第 74 回 JIPDEC セミナー講演レポート

行動ターゲティング広告の仕組みと課題

～求められるプライバシー・セキュリティ対応～

株式会社 DataSign
代表取締役社長　太田　祐一氏

私は、もともとはデータ売買側の立場で、Cookie データを収集する DMP（Digital Marketing Platform）や Cookie と個人情報を紐づける MA（Marketing Automation）を、日本で利用され始めた 2011 年頃から開発に携わってきた。この中で、Cookie と個人情報を紐づけることで、例えば問合せフォームで、本人は匿名で問い合わせをしたつもりでも、問い合わせを受ける方は本人が誰だかわかってしまう等プライバシーの問題に直面することもあった。

DMP などで広告に用いられるデータを収集されていることは消費者のほとんどが認知していないか、認知していたとしてもその実態を把握するのは困難である。また、データを購入する広告主も、データの収集場所・方法を把握できないため、「効果が出ない」「適切に収集されたデータかどうかわからない」といった問題がある。

このため、データ収集の透明性を高め、適切なデータ流通を促進させることを目的として株式会社 DataSign を設立した。

■オンライン広告の歴史

最初のオンライン広告は、1994 年に HotWired というメディアに掲載された AT＆T のバナー広告で、掲載料は 1 カ月 100 万円だったといわれている。この年に創業を開始した Amazon も、その翌年の 1995 年にはアフェリエイトプログラムを開始している。

一方、日本では 1996 年に Yahoo! JAPAN がサービスを開始し、1997 年には Microsoft の広告が掲載されている。この当時は、Yahoo!JAPAN を閲覧しているということは PC 所有者であり Microsoft Office 利用層、とターゲティングし広告出稿する価値があると判断された。

1)1996 年～メディアレップ・アドネットワークの出現

この頃、広告主、代理店、メディアというプレイヤーに加え、出稿先メディアの獲得・取

次を行うメディアレップという新たなプレイヤーが誕生した。その後インターネット利用者が急増、ネットメディアも Yahoo 等大手に限らず多種多様なものが出現しはじめテーマも細分化されてきたため、広告出稿もメディアごとではなく、商品・サービスにマッチした広告枠の売買へと変化した。1998 年には、それらを束ねて扱うアドネットワーク（車に関する広告であれば、車情報サイトとニュースサイトの車特集ページへの出稿等パッケージ化したもの）が登場し、課金形態も掲載期間に対するものからクリック数や表示回数に対するものへと変化してきた。

この頃の Cookie の動きは、A サイトを閲覧した人が B サイトも閲覧したということが後で集計すればわかるといった程度のもので、その閲覧履歴をもとに即時に何かを行うというものではなかったが、米国では 1999 年に DoubleClick（Cookie＆行動履歴）がアバカスダイレクト（通販の個人情報＆購買履歴）を買収しようとして、全米で集団訴訟が起き計画中止となるなど、プライバシーに対する懸念も表面化してきた。

2)2000 年～検索連動型（運用型）広告のはじまり

2000 年には、Google Adwords（検索ワードに合った広告を表示）が始まり、検索ワードに一番高い値をつけた広告が最上位に掲載されるオークション形式が導入された。この検索連携型広告では、メディアレップに加え、どういう検索ワードをいくらで入札するかを決める運用会社が新たなプレイヤーとして登場した。この検索連動型広告の方がディスプレイ広告より効果が高いとして、利用が急増し、検索メディアが多額の広告収入を得るようになった。

3)2005 年～ディスプレイ広告の高度化（行動ターゲティング、Facebook）

2005 年頃、JavaScript の利用環境が整い、オープンソースでレスポンスの早いデータ処理技術が提供されるようになると、ディスプレイ広告で広告の出し分けにより効果的にアドネットワークを運用できるようになった。同時に、Cookie を使ったリマーケティング・リターゲティング技術も進化し、2007 年には広告主の企業サイト閲覧時点でアドネットワークの ID を付与し、閲覧者が他のメディアサイトを訪問時に広告主の広告を表示させる仕組み等が出来上がってきた。これが行動ターゲティングのはしりである。

従来のディスプレイ広告ではデータを収集するためには各サイトを回って集める必要があったが、2010 年に登場した Facebook では、本人が Facebook に様々な情報を登録するだけでなく、多くの企業サイトやメディアサイトが「いいね」ボタンに設置したり、Facebook ログインを利用したりすることで、様々な行動履歴が FacebookID に紐づけられて一元的に Facebook に収集される仕組みが作られた。さらに、Facebook はリアル店舗での購買履歴や年収/行動データ等も購入し（現時点では中止）、ネット・リアル空間双方の行動をもとにプロファイリングの精度を高め、表示にあたっても、フィード内に友達の投稿に混ざって自然な形で、友達が「いいね」と言っている等の情報と併せた広告表示を行ったため、利用者の

クリック率は高く、多くの企業が Facebook への広告出稿に殺到した。その一方で、同時期に、はてなブックマークボタンの行動履歴をアドネットワークに販売していた事例は炎上し、サービス中止となっている。

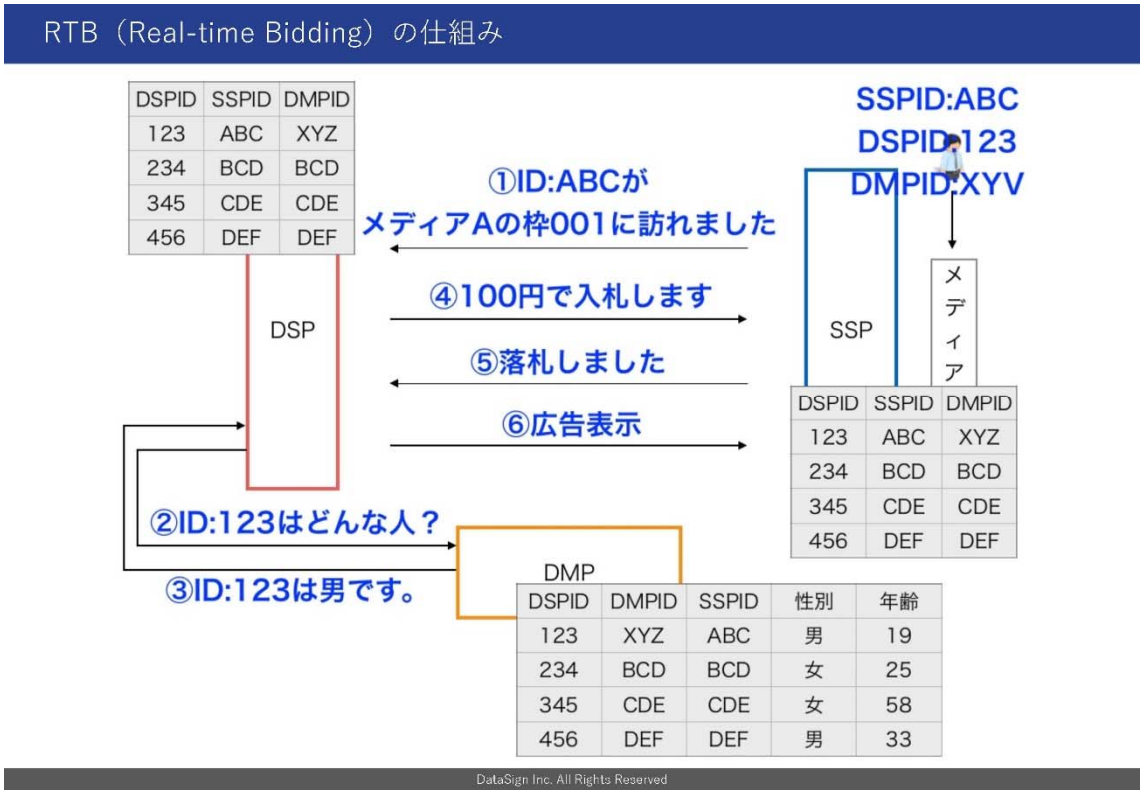
4)2010 年～オークションの登場

2010 年頃には、ビッグデータ処理技術が一般化し、多くの企業がビッグデータに基づいたマーケティングを行うようになり、より広告効果を高める手法も検討されはじめた。

広告主にとっては、広告枠自体に価値があるのではなく、そこに誰が来るかに価値がある。同じ広告枠でも、表示される広告のターゲット層が閲覧すれば広告主にとっての価値は高い。一方メディア側も、同じ広告枠であればより高価格で販売したい、自分たちが持つ履歴データをマネタイズしたいというニーズがあり、それを満たす形として、2011 年頃にはメディアを束ねて訪れた人ごとに広告表示権をオークションにかける仕組み（RTB：Real-time Bidding）が登場した。

この仕組みでは、メディア側の閲覧動向を束ねる SSP（Supply Side Platform）、広告主側の出稿依頼を束ねる DSP（Demand Side Platform）、そして Cookie 情報を束ねる DMP が「誰が来た」という情報を共有する必要がある。このため、それぞれの ID が紐づけ可能な形で管理されており、結果として個人識別性が高いデータを元に広告が配信されている。

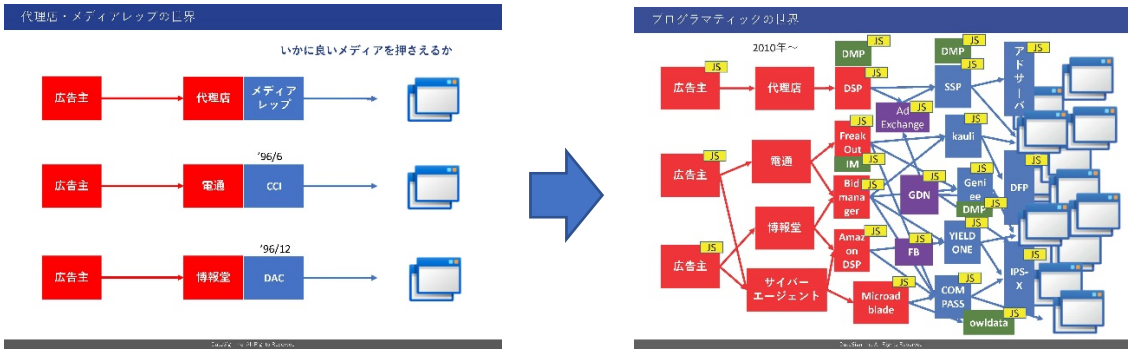
オークションで有利に落札するには、「自分だけが知っている情報」をいかに蓄えるかが勝負となるため、各社が競って質の高いデータ収集と囲い込みを行っている。



■課題

現在の仕組みでは、広告主とメディアの距離が遠くなり、その結果「どのメディアに広告出稿されるかわからない」、「どういう広告主の広告が表示されるわからない」ことが原因となって様々な課題が出てきている。

1996 年　　2011 年



1)不正サイト・不正広告問題

漫画村の問題では、漫画村を閲覧すると閲覧者には見えない「隠しサイト」にもアクセスしたことになり、そこに表示された広告についても広告収入を得る仕組みとなっていたが、広告主は隠しサイトに自社の広告が出ていることを把握するのが難しい。

また、メディア側でもどこが出稿した広告がどこを経由して表示されているか把握できないため、悪質な広告を止めることができない。

2) コンプライアンス

リターゲティング広告を利用する場合、広告主自体がいろいろなところにデータを提供しているがすべてを把握しきれていない。例えば Google Tag Manager の JavaScript だけを自社サイトに入れたつもりでも、実際にはそれに紐づいて様々なサービスに対して自社サイト訪問者のブラウザからリクエストが送られ、自社では把握していないサービスが JavaScript を実行している。クライアント PC から呼び出されているため、企業側では把握することはできない。

１日、自分が Web サイトを閲覧するとどれだけ広告事業者等にデータが送信されているか集計したところ、約 60 サイトを利用して 250 社に行動履歴が送信されていた。

3)セキュリティの問題

JavaScript は行動履歴を収集するだけでなく、フォームに入力した情報（ログイン ID やパスワード、クレジットカード番号）や Cookie 情報、位置情報の取得や、フォーム自体の

改ざん、不正サイトへの誘導も行うことができる。実際に、金融機関のログインページに国内外の複数事業者がログイン ID、パスワードの閲覧が可能な状態となっているケースもあった。また、フォーム改ざんによる被害では、委託先フォームが改ざんされフォームに入力したクレジットカード情報が第三者に二重送信されていた。こういったケースでは、いくら自社のサーバーを調査しても発見することはできない。

DataSign では、これらの課題解決の 1 つの手段として、自社サイトに埋め込まれているサービスや外部へのリクエストを検知し、閲覧者が認識できるようにオンラインプライバシー通知を自動生成したり、自社で必要としないリクエストをクライアント側でブロックするサービス「DataSign FE」を提供し、より透明性の高いネット環境作りに寄与していきたいと考えている。