カリフォルニア州消費者プライバシー法(CCPA)
実務ハンドブック

2019 年 12 月

日本貿易振興機構（ジェトロ）
サンフランシスコ事務所
イノベーション・知的財産部　スタートアップ支援課

内容

第0　エグゼキュティブサマリー

サマリー	関連頁
1. CCPAとは、消費者（カリフォルニア州の住民）に8つのプライバシーの権利を与え、当該「消費者」の「個人情報」を処理する「事業者」(Business: CCPA第1798.140条第(c)項）に8つの義務を負わせる法律である。CCPAは2020年1月1日から適用が開始される。	3頁 6頁
2. CCPAの執行としては、①カリフォルニア州司法長官による提訴による民事罰（事業者の義務に違反した場合、1件あたり最大2,500米ドル（故意の場合7,500米ドル）の民事制裁金が科され得る。)、②消費者による提訴（個人情報の性質に照らして合理的なセキュリティの手続と慣行を実装する義務を怠った結果により、個人情報が不正アクセス等された場合には、消費者によって1件（1名、1事故毎に算定）あたり、100米ドル以上750米ドル以下の法定損害賠償又は実損のいずれか大きい額の賠償請求が行われ得る。）がある。特に、カリフォルニアの消費者による民事訴訟は、日本企業の米国子会社や米国支店に対してのみならず、日本本社等の日本企業グループの米国外拠点を名宛人として提起されることも予想される。当該民事訴訟が提起された場合には、企業・組織として応訴するための膨大な訴訟費用がかかることが考えられ、これに加えて、そのような訴訟が提起されること自体による企業・組織のレピュテーションの棄損も懸念される。	8-9頁
3. 米国内に拠点を持ち消費者（カリフォルニア州の住民）の個人情報を処理している日本企業本社は「事業者」に該当する場合が多く、日本国内の日本企業本社自体がCCPAのコンプライアンス対応を執らなければならない場合が多いと考えられる。そして、この日本企業の米国子会社は共通のブランドを使用する等の関係に立つ場合には日本企業本社に「支配」されているため、自社の売上高が約2500万米ドルを超えるか否かに関わらず「事業者」に該当し、CCPAのコンプライアンス対応を執らなければならない場合が多いと考えられる。	13, 14, 17-18頁
4. (1) CCPAはCCPAの適用対象として4つのカテゴリーを想定している。 ①　「事業者」(Business: CCPA第1798.140条第(c)項) ②　「サービス提供者」(Service Provider: CCPA第1798.140条第(v)項) ③　「第三者」(Third Party: CCPA第1798.140条第(w)項)) ④　「CCPA第1798.140条第(w)項(2)に規定される者」(いわゆる「責任引受者」(liability-shifted person))	10頁
(2) 非営利団体であっても「第三者」に該当し、CCPAの適用があることが考えられる。CCPA上、消費者が第1798.120条による明示的な通知を受け、かつオプトアウトの権利を行使する機会を与えられた場合を除き、第三者は、事業者から販売された消費者の個人情報を販売してはならない（第1798.115条第(d)項）とされていることから、「第三者」としては販売禁止の条項に違反しないことを確保することが必要となる。	19-20頁
5. (1) 人事関連の個人情報の時限的な部分的適用除外（第1798.145条第(h)項）については、その範囲や期間が限定的であり、人事関連の消費者の個人情報の処理を行う事業者はCCPAへのコンプライアンス対応を執る必要がある。	24-26頁
(2) B to Bの文脈での企業等の役職員等の個人情報の処理に関する時限的な部分的適用除外（第1798.145条第(n)項）については、その範囲や期間が限定的であり、B to Bの文脈での企業等の役職員等である消費者の個人情報の処理を行う事業者はCCPAへのコンプライアンス対応を執る必要がある。	26-27頁

6. (1) CCPA 上の事業者の義務を纏めると以下の通りである。 ① 消費者への通知義務（CCPA 規則案第 2 節） ② 消費者要求への対応のビジネスプラクティスに関する義務（CCPA 規則案第 3 節） ③ 研修義務（CCPA 規則案第 999.317 条） ④ 記録管理義務（CCPA 規則案第 999.317 条） ⑤ 要求の検証義務（CCPA 規則案第 4 節） ⑥ 未成年者に関する特則の義務（CCPA 規則案第 5 節） ⑦ 差別の禁止（CCPA 規則案第 6 節） ⑧ 個人情報の性質に照らして合理的なセキュリティの手続と慣行を実装する義務（CCPA 第 1798.150 条）	33 頁
(2) 上記の事業者の義務については、CCPA 規則案が詳細にその内容を定めている。CCPA 規則案について特に注意が必要なのは、カリフォルニア州の司法長官が第 999.300 条第(b)項において「本規則に違反した場合は CCPA 違反に該当し、当該法に規定する是正措置の対象となる。」と定め、CCPA 規則案への違反が CCPA の違反であるとみなす立場を明らかにしていることである。CCPA 規則案には、CCPA の遵守に必要な社内のシステム・態勢整備の要件が細かく規定されている。本規則違反が CCPA 違反とみなされてしまうため、本規則案を注意深くチェックしながら準備を進める必要がある。	33 頁
(3) 特に、上記①の消費者への通知義務との関係では、事業者が、オンライン・プライバシーポリシーを有している場合にはそのオンライン・プライバシーポリシー、消費者プライバシー権についてのカリフォルニア固有の記述においてプライバシーポリシーを持たない場合にはその事業者のインターネット・ウェブサイトにおいて、一定の情報を開示し、少なくとも 12 ヶ月に 1 回その情報をアップデートしなければならないという継続的な開示義務があることが重要である。すなわち、2020 年 1 月 1 日以降、CCPA に対応したプライバシーポリシーを自社・自組織のウェブサイトに掲げていないことは、インターネット上の検索エンジンを使って誰でも容易にチェックすることができるため、CCPA に違反した状態にあることが明るみにでるきっかけとなることが懸念される。したがって、外部から見えやすい部分に関連する CCPA 対応は優先的に進めることが望ましいと考えられる。	33 頁
7.(1) CCPA 上は、CCPA の適用対象となる者として 4 つのカテゴリー（①事業者、②サービス提供者、③第三者、④責任引受者）が定められている。一つの法的主体が個人情報の処理業務毎に異なるカテゴリーに該当する場合もあるため、自社・自組織がこれら 4 つのカテゴリーのどれか一つにのみ該当することを前提として検討しないように注意すべきである。	66 頁
(2) 各カテゴリーに該当し CCPA の適用対象となりそうなことが判明した場合に、日本企業の日本本社及び米国子会社において連携した上で、CCPA へのコンプライアンス対応を行う場合、それぞれのカテゴリー毎に、CCPA 対応のプロジェクトを行うことが考えられる。	66-68 頁

第1　はじめに－世界の個人情報保護法/個人データ保護法違反のリスクとCCPA

1. 序文

本ハンドブックは、2018年6月に成立したカリフォルニア州消費者プライバシー法（California Consumer Privacy Act。以下「CCPA」という。）に対して、日本企業・組織が、適時適切にコンプライアンス対応を推進することを支援するために準備されたものである。

本ハンドブックは、独立行政法人日本貿易振興機構・サンフランシスコ事務所が杉本・川島法律事務所事務所代表でニューヨークオフィス・ブリュッセルオフィスのパートナーである杉本武重弁護士（日本、ニューヨーク州、ブリュッセル（B-List））に委託して執筆され[1]、その著作権は全て独立行政法人日本貿易振興機構に帰属する。

CCPAは、米国国内においては企業・組織のシステムの改修や社内態勢整備との関係で、企業・組織に非常に大きなインパクトを及ぼす法律であるとして、非常に重要視され、米国企業においても、急ピッチでコンプライアンス対応が進められてきた。CCPAは、日本にとって外交的にも経済的にも最も重要な国であると位置づけられることの多い米国の全土に影響を及ぼす強力なプライバシー保護法である。今後、日本企業・組織が、米国国内においてビジネスを行っていくうえで、CCPAの適用を受けるか否かに関わらず、企業・組織に期待される説明責任の一環として、自社・自組織として、CCPAの適用を受けるか否か、受けるとしてどのようにCCPAを遵守しているか、受けないとしてなぜCCPAの適用を受けないと判断をしたかについて、説明できる必要がある。より具体的には、明確に事前に文書化しておいた内容に基づいて、カリフォルニア州司法長官及びカリフォルニア州の消費者はもちろんのこと、CCPA遵守について監視の目を光らせる市民団体・人権保護団体に対して、十分な説明を適時に行えるように備えることが、州司法長官による執行や消費者による民事訴訟及び貴社・貴組織の対応が社会問題化されることによる炎上のリスクを未然に防ぐうえで必要である。

2. 世界の個人情報保護法/個人データ保護法違反のリスクとCCPA・米国連邦プライバシー法案との関係

欧米ではデータ保護法（Data Protection Law）は人権保護法として位置付けられてきた。そして、2018年5月のEUの一般データ保護規則（General Data Protection Regulation: GDPR）の適用開始を契機として、データ保護に関する個人の権利意識の向上とともに、EUを中心とするデータ保護監督当局（Data Protection Supervisory Authority）によるデータ保護法違反の摘発と制裁は世界的に強化の流れを辿っている。データ保護法違反には、大きく分けて、少なくとも二つのリスクがあるといえよう。

(1) リスク1：高額な制裁金を受けるリスク

a. データ保護違反に対する高額な制裁金を課す立法の広がり

国・地域	立法・施行状況	説明
欧州	GDPRが2018年5月より適用開始	高額な制裁金とルールの厳格化により世界のデータ保護法の流れをリード

[1] 杉本武重弁護士は、本ハンドブックの中で特に難解と思われる論点については、IAPP（The International Association of Privacy Professionals:国際プライバシー専門家協会）のChife Knowledge Officer（最高知識責任者）・Vice President（ヴァイス・プレジデント）、日本DPO協会の上級特別顧問、兼Tene & Associates代表取締役であるオマール・テネ（Omer Tene）氏と討議する機会を得た。また、杉本弁護士は、合理的なセキュリティ手続の項目については株式会社インターネットイニシアティブのビジネスリスクコンサルティング本部本部長小川晋平氏、同本部シニアコンサルタント堀江浩司弁護士作成の資料からヒントを得、またQ&Aの項目の一部には執筆にあたって森・濱田松本法律事務所東京オフィスの田中浩之弁護士、嶋村直登弁護士から助力を得たが、両項目ともに杉本弁護士が独自の視点・見解で整理し自ら執筆を行った。上記プライバシー専門家による本ハンドブックへの協力に関わらず、杉本弁護士が本ハンドブックの執筆責任を負っている。

米国	カリフォルニア州消費者プライバシー法（CCPA）が 2020 年 1 月より適法開始予定	米国連邦プライバシー法案についても審議されており、立法化される可能性。Facebook 事件における制裁金額を見ても厳格化の方向
中国	サイバーセキュリティ法が 2017 年 6 月より適用開始	異なる枠組みではあるものの GDPR との類似点多数
ブラジル	新しいデータ保護法が 2018 年 8 月成立、2020 年 2 月適用開始予定	GDPR 類似のルールを導入
タイ	新しいデータ保護法が 2019 年 5 月成立、2020 年 5 月適用開始予定	GDPR 類似のルールを導入。刑事罰も導入。
インド	新しいデータ保護法案の提出・審議中	GDPR 類似のルールを導入

b. 欧米における近時の執行事例では、数百億円から数千億円の制裁金決定が出されている。

(a) Facebook に対する制裁金決定（米国）

項目	内容
決定日	2019 年 7 月 25 日
制裁金の金額	50 億ドル（約 5400 億円）
事案の概要	▪ 本件は 2018 年 3 月に発覚した Facebook 社からの不正な個人情報流用に関する事案。 ▪ Facebook 社からユーザー（最大 8700 万人）の個人情報について学術目的で利用するために提供を受けた英国ケンブリッジ大学の研究者が、選挙コンサルティング会社であるケンブリッジ・アナリティカ社に不正に売却し、当該個人情報が 2016 年の米国大統領選挙において特定の候補者に有利になるように利用されたとされる。
説明	▪ 本件の決議においては、米国連邦取引委員会（Federal Trade Commission: FTC）の委員のうち共和党 3 名が賛成し、民主党 2 名が反対した。争点の 1 つは、Facebook 社の CEO であるマーク・ザッカーバーグ氏をはじめとする経営陣の個人責任が問われるべきかという点であったが、結果的には否定された。 ▪ FTC は、本件における Facebook 社の行動が FTC との 2012 年同意文書（Consent decree）に反するものであったか否かを中心に調査を行った。

米国 FTC 委員ロヒット・チョプラ（Rohit Chopra）氏は Facebook の CEO や他の役員の個人責任を追及すべきと主張した[2]。チョプラ委員によれば、同委員は FTC における米国連邦プライバシー法案及び潜在的な論点である米国連邦プライバシー法による州法への先占（pre-emption）の議論の責任者である。

[2] チョプラ委員の 2019 年 7 月 24 日付ツイッターの投稿
https://twitter.com/choprafc/status/1154010757031518209
1. It doesn't fix the incentives causing these repeat privacy abuses. It doesn't stop $FB from engaging in surveillance or integrating platforms. There are no restrictions on data harvesting tactics -- just paperwork. $FB gets to sign off on what's acceptable.
2. Mark Zuckerberg, Sheryl Sandberg, and other executives get blanket immunity for their role in the violations. This is wrong and sets a terrible precedent. The law doesn't give them a special exemption.
3. The settlement fine print gives Facebook broad immunity for "known" and "unknown" violations. What's covered by these immunity deals? Facebook knows, but the public is kept in the dark.
4. Breaking the law shouldn't be profitable. $5 billion is a lot, but Facebook can pay out of its profits. The 2012 FTC action against Google included a fine more than 5x the company's unjust gains. Can we say the same here?
Cambridge Analytica's tactics of profiling and targeting users were a small-scale reflection of Facebook's own practices. Notably, the FTC is holding individuals from Cambridge Analytica accountable for misconduct. Not so for Facebook.

(b) British Airways に対する制裁金決定（英国）

項目	内容
決定案発表日	2019 年 7 月 8 日
制裁金の金額	1 億 8339 万ポンド（約 250 億円）
事案の概要	▪ 2018 年 9 月に ICO に通知されたサイバー事故に関する案件 ▪ BA 社のウェブサイトへのアクセス記録が不正サイトに転用されたことにより、2018 年 6 月から約 50 万人の顧客データが侵害された事案 ▪ ICO は British Airways（BA 社）による GDPR 違反について 1 億 8339 万ポンド（約 250 億円）の制裁金を課する意向を発表
説明	▪ ICO の調査の結果、BA 社による脆弱なセキュリティ対策によって、氏名、住所、ログイン、カード支払、旅程予約の詳細を含む様々な情報が侵害されたことが判明した。 ▪ BA 社は事件が明らかになって以降、ICO の調査に協力し、セキュリティ設定を改善した。BA は、調査結果及び制裁内容について、今後 ICO に対して意見を述べる機会を有する。 ▪ ICO は、最終決定を下す前に、BA 社による意見及びその他の関係監督当局による見解を慎重に検討する予定。

(2)リスク 2：事業価値を毀損するリスク

企業・組織におけるデータ保護に関するレピュテーションの毀損が事業価値の毀損に直結する。消費者が違反行為を行う企業・組織に自己の個人データを利用させることを拒絶する結果、当該企業・組織にとって利用可能な個人データの質・量が低下する。利用可能な個人データの質・量が限定されることで、企業・組織の競争力が損なわれる。事業パートナーは、データ保護法を遵守しない企業・組織とのデータビジネスの連携はリスクであると評価する恐れがある。そうなると、データビジネスにおける事業パートナーとの協業に支障を来すこととなる。

(3)CCPA と連邦プライバシー法案との関係

CCPA 制定以来、マサチューセッツ州、ニューヨーク州等の 10 州以上で CCPA をモデルとする法案が各州議会に提出されている。また、包括的な連邦プライバシー法制定の機運は高まっており、2019 年 11 月下旬には、民主党の上院議員により消費者オンラインプライバシー権利法（the Consumer Online Privacy Rights Act: COPRA)が発案され、また共和党の上院議員により消費者データプライバシー法（the United States Consumer Data Privacy Act: CDPA）の「スタッフ・ディスカッション・ドラフト」が公表されており、引き続き連邦議会で検討が重ねられる状況にある。さらに、2019 年 12 月中旬には、米国下院エネルギーおよび商業対策委員会において超党派の連邦プライバシー法案のファーストドラフト、すなわち、共和党と民主党の議員が共同作業によって作成した法案のドラフト、が公表された。これは、連邦議会において、包括的な連邦プライバシー法案の採択に向けて着実な歩が進められていることを意味する。上述の民主党系の FTC 委員であるロヒット・チョプラ氏が、米国のプライバシー法違反について個人に対する厳しい制裁を科すべきことを強く主張していることも重要である。連邦法である反トラスト法上のカルテル違反により日本企業の役員等の重役が数多く禁固刑で米国国内の刑務所に収監されるといった厳しい事件がかつて生じたこともあり、将来的な個人に対する厳しい制裁の導入の行方を含め米国連邦プライバシー法の法案の検討の動向には特に注視が必要である。

第2　CCPAの概要

1. CCPAの目的

2018年6月、カリフォルニア消費者プライバシー法（California Consumer Privacy Act：CCPA）が成立した。CCPAは、憲法上のプライバシー権を促進すること及び消費者の個人情報に関連する既存の法律を補完することを意図している（第1798.175条）。すなわち、CCPAは憲法上の人権に位置づけられるプライバシー権の保護を主な目的とする法律である。

2. CCPAに関するよくある勘違いや認識

米国各地や日本国内でのCCPAに関するセミナー参加者の反応やこれまでの問い合わせ内容を踏まえると、CCPAに関して以下のような勘違いや認識が見受けられる。

- CCPAがカリフォルニア州の州法であるため、カリフォルニア州に現地法人や拠点を持たない日本企業・組織は、CCPAが自社グループの事業に影響を及ぼさないのだと勘違いしてしまった。
- CCPAが「消費者」のプライバシー法であると名付けられているため、カリフォルニア州においてB to Cのビジネスを営んでいない企業・組織は、CCPAは自社グループの事業に影響を及ぼさないのだと考えてしまった。
- CCPA違反の場合の罰金は、一見すると巨額に見えないため、CCPAがGDPRほど恐ろしいデータ保護法だとは考えなかった。また、CCPA以外にもタイやインドをはじめとするアジア各国等の他の国のデータ保護法への対応が追い付いておらず、CCPAへの対応が後回しになってしまった。
- CCPAにはカリフォルニア州の司法長官によってCCPAの規則（Regulations）が制定されるまで司法長官がCCPAを執行できないと明確に書いてあるため、CCPAの規則案が公表されるまでは、CCPAへのコンプライアンス対応の検討を始めるのを先送りした方が賢明と考えてしまった。
- CCPAの条文を読んで自力で理解しようと試みたもののCCPAの条文が分かりにくいため、どこから手を付けて良いのか分からなかった。

3. CCPAの適用開始時期

CCPAは2020年1月1日に適用開始となる。2019年10月11日に成立した改正法の概要は以下の通りである。

AB25：従業員情報についての1年間の時限的適用除外等
AB1355：B to B情報についての1年間の時限的適用除外その他様々な修正
AB874：公に入手可能な情報、非識別情報、消費者情報集合体である情報の個人情報からの除外、個人情報の定義の限定
AB1146：保証・リコールに関する修理のための自動車情報と所有者情報の適用除外
AB1564：アクセス権行使の受付方法

CCPAは、CCPAの目的を増進するための規則を採択する権限をカリフォルニア州司法長官に委ねており、この措置の期限は2020年7月1日である。そして、司法長官が執行手続を取りうる最も早い日は、2020年7月1日又は司法長官による規則が公布された日から6か月後のいずれか早い方となっている。2019年10月10日、州司法長官によるCCPA規則（California Consumer Privacy Act Regulations）のドラフトが公表され、2019年12月6日までパブリックコメントの手続に掛けられた。

4. CCPA 規則案

(1) 概説

2019 年 10 月 10 日にカリフォルニア州司法長官より CCPA に関する規則(California Consumer Privacy Act Regulations)案（CCPA 規則案）及び INITIAL STATEMENT OF REASONS（ISOR)が公表された。ISOR は CCPA 規則案の各条文の立法趣旨を知る上で役立つ。規則の施行日は、2020 年 7 月 1 日又は最終規則公表後 6 か月後のいずれか早い方であるが、州司法長官は、今回の規則案公表のプレスカンファレンスにおいて、2020 年 7 月 1 日に規則を確定させエンフォースメントを開始する見込みとの発言をした。ただし、CCPA 自体は 2020 年 1 月 1 日から施行されるため、CCPA の適用を受ける法的主体は早急に CCPA に対するコンプライアンス対応を進める必要がある。

CCPA 規則案は、CCPA 遵守のための要件・ガイダンスを細かく規定するとともに、事業者に対する新たな義務も規定している。大きく分けて、消費者に対する通知(第 2 節)、消費者からの要求への対応に係るビジネスプラクティス(第 3 節)、消費者からの要求に係る本人確認(第 4 節)、未成年者に関する特別ルール(第 5 節)及び差別の禁止(第 6 節)について規定している。

(2) CCPA コンプライアンス実務に与える影響

CCPA 規則案には、CCPA の遵守に必要な社内のシステム・態勢整備の要件が細かく規定されている。本規則案は、本規則違反が CCPA 違反とみなされると定めている。したがって、本規則案が定める社内のシステム・態勢整備の要件に、企業・組織は忠実に従う必要がある。さらに、CCPA は、カリフォルニア州に所在する米国子会社のみならず、カリフォルニア州外の米国子会社や、日本本社を含む米国外の企業・組織にも一定の要件の下に適用がある法律である。したがって、CCPA 規則案の内容は、日本本社における CCPA 対応にも大きな影響があり得る。

Q. 日本本社にも CCPA の適用があると考えているが、当社では GDPR 対応を万全に行ったので、特に対応は不要と考えているが、問題はありますか。
A. CCPA 上は、GDPR よりも明らかに厳しい義務が課せられている項目が幾つもある。例えば、要求の検証義務のように本人確認の方法について詳細な要件を CCPA 規則案が定めていたり、またプライバシーポリシーにおいて開示すべき項目についても CCPA 規則案が詳細に定めている。これらだけを踏まえても、GDPR 対応が完了している日本本社であっても、CCPA の適用がある場合には、CCPA に違反する恐れがあるため、問題があるものと考えられる。

5. CCPA とは？

(1) CCPA を一言で言うと？

CCPA とは、消費者（カリフォルニア州の住民）に 8 つのプライバシーの権利を与え、当該「消費者」の「個人情報」を処理する「事業者」(Business：CCPA 第 1798.140 条第(c)項）に 8 つの義務を負わせる法律である。

	8 つのプライバシーの権利	事業者の義務
1	略式開示請求権	(1)消費者への通知義務（CCPA 規則案第 2 節） (2)消費者要求への対応のビジネスプラクティスに関する義務（CCPA 規則案第 3 節） (3)研修義務（CCPA 規則案第 999.317 条） (4)記録管理義務（CCPA 規則案第 999.318 条） (5)要求の検証義務（CCPA 規則案第 4 節）
2	拡張開示請求権	
3	アクセス及びポータビリティの権利	
4	事業目的で個人情報の販売又は開示を行う事業者に対する情報請求権	

5	個人情報の販売に関するオプトアウト権	(6)未成年者に関する特則の義務（CCPA 規則案第 5 節） (7)差別の禁止（CCPA 規則案第 6 節） (8)個人情報の性質に照らして合理的なセキュリティの手続と慣行を実装する義務（CCPA 第 1798.150 条）
6	子供のためのオプトイン権	
7	削除権	
8	CCPA 上の消費者の権利の行使を理由として差別されない権利	

CCPA は、「事業者」以外に、CCPA の適用対象として 3 つの類型、すなわち、「サービス提供者」(Service Provider: CCPA 第 1798.140 条第(v)項)、「第三者」(Third Party: CCPA 第 1798.140 条第(w)項))、「CCPA 第 1798.140 条第(w)項(2)に規定される者」(いわゆる「責任引受者」(liability-shifted person)) を規定している。

(2) CCPA の執行

a. カリフォルニア州司法長官による提訴による民事罰（CCPA 第 1798.155 条第(b)項）

- 事業者の義務に違反した場合、違反 1 件あたり最大 2,500 米ドル（故意の場合 7,500 米ドル）の民事制裁金が科され得る。
- 事業者は、不遵守を通知されてから 30 日以内に違反を是正しない場合、CCPA に違反することとなる（30 日の是正期間)。
- 州の司法長官が CCPA の目的を促進するための CCPA 規則の制定が控えており、その制定期限は、2020 年 7 月 1 日である。実際に州司法長官による執行ができるのは、上記の司法長官による上記規則の公布から 6 ケ月後か 2020 年 7 月 1 日のいずれか早い方である（CCPA 第 1798.185 条第(c)項）

b. 消費者による提訴（CCPA 第 1798.150 条第(a)項、第(b)項）

個人情報の性質に照らして合理的なセキュリティの手続と慣行を実装する義務を怠った結果により、個人情報が不正アクセス等された場合には、以下の各救済措置がある。

- 消費者によって 1 件（1 名、1 事故毎に算定）あたり、100 米ドル以上 750 米ドル以下の法定損害賠償又は実損のいずれか大きい額の賠償請求が行われ得る。
- この場合の「個人情報」の定義は狭い。すなわち、個人のファーストネーム若しくはファーストイニシャル及びラストネームと以下の情報の組み合わせに限られる。
  - ✓ ソーシャルセキュリティナンバー
  - ✓ 運転免許の番号
  - ✓ 州の ID の番号
  - ✓ 銀行口座番号
  - ✓ クレジットカード・デビットカード番号
  - ✓ 医療・健康保険の情報
  - ✓ 納税者番号
  - ✓ パスポート番号
  - ✓ 軍用識別番号
  - ✓ 政府の文書に付与された固有の識別番号
- 法定損害賠償請求について、30 日の是正期間あり
- 差止命令、確認判決、その他裁判所が適切と判断する救済措置

c. 特に、上記ｂのカリフォルニアの消費者による民事訴訟は、日本企業の米国子会社や米国支店に対してのみならず、日本本社等の日本企業グループの米国外拠点を名宛人として提起されることも予想される。当該民事訴訟が提起された場合には、企業・組織として応訴するための膨大な訴訟費用がかかることが考えられ、これに加えて、そのような訴訟が提起されること自体による企業・組織のレピュテーションの棄損も懸念される。前述の通り、企業・組織におけるデータ保護に関するレピュテーションの毀損が事業価値の毀損に直結する。消費者が違反行為を行う企業・組織に自己の個人データを利用させることを拒絶する結果、当該企業・組織にとって利用可能な個人データの質・量が低下する。利用可能な個人データの質・量が限定されることで、企業・組織の競争力が損なわれる。事業パートナーは、データ保護法を遵守しない企業・組織とのデータビジネスの連携はリスクであると評価する恐れがある。そうなると、データビジネスにおける事業パートナーとの協業に支障を来すこととなる。

第3　CCPAの適用範囲

1. CCPAの適用要件

(1) 概要

CCPA上、「事業者」がCCPAの適用対象となることは分かりやすい。CCPA全体を通覧すると、CCPAはCCPAの適用対象として4つのカテゴリーを想定している。

- 「事業者」(Business: CCPA第1798.140条第(c)項)（下記(2)）
- 「サービス提供者」(Service Provider: CCPA第1798.140条第(v)項)（下記(3)）
- 「第三者」(Third Party: CCPA第1798.140条第(w)項))（下記(4)）
- 「CCPA第1798.140条第(w)項(2)に規定される者」(いわゆる「責任引受者」(liability-shifted person))（下記(5)）

以下、それぞれの要件を説明する。

(2) 「事業者」の要件

「消費者」の「個人情報」を処理する「事業者」にCCPAが適用される。

要件	**「事業者」の要件＝要件1又は要件2**
1	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、 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が収集され、 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、 ④カリフォルニア州で事業を行い、かつ、 ⑤以下の基準の一つ又はそれ以上を満たす、個人事業体、パートナーシップ、有限責任会社、法人、団体又はその他の法的主体を意味する。 (i) 第1798.185条第(a)項(5)により調整された年間の総収入（annual gross revenues）が2,500万米ドル（$25,000,000）を超える。 (ii) 単独又は組み合わせで5万件以上の消費者、世帯又はデバイスの個人情報を、年間ベースで、単独又は組み合わせで購入し、事業者の商業目的で受け取り、販売し、又は商業目的で共有する。 (iii) 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。
2	①上記1に定める事業者を支配し又はこれに支配され、かつ ②当該事業者と共通のブランドを共有する主体。

a. 1①「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」

「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」たことが必要であるため、営利を目的としない非営利団体は「事業者」には該当しない。しかしながら、非営利団体が事業者から消費者の個人情報の販売を受ける場合には、「第三者」（第1798.140条第(w)項）（後記(4)）としてCCPAの遵守を求められる場面がある。したがって、非営利団体はCCPAと全く無関係というわけではない。

b. 1②「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が収集され」

(a) 消費者

「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し、一意識別子による場合を含めて、どのように識別されるかを問わない。

同条は(i)一時的に又は移動の目的以外でカリフォルニア州内にいる全ての個人及び(ii)カリフォルニア州内に住居を有する個人が一時的に又は移動の目的でカリフォルニア州の外にいる場合の個人を「住民」として定義する。すなわち、「住民」は所得税の賦課対象となる住民の定義によっている。

CCPA は同州に一時的にいる者については適用されないが、カリフォルニア州の住民であってカリフォルニア州外の学校に通っている学生には適用される。

上記要件(i)「一時的に又は移動の目的で」カリフォルニア州内にいるかどうかは、基本的に個別ケースの事実と周辺事情に拠ることになる。消費者が単に一時的にカリフォルニア州内外にいるのかを決定するために必要となる手間を前提とすると、消費者の該当性については広いアプローチを採用することにならざるを得ない。

Q. CCPA の適用対象となるのはカリフォルニア州の居住者（法人は除く）の個人情報のみで他州の居住者は含まないという理解で良いでしょうか。
A. 御理解の通りで良い。CCPA 第 1798.140 条第(g)項で「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居住者である自然人」を意味し、一意識別子による場合を含めて、どのように識別されるかを問わない。カリフォルニア州の居住者には、一時的又は移動目的以外でカリフォルニア州に所在する全ての者（国籍は問わない）及び一時的又は移動目的で州外に居るカリフォルニア州の居住者の両方が含まれる。

(b) 個人情報

「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、合理的に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する。個人情報には、以下に限定されるわけではないが、特定の消費者又は世帯を識別し、関連し、叙述し、合理的に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、以下が含まれる（第 1798.140 条第(o)項(1)）。

A. 識別子。例えば、
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（IP 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、その他の類似の識別子
（注）一位識別子又は一意個人識別子とは、経時的にかつ異なるサービスにおいて消費者、家族（親権者又は保護者、及び親権者又は保護者が監護する未成年の子ども）、又は消費者若しくは家族にリンクされたデバイスを認識するために使用できる一貫した識別子を意味する。一意個人識別子には以下のものを含むがこれらに限られない。
ーデバイス識別子、インターネット･プロトコル･アドレス（IP アドレス）、クッキー、ビーコン、ピクセルタグ、モバイル広告識別子又は類似の技術、顧客番号、一意の仮名又はユーザーの別名、電話番号、又は特定の消費者又はデバイスを識別するために使用できる持続的又は確率的な識別子（個人情報の定義に列挙されたカテゴリーに含まれ又は類似する個人情報のカテゴリーに基づいていない場合よりも確実性の高い消費者又はデバイスの識別）
B. 第 1798.80 条第(e)項で述べる個人情報のカテゴリー。以下に限定されるわけではないが、以下を含む。
当該個人の名前、サイン、社会保険番号、身体的特徴若しくは記述、住所、電話番号、旅券番号、運転免許証番号、州の識別カード番号、保険証券番号、学歴、雇用、雇用履歴、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、その他の財務情報、医療情報、健康保険情報

C. カリフォルニア州法又は連邦法のもとでの保護された分類の特性。
D. 商業的情報。以下の情報を含む。
個人の財産の記録、購入、取得、検討した製品又はサービスの記録、その他の購入又は消費の履歴又は傾向についての記録
E. バイオメトリック情報。バイオメトリック情報には、以下に限定されないが、以下が含まれる。
フェイスプリント、マニューシャ・テンプレート(特徴点登録情報)、声紋のような識別テンプレートを抽出できる虹彩、網膜、指紋、顔、手、手のひら、血管パターン及び音声録音の像並びに識別情報を含むタイピング・パターン若しくはリズム、歩行パターン若しくはリズム、睡眠、健康、又は運動データが含まれる。
F. インターネット又はその他の電子的なネットワーク活動の情報。以下を含むがこれに限られない。
閲覧履歴、検索履歴、インターネット・ウェブサイト、アプリケーション又は広告との消費者のやりとりの情報
G. 地理位置データ。
H. 音声、電子、視覚、温度、嗅覚又は類似の情報。
I. 職業又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

「個人情報」には、公に利用可能な情報は含まれない。「公に利用可能」とは、連邦、州、地域の政府の記録から適法に利用可能な情報を意味する。「公に利用可能」とは、消費者が知らないうちに、当該消費者について事業者が収集したバイオメトリック情報を意味しない（第 1798.140 条第(o)項(2)）。

また、「公に利用可能」には、非識別情報又は消費者情報集合体である消費者情報は含まれない（CCPA1798.140 条第(o)項(3)）。「非識別」とは、非識別情報を使用する事業者が以下に該当する場合で、直接的にも間接的にも、特定の消費者を合理的に識別し、関連付けし、記述し、連想させ、リンクさせることのできない情報を意味する（第 1798.140 条第(h)項）。

(1)情報が関連する消費者の再識別を禁止した技術的な保護措置を実施している。
(2)情報の再識別を特別に禁止したビジネス・プロセスを実施している。
(3)非識別情報の意図しない公表を防ぐビジネス・プロセスを実施している。
(4)情報の再識別の試みをしない。

また、「消費者情報集合体」とは、個々の消費者 ID を削除した、デバイスを経由したとしても消費者又は世帯に関連付けのない又は合理的に関連付けを可能としていない、消費者のグループ又はカテゴリーに関連する情報を意味する。「消費者情報集合体」は非識別化された一つ又は複数の個別的な消費者記録を意味しない（CCPA1798.140 条第(a)項）。

（個人情報の定義）
Q.個人情報取得の目的ではない別の事業目的で撮影された映像の中に偶然映った個人の顔は、CCPA の適用対象の個人情報に含まれるのでしょうか。
A. CCPA 1798.140 条第(o)項(1)で「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するものとされている。前提として、その取得目的を問わないため、個人情報取得の目的ではない別の事業目的で取得されたかどうかは該当性判断にあたり影響を及ぼすものではないと考えられる。また、顔が識別できる個人の写真については個人情報にあたるものと考えられる。

(c) 収集

「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、受領し又はそれにアクセスすることを意味する。これには、能動的若しくは受動的に消費者から情報を受領すること、又は、消費者行動の観察を通じて情報を受領することが含まれる。

c. 1③「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」

(a) 処理

「処理」とは、自動化された手段によるかどうかにかかわらず、個人データ又は個人のデータ･セットに対して行われるオペレーション又は一連のオペレーションを意味する。

(b)「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」

CCPA 上は、消費者の個人情報を処理する目的と手段を決定する場合にのみ、「事業者」に該当することになる。したがって、他の法的主体から、消費者の個人情報の処理のみを委託され、当該処理の目的と手段の決定に一切関わらない場合には、「事業者」には該当しないことになる。但し、消費者の個人情報の処理の委託がある場合に、当該処理の目的と手段の決定に関与したかどうかについては、明確な線引きが難しい場合もある。例えば、米国子会社が日本本社に委託してカリフォルニア住民の個人情報を処理してもらうという関係がある場合、米国子会社が当該処理の目的と手段の決定を行っており、日本本社は当該処理の目的と手段の決定に一切関わらないと言えるか否かは、微妙な問題となるケースが多いと考えられる。これは日本本社は、資本関係上米国子会社を支配する関係に立つため、米国子会社からの委託の趣旨を超えて、独自の目的で当該個人情報の処理を行うことが容易であるためである。すなわち、日本本社は米国子会社と共同して消費者の個人情報を処理する目的と手段を決定し当該個人情報を収集したとして、CCPA 上の「事業者」に該当する場合が考えられるということである。

Q. 日本本社が CCPA の直接適用を受ける場合として、どのような場合が考えられるのでしょうか。当社（日本国内会社）の場合、カリフォルニア州内に米国子会社を有しており、同社の従業員（カリフォルニア州の居住者）の個人情報の共有を受けているだけなのですが、当社にも CCPA の直接適用はあり得るのでしょうか。

A. 日本本社である貴社が、米国子会社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当該消費者の個人情報を収集し、又は単独で消費者の個人情報を処理する目的と手段を決定して米国子会社を通じて当該消費者の個人情報を収集したと、評価できる場合には、貴社への CCPA の直接適用はあり得ると考える。

Q. 第 1798.140 条第(c)項(1)(ⅱ)に規定される 5 万件の個人情報の受領等の要件について、"Service provider"としてユーザーから預かるデータに含まれる個人情報も含まれるでしょうか。含まれる場合、ユーザーから預かるデータの内容を原則閲覧しないことを利用規約で定め、運用上もそのとおりとなっている場合でも結論は変わらないでしょうか。

A. CCPA 上の「サービス提供者」とは、「事業者に代わって情報を処理し、かつ、事業目的のために書面の契約により事業者から消費者の個人情報を開示される、株主又はその他の所有者の利益と金銭的便益のために組織され又は運営される個人事業体、パートナーシップ、有限責任会社、法人、団体、その他の法的主体を意味する。ただし、事業者との契約により、個人情報を受領する法的主体が、当該契約で特定されたサービスを行う特定の目的又はその他本巻で認められたもの以外の目的のために、個人情報を保持し、使用し又は

開示すること（事業者との契約によって特定されたサービス提供以外の商業的な目的のために個人情報を保持し、利用し又は開示することを含む。）を禁止する場合をいう。」とされる（CCPA 第 1798.140 条第(v)項)。「サービス提供者」は、「消費者の個人情報を処理する目的と手段を決定する」法的主体の存在を前提としたものであることから、消費者の個人情報の処理の目的と手段の決定には関与しないことが、暗に要件とされていると読むのが合理的であると考える。したがって、「サービス提供者」に該当する法的主体については、上記 1③「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」という要件への該当性が否定され、その結果として、第 1798.140 条第(c)項(1)(ⅱ)の要件の適用の検討の前提を欠くことになるため、問題とならないものと考えられる。

d. 1④「カリフォルニア州で事業を行い」

CCPA は「カリフォルニア州で事業を行」う場合に適用されるが、この基準は CCPA 上定義されていない。州法人税を所管するカリフォルニア・フランチャイズ税委員会（the California Franchise Tax Board）によれば、「カリフォルニア州で事業を行」うことは「金銭的な又は金銭的な利得もしくは利益を目的として取引に能動的に従事すること」によって構成され、カリフォルニア州外の法的主体が「カリフォルニア州で事業を行う」とみなされ得る（歳入及び課税法第 23101 条参照)。したがって、カリフォルニア州外の法的主体がカリフォルニア州の消費者の個人情報を販売し又は開示する場合は当該法的主体に CCPA が適用され得る。

e. 1⑤「以下の基準の一つ又はそれ以上を満たす、個人事業体、パートナーシップ、有限責任会社、法人、団体又はその他の法的主体」

CCPA の対象となる事業者には、上記 1①から 1④の基準を満たす限り、「個人事業体、パートナーシップ、有限責任会社、法人、団体又はその他の法的主体」は全て該当し得る。

Q. 日本の本国からの出資を受けている会社が多いと思うので、対象会社となる基準を改めて教えて欲しい。米国支店、米国子会社、色々な形態をとっている会社があろうかと思います。

A. CCPA の適用対象となる「事業者」には、米国内、米国外を問わず、幅広い法的主体が該当し得る。米国子会社は上記 1 又は上記 2 の要件を満たす場合には CCPA の「事業者」に該当し、CCPA の適用を受ける。米国内に支店や駐在員事務所を持つ日本企業・組織も、法人格を持つ主体自体は日本国内、すなわち米国外に所在することになるが、CCPA 上は上記 1 又は上記 2 の要件を満たす限り、「事業者」に該当し、CCPA の適用を受ける。

但し、第 1798.145 条第(a)項(6)に CCPA の適用除外に関する規定があり、「対象となる行為の全ての側面がカリフォルニア州外で行われている」場合には CCPA の適用がないとされている。具体的には、以下の各要件をいずれも充足する場合に「対象となる行為の全ての側面がカリフォルニア州外で行われている」ものとされる。

(a)消費者がカリフォルニア州外にいるときに事業者が個人情報を取得した

(b)カリフォルニア州で消費者の個人情報を販売する行為が一部でも行われていない

(c)消費者がカリフォルニア州にいたときの個人情報を販売していない

日本本社による消費者（カリフォルニア州の住民）の個人情報の収集・販売がこの適用除外規定に該当するかは事案によるが、通常、日本本社が収集・販売する全ての消費者の個人情報について上記(c)の要件が充足されることは考えづらく、この適用除外規定によって消費者の個人情報を収集・販売する日本本社への CCPA の適用が否定されることはあまりないと考えられる。

f. 1⑤(i)「年間の総収入が 2,500 万米ドル（$25,000,000）を超える」

年間の総収入 2,500 万米ドルはカリフォルニア州内のものに限るのか、それとも、カリフォルニア州内に限らないのか。この点は CCPA 上も明示的に記述されていないため、不明確である。

しかしながら、カリフォルニア州内で生じた総収入に限らないというのが圧倒的多数説である。これは他の二つの要件においては当該要件がいずれもカリフォルニアの消費者に関して適用されることが明示されているという事実からも明らかであると考えられる。すなわち、総収入の基準にもカリフォルニア州で生じたものに限るという限定を入れることができたのにもかかわらず、その限定は入らなかったということである。

Q. CCPA の対象基準のひとつである「年間の総収入が 2,500 万米ドル（$25,000,000）を超える」は、親会社の売上高も含むのでしょうか。たとえば、カリフォルニア州でビジネスを行っている日本法人の子会社で、その子会社単体の年間総売上高は年間の総収入が 2,500 万米ドル（$25,000,000）を超えないものの、日本の親会社の売上高を含むと年間の総収入が 2,500 万米ドル（$25,000,000）を超える場合、当該日本の子会社と親会社には、それぞれ CCPA の適用はあるのでしょうか。
A: 上記要件の総収入については事業者毎に判断する必要があり、米国子会社のみで年間の総収入を超えない場合には、当該米国子会社は要件 1 への該当性は否定される。したがって、CCPA の対象基準のひとつである「年間の総収入が 2,500 万米ドル（$25,000,000）を超える」は、親会社の売上高は含まないと考えられる。但し、日本の親会社が、要件 1 との関係で「事業者」に該当する場合であって、かつ当該米国子会社と共通ブランドを使っている場合には、「①上記 1 に定める事業者」「に支配され」、かつ②当該事業者と共通のブランドを共有する主体に該当し、その結果、当該米国子会社も「事業者」に該当することになり、CCPA が適用される。

Q. カリフォルニア州に拠点のない日本企業が、カリフォルニア州で、営業目的で、日本からカルフォルニア州の居住者へ販売促進活動をする場合、カリフォルニア州での売上が一切上がっていない段階でも CCPA の適用はあり得ますか。
A: 上記要件 1 ではカリフォルニア州での売上が一切上がっていない法的主体であっても、当該法的主体の年間のカリフォルニア州外のものを含めた総収入が 2,500 万米ドル（$25,000,000）を超える場合には、要件 1 の他の要素を満たす限りにおいて、カリフォルニア州内での売上が一切上がっていない段階でも CCPA の適用はあり得ると考えられる。

g. 1⑤(ii)「単独又は組み合わせで 5 万件以上の消費者、世帯又はデバイスの個人情報を、年間ベースで、単独又は組み合わせで購入し、事業者の商業目的で受け取り、販売し、又は商業目的で共有する」

(a) 販売

「販売」とは、金銭又はその他の価値のある対価のために、事業者が他の事業者又は第三者に対して、消費者の個人情報を、販売し、賃貸し、公表し、開示し、広め、利用可能にさせ、移転し、又は、その他口頭で、書面で、電子的若しくはその他の方法により伝えることを意味する（CCPA 第 1798.140 条第(t)項(1)）。

CCPA 上は、「…その他の価値のある対価のために」という要件が非常に広く解されているため、事業者が「サービス提供者」（後記(3)）又は「責任引受人」（後記(5)）に該当するための所定の契約を締結せずに、他の「事業者」又は「第三者」（後記(4)）に対して、消費者の個人情報を移転等している場合には、下の第 1798.140 条第(t)項(2)(A)から(D)のいずれかの例外に該当しない限り、基本的に「販売」に該当すると考えた方が良い。

第 1798.140 条第(t)項(2)

本巻の目的のため、以下の場合、事業者は個人情報を販売していない。
(A)消費者が、意図的に個人情報を開示するため事業者を使用若しくは指示し、又は第三者と意図的にやりとりするために事業者を使用する場合で、当該第三者も個人情報を販売しないとき。ただし、個人情報の開示が本巻の規定と整合する場合を除く。意図的なやりとりは、一つ又は複数の計画的なやりとりを通じて、第三者とやりとりをする意図がある場合に、生じる。あるコンテンツの一部にとどまり、消音し、中断し、又は閉じることは、第三者とのやりとりをする意図に該当しない。
(B)個人情報の販売をオプトアウトした消費者の識別子を、消費者がその個人情報の販売をオプトアウトした事実を第三者に警告することを目的に、事業者が利用し又は共有している。
(C)事業者が、事業者目的を遂行するために必要な消費者の個人情報を使用し又はサービス提供者と共有する場合で、以下の条件の両方が満たされるとき。
(i)事業者が第 1798.135 条に整合する条件で情報が利用され共有されているとする通知を提供している。
(ii)サービス提供者が、事業目的の遂行に必要な場合を除き、消費者の個人情報をさらに収集し、販売し又は使用していない。
(D) 事業者が消費者の個人情報を合併、買収、破産又は第三者が事業者の全て又は一部のコントロールを取得するその他の取引の資産の一部として、第三者に移転する場合。ただし、情報が第 1798.110 条及び第 1798.115 条に従って利用され又は共有されているときに限る。第三者が、収集時に行った約束と実質的に整合しない方法で消費者の個人情報の利用又は共有の仕方を実質的に変更しているならば、その第三者は新たな又は変更した実務について事前に通知をその消費者に提供しなければならない。その通知は既存の消費者が第 1798.120 条と整合する選択を容易に行使できることを確保するように、十分に目立ち、かつ、しっかりしたものでなければならない。本項は、不公正取引慣行法（事業・職業法第 7 編第 2 部（第 17200 条から開始）第 5 章）に違反する形で事業者が実質的、遡及的にプライバシー･ポリシーを変更すること、又はプライバシー･ポリシーに他の変更を加えることを認めるものではない。

(b) 商業目的

「商業目的」とは、他の者が製品、商品、財産、情報又はサービスについて購入し、賃借し、賃貸し、参加し、登録し、提供し又は交換することを促すことなどによりある者の商業的又は経済的な利益を高めること、又は、直接的又は間接的に商業的な取引を可能とし又は達成することを意味する（CCPA 第 1798.140 条第(f)項)。「商業目的」には、政治的な言論及びジャーナリズムを含む非商業的な言論として連邦又は州の裁判所が認めてきた言論に関わる目的を含まない。

(c) 概説

カリフォルニア州の個人から年間で 5 万件以上（1 日平均約 137 件）のアクセスがあるウェブサイトを運営し、その個人情報（IP アドレスや Cookie 識別子等も含まれる）を受領している場合には、上記(a)の通り「販売」の概念が広くなっているため、本 1⑤(ii)の要件を満たすことになる。また、文言上は、自社サイトの運営により取得する個人情報に限らず、海外企業からカリフォルニア州の住民の個人情報を多数受け取る場合にも適用があり得る点に注意が必要である。

Q. CCPA の適用基準の一つとして、5 万件以上の個人情報を、年間ベースで、単独又は組み合わせで購入し、事業者の商業目的で受け取り、販売し、又は商業目的で共有するというものがあると聞きました。この 5 万件以上のカウントの仕方を教えてください。例えば、ある個人の Email アドレスと電話番号と住所を所有し

ている場合、それを「1」とカウントするのか、「3」とカウントするのかどちらでしょうか。また、ある個人と世帯の個人、又はデバイスの所有者が重複している場合、それは1とカウントして良いのでしょうか。
A. CCPA 第 1798.140 条第(c)項 (1) (ii)の条文上の文言では「5 万件以上の消費者、世帯又はデバイスの個人情報」とされており、単純な個人情報の個数ではなく、「消費者、世帯又はデバイス」が基準となっていると解することが文言に即すると考えられる。したがって、1 人の消費者について、Email アドレスと電話番号と住所を所有している場合については、3 ではなく、1 とカウントして良いと考えられる。他方で、ある個人と世帯の個人又はデバイスの所有者が重複している場合には、1 とカウントすることをサポートする証拠がないため、保守的に考えて、3 とカウントするべきと考える。

Q. CCPA の適用基準の一つとして、5 万件以上のカリフォルニア州の居住者の個人情報を、年間ベースで、単独又は組み合わせで購入し、事業者の商業目的で受け取り、販売し、又は商業目的で共有するというものがあると聞きました。コーポレートサイト閲覧に合わせて取得される cookie や IP アドレス等の情報について、その主体がカリフォルニア州居住者かどうか判別不可能な場合、どのようにカウントすれば良いでしょうか。
A.カリフォルニア州の居住者の個人情報である可能性があるものとして数に含めて算定するのが実務上は安全と考える。

h. 2①「上記 1 に定める事業者を支配し、又はこれに支配され、かつ②当該事業者と共通のブランドを共有する主体」

グループ会社の中に要件 1 に該当する事業者があると、他のグループ会社にも CCPA が適用される可能性があることに注意が必要である。具体的には、要件 1 に該当する事業者を支配し又はその事業者により支配され、及び、その事業者と共通のブランドを有している事業者に対しても、CCPA が適用される。

「支配」とは、事業者の議決権のある種類の株式について発行済み株式の 50%超を保有し又は議決権を有すること、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、又は、事業者のマネジメントについて支配的な影響を行使する権限があることを意味する。「共通のブランド」とは、共通の名称、サービス・マーク又は商標を意味する。

そのため、グループ会社の中に要件 1 に該当する事業者（例えば、カリフォルニアで事業を行っている米国現法）を有している場合には、その親会社である日本企業にも CCPA が適用されるし、その事業者の子会社にも CCPA が適用される。

Q. どのくらいの割合の日本企業グループに対して CCPA が適用されるのでしょうか。
A. 上記(2)a からの「事業者」の要件を総合すると、消費者（カリフォルニア州の住民）の個人情報を何らかの形で処理している、日本企業本社及び日本企業の米国子会社又は米国支店が、「事業者」の要件に該当する場合のパターンとして、以下のようなものが見えてくる。

- 日本企業の米国子会社が単体で約 2,500 万米ドルの売上高を持ち「事業者」の要件に該当する。日本企業本社も単体で約 2,500 万米ドルの売上高を持ち「事業者」の要件に該当する。上記 h の要件によって日本企業本社の子会社（上記米国子会社を含む）は「事業者」に「支配」され（共通のブランドを使用していることから)、「事業者」の要件に該当し得る。
- 日本企業の米国子会社は単体では約 2,500 万米ドルの売上高を持たず「事業者」の要件に該当しない。日本企業本社は単体で約 2,500 万米ドルの売上高を持ち「事業者」の要件に該当する。上記 h の要件に

よって日本企業本社という「事業者」に「支配」され（かつ共通のブランドを使用している）る米国子会社を含む子会社は「事業者」の要件に該当し得る。

- 日本企業の米国支店は、支店自体の売上高は約 2,500 万米ドルに満たないが、当該日本企業自体の売上高が約 2,500 万米ドルを超えているため「事業者」の要件に該当する。

米国内に拠点を持ち多少なりとも消費者（カリフォルニア州の住民）の個人情報を処理している日本企業本社は「事業者」に該当する場合が多く、日本国内の日本企業本社自体が CCPA のコンプライアンス対応を執らなければならない場合が多いと考えられる（但し、上述の通り、日本企業本社が、米国子会社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当該消費者の個人情報を収集し、又は単独で消費者の個人情報を処理する目的と手段を決定して米国子会社を通じて当該消費者の個人情報を収集したと評価できることが、日本企業本社が「事業者」に該当する前提となる。また、上述の通り、「対象となる行為の全ての側面がカリフォルニア州外で行われている」場合の第 1798.145 条第(a)項(6)に CCPA の適用除外に関する規定の適用の有無の検討も必要となる。）。

そして、この日本企業の米国子会社は共通のブランドを使用する等の関係に立つ場合には日本企業本社に「支配」されているため、自社の売上高が約 2500 万米ドルを超えるか否かに関わらず「事業者」に該当し、CCPA のコンプライアンス対応を執らなければならない場合が多いと考えられる。

(3) 「サービス提供者」の要件

「サービス提供者」とは、事業者に代わって情報を処理し、かつ、事業目的のために書面の契約により事業者から消費者の個人情報を開示される、株主又はその他の所有者の利益と金銭的便益のために組織され又は運営される個人事業体、パートナーシップ、有限責任会社、法人、団体、その他の法的主体を意味する。ただし、事業者との契約により、個人情報を受領する法的主体が、当該契約で特定されたサービスを行う特定の目的又はその他本巻で認められたもの以外の目的のために、個人情報を保持し、使用し又は開示すること（事業者との契約によって特定されたサービス提供以外の商業的な目的のために個人情報を保持し、利用し又は開示することを含む。）を禁止する場合をいう（CCPA 第 1798.140 条第(v)項）。

事業者が、事業目的を遂行するために必要な消費者の個人情報を使用し又はサービス提供者と共有する場合で、事業者が第 1798.135 条に整合する条件で情報が利用され共有されているとする通知を提供しており、かつ、「サービス提供者」が事業目的の遂行に必要な場合を除き、消費者の個人情報をさらに収集し、販売し又は使用していない場合には、「販売」には該当しないため、消費者によるオプトアウトの権利の対象外となる。

また、サービス提供者に個人情報を開示する事業者は、個人情報を受け取るサービス提供者が本巻に定める制限に違反してその情報を使用している場合、その個人情報を開示するときにサービス提供者が違反を行う意図であったことについて実際に知らず又はそう信じるべき理由を持たないとき、CCPA のもとに責任を問われない。サービス提供者は、サービスを提供する事業者の義務について、同様に、本巻に定めるように CCPA のもとに責任を問われない（CCPA 第 1798.145 条第(j)項）。

したがって、事業者としては、上記契約を締結し、個人情報の提供の相手方が、CCPA 上の「サービス提供者」に該当するように対応する利点がある。

また、CCPA 規則においては次の通りサービス提供者に関するみなし規定及びサービス提供者による個人情報の利用の範囲と消費者要求の拒否の方法について定めがある。

第 999.314 条 サービス提供者

事業者でない組織にサービス提供する場合のみなし規定	(a) 人又は主体が人又は事業者でない組織にサービスを提供する範囲で、かつその他の点ではCCPA第1798.140条第(v)項の「サービス提供者」の要件を満たす場合、当該人又は主体はCCPA及び本規則の目的のためサービス提供者とみなす。
	(b) 人又は主体が事業者に代わって消費者から直接個人情報を収集するよう事業者が指示する範囲で、かつその他の点ではCCPA第1798.140条第(v)項の「サービス提供者」の他の全要件を満たす場合、当該人又は主体はCCPA及び本規則の目的のためサービス提供者とみなす。
目的外利用の例外	(c) サービス提供者は、サービスを提供する人若しくは主体から受領した個人情報又は消費者のサービス提供者との直接のやりとりから得た個人情報を、他者又は他の主体にサービスを提供する目的で利用してはならない。ただし、サービス提供者は、自らがサービス提供者となっている一又は複数の主体から受領した個人情報を、データセキュリティ事故を探知する範囲又は偽装若しくは違法な行為から保護する範囲でそれら事業者の代わりに組み合わせることができる。
消費者要求の拒否の根拠の説明	(d) サービス提供者がサービスを提供する事業者の代わりに収集、保持、販売する個人情報に関して消費者から知る要求又は削除の要求を受領した場合で要求に従わない場合、サービス提供者は消費者に拒否の根拠を説明する。サービス提供者は、サービス提供者が代わって情報を処理している事業者に直接要求を提出するよう消費者に通知し、可能な時は、当該事業者の連絡先を消費者に提供する。
事業者としてのCCPA遵守義務	(e) 事業者であるサービス提供者は、サービス提供者としての役割を超えて収集、保持又は販売する個人情報につき、CCPA及び本規則に従う。

(4)「第三者」の要件

CCPA上、消費者が第1798.120条による明示的な通知を受け、かつオプトアウトの権利を行使する機会を与えられた場合を除き、第三者は、事業者から販売された消費者の個人情報を販売してはならない（第1798.115条第(d)項）とされている[3]。この限度で「第三者」もCCPAの適用対象であり、「事業者」と「サービス提供者」とは区別される第3のカテゴリーであるといえる（但し、後述の通り、全てのサービス提供者は「第三者」に該当する。）。

CCPA上の「第三者」とはCCPAによって定義される広いカテゴリーであり、以下を含む。

a. 全てのサービス提供者

b. 当初個人情報を収集した事業者以外の事業者

c. CCPA第1798.140条第(w)項(2)に規定される者以外の者（any other person）

したがって、「サービス提供者」は広い概念である「第三者」のサブカテゴリーに位置付けられるといえる。

CCPA上の「販売」とは、金銭又はその他の価値のある対価のために、事業者が他の事業者又は第三者に対して、消費者の個人情報を移転等するものと定義される（CCPA第1798.140条第(t)項(1)）ため、第三者への個人情報の移転は、「販売」とみなされるリスクがある。CCPA上、消費者が第1798.120条による明示的な通知を受け、かつオプトアウトの権利を行使する機会を与えられた場合を除き、第三者は、事業者から販売された消費

[3] 本巻（CCPA）に違反する事業者、サービス提供者又はその他の者（other person）は、差止命令の対象になり、また、違反1件について2,500ドルを超えない額の民事上の罰金又は故意の違反1件について7,500ドルを超えない額の民事上の罰金を支払う義務があり、それはカリフォルニア州の人々の名のもとに司法長官により提起される民事訴訟において評価され回収される。本条に規定する民事上の罰金はカリフォルニア州の人々の名のもとに司法長官により提起される民事訴訟においてのみ評価され回収される（第1798.155条第(b)項）。

者の個人情報を販売してはならない（第 1798.115 条第(d)項）とされていることから、「第三者」は当該販売禁止の条項に違反しないことを確保することが必要となる。

Q. 当組織はカリフォルニア州にオフィスを構えており、カリフォルニア州の住民の個人情報を収集していますが、非営利団体であるため、CCPA の適用はないと考えていますが、正しいでしょうか。もし、当組織に CCPA の適用がある場合には、必要最小限の CCPA コンプライアンス対応としてはどのようなものが考えられるでしょうか。

A. 非営利団体であっても「第三者」に該当し、CCPA の適用があることが考えられる。CCPA 上、消費者が第 1798.120 条による明示的な通知を受け、かつオプトアウトの権利を行使する機会を与えられた場合を除き、第三者は、事業者から販売された消費者の個人情報を販売してはならない（第 1798.115 条第(d)項）とされていることから、「第三者」は当該販売禁止の条項に違反しないことを確保することが必要となる。「第三者」として取るべき必要最小限の CCPA コンプライアンス対応としては以下のものが考えられる。

1. 消費者（カリフォルニア州の住民）の個人情報を保有の有無をチェックする。そのうえで、当該個人情報の入手経路についてデータの分類化（data classification）の作業を行う。
    - データ分類化の作業とは、当該個人情報の入手経路が、①消費者からの直接の収集、②サービス提供者の契約の下での移転、③責任引受者の契約の下での移転、④事業者からの販売のいずれに基づくものかを仕分けする作業のことをいう。
2. 入手経路が上記④に該当する個人情報を他の法的主体に移転することについて必要な通知及び開示義務を遵守するための措置を講じる。
    - ④に該当する個人情報についてさらに別の法的主体に「販売」することが禁じられているが、「販売」の概念が広く定義されていることから、別の法的主体に当該個人情報を移転している場合には、通常「販売」したと見なされることになる。そのため、④に該当する個人情報を別の法的主体に移転する場合には、当該移転に先立って、当該消費者が第 1798.120 条による明示的な通知を受け、かつオプトアウトの権利を行使する機会を与えられることを確保する措置を講じる必要がある。
    - 個人情報が共有される第三者にとっての特別な通知義務：第三者が、収集時に行った約束と実質的に整合しない方法で消費者の個人情報の利用又は共有の仕方を実質的に変更しているならば、その第三者は新たな又は変更した実務について事前に通知をその消費者に提供しなければならない。その通知は既存の消費者が第 1798.120 条と整合する選択を容易に行使できることを確保するように、十分に目立ち、かつ、しっかりしたものでなければならない。
    - 上記特別な通知は、不公正取引慣行法（事業・職業法第 7 編第 2 部（第 17200 条から開始）第 5 章）に違反する形で第三者が実質的、遡及的にプライバシー・ポリシーを変更すること、又はプライバシー・ポリシーに他の変更を加えることを認めるものではない。
3. 将来的に上記④の経路で入手する消費者の個人情報を適切に扱うため、社内規則において上記 1 及び 2 の措置を継続的に執ることを義務付ける。社内研修においても当該社内規則の内容について触れる。

(5)「CCPA 第 1798.140 条第(w)項(2)に規定される者」（いわゆる「責任引受者」（liability-shifted person））の要件

a. 定義

CCPA の適用対象の第 4 のカテゴリーが、「CCPA 第 1798.140 条第(w)項(2)に規定される者」である。

CCPA 第 1798.140 条第(w)項(2)に規定される者とは、(A)事業者が書面の契約により事業目的のために消費者の個人情報を開示する相手（但し、当該契約が、当該個人情報を取得する者（すなわち、当該消費者の個人情報を開示する相手）が、(I)個人情報の販売、(II)契約で特定された特定のサービスの提供以外の商業的な目的のための個人情報の保持、使用又は開示を含む、契約で特定されたサービス提供の特定の目的以外の目的のための個人情報の保持､使用又は開示、及び(III)当該個人情報を取得する者と事業者の間の直接的な事業関係以外での、情報の保持、使用又は開示を禁止している場合であって、かつ、その者が（A）項の制限を理解しかつそれを遵守することを示す、当該個人情報を取得する者によって作成された証明書を含んでいる場合に限る。）のことをいい、(B)本巻に定める制限のどれかに違反した本項の対象となる者は、その違反の責任を負う（本項を遵守する本項の対象となる者に対して個人情報を開示する事業者は、その個人情報を取得する者が本巻に規定する制限に違反してそれを使用していたとしても、その個人情報を開示する時にその者がそうした違反を行う意図であることについてその事業者が実際に知らず又はそう信じる理由を持たない場合には、本巻のもとでは責任を負わない。）。

上記(A)及び(B)の要件は、要するに、事業者が事業目的のために消費者の個人情報を開示する相手に対して、当該相手が CCPA に違反した場合の責任を、当該相手に負わせることを、一定の条件のもとに認めるものである。「CCPA 第 1798.140 条第(w)項(2)に規定される者」は、論者によって、契約事業者（contractor）と形容されたり、又は「責任引受者」（liability-shifted person）とも呼ばれるが、本ハンドブックでは、分かりやすさのために、「責任引受者」と呼ぶことにする。

前述の通り、CCPA 上の「販売」とは、金銭又はその他の価値のある対価のために、事業者が他の事業者又は第三者に対して、消費者の個人情報を、移転等するものと定義される（CCPA 第 1798.140 条第(t)項(1)）。「責任引受者」は「第三者」には該当しないため、「責任引受者」への個人情報の移転は「販売」から除外される。

b. 「サービス提供者」と「CCPA 第 1798.140 条第(w)項(2)に規定される者」（いわゆる「責任引受者」（liability-shifted person）の比較

サービス提供者も責任引受者もいずれも事業者のためのベンダーとして行動するため、紛らわしい。両者の間には以下のような違いがある。

(a) サービス提供者は「第三者」であるが、責任引受者は「第三者」ではない。
(b) サービス提供者は法的主体である必要があるが、責任引受者は自然人を含む如何なる者でもよい。
(c) サービス提供者は処理者として行動するが、責任引受者は処理者又は管理者として行動する。
(d) サービス提供者は営利目的とするが、責任引受者は非営利であってもよい。
(e) 責任引受者は自らに課せられた契約上の制限を理解しかつそれを遵守することを示す証明書に署名しなければならないが、サービス提供者はそうした証明書に署名しない。
(f) サービス提供者は、当該サービス提供者に個人情報を移転する事業者が CCPA に違反してその情報を使用している場合、当該事業者が違反を行う意図であったことについて実際に知らず又はそう信じるべき理由を持たないとき、CCPA のもとに責任を問われない（CCPA 第 1798.145 条第(j)項）が、責任引受人にはそれに相当する責任限定の規定はない。
(g) サービス提供者の運用上のニーズは CCPA 第 1798.105 条第(d)項の下で削除の要求に従うかどうかを決定する際に考慮されるが、責任引受人の運用上のニーズは考慮されない。
(h) サービス提供者の運用上の目的での個人情報の使用は CCPA 上の「事業目的」と考えられ得るが、責任引受人の運用上の目的での個人情報の使用は CCPA 上の「事業目的」とは見做されない。

サービス提供者及び責任引受者に適用される契約の要件は以下の通り非常によく似ているが、同一のものではない。

「サービス提供者」(CCPA 第 1798.140 条第(v)項)	「責任引受者」(CCPA 第 1798.140 条第(w)項(2))
「ただし、事業者との契約により、個人情報を受領する法的主体が、当該契約で特定されたサービスを行う特定の目的又はその他本巻で認められたもの以外の目的のために、個人情報を保持し、使用し又は開示すること（事業者との契約によって特定されたサービス提供以外の商業的な目的のために個人情報を保持し、利用し又は開示することを含む。）を禁止する場合をいう」	「…当該契約が、当該個人情報を取得する者（すなわち、当該消費者の個人情報を開示する相手）が、(I)個人情報の販売、(II)契約で特定された特定のサービスの提供以外の商業的な目的のための個人情報の保持、使用又は開示を含む、契約で特定されたサービス提供の特定の目的以外の目的のための個人情報の保持､使用又は開示、及び(III)当該個人情報を取得する者と事業者の間の直接的な事業関係以外での、情報の保持、使用又は開示を禁止している場合…に限る。」

- サービス提供者及び責任引受者は、いずれも契約上、事業者のためのサービスを行う特定の目的以外の目的で個人情報を保持し、使用し又は開示することが禁止されなければならないが、責任引受者とは異なり、サービス提供者はその他 CCPA で認められた目的で個人情報を保持し、使用し又は開示することが認められている。
- 責任引受者との契約においては、サービス提供者との契約においては不要な要件、すなわち、当該個人情報を取得する者と事業者の間の直接的な事業関係以外での、情報の保持、使用又は開示の禁止を含まなければならない。

(6) 「事業者」、「サービス提供者」、「第三者」及び「CCPA 第 1798.140 条第(w)項(2)に規定される者（責任引受者)」の関係

「事業者」、「サービス提供者」、「第三者」及び「CCPA 第 1798.140 条第(w)項(2)に規定される者（責任引受者)」の関係を表で示すと以下の通りとなる。CCPA 上、「サービス提供者」と「第三者」が区別して扱われているが、「第三者」の定義を前提にすると「サービス提供者」に該当する場合には常に「第三者」にも該当することになる。

事業者	
第三者	a. 全てのサービス提供者 b. 当初個人情報を収集した事業者以外の事業者 c. CCPA 第 1798.140 条第(w)項(2)に規定される者（責任引受者）以外の者
CCPA 第 1798.140 条第(w)項(2)に規定される者（責任引受者）	

第 4　CCPA の適用除外

CCPA 上の「消費者」の「個人情報」を処理する「事業者」に該当する場合であっても、CCPA 上の適用除外規定に該当する場合には、CCPA は適用されないことになる。適用除外の概要は以下の通りである。

1. 全ての側面が州外で行われる場合の適用除外（CCPA 第 1798.145 条第(a)項（6））

第 1798.145 条
(a)本巻により事業者に課される義務は、以下の事業者の権能を制限しない。
(6)商業的な行為のどの側面も完全にカリフォルニア州の外で行われている場合に、消費者の個人情報を収集し又は販売すること。本巻の目的のため、消費者がカリフォルニア州の外にいるときに事業者が情報を収集し、消費者の個人情報の販売のいかなる部分もカリフォルニア州で生じておらず、また、消費者がカリフォルニア州にいたときに収集された個人情報が販売されていない場合に、商業的行為は完全にカリフォルニア州以外で行われたものとする。本パラグラフは、消費者がカリフォルニア州にいるときにその個人情報を事業者がデバイス上を含めて保存し、その後消費者及び保存される情報がカリフォルニア州の外であるときにその個人情報を収集するということを認めない。

対象となる行為の全ての側面がカリフォルニア州外で行われている場合には CCPA の適用がない。具体的には、以下の各要件をいずれも充足する場合に対象となる行為の全ての側面がカリフォルニア州外で行われているものとされる。

(a)消費者がカリフォルニア州外にいるときに事業者が個人情報を取得した
(b)カリフォルニア州で消費者の個人情報を販売する行為が一部でも行われていない
(c)消費者がカリフォルニア州にいたときの個人情報を販売していない

Q. 当社は日本国内に所在する株式会社であり、カリフォルニア州内には当社グループの拠点はありません。当社は取引先から消費者（カリフォルニア州の住民）の個人情報を収集していますが、全ての行為をカリフォルニア州の外で行っていますので、第 1798.145 条第(a)項(6)の CCPA の適用除外に関する規定が適用になり、当社には CCPA の適用はないと考えているのですが、正しいでしょうか。
A. 第 1798.145 条第(a)項(6)に CCPA の適用除外に関する規定があり、「対象となる行為の全ての側面がカリフォルニア州外で行われている」場合には CCPA の適用がないとされている。具体的には、以下の各要件をいずれも充足する場合に「対象となる行為の全ての側面がカリフォルニア州外で行われている」ものとされる。
(a)消費者がカリフォルニア州外にいるときに事業者が個人情報を取得した
(b)カリフォルニア州で消費者の個人情報を販売する行為が一部でも行われていない
(c)消費者がカリフォルニア州にいたときの個人情報を販売していない
日本本社による消費者（カリフォルニア州の住民）の個人情報の収集・販売がこの適用除外規定に該当するかは事案によるが、通常、日本本社が収集・販売する全ての消費者の個人情報について上記(c)の要件が充足されることは考えづらく、この適用除外規定によって消費者の個人情報を収集・販売する日本本社への CCPA の適用が否定されることはあまりないと考えられる。貴社の場合にも、上記各要件が充足されることを慎重に判断すべきであると考える。

2. 保証・リコールに関する修理のための自動車情報と所有者情報の適用除外（第 1798 条 145 条第(g)項）

第 1798.145 条

(g) 第 1798.120 条は、自動車情報や所有者情報が自動車法（Vehicle Code）第 426 条に定められた新しい自動車ディーラー、及び自動車法第 672 条に定められた自動車製造者によって保持又は共有される場合、自動車又は所有者情報が自動車保険の対象として車両修理を達成又は達成が予想されるために共有される場合、連邦規則集 49 巻第 30118 条から 30120 条により行われたリコールの場合には適用されない。ただし、新しい自動車ディーラー又は自動車製造者が他のいかなる目的のためにも自動車情報や所有者情報を販売、共有又は利用しない場合をいう。
(2) 本項の目的のため:
(a) 「自動車情報」とは、車両情報番号、メーカー名、型式、年式とオドメーター上の走行距離をいう。
(b) 「所有者情報」とは、登録された所有者又は複数所有者の氏名及び連絡先。

新しい自動車ディーラーあるいは自動車メーカーが、上記目的以外で自動車情報や所有者情報を販売、共有あるいは利用した場合は CCPA の適用除外規定は適用にならない。たとえば、自動車ディーラーが収集した所有者情報を、自動車メーカーがマーケティングの目的や研究開発目的で使用するために共有した場合、CCPA の適用除外にはならず、当該使用は CCPA 違反を問われうる。言い換えると、本適用除外規定は、自動車ディーラーや自動車メーカーが、CCPA の適用を受ける範囲を若干狭めたに過ぎない。すなわち、自動車ディーラーや自動車メーカーは本規定の存在に関わらず、CCPA へのコンプライアンス対応を行う必要がある。

3. 人事関連の個人情報の時限的な部分的適用除外（第 1798.145 条第(h)項）

第 1798.145 条第(h)項
(1) 本巻は、以下のいずれにも適用されない：
(a) 自然人が求職者、従業員、所有者、役員、オフィサー、医療スタッフメンバー又は請負人として事業者とやりとりする中で事業者によって収集された当該自然人に関する個人情報で、当該自然人が求職者、従業員、所有者、役員、オフィサー、医療スタッフ又は請負人としてもしくはかつてこれらの立場で事業者に関わる文脈に限定して収集かつ使用された範囲のもの。
(b) 自然人が求職者、従業員、所有者、役員、オフィサー、医療スタッフメンバー又は請負人として事業者とやりとりする中で事業者によって収集された当該自然人の緊急のコンタクト情報である個人情報で、ファイルについて緊急に連絡をとる文脈に限定して収集かつ使用された範囲のもの。
(c) 事業者が求職者、従業員、所有者、役員、オフィサー、医療スタッフメンバー又は請負人として事業者とやりとりする自然人に関連する他の自然人に対して特典を給付するために保持する必要がある個人情報で、これらの特典を給付する文脈に限定して収集かつ使用された範囲のもの。
(2) 本項の目的のために
(A)「請負人」とは、書面による契約によって事業者にサービスを提供する自然人をいう。
(B)「役員」とは、定款によって定められた自然人又は、他の名前もしくは役職で役員として行動するよう指定、選出若しくは任命された法人若しくは自然人によって選出された自然人及びその後継者をいう。
(C)「医療スタッフメンバー」とは、事業及び職業法（the Business and Professions Code）第 2 部（Division 2）（第 500 条から開始)による有資格の医師及び外科医、歯科医、足病医、安全衛生法(Health and Safety Code)第 1316.5 条に定められた臨床心理士をいう。
(D)「オフィサー」とは取締役会によって選出又は任命された自然人で、企業の日常業務を行う最高経営責任者、社長、秘書又は会計をいう。
(E)「所有者」とは、以下のいずれかに該当する自然人をいう。
(i) 事業者の議決権のある種類の株式について発行済み株式の 50%超を保有し又は議決権を有すること。

(ii) 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支配すること。
(iii)事業者の経営について支配的な影響を行使する権限があること。
(3)本項は第 1798.100 条第(b)項又は第 1798.150 条には適用されない。
(4)本項は 2021 年 1 月 1 日から効力を失う。

(1) 人事関連の個人情報の時限的な部分的適用除外（第 1798.145 条第(h)項）については、その範囲や期間が限定的であり、人事関連の消費者の個人情報の処理を行う事業者は CCPA へのコンプライアンス対応を執る必要がある。詳細は次の通りである。

(2) まず、上記第 1798.145 条第(h)項(1)(a)から(c)の人事関連の個人情報についても、収集時又は収集前における収集される個人情報のカテゴリー及びその個人情報のカテゴリーが使用される目的について消費者に通知する義務がある。また、個人情報の性質に照らして合理的なセキュリティの手続と慣行を実装する義務を怠った結果により、上記の消費者の個人情報が不正アクセス等された場合には以下の各救済措置がある。これらの義務はいずれも 2020 年 1 月 1 日から適用開始となる。

- 1 件（1 名、1 事故毎に算定）あたり、100 米ドル以上 750 米ドル以下の法定損害賠償又は実損のいずれか大きい額の賠償請求
  - この場合の「個人情報」の定義は狭い。すなわち、個人のファーストネーム若しくはファーストイニシャル及びラストネームと以下の情報の組み合わせに限られる。
    - ✓ ソーシャルセキュリティナンバー
    - ✓ 運転免許の番号
    - ✓ カリフォルニア州の ID の番号
    - ✓ 銀行口座番号
    - ✓ クレジットカード・デビットカード番号
    - ✓ 医療・健康保険の情報
    - ✓ 納税者番号
    - ✓ パスポート番号
    - ✓ 軍用識別番号
    - ✓ 政府の文書に付与された固有の識別番号
  - 法定損害賠償請求について、30 日の是正期間あり
  - 差止命令、確認判決、その他裁判所が適切と判断する救済措置

(3) 人事関連の個人情報であっても、上の下線部を付した以外のカテゴリーの個人情報を収集し使用する場合や上の下線部の目的以外に収集し使用する場合には、CCPA の適用除外はないため、CCPA 対応を取ることが必要である。少なくとも、以下の点を確保することが重要と考えられる。

a. データマッピングを行い、上の適用除外の枠外で、個人情報を収集・使用していないことを確認する。
b. 社内規則で上の適用除外の枠内でのみ個人情報を収集・使用することを義務付ける。
c. 上記社内規則に従い、従業員向けの CCPA トレーニングを行い上の適用除外を外れる個人情報の収集・使用を行わないことを確保する。

(4) 上記の CCPA 第 1798.100 条第(b)項による個人情報の収集時の消費者への通知は、プライバシーポリシーの一部を使用して行うことになると考えられる。したがって、収集される消費者の個人情報のカテゴリー毎に、個人情報が利用される事業目的又は商業目的を整理しておく必要がある。そのため、データマッピングを行うことは不可避である。

(5) 上記第 1798.145 条第(h)項の規定は 2021 年 1 月 1 日から効力を失うため、同日までに何らかの立法がなされない限り、上記の限度の適用除外の適用もなくなることを意味する。
(6) さらに、CCPA 第 1798.130 条は、過去 12 か月間の処理業務について消費者に開示することを事業者に義務付けているため、上記 1798.145 条第(h)項の規定の範囲内の処理業務についても、2021 年 1 月 1 日の適用開始に向けて、当該処理業務の目的や処理の対象となる個人情報のカテゴリー等に関してデータマッピングを行う必要がある。

Q.会社の役職員や求職者の個人情報も CCPA の適用対象でしょうか。CCPA 第 1798.100 条第(b)項の通知は必要でしょうか。
A. Assembly Bill 25 による改正により、CCPA 第 1798.145 条第(g)項の人事関連の個人情報の時限的な部分的適用除外が導入された。適用除外が時限的であり、かつ、部分的であることに注意が必要であるが、2021 年 1 月 1 日までの 1 年間に限り、役職員、求職者等の個人情報等、役職員の緊急連絡先情報、及び役職員の福利厚生のために必要な情報については、CCPA 第 1798.100 条第(b)項の個人情報の目的とカテゴリーに関する通知義務及び CCPA 第 1798.150 条の私人提訴権（合理的なセキュリティの手続と慣行を実装する義務を怠った結果により、個人情報が不正アクセス等された場合に限る）以外の規定の適用が除外される。

4. B to B の文脈での企業等の役職員等の個人情報に関する時限的な部分的適用除外（第 1798.145 条第(o)項）

第 1798.145 条第(n)項
（1）第 1798.100 条、第 1798.105 条、第 1798.110 条、第 1798.115 条、第 1798.130 条及び第 1798.135 条によって事業者に課された義務は、消費者が会社、パートナーシップ、個人事業体、非営利又は政府機関に対して従業員、所有者、役員、オフィサー又は請負人として活動する自然人であり、事業者との通信又は取引が、会社、パートナーシップ、個人事業体、非営利又は政府機関に関して事業者がデューディリジェンスを実施する、又は会社、パートナーシップ、個人事業体、非営利又は政府機関との商品やサービスの供給や受領の文脈に限って生じる際は、事業者と消費者間の書面又は口頭による通信又は取引を反映した個人情報には適用されない。
(2) 本項の目的のために
(a) 「請負人」とは、書面による契約により事業者にサービスを提供する自然人である。
(b) 「役員」とは、定款によって定められた自然人又は、他の名前もしくは役職で役員として行動するよう指定、選出若しくは任命された法人若しくは自然人によって選出された自然人及びその後継者をいう。
(c) 「オフィサー」とは取締役会によって選出又は任命された自然人で、企業の日常業務を行う最高経営責任者、社長、秘書又は会計をいう。
(d)「所有者」とは、以下のいずれかに該当する自然人をいう：
(i) 事業者の議決権のある種類の株式について発行済み株式の 50%超を保有し又は議決権を有すること。
(ii) 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。
(iii)事業者のマネジメントについて支配的な影響を行使する権限があること。
(3)本項は 2021 年 1 月 1 日から効力を失う。

(1) B to B の文脈での企業等の役職員等の個人情報の処理に関する時限的な部分的適用除外（第 1798.145 条第(n)項）については、その範囲や期間が限定的であり、B to B の文脈での企業等の役職員等である消費者の個人情報の処理を行う事業者は CCPA へのコンプライアンス対応を執る必要がある。詳細は次の通りである。

(2) 企業等の役職員等の個人情報については、事業者と企業等の役職員等の通信又は取引が、企業等のデューディリジェンス、企業等の商品又はサービスの提供／受領の文脈でのみ行われる限りにおいて、第 1798.100 条、第 1798.105 条、第 1798.110 条、第 1798.115 条、第 1798.130 条及び第 1798.135 条によって事業者に課された義務は適用されない。

なお、B to B の文脈で取得した企業等の役職員等の個人情報を当初の商品やサービスの供給や受領の文脈とは異なる文脈で使用・共有等を行う場合、例えば、B to B の文脈で取得した企業等の役職員等の個人情報をマーケティングの目的で使用する場合には、上記適用除外の適用はないものと考えられる。

(3) また、B to B の文脈で取得した企業等の役職員等の個人情報の処理の関係であっても、第 1798.120 条（販売のオプトアウトの権利)、第 1798.125 条（オプトアウトする消費者の差別禁止)、及び第 1798.150 条の私人提訴権（合理的なセキュリティの手続と慣行を実装する義務を怠った結果により、個人情報が不正アクセス等された場合に限る）の各条項に関しては、原則通り 2020 年 1 月 1 日から適用されるため、事業者はこれらの条項を遵守するためのコンプライアンス対応を早急に執る必要がある。

(4) 上記第 1798.145 条第(n)項の規定は 2021 年 1 月 1 日から効力を失うため、同日までに何らかの立法がなされない限り、上記の限度の適用除外の適用もなくなることを意味する。

(5) さらに、CCPA 第 1798.130 条は、過去 12 か月間の処理業務について消費者に開示することを事業者に義務付けているため、上記 1798.145 条第(n)項の規定の範囲内の処理業務についても、2021 年 1 月 1 日の適用開始に向けて、当該処理業務の目的や処理の対象となる個人情報のカテゴリー等に関してデータマッピングを行う必要がある。

Q. 会社の B to B の取引先の名刺情報（会社名、氏名、社用の連絡先等の情報のみ含まれるもの）も CCPA の適用対象でしょうか。B to B 間での電子メール・契約書・インボイスに記載されている担当者氏名はどうでしょうか。

A. Assembly Bill 1355 による改正により、1798.145 条第(n)項の B to B の個人情報の時限的な部分的適用除外が導入された。適用除外は時限的であり、かつ部分的であるに過ぎない。2021 年 1 月 1 日までの 1 年間に限り、企業等の役職員等の個人情報（名刺情報や B to B 間の電子メール・契約書・インボイスはこれに含まれると解される。）については、事業者と企業等の役職員等の通信又は取引が、企業等のデューディリジェンス、企業等の商品又はサービスの提供／受領の文脈でのみ行われる限りにおいて、第 1798.100 条、第 1798.105 条、第 1798.110 条、第 1798.115 条、第 1798.130 条及び第 1798.135 条によって事業者に課された義務は適用されない。

5. その他の適用除外規定

上記 1 から 4 以外のその他の適用除外規定は以下の通りである。

第 1798.145 条

(a)本巻により事業者に課される義務は、以下の事業者の権能を制限しない：

(1)連邦、州又は地域の法律を遵守すること。

(2)連邦、州又は地域の当局による民事、刑事、又は規制上の調査、捜査、罰則付き召喚令状、呼出状を遵守すること。

(3)事業者、サービス提供者又は第三者が、連邦、州又は地域の法律に違反しているかもしれないと合理的にまた誠実に信じる行為又は活動に関して法執行当局に協力すること。

(4)法的な主張を行い、又は弁護すること。

(5)非識別情報又は消費者情報集合体の形の消費者情報を収集し、使用し、保持し、販売し、又は開示すること。
(6)略
(b)第 1798.110 条から第 1798.135 条まで（第 1798.135 条を含む。）により事業者に課される義務は、事業者による本巻の遵守がカリフォルニア州の法律のもとでの証拠特権に違反する場合には適用されず、また、事業者が特権的通信の一部としてカリフォルニア州法のもとでの証拠特権の対象となる者に対し消費者の個人情報を提供することを妨げない。
(c)(1) 本巻は以下のいずれにも適用されない：
(A)医療情報機密法（第 1 編第 2.6 部（第 56 条から開始））で規律される医療情報、又は、1996 年医療保険の相互運用性及び説明責任に関する法律（公法 104-191）及び経済的及び臨床的健全性のための医療情報技術に関する法律（公法 111-5）により設けられた連邦規則集第 45 巻第 160 部及び第 164 部、連邦保険福祉省の発したプライバシー、セキュリティ及び違反通知に関するルールにより規律される対象の主体又は事業者関係者によって収集された保護される医療情報。
(B)以下の機関が、本条(a)に述べるように医療情報又は保護される健康情報と同様の方法で患者情報を保持する範囲。医療情報機密法（第 1 編第 2.6 部（第 56 条から開始））で規律されるヘルスケアの提供者、又は 1996 年医療保険の相互運用性と説明責任に関する法律（公法律 104-191）により成立した連邦規則集第 45 巻第 160 部及び第 164 部、連邦保険福祉省の発するプライバシー、セキュリティ及び違反通知に関するルールにより規律される対象の主体。
(C)医薬品規制調和国際会議の発行した臨床のグッド･プラクティス・ガイドライン又は米国連邦食品医薬品局の被験者の保護要件により、コモンルールと呼ばれる被験者の保護に関する連邦政府の政策による臨床試験の一部として収集された情報。
(2)本項の目的のため、第 56.05 条における「医療情報」及び「ヘルスケア提供者」の定義が適用され、また連邦規則集第 45 部第 160.103 条の「事業関係者」、「対象の主体」及び「保護される健康情報」の定義が適用される。
(d) (1) 本巻は、連邦規則第 15 巻第 1681a 条第(f)項に定める消費者レポート機関、連邦規則第 15 巻第 1681a 条第(d)項に定める消費者レポートに使用するための情報を提供する連邦規則第 15 巻第 1681s-2 条に定める情報提供者、又は連邦規則第 15 巻第 1681b 条に定める消費者レポートの利用者による消費者の信用価値、信用状態、与信能力、性格、一般的な評判、個人的な特徴又は生活様式に触れる個人情報の収集、維持、開示、販売、通信、又は使用に関する行為には適用されない。
(2) (1)は、公正信用報告法、連邦規則第 15 巻第 1681 条 et seq.による規制の対象である当該機関、提供者又は利用者による個人情報の収集、維持、開示、販売、通信又は利用に関する行為で、公正信用報告法により与えられた権限を超えて個人情報が利用、通信、開示、販売されない場合のみ適用される。
(3) 本項は、第 1798.50 条には適用されない。
(e)本巻は、連邦のグラム・リーチ・ブライリー法（公法 106-102）及び実施規則、又はカリフォルニア州金融情報プライバシー法（金融法第 1.4 編（第 4050 条から開始））により収集され、処理され、販売され又は開示される個人情報には適用されない。本項は第 1798.150 条には適用されない。
(f)本巻は、1994 年ドライバー･プライバシー保護法（18 U.S.C. Sec. 2721 et seq.）により収集され、処理され、販売され又は開示される個人情報には適用されない。本項は第 1798.150 条には適用されない。
(g) 略
(h) 略

(i)本巻により消費者の権利要求に対応し履行する事業者の義務にかかわらず：
(1)検証された消費者要求に事業者が対応する期間は、要求の複雑性及び数を考慮して、必要な場合、90 日までの追加の日数を延長することができる。事業者は、要求の受領から 45 日以内に、遅延の理由と共に、当該延長について消費者に通知する。
(2)事業者が消費者の要求に対して行動しない場合、その事業者は、遅滞なく本条により認められる対応期間内に、行動しない理由及び消費者が事業者に対してその判断について不服申し立てできる権利について消費者に通知する。
(3)消費者からの要求が明らかに根拠がなく又は特に繰り返しの性格であるために過度なものである場合、事業者は、情報提供若しくは通信の管理費用又は要求された行動を考慮して妥当な手数料を課すか、又は要求に対する行動を拒否しその要求拒否の理由を消費者に通知するか、いずれかを行うことができる。事業者は、検証された消費者要求が明白に根拠のない又は過度のものであることを証明する負担を有する。
(j)サービス提供者に個人情報を開示する事業者は、個人情報を受け取るサービス提供者が本巻に定める制限に違反してその情報を使用している場合、その個人情報を開示するときにサービス提供者が違反を行う意図であったことについて実際に知らず又はそう信じるべき理由を持たないとき、本巻のもとに責任を問われない。サービス提供者は、サービスを提供する事業者の義務について、同様に、本巻に定めるように本巻のもとに責任を問われない。
(k)本巻は、事業者に対し、通常の業務において収集しないであろう個人情報を収集したり、個人情報を通常の業務において保持するであろう期間より長期間保持したり、個人情報と見なされる方法で保持されていない情報について再識別又はその他情報をリンクさせるように求めていると解釈してはならない。
(l)本巻において消費者に付与される権利と事業者に課される義務は、他の消費者の権利及び自由に悪影響を与えない。
(m)本巻のもとで消費者に付与される権利及び事業者に課される義務は、それがカリフォルニア州憲法第 I 章第 2 条(b)に述べる者又は主体の非商業的行為と抵触する範囲では、適用されない。
(n)略

Q. Attorney-Client Privilege のような秘匿特権対象となる情報については、アクセス権行使又は削除要求において例外措置があるでしょうか。ある場合には、それを消費者に通知せずに例外扱いとしてよいでしょうか。
A. 第 1798.145 条第(b)項によれば、第 1798.110 条から第 1798.135 条まで（第 1798.135 条を含む。）により事業者に課される義務は、事業者による本巻の遵守がカリフォルニア州の法律のもとでの証拠特権に違反する場合には適用されず、また、事業者が特権的通信の一部としてカリフォルニア州法のもとでの証拠特権の対象となる者に対し消費者の個人情報を提供することを妨げないとされている。しかしながら、アクセス権行使及び削除の要求は、適用除外の範囲に含まれないと考えられる。したがって、それを消費者に通知せずに例外扱いとすることには問題があると考えられる。

第5　消費者の8つのプライバシー権

CCPA上の消費者の権利の整理の仕方は複数ありうるが、一つの整理の仕方として保障されている8つのプライバシーの権利に基づいて整理することが考えられる。以下の表において用語の対応関係とともに各権利の概要を示す。

	8つのプライバシーの権利	CCPA規則案における説明
1	略式開示請求権（第1798.100条第(a)項）個人情報を収集する事業者に対して、事業者が収集した個人情報のカテゴリー及び特定の部分を自身に対して開示するように求める権利	収集、開示及び販売される個人情報について知る権利（**知る要求**）
2	拡張開示請求権（第1798.110条第(a)項・第(b)項） 個人情報を販売し又は事業目的のために開示する事業者に対して、収集した個人情報のカテゴリー及び特定の部分、個人情報が収集された情報源のカテゴリー、個人情報を収集する事業目的又は商業目的、個人情報を共有する第三者のカテゴリーを自身に開示するように要求する権利	
3	アクセス及びポータビリティの権利（第1798.100条第(d)項） 消費者が以下の消費者の個人情報へアクセスする権利。 (1)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ー (2)個人情報が収集された情報源のカテゴリー (3)個人情報を収集し又は販売する事業目的又は商業目的 (4)事業者が個人情報を共有する第三者のカテゴリー (5)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 消費者から個人情報へのアクセスについて検証可能な消費者要求を受領する事業者は、本条により求められる個人情報を、その消費者に対して無償で速やかに開示又は送付する措置をとる。情報は郵便で又は電子的に送付することができ、電子的に提供される場合その情報はポータブルであるものとし、技術的に可能な範囲で当該消費者がその情報を障害なしに他の法的主体に送信できる容易に利用可能なフォーマットとする。事業者は、いつ消費者に個人情報を提供してもよいが、12ヶ月間に2回を超えて消費者に対して個人情報を提供することは求められない。	
4	事業目的[4]で個人情報の販売（消費者の個人情報を、金銭又はその他の価値のある約因（valuable consideration）を対価として、その事業者から他の事業者又は第三者に対	

[4] 事業目的で開示しない場合
「事業目的」とは、事業者又はサービス提供者の経営上の目的又はその他の通知された目的のための個人情報の使用を意味する。ただし、当該使用が、個人情報が収集され若しくは処理される経営上の目的、又は個人情報が収集された文脈と適合するその他の経営上の目的を実現するために合理的に必要であり、かつ、比例的である場合をいう。事業目的とは、以下である。
(1)消費者との進行中のやりとり及び並行した取引に関する監査。これには、一意の訪問者に対する広告表示回数の計測、広告表示の位置と質の検証、並びにこの仕様及び他の基準への遵守の監査が含まれるが、これらに限定されない。
(2)セキュリティ上の事故の探知、悪意、偽装、詐欺又は違法行為からの保護、及びその行為に責任を有する者の訴追。
(3)既存の意図された機能を損なうエラーを特定及び修復するためのデバッグ。
(4)短期の一時的な使用。ただし、個人情報が第三者に開示されず、かつ、消費者についてのプロファイル作成又はその時のやりとり以外における個々の消費者の経験のその他の改変（同じやりとりの一部として示される文脈上の広告のカスタマイズを含むがこれに限られない。）に使用されない場合をいう。
(5)事業者又はサービス提供者の代わりのサービスの実施。これには、事業者若しくはサービス提供者のためのアカウントの維持若しくは提供、カスタマー・サービスの提供、注文及び取引の処理若しくは履行、顧客情報の検証、支払いの処理、ファイナンシ

	して、販売、貸借、公表、開示、流布、提供、移転又は口頭、書面、又は電子その他の手段により伝達すること）又は開示を行う事業者に対する情報請求権（第 1798.115 条第(a)項・第(b)項） 収集し販売した個人情報のカテゴリー、データが販売された第三者のカテゴリー、事業目的で消費者について開示された個人情報のカテゴリーのうち過去 12 ヶ月間のものを自身に開示するように要求する権利	
5	削除権（第 1798.105 条第(a)項・第(c)項）[5] 事業者が消費者の個人情報を削除することを要求する権利	個人情報の削除を要求する権利（**削除の要求**）
6	個人情報の販売に関するオプトアウト権（第 1798.120 条第(a)項） 消費者又は消費者の権限のある代理人が事業者に対して、当該消費者の個人情報を第三者に対して販売することを止めるように命令する力を与える権利	個人情報の販売を**オプトアウトする権利**
7	子供のためのオプトインの権利：積極的な授権なしに子供の個人情報を販売しない事業者の義務（第 1798.120 条第(c)項） 事業者が子供（13 歳から 16 歳の間）又は子供の親権者又は監護者（13 歳以下の子供の場合）から当該子供の個人情報を販売する前にオプトイン同意を取得しなければならない	未成年者の個人情報の売却に関するオプトインの手続
8	CCPA 上の消費者の権利の行使を理由として差別されない権利（第 1798.125 条第(a)項） 事業者は、消費者が CCPA に関して消費者の権利を行使したことを理由として消費者を差別しない（第 1798.125 条第(a)項）（以下を含むがこれに限られない。） 。 ▪ 消費者に対する商品又はサービスの提供の拒否。 ▪ ディスカウント若しくはその他の特典の使用、又はペナルティを課すことを含め、商品又はサービスに異なった価格又は料金を請求すること。	消費者プライバシー権を行使する場合に差別をされない権利

ングの提供、広告若しくはマーケティング･サービスの提供、解析サービスの提供、又は類似サービスの提供を含む。
(6)技術開発及びデモンストレーションについての内部的研究を行うこと。
(7)事業者により所有され、製造され、事業者のために製造され、又は事業者によりコントロールされる、サービス又はデバイスの品質又は安全性を検証若しくは維持し、また、事業者により所有され、製造され、事業者のために製造され、又は事業者により制御されるサービス又はデバイスを改善、アップグレード又は向上するための活動を行うこと。

[5] 削除の要求に応じる必要がない場合
事業者又はサービス提供者が、以下の目的のために、消費者の個人情報を保持する必要がある場合、その事業者又はサービス提供者は、消費者の削除の要求に従うことは求められない（第 1798.105 条第(d)項）。
(1)個人情報が収集された取引を完了するため、連邦法に従って履行された書面による保証の条件又は商品リコール、消費者との継続的なビジネス関係の文脈のなかで合理的に予想される消費者の求める商品若しくはサービスを提供するため、又は、それ以外に事業者と消費者の間の契約を履行するため。
(2)セキュリティ事故を探知するため、悪意、詐欺、偽装若しくは違法な行為から保護するため、又はこれらの行為に責任を有する者を訴追するため。
(3)既存の意図された機能を妨げるエラーを特定し修正して修復するため。
(4)自由な言論を行使するため、自由な言論の権利を行使する他の消費者の権利を確保するため、又は法律に定める他の権利を行使するため。
(5)刑法第 2 部第 12 巻第 3.6 章（第 1546 条から開始）によるカリフォルニア電子通信プライバシー法を遵守するため。
(6)全ての他の適用可能な倫理及びプライバシー法が遵守された、公共の利益に資する公的な、又は査読される科学、歴史又は統計上の研究に従事するためであり、事業者による個人情報の削除が当該研究の実現を不可能にし、又はそれを著しく損なう可能性があるときであり、かつ消費者のインフォームド・コンセントがある場合。
(7)消費者と事業者の関係に基づき、消費者の期待と合理的に適合した事業者の内部での使用のみを可能とするため。
(8)法的義務を遵守するため。
(9)そのほか、消費者が情報を提供した目的と適合する適法な方法で、消費者の個人情報を事業者内部で使用するため。

	▪ その消費者に対して異なったレベル又は質の商品又はサービスを提供すること。 ▪ 異なる価格若しくは料金、又はレベル若しくは質の商品又はサービスを消費者が受領することを示唆すること。 本項は、提供される商品又はサービスの価格又はレベルの違いが消費者のデータにより事業者に提供される価値に合理的に関連している場合に、事業者が消費者に異なる価格又は料金を請求すること、又は消費者に異なるレベル又は質の商品又はサービスを提供することを禁止するものではない。	

第6　事業者の義務

1. 事業者の義務－総論

CCPA上の事業者の義務を纏めると以下の通りである。

(1) 消費者への通知義務（CCPA規則案第2節）
(2) 消費者要求への対応のビジネスプラクティスに関する義務（CCPA規則案第3節）
(3) 研修義務（CCPA規則案第999.317条）
(4) 記録管理義務（CCPA規則案第999.317条）
(5) 要求の検証義務（CCPA規則案第4節）
(6) 未成年者に関する特則の義務（CCPA規則案第5節）
(7) 差別の禁止（CCPA規則案第6節）
(8) 個人情報の性質に照らして合理的なセキュリティの手続と慣行を実装する義務（CCPA第1798.150条）

上記の事業者の義務については、CCPA規則案が詳細にその内容を定めている。CCPA規則案について特に注意が必要なのは、カリフォルニア州の司法長官が第999.300条第(b)項において「本規則に違反した場合はCCPA違反に該当し、当該法に規定する是正措置の対象となる。」と定め、CCPA規則案への違反がCCPAの違反であるとみなす立場を明らかにしていることである。CCPA規則案には、CCPAの遵守に必要な社内のシステム・態勢整備の要件が細かく規定されている。本規則違反がCCPA違反とみなされてしまうため、本規則案を注意深くチェックしながら準備を進める必要がある。

特に、上記(1)の消費者への通知義務との関係では、事業者が、オンライン・プライバシーポリシーを有している場合にはそのオンライン・プライバシーポリシー、消費者プライバシー権についてのカリフォルニア固有の記述においてプライバシーポリシーを持たない場合にはその事業者のインターネット・ウェブサイトにおいて、一定の情報を開示し、少なくとも12 ヶ月に1回その情報をアップデートしなければならない（CCPA第1798.130条第(a)項（(5)）という継続的な開示義務があることが重要である。すなわち、2020年1月1日以降、CCPAに対応したプライバシーポリシーを自社・自組織のウェブサイトに掲げていないことは、インターネット上の検索エンジンを使って誰でも容易にチェックすることができるため、CCPAに違反した状態にあることが明るみにでるきっかけとなることが懸念される。したがって、外部から見えやすい部分に関連するCCPA対応は優先的に進めることが望ましいと考えられる。

CCPA規則案の目次は次の通りである。

〈CCPA規則案の目次〉

節	条
第1節　総則	第999.300条　名称及び適用範囲 第999.301条　定義
第2節　消費者への通知	第999.305条　個人情報の収集時における通知 第999.306条　個人情報の販売からのオプトアウトの権利の通知 第999.307条　金銭的なインセンティブの通知 第999.308条　プライバシーポリシー
第3節　消費者要求への対応のビジネスプラクティス	第999.312条　知る要求と削除の要求の提出方法 第999.313条　知る要求及び削除の要求への対応 第999.314条　サービス提供者 第999.315条　オプトアウトの要求 第999.316条　個人情報の販売をオプトアウトした後にオプトインする要求

	第 999.317 条　研修、記録管理 第 999.318 条　世帯の個人情報へのアクセス又は削除の要求
第 4 節　要求の検証	第 999.323 条　検証に関する一般原則 第 999.324 条　パスワードで保護されたアカウントの検証 第 999.325 条　非アカウント保有者の検証 第 999.326 条　授権されたエージェント
第 5 節　未成年者に関する特則	第 999.330 条　13 歳未満の未成年者 第 999.331 条　13 歳から 16 歳までの未成年者 第 999.332 条　16 歳未満の未成年者
第 6 節　差別の禁止	第 999.336 条　差別的プラクティス 第 999.337 条　消費者データの価値の算定
第 7 節　可分性	第 999.341 条

2. 事業者の義務－各論

(1) 消費者への通知義務（CCPA 規則案第 2 節）

以下の条文において次の種類の通知のデザイン、内容及び方法等の具体的な要件を定めている。各通知の定義は以下の通りである。

条文・通知の種類	定義	目的
第 999.305 条　個人情報の収集時における通知	CCPA 第 1798.100 条第(b)項によって求められ、本規則によって定められる、事業者が個人情報を消費者から収集する際あるいは収集する前に行う事業者から消費者への通知をいう（第 999.301 条第(i)項)。	収集される個人情報のカテゴリー並びに当該個人情報のカテゴリーが利用される目的について、消費者の個人情報を収集する際あるいは収集する前に消費者に知らせること
第 999.306 条　個人情報の販売からのオプトアウトの権利の通知	CCPA 第 1798.120 条並びに第 1798.135 条及び本規則に定める、個人情報の販売からオプトアウトする権利について事業者が消費者に与える通知をいう（第 999.301 条第(j)項)。	消費者に当該消費者の個人情報を販売する（若しくは将来販売する）事業者に、個人情報の販売を中止する若しくは将来に販売を控えるよう指示する権利について通知すること
第 999.307 条　金銭的なインセンティブの通知	CCPA 第 1798.125 条第(b)項及び本規則に定める事業者が与える通知で、CCPA 第 1798.125 条第(b)項の対象となる各金銭的なインセンティブ又は価格又はサービスの差異の説明をいう（第 999.301 条第(k)項)。「金銭的なインセンティブ」には、プログラム、特典若しくは他の提供物をいい、個人情報の開示、削除若しくは販売に対する補償としての消費者への支払いを含む（第 999.301 条第(g)項)。	消費者の個人情報の保持又は販売について消費者に事業者が提供する各金銭的なインセンティブ又は価格又はサービスの差異を説明することで、それによって消費者が知識を持った上で関与を決定できること
第 999.308 条　プライバシーポリシー	CCPA 第 1798.130 条第(a)項(5)におけるポリシーをいい、個人情報の収集、利用、開示並びに販売及び自己の個人情報に関する消費者の権利に関わる事業者のプラクティスの記述をオンラインでもオフラインでも消費者が利用できるようにするという内容のステートメントをいう（第 999.301 条第(m)項)。	個人情報の収集、利用、開示並びに販売及び消費者の個人情報に関する権利にかかる事業者のオンライン及びオフラインのプラクティスの包括的な記述を消費者に提供すること。プライバシーポリシーは、個々の消費者の個人情報の特定の部分を含めてはならず、消費者ごとに個人化しなくてよい。

各通知義務との関係では、CCPA 規則において以下のような諸義務が定められている。

条文・通知の種類	各通知との関係での諸義務
第 999.305 条　個人情報の収集時における通知	収集時における通知において開示されている以外の目的での利用の禁止 事業者は、消費者の個人情報を、収集時における通知において開示されている以外の目的に利用してはならない。事業者が消費者の個人情報を収集時における通知に

	おいて既に開示されていない目的への利用を意図する場合は、事業者は新しい利用法について消費者に直接的に通知し、新しい目的による利用について消費者から明示的な同意を得なければならない（CCPA 規則案第 999.305 条第(a)項(3)）。 事業者は、収集時における通知において開示されている以外の個人情報の追加カテゴリーを収集してはならない。事業者が個人情報の追加カテゴリーの収集を意図する場合は、事業者は新しい収集時における通知を提供する（CCPA 規則案第 999.305 条第(a)項(4)）。 事業者が消費者に個人情報を消費者から収集する際、又は収集する前に収集時における通知を与えない場合は、事業者は消費者から個人情報を収集してはならない（CCPA 規則案第 999.305 条第(a)項(5)）。
第 999.306 条　個人情報の販売からのオプトアウトの権利の通知	消費者から直接的に情報を収集しない事業者が消費者の個人情報を販売する場合の義務 消費者から直接的に情報を収集しない事業者は、消費者に収集時における通知の提供を必要としないが、消費者の個人情報を販売する前に、以下のいずれかをする（CCPA 規則案第 999.305 条第(d)項）。 (1) 消費者に直接的にコンタクトを取り、事業者が消費者に関する個人情報を販売すると消費者に通知し、かつ第 999.306 条に従いオプトアウトの権利の通知を消費者に提供する、又は (2)以下のために個人情報の情報源にコンタクトを取る。 a.第(a)項及び第(b)項に従い情報源が消費者に収集時における通知を提供したと確認し、かつ b.情報源がいかなる方法で収集時における通知を与えたのか及び通知の例について記述してある署名付きの証明を情報源から取得する。証明は事業者によって少なくとも 2 年は保持され、消費者からの要求に応じて利用できるようにされなければならない。 個人情報の販売に関するオプトアウトの権利の通知義務の例外（CCPA 規則案第 999.306 条第(d)項） (1)オプトアウトの権利の通知が設置されていない期間に収集された個人情報を販売せず、又は販売しない、及び(2)個人情報を販売していない又は将来販売しないとプライバシーポリシーにて言及する。オプトアウトの権利の通知が設置されていない期間に個人情報が収集された消費者は、オプトアウトの要求を有効に提出したものとみなす。
第 999.307 条　金銭的なインセンティブの通知	事業者は、個人情報の収集、個人情報の販売又は個人情報の削除について、金銭の支払いを含む金銭的なインセンティブを補償として消費者に対して提供することができる。事業者は、価格又は差異が消費者のデータに基づき事業者に提供される価値と直接的に関連している場合、消費者に対して商品又はサービスの異なる価格、料金、レベル又は品質を提供することもできる(CCPA 第 1798.125 条第(b)項(1))。
第 999.308 条　プライバシーポリシー	事業者が、オンライン・プライバシーポリシーを有している場合にはそのオンライン・プライバシーポリシー、消費者プライバシー権についてのカリフォルニア固有の記述においてプライバシーポリシーを持たない場合にはその事業者のインターネ

	ット・ウェブサイトにおいて、一定の情報を開示し、少なくとも 12 ヶ月に 1 回その情報をアップデートしなければならない（CCPA 第 1798.130 条第(a)項（5））。

Q.個人情報の「売却」を行っていない場合には、オプトアウトページは不要という理解でいいのでしょうか。
A.御理解の通りである。CCPA 第 1798.120 条、第 1798.135 条第(a)項は、個人情報の「販売」についてのオプトアウト手続を定めており、「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らないものとしている。
ただし、「販売」の定義は、広範であり、第 1798.140 条第（t）項により、例外要件を充足しない限り、「金銭又はその他の価値のある対価のために、事業者が他の事業者又は第三者に対して、消費者の個人情報を、販売し､賃貸し、公表し、開示し、広め、利用可能にさせ、移転し、又は、その他口頭で、書面で、電子的若しくはその他の方法により伝えることを意味する」とされているため、注意が必要である。たとえば、提携先に金銭のやり取りなく情報を開示する場合はこの要件を充足すると考えられる。

そして、各通知のデザイン、通知の内容及び通知の方法については、CCPA 規則が詳細な定めを規定しており、事業者はこれらの定めに従って、各通知義務を遵守する必要がある。

a. 通知のデザイン

各通知のデザインの要件の共通点と相違点は以下の通りである。GDPR と比較して CCPA において特徴的なのは共通点の d として「障害を持つ利用者がアクセスできる。少なくとも、障害を持つ消費者がどのように他のフォーマットで通知にアクセスできるかという情報を提供する。」ことが要求されていることが挙げられる。その他のデザインの相違点は以下の通りである。

条文・通知	デザインの要件の共通点	デザインの要件の相違点
第 999.305 条　個人情報の収集時における通知	平均的な消費者が読みやすく理解しやすい方法でデザイン及び提示されなければならない。通知は、 a.平易で明快な言葉を使用し、専門用語や法律用語は避ける。 b.消費者の注意を通知に引寄せかつ読みやすいフォーマットを使用する。小さい画面上の場合も同様とする。 c.事業者が通常の業務において消費者に契約、ディスクレーマー、販売広告及び	e. 個人情報の収集が行われる前に、消費者の目に入る場所に見える又はアクセス可能である。例えば、事業者がオンラインで消費者の個人情報を収集する場合には、事業者のウェブサイト・ホームページ又はモバイル・アプリケーションのダウンロードページ、若しくは個人情報が収集される全てのウェブページに通知への明示的なリンクを設置する。事業者が消費者の個人情報をオフラインで収集する場合には、個人情報が収集される印刷物に通知を含める、又は消費者に印刷版の通知を提供する、若しくは消費者を通知が掲載されているウェブページへ案内する目立ったサイネージを設置する。
第 999.306 条　個人情報の販売からのオプトアウトの権利の通知		なし

第 999.307 条　金銭的なインセンティブの通知	他の情報を提供する言語で利用できる。 d. 障害を持つ利用者がアクセスできる。最低でも、障害を持つ消費者がどのように他のフォーマットで通知にアクセスできるかという情報を提供する。	e. 消費者が金銭的なインセンティブ若しくは価格又はサービスの差異[6]にオプトインする前に目にするよう、オンライン又は他の物理的な場所で利用できる。
第 999.308 条 プライバシーポリシー		e.消費者が区分された文書としてプリントアウトするように追加のフォーマットの形で利用できる。

b. 通知の内容

CCPA 規則においては、各通知において含めなければならない通知の内容について以下の通り詳細な定めを置いている。事業者は、CCPA 規則に規定された通知の内容に従って、各通知を行う必要がある。特に、プライバシーポリシーの内容に関する定めは、掲載すべき多くの情報の項目を順序立てて説明したものとなっており、事業者が CCPA に対応したプライバシーポリシーを準備するうえで、是非とも参照すべきものである。

通知の種類	通知の内容
第 999.305 条　個人情報の収集時における通知	(1)収集される消費者の個人情報のカテゴリー・リスト。各個人情報のカテゴリーは、収集される情報についての有意義な理解を消費者にもたらすような方法で記載されなければならない。 (2)個人情報のカテゴリー毎に、個人情報が利用される事業目的又は商業目的。 (3)事業者が個人情報を販売する場合、第 999.315 条第(a)項により求められる「私の個人情報を販売しない(“Do Not Sell My Personal Information”)」又は「私の情報を販売しない(“Do Not Sell My Info”)」と題したリンク、若しくはオフラインの通知の場合はリンク先のウェブページのウェブアドレス。 (4)事業者のプライバシーポリシーへのリンク、又はオフライン通知の場合は事業者のプライバシーポリシーのウェブアドレス。
第 999.306 条　個人情報の販売からのオプトアウトの権利の通知	(c)事業者は、以下をオプトアウトの権利の通知に含めなければならない。 (1)事業者による個人情報の販売をオプトアウトする消費者の権利に関する記述、 (2)第 999.315 条第(a)項により求められる、消費者がオプトアウトの要求[7]をオンラインで提出することができるウェブフォーム、又は事業者がウェブサイトを運営しない場合は、消費者がオプトアウトの要求を提出することができるオフラインの方法、 (3)消費者がオプトアウトの要求を提出することができる他の方法に関する指示、 (4)消費者がオプトアウトの権利を行使するために授権されたエージェントを使用する場合に求められる証拠、又は、通知を含む印刷物の場合は消費者が授権されたエージェントに関する情報を見つけることができるウェブページ、オンラインのロケーション若しくは URL、及び (5)URL 又は事業者のプライバシーポリシーへのリンク、又は、通知を含む印刷物の場合は消費者がプライバシーポリシーにアクセスできる URL 若しくはウェブページ。

[6] 「価格又はサービスの差異」とは：(1)商品又はサービスについて消費者に課された価格又は料金の差異で、割引、支払金、あるいは他の特典やペナルティの利用を通じて生じるものを含む、又は(2)消費者に提供された商品又はサービスのレベル又は質の差異で、消費者への商品又はサービスの提供の拒否を含む（第 999.301 条(l)号）。

[7] 「オプトアウトの要求」とは、CCPA 第 1798.120 条第(a)項により事業者が消費者の個人情報を第三者に販売しないよう求める消費者要求をいう（第 999.301 条第（p）項)。

第 999.307 条　金銭的なインセンティブの通知	(b)事業者は、以下を金銭的なインセンティブの通知に含めなければならない。 (1)提供される金銭的なインセンティブ若しくは価格又はサービスの差異の簡潔な概要、 (2)金銭的なインセンティブ若しくは価格又はサービスの差異の重要な条件の記述で、金銭的なインセンティブ若しくは価格又はサービスの差異に関わる個人情報のカテゴリーを含む、 (3)消費者がどのように金銭的なインセンティブ若しくは価格又はサービスの差異にオプトインできるか、 (4)金銭的なインセンティブからいつでも同意を撤回できる権利及び消費者がどのようにその権利を行使することができるかにかかる通知、及び (5)なぜ金銭的なインセンティブ若しくは価格又はサービスの差異が CCPA のもとで許可されているのかについての説明で、以下を含む。 a.金銭的なインセンティブ若しくは価格又はサービスの差異を提供する基礎となる消費者のデータの価値の公正な評価額、及び b.事業者が消費者のデータの価値を算定するために使用した方法の記述。 (3)及び(4)では消費者が当該インセンティブに対するオプトイン又は同意を行う方法及び消費者が同意を撤回できることを記載しなければならない。こうした記載の要求は消費者取引における基本的な公正さと一致するものとされている。
第 999.308 条 プライバシーポリシー	(b)プライバシーポリシーは以下の情報を含めなければならない。 (1)収集、開示及び販売される個人情報について知る権利 a.消費者が、事業者が収集、利用、開示及び販売する個人情報を開示するよう要求する権利を有すると説明する。 b.検証可能な消費者の知る要求を提出するための指示を提供し、要求をするためのオンラインの要求フォーム又はポータルが事業者によって提供されている場合はそのリンク先。 c. 消費者が提出しなければならない情報を含め、消費者要求を検証するために事業者が使用するプロセスを記述する。 d.個人情報の収集 1.事業者が消費者について過去 12 ヶ月間に収集した消費者の個人情報のカテゴリーをリストしたもの。通知は、収集される情報についての有意義な理解を消費者にもたらすような方法で記載されなければならない。 2.収集された個人情報の各カテゴリーについて、情報が収集された情報源のカテゴリー[8]、情報収集の事業目的若しくは商業目的、及び事業者が個人情報を共有する第三者のカテゴリー[9]を提供する。通知は、収集される情報についての有意義な理解を消費者にもたらすような方法で記載されなければならない。 e.個人情報の開示又は販売 1.過去 12 ヶ月間に、事業者が事業目的又は商業目的のために個人情報を第三者に開示又は販売したかに言及する。

[8] 「情報源のカテゴリー」とは、事業者が消費者に関する個人情報を収集する対象となる主体の種類で、消費者本人、公的記録の取得元となる政府機関並びに消費者データ再販業者を含むがこれらに限定されない（第 999.301 条第(d)号）。

[9] 「第三者のカテゴリー」とは、個人情報を消費者から直接的に収集しない主体の種類をいい、広告ネットワーク、インターネットサービス提供者、データアナリティクスプロバイダー、政府機関、オペレーティングシステム及びプラットフォーム、ソーシャルネットワーク並びに消費者データ再販業者を含むがこれらに限定されない（第 999.301 条第(e)号）。

	2.過去 12 ヶ月間に、事業者が事業目的又は商業目的のために第三者に開示又は販売した個人情報がある場合、個人情報のカテゴリーをリストする。 3.事業者が、積極的な許諾を得ずに 16 歳未満の未成年者の個人情報を販売するかどうかに言及する。 (2)個人情報の削除を要求する権利 a. 消費者は事業者が収集又は保持している個人情報の削除を要求する権利を有していると説明する。 b. 検証可能な消費者の削除の要求を提出するための指示又は要求をするためのオンラインの要求フォーム又はポータルが事業者によって提供されている場合はそのリンク先を提供する。 c. 消費者が提出しなければならない情報を含め、消費者要求を検証するために事業者が使用するプロセスを記述する。 (3)個人情報の販売をオプトアウトする権利 a. 消費者は事業者による個人情報の販売をオプトアウトする権利を有していると説明する。 b. 第 999.306 条に従いオプトアウトの権利の通知内容又はそれへのリンクを含める。 (4) 消費者プライバシー権を行使する場合に差別をされない権利 a.消費者は、CCPA により与えられたプライバシー権を行使するにあたって事業者から差別的な待遇を受けない権利を有すると説明する。 (5) 授権されたエージェント a.消費者が自己に代わって CCPA のもとに要求を行うために授権されたエージェントをどのように指定できるかを説明する。 (6) 詳細についての問い合わせ：消費者が又は事業者のプライバシーポリシーやプラクティスについての質問や懸念を連絡するための連絡先で、事業者が消費者との主なやりとりに使用する方法を反映させた方法を使用する。 (7) プライバシーポリシーが最後に更新された日付を記す。 (8) 第 999.317 条第(g)項の要件の対象となる場合は、第 999.317 条第(g)項(1)により集められた情報又は情報へのリンク先。

Q.プライバシーポリシーにはどんな項目を記載する必要がありますか。
A.CCPA 規則案 998.308 条第(b)項がプライバシーポリシーに記載すべき項目を以下のとおり定めている。
(b)プライバシーポリシーは、以下の情報を含む。
(1)収集、開示及び販売される個人情報について知る権利
a.消費者が、事業者が収集、利用、開示及び販売する個人情報を開示するよう要求する権利を有すると説明する。
b.検証可能な消費者の知る要求を提出するための指示を提供し、要求をするためのオンラインの要求フォーム又はポータルが事業者によって提供されている場合はそのリンク先。
c.消費者が提出しなければならない情報を含め、消費者要求を検証するために事業者が使用するプロセスを記述する。
d.個人情報の収集
1.事業者が消費者について過去 12 ヶ月間に収集した消費者の個人情報のカテゴリー。通知は、収集される情報についての有意義な理解を消費者にもたらすような方法で記載されなければならない。

2.収集された個人情報の各カテゴリーについて、情報が収集された情報源のカテゴリー、情報収集の事業目的若しくは商業目的、及び事業者が個人情報を共有する第三者のカテゴリーを提供する。
e.個人情報の開示又は販売
1.過去12ヶ月間に、事業者が事業目的又は商業目的のために個人情報を第三者に開示又は販売したかに言及する。
2.過去12ヶ月間に、事業者が事業目的又は商業目的のために第三者に開示又は販売した個人情報がある場合、個人情報のカテゴリーをリストする。
3.事業者が、積極的な許諾を得ずに16歳未満の未成年者の個人情報を販売するかどうかに言及する。
(2)個人情報の削除を要求する権利
a. 消費者は事業者が収集又は保持している個人情報の削除を要求する権利を有していると説明する。
b. 検証可能な消費者の削除の要求を提出するための指示又は要求をするためのオンラインの要求フォーム又はポータルが事業者によって提供されている場合はそのリンク先
c. 消費者が提出しなければならない情報を含め、消費者要求を検証するために事業者が使用するプロセスを記述する。
(3)個人情報の販売をオプトアウトする権利
a. 消費者は事業者による個人情報の販売をオプトアウトする権利を有していると説明する。
b. 第999.306条に従いオプトアウトの権利の通知又はそれへのリンクを含める。
(4) 消費者プライバシー権を行使する場合に差別をされない権利
a.消費者は、CCPAにより与えられたプライバシー権を行使するにあたって事業者から差別的な待遇を受けない権利を有すると説明する。
(5) 授権されたエージェント
a.消費者がCCPAのもとに自己に代わり授権されたエージェントをどのように指定できるかを説明する。
(6) 詳細についての問い合わせ：消費者に質問又は事業者のプライバシーポリシーやプラクティスについての懸念を連絡するための連絡先で、事業者が消費者との主なやりとりに使用する方法を反映させた方法を使用する。
(7) プライバシーポリシーが最後に更新された日付を記す。
(8) 第999.317条第(g)項の要件の対象となる場合は、第999.317条第(g)項(1)により集められた情報又は情報へのリンク先。

c. 通知の方法

通知の方法についてはCCPA規則が以下の通り定めを置いている。個人情報の収集時における通知及び金銭的なインセンティブの通知についてはプライバシーポリシーの一部へのリンクを提供する方法が認められており、事業者は現実的には、この方法で各通知を行うことになるものと考えられる。また、個人情報の販売からのオプトアウトの権利の通知についてはプライバシーポリシーへのリンクを貼ることが義務的である。

通知の種類	通知の方法
第999.305条 個人情報の収集時における通知	(c)事業者が個人情報を消費者からオンラインで収集する場合、収集時における通知は、第(b)項で求められる情報を含む事業者のプライバシーポリシーの一部へのリンクを提供することで消費者に与えることができる。
第999.306条 個人情報の販売	(b)消費者の個人情報を販売する事業者は、以下のとおり消費者にオプトアウトの権利の通知を提供しなければならない。

からのオプトアウトの権利の通知	(1)事業者は、ウェブサイト・ホームページ又はモバイル・アプリケーションのダウンロードページ若しくはランディングページ上で消費者が「私の個人情報を販売しない(“Do Not Sell My Personal Information”)」又は「私の情報を販売しない(“Do Not Sell My Info”)」というリンクをクリックした後に案内するインターネット・ウェブページ上にオプトアウトの権利の通知を掲載する。通知は第(c)項に定められた情報を含む又は同様の情報を含む事業者のプライバシーポリシーの一部にリンクする。 (2)消費者と主にオフラインでやりとりする事業者はまた、消費者にオフラインの方法によってオプトアウトの権利の消費者意識を促進する通知を提供しなければならない。方法には、通知を個人情報を収集する紙類に印刷する、消費者に通知を紙版で提供する、並びに消費者を通知が掲載されているウェブページへ案内するサイネージの設置を含むがこれに限らない。 (3)ウェブサイトを運営しない事業者は、個人情報を販売する事業者に消費者の個人情報の販売を中止するよう指示する権利を消費者に知らせるために、別の方法を定め、文書化し、及び遵守する。当該方法は、第(a)項(2)に定める要件に従う。 (e)オプトアウトボタン又はロゴ (1)以下のオプトアウトボタン又はロゴはオプトアウトの権利の通知を設置することに加えて使用できるが、通知の設置に代わるものではない。[規則案の修正版ではボタン又はロゴが加えられ、一般のコメントを受け付けるようにする。] (2)オプトアウトボタン又はロゴは、第 999.306 条第(c)項で定める情報を含むウェブページ若しくはオンラインロケーション又は同様の情報を含む事業者のプライバシーポリシーの一部にリンクする。
第 999.307 条金銭的なインセンティブの通知	(3)事業者が金銭的なインセンティブ若しくは価格又はサービスの差異をオンラインで提供する場合は、通知は第(b)項において求められる情報を含む事業者のプライバシーポリシーの一部へのリンクを提供することで与えることができる。
第 999.308 条プライバシーポリシー[10]	(3)プライバシーポリシーは、「Privacy」という言葉を使用した目立つリンクを通じてオンラインで事業者のウェブサイト・ホームページ若しくは又はモバイル・アプリケーションのダウンロードページ又はランディングページに設置しなければならない。事業者が消費者プライバシー権についてカリフォルニア州固有の記述を有する場合は、当該記述に「プライバシーポリシー」を含めなければならない。ウェブサイトを運営していない事業者は、消費者がプライバシーポリシーを目立つように利用可能にしなければならない。

Q.CCPA 第 100 条第(b)項の個人情報収集前の利用目的の通知については、個別通知が必要なのでしょうか、それとも、公表されたプライバシーポリシーへの利用目的の記載で十分なのでしょうか。
A. CCPA 規則案第 999.305 条第(c)項は、事業者が個人情報を消費者からオンラインで収集する場合、収集時における通知は第(b)項で求められる情報を含む事業者のプライバシーポリシーの一部へのリンクを提供することで消費者に与えることができるとしている。CCPA 規則案第 999.305 第(a)項(2)e は、個人情報の収集時における通知について、「個人情報の収集が行われる前に、消費者の目に入る場所に見える又はアクセス可能であ

[10] (1)プライバシーポリシーの目的は、個人情報の収集、利用、開示及び販売、並びに消費者の個人情報に関する権利にかかる事業者のオンライン及びオフラインのプラクティスの包括的な記述を消費者に提供することとする。プライバシーポリシーは、個々の消費者の個人情報の特定の部分を含めてはならず、消費者ごとに個別化しなくてよい。

る。例えば、事業者がオンラインで消費者の個人情報を収集する場合には、事業者のウェブサイト・ホームページ又はモバイル・アプリケーションのダウンロードページ、若しくは個人情報が収集される全てのウェブページに通知への明示的なリンクを設置する。事業者が消費者の個人情報をオフラインで収集する場合には、個人情報が収集される印刷物に通知を含める、又は消費者に印刷版の通知を提供する、若しくは消費者を通知が掲載されているウェブページへ案内する目立ったサイネージを設置する。」とされていることから、この方法に従う必要があると考えられる。

（情報通知・プライバシーポリシー）
Q.独自のホームページを持ち合わせていない場合、顧客へのポリシー通知はメール等の手段で行えばよいのでしょうか。ホームページを開設する必要があるのでしょうか。
A. CCPA 規則案第 998.308 条第(a)項(3)においては、ウェブサイトを運営していない事業者は、消費者がプライバシーポリシーを目立つように利用可能にしなければならないとされているに過ぎないことから、ホームページを開設する必要まではなく、メールで送る方法も許容されるものと考えられる。

(2) 消費者要求への対応のビジネスプラクティスに関する義務（CCPA 規則案第 3 節）

消費者要求への対応のビジネスプラクティスに関しては CCPA 規則において詳細な定めが置かれている。以下では消費者要求への対応のビジネスプラクティスに関する義務の内容を整理して紹介する。

i. 知る要求と削除の要求

知る要求と削除の要求の定義は以下の通りである。

要求の種類	定義
知る要求	CCPA 第 1798.100 条、第 1798.110 条又は第 1798.115 条により事業者が保有する消費者に関する個人情報を開示せよと要求する消費者要求をいう。以下の一又は全てに関する要求を含む（第 999.301 条第(n)項）。 (1) 消費者について事業者が持っている個人情報の特定の部分 (2) 消費者について事業者が収集した個人情報のカテゴリー (3) 個人情報が収集された情報源のカテゴリー (4) 事業者が事業目的のために販売もしくは開示した消費者についての個人情報のカテゴリー (5) 事業目的のために個人情報が販売もしくは開示された第三者のカテゴリー、及び (6) 個人情報を収集又は販売するための事業又は商業目的。
削除の要求	CCPA 第 1798.105 条により事業者が消費者から収集したその消費者の個人情報を削除するよう求める消費者要求をいう（第 999.301 条第（o）項）。

知る要求と削除の要求の提出方法は、次の通り CCPA 規則案において詳細な定めが置かれている。

第 999.312 条 知る要求と削除の要求の提出方法		
	知る要求	削除の要求
(a)/(b) 要求の提出方法	(a)事業者は、知る要求を提出するため二つ又はそれ以上の指定された方法を提供する。方法には最低でもフリーダイヤル電話番号を含み、事業者がウェブサイトを運営する場合は、事業者のウェブサイト又はモバイル・アプリケーションを通じてアクセス可能であるインタラクティブなウェブフォームを含む。これらの要求を提出するために許容できる他の方法には、指定されたｅメールアドレス、直接提出されたフォーム並びに郵便で提出されたフォームを含むがこの限りではない。	(b)事業者は、削除の要求を提出するため二つ又はそれ以上の指定された方法を提供する。これらの要求を提出するために許容できる方法には、フリーダイヤル電話番号、事業者のウェブサイトを通じてオンラインで利用できるリンク又はフォーム、指定されたｅメールアドレス、直接提出されたフォーム並びに郵便で提出されたフォームを含むがこの限りではない。
(d)削除のオンライン要求		(d)事業者は、削除のオンライン要求に関して、消費者が第一に削除の要求を明確に提出し、第二に消費者の個人情報を削除する意思を別途確認するという二段階のプロセスを使用する。
	知る要求と削除の要求	

(c)要求の提出方法を判定する場合の考慮要素	(c)事業者は、消費者が知る要求と削除の要求を提出するためにどの方法を提供するかを判定する場合、消費者とやりとりする方法を考慮する。提示された方法のうち、少なくとも一つは（知る要求の提出方法を三つ提示するよう事業者に求めるものであったとしても）事業者が消費者と主なやりとりをする方法を反映させなければならない。実例は以下のとおり。 (1)例 1：事業者がオンライン小売業者である場合、消費者が要求を提出できる方法の少なくとも一つは事業者の小売ウェブサイトを通じるべきである。 (2)例 2：事業者はウェブサイトを運営しているが、顧客との主なやりとりを小売場所において対面で行っている場合、事業者は知る要求の提出のための三つの方法を提示しなければならない。 －フリーダイヤル電話番号、事業者のウェブサイトを通じてアクセス可能であるインタラクティブなウェブフォーム及び小売場所で直接提出できるフォーム。
(e)事業者が通常の業務において消費者と直接やりとりをしない場合の知る要求及び削除の要求の提出方法	(e)事業者が通常の業務において消費者と直接やりとりをしない場合、消費者が知る要求及び削除の要求を提出する方法の少なくとも一つは、事業者のウェブサイト又は事業者のウェブサイトに設置されたリンクを通じるなどしてオンラインとする。
(f)消費者の要求の提出方法に瑕疵がある場合の事業者の対応	(f)消費者が指定された方法以外の方法で要求を提出した場合、又は検証プロセスには無関係な何らかの方法で瑕疵がある場合、事業者は以下のいずれかのとおりにする。 (1)事業者の指定する方法に従って提出された要求として扱う、又は (2)消費者に要求の提出の仕方又は要求の瑕疵を是正するための個別の指示を、該当する場合は提供する。

知る要求及び削除の要求への対応に関しては、要求の受領確認の義務という GDPR には定めが置かれていなかったものが加わっており、CCPA の方がより消費者にとって手厚い対応が義務付けられている。これに対して、知る要求及び削除の要求への対応の期限は 45 日以内に行えばよいとされており、GDPR 上の 30 日以内という期限よりは事業者にとって有利な定めとされている。

第 999.313 条 知る要求及び削除の要求への対応	
	知る要求と削除の要求
(a)知る要求又は削除の要求を受け取った場合の事業者の受領確認の期限	知る要求又は削除の要求の受領に際し、事業者は要求の受領を 10 日以内に確認し、要求をどのように処理するかの情報を提供する。事業者がすでに要求を承認又は拒否した場合を除き、提供される情報には事業者の検証プロセス及び消費者への対応が見込まれる期日を記述する。
(b) 知る要求及び削除の要	事業者は知る要求及び削除の要求に対し 45 日以内に対応する。45 日間は、要求を検証するために要する時間に関わらず事業者が要求を受領した日から起算する。必要であれば、要求に対応するために 45 日以上を要する理由の通知及び説明を事業者が消費者に提供した場合

求への対応期限	に限り、事業者は消費者の要求に対応するために 45 日を追加し、要求を受領した日から最長で合計 90 日を割くことができる。

知る要求及び削除の要求は、要求者の身元を検証できない場合には応じる必要がない。もっとも、その場合であっても、CCPA 規則案上において、単に要求を拒否するだけではなく、一定の対応義務が事業者に課せられている点に注意が必要である。また、要求に応じる場合及び拒否する場合についても、CCPA 規則案には、一定の注意事項が定められている。詳細は次の通りである。

第 999.313 条 知る要求及び削除の要求への対応		
	(c)知る要求への対応	(d) 削除の要求への対応
本人確認ができない場合の対応	(1)消費者に関する個人情報の特定の部分を開示するよう求める要求に関して、事業者が第 4 節で定める規則により要求を行う人の身元が検証できない場合は、事業者は要求者に対し個人情報の特定部分を開示せず消費者に身元が検証できない旨を通知しなければならない。要求の全部又は一部が拒否された場合は、事業者は消費者の要求を、第(c)項(2)により消費者に関する個人情報のカテゴリーの開示を求めるものであるとみなして評価する。 (2)消費者に関する個人情報のカテゴリーの開示を求める要求に関して、事業者が第 4 節で定める規則により要求を行う者の身元が検証できない場合は、事業者はカテゴリー及び他の要求された情報を開示する要求を拒否し要求者の身元が検証できない旨を通知する。要求の全部又は一部が拒否された場合は、事業者は、プライバシーポリシーに定められる、個人情報の収集、保持及び販売に関する一般的なビジネスプラクティスを消費者に提供し又は案内しなければならない。	(1) 削除の要求に関して、事業者が第 4 節で定める規則により要求者の身元が検証できない場合は、事業者は削除の要求を拒否できる。事業者は要求者に身元が検証できない旨を通知し、当該要求を代わりに販売のオプトアウトの要求として扱う。
要求への対応義務の範囲	(3)事業者は、開示が当該個人情報のセキュリティ、消費者の事業者とのアカウントのセキュリティ又は事業者のシステム若しくはネットワークのセキュリティに対し相当かつ明確で不当なリスクを与える場合は、消費者に個人情報の特定の部分を提供しない。 (4)事業者は、いかなる時にも消費者の社会保険番号、運転免許証番号又は他の政府発行識別番号、金銭的口座番号、いかなる健康保険及び医療識別番号、アカウントパスワード若しくはセキュリティに関する質問と答えを開示しない。	(2) 事業者は消費者の個人情報についての削除の要求に以下のとおり従わなければならない。 a. アーカイブ又はバックアップシステムを除いた現存するシステム上の個人情報を永久かつ完全に消す、 b. 個人情報を非識別化する、又は c. 個人情報を集合化する。
要求を拒否する場合	(5)事業者が個人情報の特定の部分に関する消費者の検証された知る要求を、連邦又は州の法律に抵触すること又は CCPA の適用除外に該当することを理由に全部又は	(6) 事業者が消費者の削除の要求を拒否する場合は、事業者は下記の全てを行う。

	一部拒否する場合、事業者は消費者に通知をし、拒否の根拠を説明する。拒否が一部のみの場合は、事業者は消費者が求める他の情報を開示する。	a. 消費者に、事業者は消費者の要求に従わないこと及び法的及び規則上の例外を含めた拒否の根拠の記述を通知し、 b. 例外の対象とならない消費者の個人情報を削除し、及び c. 例外が提供する以外の目的により保持された消費者の個人情報を利用しない。
要求に応じる場合の注意点	(6)事業者は個人情報を消費者に送信するに際し合理的なセキュリティ措置を講じる。 (7)事業者が消費者とパスワードで保護されたアカウントを保持する場合、事業者はポータルが CCPA 及び本規則により消費者の権利の対象となる個人情報を全て開示し、合理的なデータセキュリティコントロールを使用し、第 4 節で定める検証要件に適合するのであれば、安全なセルフサービス・ポータルにより消費者が個人情報にアクセス、閲覧し、ポータブルな写しを受領することで知る要求に従うことができる。 (8)特別の定めのない限り、CCPA 第 1798.130 条第(a)項(2)に参照されている消費者の検証可能な知る要求の対象となる 12 ヶ月間は、要求を検証するために要する時間に関わらず事業者が要求を受領した日から起算する。 (9)個人情報のカテゴリー、情報源のカテゴリー、及び/又は第三者のカテゴリーについての消費者による検証された知る要求を受けて、事業者は CCPA で求められる個別化した対応を消費者に提供する。事業者は、対応が全消費者に対して同じであり、かつ上記カテゴリーを知る要求への対応に含まれることが要求される全ての情報がプライバシーポリシーに開示してある場合を除き、プライバシーポリシーに概説されている事業者の一般的なプラクティスを消費者に紹介してはならない。 (10)個人情報のカテゴリーについての検証された知る要求を受けて、事業者は消費者に関して収集した個人情報の各識別カテゴリーにつき以下を提供しなければならない。 a. 個人情報が収集された情報源のカテゴリー、 b. 個人情報を収集した事業目的若しくは商業目的、 c. 事業者が事業目的のために個人情報のカテゴリーを販売又は開示した第三者のカテゴリー、及び	(3) 事業者が個人情報をアーカイブ又はバックアップシステム上に保存する場合、事業者はアーカイブ又はバックアップシステム上に保存するデータに関してはアーカイブ又はバックアップシステムが次にアクセス又は利用されるまで消費者の削除の要求に従うのを遅らせることができる。 (4) 消費者の削除の要求への対応の中で、事業者は個人情報を削除した方法を特定する。 (5) 削除の要求への対応の中で、事業者は CCPA 第 1798.105 条第(d)項により要求の記録を保持することを開示する。 (7) 削除の要求への対応の中で、事業者は消費者に選択された部分の個人情報を削除する選択肢を提示することができる。ただし、全ての個人情報を削除するグローバルオプションも提供され、かつ他の選択肢より目立つ形で提示された場合に限る。事業者は、消費者が第 999.312 条第(d)項の求めるところにより選択を確認する、二段階の確認プロセスを利用する。

	d. 個人情報のカテゴリーを収集又は開示した事業目的又は商業目的。 (11) 事業者は、個人情報のカテゴリー、個人情報の情報源のカテゴリー及び事業者が個人情報を販売又は開示した第三者のカテゴリーを、リストされたカテゴリーについての有意義な理解を消費者にもたらすような方法で記載しなければならない。	

ii. オプトアウトの要求

オプトアウト要求についても同じく CCPA 規則案上に詳細な規定が置かれている。特に注意が必要なものとしては、オプトアウト要求への事業者による対応の期限が 15 日以内と短く設定されていること、及びオプトアウト要求に関しては検証可能な要求であることが不要であるため、すなわち本人確認できない場合でも当該要求に応じる必要があるため、他の消費者要求の場合とは、異なる取扱いが必要となることが挙げられる。詳細は以下の通りである。

第 999.315 条 オプトアウト要求	
オプトアウト要求の提出のための指定された方法の提供	(a) 事業者は、オプトアウトの要求を提出するため二つ又はそれ以上の指定された方法を提供する。最低でも、明確で明白なリンクによりアクセス可能な事業者のウェブサイト又はモバイル・アプリケーション上の「私の個人情報を販売しない(“Do Not Sell My Personal Information”)」又は「私の情報を販売しない(“Do Not Sell My Info”)」と題したインタラクティブなウェブフォームを含める。これらの要求を提出するために許容できる他の方法には、フリーダイヤル電話番号、指定された e メールアドレス、直接提出されたフォーム、郵便で提出されたフォーム、ブラウザのプラグイン並びにプライバシー設定及び他のメカニズムなどのユーザー対応化されたプライバシー保護で消費者の個人情報の販売をオプトアウトする選択を伝達又は示唆するものを含むがこの限りではない。
オプトアウト要求の提出のための方法の指定の考慮要因	(b)事業者は、消費者がオプトアウトの要求を提出するための方法、事業者が第三者に個人情報を販売する方法、利用可能な技術及び平均的な消費者による使い勝手の良さを判定する場合、事業者が消費者とやりとりする方法を考慮する。提示された方法のうち、少なくとも一は事業者が消費者と主なやりとりをする方法を反映させる。
ユーザー対応化されたプライバシー保護	(c) 事業者が個人情報を消費者からオンラインで収集する場合、事業者は、ブラウザのプラグイン並びにプライバシー設定及び他のメカニズムなどのユーザー対応化されたプライバシー保護で消費者の個人情報の販売をオプトアウトする選択を伝達又は示唆するものを、そのブラウザ並びにデバイス又は判明していれば消費者に関して、CCPA 第 1798.120 条により提出された有効な要求として扱わなければならない。
一部の個人情報のみのオプトアウト要求の選択肢の提示	(d) オプトアウトの要求への対応の中で、事業者は消費者に個人情報の一定のカテゴリーの販売をオプトアウトする選択肢を提示することができる。ただし、全ての個人情報の販売をオプトアウトするグローバルオプションも提供されかつ他の選択肢より目立つ形で提示された場合に限る。
要求への対応の時間制限	(e) オプトアウトの要求の受領に際し、事業者は可能な限り速やかにしかし受領の日から 15 日以内に要求に対応しなければならない。

個人情報を販売した第三者への消費者からのオプトアウト要求の受領の通知	(f) 事業者は、消費者がオプトアウトの権利を行使した消費者要求を受領してから90日以内に消費者の個人情報を販売した全ての第三者に通知し、個人情報を販売しないように指示しなければならない。事業者は、これが完了した時、消費者に通知をしなければならない。
授権されたエージェントの使用によるオプトアウト要求	(g)消費者は、書面による許可を授権されたエージェントに提供する場合には、オプトアウトの要求を自己に代わり提出するために授権されたエージェントを使用することができる。事業者は、消費者から代理の権限が付与されたという証明を提出しないエージェントによる要求を拒否できる。ブラウザのプラグイン並びにプライバシー設定及び他のメカニズムなどのユーザー対応化されたプライバシー保護で消費者の個人情報の販売をオプトアウトする選択を伝達又は示唆するものは、授権されたエージェントを通じてではなく消費者からの直接の要求であるとする。
本人確認ができない場合にオプトアウト要求を拒否できる例外	(h)オプトアウトの要求は、検証可能な消費者要求であることを要しない。しかし、オプトアウトの要求が偽装であると事業者が誠実かつ合理的にそして文献による裏付けにより信じる場合は、事業者は要求を拒否できる。事業者は要求の当時者に要求に従わない旨を通知し、要求が偽装であると信ずる理由の説明を提供する。

CCPA規則案は、消費者が個人情報の販売をオプトアウトした後にオプトインする要求の方式について以下の通り定めている。

第999.316条　個人情報の販売をオプトアウトした後にオプトインする要求
(a)個人情報の販売にオプトインする要求は、消費者が第一にオプトインの要求[11]を明確に行い、第二にオプトインの選択を別途確認するという二段階のオプトインプロセスを使用しなければならない。
(b)事業者は、オプトアウトした消費者に、取引において個人情報の販売が取引を完了するための要件である時は、消費者がオプトインできるための指示と共にその旨を通知することができる。

CCPA上は世帯の個人情報も保護されており、そのため、次のような消費者による要求がCCPA規則案上、認められている。

第999.318条　世帯の個人情報へのアクセス又は削除の要求
(a)消費者が事業者にパスワードで保護されたアカウントを持たない場合、事業者は知る要求又は削除の要求について、集合化された世帯情報を提供することで世帯[12]の個人情報に係る対応を取得することができる。ただし、第4節に定める検証要件の対象となる。
(b)世帯の全消費者が共同で世帯情報の特定の部分へのアクセスを要求又は世帯個人情報の削除の要求を行い、なおかつ事業者が第4節で定める検証要件の対象である世帯の全構成員を個別に検証できる場合、事業者は要求に従う。

[11] 「オプトインの要求」とは、CCPA第1798.120条第(c)項により事業者が消費者に関する個人情報を販売できるとする13歳未満の子どもの親権者又は保護者、又は個人情報の販売について以前オプトアウトした消費者による積極的な許諾をいう（第999.301条(q)号)。

[12] 「世帯」とは単一の住居に居住する者あるいは数名の者をいう（第999.301条第(h)号)。

(3) 研修義務（CCPA 規則案第 999.317 条）

CCPA 対応において、特に注意が必要なのが、事業者のプライバシープラクティス又は事業者による CCPA の遵守に関する消費者からの問い合わせを担当する全ての者については、CCPA のみならず CCPA 規則における消費者の権利行使への対応方法に関して知識を持つことが必要とされており、事業者としては必然的に CCPA 及び CCPA 規則に関するトレーニングを担当者に対して行っておくことが義務付けられていることである。特に、米国子会社のみならず、米国外の日本本社等に CCPA の適用がある場合には、CCPA トレーニングを提供すべき範囲が大きくなることが考えられる。どのようにこの CCPA トレーニングを提供する義務の遵守を確保するかとの関係では、CCPA 規則案では 400 万件又はそれ以上の消費者の個人情報を年間ベースで購入等する事業者のみに義務付けられている内容ではあるが CCPA の研修ポリシーの策定及び文書化が義務付けられており、CCPA の研修ポリシーの策定及び文書化を任意で行うことが有効な対策であると考えられる。

第 999.317 条　研修	
消費者からの問い合わせを担当する全ての者の知識レベル	(a)事業者のプライバシープラクティス又は事業者による CCPA の遵守に関する消費者からの問い合わせを担当する全ての者は、CCPA 並びに本規則内の要件及び CCPA 並びに本規則のもとで消費者が権利行使するためにどのように案内するかについて知識を持っておかなければならない。
大量の個人情報を処理する事業者が負う追加の義務	(g)400 万件又はそれ以上の消費者の個人情報を年間ベースで購入、事業者の商業目的で受け取り、販売し、又は商業目的で共有することを単独又は組み合わせで行う事業者は、以下のとおりとする。 (3)事業者による CCPA の遵守に関する消費者からの問い合わせを担当する全ての者が本規則及び CCPA の要件についての知識を持つことを確保するために研修ポリシーを定め、文書化し、遵守する。

(4) 記録管理義務（CCPA 規則案第 999.317 条）

CCPA においては、GDPR 第 30 条のように処理業務の記録を維持する義務が定められていない。しかしながら、CCPA 及び CCPA 規則案上、知る要求へ対応する重い義務が定められていることから、事実上、事業者には、個人情報の処理に関して記録管理義務が定められているということができよう。すなわち、事業者がプライバシーポリシーにおいて開示することが義務付けられている内容については、予め事業者において記録管理を行っておかなければ、適切な開示を行うことができないと考えられるということである。

第 999.317 条　記録管理	
記録保持義務	(b)事業者は CCPA による消費者要求及び事業者が当該要求にどのように対応したかについての記録を少なくとも 24 ヶ月間保持しなければならない。 (c)記録は、チケット又はログのフォーマットで保持することができる。ただし、チケット又はログに要求の日、要求の性質、要求がなされた方法、事業者が要求に対応した日、対応の性質、並びに要求が全部又は一部拒否された場合は拒否の根拠が含まれる場合に限る。 (d)本項で求められる事業者による情報の保持は、当該情報が他のいかなる目的にも利用されない場合、単独では CCPA 又は本規則の違反とならない。 (e)記録管理の目的で保持される情報は、他のいかなる目的にも利用されてはならない。 (f)当該記録管理目的を除いて、事業者は CCPA のもとになされる消費者要求に応じる目的のみのために個人情報を保持することを求められない。

大量の個人情報を処理する事業者が負う追加の義務	(g)400 万件又はそれ以上の消費者の個人情報を年間ベースで購入、事業者の商業目的で受け取り、販売し、又は商業目的で共有することを単独又は組み合わせで行う事業者は、以下のとおりとする。 (1)前年について、以下の指標を蓄積する。 a. 事業者が受領し、全部又は一部従い、かつ拒否した知る要求の数、 b. 事業者が受領し、全部又は一部従い、かつ拒否した削除の要求の数、 c. 事業者が受領し、全部又は一部従い、かつ拒否したオプトアウトの要求の数、及び d. 知る要求、削除の要求及びオプトアウトの要求に事業者が実質的に対応した日にちの中間値。 (2)第(g)項(1)において蓄積された情報を、プライバシーポリシー上で又はプライバシーポリシーに含まれるリンクからアクセス可能なウェブサイト上で開示する。

Q. 保有する個人情報の取得年月日が分からない場合、開示対象期間「過去 12 ヶ月間で取得した個人情報」に含むべきでしょうか。また、個人情報の取得日を確定するために、証拠となるログ等を取る必要があるでしょうか。
A.前者については、個人情報の取得年月日を記録しておくべきであり、そうした場合に陥らないようにする必要がある。取得年月日が不明な場合には保守的に開示対象の個人情報に含めておくことが安全サイドの対応と考えられる。後者については、取得年月日の証拠は CCPA 遵守に関する説明責任を果たす観点からも防御の観点からも取得しておくべきと考える。

(5) 要求の検証義務（CCPA 規則案第 4 節）

CCPA 上、消費者要求が事業者に対してなされた場合にも、原則として、事業者は直ちに対応義務を負うわけではなく、当該要求が検証可能なものであること、すなわち要求者の本人確認ができることが、事業者が消費者要求への対応義務を負う要件とされている。但し、前述の通り、オプトアウト要求に関しては、検証可能な消費者要求である必要はない。

CCPA 上の要求の検証については、GDPR と比べて、より詳細な内容が、CCPA 規則案において事業者の義務として定められている。特に、日本本社において GDPR 対応を完了済みの場合には、CCPA が日本本社に対して与える影響を軽視しがちであるが、実際のところ、日本本社に対して CCPA の直接の適用がある場合、CCPA 規則案において定められる要求の検証に関する諸義務によって、日本本社は数多くの対応を迫られることになるものと考えられる。

第 4 節　要求の検証	
第 999.323 条 検証に関する一般原則	
要求の検証方法の策定と文書化義務	(a) 事業者は、知る要求又は削除の要求を行う消費者が事業者による情報収集の対象の個人であることを検証する[13]合理的な方法を定め、文書化し、遵守する。
身元検証の方法を決定するための考慮要因	(b)事業者が消費者の身元を検証する方法を決定するために、事業者は、 (1)可能な限り、消費者により提供された識別情報を事業者がすでに保持している消費者の個人情報と一致させる、又は本項を遵守する第三者身元検証サービス[14]を利用する。 (2)民法第 1798.81.5 条第(d)項において識別された種類の個人情報の収集を、消費者を検証する目的に必要である場合を除き、避ける。 (3)以下の要因を考慮する。 a. 消費者に関して収集され保持されている個人情報の種類、センシティビティ、価値。センシティビティ又は価値のある個人情報は、より厳格な検証プロセスが保証されなければならない。民法第 1798.81.5 条第(d)項において識別された個人情報の種類は、センシティビティがあるとみなす。 b.無権限アクセス又は削除によってもたらされる消費者への危害のおそれ。無権限アクセス又は削除によってもたらされる消費者への危害のおそれがより大きい場合は、より厳格な検証プロセスが保証されなければならない。 c.偽装又は悪意ある主体が個人情報を求めるおそれ。おそれが高まればそれに応じて検証プロセスもより厳格なものとしなければならない。 d.消費者の身元を検証するために消費者により提供される個人情報が、偽装の要求又はなりすまし若しくは偽造から保護するため十分にしっかりしたものであるかどうか。 e.事業者が消費者とやりとりする方法、及び f.検証に利用できる技術。

[13] 「検証する」とは、知る要求又は削除の要求を行う消費者が事業者による情報収集の対象の個人であることを判定することをいう（第 999.301 条第(u)号）。

[14] 「第三者身元検証サービス」とは、独立した第三者が提供するセキュリティープロセスで、事業者に要求を行う消費者の身元を検証するものをいう。第三者身元検証サービスは、知る要求と削除の要求について第 4 節に定める要件の対象となる（第 999.301 条(r)号）。

追加情報の要求の原則禁止と例外	(c)事業者は、検証を目的とした消費者への追加情報の要求を避けなければならない。ただし、事業者が事業者のすでに保持する情報によって消費者の身元を検証できない場合は、事業者は消費者に追加情報を要求することができる。この追加情報は、CCPA のもと権利行使を求める消費者の身元を検証すること及びセキュリティ又は偽装防止の目的のみに使用されなければならない。事業者は、検証の目的で収集された新しい個人情報を、消費者の要求を処理した後できるだけ早く削除するが、第 999.317 条に従うことが求められる場合はこの限りではない。
合理的なセキュリティ措置	(d)事業者は、偽装による身元検証行為を探知し消費者の個人情報への無権限アクセス又は削除を防止するため合理的なセキュリティ措置を実施しなければならない。
非識別化された消費者情報の扱い	(e)事業者が非識別化された消費者情報を保持する場合は、事業者は消費者からの要求に応じてこの非識別化された消費者情報を提供若しくは削除、又は消費者の要求を検証するために個別データを再識別する義務を負わない。
第 999.324 条　パスワードで保護されたアカウントの検証	
既存の認証プラクティスの利用の許容	(a)事業者が消費者のパスワードで保護されたアカウントを保持する場合、事業者は、消費者のアカウントに関する事業者の既存の認証プラクティスを通じて消費者の身元を検証することができる。ただし、事業者は第 999.323 条の要件に従うものとする。事業者はまた消費者のデータを開示又は削除する前に再認証を行うよう消費者に要求しなければならない。
偽装若しくは悪意の活動を疑う場合	(b)事業者が、パスワードで保護されたアカウントに対し又はそのアカウントから偽装若しくは悪意の活動を疑う場合、事業者はさらなる身元検証手続きにより消費者の要求が真正であり、知る要求又は削除の要求を行う消費者が事業者による情報収集の対象の個人であることが判定されるまで、消費者の知る要求又は削除の要求に従ってはならない。事業者は、消費者のさらなる身元検証をするために第 999.325 条に定める手続きを利用することができる。
第 999.325 条　非アカウント保有者の検証	
原則	(a)消費者が事業者にパスワードで保護されたアカウントを持たない又はアクセスできない場合は、事業者は第 999.323 条のほか本条第(b)項から第(g)項に従わなければならない。
合理的な程度の確実性	(b)個人情報のカテゴリーを知る要求に関わる事業者の遵守は、要求を行う消費者の身元を**合理的な程度の確実性**まで事業者が検証することを要件とする。合理的な程度の確実性は、消費者により提供された少なくとも 2 つのデータポイントを、事業者が保持するデータポイントで消費者を検証する目的のために信頼性があると事業者が判定したものと照らし合わせることを含む。
合理的に高い程度の確実性	(c)個人情報の特定の部分を知る要求に関わる事業者の遵守は、要求を行う消費者の身元を**合理的に高い程度の確実性**まで事業者が検証することを要件とする。これはより高い検証のハードルである。合理的に高い程度の確実性は、消費者により提供された少なくとも 3 つの個人情報を、要求者は要求の対象となる個人情報の消費者であるという署名付き宣言で偽証罪の罰則が適用されるものと共に、事業者が保持する個人情報で消費者を検証する目的のために信頼性があると事業者が判定したものと照らし合わせることを含む。事業者は全署名付き宣言を記録保持義務の一環として保持しなければならない。
	(d)削除の要求に関わる事業者の遵守は、個人情報のセンシティビティ及び無権限削除による消費者への侵害リスクの大きさによって、合理的な程度の確実性又は合理的に高い程度の確実性まで

	事業者が検証することを要件とすることができる。例えば、家族写真及び文書の削除は合理的に高い程度の確実性が要件とされるが、閲覧履歴の削除は合理的な程度の確実性を要件とすることができる。事業者は、第 4 節に定める規則に従い消費者の検証を行う際に適切な基準の適用を判定するにあたり、誠実に行動しなければならない。 ✓ 事業者に対し個人情報のセンシティビティ及び無権限削除による消費者への侵害リスクの大きさを踏まえて、確実性の程度に違いを設けて、事業者が要求の検証を行うことを求めており、事業者にとっては負担になるものと考えられる。また、削除の要求への対応を事業者において担当する者にとってもきちんとしたトレーニングや備えが必要になると考えられる。 ✓ ISOR は閲覧履歴の削除は合理的な程度の確実性で足りることを例として挙げている。
例示的なシナリオ	(e)例示的なシナリオは以下のとおり。 (1)事業者が個人情報を名前のある実在の人物と関連付けられる方法で保持する場合、事業者は消費者に事業者が保持する個人情報と一致する証拠を提供するよう求めることにより消費者を検証することができる。例えば、事業者が消費者の名前とクレジットカード番号を保持する場合、消費者の身元を合理的な程度の確実性まで検証するために、事業者は消費者にクレジットカードのセキュリティコードを提供しクレジットカードを使って最近購入したものを識別するよう求めることができる。 (2)事業者が個人情報を名前のある実在の人物と関連付けられない方法で保持する場合、事業者は消費者に自分が非名識別情報と関連付けられる唯一の消費者であることを示すように求めることにより消費者を検証することができる。これは、事業者に第 999.323 条(b)項(3)に定める要因を考慮する事実ベースの検証プロセスを行うよう求める場合もある。 上記の例示的なシナリオは受け入れ可能な検証方法のサンプルを提供したものである。
要求者の身元を検証するために合理的な方法がない場合	(f)事業者が消費者の身元を本条で求める合理的な程度の確実性の程度に検証できる合理的な方法がない場合は、事業者は要求に対してその旨を言及しなければならない。これが事業者が有する個人情報の消費者の全てに該当する場合は、事業者のプライバシーポリシーにおいてその旨を言及しなければならない。事業者は、要求者の身元を検証するために合理的な方法がないのはなぜなのかも説明する。事業者は毎年、方法が定められるかの評価を行い、当該評価を文書化しなければならない。
第 999.326 条 授権されたエージェント	
授権されたエージェントの使用	(a)消費者が知る要求又は削除の要求を提出するために授権されたエージェントを使用する場合、事業者は消費者に以下を求めることができる。 (1)授権されたエージェントに、授権されたエージェントを使用するとの書面による許可を提供する、及び (2)自らの身元を直接事業者と検証する。
エージェントによる要求を拒否できる場合	(b)第(a)項は、消費者が授権されたエージェントに遺言法(Probate Code)第 4000 条から第 4465 条による委任状を提供した場合は適用されない。 (c)事業者は、消費者から代理の権限が付与されたという証明を提出しないエージェントによる要求を拒否できる。

（権利行使）

Q.消費者からのアクセス権の行使又は削除要求の際、本人確認をどのように／どの程度すれば良いのか。

A.本人確認の例としては以下のようなものが挙げられる。

- EC サイトの場合、本人の名義の確認＋クレジットカードセキュリティコード＋購入履歴の突合せなど本人しか知りえない情報の確認を行う。
- 子供のアカウントからの問合せの場合、親に電話をして確認をとる。
- Web フォームからのリクエストの場合、多要素認証に SMS を使って携帯端末に認証番号を送り、認証番号の確認をもって本人認証とする。

(6) 未成年者に関する特則の義務（CCPA 規則案第 5 節）

CCPA 規則案上、未成年者の個人情報の販売に関するオプトインの手続を、13 歳未満と 13 歳以上 16 歳未満に分けて規定している。未成年者の個人情報の販売に関するオプトインの手続は、それぞれ「13 歳未満の子どもの個人情報を収集又は保持していることを実際に知る事業者」及び「13 歳以上 16 歳未満の未成年者の個人情報を収集又は保持していることを実際に知る事業者」のみについて義務付けられており、未成年者の個人情報を収集又は保持しない事業者は、そのような手続きを執ることを義務付けられないことに注意が必要である。

第 5 節　未成年者に関する特則	
第 999.330 条　13 歳未満の未成年者	
(a)個人情報の販売にオプトインするためのプロセス	
親権者又は保護者であることを判定するための合理的な方法の文書化義務	(1)13 歳未満の子どもの個人情報を収集又は保持していることを実際に知る事業者は、子どもに関する個人情報の販売を積極的に認める者が当該子どもの親権者又は保護者であることを判定するための合理的な方法を定め、文書化し遵守しなければならない。この積極的な許諾[15]は、児童オンラインプライバシー保護法(合衆国法典第 15 巻第 6501 条 et seq.)(COPPA)で求められる検証可能な親権者の同意に加えるものである。
例－同意を提供する者が子どもの親権者又は保護者であることを判定するための合理的な方法	(2)同意を提供する者が子どもの親権者又は保護者であることを判定するための合理的な方法には以下を含む。 a. 親権者又は保護者が偽証罪の罰則の適用の下にサインし、郵便、ファクシミリ又は電子スキャンにより事業者に返却される同意書を提供する。 b. 親権者又は保護者に、金銭的な取引に関連して、クレジットカード、デビットカード又はそれぞれ別個の取引につき主要なアカウント保有者に通知を提供する他のオンライン決済システムを使用するように求める。 c. 親権者又は保護者から訓練された人材を配置しているフリーダイヤル電話に電話をかけさせる。 d. 親権者又は保護者を訓練された人材とテレビ会議で接続させる。 e. 親権者又は保護者を訓練された人材と対面で接触させる。 f. 政府発行の ID を該当する情報データベースと突き合わせて調べることにより、親権者又は保護者の身元を検証する。この場合、親権者又は保護者の識別は検証が完了後ただちに事業者の記録から事業者により削除される。
	(b)本条第(a)項により事業者が積極的な許諾を受領した場合、事業者は第 999.315 条により子どもに代わって後日オプトアウトできる権利及びそうするためのプロセスを親権者又は保護者に通知しなければならない。
第 999.331 条　13 歳から 16 歳までの未成年者	
プロセスの策定と文書作成義務	(a)13 歳以上 16 歳未満の未成年者の個人情報を収集又は保持していることを実際に知る事業者は、第 999.316 条により未成年者に個人情報の販売をオプトインさせるための合理的なプロセスを定め、文書化し遵守しなければならない。

[15] 「積極的な許諾」とは、消費者による、個人情報の販売にオプトインするという意図的な判断を示す行為をいう。親権者又は保護者が 13 歳未満の子どもに代わる文脈においては、第 999.330 条に定める方法に従って親権者又は保護者が子どもの個人情報の販売に同意を提供したことを意味する。13 歳以上の子どもについては、消費者が第一にオプトインを明確に要求し、そして第二にオプトインの選択を別途確認するという二段階のプロセスを通じて示される（第 999.301 条第(a)号）。

	(b)事業者が 13 歳以上 16 歳未満の未成年者から個人情報の販売についてオプトインの要求を受領した場合、事業者は第 999.315 条により後日オプトアウトできる権利及びそうするためのプロセスを未成年者に通知しなければならない。
第 999.332 条　16 歳未満の未成年者	
開示義務	(a)第 999.330 条及び第 999.331 の対象となる事業者は、プライバシーポリシーにこれら条文で定める記述を含めなければならない。
オプトアウトの権利の通知義務の例外	(b)商品又はサービスを 16 歳未満の消費者に直接提供することを専らターゲットとし未成年者の個人情報を未成年者の積極的な許諾又は 13 歳未満の未成年者の親権者若しくは保護者の積極的な許諾なしに販売しない事業者は、オプトアウトの権利の通知を提供することを求められない。

Q. 未成年者に関してはどのように CCPA 規則案を遵守した実装を準備すればよいのでしょうか。
A. まず、以下のような対応を行うことが考えられる。
1. 年齢を選択させる Age gate を入れる。
2. 13 歳未満の場合、13 歳以上 16 歳未満、16 歳以上の 3 つの場合分けを行い、選択した年齢によって次に進む画面を出し分ける。

13 歳未満
- COPPA(Child Online Privacy Protection Act)と同じ趣旨で親権者の同意が必要である。
- ユーザー登録後に親権者の同意の手段としてクレジット/デビットカードでの 1 ドル等少額決済をさせる。
- 同意後、オプトアウトの機会を与えることが必要である。

13 歳以上 16 歳未満
- 必ず Opt-in 同意をとる。ブランクのチェックボックスに対して個人の意思で同意に✔をしてもらって送信してもらう。二段階の Opt-in 同意をとる。
- Opt-in 同意後、オプトアウト機会を与えることが必要である。

(7) 差別の禁止（CCPA 規則案第 6 節）

CCPA 規則案は、CCPA で定められている差別及び金銭的インセンティブについて、事例を挙げて指針を規定している。また、CCPA 第 1798.125 条の消費者のデータに基づき消費者に提供される価値、すなわち消費者のデータの価値の算定方法等や記録義務を定めている。詳細は以下の通りである。

第 6 節　差別の禁止	
第 999.336 条　差別的プラクティス	
原則	(a)消費者が CCPA 又は本規則により与えられた権利を行使したことを理由に事業者が消費者を異なる方法で扱う場合、金銭的なインセンティブ若しくは価格又はサービスの差異は差別的であり、ゆえに CCPA 第 1798.125 条により禁止される。 ▪ (d)消費者による知る要求、削除の要求又はオプトアウトの要求を事業者が CCPA 又は本規則で認められた理由により拒否することは、差別的であるとみなさない。 ▪ (f)CCPA 第 1798.145 条第(g)項(3)により事業者が合理的な手数料を課すことは、本規則の対象となる金銭的なインセンティブとみなさない。
例外	(b)本条第(a)項の定めに関わらず、第 999.337 条で定義される消費者データの価値に合理的に関連している場合、事業者は価格又はサービスの差異を提供できる。
例外－代表的な事例	(c)代表的な事例は以下のとおり。 (1)例 1：音楽配信事業者がフリーサービスと、1 ヶ月あたり 5 ドルかかるプレミアムサービスを提供する。音楽配信サービスに支払いをする消費者のみが個人情報の販売からオプトアウトすることができる場合、プラクティスは差別的である。ただし、1 ヶ月あたり 5 ドルの支払いが、事業者にとっての消費者データの価値と合理的に関連している場合はこの限りではない。 (2)例 2：小売店がメーリングリストに加入する消費者に割引価格を提供する。メーリングリストに載っている消費者が知る要求、削除の要求及び／又はオプトアウトの要求をした後も割引価格を受け取り続けることができる場合、価格レベルの違いは差別的ではない。
通知義務	(e)事業者は、第 999.307 条に従い提供する CCPA 第 1798.125 条の対象となる金銭的なインセンティブ及び価格又はサービスの差異があれば消費者に通知しなければならない。
第 999.337 条　消費者データの価値の算定	
定義	(a)CCPA 第 1798.125 条で使用される用法であるところの消費者データにより消費者に提供される価値は、消費者データにより事業者に提供される価値であり、「消費者データの価値」と称される。
文書化の義務	(b)消費者データの価値を見積もるため、CCPA 第 1798.125 条の対象となる金銭的なインセンティブ若しくは価格又はサービスの差異を提供する事業者は、消費者データの価値を算定するための合理的で誠実な方法を使用し文書化しなければならない。事業者は以下の一つ又はそれ以上を使用しなければならない。 (1)消費者データ又は典型的消費者データの販売、収集又は削除の事業者への限界価値 (2)消費者データ又は典型的消費者データの販売、収集又は削除の事業者への平均的な価値 (3)異なる価値を提供する別々の層、カテゴリー又は階級の消費者若しくは典型的消費者[16]から事業者が生み出した収入又は利益 (4)消費者の個人情報の販売、収集又は保持によって事業者が生み出した収入 (5)個人情報の販売、収集又は保持に関連する経費

[16] 「典型的消費者」とは、米国内に居住する自然人をいう（第 999.301 条第(s)号）。

	(6)金銭的なインセンティブ若しくは価格又はサービスの差異の提示、提供又は賦課に関連する経費 (7)消費者の個人情報の販売、収集又は保持により事業者が生み出した利益、及び (8)誠意をもって使用された、実際的で信頼できるその他の算定方法。

(8) 個人情報の性質に照らして合理的なセキュリティの手続と慣行を実装する義務（CCPA 第 1798.150 条）

CCPA 第 1798.150 条第(a)項(1)は、個人情報を保護するため情報の性質に適切で合理的なセキュリティ手続きとプラクティスを実施し維持する義務に事業者が違反した結果として、自身の暗号化されておらずかつ修正されていない個人情報[17]が、無権限アクセス、流出、窃取又は開示の対象となった消費者は、(a)違反 1 件について消費者一人当たりで 100 ドル以上 750 ドル以下の、又は実損害の、いずれか大きい額の損害を回収するため、(b)差止命令による救済又は宣言的救済、(c)裁判所が適切とみなすその他の救済のいずれかについて民事訴訟を提起することができるとされている。

また、CCPA 規則案においても、知る要求への対応や検証に関する一般原則との関係で、合理的なセキュリティ措置を講じることが義務付けられている。

第 999.313 条 知る要求及び削除の要求への対応
(c)知る要求への対応 (3)事業者は、開示が当該個人情報、消費者の事業者とのアカウントのセキュリティ又は事業者のシステム若しくはネットワークに対し相当かつ明確で不当なリスクを与える場合は、消費者に個人情報の特定の部分を提供しない。 (6) 事業者は個人情報を消費者に送信するに際し合理的なセキュリティ措置を講じる。 (7) 事業者が消費者とパスワードで保護されたアカウントを保持する場合、事業者はポータルが CCPA 及び本規則により消費者の権利の対象となる個人情報を全て開示し、合理的なデータセキュリティコントロールを使用し、第 4 節で定める検証要件に適合するのであれば、安全なセルフサービス・ポータルにより消費者が個人情報にアクセス、閲覧し、ポータブルな写しを受領することで知る要求に従うことができる。

第 999.323 条 検証に関する一般原則
(d)事業者は、偽装による身元検証行為を探知し消費者の個人情報への無権限アクセス又は削除を防止するため合理的なセキュリティ措置を実施する。

CCPA 上は、合理的なセキュリティ措置の基準について、特に言及はない。カリフォルニア州司法長官が 2016 年に 2 月に出したカリフォルニアデータ侵害レポート（California Data Breach Report）[18]は 30 頁において「レコメンデーション 1：インターネットセキュリティセンターのクリティカルセキュリティコントロール（Critical Security Controls）は、個人情報を収集し又は維持する全ての組織が遵守すべき情報セキュリティの最低限のレベルを定義する。組織の環境に適用される全てのコントロール（Controls）を実装しないことは、合理的なセキュリティの欠如を構成する。」と記載している。当該レポートは別紙 A（Appendix A: The CIS Critical Security Controls for Effective Cyber Defense）及び別紙 B（Appendix B: The Critical Security Controls Master Mapping (Excerpt)）において当該コントロールの内容を紹介しているが、2015 年 10 月 15 日に公表された Version 6.0 の内容に基づいているようであり内容が古くなっている。

[17] 第 1798.81.5 条第(d)項(1)(a)4 に定める自身の暗号化されておらずかつ修正されていない個人情報のことをいい、名前又はデータ要素が暗号化されておらず又は修正されていない場合で、個人のファーストネーム若しくは初めのイニシャル及びその者のラストネームと以下の一つ又はそれ以上のデータ要素との組み合わせ：(i)ソーシャルセキュリティナンバー、(ii)運転免許番号又はカリフォルニア州の識別カード番号、(iii)口座番号、クレジットカード番号若しくはデビットカード番号で、個人の金銭的口座にアクセスできるために必要なセキュリティコード、アクセスコード又はパスワードとの組み合わせ、(iv)医療情報、(v)健康保険情報

[18] https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf

CIS Controls Version 7 は最新の CIS Controls ではないものの、Center for Internet Security のウェブサイトにおいて日本語バージョンのダウンロードが可能であり参考になる[19]。次の表は、CIS Controls Version 7 の日本語版に記載されている CIS Control 1 から CIS Control 20 までの表題と内容を抜粋してまとめたものである。

	CIS Control	表題	内容
Basic	CIS Control 1	ハードウェア資産のインベントリとコントロール	ネットワーク上の全てのハードウェアデバイスを能動的に管理（インベントリ作成、追跡、修正）し、アクセス権限を許可されたデバイスだけに付与します。また、許可されていないデバイスや管理されていないデバイスを検出し、これらのデバイスがアクセス権限を取得することを防止します。
	CIS Control 2	ソフトウェア資産のインベントリとコントロール	ネットワーク上の全てのソフトウェアを能動的に管理（インベントリ作成、追跡、修正）し、許可されたソフトウェアだけをインストールし、実行可能とします。許可されていないソフトウェアや管理されていないソフトウェアを検出し、不正なソフトウェアのインストールと実行を防止します。
	CIS Control 3	継続的な脆弱性管理	継続的に新たな情報を取得、評価し、この情報に基づいて措置を講じることで、脆弱性を特定して修復し、攻撃チャンスを最小限に抑えます。
	CIS Control 4	管理権限のコントロールされた使用	コンピュータ、ネットワーク、アプリケーションの管理権限の使用、割り当て、設定を追跡／管理／防止／修正するためのプロセスとツールです。
	CIS Control 5	モバイルデバイス、ラップトップ、ワークステーション及びサーバに関するハードウェア及びソフトウェアのセキュアな設定	攻撃者が脆弱なサービスや設定を悪用できないようにするため、厳格な設定管理及び変更管理プロセスを使用して、モバイルデバイス、ラップトップ、サーバ、及びワークステーションのセキュリティ設定を確立、実装し、能動的に管理（追跡、報告、修正）します。
	CIS Control 6	監査ログの保守、監視及び分析	イベント監査ログを収集、管理、分析します。これは、攻撃を検知、理解し、攻撃からの被害を復旧する上で役立ちます。

[19] https://learn.cisecurity.org/cis-controls-download

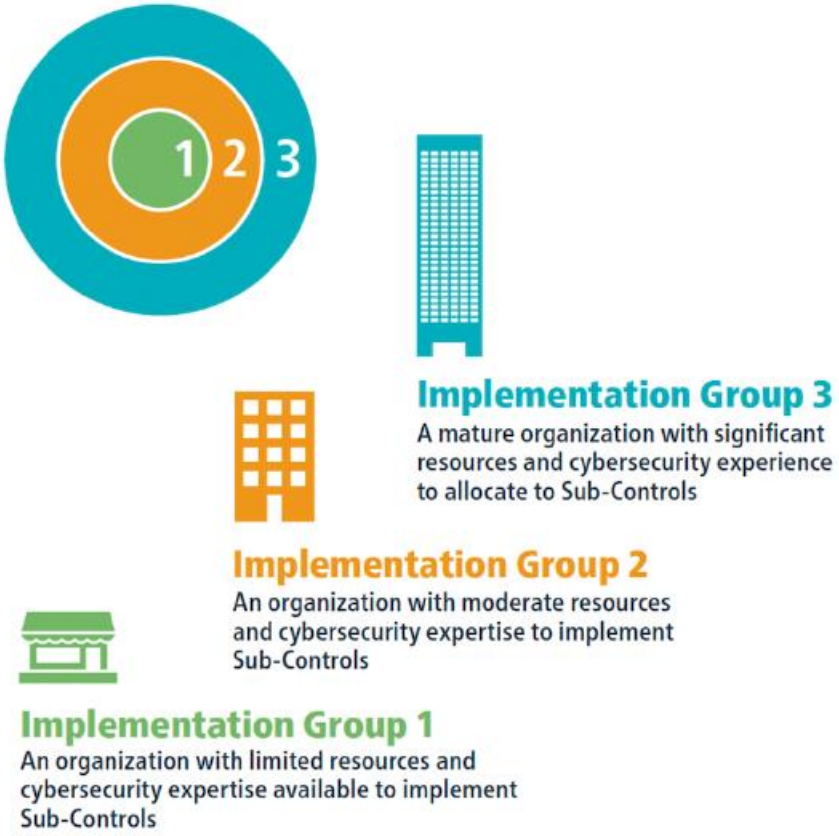
Foundational	CIS Control 7	電子メールと Web ブラウザの保護	攻撃者が Web ブラウザや電子メールシステム利用者の行動を操作して行う攻撃の対象範囲や機会を最小限に抑えます。
	CIS Control 8	マルウェア対策	企業内の複数ポイントで悪意のあるコードのインストール、感染拡大、実行をコントロールし、自動化機能を活用して迅速な防御対策の更新、データ収集、修正を可能にします。
	CIS Control 9	ネットワークポート、プロトコル、及びサービスの制限及びコントロール	攻撃者に対して脆弱性が利用可能である期間を最小限に抑えるため、ネットワーク接続デバイスのポート、プロトコル及びサービスの継続的な運用を管理（追跡／コントロール／修正）します。
	CIS Control 10	データ復旧能力	本プロセスとツールは、重要情報を適切にバックアップするとともに、実証済みの手法でタイムリーに情報を復旧します。
	CIS Control 11	ファイアウォール、ルータ、スイッチなどのネットワーク機器のセキュアな設定	攻撃者が脆弱なサービスや設定を悪用できないようにするため、厳格な設定管理及び変更管理プロセスを適用してネットワークインフラの機器設定を確立、実装し、能動的に管理（追跡、報告、修正）します。
	CIS Control 12	境界防御	異なる信頼レベルのネットワーク間を流れる情報の中から、セキュリティ上問題となるデータを検知／防止／修正します。
	CIS Control 13	データ保護	データの不正持ち出しを防止し、不正に持ち出されたデータの影響を低減し、機密情報の機密性と完全性を確保するためのプロセスとツールです。
	CIS Control 14	Need - to - Know に基づいたアクセスコントロール	許可された分類に基づき、どのユーザー、コンピュータ、アプリケーションが重要な資産（情報、リソース、システムなど）へのアクセスを必要とし、アクセス権限を持つべきであるかに関する正式な決定内容に従い、これら資産への保護されたアクセスを追跡／制御／防止／修正するためのプロセスとツールです。
	CIS Control 15	無線アクセスコントロール	本プロセスとツールは、無線ローカルエリアネットワーク（WLAN）、アクセスポイント、無線クライアントシステムのセキュリ

			ティの使用状況を追跡／管理／防止／修正するために利用されます。
	CIS Control 16	アカウントの監視及びコントロール	システムアカウント及びアプリケーションアカウントのライフサイクル（アカウントの作成、使用、休止、削除）を能動的に管理し、攻撃者に悪用される機会を最小限に抑えます。
Organizational	CIS Control 17	セキュリティ意識向上トレーニングプログラムを実施する	組織内の全ての職務について、事業とそのセキュリティに不可欠な職務を優先しながら、企業防衛に必要とされる具体的知識、スキル、能力を洗い出します。その上で、現状との差を評価し不足を特定するための全体計画を作成し実施します。そして、セキュリティポリシー、組織計画、トレーニング及びセキュリティリテラシープログラムを通じて改善を進めます。
	CIS Control 18	アプリケーションソフトウェアセキュリティ	ソフトウェアにおけるセキュリティ上の脆弱性を防止、検知、修正するため、社内開発ソフトウェアと社外調達したソフトウェア全てのセキュリティライフサイクルを管理します。
	CIS Control 19	インシデントレスポンスと管理	組織の情報と信頼を保護するため、攻撃を迅速に検知し、損害を効果的に食い止め、攻撃者の存在を根絶し、ネットワークとシステムの完全性を復元するためのインシデントレスポンス基盤（計画、明確な役割、トレーニング、コミュニケーション、管理／監督）を策定、実装します。
	CIS Control 20	ペネトレーションテスト及びレッドチームの訓練	攻撃者の目的と活動をシミュレーションして、組織の防御対策（技術、プロセス、担当者）の全体的な強度をテストします。

CIS Controls Version 7 の日本語版（2018 年 3 月 19 日付）では、以下の要素が説明されている。

- 攻撃の防御や攻撃の存在を特定する際の CIS Control の重要性（このコントロールが重要である理由）と、このコントロールが実施されない状況が攻撃者によってどのように悪用されるか
- 組織がコントロールを実装し、具体的なアクション（「サブコントロール」）をリスト化して記載
- 実装と自動化を可能にする手順とツール
- 実装構成要素を示すサンプルのエンティティ関係図

Center for Internet Security が公表する最新の CIS Controls V 7.1（2019 年 4 月 1 日付）[20]は、Version 7 に CIS Implementation Groups（IGs）として知られる、Controls の使用を優先順位をつけて行うための新しいガイダンスを導入したものである。IGs は組織が自らを分類して、セキュリティのリソースと専門性を集中させるとともに、CIS Controls の価値を最大化することを助ける、簡潔でかつ利用しやすい方法である。IGs の概念図[21]は以下の通りである。



各組織は IG1 から IG3 までのどのカテゴリーに当てはまるかを特定することが勧められる。例えば、以下のような形が考えられる。

- 家族所有の事業で 10 名以下の従業員がいる組織：IG1
- サービスを提供する地域組織：IG2
- 数千名の従業員のいる大規模な組織：IG3

IG のカテゴリーが決まれば、組織は CIS の Sub-Controls を実装することに集中することができる。組織が組織のカテゴリーを特定するために使う基準は、以下の性質に基づいている。

1. 組織によって提供されるデータのセンシティビティ及びサービスのクリティカルさ

いかなる理由（例、公共の安全、クリティカルインフラストラクチャ）でも利用可能でなければならないサービスを提供するか又はさらに制約されたセットの要件（例、連邦法）の下で保護されなければならないデータを取り扱う組織は、より先進的なサイバーセキュリティコントロールを実装する必要がある。

2. スタッフ又は契約上で示される技術的専門性の期待されるレベル

[20] CIS Controls V7.1 は次のリンク（https://learn.cisecurity.org/cis-controls-download）からダウンロード可能である。
[21] CIS Controls v.7.1 のガイドブックより参照。 https://www.cisecurity.org/wp-content/uploads/2019/04/CIS-Controls-Version-7.1-Implementation-Groups.xlsx

サイバーセキュリティの知識及び経験を取得するのは困難であるが、CIS Controls に説明されている詳細なサイバーセキュリティの緩和策の多くを実装することは必要である。CIS Controls の多くは、最低限の重要な IT の技量を必要とするのに対し、他の CIS Controls は成功裏に実装する上で深遠なサイバーセキュリティの技術及び知識を必要とする。

3. サイバーセキュリティの活動に向けて利用可能でかつ専用のリソース

時間、金及び人は、CIS Controls 内に含まれるベストプラクティスの多くを実装するために必要である。サイバーセキュリティに向けてリソースを専従させることができる企業は、今日の敵に対してより洗練された防御を行うことができる。組織の実装を支援するオープンソースのツールは利用可能なものがあるが、追加の管理及び配備にかかるオーバーヘッドを認識し考慮に入れる必要がある。

CCPA 上、個人情報を保護するため情報の性質に適切で合理的なセキュリティ手続きとプラクティスを実施し維持する義務に事業者が違反した結果として、一定の個人情報に不正アクセス等があった場合に、消費者による訴訟提起が認められていることから、日本企業としては米国内拠点及び CCPA の適用対象となる米国外拠点において少なくとも一定のセキュリティ対策を行うことが重要であると考えられる。

その際には、まず、カリフォルニア州司法長官が推奨する最新の CIS Controls V 7.1（2019 年 4 月 1 日付）及び CIS Controls V 7 の日本語版（2018 年 3 月 19 日）の内容を確認することが望ましい。そのうえで、上記の組織のカテゴリーを特定するための基準に従って、自社の組織カテゴリーの評価を簡易にであっても行ってみることが考えられる。そして、自社の組織カテゴリーが該当する CIS の Sub-Controls の内容を確認し、実装の有無をチェックすることが望ましい。

それと並行して、CCPA 上の合理的セキュリティ手続について IT セキュリティの実装に関する外部専門家に対する相談も行うべきであろう。なぜなら、CIS Controls は、個人情報を収集し又は維持する全ての組織が遵守すべき情報セキュリティの最低限のレベルを定義したものであって、組織の環境に適用される全てのコントロール（Controls）を実装したとしても、合理的なセキュリティが備わっていると評価されるとは必ずしも言えないと考えられるためである。また、CCPA 修正案 AB1035 では当初、The framework for improving critical infrastructure cybersecurity（NIST）又は NIST-SP800-171 への準拠を求めていたが現段階では記述が削除されたという経緯もあり、CCPA が求める合理的なセキュリティ手続の基準も変化する可能性がある。CCPA のセキュリティ対応のプロジェクトには比較的多額の投資が必要となることを踏まえると、CCPA 上の合理的なセキュリティ手続の基準についても最新の動向を把握しておくことが望ましいと考えられる。

第 7　CCPA 対応のプロジェクト進行と TO DO リスト

前述の通り、CCPA 上は、CCPA の適用対象となる者として 4 つのカテゴリー（①事業者、②サービス提供者、③第三者、④責任引受者）が定められている。一つの法的主体が個人情報の処理業務毎に異なるカテゴリーに該当する場合もあるため、自社・自組織がこれら 4 つのカテゴリーのどれか一つにのみ該当することを前提として検討しないように注意すべきである。すなわち、自社・自組織が個人情報の処理業務毎に複数のカテゴリーに該当することもあり得るのである。

Q. CCPA のセミナーを色々と受講しましたが、当社のカリフォルニア州の拠点には CCPA の適用がないと考えています。この結論で日本本社に報告しようと思いますが、何か留意するべき点はあるでしょうか。 A. CCPA については適用範囲に関して様々な誤解しやすいポイントがあるため、注意が必要である。例えば、貴社のカリフォルニア州拠点については「事業者」の売上高の要件（2,500 万米ドル以上）を満たさない場合でも、貴社日本本社が当該「事業者」の要件を満たし、その結果として、貴社のカリフォルニア州拠点が貴社日本本社に支配されていることを理由に、貴社のカリフォルニア州拠点についても「事業者」に該当し、CCPA の適用対象となることもあり得る。また、貴社のカリフォルニア州の拠点が非営利団体である場合であっても、「第三者」に該当することもあり得る。CCPA の適用の有無に関して CCPA 適用を否定する結論を採る場合には、外部の第三者の意見を取得する等して、慎重な検討を行うことが強く勧められる。

以上を前提として、各カテゴリーに該当し CCPA の適用対象となりそうなことが判明した場合に、日本企業の日本本社及び米国子会社において連携した上で、CCPA へのコンプライアンス対応を行う場合、それぞれのカテゴリー毎に、次のように CCPA 対応のプロジェクトを行うことが考えられる。

1.　「事業者」としての CCPA コンプライアンス対応

以下のような CCPA 対応のプロジェクト対応と To Do リストを作成することが考えられる。

「事業者」に該当する場合の CCPA 対応のプロジェクト進行・TO DO リスト
1. CCPA 対応のプロジェクトの準備
1.1　日本本社のトップマネジメントに対する CCPA 対応の必要性の説明 1.2　社内における CCPA 対応の担当部署（日本本社・米国拠点それぞれ）の決定 1.3　CCPA 対応のために必要となる予算の確保 1.4　CCPA 対応のプロジェクトマネージャー（主に事実調査を担当し、CCPA 対応文書のドラフトの作成支援等）・CCPA の専門弁護士・データ保護コンサルタント（事実調査の監督、CCPA 対応文書の雛型の提供、CCPA 対応文書の最終レビュー等）・IT セキュリティの専門家であるコンサルタント（IT・セキュリティの実装対応を担当）を選定。なお、プロジェクトマネージャーを専門弁護士・データ保護コンサルタント又は IT セキュリティの専門家であるコンサルタントが兼ねることもあり得る。
2. 事実調査に基づく CCPA 対応
2.1　以下の事実を収集するため、データマッピング質問票（事実調査票）を準備する 個人情報の取得・販売の目的、取得の情報源及び取得時期、取得・販売の対象となる個人情報の種類、消費者の種類、個人情報の件数、個人情報を開示した先の第三者の名称等 2.2　データマッピング質問票を配布し、内容を説明し、回答を回収する。回答への再質問・再回答。 2.3　記入済みデータマッピング質問票の回答を分析し、CCPA の適用範囲を確定する。そのうえで、以下の 8 つの義務に対応するための To Do を準備する。 (1) 消費者への通知義務（CCPA 規則案第 2 節） (2) 消費者要求への対応のビジネスプラクティスに関する義務（CCPA 規則案第 3 節）

(3) 研修義務（CCPA 規則案第 999.317 条）
(4) 記録管理義務（CCPA 規則案第 999.317 条）
(5) 要求の検証義務（CCPA 規則案第 4 節）
(6) 未成年者に関する特則の義務（CCPA 規則案第 5 節）
(7) 差別の禁止（CCPA 規則案第 6 節）
(8) 個人情報の性質に照らして合理的なセキュリティの手続と慣行を実装する義務（CCPA 第 1798.150 条）
2.4 上記 8 つの義務への対応としては、以下の CCPA 対応文書を準備することが考えられる。
2.4.1　個人情報の処理活動の記録の作成
2.4.2　情報通知・プライバシーポリシーの作成（「販売」のオプトアウト・オプトイン対応、金銭的インセンティブについての検討を含む。）
2.4.3　消費者の個人情報を移転させる相手との契約書の作成・レビュー（具体的には、相手を「サービス提供者」又は「責任引受者」に該当させるための契約上の手当て・交渉）
2.5 また、上記 2.3 の(1)、(2)、(5)及び(6)との関係では IT の実装、上記(8)の合理的なセキュリティの手続と慣行を実装する義務との関係ではセキュリティの実装をチェックする。遅くとも、この段階までに、IT・セキュリティの専門家をプロジェクトに関与させることが望ましい。
3. CCPA 対応の社内規則やひな型の作成
3.1　CCPA 対応の社内規則（消費者要求への対応マニュアル含む）の作成
3.2　個人情報漏洩への対応マニュアルの作成
3.3　各契約・規約類の見直し（差別禁止違反の見直し、class action waiver, arbitration clause 等）
4. CCPA 対応の社内トレーニングの実施
4.1　CCPA 対応の社内規則一式の米国拠点及び日本本社の従業員への説明
4.2　消費者要求があった場合の対応の模擬訓練
4.3　個人情報漏洩があった場合の対応の模擬訓練
5. CCPA 対応の運用
5.1　個人情報の処理活動の記録の定期的なアップデート
5.2　プライバシーポリシーの定期的なアップデート
5.3　定期的な従業員への CCPA 研修
5.4　CCPA 適用対象拠点に対する CCPA 監査

2. 「第三者」としての CCPA コンプライアンス対応

非営利団体のように「事業者」や「サービス提供者」に該当し得ない法的主体の場合には、次のような To Do リストを基本としてプロジェクトを進めることが考えられる。なお、次の To Do リストは「第三者」に該当する場合の必要最小限の CCPA 対応として考えられるものを挙げたものであることに注意が必要である。

「第三者」に該当する場合の CCPA 対応のプロジェクト進行・TO DO リスト
1. CCPA 対応のプロジェクトの準備
1.1　日本本社のトップマネジメントに対する CCPA 対応の必要性の説明（CCPA 対応が一切不要であるという誤った先入観を取り除く必要がある）
1.2　社内における CCPA 対応の担当部署（日本本社・米国拠点それぞれ）の決定
1.3　CCPA 対応のために必要となる予算の確保

1.4　　CCPA の専門弁護士・データ保護コンサルタント（データ分類化の作業の支援、CCPA 対応文書の作成等）を選定。
2. 事実調査に基づく CCPA 対応
2.1　　データ分類化を行うため、データ分類化の質問票（事実調査票）を準備する 2.2　　データ分類化の質問票を配布し、内容を説明し、回答を回収する。回答への再質問・再回答。 2.3　　記入済みデータ分類化の質問票の回答を分析し、CCPA の適用範囲を確定し、CCPA に違反しないための注意点をリストアップ。
3. CCPA 対応の社内規則やひな型の作成
3.1　　CCPA 対応の社内規則の作成
4. CCPA 対応の社内トレーニングの実施
4.1　　CCPA 対応の社内規則の米国拠点及び日本本社の従業員への説明
5. CCPA 対応の運用
5.1　　定期的な従業員への CCPA 研修 5.2　　CCPA 適用対象拠点に対する CCPA 監査

なお、CCPA 対応との関係では、「第三者」には個人情報の性質に照らして合理的なセキュリティの手続と慣行を実装する義務が課せられているわけではないが、個人情報漏洩の場合に、他の法律との関係で、当局への通知等が必要となることを踏まえると、この機会に個人情報漏洩への対応や合理的なセキュリティの手続と慣行を実装する義務への対応を行うことが望ましいと考えられる。

3. 「サービス提供者」・「責任引受者」としての CCPA コンプライアンス対応

自社・自組織が②サービス提供者又は④責任引受者に該当する場合は、②及び④に該当する前提として一定の契約の締結があるため、当該契約の内容を遵守するようにコンプライアンス対応を行うことになるため、比較的対応方法が分かりやすいと考えられる。すなわち、自社・自組織が、他の事業者から②サービス提供者との契約又は④責任引受者との契約を提示された段階で、当該契約を検討し、締結後の契約の内容を遵守するための社内態勢の整備を行うことになる。また、多くの場合、②サービス提供者又は④責任引受者のどちらかにしか該当しないということは考えにくく、個人情報の処理業務によっては「事業者」に該当するため、上記 1 の「事業者」としての To Do を基本として CCPA コンプライアンス対応を進めてゆくべきであると考えられる。

なお、自社・自組織が、消費者（カリフォルニア州の住民）の個人情報を処理しており、将来的にサービス提供者との契約の締結を事業者から求められることが明らかな場合には、前もってサービス提供者との契約の雛型を準備しておき、それを事業者に提示することで、個別に相手方である事業者が提示してくるサービス提供者の契約のレビューやコメントを行う負担を減らすという方法も実務上の対応として考えられる。また、その場合には、サービス提供者の契約を遵守するために必要な社内規則の整備や社内のトレーニングも行うことが必要になると考えられる。

第８　おわりに

CCPA へのコンプライアンス対応プロジェクトの成否は、今後遅くとも 2，3 年以内に米国において立法されることが確実な情勢となっている米国連邦プライバシー法へのタイムリーな遵守ができるか否かを占う試金石である。データが企業・組織の事業のあらゆる面で飛躍的に重要性を増していく中で、プライバシー権という基本的人権を最大限尊重した経営を行っていくことは時代の要請である。すなわち、米国でビジネスを行う日本企業・組織にとって、CCPA へのコンプライアンス対応への姿勢が、プライバシー権という基本的人権をどの程度尊重した経営を行っているかのバロメーターとなって、米国市場の参加者から厳しい監視の対象となる世の中が始まったと言えるのかもしれない。

世界のデータ保護法へのコンプライアンス対応という時代の流れの中で、日本企業・組織にとっては、これまでは良い流れがあった。すなわち、はじめに世界のデータ保護法として登場した GDPR は、日本企業・組織にとって、比較的守らなければならないものであることが分かりやすい法であった。具体的には、高額の制裁金制度（違反した場合の制裁金額が、2,000 万ユーロ以下、又は事業者の場合には、事業者グループの全事業年度の全世界売上高の 4%以下で定められる)、個人データの EEA 域外への持ち出し・移転禁止の規定、日本本社に GDPR が直接適用される域外適用の規定の存在が GDPR の分かりやすさを助けた。

他方で、今回の CCPA は、極めて重要であり、多くの日本企業・組織に関係があるのにもかかわらず、それが日本企業・組織に伝わりにくい要因が幾重にも存在する。本ハンドブックにおいては、現在の CCPA 及び CCPA 規則案について重要な情報をできる限り丁寧に日本語で解説することを試みた。言うまでもなく、本ハンドブックに示した見解に従うことが重要なのではなく、本ハンドブックに示した見解の批判に耐え得るように、自社・自組織としての CCPA への対応に関しての立場を固めておくことが重要である。場合によっては、貴社・貴組織が、外部の法律事務所から、本ハンドブックに示した見解とは異なる、貴社・貴組織の立場をサポートする法律意見書を取得し、CCPA へのコンプライアンス対応を一切取らないということも、一つの在り方であろう。それは万が一、貴社・貴組織が CCPA に違反するとしてカリフォルニア州の司法長官又は消費者によって訴追されることがあったとしても、貴社・貴組織としては十分慎重に CCPA の適用の有無を検討したことを客観的に示すことができるからである。ただ、現状、米国下院エネルギーおよび商業対策委員会において超党派の連邦プライバシー法案のファーストドラフト、すなわち、共和党と民主党の議員が共同作業によって作成した法案のドラフトが公表されており、より広範に日本企業・組織に適用される内容となることが予想される連邦プライバシー法案の存在を前提とすると、米国でビジネスを行う日本企業・組織が、一日も早く米国におけるデータプライバシー法へのコンプライアンス体制の構築に着手することが望ましいと言わざるを得ない。

本ハンドブックが日本企業・組織の CCPA へのコンプライアンス対応、ひいては米国におけるデータプライバシー法へのコンプライアンス体制の構築を、適時に促進することにつながることを期待したい。

以　上

カリフォルニア州（CCPA）実務ハンドブック

作成者：日本貿易振興機構（ジェトロ）
ジェトロサンフランシスコ事務所
575 Market Street, Suite 2400, San Francisco, CA 94105, U.S.A.
TEL:+1-415-392-1333（代表）
email:sfc-marketing@jetro.go.jp
http://www.jetro.go.jp
