新しい個人データ保護の潮流

はじめに

EU では 2018 年 5 月に GDPR（一般データ保護規則）に施行され、欧州において個人データ保護の要請が強まりました。GDPR は、欧州にとどまらず、アジア・南米などの諸外国の個人情報保護法制に大きな影響を与えています。そして、米国カリフォルニア州では、消費者プライバシーに関して、「カリフォルニア州消費者プライバシー法」（California Consumer Privacy Act of 2018）（以下「CCPA」といいます。）が制定され、2020 年 1 月 1 日に施行されました。その後、米国では CCPA と同じような州法の制定に向けた動きが加速しています。

このように GDPR から始まった個人データ保護強化の動きは全世界に広がっており、影響を受けているのは、わが国も例外ではありません。現在、個人情報保護法の改正案が検討され、これまで手付かずだった法人等に対する高額の罰金も新たに規定される見通しです。個人データを保護し、これに違反した機関、法人に高額の制裁を科すという流れが、わが国にも広がりつつあるのです。

ここでは、新しく施行された CCPA の特徴や GDPR との違いなどを確認したうえで、わが国のデータ保護に与える影響について検討してみることにします。

CCPA とは何か

CCPA は、米カルフォルニア州の住民の個人情報を保護する法律で、カリフォルニア州の消費者にプライバシーの権利を与え、消費者の個人情報を処理する事業者に権利に対応する義務などを課す法律です。セキュリティ侵害について個人の損害賠償請求権を認め、その賠償額が法律であらかじめ規定されていることが、画期的とされています。

米国には日本やヨーロッパのような分野横断的な個人情報保護法はなく、連邦にも州にも分野別の法律しかありません。CCPA もカルフォルニア州の州法であり、米国でも、米国全体を規律する連邦法の制定には至っていません。ただ、マサチューセッツ州、ニューヨーク州、ペンシルベニア州、ロードアイランド州、テキサス州等 10 州以上で CCPA をモデルとした法案が提出されており、CCPA が制定されたことは、米国全体に影響を与えていることは確かです。

CCPA が制定されたことが米国はじめ世界に大きな影響を与えている背景としては、カルフォルニア州が世界第 5 位の経済圏であり、多くの巨大 IT 企業の拠点となっていることが挙げられます。CCPA は、世界的なスキャンダルとなったフェイスブックとケンブリッジ・アナリティカのスキャンダル[1]に不満を募らせたカルフォルニア州の住民の呼びかけに

[1] 英国の選挙コンサルティング会社であるケンブリッジ・アナリティカがフェイスブックから流出した 8700 万人分のデータを使用して、英国の EU 離脱国民投票で離脱派を支援。2016 年の米大統領選ではトランプ陣営もデータを利用した疑惑を持たれました。

より、成立するに至ったという特徴もあります。

ただ、CCPA は米国でも、法律に不備があるという指摘があり、施行されたにもかかわらず、いまだに規則の改正案が発表されるなど不安定な状態が続いています。

CCPA は、カリフォルニア州の司法長官が原告となって訴訟を提起するかたちを想定しており、これを根拠づけるカリフォルニア州司法長官の規則については 2020 年 7 月 1 日に施行される予定です。ただ、カリフォルニア州の州民によるクラスアクション（集団訴訟）がすでに提起されており、その動向に注目が集まっています。

CCPA の規制の対象

CCPA が保護する個人情報は、「消費者の個人情報」ですが、ここでいう「消費者」とはカリフォルニア州の規則（Code of Regulations）で定義された カリフォルニア州の住民である自然人を意味します。

また、CCPA が規制の対象とする「個人情報」とは、特定の消費者又は世帯を、識別し、関連し、叙述し、関連付けることができ、又は直接的に若しくは間接的に合理的にリンクさせることのできる情報を意味します。特定の消費者又は世帯を識別し、関連し、叙述し、関係付けることができ、又は直接的に若しくは間接的に合理的にリンクさせることのできるものであれば、オンライン識別子であるインターネット･プロトコル･アドレス IP アドレス、メールアドレス 、アカウント･ネーム、社会保険番号、運転免許証番号、旅券番号、その他の類似の識別子が個人情報に含まれるとされます。なお、政府や州などの公に利用できる情報や保証やリコールのための修理に必要な自動車情報・所有者情報などは CCPA が適用される「個人情報」には含まれません。わが国の個人情報保護法における「個人情報」より広い情報を含むことになります。

2020 年 2 月にパブリックコメントに付された CCPA の規則改正案では、特定の消費者や特定の世帯に関連付けられない IP アドレスは「個人情報」に該当しないと明記されています。つまり、IP アドレスやクッキー識別子などのオンライン識別子はそれ単体では CCPA の規制対象である「個人情報」には含まれないと考えられますが、「直接的に若しくは間接的に合理的にリンクさせることのできる情報」であれば、条文上「個人情報」になるのですから、IP アドレスやクッキー識別子などのオンライン識別子の多くは原則として「個人情報」として取り扱わざるを得ないでしょう。

CCPA が適用されるのは誰か

「消費者の個人情報」を処理する「事業者（Business)」に CCPA が適用されます。CCPA が対象とする事業者は以下の要件に該当する事業者です。

① 自己の株主若しくはその他の所有者の利益又は金銭的便益のために組織又は運営される事業者であること

原則として非営利団体は「事業者」としては CCPA を遵守することは求められません。

② 消費者の個人情報を収集し又は自己の代わりに個人情報を収集すること

「収集」とは、何らかの手段によって消費者に関する個人情報を購入し、貸与し、集め、取得し、又はそれにアクセスすることを意味します。「収集」には、能動的あるいは受動的に消費者から情報を受領することを含み、消費者の行動の観察（いわゆるモニタリング）を通じて情報を受領することも含まれます。

③ 単独で又は他と共同で消費者の個人情報を処理する目的と手段を決定していること

個人情報を収集する事業者が消費者の個人情報を処理する目的と手段を決定しない場合には CCPA における「事業者」には該当しません。

④ カルフォルニア州で事業を行っていること

カルフォルニア州で事業を行っているかどうかの基準は CCPA には規定されていませんが、カルフォルニア州の消費者の個人情報によって利益を得たり、利益を得る目的で事業を行っている場合も含むと考えられます。たとえば、カリフォルニア州外の事業者がカリフォルニア州の消費者の個人情報を販売しまたは開示する場合は、その事業者に CCPA が適用されると考えられます。

⑤ 年間の売上総利益が 2500 万米ドルを超え、年間 5 万件以上の消費者･世帯･デバイスの個人情報を購入し、商業目的で受け取り、販売し、共有すること

年間の売上総利益が 2500 万米ドルがカリフォルニア州内で生じたものである必要があるのかは CCPA では明らかでありませんが、カリフォルニア州内で生じた売上総利益の金額にかかわらず、この基準は全体での売上総利益が 2500 万米ドル超である場合を意味すると考えられています。

また、年間 5 万件以上の消費者・世帯・デバイスの個人情報を取り扱うことは、ウェブサイトへのアクセスなどが年間 5 万件を超える場合などに容易に想定できます。また、海外企業からカルフォルニア州の住民の個人情報を受け取る場合も含まれます。

⑥ 上記①～⑤に該当する事業者を支配し･支配され、かつ当該事業者と共通のブランドを有すること

たとえば、グループ会社に上記①～⑤の要件を充足する事業者がいる場合、日本の企業であっても日本企業に CCPA が適用される可能性があります。

日本の公的研究機関については、CCPA が適用される可能性はほぼないと考えられますが、民間企業との共同研究で、カリフォルニア州の州民の情報を取得する場合などは、CCPA の適用について考慮せざるをえないでしょう。また、公的研究機関であっても、委託先事業者に CCPA の適用がないか、注意する必要があります。

厳しい CCPA 違反の制裁

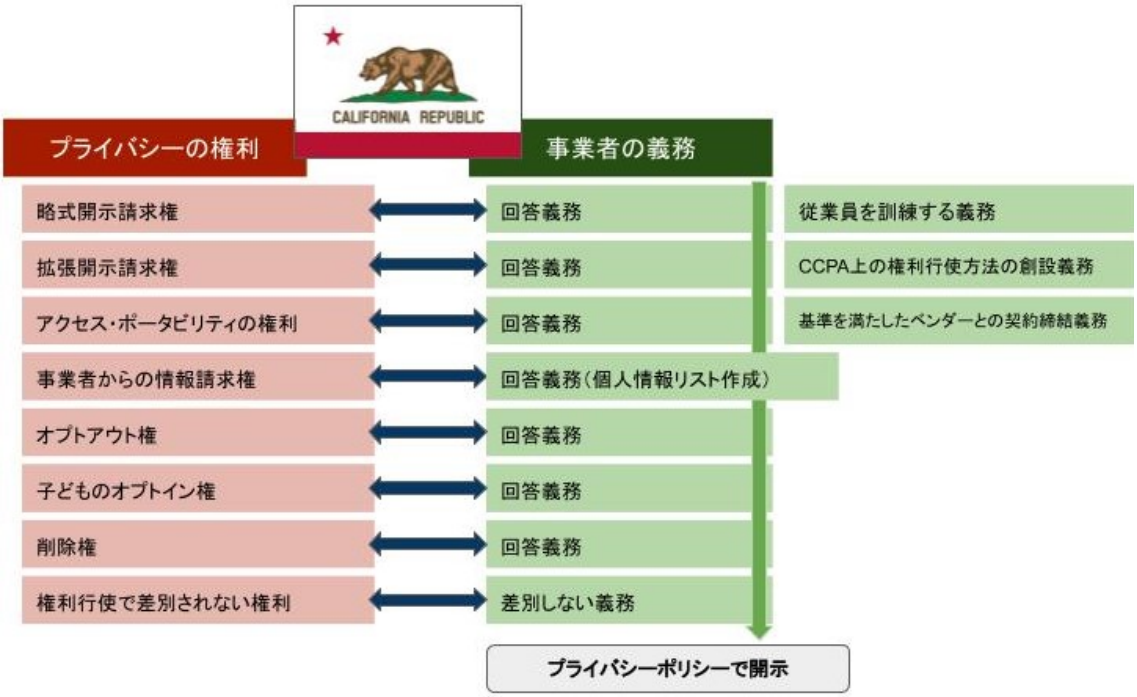
CCPA 違反については、州司法長官にが提訴することによって、事業者には、違反 1 件あたり最大 2500 米ドルの民事罰が課されます。先ほど述べたとおり、カルフォルニア州司法長官が提訴して課される民事罰については、2020 年 7 月から運用が始まる見込みです。ただ、すでにカリフォルニア州の州民によるクラスアクション（集団訴訟）がすでに提起されています。

また、CCPA によれば、セキュリティ対策を怠った結果、個人情報が不正アクセスされた場合、1 件当たり 100 米ドル以上 750 米ドルの法定損害賠償または実損のいずれか大きい額の損害賠償請求をされることになります。賠償額そのものはそれほど高額ではないと

思ったら大きな間違いです。不正アクセスにより流出する個人情報は多くの場合大量ですので、例えば不正アクセスにより 1 万件の個人情報が流出した場合、その賠償額は 100 万ドル以上 750 万ドル（日本円で約 1 億円以上 8 億円まで）となり、しかも法律によってあらかじめ賠償額が定められているので、ほぼオートマチックに高額の賠償義務を負うことになってしまいます。

CCPA の規制の中身と GDPR の規制との違い

ここでは GDPR との違いを含め、CCPA の規制の内容について簡単に見てみましょう。



CCPA の規制の概要

先ほど述べましたように、CCPA は、米カルフォルニア州の住民の個人情報を保護する法律で、カリフォルニア州の消費者にプライバシーの権利を与え、消費者の個人情報を処理する事業者に権利に対応する義務などを課す法律です。その概要は上図のとおりです。

GDPR では、データ主体の同意は個人データの取扱いの適法性根拠であり、同意の取得は大原則です。個人データを取得する場面でデータ主体の同意が原則必要になるのはもちろん、同意の取り方についても細かく規定されています。

GDPR4 条 11 項は、同意（consent）について、「自由に与えられ、特定され、説明を受けた上での、不明瞭ではない、データ主体の意思の表示を意味し、それによって、データ主体が、その陳述又は明確な積極的行為により、自身に関連する個人データの取扱いの同意を表明するもの」と定義づけています。GDPR では、こうした同意がない場合は、原則として個人データを取り扱うことはできません。

一方、CCPA ではここまで詳細に同意については規定されていません。CCPA では、消費者は、消費者の個人情報を第三者に販売する事業者に対して、その消費者の個人情報を販売しないように指示する権利を常に有するものとされ、個人情報の販売についての拒否権（オプトアウトの権利）を常に有することとされています。

事業者は、プライバシーポリシー等で、オプトアウトの手続について説明する必要があり、「Do Not Sell My Personal Information」というタイトルのウェブページを設けて、プライバシーポリシー中に、当該ページへのリンクを設定しなければなりません。オプトアウトの権利の保障は、裏を返せば、こうした事前の説明をするといったルールに従うことを条件に自由な個人情報の流通を許容するものです。これは GDPR が「オプトイン」を原則としていることとは大きく異なります。

ただ、CCPA は子どもの個人情報については同意がなければ流通を許さないという「オプトイン」の原則をとっています。すなわち、オプトアウトの権利に関する原則的ルールにかかわらず、消費者が 16 歳未満であるという認識を事業者が実際に有していた場合、その事業者は、消費者が 13 歳以上 16 歳未満の間の場合には当該消費者自身が、又は消費者が 13 歳未満の場合には当該消費者の親又は保護者が、積極的に消費者の個人情報の販売を認めていない限りは、消費者の個人情報を販売してはなりません。消費者の年齢を意図的に無視する事業者は、その消費者の年齢について認識していたとみなされます。

GDPR でも、子どもに対する直接的な「情報社会サービス（information society services）」（主にオンラインサービスのこと）で、同意を根拠に子どもの個人データを取扱う場合、その子どもが 16 歳未満であるとき（EU の各国法で年齢をさらに引き下げられる場合もあります。）は、親権者の同意または承認がある場合に限って、個人データの取扱いは適法となります。管理者は、利用可能な技術を考慮に入れたうえで、子どもの親権者が同意または承認したことを確認する「合理的な努力（reasonable efforts）」をしなければなりません。

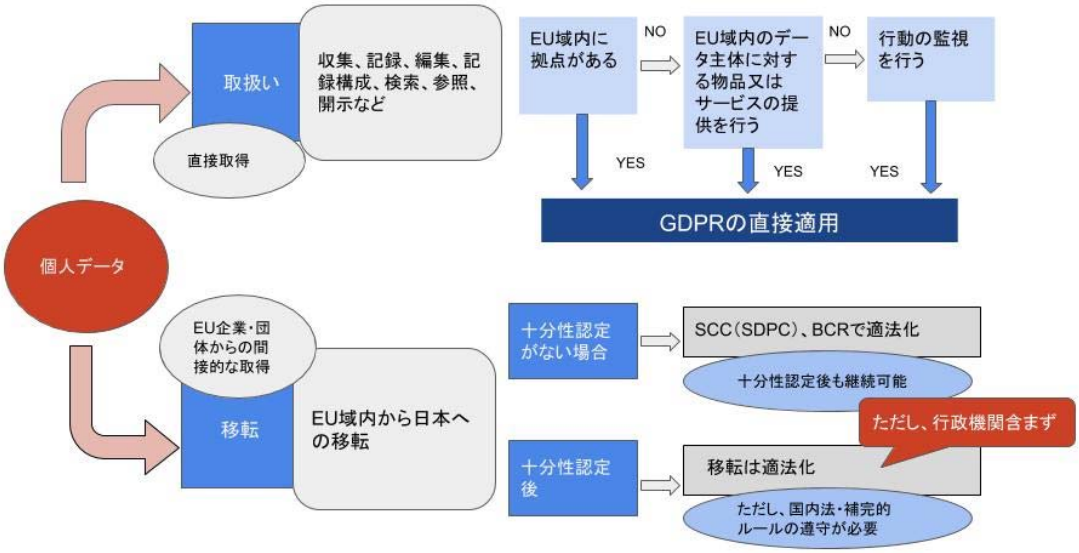
CCPA も GDPR も子どもの個人データの取扱いについては厳しく規制している点では共通しています。

また、CCPA は、GDPR と同様に消費者の「ポータビリティーの権利」を認め、事業者がこれに応じる義務を規定していますが、ポータビリティーを行うにあたって、個人データの送付先である他の主体（entity)に送信できる容易に利用可能なフォーマットとすべきことも規定しています。ポータビリティの実効性を持たせるための措置です。

GDPR が適用される主体との違い

CCPA は、先に述べたとおり、営利企業がカルフォルニア州民の個人データを収集する場合に適用されます。しかし、GDPR の適用対象は企業などの営利団体に限られません。大学や公的機関にも適用されます。

GDPR の適用については、次ページの図でまとめましたので、これを参考にしてください。



GDPR の適用関係

上図のとおり、GDPR は個人データの「取扱い」と「移転」について規制する法律です。たとえば、EU の調査機関に個人データを収集してもらい、これを日本国内に移転する場合は、当該調査機関と SCC（SDPC）という決められた契約を締結しなければなりません。また、EU の人を対象にした Web アンケートを行う場合は、それを行うのが日本の大学や公的機関であっても、その個人データの取扱いについて、GDPR が適用される場合があります。

2018 年 9 月 5 日に日本に対する十分性認定がなされ、日本の個人情報取扱事業者は「個人情報の保護に関する法律に係る EU 域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール」（補完的ルール）に従えば、GDPR の「移転」についての規制を受けないことになりました。しかし、この「補完的ルール」は、日本の個人情報保護法における個人情報取扱事業者（民間事業者）のみが対象であるため、独立行政法人等個人情報保護法が適用される独立行政法人や国立大学、個人情報保護条例が適用される地方公共団体や公立研究機関などは対象にならず、GDPR の「移転」についての規制の対象外とはならない点に注意が必要です。

GDPR 違反の制裁の実際と日本の個人情報保護法改正への影響

フランスのデータ保護当局 CNIL（情報処理と自由に関する国家委員会）は 2019 年 1 月 21 日、グーグル（Google）に対して、GDPR 違反を理由に 5000 万ユーロ（約 62 億円）の制裁金の支払いを命じました。GDPR 違反による巨額制裁金が米大手企業に課された初めてのケースです。グーグルが制裁金が課された理由は、主に情報提供の仕方と同意の取得方法についてです。

第一に、グーグルはデータ主体への情報提供が十分でなく透明性が認められないと判断

されました。グーグルは個人データを取得する場合には利用目的や法的根拠などの情報をデータ主体（本人）に説明する必要がりますが、提供されるべき情報も 5〜6 回のステップを踏む必要があり、データ主体への情報提供が適切になされていないと認定されました。

第二に、ターゲティング広告で個人データを取得する際に、デフォルトで同意することになっており、個人データの取扱いがデータ主体の明確な同意に基づいていないと判断されました。GDPR では、同意は個人データの利用目的ごとに個別的に取得する必要がありますが、グーグルは包括的に取得していたため、個人データの取扱いがデータ主体の明確な同意に基づいていない、と判断されたのです。

CNIL によれば、2017 年のグーグルの全世界総売り上げ約 960 億ユーロ（約 12 兆円）の「4 パーセント以下」を基礎に、他の事情を考慮して 5000 万ユーロの制裁金が算定されたとのことです。

このように GDPR を根拠に制裁金が課されるケースが相次いでおり、EU では GDPR 遵守が徹底されつつあるといえるでしょう。CCPA についても、2020 年 7 月以降、企業に莫大な民事罰が課される可能性があります。

ひるがえって日本の場合はどうでしょうか。個人情報保護法の 2015 年改正で、刑事罰が導入され、個人情報データベース等が強く保護されることになりました。その結果、個人情報データベース等を盗用したり、利益を図るために第三者提供した場合には 1 年以下の懲役、または 50 万円以下の罰金が科されることになりました。これに加えて、個人情報データベースの盗用などの行為が事業者の「業務に関して」行われたといった限定的な場合に、事業者にも罰金刑が併科されることとなりました。以前よりも個人情報の保護が図られたとはいえ、罰金刑が事業者に課されるケースは極めて限られているため、GDPR の制裁金などと比較してもペナルティとしては機能していないとの議論が従前からありました。個人情報保護委員会が漏えい等報告を受けた事案や報告徴収・立入検査を行った事案の数は増加傾向にあり、リクナビ問題で 2019 年 8 月に初めての勧告を行ったものの、なんらのペナルティも課されなかった事情から、個人の権利利益の保護のためのペナルティの強化は強く求められているところです。

個人情報保護委員会が 2019 年 12 月 13 日に発表した「個人情報保護法 いわゆる 3 年ごと見直し 制度改正大綱」（「改正大綱」）では、刑事罰について、法人処罰規定に係る重科の導入を含めて見直しを行うほか、課徴金制度を導入することも検討することとされています。一部報道では、法人への罰金を 1 億円に引き上げる規定を盛り込んだ改正案が 2020 年 3 月に国会に提出される見通しで、日本でも、遅ればせながら事業者に対して大きなペナルティを課す動きが出てきました。ただし、個人の権利利益の保護のために実効的なものになるかどうか、注視する必要があります。また、個人情報保護法が適用されない、研究機関や国公立大学については、今後どのような法改正がなされるのかも併せて注視しなくてはなりません。