利用者情報に関するワーキンググループ（第26回）

令和7年6月5日

【小玉利用環境課課長補佐】 ただいまから利用者情報に関するワーキンググループ第26回会合を開始いたします。事務局を務めます総務省利用環境課の小玉です。お忙しい中、朝早くからお集まりいただき、ありがとうございます。

本日は、SPSIにおけるウェブサイトの取扱いに関するヒアリングを行います。オブザーバーとして個人情報保護委員会に御参加をいただいています。また、プレゼンターとして株式会社三菱総合研究所に御参加をいただいています。なお、生貝構成員、寺田構成員は御欠席と伺っております。

資料について、三菱総合研究所様の資料として資料26-1を、森構成員資料として資料26-2を、一般社団法人新経済連盟から資料26-3を準備しております。また、参考資料として第18回WG資料の抜粋をつけております。

少し解説させていただくと、SPSIの見直しの論点として、ウェブサイトへの対象拡大に関する検討という事項がございました。そこでは、先般の11月末のWG報告書で、アプリケーションとウェブサイトで取得する利用者情報の取扱いに差異があるかどうかについて調査を行い、関係事業者やウェブサイト運営者に対する説明やヒアリング等の必要な対応を行った上で、次回以降の改定においてウェブサイトを対象とするべきか改めて検討することが適当であるとされていることから、今回検討をさせていただくということでございます。

それでは、これ以降の議事進行は山本主査にお願いしたいと存じます。山本主査、どうぞよろしくお願いいたします。

【山本主査】 よろしくお願いたします。本日は、SPSIにおける、今お話がありましたけれども、ウェブサイトの扱いにつきましてヒアリングを行います。

まず、資料26-1について、三菱総合研究所、安江主席研究員から御説明をいただき、一旦、意見交換の時間を設けたいと思います。それでは、よろしくお願いいたします。

【安江氏】 三菱総合研究所、安江です。本日もよろしくお願いいたします。

私のほうからは、アプリ・ウェブブラウザにおける利用者情報の取扱いの比較ということで御説明したいと思います。

めくっていただいて、目次になりますけれども、資料は大きく3つから構成されていまし

て、まず、議論に当たって、利用者情報というのはどこからどこまであるのかというのを抜け漏れがないようにおさらいをしたというのが1の利用者情報の全体像の確認でございます。

2で具体的な利用者情報の取扱いの比較を行っておりまして、取得可能な情報、それから利用者情報の取扱いの全体像といたしますか、スマホの中でどのように取扱いが行われているのかということと、そうした利用者情報取扱いの比較ということとなっています。3番目で、調査結果としていますけれども、全体のまとめを行っております。最後に、調査の過程で参照した資料について、参考ということをつけております。

それでは、もう一枚めくってください。こちらは今御説明があったとおりなので、詳細は割愛しますが、この赤字の部分について検討したというものです。

次のページ、その次のページお願いします。まず、利用者情報の全体像の確認ということで、スマートフォンにおいて利用者情報としてどのような情報が生成されているかという全体像を整理・分類といたしますか、確認したということになります。全体で抜け漏れがないように把握したということで、具体的には、スマートフォンのどのところでこういった情報ができているのかという生成箇所や、利用目的としてこういったものがあるのかという整理を行い、それらをまとめたという形になっています。

次のページお願いします。こちらですけれども、スマートフォンとそれを取り巻く主体といたしますか、そういったものをレイヤーの形で整理してまして、例えば、デジタル市場競争会議の資料等も参照しつつ、この資料のために整理したのになっています。

一番下にユーザーがしまして、その次の点線の箱の中がスマートフォンの端末をイメージしています。アプリストアというのはこの中にあるわけじゃないですけれども、アプリストアを通じてアプリがインストールされているということを書いております。そこから外部にアクセスしてゆき情報を取ったり取られたりということがあることを示しています。ブラウザから見るサイトですとかアプリを通じて使うサービスのサーバーというのは省略してはいますが、全体としてこういう形なのかなという整理をしております。

次のページお願いします。こちらは利用者情報の利用目的を整理してまして、プライバシーポリシー等と、それから、このページの下に注書きにある3つほどの文献、こういったものを踏まえて、利用目的としてどういうものがあるのかという全体像を整理したのになっています。表の左側の利用目的というところで、契約・取引、ユーザー管理からその他まで書いてまして、それらを細かく分類したのが右側のところで、具体的にこういった形

で使っているかという全体、主なものを整理しております。

特に赤の部分、こちらについては、第三者によるデータ利用も多くなっているのかなと
いうことで、ちょっと印をつけているということになります。

次のページをお願いします。こちらがまとめたもので、5ページ、前の前のページのレイヤー
に対応する形で一番左側の「生成箇所（レイヤー）」とありますが、それを細分化したのが「カテゴリー」で、利用者情報・利用者端末の対応関係を右側で整理しています。赤字の
部分は、「利用者や利用者端末の直接的な関係を保持しない・特定できない場合」とありま
すけれども、特定というものが直ちにプライバシーの問題ということではないですが、利用
者をいろいろとトレースしたりトラッキングする上では、こういった部分も関わってくる
ので、赤字で書いています。これらは、検討に入る前におさらいをするという趣旨でこうい
った形で整理しています。

次のページをお願いします。もう一枚をお願いします。こちらが本日の本題でして、アプリ・
ウェブブラウザにおける利用者情報の取扱いの比較について、大きく3つの観点といえます
か、3つのプロセスで行っています。

まず、取得可能な利用者情報の比較ということで、こちらは実際のプラクティスがどうか
ということもあるんですけども、まずは技術的に可能かどうかという観点から、アプリと
ウェブブラウザにおいて取得可能な利用者情報・デバイス情報の種類について整理しまし
た。

次に、スマートフォンの中でアプリやブラウザを通じてどういった形で利用者情報が取
られているのかという流れのようなものを整理しました。それが利用者情報取扱いの概観
ということですが、細かく説明が書いてありますけれども、利用者情報の流れをそういう形
で整理しています。

2. 3の利用者情報の取扱いの比較では、①から⑥の6つの観点から、アプリとウェブブ
ブラウザにおける利用者情報の取扱いについて比較を行っています。

次のページをお願いします。まず、取得可能な利用者情報の比較ということで、タイトルに
も「技術的な取得可能性」と書いてあります。表が左右2つに分かれていますけれども、そ
れぞれ「区分」というのが利用者情報の大きな固まり、それについて具体的にしたもの
が「情報項目」となっていて、「アプリ」と「ウェブ」という欄でそれぞれ取得可能かどう
かというのを書いています。

その取得可能かどうかについては、表の上に青い字で凡例を書いていますけれども、まず、

「◎」は、自らのアプリ・サイトでアカウント作成やログインなしでも取得可能である。「○」がログインしている場合に取得可能である。「△」は、少ないですが、情報の種類による、という意味です。「●」はサービスと直接関係なくてもデバイスから取得可能なもの。もちろん条件や制限等もあるんですけども、そういった形で整理しています。

アプリの場合もウェブの場合もいろいろな情報が結構取れたりする部分もあるんですけども、大きな違いとしては、右側の表のデバイスのユーザーに関する情報というところ、こちらについて、アプリは「●」が並んでいて、ウェブの場合は「○」です。ログインしている場合に取得可能で、かつ、「*5」という注釈をつけていますけれども、例えば、カレンダー・スケジュールについては、カレンダーサービスをウェブでやっている場合には取れますよ、ユーザーコンテンツとかユーザー作成ファイルを投稿するようなサイトの場合には取れますよという形で、ウェブの場合は、そういったサービスを提供している場合には取れるということが多いと思いますけれども、アプリの場合には、そうじゃなくても取れる場合もあるということを示しています。技術的にはあり得るということで、この部分が1つ大きな点なのかなというふうに考えました。

次のページをお願いします。次のページが、ウェブブラウザの場合とアプリの場合と、スマートフォンに対してどういう形で利用者情報が流れて取られていくかということを図式的に整理したものです。もちろん簡略化している部分もありますが、大きな流れを比較したいという趣旨でございます。

上の段がブラウザ、下の段がアプリで、左側に利用者のスマートフォンがあります。事業者Aとか事業者Xというのがありますが、こちらは直接サイトを運営している事業者Aとか、アプリを提供している事業者Xということになります。事業者Bとか事業者Cというのは、事業者Aが提供している、運営しているウェブサイトに対してタグを提供している事業者です。サードと書いてありますが、そういった形の関係になります。

下のほうでも、事業者Yとか事業者Zというのは、事業者Xが提供しているアプリに対してSDKを提供している事業者という形になっています。上のブラウザの場合は、事業者Aが運営しているウェブサイトのコンテンツにタグを埋め込んで、それが利用者のスマートフォンに表示されて、利用者のブラウザ上でBとかCのタグがプログラムになるんですけども一動いて利用者情報を送っていくということになります。

なお、ここでサードパーティークッキー作成と書いていますが、サードパーティークッキーの作成だけでなく、利用者情報についてブラウザの中で取れる情報を送ると

いうことも含めてあります。

また、広告に関するタグについては、これは非常に単純化してありますけれども、実際はリアルタイムビiddingという形でよりタグが多様化していますし、多段化しているといえますか、複数の段階を踏んで複雑になっていますが、この図に入れると複雑になり過ぎたので、非常に単純化した形で書いています。

アプリの場合も、SDKを使ってアプリの中でSDKが利用者端末の中から利用者情報を送ることがあるということで、こういう形になっています。

赤字の部分が、それぞれの利用者情報の取得に関する制限的なものであります。上のほうですと、ブラウザでのデータ取得に関するガバナンスがないとありますけれども、③のところ、これについては、ブラウザがデバイスデータを取るときに、W3C標準があつて、それを実装しているブラウザではガバナンスといいますか制限があるんですが、実装が義務づけられているわけではないので、ガバナンスがないというふうに書いてあります。ただし、実際多くのブラウザでは実装されているということになります。

第三者によるタグ・クッキーを用いた利用者情報の取得・取扱いにガバナンスがないというのが、上のブラウザの段の右側のほうに書いてありますけれども、こちらについても、いろいろな標準とかツールがあつて、それを使えばできるんですが、義務づけられているわけではないということです。大手のサイトとか主要なブラウザでは実装されたりしていますが、義務ではないという意味でガバナンスがないというふうに書いています。

アプリの場合は、アプリストアとかOSベンダーがいろいろなルールを定めてエンフォースもしているのので、そういった部分ではガバナンスがあるという形で整理しています。

次のページお願いします。こちらのほうではそれらも踏まえて、左側の①から⑥の観点から、アプリとブラウザにおける利用者情報の取扱いを比較しました。

まず、取得可能な利用者情報（技術的な可能性）についてですけれども、アプリについては、10ページで御説明したとおり、技術的には、多様な端末情報を利用した情報をアプリやSDKを通じて取得可能である。基本的にユーザーのアカウントとひもづいている場合が多いと思われまはすけれども、もちろんひもづいていないアプリもあるんですが、基本的にひもづいていることが多いだろうということで書いています。

ブラウザの場合は、ブラウザやタグにより取得できる情報は、アプリと比べると相対的に少ないのかなと思いますけれども、サイト閲覧履歴やサイト・フォームの入力情報が主であるという形になっています。もちろんサイトやフォームの入力情報でいろいろなものが設

けられますので、そういった点ではいろいろな情報を取り得るんですけども、実際取っているかという、相対的には少ないのかなというふうに捉えています。こちらは基本的にはユーザーとは直接ひもづかない場合が多い。もちろんログインすれば別なんですけれども、そういう形で書いております。

2番目が第三者による取扱いとルールということで、アプリの場合は第三者による取得も可能です。ルールとして、OSベンダーやアプリストアによるものと、それから業界団体等による自主ルールがあるという形になっています。SDK提供者が取得可能であって、OSベンダー、アプリストアがアプリ提供者ですとかSDK提供者に対して説明や同意取得義務あるいは禁止・制限、こういった情報は取ってはいけませんとかそういったものを設けている。それから、業界団体による自主ルールやガイドというものも存在します。

ブラウザの場合ですけれども、こちらも第三者による取得が可能で、自主ルールがあるという状況だと整理しています。タグ提供者が取得可能であるということです。ウェブサイト提供者や運営者に対する義務・禁止・制限等については、ほかからの義務・禁止・制限というのは特段ないですけども、業界団体による自主ルール・ガイドもありますし、大手のサイト運営者については、こういった形でいろいろなことをやっていくんだという自主的な取組はもちろんなされていますが、外部からの制限や規制はないというふうになっています。

③が利用者情報の取扱いのガバナンスということで、アプリの場合は、OSベンダー、アプリストアによるガバナンス、あるいは業界の自主ルールというものがそれぞれあるということです。②とも重なる部分があるんですけども、OSベンダー、アプリストアはアプリやSDKによるデータの取扱いについてルールを設けていて、従わないアプリはアプリストアで公開されないという形になっています。また、アプリ提供者は利用者SDKについて管理を求めると定めているアプリストアもあります。

他方で、こういったガバナンスというのはあくまでも、私企業、特に海外事業者によるガバナンスであるということについての留意も必要なのかなということで、非常に実効的に機能しているものだと思いますけれども、そういった面もあるのかなということを書いております。それから、こちらについても業界団体による自主ルール・ガイドがあるということも書いております。

ブラウザの場合ですけれども、利用者情報の取扱い、ガバナンスのためのツールとか仕組みが提供されています。業界の自主的ルールもあります。まず、ブラウザがサードパーティ

ークッキーの利用を制限している場合があります。また、ブラウザが端末のセンサー情報、例えば、加速度とか傾きとか、周りの明るさとかそういった環境情報、そういったものを取ることができますけれども、その場合に利用者の同意を求めなきゃいけないとかそういったものが決められておまして、それを実装しているブラウザが非常に多いんですけれども、そういったものもあります。

あるいは、ウェブサイトでほかのドメインとの情報共有とか、ほかのドメインから来たタグによる情報の取得を制限すると、そういう機能も提供されています。それらについては、ブラウザとか各ウェブサイトがルールを定めて管理・実行していくということで、それぞれが決めていくという形になっています。

大手の事業者が運営しているウェブサイトとか主要なブラウザでは、そういったものについて、基本的に対策が取られていると思われまます。また業界団体による自主ルール・ガイドも存在します。

④の利用者情報の取扱いの説明義務や⑤の同意取得義務、こちらについて、アプリの場合は、ストアとかOSによって義務づけ・ルールが定められているということです。ウェブサイトでは、各サイトに任されている形になっていますけれども、大手はやっていますがサイトによる差があるということかなと思います。

利用者による状況把握、こちらについても、アプリの場合も、差もあるかもしれませんがけれども、利用者が把握可能です。ウェブサイトの場合も、サイトによって異なる部分があって、把握しやすいサイトとそうでないサイトがあるということなのかなと見ています。

次のページをお願いします。14ページです。以上をまとめたものをサマリーとして書いておまして、一番最初に示した、取得主体、取り扱う情報の種類、利用目的・取扱い方法という観点から改めてまとめという形にしたものになります。

取得主体ですけれども、アプリの場合はアプリ提供とSDK提供者、ウェブの場合はウェブサイト運営者、タグ提供者という形に集約できるのかなというふうに考えました。

取り扱う情報の種類については、先ほど説明したとおりですけれども、アプリのほうが比較的多種類の情報を取得可能で、ブラウザのほうはアプリと比べると限られているのかなということになるかと思ひます。

それから、利用者とか端末とのひもづき状況ですけれども、アプリの場合、ユーザーあるいはアカウントとひもづいていることが多いので、そういった部分は把握しやすいとされています。ウェブの場合は、結びついている場合もちろんありますけれども、基本的にはあ

まり結びついていないということで、クッキー等識別子を用いる形でトレースしているという形が多いかと思えます。

それから、違いとしては、下のほう、アプリやサードパーティーSDKによる取扱いについてOS・アプリストアによる制限等があったりするということに対して、ウェブの場合は、それぞれのサイトやブラウザがそれぞれの判断で取り組んでいるということかと思えます。

次の次のページをお願いします。3の3です。こちらはこれまでまとめたもの、3の1と特にあまり変わらないのかなと思われるかもしれませんが、アプリとウェブブラウザそれぞれについて、個々のアプリ単独での利用者情報の取扱いと、SDKでアプリ横断的にといいますか、複数アプリにまたがって利用者情報を取り扱う場合、ブラウザの場合も、サイト単独で利用者情報を取り扱う場合とサイト横断的にという場合があると思えますので、そのこの部分の整理という視点で、これまで書いたことと似たようなことになるんですけども、表にまとめています。

いずれの場合も、複数アプリ、複数サイトにまたがる場合については、利用者の行動履歴を複数にまたがって取得可能なので、より多面的に把握可能であり、あるいは、場合によってはプロファイリングとかそういったものにつながり得るということがあるので、そのこの部分は少し注意して議論する必要があるのかなと思えます。アプリ単独とかサイト単独の場合と横断的な場合、そういう違いという視点も必要なのかなということで考えております。

それ以降、参考資料なので、必要に応じて御覧いただければと思います。

説明は以上になります。

【山本主査】 ありがとうございます。

それでは、ただいまの三菱総研様の御発表につきまして、構成員の皆様から御意見、御質問をいただきたいと思えます。早速、太田さん、よろしく願いいたします。

【太田構成員】 太田です。御説明ありがとうございました。

とてもたくさんあるのですけれども、重要なところと僕が思うところをいくつか説明させていただきます。時間が余ったらそれ以外のところもという感じでお願いしたいと思えます。

まず、5ページの生成箇所の整理というところで、オペレーティングシステムの上に、アプリの場合はアプリストアが書かれていると思えますけれども、ブラウザもアプリストアの上に載っていると思っており、サードパーティーアプリの1つとしてブラウザがあ

るという整理なのだと思いますので、そこが前提として少し違うのかなと思います。

技術的にどういう情報が取得されるかというところについて、ブラウザはアプリの1つなので、ブラウザがOSのAPIをたたけば、他のアプリと同じ情報は全て取得できるので、現状、Safariやサードパーティーのブラウザ、Braveなどがありますけれども、そういうブラウザアプリがOSのAPIをたたいているか、たたいていないかの違いだけであるというところが、この資料と僕が思っていることの大きな違いがあると思っております。

それを踏まえて、10ページについて、実はアプリとウェブで取得できる情報、技術的に取得できる情報というのは、ブラウザもAPIにアクセスできるという点で全く違いがないのですが、ブラウザで実装していないという理由で、例えば、ここで言うと通話履歴やSMSの履歴は、ブラウザがそういう情報を取得するAPIをつくっていないため取得できないのだと思うんですが、多分その他の情報はほぼ一緒だと思います。

例えば、アプリだけが取得できてウェブが取得できないと言っているデバイス情報のデバイスIDについて、アプリが取得できるとなっていますが、これはもう既に、OSが生成したID、要するに、広告IDではない端末を識別するIDは、アプリから取得できる方法はないはずです。パーミッションがないはずで、これはアプリも取得できません。

次に、デバイスのユーザーに関する情報でデバイス用認証情報に関しても、ID・パスワードと書いてありますけれども、アプリもデバイスのID・パスワードは取得できません。生体情報も取得できません。取得できるのは認証結果が取得できるだけで、それはウェブも取得できますので、これは一緒です。

電話帳・アドレス帳について、カレンダー・スケジュールの方が分かりやすいと思いますが、カレンダー・スケジュールは、アプリは取得できて、ウェブは、「○」で「*5」、自サイト・サービスで登録・入力・取得している場合と書いてありますが、アプリもIOSで言うと、Appleのカレンダーアプリを使っていたら取得できるので、要するに、Appleのサービスで登録していたらアプリで取得できるというのは、例えば、ウェブでGoogleのChromeを使っていて、Googleのカレンダーアプリを使っている場合は取得できるわけですので、それも条件としては同じだと思います。

ユーザーコンテンツ・ユーザーファイルについても何を意味しているか分かりませんが、端末上のファイル、例えば、写真をアップロードすることもブラウザからできますので、ブラウザからアクセスできます。

ヘルスケア・フィットネス情報も、これもAppleのヘルスケアアプリを使っていれば取れ

るけれども、これはブラウザも、「* 5」と一緒に、自社サービス・自社サイトを使っている場合は取得できるので、これはウェブとアプリもそんなに条件変わらないですよ。

財務情報に関しても、クレジットカード番号が取れないというのは、アプリは取れるわけではないんですけれども、Apple Payは使え、それはウェブも使えますので、同じです。

通信に関する情報はウェブだけが取れるとなっていてはいますが、これはアプリも取得できます。

そうすると、今ここに書いてある違いはほとんどなくて、通話履歴・SMS履歴ぐらいかなというところがまず言いたいことの1つ目でございます。

P11、点線の③でガバナンスがないというお話をいただいたんですけれども、ここで一番問題とすべきところは、この事業者Cというのは、事業者A、B、Cというのがブラウザであって、ブラウザの場合は、事業者Cがここには書いていない事業者Dのタグを勝手に呼び出して実行させることができるということが一番の違い、問題だと思っています。

アプリの場合は、例えば、SDKがまた違うSDK事業者を呼んできて、そのSDKをアプリで実行させることができない仕組みになっているため、ガバナンスの有無に関わりますが、ブラウザは無制限に連なって、資料にピギーバックと書いてありますけれども、ピギーバックでどんどん連なって、本当に誰かよく分からない人を事業者Cが連れてきてタグを実行することができる。アプリの場合は、そういったように連れてきてSDKを実行することができない。ここは結構大きな違いだと思っておりますので、そこは観点として抜けているかなと思いました。

それを踏まえると、最後のサマリーの15ページ辺り、ブラウザの方が取得できる情報は少ないというのは、確かに通話やAPIの利用しやすさなどは、アプリのほうが取得しやすい等あるかもしれないんですけれども、その取得したデータが誰に使われるかという観点をそこに入れる必要があり、そうすると、そんなに取得できる情報には違いはないです。

その取得した情報を誰が使えるかという観点に立つと、先ほど申し上げたように、全然知らない事業者Dがブラウザの場合は使えるけれども、アプリの場合はそのガバナンスはちゃんとありますよねというところが違いなので、その観点は追加いただきたいなと思いました。

一旦、重要なところは以上でございます。

【山本主査】 ありがとうございます。安江さん、今の太田さんの御指摘に対して、今、御回答いただけますでしょうか。あるいは、もう少し御質問を受けてから、まとめて御回答

いただくということでも結構ですが、いかがでしょうか。

【安江氏】 まず、簡単に御回答できる部分は回答したいと思います。

【山本主査】 お願いします。

【安江氏】 まず、5ページ目です。ブラウザのところですが、ブラウザもOSで標準のブラウザとそうでないブラウザがあって、サードパーティーブラウザについてはアプリストアに載っかるというのはそのとおりだと思っていますので、訂正したいと思います。

【太田構成員】 今の点について、Safariも、OS提供事業者のブラウザもアプリストアの上ののっかるという形だと思います。

【安江氏】 その上で、10ページのところです。ブラウザもアプリなのでということもあるんですけども、ここは必ずしも十分に整理できていない形もあるんですけども、ウェブとブラウザ、ブラウザという観点だとそうだと思うんですけども、ウェブとして見た場合、もちろんブラウザを通じて取れるという部分もあると思うんですけども、ウェブとして取れるものという観点で一旦整理しておりました。

なので、細かい間違いは訂正したいと思うんですけども、ここでは、アプリを通じてサービスを提供している場合とウェブサイトを通じてサービスを提供している場合、サービスの中には情報の提供というものもあるんですけども、そういった観点で見た場合どうなのかという違いで一旦整理してみたという趣旨で言っておりました。なので、ブラウザもアプリなんですけれども、ウェブサイトというもの、そういう観点で整理していました。だからこれが正しいよということではないですけども、ちょっと整理したいと思います。

それから、11ページの図ですけども、ピギーバックのところ、図で書いていなかったのは省略し過ぎたかなと思うんですけども、問題意識としてはありまして、赤字の部分で、ピギーバック対策でということも書いてありますように、そこは頭にあったんですけども、もっと明示的に示すべきでした。

一旦、回答としては以上になります。

【山本主査】 ありがとうございます。太田さん、いかがでしょうか。追加でコメントがあればお願いします。

【太田構成員】 ブラウザかウェブかみたいな話がよく分からなかったんですけども、結局、最初の議論と混ざってしまったかもしれないですが、ブラウザというアプリがあり、アプリとして例えば通話履歴とかのAPIをたたいたら取得できるというのはあるのだけれども、今はそうしていないという観点で、ウェブサイトの運営事業者がどういう情報を取得

できるかという観点で僕も話していたつもりです。

そのため、先ほどの例えばデバイス認証情報などは、ウェブで認証結果は得られ、アプリも認証結果を得られるという話や、財務情報のApple Payはアプリでも使えるしウェブでも使えるし、クレジットカード番号が見られるわけではないというのも、アプリもウェブも、ウェブサービス提供事業者も一緒というところは、先ほどの僕の主張と変わらないというところは言っておきたいと思います。

【山本主査】 ありがとうございます。

それでは、一旦質問に戻って、木村さん、お願いいたします。

【木村構成員】 主婦連合会の木村です。御説明ありがとうございます。

説明の中で、ログインしてウェブを利用するとユーザー情報を取得して、ログインしないとそれはあまり取得されないという趣旨の説明があったと思いますが、ウェブでもログインして利用する人は結構多いと思いますし、逆に、1回ログインしてしまうと、ログアウトを意識的にしないで、そのままログインした状態になっているのではないかと感じるのですが。

質問としては、利用者は本当にログインせずに利用することが多いのでしょうか。説明の中にあまりログインして利用することはないからという趣旨があったので、そのところはもう一回確認させてください。よろしくお願いいたします。

【山本主査】 ありがとうございます。安江さん、いかがでしょうか。

【安江氏】 そこは説明文がちょっとよくなかったかもしれませんけれども、今回、この中では、ユーザーがログインして使うのか使わないのかどっちが多いのかということは考慮してなくて、ログインしていても取れるのか、ログインしていないと取れないのかというところで区別をしたということですが、実際のユーザーの利用においてどうなのかということとは一旦外して検討しております。

【木村構成員】 分かりました。私の意見としては、やはりそこは重要だと思います。ログインしたかしないか、ログインしたらどうか、ログインしないからどうかというのは、利用者にとってはすごく重要なことだと思いますので、その辺りも含めて検討していければと思います。ありがとうございます。

【山本主査】 ありがとうございます。

この辺りは、太田さん、何か御意見というか、今の木村さんの御指摘に対していかがですか。

【太田構成員】 ありがとうございます。僕もその点を言おうと思って後回しにしていたんですが、おっしゃるとおり、ブラウザ、ウェブでもログインして使うし、アプリでもログインしなくても使えるアプリは多いと思います。何となく感覚的にアプリのほうがログインしているのではないかという視点で書かれているような気がしますが、ただ、実際にかと、例えば、ウェブの場合は、Facebookにログインしている、Googleにログインしているという情報が別のサイトからも参照ができてしまうということはアプリとの大きな違いかなと思います。

例えば、大体の人は、Facebookにログインしたままログアウトせずにそのままウェブを見ると思います。Googleにログインしたまま、ログアウトせずに他のサイトを見ることはすごく一般的で、そういう観点からすると、アプリよりもウェブのほうが、Googleにログインしてウェブサイトを見ているということは多く、アプリの場合は、アプリから直接Googleにログインしているかしていないかみたいなものは、SDKを入れていても取れるのは限定的なものですので、そういった観点からすると、アプリのほうが、対プラットフォームという意味では、ログインして使っていないほうが圧倒的に多いかなと思います。

【山本主査】 補足していただいて、ありがとうございます。

それでは薫さん、お願いいたします。

【薫オブザーバー】 御説明ありがとうございました。これは今の御説明に対する質問ということになるのか、事務局への質問なのか、どちらか分かっていないのですけれども、先ほどの太田構成員の質問とも一部重なりますが、アプリとウェブの違いって何なんだろうかということ、私も本WGに今年から途中参加したのでよく分かっていないのですが、先ほど太田構成員から御指摘がありましたとおり、ブラウザもアプリではないかと素朴な点として思いました。その辺りは先ほど議論されたとおりだと思っています。

次に、ブラウザの中で閲覧できる範囲のコンテンツがウェブだというイメージだと感覚的には何となく分かるのですけれども、じゃあウェブアプリがどちらなのか疑問に思いまして、例えば、今この会議をやっているWebexなどもアプリ版とウェブ版がありますけれども、ウェブ版はどっちになるのかはよく分からないところです。また、ウェブフォームなどもあると思いますが、最近ウェブスキミングなどが問題になっていると思いますけれども、そのようなフォームやウェブブラウザの中でいろいろな機能を提供しているものについては、アプリなのかブラウザなのかどういうくりにしているのか、よく分からなかったというところがありますので、その辺、基本的なところになるかもしれませんが、教えて

いただければと思っております。

【山本主査】 ありがとうございます。重要な点かと思えます。後で事務局のほうからも今の御質問に対して御回答いただければと思えます。

先に質問を続けたいと思えます。森さん、お願いいたします。

【森構成員】 ありがとうございます。御説明ありがとうございました。大変勉強になりました。太田さんに補足していただいたところも含めて、ぜひとも残していただければと思えます。重要なことかと思えます。

若干観点みたいなことの問題があつて、私が先ほどのMRIさんの御発表と太田さんのやり取りに参入するのは非常に危険ではありますが、伺っていて、安江さんはウェブ上、ウェブサイトのタグの機能について語っておられて、太田さんはもう少し全体的にウェブの利用によって取得できる情報は何かということで御指摘をされていたのかなと何となく思いました。

消費者目線で考える必要があると思うのですが、ウェブサイトの閲覧によってどういう情報が取得されたかということもやはり重要だと思えますので、それも資料に入れていただければと思えます。

そこまで含めて考えたときに、つまり、利用者の立場に立ってウェブサイトの利用とアプリの利用、一応社会的には別だが、プログラムとしてはそんなに変わらないというお話だったと思えます。我々技術に疎い人間としては、ウェブの閲覧とアプリの利用を一応区別して考えているわけですが、そのような立場に立ったときに、それぞれどういう情報を取得されているかで分けていただくことはできるのかなと思えます。

先ほどのピギーバックに関して、太田さんの御指摘のあつた点は非常に重要だと思えますので、どのような情報が取られるか、それが分かりやすくなっているか、ガバナンスが利いているかという観点を入れていただくことが重要なのではないかと思いました。

お聞きしたいのは、技術的に取得できる情報の種類はそんなには変わらないのだけれども、アプリの方が少し多いかもしれない。他方で、野放図にと言いますか、ガバナンスに関して言うと、アプリの方がアプリストアなどがある分ガバナンスが効いていて、ウェブの方が自由になっているというまとめ方ができるのかと思いましたが、そういうまとめ方でいいのかどうか、それだと不正確ではないかといった御意見をお聞かせいただければと思えます。よろしく申し上げます。

【山本主査】 ありがとうございます。安江さん、いかがでしょうか。特に最後の点です

が。御確認というところですけども。

【安江氏】 安江です。ありがとうございます。

まず、ブラウザとアプリの違いというところが最初に太田さんからあったと思うんですけども、これは自分として確たる結論ではないですが、ブラウザとアプリ、確かにブラウザもアプリなんですけれども、ブラウザの場合はサイトを提供している人とブラウザを提供しているのは違う、アプリの場合はサービスを提供している人とアプリを提供しているのが同じという部分があるので、そこでの違いもあるのかなと。だからどうだということは直ちにはないですけども、そこもちょっと気になっている部分として1つあるということです。

ブラウザ内のいろいろな機能についてアプリかブラウザかですけども、これは基本的には、ブラウザの中でもいろいろな機能を提供しているものはタグという形で整理しています。

次、森先生のお話で、今のそのままとめとしてどうなのかというところになるんですけども、確かに自分の中でも同じような感覚でして、取得できる情報の種類、差がどのくらいかということはあるんですが、アプリのほうが若干多いだろうということと、他方で、ガバナンスという点では、アプリのほうが効いていて、ウェブは自由と言えば自由なんですけれども、そういう差があると思います。

ただ、ウェブの世界というのは、いろいろなサイト提供者がいろいろな広がっていますし、エコシステムも大分変わってきてはいますが、もともとのインターネットの流れからいうと、自主的にいろいろルールを決めて自分たちでやっていくという部分があるのかなと思います。そういう意味では、自分たちでルールを決めて問題は解決してやってきたという流れもあって、第三者による厳格なルールというよりは、自分たちでやっているという流れもあるのかなというふうにも感じています。

その中で、主要なサイトとか主要なブラウザについてはきちんとやっているという部分があるので、サイトとかブラウザ全体ということなのか、そうじゃないところとやっているところの違いはどう考えるかというところは1つ残るのかなというふうにも感じています。

雑駁ですけども、以上です。

【山本主査】 ありがとうございます。森さん、何か追加でコメントありますか。

【森構成員】 ありがとうございます。できれば資料をアップデートしていただければと思います。ありがとうございます。

【山本主査】 ありがとうございます。

米田さんからチャットで書き込んでいただいていますけれども、御発言はいかがでしょうか。

【米田オブザーバー】 ありがとうございます。チャットに書いてしまいました。

学校現場でも今のような話が結構あって、アプリでしか見られない情報と、ブラウザで見られない情報、具体的には教材系がそうなのですが、学校で保護者や生徒たちが、何の情報をどっちで見たらいいのかが結構複雑になって、面倒くさくなったりしています。

また、今、生徒にとっては、スマホやPC、タブレット系がいろいろ入り混ざっているので、余計にダウンロードなどの問題が出ていところが多いので、今日の話もすごく参考になったのですが、そういった部分も今後、うまく同期していただけるとありがたいなと思います。

以上です。

【山本主査】 ありがとうございます。

それでは、呂さん、お願いいたします。

【呂構成員】 大変詳細な調査と御説明をありがとうございました。

アプリとウェブサイトの違いが話に上がっていたかと思いますが、このSPIを最初につくっていたときの発想や問題意識について、最初の策定に携わられた寺田さんがいらしたら聞いていただくのが一番正確だと思いますが、私の理解としては、当時、アプリをスマートフォンに入れて、そのスマートフォンをカバンなどに入れて持っているだけでも、自分でアプリを起動していない、つまり実際には起動されているものの、起動しているという意識が利用者になくときに位置情報を追跡されてしまったりするという、具体的な例としては、交際相手のスマートフォンにこっそりアプリを入れておいて行動監視するというものが問題になりました。

ウェブサイトの場合、基本的には自分がブラウザを使ってウェブサイトにアクセスしているときにしか情報は取られないという理解ですが、アプリだとそうでないときにも勝手に情報を取られてしまっていることがプライバシー保護上問題なのではないかというところで、特にアプリを問題視してスマートフォンプライバシーの議論が始まったものと理解していますが、現在その辺りはどうなのでしょう。ウェブサイトとアプリで情報の取り方に違いがあるのか。今、森先生からもコメントがありましたが、他の先生方からも御意見いただければと思います。

【山本主査】 ありがとうございます。先ほどの蔦さんからの根源的な御質問とも絡む話でしたので、後ほど事務局からも御回答いただきたいと思います。おそらく森さんもその辺りの御意見かなと思いますが、まずは、上沼さんからお願いいたします。

【上沼構成員】 ありがとうございます。何となく、普通のブラウザだと、確かにアプリではないと思うのですが、スマートフォンだからかなと思いつつお話を聞いていました。今、ユーザーは、ブラウザやアプリをその区別をあんまり意識せずに使っているのではないかなと思います。共通で使える場合にどういうふうに差があるのか、同じもの・同じサービスに行っているのにどう違うのかみたいな観点だともっと分かりやすいかなと思いましたが、もし可能なら御検討いただけるとありがたいなと思いました。可能であればの希望です。

【山本主査】 ありがとうございます。

それでは、森さん、お願いいたします。

【森構成員】 ありがとうございます。呂先生から先ほど制定時にどうだったのかというお話がありましたので、私からその当時の記憶をお話したいと思います。

御指摘のとおり、スマホのアプリが怖いということが割と雑誌等で特集されたりいたしました。当時から、情報収集モジュールにしてもウェブのタグにしても、同じようにサードパーティーに情報を流しているのではなからうかと思しますので、ウェブと変わらない面はあるのではなからうかという話はあったんですけども、ただ、怖い怖いということで、いろいろなところに、当時爆発的普及期にあったスマートフォンとアプリについて怖い怖いと言われることは、スマートフォンの生態系をどんどん進めていく上ではよくないというふうに判断しまして、まずは怖い怖いと言われているアプリについてやろうということで、SPI1をつくったというのがその当時の事情です。

雑誌やテレビなどでアプリの怖さを宣伝されている状況に、総務省として憂慮すべきことであるという判断でつくったというものでありまして、実は当時の社会的な反応と申しますか、アプリがやばいんじゃないかというところにピンポイントで反応したものであったかなと思います。

【山本主査】 ありがとうございます。

事務局からいかがでしょうか。何かコメントがあればと思いますけれども。

【小玉利用環境課課長補佐】 既に森先生と呂先生から、SPIの制定当初の経緯も含めて詳しく御説明いただいたので、特に付け加えることはございません。

葛先生への御回答ですが、例えば、資料の18-2を今回参考資料26-1として、出していますが、SPSIはスマホアプリの利用者情報の適正な取扱いについて記載していて、必ずしもスマホやPCからブラウザを通じてウェブサイトを開覧するときの利用者情報の取扱いについては対象に含んでいないところ、それについてどうするのかを今御議論いただいているということでもあります。

例えば、ウェブアプリはどうかと御指摘がありましたけれども、ウェブアプリは基本的に、現在のSPSIでは対象には含まれていないというイメージになるかと思いますので補足として回答を差し上げます。

【山本主査】 ありがとうございます。

時間の関係で次の発表に移りたいと思います。森さんからプレゼンをいただけると聞いていますので、よろしく願いいたします。

【森構成員】 ありがとうございます。それでは、私のほうから、今回のSPSIにウェブサイトの外部送信を入れるのかについてお話ししたいと思います。

おめくりください。このように、今回の論点に入っているウェブサイトのことをどうするんだということかと思えます。私としては、それ論点なのか、という感じはしておりますが、このように問題意識になっているということです。

おめくりください。先ほど呂先生からも御質問のありました制定経緯なんですけれども、これがSPI①当時の2012年の説明の図で、その後もいろいろなところで引用されていますけれども、要するに、スマートフォンにいろいろな情報があり、それをアプリの情報収集モジュールが外に出してしまうことがあるという問題意識で、それが恐ろしいということでございます。

これを見ていただきますと、左の一番下のところ、アプリ利用情報などがありますけれども、その1つ上にネット閲覧履歴みたいなものもありまして、時流的にはアプリ怖いということに対応したものであったのですが、本質的にはユーザー情報に関する安全・安心ということを目的としたものでありましたので、ネットの閲覧履歴みたいなものも当然心配事の対象には入っていたということであろうかと思えます。

おめくりください。ここからアプリの外部送信とウェブサイトの外部送信が同じように扱われてきたことについて少し御説明したいと思います。制定時からしばらくたってどうなってきたかということですが。

おめくりください。これはプラ研、プラットフォームサービス研究会についての御説明で

すけれども、プラットフォーム事業者に対して利用者情報の取扱いについてヒアリングをずっとやってきたわけです。それがプラ研の1つの大きなミッションだったわけですが、その中でどうだったかということについてです。

黄色いところ、利用者情報の取扱いに関する主なモニタリング項目とありまして、項目3、他アプリやサイトを経由した情報収集の状況ということで——おめくりください。点線の囲みが二重になっておりまして、中の囲みの3ポツを御覧いただきますと、情報収集モジュールやJavaScriptによる外部送信ということで、アプリとウェブをまとめて書いてしまっているわけです。

その下の小さいほうの点線囲みの外側、大きいほうの点線囲みの内側ですけれども、その段落ですが、「情報収集モジュール（イメージタグ、JavaScriptタグ）が設置されている場合等に当該アプリやウェブサイトを訪問する利用者に関する利用者情報」とあり、アプリで訪問というのはあれですけれども、このように並列的にモニタリングも行ってきたところでございます。

おめくりください。これは同じ資料、プラ研の取りまとめにおける外部送信規律の説明です。外部送信規律の説明ですから当たり前ということですが、このように、左上ですが、ウェブサイトの外部送信とアプリの外部送信を並べて、同じものですよということを説明してあります。

右下のほうはテキストになっておりまして、「ウェブサイト運営事業者やアプリケーション提供事業者が利用者の閲覧履歴等の情報を第三者のサーバー等に送信するプログラム等」ということになっておりまして、ここでも並列的に問題意識を書いております。

おめくりください。ウェブサイトにおける外部送信の仕組みということで、先ほど安江さんから御説明もありましたし、皆様御案内のこととは思いますが、一応資料上つけてありますので、簡単にお話ししたいと思います。

おめくりください。クッキーとは何かということで、釈迦に説法ですけれども、クッキーとは、サーバーとブラウザの関係をつくっていることの1つです。ブラウザがサーバーにアクセスします。初めてアクセスしたときは、サーバーがクッキーに識別番号を書き込むということです。サーバーとしては、1番の人、2番の人というふうに識別したいということです。

この書き込まれたクッキーにつきましては、ブラウザが再度サーバーにアクセスすると、今度はブラウザからサーバー側にクッキーが送信されるということです。これによって、右

の吹き出しですが、123番の人がまた来たなということが分かるわけでございます。そして、そのクッキーのもう一つの特徴として、ドメインが書かれていて、ブラウザとしては、同じサーバーからもらったものはそのサーバーにだけ返すと、そういう機能があります。

おめくりください。外部送信がいよいよ出てくるわけですが、左がファーストパーティー、右がサードパーティーとなっています。どういう違いかといいますと、左側ですが、〇×スポーツのウェブサイト、これは私が毎日チェックしているウェブサイトで、ここに閲覧のためのアクセス①をいたしますと、スポーツの結果、大谷がどうだったとかボクシングがどうだったとか、これがピンクのところに表示されます。このとき、コンテンツと一緒にウェブサイトに設置されているタグの指示がブラウザの方に行きまして、そのタグの指示によって私のブラウザは、私の知らない間ですけれども、右側の広告事業者サーバーにアクセスします。その広告事業者サーバーから、白い画像というところに広告が表示されますが、これをダウンロードしてくるということです。

左側ファーストパーティーも右側サードパーティーも、当然のことながら、サーバーとブラウザの関係ですのでクッキーのやり取りがあるということになります。〇×スポーツからもらってくるのがファーストパーティークッキー、広告事業者サーバーからもらってくるのがサードパーティークッキーで、これ以降、初回アクセス以降は、ブラウザからサーバーに送り返すことになります。

おめくりください。このとき重要なポイントとして、広告事業者サーバーはブラウザからアクセスを受けると、どこのタグの指示で来たのかが分かるということになっております。つまり、ファーストパーティーが何だったかというのが、〇×スポーツだったということが分かるということです。これが重要です。

タグの機能は様々にありまして、先ほど安江さんの御説明のとおりですけれども、いろいろな指図をブラウザに対して出すことができますので、ファーストパーティークッキーを送ってこいという指図をブラウザに出すこともあります。そうしますと、ブラウザがその〇×スポーツからもらってきたファーストパーティークッキーをサードパーティーのサーバーに差し上げるということもできるということです。

おめくりください。広告事業者サーバーは実は非常に顔が広くて、〇×スポーツのみならずいろいろなサーバーにタグを置いてもらっています。そのため、私が〇×スポーツ、スポーツ新聞だけ見ている場合じゃないということで、ニュースを見たりポータルサイトに行ったりいろいろなものを見ていると、私の認識としてはいろいろなファーストパーティー

を別々に見ているわけですが、実は同じ広告事業者のタグがそれぞれのウェブサイトにおいてありますので、私のブラウザはその指示を受けて、ファーストパーティーは変わりますが、同じ広告事業者サーバーにアクセスすることになります。

そうしますと、広告事業者サーバーはファーストパーティーがどこだったかということが分かりますので、ここを見たんだね、ここを見たんだねということが順番に分かる。その分かる内容というのは、ブラウザから送り返されてくるサードパーティークッキーによって紐付けされているということです。

おめくりください。その結果がこのようなものになっておりまして、広告事業者サーバーが私のブラウザに振った、サードパーティークッキー123番のブラウザということで、123番のブラウザさんはこのように、〇×スポーツの後、すぐにランニングシューズを見て、引越ashiを見て、ポータルを見て、ニュースを見てということが広告事業者サーバーに分かるわけでございます。もちろんどこの誰ということは分かりませんが、123番のブラウザということです。

おめくりください。ウェブの閲覧履歴をまとめたものがDMPのデータベースと呼ばれているようなものではないかと思いますが、このようなウェブの閲覧履歴の収集は非常に一般的に行われているということです。1つのファーストパーティーのウェブサイトにいっぱいタグが置いてあり、100ぐらい置いてあるところもそんなに珍しくないということがございます。

法的評価、2ポツのところですが、後からお話しします外部送信の規制ではなく、個人関連情報というものもありましたけれども、基本的にはなかったのではないかと思います。やはり原則個人情報ではないということもあって、事実上許容されてきたということかと思います。

書きませんでしたけれども、これは日本ではそうだったということございまして、海外では全然違っていて、欧州ではeプライバシー指令というもので2002年からオプトアウトかな。そして、eプライバシー規則になって、2009年から、このようなサードパーティーに外部送信するのであれば、それは本人の同意が要ということになっているかと理解しています。アメリカでも、カリフォルニア州の消費者プライバシー法が有名ですが、それ以外でも複数の州で、クッキーに紐づく情報というのは個人情報として規制の対象になっているということです。

3ポツです。外部送信のポイントとありますけれども、閲覧者に分からない、私に分から

ないうちにサードパーティーに出ているということです。そして、大々的に行われている。何が大々的かといいますと、それはタグの置いてあるウェブサイトが非常に多いということです。Googleのような事業者は、ほとんど全てと言っていいかと思えますけれども、ウェブサイトタグを置いていますので、閲覧履歴の観察・収集は網羅的に、誰がどこに行ったということを非常に幅広く、ほぼ完全な形で把握することができるということです。

最後の4ポツですけれども、我々は、ウェブの閲覧をプライベートな行為と考えてしまっているわけです。家で新聞を読んだり雑誌を読んだりすることと同じように、外形的な行為としてはそうなので、体感的にプライベートな行為と感じてしまっていますけれども、実際にはそうではないということでございます。

おめくりください。ここから、外部送信が問題になった事件についてお話していこうと思いますが、最初は、リクナビ事件と個人関連情報です。

おめくりください。リクルートキャリアが事件の当時にウェブサイトに置いていた説明ですが、赤線は私が勝手に引いたものでして、採用企業からリクナビ側にクッキー情報が送られて、リクナビ側でリクナビが保有するクッキー情報と突合してスコアを算出し、スコアを採用企業に納品するという趣旨のことが吹き出しで書いてあります。

おめくりください。今のだけでは抽象的で分かりにくいので、若干推測混じりでお話をしたいと思いますけれども、採用企業としては、例えば、就活生に対してアンケートを実施します。就活生はみんな、これは内定を取るためには回答しないとイケないということで、こぞって回答する。それをダウンロードしてきたものがこのピンク色のところです。そのタグを使ってリクルートのサーバーにアクセスしてもらいます。これは別に、画像と書きましたけれども、何でもいいわけです。透明なものでもいいし、小さいものでもいい。目的は、リクルートのサーバーにアクセスをしてクッキーのやり取りをすることです。

当然のことながら、リクルートのサーバーとしては、どこを踏んできたかということが分かりますので、採用企業のウェブサイトから来た。そして、この場合、おそらく先ほどの図からすると、ファーストパーティークッキーをリクルート側でもらうということではないでしょうか。したがって、リクルート側では、ファーストパーティークッキー、ここでは「saiyo001」としてあります。それから、自分のサーバー、リクルートサーバーでつけたサードパーティークッキー「リクルート123」、これをペアにして持つことができるということです。

おめくりください。リクルートも顔が広く、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。ただし、GoogleやMetaのように、ありとあらゆるウェブサイトということではなく、就活関連を中心にタグを置いてもらっているということです。

おめくりください。そうしますと、就活生がどこにアクセスしたかということが分かるわけですが、特に就活系サイトを中心に、123番のサードパーティークッキーのブラウザさんは、IT就活、外資系就活、メーカー就活、外資系就活、ポータルニュース、外資系就活ということで、外資系が本命であるということが分かります。そうしますと、このクライアントは、例えば、国内企業であれば多分内定を蹴るでしょうということです。これがスコアの算出ということになります。

おめくりください。口頭で御説明したことを補足して書き込んだものが、このようになっております。要するに、この場合、ウェブの外部送信が使われているということです。

おめくりください。法制度側の対応ですけれども、これをきっかけに、黄色い丸で囲んでいる部分、スコアを算出しているリクルートの方では、ファーストパーティークッキーとサードパーティークッキーしかないので、どこの誰か分からないのですが、それを採用企業に送ると、採用企業側では最初のアンケートの段階で氏名を書かせていますので、ファーストパーティークッキーと対応する氏名が分かって、これはどこの誰のスコアはこうなのか、これはよくないねといった話になるということです。もちろん、そのアンケートというのは、私の例え話でして、何でもこんなことができるということです。

おめくりください。個人関連情報の制度の説明です。

おめくりください。一言で言いますと、2ポツのところ、データベースを提供するときに、提供先が同意を取ったことを提供元が確認しなければならないという形になっております。

3ポツ、リクナビで言いますと、採用企業側でリクナビのDMP情報を買ってあなたの個人情報に紐付けるけれどもいいですかと就活生に尋ねて同意を取り、リクルート側がスコアの提供前に採用企業に対してこの同意を取っていただけましたかという確認を取ることが法制度上求められている。これが個人関連情報の規制ということになります。

おめくりください。引き続き、ケンブリッジアナリティカ事件と外部送信規律ということで、こちらは日本のリクナビ事件がかわいく思えるぐらいの大事件だったわけですがけれども、少し御説明したいと思います。

おめくりください。ケンブリッジアナリティカ事件の方が時間的には、事件としては前に起こっているわけですがけれども、外部送信のところ、これ放置でいいのか、データベースになってから提供先で個人情報に戻るところだけ抑えたのでは駄目なのではないかというこ

とが問題意識としてあったのではないかと思います。

おめくりください。外部送信と問題意識を持った電気通信事業法の関係ですけれども、電気通信事業法にはもともと通信の秘密というものがあまして、電話の利用によるプライバシーというのは高いレベルで守られていたわけです。特に、電話を使って通話をする、メールをする、そこに通信の秘密がかぶせられていた。ところが、電話の利用形態がどんどん変わってきてまして、皆様通話もメールもちろんされるでしょうけれども、その時間は短く、何を専らしているかという、ウェブサイトを見る、アプリを使うということですが、こちらが外部送信によって筒抜けになっているということです。これをおさえるということが問題意識としてあったわけです。

おめくりください。ですので、この左上の外部送信のところ、これを新しく規制しようということになったのが外部送信規律ということになります。

おめくりください。これが外部送信規律を検討した検討会、電気通信事業ガバナンス検討会報告書における外部送信規律の立法事実に関する記載ですが、上のところを御覧いただきますと、個人的法益、社会的法益、国家的法益と3つ並んでいます。

個人的法益のところ、情報漏えい等の防止のプライバシーということはもちろん外部送信については問題になり得るところかと思いますが、真ん中、社会的法益のところ、健全な言論環境の確保や、右側の国家的法益のところ、健全な民主主義システムの確保などが書いてあります。

おめくりください。これが、ケンブリッジアナリティカ事件が念頭にあるということです。簡単に復習させていただきますが、2016年、アメリカ大統領選でトランプ陣営、英国のブレグジット国民投票で離脱派をそれぞれ支援したとされる会社でございます。2018年に元社員クリストファー・ワイリーさんという人の告発でいろいろなことが発覚した。

どんなことが発覚しましたかということですが、2014年頃、ケンブリッジ大学の研究者、コーガンという人が心理クイズのアプリを作成しまして、このアプリをフェイスブック利用登録、何と云うか正確には分かりませんが、これを使ってダウンロード、インストールした30万人のユーザーと、彼らが友達として登録していたユーザー8,700万人分のデータを取得するということです。

そして、このデータに対して心理学やアド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プロファイリングを行い、神経症で極端に自意識過剰である、陰謀論に弱いと分析されたグループに対して政治広告を出しまして、さらには、愛国者団体の集

会などに誘い、先鋭化をさせていったということです。

おめくりください。これは告発本です。『マインドハッキング』というタイトルになっています。原題も非常に事の本質を突いたタイトルではないかと思えます。

おめくりください。マインドハッキング、まさに操作ですね、そのようなことになってしまっ、その操作対象の人たちは、次の大統領選、2020年の大統領選のバイデンが勝った選挙ですけれども、結果は信じられないということになりまして、連邦議事堂に突入するというような事件に発展しているわけです。

おめくりください。ちょうどこの頃、2018年、平成30年ですけれども、個人情報保護委員会がFacebook Incに対して行政指導をしております。それを見ますと、「いいね！」ボタンが設置されているウェブサイトを開覧した場合、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フェイスブック社に送信されてしまう事案ということで行政指導しておりますので、「いいね！」ボタンによる網羅的な情報収集、そして、それがユーザーに気づかれないということです。ファーストパーティーのウェブサイトに「いいね！」ボタンがある、「いいね！」ボタンを触れば、もちろんそれはフェイスブックに把握されるでしょうけれども、触らなくてもフェイスブック側で閲覧履歴を取得されてしまうことに反応しているわけでございます。

どうしてここだけ個人情報なのかと言いますとFacebookには登録情報がありまして、皆さんの氏名等を登録されているために、ウェブの閲覧履歴がここでは個人情報になるということです。

おめくりください。「いいね！」ボタンによるウェブサイトの外部送信ということですが、仕組み自体は全く先ほどの他の類いのものと変わらないということになります。いろいろなファーストパーティーのウェブサイトに「いいね！」ボタンを設置して、そのファーストパーティーのウェブサイトを見ると、ブラウザがSNSのサーバー、Facebookのサーバーにアクセスするということです。

おめくりください。ケンブリッジアナリティカ事件の教訓ですけれども、これも釈迦に説法ですが、社会の分断や国の在り方に影響される、あるいは、外国が出てくると安全保障上の問題になることとなります。

このような操作、行動に対する影響が可能になったのは、1番、詳細なプロファイリングが可能なFacebookのデータベース、2番、広告配信の仕組み、それから3番、コメントの仕組み、レコメンダーということですがけれども、この1番のプロファイリングが可能な

Facebookのユーザーデータベースというのは、「いいね！」ボタンによって集められたウェブの閲覧履歴が中心になっているのではないかと思います。

おめぐりください。最後にまとめです。ウェブサイトの外部送信とアプリの外部送信は同様に並列的にこれまで扱われてきた経緯があります。リクナビ事件やケンブリッジアナリティカ事件においても、ウェブサイトの外部送信によって収集されたデータが多く利用されたのではないのでしょうか。

SPSIの目的がスマートフォン利用者情報の安全・安心であるならば、ウェブサイトの外部送信を除外するのは不合理ではないかと思います。

私の話は以上です。御清聴ありがとうございました。

【山本主査】 ありがとうございます。

それでは、続きまして、資料26-3に基づき、新経済連盟の片岡政策部長から御発表をお願いします。その後に、森さんと片岡さんに対する御質問、コメントを受けたいと思います。

それでは、片岡さん、お願いいたします。

【片岡氏】 新経済連盟の片岡と申します。説明の機会をいただき、ありがとうございます。本日は、SPSIでウェブサイトに関する検討についての意見ということで申し上げたいと思います。

まず、前提として、新経済連盟は約500社超の会員企業がありますが、ウェブサイトを持っていない会社はほぼいないということで、多くの事業者に影響があり得るものだと思います。これは新経連に限らず多くの事業者に影響が及び得るので、大きな関心を寄せているという前提をまずお話ししたいと思います。

次のページをお願いします。まず、今我々が考えていることを冒頭にまとめておりますが、それぞれについて細かく後ほど御説明をしたいと思います。

まとめて言いますと、この青い背景のところに書いてありますが、そもそも、先ほどのお話だと、ウェブサイトというものの範囲自体も皆さんの中で共通認識を持っているのかなというのが少し疑問に思ったところではありますが、ウェブサイトについての記載がSPSIに今ないということで、具体的にどういう問題があると皆さん感じていらっしゃる、具体的な問題意識をすり合わせた上で、じゃあどういう解決手法が考えられるのかといったのをステップで考えていく必要があるんじゃないかなと思っています。まず、問題意識のすり合わせですね。

それから、問題が抽出されたところで、どういう問題や課題に対処するために、何について、誰を対象として、どういうものがあるとそれが解決になるのかということ考えた上で、ウェブサイトについてSPSIに何かを書くということがその手段になるのかというのを考えたほうが良いと思っています。

以前、SPSIの整理の話のときに新経連として申し上げたこととかぶりますが、SPSIにあれもこれもとどんどん、たくさん分量を追加していくというのは、使いにくくなってしまわないかという懸念を持っておりますので、これも前回は申し上げたこととかぶりますが、SPSI策定当初の趣旨や目的に立ち返って、現状を踏まえつつ、スマートフォンアプリの利用者情報の保護という切り口から、シンプルで目指すべき方向性を理解しやすく参照・実行しやすい指針というのがSPSIに求められる姿かなと今の段階では思っているため、対象範囲の拡大には慎重になっていただきたいなと思っています。これからもう少し細かく説明していきます。

まず、SPSIのウェブサイトへの対象拡大が必要とされる具体的な問題意識は何かというところです。こちらは先ほどお話がありましたが、そもそもSPSI、旧SPIは、2010年代初めのスマートフォンの急速な普及に伴って、黎明期の不安解消、とにかくスマホが怖いんじゃないかという不安解消や事業者のレベル引上げという観点から、スマホアプリを通じて収集される位置情報だったり連絡先、端末IDなどの利用者情報の適正な取扱いを確保することを目的として、主なターゲットとしては、アプリ提供事業者などを想定して策定されたものだと思います。ターゲットと目的が分かりやすく、うまく活用されていたものだと思います。

一方で、ウェブサイト。ウェブサイトも、先ほどお話を聞いていて、皆さんの中で、そもそもスマホのブラウザアプリの話なのか、ブラウザアプリを通じてアクセスするウェブサイトの話なのか、スマホ関係なくウェブサイト全般の話なのかというもぶれがあるなと思ったのですが、ウェブサイト自体は、スマホが関係ない話で言うと、SPI策定のはるか昔から存在していて、その種類や開設者もとてもとても多様であるという現実があります。

ちなみに、アプリ内ブラウザというのは既にSPSIに記載があり、同様に考えましようということでも記載があると思っています。一方で、ウェブかアプリかに関わらず、電気通信事業法における外部送信規律というのは、外部送信を行う電気通信事業者や第3号事業者に対して一定の行為を求めている、そちらについては既に行政や民間団体によるガイドライン等が存在している。これはSPSIとは別に存在しているという状態です。

この状態の中で、まずは、どういう問題が今発現していて、それに対してどういう人をターゲットに何をやったらいいのか、具体的な問題意識のすり合わせと、それを裏づける実態などの確認をまずやってはどうかと思いました。

次のページをお願いします。具体的な問題を抽出できたとして、こういう問題を解決するために何かをしなければいけないんじゃないかというものがまず出てきたとして、その解決方法として、どういう場でどういう手法が検討されるべきなのかというところですが、このワーキンググループは、開催要項にもあるとおり、電気通信事業、プラットフォームサービス等に係る利用者情報のさらなる保護等を目的として設置されていると認識しています。これまで、電気通信事業法やプラットフォーム事業者への継続的なモニタリング、SPSI改定、それから事業者への啓発等を通じてこのワーキンググループの目的に対応してきたと理解しています。

この範囲で、これまでの議論で、ウェブサイトを対象にすべきなんじゃないかという議論の中身を私も議事録などを拝見して確認していたのですが、検討対象に含めるべきだった意見や調査を行うべきだという意見はあったと認識しているのですが、具体的な問題について共通認識が形成されているわけではないので、具体的にどういう問題を解決するために具体的に何を検討するのかは未知数だと我々は今思っています。具体的な姿が見えないので、意見を具体的に言うのも難しい状態です。

今まで制定してきたSPSIの実効性を高めるためにも、具体的問題の解決方法が果たして本当にSPSIなのかという観点はぜひ持って検討いただきたいなと思っています。事業者に対して何か書いて示せるものだから、これにどんどん入れ込んでいこうというのだとすると、どんどん使いにくいものになってしまうかなと思っています。

同じ話になりますが、SPSIは何のために存在し、どこまで広げるのかということで、項目の再整理は進めていただいていると思いますが、ウェブサイトが対象となっていない現時点においても、様々な項目が新たに追加されたり、追加が検討されているところだと認識しています。

このまま内容が膨大になって、関係事業者が例えばすごく広がったりして、参照・実行しづらい指針とならないかというのは常に懸念をしているところです。仮に具体的な問題について共通認識が形成されて、解決方法としてSPSIへ何らかの追記をしてはどうかという検討があるとしても、誰を対象として何を目的に何を書くのかというのが重要で、それはビジネスの実態を十分に反映しているのかという確認が必要だろうと思います。

それから、SPSIにそれを追記することによってどういった影響が出るのかをしっかりと分析していただきたいなと思っているのと、改めて影響を分析した上で、SPSIは結局誰のために何を目的として存在するのか、趣旨の再確認をして、趣旨が変わっているのであれば、それは趣旨を変えるべきで、SPSIの中身に合わせるべきだと思いますし、そこまで本当に広げてどういう意味があるのかというのを考えていただきたいなと思っています。

世の中いろいろな問題意識がある中で、インターネットを通じていることを理由にあらゆる問題にSPSIで対処しようとしても際限がないのかなと思っています、SPSIは今までアプリケーションの提供者等を中心として分かりやすい指針として実効性があったと思いますので、これをむやみに広げたりすると、せっかく今まで積み上げてしてきたものが無駄になってしまうのではないかと懸念をしております。

というわけで、最初のページに戻っていただきまして、意見としては、皆様が具体的に問題だと思っていてSPSIに何か書けば解決できるだろうなと思っている事象は何なのかというのをもう少しちゃんと確認したほうがいいんじゃないかと思いました。

先ほど委員の先生方の御意見の中に、分析方法としてウェブとアプリみたいな話で総合的にやるんじゃないかと、例えば、同じサービスでどう違うのかみたいなのを考えてもいいんじゃないかという御意見もありましたが、多分いろいろな分析の切り口があると思ひまして、それはもちろんやる意味はあると思うのですが、そもそも出発点として、問題意識というか、事象というか、その辺りがまだ外側からはよく分からないので、事業者としてもかなり心配をしているという状態でございます。

新経連からの意見は以上です。

【山本主査】 ありがとうございます。

それでは、残りの時間、20分強今お二方からプレゼンいただきましたけれども、それらにつきまして意見交換できればと思います。いかがでしょうか。太田さん、お願いいたします。

【太田構成員】 太田です。御発表ありがとうございました。私からは新経連さんに質問2点があって、最後に意見も言いたいなと思うんですけども、まず、質問2点をしたいと思ひます。

先ほど片岡さんのお話の中で、先ほどのMRIさんの議論の中でも、ウェブサイトの話なのかブラウザの話なのかウェブアプリの話なのかみたいところで、そこも共通認識が取れていないというお話があったのですが、今、それがぶれてしまっているのは現状をなぜか分けてしまっているからだと思っています。先ほど話にはなかったのですが、アプリ内ブラウ

ずはSPSIの対象になっているなど、非常に現状分かりにくくなっているのは分けてしまっているからだと思っていて、そこを同じにすればより分かりやすくシンプルになると思うんですが、そうすればシンプルなると思いませんかということが質問の1点目です。

2点目に関しては、まず、新経連さんの問題意識として、問題意識のすり合わせと裏づける実態の有無の確認が必要というお話がありましたけれども、先ほどのMRIさんの資料におけるウェブにおいてガバナンスが効いていないというような問題ですとか、森先生からの発表は、前々から問題意識は共有できていて、外部送信規律においてもウェブは対象になっていて外部送信規律というものになっているから実態も確認できていると私は思っているのですが、あとどういう点が具体的に足りないと思っているのかということをお聞きしたいなと思いました。

質問2点は以上です。

【山本主査】 ありがとうございます。どうでしょうか。この段階で片岡さんのほうから御回答をもしいただければ、お願いします。

【片岡氏】 シンプルになるのではないかとところにピンと来ていないというのが正直なところで、結局、今のSPSIというのは、ターゲットになっている事業者がよりアプリ提供事業者中心になっているのですが、それがウェブサイトを広げたときに、具体的に今の項目にどう影響があるのかというのはピンと来ていないというのがまず1つあって、どちらかという、すごくいろいろ広がっていくんじゃないかという懸念を持っているという感じです。

結局SPSIをどうしたいか、どういうものを想定していますかというのがなかなか見えてこない、シンプルになるというより、どんどん広がっていくんじゃないかという意識を持っています。それは多分、ウェブサイトとなった途端にすごくいろいろな種類のいろいろなものが想定されるからだとは思いますが。その辺りをむしろ、具体的にどういうことを書こうというイメージを皆さんがお持ちなのかがいまいち分からないなと思っています。

それから、どこが足りないというより、こちらとしては逆で、何を解決するために何が今のSPSIに足りないのかが分からないので、それを皆さんの認識をすり合わせした上で、本当にそれがSPSIに入れるべきものなのか、それをすることでこういう問題が解決できるんじゃないかという道筋を確認したほうがいいんじゃないかという意見でございます。

質問に質問返しみたいになってしまう感じにはなりますが、それだけ今の皆さんのイメージが一致していないということが恐らく一番の問題、課題ではないでしょうか。それをど

うやってすり合わせていくか、やっぱり具体的な事象にひもづいて考えないとなかなかイメージが一致しないと思うので、事例を出していかないとなかなか進まないのかなとは思いました。

以上です。

【山本主査】 ありがとうございます。

太田さん、この後御意見というところですけども、確かに、具体的な問題とは何かというよりはより明確に、SPSIは立法ではありませんが、ある種の立法事実をよりクリアにしていく必要があるのかなと思いました。

先ほど森さんからはケンブリッジアナリティカ事件、リクナビ事件の2つが示されましたけれども、ケンブリッジアナリティカ事件は海外のお話だ、ということもある。リクナビ事件については、個人情報法の改正によって一定の対応がなされているというところで、そうすると、日本で今こういった議論をすることの重要性と必要性ですよね、この辺りが明確に示せないといけないのかな、という印象です。

あとは対象者をどうするのかという具体的なイメージについても、重要な御指摘をいただいているのかなと思います。それを踏まえて、後で森さんから御発言いただくとお聞きしますが、太田さんからも何かあればぜひお願いをいたします。

太田さん、いかがでしょう。

【太田構成員】 僕の意見は最後でいいので、まず、皆さんの質問が終わってからの方がいいと思います。

【山本主査】 分かりました。

じゃあ、森さん、お願いします。

【森構成員】 ありがとうございます。私は1点か2点。共通の問題意識が分からない、問題意識が共有されていないということでしたので、片岡さんのその点についてお尋ねしたいと思います。

そこはかねがねお話ししてきているのかなとは思ってしまして、まず、SPIとは何なのか、SPSIとは何なのかということについて言えば、これはスマートフォン利用者の情報の安全・安心であったということです。これは最初からそういうことでありました。ですので、片岡さんが以前、青少年の保護に広げるのかとおっしゃっていたのは、それは分かりますし、そういう意味では、アイデンティティの拡大というのはあったのだらうと思います。

しかし、利用者情報の安全・安心ということからは動いていないし、ここまでの議論とし

では、アプリによるサードパーティーへの送信とウェブサイトのタグによるサードパーティーへの送信が同じように扱われるべきではないかという問題意識だったわけです。ですので、その点が共有されていないと言われると、そんなことないと思うんですけども、どうでしょうか。

さらに言いますと、リクナビの話もケンブリッジアナリティカの話も、外部送信規律のときに既に散々したお話です。あのときは賛否いろいろありまして、その後、最終的に押し返されてみたいなきともありましたけれども、ウェブによる外部送信の利用者情報に関する問題、不安、プライバシー上の懸念ということは、それは広く共有されたから法制度の中に入ったのではないかと思います。外部送信規律が両方を対象にしているのは、それは両方ともプライバシーの問題がある、利用者情報の問題があるから法規制になったのだと思います。

ですので、なぜSPSIにおいて区別されるのか分からない、つまり、問題意識というのは、ウェブの外部送信においてもアプリの外部送信と同様に利用者情報の安全に問題があるということが共有されているのではないかと思います。この点いかがでしょうかということをお尋ねしたいです。

もしかすると片岡さんの御質問というのは、問題意識の話というよりは解決策を考えておられるのかもしれないなと思っておりまして、それはまだここで話するのはもしかしたら早いかもしれませんが、というのは、ここまで皆さんがおっしゃってきたことというのは、安江さんがおっしゃったことも私が申し上げたことも、アプリにもウェブにも同じように問題があるんだ、自分たちには分からない、利用者には分からない、スマホユーザーには分からないサードパーティーへの情報送信があるというところが問題意識として共有されていると思っているわけですが、ではどうすればいいのかというお尋ねだとすると、今の外部送信規律というのは対象が少ないわけですね。電気通信事業を営む者が基本的な対象者になっているということです。しかし、電気通信事業を営む者以外にもタグを置いてあるウェブサイトというのは無数にあって、それによって外部送信というのは粛々と行われていて、そこにおいては外部送信規律の透明性は図られていない。

図られていない場合がままあるということになりますので、それについてベストプラクティスとしてお示しして、タグを置いてあるいろいろなウェブサイトの方は、何もやっていないところいきなり来たら少し面倒くさいかもしれませんが、自分たちの大切なウェブサイト、ホームページをいじってタグを置いていただいているわけですから、ついで

に透明性を図っていただけたらどうですか、ベストプラクティスでありますけれども、そういうことが中心になってくるのかと思っています。

私の言っているお話がもし全然意味が分からないと言うことでしたらしょうがないと思うのですが、割と多くの方が普通に感じることはないかと思います。外部送信するのであれば教えてくれと。私はオプトアウトぐらいさせてくれと思いますけれども、そこは人によって違うのかもしれませんが、ウェブの外部送信がアプリと同じように行われていて、それが利用者情報の安心・安全に関して問題を生じているということ、そして、それについて電気通信事業を営む者以外についても透明性を図ってもらいたいと考えていることが問題意識であって、それが共有されていると思うのですが、その点について片岡さんはどのようにお考えになるかを教えていただきたいと思います。よろしくお願いします。

【山本主査】 ありがとうございます。

1点、私が入ってしまうとあれなんですけれども、今のお話の後半部分について、1つの懸念点は、対象者が広がり過ぎるのではないかというようなお話でしたが、今の森さんの話だと、タグを置いてあるウェブサイトがまずは対象になってくるのかなというふうにも今伺っていました。そうすると、ある種の縛りがかかるというような理解でよろしいでしょうか。

【森構成員】 縛りをかけているわけではないと思うんです。ただ、何もしていないのに、いきなり何かやれと言われたら嫌かもしれませんが、タグを置いて外部送信するわけですから、そのときに例えばサイトポリシーといったもの、様々なウェブサイトにサイトポリシーはありますけれども、ないところも結構あるわけです。そういうものを置いていただく、あるいはオプトアウトさせていただく。限定がかかっているということではないですけども、わざわざサードパーティーに外部送信しているわけですから、それに応じたことをやっていただいてもいいのではないかとということでございます。

【山本主査】 ありがとうございます。

それでは、片岡さん、お願いします。

【片岡氏】 森先生のイメージとしては、外部送信規律の対象になっていない部分について、広告タグなどサードパーティーのものを置いているところを対象に何かを記載したらいいんじゃないかというイメージで話されていることで理解しました。

我々の受け止めとしては、すごく範囲が広がるなということを感じましたし、具体的にどういものが今問題視されていて、SPSIに何を書き込むのかというのをイメージした上

で影響分析をしっかりと、それでSPSIとして本当に書くべきものなのかというのをきちんと検討していただきたいなと思いました。

当然ながら、外部送信規律の話でいろいろとさんざん議論があったことと似たような議論になるとは思いますので、そこを確認したいと思いました。

あくまでSPSIはスマホということだったと思います。そうすると、スマホのブラウザ・アプリ経由でアクセスするウェブサイトの話がされているのかなと感じましたが、いずれにしても、対象範囲が広いのと、いろいろなサイトの種類がある中で、どういう問題を解決するために書くべきなのかというのを慎重に検討していただきたいなと思っていますし、事業者としてやはり心配するところかなと思いました。

【山本主査】 ありがとうございます。

森さん、いかがでしょうか。

【森構成員】 ありがとうございます。

片岡さん、問題意識の点はいかがですか。私は、問題意識としては少なくとも我々の間では共有されているし、社会的にも外部送信の問題というのはある程度共有されていると思います。だからこそ、外部送信規律がアプリとウェブサイトで区別なくできたのだと思っていますし、例えば、あのときに、アプリはいいけれどもウェブサイトは駄目とはおっしゃっていなかったと思いますし、問題意識の共有はできていると思います。

範囲が広がるみたいなお話はありますけれども、それについて申し上げれば、スマートフォン利用者の情報の安心・安全といったときに、消費者側から見れば、スマートフォンを利用する情報というのは、アプリから出されようが自分の見たウェブサイトからつなぎかえさせられようが、それはスマートフォン利用者にとっては同じなのですよ。

事業者さんから見れば、アプリの中に情報収集モジュール入れる話とウェブサイトにタグを入れる話というのは違うのかもしれませんが、もしかしたら、例えば、所管される部局なども違って来るのかもしれませんが、消費者サイドから見れば、スマートフォン利用者として、自分が思ってもいない形で情報を取られるということは同じであり全く変わらないということでございます。

【山本主査】 ありがとうございます。

片岡さん、問題意識のところについていかがでしょうか。

【片岡氏】 広告は全て悪であるみたいな考え方には賛同できないところでありまして、結局、どういう情報がどういうふうに取りられて、それがどういう不安につながっているのか

という、そのところをしっかりと確認したほうがいいかなと思いますし、それが確認できないと事業者として影響範囲が分かりにくいかなと思います。

あと、それはウェブサイトの話なのか広告サーバーの話なのか、どっちなのかなというのが先ほどの話を聞いていても思ったりしたところです。

【森構成員】 広告サーバーの話は具体例で、サードパーティーに送信されるということを含めて話してきたと思いますが、片岡さんは仕組みが分からないとおっしゃっているのか、それとも、我々が仕組みの話をしていないとおっしゃっているのか、どういうことでしょうか。今日ずっと仕組みの話をしてきたのではないかなと思いますけれども。

【片岡氏】 仕組みの話をした上で、具体的な事象としてどういうケースが特に問題視されていて、何が不安視されているのか、それが最近の状況の変化でどういうふうに変ってきているのかということ考えた上で、SPSIにどういうことをターゲットとして書いたらいいのか考えないといけないんじゃないかと。それはSPSIに書くべきなのかなというのも考えるべきなんじゃないかという。

【森構成員】 なるほど。どんな事案で、ということですので、リクナビの話とケンブリッジアナリティカの話と有名なところでしたわけですけれども、片岡さんの想定されているどんな事案で、というのはどういうことですか。

【片岡氏】 今の外部送信規律に該当しないもので、今、世の中的に多く問題視されているようなケースですね。

【森構成員】 それはサードパーティーに知らないうちに情報が送信されるということと問題意識が共有されているのではないかなと思うのですけれども、そうじゃなくということでしょうか。

【片岡氏】 それの具体的なイメージといますか。

【山本主査】 すいません。今、まだ御質問いただいているので、少し後でもう一回、おそらく先ほど太田さんから御意見をということですので、一度、木村さんと江藤さんからの御質問を受けたいと思います。森さん、申し訳ありません。

そうしたら、木村さん、お願いいたします。

【木村構成員】 木村です。御説明ありがとうございます。

質問というより意見になると思いますが、利用者からとすると、透明性があるべきだと思います。知らないうちにいろいろな情報が取得されていて、利用されている、もちろん同意することで利用していいと納得はしているのですけれども、まだグレーだなと思うところ

はすごく感じるところです。

今日のいろいろな話を聞いていて、消費者というのはアプリとウェブサイトの利用の区別はあまりしていないのではないかとというのが私の実感で、ログインで利用しているしてないという話もありましたけれども、スマホを利用するに当たり、アプリ・ウェブサイトの区別なく保護されるものであるべきだと考えています。そういうことから考えると、SPSI策定から時間がたちまして、スマホを安全・安心に利用するという観点から、外部送信規律もありますし、時代に合わせてきちんと変更していくということが重要だと思います。その意味からも、今回、森先生の発表にありましたように、ウェブサイトを除くのは私も不適當だと思いますし、ここはきちんと入れてスマートな形で消費者保護を行っていくべきではないかと考えます。

以上です。

【山本主査】 御意見として承りました。ありがとうございます。

それでは、江藤さん、お願いいたします。

【江藤構成員】 どうもありがとうございます。森さんにお伺いしたいんですけども、ちょっと初歩的な質問になってしまうんですが。

11ページでいただいたサードパーティーの外部送信ということで、意図せぬうちに広告事業者サーバーにタグによって情報が流れているという話で、ユーザーとして現在どういった防御策が取り得るのかということで、普通のOSだったら、サードパーティートラッキング防止機能のようなものをオンにすると基本的にはこういったスキームには入っていないという理解でよろしいでしょうか。

【山本主査】 森さん、お願いいたします。

【森構成員】 私のお話はウェブサイトを中心にお話をしましたので、そんなトラッキング防止機能とか、もしかしたら何かアドオンであるのかもしれないんですけども、あんまりそういうことは細かくは知らないんですが、基本的には、普通にばんばん外部送信はされます。

ウェブサイト側から外部送信していますけれども、同意しますかというポップアップが出る場合がありますよね。また、外部送信、クッキーを使って追跡しますというお知らせが出ることもありますけれども、せいぜいそんなものじゃないでしょうか。

例えば、あんまり具体例は出したくないですけども、いろいろなウェブサイトや新聞、ニュースなどどなたでも見るような、あるいはポータルサイトなどを御覧になりますと、ポ

ップアップは全然出てこないところがあると思いますが、そういうところで50も100も外部送信されているということは普通にあります。

【江藤構成員】 なるほど。よく分かりました。

【森構成員】 それがまさにここで問題になっていることです。

【江藤構成員】 よく分かりました。消費者においてどれぐらい防御があるのか、制度によってうまくやっていないと防げない問題なのかという趣旨でした。

【森構成員】 おっしゃるとおりなのです。それを法律で何とかしようとしたのが外部送信規律でしたし、今回はせめてベストプラクティスで皆さん書いていただけないか、そういう話でございます。

【江藤構成員】 分かりました。どうもありがとうございます。

【山本主査】 ありがとうございます。

それでは、呂さん、お願いいたします。

【呂構成員】 大変丁寧に御説明いただきまして、ありがとうございます。他の先生方からの御意見も伺って、大変勉強になりました。

今から私が申し上げることが、SPSIの対象をウェブサイトを広げるべきか否かという結論に直接つながるかという自信がないのですが、お話を伺っていて思ったこととして、ウェブサイトとアプリで利用者情報が外部送信されているか、その扱いが利用者にもどのような影響を与えるかということについては、技術的に客観的に見たら、もうほとんど差異はないと思っています。

そのことについていろいろと新経連様から御指摘をいただきましたが、いろいろ理屈を立てようとしてはいるけれども、結局そこで規制されるのが困るということ、つまり、自分たちのビジネスにとって、例えば利用者情報に基づくターゲティング広告がしづらくなったら、コンバージョン率が下がるといった直接的な影響があるので、そういう事態を避けたいということなのかなと思っています。それはこのSPSIだけではなく外部送信規律もそうでしたし、古くは個人情報保護法改正の際に、端末識別情報を個人情報に入れるのかといった議論のときからずっとそうなんだろうと理解しているところです。

ただ、私としては、何でもかんでも規制すればいいかということ、そうではないと思っており、最近の動きですけれども、例えば、今年の2月にeプライバシー規則案、つまりeプライバシー指令を規則に格上げして執行力を高め、EUで統一して、いわゆる外部送信のようなものを規制することが議論されていきましたが、それが頓挫してしまったり、今、GDPRの

緩和に向けた見直しも進んでいると聞いています。それはプラットフォームがロビイングするからだというような見方もあるかもしれませんが、いずれにしても、何でも規制すれば良いのかというところで、意見の一致が見られていないということは事実だと思っています。

そうすると結局は、ターゲティング広告をするかという、これもアテンションエコノミーのような問題なのかもしれませんが、そうやって利用者情報を収集して、それぞれに合わせてパーソナライズした広告を出してアテンションを引きつけ、広告を出すことで売上げを上げていくというビジネスモデルがいいのか、というところに帰着してしまうのではないかなと思っています。

5月に、DMAの初の確定的な執行があつて、MetaのConsent or Payモデル、要するに、自分たちの情報を取られていいのであれば無料で使えるけれども、それが嫌ならば払えというモデルが違法だということで執行がされましたけれども、それによってユーザーはどう思うのか。自分たちの情報を取られてもいいからサービスを無料で使いたいというユーザーも存在すると思うのですよね。そうすると結局、ターゲティング広告で売り上げを立てるといふ事業自体どうなのか、そういった事業をレギュレーションによって制限して良いのか、根本的なアテンションエコノミーがどうなのかというところから本当は議論していくべきなのに、現状としては、ウェブサイトとアプリはどう違うのか、端末識別情報と個人情報はどう違うのか、といった、細かい理屈の部分でロビー活動を起こされたりしている状況になっているように思います。

日本は、EU対アメリカといった構図ではなく、日本にも日本のプラットフォームがたくさんいらして、日本の中で皆さんで議論できる部分も多いのに、そういった表面的な議論の対立が続いてしまうのはもったいないなというふうに思っています。

以上の根本的な問題があるということを前提としたうえで、ではこのSPSIをウェブサイトに広げるべきかという問題になると少し難しいんですけども、ただ、ウェブサイトとアプリで差異があるかといったら、差異はないと私は思っています。

【山本主査】 ありがとうございます。

まだこれから森さん、太田さんからも御発言いただきますけれども、今、呂さんがおっしゃったように、先ほどケンブリッジアナリティカ事件が引用されていたわけですが、アテンションエコノミーについては、今、自民党などでも選挙との関係で議論されているところで、ビジネス構造として懐疑的な見方も出てきているのかなと思います。日本の状況と

して、アテンションエコノミーに引き寄せて、それとの関係について解像度を上げていく必要があるのかなという気がいたしました。

おそらく片岡さんがおっしゃっていたところの1つは、実害の有無だった。どういう具体的な影響が我々個人のレベルあるいは民主主義全体に及ぶのかというところがいまいち見えないというお話かなと理解しました。日本でも、もしかしたらアテンションエコノミーとの関係である種の実害があるのかもしれない。その解像度を、日本の状況に引きつけてどのように検討していくのかということは1つポイントかなと思ったところでした。その点、森さんから何かあればと思います。

それから、プライバシーの概念との関係で、先ほどの片岡さんの御発言だと、結局は本人の権利利益に対する直接的な影響など、その辺りを問題視されているのかなというふうに思いましたが、プライバシーということを考えると、外部送信されて、その人の人となりやプライベートな側面というものが分析されるということ、それ自体がある意味でプライバシーの侵害とも言えるかもしれないわけで、プライバシー概念に関する認識の違いがあるのかなと思いました。

私的な、プライベートな側面が分析されて、その後にリコメンドションやターゲティングが行われるという、「その後」の話なのか、その点についてより解像度を上げていかなければいけないのか、それとも、そもそも、プライベートな側面が分析されているということが問題なのかというところで、議論の進め方に違いがあるのではないか。そこにある種の差分、擦れ違いが起きているようにも感じました。私からは雑駁なコメントですけれども、そういったようなことを踏まえても踏まえずともよいですが、森さんと太田さんに御意見いただいて、もし新経連さんからも何かあれば、お時間を取りたいと思います。森さん、お願いいたします。

【森構成員】 ありがとうございます。ちょっと私、言い間違いがありまして、先ほどプレゼンで2009年のeプライバシー規則と言いましたけれども、そのときはまだ規則になっていなかった指令の状態での改定だったと思いますので訂正が1点です。

もう1点は、呂先生のお話のとおり、普通に考えて、アプリの外部送信とウェブサイトの外部送信でそんな違いがあるわけではない、特に消費者の立場からすると、それに違いがあると思う人はあまりいないわけですね。プライバシー侵害と言うかどうかは別にして、意識しない間にサードパーティーに送信されてしまうことが問題だから、それを透明化しようと、オプトアウトさせてくれや同意を取ってくれという話が出てくるというのは、これは

両者の間に違いがむしろあると考えておられるなら別ですけれども、そうでないなら同じようにやりましょうというのはごく自然の問題意識で、それが共有されていないであったり、意味が分からないであったり、そういうお話はちょっとないなと思いました。

消費者視点がないということなのか、それとも、ベストプラクティスであっても対応が面倒だということなのか分かりませんが、そこに区別を設けようと、なぜウェブサイトの外部送信まで対象になるのか分からないとおっしゃっているのは、それは一般の人が聞いたら結構びっくりされるようなお話ではないかと思いました。

これが現象として近いから同じ外部送信規律という法律によって規制されていて、その立法事実も広く認識されているのに、ベストプラクティスの段階になったら、これまでアプリだけだったのになぜウェブサイトについて必要があるのか、とおっしゃると、おそらく聞いている人たちは、消費者サイドならずとも、多少なりともびっくりされるのではないかと感じたということでございます。

以上です。

【山本主査】 ありがとうございます。

太田さん、いかがでしょうか。

【太田構成員】 ありがとうございます。私からも、簡単に意見ですが、まず、SPSIは法令から一歩進んだベストプラクティスということで合意できていたと思いますが、今、外部送信規律との関係もあって、結構いびつな感じになっていると思います。外部送信規律はウェブもアプリも対象だけれども、SPSIは対象じゃないというところで、見方によっては法令から一歩後退している状態だと思います。

ただ、前回のこの議論の中で、アプリ内ブラウザは対象に含むみたいなことにもなっていて、そこはいいのに何でブラウザは入れないのといった、アプリとブラウザとで分けていることに対して分かりにくさ、いびつな状況になってしまっているのも、それはスマホのプライバシーやセキュリティと考えたときに、アプリもブラウザも変わらないというのは、森先生や呂先生のお話と一緒に。まずは、そこをきれいにしましょうというのが僕の1つ目の意見です。

最近の変わったことで言うと、SPSIも、もともとはSPIでセキュリティが入っていなかったところに、セキュリティも対象にしようと、去年追加されています。ウェブブラウザの話で、タグのガバナンスが効いていないという話はMRIさんの発表でもありましたけれども、そういった問題に対して、薦さんからも先ほど御指摘があったように、ウェブスキミングと

いうセキュリティ上の大きな問題を発生させているというのは新たな事象なのかなと思っております。

これは警視庁からもクレジットカードの被害額がどれくらいというのも出ていますけれども、実際に被害として出ていて、それはウェブにおいてタグのガバナンスが効いていない問題に直結するところだと思います。

その調査を追加でしてもいいのかもしれないですが、そういった問題も出てきていますので、SPIがSPSIになってセキュリティも対象になっていることを考えると、スマホのウェブについて問題になっているところを、ちゃんとSPSIの対象にしていくという必要があると思います。

最後に、SPSIの内容が増えているという指摘もありましたけれども、僕もそれは感じているところで、SPSIのガイドブックみたいなものをつくってもいいのではないかなという気がしています。

以上です。

【山本主査】 ありがとうございます。

片岡さんから何か付け加えることがあれば、ぜひお願いいたします。

【片岡氏】 いろいろなお話が出てくる中でも、話が広告の話になったり、先ほどのケンブリッジアナリティカの話になったり、いろいろなケースが皆さん思い浮かべているものがあるなというのを感じました。

SPSIは規制ではないと思っていまして、結局、こういうターゲットの人にこういうことをやってもらうことでこういう状況をこういうふうに変更しようという、ターゲットと目的がはっきりした上でプラクティスを書くという、そういうプラクティス集だと思っているので、それをどういうふうなものに変えていくのかという道筋を考えて、あと、やはり実務的な影響範囲や、結局、誰が対象になっているのか、それはその人たちができることなのかとも含めて、いろいろな分析が必要だと思います。

少なくとも、外側から見えていたり今までの議事録を拝見した段階で、事業者の立場で、具体的にどういうことをどういうふうにしたらどういうところに効くと思っているんだろうかというのはイメージが湧いていなかったのもそれは事実なので、その辺りをちゃんと明確にした上で慎重に検討していただけるとありがたいなと思いますし、事業者としては、物すごく膨大なやつはすごく使いにくいので、その辺りも考えていただきたいなと思いました。

以上です。

【山本主査】 ありがとうございます。

すいません。時間がオーバーしてしまって大変申し訳ありませんでした。何かここで一言言っておきたいということがあればお願いしたいと思いますが、いかがでしょうか。よろしいでしょうか。

いろいろな御議論があって、ウェブサイトについても、アプリと同じようにリスクがあるのであれば、公平性というか平等の観点から、同じリスクがあるのにもかかわらず、なぜウェブサイトはそうでないのかという話にもなってきます。そういう意味で、問題意識については、構成員としてはそれほど認識の齟齬がないのではないかと、一定の共通認識があるのではないかと私も思っております。今後、そこがより理解できるような形で整理をしていく必要があるのかなとも感じた次第です。

いろいろとまた調査を、特に消費者目線、ユーザー目線という話が出てきましたけれども、そういう目線から見てどういうふうな世界になっているのか、そういうことも含めていろいろと調査をしていく必要も出てくるのかなとも感じた次第です。

時間がオーバーしてしまって申し訳ありませんでした。また、新経連の片岡さんには貴重なプレゼンをいただきまして、ありがとうございました。改めて御礼申し上げます。

それでは、今日はここまでにさせていただいて、事務局から連絡事項をお願いいたします。

【小玉利用環境課課長補佐】 ありがとうございます。事務局でございます。本日、議論いただき、本当にありがとうございました。

次回会合につきましては、6月中旬を予定しております。詳細につきましては、追って事務局から御連絡を差し上げます。

本日の議事録につきましては、事務局で作成の上、皆様に御確認いただいた後、公表することを予定しております。

以上でございます。

【山本主査】 ありがとうございます。

それでは、時間が押してしまって、改めてお詫び申し上げます。

これをもちまして、第26回の会合を終了させていただきます。本日もお忙しい中、御出席をいただきまして、ありがとうございました。