個人情報保護強化の世界的潮流

欧州連合（EU）で一般データ保護規則（GDPR）が施行されてから約 1 年半が経過した。世界各国では、GDPR に追随するように個人情報保護法制の整備・強化が進んでおり、個人情報を取扱う企業の責任も増大している。本稿では GDPR 施行後の状況と今後の展望について概括し、2020 年 1 月 1 日施行予定の米国カリフォルニア州消費者プライバシー法（CCPA）、新興国の個人情報保護法制および日本における個人情報保護法改正の状況を報告する。

１．個人情報保護強化の世界的潮流

個人データがインターネットを介してボーダレスに利活用されるデジタル社会において、企業はマーケティング等に際して個人データを活用し、ビジネスを拡大してきている。GAFA（米国を代表する巨大 IT 企業である Google, Amazon, Facebook, Apple の総称）に代表されるプラットフォーマーがその最たる例で、データ量の増加とプロファイリングによる予測分析等により、個人データの利用価値が益々高まっている。その一方で、欧州委員会が 2019 年 3 月に公表した欧州の住民のサイバー犯罪に関する意識調査結果では、回答者の 79%がサイバー犯罪の被害者になるリスクが増加していると回答しており[1]、人々のインターネットセキュリティーに対する不安は根強い。こうした背景を踏まえて各国において個人情報の取扱いに関するルールの整備・強化が進められている。2018 年 5 月に欧州域内の個人データ保護を規定する GDPR が施行され、2020 年 1 月 1 日からカリフォルニア州ではカリフォルニア消費者プライバシー法（CCPA）が施行される。新興諸国に目を向けると、タイでは 2020 年 5 月にタイ個人情報保護法（The Thailand's Personal Protection Act）が、ブラジルでは 2020 年 8 月にブラジル個人情報保護法がそれぞれ施行予定であり、インドでも GDPR をベースにした個人情報保護法が現在策定されている。また、日本では 2020 年に個人情報保護法の改正が予定されている。

２．欧州 一般データ保護規則（GDPR）

（１）概要

GDPR は、企業による個人データの取扱いと欧州域外への移転に関する規則等個人データのルールを定めている。個人データは「識別された、または識別され得る自然人（データ主体）に関する情報と定義され、氏名、住所やクレジットカード情報だけでなく、位置情報、IP アドレスやオンライン識別子のような技術的情報など、直接的または間接的を問わず、ある個人を特定することができる情報とされている。GDPR には日本の個人情報保護法にはないデータポータビリティに関する規定があるなど、個人データの定義や個人の権利は日本の個人情報保護法よりも適用範囲が広い。

GDPR は欧州 31 ヵ国[2]の住民の個人データが対象であるが、欧州域内から域外へ個人データを移転させる場合には GDPR で定められた基準をクリアする必要がある。欧州域内に拠点がある日本企業や欧州でサービスや商品を提供している日本企業は GDPR の対象となるため注意が必要である。なお、日本は欧州委員会から十分なデータ保護の水準を確保しているとされる「十分性認定」[3]を受けており、個人データを移転する事業者間でデータ移転の際に必要となる標準データ保護条項[4]の締結や本人の明示的な同意が不要となるため企業の事務手続きは軽減されている。

また、GDPR には企業に重大な違反が発覚した場合に制裁金を課す規定があり、2,000 万ユーロもしくは全世界売上総額の 4%のいずれか高い方を上限とした額が制裁金として課せられる[5]。

（２）GDPR 施行後の状況と今後の展開

欧州委員会で法務、消費者権利、男女平等を担当するベラ・ヨロウバー委員は 2019 年 7 月に発表した GDPR 施行後 1 年を総括した声明文で、「GDPR は実を結びつつあり、欧州の人々は自身の個人データを管理するための強力なツールを実装した」と述べている[6]。

欧州委員会が 2019 年 5 月に公表したデータ[7]によると、個人データの取扱いについて、住民から欧州各国当局へ寄せられた照会（Queries）と苦情（Complains）の合計は約 14 万件、データ漏えい通知件数は約 9 万件に達した。GDPR の存在が EU 域内の住民の間で浸透し、消費者の個人情報取扱に対する意識が高まっていると考えられる。

GDPR 施行以降、企業に制裁金が課せられる事例が生じており[8]、主な事例は（図表 1）のとおりである。Marriott International の事例では漏洩元が Marriott International が買収したホテルで、買収以前からデータが漏えいしていたことが発覚し、企業買収時のデューデリジェンスの重要性にスポットがあてられた[9]。

《図表 1》GDPR 施行後の制裁金事例

企業	国	公表時期	制裁金	概要
Google	フランス	2019 年 1 月	5,000 万ユーロ	同社は個人情報の利用目的等を表示したページを複数に分散させており、監督当局は透明性のある情報を提供する義務に違反したと認定した（GDPR12 条）
British Airways	イギリス	2018 年 9 月	1 億 8,300 万ポンド	サイバー攻撃により約 50 万人の顧客データ（氏名、住所、クレジットカード）が流出した。
Marriott International	イギリス	2018 年 11 月	1 億ポンド	サイバー攻撃により約 3 億 3,900 万人の顧客データが流出した。漏えい元は同社が 2016 年に買収したホテルで、顧客データの流出は買収前の 2014 年から始まっていた。

（出典）各種資料をもとに SOMPO 未来研究所作成。

上記の状況から GDPR は一定の目的は達成しており、またすみやかに見直しが図られていると考えられる。

欧州委員会は産業界、団体および専門家に対して GDPR 施行後の影響や認識された課題に関するアンケートを実施し、2019 年 6 月に公表したレポートでその結果を概括している[10]。多くの回答者が GDPR は消費者の基本的人権を守る上で重要なものであると認識する一方、各国の国内規定が GDPR の要求を上回る場合があり、それが事業者への負担となっていると指摘している。例えば、GDPR37 条は公的機関などに対して、個人データの保護を任務とする「データ保護オフィサー」（Data Protection Officer：DPO）の任命を求めているが、ドイツでは個人データを扱う従業員が 10 名以上所属する企業は必ず DPO を任命しなくてはならない。DPO 任命による追加の人員確保は、特に中小企業への負担が重くのしかかっている。

欧州委員会が 2019 年 7 月に公表したレポート[11]では、ドイツの DPO 任命規定に触れ、今後は各国監督当局との対話を通じて GDPR で求められる水準以上の規定を設けないよう事態の改善に向けて努力を続ける旨が示されている。

また、電子通信データに関するプライバシーを保護する e プライバシー規制の最新案が 2019 年 10 月に公表され、現在も施行に向けた審議が進められている[12]。e プライバシー規則ではユーザーのオンライン行動が追跡できるクッキー情報も保護の対象となっており、今後企業がクッキー情報を取得する場合に規制の対象となり、違反が発覚した場合は GDPR と同様の制裁金が課せられる。

３．米国 カリフォルニア州消費者プライバシー法（CCPA）

（１）制定の背景

アメリカでは日本や欧州のように個人情報保護に関する包括的な連邦法や州法は存在せず、児童の情報保護を規定した COPPA[13]や医療保険分野の HIPPA[14]等の事業分野別の連邦法が存在するセクトラル方式が採用されてきた。しかし、2018 年 3 月に発生した Facebook の個人情報不正流出事件[15]や GDPR 施行を契機に個人情報の取扱に対する消費者の意識が高まり、カリフォルニア州では包括的な個人情報保護法制定に向けた法案への住民の署名が集められた[16]。これを受けてカリフォルニア州議会では法案を作成、2018 年 6 月 28 日に知事が署名し、CCPA が成立した。成立後も多くの修正案が提出され 2020 年 1 月の施行時点の条文が確定しない状況が続いてきたが、2019 年 9 月に修正案に関する議会の審議を終了し、同年 10 月 11 日に知事が署名し確定した。

（２）概要

CCPAでは適用対象とする事業者を、個人情報を取得し、その利用の目的と方法を決定する営利目的の事業者であって、カリフォルニア州で事業を行う次のいずれかの要件に該当する者としている。

- 年間売上高が 2,500 万ドルを超えている。
- 年間合計 50,000 件以上の消費者、世帯もしくはデバイスの個人情報を商業目的で入手、購入、販売、共有している。
- 年間売上高の 50%以上を消費者の個人情報の販売から得ている。

事業者にはグループ会社や当該事業者とブランドを共にする事業者も含まれるため、カリフォルニア州に子会社を開設してブランド展開する日本企業も対象となる可能性がある。

CCPA では個人情報を、カリフォルニア州の住民または世帯を、識別し、結び付け、直接もしくは間接に合理的に追跡し得る情報と定義している。世帯に関する情報が含まれるのは GDPR にもない特徴的な点である[17]。また、オンライン上の閲覧履歴、検索履歴や生態認証データ等を幅広く個人情報の範囲とすることが明記されている。

事業者には、個人情報の取得時点までに取得予定の情報の種類および利用目的を知らせる義務がある。オンラインのプライバシーポリシーまたはウェブサイトにおいて、過去12か月に取得した個人情報の種類、情報源の種類、取得等の目的、個人情報を共有する第三者の種類等を開示し、かつ12か月に１回見直すことが求められる。CCPAは個人情報となる情報の範囲がGDPRよりも広く、プライバシーポリシーの年次更改義務などGDPRでは要求されていない規定が存在するため、事業者はその差異に留意しながら対応を進めることが求められる。

カリフォルニア州の住民の主な権利と事業者の主な義務は、(図表 2)のとおりである。なお、消費者が開示請求権等の権利を行使したとしても、事業者はサービスを提供しない、商品を販売しない等消費者を不当に差別することが禁じられている。この差別禁止規定は、CCPA 独自の規定で GDPR では明文化されていない。

《図表 2》CCPA における主な消費者の権利と事業者の義務

権利の種類	消費者の権利	事業者の義務
開示請求権	当該消費者について取得した個人情報の具体的内容、情報源や個人情報を共有する第三者の種類等を開示請求できる。	消費者が開示請求をする手段としてフリーダイヤルおよびウェブサイトを含む少なくとも2つの手段を提示する。 消費者からの開示請求受領後、原則 45 日以内に対応する。 ※ただし、請求内容や件数による対応期限の延長が定められている。
削除権	事業者が収集した消費者の個人情報を削除するように求めることができる。	当該消費者の個人情報を削除し、サービスプロバイダーに記録から個人情報を削除するよう指示する。 ※ただし、一定の条件での事業者の内部利用に限る場合など、個人情報の保持が認められる例外事由がある。
販売停止権（オプトアウト権）	事業者に対して消費者の個人情報を第三者へ販売しないよう求めることができる。	消費者がオプトアウトできるようウェブページ上で"Do Not Sell My Personal Information「私の個人情報を販売しない」"というタイトルのウェブページを設定し、消費者へ当該ウェブページのリンクを提供する。

（出典）各種資料をもとに SOMPO 未来研究所作成。

CCPA違反に関するエンフォースメントとしては、消費者による提訴と州司法長官による提訴がある。

消費者は、事業者に安全管理措置に違反があり、自己の個人情報が暗号化または修正されずに漏洩した場合に、事業者に対して、損害賠償や差止を求めることができる。損害賠償の上限は、1事故1消費者ごとに100ドル以上750ドル以下の法定損害または実損害のいずれか高い方とされている。なお、法定損害賠償の場合、消費者は事業者に対して事前に違反を通知し、その日から30日以内に事業者が違反を是正し、再発防止策を提出した場合には、消費者は法定損害賠償を請求することはできない。

また、州司法長官は事業者が CCPA の規定に違反し、30 日以内に是正できなかった場合は、事業者に対して訴訟を提起でき、7,500 ドルを上限に民事上の罰金を課すことができる。

GDPR では監督当局によって課せられる巨額の制裁金が注目されるが、CCPA では住民による訴訟がクラスアクションに発展し、高額の賠償損害を負う可能性がある。

（３）今後の動向

2019 年 10 月に公表された具体的な権利行使手続き等をまとめたガイドラインへの意見募集が 12 月 6 日で終了し、現在はガイドラインの修正作業が続けられている[18]。CCPA のガイドラインには不確定要素もあるが、施行を目前に控え、多くの企業が急ピッチで CCPA への対応準備を進めている。

また、ニューヨーク州やワシントン州でも個人情報保護法案の制定にむけた動きが見られる。州レベルでの個人情報保護関連の法案制定により、個人情報を取扱う事業者の負担が増大するため、事業者は包括的な連邦法の制定を要望しており、今後の動向が注目されている[19]。

４．新興国の動向

近年、新興国[20]においても個人情報保護法制の整備・強化が進められている（図表 3）。タイ、ブラジルでは GDPR の影響を受けた法律が制定され、事業者に個人情報の取扱いに関する様々な義務が課せられており、欧米に限らず、必要な対応事項を確認し、実施していく必要がある。

《図表 3》新興国における主な個人情報保護法制動向

国名	法律	施行時期	特徴
ベトナム	サイバーセキュリティ法	2019 年 1 月 1 日	データローカライゼーション規定(取得したデータの国内保存を求める規定)あり。
タイ	タイ個人情報保護法	2020 年 5 月 27 日	GDPR をベースとした法律。実損害の 2 倍までの懲罰的損害賠償規定あり。
ブラジル	ブラジル個人情報保護法	2020 年 8 月予定	GDPR をベースとした法律。忘れられる権利、データポータビリティ規定あり。
インド	※現在制定中	未施行	GDPR をベースとした法律。重要個人情報はインド国内のサーバーに保存しなければならない。

（出典）各種資料をもとに SOMPO 未来研究所作成。

５．日本 個人情報保護法改正の動向

日本では個人情報保護法が 2017 年に改正されてから約 2 年が経過した。個人情報保護法は、個人情報保護法制の国際的な動向、情報産業技術の発展、それに伴う個人情報を活用した産業の状況等を勘案して、必要に応じて 3 年ごとに法律改正等の措置を講ずることとされている[21]。2020 年の改正に向けて個人情報保護委員会は、2019 年 4 月に「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」を公表し、意見募集を経て、2019 年 11 月 29 日に「個人情報保護法いわゆる 3 年ごと見直し制度改正大綱（骨子案）」を公表した。骨子案では、個人情報に関する個人の権利、事業者の義務を拡大する内容が示されている（図表 4）。また、個人データの越境移転の多様化を踏まえ、海外の事業者も個人情報保護委員会の報告徴収および命令の対象とされている。

《図表 4》個人情報保護法 見直しの骨子案

主な項目	概要
個人データの利用停止権	個人データの利用停止を求めることができる場合を広げ、個人データの目的外利用や不正取得がある場合だけでなく、広告・勧誘などに対しても利用停止を要求できるようにする。
漏えい報告・本人通知の義務化	一定数以上の個人データの漏えい等について、速やかに個人情報保護委員会への報告と本人への通知を行うことを個人情報取扱事業者に義務付ける。
仮名化情報	他の情報と照合しなければ特定の個人を識別することができないように加工された個人データの類型として「仮名化情報」を新たに設ける。仮名化情報については、事業者の義務が一部緩和される。
クッキー情報等の第三者提供の制限	提供元では個人データに該当しないものの、提供先において他のデータと合わせて個人データとなることが明らかな情報について、第三者提供を制限する。
域外適用	日本国内にある者に係る個人データを取扱う外国の事業者を、個人情報保護委員会による報告徴収および命令の対象とする。

（出典）各種資料をもとに SOMPO 未来研究所作成。

なお、今回の改定では、企業が個人データの削除に応じる「忘れられる権利」の導入は見送られた。今後は、骨子案をベースに年内に大綱が取りまとめられ、来年の通常国会で改正法案が提出される見込みである。

６．おわりに

個人データの利活用が進み、データ価値が高まる一方で、個人情報に関わる不祥事件が相次いでおり、消費者において自身の個人情報がどのように利用され、共有されているか関心や不安が高まっている。各国の個人情報保護法制強化の潮流は、現代社会の要請とも考えられ、GDPR が契機となって世界各地へと波及し、各国の消費者の意識や個人情報保護法制に影響を与えている。

消費者から取得した個人情報を適切に扱うことは事業者にとって消費者と信頼関係を構築するうえで最も重要な事項の 1 つである。近年では事業のグローバル化に伴いボーダレスにオンラインで個人情報が利活用されることが前提となりつつあり、Facebook の個人情報不正流出事件のように個人情報の不適切な取扱いが発覚した場合は、事業者のレピュテーションに甚大な影響を与えるだけでなく、場合によっては市場から淘汰される可能性もある[22]。個人情報が日々グローバルに利活用される現代社会において、事業者は GDPR や CCPA に対応するだけでなく、消費者が安心して個人情報を提供して情報技術の恩恵を享受できるよう、個人情報保護に向けた取組みを継続することが求められている。

【研究員　堀田周作】

---

1 European Commission, *"Internet security：what Europeans think"* March, 2019

2 EU 加盟 28 ヵ国に欧州経済領域（European Economic Area）のアイスランド、ノルウェー、リヒテンシュタインを加えた 31 ヵ国。

3 European Commission, *"EU Japan Adequacy Decision"* January 2019

4 GDPR 第 46 条
標準データ保護条項(Standard Data Protection Clause)とは当事者間で締結されるデータ移転に関する合意書のこと。

5 個人情報の漏洩があったとしても、その事実をもって即制裁とはならないが、漏洩事故が発生するということは何らかのかたちで GDPR を順守できていない可能性があると判断される。

6 European Commission, *"General Data Protection Regulation shows results, but work needs to continue"* July 24, 2019

7 European Commission, *"GDPR IN NUMBERS"* (visited August 20, 2019)

8 British Airways と Marriott International への制裁金はあくまで予告金額であり本稿執筆時点で最終的な制裁金額は確定していない。

9 日本経済新聞「米マリオットがはまった「データ管理の罠」個人情報保護のリスク、M&A 前に精査を」2019 年 7 月 17 日

10 European Commission, *"CONTRIBUTION FROM THE MULTISTAKEHOLDER EXPERT GROUP TO THE STOCK-TAKING EXERCISE OF JUNE 2019 ON ONE YEAR OF GDPR APPLICATION"*. June 13, 2019

11 European Commission, *"COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL"* July 24, 2019

12 Council of the European Union, *"Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)"*, October 4, 2019

13 Children's Online Privacy Protection Act of 1998:COPPA

14 Health Insurance Portability and Accountability Act：HIPPA

15 2018 年 3 月に 8700 万人ものフェイスブックユーザーのデータをイギリスのコンサルティング会社であるケンブリッジ・アナリティカが不正に取得し、2016 年のアメリカ大統領選挙に利用したと告発された事件。

16 BUSINESS LAWYERS、「2018 年 6 月成立、米国カリフォルニア州消費者プライバシー法の概要と日本企業に求められる対応」2019 年 9 月 10 日
カリフォルニア州では住民が作成した法案が一定の署名を集め、その後実施される有権者の投票によって可決されると法律が制定される制度が存在する。なお、住民主導で可決した法案は議会による改正ができず、改正には住民投票が必要となる。

17 世帯に関する情報例としては、車載 GPS の情報や各家庭単位の電気や水道利用量データ等が考えられる。

18 State of California - Department of Justice – Office of the Attorney General の HP (Visited Dec 10, 2019)

19 The New York Times, *"Americans Will Pay a Price for State Privacy Laws"*, Oct 14th, 2019

20 図表 3 の記載の他に、BRICs のうち、ロシアでは 2015 年 9 月に改正個人データに関するロシア連邦法が、中国では 2017 年 6 月 1 日に中国サイバーセキュリティ法がそれぞれ施行済みである。

21 2017 年の改正法で 3 年ごとの見直し規定が導入された。

22 前掲注 15 の事件において、その後ケンブリッジ・アナリティカは廃業となった。