NRI 未来創発
Dream up the future.

野村総合研究所

資料2

日米欧における
デジタル広告とプライバシーに関する規制の動向

2019年10月21日

株式会社野村総合研究所
ICTメディア・サービス産業コンサルティング部
パブリックポリシーグループマネージャー/上級コンサルタント

小林慎太郎

本日お話しさせていただくこと

1. EU
   - GDPR（EU一般データ保護規則）
   - フランス当局（CNIL）によるGoogleの執行事例
2. 米国
   - ターゲティング広告の自主規制
   - カリフォルニア州消費者プライバシー法（CCPA）
3. 日本
   - ターゲティング広告に係る個人情報保護法改正の方向性
   - Facebookに対する行政指導

GDPR（EU一般データ保護規則）の概要

GDPRは、2018年5月25日から施行

規制のEU域外への適用

EU域外へのデータ持ち出し制限（越境移転規制）

・EU住民のパーソナルデータは、
　特別な契約なしにEU域外へ持ち出せない
等

ビッグデータビジネスへの牽制

・通知と同意の義務
・消去権（忘れられる権利）
・データポータビリティ権
・異議を述べる権利
等

台帳とリスクに応じた態勢

・個人データ台帳
・データ保護責任者（DPO）
・プライバシー影響評価（PIA）
等

漏えい時の通知

・漏えい発覚後72時間以内に当局へ通知、
　本人にも速やかに通知
等

違反時の制裁金

最大で、全世界における年間売上高の
4%　または
2,000万ユーロ
のいずれか高い方

GDPRが規制対象とする個人データの範囲は、IPアドレス、クッキーIDにおよぶ。

個人データに該当する例	個人データに該当しない例
● 氏名 ● 自宅住所 ● name.surname@company.comのような電子メールアドレス ● 位置データ（例：携帯電話で用いられる位置データ） ● IPアドレス ● クッキーID ● 携帯電話の広告ID	● 法人登録番号 ● info@company.comのような電子メールアドレス ● 匿名化されたデータ

出所）欧州委員会ウェブサイト"What is personal data?"
https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en（2018年12月確認）

EU

フランスの個人情報の監督機関CNILは、Googleに対して、ターゲティング広告の透明性の欠如等を理由に、5,000万ユーロの制裁金を科した。

■ 概要

- フランスの個人情報の監督機関（CNIL）は、2019年1月21日、Googleに対して、ターゲティング広告の透明性の欠如、不十分な情報提供、有効な同意の欠如についてGDPR違反を認定し、5,000万ユーロ（約60億円）の制裁金を科した。
  - 2つの団体からGDPR施行後に受領した苦情を起点に、CNILがオンライン検査を実施して、違反の事実を確認。
  - GDPRの罰則が適用された初めての事例。

■ 違反の内容

- Googleの提供する情報へ、ユーザーは容易にアクセスすることができない。
  - 利用目的、データの保持期間、広告に利用するデータ項目等の主要な情報が複数の文書に、過剰に分散して記載されている。重要な情報にアクセスするには、5～6ステップの操作が必要。
  - いくつかの情報は、いつも明瞭で包括的でない。ユーザーはGoogleによるデータ処理を完全に理解することはできない。
- 同意が適正に取得されていない。
  - 同意取得の際に、Googleからユーザーへ十分な情報が提供されていない。
  - Googleが取得する同意において、データの利用目的が特定されておらず、明瞭なものでない。
    - Googleの同意取得方法は、Googleアカウントを作成する際、ユーザーは「利用規約に同意します」、「プライバシーポリシーでさらに説明されているとおり、個人情報の処理に同意します」というボックスにチェックマークを付けるのみ。これによってGoogleの様々なサービスに、ユーザーは同意することになっている。

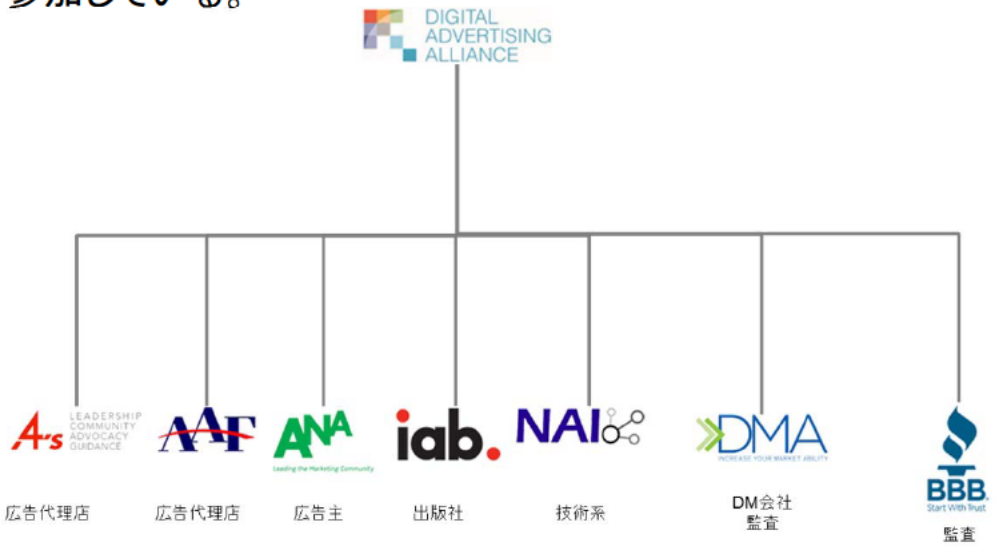
出所）CNIL” The CNIL’s restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC”（2019年1月21日）をもとに作成

米国のターゲティング広告は自主規制の枠組みで運用されている。

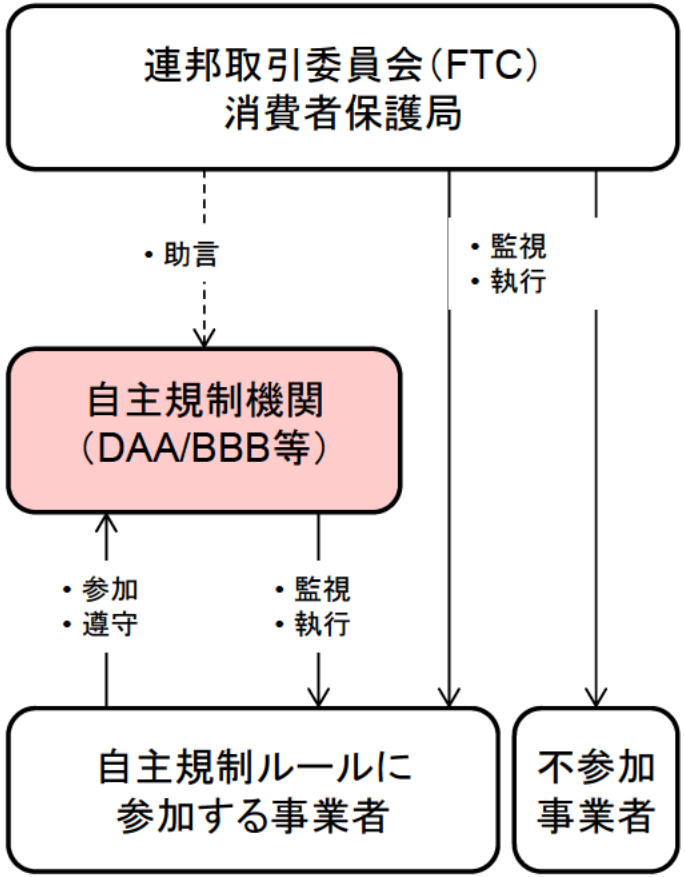
- DAA（Digital Advertising Alliance）は、ターゲティング広告に関する自主規制ルールを作成するとともに、消費者へ選択の機会（オプトアウトのサービス）を提供。

行動ターゲティング広告における自主ルールを策定し、事業者にライセンス“ｉマーク”を付与。

- DAAには、大手の広告業界団体（AAF、iab、NAI等）の他に、ルールの監視・執行を担う消費者団体BBB、DMAが参加している。



DAAによる自主規制スキーム



米国

DAAは、クロスデバイストラッキングに関する自主ルールとして、「透明性の担保」と「ユーザーのコントロール権」に焦点を当てた内容を策定。

■ 透明性の担保

- **説明責任**： 特定のブラウザまたは端末から複数のデータ、及びクロスデバイス・アプリケーションデータを収集して、別の端末の広告表示等に活用する場合、データの収集及び活用は、特定のブラウザまた端末から収集されたデータが、その他のブラウザや端末に連携している、または他ブラウザや他端末に、広告表示等の目的で、安全なことを前提に（アフィリエイト等を含めない）、他端末使用されるという事実を説明するべきである
- **データ収集・活用の停止**： 上記に記載したようなデータの収集及び活用は、ユーザー選択を通じ、ユーザーが制限できるようにする。Webサイトやアプリケーションを介して、マルチサイトまたはクロスデバイス・アプリケーションデータの収集に従事している第三者を個別にリスト化し、ユーザーが個別に選択することができるメカニズムを提供する
- **告知**： クロスデバイスによって収集されたデータが使用される場合、ファーストパーティは、同業界で開発・統一されたような、明確で意味のある目立つリンクを提供し、説明責任・開示責任を果たしているWebサイトにリンクする

■ ユーザーのコントロール権

- **選択している端末と連携されている端末のデータ収集**： 選択が実行されている特定のブラウザまたは端末に、連携されている別のコンピュータまたは端末で使用するための、マルチサイトデータ、または端末上のクロスアプリケーションデータを収集すること
- **選択している端末と連携されている端末のデータ活用**： 選択が実行されている特定のブラウザまたは端末に、連携されている別のコンピュータまたはデバイスにデータが収集されたときに、選択されているブラウザまたは端末でマルチサイトのデータまたはクロスデバイスアプリケーションデータを広告表示等に活用すること
- **ユーザーがデータの収集を許可している場合の第三者提供**： 選択が実行されているブラウザまたは端末から収集されたマルチサイトデータおよび/またはクロスデバイスアプリデータの第三者（非アフィリエイト）への提供

出所）DAA”Application of the Self-Regulatory Principles of Transparency and Control to Data Used Across Devices”（2015年11月）より作成

カリフォルニア州消費者プライバシー法（CCPA）は、世帯や端末の情報を保護対象とする。

概要

- カリフォルニア州消費者プライバシー法(CCPA：The California Consumer Privacy Act)は、州議会から提出された消費者の個人情報保護の強化を目的とする州法で、2018年7月に採択された。2020年1月から施行予定。
- 州法であるものの、カリフォルニア州には多くのIT企業が立地しており、その影響は米国に留まらず、世界中に影響がおよぶ。同州が漏えい時の通知義務を2002年に世界に先駆けて導入し、その後全米、EU等へ波及した実績がある。

主な特徴

- 世帯の情報、端末の情報が、個人情報として保護の対象となる。
- 本人による自己データへのアクセス手段の提供（データポータビリティ）を義務化。
- わかりやすいデータ販売の停止受付機能の提供を義務化。
- 侵害時の罰則を強化。法定損害賠償金：一人当たり100～750米ドル又は実損のいずれか大きい額の賠償。

対象となる事業者

- カリフォルニア州民を対象とする営利企業で、かつ以下のいずれかの条件に当てはまる者に限定している。
  - 年間売上が2,500万ドルを超える
  - 消費者、世帯、端末あわせて5万以上の個人情報を購入、商業目的で受領、販売又は商業目的で共有する
  - 年間売上の50%以上を個人情報の販売から得ている

CCPAでは、第三者提供に対して、オプトアウト、オプトインの対象行為が示されている。

■ オプトアウト

- 事業者は消費者がオプトアウトできるよう、以下の事項を行わなければならない。

- “Do not sell my personal Information”というタイトルのWebページ上に消費者がオプトアウトすることができるページへのリンクを設けること
- オンライン上のプライバシーポリシー等の中にオプトアウトの説明と上記“Do not sell my personal Information”Webページへのリンクを設けること

■ オプトイン

- 事業者は以下の場合を除き、16歳未満の消費者の個人情報を販売してはならない。
- 13歳以上16歳未満のものについては本人から明確な意思による（affirmatively）同意を取得した場合
- 13歳未満の消費者については親または保護者が同意した場合

個人情報保護法改正の方向性（ターゲティング広告）

第4節 データ利活用に関する施策の在り方　1．～4．略

5．検討の方向性　（1）～（4）略

（5）ターゲティング広告を巡る対応の在り方

○ ターゲティング広告については、現在広くインターネット広告で活用されている手法の代表例と言えるが、実態は非常に複雑かつ多様である。

○ 提供元では必ずしも個人情報でない場合であっても、提供先で照合可能な情報が保有され、個人情報になる可能性や、多様な機器・サービスから詳細な情報が集積的に統合され、特定の個人を識別でき個人情報と同値になる可能性等も考えられる。

○ ターゲティング広告のベースとなるウェブ技術は進化が著しく、本来、イノベーションを阻害することを避ける観点からも、まずは、自主ルール等による適切な運用が重要である。自主ルール等については、強制力や自主ルール等に参加していない者の存在など、一定の限界があるのも事実であるが、今後、可能な限り民間の自主性を活かしつつ、認定個人情報保護団体制度等を活用するなど自主ルールを執行可能な形としていくことを含め検討する必要がある。

○ クッキー等について、例えば、一定の要件に該当するものについて個人情報保護法上の個人識別符号とするなど、その位置付けを明確化することも考えられるが、クッキー等自体は、「識別子」としてセッション管理20を含め広範に用いられる技術であり、利用特性も多様であることから、現行法の規定に加えて、クッキー等をあえて個別に規律する必要性含め、慎重に検討する必要がある。

○ 一方、クッキー等であっても、会員情報等と紐付けられ特定の個人を識別できるような場合は、個人情報保護法上の個人情報として取り扱われる必要がある。しかし、事業者の中には理解不足と思われる事例も散見されるため、今後、委員会としても、実態を注視しつつ、適切に執行を行っていく必要がある。

出所）個人情報保護委員会「個人情報保護法いわゆる3年ごと見直しに係る検討の中間整理」（2019年4月25日）から抜粋

Facebookの「いいね」ボタン機能等に対して、個人情報保護委員会が行政指導。

■ 概要

- 個人情報保護委員会が2018年10月にFacebookに実施した指導の対象は3つあり、そのうちの1つが、外部サイトに設置されているソーシャルプラグイン「いいね」ボタンでのデータ収集に対するもの。
  - Facebookユーザーが「いいね」ボタンがリンクしてある外部サイトを閲覧すると、**当該ボタンをクリックしなくても自動的にユーザーID、アクセスしているサイトの情報がFacebookに送られ、Facebookの保有する利用者登録情報と紐づけられる**。
  - 情報の送信は、ユーザーが**Facebookアカウントを有しているかどうか、Facebookにログインしているかどうかにかかわらず**行われる。
- 個人情報保護委員会は、①ユーザーへの分かりやすい説明の徹底、本人の同意の取得、本人からの削除要求への適切な対応、②Facebook上で第三者が開発したアプリの活動状況の監視等の徹底を指導。

■ 「いいね」ボタンの設置状況

- 「いいね」ボタンは国内の公的機関や企業をはじめ、医療情報サイトなどにも設置されている。
  - 読売新聞によると、フェイスブックの「いいね」「シェア」「ログイン」は、2018年1月末で全国上場企業の売上高トップ100社のうち半数以上で確認された。外務、財務、農水省、警察庁などの公的機関や、アダルトサイト、医療情報サイト、患者らが病状をつづる「病気ブログ」でも多数設置されているという。
- ユーザーは、どのサイトに「いいね！」が設置されているか、ページを閲覧するまで分からず、閲覧するとその瞬間に情報が送信されるため、拒否できない状態にある。

出所）個人情報保護委員会「フェイスブックインクに対する指導について」（2018年10月22日）、東京読売新聞「「いいね！」ボタン設置サイト　閲覧だけで「個人情報」送信」（2018年2月25日）を参考に作成

Facebookのデータに関するポリシー

外部サイト設置の「いいね」ボタンについて

パートナーからの情報

広告主、アプリ開発者およびパブリッシャーは、利用しているFacebookビジネスツール(ソーシャルプラグイン(「いいね！」ボタンなど)、Facebookログイン、弊社のAPIとSDK、Facebookピクセルなど)を通じて、弊社に情報を送信することができます。これらのパートナーが提供する情報には、利用者のFacebook外におけるアクティビティに関するものが含まれます。これには利用者のデバイス、訪問したウェブサイト、購入履歴、閲覧した広告、パートナーのサービスの利用状況が含まれ、利用者がFacebookアカウントを保持しているかどうか、またはFacebookにログインしているかどうかに関わらず提供されます。例えば、ゲーム開発者が弊社APIを使用して利用者がどのゲームをプレイしたかを弊社に送信したり、事業者が自社ストアにおいて利用者が行った購入について弊社に情報を提供したりすることがあります。また、利用者のオンライン・オフラインアクションについて、および利用者の情報を弊社に提供する権利を有するサードパーティーデータプロバイダーからの購入についての情報が弊社に提供されます。

利用者がパートナーのサービスを訪問、利用した場合、またはパートナーが連携する外部パートナーを通して、パートナーは利用者のデータを受け取ります。これらのパートナーが弊社にデータを提供する前に、パートナーが利用者のデータを取得、利用、共有する正当な権利を有していることを弊社は当該パートナーに要求します。弊社がデータを受け取るパートナーの種類について、詳しくはこちらをご覧ください。

弊社がFacebookビジネスツールに関連してCookieを利用する方法について、詳しくはFacebook Cookieポリシーおよび Instagram Cookieポリシーをご覧ください。

出所）https://ja-jp.facebook.com/privacy/explanation（2019年1月確認）

利用者のデータ管理、オプトアウトについて

Facebookはデータプロバイダーとどのように連携していますか。

記事をシェア

Facebookは厳選したサードパーティのデータプロバイダーと協力して、広告主様が自社の製品やサービスに興味を持つ可能性の高いターゲットを探すお手伝いをしています。このようなパートナーとの連携では、プライバシーに十分に配慮しています。Facebookのサービスの利用者は、表示される広告を管理できます。

現在多くの企業がAcxiom、Oracle Data Cloud (旧名称: DLX)、Epsilon、Experian、Quantiumといったサードパーティと協力してマーケティング活動を展開しています。たとえば、自動車ディーラーが新車を購入しそうなターゲットに向けたキャンペーンを検討しているとします。さらに、過去に購入した既存の顧客に向けては、メンテナンスサービスの割引キャンペーンを周知したいと考えています。このような場合に、適切なキャンペーンで適切な顧客にリーチするためにサードパーティ企業を利用します。サードパーティパートナーは、キャンペーンでリーチする顧客を見きわめるための情報をFacebookに提供します。

Facebookは、データプロバイダーの情報をもとにターゲット層を作成する際にターゲットとなった利用者がその状況を理解し、変更できるよう対策を行っています。Facebookが特に力を入れている取り組みをご紹介します。

透明性。 Facebook広告が表示されたときに、ドロップダウンメニューをクリックして[この広告が表示される理由]を選択できるようになっています。 これにより、その広告が表示される理由を説明するページに移動します。パートナーからFacebookに提供された情報に基づいてターゲットに設定されたのかもわかります。

管理。 広告に関連づけられたドロップダウンボックスで、その広告を表示しない、またはその広告主からの広告を表示しないといった選択ができます。 データプロバイダーのウェブサイトでも、Facebookとの合意に基づくオプトアウト用フォームが提供されています。必要に応じて以下を参照してください。

出所）https://www.facebook.com/help/494750870625830（2019年1月確認）

EU

欧州司法裁判所は、Facebook「いいね」ボタンを設置した企業においても応分の責任があると判断。

■ 概要

- 欧州司法裁判所は、Facebookの「いいね」ボタンを設置している企業は、**ウェブサイトに訪れたユーザーのパーソナルデータを収集して、Facebookに送信している点で、Facebookとデータの共同管理者になり得る**ことを示した。
- 判断の理由は、ボタン設置企業は、Facebookとともに、データ処理の利用目的を決定しうる立場にある。とりわけ、ボタンが押されると、Facebookネットワークを通じて、自社製品・サービスのパブリシティを向上することができ、商業的利益を享受できるから。
- ただし、Facebookへ送信後のデータの取扱いまでは、原則、責任を負わないとした。

■ 考察

- EUにおいて、Facebook「いいね」ボタンをウェブサイトに設置する企業は、今後、消費者にデータ処理に係る情報提供と同意の取得が求められることになる。
- 日本の個人情報保護法では、Facebookへ送信される情報（ユーザID、閲覧履歴）そのものは、「いいね」ボタン設置企業において非個人情報であり、ボタン設置企業の責任は問われていない。
- 非個人情報であっても、提供先で個人情報と紐づけられる可能性が高い場合は、提供元の企業においても、プライバシー保護の観点からユーザーへの配慮が求められるのではないか。

出所）Court of Justice of the European Union” The operator of a website that features a Facebook ‘Like’ button can be a controller jointly with Facebook in respect of the collection and transmission to Facebook of the personal data of visitors to its website”（2019年7月29日）をもとに作成

課題　－今後の議論に向けて－

1. **どのような事業者に情報が渡っているのか、消費者が認知できていない**
   - スマートフォンが普及し、ITリテラシーを問わず消費者がネット利用を行うようになった反面、どのような仕組み・情報をもとに広告や宣伝のアプローチが行われているのか認知していない消費者が増えている。
   - 利用規約も消費者目線で読みやすく、かつ理解できる内容になっているとはいい難く、読み飛ばして同意している消費者が多い。

2. **多様な機器から収集したデータが統合されると、個人の識別性や機微性が高まる**
   - スマートフォンやPC、ネットに接続された家電等から収集するデータを統合して、ターゲティング広告の精度等を高める取組（クロスデバイストラッキング）では、個人の識別性や機微性が高まる。
   - 米国では、透明性の確保、ユーザーへの選択機会（オプトアウト）の提供等の自主ルールを策定して運用。ただし、更なる取組が求められている。

3. **提供先で照合可能な情報が保有されていた場合、非個人情報として提供した情報が、個人情報に変わる**
   - Facebook「いいね」ボタンに象徴されるように、非個人情報として提供したデータが、提供先で個人情報と照合されて利用される場合がある。
   - 非個人情報を受け取って、個人情報と照合して利用する場合、プライバシーポリシー等で明示することが望ましいが、多くの日本企業では未対応と推測される。プラットフォーマーへますますパーソナルデータが集中する結果となり得る。


NRI
未来創発
Dream up the future.