

令和 2 年改正個人情報保護に関する法律施行令（案）および施行規則（案） に対する意見

経営法友会

はじめに

令和 2 年改正個人情報保護法により、個人情報の一層の保護を図るとともに、事業者が利活用しやすくなる仕組みを構築する枠組みが整備されたこととなるが、具体的な実務運用にあたっては、政令・規則、さらに今後示されるガイドライン・QA の内容が重要となることはいうまでもない。

今回示された政令案・規則案については、全体としては異存ないものの、いくつかの論点で、改正大綱と齟齬がある、政令案・規則案で規定されていない、規定があっても必ずしも趣旨が明らかになっていない、具体的な基準が不明確であるなど、実務上支障をきたす内容となっていることから、以下、具体的に述べる。

また、平成 27 年個人情報保護法改正によって、いわゆる 5000 件要件が撤廃され、中小事業者を含め広く事業者に適用される法令となったことに鑑みると、すべての適用事業者が運用の際に判断に迷うことなく、実務上過度な負担を負うことなく本政令・規則を遵守することができる内容となるよう、配慮されたい。

なお、令和 2 年個人情報保護法改正にあたって、衆議院内閣委員会および参議院内閣委員会それぞれが、「国民及び個人情報取扱事業者に分かりやすいものとなるよう、消費者や事業者等多様な主体から広く丁寧に意見を聴取」すべきと付帯決議で述べている。今回のパブリックコメント手続は、かかる付帯決議に反するのではないかという疑念もあり、今後示される予定のガイドライン案や QA 案のパブリックコメント手続の際には十分な期間を設けるよう強く要望する。また、当会のみならずすべてのコメントの 1 つひとつについて、パブリックコメントの結果において丁寧に回答されたい。

1 漏えい等報告・本人通知

(1) 報告対象（規則案 6 条の 2）

ア 規則案 6 条の 2 全般

- ① まず、「個人の権利利益を害するおそれ大きいものとして個人情報保護委員会規則

で定めるもの」(個人情報保護法 22 条の 2 第 1 項)には個人データの漏えい等の「発生したおそれがある事態」は含めず、現に「発生」した場合のみ含まれるという制度設計を検討されたい。

また、もし仮に、漏えい等の「発生」に限らず、「発生したおそれがある事態」も「個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定めるもの」(法 22 条の 2 第 1 項)に該当するという制度設計をする場合であっても、漏えい等をしたことが相当程度の蓋然性をもって確認できた場合にのみ個人情報保護委員会への報告および本人への通知の義務が発生するという制度設計にされたい。

すなわち、事業者においてはいかなる事案でも漏えい等が「発生したおそれ」を否定することは難しいため、「おそれ」があるのみで報告・通知義務が発生するならば事業者の負担が大きく増大してしまうためである。

② 次に、報告・通知義務が発生する場合の判断を事業者が行うのに資するべく、報告・通知義務の有無を判断する際の指標となるような例を公表されたい。

とりわけ、規則案第 6 条の 2 各号のように「個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定めるもの」(法 22 条の 2 第 1 項)に「発生したおそれ」も含めるのであれば、現行の「個人データの漏えい等の事案が発生した場合等の対応について」(平成 29 年個人情報保護委員会告示第 1 号) 3(2)に「報告を要しない場合」として報告不要の例示を記載しているように、文言の形式的な解釈上では報告義務が発生するに見えるものの、義務が生じない事例を具体化して、判断の際の基準となるような例示を明らかにするべきと考える。

③ 上記告示 3(2)に記載のある「報告を要しない場合」に該当する場合には、改正法施行後においても報告を要しない旨を明記されたい。告示に記載のような事例は多くの事業者で少なからず発生するものであり、これらをすべて個人情報保護委員会が把握することは、報告制度の趣旨からすると必要性が低く、かつ、中小事業者も含む事業者側にも過度の負担を強いるものと考えられる。

イ 「漏えい等」の意義(法 22 条の 2、規則案 6 条の 2)

従前は努力義務であった漏えい等報告が法律上の義務となったことを踏まえ、とりわけ以下の点に留意しつつ、「漏えい等」の意義を明確にされたい。

- ① 「毀損」には、事業者が合理的な理由をもってデータを物理削除することは含まれないこと
- ② 「滅失若しくは毀損」したが、「漏えい」は発生していないことが確実である場合に

は、報告義務が発生しないこと

上記②につき補足すると、たとえば、要配慮個人情報を含む個人データが記録されているエクセルファイルを不注意で削除してしまった場合、規則案の文言どおりでは「滅失若しくは毀損」に該当することになる。しかしこの場合、「漏えい」しているわけでもなく、「委員会が事態を早急に把握し、必要な措置を講じることができるようにする」（個人情報保護委員会「改正法に関連する政令・規則等の整備に向けた論点について（漏えい等報告及び本人通知）」〔令和2年10月30日〕2頁）という報告制度の趣旨からしても個人情報保護委員会に報告する必要性が乏しい。

ウ 「高度な暗号化その他の個人の権利利益を保護するために必要な措置を講じたもの」（規則案6条の2第1号）

① 「高度な暗号化そのほかの個人の権利利益を保護するために必要な措置を講じ」ている場合には規則案6条の2第1号のみならず、2号ないし4号のいずれの漏えい等でも、報告義務の対象から除かれる（規則案6条の2第1号の「以下この条……において同じ。」）ことが一読して判別できるような条文の構造にされたい。

② 会社貸与のスマートフォンやPCを外出が多い業務の部員が紛失した際には、取引先の業務上のメール・アドレス帳等で何人の情報が紛失時に保存されていたかが確認できないこともある。そのような場合であっても、つど個人情報保護委員会に報告するという扱いでは、事業者の負担が大きいのみならず、個人情報保護委員会にとっても、国として事態を把握する必要性が高くない事態の報告が殺到することが予想される。そこで、会社貸与のスマートフォンやPCの紛失事例について、十分なセキュリティ上の措置がされている場合には、「高度な暗号化その他の個人の権利利益を保護するために必要な措置を講じたもの」に該当し、報告・通知義務を負わない制度設計にされたい。

エ 要配慮個人情報の漏えい等（規則案6条の2第1号）

漏えい等をした「おそれ」がある個人データに1件でも要配慮個人情報が含まれている「おそれ」があれば、規則案6条の2第1号に該当するのだとすれば、要配慮個人情報が含まれているおそれがないことが確実でない限り、漏えい等のおそれがあれば、ただちに同号の適用があるものと事業者としては判断することにもなりかねない。しかし、それでは、1000人という閾値を定めた同条4号の趣旨が滅却される。そこで、同条1号が適用されるのは、相当数の要配慮個人情報が漏えい等した場合に限られるべきである。少なくとも、事業者としては、要配慮個人情報が含まれることを確認していない段階においては、同号は適用されず、2号から4号に従って報告の要否を判断すれば足りることを明記されたい。

オ 財産的被害が発生するおそれがある場合（規則案6条の2第2号）

どのような個人情報の漏えいであっても、その使い方によっては、財産的被害につながる「おそれ」はありうるため、規則案6条の2第1号、3号、4号のいずれに該当せずとも2号には常に該当することになりかねない。これでは、1号、3号、4号をあえて設けた趣旨が減却される。そのため、2号の外延を以下の点に留意しつつ明確にされたい。

① 規則案では、6条の2第1号に該当すれば2号にも該当し、1号と2号との違いが不明確に思われる。たとえば、要配慮個人情報の1つである、「病歴」（法2条3項）は、仮に、本人が就職活動をしている場合に事業者が内定を与えるかどうか判断する過程で「不正に利用」すれば、本人は就職できず給与や福利厚生を受けられないという「財産的被害が生じるおそれ」があるし、就職できても「病歴」を理由に昇進できないという差別的待遇を受けることにより、昇給を受けられないという「財産的被害が生じるおそれ」がある。また、同じく「病歴」を例に挙げれば、保険会社が「不正に利用」することで本人が生命保険に不当に加入できない、加入できても不当に保険料が高くなる、住宅ローンが不当に借りられず住宅を購入できなくなるといった「財産的被害が生じるおそれ」があることは否定しきれないと思われる。そこで、たとえば、「不正に利用されることにより財産的被害（預金の引き出し又は代金の決済等による金銭の損失をいう。）」というように、2号の適用範囲・意義を明確にされたい。

② 「財産的被害が生じるおそれがある個人データ」の内容が不明確である。規則案6条の2第2号の条文上に「クレジットカード番号」といった具体例を含ませることで明確にされたい。なお、クレジットカード番号が「漏えい等」したものの、「0000-1111-3333-4444」といった番号のみが流出し、その番号がクレジットカード番号であるという事実自体は「漏えい等」していない場合も、規則案6条の2第2号に該当するのかが明確にされたい。

カ 不正アクセス等故意によるもの（規則案6条の2第3号）

① 企業として、漏えい等したことは明らかであるが、それが不正の目的によるものなのかどうかはただちにわからない場合が多い。そうであるにもかかわらず、不正な目的をもって行われた「おそれ」がある漏えい等が発生した「おそれ」があるだけで報告義務があるとするのであれば、漏えい等の懸念がある限り、すべての事態を個人情報保護委員会に対して報告する義務があることになってしまうことから、規則案6条の2第3号については、「不正の目的をもって行われたおそれ」のある漏えい等ではなく、現に「不正の目的をもって行われた」漏えい等が発生した場合にのみ、報告義務を課すとすべきである。

② 規則案6条の2第3号の「不正の目的をもって」の主体は、第三者に限るべきである。

個人情報取扱事業者およびその役職員を除くためである。すなわち、第三者によるサイバー攻撃により漏えい等が発生したおそれが場合であれば、仮に 1000 人以下の個人に関する情報が発生したおそれがある場合についても、個人情報保護委員会がそれを把握することは、セキュリティ事案に関する注意喚起を国が行うために役立つと考える。それに対して、ある事業者の一退職者による個人データの持ち出し事案（1000 人分以下）が 1 件起きたというだけであれば、法律上の義務をあえて課してまで個人情報保護委員会が把握する必要性は必ずしも高くないものと考えからである。

キ 1000 人を超える漏えい等（規則案 6 条の 2 第 4 号）

規則案 6 条の 3 第 1 項柱書における「前条各号に定める事態を知った後、速やかに」および「（報告をしようとする時点において把握しているものに限る。）」という文言からすれば、対象者が 1000 人を超えた時点ではじめて個人情報保護委員会に対する報告義務および本人に対する通知義務が生じるように解釈しうるが、必ずしも明らかではない。一定規模の漏えいの目安として 1000 人以上という数値が明記されることが検討されているが（個人情報保護委員会「改正法に関連する政令・規則等の整備に向けた論点について（漏えい等報告及び本人通知）」〔令和 2 年 10 月 30 日〕 8 頁）、事業者が漏えいの事実を把握したが、その対象者として把握している数その時点では 1000 人に満たず、時を追って 1000 人を超えた場合、あくまで 1000 人を超えたことを確認できた時点ではじめて規則案 6 条の 2 第 4 号に該当し、報告・通知対象となることを明示すべきである。

(2) 個人情報保護委員会への報告（規則案 6 条の 3）および本人に対する通知（規則案 6 条の 5）

ア 報告・通知の起算点（規則案 6 条の 3、6 条の 5）

規則案 6 条の 3 「事態を知った」および規則案 6 条の 5 「事態を知った」における、「知った」主体は、（個人情報取扱事業者が自社における漏えい等報告の実務フローを整備し、個人データの適切な管理についての責任者を任命・指定している限り、）当該責任者であることを明記されたい。

なぜなら、たとえば、営業部員が会社貸与のスマートフォンを紛失した場合、当該営業部員自身は、個人情報保護委員会への報告の可否を判断できる知見や権限を有さず、しかも、個人情報保護委員会に報告する業務を担うわけでもなく、現実には、会社の中で個人データの適切な管理についての責任者が紛失を知ってはじめて、報告義務の有無の検討および報告に向けた対応が開始されるのが実務的なフローであるからである。

他方、そのような責任者の任命・指定や実務的なフローが整備されていない個人情報取扱

事業者においては、「知った」主体について、上記の解釈とは異なる理解をすることについて反対するものではない。

イ 規則案6条の3第1項

① 規則案6条の3第1項に基づき、個人情報保護委員会に対して報告した場合、個人情報保護委員会は必ず返答を行うのか、それとも、返答を行わない場合もあるのかといった個人情報保護委員会側の対応の有無について明確にされたい。

とりわけ、従前認定個人情報保護団体に報告していた事業者の中には、個人情報保護委員会への報告がどのような結果をもたらすのかわからず不安をいただいている場合があるためである。

② 現状ある認定個人情報保護団体への報告義務は、法律上の義務も努力義務のいずれもなくなる旨を明確にされたい（この点、佐脇紀代志編著『一問一答 令和2年改正個人情報保護法』（商事法務、2020年）40頁にその旨の記載がある点は把握している）。

③ 「その他参考となる事項」（規則案6条の3第1項9号）がない場合は、「なし」として報告すればよいか明確にされたい。

ウ 速報と確報、新規と続報（規則案6条の3第2項、別記様式第一）

① 速報は法的義務とし、確報は運用上要求するという扱いに戻すことを検討されたい。もともと、個人情報保護委員会「個人情報保護法 いわゆる3年ごと見直し制度改正大綱」（令和元年12月13日）15頁の第3章第2節1.(3)の2つ目の○では「運用上、速報とは別に、一定の期限までに確報として報告を求めることとする。」と書いてあり、確報は法律上の義務とならない前提で法案が国会を通過したとの理解である。

また、他の法分野においても、速報のみを法的義務とし、確報は運用上要求するという事例は現に存在する。

たとえば、保険業法127条1項8号では、

保険会社は、次の各号のいずれかに該当するときは、内閣府令で定めるところにより、その旨を内閣総理大臣に届け出なければならない。

八 その他内閣府令（金融破綻処理制度及び金融危機管理に係るものについては、内閣府令・財務省令）で定める場合に該当するとき。

と定めており、保険業法施行規則85条1項17号において、

法第二百二十七条第一項第八号に規定する内閣府令で定める場合は、次に掲げる場合とする。

十七 保険会社、その子会社又は業務の委託先において不祥事件（業務の委託先にあつては、当該保険会社が委託する業務に係るものに限る。）が発生したことを知った場合」

とし、同じく保険業法施行規則85条6項においては、

第一項第十七号に該当するときの届出は、不祥事件の発生を保険会社が知った日から三十日以内に行わなければならない。

と定めている。保険業法に基づく実務では、速報を30日以内に提出し、調査や処分等が完了した後に最終報を提出しているため、速報のみを法的義務とすることが法体系全体の整合性という観点では望ましいと考える。

② 個人情報の取扱いを委託している委託先の漏えい等事案において、委託先は速報ベースの事項を委託元に通知すれば個人情報保護委員会への報告義務はないとされており（法22条の2第1項ただし書）、確報ベースの事項を委託元に通知することまでは求められてはいないように見える。他方、規則案によると、委託元は速報も確報も個人情報保護委員会にしなければならぬようである。委託元がかかる義務を容易に履行できるようにすべく、（仮に個人情報取扱事業者に確報を法的義務として課す場合は、）委託先が個人情報保護委員会への報告義務を免除されるためには速報ベースの通知のみならず、確報ベースの通知も委託元に行う義務を委託先に課すべきである（法22条の2第1項、規則案6条の4）。

③ 仮に、確報を法的義務として課す場合であっても、漏えい等報告（確報）は、当該事態の状況等に応じて「遅滞なく」行えばよいとすべきである。

漏えい事案の調査は、特にITリテラシーが相対的に低いと思われる業界や企業では、事態発生後、再発防止策までも含めて、30日以内で確報をすることは困難であり、現実的ではない。原因調査をするだけでも、たとえば、調査会社から見積りをとり、各社のサービスおよび料金を含めて条件を相互比較した上で選定して、正式に依頼をし、情報をやり取りするとか、プレスリリース等の準備、実施等、さまざまな作業が必要であり、専門部署があるのであればまだしも、そうでない企業には、原則30日（例外60日）は遵守しきれない。

また、規則案6条の3第1項柱書かつこ書に「報告をしようとする時点において把握しているものに限る」とあるが、「30日（または60日）以内」に確報をしなければならないという時間的・人的負担から、原因や再発防止等が網羅された完全な情報を短期間で報告しなければならない、という過度に迅速なインシデント対応を事業者に強いることになりかねない。

さらに、たとえばITのシステム開発では委託・再委託・再々委託によって1つのシステムに複数企業が関与するため、漏えい等の原因調査を実施することには相当の時間を有する。実務としては、委託元は委託先に対して、「30日（または60日）以内」という確報の期限に間に合うように、その期限から逆算して過度に短期間の確報の保証を契約で求めることが一般的になることが懸念される（さらには、当該保証が契約の重大な内容と設定され

ることが予想される)。このような構造により、委託先やさらにその先の委託先が過度な負担（実質的に不可能に近い負担）を強いられることになりかねない。

そもそも、平成 27 年個人情報保護法改正によって、いわゆる 5000 件要件が撤廃され、個人情報保護法は、中小企業を含むすべての個人情報取扱事業者に適用されることになったことを踏まえると、すべての事業者が遵守することが確実な期限を設定するべきと考える。そして、事業者の知見・規模等に応じて遵守をすることが確実な期限を一概に設定することは困難であることからして、漏えい等報告（確報）は、当該事態の状況等に応じて「遅滞なく」行えばよいとするにとどめるべきである。ただし、国民および個人情報取扱事業者からの要望がある場合に、ガイドラインにて、より具体的な報告期限の目安を定めることを一概に否定するものではない。

④ 漏えい発生直後では、規則案 6 条の 2 で定める報告対象かどうかの判断が難しい場合もあり、速報をすべきタイミングおよび仮に速報で報告した情報に誤りがあったとしても、意図的に誤った情報を事業者が報告したのでなければ個人情報保護法 22 条の 2 違反にならない旨を明確にされたい。

⑤ 規則案別記様式第一の「続報」について、「新規」の報告を「速報」で行った後、どのような場合やどのような頻度で「続報」を行うかについては、基本的に事業者側の判断に委ねられる旨を明確にされたい。

速報、続報、確報の手順が硬直的に定められると、事業者側としては負担となることから、柔軟に合理性のある選択肢を事業者がとれるように検討されたい。

⑥ 事案の性質によっては、規則案別記様式第一の「速報」と「確報」を同時に行うことも認められるのか明確にされたい。すなわち、1 度の報告で個人情報保護委員会への報告が済む場合、あえて「速報」と「確報」の 2 回の報告を行う必要はないと考えるのが合理的だが、その旨が規則案上明確ではないので、明確にされたい。

⑦ 規則案 6 条の 3 第 1 項が速報の義務を定め、2 項が確報の義務を定めているものとは理解している。しかし、他方で、2 項の冒頭が「前項の場合において」と記載されているため、1 項と 2 項の双方が速報を定めた条文とも読めないでもない。もし仮に確報を法令上の義務とするのであれば、いずれの条文に基づきかかる義務が発生するのかを明確にされたい。

(3) 本人に対する通知（規則案 6 条の 5）

① 規則案 6 条の 5 における本人に対する通知方法について、事業者によっては確実に本人に通知しうる手段を持たない可能性もあるため（たとえば、住所変更、電話番号変更）、

合理的にみて本人に通知したといえる状態であれば「通知」（個人情報保護法 22 条の 2 第 2 項）に該当することを明確にされたい。

② 本人への通知（個人情報保護法 22 条の 2 第 2 項本文）の方法については、書面、電話、ファクシミリ、電子メール、ショートメール、ウェブサイトのマイページ画面などいかなる方法でもよい旨を明確にされたい。

③ 個人情報保護法 22 条の 2 第 2 項ただし書の「本人への通知が困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置」の内容をなるべく多く例示されたい。

確かに、佐脇紀代志編著『一問一答 令和 2 年改正個人情報保護法』（商事法務、2020 年）45 頁に、「事案の概要を公表することや、問い合わせ窓口を用意して本人自身が対象となっているか確認できるようにすること等が考えられ」と記載していることは把握しているが、さらに例を充実させることによって、適切な運用が期待される。

④ 「高度な暗号化その他の個人の権利利益を保護するために必要な措置を講じたもの」（規則案 6 条の 2 第 1 号かつこ書）が漏えい等した場合の取扱いについて明確にされたい。すなわち、この場合、個人情報保護委員会への報告および本人に対する通知のいずれも不要であり、かつ、委託元への通知も不要という結論と理解しているが、その旨が条文上は必ずしも明らかではないという意見もあるため、その旨を明確にされたい（規則案 6 条の 4、6 条の 5）。

⑤ 個人情報取扱事業者について、規則案 6 条の 2 各号のいずれかの事態が生じた場合でも、「当該本人の権利利益を保護するために必要な範囲において」（規則案 6 条の 5）のみ、本人通知を行う義務を負うとされている。かかる「必要な範囲」については、基本的には個人情報取扱事業者の判断によって決めることができる旨を明確にされたい。

事業の性質や取り扱っている個人データの種類などによって事案は多様であるため、事業者が柔軟かつ合理的な対応をとれるような制度設計とするためである。

2 仮名加工情報

(1) 明確にされたい点

① （匿名加工ではなく）仮名加工情報の活用を認める意味は、仮名加工という安全措置を条件として規制を緩めて利活用を促進することにあると思われるが、この加工基準では企業としても、どこまで加工すれば十分かが必ずしも明確ではなく、必要な加工の判断が難しい場合もあり、結局保守的になり、活用されないことになる。企業が仮名加工情報を活用

するためにも、より明確かつ容易に判断できる基準、匿名加工情報と仮名加工情報との差分（加工基準の差分）を明確に示されたい。

解釈の違いにより違法となる可能性があるものであり、政令・規則においてももう少し対象を絞り込むべきではないか。もしくは、単に安全管理措置として仮名化を推奨するだけで十分であり、義務の適用除外等の緩和規定は不要ではないか。

② 仮名加工の具体例や加工手順・手順のモデルケースを明確にされたい。具体的には、文字（テキストデータ）のみならず、画像や音声の場合における仮名加工化については、今後イノベーションが進む分野でもあり、具体的な加工方法や加工手順など詳細な手順を示されたい。

③ 内部分析の範囲、変更後の利用目的の公表の粒度はどの程度のものなのかを明確にされたい。

時流に乗った情報の取扱いとするべく、企業が情報を得て、商品やサービスの向上に努めることを内部分析として判断できるようにしたいからである。

④ 仮名加工情報は、「意図をもって」作成しなければ、客観的にその情報がたまたま仮名加工情報であっても、それは仮名加工情報として取り扱わないことも可能であることを明確に示されたい。

⑤ 「個人情報に含まれる不正に利用されることにより財産的被害が生じるおそれがある記述等」（規則案 18 条の 7 第 3 号）とは、クレジット番号、銀行口座などが想起されるが、具体的にどのようなものを想定しているか明確にされたい。

(2) 解釈を確認したい事項

① 個人情報取扱事業者がその保有する個人データについて加工基準に従った加工を行っても、当該個人情報取扱事業者が当該情報を個人情報として扱い続ける限り、仮名加工情報に関する規制は適用されないと理解してよいか。

② 仮名加工情報に関する規制は適用されなかった場合、当該加工後、原データである個人情報を削除した場合、当該加工情報は個人情報としても仮名加工情報としても取り扱わないとすることは可能なのか（法 2 条 9 項、35 条の 2、規則案 18 条の 7）。仮名加工情報自体が、個人の権利利益の侵害を引き起こす可能性が低い情報であるため、かかる整理も可能と思うため、明らかにされたい。

③ 仮名加工情報が仮に漏えい等をして、仮名加工情報取扱事業者が本人に対してその旨を通知した場合については、当該通知行為は、個人情報保護法 35 条の 2 第 8 項違反にならないという理解でよいか（規則案 18 条の 9）。

たとえば、「9313357@hotmail.co.jp」のように本人が特定できない連絡先を仮名加工情報取扱事業者が保有しており、本人に対して、消費者保護・個人情報保護の観点から漏えい等を通知することは、個人情報保護法の趣旨（法1条）に反するものではないため、適法となると考える。

④ 規則案18条の7第1号の「個人情報に含まれる特定の個人を識別することができる記述等」に該当するかどうかの判断も、結局、個別具体的な活用状況に応じて変わり、ビッグデータのような大規模なデータベースでの利用であればともかく、小規模なデータベースの場合、状況によって結局氏名等を削除しても本人が特定されてしまう可能性がある。

個人情報保護法35条の2第1項には、「他の情報と照合しない限り特定の個人を識別することができないように」加工とあるが、個人情報保護委員会『『個人情報の保護に関する法律についてのガイドライン』及び『個人データの漏えい等の事案が発生した場合等の対応について』に関するQ&A』（平成29年2月16日〔令和2年9月1日更新〕）5頁のA1-16において、「特定の個人を識別することができる情報に割り当てられている識別子（例：顧客ID等）と共通のものが割り当てられていることにより、事業者内部において、特定の個人を識別することができる情報とともに参照することが可能な場合、他の情報と容易に照合することができる」と考えられると解され得るものと考えられます。」とあることを考えると、事業者内においては、ほとんどの情報が個人情報にあたると思われる（政令案5条）。

⑤ 規則案18条の7第1号の「個人情報に含まれる特定の個人を識別することができる記述等の全部又は一部を削除すること」の「等」とは、住所や生年月日等、単体では特定できなくとも組み合わせることによって特定できるものは仮名加工情報と考えてよいか。

⑥ 規則案18条の7第1号かつこ書の「当該全部又は一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換える」ことをしている限り、当該全部または一部の記述等を復元することが仮にできたとしても、同号は満たすという理解でよいか。

⑦ 加工の程度として「不正に利用されることにより財産的被害が生じるおそれがある記述等」の削除・置換（規則案18条の7第3号）をも要求するのは事業者にとって著しく負担が大きく、イノベーションを促進する観点から仮名加工情報を新設した趣旨からしても適切ではない。また、どのような個人情報の利用であっても、その使い方によっては、財産的被害につながる「おそれ」はありうるため、結局すべてを対象とすることになりかねない。

そこで、たとえば、当該文言が「不正に利用されることにより財産的被害（不正な預金の引き出し又は代金の決済等による金銭の損失をいう。）が生じるおそれがある記述等」のみ

を指すようにされたい。

3 個人関連情報

(1) 明確にされたい点

事業者において、事業活動にあたって予見可能性のある対応ができるように以下の点について明らかにされたい。

① 提供先において個人データとなることが想定される情報の第三者提供について、本人同意が得られていること等の確認を義務づけるとして、その実効性をどのように担保するのか。

② 提供先にて個人データ化すると「想定される」（法 26 条の 2 第 1 項柱書）のはどの程度の範囲か。

③ 個人情報保護委員会「改正法に関連する政令・規則等の整備に向けた論点について（個人関連情報）」（令和 2 年 11 月 20 日）9 頁にもあるように、「提供先が保有する個人データとの容易照合性が排除できない場合まで規律を適用」するものではないことを明確にされたい。

提供元の立場としては、提供先における容易照合性まで確認・調査することは事実上困難であるからである。

④ 本人同意（法 26 条の 2 第 1 項 1 号）は提供先で取得すると思われるが、具体的な方法を明確に示されたい。

実際に本人から同意を得られていることを確認するのは「提供元」なので、「提供元」が同意取得した方がスムーズな場合も多いのではないかと。提供元において第三者提供の同意を取得することを否定する趣旨ではない旨もあわせて明確に示されたい。

⑤ 本人の同意が得られていることを提供先から「申告を受ける方法」により確認する場合、「本人の同意が得られていること」を確認することで足り、具体的な同意取得の時期や方法等についてまで確認する義務は負わない旨を明確にされたい。また、仮に、申告を受けた内容が虚偽であった場合であっても、提供を受けた側は責任を問われない旨を明確にされたい。

⑥ 個人情報保護法 25 条および 26 条では、オプトアウトによる場合以外、提供年月日の記録は求められていないが、規則案 18 条の 4 第 2 号において個人関連情報の提供年月日の記録が求められている理由を明確に示されたい。

(2) 解釈を確認したい事項

① 提供先において個人データと紐づく可能性のある個人関連情報であっても、提供先が当該個人関連情報を DMP (Data Management Platform) 等のクリーンルームに置いて、個人データと紐づけずに利用するのは、「提供先において容易照合性がない=個人データとして取得していない」という理解でよいか。

② 媒体社がソーシャルプラグイン等第三者のタグを設置してクッキー等を当該第三者に送信する場合、第三者側での直接取得となり、個人関連情報の第三者提供にあたらぬという理解でよいか。

③ 提供先において、提供元から受領するクッキー情報を個人データに紐づける意図がなく、実際に個人データとの紐づけを行わなかったが、技術的には紐づけが可能であって、結果として容易照合性があった場合、個人情報保護法 26 条の 2 第 1 項第 1 号の本人からの同意を取得していなくても、提供元では同項違反とはならず、提供先においても規則案 17 条 1 項 3 号（確認記録義務）や、個人情報保護法 17 条 1 項（適正取得）の違反とならぬとの理解でよいか。

④ 意図をもって個人関連情報として扱わないと個人関連情報にならないという理解でよいか。個人情報該当性の判断は、当事者ごとに相対的に判断されるものであり、受領者側から提供を受ける情報が、提供者にとって個人情報なのか、それとも個人関連情報なのかを知ることは容易でないし、提供者側と見解が異なるケースも想定される。このような問題は時系列的に ID ベースで取得される位置情報や、購買履歴等で生じうる。受領者側の確認記録義務の内容を、個人データの受領か、個人関連情報の受領かによって混乱を招かないような配慮を求める。

⑤ 規則案 17 条 1 項 3 号イ「本人の同意」は、明示的な同意に限られず黙示でもよいという扱いにされたい。事業者の負担増加のみならず、当事者本人のいわゆる「同意疲れ」のリスクの増加も懸念されるためである（総務省「プラットフォームサービスに関する研究会最終報告書」〔令和 2 年 2 月〕12 頁）。

ア 提供元における本人同意の確認方法について（規則案 18 条の 2 第 1 項）

提供先から「申告を受ける方法その他の適切な方法」（規則案 18 条の 2 第 1 項）とされているが、「その他適切な方法」として、たとえば、口頭での申告も含むとの理解でよいか。

イ 提供元における記録義務について（規則案 18 条の 3）

① 法令に基づく場合等では、個人関連情報の第三者提供をしても確認記録義務はないという理解でよいか。

② 個人情報保護法 23 条 5 項各号の委託、事業承継、共同利用（個人データの提供があ

っても「第三者」には該当しない)となる事業者間で個人関連情報を提供する場合には、仮に提供先で個人データと紐づく場合であれば、もしくは紐づくことが想定される場合であっても、提供元において同法 26 条の 2 の確認記録義務はなく、提供先においても同法 26 条 3 項および規則案 17 条 1 項 3 号の確認記録義務はないという理解でよい。

③ 仮に個人情報保護法 23 条 5 項各号に記載の事業者間でも確認記録義務が生じうる場合、たとえば、委託者から Cookie 等のデータ分析（公開情報との参照や機械学習による受託者独自のインサイトによる分析を含む）を受託した受託者が、個人関連情報となる分析結果を委託者に納品する場合に、委託者側において分析結果について個人データとの容易照合性があれば、受託者側に本人同意の確認記録義務があるのか。

④ 自社サイト閲覧者の Cookie 等の個人関連情報を、第三者のクラウドサービス等を利用するために第三者サーバーに送信する場合において、当該第三者は個人向けサービスを広く展開しており当該 Cookie 等に紐づく個人データを保有していることが客観的に明らかな場合には、仮にクラウドサービス提供事業者自身が当該 Cookie 等を個人データに紐づける意図がない旨の申告を受けたとしても、個人情報保護法 26 条の 2 の本人同意の確認記録義務が発生するか。

⑤ A から B に個人関連情報を提供する場合、A は B から「個人データと結びつけない」旨の申告を受ければ、個人情報保護法 26 条の 2 の確認記録義務は発生しないか。B による申告だけでは足りないケースもあるのか。個人データとの紐づけの有無について B から回答を得られない場合でも、「個人データとして取得することが想定される」特段の事情がなければ、A は B に個人関連情報を提供できるのか。

⑥ A から B に個人関連情報を提供する場合、A から受領した個人関連情報を B で個人データに紐づける場合、A では個人情報保護法 26 条の 2 の確認記録義務（個人関連情報の提供）がある一方で、B では同法 26 条および規則案 17 条 1 項 3 号の確認記録義務（個人データの受領）はあるのか。

⑦ 規則案 18 条の 3 第 2 項ただし書に基づき継続的に／反復して第三者に個人関連情報を提供し、一括で記録を作成する場合、どのくらいの頻度で更新が必要か。第三者の商号変更や代表者の交代等があった場合は、記録の更新は不要と考えてよい。

4 越境移転

イノベーションの促進やデータ分析技術の向上のために、外国法人と共同で個人情報等のデータを取り扱うにあたって、今回の改正は、当該データの取扱いを大きく阻害する要因

になりかねない。たとえば、IT 企業において安価で質の高いソフトウェアを開発するためにもはや前提となってきたオフショアの活用についても、本改正による規制がボトルネックとなりかねないことに危機感を抱いているところである。

また、個人情報の利活用と個人の権利利益保護という立法趣旨に照らして考えても、本改正による越境移転規制が、個人の権利利益保護に偏りすぎている傾向がある。

したがって、越境移転による個人情報の利活用をできる限り阻害しないための方策の提案や情報提供を遂行されたい。なお、従前から公表されている個人情報保護委員会「個人情報保護法ガイドライン（外国にある第三者への提供編）」（平成 28 年 11 月〔令和 3 年 1 月一部改正〕）においては「外国にある第三者」と一括し一絡げにするのではなく、同一企業グループにある外国法人とグループ外にある外国法人とで区別して基準が提示されており、実務上大変有用であった。そのようなデータ利活用の実態にできるだけ即した基準の提示がなされることを強く求めたい。

(1) 外国にある第三者への提供に係る同意取得時に本人に提供すべき情報（規則案 11 条の 3）

ア 当該外国の名称（規則案 11 条の 3 第 2 項 1 号）について

① 外国にある第三者に対して、個人情報の取扱業務の委託を行う場合、個人情報保護法 23 条 5 項 1 号のような例外がないため、本人同意または体制整備を根拠に、当該第三者に個人データの提供を行うことになると思われる。しかし、世界に散在するベンダー企業に対してタイムリーに個人データを提供するために、規則案 11 条の 3 第 2 項の情報を開示して、本人同意を取得することは現実的に難しい。「当該外国の名称」（同項 1 号）の情報提供については、同条 3 項に例外事由が記載されているが、あらゆる場面において例外事由を適用して、具体的な国名を開示せずに同意を取得することが可能か否かが不明であり、当該例外事由の具体例を明確にされたい。

② 規則案 11 条の 3 第 3 項柱書の「特定できない」は、「特定が容易でない」とするべきである。「特定できない」という表現は、特定するための努力をどの程度行う必要があるのかが明らかでなく、事業者とクラウドベンダーとの間での交渉が長引くおそれがある。

③ 規則案 11 条の 3 第 3 項で「本人の同意を得ようとする時点において」と本人に提供する情報の時点は明確にされているところではあるが、本人の同意を取得する時点での情報に限定されること（翻って、同意取得後の情報まで提供する義務はないこと）を明確にされたい。

④ 規則案 11 条の 3 第 3 項 2 号の「本人に参考となるべき情報」としては、日本語以外

の情報も含まれるのか明確にされたい。いわゆる IT ベンダーの相当数が米国系企業であり、必ずしも日本語にて情報を提供していないことがあり、本人にとって参考になる限りでは英語での情報提供も許容することが、現実的な個人情報保護への対応であるとする。

イ 適切かつ合理的な方法により得られた当該外国における個人情報の保護に関する制度に関する情報（規則案 11 条の 3 第 2 項 2 号）について

① 外国にある第三者への提供に係る同意取得時に本人に提供すべき情報については、移転先の所在国名が特定できる場合に、「適切かつ合理的な方法により得られた当該外国における個人情報の保護に関する制度に関する情報」の提供が必要とされているが（規則案 11 条の 3 第 2 項 2 号）、同意取得時点の海外の制度に関する情報を随時調査することは事実上不可能であり、ある過去の時点での制度の情報を提供することは「合理的な方法により得られた……情報」として許容されるべきであるが、そのような不完全な可能性のある情報の提供が個人の権利保護に資するか疑問である。むしろ、移転先の国で日本と同等の保護を受けられない可能性があるというリスクの説明で足りるとすべきである。

または、諸外国の法制度については、事業者には抽象的な調査義務を課すのではなく、個人情報保護委員会等日本の公的な機関が各国と日本との法制度の差異を調査・公表し、その結果を本人に情報提供すればよいとして、事業者の情報提供義務の方法・程度について明確かつ具体的にルール化する方が、事業者の越境移転への委縮効果や情報の正確性や社会全体の効率性の観点からしてもよいのではないかと考える。

なお、調査義務の実効性を高めるためにも、事業者の規模によって、またケースによっては事業者規模にかかわらず人的・金銭的コストも過大な負担となることにも十分配慮した対応を求める。

また、仮に事業者側で調査するとしても、提供すべき外国における個人情報保護に関する制度に関する情報の具体例、モデル条項等を明確にされたい。

② 規則案 11 条の 3 第 2 項 2 号の「当該外国における個人情報の保護に関する制度」には、個人情報の保護を直接の目的とする制度のみを指し、広く消費者保護を目的とする制度は含まれない旨を明確にされたい。たとえば、米国の FTC 法は、「不公正又は欺瞞的な行為又は慣行」を禁じているが、これは個人情報の取扱いに限らずかなり広い範囲で適用されている。消費者保護法制は各国に存在することが予想されるものの、それらについても個人情報取扱事業者が情報提供しなければならないとすると、過度な負担となるためである。

③ 規則案 11 条の 3 第 2 項 1 号・2 号の「当該外国」とは、国単位で情報提供するので法的には十分であり、それ以上細かい単位（たとえば、連邦制国家における州）で情報提供する必要はない旨を明確にされたい。なお、一国でも法制度が異なるケースがあることは承

知しており、国単位の情報単位では不十分であるということであれば、どのような記載をすればよいのかを具体的に明示されたい。この場合、事業者にとって過度な負担となるような記載とするべきではない（たとえば、米国であれば、米国の州法の記載または連邦法のいずれかのみで足りるなど）。

ウ 当該第三者が講ずる個人情報の保護のための措置に関する情報（規則案 11 条の 3 第 2 項 3 号）について

① 移転元で国外の移転先事業者の講ずべき措置について確認することは現実的に難しく、事業者の越境移転への萎縮効果等に鑑み、当該情報の提供義務は削除すべきである。

② 仮に削除できないとしても（下記③④も同じ）、移転先事業者の個々の情報保護措置については、移転先事業者から開示を受けた範囲に限定すべきである。

③ 規則案 11 条の 3 第 4 項に例外事由が記載されているが、あらゆる場面において例外事由を適用して、移転先が講ずる具体的な措置を開示せずに同意を取得することが可能か否か不明であり、当該例外事由の具体例を明確にされたい。

④ 規則案 11 条の 3 第 4 項で「本人の同意を得ようとする時点において」と、本人に提供する情報の時点は明確にされているところではあるが、本人の同意を取得する時点での情報に限定されること（翻って、同意取得後の情報まで提供する義務はないこと）を明確にされたい。

(2) 移転元が講ずべき「必要な措置」（規則案 11 条の 4）

① 規則案 11 条の 4 第 1 項 1 号は削除すべきである。クラウドサービス等の場合は個別に調査シート等の対応を受けてもらえることはなく、実質的にサービス約款等の記載を確認する以上のことはできないのが現状であり、また、法務人員や外部リソースにある程度ゆとりのある一部の大企業でなければ実施することが難しく、ベンチャー企業による AI 開発等を阻害する可能性が高いと思われるためである。

② 仮に削除できないとしても（下記③～⑦も同じ）、個人情報保護委員会等でこれらの情報を調査し、情報入手できる仕組みを提供するか、記載例等を示されたい。あまりにも漠然とした表現のため、どの程度の記述が求められるのか判断が難しく、事業者ごとに差が大きくなりすぎるおそれがあるためである。

③ 「定期的に確認」（規則案 11 条の 4 第 1 項 1 号）の頻度は、たとえば、4 年に 1 回などを目安とされたい。あわせて、定期的な確認の義務について、当該事業者に情報を提供する期間が経過した後は、当該義務が課されないことを明確にされたい。

今回の改正で参照された GDPR においては、充分性認定の見直しのサイクルを 4 年とし

ている（GDPR45条3項）。これは、外国の法制度の確認を行う頻度としては4年程度を目安とすることが世界的に見ても1つの合理的な制度設計であると考えられる。

④ 規則案11条の4第1項2号の「支障が生じたとき」と「当該相当措置の継続的な実施の確保が困難となったとき」のそれぞれについて、具体例を挙げるなどして明確にされたい。

⑤ 規則案11条の4第3項柱書の「当該個人情報取扱事業者の業務の適正」は、「当該個人情報取扱事業者又は当該第三者の業務の適正」とするべきである。理由としては、第三者の安全管理措置について不必要な開示をすると、当該第三者のセキュリティに関する情報が漏えいしてしまい、かえって個人情報保護法20条に定める安全管理措置の趣旨を損なう結果となりうるためである。

⑥ 規則案11条の4第3項柱書の「求めを受けたとき」に、本人からの手数料の徴収を行うことはできない旨を明確にされたい。個人情報保護法33条が同法24条3項には適用されないので、念のため確認したい。

⑦ 規則案11条の4第4項の「全部又は一部について提供しない旨の決定」を個人情報取扱事業者はどのような場合に行うことができるのかを明確にされたい。

5 法定公表事項

(1) 「安全管理のために講じた措置」（政令案8条1号）の公表義務

安全管理措置の公表を義務づける趣旨は、本人が納得してその個人情報を託せるように、企業での安全管理措置の情報を本人に提供することにある。この点、本人にとっては、社内規程、教育、監査体制だけではなく、結局はどのような技術的な情報セキュリティ体制を構築しているかに主要な関心があると思われる、そのような技術的な情報は公表により支障を及ぼす情報である場合が多い。そう考えると、結局、公表により支障を及ぼすおそれがある項目の公表がないと本人の納得は得られないのであり、公表しても支障のない情報の提供だけでは本義務の存在価値は半減するのではないか。

仮にガイドラインで公表により支障を及ぼす情報が具体的に明示され企業としては判断ができることになったとしても、一般人である本人から本規定に基づいて公表により支障を及ぼすおそれがある項目の公表を求められることになれば、その対応に苦慮することになる。そう考えると、「安全管理措置」についての公表義務の追加は、安全管理のための秘匿の必要性と、本人の要求を満たすという点での実効性をあわせて、もう少し慎重に検討すべきである。

少なくとも現状の定め方では、改正の趣旨は全うできないと思われるので参考にされた

い。

(2) 公表すべき「保有個人データの安全管理のために講じた措置」(政令第8条1号)の内容

① 「安全管理のために講じた措置」(政令第8条1号)を公表するにしても、それぞれのデータによっても講じる安全管理措置の内容が異なることもあり、どの程度の粒度で公表を行えばよいのかがわからない。そのため、公表する必要がある事項を政令においてさらに詳細に明記した上で、あわせて、どこまで具体的に公表する必要があるのか、公表が必要な措置項目もしくは具体例を明示されたい。

② 公表することにより「保有個人データの安全管理に支障を及ぼすおそれ」(政令第8条1号かつこ書)がある場合の具体例も例示されたい。

③ プライバシーマークや ISO 認証を取得している場合には、公表する安全管理措置の内容について記載の簡略化を認めることなども検討されたい。

④ 個人情報の本人が、各企業の保有する個々のデータの具体的な保管方法に関与するというのは、現実的でないうえ、安全管理に支障を及ぼす情報も存在する。

データごとの具体的な保管方法を公表するのではなく、会社としての全般的な情報セキュリティ体制など適正なプロセスを確保するための体制に関する事項を公表事項とすることが適するものとする。

個々のデータを提供する本人の判断要素となるのは適正なプロセスを確保するための個々の企業の体制や努力といった企業姿勢であると考えられ、そのような事項が本人から把握可能となる公表事項の具体的検討と、政令による具体化を図られたい。

⑤ 公表すべき「安全管理のために講じた措置」(政令第8条1号)の中には、「個人データのやり取りにおいて、法における適用関係等について適切な検討を行」ったか否か、およびその適切な検討の結果は含まれないという理解でよいかが明確にされたい。

個人データを他人に開示するにあたっては、(a)当該開示が「提供」に該当するか否か、(b)「提供」に該当する場合に、当該他人が「第三者」(法23条5項)に該当するか否かを検討することが個人情報保護法20条に基づく個人情報取扱事業者の義務と理解している(個人情報保護委員会「個人情報の保護に関する法律第42条第1項の規定に基づく勧告等について」〔令和元年8月26日〕2(1))。

しかし、上記(a)および(b)を公表することを、中小の事業者も含むすべての個人情報取扱事業者に課すことは過度な負担となるため、公表の対象から除くべきである。

(3) 代表者の記載方法

規則案 13 条 1 号口の「代表者」とは、代表権のある者を 1 名記載すればよい旨明確にされたい。また、当該 1 名は、個人情報取扱事業者の裁量で適任者を選任すれば足りるという理解でよいか。

大企業の場合、代表権のある者が複数名いることもあり、記載の順序の検討および株主総会ごとの更新などが煩雑である。他方、代表権のある者 1 人の氏名さえわかれば本人保護の観点では十分であるからである。

6 その他（開示方法、オプトアウト届出事項、申請手続き、届出等様式や権限委任規定等）

(1) 個人情報保護法 16 条の 2 における不適正な方法による利用の禁止について

破産者マップ事件のような、相当悪質なケースが想定されているというが、条文の文言上はその規制対象が明確ではなく、広範な意味に解釈できる懸念もある。したがって、ある事業行為が「不当な行為を助長し、又は誘発するおそれがある方法」であるかどうかを判断する基準を明確にされたい。

(2) 公表すべき「保有個人データの安全管理のために講じた措置」（政令案 8 条 1 号）と同意の有効性について

安全管理措置（法 20 条）についての公表内容（法 27 条 2 項、政令案 8 条 1 号）が事実と異なっていたり、誤認を招いたりする内容を本人が同意（法 18 条、23 条、24 条等）したとしても、かかる同意の個人情報保護法上の効力には影響は与えない旨明確にされたい。

個人情報保護法上の同意は、公法上の同意であり、民法上の「錯誤」の概念がただちに適用または準用されるわけではない。そのため、個人情報保護法上の同意は、民法上の同意とは別に検討すべきである。そして、個人情報保護法に基づく公表内容と個人情報保護法の同意の効力を結びつけずとも、民事法令によって本人の保護はなしうるため、公表事項は同意の有効性に影響を与えないという整理をすべきである。

(3) 「法第 28 条第 1 項……の個人情報保護委員会規則で定める方法」（規則案 18 条の 6）

「書面の交付」による方法が適切ではない場合もあるため、電磁的記録の提供以外の方法については、事業者の判断に委ねる旨明確にされたい。なお、開示の方法に関しては、佐脇紀代志編著『一問一答 令和 2 年改正個人情報保護法』（商事法務、2020 年）76 頁におい

て、「業務の適正な実施に著しい支障を及ぼすおそれ」（法 28 条 2 項 2 号）についての解釈が記載されているが、個別の事案により「業務の適正な実施に著しい支障を及ぼすおそれ」の解釈が難しい場合も考えられるからである。

(4) 個人情報保護法 28 条の第三者提供記録の本人開示請求について

第三者提供するための本人同意は、原則として第三者を特定することまでは要せず、事業の性質・個人情報の取扱状況を鑑み、本人が同意する判断をできるために必要な情報を提供すれば足りることを明らかにされたい。当社が他の事業者（仮に「S 社」と呼ぶ）と、取引があること自体を秘密情報であると S 社との契約で約束していた場合、本人開示請求によって、第三者提供記録を本人に提示することは、S 社との秘密保持契約違反になってしまう場合、どちらを優先すればよいのか（本人へ開示請求権が優先するなど）、対応方法も含め明確にされたい。

また、上記の例で、S 社との契約違反であることを理由に当社が個人情報保護法上の開示義務を免除される場合を設けることも検討されたい。

(5) 個人情報保護法 30 条の利用停止・消去の権利について

当該停止等に対応する上で、事業者側に多額の費用が生じる場合、代替措置をとることが認められているが、「多額の費用を要する場合」について具体的に示されたい。

たとえば、一定以上の規模の企業であれば、複数の営業部署、マーケティング部署が存在し、かつ、それぞれが複数のデータベースを保有していることもある。そして、安全管理措置（法 20 条）の観点からは、それらの個人情報等データベースを名寄せしない方が望ましいという考え方もありうる。複数のデータベースに分けておくことで、仮に ID やパスワードが漏えい等した場合でも漏えい等をする保有個人データの範囲を限定でき、本人に及ぶ個人の権利利益への侵害のリスクを減らしうるからである。そして、そのような取扱いをした場合、個人の氏名やメールアドレスを把握できるだけでは、それらのデータベースに含まれる保有個人データの有無および内容を社内では容易には確認できない場合が多い。このように、社内の役職員が多く時間をかけて対応しなければ、保有個人データの有無を確認できないことがあり、こうした場合も「多額の費用を要する場合」に該当する旨を明確にされたい。

また、上記のように複数のデータベースが存在する場合に、それらをすべて名寄せして 1 つのデータベースに統合すること自体に多額の費用や時間がかかるが、統合しようとする多額の費用がかかる場合も「多額の費用を要する場合」に該当する旨を明確にされたい。

(6) 個人の請求権の拡張全般について

今回の改正により、種々の情報提供義務、開示請求対応義務、そして当該請求の結果によって個人情報の利用等停止が認められることが、事業者によるデータの取扱いを大きく阻害する要因になりかねないという懸念もあり、その点を考慮されたい。