基礎研レポート

アップルとグーグルのプライバシー対応

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. プライバシーを重視する社会情勢の先鋭化と合わせて、プライバシー保護に関する法規制も強化されてきている。それに伴って、「ビッグデータ×AI」によって個人情報を事業の核に据えてきたデジタル・プラットフォーマーも、方針転換を迫られている。

2. 現在、デジタル・プラットフォーマーのうちプライバシー保護で先行しているのは、広告収入に依存していないアップルである。アップルはプライバシーを基本的人権ととらえ、アップルのすべての製品・サービスは顧客のプライバシーと安全を徹底的に保護するために設計・開発されている。

3. アップルのプライバシー保護にかかわるポイントは、写真、マップ、FaceTime、AIアシスタント「Siri」などはデバイスの中で処理・実行され、そのデータはデバイスの中に保存される、という点である。つまり、アップルが掲げた「iPhoneの中で起こることは、iPhoneの中に残ります」というフレーズの通り、原則として個人データがデバイスの外に出ることはないということである。アップルでは、ユーザーが同社の製品・サービスを利用することで作製される個人情報は、原則、いかなる目的でも開示されず販売もされないとしている。

4. 個人情報やクッキーを活用した広告をビジネスモデルの柱とするグーグルは、プライバシーとセキュリティに関して「収集するデータの内容とその目的を明確にする」「ユーザーの個人情報を決して販売しない」「ユーザーが自分自身のデータを確認、移動、削除できるようにする」など

「７つの原則」を掲げ、プライバシー保護やセキュリティ強化へ力を入れている。特に、2020年１月、広く普及するブラウザ「クローム」において２年以内に広告目的のクッキーを利用制限すると発表するなど、具体的な対策を打ち出してきている。

5. アップルは、クッキーを、自社の製品・サービスの品質向上および「Apple News」「App Store」といった自社の広告プラットフォーム内での広告配信を目的として使用する。一方、グーグルは、クッキーを、グーグルパートナーという第三者と共有することを通してユーザー毎の最適な広告配信に使用、デジタル広告のエコシステムの中で広告収入を得るために利用している。両社とも、欧州の一般データ保護規則、米国カリフォルニア州の消費者プライバシー法でクッキーにかかわる法規制が厳格化される中、ユーザーに対して、クッキーがどのように使用されているのかについて丁寧な説明をしている。

6. 「プライバシー保護」にかかわる法規制強化の流れはもはや不可逆であり、「データの利活用」によって成長を遂げてきたデジタル・プラットフォーマーには、「プライバシー保護」の概念を製品・サービスの設計・開発段階から取り入れることが求められてきている。彼らは、今後否応なく、「データの利活用」と「プライバシー保護」の両立というテーマへより高いレベルで対峙することになる。

1――アップルのプライバシー対応

1｜プライバシーを強化するアップル

2018年のフェイスブックによる最大8700万人にものぼる個人データ流出事件などを契機として、プライバシーを重視する社会情勢はますます先鋭化されてきている。合わせて、プライバシー保護に関する法規制も強化されている。2018年５月に欧州の一般データ保護規則（GDPR）、2020年１月には米国カリフォルニア州の消費者プライバシー法（CCPA）が、それぞれ施行された。日本でも、2020年６月、改正個人情報保護法が国会で可決・成立した。それらに伴って、「ビッグデータ×AI」によって個人情報を事業の核に据えてきたGAFA（グーグル、アップル、フェイスブック、アマゾン）などデジタル・プラットフォーマーも、方針転換を迫られている。

現在、デジタル・プラットフォーマーのうちプライバシー保護で先行しているのは、広告収入に依存していないアップルである。アップルは、フェイスブックの個人情報流出事件と同時期に、プライバシーを強化したiOS 11.3をリリースした。

「アップルは2018年４月にiOS 11.3を発表し、プライバシー保護にさらなる強化を加えた。このアップデートには、ユーザーの個人データがアップルのサービスによって収集されていることを明確に示す新たなアイコンが追加された。『このアイコンはすべての機能で表示されるわけではありません。アップルが個人情報を収集するのは、機能を有効にする必要があるときや、サービスを保護するとき、またはユーザー体験をパーソナライズする必要があるときだけです』。iOS 11.3にアップデートしたユーザーへの通知には、このように説明されていた。『アップルはプライバシーを基本的人権だと考えているため、すべてのアップル製品はデータの収集と使用を最小限に抑え、可能な限りデバイス上で処理し、お客様の情報に対する透明性と管理を提供するよう設計されています』。」（『ティム・クック』リーアンダー・ケイニー著、堤沙織訳、SBクリエイティブ）

そもそも「アップルバリュー」と称する独自の価値観のなかでも、環境や教育に関する価値観と並んで、「プライバシーと安全性」に関する価値観を掲げている。「アップルは、プライバシーを基本的人権ととらえ、すべてのアップル製品は、顧客のプライバシーと安全を徹底的に保護するためにデザインされている」（同）。

注目したいのは、この価値観がアップルの事業において、どのように表現されているのか、である。コーポレートサイトにある「Appleの取り組み」にある「プライバシー」ページでは、概要、機能、プライバシーコントロール、透明性に関するレポート、プライバシーポリシーの５項目にわけて説明が用意されている。ブラウザや位置情報など重要なサービスについては、技術的な詳細まで踏み込んだ「白書」も公開されている。ここでは特に、アップルにおけるプライバシー保護の基本方針と、それが各サービスにおいてどう表現されているのか、ポイントとなる部分を見ていく。

なお、本稿で扱う各社のプライバシーポリシーは、2020年７月時点のものである。

2｜「iPhoneの中で起こることは、iPhoneの中に残ります」

まず、アップルのプライバシー保護に関する基本方針や特徴は、次のように整理することができる。

- 「プライバシーは、基本的人権」
- 「プライバシーを守り、自分の情報を自分でコントロールできるようにアップル製品を設計している」（プライバシーははじめから組み込まれている）
- 個人データはデバイス上で処理される（アップルのサーバやクラウドには保管されない）
- 個人データとアップルIDは紐付かない（個人データと紐付くのはランダムな識別子）
- ランダムな識別子を第三者と共有したり販売したりすることはない
- 個人データは「自分で管理」
- アプリケーションが写真や位置情報といった個人データにアクセスしようとするとき、許可を求めるメッセージが表示される
- 製品や機能に内蔵されているのは、アップルやほかの誰かがアクセスできる個人データの量を最

小限にするために設計された、革新的なプライバシーのテクノロジー
- 本人以外の何者にも個人データをアクセスさせないようにするセキュリティ機能

本節の小タイトル「iPhoneの中で起こることは、iPhoneの中に残ります」とは、アップルがCES2019開催中ラスベガスの街の中心に掲示した広告に書かれたフレーズである。

このフレーズのとおり、アップルの基本方針における一番のポイントは、写真、マップ、FaceTime、AIアシスタント「Siri」などはデバイスの中で処理・実行され、そのデータはデバイスの中で保存される、という点である。つまりデータそのものがデバイスの外に出ることはなく、アップルのクラウドにも保存されることはない。またクラウドに保存されている個人情報、すなわちアップルIDに紐付いた氏名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。ただし、写真、iMessage、SMS、ヘルスケア情報、Apple Musicについては、自分の意志によってアップルIDと紐付けてクラウドにバックアップすることが可能で、その場合はアップルIDと紐付けられるので個人情報として保管される。そして、個人情報が第三者に開示されるのは、アップルの業務に関係する規定上決められた企業のみであり、それ以外にはいかなる目的においても開示されず、販売もされない。

3｜アップルのサービスにおけるプライバシー保護

アップルの各サービスにおいてどのようにプライバシーが配慮されているのかを、次の通り、アップルのコーポレートサイトからの引用を交えながら整理する。

(1) ブラウザ「サファリ」：「Safariは追跡者からあなたを守ります」

「ウェブサイトの中には、サイトを閲覧するあなたの行動を何百ものデータ収集会社に監視させ、プロファイルを作成することで広告を表示するものがあります」。そのデータのなかにはクッキーも含まれている。アップルが開発したブラウザ「サファリ」はこれをブロックするインテリジェントトラッキング防止機能（ITP）を備えている。これによりユーザーの行動履歴を第三者に追跡されることがなくなる。あるサイトで閲覧した商品の広告が、別のサイトを見ているときに追いかけてくる、といったこともなくなる。

またサファリは、ソーシャルウィジェットの追跡防止機能も備えている。通常さまざまなサイトに埋め込まれているフェイスブックの「いいね」ボタンをはじめとするソーシャルウィジェットもユーザーの行動を追跡するが、「Safariはデフォルトでこの追跡をブロックして、あなたが許可しない限りソーシャルウィジェットがあなたの身元情報にアクセスできないようにします」。

(2) マップアプリケーション：「マップなら残る履歴は思い出だけ」

目的地への移動や検索の履歴、頻繁に訪れるお店や近隣エリアなど、マップアプリケーション上の情報は個人の特定を容易にする。しかしアップルのマップアプリケーションはこうした機能の多くをデバイス上で行うため、アップルがユーザーの行動を把握することはない。またこうした情報はアッ

プルIDと紐付けず、その都度かわるランダムな識別子と紐付けられるのみである。さらにこの識別子はアプリケーションを使うたびにリセットされる。ちなみにグーグルマップの場合は、利用者の同意のもとにグーグル・アカウントに紐付いて移動や検索の履歴が保存されている。

(3) 写真アプリケーション：「のぞき見されないように写真を保存します」

これもデバイス上でデータの処理を行うことを意味している。「顔やシーン、被写体の検出などは、クラウド上ではなく完全にデバイス上で行われます。そのため写真に写っているものをアップルが把握することはありません。またアプリケーションが写真にアクセスできるのは、あなたの許可がある場合だけです」。アップル独自のクラウドサーバー「iCloud」に写真をバックアップする場合は、サーバ上の写真を暗号化し保護する。

(4) 「iMessage」と「FaceTime」：「メッセージを見られるのは、送った人と送られた人だけ」

iOSデバイス間でのショートメッセージサービス「iMessage」は、原則としてエンドツーエンドで暗号化され、アップルを含め第三者が通信内容を把握できないようにしている。メッセージは「iCloud」上に保存されるが、いつでも解除が可能である。同様にアップルのビデオ通話アプリ「FaceTime」も通話は暗号化され、その内容がサーバに保存されることもない。

(5) AIアシスタント「Siri」：「Siriが学習するのは、あなたが知りたいこと。あなた自身のことではありません」

「Siri」とはiOSやmacOSに搭載された音声アシスタントである。ユーザーから話しかけられると音声で質問に答えたり命令された機能を呼び出したりする。デフォルトの設定では「Siri」とユーザーが交わした音声のやりとりがサーバに保存されることはない。基本的にすべてのデータはサーバに送られることなくデバイス上で保存、処理・実行されるというアップルの方針がここでも貫かれている。

一部サーバとのデータのやりとりが生じる場合も、アップルIDではなくランダムな識別子を使ってプライバシーを保護する。「Siriの音声や音声入力のやり取りの保存や確認をAppleに許可することで、Siriの向上をサポートする」ことが可能であるが、この設定はいつでもオフにできる。音声のやりとりはアップルのマーケティングなどに使用されることはなく、「Siri」の利便性向上に使われるのみである。

(6) 「Wallet」と「ApplePay」：「WalletとApplePayは、購入履歴を隠します」

クレジットカードやプリペイドカード、Ｓｕｉｃａなどをまとめて管理できるアプリ「Wallet」、そしてアップルの非接触型決済サービス「ApplePay」。どちらも、クレジットカード番号や購入した商品など貴重な個人情報を扱うサービスであるが、アップルがその内容を知ることはない。アップルは次のように解説している。

「Walletアプリケーションを通してApplePayにクレジットカードやプリペイドカードを追加すると、

あなたのデバイスはあなたのアカウントやデバイスに関するそのほかの情報と一緒に、カード情報を安全な方法でカード会社へ送信します。実際のカード番号が、デバイス上やアップルのサーバに保存されることは決してありません。カード番号の代わりに、固有のデバイスアカウント番号が作成され、アップルには解読できない方法で暗号化されて、あなたのデバイスの中のSecure Element に保存されます。Secure Elementにあるデバイスアカウント番号は、オペレーティングシステムから隔離されます。この番号がApplePayのサーバに保存されたり、iCloudにバックアップされることはありません」

(7) ヘルスアプリケーション：「ヘルスアプリケーションなら、あなたの記録はあなただけのもの」

アップルのヘルスケアアプリケーションは、心拍数や血圧、睡眠時間など各種の健康やフィットネスのデータを把握するアプリである。ここではどのデータを保存するのか、データを誰と共有するのか、事細かに決定できる。また「あなたのデータはすべて暗号化され、自分のパスコード、TouchID、FaceIDのいずれかを使わない限りアクセスはできません。つまり、ヘルスアプリケーションをどう使ったとしても、データを管理するのはあなただということ」。

以上アップルが提供する７つのサービスを見たが、ここで繰り返し強調されているのは、アップルは自社サービスの利便性向上など限られた目的以外ではデータを活用しない、ということである。氏名、住所、電話番号、メールアドレス、デバイスID、位置情報、クレジットカード情報などの個人情報を利用する目的については、次のようにまとめられている。

「当社は、当社の製品、サービス、コンテンツおよび広告の作成、開発、運用、提供および向上に役立てるため、ならびに損失防止と不正防止の目的のためにも、個人情報を利用します。加えて、アカウントおよびネットワークのセキュリティ目的でもお客様の個人情報を使用することがあります。これには、当社の全ユーザーの利益を図るために当社のサービスを保護し、アップロードされたコンテンツを事前スクリーニングまたはスキャニングして、子どもの性的搾取に該当するなど違法な可能性のあるコンテンツを排除する目的などが含まれます。お客様の情報を不正防止の目的で使用する場合、それはAppleとのオンライン取引に起因するものです。不正防止の目的でのデータ利用は、それが必要不可欠であり、かつ当社のお客様およびサービスの保護という正当な利益の範囲内であると当社が判断する場合に限られます。特定のオンライン取引については、公的にアクセス可能な情報源を利用して、お客様が提供した情報を検証することがあります」

また、そのままでは特定の個人と関連付けられることのない「非個人情報」の利用については、次のように書かれている。

「当社は、お客様の動向をよりよく理解して、当社の製品、サービスおよび広告を向上させるために、職業、言語、郵便番号、エリアコード、固有のデバイス識別子、リファラーURL、所在地、アップル製品が使用されている時間帯などの情報を収集することがあります」「当社は、当社のウェブサイト、iCloudサービス、iTunes Store、App Store、MacApp Store、Apple TV App Store、iBooks Store

において、および当社のその他の製品やサービスから、お客様の活動に関する情報を収集することがあります。この情報を集計して、お客様により有益な情報を提供したり、当社のウェブサイト、製品とサービスのどの部分にお客様が最も関心を持っているかを把握したりするために役立てています。統計データは、本プライバシーポリシーにおいて、非個人情報とみなされます」「お客様の明示的な合意を得て、当社は、アプリケーションのデベロッパがアプリケーションの向上に役立てられるように、お客様がデバイスやアプリケーションをどのように利用されているかについて情報を収集することがあります」

4｜クッキーを第三者に渡さないアップル

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）において論点となるクッキーの利活用については、アップル（ブラウザ「サファリ」）はどのようなスタンスをとっているのであろうか。

これについてもアップルは第三者にクッキーを渡してはいない、あくまで自社製品・サービスの品質向上のために使う、という方針が示されている。なお、クッキーは、日本の2020年改正個人情報保護法では他のデータと突き合わせることで個人が特定されない限り非個人情報として扱われるが、GDPR･CCPA管轄下では個人情報として扱われる。

「アップルのウェブサイトやオンラインサービスでは、『Cookie』（クッキー）を使用する場合があります。Cookieにより、ショッピングカートが使用でき、当社のウェブサイトでのお客様の体験をパーソナライズできます。また、Cookieを使うことにより、当社は、ユーザがウェブサイトのどの部分を閲覧したかを知り、広告やウェブ検索の効果を測定し、ユーザの動向を把握することができるため、コミュニケーションと製品の改善にも役立ちます」

またアップルは、「ICC UK Cookie Guide」（英語）のガイドラインに従って、利用するクッキーを次の３カテゴリーに分類している。以下、アップルのコーポレートサイトから引用する。

カテゴリー１「Strictly Necessary Cookies（不可欠なCookie）」：「このカテゴリーのクッキーは、ユーザーがアップルのウェブサイトを自由に閲覧し、その機能を利用する上で欠かせないものです。無効にすると、ショッピングカートや支払い処理などのサービスを利用できなくなります。」

カテゴリー２「Performance Cookies（パフォーマンスCookie）」：「このカテゴリーのクッキーは、最もアクセスが多いページなど、アップルのウェブサイトの利用状況についての情報を収集します。収集したデータはウェブサイトの最適化に使われ、ユーザーはさらに操作しやすくなります。ユーザーがアフィリエイトサイトからアップルのウェブサイトにアクセスし、さらにそこでアップル製品を購入したりサービスを利用したことをその詳細とともにアフィリエイトに知らせるのも、このカテゴリーのクッキーです。このクッキーは、個人を特定できる情報を収集しません。また、収集されたす

べての情報は集計されるため、匿名性が保たれます。」

カテゴリー３「Functionality Cookie（機能性Cookie）」：「このカテゴリーのクッキーは、ウェブサイト閲覧時のユーザーの選択を記憶できるようにします。例えば、ユーザーがいる国や地域に合わせたウェブサイトが自動的に表示されるように、アップルがユーザーの地理的な位置情報を保存する場合があります。ウェブサイト上のテキストのサイズやフォント、カスタマイズできるその他の要素などの環境設定を保存する場合もあります。選択の繰り返しを避けるために、ユーザーが閲覧した製品やビデオを記録するのも、このカテゴリーのクッキーです。このクッキーが収集した情報によって個人が特定されることはありません。また、アップル以外のウェブサイトでのユーザー行動をこのクッキーが追跡することもできません。」

2――グーグルのプライバシー対応

1｜グーグルが掲げる「7つの原則」

次に、アップルと比較対照をするために、グーグルについて見ていきたい。

個人情報やクッキーを活用した広告をビジネスモデルの柱としてきたグーグルであるので、グーグルのプライバシー対応は、アップルのそれとは必然的に異なってくる。それでも、グーグルは、2020年１月、広く普及するブラウザ「クローム」において２年以内に広告目的のクッキー、いわゆるサードパーティクッキーを利用制限すると発表した。グーグルの今後の対応が注視されている。

最初に、グーグルが掲げているプライバシーとセキュリティについての「７つの原則」を押さえておく。

(1) ユーザーとそのプライバシーを尊重する。
(2) 収集するデータの内容とその目的を明確にする。
(3) ユーザーの個人情報を決して販売しない。
(4) ユーザーが自分のプライバシーを簡単に管理できるようにする。
(5) ユーザーが自分自身のデータを確認、移動、削除できるようにする。
(6) Google サービスに業界最高水準の強固なセキュリティ技術を導入する。
(7) すべての人のオンラインセキュリティを強化するための模範を示す。

「(1)ユーザーとそのプライバシーを尊重する」「(2)収集するデータの内容とその目的を明確にする」については、GDPRやCCPAでも明記されているところである。例えば、グーグル検索や、グーグルマップでのルート案内、ユーチューブでの動画視聴など、サービスの利用状況に関する情報がそれにあたる。「世界中の情報を整理する」というミッションのもとで事業領域を広げてきたグーグルだけに、多岐にわたる情報を集めているということである。

続いて「(3)ユーザーの個人情報を決して販売しない」について、当然ながら個人情報を販売することはないが、グーグルはクッキーを個人情報として捉えてはおらず、第三者のネット広告企業などに開示、提供しているのは明白である。この「個人情報を販売しない」という表現は、グーグルやフェイスブックがしばしば使っているものである。ただ個人にまつわるデータをもとにビジネスをしているのは明らかで、誤解を招きやすい表現でもある。「直接的にそれを第三者に売却して対価を得ることはないが、個人情報に準じるデータを利活用してビジネスをしている」と理解するべきである。グーグルは、次のように明記している。

「Googleはデータを利用して、ユーザーに関連性の高い広告をGoogleサービス、パートナーウェブサイト、モバイルアプリに配信しています。これらの広告から得た利益は、Googleがサービスを開発し、それを無料で提供するために役立てられています。ユーザーの個人情報は販売目的で収集しているわけではありません。また、ユーザーが広告設定を柔軟に変更し、表示される広告をきめ細かく管理できるようにしています」

「(4)ユーザーが自分のプライバシーを簡単に管理できるようにする」「(5)ユーザーが自分自身のデータを確認、移動、削除できるようにする」は、ユーザーが自身の個人データを自らの管理下に置く、という意味である。アップルの「プライバシーデザイン」の方針とも重なる部分である。「(6)Googleサービスに業界最高水準の強固なセキュリティ技術を導入する」「(7)すべての人のオンラインセキュリティを強化するための模範を示す」では、セキュリティ技術の開発・強化を推進しつつ、そうしたプライバシー保護の取り組みを業界全体へと広げていく姿勢を打ち出している。

アップルと同様に、グーグルが持つ個人情報については共有も販売もされない。しかしクッキーなど非個人情報は広告主などと広告目的で共有されている点が、アップルと異なる点である。それは、ユーザーにとって最適な広告を表示するためである。またアップルはアップル自身の広告プラットフォームのなかで広告を配信しているが、グーグルはグーグルパートナーと言われる企業からの広告配信があるというところも異なっている。

2｜グーグルのサービスにおけるセキュリティ対策

次に、各サービスにおいて、どんなセキュリティ対策がとられているか、コーポレートサイトから整理する。

「メールの送信、動画の共有、ウェブサイトの閲覧、写真の保存などを行うと、作成したデータが端末、Googleサービス、データセンターの間を行き来します。こうしたデータをGoogleでは、HTTPS、Transport Layer Securityなどの最先端の暗号化技術で何層にも保護しているのです」

またメールソフトの「Gmail」については、「マルウェア感染やフィッシング攻撃の多くはメールが

原因です。Gmailは、他のどのメールサービスよりも、迷惑メール、フィッシング、不正なソフトウェアからユーザーを保護する機能を有しています。機械学習と人工知能を利用して、数十億のメッセージのパターンを分析し、ユーザーから迷惑メールと報告されたメールの特徴を明らかにして、それをもとに不審なメールや危険なメールの99・９％をユーザーに届く前にブロックしています」

ブラウザのグーグル「クローム」については、「セキュリティ技術は絶え間なく変化しているため、Chromeは、ユーザーが使用しているブラウザのバージョンが最新の状態であるかどうかを常時チェックしています。このチェックには、最新のセキュリティパッチや、不正なソフトウェア・詐欺サイトからの保護機能が適用されているかどうかの確認も含まれます。Chromeは自動的に更新されるため、ユーザーは常にChromeの最新のセキュリティ技術で保護されます」

また、セキュリティに関する技術や知見を業界全体に広げる働きかけとして、危険なウェブサイトにアクセスしようとすると警告を発するセーフブラウジング技術を開発し、他社が無料で利用できるようにしたことを例に挙げている。

「セーフブラウジング技術は、ウェブユーザーを不正なソフトウェアやフィッシングの脅威から守るためにGoogleが開発したもので、危険なウェブサイトにアクセスしようとすると警告を表示します。セーフブラウジングはChromeユーザーを守るだけはありません。Googleは、誰にとっても安全なインターネットを実現するため、セーフブラウジング技術を他の企業が無料で利用できるようにしたため、アップルのSafariやMozilla Firefoxなどの製品にも採用されました。現在は、30億台以上の端末がセーフブラウジングで保護されています。また、Googleでは、サイトの所有者にセキュリティ上の脆弱性を警告し、問題を迅速に修正できる無料のツールも提供しています」

3｜グーグルのプライバシー保護

プライバシーに対する具体的な取り組みについては「データの透明性」「プライバシー設定のカスタマイズ」「広告とデータ」という３項目で説明がなされている。

「データの透明性」では、どんなデータを収集しているかを明らかにしている。例えば、グーグルサービスの利用時に収集されるデータとして、検索内容、再生した動画、表示またはクリックした広告、現在地情報、アクセスしたウェブサイト、Googleのサービスにアクセスしたアプリ、ブラウザ、端末を挙げている。またグーグル・アカウントの登録時には、氏名、生年月日、性別、パスワード、電話番号、Gメールで作成および受信するメール、保存する写真や動画、グーグルドライブで作成するドキュメント、スプレッドシート、スライド、ユーチューブで投稿するコメント、追加する連絡先、カレンダーの予定などの情報をグーグルに提供、またグーグルはその情報を保護するとしている。

また収集したデータの使いみちについても説明を加えている。そこではグーグルマップが最適なルートを提案する、検索キーワードをオートコンプリートする、ユーザーが興味のあるユーチューブ動

画をおすすめする、などが挙げられている。例えばアップルの「Siri」にあたる音声アシスタント「グーグルアシスタント」については、次のように説明している。

「自宅にいるときも外出しているときも、アシスタントはいつでもサポートしてくれます。アシスタントに質問したり何かをするよう指示したりすると、アシスタントは他のGoogleサービスのデータを活用して必要な情報をユーザーに提供します。たとえば『近くのカフェは？』、『明日は傘が必要？』などと質問した場合は、最適な答えを提供するためにGoogleマップやGoogle検索の情報、ユーザーの現在地、興味や関心、好みに関するデータが使用されます。アシスタントとのやり取りから収集されたデータは、Googleアカウントのマイアクティビティツールからいつでも確認したり削除したりできます」

次に「プライバシー設定のカスタマイズ」とはどのようなものであろうか。例えば「プライバシー診断」という機能は、自身にあったプライバシー設定を選べるよう案内してくれるものである。

例えば「ウェブとアプリのアクティビティ」がオンになっていると、グーグルサービス上でのアクティビティ、何を検索してどのサイトを閲覧したかなどの情報が保存され、検索の高速化やおすすめ機能の精度向上などに活用される。また「ロケーション履歴」がオンになっていると、グーグルマップなど特定のグーグルサービスを使用していないときでも、ログイン状態のデバイスを持って訪れた場所が記録される。そのほか、他のユーザーに対して公開される情報を管理したり、表示される広告の種類を自身とより関連性の高い／低いものに変更することができる。

「広告とデータ」のページでは、グーグルにおける広告の考え方を説明するとともに、広告に使われる情報をユーザーが管理できるようになっている。例えば、グーグル検索を実行すると、検索結果と一緒に広告が表示される。その時、よりユーザーに役立つ広告を配信するために、過去の検索や閲覧履歴などを活用することがある。「以前『自転車』を検索していて今回『休暇』を検索すると、休暇中にサイクリングを楽しめる観光地の検索広告が表示される可能性もあります」とグーグルは説明している。こうした広告配信の仕組みはGメールやユーチューブなどのサービスでも基本的には同じである。つまり、どのような広告が表示されるかは、ユーザーがネット上に残した情報によるということである。

一方で、ユーザーも表示される広告を管理することができる。「たとえば、YouTubeで最近のサッカーの試合のハイライトを視聴した場合や、Googleで『近くのサッカー場』を検索した場合、Googleはそのユーザーがサッカーファンだと判断することがあります。また、Googleのサービスを利用する広告主のサイトにアクセスした場合は、そのサイトでのアクティビティを基に広告が表示されることがあります。広告のカスタマイズがオンになっている場合、カスタマイズに使用するデータ（年齢や性別、推定された興味や関心、広告主に対して以前に行った操作など）の選択や、これらのデータを使用する理由の確認、広告のカスタマイズの無効化などの操作ができます。カスタマイズを無効にして

も広告は表示されますが、ユーザーとの関連性は低くなります」

なお、「Googleでは、広告主やその他の第三者が個人を特定できないような形で、ユーザーの検索内容、位置情報、使用したウェブサイトやアプリ、表示した動画や広告、ユーザーがGoogleに提供した年齢層や性別などの基本情報を含むデータを利用することがあります」と明記されているところが、アップルとは本質的に大きく違うところである。

また、そうした情報をグーグルの「パートナー」と共有することも明記されている。「Googleは、個人を特定できない情報を公開する、またはGoogleのパートナー（サイト運営者、広告主、デベロッパー、権利者など）と共有することがあります。たとえば、Googleサービスの一般的な利用傾向がわかる情報を公開します。また、特定のパートナーに、広告および測定の目的でパートナー自身のCookieや類似の技術を使用してお客様のブラウザまたはデバイスから情報を収集することを許可しています」

4｜より最適な広告を配信するためにクッキーを活用

クッキーについてはどうであろうか。その利活用の仕方は、アップルとグーグルで異なる点の１つである。グーグルは、グーグルパートナーという第三者とクッキーを共有し、ユーザーごとの最適な広告配信に利活用している。アップルが「Apple News」や「App Store」といった自身の広告プラットフォームに閉じたなかでの広告配信にクッキーを利用するのに対して、グーグルは、言わば、デジタル広告のエコシステムのなかで広告収入を得るためにクッキーを利用していると捉えられる。

「Cookieは広告の効果を高める機能を果たします。Cookieがなければ、広告主はターゲットにリーチしにくくなり、表示された広告数やクリック回数の把握も困難になります」

「ニュースサイトやブログなど多くのウェブサイトは、Googleと連携して、訪問者に広告を表示しています。Googleは、パートナーと協力して、さまざまな目的にCookieを使用することがあります。たとえば、同じ広告を何度も表示しないようにしたり、クリック詐欺を検出して停止したり、より関連性が高いと考えられる広告（ユーザーがアクセスしたウェブサイトに基づく広告など）を表示したりするためなどに使用することがあります」

「Googleでは、Googleが配信する広告の記録をログに保存しています。通常これらのサーバーログには、ユーザーのウェブリクエスト、IPアドレス、ブラウザの種類や言語、リクエストの送信日時、ブラウザを一意に識別する１つ以上のCookieが含まれます。Googleがログデータを保持している理由はいくつかありますが、最も重要な目的は、サービスの向上とシステムのセキュリティ確保です。Googleでは、このログデータを匿名化しています。９か月経過した時点でログデータのIPアドレス部分が削除され、18か月経過した時点でCookie情報が削除されます」

5｜オープンなエコシステム「プライバシーサンドボックス」構想

クッキーに関連する最近のグーグルの動きを、以下に３つ紹介する。

１つめは、先に述べたように、ブラウザ「クローム」におけるサードパーティクッキーの利用制限である。グーグルは、2020年１月、今後２年以内に、「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（「サードパーティクッキー」）の利用を制限するとの計画を明らかにした。このことは、デジタル広告におけるターゲッティング精度の低下、しいてはデジタル広告の提供にかかわるアドテック・ベンダーの売上・利益の低下につながると考えられる。

２つめは、2020年２月リリースの「クローム80」から、ウェブのプライバシーとセキュリティの強化を目的として、「SameSite ｅクッキー（SameSite属性）」の設定を変更したことである。

「SameSiteクッキー（SameSite属性）」とは今ひらいているウェブサイトに貼られたリンク先へ移動する時（今ひらいているウェブサイトのドメインから別のウェブサイトのドメインへリクエストを送る時）、クッキーもいっしょに送るか・送らないかの設定を可能にするものである。３つの属性パターンがあり、「Strict」はクッキーを別のサイトへ送らない設定、「Lax」は送らない条件がStrictよりも緩い設定、「None」はクッキーを別のサイトへ送る設定。クッキーを別のサイトへ送る「None」設定にすると、クロスサイトリクエストフォージェリーなどセキュリティ上の脆弱性を生むことになる。

従来、クロームは「SameSite クッキー」がデフォルトで「None」になっていたことから、デジタル広告の提供にかかわるアドテック・ベンダーなどは「サードパーティクッキー」を使用してユーザーを複数のサイトにまたがって（クロスサイトで）追跡できていた。しかし、「クローム80」以降はデフォルトの設定が「Lax」に変更されたことから、クロームからアクセスするサイトと同じドメインのクッキー、つまり「ファーストパーティクッキー」しか設定されなくなった。

この「SameSiteクッキー（SameSite属性）」の設定変更によって、クッキーによるマッチング精度は低下する可能性があり、アドテック・ベンダーなどは適切な変更を行わなければ従来使えていたマーケティング資産が使えなくなる可能性も出てくる。

そして、３つめの動きが2019年８月に打ち出された「プライバシーサンドボックス」構想である。

グーグルは、クッキーの大規模な利用制限はフィンガープリントなどの不透明なテクノロジーを助長させることにつながり、逆に個人のプライバシーを損なうという考え方をとっている。そこで、グーグルが構想するのが、2019年８月の開発者向け年次会議「I/02019」で計画が発表された「プライバシーサンドボックス」である。

「プライバシーサンドボックス」とは、広告主がユーザーの個人情報に直接アクセスすることなく

ターゲティング広告を行うためのオープン・プラットフォームです。「サンドボックス」には「子供が遊ぶ砂場」という意味があるが、インターネットにおいても砂場のようにプライバシー面で安心できる空間・仕組みを創るというグーグルの意図が伝わってくる。

おおまかな仕組みはこうである。広告主ではなく、ブラウザ「クローム」がユーザーの個人情報を保有・管理する。広告主は、「プライバシーサンドボックス」にあるプライバシー保護APIなどのツールを使いながらユーザーの個人情報を利活用、プライバシーを侵害することなくターゲティング広告を行う。オープンソースで、オープンなウェブ標準にすること、サファリやファイヤーフォックスといったグーグルのサービス以外にも適用してもらうことを目標としている。まだすべてが明らかになったわけではないが、考え方次第では、グーグルを中心とする新しいターゲティング広告のエコシステムとも捉えられよう。

3――「データの利活用」と「プライバシー保護」の両立

アップルやグーグルなどデジタル・プラットフォーマーのビジネスモデルは、ITやデータの活用により、事業者、消費者、広告主など複数のユーザーを結びつけるサービスを１つのプラットフォーム上で提供するというものである。そして、デジタル・プラットフォーム上には必然的に、ユーザーの個人データ、個人情報が蓄積されることになる。このビッグデータこそデジタル・プラットフォーマー最大の強みであり、その「データの利活用」は彼らの成長の源泉となってきた。

こうした強みは、新型コロナウイルス（COVID-19）感染拡大に対する施策としても活かされている。

特に、アップルとグーグルは、それぞれ、マップアプリケーションから収集するユーザーの位置情報を利活用して、アップル『移動傾向レポート』、グーグル『COVID-19 コミュニティモビリティレポート』を作成・更新、開示している。これらレポートは、COVID-19の影響を受けて、人々のモビリティ、つまり移動がどのように変化したのかを示すものである。レポートの目的の一つは、各国当局におけるCOVID-19に関する政策立案を支援すること。これらは、ソーシャル・ディスタンシングや外出制限への効果の把握にも役立ち、また集団感染（クラスター）がどこで発生するのか、追加の医療リソースをどこに割り当てるべきなのかといった予測にも利用することができる。

例えば、グーグル『COVID-19 コミュニティモビリティレポート』の作成に使われているのは、グーグル・アカウントに記録された個人情報である。グーグル・アカウントには、設定次第では、検索や視聴の履歴といっしょに、何月何日のおおよそ何時何分にどこを訪れたのか、その訪れた地点の位置情報やその行程といった移動履歴が記録されている。レポート作成には、グーグル・アカウントでのこれら位置情報、移動履歴の記録がオンになっているユーザーから収集される匿名のデータセットが使われている。

さらに特筆すべきが、2020 年４月 10 日付けプレスリリースで発表された、アップルとグーグル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開発で協力するという取組みである。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「iOS」とグーグル「アンドロイド OS」の間で相互に運用が可能とされている。

５月には、公衆衛生当局が提供するアプリを利用する「iOS」端末と「アンドロイド OS」 端末間で相互運用を実現するアプリケーション・プログラミング・インターフェイス（API）がリリースされた。これらのアプリは、ユーザーがそれぞれのアプリストアからダウンロードできるようになっている。さらに両社は、基盤となるプラットフォームにこの通知機能を組み込むことによって、より広範な Bluetooth ベースで濃厚接触の可能性を検出するプラットフォーム構築を目指すともしている。

コロナ禍における、ユーザーの個人情報を利活用したモビリティレポートの作成、「iOS」「アンドロイド OS」連携による濃厚接触の可能性を検出するテクノロジーの開発といった、アップル・グーグルの強みを活かした施策は、「データの利活用」の観点から世界中のほとんどのスマートフォンを対象とし、高い実効性を期待することができる。

しかしその一方で、個人情報にかかわるビッグデータを持つデジタル・プラットフォーマーによる取組みという点においては、プライバシーに関する懸念を完全に拭い去ることは難しい。

本稿で概観した通り、確かにアップルやグーグルはプライバシー保護への対応を進めてきているが、彼らの取組みを文字通り評価してよいものか、疑問を呈する声があるもの事実である。実際、本年１月に開催された CES2020 での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？』では、プライバシー保護で先行するアップルでさえも、プライバシーや個人情報の保護に関して厳しい目を向けられた。

さらには本年７月 29 日、米国下院の司法委員会は公聴会「Online Platforms and Market Power（オンラインプラットフォームと市場支配力））」を開き、米国プラットフォーマー企業４社（アマゾン、アップル、グーグル、フェイスブック）の CEO がオンラインで市場支配に関して証言を行った。同公聴会は、４社それぞれが、米国反トラスト法に違反する行為を行っていないか、独占的、優越的な地位を利用して不当に利益をあげたり適正な市場競争を妨げたりしていないかヒアリング調査することが主たる目的であった。

公聴会では各社とも、反トラスト法違反の疑いや指摘に対して、世界では激しい競争が存在しているとして反論している。しかし、プラットフォーマーは、「ビッグデータ×AI」で囲い込みを推し進め、さらなるデータ収集及び AI 解析によって最適な商品・サービスやシステムを提供することで、プ

ラットフォームそのものを拡大・強化し続ける。その強大な存在は市場競争への脅威となり、分割すべきとの議論もなされている。

強さの源泉である競争戦略によって起こる独占・寡占に対する批判にどのように対処するのか。これは、個人情報やプライバシーの保護に関する議論の高まりとも相まって、米中メガテック企業に突き付けられた課題である。

「プライバシー保護」にかかわる法規制強化の流れはもはや不可逆であり、「ビッグデータ×AI」によって個人情報を事業の核に据えてきたGAFAなどデジタル・プラットフォーマーには、「プライバシー保護」の概念を製品・サービスの設計・開発段階から取り入れることが求められている。彼らは、今後否応なく、「データの利活用」と「プライバシー保護」の両立というテーマへより高いレベルで対峙することになってこよう。