プラットフォームサービスに関する研究会（第22回）

１　日時　令和２年12月４日（金）13時00分～15時00分

２　開催場所　総務省第２特別会議室（８階）

３　出席者

（１）　構成員

宍戸座長、新保座長代理、生貝構成員、大谷構成員、木村構成員、崎村構成員、手塚構成員、寺田構成員、松村構成員、宮内構成員、森構成員、山口構成員

（２）　オブザーバ

個人情報保護委員会事務局　赤阪参事官、小川参事官補佐

（３）　総務省

谷脇総務審議官、竹内総合通信基盤局長、今川電気通信事業部長、吉田総合通信基盤局総務課長、梅村データ通信課長、豊島情報通信政策課長、中溝サイバーセキュリティ統括官室参事官、小川消費者行政第二課長、丸山消費者行政第二課課長補佐、中川消費者行政第二課課長補佐、今村消費者行政第二課専門職

（４）　ゲストスピーカー

株式会社DataSign　太田代表取締役社長

野村総合研究所 小林上級コンサルタント、南島主任コンサルタント

４　議事

（１）利用者情報の適切な取扱いの確保に向けて

（２）その他

【宍戸座長】　それでは、定刻でございますので、始めさせていただきます。本日は、皆様お忙しい中お集まりをいただきまして、誠にありがとうございます。プラットフォームサービスに関する研究会（第22回）の会合を開催させていただきます。

本日の会議につきましては、新型コロナウイルス感染拡大防止のため、一部構成員及び傍聴はウェブ会議システムにおいて実施させていただいております。

では、冒頭カメラ撮りがありますので、少々お待ちください。

よろしいでしょうか。

（マスコミ退室）

【宍戸座長】　それでは、事務局から、ウェブ会議による開催上の注意事項について御案内があるということですので、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】　総務省総合通信基盤局消費者行政第二課の丸山でございます。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。

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、座長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。

そのほか、チャット機能で随時、事務局や座長宛てに連絡をいただければ対応させていただきます。

注意事項は以上になります。

なお、本日、大谷構成員は30分後をめどに御退室となります。

それでは、これ以降の議事進行は宍戸座長にお願いしたいと存じます。宍戸座長、よろしくお願いいたします。

【宍戸座長】　ありがとうございます。名前を名のれということですので、冒頭、座長、宍戸でございます。

それでは、議事に入ります。本日は、まず事務局から利用者情報の適切な取扱いの確保に向けた検討課題について御説明をいただきます。次に、オブザーバーの個人情報保護委員会事務局から個人情報の保護に関する法律等の一部を改正する法律について、次に、Date Sign様から利用者情報取扱いの実態について、野村総合研究所様から利用者情報の通知・同意取得に関する諸外国の事例について御発表いただきます。その後、これら御発表に関する質疑、それから、コメントをいただいた上で、自由討議として構成員の皆様から御意見をいただきたいと思っております。最後に、事務局から改正電気通信事業法の施行に向けた準備ということで御報告をいただく。これが本日のアジェンダでございます。

それではまず、事務局から資料１、利用者情報の適切な取扱いの確保に向けた検討課題について御説明をお願いいたします。

【小川消費者行政第二課長】　事務局の消費者行政第二課長の小川でございます。資料１に基づきまして御説明をさせていただきます。

１ページ目でございますけれども、利用者情報の適切な取扱いの確保に向けての検討課題ということでございますが、これは前回の研究会でお示しさせていただいたものと同じでございます。前回の第21回会合におきまして構成員の先生方から多くの御意見をいただいておりますので、それにつきまして、２ページ以降、カテゴリーに分けてお示しをさせていただいております。

まず２ページを御覧ください。電気通信事業法の射程ということでございます。１つ目でございますが、電気通信事業法の役割が、設備が一方においてソフトウエア化する、サービスがグローバルになるということで、電気通信事業法が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というところも視点としてあるのではないかと。また、２つ目でございますが、プラットフォームの自由と規制という在り方を含めて、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というのも１つの視点ではないかという御指摘をいただいております。

２つ目、個人情報とプライバシー保護ということでございます。１つ目の丸でございますが、情報は必ず何かに紐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。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ほうからもう少し考えていく必要があるという御指摘。また、２つ目でございますが、令和２年の個情法改正で個人関連情報の規制が導入されたということで、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、通信の秘密のみか、また、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といったような御指摘についてもいただいております。

また、次のページ、３ページでございますが、プライバシー・ポリシーについて多くの御指摘をいただいております。１つ目でございますが、プライバシー・ポリシーが長文化が進んで非常に分かりづらいということで、ポリシーの分かりやすさ、分かりやすく見せるための工夫・仕組みを今後検討する段階に来ているのではないか。

２つ目でございますが、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ということも含めた対策を考えるべきではないか。読ませることだけに専念するのではない、別の対策も考えなければいけないのではないか。

３つ目でございますが、プライバシー・ポリシーに関して、全部読めと言われても多分無理ではないか。逆に、普通というものが何かあって、普通と違うところを見せるといったような発想をするとシンプルになるのではないかということで、アプリケーションの種別のようなものを考えて、スタンダードをつくってはどうかというような御意見。

それから、次の丸でございますが、やはりこちらは利用者情報がどこでどのような目的で使われているかという事項について、レッドやグリーンなど何らかカテゴライズできないものか。特に第三者に提供されるとか、微妙な機微情報とか健康情報とか、そういう一定のカテゴリーのものについては特に注意喚起をするといったような仕組みが考えられないか。

それから、最後ですけれども、正確な情報に基づいて導入可否の判断ができるような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といった御指摘をいただいております。

次、４ページでございますけれども、プライバシー・ポリシーの公表意義ということの御指摘でございます。企業のアカウンタビリティを果たす上での公表事項の要素というのが投資判断の指標としても用いられるのではないかということで、重要性、積極的な公表されるといった御指摘もございました。

次でございますが、プライバシー・ポリシーの工夫ということで、簡略版やレイヤードアプローチについても複数の御指摘をいただいております。簡略版については、載せない理由についても御指摘を複数いただき、義務化されていないので作成しないとか、あとは、法務からリスク増と捉えられる側面もあるのではないかという御指摘もいただいております。また、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など、簡単なものを出して、詳細はこっちを見てくださいという形が推奨されているという御指摘とか、GDPRの透明性のガイドラインの中にも指摘がある、また、実装例もあるので、国際的なベストプラクティスを見るとよいといったような御指摘もいただいています。

それから、５ページ目でございます。スマートフォン・プライバシー・アウトルックについてでございます。こちらについて、2010年代から継続的な検討がなされているということで、そういう継続の意義があると。また、プライバシー・ポリシーの掲載率が顕著に向上といったような分かりやすい調査結果も出ているということで、こういうモニタリングを継続していく意義について御指摘をいただいております。また、モバイル・コンテンツ・フォーラムや広告代理店などにおいてガイドラインを作って、これを広めているという動きがあるというような御指摘もいただいております。

それから次に、同意の位置づけでございます。同意の位置づけについて、同意の取得について考慮点と限界があるということで、可能ならば、ほかの適法な根拠を使ったほうがいいというような御指摘もいただいております。

それから、共同規制的なプローチということで、透明性があり、十分情報を提供した上で同意を取るといったことについて、ガイドラインで書くことなどによってある種の共同規制的なインセンティブをつくるということも考え得るという御指摘もいただいています。

それから次、最後、６ページでございます。検討の視点ということです。①でございますが、プラットフォーム上での言論・表現の送り手と受け手の双方になるユーザーのライツの観点。それから、２つ目、ＡＩ実装も進むユーザーコンテンツの監視・削除などについて、より開かれた検証可能性を確保する。３つ目でございますが、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といった御指摘もいただいております。

簡単ですが、以上でございます。

【宍戸座長】　宍戸です。ありがとうございました。ただいまこの検討課題として、前回構成員の皆様からいただいた御意見をこのように事務局でまとめていただきましたけれども、この御説明について御質問、それから、コメントがあればいただきたいと思いますが、いかがでしょうか。オンラインで参加されている構成員の方は、チャットで私に呼びかけていただければと思いますが、いかがでございましょうか。

森構成員、お願いいたします。

【森構成員】　ありがとうございます。森でございます。御説明ありがとうございました。２ページ目なんですけれども、個人情報とプライバシー保護のところで、２番目で私の意見を的確におまとめいただいていますけれども、その後、前回の後、いろいろな法令の守備範囲について考える機会がありました。

ここに関連するのは、もちろん個人情報保護法と、あと、取引透明化法と消費者優越と電気通信事業法であると思うわけなんですけれども、ちょうど今問題となっている、ここに個人関連情報が個人情報になる前というふうに書かせていただきました。個人関連情報の状態であるところ、典型的にはウェブの閲覧履歴とその分析の情報ということですけれども、これを誰がどうカバーするかという話なんですけれども、まず個人情報になっていないものですので、個人情報保護法でというわけには明らかにいかないわけでございます。

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ますので、行けるところまで行っている、適切な改正がなされているということかと思います。一方で、取引透明化法は、取引透明化法の枠組みがありますので、特に閲覧者の閲覧履歴を収集する、取得するところ、ここで消費者に対して、閲覧者に対して一定の何か表示をするとか、同意を取るとか、そういうことを義務づけられるような立てつけの法律ではありませんので、そこのところを、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らないということもありますので、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いうことを改めて認識いたしました。

したがって、ウェブサイト、ファーストパーティーのところで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、この後、Data Signの太田さんから御説明がありますけれども、それについては、電気通信事業法のカバーする部分であると。ここで前回は、通信の秘密なのか、通信関係プライバシーなのか、ふんわりしたことを言いましたけれども、それを規律するのは性質における電気通信事業法であるのだということを意見として申し上げたいと思います。

以上です。

【宍戸座長】　ありがとうございました。ほかに、今頂いているこの資料１の検討課題についての補足的なコメントであったり、自分の意見の扱いが違うとか何か、御質問とかございますでしょうか。

ひとまず現在のところはよろしゅうございますか。後ほど全体的な討論の時間を設けておりますので、またこの後のプレゼンテーションを聴いてさらに御意見等をいただければ

と思っております。

それでは、次のアジェンダに移りたいと思います。お手元資料２でございますが、個人情報の保護に関する法律等の一部を改正する法律について、個人情報保護委員会事務局様より御説明をお願いいたします。

【赤阪個人情報保護委員会事務局参事官】　個人情報保護委員会事務局参事官の赤阪でございます。私のほうからは、本年６月に改正されました個人情報保護法の概要について御説明をさせていただきます。資料２を御覧ください。

表紙から２枚めくっていただきまして、右下のページ番号で２番を御覧ください。今回の改正の経緯でございます。個人情報保護法につきましては、2003年に成立をしたものでございますが、その後、2015年に大幅な改正が行われております。その際、いわゆる３年ごと見直し規定ということでございまして、国際的な動向、情報通信技術の進展等を踏まえて見直しを行うという規定が盛り込まれたところでございます。今回、その３年ごと見直し規定に基づく初めての改正ということで、本年の６月に改正が成立したということになっております。

次の３ページ目でございますが、本検討を行うに当たりましては、多数の委員会の開催はもとより、経済界、有識者からのヒアリング、意見募集あるいはタウンミーティング等を幅広く行いまして、広く御意見を伺った上で検討を進めてきたところでございます。

また、次の４ページ目でございますが、この間、世界的に見ても、欧米、それから、アジア各国におきましてデータの保護に関する法制度が立法されてきているところでございまして、こういう状況も踏まえながら検討を進めてきたところでございます。

次の５ページを御覧ください。こちらに今回の改正に当たりまして、個人情報を巡る状況の変化、それから、今回の改正に当たっての視点を整理してございます。左側でございますが、例えば個人情報に対する意識の高まりとか、それから、情報通信技術の一層の発展、また、その裏返しでございますが、不正アクセスをはじめとする個人データを取り巻くリスクが変化してきております。また、先ほどもありましたが、グローバル化ということで、世界各国でこういったデータに関する制度も整えられているといった背景事情があるところでございます。

今般、右側にございますが、こういう中で、いかに個人の権利利益の保護を図っていくか、それから、ＡＩ・ビッグデータ時代と言われるような技術革新がある中で、こうした保護と活用のバランスを図りながら、いかにそれらを強化していくか。そして、越境デー

タの流通の増大への対応とか、あるいは国際的な制度との調和、こういったものを図る必要があるということの観点から制度改正を行ったところでございます。

次に、改正法の内容に移りたいと思います。次、右下７ページ目にお移りください。こちらが改正法の概要でございます。大きく６つの項目に整理をしております。それぞれにつきまして、次のページ以降で御説明をさせていただきたいと思います。

８ページ目を御覧ください。こちらにつきましては、個人の権利・利益の保護という観点からその在り方について見直しを行ったものでございます。こちらに大きく５点ほど載せております。例えば１点目でございますけれども、先ほどありましたとおり、個人の個人情報に関する意識が高まっておりまして、事業者が保有しているデータについて、利用停止とか、あるいは消去を求める、こういったことのニーズが高まっているところでございます。ただ、現在におきましては、そういった利用停止・消去等の請求を行うことは法違反がある場合に限られておりまして、これにつきまして、法違反の場合に加えて、個人の権利または正当な利益が害されるおそれがある場合でも請求ができるようにするという拡充を行うこととしたものでございます。

また、②でございますが、保有個人データを事業者に対して開示を求める場合に、昨今、データにつきましては、例えば映像とか音声、こういったものも多くなってきているわけでございますが、現状、原則として書面での交付を求めるという形になっておりまして、これにつきまして、デジタルに応じた形での提供についても本人が指示できるようにするという措置を行ったところでございます。

次に、９ページ目を御覧ください。こちらにつきましては、事業者の守るべき責務についての見直しを行ったものでございます。１つ目が、①として漏えい等報告の義務化でございます。昨今、例えば事業者の不注意とか、あるいは外部からの不正アクセスによって個人データが外部に流出してしまう、漏えいしてしまうというようなニュースがよく散見されるところでございますが、現状、こうした漏えいが起こった場合には、告示に基づく任意ベースで事業者の方から委員会のほうに報告をいただいているという現状でございます。ただ、やはり昨今こういった漏えいが続出する中で、個人の権利・利益を害するおそれが大きいものについては、きちんと委員会への報告とか、あるいは本人への通知を義務化する必要があるのではないかということでこの義務化のための措置を行ったものでございます。

どういう場合にこの義務化の対象とするかについて今、規則の検討を行っているところ

でございますが、現行検討中のものについて、真ん中左のほうに薄い緑で吹き出しがありますが、そこに基準が書いてございます。１つは、要配慮個人情報が含まれる場合の漏えい、それから、不正アクセス等による漏えい、それから、財産的被害のおそれがある漏えい、これは例えばクレジットカード番号が漏えいするといった場合ですけれども、これらについては、件数にかかわりなく、漏えいした場合には報告いただくことで考えております。

他方で、こういった情報が含まれない場合においても、一定数以上の大規模な漏えい、現状、1,000件を１つの基準として考えておりますが、こうした大規模な漏えいが起きる場合には、やはり事業者のほうで安全管理体制に問題があるのではないかということで、こうした場合においても報告の義務化の対象とすることで考えているところでございます。

次の10ページ目を御覧ください。２つ目が不適正な方法による利用の禁止というものでございます。これはページの下の②の例を御覧いただければと思います。散在的に公開されている個人情報について、差別が誘発されるおそれがあることが十分に予見できるにもかかわらず、それを集約しデータベース化し、インターネット上で公開すること、こういった事案が昨今起こったりしているところでございます。上のピンクのところに戻りますけれども、こういった違法また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というものを明らかにする改正を行ったところでございます。

それから、ページを少し飛んでいただきまして、右下の13ページに移っていただきたいと思います。こちら、データの利活用に関する見直しでございます。従前から個人情報保護法におきましては、データの利活用を促すという観点から匿名加工情報という制度がございましたが、今般、個人情報と匿名加工情報の言わば中間的なものとして、仮名加工情報というものを創設いたしました。それは下の矢印のところに書いておりますが、他の情報と照合しない限り、特定の個人を識別できないように加工したものが仮名加工情報ということになります。

こういった仮名加工情報について、内部分析に限定すること等を条件に、開示・利用停止請求への対応等の義務を緩和するということで、より柔軟に活用できるような形での制度を創設したものでございます。これによりまして、下の緑のところでございますが、例えば当初の利用目的には該当しない目的に新たに使うとか、そういった形での利活用の推進が期待されるところでございます。

それから次、14ページ目を御覧ください。こちらが先ほど森構成員からも言及がござい

ましたが、個人関連情報に関する規定でございます。先ほどデータの利活用が進む中で、本人にとっては、自分の情報がどこでどのように使われているのかが分かりにくくなっている面があろうかと思います。

下のほうに例が出ております。Ａ社、Ｂ社となっておりまして、ここでは購買履歴の例でございます。Ａ社では、購買履歴を管理しているのですが、そこのＩＤは１、２、３、４ということで、誰の個人データかは分からないということで、Ａ社では個人情報とならない形で管理をしている。他方、Ｂ社においては、個人情報として管理しているものがある。このときに、Ａ社からＢ社にデータの提供を行って、Ａ社では個人データではないけれども、Ｂ社ではそれを自社のＩＤと紐づけることによって個人データとして所有するといった使われ方が起こってきているところでございます。

こうすると、なかなか本人としては関与しないところで実質的な第三者提供が行われているというような形になりかねないということで、上のところにございますが、今回、提供元では個人データに該当しないものの、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、本人同意がきちんと得られているかということを確認した上で行っていただくことを義務づけるものでございます。この場合、Ａ社で持っている情報を個人関連情報ということで法律上位置づけているというものでございます。

次に、15ページ目を御覧ください。こちらはペナルティ、罰則についての在り方の見直しでございます。下の表の罰金刑の現行部分を御覧いただければと思います。これにつきましては、現行は、個人、それから、法人共に同じ罰金が科せられているところでございますが、これにつきまして、法人と個人の資力の格差等を勘案して見直しを行うということで、法人に対しては個人よりも高い形で罰金刑の最高額を引き上げたというものでございます。

次、16ページ目を御覧ください。こちらは法の域外適用の強化に関するものでございます。経済活動・社会活動のグローバル化に伴いまして、外国の事業者が国内のユーザーに対して物品または役務を提供することが増えてございます。ただ、現行の個人情報保護法につきましては、外国の事業者に行使できる権限は、指導、助言、勧告のような強制力を伴わないものに限定されております。このような中、今般、罰則に担保された報告徴収、命令についても外国の事業者に行使できるようにする改正を行ったところでございます。

それから、次、17ページでございます。今申し上げたように、海外の事業者に個人データが第三者提供されるということが現行増えてきて、これからも増えていくことが想定さ

れるところでございますが、ユーザー本人から見ると、制度の異なる外国にデータが越境移転されることになると、どう使われるかの予見性がなかなか不安定なものになってしまうのではないかということで、海外にある第三者に個人データが提供される場合には、移転先の事業者における取扱いについて情報提供の充実を図っていただくことを盛り込んでおります。具体的には、右の下のところに「改正後」という枠がございますけれども、例えば移転する先の国の名前とか、その国において個人情報保護に関する制度があるかないかとか、あるいはその概要とか、こういったものをきちんとユーザーに対して情報提供を行った上で同意を取得することを求めることにしております。以上、少し駆け足になりましたが、改正の内容の概要でございます。

最後、19ページ目を御覧いただきたいと思いますが、今後のスケジュールでございます。法律自体は、公布後２年以内に施行ということになっております。現在、政令と委員会規則を中心に議論を進めているところでございます。こちらの絵では、１月、２月に意見募集を行うことになっておりますが、今、少し前倒しでスケジュールを進めておりまして、今のところ、年内にはこの意見募集を開始すべく今作業を進めているところでございます。その後、この政令あるいは委員会規則を補足するガイドライン、Ｑ＆Ａの内容の検討を詰めていきまして、十分な周知を行った上で、令和４年の春の施行を目指して今、作業を進めているところでございます。

それから最後に、本資料のスコープの外でございますが、本改正とは別にまた個人情報の保護法制について見直しが行われております。それはいわゆる一元化と言われているものですけれども、個人情報の保護法制につきましては、民間事業者に対するもの、それから、行政機関に対するもの、それから、独法に対するもの、それぞれ別の法律になっております。また、自治体については、さらにそれぞれの自治体において条例でルールが定められているということで、2,000個問題と言われているようなところでございます。

こうしたところが個人情報の保護のバランスを欠くであるとか、あるいは情報の円滑な流通の阻害になっているというようなことが指摘されているところでございまして、こういったものについて共通的なルールを設定して、個人情報保護委員会が一元的に監督することに向けての法改正を行うということで、今、内閣官房を中心に、総務省、個人情報保護委員会が連携して、来年の通常国会の法案提出に向けた作業を行っているところでございますので、併せて報告させていただきます。

私からは以上です。

【宍戸座長】　ありがとうございました。御質問等あろうかと思いますが、これはプレゼンテーションが終わった後、一括してお受けしたいと思っております。

そこで、続きまして、資料３、利用者情報取扱いの実態につきまして、Date Sign様から御発表をお願いいたします。

【太田氏】　Date Signの太田です。よろしくお願いいたします。画面共有します。

それでは、私からは、利用者情報の取扱いの実態ということでお話をさせていただきます。

自己紹介のところはスキップさせていただきます。

20分ということなので、駆け足になってしまうかもしれないんですが、まずはウェブとスマホでの情報の取得の実態がどうなっているかというところの説明と、プラットフォーマーによる制限と対応――この対応というのは、プラットフォーマーの対応と、プラットフォーマーが制限したことによるほかの人たちの対応みたいなところをまとめました。最後に、最近ちょっと話題にもなっている、Consent Management Platform、同意管理プラットフォームが今どんな感じになっているかというところをお伝えできればと思います。

では早速、ウェブ・スマホでのデータ取得ということで４ページ目です。現在使われているオンライン識別子ということで、先ほど個人関連情報みたいな話もありましたが、どういうふうに識別しているのか。ブラウザを識別したり、スマホを識別したりしているんですけれども、ウェブはクッキーとかローカルストレージとかフィンガープリントとか、スマホはIDFAとかAAIDとか呼ばれるんですけれども、これが具体的にどんなふうになっているかというのを今日は紹介したいと思います。

次、５ページ目、Cookieとは？というところです。こちらは実際のブラウザを見ながら説明をしていければと思いますので、画面を切り替えます。例として日本経済新聞のウェブサイトを使わせていただいているんですけれども、このように日本経済新聞のサイトに行きますと、ユーザーはこのページを見るわけなんですけれども、裏では、開発者ツールをクロームで開いているんですが、Ｆ12を押すとこれが表示されます。ここで、どういう要素があったり、どういう通信があったり、どういうクッキーが付与されているかみたいなものを見ることができまして、このページに訪れたときにどういうクッキーのやり取りがされているのかというのを見ることができます。

ここで表示されている、ここにDomainとあるんですけれども、ちょっと見にくいですかね、小さいかもしれないんですけれども、このnikkei.com、アクセスしているドメインと、

ここのクッキーのドメインが一致しているものがファーストパーティークッキーと呼ばれているもので、このnikkei.com以外に、ここにグーグルとかフェイスブックとかkrxdとか書いてあるものが、サードパーティークッキーと呼ばれるものです。

資料に一旦戻ります。今説明したのが６ページ、７ページ辺りで、８ページにCookieには何が書かれている？と。さっき見た中で、いろいろな文字列が書いてあって、人間が見てもほぼほぼ分からない、何かごちゃごちゃ書いてあるなという感じで、ここには、個人関連情報になるのか、ならないのか分からないようなものとか、いろいろなものがあります。例えばこのツイッターの、これも細かくて見にくいですけれども、一番下のlang jaとか書いてあるところとか、これはこのブラウザの言語設定が日本語だよとかそういうだけなので、別にブラウザを識別しているわけではないですよねと。ブラウザを識別しているものが何かというと、８ページの赤いところで囲まれたこのbigminingusrとか、bkuとか、c_userとか書かれたものがブラウザを識別しているIDになります。

８ページのフェイスブックに注目をしてほしいんですけれども、これまた小さくて見にくいんですけれども、c_user、1260941023と書いてあるんですが、この1260941023ってどういうIDなんだろうと。これはこういうIDは結構いろいろなところでフェイスブックが取得しているよというのが分かるように、トヨタのサイトとかも持ってきたんですけれども、10ページですが、この1260941023というのをフェイスブックのfacebook.comのスラッシュの後ろにぺっとつけますと、僕のページが出てきます。要するに、この1260941023というのは、もう完全に個人情報、個人データになるんではないかというところでございます。

これについては、フェイスブックに対して、1260941023というのがトヨタのサイトに行ったりとかいろいろなサイトに行くと送信されているというのは、個人データをフェイスブックが取得しているので注意してくださいねというのは、個人情報保護委員会からもう１年半ぐらい前、２年ぐらい前に出ているものでございます。

次に、では、こういう情報はどうやって取得しているのかというところで出てくるのがタグというものです。12ページです。こういうスクリプト――言語ですね。これはブラウザが解釈をする言語がJavaScriptというものなんですけれども、こういったJavaScriptのものと、イメタグと呼ばれているイメージタグをただ貼るというものもあります。

イメタグとJSタグと大きく２つに分けて左と右に今説明が書いてあるんですけれども、イメタグというのが、現在は主流でないのですが、ビーコンと呼ばれているものです。１掛ける１の小さい見えない画像をウェブサイトに貼って、クッキーとかIPアドレス、閲覧

ページURLを取得していくというものです。

これは昔はこういうふうにクッキー、IPアドレス、閲覧URLぐらいを取得していくというのが主流だったんですけれども、今はイメタグを使っているところはあんまりなくて、JSタグ、JavaScriptのタグが主流になっています。右側のところですね。これはイメタグと違って、様々な情報を取得したり、ページ自体を操作したりできますので、クッキー、IPアドレス、閲覧URLに加えて、ページに表示されている要素は何でも取れますし、画面サイズとかの環境の情報も取れますし、ユーザーがフォームに入力した情報とか、そういったものを取得することもできます。あと、重要なところが、このJSタグというのは、自分自身のJSタグ、自分自身がデータを取得するだけじゃなくて、他の人のJavaScriptタグを強制的に読み込ませることもできますよということができてしまいます。

それで、次の13ページは、ウェブサイト側での制御困難と書いてあるんですが、要するに、どこかのJavaScriptタグを入れると、そこから別のやつがまた呼ばれて、またそこから別のやつが呼ばれてとなると、ウェブサイト側はこのJSタグを１個貼っただけなのに、実際には、ここに書いてあるように、グーグルアナリティクスのタグを置いただけなのに、ダブルクリックのタグも出ているとか、フリークアウトのタグを入れただけなのに、インティメートマージャーのタグが出ているとか、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いくと、そんな状況になっています。

それを僕らは調べたことがあって、大体１日に60サイトぐらい見ると、14ページですけれども、自分が閲覧した60サイト以外に250の事業者にデータが１日で送信されていると。これはほとんどが広告とかアクセス解析、データ仲介事業者とか、そういったところにデータが収集されていますよという実態です。

何でこんなにほかのところのタグを呼び出さなきゃいけないのかというところは、クッキーの特性にも関係しているんですけれども、今IDsyncという画面が出ていると思うんですが、クッキーのID、先ほどのフェイスブックのIDとか、ツイッターのIDとか、ほかのいろいろなクッキーに書かれたIDって別々なんですね。なので、事業者によってIDが異なるので、例えばフェイスブックがツイッターにフェイスブックのIDこれだよと教えるときには、クッキーはこのIDだよというのをツイッターに教えてあげないといけないんですね。その通信がブラウザ上に行われていまして、この例で示させていただいたIDsyncというのは、赤いところ、treasuredataというところに対して、kanadeという、これは広告配信事業者のIDを連係している。これがいろいろな事業者間でIDの連係をどんどんしていくので、

どんどん利用者情報がいろいろなところに提供されていくという実態になっております。

こういう状況になっているというのをちゃんとウェブサイトが把握できていないよねという話が報道されたのが、16ページにありますが、これは去年の２月になります。こういう報道もされてちょっと盛り上がったは盛り上がったんですけれども、先ほどプライバシー・ポリシーがという話もありましたけれども、まだまだプライバシー・ポリシーを全然書けていないところが多くて、一番多いのが、例えばフェイスブックのIDとかって個人情報とクッキーが紐づいてはいるんですけれども、多くのサイトでいまだに、クッキーは個人情報と紐づくことはありませんみたいな感じで書いていたりするところが一番多いかなと思います。あとは、いろいろなところに、例えば全日空のトップページに訪れると、全日空以外の74の事業者にデータが送信されているんだけれども、そのことを書いていないとか、そういう問題が未だにあります。

ローカルストレージという話をしていなかったんですが、これはほとんどクッキーと同じで、ブラウザに保存される、クッキーよりも容量が多くて便利に使えるものなんですけれども、基本的にローカルストレージも同じような用途で使われていたりします。

では次に、アプリの話に移りたいと思います。18ページです。アプリでは、iOSはIDFAと呼ばれておりまして、アンドロイドではAAIDと呼ばれているものです。これはOS側でIDを発行していて、それをいろいろなアプリが使っていくという方式なので、先ほどクッキーの場合、ドメイン、事業者によってIDが違うから、その連係が大変だみたいな話をしましたけれども、これは非常にIDFAとかは便利で、１つのiPhoneを使っている人のIDFAというのは、どのアプリを使っていても一緒なので、IDのシンクをする必要がなくてとても便利ですよと。

これについて、いろいろなところにデータを提供する必要はなくて、裏側で連係しているのかと思いきや、19ページにスマホアプリを起動した際の様子ということで、スマホアプリは少ないですよねみたいな話をしようと思ったんですけれども、昨日Charlesで調べて、ニュース系のアプリ、この場で、この場だけにならない、ニュースピックスとスマートニュース、２つアプリを起動して数ページ閲覧したところ、133のホストと237のリクエストが発生しておりまして、赤く囲ったところが、これが広告とかトラッキング系のリクエストで、こういうところがIDFAを取得しながら何かしていると。広告していたりとか、一番上のMarketoなんかは個人情報と紐づけているためのシステムなので、個人情報と紐づいているんじゃないかと、こんな状況になってしまっております。

今年の８月に朝日新聞と先ほどのCharlesのこれを使っていろいろなスマホアプリを調べて、位置情報がどれぐらい取得されているかみたいなものを調査して、プライバシー・ポリシーにちゃんと位置情報を取得しますと書いてあるのかどうかというのを調査したところ、半数が位置情報を取得しますとは書いていなかったということが分かりました。

次に、プラットフォーマーの制限という話に行きたいと思います。21ページです。今まで話してきたように、クッキーとかもアプリとかもこうやって本人が知らない間にいろいろなところに何百とか情報が行っちゃうので、プラットフォーマーが、そういうことができないようにするぞというふうに言っています。サファリというブラウザは、既にサードパーティークッキーを使ったトラッキングはほぼできなくなっていて、グーグルクロームも2022年にサードパーティークッキーを使えなくするよと言っておりますし、あと、iPhoneのiOSは、2021年、来月からIDFAの利用に同意が必要となるので、先ほどのようにたくさんの情報にIDFAに紐づけてたくさんの事業者が取得しているところに同意が必要になりますよと。これが実際の画面なんですけれども、こういうものが出てくるようになってしまうので、アプリを作っている人からしてみると、こういうものを出すのか、もうトラッキング自体をやめるのかというのをどうするかというのを考えないといけないと。

こうやって制限されていくので、事業者側はどうしようとなるんですね。クッキー使えないよ、IDFA使えないよとなってくると、先ほどコメントの中でも古くて新しいフィンガープリントという言葉もありましたけれども、まさに古くて新しいフィンガープリント、またフィンガープリントを使ってみたらいいんじゃないかというのがちょっと来ているかなと思っています。今、主流は、Canvas FingerPrintingというもので、これはCanvasというブラウザの、先ほどのJavaScriptの１つの機能を使って、ブラウザに文字を書くんですね。そうすると、ブラウザの環境によって表示される文字の形が変わるので、それで特定していくという技術なんですけれども、これが精度が大体クッキーと同じぐらいですので、クッキーの代わりに使えるんじゃないかというところで、使っているところもありますよと。これもちょうど新聞社と、どこの企業が使っているみたいなものを取材しておりまして、これ言っていいのかな、多分今週末記事が出ると思います。

グーグル側は、いや、フィンガープリントとか使うなよと。サードパーティークッキー使えなくするけれども、それに代わったPrivacy Sandboxというものを用意するので、これを使ってくださいと言って、今までクッキーを使ってやっていたオーディエンスターゲティングとか、リターゲティング広告とか、コンバージョン測定とかは、w3cのWeb

Advertising Business Groupで仕様を策定して、それにのっとってやっていこうとグーグルが提案しているんですけれども、必ずしも皆これに賛成しているわけではなくて。結局、グーグルが提案しているPrivacy Sandboxというのは、要するに、ブラウザ側に情報が保持されると。ブラウザを提供しているのってグーグルでしょう。それって、グーグルが持っているのとそんな変わらなくない？と思う人もいて、かつその中の情報を広告事業者が使えないので、あまり嬉しくない。

そこで、業界団体が設立されておりまして、これはPRAMという団体なんですけれども、これは多分僕の予想ですけれども、Privacy Sandboxへの反発で、グーグル以外の広告事業者さんたちが組んで、ちょっと違う方法でトラッキングできるようにしようと皆で話し合っております。

そこで出てきたのが、そこでじゃないかもしれないですけれども、ここのPRAMの中に入っている事業者同士で、25ページですけれども、新しいメールアドレスベースのIDを使ってやり取りしようよというのが今進んでおります。Unified ID2.0と呼ばれているんですけれども、これはフォームに入力されたメールアドレスを暗号化してハッシュ化して、それをみんなで共有して、メールアドレスで追っていけば、クッキーよりもちゃんとターゲティングできるじゃないかと。

ここからCMPの話になっていくんですけれども、要するに、今までクッキーというのは、同意が必要なくて、ヨーロッパでも昔はそうだったんですけれども、何となくこっそり取れたんだけれども、今はもう同意が必要になっちゃったから、どうせ同意をするんだったら、もうメールアドレスとかそういうのでトラッキングすればよくない？というふうにも思っているようで、そこからこのような、もうちょっとフィジカルに近いようなIDを使うようになっていくのではないか、これが今後のスタンダードになっていくんじゃないかなというところでございます。

最後に、同意管理ツール（CMP）についてです。その同意を得るため、ウェブサイトでクッキーとかのデータ利用に対して同意を得るためのツールなんですけれども、GDPR、ePrivacy Directiveに対応するために発展をしてきて、日本においては、個情法改正後も特にクッキーを取得するというところに同意は必要ないんですけれども、先ほどのメールアドレスベースのトラッキングということになると、こういうもので同意を取って、みんなで共有していくことになるのかなと思っているところです。

現状、CMPがどんな感じかというところで、27ページになんちゃって同意取得みたいな

ものをやったんですけれども、これはCMPとはあんまり呼ばなくて、日本でサイトでも、要するに、アクセスしただけで、このサイトにアクセスすると、クッキーの利用に同意したものとしますよみたいなものが結構あって、これは有効な同意とみなされないのではないかと思っていますし、なぜ日本のサイトがこういうものを入れているのかというのはちょっと謎ではあるんですけれども、こういう対応をするところがちょっと前から増えてきていて、こういうものはあんまりよくないなと思っています。

あとは、なんちゃってユーザーコントロールというのが次のページです。時間も残り少ないですが、もう一回デモをさせてください。今このページに来ると、これがCMPなんですけれども、広告パフォーマンス測定とか、パーソナライズされたとか、コンテンツのパフォーマンスを測定とか、いろいろな用途別にオン・オフがあって、これ全部オフに今しています。全部オフにしているのにもかかわらず、先ほどの開発者ツールでどういう通信が行われているのかというのを見ると、しれっとグーグルアナリティクスに通信は行われていて、これは何をオフにしても全然オフにならないということが起きております。こちらのクッキーを見ても、GAのクッキーもちゃんと付与されておりまして、コンテンツのパフォーマンス測定をオフにしても測定がオフにならないというような事例が非常に多くて、これがちょっと問題だなと思っているところです。

また資料に戻ります。28ページに書いてあるんですが、技術的な問題や設定の煩雑さから正しく動作していないことが多くて、これは僕らDate Signで調べたものを論文として発表しておりまして、御興味のある人は、資料にリンクがあるので見てみてください。導入している65%のウェブサイトで正しく動作していないということが分かりました。

最後のスライドは、「こうなると良いな」と書いてあるんですけれども、先ほど森先生からもあったように、個人情報保護法だと、今、個人関連情報というのはありますけれども、個人関連情報が出来て、第三者提供したときに個人に紐づくところで提供先で同意が必要となっても、先ほどのウェブサイトで何百とかアプリで何百というのは、そこは規制の対象にほぼならないのであんまり意味がなくて、提供先で包括同意を取られてしまうと実効性はほぼないと思っております。先ほどのような状況を改善するという意味でいうと、あまり意味はないと思っております。なので、どこかでもうちょっと、提供元というかウェブサイト・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というのを公表を明確化して、ちゃんと拒否できるというものになるといいなと思っております。

私からは以上になります。ありがとうございました。

【宍戸座長】　ありがとうございました。続きまして、資料４、利用者情報の通知・同意取得に関する諸外国の事例について、野村総合研究所様から御発表をお願いいたします。

【南島氏】　野村総合研究所の南島と申します。それでは、資料４、利用者情報の通知・同意取得に関する諸外国の事例について御説明をさせていただきます。

１ページ目を御覧ください。こちらが今回の調査対象としました欧米の行政機関が定めますルールや国際規格のリストです。資料自体は50ページ近くございますが、本日はお時間が限られることから、かいつまんでの御説明となることを御容赦いただければと思います。御不明点は、後ほど御質問をいただければと存じます。

では、２ページ目に参ります。前回の研究会においても、構成員の皆様から、利用者情報の取扱いにおける通知・同意取得に関して、ハウの部分に着目した検討が重要だというふうに御意見を賜ったと伺っております。そこで、本調査では、そうした通知・同意取得に関して推奨される、または留意すべき事項について、諸外国のルールとか事業者の皆様のお取組を調査いたしました。

では、３ページ目です。まずGDPRについて調査をしております。

４ページ目をお願いいたします。GDPRでは、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について、透明性と同意のガイドラインにおいて解説をしております。

スライドを進めていただきまして、まず透明性に関してですけれども、主に第12条で規定が行われております。このスライドでお示ししております①から⑥の要素を満たす形で通知をすべきというふうに規定がされているわけです。

次の６ページ目に進みまして、ガイドラインでは、この各①から⑥の要素の中でも、６ページの右側のような形で実装することを説明しています。簡潔であるということに関しては、階層的なプライバシーステートメントによって、大量のテキストスクロールを不要とするという形で工夫案を示しています。透明性があるということに関しては、丁寧に説明する。理解しやすいとは、公開討論、消費者テストなどを実行する。容易にアクセスできるということにつきましては、トップページから２タップ以内でアクセスできるようになるといったことで説明をしています。

次のページになりますけれども、同様に同意に関しても有効な同意について４要素で規定しておりまして、この①から④の形でお示ししているというふうに調査させていただきました。

では、次の８ページ目です。こうしたGDPRのガイドラインを受けまして、ブレグジット

の関係はありますけれども、イギリスのデータ保護機関であるICOでは、１から５の工夫をより効果的に通知・同意取得を行うことができるものとしてウェブサイト上でお示ししております。１つ目が階層的アプローチ、２つ目がダッシュボード、３つ目がジャストインタイムの通知、４つ目がアイコン、５つ目がモバイル及びスマートデバイスの機能性というものです。

それぞれについて御紹介をさせていただきます。まず階層的なアプローチです。ICOのサイトでは、こういったイメージ画を用いながら、階層的アプローチはどういうものなのかということについて御説明をしております。見出しのような項目があって、そこをクリックとかタップいたしますと、詳細が表示されます。さらにその詳細から、プライバシー・ポリシー等の全文に飛ぶことができるようになっているという形で、個人の理解に応じて段階的に情報を表示するということが階層的アプローチとして示されています。こうしたアプローチを取ることによって、プライバシー情報の取扱い以外に通知すべき情報があるときなどは特に有効だろうとICOでは示しています。

次に10ページ目ですけれども、２つ目の手法としてダッシュボードでございます。ここでいうダッシュボードというのは、データの使用状況について個人が管理できるようにする画面を提供するというものです。スライド上では、アカウント設定のような画面から、プライバシーというところに飛んで、個別の自分の情報開示範囲に関して個人が設定できるようになるよという例をお示ししております。この延長線上として、先ほど太田様より御説明いただきましたCMPのようなサービスも提供されているものと思っております。

３つ目のジャストインタイムの通知については、11ページ目で御紹介しております。これはサービスを開始する、またはアカウントを作成するというタイミングで、プラポリを通じて個人情報、利用者情報の取扱いについて通知するだけでなくて、商品の購入時など異なるタイミングで通知を行うことで、改めて個人が情報を提供していることを認識するのに役立つものですということで推奨されております。例示の中では、メールアドレスを登録する際に、この登録されたメールアドレスに広告等を送りますという目的でメールアドレスの登録をお願いしますといった通知がポップアップで出ることをお示ししています。

12ページ目ですけれども、モバイルデバイス等は画面が限られることから、文章ではなくて何かイメージのような形でお伝えすることも有効ですということで例示がございます。

最後、13ページ目ですが、ここで言うモバイル及びスマートデバイスの機能性というのは、今までお伝えしてきましたジャストインタイムの通知とかアイコンと組み合わせて使

用することがより効果的というものですけれども、スマートフォンなどの振動とか音声、音によるアラートによって利用者情報の取扱いに関する通知を行うというものでございます。以上、GDPRを踏まえてICOでは、５つの手法を使うことによってより効果的な通知・同意取得ができるだろうということで例示をお示ししておりました。

次に14ページ目ですけれども、クッキー等類似の技術に対する規制に関して、同じくICOのガイドラインとか、フランスのデータ保護機関であるCNILがガイドラインとレコメンデーションを公表しておりますので、その内容についてお調べしております。

16ページ目を御覧ください。まずICOですけれども、ICOでは、クッキーの取扱いに関して、そもそも欧州ではGDPRとかePrivacy指令に基づいてクッキーの取得に際して同意が求められるわけですけれども、その同意取得に当たって、ウェブ画面上で閲覧とかをできない形での同意画面が出てくること、それをクッキーウォールというふうに表現しているわけなんですけれども、クッキーウォールを使用して同意取得を求めるということは要件を満たすものではないというふうにICOのガイドラインでは示しております。そのほか、このウェブサイトを継続的に使用することで同意していることになりますというような黙字の同意も認められませんし、何かスライダーのような形で消費者に同意をさせるような機能があったとしても、デフォルトでオンになっている場合では駄目ですよということがガイドラインでは示されております。

こうしたガイドラインの内容を踏まえまして、17ページ目ですけれども、ICOのウェブサイトでもクッキーの取得を行っているようですが、ICOのウェブサイトでは、右下のＣのマークがございまして、こちらをクリックするとスライダーが出てきて、そのスライダーはデフォルトでオフになっているという形で、今申し上げましたガイドラインに準拠する形でのクッキーの取得に関する通知・同意取得が実装されているというものでございます。

次に、CNILのレコメンデーションでございますけれども、こちらは本年の10月にCNILガイドラインと一緒に採択されました。本日は、より具体的な事例が載っていますレコメンデーションのほうを調査してお持ちしております。レコメンデーションもガイドラインも採択されたバージョンはフランス語のみで公表されておりまして、本調査自体は英語版のドラフトに基づいて行っております。まずCNILにおけるレコメンデーションでも、階層的な通知が有効な手法ということで示されております。その内容は、ICOと同じように、見出しがあって、そこをクリックすると、詳細な説明が格納されていたり、詳細な説明から

さらに全文に飛べるといったものでございます。

19ページ目です。同意取得に当たりましても、同意する、しないといったボタンが同じような形で表現されることによって、どちらかに個人を誘導するということがないという形が推奨されております。

20ページ目でございます。同意する、しないというだけでなくて、より詳細に個人が選択できるような画面を階層化することも一案ですよということがお示しされております。

以上が欧州の状況でございまして、次に米国の事例ということでCCPAの規則を取り上げております。22ページ目を御覧ください。CCPA自体は、カリフォルニア州のデータ保護法ですけれども、その通知・同意取得に当たっては、規則において細かに規定されております。なお、CCPA自体は、本年11月の大統領選と共に行われました住民投票で、CPRAという法律に改定されることが決まったわけですけれども、ここでも通知・同意取得に関しては、個人データの想定する保存期間についても通知事項として含むことが予定されております。

規則に戻りますと、23ページ目ですが、Article１から６まで構成されておりまして、通知・同意取得に関してはArticle２、NOTICE TO CONSUMERSというところが関係してございます。

24ページ目です。CCPA規則では、以下３つの場合においてプライバシー・ポリシーの作成・開示とは別に消費者への通知を義務づけております。これが個人情報の収集に関する消費者への通知、オプトアウト権に関する消費者への通知、金銭的インセンティブに関する消費者への通知というのが、プラポリとは別に個人への通知が必要な場面でございます。ICOでもジャストインタイムの通知が推奨されていたわけですが、CCPAではそれが今申し上げた３つの場合においては義務づけられているというものでございます。

それぞれの場合においてどういった内容の情報をどういった形で通知しなければならないのかということにつきましては、資料の25ページ目以降に記載してございます。例示として１つ取り上げさせていただきますと、25ページ目、個人情報を収集するときということで、収集する個人情報の種類、その利用目的、オプトアウトページへのリンク、プライバシー・ポリシーへのリンクをプラポリの通知とは別に通知しなければならないというふうに規定しております。

では、これを具体的に事業者の皆様がどのように実装しているのかということにつきましては、29ページ目にロサンゼルス・タイムズの例をお持ちしております。こちらは７月にアクセスした結果でございます。まずトップページにプライバシー・ポリシーとは別に、

収集に関する通知が用意されておりまして、ここをクリックしますと、プライバシー・ポリシーにおける、先ほど申し上げました情報の種類とか、利用目的とか、オプトアウトに関するリンクのページが表示されるようになっております。

また同様に、オプトアウトに関するページにも飛べるようになっていまして、こういった事業者の皆様の対応というのは、ＬＡタイムズだけではなくて、日本企業の現地法人も同様の対応をしております。それが30ページ目でございます。トヨタ自動車のアナハイムにあるディーラーでは、先ほど申し上げました収集に関する通知を30ページ目のような形で行っております。そこでは、情報の種類と利用目的があり、オプトアウトのリンク、プライバシー・ポリシー全文へのリンクをこういう形でお示ししております。

以上がCCPAのお話でございまして、次に32ページ目から、NISTのPrivacy Frameworkについて御紹介させていただければと思います。NISTは米国の国立標準技術研究所のことでございまして、こちらが公表しておりますサイバーセキュリティに関するフレームワークというものは多くのグローバル企業、日本企業でも採用されており、そのNISTが発表したプライバシーに関するフレームワークということで注目がされておりました。

34ページ目に、フレームワークの構成について御紹介しております。大きく３構成になっております。Core、Implementation Tier、Profilesという形で構成されております。まずCoreには、対応を図るべき観点が示されております。Tierと呼ばれる部分には、観点別に、今どういう状況なのかということを評価するための基準が示されており、最後、Profilesでは、理想とギャップを埋めるための手段が記載されてございます。

35ページ目ですけれども、NISTのPrivacy Frameworkにおいては、Coreとして、35ページ目左側のグレーのボックス、１から８のボックスが示されております。このうち、６、７、８というか、Detect以降の３つに関しては、Cybersecurity Frameworkと重複しているものでございまして、最後に「－Ｐ」がつくものがPrivacy Framework独自のものでございます。ここで見てみますと、Communicate－Pを例にとって申しますと、通知・同意取得に当たりまして、そういったプロセスをきちんと確立して、社内で浸透させましょうという形の規定がされておりました。

36ページ目でございます。こういった形でPrivacy Framework自体はやや上位理念的に規定されているものではございますが、よりそれを具体に落とした形の文書としてSP800－53という文書が改定されました。そこでは、同意や通知に関する具体的に推奨される手法についての御紹介がございます。

38ページ目でございますけれども、その文書において紹介されております、同意取得を行う上でのより推奨される手法として、TAILORED CONSENT、ジャストインタイムの同意、撤回という形で御紹介されておりまして、いずれも、冒頭申し上げましたICOやCNILの手法と類似するものがこのNISTの文書においてもお示しされております。

以降、39、40、41、42に関しましては、SP800に関する文書の御説明でございますので、割愛させていただきます。

43ページ目まで参りまして、最後に、国際規格ということで、ISOの通知・同意取得に関する標準規格について御紹介させていただきます。既に本研究会においても繰り返し言及があるものと存じますので、本日は、今まで申し上げましたレイヤードアプローチやジャストインタイムの通知以外の部分でISOの規格で御紹介されているものとして、Consent Receiptについて御紹介をさせていただければと思います。

そちらは48ページ目にお示ししております。一度同意した内容に関して、その同意の内容を個人が振り返れるようにその同意の証跡を個人に供給するというものでございまして、Consent Receiptという名称でISOの規格においてはこういったものが同意の有効性を高める手法として示されてございます。

以上が調査の内容でございました。

【宍戸座長】　御説明ありがとうございました。それでは、ここから質疑応答等に移りたいと思います。ただいまの個人情報保護委員会事務局様、Date Sign様、野村総研様の御発表について、質問やコメントがありましたらお知らせください。また、自由討議として全体を通してのコメントも併せて承りたいと思います。いかがでしょうか。

では、お願いします、木村さん。

【木村構成員】　木村です。御説明ありがとうございます。情報収集については、以前スマートフォンが使われ始めた頃に、この総務省の会議でどれだけ裏で情報取得がされているかという発表を拝見したことがありまして、そのときも大変びっくりいたしました。その事態がほぼ変わっていない状況で、やはり消費者というか利用者にとっては、何となく情報が取得されているのかなと思いつつも、やはりそうしないと使えないという、秤にかけたようなそんなところのバランスで使っているのかなというのを感想として思いました。

同意画面については、私もこの研究会で常々言っているのですけれども、とにかく分かりにくいです。実名を出していいのかわかりませんが、東京メトロのWi-Fiを接続しよう

とするときに必ず同意画面が出るのですけれども、それが日本語ではないんですね。英語だったり、中国語だったりするのですけれども、「翻訳できませんでした」と下に表示が出るのです。大体書いていることはそうなんだろうなと思って、「I agree」と押すのですけれども、でも、もしそれが日本語で書いてあったとしても、使いたい方が先なので、きっと細かくて分からないだろうし、そのまま同意してしまうだろうなというのが正直な気持ちです。

それが私の今感じるところなのですけれども、今回説明を聴いていて、やっぱり自分が何に同意しているか分からない。最後のConsent Receiptって本当にそうだなと思いましたけれども、やはり同意したことがどういうことなのかというのが分かることは大変必要だと思います。

質問ですけれども、まず赤阪様の資料ですけれども、14ページの個人関連情報の第三者提供規制というところで、本人同意が得られているというところですが、Ａ社とＢ社がデータを使うとして、利用者はどの時点でどちらに同意をするのかというのが分からなかったので、そこを具体的に教えていただきたいというのが１点目です。

次に、太田様への質問ですけれども、事例ではフェイスブックのIDをお使いになっていたのですけれども、例えばフェイスブックを使っていない場合とかほかのＳＮＳを使っていない場合は、何か特定のIDみたいなものを作成されるのかどうかというのが１点目。

それから、２点目が、21ページですけれども、もしここで同意をしないと言った場合は使えなくなってしまうのかというところが分からなかったのと、ここはマイクロソフトのインターネットエクスプローラーはないんですけれども、そちらは何か規制とかそういうものをやっているのかもし御存じだったら教えていただきたいというのが２点目です。

それから、３点目が、26ページのところでメールアドレスによる確認というのがあったのですけれども、この場合は、例えば紐づけ用のメールアドレスで可能なのか、それとも、やはり主たるメールアドレスを使う必要があるのかというところが分からなかったので、そこを教えていただきたいと思います。

以上です。

【宍戸座長】　それでは、まず赤阪さんのほうからお願いいたします。

【赤阪個人情報保護委員会事務局参事官】　個人情報保護委員会事務局の赤阪でございます。資料２の14ページの個人関連情報について御質問をいただきました。ありがとうございます。我々としては、本人から見ると、自分の情報がどこでどのように使われるかと

いうことをきちんと把握できるようにすることが重要だと思っております。その意味では、最終的に個人データとして活用するのはこの絵ではＢ社になりますので、典型的なパターンとしては、Ｂ社が、Ａ社から情報を受け取って自分のところで個人情報として活用しますよということの同意を利用者から取得していただくというようなパターンを想定しております。

【木村構成員】　ということは、利用者は、Ｂ社というのは全く知らないのだけれども、突然Ｂ社から連絡が来て、実はＡ社のデータを利用したいという連絡が来るというイメージですか。

【赤阪個人情報保護委員会事務局参事官】　そういう意味ではここの絵を御覧いただければと思いますが、Ｂ社でももともとこの顧客のリストみたいなものは持っていて、そこにＡ社から持ってきている、ここだと例えばIDの１、２、３、４というのがうまくリンクしているものであった場合に、Ａ社からは個人に紐づいた形ではもらっていないけれども、自社ではそれを紐づけることができて、それを個人データとして充実させていくようなパターンを想定しています。ですから、Ｂ社においてはそれぞれのユーザーとはすでに接点を持っているという形になるので、そこで同意を取得していただくことを想定しています。

【木村構成員】　分かりました。典型的な事例はそういうことだということですね。

【赤阪個人情報保護委員会事務局参事官】　はい。

【宍戸座長】　ありがとうございます。それでは、太田さんのほうからお願いいたします。

【太田氏】　ありがとうございます。まず１つ目のフェイスブックを使っていない場合はどうなるのかという話なんですけれども、この資料の９ページ目に、トヨタさんのこれですね。これ、c_userというのは、フェイスブックを使っている人の個人が特定できるIDが書かれているんですけれども、その２つ上にfrというのがあって、これがフェイスブックを使っていない人にも一律に付与されるブラウザを特定するためのクッキーですので、使っていない人はこのfrというものでトラッキングをされていくということになります。

２つ目の質問なんですけれども、21ページですかね、同意をしない場合にどうなるかですけれども、こちらはアプリでこういう画面が出てきて、この画面でいうと、「Appにトラッキングしないように要求」というのを押すと、もともとIDFAの値で端末を識別できるＩＤが入っているんですけれども、それが全部000000という値になって特定できないようになります。

３つ目は、インターネットエクスプローラーはどうなのかという話で、インターネットエクスプローラーは今のところサードパーティークッキーは使える状態で、今、インターネットエクスプローラーはエッジというものに変わっていまして、エッジがクロミウムというクロームも採用している同じベースのブラウザに変わっているんですけれども、2022年になったら、多分そのクロミウム自体でサードパーティークッキーを使わなくするので、エッジも使わなくなるのではないかとは言われているんですが、今のところ、公式な見解は出ていないという認識でございます。

最後に、メールアドレスの件ですが、25ページですね。Unified IDという形でメールアドレスベースでトラッキングしていこうというものなんですが、どのメールアドレス、何のメールアドレスを使うかというのは、多分個人に選択の余地はなくて、事業者側が、じゃ、このメールアドレス使おうといって決まって、ハッシュ化をして、それでトラッキングしていくということになると思います。

以上です。

【木村構成員】　複数持っている場合はどうなるのですか。

【太田氏】　複数持っている場合は、例えば先ほどちょっと話にも出したMarketoさんとか、複数のメールアドレスを持っていても、ファーストパーティーのクッキーで別のメールアドレスが同じ人だと分かったり、そうやって頑張って名寄せをして、そこで一番プライマリーなIDとして何かを事業者側で決めて、複数のやつがあっても、このメールアドレスはこっちのメールアドレスと一緒だよというものを裏側で持っているようなイメージになります。

【木村構成員】　分かりました。

【宍戸座長】　よろしいですか。次に、新保先生から御発言の希望が出ていますので、新保先生、お願いします。

【新保座長代理】　新保です。では、私から発言をさせていただきたいと思います。今日は質問ではなくて、今回の御報告は非常に貴重な御報告で、特にこういった情報を取るときの同意要件がさらに今後重要になるであろうと思うんですけれども、一方で、そもそも論になってしまうので、また今からどういうふうに議論するかということも含めて従来からちょっと疑問に思っているところとして、同意ということについて、今回もさらに同意を取ることが重要であるという意見とか手続がある一方で、そもそもこの同意の位置づけとか、この同意ってそもそも何なのかということについては、従来からいろいろと意見

があってあまり整理されていないところがあるかと思います。

大きく２つなんですけれども、１つは同意の取得手続や方法と、もう一つが同意の効力の問題。１つ目の同意の取得手続の方法とか手続についての問題については、同意の取得方法であるとか、同意の取得の対象範囲、さらには、個別の同意なのか、包括同意なのかということについて、同意をどのように取得するのかという手続は、かなり様々な面で検討が進められてきていると。とりわけ、クッキーの取得に当たっての同意とか、手続的な方法とか、あとは、ユーザーインターフェースも含めて、その方法や手段についてはかなり精緻な検討が進められてきているかと思います。

また、当初、経済産業分野の個人情報保護ガイドラインのように、同意を取得する方法についてかなり具体的な方法を明示するなど、その取得方法の手続については従来から議論がなされているところかと思いますけれども、一方で同意の効力については、例えば個人情報保護法は、18条のみ契約と書いてありますので、そうすると、それ以外の同意については、法律行為なのか、事実行為なのかということについては意見があるところかと思います。そうすると、例えば契約に伴って取得する同意についての法律行為としての同意要件として同意を課していることになるのか、あくまで本人が確認したということを確認する事実行為としての同意なのかということについて、この点があまり定かではない部分が多いと思います。

この点を踏まえると、今後、同意を取得するということが重要になっている、これがさらに重要になるわけですけれども、そうすると、同意のそもそもの効力がどのような形の効力があるのか、本人はそれをどこまで同意することによって、逆に言うと自分の責任を負うのか。事業者側は、本人からどこまで同意を求めること、また求めたことによって、結果的に法的にどのような効力があるのかということについては少し整理をする場があってもよいのかなと思いました。

以上であります。

【宍戸座長】　新保先生、ありがとうございました。それでは次に、崎村さんから御発言の希望が来ています。崎村さん、お願いします。

【崎村構成員】　ありがとうございます。幾つかあるんですけれども、まずメールアドレスベースのIDというのがありましたよね。これって実は結構危惧しております。というのは、メールのリサイクル問題というのがあって、メールアドレスって、例えばアメリカのヤフーなんかだと、その人がやめると、ほかの人に割り当てられるんですよね。このと

きに違う人に違う情報が結びつけられて間違ったプロファイリングがされてしまう可能性があるというのをちょっと危惧していて、その辺がどうなっているのかなというのは興味があるところです。

それから、２点目が、Consent Receiptという話があって、どうも大変すばらしい御紹介ありがとうございました。実は私、ISO/IEC 29184のプロジェクトリーダー、主査なものですから大変ありがたく思っております。これ、今々の考え方だと、コンセントのレシートを送るというよりも、データのレシートを送ったほうがいいよねという考え方が出てきています。なぜかというと、データプロセッシングのための適法な根拠というのは、同意だけじゃなくてほかの根拠もいろいろあるわけですよね。それによってもやっぱりデータの受領とか、あるいはデータの使用とかがあるので、そういったことに関するレシートを送ったほうがいいのではないかという考え方が今々出てきているので、それは御紹介しておきます。ISO/IEC 29184のほうには盛り込めなかったんですが、そういう話が出てきていて、29184のフォローオンプロジェクトで27560だったと思うんですが、今、作成されていて、そちら側にはそれが入ってくるかもしれません。

３番目のサードパーティークッキーの話なんですけれども、これって実はセキュリティとかプライバシーを守るためにサードパーティークッキーを使う例も実はあります。これと、ある意味個人のプライバシーをターゲットにした、侵害するような形での使い方の区分けが非常に難しくなってきて、しかも後者ばかり注目を浴びて、じゃ、全部やめてしまえというふうな風潮になっているのが現在なんですけれども、それをすると、逆にプライバシー的にまずいことが起きるということもいろいろ考えられているので、この辺りについては結構慎重に扱うべきなのかなとは思っています。

今、このクッキーや何かのことに関していうと、グーグルさんとアップルさんが非常に大きな力を持っちゃっているんですね。そこの競争法的な考え方というのもちょっと頭の片隅に入れておく必要があるかもしれないということを申し上げておきます。

以上です。

【宍戸座長】　ありがとうございました。それでは、ほかに御質問や御発言いかがでしょうか。

【森構成員】　お願いします。

【宍戸座長】　では、森先生、お願いします。

【森構成員】　ありがとうございます。森です。御説明ありがとうございました。いず

れも非常に有益な情報を含んでいたと思います。もちろん初めて伺うわけではないというものもありましたけれども、いずれにしても非常に重要なコンテンツだと思いますし、これを教訓にして進めていかなければいけないと思います。

まず太田さんの御説明なんですけれども、これを伺って思うのは、やはりこれは、木村さんからもお話がありましたけれども、スマートフォンプライバシーイニシアティブの話なんだなということを改めて思うわけでございます。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というところにフォーカスをしておりまして、状況が変わらない、もちろん問題状況というのは非常に深刻な問題状況があるわけですけれども、例えばアプリのプライバシー・ポリシーの掲載率は上がりましたというレベルでは向上しましたけれども、太田さんのお話を聴いてみると、書かれたとおりになっていないというようなことであったりとか、あるいはIDがスタティックなものになったりとか、事態がよくなったとは言えない。SPIの課題設定のところはある程度クリアされましたけれども、やはりもう一段階踏み込んだことをしないと、どうにもならなくなっている状態であるということがはっきりしたのではないかと思います。

私はプラットフォームサービスに関する研究会で通知と同意の検討をすることは非常に重要だと思っておりまして、このまま御検討いただくべきだと思いますし、恐らくそれは世界的にもそういう認識があるから、いろいろなところで同意に関するガイドラインというのが出てきて、同意の有効性が厳しく検討される。言ってみれば、なかなか有効な同意になりにくくなるという状況がつくられているのではないかと思います。

しかしながら、やはり事柄が複雑になればなるほど、同意の果たす役割というのはどうしても少なくならざるを得なくて、それはユーザーが同意したからいいでしょうというふうにはなかなか言えなくて、やっぱりそもそもの仕組みがどうなっているのかというところの話をしていかざるを得ないのかなと思います。

ですので、例えば今日のJavaScriptのお話であれば、それはこういうことをやっていますよというふうにユーザーに見せて同意してもらうということの前に、その１つ前に、どういうウェブサイトにするかということをファーストパーティーが考えないといけない、検討しないといけないわけですね。これ、なかなか難しい問題です。少し前に霞が関のウェブサイトもJavaScriptを置いているということで報道されていたケースがありました。それはすぐに改めたということのようですけれども、ことほどさように難しい問題です。

例えばJavaScriptを置くときにIDとパスワードを入力するページに置いていいのかとか、

JavaScriptを置くときに、先ほど御説明のありましたサードパーティーのJavaScriptを読み込むようなJavaScriptを設置していいのかとか、そういうことをファーストパーティーが、これはファーストパーティーが自分のウェブサイトについてやることですから、業者に「皆さんやっています」と言われて、「ああ、そうですか」とやるのではなくて、どういう情報取得、情報提供が発生するウェブサイトを作るのかという、その作り方においてのあるべき姿というのがあるはずであって、まずはそれをやると。そもそもそんなことしなくていいんだったらしない。

ということがまずありまして、サードパーティーに提供する場合に必要があってアナリティクスに渡す場合に、そのことについて同意してもらうという話なので、同意は２段階目の話でして、１段階の話、ファーストパーティーのウェブサイトはどのようにあるべきかということを検討する必要があると思います。

以上です。

【宍戸座長】　森先生、ありがとうございました。ほかに。寺田さん、お願いします。

【寺田構成員】　JIPDECの寺田でございます。同意のところで考え方の部分で少し最近ずっと違和感を感じています。どんどん細かくなって、手続関係の話になっていくんですが、そもそもこの同意って何のためにするんだったっけというところがだんだん忘れられて、形骸的なものになってきつつあるなとちょっと感じています。

同意を取るのに必要なものとして、まずはどんなデータなのか、位置情報なのかとか、そういったお話になると思いますけれども、これが重要なのか、それとも、方法、例えば第三者に提供するんだとか、加工するんだとか、あるいはそれが誰であるとか、そういったことが重要なのか、それとも、何に使うかという利用目的が重要なのか、そういったところをこのところずっと詰めていると思うんですが、個人的な意見として、本当に重要なのは、その結果の影響、ユーザーに与える影響、消費者に与える影響がどうなのかというところが本当は一番重要なんだろうと。

これまでどうしても細かい手続論とかの話になっていると、ルールベースの話になってしまうんですが、本当に重要なのはアウトカムベースだと思っていますので、そういったアウトカムベースでもう一度見直して、どう整理していくべきかというようなこともちょっと考える必要があるんじゃないかなと思っています。この考え方は、最近の特にアメリカがリスクマネジメントの考え方で、SP800－53なんかもそうですけれども、その方向にかなり振ってきていますので、グローバルの流れとしても、これ以上細かくしてもという

部分から少しずつアウトカムベースに変わりつつあるような気がしますので、ここの議論でもそういった視点というのももう入れていく必要があるんじゃないかなと思っています。

以上です。

【宍戸座長】　ありがとうございました。次に、宮内先生から御質問があるということですので、宮内先生、お願いします。――オンにならないということですね。

その間に、崎村さんのほうから、アウトカムベースに賛成ですという話がコメント欄に書かれています。

【手塚構成員】　その関係でいいですか。

【宍戸座長】　では、先に、手塚先生、お願いいたします。

【手塚構成員】　すみません、宮内さん。先にさせていただきます。今、寺田さんのおっしゃったことは私も大賛成で、やはりアウトカムをしっかりと一度整理していく必要があるかなというのをこのところ強く感じています。それと併せて、当然手続論といいますか、今までやってきている内容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というのを一度やるべきかなと思っております。

以上です。

【宍戸座長】　ありがとうございます。宮内先生、大丈夫でしょうか。――チャットで質問されるということですね。

その前に、崎村さんのほうで、１つ言い忘れたというのは、これは御発言ですか。

【崎村構成員】　要は、クッキーのところで話したのは、言いたかったことは、手段を規制するということは限界があって、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ませんよねということを言いたくてクッキーの話を始めて、途中で何か忘れてしまったので、補足しますということでございます。

【宍戸座長】　ありがとうございます。それでは、宮内先生の御質問はチャットでお待ちすることにして、ほかにいかがでしょうか。

その間に、少し私から、太田さんにお伺いをしたいんですけれども、サードパーティークッキーなどの問題で、アドブロッカーとかｕブロックオリジンのような、言わば消費者の側が、自分がトラックされないように自衛するというアプリやサービスがありますね。あれは今の状況の中で有効なのかどうかであったり、多くの利用者、消費者がその手のサービスを利用しないということがあるのだとすると、それはどういうところが問題があっ

てそうなっているのかとか、その辺の話をお伺いできればと思うんですが、いかがでしょうか。

【太田氏】　ありがとうございます。アドブロッカーについてですけれども、物にもよりますが、非常に有効なものだとは思います。ただ、アドブロッカーブロッカーみたいなものもありまして、そういったものを導入しているサイトもあって、アドブロッカーが入っていると、アドブロッカーを使っているから見せないよとか、そういった対応はしているんですけれども、ただ、ほとんどのサイトにおいては、アドブロッカーというのは非常に意味があって。

かつ、アプリに関しては、有料アプリの１位ってずっとアドブロッカーなんですね、この３年ぐらい、三、四年ずっと１位で、トラッキングされたくないというよりは、そこで情報、要するに、ギガが減るのが嫌だからブロックしているということなんですが、ただ、そこもブロックしているというのは広告の表示の部分ですので、裏側で情報を取得しているというところのブロックまで及んでいなかったりとか、そこをメールアドレスベースのトラッキングとなってしまうと、そういった情報でやらなくなってしまうので、むしろそういうところを超えてやるために、ちゃんとメールアドレスベースでやっていこうよというふうにゲーム業界団体は考えているのかなと思っています。

【宍戸座長】　分かりました。ありがとうございます。

それで、宮内先生から御質問が来ております。太田さんの21ページについて、現在のブラウザでもブロックの機能があります。ファイアフォックスだとクロスサイトブロックやフィンガープリントブロックができます。現在でもブロックはできるが、非常に不便になるということなのか、機能自体が不足しているということなのか教えてくださいということですが、これはいかがでしょうか。

【太田氏】　今のお話と似たような感じだと思いますが、ブロックもできるし、そんなに非常に不便になるということはないんですが、たまに、先ほどの崎村さんもおっしゃったセキュリティ用に使っているサードパーティークッキーとか、本人認証用に使っているサードパーティークッキーも使えなくなってしまうので、そこで不便が出ることはあるんですが、ほとんどの場合はあんまり不便は出ないです。

ただ、一番問題視、僕もあまりアドブロッカー賛成派ではないんですけれども、それは一番大きな問題としては、広告とかがブロックされてしまうと、要するに、メディアはどうやって食べていくんだというところと共存させるために、ブレイブとかそういったとこ

ろがお金を分配する仕組みなどをつくろうとはしていますけれども、なかなかそこまでドラスティックに広告のエコシステムが変わることはないので、そこがちゃんと広告を表示して収益を発生させるというところと、個人がそういったうざい広告とかをブロックできるというところをどう両立するかというのは非常に難しい問題かなと思っております。

【宍戸座長】　ありがとうございます。宮内先生から、機能はあるけど、強制はできない状況だということですねという御確認がありますが、そういうことで？

【太田氏】　そうですね。

【宍戸座長】　ありがとうございます。まだ時間ございますので。

【森構成員】　じゃ、お願いします。

【宍戸座長】　森先生、お願いします。

【森構成員】　ありがとうございます。私も太田さんに改めて教えていただこうと思うんですけれども、これまで例えば今のアドIDとかIDFAとかのリフレッシュできる、ユーザーが一旦変えたり、ゼロにしたりできるものに到達するまでに、スタティックなIDは駄目だという議論を経てこういうふうになってきたと思うんですけれども、もちろんブラウザがサードパーティークッキーを使えなくしたからみんなが困るよというのは困るのかもしれませんけれども、そこでまたブラウザフィンガープリントとか、さっきのUnified ID2.0とかそういったものがメールアドレスベースというときに何が困るかというと、それは当然のことながら、メールアドレスなんてそんな簡単に変えるわけにいかないので、複数持っていてもまたIDsyncが行われるわけでしょうから、そこがやっぱり一番大きな問題だと思うんですけれども、そういったことは世の中的にといいますか、業界的に許容されているものなのでしょうか。何かあまり、こんなの駄目だという強い話が聞こえてこないような気もちょっとしているのですが、その辺について教えていただければと思います。

【太田氏】　ありがとうございます。確かに以前はＵＤIDとかも変更できないようなIDでトラッキングしていこうという流れがあって、いや、それじゃ駄目だから、IDFAというのを作って、ちゃんとOSの設定で変えられるようにしていこうという流れがあった中で、それと逆行するようなフィンガープリントとかメールアドレスベースとかというのはあるんですが、要するに、そこにオプトアウトがどこかでできればいいだろうという考え方だと思います。なので、メールアドレスベースでトラッキングはしているけれども、嫌な人はここのボタンをポチッと押せば、それはこちら側ではちゃんとオプトアウトしますよというふうなものをちゃんとつくっておけば大丈夫であろうというのが業界の考え方だと思

います。

ただ、個人的に思うのは、IDFAのリフレッシュをしたりというのは完全にOS側でやっていて、自分の操作で、要するに、自分側でちゃんとIDが出ていないかとかが分かるんですけれども、オプトアウトしましたよというのは、完全に事業者側でそれをハンドリングして、ちゃんとオプトアウトされているかどうかというのはこちら側では分からないので、そういう意味ではちょっと逆行はしているんですが、業界団体としては、ちゃんとオプトアウトというボタンを設けて、そのデータを使わないようにすればオーケーだよねという認識だとは思っています。

もう一つ補足すると、今、いろいろな広告のサードパーティークッキーでオプトアウトしますボタンっていろいろなところにあると思うんですけれども、ちなみに、そのオプトアウトボタンを押したときにちゃんとオプトアウトできているのかどうかみたいなのを調べたものもあるんですが、７割ぐらいがちゃんとオプトアウトできていないみたいなそういう研究もあったりして、あんまりオプトアウトって信用できないなと僕は思っているところでございます。

【森構成員】　ありがとうございました。

【寺田構成員】　補足。

【宍戸座長】　寺田さん、お願いします。

【寺田構成員】　すみません、私ももともと広告の業界とかということもあるので。Unified ID2.0とかこの辺の考え方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ところがあります。なので、本当にこれがちゃんと業界で話をして、同意を取るというのを業界の中で誰でも分かるような仕組みとかという形にすれば、ある意味、理想的な最初の入り口にはなると思います。

オプトアウト系の問題は、これ以外にもちょっといろいろ引っかかる部分があって、これがデータが流通していく中で、CMPとかといった仕組みでどこまで、最後まで徹底的にトラッキングできるかどうかというのとのせめぎ合いが起きます。徹底的にトラッキングができれば、ちゃんと仕組みをつくれば、オプトアウトとかというのも必要なところでできるということになるんですけれども、もう一方で、徹底的なトラッキングができてしまうことがいいのか・悪いのか問題というのも起きているのは事実なので、この辺りは多分、業界だけではなくて、消費者であったりとかそういったところの中で、何が許されて、どこまでは危ないのかというような、何か一種の線引きをしないと難しいんじゃないなとい

うふうにはちょっと思っています。

【森構成員】　さらによろしいでしょうか。

【宍戸座長】　では、森先生。

【森構成員】　ありがとうございます。そうしますと、じゃ、オプトインでそういう何かえぐいIDを作ってくださいという人がいるとはちょっと思えないんですけれども、そこがよく分からないなということが１点です。

あと、２点目は、私も伺っていてそうだと思いました。オプトアウト、どこかで統合的に管理していなければ、メールアドレスをハッシュ化した数値なんていうのはアルゴリズムが決まっていれば誰でも作れるわけで、いろいろなところで使っているやつをいっせのせでオプトアウトすることなんて難しんじゃないかというふうに思いましたので、後半については寺田さんのおっしゃるとおりだなと思いました。

【宍戸座長】　ありがとうございます。さらに、崎村さんから御質問が来ています。１つは、太田さんへ、Do Not Callと同様の動きはないのでしょうかという御質問です。太田さんからお願いできますか。

【太田氏】　はい。多分、Do Not Trackの話だと思うんですけれども、Do Not Trackって１回あったんですが、それは失敗して、また新しい、ちょっと名前忘れちゃったんですけれども、新しいものが出てきてはいて、ちょっと僕もそれがDo Not Trackと何が違うのかというところまで追えていないんですけれども、同様の動きはありますというところだけお伝えします。

【崎村構成員】　たしかDo Not Trackってあれですよね、ブラウザベースですよね。

【太田氏】　そうです。

【崎村構成員】　僕がDo Not Call同様と言ったのは、あれは中央にレポジトリがあって、そこにある人にはやっちゃいけないみたいな感じですよね。

【太田氏】　あー、それは僕は分からないですね。

【崎村構成員】　あと、ブラウザだけに注目しているとアプリの側が落ちるので、そこのところはどうなのかなというのがあってですね。

【太田氏】　おっしゃるとおりだと思います。

【宍戸座長】　ありがとうございます。それから、もう一個、崎村さんから赤阪さんへ、知られないように個人に関連する情報を取得しようとする傾向が強いように思うのですが、そのようなものは欺瞞的な慣習であると言えないでしょうかということで、これは個人情

報保護委員会と公取の権限にも関わる問題ではありますけれども、お答えいただける範囲でいかがですか。

【崎村構成員】　補足します。実は先ほど太田さんからありましたように、JSタグなんかを使って、思いもよらないようなところがどんどん情報を吸っていくわけですよね。そうやって分からないように分からないようにデータを取っていこうとする傾向がすごく強いように感じたんですけれども、そういったものというのは何か欺瞞的な慣習であるとか、何か制度的に何とか手当てをしていくような方向というのは考えられないんでしょうかと、そういう御質問でございます。

【赤阪個人情報保護委員会事務局参事官】　ありがとうございます。最初に森先生からも御指摘いただいたところですけれども、個人情報保護法は、個人情報として取扱いをするところで規律をかけていく法律になっておりまして、そういった中で、今回、個人関連情報自体はかなり定義としては幅広いものになっているわけですが、それが個人情報として取り扱うことを前提に取得する場合に今回規律にかけるところでございます。今回まずはそういうところからスタートしているところでございますが、世の中の動きはいろいろあるかと思いますので、そういったところは我々でできるところ、あるいは関係省庁でできるところも含めて引き続き検討していきたいと思っております。

【宍戸座長】　ありがとうございました。よろしいですか、崎村さん。

【崎村構成員】　はい、ありがとうございました。

【宍戸座長】　時間が押していますが、寺田さん、簡潔にお願いします。

【寺田構成員】　先ほどの崎村さんのDo Not Call、Do Not Trackingの話ですけれども、最新の情報だと、CPRA、11月にカリフォルニアで住民投票で可決、まだされていないのかな、一応、可決されるのはほぼ間違いと言われているものですけれども、この中で「共有するな」という、そういうボタンを設定しなければならないという義務化というのがあって、Do not tracking2.0というような言われ方をしているようなそういう仕組みが提案されています。情報です。

【宍戸座長】　ありがとうございました。まだいろいろ御意見や御質問等あろうかと思いますが、予定した時間ですので、ひとまず今日のところはここまでとさせていただきたいと思います。

私から一言申し上げますと、今日は、これまでの状況を把握した上で、かなり実質的に問題をどう捉えるかということについて重要な御指摘が幾つもあったと思いま

す。

一方で、新保先生からは、同意の取得方法を超えて、同意の効力とか、そもそもの同意の法的性格とは一体なのかということについての問題提起がございました。また、この場では、クッキーを規制する、何か具体的な手段を規制するということを超えて、アウトカムベースでの規制をきちんと考えていくべきでないかという御指摘がございました。

もちろんきちんとしたアウトカム、特に個人の権利利益あるいはプライバシー等にとってどういう影響があるのかということを実質的に考えていくことはとても大事であります。また他方で、現状において特にクッキーだったり、フィンガープリントにしてもそうですけれども、今後かなり問題がありそうな技術が、まさに今の使われ方だとアウトカムとして非常に問題がありそうだということも太田さんからいろいろインプットをいただきましたので、これらの本日いただいた情報、御意見等を踏まえて、利用者情報の取扱いについては議論をさらに深めていく必要があると思っております。本日はありがとうございました。

実はまだこの後アジェンダがございまして、もう少しお付き合いいただきたいのですけれども、最後に、資料５、改正電気通信事業法の施行に向けた準備について事務局から御報告があると伺っておりますので、よろしくお願いいたします。

【小川消費者行政第二課長】　事務局の消費者行政第二課長、小川でございます。資料５に基づきまして、改正電気通信事業法の施行に向けた準備について御説明をさせていただきます。

まず１ページ目を御覧ください。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の解説のところでございますけれども、今回電気通信事業法の改正に伴いまして、外国法人についての規定の整備が行われたことに伴いまして、解説のところでございますが、外国法人が日本国内において電気通信役務を提供する電気通信事業を営む場合、外国から日本国内にある者に対して電気通信役務を提供する電気通信事業を営む場合にも適用されるという形に電気通信事業法はなりますので、ガイドラインについても、当該外国法人に適用されるといった形で修正をさせていただく予定でございます。

それから、２ページ目を御覧ください。前回も軽く御報告をさせていただきました、通信の秘密の確保に支障があるときの業務の改善命令の発動に係る指針の案につ

いて御説明をさせていただきます。まず、趣旨についてはこの四角の中にあるとおりでございます。１番、策定の趣旨といたしまして、（１）でございますが、通信の秘密に関連した規定として、まず憲法21条、それから、電気通信事業法４条がございます。また、電気通信事業法29条でございますが、電気通信事業者に対しまして、業務の方法の改善その他の措置を取るべきことを命ずることができる事項の１つとして、電気通信事業者の業務の方法に関し通信の秘密の確保に支障があるときということが規定されておりまして、この命令に違反した者に対する罰則が法186条第３号ということで規定されております。

（２）でございますが、この執行指針の策定の趣旨でございます。通信の秘密の確保に関する考え方を明らかにするとともに、総務大臣が各事業者の取組が十分機能していないとして業務改善命令を発する基準や事例を指針として類型的に示して、透明性・予見可能性を高めるということを目的とするものでございます。

次のページを御覧ください。２番、業務改善命令の執行指針でございます。（１）といたしましては、先ほど申し上げたように、法第29条第１項第１号の趣旨ということで、ここで、（２）でございますが、電気通信事業者の考え方としては、事業法に基づきまして登録または届出の対象となる者でございます。

業務の方法でございますが、業務の管理運営方法、窓口業務等の日常業務の取扱方法など通信の秘密に係る情報を取り扱う場合の業務全般ということになっておりまして、社内規則等のみで形式的に評価されるのではなくて、業務の実情に照らして客観的に評価されるということで、また、取扱いが人か機械かは問わないということになっています。

（４）でございますが、通信の秘密の確保に支障があるときでございます。通信の秘密の範囲としては、個別の通信に係る通信内容のほか、いわゆるメタデータ、通信の日時、場所、通信当事者の氏名、住所などについても含まれるということになりまして、支障があるときというのは、通信の秘密の取扱いが不適切な場合、また保護するための態勢が不十分である場合などでございます。

４ページでございます。この執行指針におきましては、通信の秘密の確保に支障があるときとして、想定されるケースについて４つに類型化して例示をするということになっております。①としては、通信の秘密に係る情報の取扱いを示したポリシー・方針が不適切な例、②といたしましては、通信の秘密の取得・利用等が不適切な例と

いうことでございます。

５ページでございます。③といたしまして、情報管理態勢が不適切な例として、組織的、人的、物理的、技術的、それぞれ例を示させていただいております。最後に、④でございますが、苦情・相談等対応態勢が不適切な例ということで示させていただいております。執行指針については以上でございます。

次、６ページでございます。こちらも前回御紹介をさせていただいたものでございますが、利用者からの同意取得の在り方に関する考え方を明らかにするために、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の解説の参照文書としてこの文書について公表するという予定でございます。

１つ目でございますが、通信の秘密における同意取得の意味ということで書かせていただいております。（１）でございますが、通信の秘密の保護趣旨は、表現の自由、プライバシー、安心安全な通信といったことでございまして、個々のユーザーの通信情報の取得・利用などについては、通信当事者である利用者の有効な同意または違法性阻却事由がある場合によって適法化されるということでございます。

（２）の①でございますが、通信の秘密を侵害する行為は、通信当事者以外の第三者による知得、窃用、漏えいを意味しますけれども、有効な同意がある場合は、通信当事者の意思に反さない利用であるため、通信の秘密の侵害に当たらないというふうに解されるわけでございます。

７ページを御覧ください。（２）でございますけれども、有効な同意のために必要とされる同意取得の在り方として、電気通信事業法 29 条における同意の取得の在り方として、こちらでは業務の方法として外形的に示される同意取得の在り方として、例えば個別具体的かつ明確な同意というのがございます。こちらにつきましては、矢印の下ですけれども、有効な同意、すなわち、利用者から見て真に理解して同意しているかというのにつながるというふうに言えるものでございます。

それから、（３）でございますが、先ほど御説明させていただきました執行指針の効果ということでございます。同意の取得の在り方に関する参照文書は、先ほどの執行指針と組み合わせて参照することが有効というふうに考えられます。

８ページでございます。２番でございますが、通信の秘密の侵害を防止する観点からリスク分析の重要性ということでございます。（１）の①でございますが、プライバシー影響評価（PIA）の通信の秘密への応用ということで、通信の秘密に関する情報

は、プライバシー性の高い重要なデータということで、通信の秘密に係る主体の権利、自由に対する影響やリスクを適切に把握し管理することが重要ということで、また、応用することで表現の自由や安心安全な通信網への利用者の信頼・期待も検討し得るということです。

②でございますが、リスク評価を応用した有効な同意の取得の在り方というのが考えられるということでございまして、利用者の有効な同意が取得されているということで実質的に評価できる場合に、この手続が取られるということでございます。ただ、その場合にも、代替的な利用者保護は図られている必要があるということでございます。

また、業界団体の場においてリスク評価などを行った上で、業界ルールを策定するということも考え得るということでございます。

１つ飛ばしまして 10 ページでございます。こちらでは、有効な同意・同意取得の在り方について書かせていただいております。基本的には、個別具体的かつ明確な同意であることが有効な同意では必要でございます。また、利用者の理解が困難なものというのは正当化根拠とできないということです。個別とは、サービスごとに通信の秘密の取扱いについての同意ということを本人が認識するということでございます。それで、具体的というのは、利用者がその同意の内容・意味を正確に認識し、十分に理解した上で、真意に基づいて行った同意であるということが求められます。また、②でございますが、明確とは、画面上でのクリック、チェックボックスへのチェックや文書による同意など外部的に同意の事実が明らかな場合ということが考えられます。また、③その他でございますが、情報取得等の時点以前に同意がなされる必要があるということでございます。

11 ページ以降が、このような考え方に基づきました個別ケースの検討ということで事例をお示ししているということでございます。有効な同意とは、通信当事者がその意味を正確に理解した上で真意に基づいて同意したと評価できる必要があるということで、（１－１）でございますが、ユーザアカウント作成時における一括同意ということを示させていただいております。通信の秘密に係る情報の活用方法について束ねて一括で説明して同意取得することについても、利用者が明確に認識、理解した上で、真意に基づいた同意であると評価できる場合には有効な同意として認められ得るということでございますが、その場合、後に個別のサービスごとに同意撤回できるよ

うにすることが求められるということで書かせていただいております。

それから、（１－２）でございます。２階層による同意取得として、１階層目はレイヤードアプローチでございますけれども、明確かつ平易な言葉を使用した分かりやすい概要版を提示するということで、２階層目に、関心がある方には、クリックした場合に詳細な情報が示されるというような形が考えられると。また、後に個別サービスごとに同意撤回でき、かつ撤回するためのページへのアクセスが容易などの方法が考えられるということでございます。

それから、最後、12 ページでございます。（１－３）でございますが、既存のサービスに付加的サービスを追加する場合の同意取得の在り方でございます。こちらについて、付加的なサービスが当初サービスから通常想定され得る利用と言えない限りは、新たな利用目的についての同意が追加で必要ということでございます。

それから、（２）同意の管理でございます。こちらは、プライバシーダッシュボードなどの仕組みにつきましては、事業者の透明性を確保して、利用者の同意撤回等を容易にするものとして推奨されるということで、利用者が容易に同意管理をできる仕組みを有していることは、同意手続を簡素化させる一事情として評価され得るということでございます。それで、同意取得時点で一括して同意を取得している場合は、同意撤回は個別サービスごとにできるなどの仕組みが通常求められる。また、定期的に利用者にリマインドすることで、利用者の同意の意思を確認することは望ましい取組として評価されると、こういった内容になっております。

以上でございます。

【宍戸座長】　ありがとうございました。

その他、事務局から、今後の進め方などについて連絡事項があればお願いいたします。

【小川消費者行政第二課長】　参考資料４を御覧ください。参考資料４につきましては、前回お示しさせていただいた内容でございますが、来年２月、３月には違法有害情報、誹謗中傷、フェイクニュース関係のフォローアップも予定されていること、また、利用者情報の適切な確保については、論点も多いことを踏まえまして、議論の効率的な進め方を含めまして宍戸座長と御相談させていただきたいと思っております。

また、次回会合につきましては、別途事務局から御案内をさせていただきます。

事務局からは以上でございます。

【宍戸座長】　ありがとうございました。これにて本日予定された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（第22回）会合を終了とさせていただきます。本日は、皆様お忙しい中御出席をいただきまして、誠にありがとうございました。