

拡大利用で、 ジワジワ危なくなるマイナンバー

監視社会構築に向けた血税浪費の新たな永久公共事業は破たんの気配

マイナンバーは、国民全員に生涯不変の12ケタに背番号を振り、各人の幅広い個人情報紐付けし国家が束ねるためのマスターキー。直訳すると「私の背番号」。正式には「個人番号」といい、まさに「国民背番号」である。また、「マイナンバーカード」（ICカード）は、電子政府サイト（マイナポータル）にログイン（アクセス）する際のツールであり、「国民登録証カード」「国内パスポート」でもある。政府は、国民に常時携帯させることを狙っている。

マイナンバーで国民の個人情報を紐付け監視し、カードで国民の所在確認をする仕組みは、「監視社会」につながる。憲法13条は「すべて国民は、個人として尊重される」と定めている。もっと憲法学者から異論があってよいのではないか。

2002年に、わが国初の国民背番号制として「住基ネット」が導入された。当時、政府は、国民全員に11ケタの「住民票コード」を振り、「住基カード」を持たせれば、電子政府を実現できるとPR。だが、結局大失敗。これまで初期投資に3,000億円、その後の運営費に年120億円もの血税の支出が続く。そして、今度は「マイナンバー」である。

「マイナンバー」や「マイナポータル」は、「税と社会保障の効率化」や「電子政府の構築」

に必須というのが政府のPR。だが、国民には「監視社会」ツールにしか見えない。マイナポータルは、パソコン（PC）＋マイナンバーカード＋ICカードリーダー3点セットがないと、電子政府サイトにログインできないモデル。だが、スマホやタブレット端末を持ち歩く時代に入り、明らかにガラパゴス化、時代遅れ。

今や、サイトのログインには「パスワード＋Q&A」を使うモデルが世界の主流だ。安全対策には、「ワンタイムパスワード」を使う。豪州の電子政府（myGov）が適例だ。マイナンバーカード交付は頓挫の連続。人口1億3千万の国で、カードを全員に持たせる政策自体が無謀。

「カードの廃止」に舵を切り、サイトにはカードなしでログイン可能とすべきだ。でないと、カード交付は血税浪費の永久公共事業で、住基ネットの二の舞は必至。国民の多くは、4基本情報に加え、顔写真、入れ墨のような背番号が記載され、紛失したら危ないカードなど持ち歩きたくない。

政府は、マイナンバーの官民での拡大利用に意欲的だ。すでに預貯金口座のマイナンバー管理のための法改正をした。だが、人生80年の時代にあって、生涯不変のマイナンバーの汎用は愚策。パスワードを頻繁に変えてなりすまし犯罪に対峙する時代に逆行する。ネット取引全盛の今日、こんな愚策を続ければ、ジワジワ危なくなる。各所へのハッカー攻撃でマイナンバー付き個人情報の大量流出、大被害の発生は不可避だ。わが国が、アメリカや韓国のように番号を悪用したなりすまし犯罪者天国化するのは時間の問題である。

◆主な記事◆

- ・巻頭言～拡大利用で危なくなるマイナンバー
- ・視界不良の電子政府構想
- ・Q&A：個人番号の漏えいへの実務的な対応
- ・アメリカでのなりすまし申告被害者の救済手続
- ・GAO報告書によるなりすましと租税詐欺

2016年10月21日
PIJ代表 石村 耕治

石村耕治PIJ代表に辻村PIJ中村編集局長聞く

視界不良の電子政府構想（マイナポータル）

— 求められる「国民がマイナンバーを監視する」スタンス！ —

話し手 石村 耕治（PIJ 代表）

聞き手 中村 克己（PIJ 編集局長）

【内容目次】

- ◆「番号をJ-LISから直接収集する政策」への転換が必要
- ◆個人番号カード詐欺容疑で全国初の逮捕
- ◆番号やカードの「ネット空間」利用とは
- ◆どうなるわが国の電子政府制度
- ◆ガラバゴス化、時代遅れのマイナポータル
- ◆3点セットを知らない一般市民
- ◆マイナポータルは無用の長物では
- ◆破たんした住基ネットで何を学んだのか
- ◆番号やカード不要のオーストラリアモデル
- ◆マイナポータルへのログインに番号カードを使う愚策
- ◆利便性 対 セキュリティ対策
- ◆データセキュリティにはOTPの利用を
- ◆情報連携（データマッチング）の前途
- ◆情報連携には、直接マイナンバーは使わない
- ◆ガラ系のマイナポータルは時代遅れ
- ◆ジワジワ危なくなるマイナンバー

◆「番号をJ-LISから直接収集する政策」への転換が必要

（中村）住民票コードを導入した住基ネットでは大反対した旧民主党、天下をとった途端に変節し、個人番号（マイナンバー）導入に転じました。その後誕生した自公政権、さらには朝日など大新聞が旗振りをし、市民団体などの反対を尻目に、個人番号（マイナンバー）は翼賛的に導入されました。

そして、今、サラリーマンやOLは、勤務先へ個人番号（マイナンバー）を提出するように求められますが、提出状況はどうなのでしょう？ 年末に向けて改めて取得できなかった番号の要求が予想されますが。

（石村）健康保険や年金関係への個人番号の利用は先延ばしされました。しかし、税金関係では、

年末に向けて改めて取得できなかった番号の要求が予想されますね。

（中村）いつも思うのですが、税務当局や共済組合、健保組合、年金機構とかは、個人番号の発行元である地方公共団体情報システム機構（J-LIS／ジェーリス）から直接マイナンバーを入手できないのでしょうか？

（石村）できると思います。事実、共済組合は、「平成29年1月以降、個人番号の収集を開始する予定になっていますが、平成28年12月31日以前に資格を有する組合員およびその被扶養者の個人番号については、基本4情報（氏名、住所、生年月日、性別）を基に、J-LIS／ジェーリスから一括取得する予定です。」とアナウンスしています。健保組合、後期高齢者医療広域連合なども、同じような方向性を打ち出しています。

（中村）ということは、最初から、事業者に、従業員やその家族の個人番号を提出させる必要がなかったのではないのでしょうか？

（石村）その辺は、役人の狡猾さでしょうか、組合や年金機構側の「賦役はできるだけ事業者側に課す」という「役人／職員ファースト、国民／民間事業者ラスト」の伝統に縛られていることがあるのでしょうか。

（中村）税務署も、そういった状態なのでしょうが？

（石村）税務署は申告納税制度という、「納税者にタダ働きさせる仕組み」に慣れ切っています。事業者、役員や従業員、その家族の個人番号を収集して、マル扶（扶養控除等申告書）にかかせるのは当然と思っているわけです。

（中村）税理士会は、こんな実務を続けていたら、小規模企業に大量の個人番号が「沈殿」してしまう、と感じているのではないのでしょうか？

（石村）そういう税理士もいるでしょう。しか

し、大半は、自分らは「税務署のお手伝いさん」という認識ではないでしょうか？クライアントである「納税者ファースト」の税理士は少ないと思います。税務署と納税者の仲裁人になって、事を丸く収めることが職業と思っている税理士も多いと思います。

（中村）過当競争のなか、税理士は生きるのは容易ではないから、「自分ファースト」になっている・・・（笑い）。

（石村）ともかく、税務署も、個人番号をJ-LIS／ジェーリスから直接収集する政策へできるだけ早く転換する必要があります。税理士会も「クライアント・ファースト」の視点にたって、税務署は個人番号（マイナンバー）をJ-LIS／ジェーリスから直接収集する政策へ転換するように求める必要があります。

◆個人番号カード詐欺容疑で全国初の逮捕

（中村）埼玉県熊谷市で、全国で初めて個人番号カードの不正入手で逮捕者がでましたね。毎日新聞2016年8月30日（火）に、「個人番号カード詐欺容疑で逮捕 全国初」の見出しで、次のような記事が掲載されていました。

マイナンバー制度の個人番号カードを親族になりすましてだまし取ったとして埼玉県警熊谷署は29日、同県熊谷市樋春、無職、A容疑者（49）を詐欺や有印私文書偽造・同行使などの容疑で再逮捕、妻（46）も同容疑で逮捕した。同署によると同カード詐欺容疑の逮捕は全国初。

容疑は2月22日ごろ、親族名義のカード申請書を不正入手。A容疑者の顔写真を張って交付を申し込み、4月22日に市の行政出張所でカードをだまし取ったとしている。

A容疑者は7月28日、この親族のパスポートも不正入手したとして旅券法違反容疑などで逮捕され「悪いことをした時に親族の名前をかたるために入手した」と供述したといい、同署はカード詐欺の動機も追及する。

熊谷市の清水輝義（きよし）市民課長は「親族の住所とA容疑者の自宅が同じで、見た目の年齢も似ていたことなどから、親族と同一人物と信じてカードを交付してしまった」と説明している。

（石村）この記事を読む限りでは、個人番号（マイナンバー）よりは、ICカードの搾取で、サラ金とかへの利用が狙いではないかと思います。住基カードの時代にも、未成年者が、年齢を偽ってナイトライフ・ビジネスで働くために不正取得する

【図表1】個人番号カードのイメージ



ケースなどが散見されました。いわゆる、不法就労する、あるいは不正貸付けを受けるための「なりすまし」です。とくに、これからは、正規に働くには、雇用主への個人番号（マイナンバー）の提示が必要ですから、こうした不正取得が増えることも予想されます。

（中村）ということは、他人になりすますために「本人確認（番号確認＋身元確認）」に使える個人番号カードを搾取したいということですね。

（石村）そうです。これからは、雇用主と通謀し、他人の個人番号カードを借りて就労するケースも増えてくると思います。

（中村）住基カードの場合は、番号（住民票コード）がカード面に書かれていません。これに対して、個人番号カードでは、番号（マイナンバー）がカード面（裏面）に書かれています。この点については、どのような問題があると思いますか？

（石村）現段階では、個人番号（マイナンバー）の民間機関での自由な利用が認められていません。ですから、現実空間での個人番号（マイナンバー）や個人番号カードの悪用、不正使用は、就労などに限定されると思います。

◆番号やカードの「ネット空間」利用とは

（中村）ということは、「現実空間」ではなく、「ネット空間」では、「カード」の利用価値はあるということでしょうか？

（石村）現段階では、電子政府ポータル（マイナポータル）サービスは開始されていません。したがって、一般市民の多くは、「ネット空間」で個人番号（マイナンバー）やカードをどう使うことになるのか、ていねいに説明しても、ほとんど理解できないわけです。政府が想定しているように、番号の民間での自由な利用がゆるされるとすると、さまざまな不正行為が出てくると思います。

（中村）現時点では、自宅のパソコン（PC）から納税申告やさまざまな行政上の電子申請ができ

る・・・など、一般の庶民には、`夢物語、で、想定外の話になってしまうわけですね。テレビの「マイナンバー特集」番組などをみていても、次元が低いですからね。

(石村) 仰せのとおりです。ある業界新聞から、「マイナンバーの課題」について執筆依頼を受けました。そこで、マイナポータル（情報連携基盤）についてふれたのですが、編集者がまったく理解できないわけです。伝統的な現実空間での「番号を使った監視社会」のイメージから抜け出られないわけです。ネットバンキングのような取引をしている人などを除けば、ネット犯罪に個人番号（マイナンバー）がどう悪用されるのかなど、いくらていねいに説明しても想定できないわけです。

(中村) 市民団体の方々の大半も、そんな感じではないでしょうか？CNN編集局には、「CNNニュースの内容は難しすぎて理解できない。もっと庶民向けの記事が欲しい・・・」といった読者投書も届いていますからね。

(石村) まあ、本当は、そうした素朴な感情が大事だと思います。`執筆者と読者との間での認識の乖離、は、`悩ましい、ことだと感じています。例えば、「わが国のマイナポータルでは、ログインに、個人番号（マイナンバー）ではなく、個人番号（IC）カードに内蔵された電子証明書／公的個人認証（PKI=Public Key Infrastructure）を使う・・・」と書くと、大半の読者はもうついていけないわけです。

(中村) 難しいところですね。こうしたシステムを構築するお役人とか、IT企業、学者先生は、血税をふんだんに吸って一般庶民には理解できないものを仕上げて、結果が悪くとも、へっちゃらですからね。

(石村) まあ、ですから、政産官学の連中は好き勝手にやられているのでしょうか。2002年に、わが国初の国民背番号制として「住基ネット」が導入されました。当時、役人やIT業界、彼らに協力した金魚の●●●のような学者は、国民全員に11ケタの「住民票コード」を振り、「住基カード」を持たせれば、電子政府を実現できると持ち上げました。しかし、結局大失敗でした。

(中村) これまで初期投資に3,000億円、メルトダウンしたシステムのその後の運営費に年120億円もの血税の支出が続いていますね。

(石村) しかし、このシステムを立ち上げた政産官学の連中は、誰一人として責任を取らないわけ

です。まさに、この連中は、血税をふんだんに吸って一般庶民には理解できないものを仕上げて、大失敗したあげくの果てに、責任は回避するわけです。

(中村) 周りを見渡すと、原発、東京都の築地市場など各種の再開発事業等々、例をあげればきりがありませんが・・・。

(石村) 残念ながら、キャンパスへ行くと、金魚の●●●のような連中がウジャウジャいるわけです。役人から声がかかると偉くなった気になるようです。また、役所や役所の御用聞きで生きてきているシンクタンクなどから天下ってきて、役所のエージェント（手先）のような立ち振る舞いをして自己満足している連中も多いわけです。やはり、こうした政産官学がスクラムを組んだ巨悪を告発するには、素朴な市民パワーが必要なわけです。

◆どうなるわが国の電子政府制度

(中村) 素朴な市民パワーに応えられるように議論ができるかどうか自信がありませんが。電子政府（e-Gov, e-Government）制度とは、従来の縦割り行政を排し、ネット上で各種電子行政サービスを統合し「ワン・ストップ・サービス」を実現しようという構想です。行政の効率化、利便性の向上に結び付くはずのプランなわけです。

(石村) ところが、「理想と現実」の乖離が大きすぎますよね。

(中村) 仰せのとおりですが、その辺はさておいて、共通番号（個人番号・法人番号）を利用した電子政府制度（情報提供ネットワークシステム／マイナポータル）を活用することで、本当に、ネット経由で各種の行政申請（申告）をしたり、さまざまな情報を受け取ったりすることができるようになるのでしょうか？

(石村) 大失敗した住基ネットの例をみる限りでは、そうなる可能性は低い、といえます。もっとも、電子政府サービス（マイナポータル／情報提供ネットワークシステム）、現時点では、①本人確認と②情報連携に加え、③「情報提供等記録開示機能」【複数の行政機関内で行われた自分の情報のやり取りのチェック】に限られています

が・・・。

(中村) 現実には、この程度の限られた内容のメニューですら、開始時期が延期されましたが・・・。

(石村) 「机上の空論」が闊歩している証拠です。

(中村) 私もそう思います。現在、個人番号（マ

イナンバー)の付番作業は一段落、通知カードの配付問題も一応沈静化しました。

(石村) 一方、個人番号カードの交付も、J-I S/ジェーリスでの不具合が続き、何度も頓挫しましたが・・・。

(中村) ともあれ、これも8月末現在では、交付準備が97%完了したと報道されています。総務省によると、全国1741自治体のうち、1694自治体がカード発行の通知書の送付を完了したとしています。

◆ガラパゴス化、時代遅れのマイナポータル

(石村) 一時は、住民が個人番号カードを申請しても、発行通知書を受け取るまでに数か月かかっていましたから、問題状況は脱したということでしょう。しかし、多くの市民は、個人番号カードを「本人確認(番号確認+身元確認)」に使うために取得していると思います。大方は、行政への電子申請に必須のツールだとは思ってもいないわけです。

(中村) 個人番号カードは、任意取得が原則ですよ。にもかかわらず、政府がカード交付に躍起になっているのはなぜなのでしょう。

(石村) この背景には、政府ポータルサイト/マイナポータルにログイン(アクセス)するのに、個人番号(マイナンバー)カードが必須のツール(道具)になっているからです。

(中村) つまり、個人番号カードがないと、各人は電子政府の利便性を実感できないからということですよ。

(石村) そうということです。個人番号カードがな

【図表2】本人確認【個人番号確認+身元確認】の方法の選択

【個人番号の確認】	【身元の確認】
一般的な方法 ①通知カード OR ②住民票(番号付き)	一般的な方法 ③運転免許証 OR ④パスポート
⑤個人番号カード	

いと、各人は電子政府サービスを利用できないデザインになっています。ただ、先ほどからお話しているように、一般市民には、この辺の理解はまだです。

(中村) 一般市民は、まさに、個人番号があれば、本人確認(番号確認+身元確認)は楽にできるといった程度の認識ですね。意識の高い市民レベルでは、「個人番号カードを「国民登録証カード」「国内パスポート」を携行させようと画策している、と見ています。私の知る限りでは、個人番号カードが、電子政府サービス(マイナポータル/情報提供ネットワークシステム)へのアクセス(ログイン)に必須のアイテムという認識を持っている人はほとんどいないと思います。

(石村) ただ、マイナポータルでは、IC仕様の個人番号カードだけが必須アイテムというだけではありません。さらに「ICカードリーダー」を持っていないと、マイナポータルサイトにログイン(アクセス)し、電子行政サービス(現時点では情報提供等記録開示機能に限りま

す。)

【図表3】ICカードリーダーのサンプル



ならない仕組みになっています。

(中村) ということは、マイナポータルサイトの利用を希望する人は、個人番号カードの他に何が必要となりますか？

(石村) 利用希望者は、個人番号(IC)カードを取得し、ネット環境が整っており、パソコン(PC)があり、さらにICカードリーダーが必要です。

(中村) つまり、「ICカード+パソコン(PC)+ICカードリーダー」の3点セットが必要ということになるわけですね。

(石村) 仰せのとおりです。ICカードリーダーなど、どの世代でも見たこともない人も多いのではないのでしょうか？住基ネットで、電子政府サービスが普及しなかった大きな原因の1つが、ICカードリーダーがないと電子政府サービスにログインできない、ところにあったわけですが・・・。

(中村) マイナポータルでは、懲りずに、また同じことをやっているわけですね。

(石村) そうです。まるで他人事・・・。失敗しても血税が転がり込んでくるITハイエナ企業の

いいなり・・・。

◆3点セットを知らない一般市民

(中村) 政府広報では、「マイナンバーを活用して、他機関と情報連携を行い、定期報告の添付書類など皆さま方の負担が軽減され利便性が向上します。」とPRしていますが。

(石村) 個人番号（マイナンバー）さえあれば、誰でも電子政府（マイナポータル）サービスが利用できるように響きです。

(中村) こうしたPRの仕方は大問題ですよ。

(石村) 個人番号ICカードがあっても、ネット環境が整い、パソコン（PC）やICカードリーダーがないと、電子政府サービスは利用できないことなど、ほとんどの市民は知らないわけです。

(中村) 逆に、3点セットが揃わないと使い物にならないと知ると、一般市民は、`利便性の悪いマイナポータルなど要らない、と騒ぎ出すかも知れませんね。

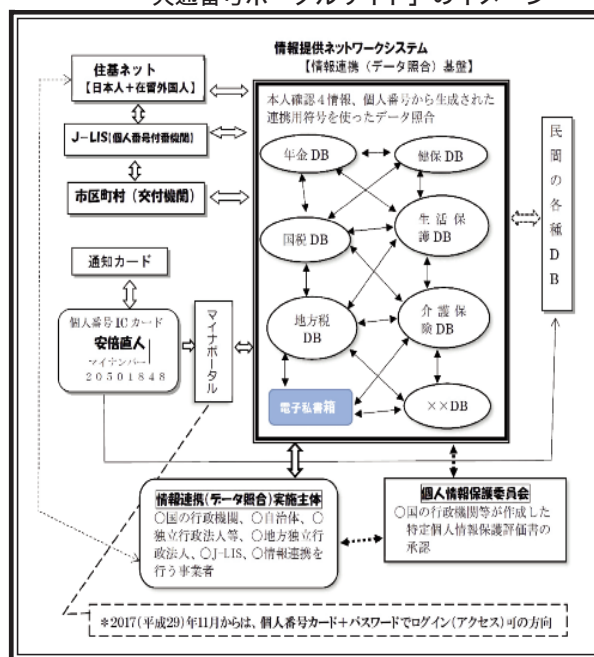
(石村) まあ、簡単にいえば、普及しないということでしょう。いずれにしろ、マイナポータルサイトを一般の市民が利用できるようになるには、相当の時間と教育が必要となります。人口の高齢化とともに、誰でも電子政府サービスが使いこなせるようになるには、いわゆる「デジタルデバイド」【インターネットやPCなどの情報技術（IT=information Technology）を利用したり使いこなしたりできる人と、そうでない人の間に生じる、貧富や機会、社会的地位などの格差】の解消も大問題で、相当の支援が必要です。

◆マイナポータルは無用の長物では

(中村) マイナポータルや情報連携（データ照合）の稼働も延期になりました。システムを管理運営する特殊法人J-LIS／ジェーリス（地方公共団体情報システム機構）が諸悪の根源のような論調ですが、どうなのでしょう。

(石村) 今年（2016年）1月のマイナンバー制度稼働後、J-LIS／ジェーリスでの個人番号カード・システムの不具合が相次ぎ、カード交付もトラブル続きなのは事実です。8月末には正常化したようです。これまでのところ、発行総計で1千万件を超える程度です。しかし、問題の根源はJ-LIS／ジェーリスにあるのではなく、

【図表4】日本の個人番号と番号カードを使った政府の「共通番号ポータルサイト」のイメージ



1億3千万人にも及ぶわが国の人口規模にあるのではないかと思います。

(中村) 人口が100万人前後の自治体で行政ICカードを発行するのはわけが違うということですね。

(石村) 仰せのとおりです。人口が1億3千万人にも及ぶこの国で、全員に個人番号カードを持たせようとする発想自体にムリがあります。政府が構想しているマイナポータルは、全国民にかかわる巨大なシステムです。こうした巨大なシステムの管理運営を、役所からの天下りが司令塔を務める自治体共同の組織であるJ-LIS／ジェーリスに委ねること自体が問題の根源です。一言でいうと`荷が重すぎる、ということです。

◆破たんした住基ネットで何を学んだのか

(中村) わが国最初の電子政府構想である、3点セット【ICカード＋パソコン（PC）＋ICカードリーダー】住基ネット（住民票コード、住基カード）は、3,000億円もの血税をブラックホールに注ぎ込んだあげくメルトダウンしました。3点セット【ICカード＋パソコン（PC）＋ICカードリーダー】が必須のアイテムとなっていることが失敗の主な原因の1つでしょう。ところが、新たな電子政府構想であるマイナポータルでも、ログインには前述の3点セットが必須のアイテムになっています。

(石村) ある意味では、時代遅れのデザインにな

っているといえます。

(中村) このまま当初の設計図どおりにすすめて行けば、住基ネットの二の舞になるは必至ですね。マスメディアのなかには、番号と番号カードを使った電子政府制度は、旧ソビエト連邦のバルト三国の一つであるエストニアでは、うまくいっているとPRしているところもあります。あんな小国にできるのに、IT大国の日本で、なぜこんなにトラブル続きなのかといったトーンですね。

(石村) 確か、〃財界のPR紙とやゆされる日経、の論説委員(?)が書いた提灯記事だと思えますが。エストニアの人口は134万人程度です。こんな自治体が国家に変身したような小国のサンプルは、1億3千万の人口を擁する日本には参考にならないわけです。

(中村) 破たんした住基ネットで何を学んだのでしょうか。わが国の新たな電子政府モデル(マイナポータル)では、全員に個人番号カードを持たせようとするところが最大の欠陥だと思います。

(石村) しかし、IT企業からすれば、1億3千万人も〃宝の山、は、〃カネのなる木、です。生死、結婚、異動等々、そのたびのICカードの需要がある。世界的にはICカードを使わない電子政府モデルが主流になってきていても、ICカード需要はそう簡単にあきらめきれないのでしょう。

(中村) ICカードを使う電子政府モデルでは、スマホ端末などからは電子政府サービスのログインができないのは、当然わかっているやっているとことです。

(石村) そうだと思います。しかし、〃番号カードの発行、という、制度導入の入口付近でこれだけトラブっている日本モデルは、できるだけ早く大幅に見直さないと、うまく軌道に乗せられないことははっきりしてきていると思います。

(中村) 天下御免の中央のお役人の考えを変えさせるのは至難ですね。

(石村) 日本モデルでは、マイナポータルへのログインに利用できる端末は、パソコン(PC)だけです。PCには、ICカードリーダーを取り付けることが可能です。ところが、政府の計画では、将来的には、利用端末を、スマートフォン(スマホ)、タブレット、ケーブルTV、コンビニ端末などへ広げていく方向です。スマホやタブレットのように、端末機器によっては、ICカードリーダーを取り付けることができない、あるいは、装着すると機能不全を起こすものもあります。

(中村) ということは、個人番号カードを使わな

いでも、マイナポータルにログインできる仕組みを用意する必要があるということですね。

(石村) 端末機器の多様化の波に乗れない日本の電子政府モデルは、いずれは破たんすると思います。利便性とデータセキュリティ対策との調和が重い課題です。個人番号カードの交付がうまくすすまないのなら、これを好機ととらえ、いつそのこと、オーストラリアのような個人番号ICカードを使わない電子政府(マイガブ/myGov)モデルに移行すべきです。

(中村) 私は、石村代表らと昨年秋、オーストラリア税制視察に行き、オーストラリア国税庁(ATO)のホワイト副長官から、電子政府モデル「マイガブ/myGov」や、出来てホヤホヤの「myTax」についてレクチャーを受けています。したがって、若干知識はありますが、読者のために、オーストラリアモデルを参考に、番号カード不要の電子政府モデルについて説明してください。

◆番号やカード不要のオーストラリアモデル

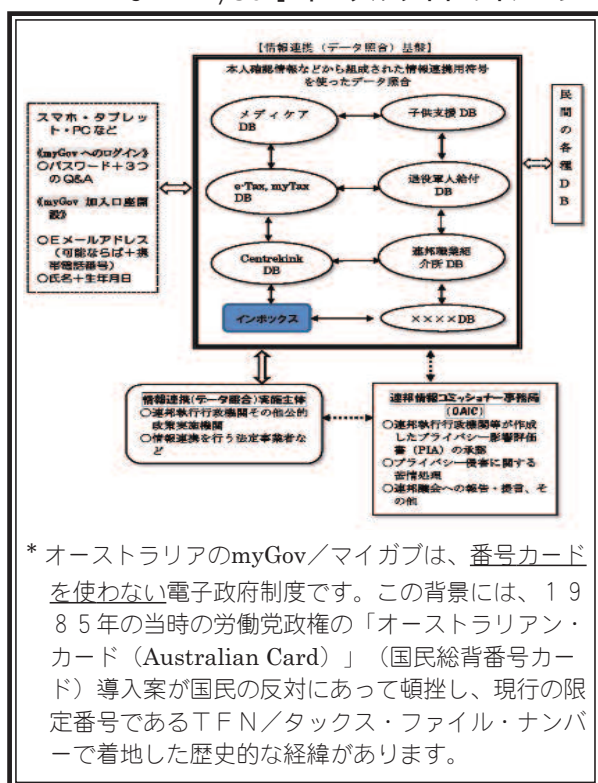
(石村) 分かりました。オーストラリアの電子政府モデル(マイガブ/myGov)については、CNNニュースで、すでに何度か紹介しています。このオーストラリアの電子政府モデルでは、ポータルサイトへのログインにIC仕様の番号カードは使っていません。「7ケタのパスワード+3つのQ&A」でログインできます。

(中村) オーストラリアの電子政府モデル(マイガブ/myGov)では、スマホやタブレットなど多様な端末を使ってポータルサイトにログインできるように、番号ICカードやICカードリーダーは必要ないわけですね。

(石村) そうです。政府ポータルサイト(マイガブ/myGov)には「7ケタのパスワード+3つのQ&A」でログインします。ですから、日本でも、オーストラリアモデルを参考にして、「パスワード+Q&A」ポータルサイトにログインできるようにすればよいわけです。IC仕様の番号カードを使うのをやめるべきです。

(中村) マイナポータル(日本モデル)では、少なくとも1億枚ものICカードが発行されないと、大多数の国民が電子政府サービスを楽しむことができません。ただ、見方を換えれば、日本モデルは、まさに〃IT利権ファースト、のモデルそのものですね。

【図表5】オーストラリアの背番号と番号カードを使わない「myGov」ポータルサイトのイメージ



（石村）仰せのとおりです。国民の利便性は後回しのモデルですね。オーストラリアの人口は2,300万人です。この程度の人口でも、全員に政府ポータルサイトにログインするためのカードを発行するのは、大規模な公共事業になります。ところが、1億3,000万の人口を抱える日本では、生死や異動の数が膨大になります。それこそ、IC仕様の番号カード発行は、大規模な永久公共事業になります。

（中村）個人番号カード発行を延々と続けることで、IT利権、をはかるだけでなく、永久の公共事業を狙っているわけですね。

（石村）仰せのとおりです。今や、スマホやタブレット端末全盛の時代です。将来を見据えて、ICカードリーダーのいる個人番号カードを使わないでも、マイナポータルにログインできる電子政府モデルが求められているわけです。血税のムダ遣いも防げます。

◆マイナポータルへのログインに番号カードを使う愚策

（石村）誤解を解くために言っておきますが、わが国の電子政府モデル（マイナポータル）においては、ログインに個人番号カードを使うことにな

っています。しかし、12ケタの個人番号／マイナンバーそのものを使うわけではないのです。つまり、使うのは、個人番号カードのなかのICチップの部分です。

（中村）つまり、個人番号カードのICチップに登載された公開鍵方式のPKI（電子証明書／電子印鑑機能／公的個人認証）を使うわけですか？

（石村）そうです。成りすましの防止、安全なログインがねらいです。ところが、オーストラリアモデルでは、政府ポータルサイト（マイガブ）へのログインには、PKI（電子証明書／公的個人認証）を使っていないのです。代わりに「パスワード+3つのQ&A」を使っています。

（中村）つまり、まず、政府ポータルサイト（マイガブ）のログインには、パスワード+3つのQ&Aを使うわけですね。

（石村）そうです。ログインができ、さらに例えば納税申告をする場合には、課税庁（連邦国税庁／ATO）のサイトにアクセスします。そのうえで、納税者番号（TFN／タックスファイルナンバー）でログインし、申告作業をするわけです。したがって、わが国とは異なり、オーストラリアの場合、原則として、政府ポータルサイトへのログインに「PKI」（Public Key Infrastructure／電子証明書／公的個人認証）を使っていないわけです。ちなみに、わが国では「JPKI」と呼んでいます。

◆利便性 対 セキュリティ対策

（中村）わが国では、税務行政分野では、すでに電子申告（e-Tax、eLTax）においてPKI（電子証明書／公的個人認証）が格納されたICカードを使ってきています。税理士などでは、PKIが格納された税理士会発行のICカードを使って電子申告を続けてきています。

（石村）確かに、税理士を使った代理人申告では、PKIが格納されたICカードを使った電子申告は何とか軌道に乗りました。しかし、税理士を使わない、納税者の本人申告では、PKIが格納された住基ICカードを使った電子申告は余り普及していません。

（中村）3点セット【ICカード+パソコン（PC）+ICカードリーダー】を使う電子申告は、利便性が悪く、非効率なのが原因ですね。

（石村）そうです。ところが、新たな電子政府モ

デルであるマイナポータルでは、また、同じ3点セットを使うというのですから・・・。

（中村）大失敗した電子政府構想である住基ネットからまったく学んでいませんね。

（石村）政府ポータルサイトへのログインにPKIが格納された個人番号ICカードやICカードリーダーを使うのは、「データセキュリティ確保」、つまり「安心・安全」の面からはプラスのように見えます。しかし、「利便性」の面ではマイナスですね。

（中村）利便性をとるか、セキュリティをとるかの問題になってきますね。

（石村）ただ、わが国での電子申告の経験からして、パソコン（PC）をベースに番号ICカードやICカードリーダーを使う電子政府モデルは、スマホ、タブレット端末全盛の時代に入り、利用は広がらないのは目に見えています。

（中村）個人、とくに一般のサラリーマン／給与所得者の場合、年一回の確定申告、還付申告のために、ICカードを取得し、ICカードリーダーまで備えて電子申告をするのは、苦痛ですよ。法人の場合、多くは税理士関与電子申告です。この場合は、税理士会などが発行しICカードに格納された税理士の電子証明書／電子印鑑だけ電子申告ができます。

（石村）以前は、税理士関与電子申告でも、税理士と納税者双方の電子証明書／電子印鑑が必要であったものを、簡素化した経緯があります。それで、税理士関与の電子申告も大きな伸びを記録しました。個人納税者についても、課税庁は、電子証明書／電子印鑑を使わない効率化した電子申告を導入しましたね。

（中村）平成10年度くらいからでしたか、税務署がタッチパネル方式による自動申告書作成機を設置し、銀行のATMのように、画面上の該当箇所に触れていけば、簡単に申告書が作成できるように対応しました。税務署の確定申告書等作成コーナーでは、画面案内に従って金額等を入力することにより、確定申告書等を作成することができ、作成したデータはe-Taxで送信することがで

きます。ということは、ICカードがネットとなっているからです。

（中村）税務行政分野での電子申告の経験からして、番号カードやICカードリーダーを使う電子政府モデルでは、電子行政サービスの利用は広がらないのははっきりしています。

（石村）スマホやタブレット端末にICカードリーダーを装着するのでは、手軽さ、利便性の面でマイナス効果だけです。

（中村）スマホにICカードリーダーを装着したら、不具合を起こす可能性もありますからね。

（石村）これまでの体験などを織り込んで考えると、わが国でも、政府ポータルサイトへのログインには、PKIが格納されたICカードを使うのをやめて、オーストラリアモデルに倣って、「パスワード＋3つのQ&A」を使う方向をめざすべきでしょう。

（中村）これによって、ICカードリーダーも不要になり、PCだけでなく、スマホやタブレットなど多様な端末を使って、政府ポータルサイト（マイナポータル）にログインできるようになりますからね。

（石村）PKIが格納されたICカードを使ってホテルの予約をすることを義務づけたらどうなるか考えたら、一目瞭然です。

（中村）誰もネット予約はしなくなるでしょうね。

（石村）データセキュリティよりも、利便性を優先すべきです。オーストラリアの若い世代は、PCよりも、スマホ、タブレット端末に利便性を感じているようです。

（中村）近年、新たに導入された電子申告の一種である「マイタックス（myTax）」は、スマホ、タブレット端末を通じた申告を可能としたものですね。

（石村）そうです。わが国とは異なり、オーストラリアは、年末調整もないし、原則全員確定申告をする国です。若い世代向けに「マイタックス（myTax）」を立ち上げ、できるだけ簡素なスマホ、タブレット端末を通じた申告を可能にした意味は大きいと思います。

【図表6】タッチパネル方式による自動申告書作成機



◆データセキュリティにはOTPの利用を

（中村）オーストラリアでは、所得税の電子申告を、スマホ、タブレット端末を使ってでき、政府ポータルサイト（myGov）にログインする際には、「パスワード＋3つのQ&A」を使うわ

【図表7】タブレットでマイガブにログインできる！



けですね。しかし、この程度のデータセキュリティでは、不安を感じる人もいると思います。この場合、PKI(電子証明書／公的個人認証)に代わるセキュリティ対策は採られていないのでしょうか？

(石村) オーストラリアの場合、不安と思う人は、「パスワード＋3つのQ&A」に代えて、「ワンタイムパスワード／オーテーピー（OTP＝one time password）」を使うことも可能です。オーストラリアでは、「単一回利用コード（single use code）」、「マイガブ・セキュリティ・コード（myGov security code）」と呼んでいます・・・。

(中村) ネットバンキングなどで幅広く使われているセキュリティ対策で、わが国では、使い捨てパスワード、と呼ばれているものですね。

(石村) そうです。「ワンタイムパスワード（OTP）」、「単一回利用コード」とは、一定期間ごとに自動的に新しいパスワードに変更され、しかも、一度しか使うことができないパスワードです。一度使ったパスワードは、再度利用できないことからセキュリティが高いわけです。また、固定パスワードと比べると、ワンタイムパスワード（OTP）、単一回利用コードは、一定期間ごとに自動的に新しいパスワードに変更されることから、悪用されるリスクが低いわけです。一般に、スマートフォンアプリが選ばれます。

(中村) オーストラリアでは、「ワンタイムパスワード（OTP）」、「単一回利用コード」は、「パスワード＋3つのQ&A」に代えて使うということですね。手続は簡単なのでしょうか？

(石村) 基本はネットバンキングの場合と同様です。国内用の携帯電話番号をもっているオーストラリア市民であれば、政府ポータルサイトであるマイガブ（myGov）への加入時、あるいはそれ以降に、マイガブ所管のサイトにアクセスし、電子申請をすれば、誰でも単一回利用コード（マ

イガブ・セキュリティ・コード／ワンタイムパスワード（OTP））を利用できます。

(中村) 利用は一般化しているのでしょうか？

(石村) これは完全に本人の選択ですし、利便性とセキュリティのバランスをどう考えるかの問題だと思います。課税庁（ATO）とかは、利用するか同課の選択を完全の本人に任せているようです。

(中村) ということは、オーストラリアの場合は、電子政府、政府ポータルサイトのセキュリティ対策には、厄介なPKI（電子証明書／公的個人認証）をまったく使っていないのでしょうか？石村代表と昨年秋にオーストラリアへ行き、ATOのホワイト副長官からmyTaxレクチャーを受けた際に、私も、気になっていた点でしたが。

(石村) オーストラリアでは、電子健保（eHealth）プログラムを扱う省庁、その政策実施機関（メディケア）などでは、医療機関との間での機微情報（センシティブ情報）のやりとりに、PKI(電子証明書／公的個人認証)を使っています。一方、課税庁（ATO）と納税者、税理士（tax agents）、税理士法人（Tax Agents Pty Ltd）などとの間では、インターネット接続を提供する専用線接続などを使っているようです。利便性を優先するためようです。

(中村) ただ、どんなにデータセキュリティを高くしても、すぐに破られる時代ですからね。

(石村) わが国での経験からも分かるように、絶対に安心・安全なセキュリティなんてありません。「ワンタイムパスワード／OTP」も同じでしょう。マルメール、ランサムメール等々・・・。まさに、イタチごっこです。

◆情報連携（データマッチング）の前途

(中村) わが国では、「情報連携（データマッチング）」を始める方向ですが、各国の電子政府モデルをみて見ても分かるように、政府ポータルサイトの構築がベースとなりますね。

(石村) そうです。ただ、デザインやコンテンツは、国により異なります。わが国の情報提供ネットワークシステムとか、オーストラリアのマイガブ（myGov）は、一般に「情報連携（データ照合）基盤」と呼ばれます。この名称からも分かるように、コンピュータを使った個人情報照合する機能を持ちます。

(石村) 情報連携（データ照合）は、例①国の複

数の行政機関内、例②複数の自治体間、例③国と自治体の機関間、さらには例④国や自治体と各種公的政策実施機関（例えば、日本年金機構、日本学生支援機構などとの間における個人情報のやり取りが検討されています。

（中村）つまり、生活保護の申請をすると、③国税情報と市町村の情報を照合して適格者かどうかをデータ審査ができるといった具合ですね。

（石村）そういった照合が可能になる方向です。また、高校生や大学生が日本学生支援機構の学資ローン（奨学金）の申請をします。この場合、本人のマイナンバー、保護者のマイナンバーの提示を求め本人確認をします。そして、仮に、本人の返済が滞ったとき、返済猶予を申請してきたときには、例③本人の国税情報（所得）などとデータ照合して、本当に返済能力がないのかなどをチェックすることができることになる方向です。これは、オーストラリアの「卒業税／授業料後払いプログラム（graduate tax program／higher education loan program／HELP）をモデルとしたものです。（HELPについて詳しくは、国税制研究第2号（2016年）21頁以下参照。Available at: <http://jti-web.net/archives/category/kikanshi>）

（中村）つまり、情報提供ネットワークシステムとは、悪いことしていなければ怖くない「ソフトな監視社会、構築の基盤をつくるということですね？

（石村）まあ、素敵な表現です（笑い）。ともかく、情報提供ネットワークシステム（マイナポータル）とは、社会インフラとして「情報連携（データ照合）基盤」をつくるわけです。この基盤を使って、さまざまなことが検討されています。図示すると、【図表8】のとおりです。

（中村）わが国の電子政府制度（政府ポータルサイト／マイナポータル）には、「情報連携（データ照合）基盤」をベースに、いろいろなメニュー（機能）が盛られているわけですが。わが国の1億3,000万人という人口規模を考えると、計画どおりすすめられるのでしょうか？

（石村）住基ネットと同じように「破たん」の臭いがプンプンしてきます。まあ、役人は、「失敗しても、所詮、投下資本は「税金、」という感覚ではないかと思います。

◆情報連携には、直接マイナンバーは使わない

【図表8】マイナポータルに盛り込むことが計画されている主な機能

①情報提供等検索機能
【情報主体が、行政機関等の間で行われた自分の情報のやり取りをチェックする機能】
②自己情報表示機能
【情報主体が、行政機関等が保有する自分の情報を確認する機能】
③お知らせ表示機能
【税金の申告期限、予防注射、その他のお知らせを受け取る機能。いわゆる「電子私書箱」機能】
④ワン・ストップ・サービス
【住所変更届出をすれば、すべての機関へ通知できる機能、国税・地方税・年金等の窓口の一元化機能など】
⑤その他

（石村）いずれにしろ、政府ポータルサイト／マイナポータル内での情報連携（データ照合）に直接個人番号／マイナンバーは使いません。「符号」を使うことになっています。これは、住基ネット最高裁判決（平成20年3月6日判決・民集62巻3号665頁）が、「直接住民票コードを使って情報連携を行わない限り違憲とはならない」とした趣旨を織り込んだ結果です。

（中村）言い換えると、直接個人番号／マイナンバーを使って情報連携（データ照合）を行う設計では、「マイナンバーは憲法13条などとぶつかり違憲となる」可能性が高いということですね。

（石村）仰せのとおりです。マイナンバー違憲判決を避けるための制度設計、対応です。

（中村）こうした「符号」は、個人番号／マイナンバーからしか組成できないのでしょうか？

（石村）いいえ。「氏名・生年月日・性別など」を使って組成することも可能です。つまり、個人番号／マイナンバーがないと組成できないわけではありません。

（中村）となると、政府ポータルサイト／マイナポータル内での情報連携（データ照合）は、個人番号／マイナンバーがなくともできる。マイナンバーは要らない。

（石村）ですから、政府ポータルサイト（マイナポータル）へのログインにも、個人番号は不要です。個人番号カードはIC部分に格納されたPKI（電子証明／公的個人認証機能）を使うだけです。

◆ガラ系のマイナポータルは時代遅れ

(中村) グローバルには、政府ポータルサイトへのログインにはスマホ、タブレット端末を使うモデルが主流になってきているとのことです。

(石村) PCよりは、スマホやタブレット端末を頻繁に持ち歩く時代に入っています。ところが、わが国のマイナポータルは、3点セット【ICカード+パソコン(PC)+ICカードリーダー】が必須です。

(中村) まさに、時代遅れのガラ系の代物といえますね。

(石村) PKI(電子証明/電子印鑑)は、J-LIS/ジェーリスから切り離し、各自治体、各種民間の認証機関が発行したものを活用し、かつ「国家統一仕様、カード一辺倒、の考えを捨てる必要があります。その上で、思い切って「個人番号カードの廃止」に舵を切り、個人番号カードなしで、政府ポータル(マイナポータル)サイトにログインできる仕組みにすべきです。データセキュリティには、オーストラリアの政府ポータルサイト(マイガブ/myGav)では、「パスワード+3つのQ&A」を使っています。

(中村) これでは不安と思う人には、「パスワード+3つのQ&A」に代えて、「ワンタイムパスワード/オーテーピー(OTP)」、「単一回利用コード(single use code)」を使う途を開けばよいわけですね。

(石村) そうです。個人番号カードのIC部分に格納されたPKI(電子証明/公的個人認証機能)を使ってセキュリティを高める、そのためにICカードリーダーは必須の電子政府モデル・制度設計はいただけません。

(中村) 現在計画されているマイナポータルの各種機能が盛りだくさんのメニューは、永久工事、永久公共事業につながります。IT利権のメニュー表、のようなものですね。

(石村) スタック(事故)が頻繁に起きるでしょう。

(中村) ICカード発行段階でもたついて、今後、本格的に稼働させるには、ポータルサイトの規模は巨大すぎますよね。頓挫する可能性が余りにも高いといえます。

(石村) 入口でつまづいているのが現実ですからね。3,000億円もの血税を注ぎ込んだあげくメルトダウンした、わが国最初の電子政府構想である住基ネット(住民票コード/住基カード)失

敗へのしっかりした反省がないから、こうなるのだと思います。政産官学で血税を浪費する構想を次々打ち出すものの、失敗しても誰も責任をとらない・・・今回のマイナポータルもまったく視界不良です。

(中村) 石村代表、「ICカード+パソコン(PC)+ICカードリーダー」の3点セットを使うわが国の電子政府モデル(マイナポータル)が、スマホやタブレット端末全盛の時代に入り、ガラ系と化している現実を鋭く指摘くださり、とても有益でした。それから、わが国の人口規模から考えて、個人番号カードに固執するマイナポータルは、うまく行かないのでないかと感じました。個人番号カード交付事業は、まさに「IT利権、そのもので、血税浪費の永久公共事業であることも分かりました。目からうろこが落ちました。最後に一言、お願いします。

◆ジワジワ危なくなるマイナンバー

(石村) 政府は、個人番号(マイナンバー)の官民でのエスカレート利用に意欲的です。すでに預貯金口座の個人番号(マイナンバー)管理のための法改正をしました。しかし、よく考えてください。人生80年の時代にあって、生涯不変の個人番号(マイナンバー)の汎用はまさに愚策そのものです。パスワードを頻繁に変えてなりすまし犯罪に対峙する時代にあきらかに逆行します。ネット取引全盛の今日、こんな愚策を続ければ、ジワジワ危なくなります。各所へのハッカー攻撃、マルメール攻撃で個人番号(マイナンバー)付き個人情報的大量流出、大被害が発生は避けられません。わが国が、アメリカや韓国のように番号を悪用したなりすまし犯罪者天国化するのは時間の問題ではないと思います。「国民がマイナンバーを監視する」スタンスが求められています。

(中村) 貴重な一言、ありがとうございました。個人番号(マイナンバー)の汎用にストップをかけ、なりすまし犯罪者天国化にもストップかけないといけません。目下のところは、今回、石村代表にお話いただいた住基ネットで学んだはずのICカードが何の反省もなくまた進められており、重大な問題だと思います。血税浪費の永久公共事業である個人番号カード交付に、国民はもっと関心を払わないといけないと思います。

Q & A

個人番号の漏えいへの実務的な対応

石村 耕治（PIJ 代表）

Q 15人ほどの社員をかかえる企業です。総務、経理などの事務のために、役員や社員などから収集、管理していた個人番号（マイナンバー）や特定個人情報（番号付き個人情報）を漏えいしてしまいました。事業者としては、どのような対応をすればよいのでしょうか。

A 企業（事業者）が取り扱う個人番号（マイナンバー）や特定個人情報（番号付き個人情報）が漏えいしてしまったとします。あるいは企業（事業者）の番号取扱事務が番号（マイナンバー）法に違反しているか、そのおそれがあるとしています。個人情報保護委員会（旧特定個人情報保護委員会）は、こうした場合の対応方法を例示しています。具体的には、問題法人に「漏えい等の発覚時の対応」のみを求める場合と、委員会等に対する「漏えい等の報告」までも求める場合に分けて対応方法を例示しています。さらに、委員会等に対する「漏えい等の報告」については、それを問題法人の努力義務とする場合と、「重大な事態」が生じたことを理由に、問題法人の法令上の義務とする場合とに分けて対応方法を例示しています。

解説

1 「漏えい等の発覚時の対応」および「漏えい等の報告」

個人情報保護委員会は、個人番号（マイナンバー）や特定個人情報の漏えいその他の個人番号（マイナンバー）法違反またはそのおそれがあるケースへの対応方法を例示しています。その典拠としては、平成27年12月25日に「特定個人情報の漏えいその他の特定個人情報の安全の確保に係る重大な事態の報告に関する規則」（平成27年特定個人情報保護委員会規則第5号）を制定し、併せて「事業者における特定個人情報の漏えい事案等が発生した場合の対応について」、関連Q&A、「中小企業の方へ：マイナンバー（個人番号）が万が一漏えいしてしまったら」などを公

表しています。

企業（事業者）において、個人番号（マイナンバー）や特定個人情報の漏えいが発覚したとします。この場合、具体的な対応は発生したケースにより異なります。個人情報保護委員会などがつくったこれら規則、資料、Q&Aなどをもとに対応策や報告要件などをまとめると、次のとおりです。

（1）「漏えい等の発覚時の対応」とは

企業（事業者）に求められる「漏えい等の発覚時の対応」手順は、次のとおりです。

「漏えい等の発覚時の対応」手順

- | |
|--|
| ① 企業内部における報告、被害の防止拡大 |
| 責任ある立場の者に直ちに報告するとともに、被害の拡大を防止するために迅速に、以下の②～⑤を実施すること。 |
| ② 事実関係の調査、原因の究明 |
| 事実関係を調査し、その原因を究明すること。 |
| ③ 影響範囲の特定 |
| 前記②で把握した事実関係による影響の範囲を特定すること（例えば、誰の、どのような特定個人情報が、どこに漏えいしたのかなど）。 |
| ④ 再発防止策の検討・実施 |
| 前記②で究明した原因を踏まえ、再発防止策を検討し、速やかに実施すること。 |
| ⑤ 影響を受ける可能性のある本人への連絡等 |
| 二次被害の防止、類似ケース再発回避の観点から、ケースの内容に応じて、事実関係等について、速やかに本人に連絡し、または本人が容易に知ることのできる状態におくこと。 |
| ⑤ 影響を受ける可能性のある本人への連絡等 |
| 後記「漏えい等の報告」を参照のこと。 |

(2) 漏えい等の報告

企業（事業者）に求められる個人情報保護委員会への「漏えい等の報告」の要件は、次のとおりです。

「漏えい等の報告」要件

① 個人情報保護委員会への報告

個人情報保護委員会ウェブサイトに掲載している様式（http://www.ppc.go.jp/files/pdf/271225_jigyousya_houkokuyousiki.pdf）に事実関係や再発防止策など必要な事項を記載し、速やかに個人情報保護委員会に郵送で報告するように努めること。つまり、この場合は、報告は努力義務。ただし、影響を受ける可能性のある本人すべて（情報主体全員）に連絡した場合、外部に漏えいしていないと判断される場合等の要件を全て満たす場合には、個人情報保護委員会への報告は不要。

② 所轄官庁への報告

所管官庁のガイドライン等に従って報告が必要な場合には、そこへ報告すること。この場合は、その所管官庁から個人情報保護委員会に報告されるので、前記①の報告は不要。

③ 「重大な事態」が生じたことを理由とした個人情報保護委員会への報告

この場合の報告は法令上の義務（平成27年特定個人情報保護委員会規則第5号）。ちなみに、「重大な事態」とは、次のようなケースを指す。

- ・ 漏えい・滅失・毀損または番号（マイナンバー）法に反して利用・提供された特定個人情報にかかる本人の数が100人を超える場合
- ・ 特定個人情報ファイルに記録された特定個人情報を電磁的方法により不特定多数の者が閲覧することができる状態になり、かつ、その特定個人情報が閲覧された事態
- ・ 不正の目的をもって、特定個人情報ファイルが記録された特定個人情報を利用し、または提供した者がいる事態など

媒体（USBメモリ）をカバンに入れて持ち帰る途中でカバンごと紛失してしまいました。この場合には、どのように対応したらよいのでしょうか。

「発覚時の具体的な対応策」

① 企業内部における報告、被害の防止拡大

企業の責任ある立場の者（例えば、その企業が「特定個人情報等取扱規程」を定め、特定個人情報等保護責任者を置いている場合には、その者）に直ちに報告する。同時に、警察等への紛失届の提出および当日の行動範囲に落ちていないかの確認をするなど、USBメモリを探し回収に努める。加えて、被害の拡大を防止するために迅速に、以下の②～⑤を実施する。

② 事実関係の調査、原因の究明

USBメモリをどのように取り扱っていたのかについて、本人から事情を聴取し、特定個人情報等取扱規程などに沿った取扱いをしていたのか、それともそれらに沿わない取扱いをしていたのかを確認し、紛失に至った原因を究明する。

③ 影響範囲の特定

前記②で把握した事実関係による影響の範囲を特定する。つまり、USBメモリ保存データに誰のどのような情報が含まれていたのかを特定し、外部に情報が流出した場合の影響を想定する。また、USBメモリの保存データの暗号化やパスワード設定の状況を確認する。さらに、USBメモリが回収できた場合には、回収までの経緯を確認し、不特定の者に情報が漏えいしていないかを確認する。

④ 再発防止策の検討・実施

前記②で究明した原因を踏まえ、再発防止策を検討し、速やかに実施する。つまり、発生原因が人的原因か特定個人情報等取扱規程などのルール自体の欠陥にあるのかを特定し、再発防止のための対応方法（例えば、個人番号（マイナンバー）の基本的な取扱いに関する研修の実施、ルールの改訂等）を検討した後、職員に周知して適切に実施する。

⑤ 影響を受ける可能性のある本人への連絡等

影響を受けるであろうUSBメモリ保存データに含まれる情報の該当者に連絡をして、漏えいの事実について謝罪をし、不審電話による詐欺被害（例えば、金銭の要求など）の防止のための注意を喚起する。また、個人番号（マイナンバー）が漏えいして不正に用いられるおそれがあると認められるときは、マイナンバーの変更を住民登録地の市区町村の窓口で請求できるので、その手続について窓口にお問い合わせるように本人に説明をする。

⑥ 個人情報保護委員会等への報告の要否の確認

個人情報保護委員会等への報告が必要かどうかを確認し、必要な場合には報告をするように努める。とりわけ、「重大な事態」が生じたときには、個人情報保護委員会へ報告しなければならない。

2 発覚時の具体的な対応策の検討

個人情報保護委員会は、紛失や漏えい等の事実の発覚時対応のヒントを例示しています。そこで、以下の事例を参考に、企業（事業者）における個人番号（マイナンバー）、特定個人情報の紛失、漏えいの可能性があるケースをアレンジし、「発覚時の具体的な対応策」を検討してみます。

企業（事業者）の経理担当者が自宅で作業をするために、役員や職員とその家族の個人番号（マイナンバー）や特定個人情報を保管している電子

3 個人番号（マイナンバー）が漏えいと刑事責任

企業（事業者）の個人番号（マイナンバー）取扱事務は極めて煩雑で、この事務にかかる負担は相当重いわけです。こうした過重な負担は、事業者の生業に大きな影響を及ぼします。当然、漏えい問題が起きても対応が後手にまわることが想定されます。

わが国の個人番号（マイナンバー）制は、源泉徴収や年末調整のような税務事務や年金や健康保険のような社会保障事務などに必要との理由で、事業者の手許に役員や職員とその扶養家族、さらには法人の取引者の個人番号（マイナンバー）を、必要以上に蓄積することにつながる危ない仕組みになっています。このままでは、多くの小規模企業が過重な番号取扱事務負担についていけなくなり、個人番号（マイナンバー）特定個人情報の紛失・漏えいなどが各所で続出することが懸念されます。

この点、例えば、オーストラリアが導入する番号制（TFN＝タックス・ファイル・ナンバー）では、事業者が、その役員や従業員の扶養家族の個人番号（個人のTFN）までも収集し、手許に蓄積する必要はありません。なぜならば、全員確定申告するのを原則とし、年末調整などは設けていないからです、また、税制上の人的控除から手当の支給に切り替えています。さらに、勤務先や取引先に自分の番号（TFN）の提示を望まない納税者には、高めの税率で源泉課税をし、確定申告で調整できる仕組みにしています。加えて、給与所得や預貯金の利子を含む投資所得には「個人番号（個人のTFN）」を使う一方で、事業性所得（事業所得や不動産所得など）を生む取引には消費税（VAT／GST）の「事業者番号」を使っています。これによって、講演・執筆活動などをする作家や大学教員を含む自営業者などは、事業上の取引に個人番号（個人のTFN）を使わなくともよい仕組みにしています。こうした方策によって、個人番号（個人のTFN）が必要以上に拡散し、勤務先や取引先などに蓄積・沈殿しないようにしているわけです。（石村耕治「急がれる個人事業者や家族の個人番号のダダ漏れ防止対策：諸外国では複数番号の導入・確定申告で対応」CNNニュース85号参照）。

ところが、わが国ではこうした番号拡散防止策が講じられていません。このままでは、法定の保

管期間が過ぎても、個人番号（マイナンバー）が消去されない、あるいは特定個人情報に記された書類が廃棄されないで、事業者の手許に大量に「沈殿」していくのが懸念されます。こうした野放図な番号取扱事務を続けて行けば、じわじわと危なくなり、各所で個人番号（マイナンバー）や特定個人情報が漏えいしていくことは避けられません。

企業（事業者）は、問題行為で特定個人情報を流出・漏洩を許してしまっても、一般に罰則はありません。ほかにも、罰則の適用のない問題行為はさまざま想定されます。一覧にしてみると、次のとおりです。

刑事制裁の対象とならない事業者の問題行為とは

- ・事業者が、番号（マイナンバー）法令やガイドラインなどに従い「特定個人情報等の適正な取扱いに関する基本方針」や「特定個人情報等取扱規程」などをつくって、組織としての安全対策を実施していない。
- ・事業者が、税理士や社会保険労務士などとの間で特定個人情報等取扱業務委託契約書を交わし、その事務の委託先の監督を行っていない。
- ・事業者が、個人番号（マイナンバー）の利用目的を特定し、役員や職員とその扶養親族に通知していない。
- ・事業者が、個人番号（マイナンバー）を取得する際、本人確認（番号確認＋身元確認）を行っていない。
- ・事業者が、鍵の掛かるキャビネットの設置など物理的な安全措置を講じていない、ファイアウォール、ウィルス対策ソフトなどを購入し、情報漏えい対策を行っていない。
- ・事業者が、個人番号（マイナンバー）が記載された書類をシュレッダーで廃棄せず、燃えるゴミとして廃棄している。
- ・事業者が、すでに退職した職員の個人番号（マイナンバー）が記載されている書類を、法定保存期間を超えて保管している。
- ・事業者が、職員等への必要な教育・研修を行っていない。
- ・事業者のパソコンがコンピュータウィルスに感染する、あるいはマルウェアが添付された標的型のメール攻撃に会い、役員や職員とその扶養家族の個人番号（マイナンバー）が漏洩してしまった。

いずれにしろ、企業（事業者）が、こうした瑕疵ある番号取扱事務を行った場合には、個人情報保護委員会から報告を求められることがあります。また、立入調査を受ける可能性もあります（番号利用（マイナンバー）法35）。しかし、「不当な利益をはかる目的」、つまり第三者と結託するなどの不正な手段が使われるなどしない限り、番号利用（マイナンバー）法に抵触するとし

ても、番号利用（マイナンバー）法に基づく刑事制裁（48条～57条）の対象になることはありません。これは、ある意味では、当然のことです。なぜならば、企業（事業者）にとっては、このような危ない番号の取扱事務のタダ働きを強いられたいうえ、少しでもミスすれば罰則までかされるのではたまったものではないからです。

4 個人番号（マイナンバー）が漏えいと民事責任

企業（事業者）は、問題行為を行っても多くの場合は刑事制裁の対象とはならないのは当然であるとしても、民事責任については別です。民間の事業者が一番危惧していることは、個人番号（マイナンバー）が漏えいした場合を含め、こうした問題行為に対する民事責任の問題です。

個人情報保護委員会などの各種資料では、漏えい等に伴う民事責任の問題には意図的に触れないようにしています。番号取扱事務普及の妨げになることを危惧しての沈黙でしょう。しかし、これでは、まったく不誠実、どっちつかずで、誰の権利利益を保護するための委員会なのかが不透明です。

確かに、企業（事業者）の経理担当者あるいは総務担当者が自宅で作業するために、個人番号（マイナンバー）を保管している電子媒体（USBメモリーやSDカード）をカバンに入れて持ち帰る途中でカバンごと紛失してしまった場合に、どのように対応するかは重い課題です。ただ、企業（事業者）が、番号取扱事務へのタダ働きを強いられたいうえ、個人番号（マイナンバー）ないし特定個人情報を漏えいさせた場合には、民法上の不法行為責任（民法709条）を問う民事訴訟に引き出され、損害賠償を請求される可能性があることは、もっと頭の痛い問題です。

一方、自分の個人番号（マイナンバー）が漏えいし、不正に用いられるおそれがあると認められるときには、当該本人は、住民登録している市区町村の窓口で、個人番号（マイナンバー）の変更を請求することができます（番号利用（マイナンバー）法7条2項）。こうした手続をするにあたり、新たな番号カードの再交付を受ける手続の場合を含め、仕事をしている者であるときには、少なくとも一度は仕事を休んで市区町村の窓口まで本人が出向かなければなりません。このことから、企業（事業者）は、個人番号（マイナンバ

ー）ないし特定個人情報を漏洩させてしまった場合には、被害にあった本人の日当（またはその半分）や交通費、その他慰謝料を支払う必要が出てくる可能性があります。ちなみに、一連の個人情報漏えい事件判決では、一般に、慰謝料として1人あたりおおよそ5,000円～15,000円の範囲で支払いが確定しています。

仮に、企業（事業者）が、個人番号（マイナンバー）が漏えいさせてしまった場合で、漏えい件数が大きくなると、相当な金額の損害賠償を覚悟しなければならなくなるといえます。こうした支払も、漏えい対応上の重い課題です。規模の大きい企業では、損害保険に加入するなどの対策も避けて通れません。

【参考法令等】

- ・特定個人情報の漏えいその他の特定個人情報の安全の確保に係る重大な事態の報告に関する規則（平成27年特定個人情報保護委員会規則第5号）
- ・特定個人情報保護委員会 事業者における特定個人情報の漏えい事案等が発生した場合の対応について（平成27年特定個人情報保護委員会告示第2号）
- ・特定個人情報保護委員会 事業者における特定個人情報の漏えい事案等が発生した場合の対応におけるQ&A（平成27年12月25日）
- ・個人情報保護委員会 中小企業の方へ：マイナンバー（個人番号）が万が一漏えいしてしまったら
- ・個人情報保護委員会 特定個人情報の漏えい等報告について（事業者用様式）
- ・個人情報保護委員会 特定個人情報の漏えい事案等が発生した場合の報告要領について
- ・個人情報保護法（平成27年5月30日現在、一部未施行）50条～65条
- ・番号（マイナンバー）法（最終改正平成28年6月3日）7条2項、35条、48条～57条
- ・民法 709条

【参考文献】

- ・石村耕治「急がれる個人事業者や家族の個人番号のダダ漏れ防止対策：諸外国では複数番号の導入・確定申告で対応」CNNニュース85号（PIJ、2016年5月）<http://www.pij-web.net/data/CNN-85.pdf>
- ・石村耕治「オーストラリアの背番号も番号カードも使わない電子政府：電子政府構想の日豪比較」CNNニュース85号（PIJ、2016年5月）<http://www.pij-web.net/data/CNN-85.pdf>
- ・石村耕治・我妻憲利「対論・オーストラリア情報コミッション事務局（OAIC）の活動を知る：わが国の「名ばかり個人情報保護委員会」を糾す」CNNニュース86号（PIJ、2016年7月）<http://www.pij-web.net/data/CNN-86.pdf>
- ・第二東京弁護士会情報公開・個人情報保護委員会編『Q&A 改正個人情報保護法』（新日本法規、2015年）
- ・岡村久道『番号利用法』（商事法務、2015年）
- ・石村耕治『現代税法入門塾（第8版）』（清文社、2016年）

アメリカで猛威を振うSSNを悪用したなりすまし納税申告

アメリカでのなりすまし申告被害者の救済手続

他人に社会保障番号（SSN）を悪用され
なりすまし納税申告された場合の対応策

石村 耕治（PIJ 代表）

◆はじめに

アメリカでは、個人の共通番号である「社会保障番号（SSN=Social Security Number）」を搾取し、巧妙な手口で悪用したなりすまし犯罪（IDT=identity theft）が、全米規模で猛威を振っている。

こうした背景には、社会保障番号（SSN）の利用規制をしないで、野放図に官民の幅広い分野で自由に利用させてきた経緯がある。対面取引が陰りを見せる一方で、ネット取引、電子納税申告などが急激な伸びを示してきており、これが、SSN悪用に拍車をかけている。連邦議会でも、他人のSSNを悪用による虚偽申告の急増について繰り返し問題にし、対応策を模索してきている（CNNニュース73号、75号参照）。

アメリカの場合、連邦個人所得税の課税期間は暦年である。つまり1月1日から12月31日までである。課税最低限を超え、追加納税の必要がある個人納税者（納税申告者）あるいは税金を払い過ぎの納税者（還付申告者）は、様式1040〔連邦個人所得税申告書（Form 1040）〕を法定期限までに提出しなければならない。様式1040の提出期限は、翌年の4月15日（2016年については休日はさむことになるので4月18日¹）である（IRC6072条a項）。

連邦課税庁であるIRS（Internal Revenue Service／内国歳入庁）は、2015年期を例にすると、2億430万件を超える納税申告書および法定資料を全米10か所のIRSキャンパス申告センターで処理している²。

【図表1】アメリカのSSNカード（サンプル）



IRSは、早くから個人の納税者番号（ITIN=individual Taxpayer Identification Number）として、SSN（社会保障番号）を税務に転用して使ってきた。しかし、他人のSSNを悪用した不正申告が年々急激に増加し、その対応に苦慮してきた。

2011年1月には、IRSは、なりすまし（IDT）不正申告被害者向けに、9ケタのSSNとは別途の6ケタの限定番号「身元保護個人納税者番号（IPPIN=Identity Protection Personal Identification Number）」を交付・利用に踏み切っている。

この新しい身元保護個人納税者番号（IPPIN）は、納税者に成りすまし犯罪（IDT）の被害リスクがある限り継続的に、次の申告期の開始前までに発行される。2012年申告期に、IRSは25万2,000人に身元保護個人納税者番号（IPPIN）を発行している。

一方、国防総省（DOD=Department of Defense）は、長い間、個人番号として使ってきた共通番号（SSN／社会保障番号）の利用を止めて、新たな11ケタの「国防総省本人確認番号（DOD ID number）」を使うことにした。

こうした共通番号（SSN）から分野別の限定番号【IRSのIPPIN、国防総省のDOD ID

¹ ただし、提出期限日が、土曜、日曜または祝日となる場合は、その次の営業日が申告書の提出期限となる（IRC7503条）。

² See, IRS, Data Book 2015, at 2. Available at: <https://www.irs.gov/pub/irs-soi/15databk.pdf>

numberなど】の利用にみられるように、連邦各省庁はなりすまし犯罪（IDT）撲滅に向けて対応を急いでいる。しかし、SSNの悪用、不正申告の増加にはストップがかかっていない。状況は改善に向かうというよりは、悪化の一途をたどっている。

近年は、フィッシングのみならず、標的型マルウェアメールやランサムメールなどを使って、大量のSSNやSSN情報を搾取し、不正申告に悪用するケースも目立ってきている。

1 ネットを使ったなりすまし申告とは

アメリカでの成りすまし犯罪は、従来、現実空間（real space）で深刻化していた。しかし、IT技術の進展とともに、近年では、ネット空間／サイバースペース（cyber space）でのなりすまし犯罪が急激な広がりを見せ、目に見えないところでの対策に手を焼く事態になってきている。

（1）「フィッシング」や「マルウェア」とは

ネット空間／サイバースペースで、不法に個人情報収集する手法には、大きく分けると、「フィッシング」と「マルウェア」がある。

①フィッシングとは

「フィッシング」とは、IRS、インターネット・プロバイダー、金融機関などの名を語り正規のEメールやウェブサイトを装い、共通番号（SSN）、暗証番号やクレジットカード番号などを詐取する手法である。「釣り」を意味する「fishing」が語源であるが、偽装の手法が洗練されていることから「phishing」と綴っている。

リンクをクリックすると、そのIRS、インターネット・プロバイダー、金融機関の正規のWebサイトと、個人情報入力用のポップアップウィンドウが表示される。メインウィンドウに表示されるサイトは「本物」で、ポップアップページは「ニセモノ」である。本物を見て安心したユーザーがポップアップに表示された入力フォームに共通番号（SSN）、暗証番号やパスワード、クレジットカード番号などの秘匿情報を入力・送信すると、犯人に送信される。

②「マルウェア」とは

「マルウェア（malware）」とは、具体的には

コンピュータウイルス、ワーム、スパイウェアなどをさす。「mal」は「過誤、災難」を意味することから、パソコンに悪害を及ぼす有害なソフトウェアをさす造語である。

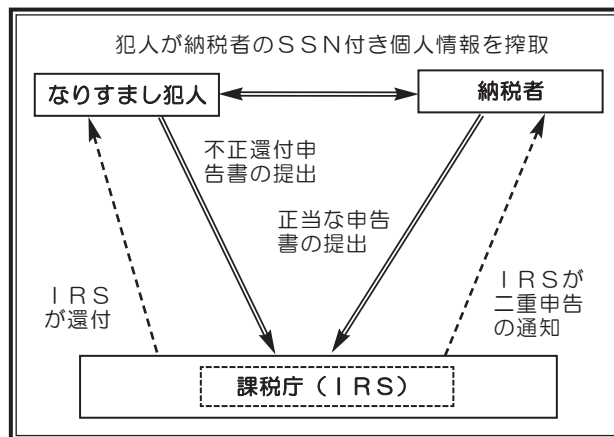
犯人は、この有害なソフトウェアを使って他人のパソコン（PC）に侵入してウイルス感染や破壊活動を行ったり、成りすまし犯罪に使うための共通番号（SSN）、暗証番号やパスワード、クレジットカード番号などの秘匿情報などを自分に送信させたりすることができる。「標的型マルウェアメール」とも呼ばれる。わが国でも、日本年金機構が、マルウェアメールで大量の年金関連顧客情報を抜き取られたことで大きなニュースになった。

（2）なりすまし不正申告の急増

アメリカにおけるなりすまし犯罪（IDT）は、伝統的には、ネット空間よりも、現実空間（real space）で多発している。つまり、個人の財布や郵便物などから個人の情報を抜き取り、それらをなりすまし犯罪に使うという手法である。また、個人情報の抜取は、古くなり廃棄されたパソコン（PC）や、行政機関や企業が捨てた書類やごみ箱に捨てられたレシートなどを使って行われるケースも少なくない。さらに、なりすまし犯罪者は、無断で被害者の請求書等の送付先の住所変更をして被害者の個人情報を入手し、それをなりすまし犯罪に盗用する手口を使うこともある。

税や社会保障関連のなりすまし犯罪は急増している。とりわけ、納税者が他人によるなりすまし（IDT）不正還付申告の被害が深刻である。その構図は、おおむね次のとおりである。

【図表2】なりすまし不正還付申告の構図



不正還付申告関連のなりすまし犯罪（IDT）は、犯人がさまざまな手段を用いて不正に入手し

た納税者（本人／被害者）共通番号（SSN）やSSN付き個人情報などを使って還付申告（tax refund）することによって行われる。なりすまし不正還付申告の場合、通例、納税者本人（被害者）は、IRSから重複申告などが行われている事実の通知を受けるまでは分からないことが多い。電子申告（e-file）の普及も手伝ってか、IRSは、なりすましの不正還付申告の著しい増加に手を焼いている。

犯人は、偽名の使用ではなく、不正に入手した他人の氏名や共通番号（SSN）、ラップトップのPCと電子私書箱を使って容易に税金の不正還付を受けている実態がある。とりわけ、これら不正還付申告では、確定申告期のはやい時期に、納税者本人（被害者）が還付申告をするよりも先に還付申告をしているのが特徴である。

現在、IRSは、支払調書と申告情報との突合（データ照合）に各納税者の共通番号（SSN）に大きな信頼を置き、かつ、早い者順に還付のためのデータ・マッチングを実施し、還付金を送金する態勢にある。一方、なりすまし還付申告者も、還付金の受取に、現金小切手ではなく、金融口座への振込を希望することも、なりすまし犯罪の発覚を遅らせる要因になっている。

（３）IRSの名を語ったフィッシング・メールの急増

近年増加傾向にあるのが、課税庁（IRS）の名を語って納税者情報を入手する手口である。電話や手紙、電子メール（Eメール）などで、犯人が、共通番号（SSN）氏名、生年月日を含むSSN付き個人情報の入手を図ろうとするケースが増えてきている。現実には、課税庁（IRS）は、電話や手紙、Eメールで納税者に個人情報のみを提出するように要請することはない。しかし、犯人のこうした手口に引っかかる納税者も少なくない。

各種の取引規制や消費者保護などの業務を所管する連邦取引委員会（FTC＝Federal Trade Commission）によると、近年の傾向としては、電話や手紙などを使った不正な納税者情報の入手よりも、ネット空間を通じ、フィッシング・メールなど洗練された偽装手法を駆使して不正な納税者情報を入手する手口が急増しているという。

税務関連では、最悪期の2012年に最初の2ヵ月間だけでも、数億人のインターネットユーザーを対象としたフィッシング・メールが3度も頒

布されている。2012年1月のIRSの名を語った偽装メールでは、ユーザーがポップアップに表示された入力フォームに氏名・住所・共通番号（SSN）・生年月日などの秘匿情報を入力・送信すると早期の税金還付が受けられる旨を告知していた。

また、同じく、2012年2月の偽装メールでは、納税申告書を提出しなければ1万ドルの加算税が課されることをうたい、ポップアップに表示された入力フォームに氏名・住所・共通番号（SSN）・生年月日などの秘匿情報を入力し確認を促す通知が行われた。

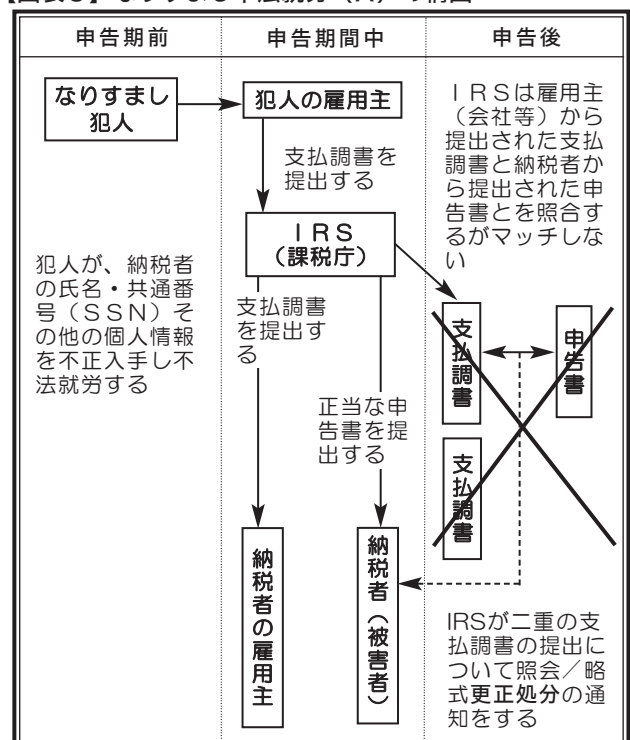
この事件後、IRSは緊急の対応策を講じたものの、次々と出現する新手のサイバー詐欺に、対策が後手に回り、連邦議会などから厳しい追及を受けている。

（４）なりすまし不法就労と不正申告

不法就労が絡んだなりすまし不正申告が、IRS（連邦課税庁）にとり、かなり厄介な問題となっている。犯人は、極めて巧妙な手段を用いて不正に入手した納税者（本人）の氏名や共通番号（SSN）付き個人情報を使って、短期の仕事に就くことが主なねらいであるからである。

IRSは、申告期前になりすまし不法就労の事実をつかむのは至難の業である。なぜならば、IRSは、なりすまし犯人の雇用主からの給与所得

【図表３】なりすまし不法就労（Ａ）の構図



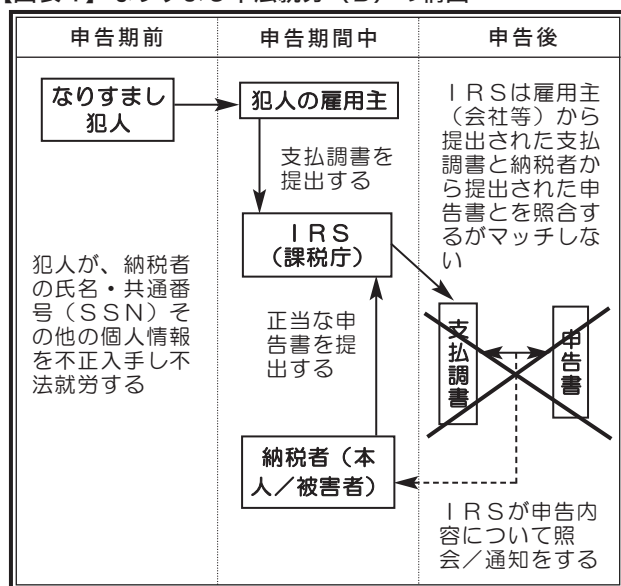
関連の支払調書の提出を受け、被害者である納税者本人の確定申告を受けて、申告後に双方のデータを突合（照合）してはじめて犯罪事実を認識するケースが多いからである。

【図表3】からわかるように、なりすまし不法就労の場合、不正還付申告を目的とする場合とは異なり、ほとんどの場合、犯人は確定申告をすることはない。一方、被害者である納税者（本人）は、事実を知らずに確定申告をすることになる。

IRSは、なりすまし犯人の会社や事業主（雇用主）から提出された支払調書と、被害者である納税者（本人）が給与所得者（wage earners）である場合にはその雇用主から提出された支払調書を受け取ることになる。

この場合、IRSは、その納税者が複数の事業者のもとで就労できる状況にはないと読んだときには、どちらか一方はなりすまし不法就労ではないかと疑うことになる。そして、IRSは、その納税者に対して、「誰か他人があなたの名前や共通番号（SSN）を使って不法就労をしているのではないか」との照会／通知を行うことになる。

【図表4】なりすまし不法就労（B）の構図



一方、【図表4】のように、被害者である納税者（本人）が自営業者（self-employed）などで、給与所得者でない場合には、雇用主から課税庁（IRS）に支払調書の提出がない。この場合、本人から提出された申告内容となりすまし犯人の会社（雇用主）から提出された支払調書の内容とを照合（突合／データ照合）することになる。当然、双方はマッチしないことになり、IRSは被害者である納税者（本人）に照会／通知を行うこ

とになる。

この場合も、被害者である納税者（本人）は、IRSからこうした紹介／通知を受けてはじめて自分が成りすまし犯罪の被害にあっていることに気づくことになる。

2 アメリカでのなりすまし申告被害者の救済手続

例えば、ニューヨーク州に住所を持つ合衆国市民である納税者が、様式1040〔連邦個人所得税申告書（Form 1040）〕に必要事項を記載し、追加納税あるいは税金の還付（tax refund）を受けるための電子申告をするとする。この場合は、IRSのウェブサイトからマサチューセッツ州にあるIRSアンドーバー（Andover）キャンパスの申告処理センター（Internal Revenue Submission Processing Center）宛に、様式1040に法定資料を添付して電子送付することになる。

一方、様式1040を文書で申告する場合には、ミズーリー州にあるIRSカンザスシティ（Kansas City）キャンパスのIRS申告処理センター（Internal Revenue Submission Processing Center）宛に、法定資料を添付して郵送することになる。

郵送先：
Internal Revenue Submission Processing
Center 2306 East Bannister Road
Kansas City, MO 64131



IRSカンザスシティ（Kansas City）キャンパス
Public use

ところが、所管のIRSの申告処理センターから、誰かがすでにその納税者のSSNや個人情報を使って還付申告をしている旨の通告（Notice CP 2000等）を受けたとする。

この場合、なりすまし申告の被害にあった納税者は、どのような手続を踏んだらよいのであろうか。

(1) IRSからの通知

一般に、他人が自分のSSNや個人情報を利用して、様式1040〔連邦個人所得税申告書〕を提出した場合、本人が自分の申告書を提出するまでは、二重の申告が行われている事実は容易に発覚しない。

IRSの申告処理センターは、同じSSNの記載された2通の様式1040〔連邦個人所得税申告書〕を受領した場合、第2番目の様式1040を受理しないことになる。IRSは、第2番目の様式1040を提出した納税者に対して、その年分の様式1040がすでに受理されている旨を記した通知(Notice CP 2000等)を文書で行うことになる。

この通知を受けて、納税者は必要な手続を開始することになる。

もっとも、IRSからの通知がない場合でも、他人が自分になりすまして様式1040を提出していると疑われるときには、その納税者は必要な手続を開始することも可能である。

【図表5】様式1040〔連邦個人所得税申告書 (Form 1040)〕 (1頁)

(2) 様式14039 (Form 14039) への記載 納税者が、誰か他人が自分のSSNを使いなり

すまして様式1040〔連邦個人所得税申告書〕を提出しているとの疑いを持ったとする。この場合、その納税者は、所管のIRSの申告処理センターに、様式14039〔身元盗難宣誓供述書 (Form 14039: Identity Theft Affidavit)〕に必要な事項を記載して提出することになる。いわゆる「被害届」の提出である。

この様式14039〔身元盗難宣誓供述書〕には、被害者の詳細、コンタクト先、被害納税者の代理人がいる場合には、その詳細、宣誓、日付、署名などを記載するように求められる。

【図表6】様式14039 (身元盗難宣誓供述書) (抜粋)

(3) 様式14039 (Form 14039) の送付

なりすまし (IDF) 不正申告の被害を受けた納税者は、`被害届`である様式14039〔身元盗難宣誓供述書〕に必要な記載をしたうえで、自分の社会保障カードのコピーおよび運転免許またはパスポートその他身元確認のできる証拠のコピーを添付して、IRSに送付することになる。

また、納税者は、IRSから、不正申告に関するその他の通知 (Notice CP 2000等) をもらっている場合には、そのコピーも添付する必要がある。

被害者である納税者は、これまでIRSがなりすまし不正申告に関係するいかなる通知をもらっていない場合には、下記の住所に書類を郵送することになっている。

郵送先：Internal Revenue Service

P.O. Box 9039

Andover, MA 01810-0939

IRSは、被害届（様式14039〔身元盗難宣誓供述書〕）の提出を受けて、専従班【なりすまし被害者支援班（IDTV A=Identity Theft Victim Assistance）】が早急に事案を精査し、必要な対応策を講じることになる。

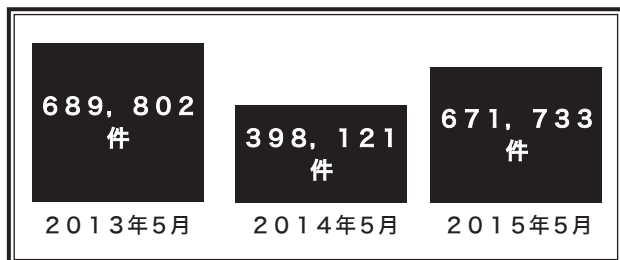
（４）IRSの納税者保護プログラム（TPP）

IRSは、なりすまし不正申告の問題に対応するための納税者保護プログラム（TPP=Taxpayer Protection Program）を組んでいる。TPPでは、なりすまし不正申告ではないかと疑われる場合には、その申告書を提出した納税者に、IRSにコンタクトして、30日以内に自分の身元確認を行うように求める書簡を送ることになっている。

また、なりすまし不正申告の被害を受けたと思う納税者は、TPPに電話または電子メールでコンタクトを取り、対応について相談することができる。

ちなみに、IRSは、納税者保護プログラム（TPP）を通じて、2015年5月末までの1年間に、なりすまし（IDT）の疑いのある6万71,733件（重複は除く。）の不正申告書を確認している〔See, IRS, Global Identity Theft Report (May 31, 2015); IRS, Global Identity Theft Report (May 31, 2014)〕。

【図表7】TPPで確認されたなりすまし不正申告件数の推移



3 IRSのなりすまし不正申告防止策と被害者救済策の概要

IRSは、2004年から継続的に、税務関連なりすまし問題への包括的な対策を実施している。これら一連の対策は、基本的には税務行政におけるなりすまし犯罪の防止・減少をねらいとし

たものである。大きく分けると、不正防止策と被害者救済策の二つの柱からなる。

具体的には、納税者教育の視点から、なりすまし不正申告犯罪の手口や対処方法、被害者救済手続の利用方法、被害者へのカウンセリング、なりすまし不正申告で被害を受けた個人納税者向けの「身元保護個人納税者番号（IPPIN=Identity Protection Personal Identification Number）」の発行などである。

一方、IRSの納税者サービス改善の面からは、なりすまし不正申告で財政的のみならず心理的にも被害を受けた納税者への電話や窓口での対応の仕方や被害者救済手続の説明の仕方などについて、現場で被害者へ対応する職員の定期的な研修の実施である。

（１）IRSとDOJ共同のなりすまし還付防止策

IRSは、なりすまし不正申告対策としては、2011年初頭に、高度申告書処理プログラム（Enhanced Return Process Program）を稼働させた。このプログラムおよびその後の関連プログラムで、IRSは、連邦司法省（DOJ=Department of Justice）と各地区の連邦検事正事務所（local Assistant U.S. Attorneys' Offices）の協力を得ながら、次のような具体的な対応策を講じている。

【図表8】なりすまし不正申告防止策と被害者救済策の概要

①潜在的なりすまし不正申告の機械的な検索・ろ過の強化

IRSは、申告書処理前あるいは還付前に過誤申告を機械的に探知する能力を増強するための検索・ろ過するための新たなシステム（account indicators／納税者別情報口座追跡警鐘制）を稼働させた。このシステムでは、納税者の納税状況に一定の変化が生じている場合に、その納税者の申告書に警鐘が付くかたちになっている。従来からIRSの申告処理システムでは、当年の申告と前年の申告との間に納税状況に大きな変化が生じた場合には、警鐘、ヒット（当たり）が付くかたちにデザインされていた。しかし、必ずしもなりすまし不正申告に対応したものではなかった。そこで、潜在的なりすまし不正申告を機械的に検索・ろ過する機能を強化した。

ただ、こうした検索・ろ過機能の強化策には問題がないわけではない。2009年を取ってみても、1千万件の納税者の住所変更、4,600万件の雇用主変更、何百万件の死亡と出生がある。実際に、これらの変更情報や新規情報が、過誤申告・不正申告の探知システムにおいて、警鐘、ヒットとなる主

な原因となっている。これらの警鐘、ヒットされた申告事案は、手作業で丹念に精査する必要がある。しかも、処理を必要とする件数が膨大であり、すべてのヒット事案を精査すると、税額の還付が遅延する結果につながる。

このように、潜在的なりすまし不正申告の機械的な検索・ろ過の強化によるヒット事案の増加は、税額還付の遅延と表裏一体の関係にあり、諸刃の剣にもなりかねない問題もある。

②身元保護個人納税者番号（IP PIN）の発行

2011年1月から、IRSは、なりすまし不正申告の被害を受けた個人納税者向けに「身元保護個人納税者番号（IP PIN=Identity Protection Personal Identification Number）」の発行の試行を始めた。共通番号（SSN）はいったん他人に不正使用されると、その被害を食い止めることは難しい。

現在のアメリカのように、一つの番号を多目的（汎用）するフラット・モデルの共通番号制は、なりすまし犯罪の餌食にある可能性が高く、時代遅れで極めて危険な番号制に仕組みである。共通番号（SSN）では成りすまし不正申告への抜本的な対策は難しい。言い換えると、分野別に異なる番号を使い、各種情報を紐付け・データ照合するセクトラル・モデルの番号制が安全で今の時代にもマッチする。

こうしたことも織り込んで、IRSは、なりすまし不正申告の被害を受けた個人納税者を対象に課税分野に限定して使用する「身元保護個人納税者番号（IP PIN）」を発行することにした。

ちなみに、2011年に、国防総省（DOD=Department of Defense）は、これまでの共通番号（SSN）に換えて、新たな国防総省本人確認番号（DOD identification number）を導入し、この分野別の個人番号を「共通アクセスカード（CAC=Common Access Card/DOD ID card）」に表記することになった。

わが国では、現在、アメリカにまねて、この時代遅れの危ないフラット・モデルの共通番号制を採用する方向だが、今一度精査する必要がある。法人、個人とも課税庁が発行する納税者番号を使うべきである。

③データ照合の早期実施

現在、IRSは、確定申告期間が過ぎてから、会社をはじめとした各種支払機関から提出された支払調書と納税者から提出された申告書とのデータ照合（突合）を実施している。しかし、これでは、なりすまし申告の発見が遅れることになる。そこで、データ照合をできるだけ早めることで、なりすまし犯の発覚に努めることとする。

④故人納税者の身元を使った不正申告対策

IRSは、故人納税者の身元を使ったなりすまし不正申告の増加に頭を悩ませている。すなわち、なりすまし犯人は、インターネット・サーフィンをし、最近死亡した納税者の氏名・住所・共通番号（SSN）などを探し出して、なりすまし不正申告

に使う事案の増加である。

そこで、IRSは、故人納税者の金融機関口座を確認・監視するシステムを稼働させている。現在、約23万の金融機関口座が指定されている。

また、社会保障省（SSA）と協同で、死亡者情報の早期確認態勢の確立に努めることにした。

⑤IRS査察部門でのなりすまし不正納税申告への対応

IRSは、査察／租税犯則部（CI=Criminal Investigation division）の人員を活用し、他人の氏名・共通番号（SSN）などを盗用したなりすまし不正納税申告を探索、調査、防止策を強化している。2011財政年度において、IRS査察部は、276件のなりすまし不正納税申告を調査し、218件の告発を行った。そのうち、165件を有罪に持ち込んだ。その後も、なりすまし犯罪（IDT）で、起訴、有罪判決を受ける者の数は減少していない。

もっとも、なりすまし不正納税申告にかかる刑事告発は、本来、連邦司法省（DOJ=Department of Justice）の所管であり、IRSがこの種の事案に積極的に対処することには限界があるのも事実である。

2012年1月に、IRSとDOJは、105件のなりすまし不正納税申告に関する全国捜査を実施した。この23州に及ぶ全国捜査に関連して、IRSは、150箇所の還付小切手を換金する事業者を訪問調査し、なりすまし不正納税申告犯との関与の実態を究明した。

こうした一連のなりすまし不正納税申告に関する調査や摘発を行うことにより、一定の犯罪抑止効果は期待できる。ただ、2009年に摘発したなりすまし不正還付申告を例にみても、平均で一件あたり不正還付額は約3,400ドル程度である。血税を使った対応に対しては、「費用対効果」の面で大きな疑問符が付いていることも忘れてはならない。

（2）なりすまし不正申告への納税者心得10箇条

IRSとFTCは、納税者がなりすまし不正納税申告被害にあわないようにするために、次のような「納税者心得10箇条」を公表している。

【図表9】なりすまし不正申告への納税者心得10箇条

第1	IRSは、Eメールで納税者と接触を始めることはありません。
第2	あなたが、IRSの名を語った詐欺のEメールを受け取ったときには、IRSのphishing@irs.govへそのEメールを転送してください。
第3	なりすまし犯は、次のような手口であなたの個人情報入手します。 ・あなたの財布を盗む ・電話やEメールで、誰かがあなたの個人情報

報を必要としていることを装う

- ・あなたの個人情報を求めてゴミ箱などをあさる
- ・あなたが安全でないインターネット・サイトへ提供した情報を入手する

第4 あなたが、「www.irs.gov」ではじまらないIRSの名を語った請求をするインターネット・サイトを発見した場合、それをIRSのphishing@irs.govへ電子メールで通知してください。

第5 安全なインターネット・サイトかどうかを確認したい場合には、FTC（連邦取引委員会）、www.ftc.gov/idtheftにアクセスしてください。

第6 あなたの共通番号（SSN）が盗まれた場合、他人がそれを使って職に就くかも知れません。この場合、その他人に給与を支払った雇用主が、あなたの共通番号（SSN）と支払給与額を記載した支払調書をIRSに提出するかも知れません。したがって、あなたが確定申告をした場合に、IRSは過少申告とみなす可能性があります。

第7 IRSから、複数の納税申告書が提出されている旨の通知、または、あなたが知らない雇用主から給与所得の支払調書が提出されている旨の通知を受け取った場合、あなたの身元が盗用された可能性が出てきます。この場合、できるだけ速やかにIRSの通知書に記載された連絡先へ応答してください。

第8 現時点で、あなたの納税記録がなりすまし被害にあっていないとしても、財布の紛失、クレジットカードの利用歴や信用報告書に疑問を感じる場合には、あなたはIRSに対して自己の正確な身元を提供する必要があります。この場合、あなたは、社会保障番号カード、運転免許証、パスポートのような行政機関発行の有効な本人確認情報の副本を、警察署発行の紛失証明書や、様式14039〔身元盗難宣誓供述書（Form 14039: ITA=Identity Theft Affidavit）〕を添えて、提出する必要があります。なお、あなたは、IRSの身元保護機動班（Identity Protection Specialized Unit）、相手方払い電話800-908-4490にコンタクトできます。あなたは、www.ftc.gov/idtheftにアクセスして、FTC発行の手引書を参照しながらなりすまし被害報告書を作成することができます。

第9 あなたは、課税目的で、仕事に就いた場合には雇用主に、自己の口座を開設している金融機関に対して、あなたの共通番号（SSN）を提示してください。あなたの共通番号（SSN）を記載したカードや書類を日常的に持ち歩かないでください。

第10 なりすまし犯罪の被害報告の仕方、フィッシングその他不正行為の手口をはじめとしたなりすまし犯罪に関する詳しい情報につ

いては、IRSのHPの「なりすまし犯罪（IDT=Identity Theft）に関するサイトへアクセスしてください。

4 I P P I Nとは何か

2011年1月から、IRSは、身元保護PINプログラム（Identity Protection PIN program）を開始している。このプログラムは、IRSが、なりすまし被害にあった個人納税者向けに、独自に「身元保護個人納税者番号（I P P I N=Identity Protection Personal Identification Number）」を交付することが目的である。

自分のSSN（社会保障番号／共通番号）が他人に悪用され、なりすまし犯罪の被害者となった個人納税者が、SSN以外の公認の番号で納税申告書の提出ができるように支援することがねらいである。I P P I Nは、IRSが発行する6ケタの番号である。連邦の様式1040〔連邦個人所得税申告書〕事務にのみ利用できる限定番号である。

連邦個人所得税申告では、単身者申告、夫婦個別申告（MF S=marriage filing separately）のほか、夫婦合算申告（MF J=married filing jointly）もできる。夫婦合算申告（MF J）を選択し、配偶者のどちらかがなりすまし被害者である場合も考えられる。この場合、なりすまし被害を受けた配偶者は、I P P I Nの交付を受けて、様式1040〔連邦個人所得税申告書〕にそのI P P I Nを記載することになる。一方、なりすまし被害者ではない配偶者は、様式1040〔連邦個人所得税申告書〕に、SSN（共通番号／社会保障番号）を記載することになる。

I P P I N（身元保護個人納税者番号）を新たに制度化した理由は、納税者が以前にIRSに対して自分の身元を証明する情報を提供しており、かつ、IRSが当該納税者は有効なSSN（共通番号／社会保障番号）の保有者であることを確認できるようにすることにある。

納税者は、IRSから交付された身元保護個人納税者番号（I P P I N）を使って申告書を提出すると、申告時に、標準的な申告手続により有効な納税申告書を提出したものと正式に処理される。

（1）I P P I Nの交付手続

自分のSSNが悪用され、なりすまし不正申告

の被害を受けた個人納税者が、身元保護個人納税者番号（IP PIN）の交付を希望するとする。この場合、当該納税者は、まず、IRSに対してオンライン（ネット）、または電話で、IP PINを申請する自分が、本人であることを証明するように求められる。したがって、申請者は、IRSから確認コード（information code）を受領するために、電子メールアドレスと携帯電話等でIRSとコンタクトできるような環境にあることが必要になる。こうした環境設定が整い、IRSによる身元確認が完了すれば、申請者は、オンラインでIP PINの交付を受けることができる（IRS.gov/getanippin）。

その後、IRSは、その納税者に対して、毎年12月に「通知書CP01A〔私どもIRSはあなたにIP PINを交付した（Notice CP01A: We assigned you an IP PIN）〕」を用いて、新しいIP PINを郵送で交付することになっている。

ちなみに、現行のルールでは、納税者はいったんIP PINの交付申請をし、それが認められた場合には、任意にIP PINの利用を止めること（opt out）はできないことになっている。その後の課税年にわたっても、当該納税者はあらゆる自分の連邦個人所得税関係の納税申告書や各種法定資料に、SSNに代えてIP PINを記載するように求められる。

（2）IP PINの再発行（再交付）

納税者が、IP PINが記された通知書CP0

【図表10】通知書CP01A（IP PIN通知書）
（抜粋）

Department of the Treasury
Internal Revenue Service

Notice CP01A
Tax year 2015
Notice date December 2015
To contact us Phone

Page 1 of 2

Important information about filing your 2015 federal tax return
We assigned you an Identity Protection Personal Identification Number

Our records show that you either:

- were previously a victim of identity theft, or
- notified the IRS that you experienced an incident that could potentially expose you to identity theft, or
- requested an identity protection personal identification number (IP PIN).

We placed an indicator on your account and assigned you an IP PIN for calendar year 2015. The IP PIN helps verify a return filed with your social security number was filed by you. You'll need to use this IP PIN when filing any Forms 1040 during the calendar year beginning in January.

If you fail to use your assigned IP PIN, we could reject your return or delay the processing of your return.

Your assigned 2015 IP PIN is: [REDACTED]

What to remember about your IP PIN

You must use this IP PIN to confirm your identity on your current tax return and any prior year returns filed during the calendar year. We'll send you a new IP PIN each December by postal mail. Therefore, be sure to file Form 8822, Change of Address, if you change your mailing address.

What you need to do

- Keep this letter in a safe place. You'll need it to prepare your tax return.
- When you file your federal tax return, enter the IP PIN in the correct place:
 - If filing electronically, your tax software or preparer will tell you when and where to enter it.
 - If filing a paper return, enter your IP PIN in the gray box marked "Identity Protection PIN" to the right of "Spouse's signature and occupation." If you're married and filing jointly, only the spouse listed first on the tax return needs to enter his or her IP PIN.
- Note: The second spouse's IP PIN still protects his or her account even though it's not entered on a jointly filed paper return.
- If you don't have to file a tax return, you won't need to use your IP PIN. We still protect your account from fraudulent filing.

1A〔IP-PIN通知書〕を紛失した、あるいは新しいIP PINを受け取っていないとする。この場合、当該納税者は、IRSに届出をし、既定の身元確認手続を踏んだうえで、IRSからIP PINの再交付（再発行）を受けることができる。

（3）州所得税との関係

IP PINは、連邦個人所得税の申告に関してのみ使用できる番号である。したがって、州の個人所得税の申告には使用することができない。また、州が個人所得税に関しなりすまし被害者向けに独自のIP PINを交付している場合、そのIP PINは、連邦の個人所得税申告には使用することはできない。

（4）IP PINの交付実績

この新しいIP PINは、納税者になりすまし（IDT）不正申告の被害リスクが続く限り、継続的に毎年、申告期の開始前（通例、各年12月末）までにIRSから交付される。

IP PIN導入直後の2012年申告期をみると、IRSは、25万2,000人にIP PINを交付している。

5 IRSからの身元確認の求め

IRSは、怪しい様式1040〔連邦個人所得税申告書〕の提出をストップしたい場合には、納税者に、書簡5071C（Letter 5071C）を送付することになっている。書簡5071Cは、2015年に導入された。納税者の正確な身元を確認することを目的としたものである。身元確認がすめば、その旨は、郵便で通知される。IRSは、この通知を電話や電子メールでは行わないことになっている。

身元確認にあたり、被害者である納税者は、IRSに、次の情報を提供するように求められる。

【図表11】書簡5071C（Letter 5071C）で提出が求められる情報

- ①氏名、生年月日および連絡先情報
- ②SSNまたは個人納税者確認番号（ITIN=individual taxpayer identification number）
- ③前課税年の連邦所得税申告書（様式14039）、様式W-2〔給与所得の源泉徴収票（Form W-2: Wage and Tax Statement）〕、別表A〔項目別控除明細表（Schedule A: Itemized Deductions）〕など

◆むすびにかえて

誰か他人が自分のSSNを悪用し自分になりすまして、連邦個人所得税申告書（様式1040）を提出していると疑いが出てきたとする。この場合には、そのなりすまし犯罪者（IDT）は、税務だけでなく、他の情報犯罪にも関与している可能性が出てくる。とりわけ、アメリカでは、他人のSSNを悪用してつくられたクレジットカード詐欺が重大な社会問題になっているからである。

したがって、IDTの被害者は、まず、アメリカ3大信用情報機関に連絡して、他人が自分のSSNを悪用して、クレジットカードをつくり、支払不能に陥り、ブラック情報として登載されていないかどうかをチェックする必要がある。そのうえで、これら信用情報機関が、自分が知らないところで開設されたクレジット口座に関するクレジット情報を不要に蓄積しないように凍結する手続をとる必要がある。

FTC（連邦取引委員会）が公表したなりすまし犯罪（IDT）報告によると、FTCに対して被害届、すなわち「身元盗用被害届・宣誓供述書（Identity Theft Victim's Complaint and Affidavit）」の提出により報告があった被害／苦情件数は、国民全体で2015年は49万件あまり（2014年は33万2,600件余り）、不法就労など給与所得還付申告関係で2015年は22万件あまり（2014年は10万9千件余り）である（IRSとFTCとの被害報告件数は必ずしも一致しない。）

すでにふれたように、連邦課税庁であるIRSは、2011年1月から、身元保護PINプログラム（Identity Protection PIN program）を開始した。IRSは、身元保護個人納税者番号（IP PIN）導入直後の2012年申告期実績で、25万2,000人にIP PINを交付している。その後、交付件数は次第に増え、2015暦年分申告期（2016年1月15日～4月18日）には、270万件的身元保護個人納税者番号（IP PIN）を交付（紛失等による再交付分は除く。）している。

全国納税者権利擁護官（NTA=National Taxpayer Advocate）」は、IRS内部にありながら、納税者権利擁護官サービス（TAS=Taxpayers Assistance Service）を提供することにより、IRSの執行部門から独立して納税者からの苦情処理

や、執行体制の見直しを求める報告を連邦議会に行う組織である。NTAは、その年次報告書（annual reports）で、毎年のように、IDT問題の深刻さとIRSの対応の不十分さを指摘している。IRSのIP PINの発行件数は増減を繰り返して、IRSの身元保護機動班（Identity Protection Specialized Unit）もその力量は定かではない、申告期になりすまし（IDT）被害に苦しむ納税者がIRSの納税者保護プログラム（TPP）にコンタクトしても電話は繁忙を理由にほとんどつながらないなど、IRSがIDT対応で抱える問題点を鋭く指摘し、IRSに抜本的なIDT対策の講じるように勧告する報告を行っている。

アメリカは、おおよそ3億2,160万人の人口を抱え、年間2億430万件を超える確定申告書の提出がある。IRSは、納税者保護プログラム（TPP）を通じて、2015年5月末までの1年間に、なりすまし（IDT）の疑いのある67万1,733件（重複は除く。）の不正申告を摘発している。また、2015年暦年分申告期に、IRSは、270万件的IP PINを交付（紛失等による再交付分は除く。）している。

このような数値をどのようにとらえるは悩ましいところである。ただ、共通番号であるSSNの悪用は深刻で、税務分野だけをみて見ても、不正利用が年をおうごとに巧妙になり、対応が後手に回っている感も否めず、減少の兆しを見せていない。IRSやFTC、DODなど行政側となりすまし犯（IDT）とがイタチごっこを繰り返しており、手が付けられなくなっている実情を垣間見ることができる。

わが国政府も、個人番号（マイナンバー）の官民事務への幅広いエスカレート利用に走る愚策を進めていることから、危ない共通番号（SSN）の悪用、なりすまし犯罪対策でムダカネを使い、悪銭苦闘しているアメリカの実情は、対岸の火事といっちはいられない。このまま利用拡大の愚策を進めれば、ジワジワと、アメリカのようななりすまし（IDT）犯罪者天国と化すのも時間の問題であろう。

連邦議会・政府検査院(GAO)の報告書(16年5月公表)を読む 【紹介】『なりすましと租税詐欺』(GAO報告書)

石村 耕治 (PIJ 代表)

◆はじめに

アメリカでは、個人の共通番号である「社会保障番号(S S N=Social Security Number)」を搾取し、巧妙な手口で悪用したなりすまし犯罪(I D T=identity theft)が、全米規模で猛威を振っている。

連邦課税庁である内国歳入庁(I R S=Internal Revenue Service)は、このところ、矢継ぎ早に、なりすまし不正申告防止対策を打ち出して対応に努めている。しかし、なりすまし不正申告はさらに悪化の一途をたどっている。

アメリカの政府検査院(G A O=Government Accountability Office)は、連邦議会の要請にしたがい、2016年5月に、報告書『なりすましと租税詐欺(Identity Theft and Tax Fraud): 内国歳入庁は納税者保護プログラムのリスク査定を改訂する必要がある(IRS needs to update its risk assesment for the taxpayer protection program)』(A4 63頁)を作成し、議会に提出した。

アメリカの政府検査院(G A O=Government Accountability Office)は、わが国の会計検査院のモデルともなった連邦議会直属の機関の1つである。その検査の90%以上は、連邦議会からの検査要請に基づいて実施されている。

GAOの報告書『なりすましと租税詐欺(Identity Theft and Tax Fraud)』では、I R Sの他人のS S Nを悪用したなりすまし不正申告対策に一定の評価を下しながらも、現在のなりすまし不正申告対策の改訂を求め、次のような報告を行っている。

◆GAOはなぜこの検査を実施したのか

2014年、内国歳入庁(I R S)は、概算で225億ドルものなりすまし(I D T=identity theft)不正還付の防止に成功した。しかし、その一方で、31億ドルにもものぼるなりすまし(I D T)不正還付にに応じてしまった。なりすまし(I D T)不正還付は、個人の身元確認情報を入手

し、それを悪用し不正な還付申告を行う形で行われる。I R Sは、納税者の本人確認やなりすまし(I D T)不正還付の防止に努力しているものの、この種の犯罪は進化し、対策コストも高くなっている。

政府検査院(G A O)は、I R Sのなりすまし(I D T)不正還付対策を検査するように要請を受けた。本報告書は、(1) I R Sの納税者保護プログラム(T P P=Taxpayer Protection Program)のパフォーマンスを査定し、かつ、(2) I R Sの2014年度のなりすまし(I D T)不正還付対策コストの評価を行うものである。GAOは、I R Sの納税者保護プログラム(T P P)を査定するために、I R Sの検討結果や指導書をレビューし、かつI R Sの職員と面談を実施した。加えて、GAOは、異なる視角からI R Sの納税者保護プログラム(T P P)分析を実施した場合には、どのような効果が得られるのかを検証するためのシナリオ分析を実施した。I R Sのなりすまし(I D T)対策コスト評価を支援するために、GAOは、GAOコストガイド(GAO Cost Guide)に示された選択的最良の実務に基づきI R Sの方法論を評価した。

◆GAOの勧告事項

GAOは、I R Sが自己の納税者保護プログラム(T P P)を改訂し、かつ、今回の査定において特定されたリスクを縮小するための適切な行動をとるように勧告する。加えて、GAOは、還付額のしきい値を撤廃し、かつ利用できるあらゆる申告水準のデータを活用できるようにし、なりすまし(I D T)対策コスト評価を改善するように勧告する。

I R Sは、GAOのI R S納税者保護プログラム(T P P)に関する勧告、およびI R Sのリスク査定の改訂に同意した。I R Sは、GAOのなりすまし(I D T)対策コスト評価勧告に沿った行動を実施した。

◆GAOが発見した事項

IRS納税者保護プログラム(TPP=Taxpayer Protection Program)：TPPとは、疑念のある納税申告者の身元を確認することにより、なりすまし(IDT)不正還付を防止するプログラムである。IRSは、納税者保護プログラム(TPP)を強化する努力をする一方で、不正を行った者が、その後もすり抜け、不正還付を行っていないかのチェックを実施している。TPPでは、真の納税者が知っているべき質問に答えさせることにより納税者の本人確認を実施している。しかし、不正を行った者は、納税者の個人確認情報(PII=personal identification information)を入手することにより、すり抜けられる。IRSは、160万件の申告書が納税者保護プログラム(TPP)の対象となると見積もっている。これは、2015年申告期では、TPPの本人確認をすり抜けた7,200件ほどのなりすまし不正申告者に対して3,000万ドルを還付することにもつながることを意味する。GAOの分析では、この金額はもっと高くなると見積もっている。IRSは2012年期中において納税者保護プログラム(TPP)のリスク査定を実施したのにもかかわらず、その後、IRSは、なりすまし(IDT)不正還付への現存する脅威〜とりわけ不正申告者のうち、本人確認用の質問をすり抜けるに使う真の納税者の個人確認情報(PII)を保有する者の脅威〜を反映させた形でリスク査定に改訂を加えていない。連邦の電子本人確認ガイダンスは、各機関にプログラムのリスク査定を実施するように義務づけている。改訂されたリスク査定は、納税者保護プログラム(TPP)を強化し、IRSの本人確認の機会の支援につながる。本人確認の強化

は、IRSの歳入損失を少なくし、かつ、不正の被害者となるまじめな納税者が数を減少させる。

なりすまし不正還付コスト評価(IDF Refund Fraud Cost Estimate)：GAOの勧告に従い、IRSは、2014年期中なりすまし不正還付コスト評価を改善するための努力の一環として、新たな方法論を採用した。しかし、評価には、特定の還付額層のしきい値にあてはまらない申告書は含んでいない。IRS職員によると、当該しきい値はIRSの執行事務に優先順位を付けるためのものであるという。しかしながら、しきい値を置くということは、不完全な評価を招くことにもつながる。改善された評価は、どのようにして不正がIRSの防御をすり抜けているのかをよく理解するに役立つ。GAOコストガイドは、コスト評価にはあらゆる関連費用を含むように求めている。加えて、IRSが不正を防止により得た還付額の評価は、グローバル報告書に基づくものとする。グローバル報告書では、IRSが不正申告書を捕えた場合にはその都度計算に入れることになっており、申告書によっては、複数の数を計算に入れることになる。IRSはこの情報源を使用する。なぜならば、なりすまし(IDT)不正還付に関する公式な記録であることからである。GAOコストガイドは、各機関は、評価にあたっては原始データを使用すること、さらには、そのデータには失念も含むこととしている。グローバル報告書によること、したがって申告書段階でのデータを使わないことにより、IRSは、なりすまし(IDT)不正還付に関する不正確な評価にもつながる。このことは、増大するなりすまし(IDT)不正還付を監視しかつそれに戦闘を挑むIRSや議会の努力を無にすることにもつながる。

プライバシー・インターナショナル・ジャパン
(PIJ)

東京都豊島区西池袋3-25-15 IBビル10F 〒171-0021

Tel/Fax 03-3985-4590

編集・発行人 中村克己

Published by

Privacy International Japan (PIJ)

IB Bldg. 10F, 3-25-15 Nishi-ikebukuro

Toshima-ku, Tokyo, 171-0021, Japan

President Koji ISHIMURA

Tel/Fax +81-3-3985-4590

<http://www.pij-web.net>

2016.10.21 発行 CNNニュースNo.87

入会のご案内

季刊・CNNニュースは、PIJの会員(年間費1万円)の方にだけお送りしています。入会はPIJの口座にお振込み下さい。

郵便振込口座番号

00140-4-169829

ピー・アイ・ジェー (PIJ)

NetWorkのつぶやき

・わが国の人口は1億3千万人弱、個人番号カードの申請・交付実績はその1割程度。カード必須のマイナポータルは早、破たんの気配?? 血税浪費、時代遅れのカード発行を停止し、「暗証番号+Q&A」でログインできるシステムへの移行は急務 (N)