総務省
デジタル空間における情報流通に係る制度ワーキンググループ（第４回）

未定稿

資料４－２

違法・有害情報に関する諸外国の対応状況

株式会社野村総合研究所

コンサルティング事業本部
ICT・コンテンツ産業コンサルティング部

2025年4月3日

Envision the value,
Empower the change

目次

１．違法・有害情報に関するその他の措置（諸外国動向調査①、②以外）

1－1．レコメンダシステムに関する対応

各国制度の概要（DSA・OSA）

項目	DSA（Digital Services Act）	OSA（Online Safety Act）
背景・目的	• 市民がニュースの消費や政治的議論におけるソーシャルメディアの重要性に鑑み、レコメンダシステムの悪用による偽情報の拡散を問題視。 • レコメンダシステムに関する説明責任のスタンダードや情報源の信頼性を示す指標をユーザーに提供することで、公共の利益に関する信頼性の高い情報の流通と意見の多様性の確保を目指している。	• レコメンダシステムには、ユーザーの体験向上やエンゲージメントの最大化等のメリットがあるものの、レコメンダシステムのアルゴリズムが「エコーチェンバー」や「フィルターバブル」を引き起こすこと、リスクを持つ違法コンテンツの拡散を増幅することを問題視。 • レコメンダシステムの設計を調整する際に自社のサービス上で実施するテストにおいて、組み込むべき安全性指標を推奨することで、サービス提供事業者は、自社のレコメンダシステムが違法コンテンツのリスクにつながるかどうかを理解でき、アルゴリズムに関連するリスクを適切に管理し、流通・拡散する違法コンテンツの量の削減につなげることを目指している。
制度の概要	• PF事業者がレコメンダシステムを使用している場合、利用規約に「レコメンダシステムで使用する主なパラメータ」と「利用者が当該パラメータを変更できる選択肢」を平易かつ分かりやすい言葉で記載することを義務付け(27条)。 • レコメンダシステムを使用しているVLOP/VLOSEに対しては上記の義務に加え、プロファイリングに基づかない選択肢を提供しなければならないことを義務付け（38条） • また、リスク評価（34条）を踏まえた軽減措置（35条）の例として、「レコメンダシステム等のアルゴリズムシステムの適合」がある（35条1項(d)）	• ユーザー間サービス提供事業者に対し、安全義務（10条4項）の１つとして、サービスの機能、安全設計に関する措置を組み込むことを義務付け。 • OSAに基づきOfcomが策定した「安全義務に関する行動規範」において、自社のレコメンダシステムをリリース前に実施するテストの際に、推奨される措置を規定。

1－1－1．EUにおけるDSA （Digital Services Act）の レコメンダシステムに関する対応

PF事業者がレコメンダシステムを使用している場合、使用する主なパラメータを利用規約に明記など、一定の対応を義務付け。

- PF事業者がレコメンダシステム（※1）を使用している場合、利用規約に「レコメンダシステムで使用する主なパラメータ」と「利用者が当該パラメータを変更できる選択肢」を平易かつ分かりやすい言葉で記載することを義務付け(27条)。
- レコメンダシステムを使用しているVLOP/VLOSEに対しては上記の義務に加え、プロファイリングに基づかない選択肢を提供しなければならないことを義務付け（38条）
- また、リスク評価（34条）を踏まえた軽減措置（35条）の例として、「レコメンダシステム等のアルゴリズムシステムの適合」がある（35条1項(d)）

＜レコメンダシステムの透明性（27条）＞

対象事業者	● レコメンダシステムを使用するPF事業者
義務の内容	● **利用規約に、以下の内容を平易で分かりやすい言葉で記載しなければならない**（27条 1 項） - レコメンダシステムで使用される主なパラメータ - 利用者が当該パラメーターを変更できる選択肢 ● **上記の主なパラメータには**、特定の情報がサービス利用者に提案される理由を説明するものとし、**少なくとも以下が含まれなければならない**（27条2項）。 -サービス利用者にレコメンドされる情報を決定する上で、最も重要な基準（27条2項a） -当該パラメータがなぜ重要であるかの理由（27条2項b） ● 第 1 項に従い、**複数のレコメンド方法を選べる場合、利用者が自分の好みのレコメンド方法をいつでも選択・変更できる機能を提供しなければならない。**当該機能は、情報の優先表示が行われているオンラインインターフェース内の該当箇所から、直接・簡単にアクセスできる状態でなければならない（27条3項）

＜レコメンダシステムにプロファイリングに基づかない選択肢の提供（38条）＞

対象事業者	● レコメンダシステムを使用する大規模PF事業者（VLOP）
義務の内容	● レコメンダシステムに少なくとも1つ、**プロファイリング**（※2）**に基づかない選択肢を提供しなければならない。**(38条)

（※1）レコメンダシステム：ユーザーによって開始された検索の結果として、又はその他の方法で表示される情報の相対的な順序又は優先順位を決定することを含め、ユーザーにオンラインインターフェイスでの特定の情報を提案し、又はその情報に優先順位を付けるためにオンラインプラットフォームによって使用される完全又は部分的に自動化されたシステム
（※2）「プロファイリング」とは、個人データを使用して自然人に関する特定の個人的側面を評価すること、特にその自然人の仕事のパフォーマンス、経済状況、健康、個人的な好み、興味、信頼性、行動、場所、または移動に関する側面を分析または予測することからなる、個人データのあらゆる形式の自動処理を意味する（一般データ保護規則（GDPR）4条4項）。

（参考）DSAのレコメンダシステムに関する制度―背景

レコメンダシステムによる偽情報の拡散などの政治的言論空間への悪影響が問題視されていた

- DSAの制定に先立ち、欧州委員会が2020年に公表した「欧州民主主義行動計画（Europe Democracy Action Plan）」において、DSAおよび「偽情報に関する行動規範」の目的として**レコメンダシステムに関する規制**が示されている。
  - 欧州委員会による同計画のコミュニケ（声明文）では、市民がニュースの消費や政治的議論におけるソーシャルメディアの重要性に鑑み、**レコメンダシステムの悪用による偽情報の拡散を問題視**している。
  - また、レコメンダシステムに関する説明責任のスタンダードや情報源の信頼性を示す指標をユーザーに提供することで、**公共の利益に関する信頼性の高い情報の流通**と**意見の多様性**の確保を目指している。
- 上記の背景には、SNSのレコメンダシステムが異なる意見をもつユーザー間の対立を深め、世論の分断を助長するよう作用したという問題意識が見てとれる。
  - 特に「ケンブリッジ・アナリティカ事件」では、Facebookのレコメンダシステムを利用して、ターゲティング広告や政治的メッセージの表示を意図的に操作することでユーザーの認知や行動に作用し、2016年の米国大統領選挙や英国のEU離脱の選挙結果に影響を与えたとされる。

4.2 オンラインプラットフォームのさらなる義務と説明責任（「欧州民主主義行動計画に関するコミュニケ」より一部抜粋）

ソーシャルメディアプラットフォーム上で交換される情報は、ニュースの消費や政治的議論においてますます重要になっている。・・・（中略）・・・市民が関連情報にアクセスしやすくするランキングやレコメンダアルゴリズムといったシステムも、特に組織的な偽装行為を通じて、オンラインプラットフォーム上で**偽情報の広範な拡散を容易にするために操作される可能性**がある。プラットフォームによる入念な検査と、ユーザーや研究者に対する有意義な透明性は、このような脅威をよりよく理解し、対処するのに役立つ。

・・・「強化された偽情報に関する行動規範」は、以下の目的を達成を企図する:

―レコメンダシステムおよびコンテンツのランキングシステムに対する**説明責任のスタンダード**（共同作成のベンチマーク）を策定し、**情報源の信頼性を示す指標へのアクセス**をユーザーに提供することで、**公共の利益に関する信頼性の高い情報の可視性を十分確保し、多様な意見を担保する。**・・・

出所）欧州委員会 「欧州民主主義行動計画に関するコミュニケ」 https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0790

（参考）事業者による取組状況｜欧州におけるレコメンダシステムに関連する利用規約等の内容 TikTokの例

利用規約の記載

内容

プラットフォームでは、ユーザーや他のユーザーがコンテンツを作成、閲覧、操作、共有したり、他のユーザーとやり取りしたりすることができる。また、TikTokアプリでは「For You」フィードを用いて、ユーザー体験の一部をパーソナライズすることができる。「For You」フィードは、TikTok独自の機能で、レコメンダシステムを使用して、ユーザーが興味を持ちそうな幅広いコンテンツ、クリエイター、トピックを発見できるようにする。レコメンドされるものを決定する際、システムはいいね、共有、コメント、検索、コンテンツの多様性、人気動画などの要素を考慮する。詳しい内容は「TikTokがコンテンツをおすすめする方法」を参照ください。

「TikTokがコンテンツをおすすめする方法」の記載（「おすすめフィード」の説明を一部抜粋）

内容

【TikTokでコンテンツがレコメンドされる仕組み】 **DSA第27条1項・2項に関係する内容**　　：NRIが関連性を確認した条文

TikTokは複数の要素に基づいて、コンテンツがユーザーとどれほど関連が高いか、およびコンテンツにユーザーがどれほど興味を持つかを推測し、コンテンツをおすすめしています。主な3つの要素は、ユーザーによるリアクション、コンテンツの情報、およびユーザーの情報です。

- **ユーザーのリアクション**
  - 「いいね」したコンテンツ、シェアしたコンテンツ、コメントしたコンテンツ、フル視聴またはスキップしたコンテンツ、フォローバックしたフォロワーのアカウント。
- **コンテンツ情報**
  - サウンド、ハッシュタグ、視聴回数、コンテンツが公開された国。
- **ユーザー情報**
  - デバイス設定、言語設定、場所、タイムゾーンと日付、デバイスの種類。

ほとんどのユーザーにとって、動画の視聴に費やした時間など、**ユーザーのリアクションは通常、他の要素よりも重視**されます。

【TikTokがコンテンツをおすすめする方法に影響を与える他の要素】 **DSA第27条1項に関係する内容**

- 関連度の高いコンテンツ、新しく多様およびクリエイターとの出会いがあるコンテンツ、新しい視点や発想を体感できるコンテンツをバランスよくおすすめするために、自分が表明している**興味とは関連がないコンテンツがおすすめフィードに表示される可能性**がある。
- **一部のユーザーには適していないと思われるコンテンツ**が、おすすめとして表示される可能性が低くなるようにしている。

【TikTokに表示される内容をコントロールする方法】 **DSA第27条3項、第38条に関係する内容**

TikTokに登録するときに、興味のあるカテゴリーを選択することに加えて、以下の機能を使用すると、おすすめフィードに表示される内容をコントロールできる。

- **興味がない**
  - 特定のコンテンツに興味がない場合は、そのコンテンツに興味がないことをTikTokにシェアすると、似たコンテンツが表示される頻度が減る。
- **フィード更新**
  - おすすめフィードでおすすめされるコンテンツを更新したり、人気のコンテンツに「いいね」やコメントなどをすることで、おすすめフィードのおすすめコンテンツを再度コントロールできる。
- **動画キーワードのフィルター**
  - フィルターを使って、フィードから、特定のキーワード、類似キーワードおよびハッシュタグを含むコンテンツを除外できる。

出所）以下の公開情報より一部を抜粋して記載。より詳細な例示は出所を参照。
利用規約：https://www.tiktok.com/legal/page/eea/terms-of-service/en
おすすめする方法： https://support.tiktok.com/en/using-tiktok/exploring-videos/how-tiktok-recommends-content

（参考）行政機関の制度の執行状況｜27条・38条違反に関する調査（AliExpressの場合）

2024/3/14
法的手続開始

- 欧州委員会は、AliExpress（※）がDSAに違反している可能性があるかどうかを評価するための法的手続を開始。
- AliExpressは、VLOPに指定されており（2023年4月指定）、AliExpressは、レコメンダシステムで使用される主なパラメータを公開し（DSA27条）、プロファイリングに基づかない選択肢を少なくとも 1 つユーザーに提供する（DSA38条）ことが義務付けられているが、これらを提供していないことが疑われた。

※中国最大の越境小売ECプラットフォームを運営するアリババの国際市場向けECプラットフォーム

調査の焦点	内容
レコメンダシステムの透明性（ユーザへの説明）の不履行	• AliExpressは利用規約において、ユーザが特定の情報を利用できるようにしているが、その情報は表面的にレコメンダシステムに言及するに留まる。欧州委員会は、この情報では、**プロファイリングやユーザーのオンライン上の行動に基づいてレコメンドされている情報（レコメンダシステムに影響を与えるさまざまなパラメータ/システムについて等）を適切に説明できていない**と疑っている。このような不備が確認されれば、DSAの第27条1項・2項の違反となる。
プロファイリングに基づかないレコメンダシステム提供の不履行	• さらに、AliExpressはユーザーが利用できるプライバシー設定のオプトアウトの選択肢が限られていること（選択肢が住所、端末情報、閲覧履歴のみのオプトアウトに限定されている）を考慮すると、**ユーザが、各レコメンダシステムについて、プロファイリングに完全に基づかない選択肢を選択できない**のではないかと疑っている。このような行為が確認されれば、DSAの第38条に違反することになる。

※：その他、AliExpressは本手続で、DSAの16条（通知と対応メカニズム）、20条（異議申立て制度）、26条（オンライン プラットフォームでの広告）、30条（トレーダーの情報提供）、34条（リスク評価）、35条（リスク軽減措置）、39条（オンライン広告の透明性向上）、40条（研究者のデータアクセス）の違反についても疑われている。

出所）https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1485

（参考）DSA（アルゴリズム関係）の執行支援機関（ECAT）

- 名称：欧州アルゴリズム透明性センター（ECAT）
- 設立：2023年4月
- 所在地：スペイン（セビリア）
- 設立目的：デジタルサービス法（DSA）の執行を支援するための科学的・技術的専門知識を提供し、オンラインプラットフォームや検索エンジンによって導入されている**アルゴリズムシステムの影響に関する研究を進めることを目的**。
- その他：通信ネットワーク・コンテンツ・技術総局（DG CONNECT）と緊密に連携して活動。

活動項目	具体的内容
プラットフォームの調査・分析	• アルゴリズムシステムの検査を通じてDSAの執行を支援 • アルゴリズムシステムの動作を理解するための技術的テスト • 規制当局や研究者によるデータアクセス確保の手続きに関する助言
科学的研究と将来展望	• アルゴリズムシステムによる短期・中期・長期の社会的影響の研究 • 非常に大規模なオンラインプラットフォーム（VLOPs）や非常に大規模な検索エンジン（VLOSEs）に関連するシステミックリスクの特定・測定・対策の検討 • 特にレコメンドシステムや情報検索を対象とした、公正・透明・説明可能なアルゴリズム手法の実践的手法の開発
ネットワーキングとコミュニティ形成	• 国際的な関係者との知識共有や討論の促進 • DSAによって得られるデータを用いた研究の知識ハブとしての役割

（出典）https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/illegal-harms/volume-2-service-design-and-user-choice.pdf?v=390978　を基にNRI作成

１－１－２．英国におけるOSA （Online Safety Act）の レコメンダシステムに関する対応

（参考）OSAにおける施行スケジュール

OSAにおける各種義務は、義務の対象となるサービスの種類に応じて、3段階に分けて施行する予定となっており、Ofcomには、情報の種類等に応じて（フェーズ1~3）、行動規範およびガイダンスの発行が義務付けられている

■ OSAの監督・執行は、Ofcomが担う。

- OSAの施行に際しては、**Ofcomに対して、オンラインサービス事業者に課される義務に対する行動規範（Code of Practice）の公表が義務付けられている（41条）**
- また、PF事業者が同法が定める義務の遵守を支援するための**ガイダンスを発行することも義務付けている（52条、53条、54条等）**

Ofcomによる、行動規範やガイダンスの整備

	フェーズの概要	ステータス　灰字：今後の予定
フェーズ1: 全てのサービスに課される義務	• 全てのサービスに課される義務に関する行動規範やガイダンスを整備 • リスク評価義務（9条）、安全措置義務（10条）、ユーザーからのコンテンツ報告・苦情受付義務（20条、21条）、テロコンテンツ等への対処通知義務（121条）、CSEAコンテンツのNCAへの報告義務（66条）等が該当	• （2023年11月）行動規範・ガイダンスに関するパブコメを公表 • （2024年12月）パブコメを受け、行動規範・ガイダンスを確定 • （2025年3月17日~）事業者は、リスク軽減措置を講じる義務を負う
フェーズ2: 子供にアクセスされる可能性が高いサービスに課される義務	• 子供にアクセスされる可能性が高いサービスに課される義務に関する行動規範やガイダンスを整備	• （2024年5月）行動規範・ガイダンスに関するパブコメを公表 • （2025年4~6月）行動規範・ガイダンスを確定予定
フェーズ3: 大規模サービスに課される義務	• 大規模サービス（特定カテゴリーサービス）に課される義務に関する行動規範やガイダンスを整備 • ユーザーエンパワーメントに関する義務（14条、15条）本人確認義務（64条、65条）が該当	• （2024年3月）行動規範・ガイダンス作成のためのエビデンス募集を開始 • （2025年1~3月）行動規範・ガイダンスのパブコメ予定 • （2025年10~12月）行動規範・ガイダンスを確定予定

出所）Statement: Protecting people from illegal harms online – Ofcom等よりNRI作成

OSAにおけるレコメンダシステムに関する対応

ユーザー間サービス提供事業者に対し、安全義務（10条4項）の１つとして、サービスの機能、安全設計に関する措置を組み込むことを義務付け※。「安全義務に関する行動規範」において、自社のレコメンダシステムをリリース前に実施するテストの際に、推奨される措置について規定。

※ OSAに基づきOfcomが行動規範(“Illegal content Codes of Practice for user-to-user services”)を策定（ 2024年12月）（41条）。PF事業者は、当該行動規範を参照しながら、安全義務を履行する。

■ 行動規範において、**レコメンダシステムに関するテストを実施する事業者に対して、以下の措置を推奨。**

	推奨される措置の内容
安全性指標の作成を推奨	PF事業者は、**レコメンダシステムの設計・調整に際して**、自社のプラットフォーム上で**テストを実施する場合**、**安全性指標（safety metrics）を作成・分析すべき**である。
安全性指標の内容	**安全性指標は**、現行のレコメンダシステムと比較して、当該設計変更により英国ユーザーが**違法コンテンツに接触するリスクが高まるか否かを判断できるもの**であり、**次の内容**（またはそれに相当する情報）**を含む**こと： a) **テスト期間中に寄せられた苦情に基づき、違法コンテンツ**またはその**疑いのあるコンテンツとして評価・識別されたコンテンツの総数** b) 上記a)の各コンテンツについて： i) 当該コンテンツが**ユーザーに表示された回数**（**インプレッション数**） ii) 当該コンテンツを表示されたユニークユーザー数（**リーチ数**）
テストの環境整備	PF事業者は**以下を確保すべき**である： a) 違法コンテンツまたはその疑いのあるコンテンツに関する**苦情を処理できる**よう、**テスト環境が適切に設定**されていること b) プラットフォーム上での**テスト期間**が、**苦情の受付可能な期間として十分である**こと c) **安全性指標の作成に必要な情報**が、**テスト期間中保持**されること
テストの記録保持	PF事業者は、プラットフォーム上で実施した**各テストの結果を記録したログを維持**すべきであり、**以下を含む**こと： a) 各レコメンダシステムの**バリエーションごとの安全性指標** b) 各レコメンダシステムの**バリエーションの設計特性に関する説明** c) テスト結果に基づいて、**どのバリエーションを採用するかについての設計上の決定**
テストの記録の活用	PF事業者は、このログが以下を満たすようにすべきである： a) コンテンツレコメンダシステムの開発およびテストに直接または間接的に関わる従業員が、容易にアクセスできること b) 将来のレコメンダシステムの設計調整時に、関係者（relevant individuals）がこのログを参照すること

（出典）https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/illegal-harms/illegal-content-codes-of-practice-for-user-to-user-services-24-feb.pdf?v=391889 を基にNRI作成

（参考・第３回資料再掲）安全義務に関する制度｜第10条「違法コンテンツに関する安全義務」

■ **ユーザー間サービスや検索サービスを提供する事業者に対して**「違法コンテンツに関する安全義務」を**義務付け** (10条) 。

措置内容	条文
サービスの設計または運営に関連する以下の措置を講じる義務	10条２項
・優先的違法コンテンツに個人が接触することを防止 ・優先的犯罪の実行または支援に使用されるリスクを、最新の違法コンテンツリスク評価に基づき効果的に軽減・管理 ・最新の違法コンテンツリスク評価で特定された個人への害のリスクを効果的に軽減・管理	(a)～(c)
サービスを次のように運営する義務	10条３項
・優先的違法コンテンツが存在する期間を最小限に抑えるために適切なシステムおよびプロセスを利用してサービスを運用 ・違法コンテンツの存在を通知された場合、または存在を認識した場合、そのコンテンツを迅速に削除するようサービスを運用	
上記の義務（10条2項・3項）について、以下の分野において措置を組み込む義務	10条４項
・リスクの管理 ・機能・アルゴリズム設計 ・利用規約 ・特定コンテンツのアクセス管理 ・コンテンツモデレーション ・ユーザーサポート ・スタッフの方針と実務	(a)～(h)
以下をサービスの利用規約に含め、適用する義務	10条5項、6項
・違法コンテンツから個人を保護する方法	(a)
プロアクティブ技術に関する情報（技術の種類、使用タイミング、機能の仕組みを含む）をサービスの利用規約に含める義務	10条７項
利用規約の規定が明確で、アクセスしやすいことを確保する義務	10条８項
リスク評価の結果をサービス利用規約に要約し、利用規約に記載する義務(大規模なユーザー間サービス事業者（カテゴリー１サービス)のみ義務）	10条９項

出所）Online Safety Act 2023よりNRI作成

（参考）OSAのレコメンダシステムに関する制度―背景

OSAの立法時の議論においては、レコメンダシステムには、ユーザーの体験向上やエンゲージメントの最大化等のメリットがある一方で、有害コンテンツの増幅やエコーチェンバーの発生等の懸念があり、安全義務の１つに盛り込まれることとなった。

	レコメンダシステムのメリット	レコメンダシステムへの懸念
オンライン危害に関する白書（Online Harms White Paper）での記載（2019年３月）	■ －（特に記載なし）	**エコーチェンバー・フィルターバブルの発生** ■ *ソーシャルメディア・プラットフォームは、「エコーチェンバー」や「フィルター・バブル」を引き起こす可能性のあるアルゴリズムを使用している。* ■ *これは、ユーザーが反論や反対意見を持つ他の情報源を見ないようにすることで、偽情報を助長する可能性があり、また、あるストーリーが実際よりもはるかに広く信じられているとユーザーが認識することを意味する。*
法案に関する英国下院での議論・修正（2022年３月）	***ユーザーの体験向上・エンゲージメントの最大化*** ■ *個々のユーザー向けにキュレーションされた環境を設計することで、ユーザーが興味を持ち、関わりたいと思うコンテンツを提供し、プラットフォームでの体験を向上させることができる。* ■ *この背後にある商業的な要請は、人々の注意を引き、エンゲージメントを最大化することである。*	**有害コンテンツの増幅** ■ *エンゲージメントを最大化するように設計されたアルゴリズムは、危害のリスクを生み出すコンテンツの増幅を直接もたらす可能性がある。例えば、5つのソーシャル・メディア・プラットフォームにおいて、反ユダヤ的と手動で特定された714の投稿が、6週間で730万インプレッションに達したことが明らかになっている。* ■ *2018年にYouTubeは、視聴されたすべての動画の70％以上が、レコメンドに応じて視聴されていると述べた。*

出所）Online Harms White Paper - GOV.UK、Draft Online Safety Bill - Joint Committee on the Draft Online Safety Bill等よりNRI作成

2023年11月に行われた行動規範・ガイダンスに対するパブリックコンサルテーションでは、レコメンダシステムに関して、下記の懸念点が寄せられた。

ステークホルダーからの、レコメンダシステムに関する意見

主体	意見の分類	意見の内容
事業者	リスク評価義務との関係	• 法令における「重大な変更」に関するリスク評価義務により、設計変更に伴うユーザーリスクの評価が既に求められており、それよりも緩やかな変更を対象とするような新たな評価義務をOfcomが推奨する正当な理由はない。また、全てのレコメンダシステムの変更が本措置の対象となる可能性がある（Google）
	安全性指標の収集頻度	• 多くのレコメンダシステムの調整が最終的に本番環境に導入されないことを踏まえ、安全性指標の評価は年1回、半年に1回、四半期ごとなど、定期的に行うべきである（LinkedIn）
	遵守に伴うコスト	• レコメンダシステムは段階的な変更が頻繁に行われることから、本措置によりプラットフォーム上テストの「遵守負担が増大する」（Google）
英国データ保護機関（ICO）	個人情報の取扱い	• 本措置の実施にあたり、安全性指標に個人データの処理が必要となる可能性がある（英国データ保護機関（ICO））
学術機関	有害性の証拠不足	• レコメンダシステムによって違法コンテンツが広範に拡散されていると示す十分な研究が存在しない（スウォンジー大学 サイバー脅威研究センター）

（出典）https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/illegal-harms/volume-2-service-design-and-user-choice.pdf?v=390978 を基にNRI作成

１－１－３． 豪州・NZにおけるレコメンダシステムに関する対応

豪州／ニュージーランドにおける行動規範｜

レコメンダシステムの透明化に関係するコミットメント（関係部分抜粋）

＜豪州（Australian Code of Practice on Misinformation and Disinformation ）＞

成果（Outcome）	内容
成果1e：利用者は、署名者によるレコメンダシステムの使用に関する一般情報にアクセスでき、レコメンダコンテンツに関する選択肢を持つことができる。	5.14. 検索エンジンを除き、主として一般向けに情報を配信することを目的とし、レコメンダシステムを使用しているサービスを提供する署名者は、以下のことを約束する： A. 利用者がそのサービスでアクセス可能な情報の優先順位をどのように決定しているかについて、利用者が知ることができる情報を提供すること B. レコメンダシステムが提示するコンテンツに関して、サービスの性質に応じた利用者の選択肢を提供すること 注記：例えば、オンライン新聞社がニュース記事の下に提供するコメント欄は、主たるサービスである編集責任のあるニュースの発信に付随する機能であり、この義務の対象とはならない。

＜ニュージーランド（Aotearoa New Zealand Code of Practice for Online Safety and Harms）＞

成果（Outcome）	対策
成果9. ユーザーが、自分が目にするコンテンツやオンライン上での体験・交流について、自らコントロールできるようにする	対策37. ユーザーが、自分の閲覧するコンテンツ、フィードの性質、またはオンラインコミュニティに対して適切なコントロールを行えるようにするための方針、手続き、製品、またはプログラムを導入・実施・維持する。
	対策38. ユーザが見る広告の適切さを制御できる機能を備えた製品を導入し、それを継続的に提供する。

１－２．収益化停止に関する対応

DSAの収益化停止に関する制度

DSAにおいては、PF事業者に対して、ユーザーに対する収益化停止措置を義務付ける制度はない。他方、違法コンテンツまたは利用規約に反するコンテンツについて、PF事業者がユーザーに対するコンテンツモデレーションの一つとして、収益化停止措置を行った場合には、当該措置に関する異議申立ての方法について、当該ユーザーに通知することを義務付け

収益化停止措置に言及のある前文	（54項） **ホスティングサービス提供者が、ユーザーが提供した情報が違法コンテンツである、または利用規約に反すると判断し**、情報を削除・非表示にしたり、視認性や**収益化を制限する措置を取る場合**（例えば通知を受けた場合や自発的に、完全に自動化された手段を用いる場合も含む）、その**提供者は**、当該サービスの**受領者に対し**、その**判断の内容・理由・異議申立てが可能な手続について、明確かつ理解しやすい方法で通知しなければならない。** **この義務は**、情報が**違法と判断された場合に限らず**、**利用規約に適合しないと判断された場合にも適用**される。 また、通知を受けたことによって当該判断が下された場合には、通知者の身元は、その情報が違法であることの特定に必要な場合（例：知的財産権侵害）に限り、サービスの受領者に開示されるべきである。 （55項） **視認性の制限とは**、検索順位やレコメンダシステムでの格下げ、受領者に対するアクセス制限、あるいは受領者が気付かない形でのコミュニティからの排除（いわゆる「シャドウバン」）などを指す。**広告収益を通じた収益化の制限には、支払いの停止または終了も含まれる。** ただし、ボットや偽アカウントなどを用いたサービスの意図的な操作により配信される大量の不正な商業コンテンツに関しては、理由の説明義務は適用されない。 ホスティングサービス提供者の決定に対して異議を申し立てる他の手段とは別に、サービスの受領者には常に、各国の法律に従って裁判所での実効的な救済手段が保障されなければならない。
内部異議申立て制度 (DSA20条1項)	**オンラインプラットフォーム提供者は**、**サービスの受領者**（通知を提出した個人や法人を含む）**に対し**、**次に定める決定の通知日から少なくとも6か月間、効果的な内部異議申立て制度へのアクセスを電子的かつ無償で提供しなければならない。これにより、受領者は**、通知に基づく決定、または受領者の提供した情報が違法コンテンツである、または利用規約に反するとの理由に基づく**以下のような決定に対して**、**異議申立てを行うことができる**： • (a) 当該情報を削除・非表示にする、または視認性を制限するか否かに関する決定 • (b) サービスの提供を全部または一部停止・終了するか否かに関する決定 • (c) 受領者のアカウントを停止・終了するか否かに関する決定 • (d) **受領者が提供する情報の収益化を停止・終了・その他制限するか否かに関する決定**

（参考）事業者による取組状況｜収益化停止の対象となる基準：YouTube (Google)

「広告掲載に適したコンテンツのガイドライン」の「広告収入が制限/まったく得られない」コンテンツに関する記載（一部抜粋）

内容

広告に適さないコンテンツが見つかった場合、収益化の状態が「広告の制限/広告が全く表示されなくなる」可能性がある。
好ましくない主なトピックは次のとおり。

不適切な言語
- 最初の 7 秒間にかなり汚い言葉 (f*ck など) が使用されているか、タイトルまたはサムネイルに中程度の汚い言葉 (「sh*t」など) が使用されている。

暴力
- 教育またはドキュメンタリーのチャネル設定で、明らかな負傷/死体、サムネイルまたはコンテンツの冒頭でのゲームの残酷な暴力、武力紛争の映像、悲劇の生々しい詳細の説明を含むコンテンツ。外国のテロ組織に関するコメディー的な言及または一瞬の映像。

アダルトコンテンツ
- 性交の描写、またはサムネイルで性器に焦点が当てられているもの、性行為のアニメーションを含む刺激を伴わない性教育、性的テーマを伴ういたずら、最小限の衣服に焦点を合わせたダンス、ダンスで性的な身体部位を意図的に触ったり、性的な身体部位に長時間焦点を当てたりするコンテンツ。

衝撃的な内容
- 人間や動物の体の部分のグラフィック画像など、隠蔽されておらず、衝撃を与えることを意図していないが、全体的な背景を提供する衝撃的なコンテンツ。

有害行為や信頼できないコンテンツ。非専門的、非管理環境で行われた行為を含む、身体的危害や苦痛を示すが、それに焦点を当てていないコンテンツ。

憎悪や中傷的な内容
- 個人またはグループにとって不快な可能性があるが、教育、ニュース、ドキュメンタリーに使用されるコンテンツ。

娯楽用薬物および薬物関連コンテンツ
- 違法薬物の使用（注射を含む）または製造に焦点を当てた非教育的かつ非情報的なコンテンツ。違法薬物の使用を促進または美化する意図はありません。麻薬取引組織の暴力的な状況（人質など）や公共広告を描写した教育コンテンツ。

銃器関連コンテンツ
- 管理された環境以外での銃の使用、防護具なしで他人に対してエアガンやボール弾（BB）ガンを使用する。

デリケートなイベント
- 無神経/搾取的なコンテンツを削減するためのGoogleの能力に重大なリスクをもたらす事象または展開を指す。（2022年3月23日: ウクライナ戦争のため、戦争を悪用、否定、容認するコンテンツは、追って通知があるまで収益化の対象外となっている。）

不正行為を助長する
- 不正アクセスを行う方法を視聴者に教えることを目的としたコンテンツ。資産の行動規範に反する行為を表示する。学術論文執筆サービスや、競争力のあるeスポーツで勝つためのハッキング方法など、誤解を招いたり不正行為を助長したりする製品やサービスを紹介する。

子供や家族に不適切なコンテンツ
- 不正行為やいじめなどの悪質な行為を助長して子供に影響を及ぼすコンテンツ、または子供に重大な身体的または精神的危害を与える可能性のあるコンテンツ。

タバコ関連コンテンツ
- タバコやタバコ関連製品を宣伝するコンテンツ。

扇動的で屈辱的な
- 不当に煽動的、扇動的、または品位を傷つけるコンテンツ。

出所）以下の公開情報より一部を抜粋して記載。より詳細な例示は出所を参照。
https://support.google.com/youtube/answer/6162278

（参考）事業者による取組状況｜収益化停止の対象： X

■ 「クリエイター収益化基準」にて「行動基準」、「コンテンツ基準」を設けている。この基準に違反した場合、重大性と違反履歴に基づき、①収益化機能の一次停止または永久停止、②Xから収益を得る他の製品の一次または永久停止、③Xへのアクセス制限/停止、④アカウントの拡散制限、等の措置が取られる。

クリエイター収益化基準の収益化制限/停止に関する記載（一部抜粋）

内容

【行動基準】

勧誘

- 違法、不法、またはあなた自身、他の人、または動物に害を及ぼす行為やコンテンツと引き換えに、金銭や約束を要求したり提供してはならない。
- 物理的な商品やサービスと引き換えに、通貨や約束を要求したり提供してはならない。
- 性的サービスと引き換えに金銭や約束を要求してはならない。
- コンテスト、懸賞、その他のプロモーションの必須エントリー方法として、支払いやコンテンツの収益化を可能にする X 機能を使用しない。

詐欺および欺瞞

- アカウントに関連してどの人物またはどの団体が報酬を受け取るかについて欺瞞するなど、人々を騙してあなたと関わらせたり、あなたに報酬を支払わせたりしてはならない。

プラットフォームの操作とスパム

- プラットフォームの操作とスパムに関するポリシーで禁止されている種類の行為には関与しない。これには、エンゲージメントを人為的に高めようとしたり、X 製品の機能を悪用して他の人の体験を妨害しようとしたりすることが含まれる。

現地の法律

- X で収益を得る際は、適用される現地の法律および規制を遵守する責任がある。

【コンテンツ基準】

（禁止されているコンテンツ：収益化の対象外）

欺瞞行為および違法行為

- 違法なコンテンツ、製品、サービスを紹介するコンテンツ。（例：娯楽用薬物または薬物関連器具、処方薬と医薬品、ギャンブル・賭け・宝くじ・抽選の商品およびサービス 、武器・弾薬・爆発物の販売、等）

（制限されたコンテンツ：収益化が制限される可能性）

成人向けまたは性的な内容

- 過度に挑発的または性的に挑発的な活動、ポルノ、ヌード、または暗示的な性行為を特徴とするコンテンツ。（例：性行為・性器・性玩具・性的な体液の描写、エスコートや売春サービスに関連するコンテンツ、性行為に特化した「出会い系」サイト、等）

露骨で不快、暴力的な内容

- 現実または架空の犯罪、過度に暴力的、または衝撃的な内容を扱ったコンテンツ。（例：死、拷問、重症・過度な流血、犯罪行為、等）

憎悪や過激なコンテンツ

- 人種、民族、性別、性的指向、性自認、年齢、能力、国籍、宗教、カースト、暴力行為の被害者や生存者、その親族、移民ステータス、重病患者などに基づいて、個人またはグループに対して憎悪的な行為を描写または表現したり、嫌がらせ、辱め、または侮辱したりするコンテンツ。

センシティブなコンテンツ

- 悲劇、紛争、集団暴力、または物議を醸す政治問題や社会問題の悪用に関連するコンテンツ。（例：自然災害または産業災害 、戦争と武力紛争、議論の余地のある社会問題、等）

強い言葉遣い

- 口頭、書面、検閲、またはその他の表現形式で、露骨、軽蔑的、または下品な言葉が使用されているコンテンツ。（例：冒涜 、下品な表現、攻撃的な発言、下品なジェスチャー、等）

出所）以下の公開情報より一部を抜粋して記載。より詳細な例示は出所を参照。
https://help.x.com/en/rules-and-policies/content-monetization-standards

（参考）欧州・豪州・NZにおける行動規範

欧州・豪州・NZにおいては、行動規範レベルで、偽情報の流通・拡散の防止を目的として、ユーザーの収益化や広告掲載に係る事前審査の強化に向けた取組が推奨されている。

欧州・偽情報に関する行動規範（関係部分抜粋）	豪州・Australian Code of Practice on Misinformation and Disinformation（関係部分抜粋）	NZ・Aotearoa New Zealand Code of Practice for Online Safety and Harms（関係部分抜粋）
コミットメント１：偽情報の拡散に対する資金提供の阻止 広告掲載に関与する署名者は、偽情報の拡散への偽資金供給を断ち、コンテンツが収益化の対象となるかどうかを判断するための方針及びシステム、広告の収益化および掲載に関する統制手段、広告掲載の統制やサービスの正確性・有効性に関する報告データの改善することを制約する。 そのため、広告の販売に関与する該当する署名者（メディアプラットフォーム、出版社、アドテク企業を含む）は、偽情報コンテンツの隣接または繰り返し違反する情報源への広告掲載を防ぐための、実効的な執行及び是正措置を講じることや広告のリンク先・遷移先ページや掲載元の検証を可能にする措置を導入することなどの方針を導入する。 また、収益化対象コンテンツや広告収益分配プログラムにおける適格性要件および内容審査プロセスを必要に応じて強化し、偽情報対策方針に継続的に違反する行為者を排除できるようにする。 広告の購入に関与する該当する署名者（広告主および広告代理店を含む）は、偽情報コンテンツの隣や、繰り返し偽情報を掲載する場所への広告掲載を効果的かつ透明性のある方法で回避している広告販売者を通じて広告を出稿する。	5.16 署名事業者は、偽情報や誤情報に対する広告および／または収益化インセンティブを妨げることを目的とした方針やプロセスを導入する。 5.17 上記5.16に基づく方針やプロセスには、例えば以下のようなものが含まれ得る： A. ブランドセーフティや検証ツールの活用を推進または組み込むこと B. 第三者検証会社との連携を可能にすること C. 広告主がメディア購入戦略やオンライン上の評判リスクを評価できるよう支援または許可すること D. 広告主が広告の掲載状況を監視し、掲載先を選択できるように、クライアント専用アカウントへの必要なアクセスを提供すること E. 偽情報や誤情報を拡散するアカウントやウェブサイトへの広告サービスおよび有料掲載の提供を制限すること	対策32. 偽情報の流通・拡散により利益を得ている利用者に対して、広告の配信を妨げたり、経済的な動機を弱めたりすることを目的とした方針・手続き・製品などを導入し、それを実施・維持すること。

1－3．ユーザーエンパワーメントに関する対応

1－3－1．EUにおけるDSA （Digital Services Act）の ユーザーエンパワーメントに関する対応

DSAでは、ユーザーエンパワーメントに関連して、PF事業者に対して、サービスを利用するユーザーの判断や、表示されるコンテンツ・広告の自律的な管理を支援する機能の提供を義務付けている

	義務の内容
利用規約において、ユーザーに対する措置や異議申立手続について明確・平易に公開する義務（14条）	• 仲介サービス提供事業者に対して、ユーザーに提供する情報に課すあらゆる制限（**コンテンツモデレーションに関する方法、手順・措置等）に関する情報や、内部の異議申立て処理システムの運営ルールを、明確、平易でわかりやすく利用規約に記載**しなければならない（14条1項）。 • VLOP/VLOSEはユーザーに対し、**利用可能な救済措置及び救済メカニズムを含む、簡潔でアクセスしやすく機械で読み取り可能なサマリーを提供**しなければならない（14条5項）。 • VLOP/VLOSEはサービスを提供するすべての加盟国の公用語で利用規約を公表しなければならない（14条6項）。
レコメンダシステムの透明性確保義務（27条）	• レコメンダシステムを使用するPF事業者は、**使用される主なパラメータやパラメータを修正・変更できる選択肢を平易で分かりやすい言葉で利用規約に明記**し（27条1項）、特定の情報をレコメンドする理由を説明しなければならない（27条2項）。 • 複数のレコメンド方法を選べる場合、**ユーザーが希望するレコメンド方法をいつでも選択・変更できる機能を提供**しなければならず、当該機能は、情報が優先表示されているオンラインインターフェース内の該当箇所から直接かつ容易にアクセスできなければならない（27条3項）。
表示される広告の透明性確保義務（26条）	• オンラインインターフェースに広告を掲載するPF事業者は、各ユーザーに**表示される個々の広告について、その情報が広告であること、広告が代表している自然人または法人、広告の支払者、広告表示を決定するための主なパラメータとその変更方法について、ユーザーが明確、簡潔でリアルタイムに識別できるようにしなければならない**（26条1項）。 • PF事業者は、提供するコンテンツが商業的コミュニケーションであるかをユーザーが申告する機能を提供しなければならず、申告について他のユーザーが明確な方法でリアルタイムに識別できるようにしなければならない（26条2項）。
AI生成物等へのラベリング機能の提供（35条1項(k)）	• VLOP/VLOSEに対して「軽減措置」を義務付けており、34条に従って特定されたシステミックリスクに合わせた、合理的、比例的かつ効果的な緩和措置を、基本的権利に与える影響に配慮して講じなければならない（35条）。 • 当該軽減措置の例示として、**AI生成物等へのラベリング機能**（人物や事象に著しく類似し、誤認させるような画像、音声、動画がオンラインインターフェースに表示される際に目立つマークによって区別できる機能）**の提供**が挙げられている。

（参考）偽情報に関する行動規範

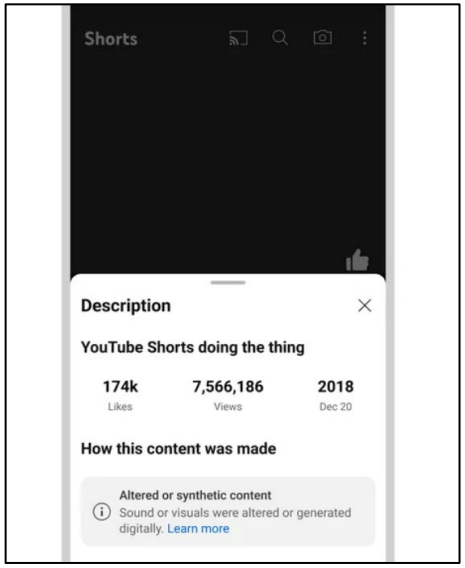
偽情報に関する行動規範では、ユーザーに対して偽情報の識別支援やメディアリテラシーの向上、レコメンダシステムの透明性等について規定。

	推奨される措置の内容
利用者への情報提供・判断支援	(1) 偽情報の識別支援 • ファクトチェック機関と連携し、偽情報と判断された投稿にラベルや注意表示を行う。 • コンテンツがファクトチェック対象である旨をユーザーに通知する仕組みを整備。 • コンテンツを共有したユーザーにも通知を送る。 • 通知・表示回数、再共有数の減少などを測定し、効果を評価。 (2) 信頼性の可視化 •「信頼性指標（例：トラストマーク）」の導入。 • 信頼性評価の基準は公開され、政治的中立・公正性・独立性を確保。 • 出版社には「意見表明の機会（聴聞権）」が与えられ、異議申立てが可能。 • 評価の誤りは訂正され、評価結果の更新や出版社の改善も反映される。
メディアリテラシーの向上	• コンテンツに文脈を付加するツールや評価ガイドを提供し、利用者のリテラシーと批判的思考力を育成。• 偽情報や悪意ある戦術（TTPs）に対するEU全域での啓発キャンペーンを実施。 • 各種ツール・活動は専門家（欧州委員会・EDMO（European Digital Media Observatory）・大学等）と連携して設計・評価。
レコメンドシステムの安全化と透明性	• 偽情報の表示機会を減らし、信頼できる情報の可視性を高める設計とする。 • レコメンドが使用している主要なパラメータ・判断基準を公開し、透明性センターや利用規約において情報提供。 • 利用者はレコメンドシステムの設定を自分で選択・変更可能とし、その選択肢も提示。
メッセージアプリにおける対策	• 利用者が信頼できる情報源にアクセスし、偽情報の拡散を抑止する機能を導入（例：正確な情報提供キャンペーン、転送制限機能、外部コンテンツにラベル表示）
通報機能と異議申立て制度	• 濫用（例：大量通報）にも配慮しつつ、利用者が偽情報と思われるコンテンツを通報するためのユーザーフレンドリーな機能を提供。 • 違反として処理された場合は理由を説明し、それに対する利用者からの異議申立ての機会を提供。
研究・評価の実施と透明性の確保	• 施策の効果を測定し、透明性センター等で報告・公開。 • 独立監査や第三者評価、苦情処理の仕組みも整備。 • EU加盟国ごとにデータを収集・報告し、地域差の分析にも活用。

（出典）The Code of Conduct on Disinformation | Shaping Europe's digital future を基にNRI作成

各事業者は生成AIの対応として、投稿者にAIツールを用いて作成したコンテンツであることを申告させるシステムと、自動的にラベル付けするシステムを展開している

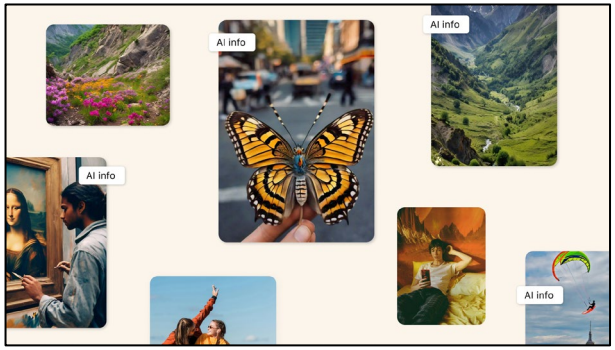
YouTubeの取組



AI ツールの使用を含め、リアルな改変または合成コンテンツを作成した場合に、クリエイターに開示を求めます。クリエイターがコンテンツをアップロードするときに、リアルな改変または合成素材が含まれていることを示すための新しいオプションが提供

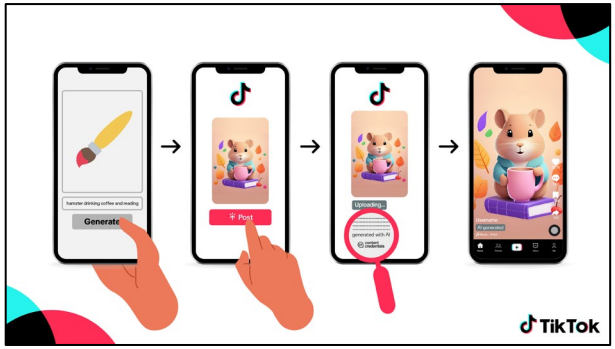
YouTube: https://blog.youtube/inside-youtube/our-approach-to-responsible-ai-innovation/
Instagram:https://about.fb.com/news/2024/04/metas-approach-to-labeling-ai-generated-content-and-manipulated-media/
TikTok: https://newsroom.tiktok.com/en-us/partnering-with-our-industry-to-advance-ai-transparency-and-literacy

Instagramの取組



業界標準の AI 画像インジケーターが検出された場合、またはユーザーが AI 生成コンテンツをアップロードしていることを明らかにした場合、より広範な動画、音声、画像コンテンツに「AI 情報」ラベルの追加

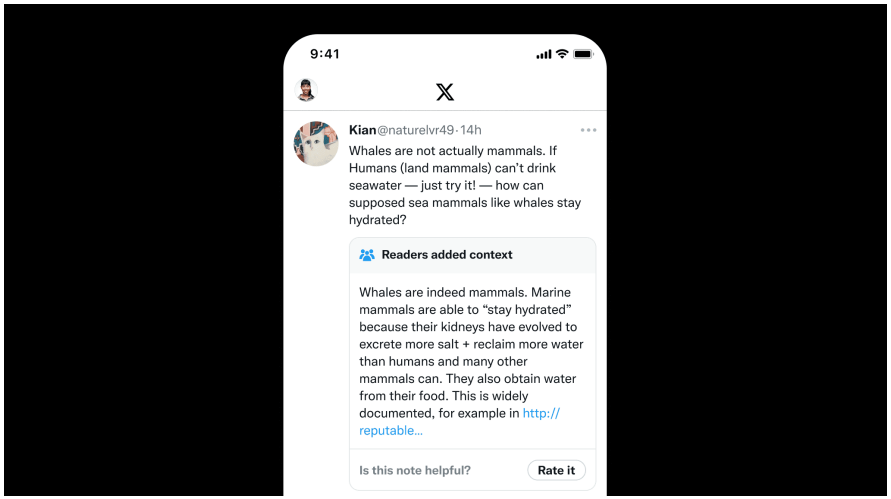
TikTokの取組



TikTokは、特定の他のプラットフォームからアップロードされたAI生成コンテンツに自動的にラベル付けを開始

情報の信ぴょう性を確認・確保するために、Xではコミュニティノートを用いたユーザによる監視、TikTokではファクトチェック団体による監視が行われている

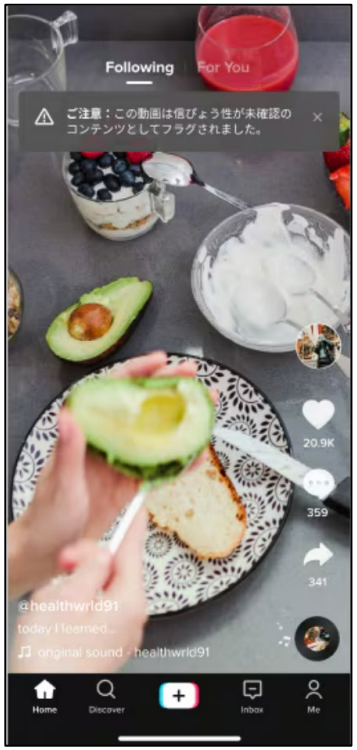
Xの取組



コミュニティノートは、Xのユーザーが協力して、誤解を招く可能性のある投稿に役立つメモを追加できるようにすることで、より情報に富んだ世界を実現することを目指す。特徴として、以下がある。

- ✓ 寄稿者はメモを書いて評価する
- ✓ さまざまな視点から役立つと評価されたメモのみが投稿に表示される
- ✓ Xが何を表示するかは選べない、人々が選ぶ
- ✓ オープンソースで透明性向上

TikTokの取組



ファクトチェックを行う世界18団体と提携し、50以上の言語に対応したコンテンツ審査を行っている。
偽情報が含まれている可能性があるとして信ぴょう性の低いコンテンツと判断された動画には、「信ぴょう性が未確認である」ことを表示するラベルが付く。

X: https://communitynotes.x.com/guide/en/about/introduction
TikTok: https://www.sankei.com/article/20240516-NVWOFI2PZZB7RF2UHMAEFQ2KSA/photo/DAFUO5OQLVDNBEYD4J23V7YJX4/

１－３－２．英国におけるOSA （Online Safety Act）の ユーザーエンパワーメントに関する対応

OSAでは、ユーザーのエンパワーメント評価（14条）、エンパワーメント義務（15条）が規定されている

■ オンライン安全法では、大規模かつコンテンツレコメンダシステムを有するユーザー間サービスをカテゴリー1サービスとし、追加で義務を課している。

オンライン安全法 Part3 2章「ユーザー間サービスの注意義務」

セクション名	条項	タイトル	カテゴリー２サービス	カテゴリー1サービス
ユーザー間サービス：義務の範囲	7	ユーザー間サービスの提供者：注意義務	●	●
	8	注意義務の範囲	●	●
ユーザー間サービスの違法コンテンツ義務	9	違法コンテンツのリスク評価義務	●	●
	10	違法コンテンツに関する安全義務	●	●
子供にアクセスされる可能性の高いサービス	11	子供のリスク評価義務	●	●
	12	子供を保護するための安全義務	●	●
	13	子供を保護するための安全義務：解釈	●	●
カテゴリー1サービス	**14**	**アセスメント義務：ユーザーのエンパワーメント**		●
	15	**ユーザーのエンパワーメント義務**		●
	16	**ユーザーのエンパワーメント義務：解釈**		●
	17	民主的に重要性のあるコンテンツを保護する義務		●
	18	ニュースパブリッシャーのコンテンツを保護する義務		●
	19	ジャーナリスティックコンテンツを保護する義務		●
コンテンツに関する報告および苦情処理手続きに関する義務	20	コンテンツ報告に関する義務	●	●
	21	苦情処理手続きに関する義務	●	●
横断的義務	22	表現の自由とプライバシーに関する義務	●	●
	23	記録保持とレビュー	●	●

出所）https://www.legislation.gov.uk/ukpga/2023/50/contents/enacted

（参考）OSAにおける施行スケジュール

OSAにおける各種義務は、義務の対象となるサービスの種類に応じて、3段階に分けて施行する予定となっており、Ofcomには、情報の種類等に応じて（フェーズ1~3）、行動規範およびガイダンスの発行が義務付けられている

■ OSAの監督・執行は、Ofcomが担う。

- OSAの施行に際しては、**Ofcomに対して、オンラインサービス事業者に課される義務に対する行動規範（Code of Practice）の公表が義務付けられている（41条）**
- また、PF事業者が同法が定める義務の遵守を支援するための**ガイダンスを発行することも義務付けている（52条、53条、54条等）**

Ofcomによる、行動規範やガイダンスの整備

	フェーズの概要	ステータス　灰字：今後の予定
フェーズ1: 全てのサービスに課される義務	• 全てのサービスに課される義務に関する行動規範やガイダンスを整備 • リスク評価義務（9条）、安全措置義務（10条）、ユーザーからのコンテンツ報告・苦情受付義務（20条、21条）、テロコンテンツ等への対処通知義務（121条）、CSEAコンテンツのNCAへの報告義務（66条）等が該当	• （2023年11月）行動規範・ガイダンスに関するパブコメを公表 • （2024年12月）パブコメを受け、行動規範・ガイダンスを確定 • （2025年3月17日~）事業者は、リスク軽減措置を講じる義務を負う
フェーズ2: 子供にアクセスされる可能性が高いサービスに課される義務	• 子供にアクセスされる可能性が高いサービスに課される義務に関する行動規範やガイダンスを整備	• （2024年5月）行動規範・ガイダンスに関するパブコメを公表 • （2025年4~6月）行動規範・ガイダンスを確定予定
フェーズ3: 大規模サービスに課される義務	• 大規模サービス（特定カテゴリーサービス）に課される義務に関する行動規範やガイダンスを整備 • ユーザーエンパワーメントに関する義務（14条、15条）本人確認義務（64条、65条）が該当	• （2024年3月）行動規範・ガイダンス作成のためのエビデンス募集を開始 • （2025年1~3月）行動規範・ガイダンスのパブコメ予定 • （2025年10~12月）行動規範・ガイダンスを確定予定

出所）Statement: Protecting people from illegal harms online – Ofcom等よりNRI作成

大規模かつレコメンダシステムを有する事業者に対して、成人ユーザーに関する評価（ユーザー層の実態や特定のコンテンツへの接触可能性等）を義務付け（14条）。
成人ユーザーに対して、ユーザーエンパワーメントに関する機能（特定のコンテンツへの接触頻度を減らす機能や未認証ユーザーをフィルターする機能等）をサービスに含めることを義務付け（15条）。

対象事業者	● カテゴリー１サービスを提供する事業者 ※ カテゴリー1サービスとは、以下のいずれかの条件を満たすサービス。 ①コンテンツレコメンダシステムを有し、英国人口の約50%に相当する3,400万人以上の英国ユーザーを有する ②ユーザー生成コンテンツの転送又は再共有をユーザーに許可し、コンテンツレコメンダシステムを有し、英国人口の10%を占める700万人以上の英国ユーザーを有する
成人ユーザーに対するユーザーエンパワーメントに関する評価義務(OSA14条)	● 成人ユーザーが表示されるコンテンツを自らコントロールできるという目的を達するために、以下の事項を評価することを義務付け。 • 自社サービスのユーザー層の実態 • 特定のコンテンツ（※）の流通状況 • 特定の特性（特定の人種、宗教、性別、性的指向等）を持つユーザーへの影響の有無 • サービスの機能、設計、運用が特定のコンテンツの流通・拡散に与える影響 （※）「自殺または故意の自傷行為を奨励するもの」、「摂食障害を奨励するもの」、「特定の人種、宗教、性別、性的指向、障がい者、性転換者などを虐待の対象とするもの/などへの憎悪を煽るもの」等
成人ユーザーに対するユーザーエンパワーメント義務(OSA15条)	① 成人ユーザーが表示されるコンテンツを自らコントロールするために利用可能な機能を、合理的に適切な範囲内でサービスに含める義務。 ② 上記の機能とは、以下に関するシステムまたはプロセスを使用すること a. ユーザーが、サービス上に存在する特定のコンテンツに遭遇する可能性を低減する b. サービス上に存在する特定のコンテンツについて、ユーザーに警告する ③ ①に関するすべての機能が、すべての成人ユーザーに提供され、かつ、容易にアクセスできることを確保する義務。 ④ ①に関する機能とユーザーがそれらの利用方法を明記した明確な規定を利用規約の中に含める義務。 ⑤ 成人ユーザーが未認証ユーザーを排除することを希望する場合、それを実現できる機能をサービスに含める義務。ここでいう機能とは、ユーザーが希望する場合に、以下に関するシステムまたはプロセスを使用すること ● 未認証ユーザーが本サービス上で生成、アップロード、共有するコンテンツへ接触することを防止する ● 未認証ユーザーが、本サービス上で生成、アップロード、共有するコンテンツにそのユーザが遭遇する可能性を低減する

2．情報発信・流通の態様に着目した対応

PF事業者に対して、違法コンテンツを繰り返し発信したり、明らかに根拠のない通知や異議申し立てを行ったりするユーザーについて、事前の警告の上、サービスの提供を停止することを義務付け（23条１項・２項）。PF事業者は、これらの不正利用に関する方針を利用規約において明記する必要がある（23条4項）

不正利用の対象

＜違法コンテンツを繰り返し発信する行為に対する対応＞

■ PF事業者は、**明らかに違法なコンテンツを繰り返し発信するユーザーに対して、事前の警告を行った上**で、合理的な期間、**サービスの提供を停止しなければならない**。（23条1項）

＜明らかに根拠のない通知や異議申立てに対する対応＞

■ PF事業者は、**明らかに根拠のない通知や異議申立てを頻繁に提出する個人または団体、または異議申立人**による、16条および20条に規定する通知および措置メカニズムおよび内部苦情処理システムを通じて提出された通知・異議申立ての処理を、**事前の警告を発した上**で**合理的な期間停止しなければならない**。（23条2項）

不正利用の判断材料

■ 停止を決定する場合、PF事業者は、関連する入手可能な明確な情報すべての事実および状況を考慮して、対象の個人、団体または申立人が1項・2項に言及される不正利用に関与しているかどうかを、ケースバイケースで、適時に、忠実かつ客観的な方法で評価しなければならない。考慮する情報には、少なくとも以下が含まれるものとする：

a. **所定の期間内に提出された、明らかに違法なコンテンツ、または明らかに根拠のない通知や苦情の絶対数**
b. **所定の期間内に提供された通知や苦情の総数に対するその相対的割合**
c. **違法コンテンツの性質を含む悪用の重大性とその結果**
d. **特定が可能な場合、対象個人、団体、または申立人の意図**

（23条3項）

■ PF事業者は、**1項・2項で言及された不正利用に関する方針を、明確かつ詳細な方法で利用規約の中に明記**し、特定の行為に該当するかどうかを評価する際に考慮する事実および状況の例ならびに利用停止の期間を示さなければならない。（23条4項）

出所）DSA23条　https://www.eu-digital-services-act.com/Digital_Services_Act_Article_23.html

（参考）事業者による取組状況｜欧州における不正利用への対応に関連する記載内容：YouTube (Google)

：NRIが関連性を確認した条文

利用規約の記載　DSA第23条1項・2項・4項に関係する内容

内容

【サービスの利用】
- （前略）自動化された手段（ロボット、ボットネット、スクレーパーなど）を使用してサービスにアクセスしないこと。
- 根拠のない、迷惑な、または軽率な提出を含む、報告、フラグ付け、苦情、紛争、または異議申し立てのプロセスを悪用しないこと。
- YouTubeポリシーおよびガイドラインに準拠しないコンテストを本サービス上でまたは本サービスを通じて実施しないこと。

【コミュニティガイドライン違反警告】
- YouTube では、コミュニティガイドラインに違反するコンテンツに対して「違反警告」のシステムを運用している。違反警告ごとに制限が異なり、YouTube からチャンネルが永久に削除される可能性がある。違反警告がチャンネルに及ぼす影響の詳細については、「コミュニティガイドライン違反警告の基本」を参照。違反警告が誤って発行されたと思われる場合は、異議を申し立てることができる。

「スパム、欺瞞行為、詐欺に関するポリシー」の記載（一部抜粋）　DSA第23条1項に関係する内容

内容

下記の説明のいずれかに該当するコンテンツは、YouTube に投稿しないこと。
- 動画スパム: 何度も投稿される、**繰り返されている、あるいは不特定多数に向けたコンテンツ**
- 繰り返しのコメント: 同じ内容のコメント、不特定多数に向けたコメント、**コメントの繰り返しを大量に投稿**する。

「コミュニティガイドライン違反警告の基本」の記載（一部抜粋）　DSA第23条4項に関係する内容

内容

コンテンツがコミュニティ ガイドラインに違反している場合、チャンネルに警告が出されることがある。

①警告
間違いは起こるものであり、ポリシーに違反することは意図的ではないことは理解しているため、最初の違反は通常「警告」のみになる。この警告を90日後に期限切れにするには、ポリシートレーニングを受講する必要がある。

②ファーストストライク
コンテンツがポリシーへの不遵守が2回目に判明した場合、ストライクが発行される。このストライクにより、1 週間、次の行為が禁止される。
（動画やライブストリームをアップロードする、スケジュールされたライブストリームを開始する、プレミア公開を作成する、等）

③セカンドストライク
①の警告と同じ90日の期間内に2回目のストライクを受けた場合、2 週間コンテンツを投稿できなくなる。

④サードストライク
同じ90日間に3回の警告を受けると、チャンネルが YouTube から永久に削除される可能性がある。各警告は、発行されてから 90 日間は効力を持つ。

※NRIが以下の公開情報より確認できたものを整理
利用規約： https://www.youtube.com/static?gl=FR&template=terms
スパム、欺瞞行為、詐欺に関するポリシー：https://support.google.com/youtube/answer/2801973?hl=en&ref_topic=9282365
コミュニティガイドライン違反警告の基本：https://support.google.com/youtube/answer/2802032

（参考）事業者による取組状況｜欧州における不正利用への対応に関連する記載内容：Instagram (Meta)

：NRIが関連性を確認した条文

利用規約の記載（一部抜粋）	DSA第23条1項・2項・4項に関係する内容
内容	【お客様の義務】 • 本規約または当社のポリシー（特にコミュニティガイドライン、メタプラットフォーム規約、開発者ポリシー、音楽ガイドラインを含む）に違反する（または他者に違反を幇助または奨励する）ことはできない。 • サービスの運営を意図して妨害したり、損なったりする行為は禁止されている。これには、詐欺的または根拠のない報告や異議申し立てを行うなど、報告、紛争、異議申し立てのチャネルを悪用することも含まれる。 【コンテンツの削除およびアカウントの無効化または終了】 • 当社は、コミュニティまたはサービスを保護するため、またはお客様が当社にリスクや法的リスクをもたらす場合、本利用規約または当社のポリシー（当社のコミュニティ基準を含む）に違反した場合、お客様が繰り返し他者の知的財産権を侵害した場合、または法律により許可または義務付けられている場合、お客様へのサービスの全部または一部の提供を直ちに拒否または停止することができます（Meta製品およびMeta Company製品へのアクセスを終了または無効にすることを含む）。 • アカウントが誤って終了されたと思われる場合、またはアカウントを無効化または永久に削除したい場合は、ヘルプセンターにご相談できる。

「スパム」に関するコミュニティガイドラインの記載（一部抜粋）	DSA第23条1項に関係する内容
内容	以下は禁止されている。（一部抜粋） • スパム：視聴を人為的に増やすために利用者をだましたり、欺いたり、混乱させたりすることを意図したコンテンツの禁止 • （例）スパムであるサイン（**同じコンテンツを繰り返し投稿するなど**）または信頼性が疑われるシグナルがある、低い頻度で利用されているアカウントを制限する可能性

※NRIが以下の公開情報より確認できたものを整理
利用規約： https://help.instagram.com/termsofuse?vanity=termsofuse
スパムに関するコミュニティガイドライン：https://transparency.meta.com/fr-fr/policies/community-standards/spam/

（参考）事業者による取組状況｜欧州における不正利用への対応に関連する記載内容：TikTok

：NRIが関連性を確認した条文

利用規約の記載　DSA第23条1項・2項・4項に関係する内容

内容

【プラットフォームの使用】
- 私たちのコミュニティガイドラインプラットフォーム上のすべてのユーザーとすべてのコンテンツに適用されます。プラットフォームを使用する場合、コミュニティ ガイドラインに違反するコンテンツを作成、投稿、共有、リンク、またはその他の方法でやり取りすることはできません。
  - スパムやなりすましアカウントの運用、または当社のコミュニティガイドラインに詳述されているその他の手段による不正な商業行為に従事すること。
  - 明らかに根拠のない異議申し立て、報告、通知または苦情を提出する。

【関係性の制限/停止】
- あなたのアカウントが利用規約に違反した回数を記録します。繰り返し違反したり、重大な違反を1回でも犯した場合、アカウントが永久に禁止される可能性があります。詳細については、「コンテンツ違反と停止」を参照。

コミュニティガイドラインの記載（一部抜粋）　DSA第23条1項に関係する内容

内容

【「アカウントと機能」に関するコミュニティガイドライン】
TikTokのガイドライン違反には、アカウントに対する措置をとることがある。
- TikTokのプラットフォームで許容されているが**「For You」フィードの対象外であるコンテンツを繰り返し投稿**すると、アカウントとそのコンテンツが「For You」フィードの対象外となって検索されにくくなるなど、推奨の対象外になる可能性

【「誠実さと信頼性」に関するコミュニティガイドライン】
スパムと欺瞞行為として、以下を禁止。
- **大量のスパムメールの大量配布**

「コンテンツ違反と停止」の記載（一部抜粋）　DSA第23条4項に関係する内容

内容

- 違反によりコンテンツが初めて削除された場合、アカウントに警告が発行される。（この際、コンテンツが削除された理由、コンテンツが違反したガイドライン、および当社が誤りを犯したと思われる場合に異議を申し立てる方法を説明する通知が届く。）
- 最初の違反が重大な場合は、アカウントを禁止する場合もある。当社のシステムでは、アカウントがコミュニティガイドラインに違反した回数をカウントし、最初の警告以降の違反ごとにアカウントにストライクが発行される。
- 繰り返し違反した場合、または1回の違反の重大度によっては、アカウントを永久に禁止する場合がある。
- アカウントに対する警告は 90 日後に期限切れとなり、永久アカウント禁止の対象から外れる。
- コンテンツまたはアカウントが誤って削除されたと思われる場合は、この決定に対して異議を申し立てることができる。

※NRIが以下の公開情報より確認できたものを整理
利用規約： https://www.tiktok.com/legal/page/eea/terms-of-service/en
「アカウントと機能」に関するコミュニティガイドライン： https://www.tiktok.com/community-guidelines/en/accounts-features
「誠実さと信頼性」に関するコミュニティガイドライン： https://www.tiktok.com/community-guidelines/en/integrity-authenticity

（参考）事業者による取組状況｜欧州における不正利用への対応に関連する記載内容：X

：NRIが関連性を確認した条文

利用規約の記載	DSA第23条1項・2項・4項に関係する内容
内容	【サービスの不正使用】 • 本サービスにアクセスまたは使用する際に、以下のいずれの行為も行ってはなりません。（一部抜粋） 　• 当社のプラットフォーム操作およびスパム ポリシーまたは報告機能の不正使用ポリシー（「信頼性」に関するポリシー）を含むその他の規則やポリシーに違反する行為に従事すること。 【本規約の最後】 • 当社は、以下のいずれかに該当すると合理的に判断した場合、いつでもお客様のアカウントを停止もしくは終了し、サービスの全部または一部の提供を停止することができる。（お客様が本規約または 当社の規則およびポリシーに違反した場合（一部抜粋）） • アカウントが誤って終了したと思われる場合は、ヘルプセンターに記載されている手順に従って異議を申し立てることができる。

「信頼性」に関するポリシーの記載（一部抜粋）	DSA第23条1項・2項に関係する内容
内容	Xで人々の体験を操作・妨害してはならない。（一部抜粋） • コンテンツスパム：大量の、重複した、無関係な、または一方的な方法でコンテンツを共有または投稿して、人々の体験を妨害することの禁止 　• **大量かつ攻撃的な大量の一方的な返信**、メンション、またはダイレクトメッセージを送信すること 　• **同じコンテンツを繰り返し投稿および削除**する 　• 元の投稿のトピックとは無関係なコンテンツで返信してコンテンツを宣伝する。 　• 一般に「コピペ」として知られる、**同一またはほぼ同一の投稿を重複して繰り返し投稿**したり、同一のダイレクトメッセージを送信、等 • エンゲージメントスパム: トラフィックに人為的な影響を与えたり、ユーザーのエクスペリエンスを妨害したりするために、X エンゲージメント機能を不正に使用することは禁止されています。 　• 手動/自動で、**同じ投稿またはアカウントを繰り返し報告**するなど、重複したレポートまたは虚偽のレポートを大量に提出すること。

※NRIが以下の公開情報より確認できたものを整理
利用規約： https://x.com/en/tos
「信頼性」に関するポリシー： https://help.x.com/en/rules-and-policies/authenticity

DSAにおいては、リスク評価・軽減措置に関する前文において、システミックリスクがもたらす悪影響の例示の１つとして、botを利用した偽情報の流通・拡散が挙げられている。（前文84項、104項）。

DSAにおいてbotに関する言及のある前文	＜リスク評価に関連するもの＞ （第84項） ・・・**非常に大規模なオンライン プラットフォームや非常に大規模なオンライン検索エンジンのプロバイダーは、特に、サービスの設計と機能、サービスの意図的で、多くの場合は組織的な操作と使用、またはサービス利用規約の組織的な違反が、このようなリスクにどのように影響するかを評価する必要がある。このようなリスクは、たとえば、偽のアカウントの作成、ボットの使用、サービスの欺瞞的な使用、その他の自動化または部分的に自動化された動作などのサービスの不正使用を通じて発生する可能性があり**、違法なコンテンツであるか、オンライン プラットフォームまたはオンライン検索エンジンの利用規約に準拠していない、偽情報キャンペーンに寄与する情報が急速に広く一般に広まる可能性がある。
	＜リスク軽減措置に関連するもの＞ （第104項） ・・・・・・検討すべきもう一つの領域は、偽情報や操作および濫用行為、未成年者への悪影響など、社会および民主主義に対する**システミックリスクの潜在的な負の影響である。これには、ボットや偽アカウントを使用して意図的に不正確または誤解を招く情報を作成するなど、偽情報を含む情報を増幅することを目的とした協調的な操作が含まれ、経済的利益を得ることが目的となることもあり、**特に未成年者などのサービスの脆弱な受信者にとって有害である。このような分野に関連して、**超大規模オンラインプラットフォームまたは超大規模オンライン検索エンジンが特定の行動規範を遵守し、それに従うことは、適切なリスク軽減措置であると考えられる**。・・・特定の行動規範への参加および実施という事実だけでは、それ自体では本規則の遵守を推定すべきではない。

３．特定の場面（災害・テロ等）に限った特別な対応（EUにおける対応）

概要｜特定の場面（災害・テロ等）に限った特別な対応（EUにおける対応）

項目	DSA（Digital Services Act）
制度上の概要	• 欧州デジタルサービス会議は、欧州委員会に対し、危機的状況についての、危機対応プロトコルを作成を開始するよう勧告することができる（48条）。 • 危機が発生した場合は、欧州委員会は欧州デジタルサービス会議の勧告に基づき、VLOP・VLOSEに対し、深刻な脅威を防止等するための、適切で効果的な措置の特定・適用などの危機対応の措置要求を行うことができる（36条）。
危機の定義	• DSA本則では「危機」についての具体的な定義はないが、前文において、危機として武力紛争やテロ行為、自然災害、パンデミックを例示。 • また、「危機の発生」及び「危機的状況」については、公共の安全又は公衆衛生に対する異常事態の場合とされている（36条２項、48条）
規定制定の背景・執行状況	• 第36条の危機対応メカニズムは、ロシアのウクライナ侵攻に伴う情報操作への懸念の高まりから、追加された規定である • 第36条による危機対応メカニズムが施行された事例は確認されていない（25年2月時点）

DSAでは、危機対応メカニズム（36条）、危機対応への協力（48条）が規定されている

規律	該当条文		仲介サービス	ホスティングサービス	オンラインプラットフォームサービス	VLOP・VLOSE
違法コンテンツに関する措置命令・情報提供の命令	第二章	第9条・第10条	●	●	●	●
連絡先（対DSC、対欧州委員会、対閣僚理事会）、サービス提供者の窓口、法定代理人		第11条・第12条・第13条	●	●	●	●
利用規約の要件		第14条	●	●	●	●
仲介サービス提供者に対する透明性報告義務		第15条	●	●	●	●
利用者への通知・行動の仕組み、情報提供・理由の記載義務		第16条・第17条		●	●	●
刑事犯罪の疑いに関する通知		第18条		●	●	●
内部苦情処理体制・救済の仕組みと法廷外紛争解決		第20条・第21条			●	●
信頼された旗手		第22条			●	●
悪用に対する措置と保護		第23条			●	●
オンライン・プラットフォームのプロバイダーに対する透明性報告義務		第24条			●	●
オンラインインターフェースのデザインと構成		第25条			●	●
オンラインプラットフォームでの広告		第26条			●	●
レコメンダシステムの透明性		第27条			●	●
未成年者のオンラインでの保護	第三章	第28条			●	●
超大規模オンライン検索エンジン		第33条				●
リスク評価、リスク軽減		第34条・第35条				●
危機対応メカニズム		第36条				●
独立監査（外部リスク監査と公的説明責任）		第37条				●
レコメンダシステム		第38条				●
オンライン広告の透明性向上		第39条				●
データへのアクセスと精査（当局・研究者）		第40条				●
コンプライアンス機能		第41条				●
透明性報告義務		第42条				●
監督手数料		第43条				●
標準		第44条		●	●	●
行動規範、オンライン広告・アクセシビリティの行動規範		第45条・第46条・第47条		●	●	●
危機対応への協力		第48条		●	●	●

出所）DSA https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2065#art_22

DSAでは「危機」についての具体的な定義はないが、前文では、武力紛争やテロ行為、自然災害、パンデミックを例示。また、「危機の発生」及び「危機的状況」については、公共の安全又は公衆衛生に対する異常事態の場合とされている（36条２項、48条）。

■ DSAにおいては、「危機」が発生した場合には、欧州デジタルサービス会議は、欧州委員会に対して、危機対応プロトコルの作成を勧告でき（48条）、欧州委員会は、VLOP・VLOSEに対して、危機対応の措置要求を行うことができる（36条）。

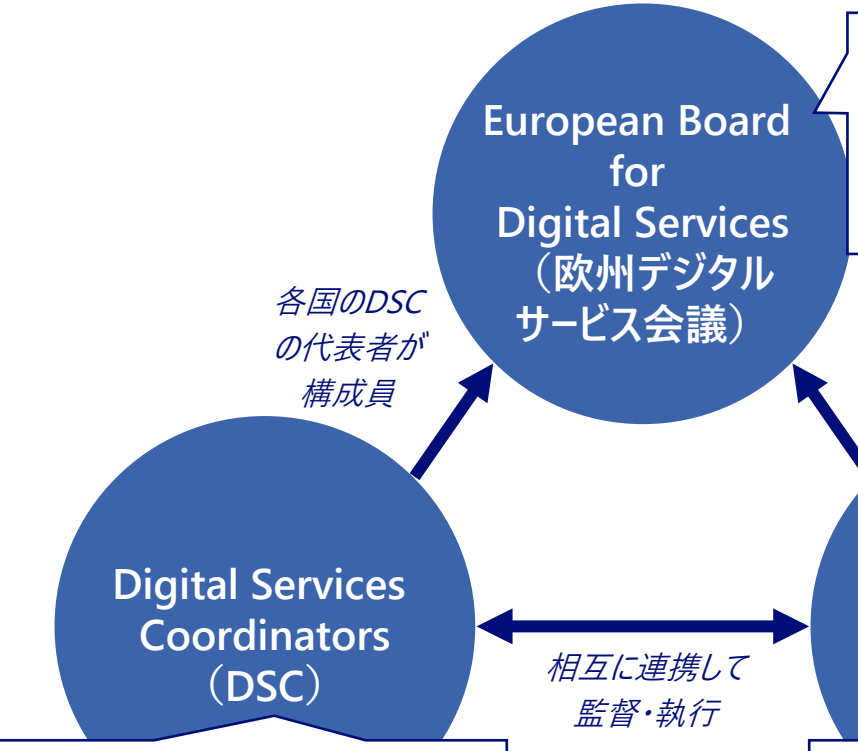
擁護	定義
危機 （crisis）	• **“危機は、連邦内またはその重要な地域において、公共の安全または公衆衛生に対する重大な脅威をもたらす異常事態が発生した場合に発生したものとみなされる”**（第36条2項） • 前文（91）では、下の言及がある。 “危機は、連邦またはその重要な部分において、公共の安全または公衆衛生に対する重大な脅威につながり得る異常な状況が発生した場合に発生すると考えられるべきである。このような危機は、**武力紛争**や**テロ行為**（新興の紛争やテロ行為を含む）、**地震**や**ハリケーン**などの**自然災害**、**パンデミック**や**公衆衛生**に対する国境を越えたその他の深刻な脅威から生じる可能性がある”
危機的状況 （crisis situations）	• **“公共の安全または公衆衛生に影響を及ぼす異常事態”**（第48条）

出所）EU-Lex「Document 32022R2065」https://eur-lex.europa.eu/eli/reg/2022/2065/oj -

特定の場面（災害・テロ等）に限った特別な対応（EUにおける対応）

参考）DSAにおいて、VLOP/VLOSEへの監督・執行は欧州委員会、その他事業者への監督・執行はDSCが担う

■ DSCの代表と欧州委員会で構成される「欧州デジタルサービス会議」がDSCと欧州委員会を支援する。



独立した諮問機関として各国のDSAと欧州委員会と協力し、支援する

- ✓ DSCと欧州委員会の効果的な協力への貢献
- ✓ DSAに関連する新たな問題についての調整や分析への貢献
- ✓ VLOPやVLOSEの監督におけるDSCや欧州委員会への支援

加盟国内におけるDSAの監督・執行の権限を有する

（ただし、VLOP・VLOSEに対する監督・執行は欧州委員会が担う）

- ✓ EU加盟国はDSAの適用および執行に責任を有する所管当局としてDSCを指定する
- ✓ DSCは独立した主体として、DSAの執行の権限と責任を国内において負うとともに、欧州委員会ならびに他の加盟国との連携を行う

VLOP・VLOSEの指定と監督・執行を担う

- ✓ 欧州委員会は、VLOP・VLOSEのみに課される追加義務について、独占的な監督および執行の権限を有する（追加義務以外についても、VLOP・VLOSEに対する監督・執行する権限を有する）
- ✓ 欧州委員会と各国のDSCは、DSAを一貫して効率的に適用するために、緊密に協力し、相互に援助しあう

出所）EU-Lex「Document 32022R2065」https://eur-lex.europa.eu/eli/reg/2022/2065/oj -
https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

第48条にもとづき、欧州デジタルサービス会議は、欧州委員会に対して、危機プロトコルの作成の開始を勧告することができる。

■ 第48条では、**欧州デジタルサービス会議は欧州委員会に対し**、オンライン環境における危機的状況に対処するため、**自主的な危機プロトコルの作成を開始するよう勧告する**ことができると規定（第1項）し、**欧州委員会はVLOP・VLOSE等に対して危機対応プロトコル（信頼できる情報の強調、緊急連絡窓口の設置、通報対応・コンテンツ審査等について通常時よりも人員・資源の強化）への参加を奨励・促進**し（第2項）、危機プロトコルにおいては、プロトコルにおいて対処すべき「危機」の特定や各機関の役割分担、始期・終期の条件等について規定（第4項）。

項目	【第48条】
自主的な危機対応プロトコルの策定開始の勧告（1項）	• 欧州デジタルサービス会議は欧州委員会に対し、オンライン環境における危機的状況に対処するため、自主的な危機プロトコルの作成を開始するよう勧告することができる
危機対応プロトコルにおける措置（2項）	• 欧州委員会は、VLOP・VLOSE、必要に応じてそのほかの事業者に対して、危機対応プロトコルの策定、テスト、適用に参加することを奨励し、促進する。危機対応プロトコルには以下の措置を含めることを目指す ➢ 公的機関やその他の信頼できる機関からの危機に関する情報を目立つように表示すること ➢ 危機管理のための特定の連絡先窓口を指定すること ➢ 通知（16条）、内部苦情処理体制（20条）、Trusted Flagger(22条）、悪用に対する措置（23条）、軽減措置（35条）に定める義務の遵守に充てられる資源を、危機的状況から生じる必要性に適応させること
加盟国当局・その他組織の関与（3項）	• 欧州委員会は、必要に応じて加盟国の当局を関与させ、また、危機対応プロトコルの策定、検証、適用監督において、欧州連合の機関、事務局、および機関を関与させることができる。欧州委員会は、必要かつ適切な場合には、危機対応プロトコルの策定において市民社会組織またはその他の関連組織を関与させることもできる
危機対応プロトコルの規定内容（4項）	• 欧州委員会は、危機対応プロトコルが以下のすべてを明確に規定することを確保することを目指す ➢ 危機管理プロトコルが対処しようとする特定の異常な状況およびその目的を決定するための具体的なパラメータ ➢ 各参加者の役割、危機管理プロトコルの発動前および発動後の各参加者が講じる措置 ➢ 危機管理プロトコルを発動すべき時期を決定するための明確な手順 ➢ 危機管理プロトコルが発動された後に講じられる措置の実施期間を決定するための明確な手順 ➢ 表現の自由や非差別等の基本的権利の行使に対する悪影響に対処するための保護措置 ➢ 危機的状況が終結した時点で、とられた措置、その期間、結果を公表するプロセス
危機対応プロトコルの修正（5項）	• 欧州委員会が、危機管理プロトコルが危機的状況に効果的に対処していない、または基本的権利の行使を保護していないと判断した場合、欧州委員会は、追加措置の実施を含め、危機管理プロトコルの修正を参加国に要請する

出所）DSA Observatory「The DSA's crisis approach: crisis response mechanism and crisis protocols」
https://dsa-observatory.eu/2023/02/21/the-dsas-crisis-approach-crisis-response-mechanism-and-crisis-protocols/

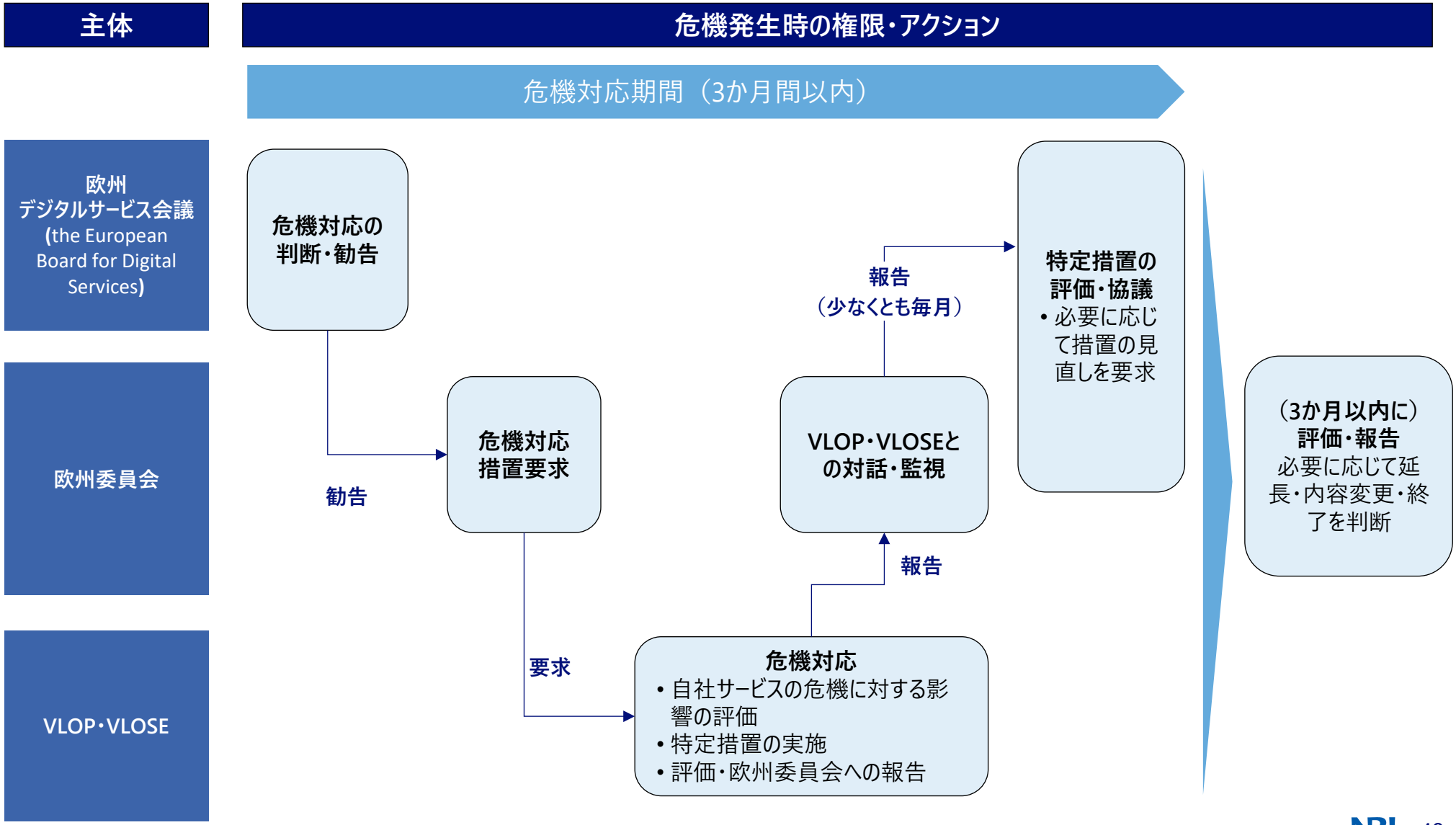
第36条にもとづき、欧州委員会はVLOP・VLOSEに対し、危機対応の措置要求を行うことができる。

■ 第36条では、欧州委員会は**欧州デジタルサービス会議からの勧告**に基づき、**VLOP・VLOSEに対し、危機的状況に起因するリスクを軽減するための一定の措置を講じるよう求めることができる**と規定している

項目	【第36条】
危機対応の採択とVLOP・VLOSEに課せられる義務（1項）	• 危機が発生した場合、欧州委員会は欧州デジタルサービス会議の勧告に基づき、VLOP、VLOSEに対し、以下の措置を講じることを求める決定を採択することができる ➢ 危機における深刻な脅威に対して、自社サービスの関与の状況・可能性を評価すること ➢ 上記の評価に対して、具体的かつ効果的な措置を適用すること（35条（軽減措置）や48条（危機対応への協力）も含めた措置を講じること） ➢ 一定の期日または決定で特定される定期的な間隔で欧州委員会に報告すること
危機の始期（2項）	• 危機は、異常な状況が欧州連合またはその相当部分における公の安全または公衆衛生に深刻な脅威をもたらす場合に発生したものとみなされる
欧州委員会による採択の要件（3項）	• 欧州委員会は、第1項に定める決定を行う場合、以下のすべての要件が満たされることを確保しなければならない ➢ 危機の重大性、措置の緊急性等を踏まえた上で、採択が厳格に必要、正当、均衡が取れていること ➢ 特定の措置が取られるべき合理的な期間を特定すること ➢ 期間は3か月を超えない期間に限られること
採択後の欧州委員会の措置（4項）	• 欧州委員会による採択後の措置を規定 ➢ 対象となるサービス事業者への決定の通知、決定の一般への公開 ➢ 欧州デジタルサービス会議への決定の通知と意見収集、進捗の報告
特定の措置の選択（5項）	• 具体の特定措置の決定は、対象となるVLOP・VLOSEに委ねられる
欧州委員会による対話（6項）	• 欧州委員会は、当該事業者と対話を行うとともに、規定された要件を満たしていることを確保すること
欧州委員会による監視（7項）	• 欧州委員会は、特定措置の適用を監視し、（少なくとも）毎月、欧州デジタルサービス会議に報告すること • 特定措置が効果または均衡を欠くと判断した場合、欧州委員会は欧州デジタルサービス会議と協議した上で、当該特定措置の見直しを当該提供者に対して要求する決定を採択することができる
欧州委員会による報告（11項）	• 欧州委員会は、危機終結から3か月以内に、それらの決定に従って採択された特定措置の適用について報告すること

出所）DSA Observatory「The DSA's crisis approach: crisis response mechanism and crisis protocols」
https://dsa-observatory.eu/2023/02/21/the-dsas-crisis-approach-crisis-response-mechanism-and-crisis-protocols/

危機対応メカニズムは、欧州デジタルサービス会議の勧告を起点とした対応が行われる。



第36条の危機対応メカニズムはロシアのウクライナ侵攻に伴う情報操作への懸念の高まりから、追加された。市民団体からの批判を受け、危機対応の最長期間（3か月）を設定した。

危機対応メカニズムをめぐる動向

年月日	概要	背景・詳細

2022年3月15日	• 第3回トリローグ（非公開）で第36条の危機対応メカニズムを追加	• ロシアによるウクライナ侵攻開始（2月24日）
		• 閣僚理事会がRussia TodayとSputnikの放送禁止を決定（3月2日）
		• プラットフォームに対し上記の両メディアのコンテンツの流通禁止を義務化
		  • EU域内でサービスを提供している衛星テレビやインターネットのプロバイダーは、プラットフォームを通じて両メディアのコンテンツが配信されないよう義務付けた。
		  • 違反への罰則や執行方法は各国に委ねられている。
		  • 市場関係者を対象とする経済制裁として実施しており、既存のEUのメディア規制（視聴覚サービス法等）とは別建てとして整理されている。
		• ロシアのウクライナ侵攻によって生じた、オンライン上の情報操作(manipulation)に対する影響を背景に、危機対応メカニズム（36条）を導入

2022年4月12日	• 38の市民団体が危機対応メカニズムに対する懸念を表明する声明に署名	＜主な指摘＞ • 「危機（crisis）」の定義を特定の脅威に限定すべきであり、現状は欧州委員会に危機対応を何年も維持する権限を与えている • 危機対応の期限を含んでおらず、裁判所による差止め以外に欧州議会による再検討の機会を設けるべき • 危機対策が「厳密に必要かつ相応」であるかを欧州委員会が評価するのでなく、独記した司法機関や裁判所が定期的に行うべき
2022年7月5日	• 欧州議会で最終文書を承認	• 第36条3項cで危機対応の最長期間を3か月に設定

出所）EURACTIV 「EU rolls out new sanctions banning RT and Sputnik」 https://www.euractiv.com/section/digital/news/eu-rolls-out-new-sanctions-banning-rt-and-sputnik/
EDRi 「ON NEW CRISIS RESPONSE MECHANISM AND OTHER LAST MINUTE ADDITIONS TO THE DSA」 https://edri.org/wp-content/uploads/2022/04/EDRi-statement-on-CRM.pdf
DSA Observatory「The DSA's crisis approach: crisis response mechanism and crisis protocols」
https://dsa-observatory.eu/2023/02/21/the-dsas-crisis-approach-crisis-response-mechanism-and-crisis-protocols/

第36条による危機対応メカニズムが施行された事例は確認されていない（25年2月時点）。

- 欧州委員会HPで公開されている、VLOP・VLOSEの監視施行に関する情報では、第36条・48条にもとづく執行事例は確認されていない
- 第36条・第48条は欧州デジタルサービス会議の勧告に基づいて行われると規定されているが、過去10回の会議（2025年2月末まで）において、第36条・第48条に関連する議題は確認されていない
  - 2024 年6月の第5回会議から設置された8つのワーキンググループにおいても、危機対応メカニズムや危機対応プロトコルに関連するワーキンググループは設置されていない

出所）欧州委員会 https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses
https://digital-strategy.ec.europa.eu/en/policies/dsa-board-working-groups

参考）「偽情報に関する行動規範」では、「危機」に関し、署名事業者に対して、ユーザーインターフェースの設計や危機対応措置の公表、危機対応システムの構築を求めている。

■ 署名事業者の透明性レポート（24年9月公表版）では、ロシアによるウクライナ侵攻、ハマスとイスラエルの紛争に関して、コミットメントへの取組状況が記載されている。

分野	コミットメント・措置	内容
ユーザーのエンパワーメント	コミットメント22 措置7	（**ユーザーインターフェースの設計**） • 関連署名団体は、公共や社会が特に関心を持つ話題や**危機的状況**において、利用者を信頼できる情報源に導くような製品や機能（情報パネル、バナー、ポップアップ、地図やプロンプト、信頼性指標など）を設計し、適用する。
透明性センター	コミットメント35 措置4	（**危機対応措置の公表**） • **危機的状況**において、署名団体は透明性センターを利用し、**危機**に関連して講じられた具体的な緩和措置に関する情報を公表する。

常設タスクフォース	コミットメント37
	措置2
		（**危機対応システムの構築**）
		• 署名団体は、タスクフォースにおいて、特に（これに限定されるものではないが）以下の業務に取り組むことに同意する：
		  • 選挙や**危機**のような特殊な状況下で使用するリスク評価手法と迅速な対応システムを確立する。
		  • 選挙や**危機**のような特別な状況下で各団体と協力・調整する。

監視体制の強化	コミットメント42	（**情報・データの提供**） • 関連する署名団体は、選挙や**危機**のような特別な状況において、欧州委員会の要請があれば、タスクフォースによって確立された迅速な対応システムに従い、特別な報告書や定期的な監視の中の特定の章を含む、相応かつ適切な情報やデータを提供することを約束する。

出所）欧州委員会(2023)「The Strengthened Code of Practice on Disinformation2022」
https://disinfocode.eu/wp-content/uploads/2023/01/The-Strengthened-Code-of-Practice-on-Disinformation-2022.pdf -

4． 法制度の執行権限・体制

各国制度における執行体制・権限の概要（DSA・OSA）

項目	DSA（Digital Services Act）	OSA（Online Safety Act）
執行体制・執行権限	• 各加盟国内における監督・執行権限はDSCが担う。 • VLOP/VLOSEに対する監督・執行は、欧州委員会が担う。 なお、執行に当たっては、欧州委員会はDSCの協力を得ながら調査を実施し、欧州デジタルサービス会議の意見を踏まえた予備的見解を経て違反を決定。	• SNS等のユーザー間サービス及び検索サービスを提供する事業者に対する監督・執行は、Ofcomが独立した規制当局として担う。 なお、執行に当たっては、Ofcomは調査を実施し、違反仮通知の発出、サービス提供者の意見陳述を経て、義務違反と判断した場合には違反を決定。

4－1．　EUにおけるDSA （Digital Services Act）の執行権限・体制

DSAの執行にかかる規定

第Ⅳ章 実施、協力、制裁及び執行	
第1節 所轄官庁と各国デジタルサービス・コーディネーター	
第49条	所轄官庁とデジタル・サービス・コーディネーター
第50条	デジタルサービス・コーディネーターの要件
第51条	デジタル・サービス・コーディネーターの権限
第52条	罰則
第53条	異議を申し立てる権利
第54条	報酬
第55条	活動報告
第2節 権限、協調調査及び一貫性メカニズム	
第56条	権限
第57条	相互援助
第58条	デジタルサービスコーディネーターの国境を越えた協力
第59条	欧州委員会への照会
第60条	共同調査
第3節 欧州デジタルサービス会議	
第61条	欧州デジタルサービス会議
第62条	会議の構成
第63条	会議の任務

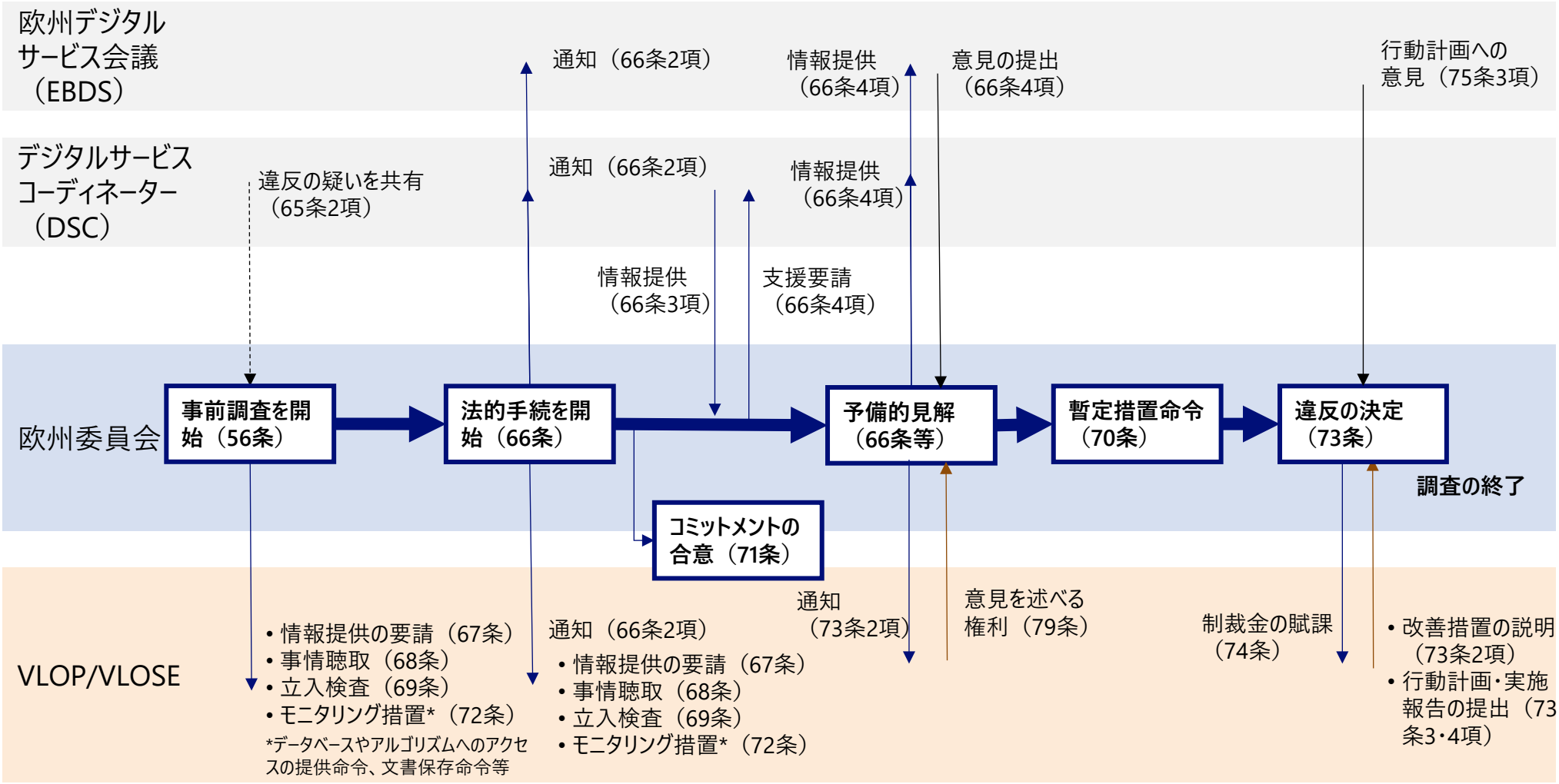
第Ⅳ章 実施、協力、制裁及び執行（つづき）	
第4節 超大規模オンラインプラットフォームおよび超大規模オンライン検索エンジンの提供者に関する監督、調査、遵守及びモニタリング	
第64条	専門知識及び能力の開発
第65条	超大規模オンライン・プラットフォームおよび大規模オンライン検索エンジンの提供者の義務の実施
第66条	欧州委員会による法的手続の開始と調査への協力
第67条	情報提供要請
第68条	事情聴取と回答を受ける権限
第69条	調査の権限
第70条	暫定措置
第71条	コミットメント
第72条	モニタリング行為
第73条	違反
第74条	制裁金
第75条	第III章第5節に定められた義務違反に対する救済措置の監督強化
第76条	定期的な制裁金の支払い
第77条	制裁金賦課の制限期間
第78条	罰則の執行期限
第79条	聴聞権と記録へのアクセス権
第80条	決定事項の公表
第81条	欧州連合司法裁判所による審査
第82条	アクセス制限の請求と国内裁判所との協力
第83条	欧州委員会の介入に関する実施法

第Ⅳ章 実施、協力、制裁及び執行（つづき）	
第5節 執行に関する共通規定	
第84条	職業上の秘密
第85条	情報共有システム
第86条	代理
第6節 委任法および実施法	
第87条	委任の発動
第88条	委員会手続き

出所）EU-Lex「Document 32022R2065」
https://eur-lex.europa.eu/eli/reg/2022/2065/oj -

VLOP/VLOSEに対する執行の手順とステークホルダーの動き

DSA違反の疑いがある場合に欧州委員会が事前調査を開始。DSCの協力を得ながら事業者に対する強力な調査権限を有し、欧州デジタルサービス会議の意見を踏まえた予備的見解を経て違反を決定



出所）DSAの各条文を基にNRI作成　https://www.eu-digital-services-act.com/Digital_Services_Act_Articles.html

（参考）各国におけるDSC（Digital Services Coordinators）の任命状況（2025年2月現在）

■ 2025年2月5日現在、EU加盟国27か国中25か国がDSCに任命した機関を公表している。
■ 公表している25か国のうち、19か国が通信系の当局をDSCに指名している。

：通信系当局
－　：なし

加盟国	DSC任命機関
オーストリア	Austria Communications Authority（オーストリア通信局）
イタリア	Authority for Communications Guarantees（通信規制庁）
ベルギー	－
ラトビア	Consumer Rights Protection Centre（消費者権利保護センター）
ブルガリア	Communications Regulation Commission（通信規制委員会）
リトアニア	Communications Regulatory Authority (RRT)（通信規制局）
クロアチア	Croatian Regulatory Authority for Network Industries (HAKOM)（クロアチアネットワーク産業規制庁）
ルクセンブルク	Competition Authority（競争庁）
キプロス	Cyprus Radiotelevision Authority（キプロスラジオテレビ局）
マルタ	Malta Communications Authority（マルタ通信局）
チェコ共和国	Czech Telecommunication Office（チェコ通信局）
オランダ	Authority for Consumers and Markets（ACM）（オランダ消費者市場庁）
デンマーク	Danish Competition and Consumer Authority（デンマーク競争・消費者庁）
ポーランド	－

加盟国	DSC任命機関
エストニア	Consumer Protection and Technical Regulatory Authority (CPTRA)（消費者保護・技術規制庁）
ポルトガル	National Communications Authority (ANACOM)（国家通信局）
フィンランド	Finnish Transport and Communications Agency (TRAFICOM)（フィンランド運輸通信庁）
ルーマニア	National Authority for Management and Regulation in Communications (ANCOM)（通信管理規制機関）
フランス	Regulatory Authority for Audiovisual and Digital Communication (Arcom)（視聴覚およびデジタル通信規制局）
スロバキア	Council for Media Services（メディア・サービス評議会）
ドイツ	Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railways (BNetzA)（ネットワーク庁）
スロベニア	Agency for Communication Networks and Services of the Republic of Slovenia (AKOS)（スロベニア通信ネットワーク・サービス庁）
ギリシャ	Hellenic Telecommunications and Post Commission (EETT)（通信・郵便委員会）
スペイン	National Commission for Markets and Competition（国家市場競争委員会）
ハンガリー	National Media and Infocommunications Authority（国家メディア情報通信局）
スウェーデン	Post and Telecom Authority（郵便・電気通信局）
アイルランド	Media Commission（メディア委員会）

出所）欧州委員会「Digital Services Coordinators」https://digital-strategy.ec.europa.eu/en/policies/dsa-dscs -

VLOP/VLOSEに対する執行｜規定内容（1/2）

欧州委員会はVLOP/VLOSEのシステミックリスク管理に対する義務について、排他的な監督および執行の権限を有し、関連するDSCと協力しながら調査権限を行使できる

	義務の内容
権限（56条）	• **欧州委員会はVLOP/VLOSEによるシステミックリスク管理に対する追加的義務**（33条～43条）に関する監督および執行の**排他的権限**を有し（56条1項）、その他のDSAの監督および執行の権限を有する（56条2項）。 • 加盟国および欧州委員会は、緊密に協力してDSAの規定を監督、執行する（56条5項）。
欧州委員会による法的手続の開始および調査への協力（66条）	• 欧州委員会は、DSAに違反した疑いのある**VLOP/VLOSEの関連行為に関して**、違反決定が採択される可能性を考慮して**法的手続きを開始でき**（66条1項）、すべてのDSCおよびEBDS、関係するVLOP/VLOSEに通知する（66条2項）。 • 欧州委員会は調査権限の行使に当たり、関連するDSCに支援を要請でき（66条3項）、**DSCおよびEBDSに権限の行使および予備的見解に関するすべての関連情報を提供**する。EBDSは予備的見解に関する意見を欧州委員会に提出し、欧州委員会は当該意見を最大限考慮する（66条4項）。
情報提供要請（67条）	• 欧州委員会は、単なる要請または決定によりVLOP/VLOSEおよび独立監査主体等の関係者に合理的な期間内に**違反の疑いに関連する情報の提供を要請**できる（67条1項）。 • 要請においては、法的根拠や目的、期限および不正確・不完全・誤解を招く情報を提供した場合に課される**制裁金**を定めなければならない（67条2～3項）。
事情聴取と回答を受ける権限（68条）	• 欧州委員会は、違反の疑いに関連する調査対象事項に関する情報の収集を目的として任意の事情聴取を行える（68条1項）。
立入検査の権限（69条）	• 欧州委員会は、VLOP/VLOSEや関係する者の**施設において必要なすべての検査を実施**でき（69条1項）、組織、機能、ITシステム、アルゴリズム、データ処理および業務慣行へのアクセスと説明の提供等（69条2項(d)）を求めることができる。 • VLOP/VLOSEが検査に反対している場合、加盟国は国内法に従って強制措置の形で検査を実施できるよう必要な支援を行わなければならない（69条8項）。
暫定措置（70条）	• 違反決定が採択される可能性がある法的手続きの文脈において、サービス受領者に深刻な損害が生じるリスクがあり緊急を要する場合、欧州委員会は**予備的見解を根拠**として決定によりVLOP/VLOSEに対して**暫定措置を命じることができる**（70条）。

出所）DSA https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2065

DSA違反の決定前に欧州委員会は予備的見解を通知し、VLOP/VLOSEはコミットメントを申出できる。違反が決定した場合、VLOP/VLOSEは行動計画を提出し、モニタリングされる

	義務の内容
コミットメント（71条）	• 法的手続きの過程において、VLOP/VLOSEがDSAの関連する規定の遵守を確保する旨のコミットメントを申し出た場合、欧州委員会は決定によりコミットメントの拘束力を認め、さらなる措置の根拠がない旨を宣言できる（71条1項）。 • 欧州委員会は、決定の根拠となった事実に重大な変更があったり、VLOP/VLOSEがコミットメントに反する行為を行ったりした等の場合に**法的手続きを再開できる**（71条2項）。
モニタリング行為（72条）	• 欧州委員会は、VLOP/VLOSEによるDSAの有効な実施と遵守を監視するために必要な措置を講じることができる。措置には**データベースやアルゴリズムへのアクセスと説明を提供**するよう命じたり、義務の履行や遵守の評価に**必要な全ての文書の保存義務を課す**ことを含みうる（72条1項）。
違反（73条）	• 欧州委員会は、VLOP/VLOSEがDSAの関連規定、暫定措置、コミットメントのいずれかを遵守していないと判断した場合、違反決定を採択する（73条1項）。 • 欧州委員会は、**違反決定の前にVLOP/VLOSEに対して予備的見解を通知**し、予備的見解に効果的に対処するために欧州委員会またはVLOP/VLOSEが講じるべき措置について説明しなければならない（73条2項）。 • 欧州委員会は、違反決定においてVLOP/VLOSEに対し遵守に必要な措置を合理的期間内に講じること、VLOP/VLOSEが講じる予定の措置に関する情報を提供することを命じ（73条3項）、VLOP/VLOSEは措置の実施後に欧州委員会に説明を提出しなければならない（73条4項）。
VLOP/VLOSEによるシステミックリスク管理に対する追加的義務（33条～43条）の違反に対処するための救済措置の監督強化（75条）	• 欧州委員会は、VLOP/VLOSEが**システミックリスク管理に対する追加的義務**（33条～43条）のいずれかに違反して違反決定を採択する際、VLOP/VLOSEに対し合理的な期間内にDSC、欧州委員会、EBDSに**違反の是正に必要な措置を定めた行動計画を作成し、伝達**することを求めなければならない（75条2項）。 • 行動計画の受領後1か月以内に、**EBDSは行動計画に関する意見を欧州委員会に伝え**、その1か月後に欧州委員会は行動計画に定められた措置が違反の是正に十分かどうかを決定し、実施のための合理的な期間を定める。**欧州委員会は行動計画の実施をモニタリング**し、VLOP/VLOSEは監査報告書を遅滞なく欧州委員会に報告し、行動計画の実施に向けた最新情報を提供し続けなければならず、欧州委員会は監視に必要な情報の提供を要請できる（75条3項）。 • 欧州委員会は、行動計画の実施状況およびモニタリングについて、EBDSおよびDSCに随時報告しなければならない（75条3項）。

出所）DSA https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2065

参考）関連するその他の規定

	義務の内容
DSCに関する規定（49条～51条）	• 加盟国は、1つ以上の管轄当局をデジタルサービスコーディネーター（DSC）に指名し（49条1項）、**DSAの監督および執行に関して国内レベルの調整を担当するとともに、欧州デジタルサービス会議（EBDS）や欧州委員会と協力**する（49条2項）。 • DSCは公平、透明、迅速な方法で職務を遂行するために必要な資源を確保し、加盟国はDSCの予算管理における十分な独立性を確保しなければならず（50条1項）、外部からの影響を受けず、完全に独立して行動しなければならない。（50条2項）。 • DSAに基づく任務の遂行に必要な場合、自国の権限に服する仲介サービス提供者の行為に関して**調査権限**（51条1項）、**執行権限**（51条2項）を有する。
制裁（52条）	• 加盟国は、仲介サービス提供者によるDSAの違反に適用される制裁に関する規則を自国の権限の範囲内で定め、確実に実施されるよう必要な全ての措置を講じなければならず（52条1項）、制裁は効果的で均衡がとれており、抑止力があるものでなければならない（52条2項）。 • 加盟国は、DSAで定められた義務の不履行に課されうる制裁金の最高額が、当該仲介サービス提供者の前会計年度における全世界年間売上高の6%、定期的な制裁金となるよう確保しなければならない（52条3項）。
異議申立ての権利（53条）	• サービスの受信者およびDSAにより権限行使を付与されたあらゆる団体は、仲介サービス提供者にDSA違反を申し立てる権利を有し、当該仲介サービス提供者はサービスの受領者が所在または設立されている加盟国のDSCに異議申立てができる（53条）。 • 両当事者は国内法に従って意見を述べ、異議申立ての状況に関する適切な情報を受け取る権利を有する（53条）。

出所）DSA https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2065

DSAの執行について①（欧州委員会担当（DG CONNECT）による聞き取り）

【組織体制・人員配置について】

●**欧州委員会（DG CONNECT）では、DSAの監督と執行に特化した３つのユニットがある。**
（1年半前は30~40人程度であったが**３倍に増強された**）

- 規則遵守の監督・調整を担当するユニット（30人程度）
- DSAの執行を担当するユニット（60～70人）
- 経済・技術評価ユニット※データの分析や技術的な分析を担当 （30人程度）

●年末（2025年末）までには200人まで職員（法的サポートやその他の専門家を除外した数字）を増やす予定。

●ECAT（The European Centre for Algorithmic Transparency）は、DSAの執行を支援するための科学的・技術的な専門知識を提供。また、オンラインプラットフォームや検索エンジンによって展開されるアルゴリズムシステムの影響に関する研究を行い、その成果を提供。

●DG CONNECTでは、特定のVLOPSEsごと/水平的な問題（未成年者保護、オンライン犯罪、データアクセス、リスク評価等）ごとのマトリックス構造で担当が決定。

●DSAの執行のため、アルゴリズム分析、法務、経済分析、法律、ポリシー、経済、データ分析の専門家がいる。

※欧州委員会担当（DG CONNECT）から聞き取った内容について、NRIにおいて要約したもの。

DSAの執行について②（欧州委員会担当（DG CONNECT）による聞き取り）

【事前調査の端緒】

- **定期的なモニタリングにおいては、違法コンテンツ、選挙の完全性、未成年者保護、オンラインマーケットプレイスでの違法製品に関するものが優先。**選挙の完全性については、例えば、選挙の際に偽情報が組織的に流通・拡散され、それによって選挙の完全性が危険にさらされていないかどうか等についてモニタリングをする。

- VLOPSEs がDSAの規則を遵守しているか監視するに当たり、**DSCが一般の国民や団体から苦情を受け付けるチャネルや、内部告発システム（DSA whistleblower tool） として、内部告発を受けるチャネルを活用。また、市民団体からの通報を定期的に報告を受けている。**一例として、フランスの団体が有料のFacebook広告の中で偽情報や不正な詐欺情報があることを発見したが、これをMetaに対しての調査開始の証拠として利用した。**市民団体が有する専門知識は、DG CONNECTの専門知識と活動を補完することができるため、連携は大切。**

- **サービス上のコンテンツについて、当局が常時かつ積極的に監視することは、DSAの下では禁止。**実際には、PF事業者や当局だけでコンテンツ全てを監視することは不可能であるため、**DSAの目的の1つは、 PF事業者、ユーザー、市民社会、当局を含む利害関係者の間で、オンラインの安全性を強化する責任を分散させることである。欧州委員会は、全体的な枠組みが機能しているかどうかを監督する。**基本的なアプローチは、すべての利害関係者がDSAの執行において、自らの役割を果たすことを確保すること。

※欧州委員会担当（DG CONNECT）から聞き取った内容について、NRIにおいて要約したもの。

DSAの執行について③（欧州委員会担当（DG CONNECT）による聞き取り）

【調査方法】

- DSA第68条第1項に基づくインタビュー手続が必要な場合には、PF事業者の担当者へのインタビューを行うことが可能。これは、第三者の関与を得て実施することもできる。ただし、これまで、第三者が関与するものと関与しないものいずれのインタビューも行われていない。必要に応じて、DSAの第69条(2)(a)に基づく立入検査も実施される。

【調査・分析対象】

- **通知メカニズム**
  - PF事業者は、ユーザーが違法コンテンツにフラグを立てることができるような機能（通知メカニズム）を実装する必要がある。
  - 監督・執行当局は、通知メカニズムが適切に機能しているかどうかを評価する。
- **システミック・リスクの評価および軽減の報告書**
  - VLOPSEsは、サービスから生じるリスクを評価し、適切な緩和措置を実施し、報告書に詳述する必要がある。
  - 欧州委員会は、VLOPSEsが、未成年者に対するリスクを含め、サービスから生じるリスクを適切に評価し、適切な緩和措置を実施しているかを分析する。
- **研究者のためのデータへのアクセス**
  - VLOPSEsは、特定の要件を満たす研究者に対して、VLOPSEsの公開および非公開データへのアクセスを許可し、研究者がVLOPSEsのシステミックリスクを調査できるようにすべき。
  - 欧州委員会は、VLOPSEsが研究者の調査を不適切に阻害した場合、調査を開始することができる。

※欧州委員会担当（DG CONNECT）から聞き取った内容について、NRIにおいて要約したもの。

DSAの執行について④（欧州委員会担当（DG CONNECT）による聞き取り）

【執行】

- **DSAは、制裁を課すことを目的としたものではなく、サービスの安全性を高め、利用者の基本的権利が保護されることを確保するために、欧州委員会がPF事業者との対話に関与することを目的としている。**そのため、PF事業者のコンプライアンスの不備が指摘された場合、PF事業者、欧州委員会および市民社会の間の継続的な対話において改善が求められる。PF事業者は是正措置を講じることが期待されており、そうでなければ、PF事業者は多額の罰金を科される可能性がある。

- **DSAの執行について、欧州委員会によるPF上のコンテンツに対する常時監視に似ているといわれるが、これは事実ではない。**その代わりに、**欧州委員会は、PF事業者がオンラインリスクに対処するために必要なプロセス、システム、手順を実施しているかどうかを継続的に評価し、個々の違法情報を特定しない。**DSAにおいては、欧州委員会は、PF事業者がアルゴリズムを通じて脅威が増幅されているかどうかを監視し、システムと運用構造をチェックする。PF事業者は、自らのプラットフォームとそれがもたらすリスクを評価し、欧州委員会は、DSAの下で要求されるこれらのシステムと運用構造の適切性・有効性を監督する。

- これまでDSA第69条(2)(d)(サービス提供者が保有するデータ及びアルゴリズムへのアクセス)に基づく執行の事例はない。しかし、いずれは第69条に基づく調査が行われることが予想される。この規則の下では、執行に関連するすべてのシステムにアクセスすることができる。なお、調査のために現場での立ち入りは必ずしも必要ではない。

- どのようなデータとアルゴリズムへのアクセスにあたり、どの程度の粒度（例：当該情報が記録された個別の文書単位、○○に関して記された情報一式など）のものをアクセスできるよう命令するかについては、ケースバイケースだが、**当該トピックに関連するものであれば、APIなどすべてにアクセスできる。**この執行には正当な理由が必要であるため、PF事業者は、アクセス要求に対して法的に異議を申し立てることができる。

- **欧州委員会は、データ分析能力を有するECATと協力。**欧州委員会は、AI、機械学習、生成AIを組み込んだオープンソースソフトウェアに基づく分析のための独自のソフトウェアを有している。また、PF事業者に情報提供を要求した場合、膨大なデータを受領することもあるが、当該データを管理するために、欧州委員会は電子情報開示ソフトウェアを活用。さらに、欧州委員会は分析支援を得るために外部の専門家とも契約している。

※欧州委員会担当（DG CONNECT）から聞き取った内容について、NRIにおいて要約したもの。

DSAの執行について⑤（欧州委員会担当（DG CONNECT）による聞き取り）

【リスク評価に関する執行】

- **DSA第34条(リスク評価)は、有害情報から生じるリスクにも対処している。**他方、偽情報そのものが必ずしも問題ではないため、条文上は偽情報については、明示的に言及していない。偽情報に対する懸念は、例えば、選挙の完全性、公共の安全、健康を損なう可能性のある偽情報が流通・拡散されることによって生じる悪影響にある。したがって、第34条および第35条は、PF事業者に対し、例えば、偽情報の拡散が選挙の完全性を損なう場合には、評価し、軽減措置を講じることを要求している。欧州委員会は、2024年の欧州議会選挙に先立ち、選挙の完全性に対するリスクに対処する方法に関するベストプラクティスを概説した、VLOPSEsのためのガイドラインを公表した。
- PF事業者は、**年1回のリスク評価を実施することが求められる。**さらに、新しいアルゴリズムなどの新機能から生じるリスクも、実装前に評価する必要がある。

※欧州委員会担当（DG CONNECT）から聞き取った内容について、NRIにおいて要約したもの。

DSAの執行について⑥（欧州委員会担当（DG CONNECT）による聞き取り）

【リスク軽減措置に関する執行】

- 各種行動規範の遵守がリスク軽減措置（ DSA第35条(リスク軽減措置) ）の担保の際に考慮されるが、事業者から受け取る監査レポートや市民団体から受け取った証拠を基に、対策が明らかに不足していると判断した場合に調査を開始する。
- **欧州委員会がリスク評価・軽減措置義務の違反を評価する際には、事業者間で対応を比較し不足している部分が無いかを確認する。**例えば、5つのPF事業者を調査し、そのうち4つのPF事業者において最先端の対策と考えられるものを実施しているが、残りの1つが実施していない場合、そのプロバイダーは違反している可能性があると判断する。**違反の評価は、次のような様々な基準に基づいて行う。**
  - ✓ その措置が合理的であるかどうか。
  - ✓ PF事業者の規模に見合ったものであるか。
  - ✓ リスクに効果的に対処しているか。
- 一方で、**DSA上、PF事業者が取るべき対策を具体的に規定はしていない。**これは、**PF事業者のシステムの変化や技術の進歩があるためである。重要な焦点は、PF事業者がこれらの変化に適切に適応しているかどうかである。**例えば、3～5年前には、PF上での効果的なコンテンツモデレーションに5,000人の人員が必要であったが、今日では、AIの進歩により、コンテンツモデレーションに必要な人員がもっと少なくて済む可能性がある。こうした変化に対応することが不可欠。したがって、DSAにおいては、特定のツールや方法を指定するのではなく、取られた措置の有効性に焦点が当てられた。
- 一部のPF事業者は以前、法的解釈が十分に明確でないと主張していた。しかし、このフレームワークは、 PF事業者が、技術の発展を考慮して、提供するサービスに最も適した措置を取ることができるように、十分に柔軟であることを意図している。
- 欧州委員会は政治的中立性を維持しつつ、DSAを客観的かつ公平に執行する。DSAの執行にあたって、欧州委員会は、欧州司法裁判所を含む欧州裁判所の監督の下で活動する。したがって、**欧州委員会が下したいかなる決定についても、欧州裁判所においてPF事業者によって異議を申し立てられる可能性がある。**

※欧州委員会担当（DG CONNECT）から聞き取った内容について、NRIにおいて要約したもの。

Trusted Flaggerについて（欧州委員会担当（DG CONNECT）による聞き取り）

- **DSCは、その独立性を確保し、DSAの執行において客観的な決定を行う必要がある。**したがって、DSCは、公平、透明かつ適時に執行業務を遂行することが求められる。DSCは、その独立性に影響を与えないように、その管理において十分な自律性を有していなければならない。
- **欧州では、Trusted Flaggerの地位と活動は全く新しいものではない。**DSAが実施される前から、多くのPF事業者は、虐待、薬物、その他の違法コンテンツを発見するために、市民社会組織との協力枠組みをすでに確立していた。これらの市民社会活動は、多くの場合、財団、公的機関、またはPF事業者によって資金提供されている。PF事業者とTrusted Flaggerとの間の自発的な協力の経験に基づいて、DSAは現在の法的枠組みを提供している。
- Trusted Flaggerのガイドラインは、2025年の第2四半期に発表される予定である。DSA第22条に基づき、Trusted Flaggerは、専門知識を有し、 PF事業者からの独立性を維持し、その業務を厳格に実施することが求められる。また、年次報告書の公表も義務付けられているため、法律に定められた要件を満たさなくなった場合には、認定を取り消すことができる。
- PF事業者が公表した透明性レポートと透明性データベースによると、Trusted Flaggerからの通知の数は現在少ない。これは、昨年下半期に初めてTrusted Flaggerの認定を受けたため、制度の運用自体がまだ短いことや、一部の加盟国では認定していない場合もあるため。認定制度自体も、今後、さらに進むことが期待される。

※欧州委員会担当（DG CONNECT）から聞き取った内容について、NRIにおいて要約したもの。

４－２．英国におけるOSA （Online Safety Act ）の執行権限・体制

執行制度の概要

オンライン安全法Part7では、当局Ofcomの権限及び義務について定めている

	項目		条項
Part 1	イントロダクション・全体概要		第1条-2条
Part 2	用語の定義		第3条-5条
Part 3	ユーザ間サービスや検索サービスに課される義務	1章：イントロダクション	第6条
		2章：ユーザ間サービスの注意義務	第7条-23条
		3章：検索サービスの注意義務	第24条-34条
		4章：子供のアクセス評価	第35条-37条
		5章：不正広告に関する義務	第38条-40条
		6章：行動規範とガイダンス	第41条-54条
		7章：Part3の解釈	第55条-63条
Part 4	ユーザ間サービスや検索サービスに課される更なる義務	1章：本人確認	第64条-65条
		2章：子供の性的搾取と虐待に関するコンテンツの報告	第66条-70条
		3章：利用規約：透明性、説明責任、表現の自由	第71条-74条
		4章：死亡した子供の利用者	第75条-76条
		5章：透明性レポート	第77条-78条
Part 5	ポルノコンテンツを提供する事業者に課される義務		第79条-82条
Part 6	違反時の罰則（罰金）		第83条-90条

	項目		条項
Part 7	OFCOMの権力と義務	1章：一般義務	第91条-93条
		2章：規制対象となるユーザ間サービスおよび検索サービスのカテゴリー登録	第94条-97条
		3章：検索サービスの注意義務	第98条-99条
		4章：インフォメーション	第100条-120条
		5章：テロ・コンテンツおよびCSEAコンテンツに対処するための通知	第121条-129条
		6章：執行権限	第130条-151条
		7章：委員会、調査及びレポート	第152条-164条
		8章：メディアリテラシー	第165条-166条
Part 8	不服申し立てと苦情	1章：不服申し立て	第167条-168条
		2章：苦情	第169条-171条
Part 9	規制サービスに関する国務長官の機能		第172条-178条
Part 10	通信に関する犯罪		第179条-191条
Part 11	補足		第192条-225条
Part 12	解釈と最終規定		第226条-241条

https://www.legislation.gov.uk/ukpga/2023/50/contents/enacted
https://www.OFCOM.org.uk/__data/assets/pdf_file/0027/211986/understanding-online-false-information-uk.pdf

規制当局の体制等｜OSA

規制当局

OFCOMを独立した規制当局とする。

ガバナンス

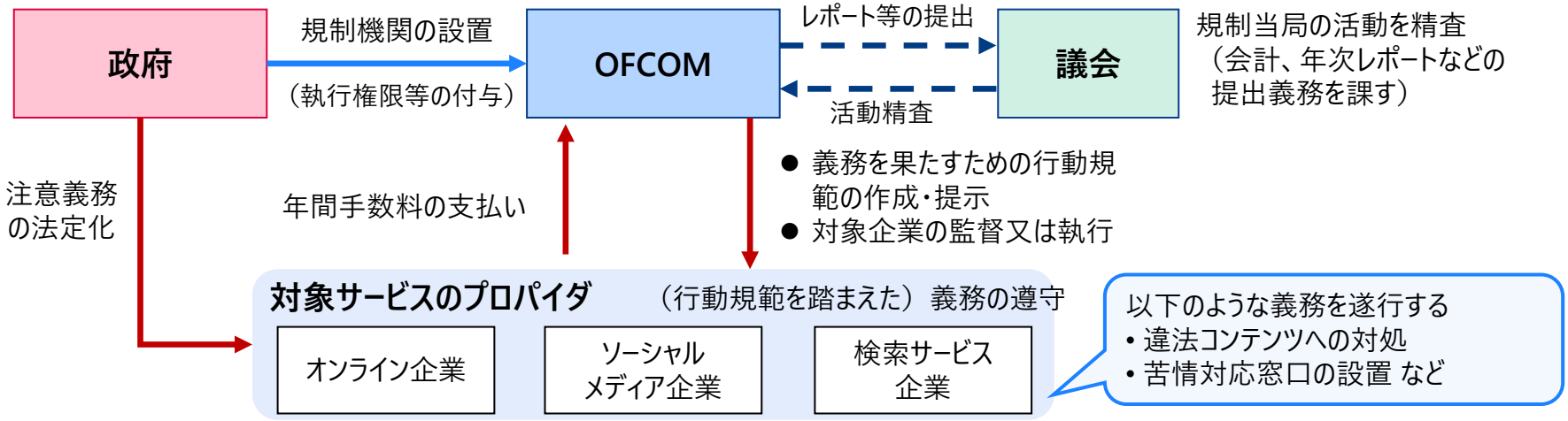
- 政府は、行動規範の作成や年間手数料の徴収に関する閾値の設定等、規制の政策意図を維持する手段を有する
- 国務大臣はOFCOMに対し以下の権限を有するが、運用上の問題に踏み込む等OFCOMの独立性を妨げることはしない
  - 規制の範囲や行使についての明確なガイダンス（議会で承認）を発行する
  - オンライン被害規制に関連した戦略的優先事項の声明（OFCOM等、関係者と協議を経る）を出す
  - OFCOM理事会のメンバーを選任する

議会への説明責任

- OFCOM は、年次レポートと決算書を議会に提出し、特別委員会の精査を受ける
- 国務大臣は、発効後 2～5 年後に制度の有効性の見直しを行い、レポートを作成して議会に提出する。議会は、レポートの調査結果について議論する機会を持つ

規制当局の活動資金

- **グローバルでの収益が一定の閾値以上の企業に対し、OFCOMへの届出と年間手数料の支払いを要求**
  - 閾値は、産業界との協議に基づきOFCOMが設定し、大臣の承認が必要
- 全企業が負担する手数料の総額は、オンライン被害規制の運営にあたりOFCOMが負担する費用に比例
- 個々の企業が支払うべき金額は以下の2つの指標に基づき算出
  - グローバルでの年間収益
  - 企業の活動（サービスにおける特定機能の有無などを勘案し、詳細はOFCOMが決定）



出所） Online Safety Act: explainer - GOV.UK、Guidance to the regulator about fees relating to the Online Safety Act 2023 - GOV.UK等よりNRI作成

OSA違反の疑いがある場合にはOfcomが調査を開始。違反仮通知の発出、サービス提供者の意見陳述を経て、なお義務違反と判断した場合には違反を確定する

	調査開始・情報収集	違反仮通知の発出	意見陳述	違反の決定
Ofcom	**以下等の権限を行使し、情報収集を実施** • 情報の要求（第100条） • インタビュー要求（第106条） • 立ち入り検査（第107条）	**•違反仮通知*のサービス提供者への通知**（第130条） •違反仮通知には、違反の内容や根拠などが記される	**•サービス提供者が意見陳述できる期間を設けることが義務付けられている**（第130条）	**• 確認決定のサービス提供者への通知**（第132条） • 確認決定には、違反があった旨およびその詳細な理由、サービス提供者に対して科される措置命令や罰金が具体的に指示される
サービス提供者	• -	• -	**• Ofcomの指摘に対する説明や訂正などを主張**（第130条）	• 確認決定に記載された要件に従う義務を負う（第132条）

出所）OSA条文を基にNRI作成　https://www.eu-digital-services-act.com/Digital_Services_Act_Articles.html
注）OSA法令で、違反仮通知=“provisional notice of contravention”、確認決定=“confirmation decision”とされている

Ofcomは、情報通知書発行・熟練者からのレポート要求等の情報収集権限を有する

Ofcomが有する情報収集権限の概要

a. **情報通知書の発行（第100条）**
- Ofcomがオンライン安全機能を行使する、または行使するかどうかを決定する目的で、特定の情報を求める通知発行することができる

b. **熟練者(Skilled person）からのレポートの要求（第104条）**
- Ofcomは、Ofcomを支援するために必要と判断した場合に、Ofcomに報告書を提供する熟練者（Skilled person）を任命することができる
- Skilled personとは、報告書を提出するのに必要な技能を持ち、Ofcomが指名または承認した人物

c. **面接への出席要求（第105、106条）**
- Ofcomが、規制対象サービスが関連要件を遵守していない、または遵守していない可能性について調査を開始した場合、Ofcomは面接を要求し、通知することができる

d. **立ち入り、検査、監査の権限行使者の許可（第107条）**
- 令状なしの立入検査
- 監査の実施
- 施設への立ち入り検査の令状申請・執行

e. **他の管轄規制当局と協力した情報共有（第114条）**
- 通信法（2003年）にもとづいた情報開示に関する一般的な制限を受ける一方で、同法の例外規定が適用される場合は情報提供者の同意なしに情報を開示することができる

出所） Online Safety Act 2023　等をもとにNRI作成

当局の執行権限｜OSA

Ofcomは、サービス提供者に対して違反仮通知を発出する権限を有する

Ofcomが有する違反仮通知発出の権利（第130条）

- Ofcomは、サービス提供者がOSA条項（131条に定めるもの）に違反したと合理的に信じるに足る理由がある場合、サービス提供者に対して、**違反仮通知を発出することができる。**
- 違反予備通知は以下を明示しなければならない。
  - A) 通知内容に関して、当該人物が**OFCOMに意見陳述（および関連する証拠の提出）を行うことができること**
  - B) そのような意見陳述が提出できる期間。

違反仮通知を発することができる、OSA上の条項（第131条）

条項	内容
第9条	違法コンテンツに関するリスク評価
第10条	違法コンテンツ
第11条	子どもに関するリスク評価
第12条	子どものオンライン安全
第14条	第15条(2)の義務に関連する評価
第15条	ユーザーの自律性の確保
第17条	民主主義的に重要なコンテンツ
第18条	ニュース発信者のコンテンツ
第19条	報道目的のコンテンツ
第20条	コンテンツの通報体制
第21条	苦情処理手続き
第22条	表現の自由およびプライバシー

条項	内容
第23条	記録の保存および見直し
第26条	違法コンテンツに関するリスク評価
第27条	違法コンテンツ
第28条	子どもに関するリスク評価
第29条	子どものオンライン安全
第31条	コンテンツの通報体制
第32条	苦情処理手続き
第33条	表現の自由およびプライバシー
第34条	記録の保存および見直し
第36条	子どものアクセス評価
第38条	詐欺的広告（1回目）
第39条	詐欺的広告（2回目）

条項	内容
第64条	ユーザーの本人確認
第66条	CSEA（児童性搾取・虐待）コンテンツのNCA（国家犯罪庁）への通報
第71条	サービス利用規約に基づくユーザー対応
第72条	サービス利用規約
第75条	死亡した子どものユーザーに関する情報
第77条	透明性レポート
第81条	プロバイダーが提供するポルノコンテンツ
第83条	OFCOMへの通知に関する手数料
第102条	情報通知に関する義務
第104条	有資格者への協力義務
第105条	調査への協力義務

出所） Online Safety Act 2023　等をもとにNRI作成

当局の執行権限｜OSA

Ofcomは、確認決定（confirmation decision）として、サービス提供者に措置の要請が可能。これを受けた場合、サービス提供者は要件に従う義務を負う

第133条「確認決定：措置の要請」

■ 確認決定（"confirmation decision"）によって、以下のいずれかまたは両方の目的のために、OFCOMが適切と考える措置（システムやプロセスの使用に関する措置を含む）を講じるよう要求することができる。

A) 通知された要件への準拠

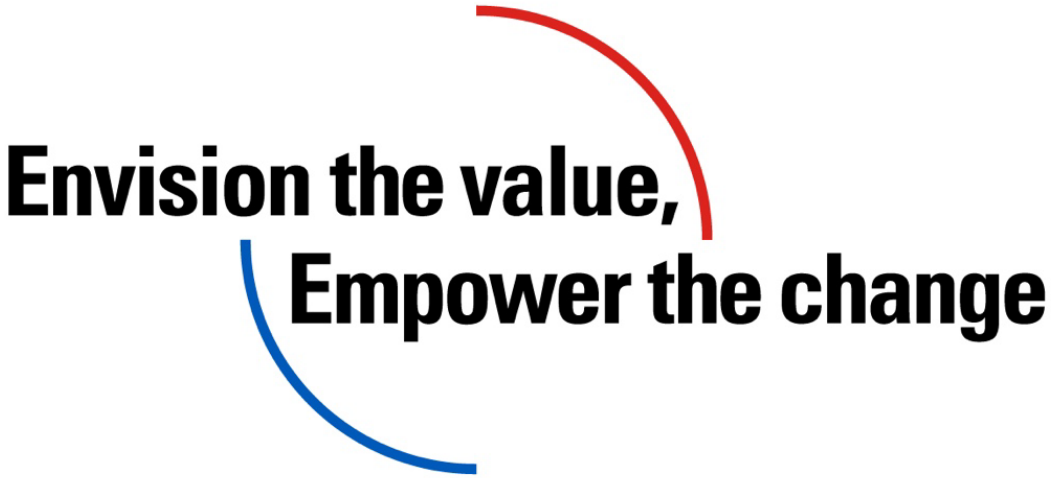
B) 通知された要件の不履行の是正

■ 確認決定には、以下の内容を明記しなければならない。

- 求められる措置の具体的内容
- その措置を課すことに関するOFCOMの決定理由
- それらの要件のうち、どれ（該当する場合）が「CSEA（子供の性的搾取・虐待）要件」として指定されたか
- 措置が関連する通知された要件の明記
- 通知された要件への不履行が発生していた期間、およびその不履行が継続しているか否か
- 各措置が実行されるべき合理的な期間、またはシステムやプロセスの使用が求められる場合には、それを開始すべき合理的な期間
- （該当する場合）そのシステムやプロセスが使用されるべき期間
- 第168条に基づく上訴権に関する詳細
- 決定に含まれる要件に従わなかった場合の結果（OFCOMが取りうる追加の執行措置に関する情報を含む）

■ **確認決定を受けた者は、その決定に含まれる要件に従う義務を負う。**

出所） Online Safety Act 2023　等をもとにNRI作成


Envision the value,
Empower the change