消費者委員会　消費者をエンパワーするデジタル技術に関する専門調査会（第8回）
議事録

内閣府消費者委員会事務局

消費者委員会　消費者をエンパワーするデジタル技術に関する専門調査会（第8回）
議事次第

1．日時　令和6年9月24日（火）13:00～14:57

2．場所　消費者委員会会議室及びテレビ会議

3．出席者

（委員）

【会議室】

橋田座長、森座長代理、坂下委員

【テレビ会議】

相澤委員、荒井委員、田中委員、鳥海委員、原田委員、松前委員、山口委員

（オブザーバー）

【テレビ会議】

大澤委員、柿沼委員、黒木委員、山本委員

（事務局）

小林事務局長、後藤審議官、友行参事官、江口企画官

4．議事

（1）開会

（2）①森座長代理プレゼンテーション

②松前委員プレゼンテーション

③大澤委員プレゼンテーション

（3）閉会

≪1. 開会≫

○橋田座長　本日は、皆様、お忙しいところをお集まりいただきまして、ありがとうございます。

ただいまから、消費者委員会第8回「消費者をエンパワーするデジタル技術に関する専門調査会」を開催いたします。

本日は、森座長代理、坂下委員は会議室で、相澤委員、荒井委員、田中委員、鳥海委員、原田委員、松前委員、山口委員はテレビ会議システムにて御出席いただいております。山口委員は少し遅れて参加されます。

消費者委員会からオブザーバーとして柿沼委員、黒木委員、山本委員はテレビ会議システムにて御出席いただいております。今回は大澤委員にもオブザーバーとしてテレビ会議システムにて御参加いただいております。

なお、本日は所用により星野委員は御欠席との御連絡をいただいております。

また、本日は、森座長代理、松前委員及び大澤委員に御発表をお願いしております。

それでは、本日の会議の進め方等について、事務局より御説明をお願いします。

○江口企画官　議事に入る前に配付資料の確認をさせていただきます。お手元の議事次第に配付資料を記載してございます。もし、不足等がございましたら事務局までお知らせください。

本日は、報道関係者を除き、一般傍聴者はオンラインにて傍聴いただいております。議事録については後日公開いたします。

以上でございます。

○橋田座長　これまで3回にわたり今後期待される消費者をエンパワーするデジタル技術の活用について御発表を伺い、意見交換をしてきました。

今回は社会実装に向けた課題等の整理について議論していきたいと思います。議論するに当たって、森座長代理、松前委員及び大澤委員より御発表いただいた後、質疑応答・意見交換をさせていただく予定です。全体を通じて委員からの積極的な御発言をお願いいたします。3人の方にまとめて発表いただいた後に議論と、普段とフォーマットが違いますので御注意ください。

まずは森座長代理から20分程度で御発表をお願いいたします。

≪2. ①森座長代理プレゼンテーション≫

○森座長代理　御紹介いただきました森でございます。

本日は「外部送信に関する規制と消費者問題のドグマ」というテーマでお話をさせてい

ただきます。スライドがたくさんありまして、時間はあまりありませんのでかいつまんで御説明をしたいと思います。

また、外部送信という皆様がお好きでないテーマかもしれませんけれども、聞いていただきますと必ず分かっていただけると思いますので、よろしくお願いいたします。

目次ですけれども、こんな感じで4つお話しいたします。1番、広告のためのデータの収集ということでcookieなどの御説明をしまして、2番、データベースの濫用と個人情報保護法の改正、この問題に対して個人情報保護法がどのように入ってきたかということです。3番、データベースの濫用と電気通信事業法の改正、電気通信事業法側からも手当てがされているということです。最後に消費者保護のドグマということで、本日申し上げたかったことを申し上げるということになっております。

まず、広告のためのデータ収集ということですけれども、cookieによるウェブ閲覧履歴の追跡ということでございます。この問題が法律の世界にはっきりとした形で入ってきたのは2018年（平成30年）に、個人情報保護委員会がFacebookの米国の本体を「次のとおり指導を行いましたのでお知らせします。」「いいねボタン」が設置されているウェブサイトを閲覧した場合、ボタンを押さなくてもユーザーIDやアクセス履歴等の情報がFacebook社に送信されてしまう事案」ということで法律の世界に入ってきております。これは以前からいろいろな議論がありましたけれども、ここではっきりと入ってきているということです。

皆様御案内の方もいらっしゃるかと思いますけれども、cookieとはということで、cookieとサーバーについての一般的な御説明をいたします。

ブラウザがサーバーにアクセスしますと、初回のアクセスでサーバーからブラウザに対して識別番号、識別子（cookie）が書き込まれます。2回目以降、ブラウザが同じサーバーにアクセスすると、ブラウザからサーバーにそのcookieを送信します。cookieにはドメインが書かれていて、サーバーの名前が書かれていて、同じサーバーにcookieを送り返す。違うサーバーからもらったものを送り返すのではなく、同じサーバーからもらったものを送り返します。ですので、あるサーバーから123番という番号が振られていれば、そのサーバーに123番のcookieを送り返す。そうすると、サーバーのほうは123番がまた来たなということが分かるということです。

どうしてこんなことをしているのかということですけれども、私がユーザー認証の必要なウェブサイトに入ってコンテンツを楽しく見まして、次のページを読もうと思って次のページに行ったとすると、もう一度パスワードを入れてください、そういうのは非常に困るわけです。ですので、サーバー側でこのブラウザは先ほど来た123番だから、先ほどユーザー認証したばかりだから通してやろうということになっております。

私はモールでビールを買いまして、そういえば、電球が切れたから電球も買おうということで、電球のほうに行きましたら買い物かごが空になっている、そういうことは困りますのでcookieでサーバーを区別して、123番は先ほどビールを買った人だから買い物かご

をそうしておかなければいけないなというようなことをするために、このようになっておるということでございます。

これは広告の場面、サーバーが2つになりますのでややこしくなりますが話は同じです。私はサッカーとかボクシングの結果を見るために毎晩スポーツ新聞のサイトを見ております。○×スポーツと仮にしておりますけれども、閲覧しにいきますと、このピンクのところにサッカーの結果とかそういうものが表示されてくるわけです。そのとき画像という白い部分が抜いてありますけれども、これは広告がここにあるわけです。広告に関しては○×スポーツのウェブサイトにあるのではなくて、広告事業者のサーバーにあるものをダウンロードしてきて一緒に合体させて見せているということです。

②のところですけれども、もちろんこのピンクのコンテンツが来まして、このときにタグと呼ばれる短いプログラムをブラウザが読み込みまして、このタグに「広告事業者のサーバーにアクセスして広告画像を取ってこい」という指示が書いてあります。はい、分かりましたということでブラウザがアクセスをするわけですけれども、サーバーとブラウザの関係ですので当然cookieのやり取りがある。私が初めて○×スポーツにアクセスしたときにcookieをもらってきておりまして､2回目以降はそれを○×スポーツに返しているということです。

タグの指示で私のブラウザが「分かりました！」ということで、右側の広告事業者サーバーにアクセスします。④です。画像をもらってきますけれども、このときサーバーとブラウザの関係ですのでcookieのやり取りが発生する。それが⑤です。私はこのタグによる指示を受けて、私のブラウザが広告事業者のサーバーにアクセスしていることには気付かないということです。私が見ようと思って見にいっている○×スポーツのウェブサイト、これをファーストパーティーといいます。タグの指示でブラウザが自動的にアクセスしているウェブサーバーをサードパーティーといいます。

したがって､ファーストパーティーからもらってきたcookie､ここでは左側の吹き出し、「○×001」としておりますけれども、これがファーストパーティーcookie、サードパーティーからもらってきたcookie、ここではAD、広告なのでサーバーの名前はADです。仮にADとしておきます｡このサードパーティーcookieは仮に｢AD123｣にしているということです。タグの指示で自動的にアクセスして画像をもらってくるという④⑤のところ、これを外部送信といいます。

次のスライドは④⑤のところを大きくした感じになっておりまして、通し番号も同じなのですけれども、何が説明として付け加わっているかといいますと、⑥のところなのですが、④のタグによるアクセス、自動的に指示を受けてブラウザがアクセスするわけですけれども、このアクセスの際に、広告事業者サーバーとしては、誰の指示で来たか、誰のタグを踏んで来たかということが分かるようになっております。○×スポーツのタグを踏んで来たことが分かるようになっております。幾つか方法がありますけれども、例えばファーストパーティーcookieをタグがブラウザに送らせるということがあるのです。広告事業

者サーバーにアクセスしてファーストパーティーcookieを渡しなさいということになりますと、先ほどのファーストパーティーcookieとしてブラウザがもらっている「○×001」を広告事業者サーバーに渡す。そうすると、これは○×スポーツを踏んで来たのだなということが分かる仕組みになっております。

○×スポーツの指図で来たのだなということが分かる結果として、広告事業者サーバーとしては、このサードパーティーcookie「AD123」のブラウザは、ここに来る直前に○×スポーツを見たということが分かるわけでございます。

広告事業者サーバー、実はすごい顔が広くて、いろいろなウェブサイトにタグを置いてもらっています。ですので、私もスポーツ新聞ばかりを見ているわけにいきませんのでいろいろなウェブサイトを見るわけなのですけれども、実はその都度、私のブラウザはそのウェブサイトのタグ、例えばウェブサイトＡとありますけれども、その次に見たウェブサイトＡへのタグの力で、またまた広告事業者サーバーにアクセスをして、そことやり取りをしている。広告事業者サーバーとしては「AD123」がまた来たではないか、先ほど来たばかりなのにということで、先ほどは○×スポーツだけれども、今度はウェブサイトＡのタグを踏んで来たのだなということが分かるわけでございます。

そのようにいたしまして、こんな感じで「AD123」のブラウザのアクセス履歴を広告事業者サーバーは把握することができるということでございます。このようにしてつくったデータベースをDMPのデータベースといいます。

こういう行為は非常に一般的に行われています。ほぼ全てのウェブサイトにタグが置いてある。Googleに関していうと、ほぼ100％近いウェブサイトに置かれているということです。そのようにして、ウェブの閲覧履歴を皆様例外なく取得されているわけです。当初問題だというような話もあったのですけれども、特に日本では個人情報ではないということもあって、長い間事実上容認されてきたということでございます。

問題点ですけれども、3ポツのところに書かせていただきました。閲覧者に分からない形で収集されているということ、それから、極めて大々的に行われているというこの2つが問題です。多くの人、私も含めてウェブを閲覧する行為をプライベートな行為と考えているということです。それはどうしてかというと、新聞を読んだり雑誌を読んだりする同じ気持ちで私たちはウェブブラウジングをしております。私が新聞のどの記事を読んでいるか、電車の中とかだったら、よく注意すれば分かるのかもしれませんけども、普通は分からない。雑誌もそうでございますが、ウェブサイトに関しては誰かに完全に把握されている、プライベートな行為ではないということです。

その次に、インターネット広告表示の仕組みというのがありますけれども、これは時間がありませんので省略をさせていただきまして、資料だけ御参考に残してあります。

Facebookの何が問題かというところからお話をしたいと思います。事実上許容されていたと言っているけれども、先ほどFacebookが行政指導されたとかいう話があったよねと、実は○×スポーツに広告事業者が置いているタグもFacebookが置いている「いいねボタン」

も同じ機能を持っております。したがって、この左も右も同じということです。

Facebookは行政指導されて広告事業者はどうして事実上許容されているのですかということですけれども、Facebookは実はこのように私自身が登録した情報を持っているということです。そして、その登録情報と一緒に「AD123」のブラウザのアクセス履歴を管理しておりますので、Facebookにとっては、これはどこの誰か知らないけれども、とにかく「AD123」のブラウザのウェブ閲覧履歴ということではなく、私、森亮二のウェブの閲覧履歴であるというものとしてこれを管理していることになります。「いいねボタン」の仕組みも同じですので、「いいねボタン」のあるウェブサイトに行けば、ボタンを押さなくてもウェブの閲覧履歴が収集されまして、それが個人情報として集められてくるということです。

Facebookの場合は一般の広告事業者と違って個人情報として取得しているということです。そうしますと、個人情報を偽り、その他不正の手段により取得してはならないという20条1項、適正取得義務というものがありますけれども、これに違反している可能性があるのではないのかということで、行政指導の対象になったということでございます。

そうこうするうちに、SNSではない、FacebookではないDMP事業者のサービスで個人情報に紐付けるものが出てきます。それを私は「2人Facebook」と勝手に呼んでいるわけですけれども、どういうことかと言いますと、Facebookの場合は登録情報を持っておりましたから、それは私が自分で入力したものですけれども、それで個人情報となりました。しかしながら、そうではない場合、例えば広告事業者、DMPを持っている事業者が、自分としては誰か分かりませんけれども、それを事業会社に提供して、そこで個人情報になるという現象ができてきたのです。

私は○×スポーツの登録ユーザーでして、○×スポーツ的には私が来たらファーストパーティーcookieを見て、これは森亮二だなと分かるわけですけれども、当然○×スポーツとしては自分のウェブサイトの中のどこを見ているかということしか分からない。サッカーとボクシングだけということ、ところが、もしかしたら、ほかのスポーツにも関心があるかもしれないし、何かほかのお勧めができるかもしれないということで、DMPのウェブの閲覧履歴などを買ってくるというサービスが出てくるようになります。例えば化粧品のECサイトなどはすごく規模も大きいですし、また、いいレコメンデーションをしてくれるのです。そう聞いております。

彼らからしてみれば、これまでどんなものを買いましたかとか、登録情報で年齢が分かるとか、体質が分かるとか、そういうのは分かるのですけれども、できれば他のことも知りたい、スポーツをする人ですかとか、食べ物はどんなものが好きですかとか、外に出て赤外線に当たりますかとか、そういうことが分かればもっといいレコメンデーションができるのです。ですので、自分のドメインの外でそのユーザーがどのように行動しているかということを知るということは、B to Cの事業者にとっては非常にありがたいこと、非常に需要のあることです。しかしながら、逆にユーザーからしてみれば、名前とかをさらして付き合う事業者が日々のウェブの閲覧履歴を把握しているというのはいただけない話で

はないかということでございます。

そうこう言っているうちにリクナビの事件が起こりました。これがまさに「2人Facebook」のケースになりますので、この点について御説明をしていきたいと思います。リクナビ事件ですけれども、どんな事件だったかということですが、リクルートキャリアが就活中の学生が内定を辞退する確率、内定辞退率を判定したデータを契約する採用企業に販売していたことが判明しました。

内定辞退率なんて、その就活生がどのぐらいの割合でうちの会社の内定を蹴るのかということですから、そう簡単に分からないような気がいたしますけれども、どのように計算していたかといいますと、2ポツのところ、①採用企業から提供を受けた過去の内定辞退状況、こういう人がこれぐらい辞退している、そうすると、この人も同じではないかということ、②就活生の登録情報等、学歴ですとか、英検何級ですとか、そういうことでしょうか、これも重要でしょう、③就活学生の就活サイトと内外のウェブサイトの閲覧状況を基にAIによる分析、このウェブサイトの閲覧状況こそ問題なわけですけれども、実はリクナビの事件は途中から変更があるのですけれども、途中まではリクルート側では個人情報でなく、採用企業に行くと個人情報になるという仕組みになっておりましたので、その前提でお話をさせていただきます。

左側の絵は事件直後にリクルートキャリアのウェブサイトにあったものをコピペしているだけですが、契約企業、採用企業といったほうが分かりやすいと思いますので採用企業といいますけれども、①②③に何て書いてあるかと言いますと、①ではcookie情報が採用企業からリクナビへと書いてあります。②はリクナビではそれをリクナビのcookie情報と突合してスコアを算出と書いてありまして、③ではスコアを採用企業に納品と書いてあります。この①②がどういうことか分かりにくいので、これを推測も交えて解明していきたいと思いますけれども、恐らくこんな感じではなかったか。

まず、採用企業側で就活生の皆さんに就活生アンケートというものを取ります。そうしますと、その就活生は当然のことながら全員このアンケートのフォーマットをダウンロードします。このとき当然ファーストパーティーcookieのやり取りが就活生のブラウザと採用企業のウェブサイトの間である。

そして、就活企業のウェブサイトには、このピンクのところのアンケートのクエスチョンに加えてタグが置いてありまして、リクルートサーバーから画像を取ってこいという指示が書いてあります。これは別に広告を貼る必要はないので広告ではなくて何でもよいので、アクセスさせるためだけに画像を取ってこいと言っているので、画像は極めて小さく見えないもの、透明なものでもよいわけです。就活生のブラウザは、はい、分かりましたということで、自動的にリクルートのサーバーにアクセスをいたしまして、画像をダウンロードして、そこにサードパーティーcookieのやり取りが生じるということになります。先ほどと同じです。採用企業側のファーストパーティーcookieは「saiyo001」、リクルート側のサードパーティーcookieは「リクルート123」としてあります。

リクルートは顔が広くて様々なウェブサイトにタグを置いてもらっていますけれども、これは広告事業者とは少し違いまして、様々と言ってももっぱら就活系のウェブサイトにタグを置いてもらっているということでございます。したがって、就活生が採用企業のウェブサイトでアンケートを答えた後に就活系のウェブサイトにアクセスをしますと、その履歴がこのようにして把握できることになります。「リクルート123」のブラウザのアクセス履歴はこのようになっています。IT就活、外資系就活、メーカー就活、外資系就活、外資系就活、ポータル、ニュースということになりますので、もし、採用企業が純然たる国内企業であったならば、これは結構内定を蹴る確率が高いと、そのようなサービスです。

そして、それがどのように個人情報になるのかということですけれども、先ほどの絵を補足的に説明したのがこちらでして、採用企業のcookie情報というのは恐らく採用企業のファーストパーティーcookieでありましょう、それがリクナビに行きまして、リクナビではそのファーストパーティーcookieと自分のサードパーティーcookie「リクナビ123」を組み合わせて、閲覧履歴をベースにスコアを算出します。リクナビはcookieを2つ持っておりますけれども、これが誰かはリクナビには分からない。

3番でスコアを採用企業に納品しますが、納品されたスコアのデータベースには採用企業のファーストパーティーcookieがついておりますので、採用企業としては最初にアンケートに答えてもらったときに、ファーストパーティーcookieのやり取りプラス、ここにアンケートの回答者の名前が書いてありますので、これが誰それくんのスコアであるということが分かる、そういうサービスではなかったかということでございます。そんなことが原因となりまして、これを個人関連情報、法制度で対応しようということになりました。

リクナビについてのまとめですけれども、DMP、データベースは広告だけに使われるものではないということが広く認識されるきっかけになりました。内定辞退率みたいなものを計算できるということです。

3ポツですが、その人はどんな人という質問に幅広く答えられます。これまで広告として、その人は何を買いそうかということであればオーケーであったわけですけれども、内定を辞退しそうかとか、職場に満足しているかとか、そういうことに関しては当然抵抗があるはずであります。

個人関連情報という制度ができましたが、それについては提供先で個人情報に戻すというところに着目して、もちろん個人情報ではないと個人情報保護法で規制できないので当然なのですけれども、個人情報に戻すというところに着目して、もし、提供先で個人情報に戻すのだったらば、本人の同意を得たことを確認してから提供しなければいけないという規制になったわけでございます。

続きまして、電気通信事業法のお話をしたいと思います。先ほどは、結局個人情報に戻すところで規制するという話なのですけれども、引っかかるのは情報を集めるところ、外部送信はどうなのと誰もが思うところでございます。

これは電気通信事業法の改正を議論したガバナンス検討会の報告書なのですけれども、

個人的法益、社会的法益、国家的法益とありまして、個人的法益はもちろんプライバシー等なわけですが、社会的法益、健全な言論環境の確保とか、3番の国家的法益、健全な民主主義システムの確保とか、こんな大きな話になっているけれども、これは何なのかといいますと、これが実はケンブリッジアナリティカ事件から来たものでございます。

ケンブリッジアナリティカ事件は御案内かと思いますが簡単に復習をしておきますと、2016年の大統領選挙でトランプを支持し、英国のブレグジットで離脱派を支援したとされるコンサルティングの会社でして、事件自体は2018年にクリストファー・ワイリーという人が告発して発覚をしております。

どんな事件だったかといいますと、ケンブリッジ大学の研究者が心理クイズアプリを作成しまして、このアプリをFacebook上でダウンロードした30万人のユーザー、彼らが友達として登録していたユーザー計8700万人のデータをFacebookから取得します。これは漏えいでも何でもないです。これはそういう仕組みになっていたということです。このデータベースについて心理学やデータ分析、あと、テクノロジーなどの専門家チームがマイクロターゲティングの手法で詳細なプロファイリングを行いまして、神経症で自意識過剰であるとか、陰謀論に傾きやすいとか、怒りに流されると分析されたグループに対して政治広告を出しまして、愛国者団体の集会に誘うなどしまして先鋭化させていったということなのです。

これは告発本なのですけれども、非常にすごい本ですので、ぜひお読みいただきたいと思います。さわりのところを引用しておりますけれども、時間がないので省略をさせていただきます。どんな誘導をしていたかということなのですけれども、Facebookのデータベースを使ってプロファイリングをして、例えば衝動的怒りに流される人を探します。この人に対してメッセージを出していくわけなのですけれども、フェイクグループ、ケンブリッジアナリティカが勝手につくったグループです。何々郡愛国者とか、そういうもっともらしい名前がついている、そこに誘い込んでエコーチェンバーの効果で先鋭化させるということです。DMPのデータベースを持っておりますので、これをうまく分析すれば、怒りに流されるとか、陰謀論に弱いとかが分かってしまうということなのです。

ケンブリッジアナリティカの教訓ですけれども、選挙に影響を与える目的ですが、その過程で社会の分断が生じるということがあります。選挙に影響を受けるということは、国の在り方に影響されるということです。そして、証明はされていないのですけれども、外国の関与、ロシアの関与があったのではないかとも言われておりまして、そうなってくると、安全保障上の問題もあるということです。

どうしてこんなことになったのかということですけれども、それは詳細なプロファイリングが可能なFacebookのユーザーデータベースがあったから、そして、一人一人に出し分けられる広告配信の仕組み、レコメンドの仕組みがあったからです。それらによって人が操作されまして、狙いどおりの行動を取ることになったのではないかということです。そして、操作された人たちは大統領選の結果、2020年のバイデンが勝った大統領選すら信じ

られなくなって、さらなる国家的混乱を巻き起こすことになりましたということです。ちなみに2023年、去年なのですけれども、ブラジルでも連邦議事堂突入事件と同じような事件が起こっています。これは背景にケンブリッジアナリティカみたいなものがいたのか、いなかったのか全く分からないのですけれども、あまりにも事件としてはよく似ていたということでございます。

こういうことに対応して、ボトムアップで、つまりユーザーリテラシーで対応しようではないかという話が日本でもありました。これは時間がありませんので省略をさせていただきまして、電気通信事業法はそんなことも踏まえつつ、今の社会的法益と国家的法益もそうなのですけれども、外部送信というのは個人的法益ももちろん問題になるわけです。

電気通信事業法というのは、もともと通信サービス利用者の保護とか通信の信頼確保を目的としています。そして、そのためにこれまでは通信の秘密という考え方で通話とかメールとかを守っていたわけです。それは実際守られていたわけですけれども、今、スマホを使って皆さんが何をされるかといいますと、通話をしたりメールをしたりする時間よりも、ウェブサイトを見たりアプリを使ったりする方がはるかに長いということです。ところが、こちらが守られていない、こちらが筒抜けになっているという問題があるわけです。ここを通信関連プライバシーということで守っていきましょうということになります。

順番でいうと、最初の外部送信のところに規制をかける、これが電気通信事業法の規制になったわけでございます。黄色いのは先ほどの個人情報保護法の規制です。電気通信事業法の規制、義務を負う人が限られていて狭い、それから、義務の内容が通知・公表にとどまっている、オプトアウトぐらいあってもよかったのではないかと思いますけれども、そういう問題はありますが、このようになりましたということです。

最後に、消費者保護のドグマということで、ドグマという言い方はよくないのかもしれませんけれども、あえて申し上げたいと思います。

消費者保護に2つのドグマがあったのではないかと思っておりまして、第1のドグマは消費者被害とは金銭的被害と健康的被害であるというドグマです。第2のドグマは、消費者被害は契約によってもたらされるというドグマです。しかし、本日お話しました外部送信の問題においては金銭被害とか健康被害は起こらないということです。それから、契約関係が全くない事業者によって閲覧履歴の収集が行われることが十分あり得るということです。同じようなことは、現代社会ではしばしば起こります。公共の場所に設置されたカメラ等のセンサー、それから、IoTの場合、家電ですから家電メーカーと直接の契約はありません。製造物責任を問うことはできるかもしれませんけれども、契約があるのは買ってきた小売の販売店だけということです。

だけれども、データを取られるだけだから大したことはないのではと、いえいえ全くそんなことはありません、2ポツのところを見ていただきますと、消費者にとって不利なことを知られる、これがリクナビ事件でした。それから、脆弱性プロファイリングに基づく操作を受けることがありました。これがケンブリッジアナリティカ事件でした。

最後ですが、現在の消費者保護は2つのドグマから離れるとともに、インターネットやプラットフォームが社会に与える仕組みを理解して、消費者に対する搾取が現在どのように行われているかを把握する必要があるということでございます。

以上です。御清聴ありがとうございました。

○橋田座長　ありがとうございました。

ディスカッションは後でやりますので、次の御発表に移りたいと思います。

「プライバシー・個人情報保護等の観点から留意すべき点」などについて、松前委員より20分程度で御発表をお願いいたします。

≪2. ②松前委員プレゼンテーション≫

○松前委員　では、私からは「プライバシー・個人情報保護の観点から留意すべき点」というタイトルでお話をさせていただきます。

まず、本日、消費者をエンパワーする技術について、プライバシー・個人情報保護の観点から留意すべき点というお題を事務局からいただいておりますけれども、そもそも消費者をエンパワーする技術とプライバシー・個人情報保護との関わりというものを考えたときには、一応2つの側面を挙げることができるかと思います。

一つが、まず、消費者をエンパワーする技術の開発・提供等のために一定の個人情報の処理が必要な場合、これは本調査会でも紹介されていたかと思いますけれども、例えば高齢者の見守りのためにカメラで高齢者の様子を撮影するとか、移動履歴を把握するとか、あとはパーソナルAIアシスタントなどに関してパーソナライズのために個人情報の収集が必要になってくるといった場合です。

もう一つ、これは今御説明した側面と重なるところもあるのですけれども、個人情報のコントロール自体に関して消費者をエンパワーする技術というものもあります。これは技術によるエンパワーの対象が個人情報の管理やコントロールであるという意味ですけれども、本調査会ではこういった技術の例として、同意管理ツールやプライバシー保護技術等々が紹介されていたかと思います。

そこで、本日の報告の流れですけれども、最初に、消費者をエンパワーする技術の開発・提供の際に個人情報の処理が必要な場合というものを念頭に置いて、プライバシー・個人情報保護の観点から留意すべき点についてお話をしたいと思います。この際、ひとつ御承知おきいただきたいのが、この調査会では様々な技術が紹介されてきたかと思いますけれども、どのようなプライバシー・個人情報保護の問題があるかというのは、それぞれの技術の開発・提供等においてどのような個人情報をどのように利用するかというところによって様々な論点があり得ますので、あくまでも一般的な論点の紹介ということで御承知お

きいただければと思います。

続けて、2つ目情報主体のコントロールに関する議論というところですけれども、先ほどお話ししたように、これは情報主体の個人情報に関するコントロールのエンパワーという技術にも関連してきますし、そもそもプライバシー・個人情報保護の議論では、個人情報のコントロールというのは一つの重要な論点になっておりまして本調査会でも議論の俎上に上っていたかと思いますので、情報主体のコントロールに関する議論も少し御紹介させていただきまして、最後に若干の考察という形で進めたいと思います。

まず、プライバシー・個人情報保護の観点から留意すべき点ですけれども、こちらは先ほども申し上げましたとおり、それぞれのエンパワー技術との関連で、どのような個人情報をどのように利用するかというのはそれぞれ異なってきますので、様々な技術の開発・提供等においてそれぞれ、ここに書いてあるものは本当に一例ですけれども、多様な個人に関する情報が収集される可能性があるということになります。

一応参考として、皆様御案内かと思いますけれども、日本の個人情報保護法制、特に今回民間部門の方が関わりが強いかと思いますので、民間部門のルールの概要を挙げておきました。そもそも個人情報保護法の適用があるのか、取得、利用、保管、管理、第三者提供の各段階での義務、それから、開示請求等への対応等、様々なルールがありますので、この辺りに配慮しながら個人情報を取り扱っていく必要があるということが、まず大前提になります。

これを前提として、特に留意すべき点を幾つか挙げるとすると、まず、収集・利用される個人情報の種類については、2つ目の四角の要配慮個人情報、海外ではセンシティブ情報といったりもしますけれども、ここに該当するような場合には注意が必要になるかと思います。これは人種、信条、社会的身分、病歴、それから、犯罪の経歴等など、本人に対する不当な差別・偏見、その他の不利益が生じないように、その取扱いに特に配慮を要する情報と定義されますけれども、これに関しては取得に際して原則として本人同意が必要になりますので、ここは特に高齢者の見守り等々の場面においては注意が必要になってくるかと思います。

それから、身体に関する情報と書いておきましたけれども、最近規制が強化される傾向にあるのが、この身体周りの情報になるかと思います。ここには顔情報、音声情報、バイタル情報等と挙げましたけれども、これらの中にはもちろん個人情報に該当するものもありますし、要配慮個人情報に該当する場合もあると思いますので、それぞれ情報の性質に応じて適切な取扱いが必要になるかと思います。

一つ注意すべき点として※のところですけれども、仮に要配慮個人情報に該当しなかったとしても、例えば見守りカメラなどを想定しますと、極めてプライバシー性の高い情報が収集される可能性もあります。こういった場合はプライバシーの権利との関係でも、取扱いに注意が必要になってくるというところが留意すべき点かと思います。

また、下に2つ挙げておきましたのは、これは身体に関する情報に関連して最近国際的に

規制強化がされているところです。例えばAI顔識別技術に関しては特に公的機関、法執行機関が公共空間においてAI顔識別技術を使うといったようなことがAI規則ですとか､あと、米国の幾つかの都市で禁止されていたりします。また、感情認識技術、これは表情や声の感じなどからその人の感情や意図などを分析するものですけれども、これもAI規則において規制が必要なハイリスクのAIシステムであると位置付けられておりますので、この辺りも留意点になるかと思います。

次ですけれども、情報主体の性質と書きましたが、この調査会でも消費者の脆弱性というものに注目して消費者をエンパワーするというところが一つの大事なポイントになっているかと思います。個人情報保護の世界でも脆弱性のある主体の個人情報については特別な配慮が必要だと言われています。特に脆弱性のある主体として挙げられているのが、高齢者、子どもといった主体になります。例えばEUのGDPR前文75条では、個人データの取扱いによるリスクが生じ得る場合の一つとして脆弱性のある主体に関する場合というものを挙げておりまして、GDPR自体はこの例示として子どもだけを挙げているのですけれども、EUの29条作業部会が出している関連文書等々を見ますと、子どものほか、高齢者であるとか、障害を有する人、被用者等がこの脆弱性のある主体に含まれ得るということが言われています。

こういった脆弱性のある主体に関しては、自身の個人情報の処理が含むリスクについての認識であるとか、理解の能力が不足する傾向がどうしてもありますので、例えば個人情報の処理に関する通知・同意、あるいは権利行使の場面においては特別な配慮が必要であるということが言われています。特に子どもの個人情報に関しては、今日は時間の関係で説明を割愛しますけれども、国際的に規制強化の流れがあるということは申し添えておきます。

もう一つの注意すべき情報主体としては、ユーザー以外の第三者というのがあります。この調査会でも議論があったかと思いますけれども、特にスマートデバイス等、スマホにしても、スマートTVやスマートスピーカー等々にしても、音声だったり映像だったりいろいろありますけれども契約しているユーザー以外の第三者の個人情報が入り込んでしまう可能性がありますので、こういったユーザー以外の第三者の個人情報の処理について、例えば通知・同意をどうするのかといったようなところも問題になってくるかと思います。

今お話しした通知・同意に関しては、消費者のエンパワーのための技術ということで、今回は特に民間部門を中心に考えているかと思いますので、通知・同意をどのように行うかというのは極めて重要な論点の一つになるかと思います。

通知・同意の在り方に関して、まず、個人情報保護法制や関連の法政策においては、いわゆる通知・選択アプローチ、要するに本人に通知して、本人が選択をするというようなアプローチの重要性が国際的に重視されてきております。

日本の個人情報保護法では通知・同意がどういった場面で求められているかというと、まず通知に関しては、利用目的等を通知・公表する、それから、個人データの第三者提供

に関するオプトアウトの際の通知といった場面で通知が要求されています。

同意に関しては、一般の個人情報の取得については日本では同意は不要なのですけれども、先ほどお話ししたように要配慮個人情報の取得の場面では原則として同意が必要になります。また、目的外利用を行う場合や、外国にある第三者も含みますけれども第三者提供の場面でも原則として本人の同意が必要になってきます。

一方で、通知・同意をめぐっては、前回も議論になっていたかと思いますけれども、最近いろいろな課題が指摘されてきていまして、一つには通知を認識するのが難しいという問題があります。通知というのは多くの場合、プライバシー・ポリシーの形で行われますけれども、これ自体が非常に小さかったりして見えにくい、どこにあるか分からない、それから、非常に膨大である、頻繁に表示されるということで、結局プライバシー・ポリシーを読まない人が多いという点が問題視されています。また、読んだとしても専門用語が非常に多いとか、あとは個人情報の将来的な処理も含めてリスク判断をするのは一般の消費者にとっては極めて難しいといったことが言われていて、プライバシー・ポリシーを読んでも十分に理解できないといった問題もあります。

こういった通知・同意をめぐる課題というのは、先ほどお話しした高齢者や子どもに関してはより深刻化する可能性がありますし、IoTの文脈ではスマートデバイスやセンサーはかなり小さいものが多いので通知を有効に行い得るスクリーンがない、ビックデータ・AIの文脈においては、そもそもどのように個人情報を利用しているのかがより分かりにくくなるといったところで、こういった通知・同意をめぐる課題というのがより深刻化しているというのが現状です。

また、基本的に同意というのは自由意思に基づいて、任意のものとして行われることが必要になりますけれども、デジタル社会においては皆さん御案内のとおり、様々なサービスを使うときに不可避的に個人情報の処理が求められる場面がかなり多くなっていますので、結局は個人情報の処理に同意してサービスを使うのか、あるいはサービスを使わないかの二者択一のアプローチを迫られることになるという問題があると言われています。

さらに、選択・意思決定に付随する様々なバイアスの問題も、もともとの人間の意思決定に関する問題として指摘されています。

こういった問題に関する対策ですけれども、法制度における対応策としては、一つには規制強化が行われているということがあります。これはあくまでも例ですけれども、通知に関してはGDPR、それから、アメリカのカリフォルニア州消費者プライバシー法（CalCPA）において、そもそもこの通知というのは読みやすい、理解しやすい態様で行うべきであるということで、そういった態様で通知を行うことを義務付けるものや、通知の具体的な形式や手続等について、かなり細かな規定を置くような場合もあります。同意に関しては、GDPRが有名ですけれども同意の要件を厳格に定めるという対応や、他の事項を含む一般的な利用規約への同意やダークパターンを用いて取得された同意は同意とは評価できないというような規定を置いているものもあります。このダークパターンに関する規定はカリフ

ォルニア州消費者プライバシー法の規定です。

ここまで通知・同意の話をしましたけれども、この調査会ではパーソナルAIのお話も出ておりましたので、AIに関しても少しだけお話しします。AIに関してはそれぞれの段階において個別の論点がありますけれども、重要な論点の一つになるのが機械学習の段階での個人情報の利用かと思います。

この点については、日本でも個人情報保護委員会がオープンAIに対して注意喚起をしていましたけれども、特に日本の個人情報保護法との関係では、先ほどから出てきております要配慮個人情報の取得について、特にウェブ上で公表されている情報を集めてくるような場合は同意を取るのがかなり難しくなりますので、そういったところが一つ問題になっています。

それから、EUなどにおいてはそもそも個人情報の処理行為全てについて同意を含む適法化根拠が要求されていますので、EUではどの適法化根拠に基づいて処理を行うのかといった辺りが、特にChatGPT等に関しては議論されています。

それから、個人情報を分析してその人の人物像や行動を予測するというAIプロファイリングですけれども、これはパーソナルAIアシスタント等に関連して問題になる可能性があるかと思いますが、AIプロファイリングについてはここに挙げているように様々な危険が指摘されています。

規制の動向、これも一例になりますけれども、例えばGDPRでは同意なくしてプロファイリングを含む自動化された意思決定の対象とされない権利が規定されていたり、あとは先ほども言及したAI規則では、許容できないリスクのあるシステムというところで4つ、詳細は割愛しますけれども、こういったシステムが禁止されていたりします。

ここまでプライバシー・個人情報保護の観点から留意すべき点についてお話をしてきました。

次に情報主体のコントロールについてですが、これは冒頭にも申し上げましたけれども、プライバシー・個人情報保護の議論においては非常に重要な論点の一つですし、また、コントロールに関するエンパワーメント技術もありますので、その辺りも含めてお話をしたいと思います。

情報主体のコントロールに関する制度ですけれども、まず、日本の個人情報保護法においては、実はコントロールという言葉は使われておりません。本人関与のための制度という位置付けで、開示・訂正等、利用停止等の各請求権や、個人情報の取扱いに関する本人の同意に関する規定が置かれています。

この情報主体のコントロールについては、現在、例えばEU・米国等において個人の権利を拡充したり強化したりする動きがあります。これに関しては、先ほどお話しした通知・同意に関する規制強化も含まれてきますけれども、それ以外の個人の権利というところでいいますと、例えばGDPRではデータ保護の権利というものを基礎として個人の各権利が規定されております。

また、カリフォルニア州消費者プライバシー法では消費者のコントロール――カリフォルニア州の消費者プライバシー法はコントロールという表現を用いていたりしますけれども――このコントロールのための各権利が規定されています。

これらの権利の内容について、一応参考として次のページに記載しておきましたけれども、アクセス権、これは日本の開示請求権に相当しますが、それから、訂正権、消去権に加えて、ここに挙げているような様々な権利が規定されています。ちなみにデータポータビリティーというのが日本でもよく議論になりますけれども、アメリカではデータポータビリティーを権利として規定するという例はあまりなくて、カリフォルニア州消費者プライバシー法でもあくまでもアクセス権の行使に関する事業者の義務として、消費者が別の組織に情報を移転しやすいようなフォーマットで開示しましょうといった形での規定が置かれています。

加えて幾つか注目すべき点を挙げておきますと、2つ目の四角ですけれども、個人情報の販売又は共有からのオプトアウトの権利というものも定められています。この共有には行動ターゲティング広告等も含まれるといわれていまして、オプトアウト選好信号による消費者のオプトアウトの方法が規則等で定められているところが特徴的な点になります。他にも、子どもの個人情報に関する特例や、センシティブ情報の利用を限定する権利、更にこれらの権利行使全般に関して不利益な取扱いを受けない権利といったものも定められております。

このようにEU・米国では個人の権利の拡充や強化の動きがありますが、自己情報コントロールないし自己情報コントロール権というものについては幾つか注意しておくべきというところがありますので、そこをお話ししておきます。

もともと自己情報コントロール権というのはプライバシーの権利の理解として、アラン・ウェスティンが1960年代に提唱したものです。実は当時からいろいろと批判もあったのですけれども、最近、特に自己情報コントロール権への疑義とか、その限界をめぐる議論というのがアメリカではもちろん日本でも、場合によってはEUでも見られるようになってきています。これは先ほどお話しした通知・同意の課題というところに象徴される問題でもありますけれども、そもそも自己情報のコントロールというものの実行可能性への疑義や、理論面での課題も指摘されております。

さらに言うと、個人情報保護法制における自己情報コントロールの位置付けというのも、もちろんこれは理念として強調されることが多いのですけれども、個人情報保護法制において本当にそれが中核的な権利として位置付けられるのかどうかといった辺りはいろいろ議論があるところですので、コントロールの重要性を否定するものではないのですけれども、情報主体のコントロールというものを考えるときには、その内容や範囲、あるいは仮にコントロール強化のための権利規定を作るとすれば、例外規定をどうするのかといった辺りの検討も必要になるかと思います。

それから、冒頭に申し上げたように、この調査会でも紹介されておりました情報主体の

コントロールに関するエンパワーのための技術というところも、少しだけ御紹介させていただきます。これについても様々な仕組みが提唱されていて、ここに挙げておりますのは全く網羅的なものではありませんし、必ずしも技術的な仕組みとは言いにくいものも含んでおりますけれども、個人情報保護法政策関連の文書でよく上がってくるものをピックアップしております。

例えば1つ目のところですが、今日お話しした通知・同意に関するコントロール強化の仕組みとしてはプライバシー・アイコン、これはどういう情報が処理されているか、情報処理をビジュアライズするようなアイコン、マークですけれども、こういったものを使うとか、あとは階層的な通知、これは一気にテキストでプライバシー・ポリシーを出すと、先ほどもお話ししましたように誰も読まないということが起こり得ますので、重要な情報や、どこにプライバシー・ポリシーがあるのかという情報を最初に出しておいて、そこからプライバシー・ポリシーに誘導して、最終的にはより詳しいFAQ等に誘導するといった形で通知を行うものですが、こういった仕組みも重要だと言われています。

他にも、プライバシー・ダッシュボード、GPC（グローバル・プライバシー・コントロール）は後でお話しします、それから、同意管理システムはどちらかというと事業者側の同意の管理の話ですけれども、こういったものが最近重要な通知・同意に関する仕組みとして挙げられています。

次に2つ目のところですけれども、パーソナル・プライバシー・アシスタントです。ユーザーのプライバシー選好を個人情報を分析してある程度決定して、自動でプライバシー設定を行ってくれたり、あとはアドバイスをくれたりといったようなものも考えられているようです。

それから、パーソナルデータストア（PDS）も記載しておきましたが、これは、OECDのプライバシー保護技術（Privacy Enhancing Technologies: PETs）に関する最近のレポートのように、PDSをコントロール強化のためのPETsの一つとして挙げる場合もあるということで一応記載しておきました。

今日特に申し上げたかったのは、3つ目の小さい四角になりますけれども、プライバシー・個人情報保護の世界では、こういった技術的な保護措置というものが法制度において要求される場合があるということです。例えばプライバシー・アイコンに関してはGDPRで義務付けではないのですが言及されています。また、先ほど御紹介したカリフォルニア州消費者プライバシー法における、個人情報の販売や共有からのオプトアウト選好信号による消費者のオプトアウトに関しても、司法長官が公表しているFAQで、例えばGPCを使えるのではないかという形で、手段としてGPCが紹介されています。これはウェブサイトの管理者に対してユーザーのプライバシー選好、この場合、データの販売や共有についての選好になりますけれども、これを伝えることができるような仕組みです。こういった技術的な仕組みに関して、法制度において言及されること、あるいは要求されることがあるというところが一つ、プライバシー・個人情報の世界において特徴的なところかと思います。

それに関連しますけれども、もともとプライバシー個人情報に関しては技術的な保護措置の重要性が言われてきておりまして、先ほど出てきましたPETsのほか、プライバシー・バイ・デザインやプライバシー・バイ・デフォルト等、法制度に組み込まれているものも結構あります。

ただ、これらのコントロール強化のための技術的な仕組みについては、それぞれ課題も指摘されておりまして、例えばプライバシー・アイコンのように通知を非常に簡単にしていくと、逆に透明性のパラドックスといって内容が分かりにくくなるという問題であったり、あとは技術によっては情報主体にある程度のリテラシーが必要になるものもありますので、そういったものについては個人の負担や責任が増大してしまうのではないかといった懸念、それから、技術の成熟度やインセンティブをめぐる問題といったものが指摘されています。

最後に、考察というほどでもありませんけれども、消費者をエンパワーする技術というところに関して一つ注意しておくべきことは、万能薬はないということかと思います。エンパワーのための技術の開発・提供において個人情報を使う場合はもちろんですけれども、仮に使わないとしても、例えばパーソナルAIについて消費者に情報提供、通知をするというような場合において、どうしても消費者の認識や理解の限界がありますので、脆弱性を持っている主体はもちろんですけれども、消費者一般に関してもこの辺りの問題を完全に解消することは困難かと思います。

ですので、その下の2つですけれども、場面や文脈に即して適切な技術を選択していくということや、必要に応じた法規制等との組み合わせといったところが重要になってくるかと思います。これについては先ほど御紹介したプライバシー・個人情報保護のための技術と法制度の在り方というところが少し参考になるかもしれません。プライバシー・個人情報保護の世界では、例えば法制度による技術の導入の義務付けをしたり、例えばPETsについて様々なガイダンスを出したり、成熟度評価の基準を出したりといった形で、技術の導入や実施に関するガバナンスも考えられていますので、こういったところは一つ参考になるかと考えております。

私からの報告は以上とさせていただきます。御清聴どうもありがとうございました。

○橋田座長　ありがとうございました。

次に「消費者をエンパワーする技術の活用及び事業者による消費者のデータの扱いに関する課題」について、大澤委員から10分程度で御発表をお願いいたします。

≪2. ③大澤委員プレゼンテーション≫

○大澤委員　御紹介いただきました大澤と申します。本日、消費者委員会の委員として単

発的に参加させていただいております。

最初に申し上げておきたいのですが、私がお話をいただいたときには、民法・消費者法の専門家として10分ぐらいでコメントをということでした。私が今日お話ししたいと思っておりますことは大きく分けると2点あります。

一つが、消費者をエンパワーする技術の活用ということで、その活用に当たって、それを実装する場合の課題を主には民法や消費者法の観点から、どちらかというと総論的に申し上げるところが1点目です。エンパワーする技術としては、具体的にこれまでの本専門調査会で取り上げられておりました過去の資料を見て参考にさせていただきました。

2点目がタイトルの後半の方ですが、事業者による消費者のデータの扱いがもたらす、例えば消費者のどのような利益が損害されているのか、あるいは、それに対してどういう対応があり得るのかというのを民法・消費者法の観点からお話ししたいと思います。

まず1点目ですが、消費者をエンパワーする技術の活用に当たってというところで、最初に申し上げておきたいことなのですが、私自身は消費者をエンパワーするために今のデジタル技術等々を使うということについては決して後ろ向きではありません。むしろ使える技術に関しては、消費者をエンパワーするためにぜひ活用したほうがよろしいのではないかというのは初めに申し上げておきます。

ですので、本日、民法及び消費者法を研究している立場から、この点はどのように考えればよいのでしょうかということで問題提起をする形になりますが、決してこういった技術を活用することを否定的に捉えて言っているわけではないということは、あらかじめ御理解いただければと思います。立場的に民法と消費者法を専門としている立場から、こういったことが問題になり得るのではないかということを申し上げたいと思っていますので、その点は御理解をいただけるとありがたいです。

まず、専門調査会でも恐らく論点として出てきたのではないかと過去の配付資料とかを見て思いましたけれども、消費者をエンパワーする技術をより推進するために、これを実施・実装するために、例えばどのような技術、消費者をエンパワーする技術としてきっちりとしたものであるという認証制度を設けるとか、今、製品等でも認証制度があると思いますし、あるいはいわゆるその消費者ファーストの経営をしている事業者を例えば表彰したり認証するというのは今でもあると思いますが、こういった認証制度ですとか、あるいは私の方で考えたのは消費者に例えばその技術を導入にするために、消費者に補助金とかを導入するということが、こういった技術を実装する上で、特にインセンティブを高めるためにはあり得るのではないかと思います。

例えば補助金として私がイメージしていますのは、これはデジタル技術ではないのですが、例えば今も複数の自治体で行われていますけれども、迷惑電話をブロックするような機能とか、あるいは電話の録音機能がついたような電話機を買うときに、自治体が希望する消費者に補助金を支払う、例えば5,000円支援をするとか、そういったものを想定しています。こういった補助金を導入することによって、消費者にこういった技術をぜひ使って

くださいとか、あるいは逆に事業者に対して認証制度を使うことで、事業者にこういう技術を積極的に開発してもらうということが考えられると思います。もちろんこういったことを実装するときには前向きに考えていい話ではないかと思っております。

事業者の認証制度に関しては言うまでもないことですが、技術を消費者の利益のために用いているということであれば、そういう事業者にインセンティブを与えるというのはもちろん検討すべきことだと思いますし、消費者の補助金というのは次のスライドで申し上げますけれども、こういったエンパワーする技術を実装するときに、消費者によって例えばお金、あまり十分な経済状況にないという消費者がそういう技術を導入することができない。先ほどの松前委員の話でも出てきたと思うのですが、消費者の中にはタブレットとかパソコンとかを持っていない、あるいは持つことができない、そういう経済状況にある方もいると思いますので、そういう消費者の格差を防ぐために、消費者への支援をするということは、当然考えるべき課題だと思っております。

問題は、認証制度ですとか補助金を導入するとき、恐らく私はここが一番大事な点ではないかと思っているのですが、この技術が本当にエンパワーをするのだろうかということ、品質を保証するということが必要になってくると思います。法制度的に認証制度、あるいはインセンティブを与えるような補助金等々、あるいは逆に例えば事業者が制裁等々を課せられそうになったとき、ある事業者がある行為をしたときに、それを減免してもらえるというのは法制度的にも導入は可能ですし、現に今でも存在をしていると思います。

例えば景品表示法には、先日の改正によって確約手続というのが入りましたし、あとは課徴金を事業者が消費者に自主的な返金をするという返金計画を示せば、そして、返金措置を行えば課徴金額が減額されるということが行われていますので、きちんとエンパワーする技術を開発している事業者に、そういった一定のインセンティブを与えるような制度を法制度的に設けたりするということはもちろん可能だと思うのです。

それに当たっては、今までの2つの報告を伺っていても、例えばどういうリスクがあるかとか、そういうことは後で申し上げますけれども、いわゆる技術が本当に消費者をエンパワーするということを保証していかなくてはいけないという問題があると思います。つまりきちんと、この技術であればリスクも最小限で、ベネフィットよりリスクが上回ってしまうのは一番避けなくてはいけませんので、リスクも最小限で消費者をエンパワーするのだということを保証することが必要になってきます。

問題は誰がこの技術を保証するのかということで、これは今、同じく消費者委員会の専門調査会が立ち上がっているパラダイムシフトの方の専門調査会にも関係してきますが、これは正に消費者法の担い手の問題でもあります。こういったエンパワーする技術であるということを保証する主体としては、もちろん消費者庁ですとか、あるいは関係省庁としてデジタル庁、総務省といった省庁が、この技術であればリスクよりもベネフィットの方がはるかに上回って消費者をエンパワーするのですということを保証するということとして、まず、国がそれを保証するということも考えられます。

他方で、国ではなく、正に官民でいうと民の力をこれに当たって借りるということもあり得ると思います。例えば消費者団体は法的に認められている適格消費者団体の差止め訴権を通して、不当勧誘ですとか、事業者が使っている契約条項の中に不当なものがあるかどうかということを自主的にモニタリングしていると同じような役割を果たしていますが、消費者団体がこういう技術についてのモニタリングを行うことも考えられると思います。もちろんこれは国だけがやることでもないし、消費者団体だけがやる話でもないと思いますが、消費者団体に技術のモニタリングの役割を担わせるときには問題が2つあります。

一つは、消費者団体は既に結構差止め等々、あるいは被害回復に当たって十分な役割を果たしておりまして、しかし、決して人的にも、あるいは経済的にも余裕があってという状況ではないと思いますので、そういった消費者団体に技術のモニタリングを担わせるということであれば、それは国の支援等々を行う必要があると思います。

もう一つは、消費者団体が技術のモニタリングをするとしましても、こういった技術が本当に消費者をエンパワーするかどうかということは消費者団体に任せるのではなくて、ある程度の技術であればベネフィットの方がリスクよりも上回るということを国がある程度保証する必要があると思います。

次に、この技術を実装するに当たっては、消費者の新たなリスクがこの技術によって発生する、現に発生し得るのであれば、その技術をいかにして最小化するかということもありますし、あとは消費者の側がこういう新しい技術で、確かに自分たちを助けてくれる、エンパワーしてくれるのかもしれないけれども、不安があると感じれば、それをなるべく解消していくために、例えば民法、あるいはどちらかというと消費者法の問題として、法的にどのようなことをやっていく必要があるかというのを考える必要があると思います。

例えば先ほど松前委員の報告でもデータについてのいろいろお話、非常に勉強になりましたけれども、どうしても消費者のデータを活用することが必要になってきますので、そうすると、消費者からすると自分がデータを取られてしまうのではないかと、ネットでつながってしまうことで、自分の情報が流出してしまうのではないかという不安を持ってしまう可能性があります。私は一消費者としてそういう不安を持ってしまいますので、そういった不安を解消することが必要になってきます。

ただ、これを解消するというときに、単純に消費者に対してこのように気を付ければデータを搾取されないとか、こういうことをしてくださいという情報提供するだけではなくて、現にデータ収集をする必要がある技術であるときに、それによるリスクをいかに最小化するかということを情報提供にとどまらず考える必要があると思っております。

例えばパーソナルAIを例に挙げますと、これはもちろん消費者のパーソナルデータを基にしているということなのですが、単純にデータの搾取とかそういったことよりは、正にAIによって、ともすると、知らないうちに自分の本意ではない契約をしてしまっているかもしれないということに消費者が気付かないということもあると思うのですが、こういった新しいリスクがエンパワーする技術によって発生しないとは言えないと私は思っており

ます。あるいはプライバシーの問題とかもあると思いますので、私もあくまで一般論でお話をしていますが、こういったリスクへの消費者の不安をいかにして解消するか、あるいはリスクをどのように最小化するかということは、個人情報保護法だけではなくて、消費者法や民法の考え方に従って考えていく必要があると思います。

もう一つ、むしろ私はこちらが一番気になっていることなのですが、消費者をエンパワーする技術というのは、例えば高齢者を見守るためにこういう技術を使うとか、いわゆる消費者の中でも特にエンパワーする必要がある、属性等々、例えば年齢とか、あるいは認知機能､あるいは病気があるかどうかとか､判断ができなくなってきているかどうかとか、いわゆる脆弱な消費者をエンパワーするために、こういった技術を使うということも前向きに検討する必要があると思います。

他方で、技術を活用することによって、新たな消費者の格差が生じてしまうということはないかというのが、個人的には一番気になっているところです。例えばこういった技術を使える消費者と使いたい消費者、あるいは技術を使いたくても使えない消費者、あるいは使いたくないという消費者がいます。技術を使えないときに、それは様々な理由があって、例えばリスクの判断がきちんとできる消費者と、難しくてよく分からないという消費者もいますし、あるいは経済的な問題ももちろんあります。そういった技術につなげるようなパソコン等々を持つお金がないとか、こういった消費者があります。

そういったときに、技術について、あるいは技術ももちろん知識もそうですが、そういったことに伴う新しい消費者の格差を生じさせないのだろうかというのが一つ気になっているところです。つまりエンパワーするために、従来この消費者委員会、あるいはパラダイム専門調査会でもずっと言われている消費者に様々な脆弱性、弱い部分がありますと、それは情報・交渉力の格差ではなくて、こういったデジタルによって発生している格差があるということ、いろいろ言われている状況の中で、こういった技術を使ってエンパワーするというときに、これにうまく乗れる消費者とそうではない消費者が出てきてしまうのではないかというところが気になっているところになります。

次に、データ搾取に関してということです。ここで一つ問題提起をしておきたいのはデータ搾取によって侵害される消費者の利益についてですが、これは民法でいうと恐らく不法行為法の問題なのだろうと思いますが、はっきり言いますと、民法の今の学会の不法行為の議論で、この問題はまだ十分に扱われているわけではないと私は認識しています。

このデータ搾取・利用によって消費者がどういう不利益を受けるのかというと、従来であれば、例えばプライバシーを侵害されているのではないかとか、そういったことが言われていたと思います。恐らく問題となるのは、消費者が気付かないうちにこういったデータを使われたり、あるいは第三者に提供されてしまっているということになったときに、そこで侵害されている消費者の利益は一体何だろうかというところになります。

いわゆるプライバシーという本当に古典的な考え方だと、私生活をのぞき見されるといったことによく結びついていたと思うのですが、消費者はのぞき見されているという自覚

が、この状況ではないことが大多数ではないかと思っています。

もう一つ、不法行為の問題で言いますと、先ほど森先生の御報告にも出ていましたが、いわゆる消費者の利益侵害を考えても、契約の話だけで進めることも限界でもあると思うのですが、森先生の御報告にもありましたように、消費者から見たデータをめぐる事業者というのは多岐にわたります。その意味では、いわゆる加害者という言い方をしていいのか分からないのですが、データに関連している事業者というのが、消費者の直接の契約の相手方であるということよりは、むしろ消費者とは何の関係もない事業者がそういうことを行っているところも問題になってきます。だからこそ不法行為の問題だということにもなるのだと思うのですが、もしかしたら、ここで消費者が気づいてもいない状況で一体どういう利益を侵害されるのだろうかということが問題となります。

消費者法分野には不招請勧誘の禁止という規定があります。これは例えば訪問販売で、消費者が訪問販売を望んでいないのに勧誘を受けてしまう、要は不招請なので望まない勧誘を拒むことができるという考え方であり、実際にこれは法制度として存在していますが、不招請勧誘の禁止というのを正当化するときに、望まない勧誘によって消費者の何の利益を侵害するかというときに、よく言われるのは私生活の平穏を害するからであるということが主張されることがあります。しかし、例えばAIによるプロファイリング、データ搾取による消費者の侵害のときには、消費者は私生活の平穏を害されている自覚がないと思います。そうすると、従来のいわゆるこういうデータと関係ない消費者への勧誘の場面と侵害されている雰囲気が違っているということになります。

そして、契約のところに少し話を戻しますと、読む限りではこの専門調査会でもなさっていたので、その資料を拝見しましたが、消費者の認知過程に入る形での勧誘について、これをどう捉えるかというのは、民法・消費者法でも議論が始まったところではあります。ここで問題となるのは、消費者は恐らく気が付かないまま誘導されていますので、例えば強迫を受けた場合のように恐怖心を持っているわけでもなければ、詐欺を受けたときのように騙されているわけでもないということになります。

そうすると、よく言われることは消費者契約法、消費者法の場面では困惑していたとも言えないので、浅慮という言葉をよく使いますけれども、あまり考えずに消費者がコントロールされてしまっているということが言われています。問題はこのことをどのように評価するかということ、そして、これを法的に、例えば消費者の契約の離脱を認めるとしてどのようなことが方法としてあり得るのかということを考える必要があります。

例えば消費者が気が付かないうちに契約をしてしまっているときに、これをなるべく防ぎたい、あるいはそれによって契約をした消費者が自分の意思表示を取り消したいときに、いろいろな方法があり得なくはないと思うのですが、例えばこういった消費者の認知過程に入る形での勧誘というのを不当な行為であると言えるのであれば、例えばそれに行為規制、いわゆる行政規制をかけるとした上で、それに意思表示の取消権を結び付けることは、今、特定商取引法でも行政規制に違反する意思決定があった場合に取消権がありますので

不可能ではないですが、問題は認知過程に入る形の勧誘を不当な行為と評価できるかどうかというところになると思います。

仮に不当な行為だと評価できるのであれば、行為規制の対象ということにして取消権を結び付けるということはできるかもしれませんし、あるいはクーリングオフもできるかもしれませんが、このような消費者の認知過程に入る形での勧誘を全て要は悪と捉えることができるかということでは慎重な検討が必要だと思います。

そうだとすると、せめて消費者に気付きを与える技術とか、ダークパターンを見抜く技術を提供するということ、個人的にはこちらが開発されると非常に望ましいのではないかと思っています。そういたしますと、1つ目の論点の技術を評価できるかどうかということとか、その技術を使える・使えないということによる格差を生みださないかという話に戻ってまいります。

ちょっと時間を超過しましたが、あとは質疑応答で対応させていただきたいと思います。どうもありがとうございました。

○橋田座長　ありがとうございました。

大分時間が押しているのですけれども、今の森座長代理、松前委員及び大澤委員からの御発表への御質問・御意見をお願いいたします。御意見・御質問のある方は挙手、又はチャットでお知らせください。

原田委員、よろしくお願いします。

○原田委員　3名様、すごく勉強になりました。ありがとうございます。

今、大澤先生がおっしゃっていたように、多分個人情報とかを使って外部送信したりとか、利用したりとかということと、あとはダークパターンとか不正な広告が出るというところは分けて考えなくてはいけないのだろうなと思いました。不正な広告とかアフィリエイト広告とか悪質な広告は、個人に結び付ける情報を使われたことによって、そこに悪質な広告が出てきて、それで被害に遭ってしまう、きっかけになってしまう、なので、基本的には別問題として、広告の部分については不正な広告を見たい消費者はいないでしょうから、そこら辺はAIでがっちりと不正な広告が出ないようにしてもらっているとか、もしくはAIで弾いたり、もしくはプラットフォーム側で努力をしていただくようなのが別途必要なのだなと思いました。

それで、森先生と松前先生に聞きたいのですけれども、森先生の方で、今お話ししたように、どちらかというと外部送信された後に使われた情報で、消費者が不利益をこうむってしまう、リクナビ事件みたいなものがあったというような御報告でしたけれども、これがいわゆる外部通信をするときにオプトアウトが消費者の方でできないというような、要は通知をすればいいみたいな形に落ち着いてしまったような経緯というか、そういったところを教えていただければと思います。

最近はブラウザとかの方で、Appleさんとかもプライバシー保護ということでそういう情報を取らない。ブラウザ側の方でそういう仕組みを入れるようにしてきたけれども、こ

れはいたちごっこなのかもしれませんが、それである程度の効果が出るのかというところは森先生に聞いてみたいです。

あと、松前先生の方で、消費者はどうしてもデジタルの世界に関しては技術的な差と知識力の差に圧倒的に差がある世界だと思っております。特に個人情報に関しましてもコントロールという言葉が出てきたと思うのですけれども、実際は消費者がコントロールできることはほとんどなくて、結局プライバシー・ポリシーに同意することしかできなくて、オプトアウトができるとかオプトインができるものというのは結局せいぜい広告メールをオプトインするみたいな程度ぐらいしかコントロール権がないのです。

そうすると、結局同意しなければ使わないでということになってしまうので、そうすると、使わないわけにはいかないから泣く泣く同意せざるを得ない、これは決してコントロールといえるレベルの話ではないと思うのです。そうすると、例えばプライバシー・ポリシーとか、そういうような内容とか、要はAIとかも含めて第三者が使っているとか、そこで使ったりするときに、プライバシー・ポリシー自体の項目とかをオプトインするみたいな形にしていけば、自分の個人情報はここまで使っていいですと、それでAIで使ってくださいみたいなオプトイン形式にすると大分解消される可能性があるのかどうか。

特にお子さんとか高齢者とかに関しましては、知識とか文章とかプライバシー・ポリシーとかを読んだり理解することが難しかったのが、例えば見守る方々がオプトインをしていくことで、この人はこういう情報を使ってもらってAIで保護してもらおうみたいなことで、オプトインの形でいけるということで、何かうまく回るものがあるのかどうか、ちょっと回りくどいですがお願いします。

○橋田座長　まず、森座長代理にお答えいただけますか。

○森座長代理　御質問ありがとうございました。

まず､外部送信技術がどうして通知公表になってしまったのかということですけれども、これは立法時のすったもんだといいますか、押し合いへし合いでそのようになりました。検討会ではオプトインでというところまで提案としては出ていて、私は少なくともオプトアウトで行くべきであると考えていたわけですけれども、その後、事業者側からの反対がありまして、また、そこに政治家の先生が絡んでくるようなことがありまして、後で報道をお送りしますけれども、今、官僚の皆さんは全然守られない立場にあって、そういうプッシュに対して押し返す制度的な担保を持っていないわけです。それで通知公表になってしまったというのが実際のところです。

また、御注目いただきたいのは規制対象範囲なのですけれども、電気通信事業者と三号事業者みたいなことになっていまして、いやいや限定し過ぎでしょうと、本来ウェブサイト全般の話ですので、もちろんいきなり何もしていないところに規制が下りてくるというのは、規制される方としては困るわけですけれども、わざわざウェブサイトをいじってタグを入れているわけですから、外部送信している人はそれについてちゃんとオプトアウトさせましょうというのは全然大変なことではないのではないかなと思っておりまして、い

ずれにしましても、そういう押し合いへし合いで小さい規制になってしまったということでございます。

以上です。

○原田委員　ありがとうございます。

今後変わる可能性はないのですか。

○森座長代理　そんなことがまかり通ってはいけないと、少なくとも私は思っておりますので、必ず変わると思っております。

○原田委員　ありがとうございます。

○橋田座長　あと、松前委員と大澤委員への御質問もあったと思います。

○松前委員　御質問どうもありがとうございます。

まさに今御指摘いただいたところ、今日は同意の任意性というところでお話ししましたけれども、本当におっしゃるとおりで、結局個人情報の処理に同意しなければサービスが使えないというところでも仕方なく同意しているというのが多くの人の実態だと思います。こういった問題に対して、オプトインにすればいいかということなのですけれども、オプトインにするとなると、恐らくその都度一つ一つ同意していくということになると思うのですが、それはそれでオプトアウトよりはよいという考えもあり得るとは思います。

ただ一方で、今回、通知・同意の課題のところでお話ししましたように、どうしても同意が頻繁ですと、同意疲れとよく今言われますけれども、あまりよく考えずにどんどん同意ボタンを押していってしまうとか、結局はオプトイン同意の回数が増えたら増えたで、消費者としては面倒であったり手間であったりするということになる可能性がある中で、必ずしも十分に理解してそこで同意したかというと疑問が残る、結局は同じような問題というのがどうしても残ってしまうのではないかなと思います。

ですので、オプトインでやるというのも方策としてはあり得ると思いますけれども、今日お話ししたような課題が十分に解消されるかというと、やや難しいところはあるのかなと思います。

それに関連して、例えば個人情報保護に関する法規制の方で行われていますのは、同意の任意性との関係で、そもそも個人情報の処理に同意しないとサービスを使えないような場面で同意を適法化根拠とすべきでないといったことを指摘するガイドライン等が、例えばEUの方でよく出ていますので、そういった形での対応もあり得るかと思います。

○原田委員　ありがとうございます。

大企業ほど、うちのサービスを使いたかったら、何でも取るから同意してという、個人情報保護法がそうなってしまっているので、結局利用目的に書いておけばいいみたいな状態で全然選択させてくれない。そういうところで結局消費者はコントロールできないと思ったのです。それは歯がゆいなと、先生の話を聞いていて思いました。

○松前委員　コントロールという考え方自体に限界が見え始めているという議論も、今日も少しお話ししましたけれども、ありますので、いろいろな方策を組み合わせて対応して

いくということになるのかなと、個人的には思っております。
○原田委員　ありがとうございます。
○橋田座長　今の件に関して、大澤委員からコメントがあればお願いします。
○大澤委員　私は今の松前先生の御発言を伺ってすごく共感しながら聞いておりました。
1点付け加えるとしますと、同意については松前先生がお答えになっていましたので、参考までにでもあるのですが、私は報告の中で、消費者に情報提供するのは、いわゆる契約的な発想では限界があるということを少し申し上げたのですが、他方で、今の同意に関して言いますと、むしろ契約的な発想というのが、逆に日本の個人情報の同意取得の場面で少なすぎるような印象を持っています。
これはどういうことを言っているかといいますと、こういう情報をこういう目的で使いますと消費者に同意を求めていく場面はどこで発生するかというと、例えばいわゆるECサイトを使うときとか、アプリを使うときとか、そういうときだと思うのです。日本でもプライバシー・ポリシーと言葉をよく使っていたりとか、利用規約とか、いろいろな名前が付いていますけれども、これに関して日本は個人情報保護法、いわゆる公法なのでという発想が強いように思うのです。
例えば私が日頃勉強しているフランス法の場合は、消費者が同意しない限り、例えばアプリを使ったりとか、ECサイトでのお買い物はできないので、事実上これは強制されている状況であるということが結構意識をされていて、そのために消費者にきちんと納得して同意してもらうために、例えば約款とかプライバシー・ポリシー、日本で言うとそういうものですけれども、同意を求めるための利用規約という書き方をした条項を使っている、これは不当なのですということを正に契約条項の不当性と同じように考え方を示されていますので、むしろここに関しては契約の同意と同じような考え方があったほうがいいかなと思いました。あとは全面的に共感いたします。
○原田委員　ありがとうございます。非常にその点は心強く思いました。
○橋田座長　次の御質問は森座長代理、お願いします。
○森座長代理　私からは松前先生に1点、大澤先生に2点御質問がございます。先生方、どちらの御説明も大変勉強になりました。ありがとうございました。
松前先生にはコントロールのところについてお尋ねしたいと思っておりまして、コントロールについては先ほどの同意疲れのような話があって疑問があるということなのですけれども、それは全く御指摘のとおりかなと思っておりまして、ですので、そういうなんちゃって同意みたいなものは無効であるという、それだけのことではないかと思うのです。そういうものは任意性がなかったり、あるいは理解できていなかったりして無効ということで消費者側では困らない。事業者側ではデータが使えないということになるわけです。
公共性のある分野ではもちろんこれは、がん登録法等によって現在も同意なく利用できる、場合によってはもうオプトアウトもない形で利用できるということにいろいろなところでなってきているかと思っていまして、強い公共性のあるところ、医療情報、災害情報

などでそういう方向に展開するのはいいと思います。あとはなんちゃって同意を無効にすればいいだけなのではないかなと私は思っております。

私は実務家ですので、プライバシーの本質かどうかみたいなことについて元々興味があったわけではないのですけれども、同意に関するお話、コントロールに関する日本での議論を伺っていますと、同意は駄目なのだと、消費者は理解できないから同意とかコントロールとかできないのだというところまでは分かるのですけれども、それで同意は無効です、終わりということなのかなと思ったら、そうではなくて、同意は無理なので、同意なしにどんどん使えるようにしましょうという話になっていると思います。

コントロールではない、適正な取扱いなのだというお話ですけれども、では、適正な取扱いは何ですかとお尋ねしますと、それは今後の課題ですみたいなことになりまして、それだと保護のレベルがただただ切り下がっているだけなのではないかと思っております。私はそういう意味でコントロールについては問題があるという考え方には賛成できないなと思っておりますので、松前先生に私の考え方についての御意見を伺えればありがたいなと思っております。

大澤先生に対しては2点お尋ねしたいと思っておりまして、資料の4ページの不法行為のところ、正にそういう問題かと思うのですけれども、消費者は気付いていないということです。他方で本日お話ししました外部送信のような大々的なことが行われていまして、今、個人情報保護委員会では御案内のとおりなのですけれども、団体訴訟というものを検討しています。差止めと被害回復のどちらについても、現在、消費者契約法と消費者裁判手続特例法にあるものを、早く言ってしまえばプライバシーにおいて拡大するということです。そういうことを検討しましておりまして、これがここに効果的な対応になるのかということについて御意見を伺えればと思います。

もう一つはそもそも論で、不法行為の問題だと思うのですけれども、民法のプライバシー侵害について、あまりデータとの関係でお話を伺わないといいますか、分かりやすく言いますと、こういう政府の検討会でも憲法の先生方はたくさん出てこられて、大変深く研究されているのですけれども、民法の先生が出てきて不法行為のお話をしてくださるということはあまりないのです。下手をすると私が出てきて、カメラに関する裁判例のお話をしているわけですけれども、民法の世界において不法行為、そして、データに関するプライバシーというのが現在どういう状況にあるのかということについて教えていただければと思います。よろしくお願いします。

○松前委員　先生、大変重要な御指摘をどうもありがとうございます。

まず、同意に関して、無効な同意であってそれだけのことではないかということですけれども、法的には無効な同意になるという点はおっしゃるとおりかと思います。今日、私が申し上げたかったのは、正に先ほどなんちゃって同意とおっしゃっていましたけれども、実際に法的には無効と思われるような同意がまかり通っていることによって、現実には通知・同意に関して様々な実際上の課題が生じているという点になります。私の考えとしま

しては、コントロールをやめた方がいいとか、そういうことではなくて、無効と評価されるような同意が現実にまかり通っていて、実際上、法的には無効と思われるような同意に基づいて個人情報の処理がなされている現状について何らかの対応が必要なのではないかということです。例えばEUですと、先ほどもお話ししましたけれども、任意性のところをきちんと評価するとか、法執行が厳格になされていたりします。他方で日本ではその辺りについてそこまで厳しい法執行をしているようにも見えませんし、そもそも同意の要件も法律上規定されていませんので、何らかの対応が必要なのではないかというところが私の申し上げたかったことです。

また、個人情報の処理に当たっては同意以外の適法化根拠ももちろん使えますので、その辺りも精査して使えばいいと思うのですけれども、ほかの適法化根拠をどう使うのかという辺りについても、あまり十分な検討がされていないような気がいたしますので、そういったところも含めて検討をもう少し進めていく必要があるのではないかと考えております。以上が実務上の方の課題になります。

これに対して理論的な課題として、自己情報コントロール権の問題があるわけですが、これについては本当にいろいろな議論があるところで、まず私の考えとしては、プライバシーを研究している立場から、プライバシー権を自己情報コントロール権と解することについて疑義を持っているというところです。また、自己情報コントロール権自体を否定しているということではなくて、自己情報コントロール権についてはこれまでも様々な問題が指摘されてきておりまして、例えばプライバシー権の解釈としてそれが適切なのかといった点以外にも、コントロール権といったときに、コントロールとは何を意味するのか等の議論もありますので､理論的に検討してみる必要があるのではないかというところです。

もちろん通知・同意を巡る課題があるからといって、それが自己情報コントロール権が問題であるということにそのまま繋がるわけではありませんけれども、通知・同意にも関連する問題として、この自己情報コントロール権を巡る問題についても言及させていただきました。今日はいろいろ端折ってお話をしましたが、私自身は、コントロールをなくしていいということではなくて、どちらかというと、もう少しきちんと規制すべきところはした方がいいという意見を持っております。御質問の回答になっているか分かりませんけれども、ありがとうございました。

○森座長代理　ありがとうございました。

○橋田座長　大澤先生、いかがですか。

○大澤委員　御質問いただきありがとうございました。

まず1点目ですが､団体訴訟ということでは､個人的には前向きに検討してほしいと思っています。理由は幾つかあって、一つは、個人情報保護侵害に関して例えば被害を受けた一般人､仮に消費者と呼びますと､1人で訴訟を起こすという状況よりは､同じような被害を受けている消費者が複数いることは十分あり得ると思うので、団体訴訟というのはあり得るかなと思います。確かフランスは個人情報保護に関してグループ訴権、日本でいうと

被害回復方法ですけれども、そちらを設けていますので十分あり得ると思います。逆に被害回復だけではなくて、いわゆる差止めの方も十分なじむのではないかと思います。

そのときに一つ考えますのは、今日の報告のときに十分に申し上げることできなかったのですが、消費者のどういう利益が侵害されるかというときに私が考えましたのは、プライバシーということではないのですけれども、例えば消費者が本当に自分の意思で、かつ熟慮して決定しているかどうかというときに、それは誘導されてしまっているので、最終的にはもちろん自分で、例えばターゲティング広告とかを見てこれはいいなと思って自分で買っているといえば買っているのでしょうけれども、それをあまり考えずにコントロールされて買ってしまっているというところです。

従来、取引の場面でも消費者に自己決定権があって、要は自分の意思できちんと意思決定できているかどうかというときに、自己決定権という言葉を取引の場面で使っていることが民法の一部の研究者であったり、あるいは消費者法の専門家でもいたわけですけれども、むしろ、もしかすると、この画面にその考え方がなじむような気もします。

問題は、消費者一人一人個人がきちんと自己決定していませんということになると、むしろこれは個人訴訟になじむような感じもするのですが、消費者の集団的な利益として、どういう利益がこの場合は侵害されているかということをどのように考えていくかということではないかと思いました。ただ、私は個人的には団体訴訟は前向きに検討の余地があるように思います。

2点目なのですが、これはむしろ私の方が伺いたいぐらいで、総務省さんとか、いろいろなところでの専門家の会議を見ていまして、特に憲法の先生がこの問題にたくさん出ていらっしゃいますけれども、民法も専門家はあまりいないとも思うわけですが、民法の方でこの辺りの問題、例えばどういう権利が侵害されているのかという話に関しては、例えば若手の研究者で関心を持って始めている研究者が出てきていると思います。確かに現状、民法の研究者よりは憲法の先生方の方がこの問題に関心を持たれているのではないかと思います。

ただ、私自身は民法の特に不法行為、利益侵害、どういう侵害利益なのかという観点からの検討というのは当然必要だと思っておりますので、私自身も一応消費者法だけでなく民法もやっていますので、そういう立場から今後検討させていただきます。不勉強で申し訳ありません。

○森座長代理　とんでもないです。ありがとうございました。

○橋田座長　では、次の御質問を田中委員、お願いします。

○田中委員　御説明どうもありがとうございます。大変勉強になりました。この分野は門外漢なので2点、松前先生がお分かりであれば教えていただきたいです。

まず1点目、法律の分野で個人の認知的限界というものはどのように扱われているのかという点について教えていただきたいと思います。脆弱性とかautonomyという言葉はしばしば目にするのですけれども、これらとどのように関連付けられているのか、もしお分か

りであれば御教示いただきたいと思います。

というのも、松前先生の最後の方のスライドで、コントロールのお話で情報主体のリテラシー不足に対して、個人の責任の全体に対する懸念ということに言及されておりましたけれども、私も非常に類似した懸念を持っております。脆弱性として子供や高齢者を想定するのは非常に大事だと思います。

一方で、森先生からも御紹介があったようなケンブリッジアナリティカの事件のように、複数のデータを紐付けすることによって心の特徴を高度に分析して、それを悪用するという行為に対しては、子供や高齢者に限らず多くの人が気付くのは非常に困難だと思います。そういった情報の非対称性がある場合や認知の限界を超えたような悪用に対しては、リテラシーを高めるだけでは対応不十分な場合があると思います。こういった情報主体のリテラシー不足という説明の仕方というのは情報の非対称性や人の認知的限界を踏まえた上で行うべきではないかと思いまして、個人の認知の限界というものが法体系の中でどのように扱われているのか教えていただきたいと思います。

2点目ですけれども、CalCPAのダークパターンを用いて取得された同意を認めないという動きに関して、カリフォルニアのプライバシー保護局が今月、ダークパターンに関する執行勧告を発表したというニュースを拝見しました。この勧告の波及効果というか、今はカリフォルニアですけれども、特に日本への影響力みたいなものについて教えていただきますと幸いです。よろしくお願いいたします。

○松前委員　貴重な御指摘をありがとうございます。

まず1点目、個人の認知的な限界というものが法体系の中でどう扱われているのかという御質問だったかと思いますが、この点につきましては、例えば今日御紹介した日本の個人情報保護法やGDPRにおいて、明確に個人の認知的限界に関する規定が置いてあったりするということは、私の知る限りではないと思います。

ただ、今日お話ししたように、例えば脆弱性のある主体、とりわけ高齢者や子どもについてはそういった問題が指摘されていたりするのと、あと、今日は時間もありませんでしたので詳しくは書いていないのですけれども、おっしゃるとおり高齢者や子どもといった脆弱性のある主体以外の消費者にもこういった認知的な限界があるということは個人情報保護の世界でも当然認識されておりまして、とりわけ今日御紹介した通知・同意をめぐる課題との関連で、少し前から学説や、政府機関等が出している報告書といったところで論じられてきているという状況になります。

こうした議論を背景として置かれた規定の一つが、二つ目のご質問のダークパターンに関するCalCPAの規定かと思います。御指摘の勧告は私の不勉強で把握できていませんけれども、CalCPAに関しては、日本の事業者にも場合によっては影響してくる可能性がありますので、日本の事業者もある程度注意していく必要があるということにはなるかと思います。

○田中委員　ありがとうございます。

○橋田座長　ダークパターンに関しては、以前に事業者さんからのヒアリングをしたときに、マネーフォワードさんから御紹介されたお話で、銀行のAPIなどを使って家計簿アプリを運用しているのだけれども、銀行がもともと提供しているユーザーインターフェースは結構ダークパターンに近いというか、それっぽいものがあるのだけれども、間にマネーフォワードが入ることによってそういうのを排除して、もっと素直なユーザーインターフェースになっているというお話がありました。

私がやっているパーソナルAIでも同じなのですけれども、事業者に勝手にユーザーインターフェースを作らせるのではなくて、APIを提供せよというのが一番本質的なソリューションになるのではないかと考えております。ダークパターンを検出して対処するというのはもちろんいろいろな研究がありますけれども、どうしてもいたちごっこになるのではないかなという気がしているところです。

他に御質問・御意見がありましたらお願いします。

森座長代理、お願いします。

○森座長代理　先ほど原田委員からいただきました御質問の後半部分にお答えしてなかったかなというのを思い出しまして、たしかiPhoneのインテリジェント・トラッキング・プリベンションが効果を上げているかという御質問があったのはなかったかと思います。

効果はめちゃめちゃあると思います。要するにcookieを使った外部送信ができなくなってしまうということです。ただ、実はそれがこのままだと困るということで、あの手この手で回避する方法を利用側も編み出していまして、例えばよく言われているのはフィンガープリントという仕組みなのですけれども、ブラウザのセッティングだとかOSのバージョンだとかいろいろなものを組み合わせて、様々なものを組み合わせるとブラウザが識別できてしまうということになって、cookieに代わる識別子を何とか、私の御説明で言えば広告事業者がサーバーの方で編み出して、それによって閲覧履歴を取れるようにしていこうということがありまして、そこのところはいたちごっこになっていると聞いております。

以上です。

○原田委員　フォローしていただきましてありがとうございます。

最近AppleとかもCMとかでプライバシー保護とか、あと、Googleさんも自分たちでやるとかというようなことを言っていたものですから、サードパーティーcookie自体がブラウザではねてくれれば、それはそれでオプトイン状態でデータを提供してくれるのであれば本当に有り難いけれども、恐らくまた別の方法が幾らでもあるみたいなことを聞いたことがあったので、いたちごっこになると思ったのですけれども、答えていただきましてありがとうございます。

○橋田座長　それに関して言うと、Safariはいいと思うのですが、GoogleがChromeサードパーティーcookieを止めると前から言っていたのですけれども、止めるのを止めたというか、予定を延期したという話が最近あったと思います。なかなかそれに対応する技術の開発が追い付いてなかったのではないかと思います。

一方、cookieはもちろん役に立つ場面もあるわけで、森先生の御発表の中にもそういうことがありましたけれども、cookieが全くないと自分に全く似つかわしくないような、全く関係ないような情報が出てきてしまったりするので、使い方の問題という面はあるのではないかという気がします。

鳥海委員、お願いします。

○鳥海委員　森座長代理に質問です。今回御紹介いただいたのがリクナビの話とケンブリッジアナリティカ事件、比較的メジャーなところの話を改めて御説明いただいてより詳しく知れて参考になりました。これ以外にもいろいろな悪用の仕方といいますか、あまりよくない使われ方が結構考えられるのかなとは思っているのですけれども、この2例が有名すぎて、それ以外の事例をあまり聞かない気がするので、何か国内外でこれ以外でも重大な問題をはらむ使われ方をした事例がありましたら教えていただけますでしょうか。

○森座長代理　鳥海先生、御質問ありがとうございます。

私の知る限り報道はされておりません。これは2つとも話が大きくなったということと、あと、こういう事件は重要な告発者がどうしても必要なのです。例えばケンブリッジアナリティカにしてもワイリーさんが新聞と上院議員に対し告発したことによって初めて明るみに出て、そうでなかったら分からないままだったかもしれませんし、先ほどブラジルの例をお見せしたのもそういう含みもあるわけでございます。もちろん私が勘繰っているだけで、そんなコンサルの悪い策動はなかったということなのかもしれませんけれども、それにしてもあまりにも似ているということで、明るみに出にくいという性質があります。

そうでありますと､私としてもなかなか御説明しにくいところではあるのですけれども、ただ、個人的に知っているところとしましては、企業は従業員に対してアンケートを取ることができます。そこからDMPを持っている事業者のウェブの閲覧履歴等にDMBのデータベースに紐付けをすることができますので、企業と従業員の関係で、企業としましては従業員の方の就労環境についての安全配慮義務というものがありますので、例えば過度なストレスを受けていないかとか、健康な心身で過ごしているかということについて、企業としては関心を持ってもそれほど責められないところがあります。そのために、従業員の皆さんにウェブサイトでアンケートを取ったついでに外のDMPとくっつけておこうかなということでくっつけまして詳細に調べる。そういうことをしてもいいか、という相談を受けることがあります。

そのときに、私はそれ自体既に駄目だと思うのですけれども、場合によっては、もしかして職場に不満があるのかないのかぐらいだったらいいのかもしれませんけれども、転職しようとしているのではないかとか、情報漏えいをしようとしているのではないかとか、そういうこともウェブの閲覧履歴が把握できれば分かるということになりますので、そういった会社と従業員の関係でDMPを使うということは、そういうことをやってもいいですかという形で相談されたことがあります。

ですので、もしかしたら、世の中にはそういうことがあるかもしれませんし、同じよう

なことは学校と生徒さんとか、アンケートを取れるような関係です。ほとんど全員からアンケート回答が期待できるような場面では、そのデータをDMPとくっつけることは十分考えられますし、いろいろな形でどんな質問にでも答えられますので、いろいろなところでDMPはもしかしたら悪用されているかもしれないなと私は思っております。

○鳥海委員　ありがとうございます。

今、情報漏えいという話がありましたけれども、きっと情報漏えいを事前に防ぐ目的であれば使えたりする方法もありそうな感じもあるのですけれども、この辺はなかなかできないという理解でよろしいのでしょうか。

○森座長代理　実は情報漏えいに関しては、DMPと関係ないちゃんとしたサービスで、ちゃんとしたというか割とオープンなサービスでいっぱい出ていまして、一つは従業員のメールの監視です。あと、メールを監視しましてキーワードにフラグを立てて、何かやばそうなコミュニケーションをしていたら、その人のメールのアカウントを集中的にチェックするとか、そういうサービスは実際にあります。セキュリティベンダーが出しています。

その場合は従業員に、特に情報漏えいが問題になるような部署については、あなたたちのメールは会社のアカウントであったらチェックしますからということは適法にできるわけでございますが、全社的にDMPの情報とくっつけていいですかというのは、私としては同意が無効になることもある、任意性がないことによって、従業員の方ですからなかなか嫌とは言えませんけれども、私は適法性は微妙だなと思っております。

○鳥海委員　その辺をちゃんと調べるなら、もっとちゃんと真っ当な方法でやれということですね。ありがとうございました。

○橋田座長　他に御質問がありましたらお願いします。

森座長代理の発表の中で、リクナビに関して、経緯はあまりよく覚えていないので伺いたいのですけれども、同意なしに名寄せしては駄目という話と、それから、これは同意があっても内定辞退率みたいなことを伝えるのはまずいだろうという2つあったと思っていたのですけれども、2番目のほうの論点が今日は出てこなかったので、その辺りはどう決着したのでしたか。

○森座長代理　このケース自体は法執行されて行政指導を受けていまして、駄目ということになっていますけれども、個人関連情報の制度が後からできましたので、個人関連情報の説明をするときに、リクナビみたいなものも同意を取っておけばよかったのですという説明をされているかというと、そういう説明はされていません。購買履歴とかそういうもので説明をされていまして、リクナビみたいなものだと、採用企業の方が就活生とか、私が先ほど申し上げました会社の方が従業員にとかいうのは嫌と言えませんので、それはそういう同意は無効なのではないかなということになりますと、現在の個人関連情報の規定上も同意を確認しないと提供できませんというときの同意、これはもちろん有効な同意が求められますので、個人情報保護法上も駄目ということになるのではないかと思います。

○橋田座長　他に御質問はよろしいでしょうか。

大分時間が過ぎてしまっているので､この辺りで今回の議論を切り上げたいと思います。御議論ありがとうございました。

最後に、事務局から事務連絡をお願いいたします。

≪3. 閉会≫

○江口企画官　本日は長時間にわたりありがとうございました。

次回の会合につきましては確定次第御連絡させていただきます。

以上です。

○橋田座長　それでは、本日はこれにて閉会とさせていただきます。

お忙しいところを御参集いただきまして、ありがとうございました。

以　上