JavaScript によるクライアント PC 操作の法律問題

若江雅子[†1]　森亮二[†2]　吉井英樹[†3]

概要：アドテクノロジーが急速に進化する中、広告業界を中心に、個人に関する大量のデータ収集と流通が進んでいる。これらは、収集の「入口」においては個人の使用端末を識別する情報に過ぎないため個人情報保護法の規制を受けないが、事業者間でやりとりされるうち、事業者の保有する情報によっては個人情報に変わり得るものである。しかし、その流通の実態は見えにくく、データ当事者である個人が関与するのは難しい。本研究では、こうした実態について、主に JavaScript を駆使することで大量のデータ流通を実現しているフェイスブックや DMP 事業者のケースについて検証し、これに対して現行法がどう対応しうるのか、JavaScript 設置者の責任はどうあるべきか、考察する。

キーワード：JavaScript、cookie、Facebook、DMP、個人情報保護法

Legal Issues relating to “Manipulation” of Client PC with JavaScript

Masako Wakae[†1]　Ryoji Mori[†2]　Hideki Yoshii[†3]

Abstract: This paper discusses collection and distribution of large amounts of personal data through rapidly evolving ad technology. These data do not fall on the category of “personal information” as defined in the Act on the Protection of Personal Information, but as a result of transfer between business entities, these data may change to the personal information. While data subjects are not aware of such collection and distribution, it is difficult for them to set up a protest. We will examine circumstances where business entities such as, Facebook and DMP operators use Java Script and consider how existing laws can address this situation as well as the potential legal liability of a website manager who set JavaScript in his website.

Keywords: JavaScript、cookie、Facebook、DMP、Act on the Protection of Personal Information

1. はじめに

2018 年春、コインマイナーと呼ばれる手法で、ウェブサイト訪問者に仮想通貨のマイニングを手伝わせていたサイト運営者が不正指令電磁的記録（ウイルス）供用などの容疑で相次いで摘発された。訪問者のパソコンに計算作業をさせる JavaScript がウイルスにあたると判断されたものとみられるが、この事件は少なからぬ衝撃をもって受け止められた。これまで、サイト開設者が訪問者のブラウザに JavaScript を実行することは許容されると解され、様々な用途で使われてきたからだ。「Web サイトは『サイト開設者の庭』であり、『庭を見に行ったところ不愉快になった』のなら、『戻る』ボタンを押してその庭から離脱すればよいのである」aとして、コインマイナー用 JavaScript の設置者を擁護する声もあった。だが、一般的なユーザーの目線に立てば、気づかないうちにブラウザに様々な指示を与えられることに納得がいかないというのも事実であろう。

この事件で想起されたのは、現在、オンライン広告の世界でユーザー情報の収集に広範に用いられている JavaScript と何が違うのか、仮にコインマイナー用の JavaScript が違法であるならば広告用の JavaScript も違法になるのではないか、という点ではないか。刑法のウイルスの定義は、「正当な理由がないのに」他人のパソコンに「意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき」「不正な指令を与える」ものだが、このうち「意図に反する動作をさせる」という点では広告用 JavaScript は十分に当てはまるだろう。コインマイナーの場合、サイト訪問者がそのサイトを離れればそれ以降、影響を与えることはできないが、広告配信用に訪問者の情報を取得する JavaScript の場合、そのサイトから離脱した後も、取得されたデータは訪問者の意図と関係なく流通するのであるから、よりタチが悪いともいえる。しかも、こうした広告用 JavaScript は後述する手法により、サイト開設者さえ想定しない多数の外部事業者からの実行も可能にしているのである。『サイト開設者の庭』であったはずのウェブサイトはもはや、訪問者はもとより、時には開設者さえも気づかぬ間に、第三者に様々なことをさせられる状況にある。

オンライン広告が急成長を遂げる中、私たちはネットを利用する度に趣味嗜好や性別、年齢、居住地、年収などのデータを集められているが、それらがどんな事業者に取得され、誰に渡され、どう活用されているかを把握し、コントロールすることはほぼ不可能となっている。背景には様々な要因があると思われるが、本論文では、「入り口」において取得されるデータの形態が、ブラウザや端末を識別

†1 情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY
†2 英知法律事務所
EICHI LAW OFFICES,LPC.
†3 ソフトバンク株式会社
SoftBank Group Corp.

1.1.1 a 高木浩光@自宅の日記「懸念されていた濫用がついに始まった刑法 19 章の 2「不正指令電磁的記録に関する罪」（2018 年 6 月 10 日）

する端末識別子bに紐付くものであり、その結果、我が国の個人情報の保護に関する法律（以下、「個人情報保護法」。）の規制対象外として流通している点に着目した。端末識別子に紐付いた情報は、それらのみでは個人識別性がないが、提供先が保有する情報と突合された場合に個人情報に変わり得る性質のものである。だが、提供元では個人識別性を有さない情報が、第三者に提供され、その結果、提供先で個人識別性を有する情報となった場合、第三者提供の規制を受けるかどうかといった問題は、必ずしも明確な整理がなされていないのが実情である。そこで、本論文は、端末識別子に紐付いた情報が広告ネットワークの中で個人情報に変わっている実態を明らかにした上で、こうした情報の流通について現行法により規制が可能かという点の検討を試みる。ことに、JavaScript などを駆使した広告技術が、当事者の想定を超える情報流通を可能にした点に注目し、JavaScript 設置者の法的責任についても検証したい。

2. 関連研究

クッキー等の端末識別子に紐づいた個人に関する情報を個人情報保護法で保護対象とすべきかどうかについては、同法の平成 27 年改正の検討段階で IT 総合戦略本部の有識者会議「パーソナルデータに関する検討会」の「技術検討ワーキンググループ」が報告書cをまとめている。ここでは、端末識別子に紐付いた情報を「識別非特定情報（それが誰か一人の情報であることが分かるが、その一人が誰であるかまでは分からない情報）」に分類し、他の情報との突き合わせ等により個人情報となり、「広く情報が拡散してしまった後に個人が特定され、何らかの個人の権利利益が侵害されるような事態が生じる」可能性を指摘していた。

スマートフォンについても、総務省の有識者会議が、アプリのインストールによって、端末識別子に紐尽く様々な情報がアプリ提供者のみならず、広告事業者にも送信されている実態を検証し、プライバシーポリシーなどによる利用者への告知が必要であると指摘しているd。

3. 広告事業者によるウェブ行動履歴の収集

3.1 アドテクノロジーの変遷

世界で最初のオンライン広告は 1994 年 10 月 27 日、Wired 誌のデジタル版「Hot Wired」に掲載された AT&T 社のバナー広告だったとされるe。日本での登場は 1996 年、「Yahoo！JAPAN」への掲載が最初であるf。当初は、媒体社が広告主側から広告を受け取ると、媒体社が自社のウェブページにそのまま掲載する「ベタ貼り方式」だったが、次第に広告枠を外部化し、「アドサーバ」で広告配信や管理を行う方式に移行していく。これは、媒体のウェブコンテンツを送り出すウェブサーバとは別に、外部に置かれたアドサーバから広告だけを配信する仕組みである。広告配信がウェブサイトのアクセスから切り離されることで、柔軟な運用が可能となり、配信可能数や配信期間の管理、どの広告が何回表示されて何回クリックされたかという効果測定などの技術も進んでいったg。当初はアドサーバの管理者は媒体社が主であったが、広告会社など第三者がアドサーバを管理する「第三者配信」の仕組みが主流となっていくと、運営母体の異なる様々なサイトの広告をアドサーバでネットワーク化する「アドネットワーク」が形成されていくようになる。アドサーバを管理する広告会社がサイト横断的に広告の受注を請け負うことができるようになっただけでなく、ユーザーの行動を複数の媒体にわたって追跡し、データ取得することも可能になっていった。このほか、媒体社などのサプライ側と、広告主などのデマンド側をつなぐ広告市場「アドエクスチェンジ」も登場、広告主側や媒体社側がインプレッションごとに必要な在庫を巡って瞬時に入札を成立させることも可能になっていく。

こうした動きのなかで存在感を増していったのが、ユーザーの閲覧履歴や購買履歴、デモグラフィック情報（性別、年齢、居住地域、所得、職業、家族構成など）などである。ユーザーのデータを事業者間で交換するデータエクスチェンジという仕組みも登場。DMP（Data Management Platform）とよばれる、ユーザーデータの収集・蓄積・統合・分析を行うプラットフォームも現れ、企業が自社で蓄積したデータを活用するために用いるタイプのほか、第三者から集めたデータを統合して第三者に提供するタイプも存在する。

3.2. JavaScript を駆使した ID 統合

では、こうしたユーザーデータは、具体的にどのように集められ、事業者間をどう流通するのか。現在の主流は、JavaScript とクッキーを活用したものである。

クッキーとは、ウェブサイトの提供者が、閲覧者のコンピューターにブラウザを介して一時的に書き込むデータで、閲覧者の識別や認証のために使われる。例えば、ユーザーがウェブサイト A を閲覧した際、A のサーバはユーザーのブラウザに対してクッキーを送りつける。二度目以降に A を閲覧する際、ブラウザはこのクッキーを送り返すため、A のサーバは同じ閲覧者が訪問したことを確認できる。こ

b総務省の「利用者視点を踏まえた ICT サービスに係る諸問題に関する研究会・スマートフォンを経由した利用者情報の取扱いに関するＷＧ」の報告書「スマートフォン・プライバシー・イニシアティブ」（2012 年 8 月 http://www.soumu.go.jp/main_content/000171225.pdf）では、利用者の識別に係る情報として、契約者・端末固有 ID（Android ID、UDID、IMSI、IMEI、MAC アドレス等）に加え、クッキー技術を用いて生成された識別情報も含めており、本論文ではこれらを端末識別子として論じる

c 技術検討ワーキンググループ報告書（2014 年 12 月）
http://www.kantei.go.jp/jp/singi/it2/pd/dai10/siryou1-2.pdf

d総務省スマートフォン アプリケーション プライバシーポリシー普及・検証推進タスクフォース「スマートフォン・プライバシー・アウトルック Ⅰ~Ⅳ」（2014 年~2017 年）
http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/smartphone_privacy.html

e DEGIDAY（2017 年 11 月 27 日）
https://digiday.jp/publishers/history-of-the-banner-ad/

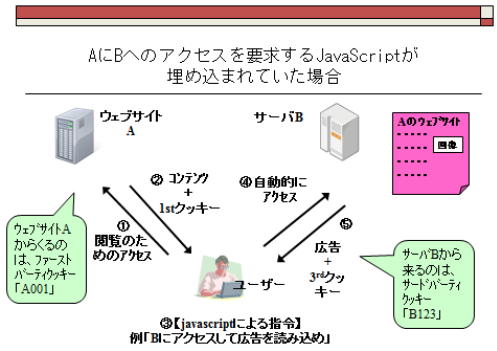
f 広瀬信輔「アドテクノロジーの教科書」（翔泳社）

g 日本インタラクティブ広告協会「インターネット広告の基本実務 2016 年度版」

れはユーザーの訪問したウェブサイトが発行した「ファーストパーティクッキー」で、クッキーの発行元ドメインは、訪問サイトのドメインと一致する。

これに対し、ユーザーが訪問したウェブサイト以外の事業者が発行するクッキーを「サードパーティクッキー」と呼ぶ。例えば、ウェブサイトAと広告事業者Bとが提携し、Aを訪れたユーザーのブラウザに対し、Bのサーバにアクセスするよう指示を与えると、このユーザーのブラウザはBのサーバにアクセスする。するとBのサーバもこのユーザーにクッキーを発行する。これがサードパーティクッキーで、ユーザーはアクセスしたつもりのないBから、ブラウザを識別される状態になる（図1）。

図1. サードパーティクッキー発行の仕組み



この時、Bはリファラhの参照などによって、このユーザーがサイトAからの訪問者であることが分かる。もし、Bが、サイトAばかりでなく、サイトCやDやEなどとも同様に提携していれば、Bはユーザーが CやDやEを閲覧したことも把握できる。Bが多くのサイトと提携すればするほど、ユーザーのウェブ上の様々な行動履歴がクッキーを介して統合されていくことになる。

こうしたサードパーティによるユーザーの「名寄せ」には、かつては画像タグが多用されたが、最近は JavaScript の使用が主流となっている。JavaScript を使うことにより、サーバからブラウザに対して指示できることの内容は拡大し、単なるアクセス要求だけでなく、より広範な情報収集が可能になった点が注目される。例えば、ポインタの位置やクリックの有無、入力内容などの情報を送信させることで、ニュースサイトでどんな記事をどのくらいの時間をかけて読んだのか、何をクリックし、どんな文字列を入力し、何を購入したのか、といった情報を得ることも可能である。

さらに状況を複雑にしているのが、サーバ側でブラウザに対し指示ができるという JavaScript の特性を使った JavaScript の「入れ子構造」である。サイト運営者が、広告会社などと提携して閲覧者をその広告会社のサーバにアクセスさせる JavaScript を設置する際、その広告会社のサーバに、新たに別の広告会社などへのアクセスを指示する JavaScript を設置するといった手法で、「ピギーバック」などと呼ばれるi。結果として、サイト運営者にすれば設置を許可した覚えのない第三者のサーバにも、閲覧者のブラウザへの JavaScript 実行を許し、各種情報を送信させることになる。例えば、タレントのコマーシャル起用で知られる大手スポーツジム運営会社の場合、2018 年 5 月の調査時点でサイト閲覧すると閲覧者のブラウザは 86 の広告会社や解析会社などにアクセスし、情報を送信することとなっていたがj、筆者らがこのジム運営会社にたずねたところ、把握していたのは代理店 1 社に依頼した 6 事業者の 11 の JavaScript のみであり、残る 75 の情報送信先については気づいていなかった。

このように多数のサードパーティクッキーに紐づけられたユーザーの情報は現在、広告事業者の間で広く共有されるようになっている。「クッキーシンク」と呼ばれる手法で、それぞれ管理しているクッキーを同期させ、ブラウザ識別のための ID を連携させることで、それぞれの保有するユーザーのデータを拡大しているのである。

4. クッキーデータが個人情報に変わるケース

4．1．FBの「いいね！」ボタン問題

これまで述べてきたユーザーのウェブ行動履歴の収集は、収集対象がブラウザを識別するクッキーに紐付いた情報であり、特定の個人を識別しないと考えられてきた。このため、個人情報保護法の規制対象外であるとして法的に許容されてきたといえよう。しかし、非個人情報であっても、個人情報を保有する事業者の下で他の情報と統合されれば、個人情報に変わり得る。その典型的な例が FB の「いいね!ボタン」などソーシャルプラグインを巡る問題である。

「いいね！ボタン」は、FB 上で会員が投稿に肯定的な意志を示すために使われるだけでなく、FB 以外のウェブサイトにも設置できるソーシャルプラグインである。サイトの訪問者が、そのコンテンツに関心を抱いたときにクリックすれば、その回数がカウントされるため、サイト開設者がユーザーの関心度を把握するのに活用される。一方、クリックした訪問者は、そのコンテンツを FB の友達と共有したり、コンテンツの更新情報を受けたりすることができる。その利便性の高さから広く普及し、データ解析会社「データサイン」の調査では 2018 年 1 月現在、国内約 18 万サイト中、3 万 1252 サイトで設置が確認されたk。また、国内売上高トップ 100 の上場企業lでは 2018 年 2 月現在、半数以上が設置m、公的機関では首相官邸、外務省、財務省、

h ブラウザがサーバに送信する、リンク元サイトの URL のこと。

i ScaleOut「piggyback を勉強してみる」
http://www.scaleout.jp/26905/
j データサイン社プライバシーポリシー調査（2018 年 5 月）
k データサイン Web サービス調査レポート（2018 年 1 月）
https://datasign.jp/blog/datasign-report-docodoco-20180626/
l 日経新聞売上高ランキング（2018 年 1 月 22 日現在）
https://www.nikkei.com/markets/ranking/page/%3Fbd%3Duriage
m 読売新聞「「いいね！」ボタン設置サイト　閲覧だけで「個人情報」送信　保護法抵触か」（2018 年 2 月 25 日）

警察庁、農水省、陸、海、空自衛隊などが設置していたn。

しかし、「いいね！ボタン」の実態は、前述した JavaScript によるサードパーティクッキーの収集と同様のものである。サイト運営者が、自らのサイトのウェブ文書に、FB が公開している「いいね！ボタン」用の JavaScript を設置することによって、サイト閲覧者のブラウザに紐付いた情報を、FB に送信させるものである。「ボタン」という名称から、閲覧者はボタンをクリックした場合にのみ何らかの情報が FB に送信されると想像しがちであるが、実際には、クリックの有無に関係なく、閲覧しただけで自らのブラウザに紐尽く情報を FB に送信しているのである。

しかも、実名登録による利用を原則としている FB の場合、FB は会員の個人情報を保有している。このため、サイト訪問者が FB の ID を持っており FB にログインした状態にある場合、FB 側は、そのブラウザに発行したクッキーから、どの会員のブラウザであるか照合することが可能となる。たとえ、この時点でログインしていなくても、次回に FB を利用する際、この訪問者がクッキーを消去しない限り、過去の訪問履歴と照合することが可能となる。このような仕組みから、閲覧ブラウザが FB に送信する情報は非個人情報のクッキーデータであるが、FB が取得する時点で FB 利用者分については個人情報になると解される。

FB によれば、国内の有効ユーザー数は 2017 年 9 月時点で 2,800 万人oおり、前述の通り、国内の多数のサイトが「いいね！ボタン」を設置していることを考えると、膨大な個人の閲覧履歴が FB に集積されていることになる。

問題と思われるのは、以下のような点である。

第一に、利用者への周知の問題である。一般の利用者には、FB と資本関係がないなど一見無関係と思われる企業等のサイトを閲覧しただけで、クリックもしていないのに、FB に閲覧情報が送られるとは予想しないであろう。2018 年 3 月時点で、FB の国内広報担当は「FB のソーシャルプラグインが設置されたサイトを会員が閲覧した場合に送信される情報は、個人情報として扱っており、プライバシーポリシーでも説明している」と回答した。FB のサイト上には「サービス(いいね！ボタン、Facebook ログイン、広告、効果測定など)を利用した外部ウェブサイトや外部アプリを利用者が閲覧または使用したとき、弊社はその情報を収集します。これには利用者がアクセスしたウェブサイトやアプリ、それらのウェブサイトやアプリ内でのサービスの利用状況に関する情報、またアプリやウェブサイトの開発者や発行元が利用者や弊社に提供する情報が含まれます」と記載していたpが、具体的にどのような情報が収集されるのかはっきりせず、また、「いいね！ボタン」がどのウェブサイトに設置されているのかも書かれていなかった。そして、「いいね！ボタン」を設置しているサイト運営者が、プライバシーポリシーで FB への情報送信を説明しているケースは国内売上高トップ 100 の調査時点で皆無だったq。

第二に、利用者がこのような方法による収集を拒否することがほぼ不可能な点である。前述のように、利用者にはどのサイトに「いいね！ボタン」が設置されているか事前に分からず、閲覧によってボタン設置に気づいた時には、もう FB に閲覧情報は提供された後である。また、ＦＢに送信されたくないと考えた場合でも、オプトアウトなど事後的に拒否する仕組みもこの時点で用意されていなかった。

第三に、FB は「いいね！ボタン」などの設置基準を定めておらず、収集情報の機微性についての配慮に欠ける点である。設置サイトの中には、アダルトサイトなど閲覧の事実を他人に知られたくないと考えるようなサイトや、自分や家族が特定の病気にかかっていることを推測させるような医療情報サイトなども含まれていたr。

このような情報収集の法的評価については、プライバシー侵害と個人情報保護法の両面から検討すべきである。まず、プライバシー侵害にあたるかどうかについては、取得型のプライバシー侵害に関する裁判例が参考になるだろう。

警察による車両ナンバープレート読み取りシステム「N システム」に関する裁判例（東京地判平成 13 年 2 月 6 日）sは、プライバシー侵害 に関する適法性の判断基準として、取得、保有、利用される情報が①個人の思想、信条、品行等に関わるか、などの情報の性質、②取得の目的が正当か、③取得の方法が正当か、などを総合的に判断すべきとしている。この事案では、裁判所は N システムによる権利侵害は認められないと結論づけたが、「仮に、N システムの端末が道路上の至る所に張りめぐらされ、そこから得られる大量の情報が集積、保存されるような事態が生じれば、運転者の行動や私生活の内容を相当程度詳細に推測し得る情報となり（略）目的や方法の如何を一切問わず収集の許される情報とはいえないことも明らかである」などとして、網羅的な情報収集が権利侵害となる場合があることを正面から認めている。

N システム事件で裁判所が使用した基準を本件にあてはめてみれば、以下のようになるであろう。①の情報の性質については、ウェブの閲覧履歴であり、一般に個人の思想、信条、品行等を推知しうるものであるうえ、「いいね！ボタン」の設置基準が定められていないためアダルトサイト閲覧などの履歴も収集されてしまう。②は、広告目的であり、人の生命、身体、財産の保護を目的とする防犯等に比べればその重要性は一段落ちるものである。さらに、③の方法

n 前掲注 m

o フェイスブックジャパン 2017 年 9 月 14 日発表

p この時点で、FB の「データに関するポリシー」のページの中の「Facebook が収集する情報の種類」の 6 番目のカテゴリ「Facebook サービスを使用するウェブサイトやアプリからの情報」に記載されていた

q 前掲注 m

rr 前掲注 m

s東京地裁平成一〇年（ワ）第五二七二号　損害賠償請求事件
http://www.translan.com/jucc/precedent-2001-02-06.html

については、前記のとおり、(a)「いいね！ボタン」の設置されたウェブサイトを閲覧しただけで閲覧履歴が収集されることはユーザーにとって不意打ちの恐れがあること、(b)オプトアウトが認められていないこと、などから取得方法の正当性に疑問がある。以上の点から、FB による情報収集がプライバシー侵害にあたると判断される可能性は十分にあるというべきである。

次に、個人情報保護法の規定については以下のとおりである。本件についての見方として、理論的には①FB を個人情報の取得の主体とし、ボタン設置サイトを FB から取得の委託を受けたものとする見方と、②ボタン設置サイトが一旦、個人情報を取得し、後に FB にその情報を提供した、とみる見方があり得るが、まず、①について考えたい。

①のケースでは「個人情報取扱事業者は、偽りその他不正の手段により個人情報を取得してはならない」と定める第 17 条に抵触する可能性が考えられる。

「いいね！ボタン」はその形状や名称から、あたかも、閲覧者がクリックした場合にのみ何らかの動きが起きると想像させるが、実際にはクリックの有無にかかわりなく、閲覧した瞬間に、FB 会員の個人情報を FB に取得される形となっている。これが多くの一般人の予想を裏切るものであることは、閲覧者はもとより、ボタンを設置するサイト運営者の多くが、閲覧するだけで情報が送信されると認識していなかったことからも明らかである。例えば、ある大手自動車メーカーは、報道の取材に対して、「商品の宣伝になると思って設置しただけで、まさか閲覧するだけで情報送信させる仕組みとは思わなかった」と回答しているt。

しかし、個人情報の取得者は FB であるとした場合でも、取得の「入り口」となるボタン設置サイトの運営者に法的責任はないのであろうか。この構図は、スマートフォンでアプリを使用した際、アプリ提供事業者がアプリに組み込んだ広告会社などの情報収集モジュールによって、利用者のデータが広告会社などの第三者に送信されるケースと似ており、総務省の有識者会議の報告書「スマートフォン・プライバシー・イニシアティブ」uが参考になる。

報告書は「情報収集モジュール提供者は、一般に利用者に対する接点を直接持っておらず、利用者側も何の情報収集モジュールが入っているか等の情報を提供されない限り知り得ず、情報収集モジュール提供者のウェブページを参照する等の措置もできない。（中略）このため、詳細は情報収集モジュール提供者が掲載するプライバシーポリシー等を通知又は公表し説明する必要があるものの、アプリケーション提供者のプライバシーポリシーにおいて情報収集モジュール別に最低限必要な情報を利用者に通知又は公表するなど、アプリケーション提供者と情報収集モジュール提供者の間の役割分担により透明性を高めることが現実的かつ必要ではないかとの指摘がある」vとする。さらに、「アプリケーション提供者が本人に対して適切な説明をしていないことを知りつつまたはそのことを知るべくして必要な対策を講じることなく、情報収集モジュールを配布し、結果として、本人の認識なくアプリケーションから情報を取得することは、第 17 条の違反となる可能性があると指摘される」wとも記載している。

アプリケーション提供者を「いいね！ボタン」設置サイトに、情報モジュール提供者を FB に、それぞれ当てはめて考えた場合、利用者にわかりやすい通知をすることなしに「いいね！ボタン」を設置することは、FB のみならず、「いいね！ボタン」の設置サイトの事業者も個人情報保護法 17 条違反に該当する可能性があることが示唆される。

個人情報保護委員会は、新聞紙上で「いいね！ボタン」の問題が報じられたxことを受け、委員会ホームページ上で注意喚起を掲載yし、ボタン設置のサイト運営者に対し、①閲覧するだけで利用者のブラウザ等の情報が送信されてしまうこと、②送信先事業者の保有情報によっては個人情報にあたる可能性があること、などを理解するよう求め、それでも設置する場合にはプライバシーポリシーに分かりやすく記載するよう注意喚起したが、これは前述の SPI の見解と同趣旨のものと思われる。

一方、このような、FB を情報取得の主体、ボタン設置サイト運営者を FB から情報取得を委託された者、とみる考え方は利用者の立場に立つと分かりにくいという問題がある。利用者が能動的にアクセスしているのは、あくまでボタン設置サイトであり、ブラウザが裏で FB のサーバにもアクセスしていることに気づくのは難しい。利用者にすれば、実質的には、ボタン設置サイト運営者に情報を取得され、ボタン設置サイトから第三者である FB に提供されたと考える方が自然であるとの見方もある。この場合の法的問題については６．において後述する。

４．2. DMP 事業者のデータ提供を巡る問題

前述の通り、DMP と呼ばれるプラットフォームでは、様々な事業者から集めたクッキーや広告 ID、または DMP 事業者が発行した ID に紐尽くユーザーデータを集め、統合、分析し、さらには外部に提供している。そのデータ量は膨大で、国内のパブリック DMP 最大手「インティメート・マージャー」の場合、4. 7 億ブラウザの情報を保有しているとうたっているz 。こうして集められたデータは、性別、年齢、職業、家族構成、居住地区、趣味、興味など

t 前掲注 m
u前掲注 b

v前掲注 b　49 頁
w前掲注 b　50 頁脚注 17
x 読売新聞「「いいね！」ボタン設置サイト　閲覧だけで「個人情報」送信保護法抵触か」(2018 年 2 月 25 日)、「ネット広告　閲覧者の情報収集　「端末」「個人」危うい結合」(同 3 月 2 日)
y 個人情報保護委員会「SNS の「ボタン」等の設置に係る留意事項」
https://www.ppc.go.jp/news/careful_information/sns_button/
z インティメート・マージャーのニュースリリース（2018 年１月２５日）
https://corp.intimatemerger.com/archives/2041/

多岐にわたって分類され、例えば趣味も、単に「スポーツ」でなく、ゴルフ、テニス、登山など詳細に区分され、例えば、インティメート・マージャーの場合、5000 を超えるセグメントで区分しているというaa

これらのデータは、クッキーなどの識別子に紐付いた情報であり、それ自体は個人情報ではないとしても、顧客情報を保有する事業者に提供され、顧客情報と突合させれば個人情報に変わりうるものであることは、これまで述べてきた通りである。顧客から見れば、DMP 事業者からの情報提供によって、その企業に直接提供した訳ではない個人情報を拡張されてしまうことになる。そして実際に、「顧客情報の拡張」をうたい文句として、ユーザー企業への営業を展開している DMP 事業者もいる。

例えば、DMP 事業者トレジャーデータのウェブサイト上では、データ活用のための同社のツールを導入した国内大手の飲料メーカー、キリンの事例として以下のような紹介をしているbb 。

「そこで今年から導入したのが、トレジャーデータが提供するデータマーケティング基盤『TREASURE CDP』だ。TREASURE CDP は、オウンドメディアのアクセスログ、広告配信ログ、CRM のコミュニケーションログなど企業が保有する顧客データだけでなく、セカンドパーティ・サードパーティの DMP が提供するオーディエンスデータを収集・統合管理してデジタルマーケティングのパーソナライズを可能にする。外部データを自社の顧客データと統合することで、顧客の姿をより鮮明にしようと考えたのだ」「他のデータとのマッチングがしやすくなることで、顧客のことをどんどん深堀して理解できるようになります」cc

DMP 事業者が、クッキーなどの識別子に紐尽く情報を、個人情報を保有する企業に対して提供し、提供先企業の中で識別子を同期させることで個人情報を拡張しているとすれば、意図しない形で自分の情報を提供される個人にとって、プライバシー侵害の恐れがあるというべきであろう。

先ほどは、取得型のプライバシー侵害について検討したが、プライバシー侵害の事案の多くは提供型であり、提供型について裁判例の多くは、①一般人の感受性を基準にして当該私人の立場に立った場合公開を欲しないであろうと認められる事柄を提供・公開される場合にプライバシー侵害を認めている。ただし、②その情報が誰の情報か分からない匿名情報である場合には、プライバシー侵害にはあたらないとする事例が散見される。

DMP 事業者の提供する属性データは、詳細なウェブの閲覧履歴に基づくもので、本人の趣味・嗜好、生活様式に加えて思想・信条にかかわるものまで含みうるものであるため、①のケースに該当する事柄であるといえよう。さらに、②について検討すると、提供先の企業においては、提供された情報がどの会員のものか特定できてしまう性質のものであるため匿名情報ではない。従って、DMP 事業者による属性データの提供は、それが提供先で個人情報となる場合、プライバシー侵害と評価される可能性がある。

サードパーティクッキーを利用した情報収集には、かねてプライバシーの問題があるとされながらも、それが匿名状態での収集であることから、個人情報保護法に抵触せずプライバシー侵害にも当たらないとして許容されてきた面がある。しかし、収集された情報を意図的に個人情報と結合・突合するならば、その行為は、許容されてきた一線を越えるものであるように思われる。個人情報保護法上の評価については、６．において後述する。

・５．海外の規制

欧州連合（EU）では 2018 年 5 月 25 日、GDPR（General Data Protection Rules・一般データ保護規則）が施行されたdd。EU ではこれまで、1995 年に制定されたデータ保護指令の下で各国が国内法を制定してきたが、GDPR は EU 単一のルールとして加盟国に直接に適用される。

GDPR ではこれまでより事業者に対する制裁が強化され、データポータビリティの権利や忘れられる権利なども新たに盛り込まれたが、保護すべきデータの定義は従前通りである。個人データは「識別された、または識別され得る自然人（「データ主体」）に関するすべての情報」と定義され、例えば、「自然人の氏名」や「識別番号」「所在地データ」などのほか、「メールアドレス」「オンライン識別子（IP アドレス、クッキー識別子）」なども含まれる。

個人データの取得や第三者提供などは、個人データを取り扱う行為はすべて「処理」と定義され、処理が適法となる場合は限定列挙されている。データ主体の同意がある場合のほか、「正当な利益」のために処理が必要な場合にも処理が適法となる。「正当な利益」の中には「ダイレクトマーケティングのための処理」も含まれるとされており、広告配信のための収集が適法とされるかどうかは今後の動向に注視する必要がある。

GDPR とは別に、現行の「e プライバシー指令」（e Privacy Directive）に代わる「e プライバシー規則」（e Privacy Regulation）が成立間近とされている。通信当事者のデータを保護するために取扱事業者を規制するもので、成立すれば、現行の指令が対象としている通信会社のほか、FB や WhatsApp、Skype など、ネット上のメッセージや音声のサービス提供事業者にも適用されることになる。特にサードパーティクッキー等を使った情報の取得や提供を含めて利

aa インティメート・マージャーのニュースリリース（2016 年 4 月 14 日）
https://corp.intimatemerger.com/archives/1855/
bb トレジャーデータのサイト　事例・顧客「キリン」
https://www.treasuredata.co.jp/customers/kirin/
cc キリンは 2018 年 7 月時点での質問に対し、拡張したデータの管理方法については詳細を明かさなかった。

dd 個人情報保護委員会　日本語仮訳
前文 https://www.ppc.go.jp/files/pdf/gdpr-preface-ja.pdf
条文 https://www.ppc.go.jp/files/pdf/gdpr-provisions-ja.pdf

用者の事前同意を義務づけ、オプトアウトは認めず、違反すれば制裁金が課されることになる見通しである[ee]。

2015 年 11 月には、ベルギーの情報保護当局（the Commission for the protection of privacy (CPP)・現 the Data Protection Authority（DPA））が FB を相手取って起こした訴訟で、ベルギーの裁判所は FB が「いいね！ボタン」を設置した外部サイトでの閲覧履歴を追跡し、FB 利用者以外のユーザーも含めて閲覧履歴を追跡していたことについて、ベルギーの情報保護法に違反しているとの判断を示した[ff]。FB が登録情報を持たない FB 利用者以外の閲覧履歴は、日本の個人情報保護法では個人情報には該当しないが、ベルギーの裁判所はクッキーなどのオンライン識別子も保護すべきとして、このような判断を示したと考えられる。

一方、米国では米国連邦取引委員会（FTC）が 2010 年、ウェブ上のトラッキングを拒否する「Do Not Track」の仕組みをブラウザの機能の一部として追加するよう勧告している。既にこの機能がデフォルトでオンになっているブラウザもあるものの、対応しないことをプライバシーポリシー等で宣言する運用も許容されている。2015 年 2 月に提案された「消費者プライバシー権利章典」では、個人データの定義に端末に結びつくデータも含むとし、具体例として端末 ID も列挙されたが、法制化の目途は立っていない。

・６．提供先で個人識別性を獲得する提供行為の評価

これまで述べてきたように、インターネット広告の世界では、非個人情報として取得された情報が、他の事業者に提供された結果、個人情報に変わるケースが想定される。DMP 事業者がオンライン識別子に紐づけられた情報を、顧客情報を保有する第三者に提供するケースが典型的である。また、FB の「いいね！ボタン」のケースについても、ボタン設置サイト運営事業者が取得した非個人情報を FB に提供した結果、個人情報に変わったとの見方もあり得る。

そこで、こうした状況に対する、個人情報保護法の第三者提供に関する規制の適用可能性について考えたい。

個人にかかわる情報が同法で保護対象としている個人情報に該当するかどうかは、原則として事業者ごとに相対的に判断されるものである[gg]。第三者提供の場面においては、提供元においては特定の個人を識別する情報であるが、提供先では特定の個人識別性はないという場合があるうる。例えば、A 社の「社員番号１２３４５」という情報は、社員名簿を保有する A 社にとっては、特定の個人を識別する情報であるが、これが B 社に提供されたとしても、個人識別性はない。この場合に、個人情報保護法 23 条の第三者提供にかかる規制の適用を受けるかについては、提供先において特定の個人が識別できる場合に限り適用されるべきであるとする「提供先基準説」も存在するが、現在は、提供元において特定の個人が識別される場合には、同規制が適用されるという「提供元基準説」が通説となっており[hh]、政府の国会答弁もこの立場を支持している[ii]。

しかし、前述のように、インターネット広告の世界でしばしば生じているのは「提供元において個人識別性がないが、提供先において個人識別性がある」（以下、この場合を「提供元×提供先○」とする。）というケースである。前記の提供先基準説、提供元基準説に関する議論は、「提供元において個人識別性があるが、提供先において個人識別性がない」（以下、この場合を「提供元○提供先×」とする。）というケースが議論の前提であり、「提供元×提供先○」というケースについては十分な検討がなされてこなかった。

そこで本稿では、「提供元×提供先○」のケースについても正面から検討することとし、さらには、「提供元○提供先×」という従来の議論の対象となったケースについても、提供元基準説に再考の余地がないか検討することとする。

まず、「提供元×提供先○」のケースについて、23 条を適用すべきかどうか。これについては、共同研究者間でも意見が分かれた。

「提供元×提供先○」のケースにおいても提供元基準を維持し、23 条を適用すべきでないとの立場は、提供元基準を一貫させる方が法的安定性に資することに加えて、提供先で個人情報となることについては、取得の規制（17 条（適正な取得）、18 条（取得に際しての利用目的の通知等））により対処すればいいことを理由とする。

これに対して、23 条を適用すべきとする立場の理由は以下のとおりである。すなわち、提供先において個人識別性がある場合にこそ、権利利益の侵害のおそれがあることを考えれば、「提供元×提供先○」のケースにおいては、23 条の規制を適用すべきである。提供元の提供行為こそが権利侵害の原因であるため[jj]提供先に対する取得規制のみの問題とすることは適当ではない。23 条適用に際して障害となるのは、通常、提供元からみて提供先における個人識別性があるか否かが明確でないということである。しかし、提供元において、提供する情報が提供先で個人識別性を獲得する蓋然性が高いことを認識しているのであれば、当該提供行為は、実質的に個人識別性のある情報の提供と同様

---

ee European Commission
https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation

ff Data Protection Authority
https://www.dataprotectionauthority.be/news/judgment-facebook-case

gg例外として個人識別符号、顔画像、氏名等は、すべての事業者との関係で個人情報である絶対的個人情報である。

hh森亮二, パーソナルデータの匿名化をめぐる議論（技術検討ワーキンググループ報告書）, ジュリスト, 2014 年 3 月号 No.1464,

ii 2015 年 5 月 28 日参議院内閣委員会（政府参考人向井治紀）「日本の個人情報の定義は、容易に照合できる、他のデータと合わせて個人が識別できるものというふうになっているところでございます。その際に、情報を移転する際に、容易に照合するのは情報の移転元か移転先かという議論がございます。日本の場合、これは情報の移転元で容易照合性があるということで解釈が統一されておりまして」

jj たとえば、3.2 で紹介したピギーバックのケースのように、一つのウェブサイトを閲覧したことにより、大量のサードパーティに閲覧履歴の提供がなされるような場合には、この問題は顕著である。

であると評価することが可能である。従って、「提供元×提供先○」のケースであっても、情報が提供先で個人識別性を獲得することを提供元があらかじめ知っている場合、または容易に知りうる場合には、個人識別性のある情報の提供と同様であると評価して、23 条を適用すべきであるkk。

一方、23 条との関係で後者の考え方、つまり提供先における権利利益の侵害のおそれを重視して、「提供元×提供先○」のケースにおいて提供元基準を否定する考え方を採る場合、従来の提供元基準説（これは「提供元○提供先×」のケースが前提である）についても、見直すべきかどうか、検証を試みる必要があるだろう。より具体的には、提供先では個人識別性がないことが明白な場合等については、23 条の適用除外にできないか、という点が問題となる。ここにおいても、通常、提供元からみて提供先における個人識別性があるか否かを知っているか、または容易に知りうるかという点が重要になると思われる。なぜなら、仮に提供元が、「提供先において、個人が識別される可能性は全くない」と合理的に判断できるのであれば、そのような提供は、実質的には権利利益の侵害のおそれを伴うものではないからである。

実のところ、この「提供先において個人識別性を獲得するか否か」という問題は、匿名加工情報の加工方法において議論されてきた問題である。匿名加工の中心的課題は、提供先において、個人識別性を持たないようなものに加工することである。我々が検討する「提供元基準説においても、提供先において個人識別性の可能性がない場合には、23 条の適用除外としてよいのではないか」という問題は、「どのような加工がなされれば匿名加工情報として、23 条の適用を受けないことになるか」という問題と、実質的には同一であると思われる。してみれば、提供元基準説を微妙に修正することは、匿名加工情報の制度との関係を複雑にするものであり、必ずしも適切な方向性ではないものと思われる。したがって、「提供元○提供先×」の場面における提供元基準説を修正する必要はないと考える。

以上をまとめると、「提供元×提供先○」のケースにおいては、情報が提供先で個人識別性を獲得することを、提供元が知り、また容易に知りうる場合には、23 条を適用すべきであるとする意見と、提供元基準を一貫し 23 条を適用すべきでないとする意見があった。また、「提供元○提供先×」のケースにおいては、従前どおりの提供元基準説を維持し、常に 23 条を適用すべきであるとの結論となった。

「提供元×提供先○」のケースにおける 23 条提供の適否については、共同研究者間において意見が分かれたものの、そもそもこのようなケースを実現可能とする端末識別子情報についての法的扱いを見直すべきことについては、意見の一致を見た。具体的には、端末識別子情報を個人情報に含めること、あるいは個人情報保護法の改正に関する議論の過程で提唱された「準個人情報ll」 のような個人情報に準じるものとして保護対象とすることなどが考えられる。

技術が大きく進展する中では、「氏名等と結びつけば個人情報で、そうでないものは個人情報でない」とするこれまでの整理には限界が来ている。平成２７年改正法で新たに個人情報の概念として加えられた個人識別符号は、氏名等に結びつくかとは無関係に、一意性を有するか、簡単に変更することができないか、本人に連絡できるか等の要素を基準に一定の符号が個人情報でありうることを確認したものである。端末識別子も、これに加える方向で見直しをするべきではないだろうかmm 。

・７．おわりに

2016 年アメリカ大統領選では、ケンブリッジ・アナリティカによる FB のユーザー情報流用疑惑や、ロシアの工作員が出稿したとされる FB 広告による介入疑惑も浮上した。SNS を通じたデジタル・ゲリマンダー（SNS による世論操作を通じた投票行動への影響力行使をいうnn）はインターネット広告の世界でこそ、現実味を帯びたものといえよう。

端末の識別情報は、完全に個人を特定する情報とはいえないが、一人が 1 台の端末を常時携帯するような状況下では、個人を特定する情報とほぼ同一のものと考えても差し支えないだろう。加えて、例えば、対面販売では購入しにくいような商品もオンライン上では購入しやすいなど、思想信条のような個人の人格にかかわるきわめてセンシティブな個人情報が端末識別情報に紐づけられる可能性も高いといってよい。また、政治的扇動などを行う上で、その対象がどこの誰なのかを知る必要は必ずしもなく、個人の使用端末に働きかければ効果を発揮することを考えれば、端末識別子の重要性はますます高まるといえる。こうした現状に鑑み、端末識別情報の流通に対して、データ当事者である利用者本人が関与できる仕組みを作る必要がある。

参考文献

[1]一般社団法人日本インタラクティブ広告協会「インターネット広告の基本実務 2016 年度版」

[2]森亮二「インターネット広告に関する最近の法律問題」（国民生活研究、2016 年）

[3]広瀬信輔「アドテクノロジーの教科書」（翔泳社、2016 年）

kk 「いいね！」ボタン設置者による提供行為が認められるかについては、議論がありうるが、本人による追跡可能性を考えれば、提供行為を認めたうえで 23 条を適用することが適切であるとの立場もありうる。

ll 2014 年 4 月 16 日「第 7 回パーソナルデータ検討会資料」「（仮称）準個人情報」の新設について「特定個人を識別しないが、その取扱いによって本人に権利利益侵害がもたらされる可能性があるもの（技術検討 WG における「識別非特定情報」に含まれるもの）を新たに類型化し、これを定義することとしてはどうか」
http://www.kantei.go.jp/jp/singi/it2/pd/dai7/siryou1-2.pdf

mm 言うまでもなく、このような規制強化は、国内市場で活動する外国事業者に対して 75 条の域外適用規定等を用いた法執行が実効的に行われることを前提とする。端末識別子に紐づく国民の個人情報は、外国事業者によっても大量に取り扱われており、内外事業者間の公正競争の問題を別にしても、これらの外国事業者に対する法執行がなされなければ国民の権利利益の保護の実を上げることにはつながらないのである。

nn湯淺墾道「デジタル・ゲリマンダーの法規制の可能性」（情報処理学会）
http://www.ipsj.or.jp/event/fit/fit2017/FIT2017_program_web/data/html/event/eventA7_180.pdf