利用者情報に関するワーキンググループ（第３回）

令和６年４月16日

【山本主査】　本日も、皆様、お忙しい中お集まりいただきまして、ありがとうございます。定刻となりましたので、利用者情報に関するワーキンググループ第３回会合を開催いたします。

本日の会議につきましては、ウェブ会議システムにより開催しております。議事に入る前に、事務局よりウェブ会議による開催上の注意事項について御案内がございます。よろしくお願いいたします。

【川野利用環境課課長補佐】　事務局でございます。総務省利用環境課の川野でございます。

まず、事務局より、本日のウェブ会議による開催上の注意事項について御案内をさせていただきたいと存じます。

本日の会合の傍聴者につきましては、ウェブ会議システムによる音声及び資料投影のみでの傍聴とさせていただいております。事務局において傍聴者は発言ができない設定とさせていただいておりますので、音声設定を変更しないようお願いいたします。

また、本日の会合につきましては、記録のため録画をさせていただきます。

次に、構成員におかれましては、ハウリングや雑音混入防止のため、発言時以外はマイクをミュートにしていただいて、映像もオフにしていただきますようお願いいたします。

御発言を希望される際には、事前にチャット欄に発言したい旨を書き込んでいただくようお願いいたします。それを見て、主査から発言者を御指名いただくような方式で進めさせていただきたいと存じます。

発言する際には、マイクをオンにして、映像もオンにして御発言ください。発言が終わりましたら、いずれもオフにお戻しください。

接続に不具合がある場合は、速やかに再接続を試していただくようお願いいたします。

その際、チャット機能で随時事務局や主査宛てに連絡をいただければ、対応させていただきます。

本日の資料でございますけれども、本体資料として資料３－１から３－４、参考資料として３－１から３－３を用意しております。

注意事項は以上になります。

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】　それでは、まず、本日は、第１部として、スマートフォン上のプライバシー対策のうち、ダークパターン対策に関しまして、三菱総合研究所の安江様から、続きまして、Apple及びGoogleにおけるスマートフォン上のプライバシー確保に係る取組に関しまして、日本総合研究所の小竹様より御発表をいただきます。

次に、第２部といたしまして、利用者情報に係るモニタリング等のうち、過去のモニタリング結果に関し、事務局発表の後、非ログイン利用者の保護の在り方に関し、日本総合研究所の小竹様より御発表をいただきます。

なお、前回の会合と同様、本日の会合での議論に必要があると考えられるため、一般社団法人日本インタラクティブ広告協会（JIAA）様にオブザーバーとして御出席をいただきたいと思います。この点、御異議はございませんでしょうか。

（「異議なし」の声あり）

【山本主査】　ありがとうございます。

それでは、御異議ございませんでしたので、それぞれ御出席の上、議事に入りたいと思います。

なお、本日の質疑・意見交換につきましては、第１部と第２部における御発表の後で、それぞれ質疑の時間を設けて、構成員の皆様から御意見をいただきたいと思います。

それでは、三菱総合研究所の安江様から御発表をお願いしたいと思います。

御準備はいかがでしょうか。

【安江氏】　三菱総合研究所、安江です。本日は、よろしくお願いいたします。

【山本主査】　よろしくお願いいたします。

【安江氏】　それでは、早速ですけれども、資料の説明を始めたいと思います。

私のほうから、ダークパターン及びプロファイリングについてということで、EUの動向を中心に説明したいと思います。

まず目次ですけれども、最初にダークパターンについて御説明して、次にプロファイリングについて説明し、最後に簡単なまとめをしたいと思っております。

ダークパターンについては、デジタルサービス法での規定・言及を見た上で、各国機関のダークパターンに関する報告書にどういうものがあるか、それから、それらでどういっ

た定義や説明がされているかを見た上で、ダークパターンが具体的にどういうふうに分類されているかをそれぞれ整理しています。その後、ダークパターンの状況や実態について調査例が幾つかありますので、それらについて御紹介した後、ダークパターンに関する規制動向という順序で説明したいと思います。

最初に、デジタルサービス法での規定ですけれども、御存知のとおり、25条で規定されています。法案審議の中では、欧州議会による修正版（2022年１月）ぐらいから明示的にダークパターンというものが導入されて、議論が始まったというふうに認識しており、官報掲載版ではこの25条と序文の67で具体的に言及されています。

25条では、赤字で強調していますけれども、サービスの受領者、サービスの利用者を欺いたり操作したりするような方法で、またはそのサービスの利用者が自由かつ情報に基づいた決定を行う能力を実質的にゆがめたり損なったりする方法でオンライン・インターフェースを設定、構成、運営してはいけないというふうにしていて、具体的な規制対象や要件、判断基準は、恐らくガイドラインをこれからつくって示されると思いますけれども、この25条では、特にこの３つを注意しなさいということで、この３項の（a)、(b)、(c)、特定の選択肢をより強調する、既に選択を行っているにもかかわらず他の選択肢の選択を繰り返し要求する、サービスの解約を加入より難しくするといったようなことを特に注意すべきと書かれています。

また、２項にありますように、指令の不公正商慣行指令（UCPD）とGDPR、これらでダークパターンあるいは欺瞞的な取引といったものを規制する部分があって、それらが影響しない部分について規制するということが書かれています。

序文67のほうは、今のことをもう少し文章で説明した形になっています。

次に、各機関のダークパターンに関する報告書で、主なものと思われるものを幾つか拾っていますけれども、まず、欧州連合では、欧州委員会がデジタル環境における不公正な商慣行に関する行動科学的研究といった分厚い報告書を出していて、ここでダークパターンの事例や分類を行っています。

それから、欧州委員会とCPC、これは欧州の消費者保護当局のネットワークですけれども、これが共同して、欧州の399のオンラインショッピングサイトに関して調査を行った結果、148のサイトでダークパターンが使われていたという調査結果があります。

それから、欧州データ保護会議で、GDPRに基づいて、SNSにおけるダークパターンを対象としたガイドラインを出しています。

また、米国では、FTCが「ダークパターンを明らかにする」といったようなタイトルになりますが、スタッフレポートという形で、実際の執行事例とかに基づいてダークパターンの全体像や、分類、事例といったものを細かく述べている報告書を出しています。

OECDでも、こういったものを参照しながらレポートをまとめるという形で、各国に注意喚起をする形になっています。

次に、それぞれのダークパターンの定義・説明を拾っています。ダークパターンというのは、御存じのとおり、UX（User Experience）デザイナーのHarry Brignull氏という方が、2010年に最初に提唱したものと言われていますけれども、その定義も様々ありますが、大筋は概ね同じです。このBrignull氏の定義ですが、欺瞞的パターン、別名「ダークパターン」とは、何かを買ったり申し込んだりするなど、利用者の意図しないことをさせる、あるいはウェブサイトでアプリで使われる策略であるとしています。もともとはこの「欺瞞的パターン」という言葉はなく、「ダークパターン」とは、という表現でしたが、現在は「欺瞞的パターン」が主で、別名「ダークパターン」という形になっております。他でも、最近は「欺瞞的パターン」が使われることが多くなっています。

欧州委員会は、これとほぼ同じですけれども、「誘導」や「操作する（manipulation）」という点を強調している部分が１つ特徴かと思います。

また、OECDは、それらをもう少し包括的にカバレッジを広げて、より丁寧に説明していると言えるかと思いますけれども、基本的にはそれぞれ同じような定義をしていると言えると思います。

次に、分類ですが、こちらも様々な分類軸の違いは多少ございますが、挙げているものはほぼ同じです。

FTCと欧州委員会は、見た目は少なく見えますけれども、これらにさらに細かい分類があります。省略した形でお示ししていますけれども、それぞれ同じようなものを挙げているという形になっています。

次のページからが、それぞれの具体的な分類です。

Brignull氏の分類について、１年半前ぐらいに見たときとは、中身は同じものが多いのですけれども、ラベリングなどは結構変わっていて、随時アップデートされており、今現在ではこういった形になっています。

FTCは非常に多くの種類を挙げていて、彼らがこれだけの数を執行してきたということを示している部分でもあるんですけれども、この資料でいうと７ページにわたっています。

詳細は時間の関係もあって割愛いたしますが、こういった分類がされています。

OECDは少しコンパクトにまとめていますけれども、中身としては、やはり同じです。

欧州委員会は、二通りの分類軸を示していて、１つは、伝統的と彼らが言っていますけれども、オーソドックスな分類をしていて、体系的に分類されているという部分では分かりやすいんですけれども、これも挙げているものは他とほぼ同じです。

具体的には、情報の非対称性と自由な選択の抑圧というものから、それぞれ細かくブレークダウンしていく形になっています。

情報の非対称性というのは、情報の出し手と受け手の非対称性だけではなくて、出している情報について、事業者に都合のいいものを強調して、都合の悪いものはあまり見せないこと含め、そういったものも含めて非対称性と書かれているかと思います。

次がもう１つの分類です。行動科学的分類と欧州委員会が言っていますが、これはユーザーデータに基づいたデータドリブンなパーソナライゼーションを用いた操作的なダークパターンが要注意だと説明されており、このような表を示しています。

表の青い部分は、私のほうで少し補足的に加筆したものですが、それ以外のところは欧州委員会が出した表で、縦軸が「意思決定要素」になっています。一つは、お金はこれだけだけれども、もうちょっと使ってもいいかと思わせてしまうという予算制約への影響で、もう一つが、そもそもお金を使うか、買うか、買わないかを決めておらず、どっちにしようかなみたいな、あるいは絶対買わないぞと思っている人に買わせるといったような選好性の形成といわれているものでこの２つの要素からなっています。

横軸は「分かりにくさ」です。①商品がどういうものかというものの分かりにくさ、それから、②どういうコストがかかるかという分かりにくさ、③選択に手間がかかるあるいは、こうしたいんだけれども、どうやっていいか分からない、そういった３つの要素で、縦軸と組み合わせて合計６つの分類をつくっています。欧州委員会が特に強調しているのが、赤字で書いてある、下３つです。いずれも「操作的な」ということで、データを用いて、そのユーザーの弱いところを責める、そういったようなパターンが要注意だということを言っています。

もう１つ、EDPB（欧州データ保護会議）が出しているソーシャルメディアにおける欺瞞的デザインパターンに関するガイドライン、こちらでもダークパターンの分類を出していますが、これが分類の全体像です。６つのカテゴリーで合計16のパターンを示しています。

それぞれの説明はここにあるとおりですけれども、これも細かいので読んでいただけれ

ばと思います。

また、それぞれに関してGDPRでどういった規定に違反する可能性があるかというものも示していて、それを回避するためにどういうベストプラクティスがあるかを併せて示しています。

これはEDPBが作成したものなので、基本的にはデータ保護という観点からであり、欺瞞的な商取引については少し視点としては弱いかもしれませんけれども、ユーザーのデータ保護という面では、こういったものを挙げているということになります。

続きまして、ダークパターンの実態調査を２つ御紹介したいと思います。

１つは、先ほど言いましたように、欧州委員会とCPCネットワークが共同でやっているものですが、これは「Sweep」という調査名で、毎年テーマを変えています。これは2022年の調査ですけれども、その翌年はインフルエンサーに関する調査など、毎年テーマを変えており、2024年はダークパターンについてやっています。

欧州の、自社ブランドで物を売っているウェブサイト399と、その中でアプリを提供しているのがうち102あったということで、399のサイトと、その中で提供されているアプリ102を対象に、ダークパターンが使われているかどうかということを調査しています。

この調査では、偽のカウントダウンタイマーと、特定の選択肢に誘導するようなデザインや言葉、ワーディング、それと、情報を隠したり、見えにくくするといったものを典型例として挙げて、それぞれ幾つあるかということをカウントしたものになりますけれども、ウェブサイトの場合は、399のうち148サイトで３つのダークパターンのどれか１つが使われていて、アプリについては、102のうち27です。こちらが３つのダークパターンのうちのどれか１つを使っていたということで、それぞれ４割弱とか、４分の１強とか、そう割合で使われているということになります。

加えて、御存じかと思いますけれども、日本でも、ユーザー調査や、広告審査の状況といったものについても情報が出されていて、そういったものでもやはりダークパターンが増えているといったような結果が示されているという状況かと思います。

次が、プリンストン大学とシカゴ大学がかなり大規模にやったもので、調査時点としては、2018年ということで少し古いんですけれども、非常に大規模にやられたということで、こちらも御紹介したいと思います。

ダークパターンの使用状況に関する大規模な調査と、調査結果に基づく認知バイアスの観点からの分類を実施して発表しています。Alexaランキングといって、今はちょっとサ

ービスをやめてしまっていますけれども、ウェブサイトのアクセス数のグローバルなランキングがありますが、その上位36万1,000サイトから条件に合うものを自動的に絞り込んで、最終的に１万1,000超のショッピングサイトについて調査し、そのうち1,254のサイトでダークパターンが見つかり、ダークパターンの形としては、1,818パターンがあったとされています。サイト数で言うと、１万1,000強のうちの1,257、11.1％のサイトでダークパターンが把握できた、見つかったとされています。ただ、これは最低限のダークパターンで、それ以外のパターン、今回の調査方法では引っ掛からないものもあるので、「少なくとも11.1％」だとも言われていますけれども、こういったものがあったという結果になっています。最終的な判定は、機械的に抽出した後で、専門家がダークパターンに該当するか否か評価しているという形で行っています。

また、ダークパターンを自分で設けるだけではなくて、いわゆるターンキー・ソリューションということで、サービス契約者がそのまま使えるような、そういったダークパターンのサービスも第三者から提供されていて、22の第三者組織、事業者も見つけたという結果になっています。

どういったダークパターンがあるかという分類と、それがどのくらいあったかという事例数がこちらの表になります。分類自体はそれぞれ、これまでに御紹介したものとほぼ同じですが、事例でいうと、残り僅かですと示す在庫僅少通知やもう少しで終わってしまうことを示すカウントダウンタイマー、何人のユーザーがこのサイトを見ていることを示す活動通知、羞恥心の植付け、A、B、Cという３つの選択肢があるとして、Cを選んでほしくない場合には、Cも選べますけれども、こういう場合しかないでしょうとか、ほとんどの人がAとかBを買いますよとか、そういったような形です。そういったものが多いという結果になっています。

ここに挙げられたダークパターン、それぞれが全部直ちにダークパターンかというと、そうではなくて、例えば、カウントダウンタイマーも、正しいカウントダウンタイマーもありますし、活動通知も正しいものもあります。それぞれが常にダークパターンなのか、ケース・バイ・ケースなのかということについても分類されていて、それがこの表になります。

黒で「常に」というのが、これをやったらダークパターンだというもので、「時々」とあるものはケース・バイ・ケースということになっています。

そういう点も踏まえて、専門家が評価しているわけでもありますけれども、こうした分

類に加えて、認知バイアスでどういったものが関係しているかという分析もされています。それぞれの説明は、こちらのページを御覧いただければと思います。

また、サイトのアクセス数とダークパターンの出現率の関係も分析されていて、このグラフの横軸はアクセス数のランキングなので左にいくほど人気が高い、アクセス数ランクが小さいということはランクが高いということなので人気がある、ということになります。逆に右にいくほど人気が下がっていくんですけれども、左にいくほどダークパターンの出現率が高い傾向があったということです。ここに載せていませんけれども、統計的な回帰分析も行って、そういう傾向があるというふうに書かれてて、人気サイトではダークパターンも結構使われているという結果になっています。

次が規制動向ですけれども、全般的な動向としては、ダークパターンを明示的に規制しているものはまだあまりないということと、EUでは様々な法律を使って規制しているということがあります。

プロファイリングについては、GDPRの定義のとおりとなります。

それから、どういったものがあるかという具体例は意外とないんですけれども、ソーシャルメディアにおけるターゲティングのガイドラインではもう少し詳しい事例も載せていて、ここではその３つの分類を示しております。

規制ですけれども、こちらもGDPRでどういったものが関係するかというものを示しています。これ以外にも当然、５条、６条、７条、12条とかあるんですけれども、21条、22条以外にもこういったものが関係し得るということで、これらはガイドラインに記載があるので御承知かとも思いますけれども、表にして載せています。

DSAでは、こちらに示しているのはまず関係する序文ですけれども、具体的な条文としては、26条の特別カテゴリーデータを使ったプロファイリングについて広告を出してはいけない、28条の未成年者に対してプロファイリングに基づく広告を出してはいけない、38条のレコメンダーシステムに関してはプロファイリングに基づかないオプションを用意しろ、これは超大規模プラットフォームについてということになりますけれども、そういったものが挙げられています。

DMAに関しては、ゲートキーパーの監視の中でプロファイリングという観点も重要だということが序文で述べられていて、20条、15条、46条で具体的にそういった観点からも監視するんだということが定められています。

それから、「消費者保護規則のより良い執行と現代化に関する指令」（現代化指令）の中

では、プロファイリングに基づいたパーソナライズド・プライシングについて規定が定められているという形になっています。

まとめになりますけれども、ダークパターンについては、先ほど言いましたとおり、EUで様々な多面的な規制が始まっているということかと思います。

プロファイリングについても、様々な法律で規制されているということと、資料には詳細は書いていませんけれども、米国カリフォルニア州で、プロファイリングや、自動意思決定技術に関する規制案が昨年11月に出ているという形になっています。

それから、ダークパターンとプロファイリングは組み合わされて使われるんだと、EUが「操作的な」とも言っていますけれども、そういった論文も様々ありますので、別々のものではなくて、両方見ていく必要があるよということが言われているという部分でもあります。

最後に、様々な法律が出てきたので、簡単な整理という形ですけれども、様々な側面から規制が考えられていますよということを図にしました。

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、次に、日本総合研究所の小竹様からプレゼンをお願いいたします。よろしくお願いいたします。

【小竹氏】　承知いたしました。

それでは、アプリストアの規約、Google、Appleのアプリストアの規約ですとか、取組についてお話しさせていただきます。

本調査は2022年１月にも実施しておりまして、そこからのアップデートという形になりますので、基本的に、お話しする内容は、２年前からの更新部分のみに限定してお話しさせていただければと思っております。

今回の調査の項目としては、大きく３つございます。

１つ目が、Google、Appleが開発者向けに提供しているデベロッパーのプライバシープログラムポリシーですとか契約のところで、どういうような規約等が定められているか。

２つ目は、こういう規約を受けて、具体的にどういう取組を発表していたり、もしくは、Android、iOSのOSの機能として、どういうものをアップデートして備えたりしているかというところ。

３つ目が、実際の審査の方法、アプリストアにおける通知アプリケーションにおける、

どういうような仕組みを用意しているのかというところになっております。

今回は、①と②について、時間をかけて説明させていただければと思っております。

では、まず①の規約、ガイドラインの記載内容ですけれども、こちらは大きく、ユーザーの通知方法、通知内容でどういうことを定めているのか、データの取得方法、取扱いに関してどういうことを定めているのか、それを破った場合の罰則でどういうことを定めているのか、特定の条件に該当するアプリに関しては、別途規約等をつくっておりますので、こちらに関しては、このアプリに対して通知方法、通知内容等でどういうものがあるのかを１枚でまとめております。

まずはプライバシーポリシーに関する規約ですけれども、前回からの更新部分は、赤色の部分ですが、GoogleもAppleと同じように、全てのアプリに対してプライバシーポリシーを設置を義務づけるというところを規約に明記しております。これによってGoogle、Appleともに全てのアプリにおいてプライバシーポリシーの設置が義務化され、足並みがそろったのかというところになっております。

２点目が、アプリが収集・共有する情報のアプリ紹介ページでの個別通知に関する規約ですけれども、これは具体的に何を言っているかというと、少し上の実例であるんですけれども、Googleですと、データセーフティという形で、このアプリケーションがどういうような情報を個別にやっているのか、詳細を表示すると、その利用の目的ですとか、どういう情報なのかというところが、アイコンを通じて少し詳細に見られるような形でやっています。

同じようにAppleに関しても、ユーザーのトラッキングに使用されるデータと関連づけられるデータで、アイコンでどういうものが取れるか見せていますが、こちらに関する規約になっております。

こちらはもともとAppleが先にやり始めて、2022年７月にGoogleが同じように規約で公開を義務化しておりまして、そこの部分が前回からの更新部分で、足並みがそろったのかなという形になっております。

３点目が、データの収集・保存・使用・共有に関する規約です。こちらはデータの収集・保存の部分と、取得したデータをどう使用・共有するかまとめたものですが、前回からの更新部分としては、Google、Appleともにアカウント削除要件を追加しております。

こちらは、アプリ内でアカウントを作成する機能を追加した場合には、必ずそのアカウントを削除できる機能もつけなさいという要件になっております。

それ以外については、もともとユーザーからの同意取得の義務、必要最低限の取得義務、あとは、データの使用・共有の場合には事前に許可を取りなさいというところは、前々から定められていて、Google、Appleともに特に差はないという形になっております。

４点目が、特定の条件に該当するアプリに対する規約です。特定の条件に該当するアプリとしては、大きく２つに分かれまして、１つ目が子供を対象とする場合、２つ目が特定のデータを扱う場合で、特定のデータとしては、健康、医療、フィットネスのヘルスケアデータと、位置情報のデータが、Google、Appleともに個別に定められてます。

子供の部分は前々から定められていて、少し補足説明しますと、Google、Appleで大きく違うところとしては、広告掲載に関して、Googleの場合は、Googleのポリシーに準拠していると自己認定している広告SDKのみ使ってくださいとなっているのに対して、Appleは、子供向けのアプリでは、サードパーティ製の分析・広告機能は完全に禁止というところで、少し差は出ています。

前回の調査からの更新部分に関して言うと、これまでは健康・フィットネス・医療データの取扱いに関して、Appleのみ個別に規約で定めていましたが、GoogleもAppleに合わせるような形で、既に文面自体は出ているんでけれども、２０２４年５月末から発効、有効化させるべく、条文が加わるとのことです。プライバシー、詐欺、デバイス不正使用に関するポリシーの準拠義務や、アプリ内に必ずプライバシーポリシーの掲載を義務にしなさいですとか、あとは、アプリのコア機能と、なぜ今回、健康関連データを収集するのかという関連性をユーザーに明確に示しなさいですとか、必要な権限等は必ず削除しなさいというようなところが義務化された形になっております。

最後に、違反アプリに対する罰則に関する規約の部分ですけれども、こちらは前回の調査から大きく変化はないという形になっております。Google、Appleとも基本的には枠組みは一緒で、まずは個別のアプリが規約に違反した際にどうするかというところと、それを繰り返した場合に、デベロッパーの単位でどういう罰則をするのかとをそれぞれ定める形になっております。少しAppleのほうが細かく記載はあるのかと思いますが、、基本的にやっていることは大きく変わらないのかなというところです。

次に、こういうことを受けまして、具体的にこの２年間でGoogle、Appleがどういう取組を実施してきたのかをまとめたものが、11ページからになっております。

こちらについては、ユーザーのデータの取扱いに関して、規約の変更、取組、審査を厳しくする、そういうものの変遷と、あとはOSレベルで何か具体的にどういう取組、機能を

追加したのかに分けて整理しております。

ユーザーデータの取扱いに関しては、今、規約のところで説明したように、「データセーフティセクション」の義務化や、アカウントデータの削除オプションの導入、先ほど申しましたように、健康アプリ、医療、ヘルスケアデータを取得するものに関しては、より厳しいポリシーを導入して適用する、あとは、これはまだ決定ではないですが、2024年８月頃に、写真と動画へ広範囲な権限を要求するアプリに対しては審査を厳しくしますということを追加予定と発表しております。

OSレベルでは、アプリ、写真、動画で、全部の写真、動画をアプリに公開するのか、１枚１枚選択したものだけ公開できるようにするのか選べる機能がついていますが、そちらに関して、全ての動画、写真を要求するものに対しては、なぜそこまで必要なのかをしっかりと審査で見ていきますということになるのかなと思っております。

また、「AdID」や、広告配信周りについて、少し動きがあり、2022年２月、ちょうど２年前に、AdIDの２年間はサポートをしますということを発表しましたが、２年たった2024年３月の時点で、何か具体的にサポート継続、廃止等の方針の更新がなされたかというと、なされていなくて、どういう状況かというのが見えない状況です。

同じくして、プライバシーサンドボックスについて、新しい広告配信の仕組み、広告の効果測定、ユーザーを識別するような仕組みが発表されて、その１年後にベータ版が提供されています。

OSレベルでも、Appleが強化している部分について、GoogleもAppleの機能を見習いつつ、いろいろな機能を追加しています。

基本的には、利用者情報のアクセスに対して細かく許可を出せると、例えば、オーディオ、画像、動画、個別に許可を要求できるよう、基本的にはユーザーのコントロールの機能が上がる方向に変わっていると思っております。

次に、Appleの利用者情報に関する取組について、ユーザーデータの取扱いに関して、大きな点については、「プライバシーマニフェスト」が2023年12月から導入されて、それが2024年５月から義務化されるということが一番大きい点になっているのと思っております。

この「プライバシーマニフェスト」は、App Storeにアプリを申請する際に、そのサードパーティSDK及び自分のプログラムアプリ内に含まれているAPIが、今のiOS17、新しい仕組みで一覧化されますので、その情報を取得するAPIに対して、なぜ使用しているのかを

開発者が記載して提出することを義務づけているところ、例えば、このアプリで、こういうデータはトラッキングに使います、こういうデータは関連づけとして取りますという形で自己申告制だったんですけれども、そちらが自己申告制ではなくて、プログラムの内容に基づいてAPIが一覧化されて、それに対して開発者が、理由や、目的等を記載しなければいけなくなるというところで、大きな変化点なのかというふうに思っております。

OSレベルのユーザーのデータの取扱いに関しては、ユーザーのデバイスの各種機能を止めるようなロックダウンモード、あとは、リマインダーの機能みたいな形で、１回このアプリを利用した際に、ポップアップで許可を出しても、これはこのままでいいんですかとリマインドで出してくれるような機能が追加された形になっております。

こちらは、それを時系列に並べたものになっておりますので、お時間のあるときに見ていただければと思いますが、基本的には、Appleが先行的に取り組んで、１年から２年遅れでGoogleが同じような取組を実施していくという流れが見てとれるかと思っております。

次に、実際の審査状況について簡単に触れさせていただきます。

実際の審査状況に関しては、Apple、Google等、公開しておりませんので、開発者ブログ等から、どういうところで拒否されたのか、有識者へのヒアリングを踏まえてまとめたものになっております。

基本的には、個人情報、位置情報などを取得する場合には、個別で、なぜこれを使うのかとメールで問合せが来て、それに対して、利用目的等をきちんと回答できないと、アプリをチェックされてしまって公開できないと、確かに利用の目的や正当性は、なかなか機械で判断が難しいところについては、目視、人手で、Google、Appleともにチェックしているというところが伺える内容であったというところになっております。

App Storeやアプリにおける通知の仕組みに関しては、これはこれまでの弊社の実施したSPO等での調査内容をまとめたものになっておりますので、お時間のあるときに見ていただければいいのかなというところで、Google、Apple、ほぼ仕組みは同じなんですけれども、若干Googleのほうが、例えばアプリのインストールに取得する情報が全て表示される、iOSのほうがトラッキングに対する同意取得画面があるというような差がある形になっています。

最後に、調査結果の総括ですけれども、こちらが2020年１月から、Google、Appleどちらかで対応状況の更新があったものを一覧化したものになっております。

その中で、大きな項目としては２つありまして、１つ目がアカウント削除要件の追加で、

アプリにアカウント作成機能がある場合には、きちんと削除機能も必須とするというところは新しい取組で参考になるのかなと思っております。

２つ目が「プライバシーマニフェスト」で、ある意味、これはプライバシーポリシーですので、外部送信規律に関するような内容、情報取得と目的について、自己申告制ではなく、しっかりとプログラムの内容に基づいて記載してくださいと、それをできるような仕組みをつくって義務化したというところは、大きなポイントになっております。

以上が、この調査結果の御報告になります。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、ただいまのお二方の御説明につきまして、構成員の皆様から御意見をいただければと思います。大体40分程度、11時15分ぐらいまで質疑の時間とさせていただきたいと思います。いかがでしょうか。

それでは、まず、太田さん、お願いいたします。

【太田構成員】　御説明ありがとうございました。私からは、幾つか質問をさせていただければと思います。

まず、三菱総研さんの御発表について、ダークパターンの種類を様々お示しいただきましたが、私もダークパターンについては様々調査しており、これはダークパターンなんだろうかみたいなものも含まれて、それは別にいいのではないのかみたいなものもたまに含まれているなという印象でして、このダークパターンの分類の中で悪質さを示すような指標はあるのかをお聞きしたいと思いました。先ほど、30ページ目でそれっぽいものが図示された気がしましたが悪質さを示しているのか知りたいと思いました。

それに関連して、27ページ目で行われている調査で、３つのダークパターンについて調査をされているということで、特に悪質な３つを取り出して調査をしているということなのか、そうではないのかというところを知りたいと思いました。

同様に28ページについて、調査結果の中に、ダークパターンは二千数件、欺瞞的なものが183件と書いてあって、要するに、ダークパターンの中でも、欺瞞的なものと、そうではないものという分類が28ページ目の調査で行われていると思っており、どういう差があるのか知りたいと思いました。

次は、ダークパターンに関連するんですけれども、小竹さんに質問で、Appleは、アプリがこういうダークパターンをやっては駄目というルールがあったと思っていて、それがどういったダークパターンなのかを調査されているかというところと、Googleの中ではダ

ークパターンを禁止するような条項があるかを知りたいと思いました。

以上です。

【山本主査】　ありがとうございます。

それでは、まずは安江さんからお答えいただければと思いますが、いかがでしょうか。

【安江氏】　安江です。御質問ありがとうございます。

まず、悪質さを示す指標について、様々なレポートがありますが、これが悪質だというものは特に示されていないのですが、おっしゃられたように、このパターンに当てはまるからすなわちダークパターンであってこれはいけないことだよね、ということも言えないということだと思っていて、質問でも言及いただきましたけれども、30ページにあるような「常に」当たるんだということと、「時々」当たるんだというような区別がされているのは、この文献以外ではあまり見なかったですが、これからは多分そういったものが出てくる。それで、183件が欺瞞的な行為を行っていると思うんですけれども、これもあまり詳しい説明は載っていなかったので、他との違いは不明ですが、恐らく、実際どういうことがされているかということを機械的に見て、かつ、これはだます意図があるということを専門家が評価して、さらに特に悪質だというものが183ということだと思います。その具体的な指標や基準というのは、まだあまり明確ではないと感じています。

ほかの２点目、３点目について、27ページの３つのパターンについては、これが特に悪質だというような説明は特になく、これについて調査しましたというだけなので、これを選んだ理由は、恐らく、典型的なものということで、悪質さという観点ではないのかと思います。

私からの回答は以上になります。

【山本主査】　ありがとうございます。

それでは、後半の質問について、小竹様から御回答をお願いいたします。

【小竹氏】　まず、「ダークパターン」というような言葉でAppleは示していませんが、例えば、トラッキングの許可を求めるAppに関するところで、追加の説明の表示はいいけれども、不要なデータアクセスに誘導したり、それを何度も執拗に求めたりはいけないというような文章の記載はたしかあったかと思っております。ただ、そこがすごい分類をされていて、何か具体的な事例とかまで見せて、こうしなさいというようなところまでの記載ではなかった認識です。

【太田構成員】　ありがとうございます。Google側は、特にそういうものはないという

認識でよろしいでしょうか。

【小竹氏】　そうですね。Google側に関しては、そういう視点でしっかり見ていなかったというところもあるんですけれども、明確にそういう記載が、印象に残るほど強く書かれてはいなかったと思っております。

【太田構成員】　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、森さん、お願いいたします。

【森構成員】　御説明ありがとうございました。お二方ともに、すごい知りたかったことについてお調べいただいて教えていただいたと思います。大変学ぶところの多いプレゼンでした。

安江さんに対して１つお伺いして、小竹さんの御発表に３点ほど意見を申し上げたいと思います。

まず、安江さんの最後のお話で、プロファイリングとダークパターンの関係、この両者を関係づけて、そういう問題意識があるというお話でしたけれども、それをもう少し御説明いただいてもよろしいでしょうか。

というのは、プロファイリングの場合、御説明の冒頭にもありましたけれども、データの取得の仕方が問題で、ソーシャルメディアにおけるターゲティングのところですけれども、提供データと観察データと推定データになっていますので、基本的にはユーザーインターフェースの問題であるダークパターンが、どういうところでプロファイリングと関係してくるのかなと思いましたので、教えていただければと思います。

小竹さんの御発表について、本当になるほどそうなんだと思って伺っていましたが、１つは、やはりAppleとGoogleのストアにおける足並みが結構そろっているということを明らかにしていただいたと思っていまして、その辺が我々の言うところの通信関連プライバシーの具体的な中身になってきているのかなと感じました。外部送信の文脈で我々はそういうことを言い出したわけですけれども、実際の中身をプラクティスによって形成しつつあるのかと思いました。それが１点目です。

２点目は、そのこととも関係するんですけれども、Appleが先行して、２年ぐらいしたらGoogleが追随して、大体同じような内容になっているということは何を意味しているかということですが、Googleとしても、Appleと一緒に行動する必要性はないわけですが、それがそろってしまっているのは何かというと、やはりユーザーの期待というものを、あ

る程度感じ取ってそうなっているのかと思います。ユーザーのアプリについての期待、アプリの情報収集についての期待、外部送信についての期待というものが大体そろってきていて、それで非常に広い範囲で寡占事業者となっている２つのストアにおいて、同じようなルールになっているのかと感じました。

３番目は、iOSの「プライバシーマニフェスト」ですけれども、すみません、中身を知りませんでしたけれども、これも本当にすばらしいことだなと、そういう形で透明化が行われるのが、真にユーザーにとっていいことなんだろうなと思いました。

以上です。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、安江さんへは御質問ということだったと思うので、安江さんから御回答をお願いできますでしょうか。

【安江氏】　質問ありがとうございます。結構難しいところを聞かれてしまったんですけれども、まず、資料の後ろの方で、まとめ、44ページ、プロファイリングとダークパターンの関係の問題点、危険性を指摘する論文が幾つかあると言ったんですけれども、斜め読みよりもうちょっと深いぐらいのレベルではありますが１つ読んだところでは、まだ具体的にこうこうこうだからということよりは、プロファイリングとダークパターンはやっぱり組み合わされて使われることがあるので、そういう点からもそれぞれちゃんと対策を打たなければいけないという主張が多いという印象です。調べた印象としては、まず、ダークパターンは、そもそも形、やり方がどうだということよりは、やっぱり欺瞞的な、あるいはユーザーが意図しない、嫌がっているにもかかわらずやらせるというところが問題だと、それは定義にも書かれていて、先ほど太田さんの質問で答えそびれたんですけれども、形式というよりは、欺瞞的だ、ディセプティブだということが最近強調されていることもそこにあると思うんですけれども、だますときに、プロファイリングで取った情報を使って、それを悪用するということが問題だというのは、あまり強調されていなくてもあると思いますし、DSAで特別カテゴリーデータを使ってはいけない、未成年者に対してやってはいけないという規定があるのも、ダークパターンを使ってはいけないというのも、多分そういうことと関連しているのかなと思います。

ターゲティングのガイドラインでも、そういうことが書かれていますし、ダークパターンとプロファイリング、それぞれの中で問題提起がされて対応策が考えられている中で、多分これからもうちょっとそういうところが組み合わされて対応が必要だということが言

われていくと思いますし、欧州委員会のレポートの中でも、操作的なダークパターンがいけないということを、第２世代のダークパターンみたいな言い方もしているんですけれども、これから問題意識として、もうちょっと具体的になっていくというフェーズなのかなと思っています。

あんまり大した答えではないんですけれども、そういった捉え方をしています。

【森構成員】　ありがとうございました。

そうしますと、もしかしたら、ダークパターンというのは、ユーザーインターフェースだけに限った話ではないのかなと、なくなりつつあるのかなというふうに……。

【安江氏】　そうですね。定義の中でも、「ダークパターンとは」というよりは、「別名ダークパターンと言われるディセプティブパターンというのは」というふうに書き換えられていますので、インターフェースの形だけではなくてというところは、多分これから広がってきているという、専門家もそういうふうに見ているのかなというふうにも感じます。

【森構成員】　はい、分かりました。ありがとうございました。

【山本主査】　私は、プロファイリングによって特定のユーザーの属性や脆弱性が分かったときに、それに合わせて決定環境を変化させる、UIを個々の属性、脆弱性に合わせて変化させることがあり得るのかなと思いました、UI、決定環境を当該ユーザーの脆弱性に合わせて変化させるということになると、やはり相当、意思決定に影響を与え得ると思いましたがいかがでしょうか。

【安江氏】　私の説明もよくなかったかもしれませんけれども、UIではない別の手口ということではなくて、当然、UIなんですけれども、UIの形とか在り方だけではなくて、そこにそういう意図が入ってきますし、それから、今見られている典型的なダークパターンというのも、ユーザーの脆弱性に応じて、使い分けられていくということになると思いますので、そういう点では、融合した捉え方が必要という理解なので、山本先生がおっしゃったことと違うということではないと思っています。

【森構成員】　なるほど、ありがとうございました。よく分かりました。

【山本主査】　ありがとうございます。後半のところも非常に重要な御指摘を森さんからいただいたと思います。ありがとうございました。

それでは、生貝さんからお願いいたします。

【生貝主査代理】　お二方とも大変貴重な御示唆、ありがとうございました。

安江さんに感想が１つと、小竹さんに質問が２つという形になります。まず、安江さん

の整理に関しては、プロファイリングという部分に関しては、恐らくアメリカのFTCも、最近、20年くらい前、積極的に使っていた「プロファイリング」という言葉自体はあまり使わなくなっているのだけれども、最近はまさにAIのフェアネスや、アルゴリズムの問題という形で、非常に活発に取り組んでいる部分が、law enforcementも含めて、FTC法第５条に基づいてあるんだろうと言ったときに、恐らくその辺りの最近のFTCの活動が、今、森先生、山本先生がおっしゃっていたような、ある種のダークパターンとプロファイリングの接点として、FTC法５条、まさにディセプティブな取組を罰するといったようなことの中に含まれてくるような気がいたしますので、今後何か機会があれば、まさにFTCのAIや、昔で言う「プロファイリング」という言葉に関わる活動も、もしかするとスコープに入れても見えてくるものがあるのかなと感じましたのがまず１点でございます。

それから、小竹様の御発表については、実は僕も太田さんの御質問と関連して、いわゆるApple、Googleの規制の中に、ダークパターンや、プロファイリングに関するものがどの程度含まれているのかなということを聞こうとしたんですけれども、関連するお答えも既にいただいたので、他方で、恐らくアプリに対する設定、まさにApple、Googleによる規制があり、そしてまた他方で、前半、まさに安江さんに御紹介いただいたような国家による規制があり、２つのレイヤーがあり、この２つは様々な形で絡まり合っている。そうしたときに、例えば、欧州域内で特定のダークパターンやプロファイリングに関する行為が禁止されていたら、Appleによる利用規約の運用や執行も、欧州域内では、それを無視するということは、恐らくないのだろうなといったような論点が恐らく出てくる。

そうしたときに、これはもし何か分かればなんですけれども、例えば欧州でこういったダークパターン、プロファイリングに関する規律が厳しくなっているときに、特定の法域、EU域内に関する利用規約のエンフォースメントに関する影響が何か見てとれることがもしあれば教えていただきたいというのが１点目です。もう１つ、今後、僕も勉強したいというところですけれども、実は、Appleのアプリストアも、Googleのアプリストアも、デジタルサービス法の、まさにVLOPに指定されている。VLOPでなくても、既に安江さんの参考資料にあったとおり、コンテンツモデレーションに関する、これ、広いんですよね、迅速あるいは透明、アカウタブルな対応といったようなものが広く求められてきているというふうに言ったときに、各アプリストアの、やはりこういった様々な問題のあるアプリに対する対処の在り方が、VLOP指定以降、何か変化があったのかどうかというのが最近気になっておりますというのが２点目でございます。もし何か関連してお知りのことがありまし

たら。

【山本主査】　ありがとうございます。

それでは、FTCの話は、安江さんですか。どうでしょうか。

【安江氏】　FTCについて、直近のところで、プロファイリングとダークパターンに関しては、FTCが出したこの資料にも入れたレポートでは、プロファイリングはあまり強くフォーカスされていないですけれども、おっしゃっているように、FTC法第５条のディセプティブな行為の禁止ということで、御存じのとおり、2000年ぐらいから行動ターゲティング広告、あるいは、2010年代半ば頃ですか、ホワイトハウスも含めて、ビッグデータ分析によるリスクの指摘というのはなされてきていて、最近は、AIのフェアネスなどですけれども、御指摘のとおり、プロファイリングという言葉は使っていないですけれども、そういった事象について強い問題意識を持っていますし、FTCはやっぱり、自分たちはすごい執行権限を持っているんだということも認識してやっているので、そういったところでは見ていく必要があるのかなと思って意見を拝聴しました。

【生貝主査代理】　ありがとうございます。まさに「プロファイリング」という言葉に必ずしもこだわらず、問題領域を設定する方法も何か常に考える必要があるんだろうなと感じていたところでもありました。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、後半の御質問は小竹さんにお答えいただければと思いますけれども、いかがでしょうか。

【小竹氏】　１点目について、EU含む、地域ごとの規制、法律に対する対応は、Apple、Googleともにしっかりとやっているのかなというところで、それごとに変えている印象になっております。

直近のものですと、EUにおいて、デジタル市場法が適用されたことによって、SafariやiOSにおけるWebKITの前提をなくしなさいとあったので、それに対応しましたというところで、ここには詳細が載っていませんが、例えば、デベロッパーがアプリ開発に当たってWebKIT以外のブラウザエンジンを使用できるようにしなさいという形にEUで言われたので、それを対応したのはEU域内のみという形で、EU域外ではそれは認めていないという形に規約が変わっていたり、こういうような形で、ダークパターン等についても、EUで先行的に規制が発生した場合には、EU域内においてはここまで禁止しますとか、そういうような規約を加えて、かつ、EU内に対するアプリに対しては、そこまで何かしらチェックするよう

な対策を加えてくるのかと推測されます。

２点目については、申し訳ないんですけれども、実際の審査状況は基本的に非公開で、それを時系列でどう変わったか追ったわけではないので、規制があった後に大きく変わったかは、今、把握しておりません。

以上になります。

【生貝主査代理】　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、次に、寺田さん、お願いいたします。

【寺田構成員】　よろしくお願いします。各国の詳細な調査の御発表、ありがとうございます。私からは、御発表や、これまでの構成員の皆さんのお話を受けて、今後どう対応すべきなのかなということに関して、考え、意見を述べさせていただきます。

まず、ダークパターン、それから欺瞞的な行為について、今回、改定を検討しているSPIで明確に禁止であるということを示す必要があるだろうと。その上で、想定されるユーザーインターフェースや、対象者ごとの対応については、ある程度、具体的に例示することが必要なのではないかと考えています。

特に、ダークパターンに該当するかしないかということに関しては、事業者側でも非常に判断に悩むことがある。例えば、解約までの画面遷移の回数とか、こういったものを含む方法、それから解約することによって不利益が起こる場合の注意喚起の説明の程度など、情報の取得の際の都度のポップアップの頻度、それから、行動変容を促す場合の表現の程度とか、非常に難しい線引きの必要があるのかと思っています。こういったことについては、具体的な線引きの言及といったもの、どこまでできるのかはかなり難しいですけれども、一定程度やはり示していく必要があるだろうと思っています。

その上で、これらに関して法的根拠を与えるために、やはりダークパターンの禁止については、ぜひ電気通信事業法で明確に禁止する条項を加えていただければいいのではないかと考えています。

プロファイリングですが、プロファイリングが全て悪であって、一律禁止のような誤解、誤ったイメージがちょっと広がりつつあるのかなということも考えていますので、どのようなプロファイリングがまずいのかということを明確にする必要があるのかなと思っています。

その際、子供や情報弱者、あるいはセンシティブな情報に関して、これらは除いて、デ

ータの収集や処理の仕方ではなくて、利用方法に重点を置いた、そういった視点で検討する必要があるだろうと思っています。

利用者が自ら収集あるいは処理についてコントロールするというのは、前回の御発表でも分かったとおり、なかなか難しいだろうということで、これはやはり利用者に不利益とか差別、こういったことを与えない利用とはどういったものなのかということを重視した禁止事項を示すことが重要なのかなと思っています。その上で、不安を払拭するような説明も必要であるというふうに、これらを明確にしていくということも重要なのかなと思っています。

私のほうからは、以上、意見の発表になります。ありがとうございます。

【山本主査】　ありがとうございます。

２点、SPIとの絡みでダークパターンの話、それからプロファイリングの話を後半にしていただきました。プロファイリングの規律の在り方についてですが、安江さんに、例えばEUが、プロファイリングの規律をどういう考え方に基づいてやっているのかについて、少し御説明いただいてもよろしいでしょうか。コンパクトにまとめると、結局こういうことだということがあれば、おっしゃっていただければと思います。

何が言いたいかと申しますと、例えば、子供や、特定の人たちを対象にして、禁止する、センシティブ情報を例えば使わないという禁止的な形でやっていくというアプローチと、さっき寺田さんがおっしゃるような本人にコントローラビリティを与えていくというアプローチが多分両方あり得て、EUが両方考えているのか、それとも、コントローラビリティよりも、特定事項の禁止という方向で言っているのか、その辺の関係性だと思うんですけれども、少し御示唆いただいてもよろしいでしょうか。

【安江氏】　はい、分かりました。

まず、プロファイリングに関しては、GDPRにおいては、21条で、まず、異議を述べる権利があって、プロファイリングされないという、しないでねということを言える権利があるということと、22条では、データ主体に関する法的効果や重大な影響を与えるようなプロファイリングに関しては、基本的にはやってはいけないという形になっているということです。

35条で、そういったプロファイリングをする場合や、特別カテゴリーデータを用いたようなプロファイリングをする場合には、事業者は、コントローラーは、データ保護影響評価をしなければいけないという形になっていて、こういうプロファイリングは駄目という

ことは具体的にはやっぱり難しいと思いますので、基本的には、ユーザーが嫌と言う権利と、「重大な影響」という言い方になっていますけれども、その場合には駄目という形になっています。22条に関してはガイドラインが出ていると思いますけれども、そういう形になっています。

一方、DSAでは、未成年者に対するプロファイリングに基づく広告は駄目だとか、特別カテゴリーデータを用いたプロファイリングによる広告は駄目という形の禁止を、特定した形で定めているという形になっていると思います。

【山本主査】　ありがとうございました。大変よく分かりました。

やはりここは排他的ではないのかなという印象があります。禁止的、制限的なアプローチと、それからコントローラビリティというか、本人の関与を認めていくというアプローチとの関係ですね。寺田さん、この辺はいかがでしょうか。排他的でなくて両方考えていくということになるのか、それともどっちかなのか、相互に排他的なのかというと、どうでしょうか。

【寺田構成員】　排他的にしなければならないものというものも存在するんだと思っています。子供や、センシティブな情報、こういったものに関しては、やはり排他的に考えるべきなんだろうなということがあるのかなと思っています。

もう１点、これはアメリカの特徴ですけれども、機会均等ということで、例えばプロファイリングをした広告の中で、不動産などは、広告を出す地域が高額な収益のある人の場所に出しますとか、逆に、貧困な方が集まっているようなところには、その広告は出さないとか、これは日本でよくやるパターンですけれども、これはアメリカでは禁止されている、機会均等でなければならないという形で、この辺り、正直、グローバルでこうあるべき、このパターンでなければならないみたいなものは、非常に設定しにくいと。日本においてどうあるべきかというのは、別途考える必要があるのかなと思っています。

その上で、やはり有益なプロファイリングというのは当然存在するので、こういったところを阻害しないような形のものも、念頭に置きながら、ここはかなり難しいことを考えないといけないと思うんですけれども、幾つかの方法がやはり並列的に存在するんだろうと思っています。

以上です。

【山本主査】　ありがとうございました。

それでは、木村さん、次によろしくお願いいたします。

【木村構成員】　木村です。よろしくお願いいたします。御説明ありがとうございます。

最初に、大したことないかもしれませんけれども、安江さんの資料のP19のダークパターンのところで、「ゴキブリ捕獲器」とありますが、これはゴキブリの「ごきぶりホイホイ」みたいに黙って入って、そのまま捕らわれてしまうという意味でいいのか、１点、質問させてください。

次に意見、感想になりますが、今、カタカナ言葉はすごく消費者がイメージしにくくて、「ダークパターン」という、この言葉もしかりで、まだ「欺瞞的パターン」と言ったほうがイメージしやすいのかなというのは正直思ったところです。消費者が気づかずに誘導されてしまっているということで、望むようなコンテンツにたどり着けない、だからトラブルが起こってしまうというところで、日本だと、どうなんだろうなと思っています。３月の中頃に、全国消費者大会がございまして、そこで文化学院大学の学生さんたちが、ダークパターンについて調査をして発表されました。それによると、日本のほとんどの企業でダークパターンを使用しているという結果になりまして、彼らは問題だということで、法規制を求めて、消費者庁に意見書を出したそうです。ただ、そのことが総務省に届いているのかどうかというのは、私はそこまでは分からないんですけれども、とにかく日本においても、若い方がそうやって危険性を感じているということもありますので、消費者保護ということで、きっと消費者庁に意見書を出したと思いますが、省庁間で連携をすることが必要であると強く感じました。海外の例をご説明いただきましたけれども、やはり今後、日本で法規制をきちんとしていく必要があると感じています。

プロファイリングに関しても、自分の情報がどのようなものかということが自分で確認できないということが、とても不安になっていると思います。これをどうしていくのかという観点を、ぜひお願いしたいと思います。

それから、利用者情報についてですけれども、消費者が自己申告で設定するというのは、やはりなかなか難しいと思っております。事業者がきちんと設定をして、消費者が必要に応じて変更できるというのが本当は理想でしょうけれども、なかなかそこは難しいというところと、まだまだどういう設定をすればいいのかということが中途段階なのかなというところで、今後もそういうところはきちんと変更していただいて、消費者の不安を少しでも少なくしていただければと思います。

以上でございます。

【山本主査】　ありがとうございます。

御意見がほとんどかなと思いましたけれども、最初の……。

【木村構成員】　１点だけ、ゴキブリ捕獲器だけ、お願いします。

【山本主査】　そうですね。基本的にはそのような理解でいいと思いますが、安江さん、お願いいたします。

【安江氏】　18ページに、解約が困難とありますけれども、知らないうちに入ってしまって、入ってしまうと出るのが難しいという意味で使われています。ダークパターンの名称については、結構スラング的なものもいっぱいあるのでなかなか難しいですけれども、そういったような説明をされております。

以上です。

【木村構成員】　ありがとうございました。分かりやすい例えですけれども、誤解を招くのかなと思いましたので質問させていただきました。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、江藤さん、お願いいたします。

【江藤構成員】　安江さん、小竹さん、どうもありがとうございました。

私からは、安江さんにお伺いさせていただきたいんですけれども、今回の問題、「ダークパターン」という名前に代表されるとおり、本来的な詐欺のような問題であれば直接的に法律規制することで足りるんですけれども、実際には、ダークパターンは、今までは消費者庁の所管の法律などで少しずつ規制がされるようになっていて、しかし、その中でもダークパターンという形で包括的な定義をすることには非常に慎重で、というのも、今お伝えしたように、本来的には、この問題は詐欺でもない。どちらかというと、消費者側のある程度の錯誤を売手の側が惹起しようとしているというような巧妙なスキームというものなので、もし本当にこれについて消費者が不満であるとすれば、市場で排除されるというのが原則で、そういう業者がいるということがだんだん口コミで広まると、あそこの業者は汚いことをやって稼ごうとしている、使わないでおこうというのが市場の健全な在り方だと思いますが、頂いた資料の32ページでは、ダークパターンを含むウェブサイトに対する分布を見ると、実は人気のあるウェブサイトにダークパターンが現れやすいということで、本来的な今の話からすると、逆の結果が出ているかなというところが私から見ると気になりました。その点を御説明いただきたいというのが１つです。

２つ目は、先ほど木村さんがおっしゃった点は私も重要だと思っていまして、この問題、今回はガイドラインですけれども、ダークパターンという形で大きく打ち出すのか、それ

とも、最近のヨーロッパの傾向のように、欺瞞的というところを強く打ち出すのかで大分規制の仕方の印象も変わってくるかなと思っていますので、最近ヨーロッパでの第２次パターンですか、欺瞞的というふうに流れていることとの関連でも、今回、日本の規制を鑑みたときにどうすべきかということについて御助言いただけるとありがたいなと思っております。

小竹さんに対しては、GoogleとAppleの間でお互いが切磋琢磨する形で様々なポリシーが改定されていっているということがよく分かったんですけれども、例えば17ページの資料などを拝見させていただくと、このトラッキング表示について、ポップアップで表示するかどうかでは差がついていて、こういう差はどういうことで出てきているのか、こういうものもまた２年ぐらいたつとGoogleで追いついてくる問題なのか、そういったところを含めて御教示いただけると幸いです。どうぞ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。

それでは、安江さんから、お願いいたします。

【安江氏】　質問ありがとうございます。

まず、32ページのグラフは最初に太田さんからいただいた質問とも絡むと思いますが、ダークパターンが見つかったウェブサイトの比率ということで縦軸がありますけれども、このダークパターンがどのくらい悪質かというところが分からないこともあって、これはこの文献の中でも、このグラフがあって、単純な１センテンス、２センテンスの結果についての説明があるのみなので、今おっしゃられたような因果関係については、踏み込んだ分析がされていないということだと思います。

ただ、ダークパターンというのは、悪意があったかないかは別として、やっぱり消費者の背中を押すという部分はあると思うので、それによって人気が上がっている部分、あるいは、逆に、使っていることによって、そのサイトから離れられないなど、様々な要素があると思うので、その辺の分析は深くしないといけないのかと思います。

２点目の質問はすごく難しい質問ですけれども、ダークパターンというのは現れた結果だと思うので、基本的には欺瞞的というところがやっぱり重要だと思っていて、資料の次の33ページでも、デジタルサービス法では「ダークパターン」という言葉を使っていますけれども、ほかの法律やレポートでは「欺瞞的な取引」とか、そういった言葉も多く使われていますし、具体的な内容としては「データを不公正な方法で取る」とか、あるいは「ユーザーを操作する」ということがあるので、そういった点を考えていくと、「ダーク

パターン」と「欺瞞的」とどっちがいいかという二択はなかなか難しいですけれども、ダークパターンということだけにこだわり過ぎないほうがいいのかなという印象を受けています。

以上です。

【山本主査】　ありがとうございます。

江藤さん、いかがでしょうか。今の安江さんの御回答に対しまして何かございますか。

【江藤構成員】　大丈夫です。ありがとうございます。

【山本主査】　ありがとうございます。

それでは、次に、小竹さん、お願いいたします。

【小竹氏】　Appleの取組のほうが先行している理由としては、純粋にビジネスモデルの違いといいますか、Googleは、やはり広告でもうけているところがございますので、本音としては、そういう規制はやりたくないけれども、やっぱりAppleがやっている以上、それにしていかないと、どんどん差がついてしまうというところも、多分もともとのビジネスモデルの差としてあると思います。また、OSのモデルの差といいますか、iOSに関しては基本的にはAppleが垂直統合で使っているので、変えるのであれば強制的に変えていけるんですけれども、Androidの場合は広くオープンソースで公開しているので、あまりにも新しい機能をどんどん入れていくと、それに対応していないAndroidスマホも大量に残ってしまいますし、そういうところもあって、時間をかけて、Appleがやったので、うちも対応しましたよと、ある意味、これは推測ですけれども、ほかの開発メーカーに対する言い訳的なところに使えるというところもあって、Appleを追随する形になっているのかなと推測しております。

【山本主査】　ありがとうございます。

江藤さん、いかがでしょうか。

【江藤構成員】　よく分かりました。どうも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、呂さん、お願いいたします。

【呂構成員】　本当に勉強になる御発表、ありがとうございました。

私からは、ダークパターンの御発表について、１点意見ですけれども、寺田さんもおっしゃっていたとおり、今回SPIを改定するということで、表現の仕方については今いろいろと議論がありましたが「ダークパターン」という横串の概念を通して、様々な欺瞞的な

商取引慣行について検討、注意喚起していくことは、良い方向性だと思いました。

江藤様からも御指摘がありましたが、既に、詐欺や錯誤については個別の法律で規制があります。私も以前、ダークパターンについて調べたことがありますが、既存の法律でダークパターン的な行為が個別に規制されている部分も随分あり、例えば、消費者契約法、個人情報保護法、独禁法、景表法、特定商取引法、特定電子メール法など、様々な法令に散らばっていますので、SPIでダークパターンについて記載する場合には、こうした既存の規制も紐付けて記載することが考えられると思います。もちろんダークパターンには様々な類型があり、直ちに違法というものばかりではないので、ガイドラインレベルで記載するということに意味があるのだと思いますが、特定の行為については既に違法であり執行される可能性があるということで、既存の法律を整理して紐付けておくと、実効性という観点からも意味があるのではないかと思いました。

私からは以上です。

【山本主査】　ありがとうございます。

それでは、森さん、いかがでしょうか。

【森構成員】　手短に。２回目で申し訳ございません。寺田さんのお話に若干反論させていただこうかなと思って、すみません。

１点目は、ユーザーがコントロールできないというお話でしたけれども、もちろん同意の問題等は私も承知していますが、こうやってGoogleとAppleがデータの利用について同意を必須にしていて、アプリに至ってはオプトアウトも部分的に、オプトアウトといいますか、同意の撤回ですよね、それも部分的に求めているというような状況で、ユーザーコントロールできないですとだけ、したがって、ユーザーのコントロール権を認めないというのはナイーブに過ぎるのではないかということが１点です。

それから、現状認識として、プロファイリング全てが悪いとされているのではないかということでしたけれども、これは現状認識の問題ですから、単に意見の違いということだと思うんですけれども、私はそんなふうには思われていない、世の中的にそうはなっていないと思っていまして、プロファイリングは個人情報の取得ではないという解釈が通説化しているので、割とプロファイリングというのは、やりやすい制約のない状況になっているのではないかと思います。

３点目、これが一番申し上げたいことですが、利用目的に着目した制約が適切であると、差別をもたらすような理由目的ではないことが重要だと、プロファイリングに関して、そ

ういうお話でしたけれども、私は、利用目的がどうかということ以前に、どのような性質の情報をプロファイリングによって生成するのかということが非常に重要だと思っていますので、利用目的もさることながら、もちろん利用目的も重要ですけれども、それと同じぐらい、どんな情報を生成するプロファイリングなのかということに着目することが重要だと思います。

以上です。

【山本主査】　ありがとうございます。

寺田さんから再反論ということかもしれませんけれども、よろしくお願いいたします。

【寺田構成員】　再反論ではなく、利用者のコントロール権というのは、それはもちろん前提として必要だと思っています。その上で、でも、どんどん難しくなってきて、やるのが難しい、中にはコントロールを初めから放棄してしまうような人もいるようなので、そういった人たちもちゃんと念頭に入れるということでいくと、コントロール権だけではないやり方も必要だろうということでお話しさせていただいています。

それから、プロファイリングは、もうこれは皆さんがどう考えているかということですけれども、単純に方向性として、プロファイリングは、そのものが悪みたいなイメージがだんだん強くなってきているなというのはちょっと感じるところがあるので、これは人によって違うのかなとは思いますけれども、公的機関で、パンデミックなどが典型的で、安全保障上の問題みたいなところでは、ある程度、プロファイリングが必要な部分もあるんだろうと思っていますので、そういったものに関して、特にパンデミックの際に、プロファイリングみたいなものが悪みたいなイメージがちょっと強く出たことがあったので、そういうことが惹起されるようなことがないようにするべきかということでお話しさせていただきました。

３つ目は、これも利用目的のという部分は、ユーザーが皆コントロールできればいいですけれども、そうできない場合のことを考えると、利用目的というものももっと重視すべき、特に最近、単純に取得だけに、最近、EUやアメリカは取得だけという方向からどんどん利用目的部分を増やしていっているようですけれども、日本でもそういった利用目的の部分がちょっと軽視されている部分があるので、重視すべきではないかなということでお話しさせていただきました。

以上です。

【森構成員】　御発言の御趣旨がよく分かりました。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、第１部はここでと思いますけれども、私から２点ほど。１点は、ダークパターンについては、どう呼ぶのか様々な議論があるかもしれませんが、SPIで取り込んでいくという方向性については特に異論はなかったように感じましたので、今後、その方向でも検討していければと思いました。

それから、最後の点ですけれども、やはりプロファイリングについても、今の寺田さんの御発言からも、禁止的なものと、コントローラビリティを認めるということは、相互に排他的なところではない。例えば、子供の場合には、本人の同意があったとしても、やはりこれは禁止だという、ある種の排他性があるのかもしれませんが、両方ともあり得るというか、排他的でないと感じましたし、利用目的なのか、それとも分析対象なのかというところも、やはりこれも排他的ではないのかなというふうに思いましたので、これは両面を見みながら、今後、議論を深めていければというふうに感じた次第です。

それでは、続きまして、第２部ですけれども、利用者情報に関わるモニタリング等に関して、事務局からお願いいたします。

【川野利用環境課課長補佐】　事務局でございます。それでは、第２部を説明させていただきたいと存じます。資料３－３、利用者情報の取扱いに関するモニタリングについて、説明させていただきます。

第１回利用者情報ワーキンググループでもお話しさせていただいておりますけれども、スマートフォン上のプライバシー対策に関わる論点とともに、利用者情報に係るモニタリング等につきましても論点と挙げさせていただいているところでございます。

１ページを御覧ください。

利用者情報のモニタリングにつきましては、枠内１ポツ目に記載させていただいておりますように、「電気通信事業における個人情報等の保護に関するガイドライン」において、同ガイドラインの遵守状況及び電気通信事業者による事業の取扱いについては、定期的にモニタリングを行い、現状を把握することとされております。

昨年度は、プラットフォームサービスに関する研究会において、デジタル広告市場の競争評価最終報告で確認することとされておりました項目等を中心にヒアリングを実施いたしまして、各事業者の取組の確認を行ったところでございます。

２ページを御覧ください。

御参考までに、昨年度実施しましたモニタリングの資料となっております。

昨年度は、デジタル広告市場の競争評価最終報告において確認することとされた項目等を中心に、各事業者の取組状況の確認を行っております。

また、３ページがデジタル広告の観点における各社の取組について、各社に記載いただきましたヒアリングシートとなっております。

４ページを御覧ください。

これらのヒアリングシート及び研究会における事業者へのヒアリングを通じまして、プラットフォームサービス研究会において取りまとめられた内容となっております。

１ポツ目から３ポツ目は枠組みの話となっておりますけれども、４ポツ目に関しましては、寺田先生から御意見を頂戴したところと思いますけれども、新たなターゲティング手法の登場等の業界の動向を踏まえながら、プラットフォーム事業者における情報取得の方法等、利用者情報の取扱いについて確認していく必要があるということ。

５ポツ目でございますけれども、モニタリングを行うに当たっては、プラットフォーム事業者がアカウントを使用してない利用者やログインしてない利用者からも情報を取得していること、第三者や、第三者のウェブサイトを通じて情報取得していること等に関し、利用者保護の観点から、対応を行うべきではないか検討を行うことが必要であるというふうにされておりました。

モニタリングの結果につきましては、参考資料３－２、利用者情報のモニタリング結果、2023年11月８日がございますので、こちらを御参照いただければと存じます。

５ページを御覧ください。

今年度のモニタリングの進め方の案となっております。

今年度のモニタリングに当たりましては、昨年度の取組も踏まえまして、より効率的に、効果的にモニタリングを実施できればとのことで、本日、先生方から頂戴する御意見を踏まえまして、ヒアリング項目を確認させていただいた上で、ヒアリングシートを昨年度より少し早めに事業者に送付し、ヒアリングに向けて準備していきたいと考えております。

また、主なモニタリング対象事業者といたしましては、昨年度と同様に、プラットフォーム事業者に加えまして、大手通信事業者を想定しているところでございます。

具体的なモニタリングの観点について説明させていただきます。

６ページでございます。

プラットフォーム事業者につきましては、昨年度のモニタリングを踏まえまして、プラットフォーム研究会から受けた提言、本ワーキンググループにおけるスマートフォン上の

プライバシーの在り方の検討の中で、事業者における状況について確認することが必要とされた論点を踏まえ、以下の観点でモニタリングを実施することとしてはどうかと考えております。

一番左側に書いている１、２、３、４は、透明化法における主な確認項目でございまして、こちらに「５その他」を追加いたしております。

また、昨年度のヒアリング項目を参考までに書かせていただいていて、右側に今年度の主なモニタリング観点案を記載しております。

取得する情報の内容、取得・使用の条件の開示について、あと、ターゲティング広告を実施する旨及び事前の設計の機会やオプトアウト機会の提供につきましては、４ページでお示しいたしましたプラットフォーム研究会で御提言いただいた内容を記載させていただいております。

本日、後ほど日本総研様からも、この点に関しまして、調査研究の内容等を御発表いただけるかと存じます。

また、ログインの有無やアカウントの有無について、利用者に対する説明の水準に差異がないか。非ログイン・非アカウント保有の利用者に対して適切な説明がなされているか。利用者から直接取得ではなく、第三者や第三者の運営するウェブサイトを通じて利用者情報を取得・利用していることについて、利用者に適切な説明がなされているか。３点目、４点目に関しましては、昨年度もモニタリングを行っておりまして、こちらに関して改めて確認するべき項目があるか。

５その他としまして、利用者のターゲティング手法に変化がある中で、利用者情報を取得・利用するに当たり、同意の取得やオプトアウト機会の付与など、利用者関与の機会が設けられているか。

また、利用者が容易に認知・理解できるようになっているか。

その他、モニタリングの進め方について、工夫すべき点はあるかといったようなことで記載させていただいているところでございます。

次に、７ページを御覧ください。

こちらは、昨今、電気通信事業者において、委託先等を通じて大量の利用者情報の漏えいが発生する事案がございます。参考資料３－３を添付しておりますけれどもNTT西日本、NTTドコモの例を記載させていただいております。

これらの具体的な事案も踏まえまして、利用者情報の取扱いを委託する場合には、再委

託先も含めて適切な監督を行うことが重要と考えられますので、以下の項目について確認できればと考えております。

１、２と記載させていただいておりますけれども、観点案を各々示させていただいております。それぞれ委託先の監督について、安全管理措置について、また、その他として、項目案、観点案を示させていただいておりますので、御確認をお願いできればと存じます。

本日、先生方から御議論いただいた内容を踏まえまして、３ページに昨年のヒアリングシートを載せておりますけれども、こういったヒアリングシートを、次回、５月下旬頃の会合をめどに、事務局から再度お示しさせていただきまして御議論いただければと考えているところでございます。

説明は以上でございます。どうぞ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した。

それでは、続きまして、日本総合研究所の小竹様から、非ログイン利用者の保護についてですけれども、ちょっと時間が押しておりますので、少し巻きぎみでお願いできればと思います。大変申し訳ありません。よろしくお願いします。

【小竹氏】　承知いたしました。日本総合研究所の小竹でございます。

それでは、アカウント未取得者、非ログイン時のサービス利用者の利用者情報の取扱いについてです。

今回調査した内容といたしましては、大きく２つございます。

１つ目が、プライバシーポリシーにおいて、非ログイン時、サインアウト等の状態で使った場合に、どういう情報が取られるか等について、明確に記載があるかについて、この７社のプライバシーポリシーを読ませて、少し日本総研の主観が入った部分はありますが、評価させていただいたというところになっております。

２つ目が、この７社の代表的なサービスにおいて、特に④です、利用者情報の管理機能について、ログイン時と非ログイン時で提供されるものに差があるかどうか。どういうものが提供されているかを調査したものになっております。

時間が限られているところ、ポイントだけ、①がメインになりますので、少し時間をかけて、その後は、④だけ御報告させていただければと思っております。調査項目についても説明しながら報告させていただきます。

まずは、プライバシーポリシーでの記載について、１点目は全体で記載があるかどうか。非ログイン時の情報の取扱いに関して、明確に、こういう場合に非ログイン時でも取りま

すという記載があったのは、７社中３社、Google、Meta、Xについて記載があった形になっております。

なぜ三角になっているかというと、例えば、利用者情報の取扱いに関して、情報の取得、目的、第三者の共有、利用者の関与、それぞれについて非ログイン時について書かれていたわけではなくて、ある一部の項目にだけ、基本的には取得情報に関して、非ログイン時はこうですよという記載があるだけで、じゃあ、それがどういう目的で、非ログインで取られた情報は、他と取扱いが違うのかというところは分からなかったので、三角になっています。

記載方法の分かりやすさに関しても、どこかに分けて書かれているというよりは、その取得情報の項目のところを細かく読んでいくと、あるんだというところが分かる形になっていたので、分かりやすさとしても三角という形になっております。

例えば、Googleの場合ですと、例えばGoogleアカウントでログインしてないときでも情報は保存しますと書かれていて、ただ、どういう情報を取得しているのかというのが明記されていなかった形になっております。

Metaが一番分かりやすかったんですけれども、弊社が取得する情報の中に「アカウントをお持ちでなくても」というところをクリックすると、別のポップアップが出て、ここに取得する情報と、目的の例が書かれているという形になっております。

Xの場合には、非ログイン時の「情報取得」に関して、さらにその中のログ情報の項目の中の最後の一文に、サインアウトした場合であっても、こういう情報は受領しますという形で、よく読み込めば分かるというような形になっています。

ここからは個別の記載と、もともとは、ある程度書かれていて、個別ごとにどうなっていくのかを分析しようと思っていたんですけれども、７社中３社しか書かれていなかった、それも一部の項目であったので、ここからは、書かれている、書かれていないだけではなくて、その文章の中から、非ログイン時でも推測できるかどうか、よく読み込むと、多分これは取得されるのではないかと、若干、私の主観にもなっているんですけれども、推測可能かどうかでも判断は入れております。

基本的に、多くのサービスの事業者様として、ユーザーがログインしていようが、ログインしていなかろうが、結局、うちのサービスを利用しているんだから、そこで情報は取られるところをなぜ分けて書くのかという言い分もあるのかなと思っていて、例えば、サービスの利用に関するところですとか、アプリ、デバイス等のところ、パートナーなどか

ら、第三者から得る情報に関しては、サービスを利用する場合には、こういう情報を取得しますと書かれているので、ログインしようが、非ログインであろうが、こういう情報は取得されるのかなと、全体的に推測できるとされたと考えます。

一方、アカウント登録に関する情報に関しては、登録した場合に、ユーザーが提供した場合にだけ取得しますと書かれているので、こういうものは多分取得されないだろうというところが推測される形になっております。

Google、Meta、Xについては、先ほども申しましたように、ある程度、取得情報に関しては、非ログイン時に関して分けた記載が見当たったところ、一部丸になっております。

次に、情報の取得、目的、共有に関しては、基本的には、明確に分けた記載にはなっていないですし、個別の記載から、非ログイン時に取得した情報は、こういうふうに扱いますとも読み取れなかった。

一方、Metaに関しては、三角になっている理由としては、利用の目的別に表になって利用する情報が一対一で記載されておりますので、例えばMetaの場合ですと、第三者から得る情報は、アカウントがなくても使うということが分かっているので、その情報を使う目的を照らし合わせれば、非ログイン時でもこういう目的のために使われるんだなと一定程度推測可能というところで、三角にしています。

最後に、アカウントとの関連づけで、非ログイン時の取得した情報について、何かしら保有しているアカウント、もしくは第三者のパートナー等から取得した情報とひもづけられるのか、ユーザーからすると、非ログインで利用するんだから、それほど情報を推測されたくない、もしくは、そこまで取られたくないという思いで利用しているところもあるのかなというところ、裏側で、何かほかのものと意図しないひもづけをされる、関連づけをされるというところは、なかなか想像しにくい部分なのかなと思いますが、そういうところについて記載があるかどうかになっております。

Xに関しては、明確にサインアウトした端末につきましても、ほかのブラウザもしくは端末と関連づけることがあると書かれておりますので丸にしておりまして、LINEヤフーや楽天については、明確といいますか、第三者のパートナーとの情報のひもづけに関して記載がありましたので、その内容を読むと、推測される、関連づける可能性はあるのではないかというところで、三角としております。そうではない可能性も十分あるんですけれども、そう読み取れたというところです。

Google、Meta、TikTokについては、そもそもそういうことすら明確な記載がなかったの

で、読み取りようがなかったというような結論になっております。

Appleに関しては、そういう情報は関連づけを基本的にしませんよと、一応ポリシーとして表示しておりましたので、三角としております。

最後、２点目で、利用者情報の管理機能についての結果ですけれども、４点目で、どういう結果だったかを御報告させていただきます。

様々な機能を７社見て、共通的なものとしてあったのが、アクティビティ情報の管理機能と、広告の設定、各サービスのサービス内での広告配信と、各社さん、プラットフォーマーとして持っている情報をベースに、サービス外でのパートナーのサイトでの広告配信等もしておりますので、そちらへのコントロール機能を両方見ております。

AppleとFacebookに関しては、そもそもAppleはそういう広告サービスは積極的ではないので、そういうサービスはログイン時も提供していないですし、Facebookは、そもそもログインしていないと利用できない状態であったので対象外としています。広告に関しては、Yahoo！を除いて、５分の５を提供しているというような形になっております。

一方、アクティビティ情報に関して、Yahoo！の場合には、広告設定がない代わりに、非ログイン時でも蓄積された検索履歴ですとか、利用履歴を削除できる機能がございますので、多分これを削除すれば広告に利用できないという形で、対になっているのかなと思っております。

アクティビティ情報の削除に関しては、Yahoo！とGoogle検索以外では提供されておらず、TikTok、X、楽天、App Store利用者は、検索履歴、アクセス履歴等が残るとは思いますが、それに対して、ダウンロードや削除という機能はなかったという形になっております。

その他として、Xについては、先ほど申しましたように、明確にサインアウトした情報についても、何かしらのひもづけをして推測をしますということは明言していますが、それに対になる形として、非ログイン時でも、こういう推測される識別情報に関して、オンオフをできるような機能が備わっています。

最後に、総括ですけれども、まずはプライバシーポリシーにおける非ログイン時の利用者情報の記載に関して、７社中３社で限定的だった。

その記載があった３社についても、情報取得の一部の項目でのみ言及しているので、非ログイン時にどういう情報が何のために取られて、それがどういうところで利用され、共有の可能性があって、それの利用者関与の機会等がどう提供されているのか全体像がぱっ

と分かる状況ではなかったのかなというところになっております。

ただ一方で、各社のプライバシーポリシーの記載から、非ログイン時でも、他の利用者情報は、特にサービスのログや、利用状況等は取得されていて、パートナーから取得した情報と関連づけ、それに基づいた推測等は行われているのではないのかなという可能性が読み取れたというところになっております。

３つ目の利用者情報の管理機能に関しては、非ログイン時でも広告配信関連の機能は大半の事業者で提供されておりましたというところです。

アクティビティ情報の管理機能に関しては、限定的であったから２社のみでした。

今後の課題・取組といたしましては、やはり非ログイン時の情報の取扱いについて、利用者が情報を容易に把握できる状態ではないというところと、多分、何かしらの識別子で非ログイン時でもひもづけられている、推測されている可能性があるので、利用者として想定がしづらいのではないかと思っております。

ですので、非ログイン時の利用者情報の取扱いの通知・公表の記載のルールや、ベストプラクティス、特にほかの情報との関連づけに関して検討した上で、浸透させていくことが重要なのかなと考えた次第でございます。

以上が調査結果の報告になります。

【山本主査】　ありがとうございます。

それでは、ただいまの御説明、非ログイン利用者の保護のお話と、前半は事務局から、利用者情報モニタリングの新たな観点について御説明いただきましたけれども、この点について、残り15分弱ぐらいですけれども、構成員の皆様から御意見をいただければと思います。いかがでしょうか。

では、寺田さん、お願いいたします。

【寺田構成員】　こちらも非常に詳細な御説明をありがとうございます。

全部の規約やプライバシーポリシーを洗うのは非常に大変な労力が必要なので、逆に言えば、それだけの労力が必要ということはなかなか利用者には伝わりにくいということで、この辺りの改善をどう考えていくのかということも重要かなと思います。

まず、ログインしていない場合のプライバシー保護に関する規約ですが、前回も私からお話しさせていただきましたが、ログインせずに利用するということは、そもそも情報を取得されたくないと考えている場合もやはり前提としてあり、そうすると、ログインしない場合にはどのような扱いになるのかといった説明は、ログインしている場合と変わりな

く、できるだけ分かりやすいところにあるべきであろうと思っています。同時に、非ログインの場合でも、ファーストパーティCookie、利用者を識別可能なIDなどを取得している場合が多いですので、こういったものに関しては、やはりオプトアウトができるようにしていくということも今後進めていく必要があるだろうと思っています。

モニタリングについてです。こちらも経年変化や事業者間の差を可視化できるような、そういったKPIの設定を、もう少し考えるべきかと思っています。

本日、前半で御発表のあったダークパターンやプロファイリングについて、これは事業者側がこういったことをしていますよという申告だけでは、実態が分からないことが多く、第三者による実態調査などを、モニタリングの中に含めるのか、別途考える必要があるだろうと思っています。

一方で、委託先管理などの安全管理措置は、外部から観測することが非常に難しいと、大手については、報告義務が課されていたり、個人情報に関しても何らかの形で公表すべきということが法律で制定されたりしていますが、利用者情報に関しても、同じように、少なくとも公表を義務化する必要があるのかなと思っています。

それから、以前から私が指摘させていただいているサードパーティcookieが利用できなくなるということに関しては、実際に動いているのがファーストパーティデータをどんどん活用していきましょうとか、ユニバーサルIDのような新たな識別子をつくりましょうとか、データクリーンルームのように、非常に利用者に分かりにくい手法といったものがどんどん広がってきています。これらは、いずれも基本的には個人データを利用した第三者提供に該当する場合が非常に多いです。そうなってくると、同意の有効性が大きな問題になってくるだろうと。したがって、同意の有効性についてモニタリングをするとか、KPIをちゃんと設定するということが、今後、絶対必要になるだろうと思っています。

ちょっと多岐にわたりましたが、私からの意見は以上になります。

【山本主査】　ありがとうございます。

それでは、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。

私からも、御説明にもあったように、なぜ非ログインで使うかというと、やはり利用者が情報を取得されたくないですとか、関連づけたくないということでログインしていないということもあると思いますし、１人で複数のアカウントを持って、実情に応じて使い分けているという方もいらっしゃると思います。

１点、ちょっと分からないのが、非ログイン時とログイン時が同じ端末、例えば複数のアカウントでも同じ端末の場合、情報として関連づけられてしまうのか、それとも、そのアカウントに応じて情報がまとまるのかというところは、理解ができないので、ここを教えていただければと思っております。

また、意見になりますけれども、ネットを利用していますと、本当に広告がうるさくて、もうこれ、買ったからこの広告は要らないよ、と思うものが何回も何回も出てきます。たとえ情報の削除機能があったとしても、すごく分かりにくくて、本当にどうすればいいのかということが分からないことが多々あると思います。それから、非ログインのときにどうするかを利用者にきちんと分かりやすく提示していただきたいというのは同意でございますので、そこはお願いしたいと思っております。情報漏えいについては、今、大手はかなり公表していまして、やはり知らない間に利用者に不利益があるかもしれないので、きちんと公表していくということは、今後も続けていく必要があると考えております。

以上です。

【山本主査】　ありがとうございました。

１点、御質問が含まれていたと思いますけれども、時間の関係で、後で御回答させていただければと思います。

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した。大変有益な情報をいただいたと思います。

私は、この非ログイン時の情報の取扱いは非常に重要だと思うんですが、さらに言うと、アカウントを持ってない場合の情報の取扱いが非常に重要だと思っていまして、その場合、利用規約等を目にする機会は全くないわけなので、ある意味では、非ログイン時以上に、ユーザーにとってみれば、このときはユーザーではないですね、生活者にとってみれば、そういう情報を利用されることに対する抵抗感は強いのかと思います。それに関して、資料の６ページに、Metaの非ログイン時の情報取扱いの記載のところに、利用者がアカウントなしで弊社製品を利用し、または弊社製品でアクションを実行するとありますが、この記載ですよね。これは何となくイメージ的には、パートナーサイト、Metaに対して外部送信をするサイトを見たときの状況のお話なのかなと感じましたし、抽象的で分かりにくいですけれども、もしお分かりでしたら、Meta製品でアクションを実行するとか、Meta製品を利用するということの中に、単に「いいね」ボタンが設置されているだけのパートナーサイトを見る、これは消費者の立場からしてみれば、Metaの製品を利用しているとか、Me

taの製品でアクションを実行しているということには全くならないわけですけれども、その場合も含まれているのかどうかということ、また、さらには、アカウントを持っていない人に対するトラッキングについて、各社が何らかのコメントを出されているのかというようなことについて、もし情報があれば教えていただきたいと思います。

以上です。

【山本主査】　ありがとうございます。

森さん、すみません。これもちょっと時間の関係で、後で……。

【森構成員】　はい、もちろんです。

【山本主査】　ありがとうございます。

それでは、太田さん、お願いいたします。

【太田構成員】　森先生とほぼ同じことを言おうと思っておりまして、アカウントが非ログインというのは、アカウントを持っている人と持っていない人に分かれると思いますので、それぞれどういう書き方になっているか、実態を調査するということが必要なのかと思っております。

こちらはモニタリングにも関連すると思いますが、寺田さんからもお話がありましたとおり、非ログイン時も特にそうなんですけれども、データの収集の実態がどうなっているかというのは調査を行う必要があるのではないかと思っております。

その実態調査を行ったときに、どういったプラットフォーム事業者がデータを収集しているかは、一定出せると思いますが、その上で、情報を集めているプラットフォーム事業者は、小竹さんから発表いただいたこの調査対象となっているようなところ以外にも、ユーザーと直接接点を持たない広告のプラットフォームも、同じようにデータを収集していることについては、もう少し注目したほうがいいかと思っておりまして、モニタリングの対象事業者に、そういった広告プラットフォーム事業者も入れるべきなのかなと思っております。

ヒアリングシートについてですが、今の観点で、他アプリやサイトを経由した情報収集の状況というところ、大項目の３です。その質問の仕方が、去年のヒアリングシートの回答状況を見ると、事業者ごとに解釈が異なるなど、分かりにくいところが多いので、書き方の見直しをしていただきたいなと思っております。

以上です。

【山本主査】　ありがとうございます。

それでは、生貝さん、お願いいたします。

【生貝主査代理】　こちらのプラポリの調査というのは、グローバルプラットフォームであっても、基本的に日本ユーザー向けのプラポリということでございますでしょうか。そうしたときに、御案内のとおり、ノンユーザーの情報収集に対するGDPRの適用に関しては、それこそ2016年ぐらいから結構CNILが積極的にやったほか、当然、eプライバシー指令の国内法もあるし、または、他のアプリからの情報の統合に関しては、ドイツの連邦カルテル庁エンフォースメント及びそれを直接的に受けたか、デジタル市場法５条１項のサービス間データ組合せの制限といったような、様々な規律があるところ、例えばヨーロッパ向けのプラポリというのか、当然、ノンユーザーである以上、GDPR上、６条（f）に基づいて扱わざるを得ないですけれども、それでもアクセス権や、消去権、その他は全部適用されるというのがヨーロッパの法のつくりでありますので、法の変更を受けて頻繁に変わっていると思うんですけれど、欧州のプラポリに相当するものを１回眺めてみると、日本のだけでもすごく大変な作業なので、作業的にどうかということはあるんですけれど、すごく違うランドスケープが見えてきて、同じことをお願いするのかどうかはさておき、ある種のベストプラクティスを目指していくところというものも、もしかすると見えてくるのかなと思いました。

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、最後、江藤さんからお願いいたします。

【江藤構成員】　非ログイン時の情報の有用性について、プラットフォーム事業者において、ログイン時と非ログイン時だと、非ログイン時のほうが情報についてアイデンティファイできる可能性は低いということもあるのだろうという反面で、それが有効に使われれば、プロファイリングや、ターゲティングなど、十分に有効に機能し得るということですけれども、実際に非ログイン時でどの程度有用性があるのかを確認しておくことも重要かと思っています。

というのも、我々は、やっぱりログインしないときというのは、私たちのほうからはログインしていないんだから、それほどの情報は取れないだろう、あるいは、それほど情報は結びつけられないだろうとたかをくくっているところもありますが、事業者ではそうではなくて、これは実はかなり有用な情報だということであれば、ログインしている場合とは違って、どのぐらい我々の情報内部に浸食することが可能となっているのかという実態

を把握できるとありがたく思っております。

以上です。

【山本主査】　ありがとうございます。

今いろいろと構成員の方からお伺いした中では、やはりまず実態がよく分からないところだということだと思います。その調査なりモニタリングの必要性は浮き彫りになったのかなというふうに感じました。

太田さんからチャットで入っているんですけれども、これはすみません、時間の関係で今、読み上げられませんが、事務局におかれましては議事録に残すようにお願いいたします。(以下点線囲い部分)

---

先ほど発言した件も含めて、全体的な意見をこちらで述べさせてください。

1.ダークパターンと通知や同意等のあり方について

特に現行の法律で既に禁止されているものは当然ですが、ダークパターンとされる中でも欺瞞的なものをSPIの中で例示し禁止すべきと思います。

その上で、ダークパターンと同意のあり方についても整理が必要だと思います。

AppleもGoogleもデータの収集や仕様に対して同意を必須としていますが、アプリ利用開始時の規約同意で、すべてのデータ利用に対して同意をさせる、というのは、欺瞞的なダークパターンと言えると思いますし、非ログイン時のデータの取扱いについて、書いていない、どこに書いてあるかわからない、というようなものも、ダークパターンであると言えるのではないか、という観点でも検討し、SPIで方向性を示すべきと思います。

2.スマホウェブについて

AppleやGoogleの規約改定や審査によってアプリ環境は良くなっていると思いますが、アプリだけの話になっていて、Appleが導入するPrivacy ManifestoもアプリのSDKだけが対象になっています。

一方でスマホからアクセスするウェブ、これはアプリ内のウェブも含みますが、こちらについては、SPIも含め、スマホウェブの外部送信に関しては言及されていないことは問題だと思っていますので、今回スマホウェブにも焦点をあてるべきだと思います。

3. モニタリングについて

モニタリング対象として、プラットフォーム事業者や大手通信事業者とされているが、プラットフォーム事業者には例えばCriteo等の直接エンドユーザーにサービス提供していない広告プラットフォーム事業者も、実態を把握した上で、モニタリング対象とすべきだと思います。

特に外部送信規律について、できれば実態を踏まえた上でモニタリングを行うことが望ましいと思っておりますので、

非ログイン時のデータ収集を含めて外部送信について実態調査（または既存調査を参照）をおこなった上で、広告プラットフォーム事業者もモニタリング対象としていただきたいです。

ヒアリングシートについては、昨年のヒアリングシートですと「他アプリやサイトを経由した情報収集の状況」については、事業者ごとに会社が異なったりしており、分かりにくいと感じていますので、見直しをお願いしたいです。

---

それでは、幾つか御質問が、木村さん、あるいは森さんからも出ていたかと思いますので、この点、小竹さんから、もしお答えできるのであれば、手短にお願いできればと思います。いかがでしょうか。

【小竹氏】　まず、生貝さんから言われたのは、プライバシーポリシーの日本対象になります。

森先生からいただいた非ログイン時のお話と、アカウントを持っていない場合については、今回、同じものと捉えて、基本的には、ログインしているか、それともそれ以外の場合かで記載があるかというようなところで推測させていただいております。

もう１つあった、「いいね」ボタン、LINEさんのWrikeツールに関しての記載については、今回、載せてはいないですけれども、例えば、Metaの場合ですと、ここのパートナー、ベンダー、その他の情報からみたいなところを開くと、その中に他社のサイトに載っていたボタンを押した経由で、こういう情報を取得しますみたいな書き方は、一応個別には書かれている情報にはなっておりまして、その中に、非ログイン時でも、アカウントがない場合でも、何かしら情報は取るところがあり、LINE、Yahoo！につきましても、個別の情報のここの中で、パートナーの第三者から得る情報の中には、他社に設置されたプラグイン

等を使った場合には、こういう情報を取得しますとは個別に書かれております。そこがログイン時と非ログイン時で分かれて書かれていたわけではないですけれども、押せば、こういう情報は取得しますよというところは書かれていた結果になっております。

【山本主査】　ありがとうございます。また今後も恐らくいろいろと、この点は議論があると思いますので、また引き続きどうぞよろしくお願いいたします。

それでは、予定の時間になっておりますので、今日の議論はここまでにさせていただければと思います。

事務局に確認ですけれども、このヒアリングの新しい観点等については、また別途、議論する機会はありますよね。

【川野利用環境課課長補佐】　はい。今回、事務局資料で言いますと、５ページ目にお示しさせていただいていたかと思いますが、本日いただいた御意見を基に、実際に３ページに昨年のヒアリングシートを記載しておりますけれども、実際に何を事業者にお伺いするのかを確認させていただいた上で、これを御議論いただく場を設けられればと考えております。

【山本主査】　はい、承知しました。それでは、まだこれが最後ではないということですので、また引き続き御意見等をいただければと思います。

それでは、次回会合等々につきまして、連絡事項ですけれども、事務局からお願いいたします。

【川野利用環境課課長補佐】　次回の会合につきましては、別途事務局から御案内をいたします。

事務局からは以上になります。ありがとうございます。

【山本主査】　ありがとうございます。

それでは、多少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。以上で利用者情報に関するワーキンググループ第３回会合を終了とさせていただきます。本日も、皆様、お忙しい中、御出席いただきまして、ありがとうございます。