



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主な論点

2021年6月4日
事務局

1. プラットフォームサービスに係る利用者情報を巡る現状と課題

- (1) プラットフォームサービスに係る利用者情報の現状と課題
- (2) 現行制度と政策
- (3) 海外動向

2. プラットフォーム事業者等による利用者情報の取扱いのモニタリング結果

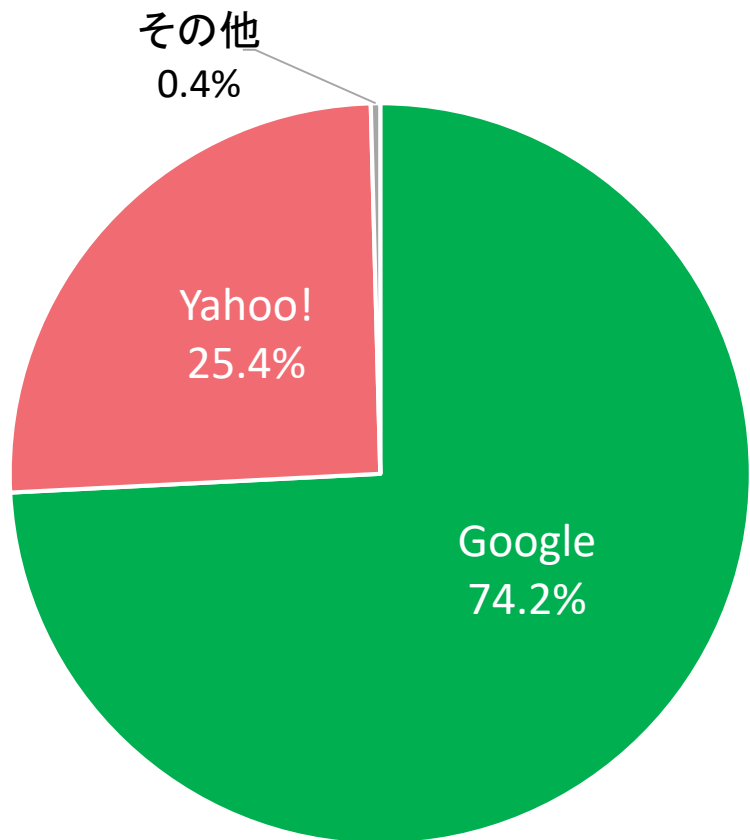
3. 今後の取組の方向性

- (1) 利用者情報の適切な取扱いの確保に向けた論点
- (2) 今後の取組の方向性

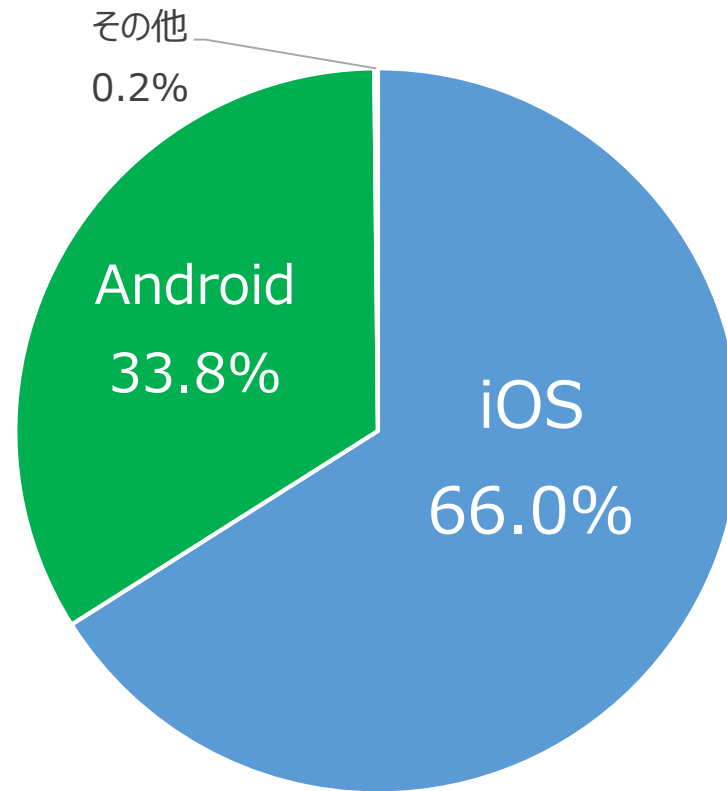
論 点

- 今後のAIの活用やIoT化の進展に伴い、データ流通環境等が大きく変化することが想定される。
- スマートフォンやインターネットは社会経済活動のインフラとなっている。インターネットへの接続についても大半がモバイル経由。生活のために必要なサービスがスマートフォン等経由で提供され、人々の日常生活における重要性が高まり、より機微性の高い情報についても蓄積されつつある。また、ポストコロナ時代に向けて、デジタルシフトが更に進んでいく。SNS、動画共有サイト、ニュース配信、検索等含めた情報流通もスマートフォン経由等が中心となる。
- この中で、様々なサービスを無料で提供するプラットフォーム事業者の存在感が高まっており、利用者情報が取得・集積される傾向が強まっている。イノベーションや市場の発展を維持しつつ、利用者が安心してスマートフォンやインターネットを通じたサービスを利用していくことができる環境を確保していく上でも、関係する事業者それぞれにおいて利用者情報の適切な取扱いが確保されることが重要である。
 - (参考1) 我が国において、iOS(iPhone)のシェアは約7割、Androidのシェアは約3割。各OS対応のアプリは、App Store(iOS)及びGoogle Play(Android)から入手可能。
 - (参考2) モバイルブラウザのシェアは、Appleが提供するSafariが約6割、Googleが提供するChromeが3割強となっている。デスクトップ(PC)ブラウザのシェアについては、Googleが提供するChromeが約6割、Microsoftが提供するEdge及びIEが2割強、Appleが提供するSafariが約1割。
- 利用者の利便性と通信の秘密やプライバシー保護とのバランスを、どのように確保していくか。プラットフォーム機能が十分に発揮されるようにするためにも、プラットフォーム事業者がサービスの魅力を高め、利用者が安心してサービスが利用できるよう、利用者情報の適切な取扱いをどのように確保していくか。

モバイル検索エンジンシェア(日本)
2021年4月

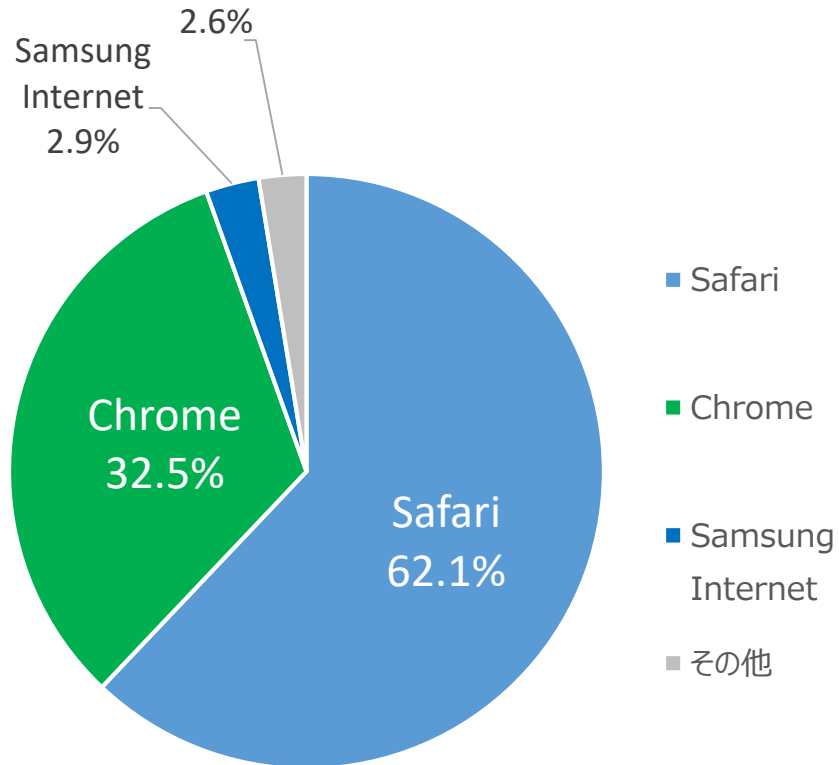


モバイルOSシェア(日本)
2021年4月

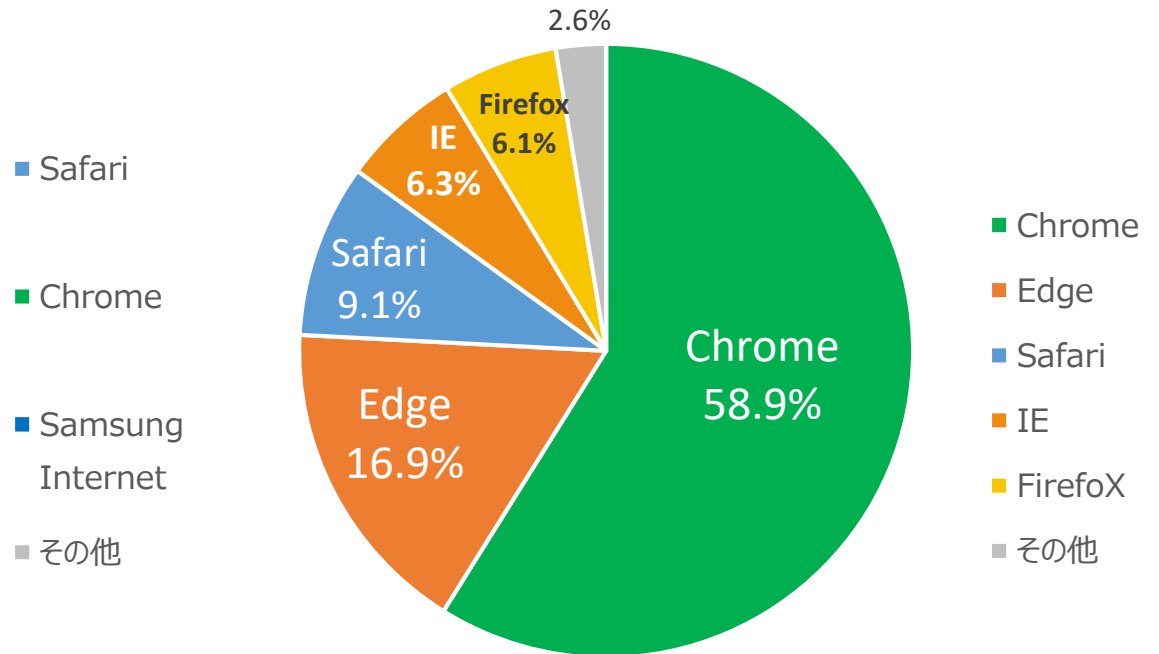


出典: StatCounter Global Statsから総務省作成

モバイルブラウザシェア(日本) 2021年4月

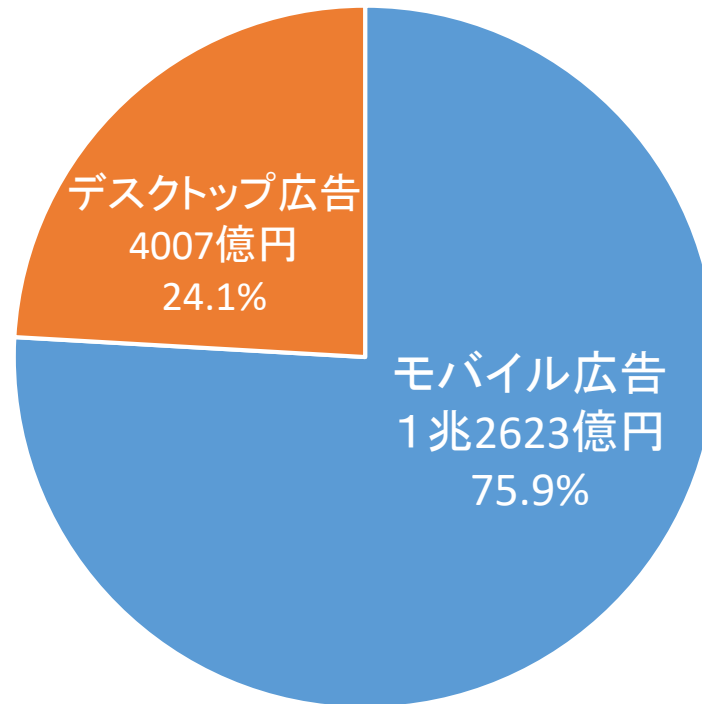


デスクトップブラウザシェア(日本) 2021年4月



出典: Stat Counter Global Statsから総務省作成

インターネット広告媒体費(日本) 2019年 総額1兆6630億円



出典: 2020年4月3日 電通報
「日本の広告費 インターネット広告媒体費詳細分析 No.2」
から総務省作成

論 点

- スマートフォンやタブレットなどの通信端末の位置情報や、ウェブ上の行動履歴、利用者の端末から発せられ、または、利用者の端末情報に蓄積される端末IDやクッキーなどの端末を識別する情報等の実態はどのようになっているか。
- スマートフォンにおいては、様々なアプリケーションが利用されている。アプリケーションのプライバシーポリシーの掲載率は大幅に向上してきているが、内容面の分かりやすさや簡略版の掲載に課題がある。また、OSにより一定の情報へのアクセスを行う場合に利用者に個別許可を求める機能等も導入されている。
- First Party CookieとThird Party Cookieがあり、Third Party Cookieには、SNS事業者、広告事業者、アクセス解析事業者、データ仲介事業者等に情報を送信するものが多く見られる。Webビーコン、イメージタグやJavaScriptなどによる情報収集も多く行われている。
- ウェブサイト管理者が実情を把握しにくく、プライバシーポリシーがきちんと書けていない場合がある。また、利用者にとってもプライバシーポリシーが分かりにくいという課題がある。

これまでの主な意見

【スマートフォンのアプリケーション等の実態】

- コロナ禍での接触確認アプリなどツール導入においても、誤解に基づき導入に慎重になる個人や自治体もあったため、そのアプリが利用する個人データや境界領域にある情報の取扱いについて、正確な情報に基づき導入可否の判断ができるよう分かりやすさを重視した仕組みを導入することが必要ではないか。【大谷構成員(第21回PF研)】
- 国内・海外の人気アプリともに、プライバシーポリシーの掲載率はほぼ100%。新着アプリでも掲載率は80%以上。2016年以降、Google、Appleがスマートフォンのアプリケーションのプライバシーポリシー掲載に関するガイドラインの策定や規制強化を実施してきたことの影響が大きいと考えられる。Googleは、アプリ開発者に対して、2016年12月にプライバシーポリシーが掲載されていないアプリへの警告、2017年には個人情報をユーザーの同意なく収集するアプリに対する警告を送付。Appleは、アプリ開発者に対して、2016年6月にApp Store審査ガイドラインを大幅に改正、2018年8月には全てのアプリにプライバシーポリシーの掲載を義務付けた。【JRI(第21回PF研)】

これまでの主な意見

【スマートフォンのアプリケーション等の実態（つづき）】

- 会社全体やサービス全体を対象としたプライバシーポリシーの掲載が主流で、アプリがどの情報をどの目的のため取得するか読取り難い。また簡略版の掲載については浸透していない。Googleは、Android6.0から危険と分類されたスマートフォンの機能や情報にアクセスする場合には、アプリ内で個別に利用者の同意を得るモデルに変更。Appleは数年前からプライバシー性の高い情報にアクセスする際にはアプリ内で個別に同意を得る仕様であったが、iOS10では同意を取得する際に説明文(情報の取得理由・利用目的)の記載が必須となった。【JRI(第21回PF研)】
- スマートフォンのアプリについては、広告ID(iOS:IDFA,アンドロイド:AAID)があるが、アプリを起動するとニュース等を閲覧するだけでも広告やトラッキング系の情報提供が数多く行われていた。調査した結果、位置情報を取得するアプリのうち半数はプライバシー・ポリシーにその旨記載がなかった。【太田構成員(第22回PF研)】
- スマートフォンの利用としてこれまでエンタメ周りが多かったが、社員証・学生証をアプリで代替したり、学校成績証を入れたり、医療情報・健康情報を保存して一元的に管理するなど、よりリアルかつ機微性の高い情報についても蓄積されつつある。また、AI・IoTやビッグデータにより、これまで取れなかったコミュニケーションベースのデータなども集めて推測、推定データとして使うようになってきている。【JRI(第4回WG)】
- 取得経路として、一つのアプリの中に様々な機能が搭載され色々な情報が取られて事業者間で情報共有されるというところで、直感的な分かりにくさがある。更に、取得方法・取得経路の動きとして、スーパーアプリ化の流れがあり、情報の流通が非常に見えにくくなる。また、サイバー・フィジカルの一体化の動きが進み、Beaconやカメラ情報など含めてリアル端末とアプリの連携も進む中で、取得経路・手法が複雑化する中で利用者への透明性確保が課題。【JRI(第4回WG)】

これまでの主な意見

【ウェブサイトにおけるCookie等の実態】

- First Party CookieとThird Party Cookieがあり、Third Party Cookieには、SNS事業者、広告事業者、アクセス解析事業者、データ仲介事業者等に情報を送信するものが多く見られる。SNSのIDが付番されSNSアカウント情報と紐付けられ、取得されたデータは個人データになる可能性があるため、設置サイトの運営者が利用者に周知する必要があることが個人情報保護委員会から注意喚起されている。【太田構成員(第22回PF研)】
- Third Partyによる情報取得の方法として、従来はイメージタグ(イメタグ:1ピクセルの見えない画像)をウェブサイトに貼ってCookie、IPアドレス、閲覧ページURL等を取得していたが、今はJavaScriptのタグ(JSタグ)が主流。イメタグより多くの情報取得(ページに表示される情報や入力される情報等も取得可能)やページ操作、他のJSタグの強制的読み込み等も可能となっている。ウェブサイト運営者も知らないうちにJSタグがどんどん増えて制御困難な場合もあり、事業者間でID連係(Idsync)等がされる場合もある。【太田構成員(第22回PF研)】
- ウェブサイト管理者が実情を把握しにくく、プライバシー・ポリシーをきちんと書けていないサイトが多い。例えばSNSのIDは個人データと紐付く場合も多いが、多くのサイトでcookieが個人情報と紐付くことはないと記載している。また多数の事業者にデータを送付しているがその旨の記載がない事例も多い。【太田構成員(第22回PF研)】
- 広告における利用者情報を扱った場合の課題として、ユーザーを特定もしくは識別する、あるいはサイトや事業者を超えて利用するといったところが挙げられる。第三者配信広告は、ユーザーから見た場合に、誰が配信し、自分のデータがどう扱われているか分からない。なお、それ以外に、自社で広告枠を作って自社で広告を集めるといったファーストパーティーのデータを使う広告がある。【寺田構成員(第3回WG)】
- ファーストパーティーであるWebサイトのタグにより、広告事業者サーバーへアクセスが指示される。広告事業者サーバーはどのWebサイトからアクセスを指示されたか把握するとともに、Third Party Cookieを発行し送信。広告事業者サーバーは、Third Party Cookieをキーにしてウェブサイトの閲覧履歴を作成できる。このような閲覧履歴を把握し分析できる仕組みをDMPという。同じことは、同じ仕組み、リクナビの場合も全く同じである。【森構成員(第4回WG)】



論 点

【ブラウザや広告ID】

- モバイル及びPCともにプラットフォーム事業者が提供するブラウザが高いシェアを有しており、AppleのSafari（モバイル/PC）においてThird Party Cookieをはじめクロスサイトトラッキングが既にブロックされている。このような動きはFirefox等の他のブラウザでも見られ、GoogleのChromeにおいてもThird Party Cookieの段階的廃止（2022年に完全廃止）が予定されている。
- Appleの提供するIDFA(Identifier For Advertisers)を利用するために2021年4月26日以降、利用者の同意が必要となった（ATT：App Tracking Transparency Framework）。
（参考）Googleの提供するAAID（Advertising ID）はIDFAと同様の機能を提供している。
- Googleは、2019年にPrivacy Sandbox Projectを発表。FLoC（Federated Learning of Cohorts）としてBrowserの中で機械学習を利用して行動履歴をAIにより分析し、同種の興味関心を持つ数千人のグループ（Cohorts）としてターゲティング広告の対象とすることを提案。Chrome Browserの中で初期トライアルを開始。FLEDGE（First Locally-Executed Decision over Groups Experiment）として広告のオークションを「信頼できるサーバー」で行うとしている。

【業界団体や業界の動き】

- 業界団体であるIAB（欧州インタラクティブ広告協議会）が中心となり、GDPRに準拠し、TCF(Transparency and Consent Framework) を公表、これをベースとしたCMP(Consent Management Platform) の動きが進んでいる。
- フィンガープリントやUnified ID2.0（メールアドレスハッシュ化）などによるトラッキングを検討する動きもある。同意取得の在り方やオプトアウトの在り方について課題が指摘される。

これまでの主な意見

【トラッキング等に関するプラットフォーム事業者及び業界の動向】

- 端末の中のデータを個別に分類して、個人情報¹の該当有無を判断するのではなく、もう少し全体でそういった情報は必ず何か²にひもづく可能性があるということを前提にした上で考えていく必要があるのではないかと。古くて新しい問題としてフィンガープリントとか、駄目だと言っているにも関わらず検知されないからということでDPIのようなこととか起こり始めているとも聞いており、もう少し大きな枠組みで、やっていいこと、いけないことといった概念の方からもう少し考えていく必要があるのではないかと。【寺田構成員(第21回PF研)】
- プラットフォーマーの提供するブラウザでThird Party Cookieによるトラッキングが制限され、2021年以降アプリにおけるIDFAの利用に同意が必要となり、Privacy Sandbox等の提案もある。一方、Canvas Finger Pringing等の別の手法や、同意を取得した上でメールアドレスに基づく情報やIDによるトラッキングを検討する動きもある。業界としてフィンガープリントやメールアドレスベースのトラッキングについてはオプトアウトの仕組みを準備することにより対応しようとしていると認識しているが、オプトアウトの信頼性の問題はあります。【太田構成員(第22回PF研)】
- Third Party Cookieはセキュリティやプライバシーを守るために使われる例もあるが、プライバシーを侵害する使い方が注目され全部やめるという風潮になっており、この辺りは結構慎重に扱うべきなのかと思う。Cookie等についてもプラットフォーム事業者が大きな力を持ってしまっており、競争法的な考え方というのも頭の片隅に入れておく必要がある。メールアドレスベースのIDについては、メールのリサイクル問題があり、間違っただプロファイリングがされてしまう可能性があることをちょっと危惧している。【崎村構成員(第22回PF研)】
- 固定的IDは問題という議論を経てリフレッシュできるIDFA等が導入された流れがある。一方、ブラウザフィンガープリントやUnified ID2.0等がメールアドレスベースという時に簡単に換えられないと思うが、それは業界的に許容されるのか。そのようなIDを作ることをオプトインで同意する人が想定されるのか。色々なところで使っているものを一斉にオプトアウトすることは難しいのではないかと。【森構成員(第22回PF研)】

これまでの主な意見

【トラッキング等に関するプラットフォーム事業者及び業界の動向（つづき）】

- 業界においては、独自IDを考える方向、ファーストパーティークッキーをより活用する方向、コンテクスチュアルターゲティング等の方向が検討されている。代替IDについては、現在よく聞くのが Unified ID 2.0(メールアドレスを暗号化してIDとする等)とDevice Fingerprintingの2つであり、Third Party Cookieとほぼ同じ効果が期待されるが、物議もかもしている。また、First Party同士でデータ流通の仕組みも色々なものが提案され考えられている状況。【寺田構成員(第3回WG)】

【トラッキング等に関するプラットフォーム事業者の最近の動き】

- Apple Inc.からの発表および質問から回答があったように、iPhoneアプリに関しては、ポップアップで許可を押させれば、事業者をまたいだ端末識別(IDFAを用いたトラッキング)が可能であり、利用目的は限定されない。また、IDFV(ID for Vender)に関しては、1st Party に閉じているという説明があったが、同じ開発元のアプリであれば、アプリをまたいだ端末識別が可能であり、ユーザーのコントローラビリティはない。一方Safariブラウザの仕様を考えると、同意の有無に関わらず、事業者やサイトをまたいだ計測を一方向的にブロックする仕様になっており、1st Party Cookieについては、ユーザーがCookieを削除するという一定のコントローラビリティは確保されている。また、Google Analyticsなどの1st Partyが計測を行うことに関して、Googleではサイト利用者にオプトアウトリンクを示すように利用規約で義務付けている。【太田構成員(第2回WG)】
- ID for Vendorsというのは、同一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、ファーストパーティーアドとなるので、App Tracking Transparency(ATT)のプロンプトでブロックされることはない。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、プロンプトによってコントロールされることになる。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、ポリシーに関わるコンポーネントがある。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、ユーザーの同意が必要になる。ポリシーコンポーネントに関しては、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、フィンガープリンティングもできないということ、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る。【Apple(第2回WG)】

これまでの主な意見

【トラッキング等に関するプラットフォーム事業者の最近の動き（つづき）】

- サードパーティークッキーには制限がかかってきているが、ファーストパーティーのクッキー使用は残るため、クッキーレス時代になるわけではない。IDFA (Appleの広告ID) についても、利用者の事前同意を取得すれば使えるため、なくなるわけではない。欧米のプライバシー保護の法律などに合わせて、グローバルなプラットフォーム事業者が様々な施策を打ってきており、同意、オプトアウト、コントロール性、アカウントビリティなどが重視する方向となっている。【寺田構成員(第3回WG)】
- Appleの場合には、広告ID (IDFA) について利用する場合には、2021年4月中に利用者の同意を必要とする方向。また、既に、ウェブブラウザのSafariにおいて、Third Party Cookieやクロスサイト・トラッキングをブロックしている。AppleはATT (App Tracking Transparency Framework) を通じてIDFAの同意を取る仕組みとなっており、SKAdNetworkという分析の仕組みが用意されているが制限がかなり厳しい。また、アプリのマーケットプレイスであるAppStoreにおいて、実際に収集するデータの詳細な情報や用途を開示することを義務づけている。【寺田構成員(第3回WG)】
- Googleの場合には、ウェブブラウザのChromeにおいて、2022年に(Third party Cookieを)完全廃止という方向でアナウンスされている。これに合わせて、クッキー以外にも特定の個人もしくは個人を識別するようなIDは自社商品の間では採用しないとアナウンスしている。また、広告IDについても、永続的なIDとの関連付けなどを行う場合には、同意をするようにという流れになっている。GoogleはPrivacy Sandbox Projectで端末の中で個人ではなく集団としてIDを付けて集団にターゲティングできる仕組みを用意している。リターゲティングについては、FLEDGEという第三者の信頼できるサーバーを使うとしているが具体的なところは見えてきていない。端末の中か外かの違いはあるが、プロファイリングに該当する可能性。GDPRの適用についてGoogleと欧州当局の間でも調整中と思量。【寺田構成員(第3回WG)】
- プラットフォーム事業者に対してのみ必要以上の規制を課してしまうと、現在AppleやGoogleが行っているようにルールメーカーにしてしまい、結果的に市場競争環境の阻害であったりとか、ウオールドガーデンで消費者への不利益を助長したりとか、こういった部分も危惧される。【寺田構成員(第4回WG)】

これまでの主な意見

【業界団体等の最近の動き】

- Unified ID2.0等についての一番根本的な違いは、最初に同意を取るか取らないかということ。本当にこれが業界でちゃんと話しをして、同意を取るというのを誰でも分かるような仕組みとか形にすれば、ある意味理想的な最初の入り口になると思う。オプトアウト系の問題は、データが流通していく中で、CMPといった仕組みで最後まで徹底的にトラッキングできるのかどうかとのせめぎ合いが起きる。徹底的なトラッキングができれば、ちゃんと仕組みを作れば、オプトアウトとも必要なところでできるということになるが、もう一方で、徹底的なトラッキングができてしまう方がいいのか・悪いのかという問題も起きているのは事実。業界だけではなく、消費者などの中でも、何が許され、どこまでは危ないか等の一種の線引きをしないと難しいと思う。【寺田構成員(第22回PF研)】
- 業界自主ルールに基づいた従来型のターゲティング広告を継続するとともに、トラッキング制限に伴う代替のIDソリューションの模索をする必要がある。【JIAA(第1回WG)】
- アドフラウドを含む無効配信の除外と広告掲載先品質に伴うブランドセーフティの確保に関して事業者を認証し公開するJICDAQの取組が2021年4月開始された。【JIAA(第1回WG)】
- 業界団体であるIAB(欧州インタラクティブ広告協議会)が中心となり、GDPRに準拠し、TCF(Transparency and Consent Framework)を公表、これをベースとしたCMP(Consent Management Platform)の動きが進んでいる。業界団体であるIABにおいてProject Rearcとして、Global Privacy Platformについて3月に意見募集の素案を発表している。これは、TCFをベースに各国規制に対応するものとして規格化し、監査できる仕組みの素案。【寺田構成員(第3回WG)】
- またPRAM(Partnership for Responsible Addressing Media)として、広告主協会や広告協議会などにより、同意取得も含めた代替IDの基準やアーキテクチャーを考える動きもある。Unified IDもメールアドレスという機微な個人情報に当たるため、どう同意を取得し扱うのかをPRMAで協議中。取得時は個人情報、流通時は個人情報と切り離すといったことも検討してる模様。日本は個人情報は同意を前提としない、クッキーについては個人情報と紐付かなければ個人情報保護法の対象外など法律の立て付けが少し異なり、日本の業界団体は国内の法令遵守を前提で動くが、グローバルなプラットフォーム事業者の方向もあり、対応がばらばらになっている状態。【寺田構成員(第3回WG)】

これまでの主な意見

【トラッキング等に関する最近の動きに係る課題】

- 第一の論点は、ユーザーレベルのIDをどうとらえていくか（Appleは有効な同意を求めている、GoogleはユーザーレベルIDを禁止し集合的なものとして考えていく方向）。第二の論点は、ドメインを超えて情報を共有するクロス・サイトトラッキングについてどうすべきか。第三の論点は、有効な同意は何かということ。同意の流通の範囲はどこまで、持続期間や処理・加工はどこまで許されるのかといった議論。ユーザーレベルIDがなくても、プロファイリングの論点はありうる。【寺田構成員（第3回WG）】
- ターゲティングが失われると、広告の価値・単価が下がるとか、無差別化で合わない広告が表示される、モバイル広告の議論なども検討が必要だろう。また、SNSやECサイトや動画サイトは、ファーストパーティーとして多くの情報があり、これらデータ収集に頼った広告が増える可能性もあり、クロスサイトのアドテクが進むという心配もある。【寺田構成員（第3回WG）】
- アドフラウドは非常に技術的に巧妙な仕組みを使っており、どんどん高度化していくので、プラットフォーム自体への規制といった取組とはまた異なる仕組みで取り組んでいく必要があると思われる。ターゲティングには、一定程度効果がある。利用者にどこまで説明し透明性を持たせても、利用者サイトでそれを納得できる仕組みを作れるのかというのが今後問題になる。【寺田構成員（第3回WG）】
- 同意を取得する仕組みを作れば、eプライバシー規則への対応もできると思量、同意の取り方は個人個人感じ方が違うところもありどの辺りがリーズナブルで有効性と利便性を合わせて一番よい落としどころになるかということについてはまだ色々と議論が必要と認識。【寺田構成員（第3回WG）】
- Unified IDやフィンガープリントによるファーストパーティーデータの突合や、位置情報による推定からファーストパーティーデータの特定などがあり、やり方についての透明性確保が非常に難しくなっている。原則的に何をしてはいけないうか、何を説明すべきかをもう一度見直す必要があると感じている。【寺田構成員（第4回WG）】

論 点

【個人情報保護法及び電気通信事業GL】

- 事業者による個人情報の取扱いについて個人情報保護法により規律されている。令和2年改正で、個人の権利の在り方に関して、保有個人データの開示方法や利用停止・消去等の請求権の要件緩和、事業者の守るべき責務の在り方に関して、漏えい等事案の報告及び本人通知の義務化、事業者の守るべき責務の在り方について、違法又は不当な行為を助長する等の不適正な方法により個人情報を利用してはならないこと、事業者による自主的な取組を促す仕組みの在り方に関して、特定部門を対象とする団体の認定、データ利活用に関する施策の在り方に関して、仮名加工情報の創設や個人関連情報の第三者提供規制、ペナルティの在り方、域外適用の拡大や越境移転時における情報提供の充実等について、見直しが行われた。また、令和3年にはデジタル社会の形成を図るための関係法律の整備に関する法律が成立した。両改正とも令和4年4月施行予定である。
- 電気通信事業法に通信の秘密が規定されており、本年4月から令和2年改正（域外適用）が施行された。
- 電気通信事業における個人情報保護に関するガイドライン（電気通信事業GL）において、電気通信事業分野の個人情報保護及び通信の秘密等について規定されている。（電気通信事業GLにおいて、電気通信事業の性質などを踏まえ、個人情報保護管理者、プライバシーポリシー、各種情報の取扱い（通信履歴の記録、位置情報等）についても規定されている。）個人情報保護法の令和2年改正及び電気通信事業の性質等を踏まえた上で、電気通信事業GLの見直しを検討する必要がある。

【SPI及びSPO】

- スマートフォンの利用者情報の適切な取扱いについて検討し、スマートフォン プライバシー イニシアティブ（SPI）を2012年に公表。スマートフォン利用者情報取扱指針として、6つの基本原則とアプリ提供者、情報収集モジュール提供者等の利用者情報取得者における取組、アプリ提供サイト運営者等の関係事業者における取組を示した。
- SPIの実施状況等について2013年からスマートフォン プライバシー アウトルック（SPO）として毎年継続的に調査を実施しこれを公表してきている。主に、人気アプリ100、新着アプリ100についてプライバシーポリシーの掲載有無、掲載の場合にはSPIに定められた8項目の記載状況等を調査、プライバシーポリシーの掲載率などは向上してきている。
- 直近とりまとめられたSPOⅧにおいて、人気アプリはAndroid、iOSともにプラポリの掲載率は昨年同様100%に近い形であり、重要とされる事項（アプリ提供者名、取得項目、利用目的、第三者提供の有無等）も記載率は高い。一方、新着アプリは、Androidのプラポリ掲載率が60%台まで大きく下がっており、SPIに定められた項目の記載率もAndroid/iOSともに下がっており少し質の低下が見られる。

論 点

【SPI及びSPO（つづき）】

- 電気通信事業GLにおいてもSPIを踏まえた規定（アプリケーションポリシーを提供する場合、アプリケーションを提供するサイトを運営する場合、アプリケーションのプライバシーポリシーに記載すべき具体的項目）が設けられており、SPIの内容を踏まえた事業者団体のガイドライン等も策定されている。
- アプリマーケット運営事業者の取組としては、Google、AppleともにOSのバージョンを上げるたびに、プライバシー関連機能は強化されている。Appleは、App Storeのアプリ紹介ページに、アイコンで取得される情報と利用目的について分類して表示しており、アプリ提供者にはアプリ更新や新規アプリの際の情報提出が義務化されている。

【位置情報プライバシーレポート】

- 位置情報プライバシーレポートは2014年に策定され、電気通信事業者が取扱う位置情報として基地局に係る位置情報、GPS位置情報、Wi-Fi位置情報の概要について整理した上で、十分な匿名化の枠組みについて検討。これを踏まえ、「十分な匿名化」の加工基準等がまとめられ、民間ガイドラインが作成された。また、利活用モデルなどについて検討された。
- 位置情報について端末から直接取得されるものだけでなく、他の色々な手段や情報から位置情報が取得できるようになってきている（例えば、リアル店舗での購買履歴はすべて位置情報になるのが実情である。）ことを前提とした上で、位置情報の精度・種類・性質等も踏まえた上で、その取扱いの在り方について検討していくことが重要ではないか。
- 電気通信事業GL・解説において、位置情報プライバシーレポートを踏まえた記載（通信の秘密に該当する位置情報及び通信の秘密に該当しない位置情報等の取扱いについて）があり、これを踏まえ事業者団体のガイドライン等も策定されている。

論 点

【JIAA】

- JIAAにおいて、インターネット広告ビジネスにおいて取得・利用されている個人に関する情報の取扱いについて、事業者向けの指針として、「プライバシーポリシーガイドライン」（2004年策定、2017年再改定）、「行動ターゲティング広告ガイドライン」（2009年策定、2016年再改定）を策定。JIAAはガイドラインの啓発活動を行うとともに、技術の進展やビジネスの実態の変化に応じ見直しを行っている。行動ターゲティング広告ガイドラインでは、行動ターゲティング広告でのユーザーへの「透明性の確保」と「関与（オプトアウト）の機会の確保」の徹底を原則とし、媒体運営者、情報取得者、配信事業者に区分してその事業領域ごとに遵守事項を規定している。
- JIAA会員社は広告配信事業者がメインであり、会員社ではない媒体社や広告主にまでは直接規律が及ばないという課題が指摘される。
- アドフraudを含む無効配信の除外と広告掲載先品質に伴うブランドセーフティの確保に関して事業者を認証し公開するJICDAQの取組が2021年4月開始された。

【デジタル広告市場】

- 本年4月にデジタル広告市場の競争評価の最終報告が発表されており、課題⑩パーソナルデータの取得・利用に係る懸念の対応については、電気通信事業における個人情報保護に関するガイドラインなどの見直しにより対応することとされた。

これまでの主な意見

【令和2年個人情報保護法改正】

- 本人の関与を強化する等の観点から、利用停止・消去等の個人の請求権の要件を緩和し、保有個人データの開示方法について電磁的記録の提供を含め、本人が指示できるようにする改正を行った。また、事業者の守るべき責務に関し、委員会への漏えい等報告及び本人への通知を義務化し、詳細は規則等で定めることとした。また、違法又は不当な行為を助長する等の不適切な方法による個人情報の利用を禁止する改正を行った。【個人情報保護委員会事務局(第22回PF研)】
- データ利活用に関する見直しとして、イノベーションを促進する観点から仮名加工情報の制度を導入するとともに、個人関連情報の第三者提供規制を導入し、提供先において個人データとなることが想定される情報の第三者提供については、本人同意が得られているか等を確認することを義務化した。また、命令違反等に対する法定刑を引き上げるとともに、報告徴収や命令を可能とする形で域外適用を強化している。外国にある第三者に個人データが提供される際に移転先に係る情報提供の充実も盛り込んでいる。今後改正法の円滑な施行に向けて、政令、委員会規則、ガイドライン、Q&Aなどについて準備を進めていく予定である(※)。【個人情報保護委員会事務局(第22回PF研)】

※政令、委員会規則については、本年3月24日に公布済み。

これまでの主な意見

【スマートフォン プライバシー イニシアティブ、スマートフォン・プライバシー・アウトルック】

- スマートフォン・プライバシー・アウトルックについて、2010年代から継続的な検討がなされていることそのものが非常に大きな意義があり、総務省の取組として引き続き継続してほしい。2014年以降の調査により、プライバシーポリシーの掲載率が顕著に向上しているということが非常に分かりやすい調査結果として出ており、継続性の意義がある。【新保座長代理(第21回PF研)】
- モバイル・コンテンツ・フォーラムがSPIの内容を受けてガイドラインを作成し会員に広めており、一部の情報収集モジュールはSPIの内容を踏まえてプライバシーポリシーへの記載方法を周知している動きもある。【JRI(第21回PF研)】
- 広告代理店において、ガイドラインを作り会員会社に対してそれを守るように促している。モバイル・コンテンツ・フォーラムのガイドラインは地方公共団体のアプリでも利用例がある。【寺田構成員(第21回PF研)】
- 2013年からスマートフォン・プライバシー・アウトルックについて毎年調査が実施され今回Ⅷがとりまとめられた。主に、人気アプリ100、新着アプリ100についてプライバシーポリシーの掲載有無、掲載の場合にはSPIに定められた8項目が記載されているかを調査。人気アプリはAndroid、iOSともにプラポリの掲載率は昨年同様100%に近い形。重要とされる事項(アプリ提供者名、取得項目、利用目的、第三者提供の有無等)も記載率は高い。一方、新着アプリは、Androidのプラポリ掲載率が60%台まで大きく下がっており、SPIに定められた項目の記載率もAndroid/iOSともに下がっており少し質の低下が見られる【JRI(第4回WG)】
- アプリマーケット運営事業者の取組としては、Google、AppleともにOSのバージョンを上げるたびに、プライバシー関連機能は強化されている。Appleは、App Storeのアプリ紹介ページに、アイコンで取得される情報と利用目的について分類して表示しており、アプリ提供者にはアプリ更新や新規アプリの際に情報提出が義務化されている。【JRI(第4回WG)】

これまでの主な意見

【位置情報プライバシーレポート】

- 2014年に策定された位置情報プライバシーレポートにおいて、電気通信事業者が取扱う位置情報として**基地局に係る位置情報、GPS位置情報、Wi-Fi位置情報**の概要について整理した上で、**十分な匿名化の枠組み**について検討。これを踏まえ、「**十分な匿名化**」の加工基準等がまとめられ、**民間ガイドライン**が作成された。また、利活用モデルなどについて検討された。【高橋構成員(第1回WG)】
- **位置情報に対するイコールフットイングのニーズ**がすごく高いと認識。今後の議論において、ただ位置情報といっても対象とする種類が色々あるという話と、事業者の範囲も多岐にわたると思ひ、そこを明確化する必要があるだろう。携帯の基地局で言えば、電気通信事業者、キャリアだけでいいが、Wi-fi、ビーコンになってくると、電気通信事業者のほかにプラットフォームが入ったり、Wi-fi、ビーコンを設置する事業者が入ってきて、範囲が広がってくる。恐らくここが一番イコールフットイングが問題になってくるのではないか。【小林構成員(第1回WG)】
- GPSについても、位置情報を測位するもので、**プラットフォーム、アプリ提供事業者、電気通信事業者の間の何かこの整理**がいるだろう。コンビニの購買履歴や鉄道の乗降履歴等、こういったものに付随される位置情報となると、なかなか電気通信事業分野を超えてしまうのかなということがあって、こういったものを今回の射程にするというのはどうか。NTTドコモがdポイント事業を使って購買履歴や様々なデータをシームレスに集めてといったことがあったりすると、それも入ってくるのかもしれない、こういったものも今回の射程に入れるべきなのかどうかというのを事業者がどうお考えになっているのか。【小林構成員(第1回WG)】
- 12ページのWi-Fi位置情報について、受信強度(RSSI)と到達時間差(TDoA)測位の使い分けで、電波の反射を理由に挙げられているが、むしろTDoAは少なくとも10m×10m以上の部屋がないと、電波の到着時間差が測るのが難しいためである反射、つまり狭い空間におけるマルチパスの影響はTDoAよりもRSSIの方が大きいのが実状かと思う。Wi-Fiであったり、GPSといった、そういった測位を使った情報にどうしても話が特化していくが、現実には、例えば、**購買履歴**でも、**どこの店で買ったという時点で、店の名前で位置情報が取れるというのが実情**だと思う。よって、今後そういったプライバシー、こうしたところの位置情報を議論するとき、やはり**位置情報というのがいろいろな手段で取れるということ**を前提にしていけないといけないと考えている。【佐藤構成員(第1回WG)】

これまでの主な意見

【位置情報プライバシーレポート（つづき）】

- 位置情報を、今の考え方でいくと、通信事業者にとってどんどん不利になっていくような検討ばかりになっているのではないかというのを気にしている。キャッシュレスが進むと、当然店舗というところで位置情報というのがもうPOI、それ自身がもう意味を持っている状態になっている。あるいは、カメラでも、場所によって、場所を特定して、そこで何が行われているのかという場所の情報プラス、そういった行動であったりとか、附帯の情報というのが非常に増えた状態になってきているということで、位置情報の考え方そのものを、現在の考え方からもう少し変えていく必要があるのではないかというのを感じている。【寺田構成員（第1回WG）】
- 位置情報を広げて考えるべきというのは全く同感。来店記録は位置情報になる場合があると考えられる。Wi-Fi位置情報はスマホのMACアドレスで管理され、それが複数の店舗間で結びつけられれば移動履歴にもなる。それは例えば顔画像でも同様のことがいえ、同じ人の顔がこの店に行った、あの店に行ったということで同じようなことが起きる。よって、技術的観点から、寺田構成員の御指摘はまっとうなものだと思う。【高橋構成員（第1回WG）】
- 位置情報についても、電気通信事業法等が、現在の実態からズレてきているように感じた（同じ情報実践をしても、形式的に異なる規律がかかる、など。憲法14条の問題にも関わる。）。実態に合致した規律枠組みの再構成が重要ではないか。また、その新たな規律枠組みについては、海外事業者にもわかりやすいものが必要だと感じる。【山本主査代理（第1回WG）】
- イコールフットイングである必要があるだろうと思っている。位置情報なんかが特に典型のもので、キャリアばかりが厳しくなっていくという形はおかしくて、同じようなサービスを行う、電気通信サービスを行う者に関してイコールフットイングで考えていくというのを、常に念頭に置いておく必要がある。【寺田構成員（第4回WG）】
- 位置情報について、端末が直接吐き出すものだけでなく、他の情報から位置情報が分かる場合も対象にするかは論点にした方がよい。例えば、リアル店舗での購買履歴はすべて位置情報になる。【板倉構成員（第4回WG）】

これまでの主な意見

【JIAAガイドライン】

- ユーザーに関する情報を活用したターゲティング広告は、企業にとって有用であると同時に、ユーザーにとっても興味関心のある広告に接する機会が増えるという利点がある。一方、ユーザーがプライバシーに関する懸念や広告に対する不信感を抱かないように、事業者が取得したどのような情報が広告に利用されているか、ユーザーが容易に知り、十分な情報をもとにデータの取得又は利用の可否を選択できる簡便な仕組みを提供する必要。【JIAA(第1回WG)】
- インフォメーションアイコンや各社のプライバシーポリシーからオプトアウトが選択できるようになっており、消費者が選ぶことができるようになっている。インフォメーションアイコンプログラムの認定を受けた事業者は13社、相当の広告にアイコンが表示されている。【JIAA(第1回WG)】
- JIAAはインターネット広告ビジネスにおいて取得・利用されている個人に関する情報の取扱いについて、事業者向けの指針として、「プライバシーポリシーガイドライン」(2004年策定、2017年再改定)、「行動ターゲティング広告ガイドライン」(2009年策定、2016年再改定)を策定。ガイドラインの啓発活動を行うとともに、技術の進展やビジネスの実態の変化に応じ見直しを行っている。行動ターゲティング広告ガイドラインでは、行動ターゲティング広告でのユーザーへの「透明性の確保」と「関与(オプトアウト)の機会の確保」の徹底を原則とし、媒体運営者、情報取得者、配信事業者などに区分してその事業領域ごとに遵守事項を規定している。インフォメーションアイコンやオプトアウト等の施策に一定の評価が得られているが、認知を高める周知が必要。同じ広告の繰り返し表示の問題には、フリークエンシーコントロールなどの施策もあるが、広告配信の仕組み上のコントロールの難しさもある。ターゲティング広告の望ましいあり方をユーザー視点で再考することが必要。【JIAA(第1回WG)】
- ターゲティング広告の消費者の不安はその仕組みが見えていないことに由来する側面。DDAIというオプトアウトサイトでターゲティング広告の仕組みを説明する啓発のページを設けている。【JIAA(第1回WG)】
- 業界の取組として大変重要。どうしても業界のソフトローといったものは、なかなか外部から実際の取組というものが見えづらくなるどころ、今日の質疑で具体的などころがかなり段々わかってきた部分がある。こういった場での外部からの様々な意見を受け入れていくという意味でも、まさに継続的に意見交換をしていく、共同規制のような取組というものを作っていくことができるかということが大変重要と思った。【生貝構成員(第1回WG)】

これまでの主な意見

【JIAAガイドライン（つづき）】

- JIAA会員社は広告配信事業者がメインになっており、そこでプライバシーポリシーにきちんと書こうといったことは会員社が遵守しているという状況であっても、その会員社が情報を集める先というのは、媒体社であったり広告主のサイトであったりしてそこまで規律が及んでいないというところは、JIAAも課題として上げていたと思うので、そういったところに規律が及ぶような仕組みをJIAA含めて考えていければいい。【太田構成員（第1回WG）】
- JIAAの会員企業や本日の事業者の取組は大変先進的で、参考になるところもたくさんあって素晴らしいと思う一方で、世の中に出回っているプライバシーポリシーにはそうではないところがたくさんある。利用者の観点から見ても、読んでもプライバシーリスクがあるのかないか判断しようがないというものがほとんどではないか。今後の検討にあたっては、先進事例を色々紹介してすばらしいものを褒める取組とともに、一般のサイトもより透明性を求め、個人が利用するときにプライバシーのリスクがあるのかないかをきちんと判断できるようなプライバシーポリシーへのステップアップを検討いただくといいのではないかと思う。【沢田構成員（第1回WG）】
- 事業者自身がどういう風に利用者の情報を使うかということと共に、サイト運営者として、第三者がデータを収集する接点としてのウェブサイトやアプリケーションの運営に当たってのポリシーや、広告主としてのポリシー、どんな仲介サービスを使い、どんな考え方でマーケティングしていくのか（JIAAのガイドラインを遵守しているとか、海賊版サイトには広告を出さないとか）、そういったことも含めて、これら3つくらいのポリシーをそれぞれ企業が開示していくような取組が望ましいのではないか。【沢田構成員（第1回WG）】

【デジタル広告市場の競争評価】

- 本年4月にデジタル広告市場の競争評価の最終報告が発表されており、そちらの課題⑩パーソナルデータの取得・利用に係る懸念の対応については、電気通信事業における個人情報保護に関するガイドラインなどの見直しにより対応する、ということとされている。【宍戸主査（第4回WG）】

論 点

- 米国
 - 【米国の個人情報保護関係規制】
 - ・米国では、公共部門と民間部門毎に、連邦や州の個別法（例：金融、子供のデータ、健康データ等）に個人情報に関する規定が設けられている。
 - ・FTC（Federal Trade Commission）は「不公正若しくは欺瞞的な行為又は慣行を禁止」するFTC法第5条に基づき、企業のプライバシーポリシーやITセキュリティ等に関しても規制・執行。
 - 【カリフォルニア州CCPA/CPRA】
 - ・カリフォルニア州消費者プライバシー法（CCPA：California Consumer Privacy Act）は2020年1月施行、7月当局による執行開始。CCPAにおいて、個人情報の収集やオプトアウト権に関しては、プライバシーポリシーへの記載だけでなく、これとは別に消費者への通知が必要とされる。例えば、個人情報の収集に係る通知を行う際のルール（専門用語を避けた簡潔でわかりやすい表現、小さな画面でも読みやすく目立つ形式等）を定め、通知内容として個人情報の種類一覧、個人情報の種類ごとの利用目的、オプトアウトページ及びプライバシーポリシーへのリンク（オフラインの場合はURL）等を定めている。ある意味階層表示の一つと分類できる。
 - ・2020年11月住民投票が行われ、CCPAを改定するカリフォルニア州プライバシー権法（CPRA：California Privacy Rights Act）が成立。通知項目としてクロスサイトトラッキングに関する事項や個人データの保存期間等が含まれることとなった。また、Third Party Cookie等を利用したクロスサイトトラッキングに対応した「共有するな」ボタンの義務化が定められた。
 - 【NIST Privacy Framework】
 - ・米国国立標準技術研究所（NIST）によってNIST Privacy Framework（NIST PF）は、個人のプライバシー保護を実現する上で参考にすべき枠組みとして、セキュリティ分野の枠組みであるNIST Cybersecurity Framework（NIST CF）の姉妹編として作成され、NIST CFとNIST PFをシームレスに統合した文書としてSP800-53が提示されている。この中で、同意取得を行う際の推奨手法として、同意をよりカスタマイズするTailored Consent、ジャストインタイムの同意、同意の撤回などを記載。通知を行う際の推奨手法として、ジャストインタイムの通知などを記載。プライバシー影響評価についても言及している。

これまでの主な意見

【米国】

【カリフォルニア州CCPA/CPRA】

- CCPA規則においては個人情報の収集やオプトアウト権に関する消費者への通知はプライバシーポリシーとは別に消費者への通知が必要とされる。例えば、個人情報の収集に係る通知内容は、収集する個人情報の種類、利用目的、オプトアウトページのURL、プライバシーポリシーへのリンク等とされる。【NRI(第22回PF研)】
- CCPA規則では利用規約やプライバシーポリシーの作成・開示とは別に、プライバシーポリシーの中から重要なものを別のリンクとして表示して消費者へ通知することを州法として義務づけている(CCPA通知、オプトアウトリンクなどとして表示)。これもある意味階層表示の一つと分類できる【小林構成員(第2回WG)】
- CPRAにおいて「共有するな」ボタンの義務化があり、Do not tracking2.0という言われ方をしている。そういう仕組みの提案がある。【寺田構成員(第22回PF研)】

【NIST Privacy Framework】

- NIST Privacy Frameworkに係るSP800-53文書において、同意や通知に関する具体的に推奨される手法として、Tailored Consent、ジャストインタイムの同意、同意の撤回などICOやCNILと同様の工夫が示されている。NIST Privacy FrameworkのCoreにおいて、8つ定められており、1-5がPrivacy Framework独自で通知・同意取得に当たりプロセスをきちんと確立し社内で浸透させましょうという形の規定がされている。6-8はCybersecurity Frameworkと重複。【NRI(第22回PF研)】

1. (3) 海外動向

論 点

- EU
【GDPR】
 - ・EUでは、個人データやプライバシーの保護を1995年から適用されていた「EUデータ保護指令（Data Protection Directive 95）」より厳格に規定し加盟各国に直接適用する法として、一般データ保護規則（GDPR：General Data Protection Regulation）が2018年5月に施行された。
 - ・GDPRの規定に関して、同意、透明性、自動化された個人に対する意思決定とプロファイリング、データ保護影響評価（DPIA）、データポータビリティの権利等についてガイドラインが定められ、詳細に解説されている。
 - ・同意については、「同意に関するガイドライン」においてGDPR第4条(11) に規定する有効な同意の要素である、「自由/自由に与えられた」、「特定の」、「説明を受けた」、「不明瞭でない意思表示」について解説し、情報を提供する在り方や有効な同意を得るための追加的条件（同意の証明、同意の撤回）を定めている。
 - ・透明性は、市民が自らに影響を及ぼすプロセスについて理解し、必要に応じてこれに意義を唱えられるようにすることで、そうしたプロセスへの信頼を生み出すためのものと位置づけられている。「透明性に関するガイドライン」において、GDPR第12条に規定する「簡潔で、透明性があり、理解しやすく、容易にアクセスできる」、「明瞭かつ平易な文言が使われなければならない」などについて解説している。
情報全体を包括的に提供する要件がある一方、その情報を簡素で、透明性があり、理解しやすく容易にアクセスしうる形式でデータ主体に提供するという要件を両立する観点から、階層的なプライバシーステートメント/プライバシー通知、プライバシーダッシュボード、ジャストインタイムの通知、アイコンなどが手法として推奨されている。
対象とする者の平均的な人々に理解されるものであることが求められ、ユーザーインターフェイス/通知/ポリシーなどの有効性について確信できない場合にはユーザーによる公開討論、可読性テスト、業界団体・消費者擁護団体・規制当局との対話の仕組みを通じた試験を行うことができるとされている。
アプリの場合ダウンロード前やダウンロード後 2 タップ以内にアクセスでき、アプリ固有のプライバシー情報を示すことなどが示されている。
 - ・GDPRはプロファイリング及び自動化された個人に関する意思決定が個人の権利に正当化されない影響を与える形で使用されないことを確保する規定を導入している。

1. (3) 海外動向

論点

【GDPR (つづき)】

- ・実装例を含め国際的なベストプラクティスを見るとよい。

(参考) 英国データ保護機関 (ICO: Information Commissioner's Office) による推奨される通知・同意取得における工夫: ①階層的アプローチ、②ダッシュボード、③ジャストインタイム、④アイコン、⑤モバイル及びスマートデバイスの機能性の5つの手法を公表。また、仏国データ保護機関 (CNIL) もGoogleのAgreementの中にプライバシーポリシーの仕組みとして階層的アプローチ

【ePrivacy指令/ePrivacy規則案】

- ・2002年のePrivacy指令に基づきCookie設定について情報提供、拒否権提供が義務づけられ、2009年同指令改正によりCookie設定について同意取得を義務付けた。2018年GDPRにより同意の要件が厳格となった。
- ・EU閣僚理事会でePrivacy規則案について合意され、2021年2月に公表された。EU閣僚理事会及び欧州議会による正式な立法手続が開始されている。
- ・ePrivacy規則案は、GDPRの特別法。電子通信サービス (ECS) 及び利用者の端末装置の情報の取扱いを規制。
- ・域外適用の明文化 (第3条)、規制対象となる電子通信サービスの範囲拡大・適用対象の明確化と電子通信データ処理を規制 (第5条～第7条)、端末装置のデータ処理・蓄積機能の利用、端末装置からの情報取得を規制 (第8条「いわゆるクッキー等規制」) を規定。クッキー等に係る同意取得方法 (第三者による代行やブラウザ設定による同意も可能)、同意を取得せずクッキー等を設定できる場合の明確化、同意証明方法、同意撤回権の通知等を明確化している。同意がなくとも「正当な利益」で広く許容されるという考え方は採用されなかった。
- ・欧州司法裁判所の考え方が取り込まれており、最初からチェックされたチェックボックスを示し利用者が同意を拒否するためチェックを外さなければならない状況では有効な同意は取得しえないとされている。また、広告最適化のためにThird Party Cookieを設置するウェブサイト管理者は、当該Cookieの設定元の第三者であるネット広告代理店、ソーシャルメディアなどとともに、GDPR上の共同管理者の立場に立ち、個人データの利用目的について利用者に情報提供し、利用者から同意を取得する義務を負う。

1. (3) 海外動向

論点

【DSA（規則案）】

- ・2020年12月に公表されたDigital Service Act（DSA）（規則案）において、オンライン広告の透明性確保に関するオンライン・プラットフォームに対する規律（広告であること、広告主及び広告表示決定に用いられた主なパラメータ等を表示する義務）、超大規模オンライン・プラットフォームに対する規律（広告表示から1年後まで広告内容・広告主・広告表示期間・使用された主なパラメータ・受領者総数に係るデータベースを編纂・APIを介して一般に利用可能とする義務等）が提案されている。オンライン広告の透明性をさらに向上させるため、行動規範の策定を奨励・促進。
- ・欧州委員会は、超大規模オンライン・プラットフォームがDSAの規則を実施し遵守しているかどうかをモニタリングし、不遵守の場合などには罰金・違約金などを課すこともできるとしている。

これまでの主な意見

【EU】

【GDPR】

- CNILのGoogleに対する制裁の中でも透明性ある情報提供という中で、プライバシーポリシーの仕組みとしてレイヤードアプローチがアグリーメントの中に含まれていた。GDPRの透明性のガイドラインの中に、レイヤードプライバシーポリシーのアプローチに関する在り方がかなり詳細に記述されており、やり方として参考になると思われる。実装例もあると思われる、国際的なベストプラクティスを見るとよい。【生貝構成員（第21回PF研）】
- GDPRの通知・同意取得に当たって推奨される方法や留意すべき事項は、透明性と同意のガイドラインにおいて解説されている。GDPR第12条「簡潔で、透明性があり、理解しやすく、容易にアクセスできる方式」の実現のためにガイドラインで示された推奨される通知方法・工夫の例として、階層的なプライバシーステートメント、丁寧な説明、公開討論・消費者テストの実施、トップページからのタップ数等がガイドラインで示されている。【NRI（第22回PF研）】
- 「プロファイリング」は「自動化された決定」の一類型であり、推知することだけを指すわけではない。権利利益侵害というのも迷惑メールとかそういう話ではなく、GDPRのGLでも差別されるような類型が多い。一番多いのは保険とか、あと就職差別とか学校とかいう類型で、日本だと、消費者裁判特例法でやったような男女差別（医大の入試等）。そういうところをGDPRだと、自動化された決定のところで読んでいたりしている。【板倉構成員（第4回WG）】
- GDPRにおけるプロファイリングの定義は、「自然人と関連する一定の個人的側面を評価(evaluate)するための・・・個人データの自動的な処理」となっている。【山本主査代理（第4回WG）】

1. (3) 海外動向

これまでの主な意見

【GDPR (つづき)】

- GDPRを踏まえ、より効果的に通知・同意取得を行うことができる工夫として、英国ICOにおいて推奨される通知・同意取得における工夫は、①階層的アプローチ、②ダッシュボード(この延長としてCMP等もある)、③ジャストインタイム通知、④アイコン、⑤モバイル及びスマートデバイスの機能性の5つの手法を挙げている。【小林構成員(第2回WG)】

【ePrivacy指令/ePrivacy規則案】

- 欧州においてGDPR及びePrivacy指令に基づきCookie取得に際して同意が求められている。ICOガイドラインにおいて、Cookie取得に同意しないとウェブ画面を閲覧できない同意画面(クッキーウォール)や黙示の同意、デフォルトオンは認められないとされている。CNILガイドラインにおいても、階層的な表示が有効とされ、同意取得に当たり個人を誘導することがない形が推奨されている。【NRI(第22回PF研)】
- この分野はハードローとソフトロー、そのどちらともつかないような様々な規範というのが非常に複雑に存在しているといった中で、ePrivacy規則は今日のテーマのほとんどを1つのルールブックとしてまとめようとする試みであり、まさに規範そのものの技術進化に合わせたアップデートというところを含めて、どうルールブック全体の見通しをよくしていくかということが改めてこの分野でも重要と感じた。【生貝構成員(第1回WG)】
- ePrivacy規則案について、EU加盟国間で合意成立・立法手続開始を行っている。域外適用の明文化(第3条)、規制対象となる電子通信サービス(ECS)の範囲拡大・適用対象の明確化と電子通信データ処理を規制(第5条～第7条)、端末装置のデータ処理・蓄積機能の利用、端末装置からの情報取得を規制(第8条「いわゆるクッキー等規制」)を規定。同意を取得せずクッキー等を設定できる場合の明確化、クッキー等に係る同意取得方法(第三者による代行やブラウザ設定による同意も可能)、同意証明方法、同意撤回権の通知等を明確化している。アカウント乗っ取り等を検知するためのセキュリティ目的利用も明記された。【IIJ(第2回WG)】
- 端末装置が有する処理機能の利用というのが新たに規則範囲に加えられた。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る。グーグル社のPrivacy Sandboxのように端末装置でAI処理を利用したターゲティング広告やIoT機器やコネクテッドカー等についても対象となる可能性が出てきた。【IIJ(第2回WG)】

これまでの主な意見

【ePrivacy指令／ePrivacy規則案（つづき）】

- eプライバシー規則案において、欧州司法裁判所の考え方が取り込まれており、ウェブサイト管理者は、クッキー設定元の第三者であるネット広告代理店、ソーシャルメディアなどとともに、GDPR上の共同管理者の立場に立ち、個人データの利用目的について利用者に情報提供し、利用者から同意を取得する義務を負う。また、あらかじめチェックが入れられたチェックボックスを示し、利用者が同意を拒否するためにはこのチェックを外さなければならない状況では、有効な同意は取得しえないとされている。また、同意がなくとも「正当な利益」で広く許容されるという考え方は採用されなかった。正式な立法手続に移りつつある。【森構成員(第4回WG)】

【DSA（規則案）】

- 2020年12月に公表されたDigital Service Act(DSA)案において、オンライン広告の透明性確保として、オンライン・プラットフォームに対しては広告であること並びに広告主及び広告表示決定に用いられた主なパラメータ等を表示する義務、超大規模オンライン・プラットフォームに対しては広告表示から1年後まで広告内容・広告主・広告表示期間・使用された主なパラメータ・受領者総数に係るデータベースを編纂・APIを介して一般に利用可能とする義務が示された。また、オンライン広告の透明性をさらに向上させるため、行動規範の策定を奨励・促進する。【MRI(第24回PF研)】
- 欧州委員会は、超大規模オンライン・プラットフォームがDSAの規則を実施し遵守しているかどうかをモニタリングし、不遵守の場合などには罰金・違約金などを課すこともできるとしている。【MRI(第24回PF研)】

論 点

- ISO/IEC
 - ・ISO/IEC29184（消費者向けオンラインサービスにおける通知と同意・選択）において、レイヤードアプローチを推奨。通知は処理の根拠に関わらず常に必要でありその内容は第三者にも示されるべきであると考えられる。同意は適切な状況において、PII主体に十分な情報が与えられた上で自由にされる必要があり、意図的な行動により同意を得るとともに、同意の修正や撤回が簡単にできることが望ましい。
 - ・付属書において、PCやスマートフォンで同意を得る場合のユーザインタフェースの例や、同意領収書（Consent Receipt）又は同意記録（Consent Record）の例が示されている。

これまでの主な意見

【ISO/IEC】

- ISO/IEC29184の議論の中では以下のようにされた。同意の取得には考慮点と限界が多く、可能ならば、他の適法な根拠を使った方が良い。そうすることにより、同意によらなければならないものは、同意を求める事自体が例外的なものとして個人に対する注意喚起になる。一方、通知は、処理の根拠に関わらず常に必要であり、その内容は第三者にも示されるべき。【崎村構成員（第21回PF研）】
- 分かりやすいポリシー、プライバシーノーティスの事例として、ISO/IEC29184で実際に求められているレイヤードアプローチにより、簡単なものを出し、詳細はこっちを見て下さいという形を推奨している（NTTドコモの事例）。EDPB（European Data Protection Board）やプラットフォーム事業者も検討に参加しており今後の変化に期待。【崎村構成員（第21回PF研）】

論 点

- 主要な電気通信事業者及びプラットフォーム事業者における利用者情報の取扱いについて、利用者情報の取扱いの状況、利用規約・プライバシーポリシー、アプリやサイトを經由した情報収集の状況、他社へのデータ提供、他社との連携の状況、サードパーティーによる情報取得への対応方針、アプリ提供マーケット、PIA・アウトカムについての考え方についてヒアリングシートへの記入及びモニタリングを行った。主な論点は下記のとおり。
 - ・ プラットフォーム事業者による利用者情報の取扱いの状況はどのようになっているか。【項目1】
 - ・ 利用規約やプライバシーポリシーの内容はどのようになっているか。特に、各事業者において様々な形で利用者へ分かりやすく伝えるための工夫、透明性確保のための工夫はどのようになっているか。（階層的アプローチ、ダッシュボード、ジャストインタイム、アイコン、モバイル及びスマートデバイスの特徴の利用等プライバシーポリシーにおける工夫はどのようになっているか。）【項目2(1)、(2)】
 - ・ ユーザーテストの実施や有識者の意見を聴くなどしながら対応が行われているか。利用者にとってそれぞれ異なる各取組を見つけにくい点やより分かりやすくするための課題があるか。【項目2(2)】
 - ・ 利用者が利用者情報の提供や利用を希望しない場合のオプトアウト等、利用者による事後的なコントロールの提供状況はどうなっているか。データポータビリティについてどのような取組を行っているか。（オプトアウトやデータポータビリティがある場合、利用のしやすさに課題はないか）【項目2(3)、(4)】
 - ・ 位置情報などプライバシー性の高い情報についてについてスマートフォンやウェブから取得する際に、どのような形で利用者の同意を得た上で、どのような配慮を行っているか。
 - ・ 他アプリやサイトを經由しどのように情報収集を行っているか。【項目3】他社へのデータ提供、他社との連携の状況はどのようになっているか。【項目4】サードパーティーによる情報取得に関してどのような対応方針か。【項目5】
 - ・ アプリ提供マーケットにおいて、アプリ提供者にどのような働きかけをしているか。【項目6】
 - ・ PIAについてどのように実施されているか、利用者へ与える影響（アウトカム）についてどのように考えてサービス設計をしており、利用者への説明が行われているか。プロファイリングがどのように行われており、どう使われているか。【項目7】

項目1 利用者情報の取扱いの状況について

項目2 利用規約・プライバシーポリシーについて

(1) プライバシーポリシーの内容

(2) 透明性確保のための工夫

(3) オプトアウトやダッシュボードの導入状況

(4) データポータビリティ等への取組状況

項目3 他アプリやサイトを經由した情報収集の状況

項目4 他社へのデータ提供、他社との連携の状況

項目5 サードパーティーによる情報取得への対応方針について

項目6 アプリ提供マーケットについて(※アプリ提供マーケットを運営している場合)

項目7 PIA・アウトカムについての考え方

論 点

【利用者情報の取扱いの状況】

- ・提供するサービスや事業モデルやデータ取扱いに当たっての考え方等に応じて、個別の電気通信事業者やプラットフォーム事業者の取得している情報がそれぞれ異なっている。広範な取扱いの全体像を一般の利用者に説明・理解させることは容易ではない場合も多い。

【利用者へ分かりやすく伝えるための工夫、透明性確保のための工夫】

- ・各事業者において、プライバシーポリシーだけでなく、プライバシーポリシーの内容を分かりやすく簡潔に説明したプライバシーセンターを設けたり、プライバシーのガイダンスやヘルプセンターを設けるなど説明を工夫している。
- ・アカウントの設定画面等から、利用者が利用者情報の取得や第三者提供や連携を含む取扱いについて事後的に把握・管理できるようにしている事業者もある。
- ・利用者がプラットフォーム事業者による情報取得や取扱い、第三者提供や連携の影響（集められる情報、利用目的、利用されるリスク等）を簡単に把握できることが重要ではないか。

【利用者や外部からの意見、ユーザーテスト】

- ・利用者は多様であり、背景、知識、経験などが異なることを踏まえ、ユーザーテストなども活用しつつ、利用者が理解できるように、多様な方法を用意する必要があるのではないか（例えば、金融商品は法律の中で消費者の多様性を考慮した規制がある）。
- ・消費者が想定しづらいものやプライバシー性が高い情報の取得等について、注意喚起をする仕組みが必要ではないか。
- ・情報開示が進展する中で、情報開示の視点で外部レビューやモニタリングを行っていくことが重要ではないか。

これまでの主な意見

【データ取扱いに当たっての考え方】

- データ最小化はとても重要な考え方で、アップル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る。しかし、利用者にとってとても分かりづらく、プラットフォーム側としても実施するのが難しいものだと思っている。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。【高橋構成員(第2回WG)】
- 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いる。法律の専門家やプライバシーエンジニアやディ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ことはこの段階から議論する。【Apple(第2回WG)】
- そのうちの一つにデバイス上での処理というものがある。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うが、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いる。顔認証に関して、デバイス上にテクノロジーが載っているので、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、純粹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いる。【Apple(第2回WG)】
- もう一つがマップの話で、Appleの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いる。それを使ってサーバーと通信を行うことになるので、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。【Apple(第2回WG)】
- データの最小化に関わるこれら2つの事例のように、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、アプリでも同じことができる。【Apple(第2回WG)】
- プライバシーとセキュリティは中核であり、Google製品を通じ包括的にこれらの保護を提供するようにしている。利用者が自分のプライバシーを簡単に管理できるようにするというコミットメントをしている。ユーザーの個人情報を誰に対しても決して販売しない。広告のパーソナライズのためにセンシティブな情報(人種、宗教、性的指向、健康など)を利用しない。【Google(第3回WG)】
- パーソナル化された広告によって自由でオープンなウェブが可能となっている。広告主やクリエイターがユーザーにとって有用なコンテンツを無料か低料金で提供することをサポートしている。【Google(第3回WG)】

これまでの主な意見

【データ取扱いに当たっての考え方（つづき）】

- ウェブ上のThird Party Cookieに替わるプライバシーに配慮した代替案について、新たなアプローチであるPrivacy Sandboxを提案している。Privacy Sandboxは、個人的に特定可能であるeメールのハッシュ化や個人を特定するクッキーの暗号化ということではなく、Privacy Sandboxの中の一つのツールであるFLoCにおいて、**プライバシーを特定する情報はサービスの中から取り除きたいというアプローチをとろうとしている**。個人が特定されるものを取り除いて同じ興味関心をもつコホートの中に入れている。そして、そのコホートのユーザーグループごとに広告などのサービス提供を行っていく。【Google(第3回WG)】
- (FLoCのサイズについては、) 具体的にどれくらいのサイズになるかというレンジは未定であるが、我々が提供する製品のユーザーの多様なレンジをFLoCに反映したいと考えているため、何千単位のユーザーのレンジになるものと思われる。【Google(第3回WG)】
- 現在何とおりの方法で対応を計画しようと考えている。1点目として、**オプトアウトできるようにする**。つまり、**パーソナライズされた広告の表示を求めないユーザーは、完全にオプトアウトできる**。その広告を受け取らないという選択肢を用意することである。あるいは、**ユーザーが見たくない広告があった場合には、それを完全にオフにすることができる**。これを行うことによって、FLoC側で、違ったものを割り当てていた、この人に合っていない、と**学習し、それに合わせて調整を行う**。【Google(第3回WG)】
- 電話番号やメールアドレスのアップロードについては、LINEとして使っているということはないということだが、**LINE広告のリターゲティングタグや広告のタグ、SDKについては、LINEとしても利用しているということだった**。広告主サイトに訪れると、LINEが情報を取得するということを広告主サイトに行った人が分かるように、**LINEとして、広告主サイトでこういうふうに表示しようとか、こういう同意を取ろうといったことを広告主に何かお願いをしているのか。お願いしているのであれば、それが実際に行われているかということを確認しているのか**。【太田構成員(第4回WG)】

これまでの主な意見

【利用者への分かりやすく伝えるための工夫、透明性の確保】

- 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、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いる。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。いただいた御意見等を踏まえ、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。【ヤフー(第2回WG)】
- Yahoo株式会社の姿勢は、利用者のデータを活用する、という事実をはじめ、データ連携先など全て隠さずに見せることで、正直な会社という信頼を得られているのだと思う。(当該調査で利用者コメントにあったとおり。)、Yahoo株式会社のプライバシーセンターは例示も含めてかなりわかりやすく記載されていて、良いと思った。【沢田構成員(第2回WG)】
- 面倒くさがりの利用者は、実際には、熟慮して個別にオプトアウトしたりはしないかも知れないが、不都合なことを隠していないと思えることがまず重要で、Apple Inc.のように利用者を選択を委ねる方法も、透明性確保の一環と捉えられと思った。もちろん、しっかりと詳細を知りたい利用者には情報開示は何よりも重要。【沢田構成員(第2回WG)】
- データの収集や使用方法、利用者自らによるデータ管理について、分かりやすい情報提供をするように努めている。例えば、新規アカウント作成時に、Facebookで共有された情報をコントロールされるための様々な機能を紹介するプライバシーのガイダンスやプライバシーツアーを提供している。ヘルプセンターにおいて、広告支援サービスがどのように機能しているのか仕組みについても広範に情報を提供している。より詳しい情報としてプライバシー基本ガイドを提供。【Facebook(第3回WG)】
- 昨年夏にはプライバシーチェックアップという機能など広告の設定に焦点を当てた新しいモジュールを用意。また、透明性。明瞭性、コントロールという3つの原則に基づき、なぜこの広告が自分のフィードに表示されている理由を示しこれをコントロールする機能を、利用者が容易に使えるような形で用意している。【Facebook(第3回WG)】
- ユーザーのデータの収集や利用について、Googleアカウントの設定の中でユーザー自身が、削除(頻度や自動削除など)の設定を行うなど、自分のデータをどのように共有するか管理することができる。【Google(第3回WG)】

これまでの主な意見

【利用者への分かりやすく伝えるための工夫、透明性の確保（つづき）】

- プライバシーポリシーの内容を分かりやすく簡潔に説明した**プライバシーセンター**を設けており、プライバシーポリシーのポイントや問合せ窓口などについて掲載。プライバシーポリシー以外に、個別のサービスや機能を利用する場合に同意を取得する場合に、例えば通信の秘密に関する同意を取得する際に**簡潔な表示と詳細が確認できる画面の2画面構成**としている。【LINE(第4回WG)】
- パーソナルデータを外部連携して第三者提供する際には、**アイコンなどを利用して提供先の第三者がどこなのか、提供する情報は何か分かりやすく表示**した上で、下の許可ボタンを押して第三者提供の同意を取得するようにしている。また、**LINEアプリ内の設定から、簡単に外部アプリとの連携を解除**することが可能となっている。【LINE(第4回WG)】
- 論点整理に関して、プラットフォーム事業者間で、利用者への実際の影響のでこぼがないかどうかの整理を要望。利用者の保護が大事だという話があったが、基本的に利用者がプラットフォーム事業者からの**情報取得の影響を簡単に把握**できて、結果として、**どのプラットフォームを使っても不利益を被らないことが大事だと考えている**。影響というのは、具体的には**集められる情報、その利用目的、利用されるリスク**などに代表される。【高橋構成員(第4回WG)】
- 位置情報に関しては、位置の精度や移動履歴の期間などで考察できる。これは第1回目の位置情報検討のプレゼンでまとめている。取得手段が異なっても利用者にとって**同じことが起きている現状**があり、マクロにまとめる必要がある。これらの整理によって、**プラットフォーム事業者からの影響が類型化され、利用者の理解が容易になる**ことを想定。また、こういった類型化は変化が激しいイノベーションの起きている分野であるため、**柔軟かつ高頻度に把握し続ける必要**もある。【高橋構成員(第4回WG)】

これまでの主な意見

【利用者やステークホルダー・有識者など外部からの意見の反映、ユーザーテストの実施】

- パーソナルデータ憲章の策定に関連して、パーソナルデータ憲章運用委員会やPIAを運営する中において、有識者会議との連携しステークホルダーの方との連携を現在行っている状況。【NTTドコモ(第1回WG)】
- 第三者委員会を設けており、その中に消費者団体の代表の方にも入っていただき、ご意見をいただくようにしている。また、お客様に対して公開しているような公開しているようなプライバシーポータル構築に向けては、ユーザー調査などを通してユーザーのご意見も取り入れながら日々改善している。【KDDI(第1回WG)】
- ユーザーへのアンケートを事前に実施したりして、今後どういう文言で、例えばわかりやすさがきちんと伝わるかやそういったところを行う点と、外部の有識者に入っていて、そこからのご意見をいただいている。【ソフトバンク(第1回WG)】
- 外部の有識者の方からご意見いただきながらまとめている。【楽天モバイル(第1回WG)】
- 位置情報の業界の会社が集まり、LBMAという団体を作り、プライバシーのガイドラインを作って展開し、毎年監査等も行うこととしている。【Agoop(第3回WG)】
- ユーザーのテストについて、当然やっていて、また、今四半期というか、半期に大規模なものをやろうとしている。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る。【ヤフー(第2回WG)】
- ユーザーへの影響について、PIAを実施したり、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、DPOが個々の取組一つ一つに入っていて、消費者の代表として言うなどあるが、しっかりしていきたいと思っている。影響が分かるかどうかというところはなかなか難しく、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。お客様の期待を裏切るといのが一番は我々の怖いことでもあるので、私たちの中でどういうようなことを情報開示していけばいいのかということ真剣に考えて、取組を進めてまいりたいと思っている。【ヤフー(第2回WG)】
- プライバシーレビューを通じプライバシーを考慮しながらプロダクトをデザインする工夫を実装。デザインの専門家などとも関わりを持ちながら、ユーザーに透明性、コントロールを提供するための課題を研究し、「人を中心に据えたプライバシーデザインの在り方」というホワイトペーパーを昨年7月発表。個人情報に関する通知の一般的アプローチはない、利用者に対して、情報の種類、商品やサービスの種類、利用者自身の特性に応じて様々な手法で行うことが必要であり、情報を階層的に適切なタイミングで適当な文脈の中で提供することが認められるべきと考えている。【Facebook(第3回WG)】

これまでの主な意見

【利用者やステークホルダー・有識者など外部からの意見の反映、ユーザーテストの実施(つづき)】

- 第1点目に、利用者が理解できるようにということは色々な場で議論をされるが、その前提として実は利用者は多様であり、背景だとか知識や経験も違うため、やはりそれを踏まえる必要がある。そうしたときに、方法も、これが利用者にとって、利用者が理解できる方法の1つというふうにするのではなくて、やはり多様な方法を用意する必要があるのではないかなと思う。参考として、金融商品の販売に関して、法律の中で消費者の多様性を考慮した規制があるため、そういったことも検討すべきではないかと思っている。【古谷構成員(第4回WG)】
- 第2点目は、利用者側がデータの複雑な利用のされ方であるとか、同意が分かりにくいとか、色々な問題があることを考えると、注意喚起といったところも非常に必要だと思うので、必要に応じて、注意喚起ができるような重要な点、不利益が、場合によってはかかってしまう可能性があるところで、消費者が気づかないといったようなところは、注意喚起する仕組みというのは、必要だと思う。【古谷構成員(第4回WG)】
- 第3点目は、情報開示であり、事業者の取組が、実際にどのような考え方でデータが取得されて、利用されたかと、あるいは問題が発生したのか、しなかったのかというようなことも含めて、どのように改善したかといったようなレビューがやはり必要。理想的には外部レビューだが、実はこの分野のデータに関してはあまり見られないかと思うが、サステナビリティに関する分野は、実はそういったレビューであるとか、情報開示の分野が急速に進展しており、やはり同様に、そういった情報開示の視点でレビューをしていくという観点が必要ではなかろうかと思っている。【古谷構成員(第4回WG)】

論点

【オプトアウトやデータポータビリティ】

- ・オプトアウトの提供の有無については、全ての事業者が回答。オプトアウトの仕組みはダッシュボードやアカウント設定などを通じて大半の事業者において提供されている。また、この他、データの保存や保存期間、広告への利用の設定などを通じ、データの取扱いを一定程度コントロールする仕組み等を提供している場合がある。
- ・オプトアウトを行うと、オプトアウトした情報の取得が停止されるとともに、オプトアウト前に取得されたデータは利用されなくなるとしている。一方、当該データが消去されるのかどうかははっきりしない場合もある。
- ・データポータビリティの提供の有無については、全ての事業者が回答。海外プラットフォーム事業者は全てデータポータビリティに対応済との回答であり、利用者のコンピューターへのダウンロードや一部の第三者への転送等が可能とされている。携帯電話事業者及び国内プラットフォーム事業者はデータポータビリティに対応していない又は一部のデータのみダウンロード可能との回答であった。
- ・改正個人情報保護法の施行に向け、電磁的記録による開示請求対応の準備を進めるとの回答が複数みられた。

【位置情報等】

- ・位置情報はプライバシー性の高い情報として、厳密な管理を行っている。位置情報の種類に応じて、取得する際に同意を取得するかオプトアウトを提供等をしている。住所等を推定されないように、位置情報の加工や取扱いにおいても注意が払われている。端末からGPS等の位置情報を取得する場合、OSの機能により同意取得が行われる。
- ・一方、Beaconや店舗における電子マネー決済など端末情報と別の情報を組み合わせて位置情報が取得できる手段が増えてきている。これら位置情報についての通知・公表や利用者の同意の在り方などについて新たな課題がある。

【デジタル広告】

- ・広告主がメールアドレスや電話番号をアップロードし、ハッシュ化した上で当該事業者が保有するメールアドレスや電話番号と突き合わせするタイプの広告サービスを提供する事業者がある。
- ・様々な形でクロスデバイスの情報が取得されており、一般利用者にとって全体像を理解することが容易ではない状況。また、広告サービスを利用するサイト運営者や広告主等が、自らを經由し提供される個人情報等について、利用者に対してどのような説明や同意取得等をするべきかを必ずしも明確に把握・理解していない場合もあると考えられる。

論 点

【アプリ提供マーケット】

- Apple及びGoogleのアプリ提供マーケットは、アプリがアクセスしようとしている利用者情報について、利用者が十分な情報を得た上で判断できるように、アプリ提供者（デベロッパー）に義務付けを行ったり、情報提供を行うなどの支援を行っている。SPIを参照すべき政府のガイドラインの一つとして提示しているアプリ提供マーケットもあった。
- App Store Reviewガイドラインにおいて、アプリのプライバシーポリシーにおいて利用者情報の取扱いについて詳細に規定すること、データ収集についての同意取得や同意の撤回の提供、目的でデータの用途を十分説明すること、ユーザーのアクセス許可設定を尊重すること、不要なデータアクセスに同意するよう誘導や強制しないこと等を示している。
- Google API利用規約は、アプリ提供者が収集、使用、他社と共有する利用者情報について明確かつ正確に定めたプライバシーポリシーを提供し遵守することを義務づけている。また、明示的な同意なく、利用者の非公開データを第三者に開示すること、スクレイピング、データベース構築その他利用者情報の恒久的コピー作成等を禁止している。

【PIA】

- PIAの実施状況については、全ての事業者が何らかの形で回答。一方、独自のPIAを行っているとしているが、その基準が明確ではない場合がある。また、PIAの結果も公表されていない場合が多い。

これまでの主な意見

【オプトアウトの提供】

- オプトアウトすると、オプトアウト前に取得した位置情報は利用されなくなる仕組み。【NTTドコモ(第1回WG)】オプトアウト以後取らないことと加えて、オプトアウト以前に収集したデータについても利用を停止。【KDDI(第1回WG)】オプトアウト以降の情報に限らず、オプトアウト以前に預かった位置情報についても使用されない。【楽天モバイル(第1回WG)】
- サービスを無料で提供できているのは、パーソナライズド広告ビジネス、そこから得られる収益があるからであり、オプトアウトという機会は提供していない。一方、フェイスブック外のアクティビティや広告の設定という機能を通じて、消費者が自らのデータをコントロールする機会を提供している。【Facebook(第3回WG)】
- どのデータがGoogleに保存されるかユーザーが管理できる。初期設定では、18ヶ月で自動削除される設定や、特定の頻度(3ヶ月、18ヶ月)ごとに自分の情報を削除することもできる。Googleアカウントを作成する際に利用規約に同意するだけでなく、事後にもパーソナル化したサービスからのオプトアウトやパーソナル広告をやめることもできる。【Google(第3回WG)】
- ユーザーがデータの収集をやめたいときは、停止方法をホームページ公開している。【Agoop(第3回WG)】
- 通信の秘密に関する同意の取得とそのオプトアウト、位置情報に関する同意の取得とそのオプトアウトなどがいつでもLINEアプリ内で可能となっている。【LINE(第4回WG)】

【データポータビリティの提供】

- データポータビリティに関して、2018年からApple、Google、Facebook、Microsoft、Twitter等が連携し、Data Transfer Projectを実施。2020年には、Google PhotoやDropboxなどの他のサービスやアプリと連携し、Facebookの写真や動画のデータを転送・共有できる新しいツールを公表。2021年4月にはGoogle DocsやWordPressにも対応し、利用者がメモや投稿を転送・共有することを可能とした。【Facebook(第3回WG)】
- データは2種類のフォーマットでダウンロードされる。1つは機械の読み取りがより容易であるJSON、もう1つはHTMLフォーマット。このツールによりダウンロードされる類いのデータは、投稿されたもの全て、写真、プロフィール情報、それから友達のリスト等と、その他もある。完全なリストに関しては、ヘルプセンターにあるリストを確認いただける。【Facebook(第3回WG)】

これまでの主な意見

【データポータビリティの提供（つづき）】

- Data Transfer Projectは、個社と個社の間での直接のデータのやり取りを可能にする仕組みである。参加するに当たっては、参加を希望する事業者自身がエンジニアリング作業を行う必要がある。そしてまた、それぞれの移転するデータの種類に関しても、対応して参加する流れとなる。現実には大手企業間での実施、利用がリードしているが、小規模事業者の参加も実際にスタートしている。【Facebook（第3回WG）】
- データポータビリティについては、2007年から取組みを始めており、現在ではGoogle Takeoutというプロダクトができており、ユーザーのデータ、eメール、写真などを外に持ち出すことが可能。今後更にツールを開発してユーザーへの啓蒙ももっと行う必要があると認識。【Google（第3回WG）】

【位置情報】

- 直接的な個人情報である氏名、住所、電話番号などは一切収集せず、広告IDも収集していない。位置情報はプライバシー情報であるため、個人情報相当と定義し、厳密な管理を行っている。集めた位置情報を分析・加工して、人がいつ、どこに、どれぐらいの人の量がいるのか統計加工してデータを開発・提供している。まさに今、コロナ感染症対策というところで日々人流データとして、ニュース等も通じ人々への情報提供に活用されている。【Agoop（第3回WG）】
- 位置情報のデータを収集するときに関して、ユーザーベネフィットの設計をPIAの一環としてしっかりやっている。（利用者が位置情報を使う目的や機能に関する内容が利用者にとって利益がある形にあっていないと、単なるデータ収集になってしまう。）【Agoop（第3回WG）】
- 利用者から位置情報を取得する際には、利用規約に記載するだけではなく、それを抜き出して、個別のポップアップでどういったデータを取っているか、目的や第三者提供の有無も含めて個別に同意を取得することを徹底している。位置情報は、OS側でもパーミッションを取ることを強化しており、気づかずに位置情報が使われることはない設計になっていると思量。データを第三者提供する際には、居住地周辺の情報を秘匿化しデータを削除して提供。【Agoop（第3回WG）】
- データ取扱いについての社内ガイドラインを作り、外部提供LBMA時の承認フロー体制を構築し、定期的な外部監査を受ける（Pマーク、ソフトバンクグループ子会社監査、LBMA Japanによる遵守監査の3つ）を受けている。また社員の教育体制を徹底している。また、PIA評価についてもやっている。一貫通貫のセキュリティ担保を意識した設計をして、社会のためのビッグデータ価値を高め貢献していきたい。【Agoop（第3回WG）】

これまでの主な意見

【位置情報（つづき）】

- 位置情報を例にすると、お客様の端末の設定で、位置情報の送信を許可していない場合には、位置情報は送信されないとあるが、これはGPS又はOSの機能設定を前提に書かれていると思う。利用者がこのプライバシーポリシーに従って位置情報の取得を止めたとしても、Beaconや店舗QR決済などにより位置情報が取得できてしまう。直接的なセンサーやOS機能だけではなく、プロファイリングを含めて間接的な機能で取得する方法が色々出てきている。利用者はプロファイリングなどに関してなかなか想像が及ばないところなので、それを含めて包括的な書き方をするとよい。【佐藤構成員(第4回WG)】取得している位置情報は、基本的にはGPS位置情報。Payの決済履歴やBeaconの情報については、例えば、決済履歴であればこの店舗で決済を行ったという情報もわかるし、Beaconの情報もわかるが、社内では位置情報には分類していない。ただ、いずれも安全に管理している。【LINE(第4回WG)】

【デジタル広告】

- 広告主がメールアドレス情報又は電話番号情報を使用する権利を取得し、その上でハッシュ化された情報がFacebookのシステム上でマッチングされその形で使用されることとなる。広告主が彼らの顧客に関して持っている情報に関して適切な使用をするところに同意をもらっている。【Facebook(第3回WG)】
- Facebook外のアクティビティについてもコントロールが設定されており、このコントロールを通じて、Facebookが当該ユーザーのFacebook外アクティビティについてどのような情報を保有しているか、全て確認可能である。カスタムオーディエンスに関しては、作成の仕方は存在している。Facebookは、電話番号、メールアドレスは全てハッシュ化された形で受領するため、そのままの形で受領することはない。アップロードされた電話番号、メールアドレスは、ハッシュ化を通じてマッチングされている。【Facebook(第3回WG)】
- 広告配信のセグメントについては、例えばファッション好き、車好きといった関心の度合いと、ユーザーの年代、属性を掛け合わせた程度。ユーザーの健康情報、政治的な信条、宗教的なものなどの機微情報を推定するプロファイリングは行わないルールとなっている。PIAを行い、利用者に不利益を及ぼさないような内容になっているかどうかも確認している。【LINE(第4回WG)】

これまでの主な意見

【デジタル広告（つづき）】

- LINEとして取得する利用者情報、サービス利用に当たり取得する情報の2種類以外にも、LINE広告のリターゲティングタグが広告サイトに張られていて、LINEが情報取得している場合もあると考えられる。【太田構成員（第4回WG）】
LINEのポリシー等において、第三者からもパーソナルデータを取得するということは説明している。【LINE（第4回WG）】

【PIAの実施】

- 様々な他社様の事例や有識者の先生方のご意見も頂戴しながら、最終的には自社の中であるべき姿を検討して、現在の制度を作り上げている。PIAで行った評価については、現時点で公表していない。【NTTドコモ（第1回WG）】
- JIS規格されたPIAへの手法に準拠するわけではなく、参考にして、当社のデータ取扱い等の実情を踏まえプライバシー上の配慮が十分なされているか等を、サービス開始前に評価する運用フローを作成中。【KDDI（第1回WG）】
- 何か基準に則って何かのガイドライン等に則ってという形ではなく、弊社独自で外部の有識者の方も含めてご参考にさせていただいているという形。現時点で公表していない。【ソフトバンク（第1回WG）】

論 点

【利用者情報を取巻くグローバルな情勢の変化】

- プラットフォーム事業者等は、網羅的なプライバシーポリシーを作成するだけでなく、利用者情報の取扱いの説明について様々な工夫を行っている。しかしながら、一般利用者にとって理解・把握は困難である場合も多い。
- 生活にスマートフォン等が不可欠になる中で、利用者情報の質や量が拡大し、機微情報や機密情報も含まれる可能性。更に、スマートフォン等の利用者情報と、電子マネーを使った決済やBeaconなどの外部情報も結びつきうる。
- これら利用者情報等がクロスデバイスで取得・集積・分析され、プロファイリングやターゲティングも高度化・精緻化。商品広告の表示や効果測定のための目的だけでなく、様々なマイクロターゲティング、プロファイリング結果を踏まえた採用や与信などの個人に影響を与えうる意思決定にも用いられるおそれもあり、利用者情報を提供した結果の本人に対する影響・アウトカムを予め説明することが困難となる場合もある。このような利用者情報の取扱いが社会へ様々な影響を与える可能性が指摘される。
- このような情勢等も踏まえ、各国はクロスデバイスの情報の取扱いに関して、本人同意を求めたり、事後的な検証可能性を高めるための透明性確保や報告・公表義務を課すなどの規制強化を進めているところであり、グローバル展開するプラットフォーム事業者もこれに対応しつつある。
- 我が国においても、利用者保護の観点から、このような業界の状況やグローバルな規制状況なども踏まえつつ、適切な対応が求められるところ。

【利用者情報の適切な取扱いの確保】

- スマートフォンやタブレットなどの通信端末の位置情報や、ウェブ上の行動履歴、利用者の端末から発せられ、または、利用者の端末情報に蓄積される端末IDやクッキーなどの端末を識別する情報等については、通信の秘密やプライバシー保護の関係で、その適切な取扱いの確保のために、どのように規律すべきか。
- 異なるアプリやサイトを通じた横断的なパーソナル・データの取得・収集・分析に係る事項の開示についてどのように行うことが有用であると考えられるか。またプロファイリングについてどう扱うべきか。

論 点

【利用者情報の適切な取扱いの確保（つづき）】

- 第一に、アプリ提供者やウェブサイト運営者が、当該アプリやウェブサイトでどういう情報取得や情報提供が必要であるか検討し把握することが必要ではないか。第二に、これを踏まえ、利用者が理解できるように、取得する情報の種類や用途などに応じて、通知・公表又は同意取得、対象範囲、形式（個別同意・包括同意）等について検討を行う必要があるのではないか。
- プロファイリングの有無や情報利用による利用者へ与える影響（アウトカム）が重要であり、これを利用者に伝えていく必要があるのではないか。特に受けうる不利益についての情報が重要ではないか。PIAを考慮すべきではないか。

【プライバシーポリシーの工夫】

- プライバシー・ポリシー等について、分かりやすく見せるための仕組みや工夫というものを検討する必要があるのではないか。例えば、階層的な通知、個別同意、プライバシー設定の工夫は、プライバシーポリシーの読みやすさを高めるとともに、個人によるコントロールを高めること等を通じて、特に自己効力感が高く、抵抗感も強い利用者に対して効果的であるとともに、様々な性格の利用者の理解や安心に資するものではないか。簡略版の作成も有用ではないか。Consent Receiptのように自分が何に同意しているか事後的に分かることも有用ではないか。
- また、第三者提供、機微情報の取得・利用、通常は想定されない利用等は特に注意喚起をする仕組みが必要なのではないか。

これまでの主な意見

【アウトカム・プロファイリング・PIA】

- 同意についてどんどん細かくなり手続関係の話になるが、そもそもの同意の目的が忘れられ形骸的なものになってきつつあると感じる。同意を取るのに必要などんなデータ(位置情報等)か、利用目的か、第三者に提供・加工する等かなに重要なのか考えている。本当に重要なのはその結果利用者に与える影響、アウトカムではないか。手続論・ルールベースの話になってしまうが、アウトカムベースでもう一度見直してどう整理するか考える必要がある。グローバルの流れも、リスクマネジメントの考え方で(SP800-53等も)少しづつアウトカムベースに変わりつつあり、そのような視点を持つ必要がある【寺田構成員(第22回PF研)】
- 寺田構成員の意見に大賛成。アウトカムをしっかりと一度整理していく必要があると強く感じる。それと併せて、今までやってきている内容・手続論とどうやってそれらが結びつくかという点を最後はゴールとして考えて整理していくのを一度やるべきかなと思っている。【手塚構成員(第22回PF研)】
- アウトカムベースに賛成。手段を規制するのは限界があり、いたちごっこになるので、どういうアウトカムになってはいけないのかというアウトカムベースでやるように規制対象を変えていかないといけない。【崎村構成員(第22回PF研)】
- 全体のご報告を通じて、ある種のズレを感じた。例えば、JIAA様も含め、プライバシー保護等に向けて積極的に取り組みを行っており、それ自体高く評価しているが、他方で、それが本当に消費者の知りたいこと、社会のために本当に必要なことと合致しているのか、疑問がないではない。例えば、消費者が本当に知りたいのは、どのような情報が取得されるか、ではなく、取得された情報からどのような分析(プロファイリング)がされるのか、どこまで細かくセグメントが切られるのか(セグメントの粒度)なのではないか、こうした分析によりどのような不利益を受けうるか(例えば内定辞退率のプロファイリング・スコアリングは就職活動に影響しうる、政治的信条や心理的脆弱性等のプロファイリングは投票行動に影響しうる、など)、ではないか。しかし、現状、こうしたことについて、十分な透明性が確保されているとはいえないように思われる。【山本主査代理(第1回WG)】
- 情報分析(プロファイリング)による人権へのリスク、民主主義へのリスクが実体的に評価されるには至っていないように感じた。今後は、情報分析やセグメント化(ターゲティングの根拠)の透明性やリスク評価についても焦点を当てていくべきではないか。【山本主査代理(第1回WG)】

これまでの主な意見

【アウトカム・プロファイリング・PIA（つづき）】

- アウトカムベースでというところが出てくるが、本来は、その前にゴールベースということで目標を考えなければいけないのだが、ここは誰にとっても、ステークホルダーにとってモアベターだという話になってくると、公正な市場競争による淘汰を妨げるようなことも起こってしまうため、ちょっと時間をかけて考える必要がある。アウトカムベースに関しては範囲を絞れば、ある程度、考えられるのではないかと。例えば、同意と通知に関して調査されているが、これをいわゆるベストプラクティスとしてまとめて、PIAで参照できるようなものにしていくというような考え方がある。特に弱者に対する不利益とか差別が起きないように、ベストプラクティスを、考えていく。それを守れなければ、当然、規制等を考えるということかと思っている。【寺田構成員（第4回WG）】
- ユーザー情報を行動ターゲティングをして政治広告をする場合に問題があるのではないかと。1つは、公正な思想・政策の競争の観点ということ。もう一つは、個人に対する不当な刺激・誘導のおそれと、それによる弊害が大きいのではないかと、この2点の問題点が、行動ターゲティングによる政治広告にはあるのではないかと、このような政治広告は禁止すべきではないか。【森構成員（第4回WG）】
- 日本は通信の秘密により思想・信条の自由の一部を担保しているところがあり、行動ターゲティングと政治広告の関係というのは、恐らく今後、避けて通れない課題と思う。【佐藤構成員（第4回WG）】
- ここで禁止される政治広告というのは一体何なのかということについて、しっかり定義をする必要がある。特に公職選挙法上禁止される選挙運動のための有料広告の禁止との関係とか、いろいろ整理していく必要は今後出てくるだろう。さらに有料広告ではない記事やいわゆるインフルエンサーの投稿等についても、当然、投票行動というのは影響を受けるため、例えば、前堤となる政治的信条に関するスイッチ、プロファイリング、プロファイリングの言葉については、透明性も、今後は重要になるかなと思っている。【山本主査代理（第4回WG）】
- プライバシーポリシーの書きぶりが、端末側のその各種情報に関わるセンシング機能を前提として各種情報の取得可否を行っている。しかし、利用者がプライバシーポリシーに従いその各種情報の取得を止めても、プロファイリングを含めて、他の情報から間接的に取得できている状況。位置情報を含めて、各種情報を間接取得をしているのであれば、それをプライバシーポリシーに丁寧に記載して、必要があれば取得を停止する方法を記載させるべきではないか。【佐藤構成員（第4回WG）】

これまでの主な意見

【アウトカム・プロファイリング・PIA（つづき）】

- プロファイリングをしても、それが統計目的であれば、GDPR上は統計目的のほうの規律で、割と安全管理措置だけに寄ったようなものに規律が緩まる。日本でも、個人情報保護法の解釈では、統計目的の場合は利用目的に書かなくていいという、割とざっくりしたのがあって、実務的には重要だったりする。その辺の整理も含めて、統計目的というのは、手法がプロファイリングとか自動決定であっても、それは規律が違うのだという考え方は、参考になると思われる。(プロファイリングしても、統計目的である限りは、GDPRも規律を緩めている(89条、前文162ページ)【板倉構成員(第4回WG)】

【プライバシー・ポリシーの課題】

- プライバシー・ポリシーをめぐる大きな課題としては長文化が進んでおり非常に分かりづらい。長文のポリシーと、短いステートメントなどもあるが、ポリシーの分かりやすさと、分かりやすく見せるための仕組みや工夫というものを今後検討する段階に来ているのではないか。特にユーザーインターフェースのデザインや工夫による見やすさを考えるべきではないか。【新保座長代理(第21回PF研)】
- プライバシー・ポリシーを読まない、見ない、あるいはそもそも理解できない人も存在することも含めた対策を考えるべきではないか。分かる方には当然ちゃんとした説明が必要であるが、プライバシー・ポリシーを読ませることだけに専念するのではない別の対策というものを考えないといけないのでは。【寺田構成員(第21回PF研)】
- プライバシー・ポリシーに関し、全部読めと言われても多分無理ではないか。普通というのが何かあって、普通と違うところを見せる形だと非常にシンプルになる。例えば、アプリケーションの種別等を考えてそのスタンダードを作り、差分を一番最初に表示する方法を考えていくと効果的ではないか。【宮内構成員(第21回PF研)】
- 同意を求められる事項、その中でもアプリの情報、利用者情報がどこでどのような目的で使われているのかといった事項については、レッドやグリーンなど何らかのカテゴリ化できないものか。特に第三者に提供されるもの、かなり微妙な機微情報や健康情報が提供されるなど一定のカテゴリのものについて、特に注意喚起をするような仕組みでプライバシー・ポリシーや簡略化されたステートメントに注意喚起するというような仕組みをどこかに導入できないか。【大谷構成員(第21回PF研)】

これまでの主な意見

【プライバシーポリシーの工夫（階層的な通知等）】

- 利用者情報の取扱いについて、利用者と事業者間のコミュニケーションがより円滑になり利用者により理解し安心してもらえる通知・同意取得の工夫について5つの類型（階層的な通知、タイムリーな通知、個別同意、プライバシー設定、同意の証跡）に整理。通知・同意取得に対する利用者の考え方の違い（企業の情報利用に対する抵抗感、ネットサービスの利用における自己効力感、面倒と感じる気質）により、利用者を分類した上で、階層的な通知、個別同意、プライバシー設定の3つについて検証。【小林構成員（第2回WG）】
- 自己効力感が高く、抵抗感も強い利用者（Seg.1）は、先進的なネットサービスの利用に意欲的。抵抗感が強い利用者ほど、自身の情報の取扱いに敏感であり、内容に応じてサービスそのものの利用を忌避する傾向。通知・同意取得する際に、利用者の理解や安心に資する工夫を講じることは、先進的なサービスの利用意向の高い利用者へ訴求。階層的な通知、個別同意、プライバシー設定の工夫は利用者の理解や安心に資する。【小林構成員（第2回WG）】
- 具体的には、階層的な通知（目次（見出し）と詳細の工夫又は重要事項と全文の工夫）を講じると、利用者全体の2割強（Seg.1は約3割）が現状よりしっかり読むと回答。個別同意は利用者全体の6割強（Seg.1は約8割）が利用したいと回答し、実装に対してニーズが高い。プライバシー設定（ダッシュボード）は利用者全体の約7割（Seg.1は約8割）が利用したいと回答、自己効力感の低いグループでも5割以上の利用者が利用意向を示した。ネットサービスの健全な成長のために、利用者の理解や安心に資するこれらの通知・同意取得の工夫の普及が求められる【小林構成員（第2回WG）】
- 小林構成員の発表に関して、個別同意やプライバシー設定に対して、利用意向が高いことから、面倒と思うよりも、個人が自分でコントロールしたいことが明らかになっている。【太田構成員（第2回WG）】
- 欧州の消費者は、GDPRのような同意中心の規制アプローチを本当に望んでいるのか（面倒くさくないか）？と常々疑問に感じていたが、小林構成員の報告を伺い、自分が「企業の情報利用に抵抗感がありながらも面倒と感じる依存気質」だからだということがわかった。このような層にも、個別同意やプライバシー設定が好意的に受け入れられる理由は、それによって企業の姿勢（お任せしても大丈夫な相手かどうか）が判断できるからだと思う。【沢田構成員（第2回WG）】
- 利用者にとって分かりやすく安心できる通知・同意の取得は重要。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素晴らしい。一方、利用者の考え方だけではなくその時の状況、サービス、相手などによっても影響を受けるため、考え方だけで決めるのは危ない部分がある。【古谷構成員（第2回WG）】

これまでの主な意見

【プライバシーポリシーの工夫：簡略版の作成】

- 簡略版を載せない理由として、法務部がプライバシーポリシーは自組織を守るためであって、個人を守るためではないとして強く拒否する事例を聞いている。【崎村構成員(第21回PF研)】
- 簡略版については義務化されていないので作成しない側面と、一部しか見ないことによる苦情の可能性などを法務からリスク増ととらえられる側面がある。利用者が構造を理解してくれればやりやすくなるが、現状はリスクマネジメントの観点からやらないというのも結構ある。【寺田構成員(第21回PF研)】

論 点

① 電気通信事業法・個人情報保護法等を踏まえた対応

- 利用者の端末情報がOS事業者、通信事業者、プラットフォーム事業者、アプリ事業者等によって、利用者の意思に反して取得・活用されていたとすると、「通信の秘密の対象であるか否かに係わらず、プライバシー上の適切な保護を検討する余地が生じるところ、端末情報の適切な取扱いの確保のための具体的な規律の在り方については、eプライバシー規則（案）の議論も参考にしつつ、今後検討が必要」となるのではないか。
- 利用者端末情報（cookieや端末の設定等）とそれに紐付く情報について、通信関連プライバシーとして保護されるべき利用者の権利として、把握されるべきではないか。電気通信事業者に着目するのではなく、利用者の権利に着目していく必要があるのではないか。このような利用者端末情報等を取り扱う者において、通信の秘密及び電気通信サービス利用者のプライバシー保護を行うことを確保していく必要があるのではないか。
- ターゲティング広告やプロファイリングを使った利用者への影響について後から検証できる環境を整え、透明性を確保していく観点から、利用者情報の利用の状況についての公表や保存についての仕組みについて考えていく必要があるのではないか。
- 適切な利用者情報の取扱いを確保する観点から、まずは共同規制としての形を整えるために、電気通信事業GLにおいて必要とされる事項を定めた上で、当該GLの遵守状況や事業者の自主的な取組の状況について、定期的にモニタリングを行うべきではないか。そのため、電気通信事業GL等において、定める事項（例：表示や公表、望ましい取扱い等）について検討していく必要があるのではないか。

なお、上記の電気通信事業GL及びそれを踏まえたモニタリングで、事業者の適切な対応が得られない場合については、新たな制度化（例：表示義務、公表義務等）の導入について検討していくことも必要となるのではないか。

これまでの主な意見

【個人情報保護法及び電気通信事業法等】

- 個人情報保護法の令和2年改正において個人関連情報の規制が導入されたが、個人情報になる前、特定の個人を識別することができるものになる前の部分の扱いが、通信の秘密のみなのか、もう少し通信関係プライバシーのようなものを考えて保護しなければならないのか、日本の場合はGDPR等にと比べると個人情報の範囲が狭いということがあり、それにより穴になっているところを考えていかなければならないのではないか。【森構成員(第21回PF研)】
- 競争ルール等の包括的検証の報告書等でしばしば電気通信事業法の役割の変化について言及があった。設備が一方においてソフトウェア化することとサービスがグローバルになるということを通じて、電気通信事業法が電気通信事業者規制法から電気通信サービス利用者保護法に転換を迫られざるを得ないのではないかというところから、各論を検討しなければならないのではないか。【森構成員(第21回PF研)】
- 電気通信事業法自体が、事業者規制の法律から、利用者保護の法律への転換を迫られている。今求められるのは、電気通信事業者の規制ではなく、電気通信サービス利用者の保護ではないか。【森構成員(第4回WG)】
- 個人情報になっていないものは個人情報保護法でというわけにはいかない。個人情報保護法は、令和2年改正で個人関連情報を導入しており行けるところまで行っており適切な改正がされている。取引透明化法は、取引透明化の枠組みがあり、閲覧者の閲覧履歴を収集する、取得する場面において、消費者・閲覧者に対して一定の何か表示をしたり同意を取る等について義務づけられるような立てつけの法律ではない。消費者優越についてはまだなかなか具体的な法執行の段階に至っていないということもあり、やはりここをカバーできるのは電気通信事業法だけであると改めて認識する。ウェブサイト、ファーストパーティーのところではクッキーやフィンガープリントやそういったものについて情報を取得する行為、タグを設置して情報を取得する行為等については、それをカバーして規律するのは電気通信事業法であるのだと考えられる。【森構成員(第22回PF研)】
- 「利用者の端末情報がOS事業者、通信事業者、プラットフォーム事業者、アプリ事業者等によって、利用者の意思に反して取得・活用されていたとすると、通信の秘密の対象であるか否かに係わらず、プライバシー上の適切な保護を検討する余地が生じうるところ、端末情報の適切な取扱いの確保のための具体的な規律の在り方については、eプライバシー規則(案)の議論も参考にしつつ、今後検討が必要」と親会中間報告書でされている。【森構成員(第4回WG)】

これまでの主な意見

【個人情報保護法及び電気通信事業法等（つづき）】

- 利用者端末情報(cookieや端末の設定等)とそれに紐づく情報については、上記の観点から、通信関連プライバシーとして保護されるべき利用者の権利として、把握されるべきではないか。通信の秘密に加えて、電気通信サービス利用者のプライバシー保護も同法の目的として考えるべきではないか。そう考えれば、保護すべき義務を負うのは、電気通信事業者のみならず、このような利用者端末情報等を取り扱う者全てと考えられる。電気通信事業者に着目するのではなく、利用者の権利に着目し、それを扱っている人を広く対象にすべきではないか。【森構成員(第4回WG)】
- 森先生に御指摘いただいた電気通信事業法を、電気通信事業者の規制から電気通信サービスの利用者の保護への転換というのは、私も強く賛同する。【佐藤構成員(第4回WG)】
- 規制のレベル、強度についてだが、自主規制には限界があるのではないか。JIAAから、自主規制のお話があったが、これは非常に十分に行われていて、JIAAの中では達成率は高いが、自主規制によるカバー率が低いということなのではないか。表示義務、同意取得義務を法律の義務として課した上で、その具体的な方法について、事業者団体等に委ねる形の共同規制がいいのではないか。【森構成員(第4回WG)】
- 事業者に事後的に報告義務を課すことも検討をしてはどうか。【古谷構成員(第4回WG)】
- 森先生からお話いただいた内容は、私も非常に方向性として大きく共感するところが多くある。しっかりと、まさに法的な基盤というものをしっかりした上で、自主的な形をどのように作り込んでいくのかといったような方向性で、ぜひ考えていただきたい。【生貝構成員(第4回WG)】
- デジタルサービス法でいうところの超巨大プラットフォームに対して課されている義務である、行動ターゲティング広告に関する、どういうターゲットにどういう広告を出し、それが、どのくらい見られたといったふうな情報の広告インベントリーの作成と、そしてそれに対するリアルタイムのAPIのアクセス確保は、この文脈でこそ、まさしく山本先生がおっしゃった意味と近い形で考えていく必要がある。まさしく、それぞれがどのように自分の情報、そしてそれが実際のサービスの上でどのように反映してきているのか、そういうことをしっかりと利用者に伝えていくということが、大変重要である。政治広告全体というものを、定義を含めて規制するのは難しいといったときに、やはり広告、まさにやはりそれが後から検証できる、そしてまさに議論の俎上にしっかり上ることができるという状態を確保する意味でも、そういったようなまさしく検証するための前提としての情報の保存と、仕組みというのは考えていく必要がある。その際には、大きいプラットフォームのようなどころだからこそやっていただく、守っていただくべき部分というものは何なのかということも考慮する必要がある。【生貝構成員(第4回WG)】

これまでの主な意見

【取引透明化法、消費者優越、独占禁止法】

- 個人関連情報が個人情報になる前のウェブの閲覧履歴とその分析の情報等について、個人情報保護法、取引透明化法、消費者優越、電気通信事業法等のうちどれでカバーするかという話について検討が必要。【森構成員(第22回PF研)】

【共同規制的なアプローチ】

- 我が国で同意は個人情報保護法だとすごくあっさりした書き方であり、通信の秘密に関する場合は非常に重くなっている。GDPRで言うように、透明性があり十分情報を提供した上で同意を取ることについて、法令レベルではないとしても、電気通信ガイドライン等で書くことにより、ある種の共同規制的な、インセンティブをつくることが考え得る。【生貝構成員(第21回PF研)】
- 通知とか公表とか表示義務を課すという話は賛成だが、同意の取得に関しては少し慎重に考えたい。ユーザーとして同意を求められてもうっとうしいというのものもあるが、義務づけることによる副作用も考えなければいけないと思う。事業者にとり同意を取っていることが免罪符になってしまう可能性もあるのではないかな。結果として、同意スキームを作る方に引っ張られ、前段の「きちんと情報提供し分かるように説明する」ということがおろそかになる恐れがあるのではないかな。同意がどういうときに必要かとか、取得する方法とかを細かく決めれば決めるほど、ユーザーではなく、ルールやルールを作る規制当局を見てしまうのではないかな。また「このツールを使えば同意取得義務は全てクリア」というサービスが出るとさらに何も考えなくなることを懸念。ユーザーのほうを向いて、マネジメントを巻き込み、自社のデジタルマーケティングについてのポリシーを自分の言葉で書いてほしい。法的な枠組みは緩やかな表示義務、努力義務等にとどめ、ある程度自由度を確保した上で、専門家がレビューし、レーティングするというのが良いのではないかな。【沢田構成員(第4回WG)】

論 点

②電気通信事業GL・指針等における対応

- これまで総務省において策定してきた電気通信事業における個人情報保護に関するガイドライン、位置情報プライバシーレポート、スマートフォン プライバシー イニシアティブ等の指針等については、どのように見直していくことが適切か。

【関係する各事業者における対応】

- スマートフォン プライバシー イニシアティブの考え方なども参照しつつ、スマートフォン及びウェブにおいて、プラットフォーム事業者、アプリケーション提供事業者、ウェブサイト運営者、広告事業者等関係する各事業者がそれぞれ適切に対応ができるような環境整備をガイドラインや指針等も通じて検討していく必要があるのではないか。
- プラットフォーム事業者、アプリケーション提供事業者、ウェブサイト運営者、広告事業者等の利用者情報を取得する事業者は、自らが取得する利用者情報及び情報収集モジュールやタグなどについて十分把握した上で、取得する利用者情報の種類や利用目的などに応じて、利用者が理解できるように通知・公表や必要に応じた同意取得を行うことが重要ではないか。

【同意と通知のベストプラクティスの検討・GLや指針等としての公表】

- 同意と通知について、いわゆるベストプラクティスとしてまとめて事業者が利用者情報の取扱いに関する通知・公表や同意取得を行う際に参照できるようなものとして示していくこととしてはどうか。
- 利用者が実質的に理解した上で必要な判断ができるように、判りやすい通知・公表又は同意取得の手法を検討することが重要ではないか。（スマートフォンや当該サービスの内容、利用者の特性等も考慮することが有用であり、ユーザーテストやステークホルダーの意見等も適切に活用すべきではないか。）
- プラットフォーム事業者内に蓄積されたパーソナルデータについての開示・利用条件・選択機会の提供を行っていくことが重要ではないか。利用者が自らの利用者情報の取扱いについてコントロールができる観点から、どのような工夫や選択肢が有用であると考えられるか。（ダッシュボード、オプトアウト有無・方法の開示、データポータビリティ有無・方法の開示、選択機会の通知やガイダンス等）

論 点

②電気通信事業GL・指針等の検討

【電気通信事業GL】

- 個人情報保護法の改正への対応した改正の検討
 - 別添のとおり、それぞれ対応した改正を検討する
 - 電気通信事業の固有の事情などを踏まえ、より適切な事例などについて検討する
- 利用者情報の適正な取扱いの確保に向けた改正の検討
 - ① プライバシーポリシーへの記載
 - ・ プライバシーポリシーの公表（第14条第1項）
 - プライバシーポリシーに記載すべき事項や留意すべき事項について、GL/解説の改正検討をしてはどうか（分かりやすい通知・公表や同意取得、オプトアウトの有無や方法、データポータビリティの有無や方法等）
 - ・ アプリケーションソフトウェアに係るプライバシーポリシー（第14条第2項・第3項）
 - SPIのアップデートなども踏まえ、GL/解説の改正検討をしてはどうか
 - アプリケーション作成者、情報収集モジュール提供者、広告事業者、ウェブサイト管理者等が留意すべき事項について、指針をまとめた上でこれを参照する形で記載を検討してはどうか
 - ② ベストプラクティス
 - ベストプラクティスについてまとめた上で、GL/解説の改正又は参照を検討してはどうか
 - ③ モニタリングの実施
 - ①・②の状況について、定期的にモニタリングを行い、必要に応じてGL改正等も検討してはどうか

【スマートフォン プライバシー イニシアティブ（SPI）】

- ・ 考え方そのものの有効性は変わらないが、外部の状況を踏まえ検討（必要に応じ電気通信事業GLへ）

【位置情報プライバシーレポート】

- ・ 端末情報以外の他の情報の扱いも視野に入れた上で検討（必要に応じ電気通信事業GLへ）

| 改正項目 | 電気通信事業GL改正の方向性(案) |
|-------------------------|---|
| 短期保存データの保有個人データ化 | 第3条柱書の規定を維持。解説2-8における関連の記載を削除。 |
| 不適正利用の禁止 | 第5条の次に規定を新設。解説に事例を含め説明を記載。電気通信事業者特有の事例について追加すべきか検討。 |
| 漏えい等報告・本人通知の義務化 | 第14条の次に規定を新設。解説に事例含め説明を記載。電気通信事業者特有の事例について追加すべきか検討。 |
| オプトアウト規定における第三者提供範囲の限定 | GL第15条第2項を改正。解説に事例を含め説明を記載。 |
| 越境移転時の本人説明充実化 | GL第16条を改正。解説においてガイドライン(外国第三者提供編)を参照。電気通信事業者特有の事例について追加すべきか検討。 |
| 個人関連情報第三者提供時の本人同意確認の義務化 | GL第18条の次に規定を新設。解説に事例含め説明を記載。電気通信事業者特有の事例について追加すべきか検討。 |
| 保有個人データに関する公表事項等 | GL第19条第1項第1号を改正、同条同項第3号の次に規定を追加。解説に事例と共に説明を記載。 |
| 保有個人データの開示方法 | GL第20条第1項・第2項を改正。解説に事例含め説明を記載。 |
| 第三者提供記録の開示請求 | GL第20条第5項を新設。解説に事例含め説明を記載。 |
| 利用停止・消去等の要件緩和 | GL第22条第5項・第6項を新設。解説に事例含め説明を記載。 |
| 仮名加工情報の創設 | GL第28条の前に規定を新設。解説でガイドライン(仮名加工情報・匿名加工情報編)を参照。 |
| 域外適用対象拡大 | GLにおける規定内容について、検討。解説において、域外適用の対象となる事例、対象とならない事例を記載。 |
| 認定団体制度の充実 | GLにおける規定内容について検討。解説において、ガイドライン(認定個人情報保護団体編)を参照。電気通信事業者特有の事例等について追加すべきか検討。 |
| ペナルティの引上げ | - |

これまでの主な意見

【同意取得の在り方に関する課題】

- スマートフォンが使われ始めた頃に総務省の会議でどれだけ情報取得がされているかという発表を聞き大変驚いたが、その実態がほぼ変わっていない状況で、利用者にとって何となく情報が取得されているのかなと思いつつそうしないと使えないというはかりにかけたようなバランスで使っている。同意画面については、とにかく分かりにくい。消費者としては使いたいほうが先で、細かくて分からないだろうしと思い、そのまま同意してしまうというのが正直な気持ちである。Consent Receiptのように、自分が何に同意しているか分かることは大変大切だと思う。【木村構成員(第22回PF研)】
- プラットフォーム研で通知と同意の検討をすることは非常に重要であり、世界的にもそういう認識があるから色々なところで同意に関するガイドラインが出てきて同意の有効性が厳しく検討されている。しかし、事柄が複雑になればなるほど、同意の果たす役割は少なくならざるをえず、ユーザーが同意したからよいではなく、そもそもの仕組みから話しをする必要がある。例えば、本日のJavaScriptの話も、同意は2段階目の話で、まず1段階目としてどういう情報取得・情報提供が発生するウェブサイトにするのかファーストパーティーがまず検討しなければならないのではないか。【森構成員(第22回PF研)】
- 同意をどのように取得するのかという手続、同意の取得の対象範囲、個別同意か包括同意か等は、様々な場面で検討されている。クッキー取得時の同意やユーザーインターフェース等も精緻な検討が進められている。一方、同意の効力については、法律行為か事実行為かも意見がある。今後同意取得が更に重要になる中で、同意のそもそもの効力、本人の同意による責任や事業者側への法的効力等もなども少し整理する場があってもよいのではないか。【新保座長代理(第22回PF研)】
- 同意疲れとの関係に関しては、意味もわからず同意ボタンが出てきて、とりあえず同意ボタンを押さないと先に進めない、ポップアップが邪魔という、理解できないままの意味のない同意に対して面倒と感じると理解。その上で、利用者情報の取得や利用に関して、ただ同意を得ることが必要になるという規律は意味をなさず、適切な通知およびコントロール性の確保が重要なのだと思う。【太田構成員(第2回WG)】
- それぞれの会社の考え方や、ブラウザ、アプリによってもユーザーがコントロールできる範囲がまちまちであるため、利用者のみならず事業者も混乱している状況が発生している。よって、取得する情報の種類や用途に応じて一定の規律を示すことが必要であると考え。【太田構成員(第2回WG)】

これまでの主な意見

【同意取得の在り方に関する課題（つづき）】

- SPIもファーストパーティー側でアプリプラポリという形で、外部に提供している事実、提供する情報、提供する方法、提供する相手が誰か、オプトアウトの方法を明らかにすべきではないか、そういう考え方であった。規制の方向性①はまず、ファーストパーティーに対して、表示義務を課してはどうかということで、利用者端末情報等をサードパーティーに提供していること、提供する情報、提供の方法、提供先のサードパーティーは誰かということ。あとは、オプトアウト情報、サードパーティーへの提供をやめるにはどうすればいいかということ。また、提供について同意取得を義務づけることも考えられるのではないか。【森構成員(第4回WG)】
- 規制の方向性②は、サードパーティーについても一定の表示義務を課すべきではないか。利用者端末情報を取得していること、取得している情報、取得の方法、それから利用目的、オプトアウト情報。SPIにも同じような趣旨のことが書かれているということ。規制の方向性③は、ファーストパーティーがタグ設置等の業務を委託する、委託先事業者に対しても何らかの義務を課すべきではないか。委託先に任せていたから自分たちはよく分からないというファーストパーティーが相当数おり、委託先側からファーストパーティーに対して、タグを置きませんかという働きかけをすることも多い。【森構成員(第4回WG)】
- 森先生の説明でいうところのサードパーティーに当たる情報取得者は、ファーストパーティーに対して利用者に説明を行うように規約やガイドラインで示していることが多いが、実際にはSPOⅧの調査でも明らかのように「6-2.利用者情報の送信先の記載」「6-3.情報収集モジュールに関する記載」については、掲載率が低い状況であり、網羅もされていないと考えられる。ファーストパーティーとしては、サードパーティーの規約やガイドラインに書いてあっても特に規制はないということで対応がおろそかになってしまっている状況と考えられるため、森先生のご提案のようにファーストパーティーにおいて利用者に表示義務を課すことに賛成する。【太田構成員(第4回WG)】

これまでの主な意見

【同意管理ツール（CMP）、同意の証跡（Consent Receipt）】

- ISOの通知・同意取得に関する標準規格において、レイヤードアプローチやジャストインタイムの通知とともに、有効な同意を高める手法として同意の証跡（Consent Receipt）がある。【NRI（第22回PF研）】
- ウェブサイト上における利用者の同意管理ツール（CMP）において、同意前から情報取得、取得拒否しても取得が継続されるなど、正しく動作していない場合も多くみられる。提供先は包括同意を取られると実効性はほぼないと思われる。提供元（ウェブサイト・アプリ側）で、どういう事業者がどういう情報を取得しているか公表を明確化しちゃんと拒否できるとよいのではないか。【太田構成員（第22回PF研）】
- アドブロッカーについては物にもよるが、ほとんどのサイトにおいては非常に有効なものだと思う。一方、広告がブロックされてしまうと、メディアとして収益をどう確保するかという問題がある。ドラスティックに広告のエコシステムが変わることがないので、広告を表示して収益を発生させることと、個人が広告をブロックできることをどう両立するかは非常に難しい問題かなと思う。【太田構成員（第22回PF研）】

【スマートフォン プライバシー イニシアティブ、スマートフォン・プライバシー・アウトLOOK】

- 太田氏の説明を伺い、やはりこれは木村構成員からもお話があったがスマートフォン プライバシー イニシアティブの話だと改めて思う。スマートフォン プライバシー イニシアティブは、ユーザーに対する情報提供にフォーカスしているが、状況は変わらず、深刻な問題状況にある。アプリのプライバシー・ポリシーの掲載率は上がったが、書かれたとおりになっていないなかったり、IDが固定的なものとなったり、事態がよくなったとはいえない。やはりもう一段階踏み込んだことをしないとイケない状態であることがはっきりしたのではないか。【森構成員（第22回PF研）】

論 点

③ 定期的なモニタリングの実施

- 国内外のプラットフォーム事業者、電気通信事業者など関係者による継続的な対話を通じた自主的な取組を促し、その履行状況をモニタリングするという共同規制的なアプローチを適切に機能させることが重要。取り扱う利用者情報の内容や利用目的等も考慮した上で、あらかじめ必要とされる事項をガイドラインなどで示した上で、関係事業者及び事業者団体による自主的な取組を進め、その状況を定期的にモニタリングして結果を公表することにより、透明性・アカウントビリティを確保していくことが有用ではないか。
- 利用者情報の取得により何が起こるか示すと分かりやすいのではないか。PIAや利用者へ与える影響（アウトカム）の検討も有用ではないか。引き続き検討が必要ではないか。弱者に対する不利益とか差別が起きない観点からも、ベストプラクティスを考えていくことも重要ではないか。
- モニタリングを通じて、事業者による対応状況等について確認し、必要に応じてガイドラインを見直してはどうか。
- ガイドライン等を通じたモニタリングによる透明性・アカウントビリティの確保が十分に図られない場合等においては、新たな制度化を視野に入れた検討を進める必要があるのではないか。

④ 利用者の理解促進・外部レビュー

- 利用者情報の取扱いに関する消費者の不安はその仕組みが見えていないことに由来する側面がある。業界の自主的な取組みが外部から見えづらい部分もあるため、外部に開かれた形で対話や情報発信を継続し、透明性を高めていくことも重要ではないか。（例えば、ターゲティング広告の仕組みを説明する啓発・情報発信を行うことや、オプトアウトサイト等により利用者の選択の機会を提供することも重要ではないか。）
- プライバシー・ポリシーの公表意義は企業活動の透明性やアカウントビリティの観点からも社会的・制度的に大きい。（海外で行われているように、）専門的見地から事業者のプライバシーポリシー等利用者情報の取扱いや説明・同意等の在り方について外部レビューが実施され、その結果が公表されることも有用なのではないか。

これまでの主な意見

【透明性の確保】

- 今後の方向性としては、同意をどう取るかよりも、利用者が、自分に関するデータを(集約・分析される前提で)提供しても良い相手かどうかを総合判断できるだけの「十分な情報開示」を中心に据えたインセンティブ設計が必要ではないか。【沢田構成員(第2回WG)】
- 資料1において参照されていた英国ICOの推奨事項はとても良いので、これを参考に、それぞれの事業者が、自社の顧客層の特性を勘案して工夫を凝らしていただけると良いと思う。その上で、第三者がその「透明度」をレーティングする、といった形であれば、利用者情報の保護に資する新たな技術や方法の導入・促進に繋がりやすいと思う。他方、透明性が不十分なまま”怠惰な利用者”を取り込むケースや、開示された情報に虚偽や誤りがあった場合のことを考えると、実効性を担保するためには、何らかのペナルティを検討する必要があるかもしれない。【沢田構成員(第2回WG)】
- 透明性評価の1つの基準として、利用者に同意を求めるときに利用者目線での説明が十分になされているか、という視点を挙げておきたい。「当社が〇〇することについて同意しますか？」だけでは、利用者はよくわからないまま同意してしまう可能性がある。同意した結果、利用者に何が起こるのかの説明を加えるのが望ましいと思う((例)「あなたはこんなニーズを持っている可能性がある」と当社が推測した情報に基づいて、他社の広告が表示されます。)また、同意しなかった場合にどうなるかも説明して欲しい。【沢田構成員(第2回WG)】
- ネット広告等は非常に技術が高度化をしている中で、事業者や業界団体が今使われている技術というものがどういうものなのかということ、消費者に御説明いただく仕組みというのが必要になると思う。また、沢田構成員の御意見にもあったが、事業者がやっていることを第三者的に評価をする、どちらかというと消費者の立場だが、評価する組織というものを、これから育成していく必要があるのではないかと考えている。【佐藤構成員(第4回)】

これまでの主な意見

【プライバシーポリシーの公表意義】

- プライバシー・ポリシーの公表意義が社会的、制度的に大きく変化している。企業のアカウントビリティを果たす上での公表事項の要素として投資判断の指標としても用いられつつある。プライバシー・ポリシーをスコアリングするサイトも出てきている。個人情報やプライバシー保護は、企業のアカウントビリティの観点から定着しつつある。また、法定公表事項について、改正個人情報法を踏まえ保有個人データに関する事項の公表等を積極的に行うことが期待される。【新保座長代理(第21回PF研)】

論 点

⑤ 国際的な対話と連携

○利用者情報の取扱いについては、グローバルに共通した課題であり、各国規制当局においても検討が進んでいる。また、グローバルに利用者情報を取扱うプラットフォーム事業者も複数存在しており、その取組による影響も大きくなっている。我が国において取組みを進めるとともに、国際的な対話と連携を進めることが重要ではないか。

これまでの主な意見

【検討の視点】

□ プラットフォームの自由と規制の在り方をめぐってEU等で様々な動きがある中で、日本の関係法・政策形成の意義・重要性をよりグローバルな規模でこれまで以上に可視化していくために、従来よりももう一步踏み込んだ、シンプルかつより包括的なコンセプトないしは規範的な基軸を打ち出していくのも、政策戦略の将来構想としてあり得るのではないか。「同意」の在り方、ユーザーのモラル、プラットフォーム事業者の自主的取組・透明性・アカウントビリティに関する施策を基盤とした上で、これらと相互排他的な代替措置としてではなく、さらなる実効性の確保に向けた追加的な担保措置を促すものとして、例えば①プラットフォーム上での言論・表現の送り手と受け手が相互に互換的な存在となるユーザーのモラル・倫理・責任に加えて、その「権利」の視点もより前面に打ち出すユーザーライツの観点、②AI実装も進むユーザーコンテンツ監視・削除等のシステムに関して、公的部門での規律が必ずしも及ばないブラックボックスの事実状況を把握し、より開かれた検証可能性を確保 ③事前ないしプロアクティブに公正性、公平性などの社会的価値を、システムのデザインに積極的に組み込んでいくこと。の3つの観点が挙げられる。【山口構成員(第21回PF研)】