個人情報保護法のいわゆる３年ごと見直しの検討の充実に向けた事務局ヒアリング
議事概要

１　日　時：令和６年 11 月 22 日（金）17:00～

２　場　所：個人情報保護委員会

３　出席者：

（１）ヒアリング対象者：

中央大学国際情報学部　石井夏生利教授

京都大学大学院法学研究科　曽我部真裕教授

（２）個人情報保護委員会事務局：

佐脇事務局長、西中事務局次長、小川審議官、吉屋参事官、香月参事官

４　議事の概要

（１）ヒアリング対象者からの説明

①石井教授から、資料１に基づき主に以下の点について説明があった。

・（参考４[1]）１　「自律的なガバナンス」へ期待することはもはや現実的ではない。同意の形骸化を放置することも懸念。プライバシーや個人情報保護に対する本人の権利利益が本人の努力を求めることなくデータのライフサイクルを通じてデフォルトで保障されている体制、プライバシー・バイ・デザインに即した取組が必要。

・公的機関、民間事業者ともに、アカウンタビリティの確保、遵守の責任は義務を負う側の主体にある。

・リスクベースの考え方に基づくルール形成が一層重要性を増す。

・（参考４）１⑧　データポータビリティについて、反対はしないが本人関与の仕組みには限界がある。

・（参考４）２　本人に影響のない範囲でデータ利用されていることを担保する仕組みが必要。

・（参考４）３　緩和の必要性はあるが、取扱いの適法性を裏付ける基準等や安全管理措置、影響評価等の仕組みとセットで考える必要がある。

・（参考４）４　委託先の監督が実質的に機能しないのであれば、主たる責任主体となるべき者への規律が必要。

・（参考４）５　識別可能性は通常識別子を通じて達成されることも踏まえ、端末の識別子等を個人情報に含めるべきと考える。

---

[1]　（参考１～４）について、第 310 回個人情報保護委員会　資料１―１「『個人情報保護法のいわゆる３年ごと見直しの検討の充実に向けた視点』に関するヒアリングの概要について」別添１の参考１～４を参照。

・（参考４）６①　妥当。（参考４）６②は特別の規律が必要であろう。
・他の法分野の議論との関わりが個人データ保護の分野において生じている。競争法、消費者法との関わり、他の監督当局との協力連携の必要性が高まる。
・医療については、次世代医療基盤法、がん登録推進法、倫理指針等の議論が個別に複雑に進んでおり、その保護レベルの妥当性が説明困難ではないか。
・（参考４）５　情報通信分野では、識別子等に個人情報概念を拡大する方向に賛成。識別子等による個人の追跡やプロファイリングのリスクがあり、保護対象とすべき。
・（参考４）１③　教育データについては、公的部門のルール見直しが急務。法定代理人と子供の利益が相反する場合や、保護者側のリテラシーへの配慮がある。
・（参考４）１⑥　プロファイリングについては、幅広くオプションを考える必要がある。

②曽我部教授から、資料２に基づき主に以下の点について説明があった。
・（参考３）　現行法は形式的ルールを基調としているがゆえに問題が起きている。一方、実体的ルールには不明瞭なところがあって、その明確化のために、個人情報保護委員会（以下「委員会」という。）の執行事例や裁判例等の事例の蓄積が必要である。
・（参考３）　委員会の執行事例は公表されたものは必ずしも多くない中で、実態ルールにいきなり移行すると大転換になる。形式的ルールという基本的方針を維持しつつ、実態的ルールを一部導入していくのが「現実的な方法」ではないか。
・（参考２）　視点においてリスクに着目した点が評価できる。リスクを言語化して区別し、それに応じて対処していくことにより、リスクが低い場合／高い場合に応じて、特別の規律を導入することができる。
・（参考４）１①　当事者間の自律的なガバナンスというが、そもそも対等な関係ではなく、自律的なガバナンスが成立する前提を欠いている。委員会による法執行、民間団体による差止請求、ADR 等。非対称性を埋める手段が重要。子供ではより顕著。
・（参考４）１④　利用目的変更に制限がなければ、本人に不利益を及ぼす可能性がある。不利益とならない場合には、常に同意が必要ではないかもしれない。
・（参考４）６①　要配慮個人情報の規制は、同意が厳格ではない、推知は取得の対象外とされる、利用のされ方によらない形式的ルールであり過剰／過少規制が生じやすい。実体的ルールの考え方を導入し、PIA 導入等

の規律が必要。

・（参考４）１⑦　課徴金導入については、悪質な個人情報の利用事案が相次いでおり、課徴金制度の立法事実を提供している。課徴金導入により、企業のインセンティブ構造を変えることができ、さらに発展させてリーニエンシー制度も導入できれば効果が期待できる。そのためには、委員会の執行能力の異次元の強化が必要になる。

（２）各ヒアリング対象者と事務局との主な質疑応答は以下のとおり。

当事者間の自立的なガバナンスについて　※「参考資料１－１（参考４）１」関連

（事務局）

○　当事者間の自律的なガバナンスの限界について御指摘があった。曽我部教授の資料の中で、現行制度の位置付けを定義したことについて、現行制度の正当化を目的としているのであれば、あまり賛成できないと書いてあった。これについては、私どもは、個人情報保護法制定時の基本的なコンセプトをひも解いていけばそうだったという意味で記述してみたということに過ぎず、ドグマとして維持しないといけないと思って書いたわけではない。一方で、個人の様々な請求権その他が法文上書いてあることについて、それがいわゆる個人が自らの情報を自らの思うように取り扱うことを大事にすべきだという意味合いの具体化として位置付けるというような発想もあるわけだが、ここはあくまでも個人が、自分が預けたデータがどう取り扱われているかについて関与するトリガーとして位置付けられていることを整理しておくという意味では、位置付けを明確にするという意図はあった。その上で、お二方とも、本人が関与して規律を貫徹するのは非現実的だというお話だったかと思う。とはいえ、現行制度上でいえば、例えば安全管理措置や開示義務など、個人情報取扱事業者に直接係らしめている義務体系は多くあり、そう考えると、個人の責任にしてしまっている部分は何にどのように使われているかについて、個人がモニタリングし、納得・了解し、そのとおりになっておらず事業者に落ち度があれば、エグジットできることになっている。より事業者に寄せた規律にしていく制度設計に変える場合には、利用目的規律その他の部分をポジティブに制度化した上で、そこの義務規定を強化し、その有り様について、国ないし委員会がウォッチする制度設計が想定される。より具体的に、当事者間の自律的ガバナンスによらない世界にしていく場合に、象徴的には何をどうすることがそれに該当するのか、もしヒントがあれば教えていただきたい。

（石井教授）

○　おっしゃるように、利用目的の規律、モニタリング、さらにそれを是正

する仕組みを強化していくのが第一段階としては考えられるだろう。まさにこの点が大転換できるかどうかの論点になっていると思っている。現状、要配慮個人情報は除いて、取得の規制は基本的になく、また取得の解釈にも議論があるところ。そうしたことを踏まえると、取扱いそのものに制限をかけていく、プロセシングといったものに対する規律を課すのが次の段階として考え得るのではないか。さらに、脆弱な主体は別の考慮が必要。特に子供の教育データの利活用で、子供の情報を取り扱うときに、教育委員会がデータを取得し、民間事業者に委託するという形態が取られるが、そのときに、子供・保護者の同意があっても、目的によってはデータの取扱いが認められない場合があるのではないか、すなわち、同意があっても駄目な使い方があると思うので、より脆弱な主体に対する取扱いについて、利用目的を縛るなど、そういう考え方もあり得るのではないか。

（曽我部教授）

○　組替え後の立法の建付けにも依存すると思うが、今後の立法も、基本的には形式的ルールを基調とする。つまり、特別な理由がない場合には、利用目的そのものの設定も事業者が自由にでき、GDPR のような正当化根拠を要求しないものに関して言うと、基本的には、現行法の建付けが継続するわけだが、その場合においては、非対称性を埋めるような手段を設けていくということか。すなわち、現状、本人がアプローチしていくことになるが、それがなかなかおぼつかないときに、消費者団体で対応するとか、本人が権利行使をしたときに、当事者間において事業者が応じないようなときには、裁判に訴えなくても権利が実現できるような手法によって非対称性を埋めていくというアプローチになるだろう。他方で、実体的ルールを一部導入して形式的ルールを修正するときには、事業者のこういう目的で、こういう情報をこのように取り扱っていいのかということ自体が実体的ルールに縛られることになり、それはまさに自律的なガバナンスではなくなっていく。本人の異議申立てなどは端緒だと思うが、それを委員会等がチェックしていくという流れになる。結局、前提となるルールがどういったものになるのかによって、シナリオとして変わってくるのではないか。

守られるべき利益の外延に係るリスク　※「参考資料１－１（参考４）５②」関連

（事務局）

○　（A）～（D）のリスクの例を書いているが、これについて優先順位付けをあえてするとした場合どのように思われるか、もし御見解があればお聞きしたい。

（石井教授）

○　優先順位と言われるとなかなか難しいが、（A）～（D）のいずれも非常に重要性が高く、それぞれに関連しているのではないか。(A)、(B)、(C)の順番で大事というように優先順位付けをすることはなかなか難しい。関連性がそれぞれある。

（曽我部教授）

○　結論としては、石井先生と同様で、例えば（A)、(B)、(C)、(D）の順番で優先順位が高いとは語れない。例えば、(A）は「評価・選別し、それに基づいて、特定個人に影響を与える行為を行うことのリスク」といっても、これはGDPRのプロファイリング、自動決定の規制にもあるように、何に関する決定なのか、採用に関する決定なのか、広告配信に対する決定なのかというのは全然違う。よって、(A）でも重要なものもあれば、そうでもないものもあるだろうということ。そのほかも同様。ただ、(C）に関しては、一般的に不法行為、あるいはプライバシーの問題にされているところであって、自身の秘匿したい領域。これも様々あるとは思うが、非常に秘匿性の高いものが暴露されるのは、一般的に言っても大きなリスク、重大な問題なのだろう。他方、(D）に関して言うと、それ以外、つまり、これは自己情報コントロールの話だと思うが、コントロールができないこと自体が大きな問題だとはあまり思わず、(D）に関して言うと、比較的重要ではない、ということか。コントロールができないことにまつわって、何か別の弊害が生まれるときに問題となるので、制御できないこと自体に一般的に大きな不利益が付きまとうかどうかは分かりにくいところではある。ということで、一般的に言うと、(C）の一部は非常に重大、(D）はあまり重大ではないという印象。(A）と（B）はものによるところではないか。

（事務局）

○　（A）～（D）に関して、とりわけ（B）の勧誘等にデータが使われるようなことよりも、(A）の評価・選別によって個人に一定の影響を及ぼすほうが、個人情報保護法としてフォローすべきリスクとしてははるかに重要なものであるというような議論もある。例えばCookieその他の識別子を取り巻く議論においては、それによってあまり接点を持ちたくないという発想から、それを接点としてアドレスされることそのものについて、本人にとってコントローラブルであったほうがより良いという主張がある。そういった立場からすると、(B）は重要な観点だという議論も成り立つ。その点について、(B）については二の次でいいという議論があった場合に、お二方はそうでもないという御判断だと受け止めたが、その点についてコメントあればいただきたい。

（石井教授）

○　今の御質問は、(A) と (B) の重要度には顕著な差があるかということかと理解したが、全くそのようなことはない。曽我部教授がものによるとおっしゃったとおりで、例えばCookieを使って勧誘する行為で意思決定を歪められるのもプライバシー侵害の一つと捉えることができ、(A) のほうが圧倒的に重要ということはない。意思決定が歪められると、ケンブリッジアナリティカ事件のような、よく知られている事件が取り上げられる話も出てくるところであり、具体的な弊害につながり得るリスクという意味では、(A) であっても、(B) であっても変わらない。もちろん (C) であっても変わらないし、(D) は、コントロールできないこと自体よりも、それによってどのような弊害が生じるかということを見るべきで、弊害が生じた時点や弊害が懸念される時点を軸に評価することになるだろう。優先順位で明確な差があるわけではないということ。また、弊害の観点から整理していくことが適切なリスクの考え方を整えていく上で重要であり、偏った考えにならないようにする意識が大事。併せて、人によっては、特定のリスクが非常に危険だと思う可能性もあるが、具体的な規律に即して考えていくことが求められるべきである。AI 採用のことに資料の中で言及したが、これは現実に起こっている問題であり、録画面接などを行って、事業者側が説明もせずに録画と質問を受けて、応募者がそれに答える。応募者がきちんとした説明を受けていない中で録画面接を受けて、目の動きや話し方、どのような言葉を使ったかなど、そういう情報が取得され、裏で分析されて、当該仕事への適合性が計られるということが実際に起きている。こうした具体例を拾いつつ、リスクを評価していくことも、アプローチとしてあり得るのではないか。

（曽我部教授）

○　リスクに関しては、データ保護の目的をどう捉えるかというある意味哲学的論争の領域に入っているかと思うが、私個人の立場は石井教授と同様で、データ保護の目的が多元的なものであって、様々なデータ保護にまつわる本人に対する不利益を幅広く拾って、そういった不利益から幅広く保護を提供するのがデータ保護の目的だと考えているので、(A) だけが重要だという立場には立たない。１点補足だが、(C) で、先ほど秘匿したい領域について、秘匿性の高いものについては非常にリスクが高いのではないかと申し上げたが、他方で、データによる監視に関しては、秘匿性の高い領域だけではなくて、日常生活であっても、常に監視されていることによる生活全般の萎縮のリスクもあるので、それはそれとして軽いものではないと思っている。したがって、(C) は秘匿したい領域と限定してしまうと、日常生活が全般的に監視されるところを捉え切れるのかどうか気になったので、リスクとして別立てするのか、(C) の中に含めるのかは別として、そういったリスクも考えていただくのが良いのではない

か。

（事務局）

○　仮にデータ保護の目的が多層的・多元的であるとした場合に、当事者間の自律的ガバナンスを超えて、より実体的ルールを重視した法体系に変えていくことになると、何を基準にし、どういう優先順位で、より重大なものであるとラベルを貼り、執行リソースを寄せていくかという戦略的判断が必要になる。一方で、多元的・多層的であるがゆえに裁量は広くなるので、執行当局としてはある意味やりがいがある一方で、どうしていくかということについては相当な時間と歴史を紡ぎながら考えることが許されるかどうかも含めて、大問題になってくるように思う。したがって、その場合に、準則のようなものはどこからリファーすればいいのか。他方、プライバシー・バイ・デザインのように、十数年来インプリメントされてきた手法論があり、そういったものに還元できた場合には、今申し上げたようなデータ保護による守るべき価値みたいなものに降りずに、一定の世界共通の手法論によって担保できる世界ももしかしたらあるかと思いつつ、この辺りの悩みをどう解消すればいいのかについて、ヒントがあれば教えていただきたい。また、その場合、消費者にとっての情報の非対称性はあると分かった上で、国の行政機関であるので、様々な権力的なツールによって情報を引き出すことはあり得るものの、それであっても、ある程度事業者側からデフォルトで相当な情報公開がないと、世間のリクエストにタイムリーに応えるようなパフォーマンスを発揮できるのだろうかという懸念もあり、その辺りの実効的な執行を可能にするために、どれぐらいの情報の開示を事業者に求めるべきなのかということも含めて、もしコメントあればいただきたい。

（石井教授）

○　実体的なルールの導入のところについて、GDPR では、諸原則を掲げ、その諸原則の一つに適法な取扱いが入っており、適法な取扱いを担保するためのさらなる要件として、同意や契約の履行、法的な義務、正当な利益などが掲げられるという建付けになっている。日本の個人情報保護法は、OECD プライバシーガイドラインの諸原則などを念頭に置いたルールにはなっているが、建付け自体は GDPR と大きく違うことは否めない。そういう中で、実体的ルールを入れるとなると、先行する GDPR の規制などを参考にすることになってくるだろう。そのときに、似たような形のルールを設けるとすれば、適法な根拠のどれに当たるかということを事業者が異常に気にするのが、恐らく日本で想定される事態になる。EU の法執行機関が駄目だと言っているのは、同意の要件や正当な利益のところではないかと思う。よって、同意の部分に手を入れてみることや、個別の EU の執行状況の中で使われている規定を踏まえて、日本の利用目的を縛る

などの対応はあり得るのではないか。「同意」といっても、日本の解釈の「同意」だと緩やかなので、その辺りを縛っていく必要はあるだろうが、具体的な執行事例を踏まえて使える規定を絞り込んでいくことも一つ考えられるかもしれない。リスク評価というか、バイ・デザインは諸原則を掲げている。実施方法としては、PIA が一番分かりやすい例だとされており、事業者が大量のデータを扱う、プロファイリングを行うなど、一定のリスクが高いと見られる場合に、リスク評価を行い、その結果を公開することでアカウンタビリティを求めていく。ただ、PIA を公開していることをもって正当化されてしまうと、またそれも実効性がなくなってしまうので、公開されたものを専門家が評価できるような仕組みや、そうしたものも併せて検討すると実効性があるのではないか。

（曽我部教授）

○　執行のためにリスクを特定する必要があるか、というところだが、そもそもそれが果たしてそうなのかと思う。リスク分類をどのように使っていくのかということで、一つ考えられるのは、GDPR みたいに完全に実体的ルールに移行した場合であっても、結局、正当な利益との関係で最小限度の利用かというところは、一義的には事業者が判断し、そこについて、いわゆる憲法学でいう厳格な審査をするわけではないはずなので、そこをモニタリングするときに、執行当局がリスクの質とか程度を厳格に判断する局面がどこまであるのかというのは、よく分からないところ。もう一つは、実体的ルールに移行し切らないときに、今回の視点のようなアプローチのときに、リスクの高いものに関しては特別な規律を導入する、一般的には、現行法どおり、形式的ルールを基調とするというときには、制度をつくるときにリスクを特定して、このリスクに備えるために、こういう特別な規律を導入するのだという形でつくるわけなので、そこに関しては、執行時には、特段リスクについて詳細な価値付けをしていく必要が必ずしもないのかもしれない。さらに考えられるのが、例えば課徴金が入ったときに、結果に応じて課徴金の額を設定することが考えられるが、そこは個別の事案なので、このケースでは、こういう点に照らして、非常に重大な問題があったというところで、個別に具体的事例に即してやっていくことになるか。したがって、具体的な執行の場面で、例えば今４つ挙がっているリスクのどれに当たるのか、どれが重要なのかとか、そういったことを直接判断する局面はどれほどあるのかと今お聞きして思った。

（事務局）

○　更問になるが、実体的ルールを前提に執行する場合、どんな場合に何をすることになるか。つまり、正当化を行う場合の事業者の言説は、事業者の責任で取りあえず出してもらい、それとの関係で嘘をついているかどうかを見極めることになるか。

（曽我部教授）

○　結局、先ほどの自律的なガバナンスとも関わると思うが、問題提起自体は、消費者というか、本人に上げていただく必要があり、異議申立てがあったときに、その建付けで本当に正当な利益とか必要最小限なのかというところを執行当局が審査することになると思うが、観点としては「正当な利益」が本当に正当かというところと、それとの関係で必要最小限のデータ利用になっているのか、目的と手段を審査するところだと思うが、それに関して、一つは「正当な利益」とは何かというのは、恐らく、そこはガイドラインや執行事例の中で固まっていくところだろう。「必要最小限」については、ある程度具体的事案の中で事業者にも主張させる中で判断できるということで、いずれにしても、目的と手段を審査するので、リスクそのものが直接正面から出てくるということではないのかなと思うがどうか。

プロファイリングに係る規律について　※「参考資料１－１（参考４）１⑥」関連

（事務局）

○　曽我部教授の資料では、プロファイリングについて、項目の適切性やアルゴリズムなどの観点に着目した御指摘があった。それらはGDPRなどでプロファイリング規制として掲げているものの、必ずしもメインの視点でもないかと思う。例えば石井教授から見られた場合に、曽我部教授が御指摘されているような観点でのチェックという発想は、どのように思うか。

（石井教授）

○　曽我部教授がお書きになっているプロファイリング過程の適正性確保は重要だが、それにとどまらず、GDPR以外の法令でもルールが入ってきていることを踏まえて、可能なオプションを整理することが、私が主張したかったこと。曽我部教授がお書きになっている項目の適切性や適正性確保は、当然ながらその中に含まれる。問題は、プロファイリングがいろいろな場面で法令を定めるときの関心事項になっていることは否めない。様々なルールの定め方がデジタルサービス法やAI規則などでも入ってきているので、個人情報保護法にプロファイリングを定めるときに、どういうオプションがあり得るのかということが重要。透明性の担保は言うまでもなく、リスクの高い使い方、例えばAIシステムが自然人のプロファイリングを実施するときには、常にハイリスクとみなすというAI規則のルールがある。その辺を踏まえて、リスク評価を必要とする取扱いや、許容できない使い方はあると思うので、それを整理すること、また、異議申立権がどの程度効果を持つのかは分からないが、そういう仕組みも拾っ

ていく。自動処理決定は、個人の権利として定められているが、これは禁止規定として理解されているので、何かしら取扱いの類型においては禁止すべきものがあるかもしれない。そのような整理が必要であるかということ。例えば脆弱な主体に働きかけるようなものや、機微な情報を扱うもの、それだけでもリスクがいかにも高まりそうなものがあると思うので、そういう仮定での検討が進められると良いかと思った次第。

（曽我部教授）

○　石井教授の資料、あるいは今のコメントと私の資料は、矛盾はないと思っている。私の先ほどのアセスメントのところは、個人情報保護法の守備範囲内での規律と記載させていただいており、例えばターゲティング広告への利用禁止のようなものは、個人情報保護法というよりは、消費者保護法の領域なのかと思っており、石井教授は、そういったものも含めて、割と幅広な観点からいろいろな規律を挙げていただいているのに対して、私の今の段落の趣旨としては、個人情報保護法、プロパーの中で柱となる規律と考えたときに、プロファイリング過程の適正性の確保が一番重要なのではないかという御提案。そういう意味では、石井教授の御議論、あるいは資料とは特段矛盾はなく、若干観点が違うということかと思っている。

（事務局）

○　いろいろな守備範囲とか消費者政策、あるいは競争政策その他との関係が深まっている、連携しないといけないところが増えている気がする。AI などが典型だが、様々なリスクをどういう守備範囲でカバーするのか、その場合に委員会がどういう立ち位置で何をするのかということについて、委員会だけで考えていてもしようがないところがあることはよく分かっており、できれば国内でも消費者庁なり、公正取引委員会などと改めてそのような議論をし、問題意識を共有することも進めたいと考えている。

以上