帯３名の氏名、生年月日、性別、本籍、住民票コードが記載されていた。同日18時過ぎには誤って配布した転出証明書を回収し、正規な証明書を交付した。同市によると証明書交付時の確認が不十分だったとして内容確認の徹底により再発防止を目指すとしている。8

２　4M-5EとVTAを組み合わせたヒューマンエラー分析の適用実験

前章の結果より、ヒューマンエラー分析に4M-5Eが最適であり、更にVTAを併用し、事故の事実関係を明確にする資料として利用すれば分析効果があがることが明らかなった。

この新たな手法を、実際に既に発生しているマイナンバー漏洩事故に適用し、情報漏洩事故原因の大きな要因を占めると予想されるヒューマンエラーの防止に有用であるかどうかの事実験を行うこととした。

以下の手順に添ってヒューマンエラー分析の適用実験を行った。

手順1：事故報告書を作成
手順2：VTAのフローチャートにより、関連者や関連物を時系列時系列で整理

手順3：4M-5Eの適用

手順1：事故報告書を作成

茨城県取手市の公式HP上に記載された事故報告内容に内容に基づき事故報告を作成した。結果を以下事故報告書に記す。

手順1：事故報告書を作成

【事故報告書】

タイトル：茨城県取手市における個人番号（マイナンバー）を誤記載した住民票交付

施設名：茨城県取手市

発生日時：2015年10月5日（月曜日）から9日（金曜日）

発生状況：自動交付機で発行された住民票に、個人番号が記載された住民票を69世帯、100名に交付

発生場所：取手本庁舎及び藤代庁舎の自動交付機

発生設備及び機器：自動交付機

事故の原因：取手市の電算業務委託業者である茨城計算センターが自動交付機発行システムを設定する作業で、個人番号を記載しないこととする設定を怠ったため、今回の事件が発生した。

結果／影響：個人番号が記載された住民票を69世帯、100名に交付

法律区分：個人情報、プライバシー

[状況]

10月5日（月曜日）から9日（金曜日）まで、市内2か所にある自動交付機で発行された住民票に、個人番号が記載された住民票を69世帯、100名に誤って交付した。10月9日（金曜日）午後2時ごろ、市民から取手本庁舎の自動交付機で10月8日(木曜日)交付を受けた住民票に個人番号が記載されているとの連絡を受けた。本来自動交付機による発行では、個人番号を記載しない仕様としていたが、確認したところ住民票に個人番号が記載されていることが判明した。

今後の対応

自動交付機への対応

10月9日(金曜日)午後2時過ぎ、取手本庁舎及び藤代庁舎の自動交付機を停止した。茨城計算センターに自動交付機の設定を行うよう指示し、午後2時30分ごろに復旧した。 現在、自動交付機で交付されている住民票には、個人番号の記載はない。

個人番号が記載された住民票を交付した市民への対応

10月10日(土曜日)から12日(月曜日)にかけて市民課職員が対象者宅へ訪問し、謝罪を行った。対象者には新たな住民票を準備し差し替えを依頼した。

(1) 10月3日(土曜日)
電算業務委託業者である茨城計算センターが設定作業を実施

(2) 10月5日（月曜日）から9日（金曜日）まで
市内2か所にある自動交付機で発行された住民票に、個人番号が記載された状態で69世帯、100名に交付

(3) 10月9日（金曜日）午後2時ごろ
市民から取手本庁舎の自動交付機で10月8日(木曜日)交付を受けた住民票に個人番号が記載されているとの連絡を受けた。

(4) 10月9日(金曜日)午後2時過ぎ
取手本庁舎及び藤代庁舎の自動交付機を停止した。茨城計算センターに自動交付機の設定を行うよう指示し、午後2時30分ごろに復旧した。

(5) 10月10日(土曜日)から12日(月曜日)にかけて
市民課職員が対象者宅へ訪問し、謝罪した。対象者に新たな住民票を準備し差し替えを依頼した。

[紛失した個人情報]　特に無し

[原因]　茨城計算センターが設定作業の設定ミス

[対策]

・茨城計算センターによる自動交付機の設定変更

・市民課職員が対象者宅へ訪問し、謝罪を実施。

・新たな住民票を配布

［影響/被害］

本件に関し、情報流失等の被害報告は無し。

手順2：VTAのフローチャートにより、関連者や関連物を時系列時系列で整理

VTAのフローチャートにより、関連者や関連物を時系列で整理した結果を図7-1で示した。

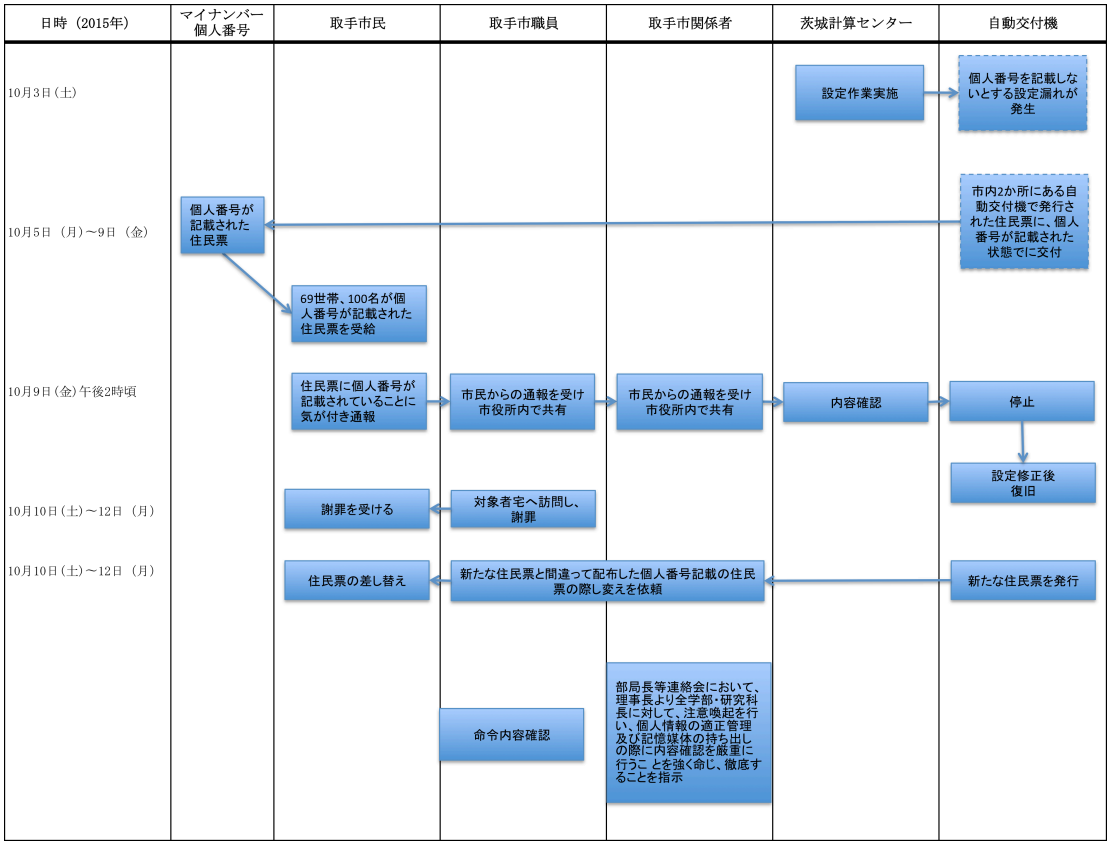

図7-1　VTAフローチャート結果　（出所：筆者作成）

関連者として「取手市民」「取手市職員」「取手市関係者」「茨城計算センター」、関連物して「マイナンバー（個人番号）」「自動交付機」を挙げた。茨城計算センター社員による設定ミスが発生してから、それらの関係性について時系列で整理した。

手順3：4M-5Eの適用

以下の4M-5Eの手順に添って分析を進めた。

[Man：作業者の心身的な要因、作業能力的な要因]

１．身体的要因

取手市職員と茨城計算センター社員の身体的な要因は、取手市からの報道発表には一切記載が無いことから要因分析が不可能である。

しかし「個人番号制度開始前の10月3日（土曜日）に、住民基本台帳システム及び自動交付機について、10月5日（月曜日）からスタートできるよう市の電算業務委託業者である茨城計算センターが設定作業を行いました。」と取手市のHPに掲載されているとおり、作業が直前の週末に実施されていることから、疲労や精神的な焦りなどがあった可能性がある。

２．心理生理的要因

取手市職員と茨城計算センター社員の思い込み、推測などの主観的な要因と過度の緊張、焦り等の心理的なストレスの他、病気、睡眠不足等の生理的なストレスなどの要因は取手市からの報道発表には一切記載が無いことから要因分析が不可能である。

しかし「個人番号制度開始前の10月3日(土曜日)に、住民基本台帳システム及び自動交付機について、10月5日(月曜日)からスタートできるよう市の電算業務委託業者である茨城計算センターが設定作業を行いました。」と取手市のHPに掲載されているとおり、作業が直前の週末に実施されていることから、心理生理的な要因があった可能性がある。

３．技量

取手市職員と茨城計算センター社員は、住民基本台帳システム及び自動交付機について、10月5日(月曜日)からスタートした業務を行っていた。従って作業を行う上で十分な技能が無かったり、作業に不慣れであったりした可能性がある。

４．知識

取手市職員と茨城計算センター社員は、住民基本台帳システム及び自動交付機について、10月5日(月曜日)からスタートした業務を行っていた。従って新たな業務に対する知識の不足、誤った理解等が事故の要因になっている可能性がある。

５．不正

取手市職員と茨城計算センター社員は、取手市民から住民票に個人番号が記載されていることに気が付き通報をした事に対して対応を行っている点や、今回の作業ミスにより彼らに金銭面等、何らメリットが無い点を考えた場合に、この項目は情報漏洩事故との関連性は無い。

６．作業実施

茨城計算センター社員による設定作業の中で「個人番号を記載しないとする設定漏れが発生」と報告があることから、作業実施のタイミング、作業対象、作業順序、整理整頓の実施などが事故の要因になっている可能性がある。

[Machine：設備・機器・器具固有の要因]

１．機器

取手市の発表では「自動交付機発行システムを設定する作業で、個人番号を記載しないこととする設定を怠った」とあることから自動交付機の故障や動作不良など、機器固有の問題は情報漏洩事故の要因ではない。

２．設計・機能

取手市の発表では「自動交付機発行システムを設定する作業で、個人番号を記載しないこととする設定を怠った」とあることから、設計上は問題が無いかもしれないが、事前に設計でマイナンバーを住民票に印字しないようにすれば情報漏洩時の発生を回避出来た可能性がある。

３．品質

取手市の発表では「自動交付機発行システムを設定する作業で、個人番号を記載しないこととする設定を怠った」とあることから設備や機器が老朽化しているなどの機器の固有の問題が事故の要因となっている可能性は低い。

４．物理的・化学的挙動

設備や機器の作業の結果生じた現象により事故に影響を与えた要因は特に無い。

[Media：作業者（取手市職員と茨城計算センター社員）に影響を与えた物理的、人的な環境の要因]

１．作業環境

今回の情報漏洩事故について、取手市からの報道発表には取手市職員と茨城計算センター社員に影響を与えた人工的な環境と自然環境についての記述が一切無かったことから、特殊な環境下に取手市職員と茨城計算センター社員が置かれていた可能性は低い。

２．コミュニケーション

取手市民、取手市職員、取手市関係者、茨城計算センター社員への情報伝達の不足に起因する要因や、必要な情報伝達方法がありながらも十分に機能していないなどの要因が情報漏洩事故の原因となっていないかという点については取手市民から、住民票に個人番号が記載されていることに気が付き通報した時点から、取手市役所を経由して茨城計算センターに伝達され、自動交付機が一時停止され、設定終了後に復旧するまで30分程度の短い時間で実施されていることから可能性は低い。

３．作業条件

取手市職員と茨城計算センター社員は、住民基本台帳システム及び自動交付機について、10月5日(月曜日)からスタートした業務を行った。従って人員不足のため勤務体制が不十分であった可能性がある。またサービス開始直前であったため、残業などを実施していたなど勤務条件が不適当であった可能性がある。

４．職場状況

人間関係や職場の慣習、組織風土などに関する要因について調査する項目である。

大学教員は情報漏洩事故発生当時に業務に関する作業を行っていなかったことから人間関係や職場の慣習、組織風土などは事故とは何ら関連は無い。

[Management：組織における管理状態に起因する要因]

１．組織

組織の管理、運営に関する要因について調査する項目である。予算や経営方針、責任体制の要因を含む。

茨城県取手市では「取手市地域情報化計画[30]」に基づき2003年に情報セキュリティポリシーを策定しており、市長をトップした管理体制下、市民に信頼されるセキュアな情報化の推進を進めている。

また事故の要因となった自動交付機の設定作業を業務委託された茨城計算センターについても、その公式HPのトップページ[31]において茨城計算センターは行政情報システムを手がける会社であり、個人情報と行政情報を取り扱う会社として、情報セキュリティに対する責任体制を徹底している。更には、ISIM（情報セキュリティマネジメントシステム）に基づき、個人情報、行政情報の管理・保管において徹底したセキュリティ対策を確立していると述べており、主たる業務に関する情報セキュリティの重要性を会社として認識し、その体制やセキュリティ管理の徹底を図っている。

以上より取手市と茨城計算センターは、予算、個人情報を取り扱う方向性、責任者及び責任体制は整備されており、今回の事故にその要因は影響していない。むしろ完備された体制やドキュメントの問題ではなく、実運用レベルの手順の中で起きた事故である可能性が高いと考えられる。

２．規則

前述のとおり茨城県取手市では「取手市地域情報化計画」[30]に基づき2003年に情報セキュリティポリシーを策定しており、運用面も考慮したうえで「情報セキュリティーポリシ

一実施手順 」も準備していることから規則に関するドキュメント整理とドキュメントに応じた手順の準備は今回の事故に影響した可能性は低い。

茨城計算センターについてもISMSによる運用を徹底しており規則類の不備は今回の事故に影響した可能性は低い。

３．作業計画

不適切な作業計画に関する要因について調査する項目である。今回の情報漏洩事故は事故報告書とVTAとで整理したとおり取手市の電算業務委託業者である茨城計算センターによる自動交付機の設定作業で起きた設定誤りが事故の原因である。従って以下の観点で作業計画において何らかの不備があったと考えられる。

・工程など作業スケジュールが不適切

・作業計画が不十分

・作業内容に不備があった。

・管理者による作業内容と計画のレビューが不十分

・作業時のリスク評価と対策が不十分

・マイナンバー漏洩のリスクの可能性チェックが不十分

４．教育訓練

茨城県取手市では定期的な情報セキュリティ研修の実施や、関連したeラーニング研修の受講を行っており、情報セキュリティ研修の不備が今回の事故に影響した可能性は低い。

茨城計算センターについてもISMSによる運用を徹底しており、教育訓練の不備は今回の事故に影響した可能性は低い。

しかし今回は事故が実際に発生しており、取手市と茨城計算センターともに次の2項目について実施が出来ていなかった可能性がある。

・教育、研修、啓発等を行ったが、指導員、教材、教育環境などが十分ではなく「教える側」に問題があった。特にその教育訓練内容にマイナンバー交付に関連した今まで経験していない新たな業務内容が発生しており、細かな現場レベルの作業項目まで教育内容に整備されてなかった。

・教育、研修、啓発等を行ったが本人「教えられる側」のセキュリティ知識や意識が不足していた。特にその教育訓練内容にマイナンバー交付に関連した今まで経験していない新たな業務内容が発生しており、細かな現場レベルの作業項目まで意識して習得することが出来なかった。

５．不正

管理者が関与する不正行為についての調査項目である。

管理者による不正行為の指示、黙認、隠蔽などは今回の事故とは関係がない。

６．確認

マイナンバー交付に関連した今まで経験していない新たな業務内容の確認手順が検討されていない可能性があった。

また管理体制については次の2つの作業中において確認体制（ダブルチェック）が機能していなかった可能性があった。

・茨城計算センターが自動交付機発行システムを設定する作業において

個人番号を記載しないこととする設定をする際に複数人でのチェックと管理者のチェックを実施していなかった。また取手市の職員も作業立会を実施しなかった。もしくは立会をしたが十分な確認手順が無かった、もしくは確認をする体制が整備されていなかった。

・茨城県取手市職員が住民票個人票の交付をする作業において

窓口職員が請求内容と印刷された住民票個人票の記載内容の突合確認を怠った。

７．変更措置

茨城計算センターが自動交付機発行システムを設定する作業に関する計画変更が当初の作業計画と大きく異なる点は無かった。

８．組織要因・風土

組織の文化、考え方、風土などが事故の要因となっているか調査する項目である。

具体的にはルール違反が日常化していたり、安全性よりもコストが重視されていたり、問題が発生した場合に隠蔽したりするなどの不正行為が組織の中で行われているかどうかなどを調査する必要があるが、今回の情報漏洩事故においてそのような事が行われていた可能性は低い。

［Education：職務遂行のために必要な能力、意識を向上させるための対策］

１．知識教育

茨城県取手市は管理体制下において既に整備されている情報セキュリティポリシーとその手順書、それらに基づいた情報セキュリティ研修の実施や、関連したeラーニング研修の受講を行っており、またと茨城計算センターについてもISMSに基づいて知識教育に準備していると考えられる。

従ってマイナンバー交付に関連した今まで経験していない新たな業務内容の知識教育を作業マニュアル、教育用教材に追記し、講習会や説明会で受講者に知識付けすることが必要である。

２．意識教育

本項目についても１．知識教育と同様に教育体制やドキュメントは整理されているため

マイナンバー交付に関連した今まで経験していない新たな業務内容の意識啓発を行う。特に既に事故が発生しているため事故の事例を紹介することにより、受講者のセキュリティ意識に関する啓蒙活動を行うと効果的であると考えられる。

３．実技

マイナンバー交付に関連した今まで経験していない新たな業務内容についてOJT（On the Job Trainning）や実地訓練を行うことが必要である。

［Engineering：安全性を向上させるための設備、方法の技術的な対策］

１．設備機器の改善

茨城計算センターによる自動交付機の設定作業で起きた設定誤りが事故の原因であるため、設定誤りを防止する対策を準備する必要がある。考えられる対策としては個人番号が印字されないように設定を変更することである。

今回の場合は設定変更以外に自動交付機側で実施出来ることは無いため、フェールセーフの観点では取手市の職員が窓口で請求内容と印刷された住民票個人票の記載内容の突合確認を実施することが求められる。

２．工程の改善

自動交付機の設定作業で起きた設定誤りが事故の原因であるため、個人番号が印字されないように設定変更をした後で、個人番号が印字されていないか自動チェックする機能を具備するとダブルチェックが可能となる。

３．基準の見直し

今回の情報漏洩事故を受けて自動交付機の設定作業で特に基準を設ける必要性は無い。

［Enfrocement：業務を確実に実施するための強化・徹底に関する対策］

１．規定化

今回の情報漏洩事故を受け、マイナンバー交付に関連した今まで経験していない新たな業務内容について情報セキュリティポリシー等を必要に応じて改定する。

２．評価・指導

マイナンバー交付に関連した今まで経験していない新たな業務内容について作業内容の評価、指導及び注意喚起を行う。またISMSでのPDCAサイクルの実施徹底やセキュリティ監査の実施も対策案として検討すべきである。

３．危険予知活動

業務における箇所の抽出や、危険を未然に防ぐ対策を講じるための対策

危険予知活動の徹底や、取手市職員や茨城計算センター社員の体調確認などが該当するが、今回の情報漏洩事故にはあまり関連性は無い。

［Example:　具体的な事例を示す対策］

１．模範事例

情報漏洩事故を未然に防止するための認識向上を図るための対策として今回の情報漏洩事故を事例としてまとめる。

２．水平展開

共通性のあるトラブル等の情報を共有するための対策として、また新たな情報漏洩事故が発生した際には事例を収集し、事例集化することによる知識やノウハウを関連組織で共有する。それらについてデータベースによる情報の共有を実施する。

［Environment:　物理的な作業環境を改善する対策］

１．作業環境の改善

業務に対する注意力を図るための対策。

照明、騒音、温度、湿度等、適した作業環境を整えるというものであるが今回の情報漏洩事故では特に影響は無い。

以上4M-5Eヒューマンエラー分析手法に基づいてヒューマンエラー分析を実施し、対策立案を行った結果を表7-1に示す。

表7-1　4M-5Eマトリックス結果

		4M			
		Man 心身的な要因、作業能力的な要因	**Machine** 設備・機器・器具固有の要因	**Media** 物理的、人的な環境の要因	**Management** 組織における管理状態に起因する要因
	脆弱性の具体的な要因を記載する。 要因が複数ある場合は行を追加する。	・作業が直前の週末に実施されていることから、疲労や精神的な焦りなどがあった可能性 ・マイナンバー交付に関連した今まで経験していない新たな業務作業を行う上で十分な技能が無かったり、作業に不慣れであったりした可能性 ・新たな業務に対する知識の不足、誤った理解等が事故の要因になっている可能性 ・作業実施のタイミング、作業対象、作業順序、整理整頓の実施などが事故の要因になっている可能性	・設定のとおり印字されているかのチェック機能が不備	・人員不足のため勤務体制が不十分であった可能性 ・サービス開始直前であったため、残業などを実施していたなど勤務条件が不適当であった可能性	・体制や規定は整備されていたが、実運用レベルの手順の整理に不備 ・工程など作業スケジュールが不適切 ・作業計画が不十分 ・作業内容に不備 ・管理者による作業内容と計画のレビューが不十分 ・作業時のリスク評価と対策が不十分 ・マイナンバー漏洩のリスクの可能性チェックが不十分 ・マイナンバー交付に関連した今まで経験していない新たな業務内容について細かな現場レベルの作業項目まで教育内容が未整備 ・教受講する側も細かな現場レベルの作業項目まで未習得 ・茨城計算センターが自動交付機発行システムを設定する作業において個人番号を記載しないこととする設定をする際に複数人でのチェックと管理者のチェックを未実施。 ・取手市の職員が作業立会を未実施。 ・立会をしたが十確認手順が不十分かもしくは確認をする体制が未整備 ・茨城県取手市職員が住民票個人票の交付をする作業において窓口職員が請求内容と印刷された住民票個人票の記載内容の突合確認を怠った。
5E	Education 職務遂行のために必要な 能力、意識を向上させる ための対策	・マイナンバー交付に関連した今まで経験していない新たな業務内容の知識・意識教育を作業マニュアル、教育用教材に追記し、講習会や説明会で受講者に知識付けすることが必要 ・同様にOJT(On the Job Trainning)や実地訓練により必要な能力を習得	－	・勤務体制の見直し ・勤務条件の見直し	・マイナンバー交付に関連した今まで経験していない新たな業務内容の知識・意識教育を作業マニュアル、教育用教材に追記しが未実施。講習会や説明会を実施 ・担当の取手市職員や茨城計算センター社員向けのOJT(On the Job Trainning)や実地訓練を実施
	Engineering 技術、工学的な対策	－	・自動交付機の設定を個人番号が印字されないように変更 ・個人番号が印字されていないか自動チェックする機能を具備	－	－
	Enforcement 強化、徹底による対策	・取手市の職員が窓口で請求内容と印刷された住民票個人票の記載内容の突合確認を実施	・作業を手順化しマニュアルの制定、変更を行う	－	・マイナンバー交付に関連した今まで経験していない新たな業務内容について情報セキュリティポリシー等を必要に応じて改定 ・作業内容の評価、指導及び注意喚起を実施 ・ISMSでのPDCAサイクルの実施徹底やセキュリティ監査を実施 ・作業工程やスケジュールなどをルール化
	Example 模範、事例による対策	・今回の情報漏洩事故の事例を作成	－	－	・今回の情報漏洩事故を事例としてまとめる。 ・新たな情報漏洩事故が発生した際には事例を収集し、事例集化することによる知識やノウハウを関連組織で共有する。
	Environment **物理的な作業環境を改善する対策**	－	－	－	－

Man（作業者の心身的な要因、作業能力的な要因）に関する脆弱性として以下の点が明らかとなった。

（以下脆弱性）

・作業が直前の週末に実施されていることから、疲労や精神的な焦りなどがあった可能性

・マイナンバー交付に関連した今まで経験していない新たな業務作業を行う上で十分な技能が無かったり、作業に不慣れであったりした可能性

・新たな業務に対する知識の不足、誤った理解等が事故の要因になっている可能性

・作業実施のタイミング、作業対象、作業順序、整理整頓の実施などが事故の要因になっている可能性

この脆弱性に対する対策案をマトリックスが交差した点から導き出した結果を以下のとおり項目毎に示す。

脆弱性に対する対策案（マトリックスで Man と Education が交差した項目）

・マイナンバー交付に関連した今まで経験していない新たな業務内容の知識・意識教育を作業マニュアル、教育用教材に追記し、講習会や説明会で受講者に知識付けすることが必要

・同様にOJT(On the Job Trainning)や実地訓練により必要な能力を習得

脆弱性に対する対策案（マトリックスで Man と Enforcement が交差した項目）

・取手市の職員が窓口で請求内容と印刷された住民票個人票の記載内容の突合確認を実施

脆弱性に対する対策案（マトリックスでManとExampleが交差した項目）

・今回の情報漏洩事故の事例を作成

Machine（設備・機器・器具固有の要因）に関する脆弱性として以下の点が明らかとなった。

・設定のとおり印字されているかのチェック機能が不備

脆弱性に対する対策案（マトリックスで Machine と Engineering が交差した項目）

・自動交付機の設定を個人番号が印字されないように変更

・個人番号が印字されていないか自動チェックする機能を具備

脆弱性に対する対策案（マトリックスで Machine と Enforcement が交差した項目）

・作業を手順化しマニュアルの制定、変更を行う

Media（物理的、人的な環境の要因）に関する脆弱性として以下の点が明らかとなった。

・人員不足のため勤務体制が不十分であった可能性
・サービス開始直前であったため、残業などを実施していたなど勤務条件が不適当であった可能性

脆弱性に対する対策案（マトリックスで Media と Education が交差した項目）

・勤務体制の見直し
・勤務条件の見直し

Management（組織における管理状態に起因する要因）に関する脆弱性として以下の点が明らかとなった。

・体制や規定は整備されていたが、実運用レベルの手順の整理に不備
・工程など作業スケジュールが不適切
・作業計画が不十分
・作業内容に不備
・管理者による作業内容と計画のレビューが不十分
・作業時のリスク評価と対策が不十分
・マイナンバー漏洩のリスクの可能性チェックが不十分
・マイナンバー交付に関連した今まで経験していない新たな業務内容について細かな現場レベルの作業項目まで教育内容が未整備
・教受講する側も細かな現場レベルの作業項目まで未習得

・茨城計算センターが自動交付機発行システムを設定する作業において個人番号を記載しないこととする設定をする際に複数人でのチェックと管理者のチェックを未実施
・取手市の職員が作業立会を未実施
・立会をしたが十確認手順が不十分かもしくは確認をする体制が未整備
・茨城県取手市職員が住民票個人票の交付をする作業において窓口職員が請求内容と印刷された住民票個人票の記載内容の突合確認を怠った。

脆弱性に対する対策案（マトリックスで Management と Education が交差した項目）

・マイナンバー交付に関連した今まで経験していない新たな業務内容の知識・意識教育を作業マニュアル、教育用教材に追記しが未実施。講習会や説明会を実施
・担当の取手市職員や茨城計算センター社員向けのOJT(On the Job Trainning)や実地訓練を実施

脆弱性に対する対策案（マトリックスで Management と Enforcement が交差した項目）

・マイナンバー交付に関連した今まで経験していない新たな業務内容について情報セキュリティポリシー等を必要に応じて改定
・作業内容の評価、指導及び注意喚起を実施
・ISMS での PDCA サイクルの実施徹底やセキュリティ監査を実施
・作業工程やスケジュールなどをルール化

脆弱性に対する対策案（マトリックスで Management と Example が交差した項目）

・今回の情報漏洩事故を事例としてまとめる。
・新たな情報漏洩事故が発生した際には事例を収集し、事例集化することによる知識やノウハウを関連組織で共有する。

３　適用実験結果について

事故報告書の作成と並行してVTAを作成し適用実験を行った。VTAのフローチャートにより、関連者や関連物を時系列で視覚化出来た。従って事故の事実関係を明確にすることが出来た。

その結果、4M-5Eについてはそれぞれの項目に基づき理路整然と問題点を抽出できるため、それぞれの項目毎にその背後要因の探索が容易に実施出来る。結果として対策案がマトリックスにおいて各項目の交差点上に容易に導き出されることから対策立案も容易に実施可能であった。

今回取り上げた事故は、事故の経緯が大阪市立大学や取手市より報道発表で公開されていたため、ある程度詳細な分析が可能であった。分析の材料としてはより多くの情報を得られたほうが、より有効な対策案が立案可能となる。

ヒューマンエラー分析の知識が無い現場の地方自治体職員や関連の民間会社社員でも手順にそって手法を活用すれば十分は分析結果と対策案の立案が可能であると考える。今後、マイナンバーの情報漏洩事故が不幸にも発生してしまった場合にはVTAと4M-5Eとを組み合わせたヒューマンエラー分析手法を適用することで要因分析・対策立案を実施することが可能である。

また個々の取り組みで得られた情報をデータベースとして蓄積し、情報漏洩事故対応や防止策立案に役立てる仕組み作りも必要である。

第８章　本研究のまとめとマイナンバーのセキュリティを高めるための提言

本研究の目的は、マイナンバー制度施行に関して懸念されている情報漏洩事故の可能性と防御策を検討する事であった。

2016年1月施行予定の共通番号（マイナンバー）制度によって日本に居住する外国人を含む全住民に付与されるマイナンバーの漏洩防止は、個人情報の保護という点だけでなく今後の我が国の情報通信産業の競争力強化という観点からも重要な課題である。

「第１章　マイナンバー法とセキュリティ対策の概要」

本研究の目的はマイナンバーを民間利用する場合のリスク評価を行うことであった。

住基ネットとマイナンバーで大きく異なる点は、住基ネットの利用範囲が住民サービスに限定されているのに対し、マイナンバーの利用範囲が民間利用にまで拡大されている点である。主管官庁である内閣官房や内閣府等は様々な観点からのマイナンバー制度における個人情報保護対策の検討を行っているがセキュリティに完全は無いことから、既に法整備されたマイナンバー法を除いた「技術」「体制」の2つの分野に焦点を絞り、安全措置の中で対策や実際の運用で整備された点を明らかにした。

「第２章　個人情報漏洩事故に関する従来研究」

日本で話題となった日本年金機構の個人情報漏洩事故や海外における遠隔からアクセスされ自動車の制御を奪われる実験などの報告を調査し、最新の攻撃手法やその防御法について学び、攻撃手法がマイナンバーの民間利用の際にどのような脅威となるか考察した。

日本年金機構の事故からは、例えば、「新種」のウイルスにも対応出来る対策を検討する、個人情報をファイル共有サーバへ保存する際のアクセス制限を行う、 個人情報を保存する場合にはファイルに「人に推測されにくいパスワード」を設定することをシステムで検知する仕組みを取り入れるなどの対策案が提示された。

一方で遠隔からアクセスされ自動車の制御を奪われるリスク、スマート冷蔵庫の脆弱性があり、悪意のある第三者に利用されるとGoogleサービスへのログイン情報が盗まれるリスクなど最新の攻撃手法が矢継ぎ早に開発されていることからその対策案の立案も急務である。

情報漏洩事故に関する技術面（システム上の安全措置（技術））の研究は、日本国内においても2006年に個人情報保護法が施行されて以来、情報漏洩事故の社会的関心の高まりを受けて、自治体、民間企業において行われてきた。代表的な情報漏洩対策手法として強制アクセス制御により情報漏洩を防止、ログ分析による情報漏洩監視、漏洩したファイルの追跡などが挙げられるが、企業におけるセキュリティ対策は いたちごっこの側面があ

り、完全なセキュリティ対策システムというものは存在しない。従ってシステムの運用を通して対策の見直しやフィードバックを繰り返していく必要があり、更にはインシデントが発生した際に、 素早く状況を把握し、対策立案・実施するためのセキュティ活動専門組織が必要である。

体制（人や組織）に関する従来研究は、情報漏洩事故が増加の傾向にあり、事故原因のにおけるヒューマンエラーに起因する事故が全体の80.5%を占めることから、その重要性が指摘されている。

ヒューマンエラーに起因した情報漏洩事故については、エラー発生の詳細な状況分析と対策立案の手法について具体的な方法が提示される必要があるが情報セキュリティ業界ではその標準化がが始まって日が浅い。従って情報セキュリティ分野においては主に航空、鉄道、船舶、電力、ガス、原子力、医療などの各分野で確立された手法を情報セキュリティ分野の情報漏洩事故に適用する形で多くの研究が進められている。代表的なヒューマンエラー分析手法である「4E-4M」、「Medical SAFER」、「VTA」等をITセキュリティの情報漏洩事故のにおけるヒューマンエラー分析に適用出来るかについて近年研究が行われてきた。

しかし従来研究からは代表的な手法を「実際に発生した情報漏洩事故」のヒューマンエラー分析に適用し、分析した事例は１件しか報告されていない、またマイナンバーの情報漏洩事故が発生したのが2015年10月以降であり、現時点（2015年10月末）ではヒューマンエラー分析ツールに適用した例が無いなど、適用実績がほぼ無いことが明らかになった。

海外におけるマイナンバー類似サービスとそのセキュリティについての調査では、「シンガポールの「eCitizen」などが参考となった。しかし多くの国で既に情報漏洩事故が発生している。

従来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が報告された。

韓国政府は韓国において多発する情報漏洩事故を防ぐため、代替手段(I-PIN など)を提供することにより、万が一I-PINが漏洩しても住民登録番号の直接的な漏洩を防ぐなどの取り組みを行っていることが明らかになった。

従来研究では、実際に国内外で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、事故事例を詳細に分析した事例が少ないため、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。すなわちより多数の事故事例を収集し、その分析から得られた攻撃場所、攻撃手法、頻度、攻撃の技術レベルなどの情報に基づき対策を立案する必要がある。
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結果を次章にてまとめた。

「第３章　諸外国におけるマイナンバー類似サービスの情報漏洩事故分析」
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米国、韓国において発生した情報漏洩事故を調査し、事故の発生場所、脅威種別、技術的難易度を明らかにした。
以下に日米韓の情報漏洩事故の比較を行った結果を述べる。

・ 米国における情報漏洩事故の88%が大学、企業などの民間サービスで発生している。脅威の種別に第一位はハッキング38％であり、技術的に高度な攻撃手法が使用されているケースが全体の31%であった。
・ 米国におけるSSNDOB(SSN Data of Birth)問題と呼ばれたデータ仲介業者のハッキングによる情報漏洩事故では、最新のアングラサイトも含めかなり広範囲を網羅して情報漏洩について監視すべきであること、最新のセキュリティ技術（アンチウイルスソフトなども含め）を実装しても起こり得るリスクに対して予防策だけでなく、軽減策、回復策の3つの段階での対策について講じる必要があること、ハッカー集団も含め様々な組織の活動状況を監視必要があること、最新のITサービス（今回は仮想通貨）に着目し、その利用範囲はマイナンバーとの相関関係を把握してリスクを予見すること、などの必要性が明らかとなった。
・ 韓国における情報漏洩事故の86%が民間企業で発生している。脅威の種別に第一位はハッキング43％であり、技術的に高度な攻撃手法が使用されているケースが全体の57%であった。また文化的な背景を象徴してオンラインゲーム、オークション、ソーシャルネットワークに関連した大きな情報漏洩事故が発生している。脅威種別もハッキングが高い割合を占めており攻撃手法も技術的に高度な割合が高かった。

・　日本における漏洩事故の発生箇所は、全て発行元の自治体であった。ID詐称で全体の9割近くを占めており攻撃手法も技術的に低度な割合が多かった。住基カードの名前を砂消しゴムで消して別名を記載するような技術的に難易度が低いID詐称も発生しており、運用面からの対策の必要性も示唆される。

日米韓における情報漏洩事故比較の結果から、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明らかとなった。
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、次章においてシミュにレーションモデルに基づいたリスク評価を実施した。

「第４章　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」

マイナンバーの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一般的なシミュレーションモデルを構築し、そのモデルについて独自に考案したリスク評価手法を用いて情報漏洩のリスク評価を行った。シミュレーションの結果、マイナンバーの民間サービス利用時には、「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か所が重大なセキュリティホールになる可能性があることを明らかにした。

それぞれの設備に対するリスク評価を実施したところ、以下リスクが明確になった。

- ID 詐称
- マルウェア感染やハッキング
- 盗難
- 他で入手した個人番号で他の従業員がアクセス

それらへの対策として以下を示す。

- 付箋紙をPCや机に張らない
- 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
- OSやソフトウェアのパッチ適用やバージョンアップを実施する
- 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を実施する

－ 個人情報リスト、パソコン、磁気テープなどの保管場所をキーロックするなどでセキュアにする

リスク評価とセキュリティ対策が立案出来たが一般的な結果に留まったことから、より詳細なシミュにレーションモデルに応じたリスク評価が必要であると考えた。次章に実施したリスク評価の内容を記す。

「第５章　大学におけるマイナンバーの利用シミュレーションとリスク評価」

具体的なリスク評価の実施のため民間利用の例として大学を選定し、既に発生した個人情報漏洩事故を調査分析した。それぞれの事故において、誰（人物）が、どのような業務を行っている際に発生したのか、またその攻撃についてどのような脅威種別で、実現するためにどの程度の技術難易度が必要とされるのか、について明確にした。実際の国内大学におけるマイナンバー利用の業務ごとのシミュレーションモデルを構築し、そのリスク評価を独自の手法で実施し、必要なセキュリティ対策を立案した。

RSiciliano（2010）の報告にあった、米国においてソーシャルセキュリティナンバー（SSN）の情報漏洩事故の発生確立が最も高い場所である大学について、実際に日本国内の大学での情報漏洩事故について分析した。

日本国内の大学では情報課を中心にセキュリティ事故防止に向けISMSの導入や個人情報漏保護のルール策定が行われてきたが一部の大学で従来導入されたものの多くの大学ではまだ未着手であるなど課題が多い。そのような状況を反映して、大学における情報漏洩は2013年9月から2015年1月の間に判明しただけでも30件の情報漏洩事故が報告されていた。

それら情報漏洩事故の内容を分析した結果、情報漏洩に関連した人物別では学生がわずか3%(30件中1件)であった。職員が57%(30件中17件)、教員が40%(30件中12件)であることからセキュリティ意識が低いと思われた学生ではなく、教職員がセキュリティホールとなっていることが判明した。

従って教職員へのセキュリティ対策が今後は更に必要となることが判明した。それらの情報も参考にし、日本国内の大学においてマイナンバーが利用されることを想定したシミュレーションに基づきリスク評価を実施した結果、業務内容については情報漏洩事故が多いものから教務40%(30件中12件)であり、次いで研究活動27%(30件中8件) であることが判明した。

それらの情報に基づいた評価基準を策定し、登場人物である学生、教員、職員の日々の作業においてマイナンバーを利用すると仮定した上でのリスク評価を行った結果、ネットワーク接続型ハードディスクの設定不備などの対策不備が全体の50%(30件中15件)、USB、PC等の盗難・紛失等が40%(30件中12件)発生している。この2つの事故の合計で事故全体の90%(30件中27件)をヒューマンエラーが占めることから、ヒューマンエラーの防止策の重要性が改めて示された。

次章では、これらの結果を受け、情報漏洩事故におけるヒューマンエラーの防止策について考察を進めた。

「第６章　ヒューマンエラーの防止策」

航空、鉄道、船舶、電力、ガス、原子力、医療などの各分野で確立された代表的なヒューマンエラー分析手法の「4M-5E」、「VTA」、「Medical SAFER」、についてどの手法が情報漏洩事故の分析にもっとも適しているか実際に発生した漏洩事故を適用し（１）事象の整理の容易性、（２）問題点の抽出の容易性、（３）背後要因の探索の容易性、（４）考えられる対策立案の容易性、（５）分析者間の結果のバラつきの少なさ、（６）実施する対策の決定の容易性、（７）実施した対策の効果の評価の容易性などの観点から比較した結果、4M-5EとVTAのフローチャートを併用したモデルが最適であることが明らかになった。

4M-5Eのそれぞれ「Man（人間）、Machine（機械）、Media（媒体）、Management（管理）」に対して対策すべき5E 「 Education（教 育）、Engineering（工学）、Enforcement（強化・徹底）、Example（模範・事例）、Environment（作業環境）」が非常に明確となっているため対策の効果をそれぞれの項目毎に確認出来るからである。またVTAのフローチャートを加える事により、関連者や関連物が時系列で視覚化される点から更に分析効果があがることが明らかとなった。次章ではこの手法を実際に発生したマイナンバー漏洩事故に適用する実験を行った。

「第７章　4M-5EとVTAを組み合わせたヒューマンエラー分析のマインナンバー漏洩事故への適用実験」

VTAと4M-5Eの組み合わせ分析手法を茨城県取手市における個人番号（マイナンバー）を誤記載した住民票交付事件に適用実験した結果、VTAを用いて関連者や関連物を時系列で

視覚化し、その関連性を明確にしたうえで4M-5Eを適用したところ、分析項目毎に問題点を抽出出来た。またそれぞれの項目毎にその背後要因の探索が容易であり、最終的に対策案がマトリックスにおいて各項目の交差点上に容易に導き出された。

ヒューマンエラー分析の知識が無い現場の地方自治体職員や関連の民間会社社員でも手順にそって手法を活用すれば十分な分析結果と対策案の立案が可能であると期待される。

今後、マイナンバーの情報漏洩事故が不幸にも発生してしまった場合にはVTAと4M-5Eとを組み合わせたヒューマンエラー分析手法を適用することで要因分析・対策立案を実施することが可能である。

今回の事故は、事故の経緯が大阪市立大学や取手市より報道発表で公開されていたのである程度詳細な分析が可能であった。分析の材料としてはより多くの情報を得られた方が、より有効な対策案が立案可能となるため、個々の取り組みで得られた情報をデータベースとして蓄積し、情報漏洩事故対応や防止策立案に役立てる仕組み作りも必要である。

「第８章　本研究のまとめとマイナンバーのセキュリティを高めるための提言」

これらの結果に基づき、マイナンバーを運用管理する官公庁、地方自治体および民間企業に対して以下の提言を行う。

- 事故が発生した場合は、マイナンバーが漏洩するリスクと対策案を考える手法としてシミュレーションモデルを用いたリスク評価を活用する

- 今後、予想した内容か、そうでないかに拘らず不幸にも情報漏洩事故が発生してしまった場合には更なる原因分析を行い、対応する組織においてはセキュリティ対策を講じる

- 発生した事故がヒューマンエラーに起因するものであった場合は、「VTAと4M-5Eとを組み合わせたヒューマンエラー分析手法」を活用する。

ヒューマンエラー分析の知識が無い現場の地方自治体職員や、民間会社社員でも十分な分析と、その結果から対策立案が可能である。

－　また個々の組織の取り組みで得られた情報をデータベースとして蓄積し、情報漏洩事故対応や防止策立案に役立てる仕組みを作る。

本研究の後半は、情報漏洩対策で重要なヒューマンエラー防止策に特化した。第8章において「4M-5EとVTAのフローチャートを併用したモデルが最適である」と明記しているが、実際に情報漏洩事故が発生した大阪市立大学の関連者である職員、教員、そして同様に茨城県取手市においても取手市職員や茨城計算センター社員が利用した結果のフィードバックを実験結果に反映し、4M-5EとVTAのフローチャートを併用したモデルが最適である裏付けを行うことは非常に重要である。利用の結果改善すべき内容や項目が見つかった場合は、M-5EとVTAのフローチャートを併用したモデルに反映し、より効果的なモデルになるように修正する作業も、今後は必要である。また、今回の適用実験については一例を試しただけであることから、実際にマイナンバーを扱う自治体職員や民間職員の方が試した結果を蓄積することにより、4M-5EとVTAのフローチャートを併用したモデルが最適であることを証明する検証が必要である。その際には4M-5EとVTAのフローチャートを併用したモデルの使用に関するアンケートを実施することでヒューマンエラー分析の知識が無い現場の地方自治体職員や、民間会社社員でも十分な分析と、その結果から対策立案が可能である事の確認を行う事が重要である。こちらも同様にヒューマンエラー分析の知識が無い現場の地方自治体職員や、民間会社社員でも十分な分析と、その結果から対策立案が困難である事がアンケートから判明した場合は、より使い勝手の良いモデルになるように修正する作業も今後は必要である。

また、本研究ではエンドユーザ、スタッフ、システムという3段階モデルを想定したが、マイナンバーの導入が現実のものになるにつれ、マイナンバーを管理する専門業者が登場し、より複雑なモデルをベースにした検討も必要となってきている。既に市場ではマイナンバーを管理するシステムが、従来から行われてきたオンプレミスと呼ばれる企業などが情報システムを自社で保有し、自社の設備において運用するタイプとクラウドと呼ばれるインターネット側に使いたいサービスの資源が置かれ、利用者はインターネット経由でそのサービスを利用出来るタイプの主に2種類で提供されている。このようなサービス提供者の増加により、マイナンバーの流通が複雑となることから、新しい登場人物の役割がより明確になった段階で、それらを組み込んだ新しいモデルを構築することが必要だと考えている。

4M-5EとVTAのフローチャートを併用したモデルは、ヒューマンエラー分析の知識が無い自治体職員や民間企業社員を対象としている。これらの人々は、ヒューマンエラー分析の知識が十分では無いかもしれないが、現場の業務の知識は十分有している。現場の業務の中でセキュリティ教育や、使用するシステムのセキュリティを高める努力が自治体や民間企業を通じて日々行われている。従って、実際にはヒューマンエラー分析の知識が無く、業務にも携わっていない一般の人々が原因となる情報漏洩事故の発生件数の方が多いものと容易に予想される。この点に関しては第４章「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」においてそれぞれの設備に対するリスク評価において利用者設備の項目で、ID詐称、マルウェア感染やハッキング、盗難、他で入手した個人番号で他の従業員がアクセスするなどのリスクを明確にし、それらへの対策として、付箋紙をPCや机に張らない、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、OSやソフトウェアのパッチ適用やバージョンアップを実施する、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を実施する、個人情報リスト、パソコン、磁気テープなどの保管場所をキーロックするなどでセキュアにする、などを提示した。これらは情報漏洩事故対策案としては非常に一般的な内容であるが、依然としてそれらのリスクが減っていない事が問題であり、一般の人々への対策も引き続き実施する必要がある。先述のIPAからは「SOHO・家庭向けセキュリティ対策マニュアル(Ver1.20)」が公開されている。この資料は、日常的にインターネットを使用するSOHO及び家庭ユーザ向けのインターネットセキュリティマニュアルとされており、その構成は、インターネットに存在する脅威について、クライアントOSやブラウザ、メールソフトのセキュリティ設定、サーバOSと各種サービスのセキュリティ設定手順、ルータのセキュリティ設定手順、通信機器類（スイッチ等）の設定、インターネット回線別の特徴、サーバやネットワーク管理の方法、不正アクセス被害に遭った場合の対応となっている。内容を一読したところ、確かにセキュリティの専門用語を一般の方が理解出来るように体系的に丁寧に説明されているが、依然としてそれなりのスキルや知識が無いと理解する事は容易では無いと思われた。従って市役所や区役所などの地方自治体の窓口でもセキュリティ対策、セキュリティ対策啓蒙活動、注意喚起などを行う必要がある。

次に、高度なハッキングの脅威も今後増加することが、諸外国の調査から容易に推測出来るため対策案の立案が必要であるが、本研究では、その点に深く触れていない。マイ

ナンバーの前身に相当する住基ネットにおいては、システムの構成等の技術情報は完全に秘密裏に管理されており、マイナンバーにおいてもそれが踏襲されている。そのため、システムそのものに対するハッキング等の情報漏洩リスクそのものを本研究で研究対象とすることが困難であった事が理由である。例えば、長野県（2012）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」においては、インターネット側から市町村の庁内ネットワークを経由した住基ネットシステムへの不正アクセス及び住基ネットシステムからの本人確認情報漏洩の可能性を確認し、有効な対策を講ずるための資料を得ることを目的として行われたとしている。長野県の庁内ネットワークは機密情報であり、民間調査会社と県庁職員の一部の関係者にのみ調査のために公開されている。背景として長野県が当時、住基ネットの導入に反対の姿勢を示しており、その理由の最たるものとして個人情報漏洩の危険性がある点を指摘していた事も調査の後ろ盾となっている点を加味しても、長野県による積極的なセキュリティ対策への取り組みと、その結果の公開事例は当時話題となったとおり、極めて異例であった。更に総務省、厚生労働省などの中央省省庁を含めた国の機関とそれらを繋ぐ全国ネットワークに関する機密度は地方自治体以上に高く、そのネットワーク構成とシステム構成の詳細は当然公開されていない。このような状況からマイナンバーの「情報提供ネットワークシステム」についても高度なセキュリティシステムが構築されることが予想されると第１章で述べた。同様に民間利用を行う民間企業側でもマイナンバーが流通するであろうネットワーク構成やシステム構成は最高レベルの企業機密情報であり、民間会社幹部、情報システム関係の管理部門、その他ネットワーク構築やシステム構築とその運用に携わった受託会社の一部関係者のみが知り得る情報である。研究目的であったとしても、そのような機密情報に基づき情報漏洩事故の可能性を探ることを目的とした民間利用のシミュレーション構築とリスク評価を本研究で扱うことは極めて困難であった。

高度な攻撃による情報漏洩事故は起こって欲しくはないことではあるが、実際にマイナンバーのシステム本体にかかわる情報漏洩事故が発生してしまったタイミングで発表される事故報告書をベースにして評価を行うことが必要である。日本年金機構の報告（2015）などがその一例にあたる。国の威信をかけてセキュアに構築したシステムが高度な攻撃により不正侵入を許してしまったことは残念であるが、事故から学んだ教訓を迅速に反映して将来の対策の糧とすることが重要である。

Acquisti(2009)らは、SSNを統計学的手法にて推測するDBを構築し、上述した個人情報と関連付けてSSNを推測するという新しい手法を提示しているが、同様にマイナンバーにおいても12桁の数列を推測する事は数字生成の規則が判明すれば可能であるという考えに基づくと不可能ではない。マイナンバーの数列生成については総務省令第八条法第八条第二項の規定によると、「個人番号とすべき番号は、機構が同条第三項の規定により設置される電子情報処理組織を使用して、作為が加わらない方法により生成する次に掲げる要件に該当する十一桁の番号及びその後に付された一桁の検査用数字（個人番号を電子計算機に入力するときに誤りのないことを確認することを目的として、当該十一桁の番号を基礎として総務省令で定める算式により算出される零から九までの整数をいう。第三号において同じ。）により構成されるものとする。

一　住民票コードを変換して得られるものであること。

二　前号の住民票コードを復元することのできる規則性を備えるものでないこと。

三　他のいずれの個人番号（法第七条第二項の従前の個人番号及び個人番号とすべき番号を含む。）を構成する検査用数字以外の十一桁の番号とも異なること。」とされている。

住民票コードを変換して得られるものであるが、それを復元することのできる規則性を備えるものでないことという表記から、ハッシュ等に用いられる一方向性関数の利用が推測される。従って利用された一方向性関数を解読することがマイナンバー12桁の推測を可能とする。この点は大きなセキュリティホールである。また一方向性関数によるマイナンバーの生成アルゴリズムそのものは極一部の関連者や研究者が知る国家機密であるが、それらが情報漏洩するリスクも全くゼロでは無い。個人番号の生成・通知及びマイナンバーカードの作成を行う運用機関は地方公共団体情報システム機構である。地方公共団体情報システム機構の全国センターにあるデータセンターやサーバには、日本国民の個人情報が集中しているため総務省は、全国センターの所在地を「テロリストの標的になる恐れがある」として公表していない程、セキュリティについては最新の注意が払われていると思われるが、国家レベルのテロの標的となり、例えば信頼していた職員が内部犯行を行うことも否定はできない。このようにマイナンバーそのものが知られるリスクの分析調査は機密事項であり公開されていないことから、どの程度セキュアであることすら一般市民が知る術は無い。

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国民にとって最大の懸念事項として関心を集めている。また実際には既にマイナンバーの漏洩事

故が発生しており、国民の懸念は拡がる一方である。前身の特定個人情報保護委員会を改組して平成28年1月1日に発足した個人情報保護委員会は、「マイナンバー（個人番号）をかたる不審な事案について」を公開している。それによるとマイナンバーが漏洩しているという虚偽の内容のメールを市民に送り、本文から不審なサイトへのアクセスを求めるものや、マイナンバーのセキュリティ対策にかかる費用を電話で請求するなどが報告されている。同様に独立行政法人国民生活センターはマイナンバー精度に便乗した不審な電話等に対する注意喚起を行っている。それによると「個人情報を調査する」とか「口座番号を教えてほしい」などといった不審な電話等に関する相談が全国の消費生活センターに寄せられているとている。助言として

「マイナンバーの通知や利用手続き等で、国や自治体の職員が家族構成、資産や年金・保険の状況等を聞くことはありません。」「不審な電話はすぐに切り、来訪の申し出があっても断ってください。」「万が一金銭を要求されても決して支払わないようにしましょう。」「少しでも不安を感じたら、すぐにお住まいの自治体の消費生活センター等にご相談ください（消費者ホットライン188）。」としているが今後も被害の増加が懸念される。

個人情報保護委員会から、「番号制度ヒヤリハット事例」が公開されており、その一部を以下に紹介する。

1例目は住宅ローンの申込みのために金融機関に提出しようとした住民票（写）の「個人番号」欄に記載されている番号が、マイナンバー（個人番号）であることを知らずに、提出してしまいそうになった事例が報告されている、今回の場合は、利用者が金融機関にマイナンバーを提示する必要が無い点、金融機関側もマイナンバー提示を求めたい点について防止するためのシステム面及び運用面での対策が必要であった。例えば運用面であればマイナンバーが不要な場合は、マイナンバーが記載されない書類を要求するなどである。

2例目は人事異動の際に従業員名簿を修正した。その社員名簿を社内の電子掲示板に掲示しようとした際に謝って同じフォルダーに保存していた「個人番号管理簿」というマイナンバーが記載された別の名簿を掲示しそうになったという事例である。マイナンバーが記載されたファイルは慎重に管理する事が必要である。掲示の際には複数人で不要なシートの確認をするなども有効な手段である。

3例目は、マイナンバーカードが入った財布を紛失してしまったという事例であるが、これは今後も頻発することが予想される。マイナンバーカードを紛失した際は住民票のあ

る市区町村やマイナンバー総合フリーダイヤル（０１２０−９５−０１７８）に早急に連絡する事が必要である。

4例目は、マイナンバー（個人番号）が記入された書類を施錠できるキャビネットに保管していたが、書類を整理しておらず年度末の文書廃棄の際に他の廃棄書類と一緒に捨ててしまいそうになった事例である。マイナンバー（個人番号）が記入された書類は機密情報であり施錠付きのキャビネットに保管するなど個人情報の取扱いと同等の厳しい管理が必要である。

最後はマイナンバー（個人番号）を扱う担当者宛の書留郵便を担当者の代わりに受領したが、その書類を担当者に渡すのを忘れそうになったという事例である。マイナンバー（個人番号）が記載された郵便物の取扱い方法などをセキュリティポリシーで規定し、その保管場所なども決めておくなどの運用面での整備が重要である。

このように既に発生した「マイナンバー（個人番号）をかたる不審な事案」と「番号制度ヒヤリハット事例」からは、今後の被害の増加が予想される事から、その対策立案が必要である。

本研究はマイナンバーの民間利用時におけるリスク評価を行った。マイナンバーが国民の生活に浸透する際には非常に重要な内容である。一方で総務省の公表したデータでは、マイナンバーの前身の住基ネットにおいて、住民基本台帳カードの交付状況は平成27年3月31日の時点で有効交付枚数がわずか約710万枚であった。710万枚を人口数約1億2,844万人で割ると配布率はわずか5.5%であった。配布率だけ見ると政策としては失敗であり、その普及拡大が重要な課題である。政府から住民基本台帳カードの交付状況に関する明確な分析調書は公開されていない。従って、住民基本台帳カードの交付状況が低調である点をどのように補ってマイナンバーを定着させるかについて明確になっていない。このような状況下ではマイナンバーに関して反対意見を述べる国会議員や国民が存在するのも致し方無いのが事実である。

住基ネットが定着しなかった理由として調査をした訳ではないが、IT サービスが定着しない場合の例を考えた場合は、やはりサービスとしての必要性が低かったのではないかと推察できる。本当に必要なサービスであればもっと定着していたのでは無いかと考える。セキュリティの観点から、プライバシーの侵害や情報漏洩事故のリスクを考慮して反対意見が出たのもの事実である。また、システムの円滑な運用が出来ない場合にも定着化が阻

害されたり、遅延したりすることも事実である。実際に、地方公共団体情報システム機構によるシステムの不具合が発生した事により 1,019 万人の希望者に対して 2016 年 3 月までに 227 万枚しか交付できなかったとしている。地方公共団体情報システム機構による障害原因の報告によると中継サーバー内の障害によって、市町村の統合端末から接続出来ない状態が続いた障害原因は以下の 2 つである。1 点目は暗号化と復号化を担う「耐タンパ装置」に処理の対応状況が返答されず、装置が作動していなかった点である。2 点目は業務アプリケーションがデータ処理を行う際にプログラムに不具合があり、業務アプリケーションが異常終了した点である。

システムに障害が発生し、サービスの提供が滞ってしまうと、マイナンバーシステムのように全てシステムで一貫したサービスを提供する場合には非常にクリティカルなミスとなってしまう。今後のマイナンバー定着に向けてシステムの安定運用によるサービスの安定供給を期待したい。

セキュリティ対策を含めたマイナンバー制度の定着に向けて課題は山積している。
しかし、国民ID制度を国家の情報戦略として推進している諸外国に対抗するために、マイナンバー法は単なる個人情報の保護という点だけでなく、今後の我が国の情報通信産業の競争力強化という観点からも重要な課題である。マイナンバー関連の情報漏洩事故を恐れ、我が国の情報通信産業の競争力強化を阻害することは避けるべきである。

今後もマイナンバーの漏洩事故は発生することが予想されるが、様々な対策を講じて対抗し、国民全体で国民ID制度としてマイナンバーを推進すべきだと考えている。その対策立案の過程において本研究内容が少しでも役に立てば幸いである。

文字数：128,591

謝辞

同志社大学大学院ビジネス研究科教授の北寿郎先生には研究主査として三年間指導頂き心から感謝致します。

副査として同様にご指導頂きました（順不同）京都大学情報環境機構IT企画室教授の斉藤康己先生と同志社大学理工学部教授の金田重郎先生にも感謝致します。

また年に2回開催されるTIM（Technology and Innovation Management)特殊研究では様々な専門分野の先生方から研究に対するご意見を拝聴出来き、研究を進めるうえでの大きな助けを頂きました。

同様にITECの宮田秀典先生をはじめとした関係者の方に多大なるご協力を頂きましたことにこの場を借りてお礼申し上げます。

研究業績

１）学術論文

＜査読論文＞

Takeshi Niiyama, Toshiro Kita, ″It Security in National Identification Number, Risk Evaluation At University″, Takeshi Niiyama, Toshiro Kita, International Journal of Advanced Computer Technology IJACT, Volume-4 Issue-5, Publish On October 25,2015 pp.1-7

２）国際会議発表（論文）

＜査読論文＞

Takeshi Niiyama, Toshiro Kita, ″Information Security in National Identification Number - Called My Number in Japan″, International Conference on Business Innovation and Technology Management, Oct 2014, pp.290-326

＜口頭発表＞

Takeshi Niiyama, Oct 18th 2014 Osaka, Osaka International House Foundation

＜口頭発表＞

Takeshi Niiyama, ″Information Security in National Identification Number - Called My Number in Japan″, Takeshi Niiyama, Cyber Security in Romania (Cibiu) 2014, at Romania (Cibiu)

３）国内会議発表

＜論文＞

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」電子情報通信学会 No.119, 2015年, pp.23-30

＜口頭発表＞

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」第70回コンピュータセキュリティ・第14回セキュリティ心理学とトラスト合同研究発表会,,2015年7月3日, 名古屋市中小企業振興会館 吹上ホール

４）その他（ITEC ワーキングペーパー等）

新山 剛司・北 寿郎　「共通番号(マイナンバー)制度における情報セキュリティ-民間利用におけるリスク評価-」 新山 剛司・北 寿郎.　同志社大学 技術・企業・国際競争力研究センター ワーキングペーパー No.14-03　全 21 頁

参考文献

【日本文献】

書籍

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 年

Reason，James（林芳央監訳）『ヒューマンエラー認知科学的アプローチ』海文堂,1994

文献

荒井正人　他　「情報漏洩防止システムの提案」『社団法人 情報処理学会　研究報告 IPSJ SIG Technical Report』2004，61-67 頁

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，87-103 頁

伊藤 博子　他　「m-SHEL モデルを用いた船舶運航のヒューマンファクター分析」『日本航海学会論文集（110）』公益社団法人日本航海学会，2004 年，83-91 頁

今村圭　「マイナンバーを活用した官民連携の今後」『株式会社三菱総合研究所自治体チャネルプロジェクト』（2015 年 11 月 16 日 Web 閲覧日）
http://www.mri.co.jp/opinion/column/localweb/001346.html

上繁義史　「大学入学時における学生の情報セキュリティに関する理解状況について」情報コミュニケーション学会研究報告　2012 年，10-26 頁

上田哲史　「[招待講演]徳島大学情報化推進センターにおける ISMS 構築について」，情報処理学会研究報告．IOT,［インターネットと運用技術］2011-IOT-14(5)，1，2011-07-08　一般社団法人情報処理学会　2011 年，1 頁

上野伸一　「ICTリスクの軽減を実現するヒューマンエラー分析」『FRIコンサルティング最前線．Vol.3』2011年，121-126頁

上原哲太郎　他　「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)，2004 年 1-6 ページ

浦川順平　他　「ソーシャルメディアにおける 情報漏洩防止手法の提案」『情報処理学会研究報告 2010 年度(5)』2010，1-7 頁

江崎郁子　他　「個人情報漏洩防止のための ヒューマンエラー対策（特集 安全と安心の追求)」三菱総合 研究所所報．2005年，66-83頁

川越秀人 他　「情報セキュリティのヒューマンファクタ」『情報処理学会研究報告 Vol.2008,No.45』2008，13-18頁

河野龍太郎　「MEDICALSAFERの開発について」ImSAFER研究会公式HPにて公開 http://medicalsafer-kts.com/index.html，（2015年11月16日Web閲覧日）

河野龍太郎　「ヒューマンエラー低減技法の発送手順：エラープルーフの考え方」『日本プラント・ヒューマンファクター学会誌第 4 巻第 2 号』1999 年，121-130 頁

危険物保安技術協会　北九州市消防局　「VTA 手法の活用とあいさつ、声かけ、対話」『Safety & Tomorrow No.132』2010年，41-48頁

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 年，347-350 頁

木村長人　「自治体の情報化におけるプライバシー保護をめぐる問題」東京大学大学院学際情報学府修士課程　修士論文　2004

葛野弘樹　「Android アプリケーションに対する情報フロー制御機構の提案」Computer Security Symposium 2011,2011 年, 19-21 頁

原子力安全技術センター（公財），公式HP「トラブル事象分析手法4M-5E」
http://www.n-iinet.ne.jp/4M-5E.htm　（2015年11月17日Web閲覧日）

原子力安全技術センター（公財）「4M-5E 分析手法マニュアル」公式 HP にて公開
http://www.n-iinet.ne.jp/Manual4M-5E.pdf　（2015年11月17日Web閲覧日）

財団法人自治体国際化協会　「各国の電子自治体の推進状況　平成 17 年度海外比較調査」2006

榊原裕之 他　「ログ分析による情報漏洩監視」『情報処理学会研究報告　IPSJ SIG Technical Report』2011 年, 1-6 頁

坂本泰久　「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)」『高度情報通信ネットワーク社会推進戦略本部第 25 回電子行政に関するタスクフォース　資料 2-1 』2012 年, 1-25 頁

島田達巳　他　「国民からみた共通番号制度の諸問題」『経営情報学会　全国研究発表大会要旨集 2012 年』237-240 頁

JETRO/IPA(渡辺弘美)「米国における個人情報漏洩の現状と対策」『ニューヨークだより 2005 年 4 月』2005 年, 1-24 頁

崔　裕溶　「韓国の個人情報保護法の内容と個人情報保護管理体系」日本のプライバシー・個人情報保護とマネージメントシステムの国際標準化シンポジウム」『第１回「日本をとりまく国際動向と日本の現状」研究論文』2012，39-46 頁

鈴木史比古 他　「JR 東日本版 4M4E 分析手法の開発と導入・展開」『JR East Technical Review，No.21』2004，pp.31-34

関岡保二 「経営組織におけるエラー管理--4M-4E マトリックス法と m-SHEL モデル」中央学院大学商経論叢 19(2)，2005-03-31，2005 年，67-78 頁

総務省　(国際大学グローバル・コミュニケーション・センター)「諸外国における国民 ID 制度の現状等に関する調査研究 報告書」　2012 年

総務省　公的個人認証サービスの民間拡大について　2014年，1-13頁

総務省　「スマートフォン上のアプリケーションにおける利用者情報の取扱いの現況等」『スマートフォン アプリケーション プライバシーポリシー 普及・検証推進タスクフォース報告書』2014

高川健一　「海外の原子力発電所における運転員ヒューマンエラー事例の新しい分類と利用しやすい事例シートの作成」『INSS JOURNAL』（株）原子力安全システム研究所，2004，　95-106 頁

高木浩光　他　「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』2013 年，1-8 頁

田島浩一　「広島大学におけるセキュリティ脆弱性診断の実施とその評価」　学術情報処理研究 No.18，2014 年，16－23 頁

舘剛司　「外部からの脅威に対するセキュリティ技術の動向」『ビジネスコミュニケーション 2006 Vol.43 No.10』2006年，14-17頁

千葉武史　他　「4M4E を用いたヒューマン エラー分析手法の研究」『JR EAST Technical Review，No.9』2004 年，30-35 頁

張 睿暎　「韓国における個人情報保護法制の問題と改善案」『東京都市大学環境情報学部紀要　掲載号 11』2010 年，39-46 頁

手塚悟　「我が国におけるサイバーセキュリティの状況」シンポジウム:
サイバーセキュリティ産業化：日本の課題とイスラエルの動向」2015,1-50 頁

寺田有美子　「企業における個人情報保護対策の取り組み」『UNISYS TECHNOLOGY REVIEW 第 86 号』2005 年，50-67 頁

富樫由美子　他　「企業の情報セキュリティ対策における ヒューマンエラー管理実践に向けた検討」『情報処理学会研究報告』2009，1-7頁

独立行政法人情報処理推進機構（IPA）「2013 年度情報セキュリティ事象被害状況調査報告書資料」2013 年，　P21 頁

独立行政法人情報処理推進機構（IPA）「情報セキュリティ人材の育成に関する基礎調査」2014，1-119 頁

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 43 号』2004 年，21-15 頁

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　『平成26年度10月版マイナンバー　社会保障・税番号制度　概要資料』2014年，6頁

内閣府　「社会保障・税の番号制度に関する世論調査」第２章（１）

永井好和　「国立大学における情報セキュリティ事故コスト定量化方式　秋季大会プログラム　2008 年，16－23 ページ

中川かおり　「米国における個人情報保護の動向　国立国会図書館調査及び立法考査局外国の立法 231」2007，59-85 頁

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　(2015年11月17日Web閲覧日)

成澤寛　「私立大学における個人情報保護」東邦学誌 第 35 巻第 1 号　2006 年，123-140 頁

新原功一　他　「情報セキュリティインシデントに対するヒューマンエラー対策の提案」FIT2013(第 12 回情報科学技術フォーラム) 2013，　57-63 頁

日本ネットワークセキュリティ協会「スマートフォンの安全な利活用のガイドライン 2013」，2013 年

日本ネットワークセキュリティ協会 セキュリティ被害調査ワーキンググループ「2007 年情報セキュリティインシデントに関する調査報告書,Ver.1.2,2008」3頁

日本ネットワークセキュリティ協会 セキュリティ被害調査ワーキンググループ「2007 年情報セキュリティインシデントに関する調査報告書,Ver.1.2,2008」2008年，12-22頁

日本年金機構　「不正アクセスによる情報流出事案に関する調査結果報告書」2015

堀田周吾　「個人識別情報の不正取得・不正使用に対する刑事訴追」『駿河台法学　第23巻第1号（通巻第43号）』2009，1-23頁

ベライゾン　「2014年度データ漏洩／侵害調査報告書」『エグゼクティブサマリー2014年』2014年,

牧野　英克　「情報セキュリティ事故再発防止策についての考察」『産業経済研究所紀要第17号2007年3月』2007　65-90頁

村上靖　「情報セキュリティ事件・事故の分析と対策に関する考察」『情報処理学会研究報告』2010，1-8頁

李中淳　他　「情報連携基盤のビジネスプロセスフローの制御に係るセキュリティに関する研究」社団法人電子情報通信学会，2013，225-229頁

安岡 美佳　「デンマーク電子政府の試み　国立社会保障・人口問題研究所」『特集：社会保障制度における財源徴収と情報管理の国際比較　海外社会保障研究 Autumn2010　No.172』2010，17-30頁

【外国文献】

Anderson, Alicia., "Effective Management of Information Security and Privacy," *Educause Quartely*, January 1, 2006, pp.15-20

Acquisti, Alessandro., "Faces of FaceBook Privacy in the Age of Augmented Reality," *Black Hat USA*, 2012

Acquisti, Alessandro., "Predicting Social Security numbers from public data," *PNAS (Predicting Social Security numbers from public data), Carnegie Mellon University*, 2008, pp. 10975–10980

Krebs, Brian (Washington Post)., blog Krebs on Security, "SSNDOB (Date Of Birth),"
http://krebsonsecurity.com/2013/09/data-broker-giants-hacked-by-id-theft-service/
(2015 年 11 月 17 日 Web 閲覧日)

Miller, Charlie., Valase , Christopher., "A Survey of Remote Automotive Attack Surfaces," *BlackHat2014*, pp.1-94

Kitamura, Naoshi., "A practical improvement of information security management for local government in Japan," *Carnegie Mellon University Information Security Master Thesis*, 2006

Christin, Nicolas., "Traveling the Silk Road A measurement analysis of a large anonymous online marketplace," *Technical Reports: CMU-CyLab*-12-018, 2012, pp.1-26

Honda, Masami., "My Number Act and Government CIO in Japan," *International Academy of CIO Japan 2012*, pp.1-6

OECD "National Strategies and Policies for Digital Identity Management in OECD Countries," 2011, pp.1-89

Pen Test Partners, blog 2015 (2015 年 11 月 17 日 Web 閲覧日)
https://www.pentestpartners.com/blog/hacking-defcon-23s-iot-village-samsung-fridge/

Siciliano, Robert., "Top Ten Most Dangerous Places to Leave Your Social Security Number,"
http://robertsiciliano.com/blog/2010/10/18/mcafee-reveals-the-top-ten-most-dangerous-places-to-leave-your-social-security-number/ (2015 年 11 月 17 日 Web 閲覧日)

Siciliano, Robert., "Requests For Social Security Numbers Leads to Identity Theft,"

http://robertsiciliano.com/blog/2009/06/16/requests-for-social-security-numbers-leads-to-identity-theft/ （2015 年 11 月 17 日 Web 閲覧日）

Niiyama, Takeshi., “Thwarting information security threats in modern anonymous P2P software,” *Carnegie Mellon University Information Security Master Thesis*, 2006

Moore, Tyler., Christin, Nicolas., “Beware the Middleman Empirical Analysis of Bitcoin-Exchange Risk” *Financial Cryptography and Data Security 2013*, pp.1-8

＜ホームページ：以下 2015 年 11 月 17 日 Web 閲覧確認＞

1. 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
（2015 年 11 月 17 日 Web 閲覧日）
http://www.cas.go.jp/jp/seisaku/jouhouwg/index.html

2. 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）
（2015 年 11 月 17 日 Web 閲覧日）
http://www.soumu.go.jp/main_sosiki/jichi_gyousei/daityo/mynumber_rfi.html

3. Hackers Remotely Kill a Jeep on the Highway-With Me in It（遠隔からの自動車操作） （2015 年 11 月 17 日 Web 閲覧日）
https://www.youtube.com/watch?v=MK0SrxBC1xs

4. ヒューマンエラーの定義（Wikipedia） （2015 年 11 月 17 日 Web 閲覧日）
https://ja.wikipedia.org/wiki/ヒューマンエラー

5. 情報セキュリティ心理学とトラスト（Security Pasychology & Trust）
（2015 年 11 月 17 日 Web 閲覧日）
http://www.sig-spt.org

6. eCitizen （2015 年 11 月 17 日 Web 閲覧日）

http://www.ecitizen.gov.sg/Pages/default.aspx

7. Death Master File (2015年11月17日Web閲覧日)
http://en.wikipedia.org/wiki/Death_Master_File

8. SSNの番号割り振りの経緯 (2015年11月17日Web閲覧日)
http://www.socialsecurity.gov/employer/stateweb.htm

9. Anderson Hays CooperのTV番組「フェースブックからソーシャルセキュリティナンバー(SSN)を詐称する事例」 (2015年11月17日Web閲覧日)
https://www.youtube.com/watch?feature=player_embedded&v=8_JOWZ8hQ5Y

10. Maplestoryの情報漏洩事故 (2015年11月17日Web閲覧日)
http://news.livedoor.com/article/detail/6069137/

11. Maplestory 公式HP (2015年11月17日Web閲覧日)
http://maplestory.nexon.net/landing/

12. 趙(ITジャーナリスト)のコラム(韓国インターネット振興院が運営する「住民登録番号クリーンセンター」のホームページ) (2015年11月17日Web閲覧日)
http://pc.nikkeibp.co.jp/article/column/20120127/1040663/?rt=nocnt

13.「コグル」ホームページの紹介 (2015年11月17日Web閲覧日)
http://podpod.wo.to/cogle.php

14. 福井県勝山市「ライフサイクルインデックス」(2015年11月17日Web閲覧日)
http://www.city.katsuyama.fukui.jp/docs/uploads/data/9189_data_lib_data_130613112950.pdf

15. ISMS　（2015 年 11 月 17 日 Web 閲覧日）
http://www.isms.jipdec.or.jp/isms.html

16. ISMS ユーザーズガイド　P33　（2015 年 11 月 17 日 Web 閲覧日）
http://www.isms.jipdec.or.jp/doc/JIP-ISMS113-21.pdf

17. ISMS 認証取得組織検索より　（2015 年 11 月 17 日 Web 閲覧日）
http://www.isms.jipdec.or.jp/lst/ind/index.html

18. 日本国内大学において発生した情報漏洩事故　（2015 年 11 月 17 日 Web 閲覧日）
http://www.security-next.com/053330

19. 同志社大学の「電算処理　業務システム一覧」　（2015 年 11 月 17 日 Web 閲覧日）
https://www.doshisha.ac.jp/attach/page/OFFICIAL-PAGE-JA-582/8906/file/dd4200.pdf

20. 学生カードの利用状況
http://it.doshisha.ac.jp/information/ic_card/outline.html

21. 同志社の個人情報保護の基本方針　（2015 年 11 月 17 日 Web 閲覧日）
http://www.doshisha.ed.jp/privacy/index.html

22　個人情報の保護に関する規程　（2015 年 11 月 17 日 Web 閲覧日）
http://www.doshisha.ed.jp/privacy/regulations.html

23　大阪市立大学の公式 HP　教員の USB メモリ紛失による個人情報の漏洩事故
（2015 年 11 月 17 日 Web 閲覧日）
http://www.osaka-cu.ac.jp/ja/news/2014/j5tx6o

24　大阪市立大学　情報セキュリティポリシー　（2015 年 11 月 17 日 Web 閲覧日）

https://www.osaka-cu.ac.jp/misc/reiki_int/reiki_honbun/x021RG00000140.html

25　NTT 東日本、NTT 西日本　個人情報保護のための取り組み（情報漏洩防止のため指紋認証付きアクセス制限機能付き USB メモリの説明）　（2015 年 11 月 17 日 Web 閲覧日）
http://www.ntt.co.jp/csr/2010report/safety/activity08.html

26　独立行政法人国民生活センターより注意喚起　（2015 年 11 月 17 日 Web 閲覧日）
http://www.kokusen.go.jp/news/data/n-20150915_1.html

27　マイナンバー占い　（2015 年 11 月 17 日 Web 閲覧日）
http://マイナンバー.biz/mainanbauranai.html

28　個人番号（マイナンバー）を誤記載した住民票交付の経緯と対応　（茨城県取手市）（2015 年 11 月 17 日 Web 閲覧日）
https://www.city.toride.ibaraki.jp/index.cfm/8,49277,16,126,html

29　札幌市厚別区　マイナンバー誤交付　住民票発行機の操作ミス
（2015 年 11 月 17 日 Web 閲覧日）
http://dd.hokkaido-np.co.jp/news/society/society/1-0190599.html

30　取手市地域情報化計画　（2015 年 11 月 17 日 Web 閲覧日）
http://www.city.toride.ibaraki.jp/index.cfm/11,23196,c,html/23196/20130508-151754.pdf

31　茨城計算センター　公式 HP でのセキュリティ宣言　（2015 年 11 月 17 日 Web 閲覧日）
http://www.iacnet.co.jp

付録

表１　個人情報保護ワーキンググループ　構成員情報

構成員	所属役職	専門	論文、書籍
石井　夏生利	筑波大学図書館情報メディア系准教授	プライバシー権 個人情報保護法	『マイナンバーと情報セキュリティ』　情報セキュリティ総合科学/pp.87-103, 2012-11 『EUデータ保護規則提案と消費者プライバシー権利章典』Nextcom/pp.30-37, 2012-05 『諸外国等の個人情報保護制度の実態調査検討委員会報告書(消費者庁)*EMPTY*, 2009-03
宇賀　克也	東京大学大学院法学政治学研究科教授	個人情報保護、情報公開、行政手続	『個人情報保護法の逐条解説』〔第3版〕（有斐閣、2009年） 『解説個人情報の保護に関する法律』（第一法規、2003年） 『大量閲覧防止の情報セキュリティ』（編著）（地域科学研究会、2006年）
大谷　和子	（株）日本総合研究所法務部部長	個人情報保護、プロバイダ責任制限法	『ITユーザの法律と倫理』（情報フロンティアシリーズ）[単行本]
小向　太郎	(株)情報通信総合研究所主席研究員	情報法、個人情報保護	『デジタル・ネットワークと著作権制限規定』法政理論（新潟大学）第41巻第3・4号（2009） 『世界中の情報』とデジタル・フォレンジック』日本セキュリティ・マネジメント学会誌第22巻第3号（2008）
新保　史生	慶応義塾大学総合政策学部准教授	法学、公法学	『OECDプライバシーガイドライン － 30年の進化と未来』OECDプライバシーガイドライン － 30年の進化と未来 ；；；；2014/02 『新基本法コンメンタール　情報公開法・個人情報保護法・公文書管理法―情報関連7法』日本評論社 ；；P.608　(206-210)　；2013/09/28
（座長代理） 長谷部　恭男	東京大学大学院法学政治学研究科教授	憲法	『憲法の円環』（岩波書店、2013年） 『情報法』（有斐閣、2012年）
樋口　範雄	東京大学大学院法学政治学研究科教授	英米法、医事法、信託法	『はじめてのアメリカ法』（2010年・有斐閣） 『信託と契約』信託法研究21号57-88頁（1997年）
藤原　静雄	中央大学法科大学院教授	行政法 公法学	『情報公開法改正案についての備忘録』―大臣試案に対する意見書と審議過程― 『第3国への個人データ移転と「個人データの処理にかかるプライバシー保護の国際標準草案のための共同提案』　季報情報公開個人情報保護、行政管理研究センター

（座長） 堀部 政男	一橋大学名誉教授 特定個人情報保護委員会委員長	英米法 情報法 プライバシー権	『JIS Q 15001:2006　個人情報保護マネジメントシステム要求事項の解説』日本規格協会 2006．6 「個人情報保護法制化の背景と課題」,4～10 頁　法律のひろば 2 月号（2001．2）
玉井　哲雄	法政大学理工学部創生科学科教授	ソフトウェア工学	『モデルに基づく誤り特定と反例修正候補の提示』ソフトウェアエンジニアリング最前線　（ソフトウェアエンジニアリ ングシンポジウム 2009 論文集）
三宅　弘	弁護士	官僚制、政策過程	『制度設計の行政学』（慈学社出版，2007 年）
（座長代理） 森田　朗	学習院大学法学部政治学科教授	行政学	『政治空間の変容と政策革新（3）分権改革の動態』（東京大学出版会，2008 年）

表 2　情報連携基盤技術ワーキンググループ　構成員情報

構成員	所属役職	専門	論文や書籍
新井　悠	ラックホールディングス（株）	セキュリティ技術	『アナライジング・マルウェア ―フリーツールを使った感染事案対処（Art Of Reversing）』新井 悠、岩村 誠、川古谷 裕平、 青木 一史（2010/12/20） ネットワーク攻撃詳解―攻撃のメカニズムから理解するセキュリティ対策 三輪 信雄、 新井 悠（2002/3）
飯島　淳一	東京工業大学大学院社会理工学部研究科長	情報システム学 システム理論	CIO 学 IT 経営戦略の未来（共著），東京大学出版会，Nov．2007． 成功に導くシステム統合の論点，日技科連出版社，Oct．2005．
大山　永昭	東京工業大学像情報工学研究所教授	光情報処理、画像工学	『大山永昭、「画像の電子保管と IS&C システムー技術的基準とセキュリティ機能ー』，新医療，1994 年 7 月号，36-40(1994)
小松　文子	（独）情報処理推進機構　情報ｾｷｭﾘﾃｨ分析ﾗﾎﾞﾗﾄﾘｰ長	情報セキュリティ経済	『情報セキュリティエコノミクスの挑戦』，　情報処理学会第 11 回ｺﾝﾋﾟｭｰﾀｰｾｷｭﾘﾃｨｼﾝﾎﾟｼﾞｳﾑ（CSS2008）（改）
坂本　泰久	日本電信電話（株）情報流通ﾌﾟﾗｯﾄﾌｫｰﾑ研究所	情報工学	『Web サイトにおけるユーザーのふるまいに関する分析手法』 1997-03-12 一般社団法人情報処理学会
佐々木　良一	東京電気大学　未来科学部情報メディア学科教授	情報セキュリティ	『IT リスクの考え方』　岩波新書　2008 年 『インターネットセキュリティ 基礎と対策技術』　オーム社　1996 年

神成　淳司	慶應義塾大学 環境情報学部 准教授	情報工学	『小規模農家向け安定的高収益農業の検討』,情報社会学会論文誌（2008） 『IT』から「AI」へ　匠の技を伝える仕組み」,JA 経営実務,No.814(2010)
手塚　悟	東京工科大学 コンピュータサイエンス学部 教授	情報セキュリティ、電子認証、署名、政府システム	『情報セキュリティの基礎』　共立出版　2011/10 『携帯端末と公共端末の連携による認証システムの提案』　第 10 回情報科学技術フォーラム(FIT2011)予稿集 2011/09
戸田　夏生	（財）地方自治情報センター 理事長	不明	N/A
松本　泰	セコム(株)ＩＳ研究所 基盤技術ディビジョン 認証基盤グループリーダ	情報セキュリティ	N/A
山口 英	奈良先端科学技術大学院大学 教授	情報セキュリティ	『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 年）』（岩波書店、2002 年）

表 3　eCitezen のサービス例

略称	組織名	サービス数	Service (Example)	アプリケーション		※
				Android	iOS	
ACRA	会計企業規制庁	2	ビジネス情報管理	N/A	N/A	
AGD	会計局	2	公務員、年休受給者によって被った医療費の政府負担分請求 政府関係組織に対するベンダーの請求書提出ポータル	N/A	N/A	
AIC	統合ケア庁	8	長期医療に対するケア	N/A	N/A	
AVA	農産物・家畜庁	26	畜産品評会の申請と支払	N/A	N/A	

BCA	建築・建設庁	4	建築プランと情報の調査とコピー作成の申請 オンライン申請と問合せ 建築プランの費用のための e-Payment（電子ペイメント）	N/A	CONQUAS	
CAAS	民間航空庁	7	CAAS が提供する無料のメール通知 航空免許の申請と更新 危険通知等サービス	N/A	N/A	
CEA	不動産仲介業評議会	1	不動産エージェンシーとセールスマン登録	CEA@SG	CEA@SG	必要
CMC	コミュニティ 調停センター	2	コミュニティ調停センターでのボランティア登録 コミュニティ調停センターでの判例登録	N/A	CMC Reports	
CNB	中央麻薬取締局	2	規制物質の輸出入に関する許可申請	N/A	iChoozeLife	
CPE	私立教育審議会	4	私立校と、その授業内容の検索	N/A	N/A	
CPFB	中央積立基金局	18	自営業経営者のための支払いサービス 政府有料育児休業制度のための支払いサービス 負債のチェック 投資や貯蓄の管理	N/A	CPF Tools	
DOS	統計局	6	統計局への支払い 経済や社会に関する統計情報の購入 ビジネス調査依頼とその結果報告	N/A	N/A	
ECDA	幼児開発庁	1	幼児を持つ親や幼稚園の教員等の為の幼児教育や養育などのワンストップポータル	APParent in Sg	N/A	必要
ELD	選挙庁	3	選挙人としての登録 登録者の登録情報の確認	N/A	N/A	
HDB	公営住宅局	24	公営住宅への応募超過状況確認 駐車違反に関する書類提出	Mobile@HDB	Mobile@HDB	必要
HPB	健康促進局	3	学生健康センターの予約と変更 体重チェックや管理サポート 喫煙者のプロファイルに基づき支援	iDAT HPB	iDAT	不要

HAS	保健科学庁	12	医療機器、健康製品、化粧品を扱う店の情報 認可を持つ薬局や漢方薬店の情報 毒物取扱い資格者の情報 タバコ販売店の情報 違法業者の報告サイト 輸血銀行の予約 輸血ドナーの窓口情報	N/A	N/A	
ICA	入国管理局	14	APEC ビジネストラベルカードの申請 NRIC (National Registration Identity Card) のオンライン申請 VISA 延長申請	N/A	N/A	
IDA	情報通信開発局	2	電気通信（販売業）登録や電気事業通信設備登録	eCitizen OneInbox	eCitizen OneInbox	必要
IE Singapore	国際企業庁	1	貿易統計情報公開	globalisingSG	globalisingSG	不要
IPOS	知的財産権庁	3	特許や商標の登録、検索、と取引	IP Equip	N/A	
IPTO	債務超過局	31	個人積立金の利用申請、破産申請 破産免責申請 貸金業免許試験、申請	N/A	N/A	
IRAS	内国歳入庁	3	所得、個人所得税、企業税、固定資産税財産税の支払い	N/A	IRAS SG	
JTC	工業開発庁	2	企業用地、ビル等の売買	JTC m-Statement	JTC	不要
LAB	法律扶助局	2	弁護士の登録 LAB への支払い	N/A	N/A	
LTA	陸運局	18	自動車税支払、更新、Off Peak Car (OPC) と言う週末や夜間・早朝の限られた時間帯でしか基本的には運転できない車両のライセンスの払い出し 車両保険の明細	Land Transport Authority	MyTransport	不要
MAS	通貨金融庁	1	証券、先物を規制の中で取り扱っている個人の記録	N/A	N/A	
MCI	情報通信省	1	シンガポール政府の電子通信プラットフォーム 省庁、公共サービスの連絡先リストを提供	www.gov.sg	www.gov.sg	不要
MFA	外務省	2	eRegister システムによる海外渡航支援	MFA@SG	MFA@SG	不要

MHA	内務省	1	会社や団体の登録	Home Team News	Home Team News	不要
MINDEF	国防省	40	兵役に関する業務全般（登録、活動記録、給与など）を管理	N/A	N/A	
MLAW	法務省	1	海外弁護士試験に関する受験料納付など	N/A	N/A	
MOE	教育省	3	シンガポールの学校のデータベース シンガポールの学生のための教育とキャリア開発	Parents in Education	Parents in Education	不要
MOF	財務省	2	公共部門への請求金額の公開など	Singapore Budget	Singapore Budget	不要
MOH	保健省	5	・病院、老人ホーム、臨床検査室、X 線検査室、診療所、歯科診療所のためのライセンス料の支払い ・医療従事者が薬剤や注意薬物にアクセスすることができます	MOH iHealth Sg	MOH iHealth Sg	不要
MOM	人材開発省	34	事故報告書の修正と提出 企業ライセンス（会計基準等を準拠した有料企業に付与）	ergo@WSH Snap@MOM	ergo@WSH Snap@MOM	不要
MPA	海事港湾庁	1	MPA への料金支払い	N/A	N/A	
MSF	社会家族開発省	21	養子縁組の為の E-Learning	DatingGoWhere	DateGoWhere	
MUIS	イスラム教評議会	5	オンライン神学校 寄付 オンライン証明書の発行 食施設の紹介 ポータルサイト	Office of the Mufti	Office of the Mufti	不要
NCSS	国家社会福祉審議会	1	障碍者、高齢者への共同募金	N/A	N/A	
NEA	環境庁	21	埋葬、火葬、墓地等に関する申請	myENV Lightning@SG	myENV Lightning@SG	不要
NHB	国家遺産局	2	遺産に関する情報提供を 40 個のコースで実施 助成金のための情報とアプリケーション 国家遺産委員コレクションからデジタル化された工芸品や美術品のオンラインリポジトリ	Singapore Heritage Trails	Singapore Heritage Trails	不要

NLB	国立図書館局	5	オンラインでの写真、画像、音声管理	National Library Board	National Library Board SG Memory	不要
NPARKS	国立公園局	11	キャンプ、BBQ、撮影許可等の許可申請 植物園の見学等の予約や申し込み ボランティア応募 遺産ツリーの指定	N/A	sParks*	
PA	人民協会	10	PA に関わる活動、施設関連、関連団体、メンバーとの交流などが全てワンストップでオペレーション出来るサイト 料金の支払いや情報提供など	OurCommunity.SG	OurCommunity	不要
PDPC	個人情報保護委員会	1	テレマの会社から電話を受けないための登録	N/A	N/A	
PSD	公共サービス局	1	求人ガイド 公共サービスの電子雑誌	Post n Poll	Post n Poll Challenge Magazine	不要
PUB	公益事業庁	13	公益事業庁の施設の補修費用請求	Save My Water	Save My Water	
REACH	市民活動監査局	5	電子投票ポータル REACH の運用 最新の世論調査に参加、政府の政策にご意見やご提案を送信、様々な政府機関が公開協議に参加、若者用の関連ポータルサイト	N/A	N/A	
SC	税関	1	罰金、授業料、認定料、その他の手数料の支払い	N/A	N/A	
SCDF	民間防衛局	7	緊急レポート	mySCDF	mySCDF	不要
SDNC	歯科医師評議会	2	歯科医登録 業務証明書、登録、罰金支払いなどの情報更新と関連の支払い	N/A	N/A	
SGH	総合病院	3	診断書の申請 予約 訪問者管理システム	N/A	N/A	
SINGHEALTH	保険サービス	2	SingHealth のクリニックや専門センターとの医療の予定を予約	Health Buddy	Health Buddy	不要

SLA	シンガポール土地管理局	5	シンガポールのストリートディレクトリやその他の地図関連サービス	N/A	N/A	
SMC	医療評議会	1	医師の登録、更新するための支払い	N/A	N/A	
SP	理工学院	6	コースやプログラムへの登録等 卒業者の成績証明書	SP Mobile SP Map 等	SP Mobile SP Map 等	不要
SPC	薬局評議会	1	薬剤師の登録、更新するための支払い	N/A	N/A	
SPF	シンガポール警察	15	私立探偵、警備員の免許申請と更新 芸能活動等の許可申請と更新 武装及び爆発物取扱い申請と更新 自警団への応募	Police@SG	Police@SG	不要
SPRING	規格生産性革新庁	2	機器が消費者保護（安全要件）登録方式で登録されているか確認可能	N/A	N/A	
SSC	スポーツ評議会	3	関連組織、関連者、各施設への連絡先などの情報提供 スポーツ施設の予約 スポーツ･ライブラリから書籍や視聴覚資料をレンタル化	N/A	N/A	
STB	政府観光局	1	トラベルガイド携帯アプリの提供 ライセンス料金の支払いなど	YourSingapore Guide	N/A	
SUBCT	下級裁判所	1	原告の主張文提出	N/A	N/A	
URA	都市再開発庁	12	不動産情報の提供（販売価格、賃貸、空室、民間住宅、商業、工業所有の供給に関する情報） 駐車券の発券	Property Market	Property Market Information	不要
WDA	労働力開発庁	1	仕事検索　（職種、給与、待遇など）	Go Rush!	Go Rush!	不要

※Registration Numberの要否