Ⅱ 欧米を中心とした新しいデータ保護にまつわる動き

一般社団法人Privacy by Design Lab　代表理事　**栗原 宏平**

2018年５月30日のGDPR（EU一般データ保護規則）施行から約２年半が経過し、個人データ保護を取り巻く環境も徐々に変化しつつある。特に国を越えたデータ移転に関しては、これまで議論されてきていた欧州米国間でのプライバシーシールドが無効になるなど、今後国を越えたデータビジネスへの影響もより広がっていくと考えられる。

Ⅱ-1．欧州のデータ保護関連動向

1．GDPR下での判例とその傾向

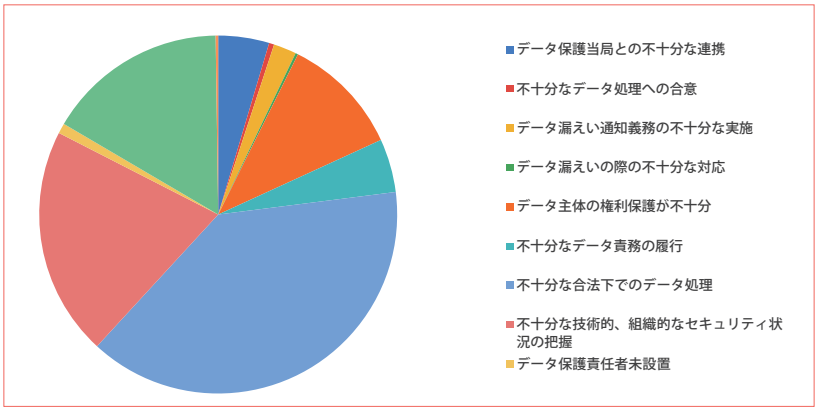
GDPRが施行されて以降、2020年11月８日（レポート執筆時）までの約２年半の期間で435件の制裁金事例が発表されている。制裁理由を順に見ていくと最も多かったのが、不十分な合法下でのデータ処理（169件）、次いで不十分な技術的、組織的なセキュリティ状況の把握（90件）、データ保護下でのデータ処理規則コンプライアンス違反（71件）となっている。上位３つの理由が全体の75％を占める結果となり、組織内でのデータ処理やコンプライアンス違反が数多く制裁理由として挙げられている（複数の制裁理由を指摘されている事例については、その中でも制裁理由として取り上げられている上位理由とした）。

制裁金事例が多い点については、企業内での個人データを取り扱う機会が増えたことも一つの理由と考えられるが、それ以外に組織内で個人データに関する共通認識がうまく浸透できていない点も考えられる。消費者保護の観点からは、事前に十分なデータ保護の対応を実施することに加えて、消費者からの問合せや個人データ漏えいが起きた際の適切な通知および対応などが早急に求められる。

GDPRに関しては、GAFAを始めとした大手テクノロジー企業に注目がいくことが多いが、実際は中小企業や非テクノロジー系の企業など、これまで個人データを十分に取り扱っていなかった企業が急速なデジタル化対応を進めていく中で、十分に内部体制が整備されていないことによって問題になるケースも少なくない。そういった意味では、昨今DXと呼ばれるようなデジタル化を推奨するだけでなく、内部での個人データ保護、および個人データ処理に関しては組織ガバナンスとして適切に対策を講じる必要がある。

2．GDPR下で執行の問題

制裁金に関してはこれまでの制裁金に関する発表を参考に紹介してきたが、一方でGDPR下のデータ保護法の下での執行に大きな課題が生じてきている。執行における問題点として、執行に係る制度設



図Ⅱ-１．GDPR Trackerよりインシデント別分類（2020/11/８時点）

計が挙げられる。欧州域内の複数国に跨りデータ利用を行う事業者に対してはワンストップショップと呼ばれる制度を導入し、代表監督当局（Supervisory Authority）と呼ばれる1カ国（大抵は本社がある国）の監督当局から承認を得ることによって、その他の国からは承認を得る必要がなくなる制度を採用している。これは、複数国に跨ってデータビジネスを実施する際の手続きを緩和するために導入が決定した制度で、域内のデータ流通の意味合いでも有効に機能すると考えられていた。しかし、実際は管理当局と他国のデータ保護監督当局（Data Protection Authority）が執行の意思決定を行うための情報提供での連携が必要になるなど、執行までの手続き上多くの問題が発生しており、想定以上に執行まで時間がかかっている。

ワンストップショップの適用と異なる決定が発表された例としてはGoogleがフランスのデータ保護監督当局によって透明性のある情報提供を行う義務に違反したとして制裁を課せられたケースがある。このケースでは最終的にGoogleの欧州統括拠点があるアイルランドデータ保護監督当局ではなく、フランスのCNIL（データ保護監督当局）が管轄権限を有する、とフランス国家評議会（Conseil d'etat）によって発表されている。Googleはアイルランドデータ保護監督当局が執行を実施していると主張していたが、データを活用してビジネスを展開する地域によって判断されるべきという判断になったケースである。

他方で、Facebookのケースではベルギーデータ監督当局との間でデータ保護に関する調査で意見交換を行った上で、どの国が代表監督当局として調査を実施するか検討に入るなど、ケースによって判断が異なり、現時点で明確な解は見つかっていない状態である。

テクノロジー企業の本社が集積するアイルランドでは、2019年10月に160万ユーロを追加で予算調達し、人員の増加を実施すると発表しており、調査体制を強化していく考えである。これにより、各国のデータ保護監督当局との連携をスムーズに行いテクノロジー大手企業への対応も強化していく方針で進めている。

3．市民団体を通じた訴訟問題

GDPRの執行に関する問題に対して、市民団体や弁護士事務所による集団訴訟も徐々に始まっている。英国とオランダでは、セールスフォースとオラクルが展開するリアルタイムビディング（広告のオークション入札）に対して、十分にユーザ同意を取得しない状態でデータ処理を実施しているとして集団訴訟が起きている。このケースではThe Privacy Collectiveと呼ばれる非営利組織が中心となり、アムステルダムの地方裁判所に申立てを行っている。提供するサードパーティCookieや広告に関するテクノロジーの解釈を争点として訴えを起こしているBureau Brandeisと呼ばれる法律事務所が訴訟を担当しており、同様にロンドンの高等裁判所ではCadwalader法律事務所が担当し訴訟を行っている。こういった集団訴訟が起こり始めている背景には、各国のデータ保護監督当局がアドテクノロジー（リアルタイムビディングを含む）に対して、適切に制裁を加えることができていないという背景がある。

英国ICO（情報コミッショナーオフィス）は2020年始めに複数のプライバシー関係者よりアドテクノロジーのデータ保護違反に関して指摘を受け、調査を開始しているにも関わらず、一定の成果を上げられていない点が指摘されている。特にデータ保護評価（DPIA）に関しては、制度として未成熟な部分が多く、データ保護監督当局も精査を行うにあたり、相当の労力が必要とされている。そのため、市民団体やプライバシー専門家からはデータ保護監督当局のリソース不足や不備などが指摘され、監督当局を通さずに集団訴訟を行うケースが生まれていると考えられる。

別のケースでは、英国のUberがADLU（アプリドライバー宅配便組合）によって採用するアルゴリズム問題を指摘されている。オランダの裁判所で行われて争点になった問題は、採用したアルゴリズムを通じて機械がドライバーに対して利用停止を促す仕組みを実装していた点が指摘されている。GDPR第22条では、「プロファイリングを含む個人に対する自動化された意思決定」という項目で、データ管理

者がデータ主体（この場合はドライバー）の権利を安全に守るために機械処理に加えて人の介入が必要なケースも定めており、Uber側でのデータ処理が適切に行われていないのではないかということがこのケースの争点になっている。背景として、ドライバーがサービス提供において不正を実施していないと主張したにも関わらず、その主張を十分に検討せず、ドライバーが不正な行為を働いたとしてシステム上で自動利用停止処理を行ったことが発端となった。Uber側は内部スタッフによって利用停止処理かどうかを精査した上で決定したと表明しているが、Uberが明記する不正に対する解釈があまりにも広義であるために、説明責任の要求をドライバーは求めている。

紹介した2つのケースは共に新しいテクノロジーを組織内部で実装し処理した事例になるため、データ保護監督当局だけでは調査および判断が難しいケースである。監督当局のリソース問題に加えて、緊急性を要する場合などは監督当局を通さずに弁護士事務所や市民団体、組合等の第三者機関を通じた訴訟などが今後も増えていくと考えられる。

4．EU-USプライバシーシールドの無効化

2000年にEUから米国にデータ移転する枠組みとして欧州委員会と米国間で合意されたセーフハーバー協定が2015年10月6日に無効（Schrems I事件）とされて以降、協定にかわる新たなフレームワークを認めるよう議論が行われ、その結果、新たな枠組み「プライバシーシールド」が2016年8月1日から開始された。しかし、2020年6月16日欧州司法裁判所（ECJ）よって「欧州が要求するデータ保護レベルに米国国内法が条件を満たしていない」と判決が下され、プライバシーシールドは無効となり、このフレームワーク利用を検討中、および、すでに利用していた米国の5,000社以上の企業が影響を受けることになった。以後は標準契約条項（SCC）を利用し、個別のケースで欧州が定める要求に十分対応できているかを精査した上で、データ移転が可能かどうかの判断を行うことになる。

条項に関しては各国のデータ保護監督当局によって精査粒度が異なることに加えて、個別企業によってはデータ移転が認められないケースがある。実際、Facebookは欧州と米国の間でのデータ移転について、欧州本社を管轄するアイルランド裁判所により、9月14日に一時的に停止するよう要求されている。

欧州と米国間では特に民間企業に対して政府による介入が合法か違法か、が問われており、欧州側は米国の既存法の下で十分にデータ保護が実現できないとして今回のフレームワークの停止に踏み切っている。米国の既存法として問題視されているのが外国情報監視法（FISA）第702条である。米国下院での可決により、国家安全保障局（NSA）が令状なしでインターネットを監視できる外国情報監視法の延長を2018年1月から6年間認められることになった。民主党および共和党の一部の議員からは反対の声が上げられたが、法によってNSAがプライバシーへの介入が可能になる期間が延長され、欧州側では米国の外国情報監視法に対する懸念からプライバシーシールドの停止に踏み切ったとされる。

フレームワーク停止問題はすでにプライバシーシールドを利用してデータ移転を実施している企業が存在していたため、対応の修正が求められる点と、中小事業者にとっては個別対応コストが重くのしかかるという点が挙げられる。

前者に関しては、Amazon社が2020年11月にドイツの欧州社会データ保護組織（EuGD）からミュンヘン裁判所に訴訟を起こされている。プライバシーシールド無効が発表されてから2カ月以上が経った段階で移行が進んでいないという理由で、消費者保護の観点から訴訟に踏み切った。

プライバシーシールドの無効化は、主に各国の政府による介入が合法的に行われるかどうかが一つの争点になっており、現在十分性認定が行われている国に関しても再度見直し等が入る可能性はある。

プライバシーシールドの無効化に伴い、欧州の一部の国ではデータ保護監督当局によって米国のクラウドシステム以外を利用するように推奨する動きが出始めている。CNILはマイクロソフトのAzure、AmazonのAWS、GoogleのCloudサービス以外を利用する推奨通知を実施している。健康データ等センシティブなデータに関しては国レベルのシステム利用

を推奨し始めている。外国情報監視法による米国企業への影響は欧州域内のビジネスにも及びつつある。

SCCに関しては2020年12月10日までコンサルティング期間が準備されており、コンサルティング後の2021年の早い段階から改訂版が発表される予定である。改訂版ではこれまで明記されていなかった点が明記されることに加えて、越境データ移転に関して事前の審査がより明確に求められるようになる。

改訂版は既存のSCCよりも広範囲に確認事項が要求される予定で、特に越境データ移転に関してはデータを輸出する国とデータを輸入する国（たとえば、欧州のフランスから米国へデータを移転する場合）、のデータ保護レベルが輸出国のデータ保護レベルに十分に準拠しているかの査定が要求される。

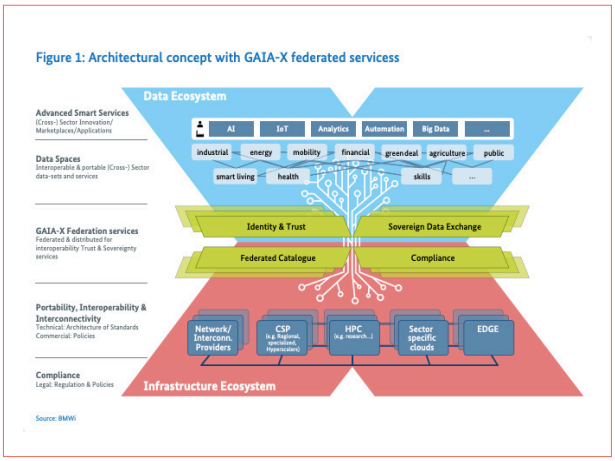
既存のSCCではデータ管理者、データ処理者に関するデータの処理に限定されていたため、それ以外の項目に関しては個別に複雑な項目を処理する必要があり、非常に非効率であった。改訂版に関しては、データ処理者間、およびデータ処理者とデータ管理者間に関しても明記される予定で、複雑なGDPRのデータ保護に幅広く対応できるように項目を広げる検討が進んでいる。

個人データのセキュリティ強度に関してはより厳格に求められる予定で、特にデータ輸出者が拠点を置く国のデータ保護レベルに関しては、政府からのデータアクセスが法的に認められるか否かが争点になる。そのため、十分な技術評価と厳格な管理が必要になる。

改訂版のSCCが有効になるまでは、既存のSCCを活用することが求められる。改定後はデータ輸出者とデータ輸入者間での見直しが必要になる。

5．欧州統一のクラウドシステムの開発

欧州ではデータ保護規則以外にもさまざまな個人データにまつわるプロジェクトをスタートさせており、欧州間で統一したクラウドシステムの開発も進めている。GAIA-Xは代表的なプロジェクトの一つである。2019年にドイツ、フランス政府の取組みとしてスタートしたプロジェクトは、財団本部をベルギーに持ち、合計で22の組織と団体（フランス11、ドイツ11）で構成されている。



図Ⅱ-２．GAIA-Xのコンセプトの図　GAIA-X資料より

GDPRや欧州サイバーセキュリティ法の下で透明性と相互互換性を担保した欧州独自のデータ共通インフラとして実装が進んでいる。

プロジェクトの背景としては、中国、米国によるクラウドマーケットの寡占化への対抗と域内の個人データへのセキュリティ懸念から独自のシステム構築に踏み切った形で、域内でのパートナー連携を今後は拡大させていく予定で、データ主権を個人に提供したクラウドシステムの設計を目指している。

6．欧州域内でのデジタルサービス提供者への新たな規制

欧州では2000年７月に電子商取引指令と呼ばれるオンラインサービスにおける指令を定めており、オンラインサービス事業者に対して透明性のある情報の提供、電子契約と中間事業者の法的責任の制限や商業的なコミュニケーションの必要性を求めている。指令は欧州域内のデジタル単一市場での電子商取引に対して、消費者との公正な取引を実現するための基準としての役割を担っている。

現在、電子商取引指令に関して新しく法制化の動きが始まっており、デジタルサービス法（Digital Service Act）と呼ばれる取引指令を規制化する議論が進んでいる。これはデジタルサービスを利用する消費者に対して、プラットフォーム企業が適切な

ユーザコンテンツ運営に対して法的責任を持つものである。これによりデジタルサービスを展開するプラットフォーマー企業はオンラインサービス上で提供されるコンテンツに対し、アルゴリズムやシステム等の透明性を担保するなど、一部責任を課せられることになるが、サーバを通じて違法なコンテンツが流通した際のプラットフォーマーの責任は免除される可能性がある。これは、取引指令から引き継がれる可能性が高い免除内容の一つで、現在責任の所在に関して議論が行われている。

プラットフォーマーに対しては相互に互換性のある仕組みを検討し、データ共有が実現できるように取り組むように働きかけを行っている。実際に、大手EC取引事業社（Amazon、Alibaba、eBay、楽天等を始めとしたオンライン商取引事業者）、ソーシャルメディア等サービス事業社（Facebook等）と欧州委員会ディディエ・レンデルス議員は面会を行い、コロナ禍でプラットフォームを利用する不正取引事業社の取締りに関して協力するように訴えかけている。特にコロナ禍では、インターネットプラットフォームを介して商品を購入する機会が増えたことにより、不正な取引や詐欺取引が横行していることから、消費者保護に向けた協力を進めていきたいという意向を欧州委員会では示している。

7．デジタル広告のフレームワークに関する動き

ネット広告業界団体のIAB 欧州（Interactive Advertising Bureau）はIAB Tech Labと協力し、2019年８月21日にTCF v2.0（透明性と同意のフレームワーク）を発表し、広告主や媒体を運営する企業、アド（広告）テクノロジーベンダーらが規制への準拠を支援する枠組みを公開している。このフレームワークに沿ってCMP（同意取得・管理プラットフォーム）等の実装が行われており、アドテクノロジーベンダーの間で幅広く普及が期待されていた。

GDPRや想定されていたeプライバシー法（2017年より検討が進んでいたが、現時点では業界団体からの反対等もあり、2021年の制定も見送る方針）対策としてフレームワークを標準的に活用する機運が高まっていた。しかし、10月にベルギーデータ保護監督当局より、IAB欧州が提供するTCFに関して、GDPRが定める法的な要求を満たしていない、RTB（リアルタイムビディング）のような広告オークションの仕組みは高速で個人データの取引が行われるため、法で定めるデータセキュリティ要求に見合っていない、という見解が調査を通じて発表された。

これに対してIAB欧州側はブログを通じて指摘を受けた点に対する返答と、引き続きデータ保護監督当局とは意見交換を行っていくと発表した。加えて、今回のベルギー当局からの調査に関しては第一回のレビューでフレームワーク運営すべてに影響することはないと発表している。今後は、ベルギーデータ保護当局以外とも定期的に情報交換およびフレームワーク自体の改善も発表していくと考えられるため、アドテクノロジー分野のビジネスはフレームワーク動向に注目が必要だと考える。

TCF以外にも各国の個人データ保護法の下で明確に個人データに関する定義を定めていない地域もあるため、アドテクノロジービジネスに関しては、各国のデータ保護制度の変化に敏感に対応していくことが必要になる。

8．日本に関連した今後の影響

（1）GDPR対策の動き

GDPRを前提にしたガイドラインが数多く発表されているが、事業者としてはガイドラインの読込みを前提知識として準備が必要になると考えられる。国内ではテクノロジー大手企業を中心に多額な賠償金の判例が取り上げられることが多いが、中小規模の企業を対象にした判例も数多く公開されているので、所属する業種に合わせてどういったインシデントが起きる可能性があるか、事前に確認した上で対策を実施する必要がある。

データの越境移転に関しては、2021年のBrexit後の欧州と英国間でのデータ移転に関する議論が大きなテーマになると考えられる。これまで英国と日本でデータ移転を実施していた企業も見直しが入る可能性があるので、今後の動向およびアップデートに注目する必要がある。

（2）フレームワークの妥当性に関する動き

デジタル広告を始めとしてこれまで数多くのフレームワークを業界団体が開発してきているが、ここにきてフレームワークと法の整合性に関する議論が行われている。代表的なデジタル広告のフレームワーク（TCF）に関しては、ベルギーデータ保護監督当局より前述のとおり指摘されており、今回の調査以外にも、法との整合性に関する議論を実施していく中でフレームワーク自体が修正される可能性がある。そのため、現在利用しているGDPR対策ソリューションが十分にGDPRの要求を満たしているか、見直しも迫られる可能性も出てくるため、今後の判決や動向のアップデート、およびデータ保護インパクト評価（DPIA）を行う必要があると考える。

Ⅱ-2．米国のプライバシー関連動向

1．CCPAの施行とプライバシー判例動向

2020年1月より施行されたCCPA（カリフォルニア州消費者プライバシー法）は施行当初、子供のプライバシー等を中心に精査を行うと発表されており、7月1日には最終的な修正案が司法長官によって承認された。修正案の中にはいくつか個人データの取扱いに関してポイントとなる点が見られる。

一つがAB713（匿名化された健康情報に関する法案）によるCCPAの適用除外である。これは、HIPPA（医療情報のポータビリティおよびアカウンタビリティ法）の要件に従い、匿名化された情報に関してCCPAの適用条件が除外されるというもの。これまではHIPPAとCCPA双方で匿名化に関する条件が異なっていたため、双方の法律が適用されることで医療関連のデータ処理が複雑になることが問題とされていた。今回はその修正が加えられた形となった。加えてAB1281（従業員情報および企業間取引における個人データに関する法律の適用猶予を2022年1月1日まで延長する法案）が9月に承認されたことである。なお、11月3日に実施された住民投票によってカリフォルニアプライバシー権利法（CPRA）が承認されたため、適用除外は2023年1月まで延長された。

2．2020年にCCPAの下で起きた訴訟

2020年1月に施行されて以来、CCPAの下で23件の訴訟が確認されている（IAPP調べ、2020年10月19日まで）。代表的な訴訟は2月3日に提訴されたセールスフォースおよび子供服販売のハンナ・アンダーソンに対する集団訴訟の問題である。この訴訟ではセールスフォースのソリューションから流出した個人データに関して、暗号化された個人データが不正アクセスを受けた場合にCCPA違反となるかどうかが争点になっている。

Zoomに対する集団訴訟問題は、利用者に対して明確な同意なくFacebookを含む第三者に対して個人データを公開していた問題が問われている。この問題は、ZoomがSDK（ソフトウェアデベロップメントキット）と呼ばれるFacebookが提供していたソフトウェア開発キットを導入することで、開発キットを通じてFacebookに同意なく個人データが渡っていたにも関わらず、プライバシーポリシー等で十分に説明を実施していなかった点が争点になっている。

これ以外にもソーシャルメディアサービスを中心として訴訟が起こっており、今後、カリフォルニアを中心にデータビジネスを展開する際には事前に対策を確認しておく必要がある。

3．カリフォルニア州プライバシー権法の可決と今後

大統領選が行われた11月3日にカリフォルニアでは複数の住民投票が同じタイミングで実施された（最終的に賛成9,233,900票、反対7,203,295票で可決）。CPRAはCCPAの提案にも関わったプライバシー保護団体の「カリフォルニアンズ・フォー・コンシューマ・プライバシー（Californians for Consumer Privacy）」によって推進され、これまでCCPA下で争点になっていたデータの第三者提供の解釈を“Selling（販売）”ではなく、“Share（共有）”と解釈して規制を回避しようとする企業に対し、よりプライバシーが保護される仕組みを設計する狙いから始まっている。CPRAは2023年1月以降で施行

される予定で、それまではCCPAの下でプライバシー規制が行われる。CPRAの施行によって変化していくポイントとしては、以下の点が考えられる。

・ビジネス目的での個人データ共有の制限
・正確な位置情報、人種、医療情報等のセンシティブな個人データにあたる情報の利用制限
・必要以上の個人データ保持の禁止
・16歳以下の個人データに対する罰則の強化
・カリフォルニア州プライバシー保護庁の設置
・消費者のプライベート権利の拡大
・オプトアウトリンクへの新たな責務の作成

これ以外にCCPAでは“Sell”という解釈だけでなく、“Sharing”という文言が追加され、新しく金銭的な見返りに関わらず、第三者間でビジネス上価値のある行為を行っている場合（“cross-context behavioral advertising（クロスコンテキスト行動ターゲティング広告）”）に適応されることになる。

消費者は“Sell”、“Sharing”が行われたデータをオプトアウト請求できるというのがCCPAに追加される新しい考え方である。これ以外にも一部消費者に対して権利を認めるなど、CCPAと比較してプライバシー保護を強化した形の法案として検討されていく予定である。

4．米国連邦プライバシー法の制定と議論

連邦プライバシー法に関する政策は民主、共和両党からすでに提出されており、選挙後に一部動きがあると考えられる。民主党上院議員により2019年11月に消費者オンラインプライバシー権法（COPRA）が提出されている。背景にはオンラインを通じたサービス利用が拡大したことに加え、消費者のプライバシー権を守るだけでなく、消費者の同意なくデータ利用を進める事業者に対する懸念と姿勢を変えていく必要性から法案の提出に至っている。

一方の共和党上院議員により消費者データ保護法（CDPA）、米国消費者データプライバシー法（USCDPA）が提出され、米国国民が消費者として事業者に対し責任を追及できる権利を認めるものとして議論が進められている。

CDPAに関しては両党でも合意されており、今後上院での議論が進められていくと考えられるが、一方で事業者に対して猶予を与えるような解釈にならないか、健康データとは一体何か、など明確になっていない点も多く、今後の議論を通じて具体化していくと考えられる。

連邦法で争点になっているのがプリエンプション（州の法規に対する連邦法規の優先）に関する問題で、消費者が居住する州によってプライバシー保護に対するレベルが異なることを現時点では懸念しており、消費者保護の一貫性を前提にした上で議論が進められていくのではないかとBROOKINGS等の現地メディアが予測している。

連邦法の議論に関しては、USCDPAを修正する形で2020年９月に紹介されたSAFE DATA法（データアクセス、透明性、アカウンタビリティにおける米国のフレームワークを制定した法律）、民主党上院議員、無所属の上院議員が提出した米国生態情報プライバシー法（同意なく生態情報を取得し、取引を行うことは違法であり、顔認識や機械学習等のテクノロジーを活用する際に検討が必要）なども検討されており、連邦プライバシー法の動向は引き続き注目が必要な分野である。

大統領選後はこれまで提出されてきた連邦プライバシー法に関して一部議論が進む可能性があるので、米国で展開する事業者はそれぞれの分野で確認が必要になると考えられる。特にコロナ禍での医療データおよび子供のデータ等は連邦取引委員会（FTC）から警告を受けるケース（TikTokの訴訟等）も増えてきているので、対策が必要になると考えられる。

5．顔認識技術に対する動き

顔認識技術に関してはIBMやマイクロソフト等、これまでに開発を主導してきた企業が一部開発を中止するなど、転換期に差し掛かっている。背景として、技術的な問題に加え、社会全体で顔認識技術に対する姿勢が変化してきているため、社会全体で実装を積極的に進めていく動きに変化が起きている。

米国のオレゴン州ポートランドでは2021年１月よ

りポートランド警察での顔認識技術の利用、および公園や建物等の公共施設（公の学校は除く）での技術の採用を禁止する投票を可決した。ブラック・ライヴズ・マター騒動以降、カリフォルニア州のサンフランシスコ、オークランド、マサチューセッツ州のサマービルの地下鉄でも顔認識技術の利用を禁止する動きが出てきている。

2008年に各州に先駆けて生体認証に関連した法律の制定を行ったイリノイ州では、2015年11月20日にFacebookの顔認証によるタグ付けでのクラスアクション訴訟を一時却下したものの、2020年１月29日にFacebook側から訴訟に対して和解金として600億円を支払う合意を発表している。

アメリカ合衆国税関・国境警備局では生体認証を活用した出入国プログラム（CBP）を実施していたが、政府アカウンタビリティ局（GAO）によって実施された監査で技術的、および運用における問題が発覚し（利用者からのデータ提供要求への不十分な対応、顔認識がどの時点で実施されているかサイト上などで不十分な説明等）、NEC等のパートナー企業に対してもプライバシーを前提にしたコンプライアンス要求に従うように通知された。

GAOによる指摘の中には、CBP全体で十分にプログラムのポリシー設計がなされていなかったこと、技術提供を行うパートナーの監査を十分に実施していなかったことなどが指摘され、同時に技術自体のバイアス等が指摘された。

公共施設に関してはニューヨーク州で2022年までに一時的に学校内での顔認識技術利用を禁止すると発表された。背景にはニューヨーク自由人権協会から2019年にニューヨーク州教育部門が顔認識技術をLockport City Schoolsで採用した件に関して訴訟を起こしていたことが発端となり、学生のデータ保護の権利を毀損しているとして、学生の親から要望を受けていたものである。

このように公の施設や場所での顔認識技術に関する風当たりは徐々に強くなり始めており、技術的な正確性だけでなく、導入にあたってのリスクを十分に検討しておく必要がある。

6．市民および第三者機関によるプライバシーモニタリング組織の動き

法律によるプライバシー規制に加えて、非営利組織や人権団体などを通じた訴訟、およびクラスアクションのケースが徐々に際立ってきている。アメリカ自由人権協会（ACLU）、ACLUイリノイを含めた複数の非営利、人権団体は顔認識技術を提供するClearviewAIに対して訴訟を行い、顔認識技術の危険性に警鐘を鳴らしている。

イリノイの裁判所に持ち込まれたケースでは、イリノイ州の生体認証情報プライバシー権法（BIPA）の下でソーシャルメディア上の個人データをスクレーピングし、個人の同意なくプロファイリングを実施していることを問題としている。ClearviewAIは訴訟を受けて民間企業とのデータ販売の契約（イリノイ州内）を停止し、ライセンスを提供する政府機関のみの契約に変更した。これによってBIPAによる訴訟の免除を訴えているが、それに対して人権団体等からはClearviewAIから原告に対しての説明がないことに加えて、第三者へのデータ提供契約による被害に対しての法的な責任の議論がなされていないことなどを継続して訴えている。

ACLUなどの人権団体以外でもアプリから取得される個人データ権利侵害が発生していないか指摘、警告する第三者組織が誕生している。Future of Privacy Forumよりスピンアウトした国際デジタルアカウンタビリティカウンシル（IDAC）は代表的な非営利組織の一つで、AppleやGoogleが展開するアプリストアを通じてダウンロードできるアプリの調査を実施し、個人データの権利侵害が考えられる際は警告や公表などを実施している。SDK等開発環境をより快適にする仕組みが徐々に普及する一方で、こういった仕組みを通じて違法にデータを取得する（厳密にはプライバシーポリシー上で定義された以上のデータを取得、およびSDK等を提供する第三者へ同意なく転送される）ケースも増えてきており、違法なケースを未然に防ぐために第三者組織が組成され、調査にあたっている。

組織内には弁護士を始めとした法の専門家に加えて、テクノロジーに長けたエンジニアなど複数の

バックグランドを持つ専門家が参加し調査にあたっている。このような動きは各国で非営利組織を中心に立ち上がっており、各国の非営利組織間の連携が今後は進んでいくと考えられる。

10月に発表されたTechcrunchの記事ではIDACが対応したケースが紹介されている。Googleのデータポリシーに違反していた3つのゲームアプリ（Princess Salon、Number Coloring、Cats & Cosplay）がストア上から削除されており、Unity、Umeng（アリババグループのアプリプロモーションプラットフォーム）、Appodeal（モバイル収益化プラットフォーム）のSDKsを活用してアンドロイドID、アンドロイド広告IDを取得していたことが原因となった。特に子供が利用するゲームコンテンツなどはプライバシーポリシーを含めた同意を十分に検討する必要（親の同意含め）があり、ストアなどのプラットフォームのプライバシーポリシーとの整合性（Inconsistency）が求められる。

7．日本に関連した今後の影響

（1）連邦法に関する議論

米国ではオバマ政権以来、連邦法を前提としたプライバシー法に関する議論を積極的に進めてきた。テクノロジーの広がりに伴い、消費者保護の視点から対策が必要になっていることに加えて、越境データ移転に関してはプライバシーシールドが無効とされた判決による影響によって、国内法（消費者プライバシーよりは政府による監視の文脈）の見直しが迫られている。仮に連邦法の議論が進めば、現在の州法とのプリエンプション（州の法規に対する連邦法規の優先）に関する問題が事業者視点では重要になると考えられる。これまでは各州での対策が求められていたが、連邦法でプライバシー法が制定された場合は州法規制との関連性を確認しておく必要がある。また、取り扱うデータによっては（医療データや子供のデータ等）、これまでの法規制とどのように関連してくるのかを理解しておく必要がある。

（2）州法に関する議論

前述のとおり、カリフォルニア州では11月3日の住民投票を通過したためCCPAを改定し、CPRAを2023年施行する事が決定した。これにより住民がセンシティブ情報（位置情報、生態情報等をSPIと定義）の販売制限を要求することが可能になったことに加えて、16歳以下のユーザに対するオプトイン等の要求、カリフォルニアプライバシー保護当局の設置など、これまで以上にプライバシー強化の方向に進んでいくことになる。CCPAのように一律でオプトアウトができるような仕組みとは異なり、マニュアルでサイトごとのオプトアウトが要求されている点も今回新たに加わったポイントになる。

ACLUやEEF（電子フロンティア財団）はCPRAに対して反対の立場を主張しており、事業者側でプライバシーに厳格なユーザに対して公正なサービス提供を実施しなくなる可能性に言及している。（データ取得を拒む際にディスカウントや特定サービスへのアクセスを制限する）。以上の動きからCPRAに関しては2023年施行と少し期間が開くものの、特に広告モデルを始めとしたデータ共有型のビジネスへの影響はより強くなっていくと考えられるため、サードパーティCookieに加えて、日本企業を含めた提供先のデータ保護の内部デューデリジェンス等は、より厳しく求められると考えられる。

（3）越境のデータ移転に関して

越境データ移転に関しては直接米国からの影響を受けるというよりは、日本企業が米国企業のサービス（クラウド等）の導入を実施している場合、欧州に居住する個人のデータを米国のサービスを介して取り扱う際に問題になる可能性がある。越境データの取扱いに関しては、EDPB（欧州データ保護委員会）が発表したガイドラインで、追加の精査（Supplementary Measurement）が求められるとされており、移転元（Exporter）と移転先（Importer）がそれぞれ国を越えてデータ移転が行われる際に、移転先の国が十分にデータ保護レベルに達しているかを事前に精査する必要が出てくる。米国は欧州基準で十分にデータ保護が実施されていないため、日本企業にデータ移転が行われた際、米国サーバ上に個人データが保管されるケースなどで問題になる可能性はある。

越境移転に関しては欧州と米国の企業の間でもプライバシーシールドの無効により、数多くの中小規模事業者が損害を被ることになっている。プライバシーシールドの代替としてSCCを国ごとに確認して、導入を実施していく必要があり、今後日本と欧州の十分性の議論によっては検討が必要になる可能性も考えられる。

（4）その他の動き

大手プラットフォーマーに関しては軒並みプライバシーを重視した動きへと戦略の転換を始めている。AppleはiOS14でよりプライバシーを強化する方向性を発表している。特にアプリ等の開発者およびこれまでAppleが広告で使用していたIDFA（広告識別子）を活用してビジネスを展開していた事業者にとっては、大きく事業戦略の見直しが必要になるだろう。デジタルマーケティング活動においてプロモーションでプラットフォームを選定する際には、AndroidとiOS双方を規約レベルで見比べた上で自社に合わせたプロモーションの選定を行う必要が出てくる。

Ⅱ-3. アジア圏のプライバシー関連動向

最近ではシンガポールでの個人情報保護法（PDPA）に関する動きがいくつか発生している。Data Protection Excellence（DPEX）センターは2016年以降、4年続けて罰則に関するレポートを公表している。2016年には23件、2017年には18件、2018年には23件、そして2019年8月までには26件まで増加している。2020年に発生した例を紹介すると、自動車配車アプリのGrabが2019年8月に個人情報保護委員会（PDPC）へ展開するモバイルアプリの脆弱性を報告し、その後追加調査でGrabHitchのドライバー21,541人の個人データへ非承認アクセスが可能になっていたことが判明した。この件でPDPCより罰金として7,325ドルと120日以内にプライバシーポリシーに見直し要求を求められた。このケースでは始めの報告よりAPIのアップデートを実施していたが、十分にデータ保護対策が実施されていなかった点が問題になっている。

Ⅱ-4. 全体の総括

GDPR施行から2年以上経ち、数多くの判例が各国のデータ保護監督当局によって公表されてきている。国内では一部罰則が大きな事例として取り上げられることが多いが（当初の制裁金よりは減額されるケースも出てきている）、多くは消費者保護の観点から組織内でのデータ管理のミスやアクセス制御に関する問題、同意取得やデータの目的外利用など、組織内の初歩的なミスが指摘されることが多い。

これは企業としてデータ利用を進めていきたいという思惑がありつつも、十分に組織体制が作れていないことの現れであり、国内で取り上げられる大手テクノロジー企業への制裁と比較して、実際は中小規模の非テクノロジー企業が対象になることが多い。大手企業の場合は潤沢に資産があるため、人材や技術への投資が可能であるが、人材や資金に限界がある中小企業にとっては非常に悩ましい問題でもある。そのため、海外ではチェックポイント等を通じて事前にリスクになりそうなポイントを把握するなど、資金的に難しい場合にも対応できる方法の模索が進んでいる。

今後、GDPRだけでなくカリフォルニアで可決したCPRAに加え、ブラジル、中国など世界的に個人データの取扱いに関しては見直しが始まっているため、国内の個人データ保護に関してもある程度各国との整合性を取らざるを得ないのではないかと考える。そういった中で、特に中小規模の事業者は、できる限り必要ないデータを取得せず、かつ目的に沿った形でのみデータ利用を検討することが必要になってくるのではないか。個人データの問題は国内法だけでなく、データ移転の問題から海外動向も理解した上で、データ活用を検討する必要があり、今後はよりその流れが加速していくものと考えられる。