特 集

マイナンバー制度
― そのリスクと取扱いの要点

本年10月からマイナンバーの通知が開始され、来年の1月からは利用が始まります。市民や行政において利便性が向上する反面、不正利用や漏えいのリスクもあり、個人事業主である弁護士には、中小規模事業者として安全管理措置を講じる必要があります。

プライバシーの保護に敏感であるべき弁護士から、漏えい等による被害を生じさせるようなことがあれば、業界全体への信頼を失いかねません。

そこで本特集では、制度を概観した上で、そのリスクと取扱いの要点についてお伝えします。

宮内 宏（61期）
●Hiroshi Miyauchi
当会会員

〈略歴〉
昭和60年　東京大学大学院修士課程（電子工学）修了
　　日本電気株式会社入社
平成19年　東京大学法科大学院卒業
平成20年　弁護士登録
平成23年　宮内宏法律事務所（現 五番町法律事務所）開設

1 はじめに

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」といいます。）により、平成27年10月からマイナンバーの通知が開始され、平成28年1月からは利用が始まります。弁護士の活動にあたっては、マイナンバーを扱う機会が増えてくると思われますが、まだまだ分からないことが多い方もいらっしゃることと思います。

本稿では、マイナンバー制度を概観した上で、マイナンバーに関するリスクを示し、特定個人情報（マイナンバーを内容として含む個人情報）の安全管理措置等の、弁護士等の個人事業主を含む中小規模事業者での対応について述べることとします。

2 マイナンバー制度の概要

マイナンバーは、社会保障・税・災害対策の3分野で利用するために導入されます（法改正により、金融機関での利用も可能になります）。公共機関が、機関間で正確な情報を連携して活用し、これらの分野の業務を効果的に行うためには、国民を一意に識別することができる識別子が必要です（例えば、3で述べるワンストップサービスの実現に必要です）。このような識別子がなければ、いわゆる「消えた年金」が生じたように、国民一人ひとりについて、必要な情報を集めることができなくなり、公的サービスの提供の障害となることも考えられます。

こうした目的のもと、マイナンバー制度は、以下の仕組みを備えるものとなりました。

1 マイナンバーの指定

マイナンバーは、国民に一つずつ割り当てられます。マイナンバーは、唯一無二のものであり、原則として変更されませんので、いわば国民と一対一に対応するものとなります。

ただし、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場合には、市区町村長がマイナンバーを変更することも可能です（番号法7条2項）。

2 利用範囲の限定

マイナンバーの利用範囲は、前述のとおり、社会保障・税・災害対策に限定されますが、より具体的に、マイナンバーを扱うことのできる事務が明記されています（番号法9条、番号法別表第1）。また、地方自治体においては、条例に定めることにより、上記の目的の範囲でマイナンバーを取り扱うことが可能となります（番号法9条2項）。

3 管理された情報提供

行政手続においては、複数の行政機関等に保有されている情報が必要になることがあります。従来は、国民の側で、各行政機関から書面を取得し、必要書類をそろえて申請する方法がとられてきました。これに対して、いわゆるワンストップサービスにおいては、国民は単一の機関に申請し、行政機関の側で必要な情報を他の機関から取得して処理することになります。このようなワンストップサービスの実現や、行政機関側で給付や免除などのサービスを受けられる者を見つけて本人に通知する、いわゆるプッシュ型サービスの実現にあたって、マイナンバーは大きな効果をもたらします。

しかし、行政機関相互であっても、無制限な情報提供はプライバシーの侵害につながりかねませんから、情報提供は、必要最小限の範囲に限定されています（番号法19条）。この制限については、後述します。

4 本人確認

マイナンバー制度では、通知カードと個人番号カードの2種類のカードが発行されます。まず、平成27年10月から、通知カードが国民全員に交付され、これに基づいて、希望者には個人番号カードが発行されます。通知カードは、マイナンバーの通知だけのものである一方、個人番号カードは顔写真とICチップを備えます。個人番号カードは、それだけで一般的な本人確認の資料となります。これに対して、通知カードだけでは本人確認はできず、写真付きの公的証明書（例えば、運転免許証）などを併用する必要があります。

なお、個人番号カードに搭載されるICチップには、公開鍵暗号技術による認証機能があります。これにより、インターネット等を通じた安全な認証が可能になります。

5 自己情報の入手

国民は、マイナポータルを利用することにより、自己情報の入手が可能となります。例えば、マイナンバーの付いた自己の情報を、どの行政機関がどこに提供したかを確認できます。また、行政機関が保有する自分に関する情報や行政機関から自分に対しての必要なお知らせ情報等を自宅のパソコン等から確認できるようになる予定です。その一環として、各種社会保険料の支払金額や確定申告等を行う際に参考となる情報が入手可能になる運びです。マイナポータルにログインするためには、個人番号カード搭載のICチップによる認証が必要なため、高いセキュリティが確保されます。

マイナポータルは、平成29年1月よりサービスが開始される予定となっています。

6 特定個人情報保護委員会による監視

マイナンバーの適正な取扱いを確保するための組織として、特定個人情報保護委員会が、いわゆる3条委員会として設置されました（番号法36条以下）。同委員会は、マイナンバーを扱う実施者に対して指導・助言、勧告・命令、報告の要求・立入検査を行うことができます（番号法50条～52条）。ただし、同委員会は、各議院による調査、裁判手続、犯罪捜査

等（番号法19条12号参照）への提供およびこれらが取得した特定個人情報については、上記の指導等の適用除外となっています（番号法53条）。

3 マイナンバー制度のリスク

1 概要

マイナンバー制度では、大きく分けると、故意または過失による特定個人情報の不正利用、漏えいおよび不正な統合（データベースの統合、名寄せ、個人情報の一元管理など）のリスクがあります。また、特定個人情報の消去や改ざんというリスクもありますが、これらは、不正利用に含めて検討することとします。

図表1は特定個人情報の提供および保有の概要を示す図です。行政機関および民間企業等が特定個人情報を保有し、これが、他の行政機関に提供される仕組みです。行政機関の間での情報の連携は、情報提供ネットワークシステムを介して行われます。ただし、情報提供ネットワークシステムと行政機関の間の通信では、マイナンバーそのものではなく、当該行政機関と情報提供ネットワークシステムだけが知っている符号（マイナンバーと一対一に対応）を用います。

図表2は、特定個人情報の利用におけるリスクを示すものです。リスクは、不正利用、漏えい、不正な名寄せおよび統合が考えられます。特定個人情報の不正利用および漏えいのリスクは、行政機関、民間企業等および情報提供ネットワークシステムのそれぞれに存在します。また、不正な名寄せおよび統合については、行政機関の間での不正な名寄せおよび統合が考えられるほか、複数の経路から漏えいした情報の統合があり得ます。

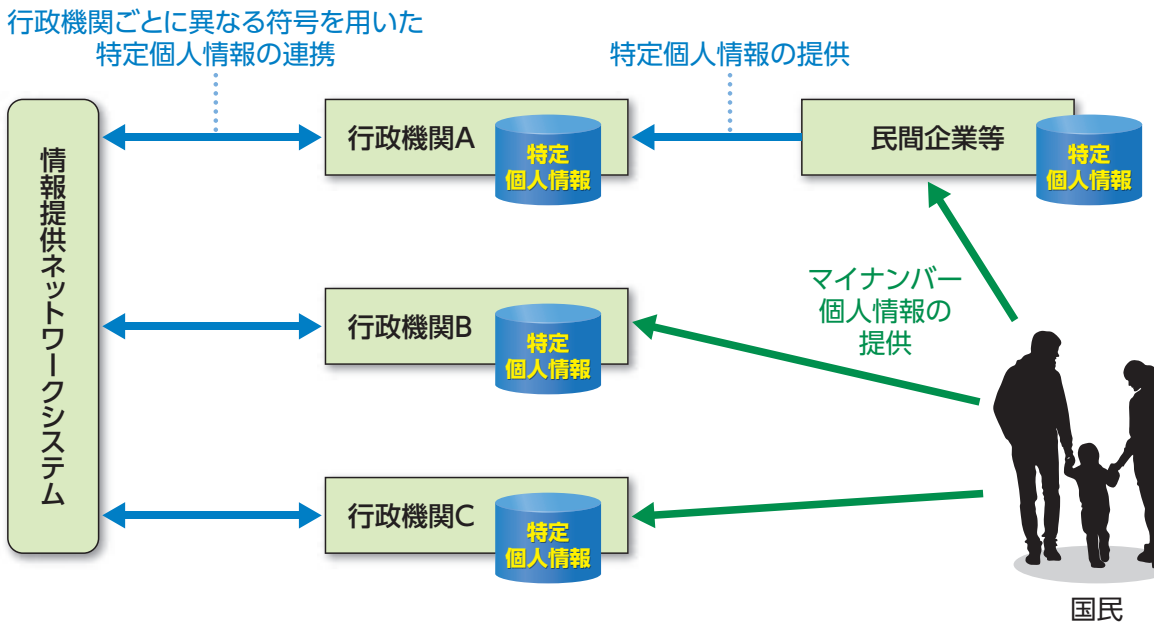
以下では、これらのリスクについて、述べます。

2 不正利用

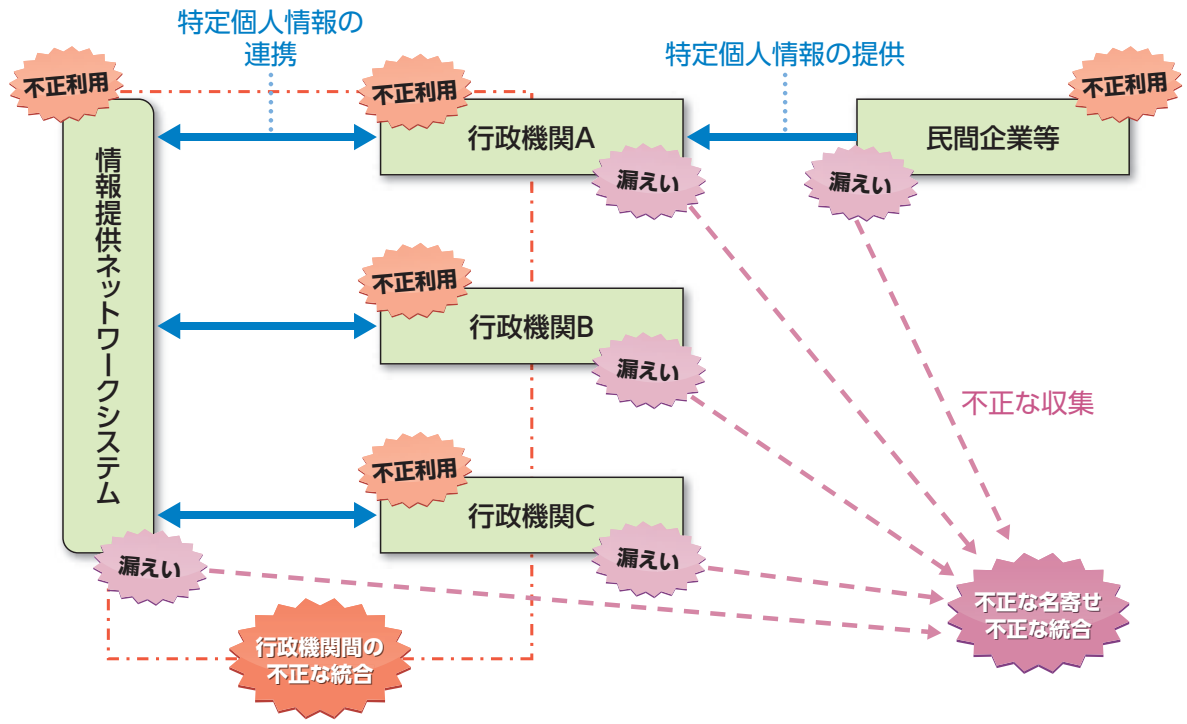
まず、不正利用のリスクについて述べます。これは、特定個人情報を扱う担当者の故意による目的外利用および不正な提供を意味しますが、対策については、消去や改ざんなども同様に考えることができます。

特定個人情報の不正利用は、罰則をもって

図表1 特定個人情報の提供と保有



図表2 特定個人情報の利用におけるリスク



禁止されています（番号法67条以下）。また、行政機関および情報提供ネットワークシステムにおいては、システム的にも、担当者以外の者を限定（アクセス制御）するとともに、アクセスログの取得により、不正利用が検出できるようにしています。このような仕組みを構築することが、情報保護評価により確保されています（番号法27条）。行政機関においても民間企業等においても、十分な安全対策が必要とされています（番号法12条）ので、アクセス制御、アクセスログの取得は必須です。この点は、情報提供ネットワークシステムについても同じです。なお、情報提供ネットワークシステムにおいては、情報機関から適法に行われた照会のみを扱う仕組みとなっているため、情報提供ネットワークシステムの担当者等が不正に情報を取得し利用することは困難です。

このように、不正利用については、制度的およびシステム的な対策が行われるものとされていますが、人間が関係する以上、実際には、小規模な不正利用を完全に防ぐことは不可能だと思われます。不正利用を防止することが重要なのはいうまでもありませんが、それと並んで重要なのは、万が一の不正利用が生じても、それを検出し、不正利用を最小限にとどめることです。被害の極小化については、後述します。

3 漏えい

（1）漏えいの防止

システムの欠陥や、担当者のミスなどからの、情報漏えいは跡を絶ちません。これとあいまって、外部からのコンピュータシステムへの侵入や、コンピュータウイルスなどの不正プログラムによる情報の窃取も多くなっています。

平成27年5月には、年金番号を含む少なくとも120万人分の情報が漏えいする事件がありました。この事件は、標的型攻撃といわれる外部からの攻撃によるものです。典型的な標的型攻撃は、担当者に同僚や関係者を装った電子メールを送付し、担当者に添付ファイルを開かせることにより、コンピュータウイルス等を担当者のPCに感染させるものです。

以前は、メール本文の日本語が不自然であるなど、比較的、看破しやすい特徴がありました。しかし、最近の標的型攻撃のメールは、巧妙化が進んでおり、簡単に見破ることはできません。電子メールの発信元および送達経路を綿密に調べれば、送信者を偽装した不正なメールであると判定できる可能性はあります。しかし、技術的には、発信元などのヘッダー情報（メールの先頭に置かれた情報で、発信元サーバ、経由したサーバなどの情報を持ちます。通常の設定では、ユーザにはヘッダーの一部しか見えません）をも偽装可能ですので、これも完全な対策ではありませんし、緊急を要する旨を装うメールであれば、綿密な確認が行われない可能性も高いと言えます。

結局、標的型攻撃に対する完全な防衛方法はありません。特に、個々の担当者の注意によって完全に防ぐことは、全く期待できません。

この点で、発信者を確実に示して、偽装を防止する方法としてS/MIMEなどのセキュアメールがあります。セキュアメールを用いている者からのメールについては、発信元を偽装することは極めて困難になります。しかし、全ての利用者がセキュアメールを利用しない限り、セキュアメールでない通常のメールも読まざるを得ませんので、当面は、現実的な対策にはなりそうにありません（攻撃者は、セキュアメールを用いていない利用者を装うことが考えられるからです）。

このように、漏えいを完全に防ぐことはできませんので、不正利用と同様に、被害を極小化することが重要であると言えます。

(2) 漏えいの影響

次に、特定個人情報の漏えいが生じた場合には、具体的にどのような被害が生じるのかを検討します。

ここで重要なのは、マイナンバー自体の漏えいと個人に関する情報の漏えいとは違うということです。個人に関する情報（例えば、氏名・住所・電話番号）があれば、情報取得者は、これらの情報を直ちに利用できます。しかし、マイナンバーだけでは、特に利用する方法はありません。例えば、本人確認は番号だけでは行いませんので、マイナンバーそれ自体が漏えいしても、そのマイナンバーの持ち主になりすますことはできないのです（番号法16条および同施行規則12条参照）。マイナポータルにも、マイナンバーだけではアクセスできず、個人番号カードが必要です。

それでは個人情報が漏えいした場合に、それがマイナンバーを含んでいても影響がないかというと、そうではありません。複数の情報漏えい事件が発生した場合に、それらに含まれる個人を紐付け（名寄せ）するためにマイナンバーが利用されることが考えられます。また、漏えいした情報に関するデータベースを、マイナンバーをキーとして統合することも考えられます。このような統合、名寄せのリスクについては後述します。

4 行政機関による名寄せ･統合

従来より、国民の情報の統一番号による管理は、国民総背番号制として批判されてきました。これは、行政機関等が国民に関する情報を一元管理し、一人ひとりの国民の情報を集約することによるプライバシー侵害を問題とするものです。

ここでは、公的機関における名寄せ・統合の技術的可能性を検討します。

確かに、マイナンバーによる管理が進めば、名寄せ・統合を徹底することが可能になります。特に、コンピュータを用いずに、紙で個人情報を管理する場合には、統一番号の有無により、名寄せ・統合の難易度は大きく違います。

しかし、今日では、ほとんどの情報はデータベースによりコンピュータ管理されています。行政機関においては、原則として、住民基本台帳ネットワークに登載されている4情報（住所、氏名、生年月日、性別）がそのまま記載されます。4情報が正確に記載されているデータベース間の名寄せや統合は、データベースの機能を使えば簡単にできますから、マイナンバーの有無による違いは非常に小さいと

言えます。

ただし、情報の更新時期が違うことにより住所または氏名にズレが生じている場合や、外字（「渡邊」の「邊」の多様な文字のように、住基統一文字に含まれない文字は、システムごとに別の管理をしている可能性があります）を利用している場合には、4情報だけでは同一人かどうか簡単に判定できないこともあり得ます。このような事情のある国民の人数についての統計はありませんが、数パーセント以下であると思われます。逆にいいますと、90％以上の国民については、マイナンバーの有無にかかわらず、技術的には、容易に名寄せ・統合が可能だと言えます。

なんらかの事情により、名寄せができなければ、公的サービスの提供に支障が生じるおそれがあります。マイナンバーの利用により、こうした国民について、確実な名寄せを行えるようになります。つまり、マイナンバーがなくても、90％以上の国民の情報は、名寄せ・統合は技術的には可能であり、マイナンバーの導入により、残り数パーセントの国民についても名寄せが可能になります。つまり、マイナンバーの導入により、この数パーセントの国民まで、公的サービスを提供できるようになる一方で、これらの国民についても行政機関等による名寄せや統合が可能になるわけです。このように、マイナンバー導入には、メリットとデメリットがあり、そのいずれをとるべきかには、議論があるところです。最終的には、立法を通じた国民による決定に委ねられるものと思います。

行政機関における特定個人情報の取扱いは、特定個人情報保護委員会の監視等に服しています（番号法50条～52条）。現在の縦割りの行政組織の下で、不正なデータベース統合が行われることは考えにくいですし、特定個人情報保護委員会の監視があることを知りながら、不正利用する危険は小さいと考えられます。

ただし、ここには2つの懸念があります。1つは、特定個人情報保護委員会の人的リソースの制限のために、十分な監視ができないおそれがあることです。特定個人情報保護委員会への人的リソースの配分は、国民のプライバシーを守るために重要なものですので、十分な配分を行うべきです。

もう1つの懸念は、特定個人情報保護委員会の監視等の適用除外があることです。衆議院・参議院による調査や、裁判手続、刑事事件の捜査、租税における犯則事件の調査などのために行政機関から特定個人情報を提供することが定められています（番号法19条12号）。このような場合には、特定個人情報の提供についても、提供先における取扱いについても、特定個人情報保護委員会の監視等の対象外になります（番号法53条）。三権分立による制限により立法・司法における取扱いを監視することは難しいと言えますし、捜査における取扱いも、監視の対象とすることには困難があることには一定の理解が可能です。しかし、行政機関による提供の可否については、特定個人情報保護委員会の監視に服するべきです。捜査等に関する特定個人情報提供の事実をその情報の本人に知らせることはできませんが、特定個人情報保護委員会が、行政機関による提供の実態を把握することは可能ですし、適切な監視をして不当な情報提供を防止すべきです。現行法では、このような権限は特定個人情報保護委員会に与えられていませんので、立法的に解決すべき問題だと思います。

5 民間における統合

情報は、一旦漏えいしてしまえば、ひそかに流通し、多くの人の手に渡るおそれが大きいものです。このような漏えいが何回か起こった場合、すなわち、一人の個人の情報が複数の機関から漏えいした場合に、これらの名寄せが行われて、その個人についての情報が蓄積されていくことが考えられます。また、複数の機関から大量の情報が漏えいした場合には、そのような情報を統合したデータベースの構築も考えられます。

米国においては、多くの情報に社会保障番号（Social Security Number）が使われているため、情報の統合が進んでおり、民間の巨

大な個人情報データベースが構築されるにいたっています（例えば、Equifax）。日本国内の企業については、帝国データバンクなどのデータベースが存在し、有償で情報を取得できますが、米国では同様な情報取得が個人についても可能になっているのです。

このような個人情報の巨大なデータベースの構築こそが、プライバシーに対する最大の脅威であると考えられます。

6 被害の極小化

国民のプライバシーを保護するためには、特定個人情報の不正提供や漏えいを防ぐことが最重要です。コンピュータを使って情報を管理すると、セキュリティ上の欠陥などからの情報漏えいを完全になくすことはできません。しかし、現代社会において、コンピュータを用いた処理の放棄は現実的ではありませんし、人的要因もありますので、完全な防衛は不可能です。そこで、仮に、情報が漏えいしても被害を極小化するための方策が重要です。

極小化の方策は、大別して、漏えい件数の極小化と、名寄せ・統合範囲の極小化が考えられます。

（1）漏えい件数の極小化

漏えい件数の極小化は、万が一、ウイルス等の不正プログラムに感染した場合の迅速な事後処理と、不正プログラムがアクセスできる件数の制限が考えられます。前者については、危機管理体制の構築を確実に行い、その実施を徹底することが重要です。後者については、システム的な対策も可能だと思われます。例えば、セキュリティが高いシステム（基幹システム等）から、個々のPC等にダウンロードする業務の場合、その業務に必要な数のデータを超えてダウンロードできないようにすること、または、一定の個数を超えたときに警告するなどの方法が考えられます。このためには、業務分析を綿密に行って、各業務および各端末で利用する特定個人情報の個数および頻度を把握し、これに基づいて管理を行う必要があります。

（2）名寄せ・統合範囲の極小化

米国の社会保障番号のように、あらゆる情報に単一の番号が使われていると、漏えいした情報の名寄せ・統合が無制限に広がってしまいます。

その対策として知られているのが「セクトラル方式」です。これは、オーストリアなどでとられている方式で、分野ごとに異なる番号を利用するものです。

今後、マイナンバーの利用領域が拡大される方向にあります（番号法附則6条1項）。しかし、マイナンバーの利用範囲を無制限に広げれば、名寄せ・統合の危険はそれだけ増大します。

例えば、医療情報に用いる番号ついては、マイナンバーとは別系統の番号とするべく検討されています。このような番号とマイナンバーとの関連づけを、きわめて限定された場面でのみ行うようにすることにより、利便性を向上しつつ、危険性を抑制することが可能になります。

4 弁護士の安全管理措置

弁護士法人はもちろん、個人事業主たる弁護士も、職員等のマイナンバーを扱うことになります。マイナンバーを扱う場合には、安全狩措置が必要となりますので、その要点を述べておきます。なお、安全管理措置については、特定個人情報保護委員会の「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」（以下「ガイドライン」といいます）に詳細な解説がありますので、詳しくはガイドラインをご覧ください。なお、ガイドラインでは、中小規模事業者（従業員100人以下の事業者であって、金融分野等の事業者以外の者）における対応方法が明記されていますので、この部分が特に参考になると思われます。以下では、中小規模事業者における対応方法を中心に説明していきます。

1 リスク分析について

一般に、安全性の確保のために最初に行う活動はリスク分析です。これは、具体的なリスク（例えば、携帯端末の置忘れによる情報漏えい）ごとに、そのリスクが現実化する可能性の大きさと、リスクが現実化した場合の影響の大きさを推定し、そのリスクへの対策を検討します。例えば、経済的損失に対しては保険に加入する（リスクの移転）方法が考えられます。可能性・影響ともに小さいものであれば、そのリスクを甘受することもあり得ます（リスクの受容）。また、リスクが大きい場合には、そのようなリスクを負う業務を避けること（リスクの回避）を考慮すべきケースもあります。多くのリスクについては、セキュリティ対策などを行ってリスクの軽減を図りますが、それでも残るリスクについては移転や受容を行うことになります。

マイナンバーを含む特定個人情報については、その漏えいによる評判の低下は大きな影響があります。しかしながら、マイナンバーを扱わないという選択肢（リスクの回避）はとれませんので、漏えいの可能性を少しでも減らしていく必要があります。

以下では、マイナンバーを用いる業務を示して、そこで必要な対策について述べます。

2 マイナンバーを扱う業務

まず、マイナンバー関係の業務分析を行います。マイナンバーの利用分野は、社会保障・税・災害対策ですが、個人事業主を含む事業者がマイナンバーを扱うのは、通常、以下の業務となります。

・税務（従業員への源泉徴収票、個人たる取引先への支払調書の発行・提出）
・社会保険（従業員の健康保険、雇用保険、年金等の処理）

また、これらに付随して以下の処理が必要となります。

・従業員・取引先からのマイナンバーの取得（本人確認を行った上での取得）
・退職等の特定個人情報の消去（不要となった情報は削除）

このように、実際には、弁護士等がマイナンバーを扱う機会は非常に限定されているのが分かると思います。以下では、これらの業務でマイナンバーを扱う場合の要点を述べていきます。なお、弁護士は特定個人情報を記載した証拠を扱うこともありますので、これにも注意が必要です。

3 事業者が行うべき安全管理措置

マイナンバーを扱うにあたっては、安全管理措置をとる必要があります。安全管理措置の検討は、以下の順序で行うことが効果的です（ガイドライン別添資料参照）。

①マイナンバーを扱う事務の範囲の明確化

税務・社会保障のために実施する事務を明確化します。

②特定個人情報等の範囲の明確化

マイナンバーと関連付けて保存される個人情報（氏名、生年月日等）を明確にして、事業者が扱う特定個人情報の範囲を明らかにします。

③事務取扱担当者の明確化

①で明確化された事務において特定個人情報を取り扱う担当者を明確にします。

④基本方針の策定

特定個人情報の適正な取扱いを確保するための基本方針を策定します。具体的には、事業者の名称、関係法令・ガイドラインの遵守、安全管理措置に関する事項、質問・苦情処理窓口などの記載が考えられます。

⑤取扱規定等の策定

①～③で明確化した事務において特定個人情報を適正に取り扱うための内規等を策定します。

⑥安全管理措置の実施

組織的安全管理措置、人的安全管理措置、物理的安全管理措置、技術的安全管理措置を行います。

これらのうち①～④は、どんなに小規模な事業者であっても必須です。しかし、⑤⑥に

ついて厳密に行うことは、小規模の事業者にはそぐわない点もあります。そこで、ガイドラインでは、中小規模事業者における簡易的な対応方法を示しています。これを中心にして、⑤⑥について、述べていきます。

4 取扱規定等の策定

取扱規定等は、特定個人情報の取得段階、利用段階、保存段階、提供段階、削除・廃棄段階のそれぞれについて、取扱方法、責任者・事務取扱担当者およびその任務について定めます。

中小規模事業者においては、特定個人情報等の取扱いを明確化しておき、担当者の変更にあたって確実な引継ぎを行うこと、引継ぎを責任ある立場の者が確認することが必要です。

5 安全管理措置

特定個人情報を漏えいや不正利用から守るための安全管理措置としては、組織的安全管理措置、人的安全管理措置、物理的安全管理措置、技術的安全管理措置が必要です。これらについて説明します。

(1) 組織的安全管理措置

組織として特定個人情報を安全に管理するための措置としては、組織体制の整備、取扱規程等に基づく運用、取扱状況を確認する手段の整備が必要です。

中小規模事業者においては、以下の措置をとることになります。

・事務取扱担当者が複数いる場合には、責任者と事務取扱担当者を区分し、それぞれの役割や担当範囲を明確にします。
・特定個人情報等の取扱状況（取得、利用、廃棄など）が分かる記録を保存します。

(2) 人的安全管理措置

事務取扱担当者に対する必要かつ適切な監督を行います。例えば、個人事業主たる弁護士が自ら事務員を監督することがこれにあたります。また、事務取扱担当者については、必要な教育を実施します。

(3) 物理的安全管理措置

特定個人情報が格納されている装置や電子媒体を、事務取扱担当者以外の者が触れることがないように管理する必要があります。

このために、装置や電子媒体を扱う場所への入退場を制限する方法や、その場所への電子機器の持込みの制限が行われます。また、装置や媒体を施錠されたキャビネット等に保管することや、特定個人情報を扱う装置をセキュリティワイヤー等で固定して、盗難を防止する方法もあります。

小規模な事業者の場合には、例えば特定個人情報の処理を特定のノートPCに限定し、このPCを物理的に管理する方法が考えられます。また、USBチップなどの可搬媒体に特定個人情報を格納し、利用するとき以外は金庫に保管する方法も考えられます。

特定個人情報等が記録された装置や媒体、書類を持ち出すことは望ましくありませんが、やむを得ず持ち出す場合には、パスワードを設定して容易なアクセスを防止するなどの処理をとる必要があります。

なお、職員の退職などにより、当該職員のマイナンバーを扱う必要がなくなり、法令等の定めによる保存期間を経過した場合には、できるだけ速やかに削除または廃棄します。この場合には、責任ある立場の者が削除・廃棄の実施を確認しなければなりません。

(4) 技術的安全管理措置

コンピュータ内の、特定個人情報を含むファイルへのアクセスを、事務取扱担当者に限定し、他の者のアクセスを防止するための管理措置です。統合文書システムなどでは、ユーザごとにアクセス可能な範囲を設定する機能がありますので、このような機能を用いてアクセス制御を行います。アクセスにあたっては、利用者の認証を、ユーザIDとパスワード、磁気カード、ICカードなどで行います。

中小規模事業者においては、特定個人情報を取り扱う機器を特定し、その機器を取り扱える事務取扱担当者を具体的に限定することが望まれます。また、機器に標準装備されて

いるユーザ制御機能（Windowsのユーザアカウント管理機能など）により、業務上必要な者だけが取り扱えるように制限することが望まれています。

外部からの不正アクセスの防止のため、インターネットとの接続にはファイアウォールを設置します。また、コンピュータウイルス等の不正プログラムを防止するため、セキュリティ対策ソフトウエアを利用します。

特定個人情報をインターネット等で送信することは、望ましくありません。しかし、やむを得ない事情により、外部に送信する場合には、VPNによる通信路の暗号化や、データファイルそのものの暗号化を行う必要があります。

なお、電子メールで暗号化ファイルを送信する場合に、そのファイルを復号するための鍵（パスワード）を電子メールで送るべきではありません。そのような方法をとると、第一に、通信路の盗聴に対しては無力です（盗聴者は、暗号ファイルだけでなく、鍵も盗聴することが考えられます）。

第二に、電子メールによる情報漏えいのうちでもっとも頻度が高いのは、誤ったアドレスへの送信です。ファイルを送るときにアドレスに誤りがあれば、鍵の送信にも同じ誤りが生じることが多いでしょうから、結局、同じ人に暗号ファイルと鍵が送られる可能性が高いのです。したがって、電子メールでの鍵の送信は避けるべきです。鍵の伝達は、電話やFAXなど、別の通信手段で行うべきです。

（5）証拠等に記載のマイナンバー

従業員や取引先のマイナンバーのほかに、訴訟等における証拠にマイナンバーが記載されていることがあります。このような証拠も特定個人情報として厳重に管理しなければなりません。また、マイナンバーの記載が立証に不要であれば、証拠として提出する際に墨塗りする等の措置が必要です。

5 おわりに

以上、マイナンバー制度の概要と、そのリスク、取扱いの要点を述べました。マイナンバーの導入は、全ての国民に行政サービスを提供するために効果的ですが、その反面、複数の経路から情報が漏えいした場合の名寄せ・統合などのリスクもあります。特に、民間で個人に関する巨大なデータベースが構築されれば、プライバシーに対する重大な侵害になりますので、情報漏えいについては十分な対策をとるとともに、万が一の漏えいにあたって被害を極小化していくことが極めて重要です。弁護士等の中小規模事業者においても、マイナンバーを扱っていく必要がありますが、大規模事業者と同様の対策をとることは困難です。したがって、規模に相応の対策を選択していくことが不必要な費用や労力を避けるだけでなく、必要な措置に集中することが可能になりますので、かえって安全な管理の実現につながります。弁護士の下からマイナンバーが漏えいするようなことになれば、法曹に対する信頼の失墜につながりますから、一人ひとりが自覚を持って管理していくことが、重要だと言えます。

平成27年9月9日に、個人情報保護法および番号法の改正法が成立しました。番号法に関して最も大きな変更は、特定個人情報保護委員会が、個人情報全般を対象とする個人情報保護委員会に改組されることです。これに伴い、番号法に含まれていた特定個人情報保護委員会に関する条文の多くが個人情報保護法に移ります。また、金融機関での個人番号の利用が一部可能となります。なお、現行法では、5,000件以下の個人情報のみを保有している場合には個人情報取扱事業者としての義務を負いませんでしたが、個人情報保護法の改正により、このような事業者も義務を負うようになります。これらに伴って、番号法の条文番号は大きく変わりますので、条文を参照する際にはご注意ください。