

オンライン安全法制の国際動向 ー英国、オーストラリアの事例を中心にー

藍澤 志津（あいざわ しづ）

主席研究員

- 専門分野：諸外国（特に英国とインド）の情報通信・デジタル分野の政策・市場動向
- 最近の研究テーマ（FMMCの年間テーマ研究）
 - （2023年度）「諸外国におけるメタバース展開動向」（英国、インド）
- その他の活動
 - 総務省情報通信審議会 情報通信技術分科会 ITU部会 衛星・科学業務委員会 専門委員（2013年～）
 - デジタル政策フォーラム アジェンダ2「データ駆動社会の基本規律」副査



坂本 博史（さかもと ひろし）

主任研究員

- 専門分野：諸外国（特にアジア・オセアニア）の情報通信・デジタル分野の政策・市場動向
 - ICT産業の経済動向
 - 各産業部門におけるICT利活用
 - ICTのマクロ経済への影響
- 主な調査実績
 - ICTの経済効果に関する調査
 - ICTの産業利活用に関する調査
 - ICTに関する国際指標についての調査



問題意識

- ソーシャルメディアサービス、動画配信・投稿サイト等、デジタルサービスの発展・普及により、インターネット上で膨大な情報やデータが流通し、誰もがこれらを容易に発信・入手することが可能となった。それに伴い、ネットいじめ、偽・誤情報、ディープフェイク、ジェンダー・ハラスメント、子どもの性的虐待、選挙操作等、オンライン上のコンテンツや行動により、人々の生活や仕事に多くの危険が生じるようになった。
- 世界ではオンラインの安全確保に向けた法整備が進展中である。特に、世界に先駆け、オーストラリアでは2021年に「2021年オンライン安全法」が成立、2023年には英国でも「2023年オンライン安全法」が成立した。また、英国、オーストラリア、アイルランド、フィジー、南アフリカ、韓国は、オンライン安全規制当局による国際協力枠組「Global Online Safety Regulators Network : GOSRN」を立ち上げた。

目的

- 先進的事例として、英国、オーストラリアのオンライン安全法制の内容・体制・影響・課題を抽出するとともに、オンライン安全規制当局による国際協力枠組「GOSRN」について考察することで、日本におけるオンライン・コンテンツによる危害の対策を考えるうえで参考となる情報を提供する。

方法

- 文献調査が中心

報告内容

- 英国の動向
- オーストラリアの動向
- 国際協力枠組「GOSRN」の動向
- 得られた知見／今後の展望・課題と日本への示唆

英国の動向

- 成立の背景と過程
- 進捗状況とスケジュール
- 法規制の枠組と実行・支援体制
- プラットフォーム事業者等の反応や影響
- 最新動向
- 得られた知見／今後の展望・課題と日本への示唆

成立の背景と過程

- ブレグジット後の英国の発展に向け、オンライン空間の安全性を高める「2023年オンライン安全法」が成立
- プラットフォーム事業者に対し、オンライン上で特に子どもを適切に保護する実践的措置の導入・遂行を義務付ける

年月	内容
2016年6月	ブレグジットの国民投票、離脱決定
2017年10月	政府「インターネット安全戦略（Internet Safety Strategy）」発表 「英国を世界で最も安全なオンライン空間にする」
2017年11月	ティーンエイジャーのモリー・ラッセルさん自殺事件（オンライン上の子どもの保護に関する世論の高まり）
2019年4月	政府「オンライン有害白書（Online Harm White Paper）」発表・諮問開始
2020年1月31日	離脱協定にもとづき、英国はEUから正式に離脱
	主権国家として独自の法律や規制の導入が可能となるとともに、国際社会における新たな存在感の確立を目指し「グローバル・ブリテン」構想を掲げる
2021年5月	「オンライン安全法案（Online Safety Bill）」草案発表
2022年12月	オンライン企業に「注意義務」を課し「合法だが有害な」コンテンツに対処するポリシーの作成・実施を義務付ける条項を削除した修正案が提出
2023年4月	WhatsApp、Signal等が第122条（Ofcomがプラットフォーム事業者に対して「認定技術」を利用して違法コンテンツを削除することを命じる内容）によるE2EE通信監視に関して公開書簡。
2023年9月	（上記に対し）政府高官「技術的に実現可能でありプライバシーと正確性の最低基準を満たしている場合にのみOfcomが介入」と発言
2023年10月	「2023年オンライン安全法」成立
2024年1月	一部施行
2024年7月	スターマー政権誕生
	サウスポートの少女殺傷事件発生

進捗状況とスケジュール

2023 Q3	Q4	2024 Q1	Q2	Q3	Q4	2025 Q1	Q2	Q3	Q4	2026 Q1	Q2	Q3	Q4	
フェーズ1：違法な危害	●「2023年オンライン安全法」成立				●Ofcom、「違法な危害に関する行動規範」決定									
	●違法な危害に関するガイダンスと規則の諮問				●サービス事業者、違法な危害に関するリスク評価を完了									
					●議会、「違法な危害に関する行動規範」承認									
					●「違法な危害に関する行動規範」発効（遵守義務）									
フェーズ2：子どもの安全義務とポルノグラフィ	●ポルノからの子どもの保護のための年齢確認／年齢推定に関するガイダンスの諮問		●子どもの保護のガイダンスと規則の諮問		●Ofcom、「子どものアクセス評価ガイダンス」決定									
					●Ofcom、「年齢保証ガイダンス」決定									
					●女性・女兒保護ガイダンス諮問									
					●Ofcom、「子ども保護規範」決定									
					●サービス事業者、子どものアクセス評価を完了									
					●対象となるサービス事業者、子どものリスク評価を完了									
フェーズ3：カテゴリー別サービスの義務					●議会、「子どもの保護規範」承認									
					●「子どもの保護規範」発効（遵守義務）									
			●「透明性ガイダンス」諮問		●「カテゴリー別サービス規範」諮問		●Ofcom、「カテゴリー別サービス規範」決定							
					●「カテゴリー別サービス登録簿」公表							●議会、「カテゴリー別サービス規範」承認		
罰金												●「カテゴリー別サービス規範」発効（遵守義務）		
			●罰金に関する諮問				●全世界売上高の閾値と通知に関する規則発行							
							●対象となるサービス事業者、全世界売上高をOfcomに報告							
								●Ofcom、罰金の原則発表						

法規制の枠組と実行・支援体制

法律名	「2023年オンライン安全法（Online Safety Act 2023）」				
成立・施行日	■ 2023年10月成立、2024年2月一部施行。3段階の諮問を実施し二次法を整備（2026年初めに完了予定）				
規制機関	通信庁（Ofcom）：「オンライン安全規制機関」として指定				
プラットフォーム事業者への義務	オンライン上で特に子どもを適切に保護する実践的措置の導入・遂行を義務付ける				
子どもへの義務	違法なコンテンツの速やかな削除・非表示対応	有害かつ年齢不相応なコンテンツへのアクセス防止	年齢制限・年齢確認システムの導入	リスク評価・透明性の確保	問題発生時の利用しやすい報告手段の提供
成人への義務	（全てのサービスは）違法コンテンツの削除及び違法行為への利用を防ぐ		（カテゴリー1のサービスは）利用規約で禁止したコンテンツの削除		（カテゴリー1のサービスは）フィルタリングツール等の提供
規制対象サービス	■ 「ユーザ間サービス」「検索サービス」（ポルノコンテンツサイト、オンラインマーケットプレイス、ファイル共有及びクラウドストレージを含む） ■ 「ユーザ間サービス」の対象（想定）：ソーシャルメディア・サービス（Facebook、Instagram、TikTok、X等）、メッセージング・アプリ（WhatsApp、Facebookメッセンジャー、テレグラム、シグナル等）、動画配信サービス（YouTube、Twitch等）、オンラインゲーム（Roblox、Fortnite、Minecraft等）、フォーラム（Reddit、4chan等）、出会い系サービス、ファイル共有及びクラウド・ストレージ・サービス（Googleドライブ、Dropbox等）、ユーザ生成型オンラインマーケットプレイス（eBay、Facebookマーケットプレイス等）、AIチャットボットとジェネレーティブAI（ChatGPT、Google Gemini、Microsoft Copilot等）（※AI生成したコンテンツを人間生成コンテンツと区別せず） ■ 「検索サービス」の対象（想定）：総合検索（Google、Bing等）、垂直検索（スカイスキャナー、Comparethemarket等） ■ 適用除外：私的通信（電子メール、SMS、ライブの聴覚通信のみを提供するサービス）、ニュース／出版物ウェブサイト（ユーザがコメントやレビューを投稿・共有）、内部のビジネス用途のサービス、公的機関が提供するサービス、教育または育児関連サービス ■ 事業体ではなく「サービス」を規制。規制対象となるかどうかは、ユーザが投稿したコンテンツをアップロード、共有、他のユーザとやりとりできるかという点がポイント。ただし、ポルノコンテンツサイトはユーザ生成コンテンツの共有が無い場合でも規制対象 ■ 全ての規模の組織、個人に適用。一部はユーザ数やサービスの機能に応じて分類、より厳しく規制 ■ 「英国へのリンク」を持つサービス（英国に相当数のユーザ、英国がターゲット市場）が対象				
規制対象コンテンツ	■ 「違法」と「有害」を区別。 ■ 「違法」（「優先的な違法な危害」17種類）：①テロリズム、②子どもの性的搾取と虐待、③ヘイト、④ハラスメント、ストーカー行為、脅迫と虐待、⑤支配的または強制的な行為、⑥親密な画像による虐待、⑦過激なポルノ、⑧成人の性的搾取、⑨人身売買、⑩不法移民、⑪詐欺と金融犯罪、⑫犯罪収益、⑬薬物と精神作用物質、⑭銃器、ナイフ、その他の武器、⑮自殺の奨励・幫助、⑯外国からの干渉、⑰動物虐待 ■ 「有害」：子どもにとって有害なコンテンツ。「最優先コンテンツ」（ポルノ、自殺・自傷行為・摂食障害を助長・奨励・指示）と「優先コンテンツ」（いじめ、虐待的・憎悪、深刻な暴力・傷害、危険なスタントやチャレンジ、有害物質の摂取・吸入・曝露）と「相当数の子どもに重大な危害を及ぼす危険性があるコンテンツ」が対象				
罰則	■ 1,800万ポンドまたは全世界の年間売上高の10%のいずれか高い方を上限として罰金。企業や上級管理職に刑事罰。コンテンツの投稿者刑事罰（刑法を改正。深刻な自傷行為の奨励・幫助、サイバーフラッシング、重大な被害を意図した虚偽情報送信、脅迫的通信、卑猥画像の悪用、てんかん患者への嫌がらせが直接適用）				

プラットフォーム事業者等の反応や影響

- 「Ofcomによる違法な危害に関する諮問」に対して提出された様々な組織からの意見等から下記の課題が抽出された。
- ライブストリーミング、私的通信（SNSや電子メール）が規制対象外となっている点も問題視。



言論の自由と安全の両立

検閲の懸念、過剰なモデレーション



実装と実施

中小企業の負担、多数・多様なサービスにおける一貫性



技術的・実践的な課題

AIと自動化（不正確になる可能性）、回避戦術対策（先手を打つ重要性）



プライバシーに関する懸念

データ収集、E2EE通信監視（プライバシーとセキュリティを危険にさらす）



国際的な意味合い

他国の法律・規制との不整合、規制の調和の必要性



イノベーションへの影響

コンプライアンス・コストによる技術投資の阻害



ユーザの意識と教育

一般市民の理解、デジタルリテラシーの向上

フェーズ1「違法な危害」を巡る動向

- Ofcom、「違法な危害に関する行動規範」決定（2024年12月）
 - 2025年3月から施行。 サービス事業者は、子どもの性的虐待、テロ、詐欺等の違法な被害の積極的軽減を求められる。
- Ofcom、オンライン安全要件遵守を支援するデジタルツールキット発表（2025年1月）
 - オンラインプラットフォーム上の違法コンテンツのリスク評価や管理のための段階的アプローチを提供。Ofcomのリスク評価ガイダンスに沿ったもので、以下の四つのステップで構成：1) 違法コンテンツのリスクの特定。2) 優先度の高いコンテンツやその他の違法コンテンツによる被害の評価。3) 安全対策の実施と行動の文書化。4) リスク評価の保守と更新。
- Ofcom、小規模サービス向けの「2023年オンライン安全法」準拠に関して情報提供（2025年1月）
 - 10万超の小規模オンラインサービスに対して、規制上の負担に対する懸念の軽減を目的に情報提供。比例性が重要であり、大規模でリスクの高いプラットフォームにより厳しいルールが適用される点を強調。ただし、違法コンテンツに関する最低限の対策（違法コンテンツのリスク評価・削除メカニズム・ユーザによる報告システム等）の導入は小規模サービス事業者にも求められる。
 - 基本的で不可欠な対策：1) 見つけやすく、理解しやすい利用規約。2) ユーザが違法または有害なコンテンツを見つけたときに報告できる苦情報告ツールとプロセス。3) コンテンツをレビューし、違法であると信じる理由がある場合に迅速に削除する能力。4) 必要に応じて連絡を取ることができるコンプライアンス担当者。
- 政府、子どもの性的虐待コンテンツを生成するAIツールを犯罪化（2025年2月）
 - 子どもの性的虐待コンテンツ（CSAM）を生成する人工知能（AI）ツールの所有、作成、配布を犯罪化。「犯罪及び警察法案（Crime and Policing Bill）」の一部として導入。内務省は世界初の取り組みとする。

フェーズ2「子どもの安全義務とポルノグラフィ」を巡る動向

- Ofcom、「子どものアクセス評価に関するガイダンス」と「子どもの年齢確認ガイダンス」決定（2025年1月）
 - 2025年7月までに、ポルノグラフィ・サービス事業者は、非常に効果的な年齢保証方法（年齢確認や推定など）の導入を求められる。 子どもが有害なコンテンツにアクセスするのを防ぎつつ、大人が合法的なコンテンツにアクセスできるようにすることを目的とする。柔軟でプライバシーに配慮したアプローチの例として、オープンバンキング、写真付き身分証明書、顔の年齢推定、モバイルネットワークによるチェック等。自己申告や年齢確認のないオンライン決済は無効とみなされる。

【参考1】Ofcomの違法な危害に関する行動規範とガイダンス①

- **2025年3月17日より、ユーザ間サービス及び検索サービスのプロバイダは、Ofcomの行動規範で提示された安全対策を講じるか、または違法なコンテンツや行為からユーザを保護するためのその他の効果的な対策を講じる必要がある。**
- **構成：①ユーザ間サービスに対して推奨する対策、②検索サービスに対して推奨する対策、③リスク評価業務に関するガイダンス、④記録保持及びレビュー業務に関するガイダンス**

●優先的な違法な危害（17種類）

①テロリズム、②子どもの性的搾取と虐待、③ヘイト、④ハラスメント、ストーカー行為、脅迫と虐待、⑤支配的または強制的な行為、⑥親密な画像による虐待、⑦過激なポルノ、⑧成人の性的搾取、⑨人身売買、⑩不法移民、⑪詐欺と金融犯罪、⑫犯罪収益、⑬薬物と精神作用物質、⑭銃器、ナイフ、その他の武器、⑮自殺の奨励・幫助、⑯外国からの干渉、⑰動物虐待。

●プロバイダが講じる安全対策の適用基準（比例性・妥当性をもって適用される）

①提供するサービスの種類（ユーザ間または検索サービス）、②サービスの機能や性能、③サービスのユーザ数、④違法コンテンツリスク評価の結果等

●対象サービスの分類

対象サービスを二つのグループに大別、さらにそれぞれを三つのサブグループに分類し、リスクに応じて対策を推奨。

1) 二つのグループ：①大規模サービス（英国人口の約10%に相当する700万人以上の月間アクティブユーザを持つサービス）、②小規模サービス（①以外のすべて、約10万と想定）

2) 三つのサブグループ：①低リスク、②シングルリスク、③マルチリスク。リスク評価業務に関するガイダンスに記載されている17種類の優先的違法危害に対するサービスのリスクアセスメントを実施する場合を想定。

【参考1】Ofcomの違法な危害に関する行動規範とガイダンス②



ユーザをオンライン上の違法な危害から保護するための対策

ユーザ間サービスのプロバイダに求められる対策	- ユーザが違法コンテンツに遭遇するのを防ぐための適切な措置を講じること - サービスを通じて犯罪が発生するリスクを軽減し、管理すること - 違法コンテンツのリスク評価を実施し、特定されたリスクを軽減し、管理すること - 違法コンテンツに気づいた場合は速やかに削除し、サービス上に存在する時間を最小限に抑えること - 利用規約で導入されている対策を説明すること - 人々が違法コンテンツを簡単に報告でき、苦情処理手続きが運用されていること
検索サービスのプロバイダに求められる対策	- 検索結果を通じてユーザが違法コンテンツに遭遇するリスクを最小限に抑えるための適切な措置を講じること - 違法コンテンツのリスク評価を実施し、特定されたリスクを軽減し、管理すること - 公開文書で導入されている対策を説明すること - 人々が違法コンテンツを簡単に報告でき、苦情処理手続きが運用されていること

出所：Ofcom.(2024/12/16). Quick guide to illegal content codes of practice.

ユーザ間サービスと検索サービス向け推奨対策の適用事例

番号	対策の項目	小規模サービス			大規模サービス		
		低リスク	シングルリスク	マルチリスク	低リスク	シングルリスク	マルチリスク
ICU A1 ～ ICU J3	【ユーザ間サービスに対して推奨する対策の項目】 ①ガバナンスと説明責任、②コンテンツ・モデレーション、③自動コンテンツ・モデレーション、④報告と苦情、⑤レコメンデーション・システム、⑥子どものユーザ向け設定・機能・サポート、⑦利用規約、⑧ユーザアクセス、⑨ユーザコントロール	事例1 違法コンテンツの迅速な削除を可能にするコンテンツモデレーション機能					
		適用	適用	適用	適用	適用	適用
		事例2 自動コンテンツモデレーション機能（ハッシュマッチングによるCSAMの検出と除去）					
ICS A1 ～ ICS G3	【検索サービスに対して推奨する対策の項目】 ①ガバナンスと説明責任、②検索モデレーション、③自動検索モデレーション、④報告と苦情、⑤設定・機能・ユーザサポート、⑥声明の公開		一部に適用	一部に適用		一部に適用	一部に適用
		事例3 違法コンテンツに対する検索モデレーション機能					
		適用	適用	適用	適用	適用	適用
		事例4 CSAMコンテンツに関する警告の提供					
					適用	適用	適用

【参考2】フェーズ3「カテゴリー別サービス」について

- 「2023年オンライン安全法」の下、対象となるすべてのオンラインサービス企業は、オンライン上の危害からユーザを保護するための適切な安全対策を講じなければならない。一部のサービスは、カテゴリー1、2A、2Bのサービスに指定され、追加義務を負う。
- カテゴリー別サービス（1、2A、2B）合計で35～60を想定。10万超とされる本法規制対象のサービスの大半は追加義務を負わない。

カテゴリー	カテゴリーの閾値（Ofcomによる勧告内容）	想定数（合計35-60サービス）
カテゴリー1 大規模なユーザ間サービス	（以下のいずれかの条件を満たすサービスに適用） ■ 条件1：コンテンツ・レコメンデーション・システムを使用。また、サービスのユーザ間部分に3,400万人超の英国ユーザがおり英国の人口の約50%を占める ■ 条件2：ユーザがユーザ生成コンテンツを転送または再共有できる。コンテンツ・レコメンデーション・システムを使用。また、700万人超の英国ユーザがユーザ間サービスを利用しており、英国の人口の約10%を占めている	12-16
カテゴリー2A 大規模な検索サービス	■ 検索サービスだが、「垂直」検索サービスではない ■ 英国の人口の約10%に相当する700万人超の英国ユーザがいる	25-40
カテゴリー2B 中小規模のユーザ間サービス	■ ユーザがダイレクトメッセージを送信できる ■ サービスのユーザ間部分には300万人超の英国ユーザがおり、英国の人口の約5%を占める	2

カテゴリー別サービス（1、2A、2B）の追加義務（Ofcomによる勧告内容）	カテゴリー1	カテゴリー2A	カテゴリー2B
透明性レポート	○	○	○
リスク評価と記録保持の厳格化された要件	○	○	
追加的な利用規約義務	○		
ニュース出版社やジャーナリスティックなコンテンツ、民主主義的に重要なコンテンツの保護	○		
ユーザのエンパワーメント機能の提供	○		
ユーザ本人確認オプションの提供	○		
不正広告の防止	○	○	
死亡した子どものユーザのサービス利用に関する情報の開示	○	○	○

英国から得られた知見／今後の展望・課題と日本への示唆

得られた知見

- 「**2023年オンライン安全法**」により導入される英国のオンライン安全規制の特徴は以下となる。
 - 事業体ではなく「サービス」が規制対象、プラットフォーム事業者の責任明確化、リスク評価の義務付け、独立性のある規制機能、年齢確認の厳格化、透明性報告の義務化、罰則規定の導入等
- 同法は、オンライン上の安全確保に向けた包括的な法的枠組である点、子どもの保護に焦点を当てた点、大手プラットフォームだけでなく小規模なサービスも対象としている点に特徴があり、一定の評価を受ける一方で、規制対象の範囲の広さ、「合法だが有害」なコンテンツの規制、暗号化通信の監視の問題、コンテンツのモニタリングや年齢確認等の実施に関する技術的な課題、実効性、イノベーションへの影響等に関して議論が続いている。

今後の展望・課題と日本への示唆

- 同法は、オンライン規制の国際的なモデルの一つと考えられ、同法の実施と影響が今後のグローバルなオンライン規制の方向性に少なからぬ影響を与える可能性がある。
- しかしながら、同法はまだ全面適用されておらず、行動規範、ガイダンス等の制定が進められている段階であり、また関連法制の導入も進められていることから、同法を含めたオンライン安全法制の全体像をとらえることが重要である。
- さらに、同法の成立においては「子どもの保護」と「表現の自由」「プライバシーの保護」の両立に向け活発な議論が行われ、現在も継続中である。日本におけるオンラインの安全の確保においても当該議論の動向、プロセスは注視すべきである。

オーストラリアの動向

- 成立の背景と過程
- 進捗状況とスケジュール
- 法規制の枠組と実行・支援体制
- プラットフォーム事業者等の反応や影響
- 最新動向
- 得られた知見／今後の展望・課題と日本への示唆

成立の背景と過程

- テロ関連コンテンツの拡散をきっかけに、既存のネットいじめ対策法を改正した「2021年オンライン安全法」が成立
- プラットフォーム事業者に対し、「オンライン上の安全に関する基本的な期待事項」の遵守を義務付ける

年月	内容
2015年3月	子どものネットいじめ対策法として「2015 年子どものオンライン安全強化法」が成立
同上	オンライン安全の専門規制機関として「eSafetyコミッショナー」が設置
2017年6月	成人のネット暴力を規制対象に拡大した改正法「2015 年オンライン安全強化法」が成立
2018年9月	「2015 年オンライン安全強化法」の規制対象に「同意のない性的画像の共有」を追加
2019年3月	クライストチャーチモスク銃乱射事件発生
2021年2月	有害／違法コンテンツの削除スキームやプラットフォーム事業者の遵守事項を規定した「2021年オンライン安全法案」が提出
2022年1月	「2021年オンライン安全法（Online Safety Act 2021）」が施行
同上	プラットフォーム事業者の遵守事項を規定する決定令 「2022年ネット安全（オンライン上の安全に関する基本的な期待事項 [BOSE] ）決定」発効
2023年6月、9月	有害／違法コンテンツ削除のための「産業コード（業界策定）」6件がeSafetyに登録
2024年4月	ウェイクリー東方教会司教殺害事件発生
2024年5月	BOSE改正。子どもの保護、生成AI及び推奨システムに対する対策を強化
2024年6月	有害／違法コンテンツ削除のための「産業標準（eSafety策定）」2件がeSafetyに登録
2024年10月	司教殺害事件に係るコンテンツ削除についての、Xとの法的係争を断念

進捗状況とスケジュール

2022	2023	2024	2025～
● 「2021年オンライン安全法」 成立 1) 基本法整備		● 「2021年オンライン安全法」 の レビュー文書公開、公的諮問実施	● <u>「2021年オンライン安全法」 改正法案の提出へ</u>
● 「2022年BOSE決定令」 発効 2) PF事業者の遵守事項		● 「2022年BOSE決定令」 改正 * 生成AI及び推奨システムに対する 対策強化。年齢確認の規定	● <u>「2021年オンライン安全法」に PF事業者の「注意義務（Duty of care）」の遵守規定を追加へ</u>
3) コンテンツ削除スキーム	● 「産業コード」 6件がeSafetyに登録 * ソーシャル・メディア・サービス * アプリ配信サービス * ホスティングサービス * インターネット配送サービス * 端末 * インターネット検索エンジン	● 「産業標準」 2件がeSafetyに登録 * 関連電子サービス * 指定インターネットサービス	● <u>「2021年オンライン安全法」 及 び「国家コンテンツ審査等級スキ ーム」 改正以降に修正か？</u>
4) 関連法令の整備		● 「国家コンテンツ審査等級スキーム」 改正に向けた公的諮問開始 ● 「誤情報／偽情報対策法案」 の提出 （12月廃案） ● 「子どものソーシャルメディア利用禁 止法案」 成立（12月）	● <u>「誤情報／偽情報対策法案」 の代 替案として、1) 性的ディープフェイ ク対策法令の強化、2) 選挙広告の誤 情報／偽情報対策法令の導入、3) AI 規制の改正、に取り組む意向</u>

法規制の枠組と実行・支援体制

法律名	「2021年オンライン安全法（Online Safety Act 2021）」
成立・施行日	■ 2021年7月成立、2022年1月施行 ■ 2024年4月に同法のレビューと公的諮問を開始（2025年以降改正法案の提出予定）
規制機関	eSafetyコミッショナー
プラットフォーム事業者への義務	「オンライン上の安全に関する基本的な期待事項（BOSE）」に基づく、実践的措置の導入・遂行、並びに定期・非定期の報告を義務付ける
義務内容	安全性に関するリスク評価／レビューの実施 サービス運営において、子どもの利益を最大考慮 暗号化等の特定機能の安全利用確保 AI、推薦等の特定サービスの安全利用確保 違法／有害コンテンツの拡散抑止
コンテンツ削除スキーム	「オンラインコンテンツスキーム」に基づき策定、登録された「産業コード」あるいは「産業標準」に従い、違法／有害コンテンツの削除を実施する。削除の適用対象は「全国コンテンツ審査等級スキーム」に規定される、「RC」「x18」「R18」分類のコンテンツが相当する。
コードの事業分類	■ 「産業コード（標準）」は、以下の事業分類を対象に個別に登録されている。 ①ソーシャルメディア ②アプリ配信 ③ホスティング ④インターネット配送 ⑤端末 ⑥検索エンジン ⑦関連電子サービス（標準） ⑧指定インターネットサービス（標準）
罰則	■ PF事業者が各種削除通告に基づく要求を遵守しない場合、500 ペナルティ・ユニット（PU.2023年7月より313AUD）の民事罰金。 ■ コンテンツの投稿者（サービスやその役員・従業員ではない）に対して刑事罰

プラットフォーム事業者等の反応や影響

「非定期報告」に基づく対策改善

- プラットフォーム事業者はBOSEの規定内容について、概ね同意している。
- ただし、個別の施策については、事業者間で対応の違いが見られており、eSafetyは個別の懸念事項について「非定期報告」を適宜、各社に要請し、オンライン安全対策の強化を促している。。
- 例えば、子どもの性的搾取及び虐待（CSEA）に関する「非定期報告」の主な内容は以下のとおり。
 - Discordは公開コンテンツ内でのCSEAを検出する対策を未実施。Xは未回答（＊罰金措置が取られた）。
 - Discordは言語分析技術に基づく検出ツールの実装なし。GoogleはYouTubeのみ実装し、他のサービスは実装なし。Xは公開コンテンツには実装済みだが、DMには実装なし。

出所：<https://www.esafety.gov.au/newsroom/media-releases/second-set-of-tech-giants-falling-short-in-tackling-child-sexual-exploitation-material-sexual-extortion-livestreaming-of-abuse>

「注意義務」規定の導入

- 政府は2024年11月、「2021年オンライン安全法」に新たに「注意義務（Duty of care）」規定を追加する意向を表明。
- 同規定のもと、プラットフォーム事業者は自社サービスに潜むリスクを主体的に評価し、軽減するための具体的な取り組みを継続的に実施することを求められる。
- 今後、技術やサービスが進化する過程においても、プラットフォーム事業者が単に設定を維持したまま放置する対応は許容されなくなる。

オーストラリアの最新動向①

「子どものSNS禁止法案」の成立

- 「2021年オンライン安全法」の改正法案「Online Safety Amendment (Social Media Minimum Age) Bill 2024」が、2024年12月に可決成立。可決から1年以内に施行の予定。
 - 16歳未満の子どもがソーシャルメディアのアカウントを作成することを禁止する内容。
 - プラットフォーム事業者には、子どものSNSアカウント作成を防止する「合理的な段階（reasonable steps）」を講じる義務がある。子ども自身や保護者に対しては義務は課されない。
 - 年齢確認技術はソーシャルメディア側の責任で採用。公的身分証明書の利用は強制されない。
 - 義務不履行に対しては、最大4,950万AUD（約48億円）の罰金措置。
 - プラットフォーム事業者には、年齢確認の際に使用した個人情報を「隔離（ring-fence）」し、破棄することが義務付けられる。
 - 義務不履行に対しては、最大5,000万AUD（約48億3,300万円）の罰金措置。
 - メッセージング、オンラインゲーム、教育や健康促進を目的としたサービス/アプリについてのアカウント作成は規制対象外。

出所： <https://minister.infrastructure.gov.au/rowland/media-release/social-media-reforms-protect-our-kids-online-pass-parliament> 等

「誤情報及び偽情報対策法案」の廃案

- 主に「1992年放送サービス法」の改正法案「Communications Legislation Amendment (Combating Misinformation and Disinformation) Bill 2024」が2024年9月に提出。同12月に成立断念。
- 現状、偽情報／誤情報に関しては、デジタル業界団体DIGIが策定した行動規範「Australian Code of Practice on Disinformation and Misinformation」により自主規制。

法案の内容

- 誤情報／偽情報の定義づけ
 - 「虚偽である、誤解を招くもの、または欺瞞的であると合理的に検証可能」で、深刻な害を及ぼす可能性のあるコンテンツと定義。公衆衛生や選挙運営に対する脅威、団体への中傷も含まれる。
- 通信メディア庁(**ACMA**)にプラットフォーム事業者への規制権限を付与
 - 情報収集と記録管理、産業コード(または標準)の登録(または策定)
 - 誤情報／偽情報に関するプラットフォーム事業者とユーザとの間の紛争処理について規則制定
- プラットフォーム事業者に透明性確保を義務付け
 - リスク評価方法、偽情報/誤情報対策の方針、およびユーザーが当該のコンテンツを特定することに寄与するメディアリテラシー計画を公開することを義務付け。

廃案の理由(批判意見)

- 「表現の自由」への懸念
- 「誤情報／偽情報」の定義の曖昧さ
- 政府により判断基準が偏向する可能性
- 法令を運用する上での**ACMA**の専門知識、執行能力の不足

得られた知見

- 「2021年オンライン安全法」は、日本を含む世界各国で同様な法律が制定されつつある中、最も先行して施行された包括的オンライン安全法制であり、運用実績も先行している。
- ただし、同法は既存の「ネットいじめ法制」を改正して成立した法令で、同時に有害コンテンツの基準も既存のレーティング制度に依存しており、AI、偽情報、年齢確認といった新興技術によって生じている課題に対する対応は不十分である。
- 1) 専門規制機関の設置：オンラインの包括的な独立規制機関eSafetyコミッショナーを設置した点、2) プラットフォーム事業者の自主的取り組みを中核にした制度である点、3) 提供業種の細分化：各業種の業務内容に応じたコンテンツ削除方法を規定している点に特徴がある。

今後の展望・課題と日本への示唆

- 同法の課題は上述の通り、新興技術に基づく新たなオンライン安全上の懸念に十分対応できていないことにある。
- 2024年5月に「BOSE決定」が改正、AIや年齢確認等への対応をプラットフォーム事業者に求めることが可能となった。
- 同法の日本に対する示唆として最重要となるものは、「ネット安全専門の規制機関の設置」であろう。同時に、そのような機関が運用する「有害情報通報システム」は、ネット安全を脅かす事態を把握するシステムとして非常に有意義である。
- ただし、国際的に拡散したコンテンツについては、法令及びeSafety権限の「域外適用」が課題となり、他国の言論団体からの介入が生じた事例もある。

国際協力枠組「**GOSRN**」の動向

国際協力枠組「GOSRN」の動向

- 2023年9月、英国のOfcom、オーストラリアのeSafetyを含む、オンライン安全規制当局の連合「Global Online Safety Regulators Network : GOSRN」が結成。国際連携強化ビジョンとして「規制の一貫性と調整」を掲げる。
- 目的は、洞察、経験、優良事例を共有し、オンライン安全規制への首尾一貫した国際的アプローチへの道を開くこと。商業的・政治的影響から独立して行動し、人権、民主主義、法の支配の尊重を遵守する方針を提示。

協力項目	内容	規制当局
規制ツール	規制ツール間の不当な乖離の最小化に向け、リスクアセスメントの方法論と評価手法の共通指標を開発	通信庁（Ofcom）（英）、eSafety Commissioner（豪）、Online Safety Commission（フィジー）、Arcom（仏）、Coimisiun na Meán（アイルランド）、放送通信審議委員会（韓国）、Council for Media Services（スロバキア）、Film and Publication Board（南アフリカ）、Autoriteit Terroristische Content en Kinderpornografisch Materiaal（オランダ）。
ユーザからの苦情	経験と証拠を共有。法域を超えた体系的コンプライアンス違反の事例に関して、調査や強制措置において緊密に協力	オブザーバー （オンライン安全規制に関する専門知識と関心を持つ団体）
情報要請	規制活動の一環として産業界への質問を調整。傾向分析に役立つ比較可能なグローバルデータを作成	5Rights（国際）、Canadian Centre for Child Protection（加）、カナダ文化遺産省（加）、European Parliament Intergroup on Children’s Rights（EU）、Family Online Safety Institute（国際）、Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e.V.（FSM）（独）、INHOPE（国際）、Netsafe（ニュージーランド）、Te Mana Whakaatu-Classification Office（ニュージーランド）、WeProtect Global Alliance（国際）
安全対策	優良事例の経験を活用し、特定の危害やリスク要因に対処するためにサービスが取り得る合理的な措置の共通セットを特定	

GOSRN：オンライン安全規制機関の権限と機能

- オンライン安全規制機関の権限と機能によるアプローチは、コンテンツベース、システム及びプロセスベース、またはハイブリッドアプローチに分類。
 - コンテンツベースでは、ユーザに対する苦情と救済（**redress**）メカニズムを通じて、有害なコンテンツに対処することに重点。システム及びプロセスベースでは、デジタルプラットフォームやサービスの設計や運用に要件を課すことで、内蔵の安全対策によりリスクを軽減することに重点。
 - 英国Ofcomによるオンライン安全規制は、システムベースのアプローチであり、サービスに対してリスク評価と違法・有害コンテンツからの保護措置の導入を要請し、一部のサービスには追加義務を課す。オーストラリアeSafetyは、コンテンツとシステム及びプロセスのハイブリッドアプローチ。コンテンツベースとしては、ユーザからの有害コンテンツの報告を受けるとともに、暴力的コンテンツに対応する権限も持つ。またシステム及びプロセスベースとしては、「産業コード」あるいは「産業標準」と「オンライン上の安全に関する基本的な期待事項（BOSE）」という二つの枠組を導入。
- 全規制機関が執行権限を持ち、啓蒙普及活動を実施。多くがユーザからの苦情を受け調査を実施。業界の行動規範を策定・施行する権限も持つ場合もある。

オンライン安全規制機関の権限と機能										＊「○」は権限有り、「×」は権限無し			
規制機関	事前規制	ユーザからの苦情と調査					情報収集と実行			予防研究と関与			
	規範、基準、 指針の策定 と施行	プロアク ティブ・コ ンテンツ・ スキャン	ユーザから の苦情を受 け付け、調 査する	コンテンツ 削除及びブ ロック通知 の発行	法執行機関 及びホット ライン・ ネットワー クとの連携	サービスの 遮断または 制限命令	監督と透明 性	コンプライ アンス違反 の通知と罰 金	裁判所命令 と差止命令	教育と意識向 上	助成金	リサーチと ホライズ ン・スキャン	業界の関与
Ofcom（英国）	○ ^{（注1）}	×	×	×	×	○	○	○	○	○	×	○	○
eSafety（豪州）	○	×	○	○	○	○	○	○	○	○	○	○	○
OSC（フィジー）	×	×	○	○	○	×	×	○	○	○	×	×	○
Arcom（フランス）	○	×	○	○	○	○	○	○	○	○	×	○	○
Coimisiun na Meán （アイルランド）	○	×	○	○	○	○	○	○	○	○	×	○	○
放送通信審議委員会 （韓国）	○	○	○	○	○	○	×	○	○	○	○	○	○
Council for Media Services（スロバキア）	○	○	○	○	○	○	○	○	×	○	×	○	○
Film and Publication Board（南ア）	○	○	○	○	○	×	○	○	○	○	×	○	○

（注1） Ofcomは法的義務を強制することができ、拘束力のない規範および指針を策定することができる。（注2） しかし、Ofcomは法執行機関及びホットラインネットワークと関わりを持っている。

GOSRN：規制対象となるオンライン上の危害

- 法的な定義や分類の枠組が異なるため、オンライン上の危害の単純比較は難しい。
- すべての法域で違法な危害や青少年に有害なコンテンツを規制しているが、具体的な定義は異なる。違法なコンテンツには、通常、子どもの性的搾取・虐待コンテンツ（CSEM/CSAM）、テロリズム・暴力的・過激主義コンテンツ（TVEC）、暴力、性的搾取、違法な薬物/武器が含まれる。ただし、一部の法域では、ヘイトスピーチ、名誉毀損、ポルノも違法と分類されている。
- 有害なコンテンツ（制限付きコンテンツや年齢に不適切なコンテンツとも定義される）は、子どもに何が有害であるかについての国の基準が異なるため、異なる。ポルノは一部の法域では違法だが、他の法域では制限されているだけとなる。
- 「虐待やハラスメント」にオンライン上のヘイトや差別を含む場合があり、「ヘイトスピーチ」には狭義（言語のみ）と広義（画像や記号含む）がある。
- 規制の権限と執行は、危害のカテゴリーによって異なる。深刻な危害（CSAM、CSEM、TVEC）は、管轄区域全体で最も厳しい規制の対象となる。

オンライン上の危害のタイプ *「○」は規制対象、「×」は規制対象外															
規制機関	CSEM／CSAM	TVEC／テロリズムの助長	ヘイトスピーチと差別	違法コンテンツ	詐欺と経済的損害	暴力の扇動と描写	偽・誤情報	画像に基づく虐待親密な画像の非同意の共有	子どものネットいじめ	虐待とハラスメント	危険行為の助長（摂食障害、自傷、自殺、危険行為等）	有害なアルゴリズムパターン	名誉毀損	国益に反する内容	ポルノグラフィ
Ofcom（英国）	○	○	○	○	○	○	× ^(注1)	○	○	○	○	○	×	×	○
eSafety（豪州）	○	○	× ^(注2)	○	×	○	×	○	○	○	×	×	×	×	○
OSC（フィジー）	○	○	×	○	×	○	×	○	○	○	×	×	×	×	○
Arcom（フランス）	○	○	○	○	○	○	○	○	○	○	○	○	○	×	○
Coimisiun na Meán（アイルランド）	○	○	○	○	○	○	○	○	○	○	○	○	×	×	○
放送通信審議委員会（韓国）	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Council for Media Services（スロバキア）	○	○	○	○	×	○	×	×	×	○	×	×	×	×	×
Film and Publication Board（南ア）	○	○	○	○	○	○	○	○	○	○	×	○	×	×	○

（注1）誤情報が外国による干渉及び虚偽通信罪に該当する場合は処罰される可能性がある。カテゴリー1のサービスは、利用規約で禁止されている場合、特定の種類の誤情報や偽情報の削除が必要となる。

（注2）eSafetyは成人によるサイバー虐待または児童に対するサイバーいじめの基準を満たすオンラインでの憎悪や名誉毀損のみを規制。オーストラリアには、特定のヘイトスピーチや差別に対処する刑事法および民事法が別途存在する。

GOSRN：規制対象となる事業体

- 規制対象となる事業体の分析は複雑で、多くの定義上の課題があるため、単純な比較はできない。特に、ソーシャルメディア・サービス、動画共有プラットフォーム及びサービス、ユーザ間プラットフォーム及びサービスを重複して提供する事業者が多く、一部を切り離して分類・定義する法域もあれば、大きくまとめて分類・定義する法域もある。
- 例えば、YouTubeやTikTok等の動画共有プラットフォーム及びサービスは、英国ではバイラル性のリスクにより規制対象事業者として別個に分類・定義されるが、オーストラリアでは法的に定義された規制対象のカテゴリーではなく、ソーシャルメディア・サービスの定義でとらえられている。
- 重要な点は、全ての国・地域が、大規模なオンラインプラットフォームとサービスを何らかの形で規制対象としていることである。

規制対象となるデジタル・サービス及びプラットフォームのカテゴリー											*「○」は規制対象、「×」は規制対象外
規制機関	ソーシャルメディア、動画共有プラットフォーム及びサービス、ユーザ間プラットフォーム及びサービス	ホスティング及びストレージサービス	ゲームサービス	アプリ配信サービス	インターネット・サービス・プロバイダ	メッセージング・サービスと出会い系アプリ	エンド・ツー・エンドの暗号化サービス	検索エンジンサービス	ウェブサイト	生成AIサービス	設備サービス
Ofcom（英国）（注1）	○	○	○	×	×	○	○	○	○	○	×
eSafety（豪州）	○	○	○	○	○	○	○	○	○	○	○
OSC（フィジー）	○	×	○	×	×	○	○	○	×	×	×
Arcom（フランス）	○	×	○	○	○	○	×	○	○	×	×
Coimisiun na Meán（アイルランド）	○	○	○	○	○	○	○	○	○	×	×
放送通信審議委員会（韓国）	○	○	○	○	○	○	○	○	○	○	○
Council for Media Services（スロバキア）	○	○	○	○	○	○	○	○	×	×	×
Film and Publication Board（南ア）	○	○	○	○	○	○	○	○	×	○	×

（注1）英国では、ユーザ間サービス、検索サービス、ポルノコンテンツサービスの提供事業者のみが「2023年オンライン安全法」に基づく規制対象となっており、「○」とマークされたカテゴリーはそれらの事業者が提供するものである。

GOSRN：規制対象となるサービス及びプラットフォームの義務

- オンラインプラットフォームの規制義務は複雑で、単純比較は難しい。規制上の義務や要件が、規制対象となるオンライン上のあらゆる種類の被害や規制対象事業者等に等しく適用されるとは限らない。さらに、規制対象事業者の単一のカテゴリ内でも規制の適用方法に大きなばらつきがある。
- ほとんどの管轄区域では、特定のプラットフォームやサービスのリスクに見合った規制を行うために、リスクベースのアプローチを採用しており、規模が大きく、リスクの高いプラットフォームに対して、より厳格で負担の大きい要件を課している。
- リスクの評価は、管轄区域によって異なっており、以下の要素を考慮している：ユーザ数と人口統計、地理的なリーチ、プラットフォームの機能、有害なコンテンツの種類と頻度、オンラインの危害の可能性（likelihood）と影響、アルゴリズムとレコメンデーション・システムの使用。

規制対象となるサービス及びプラットフォームの義務

*「○」は規制要件、「×」は非規制要件

規制機関	法的通知を受け取ることができる国内代理人の指定	コンテンツ削除、ブロック、リンク削除の通知に従う	内容通知の適時性要件を遵守する	登録された規範と基準に準拠する	情報要求への適切な対応	透明性報告及び監督要件の遵守	リスク評価の実施	適切なガバナンスの確立	記録管理	必要に応じて監査を受ける	有害で違法なコンテンツを積極的に最小限に抑える	ユーザに選択肢を与える	年齢保証システムの導入	年齢不相応なコンテンツから子どもを保護するための合理的措置をとる	E2EE及び匿名サービスの安全性を確保するための合理的措置をとる	ユーザによる報告メカニズムの提供	明確で利用しやすい利用規約の提供と実施	オンラインの安全性に関する専門教育を受ける
Ofcom（英国）	×	×	×	○	○	○	○	○	○	○	○	○	○	○	○	○	○	×
eSafety（豪州）	×	○	○	○	○	○	○	○	○	×	○	○	×	○	○	○	○	×
OSC（フィジー）	×	○	○	×	×	×	×	×	×	×	×	×	×	○	×	○	×	×
Arcom（フランス）	○	○	×	○	○	○	○	○	○	○	○	○	○	○	×	○	○	×
Coimisiun na Meán（アイルランド）	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
放送通信審議委員会（韓国）	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Council for Media Services（スロバキア）	○	○	○	○	○	○	×	×	○	×	×	○	×	○	×	○	○	×
Film and Publication Board（南ア）	○	○	○	○	○	×	○	×	×	×	○	×	×	○	×	○	×	×

GOSRN：情報収集と執行

- ほとんどの規制機関が、通知や監督機能を通じて情報を入手する権限と、金銭的な罰則や裁判所の命令による救済措置という執行権限が付与されているが、すべての違反事例において、すべての執行権限が利用できるわけではない。
- 事業中断命令や民事罰金は、違反が繰り返された後にのみ適用されることが多い。
- 一部の規制機関は、コンテンツの削除期限を逃した場合に罰金を科している。
- 罰金額は多様である。

情報収集と執行																
規制機関	コンテンツに基づく強制措置				情報収集の権利						システム・ベースの規制執行		裁判所命令の救済措置			
	書面による正式な警告	消去、削除、ブロック通知	アカウントの削除や特定の個人の排除を目的とする指示や通知	罰金	情報通知	監督権限	透明性報告要件	第三者による監査	面接要請	立ち入り、検査、監査の権限	書面による正式な警告と改善指示（誓約書等）	罰金	民事および行政罰	差止命令	サービスの遮断または制限命令（例：サービス、アクセス、支払いの遮断命令）	損害賠償
Ofcom（英国）	×	×	×	×	○	○	○	○	○	○	○	○	×	○	○	○
eSafety（豪州）	○	○	○	○	○	×	○	×	○	×	○	○	○	○	○	×
OSC（フィジー）	○	○	×	○	×	×	×	×	×	×	×	○	○	○	×	○
Arcom（フランス）	○	○	○	○	○	○	○	○	○	○	○	○	×	×	○	○
Coimisiun na Meán（アイルランド）	×	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
放送通信審議委員会（韓国）	○	○	○	○	○	×	×	○	○	×	○	○	○	○	○	○
Council for Media Services（スロバキア）	○	○	×	○	○	○	○	×	○	○	○	○	×	×	×	×
Film and Publication Board（南ア）	○	○	○	○	○	○	×	○	○	×	×	○	○	○	×	○

* 「○」は執行対象、「×」は執行対象外

まとめ：得られた知見／今後の展望・課題と日本への示唆

得られた知見／今後の展望・課題と日本への示唆

得られた知見

- 英国の「**2023年オンライン安全法**」は子どもを保護する実践的措置の導入・遂行を義務付けており、オーストラリアの「**2021年オンライン安全法**」は既存のネットいじめ法制を改正した法律である。両法はともに、社会的事件を契機とした世論の高まりを背景に成立したもので、「オンライン上の子どもの保護」に焦点が当てられている。
- その一方で、英国の**Ofcom**によるオンライン安全規制はシステム及びプロセス・ベースのアプローチをとり、オーストラリアの**eSafety**はコンテンツ・ベースとシステム及びプロセス・ベースのハイブリッド・アプローチをとっており、規制アプローチには違いがみられる。**GOSRN**に参加する国々は、人権、民主主義、法の支配等、同じ価値観を共有するとしつつも、それぞれの法制度、規制構造、社会状況を踏まえ、現時点ではそれぞれの規制には特徴がある。
- 両法を巡っては「子どもの保護」と「表現の自由」及び「プライバシーの保護」を巡る議論が活発化したが、両国の産官学民の利害関係者が、両価値の比較衡量ではなく両立することを目指し、現在もなお議論が続いている。

今後の展望・課題と日本への示唆

- 両法は以下の点から、日本を含め世界各国に影響を及ぼす可能性がある。1) 両法に基づくオンライン安全規制が特に子どもの保護における実践的先進事例となること。2) 英国の「2023年オンライン安全法」が英国外の企業にも適用される可能性があること。3) オーストラリアの「2021年オンライン安全法」は2021年に成立しており、比較的豊富な執行事例があること。4) 「GOSRN」を通じて、人権、民主主義、法の支配を遵守する立場から、今後は、国際的オンライン安全規制の一定程度の共通アプローチが形成される可能性があること。
- 現在、両国のオンライン安全法制においては、行動規範やガイダンス、関連法等の整備が進展中であり、両法を含むオンライン安全法制全体の枠組や内容をとらえることが重要である。
- 今後、注目すべき点として、両法に基づく具体的な執行事例の他に、急速に進化する**AI**技術への対応、コンテンツのモニタリング、年齢確認の仕組み等、実践的・技術的な対策の導入動向が挙げられる。



一般財団法人

マルチメディア振興センター

Foundation for MultiMedia Communications