

消費者委員会

消費者法分野におけるルール形成の在り方等検討

ワーキング・グループ

第28回議事録

内閣府消費者委員会事務局

消費者委員会
消費者法分野におけるルール形成の在り方等検討
ワーキング・グループ（第28回）
議事次第

1. 日時 令和3年5月12日（水）13:02～14:31

2. 場所 消費者委員会会議室・テレビ会議

3. 出席者

（委員）

丸山座長、新川座長代理、山本委員長、片山委員長代理

（オブザーバー）

柄澤委員、大石委員、大阪大学大学院法学研究科教授 清水真希子氏、京都大学法学系
（大学院法学研究科）教授 原田大樹氏

（説明者）

株式会社DataSign 太田 祐一代表取締役社長

（事務局）

加納事務局長、渡部審議官、太田参事官、大岡企画官

4. 議 事：

（1）開会

（2）インターネット広告の仕組みについての有識者ヒアリング

（3）閉会

《 1. 開会 》

○太田参事官 本日は、皆様、お忙しい中、お集まりいただき、ありがとうございます。

ただいまから、消費者委員会第28回「消費者法分野におけるルール形成の在り方等検討ワーキング・グループ」を開催いたします。

本日は、所用により、山本委員長が遅れての御参加、新川座長代理が途中退席との御連絡をいただいております。

議事に入ります前に、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。不足等がございましたら、事務局までお知らせください。

なお、本日の会議は、ウェブ会議による開催となります。公開で行いますが、感染拡大防止の観点から、一般傍聴者を入れず、報道関係者のみ傍聴いただいで開催となります。

議事録につきましては、後日公開することといたします。

次に、ウェブ会議による開催に当たりましてお願い申し上げます。

1つ目に、ハウリング防止のため、御発言いただく際以外は、マイクをミュートの状態にしていただきますようお願いいたします。

2つ目に、御発言の際は、あらかじめチャットでお知らせください。座長に御確認いただき、発言者を指名していただきます。指名された方は、マイクのミュートを解除して、冒頭にお名前をおっしゃっていただき、御発言をお願いいたします。御発言の際、配付資料を参照する場合は、該当のページ番号も併せてお知らせください。

なお、御発言の際には、可能であればカメラのマークのミュートを解除していただきましたら、どなたがお話しになっているかが分かりやすくなりますので、御協力をお願いいたします。

3つ目に、音声聞き取りづらい場合には、チャットで「聞こえない」「聞こえにくい」などと記入していただき、お知らせいただきますようお願いいたします。

それでは、丸山座長、以後の議事進行をよろしくをお願いいたします。

○丸山座長 座長の丸山です。どうぞよろしくをお願いいたします。

本日の議事進行についてですが、途中で私の回線が切れた場合は、復旧するまでの間、新川座長代理に、新川座長代理の回線も併せて切れた場合は、事務局に進行をお願いします。

《 2. インターネット広告の仕組みについての有識者ヒアリング 》

○丸山座長 それでは、本日の議題に入らせていただきます。

本日は、インターネット広告の仕組みについて、有識者ヒアリングを行いたいと思います。

本日は、株式会社 DataSign 代表取締役社長の太田祐一様にヒアリングをさせていただき、その後、委員、オブザーバーの皆様でヒアリングを踏まえた意見交換を行うということで進行したいと思います。これまでのヒアリングと同様の形で進めてまいりたいと思います。

それでは、まず、太田様へのヒアリングを実施します。

御入室いただきますので、委員、オブザーバーの皆様は、準備が整うまで少しお待ちください。

(株式会社 DataSign 入室)

○丸山座長 本日は、参考人として、株式会社 DataSign 代表取締役社長の太田祐一様にお越しいただいております。

本日は、大変お忙しい中、ありがとうございます。

それでは、30 分程度でお話しいただきますよう、よろしく申し上げます。

○株式会社 DataSign 太田代表取締役社長 「インターネット広告とトラッキングの実態と動向」というタイトルの資料になります。

ページ番号 2 ページ目に「自己紹介」と書いてありますが、簡単に私の自己紹介をさせていただくと、DataSign の太田と申しまして、DataSign の代表をさせていただいているのですが、そのほかにも関連するところでいうと総務省のプラットフォームサービスに係る利用者情報の取扱いに関するワーキンググループの構成員もやらせていただいたりしております。

DataSign という会社が何をしているのかというと、下のポツに書いてあるように、データ活用の透明性確保と公正なデータ流通を実現するために、DataSign を設立と書いてあるのですが、なぜそう思ったかという「DMP/MA をたくさん作ってきました」と書いてあるのですが、これは何のことか分からないと思うのですが、これまで広告のデータとかマーケティングに使うデータを収集するプラットフォームを幾つか作ってきました、その中で消費者が想像していないようなデータの収集方法とか使われ方を、プラットフォームを提供しながらやっていたのですが、よくよく考えてみると、これは消費者目線からすると、こういう情報が集められているなんて知らないし、個人目線ですると嫌だなと思いつつそういうことをやっていたのですが、その嫌だなということをやり続けるのはよくないので、そういった状況を変えていくために DataSign という会社を立ち上げております。

30 分ということなのですが、本日お話しする内容として、インターネット広告の仕組みです。先ほどインターネット広告とかマーケティングに使うデータを扱っていたところで、どういう仕組みでインターネット広告が行われているのか、その上でトラッキングをして消費者のデータを集めていくのですが、そういったところの実態がどうなっているのか、あとは最近の動向と大きく 3 点お話しさせていただければと思います。

4 ページ目に行きまして「よくイメージされるインターネット広告」と書いてあるのですが、人によってインターネット広告にどういうイメージを持っているのかは分かりませんが、多分、よくいわれるのは、アドネットワークみたいなのがあって、いろいろな広告枠、要するに広告が表示されることを束ねてやっているのだみたいな理解の方が多く思っております。

実際にそうなのですけれども、これは左下に書いてあるように、1998年ぐらいから始まった仕組みで、20年以上前から始まっているし、今でもあるのですけれども、結構トラディショナルなやり方です。

昔はこうだったのですけれども、今はどうなっているかというと、5ページ目です。「現在のインターネット広告」。「現在の」とかいいながら、この図に書いてあるものは2010年段階の話なのですけれども、先ほどのアドネットワークという存在が代理店と一緒に広告枠、表示される側を集めて、広告主はどこでアドネットワークで配信するということを決めて配信するというシンプルなものだったのですが、今はここに書いてあるように、DSPとかSSPは後で説明しますけれども、いろいろな事業者がデータのやり取りをしながら、どこかの広告主の広告をどこかの広告枠、メディア、インターネットサイトに表示していくかというのを、リアルタイムビディングと呼ばれるのですけれども、オークションをしながら広告の表示を決めていくという非常に複雑な仕組みになっております。

この複雑な仕組みに関しては、後ほど説明するのですけれども、ここで最初に説明しておきたいのが、ここに「JS」とか「SDK」と黄色いタブみたいなものがついていると思うのですが、これが情報を収集したり、広告を表示したりするためのモジュールの名前です。こういったものをいろいろな広告事業主とか広告主、インターネットのサイトとかの表示するメディアといったところが、JSと呼びますけれども、JavaScriptとか、アプリに関してはSDKで、JSとSDKの違いは、ウェブだったら大体JavaScriptで、アプリだったらSDKで覚えていただければいいのですけれども、そういったモジュールをウェブサイトに組み込んだり、アプリに組み込んだりしながら広告のデータや広告の表示を行ったりしております。

6ページ目に行ってくださいと、JavaScript(JS)タグとかSDKがどういうことをしているのか、どういう情報を取得しているのかというところを書かせていただいております。

ウェブサイト、アプリでもほぼ同じなのですけれども、まず、赤字で「オンライン識別子」と書いてあるのですが、これは後ほど詳しく説明します。オンライン識別子は、要するにブラウザを特定したり、端末を特定したりするためのIDを取得しますというのはどちらもやっています。そのほかにIPアドレスとかURL、アプリの名前といったものを取得していたり、ウェブサイトだったらページに表示されている内容とか、アプリだったらアプリに表示されている内容といったものも取得することができます。

あとは、環境情報です。ウェブサイトを表示しているブラウザの画面のサイズがどうか、画面サイズだけではなくて、例えばiPhoneのバージョンが幾つでという環境の情報です。どういう環境からアクセスしているかという情報も取得することができます。

あとは、フォームに入力されるような情報です。IDとパスワードとか、お問合せだったりするとメールアドレス、決済画面だったらクレジットカード番号も取得することができます。

広告の表示もJavaScriptタグとかSDKなどで行っております。

要するに、ここでいいたいことは何かというと、JavaScriptのタグとかSDKを広告目的で安易にウェブサイトやアプリとかに組み込んでしまうと、いろいろな情報が取得できるようになって

しまいます。こういうところに気づいていない、要するにウェブサイト事業者も広告事業主から JS タグを入れてくださいといわれるのですけれども、それでどういう情報が取得されて何ができるのかというのをあまり知らずに導入しているケースが結構あります。

7 ページに行って、オンライン識別子の話なのですけれども、これはウェブとスマホ、要するに JS タグで取得できるものと SDK で取得できるものは違うものになっておりまして、ウェブの場合はサードパーティークッキーがメインで、あとは最近、ローカルストレージやフィンガープリントとかがありますが、フィンガープリントは後ほど説明しますけれども、最近、クッキーが使えなくなるみたいな文脈でよくいわれているのがサードパーティークッキーで、要するにサードパーティークッキーが使えなくなってくると、ウェブで識別子を取得できなくなっていくので、ターゲティング、トラッキングができないということになってきていますというのが現状です。まだ使えるのですけれども、来年の1月ぐらいには使えなくなるといわれております。

スマホの場合、SDK で取得できるのは、iOS の場合は IDFA (ID for Advertisers) と呼ばれているもので、アンドロイドの場合は AAID、もしくは ADID とも呼ばれますけれども、これも広告用の ID として識別子を OS レベルで提供しています。iOS の IDFA のほうは、後ほど説明しますが、4月26日から、利用するには、アプリのところで許可しますかというダイアログが出てきて、同意必須になったので、IDFA も勝手に使うことはできなくなっています。こういったオンライン識別子を使って識別して、ターゲティング広告を打っている。

先ほどのごちゃごちゃしている RTB の仕組みをここから説明していくのですけれども、3 企業というか、企業は同じ場合もあるのですが、主に3つの登場人物がいます。

DSP と SSP と DMP という登場人物なのですけれども、それぞれ役割がありまして、DSP と呼ばれるものが、広告主側に立って、広告主の利益を最大化する。要するにデータを使って、広告の効果を最大化させるというのを広告主に向けてやっているのが DSP で、Demand-Side Platform の略でございます。

次に、SSP が、今度は広告主側ではなくて、メディア側、広告を表示する側の広告収入を最大化させる。どの広告を配信したら一番もうかるのかというのを計算して、広告を出す。

なので、DSP と SSP は、利益相反なわけです。広告主側は安く、たくさん広告を出したらいいし、メディア側は高く、たくさん出したいので、これは分かれているのが望ましいということで分かれたのですけれども、ここでデータのやり取りもしています。

DMP は、分かっていたり、SSP の中、DSP の中に組み込まれていたりするのですけれども、これは Data Management Platform の略で、この広告を表示するためのデータといったものを蓄積したり、活用したりするものを DMP と呼んでいます。

これらの3者がどのようなやり取りをしているかというのを、9 ページ目から「RTB の仕組み」ということで説明しております。ここからは流れに沿って説明していきます。

9 ページ目は、SSP です。SSP は、メディア側、例えば日経オンラインに導入されている SSP があって、日経オンラインに例えば僕がアクセスしました。そうすると、メディアには SSP が導入されているので、SSPID がオンライン識別子、先ほどのウェブでいうとサードパーティークッ

キーとして、SSP が付与する ID がユーザーのブラウザに付与されます。それが例えば ABC だったとします。

そうすると、僕が日経オンラインを訪れると、SSP が DSP 側に SSPID が ABC の人がメディア A、この場合は日経オンラインですね、日経オンラインの枠 001 は、トップページの右上とかにしましょうか、トップページに訪れましたという情報を SSP が DSP をやっている各事業者に送信します。大体全部で数十社あるのですけれども、SSP が提携している DSP に送信されます。

そうすると、DSP 側は、ID が ABC の人が日経のトップページに訪れたのだなという情報を受け取って、10 ページ目に行くと、DSP は、DSP 側での ID と SSP 側での ID のマッピングテーブルを持っていて、SSPID が ABC という人は、DSP 側の ID では 123 というので、DSP 側で特定できます。

11 ページに行ってくださいまして、では、DSPID が 123 という人は、どういう人なのか、どんなデータがあるのかというのを DMP に問い合わせます。そうすると、DMP 側には、DSP と DMP の ID のマッピングテーブルがあって、DSPID が 123 の人は、DMP 側では XYZ で、その人には「男」という情報が付与されていますと。そういう情報を DMP が DSP に返します。それが③です。

12 ページに行ってくださいますと、今度は、DSP がこの人は男なのだということが分かったら、日経に訪れた男の人に広告を見せるために、幾ら払いますと入札します。それを SSP 側に返すのです。

例えばこの DSP は 100 円で入札します。今の絵では 1 つだけになっているのですけれども、数十社が一気にばっと同じことをします。持っているデータとか価格を判定するロジックがそれぞれ違うので、DSP がそれぞれ値づけをします。いろいろな DSP が 100 円で入札しますとか、50 円で入札しますというのを SSP 側にながと送って、その中で一番高い値段を付けた人、この場合は 100 円が一番高いと仮定すると、100 円が一番高かったので、あなたが落札できましたという返信を SSP が DSP 側にして、DSP は、落札したのだったら、この広告を表示しますとあって、SSP 側に広告の画像とかを介して、実際に日経オンラインに表示されるという仕組みになっております。これが RTB という仕組みです。

なので、メディア側も SSP を介して、どこの DSP が落札して、どんな広告が出るかというのを事前に見ることがなかなか難しく、メディア側はどういう広告が出るのかというのはあまり把握できたりしないです。DSP の裏側にいる広告主側も、いろいろなところに入札していくので、ある程度分かるのですけれども、最終的にどういう広告がどのメディアに出るかというのも把握しづらい状況になっています。

その中で、SSP とか DSP、DMP が ID のやり取りをしながらそこにひもづくデータは、入札が行われると、例えばもともと DMP が男性ですという情報だけを持っていたとしても、例えば DSP 側から日経から来ましたという情報が来るので、この人は日経に来たから、ビジネス系の人なのかみたいなことが推測できるので、その情報もまた分析の中に入れて、DMP が持っている情報にこの人は男で、ビジネス系のメディアを見ていてという属性がどんどん付与されていって、いろいろなところでいろいろな情報が取得されているという状況になっております。

それで、どれぐらいの事業者がデータを取得しているのかというのを調べてみたのが 14 ページでございます。「とある生活者の 1 日」と書いてあるのですけれども、僕なのですが、調べてみたのですけれども、僕は、1 日生活すると、5 つのアプリを使って、60 のサイトを見ていました。60 サイトにアクセスしているの、日経とかいろいろなところを見ていますけれども、自分がアクセスしたという情報は、60 のサイトに自分が行った、ブラウザに来たということが分かるのは当然なのですが、先ほどのオンライン識別子を使って自分をトラッキングしている事業者がどれぐらいいるかというのを調べてみたところ、この 60 サイト 5 アプリ以外に、1 日で約 250 の事業者にデータを送信しておりました。

この 250 の事業者はどういうのがあるかというと、広告系が一番多くて 123 社で、グーグルとかの有名どころがあったり、あとはアクセス解析です。これはそんなに大きな問題にはならないのですけれども、グーグルアナリティクスとかそういったアクセスの解析です。あとは、データ仲介、データを販売している業者です。先ほどの DMP みたいなところが多いですけれども、例えばこの人は男だとか、ビジネスに興味がある人だとか、自分の情報を集めて、そこから属性を導き出して販売しているような、そういう情報を集めている会社にもいろいろと提供されているという状況になっております。

基本的にウェブは 60 サイトと 5 つのアプリなのですけれども、スマホアプリだけに絞った調査もしてみましたので、アプリを起動した場合にどういう通信がどうか、どれぐらい広告のリクエストみたいなものが送られているか、データのリクエストが送られているかというのを調べたのがこちらで「ニュース系のアプリ 2 つ」と書いてありますけれども、具体的には、SmartNews と NewsPicks です。これを 2 つ起動して、数ページ閲覧しただけで「133 のホスト」は、133 の企業とほぼ同義だと考えてください、133 の企業に 237 回のリクエスト、237 回何かのデータが送られているということが分かりました。

アプリとかウェブを見ると、いろいろなところにデータが送信されていることが分かったので、では、それをちゃんと開示しているのかということをお我々 DataSign で調べてみました。

これは毎年やっているのですけれども、最初に日経に取り上げていただいたのが 2019 年 2 月です。このときは日経の一面トップにもなったのですが、ほとんどの企業がどこにこういうデータを共有しているかというのをほとんど正しくプライバシーポリシーに書けていないということが分かりました。

16 ページにその結果が載っているのですけれども、1 位の福岡銀行は、福岡銀行のウェブサイトに訪れると、福岡銀行以外の 80 の会社にデータが送信されています。「共有先の開示」が「○」になっているのですけれども、実際はかなり判定が甘くて、この 80 の共有先のうち、1 個だけ書いてあったので「○」なのですが、他の 79 個は何も書いていないという状況です。

他の企業もそんな状況なのですけれども、企業側もどこが自分のウェブサイトからデータを収集しているかというのがあまり分からないので、書けないところもあるのですが、共有されている数と共有先の開示自体をしていないところが「×」なのですけれども、そういったと

ころも半数ぐらいありますし「○」になっていても、1個だけ開示しているという状況になっております。

あと、朝日新聞が、収集している中に位置情報がどれぐらいあるかというのを我々と一緒に調査したのですけれども、位置情報に関しても、外部業者と共有しているけれども、半数が明示していない、位置情報を取っているのに、取っているといていないというのが半数ぐらいあったという調査結果も出ております。

そんな状況の中で、クッキーや IDFA とかのオンライン識別子にそういう情報をひもづけてデータを収集することは、利用者に対して全然透明性もないし、昨今のプライバシーに対する風当たりの強さ、そういうデータの収集に対する風当たりの強さから、プラットフォーマーがこっそりとデータを収集するのはよくないから、できないようにしますとっていて、アップルは 2017 年ぐらいから ITP という仕組みでクッキーを使ったトラッキングをどんどんできなくしてしまっていて、Google Chrome のブラウザでも、来年 1 月にサードパーティークッキーを使えなくしますというアナウンスをしています。

アプリに関しても、4 月 26 日から IDFA の利用に同意が必須になりました。実際にこういうのが出ます。今説明しているのは 18 ページです。ここにアプリ名が出ているのですが、「どこどこが他社の所有する App や Web サイトを横断してあなたを追跡する許可を求めています」というのに「許可」というのを押さないと、IDFA（オンライン識別子）を使うことができないというふうになっております。

これが使えなくなってしまうと、先ほどの RTB の参加者の DMP とか DSP、SSP が困ってしまうのです。これが使えなくなったらターゲティングができないではないかということで、今、この許可を頑張って得ようというところと、サードパーティークッキーとかが廃止されてしまったときに、要するにブラウザ側に ID を保存するのが難しくなるので、フィンガープリントという技術でブラウザを特定していこうと。

これは、先ほどのどういうデータが取れるかという話のときに、環境情報が取れるというお話をしたと思うのですけれども、どういう OS で、画面サイズがどれぐらいでとか、そういう情報を組み合わせて、1つのブラウザ、1つのデバイスを特定していくという技術を使って、結構昔からあるのですけれども、また最近はやっているというところでは。

フィンガープリントは、どういう情報を使って特定しているのかというのは、結構ブラックボックスなので、取得していてもばれにくいですし、ユーザーも拒否できないというか、拒否しにくいので、日本ではフィンガープリントに関して特に規制もないので、別に規制がないのだったら、フィンガープリントでじゃんじゃんやればいいではないかと考える人も割といます。アメリカとかでは、フィンガープリントは自主規制でできなかつたり、ヨーロッパだとそもそも規制されているというところで使われなくなってきたのですけれども、逆に日本では特に規制がないので、むしろ今、使ったらいいのではないかという流れになっています。

あと、グーグルは、サードパーティークッキー、要するにオンライン識別子を勝手に取得できるようなものはなくすけれども、識別子を使わなくても広告でターゲティングできるような仕組

み、これを総称してプライバシーサンドボックスと呼んでいるのですが、御存じの方もいるのかもしれないのですが、FLoC と呼ばれる機械学習を使って、ID を指定してこの人に広告を出すのではなくて、ある何かに興味がある人群みたいなものをブラウザが作って、そのブラウザで判定されるコホート（セグメント）を利用して、広告を打つという仕組みに変えていこうと提案しているのですが、これも要するに ID、識別子を使っていないだけで、その人の興味を分析してターゲティングしているということには変わりないではないかというところと、ブラウザが直接収集して判別しているの、今まではタグや SDK とかがなければ、そこは収集の対象にならなかったのですが、ブラウザでアクセスしたら、それが全部対象になるので、そういう意味では今までよりもたくさんの情報を使っているのではないかとわれていたり、いろいろと批判の対象になっていたりします。

そういった中で、グーグルに対抗するような勢力も出てきています。識別子を使わないターゲティングは、グーグル的にはいいかもしれないのですが、他のグーグル以外の広告事業者にとっては、ID を使ってターゲティングしていきたい、そうしないとちゃんと分析もできないし、ちゃんと自分たちで分析していきたいので、別の ID を作りたいたいという業界団体を設立していますというのが、21 ページの話です。

いろいろな広告主とか広告事業者が入って、PRAM (Partnership for Responsible Addressable Media) というのを作って、ここが推進しているのが、22 ページのメールアドレスベースの ID です。今まではオンライン識別子、先ほど説明した中ではクッキーとか IDFA という端末を識別していくもので取得していたのですが、そうではなくても、メールアドレスをベースにして、広告の ID としてやり取りしたほうが、デバイスをまたぐこともできるし、同じ人がウェブサイトを見ている、アプリを使っているというところも、メールアドレスが一緒だったら人をターゲティングできるから、よりいいと。かつ、GDPR では、広告のトラッキングは同意がないとできないので、同意を取るのだったら、クッキーやオンライン識別子とかいってないで、メールアドレスを使いますということに対して同意を取ってしまえば、人を特定できるからそのほうがいいのではないという流れになってきています。

「オンライン識別子まとめ」と 23 ページにまとめさせていただいておりますけれども、これは何が書いてあるかというと、会社 1、2、3、サービス A、B、D、E とありますが、要するに、みんなやりたいのは、会社をまたいだトラッキングです。会社をまたいでオンライン識別子を使っていきたい。広告を出すときに、あそこのサイトに行った人にここで広告を出すとかしたいので、会社をまたぎたいというときに、サードパーティークッキーは規制というか、ブラウザの仕様で使えなくなってしまう。もう一つあるのは、IDFA、黄色い部分で、iOS で共通した ID を使えますが、同意が必須になっている。Unified ID 2.0 は、メールアドレスが共通なので、先ほどのメールアドレスを使っていこうというところで、ここが今、有力視されているという感じです。

あと、同意管理ツールについて少しお話ししたいのですが、先ほどの GDPR では、トラッキングに同意が必要ですので、その同意を得るためのツールとして発展してきております。24 ページです。

トラッキングするために同意が必要ということで、クッキーバナーとか CMP と呼ばれるものが日本でもいろいろとちょいちょい使われるようになってきたのですが、25 ページを見ていただくと、同意としてあまり有効ではないものです。要するに、ウェブサイトアクセスするか、アプリを利用すると、クッキーの利用とかそういったオンライン識別子の利用に同意したものとしますという書き方のものも結構多いです。GDPR 上では、もう有効な同意として認められませんといわれているのですが、こういうのが日本で残ってしまっているという状況になっております。

そういう状況になっているのは、日本では、先ほどのオンライン識別子とかオンラインの特定をしていく部分に対して、明確な法的ルールがないところが結構問題なのかなと思っております。個人情報保護法で特定の個人とひもづく場合は規制の対象になるのですが、先ほどのブラウザを特定しているとか、デバイスを特定しているというのは個人情報にならないので、その部分に関しては特に法的なルールがない。広告は特定の個人を識別していませんとずっといつてきているので、そこについてルールはありません。

ただ、GDPR 対応もあって、同意を取得しようと頑張っているのですが、25 ページのなんかちゃって同意になってしまったりするので、同意を得るといのは、あまり得策ではないかなと思っておりまして、自社のウェブサイトとかアプリで、どういう事業者が何のためにデータを収集しているかということをちゃんと公表することを明確にして、そのオプトアウト、拒否できる機会を徹底するというのが必要なのではないかと思っております。

私からは以上になります。ちょっと時間をオーバーしてしまいました。失礼しました。

○丸山座長 ありがとうございます。

それでは、引き続きになりますけれども、40 分程度で質疑応答をお願いしたいと思います。

ただいまの御説明を踏まえまして、御質問、御意見のある方は、御発言をお願いしたいと思います。

御発言をされる場合には、まずはチャット欄に質問希望である旨を投稿いただければと思います。

いかがでしょうか。

質問をお待ちしている間に、私から何点かお伺いしたい点があるのですが、よろしいでしょうか。

○株式会社 DataSign 太田代表取締役社長 はい。

○丸山座長 よろしく申し上げます。

最初に、お話できるかどうか分からないのですが、DataSign をお立ち上げになった際に、そういった広告マーケティングなどを行っている業界でデータ収集あるいは利用の仕方について、率直に嫌だなという印象を持たれたということなのですが、可能であればなのですが、嫌だなと思った事象をもう少し具体的に教えていただければと思います。これが第 1 点の質問になります。

第2点の質問としましては、私自身も日経オンラインなどを利用する際にプライバシーポリシーに行って、すごく多くの会社が並んでいて、全部を断ることなんかとてもできないと思った記憶があるのですけれども、これからの将来の流れについてお話していただいたときに少し気になりましたのが、メールアドレスでのトラッキングをするというところなのですが、メールアドレスになりますと、個人との結びつきが非常に行きやすくなってしまわないかと思ひまして、単純に、そもそもどうやってメールアドレス ID を収集していくことになるのか、具体的なイメージが素人だとつかみにくかったので教えていただきたい。また、個人情報保護法との関係で、現在は、広告などはすぐには個人情報にはならないので、なんちゃって同意なども普及しているというお話だったのですけれども、こういったメールアドレスとなった場合に、そういったお話が通用するのか、個人情報と結びつくほうが普通になってしまうのではないかという懸念はないのでしょうか。

第3点としましては、いわゆるブレイブなどの広告を出さないことをポリシーとしているブラウザについては、こういった懸念はないという理解でいいのかどうか。この3点について教えていただければと思ひました。よろしくお願ひします。

○株式会社 DataSign 太田代表取締役社長 ありがとうございます。

1つ目の嫌だと思ひた経緯というか、具体的なお話ですけれども、主には2つあるかな。

1つは、あるゲーム SNS みたいなもののデータの分析をしているときに、実際の男女比はどれぐらいなのだろうと。要するに、SNS でゲームをするときに性別も入れて登録するのですけれども、どれぐらいそをついているのだろうというのを調べようと思ひて、クレジットカード会社が持っている男女の情報と突き合わせてみたのです。要するに、クレジットカードを作るときにいつている性別と、ゲームをするときにいつている性別にどれぐらいかい離があるかというのを調べたのですけれども、そのときに、SNS で女性といつている人の6割が本当は男性だということが分かりました。そういうのをやったことがあるのですが、そもそも SNS でゲームをしている人は、女性と登録していつて、その情報が自分の使いつているクレジットカードの情報といつの間にかひもづいつていつて、本当の性別がばれるなんてことは全く想定していつないでしょうし、自分だったらそれはすごく嫌だなと思ひたのが一つ。

もう一つは、マーケティングオートメーションの話なのですけれども、今は、お問合せフォームからお問合せをすると、クッキーとかのオンライン識別子と問合せをしてきた人がひもづいつて、例えば最初に自分の名前とかメールアドレスを入れて、普通にお問合せをします、そうすると、クッキーの ID とメールアドレスや名前とかがひもづいつて保存されて、例えばその人がお問合せをする前にどういつページを見ていつたかとか、お問合せをした後にどういつページを見たかというのが分かつたりするのです。それで、この人はこのページを見ていつるから、こういう案内をしようとか、そういうことをするのですけれども、あるとき、以前、そうやってお問合せをしてきたことがある人が、そういうオンライン識別子でひもづいつているということを知らずに、お問合せフォームから名前を入れずにごい暴言を吐いたのです。そこでは名前を入れていつないのですけれども、本当は、この人がどのページに来て、どういつことを書きこんでいつるというのが裏側の

データベースではひもづいているので、前にお問合せをしてきたあの人がこんな暴言を吐いているというのを、実は事業者側は知っているみたいなことで、もしそれが自分だったらすごく嫌だなと思ったというのが、いつもしゃべっているような話です。

次に、Unified ID、メールアドレスベースお話で、まず、個人情報になるか、ならないかというところでお話しすると、これは皆さん御存じだと思いますけれども、oota●datasign.jp は個人情報だけれども、abcde@gmail.com は個人情報ではないというのは共通認識としてあると思います。ただ、例えば個人情報にならないメールアドレスがあったとしても、そこに名前とかデータベース上に個人を特定できるようなものがあれば、メールアドレス自体も個人情報になりますねというのはあります。

では、そういう情報をどうやって集めていくかということ、先ほど日経オンラインとかもお話しになりましたが、会員登録するときにメールアドレスとかを入れるので、そのときに取得したメールアドレスを使うのです。今は会員登録をしなくても見られるメディアみたいなのはたくさんあると思うのですが、多分、今後、メールアドレスでターゲティングをしていくために、記事を読むにはメールアドレスを提供してくださいというのでメールアドレスを集めていくのだと思っています。

実際にそういう動きは結構出てきていて、ソーシャルログインとかをさせてメールアドレスを収集するとか、メールアドレスを何とかゲットして、この Unified ID でトラッキングしていこうというのは、まだ正式に始まっていないのですが、そういった動きになっております。

3つ目のブレイブの件なのですが、ブレイブ自体は、オンライン識別子を保存できないようにしていますので、サードパーティクッキーを識別できないようにしているので、サードパーティクッキーを使えないという意味では、そういう情報は収集できないのですが、例えばブレイブを見ていて、メールアドレスを日経に提供して、それが Unified ID として利用されるといところは防ぎようもないですし、フィンガープリントもブレイブのブラウザを使っているという時点で結構絞り込まれたりしますし、そこにちょっと環境情報を入れるとフィンガープリントしやすいので、むしろブレイブを使っていたほうがフィンガープリントされやすいのではないかとちょっと思ったりしています。

○丸山座長 ありがとうございます。

引き続き質問が来ておりますので、よろしくをお願いします。

まずは柄澤委員からよろしくをお願いいたします。

○柄澤オブザーバー 柄澤です。御説明ありがとうございました。

2点質問がございまして、1点目は、資料の5ページの関連でございまして。私どもは保険会社のグループでございまして、グループの中のダイレクト系の保険会社がインターネット広告を主体として活用している関係で、概括的には理解していたつもりですが、今の御説明の中で、5ページに記載のとおり、ユーザーはサイトでネット広告を閲覧するまでに大変多くの事業者が関与する実態にあると理解いたしました。

DSP、SSP、DMP それぞれにつきまして、どのくらいの数の事業者が存在して、そこが寡占状態にあるのか否か、どのような事業者団体があり、また、その加入率はどうなっているのかということにつきまして、御存じの範囲で御教示いただければと思います。

2点目が、資料の26ページでございますけれども、この記載の中で、下のほうに「提供元のウェブサイト・アプリでの取得事業者の公表の明確化」が必要だがございます。大変必要な視点だと思われま。事業者のホームページ上での表示などで、こういう点についてベストプラクティスと思われる事例があれば、その内容について御教示いただければと思います。

○株式会社 DataSign 太田代表取締役社長 ありがとうございます。

1点目についてなのですが、DSP、SSP、DMP がそれぞれ何社ぐらいあるのかというのは、今すぐには正確に分からないのですが、DSP、SSP は日本でそれぞれ大体30とか50ぐらいいるかなと思います。DMP はちょっと少なくても10~20とかそれぐらいかなという印象です。それらの企業が加入している団体がありまして、JIAA（日本インタラクティブ広告協会）というのがありまして、こちらの会員数は、今、ちょっと分からないのですが、ここはDSP、SSP以外のところも入ってはいるので、多分100社ぐらいはいるのかなという感じでございます。

2点目のベストプラクティスなのですが、ベストというか、今、キャリア各社、プラットフォームと呼ばれる人たちは、今、26ページに書かせていただいたように、どこが収集しているかというのを明確にして、オプトアウトの機会をちゃんと設けようという対応をしております。

ただ、これがベストではないと思っている理由は、どこの事業者がいます、取得拒否の場合はここですというのが一応あるのですが、先ほどお話にあったように、だっとたくさん並んでいて、全てオプトアウトするのは面倒くさいし、無理だねという話があります。なので、その取得の拒否のところをちゃんと一括でできるようにするものが必要になってくるのではないかと考えておまして、その一例が24ページに「個人情報保護の設定」という画面がべらっと貼ってあると思うのですが、これはカテゴリーしか書いていないのですが「アナリティクス」とか「パーソナライゼーション」「広告」のチェックを外して、広告用途の場合は一括してオプトアウトしますとか、そういうユーザー側のコントロールが必要かなと思います。かつ、僕らもCMPツールを提供しているのですが、要するにこの広告の中にどういった事業者がいるのというところまでもちゃんと見ることができるとベストなかなと。それは見たい人が見られればよいだけで、広告を外したい人は広告を外すとか、全部嫌な人は全部外すといったのがユーザー側でちゃんとできるというのが一番よいかなと思っております。

○柄澤オブザーバー ありがとうございます。

○丸山座長 それでは、続けて、大石委員、よろしくお願ひします。

○大石オブザーバー ありがとうございます。

こういう世界のことが今まで全然分かっていなかったのが、驚くようなお話で、いろいろなところに大変興味があったのですが、一つ教えていただきたいのが、13ページのRTBの仕組みのところ、名前もよく分からないのですが、DMPにある程度基本の情報があって、そこがど

んどん回っていくということだったのですが、DMPは、費用は誰からもらうのですか。DSPなのか、どこからお金が回ってきて成り立つのかというのが一つと、例えば送られた情報で瞬時に入札されるのも初めて知ったのですけれども、SSPに出したものをその人がちゃんと見たとか、関心を持ったという情報がまたDSPからDMPに戻ったりということで、情報がどんどんDMPに蓄積されていくことになっているのかなと思ったら、すごく驚いたというか、びっくりしたのですけれども、そこら辺のことをもう少し教えていただきたいのが一つ。

あとは、俗世間の話で、アンドロイドとiOSといいますか、アップル系だと、そういう意味では、アンドロイドよりはiOSのほうがいろいろと厳しいので、個人情報の面でも安心だということをごっと聞くことがあるのですけれども、先ほどのお話の中でもそれに近いような説明もあったような気がするのですが、実際のところどうなのか、なぜそうなのかというところがもし分かれば、教えてください。

○株式会社DataSign 太田代表取締役社長 ありがとうございます。

1点目なのですが、DMPのビジネスモデルというか、マネタイズモデルは、この広告の文脈でいうと、ほぼDSP側からもらう感じになります。要するに、広告主が広告費用として例えば1,000円持っていたとすると、その1,000円を使ってDSPに効率のいい配信をしてくださいと依頼します。そのためには、DMPからちゃんとデータを持ってきて、そのデータを使って配信しなければいけないので、100円で入札しますとっている中の例えば20%ぐらい、20円分ぐらいはDMPに払いますという契約をDMPとDSPがして、100円で入札しますといて、落札したら100円発生するので、DSPは、広告主からもらった100円のうち20円をDMPに返して、そのうちの30円をDSP自身が受け取って、そのうちの50円をSSPに支払うというイメージです。

先ほどのSSP側でどういう広告に興味を持って、どういう動きをしてとか、そういう情報は、おっしゃるようにDMPにどんどん蓄積されます。それはDSP側を経由してDMPに入ることもありますし、SSPとDMPがつながっているというパターンもありますし、DMPのデータを厚くするために、SSPではなくてメディア自身、日経オンライン自身がDMPにデータを提供することもありますし、広告主側が自分たちのお客はこういう人なのだというのをDMP側に提供するといったこともありますので、DMPにはどんどんそういう情報がたまっていくことになります。

2点目のiOSのほうプライバシーの観点から安全なのかというところでは、ちょうど18ページにも書いてあるように、4月からIDFA、iOSのオンライン識別子の利用に同意が必要になったので、現時点ではiOSのほうプライバシーに配慮しているといえると思います。

アンドロイド側はどうなのかというと、アンドロイドは今も同意を取って識別することができる状態ですが、多分、今のプライバシーに配慮していないとブランディング的によくないみたいな風潮になってきているので、そこは今後、アンドロイドも対応してくるのではないかと考えてはおります。

○大石オブザーバー ありがとうございます。よく分かりました。

○丸山座長 ありがとうございます。

続けて、新川座長代理からの質問を事務局にて預かっておりますので、その点、よろしく願いいたします。

○大岡企画官 事務局の大岡です。よろしく申し上げます。

3点ございまして、1つ目は、オンライン識別子など端末情報の利用をユーザーがコントロールできる方法がありますでしょうか。

2つ目が、オンライン識別子の利用を法的に規制するとし、有効に監視することができるのでしょうか。

3つ目が、オンライン識別子の利用ルールを作る場合に、多数の事業者が自主的に参加するメリットはあるのでしょうか。

最後ですが、それに関連しまして、その利用ルールは、技術面だけではなく、倫理面ではどのような基準あるいは制限を設けることが望ましいでしょうか、また、可能でありますでしょうか。

○株式会社 DataSign 太田代表取締役社長 ありがとうございます。

1点目のオンライン識別子などの端末情報をユーザーがコントロールできるかというところでいいますと、物によってちょっと異なるのですが、サードパーティークッキーとかウェブのクッキーは、ブラウザの設定で消去することができるので、それで消去することで、自分のIDをクリアすることができます。同じような機能は、iOS、アンドロイドともにあって、OSの設定から広告識別子をリセットするとか、取得されないようにするというコントロールができます。あと、説明したフィンガープリントに関しては、そういったものがないので、コントロールはほぼできない状況でございます。

それらの利用を法的に規制するとして、有効に監視することができるのかというところですが、有効に監視というのは、どうなったら有効なのかというのはあると思うのですが、僕らが日経との調査とか朝日新聞との調査をしたように、オンライン識別子でどういうのを取得しているかというのを調査して、アプリとかを解析したり、ウェブサイトを解析するとある程度分かるので、そういう法律ができて、国が監視するというよりは、メディアとかそういったところがちゃんとやっているかというのを調査したりして、書いてあることとやっていることが違うではないかみたいなことはできるかなと思っております。

次に、オンライン識別子の利用ルールを作る場合に、事業主が自主的に参加するメリットは、多分、今はJIAAとかでもルールがありまして、行動ターゲティング、オンラインに関するガイドラインがあります。JIAAには大体の広告の配信事業者が入っておりますので、入っておくと、要するに今、規制がない中でどこまでやればいいのかということで、広告事業者も困っているのです。

今、ルールがない中で、では、どうすればいいのかとか、フィンガープリントを使っていいの、駄目なのとか、広告事業者も悪いことをしようと思ってやっているわけではないので、では、どこまでならやっていいのかという基準を知りたいというときに、JIAAの基準を見れば分かるというのはあるのですが、JIAAではフィンガープリントについては書いていないので、そこは分からなかったり、Unified IDについてもまだ出していないので分からなかったりするのですが、

事業者もどこまでやってよくて、どこまでが駄目なのかというのが今、全然分からない状態になっているので、そういうルールが法的にもちゃんとできたり、自主規制でもできたりするのは、みんなその基準でやろうということになるので、メリットはすごくあるかなと思います。

どのような基準あるいは制限を設けることが望ましいかというところ、JIAAとかそういう自主規制団体でやるのであれば、JIAAも今はちゃんとそういうガイドラインを出してやっているのですが、一番いいのは、どのように利用しているかというところに制限をかけるのが一番必要かなと思っていて、多分、JIAAで前提としているのは、あくまで広告です。要するに、その人にどういう広告を見せるかというところだけにデータを使っていて、そのほかには使っていないというところは、多分、ちゃんと明確にしないといけないと思っていて、そこが破られて炎上したのがリクナビの内定辞退率問題です。あれは広告の仕組みを利用して、内定辞退率に変換して販売していたので、そういうことは絶対にやるべきではないというところの制限を設けるのが一番必要かなと思っていて、

あと、広告に関しても、例えばフェイスブックやツイッターとかは、政治系の広告は出せないようにしているとか、そういうのにデータを使ってはいけないとか、年収の情報とかそういうので、例えばローンの広告とかはそういう情報を使ってはいけないというルールがあったりするのですが、そういう利用目的の部分でちゃんと制限を設けることと、そこは本当にそうになっているかが外側からは分からないので、ちゃんと監査をするという仕組みを作るのがいいのかなと思っております。

○丸山座長 ありがとうございます。

それでは、原田オブザーバー、お願いできますでしょうか。

○原田オブザーバー 京都大学の原田と申します。本日は、大変クリアな御説明をありがとうございます。

私から2点ほど伺いたいと思います。

1点目は、先ほどグーグルに対抗する業界団体としてPRAMができたというお話がありまして、あるいは日本でも日本インタラクティブ広告協会があるという御紹介があったところですが、国内での自主規制のような取組にどれぐらいの意味があると考えればよいかということです。

つまり、一方ではグローバルな市場で越境的な取引などが多いのですが、他方で広告になりますと、日本語の壁がありますので、ある程度国内でコントロールすることができるのかなという気もいたします。その辺りはどのように考えればよいかというのが1点目の質問です。

2点目は、先ほどの御回答にも少しあったのですが、技術的に見て、規制の実効性が確保されていることをどう検証すればよいかということです。本日のお話にありましたように、同意ベースでやっていくのはかなり無理があるというのはおっしゃるとおりだと思うのですが、他方でオプトアウトしますというふうにしても、本当にオプトアウトできているのかということをおっしゃるのを簡単に検証することができるのかどうか。もちろん、ウェブサイトを解析すればできるのかもしれないのですが、それは普通の人にはなかなかできないと思いますので、技術的に我々が選択した結果が明確に分かるような方法があるのかどうか。

あるいはウェブサイト解析とした場合には、しっかいたいというか、全てのウェブサイトを見てみないと分からないということなのか。つまり、規制の実効性を確保するためにどれぐらいのコストを見込んでいけばよいのかということについて伺えればと思います。

○株式会社 DataSign 太田代表取締役社長 ありがとうございます。

1点目の海外には PRAM があって、日本では JIAA があるというところですが、団体としての性格がちょっと異なるというところで、PRAM は、表向きにはあまりいっていないのですが、グーグルのプライバシーサンドボックスに対抗するために作られたもので、JIAA は、グーグルもフェイスブックも会員には入っています。なので、これは広告業界全体の日本の業界団体です。

先ほどの広告も、今は日本の広告の市場の半分以上がフェイスブック、グーグルとかの海外勢なのです。課題はそこにありまして、JIAA の自主規制団体に入っている、JIAA がそういう何かを出したとしても、結局、フェイスブックやグーグルとかは自分のルールでやっていってしまうので、そのコントロールがなかなか難しいところはあるという状況です。そこに対抗していくためにどうというのは、日本ではまだ団体としてはできていなくて、むしろ PRAM とかが作っていくのにそれぞれの広告事業者が乗っかるのか、乗っからないのかというところかなと思っています。

2点目の規制の実効性というところで、おっしゃるとおり、オプトアウトをして、ちゃんとそれがオプトアウトされているかどうかというのを調べるのはなかなか難しいです。そういうのを調べている論文とかもあるのですが、ちゃんとオプトアウトできていないものが多いというところも結構あったりするので、そこを調べるのはなかなか難しいです。

ポイントとしては2つあると思っていて、一つは、情報を収集する窓口になっている日経オンラインとかそういう立ち位置のメディアとか、そういう情報を収集する窓口になっているところで、そういう情報を収集して、何に使っている、嫌な人はオプトアウトできるという案内がちゃんとされているかというのが一つ。これは先ほどのようにそんなに難しくなくできる。もう一つのオプトアウトとしたときに、ちゃんとオプトアウトできているのかというのを調べるところは、結構難しいです。

なので、今、一応、技術的には、オプトアウトするときに、オプトアウトしてくださいというのを事業者側に送って、事業者側でオプトアウト情報を受け取って、オプトアウトする、しないというパターンと、オプトアウトとしたらデータ自体が送られない、要するにオプトアウトしていない状態だとデータが送信されるけれども、オプトアウトするとデータ自体が送信されないの、事業者側はオプトアウトしているかどうか分からない、要するにデータ自体がない状態になるので、そういう状況にしておけば、ユーザー側も分かりやすいというか、こういう情報が送られていないということがブラウザ上でも分かるので、そこは比較的簡単に実効性を確認することができるかなと思います。

○原田オブザーバー はい。ありがとうございました。

○丸山座長 ありがとうございます。

そのほかに御質問がある方はいらっしゃいますでしょうか。

私から。1点だけ追加で教えていただきたいのですけれども、フィンガープリントに関してなのですが、米国では自主規制で対応されていると言及されたように思うのですけれども、これはどのような団体が、どういう目的で、何を自主的に規制されているのか、教えていただけますでしょうか。

○株式会社 DataSign 太田代表取締役社長 ありがとうございます。

正確なところは今、分からないのですけれども、団体としては、IAB という団体があります。そこが属している DAA (Digital Advertising Association) というところが広告のプライバシー関連についてはいろいろと基準を出したりしているのですが、具体的にどこ部分でどのように規制しているのかというのは、今すぐには情報が分からないのですが、今はオラクルに買収されているのですが、AddThis という結構大きな広告事業者があるのですけれども、何年前に、その仕組みとして、フィンガープリントを使って情報を収集するというのを一斉に行ったのです。そうしたところ、フィンガープリントを使うなんて、ユーザーのコントロールビリティがないし、けしからぬというのでアメリカで大炎上しまして、そこからフィンガープリントは使っては駄目だという共通認識ができて、今ではそれはブラックなやり方だということで基準にもなっているという理解でございます。

○丸山座長 ありがとうございます。

そのほかに御発言希望の委員の方はいらっしゃいますでしょうか。

清水オブザーバーから質問です。よろしくお願ひします。

○清水オブザーバー 大阪大学の清水と申します。今日は大変貴重なお話をどうもありがとうございました。

この方面に非常に疎いので、的外れかもしれないのですけれども、私が理解したことによりますと、サードパーティークッキー自体、実際に物があつた程度規制されるようになったとしても、いろいろな別の手段によって、結果的には同様のことを実現するような技術的な方策が練られていて、それをできるだけ透明化する方向への試みもあるということだと思つてはいますけれども、そうしますと、これは結局、広告ベースのビジネスモデルが変わることは恐らくないという前提でよいのかどうかということと、これまでの話は、要するに業界側からのある種の自浄作用的な動きのように聞こえていたのですけれども、ユーザーの立場からおよそ何か情報が送られなくするとか、送りにくくするようなシステムを作ろうとしている人がいるとか、そういう動きがあるということはないのでしょうかという非常に素人の質問ですけれども、教えていただければと思います。

○株式会社 DataSign 太田代表取締役社長 ありがとうございます。

ユーザー側からのそういう動きは、主には広告ブロックという形で現れているのかなと思つてはいます。

まず、広告がうざいとかそういった意見を持つ人が多くて、要するに自分が見ていた商品が広告に出てきて何か気持ち悪いとか、そのように思う人が、広告ブロックツールをブラウザに入れたり、アプリでも提供されているので、そういったものを導入する人が非常に多い。

どれぐらい多いのかというと、最近は分からないのですが、直近の5年ぐらいは、ずっと iOS アプリの有料ランキング1位だったのは広告ブロッカーなのです。500円で売っているのですが、現在見てみたところ、3位になっていますが、これが有料1位をずっと獲得しております、そういった意味で広告ブロッカーはデータの収集も一部ブロックしてくれるので、広告がうざいという流れからデータが使われるところもブロックしていくという動きは、ユーザー側がこういうツールを入れることによって行われてきている。

なので、そういった流れもあって、プラットフォームのグーグルやアップルとかもこういったデータを収集するところに対して、企業側からちゃんと自主的に同意必須にするとか、サードパーティークッキーを使えなくするといった動きになっているのかなと思います。

ただ、それがメインの理由かということそうではなくて、多分、メインの理由は、一部というか、アメリカだと市民団体とかがどういうデータを使って何をしているみたいなのを結構レポートに出していたりしますので、その中で一番大きな問題となったのがケンブリッジ・アナリティカ事件だと思うのですが、そういった事件をきっかけにフェイスブックのデータが選挙行動に影響を及ぼしているとか、そういった部分のところから批判が集中して、そういった情報に制限をかけるような動きになっているというのがメインの動きかなと思っております。

日本でも同様に、リクナビの事件があって、それで規制が入ってきたというのもありますし、そういったパーソナルデータを悪用した事件がきっかけになっていて、そこをきっかけにユーザーも意識が変化して、広告のブロックとか自分のデータを出さないようにというのが今、流れとして出てきているのかなと思っております。

○清水オブザーバー どうもありがとうございました。

○株式会社 DataSign 太田代表取締役社長 ありがとうございます。

○清水オブザーバー そうしますと、広告ベースのインターネットのビジネスモデル自体に変化はないということですか。

○株式会社 DataSign 太田代表取締役社長 そうですね。そこは基本的に、今の段階ではオンライン識別子を何にするかということだけが変わって、基本的なビジネスモデルは今のところ変わらない想定です。

ただ、グーグルとかフェイスブック以外の、要するにプラットフォーム以外の広告事業主は、オンライン識別子がどんどん制限されていっているの、マネタイズがどんどん苦しくなっていて、ちょっとどう扱はされるかなと思っています。逆に、フェイスブック、グーグルはよりもうかるという状況かなと思っております。

○清水オブザーバー どうもありがとうございます。

○丸山座長 片山委員から御質問がありますので、よろしくお願ひします。

○片山委員 今日はどうもありがとうございました。

今まで本当に分からなかった世界なのですが、お話を聞いて、イメージができるようになりました。ありがとうございました。

2つほどお聞きしたいのですが、今日、いろいろな対応の取られ方の中で、アメリカで市民団体があつたり、いろいろな運動が起こっているという御紹介がありました、他の諸外国の中で、この問題に対して国家的な市民団体等の動きがあれば、御紹介いただきたいと思います。

それから、太田様がこの問題に取り組みられたのは、もともとそういう個人情報の収集のされ方に嫌な思いをしてということでしたが、ずっといろいろな調査をして全容を把握していかれて、最終的に今後、本当に望ましい情報管理・活用の在り方はどうあるべきなのか、今、どういうイメージをお持ちになっているかというのも、漠然とした質問で恐縮ですが、お教えいただければと思います。よろしく願いいたします。

○株式会社 DataSign 太田代表取締役社長 ありがとうございます。

1点目なのですが、アメリカの市民団体は、Electronic Frontier Foundation (EFF) とかが結構有名なところでありますが、ヨーロッパは、市民団体という話よりは、各国の個人情報保護当局がすごくいろいろと活動しているというイメージを持っております。先ほどお話に出たブレイブとかも、ベルギーの個人情報保護当局と一緒にグーグルがどういうデータを集めているみたいなもので告発していたり、フランスの個人情報保護当局もいろいろと調査していて、あとはドイツもです。国単位のそれぞれの個人情報保護当局、日本でいうと個人情報保護委員会みたいなところが調査して、その調査にのっとって制裁金を科すというのがヨーロッパの主な動きかなと思っております。

次に、データ活用の在り方についてですけれども、僕らが DataSign という企業でやっていることにもつながるのですが、今はプラットフォーマーやいろいろな広告事業者とかの自分ではない人がいろいろなデータを持って、自分よりも自分のことを分かっているのではないかと思うほどデータを持っていたりするのですけれども、そうではなくて、要するに自分のことは自分が一番よく知れるように、自分のデータはちゃんと自分で管理できるようにしておこうと。そこで事業者が必要な場合は、自分がちゃんと認識できる範囲で必要な情報だけ提供していく。

提供というか、アクセス権を与えるというイメージですけれども、それに全部同意していくというイメージではなくて、要するに自分の情報はこういうのがあって、こういう情報はどこの企業がどれぐらい参照していますというのが、例えば自分のパーソナルデータダッシュボードみたいなものがあって、そこで調べれば、ここが見に来ているのだみたいなものを見て、見に来た結果、どういうサービスが来ているのだろうと見て、それがちゃんと見合っていれば、これを使ってもらったほうが自分も便利になるし、そのほうが良いという判断ができるけれども、よく知らないところがデータを見に来ている、特に僕に対してもいいことがないと思ったら、そこはアクセス権を遮断するとか、そういったことができるようになるのが一番望ましいかなと思っております。

今、それに一番近いことをしているのがフェイスブックかなと思っております、データ自体は自分のところではなく、フェイスブックにあるところが僕の考え方とは違うのですけれども、フェイスブックがやっているような、フェイスブックがどこにデータを提供しているか、むしろフェイスブックが僕の情報をどこから受け取っているかみたいな情報は、プライバシーダッシュボードみたいなもので見ることができるのです。

フェイスブックが持っている情報ではなくて、自分の情報全般に関して、ちゃんと自分でできる仕組みがあるとベストかなと思っていて、僕ら DataSign はそういうのを作ろうというので立ち上げた企業でございます。

○片山委員 ありがとうございます。

○丸山座長 ありがとうございます。

他に御質問は大丈夫でしょうか。

それでは、太田様へのヒアリングは、この辺りにさせていただきます。

太田様におかれましては、大変お忙しい中、御出席いただきまして、誠にありがとうございました。

○株式会社 DataSign 太田代表取締役社長 ありがとうございます。

では、失礼いたします。

(株式会社 DataSign 退室)

○丸山座長 それでは、以上で太田様からのヒアリングについては、終了とさせていただきますと思います。

あまり認識が得られていなかったインターネット広告についての詳細な仕組みについては、認識が得られたのではないかと思います。

また、サードパーティクッキーなどの問題が解決されつつある中で、それだけでは問題が解決しないであろうという認識が得られたのではないかと思います。

また、諸外国に比して、日本に関しましては、法制の面でも、自主規制の面でも、もしかすると市民の敏感さの点でも差異があるのではないかという状況もうかがえたところでございます。

質疑のところ、日本ができることと、グローバルな観点から考えなければいけないことも指摘を受けたところでございますけれども、消費者という観点から見た場合に、気がつかないうちに同意が取られているというレベルから、一括オプトアウトがなかなかできないということ、あるいはさらに新たな形で情報が取られる手段も出てきているというところで、この点につきましては、インターネット広告について、今回得られた知識を踏まえて、今後、ターゲティング広告等、自主規制等について、検討を少し進めてみたいと思います。

本議題については、以上にしたいと思いますが、よろしいでしょうか。

では、本日の議論は以上にしたいと思います。

事務局から事務連絡をお願いします。

《 3. 閉会 》

○大岡企画官 事務局です。

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。

○丸山座長 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、お集まりいただきまして、ありがとうございました。

以 上