

2025 年における CCPA（カリフォルニア州消費者プライバシー法） 及び CCPA 規則の改正

2025 年 11 月 17 日

弁護士 小坂光矢
弁護士 竹内麻緒

<目次>

- 1.はじめに
- 2.最終規則の主な内容
 - (1)自動意思決定技術（ADMT）
 - (2)サイバーセキュリティ監査
 - (3)リスク評価
- 3.その他の改正
 - (1)個人情報の形式
 - (2)神経データ
 - (3)合併時のデータ移転
 - (4)オプトアウト・プリファレンス・シグナル

1. はじめに

2025 年 9 月 23 日、カリフォルニア州プライバシー保護局（CPPA : California Privacy Protection Agency）が提案した最終規則が承認されました。本規則は、自動意思決定技術（ADMT）、プライバシーリスク評価、サイバーセキュリティ監査等に関する内容を定めるものです。これらの内容は企業に新たな義務を課すものであり、その他の 2025 年に施行され、または成立した CCPA 規則と併せて、実務に大きな影響を及ぼすと考えられます。

2. 最終規則の主な内容

最終規則の主な内容は、以下の 3 点です。

(1) 自動意思決定技術（ADMT）（§ 7200）

ADMT（automated decisionmaking technology）とは、個人情報を処理し、計算を用いて人間の意思決定を代替または実質的に代替する技術をいいます（§ 7001(e)）。

事業者は、2027 年 1 月 1 日までに以下の事項を実施しなければならないとされています。

- ①重要な決定に ADMT を使用する場合、消費者のオプトアウト権とアクセス権を含む特定の事項を含む使用前通知（Pre-use Notice）を消費者に提供しなければならない。
- ②一定の例外を除き、消費者が ADMT の使用からオプトアウトするための手段を提供する。
- ③ADMT に関する消費者のアクセス要求に応じる。

(2) サイバーセキュリティ監査（§ 7120）

対象となる事業者は、独立した専門家によるサイバーセキュリティ監査を実施し、毎年 CPPA に監査報告書を提出しなければならないとされています。

対象事業者は、①前暦年の年間売上の 50%以上が個人情報の販売・共有によるものである事業者、又は②前暦年における年間総売上が 2,500 万ドル超であり、かつ個人情報の処理件数が 25 万件以上であるか、若しくはセンシティブ個人情報の処理件数が 5 万件以上である事業者とされています（§ 1720(b)）。

CPPA への初回の監査報告書の提出期限は、年間総売上の規模に応じて以下のとおりとされています。

- ・ 2026 年の年間総売上 1 億ドル超：2028 年 4 月 1 日（監査対象期間は 2027 年 1 月 1 日から 2028 年 1 月 1 日）
- ・ 2027 年の年間総売上 5,000 万～1 億ドル：2029 年 4 月 1 日（監査対象期間は 2028 年 1 月 1 日から 2029 年 1 月 1 日）
- ・ 2028 年の年間総売上 5,000 万ドル未満：2030 年 4 月 1 日（監査対象期間は 2029 年 1 月 1 日から 2030 年 1 月 1 日）

(3) リスク評価（§7150）

個人情報処理が「重大なプライバシーリスク」を伴う場合、事業者はリスク評価の実施が必要とされています。

「重大なプライバシーリスク」を伴う場合とは、以下の場合をいいます（§ 7150(b)）。

- ①個人情報の販売または共有
- ②センシティブ個人情報の処理（ただし、事業者が自己の従業員又は独立契約者のセンシティブ個人情報を、報酬支払いの管理、就労資格の判断および保管、雇用給付の管理、法令に基づく合理的配慮の提供、または法令に基づく賃金報告の目的のみに利用する場合を除く）
- ③消費者に関する重要な決定に ADMT を使用すること
- ④ADMT を使用して、教育プログラム応募者、求職者、学生、従業員、または事業者の独立契約者として行動している消費者を体系的に観察し、その観察に基づいて消費者の知能、能力、適性、職務遂行、経済状況、健康（精神的健康を含む）、個人的嗜好、興味、信頼性、傾向、行動、所在地、または移動を推測または推定すること
- ⑤ADMT を使用して、消費者が機微な場所（sensitive location）に存在していることに基づき、当該消費者の知能、能力、適性、職務遂行、経済状況、健康（精神的健康を含む）、個人的嗜好、興味、信頼性、傾向、行動、または移動を推測または推定すること
- ⑥消費者に関する重要な決定のために使用する ADMT を訓練する目的で、または顔認識・感情認識・その他の技術であって消費者の本人確認、または身体的もしくは生物学的な識別・プロファイリングを行う技術を訓練する目的で、消費者の個人情報を処理すること

リスク評価は、①該当する処理を開始する前に完了し文書化すること、②少なくとも 3 年ごとに見直し、必要に応じて更新すること、及び③処理が継続する間、又はリスク評価完了から 5 年間のいずれか長い期間保持することが求められます。

リスク評価については、処理目的などをリスク評価報告書に特定して文書化し、ウェブサイトを通じて当局に提出する必要があります。

なお、2026 年と 2027 年に実施されたリスク評価については、提出期限は 2028 年 4 月 1 日となっています。

3. その他の改正

2024 年 9 月末に成立し、2025 年 1 月 1 日に施行された規則において、個人情報及びセンシティブ情報の定義及び、企業買収時のデータ移転について改正がなされました（下記(1)～(3)）。

また、2025 年に成立し、2027 年 1 月に施行される規則において、オプトアウト・プリファレンス・シグナルの設置等が義務付けられました（下記(4)）。

(1) 個人情報の形式（AB1008 § 1798.140.(v)(4)(A)～(C)）

「個人情報」は、物理的形式（紙の文書、印刷された画像、レコード盤、ビデオテープなど）、デジタル形式（テキスト、画像、音声、または動画ファイルなど）、抽象的なデジタル形式（圧縮または暗号化されたファイル、メタデータ、または個人情報を出力できる人工知能システムなど）を含む様々な形式で存在することが明記されました。

(2) 神経データ（SB1223 § 1798.140. (ae)(1)(G)）

「センシティブ個人情報」に消費者の神経データ（消費者の中樞神経系または末梢神経系の活動を測定することで生成される情報であり、非神経情報から推測されたものではない情報）が追加されました。

(3) 合併時のデータ移転（AB1824 § 1798.120(a)(2)）

企業買収・合併時のデータ移転に関し、取得企業が元の事業者に対する消費者のオプトアウト指示（個人情報の販売・共有拒否）を尊重して遵守する義務が定められました。

(4) オプトアウト・プリファレンス・シグナル（AB566 § 1798.136）

ウェブブラウザに関して、合理的なユーザーが容易に発見し、個人情報の販売・共有停止を設定できるオプトアウト・プリファレンス・シグナル（OOPS）を設定することが義務づけられました。

なお、オプトアウト・プリファレンス・シグナルの仕組みとその効果については、消費者に対して明確に提示することが求められています。

以 上

ニュースレターの配信登録は[こちら](#)です。
バックナンバーは[こちら](#)でご覧いただけます。

牛島総合法律事務所
<https://www.ushijima-law.gr.jp/>