# 個人情報保護委員会（第２６６回）議事概要

１　日　時：令和５年 12 月 21 日（木）１０：３０～
２　場　所：個人情報保護委員会　委員会室
３　出席者：丹野委員長、小川委員、中村委員、大島委員、浅井委員、
　　加藤委員、藤原委員、髙村委員、
　　松元事務局長、三原事務局次長、山澄審議官、大槻審議官、
　　森川総務課長、吉屋参事官、香月参事官、小嶋参事官、
　　片岡参事官、石田参事官
４　議事の概要
（１）議題１：いわゆる３年ごと見直し（ヒアリング）

個人情報保護委員会議事運営規程（以下「議事運営規程」という。）第９条の規定に基づき、電子情報技術産業協会（以下「JEITA」という。）吉田個人データ保護専門委員会委員長及び小泉個人データ保護専門委員会客員が会議に出席した。

JEITA から資料に基づき説明があった。

藤原委員から「第１に、資料１－１、３ページの説明についてだが、漏えい等報告義務に関して、『不正の目的によるおそれがある漏えい等』の対象とする個人データを、一定件数を超えた場合に限定するという御提案だと理解した。このことについてもう少し教えていただきたく、件数を限定するとのことだが、漏えい等のおそれの段階からの報告が必要であるという前提を踏まえると、そもそも発生段階で漏えい等の件数の全体像が把握できているのか、実際にはできないケースが多いのではないかと思う。そうすると、ここで要件を限定したとしても、果たして報告件数の絞り込みにつながるのだろうかという印象であるが、そのことについてお考えを聞かせていただきたい。

第２に、同資料３ページにおいて、『おそれのある事態』において『漏えい等事案』となったケースは少ないとの記述があるが、具体的にどの位の比率なのか、定量的にお示しいただけるものはないか。

また、『漏えい等がほぼ確実になった段階』について、具体的にどのようなケースであれば事業者は漏えい等事案になり得ると判断することができるのか、貴協会において想定している基準があれば、それについても併せて示していただきたい」旨の質問があった。

これに対し JEITA から「２番目の御質問については、いずれについても今回答を持ち合わせておらず、この場で回答が難しいため、持ち帰らせていただき、データを確認しながら検討させていただきたい。

１番目の御質問については、確かに、漏えい等のおそれが発生した時点では個人データの件数がわからないという事態は非常に多い。件数の確定までに時間を要することや、そもそも個人データが含まれているかどうかが分からない場合に、そこの判断の調査に手間を要するという実態があるため、せめて、個人データが含まれている蓋然性が高い状態になってから漏えい等報告をすることが事業者の実務上妥当ではないかと考えている。その理由として、近年サイバー攻撃が頻発しており、何らかのデータが漏えい等した可能性が生じるという、いわゆるおそれの事態が多く、そうした場合に個人データが漏えい等したかどうかを調査することには手間がかかる。そうすると、速報の期限については、個人データが漏えい等した可能性が高いと分かってから３日から５日以内までとした方が、実務と整合するのではないかと思う」旨の回答があった。

藤原委員から「どのようなデータが漏えい等したかどうかが分からないため蓋然性が高まってから報告するということになると、逆に言うと、例えば、個人データが含まれているかどうか不明であるという報告の仕方等、報告方法を工夫すれば、報告は可能となるか。報告の在り方の工夫の余地がある話なのか、蓋然性がわからない段階で報告等をすること自体が事業者にとって負担という話なのか、もう少し詳しく聞かせていただきたい」旨の質問があった。

これに対し JEITA から「２点目の御質問に関しては、ある当協会の会員企業の方は、大企業であることもあり日常的にサイバー攻撃を受けており、そういったサイバー攻撃を受けた際にはインシデントのおそれがあるというアラートが上がるが、そのアラートが上がったとしても、実際に調査をすると漏えい等が発生しているケースはほぼ０％であるとのことである。そのほぼ０％のもの全てについて、おそれがある段階で報告するのは負担が大きいということであり、漏えい等が確実になった時点で報告をするという仕組みにしていただけるとありがたいという声が寄せられている」旨の回答があった。

また、JEITA から「まだ分からないという段階では、まずは調査を優先すべきであると思うので、やはり個人データの漏えい等が発生した蓋然性が高まった時点で、３日から５日以内に報告としていただいた方が事業者の実務と整合すると思う」旨の回答があった。

浅井委員から「１点目の質問だが、資料１－１、５ページ目について、PIA について、対象案件を限定した努力義務規定化が望ましいとのことだが、具体的にはどのような分野や案件において特に有効と考えているのか。例えば、生成 AI 等の新たな技術を利用する際、PIA としては、個人情報保護法

やガイドラインへの適法性を評価する以外に、具体的にどのような点について事前に評価を行うことが考えられるか、教えていただきたい。

２点目の質問だが、同ページに、DPO 設置の努力義務規定化についても言及があるが、対象とすべき事業者や分野はどういったものを想定しているか、またその理由は何かについて、教えていただきたい。

最後の質問だが、PIA、DPO とも努力義務によることを提案いただいているが、なぜ義務ではなく努力義務なのか。むしろ明確な義務と整理した方が事業者の取組が進むのではないかとも考えられるが、そのことについて意見を聞かせていただきたい」旨の質問があった。

これに対し JEITA から「まず、３番目の御質問に対する回答になるが、いきなり義務とした場合非常に負担がかかるという事業者も多いので、まずは努力義務から始めるのが良いと思い、このような記載にさせていただいた。

それから２番目の御質問に関しては、対象となる事業者や分野の想定ということであるが、こちらについては、一般個人のプライバシー侵害リスクが高い情報を多く取り扱う分野、具体的には医療や金融等が想定されると考えている。正直に申し上げると、例えば、法人顧客の名刺情報のみを保有するような、リスクの低い事業者については、当初は対象から外していただきたいという趣旨である。

１番目の御質問である PIA に関しては、努力義務規定化が望ましいと記載した背景としては、日本で PIA を実施しようとした際、何に準拠すれば良いのかという拠り所となるものがなかなか無く、実施するとなれば、GDPR の DPIA 等を参考にするしかないといった状態のため、できれば日本版 PIA の標準的な拠り所を示していただけると有り難いという趣旨である」旨の回答があった。

藤原委員から「今の浅井委員からの質問の後半部分に関連して、DPO の趣旨についてよく分かったが、先ほどＰマーク事業者の中、Ｐマーク規程の中に確かにあるため、ということになると事業者限定というよりは企業規模の話なのかということと思ったが、そうではないかということと、実際に、義務規定でなく GDPR のような第三者でもないとなると、JEITA 傘下の企業であれば、ほぼ全て DPO を置いているのではないかと思うが、そのことについて教えていただきたい」旨の質問があった。

これに対し JEITA から「御認識の通り、後段の DPO については、JEITA 傘下の企業はほぼ設置しているため、その部分に関しては、極小規模の事業者を対象から外していただく等ある程度配慮していただければ、影響は少ないと思っている」旨の回答があった。

小川委員から「資料１－１、６ページ目から８ページにかけて、生成 AI へのデータ入力や、生成 AI が出力するデータ、生成 AI による学習、それぞれに関して個人データの取扱いに関する基準を明確化して欲しいと記載いただいている。生成 AI については、文書中心のサービスが注目されているが、ほかにも画像や音声の生成 AI も存在している。また、同様のアルゴリズムを活用した機械翻訳をはじめとして、画像の認識やユーザーのプロファイリング等、様々な技術やサービスが展開されている最中である。そのため、現時点で個人データの取扱いに関する生成 AI の基準を明確化するということは、もちろん明確化の内容や粒度にもよるが、技術やサービスの進展を妨げてしまう可能性があるのではないかという指摘もある。

そこで質問だが、生成 AI に関するデータ入力、出力、学習について、現状どのような課題が生じているのかについて、具体的に教えていただきたい。

また、それらの課題がほかの技術やサービス分野でも共通しているのか、それとも生成 AI だけの課題なのか、どのような考えをお持ちか教えていただきたい」旨の質問があった。

これに対し JEITA から「１点目の御質問の、事業者においてどのような課題が生じているかについてだが、今、生成 AI の使い方等については事業者の内部でも規程を決めて取組を進めているところであるが、様々な事業部門や開発部門から、個人データや著作権に関するデータに関する質問が多く寄せられている状況かと思う。その中でも、資料の中で挙げた事例は、JEITA の会員企業の中から挙がってきた、事業を進める上で悩むところが多いので明確化して欲しいという部分である。資料の中に挙げていない例で申し上げると、自社で AI モデルを開発する場合、自社以外の事業者が提供する基盤モデルに対し、API 経由で個人データを含む学習データを入力し、追加学習を行い、医療や金融等の特定目的に特化した独自モデルを開発し、提供する場合がある。こういった場合に、どうしても個人データを入力する必要があり、それを他社の基盤モデルに入力しなくてはいけないところで、これが委託に該当するのか、第三者提供に該当するのか、それとも、そもそも提供に該当しないのか、そういった部分を明確化していただけると、開発部門において AI を開発して、提供して利用する上でのハードルが下がるため、事業を進める上での明確化をお願いしたいとの趣旨である。

２点目の御質問、生成 AI 以外の技術との関わりについては、現時点では生成 AI の中でも文字やテキストを生成するものに意見が集中しているが、資料１－１、７ページ目で挙げたようなプロファイリングに関しては、生成 AI に限らず以前から存在している課題であると思っており、こちらについ

ても事業者側ではプロファイリングによる個人データの推測というものが個人データの取得に該当するものである理解、整理で事業を進めているが、その辺りについても実態に即した形で解釈を明確化していただいた方が、事業者としてプロファイリングを利用する上での引っ掛かりの部分がなくなりスムーズになると思う」旨の回答があった。

小川委員から「最初の御回答の中で、自社以外の事業者の API を使って独自のモデルを追加するという話があったが、生成 AI 以外でも API で情報を提供することがあると思うが、そのときの扱いについてどのように考えているか聞かせていただきたい」旨の質問があった。

これに対し JEITA から「個社の解釈については述べられないが、一般的には個人データが含まれている情報を第三者に渡し、その第三者側が独自目的に利用しているような場合には第三者提供に当たるという理解であり、提供元が指定した目的の範囲内で提供先である第三者が情報を扱う場合には委託に当たると理解している」旨の回答があった。

また、JEITA から「生成 AI 以外の従来型の API の場合は委託、第三者提供の考え方で整理ができるが、生成 AI はデータを入力した場合、別のデータが出力されるという、従前の技術とは異なる面があるため、どのように解釈したら良いのかというところで迷いが生じている」旨の回答があった。

大島委員から「資料１－１、９ページ目に記載の『学術研究分野や公的部門への、十分性認定の範囲拡大』について、それぞれの分野、部門について十分性認定がないことで、実務的にどのような問題が起きているのかについて教えていただきたい。加えて、今後どういったニーズが見込まれるのかについて教えていただきたい」旨の質問があった。

これに対し JEITA から「こちらの記載については、JEITA 内の一般的な意見としてまとめており、例えば JEITA に加盟する民間企業が学術研究機関と共同で医療分野等の研究を行うような場合、欧州側の研究機関から医療に関する個人データの提供を受けるような共同研究を行う場合がある。その場合に、欧州側の研究機関から日本側の民間事業者に移転を行うよりも、学術研究機関同士で移転を行った方がスムーズであるという事情もある。そのような観点から、事業者としては十分性認定のそれらの分野の範囲拡大をお願いしたいという趣旨である。

今後については、医療分野等では、AI を活用した研究が進み、また、幅広い国の人々のデータが必要になってくることが見込まれるため、そういったニーズが増えていくと考えている」旨の回答があった。

また、JEITA から「医療関係の学術分野や、公的部門に属する病院等に関する十分性認定があると、移転がよりスムーズになるということがこの意

見の趣旨であると思っている」旨の回答があった。

加藤委員から「最近の漏えい等事案の例に鑑みると、委託先事業者や派遣職員を含めた安全管理体制の整備や、システム設計や運用を含めたヒューマンエラーの防止策、不正アクセス対策等の安全管理措置を講じることが重要だろうと考えられる。対象事業者における漏えい等を防止するために、何か自主的に行っている取組などがあれば教えていただきたい。また、そのような『取組を行うインセンティブ』又は『行わないことに伴うディスインセンティブ』となるものがあれば併せて教えていただきたい」旨の質問があった。

これに対し JEITA から「事業者側が自主的に取り組んでいる安全管理として特に多いのは、ISMS 認証、ISO27001 に準拠した認証やプライバシーマークといった、第三者認証を取得することがある。そのインセンティブだが、特に民間事業者同士の取引において、委託先に ISMS 認証又はプライバシーマークを取得していることを求める事例が増えているため、それが実質的なインセンティブとなって、サプライチェーン全体の安全管理レベルが上がるという方向になっていると考えている」旨の回答があった。

藤原委員から「学術部門、公的部門における医療分野に係る個人データの越境移転については、旧個情法時代からの課題でもあり、貴協会におかれてもいろいろ議論されていたものと思うが、先ほど大島委員の質問に対して、学術研究機関と共同で医療分野『等』の研究を行うと回答されていたが、『等』にはどの程度まで含まれるのか、例えば、医学や薬学、疫学、また、遺伝子に関する研究であれば、考古学も関係するかもしれないが、医療分野以外において実際に何か問題になっていることがあるのか、具体的に教えていただきたい」旨の質問があった。

これに対し JEITA から「JEITA における議論の中では、学術部門において医療分野以外については挙がっていなかった」旨の回答があった。

また、JEITA から「JEITA 内では、ほとんどが医療データだと思っている」旨の回答があった。

丹野委員長から「資料１－１、７ページに記載されているが、御指摘のような推測に加えて、ターゲット広告やプロファイリング等、データの最終的な利用の在り方によっては、個人の権利利益の侵害につながる可能性があると考えている。どういった事例においてそのような問題が生じ、不適正利用に当たると考えられるか、教えていただきたい。

また、技術レベルが向上するとともに、突合する情報量が増加する傾向にあることから、その懸念もますます強くなると思うが、技術的にそういった可能性を排除することはできるのかどうかについて、教えていただきたい」

旨の質問があった。
　これに対しJEITAから「１点目の御質問については、JEITAの中で特定の事案が生したというものではなく、資料に記載のとおり、就職希望者のサイト閲覧履歴等から内定辞退率を算出して個人のプロファイルに追加する事案があった。その情報自体は要配慮個人情報には当たらないが個人の人生を左右するような情報であり、個人情報等の取得に当たるということが明確化されていれば、そのような個人関連情報を第三者に提供することは防げたのではないかと思いがあり、どのような場合に不適正利用に該当するかどうかについては強く着眼しておらず、どのような場合には取得に該当するのかどうかを明確化していただきたいという趣旨で意見を出させていただいた。
　２点目の御質問については、プロファイリングを通じて推測されたデータに個人データや要配慮個人情報が含まれていた場合に、個人のプロファイルやレコードにその情報を追加しないということは、実現方法は様々存在すると思うが技術的には可能であると認識している」旨の回答があった。
　丹野委員長から「ただいま頂いた御意見も含め、個人情報保護を巡る様々な状況について、各方面の意見を聴きながら、課題を整理、審議してまいりたい」旨の発言があった。
　JEITA 吉田個人データ保護専門委員会委員長及び小泉個人データ保護専門委員会客員が退席し、続いて、議事運営規程第９条の規定に基づき、全国商工会連合会（以下「全国連」という。）塩田専務理事が会議に出席した。
　全国連から資料に基づき説明があった。
　加藤委員から「中小企業においては、必ずしも個人情報保護法の存在やその規定内容が十分に認知されているとはなかなか言えないだろうと思う。当委員会の実施したアンケート調査では、中小企業において個人情報保護法上の規定である『漏えい等報告の義務』を知らなかった事業者の割合が約80%に及んでいるというようなこともある。事業者の適切な対応を促すインセンティブや周知活動として、どのようなものが有効と考えるか。単に分かりやすく説明するだけで十分か、考えを教えていただきたい」旨の質問があった。
　これに対し全国連から「『漏えい等報告の義務』を知らなかった事業者の割合の数値については我々も承知しており、そこの部分に関する周知を達成するまでにはまだ先が長いと思っているが、今まではガイドラインの作成やパンフレットの発行・配布をしてきたが、加えて、今はそこまでは進んでいないが、SNS等のメディア媒体も活用する等を引き続き検討していきたいと思っている。

また、そもそも、こうした取組がどうして必要なのかという情報漏えいの企業リスクを周知してもらうということで、我々自身だけではなく、損保会社がサイバー攻撃のリスクに備えた保険を販売しているため、そういった各種媒体も活用させていただきながら、少しずつ進めていきたいと思う」旨の回答があった。

中村委員から「我が国において、個人情報の不適正利用事案や、個人情報データベース等の不正提供等事案が発生しているところ、諸外国における直近の執行状況も踏まえると、実効的な個人の権利救済を行っていくためには、罰則の水準の引上げや直罰化、課徴金制度の導入を検討すべきと考える。

そこで質問だが、罰則の強化についてどのように考えられるか。中小企業にとって、それが規律の理解や遵守のインセンティブとなり得るか。またどのようなことが規律の理解や遵守のインセンティブとなり得ると考えられるか、聞かせていただきたい」旨の質問があった。

これに対し全国連から「厳罰化云々については、我々で判断できることではないので、全体の流れの中で判断いただくことになると思うが、先ほどの説明でも申し上げたとおり、中小企業と小規模事業者は、大企業と比べると保有している人的面、金銭面等のリソースが違うため、そこの部分をどのように埋め合わせるかが、まず大きな課題である。規模的には、たくさんのデータを持っている事業者は限られているのかもしれないが、支払い等を行う場合ではどうしてもそういった情報が必要だということで、着手されている事業者も結構あると思うので、そのようなところをどのように保全していくかということだと思う。

できれば、小規模事業者がシステムを利用する場合に、個人情報保護が一定水準担保されるようなサービスが世の中にあり、それを安心して利用できることの認証を付与するような仕組みがあれば、どうすればいいのか分からないというボーダーライン上の人を救えるのではないかと思う。個人情報保護に関してだけではないが、パッケージとしてそのようなことをやっていただけると、一定の水準に到達できるのかなと思っている」旨の回答があった。

丹野委員長から「御説明いただいたとおり、貴団体におかれては、個人情報保護についても非常に真摯に取り組まれていると感じているが、中小企業の経営者が、より一層個人情報保護に真摯に取り組める環境を実現するために、当委員会としてどういった取組を行うべきと考えるかについて教えていただきたい。

また、最近の漏えい等事案の例に鑑みると、委託先事業者や派遣社員を含

めた安全管理体制の整備、システム設計や運用を含めたヒューマンエラーの防止策、不正アクセス対策等の安全管理措置、この三つを講じることが非常に重要だと考えるが、中小企業において、事業者として自主的に取り組んでいる内容や措置を講じるに当たっての制度的な課題等があれば教えていただきたい」旨の質問があった。

これに対し全国連から「１点目の御質問に関して、先ほどの中村委員からの御質問への回答にも関連するが、中小企業側もサイバーインシデントが発生してもよいと思っているわけではないが、限られたリソースの中で対応した場合には、一定の割合で発生してしまうということを、どのように少なくしていくかということだろうと思う。それに必要な枠組みは、制度として作っていただいているが、そういった取組を中小企業や小規模事業者が自社だけではなく、複数社で共有することで、WIN - WIN になって売上が上がるようなアプリが完成すれば、非常にうまく進むと思うが、今の段階では、どちらかというと、EC を行っている事業者や、CRM（顧客管理システム）を持っている事業者は、非常にそういう部分に関する問題意識は強いと思うが、もう少し後続のグループをどうやって進めていくかということを考えると、何らかのバックアップがあると良いと思っている。

２点目の御質問に関して、三つの対策というのはそれぞれアプローチが違うが、我々もそのことを承知しながらも、一番大きなことになってしまうのは、漏えい等が発生すると大変なことになるということが、事業者の意識にクリティカルに認識していただくということだろうと思う。そういったことが発生しないことがよいが、そういったところに重点を置いて進めていくのも一つかもしれない。また、三つの対策を総合的に組み合わせて進めていくというやり方も当然あると思うので、我々としては、どれに力点を置くかということについては、今の段階では明確なイメージは持っていないので、引き続き、委員会の議論を踏まえて進めていくことができればと考えている」旨の回答があった。

丹野委員長から「本日頂いた御意見も含め、個人情報保護を巡る様々な状況について、各方面の意見を聴きながら、課題を整理、審議してまいりたい」旨の発言があった。

以上