ICTサービスの利用環境の整備に関する研究会
利用者情報に関するワーキンググループ（第27回）

参考資料27-1

アプリ・ウェブブラウザにおける利用者情報の取扱いの比較

三菱総合研究所

モビリティ・通信事業本部　デジタルコンテンツ・データ戦略グループ

2025/6/24

目次

調査事項

- この資料では、以下の事項について調査を行った。

資料18－2

ウェブサイトに関する検討の進め方（案）

ウェブサイトへの対象拡大に関する検討については、WG報告書において「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。」とされている。

考え方

- SPSIは、スマホアプリの利用者情報の適正な取扱いに関して記載しており、スマホやPCからブラウザを通じたウェブサイト閲覧の際の利用者情報の取扱いについては対象に含んでいない。
- ウェブサイトへの対象拡大に関する検討の準備として、まずは、例えば以下のような事項について調査し、ヒアリング等も踏まえた上で、一定の整理を行っていくこととしてはどうか。

調査する事項（例）

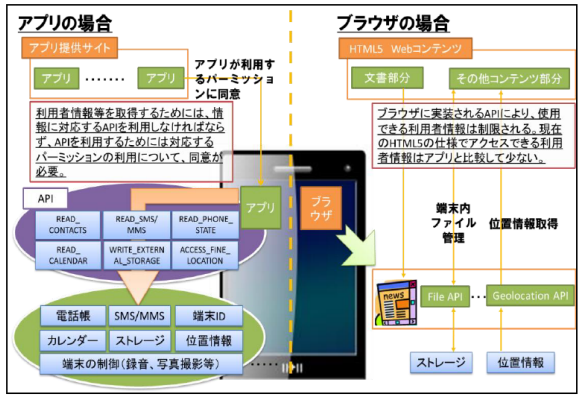
調査事項

アプリケーションとブラウザの間で、

- **利用者情報を取得する主体**にどのような差異があるか。
- **取得する利用者情報の種類**にどのような差異があるか。
- **取得する利用者情報の利用目的**や**取扱い方法**にどのような差異があるか。

→ウェブサイトを対象とするとした場合、SPSIと同じ内容が関係事業者に適用される場合とそうでない場合があるのではないか。

（参考）SPI策定当時（2012年）



「スマートフォン プライバシー イニシアティブ」（平成24年８月）P74
図表5-3 アプリケーション及びブラウザがアクセス可能な情報等の違い

出典：利用者情報に関するワーキンググループ（第18回） 資料18-2
https://www.soumu.go.jp/main_sosiki/kenkyu/ICT_services/02kiban18_02000371.html

1. 利用者情報の全体像の確認

1. 利用者情報の全体像の確認

- **比較に先立ち、スマートフォンにおいて利用者情報としてどのような情報が生成されているか、全体像を整理・分類した。**
- **利用者情報の生成箇所・利用目的に着目して全体を抜け漏れのないように把握し、スマートフォンにおける利用者情報の取扱い状況について整理する上での前提とした。**

1.1 生成箇所の整理

- スマートフォンにおける利用者情報について、大きな漏れなく検討するために、どこでどのような利用者情報が生成しているかを整理した
- デジタル市場競争会議「モバイル・エコシステムに関する競争評価　最終報告」（2023）での整理結果を踏まえた上で、端末やサービスの構造・関係も考慮して整理した

1.2 利用目的の整理

- スマートフォンにおける利用者情報について、どのような利用目的で取り扱われているのかを、国内外の政府や業界団体の報告書を参照して整理した

1.3 整理結果

- 上記の整理結果を踏まえ、スマートフォンにおける利用者情報について生成箇所別に細分化し、利用目的を踏まえて端末や利用者の特定可能性を整理した

1.1 オンライン環境における利用者情報（生成箇所の整理）

※利用者情報がどこで生成され、どのように利用され得るかを検討するために、情報の生成箇所（レイヤ）の全体像を整理した。

*1 スマートフォンを想定しているが、PCの場合もほぼ同様（相違点：各種センサがカメラ、マイク等に限られる、セキュアエレメントが無いことが多い、アプリケーションはアプリストアを介さずに直接インストールすることが多い、等）

*2 OS提供事業者によるものと、サードパーティによるものとがある

*3 アプリはサービス提供用サーバと交信してサービス提供するが、ここではサーバは省略

出典：デジタル市場競争会議「モバイル・エコシステムに関する競争評価　最終報告」（2023）図1-3-1（p.21）も踏まえて作成
https://www.kantei.go.jp/jp/singi/digitalmarket/kyosokaigi/dai7/siryou2s.pdf

1.2 オンライン環境における利用者情報（利用目的の整理）

- 利用者データの利用目的は多岐にわたるが、ここでは以下のように集約して整理した。
- 多くの場合、利用者自身や、端末・サービスの提供者自身による利用を目的としているが、「分析・改善」「広告・マーケティング等」においては、第三者によるデータ利用も多く行われている。

	利用目的	細分類・具体例
	契約・取引、ユーザ管理	端末の購入、サービス等の利用契約、ユーザ管理（顧客管理）等のため
	ユーザによる利用	ユーザによるサービス等の利用のため（直接的・主体的利用に限らず、間接的に必要な場合も含む）
	サービス等提供	サービス等（サービス、サイト、アプリ等）を提供するため
	サービス等運用・管理	サービス等やシステムの運用管理のための各種測定、セキュリティ対策、不正検知、等のため
★	分析・改善	サービス等の利用状況分析、効果測定、改善、広告効果の測定・レポート等のため
★	広告・マーケティング等	広告（ファーストパーティとして、サードパーティとして）、利用回数制限、広告対象のターゲティング、マーケティング、利用者ごとのパーソナライズ、利用者のプロファイリング等のため
	その他	法令遵守や法的義務履行等のため

注：上記分類を作成するに際して、モバイル・エコシステム/モバイル広告、デジタルプラットフォームに関する複数の文献を参照した。

例1：IAB Tech Lab, “New Privacy Taxonomy”, https://iabtechlab.github.io/fideslang/ 【参考1】参照

例2：デジタル市場競争会議,「モバイル・エコシステムに関する競争評価　最終報告」, https://www.kantei.go.jp/jp/singi/digitalmarket/kyosokaigi/dai7/siryou2s.pdf 【参考2】参照

例3：ACCC, “Digital platforms inquiry - final report”, https://www.accc.gov.au/about-us/publications/digital-platforms-inquiry-final-report 【参考3】参照

1.3 オンライン環境における利用者情報の整理

- 利用者データについて、生成個所（1.1）及び利用目的（1.2）を踏まえて以下のように整理した。

生成箇所（レイヤ）	カテゴリ（レイヤの細分類）	利用者・端末との対応関係・特定性
ユーザ	● ユーザ作成情報 ● ユーザ登録情報	• 利用者自身が作成（撮影、録音、制作、投稿等）し、利用する情報 • 利用者自身が登録する情報
オンラインサービス	● ウェブサイト、アプリ	• アプリ、ウェブサイト（ログイン）：利用者の利用履歴 • ウェブサイト（非ログイン/アカウント非保持）：ブラウザの状況、行動・閲覧履歴（ブラウザを介した間接的な関係） ※ スマートフォンでは、事実上利用者端末とブラウザが直接的な関係
広告ネットワーク	● ウェブサイト、アプリ	• アプリ（SDK）：広告の閲覧履歴 • ブラウザ（タグ、クッキー等）：広告の閲覧履歴（他サイトも含む）
アプリケーション	● アプリ	• スマートフォンではアプリが利用者端末との関係を保持、又アカウントを作成することからユーザとの関係も保持
ブラウザ	● ブラウザ	• スマートフォンでは利用者端末がブラウザアプリとの関係を保持 ※ PCでは利用者端末・OSはブラウザとの関係を必ずしも保持しない
アプリストア	● アプリストア	• OSを介して利用者端末との関係を保持
OS	● OS	• 利用者端末との関係を保持（例：スマートフォンの契約、PC・OSのオンラインユーザ登録）
アクセスプロバイダ（通信キャリア、ISP）	● サービス ● 契約者の情報	• 契約情報によりユーザとは直接的な関係が保持される • スマートフォンではキャリアにおいて端末も特定される場合が多いが、ISPでは端末は特定していない
端末・ハードウェア（デバイス）	● 通信アダプタ ● センサ ● セキュアエレメント ● 端末本体	• 端末購入により直接的な関係が保持される（スマートフォンでは契約においてユーザ登録を行う：PCでもユーザ登録を行う場合あり）

注：赤字は、利用者や利用者端末との直接的な関係を保持しない・特定できない場合

2. アプリ・ブラウザにおける利用者情報の取扱いの比較

2 アプリ・ウェブブラウザにおける利用者情報の取扱いの比較

- **スマートフォンのアプリとウェブブラウザにおける利用者情報の取扱いを具体的に整理した上で、両者を比較分析した。**

2.1 取得可能な利用者情報の比較

- アプリとウェブブラウザにおいて取得可能な利用者情報・デバイス情報の種類について、技術的に可能か否かという観点で整理し比較した

2.2 利用者情報取扱いの概観

- ブラウザ及びアプリにおいて利用者情報がどのように取り扱われているかについて、具体的に整理した
- ウェブサイト運営者やアプリによるサービス提供者などの1st Partyにおける取扱いに加え、タグ（ウェブサイト）やSDK（アプリ）を用いた3rd Partyによる収集・取扱いを整理し、それらについてどのような制限や管理が行われているかについても記載した
- ユーザ端末（図の左端）に関して、以下を図示する形で整理した
  - ユーザ端末内でのデバイスデータ取得（例：センサ情報、等）
  - 1st Partyによるデータ取得、タグやSDKの送信
  - 3rd PartyによるタグやSDKの提供、タグやSDKを通じたデータの取得
  - それらに対する制限・管理の有無

2.3 利用者情報の取扱いの比較

- 上記の整理結果に即して、アプリとウェブブラウザにおける利用者情報の取扱いについて、以下①～⑥の視点で比較を行った（①～⑥は2.2の整理図中にも示した）
  - ① 取得可能な利用者情報
  - ② 第三者による取扱いとルール
  - ③ 利用者情報の取扱いのガバナンス
  - ④ 利用者情報の取扱いの透明性義務
  - ⑤ 同意の取得義務
  - ⑥ 利用者による状況把握

2.1 取得可能な利用者情報の比較（技術的な取得可能性）

- ブラウザもアプリの一種であり、他方アプリもサーバとの通信に関する情報を取得しているので、技術的に取得可能な情報としては両者に大きな差はない。

◎：自らのアプリ・サイトで（アカウント作成やログインなしでも）取得可能　○：ログインしている場合に取得可能　△：情報の種類による　●：デバイスから取得可能（条件・制限等あり）

区分	情報項目	アプリ	ブラウザ
アプリ・サイトの利用・閲覧に関する情報	閲覧履歴・検索履歴	◎	◎ *6
	使用状況データ（操作、広告閲覧、その他アクティビティ）	◎	◎
	診断データ（クラッシュログ、パフォーマンス、その他）	◎	◎
	フォーム等入力情報	◎	◎ *1
（アプリ・サイトの）アカウント情報	アカウント・ID・PW等	○ *2	○ *2
	連絡先等（登録している場合）	○ *2	○ *2
	サービス利用・購入等の履歴	○ *2	○ *2
デバイスの情報（識別子）	デバイスID（OS生成ID、端末識別番号・ID、加入者ID、等）	×	×
	デバイス広告ID、Cookie等	● *3	●
デバイスの情報（センサ：対応センサを搭載している場合）	位置情報	● *3	● *4
	周囲の状況（環境光・照度、気圧、近接物体、等）	● *3	● *4
	その他センサ計測情報（バッテリ状態、デバイス/スクリーンの向き、等）	● *3	● *4
	ユーザの身体（手や頭部の動き等）	● *3	● *4
デバイスのユーザに関する情報	デバイス用認証情報（ID・PW・生体認証情報、等）	×	×
	電話帳・アドレス帳、ソーシャルグラフ等	● *3	×
	カレンダー・スケジュール	● *3	●
	通話履歴・SMS履歴	● *3	×
	ユーザコンテンツ・ユーザ作成ファイル	● *3	●
	ヘルスケア／フィットネス情報	○ *5	○ *5
	財務情報（決済手段、決済履歴、等）	○ *5	○ *5
	機密情報（直接取得、推知）	△	△
通信状況に関する情報	ホスト情報（端末ホスト名、IPアドレス、OS・ブラウザ、ポート番号、等）	◎	◎
	デバイスのディスプレイ情報	◎	◎
	通信・セッション情報（アドレス、プロトコル、ステータスコード、タイムスタンプ、リファラ、等）	◎	◎
その他の情報	上記以外の情報	△	△

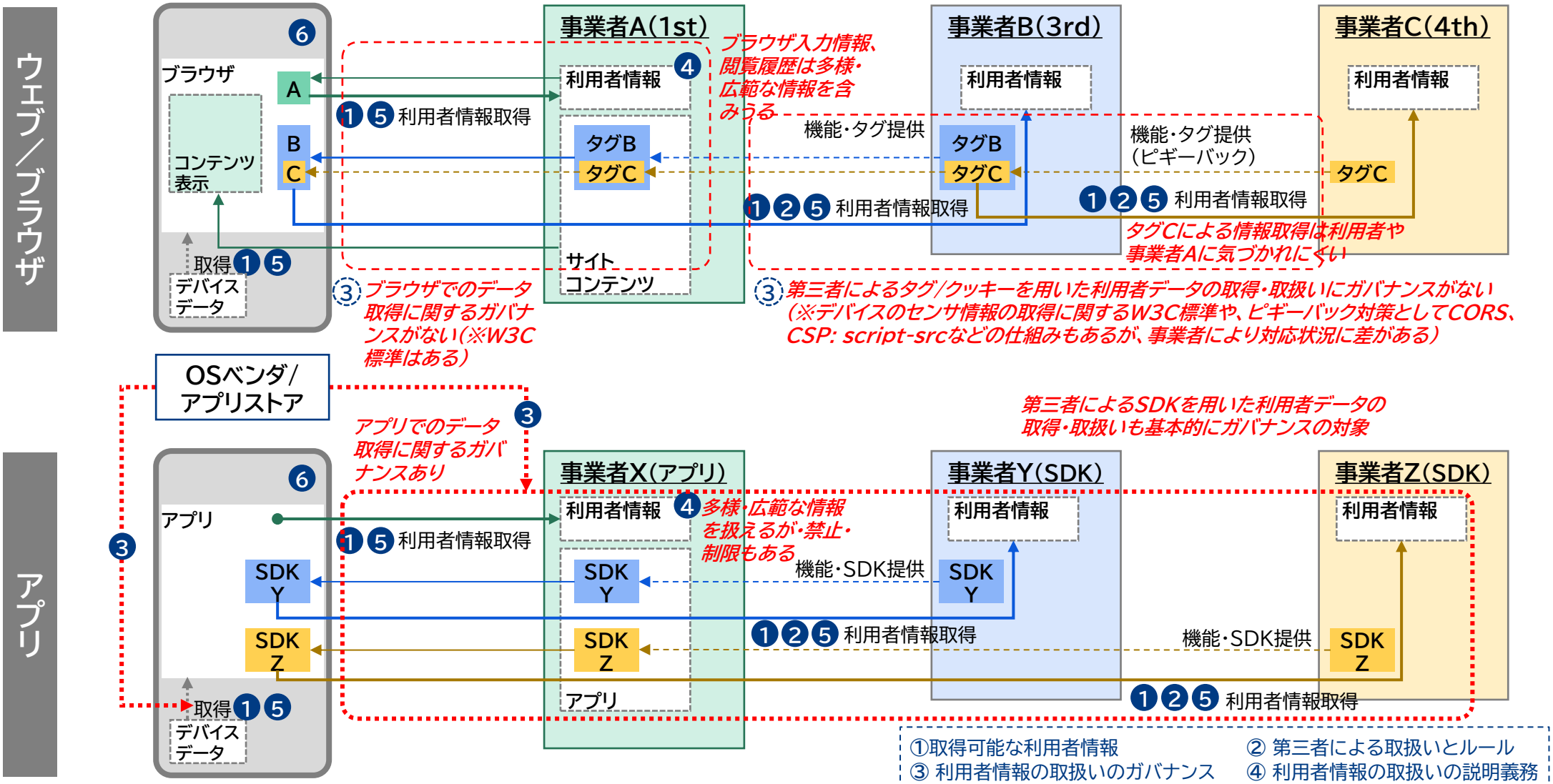
*1　入力したが未送信のデータはアプリでは取得されないが、ブラウザでは取得可能な場合がある

*2　登録してログインしている場合
*3　OS/アプリストアが定めるルールに従って取得する場合
*4　W3C標準により、ブラウザにてユーザのパーミッションを取得するダイアログが表示される
*5　自サイト/サービスで登録・入力・取得している場合
*6　Cookie等識別子を用いる場合あり

出典：各種資料より作成

2.2 アプリ及びウェブ/ブラウザにおける利用者情報取扱いの概観

- ウェブ/ブラウザとアプリにおける利用者情報の取扱いの全体像（概略的な流れ）をそれぞれ整理した。



出典：各種資料より作成

2.3 アプリ及びウェブ/ブラウザにおける利用者情報の取扱いの比較

項目*1	アプリ(アプリ提供者/サービス提供者)	ブラウザ(ウェブサイト提供・運営者)
① 取得可能な利用者情報(技術的な可能性)	**技術的には多様な端末情報・利用者情報をアプリ・SDKを通じて取得可能** • 技術的には多種類の端末データ(センサデータも含む)、利用者データを取得可能 • アプリがアカウントと紐づいている場合が多いと考えられるが、アカウントを作成せずに使用するアプリもある • アプリ上での入力データは、サービスサーバ側に送信されていない場合には取得されない	**ブラウザもアプリの一種であり、技術的に取得可能な情報は、基本的にはアプリとほぼ同様** • 技術的に取得可能な情報は、アプリの場合とほぼ同じと考えられる • ブラウザ自体はユーザ(アカウント)と直接紐づいていないが、他サービスも含めログインしているサービスのアカウントと紐づいた形で情報が取得され得る • ブラウザ上での入力データは、サーバ側に送信されていないくてもクッキー等により取得される場合がある(実際にどの程度取得されているかは不明)
② 第三者による取扱いとルール	**第三者による取得が可能:ルール(OSベンダ/アプリストア)及び自主ルール(業界団体等)あり** • SDK提供者が取得可能 • OSベンダ/アプリストアが、アプリ提供者やSDK提供者に対して説明・同意取得義務や禁止・制限等を設けている • 業界団体等(アプリ開発・提供等、広告)による自主ルール・ガイドが存在	**第三者による取得が可能:自主ルール(業界団体等)あり** • タグ(JavaScript等)提供者が取得可能 • タグの重層化(ピギーバック)により、利用者の情報が密かに取得される可能性がある • ウェブサイト提供者・運営者に対する義務・禁止・制限等は特段ない • 業界団体等(広告)による自主ルール・ガイドが存在する
③ 利用者情報の取扱いのガバナンス	**OSベンダ/アプリストアによるガバナンス、業界の自主的ルール、がそれぞれある** • OSベンダ/アプリストアは、アプリやSDKによるデータ取扱いについて、禁止・制限事項や、アプリ提供者による説明・同意取得の義務を定めており、従わないアプリはアプリストアでの公開が認められない • アプリ提供者は、利用するSDKについての管理が求められる • 他方、あくまで私企業(海外事業者)によるガバナンスであることについての留意も必要 • 業界団体等(アプリ開発・提供等、広告)による自主ルール・ガイドも存在	**ツールや仕組みが提供されており、業界の自主的ルールもある** • ブラウザがサードパーティクッキーの利用を制限している場合がある • ブラウザによる端末のセンサ情報の取得を制限・制御する仕組み(W3C標準)や、サイト側で他ドメインとの情報共有や他ドメインのタグによる情報取得を制限する仕組みがある • ブラウザ及びタグによる利用者データの取得や第三者への提供については、ブラウザ及び各ウェブサイトがルールを定め管理・実行する仕組み • 大手事業者が運営するウェブサイトや主要なブラウザでは、利用者データを保護するための対策が基本的には取られていると考えられる • 業界団体等(広告)による自主ルール・ガイドが存在する
④ 利用者情報の取扱いの説明義務 ⑤ 同意取得義務	**説明や同意取得をアプリ提供者に義務付けるルールがある** • アプリによる利用者データの取扱いについて、説明や同意取得の義務が規定されている(OSベンダ/アプリストアによる義務付け)	**ウェブサイト提供者による説明や同意取得は、サイトにより異なる** • サイトが取得する個人情報についてはプライバシーポリシーで説明し、必要な場合には同意を取得している(同意取得方法にはバリエーションあり) • クッキーについての説明や同意取得についても粒度・詳細度の差がみられる
⑥ 利用者による状況把握	**利用者が把握可能** • 当該アプリでのデータ取扱いに関する説明により、利用者が把握可能	**利用者が把握可能な程度はサイトにより異なる** • 説明状況はサイトにより異なり、利用者が把握できる程度・難易度にも差がある

*1　①～⑥について、前ページも参照

3. 調査結果

3.1 調査結果(サマリー)

- **利用者情報の取扱いにおいて、取得主体、取り扱う情報の種類、利用目的及び取扱い方法について、アプリとウェブ/ブラウザの間にどのような差異があるかを調査・比較した。**

	アプリ	ウェブ/ブラウザ
取得主体	● アプリ提供者　● SDK提供者	● ウェブサイト運営者　● タグ提供者　● ブラウザベンダ
取り扱う情報の種類	● アプリやSDKを通じて比較的多種類の情報を取得可能	● ブラウザもアプリの一種であり、技術的に取得可能な情報は、基本的にはアプリの場合とほぼ同様(実際にどこまで取得するかはブラウザやサイト運営者による)
	● アプリがユーザ(アカウント)と紐づいている場合が多いと考えられ、その場合にはアプリ提供者・SDK提供者は、利用履歴の取得や、複数の情報間の関連性を把握可能だが、アカウントを作成せずに使用するアプリもある	● ブラウザ自体はユーザ(アカウント)と直接紐づいていないが、他サービスも含めログイン状態で使用する場合、ログインしているサービスのアカウントと紐づいた形で情報が取得され得る ● クッキー等識別子を用いることで、アカウントと紐づいていない場合でも、利用履歴・閲覧履歴を取得可能な場合あり
	● 端末のセンサの情報を、API経由で取得可能	● 端末のセンサの情報を、API経由でブラウザが取得可能
	● SDKによりデータ取得やユーザトラッキングが可能	● タグを用いて、データ取得やユーザトラッキングが可能 ● タグの重層化(ピギーバック)により、利用者の情報が密かに取得される可能性がある
	● アプリやサードパーティSDKによる取扱いについて、OS・アプリストアによる制限(ルール、エンフォースメント)が存在 ● 業界団体等の自主ルール・ガイドも存在	● 他のサイト/ドメインとの情報共有やセンサ情報の取得、サードパーティクッキー等を制御・制限する機能も実装されているが、実際に用いるかはウェブサイト提供者やブラウザベンダが決定 ● 業界団体等の自主ルール・ガイドも存在
利用目的・取扱い方法	● 基本的には大きな差異はない:サービスの提供に必要な情報の取得、利用者の興味・関心・属性等の取得・分析(サービスの改善、マーケティング、ターゲティング/プロファイリング、等)、広告配信・効果計測、レコメンデーション、等	
	● アカウント保有者への働きかけが主	● アカウント保有者への働きかけ(ログインして利用するもの) ● アカウントをもたない利用者への働きかけ(サイトへのアクセス経緯や閲覧履歴等に基づくリードジェネレーション等)

3.2 調査結果（調査項目別の比較）

青字：ウェブ/ブラウザの方が相対的に問題が少ない考えられる点
赤字：ウェブ/ブラウザの方が相対的に注意が必要と考えられる点

調査項目		アプリ	ウェブ/ブラウザ
取得主体		アプリ提供者／SDK提供者	ウェブサイト運営者／タグ提供者／ブラウザベンダ
技術的可能性	サービス提供において取得する情報	アプリ・SDKにより比較的多種類の情報を取得可能	ブラウザもアプリの一種であり、技術的に取得可能な情報は、基本的にはアプリとほぼ同様
	サービスの利用・閲覧履歴	ユーザ（アカウント）と紐づいている場合には、利用履歴の取得や、複数の情報間の関連性を把握可能	クッキー等識別子を用いることで、アカウントと紐づいていない場合でも利用履歴・閲覧履歴の取得が可能な場合もある
	デバイスのセンサ情報	センサのAPIを用いてアプリが取得可能	センサのAPIを用いてブラウザが取得可能
	フォーム等入力情報	ユーザがサーバに送信した情報については取得することが可能	フォームに入力した情報は、未送信であっても取得可能（個々のサイトが未送信情報を実際に取得しているかは不明）
	ユーザアカウント情報	アプリインストール時に取得している	ログインしている場合や他サイトでのログイン情報と照合している場合には把握可能
	第三者による情報取得・トラッキング	SDKを用いることで、データ取得・ユーザトラッキングが可能	タグを用いることで、データ取得・ユーザトラッキングが可能 タグの重層化（ピギーバック）により、利用者の情報が密かに取得される可能性がある
ガバナンス/エンフォースメントによる制限	ルール・ツール	OS・アプリストアによる制限（アプリが遵守すべきルール策定、個別アプリの審査、ルールに従わないアプリはストアでは取り扱わない） 業界団体等による自主ルール・ガイド	センサ情報取得のW3C標準（※主要ブラウザにて実装） HTML機能（JavaScriptによる他サイトとの情報共有を制限する機能）（※使用するか否かはサイトが決定） 業界団体等による自主ルール・ガイド
	第三者による情報取得・トラッキング	サードパーティSDKに関するポリシー（OS・アプリストアが規定）への準拠 業界団体等による自主ルール・ガイド	サードパーティクッキーその他の識別子に関するブラウザのポリシー（実際には使用されている場合もある） 業界団体等による自主ルール・ガイド
ユーザの関与可能性	説明・同意取得	個々のアプリにおけるプライバシー説明義務（アプリストアが定める方法）	ブラウザがAPIを通じてデバイスのセンサ情報を取得する場合には同意取得を行う（W3C標準）
	確認・設定	アプリインストール時の同意取得 個別アプリ及びOSにおけるプライバシー設定・コントロール機能	サイトアクセス時のクッキーダイアログ表示（通知、同意取得、設定）（※サイトにより異なる） サードパーティクッキーや広告プライバシーに関する設定・コントロール機能

3.3 アプリ及びウェブ/ブラウザにおける情報取得範囲とリスク・対策

- **単独のアプリやサイトでの情報取得と横断的に取得する場合について、懸念されるリスクや現状で提供されている対策等を比較。ウェブ/ブラウザの場合も、横断的に取得される場合は注意が必要。**

	情報取得範囲	情報取得手段（取得主体）	取得可能な情報	利用者の把握・分析	主なルール・ガイド等
アプリ	単独	• アプリ（アプリ提供者） • SDK（SDK提供者）	• アプリでの利用履歴 • 相対的に多様な端末情報・利用者情報を取得可能	• 対象アプリを利用する個々の利用者のプロファイル・履歴が把握される • 対象アプリにおける利用者行動分析、アプリ・サービス改善、マーケティングに利用可能	• OSベンダ/アプリストアが定めるルール（アプリ・SDKがデバイスから取得する情報に関する情報に関する制限や説明・同意取得義務） • 業界団体等の自主ルール・ガイド（例：MCFガイドライン、JIAAガイドライン） • SPSI
	横断（複数アプリにまたがる）	• SDK（SDK提供者）	• SDKを用いたアプリにおける利用者に関する情報（取得情報はSDKごとに決まっている）	• 利用者の行動履歴を複数アプリにまたがり取得可能 • 利用者に関するより多面的な分析も可能	
ウェブ/ブラウザ	単独	• ブラウザ（ウェブサイト運営者）	• 対象サイトでの閲覧行動・閲覧履歴やサイト・フォームでの入力情報が主 • APIを通じて端末情報を取得可能	• 対象サイトでの個々の利用者の行動が把握される • クッキー等識別子を用いることで、サイトでの行動履歴等も把握可能 • 対象サイトにおける利用者行動分析、アプリ・サービス改善、マーケティングに利用可能	• ブラウザによる制限（サードパーティクッキー） • 端末センサ情報の情報取得に関するW3C標準 • サイト間をまたがる情報共有・情報取得を制御する技術的仕組み • 業界団体等の自主ルール（例：JIAAガイドライン）
	横断（複数サイトにまたがる）	• ブラウザ（ウェブサイト運営者） • タグ（タグ提供者）	• タグが埋め込まれている各サイトでの利用者の閲覧行動・閲覧履歴	• 個々の利用者の行動履歴を複数サイトにまたがり取得可能 • 利用者に関するより多面的な分析も可能	

参考資料

関連箇所	参考資料名
1.2節	【参考1】スマートフォンにおける利用者データの分類例
	【参考2】広告で使用されるデータの分類
	【参考3】ユーザトラッキング技術（Cookie以外）の分類例
1.3節	【参考4】スマートフォンにおける利用者情報の性質と種類（※SPSI）
2.1節	【参考5】アプリが扱う可能性のある利用者情報（※iOSアプリの場合）
	【参考6】アプリが扱う可能性のある利用者情報（※Androidアプリの場合）
	【参考7】ウェブブラウザで直接取得可能な利用者情報（※主なもの）
	【参考8】モバイルデバイスのセンサとウェブのインタラクション
2.2節	【参考9】スマートフォンアプリにおける利用者情報取得・利用の例
	【参考10】ウェブブラウザにおける利用者情報取得・利用の例
2.1節、2.3節	【参考11】ウェブサイトにおける他ドメインとの情報共有の制限
3.1節	【参考12】利用者情報の取扱主体・取得手段・利用目的の比較

【参考1】スマートフォンにおける利用者データの分類例

メッセージングデータ	携帯電話キャリアが提供するメッセージングサービス(SMS、EMS、MMS)や電子メッセージ(チャット、メール)から取得した、受信者、送信者、配信日時、添付ファイルなどの情報を含むメッセージングログのことである。このようなメッセージングデータ(特にメッセージングログ)を用いて、スマートフォンユーザのプロフィールを特定・生成する研究は珍しいが、技術的には可能である。メッセージングログと通話ログの両方は、通話明細レコード(CDR)で利用可能である。CDRは暗号化された電話番号、基地局(BTS)のID、通話日時、通話時間、SMSメタデータで構成される。CDRを使用したユーザー識別やユーザー・プロファイリングでは、通話ログの詳細が多く含まれるため、通話ログの詳細が主に使用されるが、同様のアプローチでSMSメタデータを使用することも可能である。
デバイスデータ	デバイスとオペレーティング・システムに関するデータで、サード・パーティとは無関係のものである。IMEI、Wi-FiのMACアドレス、デバイスのシリアル番号で構成され、これらの情報は重要な識別子であり、これらの情報によって携帯電話の身元がすでに明らかになっている。このデータは、自分の身元を簡単に説明できる貴重なものであるため、いかなる漏洩からも保護されなければならない。そのため、IMEIのような情報は通常、アプリのインストール時にユーザーから明示的な許可を得た後でなければアクセスできない。デバイス・データを使ってユーザー・プロファイルを識別・生成しようとする研究は前代未聞である。
(U)SIMカードデータ	(U)SIMカードデータには、電気通信事業者によって一意に識別される特定のユーザー情報が含まれる。例えば、国際携帯電話加入者ID、ICカードID、携帯電話加入者識別番号などである。デバイス・データと同様に、(U)SIMカード・データを使ってユーザー・プロファイルを識別・生成しようとする研究は、そのデータの機密性ゆえに耳にしたことがない。
アプリケーションデータ	アプリケーションがアクセスできるデータのことである。アプリケーションは、コンフィギュレーション・ファイル、ログ、一時的なデータなど、実行するためのデータにアクセスする必要がある。これらのファイルを使用したユーザー識別やユーザー・プロファイリングも聞いたことがない。デバイス間でデータが非均質であることと、(特にWhatsAppやTelegramのようなアプリにおいて)アプリケーションレベルの暗号化が厚いため、攻撃者がこのデータを取得するために労力を割くことができず、代わりに他のデータソースを選択することができないことが、2つの理由の1つであると考えられる。
利用履歴データ	電話の利用に関連するログデータである。例としては、通話ログ、閲覧履歴ログ、ネットワーク接続履歴ログ、オペレーティングシステムのイベントログなどがある。ウェブ閲覧履歴、通話履歴、アプリケーションの動作、インストールされているアプリのセットなど、ユーザーやデバイスを特定するために利用履歴データを使用した研究がある。一方、通話ログやインストールされたアプリのセットなど、このデータを利用したユーザ・プロファイリングも行われている。
センサデータ	カメラ、GPS、コンパス、加速度計、マイクなど、スマートフォンに搭載されたセンサーによって生成されたデータのことである。加速度センサーは、歩行、ジョギング、階段昇降などの人々の日常活動を観察することによって、ユーザ識別とユーザ認証のために使用され、日常生活活動を認識するためのユーザープロファイリングのために使用された例もある。また、音声、位置情報、マルチタッチ、ロコモーションを利用して、スマートフォン上で継続的にユーザ識別サービスを実現するSenGuardプロジェクトが提案されている。また、軌跡とサンプリング点間の距離関数を観測するために、あるいはユーザ識別のために様々なデータソースからユーザの軌跡の類似性を観測するために、GPSモビリティデータが利用された例もある。
ユーザ入力データ	キーストロークやジェスチャーなど、ユーザーとスマートフォンとのインタラクションから作成される。キーストロークは、キーの保持時間、エラー率、ダイアグラフや持続時間、最後のキーからの時間、頻繁に使用するキー、頻繁に使用しないキーで分析され、スマートフォンのユーザーを識別するために使用された。また、タッチスクリーンのジェスチャーを利用して、ユーザを継続的に高い精度で識別できた例もある。

出典:“A review on smartphone usage data for user identification and user profiling”, 2021, https://www.researchgate.net/publication/353534370_A_review_on_smartphone_usage_data_for_user_identification_and_user_profiling

【参考2】広告で使用されるデータの分類

広告で使用されるデータ*1

豪州ACCC(オーストラリア競争・消費者委員会)のレポートでは、GoogleとFacebookがそれぞれ自身のユーザ(プラットフォーム外とプラットフォーム内)に関して収集したデータと、Google及びFacebook自身のオンライン広告の活動を通じて収集したデータとして、下記を挙げている:

サインイン/加入データ	データが収集されるのは、ユーザーがウェブサイトやアプリにサインアップしたり、オンラインに登録したりするときである。例えば、Gmail、Facebook、その他ユーザログインが可能なウェブサイトなど、さまざまなサービスやウェブサイトにサインアップする際、ユーザはしばしば自分自身を特定する。提供される情報には、氏名、年齢、住所、電話番号、生年月日、支払詳細、さまざまな好みなどが含まれる。
クッキー	クッキーは、ユーザのコンピュータに置かれる小さなファイルで、異なるウェブサイトに固有のユーザの活動や閲覧に関するデータを保存する。ユーザがウェブサイトを訪問すると、そのウェブサイトは自動的に、目に見えない形でユーザのコンピュータにクッキーを送信することがある。このクッキーは、ウェブサイトがユーザのウェブサイトへの訪問や行動を追跡するのに役立ち、ウェブサイトがそのユーザに特化したウェブページを提供できるようにする。例えば、オンライン小売業者のウェブサイトでは、クッキーを使用して、ユーザが異なるセッションにわたってウェブサイトをナビゲートする際に、ショッピングカートに何を追加しているかを追跡することができる。
ウェブタグ	ウェブタグは、ユーザのコンピュータに送信されるファイルではなくウェブページ内に存在する要素であることを除けば、クッキーに似ている。これらのタグは、インターネットを閲覧するユーザを認識し、追跡するために使用することができる。
アドタグ	広告タグは、広告主やパブリッシャーが広告のパフォーマンスを測定し、ユーザーの広告への関与(広告の閲覧、広告のクリック)を追跡するのに役立つ。
ピクセル	ウェブサイトや広告主がさまざまな方法でユーザを追跡するために使用するピクセルには、さまざまなものがある。例えば、ユーザの技術情報(IPアドレス、使用デバイス)を収集するピクセル、ユーザが製品を購入したり、同等のアクションを完了したときに追跡するピクセル、ユーザが特定のページにどれくらいの時間滞在したかを追跡するピクセルなどがある。広告主が使用するピクセルの一例として、Facebookピクセルがある。このピクセルを使用すると、誰かがウェブサイトを訪問し、購入などのアクションを起こしたときに追跡することができる。このデータにより、広告主は将来的にFacebook広告を通じてそのユーザをターゲットにすることができる。
モバイルアプリ	モバイルアプリには、モバイルアプリの開発者がユーザを分析し、その行動を追跡するためのツールが多数用意されている。例えば、グーグルマップやその他のナビゲーションアプリは、位置情報データの追跡と収集を可能にする。アプリ開発者は、ユーザのアプリ利用に関して収集した情報を、Facebookを含む第三者と頻繁に共有する。さらに、AndroidやiOSなど、より一般的な携帯電話のオペレーティング・システムもデータ源となりうる。

*1 ACCC, “Digital platforms inquiry - final report (part 1)”, (2019), p.130, https://www.accc.gov.au/system/files/Digital%20Platforms%20Inquiry%20-%20Final%20report%20-%20part%201.pdf

【参考3】ユーザトラッキング技術（Cookie以外）の分類例

Cookie以外のトラッキング技術*2

ウェブクッキーの使用に対する消費者の認識が高まり、ウェブブラウザにクッキーのブロックを要求できるようになったことで、他のオンライン追跡技術も開発され、広く使用されるようになった。それらには以下が含まれる：

ウェブビーコン、ピクセルタグ	ビーコンやピクセルは、ウェブページや電子メールに埋め込むことができる小さなオブジェクトで、ユーザには見えない。ビーコンやピクセルが埋め込まれたウェブページや電子メールをユーザーが読み込むと、サーバに問合せてオブジェクトを読み込む。これらは、ユーザが何をクリックしたかなどの情報を収集するために使用される。
デバイス又はブラウザのフィンガープリント	特定のデバイスやユーザを識別できるようにするために、デバイスやブラウザに関する情報のパターンを収集すること。収集される情報には、ブラウザの種類、フォントの好み、オペレーティングシステム、バッテリの状態、プラグイン、タイムゾーンなどがある。この技術は、クッキーが削除されたり、ユーザログインが変更されたり、IPアドレスが隠されたり変更されたりしても、複数のオンラインセッションにわたって同じユーザを認識するために使用できる。例えば、ウェブサイトがモバイルデバイスやラップトップのバッテリ状態にアクセスし、ユーザに省エネまたは高性能のディスプレイを表示するかどうかを決定できるようにするHTML5 Battery Status APIのプライバシー分析では、オンライントラッキングを容易にする識別子を提供することが示されている。
顔認識	バイオメトリクス・ソフトウェアは、デジタル画像内の個人を識別するために使用することができる。例えば、Facebook Momentsアプリで使われているソフトウェアは、顔認識技術を応用して写真内の個人を識別する。
モバイルデバイス・トラッキング	広告を表示するモバイルアプリ、モバイルデバイスの動きを追跡できるWi-Fiネットワーク・センサ、モバイルキャリアが収集する情報、GPS追跡、近くを通過するモバイルデバイスと通信するために無線信号を使用するiBeaconやアンテナなど、消費者がモバイル・デバイス上で追跡される可能性のある方法は他にも数多くある。
クロスデバイス・トラッキング	異なるデバイス間で一人のユーザを識別するために様々な方法を使用すること。これには、複数のデバイスでユーザのログインを追跡するような決定論的手法や、フィンガープリンティング、モバイルID、オンラインクッキーを介して生成された非特定データに機械学習アルゴリズムを適用し別々のデバイス間の接続を作成する確率論的手法が含まれる。CPRCによる最近の調査では、分析対象となった広告・追跡サービスの39%がクロスデバイス追跡サービスであり、これはこれらのサービスの3分の1以上が複数のデバイス間で同じユーザを特定できることを意味するという調査結果が引用されている。
オーディオビーコン	クロスデバイス・トラッキングにおける最近の技術革新であるオーディオ・ビーコニングは、クッキーをデバイスにドロップし、デバイスのスピーカーから聞こえない超音波コードを再生するために使用することができる。

*2 ACCC, “Digital platforms inquiry - final report (part 2)”, (2019), pp.388-389, https://www.accc.gov.au/system/files/Digital%20Platforms%20Inquiry%20-%20Final%20report%20-%20part%202.pdf

【参考4】スマートフォンにおける利用者情報の性質と種類(※SPSI)

- 「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」(SPSI)では、スマートフォンにおける利用者情報の種類を以下のように整理している。

区分	情報の種類	主な例
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
	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
	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
	契約者・端末固有ID	OS が生成する ID(Android ID)、独自端末識別番号(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
	広告ID	IDFA(Identifier For Advertisers)、AdID(Advertising ID)
	ベンダーID	IDFV(Identifier for Vendor)、AppSetId
第三者の情報	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
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
	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
	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
	写真、動画等	スマートフォン等で撮影された写真、動画等

出典:「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」(2024年11月29日,を一部再構成 https://www.soumu.go.jp/main_content/000981875.pdf

【参考5】アプリが扱う可能性のある利用者情報(※iOSアプリの場合)

カテゴリー	データ
連絡先情報	• 名前:姓や名など • メールアドレス:ハッシュ化されたメールアドレスを含むが、これに限定されない • 電話番号:ハッシュ化された電話番号を含むが、これに限定されない • 物理的な住所:自宅住所、物理的な住所、郵送先住所など • ユーザーのその他の連絡先情報:アプリ外でユーザーへの連絡手段として使用できるその他の情報
ヘルスケア／フィットネス	• 健康:健康および医療に関するデータ • フィットネス:フィットネスおよび運動データ
財務情報	• 支払い情報:支払い方法、支払いカード番号、銀行口座番号など(アプリで決済サービスを利用する場合、支払い情報はアプリ以外の場所で入力される) • クレジット情報:クレジットスコアなど • その他の財務情報:給与、収入、資産、負債、その他の財務情報など
位置情報	• 詳細な位置情報:小数点以下3桁以上の緯度経度と同等、またはそれよりも高い詳細レベルでの、ユーザーまたはデバイスの場所を示す情報 • おおよその位置情報:小数点以下3桁以上の緯度経度よりも低い解像度でユーザーまたはデバイスの場所を示す情報(おおよその位置情報サービスなど)
機密情報	• 機密情報:人種または民族に関する情報、性的指向、妊娠または出産に関する情報、障がい、宗教または哲学的信念、労働組合への加入、政治的意見、遺伝情報、または生体情報など
連絡先	• 連絡先:ユーザーの電話、アドレス帳、ソーシャルグラフ内の連絡先リストなど
ユーザーコンテンツ	• Eメールまたはテキストメッセージ:Eメールまたはメッセージの件名、送信者、受信者、および内容を含む • 写真またはビデオ:ユーザーの写真またはビデオ • オーディオデータ:ユーザーの声またはサウンドの録音

カテゴリー	データ
ユーザーコンテンツ(つづき)	• ゲームプレイコンテンツ:保存したゲーム、マルチプレイヤー対戦機能、ゲームプレイのロジックのデータ、またはゲーム内のユーザー生成コンテンツなど • カスタマーサポート:カスタマーサポートの依頼中にユーザーが生成したデータ • その他のユーザーコンテンツ:ユーザーが生成したその他のコンテンツ
閲覧履歴	• 閲覧履歴:ユーザーが閲覧した、Webサイトなどアプリの外部にあるコンテンツに関する情報
検索履歴	• 検索履歴:アプリ内で実行された検索に関する情報
ID	• ユーザーID:スクリーン名、ハンドル、アカウントID、割り当てられたユーザーID、顧客番号、特定のユーザーやアカウントの識別に利用できるユーザーレベルやアカウントレベルのその他のIDなど • デバイスID:デバイスの広告IDやデバイスレベルのその他のID
購入	• 購入履歴:アカウントや個人の購入履歴または購買傾向
使用状況データ	• アプリ内の操作:アプリの起動、タップ、クリック、スクロール情報、音楽の視聴データ、ビデオの視聴数、ゲームやビデオや曲の保存場所、ユーザーのアプリ操作に関するその他の情報など • 広告データ:ユーザーが見た広告に関する情報など • その他の使用状況データ:アプリのユーザーアクティビティに関するその他のデータ
診断	• クラッシュデータ:クラッシュログなど • パフォーマンスデータ:起動時間、ハング率、エネルギー使用量など • その他の診断データ:アプリに関連する技術的診断を測定する目的で収集されたその他のデータ
周囲の環境	• 環境のスキャン:ユーザー環境におけるメッシュ、ペイン(面)、シーンの認識、または画像検出
身体	• 手:ユーザーの手の構造と手の動き • 頭部:ユーザーの頭部の動き
その他のデータ	• その他の種類のデータ:ここで言及されていないその他の種類のデータ

出典: App Storeでのアプリのプライバシーに関する詳細情報の表示:
https://developer.apple.com/jp/app-store/app-privacy-details/

【参考6】アプリが扱う可能性のある利用者情報（※Androidアプリの場合）

権限	アプリが行うことのできる操作（有効にした場合）
ボディセンサー	• バイタルサインに関するセンサー情報にアクセス
カレンダー	• カレンダーにアクセス
通話履歴	• スマートフォンの通話履歴の読み取りと書き込み
カメラ	• 写真や動画を撮影
連絡先	• 連絡先にアクセス
ファイル	• デバイス上のすべてのファイルにアクセス
位置情報	• デバイスの位置情報にアクセス
マイク	• 音声を録音
音楽とオーディオ	• デバイス上の音楽などの音声ファイルにアクセス
付近のデバイス	• 付近のデバイスの検出、接続、相対位置の特定
通知	• 通知を送信
電話	• 電話の発信と管理
写真と動画	• デバイス上の写真と動画にアクセス
身体活動	• ウォーキング、サイクリング、運転、歩数などの身体活動データにアクセス
SMS	• SMSメッセージの送信と確認

出典：「Android スマートフォンでアプリの権限を変更する」：
https://support.google.com/android/answer/9431959

【参考7】ウェブブラウザで直接取得可能な利用者情報(※主なもの)

- サーバのアクセスログ・PHP・ JavaScriptにより、ホスト、ブラウザ、ディスプレイ、ウェブ閲覧時のサーバとの通信内容、ウェブ閲覧履歴等の利用者情報・デバイス情報・入力情報を取得できる。

情報カテゴリ	アクセスログ等(サーバ)	PHP(サーバ)	JavaScript(ブラウザ)
ユーザ側ホスト情報	• ホスト名 • IPアドレス • UserAgent(OS、ブラウザ等)	• ホスト名 • IPアドレス • UserAgent(OS、ブラウザ等)	• ホスト情報 • ホスト名 • ポート番号
ブラウザ			• ブラウザ(コード名、ブラウザ名、バージョン) • ブラウザのプラットフォーム • ブラウザの使用言語 • ブラウザのUserAgent • ブラウザのビューポート(横幅・縦幅)
ディスプレイ			• スクリーンの幅・高さ・縦横比 • ディスプレイ表示色 • タッチ操作可能
通信・セッション情報	• リクエスト元IPアドレス • リクエスト内容 • ユーザーID・セッションID • アクセスされた日時 • アクセスされたサーバのIPアドレス・ポート番号 • アクセスされた(サーバ上の)ファイル • ステータスコード • データ転送量 • 処理時間	• プロトコル名・バージョン • リクエストのメソッド • リクエスト開始時のタイムスタンプ • Accept: ヘッダ • Accept - Charset: ヘッダ • Accept - Encoding: ヘッダ • Accept - Language: ヘッダ • Connection: ヘッダ • Host: ヘッダ • リファラ	• URL(フル) • プロトコル • サーチ情報(?以降) • ハッシュ(#以降) • ページURLのパス部分 • リファラ • ドメイン名
その他	• 認証ユーザ名(ユーザ側から送信) • 利用者がブラウザで入力し、サーバに送信された情報		• デバイスの各種センサ情報(→W3C標準も参照) • 利用者がブラウザに入力した情報、閲覧履歴

出典:各種資料より作成

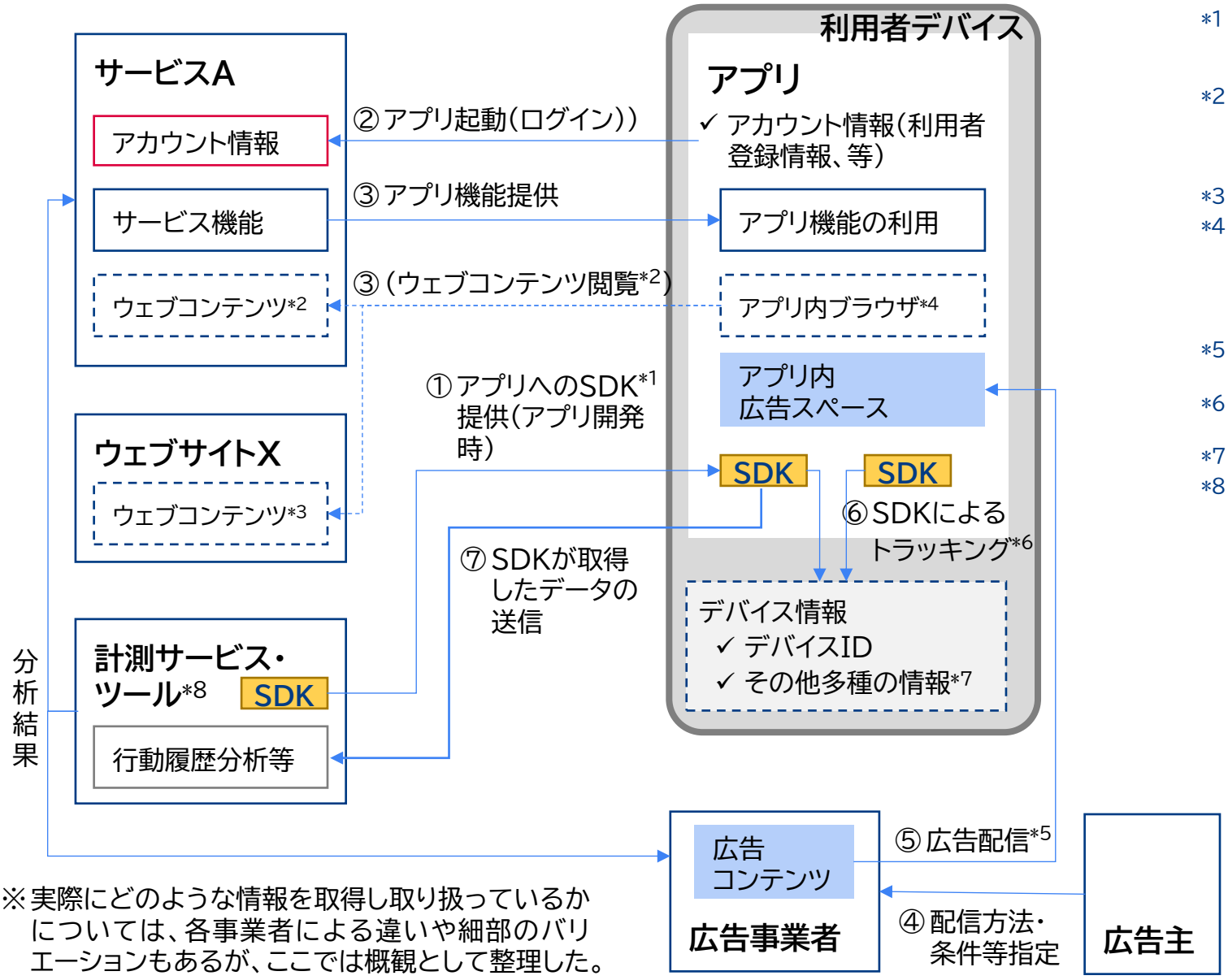
【参考8】モバイルデバイスのセンサとウェブのインタラクション

- デバイスの各種センサ情報のブラウザによる取得・利用について、W3Cにて標準化が行われており、ブラウザが情報を取得する際にユーザのパーミッションを得る仕組みも用意されている。

区分	センサ情報	API/仕様	API/仕様の機能	ステータス
実装済み	地理位置情報	Geolocation API	デバイスの位置を特定	W3C勧告(REC)
	カメラ＆マイクロフォンストリーム	Media Capture and Streams API	デバイスのカメラとマイクのストリームにアクセスする	勧告候補(CR)
実装進行中	汎用センサ	Generic Sensor API	センサデータを一貫した方法でウェブプラットフォームに公開	勧告候補(CR)
	近接センサ	Proximity Sensors	物理的な接触なしに近接物体の存在を監視する	草案(WD)
	環境光センサ	Ambient light sensors	デバイスの環境光レベルまたは照度をモニターする	草案(WD)
	バッテリーステータス	Battery Status API	デバイスのバッテリー充電レベルの提供、バッテリーレベルや充電状態が変化したときに発生するイベントによる通知	勧告候補(CR)
	モーションセンサ	Accelerometer, Gyroscope, Orientation Sensor	デバイスの動きの検出(3軸の加速度・回転速度・磁場、物理的方位)	勧告候補(CR)
		Magnetometer, DeviceOrientation Event Specification		草案(WD)
	地理位置情報	Geolocation Sensor	デバイスから地理位置情報を取得	草案(WD)
	オリエンテーションロック	Screen Orientation API	スクリーンの向きの変化の検出、特定の状態での向きのロック	草案(WD)
標準化の調査作業	NFC	Web Near-Field Communications (NFC) API	近接した2つのデバイス間の無線通信を可能にする	—
	Bluetooth	Web Bluetooth仕様	BLEモードでデバイスを検出、通信する	—
廃止機能	ジオフェンシング	ジオフェンシングAPI	特定の地理的領域へのデバイスの入出を検出	希望があれば将来再開の可能性あり
	追加のセンサ	追加のセンサー仕様	周囲の湿度変化、気圧、温度の線さ情報を取得	希望があれば将来再開の可能性あり

出典:W3C, “Roadmap of Web Applications on Mobile: Sensors and Local Interactions”,より作成, https://www.w3.org/Mobile/roadmap/sensors.html

【参考9】スマートフォンアプリにおける利用者情報取得・利用の例



※実際にどのような情報を取得し取り扱っているかについては、各事業者による違いや細部のバリエーションもあるが、ここでは概観として整理した。

*1 Software Development Kit(アプリの提供する機能のうち特定の機能を持つソフトウェアモジュール)のうち、情報収集等を行うためにアプリに組み込むもの(1つとは限らない)

*2 アプリ内で提供する情報が頻繁に更新される場合(例:ECサイトの商品情報)、アプリ向け情報の更新及びそのアプリマーケットによる審査の手間を考えて、それら情報をウェブコンテンツとして表示する場合がある

*3 アプリ使用時に外部ウェブサイトを閲覧する場合もある

*4 上記*2や*3において、ブラウザアプリを使う場合と、アプリ内ブラウザ(ブラウザモジュール)を使う場合があり、前者の場合にはブラウザアプリの取得した利用者情報はここで注目しているアプリには共有されないが、後者の場合にはアプリ内ブラウザでも利用者の閲覧情報を取得できることがある

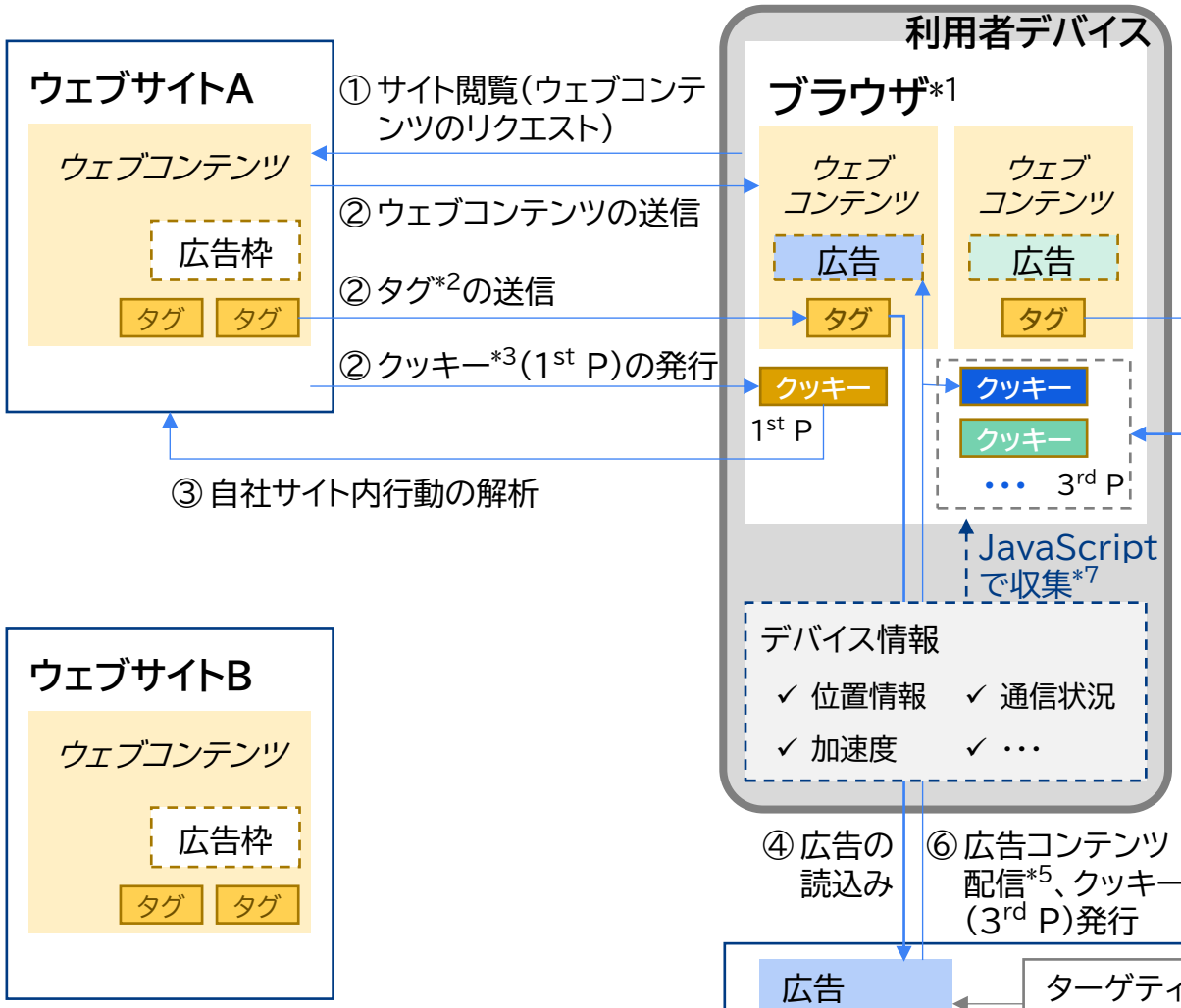
*5 アプリ内広告スペースへの広告配信においては、利用者の行動履歴の取得は困難とされている

*6 SDKによるトラッキングは原則として同意取得が必要(その他、情報取得に関するルールをアプリストアが決めている)

*7 情報の種類は非常に多岐にわたる

*8 アプリに関する行動履歴やコンバージョン情報の取得・計測には大きく2種類あり、①アプリ自体のダウンロードやインストールに関する計測(→アプリの広告やマーケティング等に用いる)、②アプリ内での利用者の行動履歴やコンバージョン情報(→サービスやアプリの改善、アプリ内での各種施策の検討等に用いる)がある

【参考10】ウェブブラウザにおける利用者情報取得・利用の例



*1 ウェブサイト閲覧の場合はブラウザの行動履歴をトラッキングすることになり、利用者≠ブラウザだが、スマートフォンの場合には実質的に利用者≒ブラウザともいえることにも留意が必要であろう(ただし、あくまでブラウザを通じて利用者とインタラクションを行う)

*2 ウェブサイト内の広告スペースに表示される広告を、広告配信サーバに読込みに行くよう指示する命令が記載されている(JavaScriptがブラウザ上で実行されて読込みに行く)

*3 スマートフォンの場合、クッキーに代わりデバイスID(デバイス固有)、広告ID(利用者がリセット可能)、ブラウザフィンガープリント等が使われることもある

*4 ブラウザの行動履歴等を取得するためのタグ(JavaScriptのプログラム)で、例えば広告のクリック、離脱、登録、申込、カートへの商品追加、購入、決済、・・・等を取得する

*5 広告を配信する事業者、アドネットワークの運営するアドサーバから広告が配信される

*6 計測タグを提供する事業者

*7 タグがJavaScriptを実行して収集することができるデバイス情報は、デバイスの位置情報、通信状況、デバイスの加速度データ等、限定されているとされる

*8 例えばオンラインプラットフォームによる広告配信の場合、利用者のアカウント情報も保有しているため、個人を識別した上で行動履歴を把握することが可能な場合もある

※実際にどのような情報を取得し取り扱っているかについては、各事業者による違いや細部のバリエーションもあるが、ここでは概観として整理した。

【参考11】ウェブサイトにおける他ドメインとの情報共有の制限

- ウェブにおいては、他ドメインとの情報共有を制限する仕組みが実装されており、ウェブサイトがこれらを用いることで、第三者による情報取得を制御することが可能。

オリジン間リソース共有(CORS)*1

- オリジン間リソース共有(Cross-Origin Resource Sharing; CORS)は、あるオリジン(ドメイン、プロトコル、ポート番号)で動作しているウェブアプリケーションに、異なるオリジンにある選択されたリソースへのアクセス権を与えるようブラウザに指示するための仕組み。ウェブアプリケーション(例:JavaScript)は、自分とは異なるオリジンにあるリソースをリクエストするとき、オリジン間HTTPリクエストを実行する。
- セキュリティ上の理由から、ブラウザは、スクリプトによって開始されるオリジン間HTTPリクエストを制限している。
  - これらのAPIを使用するウェブアプリケーションは、そのアプリケーションが読み込まれたのと同じオリジンに対してのみ、リソースのリクエストを行うことができる。
  - それ以外のオリジンからのリクエストの場合は正しいCORSヘッダを含んでいることが必要となる。
- 例えば、あるウェブサイト(ドメインA)を表示するときに、他のドメイン(B)のJavaScriptが用いられている場合、当該JavaScriptが前述のウェブサイトを経由してデータを取得する場合には、正しいCORSヘッダが必要となる。すなわち、当該ウェブサイトが当該JavaScriptによるデータ取得を認めることをサーバにて記述していることが必要となる。

CSP: script-src*2

- HTTPのContent-Security-Policy (CSP) におけるscript-srcディレクティブは、JavaScriptの情報ソースを指定する。
  - これには、スクリプトに直接読み込まれるURLだけでなく、インラインのスクリプトイベントハンドラーやスクリプト実行のトリガーとなりうるXSLTスタイルシートのようなものも含まれる。
- このCSPヘッダがある場合、指定されたドメインからのスクリプトのみを許可することになり、信頼できないドメインからのリソースをブロックすることができる。

ウェブサイトがこれらの仕組みを用いることで、ピギーバック(※)によるデータ取得も制限することができる。

※ あるタグに別のタグを組み込むこと。これにより、ウェブサイト側が意図していない形でスクリプト(例:利用者データの取得やターゲティング)が実装されることもある。

*1 https://developer.mozilla.org/ja/docs/Web/HTTP/Guides/CORS
*2 https://developer.mozilla.org/ja/docs/Web/HTTP/Reference/Headers/Content-Security-Policy/script-src

【参考12】利用者情報の取扱主体・取得手段・利用目的の比較

分類	情報取扱主体	情報取得手段	主な利用目的・利用情報（例）
アプリ	アプリ提供者 （アプリ開発者）	サービス利用履歴 （アプリ、サービス提供サーバ）	• サービス・サイトの提供（例：ECサイトのカート管理）、利用者の利便性向上（例：利用状態の保存） • 有望顧客の抽出・獲得（例：属性、利用状況、特定の情報や商品へのアクセス状況、等） • 利用者のプロファイリング（例：好みや履歴の分析、それに基づくレコメンデーション）
		情報収集モジュール （SDK）	• アプリにおける特定機能の提供 • アプリ機能やサービス内容の利用状況分析・改善（例：UI/UX改善、品揃え改善） • 広告アクセス状況の計測（無料アプリにおける広告収入の算定に用いる場合） • 広告・マーケティング施策の検討・評価
	情報収集モジュール 提供者	情報収集モジュール （SDK）	• アプリにおける特定機能の利用状況分析・改善 • 広告・マーケティング施策の検討・評価 • 利用者のプロファイリング　※アカウントと対応付けた分析も可能
ブラウザ/ ウェブ サイト	サイト運営者	1st Party Cookie	• サービス及びサイトの提供（例：ECサイトのカート管理）、利用者の利便性向上（例：ログイン状態や利用状態の保存） • サービス及びサイトの利用状況分析・改善（例：UI/UX改善、メニュー・品揃え等の改善） • 広告・マーケティング施策の検討・評価 • ブラウザのプロファイリング（例：好みや履歴の分析、それに基づくレコメンデーション）　※ログインしている場合にはアカウントと対応付けた分析が可能
		3rd Party Cookie	• 見込み顧客・有望顧客の抽出・獲得（例：ナーチャリング、リードジェネレーション、リターゲティング）
	情報収集モジュール 提供者	情報収集モジュール （JavaScript等）	• 提供している機能の利用状況分析・改善（※特定機能を提供している場合） • 広告アクセス状況の計測 • 広告・マーケティング施策の検討・評価
	広告事業者	3rd Party Cookie	• 広告効果測定、行動ターゲティング • 見込み顧客・有望顧客の抽出・獲得（例：ナーチャリング、リードジェネレーション、リターゲティング） • 利用者のプロファイリング　※オンラインプラットフォーム事業者が広告配信事業者の場合、ユーザカウント情報を保有していれば、アカウントと対応付けた分析が可能なこともある
	ブラウザベンダ	ブラウザ履歴	• ブラウザの改善（例：機能改善、UI/UX改善） • 利用者のプロファイリング　※オンラインプラットフォーム事業者等がブラウザを提供している場合、ユーザカウント情報を保有していれば、アカウントと対応付けた分析が可能なこともある

MRI 三菱総合研究所