

## [® 研究論文]

# マイナンバーカードのおもて面情報を個人情報管理で利用する場合のリスクに関する一考察

A Study on the Risks of Using the Front Information on My Number Cards  
in Personal Information Management

福永 栄一  
Eiichi Fukunaga

大阪成蹊短期大学  
Osaka Seikei College

## 概要

マイナンバーカードの利用で懸念されることは、マイナンバーカードの裏面に記載された個人番号による国民総背番号化と、個人番号とともに収集される特定個人情報の漏えいである。これらを防止するために、マイナンバーカードの裏面に記載された個人番号の利用を法律で定めた場合のみに限定している。しかし、マイナンバーカードのおもて面は公的な身分証明書として使用できることが政府や地方自治体から広報されており、個人番号が記載された裏面のような制限はない。ところが、マイナンバーカードのおもて面には氏名、住所、生年月日、顔写真などが記載されており、これらをスキャンしてデジタル情報にすればコンピュータで個人情報管理に利用できる。この情報は運用次第では個人を特定する情報として利用できる。そこで本論では、マイナンバーカードのおもて面の情報を利用した個人情報管理のリスクと影響を検証してその対応について提言した。

キーワード：マイナンバーカード、おもて面、ICチップ、個人番号、共通番号

## 1 はじめに

マイナンバー制度が始まり政府はマイナンバーカードの普及と利活用を推進している<sup>注1)</sup>。マイナンバーカードが普及し、あらゆる場面で使われれば社会のメリットは大きく、筆者もマイナンバーカードの利活用に賛成であり、そのメリットに期待している。しかし、マイナンバー制度で収集された個人情報の漏えいや個人情報の不正利用、国による個人の監視強化などに対する不安も指摘されている<sup>1) 2)</sup>。

マイナンバーカードには3つの利用箇所がある。①裏面、②ICチップ、③おもて面の3つである。マイナンバーカードの裏面には、国民一人ひとりが持つ12桁の番号<sup>3)</sup>である個人番号が記載されている。個人番号は国民一人ひとりを特定できる一意の番号であり、国民の共通番号である。共通番号であるがゆえに、マイナンバー制度から国民総背番号化の負の部分が連想され<sup>1)</sup>、国民の

権利が国によって不当に制限されるなどの不安につながる。そのようなことが生じないように、行政手続における特定の個人を識別するための番号の利用等に関する法律（以下、「番号法」と表記する）で個人番号の利用者や利用範囲を限定している。

マイナンバーカードのICチップには公的個人認証で使用する「署名用電子証明書」と「利用者証明用電子証明書」が標準的に搭載されている<sup>4)</sup>。この公的個人認証の部分とICチップの空きスペースをマイキー部分といい、ここを活用してマイナンバーカードを公共施設や商店街など民間でも活用できるようにするマイキープラットフォーム構想がある<sup>注2)</sup>。マイキープラットフォームでは利用者を一意に特定できるマイキーIDを利用する<sup>5)</sup>。このマイキーIDも国民の共通番号になりうる番号である。そのためICチップの空き領域は「市町村・都道府県等は条例で定めるところ、

投稿受理日	2017年3月31日
再投稿受理日	2017年10月16日
査読完了日	2017年11月6日

国の機関等は総務大臣の定めるところにより利用可能、新たに民間事業者も総務大臣の定めるところにより利用可能に」<sup>5)</sup>としている。この大臣認定基準は、「国民の電子証明書をセキュアに扱う体制があるか否かである」<sup>6)</sup>とされており、ICの利用においては政府主導で高いセキュリティを確保したシステムを作り、セキュリティを維持できる事業者が利用することで個人情報を守っている。

マイナンバーカード3つ目の利用箇所であるおもて面は、本人確認の際の公的な身分証明書として利用できる<sup>4)</sup>。そのため、マイナンバーカードは「文字をレーザーにより彫りこむとともに、複雑な彩紋パターンを施す等により、券面の偽造を困難にしています」<sup>7)</sup>とされている。マイナンバーカードのおもて面はアナログ情報を目視で確認することを想定しており、使用に関して特に制限はない。アナログ情報なのでコンピュータで使うことを想定していない。しかし、マイナンバーカードのおもて面には氏名、住所、生年月日、有効期限、16桁の製造番号、4桁のセキュリティコード、顔写真（以下、おもて面情報<sup>※3)</sup>と表記する）などが記載されている。このアナログ情報はスキャンして処理すればデジタル情報にしてコンピュータで利用することができる。身分証明書としてマイナンバーカードを提示された際に、マイナンバーカードのおもて面情報を利用することとその利用目的を明示しておもて面情報を取得すれば、おもて面をスキャンして処理したデジタル情報を個人情報管理のための情報として利用することができる。この情報は4章で示すように、使い次第では利用者本人を特定できる一意の番号とほぼ同様に利用可能な情報である。マイナンバーカードの裏面に記載されている個人番号やマイキーIDが有する共通番号としてのリスクとほぼ同様のリスクを有する情報である。したがって、おもて面情報も個人番号やIC部分と同様に不当に利用されることや漏えいから守られるべきであるが、おもて面は身分証明書として使用できることが強調されるばかりである。

そこで本論では、マイナンバーカードのおもて面情報を個人情報管理に利用する場合のリスクと影響、その対応について提言する。まず、マイナンバーカードの利用に関する検討例と先行研究を確認する。次に、従来のポイントカードによる個人情報管理と個人情報漏えいリスクを確認する。

さらに、マイナンバーカードのおもて面情報を利用した個人情報管理を例示する。そのうえで、マイナンバーカードのおもて面情報を個人情報管理に利用する場合のリスクと影響を検証して、その対応について提言する。

なお本論では、今後マイナンバーカードが順調に普及し、国民の多くが所持し、多くの機会に身分証明書や本人確認書類として使うことを前提として検証等を行う。また、本論で対象としている個人情報、取得に際して利用目的の明示等を行うなど個人情報の保護に関する法律（以下、個人情報保護法と表記する）に従って適正に取得・利用することを前提としている。

## 2 マイナンバーカードの利用に関する検討例と先行研究

マイナンバーカードは裏面とICチップ、おもて面の利用が考えられる。しかし、裏面の個人番号は番号法で利用者や利用範囲が限定されている。個人情報保護委員会のWebページの事業者編Q&Aの回答A6-2の後半に「個人番号の確認の際に、本人確認書類のコピーの提出を受けた場合、必要な手続を行った後に本人確認書類が不要となった段階で、速やかに廃棄しましょう」<sup>8)</sup>と記載されており、民間で裏面を利用することは考え難い。

ICチップの利用は、健康保険証や社員証、ポイントカードなどが考えられている<sup>4)</sup>。電子証明証のIDとクレジットカード番号を連携させることでクレジットカードとして活用することも考えられている。「クレジットカードについては代替というより、本来のクレジットカードはそのままに、希望者がマイナンバーカードにクレジット機能を搭載することを想定している」<sup>6)</sup>ようである。また、マイナンバーカードを親カードとして紐付けた別のICカードを組み合わせる使い方も政策提言されている<sup>9)</sup>。

図書館では、マイナンバーカードを図書館カードとして使うことについて、マイキープラットフォームを使うことを前提として、複数設置母体の図書カードを1枚にまとめられる利点を示しながら使用することの論点・課題整理がなされている<sup>10)</sup>。姫路市では、全国初となるマイナンバーカードの電子証明書を活用した図書館利用サービスを平成28年11月27日に開始したこと、今後は図書館サービスでのマイナンバーカードの利用を播

磨圏域連携中枢都市圏の市町へと拡大を図りたいこと、福崎町と神河町が平成28年度中に姫路市方式によるサービスを開始することが決定し、マイナンバーカードの共通利用が実現することになったことが報告されている<sup>11)</sup>。

マイナンバーカードのICの媒体識別番号(製造番号)をマイナンバーカード固有の番号として個人認証に使うことも研究されている。たとえば入退室管理に利用する<sup>12)</sup>ことや、カードによる安否確認として避難所へのチェックインや子供の帰宅時の見守り<sup>13)</sup>などである。様々なサービスを検討したが、マイナンバーカードのICの媒体識別番号の一部が乱数で決定されるため固有番号として利用できない<sup>14)</sup>という政策提言もある。

このようにマイナンバーカードの利用に関する検討例や研究はほとんどがICチップである。おもて面は、氏名、住所、生年月日、性別(以下、氏名等4情報と表記する)と顔写真が記載されており、身分証明書を想定した構造である。さらに政府や地方公共団体がマイナンバーカードを本人確認の際の公的な身分証明書として利用できることをマイナンバーカードの説明で必ず広報していることも、おもて面を身分証明書以外で利用することが検討されない理由である。

マイナンバーカードに関連した個人情報の漏えいや個人情報が不当に管理・利用されることへの指摘<sup>1)</sup><sup>2)</sup>もなされているが、その個人情報はマイナンバー制度によって収集される個人番号を含んだ特定個人情報である。マイナンバーカードのおもて面の情報は番号法に関係なく利用できる通常の個人情報なので、マイナンバーカードの利用と関連付けて研究されていない。しかし、マイナンバーカードのおもて面情報はスキャンして処理すればデジタル情報にして個人情報管理に利用できる。国民一人ひとりを特定できる一意の番号である共通番号とほぼ同様に利用可能である。そこで以下では、組織ごとに別々のカードを発行して個人情報を管理している現状と、マイナンバーカードのおもて面情報を利用した個人情報管理のリスクと影響を比較する。先ず次章で、従来のポイントカードを例にして、その個人情報管理と個人情報漏えいリスクと影響について確認する。

### 3 従来のポイントカードによる個人情報管理と個人情報漏えいリスクと影響

我々は数多くのポイントカードを所有して日々

持ち歩いている。カード利用者は、カードを作成するときに氏名等4情報を提供して、それ以降商品を購入してカードを提示するたびにポイントが付与され、個人情報が収集される。カード利用者は、収集された個人情報が増えるごとに、その個人情報が漏えいして不当に利用されることへの不安も増大する。

ポイントカードはTカードやPontaカード、nanacoカードなど広範囲に共通で使えるものが多くの会員を得ている。例えばTカードの会員数は2017年7月末現在で6,373万人<sup>15)</sup>、Ponta会員数は2017年8月末日で8,330万人<sup>16)</sup>、nanaco会員数は2017年2月末現在で5,350万人<sup>17)</sup>である。合計すると2億53万人になるが、これら3つ以外にも会員数が多いポイントカードが複数ある。このように、多くの会員を集めているポイントカードに個人情報が集約されつつあり、前述したカード利用者の不安は増すばかりである。

しかし、個人情報が一つのポイントカードに統合されているわけではない。1店舗限定のポイントカードを含めれば、我々はいまだに数多くのポイントカードを所有している。ポイントカードが別々に発行されることで紛失や盗難などのリスクも分散されている<sup>2)</sup>。個人情報もポイントカードごとに別々のキーで、別々の組織(場所)に分散管理されており、個人情報が一つのキーで一カ所に集中管理されることから免れている。そのため、もし一つのポイントカードの個人情報が漏えいしても、別のキーで管理されている他のポイントカードの個人情報がアクセスされることはない。また、同時に二つのポイントカードの個人情報が漏えいしても、キーが別々なので容易に二つの個人情報を1つに集約することはできない。個人情報が別のキーで別の組織に分散管理されることは、カード利用者の個人情報が漏えいして不当に利用されるリスクを低減している。

しかし、次章で示すようにマイナンバーカードのおもて面情報を利用して個人情報を管理するようになれば、一つのポイントカードの個人情報が漏えいした場合は、他のポイントカードの個人情報がアクセスされるリスクが生じる。また、複数のポイントカードの個人情報が漏えいした場合は、これら個人情報をマイナンバーカードのおもて面情報で集約されるリスクも高まる<sup>18)</sup>。

## 4 マイナンバーカードのおもて面情報を利用した個人情報管理

この章ではまず、マイナンバーカードのおもて面情報の取り込み方法を示し、次にマイナンバーカードのおもて面情報で個人情報を管理する場合のキーを示す。そしてマイナンバーカードのおもて面情報を利用した個人情報管理の例として、既存のポイントカードを代用する情報システムを例示する。

### 4.1 おもて面の情報の取り込み方法

文字や数字はOCR処理でデジタル情報に変換できる。身近なOCR処理といえば名刺管理ソフトである。名刺を読み取らせると高い精度で文字変換する。マイナンバーカードはおもて面の情報の位置が決まっているので、位置に合わせて読み取れば、読み取り精度を高くできる。名刺のように自由フォーマットの中から名前や住所を見つけ出して読み取るのではなく、フォーマットが統一されたマイナンバーカードの定まった位置から名前や住所を読み取るので、読み取り精度を高くできる。使用される文字もマイナンバーカードの基準に従ってフォントや文字の大きさなどが統一されているので、読み取り精度を高くできる。顔写真はスキャンして処理すればデジタル情報に変換できる。マイナンバーカードのおもて面に記載されている情報は、免許証と同様個人情報保護法に従えば取得して利用できる。

### 4.2 マイナンバーカードのおもて面情報で個人情報を管理する場合のキー

ここでは、マイナンバーカードのおもて面情報のどの項目が個人情報を特定するキーとして利用できるかを考える。1つ目のキー候補としてマイナンバーカードの顔写真の下の16桁の番号が考えられる。この番号についてマイナンバーカード総合サイトにメールで確認したところ、マイナンバーカードの製造番号であることが分かった。しかし、マイナンバーカードに対して一意である確証は得られなかった<sup>注4)</sup>。一意の確証はないが、製造番号なので一意に近い番号と判断した。

2つ目のキー候補として顔写真が考えられる。マイナンバーカードの顔写真はカード配布時に本人確認のために利用する写真であり、写真に関して細かく指示がなされている<sup>19)</sup>。本人を確認でき

る写真であり、顔写真をデジタルデータに変換してキーにすれば高い精度で個人を特定できると考えられる。しかし、個人を多数の中から一意で認識できる確証はない。

3つ目のキー候補として氏名、住所、生年月日、有効期限、セキュリティコード（製造番号の右に記載されている4桁の数字）の5項目が考えられる。同じ名前で同じ誕生日の2人のAさんが同じ住所に住んでいて同じ年の誕生日前にマイナンバーカードを受け取る場合などに氏名、住所、生年月日、有効期限が同じになる。さらにその二人のマイナンバーカードのセキュリティコードが同じ場合、氏名、住所、生年月日、有効期限、セキュリティコードの5項目が重複する。従って一意と言い切れないが、これらが重複する確率が極めて小さいことも明らかである。

以上の3つの候補は一意を保証できないが、3つとも重複は稀なキー候補である。そこで、3つを組み合わせたおもて面情報（氏名、住所、生年月日、有効期限、16桁の製造番号、4桁のセキュリティコード、顔写真）をキーにすることが考えられる。このキーで絶対一意になるとは言いきれないが、実際の運用上はこの組み合わせでキーが重複することも考え難い。そしてこのキーで既存のポイントカードを代用する情報システムを考える。こうすれば、万が一、おもて面情報で一意にならない顧客がいても、従来のポイントカードを使ってもらえる。このような運用を前提に、次節でマイナンバーカードのおもて面情報で既存のポイントカードを代用する情報システムを示す。

### 4.3 マイナンバーカードのおもて面情報を利用して既存のポイントカードを代用する情報システム

例えば、Aさんが衣料品店Xのポイントカードを所持している場合を考える。その場合、Aさんは衣料品店Xにマイナンバーカードとポイントカードを提示して、マイナンバーカードのおもて面情報とポイントカードのカード番号の関連付けをしてもらう（図1参照）。同時にマイナンバーカードといっしょに配布されたカードケースの目隠し部分に、そのマイナンバーカードとポイントカードを関連付したことを示す関連済シールを貼る<sup>注5)</sup>。

これ以降、Aさんは衣料品店Xにカードケースに関連済シールを貼った<sup>注6)</sup>マイナンバーカードを提示すれば、おもて面情報から関連付けたポイ

ントカードの番号 X-1234 のデータベースにポイントと購入履歴が登録される (図 2 参照)。新規でポイントカードを発行する場合は、ポイントカードを発行すると同時にマイナンバーカードのおもて面情報とポイントカードのカード番号の関連付けをし、カードケースに関連済シールを貼る。このようすれば、ポイントカードのカード番号と

関連付けてマイナンバーカードのおもて面情報で個人情報を管理することができる。他の企業も同様にすれば、Aさんは複数のポイントカードをマイナンバーカード1枚で代用できるようになると同時に、複数のポイントカードの個人情報がマイナンバーカードのおもて面情報を用いて管理されることになる。

図 1. おもて面情報とポイントカードの番号の関連付け

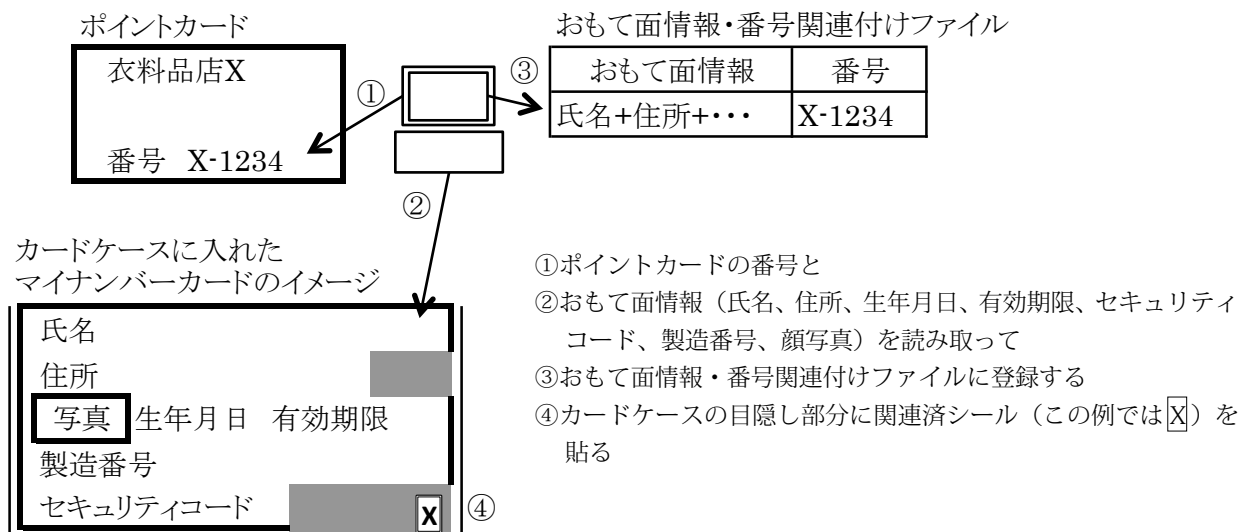
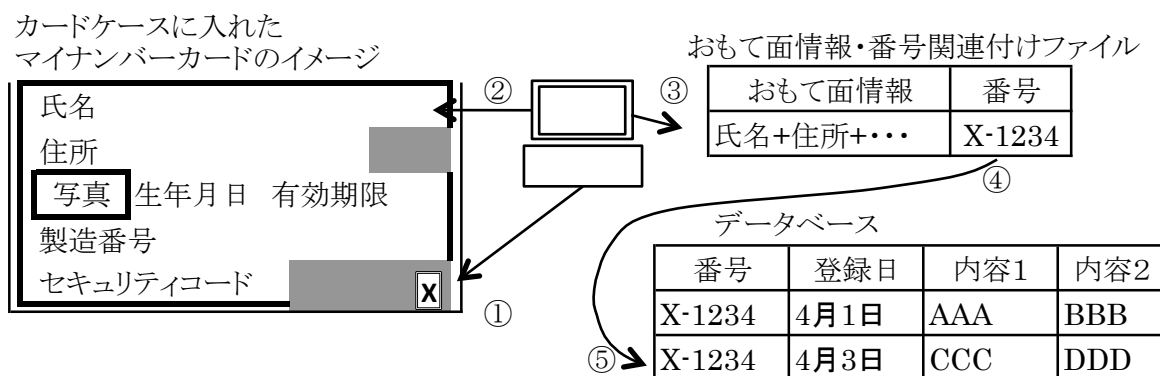


図 2. マイナンバーカードのおもて面情報でのポイントカードの代用



- ①関連済シールをチェックする
- ②おもて面情報 (氏名、住所、生年月日、有効期限、セキュリティコード、製造番号、顔写真) を読み取って
- ③おもて面情報・番号関連付けファイルを読み
- ④ポイントカードの番号を取得して
- ⑤データベースに登録する

## 5 マイナンバーカードのおもて面情報を利用した個人情報管理のリスクと影響

この章ではマイナンバーカードのおもて面情報を個人情報管理に利用する場合のリスクと影響をまとめる。

### 5.1 公的機関による管理

国や地方公共団体がマイナンバーカードのおもて面情報を利用することが考えられる。国や地方公共団体は、マイナンバーカードのおもて面情報の構造を把握している。国や地方公共団体は、おもて面に記載された16桁の製造番号の構造が分かる。もし製造番号がマイナンバーカードに対して一意であれば、製造番号をキーにして国民の個人情報を管理することができる。顔認証の精度も分かるので、顔認証で国民一人ひとりを特定できるようになった時点で顔写真の情報で個人情報を管理できる。また、氏名、住所、生年月日、有効期限、セキュリティコードの5項目での個人情報管理の可能性を考えたが、住民票を管理する側であれば正確に活用の可能性が判断できるであろう。

マイナンバーカードのおもて面情報は個人番号とは関係ないので、番号法の制限を受けない個人情報で、個人情報保護法に従って利用目的の範囲であれば自由に使える。個人番号は番号法で国民総背番号化に利用されることを防止しているが、マイナンバーカードのおもて面情報にはそのような防止策はなく、国民総背番号化に対する懸念が生じる。

### 5.2 一元管理

マイナンバー制度においては「国家により個人の様々な個人情報が個人番号をキーに名寄せ・突合されて一元管理されるのではないか」といった懸念<sup>20)</sup>を払しょくするために個人情報の管理の方法について一元管理ではなく、分散管理である<sup>20)</sup>ことが強調されている。しかし、マイナンバーカードのおもて面情報は上記に述べたように自由に利用できる。マイナンバーカードのおもて面情報を利用すれば個人情報を一か所に集めて一元管理することが可能になる。国や地方公共団体による一元管理や個人情報保護法に従った企業の共同利用や第三者提供による一元管理が可能になる。

## 5.3 個人情報の漏えい

### (1) 漏えい被害の拡大

上記のように一元管理が実施されたときは、個人情報が漏えいした場合の被害はこれまでより大きくなる。特に、ポイントカードを運営する企業がそろってマイナンバーカードをポイントカードの代用として使用した場合は、もし一つのポイントカードの個人情報が漏えいした場合、別のポイントカードの個人情報が不正に盗まれる可能性が生じるからである。マイナンバーカードのおもて面情報から関連付けられるポイントカードの番号に不正にアクセスされて個人情報の窃盗につながる可能性が高くなる。

### (2) 個人情報の集約

複数のポイントカードの個人情報が漏えいした場合、マイナンバーカードのおもて面情報から関連付けられるポイントカードの番号から複数のポイントカードの個人情報を集約することが可能になる。複数のポイントカードの個人情報がまとめられて不当に利用された場合やゆがめられて利用された場合の影響は極めて大きい。

## 5.4 長期、大量の個人情報

マイナンバーカードは有効期限が10年である。10年後に更新した場合もマイナンバーカード所有者からマイナンバーカードが新しくなったことを申告してもらい、新しいマイナンバーカードで本人確認し、登録しておいた旧マイナンバーカードの顔写真や氏名等で同一人物であることを確認すれば、新旧マイナンバーカードのおもて面情報を連結できる。連結により新しいマイナンバーカードのおもて面情報も個人情報管理で利用できる。マイナンバーは一生使うもの<sup>3)</sup>と総務省Webページに記載されており、マイナンバーカードも同様に一生使用するならば、一生分の個人情報の管理にマイナンバーカードのおもて面情報が利用できる。

従来であれば、ポイントカードの利用をA社からB社に変えればカード番号が変わるが、マイナンバーカードをポイントカードの代用として使えば、A社でもB社でもマイナンバーカードのおもて面情報が個人情報管理に利用できる。一生涯マイナンバーカードのおもて面情報が個人情報管理に利用される。この個人情報が漏えいして、不当

に利用された場合やゆがめられて利用された場合の影響は極めて深刻である。

## 6 マイナンバーカードのおもて面情報を利用した個人情報管理のリスク対応

この章では前章で確認したリスクと影響への対応をまとめる。まず、全てに共通することは、①マイナンバーカードのおもて面はデジタルデータとして利用できること、②個人情報管理に利用できること、③おもて面情報が共通番号とほぼ同様に使えることを政府、企業、国民が共通認識することである。マイナンバーカードのおもて面は身分証明書以外では使われない、氏名等4情報はICチップを利用して取得すると考え、マイナンバーカードのおもて面情報を個人情報管理に利用する可能性とそのリスクをあいまいにしたままにしておくことが最大の問題である。

### 6.1 公的機関によるガイドライン

マイナンバーカードのおもて面情報がコンピュータで利用でき、共通番号とほぼ同様に使えることを認識したうえで、政府や地方公共団体が積極的に広報して、国民に知らしめるべきである。さらに、おもて面情報を個人情報管理に利用する場合のガイドラインを決定し、ガイドラインにそった情報システムの開発・運用を指導すべきである。

マイナンバーカードのICチップは媒体識別番号の一部を乱数表示するので、固有番号とならない<sup>14)</sup>。その理由の一つは、媒体識別番号を共通番号として利用されないためであろう。また、マイナンバーカードのおもて面に表記された16桁の製造番号は、カード製造などの際に管理する番号であり、製造番号であれば通常は固有番号である。それを確認するために発番方法について質問した回答は「発番方法については、セキュリティの関係上、お答えすることが出来かねます」<sup>注4)</sup>であった。このセキュリティにも製造番号が共通番号として利用されないためという意味が含まれると考える。マイナンバーカードの個人番号は法律によって使用が制限され、ICチップ内の電子証明書は民間事業者であれば総務大臣が認めないと使用できない。使用制限できない媒体識別番号は特殊な機能を追加して固有番号にならないようにしている。マイナンバーカードのおもて面の製造番号の構造は公開されない<sup>注4)</sup>。これらは全てマイナ

ンバーカードによって作り出される国民一人ひとりを特定できる一意になりうる番号の使用を制限するためである。おもて面情報は使用制限できないのであれば、マイナンバーカードを発行する公的機関が安全に使えるように指導すべきである。

### 6.2 おもて面情報を個人情報管理で利用する場合のキー構造

おもて面情報を個人情報管理で利用する場合に、組織独自の番号や記号をランダムに追加し、組織が違えばキーが異なる仕様にする。キーが異なれば共通番号にならないので、一つのポイントカードの個人情報が漏えいしても、別のポイントカードの個人情報が不正アクセスされて個人情報の窃盗につながる可能性を低減できる。また、複数のポイントカードの個人情報が漏えいした場合もキーをもとに集約される可能性を低減できる。

### 6.3 匿名加工情報への加工とデータ消去

個人情報保護法が改正され、特定の個人を識別することができないように加工した匿名加工情報の内容が追加された。また第19条に個人データを利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めなければならないという内容が追加された。これらを尊重して、取得した個人情報はできるだけ早い段階で匿名加工情報に加工し、加工した元データもできる限り早く消去すべきである。個人が特定されない情報であれば漏えいや不当利用から守られる。

### 6.4 企業の対応

個人情報保護法への対応および上記3項目の対応に加えて、企業ではさらに以下の個別の対応が必要である。

#### (1) 本人から同意を得る

マイナンバーカードのおもて面情報を取得するのは、個人情報保護法第18条2の「直接書面に記載された当該本人の個人情報を取得する場合」にあたるので、利用目的を明示しなければならない。その際にマイナンバーカードのおもて面情報をコンピュータに取り込んで利活用することによるリスクと対応を本人に説明して同意を得る。

#### (2) おもて面情報の認識

個人情報を扱う社員全員がマイナンバーカードのおもて面情報が共通番号とほぼ同様に使え

ることを認識する。

### (3) 厳格なおもて面情報の取り扱い規定

- ・おもて面を目視で確認するだけの場合  
目で見ても内容を確認・照合するだけで、コピーをしてはいけないなどを規定する。
- ・おもて面情報をデジタル情報としてコンピュータに取り込む場合  
おもて面をスキャンして取り込むのか、目で見ても手入力するのか、おもて面をその場で直ぐに取り込むのか、コピーを取って後から取り込むのかなどを規定する。
- ・おもて面情報をデジタル情報としてコンピュータに取り込み個人情報管理に利用する場合  
おもて面情報を個人情報管理で利用する場合、キーに企業独自の番号や記号をランダムに追加すること、その仕様、匿名加工情報にする仕様と時期、データを消去する時期などを規定する。キーは原則画面上に表示しないことなどを規定する。

### (4) コピーやスキャンの中間データの扱い

誰がコピーもしくはスキャンするのか、コピーやスキャンの中間データは誰から誰に、どの部署からどの部署に渡し、どこで保管するのか、いつ破棄・消去するのかなどを規定する。

### (5) 教育の実施

これらに関して定期的・継続的に教育し、常に適切な対応がなされるようにする。

### (6) システム監査

システム監査においてこれらの対応について調査して評価する。監査する側もマイナンバーカードのおもて面情報が共通番号とほぼ同様に使えること、おもて面情報を利用して個人情報を管理した場合に生じるリスク、情報漏えいなどが発生した場合の影響を認識して監査を実施する。

## 7 おわりに

本論では、マイナンバーカードのおもて面情報を利用して既存のポイントカードを代用する情報システムを例にして、マイナンバーカードのおもて面情報を個人情報管理に利用できることを示した。そのうえで、マイナンバーカードのおもて面情報を利用した個人情報管理のリスクと影響を検証してその対応を提言した。マイナンバーカードが今後普及して利活用が進む過程において、IC

チップ内の情報のみならずおもて面情報もデジタルデータとして利用できることを考慮して、情報システムによる個人情報保護の規定や機能を定め、システム監査においてその開発、運用を調査、評価していかなければならない。

マイナンバーカードのおもて面情報を個人情報管理に利用した例や、本論で例示したシステムの運用は確認できていない。しかし、マイナンバーは一生使うもの<sup>3)</sup>であり、10年後の更新時にマイナンバーカードが廃止になっている可能性は低い。一生であれば50年後もマイナンバーカードを使っている。今後、マイナンバーカードの裏面の個人番号やICチップとともにおもて面情報も安全・安心に利活用されることが必要と考える。おもて面情報が共通番号とほぼ同様に使えることを政府、企業、国民ができる限り早く共通認識し、リスクと対応を考え、マイナンバーカード利活用の効果を最大限発揮できる仕組みの確立が必要である。

### <注>

- 1) 平成28年5月20日の閣議決定において、世界最先端IT 国家創造宣言が変更されており、国が率先してマイナンバーカードの普及と利活用を推進するため、平成28年度から国家公務員IC カード身分証のマイナンバーカードへの一体化を順次進めることや、マイナンバー制度を活用した国民生活の利便性の向上などが宣言されている。(世界最先端IT 国家創造宣言の変更について、首相官邸、<http://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20160520/siryoul.pdf> アクセス日:2017年10月12日)
- 2) 総務省Web ページの報道資料「マイキープラットフォームの運用開始等」([http://www.soumu.go.jp/menu\\_news/s-news/01gyosei07\\_02000053.html](http://www.soumu.go.jp/menu_news/s-news/01gyosei07_02000053.html)、平成29年9月21日 アクセス日:2017年10月12日)によるとマイキープラットフォームは2017年9月25日から運用が開始されている。
- 3) 性別を含めなかった理由は、マイナンバーカードといっしょに配布されたカードケースを使用すると性別が隠れて見えないためである。
- 4) マイナンバーカード総合サイトに以下の質問をして回答を得た。

#### <質問>

マイナンバーカードの写真下の16桁の製造番



号について質問します。

製造番号はマイナンバーカードに対してどのように発番されていますか？

以下の1。2。3。のどれになるか教えてください。

- 1.1 対1で発番され、製造番号が重複することは無い
2. ロット単位などで発番され、同じ製造番号が複数のマイナンバーカードにつけられている。
3. その他
3. その他の場合は、どのような発番方法か教えてください。

<回答> 2017年10月06日(金)

マイナンバーカードの顔写真の下に記載がございます16桁の製造番号は、カード製造などの際に管理する番号となっております。なお、発番方法については、セキュリティの関係上、お答えすることが出来かねます。

- 5) カードケースが無い場合は、マイナンバーカードのカードケースのような簡易のケースを渡してシールを貼ってもらう。マイナンバーカードはまだ使い方が明確になっていないので、おもて面には貼らずケースに貼るようにする。
- 6) カードケースを忘れた場合や関連済シールがはがれた場合は、提示されたマイナンバーカードのおもて面情報の顔写真と記録されている顔写真、さらに本人を見比べて関連付け済を確認する。

#### <参考文献>

- 1) 眞次宏典、マイナンバー制度の問題点について、地域総合研究、第17号、Part1、pp.97～103 (2016)
- 2) 高橋秀雄、マイナンバー制度の問題点について、中京企業研究、38号、pp.1～12 (2016)
- 3) 総務省、マイナンバー制度、[http://www.soumu.go.jp/kojinbango\\_card/01.html](http://www.soumu.go.jp/kojinbango_card/01.html) アクセス日：2017年10月12日
- 4) 総務省、マイナンバーカード、[http://www.soumu.go.jp/kojinbango\\_card/03.html](http://www.soumu.go.jp/kojinbango_card/03.html) アクセス日：2017年10月12日
- 5) 総務省、マイキープラットフォーム構想の概要～地域活性化戦略(素案)～、[http://www.soumu.go.jp/main\\_content/000405393.pdf](http://www.soumu.go.jp/main_content/000405393.pdf)、個人番号カード・公的個人認証サービス等の利

活用推進の在り方に関する懇談会、マイキープラットフォームによる地域活性化方策検討会(第2回) 配付資料 アクセス日：2017年10月12日

- 6) Card wave、都市小屋 集のICカード研究会(207) マイナンバーカードの概要と公的個人認証サービスを活用したオンライン取引の可能性、29(3)、pp.28～37 (2016)
- 7) 地方公共団体情報システム機構、「セキュリティ」もしっかり「マイナンバーカード」、<https://www.kojinbango-card.go.jp/kojinbango/security.html>、マイナンバーカード総合サイト アクセス日：2017年10月12日
- 8) 個人情報保護委員会、Q&A(回答)、<https://www.ppc.go.jp/legal/policy/answer/> アクセス日：2017年10月12日
- 9) 高村茂、政策提言 マイナンバーカードを用いた独自サービス六つの方策(後編)「見せる」だけから「子カードとの組み合わせ」まで、地方行政、Vol.10711、pp.8～11 (2017)
- 10) 奥野吉宏、「マイナンバーカード」を「図書館カード」として使用することについての論点・課題整理、[http://www.jla.or.jp/Portals/0/data/iinkai/jiyu/mynorev\\_jlajiyu\\_20170115.pdf](http://www.jla.or.jp/Portals/0/data/iinkai/jiyu/mynorev_jlajiyu_20170115.pdf)、日本図書館協会、図書館の自由通信、pp.1～8 (2017) アクセス日：2017年10月12日
- 11) 姫路市総務局情報政策室、Search!! 番号制度 マイナンバー制度の活用に向けて 姫路市におけるマイナンバーカードによる図書館利用サービスについて、J-LIS、3(11)、pp.31～36 (2017)
- 12) 安岡孝一、マイナンバーの利活用と個人番号カードの活用の実際 地方自治体や民間事業者にとっての活用の可否は、<http://hdl.handle.net/2433/217947>、OMNI-MANAGEMENT、24(10)、pp.6～9 (2015) アクセス日：2017年10月16日
- 13) 指定都市市長会、マイナンバー制度の独自活用方法の検討について、[http://www.siteitosi.jp/activity/pdf/h27\\_05\\_12\\_03\\_siryu/h27\\_05\\_12\\_03\\_03.pdf](http://www.siteitosi.jp/activity/pdf/h27_05_12_03_siryu/h27_05_12_03_03.pdf)、調査・研究・データ、政策提言プロジェクト アクセス日：2017年10月12日
- 14) 高村茂、政策提言 マイナンバーカードを用

- いた独自サービス六つの方策(前編)フェリカカード参考に「こういうアプリあれば」の発案を、地方行政、Vol.10710、pp.2～5 (2017)
- 15) CCC、6、373万人の会員基盤、[http://www.ccc.co.jp/showcase/sc\\_004051.html?cat=plat](http://www.ccc.co.jp/showcase/sc_004051.html?cat=plat) アクセス日：2017年10月12日
- 16) Loyalty Marketing、Inc.、事業情報、<https://www.loyalty.co.jp/business> アクセス日：2017年10月12日
- 17) セブン・フィナンシャルサービス、電子マネー事業、<https://www.7fin.jp/division/electronicmoney.html> アクセス日：2017年10月12日
- 18) 渡邊創、映像情報メディア関連のセキュリティ(最終回) マイナンバー制度とマイナンバーカード、映像情報メディア学会誌、Vol.70、No.4、pp.593～602 (2016)
- 19) 地方公共団体情報システム機構、顔写真のチェックポイント、<https://www.kojinbangocard.go.jp/kofushinse/checkpoint.html>、マイナンバーカード総合サイト アクセス日：2017年10月15日
- 20) 総務省、マイナンバー制度における情報連携について、[http://www.soumu.go.jp/main\\_content/000429540.pdf](http://www.soumu.go.jp/main_content/000429540.pdf)、地方財政審議会、平成28年度地方財政審議会(5月24日)議事要旨、説明資料 アクセス日：2017年10月12日