プラットフォーム規制と情報に対する責任

2026.5.13.
小向　太郎 Taro KOMUKAI, Ph.D.
中央大学　国際情報学部　教授

1. プラットフォームへの期待
    1. プラットフォームに何を求めるか？
    2. プラットフォーム上で起こる問題
    3. エンゲージメント重視の深刻な弊害
2. 違法情報に対する責任
    1. 違法情報に対する媒介者責任
    2. コンテンツ・モデレーション規制
    3. 日本：情報流通プラットフォーム対処法
3. 子どもの保護と年齢確認
    1. 子どもを取り巻くリスク
    2. SNS利用規制と年齢確認
    3. 子どもの個人情報保護

自己紹介：小向太郎

中央大学　国際情報学部　教授
大学院国際情報研究科　委員長

情報通信総合研究所取締役法制度研究部長、早稲田大学客員准教授、日本大学教授等を経て、2020年より現職

【主な著書】

『プラットフォームに正義を託せるか』日本経済新聞出版、2026年

『情報法入門（第7版）デジタル・ネットワークの法律』NTT出版、2025

『データセキュリティ法の迷走』監訳、勁草書房、2023年

『概説GDPR～世界を揺るがす個人情報保護制度』共著、NTT出版、2019

教育理念 — 実務直結の学際統合

AIデータサイエンス

キーワード： 行動情報分析 / HCI・UX / LegalTech / 法律AI / 知識工学 / テキストマイニング / ウェブシステム / 並列分散システム / IoT

勤務先例： 建設業、金融機関、情報システム開発

情報法

キーワード： 情報法 / AI・ロボット法 / AIガバナンス / メタバースの法 / プライバシー・個人情報保護 / サイバー犯罪と捜査 / ELSI

勤務先例： コンサルティング、官公庁（総務省・デジタル庁・自衛隊等）、広告代理店、製薬、ISP、電気通信、マスメディア

社会デザイン・社会実装

キーワード： ネットワークセキュリティ / サイバーセキュリティ / コミュニケーション / メディア教育 / 社会的相互作用

勤務先例： マスメディア、コンサルティング、地方自治体、教育機関、広告代理店、金融機関、情報システム開発

ロケーションと学修環境

社会人に配慮した授業時間

平日専門科目：18:50～20:30
（終業後通学可）
土曜：研究指導・必修科目
（原則対面）

ハイフレックス対応

対面・オンラインどちらでも受講可能
やむを得ない事情は教員と相談のうえ
オンライン参加が認められる場合がある

グローバルIT人材と修士号

1. AI・データ活用が競争優位の源泉となる時代に、技術を読み解き法制・倫理まで判断できる人材が不可欠
2. 国際的な規制動向（EU AI Act 等）に対応できるガバナンス知識は、今後のビジネスリスク管理に直結
3. 修士号はグローバル人材の共通言語 —— 海外パートナーや規制機関との交渉力を高める

（参考）指定機関推薦制度：企業連携型の入試制度

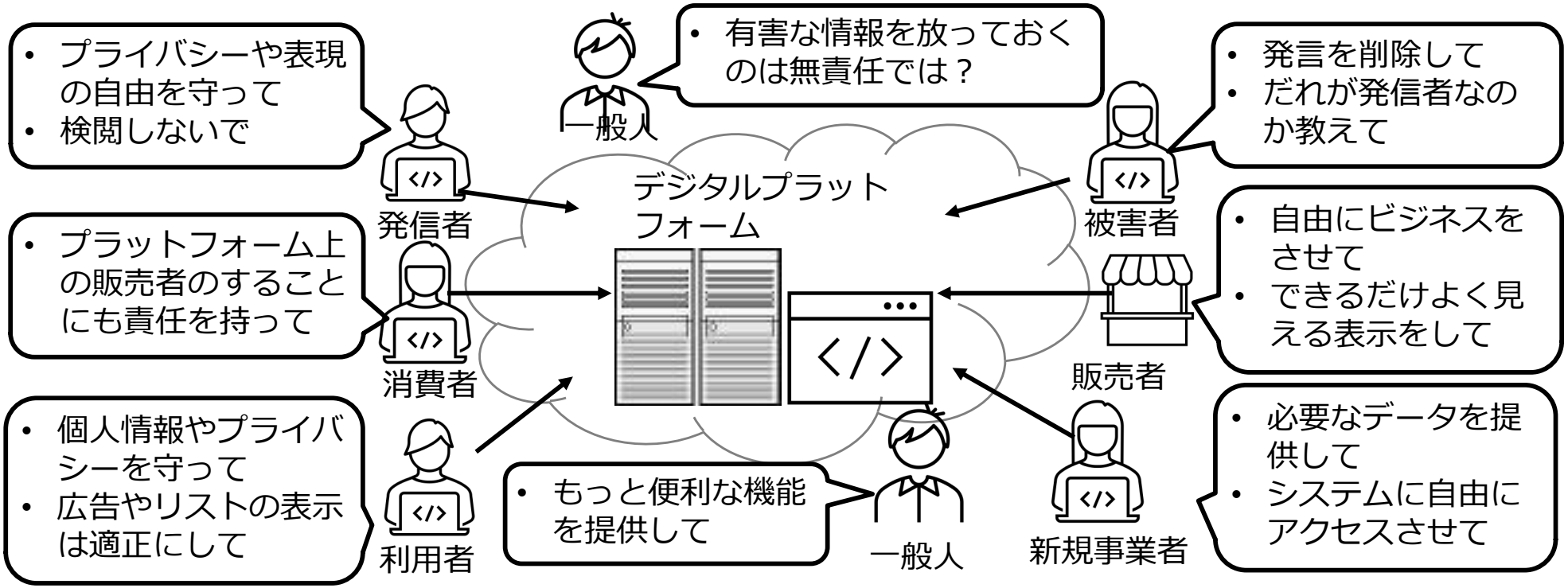
募集人員	若干名（社会人特別入学試験と合わせて15名） 各機関の推薦枠は原則1名
出願資格	本研究科が指定した企業・機関に勤務する大卒者 （入学時卒業見込みを含む）またはそれに準じる者
選考方法	書類審査 ＋ 口述試験 企業・機関からの推薦を尊重した選考を実施

※ 詳細は本研究科の募集要項をご確認ください

1. プラットフォームへの期待

1-1. プラットフォームに何を求めるか

- 二面市場または多面市場を持つデジタル・プラットフォームには、それぞれの関係者から、異なった要請がなされる
- プラットフォームのビジネスは、利用者のエンゲージメントを高めることで拡大する



出典：小向太郎『プラットフォームに正義を託せるか』（日本経済新聞出版、2026年）212頁

1-2. プラットフォーム上で起こる問題

- プラットフォームで生じる問題は多様であり、問題の種類によっても、誰にどのような責任が問われるのかは異なる

	種類	問題例
違法情報	権利を侵害する情報	名誉毀損、プライバシー侵害、著作権・商標権侵害
	禁止されている情報	わいせつ、名誉毀損、犯罪の扇動、風説の流布、情報による業務妨害、児童ポルノ等
	ネット上の犯罪	詐欺、恐喝、闇バイト、トクリュウ、オンラインカジノ、性搾取、薬物売買、禁制品の販売等
有害情報	個人への悪影響	性的情報、残酷な情報、自殺、いじめ、薬物、依存、過度なダイエット、誤った健康法等
	社会への悪影響	デマ、情報操作、社会の分断を煽る情報、差別を助長する情報
利用者等の保護	消費者保護	不当表示（ダークパターン、ステルスマーケティング）等の、販売店と消費者のトラブル、過度の囲い込み、不利益な取引の強制など
	青少年保護	有害コンテンツによる悪影響（不良化、犯罪化、自殺・自傷）、犯罪者のアプローチ、ネット依存、ネットいじめなど
	プラットフォーム独占	不当な独占的地位の維持、プラットフォーム上のビジネスに対する圧力、自社に有利な契約条件の強制など

1-3. エンゲージメント重視の弊害

Contents

Abstract: Facebook contributed to a genocide in Myanmar. Scholars, reporters, and United Nations investigators agree that the social media giant played a role in an explosion of ethnic conflict in 2017 that led to the death and displacement of hundreds of thousands Rohingya Muslims in Northern Myanmar.

Riding a wave of liberalization, Facebook entered the country and quickly dominated online spaces, with early the entire internet-connected population of the country using Facebook products. Challenges related to culture and technology meant that the conversations received little moderation. Facebook feeds quickly became populated with hateful speech, including misinformation seeded by the ruling military authority. As a result, Facebook played a critical role in the explosion of violence, especially during the 2017 genocide.

This paper argues that, even acknowledging unique challenges, the outcomes in Myanmar were a predictable result of Facebook's business model in combination with a striking lack of moderation or enforcement of the company's own code of conduct. The paper further argues that this outcome is the ultimate consequence of an atmosphere of absolute corporate impunity. With no international legal mechanism capable of holding Facebook accountable, the company operated without regard for the human rights of Myanmar's citizens. The absence of accountability mechanisms is itself a consequence of corporate power. With no changes in legal frameworks likely to result from this tragedy, this will not be the last time that Facebook will contribute to a situation like the Myanmar genocide.

Daniel Zaleznik, *Facebook and Genocide: How Facebook contributed to genocide in Myanmar and why it will not be held accountable*, Systemic Justice Journal Volume 1

- エンゲージメント優先設計が現実に引き起こした最悪のケース
- ロヒンギャの迫害
  - 2016年頃から
  - 一般市民6800人以上殺害
  - 約73万人が国外に退去
- Facebookの影響
  - 「Facebookは、憎悪に満ちたコンテンツを拡散することで、この民族浄化に決定的な役割を果たした（国連レポートより）」

2.　違法情報に対する責任

2-1. 違法情報に対する媒介者責任

- プラットフォーム上の違法情報に対する責任の考え方は、国・地域によって大きく異なる

	米国	EU	日本
法律	通信品違法230条	デジタルサービス法	情報流通PF対処法
対象情報	双方向コンピュータサービス上に第三者が発信した違法情報	事業者が媒介した違法情報、システミックリスクを生じる情報	事業者が媒介した権利侵害情報（原則として違法情報）
削除等を**行わかなった**ことによる責任	ほぼ**全面的免責**	**認識していない場合は免責**、認識後は遅滞なく削除等が求められる	**侵害について善意無過失**の場合は**免責**
削除等を**行った**ことによる責任	善意で自発的に行った行為には**責任なし**（グッド・サマリタン条項）	自主的対応をとったことだけを理由に責任は問われない	権利侵害があると信じるに足る場合のみ免責、**発信者に照会**の上削除可

出典：小向太郎『情報法入門』（NTT出版、第7版、2025年）216頁より

（参考）米国通信品位法230条に対する批判

【連邦議会上院の公聴会（2020年11月29日）】

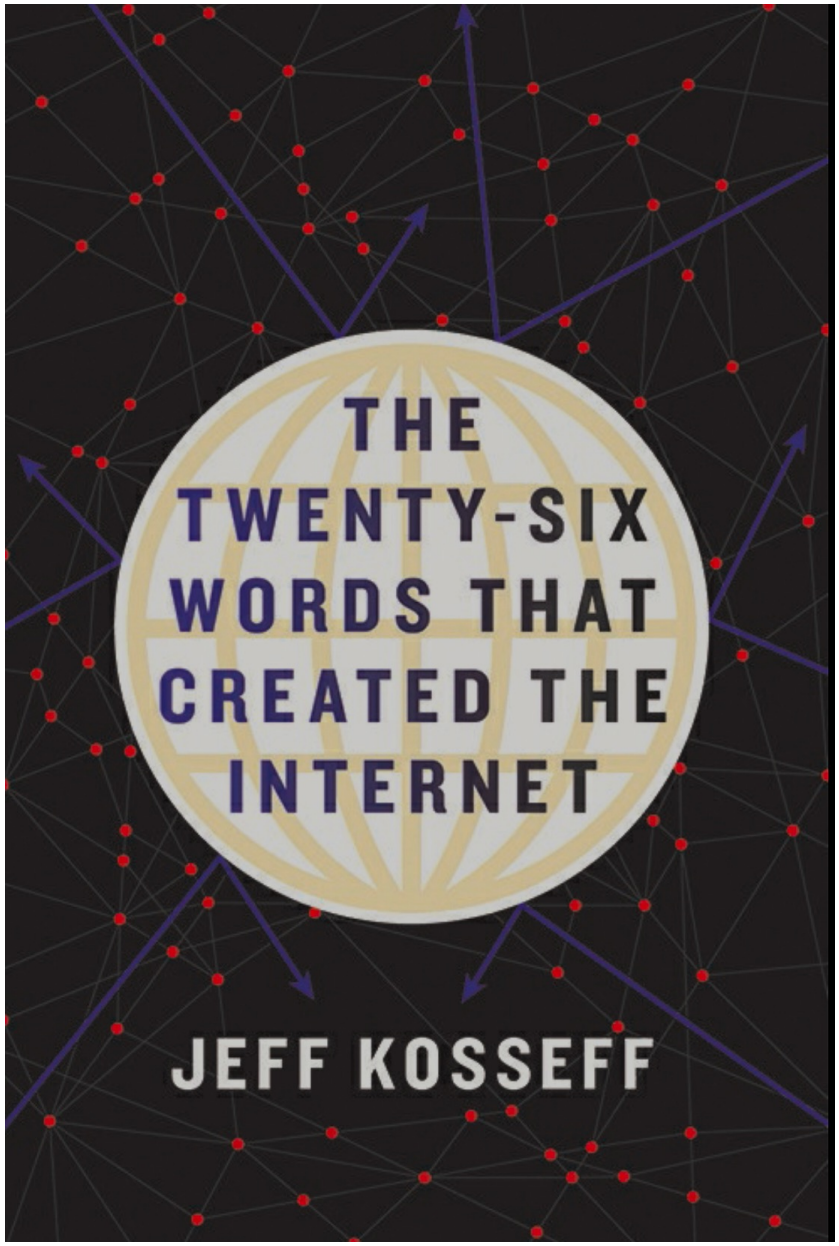
- 「230条の広範な免責は巨大IT企業に悪行を許しているのか？（Does Section 230’s Sweeping Immunity Enable Big Tech Bad Behavior?）」

共和党側の主張	民主党側の主張
• 「自分勝手に検閲のような関与」を許すべきではない	• フェイクニュースの拡散などの悪質なものや、選挙等にも影響を与えうる投稿は、もっと積極的に制限すべき

【トーマス最高裁判事の声明】

- 1996年の通信品位法制定時には，今日の主要なインターネット・プラットフォームのほとんどが存在していなかった
- 多くの裁判所は，この法律を広く解釈し，世界最大級の企業に包括的な免責を与えている
- 条文の文言からも制定経緯からもこのような解釈は取り得ない
- 条文の自然な読み方を超えて通信品位法230条の免責を拡大することが、深刻な結果をもたらす可能性がある

（参考）インターネットを作り出した24単語



- この26の言葉が、アメリカの数十億ドル規模のオンライン産業の大部分を担っていることをご存知だろうか。私たちがオンラインで何を書き、何を言い、何をすることができるかは、たったひとつの法律に基づいている（CBS 60 Minutesでの紹介）
- 「第230条は、オンライン上での自分の行動や発言には責任を持つべきだが、他人の行動や発言には責任を持つべきではないという原則を具体化したものである。この法律は、他人の発言に基づくユーザーやサービスに対する民事訴訟のほとんどを防いでいる（EFFWebページ「Section 230」https://www.eff.org/）」

2-2. コンテンツ・モデレーション規制

- 米国ではコンテンツ・モデレーションを制限する州法が制定され、促進政策をとっているEUや日本とは対照的である

	米国	EU	日本
法律	テキサス州H.B.20	デジタルサービス法	情報流通PF対処法
対象事業者	月間 5,000 万人以上のユーザーを持つSNS，コンテンツ共有事業者等	超巨大プラットフォーム事業者	大規模特定電気通信役務提供者
対象情報	事業者が削除等の対象とする情報全般	事業者が媒介した違法情報、システミックリスクを生じる情報	事業者が媒介した権利侵害情報（原則として違法情報）
コンテンツモデレーション規制	ユーザーを「検閲（センサーシップ）」することの禁止、検閲の慣行について一般および個別の開示義務	超巨大プラットフォームに、コンテンツ・モデレーションの実施を含むシステミック・リスク軽減義務	権利侵害情報に関する削除請求等についてPFの対処義務

（参考）EUデジタルサービス法の対応義務①

- カテゴリーごとに、媒介者のコンテンツに対する責任について規定
- ホスティングには対応義務（ノーティス・アンド・アクション）

種類	対象になる事業者	媒介情報に対する主な責任
単なる伝送路	伝統的な電話会社など、情報の伝送だけを提供する事業者	基本的に責任は問われない
キャッシング	情報伝達を効率化するために、インターネット上で、データの一時的保存や転送を行う事業者	伝送効率化のためであれば基本的に責任は問われない。ただし、オリジナル情報が削除された場合には削除するなどの対処が必要
ホスティング	ウェブホスティングや SNS、掲示板など、インターネット上で利用者が情報を蓄積する場所を提供する事業者	違法情報について認識していなければ責任は問われない。認識した場合には対応しなければならない。削除要請を受けて対応する義務（ノーティス・アンド・アクション）が課せられる
オンライン・プラットフォーム	ホスティングのなかで、利用者の要請に応じて情報を保存し、公衆に送信する事業者	ホスティングとしての責任に加えて、消費者や青少年保護にための義務が課せられる
超巨大オンライン・プラットフォーム	月間4500万人以上が利用しているオンライン・プラットフォーム	オンライン・プラットフォームとしての責任に加えて、社会全体に大きな影響を与える「システミック・リスク」を、評価して軽減する義務が課せられる

出典：小向太郎『プラットフォームに正義を託せるか』（日本経済新聞出版、2026年）59頁

（参考） EUデジタルサービス法の対応義務②

- 超巨大プラットフォーム（VLOPs）と超巨大検索エンジン（VLOSEs）に「システミック・リスク」評価・軽減義務

種類	概要
義務付けられている対応	システミック・リスクの評価（第34条）、リスクの軽減（第35条）、危機対応の仕組み（第36条）、独立監査（第37条）など
システミック・リスクの内容（第34条第1項）	違法コンテンツの流布、基本的権利への悪影響、民主的プロセスや治安に影響を与えるサービスの不正操作、ジェンダーに基づく暴力、未成年者への悪影響、利用者の身体的・精神的健康への深刻な影響など

【対象事業者（2025年10月）】

種類	ビジネス領域	対象事業者
VLOPs	SNS・動画等共有サイト	YouTube，LinkedIn，Facebook，Instagram，Pinterest，Snapchat，TikTok，X
	ショッピング・電子商取引サイト	AliExpress，Amazon Store，App Store，Booking.com，Google Play，Google Shopping，Shein，Temu，Zalando
	アダルトサイト	Pornhub，XNXX，XVideos
	その他	Google Maps，Wikipedia
VLOSEs	検索エンジン	Google Search，Bing

出典：小向太郎『プラットフォームに正義を託せるか』（日本経済新聞出版、2026年）69,73頁

（参考）情報流通プラットフォーム対処法

- 権利侵害情報の責任制限と、大規模プラットフォームの対処義務について定めている

媒介者の責任制限	被害に対する責任（第3条第1項）	• 削除等を行わなかった場合の「被害者」に対する責任 • 侵害を知っていたか、当然知り得えたであろうと認められる場合以外は免責
	削除に対する責任（第3条第2項）	• 削除等を行った場合の発信者に対する責任 • 他人の権利が侵害されていると信じるに足りる相当の理由があったとき • 権利を侵害されたとする者から違法情報の削除の申出があったことを発信者に連絡し、7日以内に反論がない場合
大規模ＰＦ	対応の迅速化（権利侵害情報）	• 削除申出窓口・手続の整備・公表 • 削除申出への対応体制の整備（十分な知識経験を有する者の選任等） • 削除申出に対する判断・通知（原則、一定期間内）
	運用状況の透明化	• 削除基準の策定・公表（運用状況の公表を含む） • 削除した場合、発信者への通知

出典：小向太郎『情報法入門』（NTT出版、第7版、2025年）206-207頁

（参考）プラットフォームに対する差止請求

- どのような場合に、不法行為責任や差止請求が認められるかは、行為や媒介者の種類によって異なる

対象	媒介者の責任	事例
掲示板管理者	権利侵害について知っているか，当然知ることができた場合に，一定の期待される対応を行う法的義務がある	ニフティ現代思想フォーラム事件，産能大学事件
匿名掲示板管理者	管理者には，損害発生を防止する義務があり，常に注意を払い，権利侵害があれば直ちに削除する義務がある	2チャンネル対動物病院事件，学校裏サイト事件
ツイッター	公表されない法的利益と本件各ツイートを一般の閲覧に供し続ける理由に関する諸事情を比較衡量し、前者が優越する場合には、削除を求めることができる	ツイッター投稿削除請求事件（最二小判令和４年6月24日）
検索サービス事業者	事実を公表されない法的利益と当該ＵＲＬ等を検索結果として提供する理由に関する諸事情を比較衡量して前者が優越することが明らかな場合に削除を求めることができる	グーグル検索結果削除請求事件（最決平成29年1月31日）

出典：小向太郎『情報法入門』（NTT出版，第6版，2022年）109頁より

2-3. 利用者保護の強化

- 日本では、プラットフォームに対して、ダークパターンの防止、レイティングや広告の透明性確保、プラットフォーム上のビジネスの適法性確保などを求める制度が、比較的少ない

	種類	問題例	対応する制度
利用者等の保護	消費者保護	不当表示（ダークパターン、ステルスマーケティング）等の、販売店と消費者のトラブル、過度の囲い込み、不利益な取引の強制など	景品表示法に基づく不当表示規制、取引DPF消費者保護法、特定商取引法、消費者契約法等
	青少年保護	有害コンテンツによる悪影響（不良化、犯罪化、自殺・自傷）、犯罪者のアプローチ、ネット依存、ネットいじめなど	出会い系サイトに当たる場合の登録義務、青少年の利用制限、フィルタリング提供義務等
	プラットフォーム独占	不当な独占的地位の維持、プラットフォーム上のビジネスに対する圧力、自社に有利な契約条件の強制など	私的独占、不公正な取引方法、不当な取引制限（優越的地位の濫用等）、特定DPF取引透明化法、スマホソフトウェア競争促進法

（参考）デジタルサービス法の消費者保護規制

種類	項目	概要
プラットフォーム自身の行為に対する規制	ダークパターンの禁止（25条）	自由な意思決定を、欺罔・操作・歪曲などで損なうようなインターフェースの設計・構築・運用禁止
	広告の透明化（26条）	広告であること・広告主・表示理由などを広告ごとに、明確、簡潔かつ曖昧さのない方法で、リアルタイムで識別できるようにする義務
	おすすめの透明化（27条）	仕組みを説明し、利用者が簡単に修正や要望ができるようにする義務
	未成年者の保護（28条）	未成年者向けサービスに、高いレベルのプライバシー・安全・セキュリティを確保する義務
プラットフォーム上でビジネスを行う事業者に関する義務	販売者のトレーサビリティ（30条）	販売者に関する情報を取得・確認し、消費者に提供する義務
	法令遵守を促すデザイン（31条）	EUの消費者法に基づく義務（契約前情報・製品安全情報の提供など）に沿った画面になるように設計・構築する義務
	違法な製品・サービスの情報提供（32条e）	違法な製品・サービスの提供について、違法性・販売者情報・救済手段を消費者に通知する義務

出典：小向太郎『プラットフォームに正義を託せるか』（日本経済新聞出版、2026年）66頁

3.　子どもの保護と年齢確認

3-1. 子どもを取り巻くリスク

- 想定リスクの種類によって求められる対応は異なる
  - コンタクトリスク：犯罪対策
  - コンシューマーリスク：消費者保護
  - プライバシーリスク：個人情報保護
- リスク内容について実証的な評価が求められる
  - 青少年自身の回避モチベーション
  - ポジティブな側面
  - 心身の健康への影響の程度　など

区分	リスクの概要
コンテンツ	ポルノや暴力的描写などの有害情報から悪影響を受ける
コンタクト	ネット上で接触する犯罪者などからターゲットにされる
コンダクト	いじめ・ヘイト・自傷・極端なダイエットなどを起こす
アディクト	ネット依存や特定の嗜好や思想にとらわれたりする
プライバシー	個人情報を不用意に収集され将来にわたって利用される
コンシューマ	ダークパターン等欺瞞的な商品表示などを信じてしまう

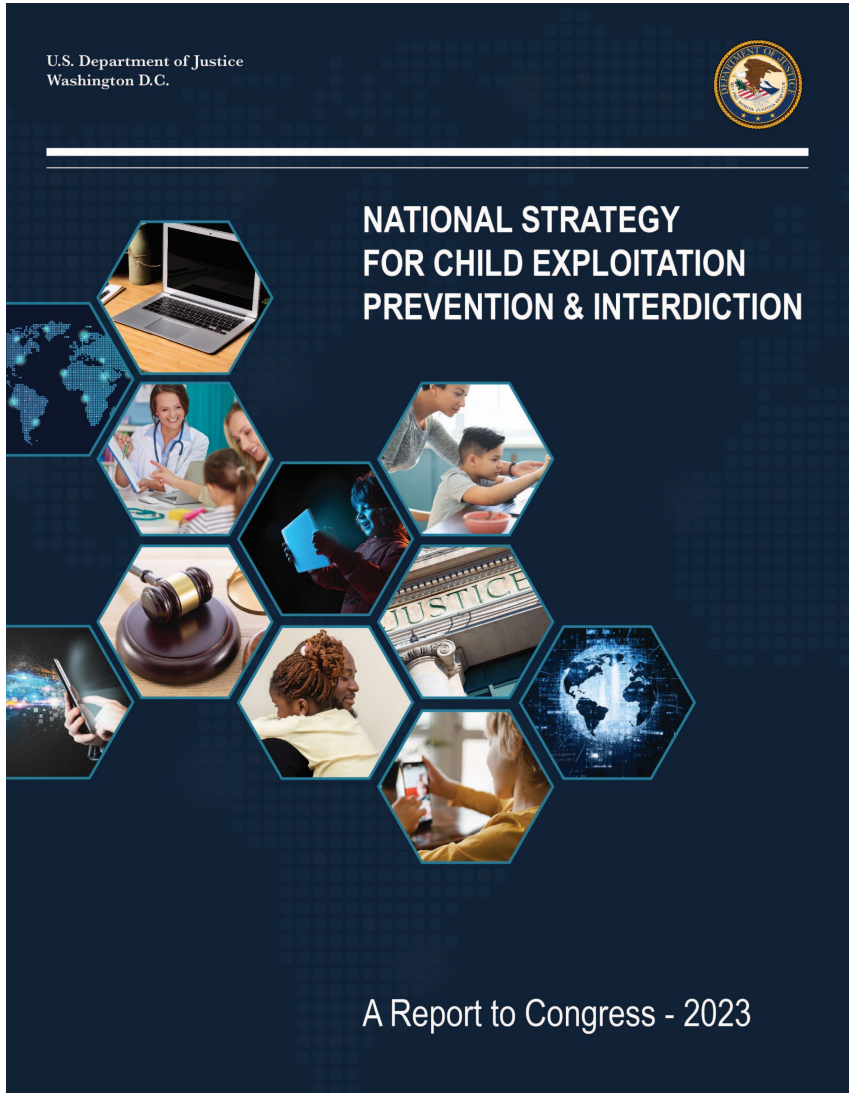
（参考）OECDレポート2021

- 2021年のOECDレポートでは、リスクを「コンテント」「コンダクト」「コンタクト」「コンシューマー」に分類して、「プライバシー」「先端技術」「心身の健康」を横断的リスクであるとしている

Risks for Children in the Digital Environment				
Risk Categories	**Content Risks**	**Conduct Risks**	**Contact Risks**	**Consumer Risks**
Cross-cutting Risks*	Privacy Risks (Interpersonal, Institutional & Commercial)			
	Advanced Technology Risks (e.g. AI, IoT, Predictive Analytics, Biometrics)			
	Risks on Health & Wellbeing			
Risk Manifestations	Hateful Content	Hateful Behaviour	Hateful Encounters	Marketing Risks
	Harmful Content	Harmful Behaviour	Harmful Encounters	Commercial Profiling Risks
	Illegal Content	Illegal Behaviour	Illegal Encounters	Financial Risks
	Disinformation	User-generated Problematic Behaviour	Other Problematic Encounters	Security Risks

OECD, Children in the Digital Environment: Revised Typology of Risks, OECD Digital Economy Papers No.302, January 2021

（参考）DOJレポート（2023年）



- National Strategy for Child Exploitation Prevention and Interdiction, 2023 REPORT TO CONGRESS
  - 児童性的虐待資料
  - 米国における児童の性的人身売買
  - 特殊な地域と集団における児童搾取
  - 域外における児童の性的虐待
  - ライブストリーミングとバーチャル児童性的人身売買
  - セクストーション、クラウドソーシング、誘引、強要
  - 独自の資源と執行の問題
  - テクノロジー
  - 犯罪者心理学
  - 協力関係
  - 犯罪防止
  - 性犯罪者登録違反
  - 遺族、介護者、および遺族ケアへのアクセス
  - 法執行官のメンタルケア等

3-2. SNS利用規制

- 最近の青少年のSNSへのアクセスを制限する規制は、心身の健康を損なうリスクを重視し、アルコールやタバコの規制根拠と類似

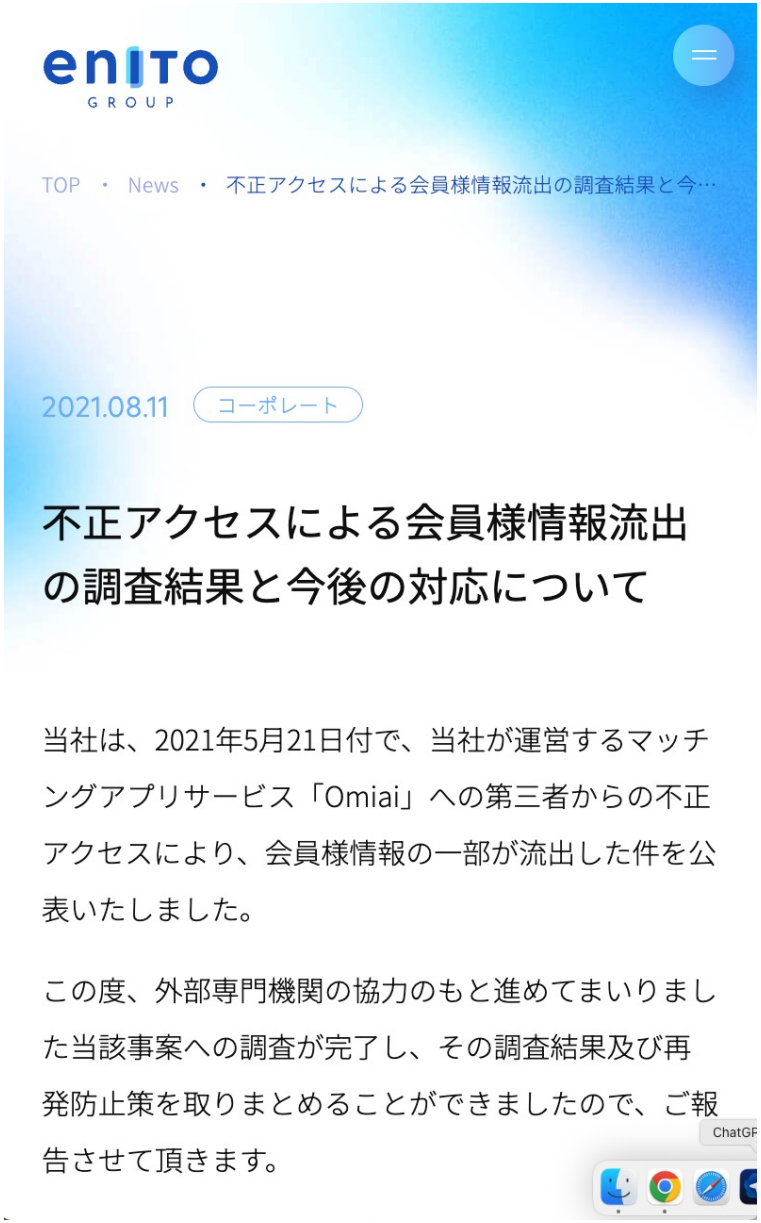
国	概要	懸念リスク
オーストラリア2025年施行	16歳未満の者がアカウントを持てないよう合理的措置	薬物乱用，自殺や自傷行為，暴力的な素材，安全でない食習慣の助長など
EU 議会提案	16歳未満のソーシャルメディア等利用に保護者同意、13歳未満は保護者の同意があっても利用不可	依存性のあるスマートフォンのサービス ：不安や抑うつ症状の増大，衝動制御の欠如，などの思春期のメンタルヘルス問題の増加
フランス 法案審議中	15歳未満のソーシャルメディアの使用を禁止し、高校では携帯電話の使用を禁止	抜け出しにくい設計になっていること、また有害情報（自傷・摂食障害・暴力的内容など）への接触
米フロリダ州	14歳未満のアカウント禁止、14～15歳は保護者の同意等	睡眠、学業、対人関係、自己像（外見・比較）への悪影響、いじめ・嫌がらせ、性的な危険（望まない接触や搾取）等
日本	フィルタリング利用の促進、18歳未満の出会い系サイト利用禁止	犯罪や自殺につながる情報，著しく性欲を興奮・刺激する情報，著しく残虐な内容の情報。性的な接触の抑制

3-3. 年齢確認

- 諸外国では、「子どもを守るためにデータを集める」というパラドックスが強く意識されている

国	確認方法	個人情報保護制度との関係
オーストラリア	• リスクに応じて，効果・負担・プライバシーのバランスで判断 • 政府発行ID・政府の認定を受けたデジタルIDサービス以外の方法を提供する義務	• 目的のために本当に必要な最小限の情報に限定する義務 • 顔画像・生体情報などの利用には，原則として本人の同意が必要
EU	• the age-verification blueprint（2025年10月ver.2） • 身元確認は年齢証明書の発行時のみで、年齢証明書体には身元データなし	• 明確で正当な目的のために必要な最低限の年齢関連属性のみを処理 • プライバシーを最大限に保護する設計・実装
米国フロリダ州	• 合理的な方法（事業者の裁量） • 実務上は、AIを活用した顔年齢推定（facial age estimation）や生体認証スクリーニングなど	• 目的外利用・必要を超える保持の禁止、秘匿義務・共有禁止 • 合理的な情報セキュリティ対策 • 外国企業の年齢確認実施禁止
日本（出会系サイト規制法）	• 公的身分証明書・クレジットカードの利用等	• 目的外利用・第三者提供の原則禁止、遅滞なく消去の努力 • 多くの事業者が本人確認の証跡を残すために保存

（参考）Omiaiの情報漏洩事案



- 事案の概要（2021年8月）
  - 出会い系サイト規制法の対象事業であるマッチングアプリ「Omiai」で，年齢確認書類画像（運転免許証等）約171万件の流出
- 保存方針
  - 退会後も10年間は利用者の個人情報を保存
  - 事件後：会員個人データは退会後90日に削除、年齢確認書類画像データは提出後72時間後に自動削除

（参考）子どもの個人情報保護

項目	米国：COPPA	EU：GDPR	日本：個人情報保護法 改正方針（2026年）
保護対象年齢	13歳未満	16歳未満（各加盟国が13～16歳の範囲で引き下げ可能）	16歳未満
親権者の同意	13歳未満への個人情報収集には、事前に「確認可能な親の同意」が必要	16歳未満（各国調整後の年齢）のオンラインサービス利用には親権者の同意が必要	16歳未満の個人情報取得・通知等の手続きは法定代理人を対象とすることを明文化
データ利用停止・削除請求	親は子どものデータの閲覧・削除を請求可能（事業者は対応義務）	「忘れられる権利」（削除権）が未成年者を含む全個人に保障（同意を根拠に取得した子どもに関するデータは特に削除が容易）	16歳未満の保有個人データについて利用停止等の請求要件を緩和（「子どもの最善の利益」の優先考慮責務）
適用対象	子ども向けウェブサイト・オンラインサービスの事業者	EU域内の個人にサービスを提供するすべての事業者	個人情報取扱事業者全般

プラットフォーム規制と情報に対する責任

- 基本的な考え方
  - 「オフラインで違法なものは、オンラインでも違法である（What is illegal off-line is also illegal on-line）」
  - プラットフォームに対しても、「違法情報」に対する責任をできる限り明確にして、対応を法的に求めるべき
- 子どものSNS利用規制
  - 年令による一律的利用制限を拙速に導入するのではなく、リスクの実態に応じた対応が必要
  - 実効的な利用抑制のためには、厳格な年齢確認にこだわるべきではなく、政府公式IDへの過度の集中も避けるべき
- 子どもの個人情報保護
  - 保護対象が広範すぎないか、実効性が確保できるかどうかなどについて検討が望まれる
  - 年齢確認情報の利用範囲の厳格化や保存期間の制限についても検討すべき