博士学位論文審査要旨

２０１６年7月１６日

論 文 題 目：　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

学位申請者:　新山　剛司

審 査 委 員：

主　査：	総合政策科学研究科	教授　北　寿郎
副　査：	理工学研究科	教授　金田　重郎
副　査：	京都大学学術情報メディアセンター	教授　斉藤　康己

要　　旨：

2016年1月に施行された共通番号(マイナンバー)制度によって日本に居住する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。

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い、そのリスクに対する対策立案を行うことである。

本研究で明らかにされたことは以下のとおりである。

1)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リスク評価を行った。その結果、「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、また具体的な事例として大学の様々な業務におけるケーススタディにより、それらで起こりうるセキュリティ事故の 90%以上がヒューマンエラーに起因するものであることを明らかにした。

2) その上で、共通番号(マイナンバー)制度におけるヒューマンエラーを分析評価する手法として、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うち 4M-5E と VTA と呼ばれる評価フローチャートを併用した新手法を構築した。この新しいヒューマンエラーの評価手法を茨城県取手市で実際に起こった個人番号(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、分析項目毎に問題点の抽出と背後要因を容易に探索できただけでなく、ヒューマンエラーに対する対策案も容易に導出できることも明らかになった。

本研究の成果は、セキュリティに関する学術分野の進展に寄与したという点で評価できるだけでなく、今後の情報化社会構築におけるきわめて有用な評価手法と基準さらには対策案までも提示可能な指針を示し得たという点で実用面でのオリジナリティも認められる。

よって、本論文は、博士（技術・革新的経営）（同志社大学）の学位論文として十分な価値を有するものと認められる。

総合試験結果の要旨

２０１６年7月１６日

論 文 題 目：　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

学位申請者:　新山　剛司

審 査 委 員：

主　査：	総合政策科学研究科	教授　北　寿郎
副　査：	理工学研究科	教授　金田　重郎
副　査：	京都大学学術情報メディアセンター	教授　斉藤　康己

要　　旨：

○総合試験実施日と時間：

2016 年 7 月 16 日 10：10～11：10

○専門分野に関する試験：公聴会における質疑応答により実施

質疑内容と評価：以下に示したように各質問に的確に回答しており、合格と判断する。

1. 本研究のオリジナリティは何か？

・ マイナンバーの民間サービス利用時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リスク評価を行った結果、「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ことを明らかにした。

・ 民間利用の一般的なモデルとして、エンドユーザ、システムおよびそのユーザ対応やシステムを運用するスタッフという 3 階層モデルを導入し、そのリスク評価を実施した。その代表的な例として、マイナンバーに類似する制度を導入している米国において最も個人情報漏洩事故が最も頻繁に発生している大学を選定し、既に発生した 30 件の個人情報漏洩事故について調査した。そこから得られた知見は以下の通りである。

① 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シミュレーションモデルを構築し、そのモデルに基づきリスク評価を行った結果、想定される事故全体の 90%をヒューマンエラーが占めた。

② エンドユーザに対応する学生やシステムに起因する情報漏えい事故はほとんどなく、システム運用スタッフに相当する職員に起因する 57%、エンドユーザと接する機会の多いスタッフに相当する教員に起因する情報漏えい事故が 40%であることが明らかになった。この結果は、大学の教職員に相当するシステム運用やエンドユーザ対応のスタッフ部門のセキュリティ対策が重要であることを示している。

③ 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最も適しているか実際に発生した情報漏洩事故を適用して比較した結果、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。

④　こ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し、セキュリティ上の問題点とその背後関係を明確にできることを確認した。

・　この手法を用いれば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十分な分析と対策案の立案が可能であることを示した。

2. 本研究の限界およびそれを克服するためのアプローチは？

・　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はできなかった。

・　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。

・　前者については、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情報をベースにして評価を行うこと、また後者に関しても新しい登場人物の役割がより明確になった段階でそれ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。

○語学試験

・　当該学位申請者は、同志社大学を卒業した後、米国カーネギーメロン大学大学院で修士学位を取得している。また、本学位論文に関する査読つきの国際ジャーナル論文と国際会議論文を英語で発表しており、十分な語学能力を有している。

よって、総合試験の結果は合格であると認める。

博 士 学 位 論 文 要 旨

論 文 題 目：　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

氏　　名：　新山　剛司

要　　旨：

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。

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い、そのリスクに対する対策立案を行うことである。後述する従来研究などから、マイナンバーの民間利用について以下の課題が明確となった。

1）民間利用する際に情報漏洩事故が発生する可能性について、既にマイナンバーと同様の公共サービスを提供している諸外国の情報漏洩事故から調査する必要がある。
2）民間利用する事を想定した利用シミュレーションモデルを構築し、そのモデルを用いて情報漏洩事故のリスク評価を実施する必要がある。
3）情報漏洩事故の約8割がヒューマンエラーであるとの報告があるが、情報セキュリティ業界ではまだヒューマンエラー分析の最適な手法が確立されていない。従って民間利用時に情報漏洩事故が発生した場合で、かつその原因がヒューマンエラーに起因したものである事を想定した場合、ヒューマンエラー分析手法の確立と防止策の立案が早急に必要である。

上記3点の課題に対して、本研究より以下の発見を導いた。

1）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と韓国において発生した情報漏洩事故の分析を行ったところ、事故発生箇所が民間企業である割合が両国において、ともに9割近い数値であったことから、マイナンバーを民間利用すると情報漏洩が発生する可能性が極めて高いことが判明した。
2）マイナンバーの民間サービス利用時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リスク評価を行った結果、「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ことが判明した。

民間利用の例として大学を選定し、既に発生した30件の個人情報漏洩事故について調査した結果、情報漏洩に関連した人物別では学生がわずか3%であり、職員が57%、教員が40%であることから、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。

独自の評価基準を策定し、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シミュレーションモデルを構築し、そのモデルに基づきリスク評価を行った結果、想定される事故全体の90%をヒューマンエラーが占めた。
3）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最も適しているか実際に発生した情報漏洩事故を適用して比較した結果、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。この組み合わせ分析

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し、セキュリティ上の問題点とその背後関係を明確にできることを確認した。
この手法を用いれば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十分な分析と対策案の立案が可能である。

本論文の構成は以下のとおりである。

第１章
マイナンバーが民間利用される際に、セキュリティ対策は完全では無いことから、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。また国内外の情報漏洩事故から最新の攻撃手法について調査し、それらがどのような脅威となるか考察した。

第２章
システム上の安全措置（技術）の研究は以前より行われているが、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。従って技術以外の観点から、システムの運用を通して対策の見直しを繰り返していくためのセキュティ活動専門組織が必要であることが判明した。
体制（人や組織）に関する研究について、情報漏洩事故が増加の傾向にあり、更に事故原因におけるヒューマンエラーに起因した事故が全体の 80.5%を占めることから、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進んでいない。従って情報セキュリティ分野に最適な手法の確立が重要である。
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を行った。米国では、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から個人のソーシャルセキュリティナンバー（SSN）を割り出すことが可能だという実験結果が報告された。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。その取り組みと結果を次章で示す。

第３章
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、韓国と日本の住基ネットにおいて発生した情報漏洩事故の比較を行った。その結果を以下に示す。

- 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た。
- 韓国における情報漏洩事故の 86%が民間企業で発生した。
- 日本における漏洩事故の発生箇所は、全て住基カード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ことから運用面での対策が必要であることが明らかとなった。

第４章
第３章の結果から、マイナンバーの民間サービス利用時には情報漏洩事故が発生する可能性が高いことが判明した。従って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リスク評価を行った。その結果、「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

とが判明した。

第５章

民間利用の例として、米国においてソーシャルセキュリティナンバーの情報漏洩事故の発生確立が最も高い場所である大学を選定し、既に発生した 30 件の個人情報漏洩事故について調査した。その結果、情報漏洩に関連した人物別では学生がわずか 3%であり、職員が 57%、教員が 40%であることから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。

独自の評価基準を策定し、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シミュレーションモデルを構築し、そのモデルに基づきリスク評価を行った。その結果、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事故全体の 50%で USB、PC 等の盗難・紛失等が 40%発生していた。この 2 つの事故の合計が全体の 90%を占め、それらはヒューマンエラーであることから、その防止策について考察を進めた。

第６章

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最も適しているか実際に発生した情報漏洩事故を適用し比較した結果、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 では各分析項目が非常に明確となっているため、対策の効果を項目毎に確認出来る利点があった。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向上する利点があった。

第７章

4M-5E と VTA とを組み合わせた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、予想通り分析項目毎に問題点の抽出と背後要因の探索が容易に実施出来たことにより対策案も容易に導き出された。

このことから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この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。

第８章

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。

- 事故が発生した際は、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。

- 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。

- 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つ仕組みを作る。