JIPDEC IT-Report 2014 Winter

特集

社会保障・税番号制度（マイナンバー制度）と個人情報保護評価

JIPDEC
一般財団法人日本情報経済社会推進協会

今年度第2号となる「JIPDEC IT-Report 2014 Winter」では、「社会保障・税番号制度（マイナンバー制度）と個人情報保護評価」について特集を組みました。

2013年5月公布の「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（番号法）」により、2015年10月から個人番号（マイナンバー）が付番・通知され、2016年1月1日以降、個人番号が利用されるようになります。このため、地方自治体では、業務の見直し・システム改修に加え、「特定個人情報保護評価（番号法PIA）」への対応が義務付けられていますが、民間企業においても、すべての企業で社員、その家族等の個人番号の収集、管理が必須となるため、保有する個人番号の取扱いに細心の注意が必要となります。

個人番号を取り扱う事業者が特定個人情報を適正に取り扱うための具体的な指針を示すため、本年12月公表の「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）」について、特定個人情報保護委員会委員長である堀部政男氏に概要の解説をお願いしました。

また、個人番号の付番、住民への通知、システム改修、個人情報保護対策、セキュリティ対策等の整備、番号法PIAへの対応が急がれる中、特定個人情報保護に対する意識が高く、すでに番号法PIAに取り組まれている地方自治体に実施体制、取組み上の問題点、課題等について、事例をご紹介いただいています。

さらに、昨今、ソーシャルメディアの普及に伴い、位置情報や購買履歴情報を集約してビッグデータビジネスに活用するなど、民間企業において大量の個人情報を取り扱う機会が増えてきています。個人情報を処理するシステムの企画・開発の段階で、潜在する可能性のあるリスクの早期発見、低減、回避、解決を図るためには、「プライバシー・バイ・デザイン」の考えを取り入れたリスク評価手法「プライバシー影響評価（PIA）」の実施が推奨されますが、このPIAの効果、必要性について、有識者の方に解説していただきました。

本誌をこれから番号法PIAに着手される地方自治体はもとより、番号制度、PIAに関わる企業の皆様の参考としていただければ幸いです。

2014年12月

一般財団法人日本情報経済社会推進協会

JIPDEC IT-Report 2014 Winter

目　　次

【特集】社会保障・税番号制度（マイナンバー制度）と個人情報保護評価

1 特定個人情報保護委員会「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）」の概要と重要性

特定個人情報保護委員会委員長（一橋大学名誉教授）　堀部　政男

1.はじめに

2015年10月1日以降に各人に「個人番号」が通知され、翌2016年1月1日以降、その個人番号が使われるようになる「番号時代」の到来が目前に迫ってきている。その根拠法は、2013年5月31日公布の「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」（平成25年法律第27号）（以下、「番号法」という。）である。番号法は、個人情報保護関係法の特別法（一般法よりも限られた範囲のものに適用される法）であって、その理解のためには一般法（特別法よりも広い範囲のものに適用される法）である個人情報保護関係法が前提となる。法の世界では特別法と一般法の関係については、「特別法は一般法に優先する」という原則がある。一般には馴染みのない言葉であるが、重要な意味を持っている。

一般法である個人情報保護関係法といっても、次のような法律がある。

・個人情報の保護に関する法律（平成15年法律第57号）（以下、「個人情報保護法」という。）
・行政機関の保有する個人情報の保護に関する法律（平成15年法律第58号）
・独立行政法人等の保有する個人情報の保護に関する法律（平成15年法律第59号）

これらに精通することは至難の技である。とはいえ、個人番号を使わなければならなくなる。そして、使い方を誤ると、罰則を科されることにもなる。

個人番号を含む個人情報である「特定個人情報」を適正に取り扱うためには、個人情報保護法のもとで策定された各種ガイドラインと同様な番号法関係ガイドラインが必要不可欠である。そのガイドラインのうち、民間事業者にとって重要なガイドラインの案が、「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）（案）」として2014年10月10日（金）から11月9日（日）までパブリックコメントに付された（締切は11月9日（日））。この意見募集に対して68の個人または団体から延べ276件の意見が寄せられた。この種の意見募集としてはその数が多く、ガイドラインに対する関心の高さが窺える。特定個人情報保護委員会は、その結果をも踏まえて、12月2日に、「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、「本ガイドライン」という。）を決定した。また、それまでの検討過程で表明された質問、意見等を参考に、「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）」および「（別冊）金融業務における特定個人情報の適正な取扱いに関するガイドライン」に関するQ&Aを作成した。そのQ&Aは、合計89に及んでいる。これらは、官報掲載日に特定個人情報保護委員会のホームページで公表されるので、併せて参照されたい。

本稿では、本ガイドラインの文章そのものを引用する場合には原則として「　　」の引用符を用いることにするが、必ずしもそのものでない場合には引用符を用いていないことをお断りしておきたい。

2.本ガイドラインの構成

本ガイドラインは、次のような構成になっている。ここでは本ガイドラインの目次そのものを掲げて、全体の構成を明らかにすることにしたい。

第1　はじめに
第2　用語の定義等
第3　総論
　第3-1　目的
　第3-2　本ガイドラインの適用対象等
　第3-3　本ガイドラインの位置付け等
　第3-4　番号法の特定個人情報に関する保護措置

3.本ガイドラインの適用対象

本ガイドラインの適用対象について見るならば、番号法は、行政機関等(行政機関、地方公共団体、独立行政法人等または地方独立行政法人をいう。以下同じ。)または事業者の別を問わず、個人番号を取り扱うすべての者に適用される。また、個人情報保護法が適用の対象を一定の範囲の者となっている個人情報取扱事業者(民間事業者で、個人情報データベース等を構成する個人情報によって識別される特定の個人の数(個人情報保護法施行令で定める者を除く。)の合計が過去6か月以内のいずれの日においても5,000を超えない者以外の者)に限定しているのに対し、番号法はすべての事業者を適用の対象としていることに留意しなければならない。本ガイドラインは、番号法の適用を受ける者のうち「事業者」を対象としている。

番号法では「事業者」について、「事業者の努力」という条文見出しで「個人番号及び法人番号を利用する事業者は、基本理念にのっとり、国及び地方公共団体が個人番号及び法人番号の利用に関し実施する施策に協力するよう努めるものとする」(第6条)と規定されているが、「事業者」そのものについては定義されていない。「国の責務」(第4条)および「地方公共団体の責務」(第5条)の次に「事業者の努力」(第6条)ということで位置付けられているので、「国」および「地方公共団体」以外の民間事業者であると理解するとわかりやすいであろう。

その「事業者」には、大企業および中小企業があり、「中小企業白書」(2014年版、701頁)の「企業ベース」によると、非一次産業計が中小企業3,852,934、大企業10,596という数字が出ている。合計すると、3,863,530となる。日本には約380万の事業者がいるといわれるのはこの数字である。また、中小企業3,852,934のうち、小規模企業は3,342,814で、全企業数に占める割合は86.5%である。

個人情報保護法でいう「個人情報取扱事業者」は、前述のように、「個人情報データベース等を構成する個人情報によって識別される特定の個人の数(個人情報保護法施行令で定める者を除く。)の合計が過去6か月以内のいずれの日においても5,000を超えない者以外の者」である。言い換えれば、5,000超であれば、「個人情報取扱事業者」に当たり、個人情報保護法の義務

規定等が適用される。個人情報取扱事業者であれば、個人情報保護法に基づいて個人情報保護のあり方について経験しているが、それに当たらない事業者（非個人情報取扱事業者）は、そのような経験をしていない。非個人情報取扱事業者数については統計がない（数字を出すのは困難である）ので、数は不明であるが、「中小企業白書」でいう「常用雇用者20人以下（卸売業、小売業、飲食店、サービス業（宿泊業、娯楽業を除く）は5人以下の企業）」である小規模企業は、非個人情報取扱事業者であることが多いのではないかと推測する。

番号法は、事業者の規模を問わず、個人情報保護法について未経験の事業者に対しても適用されるので、非個人情報取扱事業者も、改めて個人情報保護の考え方を理解し、番号法の施行に備える必要がある。ということは、本ガイドラインを検討し、番号法違反にならないようにすることが求められるということである。

なお、事業者のうち規模が比較的大きい金融機関が行う金融業務に関しては、「第4　各論」に相当する部分について、「（別冊）金融業務における特定個人情報の適正な取扱いに関するガイドライン」を適用するものとしている。

4.事業者が番号法の適用を受ける場面

それでは、どのような場面ですべての事業者が番号法の適用を受けるのであろうか。それについて本ガイドラインは、次のように具体例を示している。

「全ての事業者は、個人番号の提供の求めの制限（番号法第15条）並びに特定個人情報保護の提供の制限（同法第19条）及び収集等の制限（同法第20条）の規定の適用を受ける。また、事業者が番号法の規定の適用を受ける主な事務は、次のとおりである。

- 事業者が従業員等から個人番号の提供を受けて、これを給与所得の源泉徴収票、給与支払報告書、健康保険・厚生年金保険被保険者資格取得届等の必要な書類に記載して、税務署長、市区町村長、日本年金機構等に提出する事務（同法第9条第3項）
- 金融機関が顧客から個人番号の提供を受けて、これを配当等の支払調書に記載して税務署長に提出する事務（同法第9条第3項）
- 健康保険組合、全国健康保険協会等（以下「健康保険組合等」という。）が個人番号を利用して個人情報を検索、管理する事務（同法第9条第1項）
- 激甚災害が発生したとき等において、金融機関が個人番号を利用して金銭を支払う事務（同法第9条第4項）

さらに、事業者が、行政機関等又は他の事業者から個人番号を取り扱う事務の委託を受けた場合も、番号法の適用を受ける。」

5.番号法と個人情報保護法との関係

「1.はじめに」で「特別法」および「一般法」という言葉を使ったが、法の世界ではよく用いられるので、理解する必要がある。前述のように、特別法と一般法の関係は、「特別法は一般法に優先する」ことになっている。したがって、まずは特別法がどのようなものであるかを知り、それに規定されていないことが一般法でどのようになっているかを確認する必要がある。

すべての事業者は、特別法である番号法が特定個人情報について規定している部分の適用を受ける。

個人情報取扱事業者は、番号法第29条により適用除外となる部分を除き、特定個人情報について、一般法である個人情報保護法の規定の適用も受けることに注意しなければならない。

また、番号法においては、個人情報取扱事業者でない個人番号取扱事業者に対しても、特定個人情報に関しては、一般法である個人情報保護法に規定されている重要な保護措置に相当する規定を設けていることに留意する必要がある。

番号法では、「個人番号取扱事業者」という概念も用いられている。その「個人番号取扱事業者」は、番号法第31条では、「特定個人情報ファイルを事業の用に供している個人番号利用事務等実施者であって、国の機関、地方公共団体の機関、独立行政法人等及び地方独立行政法人以外のものをいう」となっているので、個人情報保護法第2条第3項に規定する「個人情報取扱事業者」も含まれている。ところが、番号法第32条では、「個人情報保護法第2条第3項に規定する個人情報取扱事業者を除く」となっている。これが「個人情報取扱事業者でない個人番号取扱事業者」である。本稿では前に「非個人情報取扱事業者」と記したが、この概念は番号法にはない、本稿のみの表現であり、これは「個人情報取扱事業者でない個人番号取扱事業者」である。本ガイドラインは、具体例を次のように挙げている。

「具体的には、特定個人情報の目的外利用の制限（同法第32条）、安全管理措置（同法第33条）及び特定個人情報を取り扱

う従業者に対する監督義務(同法第34条)である。ただし、これらの規定は、番号法第35条各号に掲げる者については、その特定個人情報を取り扱う目的の全部又は一部が当該各号に定める特定の目的であるときには、適用されない。」

この最後の第35条は、個人情報保護法第50条(適用除外)の規定に相当する。

6.本ガイドラインの位置付け

本ガイドラインは、特定個人情報の適正な取扱いについての具体的な指針を定めるもので、特定個人情報に関し、番号法に特段の規定がなく個人情報保護法が適用される部分については、個人情報保護法上の主務大臣が定めるガイドライン・指針等を遵守することを前提としている。

2014年3月31日現在、事業等を所管する各府省により、27 分野について40のガイドラインが策定されている(消費者庁「平成25年度個人情報の保護に関する法律施行状況の概要」(2014年10月))。

7.番号法の特定個人情報に関する保護措置

(1)保護措置の概要

番号法の特定個人情報に関する保護措置の概要は、次のとおりである。

「個人番号は、社会保障、税及び災害対策の分野において、個人情報を複数の機関の間で紐付けるものであり、住民票を有する全ての者に、一人一番号で重複のないように、住民票コードを変換して得られる番号である。したがって、個人番号が悪用され、又は漏えいした場合、個人情報の不正な追跡・突合が行われ、個人の権利利益の侵害を招きかねない。

そこで、番号法においては、特定個人情報について、個人情報保護法よりも厳格な各種の保護措置を設けている。この保護措置は、「特定個人情報の利用制限」、「特定個人情報の安全管理措置等」及び「特定個人情報の提供制限等」の三つに大別される。」

ア　特定個人情報の利用制限

個人情報保護法では、利用目的を特定し、その利用目的の範囲内に限り利用することができるにすぎないことは知られているが、番号法では、それと対比して見ると、特定個人情報の利用制限は、次のとおり限定的である。

「個人情報保護法は、個人情報の利用目的についてできる限り特定(個人情報保護法第15条)した上で、原則として当該利用目的の範囲内でのみ利用することができるとしている(同法第16条)が、個人情報を利用することができる事務の範囲については特段制限していない。

これに対し、番号法においては、個人番号を利用することができる範囲について、社会保障、税及び災害対策に関する特定の事務に限定している(番号法第9条)。また、本来の利用目的を超えて例外的に特定個人情報を利用することができる範囲について、個人情報保護法における個人情報の利用の場合よりも限定的に定めている(番号法第29条第3項、第32条)。さらに、必要な範囲を超えた特定個人情報ファイルの作成を禁止している(同法第28条)。」

イ　特定個人情報の安全管理措置等

特定個人情報の安全管理措置等は、次のようになっている。

「個人情報保護法は、個人情報取扱事業者に対して、個人データに関する安全管理措置を講ずることとし(個人情報保護法第20条)、従業者の監督義務及び委託先の監督義務を課している(同法第21条、第22条)。

番号法においては、これらに加え、全ての事業者に対して、個人番号(生存する個人のものだけでなく死者のものも含む。)について安全管理措置を講ずることとされている(番号法第12条)。

また、個人番号関係事務又は個人番号利用事務を再委託する場合には委託者による再委託の許諾を要件とする(同法第10条)とともに、委託者の委託先に対する監督義務を課している(同法第11条)。」

ウ　特定個人情報の提供制限等

番号法における特定個人情報の提供制限等は、次のように限定的である。

「個人情報保護法は、個人情報取扱事業者に対し、個人データについて、法令の規定に基づく場合等を除くほか、本人の同意を得ないで、第三者に提供することを認めていない（個人情報保護法第23条）。

番号法においては、特定個人情報の提供について、個人番号の利用制限と同様に、個人情報保護法における個人情報の提供の場合よりも限定的に定めている（番号法第19条）。また、何人も、特定個人情報の提供を受けることが認められている場合を除き、他人（自己と同一の世帯に属する者以外の者をいう。同法第20条において同じ。）に対し、個人番号の提供を求めてはならない（同法第15条）。

さらに、特定個人情報の収集又は保管についても同様の制限を定めている（同法第20条）。

なお、本人から個人番号の提供を受ける場合には、本人確認を義務付けている（同法第16条）。」

（2）委員会による監視・監督

委員会による監視・監督は、多岐にわたる。それらは、次のようになっている。

「委員会は、特定個人情報の取扱いに関する監視・監督を行うため、次に掲げる権限を有している。

・個人番号関係事務実施者又は個人番号利用事務実施者に対し、特定個人情報の取扱いに関し、必要な指導及び助言をすることができる。この場合において、特定個人情報の適正な取扱いを確保するために必要があると認めるときは、当該特定個人情報と共に管理されている特定個人情報以外の個人情報の取扱いに関し、併せて指導及び助言をすることができる（番号法第50条）。
・特定個人情報の取扱いに関して法令違反行為が行われた場合において、その適正な取扱いの確保のために必要があると認めるときには、当該違反行為をした者に対し、期限を定めて、当該違反行為の中止その他違反を是正するために必要な措置をとるべき旨を勧告することができる（同法第51条第1項）。
・勧告を受けた者が正当な理由なく勧告に係る措置をとらなかったときには、その者に対し、期限を定めて、勧告に係る措置をとるべきことを命ずることができる（同条第2項）。
・さらに、特定個人情報の取扱いに関して法令違反行為が行われた場合において、個人の重大な権利利益を害する事実があるため緊急に措置をとる必要があると認めるときは、当該違反行為をした者に対し、期限を定めて、当該違反行為の中止その他違反を是正するために必要な措置をとるべき旨を命ずることができる（同条第3項）。
・特定個人情報を取り扱う者その他の関係者に対し、特定個人情報の取扱いに関し、必要な報告若しくは資料の提出を求めること又は立入検査を行うことができる（同法第52条）。」

（3）罰則の強化

番号法では罰則が強化されたことが大きな特色になっている。これについて本ガイドラインは、次のように説明している。

「個人情報保護法における個人情報取扱事業者に対する罰則の適用は、主務大臣からの是正命令に違反した場合、虚偽報告を行った場合等に限られている。一方、番号法においては、類似の刑の上限が引き上げられているほか、正当な理由なく特定個人情報ファイルを提供したとき、不正な利益を図る目的で個人番号を提供、盗用したとき、人を欺く等して個人番号を取得したときの罰則を新設する等罰則が強化されている（番号法第67条から第75条まで）。」

ここでは別表は割愛するが、本ガイドラインは、別表について次のように解説している。

「なお、次表①から⑥までは、日本国外においてこれらの罪を犯した者にも適用される（同法第76条）。また、法人（法人でない団体で代表者又は管理人の定めのあるものを含む。以下この項目において同じ。）の代表者若しくは管理人又は法人若しくは人の代理人、使用人その他の従業者が、その法人又は人の業務に関して、次表①、②、④又は⑦から⑨までの違反行為をしたときは、その行為者を罰するほか、その法人又は人に対しても、罰金刑が科される（同法第77条第1項）。」

8.特定個人情報保護のための主体的な取組について

特定個人情報を適切に保護するためには事業者の主体的な取組が不可欠である。そこで、本ガイドラインは、そのことを次の

ように強調している。

「事業者が特定個人情報の適正な取扱いを確保するためには、経営者自らが特定個人情報に対する保護措置の重要性について十分な認識を持って適切な経営管理を行うことが重要である。その上で、事業者は、番号法等関係法令並びに本ガイドライン及び主務大臣のガイドライン等に従い、特定個人情報の適正な取扱いを確保するための具体的な方策について検討し、実践するとともに、業務の実態、技術の進歩等を踏まえ、点検・見直しを継続的に行う体制を主体的に構築することが重要である。

なお、番号法第6条において、個人番号を利用する事業者は、基本理念にのっとり、国及び地方公共団体が個人番号の利用に関し実施する施策に協力するよう努めるものとするとされている。」

9.特定個人情報の漏えい事案の発生等した場合の対応等

国際的には、個人情報の漏えいなどがあった場合には、その通知を法的に義務付ける傾向が強くなってきている(data breach notificationなどの言葉が使われている)。日本では法的義務にまではなっていないので、本ガイドラインは、特定個人情報の漏えい事案の発生等した場合の対応等について次のように記述している。

「個人情報の漏えい事案の発生等個人情報保護法違反又は同法違反のおそれが発覚した場合、個人情報取扱事業者は主務大臣のガイドライン等に基づき報告が求められているところであるが、事業者の特定個人情報の漏えい等個別の事案の取扱いについては、関係省庁等と連携を図ることとし、別に定める。」

10.個人情報取扱事業者でない個人番号取扱事業者における特定個人情報の取扱い

前述のように番号法では「個人情報取扱事業者でない個人番号取扱事業者」という概念が用いられているが、本ガイドラインは、その特定個人情報の取扱いについて次のように記述している。

「個人情報取扱事業者でない個人番号取扱事業者においても、特定個人情報について、個人情報保護法における個人情報より厳格な保護措置を求めている番号法の趣旨に鑑み、番号法に特段の規定が置かれていない事項については、個人情報保護法における個人情報の保護措置に関する規定及び当該部分に係る主務大臣のガイドライン等に従い、適切に取り扱うことが望ましい。」

11.本ガイドラインの見直しについて

本ガイドラインについては、社会情勢の変化、国民の意識の変化、技術動向の変化等諸環境の変化を踏まえ、必要に応じ見直しを行うものとする。

12.各論

以上が本ガイドラインの「総論」であって、「各論」ではより具体的に記述している。それらについて見るならば、本ガイドラインの中で、「しなければならない」および「してはならない」と記述していることがどのようなことであるかが理解できるであろう。本ガイドラインの「第1　はじめに」の最後で注意喚起しているように、「これらに従わなかった場合、法令違反と判断される可能性がある」。また、それ以外に「望ましい」と記述していることがどのようなことであるかを知ることができる。この「「望ましい」と記述している事項については、これに従わなかったことをもって直ちに法令違反と判断されることはないが、番号法の趣旨を踏まえ、事業者の特性や規模に応じ可能な限り対応することが望まれるものである」ことを認識できるであろう。

しかし、その概要を紹介する紙幅がなくなったので、本ガイドラインそのものを参照されたい。

13.おわりに

本稿の叙述からすでに明らかなように、番号法は、個人情報保護法を前提にしているので、本ガイドラインでは巻末資料として「個人番号の取得から廃棄までのプロセスにおける本ガイドラインの適用(大要)」を掲げている。これをここでも掲載することにする。

本ガイドラインはもとよりその他の問題についても、特定個人情報保護委員会（〒107-0052 東京都港区赤坂1-9-13　三会堂ビル8階 電話：03－6441－3685（代表））に問い合わせていただきたい。

・特定個人情報保護委員会
http://www.cao.go.jp/bangouseido/ppc/index.html
・特定個人情報保護委員会　法令・規則等
http://www.cao.go.jp/bangouseido/ppc/laws/laws.html

（巻末資料）

個人番号の取得から廃棄までのプロセスにおける本ガイドラインの適用（大要）

区分	個人情報保護法	本ガイドライン（番号法該当条文）
取得	・利用目的の特定（第 15 条） ・適正な取得（第 17 条） ・利用目的の通知等（第 18 条）	・第４－３－(1) 個人番号の提供の要求（第 14 条）…求める根拠 ・第４－３－(2) 個人番号の提供の求めの制限、特定個人情報の提供制限（第 15 条、第 19 条、第 29 条第 3 項） ・第４－３－(3) 収集・保管制限（第 20 条） ・第４－３－(4) 本人確認（第 16 条）
安全管理措置等	・安全管理措置（第 20 条） ・従業者の監督（第 21 条） ・委託先の監督（第 22 条）	・第４－２－(1) 委託の取扱い（第 10 条、第 11 条） ・第４－２－(2) 安全管理措置（第 12 条、第 33 条、第 34 条） ・（別添）特定個人情報に関する安全管理措置（事業者編）
保管	・正確性の確保（第 19 条） ・保有個人データに関する事項の公表等（第 24 条）	・第４－３－(3) 収集・保管制限（第 20 条）
利用	・利用目的による制限（第 16 条） ※番号法による読替及び適用除外あり ・利用目的の通知等（第 18 条第 3 項）	・第４－１－(1) 個人番号の利用制限（第 9 条、第 29 条第 3 項、第 32 条） ・第４－１－(2) 特定個人情報ファイルの作成の制限（第 28 条）
提供	・第三者提供の制限（第 23 条） ※番号法では適用除外	・第４－３－(2) 個人番号の提供の求めの制限、特定個人情報の提供制限（第 15 条、第 19 条、第 29 条第 3 項）
開示 訂正 利用停止	・開示、訂正等、利用停止等（第 25 条～第 30 条） ※利用停止等（第 27 条）は、番号法による読替あり	・第４－４ 第三者提供の停止に関する取扱い（第 29 条第 3 項）
廃棄	・該当条文なし	・第４－３－(3) 収集・保管制限（第 20 条）

注：この表は、各プロセスにおける個人情報保護法の適用条文と本ガイドラインの適用部分のイメージを記載したものです。
よって、各プロセスに正確に適用される条文とは、若干異なりますので、ご留意願います。

2 [事例紹介]地方自治体における番号制度への取組みについて

[インタビュー]

2-1.東京都の番号制度への取組み

東京都生活文化局広報広聴部情報公開課長
（特定個人情報保護検討プロジェクトチーム座長）　高橋　葉夏
広報広聴部情報公開課個人情報係長(課長補佐)　髙野　祥一

1.番号制度対応のための体制整備

1.1　組織体制

2013年5月の番号法公布を受け、東京都として早急の対策を講じる必要があることから、全庁的な体制として関係部署で構成する「社会保障・税番号制度企画調整会議」（議長：総務局行政改革推進部長）を同年4月に立ち上げた。全体の検討・調整はこの会議で行うこととなるが、制度への対応が広範囲にわたることから、課長を座長とし、課長補佐、係長級職員で構成する3つのプロジェクトチームを設置し、それぞれ1～2か月に1回程度、個別課題の検討・調整を行っている。

（1）番号制度活用検討プロジェクトチーム
- ・番号制度の独自利用・連携に係る課題
- ・プッシュ型サービス、法人番号に係る課題　等の検討

（2）特定個人情報保護検討プロジェクトチーム
- ・特定個人情報保護評価（PIA）制度の構築に係る課題
- ・評価実施に係る課題　等の検討

（3）情報システム基盤整備検討プロジェクトチーム
- ・中間サーバの整備に係る課題
- ・各業務システム等との接続に係る課題
- ・宛名情報の整備、初期突合に係る課題　等の検討

特定個人情報保護検討プロジェクトチームでは、PIAの制度構築に係る課題の検討を行うとともに、担当職員に番号制度を理解してもらうため、有識者を招いて説明会を開催した。

番号制度自体が新制度であることから、国から出された「しきい値評価」を基に、PIAに「慣れる」ため試行を行い、そこから具体的な評価の実施方法、マニュアル作り、審査側の対応、各課題の整理等を行った後、2014年10月からPIAに本格的に取り組み始めたところである。

1.2　段階的に行う条例整備

自治体の場合、法律等の規範に基づき条例整備が行われることになるが、東京都では今回の制度導入にあたり、特定個人情報の保護について、2段階による条例整備で対応することとしている。

①第1段階：PIAスタートのための条例改正

東京都情報公開・個人情報保護審議会（以下、「審議会」という。）の下部組織として、「特定個人情報保護評価部会（仮称）」を設置し、審議事項を追加するための条例改正案を2014年12月開催の都議会定例会議に提案する予定である。都議会における議決を経て、2015年1月に改正条例が施行され、第三者点検が実施される予定である。

②第2段階：特定個人情報保護制度のための条例改正・新条例の整備

個人情報保護法や個人情報保護条例を基に運用している個人情報保護制度と番号法に基づく特定個人情報保護制度は、目的・性質の全く異なる制度である。

この新制度を構築・運用するためには、条例改正とともに新たな条例の制定が必要になると考えられる。その理由は多岐にわ

たるが、その一つとして「個人情報」の定義の問題がある。番号法で地方自治体に適用される個人情報の範囲は、東京都の条例で定義されている個人情報の範囲よりも狭く定義されている。

個人情報の定義については、一見それが個人情報と判断できない内容（メールアドレスなど）であっても、他の情報（IDや職員名簿など）と照合することにより特定の個人が識別される場合は個人情報と定義されている。識別の程度に関しては、民間事業者に比べ、自治体や行政機関は厳格に識別しなければならない立場にあるため、個人情報保護法では「他の情報と『容易に』照合することができ、それにより特定の個人を識別できることとなるものを含む」と規定しているのに対し、東京都の条例では「容易に」という表現が含まれていない。個人情報保護法は民間事業者に適用されるため、民間事業者に厳格な照合性を求めることが事業の妨げとなることを避けるため、個人情報の定義について、「他の情報と容易に照合できるものを含めて個人情報」として、容易照合性を認めている。自治体の場合、相当数が東京都と同様に容易照合性を規定していないため、番号制度に対応する条例の整備においては、この点が重大な問題になると解される。

条例により厳しく広い範囲で保護していた個人情報を、番号制度に合わせて狭い範囲とすることは、自治体の立場として採り得ないものであり、既存の個人情報保護制度に混乱を生じさせない観点から、番号制度を別の制度として整備する方が、都民にも職員にもわかりやすいものになると考えている。

そのため2014年10月10日開催の審議会において、条例整備について諮問した。同年度内に答申を受け、2015年度中に条例整備を行い、2016年1月の個人番号利用開始前に体制整備を完了する計画である。

2.PIA実施に向けての準備

PIA実施にあたって、国が示す番号制度に関する指針やガイドラインではPIAに関する具体的な実施のための詳細な内容は示されておらず、自治事務として各自治体の判断に委ねられている。

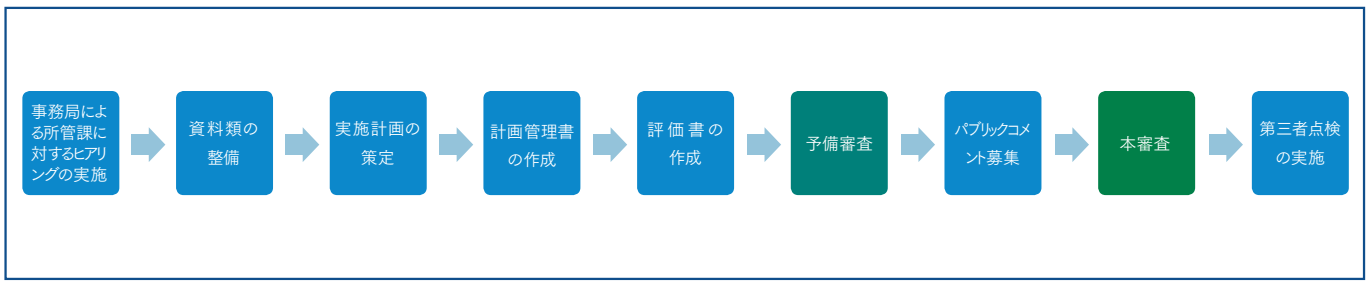
東京都としては、その取組みとして①新条例を含めた条例整備、②独自マニュアルを含めた評価の仕組みづくりを、併せて「東京モデル」として例示していきたいと考えている。

現在、特定個人情報保護検討プロジェクトチームにおいてルールを作成し、庁内に徹底・運用していくため、フローやマニュアルの作成に着手しているところである。実際、10月から評価を実施しており、マニュアル類は随時ブラッシュアップしていく。

個人情報保護制度は、個人情報の保護と活用のバランスが重要であるが、番号制度においても、個人番号の活用を促進する一方で、過度な保護措置による担当部署での負担の過度な増加は当然避けたいところであり、試行錯誤しながら着手しているところである。

PIAは図表2-1のような流れで実施することとなる。

東京都では、パブリックコメント募集などの各作業期間を算定し、全項目評価の場合は約5か月かけて実施する計画を立てている。ただしこれは順調に行った場合の期間であり、規程等が未整備である場合などは、さらに期間を要することが想定される。



図表2-1.PIA実施手順

3.PIA実施に向けての課題

PIA実施にあたり、最も重視すべき点は、評価書の作成そのものではなく、評価実施に至るまでの事前準備、特にさまざまな規程類の整備である。

たとえば、東京都全体の情報セキュリティポリシーが制定されていても、個別システムに対するポリシーや権限規定が定められていなければ、新たにルール化、整備が必要となる。そのためには、規程類の整備作業を一つひとつ所管課に担ってもらう必要がある。明確な規程類が提出されれば、リスク分析を含めさらに整理ができてくることになるため、この点を庁内で繰り返し周知しており、徐々に理解が深まってきている。

新たに導入される特定個人情報保護評価制度に対し、きちんとした規程類の整備を行うことが一番の課題であり、評価書作成を目的とするのではなく、評価書作成に至る過程の中で、いかにリスクを洗い出し、それを軽減できるかが重要と考えている。

規程類の整備に関しては、通常、業務処理は課または係単位での作業となるが、たとえばシステムへのアクセス権限について、現在は課・係全体の業務として課・係員にアクセス権限が付与されている場合が多いのに対し、番号制度では、個別事務かつ個人ごとにアクセス権限を付与するよう要求されている。このため、事務手順やマニュアルで定める等の対応が必要となることから、そのような条例改正よりもマニュアル類、ルールの整備の方が作業量としては多いと想定している。

システム改修が始まる前段階でPIAを行わなければならないが、大規模システムに関しては規程類が整備できているため、あまり問題視していない。しかし一方では、手作業やスタンドアロンでの事務処理も存在することから、小規模システムへの対応が必要である。

4.PIA実施手順・体制

PIA実施にあたり、該当業務およびシステム構成を理解していなければ審査は行えないため、所管課からの提出資料類はかなり膨大な量となる。所管課、審査担当者ともに多大な負担を余儀なくされることとなるため、マニュアル類を作成して統一的な方法を示しながら準備を進めているところである。

新制度運用に向け、ゼロから作り上げていかなければならないが、関係部署に対し、制度の全体像を示すことで、何から着手すべきかを理解してもらうようにしている。

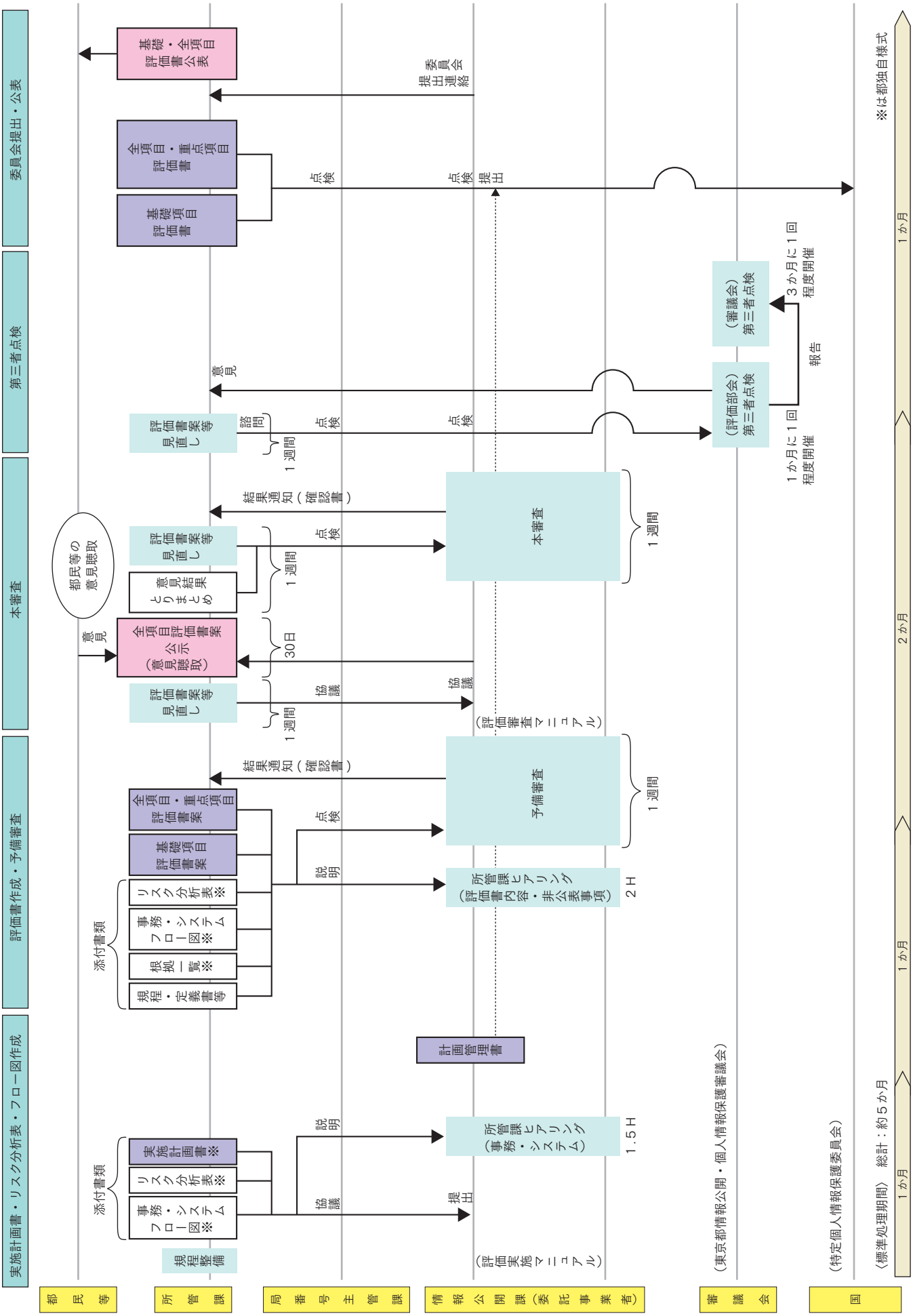
4.1　PIA実施手順

東京都では全項目・重点項目評価のため、処理期間を約5か月と見積り、2014年10月の段階で図表2-2のような事務フローで行う計画を立てている。

フロー図にある「実施計画書」はしきい値判断の手続きについて示したもので、国が定める様式には記載されていないが、東京都が独自に追加したものである。

国が示した当初の手順では、しきい値評価から開始することとなっていたが、最終的にこれが基礎項目評価に変更となったために、基礎項目評価の前にしきい値判断を行わなければならなくなった。このため、しきい値判断の手続きを明確にするため、「実施計画書」としてフローに盛り込んでいる。この段階で、各所管部署に対しヒアリングを行い、しきい値判断が正しいか否かの確認も行うこととしている。

「リスク分析表」も東京都が独自に追加したものである。全項目評価か重点項目評価にかかわらず、このリスク分析表を参照しながらリスクの洗出し、リスクへの対策が網羅できるようにした。これらの資料を参照すれば、評価書作成自体はそれほど困難ではないと考えている。やはり、規程や根拠の整備が最大の難関であると思われる。



図表2-2.「全項目・重点項目評価の事務フロー（想定）」図

PIAの実施において、東京都では「本審査」の前に「予備審査」を行うこととしている。国の指針によれば、評価書公示・意見聴取の段階で「課題が残されている」という評価書の選択肢を選択することも有り得るものとしているが、特定個人情報保護評価制度とは、国民に対し「特定個人情報を適切に取り扱っている」ことを宣言するために行うことが趣旨である。このため、東京都としては「課題が残されている内容をパブリックコメントに出すべきではない」との考えにより、予備審査でチェックを行い、課題を解消したうえで評価書案を公示・意見を聴取し、その結果を反映させて本審査に臨むべきと考えている。

このため、一般的なフローに比べ、約5か月という期間を要することとなるが、その分適確に対応できると考えている。評価対象事務の所管課に対する2回のヒアリング、予備審査を行うことで不適切な記載をなくす、この点が一番重要と考えている。より迅速な作業が遂行できるよう、国の提示する様式に加え、「リスク分析表」等の東京都独自の様式を作成している。

4.2　PIA実施上の課題

事務所管課としてどのような作業が生じるか、何を行わなければならないかなど、法律条文だけでは理解しづらい点も見られることから、関係部署職員を含め、制度の周知・普及を図っていく予定である。

今後、情報提供ネットワークシステムを介して全国で個人番号および特定個人情報の情報連携を行うことにより利便性が向上する一方で、仮に事故が発生すれば、プライバシー等に影響が及ぶ範囲は甚大となる。このような影響を最小限に抑えるためにも、まず国がPIA実施のための統一基準や評価書作成様式を提示し、それを参照して各自治体に合致した評価書作成、体制整備を図るべきではないかと考えている。

日本最大の自治体として、首都東京から重大な事故等が生じないような体制を構築すべく、本制度に対して真摯に取り組んでいる。特に2020年の東京オリンピック開催を控え、都民の皆様に安心を提供できる仕組みを整備していかなければならないと考えている。

先にも述べたが、どのようなポリシーを持って評価書を作成するかが重要である。運用まで時間がない中、外部委託も考えられるが、その際には委託先に丸投げしてしまうのではなく、評価書作成にあたってのポリシーを明確にし、所管課職員と委託先間で綿密な協議のうえで業務内容、作業手順等を把握しつつ作成していかなければならない。

PIAは一度評価書を作成すれば終わりということではなく、常に業務遂行時にリスク分析を意識しつつ、継続しながらブラッシュアップしていくことが必要である。

5.東京都の個人情報保護対策、情報セキュリティ対策に係る研修の実施

東京都では、個人情報保護対策、情報セキュリティ対策を担当する部署が分かれているが、相互連携をとりながら制度設計をして研修を実施している。

個人情報保護、情報セキュリティともに常に意識しておかなければならないことから、全職員約4万人を対象に、eラーニングを利用して個人情報保護および情報セキュリティ研修をそれぞれ年1回義務付けるとともに、情報セキュリティ担当部門によるシステム担当者向けの研修や、個人情報保護制度に関する担当者向け、新任研修、さらにPIA制度研修など、場面に応じた研修を行っている。

個人情報保護制度については、都における制度所管課の職員が講師となり、各局の個人情報保護担当者向けに研修を行い、さらにそこから局内職員に対する研修を実施するという形で行っている。

全職員に対するeラーニング研修は、各自の端末に表示される設問に回答し、一定以上の点数を取って合格するまで、繰り返し回答させる形をとっており、端末から参考資料・テキストも参照できるようになっている。

本来の研修の目的は、事故を起こさないために必要不可欠かつ重要な事項に対する意識の啓発であることから、若干の質問項目の微修正や年ごとの課題を取り入れつつも、毎年同様の内容で繰り返し研修を行い、意識を植え付けるようにしている。

職員の意識向上の成果として、年々情報セキュリティ事故、個人情報漏えい事故は減少傾向にある一方で、委託事業者などの事故件数が増加傾向にある。さらに、番号制度導入により、一層厳しい管理が求められることから、新たな仕組みづくりが必要と考えている。

個人情報保護法制定以降、職員および都民の意識の向上が図られてきていると感じており、個人情報保護制度の定着が見られる。

番号制度を軌道に乗せるためには、職員、都民に制度を理解してもらう必要がある。たとえば、本人確認用に番号カードを利用する際の取扱い上の注意点など、重要でありながらあまり周知されていない点が多いことを含め、今後個人番号の取扱いを含めた周知・普及が必要と考えている。

6.特定個人情報の取扱いに対する職員の意識

評価対象となる3分野（主税局、福祉保健局、都市整備局、教育庁等）を所管する担当者の番号制度に対する理解、意識は1年をかけて少しずつ高まってきているが、その他業務担当職員への周知・普及については、引き続き取り組んでいかなくてはならない。

番号制度に関する国の動きは遅れが目立ち、主務省令や規則が出されていない等、現在も何が具体的に対象事務に該当するかも明確になっていない状況にある。今後、番号法別表第二に係る主務省令が制定された際には、該当事務については番号法第19条の「情報提供依頼」を受けて応答義務が発生することから、さらに特定個人番号を取り扱う所管部署は増えると考えられる。

情報提供に関する問合わせや回答については、情報提供ネットワークシステムの利用が基本となり、ネットワーク利用が可能でありながら敢えて書面で応答することは、情報セキュリティの観点から基本的に認められないと解され、各所管における特定個人情報の取扱いに関して一層の意識向上を目指していかなければならない。

7.最後に

番号法は地方の事務の実情をよく把握せずに制定されているため、法律上、禁止事項としつつも、自治体における実務上対応しなければならない事項については、指針等で新たな定義や概念を創設させるような制度づくりをせざるを得なくなっている。

地方自治体は部局をまたがり、情報は横断的に利用されている。そのため、番号制度導入により行政効率の向上が期待されているが、これまで滞ることなく行われていた事務処理が、制度導入によりさまざまな規制を受ける結果、かえって非効率になってしまうのではないかとの懸念が事務所管課にはある。

現段階においても特定個人情報の範囲が必ずしも明確でないこともあり、さまざまな用語の定義づけ等を各自治体がそれぞれで決めなければならない状況ではある。そのような状況においても、他の自治体や民間機関と横断的、広範囲にわたる事務処理を行い、国民の個人情報を守る立場にある自治体として、これまでどおり事務処理を円滑、安全かつ効率的に遂行できるよう、国との調整を図りつつ、条例や体制の整備を進め、適正に対応していかなければならないと考えている。

番号制度への取組み状況は自治体によって異なっており、これから着手する自治体も多いことと思われる。今後、情報提供ネットワークシステムでつながった個人番号が安全に利用・処理されるためには、自治体間における保護対策に温度差が生じないよう、ぜひ国による統一基準、ガイドラインが策定され、これが適正に守られるようになることに期待したい。

[インタビュー]
2-2.三鷹市の番号制度への取組み

三鷹市番号制度推進本部事務局　木村　祐介

1.番号制度取組みのための体制整備について

三鷹市の規模は、人口約18.1万人、9万世帯、全庁職員数は約1,000名（教育機関職員を除く）である。

同市では、2011年より番号制度に関する国の検討会に参加し、同年12月から庁内関係部署間での情報交換会の対象範囲を徐々に広げつつ、庁内での番号制度の周知・情報共有を図っていった。

1-1　検討チーム・WGの設置（2013年4月～2014年9月）

番号制度導入における行政事務への影響が多岐にわたり、全庁的な体制整備の必要性から、2013年5月に庁内に「社会保障・税に関わる番号制度検討チーム」を、同年6月には5つの検討部会を設置して検討を行った。

（1）窓口業務・サービスのあり方の検討 WG

制度導入の円滑化を図るため、個人番号を利用する自治体の業務について、全庁内で根拠法令および事務で取り扱うべき特定個人情報の洗出し、関係部署の特定と、事業・業務単位での整理を図るための検討を行った。

（2）個人情報保護に関する検討 WG

特定個人情報の取扱いについて、特定個人情報ファイルを処理するためにシステム設計前段階での特定個人情報保護評価（PIA）の実施が義務付けられていることから、PIA実施のための体制整備・評価方法の確立、個人情報保護条例の改正等に関する検討を行った。

（3）条例改正に関する検討 WG

番号制度導入により、情報連携を活用した添付書類の省略化など、窓口業務の手順や申請様式の変更・見直しが今後行われることから、それに伴う現行条例や要綱・規則類の改正の必要性に関し、関係課への周知および改正の方針検討、改正対象となる条例の洗い出し、改正スケジュール（議案上程、事前協議、改正案作成等）の調整等を行った。

（4）市民・職員に関する検討 WG

番号制度導入に向け、市民や事業者に対する広報活動のためのスケジュール等の検討を行うとともに、全庁職員に対する制度の理解・意識向上を目的とした研修方法・研修体制についても検討を行った。

（5）システム開発・導入に関する検討サブ WG

本庁が管理する住民票への個人番号の記載や個人番号カードの交付機能、個人番号の利用分野における各種申請書の様式変更や個人番号での検索機能、情報連携を実現するための符号取得や情報提供用データの登録・管理を行う中間サーバの整備、自治体内の宛名情報を一元管理するための団体内統合宛名システムについて、PIA実施結果を反映させた改修やシステム設計・開発が必要となるため、番号制度導入に必要となるシステム開発・改修の方針・範囲等の整理に関する検討を行った。

1-2　三鷹市番号制度推進本部の設置（2014年10月～）

2015年10月の個人番号の付番・通知まで1年となった2014年10月には、番号制度の円滑な導入開始に向けた庁内推進体制を強化するため、市長が本部長を、副市長および教育長が副本部長を務める「三鷹市番号制度推進本部」（以下、「本部」という。）を設置した。現在、本部で庁内整備の推進およびPIA実施に向けた準備を進めている。

2.PIA試行および今後の対応について

2-1　PIA試行の実施（2014年2月～5月）

JIPDECによるPIA試行に参加し、国保資格業務を対象とする試行を、企画部情報推進課（検討チーム事務局）、相談・情報課（個人情報WG）、市民部保険課（主管課）の三課が共同して実施した。

試行では最も項目数の多い全項目評価書を作成することで、評価書作成に係る作業量を把握し、PIAの考え方・課題等を整理し、市としての対応方針・評価手法・評価体制を確立することを目的とした。

2-2　試行結果からみた今後の課題と対応

2014年1月の段階では、番号制度における条例改正、PIAについても何を行えばよいのか理解できておらず、国から提示された評価書作成指針だけでは取り組むことが難しいと思われたが、試行実施により、PIAに対する理解が得られたとともに、以下のように今後の課題が明確になってきた。

（1）体制の整備

評価書作成に関しては事務局および主管課の作業量が多く、継続的な取組みが必要なため、今後の運用（年1回の見直し、5年後の再実施等）等を見据えた推進体制の整備が必要となる。

（2）業務フローの整備

各局面における特定個人情報の流れ（取得から廃棄）を、客観的に読み取ることができるように、事務運用に即した業務フローおよびデータフローの整備が必要となる。

（3）各種ドキュメントの整備・見直し

システムの仕様書・要件定義書、業務マニュアル、個人情報記録項目、管理基準・管理手順書等の規程文書について、現行で不足しているものは、整備・見直しが必要となる。

（4）ISMS 指導・教育の徹底

三鷹市では、11部署でISMS認証を取得しており、セキュリティ対策・リスク分析等はISMSの考え方を活用できる。庁内で共通認識を持って取り組む必要があることから、関係部署に対して、セキュリティ対策に関する教育・研修が必要となる。特にISMS認証を取得していない課への対応が必須となる。

3.PIA実施への取組み

三鷹市の場合、しきい値判断結果では「基礎項目評価」と「重点項目評価」の件数が多いが、すべての評価書について、最低でも重点項目を実施する考えである。ただし、あらゆるリスク分析、リスク対応、管理策の妥当性を考慮すると、重点項目でも弱いとの判断を踏まえ、現在は「全項目評価」を実施する方向で評価書を作成している。

3-1　現在の取組み状況（準備段階）

番号制度に係る方針決定・庁内調整を行う本部では、具体的にどの程度の作業量が発生するか、システム改修とPIAの連動、条例改正の必要性、特定個人情報がどこで利用されるかなど、全容を把握し、体制整備を図るため、全体の作業工程表を作成し、カテゴリ別にスケジューリング、段取りの整備を行っている。（図表2-3）

PIAに関する工程表では、本部、業務主管課、システム部門別に回答すべき項目を分類・整備し、特に主管課に対する作業負荷の軽減を考慮し、段階的に回答を求めるものとしている。さらにフォローやヒアリング調査の実施、他市のパブリックコメントなども参考にして評価項目一覧表を整理している。

三鷹市では、11部署でISMS認証を取得しており、ある程度情報セキュリティに関する取組み、規程類やエビデンスの整備が進んでいることから、該当資料の提出が可能となるが、それ以外の部署に対しどのようなアプローチをとるべきか、資料の整備を含め、取組み中である。

すでに意見聴取を実施している他の自治体の評価書について、同じ業務であっても、自治体ごとに解釈が異なる部分が見受けられることから、三鷹市においては、できるだけ解釈・文言等の統一が図れるように本部で基準を設定し、回答の記入方法もある程度標準化する予定である。今後、毎年の見直しや5年後の再実施に向けた手順の確立のためにも、基準の整備が重要と考えている。

検討・作業項目	作業内容
所管課の決定	所管課（とりまとめ部署）を決定し、WGの検討範囲の設定を行う。
手法・方針等の検討	PIA について、評価書作成単位、特定個人情報ファイルの定義、スケジュール整備、パブリックコメント・第三者点検の範囲、庁内の調整、機微情報の扱い、ISMS教育の推進等の検討を行う。
PIA 試行	PIA の考え方・進め方、評価書作成に係る必要事項・職員負担等を整理するために、PIA 試行を行う。
評価書作成方法（対象件数の抽出方法等）の検討	対象件数の抽出方法、外部提供・外部委託の内容、契約書の見直し（委託先監督の強化）、手作業ファイルのシステム化等の検討を行う。
対象部署・業務の特定	別表記載の業務主管課、システム利用課、独自利用部署等を整理し、PIA の対象となる部署・業務の特定を行う。
対象のデータ抽出・整理	対象となる特定個人情報ファイルを特定し、データ件数等の抽出・整理を行う。
計画管理書の作成	評価書作成の前段作業である計画管理書の作成を行う。
研修・ヒアリングの実施	PIA 対象部署の職員に対し、研修・ヒアリング（評価書の見直し）を行う。
各種ドキュメント（ISMS 関連文書、業務フロー等）の整備	PIA 対象部署における必要書類（ISMS 関連文書、業務フロー、システム記録項目・要件定義書、庁内情報連携システム・連携項目一覧等）の整備を行う。
運用基準（情報セキュリティポリシー、アクセス制御）等の見直し	情報セキュリティポリシー、アクセス制御基準、管理者の見直し・設定を行う。
ISMS 教育・指導	PIA 対象部署に対し、評価書作成必要事項となる ISMS 教育・指導を行う。
評価書案（全項目評価書、重点項目評価書）作成	しきい値判断、評価書（基礎項目評価、重点項目評価、全項目評価）案の作成・とりまとめを行う。
外部ヒアリング（評価書案の確認・点検）の実施	全項目評価書（重点項目評価書）案の内容について、外部によるヒアリング等を実施し、評価書の記載漏れ・不足した規定類等がないか、評価書の見直しを行う。
パブリックコメントの実施	全項目評価書（重点項目評価書）案についてパブリックコメントを実施し、評価書の見直しを行う。
外部審査（第三者点検前の評価書の事前チェック）の実施	全項目評価書（重点項目評価書）案の外部審査（事前チェック）を実施し、評価書の見直しを行う。
第三者点検（個人情報保護審査会等）の実施	全項目評価書（重点項目評価書）案の第三者点検（個人情報保護審査会等）を実施し、評価書の見直しを行う。
評価書の承認（個人情報保護委員会）	個人情報保護委員会による全項目評価書（重点項目評価書）の評価（承認）を行う。
評価書の提出（特定個人情報保護委員会）	特定個人情報保護委員会（三条委員会）へ全項目評価書の提出を行う。
評価書等の見直し（番号法別表追加事務への対応、定期点検）	計画管理書の更新、評価書の修正・新規作成（別表追加、独自利用等の新たな業務）等の見直しを行う。
継続的な研修	PIA の考え方（特定個人情報ファイルの利用、委託先の監督、評価書の作成、プライバシー保護、リスク評価等）について、継続的に研修等を行う。

図表2-3.三鷹市におけるPIA作業項目および作業内容（抜粋）

3-2　評価書の作成

評価項目の作成にあたっては、試行の段階で見えなかった課題を見つけることができた。

評価書作成後の第三者点検実施にあたり、該当業務自体を知らない立場の第三者が客観的に妥当性をチェックできるのかが重要となるため、業務がわかるような記載内容、エビデンスの用意が必要となる。内部的に行っている事務で、どのように特定個人情報ファイルを入手しているのか、システムへの登録方法など、業務の一連の流れを理解していなければ妥当性判断は難しい。この点については各自治体でもまだ取組み途中のことと思われる。三鷹市では、この点を重視し、エビデンスの整備および評価書の作成に取り組んでいる。

主管課にとって、窓口などの通常業務に加えて評価書作成に取り組むとなればかなりの負荷がかかるため、その結果、業務への影響や、評価書作成の遅延が予想される。

早期に着手できていれば主管課に依頼できたが、作業期間が短い中において、主管課に負担がかからないよう配慮し、評価項目全230項目中、170項目程度（共通の記載、既存資料で記載が可能な事項等）は本部が作成している。評価書の完成は2014年度中を予定しており、主管課に対しては、最終的に評価書が作成された後に、今後の評価書の見直しや運用方法に関するフォロー・研修等を行うこととしている。

評価書作成にあたっては、やはり業務全体の把握が必要となる。自身は現在も情報推進課と兼務の立場にあり、以前は住基・税・福祉業務システムを担当していたことから、現場の業務をある程度把握しており、業務、システム、情報セキュリティ、番号法の解釈等、それぞれの視点で評価書を作成している。評価書作成においては、事業数の多い福祉分野のとりまとめが特に困難なものになると思われる。事業数が多く、すべての業務を把握している職員も少ないため、たとえば業務フロー作成等に関しては、複数の職員で取り組む必要がある。

番号法の別表に記載された業務以外でも、同一システムを使っていれば直接特定個人情報ファイルにアクセスすることになるため、これらの事業に関してもPIAの対象となる。

全体を統括する部門がどこにあるかにもよるが、業務はもとより、システムで保有する情報や庁内におけるシステム連携の仕組み等に関する知識がなければPIA対象範囲を明確にするのは難しい。

3-3　PIA実施後の体制について

業務システムの変更（システムライフサイクル）、法制度改正に伴う事務の追加・変更、番号法別表第一への追加等により、今後も継続的にPIAの見直しが生じる可能性があるため、重要な変更が生じた際の各業務主管課の対応方法、PIAとりまとめ部署への連絡等、一定の運用ルールを設ける予定である。

PIAとりまとめ部署においても、庁内における事務・組織の変更や法制度改正の動向等を監視する仕組みが必要である。

PIA評価書公表後、5年以内のPIA再実施が規定されているが、本部自体は期間限定での設置となるため、PIA再実施等に関しては、所管部署を決定の上、事務を引き継ぐことになる。そのため、制度導入時のPIA実施の中で、今後の見直し・再実施を見据えた運用マニュアル等の整備を図る予定である。PIAとりまとめ部署としての役割・作業内容を明確に文書化することで、体制変更等にも対応することが重要である。

4.三鷹市のセキュリティ対策について－ISMS認証の取得

三鷹市では、市長の方針により、市として情報セキュリティに関する徹底・強化を図るため、情報セキュリティの確保や個人情報の保護について、2004年1月から国際規格であるISO/IEC 27001（情報セキュリティマネジメントシステム：ISMS）の認証を取得し、現在、市民部市民課など11の部署で規格に基づいた情報セキュリティの維持に努めている。また、全庁（全部署）へのセキュリティ点検や研修などを行うとともに、「三鷹市情報セキュリティハンドブック」を作成し、全職員に配布するなどして、意識の向上を行い、全庁の情報セキュリティの確保に努めている。

5.市職員に対する特定個人情報の取扱い、セキュリティ対策に関する周知・教育方法

PIAに関する概要を全庁職員に周知するため、市民職員WGにて作成した「三鷹市職員のための番号制度ハンドブック（導入編）」を作成・配布している。同ハンドブックでは特定個人情報の取扱いに関する罰則強化についても掲載しており、職員への注意喚起も促している。（図表2-4）

今後は、庁内研修等の中で、具体例などを提示しつつ、特定個人情報の取扱いに関して、さらなる意識付けを図る予定である。また、市で作成している「三鷹市情報セキュリティハンドブック」や、地方公共団体情報システム機構（J-LIS）で実施しているeラーニングなど、複数の手法を活用して庁内職員に対し、漏れなく注意喚起や意識向上を図る方針である。

PIAについて研修を行う予定であるが、ISMS研修と共通した部分がある一方で、特定個人情報の取扱いなど、専門的な部分も含まれるため、PIAに特化した研修とするか、なども検討中である。

たとえば、情報資産の洗出しはISMSの範疇となるが、保有情報の詳細項目や、特定個人情報ファイルの定義はPIAの範疇となる。また、番号法改正やシステム更改等の変更が生じた際に、評価書の見直しを図らなければならないため、実施部門、推進部門としてのチェック体制の確立や、変更が生じた際の連絡体制等の構築に関しても必要となる。

番号制度の概要	根拠法令、制度の目的、個人番号の利用範囲、地方公共団体の責務、導入スケジュール
番号制度の仕組み	制度の仕組み、個人番号（法人番号）の通知、個人番号カードの交付、個人情報（特定個人情報）の提供・保護
番号制度導入により実現すること	期待される効果、情報連携によるメリット、個人番号・法人番号の利用、個人番号カードの活用、自治体事務の効率化
番号制度導入までに実施すること	庁内体制の整備、現行業務の調査、条例改正、PIA の実施、システムの整備、広報紙等による市民・事業者への周知
参考資料	番号制度関連資料、関連サイト、参考書籍

図表2-4.「三鷹市職員のための番号制度ハンドブック（導入編）」目次構成

6.最後に

番号制度に関して、番号法における個人番号利用事務として個人情報を取り扱う部門と、その他の個人情報を取り扱う部門では、制度の理解や対応について、職員間で温度差がある。しかしながら、直接関係がない部門でも、今後、個人番号カードを身分確認のために使う必要がある際の取扱いなどについて理解してもらう必要があることから、今後全庁的な研修の実施も検討している。

たとえば、行政上の守秘義務は理解していても、番号法で罰則規定が設けられていることを認識していない職員もいると思われることから、「三鷹市職員のための番号制度ハンドブック（導入編）」に注意が必要な具体的な事例を加え、研修資料として用いて周知していく予定である。

特定個人情報の取扱いに関しては、個人番号利用事務の対象となる職員に対しては、PIAを行う中で教育等を実施していく予定である。また、個人番号関係事務の対象となる職員を含めた全庁職員に対しては、番号制度導入に向けた職員研修や、現在もすでに実施している情報セキュリティ研修等の中で、教育等を実施していく予定である。

［寄稿］
2-3.川口市の特定個人情報保護の取組み

川口市企画財政部情報政策課長　大山　水帆

1.はじめに

現在、番号制度の実際の準備が各自治体で進められているが、未だどのような準備をしたらよいかわからないという話を聞く。特に特定個人情報保護評価（PIA）は自治体にとって初めての制度であり、前例がないため苦慮しているようである。私は、「マイナンバー制度に関する国と地方公共団体の推進連絡協議会」や、「特定個人情報保護ガイドライン検討会」といったものの委員をしていることから、地方公共団体の代表として、機会があればなるべく有益な情報提供を行っていきたいと考えている。今回は川口市の特定個人情報保護関連の取組み状況について紹介する。

2.番号制度対応のための体制

番号制度のための全庁的体制として、まずシステム対応の検討を先行して行うため、「番号制度に関するシステム検討部会」を立ち上げた。メンバーは番号法別表で定められている事務を行うことが想定されている部署のほか、個人情報保護担当課、事業者として給与支払報告を行う職員課、独自利用事務が想定されている乳幼児医療費助成事務担当課が含まれている。そこで、システムの影響度調査を行うとともに、番号制度に関する情報共有と各課職員に対する番号制度に対する意識付けを行った。2014年度はその部会を発展させ、独自利用や条例対応、個人番号カードの発行などシステムに限らず全庁的な検討を行う「番号制度対応検討会」に移行する。

番号制度はその影響範囲が多岐にわたるため、課をまたいだ全庁的な対応が必要だが、そういう組織が自治体にはあまりないため、対応に苦慮している所が多いのではないか。幸い、川口市の情報政策課は、横断的で横串の通った電子自治体システムを構築するため、2007年に組織改正を行い、各課から実際に電算業務を担当していた職員を集めるとともに、電算関連業務と電算経費（予算）も情報政策課に集約した。まさに電算業務において「人」、「物（仕事）」、「金」を集約した組織ができたということである。今回の番号制度対応は、システム関連の割合が高く、また各課にまたがる対応が必要であったため、情報政策課が担当することにより、番号制度の情報の整理や業務分析などの準備作業を適切に交通整理できたのではないかと感じている。しかしながら、今後はシステム関連については引き続き情報政策課が中心になるが、広報や条例対応など情報政策課に馴染まない対応も多くなることから、それらの全庁的な調整を図る必要があると思われる。

3.特定個人情報保護評価の体制

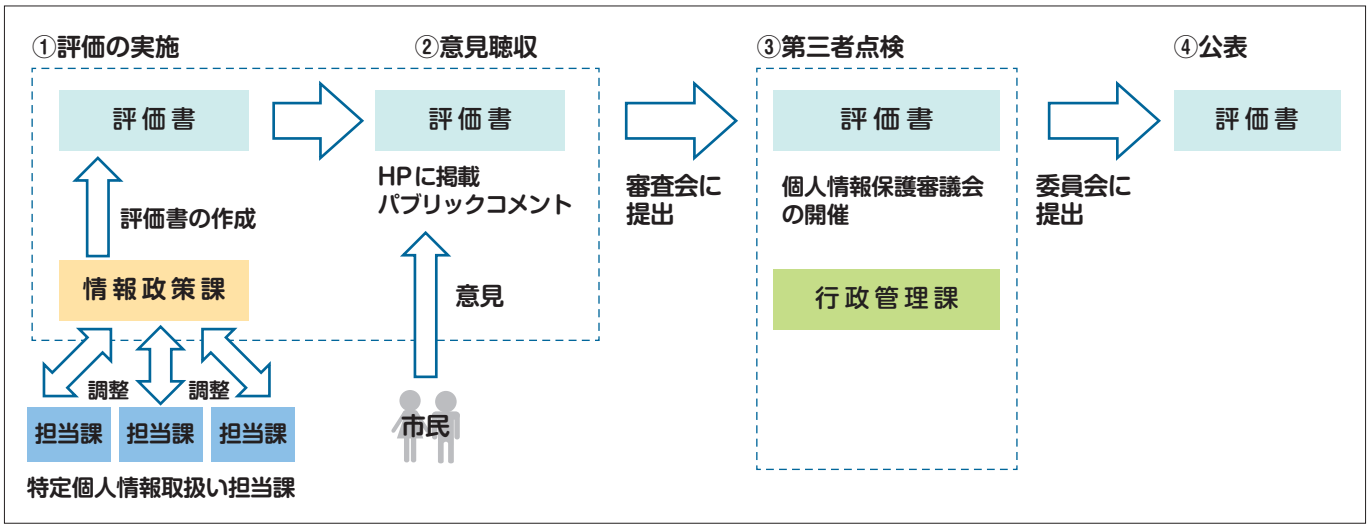
個人情報保護体制については、個人情報保護担当課がすべての自治体に存在するのと同様、PIAに関してもそれに対応する体制づくりと役割分担が重要となる。PIAを行うためには、まず担当部署の明確化を行うべきである。すなわち、

①評価を受ける部署
②評価を実施する部署
③評価をとりまとめる部署

である。

評価を受ける部署としては実際に事務を実施する部署が該当し、具体的には住民基本台帳システムであれば市民課や住民課、個人住民税システムであれば市民税課、住民税課等になる。

次に評価を実施する部署としては、システムに対する知識を有し、情報セキュリティを担当する部署が該当し、具体的にはIT推進課や情報政策課などが該当する。ただ、専門的知識が必要なことから、対応が困難な場合には、2014年度JIPDECが行っているPIA構築支援を受けることや、ベンダーの支援を受けたりすることが考えられる。また、委員会への評価書の提出や、第三者点検を行う場合の事務処理を行う評価をとりまとめる部署としては、総務課、行政管理課など、個人情報保護担当課や第三者機関として想定されている個人情報保護審議会の所管課が考えられる。番号制度主管課は、これらの役割分担を行うとともに、実際に行うことの整理を行い、PIAに備える必要がある。



図表2-5.特定個人情報保護評価の体制

4.PIAの手順整理

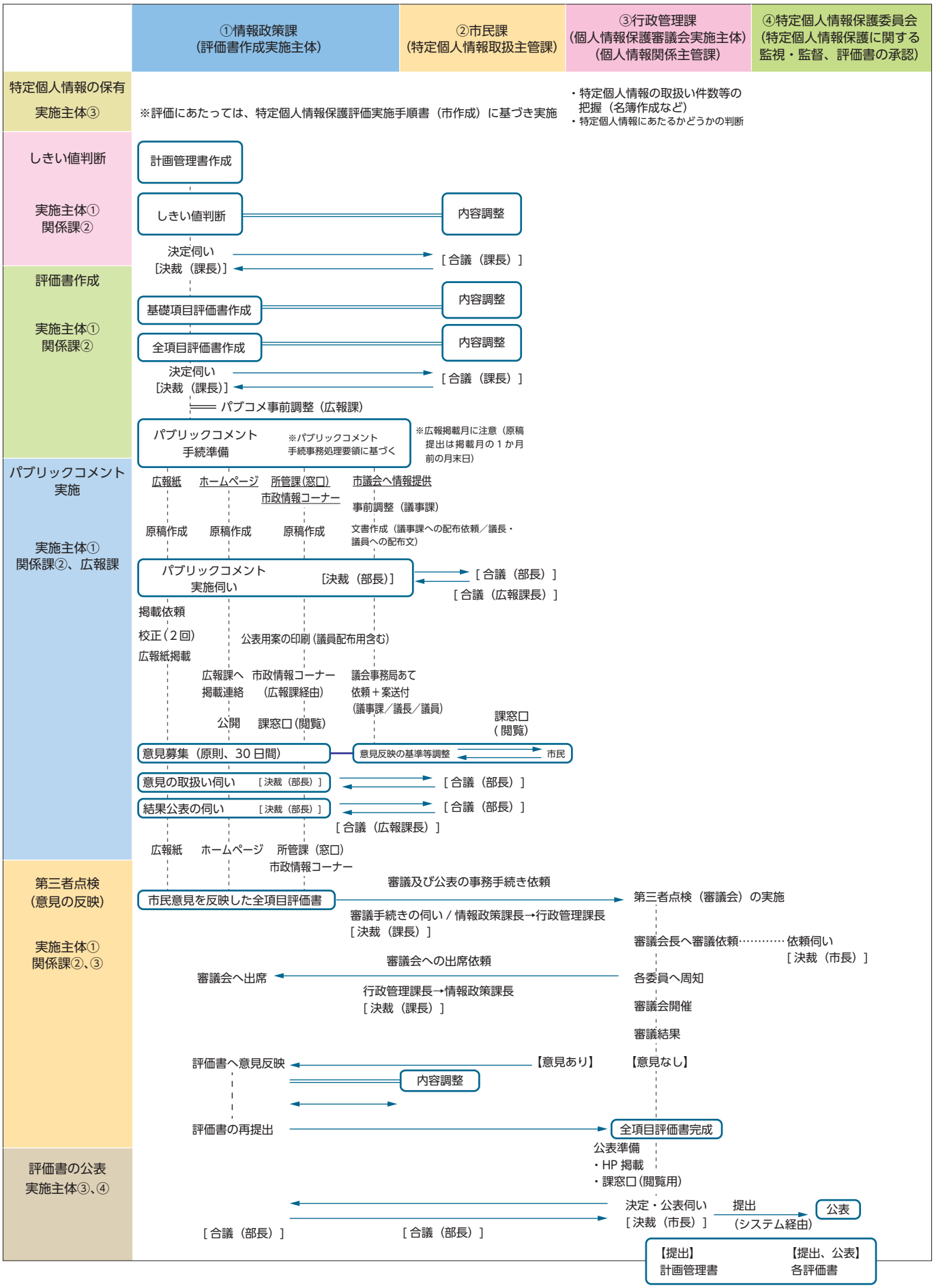
PIAを実施するにあたってはまず手順を整理する必要がある。川口市では、PIAの体制よりどのような役割分担で、どのような流れでPIAを行うのかを整理した処理フローを作成している。また、PIAは、地方公共団体においてはその長が主体となって実施することとなっていることから、特定個人情報保護委員会より公表されている評価指針に基づいてどのように実施するかを明確にするために、実施手順書を定めて実施する予定となっている。

PIAを実施するにあたっての主要な作業は、評価書の作成である。最終的に特定個人情報保護委員会に評価書を提出し、公表するまでがPIAの作業となる。具体的な手順としては

①特定個人情報台帳の整備
②実施手順書の作成
③特定個人情報評価計画管理書の作成
④しきい値判断の実施
⑤しきい値判断に基づく特定個人情報評価書の作成
⑥住民等からの意見聴取（全項目評価）
⑦第三者点検の実施（全項目評価）
⑧特定個人情報保護委員会への提出
⑨評価書の公表

を想定している。

これらの手順をまとめた処理フローが図表2-6となる。なお、フロー図は、国・地方自治体・各データ保有機関が番号制度の運用開始に向けて連携を図るための情報共有を目的としたコミュニケーションツール「デジタルPMO」に掲載しているので、自治体の方は参考とされたい。



図表2-6.特定個人情報保護評価　作業手順　【評価書名】川口市住民基本台帳システム

5.模擬PIAの実施

PIAは地方公共団体にとって初めての制度のため前例がない。それがPIAを実施するにあたって一番不安に感じていることではないだろうか。そこで川口市では、PIAの一連の作業・手続きを一通り確認しながら行う「模擬PIA」を行うことで、本番に備えることとした。この模擬PIAは、最初に想定される住民基本台帳システムを対象として実施した。対象関係部署は、評価を受ける部署である市民課、評価を行うシステム担当課の情報政策課、とりまとめを行う個人情報保護審議会所管課である行政管理課に協力をいただいた。

まず、しきい値判断と基礎項目評価書までを情報政策課にて作成し、全項目評価に該当するという結果が出た、という想定とし、その次の基礎項目評価書までの作成を行った。そして全項目評価書の内容を関係課で一つひとつ確認していき、その後、全項目評価書作成後の流れや具体的な手続き方法を、パブリックコメント、個人情報保護審議会と確認しながら進めて行った。模擬PIAを実施してみた結果、現行の個人情報保護審議会の委員がシステムに関する専門的知識が必要な評価書の内容をどこまで理解できるかといった課題が明らかになったことから、今後、個人情報保護審議会委員の改選の際には、この点についての考慮が必要という認識がなされた。全体的には、実際の手順が関係課により共有され、ある程度課題も把握できたことから成果があったと感じている。

6.システム監査体制の強化

特定個人情報保護評価書には、そのリスク対策としてシステム監査が求められている。システム監査は、通常の監査とは異なり、情報セキュリティの知識が求められることから、地方自治体において定期的、継続的に実施することは困難な場合が多いのではないか。いきなり外部監査を行うことは大変なので、まずはチェックシートによる自己点検を定期的に行うことから始め、情報セキュリティ規定の遵守性を判断する内部監査、そして外部監査とステップアップしていくような方法も有効であろう。

システム監査のポイントとしては、規定の遵守性の確認のため、とにかく記録に残すことが重要である。たとえば、パスワードを定期的に変更しなければならない規定があったとすると、それを変更した日付、変更者、変更したシステム名などが記載されたパスワード変更記録簿を整備し、さらに決裁され文書管理簿に搭載されていることが望まれるのである。コンピュータ管理区画への入退出も同様で、コンピュータ室は当然のこと、特定個人情報を取り扱う区画についてもそのような記録の管理が求められるだろう。今後のシステム監査においては、このように従来の情報資産の取扱いに加え、特に特定個人情報や特定個人情報ファイルに留意することが必要となってくる。そのようなことから、川口市では2014年度より、情報セキュリティを担当している情報政策課情報政策係を2名増員し、今まで体系的なシステム監査を行えなかった部分を強化し、継続的にシステム監査を行う体制づくりを行っている。

7.特定個人情報保護研修の実施

特定個人情報保護の取扱いは番号制度に関連する部門だけでなく、情報を取り扱うすべての職員が関係するものであり、正しく理解しておく必要がある。たとえば、今後は受付窓口などで個人番号を取り扱う機会が多くなると思われるが、安易に個人番号と紐付いた個人情報をパソコンなどに保存してしまうとそれは特定個人情報ファイルとなり、場合により法令違反となる。従来の個人情報保護法制より罰則規定の強化もされており、そのようなことのないように、できる限り機会を設けて特定個人情報保護の取扱いについて周知を図っていかなければならない。本市の取組みの事例を以下に示す。

①番号法逐条解説の配布

個人情報保護条例逐条解説が各課に配布されているのと同様、番号法逐条解説を各課に配布するとともに、管理職職員対象に行っている個人情報保護研修に2014年から番号法逐条解説を活用した特定個人情報保護の研修を行っている。

②特定個人情報保護研修の実施

一般職員向け個人情報保護研修に特定個人情報保護の内容を追加する予定である。また、すべての職員を対象に行っている情報セキュリティ研修においても、2014年度より特定個人情報保護の内容を追加して実施した。

③特定個人情報保護ガイドラインの配布

特定個人情報保護ガイドラインを配布し、その内容について研修を行う予定である。ただ、特定個人情報保護ガイドラインの内容について研修講師ができる人がいないという問題があるが、その場合はJIPDEC等の外部のサポートを受けることも有効と考える。

8.条例改正の対応

特定個人情報は個人情報の一部であり、番号法は個人情報保護条例という一般法に対する特別法としての位置付けになる。そのため、番号法と個人情報保護条例は矛盾のない整合性のとれたものでなければならない。たとえば、番号法では個人情報保護法、行政機関個人情報保護法、独立行政法人等個人情報保護法の読替え規定を定めているが、その趣旨に従い個人情報保護条例に読替え規定を定めるか、条例の構成上読替え規定では対応できない場合には、新たに条文を定めて対応する必要がある。具体的なポイントとしては、個人情報保護条例では個人情報の目的外利用または外部提供についての取扱いが定められ、審議会等に諮ること等により目的外利用または外部提供が可能となっているが、特定個人情報については、目的外利用または外部提供は生命等保護のためや大災害の場合などを除き禁止されているため、番号法と条例の整合性を図る必要がある。

9.今後の対応

特定個人情報保護ガイドラインにおいて、「しなければならない」あるいは「してはならない」と記述している部分についてはそれに従わないと法令違反となる可能性があるとされている。特に特定個人情報保護評価に記載の内容については「すべて満たすこと」とされている。したがって、特定個人情報保護評価は事前評価であるにもかかわらず、その記載内容については十分注意する必要があるということである。また、別添の対策基準については具体的に対応しなければならないことが記載されているとともに、「しなければならない」あるいは「してはならない」という記述が多いため、十分読み込んで対応しないと場合によっては法令違反となる可能性がある。この対策基準を現在満たしていない自治体においては、その体制の整備や規程類の整備を行うなど、早急に対策を行う必要がある。

今後川口市では本番のPIAを適切な時期に実施することとなるが、実施するにあたって得たなるべく多くの情報を、デジタルPMO等を通じて伝えていきたいと考えている。

社会保障・税番号制度　参考URL

・社会保障・税番号制度
http://www.cas.go.jp/jp/seisaku/bangoseido/index.html
・特定個人情報保護評価の概要
http://www.cao.go.jp/bangouseido/ppc/pia/pdf/gaiyou.pdf
・特定個人情報保護評価の概要（詳細版）（2014年9月）
http://www.cao.go.jp/bangouseido/ppc/pia/pdf/syousai.pdf
・特定個人情報保護評価指針（2014年4月20日）
http://www.cao.go.jp/bangouseido/ppc/pia/pdf/shishin.pdf
・特定個人情報評価指針の解説（2014年11月11日）
http://www.cao.go.jp/bangouseido/ppc/pia/kaisetsu/kaisetsu.html

【法律・ガイドライン等】

・個人情報の保護に関する法律（平成15年法律第57号）
http://law.e-gov.go.jp/htmldata/H15/H15HO057.html
・行政機関の保有する個人情報の保護に関する法律（平成15年法律第58号）
http://law.e-gov.go.jp/htmldata/H15/H15HO058.html
・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（マイナンバー法）（平成25年5月31日法律第27号/平成26年7月17日現在）
http://www.cas.go.jp/jp/seisaku/bangoseido/pdf/260717bangouhou.pdf
・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施行令（マイナンバー法施行令）（平成26年3月31日政令第155号）
http://www.cas.go.jp/jp/seisaku/bangoseido/seirei/26-155.pdf
・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施行規則（マイナンバー法施行規則）（平成26年7月4日内閣府・総務省令第3号）
http://www.cas.go.jp/jp/seisaku/bangoseido/seirei/26-155.pdf

【地方公共団体情報システム機構（J-LIS）】

・社会保障・税番号制度　関連情報
https://www.j-lis.go.jp/bangoseido.html

3 民間企業におけるPIAの活用と効果

デロイト トーマツ リスクサービス株式会社 サイバーリスクサービス　シニアマネジャー　　北野　晴人

※本稿は著者の私見であり所属組織の公式見解等ではありません。

1.民間企業における個人情報とプライバシーの課題

近年、ネットワーク、コンピュータ、スマートフォン等、各種技術の発展により大量の、かつ複雑で多様な情報を収集・分析できるようになった。これらの技術の活用は、新しいサービスの創出や利便性向上、社会基盤の充実等、多くのメリットを生み出している。また、日本の各種産業にとっては国際競争力を高め、グローバルな市場で生き残っていくための重要な要素となってきている。

しかし一方では、この大量に分析処理等を行う情報の中にパーソナルデータ(個人に関する情報)が含まれていることから、新規ビジネスを行おうとする企業が社会的な批判を浴びてサービス中止に追い込まれるといった事象が発生していることも記憶に新しい。これは技術の進歩によって、自由な利活用の是非が不明確な「グレーゾーン」が発生・拡大し、パーソナルデータの利活用にあたって、保護すべき情報の範囲や企業が遵守すべきルールが曖昧になりつつあることが背景にある。また同時に近年、個人に関する情報が悪用されるのではないか、といったプライバシーに関する一般社会の懸念が増大していることの表れでもある。こうした事情から、「情報を提供する個人」と「情報を収集・利用する企業」との間でどのように情報の取扱いに関する透明性を確保し、確実な合意形成とプライバシー保護の仕組みを構築できるか、という点が大きな課題の一つとなっているのである。

一連の問題発生に影響され、わが国の民間企業ではパーソナルデータの活用による新しい取組みに対して躊躇したり、計画が中断したりといった負の連鎖反応が起きており、産業界全体として、パーソナルデータの利活用に、ややブレーキがかかっている印象がある。

さらに、企業が保管・利用している大量の個人情報が漏えいし、第三者によって本人が意図しないところで流通してしまうといった問題も継続的に発生している。この問題は「漏えい」という情報セキュリティ上の懸念を再燃させているという側面と、その後の情報流通を規制できていない(いわゆる名簿屋問題)法制度の不備という側面があり、どちらも改善していくべき課題となっている。

今後、高度な情報の分析・活用による新しいビジネスを促進していくためには、これらの課題を解決し、個人(特に一般消費者)が安心して情報を提供し、サービス等のメリットを享受できる事業の構造を作り出す必要がある。だからこそ今、企業がパーソナルデータの保護・取扱いを適切に行うことが求められるのである。

これらの課題を解決するための政策として、2015年には個人情報保護法の改正が予定されており、政府の高度情報通信ネットワーク社会推進戦略本部では2013年12月20日に「パーソナルデータの利活用に関する制度見直し方針」(以下、「制度見直し方針」という。)を決定しており、その後2014年6月24日に「パーソナルデータの利活用に関する制度改正大綱(以下、「大綱」という。)」を決定している。また経済産業省ではパーソナルデータの取扱いに関して、2014年3月26日に「パーソナルデータ利活用ビジネスの促進に向けた、消費者向け情報提供・説明の充実のための「評価基準」と「事前相談評価」のあり方について」、2014年10月17日に「消費者向けオンラインサービスにおける通知と同意・選択のためのガイドライン」を公開している。さらに「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」を改正する作業を、2014年5月と9月の2度にわたって行っている。

本稿では、これらの法改正やガイドラインを視野に入れ、特に民間企業が今後のビジネスにおいてパーソナルデータを収集・活用する場合に、どのようなアプローチが望ましいかという視点で、プライバシー影響評価(Privacy Impact Assessment:PIA)およびプライバシー・バイ・デザイン(Privacy by Design:PbD)について紹介したい。なお、前述の制度見直し方針においては、プライバシー保護に対する個人の期待に応える見直しの一つとして、「プライバシー影響評価の導入」が盛り込まれている。

2.民間企業におけるPIAの活用

2-1　民間企業でPIAを活用する意義

PIAは、金融分野について標準化されているISO 22307（Financial services-Privacy impact assessment）において「自動化・ネットワーク化された情報システムを使って消費者のデータを処理することに結びつけて考えられる、プライバシーに関する問題とリスクを特定し、軽減するための重要なマネジメントツールである。」と記述されている[i]。このことからもわかるようにPIAはプライバシー保護に着目したリスクアセスメントの手法であると考えることができる。また環境影響評価と同様に、事業やサービスを企画・設計する段階で「事前に」行うことが基本とされている。

日本では2014年に入って「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」（いわゆる番号法）に基づく特定個人情報保護評価が、政府機関や公的機関、全国の自治体等で具体的に作業として始まっており、海外においてもPIAは主に政府機関や公的機関で行われている。米国やカナダなどの政府機関におけるPIAの実施と義務付けの例が知られているが[ii]、民間分野において法的な義務付けを行っている国は現時点では存在しない[iii]（ただしカナダにおいては民間に対してもセルフアセスメントツールが公開されている）[iv]。しかし、民間分野において効果がないわけではなく、むしろ積極的に活用すれば、情報を活用したい事業と適切なプライバシー保護との最適なバランスを実現することに役立つはずである。

民間企業では、すでに述べた透明性や同意取得、合意形成に関わる課題や、情報セキュリティ上の課題を解決するための方策の一つとしてPIAを活用することが考えられる。新たに事業やサービスを企画・構築する際や、それに伴う情報システムを構築する際に、あらかじめPIAを行うことでプライバシーに対する影響度を評価しておけば、その結果をもとに適切なリスクコントロールを組み込んでおくことができる。また、個人情報保護法改正後の枠組みを想定すると、近い将来にはPIAの結果を公開することで、関係する多くのステークホルダーや一般社会に対して、広く合意形成を試みることが可能になる場合もあるだろう。

2-2　民間のPIAにおける留意点

こうした目的で民間企業がPIAを行う場合には、政府機関を対象とした海外のPIAや日本の特定個人情報保護評価とは違い、事業を行う上でのビジネス的な視点を含める必要がある。構築しようと考える事業活動や、情報システムにおけるプライバシー関連のリスクを、事業への影響も含めて包括的にアセスメントすることが望ましく、そのためには次のような点に留意して計画・実行する必要がある。

（1）適法性とプライバシーの保護

・現行の個人情報保護法、および改正後の見込みを視野に入れて、適法性の確認を行う必要がある。事業を計画する段階で、取り扱う情報のどれが「個人情報」であって保護の対象であるか、第三者提供や共同利用は適切に行われる予定であるか等について検討を行う。従来は「住所や氏名などが入っていないから個人情報として扱わなくてもよいだろう」といった、法解釈上の誤解に基づく安易な判断が行われる傾向にあったが、今後は他の情報との照合容易性などを考慮した慎重な判断をする必要がある。

技術の進歩により、個人が識別・特定される可能性がある情報については、従来よりも広範囲に保護の対象と考えていく必要性が増している。しかし一方で制度見直し方針や大綱においては、匿名化措置を行うこと等、一定の条件のもとで本人の同意がなくても第三者提供を可能にする法改正が検討されている。したがって、今後は第三者提供の方法や条件、匿名化などの技術的な措置が十分であるか等について、最新の法制度に合わせた取扱いができているか、を検討・確認する必要がある。

・海外の顧客情報を扱う等、グローバルな事業を行う場合は、EUデータ保護指令等の海外法制度と、国際的な整合性に齟齬が生じないように、また海外のデータ保護機関等に対する説明責任を果たせるか、といった点についても考慮した業務とシステムの設計になっている必要がある。特にEUデータ保護指令については現在、加盟国共通の法律である「規則」に格上げする検討が行われており、近い将来罰金の大幅な引上げやいわゆる「消去する権利」（Right to erasure：従来「忘れられる権利」と呼ばれてきたもの）の保護などが実施される可能性があるため、EU域内でパーソナルデータを取り扱うような事業を構築する場合等には注意が必要である。またシンガポール、マレーシアなどアジアにも個人情報の国外持出しを原則禁止とする法制度を

新たに施行した国が存在するので、最新の状況に注意する必要がある。

・個人の権利を保護するという面から、オプトイン・オプトアウトの選択や、問合わせ窓口、情報開示・訂正・削除要求に関する窓口と対応プロセスを事前に定義し、円滑に運用できるように準備しておく(実際に消費者が問い合わせようとした時に、どこに連絡すればよいかわからないといった状態になると、そういった点まで批判の対象になる可能性がある。)。

(2)透明性の確保と合意形成

・情報取得時の、利用目的の提示、共同利用や第三者提供の有無、管理の方法等、同意の取得をわかりやすく行い、可能な限り透明性を確保することが重要であるため、それらの具体的な実現方法について確認・評価する必要がある。

実際にはWeb上での画面表示方法、同意取得のための文言の記述や取得のタイミング(利用者が同意できない場合に利用を事前に中止できるタイミングとなっているか)等については経済産業省が公開している「パーソナルデータ利活用ビジネスの促進に向けた、消費者向け情報提供・説明の充実のための「評価基準」と「事前相談評価」のあり方について」(以下、「事前相談評価」という。)や「消費者向けオンラインサービスにおける通知と同意・選択のためのガイドライン」を参考にすることができる。

たとえば、前述の事前相談評価においては同意取得の際の必要十分な記載事項として、以下の7項目を評価するべき、としている。

1) 提供するサービスの概要
2) 取得するパーソナルデータと取得の方法
3) パーソナルデータの利用目的
4) パーソナルデータやパーソナルデータを加工したデータの第三者への提供の有無および提供先
5) 消費者によるパーソナルデータの提供の停止・訂正の可否およびその方法
6) 問合せ先
7) 保存期間、廃棄

経済産業省のガイドラインは主にWeb等、インターネットを経由して行われる事業を想定したものが多いが、現実には店舗や交通機関における動画撮影や無線LANによる位置情報の取得、その後の動線分析等、物理的に看板などで表示をしなければならないものもあり得る。その場合は個人の目に触れやすいかどうか、立ち止まって読んだ上で、内容に同意できない場合には利用を取りやめることが可能な場所に掲示されているか、等の細かい検討を行う必要が出てくるので、こうした点もPIAの一部に組み込んで体系的に検討できるような仕組みにすることが望ましい。

・個人や社会との合意形成がしやすい事業構造であるか、を検討する。個人(情報主体)に還元されるインセンティブがない事業は批判される可能性が高く、社会的な意義(防災や地域の安全・安心への貢献など)がある場合には許容される可能性が高いと考えられる。ビジネスモデル自体が、個人から同意を得やすいものになっているかという視点で評価することが望まれる。

・個人や団体等、合意形成をするべき多くのステークホルダーが存在する場合は、「マルチステークホルダープロセス」に配慮することが重要な場合がある。

マルチステークホルダープロセスとは、三者以上のステークホルダーが、対等な立場で参加・議論できる会議を通し、単体もしくは二者間では解決の難しい課題解決のために、合意形成などの意思疎通を図るプロセスであり、総務省による「パーソナルデータの利用・流通に関する研究会　報告書」でも「パーソナルデータの利活用のルール策定にあたっては、「マルチステークホルダープロセス」(国、企業、消費者、有識者等多種多様な関係者が参画するオープンなプロセス)を、取り扱うパーソナルデータの性質や市場構造等の分野ごとの特性を踏まえ、積極的に活用することとすべきである。」としており、大綱では「グレーゾーンの内容や個人の権利利益の侵害の可能性・度合いは、情報通信技術の進展状況や個人の主観等複数の要素により時代ととも

に変動するものであることから、これらに機動的に対応することを可能とするため、社会通念等も踏まえつつ、法律では大枠を定め、具体的な内容は政省令、規則及びガイドラインにより対応する。また、これと併せ民間の自主規制ルールの活用を図ることとする。」としている。いわば法規制で厳密に規定できない部分を民間の関係者が協議・合意することにより自主的にルールを作る、という枠組みである。ただし従来の業界別自主規制等と異なり、何らかの第三者機関が関与して認定等を行い、その実効性を確保する枠組みを創設することになっている[v]。

企画・構築しようとしている事業やシステムについて、こうしたプロセスを経て構築された自主規制に沿っているかを確認する必要がある場合が出てくる可能性がある。また、新たにマルチステークホルダープロセスを実行して合意形成を行うことが望ましい場合があるだろう。特に利害関係が相反するステークホルダーが存在する場合や、業界全体で共通のガイドラインを作成した方がよい場合などには留意が必要であると考えられる。

(3)安全管理措置（情報セキュリティ）

・リスクアセスメントによって想定されるセキュリティ関連リスクを洗い出し、パーソナルデータの機密性・完全性・可用性に対する侵害を想定して影響度評価を行う。情報漏えい対策では機密性の保護に重点が置かれがちであるが、プライバシーという面から考えた場合は完全性にも十分配慮する必要がある。

・適切な技術的対策、組織的対策、人的対策が実施されているか（実施する予定であるか）を確認・評価する。経済産業省の「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」は2014年の二度にわたる改正作業で、技術的な対策の例示についてもさらに充実したものになっており、参考にすることができる。元来、情報システムはリスクアセスメント結果をもとに策定したセキュリティ要件を反映させて設計・開発が行われるべきであるが、それらは必ずしも十分でないのが現実である。したがって、PIAの導入に組み込む形で情報セキュリティ面においても適切なリスクアセスメントを実施できれば、いわゆる個人情報保護対策としても非常に有効なものになると考えられる。特に注目される例示の追加としては、以下のようなデータベースへの対策についてのアクセス制御に関する記述がある。こうした点も踏まえてアセスメントに活かしたい。

> ・個人データを格納した情報システムへの無権限アクセスからの保護（たとえば、ファイアウォール、ルータ等の設定）
> ＊個人データを格納するためのデータベースを構成要素に含む情報システムを構築する場合には、当該情報システム自体へのアクセス制御に加えて、情報システムの構成要素であるデータベースへのアクセス制御を別に実施し、それぞれにアクセス権限を設定することが望ましい。

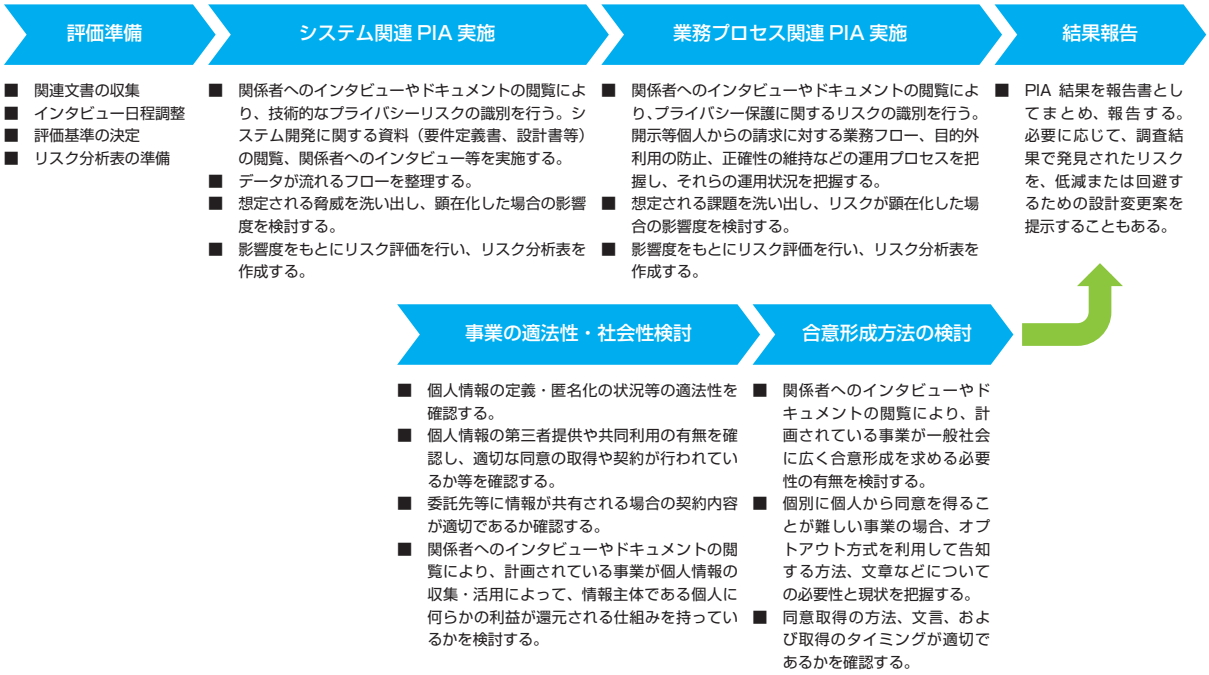
・問題が起きた際には迅速にインシデント対応が行われ、説明責任が果たせるような対策と準備が必要である。

・システムの実装と運用については、定期的に確認され、安全な状態を維持する必要があるため、このための仕組みについても確認と評価が必要である。またサービス開始後（システムの稼働開始後）については、情報セキュリティ監査を用いて確認する方法もある。

2-3　民間のPIAの実行プロセス

民間企業における事業への影響とプライバシーに対する影響の双方を考慮して、実際にPIAを実施する場合のプロセス例を図表3-1に示す。ここでは主に情報システムの技術的な面を評価する「システム関連PIA」と業務プロセスにプライバシー保護の仕組みが組み込まれているかを評価する「業務プロセス関連PIA」、適法性やビジネスモデルなどを検討する「事業の適法性・社会性検討」、透明性の確保や適切な合意形成方法等を検討する「合意形成方法の検討」という4つのカテゴリに分けて計画・実行している。各カテゴリの評価・検討は並行して行うことができるが、業務プロセスとそれを支える情報システムの機能といった、相互に依存する要素もあることに注意が必要である。全体の流れとしては、一般的に以下のようなものになる。

①あらかじめ計画されている事業やシステムの内容を可能な限り具体的に把握する。
②遵守すべき法制度やガイドライン、業界内の自主規制等を確認する。
③予定されている業務とシステムにおける情報とデータの流れを整理し、確認する。
④各種の脅威（発生することが予想される問題）を洗い出し、それらが顕在化した場合のプライバシーおよび事業に対するリスク（＝影響度）を評価する。
⑤適法性（保護対象情報の範囲や定義等を含む）の確認や、個人に対するインセンティブの有無等、ビジネスモデルに関する検討を行う。
⑥同意取得の方法やタイミング、取得のための文言など、情報を提供する個人との合意形成方法について、問題がないか検討を行う。
⑦全体をとりまとめ、リスクの大きさと優先度に従って、洗い出されたリスクへの対応策を検討する。



図表3-1.民間企業におけるPIAの実施プロセス例

2.4　PIAのレベル分け

図表3-1で示したPIAのプロセスは、実際に民間企業の現場で実施する場合、相応のスキルとコストが必要になる。したがって、対象となる事業の内容や規模、取り扱う情報の量や機微度等によっては、コスト的に見合わない場合が出てくる可能性がある。また企業規模が大きくなり、企業内の事業部門、またはグループ会社等が個別に多様な事業を行うようになると、新しい事業やシステムすべてに本格的なPIAを適用することは現実的ではない。そうした場合には、比較的簡便な方法で初期アセスメントを行い、必要に応じて本格的なPIAを計画する、という段階的な手法を検討した方が現実的であろう。さらにその場合には、簡易アセスメントの手法を社内で標準化・ルール化し、一元的な管理とガバナンスを実現する必要もある。

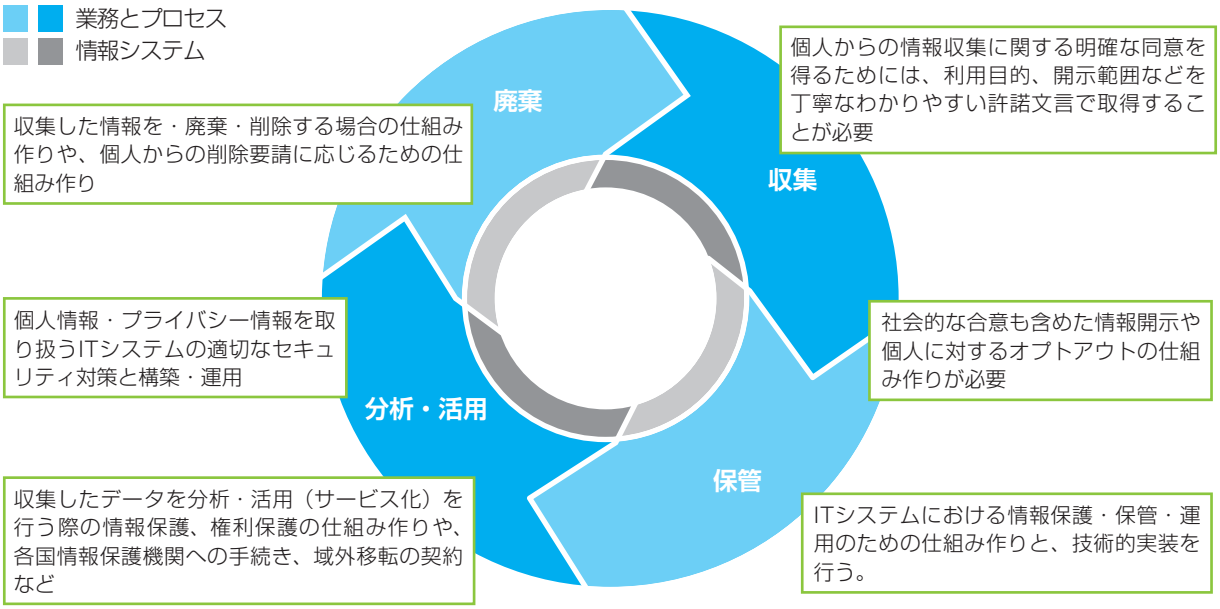
この考え方については海外の政府機関におけるPIAの仕組みにその形を見ることができる。たとえばカナダ政府の例では「コアPIA」と「フルPIA」という2種類のPIAが存在し、はじめにコアPIAを実施した上でさらなるフルPIAが必要か否かを判断する仕組みになっている。また米国の国土安全保障省（Department of Homeland Security：DHS）ではPrivacy Threshold Analysis（PTA）と呼ばれるQ&A形式のテンプレートが公開されており、新たなプログラムやシステム等がプライバシーへの影響を有するかを判断し、追加的にPIA等の必要性を判断・決定するためのツールとして利用することができる（わが国の特定個人情報保護評価におけるしきい値判断と似た仕組みである。）。

このように、リスクの大きさやコストなどを考慮したバランスのよい運用方法を検討することが結果としてPIAを企業内部に根

付かせることにつながると考えられる。

3.プライバシー・バイ・デザインのすすめ

PIAを実施した結果、認識されたリスクは何らかの形で適切にコントロールされなければ意味がない。したがって、「情報を活用したい事業と適切なプライバシー保護との最適なバランスを実現する」という目的を達成するためにはPIAによって事前の評価を行うだけではなく、その結果を反映させた形で、業務のプロセスや運営組織、それらを支える情報システムにプライバシー保護の仕組みが組み込まれなければならない。そして国内外の各種法制度、ガイドライン、さらにはOECDガイドライン等の国際的な基準を満たしている必要もある。またこれらは構築時だけでなく継続的に維持されていく必要があり、パーソナルデータの収集・保管・分析／活用・廃棄というライフサイクルに沿って適切に運用されなければならない。（図表3-2）



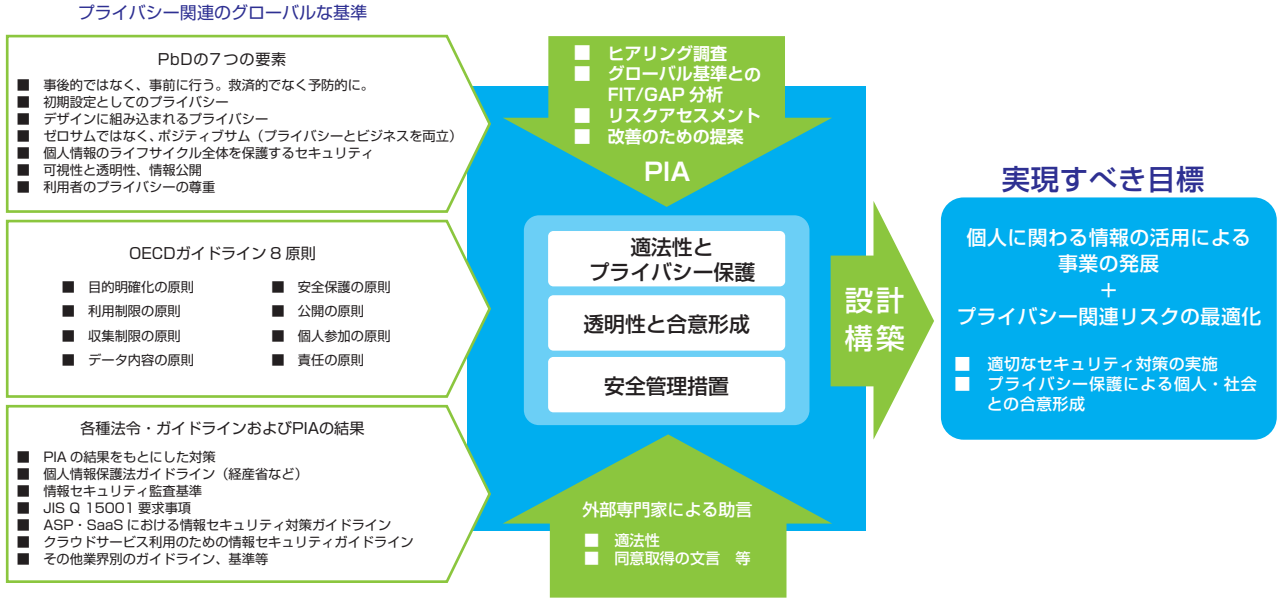
図表3-2.情報のライフサイクル全体の保護（イメージ）

このように、プライバシー保護の仕組みをあらかじめ組み込んで事業や情報システムの設計・構築をするという考え方については、カナダ・オンタリオ州情報プライバシー・コミッショナーであるアン・カブキアン博士が1990年代に開発した概念、プライバシー・バイ・デザインが国際的によく知られている。プライバシー・バイ・デザインは、以下の7つの原則から構成されている。またこれらの原則に基づいて、プライバシーに関する情報を公正に取り扱うことをFair Information Practices（FIPs）と呼んでいる。

- 事後的ではなく、事前的；救済的でなく予防的
- 初期設定としてのプライバシー
- デザインに組み込まれるプライバシー
- 全機能的－ ゼロサムではなく、ポジティブサム
- 最初から最後までのセキュリティ（すべてのライフサイクルを保護）
- 可視性と透明性－ 公開の維持
- 利用者のプライバシーの尊重

すでに第32回データ保護・プライバシー・コミッショナー国際会議（2010年10月イスラエル・エルサレム開催）においてプライバシー・バイ・デザインが「基本的なプライバシー保護の不可欠な要素として認識」されることが決議されており、EUにおけるEUデータ保護指令の規則化案“General Data Protection Regulation（一般データ保護規則案）”（2012年1月）、米国・連邦取引委員会（FTC）における”Protecting Consumer Privacy in an Era of Rapid Change：Recommendations For Businesses and Policymakers”（2012年3月）などで取り入れられている。わが国では、個人情報保護法改正を視野に入れ、総務省による「パーソナルデータの利用・流通に関する研究会報告書」等で提示されている。

こうしてみると、PIAをその入り口として、最終的にはプライバシー・バイ・デザインによる事業やサービスの企画、情報システムの構築を行うことが重要であることがわかる。各種法制度や国際的な基準とPIAの結果をインプットとして実施する、民間企業のビジネスを対象としたプライバシー・バイ・デザインのイメージを図表3-3に示す。



図表3-3.プライバシー・バイ・デザインの実施イメージ

このときPIAによって洗い出されたリスクをコントロールし、パーソナルデータの不正な収集、利用および漏えいを防ぎ、その情報を個人が管理することができるようにし、情報システム上でのプライバシー保護を強化するために利用される技術が、プライバシー保護技術（Privacy-Enhancing Technologies（PETs））である。たとえばクッキーによる追跡を拒否するツールや、個人を識別できないようにする暗号化技術、人物の画像を抽象化して個人の識別・特定ができないようにする技術等がある。また漏えいを防止するための一連のセキュリティ対策技術も広義にはPETsであると言ってよいだろう。

4.情報の活用とプライバシーの共存をめざして

PIAは従来、政府機関の行政サービスやシステムを主な対象としていたため、現行の枠組みは企業の実際のビジネスに対する影響度が、あまり考慮されているように見えない。もちろん個人のプライバシーを保護することがPIAの本来の目的であるから、それは当然のことである。しかし、法制度で義務付けられていない、任意で行う事前アセスメントである以上、企業側に何らかの利益が還元されないと、その実施は難しい。過去に行われてきた情報セキュリティ対策と同じように、企業にとっては単なる「コスト」として削減の対象になり、十分な投資を行えない可能性もあるだろう。それでは産業の発展につながる新しいサービス等の構築に、積極的に寄与できない。

そこで従来のPIAとプライバシー・バイ・デザインに対して、プライバシーに関連した事業リスクの評価手法を加えて拡張・発展させることで、事業を安全に成功・発展させるための有効なメソドロジーとして活用できるようにすること、が望まれるのである。

ⅰ 筆者による抄訳

ⅱ「Privacy Impact Assessment ：The Privacy Office Official Guidance」
（http://www.dhs.gov/privacy-compliance）

ⅲ 2014年10月時点。

ⅳ「PIPEDA Self-Assessment Tool」
（http://www.priv.gc.ca/information/pub/ar-vr/pipeda_sa_tool_200807_e.asp#）

ⅴ 内閣府が運営するWebサイト「持続可能な未来のためのマルチステークホルダー・サイト」（http://sustainability.go.jp/index.html）を参照されたい。

関連文献：

1.高度情報通信ネットワーク社会推進戦略本部「パーソナルデータの利活用に関する制度見直し方針」（2013年12月20日）
2.高度情報通信ネットワーク社会推進戦略本部「パーソナルデータの利活用に関する制度改正大綱」（2014年6月24日）
3.経済産業省「パーソナルデータ利活用ビジネスの促進に向けた、消費者向け情報提供・説明の充実のための「評価基準」と「事前相談評価」のあり方について」（2014年3月26日）
4.経済産業省「消費者向けオンラインサービスにおける通知と同意・選択のためのガイドライン」（2014年10月17日）
5.経済産業省「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」（2014年5月16日・9月26日）

4 民間企業におけるPIAの必要性について

JIPDEC マイナンバー対応プロジェクト室　室長　関本　貢

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（平成25年法律第27号、以下、「番号法」という。）」の施行に伴い、2015年10月から国民一人ひとりに対して固有の12桁の個人番号が付与されて通知が始まり、2016年1月から利用が開始される。個人番号は当面の間、社会保障・税・災害対策の分野での利用に限られてはいるが、これらの分野に関する個人の情報がこの番号と関連付けられることによって、国や地方自治体における事務の効率化、社会保障や税の給付と負担の公平化、国民に求められる各種届出等が一本化される等の利便性向上の効果が期待されている。一方、個人番号によって国民の情報が紐付けされることから、情報管理の一層の強化が求められ、国や地方自治体における個人番号を利用する事務システムには、情報セキュリティ対策を事前に評価する「特定個人情報保護評価（Privacy Impact Assessment、以下、「PIA」という。）」の実施が義務付けられている。

民間事業者においても、個人番号は法律に基づいて義務化されている従業者の給与支払いに関する給与所得の源泉徴収票の作成、厚生年金保険被保険者資格取得届の作成等事務（個人番号関係事務）に利用することになり、国等と同等に厳正な個人番号の取扱いが求められることになる。

ここでは、番号法の施行によって個人番号を利用する民間事業者におけるPIAの必要性について概観する。

2.個人番号の利用

個人番号は国や地方自治体等が保有している社会保障や税に関する個々人の情報と関連付けられることになることから、個人番号によって当該本人に係る情報を容易に参照したり利用したりすることができる反面、そのことを悪用することによって不正に持ち出されたりして個人のプライバシーの権利利益を侵害する危険性も内在している。

そのために、国や地方自治体等に対しては、個人番号を含む個人情報（特定個人情報）を取り扱うに先立って、対象事務およびその事務を支援する情報システムについて、プライバシーの権利利益の保護に配慮していることを評価するPIAを実施し、その結果である特定個人情報保護評価書を国民に公表することとなっている。

一方、個人番号は国や自治体等の利用にとどまらず、民間事業者においても従業員等に関する給与支払い、健康保険、雇用保険、年金などに関して国等に提出する事務（これを「個人番号関係事務」という。）の際に書面に従業員等の個人番号を記載する必要があることから、国や地方自治体等と同様に従業者等のプライバシーの権利利益の保護に配慮しなければならない。

分野	事務
社会保障分野	厚生年金保険被保険者資格取得届の作成
	雇用保険被保険者資格取得届の作成
	健康保険被保険者資格取得届の作成
税分野	源泉徴収票の作成
	退職所得の源泉徴収票の作成
	報酬、料金、契約金および賞金の支払調書の作成
	配当、剰余金の分配および基金利息の支払調書の作成
	不動産の使用料等の支払調書の作成
	不動産等の譲受けの対価の支払調書の作成

図表4-1.民間事業者の個人番号の利用（個人情報関係事務）

3.PIAの必要性

個人番号は、個人に関する各種情報と関連付けられて利用される。そのため、個人番号によって当該本人の各種情報に容易にアクセスすることを可能とすることから、利便性の向上が期待されているところである。このことは、言い換えると、社会保障・税・災害対策の分野に関する個人情報を取り扱う情報システムが、情報セキュリティの脅威にさらされる状況下に置かれていると、個人番号をキーとしてすべての個人情報が白日の下にさらされることになる危険な面を持っているということになる。

したがって、番号法においては、全国民・住民に関する詳細な情報を管理している国・地方自治体に対して、PIAの実施義務を定めている。

PIAは、特定個人情報を取り扱う事務やその事務に用いる情報システムに十分なリスク対策が講じられているかについて、特定個人情報の利用に先立って評価し、プライバシー等の権利利益に配慮できていることを確認する行為である。

一方、民間事業者における個人番号の利用は、現時点では限定的ではあるものの、将来的にはその利用範囲が拡大することが想定されており、従業員情報との関連付けがより広範囲になるものと考えられることから、番号法によってPIAの実施義務が課せられてはいないものの個人番号の取扱いに慎重さが求められる。

また、番号法においては、違反した場合の罰則規定が「個人情報の保護に関する法律（平成15年法律第57号。以下、「個人情報保護法」という。）」に比べ格段に重くなっていることから、この点でも、特定個人情報の取扱いへの慎重な対応・準備の必要性を認識しておかなければならない。

3-1　民間事業者の新たな義務

民間事業者は、個人情報の取扱いに関しては個人情報保護法に適合した取扱いが義務付けられているが、番号法は、個人情報保護法が求めている措置の特例（上乗せ）として厳格な保護措置を定めており、この点でも民間事業者は特定個人情報の取扱いに新たな義務が生じたことを認識しなければならない。

特例の主なものの例として次に示す。

－特定個人情報の利用制限

利用目的の範囲内であれば利用することができる（個人情報保護法第16条）が、社会保障、税および災害対策に関する特定の事務に限定（番号法第9条）されており、また、必要な範囲を超えた特定個人情報ファイルの作成が禁止されている（番号法第28条）。

－本人の同意があった場合でも、利用目的を超えた特定個人情報の利用を禁止

利用目的を超えて個人番号を利用する場合は、利用目的を変更するのではなく、改めて利用目的を特定、明示等した上で、個人番号の提供を求めなければならない。（番号法第 29条第3項により読み替えて適用される個人情報保護法第16条第1項、番号法第32条）

－特定個人情報の提供の制限

特定個人情報は限定した範囲でしか提供（番号法第19条）、収集・保管（番号法第20条）してはならず、本人から個人番号の提供を受ける場合には、本人確認が義務付けられている（番号法第15条）。さらに、提供を受けることが認められている場合（番号法第19条）を除き、他人に対して個人番号の提供を求めることを禁止（番号法第15条）している。

－個人番号に対する安全管理措置

個人情報保護法は個人データに関して安全管理措置を求めているが、番号法では個人番号についても安全管理措置義務が課せられる（番号法第12条）。

3-2　民間事業者向けの番号法ガイドラインの公表

番号法を所管する特定個人情報保護委員会は、2014年10月に民間事業者向けに、特定個人情報の取扱いに関する「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）（案）」（以下、「事業者編ガイドライン」という。）を公表した。

事業者編ガイドラインは、個人番号を取り扱う事業者が、特定個人情報の適正な取扱いを確保するための具体的な指針として定められており、この定めに従わなければならない事項(「しなければならない」および「してはならない」と記述)と、「望ましい」事項からなっている。従わなければならない事項に反した場合は、法令違反と判断される可能性がある。「望ましい」事項についても、可能な限り対応することが望まれるとされている。

以上のように、民間事業者においても事業者編ガイドラインによって厳格な個人番号の取扱いが求められていることから、社内の個人情報を取り扱う情報システムについて、情報セキュリティリスクを踏まえた保護措置を講じることが求められていると理解すべきである。

現在の給与事務、法定調書作成等の事務に関するルールおよび情報システムは個人番号の導入を前提としていないことから、導入後の姿を想定したシステムの改修等を実施しなければならない。その際、事業者編ガイドラインによる措置に対応できていない部分はどこかを明確にし、適用できるようにするためにはどのようにすればよいかを確認しておくことが重要である。

PIAは、あらかじめ特定個人情報の取扱いがルールおよび情報セキュリティリスクに対応できているかを確認し、必要な措置を事前に講じるための有効な手段として認められている。

番号法対応を図る際、対象事務はどのように変わるのか、それによって新たに発生するリスクは何かを認識して対応策を構築することになるが、これらの一連の作業はPIAの考え方に沿うものである。

先にも述べたとおり、民間事業者にはPIAの実施が義務付けられてはいないが、番号法への適合のためのツールとしてPIAを導入して対応することは意味のあることといえる。

4.おわりに

JIPDECでは、民間事業者の個人情報保護マネジメントシステムを評価し認証するプライバシーマーク制度を運用しているが、認証にあたっての重要なポイントは、マネジメントの対象である個人情報を取り扱う情報システムおよび運用手続きが、個人情報保護法およびJIS Q 15001(個人情報保護マネジメントシステム－要求事項)に反する取扱いをする可能性(リスク)を特定して、その対応策を適正に構築し運用できているかを確認して評価することにある。

プライバシーマーク認証の活動は、事前の評価を求めるPIAとは実施するタイミングの面で異なるものの、対象の情報システム等が個人情報の取扱いリスクに対応できているかを確認・評価することにおいては同等であるとの認識を持っている。

すでに1万3,000を超えるプライバシーマーク認証事業者は、個人情報の取扱い上のリスクを踏まえた対策を構築し運用する仕組みができていることから、先に示した番号法による特例となる事項を取り込むことによって、比較的容易に番号法に対応することができるといえる。プライバシーマーク認証においても、番号法を踏まえた検討を行っているところである。

これらのことから、民間事業者が番号法施行に向けた対応として、特定個人情報保護の取扱いに限定したPIAの導入も効果的であるものの、自組織で取り扱う個人情報のすべてを対象とした個人情報保護マネジメントシステムの認証を受けることで番号法対応が確認でき、PIAと同等以上の対外的なPR効果を望めることができることから、プライバシーマーク認証取得を番号法対応の選択肢とすることも有効であると考える。

プライバシーマークの知見と経験を活用して、JIPDECでは2014年から地方自治体が実施したPIAの結果である特定個人情報保護評価書について適正に評価されているかを点検するサービスを提供しており、この経験を踏まえ、プライバシーマークに連動した対応に加え、民間事業者が実施したPIA結果の点検の要請にも応じることができるよう準備を進める予定である。

〈資料〉 情報化に関する動向（2014年4月～2014年9月）

2014年4月

国内

- ワコール、不正アクセス攻撃を受け、すべてのWebサイトを約1か月間閉鎖。
- WindowsXPサポート終了に向け、最後の更新プログラムWindows Updateを公開。1年間提供。
- 「.tokyo」ドメインが運用開始。「.nagoya」に次いで2番目。
- 税制調査会、マイナンバーを銀行の預金口座に結び付ける方針を公表。
- Googleの無料メール共用サービス「Google Group」を使って空港平面図が閲覧可能に。ネット上で誰でも見られる設定にしていたことが原因。
- 警察庁、オープンSSLの欠陥攻撃が1週間で約4万4,000件を超したと発表。
- 総務省情報通信政策研究所調べ、モバイルユーザのスマホ利用率が初めて過半数超え。10代のSNS利用率がメールと逆転。
- 国立国会図書館、著作権満了の蔵書のオンデマンド販売サービスを開始。
- 電子書籍の普及とインターネット上の海賊版対策として、電子出版権を創設する著作権法の一部を改正する法律が4月25日付で成立、2015年1月施行。
- パナソニック、同社運営の会員サイト「CLUB Panasonic」で約7万8,000件の不正ログイン発覚。
- 千葉大学、4万7,000人の学生情報がインターネット上で閲覧可能に。適切なセキュリティ設定なしのPCでのネット接続が原因。
- JIPDEC、世界初の制御システムのセキュリティマネジメントシステム（CSMS）認証制度始動。三菱化学エンジニアリングと横河ソリューションサービスが認証取得。
- JavaのWebアプリケーションフレームワーク「Apache Struts」の脆弱性の影響で国税庁の確定申告書作成サービス停止や国家試験「ITパスポート試験」中止に。

海外

- Gartner調査、2014年の世界IT支出額は3兆7,710億ドルと予測。クラウド、モバイル端末関連投資が原動力に。
- AppleとSamsung間でモバイル特許を巡る新たな裁判がカリフォルニア州で開始。
- トルコ政府、エルドアン首相周辺の汚職情報をめぐり、違法リンクの削除要請にTwitterが拒否したことに対する措置で、3月から行っていたTwitterへのアクセス遮断を2週間ぶりに解除。
- 欧州議会、インターネット、モバイル関連法の全面的改革案を可決。コンテンツやプロバイダに関係なくすべてのトラフィックが平等に扱われ、エンドユーザも企業も公平な扱いが受けられるように。
- TLSやSSLを利用するためのライブラリ「OpenSSL」に情報漏えいの脆弱性が見つかり、カナダ、英国、日本で「Heartbleed（心臓出血）」脆弱性を突いた攻撃による情報漏えい被害が発生。
- 欧州連合（EU）司法裁判所、通信会社などに通話や電子メール送受信の記録保存を義務付けた「通信データ保存指令」がEU基本憲章が定める「私生活の尊重と個人情報保護という基本的権利を侵害する」として無効と判断。加盟国に是正措置を命じる。
- 米国の2013年インターネット広告市場調査、初めてテレビ広告を上回り、売上高が428億ドルに。特に伸び率が高かったのはモバイル広告。
- OECD、消費税グローバルフォーラムにおいて、国境を越えた取引に消費税を課すことを国際指針としてとりまとめた。
- Microsoft、Nokiaの携帯電話事業を買収。

2014年5月

国内

- ソニー、パソコン事業から撤退。「VAIO」は新会社で引き続き製造・販売へ。
- 3Dプリンタを使って銃を製造・所持した大学職員を銃刀法違反容疑で逮捕。
- IT総合戦略本部分科会、マイナンバー制度の利用制限をカルテ情報の管理、戸籍業務などにまで範囲を広げるよう、提言をまとめる。
- 他人のPCを遠隔操作し、電子掲示板を介してテロ、殺人等の犯罪予告を行ったPC遠隔操作事件、無実を訴えていた被告が自作自演を認め、保釈取消しに。
- MM総研調査、国内PC出荷台数が過去最高の1,651万台に。WindowsXPのサポート終了に伴う更新需要が影響。
- Yahoo! Japan、自社のウェブ閲覧履歴とカルチュア・コンビニエンス・クラブ（CCC）のTカード購入履歴情報を相互提供開始。
- JIPDEC、「PRIVACY BY DESIGN …TAKE THE CHALLENGE(日本語訳)」 Ver1.0（仮訳）を発表。
- 無線LANビジネス推進連絡会、大規模災害発生時に公衆無線LANを無料で開放するためのガイドラインで世界初の災害用統一SSID「00000JAPAN」制定。
- 松本商工会議所、JIPDECのJCAN証明書を利用したセキュリティツールを組み込んだタブレットを使い、会員向け経営相談を開始。

海外

- Apple、米国内の法執行機関やその他政府組織から求められるユーザ情報の開示に関する新ガイドライン公開。米国外の現地法人に対する要請には不適用。
- 環太平洋戦略的経済連携協定（TPP）、音楽、小説の著作権保護期間を70年に統一することで合意。
- EU司法裁判所、「忘れられる権利」を行使し、Googleに対し、検索結果の削除要請ができるとの判決を下す。
- AppleとGoogle、スマホ技術の特許侵害訴訟で和解。これまでのすべての訴訟を取り下げ、特許改革に向けた相互協力で合意。
- 米司法省、中国人民解放軍当事者5名を、サイバー攻撃により企業機密情報を盗んだとして起訴。
- 中国政府、Windows8を使用禁止に。
- 米eBay、サイバー攻撃により顧客情報漏えい。1億4,500万人にパスワード変更を要請。
- 米Strategy Analytics調査、中国の2014年携帯電話売上金額が約870億ドル。米国市場を上回る見通し。
- Google、「忘れられる権利」の認定判決を受け、欧州での検索結果の削除要請を受け付けるサービスを開始。

2014年6月

国内

- 情報通信研究機構(NICT)、世界初のレイア3スイッチにネットワーク機器の位置情報を自動的に割り当てる新世代ネットワーク技術「HANA」を実装。
- JIPDEC、サイバー空間で信頼・信用できるビジネス環境の整備にJCAN、ROBINSを活用している企業に対する「あんしんかんベストプラクティス2014」を発表。
- NICT、世界初の量子鍵配送装置からの安全な鍵(共通乱数)をスマホに転送・保存して個人データへのアクセス権設定とデータの安全保存を可能とするシステムの開発に成功。
- イー・アクセスとウィルコムが合併して新会社「ワイモバイル」に。
- 政府、原子力施設へのサイバーテロ対策強化のため、関係省庁、企業による合同訓練を実施。
- 政府、ビッグデータ活用促進のルールを盛り込んだ個人情報保護法改正の大綱案を発表。「特定個人情報保護委員会」を改組し、独立の第三者機関がビッグデータ活用ルールの適切な運用をチェックできる体制を設ける。
- 経済産業省、ビッグデータの活用を推進する「データ駆動型(ドリブン)イノベーション創出戦略協議会」創設。
- 改正薬事法施行。市販薬のネット販売ルールが規定され、一般用医薬品のほとんどがネット販売解禁に。
- 富士通研究所、世界最速のデータ受信回路を開発。
- NTTドコモ、スマホやタブレットにかざすだけで回線を認証する「ポータブルSIM」を開発。SIMカードが入っていない端末での通話やメール機能が利用可能に。
- トレンドマイクロ調査、ウェブサービスで同一パスワードの使いまわしが9割を超す。
- QRコード開発チーム、欧州特許庁(EPO)が付与する欧州発明家賞を受賞。開発20年間の活動実績により幅広い地域・年代の一般消費者に利用されていることが評価される。
- グラフ理論に基づく大規模データ解析性能を競うGraph500、理研の「京」が初の首位獲得。
- 地方公共団体情報システム機構(J-LIS)、運営管理する住基ネットシステムの操作担当者の認証に富士通の手のひら静脈認証装置「パームセキュア」を採用。

海外

- McAfeeと戦略国際問題研究所(CSIS)調査、サイバー犯罪が世界経済にもたらす損失は年間4,450億ドルと予測。特に知的資産の損失が深刻化。個人情報漏えいを原因とする損害は世界で1,600億ドルに。
- スパコンの演算性能を集計するTOP500プロジェクト、中国国防科学技術大学(NUDT)の「天河2号」が2012年から引き続き首位に。理化学研究所の「京」は第4位。
- 米連邦取引委員会(FTC)、中国C.T.S Technologyに対し、電波妨害装置を米国向けに販売したとして、過去最高額の約3,500万ドルの罰金、および違法な電波妨害装置の販売禁止などを命令。
- 米BSAとIDCによる2013年国際調査、中国のソフトウェア不正使用率は74%、不正総額は約87億ドルと、金額ベースでは米国に次いで第2位に。
- 米最高裁、米ビデオストリーミングサービス会社Aereoに対し、番組のネット有料配信は、著作権侵害にあたると判断。放送会社側が勝利。
- 国連経済社会局(UNDESA)の電子政府世界ランキング。日本は「世界最先端IT国家創造宣言」でのオンライン申請によるペーパーレス化の目標設定が評価され、2012年の18位から6位に躍進。首位は3期連続で韓国。

2014年7月

国内

- 世界で最も省エネなスパコンを評価する「Green500」で日本の「TSUBAME-KFC」が2013年11月に引き続き首位に。
- ベネッセコーポレーション、システム子会社の派遣社員による顧客情報持出し、売買で、最大約2,070万件の顧客情報漏えいの可能性。
- 内閣官房情報セキュリティセンター(NISC)、2013年度のサイバー攻撃は約508万件、前年度の約5倍に急増。特定組織や個人を狙う「標的型攻撃」も高度化。
- オムロングループ会社、JR東日本の画像情報をJRに無断で研究に流用。
- 総務省の2014年版「情報通信白書」、ビッグデータ活用で、国内全産業の売上高が60.9兆円押上げと推計。
- 情報処理推進機構(IPA)、標的型サイバー攻撃対策支援のためのサイバーレスキュー隊を発足。
- 全国銀行協会、適切な安全対策を講じている企業がインターネットバンキングの不正送金被害に遭った際の補償対象判断のための指針を発表。
- IDC調査、「ビッグデータ」の認知度は56.5%と、前年比23ポイント増。ビッグデータをマーケティング強化目的に活用する企業が42.7%と最多。

海外

- Facebook、事前の予告なしに投稿情報を選別した心理実験を行ったとして、英情報保護機関(IOC)が違法行為の有無を捜査。米電子プライバシー情報センター(EPIC)がFTCに提訴も。
- Gartner調査、世界の端末出荷で2015年にタブレット出荷がPCを抜くと予測。
- Intel、身の回りの機器をネットワークで接続する「モノのインターネット(IoT)」分野の接続性向上に取り組むコンソーシアム"Open Interconnect Consortium(OIC)"を設立。スマホやオフィス分野の機器の接続や認証技術の共通化に取り組む。
- FTC、未成年がゲーム購入後、パスワードなしで仮想通貨を購入できるシステムに問題ありとして、Amazonを提訴。
- Google、「忘れられる権利」による削除基準を話し合うための独立の諮問委員会を設置。
- Microsoft、「忘れられる権利」対応のリンク削除依頼ツールを設置。
- 欧州中央銀行(ECB)、システムの脆弱性を悪用されてWebサイト登録者のデータが流出。
- 米連邦地方裁判所、Microsoftに米国外のサーバに保存する顧客の電子メールのデータ提出を命令。異議を唱えているMicrosoftは上訴を表明。

2014年8月

国内

- 電子情報技術産業協会(JEITA)と日本画像医療システム工業会(JIRA)、保健医療福祉情報システム工業会(JAHIS)、医療・ヘルスケア用ソフトウェアの安全性確保のための「ヘルスソフトウェア推進協議会」を設立。
- 日本国内に事業拠点を持つ金融機関が標的型攻撃、フィッシング詐欺、不正送金など、サイバー攻撃に関する情報共有のための組織「金融ISAC」を設立。
- 経済産業省、「電子商取引及び情報財取引等に関する準則」を改訂。BtoC電子契約時の消費者の操作ミスによる錯誤等を修正・追加。
- 常陽銀行、フィッシング詐欺対策の一環として、JIPDECと協力して正規ドメインからの発信であることが一目でわかるなりすましメール防止「安心マーク」をメルマガ配信に導入。
- 警察庁調べ、ネットオークション詐欺被害が急増。前年同期の2倍の1,560件。
- JR東日本のSuicaポイントクラブ、29万6,000件のログイン試行を確認し、756件の不正ログイン被害が発覚。
- Facebook、飲食店の中傷書き込みに対する発信者情報開示を求める仮処分申立てにより、東京地裁からIPアドレスなどの開示命令を下される。Facebookへの開示命令は初めてのケース。
- トレンドマイクロ調べ、2014年第2四半期の国内外のなりすましによる不正ログイン数が過去最高に。ネットバンキングからの不正送金のためのウイルスは世界中で日本が最も蔓延。
- 京都市、ICTを活用した効率的な都市交通をめざし、「京都未来交通イノベーション研究機構」設立。ビッグデータ解析による快適な移動環境の整備を目指す。
- 国立情報学研究所(NII)、ビッグデータをクラスタ別に分類し解析しやすくする「データ研磨」手法を開発。
- 経済産業省、電子商取引に関する市場調査結果発表。国内BtoC市場規模は11.2兆円と、前年比17.4％増。
- トレンドマイクロ調べ、スマートデバイスの業務利用で、BYODを禁止している企業の従業員の63.1％が個人所有デバイスを業務利用。
- IPA、「ウェブサイト改ざんの脅威と対策」を公開。水飲み場型攻撃などの改ざん手口に対し、サイト構築・運営者がどのような対策を講ずべきかを整理・解説。

海外

- オバマ大統領、SIMロック解除合法化法案に署名。通信キャリアの乗換えが可能に。
- Apple、電子書籍価格をめぐる集団訴訟で4億5,000万ドルを支払う和解案を仮承認。
- AppleとSamsung、日本を含む米国外での特許訴訟取下げに同意。
- Wikipedia、「忘れられる権利」で削除された記事の一覧を掲載することで、EUの方針に対抗。
- 米病院チェーンのCommunity Health Systems、マルウェア攻撃により患者約450万人の個人情報流出。
- 米原子力規制委員会(NRC)、過去3年間で3回のハッキング被害に遭い、2回は内部資料にアクセスされていたことを公表。
- Facebook、Webセキュリティ強化のための「Internet Defense Prize」制度創設。インターネット上のユーザ保護、攻撃防御に対する研究が対象に。
- Gartner、2014年の世界全体の情報セキュリティ支出は前年比7.9％増の約711億ドルの見通し。大中華圏の情報セキュリティ支出の伸び率が2014年末までにアジア太平洋地域で最大になると予測。
- 米物流大手UPS、代理店がマルウェア感染被害を受け、顧客情報流出の可能性。
- 韓国、2,700万人分の個人情報2億2,000件が流出。情報を不正に利用して利益を得ていた16人が逮捕。

2014年9月

国内

- 全国の空港で、旅客機離着時に機内モード設定での電子機器の使用が可能に。
- 警察庁調べ、2014年上期のインターネットバンキング不正送金被害額は約18億5,200万円。前年同期比の約6倍に。法人名義口座の被害急増。
- ベネッセコーポレーション、システム子会社の派遣社員による個人情報売却件数は約3,504万件に。再発防止策として、セキュリティ企業のラックと10月末に共同出資会社設立。顧客に対する500円の補償やこどものための基金設立を発表。
- JR東日本の会員サイト、約1,152万件の不正アクセスを受け、約2万件の不正ログイン発覚。
- 法務省、民事局と法務局保有のサーバに不正アクセス被害。
- 全国銀行協会、2014年7～8月のインターネット不正送金被害が2億9,000万円と発表。
- IPA、増発する内部不正による機密情報漏えいの発生を防ぐため、「組織における内部不正防止ガイドライン」を改訂。
- ヤマト運輸、会員サービスサイトで、約1万人の不正ログイン発覚。
- 日本航空、ウイルス感染の社内PCを経由して最大約21,000件のマイレージ会員の情報が、悪意のある海外の外部サーバに送信されていることが判明。

海外

- 中国国家工商行政管理総局(SAIC)、独占禁止法に抵触する可能性から、MicrosoftにWindowsとOfficeの互換性等に関する説明を要求。
- 米連邦地方裁判所、Microsoftに対し、米国外での保存メール提出命令の執行停止を解除。ただしMicrosoftは命令に従わず。
- バングラデシュ人民共和国で「情報処理技術者試験」制度導入。「アジア共通統一試験」を実施するための協議会(ITPEC)への正式加盟により、「アジア共通統一試験」がアジア7か国で実施。
- 複数の米著名人のアカウントが標的型攻撃に遭い、AppleのiCloud上のプライベート写真がネット掲示板に流出。Appleはセキュリティ対策を強化。
- 世界経済フォーラム(WEF)の国際競争力ランキング発表。日本は9位から6位にアップ。首位は6年連続でスイスに。
- Google、「忘れられる権利」による削除要請への対応について、諮問委員会による公開ミーティングを欧州7都市で開催。
- IBM、人工知能型コンピュータ「Watson」を使ったビッグデータ分析がスマホで簡単に分析可能に。
- 米ホームセンターHome Depot、サイバー攻撃被害で顧客の約5,600万枚のカード情報流出。

JIPDEC IT-Report 2014 Winter
2014年12月15日発行（通巻第4号）
発行所　一般財団法人日本情報経済社会推進協会
〒106-0032　東京都港区六本木1-9-9　六本木ファーストビル12階
TEL：03-5860-7555　FAX：03-5573-0561
制　作　開成堂印刷株式会社