Do Not Track

実装ガイド

mozilla
Firefox

目次

これは米国 Mozilla が発行している「The Do Not Track Field Guide」の抄訳です。

この PDF の最新版と HTML 版は以下のページで公開しています。

https://developer.mozilla.org/ja/The_Do_Not_Track_Field_Guide

第 1 章 : Do Not Track の概要

オンラインプライバシーは目下、インターネット企業とそれらのサイトを訪れる人々にとって切実な課題となっています。いくつかの調査によれば、近年ユーザのプライバシーへの懸念が高まりつつあり、プライバシーを理由に家庭にインターネット環境を持たない人までいるようです[1]。そのような懸念に対するひとつの回答が、本ガイドのテーマである「Do Not Track」（行動追跡の拒否、以下 DNT）です。ユーザは、DNT の設定を有効にすることで、パーソナライズされたコンテンツよりもプライバシーを求めていることをサイトに対して示せます。あなたが所属する企業でユーザの DNT リクエストを尊重する方法を検討しているのであれば、この実装ガイドが役に立つことでしょう。

このガイドは 3 つの大きな章に分かれています。まず初めに、インターネットプライバシーの歴史に DNT がどう適応するかについて解説します。第 2 章では業種が異なる 4 つの企業を事例としたケーススタディを紹介します。DNT の実装にあたり、それらの企業が必要としたリソースと決定事項について説明し、最後にそれを一般化したフローチャートにまとめます。第 3 章は注釈付きのコードサンプルを含む DNT チュートリアルになります。DNT ヘッダの検出方法と検出した場合の対応について、実際に動作し簡単に応用できるコードを提供します。

背景

米国政府は従来、インターネット上のプライバシー保護について、企業が特定の方法でデータを収集・使用することを禁じた包括的なプライバシー法規制を行う代わりに、主に業界の自主規制に委ねてきました。有名な自主規制団体としては、Interactive Advertising Bureau（IAB）、Network Advertising Initiative（NAI）、Digital Advertising Alliance（DAA）が挙げられます。インターネット企業の多くはいずれかの団体に所属しています。これらの業界団体に参加するとメリットもある一方で、団体独自の規則に縛られることになります。例えば、NAI の会員企業はオプトアウト Cookie を提供しなければならず、NAI はユーザが会員企業のオプトアウト Cookie を有効化できる一元管理ページを用意しています。会員企業が規則に違反した場合、その団体は企業の会員資格を剥奪することができます。

米国におけるオンラインプライバシーに関する主要な法執行機関は米連邦取引委員会（FTC）です。FTC による法的措置を受けた企業は多額の罰金を科せられます。プライバシーポリシーの内容と運用実体が異なっ

1　2011 年版 Do Not Track Kids Act の序文によれば、米国在住の保護者のうち 85% が、5 年前よりもオンラインプライバシーに関する懸念が高まったと回答しています。また、調査機関の Pew によると、米国でソーシャルネットワーキングサイトを「絶対に」信用できないと答えた人の割合は、30 歳以下では 50 歳以上（14%）の 2 倍（28%）であるとされています。Mary Madden and Aaron Smith, Reputation Management and Social Media（2010 年 5 月）http://pewinternet.org/Reports/2010/Reputation-Management/Summary-of- Findings.aspx?r=1

ているといった企業の不正行為や虚偽表示に対し、FTC は適切な措置を講じる権限を与えられています。

一方、ヨーロッパでは「電子プライバシー保護指令」（ePrivacy Directive）が施行されています[2]。2009 年の改訂では、Cookie の取り扱いについて、「厳密に必要なもの」でない限りユーザの許諾が必要となりました（指令 2009/136）。加えて、一意のユーザ ID が含まれる永続的 Cookie は、個人情報に分類するとされました。ただ、企業側はユーザのオンライン体験を損なわずにこれらの新規制にどう対応すべきか解決策を見いだせていません。そうした懸念を受け、Cookie についての指令は、改訂後 1 年間は執行を猶予されています。当局は、DNT が最終的に Cookie についての同意を確立するための仕組みとなり得るかどうか検討を重ねています。

インターネットプライバシーの仕組みは通常、「通知と選択」の原理に基づいています。ひとつの例として、Web サイトはプライバシーポリシーを通じて自社のデータ取り扱い方法について通知し、ユーザはそのサイトを訪れるかどうかを選択します。実際には、プライバシーポリシーは明確で分かりやすい通知の形式にはなっていません。当然のことながら、実際にそれを読んでいる人はごくわずかです。そのため、商品やサービスを提供している企業が消費者よりはるかに情報を持っているという「情報の非対称性」が生まれています。経済学者は、市場にそうした傾向が見られる場合、自由市場に委ねるのではなく、政府が介入することで改善される見込みが高いと結論付けています。

ユーザは、特定の Web サイトを訪問しないという選択をする前に、別の選択肢を探ることもできます。そのひとつが、多くの広告会社が提供しているオプトアプト Cookie です。これによりユーザは、ターゲティング広告よりもプライバシーの尊重を望むことを表明できます。しかしながら、オプトアウト Cookie の実際の使われ方については Web サイトによって様々です。

例えば、あるオンライン行動ターゲティング広告（OBA）会社では、ユーザがオプトアウトを選択した場合、既に保存されている Cookie をすべて削除した上でオプトアウト Cookie を設定し、他に新たな Cookie を設定しない仕組みを実装しています。ある大手の検索・広告会社では、オプトアウトの要求に対して、一意のユーザ ID を「OPT-OUT」という文字で置き換えるといった対応をしています。同社は従来と同じ情報を収集し続けるものの、オプトアウトの設定をしたユーザは、全員が 1 人の巨大なユーザであるかのようにまとめて扱われます。別の大手広告・検索企業では、情報の収集方法は変えないものの、わずかに情報の取り扱い方法を変えることによって対応しています。

これら 3 つのケースではいずれも、企業は行動履歴に基づくターゲティング広告の表示を中止しています。ですが、自分たちのデータがどのように収集、使用されているのかをユーザ自身が知る手段はなく、透明性は確

2　ヨーロッパ電子プライバシー保護指令の概説より「Implementing the EU e-Privacy Directive: The Cookie Problem」参照。
https://www.cippguide.org/2011/04/12/implementing-the-eu-e-privacy-directive-the-cookie-problem/

保されていません。実際のところユーザは NAI のオプトアウト Cookie の動作ついても理解できていません[3]。

オプトアウトの意味についてユーザが混乱しているという問題のみならず、オプトアウト Cookie は技術的な課題に直面しています。オプトアウト Cookie を設定しているユーザの多くは、自分のプライバシーを守るため、Web ブラウザに保存されている Cookie をすべて定期的に削除しています。この際、オプトアウト Cookie も一緒に削除されてしまうのです。こうした問題には、オプトアウト Cookie を保持する Firefox の「TACO」アドオンや、Google Chrome に組み込まれている同様の機能を使うことで対応できますが、一部のモバイルプラットフォームのように Cookie がまったく設定されない環境ではこうした対応は取れません。

前述の通り、ユーザは自分の Cookie を管理するという選択肢も持っています。Cookie を一切保存させない、ブラウザを終了するまでの間だけセッション Cookie を使用する、あるいは多くの広告用 Cookie をスパイウェア対策ソフトで削除するといった方法で、米国内の約 30% のインターネットユーザは日常的に Cookie を削除もしくはブロックしています。ヨーロッパでは同様の対応を行っているユーザは約 50% に跳ね上がります。Cookie を用いた広告技術の前にはこうした現実が立ちはだかっています。

そのため一部の広告会社は、一般的な HTTP Cookie の使用をやめて、LSO（いわゆる Flash Cookie）、Silverlight、HTML5 といった別の形式のローカルストレージを採用しています。その他、ローカルストレージを使わずに、ブラウザのフィンガープリンティング（様々な条件を組み合わせた同一ブラウザの推定）や文字入力パターンの判別といった手法でユーザを特定している広告会社もあります。IP アドレスは準安定的な識別手段です。Windows の旧バージョンでは、（ハードウェアごとに固有の一意な識別情報である）MAC アドレスが標準でユーザの IPv6 アドレスに含まれています。また、最近のモバイル端末はほとんどが一意な識別子を持っています。

これは、たとえユーザがオプトアウト Cookie を設定し、その他の Cookie を削除し、プライバシーポリシーを読んだとしても、自分のプライバシーについて透明性を保てず、完全に管理できないということを意味します。ローカルストレージを使わない技術では特に、自分についてどのようなデータが、誰によって収集され、どのように使われているか、ユーザ自身が知る術はないでしょう。「通知と選択」によるアプローチが機能するためには透明性が前提となります。このまま米国政府が自主規制に委ねる方針を採り続けるのであれば、ユーザが自分の個人情報を管理できる新たなツールが必要となります。

2011 年 1 月、FTC 職員が、新しい有望な解決策のひとつとして Do Not Track を支持する報告書の草案を発表しました[4]。この報告書では、現在の米国における業界の自主規制だけでは法規制の強化は避けられな

3　第 38 回 Telecommunications Policy Research Conference で発表された、Aleecia M. McDonald、Lorrie Faith Cranor 両氏による論文「Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising」（2010 年 10 月）

4　米連邦取引委員会の発表「FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers」http://www.ftc.gov/opa/2010/12/privacyreport.shtm（2011 年 1 月 1 日）

いと書かれています。DNT は 2007 年に考案され、それ以来大幅な変更が加えられてきました[5]。FTC の報告書では、新法制定の代替手段となり得る、データの収集と使用をユーザがオプトアウトできるようにする仕組みとして、業界による DNT の採用が提案されています。

FTC の報告書が公開された後、2011 年春にリリースされた Web ブラウザ、Mozilla Firefox と Microsoft Internet Explorer の新バージョン、それから少し遅れて登場した Android 版 Firefox に DNT 機能が実装されました。2011 年夏には Apple の Safari も追従しました。2012 年にはインターネットユーザの約半数が DNT に対応している最新のブラウザにアップグレードすると Mozilla では予想しています。これら 3 つの DNT 対応ブラウザは、DNT を有効にするためのユーザインターフェースは異なりますが、バックエンドの対応は変わりません。

今のところ 3 つのブラウザは同じ DNT シグナルをサイトに対して送信するよう実装されていますが、将来的には別々になる可能性もあります。DNT がブラウザや Web サイトによらず常に同じ意味を持つよう、IETF と W3C という 2 つの標準化団体がその仕様を議論してきました。2011 年夏の時点では、W3C が DNT の標準化を進めていくことになっています。あなたの企業が DNT の標準化に向けた取り組みに参加を希望する、あるいはその進捗状況に興味があるということであれば、W3C のメーリングリストに参加して最新情報を入手されることをお勧めします[6]。

Do Not Track は、現時点においては米国を主な対象として議論が進められています。しかし、W3C が国際的な標準化団体であること、また、ヨーロッパの企業は電子プライバシー保護指令や Article 29 ワーキンググループの意向に従う技術的手段を見つけなければならないという圧力に直面していること、これら 2 つの事情により、おそらくこの流れは変わることでしょう。プライバシーに関するヨーロッパの状況は、通知と同意を巡って、今まさに急激な変化を遂げているのです。

Do Not Track の仕組み

最も基本的なところに立ち返ると、DNT は「ユーザが示す意思」と言えます。企業は、ユーザがプライバシーに懸念を抱いており、あなたの Web サイトにそうした懸念への対応を望んでいることを、DNT を通じてユーザから直接聞くことができます。

5　詳しくは、Christopher Soghoian の「The History of the Do Not Track Header」参照。
http://paranoia.dubfire.net/2011/01/history-of-do-not-track-header.html（2011 年 1 月 21 日）

6　第 1 回 W3C ワークショップの概要は http://www.w3.org/2011/track-privacy/report.html 参照。

技術的な観点から見ると、DNT は HTTP ヘッダの一種です[7]。DNT の設定が有効になっている場合、ブラウザは（Web ページ、画像、ウィジェット、その他各種パーツの読み込みなど）すべてのトランザクションにおいて、「DNT: 1」という文字列を HTTP ヘッダに含めて送信します。

Firefox のオプション画面を開き「**プライバシー**」を選択すると「**トラッキングの拒否を Web サイトに通知する**」という設定項目があります。これにチェックを入れると DNT が有効になります。チェックを外すと DNT ヘッダの送信は止まります。Firefox ではこの設定によって DNT の有効・無効を切り替えます（下図 1 参照）。

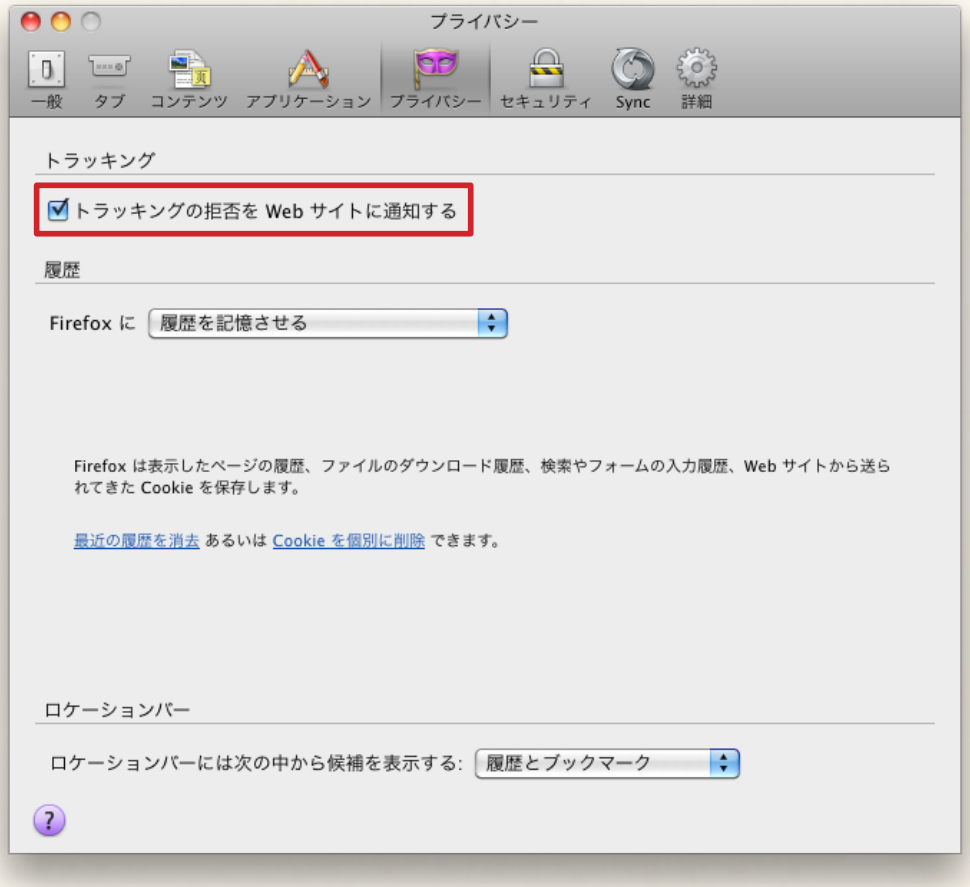


図 1: Firefox の Do Not Track 設定画面

7　HTTP ヘッダは、コンテンツの前に送受信され、各種追加情報が含まれています。例えば、現在のサイトの前にユーザが訪れていた参照元サイト、コンテンツを要求した OS と Web ブラウザの種類を示すユーザエージェント文字列などといった情報が含まれます。HTTP ヘッダは Internet Engineering Task Force（IETF）によって RFC 2616 として標準化され、何度も機能の追加を含む修正が行われています。DNT は今のところ付加的な HTTP ヘッダであり、Web ブラウザなどのユーザエージェントが自由に実装できるものの、ヘッダへの追加は義務付けられていません。

Android 版 Firefox では、デスクトップ版同様、設定の「プライバシーとセキュリティ」欄にある「追跡拒否をサイトに通知」という項目から設定できます。これを有効にすることで、Android 端末から Web ブラウジングを行う場合でも、DNT ヘッダが Web サイトに向けて送信されます。

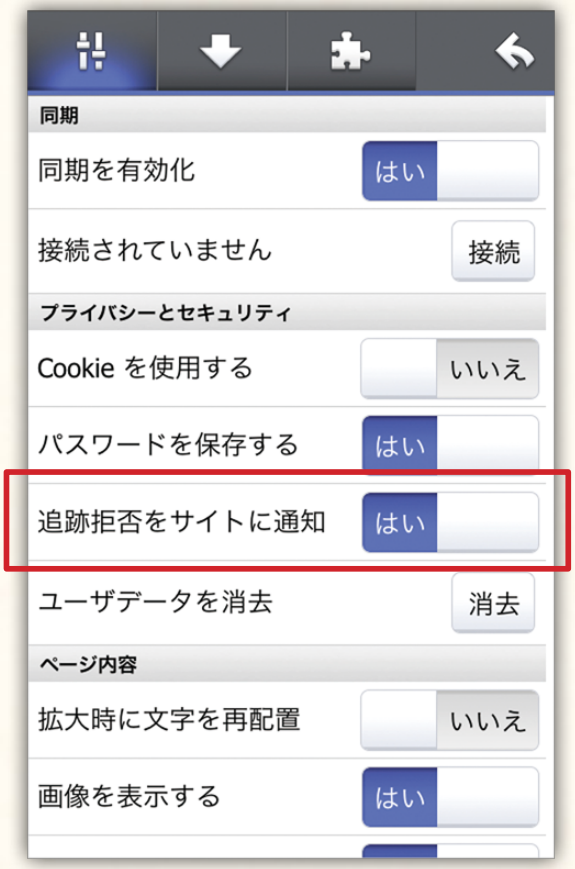


図 3：Android 版 Firefox の Do Not Track 設定画面

Firefox の「Web コンソール」や「Live HTTP Headers」アドオンなどのツールを使うと、Firefox が送受信している HTTP ヘッダを確かめることができます。以下の例は、Firefox が wikipedia.org を読み込む際に送受信した HTTP ヘッダです。分かりやすいように DNT ヘッダを黄色で強調しました。

```
GET / HTTP/1.1
Host: www.wikipedia.org
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.6; rv:2.0.1) Gecko/20100101 Firefox/4.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 115
DNT: 1
Connection: keep-alive
If-Modified-Since: Mon, 23 May 2011 07:29:40 GMT

HTTP/1.0 304 Not Modified
Date: Wed, 25 May 2011 03:53:03 GMT
Content-Type: text/html; charset=utf-8
Last-Modified: Mon, 23 May 2011 07:29:40 GMT
Age: 7
X-Cache: HIT from sq73.wikimedia.org
X-Cache-Lookup: HIT from sq73.wikimedia.org:80
Connection: keep-alive
```

ユーザが「トラッキングの拒否を Web サイトに通知する」設定を有効にすることで、Firefox は Web サイトに向けて送信する HTTP ヘッダに「DNT: 1」を追加します。このように Do Not Track はシンプルな形式で表されるのです。

トラッキングを巡る議論

Web サイトが DNT ヘッダを受け取った際に取るべき対応を決めるとなると、Do Not Track の話は複雑さを増してきます。このガイドでは、トラッキングの意味を定義するつもりも、あなたのサイトを DNT ヘッダに対応させる意図を規定するつもりもありません。その代わり、あなたが取り得るいくつかの一般的な選択肢の理解を手助けすることで、あなたのサイトとそのユーザにとって最善の判断を下せるようにすることを目的として

います。

一般的に使われるトラッキングという言葉には、多くの異なった意味合いがあります。このガイドの巻末には、そうしたトラッキングの意味を知るのに役立つ関連資料を掲載しています。例えば、一部の広告会社は、データの収集方法を変えずに済むよう、「Do Not Track」（追跡をしない）ではなく「Do Not Target」（ターゲティング広告は出さない）という言葉を用いています。しかし FTC 報告書の原案には、Do Not Track の意思をユーザが示した場合、データの使用のみならず収集も制限されると書かれています。FTC の委員と職員は、Do Not Track がデータの収集と使用いずれにも関わるものであるとして議論を続けています。

別の論点として、ファーストパーティにもサードパーティと同様に DNT が適用されるのかといった疑問や、そもそもファーストパーティの解釈が定まっていないという問題が存在します。具体例として Facebook の「いいね」ボタンのようなウィジェットが挙げられます。これはファーストパーティとサードパーティのどちらに属するのでしょうか？ あるいはアクセス解析企業は、顧客サイトから得たデータについて、ファーストパーティに当たらないからといって使用を制限されるのでしょうか？

DNT の枠組みについては合意が得られたものの、複数の関係者が様々な例外を主張しています。例えば金融機関では、ユーザが DNT を有効にしていたとしても、不正行為を防止する目的でのデータの収集・使用を求めています。企業が要求しているその他の適用除外案としては、広告料金の課金、アクセス解析、広告のローテーションや表示頻度の管理、研究開発、横断認証システム（シングルサインオン）、法執行に際してのデータ提供などが挙がっています。

初期の研究[8]では、ユーザは、ファーストパーティ、サードパーティを問わず、データの収集および使用に関する幅広い定義を DNT に期待していることが分かりました。また、不正行為防止や法執行のためといったやむを得ない例外を除き、適用除外を設けた場合、ユーザを困惑させる可能性が示されています。そのため、あなたの企業が DNT を広義で捉えれば、ユーザの期待に沿い、信頼の獲得につながることでしょう。

プライバシー技術と Do Not Tack

ユーザは、オプトアウト Cookie、ブラウザの設定変更によるセッション Cookie の強制、Cookie 自体の完全なブロックなど、多くのプライバシーツールを利用しています。そうしたツールには、バナー広告を読み込まないようにするアドオンや、Internet Explorer の追跡防止リスト（TPL）なども含まれます。これらはすべてユーザによる一方的な対応であり、インターネットの動作原理を理解しないままに用いられる場合もあります。

8　第 39 回 Telecommunications Policy Research Conference で発表された、McDonald, Aleecia M.、Peha, Jon M. 両氏による論文「User Expectations for Do Not Track」（2011 年 9 月 23 日～ 25 日）

DNT は、ユーザがプライバシーに関する意思と要望を表明できるよう考案されました。また DNT は、Cookie を使った対策だけでは不可能な問題を解決します。例えば DNT は、ブラウザのフィンガープリンティングによるユーザ特定手法や、Silverlight、LSO（いわゆる Flash Cookie）といった HTTP Cookie 以外のローカルストレージを用いている企業にも影響します。従来こうした技術に対応するには、それに関する詳しい知識が必要でしたが、DNT の仕組みでは、ユーザは一度設定を有効にして意思を示せば、その要求に対する最善の対応を各企業に任せることが可能になるのです。

DNT の実装は、業界による既存の自主規制を補完するものであり、現在あなたの企業が自主規制のために行っている投資を置き換えるものではありません。プライバシーは繊細で個人的なテーマです。自分のデータの取り扱いに安心できるかどうかの基準は人それぞれ異なります。DNT は、ユーザに自分の意思を表明する新たな手段を提供すると同時に、企業がユーザの選択肢を理解する新たな手段を提供します。

プライバシーポリシー

Web サイトのプライバシーポリシーは、DNT を有効にしているユーザを認識するのに最適な場所かもしれません。あなたのサイトが DNT に対応したら、それを知らせるために、プライバシーポリシーの上か下、もしくはページの横にバナーを貼っても良いでしょう。また、データの収集と使用という両面から、ユーザが DNT を有効にした場合にサイト側でどのような対応を行うのか明記することをお勧めします。実際にある企業では、プライバシーポリシーのページでユーザのリクエストヘッダを確認し、DNT の有効・無効を判断した上で、それぞれに応じた内容を動的に表示しています [9]。

プライバシーポリシーを通じてユーザとコミュニケーションを取る方法の欠点は、そもそもプライバシーポリシーを読む人が少ないということです。サイトの利用動向を元に、プライバシーに関する懸念が高まりそうなページを特定し、そこでユーザに通知するといった別の方法を考える必要もあるでしょう。

オプトアウト Cookie と AdChoices

オプトアウト Cookie と「AdChoices」キャンペーン [10] は、Do Not Track を補完するものです。あなたのサイトには次のようなユーザが訪れるかもしれません。① DNT は有効だがオプトアウト Cookie が設定されていないユーザ。② DNT は無効だがオプトアウト Cookie が設定されているユーザ。③ DNT が有効でオプトアプト Cookie も設定されているユーザ。これら 3 つのケースではいずれも、そのユーザがあなたのサイト上で追跡されたくないと考えていると見なして対応方針を立てることをお勧めします。DNT もオプトアウト Cookie も設

9　http://www.chitika.com/privacy 参照

10　Ad Choice では広告上にアイコンを設置します。ユーザはそのアイコンをクリックすることで、広告会社の一覧と、それらのオプトアウト Cookie を設定できるページへ移動できます。今のところヨーロッパでは、これは Cookie による意思表示の代替手段とは見られていません。詳細は http://www.aboutads.info/ 参照

定していない大多数のユーザに対しては、通常と同じプライバシー対応を取って差し支えありません。

Do Not Track と法律

DNT ヘッダに対応する実装を義務付けた明確な法規制の要件はまだどの国でも定められていません。すなわち、ブラウザの機能を用いた DNT の仕組みによる、オンラインでの行動追跡を拒否する消費者からの要求にどう対応するかを検討する場合、関連法規やコンプライアンスについて考慮しなければなりません。

現在、オンライン広告業界による自主規制への取り組みに、各ブラウザの機能として実装されている DNT への対応は含まれていません。米国では、DAA および IAB の会員企業はオプトアウト手段の提供が必須となっていますが、今のところ DNT ヘッダへの対応は求められていません。

DNT への対応にあたっては、サイトのプライバシーポリシーに記載されている法令遵守要件を拡大しなければならない可能性もあり、法的観点から熟慮すべきです。現在のところ米国では、サイトを DNT に対応させる場合、サイト内の全ページで対応を徹底させる必要があり、なおかつ、サイト側で定義した DNT の意味と、サイト利用者からの期待に対して、一貫性のある対応を取らなければならないと言われています。

業界が DNT への自主対応を表明しなかった場合、あるいは米国およびヨーロッパにおいて政策立案者による提案が受け入れられなかった場合、早ければ 2012 年には法規制が浮上するかもしれません。米国では、連邦取引委員会の理事数名と議長が Do Not Track の仕組みを支持しており、また、DNT の採用に向けて州および連邦レベルでいくつかの法案が提出されています。ヨーロッパでは、少数ながらも政策立案者が国および地域レベルで DNT の手法を支持し始めており、英国の文化・メディア・スポーツ大臣や欧州委員会のデジタルアジェンダ副委員長らがその先頭に立っています。いずれも 2012 年の中頃までに DNT 対応を実現させるとしています。

Do Not Track 対応にあたっての、関連する法規制およびコンプライアンス上のリスクに関しては、あなたの企業の法務部に調査を依頼してください。

第 2 章 : ケーススタディ

Mozilla では、いくつかの企業と DNT の実装について議論してきました。それらの企業の体験を元に 4 つのケーススタディをまとめましたので、あなたの企業で実装方法を検討する際の参考としてください。

ケーススタディ 1 : 広告会社

広告会社で DNT を実装したエンジニアに話を聞きました。ある朝、彼は出社後に技術系ニュースサイト「Slashdot」で DNT に関する記事を読み、数行のコードを書きました。実装にかかった時間は 30 分ほどでした。同社は既にオプトアウト Cookie に対応しており、既存のコードを再利用することが可能だったのです。

ユーザからのリクエストに DNT ヘッダが含まれていた場合、以下の処理を行います。

1. 同社の追跡用 Cookie に空の文字列を設定します。これにより、その Cookie に保存されている個人を識別可能な情報はすべてまとめて削除されます。
2. Cookie の有効期限を過去の日時に設定します。これにより、直ちにではないかもしれませんが、次回ユーザがページを開いたときにその Cookie は削除されます。
3. 既存のコードでは、Cookie を設定できなかった場合やオプトアウト Cookie を発見した場合に随時ログを取っていました。DNT ヘッダを検出した場合にも同様のログを取れるよう、新たなカテゴリをコードに追加しました。この処理は、コード実行時の分岐に依存しており、いかなるユーザ情報とも結びつけられていません。そのため、どれだけのユニークユーザが DNT を有効にしているかを企業側で把握する手段はありませんが、Cookie をブロックしている、オプトアウト Cookie を設定している、あるいは DNT を有効にしているユーザがトラフィック全体に占める割合を調べることは可能です。
4. オプトアウト Cookie の新規設定は行いません。DNT ヘッダを有効にしているユーザの中には自分自身で Cookie の管理を行っている人がいるかもしれないからです。オプトアウト Cookie を発行しても、ブロックされて設定されないか、すぐに削除されてしまうでしょう。オプトアウト Cookie を発見した場合に実行される既存のコードをそのまま使用し、DNT ヘッダを検出した場合もオプトアウト Cookie と同様の処理を行います。
5. DNT を有効にしているユーザがプライバシーポリシーを見た場合、そのユーザに対して直接的なコミュニケーションを行うようにしました。具体的には、プライバシーポリシーの末尾で、同社がその DNT ヘッダを認識しており、以後当人を追跡しない旨を、色付きの囲み記事で伝えることにしました。併せて、DNT はブラウザごとに設定する必要があることも記載しました。これを見たユーザは、必要に応じて使用している複数のブラウザで DNT を設定するでしょう。このメッセージの表示も、オプトアプト Cookie の対応と同列の処理となっています。DNT ヘッダが設定されていないユーザに対しては、オ

プトアウト Cookie の設定状態を色付きの囲み記事で知らせ、設定されていない場合はオプトアウト用ボタンを表示します。

この広告会社は DNT の実装について「非常に簡単で深く考えずに済んだ」と振り返りました。コード的にも実装が容易であり、プライバシーに関する意思を表明する新たな手段をユーザに提供するものだったからです。広告ネットワークとして既にオプトアウト Cookie に対応していたため、DNT への対応は簡単なことでした。同社は DNT をユーザとコミュニケーションを取るもうひとつの手段に過ぎないと捉えています。ただちに DNT に対応できる状態であり、ユーザによるプライバシーの選択を支持する姿勢を示せるというメリットを踏まえ、DNT の実装を待つ理由はないと判断したそうです。

ケーススタディ 2：テクノロジープロバイダ

次に、現在 DNT 対応を計画中のある企業に話を聞きました。同社は、デマンドサイドプラットフォーム（DSP）や広告ネットワークなどをターゲティング広告の顧客として抱えており、不正検出サービスも提供しています。また、Cookie を使用しないブラウザのフィンガープリンティングを含む様々な手法でユーザを特定しています。

この企業は、プライバシーに関する永続的な意思表明とオプトアウトの手段をユーザに提供できるという点で DNT に興味を持っていると話してくれました。Cookie による対応では、ユーザがプライバシーを守るためにトラッキング Cookie を消去しつつ、オプトアウト Cookie は保持し続けなければならないため、その仕組みを分かりやすく説明するのは困難です。DNT は、ユーザとのコミュニケーションに使えて、自社の商慣習を通知でき、また選択の手段を提供することが可能であるという点に、特に興味を持っているとのことです。同社は既にユーザが一部データの収集・使用をオプトアウトできるシステムを構築しています。また、DAA の要求水準をすべて満たしているため、DAA のオプトアウトページにも参加できる状態です。

同社の既存のソリューションに利点があるとすれば、柔軟性が挙げられます。ユーザは、同社に出稿している広告主すべてではなく一部だけのオプトアウトを設定できるのです。一方、DNT は今のところ、追跡の拒否を表明する単純なシグナルに過ぎず、ユーザは企業や広告主ごとに例外を設定することができません。同社は、DNT のメリットを考慮して今から実装する価値があると判断し、今後 DNT の改良や標準化への参加も検討したいと話しています。

ユーザからのリクエストに DNT ヘッダが含まれていた場合、以下の処理を行うと予想されます。

1. サードパーティのオンライン行動ターゲティング広告を目的としたデータの収集と使用を中止します。
2. 不正防止に必要なデータの収集と使用は継続して行います。
3. ファーストパーティのためのアクセス解析や顧客判別を目的としたデータの収集と使用の大部分は継

続します。そうした目的でのデータの収集と使用にも DNT の設定を適用するかどうかのオプションを顧客である広告ネットワークに提供し、その選択は各社に委ねます。また、すべての顧客に対して、Do Not Track の解釈や DNT ヘッダが有効な場合の対応をプライバシーポリシーに明記するよう求めます。ユーザが広告ネットワークに対して特定のオプトアウト Cookie を設定している場合、オプトアウト Cookie による指定と、ファーストパーティのために DNT を無視するポリシーが矛盾することもあり得ます。その場合は、オプトアウト Cookie の指定が尊重されます。

不正防止のために DNT を無視するという同社の方針は、最後に説明したファーストパーティとしてのデータの取り扱いという問題ほどには論議を呼ぶことはないでしょう。一方、ユーザがプライバシーを完全に守るためにはオプトアウト Cookie と DNT を同時に設定しなければならないという仕様は、DNT がファーストパーティにも適用されるかどうか、あるいはファーストパーティの定義をビジネスパートナーにまで広げるかどうかの考え方によっては、ユーザの反発を招く可能性もあります。

DNT 対応の一環として、同社は現在、ユーザ向けのオプトアウト設定ページで、DNT を有効にしているユーザに対して追加情報を提供しています。DNT ユーザがその設定ページを訪れた際には、DNT が有効であると確認した旨を通知し、DNT を有効にすることで発生する（不正防止などの）データの利用への影響について説明します。同社では、顧客企業へ DNT についての情報を受け渡す API の提供についても検討しているものの、まだ決定には至っていません。また同社では、追跡防止リスト（TPL）を指定しているか DNT を有効にしているユーザと顧客企業が対話する手助けとなることを望んでいます。そうしたエンドユーザに対しては、データの活用方法を説明し、オプトアウトを解除する機会を設けたいとしています。

ケーススタディ 3：メディア企業

巨大な知的財産ポートフォリオを持つメディア企業の例を紹介します。同社では、パートナーの Web サイトを通じてアクセスされるコンテンツのアクセス統計を保有していますが、Cookie と結び付かないプライバシーシグナルであるという DNT の特長を評価し、その採用に大変満足しています。このメディア企業はパートナーサイトのオプトアウト設定を一括管理できるページを含め、オプトアウト Cookie を使った大規模なインフラを既に保有しており、DNT への対応にもそれらの資産を活用できました。そのため、1 人のエンジニアによる数時間の作業だけで DNT の実装が完了しました。

ユーザからのリクエストに DNT ヘッダが含まれていた場合、以下の処理を行います。

1. そのユーザに対して、新規の Cookie の設定を行いません。
2. 特定のメディアコンテンツに対する全ユーザの訪問回数の集計は継続しますが、DNT ユーザは、ユニークユーザによる訪問として集計しないことにします。

3. DNT ユーザの Cookie に含まれるすべてのデータを消去します。
4. その Cookie を削除するために、Cookie の有効期限を過去の日時に設定します。

当初、このメディア企業は、Do Not Track を「中止ボタン」ではなく「一時停止ボタン」のような役割として捉えていたため、ユーザの Cookie に含まれる情報を削除していませんでした。この手法では、例えば試しに DNT を有効にし、後で再度無効化したユーザがいた場合、またその人を特定し、通常時の対応を再開することが可能でした。そうした中、あるブロガーが調査を行い、同社は DNT に対応したと宣伝しているものの、Cookie に情報が保存されたままであることに気付き、懸念を表明しました。ユーザのブラウザに同社の Cookie が残っているのに、それを同社が読み取ることはないというのは説得力に欠けます。最終的に同社は、最初の実装の意図を釈明するよりも単純に DNT ユーザの Cookie を削除する方が容易であると判断し、上記の方法に改めました。

ケーススタディ 4：ソフトウェア企業

広告業務は行っていないものの、現在、Do Not Track の実装に取り組んでいる、あるソフトウェア企業に話を聞きました。同社法務部のスタッフ 2 名によって、DNT が同社のプライバシーポリシーに与える影響について調査が開始されました。

同社はまず、自社の製品ラインをすべて表にまとめた上で、DNT ヘッダを検知できるかどうかの基準で製品を分類しました（例えば、単体のデスクトップアプリケーションは DNT ヘッダを検知できないため、DNT の影響を受けません）。そして、DNT ヘッダを検知できる製品については、その詳細を調べました。

中には、DNT ヘッダの遵守が意味をなさない製品も一部あることが判明しました。例えば、プロジェクトによっては、顧客からのフィードバックを得る目的で、100 人にも満たない小規模な研究グループを運営しています。スタックトレースやデバッグ情報を含む大量のデータを送信していることについては顧客も理解しています。この場合は、Do Not Track を有効にしているユーザに限り、ダウンロードページの一番上に注意書きを加えるのが適当であると判断しました。トラッキングを無視する設定が有効になっているにも関わらず、データの収集と使用が求められる調査に参加しようとしているとして、それに同意できなければ参加を遠慮してもらう旨を DNT ユーザに通知することにしました。

また別のケースでは、より詳細な調査が必要なプロジェクトはどれか、議論すべきエンジニアは誰か、法務部が確認を取りました。同社では、すべての対象製品について DNT への最善の対応方法を決めるため、プロジェクトリーダー 1 人 1 人に対して働きかけを行っています。

次に、すべての製品において着目すべき項目の一覧を作成しました。以下がその内容です。

- IP アドレスの記録
- HTML メールへのビーコンの埋め込み
- 社内のサイトアクセス解析ツール
- 社外のサイトアクセス解析企業

同社が契約している解析企業はオプトアウト Cookie を提供しているものの、現時点ではまだ DNT に対応していません。将来的にはどの解析企業と契約する場合も DNT の遵守を求める必要があると判断し、契約更新まで残り数か月に迫った時点で、交渉するポイントのひとつに DNT の遵守を加えました。その他 3 つの点については、データの収集・使用方法を把握した上で、DNT への最善の対応方法を決めるため、担当エンジニアと議論する予定です。これらは製品ラインをまたぐ課題なのです。

考慮すべきその他の問題

ここまで、DNT の実装が完了した、あるいは現在対応を検討中の企業の事例を取り上げましたが、他にも何社かで意思決定のポイントを中心に話を聞く機会がありましたので、それについても触れることにします。中にはあなたの企業に当てはまるものがあるかもしれません。

例えば、NAI の会員やその他の企業ではオプトアウト Cookie を提供しています。IP アドレスは一意な識別が可能であるものの、通常 Cookie のデータには含まれないため忘れられがちです。モバイル端末では、個人を特定できる手段が他にも存在します。また一部の企業は、ファーストパーティのホストに設定された、本来サードパーティに分類されるべき Cookie の扱いについても考える必要があるでしょう。

オプトアウト Cookie

ある企業は DNT の実装に当たり、同社が過去に設定したすべての Cookie を削除しようとしましたが、削除される Cookie には同社サイトのオプトアウト Cookie も含まれることに気付きました。そこでその企業は例外を設け、オプトアウト Cookie はそのままに残すことにしました。この手法では、ユーザが DNT を一時的に有効にした後再び無効化しても、オプトアウトを設定し直す必要がなくなります。これはユーザの選択を尊重しており、説明も簡単な保守的手法と言えます。

IP アドレス

本ガイドの執筆時点において、米国上院議会では、IP アドレスおよびその他の情報についてデータの保持を義務付ける新法が検討されています。将来、多国籍企業は米国と EU の法規制の矛盾に直面する可能性があるということです。IP アドレスに関する対応を検討する際には、法によって定められている最新の要求事項お

よび禁止事項を確認するようお勧めします。私たちが見てきた企業が採用していた 3 通りのアプローチを以下に挙げます。

1. ユーザの DNT 設定に関係なく、Web サーバのアクセスログへの IP アドレスの記録は続けます。アクセスログは Cookie を用いた仕組みではなく、ユーザの行動追跡の手法としてすぐに思い浮かぶものではないことから、単純に見過ごされている場合もあります。しかし、EU では IP アドレスは個人を識別可能な情報として分類されており、EU 圏からのサイト訪問者の中には IP アドレスは記録されないものであると強い期待を寄せている人がいるかもしれません。
2. アクセスログ内の IP アドレスを、最後のオクテットを外すことで切り捨てます(例えば、128.2.45.67 と 128.2.45.68 はどちらとも 128.2.45 としてまとめられ、2 つのアドレスは区別が付かなくなります)。これにより、IP アドレス先頭の 3 オクテットが同じコンピュータは最大 255 台存在することとなり、いくらかのプライバシーは確保されるため、この発想は一般的なものと言えます。しかし、切り捨てた IP アドレスであっても、企業が位置情報を参照すれば顧客の物理的な場所を把握できてしまいます。切り捨てでは匿名化は行えません。特にデータの母集団が小さい場合、切り捨てた IP アドレスに対応する特定あるいは一部のユーザを識別することは十分に可能です。ただ、完全な IP アドレスを保存する以外に選択肢がない場合、そうした切り捨てはユーザのプライバシーを保護するためのささやかな手段となります。
3. IP アドレスの記録を行わないようにします。DNT が有効になっている訪問者の IP アドレスを記録しないよう、Apache や IIS などのサーバ設定を変更することは技術的には簡単です。私たち自身がテストを行ったわけではありませんが、サンプルコードは http://donottrack.us/server より入手できます。

モバイル端末

Firefox は Android 版でも DNT ヘッダの送信に対応していますので、モバイル端末からの閲覧に最適化した Web サイトを運営している場合、そのモバイルサイトについても Do Not Track 対応が望まれます。

Android 版 Firefox の Do Not Track の挙動は、デスクトップ版とまったく同じです。ユーザがブラウザの DNT 設定を有効にすれば、HTTP ヘッダとして「`DNT: 1`」という文字列が送信されます。このように、モバイル端末でもブラウザでは DNT を設定できますが、HTTP 通信を使用しない他のアプリケーションは対象となりません。

GPS による位置情報、シリアルナンバー、UDID など、デスクトップパソコンからは取得できない、端末を特定可能な識別情報を収集する場合でも、DNT を有効にしたサイト訪問者に関しては、その収集を制限する手段を検討した方が良いでしょう。

ファーストパーティのホストに設定されるサードパーティ Cookie

一般的に、あなたのサイトが設定した Cookie の読み取り、変更、削除が可能なのはあなたのサイトだけです。しかし、いくつかの広告会社は、広告を載せているファーストパーティのサイトで、あたかも自社がファーストパーティであるかのように Cookie を設定しています。こうした状況はごく一部の企業にのみ関係することであり、あなたの企業がそれに該当しないならば、この節は読み飛ばして構いません。

サードパーティの Cookie がファーストパーティの Cookie であるかのように設定される状況を、ひとつの例を元に見てみましょう。Adverts と呼ばれる企業から広告を配信している MyNews.com というサイトを訪れたとします。ユーザは、mynews、www.mynews、そして adverts といった複数のホストから Cookie を設定されることになります。ここで、mynews や www.mynews からの Cookie はファーストパーティとして扱われ、adverts からの Cookie はサードパーティとして扱われると思うでしょう。しかし、いくつかの広告会社は自社のサードパーティ Cookie をファーストパーティの Cookie と同様に送信しているのです。この例では、Adverts の広告用 Cookie が mynews ホストに設定されることを指します。いくつかの企業がこうした手法を採用しており、Google アナリティクスの例が広く知られています[11]。Mozilla では Google と実際の運用形態について話したわけではありませんが、この節では Google アナリティクスの例を挙げて話を進めます。

私たちは、ファーストパーティのホストにサードパーティ Cookie を設定しているある広告会社と話をしました。同社は、DNT ヘッダを受け取ると、自社で設定した Cookie をすべて削除しようとします。しかし、ファーストパーティのホストに対して Cookie を設定しているため、自社が設定した Cookie を書き換えるだけでなく、他の Cookie を書き換えたり削除したりすることも技術的には可能です。例えば、ある広告会社が mynews ホストへファーストパーティ Cookie を設定すると、MyNews の Cookie はもちろんのこと、他の競合広告会社が同じ手法を使ってファーストパーティのホストに Cookie を設定していた場合も、すべて自社の Cookie 同様に削除できてしまいます。つまり、Adverts がアクセス可能なすべての Cookie を削除しようとした場合、Google アナリティクスをはじめとした、ファーストパーティとして設定されているあらゆる Cookie を削除できてしまうのです。こうした問題は、Google やそのファーストパーティが DNT を遵守しているかどうかに関わらず発生しうるのです。

Mozilla はトラッキングの意味を定義するつもりはありませんが、この点に関しては意見を表明します。上記の例のように、DNT を遵守するという名目で競合他社の Cookie を削除するのは適切ではありません。たとえファーストパーティのホストに設定されている他のサードパーティ Cookie や、ファーストパーティによって設定された本当の意味でのファーストパーティ Cookie にアクセス可能であったとしても、削除するのは自社で設定した Cookie に限定すべきです。

---

11 「Google Analytics の仕組みを教えてください」http://www.google.com/support/analytics/bin/answer.py?hl=ja&answer=55539
「Cookies & Google Analytics」https://code.google.com/apis/analytics/docs/concepts/gaConceptsCookies.html

広告会社は、DNT ヘッダを遵守する場合、以下の点に気を付けてください。

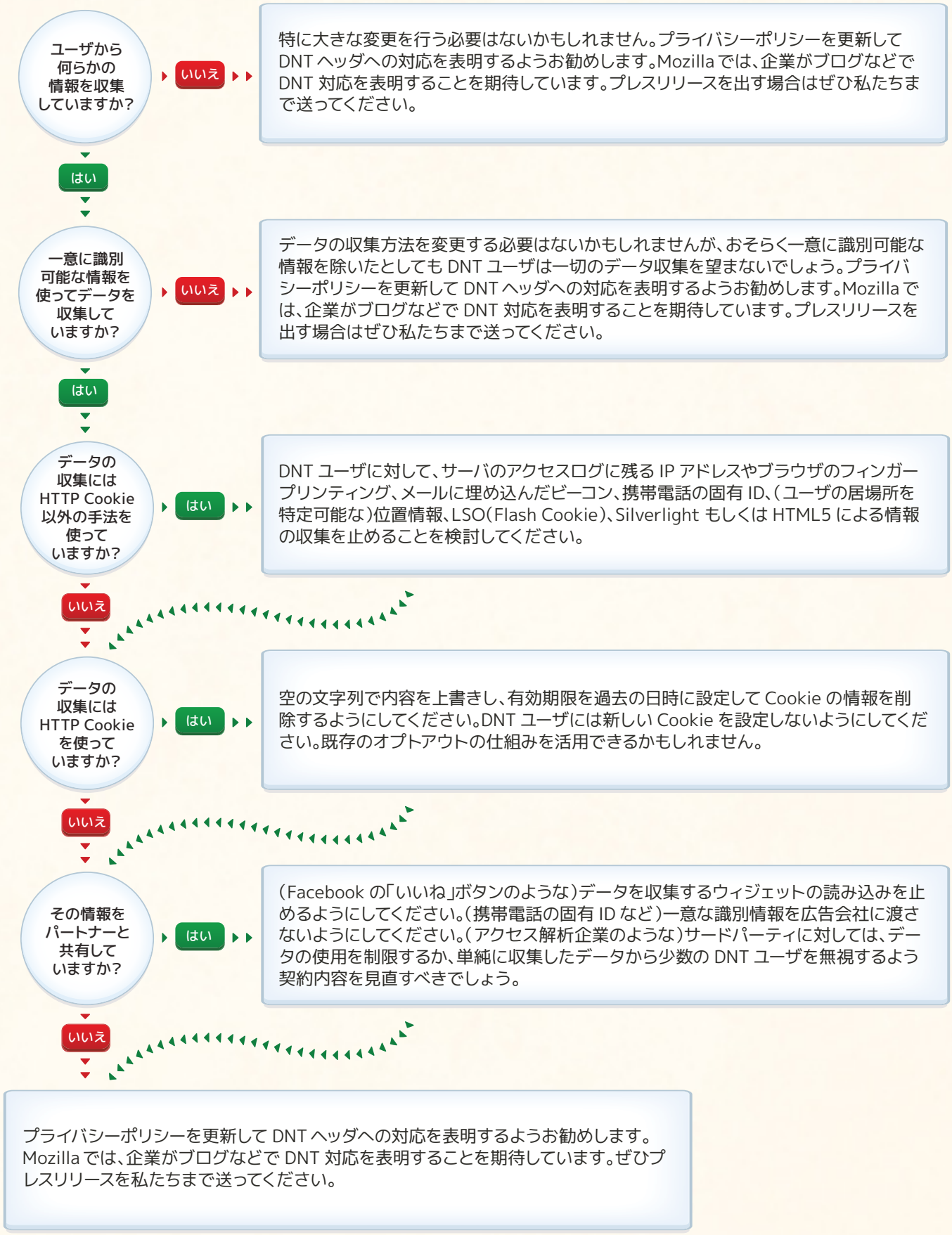
- 他のパーティによって設定された Cookie は削除しない
- オプトアウト Cookie は削除しない
- 自社で設定した Cookie はすべて削除する

簡単そうに聞こえますね。上で取り上げた広告会社は、特定の名前の 4 つの Cookie を設定しています。DNT ヘッダを検出した場合、同社が取るべき対応は、それら 4 つの Cookie を削除することだけです。しかし、ここで 1 つ複雑な問題がありました。同社は、顧客が独自の広告用 Cookie を同じディレクトリに設定できるようにする API を開放しているのです。この API を通じて設定された顧客企業の Cookie について、どのような名前が使用されているのか、同社では把握していません。そのため、自社に関連する Cookie をすべて削除できないという状況が発生してしまったのです。顧客が付けた Cookie の名前が分からないため、他のパーティの Cookie は残しつつ、自社に関連する Cookie だけを削除することが不可能だからです。

話を先に進めると、この広告会社は、同社が設定するすべての Cookie に接頭辞を追加し、その接頭辞が付いた同社の Cookie だけを削除できるよう、システムの変更を検討しているということです。この新しいシステムが稼働しても、API を通じて過去に顧客企業が設定した Cookie は残るでしょう。そうした古い Cookie はいずれ期限切れを迎えますが、それには相当な時間がかかります。それまでの間、顧客が設定した Cookie の名前をすべて調べて DNT 実装の中にそのリストをハードコードするといった対応が、ひとつの解決策として考えられます。あるいは、すべての顧客に対して、新しい命名規則に基づく Cookie への移行を促すことも可能でしょう。しかしどちらも完璧な方法ではありません。

DNT 対応フローチャート

これまでに取り上げたケーススタディはいずれも事情が異なりますが、DNT 対応を検討する際に考慮すべきことにはいくつかの共通点が存在します。私たちは、ここで取り上げなかった企業とも、モバイル端末における対応を含め、いくつかのポイントについて議論してきました。あなたの企業が実装を検討する際には、図 3 にまとめたポイントを参考にしてみてください。


ユーザから何らかの情報を収集していますか?
いいえ
特に大きな変更を行う必要はないかもしれません。プライバシーポリシーを更新してDNT ヘッダへの対応を表明するようお勧めします。Mozilla では、企業がブログなどでDNT 対応を表明することを期待しています。プレスリリースを出す場合はぜひ私たちまで送ってください。
はい
一意に識別可能な情報を使ってデータを収集していますか?
いいえ
データの収集方法を変更する必要はないかもしれませんが、おそらく一意に識別可能な情報を除いたとしても DNT ユーザは一切のデータ収集を望まないでしょう。プライバシーポリシーを更新して DNT ヘッダへの対応を表明するようお勧めします。Mozilla では、企業がブログなどで DNT 対応を表明することを期待しています。プレスリリースを出す場合はぜひ私たちまで送ってください。
はい
データの収集にはHTTP Cookie以外の手法を使っていますか?
はい
DNT ユーザに対して、サーバのアクセスログに残る IP アドレスやブラウザのフィンガープリンティング、メールに埋め込んだビーコン、携帯電話の固有 ID、(ユーザの居場所を特定可能な)位置情報、LSO(Flash Cookie)、Silverlight もしくは HTML5 による情報の収集を止めることを検討してください。
いいえ
データの収集にはHTTP Cookieを使っていますか?
はい
空の文字列で内容を上書きし、有効期限を過去の日時に設定して Cookie の情報を削除するようにしてください。DNT ユーザには新しい Cookie を設定しないようにしてください。既存のオプトアウトの仕組みを活用できるかもしれません。
いいえ
その情報をパートナーと共有していますか?
はい
(Facebook の「いいね」ボタンのような)データを収集するウィジェットの読み込みを止めるようにしてください。(携帯電話の固有 ID など)一意な識別情報を広告会社に渡さないようにしてください。(アクセス解析企業のような)サードパーティに対しては、データの使用を制限するか、単純に収集したデータから少数の DNT ユーザを無視するよう契約内容を見直すべきでしょう。
いいえ
プライバシーポリシーを更新して DNT ヘッダへの対応を表明するようお勧めします。Mozilla では、企業がブログなどで DNT 対応を表明することを期待しています。ぜひプレスリリースを私たちまで送ってください。

第 3 章：チュートリアル

Do Not Track ヘッダへの対応は、技術的なレベルではとても簡単なことです。以下のチュートリアルではサンプルコードを提供しており、すぐに実行して試すことができます。サンプルコードは Mozilla の Web サイト（http://dnt.mozilla.org/）からもダウンロード可能です。

ユーザの DNT 設定を判別するには 2 通りの方法があります。ひとつは、このガイドの読者にはおなじみと思われる JavaScript、もうひとつは PHP などのサーバサイドプログラムです[12]。PHP に限らず Ruby や他の言語においても簡単に実装可能であり、その場合、ここで示す PHP コードが処理ロジックを考える上での参考となるでしょう。

チュートリアルは以下の 3 つとなります。

1. 1 つ目のチュートリアルは、DNT 判別の基本です。JavaScript を使って Web サイトの訪問者から DNT 設定を読み取り、それをポップアップアラートとして表示する方法を紹介します。
2. 2 つ目のチュートリアルでは、JavaScript の代わりに PHP を使って DNT ヘッダを読み取ります。
3. チュートリアル 3 では、個人を特定しないデータ集計、Cookie データの削除、Cookie を期限切れにする方法について紹介しています。

12　本ガイドの英語原文では JavaScript による判別ができないと書かれていますが、Firefox を始めとする各ブラウザの現行バージョンでは可能となっているため、日本語版ガイドではそれに合わせてコードの例を更新するとともに分かりやすく簡素化しています。

チュートリアル 1：JavaScript を使った DNT 設定の判別

JavaScript による DNT 設定の判別はとても簡単です。

```
<html>
  <body>
    <script>
      var dnt = navigator.msDoNotTrack || navigator.doNotTrack;
      if (dnt && dnt == 'yes' || dnt == 1) {
        document.write('DNT は有効です ');
      } else {
        document.write('DNT は無効です ');
      }
    </script>
  </body>
</html>
```

Do Not Track の設定は navigator.doNotTrack に格納されます。最初に、このプロパティが存在するかどうかを確認しています。Internet Explorer 9 ではベンダー接頭辞付きのプロパティが使われているため、それに関しても考慮しました。プロパティが存在し、なおかつ DNT が有効の場合、このプロパティの値は yes となります。以前はこの値が（文字列の）1 でした。上記のコードではそうした新旧の仕様に対応しています[13]。navigator.doNotTrack プロパティが存在しない DNT 非対応ブラウザや、プロパティの値が有効でない場合、DNT は無効と判別されます。

上記内容の HTML ソースを dnt.html などのファイル名で保存し、それを Web ブラウザで開いてください。期待されるブラウザごとの結果の一覧がこちらになります。

- Firefox で、DNT を設定していないか無効にした場合「DNT は無効です」
- Firefox で、DNT が有効の場合「DNT は有効です」
- Opera 12、Safari 5.1（Mac 版）も Firefox と同じ結果になるはずです
- Internet Explorer 9 で、追跡防止リストが無効である場合「DNT は無効です」
- Internet Explorer 9 で、追跡防止リストが有効である場合「DNT は有効です」

13 https://developer.mozilla.org/en/DOM/navigator.doNotTrack

ここでは単なる文字列を表示していますが、実際にはオプトアウト Cookie のコードと組み合わせるなどして、広告を表示することになるでしょう。

チュートリアル 2 : PHP を使った DNT 設定の判別

次に、サーバサイドプログラムを使った例を示します。PHP コード（あるいは他の言語による実装）は Web サーバ上で実行する必要があります。ブラウザでローカル環境にある PHP ファイルを直接開いても、コードは実行されず Do Not Track ヘッダは読み取れません。あなたの Web サーバに PHP が導入されていない場合は、あらかじめインストールを行う必要があります。

```
<?php
if (isset($_SERVER['HTTP_DNT']) && $_SERVER['HTTP_DNT'] == 1) {
  echo ('DNT は有効です ');
} else {
  echo ('DNT は無効です ');
}
?>
```

上記内容の PHP コードを dnt.php などのファイル名で保存し、サーバに設置したら、ブラウザでそれに対応する URL を開きます。

DNT ヘッダが設定されており、その値が 1 の場合は、有効と判別されます。それ以外の場合（DNT ヘッダが設定されていないか、設定されていてもその値が 1 でないとき）は無効と判別されます。今のところどのブラウザも DNT ヘッダの送信方法は同じなので、JavaScript と異なりブラウザごとの差異について気にする必要はありません。

チュートリアル 3 : DNT に基づく集合データの収集

ケーススタディで述べたように、DNT リクエストへの対応には様々な方法があります。ここでは、ユーザごとにデータを収集するのではなく、訪問者全体のデータを集計するために Cookie を設定する方法の例を示します。このサンプルコードは、DNT の手法としてデータの集計を推奨する趣旨のものではないという点をよく理解してください。特に、あなたのサイトを訪れるユーザの DNT の趣旨に対する期待に沿うものではないかもしれず、採用する方法については十分な注意を促します。しかし、集合データの解析は既に実際に行われています。例えば Google は、オプトアウトを望むすべてのユーザに OPT-OUT という文字列を含む Cookie を設定

しつつ、匿名でのデータ集計を行っています。下記の JavaScript サンプルコードはそうした一般的な手法に沿ったものです。

このサンプルコードでは、DNT ステータスに基づいて、Cookie を削除し期限切れにする方法の基本についても説明しています。

```
// 以下の関数名はあくまでも例です。実装の参考としてください
function setCookie(cookie_name, string_value, time_to_expire)
{
  // 既にあなたの企業にはそのまま使用できる実装があるかもしれません。
  // なくても Web 上では多くの実装例を見つけることができます。
}

if (getDntStatus()) { // Do Not Track ヘッダを検知した場合
  // 既存の Cookie を削除
  deleteAllCookies();
  // すべての DNT ユーザに対して，　有効期限を 5 年（単位は秒）とした
  // オプトアウト Cookie の値を設定します。
  setCookie('trackingcookie', 'opt-out', time() + 60*60*24*365*5);
} else {
  // トラッキングを行うための既存のコード
}
```

DNT を有効にしているユーザが訪れた場合、まず、既に保存されているすべてのトラッキング Cookie を削除する必要があります。すべての Cookie を一度削除しなければ、DNT ユーザ向けのオプトアウト Cookie が設定されるにもかかわらず、トラッキング Cookie が残るという状況になってしまいます。そうなると、知識があり、声を上げる可能性のある一部のユーザを混乱させるかもしれません。バックエンドのデータベースにキーとそれに対応するデータを保存している場合は、キーを削除することで二度とデータを取り出せなくなる前に、あらかじめデータベースからすべての情報を削除しておいた方が良いでしょう（DNT に関する IETF の現行の草案が採用された場合、その第 8 章 1 節に従えば、サードパーティのトラッキングデータは、Cookie に含まれている情報に限らず、すべて削除されなければなりません）。

LSO やキャッシュ Cookie、HTML5 ローカルストレージ、Silverlight ローカルストレージといった、ユーザのパソコン上に保存される HTTP Cookie 以外のトラッキング情報についても同様に考えなければなりません。

HTTP Cookie のみを削除し、その他のローカルストレージをそのままにしておくと、ユーザに DNT が遵守されていないと思われるかもしれません。

既存のトラッキング Cookie を削除した後も集合データの収集を行うつもりであれば、「opt-out」などの値で新しい Cookie を設定すべきでしょう。これにより、すべての DNT ユーザがブラウザごとの識別情報の代わりに同じ識別情報を共有することになります。上記コードサンプルでは、オプトアウト Cookie の有効期間を 5 年間としています。有効期間の長さはあなたが自由に設定できますが、業界による自主規制では最短でも 5 年間と定められています。あなたがトラッキング Cookie に対して設定している有効期間と同じにしておくのが妥当かもしれません。

参考資料

DNT の歴史や背景、あるいは様々な利害関係者にとっての DNT の意義について詳しく学びたい方は、以下の資料を参照することをお勧めします。

- 業界に対して DNT の仕組みを構築するよう要請した FTC 報告書
  http://www.ftc.gov/opa/2010/12/privacyreport.shtm
- ターゲティング行動に関する FTC のガイドライン
  http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf
- DNT と親和性のあるデータ収集の方法も解説している Do Not Track クックブック
  http://donottrack.us/cookbook
- IETF の Do Not Track 原案
  http://datatracker.ietf.org/doc/draft-mayer-do-not-track/
- 電子フロンティア財団（EFF）における議論
  https://www.eff.org/deeplinks/2011/02/what-does-track-do-not-track-mean
- The Center for Democracy and Technology（CDT）の DNT の提案
  http://fec.cdt.org/DNT-2
- W3C が主催した DNT ワークショップの発表資料など
  http://www.w3.org/2011/track-privacy/