別紙２

利用者情報に関するワーキンググループ

報告書

令 和 ６ 年11月29日

利用者情報に関するワーキンググループ

はじめに

ICT サービスの拡大とともに、サービスの利用に伴う諸課題も拡大・多様化してきてきた。「令和５年　通信利用動向調査」（令和６年６月７日公表）によれば、インターネット利用における不安として「個人情報やインターネット利用履歴の漏えい」が89.4%と最も多い状況となっている。

このような課題を受け、「ICT サービスの利用環境の整備に関する研究会」（座長：宍戸　常寿　東京大学大学院　法学政治学研究科 教授）の下に開催されるワーキンググループとして、「利用者情報に関するワーキンググループ」（主査：山本　龍彦　慶應義塾大学大学院 法務研究科 教授）を設け、電気通信事業、プラットフォームサービス等に係る利用者情報の更なる保護に向けて、最近の動向等を踏まえ、専門的な観点から集中的に検討することとし、2024 年３月１日の第１回会合以降、12 回の会合を開催し、①スマートフォン上のプライバシー対策及び②利用者情報に係るモニタリング等について議論してきた。

今般、①スマートフォン上のプライバシー対策について、電気通信事業法（昭和 59 年法律第 86 号）における外部送信規律の法制化、情報収集モジュール等の情勢変化を踏まえ、スマートフォン利用者情報取扱指針を見直すべきかについて、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.その他の観点から議論を行った結果、当該指針を見直すこととし、「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）」を取りまとめたものである。

第１章　　検討の背景

１．　スマートフォン利用者情報取扱指針

スマートフォン利用者情報取扱指針は、スマートフォンの普及に伴い、アプリケーション等により取得・蓄積された利用者情報が、本人の意図しない形で外部送信されている事案が発覚し、社会問題化したことを踏まえ、総務省においてアプリケーション提供者等の関係事業者が利用者情報を取り扱う上で従うことが望ましい事項（プライバシーポリシーの作成・掲載等）をまとめたものであり、「スマートフォンイニシアティブ（SPI）」の一部として 2012 年に公表後、当該取組について検証し、その結果の取りまとめ（SPO）を随時実施の上、2015 年及び 2017 年の２度改定を行ってきた。

当該改定以降、国内制度の改正や諸外国及び民間事業者の動向に変化が生じており、当該変化を踏まえた見直しが必要と考えられる。

２．　主な国内制度の改正

スマートフォン利用者情報取扱指針の直近の改定以降、利用者情報の取扱いに関連する各種国内制度の見直しが進められてきた。2022 年４月には、個人情報の保護に関する法律等の一部を改正する法律（令和２年法律第 44 号）が全面施行となり、個人情報の不適正利用の禁止や、外国にある第三者への個人データの提供時の情報提供の充実化、個人関連情報及び仮名加工情報の新設等が規定された。

また、2023 年６月には、電気通信事業法の一部を改正する法律（令和４年法律第 70 号）が施行され、大量の情報を取得・管理等する電気通信事業者を中心に、利用者に関する情報の適正な取扱いを促進するため、情報取扱規程の策定・届出の義務付け等を定めた特定利用者情報規律や、ウェブサイトやアプリケーションを利用する際に、利用者の意思によらず自身の情報が外部に送信されている場合に、当該情報の外部送信について利用者自身で確認できるようにするため、通知・公表等の義務付けを定めた外部送信規律が導入された。

３．　諸外国等の動向

この間、国内のみならず諸外国においても、利用者情報の取扱いに関連する制度・規範の導入が行われてきた。

欧州においては、2018 年５月に一般データ保護規則（General Data Protection Regulation：GDPR）が施行された。同規則は、個人（データ主体）の権利を保護するため、識別された又は識別され得る自然人に関するあらゆる情報を個人データと定義するとともに、個人データは、データ主体との関係に

おいて、適法、公正かつ透明性のある態様で取扱われるべきこと、特定された、明確かつ正当な目的のために収集されるべきこと、その個人データが取扱われる目的との関係において、十分であり、関連性があり、かつ、必要のあるものに限定されるべきこと等を基本原則としている。利用者情報の取扱いに関連しうる具体的な規律としては、例えば、プロファイリングを含む自動的な個人データ処理に基づく決定からのデータ主体の保護や、こどもの同意に適用される要件、特別カテゴリーに属する個人データ（民族、信条、健康に関するデータ等）の取扱いを原則禁止すること等が規定されている。

また、2022 年 11 月にデジタルサービス法（Digital Services Act）の一部が施行し、2024 年２月からは EU 内の全ての対象事業者に法遵守義務が課せられた。同法の目的は、安全で予測可能かつ信頼できるオンライン環境のための調和された規則を定めることにより、仲介サービスのための域内市場の適切な機能に貢献することとしており、その中でイノベーションを促進し、消費者保護の原則を含む憲章に謳われた基本権が効果的に保護されることとされている。利用者情報の取扱いに関連しうる具体的な規律としては、ダークパターンと呼ばれるサービス利用者を欺いたり操作したりする手法の禁止、プロファイリングに基づく広告の表示や推奨システムのパラメータに係る透明性確保、未成年のオンライン保護等の義務が課せられている。

さらに、2022 年 11 月にデジタル市場法（Digital Markets Act）の一部も施行し、2024 年３月からは EU 内の全ての対象事業者に法遵守義務が課せられた。同法の目的は、ビジネスユーザ及びエンドユーザの利益のために、ゲートキーパーが存在する EU 全域のデジタルセクターにおいて、全ての事業者が競争可能で公正な市場を確保するための調和された規則を定め、域内市場の適切な機能に貢献することとされている。利用者情報の取扱いに関連しうる具体的な規律としては、消費者のプロファイリングのための技術について、独立監査済みの説明を欧州委員会に提出しなければならないとする義務がゲートキーパーに課せられている。

英国では、2022 年 12 月に、セキュリティ・プライバシーの確保の観点から、アプリ流通におけるアプリストア運営者やアプリ開発者等の役割の整理を図るため、アプリストア等に対するコード・オブ・プラクティス（行動規範）が公表された。セキュリティ・プライバシーの基本要件を満たすアプリを承認することや、ユーザに対する情報提供、開発者へのガイダンスの提示、開発者への明確なフィードバックの提供等について、アプリストア運営者及びアプリ開発者が留意すべき事項が取りまとめられている。

さらに、こどもの保護の観点からは、インターネット上のこどものデータ保護のための 15 の行動規範が示された Children's Code が 2021 年９月に施行さ

れており、英国においてこどもがアクセスする可能性があるサービスにおいては、こどもの利用に適したプライバシープラクティスが求められている。例えば、プライバシーに関する情報や規約等についてこどもの年齢に見合った言葉で記載し、個人情報がどのように利用されるのかを簡単に説明しなければならないことや、ユーザプロファイリング機能はデフォルトでオフにすること等が定められている。

米国に目を向けると、2020 年１月に、カリフォルニア州居住者の個人情報を収集等する一定の事業者に適用されるプライバシー保護法であるカリフォルニア州消費者プライバシー法（California Consumer Privacy Act）が施行され、消費者が想定しない目的で個人情報を収集しようとするときはジャストインタイム通知を行うこと、ホームページやアプリケーションのダウンロードページ等に個人情報の販売からのオプトアウト権があることに関する説明を記載すること等が義務付けられた。

2023 年１月には、プライバシー保護を強化する形で CCPA を拡張したカリフォルニア州プライバシー権法（California Privacy Rights Act）が施行され、プロファイリングを含む事業者による自動意思決定技術の利用についてのアクセス権・オプトアウト権の規定や、個人情報の販売に加えて共有についてもオプトアウト権があることについて説明を記載することの義務付け等が行われた。

４．　民間事業者の動向

国内外の制度の変化のみならず、アプリケーションやアプリケーションストアを提供する民間事業者においても、利用者情報の取扱いの在り方が変化してきた。

総務省においては、SPI で示されたスマートフォンにおける利用者情報の適正な取扱いに関する「スマートフォン利用者情報取扱指針」の浸透状況や、各種団体・企業等の取組状況を把握するため、スマートフォンアプリケーションにおける利用者情報の取扱いの現況等に関する定点調査である「スマートフォン　プライバシー　アウトルック」(以下「SPO」という。)を毎年実施してきた。調査項目の一つとして、スマートフォンアプリケーションにおけるプライバシーポリシーの掲載有無や記載内容、概要版の掲載有無について調査を行っており、プライバシーポリシーの掲載率については、2014 年の調査時には iOS で59%、Android で 72%であったところ、2021 年の調査時には iOS 及び Android ともにほぼ 100%に達している。一方、プライバシーポリシーの概要版の掲載率については、2015 年の調査以降、数%程度で推移しており、改善の傾向は見られていない。

また、SPO ではアプリケーションストア運営事業者における利用者情報の取扱いに関しても調査を行っており、Google、Apple ともに、全アプリケーショ

ンにおけるプライバシーポリシーの掲載の義務化、端末固有の識別子の OS レベルでの取得制限と広告 ID の導入、プライバシー性の高い情報の取得・アクセスに関する個別同意の取得の必須化、アプリケーションが取得する情報を簡易に確認できる仕組みの導入等、SPI の策定当初と比較し、プライバシー保護に関する取組が大きく変化してきた。

第２章　　スマートフォン利用者情報取扱指針の改定

１．　スマートフォン利用者情報取扱指針の改定に係る論点

第１章１．で記載したとおり、スマートフォン利用者情報取扱指針の直近の改定以降、スマートフォン上の利用者情報の取扱いを巡っては、関連する国内外の制度や民間事業者における取組に大きな変化があったことを踏まえ、本ワーキンググループにおいては、以下の各論点について検討を行っていくこととした。

（第１回事務局資料）

項目案	論点案
1．位置付け	• 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、一歩進んだレベルを目指すべきであるとの意見があるがどう考えるか
2．国内制度の反映	• SPI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 （例）個人情報保護法改正（R2）個人関連情報の第三者提供規制等 電気通信事業法改正（R4）外部送信規律等
3．諸外国等の動向を踏まえた対応	• 諸外国や国際標準の動向を踏まえ、SPIに追加等が必要な事項はあるか （例）子どもの利用に適したプライバシープラクティス　等
4．民間の取組を踏まえた対応	• 民間の先進的な取組等を踏まえて、SPIに追加等すべき事項はあるか （例）利用者を識別する情報の取扱い　等
5．その他	• 現状のSPIに規定しているアプリ提供事業者、情報収集モジュール提供事業者、アプリ提供サービス運営事業者、OS事業者を対象とすることでよいか • その他SPIの見直しにあたり検討すべき事項はあるか

本ワーキンググループにおいて、当該指針の位置付けについて改めて検討するとともに、第１章２．から４．までに記載したようなスマートフォン利用者情報取扱指針の直近の改定以降の国内制度の改正や諸外国及び民間事業者の動向等を踏まえ、スマートフォン利用者情報取扱指針の見直しの方向性について

議論を行い、スマートフォン利用者情報取扱指針に反映すべき事項について取りまとめ、第２章２．に記載した事項を反映の上、別添のとおり、SPI 改定案として、「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」を作成した。

２．各論点に関する検討

（１）位置付け

スマートフォン利用者情報取扱指針は、第１章１．において記載したとおり、アプリケーション提供者等の関係事業者が利用者情報を取り扱う上で従うことが望ましい事項を示したものであるが、この位置付けについて、構成員からは以下のとおり意見があった。

（構成員からの意見）

・現行の SPI の内容については既に外部送信規律として法制化されたところ、それを遵守させるだけの内容では意味がなくなってしまうため、SPI として意味のあるもの、ベストプラクティスとしてあるべき。（第 1 回森構成員）

・法令より一歩進んだレベルを求めつつも、有効性・実効性が乖離しないようにするべき。先進的な内容にして、実務がついていかなくなってしまうのは問題であり、一方で実務に合わせすぎた結果、民間に主導されて時代遅れにならないようにする必要もある。（第 1 回江藤構成員）

・諸外国と比べ、日本の個人情報保護に関わる規律は、ハードローにおいては必要最低限のものとなっていることから、ソフトローの部分も含めてユーザ保護を考えていくことは重要。（第１回生貝主査代理）

・SPI の制定当時と比べ、日本において施行されている法令で禁止された事項も増えてきたと認識している。無用な混乱を招かないように、ベストプラクティスとして望ましい方法と、実際に法で規制されている事項とを区別するとよい。（第７回呂構成員）

これらの意見を踏まえ、スマートフォン利用者情報取扱指針においては、法令から一歩進んだ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た。

一方、スマートフォン利用者情報取扱指針において望ましいこととされている事項について、法令において規制されている場合があることから、対応する事業者において混乱を招くことがないよう、区別して記載するべきとの意見があったことも踏まえ、スマートフォン利用者情報取扱指針に法的拘束力はない点を明記した上で、法令において規制されている場合には、その旨を付記する

こととした。なお、関係事業者が対応することが望ましいとされている事項について、その望ましいとされる度合いについて整理して構造的に示すことを今後検討することとした。

（２）国内制度の反映

第１章２．に記載したとおり、スマートフォン利用者情報取扱指針の直近の改定以降、個人情報保護法や電気通信事業法等、利用者情報の取扱いに関連する国内制度の改正が行われてきたところ、これらの国内制度の動向を踏まえた対応について、構成員からは以下のとおり意見があった。

（構成員からの意見）
・国内制度の反映は必ずやる必要がある。個人情報保護法と電気通信事業法とでバラバラに規律されている面があり、事業者や消費者から分かりづらくなっていることから、その対象について整理するべきではないか。（第１回寺田構成員）

これを踏まえ、個人情報の保護に関する法律等の一部を改正する法律（令和２年法律第 44 号）により規定された、個人関連情報及び仮名加工情報の新設、外国にある第三者への提供の本人説明充実化並びに不適正利用の禁止について記載することとした。また、電気通信事業法の一部を改正する法律（令和４年法律第 70 号）を踏まえ、特定利用者情報規律及び外部送信規律についても記載することとした。

（３）諸外国等の動向等を踏まえた対応

①　ダークパターンに係る対応

ダークパターンについては、EU の DSA[1]において明示的に禁止されているほか、欧州委員会、欧州データ保護会議（EDPB）、連邦取引委員会（FTC）、経済開発協力機構（OECD）等、各国の機関によるガイドラインや報告書において様々な分類がなされている。ダークパターン自体は、サービス利用者を欺いたり操作したりする手法を広く指す概念であるが、EDPB の策定したガイドラインにおいては、特にデータ保護の観点から以下のとおり分類されている。
（第３回株式会社三菱総合研究所資料 P20）

[1] DSA 前文（パラ 67）でダークパターンに言及、第 25 条にて禁止が規定されている。

4. ダークパターンの分類 （6）EDPB【分類：全体像】

- EDPBのソーシャルメディアにおける欺瞞的デザインパターンのGDPRガイドラインでは、「ダークパターン」を6カテゴリ・16パターンに分類している*1。

カテゴリー	パターン
1. 過剰負荷（Overloading） ユーザーを大量の要求、情報、オプション、可能性に埋没させ、それ以上進むことを阻止し、特定のデータ慣行を維持または受け入れさせる。	**1.1. 絶え間ない指示**（Continuous prompting）
	1.2. プライバシー迷路（Privacy Maze）
	1.3. 多過ぎる選択肢（Too many options）
2. 省略（Skipping） ユーザがデータ保護の全部または一部の側面を忘れたり考えなかったりするようなインターフェースやユーザジャーニーを設計する。	**2.1. 欺瞞的な居心地よさ**（Deceptive snugness）
	2.2. あっちを見て（Look over there）
3. 煽り（Stirring） 感情に訴えかけたり、視覚的な刺激を与えたりすることで、ユーザの選択に影響を与える。	**3.1. 感情的舵取り**（Emotional Steering）
	3.2. 簡素な見た目に隠す（Hidden in plain sight）
4. 妨害（Obstructing） ユーザが情報を入手したりデータを管理したりする行為を困難または不可能にすることによって、そのプロセスを妨げたり阻止したりする。	**4.1. 行き止まり**（Dead end）
	4.2. 必要以上（Longer than necessary）
	4.3. 誤解を招く行為（Misleading action）
5. 気まぐれ（Fickle） インターフェースのデザインが不安定で一貫性がないため、処理の内容を把握し、データに関する選択を適切に行い、さまざまなコントロールがどこにあるのかを見つけることが難しい。	**5.1. 階層性の欠如**（Lacking hierarchy）
	5.2. 非文脈化（Decontextualising）
	5.3. 一貫性のないインターフェース（Inconsistent interface）
	5.4. 言語の不連続性（Language discontinuity）
6. 暗闇に残される（Left in the dark） データ保護に関連する情報やコントロールを隠したり、データがどのように処理され、どのようなコントロールが可能なのかユーザにわからないままにするようにインターフェースが設計されている。	**6.1. 矛盾する情報**（Conflicting information）
	6.2. あいまいな表現や情報（Ambiguous wording or information）

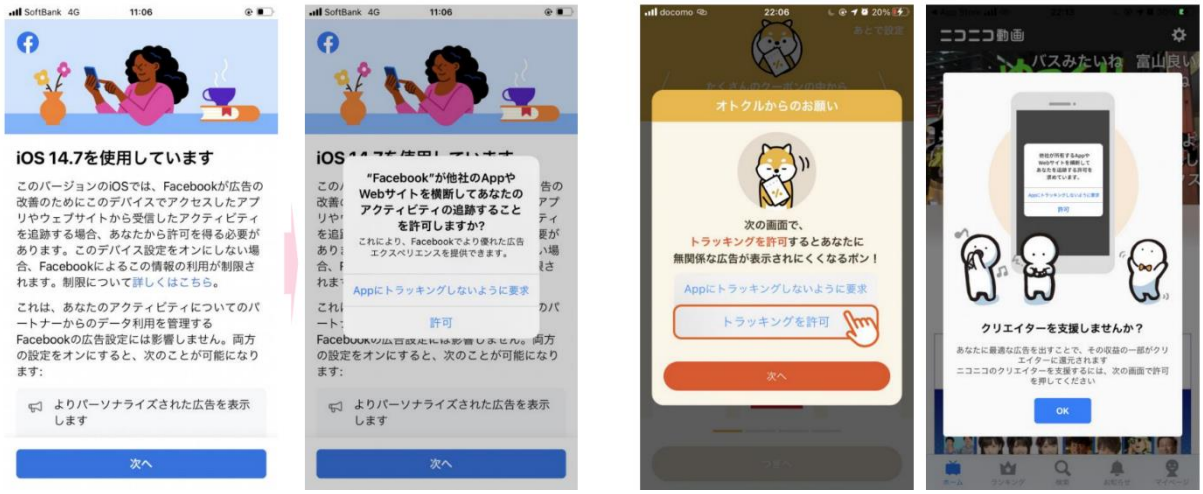
*1 EDPB, “Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them Version 2.0”

　ダークパターンとなっていることが疑われる事例としては、例えば、利用者情報の同意取得画面において同意ボタンのみが表示され、拒否ボタンが表示されない又は発見しにくい位置に表示されている例や、利用者に対し、利用者情報の取得に同意することによるメリットのみを強調した説明を行っている例が挙げられる。

（第２回株式会社マクロミル資料 P22）

問題となったGoogle同意取得ダイアログ

プレポップアップ　　ATTポップアップ　　当時、日経新聞が問題視したプレポップアップ



このような利用者情報の取扱いにおけるダークパターンについて、構成員からは以下のとおり意見があった。

（構成員からの意見）

・IDFA は利用者の同意を取っているものの、ダークパターンと見受けられるものがある印象である。どのようなものがダークパターンに当たるのか、SPI で例示しても良いのではないか。（第 1 回太田構成員）

・SPI において、ダークパターンまたは欺瞞的な行為の禁止を明確に示す必要があるのではないか。その上で、ダークパターンの判断の線引きは難しい面もあるが、具体的に例示が必要ではないか。さらに、法的根拠を与えるために、電気通信事業法で禁止する規定を追加しても良いのではないか。（第 3 回寺田構成員）

・ダークパターンとされる中でも欺瞞的なものを SPI の中で例示し禁止すべきだと思う。その上で、ダークパターンと同意の在り方についても整理が必要。Apple も Google もデータの収集や仕様に対して同意を必須としているが、アプリ利用開始時の規約同意で、すべてのデータ利用に対して同意をさせるというのは、欺瞞的なダークパターンと言え、非ログイン時のデータの取扱いについて、書いていない、どこに書いてあるか分からない、というようなものもダークパターンであると言えるのではないか、という観点でも検討し、SPI で方向性を示すべき。（第 3 回太田構成員）

・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

が、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良いと思ったところ。今の書き方だと、参考で何個か例が挙げられているけれども、この参考の中にも書いていないが、よく同意を促すようなもの、例えば、iPhone の ATT の同意を得るときに、本当はできるにもかかわらず、この同意をしてくれないと何とかできない。そういった掲載であるとか、本当は同意しなくても良いのに、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良いと思っている。（第７回太田構成員）

・SPI 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ところはあるが、景表法、特定商取引法、消費者契約法と様々な法令によりダークパターンに対する対応が進んでいるところ、この SPI の文書の趣旨から大きく外れず可能な範囲で言及していけると良い。（第７回呂構成員）

・SPI としてどのような手法に注意すべきかということも言及できると良い。令和 6 年版（令和 5 年度版）消費者白書では OECD の報告書を引用しつつ、具体的に気をつけるべき手法について図解を交えて注意喚起している。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表示する方法や、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方法等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、参照すると良いのではないか。（第７回呂構成員）

これを踏まえ、EDPB によ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ことが望ましい旨記載することとした。

② プロファイリングに係る対応

プロファイリングについては、EU の GDPR[2]及び DSA[3]において、一定の規律が実施されている。GDPR においては、プロファイリングを含む自動的な決定が存在すること等についてデータ主体へ情報提供をすることや、利用者はプロファイリングを含む個人データの取扱いに対し異議を述べる権利があること、デ

[2] GDPR 第４条（「プロファイリング」の定義）、第 21 条（異議を述べる権利）、第 22 条（プロファイリングを含む個人に対する自動化された意思決定）等
[3] DSA 第 26 条（オンラインプラットフォームでの広告）、第 28 条（未成年者のオンラインでの保護）、第 38 条（レコメンダーシステム）等

ータ主体に対して法的効果や重大な影響を及ぼす、プロファイリングを含む完全に自動化された意思決定は禁止されること等が規定されている。DSA においては、プロファイリングに基づく未成年者へのターゲティング広告の禁止や、特別なカテゴリーの個人データを使用したプロファイリングに基づくターゲティング広告の禁止等が規定されている。

**　このようなプロファイリングの在り方について、構成員からは以下のとおり意見があった。**

（構成員からの意見）

・プロファイリングそのものが問題というわけではないが、例えばどういったプロファイリングをしてはいけないのか等、例示する必要があるのではないか。（第１回寺田構成員）

・プロファイリングの在り方については、GDPR は上乗せの規定があり、その点視野に入れるべき。（第１回生貝主査代理）

・プロファイリングについて、利用目的の特定・明示のところに書かれているので、これも場所が違うかもしれないが、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、それはそのとおりだと思うが、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明示させるべきではないか。（第７回森構成員）

・プロファイリングをする・しないについては書いていると思うが、何を生成しているのか、生成する情報にはライトなものもディープなものもあると思うので、その生成される項目を記載するべきではないかという意見だと理解している。要配慮情報は反映しているが、それ以外のものについても書くべきではないかということだと受け止めている。一方、ここは、事業者への御負担というところでも、大きな問題、大きなお話にもなってくると思うので、コンセンサスを取ったほうがよい。（第７回山本主査）

・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を、事前のヒアリングでも話をした。脚注 15 に、決定を行う場合の対応が記載されており、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。（第７回生貝主査代理）

・地域のプロファイリング程度であればよくても、その地域に住む人はこういう傾向である等、プロファイリングの結果を基にさらなるプロファイリングがなされることもある。要は、プロファイリングした結果、どういうものに、どういう情報になり、それが何に使われるのかというところが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ところが、セットで見られると良いと思う。（第７回太田構成員）

・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というのはあるが、それ以外の安全と思わ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かということはいく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出すのは必要であるが、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ないということを大前提にするべきと思っている。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。（第７回寺田構成員）

・マーケティング目的といっても、政治広告にも販売されており、デモグラフィック情報も様々なものがある。例えば特定の地区等をプロファイリングすると、問題があるかもしれない。サイコグラフィック情報でも、例えばアウトドア派等というのもサイコグラフィックだと思うが、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う。逆に「怒りに流される」だと問題があるだろう。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にくいところ、どういう項目でプロファイリングするのかをまずは教えてもらうというのは良いのではないか。（第７回森構成員）

・項目がいくつぐらいあるのかというか、あるいは、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、ベストプラクティスなので、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、その辺りをいろいろと確認すべきことがあるという印象がある。（第７回山本主査）

・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ところでいくと、Google のプライバシーサンドボックスでも三百数十で、多いところは数万ある。これを全部というのは現実的ではないと思う。（第７回寺田構成員）

・米国のアドテクでは、自分がどういうセグメントに属しているかを表示する

ページを作っており、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、海外でも事例はあるので、そういった形が良いと思う。（第７回太田構成員）

これを踏まえ、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記載することとした。

なお、一部の構成員から、プロファイリングにより予測・生成される情報を明示するべきとの意見もあったところ、当該取組は、利用者に対する透明性の確保に資する取組であると考えられる一方、利用者のセグメントの種類は多数に及び、その実現性には懸念があること等を踏まえ、この点については、民間事業者においては、プロファイリングにより自身がどのように分類されているかについて利用者が確認できる仕組みを提供している例があることを踏まえ、そのような取組は利用者情報の取扱いの予測・想定に資するものであると考えられる旨、記載することとした。

（４）民間の取組を踏まえた対応

① センシティブ情報への配慮及びこども等の利用者情報の保護

センシティブ情報の取扱いについても、GDPR[4]及びDSA[5]において一定の規律がなされている。GDPRにおいては、民族、信条、健康に関するデータ等の特別カテゴリーに属する個人データの取扱いは原則として禁止しており、取り扱う場合にはデータ主体の明確な同意を取得することが求められている。また、DSAにおいては、GDPRの特別カテゴリーに属する個人データに基づくプロファイリングを行うことでターゲティング広告を表示することが禁止されている。

こどもの利用者情報の取扱いについては、第１章３．において記載したとおり、欧州のDSA[6]、英国のChildren's Code[7]、米国のCOPPA[8]等の諸外国法令に

[4] GDPR第９条（特別な種類の個人データの取扱いの禁止）
[5] DSA第26条（オンラインプラットフォームでの広告）
[6] DSA第28条（未成年者のオンラインでの保護）
[7] 英国の情報コミッショナーオフィス（ICO: Information Commissioner's Office）によりインターネット上のこどものデータ保護のために制定された15の行動規範（2021年９月施行）。
[8] Children's Online Privacy Protection Actの略。米国連邦取引委員会（Federal Trade Commission: FTC）の提言により、オンライン上のこどもの個人情報が保護者の管理下で安全に保たれることを目的に制定（2000年４月施行）。

おいて、その保護に関する規定がなされている。

これらの情報については、諸外国の法令において規律されているほか、民間事業者においては、以下のような対応が見受けられる。

（第３回日本総研発表資料Ｐ８特定の条件に該当するアプリに対する規約）

項目		Google （デベロッパープログラムポリシー、Play Consoleヘルプより抜粋）	Apple （App Reviewガイドラインより抜粋）
子ども（※1）を対象とする場合	法の遵守	• 法律・規制の遵守義務（※2）	• 法律・規制の遵守義務（※2）
	データ収集等の制限	• 子どものデータ収集にあたり情報を開示する義務（※3） • 子どものユーザだけを対象とする場合、位置情報の収集・共有等を禁止等	• 法律に準拠する目的のみでの生年月日や保護者の連絡先の要求許可
	広告掲載	• GooglePlayポリシーへの準拠を自己認定（Googleがリスト公開）している広告SDKバージョンのみ使用可能	• サードパーティ製の分析・広告機能の禁止
	プライバシーポリシー	記載なし	• プライバシーポリシーの設置義務（※5）
特定のデータを扱う場合	健康・フィットネス・医療データ	◆2024年5月31日発効予定 • プライバシー、詐欺、デバイスの不正使用に関するポリシーに準拠する義務 • アプリ内へのプライバシーポリシーの掲載義務 • アプリのコア機能と健康関連データの収集との関連性をユーザーに明確に示す義務 • アプリのコア機能の実行に必要のない、危険な権限を削除する義務	• 広告、マーケティング目的等で、使用・共有の禁止 • 虚偽データが書き込まれないよう配慮する義務 • 健康に関する臨床調査を実施するアプリでは、参加者本人、未成年の場合は親または保護者から同意を得る義務/独立した倫理審査委員会の適切な承認を得る必要
	位置情報データ	（アプリを通じて取得したデータの収集・使用・共有の目的はアプリ機能の提供や改善に直接関係するもの限定）（※4）	• アプリの機能またはサービスと直接関連する場合のみに利用限定
	その他データ公開の禁止例	• 個人の財務情報・支払い情報・政府発行の個人識別番号 • （未許可での）非公開の電話帳や連絡先情報	記載なし

このようなセンシティブ情報及びこども等の利用者情報の在り方について、事業者及び構成員からは以下のとおり意見があった。

（構成員からの意見）

・日本の個人情報保護法制では青少年について特別な規定が置かれていないが、青少年や脆弱な個人の保護、要配慮個人情報の取扱いについて、ソフトロー面で考えていく必要があるのではないか。（第１回生貝主査代理）

・アプリケーションが健康・フィットネス・医療データを取得する場合には、アプリ内にプライバシーポリシーを掲載することや、当該データの収集とアプリケーションの中心的な機能との関連性について、利用者に対して明確に示すことを義務化。（第５回 Google 提出資料）

これを踏まえ、センシティブ情報の取得時には本人の同意を取得することや、プロファイリングによりセンシティブ情報を予測・生成する行為は原則として実施せず、実施する場合には本人の同意を取得することが望ましい旨記載するとともに、こどもの利用者情報を取得する場合には、事前に法定代理人か

ら同意取得を行うことや、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は実施しないことが望ましい旨記載することとした。

② 必要最小限の利用者情報の取得

GDPR[9]では、個人データの取扱いに当たり、その利用目的との関係において、十分であり、関連性があり、かつ必要のあるものに限定されなければならないこととされている。この点、アプリケーションストア運営事業者においては、アプリケーション提供事業者に対し、必要最低限のデータ取得とすることを義務付ける等の取組が行われている。

（第３回日本総研発表資料Ｐ７）

項目		Google （デベロッパープログラムポリシーより抜粋）	Apple （App Reviewガイドラインより抜粋）
データの収集・保存	ユーザからの同意取得義務	必須	必須 （簡単な同意撤回オプション付加義務あり）
	必要最低限のデータ取得義務	必須	必須
	必要最低限のアカウントログイン義務	記載なし	必須
	アカウント削除要件	必須	必須
	その他（一部）	◆個人情報や機密情報が必要になることをユーザが合理的に予測できない可能性がある場合、データの収集、使用、共有について、アプリ内で開示し、直後に同意をリクエストする義務	◆アプリを利用してユーザのパスワード等プライベートデータを密かに取得することの禁止 ◆SafariViewController（Apple指定UI）の使用義務 ◆ユーザ以外のソースから取得したまたは未同意の個人情報を収集するアプリの禁止
データの使用・共有	事前にユーザ許可取得の義務	必須	必須
	目的外利用の禁止	必須 （ユーザーが合理的に予期する目的に適合するアプリとサービスの機能、およびポリシーにのみ許可する）	必須
	その他（一部）	◆特定の操作における個人情報と機密情報へのアクセスに関する制限（表形式の要件）	◆未許可のユーザプロファイル構築禁止 ◆分析や広告目的でユーザのデバイスにインストールされている他アプリの情報収集の禁止

これを踏まえ、アプリケーションの主要な機能に関係する機能のみにアクセスする等、利用者情報の取扱いはその利用目的との関係において最小限の範囲とすることが望ましい旨、記載することとした。

③ 同意の撤回方法のプライバシーポリシーへの記載

GDPR[10]では、同意の要件として、データ主体がいつでも容易に同意の撤回をすることができる権利を有することが定められている。この点、OS 提供事業者においては、アプリケーション提供事業者に対し、同意を無効にする方法をプライバシーポリシーに記載することを義務付けている例が見られる。

[9] GDPR 第５条（個人データの取扱いと関連する基本原則）
[10] GDPR 第７条（同意の要件）

（第３回日本総研発表資料Ｐ5）

項目			Google（デベロッパープログラムポリシーより抜粋）	Apple（App Reviewガイドラインより抜粋）
プライバシーポリシー	対象		すべてのアプリ	すべてのアプリ
	設置義務		あり（2022年7月より義務化）	あり（2018年10月より義務化）
	記載場所		Google Playの各アプリページとアプリ内の両方	App Storeの各アプリページと各アプリ内の両方
	必須記載項目	収集するデータの種類	必須	必須
		データの収集方法	必須	必須
		収集するデータの用途	必須	必須
		共有するデータと共有先	必須	必須
		データ保存/削除のポリシー	必須	必須
		その他	◆アプリの主体を明記、もしくはアプリ名を明記 ◆連絡先または問合せ方法 ◆ユーザの個人情報や機密情報を安全に処理するための手順	◆ユーザが同意を無効にする方法やユーザデータの削除をリクエストする方法

これを踏まえ、簡単にアクセスでき、かつ分かりやすい方法で同意の撤回でできる機会を提供し、またその方法についてプライバシーポリシーに記載することが望ましい旨、記載することとした。

④ 事業者横断的なトラッキングに係る対応及び位置情報や写真データ等の適正な取扱い

EU の ePrivacy 指令[11]においては、利用者の端末に保存されている情報にアクセスする場合には、データ主体から事前の同意を取得することが規定されている。この点、民間事業者においては、利用者の端末の広告 ID を取得することにより事業者横断的なトラッキングを実施する場合や、位置情報及び写真データへのアクセスを行う場合に、ポップアップ表示を行うこと等により、利用者からの同意を取得する取組が見受けられる。

[11] ePrivacy 指令第５条第３項（ユーザの端末機器情報の保護）

（第３回日本総研発表資料 P22、P25）

【Apple】

【Google】

このような事業者横断的なトラッキングの実施や、位置情報及び写真データ等の取扱いの在り方について、事業者及び構成員からは以下のとおり意見があった。

・アプリケーションは事前の同意なしにユーザや端末に係るデータを収集してはならず、同意の取消にも速やかに対応すべきこととしている。（第５回 Apple 発表）

・アプリケーションによるユーザのトラッキングはユーザによる許諾を必要とすることとしており、許諾を得るための標準的なポップアップ表示を提供している。（第５回 Apple 発表）

・アプリケーションが位置情報にアクセスする場合には、ポップアップ表示によりユーザの同意を取得することとしており、また提供する位置情報の頻度や粒度を選択できるようにしている。（第５回 Apple 発表）

・アプリケーションが写真データにアクセスする場合には、ユーザの同意を取得するとともに、アクセス範囲を一部に限定することができることとしている。（第５回 Apple 発表）

・プライバシーの保護レベルについて、Apple や Google のプライバシーポリシーや iPhone における ATT 等をデファクトスタンダードとしてベンチマークにするべき。モバイルエコシステムに関する検討が進んでいるが、プライバシーやセキュリティのための事業者の取組がベンダとの関係で競争阻害的であるという指摘がなされているところ、どのようなレベルが不当であるのか、今後議論になるのではないかと思う。iPhone における保護レベルが切

り下げられることがないようにするべき。（第１回森構成員）

これを踏まえ、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場合には同意取得を行うことや、位置情報や写真データ等にアクセスする場合には、同意取得を行うとともにアクセス範囲の限定等の設定を可能とすることが望ましい旨記載することとした。

⑤ 取得情報や利用目的の概要の分かりやすい掲示

スマートフォン利用者情報取扱指針においては、アプリケーションによる情報の取得等について明確かつ適切に定めたプライバシーポリシーを公表することが望ましいこととしている。また、その運用においては、プライバシーポリシーの分かりやすい概要を作成し、利用者が容易に参照できる場所に掲示することが望ましいこととしている。

この点、民間事業者においては以下のような取組が行われている旨、説明があった。

・アプリケーションがユーザや端末に係るデータを収集・利用等することについて説明したプライバシーポリシーを公表することを義務付けるとともに、収集するデータや利用目的の概要をアイコンとともに示したプライバシーニュートリションラベルへの記入を義務化。（第５回 Apple 発表）

・プライバシーポリシーの設置を義務化するとともに、アプリストアの個別ページ内に「データセーフティセクション」を設け、アイコン等で収集しているデータの内容や共有方針を記載することを義務化。（第５回 Google 提出資料）

・プライバシーポリシーの概要版の掲載が浸透していないところ、利用者にとって分かりやすく容易に理解できる環境を整えることが重要ではないか。（第１回日本総研発表）

（第３回日本総研発表資料 P19、P24）

（第３回日本総研発表資料Ｐ６アプリ紹介ページについて）

項目		Google （デベロッパープログラムポリシーより抜粋（※1））	Apple （App Reviewガイドラインより抜粋（※2））
対象		すべてのアプリ	すべてのアプリ
公開義務化		2022年7月	2020年12月
表示場所		Google Playの各アプリページ	App Storeの各アプリページ
記載が必要な情報	収集するデータの種類	デベロッパまたはサードパーティパートナーが収集するデータ全て	デベロッパまたはサードパーティパートナーが収集するデータ全て
	収集するデータの用途	必須	必須
	ユーザに紐づけられるデータ	記載なし	**必須**
	ユーザのトラッキングを行うデータ	記載なし	**必須**
	プライバシーポリシー	必須	必須
	その他（抜粋）	（任意）独立したセキュリティ審査を受けた申告 （子どもを対象とするアプリの場合必須）GooglePlayのファミリーポリシーに準拠していることを表示	（任意）プライバシー選択；アプリのプライバシー設定のオプションや管理方法をユーザーが詳しく確認できる一般公開URL（ユーザーが子どもかどうかなど条件に応じてデータ収集の方針が異なるといった情報を含む）

これらを踏まえ、プライバシーポリシーを利用者に分かりやすく示す方法として、その記載事項の概要について、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方法が考えられる旨、記載することとした。

（５）セキュリティ

2024 年２月より、総務省において、セキュリティ分野の有識者で構成される「サイバーセキュリティタスクフォース」の下に「ICT サイバーセキュリティ政策分科会」が設置され、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が検討されている。同分科会において、スマートフォンアプリにおけるセキュリティを確保していく上での課題等について議論されたところ、関係団体からは以下のとおり意見があった。

・スマホアプリにおけるサイバー脅威は、「スマホアプリの脆弱性（セキュリティホール)」と「不正アプリ（マルウェア)」の２つの観点で考える必要があり、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。アプリ開発者及びアプリストアは、アプリを提供する際のセキュリティ確保において大きな役割を担っている。(第１回分科会　一般社団法人日本スマートフォンセキュリティ協会発表)

・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が必要。ただし、アプリ診断のみでは十分ではなく、アプリのセキュリティやプライバシーの状態を改善するためには、セキュア設計・開発ガイド（アプリのセキュリティ要件やリスク分析、セキュアコーディングの指針、セキュリティテストの方法等をまとめたもの）のサポートが必要。(第５回分科会　OWASP (The Open Web Application Security Project))

さらに、本ワーキンググループにおいて、KDDI 株式会社から、令和５年度「通信アプリに含まれうる不正機能の検証に関する実証」について説明があった。本事業では、国内解析事業者の解析能力の水準の把握や、アプリにおける利用者情報の取扱慣行等を整理するため、代表的なアプリに対して実際に技術的解析（スクリーニング解析、表層解析、詳細解析）を実施するとともに、利用者の意図しない利用者情報の取扱いの実態や諸外国におけるスマートフォンアプリ規制動向に係る文献調査を実施し、その結果を踏まえ、以下のような意見があった。

・ 利用者情報の保護のためには、アプリ開発者のみならず、アプリストア運営者等の関係者も含めて、適切な対応を取ることが重要である。現行の SPI では、プライバシーの観点から関係者が遵守すべき方向性を示しているが、脆弱性があるアプリや不正なアプリにおける利用者情報の取扱い等に係るセキュリティの観点は明示的に含まれていない。英国の DSIT の「Code of practice for app store operators and app developers」も参考に、セキュリティの観点から、脆弱性があるアプリへの対応等を SPI に盛り込むことが望

ましいと考えられる。なお、その際、日本スマートフォンセキュリティ協会（JSSEC）が策定した「スマートフォンアプリケーション開発者の実施規範（第一版）(2024 年 3 月 8 日）も参考にすることが望ましい。(第 7 回 KDDI 株式会社）

以上に関し、構成員からは以下のとおり意見があった。

（構成員からの意見）

・まさにアプリに関しては、プライバシーとサイバーセキュリティは一体で論じていかなければならない。セキュリティにしっかり取り組んでいくことは大変望ましいこと。(第 7 回生貝主査代理）

・ SPI にセキュリティを加えるのは大変良いこと。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るので、可能な限りこのように１カ所にまとめると良い。(第 7 回寺田構成員）

・ 「セキュリティ・バイ・デザイン」という言葉は、基本原則として広く流通するものとするのが良い。(第 7 回生貝主査代理）

これらを踏まえ、基本原則にセキュリティ・バイ・デザインを記載するとともに、アプリケーション提供者や情報収集モジュール提供者において、セキュリティ・バイ・デザインや脆弱性があるアプリへの対応を実施することが望ましいこと、アプリストア運営事業者等において、アプリストアとしての基本的対応、脆弱性があるアプリへの対応、不正なアプリへの対応、アプリ削除・掲載拒否時の対応を実施することが望ましいこと等について記載することとした。

第３章　　今後の課題

本ワーキンググループの検討においては、第２章で記載したとおりスマートフォン利用者情報取扱指針の改定事項について議論があったほか、以下の事項については、今後の課題として引き続き検討を行うべきとされた。

①　対象スコープ（デバイス）

スマートフォン利用者情報取扱指針は、スマートフォン上のアプリケーションに関する利用者情報の取扱いについて、関係事業者において対応することが望ましい事項を記載したものであるところ、その対象とするデバイスの範囲について、構成員から以下のとおり意見があった。

（構成員からの意見）

・タブレットやスマートウォッチ、スマート家電、コネクテッドカー等、スマホ以外のデバイスを対象にする必要はないか。そのまま SPI を対応させることは難しいかもしれないが、例えばスマホと違いがあるのか、どのような点が共通しているか、調査検討する必要があるのではないか。（第 1 回寺田構成員）

（対応の方向性）

まずは、対象範囲はスマートフォンとしつつ、スマートフォンとそれ以外のデバイスにおける利用者情報の取扱いについて、どのような点が共通し、又は異なるか等について調査等を行った上で、次回以降の改定の際に議論することが適当である。

②　対象スコープ（ウェブサイト）

スマートフォン利用者情報取扱指針は、スマートフォン上の利用者情報の取扱いのうち、アプリケーションにおける望ましい対応について記載したものであるところ、ウェブサイトを通じて取得される利用者情報の取扱いについて、構成員及びオブザーバから以下のとおり意見があった。

（構成員からの意見）

・今回の改定案について、「本指針はブラウザを通じて利用者情報を取得する場合にも適用される」と明記しているため、今後、ウェブサイトに関しても、関係事業者において本指針に記載の取組が実施されることを希望する

（第８回木村構成員）

・外部送信規律においてもアプリケーションとウェブサイトに対する規律に差異はなく、JIAA 様が策定しているガイドラインにおいても両者について特段差異を設けていないことから、ウェブサイトも SPI の対象に含めるべきことは明らか。また、法令から一歩進んだレベルを目指すべきであるという意見も踏まえれば、アプリケーションに限定すべきではない。一方、ウェブサイト運営者に対する十分な説明が必要であるという点は JIAA 様の指摘のとおりであり、次回改定時には、ウェブサイトも対象に含めることを念頭に、啓蒙活動を推進していくべき。（第８回太田構成員）

・SPI の適用対象をアプリケーションに限定する修正は適当ではなく、ウェブサイトも適用対象とすべき。この問題は外部送信規律を規定した令和 4 年電気通信事業法改正の際にも十分な議論がなされたもの。同改正では、電気通信事業者及び三号事業者に対して外部送信に係る通知・公表の義務が課せられたことは、外部送信に係る透明性の確保の強い必要性が認識されたことによるものである。法の適用対象が電気通信事業者等に限定されたことは、電気通信事業法の適用範囲に由来するものであり、電気通信事業者等とそれ以外の主体が行う外部送信にその性質に違いはなく、外部送信に係る透明性の確保の必要性にも違いはない。ウェブサイトに係る外部送信を原則オプトインとする諸外国の立法例もある現状において、通知・公表がベストプラクティスでないとしてしまうことには違和感がある。（第８回森構成員）

（オブザーバからの意見）

・「アプリケーション等」の定義が「アプリケーション及びウェブサイトの総称」となっている点について、アプリケーション内のブラウザが表示するウェブサイトが含まれることに異存はないが、ウェブサイト全般が対象になることについては、アプリケーションとウェブサイトの差異に関する調査や関係者等へのヒアリング、ウェブサイト運営者に対する十分な説明を行った上で検討すべき。（第８回 JIAA 柳田オブザーバ）

（対応の方向性）

まずは、対象範囲はアプリケーションとしつつ、アプリケーションとウェブサイトとで取得する利用者情報の取扱いに差異があるか等について調査等を行い、関係事業者やウェブサイト運営者に対する説明やヒアリング等の必要な対応を行った上で、次回以降の改定において、ウェブサイトを対象とするべきか、改めて検討することが適当である。

おわりに

本ワーキンググループにおいては、直近で 2017 年に改定されたスマートフォン利用者情報取扱指針について、電気通信事業法における外部送信規律の導入や情報収集モジュール等の利用者情報を巡る情勢変化を踏まえ、国内外の制度、民間の取組等を踏まえた見直しについて検討を行い、その改定案について取りまとめを行った。本報告書の内容及び改定後のスマートフォン利用者情報取扱指針を踏まえ、各関係者において、それぞれ必要な対応が行われることが期待される。

スマートフォンにおけるイノベーションの変化の速度は速く、プラットフォーム事業者やアプリケーション提供者を取り巻く環境も大きく変化していくことが想定される。そのような中、スマートフォンアプリケーションの利用者情報が適正に取扱われ、利用者がスマートフォンやそれを通じて提供される利便性の高いサービスを安全・安心に利用できる環境を確保していくためには、総務省において、国内外の制度の動向について適切に把握するとともに、アプリケーション提供事業者をはじめとする関係事業者の取組状況について確認し、スマートフォン利用者情報取扱指針の見直しを適時適切に検討することが適当である。また、第３章において記載した今後の課題については、対応の方向性として示した事項について、速やかに検討を行うことが適当である。

別添

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・抜粋）

利用者情報に関するワーキンググループ

令和６年〇月〇日

1. スマートフォン利用者情報・セキュリティ取扱指針

（前文）

情報通信インフラとしてスマートフォンが急速に普及した中で、スマートフォン利用者のリテラシーのレベルの多様化が進んでいる。利用者に一定の自己責任が求められるとしても、利用者の不安を解消し、利用者が安全にスマートフォンを利用できるようにするためには、スマートフォンにおける利用者情報を利活用する関係事業者等が責任を持って、利用者情報の適正な取扱いに努める必要がある。具体的には、当該関係事業者等が個人情報保護やプライバシー保護の観点から利用者情報を適正に取り扱うとともに、利用者に分かりやすい説明を行い、利用者の理解及びそれを踏まえた選択を促すことが求められる。

本指針は、法令上義務付けられてはいないものの、スマートフォンにおける利用者情報を取り扱う上で実施することが望ましいと考えられる事項について、国内の関係法令[1]や諸外国の制度の動向、民間事業者における取組等を参考に取りまとめたものである。スマートフォンを巡っては、新たな技術・サービスが次々と出現し、利用者情報の適正な取扱いの観点から、今後新たな課題が生じることも考えられることから、本指針は随時見直しを行うこととする。

また、スマートフォンのサービス構造において、多様な関係事業者等がサービス提供や利用者情報の取扱いに関わっており、本指針の目的を達成する上で、利用者情報を取得する事業者等のみでは対応できる範囲が限られる場合があるため、アプリストア運営者・OS提供事業者等の関係事業者等も連携し対応していくことが重要である。

[1] 直近では、個人情報の保護に関する法律等の一部を改正する法律（令和２年法律第 44 号）により不適正利用の禁止や外国第三者提供時の情報提供の充実化等が規定されたほか、電気通信事業法の一部を改正する法律（令和４年法律第 70 号）により、特定利用者情報規律及び外部送信規律が導入されている。

1.1. 総則

1.1.1. 目的

- 本指針は、スマートフォンアプリケーションの利用者情報の適正な取扱いに関し、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）、プライバシーに関する判決、電気通信事業法（昭和 59 年法律第 86 号）、その他の関係法令等の趣旨を取り入れつつ、諸外国における制度の動向や、民間事業者におけるプライバシー保護に係る取組等も踏まえながら、スマートフォンアプリケーションに係る関係事業者等が取り組むことが望ましい基本的事項を定めたものである[2]。本指針自体が法的拘束力を持つものではないが、関係事業者等がこれらの事項に取り組むことにより、次に掲げる事項を達成し、もって、スマートフォンにおけるイノベーションの継続的な創出や市場の中長期的な成長を促進し、利用者がスマートフォンやそれを通じて提供される利便性の高いサービスを安全・安心に利用できる環境を整備することを目的とする。
    ① 関係事業者等による関係法令等の遵守に資すること
    ② 利用者が自らの利用者情報の取扱いに関する情報を十分に得て、アプリケーションの利用に関し適切に判断し、行動することを支援すること

1.1.2. 定義

① 利用者情報

- 利用者の識別に係る情報、利用者の通信サービス上の行動履歴に関する情報、利用者の状態に関する情報等、スマートフォンにおいてスマートフォンの利用者の情報と結びついた形で生成、利用又は蓄積されている情報（電話帳等の第三者に関する情報を含む。）の総称。個人情報保護法における個人情報や、電気通信事業法における特定利用者情報を含む[3]。

（参考）

[2] 本指針は、スマートフォン上のアプリケーションについて関係事業者が取り組むことが望ましい事項を定めたものであるが、ウェブサイトにおいて同様の利用者情報の取扱いが生じる場合があり、その関係事業者は本指針に定める事項を参考に対応を図ることが考えられる。

[3] 本指針は、利用者情報一般の適正な取扱いに関し、関係事業者が取り組むことが望ましい基本的事項を定めたものであり、本指針自体が法的拘束力を有するものではないが、個人情報保護法や電気通信事業法が適用される場合には、両法に従い対応する必要がある。

No.	情報の種類	具体例	適用される規律
(1)	通信の秘密に該当する情報で、個人情報でないもの	・電気通信役務の利用者である個人の通信の内容(特定の個人を識別することができるものを除く。) ・電気通信役務の利用者である法人の通信履歴	電気通信事業法
(2)	通信の秘密に該当する情報で、個人情報であるもの	・電気通信役務の利用者である個人の通信履歴(特定の個人を識別することができるものに限る。)	電気通信事業法 ＋個人情報保護法
(3)	電気通信事業法第27条の5第2号の情報で、個人情報でないもの	・電気通信役務の登録者を識別できるIDで、個別の通信に紐付かないもの(特定の個人を識別することができるものを除く。) ・電気通信役務の契約者データベースにある法人契約者名	電気通信事業法 【←令和4年改正法により追加】
(4)	電気通信事業法第27条の5第2号の情報で、個人情報であるもの	・電気通信役務の契約者データベースに含まれる契約者の登録情報(特定の個人を識別することができるものに限る。)	電気通信事業法 【←令和4年改正法により追加】 ＋個人情報保護法
(5)	電気通信事業法第27条の5第2号の情報でもなく、通信の秘密に該当する情報でもない、個人情報	・店頭で電気通信役務の利用者に対して行ったアンケートに記入された情報(氏名・住所等により分類整理されていないもの。特定の個人を識別することができるものに限る。)	個人情報保護法

なお、「具体例」欄に示している内容は、あくまでも一例であって、網羅的なものではありません。

② OS

- コンピュータシステム全体を管理するソフトウェアで、基本的な機能を提供するもの。

③ アプリケーション

- 通話やEメール等のコミュニケーションツール、ブラウザ、写真、ゲーム等の様々な機能をスマートフォンで実行するための利用者向けソフトウェア(OS を除く)。

④ アプリケーション提供者

- アプリケーションを提供する事業者又は個人。

⑤ アプリストア

- アプリケーションを提供するストアのことで、利用者はこのストアからアプリケーションをダウンロードする。

⑥ 情報収集モジュール[4]

- アプリケーションに組み込んで利用される一連のプログラムであって、利用者情報を取得するための機能を持つものをいう。

⑦ 情報収集モジュール提供者

- アプリケーション提供者に対し、情報収集モジュールを提供する事業者（当該事業者がアプリケーション提供者に当たる場合を除く。）。

⑧ アプリケーション提供者等

- アプリケーション提供者及び情報収集モジュール提供者の総称。

⑨ 関係事業者等

- スマートフォンをめぐるサービス提供に関係している事業者等。具体的には、アプリケーション提供者、情報収集モジュール提供者、アプリストア運営事業者、OS 提供事業者、移動体通信事業者、端末製造事業者、その他関係しうる事業者等（アプリケーション紹介サイト運営者、広告関係事業者等）のこと。

⑩ プライバシーポリシー

- 関係事業者等が個人情報保護又はプライバシー保護を推進する上での考え方や方針を明らかにする文書[5]。本指針においては、スマートフォンにおいて提供されるアプリケーションや情報収集モジュールについて、具体的な取得情報の項目、利用目的等を記載したものを想定している[6]。

⑪ 通知又は公表

- 「通知」は、書面（郵送等）、電子メール、口頭（電話等）等のいずれかの方法で個別に伝えること。「公表」は、官報・公報・新聞紙等への掲載、インターネット上での公表、パンフレットの配布、窓口等への書面の掲示・備付等のいずれかの方法により公にしておくこと（スマートフォンの場合、通知は書面、電子メールやアプリによるポップアップ等、公表はアプリケーション上又はウェブサイト等へのリンクを張ること等により行うことが想定され

[4] これには、分析ツール、広告ネットワークを含む。
[5] 「プライバシーポリシー」の名称でなくても、利用者情報の取扱いに関する方針を含む。
[6] プライバシーポリシーについては、事業者単位で作成されるもの及びアプリケーション単位で作成されるものがあるところ、本指針においては、基本的にはアプリケーション単位で作成されるものを想定しているが、事業者単位で作成されるものも含まれる。

る。)。

⑫ 個別の情報に関する同意取得[7]

- アプリケーション(組み込まれた情報収集モジュールを含む。以下同じ。)により取得される個別の情報(電話帳、位置情報等)について、取得や取扱いについて独立した形で同意を取得すること。[8]

⑬ ダークパターン

- 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歪めたり損なったりする方法で、ユーザインタフェースを設計・構成・運営すること。

⑭ セキュリティ

- 「情報」と「機能」の両面において守るべき資産を脅威から保護すること。本指針においては、利用者情報へのアクセス管理等の対策によって利用者情報が利用者による同意の範囲内で適切に保護されている状態が達成されることや、スマートフォンの機能が利用者の操作やあらかじめの同意なく勝手に利用されてしまうことを防ぐこと。

【補足】

１．利用者情報の取得の有無による区別について

本指針の適用対象たるアプリケーション提供者及び情報収集モジュール提供者には、スマートフォンから利用者情報を自ら取得しない者も含まれる。これは、例えば、アプリケーション提供者がプライバシーポリシーを掲示等していない場合、アプリケーション提供者が利用者情報を取得していないためプライバシーポリシーを掲示等していないのか、利用者情報を取得しているにもかかわらずプライバシーポリシーを掲示等していないのかが不明であること、及び、アプリケーション提供者が利用者情報を取得しない場合であっても、情報収集モジュールにより利用者情報がスマートフォン外部に送信され情報収集モジュール提供者による取得となる場合があることなどに鑑み、利用者が自らの利用者情報の取扱いに関する情報を十分に得て、アプリケーションの利用に関し適切に判断し、行動することを支援するという本指針の趣旨に

[7] 同意取得の方法について、個人情報保護法においては、「事業の性質及び個人情報の取扱状況に応じ、本人が同意に係る判断を行うために必要と考えられる合理的かつ適切な方法によらなくてはならない」とされており（個人情報の保護に関する法律についてのガイドライン（通則編）（平成 28 年 11 月策定。令和５年 12 月一部改正　個人情報保護委員会。以下「ガイドライン通則編」という。）2-16 参照。）、事案に応じて適切な同意取得の方法を検討する必要がある。プライバシー上の懸念が生じうる情報に係る同意取得においても、同様に、情報の性質等に鑑み事案に応じた検討が必要となる。

[8] アプリケーションに係るプライバシーポリシー等に基づき、アプリケーションの利用者情報の取得や取扱いについて一括して同意を取得するアプリケーションに関する同意取得とは異なることに留意。

鑑みたためである。ただし、スマートフォンから利用者情報を自ら取得しない場合には、本指針の取得を前提とした箇所は、適用されない。

２．「取得」について

この指針の適用については、アプリケーション上において利用者本人が自ら利用者情報を提供するか、利用者情報が自動的にアプリケーションの外部に送信されるかにかかわらず、スマートフォン外部へのアプリケーション提供者等に対する利用者情報の送信があれば、通常、当該アプリケーション提供者等による取得があったといえる。

３．広告関係事業者について

広告関係事業者は、その事業形態にもよるが、アプリケーション提供者又は情報収集モジュール提供者に当たる場合が多いと考えられる。

４．アプリケーション内のブラウザを通じて取得される利用者情報について

スマートフォンの利用者情報については、アプリケーションの利用に伴い取得されるほか、当該アプリケーション内のブラウザでウェブサイトを利用する際に、当該アプリケーションの提供者により取得される場合があるため、本指針はアプリケーション内のブラウザを通じて利用者情報を取得する場合にも適用される。アプリケーション内のブラウザが表示するウェブサイトに Javascript タグ等を追加的に組み込むことで、利用者情報を取得する場合には、当該 Javascript タグ等についても、本指針における情報収集モジュールと同等に取扱うこととする。

1.1.3. 本指針の対象者

- 本指針は、アプリケーション提供者等を中心として、スマートフォン上の利用者情報の取扱いに係るあらゆる関係事業者等において、それぞれの役割に応じた形で適用されることを想定している。なお、アプリストア運営事業者、OS 提供事業者、移動体通信事業者、端末製造事業者、その他関係しうる事業者等がアプリケーション又は情報収集モジュールを提供し、利用者情報を直接取得する場合、当該事業者等は、アプリケーション提供者又は情報収集モジュール提供者に該当し、それぞれの取組みを行うものとする。

1.1.4. 基本原則

- スマートフォンにおける利用者情報の取扱いについて、アプリケーション提供者等は、次に掲げる基本原則に従うことが望ましい。

① 透明性の確保

- 利用者情報の取得・保存・利活用・第三者提供・消去及び利用者関与の手段の詳細について利用者に通知し、又は容易に知りうる状態に置く。利用者に通知又は公表あるいは利用者の同意を取得する場合、その方法は、利用者がアプリケーションを利用する際の方法等を考慮して利用者が容易に認識かつ理解できるものとする。

② 利用者関与の機会の確保

- その事業の特性に応じ、その取得する情報や利用目的、第三者提供の範囲等必要な事項につき、利用者に対し通知又は公表あるいは必要な場合には同意取得を行う。また、利用者情報の取得停止や利用停止等の利用者関与の手段を提供することととする。これらの利用者関与の機会の確保に当たっては、利用者が容易に理解できる方法で情報提供を行うこととする。

③ 適正な手段による取得の確保[9]・不適正利用の禁止

- 利用者情報を適正な手段により取得することとする。また、取得した利用者情報について、違法又は不当な行為を助長し、又は誘発するおそれがある方法で取り扱わないこととする。

④ 適切な安全管理の確保

- 取り扱う利用者情報の漏えい、滅失又はき損の防止その他の利用者情報の安全管理のために必要・適切な措置を講じることとする。

⑤ 苦情相談への対応体制の確保

- 利用者情報の取扱いに関する苦情相談に対し適切かつ迅速に対応することとする。

⑥ プライバシー・バイ・デザイン／セキュリティ・バイ・デザイン

- 開発時から、利用者の個人情報やプライバシーが尊重され保護されるようにあらかじめ設計することとする。利用者の個人情報やプライバシーに関する権利や期待を十分認識し、利用者の視点から、利用者が理解しやすいアプリケーションやサービス等の設計・開発を行うこととする。
- 開発時から、セキュリティが適切に確保されるよう、アプリケーションの企画及び設計の段階から、セキュリティの確保について検討し、適切な仕組みをアプリケーションに組み込

[9] 個人情報保護法上、「偽りその他不正手段」により個人情報を取得してはならないとされている（同法第 20 条第 1 項）。この点、「不正の手段」には、「偽り」のほかにも、不適法な又は適正性を欠く方法や手続も含まれ、具体的な判断については、事案ごとに同法その他の法令の趣旨や社会通念に委ねられると解されている（園部逸夫ほか『個人情報保護法の解説 第三次改訂版』（令和 4 年、ぎょうせい）161 頁）。

むこと。

⑦ 特定の情報及び利用者の属性に応じた配慮

- 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特定の情報について適切な配慮を行うとともに、利用者の属性に応じ必要な対応を行い情報を適正に取り扱うこととする。

【補足】

個人情報保護法における個人情報への該当性等について

個人情報保護法において「個人情報」とは、「生存する個人に関する情報（※）であって」、「当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）」（法第２条第１項第１号）、又は「個人識別符号が含まれるもの」（同項第２号）をいう。

※本欄では生存する利用者に関する情報を想定する。

【単体で特定の個人の識別性がある場合】

スマートフォンからアプリケーション提供者等が取得する利用者情報に特定の個人の識別性がある場合、個人情報となる。例えば、電話帳においては、一般的に氏名と組み合わせた電話番号及びメールアドレス等、特定の個人の識別が可能な情報が登録される場合が多く、一般的に電話帳を取得すると個人情報を含む内容を取得することになると考えられる。契約者情報も、一般的に、氏名と組み合わせた住所等を含み特定の個人の識別が可能であるため契約者情報を取得すると個人情報として取り扱う必要があると考えられる。

【他の情報と容易に照合でき、それによって特定の個人の識別性を獲得する場合】

また、スマートフォンからアプリケーション提供者等が取得する利用者情報単体でみた場合に特定の個人の識別性がない場合であっても、取得した者が有している情報等、他の情報と容易に照合し特定の個人の識別性を獲得する場合には個人情報となる。例えば、電話番号、メールアドレス、契約者・端末固有 ID、ログイン ID 等が情報単体では特定の個人の識別性がない場合でも、契約者の氏名等個人情報と容易に照合することができる場合には特定の個人の識別性を獲得する。

また、ログインのための識別情報は、通常、単なる数字や記号等、それ単体では特定の個人の識別性を有しない。

上記の各 ID のいずれについても、それ自体にアルファベットの氏名を含む場合等、特定の個人の識別性を有することがある。

【行動履歴や利用履歴に関する情報】

行動履歴や利用履歴に関する情報としては、GPS や基地局・Wi-Fi アクセスポイント情報に基づく位置情報、通信履歴（通話内容・履歴、メール内容・送受信内容等）、ウェブサイト上の行動履歴等が蓄積される場合がある。また、アプリケーションの利用により蓄積される情報やアプリケーションの利用ログ、システムの利用に関するログ等が蓄積されることもある。これらは、それ自体で一般には特定の個人の識別性を有しないことが多いと考えられるが、長期間網羅的に蓄積した場合等において、態様によって特定の個人を識別可能となる結果、個人情報に該当する場合もある。移動履歴は、短期間のものでも、自宅、職場等の情報と等価になる場合がある。また、大量かつ多様なこれらの履歴の集積については、個人の人格と密接に関係する可能性が指摘される。

【図表 1：スマートフォンにおける利用者情報の性質と種類】

区分	情報の種類	情報の種類	利用者による変更可能性	特定の個人の識別性等
第三者に関する情報	電 話 帳 で管理されるデータ	氏名、電話番号、メールアドレス等	×～△	電話帳には一般に氏名、電話番号等が登録されることが多く、特定の個人の識別性を有している場合が多い。
利用者の識別に係る情報	氏名、住所等の契約者情報	氏名、生年月日、住所、年齢、性別、電話番号等の情報や、クレジットカード番号等の個人信用情報等	×～△	契約者情報には一般に氏名、住所等が含まれており、特定の個人の識別性を有している場合が多い。
	ログインに必要な識別情報	各種サービスをネット上で提供するサイトにおいて、利用者を特定するためにログインさせる際に利用される識別情報	△～○ 利用者が必要に応じて変更・修正を行うことが可能	・ログインのための識別情報は変更可能な場合も有り。 ・ログインのための識別情報は、それ自体で氏名等、特定の個人の識別性を有する場合もある。単なる数字や記号等で単体では特定の個人の識別性を有さない場合もあるが、アプリケーション提供事業者等において他情報と容易に照合できる場合、特定の個人の識別性を有する。
	クッキー技術を用いて生成された識別情報	ウェブサイト訪問時、ブラウザを通じ一時的に PC に書込み記録されたデータ等	○ 利用者が必要に応じて消去することが可能	・利用者がブラウザ上で消去やオプトアウトを行うことが可能。 ・単体では特定の個人の識別性を有しないが、発行元等において他情報と照合し特定の個人の識別性を有する場合がある。
	契約者・端末固有 ID	OS が生成する ID（Android ID)、独自	×	・スマートフォンの OS やシステムプログラム、SIM

		端末識別番号（UDID）、加入者識別 ID（IMSI）、IC カード識別番号（ICCID）、端末識別 ID（IMEI）、MAC アドレス、Bluetooth Device Address 等	端末交換や契約変更をしない限り変更が困難	カード、端末そのもの等に割り振られ管理される。利用者は端末交換や契約変更をしない限り変更困難。 ・単体では特定の個人の識別性を有しないが、他の情報と容易に照合できる場合、特定の個人の識別性を獲得する可能性がある。 ・同一 ID に紐付けて行動履歴や位置情報を集積する場合、プライバシー上の懸念が指摘される。
	広告 ID	IDFA（Identifier For Advertisers）、AdID（Advertising ID）	○ 利用者が必要に応じて、許可・変更・修正を行うことが可能	・単体では特定の個人の識別性を有しない。他の情報と容易に照合できる場合、特定の個人の識別性を獲得する可能性がある。 ・利用者が OS 機能やその設定によって、各アプリケーションでのアクセスを個別にオプトイン又はオプトアウトすることが可能。
	ベンダーID	IDFV（Identifier for Vendor）、AppSetId	× オプトアウトの手段が提供されていないケースがある	・同じデバイス上で動作する同じベンダー（アプリケーション提供者）のアプリでは同じ値となる識別子。 ・単体では特定の個人の識別性を有しない。他の情報と容易に照合できる場合、特定の個人の識別性を獲得する可能性がある。
通信サービス上の行動履歴や利用者の状態に関する情報	通信履歴	通話内容・履歴、メール内容・送受信履歴	×～△ 端末や電気通信事業者のサーバーにおいて管理	・通信相手、記録の性質等により特定の個人の識別性を有する場合がある。 ・電気通信事業者の取扱い中のものは通信の秘密の保護の対象。 ・通信履歴はプライバシー上の懸念が指摘される。

	ウェブサイト上の行動履歴	利用者のウェブサイト上における閲覧履歴、購買履歴、検索履歴等の行動履歴	×～△ 端末やウェブサイト管理者、アプリケーション提供者等のサーバーにおいて管理	・利用者の行動履歴や状態に関する情報については、内容・利用目的等によりプライバシー上の懸念が指摘される。 ・蓄積された場合等、態様によって個人が推定可能になる可能性がある。
	アプリケーションの利用履歴等	アプリケーションの利用履歴・記録されたデータ等、システムの利用履歴等		
	位置情報	GPS 機器によって計測される位置情報、基地局に送信される位置登録情報、Wi-Fi ルータによって計測される位置情報、Bluetooth ビーコンによって計測される位置情報[10]		
	写真・動画等	スマートフォン等で撮影された写真、動画等		・内容、利用目的等によりプライバシー上の懸念がある。 ・個人が判別できる写真・動画等は、個人情報に該当する。

10 「位置情報プライバシーレポート」https://www.soumu.go.jp/main_content/000434727.pdf

外国事業者について　近年は外国事業者によるアプリケーションや情報収集モジュールの提供が多く行われている。この点について、個人情報保護法第 171 条においては、個人情報取扱事業者、仮名加工情報取扱事業者、匿名加工情報取扱事業者又は個人関連情報取扱事業者が、国内にある者に対する物品又は役務の提供に関連して、国内にある者を本人とする個人情報、当該個人情報として取得されることとなる個人関連情報又は当該個人情報を用いて作成された仮名加工情報若しくは匿名加工情報を、外国において取り扱う場合についても、適用することとされている。

また、利用規約等において、専属的合意管轄裁判所を外国裁判所とし、準拠法を外国法としている場合においても、消費者である利用者からの訴訟提起の際や、不法行為に基づく請求の際には、日本の裁判所に国際裁判管轄が認められ、準拠法を日本国法とされる可能性がある。

したがって、外国事業者であっても、我が国においてサービスを提供する場合には、本指針を参照すべきである。

1.2. アプリケーション提供者等における取組

（アプリケーション提供者及び情報収集モジュール提供者）

1.2.1. アプリケーション提供者の取組

≪期待される役割≫

- アプリケーション提供者は、利用者情報を取得する場合、自身の利用者情報の取扱いに責任を負っていると考えられる。
- アプリケーション提供者は、アプリケーションを提供する場合において、当該アプリケーションによる情報の取得等について明確かつ適切に定めたプライバシーポリシーを公表することが望ましい。
- アプリケーションに組み込む情報収集モジュールに関しても、自己の意思で組み込み、情報収集モジュールから利益を得ている場合もあることから、情報収集モジュールの組み込みにあたって上記の点に十分に配慮するとともに、情報収集モジュールの透明性の確保や利用者関与の機会を確保することができるよう、情報収集モジュール提供者と協力すること望ましい。
- 利用者情報を取得しないアプリケーション提供者においても、利用者に対し、利用者情報を取得していない旨等を、あらかじめ通知又は公表することが望ましく、また、そのアプリケーションに組み込まれた情報収集モジュールにより利用者情報の取得が行われる場合は、その旨をあらかじめ通知又は公表し、オプトアウトの機会を提供することが望ましい。

≪具体的な取組内容≫

1.2.1.1. プライバシーポリシーの作成[11]

- アプリケーション提供者は、個別のアプリケーションについて、以下の①から⑩までの事項について明示するプライバシーポリシーをアプリケーションごとに日本語であらかじめ作成し[12]、利用者が容易に参照できる場所に掲示又はリンクを張ることが望ましい。

① アプリケーション提供者の氏名又は名称及び連絡先等

- アプリケーション提供者の氏名又は名称及び連絡先等[13]を記載することが望ましい。

---

11 メッセージ媒介サービス、SNS、検索サービス、ホームページの運営等の対象となる電気通信役務を営んでいる電気通信事業者は、外部送信規律への対応が必要となる。詳細については、1.2.1.7.を参照すること。

12 一のプライバシーポリシーに、複数のアプリケーションについてまとめて記載する場合であって、アプリケーションごとに取得・利用する情報が異なる場合には、取得・利用する情報の内容や利用目的等について、アプリケーションごとに分けて記載することが望ましい。

13 個人情報を取り扱う場合は、氏名又は名称及び住所並びに法人にあっては、その代表者氏名

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

- アプリケーション提供者が利用者情報を取得する場合に、スマートフォン外部への送信等により取得する旨を記載するとともに、その取得する利用者情報の項目・内容を列挙することが望ましい[14][15]。また、アプリケーション提供者が利用者情報を取得しない場合は、その旨を記載することが望ましい。
- 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係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等、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。

③ アプリケーション提供者による取得方法

- アプリケーション提供者が利用者情報を取得する場合に、利用者の入力によるものか、アプリケーションがスマートフォン内部の情報を自動取得するものなのか等取得方法を明確に示すことが望ましい。

④ 利用目的の特定・明示

- アプリケーション提供者が利用者情報を取得する場合に、利用者情報を、アプリケーション自体の利用者に対するサービス提供（提供するサービス概要を簡単に記載する等）のために用いるのか、広告配信・表示やマーケティング目的のために取得するのか、それら以外の目的のために用いるのかを明確に記載することが望ましい。
  - アプリケーション自体が利用者に提供するサービス以外の目的のために利用する場合については、利用者が利用目的や利用方法を容易に想定できないことから、利用目的と取得する利用者情報の項目の関係について丁寧な説明を行うことが望ましい。
  - 広告配信・表示やマーケティング目的のために利用者情報の取得を行う場合には、適切にその目的を明示することが望ましい。利用者に対してターゲティング広告等の配信を行う場合にはその旨記載することが望ましい。
  - 利用者に関する行動・関心等の情報を分析するいわゆるプロファイリング[16]を行う場

[14] その際、利用者への影響が大きいと考えられるものから順に記載する等、利用者が理解しやすい方法で記載することが望ましい。
[15] 例えば、プロファイリングにより利用者を分類する場合において、利用者が本人の分類の状況を確認できるようにすることは、利用者情報の取扱いの予測・想定に資すると考えられる。
[16] GDPR では「自然人と関連する一定の個人的側面を評価するための、特に、当該自然人の業務遂行能力、経済状態、健康、個人的嗜好、興味関心、信頼性、行動、位置及び移動に関する側面を分析又は予測するため、個人データの利用によって構成されるあらゆる形式の個人データの自動的な取扱いを意味する。」（第４条）と定義されている。

合には、どのような取扱いが行われているかを利用者が予測・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[17]。

- 現段階では利用目的が明確ではなく、将来的な活用を見込んで利用目的の範囲を定めず様々な利用者情報を取得することは、必ずしも利用目的が特定されているとはいえないため、想定される利用目的の範囲をできるだけ特定し利用者に通知又は公表あるいは同意取得をした上で、その範囲で情報を取得し取り扱うことが望ましい。

⑤ 第三者提供、外国の第三者に対する提供、共同利用及び情報収集モジュールに関する記載事項

［第三者提供に関する記載事項］[18]

- アプリケーション提供者が取得した利用者情報を第三者提供する場合（第三者が当該情報にアクセスする権限を付与する場合を含む。）、第三者への提供を利用目的とすること及び第三者に提供される利用者情報の項目等を明確にプライバシーポリシーに記載することが望ましい。

［外国の第三者等に提供する場合の記載事項］[19][20]

- 外国にある第三者や委託先、共同利用相手へ利用者情報を提供する場合には、外国にある第三者等への提供を利用目的とすること、提供される利用者情報の項目及び提供先の第三者等の所在国の名称等をプライバシーポリシーに記載することが望ましい。

［共同利用する場合の記載事項］

- アプリケーション提供者が、特定の者と利用者情報を共同利用する場合には、①共同利

---

17 プロファイリング結果に基づき、利用者にとって重要な決定が自動的に行われることがある場合には、その旨や当該決定に至る際に依拠する基準等を明示することが望ましい。

18 アプリケーション提供者が取得した利用者情報を第三者提供する場合、あらかじめ本人の同意を取得することが適切である。ただし、本指針では具体的に取り扱わないが、オプトアウトによる第三者提供を否定するものではない。なお、個人データの第三者提供に該当する場合には、個人情報保護法に基づき、原則としてあらかじめ本人の同意を取得しなければならない（同法第 27 条第 1 項）。

19 個人データに該当する利用者情報を外国（個人情報の保護に関する法律施行規則（平成 28 年個人情報保護委員会規則第 3 号。以下「個人情報保護委員会規則」という。）で定める外国を除く。）にある第三者（同規則第 16 条で定める基準に適合する体制を整備している者を除く。）に提供する場合、個人情報保護法により、原則として、提供先の第三者の所在国における個人情報の保護に関する制度、当該第三者が講ずる個人情報の保護のための措置その他当該本人に参考となるべき情報提供を行った上で、外国にある第三者への提供を認める旨の同意を取得することがあらかじめ必要になることに留意。なお、個人情報保護委員会規則で定める国とは、平成 31 年個人情報保護委員会告示第 1 号に定める国を指す。

20 総務省告示により指定された電気通信事業者は、特定利用者情報を外国に保存する場合や外国の第三者に委託する場合には、情報取扱方針に必要な事項を記載する必要があることに留意が必要である。

用をする旨、②共同利用される利用者情報の項目、③共同して利用する者の範囲[21]、④利用する者の利用目的[22]、及び⑤当該利用者情報の管理について責任を有する者の氏名又は名称[23]及び連絡先[24]を明確にプライバシーポリシーに記載することが望ましい[25]。

［情報収集モジュール等に関する記載事項］

- 情報収集モジュール提供者の提供する情報収集モジュール（以下単に「情報収集モジュール」という。）が組み込まれていない場合は、アプリケーション提供者以外の第三者が情報収集モジュールを用いて利用者情報を取得しない旨をプライバシーポリシーに記載することが望ましい。
- アプリケーション提供者が情報収集モジュールを組み込む場合、アプリケーションを通じた情報収集の実態について明らかにする上で、アプリケーション提供者は、自らが組み込んでいる情報収集モジュールを用いたサービスの名称、提供者等の基本的な情報について、利用者に対して説明することが望ましい。
- 具体的には、アプリケーション提供者は、アプリケーションに情報収集モジュールを組み込んでいる場合、アプリケーションのプライバシーポリシーにおいても、①組み込んでいる情報収集モジュールの名称、②情報収集モジュール提供者の名称（外国にある第三者の場合はその国名）、③取得される利用者情報の項目、④利用目的、⑤情報収集モジュール提供者による情報利用の有無（ある場合はその目的）、⑥第三者提供・外国の第三者への提供・共同利用の有無等[26]について情報収集モジュールごとに記載するとともに、各情報収集モジュール提供者のプライバシーポリシーにリンクを張る等して容易に参照できるようにすることが望ましい（情報収集モジュール提供者のプライバシーポリシーが日本語でない場合、アプリケーションのプライバシーポリシーにおいてその概要を

---

21 共同利用する者の範囲には、必ずしも共同利用者の名称等を個別に全て列挙する必要はないが、本人がどの事業者まで将来利用されるか判断できる程度に明確にする必要がある。

22 利用目的は、全て記載する必要がある。利用者情報の項目によって利用目的が異なる場合は、項目ごとに利用目的を区別して記載することが望ましい。

23 全共同利用者の中で、第一次的に苦情の受付・処理、開示・訂正等を行う権限を有する者の氏名又は名称を記載する。

24 ⑤について、個人データを共同利用（個人情報保護法 27 条５項３号）する場合には、当該個人データの管理について責任を有する者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名を、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置く必要がある。なお、個人データの共同利用については注釈 25 も参照。

25 個人情報保護法上、特定の者との間で共同して利用される個人データを当該特定の者に提供する場合であって、個人情報保護法第 27 条第 5 項第 3 号に規定されている情報を、提供に当たりあらかじめ本人に通知し、又は本人が容易に知り得る状態に置いているときには、当該提供先は、本人から見て、当該個人データを当初提供した事業者と一体のものとして取り扱われることに合理性があると考えられることから、第三者に該当しないこととされているところ、必要な事項を本人に通知し、又は本人が容易に知り得る状態に置いていない場合には、これに当たらないことに留意する必要がある。

26 情報収集モジュールにより③取得される情報の項目、④利用目的、⑤第三者提供・共同利用の有無等について、情報収集モジュールのプライバシーポリシーやウェブサイト等に明示されている場合、そのリンクを張る等により代えることも可能であるが、その場合には、リンク先の記載の概要を併記することが望ましい。

明示する)。なお、その際、情報収集モジュールによりスマートフォン外部に利用者情報が送信される旨が分かるようにプライバシーポリシーに記載し、利用者の求めに応じて情報送信又は利用の停止(オプトアウト)の機会を提供することが望ましい。

⑥ 同意取得の方法及び利用者関与の方法

- 同意取得の方法:同意取得の対象となる利用者情報の範囲・取扱方法等についてプライバシーポリシーに記載することが望ましい。また、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。
  - 利用者情報の取扱いについて同意しなければ利用することができない機能と、同意をせずとも利用することができる機能がある場合には、同意を取得する前に明示するとともに、あらかじめ同意をしない選択肢も提示することが望ましい。
- 利用者関与の方法:利用者情報の取得・利用を中止する方法等をプライバシーポリシーに記載することが望ましい。
  - アプリケーション提供者による利用者情報の取得・利用を中止してほしい場合に、アプリケーションそのものをアンインストールする以外に方法がないときは、その旨プライバシーポリシーに記載することが望ましい。
  - アプリケーションを使用しながら、アプリケーション提供者による利用者情報の取得が中止される方法がある場合、又は利用者情報の取得は継続されるがその利用が中止される方法がある場合には、そのいずれであるかが分かるようにしてプライバシーポリシーに記載することが望ましい。
  - 利用者情報の取得・利用を中止することにより利用することができなくなる機能がある場合には、利用できなくなる範囲について明示することが望ましい。
  - プロファイリングを含むアプリケーション提供者による利用者情報の取扱いに異議がある場合に、その旨アプリケーション提供者へ申し立てる方法についてプライバシーポリシーに記載することが望ましい。

⑦ 問合せ窓口

- アプリケーション提供者が利用者情報を取得する場合に、利用者情報の取扱いに関する問合せ窓口の連絡先等(電話番号、メールアドレス、問い合わせフォーム等)をプライバシーポリシーに記載することが望ましい。

⑧ プライバシーポリシーの変更を行う場合の手続

- プライバシーポリシーの変更を行った場合の通知方法等を記載することが望ましい。

⑨ 利用者の選択の機会の内容、データポータビリティに係る事項

- 利用者情報の取得・利用の停止を利用者が求めることができるか否かをプライバシーポ

リシーに記載するとともに、停止を求める方法や停止後にアプリケーションを継続して利用することが可能であるかについて記載することが望ましい。

- データポータビリティを確保している場合には、利用者情報の移転を行う方法や、移転先の条件についてプライバシーポリシーに記載することが望ましい。

⑩ 委託に関する事項

- 利用者情報の委託を行う場合には、委託を行う情報の内容や委託先、委託の目的をプライバシーポリシーに記載することが望ましい。

【補足】

プライバシーポリシーは、基本原則に定められた「透明性の確保」や「利用者関与の機会の確保」等を実現するための中核となる手段である。そのため、アプリケーション提供者の取組として、まずプライバシーポリシーの具体的な作成項目を示している。

様々な利用者情報が大規模に蓄積されるスマートフォンにおいては、アプリケーションのプライバシーポリシーについては原則として企業全体のプライバシーポリシーやアプリケーションの利用規約と別に策定されることが望ましい。また、アプリケーションのプライバシーポリシーを策定する際には、企業全体のプライバシーポリシーや当該アプリケーションの利用規約との整合性について確認し、必要に応じて調整を行うことが期待される。

なお、利用者から観た際に、利用者情報の取得がされないためプライバシーポリシーを作成・公表していないのか、取得がされているにもかかわらず作成・公表していないのか不明確であると利用者が不安になる可能性があるため、利用者が自らの利用者情報の取扱いに関する情報を十分に得て、アプリケーションの利用に関し適切に判断し、行動することを支援するという本指針の趣旨に鑑み、利用者情報をアプリケーション提供者が取得していない場合においてもプライバシーポリシーを通知又は公表することが望ましい。具体的には、アプリケーション提供者が利用者情報を取得していない場合には、①、②、⑦及び⑧を記載したプライバシーポリシーへのリンクを張る、又はアプリストアのアプリケーション紹介文において記載する等して公表することが考えられる。

1.2.1.2. プライバシーポリシー等の運用

（１） 通知・公表又は同意取得の方法

[一般的な取扱い]

- アプリケーション提供者は、プライバシーポリシーを定め公表するとともに、アプリケーションをダウンロード又は利用開始しようとする者が容易に参照できる場所に掲示又はリン

クを張ることが望ましい[27]。

- アプリケーションをダウンロード又は利用開始しようとする者がスマートフォンの画面上で容易に理解できるように、プライバシーポリシーの分かりやすい概要を作成して利用者が容易に参照できる場所に掲示又はリンクを張る等、利用者にとって分かりやすい方法[28][29]で示されることが望ましい（概要から詳細なプライバシーポリシーへリンクを張る方法等も有用である）。
- プライバシーポリシーによる通知又は公表あるいは同意取得は、原則として利用者がアプリケーションをダウンロード又はインストールあるいは利用開始しようとする前に行うことが望ましく、それらの時点で行うことが難しい場合には、初回起動時に処理が実行される前に行うことが望ましい。
- 特に同意取得を要する利用者情報[30]については、アプリケーションをダウンロード又はインストールあるいは利用開始する前、初回起動時に処理が実行される前など、当該情報を取得するための処理が実行されうる前に同意取得が行われるように設計することが望ましい。
- アプリケーションに関する OS によるパーミッションは一般にアプリケーションがどのような情報にアクセスするかを示しているが、利用目的やスマートフォン外部への送信・第三者提供・共同利用の有無等の項目の記載がない場合には、OS によるパーミッションのみでは本項に示す通知又は公表あるいは同意取得として十分ではない[31]。OS によるパーミッションが表示される際に別途[32]アプリケーション提供者が作成したプライバシーポリシーのリンク先を示す等の方法により通知又は公表を行うか、必要に応じて個別の情報に関する同意取得等を行うことが望ましい。

[同意取得等を要する利用者情報の取扱い]

- アプリケーション提供者による、プライバシー性が高いと考えられる利用者情報の取得又は利用のうち、現状の利用実態を踏まえ代表的なものの取扱いについて、以下のとおり

---

27 アプリケーションをダウンロード又は利用開始した後に利用者がプライバシーポリシーを確認した場合、既に利用者情報が取得されている可能性があるため、利用者がアプリケーションをダウンロード又は利用開始する前に通知又は公表することが望ましい。なお、原則としてアプリストアのアプリケーション紹介ページにプライバシーポリシーへのリンクを張ることが望ましい。ただし、アプリケーションの利用開始後に利用者がプライバシーポリシーを容易に確認することを可能とするため、アプリケーション内にもプライバシーポリシーが掲示されていることが望ましい。

28 例えば、1.2.1.1.に示した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方法が考えられる。

29 利用者の属性（こども、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。

30 病歴、健康診断の結果等の要配慮個人情報に該当する利用者情報を取得する場合、個人情報保護法により原則として同意の取得が必要になることに留意（同法第 20 条第２項）。

31 OS のパーミッション等において、実際に取得される情報の項目及び利用目的等が具体的に記載されるような形式がとられた場合等には、当該パーミッションにより通知・同意を行う可能性もある。

32 OS のパーミッションを表示する際に合わせて表示される自由記入欄にプライバシーポリシーを表示することも一案と考えられる。

個別に対応することが望ましい。

① 個人情報を含む電話帳情報　アプリケーションが提供するサービスの目的に応じ必要とされる範囲（フィールド）を限定するとともに、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[33]。

② センシティブ情報[34]　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ついては、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[35]。また、プロファイリングによりセンシティブ情報を予測・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。

③ こどもの利用者情報[36]　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じることが望ましい[37]。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[38]。また、特に低年齢のこども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[39]。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

---

33 その場合であってもこれらの情報は第三者に関する個人情報を含むにもかかわらず、一方当事者である利用者の同意のみしか得られていないため、利用者の一定の責任を免れない場合もあると考えられる。

34 人種・信条・病歴等のほか、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その取扱いに特に配慮を要する利用者情報をいう。

35 個人情報保護法上の要配慮個人情報を取得する場合には、同法第 20 条第 2 項に従い、原則としてあらかじめ本人の同意を得ることが必要である。

36 対象とする年齢範囲については、例えば米国の児童オンラインプライバシー保護法（COPPA）は 13 歳未満を対象としているほか、GDPR におけるこどもの同意については、16 歳未満（加盟国ごとに 13 歳を下回らない範囲で設定が可能）の場合は親権者による同意が必要とされており、これらを参考とすることが考えられる。

37 英国 Children’s Code（Age Appropriate Design Code ）が示す行動規範も参照しながら、プライバシーポリシーの作成・運用、アプリの開発等を行うことも考えられる。

38 こども向けのプライバシーポリシーを別途用意することも有用である。

39 個人情報保護法上、本人同意の取得が必要であり、当該本人が未成年である場合については、「対象となる個人情報の項目や事業の性質等によって、個別具体的に判断されるべきですが、一般的には 12 歳から 15 歳までの年齢以下のこどもについて、法定代理人等から同意を得る必要があると考えられ」るとされていることにも留意が必要である（個人情報保護委員会「『個人情報の保護に関する法律についてのガイドライン』に関する Q&A」QA1-62）。

示は実施しないことが望ましい。

④ 利用者行動のトラッキング　利用者は、端末やアプリケーション等によって提供される広告 ID 等の識別子に関連付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、特定の個人の識別性を獲得する可能性があると考えられること、また、特定の個人の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が可能となることから、プライバシー侵害を回避する観点又は利用者利益の保護の観点から、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[40]。

⑤ 契約者・端末固有 ID 等、契約や端末に対して一義的に指定・作成され、利用者側で変更が困難であるが、幅広い主体により利用される可能性があるものが ID 等の情報を取得するアプリケーション提供者等において特定の個人の識別性を有する情報と結びつきうる形で利用される場合　同一 ID の上に様々な情報が時系列的に蓄積し得ること、当該アプリケーション提供者等又は第三者において特定の個人の識別性を有する可能性があることから、個人情報保護法への抵触やプライバシー侵害の可能性を考慮し、個人情報に準じた形で取り扱うことが望ましい。具体的には、取得される項目及び利用目的を明確に記載し、その目的の範囲内で適正に扱うこととすることが望ましい[41]。

⑥ GPS 等による位置情報[42]は、アプリケーションが提供するサービスの提供又は機能に直接関連する場合に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等、取扱いに留意することが望ましい。

⑦ 通信内容・履歴、メール内容・送受信履歴等の通信履歴の取得　通信相手等の特定の個人の識別性を有する場合があること、及び通信の内容を含むプライバ

---

[40] 電気通信事業法における外部送信規律は、同意の取得を義務とするものではなく、通知又は容易に知り得る状態に置くことを求めるものであるところ、ここでは取り組むことが望ましい事項として記載している。

[41] これらの情報は個人情報や個人関連情報に該当し得るため、個人情報保護法の規定を遵守する必要があることにも留意が必要。

[42] 位置情報の同意取得については、例えば、総務省の「位置情報プライバシーレポート～位置情報に関するプライバシーの適切な保護と社会的利活用の両立に向けて～」（平成 26 年 7 月）も参考となり得る。また、電気通信事業者においては、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第 41 条も合わせて参照されたい。

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[43]。

⑧ スマートフォンのアプリケーションの利用履歴[44]やスマートフォンに保存された写真・動画　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等、取扱いに留意することが望ましい。

【補足】

1.　プライバシーポリシー等の運用

プライバシーポリシーにより、利用者に対し、利用者情報の取得等に関して説明することは、アプリケーション提供者が社会の信頼を確保するために重要である。

個人情報の保護に関する基本方針では、プライバシーポリシー等を策定・公表することにより、「個人情報を目的外に利用しないことや苦情処理に適切に取り組む等を宣言するとともに、事業者が関係法令等を遵守し、利用目的の通知・公表、開示等の個人情報の取扱いに関する諸手続について、あらかじめ、対外的に分かりやすく説明することが、事業活動に対する社会の信頼を確保するために重要である」ことが示されている。

さらに、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においては、「電気通信事業者は、アプリケーションソフトウェア（以下「アプリケーション」という。）を提供する場合において、当該アプリケーションによる情報の取得等について明確かつ適切に定めたプライバシーポリシーを公表することが適切である」ことが定められており、事業者単位でのプライバシーポリシーではなく、アプリケーション単位でプライバシーポリシーを定め、公表することが示されている。

こうした観点により、1.2.1.1.プライバシーポリシーの作成において、具体的なプライバシーポリシーの項目を示しているが、プライバシーポリシーは、あくまでも手段であり、適切に運用されて初めて、利用者の信頼を得ることができるとともに、アプリケーション提供者の関係法令等の遵守に資するものである。そこで本節では、プライバシーポリシー等の運用に関わる具体的な取組を示した。

---

43 通信の相手方や内容に含まれる第三者の同意を得ない場合に、アプリケーション提供者等や利用者が一定の責任を免れないこともあると考えられる。

44 アプリケーションの品質向上等のために当該アプリケーションの利用履歴等を活用することは、アプリケーションにより提供されるサービス提供の一環と考えられるため、プライバシーポリシー等に明示しアプリケーションに関する通知又は公表あるいは同意取得を行うことで可能である。一方、他アプリケーションの利用履歴等については、分析、広告配信・表示やマーケティングを目的として取得することは望ましくない。アプリケーションのサービス提供に関連する場合であっても、個別の情報に関する同意取得を行うことが望ましい。

2. プライバシーポリシーの掲示場所等

プライバシーポリシー等を適切に運用し、透明性を高めるためには、利用者が容易にプライバシーポリシーを確認できることが重要である。そのような観点から、容易に参照できる場所に掲示又はリンクを張ることを求めている。

3. 通知・公表又は同意取得のタイミング

まず、アプリケーションをダウンロード又は利用開始した後にプライバシーポリシーを確認した場合、既に利用者情報が取得されている可能性があるため、利用者がアプリケーションをダウンロード又は利用開始する前に通知又は公表することが望ましい。なお、原則としてアプリストアのアプリケーション紹介ページにプライバシーポリシーへのリンクを張ることが考えられるが、一方で、アプリケーションの利用開始後に利用者がプライバシーポリシーを容易に確認することを可能とするため、アプリケーション内にもプライバシーポリシーを掲示することが望ましい。

4. 同意取得等を要する利用者情報の取扱い

「プライバシー情報の収集について、本人の同意がある場合や、収集方法等に照らして定型的に推定的同意があると認められる場合には、人格的自律ないし私生活上の平穏を害する態様で収集されたということはできない」（東京地判平成 22 年 10 月 28 日客室乗務員 DB 事件）といった裁判例等、プライバシー性の高い情報を取得・利用・提供する場合、本人の同意があればプライバシー権侵害に当たらない場合がある。そのような観点から、アプリケーション提供者等がプライバシー性の高い利用者情報を取得する場合又はプライバシー性の高い態様で利用者情報を利用する場合には、個別の取得・利用に関する同意を取得することによりプライバシー侵害を回避しうる。

有効な同意と認められるかは、事案に応じて検討が必要である。例えば、アプリケーションに関する OS によるパーミッションにより「アプリケーションが当該情報にアクセスする権限」に対する許諾を得たとしても、「利用目的」、「利用者情報の外部送信」及び「第三者提供」について説明がない場合には、単体では第三者提供に係る同意取得の条件を満たしているとはいえないとの指摘がある。

（2） 利用者関与の方法

- 利用者情報が、プライバシーポリシーに反して、取得され又は取り扱われていることが明確である場合等については、利用者からの申出を受け利用の停止又は消去を行うことが望ましい。また、その手段についてプライバシーポリシーへ記載する等、利用者にとって参照しやすい方法で情報提供されることが望ましい[45]。

[45] 個人情報保護法上、保有個人データが特定された利用目的の達成に必要な範囲を超えて取り扱われて

- 利用者が利用者情報の範囲・取扱方法について同意した場合であっても、その同意の後に、簡単にアクセスでき、かつ、分かりやすい方法で当該同意の撤回等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。
  - 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。

（3） アプリケーションの更新等によるプライバシーポリシーの変更

- アプリケーションの更新等によりプライバシーポリシーを変更する場合は、利用者に対し、通知することが望ましい。
- アプリケーションの更新等によりプライバシーポリシーに定めた利用目的から関連性を有すると合理的に認められる範囲を超えて利用目的が変更となる場合には、利用者から同意を取得することが望ましい[46]。
- なお、アプリケーションの更新等により、当初の同意取得の対象であった利用者情報の範囲・取扱方法が変更される場合には、元の利用者情報の範囲・取扱方法について、利用者との間での合意が成立しているため、利用者から同意を取得することが必要となる。

1.2.1.3. 苦情相談への対応体制の確保

- 利用者情報を取得するアプリケーション提供者は、利用者情報の取扱いに関する苦情や相談の適切かつ迅速な処理に努める。具体的には、苦情相談の窓口・連絡先を設置する等必要な体制の整備に努めることが望ましい。

［情報収集モジュールを組み込む場合の取扱い］

- アプリケーション提供者は、利用者から、情報収集モジュール提供者による利用者情報の取扱いに関する苦情相談があった場合であって、自らその苦情相談を処理することができないときは、情報収集モジュール提供者の相談窓口・連絡先に利用者を誘導することが望ましい。

いる場合等一定の場合については、本人は当該保有個人データの利用の停止又は消去を請求することができ（同法第 35 条第 1 項）、また、保有個人データが第三者提供等に関する規制に違反して第三者に提供されている場合には、本人は当該保有個人データの第三者への提供の停止を請求することができる（同条第 3 項）とともに、保有個人データを当該個人情報取扱事業者が利用する必要がなくなった場合等においては、本人は当該保有個人データの利用停止等又は第三者への提供の停止を請求することができる（同条第 5 項）。また、これらの請求に応じる手続は、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置かなければならないこととされている（同法第 32 条第 1 項第 3 号）。

[46] 個人情報については、利用目的の達成に必要な範囲を超えて利用する場合には、原則としてあらかじめ本人の同意を取得しなければならないことに留意が必要である（個人情報保護法第 18 条第 1 項）。

1.2.1.4. 適切な安全管理措置

- 取り扱う利用者情報が漏えい、滅失又はき損の危険にさらされることがないように、利用者情報の安全管理のために必要かつ適切な措置を講じることが望ましい[47]。
- 利用目的に必要な期間に限り保存し、目的達成等により不要となった際には、適切に消去することが望ましい。
- 利用者がアプリケーションをアンインストール等したこと又は一定期間利用していないことが判明した後のデータの保存期間、その後の処理等についてあらかじめ定めておくことが望ましい。
- 利用者情報を取得するアプリケーション提供者が、利用目的の達成に必要な範囲において、利用者情報の取扱いの全部又は一部を外部委託する場合は、委託先における利用者情報の取扱いの安全管理についても監督することが望ましい[48]。

1.2.1.5. アプリケーションの開発時における留意事項

- アプリケーション提供者は、利用者の個人情報やプライバシーが尊重され保護されるように、アプリケーションの企画及び設計の段階から、当該アプリケーションにおける利用者情報の取り扱われ方について検討し、適切な仕組みをアプリケーションに組み込むことが望ましい。アプリケーション提供者がアプリケーションの開発を委託する場合、委託先とともに利用者情報の取扱いに関する要求事項を整理し、当該要求事項がアプリケーションに組み込まれるよう指示し、監督することが望ましい。加えて、アプリケーション提供者は、あらかじめプライバシーポリシーを作成するとともに、委託先からのアプリケーションの納品を受ける際に、プライバシーポリシーの記載事項とアプリケーションの挙動が一致するかを検証することが望ましい。

1.2.1.6. ダークパターン回避の対応

- 利用者利益の保護を図るため、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歪めたり損なったりする方法で利用者情報の取扱いを行わないことが望ましい[49]。

【補足】

---

47 個人情報取扱事業者は、その取り扱う個人データの漏えい等の防止その他の個人データの安全管理のため、必要かつ適切な措置を講じなければならず、講じなければならない措置には、個人情報取扱事業者が取得し、又は取得しようとしている個人情報であって、当該個人情報取扱事業者が個人データとして取り扱うことを予定しているものの漏えい等を防止するために必要かつ適切な措置も含まれる。（個人情報保護法第 23 条）。

48 個人データについては、委託した個人データの安全管理が図られるよう、当該委託先に対する必要かつ適切な監督を行わなければならないことに留意が必要である（個人情報保護法第 25 条）。

49 本指針においては、あくまで望ましい事項として記載しているが、関係する他法令においてこのような取扱いが禁止されている場合には、当該法令に従い対応する必要がある。

ダークパターンの具体的な事例は、例えば以下の場合が考えられる[50]。

- アプリケーションの利用開始後に利用者情報の取得・利用をオプトアウトすることが可能であるにもかかわらず、利用開始時には同意を拒否する選択肢が提示されず、デフォルトで同意をすることとなっている場合。
- 同意を取得する場合の操作に比べ、同意を撤回する場合の操作が煩雑になっている場合、又は同意を撤回する方法に容易に到達することができない場合。
- 同意の取得画面において、同意ボタンが目立つように表示されており、拒否するボタンが表示されていない又は目立たない形で表示されている場合。
- 利用者が一度拒否したにもかかわらず、同意が得られるまで繰り返し同意取得画面を掲出する場合。
- 同意の取得画面又はその直前の画面において、利用者情報の取得・利用に同意することによるメリット又は同意しないことによるデメリットのみを強調し、同意へ誘導している場合。
- 同意取得時に、利用者に対して金銭等のインセンティブを提示することにより、同意へ誘導している場合。
- 同意取得時に、後で同意を撤回する方法が用意されている旨説明していたにもかかわらず、実際には同意を撤回する方法が用意されていない場合。情報の取得範囲を利用者が設定できるようにしている場合において、より多くの情報を取得する選択肢がデフォルトで選択されている場合。

1.2.1.7. 電気通信事業法への対応

- 通信の秘密[51]に該当する利用者情報の取扱いについては、電気通信事業法第4条において、電気通信事業者の取扱中に係る通信の秘密は侵してはならないこととされている点に留意が必要である。
- 総務省告示により指定された電気通信事業者においては、特定利用者情報の取扱いについて、情報取扱規程の策定・届出、情報取扱方針の策定・公表等の対応を行わなければならない。詳細については、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を参照すること。
- メッセージ媒介サービス、SNS、検索サービス、ホームページの運営等の対象となる電気通信役務を営んでいる電気通信事業者は、利用者に関する情報を利用者の端末の外

[50] パターンの具体的な事例については、欧州データ保護会議（EDPB）による”Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them”（https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en）や、OECDによる”Dark Commercial Patterns”（https://www.oecd-ilibrary.org/science-and-technology/dark-commercial-patterns_44f5e846-en）を参考に記載している。

[51] 通信内容にとどまらず、通信当事者の住所・氏名、発受信場所、通信年月日等通信の構成要素及び通信回数等通信の存在の事実の有無を含む。

部に送信させる場合[52]には、送信される情報の内容や送信先、利用目的等について通知、公表、本人同意の取得又はオプトアウト措置を行わなければならない。詳細については、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を参照すること。

- 本人同意の取得及びオプトアウト措置については、必ずしも法令上の義務が課されるものではないが、利用者関与の機会の確保の観点からは、本指針を参考に対応することが望ましい。

1.2.2. 情報収集モジュール提供者の取組

≪期待される役割≫

- 情報収集モジュール提供者は、利用者情報を取得する場合、自身の利用者情報の取扱いに責任を負っていると考えられる。
- 加えて、情報収集モジュール提供者は、情報収集モジュールの挙動や取得した情報の利用に一義的に関与していることから、情報収集モジュールの利用者情報の取扱いに関する透明性等が確保されるようアプリケーション提供者を支援することが期待される。

≪具体的な取組み内容≫

1.2.2.1. プライバシーポリシーの作成

- スマートフォンから利用者情報を収集する情報収集モジュール提供者は、1.2.1.1 を踏まえ、プライバシーポリシーを作成することが望ましい。その際、1.2.1.1 の適用に当たっては、適宜、「アプリケーション提供者」を「情報収集モジュール提供者」と、「アプリケーション」を「情報収集モジュール」と読み替えるものとする。

1.2.2.2. プライバシーポリシーの運用等

- 1.2.1.2 を踏まえて、プライバシーポリシーの運用等を実施することが望ましい。その際、1.2.1.2 の適用に当たっては、適宜、「アプリケーション提供者」を「情報収集モジュール提供者」と読み替えるものとする。
- ただし、アプリケーションの利用者に対する通知又は公表あるいは同意取得に関しては情報収集モジュール提供者自身が実施することは困難だと考えられ、アプリケーション提供者を介して行われることが想定されるため、情報収集モジュール提供者は、関連する内容を含むプライバシーポリシーを公表し、アプリケーション提供者へ通知することが望ましい。
- アプリケーションの利用者から、情報収集モジュール提供者に対し、取得した利用者情報に関する問合せ又は取得した利用者情報の消去等の申出があった場合、必要に応じ

[52] 委託先に対する送信についても例外ではないことに留意が必要である。

てアプリケーション提供者と協力し、これに応じることが望ましい[53]。

- プライバシーポリシーの内容について変更があった場合は、プライバシーポリシーを更新するものとし、プライバシーポリシーの内容について重要な変更があった場合には、プライバシーポリシーを更新し、公表するとともに、アプリケーション提供者へ通知することが望ましい。

1.2.2.3. 苦情相談への対応体制の確保、適切な安全管理措置及びダークパターン回避の対応

- 苦情相談への対応体制の確保及び安全管理措置については、1.2.1.3、1.2.1.4 及び 1.2.1.6 を踏まえて取り組むことが望ましい。

1.3. 他の関係事業者等における取組

- 適切な取扱いや利用者における安全・安心の向上のために、アプリケーション提供者等以外の関係事業者等についても、基本原則等を考慮しつつ、以下のような取組をそれぞれの立場で、また相互に協力しつつ進めることが望ましい。

1.3.1. アプリストア運営事業者[54]、OS 提供事業者

- アプリストア運営事業者は、アプリケーション提供者等において、「1.2 アプリケーション提供者等における取組」で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確認することが望ましい。
- アプリストアへのアプリケーションの登録審査時に本指針を踏まえた基準等を作成し、あらかじめ公表することが望ましい。
- アプリケーションの掲載を拒否する場合には、その理由について、アプリケーション提供者に対して適切なフィードバックを行うことが望ましい[55]。
- アプリストアの個別のアプリケーションページ上に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、表示すべき事項や標準的なアイコンを示す等、アプリケーション提供者等に対し、適切な対応を行うように支援することが望ましい。
- 説明や情報取得の方法が適切ではないアプリケーションが判明した場合の対応（アプリストアから削除する等）を実施するとともに、連絡通報窓口を設置することが望ましい。

---

53 本人確認が不可能な場合等適切かつ合理的な方法により当該申出に応じることが出来ない場合は、利用者に対し、その理由とともに応じることが出来ない旨を説明する。

54 アプリストアの運営に当たっては、例えば、英国の “Code of practice for app store operators and app developers” (https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers/code-of-practice-for-app-store-operators-and-app-developers-new-updated-version) （以下「英国コード・オブ・プラクティス」という。）が示す行動規範を参照することが考えられる。

55 アプリケーション提供者へのフィードバックの方法については、英国コード・オブ・プラクティスにおける開発者に対する明確なフィードバックに関する規範を参照することが考えられる。

- OS によるパーミッションがある場合、利用者に分かりやすい説明を行う努力を継続する。目的に応じ注意すべきパーミッション等がある場合、利用者が安全に利用できるための方策を検討することが望ましい。
- 必要に応じ関係事業者や業界団体等とも協力しつつ、アプリケーション提供者等に対し啓発活動を進めることが望ましい。

【補足】

アプリストアにおいて、仮にプライバシー侵害を行うアプリケーションが多数販売されているような場合、アプリストア運営事業者は、ユーザーに対して注意喚起その他の義務を負うと解される可能性があることから、アプリケーション提供者等に対する、各種取組を行うことが望ましい。

なお、アプリストアや OS の利用規約等において専属的合意管轄裁判所を国外の裁判所とし、準拠法を外国法としている場合においても、消費者である利用者からの訴訟提起の際や、不法行為に基づく請求の際には、日本の裁判所に国際裁判管轄が認められ、準拠法を日本国法とされる可能性があることは既に述べたとおりである。

1.3.2. 移動体通信事業者・端末製造事業者

- スマートフォン販売時等に、既存チャンネルを通じて利用者に必要事項を周知することが望ましい。（例えば、従来の携帯電話との違い[56]、情報セキュリティやプライバシー上留意すべき点等の周知等）
- 移動体通信事業者のアプリストアにおいて、アプリケーション提供者等に対し、適切なプライバシーポリシー等の作成・公表等の対応を促すことが望ましい。プライバシーポリシー等の表示場所を提供する等、アプリケーション提供者等に対し、適切な対応を行うように支援するとともに、必要に応じ関係事業者や団体等とも協力しつつ、アプリケーション提供者等に対し啓発活動を進めることが望ましい。
- 移動体通信事業者のアプリストアにおいて、説明や情報取得の方法が適切ではないアプリケーションが判明した場合の対応（アプリストアから削除する等）を実施するとともに、連絡通報窓口を設置することが望ましい。
- 今後「利用者」として増加する可能性があるのは、現在スマートフォンを使いこなしている層に加えて、ICT リテラシーに乏しい消費者、高齢者等と考えられることから、移動体通信事業者はリテラシーに応じたスマートフォンの機器やサービス設計、周知啓発活動を端末製造事業者との協力も考慮しつつ検討することが望ましい。

【補足】

[56] 水平分業モデルで PC と類似した自由度があるが、マルチステークホルダーで自己責任リスクがあるスマートフォンの違いを十分周知する必要がある。

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は、「電気通信事業者は、アプリケーションを提供するサイトを運営する場合において、当該サイトにおいてアプリケーションを提供する者に対して、当該アプリケーションによる情報の取得等について明確かつ適切に定めたプライバシーポリシーを公表するよう促すことが適切である」と定められており、各関係者の取組の促進に資することが期待される。

1.3.3. その他関係しうる事業者等

- 独自の基準に基づきアプリケーションの推薦等をしているアプリケーション紹介サイトやアプリケーションに関する広告は、利用者がアプリケーションを認知し、選択する際に影響力を有する情報源となる場合がある。
- アプリケーション紹介サイト運営者、アプリケーションを通じて取得された利用者情報を用いて広告に関する事業を行う者等関係する事業者は、可能な限りプライバシーポリシー概要の掲載等を検討したり、説明や利用者情報取得、第三者提供等の方法が適切でないアプリケーションが判明した場合の対応を検討する等、基本原則や指針等を考慮しつつ、望ましい取組を協力して進めることが期待される。

1.4. セキュリティの確保に係る取組

1.4.1. アプリケーション提供者等

1.4.1.1. アプリケーション提供者

［セキュリティ・バイ・デザインを確保するための取組］

- アプリケーション提供者は、アプリケーションの開発時には、セキュリティが適切に確保されるよう、アプリケーションの企画及び設計の段階から、当該アプリケーションにおけるセキュリティの確保について検討し、適切な仕組みをアプリケーションに組み込むことが望ましい（例：業界標準の暗号化技術の使用、最小権限、セキュアコーディング　等）。
- アプリケーション提供者は、提供するアプリケーションにおいて使用する情報収集モジュールについて、セキュリティの確保の観点から内容を確認することが望ましい。

［脆弱性があるアプリケーションへの対応等］

- アプリケーション提供者は、アプリケーションに係る脆弱性情報を継続して収集するとともに、アプリケーション内に発見された脆弱性について適切かつ迅速に報告を受けられるよう、脆弱性情報の窓口・連絡先を設置する等必要な体制の整備に努める。
- アプリケーション提供者は、アプリケーションを提供する際にはセキュリティの確保に影響を与え得る脆弱性が含まれないようにあらかじめ確認するとともに、セキュリティの確保に影響を与え得る脆弱性が発見された場合には、アプリケーションのアップデートを適切かつ迅速に提供する等、必要な対応を取ることが望ましい。
- アプリケーション提供者は、提供するアプリケーションにおいて個人情報漏えい等のセキュリティインシデントが発覚した場合には、関係者に対して適切かつ迅速に周知するよう努める。

1.4.1.2. 情報収集モジュール提供者

- 情報収集モジュール提供者は、1.4.1.1を踏まえ、セキュリティの確保に取り組むものとする。その際、1.4.1.1 の適用に当たっては、適宜、「アプリケーション提供者」を「情報収集モジュール提供者」と、「アプリケーション」を「情報収集モジュール」と読み替えるものとする。

1.4.2. アプリストア運営事業者、OS 提供事業者

- セキュリティの確保の観点から、アプリストア運営事業者は、次に掲げる取組を進めることが望ましい。

［アプリストアとしての基本的対応］

① アプリ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、当該要件を満たしているかを審査する（例：業界標準の暗号化技術の使用、最小権限、セキュアコーディング　等）

② アプリストア内で提供されるアプリケーションについて、利用者情報が保存・処理される法域、利用者情報へのアクセスが許可される者の範囲、利用者情報へアクセスする目的、アップデートの最終更新日等の情報を公開し、利用者が購入及びダウンロードする前に確認可能な場を設ける

［脆弱性があるアプリケーションへの対応］

③ アプリストア内で提供されるアプリケーションが、脆弱性報告のための窓口を有し、かつ、アプリケーション提供者が適切なタイミングで脆弱性を開示するための手続を有していることを確認する。

④ アプリケーション提供者からアップデートが提出された場合には、利用者に対してアプリケーションが最新版にアップデートされるよう促す等、必要な対応を取る

⑤ アプリケーションが長期間アップデートされない場合には、アプリケーション提供者にアプリのサポート状況を確認する

［不正なアプリケーションへの対応］

⑥ アプリストアにおいて、利用者等が不正なアプリケーションを報告できるよう報告窓口を設置する

⑦ 不正なアプリを発見した場合には、速やかに当該アプリを削除するとともに、当該アプリケーションを作成したアプリケーション提供者が開発した他のアプリケーションについても調査を行う

［アプリケーション削除・掲載拒否時の対応］

⑧ アプリケーションの掲載を拒否する場合には、その理由について、アプリケーション提供者に対して適切なフィードバックを行う[57]

- OS提供事業者は、利用者のためにセキュリティやプライバシーを保護するため、アプリストアが上記の取組を実施す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。

[57] アプリケーション提供者へのフィードバックの方法については、英国コード・オブ・プラクティスにおける開発者に対する明確なフィードバックに関する規範を参照することが考えられる。

2. 今後の技術・サービスの進展に対する柔軟な対応

- 本指針は、新技術・サービスの進展、利用者情報の利用形態の変化等を踏まえ、必要に応じ、見直しが図られることが望ましい。

【補足】

今後、IoT 等の新技術・サービスが急速に進展することが予想される。本指針は、関係事業者等に対する、スマートフォンにおける利用者情報の取扱いに関わる取組を定めたものであるが、IoT 等の新技術・サービス等にも準用可能なものも存在すると考えられる。ただし、本指針は、必ずしも IoT 等の新技術・サービスを想定したものではなく、IoT 等の新技術・サービスに本指針を準用する場合には、十分な検討が行われることが望ましい。

また、多くの情報収集モジュールがアプリケーションに組み込まれていること、関係事業者等の利用者情報の取得、送信、利用等への関わり方が複雑化していること等、実際の情報利用の仕組みが極めて複雑化しており、利用者が自身の情報の取り扱われ方について、理解し、判断するということが今後困難となることが予想される。そのような中で、今後、利用者に対する、利用者が自ら判断するための十分な情報提供が難しい場合について、利用者情報の取扱いの在り方を検討する必要が生じることも想定される。

（以下略）

参考資料

1. 「利用者情報に関するワーキンググループ」概要

・開催要綱

・開催状況

2. 各種資料

「利用者情報に関するワーキンググループ」開催要綱

1　目的

本ワーキンググループ（以下「WG」という。）は、「ICT サービスの利用環境の整備に関する研究会」の下に開催される WG として、電気通信事業、プラットフォームサービス等に係る利用者情報の更なる保護等に向けて、最近の動向等を踏まえ、専門的な観点から集中的に検討することを目的とする。

2　名称

本 WG は、「利用者情報に関するワーキンググループ」と称する。

3　検討事項

（１）電気通信事業、プラットフォームサービス等に係る利用者情報の取扱い等の在り方の検討
（２）電気通信事業者、プラットフォーム事業者等の関係事業者及び関係団体等による取組の実態把握
（３）その他

4　構成及び運営

（１）本 WG の主査は、ICT サービスの利用環境の整備に関する研究会の座長が指名する。
（２）本 WG の構成員は、別紙のとおりとする。
（３）本 WG の構成員は、中立の立場をもって、専門的知見に基づき議論を行う。
（４）主査は本 WG を招集し、主宰する。
（５）主査は、必要があると認めるときは、主査代理を指名することができる。
（６）主査代理は、主査を補佐し、主査不在のときは主査に代わって本 WG を招集し、主宰する。
（７）本 WG の構成員は、やむを得ない事情により出席できない場合において、代理の者を指名し、出席させることができる。
（８）主査は、必要に応じ、オブザーバーを招聘することができる。
（９）主査は、必要に応じ、構成員以外の関係者の出席を求め、意見を聴くことができる。
（10）その他、本 WG の運営に必要な事項は、主査が定める。

5　議事・資料等の扱い

（１）本 WG は、原則として公開とする。ただし、主査が必要と認める場合については、非公開とする。
（２）本 WG で使用した資料は、原則として、総務省のウェブサイトに掲載し、公開する。ただし、公開することにより、当事者若しくは第三者の利益を害するおそれがある場合又は主査が必要と認める場合については、非公開とする。
（３）本 WG の議事概要は、原則として公開する。ただし、主査が必要と認める場合については、非公開とする。

6　その他

本 WG の事務局は、総務省総合通信基盤局電気通信事業部利用環境課が行う。

（別　紙）

「利用者情報に関するワーキンググループ」構成員

（敬称略・五十音順）

【構成員】

（主査）	山本　龍彦	慶應義塾大学大学院　法務研究科　教授
（主査代理）	生貝　直人	一橋大学大学院　法学研究科　教授
	江藤　祥平	一橋大学大学院　法学研究科　教授
	太田　祐一	株式会社 DataSign　代表取締役社長
	木村　たま代	主婦連合会　国際規格化推進マネージャー
	寺田　眞治	一般財団法人日本情報経済社会推進協会　客員研究員
	森　亮二	英知法律事務所　弁護士
	呂　佳叡	森･濱田松本法律事務所　弁護士

【オブザーバー】

個人情報保護委員会事務局

「利用者情報に関するワーキンググループ」開催状況

第１回 （2024 年３月１日）	○利用者情報の適切な取扱いの確保に関する背景及び現状について ・事務局説明 ○SPI の改定に向けた有識者ヒアリング① ・有識者発表：日本総合研究所、生貝主査代理
第２回 （2024 年３月 18 日）	○SPI の改定に向けた有識者ヒアリング② ・有識者発表：慶應義塾大学・新保教授、モバイル・コンテンツ・フォーラム、マクロミル
第３回 （2024 年４月 16 日）	○SPI の改定に向けた有識者ヒアリング③ ・有識者発表：三菱総合研究所、日本総合研究所 ○利用者情報の取扱いに関するモニタリングの進め方について ・事務局説明 ○利用者情報の取扱いに関するモニタリングに向けた有識者ヒアリング ・有識者発表：日本総合研究所
第４回 （2024 年５月 24 日）	○利用者情報の取扱いに関するヒアリングシート（案）について ・事務局説明
第５回【非公開】 （2024 年６月７日）	○SPI の改定に向けた事業者ヒアリング ・事業者ヒアリング（Apple Inc.） ・書面提出（Google LLC）
第６回【メール審議】 （2024 年６月 10 日～同年６月 11 日）	○利用者情報の取扱いに関するヒアリングシート（案）について
第７回 （2024 年６月 28 日）	○SPI 改定案について ・事務局説明
第８回【メール審議】 （2024 年７月９日～同年７月 12 日）	○SPI 改定案について
第９回 （2024 年９月３日）	○利用者情報の取扱いに関するモニタリング（事業者ヒアリング①）
第１０回 （2024 年９月４日）	○利用者情報の取扱いに関するモニタリング（事業者ヒアリング②）
第１１回 （2024 年９月９日）	○利用者情報の取扱いに関するモニタリング（事業者ヒアリング③）
第１２回 （2024 年９月 30 日）	○利用者情報に関するワーキンググループ報告書（案） ○利用者情報の取扱いに関するモニタリングについて

※下線部が、スマートフォン上のプライバシー対策に係るもの