スマートフォン利用者情報取扱指針の改定に係るヒアリングについて

（Google回答）

2024年6月7日

1　ヒアリング依頼事項

	ヒアリング依頼事項	関連資料
Google Play ＆Android OS	アプリストアの規約・審査方針の内容、規約の遵守状況に係る御社の取組については、利用者情報に関するワーキンググループ第３回のうち、資料3-2のとおり日本総研から発表しているが、当該内容（及び関連する取組）について。	第3回利用者情報に関するWG 資料3-2
プライバシーサンドボックス	現時点でSPIへの反映に含まれるかどうかとは別に、今後検討が必要と考えられるため、サードパーティクッキー廃止に伴うプライバシーサンドボックスの導入など技術的動向について。	第1回利用者情報に関するWG 資料1-2 (p.11&45)

2　Google回答

（1）Google Play 及び Android OS

- 第3回利用者情報に関するワーキンググループにおいて、日本総研様から、Googleによる関連する取組として、下記の項目につきご発表いただいたと承知しております。

項目	概要	実施時期	関連URL
プライバシーポリシーの設置義務化（規約変更）	• Goolgeが利用者情報の取得有無にかかわらず、全てのアプリを公開する場 合にプライバシーポリシーの設置の義務付け	2022年7月から	https://support.google.com/googleplay/android-developer/answer/10787469
アカウント削除要件の追加	• アプリにアカウント作成機能を作成する場合には、アカウント削除機能を必須とする要件を追加	2023年4月から	https://support.google.com/googleplay/android-developer/answer/13316080?sjid=8471729585777815175-AP#account_deletion

目的外利用の禁止	• Goolgeがガイドラインに「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」と明確化	2024年3月から	https://support.google.com/googleplay/android-developer/answer/10144311?hl=ja
健康・フィットネス・医療データを取得するアプリに対する規約追加（特定の条件に該当するアプリに対する規制強化）	・Googleが健康・フィットネス・医療データを取得するアプリに対する規約を追加（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など）	2024年5月から	https://support.google.com/googleplay/android-developer/answer/13996823?hl=ja
アイコン等でデータ収集・共有方針の義務化	• Googleが「データセーフティセクション」開示の義務化	2022年7月から	https://support.google.com/googleplay/android-developer/answer/10787469?hl=ja

- Googleにおきましては、上記に加え、前回 2017 年のスマートフォン利用者情報取扱指針改定以降、Google Play 及び Android OS に関するプライバシー・セキュリティ関連の取組として、以下のような取組を行っています。

項目	概要	実施時期	関連URL
機密情報へのアクセスに関する権限と API	・アプリが機密情報にアクセスする権限や API をリクエストできる要件につき規定しています。 ・アプリが現在提供している機能やサービスの実装に必要かつ、アクセス権限が Google Play ストアの掲載情報に掲載されている場合に限られる。ユーザーデータやデバイスデータへのアクセスを必要とする機能や目的が公開されていないもしくは実装されていない場合、または認可されていない場合には、機密情報にアクセスする権限や	2018年から	https://support.google.com/googleplay/android-developer/answer/13986130?hl=ja&ref_topic=9877467&sjid=14990478638112713758-AP

	API は利用できません。		
Google Play プロテクト	・Google Play プロテクトは、マルウェアや望ましくないソフトウェアに対するプロアクティブな保護機能であり、Google Play のサービスを備えたすべての Android デバイスで有効になります。 ・Google Play プロテクトは、世界中の30億以上の Android 端末において毎日 1,250 億個のアプリをスキャンして、マルウェアや不要なソフトウェアからユーザーを保護しています。有害な可能性のあるアプリが見つかった場合、Google Play プロテクトは警告の送信、アプリのインストールの防止、アプリの自動的な無効化などの特定のアクションを実行します。 ・Google Play プロテクトは、Google Play ストアに限らず常にAndroid 端末全体においてユーザー保護を提供してきました。オンラインでもオフラインでも、インストール元に関係なく、デバイスに有害な可能性のあるアプリがダウンロードされていないかチェックします。	2017年5月から	https://developers.google.com/android/play-protect https://support.google.com/googleplay/answer/2812853?hl=ja
アプリの権限の自動リセット機能	・Android 11 では、アプリの権限を自動リセットする機能を導入しました。この機能は、アプリが数か月にわたって使われなかった場合にランタイム権限（アプリが許可をリクエストした際に、プロンプトがユーザーに表示されるもの）を自動的にリセットするので、ユーザーのプライバシー保護に役立ちま	2021年10月から	https://android-developers-jp.googleblog.com/2021/10/making-permissions-auto-reset-available.html?m=1

	す。この機能は、Google Play 開発者サービス を搭載し、かつ Android 6.0（API レベル 23）以降を実行しているデバイスで自動的に有効化されます。		

（2）プライバシー サンドボックス

① プライバシー サンドボックスのスケジュール

- Chrome （ウェブ）- 2020年のプライバシー サンドボックス発表以来、提案、オリジントライアルを経て、2023年9月に広告APIがChromeに一般提供され、2024年1月からはChrome ユーザーの1%のCookieが無効化され、アドテク事業者は CMA[1] のガイドラインに沿った検証テストの結果を提出することになっています。その後 CMA の Standstill 評価期間を経て、2025年初頭にサードパーティCookieが段階的に廃止される予定です（最新のスケジュールはこちら）。
- Android - 2022年2月、Android でもプライバシー サンドボックスを開発することを発表しました。デベロッパー プレビューから始まり、2023年頭から Android 13でベータ テストを開始し、現在テストの対応デバイスを拡大中です。[2]

② プライバシー サンドボックスの取組の概要

- プライバシー サンドボックスの取組は、オンラインのユーザー プライバシー保護を強化しながら広告を含む重要なビジネス モデルをサポートするツールを企業や開発者に提供することを目的としています。デジタル事業を継続するだけでなく、無料でオープンにアクセスできるインターネットを維持することは、人々が公平に情報へアクセスできる環境を守ることにつながります。
- ウェブサイト間のトラッキングを制限するために、サードパーティCookieを廃止し、フィンガープリント[3]に代表されるような隠されたトラッキングを制限します。またADIDなどの識別子を使用することなくユーザーのプライバシー保護を強化する技術開発を目指しています。具体的には、差分プライバシー、K-匿名性、デバイス上でのストレージ及び演算、信頼される実行環境（Trusted Execution Environment（TEE））、データ アカウンタビリティ ツールなど、多くのプライバシー強化技術（Privacy Enhancing Technologies（PETs））を活用しています。これらの技術を組み合わせることで、ユーザー情報を保護し、開発者に有用な機能を提供することができます。

---

[1] Competition and Markets Authority

[2] デバイス レベルの識別子を必要とせず、さまざまなデベロッパーのアプリでユーザーレベルのトラッキングを制限できる効果的なソリューションを開発することを目指しています。ADID のポリシー変更については現時点では発表されていませんが、今後の変更については事前に十分な告知を行います。

[3] 個人を識別するためにウェブサイトがブラウザに要求して取得する、ユーザーのソフトウェアやハードウェアに関する情報

- プライバシー サンドボックスはオープンな取組です。2020 年から始まった新たな技術の提案、機能テスト、一般提供など、各段階で W3C[4] や github な[5]どの公なフォーラム上でエコシステムの様々な関係者と議論し、これまでに 3100 を超えるフィードバックをいただきました。エコシステム全体にとって役立つものにするには、オープンなコラボレーションは必要不可欠だと考えています。
- また規制当局や業界団体とも対話を重ねています。イギリスのCMAに対して透明で公平な開発を担保するために公にコミット（英語）しています。重要な点は、Google の広告製品やサイトを優遇しないようにすることであり、CMA 及び ICO[6] の監督の元に開発が進められます[7]。このフレームワークはグローバルに適用しています。日本の関係省庁や業界団体とも対話を重ねています。

  ※ プライバシー サンドボックスはオープンな取組であり、他のブラウザにも開放されています。W3C上で、2021 年に Private Advertising Technology Community Group (PATCG) が作られ、広告をサポートするウェブの機能や API 、ユーザー保護について議論されています。PATCG は Apple、 Mozilla、 Microsoft、 Google などのブラウザが参加しています。

  ※ これまでアップル社が iOS のブラウザに対して設けていた制限により、プライバシー サンドボックスは Chrome ブラウザを含めiOSでは現在利用できません。

[4] World Wide Web Consortiumは、ウェブで使用される各種技術の標準化を推進するために設立された標準化団体、非営利団体
[5] GitHubは世界中のプログラマーによって使われている、プログラムのソースコードを、オンラインで共有・管理するサービス
[6] Information Commissioner's Office
[7] CMA 及び Google によるエコシステムからのフィードバックを含む四半期ごとのレポートはこちら

- サードパーティ Cookie が廃止され、隠されたトラッキングや ADID が制限されても企業や開発者が事業継続ができるよう、主要な活用事例に合わせて 20 を超える専用技術を用意しています。第 1 回利用者情報に関するワーキンググループにおいて、Topics API 、Protected Audience API 、及び Runtime SDK についてご紹介があったと承知しておりますが、広告関連 API だけではなく、ユーザーログイン、コンテンツのパーソナライズ、不正行為検知など、技術は多岐にわたります。スマートフォン上では、Chrome とアプリの両方が対象となるため、両方の技術について以下に記述します。

API / 専用技術		**概要**
プライバシー保護強化する広告関連 API		アプリとウェブで共通のコンセプトですが、実装技術は異なります。必要最低限の情報を必要な事業者に提供する、デバイス上の保存や演算、データの集計やノイズ化などの技術を組み合わせることでユーザープライバシー保護を強化しています。
ウェブおよびアプリ向け	Topics API	[ウェブ] Topics は、ユーザーのウェブ閲覧履歴に基づいて、ブラウザがそのユーザーの関心の高いカテゴリを推測します。Topics を使うと、サードパーティ Cookie のように、訪問した特定のサイトの情報がウェブを横断して共有されることがなくなります。Chrome 上で、トピックの表示、不要なデータの削除、無効化を設定できます。 [アプリ] Topics は、ユーザーのアプリ使用状況に基づき、そのユーザーの関心の高いカテゴリを推測します。アプリや広告プラットフォームは、Topics を使用することで、ユーザーにとって関連性の高い広告を表示できます。カテゴリのトピックの選定はユーザーの端末上だけで実行されるため、ユーザーが使用しているアプリに関する情報が外部の第三者と共有されることはありません。また、ユーザーは自身のデバイスでトピックを確認したり管理することができます。
	Protected Audience API	[ウェブ] Protected Audience API は、サードパーティ Cookie に依存することなくリマーケティングを可能にする、つまりこれまでに関心を持ったサイトや商品をユーザーに再提案する新しい方法です。ウェブ ブラウジング中にユーザーが広告主のサイトにアクセスしたとき、そのサイトからユーザーのブラウザに対して、今後もこのユーザーに同じ広告主の広告を表示したいと通知できます。それだけでなく、ユーザーに表示したい具体的な広告や広告の表示に対して支払える金額などの情報も、ユーザーのブラウザと直接共有できます。このような通知が行われた後でユーザーが広告スペースのあるウェブサイトにアクセスすると、ブラウザのアルゴリズムにより、表示できる広告について情報が提供されます。 [アプリ] Protected Audience API では、アプリのデベロッパーが定義する「カスタム オーディエンス」とアプリ内のインタラクション履歴に基づいて広告を表示する新しい方法が導入されま

		す。これらの情報および関連付けられた広告はローカルに保存されるため、ユーザーの識別子が外部の関係者と共有されることはありません。これにより、企業はプライバシーに配慮した方法で既存の顧客にリマーケティングできるようになります。
	Attribution Reporting API	[ウェブ] マーケターは現在、個人のウェブ閲覧行動や広告効果に関するデータを収集するために、サードパーティ Cookie を活用しています。広告主がユーザーのプライバシーを保護しながら関連性の高い広告を掲載し、その効果を検証できるように、プライバシー サンドボックスはサードパーティCookie を新たな効果測定ツールやレポートツールに置き換えて、異なるウェブサイトを横断して個人が識別されないようにします。これらに関連する提案は複数あります。 [アプリ] 現在、マーケターは、広告効果を評価するために、広告 ID などのクロスアプリ識別子やデバイス識別子を利用しています。Attribution Reporting API は、現在の測定方法をユーザー単位でトラッキングする仕組みに依存しないソリューションに置き換え、ユーザーのプライバシー保護を強化する取組です。
隠されたトラッキングの制限		
アプリ向け	Runtime SDK	サードパーティの広告コードをアプリのコードから分離して実行するためのプロセスを提供します。これにより、サードパーティの広告プロバイダーがアクセスできるアプリとそのユーザーデータは制限され、ユーザーにより高いセキュリティを提供し、プライバシー保護を強化することができます。
ウェブ向け	User-Agent Client Hints	User Agent 文字列は、ユーザーが訪問するサイトが正しく表示され機能するために、ユーザーが使用するブラウザとデバイスに関する詳細を識別させるためのものです。しかし、User Agent 文字列は、いわゆるパッシブ フィンガ プリントに使われてしまう重大な問題もあります。User-Agent Client Hints API は、サイトが必要な情報を直接リクエストできるようにし、最終的にはUser Agent 文字列に含まれる詳細情報を減らして、インターネット上で共有されるユーザー情報を制限しま す。
	User-Agent Reduction	User-Agent Reduction は、パッシブフィンガープリントに使用される可能性のあるUser Agent 文字列に含まれる識別情報を、最小限に抑える取組です。
	DNS-over HTTPS	DNS-over HTTPS は、ドメイン ネーム システム（DNS）のクエリと応答をHTTPS メッセージ内にエンコードすることで暗号化するプロトコルです。これにより、ユーザーが訪問したサイトを攻撃者が把握したり、ユーザーをフィッシングサイトに誘導するのを防ぐことができます。

	IP Protection	IP Protection は、IP アドレスを隠すことを目指すプライバシー サンドボックスの提案です。最低でもIP アドレスが確実に隠されることを保証し、サイトが直接接続を希望する場合は、追加の作業を行ってIP アドレスを悪用しないことを証明できるようにします。
	Storage Partitioning	Storage Partitioning は、サイト上の埋め込みサービス、つまりサードパーティのコンテキストで使用されているものがある場合、ストレージや通信に使用されているいくつかのウェブ プラットフォーム API をパーティション化します。これにより、既存のサイトとの互換性をほぼ維持したまま、ウェブをより安全でユーザーのプライバシーが保護された状態に保つことができます。
	Network State Partitioning	ブラウザのネットワークリソース（接続、DNS キャッシュ、代替サービスデータなど）は、一般的に幅広く共有されています。Network State Partitioning は、これらのリソースがファーストパーティのコンテキスト間で共有されないよう、この共有された状態の大部分をパーティション化します。このため、各リクエストには、リソースを再利用するために致する必要のある「ネットワークパーティションキー」が追加されます。 この追加のキーにより、サイトが他のサイトをロードして学習した共有リソースをメタデータにアクセスできないようにし、ユーザーのプライバシーを保護します。
	バウンストラッキング対策	バウンス トラッキング対策は、コンテキストをまたいでユーザーを認識するバウンス トラッキングの機能を抑制または排除します。ステートフル リダイレクトを使用して実装されている、ユーザーにとって重要なユースケースのサポートは維持されます。
ウェブサイト間におけるプライバシー保護の強化		
ウェブ向け	Related Website Sets	ウェブサイト間トラッキングを制限する現在の試みは、一般的な状況に対応していません。例えば、組織によっては、異なるドメインの関連サイトを持ち、それらのドメイン間で動画のようなリソースをロードしたり、別のアクティビティを実行する必要があるかもしれません。 このプライバシー サンドボックスの提案では、こうした同じエンティティに属するドメインを「Related Website Set」として宣言することができます。そのRelated Website Set 以外のドメインでは、ユーザーのプライバシーを保護するため、情報のやり取りが制限されます。
	Shared Storage	ウェブサイト間トラッキングを防ぐため、ブラウザはキャッシュやlocalStorage といったあらゆる形態のストレージを分離しはじ

		めています。しかし、共有ストレージを必要とする正当なケースも多く、Shared Storage API の提案はそれらに対応することを目的としています。この提案では、パーティション化されていない「共有ストレージ」を提供し、その中のデータは安全な環境でのみ読み 取れるようにする予定です。
	CHIPS	チャット ウィジェットや埋め込み地図などの埋め込みサービスは、正しく動作するために、指定されたサイトでのユーザーのアクティビティについて知る必要がある場合があります。プライバシー サンドボックスが提案するCHIPS (Cookies Having Independent Partitioned State) は、パーティション化された Cookie を使って、必要なCookie が指定されたサイトと埋め込みウィジェット間でだけ「サイトを横断して」動作することを許可するようブラウザに指示するものです。
	Fenced Frames	Fenced Frame は、iframe のような埋め込みタイプのフレームで、ホストページと通信することはできません。Fenced Frame API は、トップサイトと識別子を結合できなくなるため、パーティション化されていないストレージに安全にアクセスできるようになります。
	Federated Credential Management	Federated Credential Management は、サードパーティ Cookie を使わずに ID を連携します。このAPI は、サインインからサインアウト、セッションが失効した際の再度のサインインなど、サードパーティ Cookie が使われる場合や場所で、ID の連携に必要な手段を提供します。
スパムや不正行為対策		
ウェブ向け	Private State Tokens	Private state token は、ウェブサイトがボットや悪意のある攻撃者を実際の人間のトランザクションと区別 するためのものです。サイトは、アカウントへの定期的なログインなど、サイト上でのユーザーの行動に基づいて、そのユーザーのブラウザに対して Private state token を発行することができます。また、他のサイトがボットか実際の人間かを確認したい場合には、そのPrivate state token でユーザーが正当であることを確認できます。Private state token は暗号化されているため、個人を識別したり、信頼できるイ ンスタンスと信頼できないインスタンスを接続してユーザー アイデンティティを検出したりするこ とはできません。

以上