

## 第 77 回 JIPDEC セミナー講演レポート

### インターネット広告業界の取り組みと信頼構築のヒント

D.A.コンソーシアムホールディングス株式会社  
テクノロジー&データ戦略センター 広告技術研究室  
チームリーダー 原田 俊氏

インターネット広告業界では、広告主との信頼性、生活者との信頼性に対しそれぞれ課題がある。今日は、生活者との信頼性に関する問題である、プライバシー保護、ユーザー体験、政治広告の 3 つのテーマについてフォーカスしてお話していきたい。



#### データ活用とプライバシー保護

広告ビジネスは生活者の許可をもとに行う前提となっているが、その手段はこれまでオプトアウトが主流で、プライバシーポリシーで利用目的やオプトアウトするための手段を通知する方法を取っていた。

米国では、広告主、広告会社、媒体社が加盟する Digital Advertising Alliance (DAA) というプライバシー領域に関する業界団体が、通知や同意取得に関する自主規制ガイドラインを作成し、これに準拠する事業者インフォメーションアイコンの使用を認めている。DAA では、その他にも、ターゲティングしている事業者を確認してオプトアウトできるツール (WebChoices) や、モバイルアプリの広告表示で使用されている Google や Apple が提供しているモバイル ID の上に仮想 ID を構築し、事業者単位でオプトアウトを設定できるアプリ (AppChoices) を提供している。

また、業界標準化まではされていないが、プラットフォーム各社はユーザーが自分はどういう傾向・属性に分類されているか自分で確認できるプライバシーダッシュボードを提供している。これらの取り組みは、広告業界では信頼性・透明性を高めるものとして評価されている。

しかし、GDPR が施行されたことによりプライバシー保護のレベル感が変わってきた。GDPR では同意取得を前提としており、これに合わせて Google がプライバシーポリシーを変更したり、YouTube がサードパーティツールによるトラッキングを廃止、さらに消費者により分かりやすく説明するための取り組みなどが行われている。

米国のインターネット広告業界団体 Interactive Advertising Bureau (IAB) は、GDPR によりオプトアウトからオプトインへの変更が必要となった業界プレイヤーの対応策をまとめた「GDPR Transparency and Consent Framework」を発表、その中で、企業ごとに対応するのではなく業界として対応していくため、Consent Manager Provider (CMP) と呼ばれるツールも標準化している。これは、ユーザーに利用目的を通知し、目的ごとに同意取得させ、データにアクセスを許すベンダーの選択をしてもらい、その結果（利用目的およびベンダーごとの同意取得有無）を広告取引におけるオークションや DMP とのデータのやり取りに反映させるもので、欧米ではグローバルプレイヤーを中心に利用されはじめている。

### ブラウザのプライバシー保護強化の流れ

Apple の MacOS/iOS における Safari ブラウザは、バージョンが上がるごとにプライバシー保護施策が高度化しており、最新バージョンではクロスサイトトラッキング（サイトを横断してのトラッキング）がデフォルトで除外となっている。この流れに Firefox 等の他ブラウザも追随しており、サードパーティ Cookie が利用できない環境が増えつつある。さらに、広告システムごとに異なる ID 体系をそろえるために行われる CookieSync によって、サイトの読込速度が低下しユーザビリティが損なわれたり、データの集合における重なり部分しか利用できないことで、ターゲティング可能なオーディエンスのボリュームが減少（全体の 27% 程度にまで落ち込む）してしまうといった問題も起きている。

この問題に対応するため、米国では DigiTrust という仕組みを導入している。これまでは広告会社がそれぞれ媒体社サイトにタグを張っていたが、DigiTrust は業界で 1 つの共通ドメインをファーストパーティ Cookie に書き込み広告配信システムと共有することで、サードパーティ Cookie や CookieSync の問題を解消させようとするもので、すでに全世界の大手ベンダーが利用していることで、85% 程度のトラフィックで DigiTrust のしくみが利用されているという。

### プロファイリングについて考える

GDPR ではプロファイリングが問題になっているが、そもそもの「プロファイリングとは何なのか」についてはあまり触れられていない。よく、「ネット広告でターゲティングをするための自動処理がプロファイリングと呼ばれ、その行為自体に問題があるのではないか」と言われることがあるが、では、GDPR でいう「問題性のある自動処理」とはどのようなものが考えられるのだろうか。

現在のターゲティング手法としては、広告主サイトの閲覧状況をもとに媒体メディアにも広告を出すリターゲティングや、属性データや興味関心、位置情報をもとにしたオーディエンスターゲティング、広告主顧客データとマッチした層に広告を出すカスタムオーディエンス等がある。

リターゲティングは「気持ちが悪い」と言われやすい手法だが、データの活用方法はシンプルで「サイトに来た。商品ページを見た」という情報だけで広告を表示しており、これをプロファイリングとするのは疑問が残る。

また、個人データを使うカスタムオーディエンスは、広告主が持つ個人データが広告システムと連動する仕組みが「気持ち悪い」と感じさせたり、「法律上問題がないのか」という話になるが、手法としてはデータマッチングなので、これもプロファイリングとは異なるように思われる。

反対に、性別や年齢等シンプルに見える属性ターゲティングが、実は一番プロファイリングに関係するのではないかと考えている。先日、消費者団体の訴えにより Facebook が民族や宗教等ではターゲティングできないようにしたが、これまでも性別や年齢、家族構成等の属性が就職や入居審査、クレジットカードの信用スコアリング等の際に差別的に使われたケースもある。差別につながるデータ活用は問題外だが、使われ方によっては単純な属性でも不快に感じる場合が少なくないのではないか。

思うに、どんなに正しい経路でデータを取得し、手順に則った正しい処理を行ったとしても、消費者は最終的なアウトプットである広告（クリエイティブ）しか見ることができないため、そこで少しでも不信感や不快感を抱かせてしまったら、その広告は失敗であり、「その処理が“プロファイリング”ではないか」と言われても反論はできないのではないか。

データを多数保有することでビッグブラザー的だと揶揄される Google では、個別の広告ごとに「なぜあなたにこの広告が出たか」を表示する「Why this ad?」機能を追加するなど、どんなデータを持っているかを提示するだけでなく、どのようにキャンペーン等で使っているかを示し、データ活用全体の透明性を図ろうとしている。これはアウトプットしか見られず、処理の透明性を担保できない広告という業態においてきわめて有効な透明性の手法ではないか。

さて、私は広告配信事業者、DMP 事業者の団体である DDAI (Data Driven Advertising Initiative) の運営に携わっており、そこでは広告配信事業者のオプトアウト機能を一括提供しているが、オプトアウト手続きをしたユーザーに行ったアンケート結果では、オプトアウトの理由は以下のとおりであった。

- 個人情報を使われているようで気持ち悪い 41% → プライバシーの問題
- 好まない広告が出てくるから 33% → 関連性の問題
- 同じ広告が出てくる 22% → フリークエンシー過多の問題
- その他（鬱陶しい、コンテンツが見づらい、通信速度が遅くなる） 5% → 広告フォーマットの問題

## 広告とユーザー体験

追いかけてくる広告（サイト内の操作時に常についてくる広告やサイト間をまたがって表示される広告）や重い広告（リッチな広告やタグが貼られすぎのページ）は、「うざい広

告」と評判が悪いだけでなく、ユーザーをアドブロック利用に向かわせてしまう。日本でのアドブロック利用はまだ 10%程度だが、米国では 30%まで達しビジネスモデルに大きな影響を与えている。

このため IAB では「LEAN」原則（Light（軽量で）、Encrypted（暗号化され）、Ad Choice Supported（プライバシー保護基準を満たし）、Non-Invasive Ads（ユーザー体験を阻害しない広告））を発表し、それに基づき広告フォーマット基準を改定し、時代に合わなくなった広告フォーマットを廃止するなどの自主規制を行っており、Google も自動再生動画広告の廃止や業界団体でユーザー体験を阻害するとされた広告フォーマットでの Google 広告掲出を禁止している。

また、オプトアウトは配信事業者単位でターゲティング広告停止になるためユーザーデータが保持できず、ターゲティングもユーザーが嫌な広告の出し分けも不可能となってしまうが、アドミュートであれば広告クリエイティブ単位で拒否が可能になるので、Google や LINE、Facebook 等でも導入されている。

## 政治広告と透明性

政治と広告、インターネットを巡っては様々な問題があるが、その 1 つがフェイクニュースである。これは、悪意のあるプレイヤーが間違った情報を意図的に拡散しているもので、これに対して Google はかなり積極的に対応しており、例えば誤った内容を伝える動画コンテンツには Wikipedia 等別のソース情報を表示させたり、ファクトチェックが行われたものにラベルを表示して事実に基づいたものであることを証明する試みを行っている。

もう 1 つの問題としては、Cambridge Analytica 問題のようなプラットフォームのハッキングともいえるものがある。この問題は、Facebook がただのツールではなく、利用者にとってニュースの主要入手手段、つまり普段意識しないが、確実に現実認識の手段となっていることが関係している。Facebook は二度と政治に関連して同様の問題が起きないように、海外からの政治広告の排除、ロシア政府に関連するアカウントやページの廃止、問題を研究する機関の設立、また政治広告のターゲティング状況や予算等を可視化するツールを提供する等して、透明性の確保を図ろうとしている。Twitter も同様の取り組みを行っており、業界団体の DAA も政治広告の透明性を高めるための自主規制原則を発表した。

## 信頼性構築の方向性

とかく大手プラットフォーム各社が問題視されがちであるが、実際の企業や業界団体の取り組みを見ていくと、プラットフォーム各社が最も真摯に対応しているのを見て取れる。しかし、その想定を上回る問題が日々起きているというのが現状ではないだろうか。

広告のユーザー体験でいうと、広告を見る（広告商品を買う）ことで媒体者に広告収入が入り、消費者はそれにより無料でコンテンツの提供を受けられるという本来のバリューエクステンジが、アドブロックツールが象徴するように、現在壊れてかけており、再構築が

必要となってきたと感じる。消費者意識調査では、データの種類よりも、データの利用目的、消費者が受けるメリットによって企業のデータ活用の許容度が異なるというデータもある。

また、バリューエクステンションを再構築する前に、そもそも媒体社や広告主がデータを渡す信用に足る相手かどうかが問われている。まずは信頼性の構築が必要だ。信頼性構築の方向性としては、本日見てきた通り、データの利用目的や保有データの開示、アウトプットにおけるデータ利用方法の開示、ユーザビリティの改善、トレーサビリティの提供などが挙げられ、広告業界のみならず、他の業界にとっても参考になる部分はあるのではないかと。