Doshisha University

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

IT Security in National identification number
Risk evaluation in Commercial Use

Takeshi Niiyama / Toshiro Kita

ITEC Working Paper Series
14-03
June 2014

ITEC
Institute for Technology, Enterprise and Competitiveness

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－

IT Security in National identification number
Risk evaluation in Commercial Use

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 14-03

新山剛司
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
602-8580 京都府京都市上京区今出川通烏丸東入
Tel：075-251-3183
Fax：075-251-3139
E-mail: tn48174817@gmail.com, kbl1003@mail3.doshisha.ac.jp

北 寿郎
同志社大学大学院ビジネス研究科
602-8580 京都府京都市上京区今出川通烏丸東入
Tel：075-251-3183
Fax：075-251-3139
E-mail: tokita@mail.doshisha.ac.jp

キーワード:
情報セキュリティ、リスク評価、リスク分析、マイナンバー、住民票コード、ソーシャルセキュリティナンバー（以下 SSN)、住民登録番号（以下 RRN）

本文内容の専門領域:　情報セキュリティ、公共政策

著者の専門領域:　情報セキュリティ、情報工学

要旨：
2016 年 1 月施行予定の共通番号（マイナンバー）法においてマイナンバーに関連する情報漏洩事故の発生が施行前から最大の懸念事項として関心を集めている。

情報セキュリティ対策としては総務省を中心に政府機関の為の統一管理基準が設けられ、ま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で対策方法や運用について議論されている。情報システムの調達の指針においても同様に厳しいセキュリティ基準が設けられている。

本研究では、既にマイナンバーと同様の公共サービスを提供している諸外国において実施された先行研究や、既に発生した情報漏洩事故から得られた情報を基にマイナンバー施行後に発生が予測される情報漏洩事故について分析した。得られた結果から、今後マイナンバー制度を運用する中央省庁や地方自治体に対して、予見される情報漏洩事故について実践的な提言を試みる予定である。

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

1. はじめに

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

情報漏洩事故を防止するために事前に検討する項目としては、様々な観点からのアプローチが必要である。例えばシステム構築という観点では、総務省が提供する「情報提供ネットワークシステム」と各自治体の既存システムである「基幹系システム」、「内部事務システム」などのシステム群についての「セキュリティポリシー策定」、「システム脆弱性検査」、「緊急時の対応を含めた体制確立」などの複数の項目について慎重に準備する必要があり、その点については総務省中心に進められている。

具体的には「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が政府により構築される予定であり、行政機関を結ぶネットワークの間では、個人情報はシステム毎に「符号」と呼ばれる利用番号を用いられ完全に匿名化されている。情報連携が始まると、この「符号」が各システムのインターフェース（接続）部分まで流通する。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のみ閉じた形で利用される。符号には、マイナンバーや氏名、住所など個人を特定できる情報は一切含まないため、高度なセキュリティシステムと位置付けされている。

総務省「社会保障・税番号制度の概要資料」では、「諸外国の問題点を踏まえた制度」により安心・安全を確保することが記載されている。そのための 2 大措置として「制度上の保護措置」「システム上の安全措置」が定義されており、必要なセキュリティ対策を講じることが述べられている。

（http://www.cas.go.jp/jp/seisaku/bangoseido/pdf/gaiyou_siryou.pdf）

しかしマイナンバーの民間利用では公的個人認証法の民間拡大について、医療機関、金融機関、ショッピングサイトへの利用などが明記されており、各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必要性が生じるが、諸外国の情報漏洩事故が示す通り情報漏洩場所が拡がることから情報漏洩の可能性が高くなることは否めない。

（http://www.kantei.go.jp/jp/singi/it2/senmon_bunka/number/dai2/siryou1.pdf）

また過去の情報漏洩事故においては、システムやセキュリティの専門家が想像もしないアプローチから情報漏洩事故が発生しているケースも存在する。これらの問題意識のもと、本稿では既にマイナンバーと同様の公共サービスを提供している諸外国において発生した情報漏洩事故について考察した。

今後は、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中央省庁や地方自治体に対して、予見される情報漏洩事故について実践的な提言を試みる予定である。

2. 先行研究について

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

一方、石井(2012)は、セキュリティの一般概念である CIA（Confidentiality（機密性)、Integrity（完全性)、Availability（可用性））という三要素を用いてマイナンバー法に関するセキュリティの考え方について考察し、マイナンバー法自体は個人情報保護法などの日本特有の事情に大きく影響され、Confidentiality（機密性）を重視した法案であり、それに違反した場合の法定刑も厳格であることなどを報告している。このことは単にシステムの安全性の観点だけでなく、法制度の観点からも情報漏洩に対する厳格な対応について言及している為、犯罪抑止力となることが期待されている。

このように一見するとマイナンバーにおけるセキュリティに関しては安心できるかのように思われるかもしれない。

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

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。Alessandro(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いて作成した図1を用いてそのメカニズムを詳細に解説する。

Alessandro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。

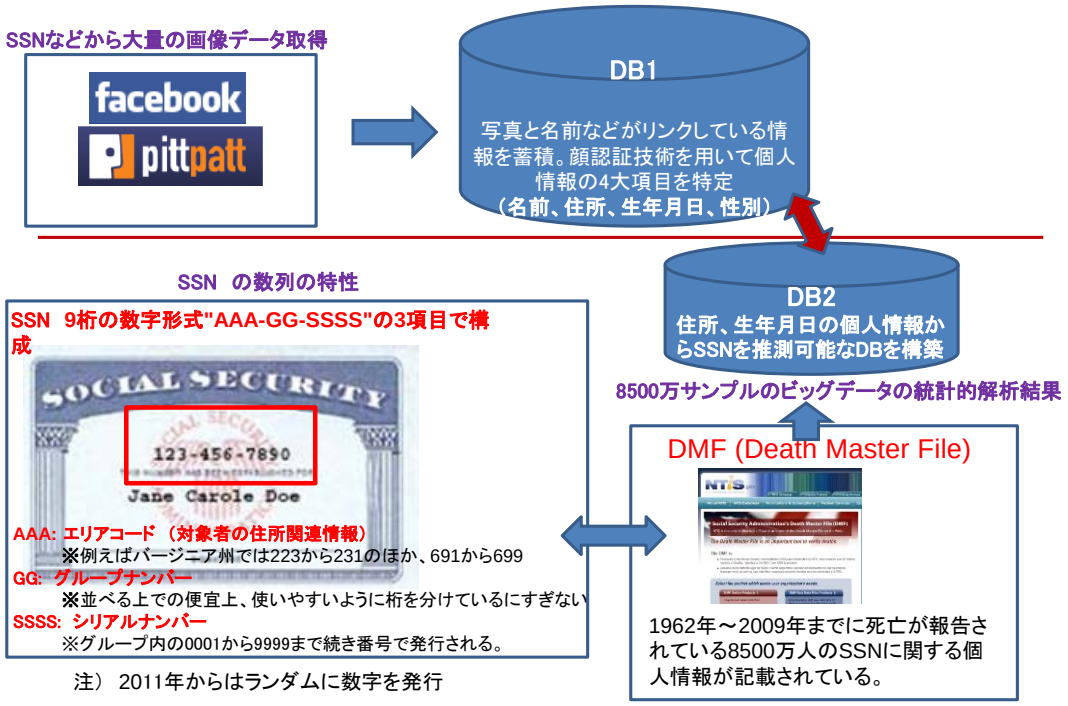


図1　Faces of FaceBookのメカニズム

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））から、1980年以来公表されているDeath Master File（以下DMF ）というDBが存在している（http://en.wikipedia.org/wiki/Death_Master_File）。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Alessandroは指摘している。SSNの番号割り振りの経緯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。

（http://www.socialsecurity.gov/employer/stateweb.htm）

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ことが示唆されている。

マイナンバーにおいて、羅列された12桁の数字を推測可能かどうかについての議論は、将来の研究テーマと位置づけこの場では論じない。ここではマイナンバーに関連した情報漏洩事故について体系的に整理するために、このリスクは番号そのものを推測できる脆弱性、そしてフェースブックなどのソーシャルネットワークで誕生日や出身地など容易にSSN等の個人情報を入手できる脆弱性の存在を示唆するものとして位置付けた。

先行研究では、諸外国の問題点について網羅性が低く、情報漏洩事故が発生する可能性について更なる分析が必要である。

また、新山 (2007)による報告では、一度インターネットに漏洩した電子データを回収することの技術的難易度が主に示されている。

一般的に難易度は次の 4 つに分類される。例えば法律の観点からは、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ーや警察関係者、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。また技術の観点から、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ケースが散見される点が挙げられる。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。

これらの先行研究から、情報漏洩が起きた場合の回復策の困難性を鑑み、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。

3. 諸外国における情報漏洩の調査手法について

3.1 調査条件

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ものとする。

3.2 調査項目について

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。

- 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項
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 メモリなどの各種記憶媒体）や単なる対策不備の場合

4. 米国のソーシャルセキュリティナンバー（SSN）の情報漏洩事故について

4.1 米国における情報漏洩事故

調査条件に基づき、情報漏洩事故を以下のとおり、表1「米国におけるSSN情報漏洩事故一覧」にまとめた。

表1　米国に於けるSSNの情報漏洩事故一覧

No	年	内容	発生場所	脅威種別	技術難易度（高中低）
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したものであることが判明	企業DB（LexisNexis、Dun & Bradstreet、Kroll Background America	ﾊｯｷﾝｸﾞ	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。模倣した声で友人になりすまし、SSNを入手	Face Book	ID詐称音声模倣によるなりすまし	低
3	2011/11	2000年～2005年の間に数学のコースを受講した7093人のSNSNS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SNSNSが漏洩	大学DB（ウィスコンシン大学）	ﾊｯｷﾝｸﾞ	高
5	20011/8	関係者43,000人の氏名とSNSNS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（ディレクトリートラバーサル）	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、SNSNS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SNSNS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

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）	ﾊｯｷﾝｸﾞ	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）	ﾊｯｷﾝｸﾞ	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）	ﾊｯｷﾝｸﾞ	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いるが、上記検索条件では2002年の事故が最も古いものであった。

漏洩事故の内容は様々であるが、発生場所はそれぞれ、大学44%（7件）、企業50%（7件の内訳としてソーシャル・ネットワーキング・サービス（SNS）（Face Book）が1件報告されている）、自治体　6%（1件）であった。

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。

事故の技術的な難易度を分析したところ、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予測できる。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。

ハッキングが全体の38%（6件）を占めている。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。

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。

マカフィーの調査結果では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（図2のような）報告されている。

（http://robertsiciliano.com/blog/2010/10/18/mcafee-reveals-the-top-ten-most-dangerous-places-to-leave-your-social-security-number/）

この報告によると、1位は大学、2位は銀行等金融機関、3位は病院と続き、以下は行政機関、NPO、ハイテク産業、医療施設とある。

Webでの検索結果とこの報告によると、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場所が新たに増えることが容易に予測できるため、広範囲なセキュリティ対策が、自治体と民間企業の連携により、講じられることが求められる。

情報漏洩事故一覧の中で特徴的な事故について次項以降で紹介する。

図2 米国におけるSSN情報漏洩事故発生場所ランキング

4.2 Robert Siciliano の報告

表1「米国におけるSSNの情報漏洩事故一覧」のNo.2は、マカフィーの外部セキュリティコンサルタントでSSN漏洩事故に詳しいRobert Sicilianoによる報告である。フェースブックから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。まず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して、アガサの声を真似てアガサ本人としてサンディーに電話してSSN聞き出すと言う簡単な手法である。この事故の紹介により、Alessandro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SSNを入手できる脆弱性の存在が予測できる。

（https://www.youtube.com/watch?feature=player_embedded&v=8_JOWZ8hQ5Y）

4.3 SSNDOB（Date Of Birth）問題

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が報告されている。
（http://krebsonsecurity.com/2013/09/data-broker-giants-hacked-by-id-theft-service/）

Brian Krebs氏（Washington Postの元記者）が運用するブログ「Krebs on Security」に掲載された情報を基に、筆者独自の理解で作成した図2を用いてこの情報漏洩事故の問題を分析した。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。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が悪意のあるものだと検出しなかったと伝えている。

この手法はハッカー(hacker)と活動家(Activist)を組み合わせたhacktivist（ハクティビスト）と呼ばれる政治的ハッカー集団のUGNaziが明らかにしたものである。システム自体の脆弱性が示唆されるが、高度なハッキング技術が用いられていることから、対策の難易度も高いものが求められる。

この事件では漏洩した個人情報（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。

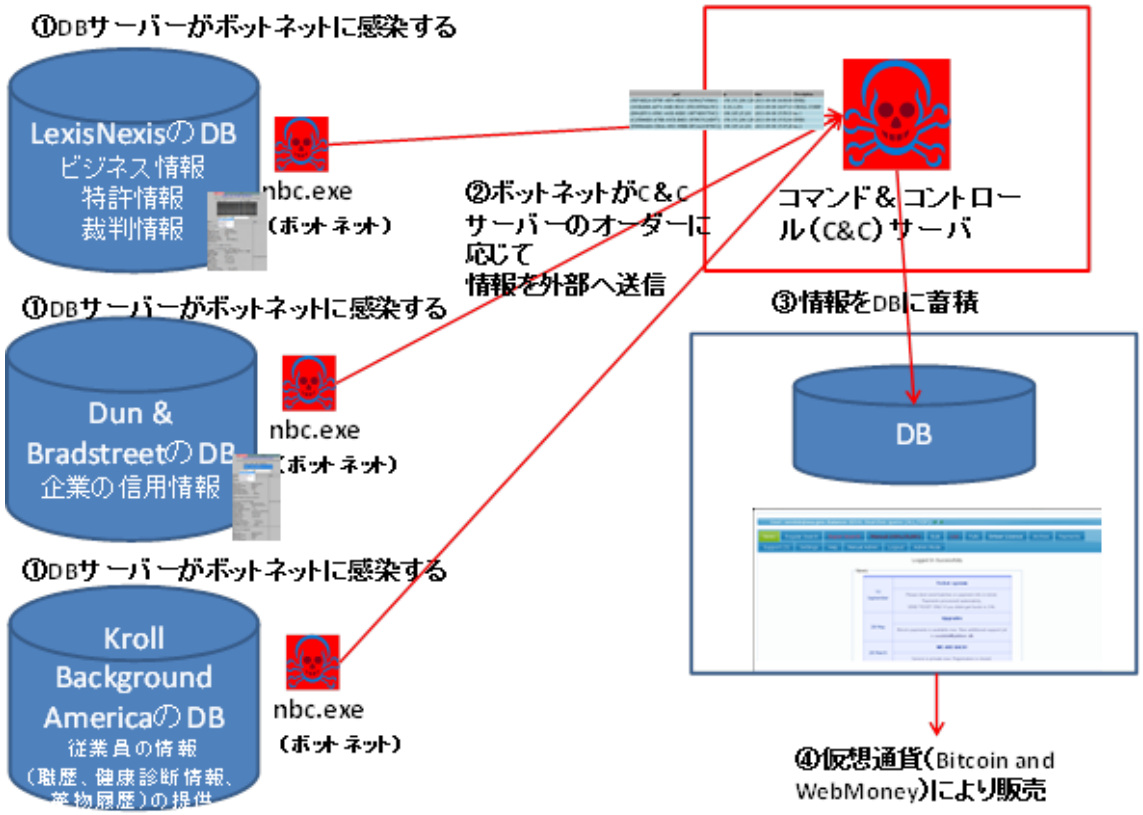


図3　SSNDOB問題

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。

5. 韓国の住民登録番号（Resident Registration Number（以下 RRN））における情報漏洩事故について

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、情報漏洩事故を以下のとおり、表2「韓国におけるRRN情報漏洩事故一覧」にまとめた。

表2　韓国におけるRRN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（高中低）
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SNS「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	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し、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していた	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件が発生	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特徴であり、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の大きな社会現象となったこともあり、特徴的である。

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。

6. 日本で報告されている住民票コードの漏洩事故について

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。

6.1 日本における情報漏洩事故

情調査条件に基づき、情報漏洩事故を以下のとおり表3「日本における住民票コード情報漏洩事故一覧」にまとめた。

表3 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（高中低）
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	自治体 DB （大阪府大阪市天	ID 詐称	低

		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	王寺区）		
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 偽称	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 偽称	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 偽称	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
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 が、路上生活者の男性ら 2 人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つくり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 偽称	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 偽称	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
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 偽称	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 偽称	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。

技術難易度が「低」で発生した情報漏洩事故の一例を挙げる。

6.2　技術難易度が低で発生した情報漏洩事故の一例

筆者の理解で独自に作成した図4に基づき、2006年に北海道札幌市で発生した情報漏洩事故について調査した。

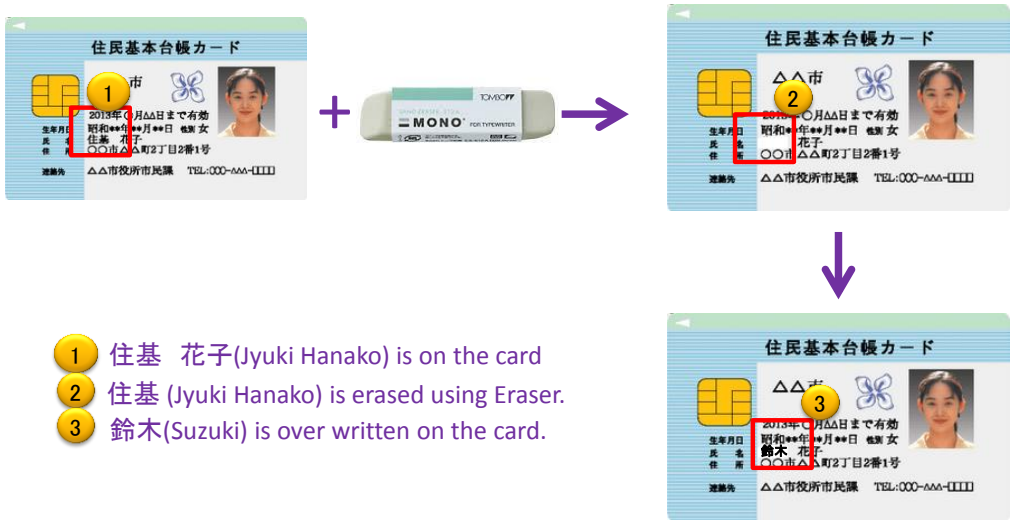


図4　住民票コードにおいて技術難易度が「低」で発生した情報漏洩事故の例

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。

7.　日米韓の情報漏洩事故の比較についての考察

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4「諸外国の情報漏洩事故比較一覧」にまとめた。

日本では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である。

上述2項目より、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。

民間利用が広がると対策場所も拡大し、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。

表4　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（高中低）		
	自治体	大学	企業	ハッキング	盗難	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

*オンライン（SNS、ゲーム、オークションを含む）

**ウイルス感染

以下に先行研究と日米韓の情報漏洩事故の比較についての考察から得られた知見をまとめた。

- 先行研究として、カーネギーメロン大学 Alessandro らのチームによる報告によると、予測困難な情報漏洩事故の可能性を技術的に高度な手法で予見しており、幅広い知見に基づいた対策を講じる必要性を示唆している。
- 米国における 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 搾取と偽称で全体の 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。
- 最後に日米韓の情報漏洩を比較したところ、利用範囲に応じた情報漏洩事故が発生していた。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ことの可能性を示すに十分なデータであった。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。

8. 今後の研究予定

諸外国における情報漏洩事故については、ID 番号の有効利用のランク付けについて経済協力開発機構(OECD)の報告書「Comparison many countries about National Identification Number and its IT security」で報告されており、それら諸外国における情報漏洩事故について更なる調査を実施する予定である。

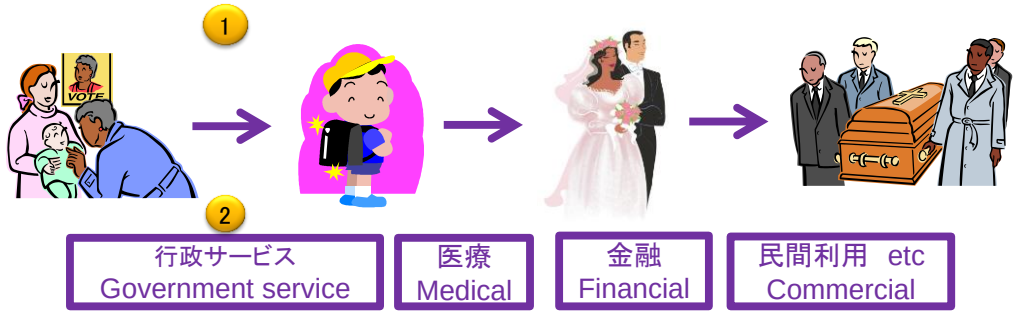
また諸外国における情報漏洩事故の情報等を参考に、人が生まれてから亡くなるまで、どのような形でマイナンバーと関わるのかについてシミュレーションを行い、その際のリスク評価について考察を行う。

図 4 は概要であるが、詳細なライフサイクルを描き、その中でマイナンバーが民間利用の際にどのように流通するかシミュレーションを構築する。その利用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、そのリスク評価について重み付けを行う予定である。

マイナンバー法に関係したセキュリティ対策としては、総務省を中心に、政府機関の情報セキュリティ対策のための 統一管理基準が設けられ、ま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で対策方法や運用について議論されている。情報システムの調達の指針においても同様に厳しいセキュリティ基準が設けられている。

（総務省：
http://www.soumu.go.jp/main_sosiki/jichi_gyousei/daityo/mynumber_rfi.html）

図 4　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



1 モデル構築（ライフサイクルにおいてどのイベントでマイナンバーに関わるか）
Make Model (What events are related to “My Number”

2 利用シーン構築
Make Use-Case

3 リスク評価（諸外国の事故より、場所、攻撃手法、脅威種別により点数付（予定）
（諸外国の事故が日本で起こりえないか検証）
Risk Evaluation based on Criteria made by leakage in Foreign countries
Same incidents will happened or not.

一方でセキュリティ対策については、諸外国（米国及び韓国）においても同様に対策が講じられるにも拘らず、実際に情報漏洩事故が発生している。

第1章で分析した諸外国における情報漏洩事故の結果から、民間利用における情報漏洩事故を予見するためのヒントが多数見つかった。諸外国のおける民間利用の状況や、社会情勢など様々な情報から、来るべくマイナンバーの利用についてのリスク評価に関する研究を計画している。

今後の研究では、総務省、及び関連したITベンダーなど構築する側の立場ではなく、利用者側の視点を中心にリスクの予見に取り組む必要があると考えている。具体的な手法として、施行後にマイナンバーが民間利用される際に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シミュレーションを行い、その際のリスク評価について考察を行う。予見されたリスクについては政府機関、地方自治体に提言し、事前の防止策としての一助となることを切に願っている。

参考文献

＜英文＞

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

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

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

＜和文＞

北寿郎（2004）e-Japan：Composition of Confrontations in Juki-net
情報科学技術レターズ, 情報処理学会 347-350

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