海外法規制違反 111 事例集

GDPR、CCPA、COPPA、PIPA、LGPD 等

2023 年～2026 年 5 月公表
世界 21 の国・地域の
執行・制裁事例 111 件を整理・解説

【サンプル版】
5 事例収録

石塚リサーチ
創業 1989 年
海外調査実績 500 件以上
https://www.ishizuka-research.com

ISHIZUKA
RESEARCH
SINCE 1989

Adobe（ソフトウェア開発・クラウドサービス事業者）
ROSCA 違反で 1 億 5,000 万ドル（約 225 億円）相当の和解パッケージを提供
（国：米国）（公表日 2026 年 3 月 23 日）【消費者保護法違反】

事案概要

米国司法省は、アドビがサブスクリプション・サービスの解約を不当に妨げたとするオンラインショッパー信頼回復法（ROSCA）違反の疑いを解決するため、総額 1 億 5,000 万ドル相当の和解に応じたと発表した。同社は、年間契約プランへの加入時に高額な早期解約料の存在を十分かつ明確に開示していなかったほか、解約手続において多数の画面遷移や確認操作を利用者に求めるなど、複雑な解約プロセスを設計していたと指摘された。

米国当局は、こうした重要条件の開示不足や解約妨害的な画面設計（UI/UX）を「消費者を意図的に騙すような画面設計（ダークパターン）」として問題視した。今回の合意に基づき、同社は金銭的負担に加え、自動更新契約や解約料に関する重要条件の明確な表示、利用者が容易に解約できる仕組みの導入等を求める命令に従うこととなった。
出所：Adobe Agrees to $150 Million Settlement and Injunction to Resolve Alleged Violations of Restore Online Shoppers' Confidence Act
https://www.justice.gov/opa/pr/adobe-agrees-150-million-settlement-and-injunction-resolve-alleged-violations-restore-online

主な適用法規

オンラインショッパー信頼回復法（ROSCA: Restore Online Shoppers' Confidence Act）
第 4 条第 1 号：課金情報取得前に、すべての重要な契約条件を明確かつ目立つ形で開示する義務
第 4 条第 2 号：課金前に消費者の明示的なインフォームド・コンセントを得る義務
第 4 条第 3 号：消費者が継続的な課金を停止するための「簡便な手続きを提供する義務」
https://www.ftc.gov/system/files/documents/statutes/restore-online-shoppers-confidence-act/online-shoppers-enrolled.pdf

日本企業への示唆

本事例は、米国でサブスクリプション型ビジネスを展開する日本企業に対し、顧客の「解約のしやすさ」を契約獲得と同様に重視すべきであることを強く示唆している。米国当局は、解約を意図的に困難にする「ダークパターン」を厳しく監視しており、ROSCA に基づき、契約条件の不透明な提示や複雑な解約手続きを重大な法違反とみなすのである。特筆すべきは、今回のように高額な金銭的制裁に加え、将来の業務改善を強制する恒久的差止命令が下される点である。

日本企業は、UX デザインが消費者を欺く構造になっていないか、法務とマーケティング部門が連携して点検を行う必要がある。解約プロセスを、申し込み時と同等かそれ以上に簡便なものに設計することは、単なる顧客サービスではなく、巨額の法的リスクを回避するための経営上の防波堤となるのである。

The Walt Disney Company（動画配信・エンターテインメント事業）
CCPA 違反で 275 万ドル（約 4 億円）の制裁金 –「オプトアウトしてもデータ共有が継続する構造」を問題視（国：米国）（公表日 2026 年 2 月 11 日）【個人情報保護法違反】

事案概要

カリフォルニア州司法長官は 2026 年、The Walt Disney Company に対し、カリフォルニア州消費者プライバシー法（CCPA）違反を理由として 275 万ドル（約 4 億円）の制裁金を科したと公表した。当局によれば、Disney は Disney+、Hulu、ESPN など複数サービスにおいて、利用者へ個人データ共有停止（オプトアウト）機能を提供していたものの、その設定が一部デバイスやサービスへ適切に反映されていなかったということである。

具体的には、利用者が 1 つのデバイスやサービス上で、広告目的等のデータ共有停止（オプトアウト）を選択しても、別デバイスや別サービスでは共有が継続されるケースが存在していた。また当局は、利用者へ複数回にわたり別々のオプトアウト操作を求める構造についても問題視した。本件では、オプトアウト機能自体は存在していたにもかかわらず、「実際には完全に停止できていなかった」点が重視されている。
出所：California Won’t Let It Go: Attorney General Bonta Announces $2.75 Million Settlement with Disney for Violating CCPA
https://oag.ca.gov/news/press-releases/california-wont-let-it-go-attorney-general-bonta-announces-275-million

主な適用法規

CCPA：カリフォルニア州消費者プライバシー法 / CPRA：カリフォルニア州プライバシー権法（消費者のオプトアウト権・データ共有停止権関連規定）

日本企業への示唆

本件の本質は、「形式的にオプトアウト機能を用意しているだけでは不十分」と判断された点にある。従来、多くの企業では、利用者が設定画面上で「オプトアウト」を選択できれば一定の法対応を行っているとの認識があった。しかし近年の海外執行では、単に機能が存在するだけではなく、本当に全サービスへ反映されるか、別デバイスでも有効か、利用者へ過度な操作負担を与えていないか等、実際にデータ共有停止が実現されているかまで問われる傾向が強まっている。

本件では、情報漏えいや不正アクセスではなく、「オプトアウト画面設計（UI/UX）や設定反映不備」自体が約 4 億円規模の支払い措置につながった。本件は動画配信事業者だけでなく、SaaS、EC、広告事業、アプリ、複数サービス展開企業など、日本企業全般に重要な示唆を与える。特にグループ企業横断、複数アプリ横断、クロスデバイス型のデータ共有を行っている企業では「一部だけ停止」「別サービスでは継続」といった構造が、今後海外規制当局から問題視される可能性がある。

特に近年の米国では、「利用者が簡単かつ完全に権利行使できるか」を重視する方向へ執行が強まっており、「設定画面が存在しているから問題ない」という従来型感覚だけでは対応できない時代になっている点に注意が必要である。

Reddit（米国の大手ソーシャルメディア企業）

英国における 13 歳未満の子供の個人データの違法処理で約 27 億円の制裁金（国：英国）（公表日 2026 年 2 月 24 日）【個人情報保護法違反、児童オンラインプライバシー保護違反】

事案概要

英国情報コミッショナー事務局（ICO）は 2026 年 2 月、SNS サービスを運営する Reddit, Inc. に対し、子供のプライバシー保護に関する不備を理由として 1,447 万ポンドの制裁金を科した。ICO は、Reddit が利用者の年齢を十分に確認しないままサービスを提供していた結果、13 歳未満の子供が多数利用していた可能性があると判断した。また、子供の利用に伴うリスクを十分に評価しておらず、子供を不適切または有害なコンテンツから保護するための措置も不十分であったと指摘した。

さらに、子供の個人情報の取扱いに伴うリスクを評価するための DPIA（データ保護影響評価）の実施が不十分であった点も問題視された。また ICO は、Reddit が 2025 年 7 月に導入した「アカウント開設時にユーザーが自分の年齢を自己申告する」方式では容易に偽れるため不十分と判断した（より厳格な年齢確認方法を用いる必要がある）。
出所：Monetary Penalty Notice: Reddit, Inc.
https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2026/02/reddit-issued-with-1447m-fine-for-children-s-privacy-failures/
https://ico.org.uk/action-weve-taken/enforcement/2026/02/reddit-inc

主な適用法規

■UK GDPR 第 6 条・第 8 条：個人データ処理に必要な適法な根拠、および 13 歳未満の子供のデータ処理に際する親権者の同意取得を義務付ける条項。
■UK GDPR 第 5 条第 1 項(a)：個人データは適法・公正かつ透明な方法で処理されなければならないとする透明性原則を定める条項。
■UK GDPR 第 35 条：高リスクな処理を行う前に DPIA（データ保護影響評価）の実施を義務付ける条項。
https://www.legislation.gov.uk/eur/2016/679/contents

日本企業への示唆

本事例は、子供がアクセスする可能性のあるオンラインサービスにおいて、年齢確認の実効性が法的義務として厳格に問われることを示している。Reddit は利用規約で 13 歳未満の利用を禁止していたにもかかわらず、技術的な年齢確認を怠ったとして制裁を受けた。「規約に書いてあれば足りる」「自己申告で十分」という考え方は英国では通用しない。

日本企業がゲーム・SNS・動画配信など子供がアクセスしうるサービスを英国・欧州向けに展開する場合、身分証明書の確認や第三者機関による年齢認証など技術的に実効性のある年齢確認手段の実装が求められる。また、子供のデータ処理に関する DPIA（データ保護影響評価）の事前実施も義務であり、サービス設計段階から組み込む必要がある。

日本国内でも子供向けサービスの規制強化の議論が進んでおり、英国・EU の執行動向は今後の国内規制の方向性を先取りしている可能性がある点も認識しておく必要がある。

FREE（Free Mobile／Free）フランス大手通信事業者
GDPR 違反で総額 4,200 万ユーロ（約 67 億円）の制裁金（国：フランス）
（公表日 2026 年 1 月 14 日）【個人情報保護法違反】

事案概要

フランス個人情報保護委員会（CNIL）は、大手通信事業の Free Mobile および Free に対し、大規模な個人データ漏えいと不十分なセキュリティ対策を理由に、前者へ 2,700 万ユーロ、後者へ 1,500 万ユーロの制裁金を科した。攻撃者が両社の情報システムに侵入し、2,400 万件の契約データ（国際銀行勘定番号を含む）に不正アクセスしたことが発端である。調査の結果、特に従業員のリモートワークに使用されている VPN 認証の脆弱性や、異常検知能力の欠如など、GDPR 第 32 条が求める適切な技術的・組織的安全管理措置が欠如していたと認定された。

また、GDPR 第 34 条に基づく「利用者（データ主体）への通知内容」が不十分で、影響や必要な対策を利用者が理解できなかった点も問題視された。さらに Free Mobile は、旧契約者データを過剰に長期間保存し、GDPR 第 5 条 1(e)の保存期間制限原則にも違反していた。
出所：Sanction à l'encontre de la société FREE
https://www.cnil.fr/fr/sanction-free-2026

主な適用法規

GDPR（一般データ保護規則）第 32 条・第 34 条
GDPR 第 32 条は、管理者および処理者に対し、個人データを保護するための適切な技術的・組織的安全管理措置を講じる義務を定める規定である。暗号化、アクセス管理、脆弱性管理、可用性確保、定期的な評価などが求められる。

第 34 条は、個人データ侵害が個人の権利・自由に高いリスクをもたらす場合、遅滞なくデータ主体へ通知する義務を定める。通知には侵害の性質、影響、推奨される対策などを明確に含める必要がある。両条文は、侵害防止と発生時の透明性確保を目的とする中核規定である。
https://eur-lex.europa.eu/eli/reg/2016/679/oj

日本企業への示唆

本件は、GDPR 第 32 条が求める安全管理措置の水準が極めて高く、基本的な脆弱性管理の不備だけでも巨額制裁につながることを示すものである。日本企業が EU 居住者の個人データを扱う場合、VPN 認証、アクセス管理、ログ監視、異常検知など、侵害を前提とした多層的防御を実装し、定期的に評価・改善する体制が不可欠である。

また、侵害発生時には GDPR 第 34 条に基づき、影響範囲、リスク、推奨対策を明確に示した通知を迅速に行う必要がある。通知内容が曖昧であれば、それ自体が違反と評価される。さらに、旧契約者データの過剰保存も問題視された点から、保存期間の設定と削除プロセスの実効性確保が重要である。日本企業は、形式的な規程整備ではなく、実務運用の実効性を継続的に検証する姿勢が求められる。

イタリアの保育園
園児写真・監視カメラ運用で約 170 万円の制裁　―　「保護者同意があっても正当化されない」と判断（国：イタリア）（公表日 2025 年 11 月 18 日）【個人情報保護法違反】

事案概要

欧州データ保護会議（EDPB）は 2025 年、イタリアのデータ保護当局（Garante）が、保育園に対し、未成年者の個人データ処理に関する複数の GDPR 違反を理由として、1 万ユーロ（約 170 万円）の制裁金を科した事案を公表した。本件で問題となったのは、保育園側が、園児らの写真や映像をウェブサイトや Google Maps プロフィール等へ掲載していた点である。当局によれば、掲載されていたのは、睡眠中の様子、食事中の様子、おむつ交換に関連する場面など、極めて私的・繊細な状況を含む内容だった。また、園内には監視カメラも設置されていたが、必要な手続や法的整理が不十分だった点も問題視された。

保育園側は、保護者から同意を取得していたとしていたが、イタリア当局は、「親が同意していても、子供の写真や映像をインターネット上に公開することが子供の利益に反する場合がある」と判断した。さらに当局は、保護者が実質的に写真利用への同意を拒否しにくい構造になっていた点も問題視した。本件では、制裁金、データ処理禁止、画像削除命令などが命じられている。
出所：Minors: Italian SA sanctions nursery school. Cameras installed without safeguards and photos of children published online
https://www.edpb.europa.eu/news/national-news/2025/minors-italian-sa-sanctions-nursery-school-cameras-installed-without_en

主な適用法規

- GDPR 第 5 条第 1 項(a)（適法性・公正性・透明性原則）
- GDPR 第 6 条（個人データ処理の適法根拠）
- GDPR 第 35 条（データ保護影響評価／DPIA）

日本企業への示唆

本件は、保育事業や教育事業を営む企業に限らず、子供の写真や動画を取り扱う可能性のある日本企業全般にとって重要な示唆を含んでいる。近年、企業のウェブサイト、SNS、広告、イベント紹介、店舗 PR、地域活動紹介などで、子供の写真や動画を利用するケースは少なくない。

GDPR では、単に「保護者の同意を取得している」というだけでは十分とはみなされない可能性がある。特に、子供の顔写真、睡眠中・食事中など私的性格の強い場面、日常生活の様子、SNS 等による拡散可能性などについては、慎重な検討が求められる。

また欧州では近年、「親が同意したか」だけではなく、子供本人の尊厳、将来的な不利益の可能性、子供の最善利益を重視する方向へ規制・執行が強まっている。そのため日本企業も、「保護者同意があるから問題ない」という従来型の感覚だけではなく、子供データの公開自体が本当に必要なのか、公開範囲や掲載内容は適切か、といった観点から慎重に検討する必要がある。