米国個人情報保護規制最新動向
（日本DPO協会 第50回個人情報保護セミナー）

森・濱田松本法律事務所外国法共同事業　パートナー
慶應義塾大学大学院法学研究科特任教授（非常勤）
弁護士・ニューヨーク州弁護士　田中 浩之

2026/2/26

MORI HAMADA

Lawyer Profile

パートナー

田中 浩之

Hiroyuki Tanaka

弁護士(第二東京弁護士会所属)

ニューヨーク州弁護士

慶應義塾大学大学院法学研究科
特任教授(非常勤)

Direct 03-6266-8597
Mail hiroyuki.tanaka@morihamada.com

MORI HAMADA

主要な取扱分野

- データ・プライバシー(国内外の個人情報保護規制を含む)、AI、知的財産、デジタル法制、IT(システム開発紛争を含む)

著作・論文

- 『サイバネティック・アバター(CA)と法』(弘文堂、2025年、共著)
- 『EUデータ法を中心としたEUデジタル法制への実務対応のポイント』(Business & Law 実務解説、2025年)
- 『クロスセクター・サイバーセキュリティ法』(商事法務、2025年、共著)
- 『グローバルデータ保護法対応Q&A100』(中央経済社、2024年、共著)
- 『生成AIと知財・個人情報Q&A』(商事法務、2024年、共著)
- 『ゼロからわかる生成AI法律入門』(朝日新聞出版、2023年、共著)
- 『ChatGPTの法律』(中央経済社、2023年、共著)
- 『AIプロファイリングの法律問題 AI時代の個人情報・プライバシー』(商事法務、2023年、共著)
- 『60分でわかる！改正個人情報保護法 超入門』(技術評論社、2022年、共著)
- 『「対話で理解する」「学びを実務へ」情報管理のエッセンス』(会社法務A2Zで連載中、共著)
- 『システム開発訴訟[第2版]』(中央経済社、2022年、共著)
- 『改訂版 ビジネス法体系 知的財産法』(第一法規、2025年) その他多数

講演

- 「EUデータ法を中心としたEUデジタル法制等への実務対応(サイバーレジリエンス法、NIS2指令、DSA、AI法、AIを踏まえた製造物責任の改正、GDPR等もカバー)」
- 「生成AI活用の法的問題点と実務上の対応」
- 「アドテクノロジーの導入及び第三者提供を中心とした個人データの利活用規制対応の実務～近時の解釈動向を踏まえて～」
- 「グローバル(欧米・中国・アジア主要国等)データ保護規制の要点比較と最新実務対応」 その他多数

経歴

慶應義塾大学法学部法律学科卒業、慶應義塾大学大学院法務研究科修了、ニューヨーク大学ロースクール修了

Clayton Utz法律事務所 シドニーオフィスで執務(2013年～2014年)

主な活動

- 2023年～慶應義塾大学大学院 法学研究科 特任教授(非常勤)(2024年～法務研究科グローバル法務専攻非常勤講師を兼担[担当授業科目:INTELLECTUAL PROPERTY FROM A GLOBAL PERSPECTIVE])(～現在)
- 慶應義塾大学 グローバルリサーチインスティテュート サイバーフィジカル・サステナビリティ・センター 構成員(2023年～現在)
- AI法研究会 生成AI部会長(2023年～現在)
- 一般社団法人日本DPO協会顧問(2019年～現在)

受賞歴等

- 日経企業法務税務・弁護士調査」の活躍した弁護士ランキングで複数回選出(2025年:AIガバナンス分野で企業が選ぶ弁護士第6位。2024年:AI・テック・データ分野で企業が選ぶ弁護士第3位。2022年:知財分野で選出。2019年:データ関連分野で企業が選ぶ弁護士第5位)
- Lexology indexのDataの分野でGlobal Elite Thought Leader に選出
- Lexology indexのArtificial IntelligenceのTransactional & AdvisoryとRegulatory & Compliance分野で選出
- 弁護士ドットコムの「弁護士と法務部が選ぶベストビジネス弁護士100」でAI・IT部門で選出
- Thomson Reuters Stand-out Lawyers - independently rated lawyersに選出
- Best Lawyers® でPrivacy and Data Security Law及びTechnology Lawの分野で選出
- IAM Patent 1000 – Japan (Litigation)で選出

米国法の全体像

1

米国データ保護法の全体像①

- **連邦法**
  - **包括**的な連邦データ保護法は現時点では存在しない
  - 分野毎に**個別**の連邦法は存在している（セクトラル方式）
  - （例）
    - 銀行等の金融機関に適用される連邦法であるGramm-Leach-Bliley Act（GLBA）：15 U.S.C. 6801 - 6809 中に、個人情報の処理に関する規定もある
    - 医療関係についてのHIPAA / HITECH
    - **子供関係：13歳未満の子供**のオンラインにおける個人情報の扱いに関する連邦法であるChildren's Online Privacy Protection Act of 1998（**COPPA**）・・・**最近規則が改正**
    - ビデオプライバシー保護法（Video Privacy Protection Act）（**VPPA**）・・・集団訴訟の原因となっている
  - **FTC法**について：連邦法であるFederal Trade Commission Act（FTC法）5条（a）「**不公正又は欺瞞的な行為又は慣行**」の禁止により、個人情報に関する「不公正又は欺瞞的な行為又は慣行」について執行を行っている

米国データ保護法の全体像②

- **州法**
  - **包括**的な州法
  - ✓ カリフォルニア州のCCPA・・・**規則が最近改正**された
  - ✓ 他にも多数の州で存在
  - **個別**州法
  - ✓ イリノイ州の生体認証情報プライバシー法（**BIPA**）やカリフォルニア州のCalifornia Invasion of Privacy Act (**CIPA**)の等・・・集団訴訟の原因となることもあり注意が必要
  - ✓ **子供**関係：カリフォルニア州のAge-Appropriate Design Code Act(現在地裁の仮差止命令により執行が出来ない状態)、アーカンソー州オンラインプライバシー法、ニューヨーク州児童データ保護法

CCPA規則改正について

2

CCPAについて

- CCPAとは？
  - California Consumer Privacy Act
  - 2018年6月28日に制定されたカリフォルニア州の包括的な個人情報保護規制
- CPRA（CCPA2.0）とは？
  - California Privacy Rights Act （CPRA）
  - CPRAは、CCPAを改正して更なる規制強化をする（事業者への適用のための数的な基準の緩和等一部は規制緩和）ための法令
  - 州務長官の認証を経て、**2020年12月16日**に正式に成立
  - **2023年1月1日に施行済**
  - California Privacy Protection Agency及び州の司法長官の執行開始は、**2023年7月1日以降**であり、**同日以降**の違反が対象（1798.185（d））
  - CPRAにより改正されたCCPA（以下単に「CCPA」という）は、**2022年1月1日以降**に収集される個人情報に適用（SEC.31、1798.130.（a）（2）（B））
- **CCPA規則改正**：2025年に規則が改正。2026.1.1から適用開始だが、適用猶予あり

CCPAの適用場面①（総論）

- **CCPAは誰に適用されるか？**
  - CCPAが適用される“Business”（「事業者」）（CCPA：1798.140（d））
  - これに加えて、CCPAは、「サービス提供者」、「契約者」、「第三者」をも名宛人としており、「事業者」に該当しない場合であっても、CCPAを遵守しなければならない場合があり得ることに注意が必要である

CCPAの適用場面②

- **CCPAが適用される“Business”（「事業者」）（CCPA：1798.140（d））**
  - 以下の①及び②の両方の条件を充足する場合
    - ① 消費者（＝カリフォルニア州の居住者）の個人情報を取得し（第三者を通じて取得する場合や第三者と共同して取得する場合を含む）、その処理の目的と手段を決定する**営利目的の事業者**であり、カリフォルニア州で「事業」を行っている
      - ※ 州内に拠点があることは要件ではないと解される
    - ② 以下の（a）から（c）までのいずれか一つの条件を充足する
      - （a） **年間総収益**（annual gross revenues）が**2662万5000米ドル（2025.1.1から増額。隔年毎に消費者物価指数を踏まえて、数値は見直し）**を超えている
        - ※ カリフォルニア州における収益やカリフォルニア州居住者からの収益には限られない
        - ※ **CCPAで、各暦年の1/1で前暦年の年間総収益をみることが明記**
      - （b） **1年あたり**で、合計で**10万**以上の**消費者**（＝カリフォルニア州の居住者）、（カリフォルニア州の居住者に結びつく）**世帯**の個人情報を購入、受領、販売、又は共有している
      - （c） 年間収益額の50%以上を消費者（＝カリフォルニア州の居住者）の個人情報の「**販売**」又は「共有」から得ている

CCPAの適用場面③

- **CCPAが適用される“Business”（「事業者」）（CCPA：1798.140（d））**
  - 事業者を**支配**し、又はこれに**支配される**事業者であり、かつ、**共通のブランド**を有し、**当該事業者が消費者の個人情報を共有する**事業者
    - 「支配する」とは以下のいずれかを意味する。①事業者の議決権ある発行済み株式の50%超を保有し又はその議決を行う権利を有すること②方法を問わず、取締役その他これと同様の機能を有する者の過半数の選任を管理すること③事業者の経営に関し支配的な影響を行使する権限を有すること
    - 「共通のブランド」とは、共通の名称、サービス・マーク又は商標であって、平均的消費者がこれらを共通にする者が共通の所有関係にあると理解するものを意味する
  - 複数の事業者により構成されるジョイントベンチャー又はパートナーシップであって、各事業者が40%以上の持分を有するもの
    - ジョイントベンチャー又はパートナーシップ及びその当事者である事業者は、それぞれ、別個の単一事業者とみなされる。但し、各事業者が保有する個人情報は、当該ジョイントベンチャー又はパートナーシップに開示されないことを条件とする
  - 上記以外のカリフォルニア州で事業を行っている者であって、カリフォルニア州プライバシー保護局に対し自ら任意でCCPAに従うこと及びこれに拘束されることを保証（certify）した者

CCPAの適用場面④（適用除外）

- **全ての側面が州外で行われる場合の適用除外（CCPA：1798.145（a）（7））**
  - 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**には適用なし
  - 具体的には、以下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居る時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居た時に収集された個人情報を販売していない

- **他の法律で規律される個人情報についての適用除外（1798.145（c）から（g））**
  - 1798.145（c）：医療情報・健康情報
  - 1798.145（d）：信用情報
  - 1798.145（e）：GLBA又はCalifornia Financial Information Privacy Act（CFIPA）に従って取得、処理、販売、開示された個人情報については、CCPAは適用されない
  - 1798.145（f）：運転者個人情報保護法関係
  - 1798.145（g）：AB 1146（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）により追加

CCPA対応のTO DO案①

（CCPA対応のTO DO）（水色ハイライトは、CPRAによる改正対応での追加、黄緑ハイライトは、CCPA規則改正による対応の追加）

- **情報通知・プライバシーポリシー**の作成 / 見直し（CPRAによる改正での追加項目を追記。規則改正で、サービス提供者や契約者に開示した個人情報の種類の通知が必要に）
- **「販売」・「共有」**についての検討
  - 「販売」・「共有」がある場合、**オプトアウト・オプトイン**対応（**Do Not Sell or Share My Personal Information**ページ**又は代替オプトアウトリンク**の準備。CCPAとの関係では、オプトアウトプリファレンス信号対応について検討。CCPAとの関係では、特に、クロスコンテクスト行動広告対応について検討）CCPA対応のため、未成年者オプトインの再同意についての規制強化（16歳になるまで待つ必要あり）に対応し、**販売・共有先の第三者との契約**を準備
  - **販売・共有のオプトアウトの表示対応（2026.1.1～）**
    - オプトアウトプリファレンス信号関係（§7025(c)(6)）：例えば、事業者は、あるブラウザ、デバイスまたはオプトアウト設定シグナルを利用する消費者が、自社Webサイトを訪問した場合、そのWebサイト上に"**Opt-Out Request Honored**"と表示
    - 個別のオプトアウト要求関係（§7026(g)）：例えば、事業者は、そのWebサイト上に"**Opt-Out Request Honored**"と表示しまたは消費者が個人情報の販売をオプトアウトしたことをトグルまたはラジオボタンで表示
- **個人情報の収集・削除（保持）・販売についての経済的インセンティブ**についての検討と通知・同意の準備
- **サービスプロバイダ・契約者**との契約の作成 / 見直し（CPRAによる改正での厳格化に対応）

CCPA対応のTO DO案②

（CCPA対応のTO DO）

- CCPA対応の社内規則（**社内規程**）の作成（CPRAによる改正での追加項目を追記）
- **データ主体の権利行使**への対応（**マニュアル**策定、**フリーダイアル**その他の窓口準備。CPRAによる改正で訂正請求権、知る要求の範囲拡大、削除権に伴う通知義務等CPRAによる改正で追加された対応についての対応知る要求への対応拡大。

  また、規則改正により、以下の対応が必要

  ✓訂正権：事業者が、消費者が不正確であると主張する情報の取得元ではない場合には、当該消費者の請求を処理することに加えて、事業者は、当該不正確とされる情報を取得した提供元の名称を消費者に提供しなければならない。または、これに代えて、当該情報の提供元に対し、その提供した情報が誤っており、訂正されるべきであることを通知しなければならない（規則§7023(i)）

  ✓知る要求・訂正権：事業者が保有している所定の重要な個人情報について、なりすましによる開示/訂正を防ぐために、確認済みの消費者が提供する情報と同一であるかどうかを、当該消費者が確認できる方法を提供しなければならない（規則§7023(j)/7024(d)(ii)）
- **個人情報漏洩**への対応マニュアルの作成
- 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）
- **データセキュリティ**対策の検証（CPRAによる改正で範囲拡大）

CCPA対応のTO DO案③

（CPRAによる改正で追加となったCCPA対応のTO DO）

- **規則§7002の明示的同意**要否について検討して、必要な場合は同意取得
- オプトイン同意が必要な処理がある場合には、**オプトイン同意がCCPA規則§7004の要件（選択の対称性やダークパターンの禁止を含む）を充足**したものとなるようにする（CCPA規則改正により、選択の対称性について、「Yes」ボタンが「No」ボタンよりも目立つ形を禁止した。また、禁止されるダークパターンの例が追加されており、ウェブサイト上で同意を求めるポップアップ画面について、消費者が「同意する」に相当するボタンを積極的に選択することなく、その画面を閉じたり、他のページへ移動したりしただけで同意したことにすることはできないとされていたり、虚偽の緊急性[カウントダウン等]により誘導される選択はダークパターンであるとされている）
- 消費者の特徴を推測する目的での**機微な個人情報**の利用についての検討（CCPA規則改正により、機微な個人情報に、事業者が実際に知識を有する、16歳未満の消費者に属する個人情報が追加。また、機微な個人情報についての制限権について、機微な個人情報の収集と同じ方法での通知義務が追加）
  - ➡ 消費者の特徴を推測する目的での機微な個人情報の利用がある場合、**Limit the Use of My Sensitive Personal Information**ページの準備
- 個人情報の**保持期間**の設定とその期間を超えた保持をしないようにする

CCPA対応のTO DO案④

（**CCPA規則改正で対応が新たに必要となったCCPA対応のTO DO**）

- **消費者に対する重要な決定にADMT(自動化された意思決定技術)を利用する事業者の義務**
  - 使用前の通知+アクセス権 + オプトアウト権対応（**2027.1.1**～）
  - なお、消費者に対する重要な決定にADMTを利用することについては、以下の高リスクデータ処理にもあたるため、リスク評価が必要+大規模事業者については、自動化された意思決定についての権利行使についても記録保持+開示義務の対象となる
- **高リスクデータ処理**についてのリスク評価義務（**2026.1.1**～。ただし、2025年以前に開始された処理については**2027.12末**までにリスク評価を完了すればよい。CPPA（当局）への年次報告書の提出期限は、2026年・2027年に実施するリスク評価については**2028.4.1**、2028年以降に実施するリスク評価については、評価実施の翌年の4.1）
  - 高リスクデータ処理がある場合、①事前にリスク評価を実施し②年次報告書をCPPAに提出しなければならない。評価は少なくとも3年ごとに見直し、処理活動に重大な変更が生じた場合は45日以内に更新が必要
- **サイバーセキュリティ監査**（サイバーセキュリティ監査完了の証明書のCCPAへの提出の初回期限は、事業者の年間売上高が1億ドル超の場合は**2028.4.1**、5000万～1億ドルの場合は**2029.4.1**、5000万ドル未満の場合は、**2030.4.1**。それ以降年次報告）
  - 一定の要件（①前暦年に、年間収益の50%以上を消費者の個人情報の販売・共有から得ている又は②年間総収益がCCPA適用基準を充足し、かつ、前暦年に(i)25万人以上の消費者または世帯の個人情報を処理したこと若しくは(ii) 5万人以上の消費者のセンシティブ個人情報を処理したこと）を充足する場合に暦年毎にサイバーセキュリティ監査を実施して、サイバーセキュリティ監査完了の証明書をCPPAに提出

高リスクのデータ処理に関するCCPA上の義務①

- 消費者の個人情報の処理が、第(b)項に定める消費者のプライバシーに重大なリスクをもたらす事業者はすべて、その処理を開始する前にリスク評価を実施しなければならない。以下の各処理行為は、消費者のプライバシーに重大なリスクをもたらす（規則§7150）

(1)個人情報を販売または共有すること

(2)機微な個人情報を処理すること（従業員・独立契約者関係の例外あり）

(3)消費者に関する重要な決定のためにADMT（自動化された意思決定）を使用すること。

(4)消費者が教育プログラムの申込者、求職者、学生、従業員、または事業に対する独立契約者(業務委託先)としての資格において行動している場合に、当該消費者の体系的な観察に基づき、当該消費者の知能、能力、適性、業務遂行能力、経済状況、健康状態（精神的健康状態を含む）、個人的嗜好、関心、信頼性、素質、行動、所在地、または動作を推論または推定するために自動処理を使用すること

高リスクのデータ処理に関するCCPA上の義務②

- 消費者の個人情報の処理が、第(b)項に定める消費者のプライバシーに重大なリスクをもたらす事業者はすべて、その処理を開始する前にリスク評価を実施しなければならない。以下の各処理行為は、消費者のプライバシーに重大なリスクをもたらす（規則§7150）

(5)消費者がセンシティブな場所に存在しているという事実に基づいて、自動化された処理を用いて、消費者の知能、能力、適性、業務上のパフォーマンス、経済状況、健康状態（精神的健康を含む）、個人的嗜好、関心、信頼性、素因、行動または移動を推論または推定すること（当該センシティブな場所において消費者に対して商品を配送する、または消費者のために移動手段を提供する目的のみに個人情報を利用する場合は含まれない）

※「センシティブな場所」とは、次のいずれかの物理的場所をいう。医療施設（病院、診療所、救急医療施設および地域保健クリニックを含む）、薬局、ドメスティック・バイオレンス（DV）被害者のためのシェルター、フードパントリー（食料支援施設）、住宅支援施設／緊急避難所、教育機関、政党事務所、法律サービス事務所、労働組合事務所、礼拝施設

(6)事業者が、消費者に関する重要な決定のために ADMT を訓練するため、または消費者の本人確認を行なう、もしくは消費者の物理的/生物学的な識別/プロファイリングを行う顔認識、感情認識、その他の技術を訓練するために使用する目的で消費者の個人情報を処理すること

高リスクのデータ処理に関するCCPA上の義務③

- 年次報告書の提出義務：上級管理職が宣誓し、署名した年次報告書をCPPAに提出する必要がある（規則§7157(a)-(c)）
- CPPAおよびカリフォルニア司法長官（AG）は個別のリスクアセスメントの提出を求める権限を有し、請求を受けてから30日以内に提出しなければならない（規則§7157(e)）
- 事業者は、該当する処理活動を開始する前にリスクアセスメントを行い、3年ごとまたは処理活動の重大な変更が生じたときにレビューおよび更新をしなければならない（規則§7155(a)）
- リスクアセスメントでは、以下を明示する必要がある：処理の目的、処理する情報の種類（機微な個人情報を含む）、処理に関するその他の事実関係、処理活動による利益（事業者・消費者・利害関係者・公衆への利益）・消費者プライバシーに対する負の影響、予定している安全対策（サイバーセキュリティ・統制措置等）（規則§7152(a)）
- 本義務は、2026.1.1から適用開始となっているが、2025年以前に開始された処理については2027.12末までにリスク評価を完了すればよい。CPPA（当局）への年次報告書の提出期限は、2026年・2027年に実施するリスク評価については2028.4.1、2028年以降に実施するリスク評価については、評価実施の翌年の4.1）

CCPA上のセンシティブ個人情報（参考）

- **センシティブ個人情報の定義（1798.140（ae））**

  以下のいずれかを意味する

  （1）以下のいずれかを明らかにする情報

  （A）消費者の社会保障番号、運転免許証番号、州の身分証明書番号又はパスポート番号

  （B）消費者のアカウントログイン、金融口座、デビットカード又はクレジットカード番号と、アカウントへのアクセスに必要なセキュリティー若しくはアクセスコード、パスワード又は認証情報との組み合わせ

  （C）消費者の**正確な位置情報**：デバイスから得られ、半径1,850フィート（約564メートル）以下の円内で消費者の位置を特定するために現に利用され又は利用される予定のデータ（規則で定めるデータを除く）（1798.140（w））

  （D）消費者の人種若しくは民族的出自、宗教的又は思想上の信念又は組合員か否か

  （E）消費者の手紙、電子メール及びテキストメッセージの内容（但し事業者がその相手方である場合を除く）

  （F）消費者の遺伝データ

  （G）**消費者の中枢神経系又は末梢神経システムの活動を測定することによって生成される情報で、非神経情報から推測されない情報）（2025.1.1適用開始の改正）**

  （2）消費者を一意に識別する目的で行われる生体情報の処理

  （3）消費者の健康、性生活または性的指向に関して収集され、分析される個人情報

  （4）事業者が当該消費者が16歳未満であることを実際に認識している消費者の個人情報。なお、事業者が消費者の年齢を故意に無視した場合には、当該事業者は消費者の年齢について実際の認識を有していたものとみなされる

ADMTについての義務①

- 消費者に対する重要な決定にADMT(自動化された意思決定技術)を利用する事業者の義務
- ✓ 使用前の通知(規則§7220)
- ✓ アクセス権 (規則§7222)対応
- ✓ オプトアウト権(規則§7221)対応
- 「ADMT」とは、個人情報を処理し、計算処理を用いて人間による意思決定を代替する、または実質的に代替するあらゆる技術をいう。(規則§7001(e))
- ✓ 「人間による意思決定を実質的に代替する」:事業者が当該技術の出力結果を、人間の関与なしに意思決定のために用いること
- ✓ 「人間の関与」とは、以下のすべてを満たすことを要する(A) 人間の審査担当者が、当該技術の出力結果をどのように解釈し、意思決定に利用するかを理解していること(B) 当該技術の出力結果および意思決定を行い、または変更するために関連するその他の情報を確認し、分析すること© 上記(B)における分析に基づき、当該意思決定を行い、または変更する権限を有していること

ADMTについての義務②

- 「ADMT」とは、個人情報を処理し、計算処理を用いて人間による意思決定を代替する、または実質的に代替するあらゆる技術をいう。

✓ ADMTには、人間による意思決定を代替し、または実質的に代替するプロファイリングも含まれる。

✓ ADMTには、ウェブホスティング、ドメイン登録、ネットワーキング、キャッシング、ウェブサイトの読み込み処理、データ保存、ファイアウォール、アンチウイルス、アンチマルウェア、スパムおよびロボコールのフィルタリング、スペルチェック、計算機、データベースおよびスプレッドシートは含まれない。ただし、これらが人間による意思決定を代替しない場合に限る

✓ 「重要な決定」：金融/融資サービス、住宅、教育への登録、雇用/独立契約(業務委託)の機会/報酬、医療サービスの提供に関する承認・否認の決定（規則§7001(ddd)）

サイバーセキュリティ監査についての義務

- 以下のいずれかの要件を充足する場合に暦年毎にサイバーセキュリティ監査を実施しなければならない（規則§7120）

  ①前暦年に年間収益の50%以上を消費者の個人情報の販売・共有から得ている

  ②年間総収益がCCPA適用基準を充足し、かつ、前暦年に(i)25万人以上の消費者または世帯の個人情報を処理したこと若しくは(ii) 5万人以上の消費者のセンシティブ個人情報を処理したこと

- サイバーセキュリティ監査完了の証明書のCCPAへの提出の初回期限は、事業者の年間売上高が1億ドル超の場合は2028.4.1、5000万～1億ドルの場合は2029.4.1、5000万ドル未満の場合は、2030.4.1。それ以降年次報告（規則§7121）

- サイバーセキュリティ監査の実施が義務付けられるすべての事業者は、適格であり、かつ客観性および独立性を有する専門家を用いて当該監査を実施しなければならない。当該監査は、監査専門職において一般に受け入れられている手続および基準に従って実施されなければならず、これには、米国公認会計士協会、公開会社会計監督委員会、情報システム監査統制協会、国際標準化機構によって提供または採択された手続および基準が含まれる（規則§7122）

- 規則§7123(c)には、インシデント対応を含む18項目の評価項目が決められている

- サイバーセキュリティ監査完了の宣誓・署名付の証明書を暦年毎にCPPAに提出（規則§7124）

他の州の包括法について

3

カリフォルニア以外の各州の包括的プライバシー法制定①

- **カリフォルニア**以外の各州で包括的プライバシー法の制定の動きが活発
  - 2022年までの間は以下の順で成立した（施行済）
    - **ヴァージニア州消費者データ保護法**（**2023年1月1日**施行）
    - **コロラド**州プライバシー法（**2023年7月1日**施行）
    - **ユタ**州消費者プライバシー法（**2023年12月31日**施行）
    - **コネチカット**州個人情報・プライバシー・オンライン監視法（殆どの条文は、**2023年7月1日**施行。なお、コネチカット州法の改正で、18歳未満の消費者についての追加の義務が導入され、一部は、2024年7月1日、残りは、2024年10月1日施行）
  - 2023年になって相次いで以下の州でも成立
    - **テキサス**州（**2024年7月1日**施行）
    - **オレゴン**州（**2024年7月1日**施行）
    - **モンタナ**州（**2024年10月1日**施行）
    - **アイオワ**州（**2025年1月1日**施行）
    - **デラウェア**州（**2025年1月1日**施行）
    - **テネシー**州（**2025年7月1日**施行）
    - **インディアナ**州（**2026年1月1日**施行）

    ※ なお、2023年6月成立の**フロリダ**州法は、後述する子どもに関する定めを除き、大規模テクノロージー企業のみに適用され、他州の包括的プライバシー法とは異なるため、紹介していない

カリフォルニア以外の各州の包括的プライバシー法制定②

- カリフォルニア以外の各州で包括的プライバシー法の制定の動きが活発
  - 2024年になって相次いで以下の州でも成立
    - **ニュージャージー州（2025年1月15日に施行予定）**
    - **メリーランド州（2025年10月1日に施行予定）**
    - **ネブラスカ州（2025年1月1日に施行予定）**
    - **ニューハンプシャー州（2025年1月1日に施行予定）**
    - **ケンタッキー州（2026年1月1日に施行予定）**
    - **ミネソタ州（2025年7月31日に施行予定）**
    - **ロードアイランド州（2026年1月1日に施行予定）**

米国包括州法の適用場面①

- **いずれも雇用関係や企業間取引（B2B）には適用されないことは共通**
- ヴァージニア州：ヴァージニア州で事業を行う者、またはヴァージニア州の居住者**（B to B・雇用関係除く）**を対象とした製品またはサービスを生産する者で、(i)暦年中に10万人以上の消費者の個人情報を管理または処理する者、または(ii)2万5千人以上の消費者の個人情報を管理または処理し、個人情報の販売から総収入の50%以上を得る者に適用される（§ 59.1-572.A）
- コロラド州：①コロラド州で事業を行っている、またはコロラド州の居住者**（B to B・雇用関係除く）**を意図的に対象とした製品やサービスを生産または提供しており、かつ、②(i)1暦年中に少なくとも10万人以上の消費者の個人情報を管理または処理している、または(ii)個人情報の「販売」から収益を得ているか商品やサービスの価格の割引を受けており、25,000人以上の消費者の個人情報を処理または管理している場合
- ユタ州：①ユタ州内で事業を行う、またはユタ州の居住者**（B to B・雇用関係除く）**を対象とした製品・サービスを生産しており、**かつ**、②年間収益が2,500万米ドル以上であり、③以下の(i)又は(ii)のいずれかを充足する者(i)1暦年中、10万人以上の消費者の個人情報を管理または処理する場合(ii)企業の総収益の50%以上を個人情報の「販売」から得ており、2.5万人以上の消費者の個人情報を管理または処理している場合
- コネチカット州：コネチカット州で事業を行うか、コネチカット州の居住者**（B to B・雇用関係除く）**を対象とした製品またはサービスを製造しており、かつ、前暦年中に以下のいずれかを行っていた事業者①少なくとも10万人の消費者（コネチカット州の居住者）の個人情報を管理または処理（支払い取引の完了のみを目的として管理または処理される個人情報を除く）②少なくとも2.5万人の消費者の個人情報を管理または処理し、総収益の25%以上を個人情報の販売から得ている（なお、消費者健康データ管理者の義務は、コネチカット州で事業を営む者及びコネチカット州住民をターゲットとして製品またはサービスを提供する者に広く適用される）

米国包括州法の適用場面②

- **テキサス州**：①テキサス州で事業を行い又はテキサス州の居住者が**消費する**製品やサービスを製造しており、かつ、②個人データの処理または販売に従事しており、かつ、③**米国中小企業庁（SBA）が定義する中小企業**（原則は従業員500人未満の独立企業であるが**多数の例外あり**）でないこと
- テネシー州：テネシー州内でビジネスを行う、またはテネシー州の居住者を対象とした製品又はサービスを製造する者で、1暦年中に以下のいずれかに該当する者に適用される：①少なくとも10万人の消費者の個人情報を管理または処理する②少なくとも2.5万人の消費者の個人情報を管理または処理し、個人情報の販売から総収入の50%以上を得ている
- モンタナ州：モンタナ州で事業を行う者、またはモンタナ州の居住者を対象とした製品又はサービスを製造する者で、以下のいずれかに該当する者適用される　①5万人以上の消費者の個人データを管理または処理する。ただし、決済取引の完了のみを目的として管理または処理される個人データは除く。②2.5万人以上の消費者の個人データを管理または処理し、個人データの販売から総収入の25%以上を得ている場合
- アイオワ州：アイオワ州で事業を行い又はアイオワ州の居住者を対象とした製品やサービスを製造する者で、1暦年中に以下のいずれかに該当する者に適用される：①少なくとも10万人のアイオワ州居住者の個人情報を管理または処理している②少なくとも2.5万人のアイオワ州住民の個人情報を管理または処理し、総収入の50%以上を個人情報の販売から得ている場合

米国包括州法の適用場面③

- インディアナ州：インディアナ州で事業を行う者、またはインディアナ州の居住者を対象とした製品やサービスを製造する者で以下のいずれかに該当する者に適用される：①10万人以上の顧客の個人情報を管理または処理している。②少なくとも2.5万人のインディアナ州の居住者の個人データを管理または処理し、個人データの販売から総収入の50%以上を得ている
- デラウェア州：デラウェア州で事業を行う者、または州の居住者を対象とする製品もしくはサービスを製造する者であって、前暦年に以下のいずれかを行った者に適用される：①3.5万人以上のデラウェア州の居住者の個人情報を管理または処理する。ただし、支払取引を完了する目的でのみ管理または処理される個人情報は除く。(2)1万人以上のデラウェア州の居住者の個人情報を管理または処理し、個人情報の販売から総収入の20%以上を得ている
- オレゴン州：オレゴン州内で事業を行う者、またはオレゴン州の住民に製品もしくはサービスを提供する者で、1暦年中に以下の行為を行った者に適用される：①10 万人以上のオレゴン州住民の個人情報を管理または処理する場合（支払取引を完了する目的のみで管理または処理される個人情報を除く）②2.5万人以上の消費者の個人情報を管理または処理する一方、個人情報の販売から年間総収入の25%以上を得ている場合
- **ロードアイランド州**：直前の暦年において以下のいずれにも該当するコントローラーに適用される。ロードアイランド州内で事業を行っている、またはロードアイランド州の居住者を対象とした製品またはサービスを提供している。かつ、次のいずれか一方を満たす場合①少なくとも35,000人のロードアイランド州の顧客の個人データを管理または処理していること②10,000人のロードアイランド州の顧客の個人データを管理または処理しており、かつ個人データの販売から総収入の20%超を得ていること（**ただし、プライバシー通知の要件は、**ロードアイランド州の顧客の個人識別情報を収集・保存・販売する商業的ウェブサイトまたはインターネットサービスプロバイダーであるコントローラーにも**広く適用**）

米国包括州法の適用場面④

- ニュージャージー州：ニュージャージー州で事業を行うか、ニュージャージー州の住民を対象とした製品やサービスを提供するコントローラーであり、かつ、①ニュージャージー州の10万人以上の消費者のデータを管理または処理するか、または② ニュージャージー州の2万5千人以上の消費者の個人情報を管理または処理し、個人情報の販売から収益を得る（または商品やサービスの価格において割引を受ける）場合
- ネブラスカ州：①ネブラスカ州で事業を行う、または**ネブラスカ州の住民が消費する製品やサービスを生産する者**または②個人データを処理するまたは販売に従事する者であって、連邦中小企業法で定められた中小企業ではない者
- ニューハンプシャー州：個人情報の処理の目的と手段を決定する者であり、ニューハンプシャー州で事業を行う者、またはニューハンプシャー州の住民を対象とした製品やサービスを生産する者で、1年間の期間内に以下のいずれかに該当する者①3万5千人以上の一意のニューハンプシャー州消費者の個人情報を管理または処理する者②1万人の一意のニューハンプシャー州消費者の個人情報を管理または処理し、個人情報の販売から総収入の25%以上を得ている者
- ケンタッキー州：①暦年内に、10万人以上のケンタッキー州の消費者の個人情報を管理または処理する者又は②2万5千人以上のケンタッキー州の消費者の個人データを管理または処理し、個人データの販売から総収入の50%以上を得ている者
- メリーランド州：個人情報の処理の目的と手段を決定する者で、メリーランド州で事業を行う者、またはメリーランド州の住民を対象とした商品やサービスを提供し、暦年内に以下のいずれかに該当する者①3万5千人のメリーランド州の消費者の個人情報を管理または処理する者②1万人以上のメリーランド州の消費者の個人情報を管理または処理し、個人情報の販売から総収入の20%以上を得ている者

COPPA規則の改正を含む子供関係の規制について

4

米国の子供関係の規制の全体像①

- **データ保護法（前掲）**
  - 連邦法：**COPPA（2025年に規則が改正）**
  - 州法
  - ✓ 包括州法
  - ✓ 個別州法：カリフォルニア州**Age-Appropriate Design Code Act(現在地裁の仮差止命令により執行が出来ない状態)、アーカンソー州オンラインプライバシー法、ニューヨーク州児童データ保護法**

- **不公正・欺瞞的行為/慣行の禁止による消費者保護**
  - 連邦法：FTC法5条。州法：FTC法5条に相当するような各州の規制

- **年齢シグナル法（アプリストア責任法）**
  - **テキサス**（2026.1.1から適用開始予定であったが、米国連邦地方裁判所テキサス州西地区オースティン支部が2025年12月23日付で**仮差止命令**を出したため、同日での施行は一旦されていない。テキサス州司法長官は、米国第5巡回区連邦控訴裁判所への控訴を行なっており、今後の動向が引き続き注目される）
  - ユタ、ルイジアナ、カリフォルニア

米国の子供関係の規制の全体像②

- **ソーシャルメディア規制**
  - 州法によりソーシャルメディアについて様々な規制を課す立法がなされている。州によりアプローチが異なり、一定年齢未満の利用禁止、年齢確認/保護者同意、**アルゴリズム/中毒性フィード規制**、特定有害コンテンツ規制、利用時間制限/夜間利用制限、学校での利用禁止、学校でのリテラシー教育、ダイレクトメッセージの制限、警告表示・情報公開義務、保護者用管理ツール提供等がある
  - 多くの州の規制が修正1条違反により差止めになっている。差止めとなっていないものとして、**ニューヨークのSAFE for Kids Act**では、ウェブサイト・アプリ等で「依存性フィード」（ウェブサイト、オンラインサービス、オンライン/モバイルアプリケーションの利用者によって生成/共有された複数のメディアコンテンツが、同時または順次に、利用者に表示されるために**推奨、選択、または優先順位付け**される仕組み。ただし、その推奨、選択または優先順位付けが、全部または一部において、**当該利用者またはその利用者のデバイスに関連付けられた情報に基づいて行われる**場合に限る。例：各ユーザの視聴履歴に応じて次に再生する候補となる動画を推奨するような仕組み）をサービスの重要な構成部分とするものが、保護者の同意なしに18歳未満の未成年者へ「依存性フィード」を提供することを禁止している（規則公布から180日で適用開始予定だが、規則案が公表されパブコメが行なわれた状況であり、まだ適用開始になっていない）

米国連邦法COPPAの概要①

- COPPA＝Children's Online Privacy Protection Act of 1998
- COPPAに違反した場合には、**FTC法5条**違反により執行される可能性がある
- 2025.6にCOPPA規則が改正され規制が強化された。原則**2026.4.22**から規則改正による義務が適用開始
- 適用対象事業者：13歳未満の子ども向けウェブサイトの運営者・オンラインサービス提供者、13歳未満の子どもから個人情報を取得していることを現実に認識しているウェブサイト運営者・オンラインサービス提供者→実務上は、**混合対象**サービスが重要であり、**中立的なAge Gate**により、13歳以上と判断された者については対応しないことが可能（**規則改正**で、§ 312.2で混合対象サービスについて明文化された）
- 適用対象となる個人情報は以下（規則§ 312.2）

  「オンラインで収集される、特定の個人を識別できる情報をいい、以下を含む」（**例示列挙**）。「(1) 名および姓(2) 番地および市区町村名を含む、自宅その他の物理的住所(3) 本条に定義されるオンライン連絡先情報(4) 本条に定義されるオンライン連絡先情報と同様の方法で機能するスクリーンネームまたはユーザー名(5) 電話番号(6) 社会保障番号、州発行の身分証明書番号、出生証明書番号、またはパスポート番号などの、(7) 時間の経過および異なるウェブサイトまたはオンラインサービス間においてユーザーを認識するために使用され得る永続的識**政府が発行する識別番号（規則改正で追加）**別子。これには、クッキーに保存される顧客番号、インターネット・プロトコル（IP）アドレス、プロセッサまたは端末のシリアル番号、もしくは固有のデバイス識別子などが含まれるが、これらに限定されない。(8) 当該ファイルに子どもの画像または音声が含まれる写真、動画、または音声ファイル(9) 番地および市区町村名を特定できる程度に十分な位置情報(10) 指紋、手形、網膜パターン、虹彩パターン、DNA配列を含む遺伝情報、声紋、歩行パターン、顔テンプレートまたはフェイスプリントなど、個人を自動または半自動で識別するために使用され得る**生体識別情報（規則改正で追加）**(11) 本定義に記載された識別子と組み合わされ、事業者がオンラインで子どもから収集する、当該子どもまたはその親に関する情報」

米国連邦法COPPAの概要②

- **通知義務**（規則§312.4）：COPPAの適用がある事業者は、①**保護者への直接通知**として、どんな情報を子どもから収集して利用するか、事業者の情報についての開示のプラクティスについて通知する義務に加えて、②**ウェブサイト・オンラインのサービス画面上での所定事項の通知**もしなければならない。**規則改正**で、①保護者への直接通知に、個人情報を何に使うか及び第三者への開示の場合の追加の通知義務を追加し、②ウェブサイト・オンラインのサービス画面上での所定事項の通知義務も強化した
- **同意取得義務**（規則§312.5）子どもからの個人情報取得の前に、あらかじめ、親から**検証可能な同意**を取得しなければならない。一定の一回的な情報利用（規則§ 312.5(c)(3)）や内部運用のための永続識別子の利用（規則§ 312.5(c)(7)。なお、**規則改正**により、この場合でも、当該永続識別子についての所定の通知は必要：規則§312.4(d)(3)）等の同意取得義務の例外もあり。**規則改正**により、①**収集・利用**用の同意と②**第三者開示**用の同意（不可欠なものを除く）を**分けて**同意を取る義務が追加。また、**規則改正**で新しい親からの検証可能な同意取得方法が追加。
- **親の請求に応じて**、子どもから収集された個人情報を**確認**し、そのさらなる利用または保持を**拒否**するための合理的な手段を提供しなければならない（規則§312.6）
- 子どもがアクティビティ（ゲームや懸賞等）に参加するための条件として、**必要となる以上の情報を取得してはならない**（規則§ 312.7）
- 子どもから収集した個人情報の機密性、安全性、完全性を保護するための合理的な手順を確立し維持しなければならない→**文書化された情報セキュリティプログラム**を策定・維持・実施しなければならず、**年次**リスク評価、第三者ベンダのデューデリジェンスが必要（規則§312.8）（**規則改正**で導入）
- 事業者は、オンラインで子どもから収集した個人情報を、その情報が収集された**目的を果たすために合理的に必要な期間のみ保持**し、無期限に保持してはならない+**文書化された保持方針**を策定・実施・維持しなければならない（規則§312.10）こととなった（**規則改正**で導入）

米国COPPA規則の改正内容

- **COPPA規則の改正内容**
  - ターゲット広告目的での第三者とのデータ共有に対する個別の保護者の同意を要求
  - 子どもの個人情報の保持を、収集された特定の目的を果たすために合理的に必要な期間のみに制限し、子どもの個人情報を無期限に保持することを禁止し、書面によるデータ保持ポリシーの採用を要求
  - 子ども向けとミックス（混合）の定義明確化
  - 「個人情報」の定義について、生体認証識別子および社会保障番号以外の政府発行の識別子を含むように拡大
  - 保護者への通知要件の拡大
  - 検証可能な保護者の同意を得るための追加的な方法の列挙
  - データセキュリティ要件の強化
  - セーフハーバープログラムの監督と透明性の向上

年齢シグナル法(アプリストア責任法)①

- 米国では近時、複数の州で、未成年者のアプリ利用の際の安全を強化するための年齢シグナル法(アプリストア責任法)が可決されている
- アプリストア責任法は、たとえば、以下のような規律を課している

  ①アプリストアは、ユーザーが当該アプリストアでアカウント作成をする際、年齢確認を行う

  ②アプリ開発者は、各アプリ及びアプリを通じて購入できる各商品に年齢レーティングを設定する

  ③アプリ開発者は、アプリストアから受領した年齢確認情報を使用して各アプリユーザーの年齢区分を確認し(アプリ開発者自身がユーザーに対して直接年齢確認を行う必要はない)、ユーザーが未成年者(18歳未満)の場合には、ユーザーの保護者の同意の有無を確認するためのシステムを構築・実施する

  ④アプリ開発者は、アプリに適用される利用規約又はプライバシーポリシーに重要な変更を加える際には事前にアプリストアへ通知し、当該通知を受けたアプリストアは保護者の同意を更新する、といった規律を課している

年齢シグナル法(アプリストア責任法)②

- 現在アプリストア責任法が可決されている州
  - テキサス州(2026年1月施行予定であったが、2025年12月23日にテキサス州連邦地裁で憲法違反を理由に仮差止命令が出されたため未施行)
  - ユタ州(2025年5施行予定。ただしアプリストア及びアプリ開発者の遵守義務は2026年5月から有効になります。)
  - ルイジアナ州法(2026年7月施行予定。2025 Louisiana Laws Revised Statutes Title 51 - Trade and Commerceの§51:1771～1775)
  - カリフォルニア州(2027年1月施行予定。アプリストアだけでなくOS提供事業者にも義務が課されることやアプリの同意に保護者の同意を求めないこと、モバイルデバイスのみならずPC等向けのアプリも対象となることなど他の3州とはやや内容が異なる)
- テキサス州に続いて、今後、他の州法についても同様に差止訴訟が提起される可能性がある

年齢シグナル法(アプリストア責任法)③

- 施行差止がされる可能性があるとはいえ、こうしたアプリストア責任法を制定する動きは今後他の州にも広がっていくことが予想される
- 米国のユーザーが利用するアプリを提供している事業者においては、アプリストアが公表しているアプリストア責任法への対応方針(Appl Store、Google Play)などを確認の上、必要な対応を前もって検討・整理しておくことが推奨される
- 実際にアプリストア責任法に対応することによりユーザーの年齢確認情報をアプリストアから**受領**する場合、13歳未満と確認されたユーザーに関して、COPPA(児童オンライン保護法)を遵守する必要が生じることにも注意が必要。COPPAは、(a)13歳未満の児童を対象としたウェブサイト又はオンラインサービスの運営者、又は(2)13歳未満の児童から個人情報を収集又は管理していることを実際に知っている運営者に適用されるところ、アプリストアがアプリ開発者に、当該ユーザーが13歳未満であることを通知した場合、開発者は、13歳未満の児童から個人情報を収集又は管理していることを「実際に知っている」とみなされるためである

連邦法の改正の動向（119th Congressで審議されているものの例）

- Children and Teen's Online Privacy Protection Act（COPPA 2.0）：現行COPPAで保護される年齢（13歳未満）を、17歳未満まで拡大。子どもおよびティーンに対するターゲティング広告の禁止や、未成年者自身または保護者がオンラインサービス上の情報を削除できる「イレイサーボタン」の設置を義務化

- Kids Online Safety Act（KOSA：上院版/下院版）：オンラインサービス事業者に対して、17歳未満の未成年者が利用するプラットフォームについて想定される性的搾取等の一定のリスクについての所定の対応、通報受付窓口、保護者・未成年向けの保護ツール等を義務化。上院版の方が厳格。なお、118th Congressでは、COPPA2.0+KOSAをまとめた Kids Online Safety and Privacy Act（KOSPA）というパッケージが上院を通過するも、下院を通過せず成立しなかった

- App Store Accountability Act：州のアプリストア責任法と同様の規制

- Shielding Children's Retinas from Egregious Exposure on the Net Act（SCREEN Act）：商業目的のウェブサイト等のインタラクティブなコンピュータサービスを対象とし、18歳未満の未成年者がオンラインポルノコンテンツ等の有害なコンテンツにアクセスすることを防ぐ年齢ゲートシステムの導入義務を課す法案

- Safeguarding Adolescents From Exploitative BOTs Act（SAFE BOTs Act）：17歳未満の未成年者が利用する消費者向けAIチャットボットに特化した規制（AIシステムであることの明示、自傷行為に関する入力があった場合の危機支援情報の提示、長時間使用に対する注意喚起、ポルノコンテンツ等の有害コンテンツに対応するポリシー策定等）

- 他にもこの分野に関する様々な法案が提出されている

集団訴訟について

5

集団訴訟総論

- **私的訴権+法定損害賠償請求権**がある古い法令を現代の技術にあてはめて適用して、和解狙いで集団訴訟を提起する事例が増加している
- 多くの企業に請求のレターが届いており、対応に注意が必要
- よく使われるのは以下の法律

✓ VPPA：連邦法

✓ イリノイ州のBIPA等

✓ カリフォルニア州のCIPA

VPPA（連邦法）

- ビデオプライバシー保護法（Video Privacy Protection Act）は、ビデオテープサービスプロバイダーによる消費者の個人情報開示に原則消費者の**同意**を要求する法律
- 元々は、レンタルビデオ店等でのレンタルビデオの履歴の第三者への提供を規制することを目的とした法律として1988年に制定されている
- 違反には実損又は2,500ドルという**法定損害**のいずれか高い方の賠償請求権が定められている
- ウェブサイトで動画を視聴する機能を有しているウェブサイトが、その動画を視聴した個人の個人情報をSNSや分析サービス事業者等に提供していること等が集団訴訟の原因となっている

イリノイ州のBIPA等

- 生体情報・生体識別子に適用され、所定の通知・**書面**同意、安全管理等を要求
- 違反には実損又は1,000ドル（故意・重過失の場合には5,000ドル）という**法定損害**のいずれか高い方の賠償請求権+**私的訴権**が定められている
- 他州でも類似する法律が既に成立したり、法案が提出されたりしている
- 顔認証を含む生体認証等で集団訴訟が起きている

カリフォルニア州のCIPA

- CIPAは、盗聴規制の法令。**通信の両当事者同意**がない場合に盗聴を規制
- 1件の違反につき最大5,000ドルの**法定損害賠償**を請求可能+**私的訴権**あり
- ウェブサイト上での行動履歴等の提供行為やチャットボット設置等を行なうウェブサイト運営事業者や当該技術の提供者について集団訴訟が提起されている
- 原告側代理人の主張：①ユーザーのオンライン行動をオンライントラッキング技術を通じて第三者へ送信する企業は、ユーザーの事前同意なしに通信を盗聴しているのでCIPA違反であるとの主張②オンライントラッキング技術が、ペンレジスタ又はトラップ・アンド・トレース装置に該当するとして、裁判所の命令なしに装置を設置する行為がCIPA違反であるとの主張
- 近時、元々の想定と異なる法令の使い方がされており、2025年に改正により適用範囲を狭めて混乱を防ごうとする動きがあったが、改正は、成立しなかった
- 従来、CCPA対応としては、販売・共有のためのオプトアウト対応を原則と考えていたが、CIPAの集団訴訟の対策を考えると、保守的には、GDPR型のオプトイン方式のクッキーバナーの採用が安全といえる