2019.11.01

情報セキュリティニュース ＜2019 No.2＞

米国におけるプライバシー法制と CCPA について

【要旨】
■米国カリフォルニア州で、消費者プライバシー法（The California Consumer Privacy Act of 2018（以下 CCPA））が 2020 年 1 月から施行される。
■CCPA は、カリフォルニア州の住民の個人情報を保有する企業に対し、消費者からの情報の開示や削除、売却停止の請求に応じる義務を規定しており、日本国内に拠点を置く企業であっても現地法人が一定の要件に該当する場合は、適用対象となり得る。
■CCPA の要求事項は日本の個人情報保護法や EU 一般データ保護規則（GDPR）にはないものも多く、企業は各条文の内容の理解にとどまらず自社の置かれている状況を適切に把握した上で実務対応計画を進めていくことが望ましい。
■本レポートでは、米国におけるプライバシー法制と CCPA の概要を解説する。

１．米国におけるプライバシー保護法制の現状

米国のプライバシー保護法制は、公的部門に関してはPrivacy Act of 1974が制定されているが、民間部門に関しては、機密性の高い情報を扱う分野（金融、通信、医療など）[1]を除き、包括的な連邦法は存在しない。

米国において個人情報を取り扱う企業は、プライバシーポリシーなどを通じて自らが個人情報をどのように取り扱うのかを公表するが、このプライバシーポリシーの内容は、基本的には各企業が自由に定めても構わない。すなわち、自主規制のもと個人情報を取り扱っている。

その上で企業が自ら公表しているプライバシーポリシーの内容に反する個人情報の取扱いをすると、連邦取引委員会（FTC）法5条にいう、個人情報に関する「不公正・欺瞞的行為または慣行」に該当し、課徴金などの制裁を受ける。

また、州法レベルでもプライバシー保護に関する様々な包括的でない個別法が存在しているが、その内容は統一されていない。

なお、この度、包括的な州レベルのプライバシー法となるCCPAを制定・施行するカリフォルニア州においても、現状は以下のプライバシー保護に関する複数の個別法が存在する。

・セキュリティ侵害通知法
・シャイン・ザ・ライト法[2]
・追跡防止法（Do Not Track法）
・消しゴム法（いわゆる「忘れられる権利」）　　など

２．CCPAの適用範囲

CCPAは、カリフォルニア州の住民のデータを保有する企業が、消費者からのデータの開示や削除、売却停止の請求に応じる義務を規定しており、2018年6月に成立し、2020年1月に施行が予定されている。以下にその適用範囲を示す。

---

[1]機密性の高い情報を扱う分野における連邦法
金融機関：グラム・リーチ・ブライリー法（GBLA）、通信分野：通信法、電子通信プライバシー法、迷惑メール防止法など、医療分野：医療保険の相互運用性および責任に関する法律（HIPPA）など

[2]シャイン・ザ・ライト法
ダイレクトマーケティングを目的として第三者と共有する個人情報の内容を請求する権利をカリフォルニア州の居住者に付与する法律。

（１）保護対象となる「個人情報」の適用範囲

CCPAでいう個人情報とは、「特定の消費者または世帯を、識別し、関連し、叙述し、関連付けることができ、また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」と広く定義している。「消費者」とは、2017年9月1日時点におけるカリフォルニア州の規則（Code of Regulations）第18巻の第17014条において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する。

日本の個人情報保護法では、「特定の個人を識別できるもの」を個人情報と定義しているが、CCPAでは「消費者（本人）」のみならず「世帯」も対象となること、および、「識別」のみならず「関連」、「叙述（説明）」、「関連付ける」情報も含まれる点に留意が必要である。

CCPA 1798.140条(o)に、具体的に例示されている個人情報を以下に示されており、極めて広範囲である。一方で、従業員情報や企業間取引で得た消費者情報の一部は除外されている。

（A）実名、別名、郵便住所、一意個人識別子、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、e 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、はその他の類似の識別子
（B）カリフォルニア州民法1798.80条の細区分 (e) に記載されている個人情報のカテゴリ（氏名、署名、社会保障番号、身体的特徴または説明、住所、電話番号、パスポート番号、運転免許証または州の身分証明書番号、保険証書番号、教育、雇用、雇用歴、銀行口座番号、クレジットカード番号、デビットカード番号、またはその他の金融情報、医療情報、健康保険情報）
（C）カリフォルニア州法または連邦法のもとでの保護された分類の特性
（D）個人の財産の記録、購入、取得または検討した製品またはサービスの記録、または、その他の購入または消費の履歴または傾向についての記録を含む商業的情報
（E）バイオメトリック情報
（F）インターネットまたはその他の電子的なネットワーク活動の情報
※閲覧履歴、検索履歴、及び、インターネット･ウェブサイト、アプリケーションまたは広告との消費者のやりとりの情報を含むが、これに限られない
（G）地理位置データ
（H）音声、電子、視覚、温度、嗅覚、または類似の情報
（I）職業または雇用に関する情報
（J）家族教育権とプライバシー法(20 U.S.C. section 1232g, 34 C.F.R. Part 99)に定める公に利用可能な個人識別情報でないと定義される教育上の情報
（K）消費者についての選好、性格、心理的傾向、性質、行動、態度、インテリジェンス、能力及び素質を反映する消費者のプロファイルを作成するために本項で識別された情報から引き出された、推定

（２）「事業者」の適用範囲

CCPAでは、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ている以下のいずれか1つの要件に該当する営利目的の法人がCCPAの対象となる「事業者」と定義している。

・ 年間の売上高が2,500万ドルを超える
・ 年間で50,000件以上の消費者、世帯またはデバイスの個人情報を購入し、事業者の商業目的で受け取り、販売し、または商業目的で共有する
・ 消費者の個人情報の販売から年間収入の50%以上を得ている

上記要件に該当する事業者を「支配する」または「支配される」事業者もCCPAの対象となる。例えば、議決権のある株式の50%超を保有することや、役員の過半数を選任若しくは役員と類似した職務を果たす個人の選任を何らかの方法でコントロールすることができ、かつ、共通の名称、サービス･マークまたは商標を使用する場合がこれに該当する。

すなわち、日本国内に拠点を置く企業であっても、支配される企業（親会社）または支配下にある企業（子会社）が上記要件に該当すればCCPAを遵守する必要がある。

３．CCPAにおいて企業が求められる義務

CCPAにおいて企業が求められる主な義務を以下に示す。

（１）プライバシー情報収集に関する通知

消費者の個人情報を収集する事業者は、収集時点またはその前に、収集される個人情報のカテゴリ、および当該カテゴリの個人情報を利用する目的を消費者に通知しなければならない。
また、事業者は、本条に基づく通知の消費者への提供なしに、消費者に関する新たな個人情報のカテゴリを収集せず、または収集した個人情報を新たな目的のために使用してはならない。
これは日本の個人情報保護法が定める「利用目的の通知」などと類似した規定といえる。

（２）消費者からの情報開示請求への対応

消費者は、事業者に対して以下の情報を開示するように要求することができ、事業者はこれを開示しなければならない。

- その消費者について事業者が収集した個人情報のカテゴリ
- 個人情報が収集された情報源のカテゴリ
- 個人情報を収集しまたは販売する事業目的または商業目的
- 事業者が個人情報を共有する第三者のカテゴリ
- その消費者について事業者が収集した個人情報の特定の部分
- 自身の個人情報の販売・提供の内容（誰に・どんな情報を提供したか）

また、事業者は、消費者から各種開示請求ができる手段について、2つ以上の手段を利用できるようにし、その手段には少なくともフリーダイヤル番号を、また事業者がインターネット･ウェブサイトを有している場合にはウェブサイト･アドレスを含まなければならない。
消費者から受けた情報開示請求に対して、事業者は原則として45日以内に無償で開示しなければならない。
日本の個人情報保護法においても「保有個人データに関する事項の公表等」「開示」にて規定されているが、自身の個人情報の販売・提供の内容（誰に・どんな情報を提供したか）までは現行法では規定されていない。「いわゆる3年ごと見直しに係る検討[3]」を踏まえた2020年に予定されている改正内容を注視いただきたい。

（３）第三者提供の制限（オプトアウト）

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（オプトアウト）を常に有する。
また、消費者が16歳未満の場合は、以下のものが積極的に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らない（オプトイン）。

- 消費者が13歳から16歳までの間の場合：消費者本人
- 消費者が13歳未満の場合：消費者の親または保護者

消費者の個人情報を第三者に販売する事業者は、その情報が販売される可能性があること、および消費者がその個人情報の販売について「オプトアウトの権利」を有することについて消費者に通知する必要があり、消費者が個人情報の販売をオプトアウトできるように、事業者はインターネットのウェブページにおいて、「私の個人情報を販売しない（Do Not Sell My Personal

[3]「いわゆる３年ごと見直しに係る検討」
現行の個人情報保護法より、情報通信技術の進展が著しいこと等から、３年ごとの見直し規定が設けられている。

Information）」と題したインターネット･ホームページへの明示的なリンク（いわゆる「オプトアウトボタン」）を提供しなければならない。
また、消費者から受けたオプトアウト請求に対して、事業者は原則として45日以内に当該消費者の個人情報の第三者提供を停止しなければならない。
日本の個人情報保護法では、個人情報を第三者に提供する場合、原則本人の同意が必要だが、CCPAにおいては原則自由であり、消費者がオプトアウト権を行使したら提供を止めればよい点に留意いただきたい。
なお、日本においてオプトアウトによる個人情報の第三者提供を行う際は、個人情報保護委員会への届出が必要である。

（４）削除権
消費者は、事業者が消費者から収集した個人情報を削除するように求める権利を有し、事業者は、消費者に個人情報の削除を要求できる権利があることを開示しなければならない（例外となるケースもあり）。
また、消費者から受けた削除請求に対して、事業者は原則として45日以内に当該消費者の個人情報の削除をしなければならない。
なお、削除権は2018年5月に施行したGDPRにおいても、一定の条件の下で「忘れられる権利」として保障されている。
現在の日本の個人情報保護法では、保有個人データの内容が事実でないときに訂正、追加または削除を請求したり、事業者が法令に違反して取得した保有個人データのみ利用停止等を請求することができるが、「いわゆる3年ごと見直しに係る検討 」ではこの利用停止権について検討が行われている。2020年に予定されている改正内容を注視いただきたい。

（５）消費者の権利行使に関する差別的取扱の禁止
事業者は、消費者がオプトアウト等の権利を行使したことにより、消費者を差別してはならない。CCPAでは、以下の行為を禁止事項として例示するが、これに限られない。

（A）消費者に対する商品・サービスの提供の拒否
（B）ディスカウント若しくはその他の特典の使用、またはペナルティを課すことを含め、商品・サービスに異なった価格・料金を請求すること
（C）その消費者に対して異なったレベル・品質の商品・サービスを提供すること
（D）異なる価格・料金・レベル品質の商品・サービスを消費者が受領することを示唆すること

（６）プライバシーポリシーの更新
事業者は、オンライン上のプライバシーポリシーに以下事項を記載しなければならない。また、少なくとも12か月に1回その情報をアップデートしなければならない。

- 消費者の情報開示請求権
- 消費者の権利行使に関する差別的取扱の禁止
- 消費者から各種開示請求ができる手段
- 過去12か月に事業者が収集した消費者の個人情報のカテゴリー･リスト
- 個人情報が収集された情報源のカテゴリー・リスト
- 個人情報を収集しまたは販売する事業目的または商業目的
- 事業者が個人情報を共有する第三者のカテゴリ
- 過去12か月間に販売された消費者の個人情報のカテゴリー･リスト
- 過去12か月間に事業目的のために開示された消費者に関する個人情報のカテゴリー･リスト

４．違反時の州司法による制裁と消費者からの損害賠償請求
CCPAの規定に違反した事業者は、州司法長官から30日以内に違反を是正するよう通知を受ける可能性があり、この通知後も違反が是正できない場合、以下のの罰金（民事罰）を科せられる可能

性がある。

・違反1件につき最大2,500ドル
・故意だと認定される場合には最大7,500ドル

また、事業者がCCPAで求められる個人情報を保護するためのセキュリティ手続きやプラクティスの実施・維持義務に違反した結果、暗号化されていないまたは生データのままの個人情報が、無制限アクセス、流出、窃取または消費者の意図しない開示にあった場合、消費者は、以下に従って民事訴訟を提起することができる。

・違反1件について消費者一人当たりで100 ドル以上750 ドル以下または実損害のいずれか大きい額の回収
・差止命令による救済または宣言的救済
・裁判所が適切とみなすその他の救済

５．プライバシー法制への対応のポイント

CCPA の要求事項は、開示する情報の範囲やオプトアウトの手段、差別的取扱の禁止、プライバシーポリシーの更新など、日本の個人情報保護法や GDPR にはないものが多く存在する。

【表 1】日米欧におけるプライバシー法制の概要比較

	米国カリフォルニア州	EU	日本
法律	CCPA	GDPR	個人情報保護法
施行時期	2020 年 1 月	2018 年 5 月 25 日	2005 年 4 月 1 日施行 2017 年 5 月 30 日改正
個人情報の定義	特定の消費者または世帯を、識別し、関連し、叙述し、関連付けることができ、また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	個人データを、直接的または間接的に識別あるいは識別可能な EU 内に所在する自然人に関する情報	生存する個人に関する情報であって、特定の個人を識別することができるもの（他の情報と容易に照合でき、それにより特定の個人を識別することができるもの含む）または個人識別符号が含まれるもの
個人情報の定義の特徴	携帯電話番号、端末 ID、クレジットカード番号、メールアドレス、会員 ID、IP アドレス、クッキーID、位置情報も対象。 「世帯」も対象。 「識別」のみならず「関連」、「叙述（説明）」、「関連付ける」情報も対象。	携帯電話番号、端末 ID、クレジットカード番号、メールアドレス、会員 ID、IP アドレス、クッキーID、位置情報も対象。	携帯電話番号、端末 ID、クレジットカード番号、会員 ID、IP アドレス、クッキーID、位置情報などは単体では対象外。 ※ただし、複数情報を組み合わせて特定の個人を識別し得る場合は、これらも個人情報に含まれる。
本人（データ主体）の権利	・開示請求 ・第三者提供の停止請求 ※オプトアウトがベース ・削除権	・同意撤回の権利 ・異議申立ての権利 ・通知を受ける権利 ・データの訂正・消去を求める権利 など	・開示請求 ・第三者提供の停止請求 ・データの内容が事実でないときのみ訂正、追加または削除の請求 ・事業者が法令違反して収集した場合のみ利用停止請求

同意の取得	明文化されていないが、個人情報の収集にあたり利用目的を通知することが義務付け	厳格に規定	目的外利用、要配慮個人情報の取得時、第三者提供時に同意を規定
データ漏えい時の監督機関への通知	別の法律において被害者への通知を義務付け 500 を超える漏えいの場合、電子的手段で司法長官へ通知 ※具体的な期限の規定はなし	データ漏洩発覚から 72 時間以内の監督機関への通知義務	個人情報保護委員会等に速やかに報告するように努める義務
違反時の制裁	州司法長官から：故意だと認定される場合には最大 7,500 ドル	最大で 2,000 万ユーロ、または、事業者の場合には前会計年度の全世界年間売上高の 4%のいずれか高い金額	個人情報保護委員会の命令に違反した場合や報告徴収・立入検査に協力しなかった場合等に、罰則を規定。 個人情報データベース等不正提供罪に該当する行為については1年以下の懲役あるいは50万円以下の罰金。

CCPA に対応するには、社内のどこに・どのような情報が存在するのか把握するデータ・マッピングは当然のこと、保有する個人情報の名寄せ・紐づけ（※世帯も対象となるため）と、消費者からの開示・オプトアウト・削除請求に対し 45 日以内に対応できるシステム等の構築、プライバシーポリシーのアップデートのため保有する個人情報のメンテナンスは必須となる。

企業は各条文の内容の理解にとどまらず、自社の置かれている状況を適切に把握した上で実務対応計画を進めていくことが望ましい。

ＭＳ＆ＡＤインターリスク総研㈱　リスクマネジメント第四部
マネージャー・上席コンサルタント　　岡田　智之