マイナンバーで何が変わるか※

井　上　禎　男※※

第１回
「私」の番号は、どこで、何に使われるのか（2015. 09. 03公表）
第２回
管理する側（組織）とされる側（「私」「本人」「個人」）との関係（2015. 09. 11公表）
■　管理する側が意識すべきこととは
■　「ベネッセ事件」が提起したこと――“パートナー”の選択と信頼
第３回
行政の効率化と行政サービスの利便性向上
［上］（2015. 09. 20公表）
■　官・行政／民・企業――双方での対応と「効率化」
［中］（2015. 09. 21公表）
■　「私」「本人」「個人」にとっての“メリット”は？
［下］（2015. 09. 22公表）
■　「私」の情報は、「私」にしか守れない
■　「私以外」の情報を「私以外」の誰かに渡す場合には、「本人」の同意を得ることが原則
第４回
事業者がなすべきこと①（管理体制の構築、取得・利用・提供および保管・廃棄の留意点）
［上］（2015. 09. 28公表）
■　個人情報と特定個人情報での対応の違い
■　組織的安全管理措置
［中］（2015. 09. 28公表）
■　物理的安全管理措置・技術的安全管理措置・人的安全管理措置
［下］（2015. 09. 28公表）
■　取得・利用・提供、保管・廃棄の運用
最終回
事業者がなすべきこと②（委託等の物理的安全管理措置を中心に）
［上］（2015. 10. 13公表）
■　委託、委託先による再委託、再委託先からの再再委託
■　“パートナー”とは一心同体
［下］（2015. 10. 13公表）
■　“パートナー”の選択に際して

※　本稿は、2015年９月から10月にかけて全５回にわたって福岡大学ウエブサイト（HP）［2015年10月時点でのURLは、http://www.fukuoka-u.ac.jp/］上に掲載・公表された［研究者コラム］「マイナンバーで何が変わるか」を転載したものである。

※※　福岡大学法学部准教授

第１回　「私」の番号は、どこで、何に使われるのか（2015. 09. 03公表）※

今回から全５回シリーズで「マイナンバーで何が変わるか」と題したコラムをお届けします。コラムを担当するのは、井上禎男准教授（法学部）です。

井上准教授は、法学部で行政法、情報法を担当しています。行政法の中でも、特に情報法・情報政策が専門分野です。社会的には、経済産業省（原子力関係）や福岡市などの情報公開・情報保全に関する委員、佐賀県や福岡県内の各自治体での個人情報保護に関する委員、プライバシーマークの審査委員等を歴任しています。また、個人情報保護に関する審議会・審査会委員の立場から、複数の自治体でマイナンバー、特定個人情報保護に関する評価やその支援業務に携わっています。

今年（2015年）の10月から、住民票を有する国民一人一人に12桁の番号である「マイナンバー」（以降は「個人番号」とも呼びます）の通知が開始されます。来年（2016年）１月からは、①社会保障（年金・雇用保険・医療保険・福祉分野の給付・生活保護などに記載）、②税（申告・届出などに記載）、③災害対策（被災者台帳作成事務などに利用）の各分野の行政手続で、個人番号が必要になります。

もっとも、税や社会保険の手続を行うのは個人だけではありません。そのため①や②の分野では、行政のみならず民間事業者での取り扱いも生じます。つまり、「私」が給与や報酬を受け取る立場にある場合、これを支払う側である会社やバイト先などでも、「私」や「私」の扶養家族の個人番号を源泉徴収票や支払調書に記載しなければならなくなります。健康保険・厚生年金・雇用保険の被保険者資格取得届についても同様です。そうすると、税務署や年金事務所に対する行政手続上の関係で、民間事業者も「私」の番号や一定の「私」に関する情報を取り扱うことになるわけです。

次回以降全５回にわたって、「私」の番号である個人番号を付すことによって管理・流通される個人情報（これを「特定個人情報」と呼びます）を取り扱う

※ 福岡大学ウエブサイト（HP）http://www.fukuoka-u.ac.jp/research/column/15/09/03094444.html（2015年９月時点での URL）

行政、民間事業者に求められること、また「私」の番号や「私」の情報に「私」がどのように向き合っていくべきかについて、考えてみることにします。

【追記】

本コラム掲載後の9月4日に、個人番号（マイナンバー）法の改正法が衆議院本会議で可決成立しました。主な内容は、本人の同意を条件として、2018（平成30）年以降に口座預金情報を個人番号と結びつけること（税務署による税務調査での残高情報の収集等）を可能にするというものです。

また今回の改正で、「メタボ検診」の記録についても2016（平成28）年から、予防接種の記録についても2017（平成29）年から個人番号と結びつけることが可能になりました。まずは、とりわけ公平な課税の徹底等を念頭に置くものと言えますが、今後も個人番号の利活用が広がりをみせることは必至でしょう。

また、必然的にわれわれの日常生活にも大きくかかわってきます。この点については、行政の効率化と行政サービスの利便性向上という観点から、第3回のコラムでふれることにします。

第2回　管理する側（組織）とされる側（「私」「本人」「個人」）との関係（2015. 09. 11公表）※

■　管理する側が意識すべきこととは

端的には、管理される側（「私」「本人」「個人」）の立場に立ったルールの策定と運用、特にその内容の一端となる安全管理措置（セキュリティのみならず、

※ 福岡大学ウエブサイト（HP）http://www.fukuoka-u.ac.jp/research/column/15/09/11090001.html（2015年9月時点でのURL）

委託先や従業員の監督・教育をも含む）の徹底に尽きます。このことは「特定個人情報」に限らず、「個人情報」（個人情報保護法上では、第２条１項で、“生存する個人に関する情報であって、その情報に含まれる氏名、生年月日その他の記述等により、特定の個人を識別することができるもの”を指します。さらに“その情報自体によって特定の個人を識別できるもの”のほか、“他の情報と容易に照合することができ、それによって特定の個人が識別できるもの”も含みます）一般にも当てはまります。

個人情報については、国や自治体の場合には「法律」（「行政機関個人情報保護法」など）や「個人情報保護条例」が“ルール”になりますが、民間事業者にとっての“ルール”は、まず法律（「個人情報保護法」）であり、さらに独自に定めた「規程」や「規則」の類になります。ここでは“プライバシーポリシー”（個人情報保護［取扱］指針）や“セキュリティーポリシー”（情報セキュリティ指針）をウエブサイトなどで公表しておくことも大切です。

行政の場合には法律や条例に従った、さらには個人情報保護審査会のような第三者機関による不服申立てへの対応が図られます。しかし民間事業者の場合には、個人情報保護法第４章で課せられる義務を果たす必要とは別に、問題が生じた場合の内部的な救済体制の構築や規範化をも含めた実際の“ルール”の策定・運用には、事業者ごとの温度差や意識の希薄さが認められます。

今回の特定個人情報については個人番号（マイナンバー）法が根拠法となりますが、事業者としての対策については個人情報の場合同様に、残念ながら、行政に比べて現時点での対応の遅れが顕著です。

■ 「ベネッセ事件」が提起したこと ――“パートナー”の選択と信頼

しかしここでさらに考えるべきは、個人情報の漏洩等が事業者にとっての経済的な損失やイメージダウンを招くといった観点に終始しないことでしょう。実際にインターネットのような媒体での漏洩や流出が生じた場合には、

（二次的・三次的あるいは潜在的なものも含めて）情報の拡散は防ぎようがありません。（特定）個人情報の主体（被害者）の実質的な救済を図ることはおそらく困難でしょう。そして、事業者自らでは対応が難しいので何かしらの“プロ”に対応を委ねる、契約に基づいた特定の業務委託を行うことも一般によく行われていますが、そのことだけで安心してしまうことも非常に危険です。

昨年（2014年）７月に発覚した「ベネッセ事件」でも明らかになりましたが、そうしたパートナー・委託先の慎重な選択、継続的な監督の徹底が求められることも、本来は自らが取得・保有・管理すべき個人情報を外に投げる・預ける（委託する）以上は、当然のことといえます。

時や人が変わっても組織が存続する限りは、あくまで「私」「本人」「個人」の立場に立った“ルール”の策定や運用の徹底を、その都度、事業者自らが自覚的に継続しなければなりません。その責務は極めて重たいものです。

特に個人番号・特定個人情報についての事業者の対応問題については、第４回と第５回のコラムでふれることにします。その前に、次回第３回では、行政の効率化と行政サービスの利便性向上という観点から、個人番号（マイナンバー）制度を眺めてみることにします。

第３回　行政の効率化と行政サービスの利便性向上

［上］（2015. 09. 20公表）※

■　官・行政／民・企業――双方での対応と「効率化」

第１回で個人番号（マイナンバー）制度の目的にふれました。特に社会保障と税の両分野では、これから個人番号“自体”が不可欠になります。行政に

※ 福岡大学ウエブサイト（HP）http://www.fukuoka-u.ac.jp/research/column/15/09/20090001.html（2015年９月時点での URL）

とってみると、この分野の事務処理の効率化を図ることができ、この分野での正確な本人確認と状況把握が可能になれば、一定の公平性を担保できるわけです。

しかし個人番号制度は、既存の住基ネット※1のように、官・行政のみで完結するシステムではありません。そのため、民・企業にとってみれば、自発的・直接的にこの分野での事務処理の効率化を目指すものでもありません。そうすると、第２回で概観したような個人番号に関する新たな規範の制定や既存の個人情報等に関するルールとの整合性を図るための再考、また従業員教育や研修等の徹底のみならずハード・インフラ面でも、個人番号に対応する新たなシステムの導入や既存のシステムの変更・統合にかかるコストの負担が（も）新たに生じることになります。既存の情報管理を継続・徹底することに加えて、個人番号にかかる負担とさらなる情報漏洩のリスクを抱えることは、民間事業者にとって非常に酷なことなのかもしれません。しかしそれでも、制度設計上はNOとは言えないわけです。

個人番号制度で問題となる「私」「本人」「個人」の情報は、官（行政）でも民（民間事業者・企業）でもやり取りの対象になります。双方で求められる対応については、新たに設置された国の第三者機関である「特定個人情報保護委員会」が、各部門での「ガイドライン」を公表しています※2。民間事業者・企業等も、まずは「ガイドライン（事業者編）」の周知徹底・精査から始めるべきでしょう。

※1　住民基本台帳ネットワークシステム
1999（平成11）年の住民基本台帳法改正に基づき、「居住関係を公証する住民基本台帳［氏名、生年月日、性別、住所などが記載された住民票を編成したもの］をネットワーク化し、全国共通の本人確認ができるシステムとして構築するもの」。第一次稼動は2002（平成14）年８月、第二次稼動は2003（平成15）年８月。詳しくは、総務省の「住基ネット」ウエブサイト　http://www.soumu.go.jp/main_sosiki/jichi_gyousei/c-gyousei/daityo/index.html を参照（2015年９月時点でアクセス可能）

※2　特定個人情報保護委員会ウエブサイト（http://www.ppc.go.jp/legal/policy/）に掲載（2015年９月時点でアクセス可能）

［中］（2015. 09. 21公表）※

■　「私」「本人」「個人」にとっての“メリット”は？

「私」の番号“自体”が行政や会社での種々の届出や申告などの手続で必要になるとしても（手続は多少スムーズになるでしょうが）、そうした場面が必ずしも日常的ではないとすれば、“便利さ”や“メリット”を実感することはないでしょう。むしろ行政手続に限ってみると、住基カード※1の二の舞にならないとも限りません。

今回の個人番号（マイナンバー）制度では、2016（平成28）年１月以降、「個人番号カード」（次頁の様式参照）の交付を受けることができます。発行申請に際しては、来月（2015［平成27］年10月）以降、市区町村から住民票登録住所宛てに個人番号が記載された「通知カード」（次頁の様式参照）が送付されてきます。この通知カードと同封されている交付申請書を提出することによって、個人番号カードの交付が受けられます。

※1　住民基本台帳法による「住民基本台帳カード」（なお、住基ネットについては前掲参照）。発行率は５％程度とされる。住基カードの有効期限内は使用可能であるが、個人番号（マイナンバー）制度の開始にともない、今年［2015（平成27）年］12月で新規発行は停止される。

通知カードは、個人番号カードの交付時に回収されます（なお、個人カードの発行は義務ではありません）。個人番号カードは、本人確認のための身分証明書、カード搭載ICによる電子証明書を用いたe-Tax（国税電子申告・納税シス

＊　福岡大学ウエブサイト（HP）http://www.fukuoka-u.ac.jp/research/column/15/09/21000001.html（2015年９月時点でのURL）

通知カードの様式について

【おもて面】

【うら面】

個人番号カードの様式について

【おもて面】

【うら面】

【出典】 総務省ウエブサイト http://www.soumu.go.jp/kojinbango_card/index.html
（2015年９月時点でアクセス可能）

テム）等の各種電子申請、自治体が条例で定めるサービス（図書館利用証、印鑑登録証など）にも使用できます。

また、現在（2015［平成27］年９月時点で）はまだ議論の段階にありますが、2017（平成29）年４月から消費税が10％へと増税されることにともなう「還付」に、個人番号カードを用いることが検討されています。さらに今後は、戸籍や証券分野での個人番号制度・個人番号カードの利用範囲の拡大も検討されています。今後の対象分野や利用範囲の拡大が進んでくると、「私」「本人」「個人」のレベルで目に見える“メリット”を実感できるようになるのかもしれません。

［下］（2015. 09. 22公表）※

■ 「私」の情報は、「私」にしか守れない

■ 「私以外」の情報を「私以外」の誰かに渡す場合には、「本人」の同意を得ることが原則

住民票登録をしている住所に住んでいれば、私たちは少なくとも、通知カードを手にすることになります。通知カードは紙製で、氏名、住所、生年月日、性別（これらを「基本４情報」と呼びます）に加えて、個人番号（マイナンバー）が記載されています。すでに個人番号制度をかたった個人情報の不正取得を試みる案件も生じているようですが、ここでは「私」の情報が、あくまで「私」自身にしか守れないことを銘じておくべきでしょう。通知カードを紛失したり、安易に他人に渡すことによって「私」の情報が流出した結果、“なりすまし”等による悪用・被害が発生する可能性もあります。

なお、民間事業者等で個人番号を取り扱う者のみならず、たとえ個人であっても、個人番号に関する法定の違反行為を行った場合には罰則が科せられます[※1]。しかし、罰則があるからきちんと対処すればよい、というものでもないはずです。故意の場合は当然ですが、仮に不注意や軽い気持であったとしても、いったん漏えいが起こってしまえば、決して「本人」は救われません。

最近はSNS上での勝手な“タグ付け”や実名を挙げての批判・誹謗・中傷などの行為が日常化しています。もしそうした行為によって「本人」に損害が生じた場合、そうした行為を行った者は、当然に法的な責任（本人に対する民事上の責任のみならず、場合によっては名誉棄損等の刑事責任）を負います。ネットやSNSが「匿名」の世界だと勘違いしている人も多いですが、行為者を特定することは、技術的にさほど難しいことではありません。しかし、行為者（加害者）が何らかの法的な責任を負ったところで、（特定）個人情報

※ 福岡大学ウエブサイト（HP）http://www.fukuoka-u.ac.jp/research/column/15/09/22000002.html（2015年９月時点でのURL）

の場合には、本人（被害者・対象者）の潜在的な被害・損害の可能性はなくならないわけです（この点は、第2回でもふれました）。

「私以外」の情報を「私以外」の誰かに渡す・知らせる、SNSやネット上に公開する場合には、「本人」の“同意”を得ることが原則です。たとえ家族の「通知カード」であったとしても、カードに記載されている情報は「私以外」の情報であって、「私」の情報ではありません。不注意や軽い気持ちで行ったことが他人、場合によっては自分の家族や友人や大切な人を傷つけ、時に取り返しのつかない被害や損害をもたらす可能性があることも、しっかりと自覚しておくべきでしょう。

※1　内閣官房「社会保障・税番号制度」ウエブサイト　http://www.cas.go.jp/jp/seisaku/bangoseido/faq/faq5.html（2015年9月時点でアクセス可能）

第4回　事業者がなすべきこと①（管理体制の構築、取得・利用・提供および保管・廃棄の留意点）

［上］（2015. 09. 28公表）※

前回までの内容を踏まえて、第4回（今回）と第5回（次回・最終回）では、特定個人情報の取り扱いのプロセスに応じた対応・措置※1について、私自身が自治体で学んできた経験も加味しながら（なお、民間事業者・企業はもちろんのこと、特定個人情報の場合には自治体等も従業員等を有するすべての事業者に該当するため、「ガイドライン（事業者編）」（第3回［上］を参照）に則した対応が求められることになります）、適宜、確認してみることにします。

※　福岡大学ウエブサイト（HP）http://www.fukuoka-u.ac.jp/research/column/15/09/28162525.html（2015年9月時点でのURL）

※1　詳しくは、特定個人情報保護委員会ウエブサイト http://www.ppc.go.jp/legal/policy/document/を参照（2015年９月時点でアクセス可能）

■　個人情報と特定個人情報での対応の違い

個人情報であれ特定個人情報であれ、管理する側となる民間事業者・企業が携わる際にとどめおくべき姿勢・意識については、第２回でふれたとおりです。

しかし、特定個人情報の場合には、個人番号（マイナンバー）法によって事業者が個人番号を利用できる事務が限られています。主に社会保障および税に関して行政機関や保険組合等に手続書類を提出する際に、あくまで目的の限りで従業員に個人番号の提供を求めてこれを収集し、その上で利用・保管等を行うことになります。ここでは必要な期間を超えて保管をすることもできません。

そのため、従来から民間事業者・企業に存在する個人情報、すなわち営業の目的・用途等から収集・利用・管理している顧客情報や、特定個人情報とは別途の従業員等の個人情報とは扱いを異にすることになります。そうすると、従来からの個人情報に関する組織内での“ルール”をそのまま用いることはできず、新たに番号法やガイドラインの趣旨にそった“特定個人情報のルール”が必要になるわけです（第３回［上］を参照）。

■　組織的安全管理措置

規程等の見直し作業は、情報漏洩等の事案に対応する体制の整備（さらに救済に関する組織的な対応については第２回でふれています）等と並んで、組織的安全管理措置の一端となります。

しかし、新たに特定個人情報に関する“ルール”を策定すればおしまい、そうした“ルール”ができたことで安心・満足してしまうことが、実は最も

危ないことと言えます。肝心なのは、こうした“ルール”を継続的に運用するための組織的な体制と意識の持ち方、動機づけです。

［中］（2015. 09. 28公表）※

■　物理的安全管理措置・技術的安全管理措置・人的安全管理措置

第２回でふれたように、あくまで「管理される側」（「私」「本人」「個人」）の側に立った対応を図るのならば、漏洩等の不測の事態への対処も念頭に置いて、組織的な所管と系統、責任の所在を明確にしておくことが「利用」の前提となります。

ここではまず、組織の中で個人番号・特定個人情報を取り扱う部署が具体的にどこになるのか、その区域を明確にして管理を行う必要が生じます（物理的安全管理措置）。さらには、担当者（従業員）レベルでも、個人番号・特定個人情報ファイルへのアクセス権を誰が持つのか（アクセス権者の識別と認証については別途、技術的安全管理措置の問題になります）、さらには、事務担当者と責任者とを分離しておくことなど、組織的な所管と系統、責任の所在を明確にしておくことが第一歩です。また、ここで組織内での人事異動の可能性を考えれば、日常的な監督に加えて、当該担当者のみならず組織全体での従業員教育・研修等（人的安全管理措置）も不可欠になります。

さらにセキュリティのような技術的安全措置についても、従前以上の組織的対応が求められることになります。ウイルス対策やソフトウエア等の更新・最新化は当然ですが、新たに個人番号・特定個人情報にかかる段階ごとのアクセス制限措置を講ずるにしても、そもそも組織内での各端末においてすでにインストール済みであるソフトに関する検疫および定期的な検知徹底によるリスク回避なども考慮しなければならなくなるでしょう。

※ 福岡大学ウエブサイト（HP）http://www.fukuoka-u.ac.jp/research/column/15/09/28162727.html（2015年９月時点での URL）

実際の「管理」に際しては、前記した種々のアクセスに関する制限措置のような技術的安全管理措置に加えて、個人番号・特定個人情報に関するアクセス記録を管理しておくことも必要です。さらに管理ツール上での匿名化の工夫（例えば適切なマスキング措置を講ずること）や実際の担当者の行動レベルでの措置・対応の徹底（一時的な離席時の適切な対応等）も不可欠となります。

［下］（2015. 09. 28公表）※

■　取得・利用・提供、保管・廃棄の運用

こうした種々の「管理」体制の構築のもとに、個人番号・特定個人情報を本人から「取得」する際には、法令上での前記事務以外での「取得」「提供」ができないことを徹底するためにも、利用目的を特定した本人通知・公表が必要になります。

ここで確実に本人に伝えるためには、個別かつ直接に特定の連絡手段によって本人に連絡を取ることが原則です。その他の方法として、組織内でのイントラネットへの公表等もあり得ます。その場合には、ここでも（義務ではないですが、事業者自らが）進んで、個人番号・特定個人情報に固有の“プライバシーポリシー”さらには“セキュリティーポリシー”を明確に規定しておくこと（第２回を参照）も一案です。

そして何よりも、初手の段階での本人確認が重要になるので、既存の従業員の個人情報と「通知カード」もしくは「個人番号カード」（第３回［中］を参照）上に記載される情報とを、可能ならば本人対面のもとで照合確認すること、その際のチェックも複数人で組織的に対応することが望ましいでしょう。

「保管」「廃棄」については、社会保障および税に関しての手続書類の作成

※ 福岡大学ウエブサイト（HP）http://www.fukuoka-u.ac.jp/research/column/15/09/28163030.html（2015年９月時点での URL）

事務の処理の必要がなくなった場合で、法令上の保存期間を経過した場合に、事業者に速やかな廃棄・削除が求められます（例えば、扶養控除等申告書は7年間の保存となっており、当該期間を経過した場合には申告書記載の個人番号を保管しておく必要はなく、原則として速やかに廃棄しなければなりません）。

この点、「ガイドライン（事業者編）」では、実際に廃棄が必要となってから廃棄作業を行うまでの期間を期限の到来即日に廃棄とせずに、特定個人情報等の保有の安全性と事務の効率性等を勘案して事業者が判断すればよいとしています。いずれにせよ、個人番号・特定個人情報ファイルの削除、電子媒体等の廃棄の場合の記録の保存は必要ですから、廃棄・削除を前提とした保管体制の構築が求められることになります。

最終回　事業者がなすべきこと②（委託等の物理的安全管理措置を中心に）

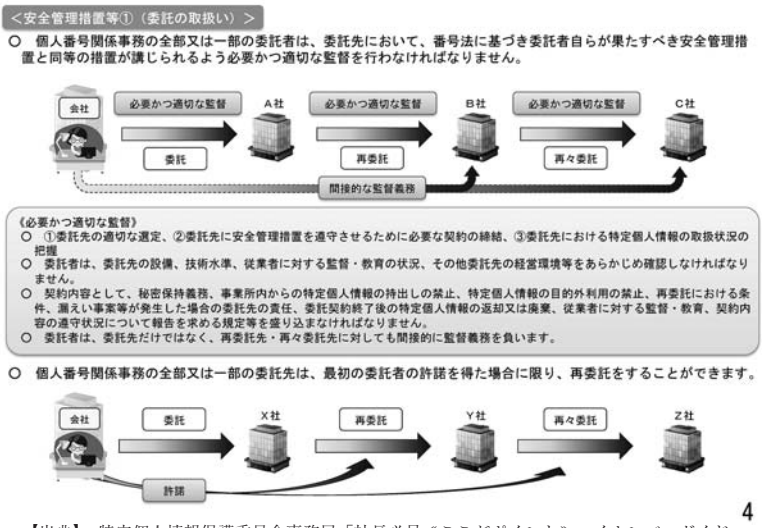
［上］（2015. 10. 13公表）※

■　委託、委託先による再委託、再委託先からの再再委託

個人・本人あるいは「私」「私以外」の立場で気をつけるべきこと（第3回［下］を参照）とは別に、事業者が組織として安全管理措置を講ずる場合に特に考えておかなければならないのは、事業者が日常的に行っている業務の委託、さらには委託先による再委託、再委託先からの再再委託等の際の対応と責任です。

この点について特定個人情報保護委員会事務局は、次のように説いています。委託等の際の関係性も明確に示されていてわかりやすいので、そのまま図表・ポイントを引かせてもらいます。

※ 福岡大学ウエブサイト（HP）http://www.fukuoka-u.ac.jp/research/column/15/10/13154546.html（2015年10月時点での URL）



【出典】 特定個人情報保護委員会事務局「社長必見≪ここがポイント≫マイナンバーガイドライン（事業者編）（平成27年２月版）」４頁　http://www.ppc.go.jp/files/pdf/270213shacho.pdf から参照・引用（2015年10月時点でアクセス可能）

■ “パートナー”とは一心同体

第２回で取り上げた、個人情報の場合の「“パートナー”の選択と信頼」に関する視点は、特定個人情報の場合にもそのまま当てはまるはずです。ただし、特定個人情報の場合には扱う情報が一般の個人情報よりも限定的ですので（第４回［上］を参照）、単純に数の上だけでみると、個人情報よりも特定個人情報の方が対象としては少なくなるでしょう。しかし、ここで数の多寡を問題にすべきではありません。顧客情報であろうが従業員情報であろうが、あくまで管理される側（「私」「本人」「個人」）の立場に立ったルールの策定と運用が不可欠であり、事業者が組織的に継続して徹底する姿勢が求められる点に、変わりはありません（第２回を参照）。

個人番号・特定個人情報の場合に求められる物理的・技術的・人的安全管理措置（第４回［中］［下］で概観しました）の根底には、組織的安全管理措置が

あります（第４回［上］を参照）。そして、新たな特定個人情報の“ルール”が「絵に描いた餅」にならないための組織自らの意識は、実は「“パートナー”の選択と信頼」にこそ、端的に現れます。

事業者が個人番号・特定個人情報への自主的な対応が難しいと判断した場合、コンサルティング会社やアドバイザー等の“専門家”に組織的な対応を相談することもあるでしょう。また、現に日常的な種々の業務委託の場面で行われている“パートナー”選びは、個人番号・特定個人情報の場合にも妥当するでしょう。しかしここで考えるべきは、“安上がり”であるといった経済性、あるいは“わかりやすい”といった単純さに惑わされることなく、あくまで自己の情報を他者に委ねることの意味を、事業者として本質的に理解しておくことです。

［下］（2015. 10. 13公表）※

■ “パートナー”の選択に際して

“専門家”ないしは“パートナー”によってなされる提案が具体的かつ十分であるか、有効かつ有益なものであるか、スケジュールや作業項目が適切に示されているか等々を精査・吟味することは、事業者として当然でしょう。

しかし、果たして“専門家”や“パートナー”としての“実”を備えている相手かどうかを見極めることは、容易ではないのかもしれません。

それでも、「ガイドライン（事業者編）」（第３回［上］を参照）にも明示されている――前掲の特定個人情報保護委員会事務局の解説頁の引用中でも明記される――「必要かつ適切な措置」に基づく監督義務は、あくまで事業者自身にあります。漏洩等の場合の責任も、第一次的には事業者自らが負います。また何よりも、第３回［下］でふれましたが、故意の場合は無論、仮に不注

※ 福岡大学ウエブサイト（HP）http://www.fukuoka-u.ac.jp/research/column/15/10/13155656.html（2015年10月時点での URL）

意でもいったん漏洩が起これば（潜在的な可能性をも含めて）決して「本人」は救われません。このことは漏洩の主体が個人であろうが、事業者であろうが、委託先・再委託先・再再委託先であろうが同じことです。

そうすると、事業者自らの「必要かつ適切な措置」を担保できる種々の項目およびその具体的な内容を、“専門家”“パートナー”との契約において明記しておくことが不可欠になります。

しかしながら、日常的な監督義務の実践は、あくまで“アクション”であるはずです。事業者自らが継続的にこれを行うためには、何よりも“ルールづくりで満足しない”、そして“専門家”や“パートナー”への“お任せで、自らが対応した気にならない”ことが肝要です。文書（組織内での“ルール”や契約書など）も確かに大切なのですが、何よりも自らの継続的な実践こそが、リスクを回避する最大の防御になるはずです。

一心同体たり得る“専門家”“パートナー”選びのひとつの目安としては、個人情報の場合にも同じことが言えますが、プライバシーマーク※1 およびISMS 認証※2 の取得を当初からの選考要件としておくことが一案です。もっとも、これらを取得さえしていれば安心・安全な“専門家”“パートナー”であるとも言えませんから、あくまでもひとつの目安として、です。と同時に、事業者自らもまた、これらの取得に積極的に臨むことが望ましいでしょう。

※1　2006年に改定された日本工業規格 JIS Q15001「個人情報保護マネジメントシステム—要求事項」に適合する個人情報への適切な保護措置を講ずる体制を整備する事業者等に対して認定・付与されるもの。一般財団法人日本情報経済社会推進協会（旧財団法人日本情報処理開発協会）（JIPDEC）ならびに JIPDEC が認定した指定機関が認定・付与の業務を担う。なお、Pマークの付与認定を受けた事業者は、2014年7月現在で13000超。申請を経て認定を受けた事業者等は、その事業活動に関し、プライバシーマーク（Pマーク）を使用することができるようになる。事業者等にとってみると、自らが個人情報の適正な利用ないし安全な取扱いを行っていることを社会にアピール

できることになるし、他方、消費者等にとってみれば、事業者等が個人情報に対する意識をどの程度有しているか、信頼をはかるためのひとつの目安となる点で利点を有する。詳しくは JIPDEC のプライバシーマーク（Pマーク）のウエブサイト（http://privacymark.jp/）を参照（2015年10月にアクセス可能）。

※2 ISMS（Information Security Management System）は「情報セキュリティマネジメントシステム」「情報セキュリティ管理システム」すなわち、国際標準規格である ISO/IEC27001およびその国内規格としての日本工業規格である JIS Q27001を指す。ISMS認証は組織内での自己診断を第一段階とするが、さらに外部・第三者機関からの認証を受けなければならない。ここで ISMS 適合性評価制度とは、「組織が構築した ISMS が JIS Q27001（ISO/IEC27001）に適合しているか審査し登録する『認証機関』、審査員の資格を付与する『要員認証機関』、及びこれら各機関がその業務を行う能力を備えているかをみる『認定機関』からなる総合的な仕組みである」（引用および認証機関一覧も含め、詳しくは、JIPDEC の ISMS 適合性評価制度のウエブサイト（http://www.isms.jipdec.or.jp/isms.html）を参照（2015年10月にアクセス可能）。

【 付 記 】

本稿は、科学研究費助成事業（学術研究助成基金助成金）（平成27年度交付分）、挑戦的萌芽研究（社会科学・法学・公法学）、井上禎男「善き監守者のためのアポステリオリ」の成果の一部である。