

プラットフォームサービスに関する研究会（第21回）

- 1 日時 令和2年11月5日（木）15時00分～17時00分
- 2 開催場所 総務省第1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、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参事官 赤阪 晋介
 - （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、片桐消費者行政第一課長、小川消費者行
政第二課長、高田消費者行政第二課企画官、丸山消費者行政第二課長補佐、中川
消費者行政第二課長補佐、今村消費者行政第二課専門職
 - （4） ゲストスピーカー
三菱総合研究所 西角主席研究員、安江チーフコンサルタント
日本総合研究所 小竹副主任研究員
- 4 議事
 - （1） 今後の検討の進め方
 - （2） 利用者情報の適切な取扱いの確保に向けて
 - （3） その他

【宍戸座長】 本日は皆様、お忙しい中お集まりいただき、誠にありがとうございます。
定刻を過ぎましたので、プラットフォームサービスに関する研究会第21回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て実施させていただいております。

それでは、事務局よりウェブ会議による開催上の注意事項について御案内がございます。よろしくお願いたします。

【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きます。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、映像もオフにさせ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いただければ対応させていただきます。

注意事項は以上となります。

なお、本日木村構成員は御欠席となります。また、大谷構成員は15時15分頃からの御参加となります。

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

【宍戸座長】 それでは、議事に入ります。

本日は、8月に緊急提言を取りまとめて以来の開催に当たりますので、事務局から今後の検討の進め方について、まず御説明をいただきます。その次に、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いただきます。さらに、生員構成委員から「利用者情報の保護に関わる欧州の状況」について、三菱総合研究所から「E U・e プライバシー規則（案）に関する議論の状況」について、日本総合研究所から「スマートフォンプライバシーアウトLOOKの取組内容の紹介」について御発表いただきます。その後、自由討議として、全体を通して構成員の皆様から御意見をいただきます。そして、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きます。本日は盛りだくさんでございますが、どうぞよろしく願いいたします。

それでは、まず事務局から、今後の検討の進め方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】 事務局の総務省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、今後の検討の進め方について（案）の御説明をさせていただきます。

1 ページおめくりください。主な検討項目の1つ目として、インターネット上の違法・有害情報に対する対応（誹謗中傷、フェイクニュース等）でございます。こちらにつきましては、まず、2枚おめくりいただきまして3ページ目を御覧いただければと思いますけれども、先ほど座長からもお話をいただきました、8月にこちらの研究会でおまとめいただきましたインターネット上の誹謗中傷への対応の在り方に関する緊急提言がございます。こちら内容の10番のところの「おわりに」でございますが、「定期的に、本緊急提言において示した様々な観点についてそれぞれのステークホルダーが行った取組状況の把握を引き続き行い、更なる対応の必要性等について検討を深めていく」という記述がございます。

また、次の4ページ目を御覧ください。こちらの緊急提言、それから発信者情報開示の在り方に関する研究会の中間取りまとめが発表されたことを踏まえまして、総務省としてインターネット上の誹謗中傷への対応に関する政策パッケージを9月に取りまとめをしております、発表しております。詳細の本文につきましては参考資料2にお付けしておりますので、適宜御参照いただければと思っております。

こちらの政策パッケージにつきまして、インターネット上の誹謗中傷に対応する対策として各府省、それから産学民のステークホルダーと連携して早急に対応を行っているところでございます、最後のところでございますが、今後プラットフォームサービスに関する本研究会において進捗状況等の検証を実施ということで書かせていただいております。

こちら、特に1番目のユーザーに対する情報モラル、ICTリテラシーの向上のための啓発活動、2番目のプラットフォーム事業者の自主的取組の支援と透明性・アカウントビ

リティの向上、4番目の相談対応の充実に向けた連携と体制整備などにつきましては、緊急提言の内容を踏まえたものでございまして、3番目のところは発信者情報開示の在り方に関する研究会の内容を踏まえたものでございます。

2番目のところの③でございますが、こちらにつきまして、プラットフォーム事業者の自主的な取組の報告等について、事業者による透明性・アカウントビリティ確保方策を促進し、取組状況の把握や評価方法の検討実施と、こちらについても、括弧内でございますが、プラットフォームサービスに関する研究会などの場を通じて今年度中にフォローアップを実施していくということが既に書かれております。

それから、ちょっと戻っていただきまして2ページ目を御覧いただければと思います。フェイクニュースの関係でございますけれども、こちらについては、まずは民間部門における自主的な取組を基本とした対策を推進するというところでございまして、1つ目の矢印のところでございますが、フェイクニュースや偽情報の実態調査を実施するというところで、こちらについては、本日の参考資料3と4に総務省が行った実態調査、公表されているものですが、こちらについて御報告としてつけさせていただいております。

それから2つ目の矢印でございますがフォーラムの設置ということで、こちらについては参考資料5にもつけさせていただいております。

それで、3つ目の矢印でございますが、プラットフォーム事業者による透明性・アカウントビリティの確保方策の実施に期待ということで、こちらについては行政から一定の関与、フォローアップを行っていくという言及がございます。

長くなって恐縮ですが1ページ目に戻っていただきまして、インターネット上の違法・有害情報に対する対応につきましては、これらのことを踏まえまして誹謗中傷、フェイクニュースともにフォローアップを行っていくということで、具体的にはこの1ページ目の矢印の2月、3月のところの四角の中を御覧いただければと思いますけれども、先ほど御説明した政策パッケージ、誹謗中傷の関係の対策の政策パッケージ、それからフェイクニュースの関係の最終取りまとめの取組状況のフォローアップというのを2月、3月に行っていくということでいかがかというような案でございます。

それから、主な検討項目の2つ目の○でございますが、利用者情報の適切な取扱いの確保に向けた在り方というところでございます。こちらについては、もう一度2ページ目の最終報告書の概要のところにお戻りいただければと思います。

こちらのIでございますが、利用者情報の適切な取扱いの確保ということで、1つ目の

四角、国外事業者に対して電気通信事業法の規律を及ぼすと、こちらについては本年5月に成立した事業法改正を反映しているところでございます。2つ目の四角のところでは、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、欧米等の議論を参考にしながら今後引き続き検討深めると、新しい時代にふさわしい通信の秘密・プライバシーの保護に係る規律の在り方を念頭に具体的な検討を進めると書かれております。

1ページ目にお戻りいただきまして、この利用者情報の適切な取扱いの確保に向けた検討ということで、こちらについて11月の〇、11月5日、本日でございますが、本日から利用者情報の適切な取扱いの確保に向けた検討ということでスタートさせていただき、12月以降検討を進めていくということではいかがかといったような案でございます。

説明は以上でございます。

【宋戸座長】 小川課長、ありがとうございます。

今課長から御説明のありましたこのプラットフォームサービスに関する研究会での検討のうち、1点、私から御報告を申し上げることがございます。2ページ、最終報告書の概要でございますけれども、こちらではフェイクニュースや偽情報への対応について、2つ目の矢印でございますが、「関係者で構成するフォーラムを設置し、フェイクニュースや偽情報の実態や関係者の取組の進捗状況を共有しつつ継続検討」ということが記載されているところでございます。

そこで、お手元の参考資料5を御覧ください。このような構成員の皆様に取りまとめいただきました最終報告書を受けまして、セーフティーインターネット協会におかれまして、Disinformation対策フォーラムの設置に御苦労いただきまして、後ろを御覧いただきたいと思いますが、去る6月に初回の会合を持ち、10月19日に第2回の会合を持っているところでございます。

戻っていただきまして1枚目、構成員はそこにお示ししているとおりでありまして、私が座長を仰せつかっております。

事業者である構成員といたしましてはFacebook Japan、Google合同会社、Twitter Japan、それからヤフー株式会社であり、またオブザーバーとしては日本新聞協会、日本放送協会、日本民間放送連盟の各メディア団体の方々と消費者庁、そして総務省に議論に加わっていただいているところでございます。

2枚目でございますけれども、偽情報流通の実態を正確に把握し、その対応について多面的に検討すべく、産学官民の多様なステークホルダーによる協力関係の構築を図り、対

話の枠組みを設けるという趣旨でございまして、引き続きこのフォーラムで議論し、またその成果につきましては、いずれこのプラットフォームサービスに関する研究会の場で最終報告書のフォローアップという形で御報告させていただくことになるのではないかと思っております。

私からの補足は以上でございます。

ここまでの説明につきまして、構成員の皆様から質問あるいはコメント等があれば承りたいと存じますが、いかがでございでしょうか。よろしいでしょうか。

ありがとうございます。今、よろしいと言っていたので、したがいまして、今小川課長からいただいた宿題を、我々が順次これからやっていくということになるわけでございます。

そこで、議題2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、事務局から御説明をお願いいたします。

【小川消費者行政第二課長】 事業局の総務省消費者行政第二課長の小川でございます。資料2、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させていただきます。

まず、1ページ目をおめくりください。まず、最終報告書における記述の抜粋でございます。こちらは皆様御案内のところでございますが、念のため言及させていただきます。

まず、最終報告書におきましての整理に当たっての基本的視点といたしまして、多様な電気通信サービスを通じて利用者情報が取得されるということで、より多くの種類の情報が、より頻繁にかつ、より多くの事業者間で共有・活用されるようになるなど、その取扱いが質・量ともに深化・拡大していくことが現在想定されるということの指摘をいただいております。

そして、また2段落目のところでございますが、ネット環境の進化に伴って多様なサービスが展開される中、累次の同意取得が繰り返され、かえって利用者の理解が不十分となるような「同意疲れ」の課題ということも指摘をいただいております。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、ウェブ上の行動履歴、それから利用者の端末に蓄積される端末IDやクッキーなど端末を識別する情報等について、プロファイリング、行動ターゲティングなど多様なサービスやビジネスにおいて活用されるということが考えられますが、一方で通信の秘密やプライバシー保護との関係でその取扱いの在り方が課題となりつつあるというような視点を御提示いただいております。

2ページ目でございますけれども、こちらで今後の検討の具体的な方向性ということで、2の(1)でございますが、いわゆる「同意疲れ」への対応ということで、より多くの利用者情報が利用者から取得されるようになると、また、同意取得時の説明も複雑で分かりにくくなるといったようなことになって、その中で有効な同意の取得とか、その際の説明の在り方について、さらに検討を深めることが必要であるという御指摘をいただいております。

また、(2)でございますが端末情報の取扱いということで、こちらについても利用者情報の取得・活用ニーズが一段と高まる中で、利用者の利便性と通信の秘密、プライバシー保護とのバランスを適切に確保することが一層重要ということで、このため、端末情報の適切な取扱いを確保するということが非常に重要になる中、具体的な規律の在り方について、欧州のeプライバシー規則(案)の議論等も参考にしながら、今後引き続き検討を深めることが必要という御指摘をいただいております。

次の3ページ目でございますけれども、その際ということで、必要に応じて、これまで総務省において策定してきた指針など、これ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や位置情報プライバシーレポートやスマートフォン・プライバシー・イニシアティブなどがございますが、それについても新しい時代にふさわしい通信の秘密・プライバシーの保護に係る規律の在り方を念頭に置いて、具体的な検討を進めていってはどうかというような御示唆をいただいているところでございます。

次、4ページ目は、こちらも既存の資料でございます。プラットフォームということで、レイヤを超えた一体的な役務提供を行うということなど、各レイヤの影響力も拡大しているということで、Society 5.0などIoT機器のデータなどを集約・分析するなどの点でもプラットフォームサービスの社会的役割は拡大するのではないかという御指摘をいただいております。

それから次の5ページ目、これも既存の資料でございますけれども、インターネットの普及・発展により、OTT事業者がグローバルに事業を展開し、社会経済活動に与える影響は大きくなっているということで、例えば①から⑤ですが、オンライン・ショッピングモールであるとかアプリストア、オンライン広告プラットフォーム、オンライン検索サービス、ソーシャル・ネットワーキング・サービスと、このそれぞれにつきまして全て、こちらの右側でございます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で、電気通信事業者が提供する電気通信役務に該当するというので、検閲の禁止とか通信の秘

密に関する規律は及ぶといったようなことについても既に資料として出させていただいております。

それから、6ページ目と7ページ目につきましては、利用者情報に関する主な規律の国際的な比較ということで、詳細の御説明は割愛させていただきますけども、日本における電気通信事業法とか、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、それから個人情報保護法、また欧州ですとGDPRとかePrivacy Regulation（案）、また米国ですと、例えばカリフォルニア州法などについて比較させていただいております。

このような状況を踏まえまして、8ページ目を御覧ください。利用者情報の適切な取扱いの確保に向けての検討課題案ということでお示しさせていただいております。こちらについては、またいろいろと御意見を賜ればと思っているところがございますが、現段階のものとして御説明させていただきます。

まず、1つ目の○でございますが、利用者の利便性と通信の秘密やプライバシーの保護とのバランスをどのように確保していくかということで、プラットフォーム事業者のサービスを利用者が安心して利用できるよう、利用者情報の適切な取扱いをどのように確保していくのか。

また、2つ目の○でございますが、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、それからウェブ上の行動履歴、それから端末IDやクッキーなどの端末を識別する情報等の実態はどうなっているかと。

3つ目の○でございますが、このような実態を踏まえまして通信の秘密やプライバシー保護の観点で、その適切な取扱いの確保のために、どのような規律をしていくべきかと。

それから、4つ目の○でございますけども、先ほども出てまいりましたが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や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・イニシアティブなどの指針について、どのように見直していくことが適切であるか。

それから、5つ目の○でございますが、非常に変化の激しい分野でもございますので、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ために、どのようなアプローチをとり具体化させていくことが適切かといったような検討課題案でございます。

以下については、参考資料でございますので御説明は割愛させていただきます。

以上でございます。

【宍戸座長】 ありがとうございます。

ただいまの事務局の御説明につきまして、質問あるいはコメントなどがございますでしょうか。ありましたら、私にお知らせいただければと思います。

それでは、新保先生、お願いいたします。これは後ほどコメントをいただくということでしょうか、今御発言があるのでしょうか。お願いします。

【新保座長代理】 スマートフォン・プライバシーはまた後ほど御説明いただいて、今の部分でもかなりいろいろとコメントがありますが、この後にスマートフォン・プライバシーなどについて、それも含めて、あと今回の改正個人情報保護法では法定公表事項の公表などの見直しなども行われますので、そこについてはまた後ほどコメントさせていただきたいと思います。

【宍戸座長】 ありがとうございます。では、後ほどお話を伺いたいと思います。

ほかにかがでしょうか。

よろしいようであれば、8ページにあります検討課題案に沿って今後の検討を進めさせていただきたいと思います。

そこで、続きまして資料3、利用者情報の保護に関わる欧州の状況について、生貝構成員から御発表させていただきたいと思います。よろしく願いいたします。

【生貝構成員】 生貝直人でございます。一枚紙の裏表に沿ってお話をさせていただきます。

私、ちょうどこの研究会から始まったのが約2年前、その当時に特に利用者情報の取扱いについても議論になり、そしてePrivacy Regulationについても御報告させていただいたところ、そのことの最新状況については、この後三菱様のほうから御説明があると承知しておりますけれども、やはり特にこの2年間で、現在進行形のことも含めて利用者情報の保護に直接あるいは広い意味で関わる動きが欧州でも様々な形で出てきております。

ここでは本当に項目や事項程度という形になるのでありますけれども、これからまさにここで検討されるテーマを進めていくに当たって継続的にフォローしていく必要があるのではないかということについて、若干アラカルト的でございますけれども御紹介させていただくということになります。

まず、1つ目の個人の同意に関する動向というところでございます。このことはまさしく、ただいま事務局から御説明いただいた事項の中でも「同意」という概念を重視されて

いるところがございますけれども、幾つか特筆すべき動きというものがございまして、まず1つは、ePrivacy Regulationがこれからヨーロッパでどうなっていくのかということはこの研究会でもある程度気にしてきたところかと思えます。現在に至るまで、それ自体はまだ成立には至っていないわけではありますが、もともとヨーロッパのほうにはePrivacy Directiveというのがございまして、これが5条3項の中でterminal equipment、まさに端末に保存された情報、ここにクッキーなどが含まれ、それを利用するに当たって事前同意が必要であると記述されていたところがございます。これは2009年のePrivacy指令改正からであります。

この同意というものが、GDPR施行前は各国ごとに暗黙の同意を認めたりといったようなところも多かったのですけれども、GDPRが施行されて以来、この事前同意というのがまさに明白でかつ自由に与えられたものではないというGDPRの同意にそろえられましたことから、この前後ほどから欧州のウェブサイトにはアクセスすると、クッキー等に必ず同意のクリックを求められるようになってきているかと思えます。ですので、ePrivacyに関して、ePrivacy Regulationを待つまでもなく、端末情報という意味では既に欧州はかなり動いており、これはもしかすると寺田様のほうがお詳しいところかと思えますけれども、それに伴って、特に広告事業者等の実際の同意の扱いですとか、デジタル広告のプラットフォームの行動を含めてかなり変わってきているところではあります。

さらに、ここには書いてございませんけれども、後で三菱様のところの参考資料にも少しございましたとおり、2019年10月には、これに関わるC J E Uの判決というものも出ておりまして、厳密には旧データ保護指令時代の行為に対して争われたものでございますけれども、まさに具体的な裁判所の動きというものも起こっているところで、引き続き注視していく必要があるかと思えます。

さらに2つ目として、これも広く日本でも報じられましたが、フランスのC N I Lが2019年1月にGoogleに対して5,000万ユーロのGDPR制裁金を科したということで、非常に大きな注目を集めたところがございます。このことというのは、まさに同意の在り方というもの1つの大きなテーマとして扱われたものでございまして、透明性のある情報提供、これはクリックを5回や6回しなければ全ての情報を把握することができなかった、あるいはターゲティング広告に関わる同意というのがデフォルトでオンにチェックされていたということ、それからアカウントを作成する前提として特定性のないデータ処理の同意を求めていたということ、これらが問題視されてこういった事態になったわけで

ございます。Googleの側もこの決定の有効性というものを裁判で争いまして、少しその係争が続いていたんですが、これもちょうど今年の8月頃だったでしょうか、正式にCNILの判断が有効だと認められたという現在進行形の動きに近いところもございます。

それから3つ目、これも日本でも大きく注目を集めましたけれども、ドイツ連邦カルテル庁によるデータ保護法の執行というところでございます。これはまだ係争中の部分がございますけれども、御承知のとおりFacebookが対象になりましたが、利用者にとって実質的に切替えや選択の余地のない、市場支配力の高いプラットフォームにおける同意というものは、どういう形であれば自由で、そして本当に本人の能動的な同意という形で評価されるのかということをめぐる議論であり、特に全ての同じルールを全ての事業者に求めるのか、あるいは特に巨大なプラットフォーム様にどういった特別な配慮をしていただくかという意味でも非常に重要なところで、このことについても直近でドイツの連邦最高裁がこの連邦カルテル庁側に少しポジティブな判断、決定の差止めを否定したということが、つい最近も報じられていたところであります。

それから2番目のところ、デジタルサービス法パッケージでございます。このことについては、非常に大きな動きでございまして、御承知のとおり昨年末までのヨーロッパのジャン・クロード・ユンケル政権の中で、ほぼ欧州のデジタル法制全体に関わる大規模な改革パッケージを実行してきたところがございますけれども、そこで手をつけなかったある種の本丸としての電子商取引指令の本格的な見直しというものが進められておりまして、これが恐らく来月の頭ぐらいには出るという、提案されるという非常にタイミングの悪い時点でのお話という形になります。

これは大きく2つの柱に分かれておりまして、既存のプロバイダ責任制限ルールの見直しを含む、全てのデジタルサービスに関わる「デジタルサービスの責任」。2番目としてゲートキーパーとしての役割を果たし強力なネットワーク効果を有する「大規模オンラインプラットフォームの事前規制手段」から構成されます。まだ詳細は出ていないのですが、今年の6月に行われたインパクトアセスメントで大まかな方向性、含まれ得る論点というものが出されておりましたので、そこを簡単に御紹介いたします。

オプション1は、基本的には既存枠組みの原則維持。いわゆるプロバイダ責任で言えばノーティスアンドアクションを含めてさらに運用をしっかりとっていくといったようなことが中心ですが、オプション2のところと比較的大きくて、特に1ポツ目の4行のところだけを見ても、例えばマーケットプレイスの商業的利用者に関するいわゆるKYCの義務で

すとか、あるいは違法コンテンツ削除に係るtrusted flaggersとの効果的な協力、それから、Disinformationに関しては、直接コンテンツ自体を規制することはないのだけれど、そういうものに用いられるサービスのリスクアセスメントをするという、こちらの研究会でもフェイクニュース対策の文脈で行ってきた議論と恐らく符合するところを、もう少し自主規制から共同規制的にしていこうというところも含まれるのだと思います。

それから、合法的なコンテンツ等の削除に対するより効果的な救済措置、そしてそれらに関わる透明性・レポート義務等々が含まれるというのがこの中の1つの柱です。

それからもう一つ個人データ、まさにGDPRでプロファイリングですとかそういったことは規律されているわけでございますけれども、コンテンツモデレーションや推薦システムのアルゴリズム、特に政治広告やマイクロターゲティングのオンライン広告等に関して、アカウントビリティを確保するための透明性／報告／独立監査義務といったようなことも含まれる見込みであります。

このことについては、まだ少し抽象的なことしか書かれていないのでありますけれども、ちょうど2週間ほど前に欧州議会のほうでこの方向で進めていくべきだといったようなポジションペーパーが出されまして、それによりまして、例えばデジタルサービスによるプロファイリング、アルゴリズムに基づく自動的決定にあらがう権利でありますとか、あるいはデジタルサービスを匿名で使う権利でありますとか、行動ターゲティング広告に関するより厳しい規律といったようなことなどのオプションが提示されているところがございます。この部分というのは特に本研究会の利用者情報の保護ということと、それからまさにDisinformationへの対策等を含めた両面に関わるところであり、よく見ておく必要があるかなと理解しております。

それから3つ目、最後のポツのところに関してはEU域外サービスへの適用、いわゆる域外適用ということと、それからこれは違法コンテンツを落とすことを継続的に怠ったとか、その他のシステムティックな違反に対する行政罰も導入する方向だということで、これも既存のライアビリティの観点からすると興味深いところかなと思います。

オプション3に関してはヨーロッパ特有の文脈ですので割愛しますが、こういったプラットフォームのルールをオーバーサイトしていくための強力な機関をつくる必要があるのではないかとこのところも含めた議論がされているところです。

それからこれは2つ目の柱ということになりますが大規模オンラインプラットフォームの事前規制手段について、こちら6月にインパクトアセスメントが行われております。

そこにおきましては、1つ目のポツのところは、ビジネスユーザーの保護強化というところで、我が国でも今年法律が成立したもののモデルになりましたオンライン媒介サービス透明性・公正性促進規則、いわゆるP to B規則の見直しを早速行って特定の行為を禁止したり、あるいはノンパーソナルデータに関するビジネスユーザーのアクセスを保障したり、セルフプリフェアリングを禁止したりといったような、これ自体非常に興味深い内容が多く含まれるのですけれども、少しスコープから外れますのでここはさておいても、対消費者に関わる事項としても、特にそういった大規模なプラットフォームに関しては、データのポータビリティに関するGDPR20条を超えたような特別の義務、あるいはインターオペラビリティそのものの義務づけというものを検討していくべきではないかといったようなこと、このことというのが、この文章の中ですとテレコミュニケーション規制の経験というものの違いには留意する必要があるけれども、しっかり参照しながら進めていく必要があるということが書かれていたところでした。

そのほかに、DG COMP、競争総局のほうでNew Competition Tool、それからデジタル市場法という提案の動きもこれに関連して進められておりまして、これがもしかするとデジタル市場法のほうにこの後者のほうは挿入されるのかなという気もしているんですけども、いずれにしてもこれも来月には明らかになろうかと思います。

そして、3つ目に欧州データ戦略が、今年の2月に出まして、特にデータ活用の文脈では非常に日本国内でも注目を集めているところがございます。そして、その中に提案として初めて頭出しされたData Actという、2021年に提案される予定の大規模な法案パッケージがございます。

このData Actは、Business to Business、Business to Governmentのデータ共有全体に関する非常に興味深い方向を含むところですのでけれども、特に利用者情報の保護と広い意味で関わるところでは、オンラインウェアラブルデバイス等から生成されるmachine generated dataに関する個人の関与について以下のことが書かれていまして、これはちょっと拙訳ではあるのですが、個人ウェアラブルデバイス等から生成されるデータに関して、より能動的なコントロール能力を持つべきだと。そして、それが日本で言うところのPDSですとか、あるいは情報銀行と言ったようなところとも概念的に近いのだと思いますけれども、そのことというものを含めてGDPR20条に基づく個人のデータポータビリティの権利を強化することでよりサポートできるということです。今まさに並行してGDPRの見直しというのも様々な形で進められているところ、このことという

のは、やはり利用者情報の保護というのは、利用者側がサービスを自律的に選択できてこそ、移動の自由を持ってこそ初めて実際的に保護されるというところも部分的にはあるかと思しますので、少し視野に入れておいてもよいのかなと感じているところです。

特にスマート家電やウェアラブルデバイス等々、プラットフォーム事業者が取り扱うデータというのも、まさにこのオンラインの世界だけにはとどまらず、オフラインからのデータというところも併せて非常に重要になってまいりますところ、そういった取扱いというものを果たしてどう考えていくのか。

さらに、データ法の文脈ではデータ仲介者に関わる中立的なブローカーとしての役割を保障するという仕組みというものも視野に入れて、そういったパーソナルデータスペースのようなものの開発を促進していくことで、より消費者の能動的なデータ提供、活用の選択肢を可能にしていこうといったようなことも書かれているところでございます。

以上、非常に簡単でございましたが、継続的によく見ていく必要がある事項ということで御説明させていただきました。御清聴ありがとうございます。

【宍戸座長】 ありがとうございます。生員構成員の御発表にいろいろ御質問等もあるかと思えますけれども、後で一括してお受けしたいと思っております。

それでは、次にEU・eプライバシー規則案に関する議論の状況について、三菱総合研究所様より御説明をお願いいたします。

【西角氏】 三菱総研、西角でございます。

資料4を御覧ください。ePrivacy規則につきましては、2年前に本研究会第3回で御紹介しておりまして、今回はその2年分のアップデートについて御説明するという形になります。

めくっていただいて2ページ目でございます。このePrivacy規則は、現行のePrivacy指令を置き換えるという規則になってございまして、2ページ目の下半分、線を引いてあるところですが、GDPRの発効タイミングの2018年5月までに成立する予定でございましたが、そこで成立させることができずに、その後も協議が続けられてまいりました。しかしながら、昨年12月、EUの常駐代表委員会において修正案が否決されてしまいまして、審議が一旦停止しているという状況でございます。その後、改めて理事会において修正案が出されているんですけれども、現時点においてはまだ成立に至っていないという状況でございます。またコロナウイルスの影響等もあって、実質的には検討が止まっているというような状況になっております。

論点でございますけれども、最後のポツのところでございますように、電子通信メタデータ、それからクッキー等の技術により収集した情報をどうやって扱うか、その扱いの法的根拠だとか、あるいは犯罪防止等を目的とした場合にどのような例外が認められるか、こういった点がこの2年間の改修に関しては大きな論点になっているというような状況でございます。

3ページ目と4ページ目は年表というか、検討の経緯を時系列でまとめたものでございますけれども、2019年以降2年間の流れというのが4ページ目の後半の下のほう、少しハッチをかけてあるところにまとめてございます。基本的にはEU理事会において類似の規則改訂案が公開され、議論が継続しているというような状況でございます。

具体的な議論の中身ですけれども、6ページ目はePrivacy規則の目次というか条文構成でございますけれども、このページの中で赤の太字で書いてあるところが基本的にはこの2年間で修正されてきている項目でございます。

4 a の同意のところ、それから6条の電子通信データに関して許容される処理に関する規定、それから13条、14条、16条といった迷惑電話とかダイレクトマーケティングみたいな話、こういったところが主に修正されてきている内容であるということでございます。

めくっていただいて7ページ目ですけれども、こちらは前回、2年前に御説明した資料の時点で主な論点ということで4点挙げさせていただいて、ブラウザのゲートキーパー化とか、あるいは端末情報に関する同意以外の処理手段、それからM2M通信の扱い、トラッキングウォールの許容、こういった論点が当時ございまして、これにつきましては当時から変わっていないというか、基本的にはこの2年前の整理のとおりでございますけれども、1つだけ変化があるとすれば②のところです。ユーザー端末の情報利用時の同意以外の処理手段の是非というところで、この時点でも正当な利益 (legitimate interest) という考え方が提示されていたんですが、当時は反映されていなかったんですが、最新の2020年2月の修正においてこの考え方が復活してきているという状況がございます。これは次のページでまた御説明いたします。

8ページ目でございますけれども、この2年間の検討状況について一覧にしたのがこの1枚でございます。初めに、2019年5月の進捗レポートの段階で論点の整理が行われていて、これについては4点挙がっていますけれども、1つ目はePrivacy規則が新しいテクノロジーに与える影響ということで、これはM2M、IoT、それからAIの関係、こういったところに与える影響。

それから2点目としては、児童虐待、児童ポルノ画像について防止・発見・報告をどうするかといった問題。

それから3点目にデータ保持に関する問題、それから監査当局の権限、これらはEUの基本憲章との整合性についてどのように条文化するかといったような観点で議論を継続しますという論点整理が行われております。

これを踏まえて、2019年7月、9月、11月ということで2か月ごとにドラフトが出ております。7月のドラフトについては、挙げられた論点のうちで特に迷惑電話とか、あるいは求められていない通信、マーケティング通信といったものについてその範囲を明確化するような形での修正が行われたというのが内容でございます。

それから、次の9月のドラフトでは主に児童ポルノの問題について、これを検出・削除・報告する目的でどのような処理をしていいかということです。具体的にはポルノ画像等をハッシュを使って検出すると、これを認めるとしたときに、それをどのような形でePRの条文に反映させるかといった点が検討されたというところでございます。

それ以外にダイレクトマーケティングとかクッキーに関する規定の修正についても検討が行われましたが、修正自体は軽微なものにとどまったというのがこの9月のドラフトでございました。

それから、次の11月のドラフトです。こちらでは通信の秘密に関する条項ということで、これは電子通信のコンテンツあるいはメタデータの処理に関して、どのような例外要件に関してはその処理が許容されるのかといったことについて、その例外条件を列挙するような形で条文の修正が行われたというのが11月のドラフトでございました。同じく、児童ポルノは先ほど御紹介しましたけれども、同じような観点でテロ等の重大犯罪防止に関しても、これは通信の秘密の例外の事項として扱うべきだといったような意見もこのドラフトでは出されているという状況でございました。

冒頭に申し上げましたとおり、11月のドラフトの後、12月にEUの常駐代表委員会で修正案が否決されるという形になりまして、それを受けて2020年、今年の2月に改めて修正案が出たという形になっております。

この2月のドラフトにおいては、先ほど申し上げた電子通信メタデータ等の処理に関する、あるいはクッキー、あるいは類似技術の配置に関して行う法的な根拠の部分について、先ほど例外規定を列挙するというような形で申し上げましたが、それに代わる考え方として「正当な利益」という考え方が提案されたというのが2020年2月のドラフトになってお

ります。これは後ほど少し細かく説明いたします。

その後5月に進捗レポートが出ましたが、議論が止まって今に至るとというのが現在の状況でございます。

2020年2月のドラフトの中身につきましては、16ページまで飛んでください。16ページに2020年3月の改訂版で導入された「正当な利益」の考え方について御紹介しています。この「legitimate interest」という概念自体はGDPRでも参照されているものでございまして、それをどういうところに導入するのかについて、それから、仮にこの「正当な利益」を根拠とする場合にどのような条件、それから保護措置が必要なのかという点、それから、この「正当な利益」を根拠として仮にクッキー等を用いることができるとするならば、それはどのような事例、状況なのかといったような例示も行われています。これは全文の修正案という形で具体例のようなものの提示も行われているというような形でございます。

これもまだ提案が行われただけで、加盟国の意見が一致しているというような状況にはございませんので、このまま行くかどうかというのはまだ不透明でございますけれども、ePRに関して、最新の検討の状況というのはこのような状況であるという御紹介でございました。

次に、17ページ以降は、先ほどちょっとお話がありましたように裁判所の裁定が幾つか出ているということで、2点紹介させていただきたいと思います。

17ページに挙げているのはクッキーの能動的な同意に関する裁定です。こちらは2019年10月に裁判所のほうでクッキーの利用保存に関して、能動的な同意を取得しなければいけないということで裁定が出ています。具体的には背景・経緯のところがございますように、あるオンラインの宝くじ会社が、ユーザーがサードパーティーの広告を受信するということに関する同意、それからクッキーに関する同意、この2つをチェックボックスという形で同時に提示したんですけれども、2つ目のクッキーのほうには事前にチェックが入る形で提示が行われたという形で、これが有効かどうかということが争われたということです。裁定結果においては、クッキーを保存するために事前にチェックした同意ボックスは有効ではないということで、これは明示的な同意には当たりませんという判断が下されたという事例でございます。

それから次に、最後になりますけれども18ページです。こちらは英国の国内法との整合性をどう考えるかという観点で出た裁定でございますけれども、英国では安全保障・情報

機関が大量の通信データ、これは中身としてはトラフィックデータ、位置データですけれども、こういったものを取得しているという実態がございまして、これがePrivacy指令に合致するのかどうかということに関する争いが行われたという状況です。

具体的な論点ですが、先に19ページ目を御覧いただきまして、もともと英国では、英国の国内法において、中段にあります安全保障・情報機関が、電子通信サービスの提供者に対して国家安全保障の確保のための例外として通信の秘密を制限して個人データを送るよう指示して、これを受け取るというような法律になっているということでございます。この国内法が、左側にあるePrivacy指令、EUのルールに照らしたときに、適用対象外になるのか、それとも対象になるのかということがまず争われました。加えて、仮にこの適用範囲内であるとすれば、どのような規律がそこに求められるのかということが争われたということになります。こうした観点が、右側にあります欧州連合の基本条約の原理原則と照らして適正かどうかということが争われたということになります。

戻っていただいて18ページですけれども、結論としては18ページの一番下のC J E Uの決定というところでございますように、1つ目の論点、そもそも規制の範囲に含まれるかどうかということにつきましては、これは対象に含まれるという裁定が行われました。

2点目、含まれるとすればどのような要件、あるいはどの程度適用が行われるのかということに関しては、18ページの一番下の赤字のところですけれども、国家安全保障保護を保護する目的で、国家機関が、電子通信サービスの提供者に対し、トラフィックデータ及び位置データを安全情報機関に一般的かつ無差別に送信することを要求することを可能にする国内法令を排除すると、この一般的かつ無差別に送信するということが、これがある意味やり過ぎであるという判断が行われたということでございます。

最後に20ページ、具体的な判断のところを御紹介しますと、20ページの右下のところには太字で書いてありますけれども、国家安全保障の確保自体は重要な目的であるけれども、この比例制の原則ということ考えたときに、一般的かつ無差別にトラフィックデータや位置データを送信するということは、厳密に必要であり正当化されると考えられる限度を超えていると、やり過ぎであるという判断がなされたというのがこの裁定の内容でございます。

以上、e P Rの最新の状況と裁判所の判例2つについて御紹介いたしました。

【宍戸座長】 御報告ありがとうございました。

それでは、次に、日本総合研究所様からスマートフォンプライバシーアウトルックの取

組内容の紹介に基づき、御発表をお願いしたいと思います。資料5です。お願いいたします。

【小竹氏】 日本総合研究所の小竹でございます。スマートフォン上のアプリケーションの利用者情報の取扱い状況につきまして、定点調査を行っているものを取りまとめたスマートフォンプライバシーアウトルックの取組内容について、簡単に御紹介させていただきます。

資料の2ページを御覧ください。まずは、スマートフォンプライバシーアウトルックとは、というところなんですけれども、先ほど申しましたようにスマートフォンアプリにおける利用者情報の取扱いの現状等を毎年1回定点調査しておりまして、そちらの結果を取りまとめたものになっております。平成26年度に初回の調査結果が公表されまして、現在までにSPOVIまで公表されているというところで、今回全部の御紹介をしていくと時間が足りませんので、かいつまんだところを御紹介させていただければと思っております。

簡単に調査の背景というところを御紹介いたしますと、2012年8月に総務省様が公表いたしましたスマートフォン・プライバシー・イニシアティブ（SPI）で示された、スマートフォンにおける利用者情報の適切な取扱いに関するスマートフォン利用者情報取扱い指針の浸透状況ですとか、それに伴った各種団体や企業等の取組状況がどうなっているかというところを把握するための調査となっております。

調査内容がこのSPIで示された内容を踏まえたものになっておりますので、3ページを御覧いただきまして、既に御存じの構成員の方々も多いと思うんですけれども、簡単にSPIで示されたスマートフォン利用者情報取扱い指針につきまして御説明させていただきます。

基本的には下に示すように基本原則の6項目と、その中で具体的な取組としてアプリケーションごとにプライバシーポリシーを作成するというところと、そのプライバシーポリシーに記載すべき8項目ということが明確化されたということが大きなポイントだと思っております。SPO（スマートフォンプライバシーアウトルック）では、このプライバシーポリシーがきちんとアプリケーションごとに作成されているか、そしてそのプライバシーポリシーの中身がきちんとこの示された8項目の内容が書かれているかというようなところを調査する内容になっております。あとは、それに関連した取組がないかというところを調べたというところは、これまでのSPOの取組の内容になっております。本日はつきましてはそのアプリ調査、アプリケーションのプライバシーポリシーの掲載状況等の

調査の結果につきまして、概要を御説明いたします。

4 ページを御覧ください。4 ページがアプリ調査の簡単な概要になっております。これまでアプリ調査では、大きく3つのアプリを調査対象としてまいりました。1つ目が国内の人気アプリ、Android、iOS、Google Play、App Storeのトップ100アプリ、あとは国内新着アプリというところで直近1か月以内に出たようなアプリ、最後に海外との比較というところで英語圏の米国、英国のAndroid、iOSの人気アプリというところを調査対象として実施しております。

調査項目としましては、本当はもう少し多い項目をやっているんですが、主な項目としては3つになっております。1つ目がプライバシーポリシーの掲載有無というところで、Google Play、App Storeの中にプライバシーポリシーのリンクを掲載するところがあるんですけれども、そこか、もしくはアプリケーションの中にプライバシーポリシーがきちんと掲載されているかどうかというところ。

2つ目が、掲載されていた場合に、そのプライバシーポリシーの記載内容がどうなっているかというところ。こちらが大きく2つに分かれまして、1つ目がそもそもプライバシーポリシーの適用対象がどのように書かれているかと。S P Iですと、基本的にはアプリごとのプライバシーポリシーの作成というところが望ましいとしております。この理由としましては、1つの事業者が様々なアプリケーションを出してございまして、そのアプリケーションごとに取り扱う情報ですとか、その利用目的等が異なっておりますので、ユーザーのためを考えるとすればアプリごとにプライバシーポリシーをつくるのが望ましいというところで、そもそものプライバシーの適用対象がどうなっているかというところと、2点目として、そのプライバシーポリシー内にはS P Iで示されたような8項目がそれぞれ記載されているかというところと。

最後に、3点目としてプライバシーポリシーの簡略版の掲載があるかどうかと。プライバシーポリシーって非常に長くなってございまして、ものによっては3ページ、4ページにわたるようなもので、全部をしっかりと読むことは難しいというところで、重要な部分だけを抜粋した簡略版もつくるのが望ましいとS P Iではしてございまして、それがきちんと作成されているかというところが調査項目になっております。

5 ページを御覧いただきまして、こちらでまず調査結果の総括というところをさっと御説明させていただきまして、実際にグラフ等で詳細を御説明いたします。

まず、プライバシーポリシーの掲載有無というところに関しましては、直近では国内・

海外関係なく、人気アプリではプライバシーポリシーの掲載率はほぼ100%になっております。新着アプリでもプライバシーポリシーの掲載率は80%以上というところで、プライバシーポリシーの掲載ということに関しては浸透しているというように考えられます。

一方で、プライバシーポリシーの掲載内容というところになるんですけども、まずはプライバシーポリシーの適用対象というところだと、S P Iで望ましいとしたアプリごとのプライバシーポリシーを掲載している割合は10%程度で、会社全体ですとかサービス全体、例えばGoogleですと、Googleのサービス全体で同じプライバシーポリシーを提示する形になっておりますし、例えばLINEさんですとLINE GAMESですとかLINEのコミュニケーション、LINEのサービス分類ごとのプライバシーポリシーの提示という形を取っておりますし、そういう会社全体ですとか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今は主流というところになっております。

次に、S P Iで示された8項目の記載というところなんですけれども、こちらは国内・海外の人気アプリともにS P Iの8項目の中でも特に重要性が高い、誰がどういう情報を何のために取得して、さらにそれが外部ですとか第三者に提供されるのかどうかという非常に重要な部分に関しましては、国内・海外の人気アプリともに記載率はほぼ100%というところになっております。

というところを総括いたしますと、プライバシーポリシーの掲載率も高いですし、人気アプリであれば、会社全体やサービス全体というような掲載にはなっているんですけども、重要な項目に関しましてはきちんと書かれているような状況なのかなと思っております。

ただ、1点だけ浸透してないところとしましては最後のプライバシーポリシーの簡略版の掲載というところなんですけれども、こちらの簡略版の掲載に関してはほぼ浸透していないと。国内・海外新着アプリともにどの調査最初においても掲載率は数%というところで、簡略版、分かりやすいプライバシーポリシーの掲載というところはまだほぼ進んでいないというところになっておりますというところです。

以降、6ページからは、少し駆け足になりますけれども調査結果の詳細を御説明いたします。こちらのプライバシーポリシーの掲載状況、左側がAndroid、右側がiOSで、青色が国内の人気アプリ、オレンジ色が国外の新着アプリで、灰色が海外の人気アプリというところになっております。こちらを見ていただくとおり、2016年10月以降から一気に右肩上がりですとプライバシーポリシーの掲載率が上がっております。この内容としまして

は、Google、Appleが、Google Play、App Storeのガイドライン等でスマホアプリにおけるプライバシーポリシーの掲載を義務化ですとか規制強化をした影響という形になっております。

7ページを御覧いただきまして、こちらがGoogleの取組なんですけれども、Googleは2016年12月から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通知を送信して、さらにその1年後にもう少し強い義務化というようなことを警告して、たしかこの1、2か月後からプライバシーポリシーを提示していないようなアプリケーションはGoogle Playから削除されたりとか、申請を申し込んでもリジェクトされるような形になっているということになっております。同じような取組をAppleも実施しておりまして、8ページなんですけれども、Appleのほうも2018年8月、真ん中のところですが、基本的には全てのアプリケーションに対してプライバシーポリシーが必要というところを明示して、2018年10月からプライバシーポリシーがないものに関しましては審査でリジェクトする、もしくはApp Storeから削除するというような取組を実施しているというような形になっております。

次に、9ページを御覧ください。こちらはプライバシーポリシーの適用対象というところで、こちらは国内人気アプリで、左側がAndroid、右側がiOSというところなんですけれども、黄色のところは先ほど主流と言いました会社全体・サービス全体を対象としたプライバシーポリシーの割合になっております。青色が個々のアプリを対象としたプライバシーポリシーということになっておりまして、基本的には青色の部分は10%前後で推移している。この定点調査をしていますと、個々のアプリを提供する事業者さんというのは基本的には決まっております、基本はドコモさんですとかKDDIさんですとかのキャリアさんがSPIに従って個々のアプリを対象としたプライバシーポリシーをつくっているという状況で、それ以外の事業者さんにつきましては、基本的には会社全体・サービス全体を対象としたプライバシーポリシーを提示するという流れになっているというところなんです。

10ページ、11ページがそれぞれ新着アプリ、海外アプリなんですけれども、基本的には同じ傾向になっておりますので詳細は割愛させていただきます。

次に、12ページを御覧いただければと思っております。この状況を踏まえまして、プライバシーポリシーからは各アプリケーションがどういう情報を取得するのかというのは分からない状況なんですけれども、ただGoogle、Appleとともに、Android、iOSの機能として個々のアプリごとにどういう情報を取得するかとか、最近ですとアプリケーションの中

でカレンダー、カメラ、電話帳、位置情報、SMSですとかそういうプライバシー性の高い情報に関しましては個別で同意を取得するような形になっておりますので、プライバシーポリシー上ではどういう情報を取得するかというところは分からないんですけども、アプリケーションの中、OSの機能を活用すれば各アプリがどういう情報を取る可能性があるのかというところは分かるようになってきているということになっております。

12ページはGoogleの取組で、13ページがAppleの取組を簡単に紹介したものになっております。ここには載っていませんがiOS14、今年出されたところではさらにAppleさんは強化しております、位置情報ですと、位置情報を提供する・提供しないだけではなくて、正確な位置情報を提供するのか、曖昧な位置情報を提供するのかということも選べるようになっておりますし、写真に関しても、写真のライブラリー全体へのアクセスだけではなくて、一枚一枚の写真ごとにどのアプリに提供するかというところを選べるようになってきているということで、この辺りの機能は年々非常にプライバシー保護のほうに動いているのかなというところになっております。

14ページからがSPIで示された8項目の記載状況というところになっております。薄い青色がついているところがSPIの8項目の中でも特に重要性が高いと考えられる項目なんですけれども、国内の人気アプリに関しましては2014年から調査しているところもありまして、こちらを見ていただきますと、例えば上から2行目の取得される情報の項目に関しましては、2014年2月ですと8割ぐらい、iOSですと6割ぐらいしか書かれていなかったところが、直近の2018年12月の調査ですと9割超え、ほかの項目に関しましても基本的には重要と考えられる項目に関しましては100%に近づいているということで、プライバシーポリシーの質といいますか、書かれている内容というのは非常に充実してきているのかなと思っておりますというところです。

15ページの新着アプリに関しましても基本的には同じような傾向にはなっておりますが、ただやはり人気アプリと比べますと、全体的に8項目の記載率は若干低い形になっているのかなというところになっております。

次に16ページへ行きまして、こちらが海外人気アプリになっております。海外人気アプリのところも、基本的には青色がついた重要性が高いと思われる項目に関しては、国内と同じように記載率はほぼ100%になっております。ただ日本と大きな差がある部分といたしましては、印がついていなくて少し分かりにくいんですけども、下から4行目の⑥-2の利用者情報の送信先の記載の有無というところに関しましては、国内の人気アプリで

すと5割程度しか書かれていないところが、海外系ですと7割とか6割ぐらいと高いというところで、この辺りは多分GDPR対応というところで、第三者などに送信する際はしっかりと送信先を記載するというところが海外のほうが進んでいるのかなというところの差が出ているところだと思っております。

あとは17ページです。プライバシーポリシーの簡略版の掲載状況というところで、基本的にはどの調査対象においても数%程度でずっと推移していて、こちらが伸びる兆しはなかなか見えないなというところで、分かりやすいプライバシーポリシーというところはなかなか浸透していないというところになっております。

以上が今回の調査結果なんですけれども、18ページ以降は参考資料というところで、SPOのほかの調査項目も特徴的な部分を載せておりますので、お時間があるときにというところなんですけれども、少し興味深いところといたしまして最後のページ、24ページを御覧いただければと思うんですけれども、こちらは人気アプリにおけるカテゴリ別のアプリの構成比の推移を表しております。これは1年間の推移なんですけれども、2019年10月と2018年12月を比べたものなんですけど、全体的にゲームやエンターテインメント系のものが減って、ファイナンスとかほかのものが増えていると。こちらは、今データとしてはパッと出ないんですけれども、この調査を始めた2014年2月頃の調査ですとゲームが全体の人気アプリの5割ぐらいを占めている状況であったというところは覚えております。そういうところで言いますと、やはりスマートフォンの役割といいますか、昔は多分エンターテインメント中心で使われていたところが、ファイナンスですとかキャッシュレスのもので使ったりとかいろいろ用途が広がっていく、逆にそういうよりリアルに近い用途が広がれば広がるほど、スマートフォンが持つ情報も非常にプライバシー性の高いものが増えているのかなと思っております。

実際日本では実施されておりましたが、Appleですと米国、カナダ、英国で医療機関の医療情報を、自分の医療情報を全てAppleヘルスに統合できるようなサービスも出てきておりまして、そこを眺めると、自分が予防接種をいつ何回受けたとか、どういうアレルギーを持っているとか、どういう薬が処方されたかというようなものが全て統合されているようなサービスをAppleが進めておりますので、スマートフォンの中に蓄積される情報というのは、非常に個人のよりリアルな生活に関わっていくものになっていくのかなと感じているところでございます。

すみません、少し長くなりましたが、以上がSPOの紹介になります。

【宍戸座長】 興味深い御報告、ありがとうございました。

それでは、ただいまの生貝構成員、三菱総研様、日本総研様の御発表について、質問あるいはコメントがあれば承りたいと思います。ある方は私にお知らせいただければと思いますが、いかがでしょうか。まず、森構成員、お願いします。

【森構成員】 ありがとうございました。森です。いずれの御報告も大変興味深く拝聴いたしました。勉強になりました。ありがとうございました。

まず、生貝先生に2点教えていただきたいと思いますが、資料3の裏面と申しますか2ページ目のところなんですけれども、②の大規模オンラインプラットフォームの事前規制手段のところでも2ポツ、対消費者に関わる事項として、「個人データのポータビリティに関する特定の要求、またはインターオペラビリティの要求」とあるのですけれども、このポータビリティとは別にインターオペラビリティというのはどういうことなのかと思いましたので、教えていただければと思います。もしかしたら個人の指示に基づいて事業者間でやり取りをするときのやり取りのしやすさみたいなことなのかとも思ったんですけども、教えていただければと思います。

それからその下、3の四角の中なんですけれども、ここで3行目にお書きいただきましたこの個人データスペースということなんですけど、これは我々が言うところの、同じPDSでもパーソナルデータストアのような機能のものなのか、それともそれとは若干違うものなのかということをお教えいただければと思います。よろしくをお願いします。

すみません、三菱総研さんにも教えていただきたいことがありまして、1点だけなのですが、16ページのlegitimate interestでして、これは長年どうなるんだろうと思っていたことと同じかどうかなんですけれども、いわゆる広告事業者であって、SNSのようにユーザーとの接点を持たないもの、典型的にはDSPのようなものがそうだと思いますけれども、広告主に対してターゲティング広告の配信を請け負いますと、そのためにウェブサイトにはJavaScriptを置いてもらって閲覧履歴を収集すると、そういうビジネスをしているところが、かの地では、それによって集まった情報というのも直ちにパーソナルデータ、個人情報かと思しますので、その処理について正当化根拠が必要なわけなんですけれども、もしこれが同意が要るんだとしたら、その正当な利益で駄目だったんだとしたらば同意が要るということで、ユーザーとの接点がないからどうされるんだなというように思っていたわけですが、そここのところの問題がある種解決したといいますか、正当な利益を根拠にお仕事ができるようになったということ、そういう理解でよろしいのでしょうか。16ページでは

4つの項目に分かれていまして、「正当な利益」を根拠とできる事例の2ポツのほうが、エンドユーザーから同意を取らなくてもターゲティング広告を配信する、そのことが正当な利益であると書かれているのかなというように思っています、そう理解したんですけど、その理解でいいかどうかということを確認させていただければと思います。よろしく願いします。

【宍戸座長】 それでは、まず生貝構成員、お願いします。

【生貝構成員】 御質問ありがとうございました。

まず、私のほうの2ページ目の上から6行目にありますインターオペラビリティの要求というところに関しては、これもまだ具体的な姿というのが出てきておりませんので、いろいろな提案とかをされている段階という認識なのですけれども、ここに書かれていることは、ここでの記述は非常に簡単なんですけれども、全ての大規模プラットフォーム事業者にも適用されるというよりは、競争上の問題があるときに、ある種のレメディの解決的措置としてそれを求めることがあるといったような位置づけであるので、実際に実行される局面というのは限られていると認識しているのですが、このインターオペラビリティというのは、恐らく半分は、部分的にはデータのポータビリティを円滑にする上でのインターオペラビリティという部分もあるかと思うのですけれども、少なくとも視野としてはサービス自体のインターオペラビリティというところまで入れているようであります。例えばメッセージングございますとか、そういうところは相互接続を求めるようなことというのもあり得るのではないかということは、従前から競争政策のレポートで欧州では言及されていたところではあり、ただ、ここまで要求するのはかなり踏み込んだ措置かと認識しておりますので、どう出てくるか、楽しみではあります。

それから2番目に、ボックスの中の3つ目の個人データスペース、このことに関していろいろな議論がされているようではあるのですけれども、比較的いわゆる情報銀行と呼ばれるものに近いのかなと思います。それが欧州データ保護法上、果たしてどの程度の包括同意が可能なのかといったようなところも含めてかなりリサーチ等が行われているところであるようでありまして、また、さらに下のほうに新しいデータ仲介者のルールといったようなところもございますけれども、ある種、日本で言うところの認定といったようなことに近いような中立性の確保ということも視野に入れて考えているようであります。全て正しいかどうかは分からないんですけれども、私の認識としてはそのようなことです。

ありがとうございます。

【宋戸座長】 ありがとうございます。

森先生、今の生貝構成員の御回答でよろしいですか。

【森構成員】 ありがとうございます。結構です。

【宋戸座長】 次は、それでは三菱総研様、お願いいたします。

【安江氏】 三菱総研の安江です。私から回答します。

ご質問の記載についてはサービスの事例として挙がっているのですが、どういう事業者がどういうサービスを行っている場合にlegitimate interestに当たるのかという点について、もう少しちゃんと定義すべきだという意見が加盟国から出ていることもありまして、対象となる事業者・サービスや具体的な条件については、おそらくまだまだ議論が詰まっていなくて理解しています。

【宋戸座長】 ありがとうございます。

【森構成員】 ありがとうございます。

【宋戸座長】 それでは、ほかに今のお三方の御発表について御質問あるいは御意見はございますでしょうか。それでは、お願いいたします。

【宮内構成員】 宮内でございます。

これは日本総研の方に教えていただきたいんですけども、この中で簡略版の有無というのは結構まだこれから課題があるというようにお話しいただいたと思います。

私分からないだけかもしれないですけど、簡略版というのは何と何と何が書かれていれば簡略版ということになるのかというのを教えていただきたい。要するにこれが載っているかどうかの基準がどこにあるかということです。例えばアプリケーションをインストールするときには、これとこれとこれは取りますよとかそういうことは結構最初に出てきて、「はい」を押ししたりしているわけですけど、そういうものでは不十分ということだと思います。具体的にはどういうものをもって簡略版と言っているかを教えていただきたいと思います。お願いします。

【宋戸座長】 日本総研さん、お願いします。

【小竹氏】 それでは、17ページを御覧いただければと思っております。ドコモさんの例を出させていただいているんですけども、基本的には取得する情報とその利用目的と、あとはそれが第三者、取得者であるドコモさん以外に提供されるのかどうか、提供されるのは誰かというところが、基本的にはそのポイントが書かれているということが重要なかなと思っておりますというところです。

取得する情報だけですと、じゃあ、それって何のために提供して、それで提供した後にほかの人に行くかどうか分からないと判断しにくいというところもございますので、その辺りを簡潔に記載したところを簡略版として考えております。

【宮内構成員】 ありがとうございます。

そうしますと、完璧な簡略版じゃなくても程度問題みたいなことで、割と書いてあるけどどこまでは書いていないとか、そういうのもいろいろあると思います。どのようになっていけばいいのかなというのは、まだ私の頭の中で整理できていないんですけど、例えば第三者に提供するのがないだったら、ないって書かなくてもそんなに不都合はないかなという気もするんです。あるときだけばいいんじゃないかとか、どこまで出しているのかとか、その程度がどうというのも見ていかないと実態というのがよく分からないんじゃないかなと思っています。ここにゼロ%とか書いてあるんですけど、でも、ゼロ%といっても、この辺りまで書いてるのは20%あるんだよとか、そういうような状況というのはいかがでしょうか。

【小竹氏】 基本的にこういう簡略的に分かりやすいものがあるのはほぼないという状況です。皆さん、やはりもうプライバシーポリシーの全文の細かいものを載せているというような状況で、結構多分読み慣れた人が読まない、どういう情報がどういので取られて、どこに提供されているのかというところを読まない、パッと理解できないような状況なのかなというように正直思っております。細かい字になっていて、結局これは本当に同意の在り方の問題はあるんですけども、多くの消費者の方は何となくパッと細かい字を見て、まあ、いいかという形で同意しているというような状況なのかなと正直思っておりますというところです。

【宮内構成員】 分かりました。簡略版の定義に関わらず、割と出していないのがほとんどだよと、こういうことには変わりがないということですね。

【小竹氏】 そういうことです。

【宮内構成員】 ありがとうございます。

【宍戸座長】 ありがとうございました。

では、松村先生、お願いします。

【松村構成員】 今の点、私も疑問に思ったものですから。全く同じ17ページで、ドコモの簡略版のようなものはとてもありがたいと思って見えて、プライバシーポリシーに限らず、それ以外の約款でもこういう格好で重要なものの要点がまず示され、より詳しく

はこちらを見よ、とやってくれるとすごくありがたい。でも実際に大半のケースではこういう2画面になっていないわけですよね。これはどうしてでしょうか。日本総研に聞いても答えようがないかもしれないのですが、こういう簡略版で出してしまって、その簡略版の中で重要なことが書いていないと後から何か問題になるとか、訴訟になるとか、そういう法的な理由などでつくるのをためらっているのでしょうか。もし何か理由が思い当たれば教えていただきたい。

以上です。

【宋戸座長】 日本総研さん、お願いします。

【小竹氏】 こちらの理由といたしましては、つくる義務がないからというところなんだと正直考えております。簡略版をつくって詳細版をつくらせるとすると二度手間になるところで、ウェブページに掲載するのであればその両方を載せなきゃいけないですし、仮にプライバシーポリシーを改訂する場合は二重で改訂の手間がかかるというところで、その義務がないから、別に簡略版を載せなくても、まあ、App Store、Google Playからアプリを削除されたりですとか、審査をリジェクトされるというところがないからなのかなと正直思っております。

逆にApple、Googleが簡略版を必ず載せることとした瞬間、多分掲載率はもう100%に近くなるのかなというのが、特にスマホアプリにおいてはもうこの2社のプラットフォームの規制の状況に非常に影響を受けるというのが実情かなと思っております。

【宋戸座長】 よろしいでしょうか。ありがとうございます。

それでは、新保先生、それから崎村さんからそれぞれ御希望がありますので、まず、新保先生、お願いします。

【新保座長代理】 慶應義塾大学の新保です。よろしくお願いいいたします。私からは主にスマートフォン・プライバシーを中心に3つ意見を述べさせていただきたいと思っております。

まず、直接スマートフォンプライバシーアウトLOOK、SPO、今日も御紹介いただきましたけれども3つともプライバシーポリシーに関する意見です。1つ目は継続性についての意義は非常に大きいと思っております。この取組は2012年から行われています。なかなかネットの分野で、こういう分野で2000年、2010年代からずっと続いているという取組というのはなかなかないと思っております。このような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ると思っておりますので、この取組については、総務省の取組として引き続き継続していただければなと思っております。特に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調査結果からも非常によく分かりやすい結果として出ておりますので、当初は2012年に始まって、その翌年から調査が始まっていますので、2014年以降の調査としてかなり大幅に掲載率が上がっているという、この継続性の意義を今後も続けていただきたいという要望が1点目。

2点目は、先ほど御質問がありましたけどもプライバシーポリシーを分かりやすく短く見せるということについての課題は、なかなかこれは難しいところがありまして、2つ目の意見としては、プライバシーポリシーをめぐる非常に大きな課題としては長文化が進んでいると、非常に長文で分かりづらい。これは今に始まったことではなくて、例えば2015年にアムステルダムで開催されたI C D P P Cというプライバシー・コミッショナー会議では、オランダのコミッショナーが挨拶で、背景に長文のプライバシーポリシーを延々とスクロールして、皮肉交じりに話が終わるまでずっとプライバシーポリシーがスクロールし続けられていたと、それほど長文化が進んでいるということが一つ理由としてあるかと思えます。

ポリシーとステートメントの違いが日本国内ではあまり区別されていませんので、長文のそういったポリシーというのは、これは文字どおりのポリシーです。一方で、日本の場合は短くてもポリシーと呼んでいるので、短いのはステートメントと考えられますけれども、特にセキュリティなどについてはステートメント、特にJ I SとかI S M Sなどについてはステートメントをどうするかということが従来から明確になっているわけですが、ここでポリシーの分かりやすさと、もう一つ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と。特にユーザーインターフェースですけれども、S F Cの研究所ではリーガルデザイン・ラボというラボでリーガル・コミュニケーション、リーガルテックだけでなくリーガル・コミュニケーションというものも研究を行っておりまして、法、それから法文書といったものを分かりやすく伝えるためのツールボックスとかユーザーインターフェースとかユーザーエクスペリエンスといったようなインタラクションデザイン、これを、今後は見やすさをどうするかということを考える段階に来ているのではないかとというのが2つ目。

最後に3つ目ですけれども、プライバシーポリシーの公表意義というのが社会的、制度的に大きく変化していると思えます。その変化も2点ですが、これは御関心のある方は今後見ていただくと、格付における要素の1つになっております。とりわけアカウンタビリティを果たす上での公表事項の要素となりつつありますので、投資判断における指標とし

でも用いられつつあると。さらに、このプライバシーポリシーをスコアリングするというサイトも最近は出てきております。ですから、個人情報の保護、プライバシー保護というのは企業のアカウントビリティを果たす上での責任としても定着しつつあると、それが直接格付にもつながっていると。

2点目は、法定公表事項としての公表意義について、今般、2020年の改正個人情報保護法におきましても、法定公表事項について、保有個人データに係る事項の公表の改正が行われたところでありますけれども、この法定公表事項としての公表について、従来から民間部門における取組として取組がなされてきたところが、今後は積極的にそういったところも含めて検討を行うということが必要ではないかと思っております。

以上、3つ大きく意見を述べさせていただきました。

今、気がついたんですけども、カメラオンにしなくてよろしかったんですね。一応今気がついて、カメラをオンにせずに、安定的に音声をお伝えするためにカメラはオフでお伝えいたしました。

以上であります。

【宍戸座長】 ありがとうございます。非常に分かりやすく聞こえました。また貴重な御指摘、ありがとうございます。

それでは、崎村構成員からは御発言内容を一応書き込んでいただいておりますが、音声がつながっているようであればお願いします。

【崎村構成員】 崎村でございます。お世話さまです。聞こえますでしょうか。

【宍戸座長】 よく聞こえます。

【崎村構成員】 画像オンにする駄目かもしれないので、同じくこのままでいきます。

まず、簡略版を載せない理由としてなんですけども、実は、私が知っている事例では、現場は簡略版を載せたかったんですが、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という事例がありましたので御参考までに、これは海外の事業者ですけども共有しておきます。

2番目、分かりやすいポリシーというか、ポリシーなのか、プライバシー通知、プライバシーノーティスとしては、今年の6月に発効されたISO/IEC 29184で実際に求めています。これは今月中に日本語版も出る予定になっています。こちらではレイヤードアプローチです。ドコモさんの事例がまさにそうになっていると思うんですが、簡単なものを出して、詳細はこっちで見てくださいというやつで、これを推奨しています。欧州当局、

European Data Protection Boardとかプラットフォーム事業者も検討には参加しておりますので、こういうものが出ることによって今後変化が出てくることを期待しています。具体的にはプラットフォーム事業者等のあるアプリケーション事業者の現場が法務部に對して交渉する武器になってくれればいいなというように思っていたりします。

3点目です。これは質問なんですけれども、アプリケーションのアクセス権限である程度カバーできるというようなお話があったと思うんですが、これだと利用目的がよく分からないような気がするんです。利用目的の部分はどうのようにカバーされているのかというようなことで、もし情報がありましたら御教示いただければ幸いです。

以上でございます。

【宍戸座長】 ありがとうございます。

それでは、最後の点について日本総研様、いかがでしょうか。

【小竹氏】 13ページを御覧いただければと思っております。iOSに関しましては、このiOS10から、このアプリ内で許可を取る際に「写真へのアクセスを求めています」、この下に何のために取るのかというところ、取得の理由ですが、利用目的は記載しないといけないというように義務化されておりますので、Appleの場合はしっかりと読み込めば、同意のたびにこの小さい文字を読み込めばある程度何のために取るのかというのは分かる形になっております。ただ、逆にGoogleの場合はそういう仕組みはありませんので、Googleの場合ですと、どうしても推測するしかないというような状況なのかなと思っております。なので、iOSではある程度対応可能かなというところでは。

【宍戸座長】 崎村さん、よろしいですか。

【崎村構成員】 ありがとうございます。結構です。

【宍戸座長】 ありがとうございます。

それと、今、山口先生からチャットでコメントと提案をお送りいただけるということですが、それでよろしいですか。御発言されますか、山口先生。難しいようであれば、コメントをチャットのほうで承ります。

それでは、ほかにここまでのところ、御報告3つについて御質問それからコメント等がございますでしょうか。では、手塚先生、お願いします。

【手塚構成員】 今のスマートフォンプライバシーアウトLOOKの御紹介をいただいた日本総研さんにちょっとお聞きしたいんですけども、こういうものは各アプリケーションベンダーと申しますか、ここで言うとiOSをしているAppleですとか、Googleですとか、そ

ういうところが自前で考えて今進めているというところだと思うんですが、これに対して公的なところ、NPOでもいいんですが、そういうようなところでこういうものに対しての指針ですとかガイドラインとかそういうものを出しているようなところはあるのかという点ではいかがですか。

【宋戸座長】 日本総研さん、お願いいたします。

【小竹氏】 日本国内の事例ですと、例えばモバイル・コンテンツ・フォーラム様がSPIの内容を受けて、スマートフォンのアプリケーションを出すときには、SPIの内容を示すためにはこういうプライバシーポリシーを出したほうがいいというようなプライバシーのひな形みたいなものをおつくりして会員の方に広めていたりですとか、一部の情報収集モジュール、スマートフォンアプリに広告を出すためのモジュールを提供している事業者さんの中にはSPIの内容を踏まえて、仮にアプリの中に広告を出す際にはこういうプライバシーポリシーを書いて、しっかりうちのモジュールを使っているというところと、うちのモジュールのプライバシーポリシーのリンクは載せてくださいというように働きかけている事業者さん等もおりますので、すみません、全体を把握しているわけではないんですけども、GoogleやApple以外の団体様でも動かれているところはあるのかなと思っておりますというところです。

【宋戸座長】 先に手塚先生。

【手塚構成員】 大丈夫です。

【宋戸座長】 大丈夫ですか。

では、寺田構成員、お願いします。

【寺田構成員】 今回の日本総研さんの件に関してちょっと補足させていただきます。

モバイル・コンテンツ・フォーラムの常務理事をやっておりますので、それとガイドラインは私が書いていますので、これに関してはかなり広めさせていただいているのと、あと、地方公共団体のアプリケーションでもこちらのほうを利用させていただいているとか、そういった活動はさせていただいています。

もう一つのお話がありましたけど、2、3年前までは私、広告代理店でしたので、こちらのほうでもこういったガイドラインをつくって、いわゆる会員会社に対してはそれを守るということのをかなり厳し目に進めている業界だと思っています。

補足です。以上になります。

【宋戸座長】 ありがとうございます。

ほかに御報告について御質問、御意見あれば。では、生貝構成員、お願いします。

【生貝構成員】 ありがとうございます。

先ほどからお話に出ていたこのプライバシーポリシーの要約というところに関してなんですけれども、特にヨーロッパとの兼ね合いで言いますと、先ほど最初に少し御説明させていただいたC N I LのGoogleに対する制裁の中でも透明性のある情報提供という中で、まさに崎村先生がおっしゃるところのレイヤードアプローチによるプライバシーポリシーのような仕組みをしっかりと作っていかねなければならないといったようなところも、たしかアグリーメントの中に含まれていたという記憶です。ほかにもGDPR文脈ですと、2018年4月に出されたコンセントではなくてトランスペアレンシーのガイドラインの中で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というのがかなり詳細に記述されていたりして、やり方としては参考になると思いますし、恐らく諸外国の中ですとGoogleさんを含めて実際に対応しているところも多いかと思しますので、これはいろいろと国際的なベストプラクティスを見てみるといいのではないかなと思います。我が国ですと、同意のほうで片づけるかというのはちょっと比較法的に難しいんですけど、例えば我が国の同意は個人情報保護法ですとすごくあっさりした書き方をされていて、逆に通信の秘密ですと非常に重たくてといったときに、まさにGDPRで言うところの、あそこまで堅くはしなくても、透明性やインフォームドコンセントといったようなものを、法令レベルではないにしても、例えば電気通信ガイドライン等でこういうものだというように書いていくことである種の共同規制的な、こういったもののインセンティブということもつくることが考え得るのかなというようにお聞きしていて少し感じたところでした。

以上です。

【宍戸座長】 生貝構成委員、ありがとうございました。

では、寺田構成員。

【寺田構成員】 すみません、今の簡略版に関してもちょっと補足させていただきます。コンテンツ側の代表でもありますので。

端的に言ってしまうと義務化されていない、それから怒られることがないというのが最大の点ではあるんですが、もう一つありまして、これを書いて、ここだけを読んで「はい、オーケー」とやっちゃって、実はもっと細かいところは当然その先にあるんですが、そんなことは書いていなかったじゃないかという、そういったある意味危険性もある、リスクもあるということで、こういった部分で、法務とかそういった部分から余計なことをす

るとリスクが増えるという考え方というのが結構あるというのが現実問題です。

逆に言えばそういったところが担保される、そこだけでオーケーというわけではなくてあくまでも簡略版ですよと、本当に細かいことはちゃんと後ろにあるんですよということユーザーがちゃんと理解していただけるような構造になってくればこういったところというのもやりやすくなるんだと思いますが、現状でいくと、そこだけ見てしまって「はい、以上」と思ってしまう方々もいるという、そういったリスクマネジメントの関係からやらないというのも結構あります。

以上です。

【宋戸座長】 貴重なお話、ありがとうございました。

ほかに御報告について御質問等はございますでしょうか。

なければ、残された時間で、既に幾つかいただいているようにも思いますが、今日の議題1、議題2、全体を通じての自由討議の時間とさせていただきます。この研究会での今後の議論の在り方を含めまして自由に御意見をいただきたいと思いますが、いかがでございましょうか。では、寺田構成員。

【寺田構成員】 今まではどちらかというところ「ごめんなさい」に近いようなお話をしていたんですけども、今度は逆にそういったところを代表するような形も含めて考えていきたいなということを意見として出させていたきたいと思っております。

2つありまして、1つはいわゆる同意疲れ関係です。非常に分かりやすいインターフェースをつくらうとか、こういったことというのは、実は業界の中でもずっと考えて進めているところというのはあります。が、現実問題としてどんなに頑張ってもある一定以上は必ず書かないといけないものというのは存在すると。それがあということだけでそもそも読まない方とか、よくアンケートを取ると、「読みましたか？」と聞くと「読みました」とあるんですが、あれはかなり偏っていて、実は読んでない、ただ見ただけという、いわゆる読むということは理解するという部分も含まれるんですが、ただ「そういうのがあったよね」というだけみたいの方とか、こういった方に対してどうやって対応していくのかということは、実は正直言いまして、もう説明だけを一生懸命するとか、インターフェースで頑張るというだけではなくて、そもそもそういった説明を読まない、見ない、あるいはそもそも理解できない人というものも存在するんだという、そういった部分も含めた対策というのをそろそろ考えないといけないんじゃないかなと思っています。

これは、説明はなくていいということではなくて、それが分かる方には当然ちゃんとし

た説明が必要ですし、そうでない方々、あるいはここでは大人の方を考えていますが、子供であったりとか御高齢の方であったりとかそういった方のことも考えて、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そろそろ考えないといけないんじゃないのかなというのが一つ意見です。

もう一つの意見としましては、端末の中のデータであったりというのを個別に分類して、これは使っていいよ、これは使っては駄目だよ、これは個人情報だよ、これは該当しないよというような細かい分類ではなくて、もう少し全体でそういった情報というのは必ず何らかの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んじゃないかなと思っています。特に、最近また古くて新しい問題でフィンガープリントとか、それから、さすがにこれは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とディープパケットインスペクションのようなこととか、こういったことが起こり始めていると聞いていますので、個別、個別のデータがどうのこうのという分類ではない、もう少し大きな枠組みで、やっていいこと、いけないこととか、そういった概念のほうからももう少し考え直していく必要があるんじゃないかなというように思いました。

以上、2つ意見です。

【宍戸座長】 ありがとうございます。

ほかに御意見等はいかがでしょうか。宮内先生、お願いします。

【宮内構成員】 今の御意見ともかなり関係あるんですけども、見てもプライバシーポリシーが理解できない人とか、そもそも読まない人はたくさんいると思うんですが、全部読めと言われても多分無理だとは思うんです。そこで、これは無理なことを今から言うかもしれないんですけども、普通というのが何かあって、普通と違うところというのを見せるような形だったら、非常にシンプルに見られるんじゃないかというように思うわけです。ただ難しいかなと思っているのは、普通というのが全てのアプリケーションに普通と言ってしまうと、それはすごく設定しにくいですし、アプリケーションごとに全部違ってくると思います。アプリケーション種別みたいなことを考えて、その普通というのを、スタンダードをつくって、そことの差分を一番最初に表示するような、そういう方法を考えていくと少し効果的かなというように考えました。

以上です。

【宍戸座長】 ありがとうございます。

ほかにいかがでしょうか。

では、山口先生から、資料1・資料2に関し、今後の全体的な方向性や検討課題等について、コメントでいただいていることを、私から御紹介しておきたいと思います。

山口先生からは、いわゆる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機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。

より具体的な提案として、これまでこの研究会で繰り返し重要性が指摘されてきた、「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、例えばということで以下の3つを挙げておられます。

第1は、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について、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こと、つまりユーザーライツの観点。

2番目に、AI実装も進んでいる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していくこと—algorithmic verifiability—と書いていただいています。

それから3番目に、事後にとどまらず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—、つまりプロアクティブフェアネス。これら3点なども検討に値するかと存じますというのが山口先生からのコメントでございました。

それでは、次に、大谷構成員からお願いいたします。

【大谷構成員】 大谷でございます。ありがとうございます。

これまでの御説明などを聞いた雑駁な感想と、そして意見を申し上げます。宮内構成員がおっしゃっていたことに極めて近いこととなりますけれども、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一定のカテゴリーを、例えばレッドであるとかグリーンであるとか、何らかのカテゴリ化ができないものかなというのを常々考えております。特にアプリの提

供元だけではなく、第三者に提供がなされるものですか、あるいはかなり微細な機微情報、あるいは健康などについての情報が提供されるものであるとか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であるとか、あるいは簡略化されたステートメントというもの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だろうかというのは、宮内構成員がおっしゃっていたように大分無理めのことかもしれないですけども、そのようなことが必要なのではないかなと感じている次第です。

特にそのように思いましたのは、このコロナ禍で接触確認アプリなど、様々な似たようなツールの導入に当たりまして、それがプライバシーに与える影響が大きいのではないかと、部分的には誤解に基づいて導入に慎重になられる個人であったり、あるいは自治体といった組織などがあたりということもありましたので、正確にそのアプリケーションが利用する個人データ、あるいは個人データと言えるかどうか分からない境界領域にあるような情報の取扱いについて、分かりやすく理解が進むような仕組みを導入していくことが必要ではないかと思ったからでございます。

これらの課題については、アプリケーションの提供者だけではなく、それぞれのステークホルダーがそれぞれの立場で一定の役割を果たしていかなければいけないと思っておりますし、先ほども御説明のあったプラットフォームでAndroid、iOSでそれぞれにプライバシーポリシーの提供というのを義務づけるような自主的な取組がなされたことによってプライバシーポリシーの掲載率が向上しているということもありますから、プラットフォームに対して期待するところもでございます。また、アプリの提供者それ自身にも求めるべきところがあるかと思えます。

他方、利用者自身もどのようにそういった情報を活用していることが自分自身の身を守ることになるのかといった理解を進めるためにも、このプラットフォームサービスに関する研究会というのはいつも総合的な視点での政策パッケージを用意しているところですけども、このテーマについてもそれぞれの関係者、ステークホルダー、利害関係者に望まれる事項というのをうまく整理していくことによって、政策上の目的に少しでも利益にかなったような形に進んでいければと思っております。

以上でございます。

【宍戸座長】 大谷構成員、ありがとうございました。

ほかにもございますでしょうか。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。

資料2の今後の検討課題の8ページについて申し上げます。これは本当に短いながらも行き届いたことを書いていただいている、もう付け加えることはないと思って拝見しておりましたけれども、念のためちょっと細かいことを補足させていただきます。

まず、4ポツのところですけれども、今後のAIの活用やIoT化の進展に伴って、データ流通環境等が大きく変化することが想定されるというところで、電気通信事業における個人情報ガイドラインと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・イニシアティブの見直しを検討していかなければいけないわけですが、併せて、分かりやすいところでは昨年ですか、競争ルール等の包括的検証の報告書が出ましたけども、そこでしばしば言及されたのが電気通信事業法の役割の変化ということがあったかと思えます。電気通信設備というものを基本概念として、電気通信役務であるとか、電気通信事業者であるとか、そういうものを決めていっているわけですけれども、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このところから、こういった各論を検討しなければいけないのではないかと思います。

そのこととの関係で、3ポツのようなまさにクッキー等による情報の収集をどうするか、収集された情報をどうするかということですが、個人情報保護法の令和2年改正においては個人関連情報ということで、収集された情報が個人情報になったところで規制する、なるんだったら同意を取らなきゃいけないよという規制が新設されましたけれども、これは誠に適切な法改正であったかと思えますが、これは権利利益の保護の必要性が、個人情報になる時点でポンと発生するからそこで規制されているというよりは、やはり個人情報保護法の守備範囲が個人情報だからということによって、そこが規制の分かれ道になっているわけですし、実のところ、その手前の段階で収集された情報については権利利益の侵害のおそれ自体はあると。様々なIDをくっつけてデータベースとして存在しているわけですから、例えばそれが個人情報にくっつくだろうというような意図の下に提供する場面だけではなくて、漏えいした場合であっても、これはどこかで個人情報になるかもしれませんし、個人情報にならなくても、その人に対して広告をはじめとて様々なものをリーチすることができるデータであるということですので、そのところを個人情報になる前、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、これが通信の秘

密のみなのか、それとももう少し通信関係プライバシーみたいなものを考えて保護しなければいけないのかというところ、日本の場合はGDPR等に比べると個人情報の範囲が狭いということがありますのでそういう問題が生じているわけですが、そのところを実はこれからの検討で、狭いために穴になっているところを考えていかなければいけないのではないかと思います。

以上です。

【宍戸座長】 ありがとうございました。

まだ御意見はあるかもしれませんが、予定の時間となっておりますのでここまでとさせていただきます。

崎村構成委員からはチャットで、ISO/IEC29184の議論の中で、いわば同意の限界、ほかの適法な根拠を使ったほうがいいのではないかと、ただ同意によらなければならないものは例外的なものとして個人に注意喚起したほうがいいのではないかと。ただしnotice、通知のほうは、これは同意かどうかという処理の根拠に関わらず、常にnoticeがあるべきだと、第三者にも示されるべきだということについて補足をいただきました。

このアジェンダについての議論はここまでとさせていただきます。その他事項でございますけれども、改正電気通信事業法の施行に向けた準備について、先ほどまでの同意の議論にも関わるとは思いますが、事務局より御報告があるとのことですので、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6について御説明させていただきます。改正電気通信事業法の施行に向けた準備といたしまして、1ページ目をおめくりください。こちらは令和2年の改正電気通信事業法の概要でございます。電気通信サービスに係る利用者利益等を確保するため、外国法人などが電気通信事業を営む場合の規定の整備を行うということで、今年5月20日に公布されておまして、1年を超えない範囲内で施行される予定となっております。

こちらに関連いたしまして最終報告書に記載されている事項でございますけれども、2ページ目のところを御覧いただければと思うんですが、1の①のところでございますが、「通信の秘密」の保護をはじめとする電気通信事業法の規律が国外事業者に対しても及ぶように所要の措置を講じるということで法改正されたわけでございます。そういたしますと、②のところがございますように、行政処分（業務改善命令）についても通信の秘密の確保に支障があると認めるときには発動し得るということになります。③のところござ

いますが、このような業務改善命令の発動に係る基準、執行の指針について策定するということが望ましいのではないかとということで、矢印の1つ目のところにございますように、業務改善命令の発動の透明性・予見可能性を高めるため、業務改善命令の発動に関する一定の基準や事例を法執行に係る指針として策定・公表することが書かれております。

それで、詳細は省略しますが、次の矢印のところはどういった場合に業務改善命令を発動するケースとしてあるのかと、例えばということで既にご書いていただいております。

それから、3ページ目のところでございますけれども、⑥にありますように電気通信事業者と行政当局との間で対話を継続していくということでございます。

それから、4ページ目のところでございます、いわゆる「同意疲れ」への対応ということで、こちらについて有効な同意の取得や、その際の説明の在り方について検討を深めるということでございます。

それで、通信の秘密の関係でございますけれども、5ページ目のところは御案内のところでございまして、6ページ目のところに通信の秘密の侵害に当たらない場合ということで、有効な同意がある場合、それから違法性阻却事由がある場合と、こちらは今までの資料でございます、御参考でございます。

それで、このような状況を踏まえまして、10ページ目のところを御覧ください。先ほど御説明しましたように通信の秘密、知得、窃用、漏えいの場合に該当し得るとということでございまして、有効な同意がない場合、または違法性阻却事由がない場合に罰則の適用対象になり得るとということでございしますが、このようなときにいきなりということではなくて、まず業務改善命令がかけられ得ると、そのときにこれに関する執行指針を策定していくということでございます。また、利用者の有効な同意につきましては、現在もガイドラインのほうで記述がございしますが、個別具体的かつ明確な同意、また約款に基づく包括同意・オプトアウトなどにつきまして、同意の取得の在り方に関する参照文書を作っていくというような考え方でございます。

11ページ目のところが執行指針についての案でございます。こちらは概要でございますけれども、事業法の第29条第1項第1号の趣旨について示した上で、通信の秘密の確保に支障があるとして想定されるケースということで、3の(5)のところでございます、例えば①通信の秘密に係る情報の取扱いを示したポリシー・方針が不適切な例であるとか、②通信の秘密の取得・利用が不適切な例、また③情報管理態勢が不適切な例、④苦情・相談等対応態勢が不適切な例などについて示していくということを考えて準備を進めてまい

ります。

また、12ページでございますけれども、同意取得の在り方でございますが、こちら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の解説の参照文書として公表することを検討しているところでございます。通信の秘密における「同意」取得の意味、それからリスク分析の重要性、それから「有効な同意」・「同意取得の在り方」について説明した上で、4のところでございますが個別ケースの検討ということで、例えばユーザーアカウントを作成するときの一括同意、また2階層、これは先ほどもお話が出ておりましたところにも関連するかもしれませんが、概略を示した上で詳細も示せるような2階層にした上での同意取得、また既存サービスに付加的なサービスを追加する場合の同意取得の在り方、またその後の同意の管理ということで、その後のオプトアウトやダッシュボードなどについて、一定の個別ケースについてお示しできればということで考えております。

御説明は以上でございます。

【宋戸座長】 ありがとうございます。

その他、事務局から連絡事項があればお願いいたします。

【丸山消費者行政第二課課長補佐】 事務局の丸山でございます。

次回会合につきましては別途御案内させていただきます。

事務局からは以上です。

【宋戸座長】 ありがとうございます。

これにて、本日予定された議事は全て終了となります。

以上でプラットフォームサービスに関する研究会第21回会合を終了とさせていただきます。本日は皆様お忙しい中を御出席いただき、またオンラインで参加いただき、どうもありがとうございました。