基礎研レポート

「データの時代」と「プライバシーの時代」の両立

欧州、米国カリフォルニア州、日本におけるクッキー規制

立教大学ビジネススクール 大学院ビジネスデザイン研究科 教授
ニッセイ基礎研究所 客員研究員　田中 道昭

要旨

1. 現在、顕在化しているデジタル化の問題の一つが、個人情報保護やプライバシーを巡る問題意識である。デジタル・プラットフォーマーは、ユーザーの膨大な個人データを蓄積し、それをユーザー・エクスペリエンスの向上や新サービスの開発に生かしてきた。ユーザーも、自分のデータを提供する見返りとして、無料のサービスなど様々な恩恵を受けてきた。しかし、個人情報がどう使われているのかユーザーに対し不透明であることやプライバシー侵害のリスクなどの観点から、欧米では個人情報保護がさらに強化される傾向にある。

2. 欧州の一般データ保護規則（GDPR）、米国カリフォルニア州の消費者プライバシー法（CCPA）、日本の2020年改正個人情報保護法といった個人情報保護をめぐる法制度が厳格化されている。ここでの重要なポイントが「クッキー規制」の強化である。クッキーは、ユーザーがインターネット・ブラウジングをする際利便性を向上させる機能を持つ一方、プライバシー侵害のリスクやセキュリティに関する弊害をもたらすリスクをはらんでいる。これらリスクを背景とした「クッキー規制」の強化を通して、クッキーは個人情報として扱われるようになってきている。

3. 「クッキー規制」の強化によって大きな影響を受けているのは、デジタル広告にかかわる広告代理店やアドテック・ベンダーなど広告業界である。アドテック・ベンダーは、ターゲティング広告のためにクッキー（「サードパーティクッキー」）に依存してきた。しかし、「クッキー規制」の強化によって、クッキーを含む個人情報の第三者提供、利用・取扱いが法律上制限される。クッキーの取扱いに規制がかかれば、リターゲティング広告の精度は落ち、それに依存してきたこれまでのアドテック・ベンダーのビジネス手法は困難になってきている。

4. 「今後、クッキーはどうなるのか」について、５つに整理することができる。第一に、クッキー

は法令上個人情報として取り扱われる。第二に、デジタル広告業界がこれまでターゲティング広告に利用してきたクッキー（「サードパーティクッキー」）の利用が法令上制限される。第三に、ユーザーのブラウザレベルでトラッキング認定されるクッキーを無効化するトラッキング防止が浸透することから、法令上だけでなく技術上も、デジタル広告から「サードパーティクッキー」が締め出される。第四に、ユーザーが訪問するWEBサイトが直接発行するクッキー（「ファーストパーティクッキー」）や事業者による個人データの取得、利用、取扱いについてユーザーが明確に同意したデータ（「０パーティデータ」）が重視され、ユーザーと事業者間の「継続的で良好な関係性」がより重要となり、メディアと広告の関係に変化が生じる。そして第五に、「サードパーティクッキー」に依存しないデジタル広告の手法が使用されるようになる。

5. CES2020でパネルディスカッション『チーフプライバシーオフィサー・ラウンドテーブル：消費者は何を求めているのか？』が開催され、アップルとフェイスブックのチーフプライバシーオフィサー、連邦取引委員会のコミッショナーらが登壇した。そこでは、プライバシー保護へ積極的に取り組んできたアップルでさえも、プライバシーや個人情報保護に関して厳しい目を向けられた。プライバシー保護やその規制強化の流れはもはや不可逆となってきており、アップル、グーグルらデジタル・プラットフォーマーは今後さらなる厳しい目にさらされることになるであろう。

6. 「データの利活用」と「プライバシー重視」を両立させなければならない時代が到来している。このような中で日本がとるべき対応は、「データの利活用」「プライバシー重視」の状況を冷静に分析し、より的確な答えを見出だしていくことである。そして、むしろ後発の利益を意図的に享受するような、さらにはその両立において世界をリードするような戦略的な動きをとっていくべきである。

1――デジタル・プラットフォーマーと顕在化するデジタル化の弊害

1｜「デジタル化されたものは破壊される」

デジタルトランスフォーメーション、デジタルシフト、デジタル資本主義―。近年、「デジタル」を鍵とする経済・ビジネスのキーワードが増えてきている。デジタルは２０２０年代で最も重要な概念の１つと言ってもよいだろう。

なぜ、デジタルがこれほどまでに重要な概念となったのか。その答えは、デジタル・プラットフォーマーと言われるＧＡＦＡ（米国のグーグル、アップル、フェイスブック、アマゾン）やＢＡＴＨ（中国のバイドゥ、アリババ、テンセント、ファーウェイ）といった米中メガテック企業が示している。彼らの特徴は、特定の商品・サービスだけで収益を上げようとしていないことである。それぞれの事業領域でデジタル・プラットフォームを構築し、様々な商品・サービスやコンテンツ、ビジネスやシステムをその中に取り込みながら、「エコシステム全体」での成長を図っている。

デジタル・プラットフォーマーは、「大胆なビジョン×高速ＰＤＣＡ」のビジネス手法でも共通している。彼らのビジネスは、まず大胆なビジョンを打ち立てることから始まる。次に、そのビジョンから逆算する形で「今日何をするべきか」を明確化。そして、高速のＰＤＣＡサイクルを回し、生産性や効率を高めながらビジョンの実現にむかって邁進していく。言い換えれば、超長期思考とスピードの掛け合わせである。これによりイノベーションを何度も起こし、爆発的に成長していく。

また、この時に重要視されるのが「スケーラビリティ（拡張性）」である。「大胆なビジョン×高速ＰＤＣＡ」による爆発的な成長力を存分に生かせるのは、それだけの成長が見込める余地のある事業、つまりはスケーラビリティのある事業に限られる。したがって彼らは、そもそも拡張性のない事業には手を出そうとしない。結果として、デジタル・プラットフォーマーの成長曲線は似通ったものになっている。当然ながら、スタート時はごく小さな事業である。しかし、ひとたび軌道に乗ると、倍々ゲームのように伸びていく。１、２、３、４といったリニア（線形関数的）な成長ではなく、１、２、４、８といったエクスポネンシャル（指数関数的）な成長である。

ひとたびエクスポネンシャルな成長が始まれば、競合となるプレーヤーを含めて関連業界や企業が破壊的な影響を受けることになる。アマゾンの台頭により、書店をはじめとする多くの小売業者が閉店に追い込まれたことが、その典型例である。デジタル・プラットフォーマーが示しているのは、次の２つである。「デジタル化」されたものは、エクスポネンシャルな成長を遂げること。そして「デジタル化」は「破壊」をもたらすこと。こうしてデジタル化は、現代社会に大きな影響を与えることになったのである。

2｜「データの利活用」と「プライバシーの保護」を両立させる

しかし今、こうしたデジタル化の流れが岐路に立たされている。デジタル化の弊害が顕在化してきている。その弊害の１つが、個人情報保護の問題である。

デジタル・プラットフォーマーはこれまで、ユーザーの膨大な個人データを蓄積し、それをユーザー・エクスペリエンスの向上や新サービスの開発に生かしてきた。データこそ、彼らにとって最大の武器である。またユーザーも、自分のデータを提供する見返りとして、無料のサービスなど、様々な恩恵を受けてきた。しかし、個人情報がどう使われているのかユーザーに対し不透明であること、またフェイスブックが最大8700万人にものぼる個人データを流出させた事件が象徴するようにプライバシー侵害のリスクがあることなどを受けて、世界はにわかに個人情報保護に傾いている。

欧州では一般データ保護規則（GDPR）が、米国ではカリフォルニア州消費者プライバシー法（CCPA）が施行され、日本においても個人情報保護法の改正が６月に国会で可決した。すなわち、「データとプライバシーの両立」という潮流が起きているのである。

アップルとグーグルは、４月10日付けプレスリリースにおいて、両社が新型コロナウイルス対策として濃厚接触の可能性を検出するテクノロジーで協力するという取り組みを発表した。新型コロナウイルスの感染者と濃厚接触した可能性があるユーザーにスマートフォンで通知するという仕組みで、アップルの「iOS」とグーグルの「アンドロイドOS」の間で相互に運用が可能とされている。アップルとグーグルによるOSでの協業は世界中のほとんどのスマートフォンを対象としており、感染の監視においては高い実効性が期待できる。しかし、個人情報にかかわるビッグデータを持つメガテック企業同士の連携ということでは、プライバシーに関する懸念が残る。

今、アップル、グーグルとも、新型コロナウイルスの感染拡大への対応を契機として、また世界的に影響力の大きいデジタル・プラットフォーマーだからこそ、否応なく「データの利活用」と「プライバシーの保護」という相反する命題に、より高いレベルで対峙することが迫られている。

2――「データの時代」と「プライバシーの時代」の両立

1｜欧州・米国・日本で「クッキー規制」が強化されつつある

個人情報保護をめぐる法制度の厳格化が、世界各地で相次いでいる。欧州の一般データ保護規則（GDPR）、米国カリフォルニア州の消費者プライバシー法（CCPA）、日本の改正個人情報保護法、という３つの法律である。これら法律は「クッキー規制」とも総称される。

まず、クッキーに関する基本的な考え方を押さえておきたい。正式名称は「Cookie」。ユーザーがいつ、どのサイトを見たのかといった閲覧履歴やパスワード・ＩＤなどログインに関するデータを一時的に保管する仕組みや、ユーザーのブラウザと閲覧サイトのドメインの間でそのようなデータをやりとりする仕組みのことを指している。クッキーはユーザーがアクセスしたサイトからユーザーのブラウザに送られ、保存される。

クッキーには、大きく２つの利用法がある。１つはユーザーの利便性向上で、例えば一度訪れたサイトではＩＤやパスワードの入力を省略できるのはクッキーが機能するからである。

もう１つの利用法が広告である。クッキーをもとにユーザーの価値観や性格、行動パターン、趣味などを推測することで、最適化された広告を配信できる。しかも、あるサイトで自転車を検索したあと別のサイトに移動したらそこでも自転車の広告が表示された、といったことも起こる。このようなことが起こるのは、クッキーが２種類存在するからである。１つは、ユーザーが訪問したサイトのドメインから発行される「ファーストパーティクッキー」である。これは、そのサイト内でのみ使用できるもの。もう１つは、ユーザーが訪問したサイトとは別のドメインから発行されるクッキー、通称「サードパーティクッキー」である。サードパーティクッキーは複数のサイト間で共有することができるため、そこから、複数のサイトにまたがったユーザーの行動や興味をデータとして収集し、より精度の高い広告につなげることができる（図１参照）。その限りでは、クッキーの利用にはメリット

のほうが多いようにも感じられるかもしれない。クッキーのおかげで個人は興味のない広告を見ずに済み、広告主はムダな広告を減らせるのですからである。

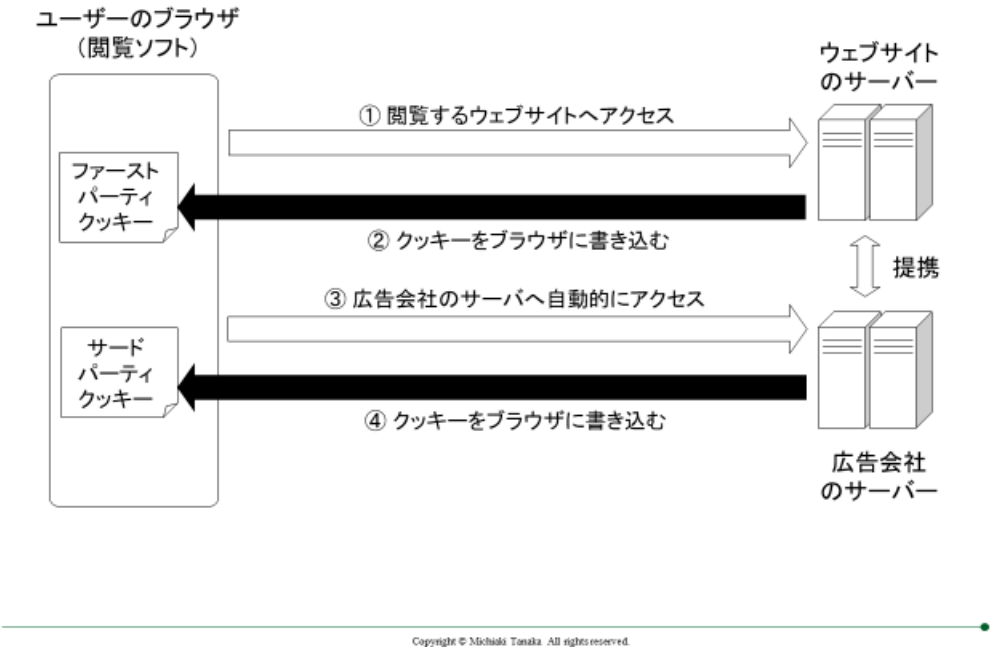

図１　クッキーの仕組み（筆者作成）

しかし、クッキー規制とはその名の通りクッキーの利用に制限をかけようとするものである。それは何故か。クッキーの利用が個人の特定につながる危険、つまり、プライバシーが侵害される危険をはらんでいるからである。

訪問したウェブサイトで広告バナーが表示される時、その広告をクリックした時、ユーザーが使っているブラウザは、広告配信サーバーから発行されたサードパーティクッキーを受け取っている。広告業者は、サードパーティクッキーを発行することでユーザーのネット上の行動を勝手に追跡（トラッキング）しているのである。

そのことをユーザーが意識することはまずない。クッキー自体は氏名や住所を含んでおらず、広告業者も、そこから年齢層や興味などを推定し、ユーザーの趣味や嗜好にマッチしそうな広告の配信に利用するのみであり、個人を特定するものではない。しかし現実には、クッキーと他のデータとを突き合わせることで個人が特定できてしまうこともあり得る。さらに、クッキーは、ユーザーのログイン状態が不正に再現されてしまったり、ユーザーが意図しないブラウザの不正操作（クロスサイトリクエストフォージェリー）が行われたりする、セキュリティに関する弊害をもたらすリスクもはらんでいる。

従来、クッキー単体で個人情報と見なされることはなかった。しかしクッキーに限らず、個人情報の保護はインターネットの拡大とともに注目されるようになった。プライバシーの権利は、日本国憲法第13条で規定された「幸福追求権」に含まれると考えられる基本的人権の１つであり、特にEUは常に世界の先頭に立ってプライバシー保護を推し進めてきたという歴史的な経緯もある。クッキー規制にかかわる法制度の厳格化は、このような背景から始まった。クッキーによる個人の分析や特定を規制すること。クッキーを収集するなら、使用目的を説明し、ユーザー本人の同意を得ること。そのような内容が中心になっている。

<table>
<tr><td colspan="2">主な比較項目</td><td>【欧州】
一般データ保護規則
（GDPR）</td><td>【米国カリフォルニア州】
消費者プライバシー法（CPA）</td><td>【日本】
個人情報保護法</td></tr>
<tr><td colspan="2">目的・理念</td><td>基本的権利としての個人データ保護の権利を保護</td><td>個人情報にかかわる消費者の権利を新しく創る</td><td>個人情報の有用性に配慮し、個人の権利利益を保護</td></tr>
<tr><td rowspan="5">何が個人情報として扱われるのか？</td><td>氏名や
個人識別番号</td><td rowspan="5">個人情報
として扱われる</td><td rowspan="5">個人情報
として扱われる</td><td>個人情報として扱われる</td></tr>
<tr><td>オンライン識別子
（IPアドレスなど）</td><td rowspan="4">個人情報
として扱われない</td></tr>
<tr><td>検索履歴や
閲覧履歴</td></tr>
<tr><td>クッキー</td></tr>
<tr><td>位置情報</td></tr>
<tr><td colspan="2">個人情報の第三者提供
における同意手続き</td><td>オプトイン</td><td>オプトアウト
（未成年者はオプトイン）</td><td>オプトイン
（条件付オプトアウト規定あり）</td></tr>
</table>

図２　欧州、米国カリフォルニア州、日本の個人情報に関する法制度の比較（筆者作成）

2｜【欧州】一般データ保護規則（GDPR）

一般データ保護規則（GDPR）は欧州が2016年４月に採択、2018年５月に施行した法律である。厳密には1995年にデータ保護指令という通達があり、この通達を法律にしたものがGDPR、という位置づけである。GDPRの対象国は、EU27カ国にノルウェー、アイルランド、リヒテンシュタインを加えた「欧州経済領域（EEA）」の30カ国。欧州データ保護会議という機関が、各国の機関と連携している。その目的や理念については「基本的権利としての個人データ保護の権利を保護」「個人データのEU域内の自由な移動」と、法律の目的条項のなかに書かれている。

GDPRが採択された経緯について、インターネットイニシアティブ（IIJ）の鎌田博貴氏は次のように解説している。

「今回のGDPRも保護指令も、個人データの取得や利用には一定の法的な根拠が必要であり、透明性、公正性を原則とするというのは同じですが、保護指令はＥＵ加盟各国が個人データ保護のための国内

法を制定するための指針という位置付けであり、実際に制定された国内法の内容は国によって差異がありました。EUには、国境に関係なくヒトやモノや資金を移動できるシングルマーケットという理念があります。保護指令をガイドラインとした国内法の内容が各国バラバラであったため、EU全域を舞台とする多国籍企業の活動に不便が生じていました。そこで、国内法の手続きを経ずに加盟国で適用できるようなＥＵの法律を定めようという機運が高まり、GDPRが生まれました。もう１つは、インターネットの浸透度です。95年というのは、民間企業や一般市民が通信手段にインターネットを使うようになった時期です。その後20年ほどたち、われわれの生活はインターネットなしでは成り立たなくなり、取り扱われる個人データの質や量、生活に及ぼす影響も95年とは比べものにならないほど大きくなっています。さらに昨今では、AI（人工知能）やIoTなどにより、暮らしの中に情報通信がさらに入ってきています。そのような状況を前提とした新しい規則が必要になったわけです」（2018年８月１日IT Media News）

GDPRでは、事業者に対して個人データの取扱い目的などをユーザーへ知らせることが義務化された。そもそも、商品・サービスの開発に際してプライバシー保護を前提にしなければいけない（バイ・デザイン、バイ・デフォルト）ことが定められている。一方、消費者に対しては、個人データへのアクセス権、個人データの取扱いを制限させる権利、データポータビリティの権利（あるプラットフォーマーから別のプラットフォーマーへとデータをそのまま移行する権利）を保障している。

GDPRの大きな特徴の１つは、「オプトイン」といって、事前に個人データの所有者の同意がなくては利用してはいけない原則があることである。つまりGDPRにはまず「個人情報は利用させない」という前提がある。そのため事業者はあらかじめ個人に対し、何の目的でいつまで使うのか、といった情報を提供し、個人からの同意を得なければならない。最近、ウェブサイトにアクセスするとまず、クッキー使用の同意を求めるポップアップが表示されることが増えてきたのは、ここに発端がある。

また個人は企業に対し、個人情報の消去を請求できる権利を持つ。これは通称「忘れられる権利」と呼ばれる。一度でもインターネット上で個人情報が拡散してしまうと、それを削除するのは個人の力では不可能。それにより精神的な苦痛を味わったり、その後の生き方に悪影響を受けたりする危険がある。しかしGDPRは個人に対し、企業に対し個人情報を遅滞なく削除することを要求できる、とした。こうした規制に違反した事業者は、違反内容によって「1000万ユーロまたは世界全体での売上高の２％の高い方」あるいは「2000万ユーロまたは世界全体での売上高の４％の高い方」の制裁金が科せられる。2000万ユーロなら日本円にして25～26億円、大変に重い刑罰だと言えよう。

GDPR、CCPA、日本の個人情報保護法では個人情報の定義が異なっている。GDPRのもう１つの特徴は、IPアドレスやクッキーなども個人情報と見なす点である。GDPRが個人情報と定義するものは何か。名前や住所、メールアドレスなどは、当然個人データとして扱われる。「物理的、生理的、遺伝子的、精神的、経済的、文化的、又は社会的なアイデンティティから識別される情報」も個人情報とされる。ここで重要なのは、IPアドレスやクッキーなど、単体では個人の特定が不可能でもほかの情報を組み

合わせることで個人の識別につながると考えられる情報を個人情報と見なしている点である。既述の通り、クッキー自体は個人を特定する情報ではないが、その人のネット閲覧履歴が蓄積されていけば、性格や趣味など、誰にも知られたくない深いところまで把握されるおそれがある。

位置情報も同様に、個人情報として扱う。いつ、どこにいることが多いのかという情報のことである、その時間帯や頻度から自宅や職場を特定することは、さほど難しいことではない。

規制の対象となるのは、どのような企業か。EUで成立した法律であるが、日本国内の企業にも影響を及ぼすことがある。EU域内でビジネスを行い、EU域内の個人の個人情報を扱うすべての組織に適用される。そのためEU域内に子会社を持つ日本企業はもちろんのこと、そのような拠点を持たなくても、EU域内にいる個人に対して商品やサービスを提供している場合や、EU域内の個人の行動を監視する場合には、日本企業であってもGDPRが適用される。

GDPRによる取締はすでに始まっている。2019年１月にはフランスのデータ保護監督機関「CNIL」がグーグルに対し、5000万ユーロの制裁金の支払いを命じた。CNILによると、ターゲット広告のためのデータ収集に関しての説明がわかりづらい、「データ収集に同意する」という項目にあらかじめチェックマークが入っていることはオプトインの原則に違反する、また収集したデータの利用方法や保存期間の説明も簡単には見つけられないことなどが問題視された。

欧州についてはもう１つ、ｅプライバシー規則という規制が話題にのぼる。ｅプライバシー規則は2017年１月に欧州委員会が提案したもので、まだ採択はされていないが、採択の方向で動いている。

ここでも、ウェブサイト運営事業者が、利用者の閲覧履歴やウェブ上の行動履歴などを含んだクッキーを活用する場合には、利用者の同意を求めることになっている。ｅプライバシー規則もGDPRと同じく欧州経済領域の30カ国が対象である。しかも個人情報の扱いを定めるものであり、両者にどういった違いがあるのか、わかりにくいかもしれない。しかし日本で言うなら、民法と会社法がそうであるように、GDPRが一般法なら、ｅプライバシー法は特別法。GDPRに比べてｅプライバシー規則はより広く細かく、個人情報を規制するものとイメージしてよいだろう。欧州委員会の資料によるとGDPRが保護するのは「すべての個人データ」、一方ｅプライバシー規則は「電気通信とデバイスにおける秘密性」と定義されている。

3｜【米国カリフォルニア州】消費者プライバシー法（CCPA）

EUにGDPRが導入されただけでもネット上での個人情報の扱いはかなり厳しくなったが、続いて米国カリフォルニア州で施行された消費者プライバシー法（CCPA）が、それに拍車をかけた。

消費者プライバシー法は、米国カリフォルニア州が2018年６月に採択、2020年１月１日に施行したものである。米国ではこれまで、個人情報保護に関する包括的な規制がなく、医療や金融など事業分

野ごとにルールがあるのみであった。「州法策定のきっかけとなったのは、州内の不動産業者が始めた住民立法の運動だ。18年３月に発覚した米フェイスブックにおける最大8700万人分の個人情報の不正流用事件の影響で、この運動が60万を超える署名を集めたことが圧力となり、18年６月に州議会が住民立法に代わる法案を可決した」（2019年10月15日　日本経済新聞）

CCPAはカリフォルニア州の司法省が管轄する。CCPAの理念について司法省は「個人情報にかかわる消費者の権利（アクセス、削除、共有など）を新しく創る」と謳う。具体的な規制としては、事業者に対して個人情報の種類や利用目的などを知らせることを義務化した。また消費者の権利として、個人情報に関する開示請求権、また個人情報を売却しないように指示する権利を保障した。CCPAにより規制の対象になるのは、カリフォルニア州で事業を行い、カリフォルニア州民の個人情報を収集し、以下の３つのうちいずれか１つの要件に該当する営利目的の法人である。カリフォルニア州に拠点を持たない日本企業であっても、対応が必要になる可能性がある。

①年間の総収入（annual gross revenues）が2500万ドル以上である
②５万人以上のカリフォルニア州民の個人情報を処理している
③カリフォルニア州民の情報を売却することで年間の収入の50％を得ている

CCPAに違反した場合は、司法長官による民事制裁金（１件2500ドル）、差止め、損害賠償請求（民事、違反１件につき消費者１人100ドル以上750ドル以下または実損害のうち大きい方、クラスアクション可）などの罰則がある。１件あたり日本円にして25～26万円、積み重なれば巨額であり、大規模な集団訴訟にまで拡大するリスクがある。企業に対して個人情報の消去を請求できる「忘れられる権利」を定めていることや、クッキーと位置情報を個人情報として扱うなど、CCPAとGDPRは似ているが、違いも多くある。例えば、個人情報の収集や利用そのものを原則的に認めている点が、GDPRと明確に異なる。というのも、GDPRは「オプトイン」であったが、CCPAは「オプトアウト」。個人データは初期設定では「使っていい」、しかし「使わないでほしい」と個人が指示すれば後から個人データの利用を禁止できる、どんな使われ方をしているか開示請求ができる、という立て付けになっている。ただし18歳未満の未成年者はオプトインが原則となっている。また、個人情報の定義についても、個人だけではなく世帯を特定できるデータが個人情報の対象となる点はGDPRと異なっている。

カリフォルニア州はこれまで、自動車の燃費基準など米国のなかでも厳しい規制を導入してきたことで知られている。今回のCCPAを受けて、ほかの州が追随する動きも出てこよう。CCPAが定める個人情報には世帯情報も含まれているなど、その意味ではGDPRよりも広い規制だと考えることもできる。

一方で、企業の対応は遅れている。GDPRの施行にあたっては２年間の準備期間があったのに対し、CCPAは手続きに手間取り、執行規則はようやく19年10月に公表された。そのため日本企業の対応も後手に回っている。

「同州で５店舗を運営する眼鏡専門店のジンズホールディングスは19年８月期の連結売上高が618億円だったが、昨年12月の時点で『顧問弁護士と協議し対象企業に該当しない』との認識。その後20年１月になり『該当する可能性が高い』と対応が揺れた。CCPAは事業者の範囲として共通のブランドを持つ場合も含まれるとしており、資本関係がないメーカーと販売代理店の間でやりとりされる個人情報についても規制対象となる可能性がある。例えば、車の所有者の情報をマーケティングなどの目的で使うためにメーカーが販売店と共有した場合には法が適用される見通し。同州の乗用車市場でシェア首位のトヨタ自動車は『保持する個人情報に関する包括的なレビューを実施している最中だ』としている。CCPAがモデルにしたとされるEUの一般データ保護規則（GDPR）に対応していてもそれが十分とは限らない。CCPAが定める個人情報は世帯情報も含まれGDPRよりも幅広い。米国で事業を展開するメルカリは『影響範囲に不透明な点があることから、注視しながら継続的に対応していく』と話す。州司法長官による罰則規定の執行が始まるのは20年７月になると見込まれている。民事訴訟の可能性など細かな規定をめぐっては専門家の間でも意見が割れており、厳密な法解釈は今後の裁判などを通じて判明する見通し。他州もその動向をうかがうCCPAは、多くのグレーゾーンを抱えたまま運用が始まることになる」（2020年１月９日　日本経済新聞）

実際、2020年２月３日、CCPA違反を含むデータ侵害を理由にして、顧客情報管理サービスを提供するセールスフォースとそのサービスを利用する子供服販売のハンナ・アンダーソンに対する集団訴訟がカリフォルニア州で提訴された。CCPAに関係する初めての案件であり、その審理の行方が注目される。

4｜【日本】個人情報保護法

規制内容の細かい違いはあっても、個人情報を第三者にわたすことについて厳しく規制するのが世界共通の傾向である。日本では、2002年に住基ネットの運用が始まったのを機に、2003年５月に個人情報保護法が成立し、2005年４月１日に施行された。目的条項には「個人情報の有用性に配慮しつつ、個人の権利利益を保護する」と書かれている。2017年５月には改正個人情報保護法が施行され、個人情報の定義が拡大、かつ明確になった。従来個人情報保護法では「個人情報＝個人を特定する情報」とされてきたが、その解釈が広くなり、例えばマイナンバーなども個人情報に含まれるようになっている。

個人情報保護法では、個人情報を取り扱う企業はその利用目的をできる限り特定しなければならないことなどが定められている。本人の同意を得ないまま、利用目的を超えて個人情報を取り扱ってはならない。個人のデータを第三者に提供する場合は、原則としてあらかじめ本人の同意を得なければならない、つまり「オプトイン」が条件となっている。個人が企業の保有するデータの利用停止や削除などを請求できる権利は、企業が個人情報を不正に取得した場合や、目的外に個人データを使ったりした場合に限られる。企業が第三者提供の停止の請求に応じる義務も、個人の同意を得ないなど違法に第三者に提供した場合に限定される。またクッキーや位置情報を、個人情報に含めていないところも、GDPRとCCPAとは異なる。そのほか、規制の内容や違反時の罰則・制裁金の額を見てもGDPRやCCPA

に比べて「ゆるい」規制であるのは明らかであり、「日本は個人情報保護において立ち遅れている」現状を如実に示している。

個人情報保護法は３年ごとに改正されるスタンスが取られている。2020年は改正の年にあたり、６月５日の参議院本会議における可決をもって改正個人情報保護法が成立した。

改正個人情報保護法において焦点になっているのは、2019年に起きた「リクナビ問題」の再発防止策である。リクナビ問題は個人情報保護におけるさまざまな論点を含んでいるため、問題の全容を整理してみたい。リクナビ問題とは、リクルートキャリア社が運営する就職情報サイト「リクナビ」が、リクナビを利用する約8000名の学生（就活生）に関して「内定辞退率」を予測したデータを顧客企業37社に販売していた問題を指す。リクナビ問題に際して、個人情報などの取扱いに関して監督を行う政府機関の個人情報保護委員会はリクルートキャリアに対して令和元年８月26日付けで「勧告」と「指導」を行った。

まず、ユーザーの同意を得ることなく顧客企業に就活生の個人情報を開示し、販売したこと、またそのような状況を放置していた管理体制の不備などが個人情報保護法に違反するとして、「個人データを取り扱う際に、適正に個人の権利利益を保護するよう、組織体制を見直し、経営陣をはじめとして全社的に意識改革を行う等、必要な措置をとること」などの勧告を行った。就活生はもちろん実名でリクナビに登録をすることから、個人を特定できる個人情報をリクナビに提供していることになる。内定辞退率はその個人情報に関連付けられており、個人情報保護法で保護される「個人情報」に該当する。同法では、個人情報を第三者へ提供する場合、本人からの事前同意の取得が義務付けられている。

また個人情報保護委員会は「指導」も行った。指導の対象は、就活生の同意はあったものの、本人への利用目的などの説明が実質的に不足したまま個人情報を外部に提供したこと。リクナビのプライバシーポリシーには、「このような目的で個人情報を開示することがあります」との説明があったが、その説明から内定辞退率のデータを提供するとは到底わからない、という理由からである。

もう１つ、リクナビ問題は、「独占禁止法違反の疑いがある」点も論点として挙げられる。具体的には「優越的地位の濫用」にあたるというものである。「優越的地位の濫用」とは聞き慣れない言葉かもしれない。ここでは、事前の同意や説明がないまま、リクナビが就活生からクッキーやオンラインでの行動履歴や閲覧履歴を収集し、ターゲッティング広告に利活用していることが問題視された。独占禁止法はもともとＢtoＢの取引が主たる対象であるが、GAFAなどに代表されるプラットフォーマーの影響力が増していることからプラットフォーマーとユーザー間、すなわちＢtoＣの取引も対象になってきている。「リクナビ問題」に関して「優越的地位の濫用」という概念は特にＢtoＣの取引を想定したもので、2019年には公正取引委員会からガイドライン『デジタル・プラットフォーム事業者と個人情報等を提供する消費者との取引における優越的地位の濫用に関する独占禁止法上の考え方』

が提出された。ここでデジタル・プラットフォーマーとされているのは主にGAFAであり、当初リクナビはデジタル・プラットフォーマーとは見なされていなかったが、「リクナビを使わざるを得ない就活生」が多い現状を鑑みると、就活生に対するリクナビもまた、優越的地位にあると見なされる。

加えて、リクナビからデータを購入した企業については「職業安定法違反の疑い」が指摘された。これは厚労省の管轄であるが、人材募集企業が応募者の個人情報を第三者から取得することは原則禁止されており、収集する場合は同意が必要という職業安定法上の規定に違反があったのではないか、という疑いがある。また購入企業にも、個人情報保護法違反の疑いがある。購入企業はリクナビと業務委託契約を結び、就活にかかわるコンサルもリクナビに外注していたが、自社が持つ就活生のデータを本人の同意なくリクナビに提供していた。ここでも論点になっているのは、本人の同意のないクッキーなどのデータの第三者提供である。クッキーは個人情報保護法においては個人情報にあたらない。しかし、就活生の個人情報を持つ第三者（リクナビ）の手にクッキーが渡れば、両者を突き合わせることで個人が特定できてしまう、ということなのである。

こうした「リクナビ問題」の現状もふまえ、2020年改正個人情報保護法の主なポイントは次の通りである。

まず企業の責務について、個人データの漏洩などが発生して個人の権利が害されるおそれがある場合、企業には個人情報保護委員会への報告と本人への通知が求められる。改正前はあくまで努力義務にとどまっていたが、改正後は義務となった。また、違法や不当な行為を助長するなどの不適正な方法で個人情報を利用してはならないことも法律上明確化された。

個人の権利について注目すべきは、個人データの利用停止や消去、第三者提供の停止に関する個人の請求権である。改正前は、企業が個人情報を不正に取得するなど、法律違反の場合に限ってこれら請求権が認められていた。しかし改正後はその要件が緩和され、個人の権利や利益が害されるおそれがある場合にも請求権が認められる。さらに、改正後は、個人データの授受に関する第三者提供記録の開示請求権も保障されることとなった。

一方で、データの利活用については、イノベーション促進の観点から、個人データから氏名などを削除、特定の個人を識別することができないように加工した「仮名加工情報」を創設、内部分析に限定することなどを前提条件に、開示や利用停止に関する個人請求権への対応義務を緩めた。プライバシーを重視するのと同時に、企業には個人データのビジネスへの利活用を促している。まさに「データの時代」と「プライバシーの時代」を両立させるという考え方である。

もっとも、提供元では個人データに該当しないものの、提供先では個人データとなることが想定される情報の第三者提供については、本人同意が得られていることなどの確認が義務付けられた。これは、先に述べたクッキーなどを念頭に置いたものと考えられる。「リクナビ問題」にもあったように、

クッキー自体は個人情報ではないが、他のデータと突き合わせることで個人が特定できてしまう場合、クッキーも個人情報として捉えられるというわけである。

ペナルティに関しては、個人情報保護委員会による命令違反や虚偽報告などの法定刑を引き上げること、データベースなどの不正提供罪や委員会による命令違反の罰金について、法人に対しては行為者よりも罰金刑の最高額を引き上げることなど、改正前よりも重い刑罰が規定された。

5｜米国アドテック・ベンダーの苦境

こうした一連のクッキー規制によって、顕著に大きな影響を受けているのは、広告代理店や種々のアドテック企業など、広告業界である。米国では、デジタル広告、リターゲティング広告などをリードしてきたアドテック・ベンダーの株価が下落したり、買収されたり、倒産するケースなども目立っている。

こうした米国のアドテック・ベンダーの苦境は、クッキーの取扱いに法的な制限がかかり、ターゲット広告にクッキーを利活用し難くなっていることが要因である。EUではGDPR以後は個人から先立ってクッキーの利用について同意をとらなければならない。米国でも現時点ではカリフォルニア州に限定されているが、連邦レベルでの個人データやプライバシー保護の法制化の動きもあり、プライバシー規制強化の流れは止められないだろう。

アドテック・ベンダーは、ユーザーが広告主などの事業者へ提供した個人情報を間接的に取得して、ユーザー毎へ最適な広告を提供してきた。しかし、GDPRやCCPAのもと、クッキーを含む個人情報の第三者提供、利用・取扱いが法律上制限される。クッキーの扱いに規制がかかれば、リターゲティング広告の精度は落ち、それに依存する事業ではジリ貧は明らかである。これまでのビジネス手法が困難になるということである。

個人も、これまで知らず知らずのうちに事業者にクッキーを利活用され、それにより恩恵を受けていたが、いざ「あなたの個人情報を利用させてください」と改めて問われると、躊躇したくなるというものであろう。もともと法制化前からクッキーの利活用に関する業界の自主規制もあり、関係企業は対策を施してきたが、これからは法律によって規制されることになる。

さらに、ユーザーが利用するブラウザにインテリジェント・トラッキング防止機能（ITP）が搭載されるなら、トラッキング認定されたクッキーは無効化されることになる。個人情報のデジタル広告への利活用が法的に規制される以前に、そもそも、ユーザー毎に最適な広告を配信するためのトラッキングに使われるクッキーが技術的に無効化されるわけである。アップルのブラウザ「サファリ」では、ITPがデフォルトでオンになっている。また、広告収入をビジネスモデルの基盤に持つグーグルも、2020年１月、今後２年以内に、ブラウザ「クローム」でネット閲覧履歴のデータが取得できるクッキーの利用を規制するとの計画を明らかにしている。このような要因でターゲット広告の精度が落ち、デジ

タル広告市場の急速な成熟化や過熱化とも相まって、アドテック・ベンダーは売上や利益が低迷、苦境に陥っている。

一方で、デジタル広告市場で新しい動きも出てきている。なかでも典型的なのはアマゾンによるSizmekのアドサーバー買収である。2019年はじめのSizmek倒産後、そのアドサーバーをアマゾンが買収した。Sizmekはデジタル広告のいわゆる第三者配信プラットフォームであり、さまざまな媒体へ最適な広告を配信する役目を担っていた。アマゾンがSizmekのアドサーバーを買収した理由は、広告主向けサービスである広告プラットフォーム「アマゾン・アドバタイジング」の強化と考えられる。

アマゾンは「ビッグデータ×AI」を広告へ活用、さまざまな広告サービスのメニューを取り揃えている。アマゾンの売上高に占める広告事業収入は４％程度と依然小さいが、その伸び率は他の事業セグメントと比較して突出している。

「アマゾン・アドバタイジング」は「アマゾンのDSP」機能も備え、アマゾン自身が持つユーザーの個人情報をもとに最適な広告コンテンツをさまざまな媒体へ配信する。DSPとは、広告主にとっての広告効果を最大化するプラットフォームのこと。最も有力なDSPといえば「グーグルのDSP」である「グーグルアドセンス」であるが、それと直接競合することになる。アマゾンは、デジタル広告市場の２大プレーヤーであるグーグルとフェイスブックに対抗していく可能性があると考えられる。

それでは、クッキー規制後に生き残る企業や広告があるとしたら、それはどのようなものか。第一には、クッキー規制の対象となっていないファーストパーティクッキーや、購買履歴やログイン情報といったユーザーの個人データを自ら蓄積している広告主と、それを利活用した広告である。彼らは、サードパーティクッキーに頼ることなく、ユーザーについての詳細なプロファイルを得ることができる。広告主はもちろん、グーグルやアマゾン、フェイスブックもここに含まれる。第二には、クッキーを含めた個人データを「ユーザーから意図的に提供してもらえる」企業と、それを利活用する広告である。キーワードは「０パーティデータ」である。

そもそも個人にまつわるデータは、これまで見てきたような「個人情報か、そうでないか」「ファーストパーティクッキーか、サードパーティクッキーか」といった複数の分類の仕方があった。そこにもう１つ、「ユーザーが意図的に提供したデータか、そうでないか」という軸を追加する。すると、次の４つに分類できる。

① 1stパーティデータ
ユーザーが訪問するWEBサイトが直接取得する個人データ。ファーストパーティクッキー、購買履歴、検索履歴などを含む。

② 2ndパーティデータ
ユーザーが訪問したＡ社が取得した１stパーティデータが、特定のＢ社へ提供されたもの。

③ 3rdパーティデータ

ユーザーが訪問するWEBサイト以外のサイトが間接的に取得する個人データ。サードパーティクッキーを含む。

④ 0パーティデータ

ユーザーが訪問するWEBサイトが個人データの取得、利用、取扱いについて、ユーザーから明確な同意を得たデータ。

１stパーティデータ、２ndパーティデータ、３rdパーティデータは、ユーザーにとって「勝手にとられる」データである点で共通する。対して０パーティデータは、フォームやアンケートなどのかたちで収集される、明確な「同意のある」データである。０パーティデータがあれば、やはりクッキーに頼ることなく、ユーザーにとって最適な広告を導く道が開けてくる。つまり、クッキー規制後に生き残るのは、１ｓｔパーティデータないし０パーティデータを蓄積し、利活用できる企業と広告のみ、と予想される。

ここで、デジタル広告業界団体の動きに言及する。GDPR施行直前の2018年４月、米国のInteractive Advertising Bureau（IAB）は、アドテック・ベンダーなどがGDPRなどの法規制に準拠することを支援するために、「透明性と同意のフレームワーク（TCF）ｖ１・１）」という枠組みを発表。2019年８月には、それを「TCF ｖ２・０」へアップグレードさせた。IABは、ニューヨークに本部を置く、世界のアドテック・ベンダー、マーケター、パブリッシャー、その他のデジタル・マーケティング関連企業が加盟する非営利組織で、グーグル、フェイスブックもメンバーとなっている。

このTCFにそって開発され、さまざまなソフトウェア・ベンダーがＢtoＢ領域で提供を促進しているのが「コンセントマネジメント」という概念である。これは、サードパーティクッキーの広告への利活用が法制度上困難になるなかで、ユーザーの個人情報の取得ないし利用・取扱いに関して、ユーザーからの同意（コンセント）を管理する、すなわち０パーティデータの取得・管理を行うソリューションである。GDPRやCCPAといった法規制に準拠するのはもちろん、ユーザーの個人情報やプライバシーの保護と事業者へのブランド・ロイヤルティ向上を同時に実現するという意図も含まれている。

6｜結局、クッキーはどうなるのか？

結局クッキーはどうなるのかについて、次の５つのポイントとして整理する。

第一に、クッキーは、欧州GDPRやCCPAにおいては法令上の個人情報として取り扱われる。もし企業がその第三者提供や利用・取扱いの際に法令違反すれば、厳しい罰則が科される可能性がある。グーグルがターゲット広告目的のデータ収集が不適切であったとして5000万ユーロ（62億円）の制裁金を科されたのは顕著な例である。よって第二に、法令上、サードパーティクッキーの利活用が制限される。現在デジタル広告のエコシステムほぼ全体がターゲティング広告でサードパーティクッキーに依存していると言っても過言ではなく、そのターゲティングの精度が低下すると考えられる。第三に、

技術上、ユーザーのブラウザレベルでトラッキング認定されるクッキーを無効化するトラッキング防止が浸透することから、デジタル広告のエコシステムからサードパーティクッキーが締め出される。アップル「サファリ」や「ファイヤーフォックス」には既にトラッキング防止機能が備えられている。グーグル「クローム」も２年以内のクッキー規制を表明している。事業者が、法令上だけでなく、技術的かつ自主的にもクッキーを使用しない動きにあるわけである。

以上のことから第四に、ファーストパーティクッキーや０パーティデータが重視される。企業には、これらを管理するコンセントマネジメントのもと、ユーザーとの「継続的で良好な関係性」が求められ、またそれによってメディアと広告の関係にも変化が生じる。そして第五に、サードパーティクッキーを使用したトラッキングとは異なる手法がデジタル広告に使用されるようになる。例えば、IAB傘下の非営利団体「デジトラスト」加盟のアドテック・ベンダーなどが共通のユーザーIDを使用してユーザーを識別するソリューション、入札の仕組みに頼らないプライベートマーケットプレイスでの広告取引などである。さらには、新しい価値観で支持をのばすブラウザ「ブレイブ」、グーグルが2019年８月に構想を打ち出したプライバシーを強化するオープンなエコシステム「プライバシーサンドボックス」にも注目する必要がある。

3――CES2020であらわになった根強い批判

1｜チーフプライバシーオフィサー（CPO）・ラウンドテーブル

2020年１月、米国ラスベガスで開催された世界最大級の家電・技術見本市「CES2020」において、「チーフプライバシーオフィサー（CPO）」によるパネルディスカッションが開かれた。CES2020において多くのセッションがある中でも、このパネルディスカッションは最も注目を集めたセッションの１つであった。

注目を集めた背景には、「データの利活用」とともに「プライバシーの保護」が求められてきた社会情勢のなかでCPOという新しい役職への関心が高まっていたこと、1992年以来28年ぶりにCESへ参加したアップルのCPOが登壇したこと、個人データ流出などでプライバシー問題の中心にあったフェイスブックのCPOも登壇したことなど、複数の理由があった。合わせて、日本の公正取引委員会にあたる連邦取引委員会（FTC）のコミッショナーが登壇したことも話題になった。

筆者自身、GAFAをはじめとするメガテック企業の「ビッグデータ×AI」の利活用と、そこにおける個人データの取扱いやプライバシー対応に関心を持ち、セッションに参加した。そこで、筆者は、プライバシー重視で高い評価を受けるアップルでさえも、FTCからはプライバシー重視への取り組みがまだ十分ではないと見なされている、その事実に驚いた。

パネルディスカッションに参加したのは、アップルとフェイスブックのCPO、FTCのコミッショナー、そして世界最大の消費財メーカーP&GのCPOとモデレーターを含めた５名であった。テーマは「チーフ

プライバシーオフィサー・ラウンドテーブル：消費者は何を求めているのか？（What Do Consumers Want?）」。成長するデータ・エコノミーや進化するテクノロジーという状況で、企業は消費者の個人データやプライバシーとどのように対峙し、それらをどのように保護する仕組みを構築していくのかについて、意見が交わされた。

そこで中心となったスピーカーは、アップルとフェイスブックであった。アップルは「プライバシーは、基本的人権です」（アップルコーポレートサイト）として、ティム・クックCEOの方針のもと厳格なプライバシー基準を設け、メガテック企業のなかでは特別強く、ユーザー保護をうたってきた。パネルディスカッションにおいて、アップルのジェーン・ホバースCPOは、アップルのプライバシー保護の方針を「消費者を運転席に置くこと（to put the consumers in the driver's seat）」と表現した。これは、ユーザーが個人データを自ら管理し、さらには個人データをどのように扱わせるかについて自ら選択するということを意味する。また「プライバシー・バイ・デザイン」というプライバシー方針にのっとり、ホバースCPOの部門にはプライバシー・エンジニアとプライバシー・ロイヤーが所属、チームとしてアップルのすべての製品・サービスの開発段階からかかわっていることが説明された。

さらに、ホバースCPOは「データ・ミニマイゼーション」にも言及。これは、「ユーザーから収集する個人データを最小限に抑える、活用する個人データを最小限に抑える」という概念であり、アップルのプライバシー方針のなかで極めて重要な位置を占めるものである。ホバースCPOは、アップルの音声認識AIアシスタント「Siri」を例に、データ・ミニマイゼーションの考え方を示した。例えば、ユーザーが「Siri」に天気予報をたずねる場合、アップルはユーザーがいる場所を広域レベルで把握するだけで、より細かい位置情報は収集しない。一方で、ユーザーが近くのレストランを「Siri」にたずねる場合、アップルは最適なレコメンデーションをするために、ユーザーが位置する緯度・経度といったピンポイントのレベルまで探索する。つまりアップルは、用途に応じて、必要最小限の個人データしか収集しない、と主張しているのである。

一方、2018年４月の個人データ流出事件を受けて「未来はプライベートです。（the future is private.）」（2019年「F8」でのマーク・ザッカーバーグCEOの基調演説）としてプライバシーやセキュリティをさらに強化・重視する姿勢を示してきているフェイスブックからは、エリン・イーガンCPOが登壇した。フェイスブックは、その最大8700万人にものぼる個人データ流出事件によって、2018年７月英国規制当局から50万ポンドの制裁金が科された。また、2019年７月には、米国でも、FTCから同事件の制裁金として50万ドルが科されている。フェイスブックがプライバシー問題の中心に置かれていたことは明白で、パネルディスカッションにおいてイーガンCPOがどのような発言をするのか、注目を集めていた。イーガンCPOは、新しい「プライバシー診断ツール」を紹介し、自分たちはプライバシー方針を遵守していると主張。その一方で、カリフォルニア州CCPAの遵守方針に関しては、「フェイスブックはサービスプロバイダーとして広告を売っているのであって個人データを売っているわけではない」、したがって同法は適用されないと発言するなど、会場から批判的に捉えられる場面も何

度か見受けられた。

正直なところ、筆者には、フェイスブックはプライバシー問題の所在や同社が社会から求められていることを本当に理解しているのか疑わざるを得ないような発言が目立ったようにも感じられた。フェイスブックに向けられた批判は、プライバシー保護の意識がそれだけ浸透していることを表している。

「アメリカ企業は消費者のプライバシーを守っていると思いますか」とモデレーターが質問したところ、アップルとフェイスブックはいずれも「自社については守っていると思います」と回答。それに対してFTCのレベッカ・スローター・コミッショナーは、「企業によるプライバシー遵守への取り組みは不十分である」と発言した。スローター氏は、個別の企業や製品・サービスを想定しての発言ではないとしているが、実際には、アップルとフェイスブックの説明をふまえての発言であるように思われた。

スローター氏は、プライバシー分野の専門家である自分からしても、企業のプライバシー規約やユーザーによるプライバシー・レベルの設定手順は複雑でわかりにくい、と主張。「今日、消費者がプライバシーチェックを通過できたとしても、データで何が起こっているのかを把握するために処理しなければならない情報量は、ほとんどの人にとって受け入れがたいものです」とスローター氏は言った。そのような中で、「プライバシーは消費者の選択である、個人データがどのように扱われるかを決めるのは消費者自身である」といった企業側の方針はいくぶん乱暴なものではないかという考え方も示した。企業側が個人データを保護するための負担を消費者側に負わせていることについて懸念を表明したわけである。その上で同氏は、「収集、保持、共有されるデータの量を最小限に抑えるべきだ」と述べた。

質疑応答では「この広告は事実に反しているのではないか？」、また「掲示された時点からの改善状況はどのようなものか？」といった質問がメディアから投げかけられた。

「この広告」とは、昨年のCES2019開催中ラスベガスの街の中心に掲げられた「iPhoneの中で起こることは、iPhoneの中に残ります。（What happens on your iPhone, stays on your iPhone.）」という、プライバシー重視の姿勢をアピールするアップルの広告である。

例えば、iPhoneの地図アプリを使った場合に生成される個人データがアップルIDに紐付けられることなく、また利用履歴がアップルのクラウド上に保存されることなく、あくまでiPhoneというデバイスの中に残るということである。

しかし「この広告は事実に反しているのではないか？」という質問に対し、ホバースCPOから完全な回答はなかったように見受けられた。確かに、アップルは、マップやAIアシスタント「Siri」など個

人の特定につながる情報はデバイス上で保存される。つまり、それらデータがアップルのサーバやクラウドに保存されることはない、またサーバに保存されているアップルIDに紐付く氏名や住所などの個人情報と紐付いていないため個人が特定されることもない、ということである。しかし、事実として、アップルIDに紐付いた氏名や電話番号などはサーバに保存され、個人の設定として写真やヘルスケア情報をアップルIDと紐付けてクラウドにバックアップすることも可能である。その点が、「この広告は事実に反しているのではないか？」という指摘につながるのである。

プライバシー保護へ積極的に取り組んできたアップルでさえもこのような厳しい目を向けられる、これほどにプライバシー重視を求める世論の声が高まっているのは、なぜか。言うまでもなく、クッキー規制の影響である。米国においては、CCPAのような法規制はカリフォルニア州に限定されている。しかしパネルディスカッションで、FTCのスローター氏は、個人的な見解としながらも「連邦レベルでも同様の法律が制定されるべきであり、それは2021年までに法制化される可能性が高い」という見通しを示している。こうしたプライバシー規制強化の流れは、アメリカにおいてはもはや不可逆となってきており、アップル、グーグルらGAFAは今後さらなる厳しい目にさらされることになるであろう。

2｜周回遅れにある日本に求められるもの

日本では、プライバシーについての米国の現状の詳細を知るビジネスパーソンは依然少なく、そもそも「チーフプライバシーオフィサー」という役職名を聞いたことがある人自体少ないのではないかと思われる。日本は、データの利活用に関して、米国メガテック企業に比べて著しく遅れをとっていることがかねてから指摘されている。また、プライバシー重視の姿勢や法規制についても、さらに周回遅れの状況である。

CES2020での重要なテーマとして「データの利活用」と「プライバシーの保護」の両立が挙げられた。「データの時代」となっていることが明白である一方、同時に「プライバシーの時代」でもある。つまり、「データの利活用」と「プライバシーの保護」を両立させなければならない時代が到来しているということである。

このような中で、日本にはどのような対応が求められているのであろうか。それは、「データの利活用」でも「プライバシーの保護」でも周回遅れであるからこそ、両者の状況を冷静に分析し、より的確な答えを見出だしていくことである。そして、むしろ後発者利益を企図して享受するような、さらにはその両立において世界をリードするような戦略的な動きをとっていくべきではないかと考える。

米国では、ここ数年、プライバシーを保護するためのテクノロジーである「プライバシー・テック」の製品・サービスが支持されている。プライバシー重視で高い評価を受けるアップルでさえも、FTCからはプライバシー重視への取り組みが十分ではないと示唆された点は驚くべきことである。日本においても、今後、こうした「プライバシー・テック」やプライバシー重視の流れが押し寄せてくると考えられる。その意味で、日本企業には今後ますます、「データの利活用」と「プライバシーの保護」

の両立に関して、本質的かつ具体的な対応が求められてくるであろう。