個人情報保護委員会（第２８９回）議事概要

１　日　時：令和６年６月12日（水）１３：００～
２　場　所：個人情報保護委員会　委員会室
３　出席者：藤原委員長、小川委員、大島委員、浅井委員、清水委員、
　　加藤委員、髙村委員、小笠原委員
　　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、澤田参事官
４　議事の概要
（１）議題１：いわゆる３年ごと見直し　有識者ヒアリングについて

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、国立情報学研究所の佐藤教授が会議に出席した。

佐藤教授から、資料１－１に基づき説明があった。

小川委員から「AIの対応について、二つ質問したい。一つ目は、10ページ緑の３ポツ目『AIの結果は、間違いや偏りが大きい。一方で学習モデルは事業者であっても開示・修正・削除は困難である。』とあり、その下に、『何らかの救済手段を設けることを検討すべき』とあるが、救済手段について何か具体的な方法かあればお聞かせいただきたい。二つ目は、直接的な救済手段にはならないとは思うが、開示や修正は難しいということもあるので、例えば生成AIであれば個人の権利利益の侵害あるいは犯罪・悪用を防止するために事業者が入力のプロンプトにガードレールを設けるなどの対策があると思う。この点についてどのようにお考えか」という旨の発言があった。

これに対し、佐藤教授から「救済手段としては、一つ言えるとすると生成AIの使われ方は、一般の民間企業が生成AIのサービスを実行していることが多いので、生成AIの使用者側の民間企業の方で考えてほしい。生成AIの結果に対して、何か差別的な表現があるのかをフィルターして見つけるなど、使用者側で制限するやり方もあると思う。本来であればそれを生成AIの作成者にさせたいが、実効性がないと思う。あとは、プロンプト・インジェクションというやり方も考えられるので、それができればやってほしい」という旨の回答があった。

清水委員から「課徴金、団体訴訟制度について、前向きな意見を頂いたが、業界団体からは萎縮のおそれがあるということで反対意見を頂いている。課徴金制度に関しては、悪質・重大事案が対象であれば、萎縮を懸念する必要はないのではないか、とのことだが、団体訴訟のうち、差止請求に関しても、対象行為を違法行為のみに限定する場合には、萎縮の懸念はないと考えてよろしいか」という旨の発言があった。

これに対し、佐藤教授から「消費者団体訴訟に関して、対象行為を違法行為のみに限定されたものを適正としている。今回、個人情報の方でも、対象行為を違法行為のみに限定すればそれほど萎縮は起きないと思っている。その方面の方に事前に聞いた限りだと、消費者団体訴訟が起きた2005年くらいに、経済界も最終的には合意したと聞いた。ただ、懸念しておいたほうがよいのは、情報に関するものは実体がないものも多いので、重複訴訟など一般の消費者訴訟では起きにくかった問題が起きる可能性があるので、情報を扱うということ前提で、上手く規律されたらよいと思う」という旨の回答があった。

清水委員から「AIに関して、権利利益の侵害があった場合に、開示・修正・停止の対応が望ましいが、技術的にできない場合は、利用者側の規制を入れるとのことだが、利用者側の規制とは具体的にはフィルターをかけるということか」という旨の発言があった。

これに対し、佐藤教授から「フィルターをかけるのも一つ。フィルターをかける前に、明らかに差別的な結果が出てくる状況であれば、利用しないということもあると思う。いろいろな状況を個人情報保護委員会で考えて、いくつかは事業者を規制することを考えるしかないのではないか。昔のAIは利用目的が決まっていたのでやりやすかったが、今は利用目的が広がっているので、生成AIの事業者の立場からすると、何に使われるか不明で手の施しようがない。生成AIを利用して、何かサービスを提供するような事業者にかなり頑張ってもらわないと上手くいかないのではないかと思う」という旨の回答があった。

清水委員から「データ類型の再整理について、検索可能性のみの要件とした場合、テキスト形式のようなものまで広まってしまうことが考えられる。個人情報が散在的に含まれる文章も、個人情報データベースとして規制すべきとお考えか」という旨の発言があった。

これに対し、佐藤教授から「微妙なところではあるが、検索できるということが、個人の権利利益の侵害につながりやすいと考えているのであれば、検索可能性で制限すべきだと思う。それ以外であれば別のやり方がある。要件を検索可能性のみにした場合の副作用として、例えばメールみたいなものもすべからく個人データになる可能性があるので、それを含めて議論いただきたい」という旨の回答があった。

藤原委員長から「11ページの『個人データを提供先がAIの学習モデル構築に利用する場合に限り、同意なしでの第三者提供を許容する考え方もありえる』とのことだが、裏返すと、学習モデルの構築のみに利用が限定されていれば、要配慮個人情報を本人同意なく取得することについても許容されるということか」という旨の発言があった。

これに対し、佐藤教授から「資料に『その考え方は下記を要件にすべき』

と記載したが、単純にやろうとするとかなり危険だと思う。要配慮個人情報に関して言うと、やらない方がよいのではないか。このような考え方を入れるのであれば、AI の結果に対して停止・修正・削除などの権利を厚く用意しないと上手くいかない。補足に記載したことはやらない方がよいという意図で記載した」という旨の回答があった。

藤原委員長から「６ページの共同利用について、『仮名加工情報に限らず、共同利用はそれが可能な客観的範囲が不明確であり、第三者提供の制限規制の潜脱に使われるおそれがあるため、共同利用可能な範囲を明確に制限すべき』との御意見を頂いた。共同利用は、個人データや仮名加工情報を共同して利用する者の全体が一つの個人情報取扱事業者と同じであると捉えることができる場合は、第三者に該当しないものとして認められるものであるところ、仮に厳格化するとした場合、どのような点を厳格にすべきと思うか、御意見等あればお伺いしたい」という旨の発言があった。

これに対し、佐藤教授から「一個人の立場から言うと、グループ会社のように、共同利用の範囲を想像できることが大事。また、技術者の立場から言うと、異なるグループ会社以外のところが入った時には、個人情報保護指針が企業によって違うので、かなり危険な状態になると思う。共同利用は外から見えにくい制度で、今のデータの分析の方法を考えると、共同利用という制度を入れたときより、個人情報保護委員会のような監督機関による監督が難しくなってきている。昔の考え方をそのままやることは危険だと思う」という旨の回答があった。

藤原委員長から「こどもの個人情報に肯定的なご意見を頂いたが、具体的にどのような点が必要とお考えか」という旨の発言があった。

これに対し、佐藤教授から「未成年者と成年者を分けるのは年齢になる。もう一つは未成年者に係る情報に起因するリスクに基づく整理と対応。ネットサービスであれば、コンテンツリスクや、よく大人がこどもを善からぬ理由で誘い出すコンタクトリストもある。ネットサービスで言うと、こどもに判断能力がないことを前提にして、ターゲティング広告を出したり、誘導したりする機能をシステム側が作ってしまうリスクもある。未成年者の個人情報に係るリスクごとにある程度低減できるように制度設計をされるべきだと思う」という旨の回答があった。

藤原委員長から「頂いた御意見も含め、個人情報保護をめぐ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。

佐藤教授が退席し、続いて、議事運営規程第９条の規定に基づき、産業技術総合研究所の高木主任研究員が会議に出席した。

高木主任研究員から、資料１－２に基づき説明があった。

浅井委員から「資料及び御説明で、個人データの規律は事業者の負担を考

慮して整備されたという旨の私の発言に言及された。データ保護の核心的利益は個人に対する評価・決定の適正性確保にあるという論旨で理解を新たにした次第で、今回の資料冒頭 1.1.の『正確性の原則』にもつながる話だと認識した。先ほどの箇所の前段において、経済界からの要望に対して義務の対象を個人データに統一してはどうかという御提案があったが、この御提案で利活用を促進する方向性において、効果的な影響という点で強調しておくべき点があれば御教示いただきたい」という旨の発言があった。

これに対し、高木主任研究員から「利活用の観点では、資料の主要意見四つのうち、一つ目と二つ目を挙げている。一つ目の正当な利益による提供を認めるためには、基本原則としてその判断基準が必要であり、単に事業者が正当と認識するだけで許すわけにはいかないと思う。その原則を導入することが前提である。そうすると、この原則は個人情報ではなく個人データに働くものであり、両者は入り組んで依存し合った関係なので、一体で改正を行わないと解決しない。したがって、日本法では忘れられているが EU 法では確実に基本原則に存在する原則によって、また、同時に個人データに限定することで、１番目と２番目の利活用が可能になる」旨の回答があった。

髙村委員から「関連性の原則について最初に確認させていただきたい。現行法では第 18 条第１項で、『特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない』と規定されているわけだが、この条文の『必要な範囲』では御指摘の関連性の原則を満たしていないという理解でよろしいか」という旨の発言があった。

これに対し、高木主任研究員から「まず、目的外利用の方に、相当な関連性を有する場合に限って目的外利用ができるという規定があり、以前の改正で『相当な』が外れたわけだが、そこにも関連性という言葉が出てくる。御質問は目的外利用禁止の規定だと思うが、目的外利用をすることによって、目的外利用を始めた時点で元の決定目的とは異なる決定目的で利用すると、目的に関連性がないデータになる可能性が高いという関係性である」という旨の回答があった。

髙村委員から「先ほどの御説明では、日本では必要性と関連性を取り違えているという御発言だったが、個情法第 18 条第１項の『必要な範囲』のみでは関連性を満たさないということか」という旨の発言があった。

これに対し、高木主任研究員から「然り。例えば公的部門で言うと、明確に所掌事務の範囲のみで、必要性がなければ使えないことになっている。関連性が問題になる民間部門の事例として、音楽プレーヤーの再生履歴から音楽の好みを統計的に推定し、機械学習でお金を返さない可能性との相関を推定し、お金を貸すか、金額をどうするかを決定することは、決定の目的に対し音楽の趣味は関連性がないという言い方になる。しかし、このようなビジネスを展開する上で、ビジネスを行う者にとっては必要な情報になる

ため、必要となったらできてしまうということ。したがって、誰であれ必要があっても関連性がなければ使えないのが関連性の原則である。公的部門でも実際に問題が起きていて、こども家庭庁で推進している事案では、困難を抱えているこどもの抽出のために家庭の様々な状況をデータ分析するという取組がなされているが、これも関連性が問題となる。彼らとしては必要がある情報を使っているという主張だが、関連性があるかを問われるということだと思う」という旨の回答があった。

髙村委員から「資料１－２の 13 ページで、関連性の原則は個人に対する評価や差別をしないという意味だという記載があるが、今の例示もその文脈か」という旨の発言があった。

これに対し、高木主任研究員から「然り。差別という言葉は多義的で注意が必要だが、資料に記載しているように形式的差別という基本に立ち返ると、人の集団を区別する目的が区別の基準と一致しているかを問われるというのが関連性の概念で、これが一致していないと差別が起きるという意味である」という旨の回答があった。

髙村委員から「現行法の第 19 条でも不適正利用が禁止されているが、先ほどは、第 19 条は個人情報を対象にしている点で問題だという御指摘だった。仮に第 19 条が個人データを対象にした場合も、御指摘の不当な評価や差別の問題は賄えないということか」という旨の発言があった。

これに対し、高木主任研究員から「そのためには、不適正利用の不適正が何を指すのか、何らか基準が必要だと思い、それが先ほどの原則を欠いているという主張につながる。結局不適正利用の中身を決めていくか新しく原則を設けるかで、内容は決めていく必要がある。現行法が不適正利用を定めたときは、『違法又は不当な行為を助長』という、他の法令の価値観に頼って不適正を決めようとしたり、この法の趣旨に反するものという説明もどこかにあったと思うが、その趣旨が不明確であったりと、結局まずそれを定めないと解決しないと考える」という旨の回答があった。

小川委員から「生成 AI について確認と質問を一つずつしたい。７ページの下から２段落目で、生成 AI の結果は利用者の入力するプロンプトと LLM の両者によって生成されるが、LLM は巨大なベクトル空間内の関数に過ぎないため、プロンプトを入力する利用者の責任が多いという解釈でよろしいか」という旨の発言があった。

これに対し、高木主任研究員から「資料にも少し補足で書いたが、著作権法の観点で生成 AI に対して議論されていることとパラレルである。著作権法では非享受目的と呼ばれる著作物に表現された思想感情を自ら享受することを目的としない場合については、複製してもよいという規定が入ってきて、日本は機械学習パラダイスと呼ばれている。この話では、自分の作品が複製されて学習入力になること自体に抵抗を示す著作権者もいる一方で、

このルールでよいと言う著作権法の先生方もいる。学習入力した著作物がそのままそこに残って出て行くわけではなく、一旦完全に分解される。その後、再構築されて出ることがあるかもしれないが、出力させた人が複製しているのだという考え方である。そのことからの類推で、要配慮個人情報が飲み込まれてそのまま出てくるというわけではなく、そういうものを出そうとすると出てくるかもしれないが、その以前の段階では個情法上問題ではないということだと考える」という旨の回答があった。

小川委員から「もう一つ、利用者の責任は確かに大きいと思うが、例えばLLM を悪用してディープフェイクなど様々な社会的リスクをもたらす可能性がある。そのため、LLM を使った AI サービスを提供したり運用したりする事業者の責任について、LLM の出力のみならず入力の抑制なども含めて、お考えがあれば伺いたい」という旨の発言があった。

これに対し、高木主任研究員から「私は入力ではなく出力を問題にすべきだと考える。たとえ利用者の責任だとはいえ、不適正な出力が続くようなことがあれば、サービス運営者である LLM 提供者も一定の責任を問われるということで、出力を規制することが考えられる。これは Google の検索エンジンが、欧州で忘れられる権利の決定で問題になったのとよく似ている。Google はただ検索結果を出しているだけだが、検索の入力をした人がある人について検索するとその人の情報が出てくる中で、検索エンジンを提供している者に対しての削除対応の義務を認めた。それと類する形で欧州においては生成 AI についても規律されていくのだと予測する。よって、昨今AI 規制が日本でも検討されているが、欧州で何が問題にされているかを技術的に正確に踏まえた上で法規制を考えないとあらぬ方向に行く可能性がある。先日はコンピューターウイルスを素人でも作れたという報道があった。本当に完成しているかは疑わしいものの、犯罪に使用されるという側面のみを強調して AI 規制だと言われつつあるが、問題はそこではない。公平性・正確性の観点で出力が妥当なものがサービスされるべきという観点で、欧州の AI 規制は進んでいる。日本でもそのことの理解が必要。そのときに、個情法ですら決定の公平性・正確性という観点を今まで忘れてきているわけなので、そこを正しくしていかないと AI 規制も乗り遅れる」旨の回答があった。

小笠原委員から「経済界からの要望への対応の関係で、本日話題にはなっていなかったが、団体訴訟制度について、業界団体から個人データの利活用の萎縮が生じるため導入は反対という意見を頂いている。この点について、何かお考えはあるか」という旨の発言があった。

これに対し、高木主任研究員から「その点については私の専門性から外れるので特段コメントはないが、そもそも個情法が何を権利利益としているか明確になっていない段階でそのような仕組みを設けても時期尚早ではな

いかと思う」という旨の回答があった。

清水委員から「資料の３ページの『1.2.統計量への集計』では、第三者提供時の利用目的の拘束の仕組みを設けるべきとの御指摘だと理解した。資料に記載いただいているように、Q７-43 との関係で、委託元３社がある中で、同じ委託先にデータを委託して処理をしてもらう場合、各社のデータを活用して得た委託先の成果物を委託元３社にも還元すべきではないかという御主旨だと理解している。この場合、利用目的が同じであれば同意は不要ということだが、利用目的を誰が確認するとお考えか」という旨の発言があった。

これに対し、高木主任研究員から「ここの利用目的で特に重要なのが、決定利用する予定がないということで、言い換えれば統計量に集計することを目的にしているということ。このような利用目的はそれなりに広く取られてよいと考える。統計量にするのであれば、どのような統計量にするかはあまり重要ではない。その範囲で目的拘束が働けばよいので、複数の事業者から出たデータが最終的に統計量としてしか使われないことが何らか保証されていればよく、それをどのように法律上義務で達成するかの具体例はここでは示していないが、立法の研究や慎重な検討のもと仕組みを構築する必要がある」という旨の回答があった。

清水委員から「統計量にしか使わないという保証は必要で、事業者の善意に任せておいては難しい部分もあるだろう。目的が同じだということで済むわけではなく、そこが課題ではないか」という旨の発言があった。

これに対し、高木主任研究員から「EU 法も同様の仕組みとなっている中、統計利用、科学歴史研究利用、公益保存の場合には、各国法でその仕組みを規定することになっている。そのときに、イギリス法もフランス法も、決定利用を禁止している。EHDS 法案も、二次利用規定の最初の条文で決定を禁止する旨規定されている。同じことを日本法にも入れるべきだが、これは匿名加工情報や仮名加工情報における再識別禁止とは異なる」という旨の回答があった。

清水委員から「現在の制度でも共同利用はあるが、その場合でも利用目的を明確にして本人通知が必要である。結果的にそれと類似すると思うが、共同利用は使えないものか」という旨の発言があった。

これに対し、高木主任研究員から「お尋ねは仮名加工情報の共同利用のことかと思う。令和２年改正の時点では問題点に気付かなかったため声を挙げることは出来なかったが、今では問題があると思っている。共同利用のモデルと仮名加工情報のモデルを合わせたときにどのようなルールになるかは二つ考えられる。一つは元々個人情報を共同利用していたグループがそのグループの中で任意の目的で仮名加工情報を作成して利用するという構成、もう一つは作成した仮名加工情報を、新たな任意のグループで共同利用

できるとする構成である。後者は一部事業者での利用が検討され、厚労科研でも検討されたが、これは、共同利用モデルはグループが固定的なものという制限に対して潜脱的ではないかと懸念している。これは先ほどの利用目的拘束のある適切な統計利用としては少し不安定なやり方で再検討が必要である」という旨の回答があった。

藤原委員長から「頂いた御意見も含め、個人情報保護をめぐ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