



自分でコントロールする ネット広告

佐藤 和明 Sato Kazuaki 茨城キリスト教大学 経営学部 教授

大学教員の傍ら、Webマーケティング関連の書籍の執筆やWebプランナーを務める。研究テーマは「ITビジネス」、特に「デジタルマーケティング」で、「分かりやすさ」をモットーに業務に従事している

アナログ広告と デジタル広告の違い

普段の生活で目にするいろいろな広告には、機能的な面で大きく異なる点があります。それはアナログかデジタルかという点です。

アナログ広告の代表は、テレビ、新聞、雑誌、ラジオの4大マスメディア広告、デジタル広告は、パソコンやスマホやタブレットなどのデジタル端末に表示される広告などで、広告主がターゲットとしている潜在顧客への広告メッセージの届き方に、特徴的な違いがあります。

2020年は新型コロナ禍で、経済活動が低迷しました。当然のことながら、日本の広告費全体は前年より減少し、アナログ広告の出稿も減少しています。しかし、デジタル広告の出稿費は、逆に伸びたのです*1。

アナログ広告の場合を、テレビCMで考えてみましょう。幅広い層に人気のあるテレビ番組でCMが流れている間に、自分が興味関心のあるCMは、どれくらい流れるでしょうか。気になるCMが1つ、2つあれば、よいほうだと思います。

一方、デジタル広告は、見る人の世代、居住地、性別、趣味や嗜好性^{しこうせい}に合わせて広告を配信することが可能です。広告主からすれば、訴求したい消費者の属性に合わせて、広告を配信で

きるメリットがあり、しかも、4大マスメディアの広告費より割安な面もあるため、コロナ禍のなかでも前年比で伸びたと考えられます。

広告主にとってメリットのあるデジタル広告ですが、受け手である消費者にとってはデメリットといえる問題点がクローズアップされてきました。それが、個人関連情報の利用問題です。

デジタル広告における 配信のしくみと問題点

日常、デジタル端末を利用している時には意識しませんが、Webサイトを閲覧することなどで、知らず知らずのうちに広告配信事業者等へ個人関連情報を提供してしまっています。広告配信事業者等は、その個人関連情報を利用し、消費者ごとの興味関心に合った広告を配信しています。このような広告を「ターゲット広告」といいます。広告主にとって「潜在顧客」へのリーチ(到達度)が高いことが特長です。

しかしながらユーザーからみると、無意識のうちに個人関連情報を提供してしまっているため、法律による規制も進んでいます。

世界の代表的な個人情報保護規制法は、EUのGDPR(一般データ保護規則)、アメリカのCCPA(カリフォルニア州消費者プライバシー法)などがあります。日本では、2020年6月に改正個人情報保護法が公布されました。

*1 電通NEWS RELEASE「2020年日本の広告費」(2021年2月25日) <https://www.dentsu.co.jp/news/release/pdf-cms/2021012-0225.pdf>

これらの背景となった個人関連情報である「ブラウザ閲覧履歴」「スマホ・タブレットの端末情報」「位置情報」などを収集・利用するしくみと対応策などを解説していきましょう。

ネット閲覧履歴Cookieを利用した広告配信

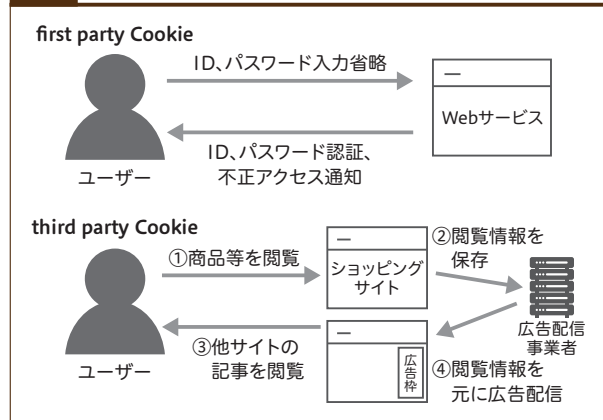
Cookieとは何か

Cookie(クッキー)は、Webブラウザ(以下、ブラウザ)でアクセスしたWebサイト(以下、サイト)から、ブラウザに保存される情報のことをいいます。ブラウザによってCookieの保存先は異なりますが、ブラウザの設定等で確認することができ、Cookieファイルにアクセスすることもできます。Cookieは、どこのサイトへ訪問したかが判別できるようになっており、アクセス履歴ともいえるものです。

プライバシーを侵害されているような印象もありますが、実はCookieにはネット利用を快適化させる機能があるのです。その1つが、Webサービスに必要となるIDとパスワードをブラウザに記憶させておく機能です。また、Cookieによって、アクセス状況を調査し、例えばユーザーがパソコンでアクセス後、新たにほかのスマホ等で同一のIDとパスワードを使ってアクセスすると、SMSやメールで認証コードが送付されてくる二段階認証機能もあり、ほかの端末から不正なログインを防止する機能として有効なため、ネットショッピングやネットバンキングなどで、広くCookieが利用されています。これらを「first party(ファーストパーティ) Cookie」といいます。

一方、広告配信に利用するCookieを「third party(サードパーティ) Cookie」といいます。first party Cookieはユーザーと利用したWebサービス間でCookieのやり取りが完結しますが、third party Cookieは複数のサイト間を横断的にトラッキング*2することが可能です。

図1 Cookieの役割の違い



例えば、ショッピングサイトで商品Aを閲覧し、購入せずにニュースサイトへ移動したとします。ニュースサイトで記事閲覧中に、商品Aの広告が掲載された場合には、third party Cookieを利用して、ニュースサイトの広告枠へ広告を表示しているのです。これを「リターゲティング広告」といいます。

first party Cookie、third party Cookieをまとめると、図1のようになります。簡潔に言えば、first party Cookieは会員証やIDの役割、third party Cookieは個人を特定しない限り*3、利用できる非個人データとなります。

ブラウザ提供事業者のCookie対応

third party Cookieは、ブラウザを提供する事業者が、前述の法規制を背景に問題視するようになりました。特にApple社は、2017年9月に業界に先駆けてthird party Cookieの防止機能であるITPを、iOS11に搭載されている自社のブラウザ「Safari」に実装しました。ITPは、「Intelligent Tracking Prevention」の略で、デジタル広告のトラッキングを防止できる機能です。現在は、同社のすべてのOSに対応しており、2021年4月現在、ITP2.3となっています。

また、「Firefox」が2019年9月からすべてのブラウザについて、「ETP (Enhanced Tracking Protection)」と呼ばれる機能を実装し、トラッキングの追跡をブロックできるようにしています。

Google社は自社ブラウザである「Chrome」

*2 アクセスしてきたユーザーがWebサイト内でどのページを閲覧しているかを追跡すること

*3 技術的には個人を特定することも可能

の対応として、2022年1月にはthird party Cookie非対応になると、ある程度の方向性を示しました。ブラウザの設定により、ユーザーの任意で選択・設定できるようになります。同様に「Microsoft Edge」も任意で選択・設定ができます。

ユーザーのthird party Cookie対策

ユーザー自ら行える対応策を述べていきましょう(2021年3月現在)。端末によって異なりますが、まずは、SafariやFirefoxの最新版を利用することで、リスクを軽減することができます。ブラウザの好みで、ChromeやMicrosoft Edgeを利用したい人は、各ブラウザの最新版で次のような設定等を行うことにより、安全なネットサーフィンを楽しめます。

Chromeの場合は、「設定」→「プライバシーとセキュリティ」→「サードパーティのCookieをブロックする」の順で設定することで、third party Cookie対策が可能です。Microsoft Edgeも、「設定」からCookieの設定を変更できます。

振り分けられた広告IDでの 広告配信

モバイル端末に付与される広告ID

デジタル端末には、固有の端末IDが付与されています。端末IDに加え、アプリをインストールすると、「広告ID」が各デジタル端末に付与されます。広告IDの呼称は、購入した端末のOSによって異なります。iPhoneやiPadの場合は「IDFA(Identifier For Advertising)」と呼ばれます。Android OSの端末は「AAID(Google Advertising ID)」や「GAID」「ADID」と呼ばれることもあります。

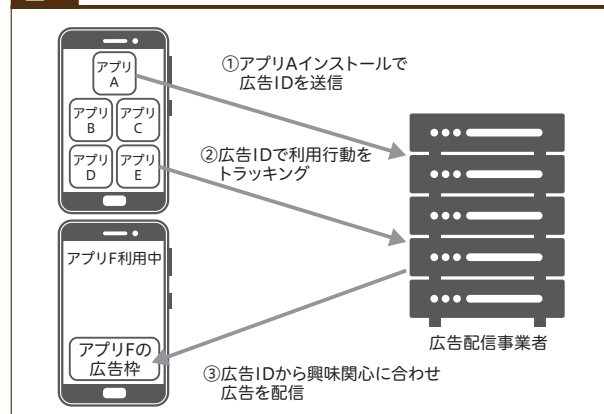
広告IDでの配信のしくみ

広告IDは、アプリ経由で、趣味や嗜好性が把握できるデータを広告配信事業者へ送信します。送信されるタイミングは、アプリ起動時とアプリ内の広告をクリックした時です。Cookieと

は異なり、アプリからデータが送信されると理解しておくといよいでしょう*4。

広告IDは、Cookieと同じく、ユーザーの特定はせずに行動をトラッキングし、広告配信事業者は、広告IDとトラッキングした情報を元に広告を配信します。図2を見てください。

図2 広告IDのしくみ



アプリAをインストールした時点で、広告IDが広告配信事業者へ送信されます。その後、スポーツ系ゲームアプリB、C、D、Eを利用した後に、広告付きのフリーアプリFをダウンロードし、利用を開始したとしましょう。

Fを利用すると、広告枠にはユーザーの興味関心(アプリB、C、D、Eの利用状況からの推測)に合わせて、スポーツ系のゲームアプリ広告が表示されます。アプリの利用による行動ターゲティング*5を行うのが、広告IDなのです。

広告IDの動向と配信ブロック

Apple社は、業界に先駆けて広告IDであるIDFAの取得を、2021年春にオプトイン化すると発表しました。オプトインとは事前承諾の意味で、IDFAはiPhoneやiPad上でアプリからの個人データのトラッキングについて、ユーザーの許可を得なければ取得できないと決定したのです。今までは承諾なしで、個人の利用状況を取得していたわけですが、今後はオプトインとなるため、ひとまず安心です。

一方、Androidの場合は、2021年現在、AAIDがオプトイン規制されていないため、

*4 Cookieの場合は、広告配信事業者がユーザーのブラウザに保存されているCookieデータをのぞきに行く

*5 ユーザーのアプリ利用行動パターンからターゲットを絞ること

ユーザー自ら設定しなければなりません。

機種によって違いもありますが、ホーム画面で「設定」を選択し、「Google」を選択します。次に表示されている「広告」を開き、「広告のカスタマイズをオプトアウトする」のスイッチをタップして「ON」にすると、アラートが出るので、「OK」を選んで設定は完了です(図3)。

図3 Android 端末での設定手順



デジタル端末の位置情報から 配信される広告

位置情報広告のしくみ

位置情報広告は、ジオターゲティング広告ともいい、デジタル端末の位置から最適な広告を配信する機能です。

広告配信のための位置情報を特定する方法には、さまざまなパターンがあります。例えば、スマホのGPS位置情報機能です。スマホのGPSは、「A-GPS」というしくみが使われています。「A」は、補助を表す英語の「Assist」の頭文字で、通常のGPSとは異なり、現在地から近い携帯電話基地局にアクセスして位置情報を割り出しています。

よく位置情報を利用するアプリを利用していると、Wi-Fiの接続時に、正確な位置が分かる等のアラートが表示されることがあります。これは、Wi-Fiアクセスポイントのルーター固有番号を住所等とともにデータベース化しているため、精度が高いからです。

Wi-Fiに関連しますが、IPアドレスも位置情報に利用されています。デジタル端末のインターネット接続先にもよりますが、地域ごとにIPアドレスが割り当てられており、IPアドレ

スの情報から広告を配信することもあります。また、Bluetoothを利用したビーコン(無線標識)もあります。GPSと異なり狭いエリア、例えば商業施設内で利用され、広告配信のみならず施設案内などにも活用できます。

位置情報広告の種類と機能停止方法

新型コロナ禍で、主要駅の人出の増減などの報道を目にしますが、これらは位置情報のしくみで概説したように、ユーザーのデジタル端末から得た情報を使っています。位置情報広告も同様のしくみで配信されています。広告主にとっては、潜在顧客を絞り込んで出稿できるため、位置情報広告は顧客獲得のチャンスとなる費用対効果の高い広告です。ポータルサイトやニュースサイトの記事中の広告にも位置情報から配信されているものがあります。目障りと思う人も多いでしょうが、便利な側面もあります。

例えば、宿泊先も決めていない、急な出張、そして取引先での打ち合わせが長引き、21時を過ぎていたと想定してみましょう。なじみのない土地でのホテル探しは、困難を極めます。そんな時に、検索エンジンで「ホテル」と検索すると、広告出稿している近隣のホテルがマップ上に表示され、ホテル探しが容易になります。

ほかにも、ピザ宅配、タクシー予約、最寄りの医療機関などのキーワード検索などで、便利に利用でき、広告主と消費者の双方にメリットのあるケースも考えられます。

一方、位置情報取得に対し快く思わない人もいます。位置情報サービスを停止する設定があります。iPhoneやiPadの場合は、「設定」から「プライバシー」を選択し、「位置情報サービス」へアクセスし、機能をオフに設定すると、位置情報を停止することができます。

Androidの場合は機種により違いもありますが、「設定」を開き、「ユーザー設定」で「位置情報アクセス」を選択し、「位置情報の使用」をオフにすると、停止できます。

パソコンにもブラウザの位置情報設定があるので、確認してみるとよいでしょう。