

## 利用者情報に関するワーキンググループ（第7回）

令和6年6月28日

【山本主査】 それでは、定刻をやや過ぎておりますけれども、利用者情報に関するワーキンググループ第7回会合を開催いたします。

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

【川野利用環境課課長補佐】 事務局でございます。総務省総合通信基盤局利用環境課の川野でございます。

まず、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いたします。

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

次に、構成員におかれましては、ハウリングや雑音混入防止のため、発言時以外はマイクをミュートにして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、主査から発言者を指名いただく方式で進めさせていただきます。発言する際にはマイクをオンにして、映像もオンにして御発言ください。発言が終わりましたら、いずれもオフに戻してください。接続に不具合がある場合は、速やかに再接続を試していただくようお願いいたします。その他、チャット機能で随時、事務局や主査宛てに連絡をいただければ、対応させていただきます。

本日の資料は、本体資料として資料7-1から7-5、参考資料7-1から7-3を用意しております。

注意事項は以上になります。

なお、本日、江藤構成員は10時45分頃までの御参加とお伺いしております。

それでは、これ以降の議事進行は山本主査にお願いしたいと存じます。山本主査、よろしくお願ひいたします。

【山本主査】 本日は、スマートフォン上のプライバシー対策に関し、御議論をお願いしたいと思っております。具体的には、これまで様々な有識者の方に、民間事業者における関連の取組や諸外国の制度を御発表いただくとともに、Apple様、それからGoogle様から各社の取組を御紹介いただきました。その上で御議論も行っていただきました。こうした御議論を踏まえる形で、事務局で改定の案を御準備いただきましたので、これについて事務局から御発表いただき、その後、御議論いただければと思っております。

また、ワーキンググループの第1回において事務局から御説明がありましたとおり、改定に当たっては、セキュリティの側面での追加を行うべく、ICTサイバーセキュリティ政策分科会において議論が行われてきましたので、株式会社KDDI総合研究所様及び総務省サイバーセキュリティ統括官室から、その議論を御報告いただきたいと思っております。

なお、前回の会合と同様、本日の会合での議論に必要があると考えられるため、一般社団法人日本インタラクティブ広告協会様にオブザーバーとして御出席いただきたいと思っておりますが、御異議等ございますでしょうか。

(「異議なし」の声あり)

【山本主査】 特に御異議がないようですので、御承認をいただいたということで、御出席をいただいた上、議事に入りたいと思います。

なお、本日の質疑・意見交換につきましては、事務局、KDDI総研様及びサイバーセキュリティ統括官室の御発表を一括して行った後で、構成員の皆様から御意見等をいただきましたと思います。

それでは、事務局より御説明をお願いいたします。

【川野利用環境課課長補佐】 事務局でございます。それでは、資料7-1及び参考資料7-2に基づき説明させていただきたいと存じます。資料を投影いたしますので、少々お待ちください。

SPI論点整理(案)ということで、御説明させていただければと思います。まず、1ページを御覧ください。

利用者情報に関するワーキングにおける議論の状況についてまとめております。当該ワーキングにおいては、①スマートフォン上のプライバシー対策、②利用者情報に係るモニタリングといった論点がございましたが、今回議論させていただきます①スマートフォン上のプライバシー対策に係る議論としては、赤字としております、第1回、第2回、第3回、第5回と、有識者による御発表や事業者ヒアリングを実施してきたところでございま

す。

2ページを御覧ください。ワーキンググループ第1回でお示した、見直しに向けた論点案になります。項目としましては、1.位置付け、2.国内制度の反映、3.諸外国等の動向を踏まえた対応、4.民間の取組を踏まえた対応、5.その他の項目に沿って論点案をお示していたところでございます。

3ページから4ページは、これまでの議論の状況をまとめております。3ページでございますけれども、第1回では、SPIの見直しに関わる論点案や、国内制度・諸外国制度・民間での取組の紹介とともに、SP0の結果や、これを踏まえた論点について日本総研様から、あと生貝主査代理よりEUデータ関連法制の紹介及び論点の御提示をいただいております。

また第2回では、SPI策定時に御担当されておりました慶応義塾大学新保教授より、策定の背景及び見直しへの示唆、あとモバイルコンテンツフォーラム様から関連ガイドライン策定の取組の御紹介、マクロミル様から消費者調査・プライバシー保護手法に係る課題について御提示がございました。

第3回におきましては、欧米におけるダークパターン及びプロファイリングについて三菱総研様から、アプリストアの規約・審査方針の内容、規約の遵守状況の概要について日本総研様から御発表がございました。

第5回では、Apple様、Google様から御発表を頂戴したところでございます。

これらの第1回から第3回、第5回の発表資料や会合での議論を踏まえまして、第1回でお示した項目・論点ごとに分類いたしましたのが5ページでございます。これらの第1回から第3回の発表資料等の反映について、御説明させていただきます。

1.位置付けでございますが、議論を踏まえた論点として、法的拘束力のないベストプラクティスであることを踏まえ、法令から一步進んだレベルを目指すべきとの意見があるが、どう考えるかとの点でございますけれども、SPIへの反映方針案として、法的拘束力のないベストプラクティスとして、関係事業者等の望ましい対応を記載することとしてはどうか。一方、法的拘束力がない点は明記すべきではないかとさせていただいております。

国内制度の反映でございますが、こちらに関しましては、SPIの最終改正（平成29年）以降の国内制度整備の状況を反映させるべきではないかということで、令和2年の個人情報保護法関連の改正（個人関連情報及び仮名加工情報の追加、越境移転時の本人説明充実化、不適正利用の禁止の追記等）。また、令和4年の電気通信事業法の改正（特定利用者情報規律及び外部送信規律の導入）に関する追記が必要ではないかとさせていただいております。

3. 諸外国等の動向を踏まえた対応につきましては、諸外国や国際標準の動向を踏まえ、右側に各点、書かせていただいておりますけれども、ダークパターンとならないための対応、プロファイリングに係る予見性確保の取組、センシティブ情報への配慮、こどもの利用者情報の保護、利用者の属性に対応した適切な配慮等が必要ではないか。

4の民間の取組を踏まえた対応としまして、目的外利用を行わないことや必要最低限のデータ取得、取得情報や利用目的の分かりやすい概要の提示、同意の撤回方法のプライバシーへの記載、利用者行動の事業者横断的なトラッキングに係る対応、位置情報や写真データ等の適正な取扱い等が必要ではないかとさせていただきます。

5. その他としまして、他のデバイスについて追記等の御意見があったところですが、実態把握を行った上で改めて検討が必要ではないか、また、本日、後ほど御発表があるかと思っておりますけれども、セキュリティに関しても追記が必要ではないかといった点があったところでございます。

6 ページ以降は、有識者発表と構成員からの御意見に照らしまして、SPI改正への反映方針案を示しております。5 ページで御説明した改正への反映方針よりも若干詳細な部分もございまして、特に差分のある部分について御説明させていただきます。

8 ページでございます。ダークパターンに関する点とでございますけれども、こちらに関しましては、欧州データ保護会議におけるガイドライン等も参照の上、原則として欺瞞的な方法による利用者情報の取扱いが行われないう、望ましい対応を追記してはどうか。また、プロファイリングに関しましては、GDPRやDSA等も踏まえ、プロファイリングに係る予見性確保の取組、プロファイリングによるセンシティブ情報の予測・生成やこどもの利用者情報のプロファイリングに基づくターゲティング広告の表示を原則として実施しないことが望ましいこと等について追記してはどうかとさせていただきます。

9 ページでございます。センシティブ情報への配慮としましては、GDPR及びDSA並びに民間の取組を踏まえ、センシティブ情報への配慮及びこどもの利用者情報の保護を追記してはどうかとさせていただきます。

10 ページでございます。民間の取組を踏まえまして、これに対する対応として、GDPRや民間での取組を踏まえ、目的外利用を行わないことや必要最低限のデータ取得について追記してはどうか。

11 ページでございますけれども、GDPRや民間での取組を踏まえ、同意の撤回方法のプライバシーポリシーへの記載について追記してはどうか。

12ページでございますけれども、GDPR及びPrivacy指令並びに民間の取組を踏まえ、事業者横断的なトラッキングに係る対応、位置情報や写真データの適正な取扱いについて追記してはどうか。

13ページにおいて、民間の取組を踏まえ、取得情報や利用目的の概要を分かりやすく提示することとしてはどうかとさせていただいているところでございます。

これらの論点整理案を反映したものとして、参考資料7-2、スマートフォンプライバシーセキュリティイニシアティブ改定案（事務局）をお示しさせていただいております。投映資料を変更いたしますので、少々お待ちください。

こちらは、改定案をお示しさせていただいております。主な改正内容について幾つか御紹介させていただきたいと存じます。

まず、ダークパターンにならないための対応としましては、例えば7ページ、1.1.2. 定義でございますけれども、⑬番「ダークパターン」として、サービスの利用者を欺いたり操作したりするような方法又は利用者が情報を得た上で自由に決定を行う能力を実質的にゆがめたり損なったりする方法と記載しております。21ページの、1.2. アプリケーション提供者等における取組のところでございますけれども、1.2.1.1. プライバシーポリシーの作成の情報収集モジュール等に関する記載事項の⑥において「同意取得の方法及び利用者関与の方法」として、同意取得の方法がダークパターンとならないよう留意することが望ましい。28ページの（2）利用者関与の方法の、同意の撤回に関する事項にしまして、ダークパターンを回避するため、同意を取得する場合と同程度の操作により同意の撤回画面へアクセスできるようにすることが望ましいというような記載をさせていただいております。また、30ページ、2.1.2. プライバシーポリシー等の運用のところでございますけれども、（2）利用者関与の方法、1.2.1.6. ダークパターン回避の対応としまして、補足事項に、ダークパターンの具体的な事例として、例えば欧州データ保護会議が示すダークパターンの具体例を参考とすることが考えられるとしております。3点ほど、ここは事例を挙げさせていただいているところでございます。

次に、プロファイリングに関わる予見性確保の取組について御説明させていただきたいと存じます。

18ページでございます。1.2.1.1. プライバシーポリシーの作成、④利用目的の特定・明示に、本人に関する行動・関心等の情報を分析するいわゆるプロファイリングを行う場合には、どのような取扱いが行われているかを本人が予測・想定できる程度に利用目的を

特定するとともに、かかる分析処理を行うことを含めて利用目的を特定することが望ましいとしております。

また、25ページ、1.2.1.2. プライバシーポリシー等の運用、(1) 通知・公表または同意取得の方法につきまして、同意取得を要する利用者情報の取扱いとしまして、③こどもの利用者情報の部分に、こどもの利用者情報のプロファイリングに基づくターゲティング広告の表示は実施しないことが望ましいとさせていただいております。

また、こどもの利用者保護といたしましては、24ページ、③「こどもの利用者情報」として、こどもが利用する可能性があるサービスを企画・開発する際には、こどものプライバシーを高い水準で確保するための適切な措置を講ずることが望ましい。例えば、プライバシーポリシーを簡潔で目立つように、利用者の年齢に適した明確な表現で記載したりすることが考えられる。また、特に低年齢の子供に関する利用者情報の取扱いに当たっては、事前に法定代理人等から個別の情報に関する同意取得を行うことが望ましい。さらに、こどもの利用者情報のプロファイリングに基づくターゲティング広告の表示は実施しないことが望ましいというふうにしております。

また、センシティブ情報への配慮といたしましては、10ページ、1.1.4. 基本原則、⑧特定の情報及び利用者の属性に応じた配慮といたしまして、利用者本人に対する不当な差別、偏見その他の不利益が生じないように、特定の情報について適切な配慮を行うとともにこのこと記載させていただいております。

また、24ページ、1.2.1.2. プライバシーポリシー等の運用、(1) 通知・公表または同意取得の方法としまして、同意取得を要する利用者情報の取扱いのところでございますけれども、②「センシティブ情報」として、不当な差別や偏見その他の不利益が生じないように、その取扱いに特に配慮を要する情報を収集する場合には、取得する情報の項目を明示した上で、個別の情報に関する同意取得を行うことが望ましい。また、プロファイリングによりセンシティブな情報を予測・生成する行為は、センシティブ情報の取得につながるおそれも否定できないと考えられることから、原則として実施しないこととし、実施する場合には利用者本人に対して個別の同意取得を行うことが望ましいというふうにしております。

また、利用者属性に対応した適切な配慮につきましては、23ページ、1.2.1.2. プライバシーポリシー等の運用、(1) 通知・公表または同意取得の方法としていまして、プライバシーポリシーの策定に当たっては、利用者にとって分かりやすい方法として、注釈27

でございますけれども、利用者の属性（子ども、高齢者等）に配慮して適切な情報提供が行われることが望ましいとしております。

また、民間事業者の取組を踏まえた対応といたしまして、目的外利用を行わないことや、必要最小限のデータ取得に際しまして、18ページでございますけれども、アプリケーション提供者の具体的な取組内容として、1.2.1.1. プライバシーポリシーの作成の、②「アプリケーション提供者が取得する利用者情報の項目等」として、アプリケーション提供者は、アプリケーションの主要な機能に関する情報にのみアクセスする。アプリケーションの実行に必要な情報に限って収集及び使用するなど、利用者情報の取扱いは、その利用目的との関係において適切で関連性があり、かつ、必要最小限の範囲とすることが望ましいとさせていただきます。

また、取得情報や利用目的の分かりやすい概要の提示といたしましては、23ページ、1.2.1.2. プライバシーポリシー等の運用の2ポツ目でございますけれども、プライバシーポリシーの分かりやすい概要の作成や、利用者にとって分かりやすい方法で示されることが望ましいとし、その例としまして、注釈26でございますけれども、例えばプライバシーポリシーに記載する事項について、アプリケーションごとにその概要を作成し、アイコン等を用いてアプリストアの個別ページに掲示することが考えられることについて記載しております。

また、同意の撤回方法のプラポリへの記載につきましては、28ページ、(2) 利用者関与の方法につきまして、利用者が利用者情報の範囲・取得方法について同意した場合であっても、その同意の後に、簡単にアクセスができ、かつ分かりやすい方法で当該同意の撤回などができる機会を提供し、また、同意の撤回方法をプライバシーポリシーに記載することが望ましいとしております。

また、利用者行動の事業者横断的なトラッキングに関わる対応といたしまして、25ページでございますけれども、「同意取得を要する利用者情報の取扱い」、④でございますが、「利用者行動のトラッキング」として、利用者は、端末やアプリケーション、ウェブサイト等によって提供される広告IDやクッキー等の識別子に関連づけられることがあり、これらの識別子を他の情報と組み合わせることで個人識別性を獲得する可能性があると考えられること、また、個人識別性は獲得しないものの利用者に対するプロファイリングを可能とし、広告等を通じて当該利用者に影響を与える可能性があることから、プライバシー侵害を回避するため、事業者横断的なトラッキングを実施するために利用者情報を取得する

際には、個別の情報に関する同意取得を行うことが望ましいとしております。

また、位置情報や写真データ等の適正な取扱いに関しましては、26ページの⑥、GPSなどによる位置情報は、アプリケーションが提供するサービスの提供または機能に直接関連する場合のみ取得することが望ましい。また、アプリケーション提供者は、プライバシー侵害を回避する観点から、個別の情報に関する同意取得を行うとともに、取得する位置情報の粒度や取得する条件について利用者が設定可能とするなど、取扱いに留意することが望ましいとしております。

また、⑧「スマートフォンのアプリケーションの利用履歴やスマートフォンに保存された写真・動画」としてアプリケーションによるサービス提供のために必要な範囲で用いられる場合を除き、プライバシー侵害を回避する観点から、個別の情報に関する同意取得を行うことが望ましい。また、アクセス範囲の限定等の設定を可能にするなど、取扱いに留意することが望ましいとさせていただきます。

こちらまでが、アプリケーション提供事業者ということの取組ということで記載させていただいているのですけれども、これらに関しまして、今度はアプリストア運営者の取組ということで、1.3.1のところを追記させていただきます。

まず、P33「アプリストア運営事業者は」というところがございますけれども、アプリケーション提供者等において、先ほども御説明してまいりましたけれども、「1.2.アプリケーション提供者等における取組」でまず取り組むことが望ましいとされている事項が、実施されているかといったことを確認することが望ましいとさせていただきます。また、アプリストアへのアプリケーションの登録審査の際に、本指針を踏まえた基準等を作成して、それであらかじめ公表することが望ましいとさせていただいているところがございます。また、アプリストアの個別のアプリケーションページ上に、分かりやすさということでございますけれども、プライバシーポリシーや取得される情報の概要等の表示場所を提供すると。また、表示すべき事項や標準的なアイコンを示すなど、アプリケーション提供者等に対して、適切な対応を行えるように促す、支援をすることが望ましいとさせていただきます。

取組のところは非常に駆け足でございますが、事務局説明とさせていただきます。どうぞよろしくお願いいたします。

**【山本主査】** ありがとうございます。

続きまして、サイバーセキュリティ統括官室、宮野様、よろしくお願いいたします。

【宮野サイバーセキュリティ統括官室参事官補佐】 総務省サイバーセキュリティ統括官室の宮野と申します。よろしくお願いたします。

それでは私から、資料7-2に沿って御説明をさせていただきます。

まず、総務省サイバーセキュリティ統括官室におきましては、平成29年より、サイバーセキュリティタスクフォースという会議を開催してございまして、その下に本年2月より、総務省が中長期的に取り組むべきサイバーセキュリティ施策の方向性を検討する場として、ICTサイバーセキュリティ政策分科会といった会議を開催してございます。この分科会におきましては、様々な観点からサイバーセキュリティについて議論をいただいているところでございますけれども、その観点の一つとして、スマートフォンアプリにおけるセキュリティの確保についても御議論いただいたというところでございます。

水色の箇所でございますけれども、同分科会における議論の概要についても簡単に御紹介をさせていただきます。まず、一般社団法人日本スマートフォンセキュリティ協会様からは、スマホアプリにおけるサイバー脅威を議論する際には、セキュリティホール、いわゆるスマホアプリ脆弱性と、それからマルウェア、いわゆる不正アプリの両面から考える必要があるといったところ、アプリ流通経路の責任において一定のセキュリティ確保が可能であり、アプリ開発者、それからアプリストアの果たすべき役割が大きいといった御議論をいただいたところでございます。

また、OWASP様より、アプリのセキュリティやプライバシーを確保するためには、アプリ診断というプロセスに加えまして、アプリのセキュリティ要件、リスク分析等についてまとめたセキュア設計・開発ガイドのサポートが必要といった御議論をいただいたところでございます。

また、この後に御説明がございまして、KDDI株式会社様からは、スマートフォンプライバシーアウトルックXについて御発表いただいたほか、イギリスのDepartment for Science, Innovation & Technology、DSITと呼ばれる組織が公表しているCode of practiceを参考に、我が国のSPIにおいてもセキュリティの観点を盛り込むべきといった御提言をいただいたところでございます。この後、KDDI様から、SPO Xと提言の具体的内容についての御発表をいただきたいと思っております、その後に、それを踏まえた総務省としてのセキュリティ関係箇所に係るSPIの改定案をお示ししたいと思っております。それでは、KDDI様から願いたします。

【山本主査】 続きまして、KDDI総合研究所の本間様、願いたします。

【本間氏】 KDDIの本間です。

それでは、今、総務省、宮野様からお話のありましたとおり、弊社で調査しましたスマートフォンプライバシーアウトルックXについて御説明させていただきたいと思います。

今、以前にも御説明がありましたとおり、総務省様では平成24年8月に、スマートフォンプライバシーイニシアティブ、通称SPIを作成しまして、平成29年7月にはSPI IIIというものを作成しています。それに合わせて平成25年より、スマートフォンのアプリケーションによるプライバシーの策定状況を調査するというので、スマートフォンプライバシーアウトルック、通称SPOと言われると思うのですが、こちらを公表しまして、昨年3月にSPO IXを公表しています。今回、弊社で、SPO Xということで調査したものについて御紹介させていただきます。

調査対象に関しては、こちらにあるとおり、300アプリ、人気アプリ200、新着アプリ100、情報収集モジュールを20ということで、それぞれAndroid、iOSは半分ずつということで実施しております。

続いて調査項目になりますが、こちらにある8項目を調査しております。こちらの概要については、それぞれ今から説明させていただきます。

初めに1つ目です。プラポリの作成・掲載状況です。こちらに関しては、人気アプリ、新着アプリとも、プラポリの掲載率が100%近くになっています。これは、SPIが広く普及してきたということと、Google Play、App Storeがプライバシーポリシーの掲載を必須化してきたということがありまして、この相乗効果によって、100%近い結果になっていると感じております。また、人気アプリ、新着アプリとも、こちらもこれまでの活動を反映する形で、いわゆるプラポリの内容が、アプリを意識したものの記載内容が増えているというのは確認できています。

一方で、アプリの構造が複雑化したこともありまして、プラポリまでのリーチするステップ数は若干増加しているというのはあるのですが、これはアプリの変化ということで、ある意味、致し方ない部分ではあるかと思いますが、そういう傾向が見られております。

続いて、電気通信事業における個人情報保護ガイドラインで推奨されている10項目について調査を行っています。これまでSPOでは、SPIに従って8項目ということで調べていたのですが、今回は、令和5年6月に改正電気通信事業法が施行されていまして、ここで推奨する項目が10項目となっていましたので、この2項目も追加して10項目、調査しています。

こちらに関してですが、新着アプリ、人気アプリともに、利用者情報の送信先に関する記載というのは大きく増加しています。また、10項目全て記載しているアプリ、これは必ず10項目あるかどうかというのもあるのですが、人気アプリで40%、新着アプリで25%という結果になっております。

また、3番目として、利用者情報に取得する状況です。こちらはAndroidのみ実施しているのですが、プライバシー性の高い項目です。電話帳・電話番号・位置情報・メールアドレスを取得するアプリの割合は減少しているものの、プライバシー性の高い情報をプラポリに記載しているアプリの割合というのは大きく増加しています。これも、OS側としてこれを取るためには個別承諾を取らなくてはいけないというがあるので、こういう意味で上昇しているのだと思っています。

続いて、4番目のプラポリの概要版作成・公表状況です。こちらに関しては、まだ残念ながら概要版の掲載率というのは10%以下ではあるのですが、新着アプリに関しては、今回の調査では大きく上昇した結果になっています。

5番目として、プライバシーポリシーの改定状況です。こちらに関しては、改版履歴を記載しているアプリというのは徐々に増加している結果となっています。

6番目です。今回、アプリ開発者の国籍ということで、どこの国のアプリかということで、国内・国外を分けて比較しています。今回、国内アプリが3分の2、海外が3分の1ということで、海外アプリが非常に増えている傾向はあるのですが、国内・海外でもプラポリの記載している量というのは基本的には変わらないのですが、海外のアプリのほうが、プラポリに書く内容が、アプリを意識しているものが非常に高くなっているというふうになっています。

また、7番目として、アプリ通知における同意取得ということに関しては、アプリプラポリ、お客様、利用者が離脱しないように工夫するというのも重要になっていまして、そういった点で工夫しているアプリというのは非常に増加している傾向が出ています。

また、利用者の権利・利益保護を妨げるおそれの有無ということで、日本語以外のプラポリというものを書いているアプリというのはかなり低下しています。ただ一方で、マーケットとアプリプラポリ、アプリから呼べるプラポリ、Google Play、App Storeから参照できるプラポリと、アプリから直接見られるプラポリで差異があるものがありましたので、これはちょっと課題かと感じております。

今後の課題・取組ということで、こちらは書いてあるとおりですが、これまでの活動を

通じて、プラポリの記載内容というのは全体的には充実しているものとなっています。一方で、先ほども説明したとおり、国内アプリは海外アプリに比べて、アプリを意識したプラポリになっていないもの、いわゆる企業プラポリみたいなものを公開しているものもありますので、この辺に関しては、国内アプリ開発者に対して、スマートフォンプライバシーイニシアティブⅢの趣旨等を一層周知していくことが求められると思っています。また、アプリの構造が複雑化してきていて、プラポリが非常に見づらいついたものもありますので、それによって、利用者がアプリを使おうとしたとき、プラポリ確認だけで負荷をかけて離脱してしまうというのは双方にとってよろしくないというものもありますので、プラポリの概要版を作成する、プラポリの同意を分かりやすくするといった工夫を尽くしていく必要があると考えています。

ということで、SP0の報告は以上となります。もし問題がなければ、続いて不正機能の検証に関する実証についても報告させていただきたいと思いますが、問題ないでしょうか。

【山本主査】 お願いいたします。

【本間氏】 それでは、令和5年度「通信アプリに含まれる不正機能の検証に関する実証」についての報告をさせていただきます。

背景と目的ですが、こちらに書いてあるとおりののですが、スマホの普及率というのは今、個人保有77.3%（2022年時点）ということで、人々の生活に、スマートフォンはもうなくてはならないものになっています。一方で、スマートフォンを常に携帯することで、行動履歴や通信履歴といったものを多数、収集・蓄積することが可能になっています。そういった背景の中、アプリ事業者が、利用者の同意の範囲を超えた利用者情報の収集をしてしまうとか、アプリの脆弱性を悪用したサイバー攻撃による利用者情報の漏えいなどの懸念が生じるというものも考えられると思っています。

こういった背景の中、本事業では、国内解析事業者の解析能力水準を把握するとともに、実際にアプリから外部送信されている情報について解析を行っています。また最後に、サードパーティーアプリストアを含めたアプリ運営者が果たし得る役割ということで、SPIに盛り込むことが望ましいセキュリティの観点を示しております。

事業概要ですが、まずはGoogle Play、App Storeから入手するアプリを選定しています。こちらは、売上げやカテゴリー、人気アプリ／新着アプリ等を考慮して選定していきまして、300アプリを選定しています。こちらに対して、スクリーニング解析ということで簡易な脆弱性審査を行いまして、アプリの評価を行っています。また、先ほど説明しましたSP0に基

づいて、プライバシーポリシーがどうなっているかという確認を行います。その結果を踏まえて、特に注目して調査したほうがいいだろうというアプリを100アプリ、Android 50アプリ、iOS 50アプリを選定しています。この収集したアプリに対して、実際にアプリを操作して、どこに通信を行っているかなどの調査を行いまして、最終的に、ここから詳細に解析したほうがいいだろうと思うアプリを83アプリ選定しています。これが、Android 41アプリ、iOS 42アプリとなっています。このアプリに対して、静的解析・動的解析を行っております。

また、文献調査としては、利用者の意図しない利用者情報の取扱いの実態の文献調査や、あとは諸外国におけるスマートフォンアプリの規制に関わる文献調査を行っております。

まず、技術的解析結果です。詳細解析によって明らかになったということ、利用者情報の外部送信に関わる実態ということです。これは、Android 41アプリ、iOS 42アプリに関して調査を行っていますが、基本的に多くのアプリがいろんな情報を送信しています。ただ、これはここにも書いてあるとおり、Androidの方が解析がしやすいというので、Androidの方が広く調査はできているというのはあるのですが、このような結果になっています。おおむね、デバイス情報、アプリ情報、OS情報というのは、アプリへの利用に関して一般的に必要な情報なのですが、そのほかにも利用者情報などを多数測定・取得しているということが確認できております。

続いて、利用者の意図しない利用者情報の取扱いの文献調査を行った結果になります。利用者の意図しない利用者情報の取扱いに関するアプリの類型整理としては、ここにあるとおり、3つの分類を行っております。1つ目は、アプリ開発者の意図したとおりアプリが動作はしているのですが、プライバシーポリシーの記載が不十分で、利用者に十分告知がないケース。おそらく、これが一番多いケースだと思っています。2つ目が、アプリの脆弱性を通して悪用した攻撃ができるケース。アプリの開発者や利用者の意図しない利用者情報が取られるケースということで、これは多くは、アプリ開発者がセキュリティ対策が不十分ということで発生する問題となると思っています。最後が、利用者に誤認を与える方法で利用者にアプリをインストールさせるというもので、こちらはある意味、マルウェア的な要素になりますので、悪意を持ってやっつけてしまっているものなので、他のものとは異なると考えています。

国内外の事例としては、類型1ではどのようなものがあるかということで、透明性が不十分なアプリというものは、例としては、QRコードリーダーで位置情報を取っていたとい

うものが挙げられます。2つ目は、脆弱性があるアプリに関しては、メッセージアプリに脆弱性があり、スパイウェアを埋め込むことができるものです。類型3は、昨今、世の中で問題になっているフィッシング詐欺などが多いとは思いますが、ウイルス対策などを偽って不正なアプリをインストールさせるといったものがあるという観点です。

一方で、OS提供事業者に対する利用者保護の取組としては、OS提供事業者に関しては、社員向けのプライバシー教育や未成年保護、プライバシーセンターなどをやって、いろいろセキュリティ対策を行っています。また、アプリストア運営者、これはGoogle Play、App Storeですが、こちらはどちらもディベロッパーポリシーやガイドライン、使用許諾などを定めて、厳格に管理を行っているという実態があります。

まとめとしまして、利用者を保護するための第三者検証の必要性ということで、SPIでも示されているとおり、スマートフォンの第三者検証をすることで、当該アプリがプライバシーポリシーに適した運用がなされているかを客観的に確認することができ、利用者がスマートフォンアプリを利用する際の判断基準として有益な情報を提供することが期待できると考えています。また、第三者検証を通じることで、スマートフォンアプリに対する信頼が熟成されることで、利用アプリを安心して利用できることになるため、利用促進につながると思っています。また、第三者検証の実施は、アプリ提供者にとっても、ある意味、お墨つきをもらえるようになりますので、有益なものになるかと思っています。

したがって、スマートフォンアプリに対する第三者検証の実施というのは、利用者保護の観点から今後必要な取組で、我が国の解析能力を維持・向上させるためには重要と考えています。また、今回のような事業を通じて、解析事業者がスマートフォンのアプリの解析を実施し、ノウハウを共有する場を整えておくことが重要かと思っています。このような技術が内側に籠もってしまって、ある意味、ノウハウ的になってしまうので、そういう意味では、技術力を今後伸ばしていくためにはこういった場も必要ではないかと考えています。

また、SPIに基づく取組を進めることの重要性ということで、こちらに関しては、SPOの実施を通じて外部送信がなされている利用者情報については、プライバシーポリシーにおいて特定されていたが、残念ながら一部の利用者情報は、プライバシーポリシー情報で特定されていない外部送信情報もあります。したがって、利用目的が明示されておらず、利用者の透明性の観点から懸念が生じるケースというのが幾つか確認できています。

また、このような状況を踏まえると、SPIの趣旨の周知徹底を図るとともに、アプリ提供

事業者、アプリストア運営者においては、SPIを踏まえて適切な対応を取っていくことが重要ということを考えています。残念ながら、本来は書かなくてはいけないものが抜けてしまっているのは、意図して書いていないというわけではないと思うのですが、十分な認知が足りていないケースもあるので、こういったことの啓発が必要と考えております。

続いて、SPIにおいてセキュリティに係る要件を盛り込む必要性ということで、利用者情報の保護のためには、アプリ開発者のみならず、アプリ運営者等、関係者を含めて適切な対応を取ることが重要と考えています。現行のSPIに関しては、プライバシー観点に関して記載はされているものの、セキュリティ観点は明示的に含まれていません。先ほど宮野様からも御紹介がありましたとおり、英国のDSITでは、Code of practiceというものを発行してしまっていて、こちらでは、アプリ開発者とアプリ提供者がどのような対策をすべきかということに記載している8つの項目があるのですが、その中にセキュリティ観点も記載されていますので、そういった意味で、SPIに、こちらにあるような、アプリ開発者に対して脆弱性がある場合の対応、セキュリティバイデザインということで、ちゃんとセキュリティを含めて設計しましょうということです。それで、アプリ運営者としても、脆弱性があるアプリなどに対する対応や、アプリストアとしてセキュリティ要件を明確にすると。最近では、Google PlayではMSAということで、脆弱性侵害があったアプリにマークをつけるような機能も出てきてはいるのですが、こういった機能を充実していくというのにも必要かなと思っています。

あと、また不正なアプリが見つかった場合の対応です。窓口として存在はしているものの、今後は、先般承認された法律でも新しいサードパーティーマーケットというものが出てきますので、そういったことも踏まえると、利用者が不正なアプリを報告できるような窓口、それも分かりやすい窓口というものと、アプリを削除した場合に、その通知方法や、当該アプリの会社の他のアプリの調査をするなどといった対応も必要と思っています。

また、これらを踏まえて、日本スマートフォンセキュリティ協会（JSSEC）が「スマートフォンアプリケーション開発者の実施規範」というものを2024年3月8日に発行していますので、アプリ開発者に関しては、こういったガイドも参考にさせていただきいかなと思っています。

**【山本主査】**      ありがとうございます。

続きまして、またサイバーセキュリティ統括官室の宮野様、お願いいたします。

**【宮野サイバーセキュリティ統括官室参事官補佐】**      ただいまのKDDI様からの発表を踏

まえまして、私から資料7-5に沿って、セキュリティ関係箇所に係るSPIの改定案について、総務省としての案を御説明させていただきます。

こちらのページに書かれておりますのは、基本的にはKDDI様から御発表いただいたとおりの案となっておりますけれども、一部の項目につきましては、プラットフォームとの調整も踏まえた案としているところでございます。

まず、アプリケーション提供者等としまして、アプリケーション提供者、情報収集モジュール等提供者が留意すべき事項として、セキュリティバイデザイン、脆弱性があるアプリへの対応等といった、大きく2つ、分けてございます。セキュリティバイデザインの具体的な事項としましては、アプリの企画及び設計の段階から適切な仕組みを組み込むこと、それから、アプリに組み込む情報収集モジュールについて、セキュリティ確保の観点から内容を確認することと記載してございます。次の脆弱性があるアプリへの対応としましては、脆弱性情報の窓口・連絡先の設置、脆弱性が発見された場合にすぐアップデートなどの必要な対応を取るということ、またセキュリティインシデントが発生した場合には関係者に速やかに周知するよう努めることなどを記載しているところでございます。なお、情報収集モジュール提供者におきましても、アプリケーション提供者と同様の取組を行うこととしているところでございます。

次に、アプリ提供サイト運営事業者が留意すべき事項としまして、2番のところでございますけれども、大きく4つのカテゴリーに分類してございます。

まず、アプリストアの基本的な対応としまして、ストア内で提供されるアプリが満たすべきセキュリティ要件を示し、当該要件を満たすかの審査プロセスを有していること、それから、利用者情報の取扱い等に関する情報を確認可能な場を設けることとしてございます。

次に2つ目の脆弱性があるアプリへの対応としましては、脆弱性報告の窓口を有するとともに脆弱性開示の手続を有すること。それから、最新版にアップデートを促すなど必要な対応を取ること。また、アプリが長期間アップデートされない場合にはサポート状況を確認することなどを記載しているところでございます。

次に、不正なアプリへの対応としまして、不正なアプリを報告できる報告窓口を有すること。それから、不正なアプリを発見した場合には速やかに削除するとともに、当該アプリ提供者のほかのアプリについても調査を行うこと。

最後の類型でございますアプリ削除・掲載拒否時の対応としまして、アプリの掲載を拒

否する場合には、アプリ提供者に適切なフィードバックを行うこととしているところでございます。

なお、図表の一番下の部分に米印で記載してございますけれども、OS提供事業者については、アプリ提供サイトが上記の取組を進めていることを奨励するとともに、必要な措置を講じることが望ましいとさせていただいているところでございます。

今、申し上げた内容としましては、参考資料7-2の37ページから38ページに同様の内容を記載してございますので、御参考までに御確認いただければと思っております。

以上が、セキュリティ関係箇所に係るSPIの改正の概要となりました。

**【山本主査】** ありがとうございます。

それでは、ただいまの御説明につきまして、構成員の皆様から御意見をいただければと思います。今回、御議論を円滑に進めるために、事務局から事前に構成員の皆様の御関心事項を確認いただきましたので、これらの関心事項につきましては、参考資料7-2のSPIの改定案に反映を既にいただいております。それらにつきまして、あるいは、それだけにとどまるものではないと思いますが、構成員の皆様からそれぞれコメントを頂戴したいと思っております。特に事前にお伝えしていなかったかもしれないのですが、御関心事項につきましては既に事務局にもお伝えいただいているかと思っておりますので、その辺りを中心に御発言をいただけると大変ありがたいなと思っております。

まず、生貝主査代理からお願いできればと思っておりますけれども、いかがでしょうか。すみません。突然の御指名で恐縮ですけれども。

**【生貝主査代理】** ありがとうございます。大変丁寧、詳細におまとめいただいて、ありがとうございました。

初回のこちらのワーキンググループの報告の際にも、やはり前回、SPIがつくられてから、改定されてからかなり時間がたっている。それで、その後に日本の個人情報保護法、電気通信事業法等の改正ですとか、やっぱり国際的にも非常に様々な規範の変化といったようなものがある中で、SPIの中にも改定案を、かなり重要な形で取り込んでいただいているかなと思います。特に、プロファイリングの位置付けですとか、あるいは子どもの保護といったようなこと。このことは、同時並行的に、様々な法制面でも幅広く議論されているところだと思いますけれども、こういった形で、やはりベストプラクティスということをしっかり組み込んでいくことというのは非常に意義のあることなのかなと思いました。

それから、サイバーセキュリティの関係です。こちらは、まさにアプリケーションというところに関しては、プライバシーとサイバーセキュリティは、やはりどうしても一体で論じていかなければならないところ、御説明いただいたように、セキュリティの関係にしっかり取り組んでいくことは大変望ましいことかと思えます。

まず、私からは以上でございます。

**【山本主査】** ありがとうございます。本当に、生貝さんからもいろいろ貴重なインプットをいただいたと思います。ありがとうございます。また何かあれば、後で御発言いただければと思います。ありがとうございます。

それから、江藤さんですけれども、先ほどもチャットで入っていたように、途中退席と伺っておりますが、ベストプラクティスという位置付けに関しましてコメントをいただいております。事務局においてこの趣旨を踏まえて反映いただいたということですが、すみません、事前に特に打ち合わせていないのですが、事務局から江藤構成員のコメントについて何か、代読ではないのですが、一言いただければ。

**【川野利用環境課課長補佐】** ありがとうございます。江藤構成員からは、事前に、ベストプラクティスという位置付けというところ、要は法的拘束力がないというところではあるけれども、それについてしっかり取り組むというような姿勢を、ある程度きちんと示したほうがいいのではないかとということで御意見を頂戴したところでございます。

あと、SPIのつくりということにも通じますけれども、基本的には、望ましい措置というのを書かせていただいて、その中で法令上義務がある部分を結構注釈等でお示しておりますが、その辺の関係性をしっかりということでございましたので、その点是对応関係が、望ましい措置、その中で法令上の義務づけがある部分といったようなところで、分かるようにということで、注釈等で少し工夫をさせていただいたところでございます。

**【山本主査】** ありがとうございます。

それでは次に、太田さんからお願いいたします。

**【太田構成員】** ありがとうございます。DataSignの太田です。

まず、今回のSPIの改定につきまして、いろいろと議論の中で対応したほうがいいよねとなったところについては、かなり反映いただいていると思っております。特に情報収集モジュールのところに関しまして、まずスマホウェブの対象になったということは結構大きな改善なのではないかなと思っております。

ただ一方で、先ほどKDDIさんからの御発表にありましたように、プライバシーポリシー

上で特定されないまま外部送信されている事例が多いというところが、御発表であったと思いますけれども、そちらについては私も、アプリとかウェブで外部送信が実際にされているのに、プライバシーポリシー上では書いていないという事例を、かなり多くというか、ほとんどそうになっているというような状況というところには、非常に高い課題感を持っているところがございます。そこには、プライバシーポリシーをちゃんとアプリごとに作成していなかったり、それもKDDIさんの発表の中で、国内アプリは企業プラポリを参照している場合が多いみたいなところで、何となく企業全体のプライバシーポリシーを提示しているというところがあって、アプリケーション単体でちゃんと検査をしてプライバシーポリシーをしっかりとつくるところは、やはり国内アプリは弱いのかなというところは示されたかなと思います。その上で、今回のSPIの中で、アプリごとにちゃんと作成することが望ましいというところが入ったということも、すごくよかったかと思います。

もう一点、ダークパターンについてですけれども、こちら、ダークパターンについての考え方がSPIで示されて、EDPBの示すダークパターンの具体例というところも参照いただいているのですけれども、今回1つ、ちょっと意見を言うとする、EDPBの示すダークパターンの中から、SPIとしてどれに対応することが望ましいのかというところは明記してもいいのかなと思ったところがございます。今の書き方だと、参考みたいな感じで何個か例が挙げられていますけれども、この参考の中にも書いていないのですけれども、よく、同意を促すようなものですね。例えば、iPhoneのATTの同意を得るときに、この同意をしてくれないと何かできませんよ。本当はできるにもかかわらず、そういった掲載であるとか、本当は同意しなくてもいいのに、同意しないと前に進めないようなものに対して、ちゃんとSPIの中で、そういうものはダークパターンになるので、やらないことが望ましいというところを書くのがいいのかと思っております。

先ほどのプライバシー上でちゃんと特定されないまま外部送信されている原因のところにもつながりますし、今のダークパターンのところにもつながるのでございますけれども、やはりアプリストアに対する対応のところ、今回のSPIの中でも、アプリストアがちゃんと、SPIの内容の中で望ましいとされていることに対して審査をするようにみたいところがあると思いますが、そこはすごく重要な点だと思っております。現時点においては、AppleのApp StoreとGoogleのGoogle Play Storeの2つですけれども、こちら、先ほどKDDIさんからも発言がありましたが、新しいアプリストアなどが出てくることが予定されていると思いますので、そうしたことを踏まえると、しっかりとアプリストア各社に対してSPIの参

照を求めていくという活動を何かしらする必要があるかなと思っております。AppleのApp Reviewガイドラインには既にSPIが参照されておりますけれども、今、古いものが参照されていますので、ちゃんとそこが更新されるようにするという活動でしたり、あとGoogleですとか、ほかのアプリストアに対しても、ちゃんとSPIを、審査する際の参考にさせていただいて、先ほどの、プライバシーポリシーに書いていないけど外部送信されているか、企業プラポリになっていてアプリのプラポリになっていないか、ダークパターンになっているといったところをちゃんと担保するために、アプリストアに頑張ってもらうように、こちらから働きかけていくことが重要なかなと考えております。

以上です。

**【山本主査】** ありがとうございます。今回のSPIの改定案の趣旨と申しますか、その位置付けについて、非常に分かりやすく御説明をいただいたのではないかなと思います。ありがとうございます。

それでは木村構成員、お願いいたします。

**【木村構成員】** 主婦連合会の木村です。

時代の流れもあって、こうやって改定していくということは本当に、望ましいというか、当然のことだと思います。それで、今回、ベストプラクティスというところで、行く行くはこれが恐らくスタンダードになっていくのではないかという期待を込めて、今回、望ましいとはしておりますけれども、やはり利用者としてみれば、そういうことをきちんとしてくださっている事業者を選択したいと思っておりますし、あと諸外国の動向を見て、やはり日本だけ遅れているというのは大変残念なことだと思いますので、その辺りも含めて今回の改定は賛成いたしますし、私のふだん申し上げていることも取り入れていただいてありがとうございます。

利用者にとってみると、送信された自分のデータなどがどういうふうに使われているかということが、本当に取得されているのか、されていないのか、そして取得された後どうなっているのかということが、データであるがゆえに分からないというのがとても不安感をあおっていると思います。そこにきちんと透明性を入れていく、規制を入れていく、セキュリティのこともきちんとやっていただくということが、利用者の安全な、そして安心な利活用につながるのではないかと考えております。

今回は必要最小限のデータ取得ということで、本当にそうなるといいなと思っておりますし、あと、同意の有無。それから、包括同意ではなくて、かなりの場面で同意をきちん

と取るということ、それから撤回が明記されていること。もう一点重要なのが、やはりこどもの利用についての視点を入れるということは、私は大変今回重要なことだと考えておりますし、加えて言いますと、こどもだけではなくて、通信に脆弱な利用者に対してもきちんと対応していくことが必要ではないかと思っております。

こうしたことを踏まえて、利用者が安全安心にきちんと使えるように、それで本来ならば利用者が迷わなくてもいいような、きちんとしたプライバシーポリシーであるとか同意取得がなされるように、今後も引き続き取り組んでいければと思っております。

以上です。

【山本主査】 ありがとうございます。

それでは寺田さんからお願いいたします。

【寺田構成員】 よろしく申し上げます。

まず、非常に幅広い関係者からの意見を取り込んでいただき、ありがとうございます。また、昨今の法改正とか業界の実態性から海外の状況などについて、非常に極めて多岐にわたるにもかかわらず、幅広く、また詳細に盛り込んでいただけました。今回、とても大きな改定となったと思うのですけれども、事務局での作業は大変だと思いますが、誠にありがとうございます。

また、今回、SPIにセキュリティを加えるということは大変よいことだと思っています。1つの事業領域に対して複数の場所からガイドラインが発行されているのは、事業者にとっても利用者にとっても非常に煩雑になりますので、可能な限りこういった形で1か所にまとめていただけるのは非常にありがたいことだと思っています。

以上とは別に、4つほど意見を述べさせていただきたいと思います。

1つ目は基本原則です。こちら、一番最初のSPIを作成したときに私から提案させていただいたものが、もう十数年ずっとそのままであったことで、そろそろ新しい課題とかも出てきていますので、今回、不適切な利用の禁止とか、脆弱なものへの配慮というのを基本原則に入れていただくことをお願いいたしました。今回、こちらに反映していただいておりますが、本当にこちらで適切であるかというのは、ぜひ先生方の御意見もお聞きしたいなと思っています。

それと、利用者情報と個人情報、それから通信の秘密というのは、非常に分かりにくい状態。特に事業者にとっては、これがあちこちに分散していて分かりにくい状態になっていたのを、今回しっかりと明示していただいたというのは非常にありがたいことだと思っ

ています。ただ、その一方で、まだもう少し検討すべきと思うところ、現在調整中と伺っておりますが、10ページのところです。個人識別性というところについて、個人情報となるのはあくまでも特定の個人が識別される場合という形になっています。クッキーとか端末IDは、特定はできないが個人を識別する。どちらかという、個人というよりは利用者を識別するという形で使われるのですが、今回あちらこちらに出てくる個人識別性というのが、特定の個人なのか、それとも特定できない個人の場合なのかというのが、やはりちょっと混在してしまっているので、この辺りの書き分けというのをもう少し丁寧にしていただければいいのかなと思っています。

それから、今国会でスマートフォンソフトウェア競争促進法というのが成立したことで、今後、施行に向けて公正取引委員会で、政令とかガイドラインというのが策定されることになっています。現在、こういったスマホのアプリとかストアについての公的機関からの全般的なガイドライン、詳細なガイドラインというのはSPIが唯一だと思います。今後は、外部送信規律が、もともとSPIにあったものが今回法律になったわけですが、これと同じような方向で、第三者によるストアの成立を見据えた法制度化というの、必ずしも全てを法制度化というわけではないですけれども、ある程度そういったことも念頭に入れながら、過不足がないよう、ブラッシュアップしていただきたいなと思っています。

最後に、「子どもの保護」の部分なのですが、非常にここは難しいところだと思っています。特に年齢制限とか、こういったところは明確に書き出せないところだと思いますけれども、26日か、発表された個人情報保護法の3年ごと見直しの中で、16歳未満を検討するというようなことが書かれていましたので、ベストプラクティスとして、この辺のところ、先行するのもありかなとはちょっと思ったりもしています。

細かいことなのですが、この「子どもの保護」というところの「子ども」の表記です。SPIでは「子ども」の「子」が漢字になっていますけれども、全省庁で全て平仮名にするということが推奨されていたかと思いますので、こちら、もう本当に細かいことですが、修正していただいたほうがいいのかと思います。

私からは以上になります。

**【山本主査】** ありがとうございます。表記の点を含めて、微調整できることがあればと思います。今後の課題についてもかなり具体的にお話しいただきまして、ありがとうございます。

すみません。寺田さん、1点目ですけれども、構成員の皆様にも考えてもらいたいとい

うような御発言があったと思うのですが、もう一度、その部分をお願いできますでしょうか。

**【寺田構成員】** 基本原則ですね。こちらに、今までは6つあったところ、今回、私からは、不適切な利用の禁止。今までは不適切な取得の禁止だったのですけれども、個人情報保護法でも不適切な利用というのが禁止になったと思いますので、こちらでも、これは対になるものとして、原則として取得だけではなくて利用に関しても、やはり不適切なものは禁止すべきということを実原則に入れるべきだろうと思います。

それから、こどもの部分であったり、高齢者であったりという、脆弱な方ですね。こういった方たちへの配慮というのも、やはり今、一番ホットな部分でもありますけれども、この部分というのもしっかりと基本原則に入れたほうがいいのではないかなということも提案させていただいています。

もちろん、先ほどお話があったとおり、セキュリティに関してのセキュリティバイデザインというのも、これは私ではないですけれども、こういったところ、基本原則を触る場合には、やはり皆さんの御意見をちゃんと聞いておいたほうがいいのかないかなと申しましたので、お話しさせていただきました。

**【山本主査】** ありがとうございます。確かに個人情報法の改正を踏まえると、先ほどの不適切な取得だけではなくて、例えば利用というのも考えていくべきなのではないかというのは確かにそのとおりかなと申しました。この辺は後でまた全体の御意見を伺う機会を得たいと思いますので、ありがとうございます。

それでは、次に森さん、お願いいたします。

**【森構成員】** 御説明ありがとうございます。寺田さんの先ほどのお話は全くごもつともといいますか、すばらしい御指摘だと思っていて、おっしゃるとおりだと思います。不適切利用の禁止を加えて、あと脆弱性のある人の保護ですよね。全く適切な御指摘だと思いました。

私、4点申し上げようと思いますが、実質的なコメントは2点のみです。先ほど来、KDDIの本間さんのお話とか太田さんのお話で、やっぱりプラボリで特定していない情報の外部送信、情報の取得というのが横行しているということであって、それがやはり、そもそもSPIの主要課題なわけですので、私のアイデアとしては、7ページの、先ほどの基本原則のところの3番目、場所はこだわらないのですけれども、適正な手段による取得の確保のところ、ちゃんと特定せずに外部送信して個人情報とくっつけたら、個人情報保護法

上の適正取得義務違反になりますよと。それを脚注に書いていただく。今回、脚注で、個人情報法違反があった場合のことを書いたというのが1つのポイント、売りだと思しますので、それは違法だということを脚注に書いていただくのがいいと思います。2018年10月に、個人情報保護委員会がフェイスブックに対して行政指導をしていますけれども、これは「いいね！」ボタンの外部送信で、かつ、それが取得先であるフェイスブックのデータベースで個人情報になったということに着目して行政指導をしている。しかもその中身は、ウェブサイトには書いていませんけれども、実質的には適正取得義務違反の疑い、適正取得義務違反のおそれということだったと思いますので、やはりそれは、プラポリに書かずに取得して個人情報にひもづけたら、個人情報保護法20条に違反するということを、脚注で書いていただくのがいいと思います。それが1点目です。

もう一つは15ページです。プロファイリングのところですか。これは、利用目的の特定・明示のところに書かれているので、これもちょっと場所が違うかもしれないのですが、プロファイリングのときに利用目的を特定して明示するとありまして、それは全くごもっともで、そのとおりだと思うのですが、やっぱりプロファイリングとの関係では、どこかでプロファイリングして生成される情報の項目、何を生成しているのかということを示していただくのがマストなのではないかと思っていまして、それがやっぱりプロファイリングとの関係では、プライバシーに一番インパクトがあることなのかなと思いますので、それを、ここではなくてもいいのですが、ここは表題が「利用目的の特定・明示」で、ほかのプロファイリングのところも拝見したのですが、どこがいいのかなと思ってしまいましたので、一応15ページとして申し上げますが、プロファイリングの結果、生成される情報の項目を明示することが望ましいというのを、SPIのどこかに入れていただくのがいいと思います。

以上がコメント2つでして、3つ目はすごくエディトリアルなことなので、ここで申し上げていいかどうか分からないのですが、太田さんの御意見を伺いたいです。私が事前にそうしようと言ったことが影響してそうなっていると思うのですが、定義のところを見ていただきますと、情報収集モジュール等の定義がありまして、情報収集モジュール等の定義が、ウェブ上のタグを含むということになっています。定義の4ページの⑥です。なっているのですが、簡単に言うと、アプリケーションの定義、3ページの③ですが、こちらは別にウェブサイトを含むことにはなっていないのです。ですので、「アプリケーション等」として、アプリとウェブサイトを含む、そして

「情報収集モジュール等」として本来のSDKとタグを含むとするパターンか、それとも、やっぱり分けて書く。アプリはアプリ、ウェブサイトはウェブサイト、情報収集モジュールはSDK、ウェブサイトのタグはタグというふうに分けて書くか、どっちかにしないと、一方が含まれていて一方が含まれていないということが発生してしまっていて、それは私のせいなのですけれども、時々書きぶりとしてあるのが、「アプリケーションに情報収集モジュール等を組み込む場合」というふうに結構たくさん出てくるのですけれども、「情報収集モジュール等」はSDKのみならずタグを含んでいるのですが、それは組み込まれていませんねという話になりますので、すみません、全くエディトリアルな、内容には影響しないのですけれども、そこをすっきりさせたほうがいいのかなと思いました。

最後に、これは本間さんに御質問なのですけれども、アプリプラポリが浅い階層で出てこないけれども、これはアプリの複雑化によるもので、やむを得ないというお話があったと思うのですが、あまりやむを得ないというのがすっきりこなかったといえますか、やむを得なくないような気がしましたので、そこについて、もしお時間があれば教えていただければと思います。

以上です。ありがとうございました。

**【山本主査】** ありがとうございます。大変重要な御指摘をいただいたと思います。

まず基本原則のところですけれども、既に、不適正な利用については事務局で反映をいただいていると理解しています。その上で、脆弱のところですけれども、後で、これはどのように事務局で受け止めて反映したのかについて、事務局から御説明を補足的にいただけるとよいかと。その上で構成員の皆様の御意見を伺うという段取りを取りたいなと思いました。

それから、プロファイリングの種別についてまで明らかにしたほうがよいのではないかという御指摘も、報告書の中で、これは私の記憶だと、要配慮のところについては個別に明記するというようなことがあったかと思うのですけれども、それ以外の部分についてどうだったかというのは、ちょっと私も記憶が今、曖昧になっていますので、この点も事務局から御確認いただいてと思いました。

それから、アプリとウェブサイトを分けて書くのか、「等」でまとめるか。正規タブも同じで、「等」でまとめるか分けるかということなのですけれども、ここも実はエディトリアルな部分以上に重要な点が含まれるかなと思いましたので、太田さんの御意見を伺った上で、また森さんの御意見があればと思いました。

そうしますと、まず、太田さんから、先ほどの森さんの御指摘に対してコメントをいただければと思います。いかがでしょうか。

【太田構成員】      ありがとうございます。5ページの③のアプリケーションの中に、ウェブサイト・ウェブアプリケーションも含めるのか、このままにして情報収集モジュール等のほうにウェブサイトの中の情報収集モジュール、今の記載のままにするのかという、どちらがいいかという質問で合っていますか。

【森構成員】      今の案は、ウェブサイト上の情報収集モジュール等にタグを含めているじゃないですか。でも、アプリケーションにはウェブサイトは含まれていないので、アプリケーションの話とウェブサイトの話とを別々に基本的には書いていて、ところが、情報収集モジュール等には、アプリのSDKとJavaScriptタグが一緒に入ってしまったので、例えば「アプリケーションに情報収集モジュール等を組み込む場合は」と書いてしまうと、文字面上は、アプリケーションにSDKとJavaScriptを組み込む場合はみたいな話になってしまうので、両方一体的に書くか、ウェブサイト・アンド・アプリケーションを、「コンテンツ」とか、あるいは「アプリ等」とか書くか。それとも、分けたほうがむしろ読みやすいのかもしれないと実は思っているのですけれども、アプリのSDKの話、ウェブサイトのJavaScriptの話というのを分けたほうが、すっきり読めるのかなという気もしてまして、どっちかじゃないかなと思ったということです。

【太田構成員】      分けるとすると、結構内容を変えないといけないところが多くなるかなという気がしているのですけど。

【森構成員】      まあ、エディトリアルなことなのですけど。すみません。

もう一件、それとの関係で見たいのが、6ページの四角囲みの4、これは補足の中の4なのですけれども、ちょっと待ってください。これは、ページ数は変わっていないかな。

【太田構成員】      8ページですね。

【森構成員】      8ページ。

【太田構成員】      ここが、「読み替えることとする」というところです。

【森構成員】      そうです。ここでは読替えになってまして。

【太田構成員】      そうですね。

【森構成員】      なので、定義で含む「情報収集モジュール」のほうは全部、定義で大きく含んでしまっているけれども、アプリとブラウザは違うものと考えて、かつ読替えだと

なっているので、それだと結構複雑ではという感じがして。

【太田構成員】 そうですね。今、聞いていて思ったところと言うと、読んでいる人からすると、アプリウェブも含むのだけれども、それは最初のアプリケーションの定義からすると、要するにアプリケーション内のブラウザしか対象になっていない。

【森構成員】 最初はですね。

【太田構成員】 そうですね。

【森構成員】 最初はそうなのですが、この読替えが出てくることによって、そうではなくて、外部送信全部なのだよと。

【太田構成員】 そうですね。そうすると、もう最初の。

【森構成員】 そう。だから、最初からもう両方、全部のほうがいいのではないかなという。そうなのですよ。

【太田構成員】 それは、聞いて、おっしゃるとおりですね。アプリケーションに入れてしまうほうが。それで、アプリケーションに入れた上で、情報収集モジュールにはタグも含まれるというのは残したほうがいいと思うのですが。

【森構成員】 そのやり方と、もうしょっぱなからアプリとウェブサイトとを分けて、アプリ及びウェブサイトというような書き方をして、アプリの場合は情報収集モジュール、ウェブサイトの場合はJavaScriptタグと書き進めていって、場合によっては泣き別れのところというのは出てくるので、アプリケーションに組み込む情報収集モジュールはと、その場合は「等」をつけずに書いてしまえば全然間違っていないので、そっちのほうが分かりやすいかなとも、思ったのですが。すみません。でも、まさしくエディトリアルなことではあるので、あまり時間を取っても申し訳ないかなと思って。

【山本主査】 そうでしたら、この点は内容に関わるというよりも、やはり分かりやすさというか、そういうところ。

【森構成員】 そうです。

【山本主査】 矛盾がないようにするという事だと思います。寺田さんからも御意見を今チャットでいただいているので、この辺りは少しアドバイスをいただいて、事務局とも少し調整をしていく必要があるかなと思いました。この会合の後に、先生方にお時間をいただいてしまって恐縮ですけど、御相談を事務局からさせていただければと思います。ありがとうございます。

【太田構成員】 ありがとうございます。

【山本主査】 それから、事務局への、先ほど基本原則周りのところ、プロファイリングの項目のところですけども、いかがでしょうか。

【川野利用環境課課長補佐】 基本原則に関しましては、寺田先生もおっしゃったように、後ほど出てくるアプリケーション提供者の取組の原則的なところになるところでございますので、今回必要である点を追記したというところではございました。

【森構成員】 すみません。ちょっと横から申し訳ないですけど、ごめんなさい。寺田さんの御指摘というのは、寺田さんの御指摘によって既に入っているけど、それについて他の構成員はどのように考えるのかということだったのかなと。

【川野利用環境課課長補佐】 その点につきましては、各々の構成員の方に御説明する中で、取り入れるべき点を反映しているものもあるところでございます。森先生の御指摘の部分というのは、現状、入れているものに加えてというところでもよろしいでしょうか。

【森構成員】 いえいえ、もう適正利用義務も入っていますし、⑧も入っていますので、新しく追加していただいてよかったなという、それだけのことで。

【川野利用環境課課長補佐】 承知しました。ありがとうございます。

【森構成員】 すみません。失礼しました。

【川野利用環境課課長補佐】 要は、特定の情報及び利用者の属性に応じた配慮といったところで、おっしゃっていただいているとおおり、プロファイリングの件とかが後ほど出てくるので、それに対する基本原則みたいなところが必要かなと思っておりまして、それに対して、利用者本人に対する不当な差別、偏見その他の不利益が生じないように、特定の情報について適切な配慮を行うとともにということに記載させていただいていたところでございます。

また、属性に応じた配慮というところでは、御関心も、議論の中でも高かった、こどもの問題でございますとか、こどもに限られない属性に応じた配慮ということもあるよねと。先ほど注釈で少し高齢者の件を追記していますということを御説明させていただいておりましたけれども、そういう趣旨で追記しているというものでございます。

【山本主査】 ありがとうございます。ここは、基本原則という、まさに骨格に関わるところでしたので、事務局からこういう形で反映したということをお伝えいただいて、皆様に確認いただきたかったという趣旨です。寺田さんのところは、今の基本原則の④と⑧で受け取っているということかなと思います。

それでは、先ほどのプロファイリングの項目についてはいかがでしょうか。

【川野利用環境課課長補佐】 プロファイリングの点は、先ほども御説明させていただいた中で、18ページのアプリプラポリの作成のところでございますとか、利用目的の特定のところ等に反映しておりますが、森先生の御指摘を踏まえまして、これは、他の構成員の先生方の御意見とかも伺った上で、もし反映が適当であるということであれば、場所については追って検討したいと存じます。

【山本主査】 現状は、先ほどの森さんの御指摘のプロファイリングの項目ないし種別については、今今のところの案の中では、望ましいという形では今のところはないという理解でよろしいですか。

【川野利用環境課課長補佐】 プロファイリングに関しまして、現状の記載では、繰り返しになって恐縮ですけど、18ページの1.2.1.1.プライバシーポリシーの作成、利用目的の特定・明示に、本人に関する関心等の情報を分析する、いわゆるプロファイリングを行う場合には、その利用目的を特定することが望ましいといったところでございますとか、25ページ、1.2.1.2.プライバシーポリシー等の運用、通知・公表または同意取得の方法、「同意取得等を要する利用者情報の取扱い」のところに、これはこどもの部分と関係しますけれども、こどもの利用者情報のプロファイリングに基づくターゲティング広告の表示は実施しないといったような部分に入れているところではございました。

また、あとセンシティブ情報への配慮といったようなところで、プロファイリングによりセンシティブな情報を予測・生成する行為は、センシティブ情報の取得につながるおそれも否定できないと考えられることから、原則として実施しないこととするといったようなところで反映しているのですけれども、森先生のおっしゃっている点が、その点、もう少し、どういったところを生成していくのかといったところを明示してもらいたいというのはという御指摘でよろしかったですか。

【山本主査】 森さんに補足していただければと思いますけど、確かにプロファイリングをする、しない、あるいはマーケティングのためにプロファイリングをする、しないということは、恐らく、私の理解では、既に、個人情報法のガイドライン上でも実施していただくような感じになっていると思うのですけれども。すみません。間違っていたら教えていただければと思いますが。

ただ、結局どういう種別の、プロファイリングでもライトなものとディープなものがあると申しますか、私もそのような理解ですので、その種別まで記載すべきなのではない

かというのが森さんの御指摘かなと思いました。ただ、結局、要配慮的なものを生成ないし予測するようなものについては、先ほど川野さんに御指摘いただいたように、一応、今回反映しております。やる場合にはそこをちゃんと明記するというような書き方になっていると思いますけれども、それ以上に、すなわち、要配慮的なものの生成・予測に当たらないけれども、プロファイリングの種別・項目について明らかにしたほうがよいのではないかというのが森さんの御指摘で、この辺りは十分に明確に今回になっていないので、これをより明確にしたほうがよいのではないかという御指摘だろうと思っています。ここは、事業者への御負担というところでも、結構大きな問題、大きなお話にもなってくるかなと思いますので、確かにコンセンサスを取ったほうがよいとは思いますが、森さん、そういう御趣旨でよろしいですか。

【森構成員】 全くおっしゃるとおりです。

【山本主査】 ということで、これは重要な点にも関わっていると思いますので、後でまた構成員の皆様から御意見を伺いたいと思います。ありがとうございます。

もう一点、本間さんへの御質問も含まれていたと思いますので、本間さんから、先ほどの森さんの御指摘、アプリプライバシーポリシーのお話だったと思いますが、お答えいただいでよろしいでしょうか。

【本間氏】 おそらく私の説明があまりよろしくなかったかなと思いますが、まずプラポリの階層の話ですけれども、プラポリの階層は森さんのほうが非常に御存じだと思いますが、何ステップぐらいで開くかという話があるが、おおむね過去の調査では、3階層ぐらいでプラポリが8割ぐらい表示されていたのですが、今年の今回の調査では、3階層で表示できていたプラポリのアプリというのが70%から75%ぐらいということで、若干低くなっていて、ただ一方で、4階層まで行くと差異がないというふうになっています。

アプリのメニューが階層化されてしまっているので、そういったメニューをつくっているアプリに関してはどうしても深くなる傾向がありますということで、ちょっと致し方ないという説明はよくなかったんですけど、アプリの傾向で、深くなるものが多くなっているというのが今の実態かと思っています。ただ、ポリシーとしては本来、比較的ステップが少ない中で表示すべきなので、それは継続して今後も啓発していく必要があるというのは変わっていません。

【森構成員】 ありがとうございます。よく分かりました。

【山本主査】 ありがとうございます。それでは森さん、ありがとうございました。また後で、もしかしたら御意見を伺うかもしれませんので、よろしくお願いいたします。

では呂さん、よろしくお願いいたします。

【呂構成員】 呂です。

今回、SPIの改定案をお取りまとめいただきまして、誠にありがとうございました。プライバシー関係の新しい課題にも対応していただきまして、セキュリティについても取り込んでいただいて、今の時代に合った、より包括的な内容のSPIに進化させていただいたものと考えております。

その上で、割と各論的な話になってしまって恐縮なのですが、かつ既に事前に取り込んでいただいたところも多いのですが、SPIの制定当時、つまり10年以上前と比べて、日本において現に施行されている法律で規則、禁止されている内容というのも増えてきたと認識しています。したがって、ベストプラクティスとして望ましい方法ということと、既に、法で規制されていることとの区別は分かりやすくしておかないと、逆に混乱を招くおそれもあるように思われまして、様々な注釈を入れていただいたところでした。

ということで、既にだいぶご対応いただいているのですが、もう少し記述を充実させられる可能性があるように思いましたのが、ダークパターンのところでして、他の章のところで出てきている内容ではあるのですが、例えば個人情報保護法で不適正利用の禁止が改正により入ったり、適正な取得に関する規律は元々ありましたけれども、そういった規律について少し付記してもいいのかなと思いましたが、同意の取り方についても、ガイドラインで、個人情報保護委員会のガイドラインと、それを受けた「電気通信事業における個人情報等の保護に関するガイドライン」で、合理的かつ適切な方法により同意を取得しなければならないということも定められていますので、そういったところを含め、少し記述を厚くしていただいてもいいのかなと。

また、SPIは、元々は名前どおりプライバシーに関することなので、どこまで取り込むかという問題はあるのですが、現在は景表法や特定商取引法、消費者契約法など、様々な方面からダークパターンに対する対応が進んでいるところですので、SPIの文書の趣旨から大きく外れない、可能な範囲で、そういった規制にも言及していけると良いように思いました。

さらに続けてダークパターンのところですが、もう少し具体的な事例といえますか、SPIとしてこういった手法に注意すべきかということも記載した方が良いのではないかと

うことで、太田さんからもコメントがあったものと認識しております。最近の政府から出ている文書で、消費者白書の最新版、令和6年版（令和5年度版）ということになりますが、そちらではOECDの報告書を引用された上で、インターフェースの図なども載せたりして、こういった手法に気をつけるべきということに注意喚起されています。その中で、クッキー同意を取得する際に「同意しない」選択肢を視認しづらくする方法や、位置情報を取得するために繰り返し同意を求める画面を出すといった、プライバシーに関する事例についてもかなり分かりやすく示されているので、もしよろしければ御参考いただけると良いかと思いました。このような形で様々な方面から注意喚起していく文書が出されているのはとても良いことなので、上手く連携できれば良いように思ったところでした。

私からは以上です。

【山本主査】 ありがとうございます。呂さんの御指摘を踏まえて、事務局でも、現状、法的に既に要請されている、あるいは義務づけられている部分と、ベストプラクティスの部分との切り分けが読み手に分かるというようなことで、いろいろとご調整いただいているところですが、さらに、ダークパターンの辺りですとか同意の取り方のところで記述を充実させることもできるのではないかということだったと思いますので、その辺りはどこまでやれるかということもあると思いますけれども、事務局には御検討いただければと思います。消費者白書の情報も貴重なインプットをいただいたと思います。ありがとうございます。

一通り御意見をいただきました。先ほど寺田さんからはチャットで御意見をいただいているところですが、1つ、目線を合わせておいたほうがよいかなと思ったのが、先ほど森さんから御指摘をいただいた、プロファイリングの種別についても明確にしていくべきではないかという点です。ここは内容にも関わってくるころだと思います。この点、寺田さん、いかがでしょう。チャットでいろいろ御発言いただいていますけれども、改めて口頭でお話しいただければと思います。

【寺田構成員】 プロファイリングに関して事業者が何をすべきかということに関しては、唯一に近いかな、DMA、EUのデジタル市場法で、ゲートキーパーに対してプロファイリングについてレポートを出せというのがあって、これがテンプレート化されています。これは、恐ろしいほど細かいところまで書かれているので、これ全部を日本で、たとえベストプラクティスでも全部入れるのはちょっと重いとは思うのですが、取捨選択していただいて、何の情報を、何にどういう処理をして、何に使うのかということに関しては、

最も大きなものとしてテンプレートの中でも書かれていますので、そういったものはベストプラクティスとして取り入れるというのは、既にもう海外では存在しているものなので、やってもいいのかなと思いました。

【山本主査】 ありがとうございます。対象者が、DMAの場合にはゲートキーパーというところをどう考えるのかとか、いろいろその違いもあろうかと思えますけれども、ある程度のところまでは書けるのではないかという御指摘だったと思えますけれども、ありがとうございます。

ほかの方はいかがでしょうか。まだ生貝さんが残っていらっしゃるとすれば、生貝さんもヨーロッパの、EUの法制にお詳しいので、この辺り、御意見があればと思いますが、いかがでしょうか。

【生貝主査代理】 ありがとうございます。どこまで書き込むか。DMAのテンプレートは、おっしゃるとおり、参考になる部分があるかなと僕も思います。

それに加えて、プロファイリングを実施することそのものと、プロファイリングに基づいた決定を行うことの両面から考えていく必要があるということ、事前のヒアリングでもお話をさせていただいて、そして今は脚注15に、決定を行う場合の対応というのを書いていただいているところですが、決定を伴うプロファイリングに関しては、そのロジックというのが1つの透明性条項としてGDPRの中でも重視されている。そういった側面をどのように考えていくかというのも1つの論点にはなるところかなと思いました。

取りあえず僕からは以上です。

【山本主査】 ありがとうございます。

ほかの方はいかがでしょうか。例えば太田さんとかはいかがでしょうか。今のプロファイリングの種別とかで。

【太田構成員】 僕は特に、今議論されている内容の方向で進めていけば問題ないと思っております。

【山本主査】 これは、私は具体的なイメージがまだ、いや、私も方向性としては望ましいかなと思っておりますが、例えば具体的にどういうことを明示する形になるのかというのは、技術的なことも分かっていないとなかなか難しいかなと思うのですが、太田さん、例えばどういうふうを書くということになりますか。例えばですけど。

【太田構成員】 なかなか難しいですね。

【山本主査】 そうですね。ここが、我々として共通のイメージを持っていないと、

なかなかベストプラクティスだよということも言えないところもあるかなと思います。森さん、この辺はいかがでしょう。どういう粒度で書く、何を書くかというところですけども。

**【森構成員】** ありがとうございます。そうですね。これは難しい問題であるとは思いますが、でも例えば今の既に原案でも、センシティブ情報については項目を明示すると書いてあると思うのです。なので、項目とは何かというのは、その項目は個人情報保護法の法律用語でありますけれども、その項目の粒度がどうなっているのかというのはあまりはっきりしていないと思うのですが、やっぱり基本的には事業者側の分類というか、事業者側のデータベースにおいて、どういう分け方をしているかということだと思えます。なので、例えば「アーリーアダプター」ということにしてチェックを入れる、0と1になっているとか、「怒りに流される」で0と1になっているとか、そういうふうにされていけば、それを言っていたきたいということだと思いますので、私としては、そんなに負担の大きなものではないと思います。

**【山本主査】** なるほど。要するに、ある種、意思決定に影響を与え得るようなセグメンテーションということになるのですかね。

**【森構成員】** もちろんそういうのもあると思いますし、そうでないものもあると思いますけれども、我々としては、やっぱりそういう、センシティブではないにしても、自分たちの脆弱性を暴かれているのではないかというところは気になりますし、センシティブではない、逆に、全然問題のないことしかプロファイリングしていませんよと。この人は関東近辺の住人ですとか、そういうことだってプロファイリングで出てくることはあるわけなので、その場合、多分、住所とか、そんな感じになると思うのですが、プロファイリングしているのはどういう情報ですか。住所とか年齢層。年齢などもプロファイリングで出てきますよね。それで、住所と年齢ですと言われたら、住所と年齢と性別ですと言われたら、そうかなと思うし、アーリーアダプターも、そうかなと思いますけれども、「怒りに流される」と言われると、いや、俺は別にそんなことないけどなと思いますし、そういうことなのではないかと思います。

**【山本主査】** 分かりました。太田さんもこの辺りは技術的な観点であり得るといえるか、可能という理解でよろしいですか。後で寺田さんにも聞いて。

**【太田構成員】** そうですね。どういうセグメントに企業が分けているかというところで、今の森先生の話だと、分けたセグメントが、先ほど森先生がおっしゃったように、地

域とか、そういうところではなくて、自分の……。

**【森構成員】** サイコグラフィックです。

**【太田構成員】** そうですね。サイコグラフィック的なものというところを分類する。それは、技術的にというか、どういうセグメントをつくっていったって、その中でちゃんとセグメントのプライバシーインパクトみたいなものを、ちゃんとアセスメントをして、そこに対応していくということは必要なのかなというのを、聞いていて思ったのですが、今ちょっと思ったのが、地域のプロファイリングはいいということになっても、例えば、プロファイリングをして地域が分かりました。それで、その地域に住む人はこういう傾向があるみたいところで、どんどんプロファイリングした結果からまたプロファイリングされていくということもあると思うので、要は、プロファイリングした結果、どういうものに、どういう情報になって、それが何に使われるのかということところが結構重要なところなので、どういうプロファイリングをしてそれを何に使っているのかということところが、セットで見られるといいのかなという気はいたしました。

**【山本主査】** ありがとうございます。

**【森構成員】** 利用目的もそうなのですが、やっぱり広告用語で言うとセグメントの切り方みたいになるのだと思うのですけれども、どういう項目を抽出しているかということによって、今の、要するにデモグラフィックでもサイコグラフィックでもということなのかもしれませんけれども、やっぱりインパクトが変わってくるので、いろんな議論はあり得ると思うのですけれども、まずは項目、セグメントを明示してもらおうというのは、第一歩としてはあるのかなという気はしますけどね。

**【山本主査】** ありがとうございます。寺田さんから御発言の希望が出ていると思いますので、寺田さん、お願いいたします。

**【寺田構成員】** 前提として、センシティブな情報というのはできるだけ使わないようにしようというのはありますが、それ以外の安全とされているデータでも、組合せ次第ではいろんなことが、推測するとか、AIを使えば、こういうのに該当する人はほかのところの情報と照らし合わせてどうのなどということは幾らでもできてしまうので、一定程度のセグメントというのを、もちろん出すのは必要ですけれども、それにプラスして重要なのは、利用目的を明示して、それ以外のことはしませんよということ、やはり大前提にするべきなのかなと思っています。これは、今回原則に入った不適正な利用の禁止というものとも連携する話になると思いますので、まずは利用目的が、差別とか不利益を起

こさない。そのために、利用目的を明確にして、それに必要なだけのデータですよね。こういうセグメントでこういう利用目的です。それ以外はやりませんというようなことを明確にしていくというのが、取りあえず一番、大枠としては、方向性としては必要なのかなと思いました。

**【山本主査】** ありがとうございます。恐らく、例えば利用目的というところで考えたとしても、1つがマーケティングかどうかということになると思うのです。恐らく森さんのおっしゃっていることの趣旨は、マーケティング目的であっても、サイコグラフィックを使ったようなセグメンテーションであると、ある種、かなり引っかけやすいということになってくるので、マーケティング目的という利用目的だけでは足りないのではないかなというのが、森さんの御指摘の中に含まれていたかなと思うのです。森さん、そういう趣旨でいいですか。

**【寺田構成員】** 利用目的を明確にして、そのためにこのデータを使いますということを示すということですね。そうすれば、サイコグラフィック的なものや、そういったものというのは含まれているか、含まれていないかというのは、利用者のほうから確認できますので。もっとも、それをやっても、AIを使ってほかのデータと突合して比較してとすると、推測できてしまうという部分があるので、これは、不適正な利用の禁止というところで止めるべきなのだろうなと思います。

**【森構成員】** マーケティングといっても、今みたいに色々な種類の広告があるわけなので、マーケティング目的といたって、最悪、政治広告だったりするものも販売はされているわけですし、デモグラフィック情報だって、太田さんの言われるとおり、色々なものがあります。例えば特定の地区だとか、そういうことをプロファイリングすると、それはそれで問題があるかもしれませんし、サイコグラフィック情報でも、例えば「アウトドア派」などというのもサイコグラフィックだと思うのですが、それは全然問題ないし、普通にマーケティングに使われると思いますので。なので、マーケティングとの関係でも、なかなか一概に、これはセーフでこれは危険と言いきいと思うのです。ですので、どういう項目でプロファイリングするのか、取りあえず教えてもらいましょうかというのは、いいのかなと思いました。

**【山本主査】** これは、私も森さんと、方向性としては非常に似たような考え方を持っていますが、現実的なところで、例えば項目が幾つぐらいあるのか、出てくるのかという部分ですとか、物すごく大量に項目がわっと例えばリスト的に出てくるようなイメージも

あったりします。ベストプラクティスなので、もちろん法的な拘束力はないわけですが、  
ども、どういう形で表示すべきなのかというところでフィージビリティを確保しなければ  
ならない。やはり我々として具体的なイメージは持っておかないと、事業者も何をして  
いいか分からないということになってしまうので、その辺り、いろいろと確認すべきこと  
があるかなという印象はあるんです。非常に重要な御意見だと思いますが、今今のところ  
で何か決めることがちょっと難しいのではないかなと思いました。これは宿題とさせてい  
ただいて、事務局とも調整しつつ、先生方からの御意見も改めていただきたいと感じた  
ところです。本当に貴重な、重要な……。

寺田さん、どうぞ。

【寺田構成員】 セグメンテーションの最初の分類はどれだけあるのですかということ  
ころでいくと、一番少ない、今回のGoogleのプライバシーサンドボックスでも三百数十で、  
多いところは数万でありますので、これはちょっとというのは、そこを全部というのはち  
よっと現実的ではないとは思いますが。

【太田構成員】 1つ、ごめんなさい。

事例としてあるのが、米国のアドテック企業とかが取り組んでいる中で言うと、自分がど  
ういうセグメントに属しているのかということを表示するようなページをアドテック事業  
者が作っていて、自分のブラウザなりアプリでアクセスすると、自分がどういうセグメン  
トに属していますよということが分かって、Googleとかもそういった対応をしていますけ  
れども、自分がどういうセグメントに属していますよということは、自分で見られて、か  
つそこからオプトアウトできるというようなところは、結構、海外でも事例はありますの  
で、そういった形がいいのかなと、聞いていて思いました。全部出すというよりは、アク  
セスしてきたその人がどのセグメントに属しているかということをちゃんと明示するとい  
う方法で、何万とかある中でも自分が属しているのは何十個ということになるので、そう  
いう表示の仕方が現実的ではないのかなと思います。

【山本主査】 なるほど。そうすると少し絞られるということですね。

いや、非常に重要な御指摘をいただきました。森さんもありがとうございます。本当に  
問題意識は私も共有していますけれども、どういうふうの実務的なところに落とし込むか  
というところかなと思いますので、そこは少し検討が必要なのかなと思いますので、  
改めてまたお諮りしたいと思います。

時間が今日はもう少し早く終わるかなと思っておりました。生貝さん、ではショートで

お願いします。

【生員主査代理】      ありがとうございます。プロファイリングの点は引き続き重要な点で、検討する必要があるかなというところと、あと、ちょっと別のところで2点ほどだけなのですけれども、最初のほうで寺田さんからいただいた原則のところ、大変充実した形で書いていただいて、これらの内容は全て残すべきかなと思うと同時に、また他方で、やはり原則というものをある程度、数としてあまり多過ぎず整理することも重要なのかと思ったときに、幾つか恐らく整理でき得る部分もあるのかなと。例えば、適正な取得と不適正な利用というところでありますとか、あるいはプライバシーバイデザインというのは原則項目の中にあるのですけれども、せつかく後ろのほうにある「セキュリティバイデザイン」という言葉が原則に入っていないのが、少しもったいないかなという気もしまして、プライバシー及びセキュリティバイデザインといったまとめ方もあろう。さらに、セキュリティと安全管理の確保といったところ、どのように使い分けるかといったようなところを含めて、現在の意図をよく生かす形で、原則として広く流通するものとしていただければと思いましたが1点目でございます。

それから、もう一つといたしまして、あと、今回もアプリストアに関して、英国のガイドライン等を参考にしながら様々なことを書いていただいているところ、やはり彼らのアプリストアの果たす役割というのは、ゲートキーパーとしても非常に大きいのだろうといいましたときに、今回のこういった求められている事項というものについて適合しないアプリについて、削除等の対応をするといったようなことが、今のところ、例えば33ページですと、方法が適切ではないアプリが判明した場合、アプリストアから削除する等の対応を実施するというふうに書いていただいているところ、このことは、片方では、ここの文脈では必ずしもないかもしれませんが、やっぱりアプリを提供する方々の予見可能性といったようなところと、またこれは片面では、やはりアプリを作っている方々が、どうして削除されたのだろう、どうすれば、まさに望ましいことに適合した形で再びちゃんと掲載し続けてもらえるのだろうといったようなことを、ちゃんと説明するといったことも、恐らくSPIとの関わりでも重要なところかなと思います。

例えば英国のアプリストア運営者のガイドラインですと、やはり拒否の正当性を説明して、アプリが承認されるためにどういった要素を変更する必要があるかを明確にした、一貫性のある実用的なフィードバックを提供する必要があるといったことが書かれていることなども参考に、まさしく、しかるべきアプリが流通していくためのフィードバックの在

り方というのも少し強調されてもよいかなと思いました。

以上でございます。

【山本主査】 ありがとうございます。いろいろと今日も、新たなものも含めて御意見をいただいたと思います。事務局のほうで私、相談しながらですけれども、修正案を作成していただこうと思っております。

ただ、いろいろ議論があるところもあるかなと思います。特にプロファイリングの辺りは、基本原則で今回掲げたことを踏まえて、どういうものがベストプラクティスなのかということを、フィージビリティも踏まえつつ考えなければいけないと思います。また各構成員の皆様に御意見を伺いつつ、修正案を作成していきたいなど、あるいは修正案の作成を事務局のほうでいただきたいなどと思っております。

また、この会合、場合によっては書面開催の場合も含まれますけれども、議論を深めていきたいと思っております。ひとまず、このような進め方でよろしいでしょうか。

(「異議なし」の声あり)

【山本主査】 ありがとうございます。それでは、事務局において必要な対応を進めていただければと思います。

事務局から連絡事項があればお願いいたします。

【川野利用環境課課長補佐】 今、山本先生からいただいた点について、事務局でも対応を検討したいと存じます。

また、次回会合につきましては、別途、事務局から御案内いたします。

ありがとうございます。

【山本主査】 ありがとうございます。

それでは、以上で利用者情報に関するワーキンググループ第7回会合を終了とさせていただきます。本日も皆様、お忙しい中、御参加、御出席いただきまして、ありがとうございました。

以上