

プラットフォームサービスに係る利用者情報の取扱いに関するワーキンググループ  
利用者情報に関する技術動向及び業界団体による自主ルール  
等の状況

---

株式会社野村総合研究所  
コンサルティング事業本部

2022年4月27日

**NRI**

*Share the Next Values!*



## 1. 利用者情報に関する技術動向

- Cookieに関する通知・同意取得の現状
- HTTPリクエスト／Cookieを通じた利用者情報の取得状況
- アプリを通じたCookieと広告IDの取得状況
- Googleアナリティクスの利用におけるサイト管理者の通知状況
- 位置情報の取得・利用実態
- 3<sup>rd</sup> party cookie廃止を受けた代替技術の動向

## 2. 業界団体による自主ルール等の状況

- NAI Code of Conduct
- IAB PRAMの取組み
- 参考) IAB PRAM Technology Standardsワーキンググループが公表する規格の詳細

# 調査対象とする利用者情報に関する技術の概要

## 1) Cookie

- Webサーバーがクライアントコンピュータに預けておく小さなファイルのこと※1。Cookieを発行し、保管することで、インターネットの接続情報や閲覧情報の維持が可能となる。
- アクセス先のWebサイトと同じドメインから発行される1st party cookieと別のドメインから発行される3rd party cookieに分けられる。

## 2) 広告ID

- スマートフォンやタブレット端末のアプリで利用される、ユーザーがオプトアウトできる、匿名かつユニークな広告用の端末識別IDのこと。広告識別子ともいう。※2
- AppleやGoogleなどのプラットフォーム事業者は、AppleのiOSは「Advertising Identifier (IDFA)」、GoogleのAndroid OSは「Android Advertising ID (AAID)」を提供している。
- IDFAやAAIDはアプリ間での共通のIDだが、広告以外の目的での使用は認められていない。

## 3) 位置情報

- 基地局、GPS、Wi-Fiを通じて取得される、通信端末の位置に関する情報。※3
  - これらに加え、ビーコン (beacon) 等により屋内測位される情報やIPアドレス、Web (閲覧・検索) 履歴などから推定される情報も位置情報として位置づけられる。
- ※ 本事業では、アプリ利用・ブラウジングを通じて取得される位置情報を取り上げる。

(出所)

※1 総務省「国民のための情報セキュリティサイト」(2021年11月27日アクセス)

※2 デジタル・アドバタイジング・コンソーシアム株式会社「デジタルマーケティング用語集」(2021年11月27日アクセス)

※3 総務省「プラットフォームサービスに係る利用者情報の取扱いに関するワーキンググループ(第1回)資料5」(2021年3月18日)

# 端末の利用によって取得される利用者情報の種類

## 取得される利用者情報の種類

端末の利用の  
状態

	1) Cookie	2) 広告ID	3) 位置情報
Webブラウジング (ブラウザでWebサイトを閲覧する)	○	—	○※2
アプリを利用する	—※1	○	○

※1 アプリ経由でブラウザを立ち上げる際に、取得されることがある。

※2 本事業ではアプリの利用を通じた情報取得について特に調査を進めた

# Cookieに関する通知・同意取得の現状

---

## 参考：

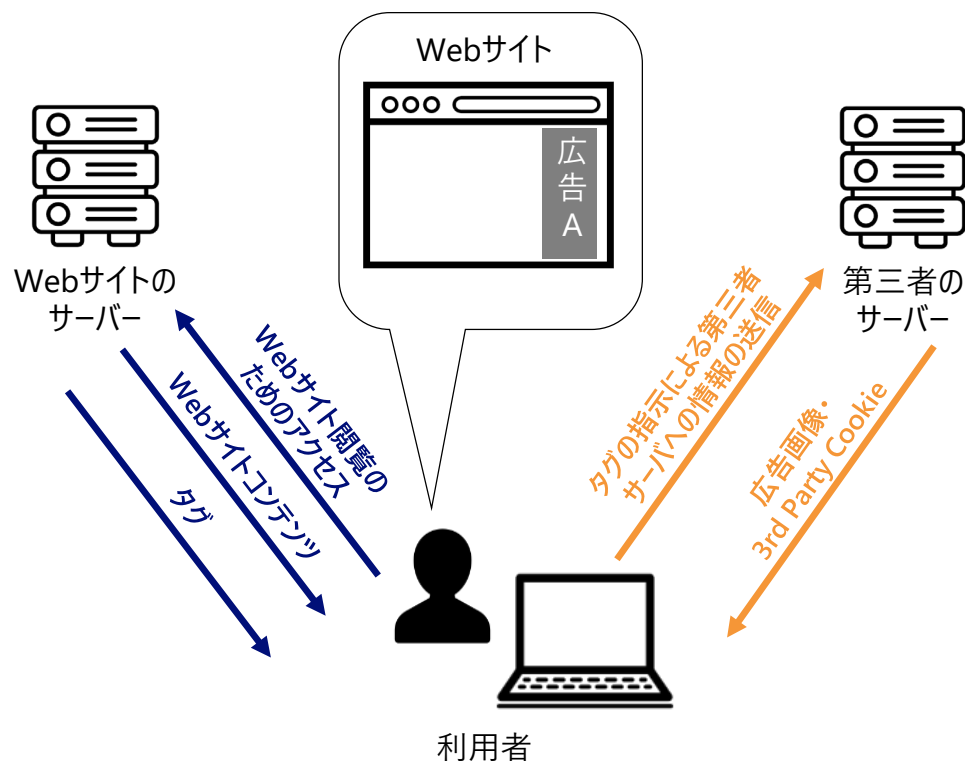
# Cookieの構成・収集方法

### Cookieの構成

項目	内容
Name ※	Cookieの名前
Value ※	Cookieの値（ここでWebサイト訪問回数を記録したり、ハッシュ化した会員IDを埋め込んだりする）広告ビジネスに利用されるデータ項目
Expires	Cookieの有効期限（記載を省略するとブラウザを閉じることにより、Cookieが無効になる）
Max-age	Cookieの有効時間（記載を省略するとブラウザを閉じることにより、Cookieが無効になる）
Domain	Cookieを送信するドメイン
Path	Cookieの送信対象となるパス
Secure	httpsの通信時のみCookieを送信する要件

※ 必須項目

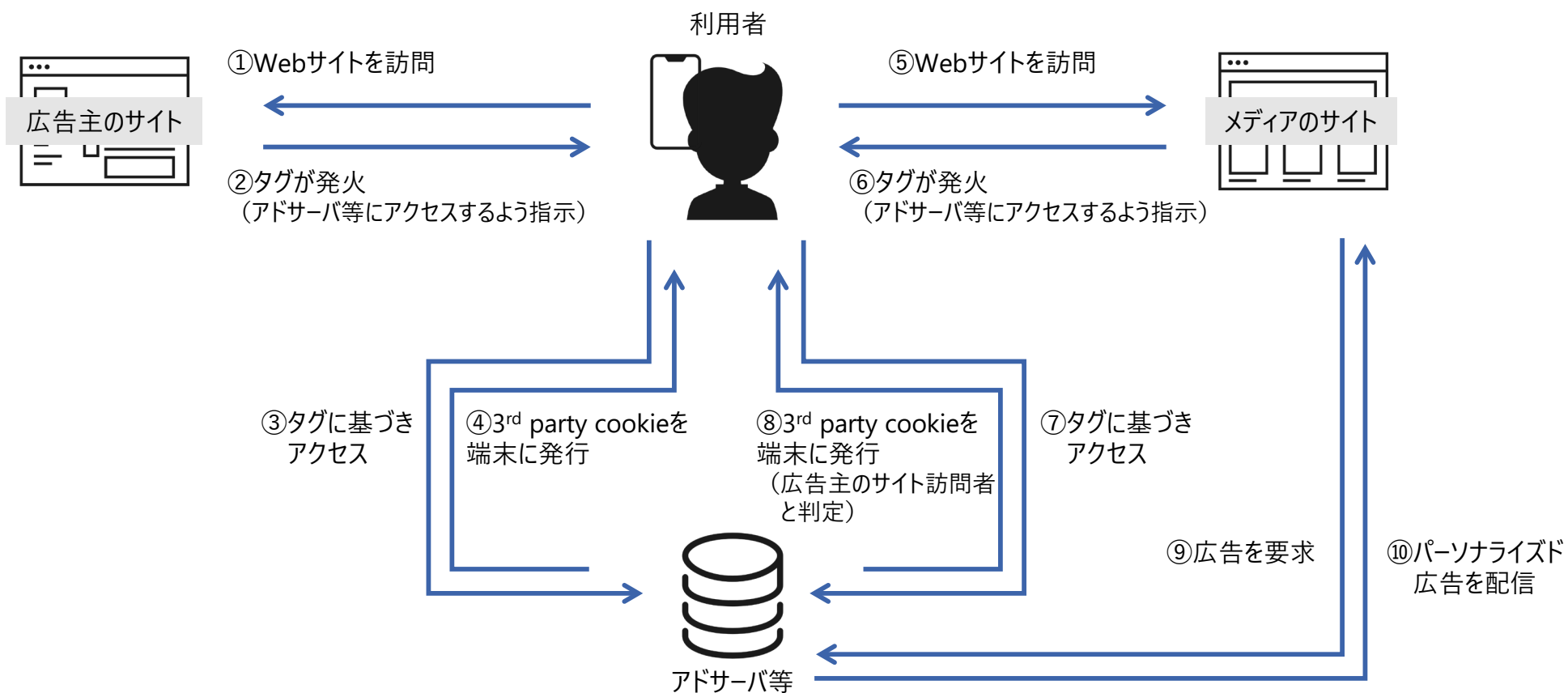
### Cookieの収集方法



(出所) 電気通信事業ガバナンス検討会 (第11回)「資料11-1 電気通信事業ガバナンスの在り方と実施すべき措置」を参考にNRI作成

# 3<sup>rd</sup> party cookieは、行動ターゲティング広告を支える重要な要素技術として利用されている。

行動ターゲティング広告の仕組み



参考：

# Web広告の出稿に関する事業者の関係性

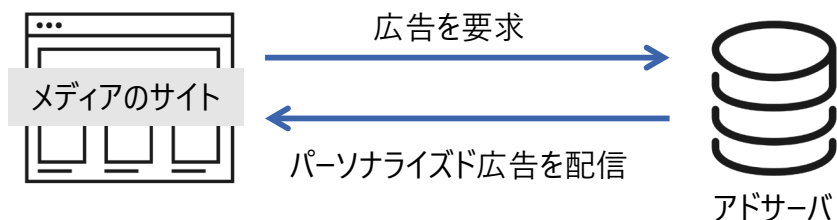
<凡例>

アドネットワーク：複数の広告枠を束ねて販売する事業者

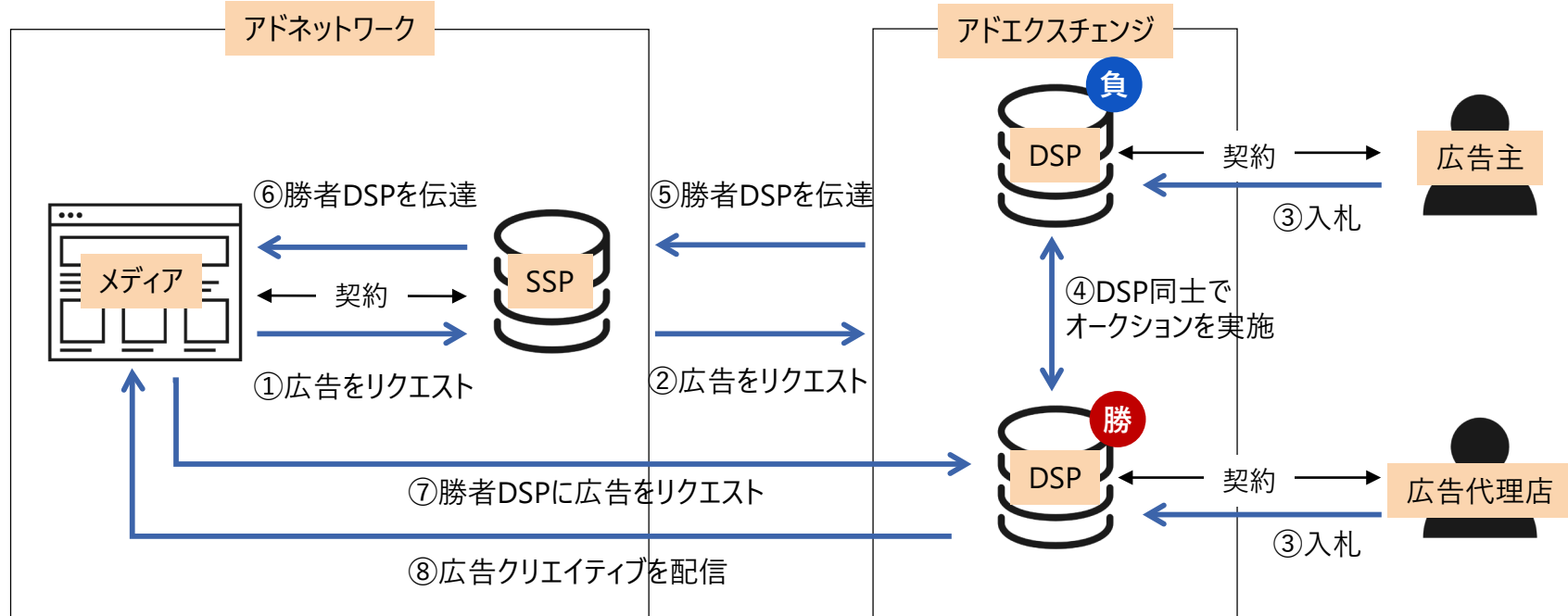
アドエクスチェンジ：広告枠の取引市場を運営する事業者

DSP（Demand Side Platform）：広告効果の最大化を支援する事業者

SSP（Supply Side Platform）：広告収入の最大化を支援する事業者



より詳細には、以下のやり取りが生じている

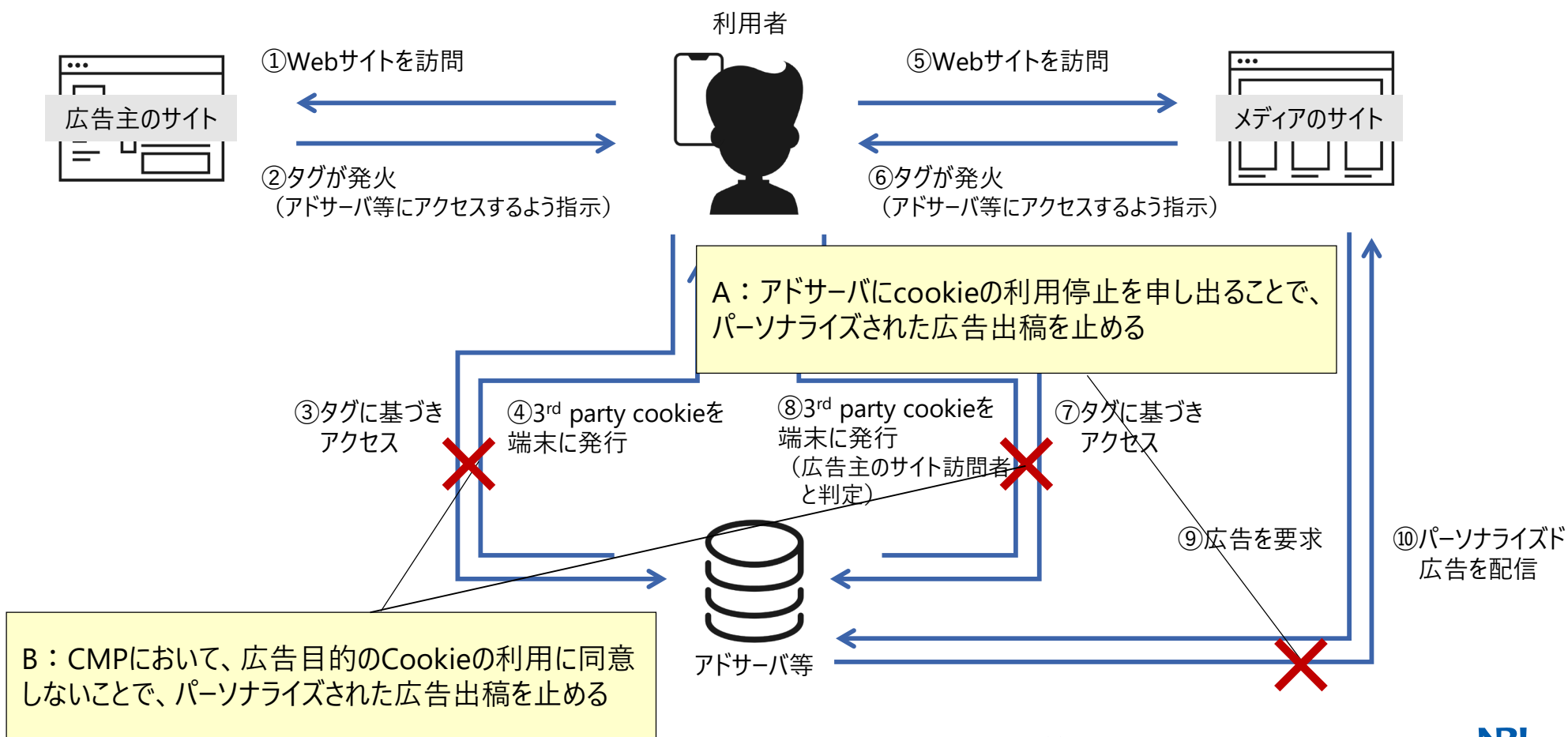




## Cookieに関する通知・同意取得の現状

利用者が行動ターゲティング広告を拒否する手段としては、A：アドサーバにcookieの利用停止を申し出る、B：CMPによりcookieの利用に同意しない、が挙げられる。

### 利用者が行動ターゲティング広告を拒否する手段



参考：

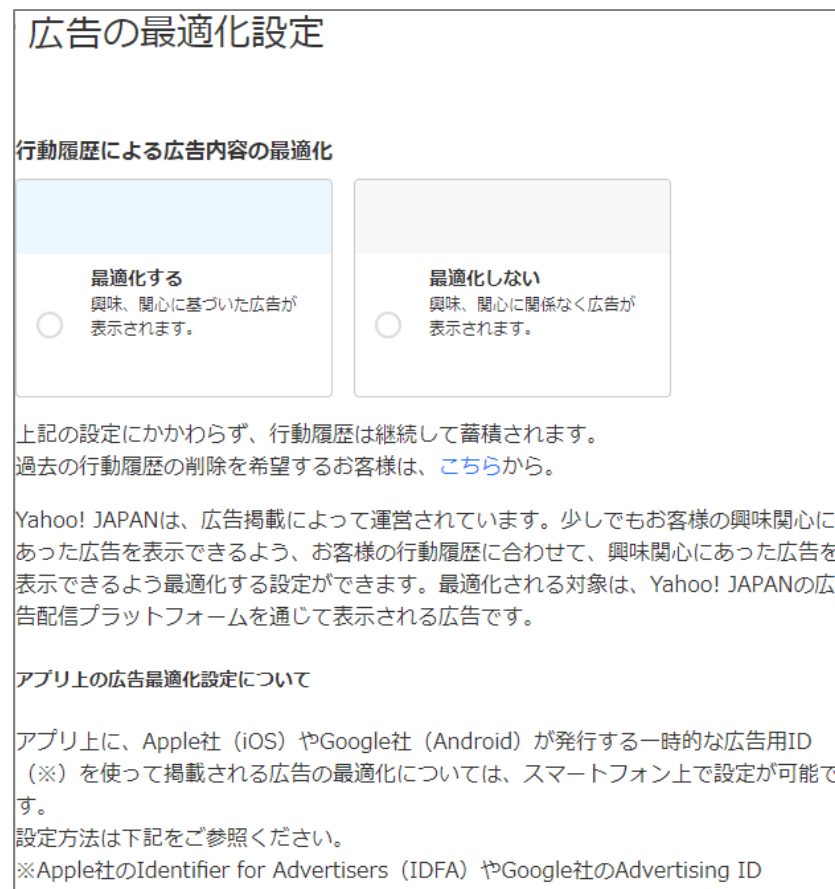
A：アドサーバにcookieの利用停止を申し出る際の操作画面例 1/2

Google広告



(出所) <https://adssettings.google.com/authenticated> (2021年11月28日アクセス)

Yahoo広告



(出所)

<https://accounts.yahoo.co.jp/privacy/optout/ads?.done=https%3A%2F%2Fwww.yahoo.co.jp> (2021年11月28日アクセス)

## 参考：

### A：アドサーバにcookieの利用停止を申し出る際の操作画面例 2/2



DDAIについて

消費者データを使った  
広告について

🔍 オプトアウト等

参画企業

会員社向け

お問い合わせ

## オプトアウト等



本サイトでは、DDAIに参画している各企業のユーザーデータを利用したインターネット広告配信を停止(オプトアウト\*)することができます。

**ただし、オプトアウトはクッキー技術を利用したターゲティングを停止するものであり、広告配信自体を停止するものではありません。**

**オプトアウトをしていても以下のような理由で同じ広告が表示されることがあります。**

- ・ 同じ広告が別のサービス経由で配信されている場合
- ・ 同じ広告がターゲティング無しで配信されている場合

オプトアウトに関するよくあるご質問については、[こちら](#)。

ブラウザ向け

アプリ向け

ブラウザ向け広告のオプトアウトをご希望の方は、以下の各サービスのターゲティング状態を確認しチェックボックスよりオプトアウトの操作を行ってください。

またオプトアウトを機能させるには、お使いのブラウザの設定で第三者からのクッキーを受け入れるようにしなければなりません。

**各ブラウザの設定方法についてはこちらからご確認ください。**

なお、オプトアウトしたサービスについては、「広告のターゲティング再開」ボタンをクリックすることにより、広告のターゲティングを再開することができます。

広告のターゲティング停止(オプトアウト)

広告のターゲティング再開

全て選択

サービス名 / 企業名	ターゲティングステータス	詳細	選択
<a href="#">どこどこad PLATFORM / 株式会社Geolocation Technology</a>	✔ 有効です	<a href="#">詳細</a>	<input type="checkbox"/>
<a href="#">i-mobile / 株式会社アイモバイル</a>		<a href="#">詳細</a>	<input type="checkbox"/>
<a href="#">IM-DMP / 株式会社インティメート・マージャー</a>		<a href="#">詳細</a>	<input type="checkbox"/>
<a href="#">ScaleOut DSP / Supership株式会社</a>		<a href="#">詳細</a>	<input type="checkbox"/>
<a href="#">adstir / ユナイテッドマーケティングテクノロジーズ株式会社</a>		<a href="#">詳細</a>	<input type="checkbox"/>

## Cookieに関する通知・同意取得の現状

### 参考：

### B：CMPによりcookieの利用に同意しない際の操作画面例

The image displays a screenshot of the Accenture website with a privacy consent overlay. The overlay is titled "accenture プライバシー設定センター" and contains the following sections:

- プライバシーについて**: 広告配信・ソーシャルメディアCookie (with a toggle switch)
- 必要不可欠なCookie**
- ファーストパーティ・アナリティクスCookie**
- パフォーマンスCookieと機能性Cookie**
- 広告配信・ソーシャルメディアCookie** (highlighted with a red box)

The highlighted section contains the following text: サードパーティの広告/ソーシャルメディアCookieは、以下の目的で使用されます。(1) ユーザーおよびユーザーの関心事項との関連性が高い広告を表示する。(2) 同じ広告が何度も表示されるのを防止する。(3) 広告キャンペーンの効果を測定する。(4) 広告を見た後のユーザーの行動を把握する。広告/ソーシャルメディアCookieは通常、サイト運営者の許可を得た上で、アドネットワークのために設置されます。このCookieはユーザーのサイト閲覧を記憶し、多くの場合、その情報が他の組織の提供するサイトの機能と関連付けられます。これにより、他サイトでユーザーが目にするコンテンツやメッセージに反映される可能性があります。

At the bottom of the overlay, there are two buttons: "設定を保存する" and "すべて許可".

In the footer of the website, there is a button labeled "Cookieの設定" (highlighted with a red box) and a red arrow pointing from the highlighted section of the overlay to this button.

The background of the website shows a navigation menu with items like "トレンド", "サービス", "業界", "採用情報", and "会社情報". The main banner features the text "クラウド・コンティニューム" and a sub-header "あらゆる機会に、いつでも対応できる力を備えるため、クラウド機能の継続的な活用を。"

At the bottom of the page, there is a small text block: "accenture.comへようこそ！当Webサイトでは、ユーザーエクスペリエンス向上のため、Cookieを使用して一部のサイト機能を有効化しています。Cookieを使用することで、ユーザーが容易にソーシャルメディアでコンテンツをシェアする事や、ユーザーが関心を持っているコンテンツの把握、アクセントゥアから個々のユーザーの関心、居住地に合わせたコンテンツや求人情報、広告の配信など、Web上でより良いサービスの提供が可能となります。詳しくは、アクセントゥアの [Cookieポリシー](#) と [プライバシーポリシー](#) をご参照ください。"

(出所) <https://www.accenture.com/jp-ja>

## 行動ターゲティング広告の実施にあたっては、JIAAが情報取得者に対し、8つの告知事項の掲出を求めている。

JIAA「行動ターゲティング広告ガイドライン」において情報取得者に求められる告知事項

---

- ① 取得の事実
- ② 対象情報を取得する事業者の氏名または名称
- ③ 取得される行動履歴情報の例示
- ④ 取得方法
- ⑤ 利用目的
- ⑥ 保存期間
- ⑦ オプトアウトの手段、その他利用者関与の方法がある場合は、その方法
- ⑧ 行動履歴情報を広告提供事業者に提供する場合は、その旨ならびに提供を受ける広告提供事業者および提供する情報の範囲

JIAA：一般社団法人 日本インタラクティブ広告協会（Japan Interactive Advertising Association）

情報取得者：自らのウェブサイト等または他社のウェブサイト等を通じて利用者の行動履歴情報を取得し、その情報を広告提供事業者に提供する、または利用させる会員社をいう。

## Cookieに関する通知・同意取得の現状

自社webサイトにおいて収集する3rd party cookieについて、個別に明示している事業者であってもオプトアウトの意味合いまでを説明している先は多くないと思われる。

### 3<sup>rd</sup> party cookieの取得に関する説明例

(出所) 株式会社ビザスク「Cookieポリシー」(2021年11月27日アクセス)

3. 第三者が発行するCookieについて

当社は、本ウェブサイトでの体験を改善および向上する目的で、本ウェブサイト以外の第三者によって発行されるCookieを使用しています。当該第三者は、利用者のCookie情報を取り扱うこととなります。

サービス名	提供会社	利用目的	オプトアウトページ
GoogleAnalytics	<a href="#">Google LLC</a>	WEBページのアクセス解析サービスです。当社ウェブサイトへの訪問状況や流入経路などから利用状況を測定しています。	<a href="#">オプトアウト</a>
FullStory	<a href="#">FullStory, Inc.</a>	WEBページのアクセス解析サービスです。当社ウェブサイトでの行動パターンなどから利用状況を測定しています。	<a href="#">オプトアウト</a>
Mixpanel	<a href="#">Mixpanel, Inc.</a>	WEBページのアクセス解析サービスです。当社ウェブサイトへの流入経路や、使用しているブラウザ・デバイス情報などから利用状況を測定しています。	<a href="#">オプトアウト</a>
MIERUCA	<a href="#">株式会社Faber Company</a>	WEBページのアクセス解析ツールです。当社ウェブサイトでの行動パターンなどから利用状況を測定しています。	なし
Intercom	<a href="#">Intercom, Inc</a>	カスタマーサポートサービスです。当社ウェブサイトへの訪問状況等をもとにお知らせの通知をおこなったり、チャット機能を提供しています。	なし
Zendesk	<a href="#">Zendesk, Inc.</a>	カスタマーサポートサービスです。お問合せ機能を提供しています。	なし
Stripe	<a href="#">Stripe, Inc.</a>	インターネットを通じた決済代行サービスです。当社サービスにおいてクレジットカードによる決済機能の提供を行っています。	なし
Marketo	<a href="#">Marketo, Inc.</a>	マーケティングオートメーションサービスです。当社サービスへのお問い合わせ、メール通知、セミナー参加状況、および当社ウェブサイトへの訪問状況などを一元管理しています。	<a href="#">オプトアウト</a>
Google広告	<a href="#">Google LLC</a>	広告出稿サービスです。当社サービスの広告配信を行っています。当社ウェブサ	<a href="#">オプトアウト</a>

3<sup>rd</sup> party cookieの収集そのものを停止するためのオプトアウト

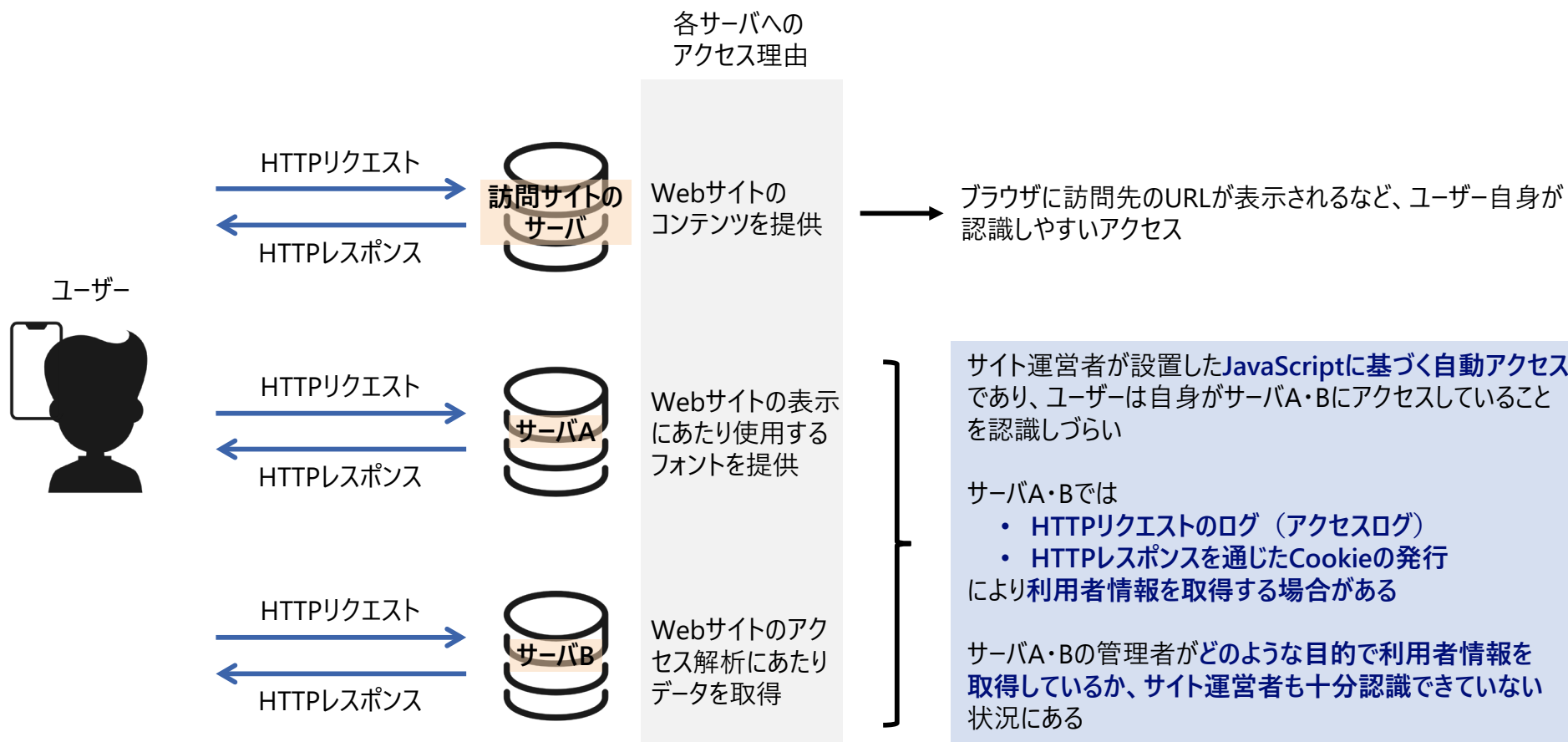
行動ターゲティング広告の配信を停止するためのオプトアウト

# HTTPリクエスト／Cookieを通じた利用者情報の取得状況

---

ユーザーインターフェースの高度化やアクセス解析等を目的にサイト運営者が設置したJavaScriptを通じて、訪問先ドメインとは異なるドメインへのHTTPリクエストが生じている。

Webサイト訪問におけるHTTPリクエストの発生状況





参考：

アクセスログにより取得可能な利用者情報の主な項目

項目	内容
リクエスト元のIPアドレス	<ul style="list-style-type: none"><li>HTTPリクエストを送ったパソコンやスマートフォン等の端末のIPアドレス</li></ul>
アクセス日時	<ul style="list-style-type: none"><li>サーバーがHTTPリクエストを受け取った日時</li></ul>
アクセス先のファイル	<ul style="list-style-type: none"><li>サーバー上でアクセスを受けたファイル</li></ul>
ステータス（アクセス結果）	<ul style="list-style-type: none"><li>アクセスに対するサーバの対応結果 例）200 = 正常（リクエスト成功）、404 = 未検出（アクセス要求したファイルが見つからない）</li></ul>
リファラ	<ul style="list-style-type: none"><li>アクセス元のURL</li></ul>
ユーザーエージェント	<ul style="list-style-type: none"><li>HTTPリクエストを送った端末の情報（オペレーションソフトやブラウザの種類、バージョン等） 例）'Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36'</li></ul>

参考：

ブラウザの拡張機能を用いた、外部ドメインへの通信状況を確認する手段

株式会社Datsignが提供するブラウザの拡張機能（追加的にブラウザに付与する機能）「教えてURL」をインストールすると、訪問先のドメインとは異なるドメインへの通信状況について可視化することができる。



# 訪問先とは異なるドメインへのHTTPリクエストを発生させているサービスとして、(株)DataSignの調査によると「広告」利用目的のものが最も多い。

カテゴリ別の検出数

#	カテゴリ名	検出数	導入率	ベンダー数
1	広告	174,378	110.09%	198
2	アクセス解析	143,800	90.78%	90
3	ウェブフォント	89,899	56.75%	12
4	ソーシャルプラグイン	62,372	39.38%	26
5	地図	59,977	37.86%	7
6	ウェブツール	58,185	36.73%	142
7	CDN	46,466	29.33%	9
8	タグマネージャ	25,824	16.30%	12
9	動画再生	22,374	14.13%	21
10	DMP	15,922	10.05%	39
11	JavaScriptライブラリ	12,902	8.15%	11
12	CMS	10,955	6.92%	53
13	セキュリティ	9,905	6.25%	14
14	ホスティング	8,119	5.13%	5
15	サイト内検索	7,372	4.65%	15

## 調査方法

- 国内16万サイトをクロールにより調査。調査対象のwebサイトにおける同一ドメインの10ページを対象とし、Webサイト閲覧時に発生している「ドメインが異なるURLへのHTTPリクエスト」からサービスを特定している。
- カテゴリ名は株式会社DataSignがサービス内容を踏まえて独自に分類したものである。

#	サービス名	検出数	構成比	運営会社
1	Display & Video 360※	52,525	30.12%	グーグル合同会社
2	Google広告	24,121	13.83%	グーグル合同会社
3	Twitter広告	15,641	8.97%	Twitter Japan株式会社
4	Facebook 広告	13,378	7.67%	Facebook Japan株式会社
5	Yahoo! 広告	9,110	5.22%	ヤフー株式会社
6	Xandr	2,933	1.68%	Xandr. Inc
7	Scale Out	2,823	1.62%	Supership株式会社
8	The Trade Desk	2,644	1.52%	The Trade Desk Japan株式会社
9	マイクロアド	2,193	1.26%	株式会社マイクロアド
10	PubMatic	2,165	1.24%	パブマティック株式会社

導入率：検出数 / 調査対象サイト数（約16万）

構成比：同一カテゴリ内の検出数の割合

※ 旧Double Click, Incが提供していたモジュール。2018年Googleに吸収合併された。

## 訪問先とは異なるドメインへの通信を発生させている 情報収集モジュールやタグ 検出数TOP100 (1/5)

### 調査方法

- 国内16万サイトをクロールにより調査。調査対象のWebサイトにおける同一ドメインの10ページを対象とし、Webサイト閲覧時に発生している「ドメインが異なるURLへのHTTPリクエスト」からサービスを特定している。
- カテゴリ名は、株式会社DataSignがサービス内容を踏まえて独自に分類したものである。

#	カテゴリ	サービス名	URL	検出数	導入率
1	アクセス解析	Google アナリティクス	<a href="https://analytics.google.com/">https://analytics.google.com/</a>	95,017	59.99%
2	ウェブフォント	Google Fonts	<a href="https://fonts.google.com/">https://fonts.google.com/</a>	68,265	43.10%
3	地図	Google マップ	<a href="https://www.google.com/maps">https://www.google.com/maps</a>	59,202	37.38%
4	広告	Display & Video 360	<a href="https://marketingplatform.google.com/about/display-video-360/">https://marketingplatform.google.com/about/display-video-360/</a>	52,525	33.16%
5	ウェブツール	Google Developers	<a href="https://developers.google.com/">https://developers.google.com/</a>	44,664	28.20%
6	アクセス解析	Google アナリティクス(gtag)	<a href="https://analytics.google.com/">https://analytics.google.com/</a>	36,415	22.99%
7	CDN	Google Cloud CDN	<a href="https://cloud.google.com/cdn/">https://cloud.google.com/cdn/</a>	30,950	19.54%
8	ソーシャルプラグイン	Facebook for Developers	<a href="https://developers.facebook.com/">https://developers.facebook.com/</a>	28,856	18.22%
9	広告	Google広告	<a href="https://ads.google.com/">https://ads.google.com/</a>	24,121	15.23%
10	動画再生	YouTube	<a href="https://www.youtube.com/">https://www.youtube.com/</a>	20,461	12.92%
11	タグマネージャ	Googleタグマネージャ	<a href="https://marketingplatform.google.com/about/tag-manager/">https://marketingplatform.google.com/about/tag-manager/</a>	20,269	12.80%
12	広告	Twitter広告	<a href="https://ads.twitter.com/">https://ads.twitter.com/</a>	15,641	9.87%
13	ソーシャルプラグイン	Twitter Platform	<a href="https://developer.twitter.com/">https://developer.twitter.com/</a>	14,642	9.24%
14	広告	Facebook 広告	<a href="https://www.facebook.com/business/ads">https://www.facebook.com/business/ads</a>	13,378	8.45%
15	CDN	BootstrapCDN	<a href="https://www.bootstrapcdn.com/">https://www.bootstrapcdn.com/</a>	12,305	7.77%
16	ウェブフォント	Font Awesome	<a href="https://fontawesome.com/">https://fontawesome.com/</a>	11,289	7.13%
17	JavaScriptライブラリ	jQuery	<a href="https://jquery.com/">https://jquery.com/</a>	11,066	6.99%
18	セキュリティ	reCAPTCHA	<a href="https://www.google.com/recaptcha/about/">https://www.google.com/recaptcha/about/</a>	9,346	5.90%
19	広告	Yahoo! 広告	<a href="https://promotionalads.yahoo.co.jp/">https://promotionalads.yahoo.co.jp/</a>	9,110	5.75%
20	サイト内検索	Google カスタム検索エンジン	<a href="https://cse.google.com/cse/">https://cse.google.com/cse/</a>	6,051	3.82%

## 訪問先とは異なるドメインへの通信を発生させている 情報収集モジュールやタグ 検出数TOP100 (2/5)

### 調査方法

- 国内16万サイトをクロールにより調査。調査対象のWebサイトにおける同一ドメインの10ページを対象とし、Webサイト閲覧時に発生している「ドメインが異なるURLへのHTTPリクエスト」からサービスを特定している。
- カテゴリ名は、株式会社DataSignがサービス内容を踏まえて独自に分類したものである。

#	カテゴリ	サービス名	URL	検出数	導入率
21	CMS	WordPress.com	https://wordpress.com/	5,693	3.59%
22	ホスティング	GitHub	https://github.com/	5,493	3.47%
23	ソーシャルプラグイン	Google+	https://plus.google.com/	4,877	3.08%
24	ウェブフォント	Adobe Typekit	https://fonts.adobe.com/typekit	4,186	2.64%
25	タグマネージャ	Yahoo! タグマネージャー	https://marketing.yahoo.co.jp/service/tagmanager/	3,528	2.23%
26	DMP	Intimate Merger	https://corp.intimatemerger.com/	3,091	1.95%
27	広告	Xandr	https://www.xandr.com/	2,933	1.85%
28	広告	Scale Out	https://supership.jp/business/scaleout/	2,823	1.78%
29	広告	The Trade Desk	https://www.thetradedesk.com/	2,644	1.67%
30	DMP	トレジャーデータ	https://www.treasuredata.com/	2,624	1.66%
31	ホスティング	Amazon S3	https://aws.amazon.com/s3/	2,618	1.65%
32	アクセス解析	Twitter アナリティクス	https://analytics.twitter.com/	2,501	1.58%
33	ソーシャルプラグイン	Instagram	https://www.instagram.com/	2,217	1.40%
34	多言語化	Google 翻訳	https://translate.google.com/	2,212	1.40%
35	広告	マイクロアド	https://www.microad.co.jp/services/adplatform/	2,193	1.38%
36	広告	PubMatic	https://www.pubmatic.co.jp/	2,165	1.37%
37	広告	OpenX	https://www.openx.com/	2,158	1.36%
38	広告	Rubicon Project Exchange	http://rubiconproject.com/	2,123	1.34%
39	ウェブフォント	FONTPLUS	https://fontplus.jp/	2,088	1.32%
40	ウェブフォント	TypeSquare	https://typesquare.com/	2,055	1.30%

## 訪問先とは異なるドメインへの通信を発生させている 情報収集モジュールやタグ 検出数TOP100 (3/5)

### 調査方法

- 国内16万サイトをクロールにより調査。調査対象のwebサイトにおける同一ドメインの10ページを対象とし、Webサイト閲覧時に発生している「ドメインが異なるURLへのHTTPリクエスト」からサービスを特定している。
- カテゴリ名は、株式会社DataSignがサービス内容を踏まえて独自に分類したものである。

#	カテゴリ	サービス名	URL	検出数	導入率
41	ヒートマップ	ユーザーヒート	https://userheat.com/	2,043	1.29%
42	ソーシャルプラグイン	はてなブックマークボタン	https://b.hatena.ne.jp/guide/bbutton	2,033	1.28%
43	人材系ツール	マイナビ新卒採用ロゴ	—	1,889	1.19%
44	広告	Google Ad Manager	https://admanager.google.com/home/	1,881	1.19%
45	アクセス解析	Yahoo Analytics	—	1,880	1.19%
46	CDN	UNPKG	https://unpkg.com/	1,856	1.17%
47	広告	Criteo	https://www.criteo.com/products/	1,811	1.14%
48	広告	LINE Ads Platform	https://www.linebiz.com/jp/service/line-ads/	1,764	1.11%
49	ウェブツール	YubinBango	https://yubinbango.github.io/	1,681	1.06%
50	広告	Xaxis	https://www.xaxis.com/	1,671	1.05%
51	広告	TAPAD	https://www.tapad.com/	1,640	1.04%
52	SSL証明書	GlobalSign	https://www.globalsign.com/	1,636	1.03%
53	広告	ONE BY AOL	https://www.onebyaol.com/	1,608	1.02%
54	CMS	BiNDup	https://bindup.jp/	1,493	0.94%
55	ソーシャルプラグイン	LINEソーシャルプラグイン	https://social-plugins.line.me/	1,490	0.94%
56	DMP	Adobe Audience Manager	https://www.adobe.com/analytics/audience-manager.html	1,462	0.92%
57	広告	BidSwitch	https://www.bidswitch.com/	1,461	0.92%
58	広告	logly lift	https://lift.logly.co.jp/	1,354	0.85%
59	マーケティングオートメーション	Pardot	https://www.pardot.com/	1,292	0.82%
60	ウェブツール	Google カレンダー	—	1,290	0.81%



## 訪問先とは異なるドメインへの通信を発生させている 情報収集モジュールやタグ 検出数TOP100 (4/5)

### 調査方法

- 国内16万サイトをクロールにより調査。調査対象のWebサイトにおける同一ドメインの10ページを対象とし、Webサイト閲覧時に発生している「ドメインが異なるURLへのHTTPリクエスト」からサービスを特定している。
- カテゴリ名は、株式会社DataSignがサービス内容を踏まえて独自に分類したものである。

#	カテゴリ	サービス名	URL	検出数	導入率
61	DMP	AudienceOne	https://solutions.dac.co.jp/audienceone	1,284	0.81%
62	広告	fluct	https://corp.fluct.jp/service/publisher/ssp/	1,275	0.80%
63	広告	i-mobile	https://adpf-info.i-mobile.co.jp/	1,271	0.80%
64	DMP	DMP DC Catalyzer	https://www.data-chemistry.co.jp/dmpdccatalyzer/	1,259	0.79%
65	DMP	Juicer	https://juicer.cc/	1,253	0.79%
66	アクセス解析	Ptengine	https://www.ptengine.jp/	1,229	0.78%
67	タグマネージャ	DataCurrent Tag Manager	-	1,224	0.77%
68	データ収集	SiteGraphics	https://www.videor.co.jp/service/communication/sitegraphics.html	1,207	0.76%
69	アクセス解析	User Insight	https://ui.userlocal.jp/	1,172	0.74%
70	ウェブツール	Amazon API Gateway	https://aws.amazon.com/api-gateway/	1,154	0.73%
71	広告	Logicad	https://www.logicad.com/	1,154	0.73%
72	広告	FreakOut	https://www.fout.co.jp/	1,144	0.72%
73	広告	AdStir	https://ja.ad-stir.com/	1,139	0.72%
74	ソーシャルプラグイン	Gravatar	https://www.gravatar.com/	1,136	0.72%
75	マーケティングオートメーション	BowNow	https://bow-now.jp/	1,109	0.70%
76	ソーシャルプラグイン	LINEで送るボタン	https://social-plugins.line.me/ja/how_to_install#lineitbutton	1,084	0.68%
77	CDN	Amazon Cloud Front	https://aws.amazon.com/cloudfront/	1,077	0.68%
78	アクセス解析	New Relic Browser	https://newrelic.com/products/browser-monitoring	1,061	0.67%
79	CMS	Wix	https://www.wix.com/	1,048	0.66%
80	ウェブツール	Amazon Cognito	https://aws.amazon.com/cognito/	1,002	0.63%

## 訪問先とは異なるドメインへの通信を発生させている 情報収集モジュールやタグ 検出数TOP100 (5/5)

### 調査方法

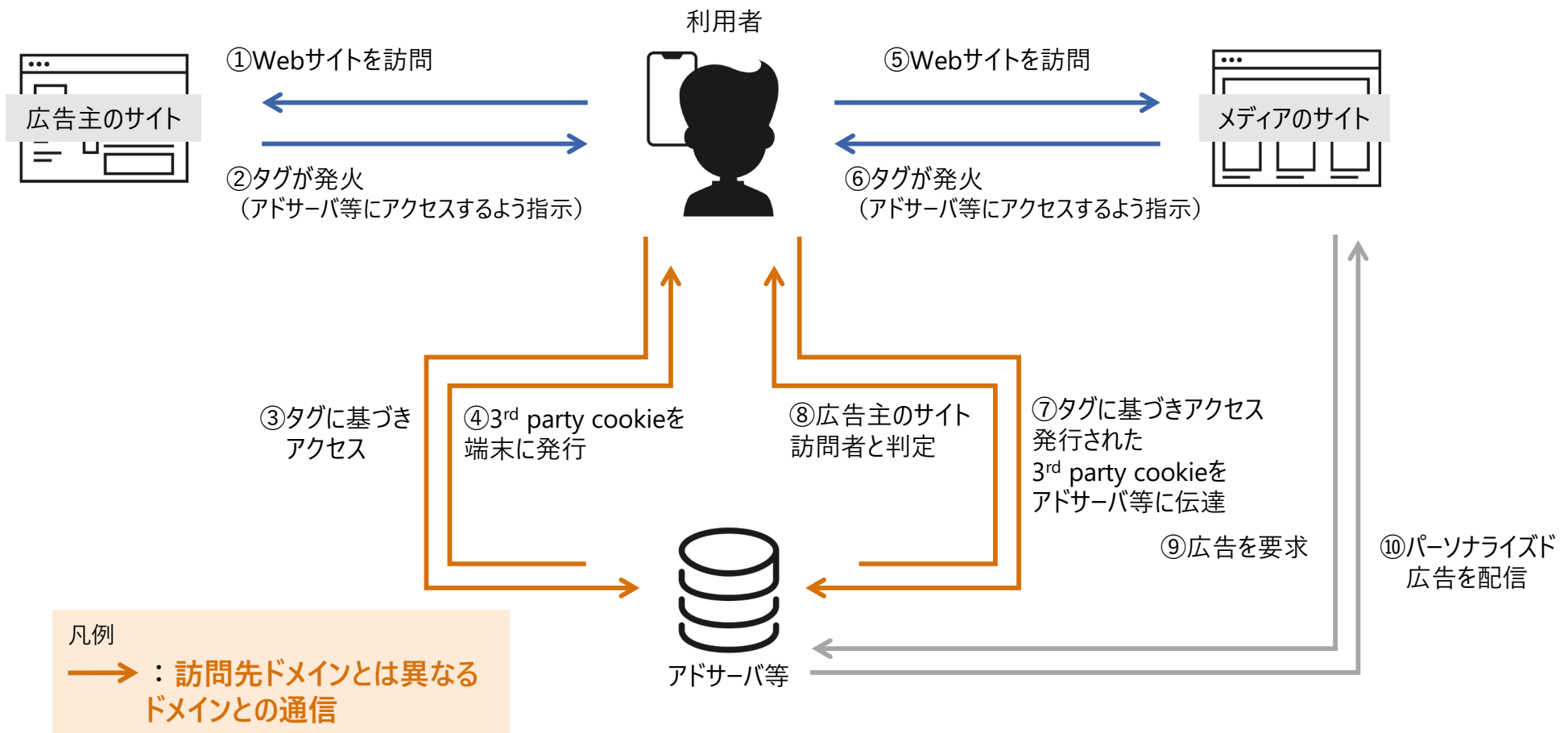
- 国内16万サイトをクロールにより調査。調査対象のWebサイトにおける同一ドメインの10ページを対象とし、Webサイト閲覧時に発生している「ドメインが異なるURLへのHTTPリクエスト」からサービスを特定している。
- カテゴリ名は、株式会社DataSignがサービス内容を踏まえて独自に分類したものである。

#	カテゴリ	サービス名	URL	検出数	導入率
81	ソーシャルプラグイン	LINE公式アカウント	https://www.linebiz.com/jp/service/line-official-account/	989	0.62%
82	広告	Taboola	https://www.taboola.com/	983	0.62%
83	広告	GMO SSP	https://gmossp.jp/	967	0.61%
84	ヒートマップ	ミエルカヒートマップ	https://mieru-ca.com/heatmap/	961	0.61%
85	広告	SpotX	https://www.spotx.tv/	939	0.59%
86	広告	MediaMath	https://www.mediamath.com/	922	0.58%
87	データ収集	LiveRamp	https://liveramp.com/	918	0.58%
88	DMP	LinkedIn マーケティングソリューション	https://business.linkedin.com/marketing-solutions	898	0.57%
89	広告	Outbrain	https://www.outbrain.com/	890	0.56%
90	広告	YIELD ONE	https://yieldone.com/	868	0.55%
91	ソーシャルプラグイン	AddToAny	https://www.addtoany.com/	855	0.54%
92	広告	TubeMogul	https://www.tubemogul.com/	815	0.51%
93	アクセス解析	AD EBIS	https://www.ebis.ne.jp/	803	0.51%
94	IR系ツール	E-IR	http://www.pronexus.co.jp/solution/listed_company/ir_sol/e-ir/	802	0.51%
95	ウェブフォント	エックスサーバー Webフォント	https://www.xserver.ne.jp/functions/service_webfont.php	774	0.49%
96	ソーシャルプラグイン	Facebookログイン	https://developers.facebook.com/docs/facebook-login	770	0.49%
97	JavaScriptライブラリ	Polyfill	https://polyfill.io/	769	0.49%
98	広告	popin	https://www.popin.cc/home/	761	0.48%
99	広告	CA ProFit-X	https://caprofitx.jp/	759	0.48%
100	アフィリエイト	a8.net	https://www.a8.net/	754	0.48%



訪問先ドメインと異なるドメインへのHTTPリクエストを通じて発行される3<sup>rd</sup> party cookieは行動ターゲティング広告を支える重要な要素技術として利用されている。

行動ターゲティング広告の仕組み



## 参考：

## HTTPリクエスト・レスポンスにおけるCookieの伝達状況

### HTTPリクエスト

- 「Cookie」フィールドにおいて発行されたCookieの情報を伝達する。

```
▼ 要求ヘッダー (1.647 KB) 生ヘッダー
```

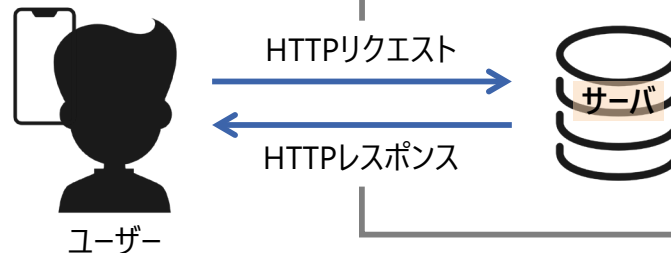
```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Cache-Control: max-age=0
Cookie: AWSALB=elzU6f/hMPLB/WbJZQkeYSqVJJaI0R/Acs1kqo3doYzkoVVLnNRPvqXfNMso8BUZP07nQGcXZu+9fp9mOwpQFv3JhczNgeC7joTOI77ODwQgKF675IU000aaAn; AWSALBCORS=etZU6f/hMPLB/WbJZQkeYSqVJJaI0R/Acs1kqo3doYzkoVVLnNRPvqXfNMso8BUZP07nQGcXZu+9fp9mOwpQFv3JhczNgeC7joTOI77ODwQgKF675IU000aaAn; website#lang=ja-JP; ASP.NET_SessionId=1deg7bqxts42xh5r5gu5wefm; SC_ANALYTICS_GLOBAL_COOKIE=647Bce85d74a49ae2bad22693a56b1fFalse; visid_incap_2631343=VltqUVODRhl1GaHhiiYzbxP5mEAAAAAQUIPAAAAAAbnSL4H80/xsL1kK0+4xKJM; nli_b1_2631343=kAPPUGuOvUCC...mEAAAAAE7hf5vOebjyGjuq3X56Qw==; incap_ses_1512_2631343=n677b5Mtu1UsNrYkL177F9Q5mEAAAAAapitwNWCQrg54QMRXwLnxKQ==; languageDetection=jp; _ga=GA1.2.1443422357.1642483857; _gid=GA1.2.1751860673.1642483857; _dc_gtm_UA-27058226-1-1; krContext=session%3A6ca12451-5344-4997-9721-b200418845bd9%3Bcontext_mode%3Aother; krt.vis=2e386d00-1dcd-49d8-85b7-b8f8cea7d96f; _fbp=fb.1.1642483860452.10633038; incap_ses_434_2631343=ov+rdvSubShBw47J+FFBpBQ5mEAAAAAU6nirTsZLXr69IPUSLpVpQ==; krt.v=message%3A5a66fe16a9a51e104c561b84
Host: www.nri.com
Proxy-Authorization: Basic bTg5NzA6CHcyMTEwMDE=
Referer: https://www.google.com/
TE: Trailers
Upgrade-Insecure-Requests: 1
```

### HTTPレスポンス

- 「Set-Cookie」フィールドにおいて、ブラウザに発行するCookieの情報を伝達する。

```
▼ 応答ヘッダー (1.009 KB) 生ヘッダー
```

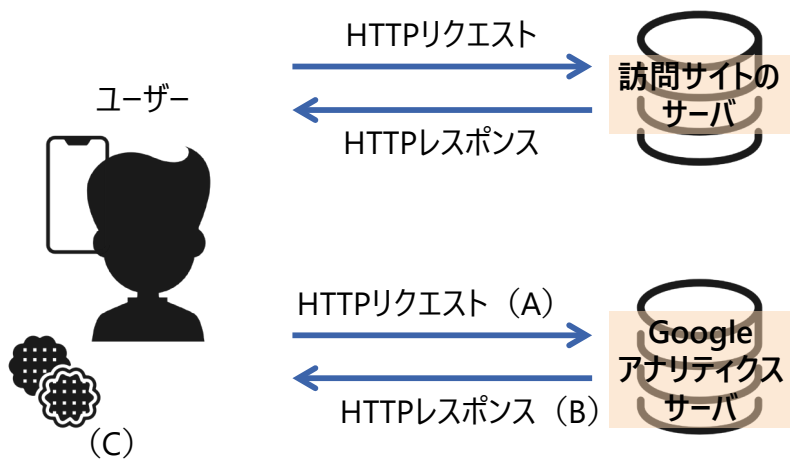
```
cache-control: private
content-encoding: gzip
content-type: text/html; charset=utf-8
date: Tue, 18 Jan 2022 05:31:23 GMT
set-cookie: AWSALB=Tu+mJIAKtdiP/oBZIXUehSCdXwJlD6kXB8nMNq87FWxRv/AGAwlvM7cZTFQOa36C8Djwepghnqm2VnrY4FSVaM711XJtZj3uN1RxisP07Uc3F7dQ+OfV; Expires=Tue, 25 Jan 2022 05:31:22 GMT; Path=/
set-cookie: AWSALBCORS=Tu+mJIAKtdiP/oBZIXUehSCdXwJlD6kXB8nMNq87FWxRv/AGAwlvM7cZTFQOa36C8Djwepghnqm2VnrY4FSVaM711XJtZj3uN1RxisP07Uc3F7dQ+OfV; Expires=Tue, 25 Jan 2022 05:31:22 GMT; Path=/; SameSite=None; Secure
via: 1.1 6727a6ce1b3b9cfb79a421186146d8a6.cloudfront.net (CloudFront)
x-amz-cf-id: oTobhEoinWbqHb_T7kg72KG3zKfIv6AQeJ5_Doff9Q_18gDahVKfg==
x-amz-cf-pop: NRT57-P3
x-cache: Miss from cloudfront
x-cdn: Imperva
x-content-type-options: nosniff
X-Firefox-Spdy: h2
x-frame-options: SAMEORIGIN
```



## 参考：Googleアナリティクスでは、HTTPリクエストと1st Party Cookieを組み合わせた情報取得を行っている。

### 初回訪問における1st Party Cookie発行の仕組み

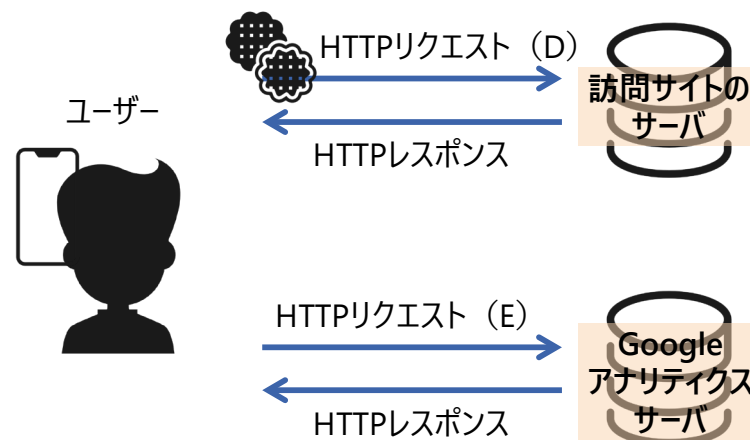
- ① 訪問サイトのhtmlに組み込まれたGoogleアナリティクスのJavaScriptに基づきGoogleアナリティクスサーバへアクセスする（A）。
- ② Googleアナリティクスのサーバからユーザーの端末に、訪問サイトをドメインとするCookieの発行依頼が下る（B）。
- ③ ユーザーの端末内でCookie（1st Party Cookie）が発行される（C）。



（出所）各種公開情報に基づきNRI作成  
実際は、初回訪問においてもGoogleアナリティクスのサーバへアクセス状況を送信しているが、仕組みの理解を促すため、詳細を割愛している。

### 2回目訪問におけるGoogleアナリティクスサーバへの情報伝達の仕組み

- ④ 再度の訪問する際、③で発行されたCookieが、訪問サイトのサーバに送信される。（D）。
- ⑤ 訪問サイトのhtmlに組み込まれたGoogleアナリティクスのJavaScriptに基づきGoogleアナリティクスサーバへ再度アクセスする（E）。  
※ このとき③で発行されたCookieに保存した情報が「URLパラメータ※」として、Googleアナリティクスのサーバへ送信される。



※ URLパラメータ：サーバに情報を送信する際の変数。変数を指定することで、サーバ側の動作を変えることができる。

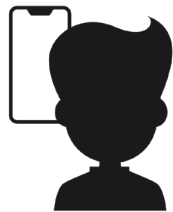
## アプリを通じたCookieと広告IDの取得状況

---

## アプリを通じたCookieと広告IDの取得状況

アプリにおいて広告バナーをタップすると、一度広告事業者のWebページを訪問した上で、  
広告主のWebページに遷移することが一般的に行われている。

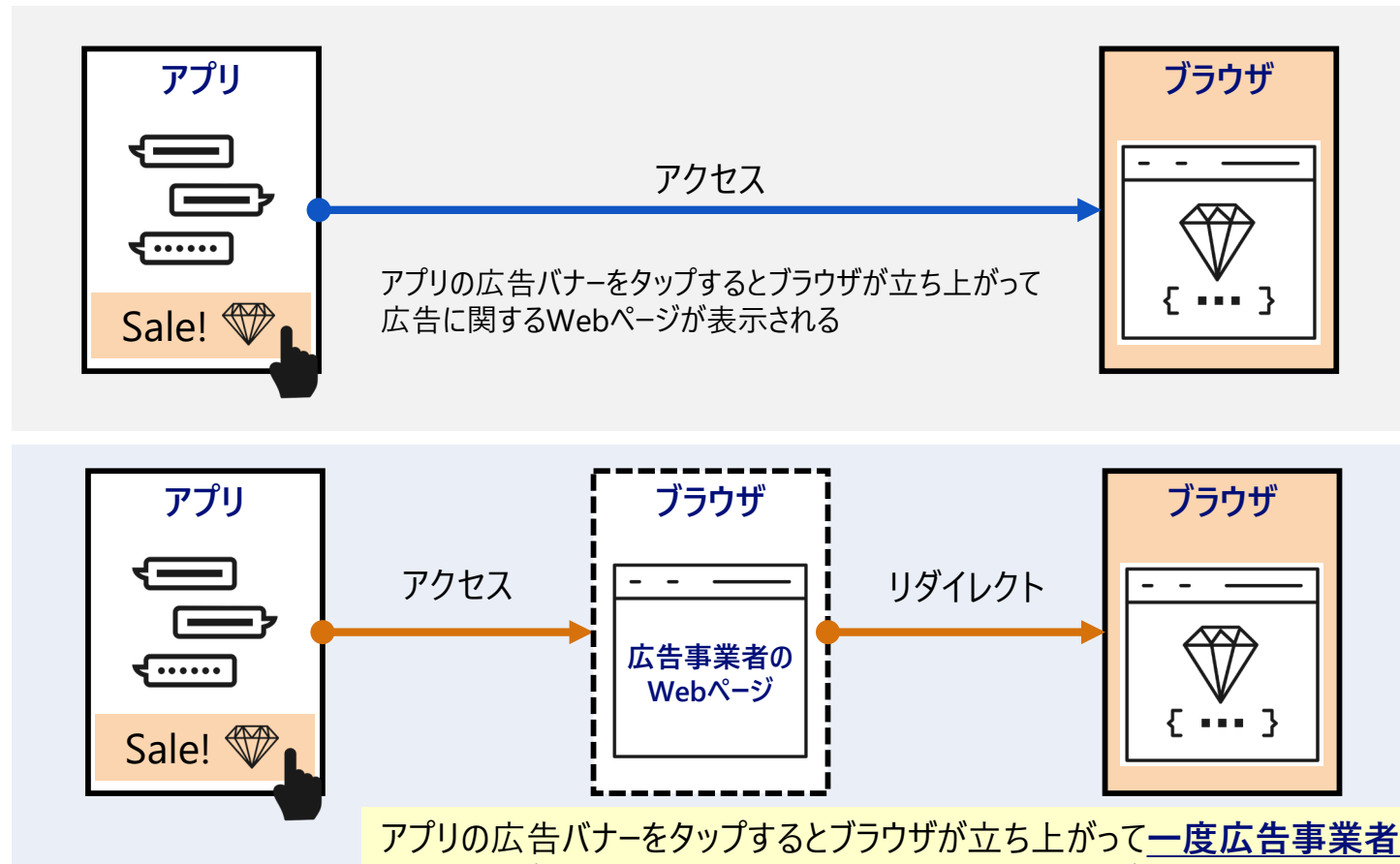
アプリ経由で広告に関するWebページを表示する際の画面遷移



ユーザー

認識しているユーザー自身がアクセス

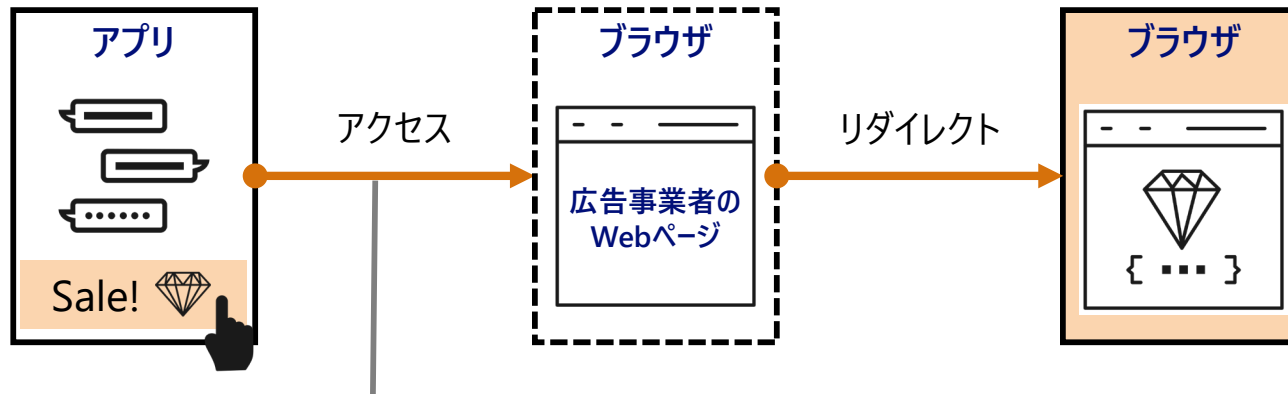
実際に生じているアクセス



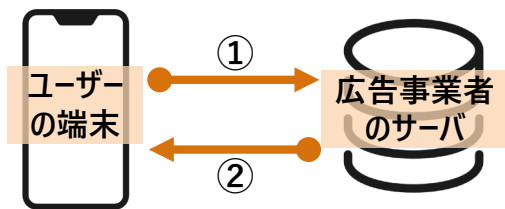
## アプリを通じたCookieと広告IDの取得状況

広告事業者のWebページを訪問する際に、端末の広告IDがURLパラメータとしてCookieとともに、広告配信事業者のサーバに送信される。

広告事業者のWebページ訪問時に生じている、端末とサーバとの通信状況

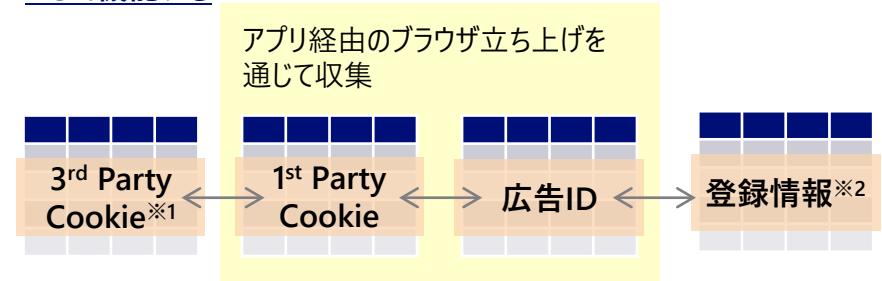


- ①：端末の広告IDが広告事業者のサーバに送信される。  
端末に広告事業者が発行する1st Party Cookieが保存されている場合は一緒に送信される。



- ②：端末に広告事業者が発行する1st Party Cookieが保存されていない場合は、広告事業者のサーバが発行指示を行う。  
(発行したCookieの情報はサーバ側に残る)

収集した広告IDは、広告事業者のシステム内で収集した情報(3rd Party Cookie)と特定のユーザー(端末)とを紐づけるキーとして機能する



- ※1 広告主のWebサイト等に設置したJavaScriptタグを通じて収集  
※2 ユーザーが事業者と契約・利用登録している場合は情報が存在

# Googleアナリティクスの利用におけるサイト管理者の通知状況

---

# 「Google アナリティクス利用規約」ではサイト管理者に対してGoogleアナリティクスの利用有無及びGoogleアナリティクスを通じたデータの収集・処理の仕組みの通知を求めている。

## 7. プライバシー

お客様は、Google が個人情報として使用または認識できる情報を Google に送信したり、第三者によるかかる行為を支援または許可したりしないものとします。お客様は適切なプライバシー ポリシーを用意および遵守し、ユーザーからの情報を収集するうえで、適用されるすべての法律、ポリシー、規制を遵守するものとします。お客様はプライバシー ポリシーを公開し、そのプライバシー ポリシーで Cookie の使用、モバイルデバイスの識別情報（Android の広告識別子、iOS の広告識別子など）、またはデータの収集に使われる類似の技術について必ず通知するものとします。また、Google アナリティクスを使用していること、および Google アナリティクスでデータが収集、処理される仕組みについても開示する必要があります。こうした情報を開示するには、「ユーザーが Google パートナーのサイトやアプリを使用する際の Google によるデータ使用」のページ（[www.google.com/intl/ja/policies/privacy/partners/](http://www.google.com/intl/ja/policies/privacy/partners/) または Google が随時提供するその他の URL）へのリンクを目立つように表示します。お客様は、本サービスに関連してユーザーのデバイス上で Cookie やその他の情報を保存、アクセスする行為が発生し、かかる行為に関する情報の提供とユーザーからの同意が必要であると法律で定められている場合には、ユーザーに明確かつ包括的な情報を提供し、同意を得るための商業上合理的な努力を払うものとします。

お客様は本サービスに含まれるプライバシー機能（オプトアウトなど）を一切回避してはなりません。お客様は、[www.google.com/analytics/policies/](http://www.google.com/analytics/policies/)（または Google が指定したその他の URL）に掲載される、該当するすべての Google アナリティクス ポリシー（「Google アナリティクス ポリシー」）に従うものとします。このポリシーは随時改訂されることがあります。

お客様は、Google アナリティクスと特定の Google の広告サービスの統合バージョン（「Google アナリティクスの広告向け機能」）を利用でき、その際 Google アナリティクスの広告向け機能に関するポリシー（<https://support.google.com/analytics/answer/2700409?hl=ja&topic=2611283>）に従うものとします。お客様が Google の広告サービスにアクセスし、これを使用する際は、当該サービスに関してお客様と Google との間に適用される規約に従うこととします。

プラットフォーム ホームを使用する場合は、<https://support.google.com/marketingplatform/answer/9047313> または Google が指定したその他の URL に掲載されるプラットフォーム ホーム追加規約（規約が改名された場合は、改名後の規約）が適用されます。この利用規約（「プラットフォーム ホーム利用規約」）は随時改訂されることがあります。



## Googleアナリティクスの利用におけるサイト管理者の通知状況

また、Google アナリティクスの広告向け機能を利用する場合は、①広告機能の内容、②Cookieの利用状況、③オプトアウトの方法についても通知を求めている。

### Google アナリティクス利用規約

#### 7. プライバシー

お客様は、Google が個人情報として使用または認識できる情報を Google に送信したり、第三者によるかかる行為を支援または許可したりしないものとします。お客様は適切なプライバシー ポリシーを用意および遵守し、ユーザーからの情報を収集するうえで、適用されるすべての法律、ポリシー、規制を遵守するものとします。お客様はプライバシーポリシーを公開し、そのプライバシーポリシーで Cookie の使用、モバイル デバイスの識別情報 (Android の広告識別子、iOS の広告識別子など)、またはデータの収集に使われる類似の技術について必ず通知するものとします。また、Google アナリティクスを使用していること、および Google アナリティクスでデータが収集、処理される仕組みについても開示する必要があります。こうした情報を開示するには、「ユーザーが Google パートナーのサイトやアプリを使用する際の Google によるデータ使用」のページ ([www.google.com/intl/ja/policies/privacy/partners/](http://www.google.com/intl/ja/policies/privacy/partners/)) または Google が随時提供するその他の URL へのリンクを目立つように表示します。お客様は、本サービスに関連してユーザーのデバイス上で Cookie やその他の情報を保存、アクセスする行為が発生し、かかる行為に関する情報の提供とユーザーからの同意が必要であると法律で定められている場合には、ユーザーに明確かつ包括的な情報を提供し、同意を得るための商業上合理的な努力を払うものとします。

お客様は本サービスに含まれるプライバシー機能 (オプトアウトなど) を一切回避してはなりません。お客様は、[www.google.com/analytics/policies/](http://www.google.com/analytics/policies/) (または Google が指定したその他の URL) に掲載される、該当するすべての Google アナリティクス ポリシー (「Google アナリティクス ポリシー」) に従うものとします。このポリシーは随時改訂されることがあります。

お客様は、Google アナリティクスと特定の Google の広告サービスの統合バージョン (「Google アナリティクスの広告向け機能」) を利用でき、その際 Google アナリティクスの広告向け機能に関するポリシー (<https://support.google.com/analytics/answer/2700409?hl=ja&topic=2611283>) に従うものとします。お客様が Google の広告サービスにアクセスし、これを使用する際は、当該サービスに関してお客様と Google との間に適用される規約に従うこととします。

プラットフォーム ホームを使用する場合は、<https://support.google.com/marketingplatform/answer/9047313> または Google が指定したその他の URL に掲載されるプラットフォーム ホーム追加規約 (規約が改名された場合は、改名後の規約) が適用されます。この利用規約 (「プラットフォーム ホーム利用規約」) は随時改訂されることがあります。

(出所) Google アナリティクス利用規約  
(<https://marketingplatform.google.com/about/analytics/terms/jp/>) (2022年2月17日アクセス)  
Google アナリティクスの広告向け機能に関するポリシー要件  
(<https://support.google.com/analytics/answer/2700409>) (2022年2月17日アクセス)

### Google アナリティクスの広告向け機能に関するポリシー要件

Google アナリティクスの広告向け機能を使用すると、アナリティクスの標準設定にはない機能を利用できるようになります。広告向け機能には以下のようなものがあります。

- Google アナリティクス リマーケティング
- Google ディスプレイ ネットワークのインプレッション レポート
- Google アナリティクスのユーザー属性とインタレスト カテゴリに関するレポート
- 広告掲載目的のデータ収集 (広告 Cookie と識別子によるデータ収集を含む) のために Google アナリティクスを必要とする統合サービス

広告向け機能を有効にすると、Google アナリティクスの標準設定で収集されるデータに加え、Google 広告 Cookie と識別子を使ったトラフィック データも収集できるようになります。Google アナリティクスへのデータの送信方法 (Google アナリティクス トラッキング コードや Google アナリティクス SDK、Measurement Protocol 経由など) に関係なく、Google アナリティクスの広告向け機能を使用する場合は、次のポリシーを遵守する必要があります。

Google アナリティクスの広告向け機能を使用する際、お客様は、適用されるすべてのデータ保護法の下で唯一のデータ管理者となります。

つまり、ユーザーを識別したり、個人情報と、Google の広告サービスまたは広告機能を介して収集されたその他の情報を結び付けることはできません。そうしたユーザーの識別や情報の結び付けを行うには、ユーザーにその旨を明確に通知し、事前にユーザーの同意を得る (ユーザーがオプトインする) とともに、そうした識別や情報の結び付けを明示的にサポートする Google アナリティクスの機能を使用している必要があります。ユーザーの同意の有無にかかわらず、Google レポートの集計データから個人のデータを導き出すことはできません。

#### Google の契約とポリシーにおける PII についての詳細

Google アナリティクスの広告向け機能を有効にしている場合は、サイトに掲載するプライバシー ポリシーで、ユーザーに次の情報を開示する必要があります。

- 導入済みの Google アナリティクスの広告向け機能の内容。
- お客様とサードパーティ ベンダーが、Google アナリティクスの Cookie などのファーストパーティ Cookie (または他のファーストパーティ ID) と Google の広告 Cookie などのサードパーティ Cookie (または他のサードパーティ ID) を組み合わせ、どのように使用しているか。
- 使用している Google アナリティクスの広告向け機能をユーザーはどのような方法でオプトアウトできるか (広告設定、モバイルアプリ向けの広告設定、NAI が定める消費者向けのオプトアウトを含むその他の利用可能な方法など)。

Google アナリティクスで現在利用できるブラウザ用のオプトアウト アドオン をユーザーに提示することもおすすめします。

# 「Googleアナリティクスを通じたデータの収集・処理の仕組み」に関して自社の説明ページへのリンクを求める以外、サイト管理者に対し具体的な通知方法に関する案内は行っていない。

### サイト管理者に対しプライバシーポリシー等でのリンクを求めている説明ページ

GOOGLE のサービスを使用するサイトやアプリから収集した情報の GOOGLE による使用

多くのウェブサイトやアプリでは Google のサービスを利用して、そのコンテンツを改善したり無料でサービスを提供したりしています。このように Google のサービスを利用するウェブサイトやアプリは Google と情報を共有します。

たとえば、広告サービス（AdSense など）や分析ツール（Google アナリティクスなど）を利用しているウェブサイトや、YouTube の動画コンテンツを埋め込んでいるウェブサイトを開覧すると、お使いのウェブブラウザから Google に特定の情報が自動的に送信されます。このような情報には、アクセスしたページの URL やユーザーの IP アドレスなどがあります。また、Google がお使いのブラウザに Cookie を設定したり、既存の Cookie を読み取ったりする場合があります。さらに、Google の広告サービスを利用しているアプリは、アプリの名前や広告配信用の固有の識別子などの情報を Google と共有します。

Google は、サービスの提供、維持、および改善、新サービスの開発、広告の効果測定、不正行為の防止、Google とパートナーのサイトやアプリに表示されるコンテンツおよび広告のカスタマイズを目的に、サイトやアプリによって共有される情報を使用します。個々の目的に沿ったデータの処理方法に関して詳しくは、Google の [プライバシー ポリシー](#) をご覧ください。Google の広告、広告配信におけるユーザー情報の利用方法、Google によるユーザー情報の保持期間に関して詳しくは、[広告](#)のページをご覧ください。

Google の [プライバシー ポリシー](#) は、お客様の情報の処理について Google が依拠する法的根拠を説明しています。たとえば、お客様の同意を得て、または Google の正当な利益（ユーザーのニーズに合わせたサービスの提供、維持、向上など）を追及する目的で、お客様の情報を処理することがあります。

なお、サイトやアプリから共有される情報を Google が処理する場合、そのサイトやアプリは、Google にお客様の情報の処理を許可する前に、お客様に同意を求めます。たとえば、サイトで収集された情報を Google が処理することに同意を求めるメッセージが、サイトのバナーに表示されることがあります。その場合、Google は、Google プライバシー ポリシーに記載されている法的根拠ではなく、サイトやアプリでのお客様の同意条項に記載されている目的を遵守します。同意を変更または撤回する場合は、該当するサイトまたはアプリにアクセスして行ってください。

## Googleアナリティクスの利用におけるサイト管理者の通知状況

# Googleが求める通知内容を十分に満たす通知を行っているサイト管理者はごく僅かに限られると思われる。

## Googleアナリティクスの利用に関する通知例（東京都環境局）

### 利用するアクセス解析ツール、取得する情報及び利用目的

当サイトにおいて利用するアクセス解析ツール、ツールの利用により取得する情報及びその利用目的は次のとおりです。

#### Google Analytics

- ツール提供者  
Google Inc.
- 取得する情報  
皆様のWebサイトの利用状況（アクセス状況、トラフィック、ルーティング等）
- 利用目的  
利便性の向上やサイトの改善のため

### Googleアナリティクスの利用有無

※なお、過去に当サイトを訪問された方が特定のページを訪問した際にお知らせ（広告）を配信することがあります。

皆様のWebサイトの利用状況については、Google社も取得し、利用します。  
詳細については、以下のURLをご確認ください。

- Google Analytics利用規約（外部サイトヘリンク）
- Google のサービスを使用するサイトやアプリから収集した情報の Google による使用（外部サイトヘリンク）

google社のプライバシーポリシーについては、以下のとおりです。

- Googleのプライバシーポリシー（外部サイトヘリンク）

Google Analyticsに関する情報は、以下のサイトからも入手できます。

- Google Analyticsに関する詳細情報（外部サイトヘリンク）  
アナリティクスヘルプ > データのプライバシーとセキュリティ > データの保護

### Googleアナリティクスを通じたデータの収集・処理の仕組み（Googleが指定するページへのリンク）

### 取得しているCookieについて

当サイトでは、アクセス解析のために以下のcookieを取得しております。

※「Cookie一覧」参照

### 取得サイトについて

上記cookieを取得しているのは以下のサイトです。

※「Cookie設定管理ツール(OneTrust)導入サイト一覧」を参照

### 広告での利用について

当サイトでは、Googleなどの広告配信事業者の広告サービス（ディスプレイ広告/リマーケティング/リターゲティング機能）を活用し、過去に当サイトを訪問された方が特定のページを訪問した際にお知らせ（広告）を配信することがあります。その際、当サイトの訪問履歴情報を取得するためにCookieを利用します。

なお、こうしたお知らせ（広告）をご希望でない場合は、お手数ですが下記「Cookie及び類似技術を無効にする方法」からデバイスに保存されたCookieの削除及びCookieを無効にしてください。

ブラウザの変更、Cookieの削除及び新しいデバイスへ変更を行なった場合には、再度設定が必要となります。

- ① 広告機能の内容
- ② Cookieの利用状況

### Cookie及び類似技術を削除・無効にする方法

#### (3) 広告配信のCookieに関して

広告配信のCookieに関しては、以下をクリックし、オプトアウトすることによって機能利用を無効化することができます。ただし、ブラウザの変更、Cookieの削除等の場合には、再度オプトアウトが必要となります。

- ヤフー株式会社 <http://btoptout.yahoo.co.jp/optout/preferences.htm>（外部サイトヘリンク）
- グーグル株式会社 <https://policies.google.com/privacy/>（外部サイトヘリンク）
- Facebook <https://www.facebook.com/legal/terms>（外部サイトヘリンク）
- スマートニュース株式会社 <http://www.smartnews-ads.com/optout>（外部サイトヘリンク）

#### (4) Google Analytics オプトアウト アドオン

Google Analytics オプトアウト アドオンを利用してGoogle Analyticsのトラッキングを拒否することも可能です。

Google Analytics オプトアウト アドオンは、JavaScriptによるデータの使用をウェブサイトのユーザーが無効にできるように開発された機能です。この機能を利用するには、このアドオンをダウンロードして、ご利用のブラウザにインストールしてください。

- Google Analytics オプトアウト アドオン（外部サイトヘリンク）

- ③ オプトアウトの方法

## 参考：海外の関連動向

# 2022年1月以降、Googleアナリティクスの利用を通じた米国へのデータ移転に関して、GDPR違反とする決定がオーストリア・フランスのデータ保護当局から下されている。

### ■ 背景：

- オーストリアの人権擁護団体noybが2020年8月にGoogle、Facebookのサービスにおいて米国へのデータ移転が生じていることはGDPR違反であるとして、欧州各国のデータ保護当局に対して行った101件の申し立ての一部に関する決定が明らかとなったもの。
- 本決定には2020年7月に欧州司法裁判所が下した欧州・米国間のデータ保護協定「プライバシーシールド」を無効とする判決（シュレムスII判決）が影響していると思われる。

### ■ 決定の内容：

- 米国に移転されたデータは米国の情報機関によるアクセスの可能性を排除するものではないため、GDPR44条（移転に関する一般原則）に違反する。
- フランスのデータ保護当局（CNIL）は申し立ての対象となったサイト管理者だけでなく、Googleアナリティクスを利用しているその他のサイト管理者に対しても、Googleアナリティクスの利用を中止するか、EU域外へのデータ移転を伴わないツールの利用を行うよう命じた。

### ■ Googleの反応：

- サイト管理者がコンプライアンスに沿った形でGoogleアナリティクスの利用を継続できるように、収集する分析データをカスタマイズできる管理機能を今後数週間以内に発表するとした。

時期	GoogleアナリティクスのGDPR違反に関する時系列の動き
2022年1月12日	オーストリアのデータ保護当局（DSB）がGoogleアナリティクスを通じた米国へのデータ移転はGDPR違反であるとの決定を公表した
2022年2月4日	GoogleがGoogleアナリティクスに関する追加機能を今後数週間以内に発表すると公表した
2022年2月10日	フランスのデータ保護当局（CNIL）がDSBと同様の決定を公表した

（出所）

noybのプレスリリース（<https://noyb.eu/en/austrian-dsb-eu-us-data-transfers-google-analytics-illegal>）（2022年2月17日アクセス）

CNILのプレスリリース（<https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply>）（2022年2月17日アクセス）

Googleのお知らせ（<https://support.google.com/analytics/answer/11609059?hl=ja>）（2022年2月17日アクセス）

## 位置情報の取得・利用実態

---

# アプリ事業者が取得する位置情報の多くは、オペレーションソフト（OS：Android、iOS）が提供する情報をAPI※経由で取得しているものである。

- OSは、GPS、携帯電話基地局、Wi-Fi、Bluetooth Beacon等から、端末の位置情報を生成している。
- OSベンダー（Google、Apple）は、電力消費量と位置の精度とを天秤にかけた、複数の情報ソースを提供している。

例）正確な位置情報を提供する代わりに電力消費量が多い情報ソース

OS別の位置情報の提供方法

OS APIの内容	Android (Google)	iOS (Apple)
位置情報を取得する パッケージ	Fused Location Provider Client (他にLocation ManagerやSensor Managerが存在)	Core Location
情報ソースの種類	<ul style="list-style-type: none"> <li>● <b>PRIORITY_HIGH_ACCURACY</b> - 可能な限り最も高精度の位置情報をリクエストする。 GPSを使用して位置情報を決定する可能性が高い。</li> <li>● <b>PRIORITY_BALANCED_POWER_ACCURACY</b> - 約100m以内の位置情報をリクエストする。 主にWi-Fiと基地局により位置情報を決定する可能性が高い。</li> <li>● <b>PRIORITY_LOW_POWER</b> - 約10km以内の位置情報をリクエストする。</li> <li>● <b>PRIORITY_NO_POWER</b> - 他のアプリが利用した位置情報の更新データを再利用する。</li> </ul>	<ul style="list-style-type: none"> <li>● <b>Standard location service</b> - 高精度・最新の位置情報を提供する。 ナビゲーションや経路の記録等に利用される。</li> <li>● <b>Significant-change location service</b> - ユーザーの位置に大きな変化があったときに位置情報を提供する。 GPSのような精度を必要とせず、省電力。 ユーザーが歩行中に周辺の観光スポットを案内するとき等に利用される。</li> <li>● <b>Visits location service</b> - ユーザーが滞在後、移動した際に位置情報を提供する。 最も電力効率が良い。</li> </ul>

※ Application Programming Interface

(出所) <https://developer.android.com/training/location?hl=ja> (2022年3月3日アクセス)

[https://developer.apple.com/documentation/corelocation/getting\\_the\\_user\\_s\\_location](https://developer.apple.com/documentation/corelocation/getting_the_user_s_location) (2022年3月9日アクセス)



OSベンダーはユーザーに対して、利用する位置情報の精度と利用タイミングを選択する機会を提供している。



正確：10フィート～160フィート（数m～50m）以内  
おおそ：1マイル（1.6km）以内



正確  
おおそ：5km四方

# OSベンダーは位置情報の利用に関して、アプリの事前審査を行うとともに、アプリ開発者向けの教育コンテンツを提供している。

## Google

- バックグラウンドで位置情報を利用する※アプリをリリースする場合は、Googleによる事前審査を必要とする。

### Google Play Academyにおける教育資料

Google Play Academy

♡ お気に入り ◀ 共有

### Google Play の位置情報の利用許可に関するポリシーを理解する

表示項目 Play Aca

ランタイムのメッセージ

高品質で安  
のひとつで  
ポリシーを  
る方法、デ  
応方法につ

位置情報の利用許可を使用するアプリで、同意を求める場合は、以下のようにする必要があります。

- はっきりと、わかりやすく示す。
- ユーザーに明確な操作を求める（例：タップで同意する、チェックボックスをオンにする）。
- 開示画面から他へ移動する操作（例：タップで移動する、戻るボタンやホームボタンを押す）を同意とみなさない。
- 自動で非表示になるメッセージや閲覧期限付きメッセージを使用しない。

Application

LOCATION

WRITE EXTERNALS

WRITE EXTERNALS

Allow Application to access your contacts?

DENY ALLOW

GET ACCOUNTS

(出所) <https://developer.android.com/training/location?hl=ja> (2022年3月3日アクセス)  
<https://playacademy.exceedlms.com/student/path/82882-google-play> (2022年3月3日アクセス)

## Apple

- App Storeへの上市にあたり、事前審査項目の1つに位置情報サービス (5.1.5) がある。

### App Store Reviewガイドラインにおける説明

#### 5.1.5 位置情報サービス

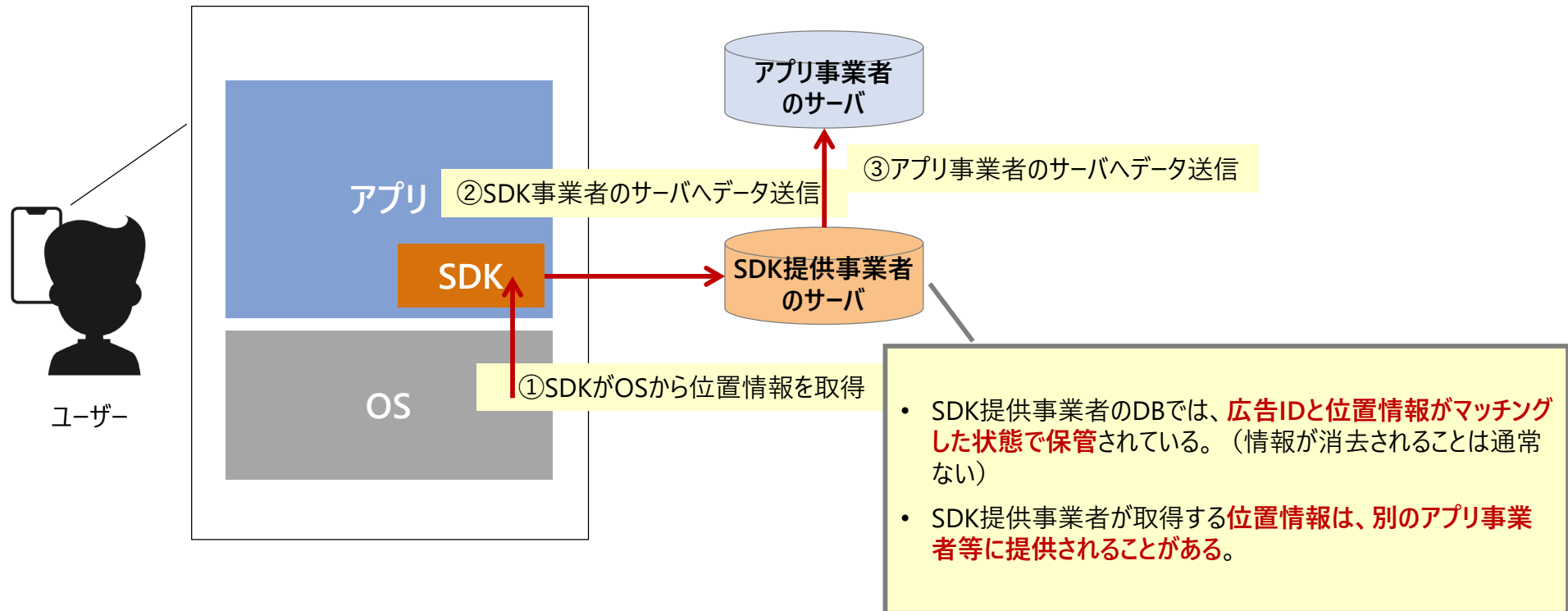
Appで位置情報サービスを使用できるのは、位置情報サービスがAppの機能またはサービスと直接関連する場合のみです。位置情報ベースのAPIは、救急サービスまたは自動車、飛行機、その他デバイスの自律制御のために使用することはできません。ただし、軽量のドローンや玩具などの小型デバイス、またはリモートコントロールの自動車警報システムなどは除きます。位置情報を収集、送信、使用する際は、事前にユーザーに通知し、同意を得る必要があります。Appで位置情報サービスを使用する場合は、Appにおけるこのサービスの目的を説明する必要があります。説明に関するベストプラクティスについては、「[Human Interface Guidelines \(英語\)](#)」を参照してください。

(出所) <https://developer.apple.com/jp/app-store/review/guidelines/#legal>



アプリに位置情報を取得するSDKを搭載している場合、SDK提供事業者が位置情報を取得したうえで、アプリ事業者へ位置情報が連携される。

位置情報取得SDKを搭載している場合の情報連携イメージ



## アプリのOSベンダーおよびSDK提供事業者それぞれにおいて、自主ルールに基づく位置情報の取扱いが進められている。

### ■ OSベンダー（Google、Apple）

- アプリ事業者による位置情報の利用ルールは、OSベンダーによって整備・監督されている。
- Google、Appleは、OSベンダーとして取得した位置情報と、検索等のサービス提供者／アプリ提供者として取得した位置情報とを分けて利用してはいないものと思われる。

### ■ SDK提供事業者

- 広告IDと紐づいた位置情報は、個人関連情報として取り扱われることになると思われるが、利用に関する現状のルールは事業者によって様々である。
- 一般社団法人LBMA Japanは自主規制を制定しているが、その内容は会員のみを開示されており、一般的なユーザーへの理解・浸透が進みやすい状況にあるとは言いづらい。

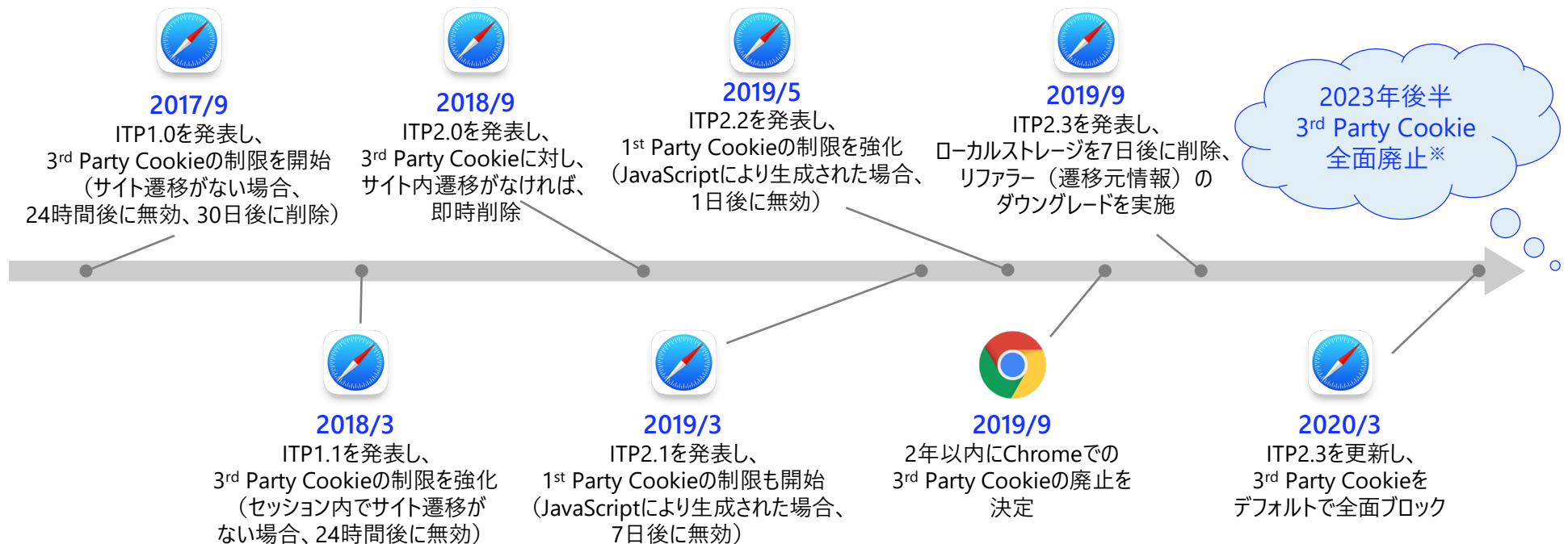
## 3<sup>rd</sup> party cookie廃止を受けた代替技術の動向

---

## 3<sup>rd</sup> party cookie廃止を受けた代替技術の動向

利用者の十分な自覚がないまま、データを収集する仕組みを問題視したAppleやGoogleは独自に3<sup>rd</sup> Party Cookieに対する規制を進めている。

### Apple・GoogleによるCookie規制の流れ



※ 2021/6に英国競争当局（CMA）の指摘を受けて、サードパーティクッキー廃止を1年延期

## 参考) IDFAに関する方針変更

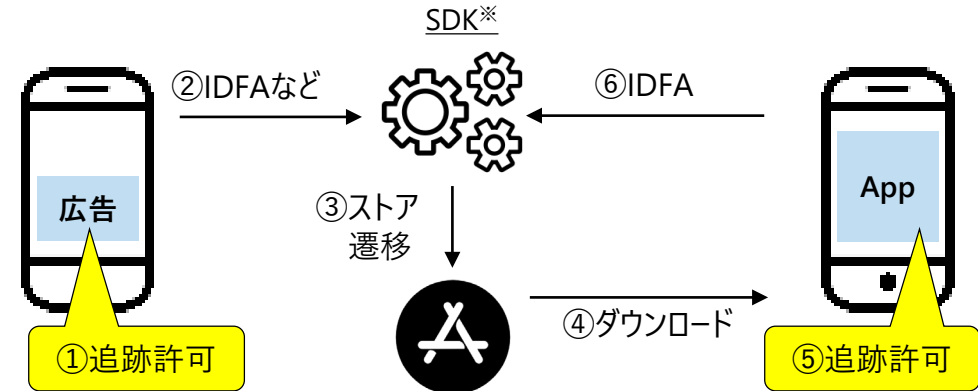
< Worldwide Developers Conference 2020での発表  
(2020年6月) >

- 「IDFA」が2020年秋のiOSのバージョンアップにより、各アプリごとに「IDFAの取得可否を確認する」仕様に変更  
→IDFAオプトイン化が21年初旬に延期され、一部仕様変更 (2020年9月)
- 米フェイスブックなどは「アップルの競争上の利益を追求している」と批判
- Financial Times誌によると、このプライバシー方針の刷新の影響を、テクノロジー調査会社Lotameが試算したところ、Snapchat (Snap)、Facebook、Twitter、YouTubeの大手SNS4社合計98億5,000万ドルの売り上げ減。2021年第3、第4四半期の4社の売上は平均でマイナス12%と試算された
- 同じくFinancial Times誌が取材したEric Seufertによると、Facebook単体でも半年で83億ドルの売り上げ減。
- 一方のAppleは、今年第3四半期の広告売上が2兆円に達し、好調

出所) 日経Xトレンド ( <https://xtrend.nikkei.com/atcl/contents/18/00421/00004/> )、ギズモードジャパン記事 ( <https://www.gizmodo.jp/2021/11/att-blows-9-85-billion-dollar.html> ) などよりNRI作成

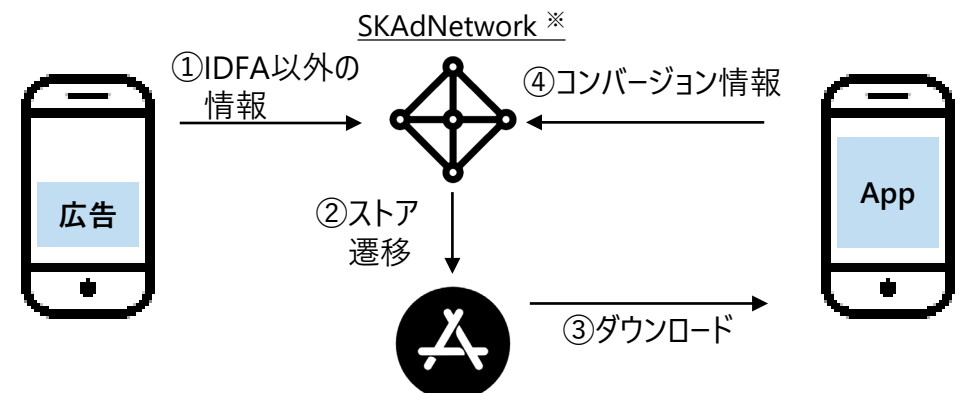
## 今後の広告配信計測方法

### ①これまでと同様の計測 + オプトイン



※SDK：アプリに組み込んで使う、広告配信に必要な機能を、ひとまとめにしたツールキットの総称

### ②Apple提供「SKAdNetwork」を活用



※SKAdNetwork：アップルが提供するプライバシーに配慮したトラッキングツール

足元3rd Party Cookieは取得禁止、広告IDはオプトイン方式へ移行の方向にあり、共通IDやクリーンルーム等の代替手段を模索する動きがある。

Cookieの代替手段として注目されている技術

---

① Unified ID 2.0

② Privacy Sandbox (FLoC ⇒ Topics、FLEDGE)

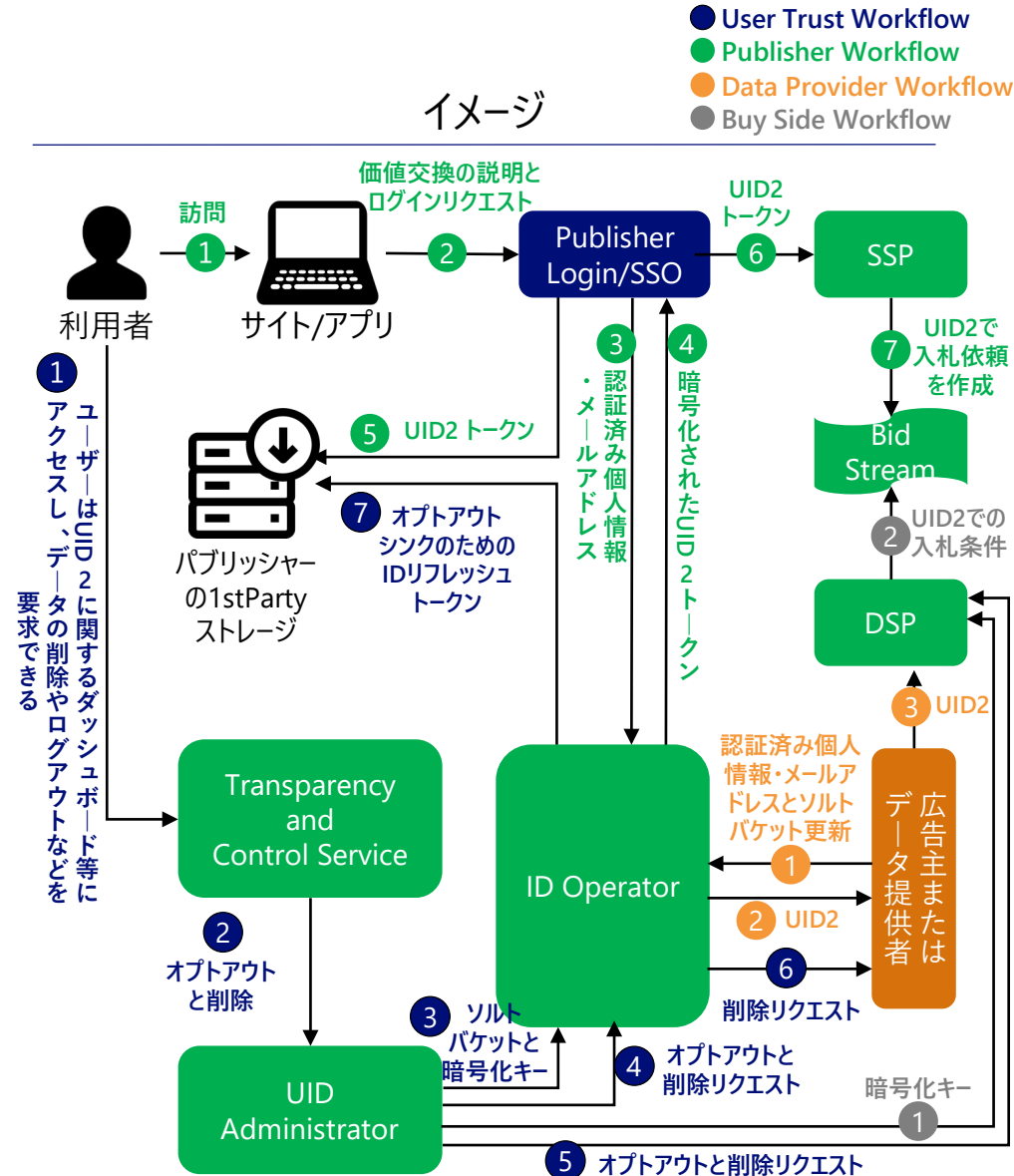
③ データクリーンルーム

# 代替手段① Unified ID 2.0

## ソリューションの概要

名称	Unified ID 2.0 (UID2)
提供組織	米国業界団体イニシアチブ「PRAM」と IAB TechLabの「Project Rearc」が推進 ※TradeDesk社が開発したUnifiedIDを元に発展
概要	<ul style="list-style-type: none"> <li>• 利用者のメールアドレスを暗号化・ハッシュ化することで識別子を作成し、利用する仕組み</li> <li>• 識別子は定期的に再作成し、独立した機関が管理する</li> <li>• 2021年よりオープンソースとして公開し、管理を独立した機関に移管。</li> </ul> <p>※主要な特徴</p> <ul style="list-style-type: none"> <li>✓ ユーザーの<b>事前同意 (オプトイン) 前提</b></li> <li>✓ <b>特定企業に依存しない</b>独立運営</li> <li>✓ <b>メールアドレス</b>を元にした共通ID</li> <li>✓ Cookieに依存しない</li> <li>✓ <b>一度のオプトアウトで、すべての利用が停止される</b></li> </ul>

## イメージ



## 参考：UnifiedID2.0の推進に関わる業界団体・取り組み

### Project Rearch

名称	Project Rearch
概要	<ul style="list-style-type: none"><li>2020年2月にカリフォルニアで開催された、IABの年次総会で発表されたIAB Tech Labが中心となって取り組んでいるプロジェクト</li><li>3rdPartyCookie廃止等の議論がある中、ポストCookie時代のフレームワークを開発する取り組みとして設立</li><li>現時点（2021年12月現在）で4つのパブリックコメントを発表<ul style="list-style-type: none"><li>✓ Global Privacy Platform</li><li>✓ Accountability Platform</li><li>✓ Best Practices for User-Enabled Identity Tokens</li><li>✓ Taxonomy and Data Transparency Standards to Support Seller-defined Audience and Context Signaling</li></ul></li></ul>

出所) IAB Tech Lab公式サイト「Project Rearch: How To Participate」( <https://iabtechlab.com/project-rearc/> ) (2021年12月7日アクセス)

### PRAM

名称	PRAM： (Partnership for Responsible Addressable Mediaの略称)
概要	<ul style="list-style-type: none"><li>2020年8月に発足</li><li>プライバシーを保護し、消費者体験を向上させながら、デジタルメディアや広告のカスタマイズ・分析などの重要な機能を進化させるために、世界の広告業界のあらゆるセクターを代表する主要な広告業界団体と企業が協力する取り組み</li><li>Project Rearchでは参加が少なかった、バイサイドのトップ層が積極的に招集されている</li><li>Project Rearchは、PRAMの技術的基盤として継続、またIAB Tech Labが「技術標準ワーキンググループ」を主導</li><li>参加団体：<ul style="list-style-type: none"><li>✓ 業界団体：4A's（全米広告業協会）、ANA（全米広告主協会）、IAB、IAB Tech Lab、Network Advertising Initiative (NAI)、WFA（世界広告主連盟）</li><li>✓ 広告主：フォード、ゼネラルモーターズ、IBM、P&amp;G、ユニリーバ、マスターカード</li><li>✓ エージェンシー：UM（an IPG Mediabrands company）、Publicis Media</li><li>✓ パブリッシャー：NBCUniversal</li><li>✓ テック企業：Adobe、LiveRamp、MediaMath、The Trade Desk など</li></ul></li></ul>

出所) IAB Tech Labブログ「IAB TECH LAB, PROJECT REARC AND THE PARTNERSHIP FOR RESPONSIBLE ADDRESSABLE MEDIA」( <https://iabtechlab.com/blog/tech-lab-and-partnership-for-responsible-addressable-media/> ) (2021年12月7日アクセス)



## 参考： Unified ID 2.0に関する直近の情勢

#	概要	詳細	日時
1	PRAMによるポストクッキー技術基盤のソースコード募集※1	<ul style="list-style-type: none"> <li>「Partnership for Responsible Addressable Media (PRAM)」が、プライバシーに配慮したアドレサビリティ実現のため、業界各社が保有／開発しているソリューションのコード提供（譲渡）を呼びかけ</li> <li>TradeDesk社がこれに応じ、開発していたUnifiedID 2.0のコードを提供し、PRAMとProject Rearcにより検証が開始</li> </ul>	2021年2月
2	Unified ID2.0のオープンソース化が発表される※3	<p>IAB Tech Labにより、正式なオープンソース化が発表された</p> <ul style="list-style-type: none"> <li>誰もがアップデートや変更を提案して機能追加し、プロジェクトをサポートできる</li> <li>技術開発は、IAB Tech LabのアドレサビリティワーキンググループとPrivacy &amp; Rearc コミットグループが指揮する</li> <li>開発したThe Trade Deskは、引き続き「貢献者 (contributor)」として関与</li> <li>Prebid.orgは、引き続き「オペレーター (operator)」組織のひとつとして、IDトークン生成を担う</li> </ul>	2021年5月
3	IAB Tech Labが「オープンソースイニシアチブ」を開始※4	<p>IAB Tech Labが、広告業界全体の透明性と協調性を高めることを目的とした、オープンソース・イニシアチブの立ち上げを発表</p> <ul style="list-style-type: none"> <li>GitHubに設置されたOpen Source Initiativeで、関連するオープンソースプロジェクトを一箇所にまとめて管理</li> <li>標準的な実装や、標準の導入に役立つツールの提供、実装のベストプラクティスとしてサンプルや参照規格を共有</li> <li>初期のコード提供プロジェクトの1つにUnified ID2.0が含まれる</li> </ul>	2021年7月

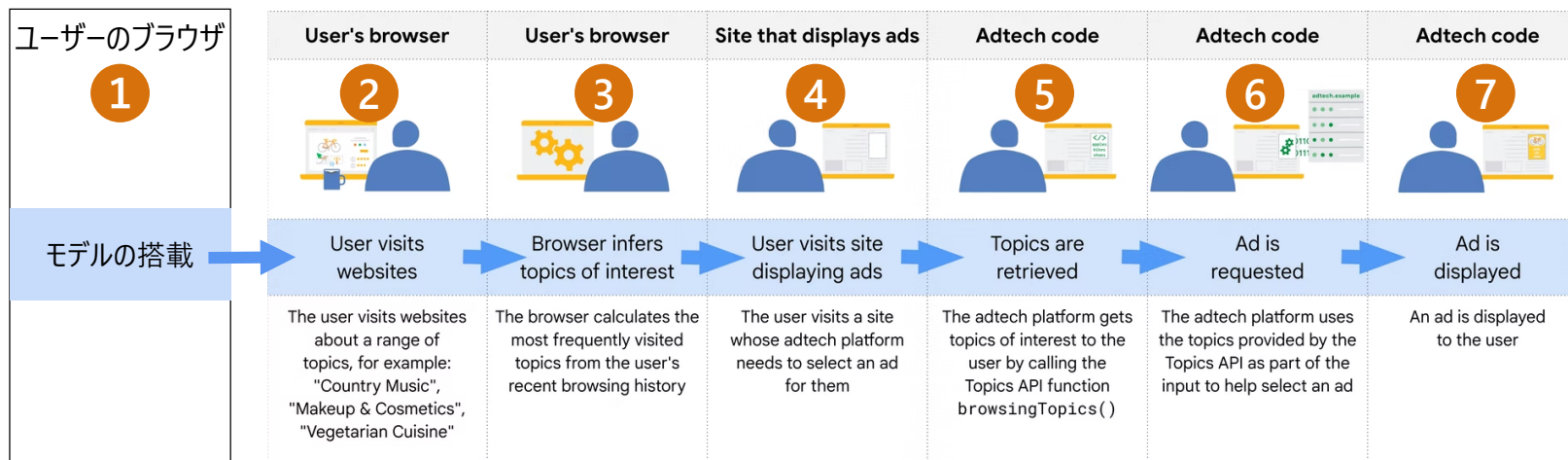
※1：「Partnership for Responsible Addressable Media (PRAM) プレスリリース「PARTNERSHIP FOR RESPONSIBLE ADDRESSABLE MEDIA INVITES INDUSTRY TO CONTRIBUTE ADDRESSABILITY CODE FOR COLLABORATIVE DEVELOPMENT」 (<https://www.responsibleaddressablemedia.com/pram-addressable-code-release>) (2021年12月7日アクセス)

※2：IABTech Lab公式ブログ「THE IMPACT OF THE TRADE DESK CONTRIBUTING UID 2.0 FOR INDUSTRY DEVELOPMENT」 (<https://iabtechlab.com/blog/the-impact-of-the-trade-desk-contributing-uid-2-0-for-industry-development/>) (2021年12月7日アクセス)

※3：IABTech Lab公式ブログ「IAB Tech Lab Launches Open Source Initiative To Increase Cross-Industry Transparency And Collaboration And Trust」 (<https://iabtechlab.com/press-releases/iab-tech-lab-launches-open-source-initiative-to-increase-cross-industry-transparency-and-collaboration-and-trust/>) (2021年12月7日アクセス)

## 代替手段② Topics

### Topicsに基づく広告表示のイメージ



- 1 ユーザーのブラウザに、ウェブサイトのドメイン名とトピックを紐づける機械学習モデルを搭載する
- 2 ユーザーがウェブサイトを訪問すると、訪問先サイトに応じたトピックがブラウザに保存される（例：フィットネスサイト⇒スポーツのトピック）
- 3 ブラウザにおいて、ユーザーの直近、最も関心の高いトピックが推定される
- 4 ユーザーが広告表示付きのウェブサイトを訪問する
- 5 アドテックプラットフォームが、ブラウザからトピックを受け取る
- 6 アドテックプラットフォームが、トピックにあわせた広告を配信する
- 7 広告が表示される

## Topicsは個別サイトの閲覧履歴を必要としない点で、3<sup>rd</sup> Party Cookieよりもプライバシー性が高いとGoogleは説明している。

### Topicsに関するGoogleの説明

Q：3rd Party Cookieと比べて、どのような点でプライバシー性が高いか

A：Topicsは、正確な訪問履歴や他サイトでの身元・行動を特定する必要がない点で、3rd Party Cookieよりプライバシー性が高いと考えられる。

Q：ユーザーは自分のトピックを確認することができるか

A：ユーザーはブラウザ上で、自身のトピックを確認できるほか、必要に応じて削除することができる。また、Topicsに基づく広告表示を利用しないことも選択できる。

Q：全てのトピックは公開されるか

A：公開される予定。現在、Googleによって約350のトピックが検討されているが、今後、オープンな形で第三者の協力を得ながら、数百～数千に増やしていくことを想定している。なお、人種、性的指向、宗教などの、センシティブなカテゴリはトピックに含めない。

Q：ブラウザのトピックは、どのくらいの頻度で更新されるか

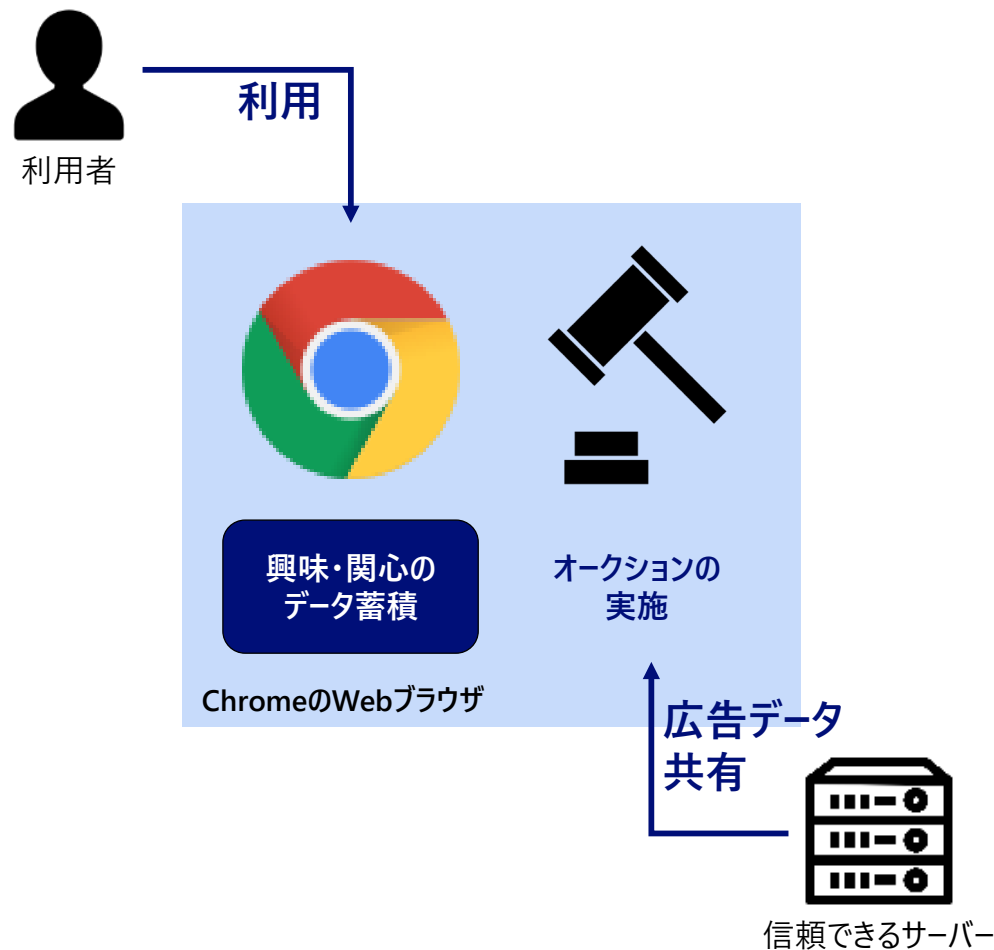
A：週次での更新を想定している。

## 代替手段③ FLEDGE

### ソリューションの概要

名称	FLEDGE
提供組織	Google
概要	<ul style="list-style-type: none"> <li>・ プライバシーサンドボックスで開発されているAPIの一つ</li> <li>・ Google提案の「TURTLEDOVE：ユーザーの興味・関心といった情報をブラウザに保存し、広告主がそれを利用可能にする仕組み」に企業の対案を反映したアップデート版</li> <li>・ FLEDGEは、リマーケティングを目的としたソリューションで、第三者がサイト間で利用者の閲覧行動を追跡できない設計             <ul style="list-style-type: none"> <li>✓ 広告主が定義する広告グループと利用者のブラウザの関連付けは、利用者のブラウザに保管される。</li> <li>✓ 利用者のブラウザが、広告を選択する「オークション」を実施。これは利用者のデバイス上でローカルに行われる。</li> <li>✓ 広告主が広告グループのデータを、利用者に関する他の情報、特に個人を識別できる情報やアクセスしたページの情報と組み合わせることはできない。広告主は、利用者がサイト運営者のサイトで、どのページを表示しているかを確認することはできない。</li> <li>✓ Webサイトおよび、それらのサイトが使用する広告ネットワークは、訪問者の興味のある広告、または広告グループの情報を利用することはできず、広告の選択は利用者のブラウザ上で行われる。</li> </ul> </li> </ul>

### イメージ



## 参考：PrivacySandboxに関する直近の情勢

#	概要	詳細	日時
1	英国の競争市場局（CMA）による調査※1	英国の競争市場局（CMA）がPrivacySandboxについて調査を開始： <ul style="list-style-type: none"> <li>1月調査開始→6月にGoogleのコミットメントに対しコンサルテーション→協議・修正可能性を検討→11月に修正コミットメントのコンサルテーション・協議→12月～変更後のコミットメントに対する意見の検討</li> </ul>	2021年1月
2	米司法省による独占禁止法違反の疑い※2	<ul style="list-style-type: none"> <li>アメリカ・テキサス州のケン・パクストン司法長官が訴状を更新、PrivacySandboxについて批判する文言を追加。</li> </ul>	2021年3月
3	電子フロンティア財団による批判※3	<ul style="list-style-type: none"> <li>FLoCについて「トラッカーは、このIDをユーザの絞り込みに使うことができ、ほかのトラッキング技術と組み合わせることでトラッキングを助長することにつながる」と非難し、「トラッキングの再発明ではなく、ターゲティング広告の無数の問題のない、より良い世界を想像するべき」と提言</li> </ul>	2021年4月
4	Microsoftのブラウザ「Edge」でFLoCが無効化されていると報道※4	<ul style="list-style-type: none"> <li>Googleが管理するオープンソースのエンジン「Chromium」を使うマイクロソフト社のEdgeで、FLoCが無効化されていることが明らかに。（「Chromium」でFLoCはデフォルトで有効）</li> <li>なお、同様に「Chromium」利用のブラウザでは「Brave」や「Vivaldi」もFLoCへの批判・懸念の指摘を実施し、採用しないことを明言</li> </ul>	2021年4月
5	欧州委員会がGoogleを独占禁止法違反で調査※5	オンライン広告技術の、市場における反競争的行為の可能性を調査開始： <ul style="list-style-type: none"> <li>調査内容として、PrivacySandboxの市場への影響調査が含まれている</li> </ul>	2021年6月
6	PrivacySandboxに関するコミットメントの提示※6 （CMA調査を受けて）	<ul style="list-style-type: none"> <li>英国の競争市場局（CMA）によるフィードバックなどを踏まえたコミットメントの提示</li> </ul>	2021年6月
7	プライバシー サンドボックスのマイルストーンに関する最新のタイムライン公開※7	<ul style="list-style-type: none"> <li>30以上の提案があり、うち4つはオリジン・トライアルで利用可能。Chromeでは2022年後半までの、主要な技術の展開を目標とする</li> <li>Chromeでは3rd Party Cookieを2023年半ば～2023年末で段階的に廃止できる。PrivacySandboxの進捗に合わせ、計画では3rdPartyCookieのサポートを2段階で廃止予定</li> </ul>	2021年6月
8	コミットメントの改訂※8 （CMA調査を受けて）	<ul style="list-style-type: none"> <li>英国の競争・市場機構（CMA）などによるフィードバックを踏まえて改訂されたコミットメントを提示</li> </ul>	2021年11月
9	FLoCの廃止、Topicsの開発開始	<ul style="list-style-type: none"> <li>GoogleがFLoC（Federated Learning of Cohorts）の開発を停止し、代わってTopicsの開発を発表した。</li> </ul>	2022年1月

※1：CMAリリース記事「CMA to investigate Google's 'Privacy Sandbox' browser changes」 (<https://www.gov.uk/government/news/cma-to-investigate-google-s-privacy-sandbox-browser-changes>) (2021年12月7日アクセス)

※2：THE VERGE記事「Google antitrust suit takes aim at Chrome's Privacy Sandbox」 (<https://www.theverge.com/2021/3/16/22333848/google-antitrust-lawsuit-texas-complaint-chrome-privacy>) (2021年12月7日アクセス)

※3：電子フロンティア財団コラム「Google's FLoC Is a Terrible Idea」 (<https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea>) (2021年12月7日アクセス)

※4：BLEEPINGCOMPUTER記事 (<https://www.bleepingcomputer.com/news/microsoft/microsoft-disables-googles-floc-tracking-in-microsoft-edge-for-now/>) (2021年12月7日アクセス)

※5：欧州委員会プレスリリース「Antitrust: Commission opens investigation into possible anticompetitive conduct by Google in the online advertising technology sector」 ([https://ec.europa.eu/commission/presscorner/detail/en/ip\\_21\\_3143](https://ec.europa.eu/commission/presscorner/detail/en/ip_21_3143)) (2021年12月7日アクセス)

※6：Google公式ブログ記事「Our commitments for the Privacy Sandbox」 (<https://blog.google/around-the-globe/google-europe/our-commitments-privacy-sandbox/>) (2021年12月7日アクセス)

※7：Google公式ブログ記事「An updated timeline for Privacy Sandbox milestones」 (<https://blog.google/products/chrome/updated-timeline-privacy-sandbox-milestones/>) (2021年12月7日アクセス)

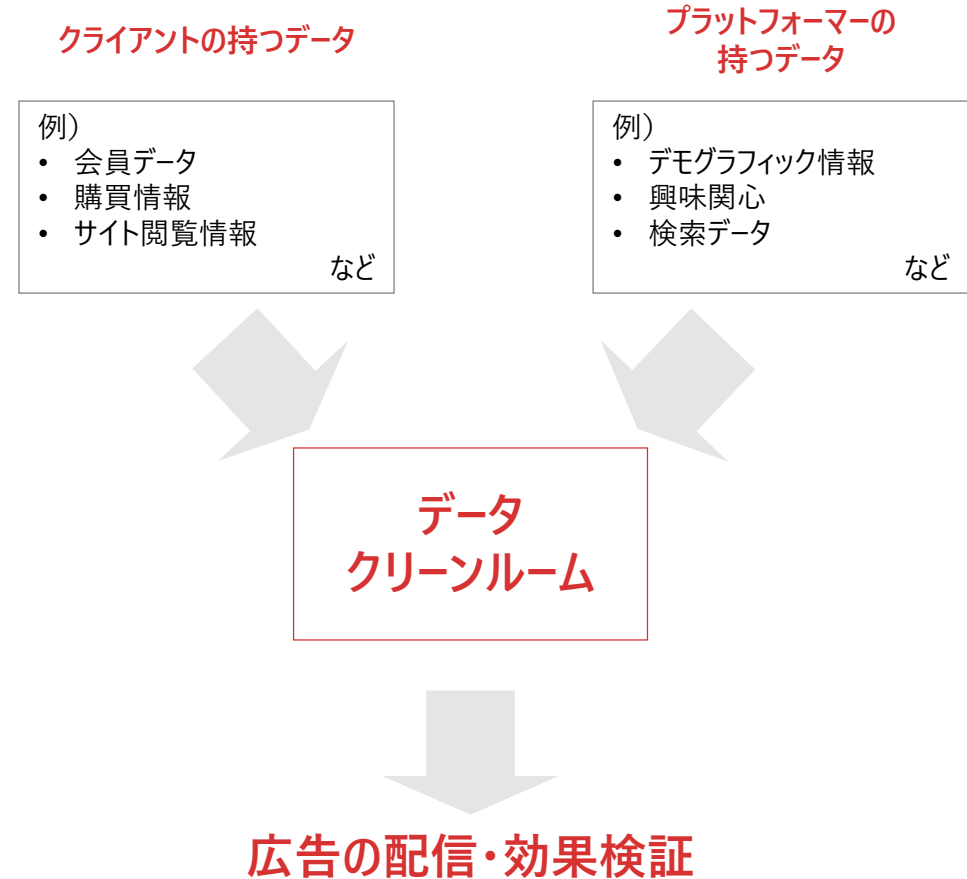
※8：Google公式ブログ記事「An update on our Privacy Sandbox commitments」 (<https://blog.google/around-the-globe/google-europe/update-our-privacy-sandbox-commitments/>) (2021年12月7日アクセス)

## 代替手段④ データクリーンルーム

### ソリューションの概要

名称	- (個別のサービス名ではない)
提供組織	Google、Amazon、Facebook、電通 (+ Twitter、ドコモ)、ヤフーなど
概要	<ul style="list-style-type: none"><li>個人情報を保有するサービス利用者（広告主等）とサービスを提供するサービス提供者（プラットフォーム等）が<b>双方のデータを突合して、広告施策を実施する</b>サービス。</li></ul> <p>※下記のような技術的な安全策が講じられる。</p> <ul style="list-style-type: none"><li>✓ サービス利用者のデータに、サービス提供者はアクセスできない</li><li>✓ サービス利用者は、突合されるサービス提供者の個人データを利用できない</li><li>✓ サービス利用者が得られる突合の結果は統計情報であり、個人データと紐づけることができない</li></ul>

### イメージ





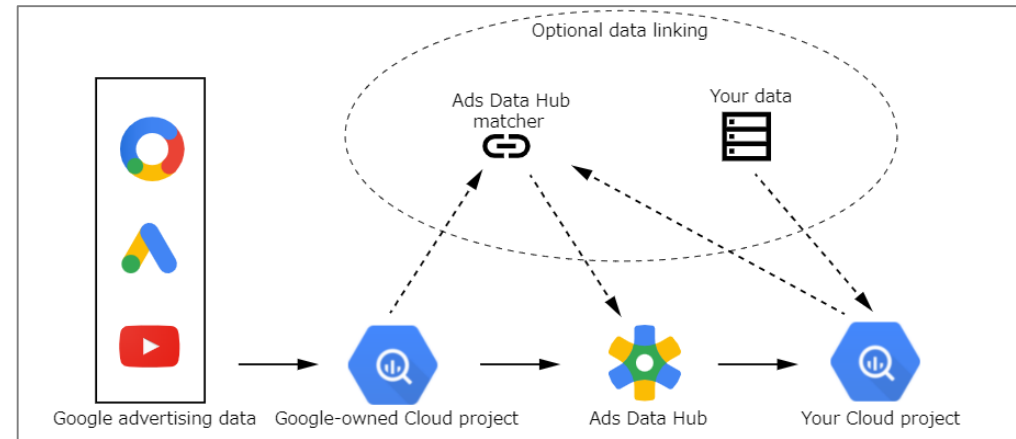
## 代替手段④' Google Ads Datahub

### ソリューションの概要

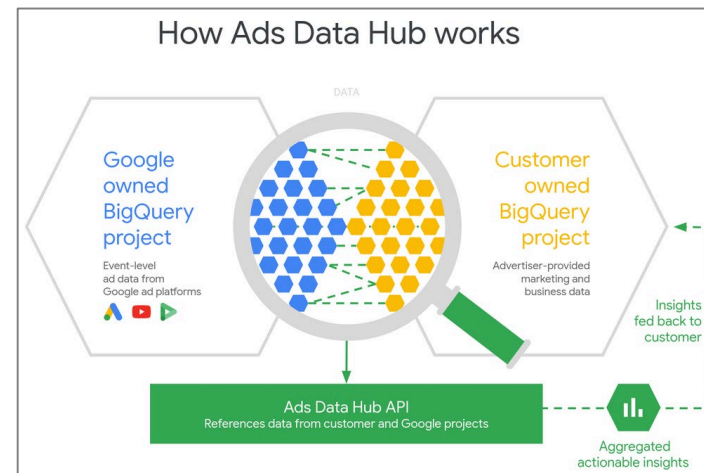
名称	Google Ads Datahub
提供組織	Google
概要	<ul style="list-style-type: none"> <li>• グーグルが提供しているデータクリーンルーム</li> <li>• Chromeがアドテクノロジーの会社向けに提供しているプライバシーセーフティな分析・セグメント作成が可能なプラットフォーム</li> <li>• <b>2017年にベータ版をローンチ</b>、以後適宜内容がアップデートされている             <ul style="list-style-type: none"> <li>• <u>広告キャンペーンの結果やインサイトをレポート</u></li> <li>• 対象広告はYouTube、Google Display Network (GDN)、DoubleClick</li> <li>• 利用者は <u>Google Cloud にアクセスし BigQuery を使ってレポートを作成する</u></li> <li>• 利用者は、<u>CRM (顧客データ) などの自社データや第三者データを Ads Data Hub にインポートし、Google 広告データと統合することが可能</u></li> <li>• プライバシー保護の観点から、Ads Data Hub から得られるのはレポート結果のみ</li> </ul> </li> </ul>

出所) Google社AdsDataHub紹介ページ (<https://developers.google.com/ads-data-hub/>) やブログ (<https://www.countand1.com/2017/05/google-ads-data-hub-beta-launch.html>) よりNRI作成

### イメージ



出所) Google社AdsDataHub紹介ページ (<https://developers.google.com/ads-data-hub/guides/intro>) より引用



出所) Google社ブログ「Investing in the next generation of measurement on YouTube」 (<https://www.blog.google/products/ads/investing-next-generation-measurement-youtube/>) より引用

## 参考：データクリーンルームに関する直近の情勢

#	概要	詳細	日時
1	GoogleがAdsDatahubを開始※1	GoogleがAds Data Hubのベータ版をローンチ	2017年5月
2	Facebook（現Meta）がAdvanceAnalyticsを発表※2	2018年5月、カリフォルニア州で開発者会議「F8」を開催し、Facebook・Messenger・Instagramの新機能として紹介。	2018年5月
3	AmazonがMarketing Cloudを開始※3,4	「Amazon Marketing Cloud」のベータ版をローンチ(2021年正式リリース※4)	2019年
4	電通・docomoによる「docomo data square」を提供開始※5	株式会社NTTドコモ、株式会社電通、株式会社電通デジタル、株式会社LIVE BOARD、株式会社D2Cの5社が、TVCM、WEB広告やデジタルOOH広告の接触から商品購買までの効果測定がID単位で可能となる、「docomo data square」の提供を開始	2020年8月
5	電通・Twitterによるデータクリーンルーム発表※6	次世代型データ統合基盤である、Data Clean Room「Twitter Data Hub Omusubi（以下、Omusubi）」の提供開始を発表	2021年10月
6	Permutive社が7,500万ドルを調達※7, 8	クリーンルームを提供するPermutive社が、ソフトバンクビジョンファンドから7,500万ドルを調達	2021年11月

※1：Google公式ブログ「Introducing Ads Data Hub: Next generation insights and reporting」([https://www.blog.google/products/ads/introducing-ads-data-hub-next\\_24/](https://www.blog.google/products/ads/introducing-ads-data-hub-next_24/))（2021年12月7日アクセス）

※2：SHAREBAKERサイト記事「Facebook Advanced Analytics Announced, Here's What You Need to Know」(<https://shanebarker.com/blog/facebook-analytics/>)（2021年12月7日アクセス）

※3：Habu社公式ブログ記事「The Key to Unlocking Advertising Intelligence in the Walled Gardens Is Through Their Clean Rooms」(<https://habu.com/resources/blog/the-key-to-unlocking-advertising-intelligence-in-the-walled-gardens-is-through-their-clean-rooms>)（2021年12月7日アクセス）

※4：Adexchanger記事「After A Two-Year Quiet Phase, Amazon's Data Clean Room Service Enters The Market」(<https://www.adexchanger.com/online-advertising/after-a-two-year-quiet-phase-amazons-data-clean-room-service-enters-the-market/>)（2021年12月7日アクセス）

※5：NTTドコモプレスリリース（[https://www.nttdocomo.co.jp/info/news\\_release/2020/08/04\\_00.html](https://www.nttdocomo.co.jp/info/news_release/2020/08/04_00.html)）（2021年12月7日アクセス）

※6：電通ニュースリリース「国内初、Twitterと構築したData Clean Room「Twitter Data Hub Omusubi」を提供開始」(<https://www.dentsu.co.jp/news/release/2021/1028-010455.html>)（2021年12月7日アクセス）

※7：MorningBrew記事「Clean rooms, explained: How they became the buzziest tool in ad tech」(<https://www.morningbrew.com/marketing/stories/2021/11/22/clean-rooms-explained-how-they-became-the-buzziest-tool-in-ad-tech>)（2021年12月7日アクセス）

※8：businesswire社記事「パーミュティブがプログラマティック広告向けのプライバシーファースト・インフラストラクチャーを目指し、7500万ドルの資金を調達」(<https://www.businesswire.com/news/home/20211104005559/ja/>)（2021年12月7日アクセス）



## 業界団体による自主ルール等の状況

---

## 業界団体による自主ルール等の概要

団体	主な自主ルール等	発行年/改定年	概要
DAA (Digital Advertising Alliance)	<ul style="list-style-type: none"> <li>Self-Regulatory Principles for Online Behavioral Advertising</li> </ul>	2009年	2009年2月に米国連邦取引委員会が提案した「オンライン行動広告に関する自主規制原則」と対応する7つの原則で構成される。
一般社団法人モバイル・コンテンツ・フォーラム (MCF)	<ul style="list-style-type: none"> <li>スマートフォンのアプリケーション・プライバシーポリシーに関するガイドライン</li> </ul>	2012年	スマートフォン プライバシー イニシアティブの遵守を必須要件としつつ、プライバシーポリシーの名称や掲示場所等に関して推奨要件を定めている。
一般社団法人 日本インタラクティブ広告協会 (JIAA)	<ul style="list-style-type: none"> <li>行動ターゲティング広告ガイドライン</li> </ul>	2016年	行動ターゲティング広告の有用性に配慮するとともに、利用者および広告主の正しい理解を得ることを目的として、行動履歴情報の取り扱いに関する原則を規定している。
IAB、IAB Europe	<ul style="list-style-type: none"> <li>IAB's Mobile Location Data Guide for Publishers</li> </ul>	2016年	モバイル位置情報の利用にあたり、広告事業者が同意取得の際に通知すべき項目等が規定されている。
WFA (World Federation of Advertisers) / GARM <sup>※1</sup>	<ul style="list-style-type: none"> <li>Global Media Charter 2018</li> </ul>	2018年	ブランドと消費者にとって、より良く機能するマーケティング・エコシステムのための条件を整えることを目的として、8つの原則を定めている。
LBMA Japan (Location Based Marketing Association)	<ul style="list-style-type: none"> <li>位置情報等の「デバイスロケーションデータ」利活用に関するガイドライン (LBMA Japanメンバーのみ全文を閲覧可能)</li> </ul>	2020年	プライバシーに配慮して、端末に紐づく位置情報等のデータの取得・利活用を行うための規定が定められている。
MRC (Media Rating Council)	<ul style="list-style-type: none"> <li>位置情報広告計測ガイドライン</li> </ul>	2020年	広告目的での位置情報の利用方法について規定している。消費者のプライバシー保護については、限定的な記載にとどまる。
NAI (Network Advertising Initiative)	<ul style="list-style-type: none"> <li>NAI Code of Conduct</li> </ul>	2020年	広告配信に関して、通知と選択の提供を求める自主規制原則を規定している。会員企業によるテラード広告に使用するデータの収集、使用、転送に、多くの実質的な制限を課している。

※1 : GARMは、2019年にWFAにより設立された業界横断のイニシアチブ「Global Alliance for Responsible Media」

# 主な業界団体の関係

(凡例)  : 国外団体、 : 国内団体

## DAA (Digital Advertising Alliance)

### BBB National Programs

- 自主規制基準、慣行、プログラムの開発に取り組む企業や法律事務所で構成
- 100社以上参加

### AAF (American Advertising Federation)

- 大手広告主等の企業会員、地域クラブからなる全国ネットワーク、大学支部で構成
- 約100社参加

### NAI (Network Advertising Initiative)

- 第三者のデジタル広告会社のみによって構成される主要な自主規制団体
- 100社以上参加

### LBMA (Location Based Marketing Association)

- 位置情報を活用したマーケティング等の促進を目的とする事業者団体 LBMA Japan
- 1,600社参加

### ANA (Association of National Advertisers)

- クライアントサイドのマーケター、マーケティングソリューションプロバイダー、業界専門家で構成
- 1,850社以上参加

### 4A's

- 広告代理店ビジネスの業界団体
- 600社以上参加

### IAB

- 大手メディアおよびテクノロジー企業で構成
- 650社以上参加

### JIAA (日本インタラクティブ広告協会)

- 282社参加

### MCF (モバイル・コンテンツ・フォーラム)

- 日本最大のモバイル業界団体
- 78社参加

## GARM (Global Alliance for Responsible Media)

### MRC (Media Rating Council)

- メディアリサーチを利用する、あらゆるメディア組織で構成
- 150社以上参加

## PRAM (Partnership for Responsible Addressable Media)

### WFA (World Federation of Advertisers)

- マーケターを代表する世界的組織
- ブランドオーナー130社、国営広告主団体60団体が参加

# NAI Code of Conduct

---

## NAIの概要

### ■ NAI（Network Advertising Initiative）とは

- 発足：2000年
  - サードパーティであるデジタル広告企業のみで構成される自主規制団体
- 目的：
  - オンライン/モバイルにおける広告目的のデータ収集・利用に関する高い基準を維持・実施することにより、オンラインエコシステムの健全性を推進する。また、使いやすいオプトアウトの仕組みを通じて、消費者がオンライン広告の体験について有意義な選択ができるよう、啓蒙と支援を行う。
- 参加団体（100企業以上）：
  - Adobe、Criteo、Google、Microsoft、PubMatic、The Trade Desk、Yahoo など

## NAI Code of Conductの概要

### ■ NAI Code of Conduct

- NAI会員企業に対して、興味関心に基づく広告（IBA）、クロスアプリ広告（CAA）、リターゲティング（総称して「テーラード広告」という）および広告配信・レポート（ADR）活動に関して、通知と選択の提供を求める自主規制原則。
- 2000年に初版が発行され、2008年、2013年、2015年、2020年に大幅に改定されている。

### ■ 2020年改定版の要点

- 2020年1月1日施行開始
- 特定のターゲット広告のために、ユーザーレベルのオフラインデータを利用することも規制するため、対象範囲を拡大
- 正確な位置情報等の新しいデータ利用に対する、オプトインコンセントの要件を拡大
- 「視聴コンテンツ広告の表示」に関するガイダンスを導入

### 2020年改定版NAI Code of Conductの目次構成

- Introduction
- 2020 NAI Code of Conduct
  - I. Definitions
  - II. Member Requirements
  - III. Accountability
- Commentary to the 2020 NAI Code of Conduct

## 広告配信・レポート（ADR）はテラード広告と区別され、オプトアウトメカニズムの提供やPII（個人識別情報）収集時の通知が求められない。

- NAI Code of Conductでは、広告配信や広告関連サービスの提供を目的とする広告配信・レポート（ADR）がテラード広告と区別されており、オプトアウトメカニズムの提供やPII収集時の通知が求められない。
- ただし、広告配信・レポート（ADR）目的であっても、データの収集、転送、使用方法を説明する、明確で目立つ通知をウェブサイト上で提供する必要がある。

用語	定義
広告配信・レポート（ADR）	<p> <b>広告配信または広告関連サービスの提供を目的とした、ブラウザやデバイスに関するデータの収集、利用のこと。</b> 特定の場所の提供、統計レポート、トラフィック分析、分析、広告掲載の最適化、広告パフォーマンス、リーチ、および頻度の指標（頻度の上限を含む）、広告クリエイティブのシーケンス、請求、特定の日に特定のウェブサイト、アプリケーション、デバイスに配信した広告の数および種類のロギングなどが含まれるが、セキュリティおよび不正防止のためのデータ収集、利用は含まれない。ADRを通じて収集されたデータが、後に、当該データから判明する又は推定される関心に基づいて広告を調整するために利用される場合、当該使用は、本規定に基づくテラード広告として取り扱われる。                 </p>
テラード広告	<p>                     個人、ブラウザ、デバイスに関する、過去に収集したデータを利用して、そのユーザー、<b>ブラウザ、デバイスにリンクまたは推論された属性、好み、興味、または意図に基づいて、提携していないウェブドメイン、アプリケーション、デバイス上でカスタマイズした広告を行うこと。</b> 興味関心に基づく広告、クロスアプリ広告、オーディエンスマッチ広告、視聴コンテンツ広告、およびリターゲティングが含まれるが、広告クリエイティブの頻度制限または順序付けを含む、広告配信・レポートは含まれない。                 </p>

## テラード広告等の目的で収集するデータの取扱いについて、6つの要件が課せられる。

## 要件

## 概要

要件		概要
A	教育	<ul style="list-style-type: none"> <li>テラード広告および利用可能な選択肢について、ユーザーを教育するための合理的な努力をする。</li> </ul>
B	透明性と通知	<ul style="list-style-type: none"> <li>テラード広告、広告配信・レポートに関するデータの収集、転送、使用方法を説明する、明確で目立つ通知をウェブサイト上で提供する。</li> <li>テラード広告や視聴コンテンツ広告のパートナー企業（広告を掲載するウェブサイト・アプリ等）に対し、当該広告に関する通知を、明確かつ目立つように掲載することを義務付ける措置を取る。</li> </ul>
C	ユーザーコントロール	<ul style="list-style-type: none"> <li>データの機密性と使用目的に見合った選択をユーザーに提供する。（ウェブベースのテラード広告については、NAIがオプトアウトツールを提供している。）</li> </ul>
D	使用制限	<ul style="list-style-type: none"> <li>親権者の同意なく、16歳未満の児童を対象としたテラード広告セグメントを作成したり、テラード広告等の結果として収集されたデータを、マーケティング上の適格性以外の目的（雇用資格等）で利用しない。</li> <li>テラード広告に関する方針、慣行に重要な変更を行う場合は、変更前に収集したデータに対して当該変更を適用する前に、オプトイン・コンセントを取得する。</li> </ul>
E	転送制限	<ul style="list-style-type: none"> <li>テラード広告、広告配信・レポートの目的でPIIを提供/利用可能にする非関連当事者に対し、PIIに関する本規定の遵守を契約上要求する。</li> <li>テラード広告等の活動の一環として収集されたDII（デバイス識別情報）を提供/利用可能にする事業者に対し、当該DIIを受信当事者が保有するPIIと結合したり、テラード広告の目的で個人を再特定しないことを契約上要求する。</li> </ul>
F	データへのアクセス、品質、セキュリティ、保持	<ul style="list-style-type: none"> <li>テラード広告の目的でPIIを保持する会員は、データへのアクセスやオプトアウト、削除請求ができる手段を利用者に提供する。</li> <li>テラード広告、広告配信・レポートに使用するデータの収集、転送、保存を行う場合は、データを保護するために合理的なセキュリティ対策を実施し、利用目的等に応じた範囲内でのみ保持しなければならない。</li> </ul>



# 「B. 透明性と通知」では、NAI会員および、そのパートナーが通知すべき事項が規定されている。

## 「透明性と通知」の要件

## 概要

<p>NAI会員のサイトで通知する事項</p>	<p>テラード広告および広告配信・レポートに関するデータの収集、転送および利用方法</p>	<p>以下の事項を含む、明確で目立つ通知をウェブサイト上で提供する。</p> <ul style="list-style-type: none"> <li>a. 会員企業が行うテラード広告および広告配信・レポートに関する活動等の一般的な説明。</li> <li>b. 企業がNAI会員であり、本規定を遵守していることを示す文書。</li> <li>c. 非関連会社のアプリにおける企業のテラード広告のオプトアウトメカニズムへのリンクまたはアクセス方法。</li> <li>d. テレビにおけるテラード広告のための、オプトアウト・メカニズムへのリンクまたはそのアクセス方法の説明。</li> <li>e. 非関連会社のウェブドメインにおけるテラード広告のオプトアウトメカニズムへのリンク。</li> <li>f. テラード広告のために企業がPIIまたはハッシュ化されたPIIを使用するためのPIIにリンクされたオプトアウトメカニズムへのリンク。</li> </ul>
<p>パブリッシャーのサイトで通知を求める事項</p>	<p>健康/政治セグメント</p>	<p>テラード広告において、健康/政治関連の情報や興味に基づくインタレストセグメントを使用する場合は、当該セグメントをウェブサイト上で公開する。標準的なインタレストセグメントを使用している会員は、すべてのセグメントのリストを開示する。カスタム興味セグメントを使用している会員は、そのセグメントの代表的なサンプルを開示するものとする。</p>
<p>視聴コンテンツ広告を行うパートナーのサイトで通知を求める事項</p>	<p>テラード広告に関するデータの収集、転送および利用方法</p>	<p>NAI会員は、契約しているテラード広告を掲載するウェブサイト/アプリに対し、以下の事項を含む通知を、明確かつ目立つように掲載することを義務付ける。</p> <ul style="list-style-type: none"> <li>a. テラード広告の目的のために、データが収集または利用される可能性があること。</li> <li>b. テラード広告目的で収集されるデータの種類。</li> <li>c. クロスデバイスリンクおよびオーディエンスマッチ広告を含む、第三者によってデータが収集される、または第三者に転送される目的。</li> <li>d. テラード広告のためのオプトアウトメカニズムへのわかりやすいリンク。</li> </ul> <p>NAI会員は、契約している視聴コンテンツ広告を行うパートナーに対し、技術的に可能であれば、画面上または最も適切なユーザーインターフェース上に、以下の事項を含む通知を、明確かつ目立つように掲載することを求める。</p> <ul style="list-style-type: none"> <li>a. テレビを通じて、視聴コンテンツ広告の目的でデータが収集または使用される可能性があること。</li> <li>b. テレビを通じて、テラード広告の目的で収集されるデータの種類。</li> <li>c. クロスデバイスリンクおよびオーディエンスマッチ広告を含む、第三者によってデータが収集される、または第三者に転送される目的。</li> <li>d. 画面上又は最も適切なユーザーインターフェース上に、視聴コンテンツ広告のオプトアウトメカニズムへの分かりやすいリンクまたはアクセス方法。</li> </ul>

## 「C. ユーザーコントロール」では、具体的なケースごとの通知・同意要件が規定されている。

凡例 ●：要対応

#	具体的なケース	オプトアウト メカニズムの提供	オプトイン コンセンルの取得	通知
1	広告配信・レポート目的でDIIを利用する場合			
2	広告配信・レポート目的でPIIを利用する場合			
3	テラード広告目的でDIIを利用する場合	●		
4	オーディエンスマッチ広告目的で、ハッシュ化されたPIIを利用する場合	● PIIにリンクされた オプトアウトメカニズム		
5	テラード広告目的でPIIを単独で、または今後収集されるDIIと統合して利用する場合	● PIIにリンクされた オプトアウトメカニズム		● PII収集時
6	テラード広告目的でPIIを、以前に収集したDIIと統合して利用する場合	● PIIにリンクされた オプトアウトメカニズム	●	● PII収集時
7	テラード広告または広告配信・レポートの目的で、センシティブ情報 を利用する場合		●	
8	テラード広告または広告配信・レポートの目的で、正確な位置情報 を利用する場合		●	
9	テラード広告または広告配信・レポートの目的で、個人名簿情報 (カレンダー、電話帳等の情報) を利用する場合		●	
10	テラード広告または広告配信・レポートの目的で、個人センサー情報 (カメラ、マイク等により収集される情報) を利用する場合		●	
11	視聴コンテンツ広告目的で、テレビから視聴コンテンツ情報の全部又は 実質的に全部を収集する場合		●	

**参考：ePrivacy指令ではCookieの利用について、説明と同意取得を求めている。  
ただし、厳密に必須なCookieについては規制が及ばない。**

**ePrivacy指令におけるCookieに関する規定（5条3項）**

：加盟国の、情報を蓄積するための電子コミュニケーションネットワークの利用又はサブスクライバー又は**ユーザの端末機器に保存された情報へのアクセスは、**関係するサブスクライバー又はユーザがDirective 95/46/ECに従い、**明確かつ包括的な説明を受け**（とりわけデータ処理の目的について）たうえて、**同意をした場合にのみ許される。**このことは、通信の伝達を促進するためのみに行われる、電子コミュニケーションネットワークに対する技術上の保存やアクセス又はサブスクライバー又はユーザから明確に要求されている情報社会サービスを提供するために、**厳密に必要な技術上の保存やアクセスを妨げるものではない**

ICOガイドライン（英）※1、CNILガイドライン（仏）※2 に示される、厳密に必須なCookieへの該当有無

Cookieの利用目的	該当有無	
	ICO	CNIL
入力内容の保持（User input）	○	○
認証（Authentication）	○	○
セキュリティ対策（Security）	○	○
コンテンツの提供（Streaming content）	○	—
ネットワーク管理（Network management）	○	○
ユーザーの嗜好の保存（User preference）	○	○

Cookieの利用目的	該当有無	
	ICO	CNIL
ソーシャルプラグイン（Social media plugins）	×	—
ソーシャルメディアトラッキング（Social media tracking）	×	—
オンライン広告（Online advertising）	×	×
クロスデバイストラッキング（Cross-device tracking）	×	—
アクセス解析（Analytics）	×	○※3

凡例：○ 該当 × 非該当 — 記載なし  
※3 クロスサイト測定、統計化しないデータの利用、第三者へのデータ提供は不可

参考資料：「欧米におけるCookie規制の最新動向と今後の展望」（NBL1168号（2020.4.15）31頁）森・濱田松本法律事務所 岡田淳弁護士ほか著

情報提供：森・濱田松本法律事務所 田中浩之弁護士

※1 Guidance on the use of cookies and similar technologies (<https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/>)（2022年3月8日アクセス）

※2 Cookies et autres traceurs : la CNIL publie des lignes directrices modificatives et sa recommandation (<https://www.cnil.fr/fr/cookies-et-autres-traceurs-la-cnil-publie-des-lignes-directrices-modificatives-et-sa-recommandation>)（2020年10月1日）

Questions-réponses sur les lignes directrices modificatives et la recommandation « cookies et autres traceurs » de la CNIL (<https://www.cnil.fr/fr/questions-reponses-lignes-directrices-modificatives-et-recommandation-cookies-traceurs>)（2021年3月18日）

## ICOガイドラインにおいて示される、厳密必須Cookieへの該当の考え方（1/2）

Cookieの利用目的	該当有無	考え方
入力内容の保持（User input）	○	<ul style="list-style-type: none"> <li>買い物かごやフォームへの入力内容を保持するためのCookieの利用は、厳密に必須なものと認められる。ただし、永続的な利用は認められない。</li> </ul>
認証（Authentication）	○	<ul style="list-style-type: none"> <li>ユーザーの認証を行うための1st PartyのセッションCookieの利用は、厳密に必須なものと認められる。ただし、永続的な利用は認められない。</li> <li>また、認証のために利用するCookieをユーザーの行動やモニタリングにも利用する場合は、同意取得が求められる。</li> </ul>
セキュリティ対策（Security）	○	<ul style="list-style-type: none"> <li>不正検知を含むセキュリティ目的で利用される1st Party Cookieの利用は、厳密に必須なものと認められる。セッションCookieよりも長い期間の保持が認められる。 例：ログイン試行時の失敗数を検出するためのCookie</li> <li>ただし、自サービス以外のオンライン・サービスのセキュリティに関連するCookieの利用や、二次的な目的のために情報が処理される場合は、同意が求められる。</li> </ul>
コンテンツの提供（Streaming content）	○	<ul style="list-style-type: none"> <li>オンライン・コンテンツ・プロバイダーが、ビデオまたはオーディオコンテンツを提供するために利用するCookieは、厳密に必須なものと認められる。</li> <li>ただし、コンテンツのパーソナライズや視聴状況のモニタリングに利用する場合は、同意取得が求められる。</li> <li>また、オンラインサービスが、第三者のオンライン・コンテンツ・プロバイダーによって提供されるコンテンツを単に埋め込む場合（例：ウェブサイトがYouTubeのビデオを埋め込む場合）、適用免除が認められない場合があり、慎重に判断する必要がある。</li> </ul>
ネットワーク管理（Network management）	○	<ul style="list-style-type: none"> <li>ロードバランシング（負荷分散）を目的としたCookieの利用は、厳密に必須なものと認められる。</li> </ul>
ユーザーの嗜好の保存（User preference）	○	<ul style="list-style-type: none"> <li>ユーザーの嗜好を保存するためのCookieの利用は、厳密に必須なものと認められる。ただし、永続的な利用は認められない。</li> <li>例えば、一定期間（例えば90日間）にわたってユーザーのCookie設定を記憶する、Cookie同意メカニズムの一部として使用されるCookieは、免除される可能性がある。</li> <li>オンラインサービスがレスポンシブデザインを使用し、デバイスの種類に応じてサイトを変更する際に利用するCookieも、厳密に必須なものと認められる。</li> </ul>

## ICOガイドラインにおいて示される、厳密必須Cookieへの該当の考え方（2/2）

Cookieの利用目的	該当有無	考え方
ソーシャルプラグイン (Social media plugins)	× (要同意取得)	<ul style="list-style-type: none"> <li>オンラインサービスがソーシャルメディアプラットフォームが提供するプラグイン等のツールを利用している場合（例：ウェブサイトにおける「いいね！」ボタンの設置）、プラグイン等が設定する全てのCookieの利用に関して同意取得が求められる。</li> <li>これは、同サービスをソーシャルメディアのプラットフォームにログインしていないユーザー（ログアウトしたユーザー、またはそのネットワークの会員でないユーザー）も利用することが想定されるためである。</li> </ul>
ソーシャルメディアトラッキング (Social media tracking)	× (要同意取得)	<ul style="list-style-type: none"> <li>ソーシャルメディアプラットフォームや第三者が、オンライン広告・モニタリング・分析・マーケティング等の目的で会員・非会員のユーザーを追跡する場合、Cookieの利用に関して同意取得が求められる。</li> </ul>
オンライン広告 (Online advertising)	× (要同意取得)	<ul style="list-style-type: none"> <li>オンライン広告の目的でCookieを利用する場合、同意取得が求められる。</li> <li>これには、頻度制限、広告提携（アフィリエイト）、クリック詐欺の検出、市場調査、製品改善、デバッグ、その他の目的など、オンライン広告で使用される、全ての3rd Party Cookieが含まれる。</li> </ul>
クロスデバイストラッキング (Cross-device tracking)	× (要同意取得)	<ul style="list-style-type: none"> <li>ユーザーのアカウントを特定のデバイスと結びつけるために、Cookieを利用する場合（例：アカウントプロフィールの一部として、第2の認証要素を提供するため、または広告を含む、あらゆる目的のために、複数のデバイスにわたってユーザーを追跡するため）、同意取得が求められる。</li> </ul>
アクセス解析（Analytics）	× (要同意取得)	<ul style="list-style-type: none"> <li>ユーザーが求めるサービスを提供するために、分析目的のCookieの利用は、厳密には必須なものではないため、同意取得が求められる。</li> </ul>



## Cookieの利用に関する同意取得にあたっては、GDPRの求める厳格な基準を満たす必要がある。

### GDPRにおける同意の定義（4条11項）

：データ主体の「同意」とは、**自由に与えられ、特定され、事前に説明を受けたいうえで、不明瞭ではない**、データ主体の意思の表示を意味し、それによって、データ主体が、その陳述又は明確な積極的行為により、自身に関連する個人データの取扱いの同意を表明するものを意味する

ICOガイドライン（英）※1、CNILガイドライン（仏）※2、DSKガイダンス（独）※3に示される同意取得方法の有効性

同意の取得方法	同意の有効性		
	ICO	CNIL	DSK
ユーザーが同意取得用のチェックボックス等を操作することなく、ウェブサイトやアプリの閲覧、スクロール、別ページへの遷移等をもって同意取得とすること	×	×	×
ブラウザやOSの設定のみに依拠して、同意取得していると判断すること	×	×	×
利用規約（terms and conditions）に含める形など、個別的でない形で同意取得すること	×	×	×
Cookie取得の同意を、ウェブサイトへのアクセス条件とすること（いわゆるCookie Wall）	△※4	△※5	×
同意するほうが拒否するよりも容易な/選択肢が目立つユーザーインターフェイスで同意取得すること	×	×	×
CMPによる同意管理	—	—	△※6

※4 正当な目的（アクセス解析や広告は含まれない）に基づき、一定のCookie利用につき同意しない場合に、一定のコンテンツへのアクセスを制限することは許容

※5 ケースバイケースで判断。同意の自由を侵害する可能性がある

※6 CMPの使用方法等に依存。同意の有効性に関する責任はテレメディアサービス提供者が負う

参考資料：「欧米におけるCookie規制の最新動向と今後の展望」（NBL1168号（2020.4.15）31頁）森・濱田松本法律事務所 岡田淳弁護士ほか著

情報提供：森・濱田松本法律事務所 田中浩之弁護士

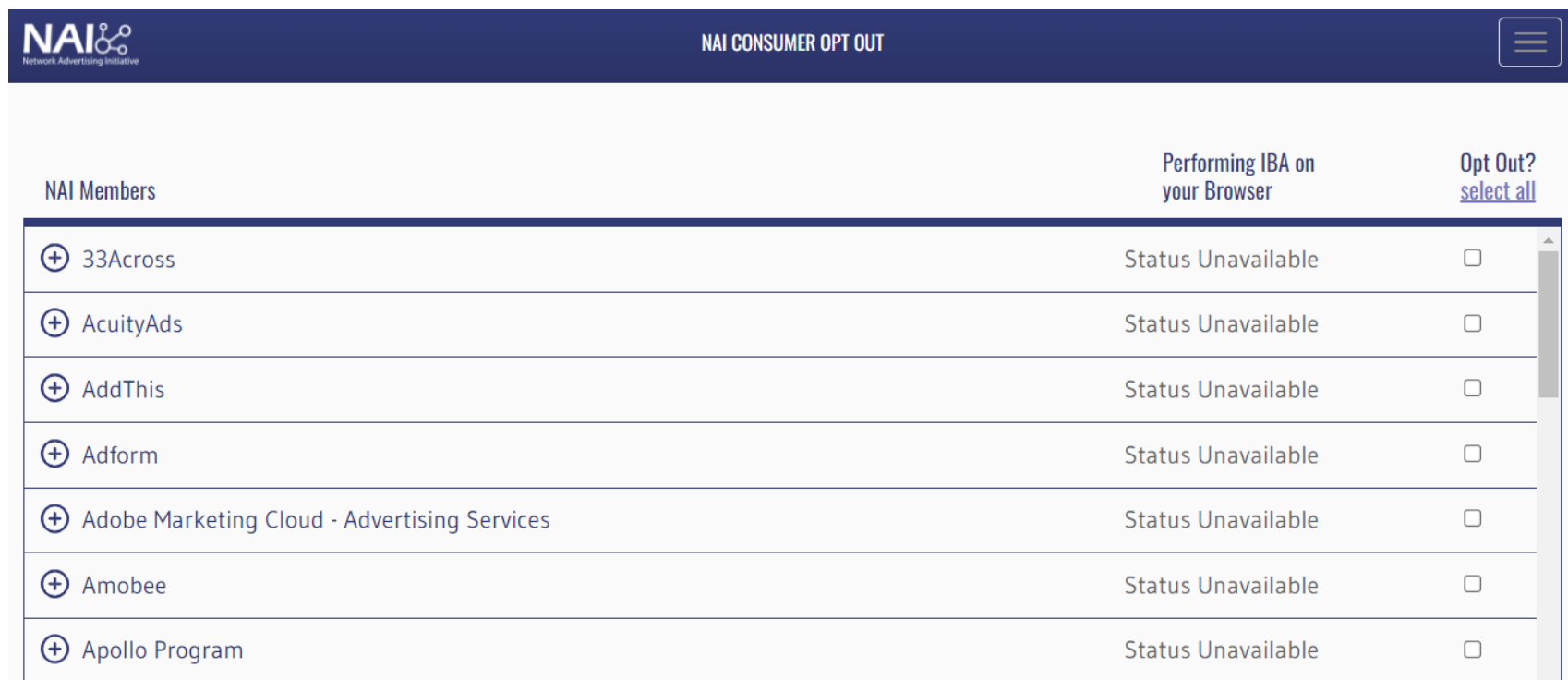
※1 ※2 P3と同様

※3 Germany: DSK publishes guidance on TTDSG (<https://www.dataguidance.com/news/germany-dsk-publishes-guidance-ttdsg>) (2021年12月21日)

# NAIは、ウェブベースのテール広告のオプトアウトツールを提供している。

- NAIは、ウェブベースのテール広告のオプトアウトツールを開発している。
- NAI Code of Conductでは、NAI会員とNAIそれぞれのウェブサイトにおいて、オプトアウトツールが利用できるようにすることを求めている。

## NAIが提供するオプトアウトツール



NAI Members	Performing IBA on your Browser	Opt Out? <a href="#">select all</a>
+ 33Across	Status Unavailable	<input type="checkbox"/>
+ AcuityAds	Status Unavailable	<input type="checkbox"/>
+ AddThis	Status Unavailable	<input type="checkbox"/>
+ Adform	Status Unavailable	<input type="checkbox"/>
+ Adobe Marketing Cloud - Advertising Services	Status Unavailable	<input type="checkbox"/>
+ Amobee	Status Unavailable	<input type="checkbox"/>
+ Apollo Program	Status Unavailable	<input type="checkbox"/>

# IAB PRAMの取組み

---



# PRAMについて

## ■ PRAM（Partnership for Responsible Addressable Media）とは

- 発足：2020年8月
  - 代表はANA（全米広告主協会）のEVPであるビル・タッカー氏、エグゼクティブディレクターに就任
- 目的：  
「消費者と企業の間で行われるアドレスブルなコミュニケーションについて、プライバシーを保護する原則、基準、インフラを開発し、データを安全に活用することで、キャンペーンの最適化や帰属性の向上、パートナー間の透明性の向上、コンテンツやサービスへの資金援助、チャンネルを超えた運用を実現する」
- 設立の経緯：  
同様の目的で「Project Rearch」が既に立ち上がっていたが、バイサイドの参加が少なかった。PRAMではバイサイドトップ層を積極的に招集。
  - Project Rearchは、PRAMの技術的基盤として継続する
  - またIAB Tech LabがPRAMの「技術標準ワーキンググループ」を主導する
- 参加団体：
  - 業界団体：4A's（全米広告業協会）、ANA（全米広告主協会）、IAB、IAB Tech Lab、Network Advertising Initiative（NAI）、WFA（世界広告主連盟）
  - 広告主：フォード、ゼネラルモーターズ、IBM、P&G、ユニリーバ、マスターカード
  - エージェンシー：UM（an IPG Mediabrands company）、Publicis Media
  - パブリッシャー：NBCUniversal
  - テック企業：Adobe、LiveRamp、MediaMath、The Trade Desk など

## PRAMに関するニュース・直近の活動状況

日時	概要	詳細
2020年8月	PRAM立ち上げを宣言	PRAMの立ち上げと、ワーキンググループの設置・役割の説明、主要な参加社や運営にかかわる人物の紹介などを実施
2020年9月	Appleに対し公開書簡を提出	IDFAのiOS14向けポリシー変更案が延期になったことに関連して、次期変更に関する疑問解消のための会合を要請
2021年1月	共同開発のために、コードの提出を業界各社に対して呼びかけ	新たなアドレスブルな仕組み作りに向けて、業界各社が開発しているコードの寄贈を呼びかけ。同時に今後の活動のマイルストーンを発表 →UnifiedID 2.0 のオープンソース化に繋がる
2021年2月	Business Practicesワーキンググループによるビジネスユースケースのドラフト発表	PRAM内のBusiness Practicesワーキンググループによって、60社以上の主要企業による業界横断的な対話を経て作成された、ビジネスユースケースのドラフトを発表
2021年3月	GoogleのIDに関する発表に対し、声明を発表	Googleが3rdPartyCookie廃止後に「代替識別子を作成せず、Google製品でも利用しない」「代わりにPrivacy Sandboxの実装を進めている」という発表に対して、業界との連携不足への失望と、PRAMへの参加要請、今後Googleと協力し、Googleの提供技術の検証・強化に関わりたい、といった内容の声明を発表
2021年4月	2021年1Qの振り返りを発表	各ワーキンググループでの実施内容や、直近のスケジュールに関して公表
2021年8月	2021年2Qの振り返りを発表	直近のワーキンググループやカンファレンスの開催、参加者の増加のほか、GoogleのリリースやAppleとのミーティングなどの実施状況についても公表

# PRAMを構成する4つのワーキンググループとその役割

## ワーキンググループの概要

### Business Practices

- 優先すべきビジネスユースケースを作成し、ソリューションの可能性を検討

### Technology Standards

- PRAMとのパートナーシップの下、IAB Tech Labが主導し、Project Rearcでの実施作業を継続
- 広告およびメディア業界と協力して、プライバシー保護のための仕様およびベストプラクティスを策定

### Privacy, Policy, and Legal

- インターネットのエコシステムにおけるユーザーを特定した、コミュニケーションのための新しい標準の開発に関連する、プライバシー、法律、ポリシー、その他の関連分野に関するガイダンスを提供

### Communications and Education

- 2021年初頭に発足
- 業界のステークホルダー、政策立案者、および一般市民に対して、パートナーシップが策定した提言やソリューションを説明

## 直近の動き

- 2020年の夏～秋に議論を実施、結果をまとめ**ビジネスユースケースのドラフトを公開**

- **4つの規格**を発表し、パブリックコメントにかけている

- 「Addressable Media Identifiers (AMI) のポリシーフレームワーク (DRAFT)」を公開予定

- PRAMの活動に関する四半期報告を定期的に公開

## 直近の活動詳細 ①ビジネスユースケース（ドラフト）

- Business Practicesグループによって発表されたビジネスユースケースのドラフトでは、9カテゴリ60個ものユースケースを用意
  - 広告主向けが4カテゴリ・33個、パブリッシャー向けが5カテゴリ・27個を占めている
  - 各ユースケースに3名の実務担当者を充て、ビジネスへの影響やリスクなどを専門家が検討している
  - 一般に公開し、より多くの人に共有されることで、他の重要なユースケースの見逃しなどを修正し、さらなる充実を図る

### 目次構成

- The Partnership for Responsible Addressable Media : PRAMの紹介
- Section 1: Advertiser Business Use Cases : 広告主のビジネスユースケース
  - Section 1.1 : Planning
  - Section 1.2 : Activation
  - Section 1.3 : Measurement
  - Section 1.4 : Optimization
- Section 2: Publisher Business Use Cases : パブリッシャーのビジネスユースケース
  - Section 2.1 : Content/Service Development
  - Section 2.2 : Audience Acquisition
  - Section 2.3 : Personalization and Delivery
  - Section 2.4 : Monetization
  - Section 2.5 : Re-Engagement / Retention
- Index
  - Cross-Functional Industry Contributors : 関係者一覧
  - Glossary : 用語集

## 直近の活動詳細 ②Technology Standardsグループによる規格発表

規格名称	概要
i Global Privacy Platform	<ul style="list-style-type: none"><li>• IAB TechLabで検討・開発しているグローバルプライバシープラットフォームに関する最初のRFC（仕様書）を発表</li></ul>
ii Accountability Platform	<ul style="list-style-type: none"><li>• デジタル広告のサプライチェーン関係者が、ユーザーの希望する設定を順守していることを証明するための標準的なガイドラインを発表</li></ul>
iii Best Practices for User-Enabled Identity Tokens	<ul style="list-style-type: none"><li>• ユーザーから提供された電子メールや電話番号に紐づけられた識別子のセキュリティとプライバシーに関するガイドラインを発表</li></ul>
iv Taxonomy and Data Transparency Standards to Support Seller-defined Audience and Context Signaling	<ul style="list-style-type: none"><li>• OpenRTB※の上に構築された既存のコンテンツとオーディエンスの分類を利用し、IAB Tech Labのデータ透明性基準に基づいて、オーディエンスセグメントの標準的な名称を作成</li></ul>

※OpenRTB：RTB（＝「Real Time Bidding」の略、広告の入札をリアルタイムで取引する方式）に関して、やり取りするデータややり取りの方法、区分などを定めた標準ルール。

# 参考：

## 4つのパブリックコメントの立ち位置整理

利用できる固有のユーザーIDがない

利用できる固有のユーザーIDがある

紐づけされない1stパーティオーディエンス  
広告主/パブリッシャーのデータが連結されない

ブラウザ・OSで紐づけされるオーディエンス  
3rdPartyでのトラッキングではない

1：1で紐づけされるオーディエンス  
広告主/パブリッシャーのデータが連結される

例：

- **コンテクスチュアルターゲティング**：  
→コンテンツ連動型広告
- **SDA (Seller-defined audiences)**  
→IAB Tech Labが開発した仕様の1つ
- **PMP (Private Marketplaces)**：  
→媒体社と広告主を限定した、クローズドな  
広告取引市場

例：

- ブラウザ内のコホートや興味関心の  
グループ：  
→GoogleのFLoCなど
- ブラウザ内での広告オークション：  
→GoogleのFLEDGEなど
- デバイス上での計測やアトリビューション  
→SKAdNetworkなど

例：

- デバイスIDやクッキーへのオプトインを獲得  
するための事前プロンプト
- **ユーザーによって有効化されたID**：  
→**UnifiedID2.0**など
- データクリーンルーム

②- (iv)

**Taxonomy and Data Transparency  
Standards to Support Seller-defined  
Audience and Context Signaling**

②- (iii)

**Best Practices for User-Enabled  
Identity Tokens**

②- (i) **Global Privacy Platform**

②- (ii) **Accountability Platform**

## ②- i Global Privacy Platformの紹介

### ■ 概要：

- IAB TechLabで検討・開発しているグローバルプライバシープラットフォームに関する最初のRFC（仕様書）として発表

※グローバルプライバシープラットフォーム

= オンライン広告事業者がグローバルな市場でプライバシーに関する法令を遵守するため、**プライバシーに関する技術の基準を合理化・統一したフレームワーク**

### ■ 特徴：

- **既存のTCF2.0のフレームワークをベース**にして作成されており、TCストリングの拡張利用などが盛り込まれている
- 各国・地域ごとに、それぞれプライバシー保護に関する法律があり、**司法権の重複**があることを認め、地域特有の要件に対しては追加情報で対応できるようにしている

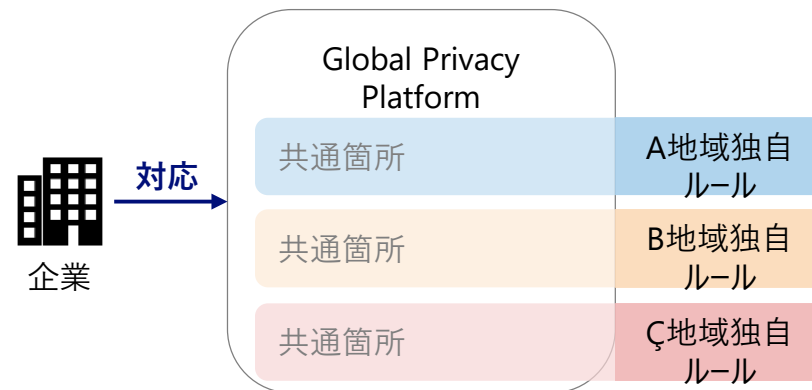
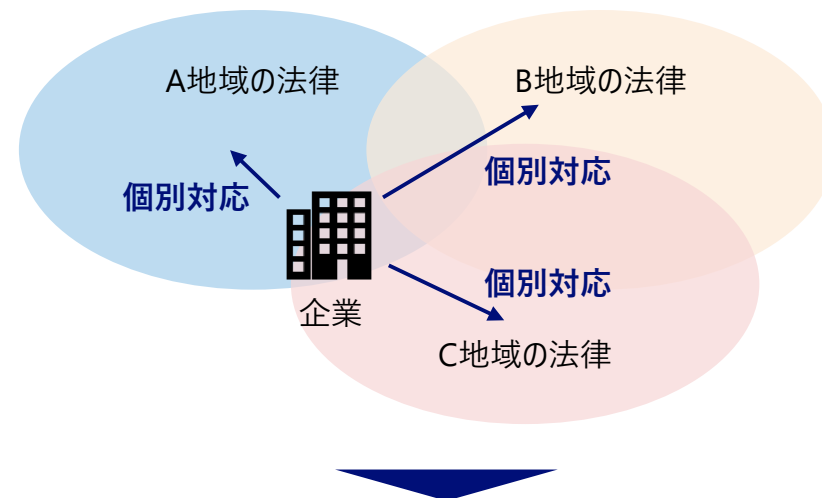
### ■ 期待される効果：

- これまでデジタル広告に関する透明性・管理のツールがなかった国や地域に、それを提供できるようになる
- デジタル広告にかかわる事業者が、地域を超えてプライバシー/データ保護を実施する場合のコストや、段階的な変化への対応コストを削減できる

### ■ 直近の動静

- 2021年3月にパブリックコメントを募集（～2021年4月まで）
- IAB Canadaは既に、Global Privacy Platformへジョイン

### イメージ



## ②– ii Accountability Platformの紹介

### ■ 概要：

- デジタル広告のサプライチェーン関係者が、ユーザーの希望する設定を順守していることを証明するための標準的なガイドライン
- 具体的には、**ログの取得手順に沿って**下記について記載
  - オープンで監査可能な**データ構造の仕様**
  - デジタル広告のサプライチェーンが、ユーザーやユーザーが訪れたデジタルプロパティなどによる設定・制限に適合していることを確実に証明する**標準的な手法**

### ■ 特徴：

- 多くの関係者に対して、**オープンに開発**が進められている
- アドレス指定可能なユーザー識別子を、別のドメインに渡す企業またはエンティティ全体を対象者としている  
(ただし、規制や契約上の合意がある場合は除外可能)
- 対象とする識別子には、**UID2.0、1stPartyのID、スマホ端末のGAIDやIDFAなどが含まれる**

### ■ 期待される効果：

- ユーザー識別子が責任ある使用をされているか確認できる
- 許可/違反を検出し続けることで、徐々に責任ある使用を促す好循環を起こす

### ■ 直近の動静：

- 2021年3月にパブリックコメントを募集（～2021年5月まで）

### 内容構成

#### Logging and Retention

- ログの記録内容・記録方法や、保存する内容についての仕様紹介

#### Log Data Submission

- 記録したログデータを提出する際の手順や提出するデータ形式を紹介

#### Log Data Availability

- 収集・提出したサンプルログについて、活用のされ方に関する説明

#### Further Decentralizing these Designs and Making them Real Time

- さらに分散化に関する今後の検討について言及



## ②—iii Best Practices for User-Enabled Identity Tokensの紹介

### ■ 概要：

- ユーザーから提供された電子メールや電話番号に紐づけられた識別子のセキュリティとプライバシーに関するガイドラインとして発表
- メールアドレスや電話番号ベースのIDを採用する場合に、1stPartyに求められる義務やセキュリティ要件に関して紹介

### ■ 特徴：

- 特に**個人情報収集・トークン構築を行う事業者に対して要求されるセキュリティの要件**について詳しく記載されている
- 独自のシステム設計にこだわらず、アドレスビリティの基本原則や設計上の制約、サプライチェーンの要件などは、業界の既存フィードバックを活用

### ■ 期待される効果：

- ユーザー提供のID（電子メールアドレスや電話番号）からIDトークンが生成され、パートナーに渡される際に、消費者に対するプライバシーの脅威が最小限に抑えられること

### ■ 直近の動静：

- 2021年3月にパブリックコメントを募集（～2021年5月まで）

### 個人データを収集・トークン構築を行う事業者に求められるセキュリティ要件例

- a. 個人を特定できる情報は、第三者と共有する前に、**甲（個人データを収集しトークン構築を行う事業者）、または甲と直接契約しているベンダーが偽名化する**
- b. トークンは、ユーザーが甲から「再識別」の通知を受け、ユーザーが法的に同意した場合を除き、**個人識別情報に直接リンクできない**。偽名化されたデータのPIIへのリンクは、甲または甲と直接契約しているベンダーによってのみ行われる
- c. 個人データへのアクセスのすべてのレベルで、**最小特権の原則**を適用する
- d. 役割に応じた**アクセスコントロール**を行い、**適切な職務分離**を行う
- e. 生の**個人識別情報**は、トークンとは別の環境で保管する
- f. データセットに、**個人特定された最小の閾値以下の情報を含めるべきではない**
- g. **時間横断的なクエリの使用を、いつ、どこで発生してはならないかを考慮し禁止する**
- h. すべての接続で、**セキュリティイベントの監査とログを有効にする**
- i. 個人データから生成したトークンは、**個人データに戻せないよう十分に暗号化およびハッシュ化する**
- j. **1stパーティまたは1stパーティと直接契約しているベンダーのみが、個人データの暗号化またはハッシュ化を行う**
- k. **暗号化および／またはハッシュ化は、1stパーティの環境内で行う**
- l. 転送中および保存中に使用される暗号化方法は、業界標準の暗号化レベル以上のものとする
- m. トークンへの不正アクセスを可能にするマッピングテーブルの維持能力を大幅に制限するため、ベンダーのエコシステムに十分な技術的メカニズムを用意する
- n. データ保持のスケジュールは、**管轄区域の関連する法的要件に従い、定義され、遵守され、最小限に抑える**
- o. データのローカリゼーションは、**適用される法的要件及び適用される司法権に従い、遵守する**

## ②—Ⅳ Taxonomy and Data Transparency Standards to Support Seller-defined Audience and Context Signalingの紹介

### ■ 概要：

- OpenRTBの上に構築された、既存のコンテンツとオーディエンスの分類を利用し、IAB Tech Labのデータ透明性基準に基づいて、オーディエンスセグメントの標準的な名称を作成している

### ■ 特徴：

- IAB Tech LabのContent Taxonomy 2.xまたはAudience Taxonomy 1.xを基に匿名化されたタクソミー・ノード（コンテンツやオーディエンスの分類）を使用
- IAB Tech Labのコンテンツとオーディエンスの分類、OpenRTBの仕様、Data Transparency Standardなどの既存のオープンスタンダードを活用
  - Googleで議論されている「FLEDGE」の仕様なども、コホート検討の参考文献として挙げられている

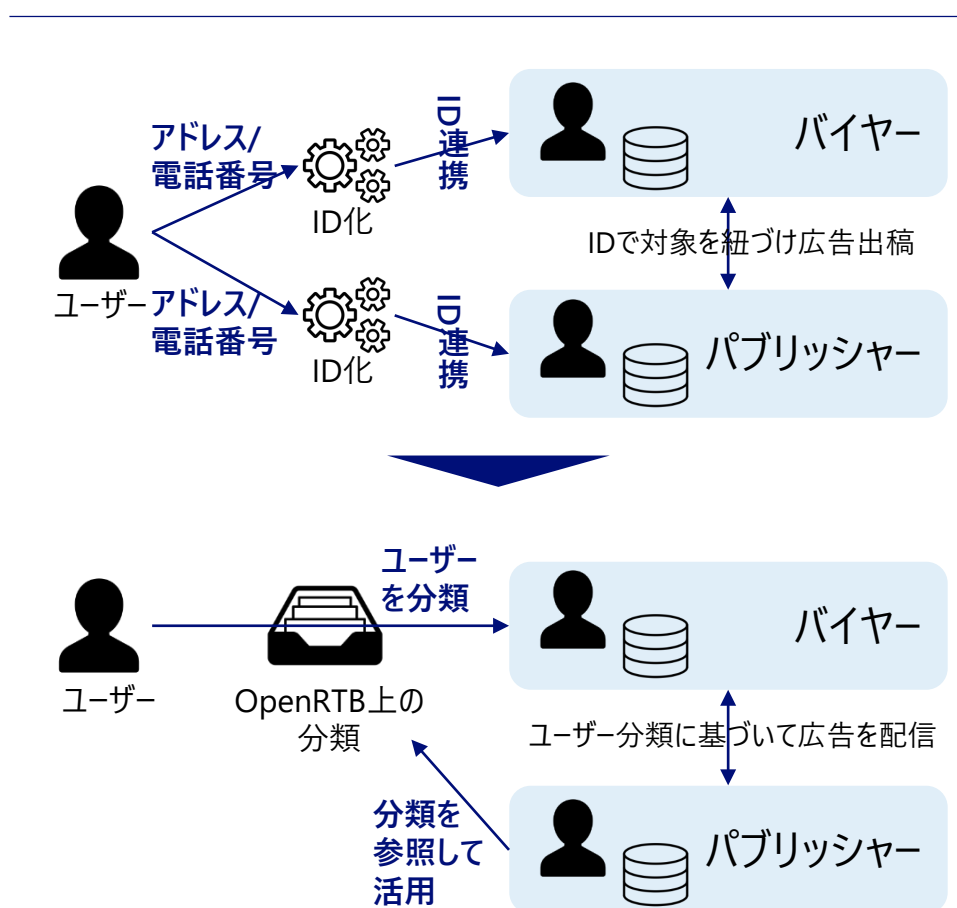
### ■ 期待される効果：

- ユーザーが提供する識別子や第三者が提供する識別子が利用できない場合など、自社とパブリッシャーのオーディエンスを直接結びつけられない場合にも、標準化されたオーディエンス分類やコンテキストの分類を用いることで、意味のあるアドレッシング（ユーザーを特定した配信）が可能になる

### ■ 直近の動静：

- 2021年3月にパブリックコメントを募集（～2021年5月まで）

### イメージ



参考) IAB PRAM Technology Standards  
ワーキンググループが公表する規格の詳細

---

## ②- i Global Privacy Platformの詳細

### 目次構成

### 概要

#### OVERVIEW

- About this RFC\*
- Goals for Early RFC
- GPP Value

※RFC: インターネット技術の標準的な仕様を記した文書

#### GUIDING PRINCIPLES

#### MULTI-JURISDICTIONAL DESIGN

#### PROPOSED ARCHITECTURE →次頁に記載

- “TC String” as a Starting Point
- Header
- Discrete Sections
- Creating a GPP String
- Dealing with Length
- GPP APIs
- Signal Integrity
- Vendor Registry
- Unified Libraries and SDKs
- Vision for Updates from TCF v20 and/or USPrivacy to GPP

#### HOW TO SUBMIT COMMENT

#### OVERVIEW

- グローバル・プライバシー・プラットフォーム (GPP) に関する初期RFC
- 初期RFCとして技術標準を市場に投入するIABの意図の明示や、過去の技術に対するフィードバック募集、アドレサビリティ・アカウントビリティとGPPの関連付けなどを目的としている

#### GUIDING PRINCIPLES

- コストのかかる、断片的な技術の削減
- プライバシーやデータ保護に関する地域差に対応し、時間をかけて収束させる
- 地域や国は、他の地域の同意なしで管轄区域をサポートすべき
- 既存の同意フォーマットを包含し、バラバラな取り組みが多くあることを認識する
- 新しい技術の採用に係るコストの最小化と新機能による価値の提供を両立させる
- 各ステークホルダーのニーズをサポートするために柔軟性が重要

#### MULTI-JURISDICTIONAL DESIGN

- 各国・地域に固有のデータ保護法があり、管轄が重複している
- このRFCでは司法権の重複を認めつつ、GPP内のシグナルが、どの法律に対応しているかを明確に示し、ユーザーの選択が、どの法域に対して行われたか、ベンダーが分かるように技術的な仕様を定める
- 具体的にはストリング (やり取りされる情報) 内に、国や地域を示すセクションを用意し、そこに特有の法的根拠や許可を与える

## ②- i Global Privacy Platformの詳細\_\_提案されている仕様

カテゴリ	概要
"TC String" as a Starting Point	<ul style="list-style-type: none"><li>TCF2.0の「TCストリング」のコンセプトに基づき、これを拡張して使用。どのデータが、どう表現されるか明確に表現したうえで、可能な限りTCF2.0向けの技術を使用できる</li></ul>
Header	<ul style="list-style-type: none"><li>PPバージョン、地域ID、文字列中の関連する地域セクションの位置を示す、インデックスのみを含むヘッダーを利用し、どの地域の要件が入っているか識別するための目次として利用する</li></ul>
Discrete Sections	<ul style="list-style-type: none"><li>TCF2.0で導入されたセグメントの概念を用い、1つの仕様で複数地域をサポートする際に活用。地域ごとの限定された変更も可能とする</li></ul>
Creating a GPP String	<ul style="list-style-type: none"><li>GPPの文字列作成時に、セクションが推奨のエンコーディングをしていれば、ヘッダとサブセクションを「・」で連結、ヘッダーのビット表現は前IDをソート順で含めて変換など、細かい作業指示を記載</li></ul>
Dealing with Length	<ul style="list-style-type: none"><li>TCF2.0と同様、実装の際文字列が長すぎる可能性がある。解決法はパブリックコメントで募集。</li></ul>
GPP APIs	<ul style="list-style-type: none"><li>TCFのAPIに似たものを用意したいが、GPPの性質から、より一般的なものを想定</li></ul>
Signal Integrity	<ul style="list-style-type: none"><li>GPPへの「シグナルインテグリティ」*技術導入をワーキンググループとして約束。現在、シグナルインテグリティに関する2つの提案を評価中</li></ul>
Vendor Registry	<ul style="list-style-type: none"><li>短期的には、TCFに近いものを既存のグローバルベンダーリストに基づき構築することを推奨。その他、TechLabのTransparency Centerが中心となる可能性についても議論中。</li></ul>
Unified Libraries and SDKs	<ul style="list-style-type: none"><li>公式のオープンソースプロジェクトのサポートを意図しており、iabpcf-esのような既存の公式オープンソースプロジェクトは、GPPで動作するように拡張、統合することができる</li></ul>
Vision for Updates from TCF v2.0 and/or USPrivacy to GPP	<ul style="list-style-type: none"><li>提案している仕様がTCF v2.0とUSPrivacyをサポートしており、将来的には、維持・サポートすべき単一の技術標準が残ることになる</li></ul>

## ② – ii Accountability Platformの詳細

### 目次構成

### 概要

#### OVERVIEW

- Guiding Principles
- Scope
  - Participant Profile
  - Use Cases

#### PROPOSED ARCHITECTURE →次頁以降に記載

- Logging and Retention
  - Identifying Senders and Receivers
  - Transmitting a Transaction ID
  - Data to Log for Submission
  - Expectations for Retention
- Log Data Submission
  - Workflow
  - Log Data Preparation
  - Query Logs
  - Submission Workflow
  - Log Data Status
- Log Data Availability
- Further Decentralizing these Designs and Making them Real Time
  - Extending Sender/Receiver Architecture
  - Potential Benefits of Further Decentralization and Real Time Hooks
  - Summary of Further Decentralization Proposal

#### FAQS

#### HOW TO SUBMIT COMMENTS

#### Guiding Principles

- デジタル広告において、透明性や制御信号への不適合を検出し、ユーザー識別子の責任ある使用/無責任な使用を実証できる
- ユーザーへの透明性とユーザーからのコントロールは、ユーザーが誰と仕事をするか、ユーザーの快適さにどのような標準的なデータ利用があるかなどを明確に定義した、ユーザーに関するデータ属性に依存する
- ユーザーが交流するデジタル・プロパティの初期選択と組み合わせたユーザー・コントロールは、特定の広告関連取引においてユーザー識別子に許可される用途を最もよく表す
- 特定の広告関連取引で、許可されていることを一貫・継続的に示し、違反を検出し、責任あるデータ収集・使用を促す好循環を生み出せる
- オープンアプローチは、クローズドアプローチよりも、はるかに好まれ、アカウントビリティ・プラットフォームのデータを、多くの関係者が利用できるようにすることで、デザインが強化される
- この規格によって、ユーザーのプライバシーやデータ保護に違反する新たな機会が生まれることがあってはならない

#### Scope

- エコシステム参加をラベル付け：「ブランド」「パブリッシャー」「サプライサイドテクノロジー」「バイサイドテクノロジー」「IDデータ検証/照合テクノロジー」「他の3rdPartyデータのプロバイダーや処理者」
- 対象となるユーザー識別子：
  - ✓ 「ユーザーが使用できるアドレスブルな識別子（UID2.0など）」
  - ✓ 「アドレスブルな1stPartyの識別子」
  - ✓ 「デバイスが提供するアドレスブルな識別子（GAID、IDFAなど）」
  - ✓ 「その他システム・アドテックベンダーによるユーザー特定目的の識別子」



## ②- ii Accountability Platformの詳細\_\_提案されている仕様「ログの記録と保持」

### カテゴリ

### 概要

#### Logging and Retention

- 送信者／受信者のペア：参加者は、「送信者」「受信者」のいずれかになることができ、通常はその両方になる
- 送信者がトランザクションIDを作成し送信、受信者はメタデータとともにそれを記録する。**このIDは任意かつペアで一意である**

#### Log Data Submission

#### Identifying Senders and Receivers

- 送信者と受信者のIDは、**堅牢なDNSシステムに依存**することを提案。ドメイン名と法人の最初のマッピングは既存のDNSシステムを使用するが、その際、**登録企業リストの使用も想定**
- 送信者と受信者が標準的なデジタル通信手段で通信する場合、**トランスポート・レイヤー・セキュリティ (TLS) が、これら2つのエンティティ間の検証を実施**
- 唯一の追加要件として、このドメインに関連する法的なデータ所有者と公開鍵とのマッピングを追跡する認証局 (CA) に言及

#### Log Data Availability

#### Transmitting a Transaction ID

- ワーキンググループで送信者/受信者ペアが、Transaction IDを送信する方法について、いくつかのオプションを検討中
- インフラの大幅な変更を必要としない、他のメカニズムについてのアイデアも募集中  
※本仕様書で言及されているアイデアについて次頁に記載

#### Further Decentralizing these Designs and Making them Real Time

#### Data to Log for Submission

- 対象となるすべての広告関連取引について、このプラットフォームへの参加者が**記録すべきフィールドと提出のプロセス**について記載
- ユーザーIDを記録するが、ユーザーデータは、**いかなるクリアリングハウスや監査法人にも提出されない**
- ユーザーIDは、MD5を使用してハッシュ化される

#### Expectations for Retention

- 所定の期間 (1日) に記録された取引データのサンプルを提出 (「ログデータの提出」参照)
- サンプリングは**データの提出時に実施、所定期間内のすべての取引について、「Data to Log for Submission」で定義したデータ構造を記録**。記録の保存方法は、本仕様書で規定せず

## Accountability Platformで記述された「トランザクションIDの送受信のアイデア」

### トランザクションIDの送信に関するアイデア

	Pros	Cons
共有されたアドレス可能なユーザーIDへの連結	<ul style="list-style-type: none"> <li>新たな送信メカニズムが必要ない</li> </ul>	<ul style="list-style-type: none"> <li>ユーザ識別子が機器のものである場合、その識別子との連結を行うことができる対象が存在しない（この仕様への参加が望まれているものの、参加しそうにない）</li> <li>この規格に参加していない事業者は、連結されたトランザクションIDの扱いに困るかもしれない。</li> <li>プライバシー・シグナルがアドレス可能なユーザ識別子を渡すことを許可しない場合、トランザクションIDは何に連結されるか？</li> </ul>
OpenRTBの拡張	<ul style="list-style-type: none"> <li>デジタル広告のサプライチェーンを流れる新しい値をサポートする共通の方法である</li> </ul>	<ul style="list-style-type: none"> <li>すべての潜在的参加者が、OpenRTBを統合しているわけではない</li> </ul>
URLマクロの利用	<ul style="list-style-type: none"> <li>サーバーサイドとクライアントサイドの統合に対応している</li> </ul>	<ul style="list-style-type: none"> <li>長さの問題がある</li> </ul>
プライバシー・シグナルへの連結	<ul style="list-style-type: none"> <li>新たな送信メカニズムが必要ない</li> </ul>	<ul style="list-style-type: none"> <li>本規格に参加していない企業は、連結されたトランザクションIDの扱いに困る可能性がある。</li> <li>長さの問題がある</li> </ul>



## Accountability Platformで定義された「記録・提出すべきデータ」形式

### 記録・提出すべきデータの形式

Field Name : フィールド名	Description : 説明文	Type : データ型	Values : 値
version	The version of this specification the record represents.	VARCHAR	Insert
timestamp	The time a transaction is logged	TIMESTAMP	Insert
senderId	Non-repudiable, eTLD+1 domain signed over TLS of the entity sending (or allowing the retrieval of) a persistent identifier usable for data processing purposes laid out by whatever privacy and data protection regime(s) the digital property is operating in.	BIGINT	A 64 byte array containing the signature described above
receiverId	Non-repudiable, eTLD+1 domain signed over TLS of the entity receiving (or carrying out the retrieval of) a persistent identifier usable for data processing purposes laid out by whatever privacy and data protection regime(s) the digital property is operating in.	BIGINT	A 64 byte array containing the signature described above
transactionRole	Whether the entity logging this transaction is logging as the Sender or Receiver. Note: a Receiver can also be a Sender for a subsequent Sender/Receiver pair in the same supply chain transaction.	BINARY	0 for "Sender" 1 for "Receiver"
transactionId	A single use transaction identifier unique to the Sender/Receiver pair for a given reporting interval (described below) as far as the Sender, who generates the transactionId knows.	BIGINT	Insert
privacySignal	The Tech Lab supported privacy signal (TC string, USPrivacy string or Global Privacy Platform string) where available and if not any known opt-out signal related to the transaction.	BIGINT	Insert

## ②- ii Accountability Platformの詳細\_\_提案されている仕様「ログの記録と保持」

### カテゴリ

### 概要

#### Logging and Retention

- 参加者は、トランザクションログのサンプルを**毎日提出**する
- ログデータ提出用のAPIが、参加者からサンプルログデータを受け取り、検証し、データの分析を希望する企業に提供する
- 本仕様書およびガイドラインでは、**参加者がログデータ提出APIと、どのようにやり取りするか**を説明している

#### Workflow

- 次頁に記載

#### Log Data Submission

#### Log Data Preparation

Jobの呼び出し処理：

- 定められた定刻に、**ログデータ提出用API**の/jobエンドポイントをsenderIdで呼び出し、ジョブ定義（ジョブID、サンプルマッチ値などを含む）を取得。
- ログデータ提出APIは、サンプルキーを参加者に提供し、提出内容を検証し、トランザクションデータを分析する主体が利用できるように保存する

#### Log Data Availability

#### Query Logs

ログ照会：

- /jobを呼び出して返された「sampleMatchValue」を使用し、**対象となる広告関連取引のMD5でハッシュ化されたユーザーIDの下一桁が「sampleMatchValue」と一致する、すべてのレコードを自分のログに照会**する
- サンプル・データを生成した後、参加者は、jobId、senderId、createdOn、numberRecordsを含むメタデータをヘッダーに付けて、結果を Avro<sup>※</sup>に書き込む

#### Further Decentralizing these Designs and Making them Real Time

#### Submission Workflow

提出処理：

- 既定のフォーマットで提出データを成形したのち、**ログデータ提出API**を呼び出し

#### Log Data Status

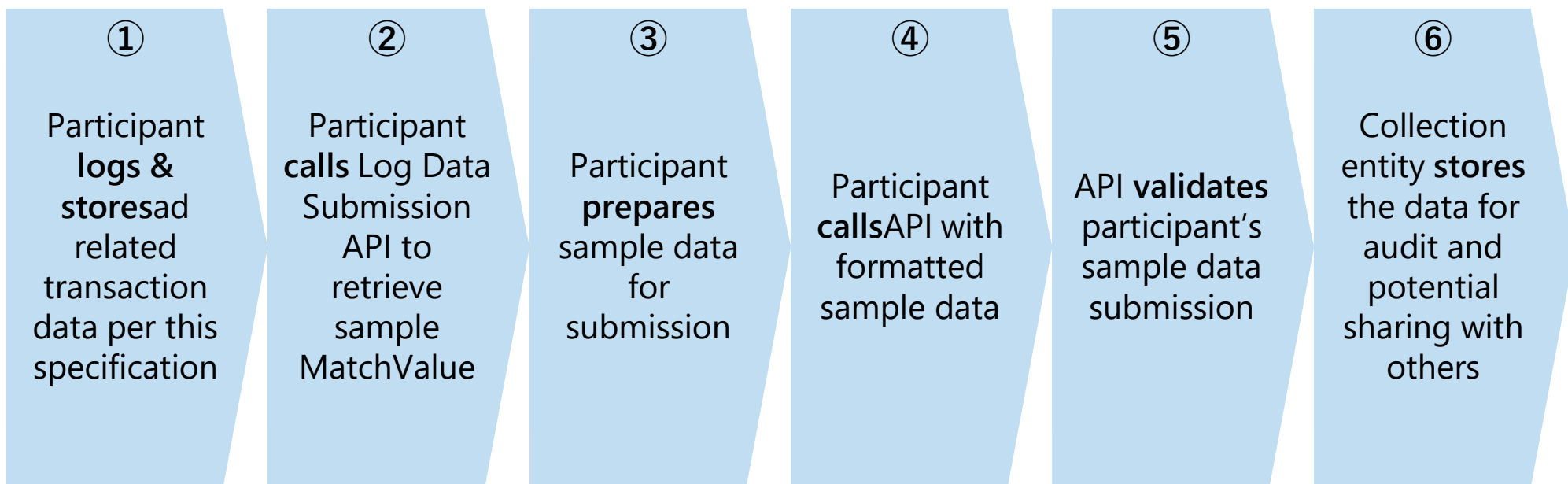
- 参加者が、その期間のサンプル提出に成功すると、参加者は、その**期間のすべてのデータをさらに4日間保持**し、政府機関などが、その後分析のために追加のデータを要求できるようにする。その後、参加者は**各自のデータ保持に関するポリシー**に従う。

※Avro：Apache Software社が提供しているデータのシリアル化するシステム

## Accountability Platformで記述された「Log Data Submission」のワークフロー

### 「Log Data Submission」のワークフロー

- 参加者は、トランザクションログのサンプルを毎日提出する
- ログ・データ提出APIは、参加者からサンプルのログ・データを受け取り、検証し、データの分析を希望する対象者に提供する
- 本仕様書およびガイドラインの中で、参加者がログデータ提出APIと、どのようにやり取りするかを説明している



## ②- ii Accountability Platformの詳細\_\_提案されている仕様「ログの利用可能性」

### カテゴリ

### 概要

#### Logging and Retention

##### <作業>

- 収集サービスでは、送信者ID、受信者ID、トランザクションIDで構成される複合鍵を用いて、参加者全員の送信者/受信者のトランザクション・ペアの提出されたログを結合する

#### Log Data Submission

##### <データの要件>

- 参加者が各取引を記録してログを提出し、その取引相手も同様に提出すると、結合されたセットには各取引の記録のペアが含まれ、両方の記録のプライバシー・シグナルは同じでなければならない。
- さらに、これらの同じシグナルは、送信者がアドレス可能なユーザー識別子を渡すべきだったかどうかを示すはずであり、時間が経てば、他の監査方法に加えて、参加者の信頼性を確立するのに役立つ貴重なツールとなる

#### Log Data Availability

##### <ログの活用>

- 明らかにプライバシーシグナルに準拠していない参加者は、通常の企業間のコミュニケーションを通じて特定され、確固たる証拠に基づいて説明を求められる可能性があり、また、アドレス可能なユーザー識別子を扱う能力に疑問を投げかけることもできる
- 一貫してプライバシー・シグナルに準拠していると見られる企業は、その信頼性に関してポジティブな評判を得ることができる。

##### ※想定される主体と分析の種類：

- このデータを用いて監査を強化する自主規制のプライバシー監査プログラム
- デジタル広告の透明性と管理メカニズムの遵守状況を判断することに関心のある研究者や規制機関
- デジタル広告の透明性と管理メカニズムの遵守状況を判断することに関心のある研究者や規制当局、説明責任を果たすためのポリシーを持つ自主規制の透明性と管理シグナリング基準
- 参加者のパートナー関係の監査に従事する商業監査人

#### Further Decentralizing these Designs and Making them Real Time

## ②- ii Accountability Platformの詳細\_\_提案されている仕様「さらなる分散化とリアルタイム性」

### カテゴリ

### 概要

#### Logging and Retention

- ウェブ・アーキテクチャとの関連で、本仕様の提案は組織識別子の生成の分散化に依存しており、また組織識別子の生成分散化は、識別子を生成するための秘密鍵/公開鍵の暗号化に依存している
- 秘密鍵/公開鍵暗号方式を採用することで、組織識別子が否認されなくなり、政府機関からライセンスされた組織識別子をコピーしたり再生したりすることで、簡単になりすましができるようになる

#### Log Data Submission

※分散化の方法 (例) : パブリックコメントで検討されるための参考として提示

- 送信者/受信者の仕様拡張：
  - ✓ 将来の監査のために、ペアでのデータ転送を各参加者が記録
  - ✓ 参加者が次の受信者にデータ送信する際に、受信した署名済みの組織識別子のチェーンを含めることを要求する
  - ✓ これにより、デジタル資産とのやり取りに伴うデータ転送について、人々、パブリッシャー、マーケッターの透明性が高まる (= 広告のリクエストから広告のレンダリングまでの一連の流れを完全に把握できるようになる)

#### Log Data Availability

- さらなる分散化とリアルタイムフック※の利点：
  - ✓ 分散型アカウントビリティ・プラットフォームのデータのリアルタイム性によって、監査フックをリアルタイムで実施できるようになる
    - アドテック：サプライチェーンコントロール機能に、リアルタイムのアカウントビリティフックを追加できる
    - 業界団体、ブラウザベンダー、OSベンダー、プライバシー保護団体なども、それぞれ異なるリアルタイムソリューションを運用し、監査をサポートできる
  - ✓ ブラウザのプラグインを、トランザクション・チェーンの検査、プライバシー・シグナル・ルールの適用、分析強化などのために構築できる

#### Further Decentralizing these Designs and Making them Real Time

※フック (Hook) : ソフトウェアコンポーネント間でやり取りされる情報を傍受し、ソフトウェアコンポーネントの動作を変更または拡張するための技術

## ②— iii Best Practices for User-Enabled Identity Tokensの詳細

### 目次構成

### 概要

#### ■ Goal/Scope

#### ■ Relevant Definitions

#### ■ Proposed Best Practices

- First-party Obligations for Transparency and Control
- Security
- Exclusions
- Access and Use

#### ■ Appendix

- Established Principles For Addressability  
：ステークホルダーに求められる要件について記載

#### Goal/Scope

- 本文書は、オンライン出版社やマーケティング担当者が、ユーザーが提供した電子メールや電話番号に関連してパーソナライズされたコンテンツやサービスを提供する際に、**ユーザーが提供したID（特に電子メール・アドレスや電話番号）を暗号化して使用するためのガイドライン**を定めている
- 本文書は、これらの値からIDトークンが生成され、アドレスビリティのユースケースをサポートするためにパートナーに渡される際、**消費者に対するプライバシーの脅威を最小限に抑えることに焦点**を当てている
- 本文書は、**独自のシステム設計にとらわれないこと**を意図しており、アドレスビリティの基本原則、設計上の制約、サプライチェーンの要件に関する業界の既存のフィードバックを活用している

#### Relevant Definitions

- **First Parties**：エコシステムの“買う”側と“売る”側の両方で、デジタルコンテンツを制作している人たち。
- **Personal Data**：個人識別情報、偽名または偽装された情報、およびユニークトークンを含む、識別可能で自然人に関連するあらゆる情報
- **Personally Identifiable Information**：特定の個人をオフラインで直接識別または記述する情報。個人の名前、物理的な居住地または郵送先住所、電子メールアドレス、電話番号...など
- **Pseudonymous**：個別に管理されている追加情報を使用せずに、特定のユーザーの個人識別情報に直接帰属させることができない方法で個人データを処理すること
- **Token or Tokenize**：企業が個人を推測、発見、または、その他の方法で識別できない、偽名化された固有の識別子



## ②-iii Best Practices for User-Enabled Identity Tokensで提案されているベストプラクティス

### カテゴリ

### 概要

#### First-party Obligations for Transparency and Control

- 個人データを収集し、それを偽名トークンとして構築し、ターゲット広告のために第三者と共有する(=「アドレスビリティ」) 甲は、**適用される司法管轄区に関連する法的要件に従い**、ユーザーに透明性とコントロールを提供しなければならない。
- Transparency (透明性) : キャンペーンや収益化をサポートするために利用するベンダーや、それらのベンダーに許可するデータ利用についての、1stパーティの選択を反映したもの
  - Control (コントロール) : 1stパーティが開示するデータ処理を、ユーザーが、さらに制限できるようにする機能的なメカニズム

#### Security

: トークン作成時に、データセキュリティとプライバシーを強化するために期待される事項

- 個人を特定できる情報は、第三者と共有する前に、**甲、または甲と直接契約しているベンダーによって偽名化する**
- トークンは、ユーザーが甲から「再識別」の通知を受け、ユーザーが法的に同意した場合を除き、**個人識別情報に直接リンクできない**。偽名化されたデータのPIIへのリンクは、甲または甲と直接契約しているベンダーによってのみ行われる
- 個人データへのアクセスのすべてのレベルにおいて、**最小特権の原則**を適用する
- 役割に応じた**アクセスコントロール**を行い、再識別から保護するために**適切な職務分離**を行う
- 生の**個人識別情報は、トークンとは別の環境で保管する**
- データセットは再識別のリスクを低減するために、**個人の特定された最小の閾値以下の情報を含めるべきではない**  
※閾値を決定する際に考慮すべき重要事項の概要は、「Taxonomy and Data Transparency Standards to Support Seller-defined Audience and Context Signaling」を参照
- 再識別のための三角測量に使用される**時間横断的なクエリの使用を、いつ、どこで発生してはならないかを考慮し禁止する**
- ローカル、ネットワーク、クラウド、およびリモートアクセスのすべての接続で、**セキュリティイベントの監査とログを有効にする**
- 個人データから生成したトークンは、リバースエンジニアリングで**個人データに戻せないよう、十分に暗号化およびハッシュ化する**
- 1stパーティまたは1stパーティと直接契約しているベンダーのみが**、個人データの暗号化またはハッシュ化を行う
- 可能な限り個人データの転送を制限するために、**暗号化および/またはハッシュ化は、1stパーティの環境内で行う**
- 転送中および保存中に使用される暗号化方法は、業界標準の暗号化レベル以上のものとする
- トークンへの不正アクセスを可能にするマッピングテーブルの維持能力を大幅に制限するため、ベンダーのエコシステムに十分な技術的メカニズムを用意する
- データ保持のスケジュールは、**管轄区域に関連する法的要件に従い**、定義され、遵守され、最小限に抑える
- データのローカリゼーションは、**適用される法的要件及び適用される司法権に従い**、遵守する

#### Exclusions

- 消費者が児童であることが判明している場合は**、消費者の個人データをトークンに組み込んだり、第三者のベンダーに渡したりできない

#### Access and Use

- いかなる第三者も、**適用されるすべての地域の法律、消費者の嗜好、行動規範、および本規約を遵守しない限り**、いかなる理由でも(個人データから生成された)トークンにアクセスしたり利用したりすることはできません。

## ②-iv Taxonomy and Data Transparency Standards to Support Seller-defined Audience and Context Signalingの詳細

### 目次構成

### 概要

- Goal
- Design Principles
- Referenced Documents and Specifications
- Background
- Key Considerations
- Approach
  - Passing Audience Taxonomy IDs and DTS Metadata to Support Audience Targeting
  - Passing Content Taxonomy IDs to Support Contextual Targeting
- Summary of Primary Open Questions
- Appendix
  - Data Transparency Standard

#### Goal/Scope

- IAB Tech LabのContent Taxonomy 2.xやAudience Taxonomy 1.xを参考にした、匿名化されたタクソミー・ノード (IAB規格でのコンテンツ分類) を使用し、パブリッシャーが定義したコンテキストやオーディエンスの属性をOpenRTB内でシグナリングするアドレサビリティのやり方を提案
- 企業の事業活動やサプライチェーンの行動への影響を最小限に抑えつつ、ウェブコンテンツやサービスのマネタイズをサポート
- 既存のオープンスタンダードを新たな方法で活用しながら、地域のプライバシーに関する期待に沿った、透明性と説明責任のあるデータアクセスと利用の促進を行う

#### Design Principles

- ユーザーの透明性とコントロール
- データの安全性と最小化：3rdPartyCookieなど、透明性がない/トラッキングされる可能性のあるデータ受け渡しに依存しないことや、リスクのあるデータの混在を制限する管理方法が必要
- 消費者の嗜好に対する技術的説明責任：Accountabilityプラットフォームとの互換性を持つ
- 後方互換性：既存のビジネスへの影響を抑え、コストや時間のかかるツールも避ける
- 他のアドレサビリティ手法の補完：あくまで、他の実行可能な設計を排除するわけではない
- 業界の成長、相互運用性、競争をサポート：持続可能で、可能な限り共通規格上でのイノベーションをサポートする



## ②-iv Taxonomy and Data Transparency Standards to Support Seller-defined Audience and Context Signalingの「アプローチ」での言及内容①

### カテゴリ

### 概要

オーディエンスターゲティングをサポートするIDとメタデータの受け渡し

#### 関連ツール・リソース

- OpenRTBと組み合わせ個人データを公開せずオーディエンスシグナリングをサポートする、IAB発表済みの仕様を紹介
- ① Audience Taxonomy：IABが統計的属性や購買意図などから作成、1,600以上の属性ノードの組み合わせでオーディエンスの特性を表現
  - ② Data Transparency Standard (DTS)：最大20のフィールドからなるスキーマで、透明性のために必要な最低限の情報開示要件を定めている
  - ③ DataLabel.org repository：DTSを支持するデータプロバイダが作成したデータラベルの業界リソース

#### OpenRTBにおける既存ツールの活用

- 既に採用されている上記関連ツール・リソースの仕様の活用について言及
- コホートメンバーとサイズ：「コホート」への政策解釈、「十分大きな閾値」への言及
  - コホート市場における差別化と競争を促進するための透明性の役割：各事業者のコホート間の違いの理解や、定義・語彙の一貫性の重要性について言及
  - コホートメタデータへのアクセスの自動化：コホートに関する構成の透明性・用語の一貫性を提供する際に有用な仕組みとして、Data Transparency Standard (DTS) や、その業界リポジトリであるdatalabel.orgを紹介。
  - 分散型コホート市場におけるデータセキュリティとアカウントビリティ：  
消費者のデータへのアクセスと使用に関する、責任ある行動を確保するために必要な4つの設定を説明
    - ①自己申告したラベリングの正確性に対するコホート開発者の説明責任
    - ②消費者のプライバシー設定に対するコホート開発者の説明責任
    - ③「十分な規模のコホート」の基準に対するコホート開発者の説明責任
    - ④サプライチェーン参加者の説明責任を果たし、コホートの混入を最小限に抑える、他のセンシティブなデータタイプを持つデータ

#### OpenRTBオブジェクトモデルの関連フィールド

- OpenRTB 2.5の3つの既存オブジェクトの組み合わせで、オーディエンス分類IDやDTSメタデータのサポートに適応
- ① ユーザーオブジェクト：広告の視聴者となるユーザーの情報に関するオブジェクト
  - ② データオブジェクト：セグメントオブジェクトと一緒に使うことで、関連オブジェクトに追加データを伝える
  - ③ セグメントオブジェクト：特定のデータ単位を伝えるキーと値のペアで、事前に取引所から入札者に公表される

## ②-iv Taxonomy and Data Transparency Standards to Support Seller-defined Audience and Context Signalingの「アプローチ」での言及内容②

### カテゴリ

### 概要

Cookieとメタデータの受け渡し  
をサポートする  
オーディエンスターゲット  
ディング

OpenRTBのオブジェクト/  
属性フィールドをDTSフィー  
ルドにマッピング

ユーザーオブジェクト、データオブジェクト、セグメントオブジェクトの各フィールドをDTSのコアフィールドにマッピングする方法の提案

オーディエンスコホートシグナ  
リングのJSON例

ユーザーデータのオブジェクト配列について、定義を記載する際のJSONの構造例示

Prebid.jsによる  
OpenRTB16内のコホート  
シグナリングのサポート

本件のサポートを行い、検証を行っているPrebid社に関する関連文書への言及

コホートプロバイダー、  
OpenRTB、  
DataLabel.org間の  
データフロー

コホートプロバイダーが入札要求に、コホートプロバイダー名、プロバイダーの内部分類名、プロバイダー独自のID、および標準化されたIDマッピングを含める場合に、DMPやDSPなどが視聴者コホートに関するDTSメタデータを取得するフローについて説明

その他の業界での使用例  
とコホートメタデータの有用  
性

分類法に基づくアプローチと業界のコホートメタデータの一元化がもたらす周辺利益として、中立的な団体が単一のメタデータを管理することで、DSPやDMP、データプロバイダーのデータ統合負担を軽減できる点などに言及

DataLabel.orgのプラッ  
トフォームとGTMへの必要  
な変更

前述のアプローチをする際に、既存のdatalabel.orgのプラットフォームとGoogle Tag Managerに対して行う必要がある変更点

コンテキストターゲティングを  
サポートするIDの受け渡し

ブラウザ、モバイル、OTT環境におけるWebサイトやアプリの、“Aboutness”を記述する標準的な方法について記載  
※ “Aboutness”は、「コンテンツの言語」「フォームファクタ※」「由来」「メディアのタイプ」などの追加属性とは区別しておく必要がある

※フォームファクタ：コンテンツのデータフォーマットや性質

## 参考：海外の関連動向

## TCFはGDPR・eプライバシー指令の遵守を目的に策定されたが、ベルギーのデータ保護当局よりGDPR違反の指摘を受けている。

## ■ 指摘の経緯：

- 2020年11月、ベルギーのデータ保護当局（APD）によるレビューで、TCFにおけるIAB Europeの役割に関し、懸念事項が指摘される。
- 2021年11月5日 裁定案の確定が近づいている旨、APDから連絡を受けたとIAB Europeが公表。
- 裁定案は、2021年11月中に欧州の他のデータ保護当局によりレビューされ、APDまたは欧州データ保護委員会（EDPB）により確定される見込み。

## ■ 争点：

- TCFでは、CMPを通じてベンダーに配信される利用者の同意取得状況等のデジタル信号を「TC Strings」と規定している。
- APDは「TC Strings」が個人データに該当し、デジタル広告のリアルタイム入札の中で、IAB Europeが「TC Strings」の共同管理者（joint controller）になりうると指摘している。

## ■ 今後の対応：

- 裁定確定後6か月以内の是正が求められており、IAB Europeの行動計画についてAPDが監督する。
- IAB Europeは本是正措置の結果、TCFがGDPRに完全に準拠した行動規範であることが公に認められるとして、裁定を歓迎する旨を表明している。

## TC String Updates - String includes new signals

TCF version 2.0 Transparency and Consent String Contents:

- General Metadata
- User Consent
- Legitimate Interest
- Publisher Controls
  - purposes
  - legal basis\*

CMP ID	Vendor Consent	Purpose Consent	Vendor LI	Purpose LI	Special Feature opt-in	Global consent	OOB Allowed?	Custom Stacks	Pub Controls
###	0/1	0/1	0/1	0/1	0/1	0/1	0/1	0/1	###

Blue: Present in v1.0  
Green: New in v2.0

\* only if the Vendor indicates flexibility

## 参考：海外の関連動向

2022年2月2日、TCFに対するGDPR違反の決定※が下された。決定ではTCFの利用までを禁止してはいないが、IAB Europeに対して制裁金の過料と是正措置の立案を求めている。

## ■ 決定の内容：

- IAB EuropeはTC stringsを通じたユーザーからの同意取得に関してデータ管理者として行動していると認められるが、データ管理者に求められる義務を果たしていない。
- CMPのインターフェースを通じてユーザーに与えられる情報は広告ビジネスにおけるリアルタイム入札の仕組みなどに鑑みるとあまりに一般的かつ曖昧で、ユーザー自身が自分の情報を管理し続けることを難しくさせている。
- IAB Europeに25万ユーロの制裁金を課すとともに、2か月以内のアクションプランの提出を求める。

## ■ 是正のポイント：

- 事業者の正当な権利を根拠とした処理の禁止
- TCF参加企業のGDPR遵守状況に対する厳格な審査、モニタリング

## ■ IAB Europeの反応：

- 業界団体の1つであるIAB Europeが広告業界全体のデータ処理活動に関して責任を負うことはありえないとして、2月11日、ベルギー市場裁判所（the Belgian Market Court）に控訴した。
- また、アクションプランの提出と是正措置期間（6か月）が認められているにも関わらず、複数のデータ保護当局がパブリッシャーに対しTCFの利用切り替えを助言していることに抗議している。

※ 本決定はGDPRにおける協調メカニズム（the one-stop-shop mechanism）の下くだされており、欧州域内の大部分のデータ保護当局による承認を得たうえで実施されている。

（出所）

the Belgian DPAのプレスリリース（<https://www.dataprotectionauthority.be/citizen/iab-europe-held-responsible-for-a-mechanism-that-infringes-the-gdpr>）（2022年2月17日アクセス）

IAB Europeのプレスリリース（<https://iab europe.eu/all-news/belgian-dpa-decision-of-2nd-february-are-other-dpas-right-to-warn-about-continued-use-of-the-tcf/>）（2022年2月17日アクセス）

IAB Europeのプレスリリース（<https://iab europe.eu/all-news/iab-europe-to-appeal-belgian-data-protection-authority-ruling/>）（2022年2月17日アクセス）

The text is framed by two decorative swooshes. The top swoosh is a gradient bar transitioning from blue on the left to red on the right. The bottom swoosh is a solid blue bar.

***Share the Next Values!***