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（第２回）

令和３年４月６日

【宍戸主査】　皆様、おはようございます。定刻となりましたので、ただいまからプラットフォームサービスに関する研究会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第２回会合を開催いたします。

本日も皆様お忙しいところお集まりいただきありがとうございます。

本日の会議につきましても、新型コロナウイルス感染拡大防止のため、構成員及び傍聴はウェブ会議システムにて実施させていただいております。

まず、事務局よりウェブ開催に関する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。

【丸山消費者行政第二課課長補佐】　総務省消費者行政第二課、丸山でございます。

ウェブ開催に関する注意事項を幾つか御案内させていただきます。

まず、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のみでの傍聴とさせていただいております。このため構成員の方々につきましては、御発言に当たってはお名前を必ず冒頭に言及いただきますようお願いいたします。

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、映像もオフにしていただきますようお願いいたします。ほか、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、主査から発言者を指名いただく方式で進めさせていただきます。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、いずれもオフに戻してください。

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。

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

本日の資料は、本体資料が資料１から資料３まで、参考資料が１から２までとなります。このうち資料３－１のApple Imc.の資料は全て構成員限りの資料となっております。構成員の皆様には別途、構成員限り資料を御用意しております。

注意事項は以上となります。

なお、本日、佐藤構成員は御欠席、小林構成員は11時までの御参加となります。

それでは、これ以降の議事進行は宍戸主査にお願いしたいと存じます。宍戸主査、よろしくお願いします。

【宍戸主査】　それでは、議事に入ります。本日はまず、小林構成員から資料１に基づき、「実効性のある通知・同意取得の在り方に関する実証事業の報告」について、次に、IIJ様から「ePrivacy規則閣僚理事会案について」を発表いただき、まとめて質疑応答を行います。その後で、プラットフォーム事業者２社様から、利用者情報の取扱いに関する取組について御発表いただき、その後質疑応答を行います。最後に、全体を通した意見交換を行います。本日のアジェンダはそのようなものでございます。

それではまず、小林構成員から資料１「実効性のある通知・同意取得の在り方に関する実証事業の報告」について御発表をお願いいたします。

【小林構成員】　野村総合研究所、小林でございます。私から「実効性のある通知・同意取得方法の在り方に関する実証事業の報告」をさせていただきます。

１ページ目に行きまして、本日お話しさせていただくことですけれども、通知・同意といいましたら、ここに参加されている皆様にとって見ると、もう10年以上前から同じことをやっていて、なかなか進歩が見られないところ、何度も同意・通知している、同意している内容についての形骸化とか、同意疲れといったようなものについて議論はされてきているんですけれども、実際にどうやったら効果的に利用者に届くのかというような議論がなかなかできていなかったのではないかと。されていたとしても、実証実験をやって、それについての効果を検証するというところにとどまっていたのではないかと。

そういう反省に立ちまして、今回の報告というのは、利用者の実際の行動の裏側にある考え方、さらには、その内側の、内面の心理の部分まで立ち入って、それを定量的に分析するという大変野心的な事業について実施しましたので、その御報告をさせていただきたいと思います。

２ページに背景と目的とありますとおり、これまでは、利用者の理解や安心につながらない状態が生じてしまっていたというのが問題意識とありまして、右側が本事業を通じて目指す姿、はっきり言えば10年以上前からこういったところを目指そうという議論があったわけですが、なかなかここまで到達しなかった。ここに例があります階層的アプローチというもの、工夫例がありますけれども、これも、こういったアプローチについては実は

もう10年ぐらい前からもあったわけですが、これがどうやったら実際に利用者に届くのかというところまでは検証できていなかったのではないかというのが問題意識の出発点になります。これをどうしたらうまくいくのかというところまで、今回の実証では一定の解をお示しできると思っております。

アプローチの方法は２つございまして、まず、２つというか順番でシリアルに２つありまして、第一段階としましては、通知・同意取得に対する考え方、これを、利用者をこれまでは全員同じようなプロファイルで捉えたところはあると思うんです。これまで、例えばリテラシーが高い人とか、それからリテラシーがそれほどない、不安な人とかという、ぼやっとした利用者のプロファイルがあったとしても、その方たちがどういうふうにそれぞれ通知・同意に反応されるのか、そういうのをどうお考えになるのかというところまでは踏み入っていなかった。これをまず踏み込むために利用者をしっかり分類しようと。画一的に捉えるんじゃなくて、ちゃんと利用者というのはどういう人たちが、どういうタイプの方たちがしっかりいるのかというのを分析するというのがまず第一段階。

それを用いて、右側ですね、その利用者のプロファイルに沿って、どんな、工夫と言いますけれども、工夫だったり、手法という言い方をしますが、例えば階層的な通知であるとか、個別同意であるとか、こういったものについて、幾つか既に取り組まれているものを改めて整理し直して、それを実際に分類した利用者に当てはめてみて、実際に、モックアップというのは、これはアプリですけれども、これをつくってみて、簡易なアプリをつくってみて、それを用いて検証するということをやりました。

これを、この後御説明する順番でいうと、まず、最初に今４ページを表示していますけれども、②番の、検証対象手法、順番が前後しますけど、まず、世の中でどんなもの、どんな工夫があるのかというところをお話しして、その後に利用者の分類、ある意味、ここが今回の実証の肝ではあるんですけれども、この利用者の分類について御説明する。最後に、実際に利用者の分類ごとに工夫を当てはめるとどんないいことがあるのか、どんなことが分かったのかという、今後どうしたらいいのかというところまで最後にお話しできればと思います。この絵で言いますと、②①③の順番でこの後の御説明を進めさせていただきたいと思っております。

次に、ここの場にもお集まりいただいている森先生、山本先生にも御参加いただいた協議会を構成して、実証事業を進めました。１点、多分この界隈ではあまりなじみがない先生、この一番上に名前が書いてありますが、安藤昌也先生という千葉工大の先生ですが、

ユーザーエクスペリエンスの専門家で、プロジェクト全体を監修いただきました。この先生は、SEPIA法という製品に対する考え方に基づいてユーザーを分類して、セグメントごとに製品評価を行うというモデルを開発された先生です。

多数の企業に対して、それぞれユーザーエクスペリエンスについて、消費者の心理に深く入り込んで、どれが効果的なのかといったことまで、アドバイスされている先生でございまして、今回それを、この安藤先生にプロジェクト全体の監修もお願いして進めてまいりました。

それと併せて、ここに名前を連ねていただいている構成員の先生、それからオブザーバーの皆さんと一緒に議論を重ねて進めてまいりました。本日、私、小林から御紹介させていただいておりますが、この事業は、野村総合研究所、南島と星という者がすごくコミットして進めてきたものでして、もし、込み入ったお話であるとか、もっと深く知りたいということが今後出てくると思いますので、また回を改めて御紹介できたらとは思っているところでございます。

前置きが長くなりましたが、ここから実施結果について進んでまいりたいと思います。最初、利用者の通知・同意取得の諸外国のルールとか事例調査、工夫を、どんなことを諸外国でされているのかというお話です。この部分については、プラットフォームサービスに関する研究会で12月に弊社の南島から発表しているので、プラットフォームサービスに関する研究会の構成員を務められている先生には復習のようなお話になるかとは思います。

今７ページ目に表示している通知・同意の工夫としては、５つぐらい、世の中のものを集約するとあるかと思っていまして、階層的なアプローチ、ダッシュボード、ジャストイン通知、アイコン、それからモバイル・スマートデバイスの機能性、ごめんなさい、こちらはイギリスの保護機関で共有している工夫でした。この後段、いろいろ御紹介した後、最後にまとめて御紹介します。

この階層的アプローチについて、例えばイギリスのICO、日本でいう個人情報保護委員会が提示している、こんな工夫があるよという階層的アプローチについては、見出しがあって、それをクリックすると、ちょっとした概要が表示されている。さらにもっと知りたい方ということになると、右側の全文が出てくるという３段階で表示されている。これは３段階ですけど、これは２段階にしたり、いろいろ工夫はあると思うんですけども、このようにすることで、一覧性だったり、あと、概要をささっと理解できるような仕組みがあるというのがこの階層的アプローチです。

ダッシュボードにつきましては、もうこれは言わずもがな、オブザーバーで参加されているドコモさんの事例が有名ですけれども、ユーザーが自分でプレファレンスを細かく設定できるサイトというのを提供して、ここで設定がいろいろできると。撤回であるとか、そういったものをここで調整できるというもの。

さらにCCPA、これはカリフォルニア州で先行して導入されているプライバシー保護のルールでございますけれども、こちらでは、上に赤い丸が４種類あると思いますけれども、従来で言う、Terms of Serviceが利用規約、その隣がPrivacy Policyとなっておりますが、これとは別に、Notice of Collectionというのと、Do Not Sell My Infoという、別出しして、要は別の、中身は一緒ですが、Privacy Policyの中身では、たがうものではないんですけれども、Privacy Policyの中から重要なものを別のリンクとして表示することを州法で義務づけたという、そういう事例でございまして。カリフォルニア州でビジネス行っている事業者はこのような形で、これは一例ですけれども、Privacy Policyとは別に通知事項を求められているという、そういうものです。これもある意味、階層表示の一つかというふうに分類できるとは思っています。

今申し上げたところを、改めて11ページ、５つに工夫の種類を分類しておりますが、この黄色いハッチのかかっているところ、ここを今回の実証の対象とさせていただいております。具体的には、階層的な通知、レイヤードアプローチと言われるものですけれども、これは見出しと詳細という話と、それからカリフォルニア州のCCPAであったように、重要事項と全文、全文とそのうちの概要という、そういうパターンのもの、それから３番目、個別に同意を求めるという仕組み、最後にプライバシー設定、これはダッシュボードのイメージでございますけども、そういったものを、都合、階層的なアプローチは２種類、個別同意、プライバシー設定のこの４種類、都合４種について、この後検討したというものです。１回挟んでまたここに戻ってくると思いますので、覚えておいてください。

次にまいります。冒頭に申し上げたとおり、本調査研究で最も重要なものが、この利用者の分類でございます。13ページ、さらっとまとめておりますが、イメージとして、どんなことをやったのかというと、それぞれ利用者の方を、きちんと属性、考え方というのが分散するように、適正に分散するように、いろいろ考え方の違う人が合うという、違う人はちゃんと抽出できるような形で選んだ10人の方に参加いただいて、それぞれインタビューを行いました。製品サービスを利用する際の、表示される通知・同意取得に対する思っていること、不安なこと、考えていることをいろいろとインタビューで探っていくわけで

すが、このときに、このインタビューが従来のものと違うのは、全て言葉を逐次、逐語録で起こしていって、この逐語録を大体２万字ぐらい、Ａ４で30ページぐらいになるものになるんですが、それを一人一人起こしていって、このピンクで書いてあったり、ブルーでハッチがかかったりしているところがありますけれども、言葉の中から、それぞれ概念というものを抽出します。

概念というのは何ですかというのは分かりづらいと思うので、もう少し言いますと、例えば自分が、自分の情報が流出して悪用されるかもしれない、だから怖いといった話とか、詐欺被害に遭うんではないかというようなことを、例えば利用者の方がばらばら言うわけですが、それをひとまとめに類似するものを集めてきて、それは、企業へ情報提供することに対するリスク、またはこれを不安というような形で概念化するという、そんな作業を丁寧にやっていきます。

この丁寧にやっていく概念というのをそれぞれ集めて、たくさん抽出するわけですけれども、最初に34の概念というのを抽出して、概念を抽出した後に、それぞれの相関関係というのを見ていく。相関関係を見ていってそれをマッピングするということもやります。それをやっていったときに、因子分析というものを背後で行って、因子分析は何かというと、言葉とか表面からは現れてこない、その背後に通底する考え方、観念というものを分析する手法ですけれども、因子分析を通じて、３つの因子に今回の調査で分析結果がまとめられました。

大きな話でいうと、この３つが上からありますが、企業の情報利用に対する抵抗感、それからネットサービスの利用における自己効力感、さらには面倒と感じる気質と。今ぱっと聞いて、すぐに頭に入ることはなかなか難しいのかもしれないんですが、この３種類に大きく利用者が感じている通知・同意を行う際に感じているもの、そういう考え方というものが分類できたと。それぞれ感じている内容をここに示している、この３つの因子から語るというのが今回の調査研究の醍醐味でございまして、割愛しますけども、背後にはこんな分析しましたというのが15ページ、今後、この後説明するグラフがたくさん出てきます。

グラフがたくさん出てきますけれども、それについては、基本はこの上側の表、企業の情報利用に対する抵抗感というのが因子１、それに対してネットサービス利用における自己効力感、自己効力感というのは、自分でサービスを利用できるかどうかについて自信があるかという意味で、言い換えれば、リテラシーが高いか低いか、それぐらい単純で思っ

てください。面倒と感じる気質というのは、ここに書いてあるとおり、先延ばししたり怠慢・依存というようなところが現れてきた気質です。

基本は上のこの４マスで考えて、そこに下の２つの面倒くさがりか、まめかというところを掛け合わせると８つのセルになるというのがありますので、基本はこの４つのセルで見ながら、さらに細かく見るときにはこの８つのセルで、そんな形でこの後のグラフを見ていただければと思います。

ざっといくと、お時間があまりないので、ざっといっちゃいますが、自己効力感が高くて、さらに抵抗感が強い人というのは、このアンケートの中であるとおり、新しい商品やサービスを利用する際に、とてもビビットに反応する人たちだということが分かります。意欲的ですね。先進的なサービスに意欲的な方というのは、実は自己効力感があって、リテラシーが高くて、だけど企業の情報利用に対しては傾向感を持っている、問題意識を持っている人たち、こういう人たちが実は新しいサービスに対して意欲的ですよということ。これは隣の８セグメントで見ても、同じような傾向が見えます。

次の18ページに行きますと、今度は、サービスの利用を心配でやめるという場合があると思うんですが、それの場合には、リテラシーというものよりもこの抵抗感というのが当然効いてきて、抵抗感が強い人については、サービスをやめることがあるというのが見てとれる。これは次のスライド、19ページでもありますけれども、不要な情報を提供する、いろんな情報をいろいろ取られ過ぎているんじゃないかという心配は皆さん持っているんですけども、これについても抵抗感がある方というのは、セグメント１、セグメント３と書いてあるところ、ピンクのところが一番分かりやすいんですけれども、このように抵抗感がすごくはっきり出ているという。セグメントごとに情報利用に対して、どんな感情を抱いているのかというのが分かりやすく見てとれるかと思います。

今のをまとめると20ページで、ここはこのとおりですが、自己効力感が高い人というのは、先進ネットサービスをどんどん使うのに意欲的ですと言いながら、その人たちというのは、サービスが危ないと思ったら、すぐそれを取り下げるという人たちですよということなので、逆に言うと、今、右側の赤枠で囲っているセグメント１というのは、ここをうまく捉えると、先進的なサービスの利用者、アーリーアダプター、イノベーターという方たちに訴求することにつながるのではないかというのはここのテイクアウェイでございます。

そのままばんばん行ってしまいますが、実施結果、ここから先は何の話をするかという

と、そういうふうに分類をしました、その分類をしましたという人たちに対して、どういう通知・同意の工夫が訴求するのかというのを検証したのが、この22ページ以降のお話になります。冒頭に申し上げたとおり４種類取り上げました。①のところは階層的な通知ですけれども、ここは見出しと詳細という、見直しだけの場合と、見出しがまず表示されて、その後にプラスの文字を押すと詳細が出てくる。それから、右側に移って、重要事項と全文というのは、CCPAにあったように、概要がまずあって、それとは別に全文が表示されるというもの。

②番に行くと、今度は個別同意ということで、ここでは第三者提供について個別に選定して、同意することができるという、そんな場面を用いて検証しています。その右側に来て、③番、プライバシー設定、ここはダッシュボードのイメージですけれども、それぞれ設定できるようにしている。

リアリティーをこの後、被験者に対して持たせるために、何となく分かると思うんですけど、これはニュースアプリの画面ですが、どこかのニュースアプリの模した感じになっていますけれども、これと、あとメッセージングアプリという２つのアプリに対して、それぞれ、先ほどの示した８メッシュの分類からそれぞれ４人ずつ計32人にインタビューを行って、これを分析して、さらにその分析した結果に基づいて、1,000人に対してアンケートを行って、回答を得ました。

結果は、時間がないのでここはじっくり説明したいところではあるんですが、残念ながら、飛ばすのはもったいないんですが、後で見ていただくということにしていただいて、この27ページまで行っていただきます。27ページ、ここで、ぱっと見てみると、ここで結果がずっとありまして、階層的な通知、それから重要事項と全文、見出しと詳細、重要事項と全文、これはいずれも２割以上が、こうやって表示されると現状よりしっかり読むと回答されたということです。

実際には、この中で自己効力感が高かったり、抵抗感が強い利用者、４マスでいうところの右上にあるメッシュの方たちというのは、さらにここの傾向が強くなっているということで、こういった取組がすごく訴求するんだというのがよく分かります。

また、下に移って個別同意については、またかなりプライバシー設定、こちらはどちらも６割以上が利用したいと言っていて、ここについては、実はメッシュの差はそれほどなくて、全体的に評判がいいという、そういうことがよく分かりました。

次のスライド、こちらが28ページになりますけども、絵で赤枠で囲っているところがリ

テラシーが高くて抵抗感が強い人、こちらについては、どの取組についても好意的な反応を示されたということで、セグメント４というのはブルーで表示されていますけども、ここは自己効力感が低い、リテラシーが低くて抵抗感もないという、とにかくサービスが使えればいいですよという人たちについては、それほど訴求はしていないんですが、ただ数字を見ていただくと分かるとおり、基本的には、こういう取組に対しては、例えばプライバシー設定についても53％が利用したいとか、そういうことを言っていますので、全く効果がないというものではないということです。

29ページについては、赤字で、点数が低いほうがいいという意味ですけれども、好意的という意味ですが、赤枠でハッチでかけているところが、好意的で示されたという話なので、個別同意、プライバシー設定について見ると、全体的に好意的な結果が出ているという、そういうデータになります。

最後30ページになりますが、これまで通知したり同意したりすることについて、いろんな工夫がされていました、というのがあるんですが、実態的にそれは全ての利用者を画一的にとらまえていた。ですが、今回の調査研究では、その利用者の分類をしっかり最初にプロファイルして、そこに対してどういう工夫が訴求するのか、こういう人たちに工夫すると、どんないいことがあるのかというのを検証したものになります。

特にこれは今、最後30ページにまとめていますが、これを全部紹介するというよりは、後で読んでいただければと思うんですけど、特にこの４番、この階層的な通知、個別同意、プライバシー設定というものについては、いずれも理解や安心に資するという話、特に自己効力感が高く、抵抗感が強い利用者、リテラシーが高くて、でも企業の利用については反発というか抵抗がある方というのは、いずれの取組も好意的な反応を示されていて、かつ、こういった方たちが実はアーリーアダプターですよというのが２番に書いてあるものでございます。

最後に５番のところ、こうした利用者の理解や安心に資する通知・同意取得の工夫の普及が求められますよということで、それぞれ「階層的な通知」「個別同意」「プライバシー設定」、効く層が違うんですよと。それぞれ訴求できる利用者というのも、実はプロファイルが大分深まってきましたということがありますので、そういったものもぜひ考慮に入れながら、行政でもやるべきことを示していく、また事業者は、自社のユーザーの特性に応じて、それぞれプライバシーに配慮した設定なり、そういうツールを提供していくことが有効だと思っておりまして、ますますさらなるこういった工夫の普及が意義あるもの

として取り組まれることが、今回の実証を通じて、皆さんにお伝えしたいメッセージでございます。オーバーしましたが、以上になります。

【宍戸主査】　小林さん、ありがとうございました。

続きまして、資料２、ePrivacy規則閣僚理事会案について、インターネットイニシアティブの鎌田様に御発表をお願いいたします。

【鎌田氏】　IIJの鎌田でございます。お手元の資料は、EUのクッキー等規制のこれまでの経緯と、最新のePrivacy規則案の概要を説明したものです。

２ページをお願いします。本日のサマリーです。２月10日に、EU加盟国が閣僚理事会でePrivacy規則案に合意して、正式に欧州議会との間で立法手続が開始されました。２番目、ePrivacy規則案では、規制対象となる電子通信サービスとして新たにインターネット接続の上で提供されるウェブメールやメッセンジャーサービスなどのOTTサービスが加わりました。３番目、ePrivacy規則案では、これまで域外適用の条文がなかったんですけれども、GDPRと同様に域外適用の条文が明文化されました。４番目、ePrivacy規則案では、同意を取得せずにクッキー等を設定できる例外的な場合が幾つか新たに明文化されました。最後５番目、これまでの各国当局のガイドラインや、欧州司法裁判所のケース・ローで次第に形成されてきたクッキー設定に関する同意取得方法とか、署名方法に関する重要なルールが規則の中で明文化されました。これらのポイントについて御説明します。

４ページをお願いします。最初に、これまでのEUクッキー規制の経緯を簡単に振り返らせていただきます。2002年にePrivacy規則案が制定されました。2009年、下ですけども、ePrivacy指令が改正されて……。

（一時中断）

【鎌田氏】　暗黙の同意などが駄目になりましたと、2018年ですね。今回、ePrivacy指令は、これまでは加盟国による国内法化を経て施行するという仕組みだったんですが、電子プライバシーについて、全てのEU加盟国、EU市民に対して同等の保護を及ぼすとともに、シングルマーケットにおいて平等な競争環境を確保する必要から、EUの全加盟国に適用される規則という法形式で、規制が必要であるという議論が高まってePrivacy規則が制定されるという経緯になったわけです。

９ページをお願いします。最新のePrivacy規則案のうち、クッキー規制に関する部分を説明します。まず１条には、この規則の保護法益が示されています。注目すべきことが２点ありまして、第一に、個人だけでなく欧州基本権憲章７条に書いてある通信の秘密、特

に法人の通信の秘密も保護法益となっています。第二に、電子通信サービスの提供に伴う情報処理が原則として規制されるんですけども、それだけではなくて、利用者端末装置の情報というのが保護の対象になっている、規制の対象になっているということです。

プライバシーや、通信の秘密という基本権を保護するためには、電子通信サービスの提供と関係するかどうかを問わず、利用者端末を私的領域として保護する必要があるというのが、ePrivacy指令以来のEUとしての基本的な考え方であろうと思われます。

12ページをお願いします。ePrivacy規則の適用対象の一つである電子通信サービスの範囲が、去年の12月に完全施行されたEU電子通信コードで拡大されました。このコードによって、新たにウェブメールとかメッセンジャーなどインターネット接続上で提供される、OTTサービスと呼ばれるものが電子通信サービスに加えられました。赤字の部分です。

13ページをお願いします。ePrivacy規則では、新たに従来のePrivacy指令では見られなかった域外適用の条項が加えられました。GDPRに並ぶものです。

20ページをお願いします。クッキー規制は、８条にずらっと書かれております。我々がクッキー規制と通称しているのは、条文に従って正確に言いますと、端末装置の処理・蓄積機能の利用、及び端末装置からの情報の取得ということになります。これらの行為は、条文によりますと、一般的に禁止される、例外的な条件が成立する場合に限って許されるという規制の構造になっています。最初の３つの例外条件は、今のePrivacy指令とほぼ同じです。このほかに新たに加えられたものとして、一定のオーディエンス測定、サービス端末のセキュリティー維持の目的とするもの、それからセキュリティーアップデートを目的とするものなどが例外的にクッキー設定が許される場合として、ePrivacy規則で新たに明文化されました。

24ページをお願いします。これは分析ですけれども、このePrivacy規則案に示されたクッキー規制について重要なポイントと私が考えますものをお話しします。まず、閲覧履歴等の行動分析によるターゲティング広告は、これまでどおり利用者の同意が必要だということになります。この点は変わりません。また、ウェブアクセス解析については、これまで非常に不明確なところがあったんですけれども、自社利用のための純粋なオーディエンス分析については、一部同意取得が不要とされました。これが明文化されました。ただ、広告と連動するようなものについては、従来どおり同意が必要です。

また、クッキー類似技術、例えばデバイス・フィンガープリンティングであるとか、HTML５のローカルストレージであるとか、そういった類似技術については、従来どおりク

ッキー規制が適用されます。

一つ注目すべきことは、端末装置が有する処理機能の利用というのが新たに規制範囲に加えられたことです。ここに新旧条文の比較が書いてありますが、処理機能の利用が新たに規制範囲に加えられましたと。恐らくスマートフォンなどの端末の処理機能が高度化したことに対応したものと思われます。これによって今グーグル社が、ポストクッキー時代の広告技術として、開発を進めていらっしゃいますプライバシーサンドボックスのように、サーバーとの間では読み書きを伴わないけれども、端末装置におけるAI処理を利用したターゲティング広告についても、ePrivacy規則の規制対象となる可能性が出てまいりました。

また、処理機能を規制対象とすることによってIoT機器であるとか、コネクテッドカーなどを対象とする、蓄積を伴わない遠隔のリアルタイム処理も規制対象となる可能性が出てまいりました。

26ページをお願いします。この先は同意有効要件、同意取得方法、同意証明方法に関する、新たに定められた重要なルールに関する説明です。まず、同意有効要件は、GDPRの同意の定義に従うとされ、従来どおりです。

27ページをお願いします。クッキー設定についての同意取得は、第三者に代行させることができるということが明文化されました。広告代理店がサードパーティ・クッキーやSDKを利用する場合、これらの広告代理店はユーザーと直接のインターフェースを持っていません。したがって、ユーザーインターフェースを持っているウェブサイトやアプリの運営者が同意を代行取得するというのは、これまで各国のガイドラインで推奨されてきた実務のやり方ですけども、こういう今確立している実務が規則の中で追認されたということになります。

28ページをお願いします。ブラウザ設定による同意が有効とされました。

29ページをお願いします。現在、市場に出回っているブラウザのクッキー設定は、GDPRが求めるような目的ごとの粒度で、クッキーの同意拒否をコントロールするというふうな設定にはなっていません。大ざっぱに拒否する、設定する、サードパーティーを断るみたいな設定しかできなくなっていて、したがって、ブラウザ設定による同意が有効というふうに規則で書かれても、実際にブラウザ設定を有効な同意と認めるような規定が意味を持つためには、さらに実装を改善して粒度を高める、目的ごとの同意をきちんと設定できるようなブラウザが必要になると思われます。

30ページをお願いします。次のページです。次に、オンライン識別子による同意取得証

明ということですけれども、本人を自然人として特定できない場合の同意証明方法として、オンライン識別子によることが認められることになりました。明文で認められました。クッキーは、ブラウザなどの端末装置を唯一識別、ユニークアイデンティフィケーションすることはできるんですが、そのブラウザを利用する自然人を氏名その他の社会的アイデンティティーで識別することまではできません。こういった場合でも、同意の対象となったブラウザを唯一識別することができる識別子を示せれば、それによって同意を証明することができるということが明文で規定されました。これも現在、業界で行われている実務を追認するものです。

31ページをお願いします。全く新たな規制として、クッキー同意について、12か月を超えない期間ごとに同意撤回権を通知することが義務づけられることになりました。

32ページをお願いします。ここは従来から、非常に議論があったところですけども、クッキー設定の同意を無料オンラインサービスの提供の条件とすることが一定の場合に認められることになります。例えば広告目的のクッキーを設定することに同意する代わりに、このニュースサイトをただで見ていいよというような、そういう感じですね。ただ、その条件として、同一のサービス提供者による同等のサービスが選択肢としてあって、その選択肢においては同意をしなくていいというような選択肢がなければならないということが条件になりました。こういう選択肢として提供されるサービスを有料サービスとすることができるかどうかについては、この明文では規定されていません。

既にePrivacy指令時代に、EUの加盟国の一部では、同意を必要としない有料サービスを有効な選択肢として認めた当局の行政実例は存在します。この点については、いろいろと考え方が違う欧州議員さんもたくさんいらっしゃるので、激しい議論になるのではないかと思います。

33ページをお願いします。これが最後のポイントで、GDPRと同様に、ePrivacy規則違反に関して是正を求めたり、あるいは、損害賠償を求めたりすることについて私的訴権が規定されました。以上、ePrivacy規則閣僚理事会案の概要を説明申し上げました。ありがとうございました。

【宍戸主査】　ありがとうございました。それでは、実はあまり時間がないのですが、小林構成員及びIIJ様の御発表について、質問、コメントがあれば若干の時間で質疑をしたいと思います。今、太田構成員とそれから古谷構成員からそれぞれ挙がっていますので、まず、それをお願いします。まず太田構成員、お願いします。

【太田構成員】　ありがとうございます。まず、小林さんに質問ですけれども、先ほどセグメントごと、８メッシュで示されていたと思うんですが、そのセグメントごとの人数の比率、要するに世の中にどのセグメントが何人ぐらい、何％ぐらいいるのかというのは、どれくらいか教えてほしいですというのが１点。

もう１点が、先ほど個別同意やプライバシー設定というのは60％以上が利用したいという意向を示していたというお話ですけれども、こちらは、例えば最初、同意疲れとかそういったお話もありましたけれども、面倒くさいというよりも、設定ができたほうがいいというのが強いという意味で捉えてよろしいんでしょうか。よろしくお願いします。

【小林構成員】　ありがとうございます。画面表示が間に合わないのでお手元で見ていただきたいのですが、16ページに８メッシュになるというのはお示ししたんですが、今回の事業の目的というのは、利用者のそれぞれの特性を分類するということで、実際にこの方たちが世の中でどれぐらいの割合で分布しているのかというのについては対象ではないんです。

そういう意味でいうと、お答えにはできないのですが、今回は、利用者を分析、それぞれの特性というのを、世の中の人にはこういうタイプの人がいるというのを分類して、それを当てはめたという、物差しをつくったというものにとどまっていて、そこの中にどれぐらいの人が、それぞれこの８メッシュに分布しているかというのはまた別の議論だと思っていまして、ここは機会があれば、調べれば調べることはできるとは思うのですが、今回については、そこまではスコープには入っていなかったというお話で御理解ください。

それから、個別同意については、スライドでいうと28ページ、これだと出ないですね。御質問は、まめかどうかということについては、今日のスライドでは、まめか、それか面倒かという気質については御提示できていないのですけれども、それほどの、ここについての顕著な差はなかったと理解しております。もし、一緒に入っている南島で答えられるようであれば、そこの太田様の回答についてお答えできますか。

【南島氏】　補足させていただきます。本会の資料においては、自己効力感と抵抗感によって、受け止め方が大きく変わるということのみを抽出してお伝えをしておりまして、面倒と感じる気質の強弱によって、確かに微妙にその反応が異なることは確認しておりますが、先に挙げた２つの軸ほどの差は見られなかったと考えております。

面白いのは、例えば自己効力感が高くて、抵抗感が強いという方たちですけど、この中でも特に面倒と感じる気質が強い人のほうが、個別同意やプライバシー設定に対して好意

的な受け止め方をしています。よくイメージされるのは、まめな人のほうがそういうのはよいのではないの、とここにいらっしゃる方も思うと思うんですけど、そうではなくて、ここに関しては、面倒と感じる気質の人のほうがよいと思うということです。

他方で、自己効力感が低くて抵抗感が強い人だと、今度はまめな人のほうが、個別同意やプライバシー設定に対して好意的に反応を示しています。細かく見ていくとセグメント別の受け止め方や反応が違う面白さがございますが、大きくは影響しないということで、御報告は割愛しております。

【太田構成員】　ありがとうございました。

【宍戸主査】　よろしいですか。それでは、太田構成員、それでよろしいですか。

【太田構成員】　大丈夫です。ありがとうございます。

【宍戸主査】　ありがとうございます。次に古谷構成員、お願いします。

【古谷構成員】　ありがとうございます。古谷です。利用者にとって分かりやすいとか安心できる通知・同意の取得というのは前から求めていたことですけれども、今回の調査でプロファイリングして、実際により分かりやすく安心できるものにということ自体は大変すばらしいと思って、一歩も二歩も進めていけたのではないかと思っております。

その上でコメントといいますか、感想ですけれども、まず、利用者の考え方によって、確かにその行動が左右されるということはあるんですけれども、実は考え方だけではなくて、そのときの状況であるとか、サービスであるとか、相手によるとか、そういったこともすごく影響してくるので、考え方だけで何かを決めるというのは危ないかという感じは実はしないでもないというのが１つ目のコメントです。

２点目ですけれども、プロファイリングして、事業者側が何かをするといったときに、何が効果的なやり方かというときに、その一つのやり方が効果的だというふうにしてしまうのか、逆に、利用者側からすると、いろんな利用者がいるわけだから、実は多様な方法を選択できるということが、多様な利用者にとって、分かりやすく安心できるものになるんだと思うんですが、そういった多様な方法を選択するということは考えられていたのかどうかというのを教えていただきたいと思いました。

【小林構成員】　ありがとうございます。野村総研、小林でございます。古谷構成員のおっしゃるとおりで、１点目はよろしいですね、そのとおりという話で。２点目の、多様な方法をそれぞれ組み合わせて利用者に提供するというのは当然そうあるべきだと思っておりまして、これはどれか一つの方法に依拠するというよりは、組合せ、恐らく今日、今

回提示した４つの仕組み、方法は、工夫ですね、いずれも効果的であったと。自分のところのサービスの特性、そのユーザーの特性に応じて、その強弱というものを考えてみたらどうかと。

これまではどちらかというのは全方位外交でやられていた、行政も、これはいいですよというのをおっしゃっていたわけですが、自分のところのユーザーのプロファイルに応じて、それぞれ強弱をつけていくということを事業者も考えられるようになってくる。その一つの材料として使ってもらえればいいのかとは思います。

【古谷構成員】　ありがとうございます。

【宍戸主査】　ありがとうございます。それでは次に、森先生、お願いします。

【森構成員】　森です。御説明ありがとうございました。ePrivacy規則の御説明、鎌田さんにお伺いしたいんですけれども、大変分かりやすく御説明いただいてありがとうございました。

一般的に情報の取得を禁止して、一定の場合に許容するということだったと思いますけれども、20ページが分かりやすくおまとめいただいていたと思うんですが、セキュリティーが理由になっていますけれども、このセキュリティーについて、セキュリティーの目的であれば、端末からも情報の取得が許されるということですけども、このセキュリティー維持というところに、５行目ですね、オンラインサービス又は端末装置のセキュリティー維持のために必要な場合、とありますけれども、もう少し何かこれについて限定があれば伺いたいと思います。よろしくお願いします。

【鎌田氏】　鎌田でございます。限定というか、セキュリティ目的のクッキー利用の一番典型的に使われていますのは、普段使っている端末と違う端末からのログインというのを検知するパターンです。クッキーというのは御承知のように端末装置を唯一識別できるので、普段使っていない例えばブラウザとか携帯からログインすると、「あれ、これクッキーが違うから違う装置でログインしているね」と。したがってこれはもしかしたら違う人が、アカウントを乗っ取っているんじゃないかという推定が働いて、「これは確かにあなたがログインしたものですか」というふうな質問のメッセージが来るみたいな使われ方が一般ですけども、そういった場合ですね。

だから、限定があるとすれば、アカウントが乗っ取られているかどうかを、きちんと検出する、みたいな場合を典型的な場合として想定しているんだろうと思います。現在の各国のガイドラインなんかでもそういう雰囲気で書いていますので、これはそういう趣旨で

つくられたんだろうと思います。

【森構成員】　ありがとうございました。よく分かりました。

【宍戸主査】　ありがとうございます。まだまだ御質問があろうかと思いますが、時間が押しておりますので、次のアジェンダに移ります。事業者ヒアリングでございます。

これの御説明につきましては、まず、最初のApple Inc.様につきましては、通訳を入れて30分以内でお願いいたします。事務局でタイムキープをしておりまして、しかるべき時間でチャット欄でApple様に合図をさせていただきます。そこでまず、Apple Inc.、ジェーン・ホバース様より御説明をお願いいたします。なお、ホバース様の御説明中、録音や撮影などは御遠慮いただければと思います。

それでは、どうぞよろしくお願いいたします。

【ホバース氏】　本日はAppleの最近のプライバシーへの取組を含め、当社のプライバシーへのアプローチについてお話しする機会をいただきありがとうございます。

現在まで15年間プライバシーに取り組んでまいりました。そういった観点から当社が今年行ったアップデートによって、ユーザーがプライバシー関連の情報を利用する方法が根本的に変化しており、新しいスタンダードを設定することができていると感じています。Appleでは、ユーザーの皆様がプライバシーを保護し、自らのデータをコントロールできるように力を注いでいます。

Appleの製品開発には４つの重要なプライバシーの原則がございます。これらは当社の行動全ての基礎となっているものでございまして、本日私がお話しすること全てにつながってまいります。

当社のプライバシーへのアプローチは、４つのプライバシーの柱で構成されております。まず、１つ目がデータの最小化です。当社は革新的なテクノロジーと技術を駆使し、当社と他社がアクセスできる個人情報を最小限に抑えています。

２つ目がデバイス上のインテリジェンス、知能であります。私たちはできるだけ多くのユーザーデータをサーバーに送信せずにデバイス上で処理することで、収集を最小限にしております。

３つ目が透明性とコントロールです。これによりユーザーは収集されるデータについて理解を深めることができ、それらデータの使用方法について自らが選択できるようになります。

そして最後にセキュリティー保護です。こちらは、プライバシーについて当社が行う活

動全ての基礎となるものです。

当社は、非常に長い間、プライバシーをAppleの製品とサービスに組み込んで設計してまいりました。私たちのお客様は、私たちの製品ではありません。そして、当然のことながらこれらの原則は私たちの製品やハードウエア、ソフトウエア、サービスなどで一体となって実現されています。

当社は新しく画期的なプライバシー機能をリリースしております。その中に含まれるものとして、位置情報がございます。iOSは他に先駆けて、ユーザーによる位置情報のコントロールを可能にし、ユーザーが許可するコントロールを一貫して拡大してまいりました。そのような形でこの分野を当社はリードしてきました。

これはiOS６で始まった進化であり、当社はiOSの位置情報を定期的に改善してまいりました。この機能ですけれども、位置情報の同意を取るということを同時に導入しております。アプリケーションの使用中にのみ位置情報をデベロッパに提供できるオプションをユーザーに提供したり、アプリケーションがバックグラウンドで位置情報にアクセスしているときに分かりやすい通知を表示したりするなど、位置情報データに関しては、リリースを重ねるごとに改善、改良され、ユーザーによるコントロールと透明性が高められてまいりました。

そして、このAppleマップによって、新しいデバイスから創出された識別子を生成し、サーバーが直接、指示を出すことができるようになっておりますので、Appleは、皆さんの位置情報、どこに行くかなどの個人的なヒストリー、履歴に関しては有しておりません。

今年、当社は新しいコントロールとして、おおよその位置情報を追加しております。この機能を使うことによって、正確な位置情報を共有することなく、今いる場所のおおよそのエリアだけをデベロッパに共有することができます。ユーザーがデベロッパにおおよその位置を提供することを選択した場合、iOSはそのユーザーの位置を含む約26平方キロメートルの範囲内の位置を解しますが、ユーザーの正確な場所は公開されません。

このおおよその位置は地元のお勧めやニュースアプリケーションに最適です。ユーザーは自分のいる都市に関連する情報を求めておりますが、役立つ結果を得るために、ここで正確な情報を共有する必要はありません。おおよその位置を利用することで、ユーザーは自分が望むデータだけを共有できる一方で、デベロッパは画期的なサービスを提供し続けることができます。

次がマイクとカメラです。アプリケーションはユーザーのマイクとカメラにアクセスし

て、様々なすばらしいことを実現することができます。そして、それらを許可なく使えるアプリケーションはありません。これまでもユーザーはアプリケーションがバックグラウンドでマイクを使っているときは、いつでも確認することができておりました。最新のOSによって、アプリケーションがデバイスのカメラまたはマイクにアクセスできるときに、ユーザーがあらゆるところで確認することができるようになりました。

アプリケーションにカメラへのアクセス権がある場合、デバイス上にグリーンのインジケーターが表示され、アプリケーションにマイクのアクセス権がある場合は、デバイス上にオレンジのインジケーターが表示されます。このインジケーターはアプリケーションがフォアグラウンドまたはバックグラウンドのどちらにあるかに関係なく表示されます。

表示されたインジケーターがどのアプリケーションのものか分からない場合は、コントロールセンターで確認することができます。さらにコントロールセンターにはアプリケーションが最近いつマイクやカメラを使用したのかが表示されます。この機能によってユーザーは安心感を得ることができます。マイクやカメラが使用されているときは常に気をつけながら、デベロッパの画期的なアプリケーションの機能を利用することができます。

当社は、ユーザーのデータがアプリケーションによってどのように利用されているのか、これについてユーザーの認知が向上するように努力してまいりました。さらに、ユーザーのデータがアプリケーション間で、広告のために利用されるその方法について、ユーザーのコントロールを強化することに力を注いでまいりました。

６月に私たちはデベロッパが自分で報告したプライバシーの取扱いについて、App Storeのアプリケーションの製品ページで分かりやすい概要を提供することを発表いたしました。12月の初めにこの情報をユーザーに公開し始めております。この新しいプライバシー情報はApp Store上の全てのアプリケーションで、デベロッパがアップデートや新しいバージョンを提出する際に要求されるものになります。

このプライバシーに関する方針の報告は、全てのデベロッパのアプリケーション提出のプロセスの一部となっております。世界中のアプリケーションデベロッパが同じ質問に回答する必要がありまして、これには当然ながらAppleも含まれています。

アプリケーションデベロッパはこのような方法で自社のラベルをAppleのデベロッパポータル経由で提供することになります。デベロッパポータルはプライバシー情報をアップロードできるシンプルなインターフェースになっておりまして、ユーザーはアプリケーションのデータの取扱いについて明確に理解することができます。そしてデベロッパはこれ

らの取扱いの変更に応じて、アップデートをすることができます。

App Storeのアプリケーションの製品ページには、そのアプリケーションが収集する可能性のあるデータの種類と、そのアプリケーションがデータを使用してユーザーをトラッキングするかどうか、または、データがユーザーに関連づけられているかどうかなどが表示されます。データの種類は３つのカテゴリーで収集されます。ユーザーのトラッキングに使用されるデータ、ユーザーに関連づけられたデータ、そしてユーザーに関連づけられないデータです。

この段階で、トラッキングとはどういう意味なのかということを御説明させていただきたいと思います。トラッキングとは、アプリケーションで収集したユーザーやデバイスに関するデータをターゲティング広告や広告効果測定を目的として、他社のアプリケーション、ウェブサイトまたはオフラインのプロパティから収集されたユーザーやデバイスに関するデータに紐付ける行為を指します。また、ユーザーやデバイスに関するデータをデータブローカーに共有することもトラッキングに該当します。

ユーザーに関連づけられたデータとは、アプリケーションのユーザーアカウント、デバイスやその他の詳細情報によって、ユーザーの個人情報にひもづけられたデータのことを指します。

また、ここではユーザーにこの関連づけられないデータというのも非常に重要であります。Appleが長年にわたり、データの最小化といったことを行ってまいりました。そこにも関連することでございます。ユーザーの個人情報に関連づけられたデータが本当に必要なのかの検討をデベロッパに実行してもらうために役立っていると考えております。

私は特にAppleのプライバシー関連のアイコンに関する取組をうれしく思っております。できるだけ簡単に情報を表示することで、ユーザーはアプリケーションをダウンロードする前に、そのアプリケーションのデータの取扱いについて、一目で確認することができます。もちろんダウンロード後も、いつでも確認することができます。

デベロッパは新しいアプリケーションを公開したり、既存のアプリケーションをアップデートしたりする際には、この新しいプライバシー情報をApp Storeに提出することが求められます。ここではデベロッパはアプリケーションやビジネスモデルを変更する必要はありません。単にアプリケーションで収集するデータ、トラッキングに使用するデータ、ユーザーに関連づけられたデータについて、ユーザーに透明性を提供するものであります。

次にアドトラッキング、追跡型広告について説明をいたします。現在では多くの注目を

集めるものでございますが、これはAppleが何年も前から取り組んできたことです。サファリはデフォルトで他社のクッキーをブロックした最初のブラウザで、これは2003年まで遡ることができます。それ以来、当社はサファリにプライバシーとセキュリティーの機能を組み込み、ユーザーが自分のデータをコントロールできるよう継続的に改善してまいりました。

2017年に、当社はインテリジェントトラッキング防止機能と呼ばれるすばらしいウェブのプライバシー機能を開発しております。サファリはユーザーがサイト間を移動するときに、データ企業がユーザーをトラッキングしないような機能を持っております。

残念ながら、ウェブがつくられた当時は誰もこのようなことを考えておりませんでした。その結果、サイトが適切に動作するのに必要なテクノロジーと、ユーザーをトラッキングするテクノロジーの違いは簡単に区別することができません。

そのような文脈を背景に、当社はこれをインテリジェントトラッキング防止機能と呼んでおります。まず、チームが高度な機械学習を活用し、どれがどのテクノロジーか、判断をいたします。次にサファリがトラッキングテクノロジーをブロックします。これはデフォルトでオンになっておりますので、ユーザーが何か設定でオンにする必要はありません。サファリはユーザーをトラッキングから保護するために、密かに働いております。

2017年にこれを導入した際、広告主の皆さんは自分たちの世界がこれで終わりだというふうにおっしゃっておりましたが、もちろんそんなことはありませんでした。引き続き、この業界は繁栄し、同時にユーザーのプライバシーも、よりよく尊重されるようになっております。

しかし、これだけにとどまらず、私たちはより多くのことを行っていきたいと考えました。最近これら全てのことをユーザーに実感し理解してもらうために、あなたのデータの１日というレポートを発表しました。このレポートの目的はユーザーをトラッキングする企業の複雑なエコシステムを明らかにすることです。

例えば、アプリケーションには、他の企業からのトラッカーが平均６個含まれております。これらの唯一の目的は、その人やその人の個人情報を収集して追跡することにあります。これらのトラッカーによって収集されたデータは、つなぎ合わされ、共有され、収集され、そして収益化されることで、この業界では年間約2,270億ドルの価値が創出されていると言われております。

データブローカーは、自分たちが直接関わりのない個人に関する個人情報を収集して売

却します。そして、最大5,000のユニークな特性を持つ人物のプロファイルを作成しています。ここに私たちがリーダーシップを示す機会があるということは明白であります。

App Storeでのプライバシー情報、2017年に公開しましたインテリジェントトラッキング防止機能やフィンガープリント対策などのサファリでの取組を基に、今年、当社はアプリのトラッキングの透明性という機能を公開しております。多くの人が皆さんにこう信じてほしいと思っている内容とは異なり、プライバシーを維持しながら広告を行うということは可能であり、それこそユーザーが望んでいることです。

企業がユーザーのデータをターゲティングや測定のためにどのように利用するのか、ユーザーのデータをデータブローカーと共有するかどうかについて、ユーザー自身が選択できるようにすべきです。Appleではプライバシーを維持した広告がどのようなものか、実証してきたと考えております。私たちは決してユーザーをトラッキングすることはいたしません。

数週間前に公開したデータアップデート以降では、広告またはデータブローカーとの共有目的で、他社の所有するアプリケーションやウェブサイトを横断して、ユーザーのデータをトラッキングする場合、デベロッパはユーザーの許可を得ることが求められます。今後のiOS14、iPadOS14、tvOS14のリリースに伴い、春先にはこの要件が幅広く義務づけられる予定であります。アプリケーションのトラッキング許可はデベロッパがIDFAを呼び出したいときにユーザーに提示されます。

デベロッパにとって、IDFAを呼び出したいかどうか、そして呼び出したい場合は、いつ呼び出したいかが重要になってきます。IDFAは、デベロッパがユーザーに広告を表示するためのユーザーコントロールツールとして、2012年に最初に導入されました。これはデベロッパがハードウエアを識別子やその他の方法を利用してユーザーのデバイスをトラッキングしており、それをユーザーがコントロールできないという懸念に応えるものでした。

当社はその後iOS10で、オペレーティングシステムをアップデートし、当時、追跡型広告を制限、と呼ばれていた機能をユーザーが有効にした場合には、ゼロの連なった文字列しかデベロッパに共有されなくなりました。

今お示ししておりますように、デベロッパはユーザーにトラッキングの許可を求める前に許可を求める理由を説明するということも選択できます。ユーザーがトラッキングを許可しなかった場合、iOSはIDFAをデベロッパに提供することはせず、その代わりユーザーの選択を送信します。

デベロッパにはユーザーの選択を尊重する責任があります。ユーザーがトラッキングを許可しなかった場合、このIDFAやハッシュ化されたeメールアドレスなどの識別子を使うことはできません。そしてまたデベロッパがファーストパーティーのデータを広告のパーソナライゼーションに使いたい場合、iOS14において、App Tracking Transparency(ATT)フレームワークを使うことなく継続的にそれを行うことができます。

これらのコントロールは、優れたプライバシー体験のための最も重要な２つの要素である透明性、そしてコントロールを促進するものであります。ユーザーはデータがどのように、誰によって収集されるのかについて知らされた上で、意思決定をすることができる、そのようにあるべきだと考えております。これはiOSにとっては自然な進化であり、先ほど御説明しましたように、長年にわたって私たちは写真、連絡先、カレンダー、位置情報など、データに対するデベロッパのアクセス権をユーザーがコントロールできるようにする許可を組み込んでまいりました。

そして、この許可を利用したいデベロッパは、iOS14で既に利用できるようになっております。今お見せしておりますのがフランスのロイターの許可の例です。当社はその時期の関連するソフトウエアリリースに応じて、春からこれらの要件の適用を開始する予定です。

ユーザーは特定のアプリケーションを個別にコントロールしたい場合、設定でそれを行うことができます。また、デベロッパからIDFAへの使用許可を求められることをブロックしたい場合、設定画面で無効化することができます。これはユーザーにとって強力なコントロールとなるだけでなく、アプリケーションごとに選択できるようにまでなっていきます。私たちはこれが正しいものと考えております。

アプリのトラッキングの透明性に関して、プライバシーサイトの機能ページに、詳細を追加しております。iOSとiPadOSのサイトにも、アプリのトラッキングの透明性に関する情報を追加しております。これらの新しい機能に関しては、プライバシーインターナショナルなどのプライバシー推進団体からすばらしいフィードバックをいただくことができております。

以上で私のプレゼンテーションとなります。御質問がございましたらお答えさせていただきます。

【宍戸主査】　御報告ありがとうございました。それでは、時間が限られていますが、こちらの構成員から質問させていただきます。ますは太田構成員、お願いいたします。

【太田構成員】　ありがとうございます。時間が限られているので、１個だけ聞かせてください。先ほどの発表の中で、IDFAは今後同意が必須となることということですけれども、それに伴って、IDFVの利用が増えてくると思っておりますと。そのIDFVについては、今のところ利用者のコントロールができない状態だと思うんですが、そちらについては、今後どのような対応を行っていくかという計画はありますか。よろしくお願いします。

【ホバース氏】　IDFAの代わりに新しい識別子として、今後作成されるもの、そういう意味でIDFVというお話をされているのですよね。

【太田構成員】　今後作成されるものと申しますか、AppleのAPIで提供されているID for Vendorの話をしております。

【ホバース氏】　ID for Vendorsというのは、デベロッパのエコシステム内におけるトラッキングを許容するものであり、こちらはファーストパーティーアドとなるので、ATTプロンプトでブロッキングされることはありません。

ID for Vendorsを使ってサードパーティーのデータを使ったり、編集したいような場合、これはプロンプトによってコントロールされることになります。このプロンプトはテクノロジーのテクニカルなコンポーネントと、それからポリシーに関わるコンポーネントがございまして、テクニカルコンポーネントに関しては、IDFAのAPIをアプリが呼び出すには、その場合、ユーザーの同意が必要になります。

ポリシーコンポーネントですけれども、こちらはアプリに対して識別子を使ったトラッキングができないということ、それからフィンガープリンティングもできないということを、アプリに対してポリシーコンポーネントが指示するような内容になっています。

【太田構成員】　ありがとうございます。

【ホバース氏】　ありがとうございます。

【宍戸主査】　太田構成員、よろしいですか。それでは高橋構成員、御質問をお願いします。

【高橋構成員】　Thank you Jane. Takahashi from NTT laboratory is speaking. I'm studying privacy technologies. My question is about data minimization and my question follows in Japanese. データ最小化について質問します。データ最小化はとても重要な考え方で、Appleがとても大きな努力をしていることをユーザーとして理解しています。しかし、この考えは利用者にとってとても分かりづらく、プラットフォーマーとしても実施するのが難しいものだと思っています。

私の質問は、その考えをプロモートするために、例えばそのサービスが完璧にできて、同時にデータを最小化するというのはどのように評価しているかということを教えてください。

【ホバース氏】　私たちはこのデータ最小化に関しては、プロダクトのデザインフェーズから取り組んでおります。法律の専門家であるとか、プライバシーエンジニアであるとか、それからデベロップメントのチームが、そのデータのフローについて議論をする際に、どれだけそのデータ収集を最小化することができるのかというのをこの段階から議論します。

そのうちの一つにデバイス上での処理というものがございます。iOSのデバイスをお使いの方であれば御理解いただけると思いますが、そのデバイス上に載っている写真というのは、かなり整理整頓された形になっております。

それから、顔認証に関してですけれども、こちらもデバイス上にテクノロジーが搭載されておりますので、これらの顔認証をしたときの情報が例えばサーバーに上がってくるというようなことはなく、純粋にそのデバイスの能力を使って、デバイス上で完結するような形になっております。

もう一つがマップの話で、先ほど説明の際にも触れさせていただいたんですけれども、Appleマップに関しては各セッションでユニークな識別子を生成しております。それを使ってサーバーと通信を行うことになりますので、その方の位置情報をこちらが収集しなければならない状況にはないわけです。

以上がデータの最小化に関わる２つの事例でございます。このような形でデバイスのパワーや知能を最大限活用することにより、収集すべきデータの量を最小化するようにしております。アプリでも同じことができます。

【高橋構成員】　ありがとうございます。今の考えはAppleが単独でデザインしていますか。それともアプリケーションプロバイダー、サードパーティーと一緒に考えているものでしょうか。

【ホバース氏】　技術自体はAppleで開発しておりまして、グローバルのデベロッパカンファレンスを行う際に、プライバシーエンジニアによるセッションを設けております。このセッションに参加していただくことによって、デベロッパは、当社が開発した関連する技術について学んでいただくことができます。

【高橋構成員】　Thank you very much Jane.

【ホバース氏】　You're welcome. Thank you.

【宍戸主査】　Thank you very much Jane. We have other questions, but we don't have enough time actually. So, we would like to ask you through the Ministry of Internal Affairs and Communications. Could you answer them as much as possible?

【ホバース氏】　Yes. We'd be happy to. If you want to inquire, please announce me. I would be happy to respond.

【宍戸主査】　Thank you very much.ということで、御質問のある方は後で事務局までメールで追加でAppleさんにお伺いできますので、よろしくお願いします。

残り時間もだんだん押しておりますけれども、続きまして、ヤフー株式会社小柳様より御説明をお願いいたします。御説明は15分以内でお願いいたします。

【小柳氏】　小柳でございます。よろしくお願いいたします。

では開始させていただきます。私はヤフー株式会社でデータプロテクションオフィサーをやっております。本日はどうぞよろしくお願いいたします。

飛ばします。まずヤフーについてでございます。当社は100以上のサービスを提供しておりまして、月間アクティブユーザー数で、お客様でありますけれども、5,000万の方々に御利用いただいているという状況でございます。そのようなヤフーとお客様との関係でございますけれども、ヤフーは非常にたくさんのお客様がいらっしゃいますので、個々のお客様をその実体のまま理解をするということができないということでございます。

ヤフーではお客様をデータで知りまして、データに基づいて、このお客様、乃至、こういったお客様はこういうことを考えているのではないかということであったり、このお客様は今こういう情報を必要としているのではないかということを推測して、よりお客様のニーズに合ったサービスを提供しようとしております。

社会が成熟してまいりまして、お客様のニーズが実に多様になっているというような現在において、いかに、個人のお客様のニーズを的確に捉えていくのかということについては、我々事業者に突きつけられた非常に困難な課題であると認識しております。だからこそ、これがお客様のサービス選択に係る競争みたいなものの主戦場になっていると認識しております。まさに我々はデータによってお客様を知るのであって、個々のお客様一人一人に寄り添った最高の提案をするために、データを使わせていただいているということでございます。

したがいまして、ヤフーを含む事業者は、お客様のプライバシーを保護することと、サ

イバーセキュリティーを高めていくことが必要になってくると認識しております。これらが担保されていなければ、お客様に御自身のデータを預けていただいたりとか、利用させていただけるというわけでもなかなかないということでございますので、これらが全ての前提と認識しております。

これを前提といたしまして、ヤフーではプライバシーを守るための３つの体制を構築しております。１つ目はCDO・DD体制というものでございまして、これはデータディレクターとDDは言うんですけれども、社内でDDと呼んでおります。この２つの設置と、データプロテクションオフィサーの設置、それからアドバイザリーボードの設置というものになります。

１つ目のCDOとデータディレクター、DDの体制ですけれども、実際のビジネスの現場において、これは短期的な利益ということを考えたときでございますけれども、そういう当然の前提がつきますけれども、お客様のプライバシーを犠牲にしてでも、例えば売上げを上げたいという誘惑みたいなものは当然あるわけでございます。ヤフーにおいては、しかしながらプライバシーが第一であるということを、これは社長の川邊も、折に触れて社内で情報発信したりとかしておるんですけれども、個々のビジネスの現場において、そういったヤフーの信頼を低下させかねないような取組が行われ得るということになった場合に、現場においてそれを是正するような役割が必要であると考えておりまして、これを担うのがDDの役割でございます。

具体的には、データの活用、具体的なデータの活用がお客様に提供できる便益と、それによってお客様に生じ得る影響のバランスが取れているのかということを含めて、データの活用の在り方について検討して、サービス内での調整を行うというものでございます。これが全社で30名程度おります。

他方で、こういった検討はそのサービス内で閉じていればいいというわけではなくて、特定のサービスにおけるデータの活用が他のサービス、乃至ヤフー全体に影響を与えるということも考慮しなければならないと考えておりましては、ヤフー全体のデータの活用について責任を負うものとして、CDOを設置しております。

次に、データプロテクションオフィサーでございますけれども、一旦そのDPOから離れまして、ヤフーのプライバシーに関するガバナンスの全体を見てみますと、ビジネスを運用する部門として当然事業部門がありまして、それと対になるような形で法務部門がございます。事業部門の中には、先ほど申し上げたDDがありまして、DDが担当領域において事

業上の必要とプライバシーへの配慮のバランスを適切に取るということについて責任を負っております。

事業部門の担当者はDDと相談をしながら、自らのサービスにおけるデータの利用等が適切にプライバシーに配慮したものになっているかということの検討を行っております。その検討をもって法務部門に相談をいたしまして、法務部門がそのデータの利活用とか、関連法令を遵守し、プライバシーへの影響を適切に配慮できているのかということをチェックします。当然それができていない場合は改善等を求めるということで、一応そのデータを使いたい事業部門と、法令であったりとか、お客様のプライバシーを守るべき法務部門が一定の緊張感の下、調整をしているということでございます。

さらに、その法務部門の中にはプライバシーPJというプロジェクトが存在しておりまして、これはエスカレーションして、法務部門から相談を上げて回答するというようなものも存在しております。このプライバシーPJには、DPOも参加しておりまして、その判断の内容であったりとか、判断の過程が適切であるのかということを監視したりとか、必要に応じて勧告をしております。

これが第１レイヤーでございまして、次に第２レイヤーとして、DDが相談を受けて、影響が大きいだろうというようなことで判断した場合等々については、CDOが主催する全社のDDが全員参加するDD会というものがございまして、CDOがそこで決裁をするということになっております。DPOは、CDOがその判断をするに当たって意見を述べ、また助言等を行っています。これの意見の中には、当然その考慮すべき事項が十分に考慮されているのかということであったりとか、また、その手続が適切に行われているのか、十分な検討がされているのかということについて意見を申し上げております。

さらにCDOまたDPOが必要と判断した場合は、社長であったりとか、ヤフーの業務執行に係る最高意思決定機関である最高経営会議に付議してその判断をすると。これに当たってDPOが必要な助言等を行うということになっております。

次に、アドバイザリーボードについてでございます。これは背景でございますけれども、いろいろデータの活用に当たって留意すべき点というのは、ここに挙げているようにいろいろあると思うんですけれども、プライバシーに関わる問題は様々な視点からその適切性を検証する必要があるだろうと考えておりまして、このアドバイザリーボードはまさにその第三者的な立場からそのチェックをしていただくということを目的に設置したものでございます。

構成員は、座長は宍戸先生にお願いしておるんですけれども、ほかに森先生もいらっしゃいますけれども、このような形でお願いさせていただいております。アドバイザリーボードで頂戴した御意見につきましては、主要なものを公開するという形で対応させていただいております。

次に、利用者情報の取扱いについてでございます。利用者情報の取扱いについては、まずお客様に分かりやすく説明するということが何より大事だと考えております。他方で、データの活用が高度化して複雑化し、また従来のようにプライバシーポリシーにおいて説明をし切るということは相当に困難になっていると認識しております。また、その事業者側でお客様ないし社会から配慮を求められているというのは個人の権利利益の侵害のおそれということだけではなくて、それを超えた不快感みたいなことであったりとか、不安感というものであろうと思っております。

したがいまして、ヤフーのプライバシーポリシーにおいては、単なるお客様との、事業者の一方的な宣言というものではなくて、契約の内容として位置づけをしているというのが一つ特色としてあるかと思っております。また、プライバシーポリシーにおいては、基本的な事柄のみを記載させていただいておりまして、その範囲で、具体的にどのようなデータの取扱いをするのかということについては、図などを用いて、分かりやすく御説明するプライバシーセンターというものを議論しております。

また、データの活用に当たってお客様のコミュニケーションで気をつけている点といたしましては、第一にはコンテキストに合ったデータの取得と利用ということでございます。お客様の予期や期待に反するようなことはできるだけしないと、できるだけというか、しないということだと考えております。したがって、お客様が予期しにくいような利用をする場合については、丁寧に事前に説明するということが必要であると考えております。

また、我々がよかれと思ってやっていることが、必ずしもお客様が求めていることとは限らないという点が重要だと思っておりまして、したがって、できるだけ多くの場面においてお客様の選択をしていただくということを重視しております。

次からはプライバシーセンターの記載の例になります。こちらは利用目的が書いてあるということでございまして、さらにパーソナルデータの利用の例がこちらでございます。具体的にどう利用するのかということについて、15項目に整理して詳細を説明させていただいております。その15項目の中の１つが広告の表示というものでございまして、どういった情報、例えばこれは検索のキーワードでございますけれども、それをどのような形で、

これは複数環境、これはプラスデバイスということでございますけれども、それを分析して興味・関心を推測して、御報告を出しているということを御説明させていただいております。そしてさらに詳細を御確認したいお客様に対してはリンクから御確認をいただけるようにしていくということでございます。そちらにはそのデータの保存期間であったり、利用しないデータの累計、オプトアウトしたい場合の具体的な実施方法等を説明しております。

15個のうちのもう一つの例として、位置情報について説明させていただいております。こちらについても同様に詳細については、御確認いただけるように御説明をさせていただいています。

こちらはプライバシーセンターではないんですけれども、第三者提供の同意をどのように取っているかということですけれども、こちらは対象になる情報と相手先等々を記載して、同意をいただいているということで、さらに設定画面のような、プライバシー設定の画面みたいなところで同意内容を確認したりとか、オプトアウトするということもできるようにしております。

これはヤフーのグループ会社との情報の連携についての設定でございますけれども、こちらも開始時にポップアップ表示して、同意を求めて、その後も多くの設定ができるように。これは個々の会社ごとにできるようにさせていただいております。

時間がないので割愛させていただきます。以上が当社のこれまでの取組の概要でございます。

次に、今後の取組でございますけれども、ヤフーにおいて特に今後取組を進めていかなければならないというものについては、様々あるという認識は十分あるんですけれども、代表的なものとしてPIAについて御説明させていただきます。PIAについては、既に試験的な導入を行っているところでございます。今後本格的な導入を進めるという段階でございます。PIAの重要なところは、サービスや機能の設計だったりとか、企画の段階からプライバシーの影響を評価して、その評価を機能改善であったりとかに生かしていくことであろうと思っております。

繰返しになってしまいますけれども、近日の社会の個人情報保護であったりとか、プライバシー保護に対する期待みたいなものは非常に高まっていると思っております。このような状況にある中で、データを利用しようとする事業者には、仕組みとしていかにこの期待に応えていくのかということが求められていると。これが重要だと認識しております。

他方で現状に目を向けますと、一つのプログラムの不具合が膨大なデータの漏えいを生じさせるということが起きたりとか、データを利用する事業者において、こういうことがあるということについて十分認識しないといけないと思っております。

また、社会からの期待に対してより敏感であって、プライバシーに対して、より適切かつ十分な配慮をする仕組みが担保されなければならないと思っておりまして、PIAを実施したいと思っております。

ヤフーにおいては、PIAという言葉を使っておりますけれども、GDPR上のDPIAのように、確実な法律への準拠というものを目的とするのではなくて、ヤフーにおいてはヤフーのサービスであったりとかシステムであったりとかは、個人情報の漏えい等を招く不具合がないのかということを十分に検証されて、本人のプライバシーへの影響が、事前に適切かつ十分に配慮をされたものとなることを担保することを目的としております。しっかり社内規定等々にも規定しながら、確実な実施を担保していきたいと思っております。

全体の詳細でございますけれども、これは詳細な内容は割愛させていただきますけれども、こういった評価を、サービスであったりとか機能の開発の初期段階で実施することによって、サービスや機能が十分プライバシーに配慮されたものとなっている体制を整えていきたいと思っているところでございます。

早口になって大変恐縮でございます。以上が御説明となります。ありがとうございました。

【宍戸主査】　それでは、ただいまの御説明について質問やコメントがあれば承りたいと思います。まず寺田さん、お願いいたします。

【寺田構成員】　お願いします。JIPDECの寺田です。ヤフーさん、データセンターなど非常に努力されていると思うんですが、実は、あるところで実験をさせていただきまして、ヤフーさんのプライバシーポリシーにたどり着けるかというのをさせていただいたんですが、非常にたどり着きにくい。20人ほどでやったんですが、２、３分かかるという状態で、実はどこにあるのかが分からないというところで、中身のコンテンツは非常に充実しているんですが、ユーザーオリエンテッドにあまりなっていないのではないかというの危惧しています。

具体的に普通プライバシーポリシーのある場所というのは一番下か、ヤフーさんの場合は一番下までスクロールというのはほとんど現実的ではないので、それ以外のところということになるんですが、一番右のペインの一番下ですよね。しかもここにプライバシーと

あるんですが、期待していたプライバシーポリシーではなく、プライバシーセンターが出てくるといった形。その後、コントロールであったりとか、そういったところを見に行く場合、意外と深い。一生懸命頑張っていらっしゃるんですが、気がついたら何となくダークパターン的なものに陥ってしまっているような気がしています。

質問というのは、こういった状態はあまりよろしくないということを前提にして、ユーザーのエクスペリエンステスト、こういったことをされているのかということと、もしされているのであるとすれば、そういったところはどういうふうに取り扱って反映されているのかということをお聞きしたいと思いました。以上になります。

【小柳氏】　ありがとうございます。厳しい御意見をありがとうございます。我々も、どこからどういうふうにリンクさせるのかというのは非常に悩ましく考えていたところで、プライバシーセンターを今のところは分かりやすいだろうというので、おっしゃるとおり、プライバシーのところからは行けるようにさせていただいております。これについて、プライバシーポリシーとセンターをユーザーさんが、プライバシーの取扱いについて実際に何かお調べになりたいと思ったとき、我々として、まずセンターから、というのが、それらの方が何しろ分かりやすく説明していたつもりだったので、そういうところもあって、そのような今のところの構成になっているところでございます。いただいた御意見等を踏まえまして、また改めて、どういうことが、在り方がより望ましいのかということについて検討させていただきたいと思います。

それからユーザーのテストについてですけれども、当然やっておりまして、また、今四半期というか、半期ですかね、大規模なものをやろうとしております。いただいた御意見等も踏まえながら、テストの具体的な設計をさせていただいて、お客様の意見をしっかり入れながら改善していきたいと思っています。ありがとうございます。

【寺田構成員】　ありがとうございます。非常に努力されているので、せっかくなので、やりやすいようになればいいと思いました。以上です。

【小柳氏】　ありがとうございます。

【宍戸主査】　ありがとうございます。それでは古谷構成員、お願いします。

【古谷構成員】　古谷です。ありがとうございます。非常にいい取組をされているという印象はあったんですけれども、例えばそのユーザーの便益と影響のバランスを取ったというところを、CDO・DD体制のところで御説明いただきましたが、影響が過小評価されがちになり得ると思います。そういったところをどういうふうに担保しているのかというと

ころをお聞かせいただきたいと思っています。恐らくアドバイザリーボードであったりとか、PIAといったところだと思うんですが、そういったところを１点お聞きしたいと思います。

あとユーザー側から言いますと、その影響というのが具体的に分からないと思うんですが、分かるようにするような工夫をしていらっしゃるか、今の寺田さんの質問と少し重なるかもしれませんが、教えていただければと思います。

【小柳氏】　ありがとうございます。ユーザーの、特に影響だと思うんですけれども、過小評価はおっしゃるとおり、ビジネス側がハンドリングしていると当然起き得ると思っております。したがいまして、おっしゃっていただいたとおり、PIAを実施したりとか、アドバイザリーボードの先生方に御意見をいただいたりとか、あと私がやっているDPOが個々の取組一つ一つに入っていって、私は消費者の代表として実は会社の中で存在しておりまして、ずけずけ言うと、相当嫌われていると思うんですけれども、そういうような形で、当然過小評価してお客様から嫌われてしまっては我々はまずいので、ここのところは私の責任だと思っておりますけれども、しっかりやっていきたいと思っております。

影響が分かるかどうかというところはなかなか難しくて、どういうコミュニケーションをすればいいのかというのが、まだ模索の段階だというのが正直なところかと思っております。隠しておいて、後で分かって怒られるというか、批判されるというか、お客様の期待を裏切るというのが一番は我々の怖いことでもありますので、これはしっかり、私たちの中でどういうふうなことを情報開示していけばいいのかということを真剣に考えて、取組を進めてまいりたいと思っております。

【古谷構成員】　ありがとうございました。

【宍戸主査】　ありがとうございました。まだまだお伺いしたいこともいろいろあるのですけれども、時間が来てしまいました。またこのヤフー様についても御質問があれば、また事務局にお寄せいただき、事務局から御回答いただくというふうにさせていただきたいと思います。

それでは、本日予定した議事は大体このぐらいですが、事務局から連絡事項があればお願いをいたします。

【丸山消費者行政第二課課長補佐】　事務局です。次回会合につきましては、事務局から御案内いたします。事務局からは以上です。

【宍戸主査】　ありがとうございます。これにて本日の議事は全て終了いたしました。

以上で、プラットフォームサービスに関する研究会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第２回会合を終了とさせていただきます。

本日は、皆様お忙しい中を御出席いただき、ありがとうございました。