# 個人情報保護委員会（第２６２回）議事概要

１　日　時：令和５年 11 月 29 日（水）１４：３０～
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、藤原委員、
梶田委員、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第９条の規定に基づき、一般社団法人日本情報経済社会推進協会（以下「JIPDEC」という。）坂下常務理事及び奥原認定個人情報保護団体事務局長が会議に出席した。

JIPDEC から、資料に基づき説明があった。

小川委員から「昨今、大規模な漏えい等事案が発生しており、そのような例に鑑みると、三つのことが考えられると思っている。

一つ目は、委託先の事業者や派遣社員を含めた安全管理体制の整備、二つ目が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、三つ目が不正アクセス対策の安全管理措置。この三つの対策を講ずることが、漏えい等の防止のために重要であると考える。

この点に関し、認定個人情報保護団体として、対象事業者における漏えい等を防止するために、どのような取組を行っているか教えていただきたい」旨の発言があった。

これに対し JIPDEC から「委託先の管理、システム設定等、不正アクセス対策について、漏えい等事故は、プライバシーマーク付与事業者で発生している事故もそうだが、その原因のうち、全体の約７割が人為的ミスであり、残りの約３割はシステムに対する不正アクセスが占めている。

まず、不正アクセスに関しては、ゼロにすることはできないというのが当協会の考えである。不正アクセスの被害に遭うことは避けられないが、被害を最小限にするためにはどうするべきか、この観点から教育をするということが一つ。

次に、人為的な部分に関しては、これは人的対策、技術的対策、物理的対策、組織的対策、この四つのルールをしっかりと順守することが大切である。

一方で事業者は、どこまで対策を行えば十分なのかがわからない。そこで、当協会では、常日頃から事例を収集し、その事例を対象事業者に情報発信す

る形で提供している。事例を見た事業者において、この事例なら導入できると判断していただくという取組を進めているのが、今の状況である」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ではないかと考える。この点について、資料１、10 ページの①に記載されているが、『指導を中心とした対応から一段引き上げた対応』という御提案があった。これについて、具体的なイメージを教えていただきたい」旨の発言があった。

これに対し JIPDEC から「もう一段階の引上げというのは、ルールがあったとしても、それが執行されないと、守らなくてはいけない、重要であるということが、なかなか事業者に肌感として伝わりづらいということがあるため、それを見せていくことが必要だろうということを意味している。

先ほどの説明の際、消費者法に関する話なども例として挙げたが、これは、消費者の被害が山のようにあり、消費者法を改正した方がいいだろうという建議が上がっての改正であった。改正後は、これだけ多くの問題があったものを改正法で正したため、執行例も増えるという傾向にある。

その例が、個情法上で、どのように実効性をもってできるかという点はあるが、事業者にとって見える化し、わかりやすく伝わる仕組みがあると良いのではないかという意味である」旨の回答があった。

髙村委員から「資料１、13 ページに関し、３点ほど質問がある。

１点目は、『PIA の実施を求める必要がある』という記載があるが、この意味が、法的に義務付けるべきだという御意見なのか、それとも、先ほどガイドラインに記載という説明があったので、努力義務として規定した方がよいという御意見なのか説明いただきたい。

２点目は、PIA の実施を求めるケースとして、具体的に、例えばどのようなケースを想定しているのかについて、説明いただきたい。

３点目は、PIA を実施する際の評価項目について、個人情報保護法やガイドライン等の適法性についてのみ評価するのか、それ以外の評価項目もあるのか、もし別に評価項目があるのであれば、どのような評価項目がふさわしいのかについて、説明いただきたい」旨の発言があった。

これに対し JIPDEC から「まず１点目について、PIA を法制の中で義務化しているのは、EU の GDPR があると思う。GDPR では、日本でいうところの要配慮個人情報や、全体のデータをモニタリングする場合等、幾つかの例があ

り、その例に該当する場合にはPIAを行うべきである旨が規定されている。

日本のサービスの中にも、そのような例が出てきている。特に令和２年・令和３年の改正個人情報保護法によって、民間事業者、国の行政機関等、地方公共団体等のそれぞれの間における、個人情報に関する壁がなくなってきている。例えば、今まで地方公共団体等しか行えなかったことを、民間事業者もできるようになってきている。そのようなことを民間事業者が行う際に、依るべき基準は必要だと思う。当初のうちはガイドライン等で示す方法はあると思うが、サービスの進み具合をみて、条文に規定することも検討してはどうかと考えている。

２点目のPIAの実施を求めるケースについてだが、ヘルスケア系、後期高齢者向けサービス、こども向けサービスについてのPIAの相談が、当協会には多く寄せられている。こうした事業では機微情報を扱うので、PIAを極力行うよう、当協会から推奨している。

３点目だが、法律に規定することや、ガイドライン等に明記するだけでは、それは要求事項である。当協会は要求事項に対して、ここまでやれば十分であるということを示さなければならない。その示す一つの基準が、日本産業規格のようなものであったり、国際標準であったりする。

PIAはISO/IEC 29134という国際標準があり、それを当協会においてリスト化している。そうしたものを活用し、十分性をチェックすることで、しっかりとした運用ができるものになると考えている」旨の回答があった。

梶田委員から「プライバシー強化技術（PETs）について、質問させていただく。資料１、７ページの説明の際に、『各企業において、その適用を考え、ときには安全性を過重に重視し、サービスが行えない等のケースもみられる。』というものがあったが、事業者において具体的にどのようなことが起こっているのか教えていただきたい」旨の発言があった。

これに対しJIPDECから「事業者の内部では、新しい技術を使おうとする際には法務のチェックを受ける。法務のチェックを受ける際に、その技術は大丈夫なのかどうかを聞かれる。それをどこまで説明できるかということが現場側では課題となる。例えば、人工知能（AI）を使おうとした際に、ここまでのことが技術的に可能だが、安全性の評価ができていないため、なかなかその機能が使えないという課題がある。

PETsも同様で、PETsというのは、秘密計算や連合学習等、幾つか技術はあるが、実は同意を取るところの認証もPETsの一つである。また、透明性を高める上では、ブロックチェーンという技術が使える。最小化してデータを使うのであれば、ゼロ知識証明が使えるわけである。様々な技術が使えるが、どこまでやれば十分なのかどうかの評価軸がまだ無い。

PIAについては、個人情報保護委員会が『PIAの取組の促進について―PIAの意義と実施手順に沿った留意点―』を作成されたように、一定程度ここまで行えばいいのではないかという基準を示されているため、広がってきている背景がある。それと同様に、PETs についても、そのようなものを考えられたらどうかという御提案である」旨の回答があった。

藤原委員から「貴協会は、主たる業務の一つとして苦情処理を対応されているが、国や都道府県レベルで行っている各種消費者相談等の窓口等とは、具体的にどのように連携されているのか」という旨の発言があった。

これに対しJIPDECから「当協会に寄せられた苦情や問い合わせの相談を、消費者団体に投げかけることや、意見交換をするような、定期的に開催しているものはないが、当協会は消費者相談等の対応を強化するため、私も所属する消費者団体の賛助会員になっている。その消費者団体には国や都道府県の消費者相談窓口担当者も数多く在籍しており、特定の事案については、消費者相談の現場に携わる方々と連携が図れるよう環境を整えている」旨の回答があった。

藤原委員から「資料１、10 ページにおいて、未報告事案の厳罰化について触れられているが、それは、JIPDEC という組織が認定個人情報保護団体としてであれ、Ｐマークの付与事業者としてであれ、一定の漏えい等事案の規模・数をほぼ正確に把握されていることが前提となっていると思うが、厳罰化を唱えられる程度の感触やエビデンスがあるということか」という旨の発言があった。

これに対しJIPDECから「ここの文脈は、先ほどの指導と執行の話に関係するものであり、もう一段階の引き上げた執行をした方がいい旨を御提案したが、法律として規定する以上は、目につかなければ何をしてもいいという形になってはいけないと思う。そこについて、厳罰化という言葉が良いかどうかはわからないが、何かしらの罰則を科するルールを考えられてはいいのではないかという御提案である。

なお、当協会としては、対象事業者からの漏えい等報告については、おおむね上がってきている所感である」旨の回答があった。

大島委員から「GDPRと、グローバルCBPRの枠組みの接点を模索して、より広いデータ流通枠組みの在り方というものについて、検討していくことが必要ではないかと考えている。CBPR認証を担っているJIPDECとして、現状どのような問題があり、またそのような、より広いデータ流通枠組みのニーズについてどのように考えているか、教えていただきたい」旨の発言があった。

これに対しJIPDECから「APEC CBPRについては、先ほど事業者の認知度

が低いと説明をした。グローバル CBPR になっていく過程での接点の話になると、様々な国に個人データが流通する DFFT の枠組みの中で、グローバル CBPR が確立していくことは、非常に良いことであり、事業者も歓迎するだろうと思う。

一方で、APEC CBPR の中の個人情報の保護要件、Program Requirements というが、これと、グローバルの場合における Program Requirements は、異なるところが出てくると思う。

以上を踏まえると、広いデータ流通の枠組みを作る際に、個人情報保護法の規定にかかわらず、何らかの要件の違反に対して、法執行が可能となるような仕組みは考えなくてはいけないのではないかと思う。ただ、グローバル CBPR は現在検討中であり、制度自体は来年以降に立ち上がるものであるため、まずは、制度として立ち上げて、各国と議論をしながら、個人情報保護委員会に御提案と御助言等を申し上げ、制度的な枠組みの構築に貢献できればと考えている」旨の回答があった。

また、JIPDEC から「事業者からは、様々なセミナーを開催した際に、色々な問い合わせを頂く。また、事業者と直接会った際に寄せられる声としては２点ある。

一つは、PRP の認証ができないのかということである。日本においても、ベンダーやプロセッサー業務を主としている事業者が多く存在しており、潜在的なニーズは高いと考える。海外に本社があり、既に当該国で APEC PRP の認証を取得している事業者からも、日本でも PRP を導入しないと、制度自体の認知度も上がらず、認証取得事業者数の向上も期待できないのではないかと思うという御意見を頂いた。

もう一つは、グループ認証についてである。今は米国とシンガポールにおいてグループ認証制度が行われており、Controller と Processor が明確に分かれているということにも起因するが、データをコントロールしている親会社と同じポリシーを一貫して使える前提があるのであれば、グループ認証できるということで、実施されている。

国際会議、グローバル CBPR の会合等で他国の審査機関や規制当局の方等と話をすることがあるが、日本に本社があり、海外に拠点がある事業者から、日本の法律上はグループ認証の枠組みがないため、グループ認証を取得するためにはどうしたらよいか問合せが入ると聞くことがある。現状、日本に親会社がある企業は親会社、海外拠点のそれぞれが個社単位で認証を受ける必要があるため、効率的な認証取得に向けて、当協会へもグループ認証の実現を希望する声が寄せられている。

グループ認証実現のためのハードルとしては、個情法上で、個人情報取扱

事業者という一義的な括りとなっている点が挙げられる。グループ認証の対象は管理者である親会社のみとなるが、管理者と処理者の区分けをするのが難しい。APEC CBPR 上の Controller と Processor の関係性にも起因する。法律を改正するのか、もう少し広い枠で考えると、EU 等との接続までも視野に入れた場合、今の APEC CBPR は事業者が APEC の枠組みに適合しているのかを確認する際、最終的には個情法で執行をかけるというルールになっているため、限界があると思う。広いデータ流通の枠組みの実現に向けて、個人情報保護法の規定に関わらず、これを超えた枠組みを検討する必要があるのではないかと考える」旨の回答があった。

丹野委員長から「資料１、９ページに関し、事業者において、個人が権利利益の行使ができる環境を整備していない場合の対応を明確化すべきという御説明があった。また、現実的に権利を行使できない可能性についても御指摘があった。

そこで、まず、例にある問い合わせ窓口が対応できないとされている点、体制整備により外国にある第三者への情報提供がなされた場合の申し出が発生し得ないという点について、もう少し詳しく御説明いただきたい。

加えて、イメージしておられるのは、事業者に環境を整備する義務を課した上で、違反した場合の措置を法律上で規定するということなのか。

また、個人の権利利益保護のための手段を増やすという観点から、消費者団体訴訟制度の導入を検討すべきという指摘もある。仮に当該制度が成立したとして、例えば、認定個人情報保護団体がその運用を担うということは考えられるか否かについても御説明いただきたい」旨の発言があった。

これに対し JIPDEC から「資料１、９ページの内容は、実際に当協会が CBPR の認証に際し事業者に伺った際に見ているものであり、事業者が法律を守るうえで極力最低限で進めようとするのは、致し方ない部分もあると思う。そこで、窓口として一つを設置しているが、消費者側に知識がないと問い合わせができない作りになってしまっているというのが、ここでの課題である。そこに対しては、環境を整備する義務を事業者に課したうえで、罰則等も進めた方がいいのではないかと考える」旨の回答があった。

また、JIPDEC から「例えば、問合せ窓口という、苦情の問合せなのか、製品の問合せなのか、何もわからない問合せ窓口が一つだけあり、当該窓口への問合せ可能な事項に令和２年改正で規定された安全管理措置の公表内容に関することも含まれる場合、全ての安全管理措置を公表することはリスク等になるため、安全管理措置に関する詳細な情報について公表することを控えている事業者もある。このような場合に、どのような安全管理措置を講じているかを確認することは可能であるものの、安全管理措置を尋ね

る問合せ窓口であることを理解している消費者がどの程度いるのかという問題がある。

令和２年改正法により、第三者提供記録の開示等、個人の権利利益が拡充されたが、この場合も同様に実態が伴っていないことが考えられる。また、基準適合体制が整備された外国等に越境移転する際は本人の同意なしで個人データを移転できるが、後で本人の求めがあった際に対応できるように準備する必要があるため、当然、最初からそれらは準備されているべきであるところ、CBPR の審査においても、消費者が理解できる高いレベルまでの実施は、事業者により濃淡がある。ただしそれは違法ではない。ガイドライン等に環境整備の具体的な対応を例示していただければ、事業者も対応しやすく、当協会としても個人情報保護法上の根拠に基づき、高いレベルでの適正な取扱いを推進しやすい。シンプルな問合せ窓口だけを設置している場合は、安全管理措置であるとか、苦情や商品サービスや、それ以外の自分が了知しない間に自身の個人データが移転されていた場合に、後で本人の求めに応じて各種対応ができるという、問合せ内容に関する注意書きを入れておくと、消費者が制度を知ることができる。せっかく法改正により個人の権利利益が拡充されたので、活用されていくべきではないかと考える」旨の回答があった。

加えて、JIPDEC から「消費者団体訴訟制度についてだが、対応できる認定個人情報保護団体は極めて限られているのではないかと思う。先日も認定個人情報保護団体の連絡会があったが、新しく認定個人情報保護団体が一つ増えたという喜ばしい報告を頂いた。しかし、全体的にみると、財務的な基盤が安定している認定個人情報保護団体がまだまだ少数であり、全体的に同じようなことができるかというと、難しいと感じる。訴訟の要因を精査するための個人情報を含む法制度に対する深い知見や、法の専門家との連携も欠かせない。もし、そのような制度を検討されるのであれば、認定個人情報保護団体を呼んでいただき、どのような形であれば対応できるのかという議論をする場を設けていただけると、私達としても積極的に意見を述べられると思う」旨の回答があった。

丹野委員長から「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。

（２）議題２：野辺地町における保有個人情報の取扱いについての個人情報の保護に関する法律に基づく行政上の対応について

事務局から、資料に基づき説明を行った。

中村委員から「地方公共団体ではLGWAN接続系や個人番号利用事務系等、複数のシステムが用いられており、システム間の個人情報等のデータ連携にUSBメモリを使用することも多いと聞いている。

USBメモリはデータ連携時の一時的記録として使用し、使用後はデータを削除することが望ましいと考える。ところが、本件のように、データ連携ごとに使用したUSBメモリの内容を消去せずにいれば、格納された個人情報の数はすぐに膨れ上がり、また、それを適正に管理せずに紛失すれば、本件や、過年度の尼崎市のような重大事案となることも考えられる。

このようなことの無いように、野辺地町の再発防止策の実施状況をよく確認していただくほか、本件についての公表や、検査等での確認を通じて、他の地方公共団体にもUSBメモリ等の取扱いや管理について周知徹底を図っていただきたいと思う」旨の発言があった。

原案のとおり決定することとなった。

なお、本議題については、事案の社会的な影響を勘案し、配付の公表資料と当該資料に係る議事録、議事概要の部分を準備が整い次第公表し、それ以外の資料と当該資料に係る議事録、議事概要の部分については非公表とすることとなった。

（３）議題３：監視・監督について

※内容について非公表

以上