

日本におけるブラウザ”Do Not Track”の制度的可能性 Institutionalization of browser "Do Not Track" in Japan

加藤 弘則[†]
Hironori Kato

1. はじめに

本稿では特定のウェブブラウザで利用可能な”Do Not Track (DNT)”を制度化、あるいは業界内での導入形態に関する足並みを揃えることで達成される利便性やプライバシー配慮の可能性について論じる。

DNT とはウェブブラウザでサーバへアクセスした際に http ヘッダーにトラッキングを拒否する情報を付与し、サーバに伝える仕組みである¹。

DNT:0 #トラッキングを拒否
DNT:1 #トラッキングを許可

図 1 DNT のイメージ

これにより、ユーザがサーバにトラッキングの拒否を明示しなくとも、主に広告目的で利用されうる cookie 情報が付与された後のトラッキング拒否の意思を示すことが可能となる。また、DNT の設定情報はブラウザで行うため、DNT を設定した場合ユーザのポリシーとして常にサーバへトラッキング拒否の意思表示ができる。

DNT 以外のトラッキングを拒否する方法は、オプトアウト²が挙げられる。オプトアウトの場合、ユーザは訪問先のサーバ(サービス)ごとに対して、トラッキングの拒否を示すための設定を行う。しかしサービスごとにオプトアウトの方法や窓口が異なるため、プライバシーを気にかけるユーザにとって、手続きが煩雑になるといえる³。しかし、我が国においては DNT の制度や業界で統一された枠組みが存在しないため、ブラウザに DNT が実装されていても、それをサービスで生かせていないのが現状である。

日本のプライバシーに関する制度に目を向けると、個人情報保護に関する法律(以下、個人情報保護法)では、ウェブ広告における cookie 情報やウェブビーコンを中心としたユーザの行動情報は単体では個人情報に該当しない⁴。しかし、2011 年の JR 東日本の Suica データ騒動をはじめ⁴、法律における個人情報の定義外のデータであっても、安易な利活用が企業のレピュテーションリスクに繋がることを示す。

個人情報保護法は改正され、2017 年 5 月⁵に全面施行されるが、そこでもウェブの cookie 情報は単体で個人情報に含まれない。また、個人情報保護法の改正の背景には、ビッグデータの利活用を活性化させる国策が存在する。データ利活用の時代においては、制度を充実させることが、プライバシーに関する紛争リスクを低下させ、データ利活用を円滑に進めることに寄与するだろう。

広告で用いられるトラッキング技術をめぐっては、例えば米国では Facebook 社が提供するビーコン情報が過度なレコメンド広告に用いられたことに起因する訴訟など⁶、プライバシー問題のリスクを孕む。しかしその一方で、スマートフォンの普及により cookie 情報は日に日に増加し、莫大な利益をもたらすウェブ広告目的で利活用されやすい環境にある。

こうした状況においては、トラッキングを拒否するユーザの意見をサービス事業者により伝わりやすくすることが紛争を防ぐために肝要であろう。本稿では、第 2, 3 章でターゲティング広告の現況とプライバシー問題に触れ、第 4 章でターゲティング広告で用いられるサードパーティ cookie 情報と法解釈、第 5 章で DNT 技術の概要と現況を検討し、第 6 章でサードパーティ cookie 情報を用いたターゲティング広告のプライバシー問題を解決するための新たな DNT 技術の提案と、制度化について触れる。

2. ターゲティング広告

ターゲティング広告とは、対象の行動履歴をもとに、購買履歴や興味などを類推してインターネット広告を配信する手法である⁷。ターゲティング広告は主に、サービス内で集積されたログとファーストパーティ cookie 情報をもとにターゲティングを行う手法と、訪問先のサーバではないサーバによってブラウザに書き込まれるサードパーティ cookie 情報を通じてターゲティングを行う手法に二分される。

2.1 サービス内のログやサードパーティ cookie 情報を利用してターゲティングを行う場合

同一のサービス内に蓄積された特定の人物のログを分析することで、その人物の趣味嗜好が類推可能となり、ターゲティング広告の配信が可能となる。例えば、あるユーザが特定のニュースサイトを訪問し、そのサイト内での記事閲覧に関する回遊ログが存在する場合、それぞれの記事閲覧ログを分析することで「その人物がどういった内容のニュースに興味を持っているか」から趣味嗜好を明らかにする。また、ニュースサイトを運営する事業者が、EC サービスを提供している場合、実際に「お金を使った」購買ログとニュースの閲覧履歴を組み合わせることが可能になるため、多くの広告において重用視される CVR (Conversion Rate) の向上が期待できる。つまり、あるサービス内での行動ログを用いてターゲティング広告の配信を行う場合、単一のサービスを提供するウェブサービスよりも、ニュース、EC、コミュニケーション、ゲームなどの多岐にわたるサービスを提供するプラットフォーム事業者の方がより詳細かつ、収益につながりやすいターゲティング広告の展開が可能となる。

[†] 東京大学大学院総合文化研究科広域科学専攻基礎科学系

2.2 アドネットワークのログを利用してターゲティングを行う場合

あるサービス内でアドネットワークを介して展開される（バナーなどの）広告によって発生するサードパーティ cookie 情報によってターゲティング広告の配信が可能となる。ウェブサイト訪問時にアドネットワークによって配信される広告が表示されたりクリックされ、ユーザのブラウザがサードパーティ cookie 情報を許容している場合、利用者のブラウザにアドネットワークに関する cookie 情報が発生する。そのため、アドネットワークによって表示された広告を閲覧したユーザが、どのウェブサイトを訪れたのかを cookie 情報の突合によってアドネットワーク事業者は判別可能である。したがって、アドネットワーク事業者は、ユーザがどのようなサービスを普段利用し、広告をクリックしているか、を包括的に分析した上でターゲティング広告の配信が可能となる。したがって、Google や Facebook などの検索エンジンやプラットフォーム事業者、いいねボタンを始めとするサードパーティ cookie 情報を配信しやすいビジネスモデルを持つ事業者の場合、アドネットワークとして膨大なデータを集積可能とし、ターゲティング広告をより洗練させられる傾向にある。

3. ターゲティング広告とプライバシー問題

ターゲティング広告では、ユーザの趣味嗜好に合わせた内容が表示されるため、クリック数や CV（Conversion）数を向上させられる。その結果、CPM（Cost Per Mille）や eCPM（effective Cost Per Mille）などの広告単価を向上させる。また、ユーザにとって（興味がありそうで）有益な広告を表示させるため、ユーザの広告体験を高めるという UX の向上にも寄与すると言えよう。しかしその反面、ユーザの行動を取得して分析することから、プライバシー問題の発生とも表裏である。

3.1 ターゲティングをめぐるプライバシー問題の事例

過度なターゲティング手法を用いたターゲティング広告やその下地となりうるデータマイニングはプライバシー問題を発生させ、時にビジネスの障壁となるばかりか、企業の名誉を傷つけるレピュテーションリスクにもなりうる。

1999 年、アドネットワークサービスを提供する DoubleClick（現 Google）は EC サービスを展開する AbacusDirect 社の買収に関連し、自社が保有する cookie 情報 ID と AbacusDirect 社の購買履歴を突合させることを発表した。その結果、FTC（連邦取引委員回）の調査と集団訴訟へと発展し、同社は敗訴して株価が半減する事態となった⁸。

また、ターゲティング広告の背景には、無数の一見無価値な行動ログをもとに解析を行い、意味のあるデータを生み出すという、データ利活用の技術が存在する。そして、個人を特定できないと思われる行動ログ同士を突合することで個人が特定され、訴訟に発展した事例が見受けられる。2006 年、米 Netflix 社が同社内に蓄積された映画作品に関するレビューログを公開してレコメンド機能開発のコンテストを行った結果、その他のデータベースと突合することで数人の個人が特定される事態へと至った⁹。その結果、

Netflix 社は訴訟へと発展し、2009 年の和解の翌年にはアルゴリズムコンテストの中止が発表された。

このように、ターゲティング広告には、ビジネスそのものが行き過ぎてしまい社会から批判されることで起こる、未だのプライバシー侵害のレピュテーションリスクと、一見無価値な行動ログの利活用により個人が特定されることで起こるプライバシー侵害のレピュテーションリスクの二種類のリスクが付帯する。

3.2 オプトアウト

現在、ターゲティング広告のプライバシーに関する一般的な対応手法はオプトアウトである。オプトアウトでは、利用者が自己の意思をサービス側に伝え、トラッキングを拒否することが可能となる。例えば、バナー上からオプトアウトの URL に遷移することで、オプトアウトが可能となるが、オプトアウト情報は cookie 情報としてブラウザに蓄積される。したがって、cookie 情報を消去した場合や、ブラウザを変更した場合にはサイドのオプトアウトが必要となる。また、オプトアウトは各サービスごとに行う必要がある。

4. サードパーティ cookie 情報と個人情報保護法

サードパーティ cookie 情報は、単体の場合個人を特定できないため、個人情報ではない側面と、他の cookie 情報と cookie 情報 sync など、他のサードパーティ cookie 情報と突合することで個人を特定できる可能性があるため個人情報ともいえる両側面が存在する。個人情報保護法（改正前）においては、個人情報の定義が「生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別できるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む）」であり、サードパーティ cookie 情報はグレーゾーンのデータといえよう。しかし、個人情報保護法の改正によって、個人情報の定義は「該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他の知覚によっては認識することができない方式をいう。次項第二号において同じ。）で作られる記録をいう。第十八条第二項において同じ。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。以下同じ。）により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む）」という文言となった。したがって、サードパーティ cookie 情報に関しては、cookie sync によって特定の個人を識別できる可能性があるため、サードパーティ cookie 情報が法律上の個人情報にもなり得る。したがって、個人情報保護法の改正にあたっては、今後サードパーティ cookie 情報のプライバシーの側面に注目が集まる可能性があり（サードパーティ cookie 情報が個人情報か否かの議論が活発となりえる）、取り扱いと取得に関する意識をより強く向けることが肝要といえよう。

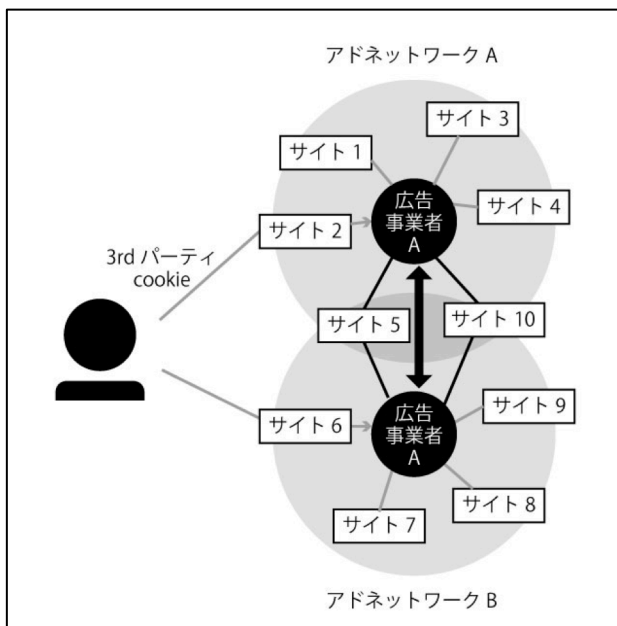


図 2 サードパーティ cookie 情報の cookie sync のイメージ

5. DNT をめぐる経緯と現況

DNT はブラウザを通して、自らの cookie 情報が利活用されることを拒否するメッセージを絶えず伝えることが可能となる。したがって、利活用を望まない人々がオプトアウトの仕組みに気付かず利活用がなされ、それが正当な手続きを経たとしても発生しうるプライバシー問題の紛争の発生リスクを低下させられる。しかしその反面、トラッキングを許可/拒否の二択しかなく、サービスごとにその意思を選択できない。

サードパーティ cookie 情報がプライバシーに関する紛争の火種となるリスクを低下させるためには、オプトアウトの仕組みをより明確にし、サードパーティ cookie 情報の利活用を望まない人々のデータを利活用しない制度作りが肝要である。

2007 年、米国の消費者団体が連邦取引委員会に対して、ウェブ上のトラッキングをコントロールする仕組みを要請した。それを受け、Christopher Soghoian, Sid Stamm, and Dan Kaminsky の 3 名が 2009 年に DNT 技術の開発に着手する¹⁰。その後、連邦取引委員会は、電話セールスを拒否する人々をリスト化した「National Do Not Call Registry」と似た形で、ウェブ上でのトラッキングを拒否する人々をリスト化する計画について言及し、2010 年には DNT 技術が発表された。現在は、W3C の Tracking Protection Working Group で技術の仕様が公開されている¹。

その後も連邦取引委員会は 2012 年に「Protecting Consumer Privacy in an Era of Rapid Change」というレポートを公表して、DNT を制度化する取り組みについて提案している¹¹。また、2013 年には、カリフォルニア州法 (CalOPPA) が改正され、ウェブ上のトラッキングについて、インターネット関連企業がどのように対応しているのかについて開示を求めた¹²。

制度が整う反面、2014 年には、ブラウザに DNT 設定が組み込まれた当初から採用していた米ヤフーが、DNT 設定の利用環境廃止を発表した¹³。米ヤフーは DNT を「効果的かつ利便性が高く、幅広く IT 企業に採用される基準ではない」と評し、「よりユーザーフレンドリーな方法を模索する」として、サービス内でのオプトアウトに移行した。

トラッキング許可/拒否の二択しか存在せず、サービスごとの細かな設定ができない DNT は、トラッキングによって生まれる利便性の可能性を排除しうる。「利便性」という言葉とともに DNT の利用環境の廃止を挙げた米ヤフーの方針は、トラッキングによって生じる利便性と真っ向に対立する DNT の側面が浮き彫りにする。

6. DNT に関する問題の所在と、制度化の可能性

消費者にとって、cookie 情報を用いたウェブ広告におけるトラッキングは、「プライバシーを侵害するもの」と捉えられる可能性がある。そのサイトを訪れたかの記憶が存在し得るかという点から、ファーストパーティ cookie 情報と比較してサードパーティ cookie 情報の方がターゲティングされた際にプライバシー侵害に関する意識が芽生えやすいといえよう。また、技術、法律（改正前の個人情報保護法）の両面から捉えた場合、cookie 情報に関しては個人情報にあたるか否かはグレーである。

ウェブサービス事業者やアドネットワーク事業者にとっては、cookie 情報の利活用がレピュテーションリスクをはらむ反面、収益源となりえ、また的確に消費者が望む情報を提供することで社会の利便性を高める側面も存在する。しかし、トラッキングによるプライバシー侵害のリスクが生まれるか否かと、利便性が向上するかはサービスと消費者の捉え方によって異なる。したがって、DNT によって一括でトラッキングを拒否した場合、適切なトラッキングによって得られるであろう利便性の向上まで損なわれてしまう。

消費者の心象によってあるトラッキングの評価が決定され、プライバシー侵害とみなされるか、という点については、そのトラッキングが起こるべくして起こったか、という理解に大きく左右されるといえよう。ファーストパーティ cookie 情報の場合、「そのサービスを利用したのだからアクセスログが残る、トラッキングされたかもしれない」という意識が働くのに対し、サードパーティ cookie 情報の場合は「どういう経緯でトラッキングされたのかわからない」というトラッキングされるに至った経緯が不明となりやすく、恐れや気持ち悪さに関する感情を生む土壌となりえる。そのため、トラッキングの拒否という点においては、cookie 情報がファーストパーティかサードパーティか、が重要な視点となる。

しかし現行の DNT については、ファーストパーティ cookie 情報とサードパーティ cookie 情報を問わずトラッキングを拒否する仕組みであるがゆえ、プライバシー意識に非常に敏感な消費者（原則型グループ^{14,15}）にとっては有用であったとしても、適宜プライバシーの侵害と利便性を天秤にかける「選択型グループ」にとっては、極端な仕組みとなりえる。「選択型グループ」にとっては、サービスごとのオプトアウトがプライバシーに配慮する有力な仕組みとなりえるが、例えばサードパーティ cookie 情報を利用す

るアドネットワークのトラッキングを拒否したい場合、アドネットワークごとにオプトアウト設定を行う必要が生じる。

また、DNT の仕組みに目を向けると、DNT はブラウザによって設定されるため、あくまでも消費者のトラッキングに関する意思をサーバに伝えるに過ぎない。したがって、その意思をトラッキングに反映するかどうかはサービス提供者側に任せられている。そのため、法制度などによる強制力が伴わない場合、トラッキングに関する意思が反映されない可能性もあるだろう。

以上を踏まえると、cookie 情報の種別ごとのトラッキング意思を示す DNT と、その制度化が考えられる。これにより、「原則型グループ」「選択型グループ」「解放グループ」の 3 パターンの消費者^{14,15}の意思を的確にサーバへ伝達することが可能となる。

DNT:00	#トラッキングを完全に拒否
DNT:01	#ファーストパーティ cookie 情報を用いたトラッキングのみを拒否
DNT:10	#サードパーティ cookie 情報を用いたトラッキングのみを拒否
DNT:11	#トラッキングを完全に許可

図 3 cookie の種別を考慮した DNT のイメージ

また、個人情報保護法の改正によって、サードパーティ cookie 情報が個人情報保護法における個人情報となった場合も、オプトアウトと同様に消費者の意思を反映でき、プライバシー問題に関する紛争のリスクを低下させられるだろう。また、cookie 情報種別による設定が可能な DNT によるトラッキングの意思表示をトラッキングに反映させるための制度化が実現した場合、現在はサービス提供者側に委ねられている、DNT による意思表示のサービス反映を強制することが可能となるだろう。

参考文献

- [1] W3C: Tracking Protection Working Group, 入手先 <https://www.w3.org/2011/tracking-protection/> (参照 2017-06-01) .
- [2] 生貝直人. "オンライン・プライバシーと自主規制-欧米における行動ターゲティング広告への対応-" 105-113 (2011).
- [3] 鈴木 正朝, 高木 浩光, 山本 一郎, "ニッポンの個人情報「個人を特定する情報が個人情報である」と信じているすべての方へ", 翔泳社 (2015).
- [4] ビジネスジャーナル: Suica のデータ販売中止騒動, 個人特定不可なのになぜ問題? ビッグデータの難点, 入手先 http://biz-journal.jp/2013/08/post_2760.html (参照 2017-06-01) .
- [5] 個人情報保護委員会, 入手先 <https://www.ppc.go.jp/personal/preparation/> (参照 2017-06-01) .
- [6] Lane et al v. Facebook, Inc. et al, 入手先 https://www.docketalarm.com/cases/California_Northern_District_Court/5--08-cv-03845/Lane_et_al_v._Facebook_Inc._et_al/ (参照 2017-06-01) .

- [7] 新保史生. "ライフログの定義と法的責任 個人の行動履歴を営利目的で利用することの妥当性." 情報管理 53.6 (2010)
- [8] Gurpreet Dhillon. " Social Responsibility in the Information Age: Issues and Controversies." University of Nevada (2001)
- [9] Bennett, James, and Stan Lanning. "The netflix prize." Proceedings of KDD cup and workshop. Vol. 2007. 2007.
- [10] The History of the Do Not Track Header, 入手先 <http://paranoia.dubfire.net/2011/01/history-of-do-not-track-header.html> (参照 2017-06-01) .
- [11] FEDERAL TRADE COMMISSION: Protecting Consumer Privacy in an Era of Rapid Change, 入手先 <https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policy-makers> (参照 2017-06-01) .
- [12] The Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575-22579 , 入手先 https://leginfo.ca.gov/faces/codes_displaySection.xhtml?lawCode=BPC§ionNum=22575 (参照 2017-06-01) .
- [13] Yahoo's Default = A Personalized Experience, 入手先 <https://yahoopolicy.tumblr.com/post/84363620568/yahoos-default-a-personalized-experience> (参照 2017-06-01) .
- [14] Westin, Alan F. "Social and political dimensions of privacy." *Journal of social issues* 59.2 (2003): 431-453.
- [15] ジャパンプライバシーセンター株式会社, <http://www.excellent-privacy.com/index.html> (参照 2017-06-01) .