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２回）

未定稿

資料２－３

違法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2月28日

NRI

Envision the value,
Empower the change

目次

1．各国制度の概要

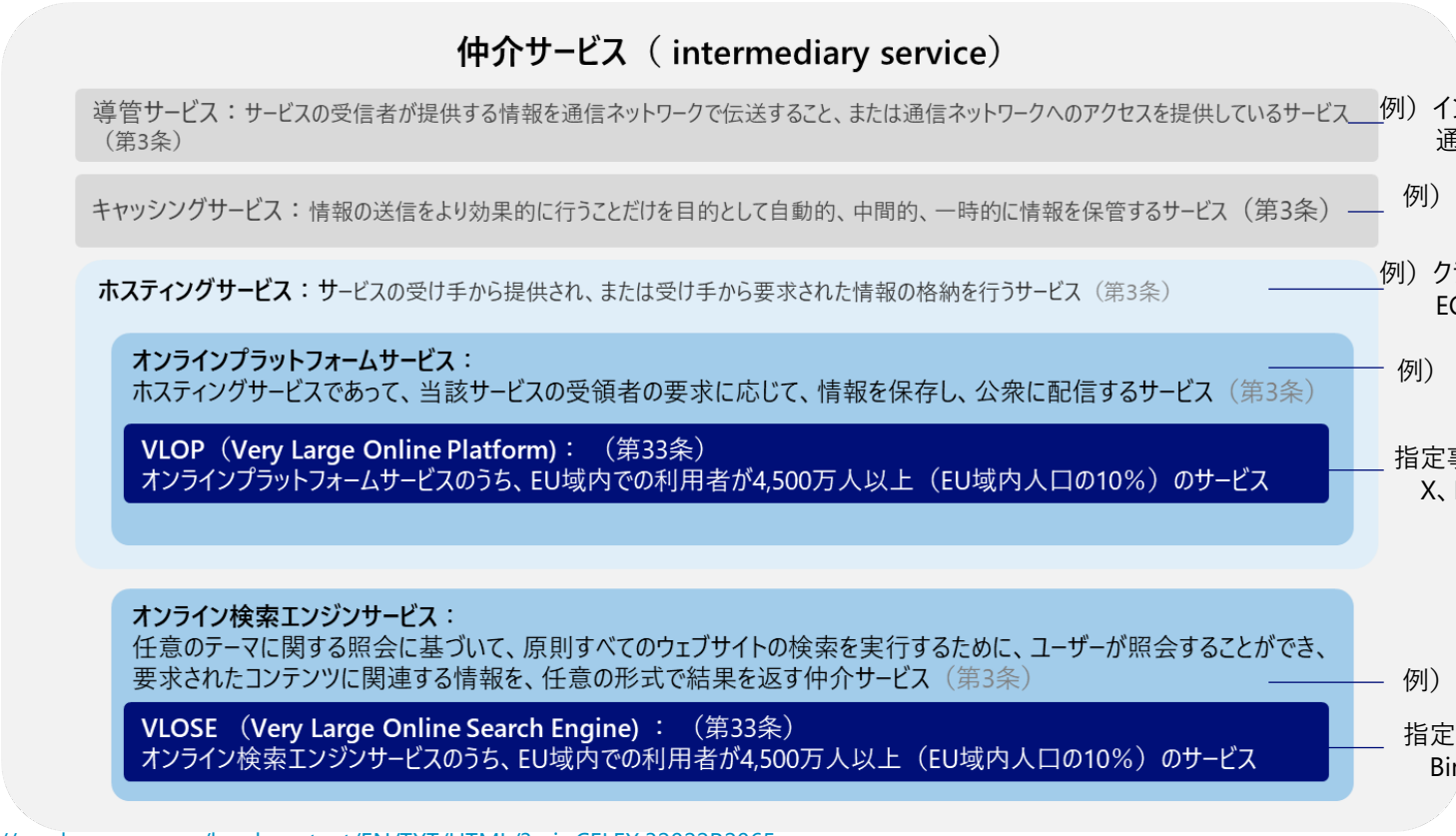
1．各国制度の概要（DSA・OSA）

項目	DSA（Digital Services Act）	OSA（Online Safety Act）
概要	• 2024年2月、EU加盟国内でデジタルサービス法が全面適用開始 • SNS等オンラインプラットフォームサービス事業者及び検索エンジンサービス等の仲介サービス等を提供する事業者に対し、違法コンテンツへの対応（行政当局への応答、削除申出への遅滞ない応答・通知等）やその運用状況の公表等の実施を義務付け。また、大規模オンラインプラットフォーム事業者等に対しては、上乗せでリスクを評価・軽減すること等を義務付け	• 2023年10月、英国においてオンライン安全法が成立（段階的に施行） • 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し、違法コンテンツへの対応（利用者からの容易な報告、迅速な削除のためのシステム・プロセス設計）やその運用状況の透明性報告書の作成を義務付け。また、ユーザー間サービス及び検索サービスに対し、違法コンテンツ又は子供に有害なコンテンツや活動によるリスクを評価・軽減すること等を義務付け
対象事業者	• SNS等オンラインプラットフォームサービス事業者、検索エンジンサービス事業者等の仲介サービス等を提供する事業者 ※EU域内に事務所が所在、または、域内の受領者に対してサービスを提供する事業者が対象 ※大規模オンラインプラットフォーム事業者（VLOP）及び大規模オンライン検索エンジン事業者（VLOSE）に対しては、最も広範な対応を義務付け	• 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 ※英国外から運営されている場合であっても、「英国との関連性を有する」サービスである限り、OSAを域外適用 ※大規模なユーザー間サービス事業者（カテゴリー1）に対しては、当該事業者に該当しない事業者（カテゴリー2）よりも、広範な対応を義務付け
対象違法情報	• EU法に反している情報またはEU法に準拠している加盟国の法律に反している情報	・テロリズムコンテンツ ・CSEA（子供の性的搾取・虐待）コンテンツ ・その他の「優先犯罪」に係るコンテンツ ・上記いずれにもその他の「優先犯罪」に係るコンテンツにも当てはまらないが、法に触れ個人に被害を与えるコンテンツ

1－1．EUにおけるDSA （Digital Services Act）の概要

制度の概要｜DSAの対象事業者

項目	内容	条項
対象事業者	● EU域内に事務所が所在する、または、域内に所在するサービスの受領者に対して仲介サービス（intermediary service）を提供する事業者 ● 仲介サービスを規模等で複数区分に分類し（下図参照）、サービスの社会的リスクに応じて提供事業者の義務を段階的に定める ● SNS事業者などのホスティングサービス事業者のうち大規模オンラインプラットフォームサービス事業者（VLOP）及び大規模オンライン検索エンジンサービス事業者（VLOSE）に対しては、最も広範な義務を課している	● 2条 ● 3条~6条 ● 33条



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

違法コンテンツの定義は、他のEU法や加盟国の国内法に委ねている。

	定義	情報に対する主な義務
違法コンテンツ （illegal content）	「違法コンテンツ」とは、それ自体または製品の販売やサービスの提供を含む活動に関連して、**EU法に反している情報またはEU法に準拠している加盟国の法律に反している情報**を意味する。（3条(h)） ※**加盟国の国内法に具体的な定義は任せている**が、前文12項ではDSAにおける認識と例が示されている。 「違法なヘイトスピーチやテロリストのコンテンツ、違法な差別的コンテンツなどそれ自体が違法であるもの、または違法な活動に関連しているという事実を考慮して適用規則が違法とみなす情報を指すものと理解されるべきである。例えば、児童性的虐待を描写した画像の共有、非合法で同意のない私的な画像の共有、オンラインストーキング、基準を満たさない製品や偽造品の販売、消費者保護法に違反した製品販売やサービス提供、著作権で保護された素材の無許可使用、違法な宿泊サービス提供、生きた動物の違法販売などがある。・・・（略）」（前文12項）	● 行政当局への応答、削除申出への遅滞ない応答・通知等（9条、10条） ● リスク評価・リスク軽減措置の実施（34条、35条）

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

（参考）DSAの各事業者カテゴリにかかる規定

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			●	●
レコメンダー 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				●
レコメンダー・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

1－2．英国におけるOSA （Online Safety Act）の概要

制度の概要｜OSAの対象事業者・対象違法情報

＜対象事業者＞

項目	内容
対象事業者	● 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。 ✓ **ユーザー間サービス** →ユーザーがコンテンツを作成して共有したり、相互にやり取りしたりできるSNSや動画共有サービス等のサービス（3条1項） ✓ **検索サービス** →ユーザーが他のウェブサイトやデータベースを検索できるサービス（3条4項） ● 「ユーザー間サービス」又は「検索サービス」については、それが英国外から運営されている場合であっても、「英国との関連性を有する」サービスである限り、英国オンライン安全法の域外適用があるとされる　（4条2項(a)） ● 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（※））に対しては、カテゴリー1サービス事業者に該当しない事業者（カテゴリー2サービス）よりも、広範な対応を義務付け ※）カテゴリ 1 サービス：コンテンツレコメンドシステムを有するサービスであって、次のいずれかの要件を満たす大規模なもの。 ①英国における平均アクティブユーザー数が3,400万人以上のサービス ②利用者生成コンテンツの転送又は再共有を利用者に可能とするサービスであって、英国における平均アクティブユーザー数が700万人以上のサービス

＜対象違法情報と当該情報に対する主な義務＞

項目	定義	情報に対する主な義務
違法コンテンツ（illegal content）	違法コンテンツとは、あらゆる種類の違法コンテンツを指す（59条） ・テロリズムコンテンツ（59条 2 項、4 項、10項） ・CSEAコンテンツ（59条 2 項、4 項、10項） ・その他の「優先犯罪」に係るコンテンツ（59条 2 項、4 項、10項、附則 7 ） ・上記いずれにもその他の「優先犯罪」に係るコンテンツにも当てはまらないが法に触れ個人に被害を与えるコンテンツ（59条 5 項）	● 認識した場合に迅速に削除すること等を目的として設計されたシステム・プロセスを使用してサービスを運用する義務（10条3項b） ● リスク評価・リスク低減措置の実施（9条、10条）

出所）Ofcom　https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/economic-discussion-papers-/understanding-online-false-information-uk.pdf?v=325850
https://www.ofcom.org.uk/__data/assets/pdf_file/0027/211986/understanding-online-false-information-uk.pdf

オンライン安全法はあらゆる種類の違法コンテンツを対象とするが、テロ等の優先犯罪に係る優先違法コンテンツは区別して把握し、よりプロアクティブな措置を講じることが求められている

- オンライン安全法は、あらゆる違法コンテンツを対象としている一方で、対象とする犯罪を「**優先犯罪**」（**priority offences**）と「その他の犯罪」に分類し、「優先犯罪」には、テロやCSEA（子供の性的搾取・虐待）等が含まれる。（59条）
- 上記の**優先犯罪に係るコンテンツを、「優先違法コンテンツ」**としている（59条）
- 違法コンテンツに対するリスク評価義務（9条）では、優先違法コンテンツ・その他の違法コンテンツを区別して把握することが求められており、安全義務（10条）では、**優先違法コンテンツに対しては存在やアクセス可能な時間を最小限にすること等**、よりプロアクティブな措置が求められている。

優先犯罪（priority offences）

1. テロ：terrorism
2. 子供の性的搾取・虐待：child sexual exploitation and abuse (CSEA)
3. 自殺ほう助：encouraging or assisting suicide
4. ハラスメント・ストーキング・脅迫・虐待：harassment, stalking, threats and abuse
5. 憎悪：hate
6. 家族関係等における支配的行動：controlling or coercive behaviour
7. ドラッグ：drugs and psychoactive substances
8. 銃器・武器：firearms and other weapons
9. 不法移民：unlawful immigration
10. 成人の性的搾取：sexual exploitation of adults
11. 極端なポルノ：extreme pornography
12. 親密画像の悪用：intimate image abuse
13. 犯罪による収益：proceeds of crime
14. 詐欺・金融サービス犯罪：fraud and financial services offences
15. 外国干渉：foreign interference
16. 人身売買：human trafficking
17. 動物虐待：animal cruelty

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

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

■ オンライン安全法の監督・執行は、Ofcomが担う。

- オンライン安全法の施行に際しては、**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サービス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 • 本資料で取り上げている義務では、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 • 本資料で取り上げている義務では、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

（参考）OSAにおける各事業者カテゴリにかかる規定

大規模サービスに対しては追加で義務がかかる

Part3「ユーザー間サービスや検索サービスに課される義務」 2章：ユーザー間サービスの注意義務

セクション	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 ※大規模で、かつコンテンツレコメンドシステムを有するサービス	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

２．違法情報に関する制度及び事業者の対応

2．違法情報に関する制度（DSA・OSA）

項目	DSA	OSA
①窓口の設置義務	＜サービス利用者＞ • 連絡窓口を整備することを義務付け（16条） ＜司法・行政当局＞ • 法的根拠に基づく命令に対しては専用窓口を設けることで、優先的に対応することを義務付け（9条、11条） ＜Trusted Flagger＞ • Trusted Flaggerからの通知に対しては専用窓口を設ける必要はないが、優先的に対応することを義務付け（22条）	＜サービス利用者＞ • 違法コンテンツに係る通知に対する窓口を設けることを義務付け（20条） ※ユーザーが違法コンテンツを容易に報告できるシステムを提供することも義務付け ＜Trusted Flagger（行政当局）＞ ※Trusted Flaggerとして、警察、その他の行政機関（労働年金省、国家犯罪庁等）を指定。 • 法律上規定はないが、行動規範において、詐欺に関するリスクの高いサービスについては、専用の報告窓口を設けることを推奨
②違法情報の判断基準	• 判断に係る具体的な基準は定めていない ※違法コンテンツの定義は、他のEU法や加盟国の国内法に委ねていることから、判断基準についても他のEU法や加盟国の国内法に委ねていると推察される。	• 一般的な違法コンテンツについて、判断に係る具体的な基準は定めていない • 違法コンテンツのうち、テロや児童の性的搾取・虐待等の「優先犯罪」に係るコンテンツについて、Ofcomが「違法コンテンツ判断ガイダンス」を発行し、判断方法を提示
③違法情報の措置方法	• 違法コンテンツに対して個人または団体が容易かつ電子的に報告できる仕組み（mechanisms）を導入し、報告された情報についての決定を遅滞なく当該報告者に通知し（16条）、削除等の措置を講じる際は、措置を決定したこと及び決定に至った理由を説明することを義務付け（17条） • なお、削除等の具体的な措置方法は指定していない	• 一般的な違法コンテンツについて、ユーザーから存在を通知された場合、または存在を認識した場合に迅速に削除すること等を目的として設計されたシステム・プロセスを使用してサービスを運用することを義務付け（10条3項(b)） • 優先違法コンテンツ（テロやCSEAコンテンツ等）について、上記に加え、存在する期間を最小限に抑えるために適切なシステム・プロセスを運用すること等を義務付け（10条3項(a)）
④異議申立て方法	• ユーザーがオンライン上で無料で利用可能な異議申立手続を提供することを義務付け（透明性についての言及はなし）	• ユーザーが利用しやすく、透明性のある異議申立手続を提供することを義務付け（無料であるかどうかの言及はなし）

２－１．　DSA：違法情報に関する制度及び事業者の対応

ホスティングサービス提供者に対して、利用者が違法なコンテンツの通報を行った場合に、その通報内容を迅速かつ公正に判断し、必要な対策を講じることを義務付け。

- 第16条では、ホスティングサービス提供者は、個人または団体が違法コンテンツであると考える特定の情報がホスティングサービス上に掲載されていることについて、個人または団体に対して容易かつ電子的に通報できる仕組み（mechanisms）を導入を義務付けている。
- ホスティングサービス提供者は、通報に基づく決定を遅滞なく通報者に伝え、決定に関する救済手段についての情報を提供する義務を負う。

項目	【第16条】
通報システムの導入義務（1項）	• 事業者は、違法コンテンツの通報を受け付ける仕組みを設け、電子的手段で簡単に通報できるようにする。
通報の要件（2項）	• 通報が適切で正確なものとなるよう、以下の情報を含める必要がある。 ➢ 違法とする理由の説明 ➢ コンテンツの正確なURL ➢ 通報者の氏名とメールアドレス ➢ 通報内容が正確であることを確認する覚書
違法性の認識（3項）	• 通報内容が明確であり、追加の法的調査をせずに違法性を特定できる場合、事業者は違法性を認識したものと見なされる。
受領確認の通知（4項）	• 通報者の連絡先がある場合、事業者は速やかに受領確認を通知する。
決定の通知と救済手段の提供（5項）	• 事業者は、通報に基づく決定を遅滞なく通報者に伝え、決定に関する救済手段についての情報を提供する。
通報の適切な処理（6項）	• 事業者においては、通報の違法性判断および通報に基づく決定について、適時かつ慎重に、恣意的でない客観的な方法で行う。

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

ホスティングサービス提供者がコンテンツの削除やアクセス無効化、金銭的支払の停止等の措置を取った場合、その理由、根拠、救済手段等について、その発信者に対して明確かつ具体的に説明することを義務付け。

■ 第17条では、ホスティングサービス提供者が、(a)サービスの受け手（recipients）から投稿された特定のコンテンツを削除あるいはアクセス無効化する、(b)金銭的支払の停止、終了または制限、(c)サービス提供の全面的又は一部停止または終了、(d)アカウントの停止または終了にあたっては、これらの措置を講ずるよりも前に、措置を決定したことと、決定に至った理由について、サービスの受け手に説明しなければならない、とされている。

項目	【第17条】
通知理由の提供義務（1項）	• 事業者は、利用者が提供した情報が違法なコンテンツである、または利用規約に反すると判断された場合で、たとえば、コンテンツの削除、アクセスの無効化、金銭的支払の停止、サービスやアカウントの停止などの制限措置を課すときは、影響を受ける利用者に対して、その制限措置を講じた理由を明確かつ具体的に説明しなければならない。
適用条件（2項）	• この理由説明の義務は、該当する連絡先が既に事業者に知られている場合にのみ適用される。制限措置が課された日以降、速やかに理由説明が行われるものとする。
理由説明に含まれる情報（3項）	• 理由説明には、少なくとも以下の情報が含まれる必要がある。 (a) 決定が情報の削除、アクセス無効化、順位低下、または可視性の制限、金銭的支払の停止等の措置を伴うかどうか、ならびにその決定の適用範囲と期間。 (b) 決定の根拠となる事実や状況、通報に基づいて決定されたのか自主的な調査によるのか、必要な場合には通報者の身元情報。 (c) 必要に応じ、決定に際して自動化手段が使用されたかどうか、その利用状況。 (d) 決定が違法なコンテンツに関する場合、依拠した法的根拠と、その根拠により情報が違法と判断される理由。 (e) 決定が利用規約との不適合に基づく場合、依拠した利用規約上の根拠と、その根拠により情報が不適合と判断される理由。 (f) 利用者が救済措置（内部苦情処理、裁判外紛争解決、司法救済など）を受けるための、明確かつ利用しやすい情報。
情報の明確性及び具体性（4項）	• 提供される理由説明は、誰にでも理解しやすく、状況に応じて可能な限り明確かつ具体的である必要がある。これにより、該当する利用者が効果的に救済措置を行使できるようになる。
適用除外（5項）	• 本条は、第9条に基づく措置命令については適用されない。

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

オンラインプラットフォーム事業者に対して、利用者が不服申立てを行うための内部苦情処理体制を提供し、迅速かつ公正に処理することを義務付け。

- 第20条「内部苦情処理体制」はオンラインプラットフォーム事業者に関する追加規定として明記されている。
- 第20条では、オンラインプラットフォーム事業者は、通報を受けた情報が違法コンテンツまたは利用規約違反であることを理由として下した決定に対して、少なくとも6ヶ月間は通報を提出したサービス受領者に対し、電子的かつ無料で苦情を申し立てることができる効果的な内部苦情処理システムへのアクセスを提供しなければならない、とされている。

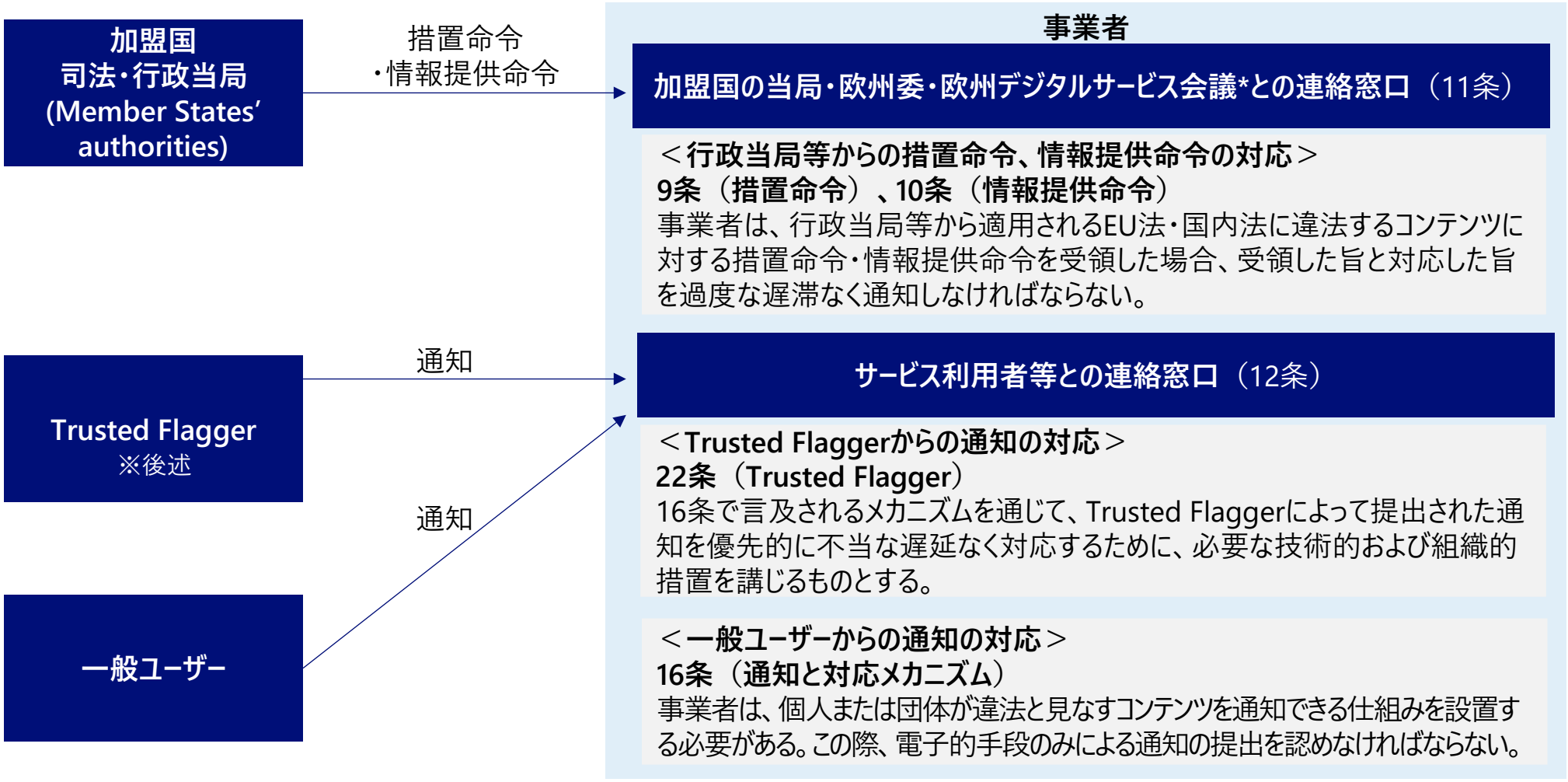
項目	【第20条】
内部苦情処理システムの提供義務（1項）	• 事業者は、サービス利用者（通知を提出した個人または団体を含む）に対し、決定後少なくとも6か月間、電子的かつ無料で苦情を申し立てることができる効果的な内部苦情処理システムへのアクセスを提供しなければならない。 【対象となる決定】 情報の削除や可視性の制限、サービス提供の一時停止や終了、アカウントの一時停止や終了、収益化機能の制限　等
苦情受付期間の開始日（2項）	• 上記の6か月の期間は、利用者が第16条第5項または第17条に基づき決定の通知を受けた日から開始する。
内部苦情処理システムへのアクセスの確保（3項）	• 内部苦情処理システムが容易にアクセスでき、ユーザーフレンドリーであり、十分に具体的かつ適切な根拠を持つ苦情の提出を可能かつ促進するものであることを確保しなければならない。
苦情処理手続（4項）	• 提出された苦情は、適時、公平、注意深くかつ恣意的でない方法で処理されなければならない。苦情に十分な根拠がある場合、提供者は速やかに当初の決定を取り消す義務を負う。
決定の通知義務（5項）	• 事業者は、苦情提出者に対し、該当情報に関する理由を示した決定と、第21条に規定される裁判外紛争解決および他の救済手段の可能性について、遅滞なく通知しなければならない。

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

①DSAにおける命令・通知の窓口整備義務

事業者に対し、当局とサービス利用者向けの連絡窓口をそれぞれ整備するとともに、当局からの命令およびTrusted Flagger(後述)・一般ユーザーからの通知への対応を義務付け

DSAにおける命令・通知の扱い（条文は一部抜粋）



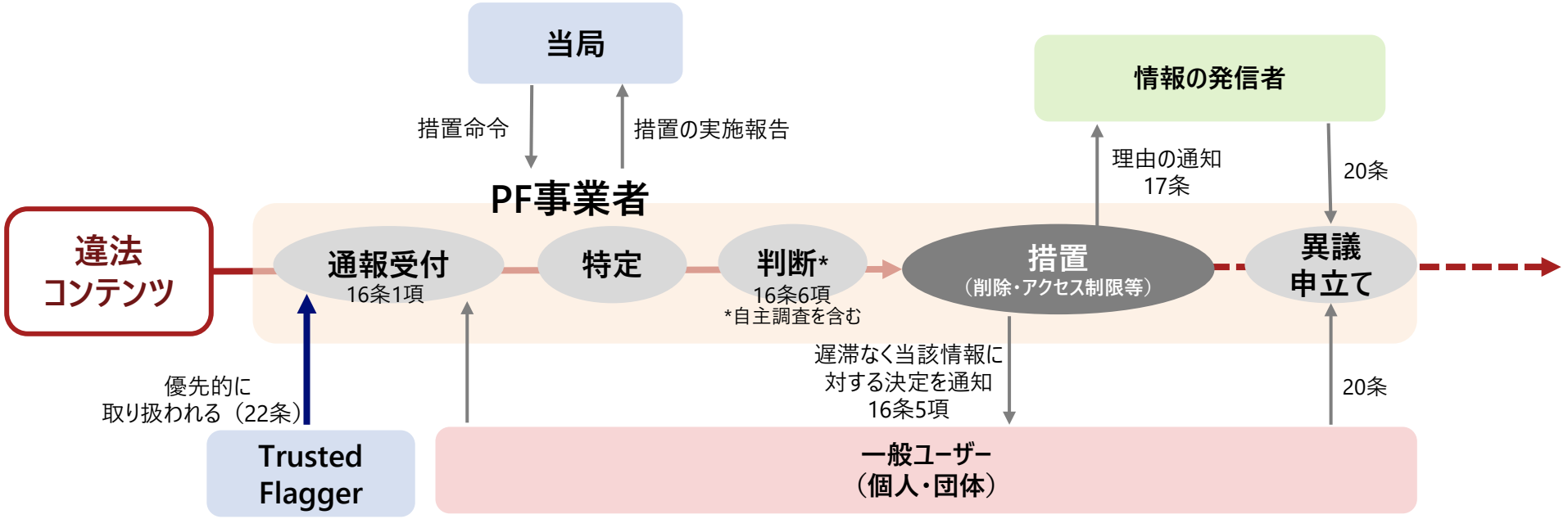
出所）DSA条文を基にNRI作成

*欧州デジタルサービス会議：DSA61条で定められている独立した諮問機関

DSAでは、PF事業者に対して違法コンテンツに関する命令・通知への対応や、ユーザーからの異議申立て等の仕組みの整備を義務付けている

■ DSAでは、PF事業者に対して違法コンテンツに関する司法・行政当局からの命令およびユーザー・Trusted Flaggerからの通知への対応や、ユーザーからの異議申立て等の仕組みの整備を義務付けている。

＜措置を行う場合の対応フローのイメージ＞

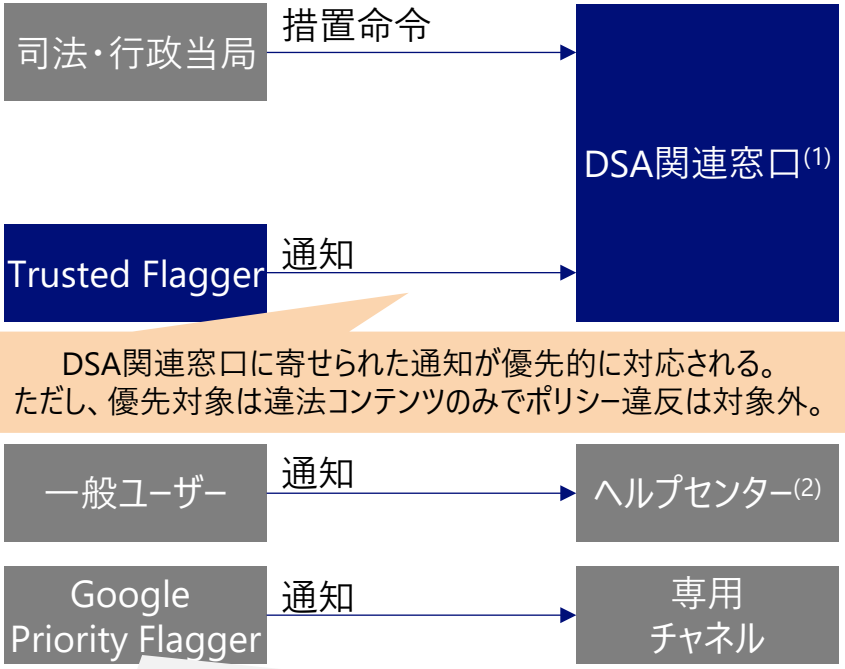


出所）DSA条文　https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2065

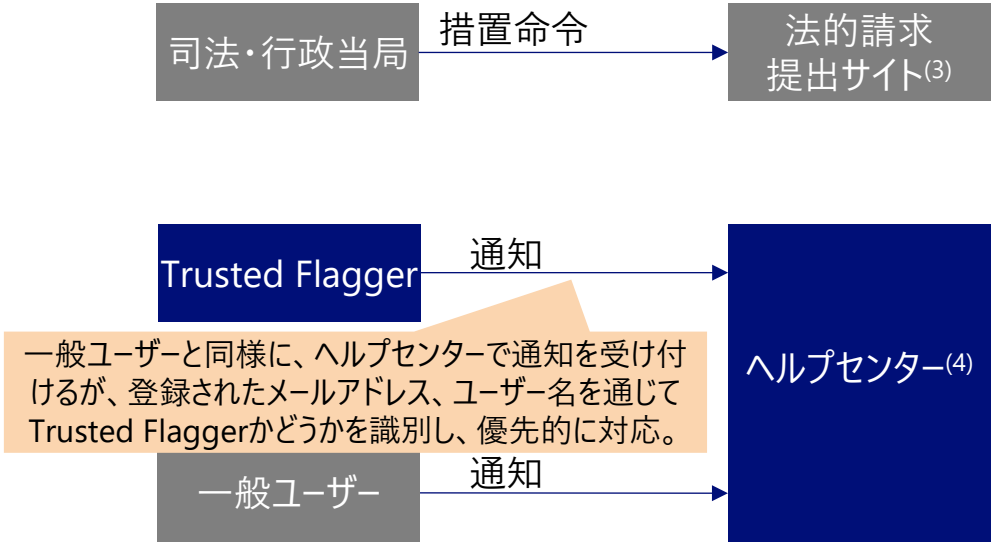
当局からの法的根拠に基づく措置命令に対しては専用窓口を設けることで優先的に対応を義務付け また、Trusted Flaggerからの通知は、優先的に対応を義務付け

＜事業者の取組例＞

Googleにおける措置命令・通知の窓口



Xにおける措置命令・通知の窓口



(1) https://support.google.com/legal/troubleshooter/13966113
(2) https://support.google.com/?hl=ja
(3) https://legalrequests.twitter.com/forms/landing_disclaimer
(4) https://help.x.com/en/rules-and-policies/european-union

TikTokへの当局からの措置命令のうち、ドイツ当局からの命令が最も多く約4割を占める。また、種類別ではテロ犯罪に関するコンテンツへの措置命令が最も多くおよそ半分である

当局・種類別の命令の数	子供の性的搾取	テロ犯罪	ヘイトスピーチ	暴力犯罪/組織犯罪	プライバシー侵害	画像の非同意共有	違法商品/サービス	嫌がらせ/脅迫	名誉毀損	消費者関連犯罪	情報関連犯罪/法廷侮辱罪	金融犯罪	国家安全保障関連の犯罪	その他	合計
オーストリア														3	3
ベルギー						1									1
ブルガリア								1							1
キプロス															0
チェコ															0
ドイツ		172	19	2	1			2						24	**220**
デンマーク		1	3		1										5
エストニア					1		1							2	4
スペイン		31												2	33
フィンランド															0
フランス		71	45	4	7		18	8				1		10	164
ギリシャ														1	1
クロアチア															0
ハンガリー			1					2						1	4
アイルランド					2		1	2			2			2	9
イタリア	1				2	11		2						9	25
リトアニア															0
ルクセンブルグ															0
ラトヴィア														1	1
マルタ															0
オランダ		2		1	1			2						2	8
ポーランド											1			2	3
ポルトガル															0
ルーマニア			1					28			14			8	51
スウェーデン														18	18
スロベニア															0
スロバキア								1			2			2	5
合計	1	**277**	69	7	15	12	20	48	0	0	19	1	0	87	556

ドイツ当局が全体の39.5%

テロ犯罪関連が全体の49.8%

TikTok: https://sf16-va.tiktokcdn.com/obj/eden-va2/zayvwlY_fjulyhwzuhy[/ljhwZthlaukjlkulzlp/DSA_H2_2024/TikTok-DSA-Transparency-Report-Jan-to-Jun-2024.pdf

①窓口の設置義務｜ 信頼できる第三者機関（Trusted Flagger制度）

DSAでは、Trusted Flaggerの条件として「専門性」、事業者からの「独立性」、判断への「客観性」があることや、EUに拠点を置く団体であることを挙げている

- Trusted Flaggerは、違法コンテンツを検出し、事業者に警告する責任を負う専門家であり、**DSAにおける戦略の重要な部分を担う特別な組織**である。
- Trusted Flaggerによって提出された通知は、**一般ユーザーによって提出された通知よりも正確であることが期待されるため、優先的に扱われなければならない**。
- Trusted Flaggerは、設立地域に関係なくDSA第22条の範囲内の事業者に対して、**EU全域で有効**である。

欧州委員会が公表しているTrusted Flaggerの条件

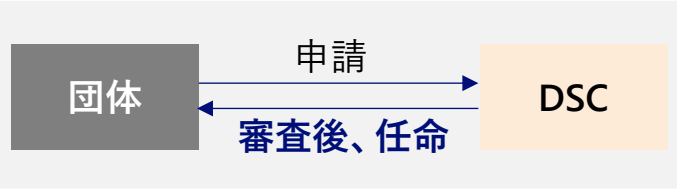
- ✓ DSC（※）は申請プロセスを監督し、団体が以下の基準を満たしていることを確認する必要がある。（22条）
  - ✓ (a) 違法コンテンツの検出、特定、通知を目的とした**特別な専門知識と能力を有する**こと
  - ✓ (b) **プラットフォーム提供事業者から独立**していること
  - ✓ (c) 通知を提出する目的で、**真摯に、正確かつ客観的に活動を実施**していること
- ✓ Trusted Flaggerの地位を申請できるのは、**EUに拠点を置く団体**のみ（22条）
  - ✓ 非政府組織、民間または準公的機関、業界団体などと規定されており、**個人は不可**。（前文61項）
- ✓ メカニズムの付加価値を低下させないように、**Trusted Flaggerの総数は制限**されるべきである。（前文61項）

（※）DSC：EU加盟国ごとにDSAの適用および執行責任を所管する組織

出所）欧州委員会「Trusted Flagger under the Digital Services Act (DSA)」 https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa

Trusted Flaggerの具体的な審査基準については、今後、欧州委員会がガイドラインを公表予定。希望団体からの申請について、各国のDSCが審査のち任命を行う（一部の国では先行してガイドラインを策定し、任命）

- Trusted Flaggerの地位を希望する団体は申請を提出し、**当該団体の設立国のDSCが要件について審査し、任命する。**
- 欧州委員会は、Trusted Flaggerの下記に関する審査基準についてのガイドラインを準備しており、2025年1Qに**パブリックコンサルテーションが予定**されている（※１）。



DSC：EU加盟国ごとにDSAの適用および執行責任を所管する組織
他の**行政当局や民間主体からの完全な独立をもって権限を行使**するものとされる（50条２項）

（参考）先行してガイドラインを策定した例
Comisiún na Meán （アイルランドのDSC）が提供するTrusted Flaggerに関するガイドライン（※２）

付与の対象となりうる組織
- ✓ 産業連盟や業界団体：知的財産所有者団体
- ✓ NGO：消費者権利団体、児童保護団体、人権団体、環境保護団体、動物権利団体、環境保護団体、動物保護団体など
- ✓ 確立されたファクトチェッカー・ネットワークのメンバー：IFCNなど
- ✓ 労働組合
- ✓ 規制対象外の公的機関：Europolまたは規制機関（DSCを除く）
- ✓ 民間または半公共団体：ホットラインのINHOPEネットワークの一部組織など

※DSA前文61項で、Trusted Flaggerは非政府組織、民間または準公的機関、業界団体などと規定されている。（個人は不可）

付与の対象となりうる違法コンテンツのリスト（15個）
- ✓ 動物に対する犯罪
- ✓ データ保護とプライバシー侵害
- ✓ 違法な発言
- ✓ 知的財産権およびその他の商業上の権利の侵害
- ✓ 市民の議論や選挙への悪影響
- ✓ 同意のない行為
- ✓ ネット上のいじめ・脅迫
- ✓ ポルノや性的コンテンツ
- ✓ 未成年者に対する犯罪
- ✓ 公共の安全に対するリスク
- ✓ 詐欺や不正行為
- ✓ 自傷行為の煽動
- ✓ プラットフォーム/コンテンツへのアクセス範囲の違法性
- ✓ 安全でないまたは違法な製品
- ✓ 暴力

（※１）欧州委員会「Trusted Flagger under the Digital Services Act (DSA)」 https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa
（※２） https://www.cnam.ie/app/uploads/2024/02/20240216_Article22_GuidanceForm_Branded_vF_KW.pdf

フィンランドのDSCであるTraficom公表のガイドラインでは、Trusted Flaggerとなる際の申請時に提示すべき情報として、「専門性」、「独立性」、「中立／客観性」を示している。

専門性

- ✓ どのような違法コンテンツを検知・識別する資格を有しているか。またその資格をどのように取得したかの説明
- ✓ 過去の違法コンテンツの検知・通報活動から得られた報告書、統計、その他類似の文書
- ✓ 違法コンテンツの検知、評価、通報に関連する内部手続きやプロセスの説明や文書
- ✓ 職員に要求される訓練または能力、および職員の能力を維持するための措置の説明
- ✓ オンラインコンテンツに関する経験がない場合、ネットワーク外の違法行為を防止するために講じた、または試みた措置の説明

独立性

- ✓ スタッフの選考手順
- ✓ スタッフの独立性の確保方法
- ✓ 資金調達構造、特にオンラインプラットフォームからの資金調達有無と、組織の総資金に占めるその割合（プラットフォーム別）

中立／客観性

- ✓ 違法コンテンツを検知・評価し、十分正確で間違いのない通知活動を行うためのスタッフの数と専門知識の確保方法
- ✓ 違法コンテンツが疑われる場合の通報手続きの説明
- ✓ これまでの違法コンテンツの通報活動の経験と証明：違法コンテンツに対する誤りのない通報数、通報の有効性（通報の結果および誤った通報を修正するための手順）

https://www.traficom.fi/en/communications/data-economy-and-digital-services/trusted-flaggers?toggle=Expertise&toggle=Independence&toggle=Trusted%20flaggers%20approved%20by%20Traficom&toggle=Carefulness

（参考）①窓口の設置義務｜ Trusted Flaggerの任命状況（2025年2月5日現在）

2024年5月以降、各国のDSCによって16の団体がTrusted Flaggerに任命されている

#	登録日（最新順）	機関名	国	専門分野
1	**2024年12月10日**	CropLife Lietuva	リトアニア	違法製品
2	**2024年11月12日**	Internet Hotline	ハンガリー	-
3	**2024年11月6日**	e-Enfance (3018)	フランス	サイバー暴力、データ保護とプライバシー侵害、違法製品、違法言論、未成年者保護違反、公共の安全に対するリスク、詐欺、暴力
4	**2024年11月5日**	Ίδρυμα Τεχνολογίας και Έρευνας Foundation for Research and Technology – Hellas	ギリシャ	-
5	**2024年11月5日**	DIGITAT ΔΙΑΔΙΚΤΥΑΚΗ ΕΝΗΜΕΡΩΣΗ Ο.Ε.	ギリシャ	-
6	**2024年11月4日**	Institutul Național pentru Studierea Holocaustului din România "Elie Wiesel"	ルーマニア	違法言論
7	**2024年10月2日**	Organizația Salvați Copiii	ルーマニア	未成年者の保護違反
8	**2024年10月1日**	Stiftung zur Förderung der Jugend in Baden-Württemberg – Meldestelle REspect!	ドイツ	-
9	**2024年8月27日**	Österreichisches Institut für angewandte Telekommunikation	オーストリア	知的財産権侵害、詐欺、不正行為
10	**2024年8月14日**	RettighedsAlliancen	デンマーク	知的財産の侵害
11	**2024年7月8日**	ECPAT Sweden	スウェーデン	子供の性的搾取
12	**2024年6月21日**	RAT auf Draht gemeinnützige GmbH<	オーストリア	未成年者の保護と子供の権利
13	**2024年6月18日**	Somis Enterprises Oy	フィンランド	サイバー暴力、違法言論、未成年者保護違反、詐欺
14	**2024年6月18日**	Pelastakaa Lapset ry	フィンランド	未成年者の保護違反
15	**2024年5月23日**	Schutzverband gegen unlauteren Wettbewerb	オーストリア	産業所有権
16	-	Tekijänoikeuden tiedotus- ja valvontakeskus ry	フィンランド	知的財産の侵害

出所）欧州委員会「Trusted Flagger under the Digital Services Act (DSA)」（2025年2月5日現在） https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa

（参考）①窓口の設置義務｜ Trusted Flaggerの財政基盤（2025年2月5日現在）

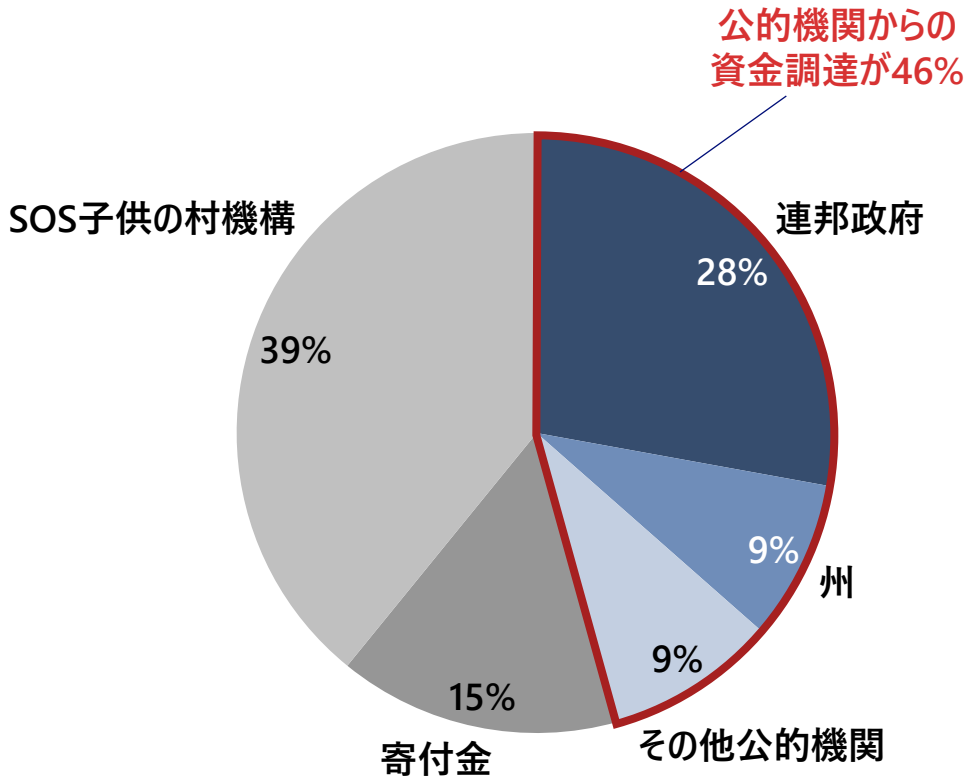
Trusted Flaggerの大半はNPOなどの市民団体。公的機関から資金を調達しているものもある

#	団体名	国	団体種別	主な財政基盤	活動概要
1	CropLife Lietuva	リトアニア	-	-	持続可能な作物生産を推進し、公共の利益を保護するCropLife Europeのメンバー。
2	Internet Hotline	ハンガリー	政府団体	国立メディア通信局	国立メディア通信局 (NMHH) が 運営するインターネット情報および支援サービス。
3	e-Enfance (3018)	フランス	**一般社団法人**	-	2005年に設立され、教育省から認可を受けている。 嫌がらせやデジタル暴力を受けた若い被害者/目撃者を支援している。
4	Ίδρυμα Τεχνολογίας και Έρευνας Foundation for Research and Technology – Hellas	ギリシャ	-	-	2003年に開始したネット上の違法コンテンツを報告するための唯一のホットライン。 INHOPE（ホットラインの国際的な連合組織）の正式メンバー。
5	DIGITAT ΔΙΑΔΙΚΤΥΑΚΗ ΕΝΗΜΕΡΩΣΗ Ο.Ε.	ギリシャ	-	-	ギリシャで活動するファクトチェック組織。 IFCN、EFCN（国際/EU内の国際ファクトチェッカー団体）のメンバー。
6	Institutul Național pentru Studierea Holocaustului din România "Elie Wiesel"	ルーマニア	国立研究所	-	2005年政府決定第902号によって設立され、ルーマニアのホロコースト研究を行う。
7	Organizația Salvați Copiii	ルーマニア	**非営利法人**	寄付等	1990年以来ルーマニアで子供の権利を擁護し促進している。
8	Stiftung zur Förderung der Jugend in Baden-Württemberg – Meldestelle REspect!	ドイツ	**私立財団**	**家庭庁**	若者のプロジェクトをサポートし、革新的な青少年教育プログラムを開発する財団。
9	Österreichisches Institut für angewandte Telekommunikation	オーストリア	-	-	人々や組織がデジタル世界の利点をより有効に活用できるよう支援する企業。
10	RettighedsAlliancen	デンマーク	-	-	インターネット上のクリエイティブ産業に良い条件を作り出す利益団体。 経済的枠組みと条件を決定づけている。
11	ECPAT Sweden	スウェーデン	**NGO**	**国立保健福祉庁**、寄付	子供の性的虐待を阻止し、防止するために活動する子供の権利団体。
12	RAT auf Draht gemeinnützige GmbH<	オーストリア	**非営利法人**	**省庁**、寄付等	緊急電話番号147を通して危機的状況にある若者を支援する団体。 年間約55,000件の依頼を受けている。
13	Somis Enterprises Oy	フィンランド	-	-	困難な状況への支援を提供する全国的なハラスメント応急処置ユニットを運営する。
14	Pelastakaa Lapset ry	フィンランド	**非営利法人**	寄付、**フィンランド社会保健団体支援センタ**等	子供たちの生活に即時かつ永続的な変化をもたらす活動をする。
15	Schutzverband gegen unlauteren Wettbewerb	オーストリア	-	-	-
16	Tekijänoikeuden tiedotus- ja valvontakeskus ry	フィンランド	**非営利法人**	**フィンランド教育文化省**	コンテンツの違法な制作や配布などの著作権侵害を防止することを目指して活動する。

出所）欧州委員会「Trusted Flagger under the Digital Services Act (DSA)」（2025年2月5日現在） https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa
各団体HP

オーストリアのTrusted Flaggerの１つであるRAT auf DrahtはPF事業者からの資金提供は受けていない一方、連邦政府などの公的機関からの資金調達が全体の46%を占める

RAT auf Draht（オーストリア）の収入構造



総収入は約2億6,800万円
（1,718,868.03ユーロ）
※ 1ユーロ＝155.9円で換算

出所）RAT auf Draht 2023年通期決算報告書を基にNRI作成
https://www.rataufdraht.at/getmedia/626a759c-2db8-418f-8787-56856173f850/RaD_Jahresbericht2023-webversion.pdf

（参考）①窓口の設置義務｜ Trusted Flaggerの運用における課題

運用課題として「リソースの制約」、「世間の誤った認識」、「普及率の低さ」が挙げられている。

■ 2024年11月のCDT（Center for Democracy & Technology）とEU DisinfoLabによるウェビナー(1)では、Trusted Flagger制度に関する課題が指摘された。

- 欧州委員会、DSC、Trusted Flagger、申請を希望する団体など、30名を超える様々な関係者が参加。

#	課題	課題の詳細
1	リソースの制約	● **Trusted Flaggerの申請が多い市民団体は、リソース面での大きな制約に直面**している。EUの助成金の中には特定のセクターを支援するものもあるが、より**広範な資金調達メカニズムが必要**である。 ● 持続的な財政基盤なしには、コンプライアンスに必要なインフラや、増大する業務量を処理するための**人的リソースを確保できない**。
2	世間の誤認識	● Trusted Flaggerが**違法コンテンツではなく、不都合なコンテンツを処理していると懐疑的な見方**が多い。 ● Trusted Flaggerに関する誤った情報の拡散は、信頼性に対する真の脅威となる。 ● Trusted Flaggerの役割を明確に定義した、**積極的な広報戦略の策定が不可欠**である。
3	普及率の低さ	● 申請者側の参加障壁として、**負担の大きい要件、明確なプロセスの欠如、具体的なメリットの不明瞭さ**が指摘された。 ● 申請手続きには時間がかかり、専門性・独立性・客観性を証明するための膨大な文書が必要である。 ● **DSC、Trusted Flagger、申請希望者の協力と知識の共有を促進するための正式なワーキンググループ**が必要。 ● ベルギーなど一部の加盟国ではDSCが任命されておらず、申請手段が無いことが課題(2)となっている。

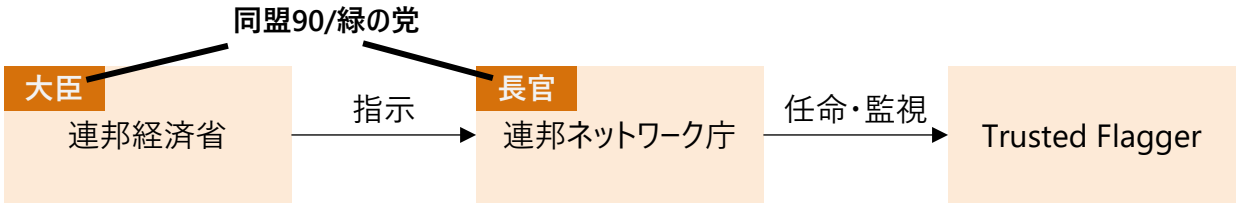
(1) https://cdt.org/insights/trusted-flaggers-in-the-dsa-challenges-and-opportunities/
(2) https://www.techpolicy.press/europes-digital-services-act-where-are-all-the-trusted-flaggers/

欧州議会において、「Trusted Flaggerの任命におけるDSCの政治的な選好の影響」について質問された。欧州委は、DSCはDSAに基づき政府・政党からの完全な独立が要求されると回答

REspect!への質問と回答：①任命プロセスの政治的中立性

Trusted Flagger任命の現状

- **Trusted Flaggerの任命と監視は連邦ネットワーク庁（ドイツのDSC）によって行われる。**
- **連邦ネットワーク庁は連邦経済省の権限と指示の下で活動している。**
- **本省大臣と連邦ネットワーク庁長官は、同盟90/緑の党のメンバーである。**



欧州議会での質問
2024年10月14日

Christine Anderson議員
Petr Bystron議員

Trusted Flaggerの任命が行政機関の政治的な意向に左右されないことは、どのようにして保証されるのか?

欧州委員会の回答
2024年11月27日

Margrethe Vestager執行副委員長

Trusted Flaggerの地位は、申請者がDSA第22条のすべての条件を満たしている場合に各国のDSCによって付与される。また、DSCの要件を定めるDSA第50条では、各国のDSCに対し政府や政党からの完全な独立が求められている。

出所）
(1) 質問 https://www.europarl.europa.eu/doceo/document/E-10-2024-002057_EN.html
(2) 回答 https://www.europarl.europa.eu/doceo/document/E-10-2024-002057-ASW_EN.html

欧州議会において、「REspect!の公的資金への依存」に関して中立性の観点から質問された。欧州委は、独立性・客観性等を損なわない限り公的資金に依存することは問題ないと回答

※独・DSCがREspect!を認可した際の「独立性・客観性等」の根拠は次ページのとおり。

REspect!への質問と回答：②公的資金への依存

資金調達の現状

- REspect!は連邦プログラム「Live Democracy!」の枠組み内で行われている。
- この**資金は連邦政府（BMFSFJ）とバイエルン州から提供**を受けている。(3)

REspect! のウェブサイト上の関連団体の表示

連邦家族・高齢者・女性・青少年省 ／ 連邦プログラム「Live Democracy!」 ／ バイエルン州 家族・労働・社会省 ／ バイエルン州

欧州議会での質問

2024年10月14日
Christine Anderson 議員
Petr Bystron 議員

Trusted Flaggerが**公的資金に依存していることについて、欧州委員会はどのように評価しているのか。**
また、そのような中立性・独立性も法律で義務付けられるべきか。

欧州委員会の回答

2024年11月27日
Margrethe Vestager副委員長

Trusted Flaggerが公的資金に依存することは、**オンラインプラットフォームからの独立性、通知の送信の真摯さ、客観性、正確性を損なわれない限り、DSAと両立**する。

出所）
(1) 質問 https://www.europarl.europa.eu/doceo/document/E-10-2024-002057_EN.html
(2) 回答 https://www.europarl.europa.eu/doceo/document/E-10-2024-002057-ASW_EN.html
(3) REspect! ウェブサイト https://meldestelle-respect.de/

独・DSCがREspect!を認可した際の「専門性・正確性・客観性」の根拠はこれまでの通知者としての経験・実績、「独立性」の根拠は事業者との金銭的なやり取りがないことを挙げている

独・連邦ネットワーク庁（DSC）公表のREspect!認可資料より抜粋（**※「根拠の概要」はNRIが作成・分類**）

要素	根拠の概要（NRI作成・分類）	具体的な根拠（独・DSC公表資料より抜粋）
特別な専門知識と能力	①これまでの通知対応の実績	**2023年に24,528件の報告を受け、そのうち8,473件の刑事告発が行われたため、特に公的犯罪において専門性を有している。**
	②連邦政府との繋がり	**コンテンツの法的評価のために連邦刑事局（BKA）およびサイバー犯罪中央連絡窓口（ZAC）と定期的に情報を交換している。**
	③通知者としての認可実績	2023年以来**TikTokのTrusted Flaggerである。**
	④スタッフの経歴	上級スタッフは専門的な**学位を持ち、活動経験が長い。**
	⑤スタッフの教育	従業員は法律に関する予備知識または第一次国家試験を証明し、**社内のトレーニングを修了する必要がある。**
慎重・正確・客観的な報告活動	①これまでの経験	**2017年以来オンライン上のヘイトスピーチに対する報告を受けており、それ以来報告の受付を継続**している。
	②通知の際のプロセス	**PF上のコンテンツの削除を要求する際に、**報告書を関連する諮問機関に伝達している。（犯罪の場合はBKA）
	③違法性を判断するプロセス	**違法コンテンツを検出して報告するために、標準化された評価基準と特殊なソフトウェアを使用した人為的評価と自動化ツールを組み合わせた多段階のプロセスを使用**している。
	④これまでの通知対応の実績	**合計24,528件（1日平均67件）の報告を受け**、最終的に約6,000件のコンテンツが削除された。2022年の合計報告数（9,914件）と比較して報告数はほぼ3倍になっている。2024年6月30日時点で合計14,543件（1日平均80件）の報告が寄せられる。そのうち、5,498件が犯罪に関連するものであった。
	⑤通知の受入れ体制	金融情報部門は匿名で報告を受けており、ヘイトと闘う全てのユーザーに報告する機会が与えられている。
PF事業者からの独立性	❶資金調達	**95%は連邦政府支援プログラム（Live Democracy）による公的資金から、5%は自己資金**から調達される。
	❷PF事業者との関わり	PF事業者との直接的な契約はなく、独立して活動していることをDSCの調査で確認した。
	❸スタッフの採用プロセス	**スタッフは、利益相反を回避するために慎重に選ばれている。**
	❹PF事業者との関わり（TikTok）	**TikTokとの金銭的な関係はないため、TikTokのTrusted Flaggerであることは独立性に矛盾しない。**

出所）連邦ネットワーク庁（ドイツのDSC） HPよりNRI作成
https://www.dsc.bund.de/DSC/DE/4TrustedF/start.html

当局からの措置命令は、全ての事業者に一定数発出されている。Trusted Flaggerによる通知は、制度が開始間もないことに起因して現状は少ない

各PFが受領した命令・通知の累計件数（事業者により対象期間が異なる）

		YouTube（2024年3月～6月）	Instagram（2024年4月～9月）	TikTok（2024年1月～6月）	X（2024年4月～9月）
司法・行政当局	措置命令	17	282	556	14
	情報提供命令	（記載なし）	3,414 ※InstagramとFacebookの合算値	7,676	8,057
Trusted Flagger	通知	0	3	0	6
一般ユーザー	通知	309,142	322,283	144,188	277,654

※Trusted Flaggerは2024年6月末時点で4団体、同年9月末時点で7団体が任命されている。

YouTube: https://storage.googleapis.com/transparencyreport/report-downloads/pdf-report-27_2024-3-1_2024-6-30_en_v1.pdf
Instagram: https://transparency.fb.com/sr/dsa-transparency-report-apr2024-instagram
TikTok: https://sf16-va.tiktokcdn.com/obj/eden-va2/zayvwlY_fjulyhwzuhyJ/ljhwZthlaukjlkulzlp/DSA_H2_2024/TikTok-DSA-Transparency-Report-Jan-to-Jun-2024.pdf
X: https://transparency.x.com/dsa-transparency-report.html
※上記レポートを基に、件数の記載のないものについては、NRIにて合算の上作成。命令・通知の対象コンテンツは、各事業者のポリシー等によって異なる可能性がある。

②違法情報の判断基準｜窓口に命令・通知を受けた際の違法性の判断プロセス

DSA上は事業者が命令・通知を受け取った際の具体的な対応方法は義務付けられていない。事業者は、自社ポリシーに基づいてコンテンツを評価し、違反が無ければEU法・各国法に基づき評価を実施。

VLOP/VLOSEに見られるコンテンツの一般的な評価プロセスと各事業者の特徴（参考：Google、Meta、TikTok、Xの透明性レポート）

プロセス	窓口を通して通知を受付	コンテンツを特定して、評価、判断する		
		① **コミュニティガイドラインや、企業ポリシー等に基づく判断**	② 前段で違反が認められない場合 **EU法・各国法に基づく判断**	③ 措置の有無を判断する
事業者の特徴（公開情報より）	**Googleの場合** ✓ 法的請求の場合は、訓練を受けた専任の法執行対応チーム（LERT）が対応する。	**Metaの場合** ✓ 評価には以下を用いる。 ✓ コミュニティガイドライン(1) ✓ Global Network Initiative(2) ✓ Corporate Human Rights Policy(3) ✓ Advertising Standards(4) **Xの場合** ✓ 評価の結果について、コンテンツが明らかに違反していない場合など必要に応じ、別のスタッフからの第2・第3の意見を求めることもできる。	**Metaの場合** ✓ 社内弁護士と外部顧問弁護士の双方によるサポートを実施。 **TikTokの場合** ✓ 法的有効性のレビューは必ず人間が実施。 **Xの場合** ✓ 必要に応じ、法律顧問に相談を実施。	**Googleの場合** ✓ 通常、違法と判断された場合、その国/地域のコンテンツのみに措置をするが、ポリシー違反の場合は全世界で措置を実施。 **TikTokの場合** ✓ 通常、違法である国において、場合によってはEEA地域全体において、あるいは世界的な措置を実施。

(1) https://transparency.meta.com/ja-jp/policies/community-standards/
(2) https://globalnetworkinitiative.org/
(3) https://about.fb.com/wp-content/uploads/2021/03/Facebooks-Corporate-Human-Rights-Policy.pdf
(4) https://transparency.meta.com/policies/ad-standards/

YouTube: https://storage.googleapis.com/transparencyreport/report-downloads/pdf-report-27_2024-3-1_2024-6-30_en_v1.pdf
Instagram: https://transparency.meta.com/sr/dsa-transparency-report-sep2024-facebook
TikTok: https://sf16-va.tiktokcdn.com/obj/eden-va2/zayvwlY_fjulyhwzuhy[/ljhwZthlaukjlkulzlp/DSA_H2_2024/TikTok-DSA-Transparency-Report-Jan-to-Jun-2024.pdf
X: https://transparency.x.com/dsa-transparency-report.html

窓口に通知を受けた際の違法性の根拠は、ポリシー違反によるものとEU法・各国法に基づく割合はサービス間で異なる

各PFが受領した通知の累計件数
（2025年2月5日時点の最新の透明性レポート）

				YouTube（Google）	Instagram（Meta）	TikTok	X
通知	通知の全件数			309,142	322,283	144,188	277,654
措置	措置の全件数			229,747*	77,986	29,091	252,599
		ポリシー違反を根拠とする場合	措置の件数（措置の全件数に占める割合）	3,542（2%*）*四捨五入	76,084（98%）	13,370（46%）	37,122（15%）
		EU法・各国法違法を根拠とする場合	措置の件数（措置の全件数に占める割合）	226,205（99%）	1,902（2%）	15,721（54%）	215,477（85%）
	通知全件数に対する措置全件数の割合			-*	24%	20%	91%

*YouTubeのレポートでは「第16条の通知1つに対して複数の措置を取ることができる。」と記載があるため、通知全件数に対する措置全件数の割合は出していません。

YouTube: https://storage.googleapis.com/transparencyreport/report-downloads/pdf-report-27_2024-3-1_2024-6-30_en_v1.pdf
Instagram: https://transparency.fb.com/sr/dsa-transparency-report-apr2024-instagram
TikTok: https://sf16-va.tiktokcdn.com/obj/eden-va2/zayvwlY_fjulyhwzuhyJ/ljhwZthlaukjlkulzlp/DSA_H2_2024/TikTok-DSA-Transparency-Report-Jan-to-Jun-2024.pdf
X: https://transparency.x.com/dsa-transparency-report.html
※上記レポートを基に、件数の記載のないものについては、NRIにて合算の上作成。命令・通知の対象コンテンツは、各事業者のポリシー等によって異なる可能性がある。

DSAでは、違法コンテンツに関し、削除等の具体的な措置方法は定めていない

■DSAでは、PF事業者に対して違法コンテンツに関する通知を受けたり、対応措置と異議申立てを行ったりする仕組みの整備を求める一方、具体的な対応措置として削除やアクセス無効化を定めていない。

- 前文では、違法コンテンツについて削除またはアクセス無効化の対応を求めている（前文50項）が、**本文ではPF事業者が実施した削除またはアクセス無効化等の措置に対する救済措置の整備を義務付ける（20条等）**にとどまる。

- 違法コンテンツに関する行政または司法当局からの措置命令に対し、**PF事業者の実施報告義務を定める（9条）が、当局は削除等の具体的な措置方法を指定していない。**

事業者が実施した措置に対してサービス利用者・団体からの異議申立てを受け付ける仕組みの導入を義務付け。PFによって申立てによる措置の撤回の割合は2割～4割とばらつきがある

■ オンラインプラットフォーム事業者は、違法性や規約に基づいて下した決定後少なくとも6か月間、電子的に無料で異議を申し立てることができる効果的な内部異議申立処理システムへのアクセスを提供するものとする。
（20条より一部抜粋）

措置に対し受領した異議申立ての件数（2025年2月5日時点の最新の透明性レポート） ※事業者により対象期間が異なる

	YouTube（Google）（2024年3月～6月）	TikTok（2024年1月～6月）	X（2024年4月～9月）
異議申立ての全件数	2,121,672	3,244,150	289,926
申立てに基づき措置を撤回した件数	255,329	1,386,593	71,327
申立ての全件数に占める撤回の割合	37%	43%	25%

YouTube: https://storage.googleapis.com/transparencyreport/report-downloads/pdf-report-27_2024-3-1_2024-6-30_en_v1.pdf
TikTok: https://sf16-va.tiktokcdn.com/obj/eden-va2/zayvwlY_fjulyhwzuhy[/ljhwZthlaukjlkulzlp/DSA_H2_2024/TikTok-DSA-Transparency-Report-Jan-to-Jun-2024.pdf
X: https://transparency.x.com/dsa-transparency-report.html

２－２．英国におけるOSA：違法情報に関する制度及び事業者の対応

OSAでは、事業者に対して、違法コンテンツの削除等を行うことを目的として設計されたシステム・プロセスを使用してサービスを運用することを義務付け。

- 一般的な違法コンテンツについて、ユーザーから存在を通知された場合、または存在を認識した場合に迅速に削除すること等を目的として設計されたシステム・プロセスを使用してサービスを運用することを義務付け（10条3項(b)）
- 優先違法コンテンツ（テロやCSEAコンテンツ）について、上記に加え、存在する期間を最小限に抑えるために適切なシステム・プロセスを用いること等を義務付け（10条3項(a)）

義務内容

項目	ユーザー間サービス【第10条】
サービスの設計・運営上の義務	以下の目的のために設計された適切なシステムおよびプロセスを用いて、サービスを運営する義務。 • 優先違法コンテンツの存在を最小限にする。 • 優先違法コンテンツがサービス上でアクセス可能な時間を最小限にする。 • 優先違法コンテンツの普及を最小限にする。 • 違法コンテンツの存在を人から知らされた場合、またはその他の方法で知った場合、当該コンテンツを速やかに削除すること。
利用規約等への記載の義務	違法コンテンツから個人を保護するための方針と手続きの詳細を、利用規約に明記し、常に適用させる義務。 また、利用規約は明瞭でアクセスがしやすいものであること。

行動規範の内容

ユーザー間サービス【第10条】に関する行動規範の概要
違法コンテンツに関する行動規範（“Illegal content codes of practice for user-to-user services”）において、コンテンツモデレーション等に関して推奨される対策を提示。 ・違法と疑われるコンテンツを審査•評価するコンテンツモデレーション機能の具備（ICU C1） ・違法コンテンツを迅速に削除できるコンテンツモデレーション機能の具備（ICU C2） ・違法コンテンツを禁止する内規の策定（ICU C3） ・コンテンツモデレーション機能のパフォーマンス目標の設定（ICU C4） ・レビュー対象コンテンツの優先順位に関するポリシーの策定（ICU C5） ・コンテンツモデレーション機能への社内リソースの割り当て（ICU C6） ・コンテンツモデレーションに従事する個人へのトレーニングの提供（ICU C7） ・コンテンツモデレーションに関わるボランティアへの資料提供（ICU C8） ・ハッシュ値やURLを利用したCSEAコンテンツの検出・削除（ICU C9・C10）

OSAでは事業者に対して、ユーザーが違法コンテンツや子供にとって有害コンテンツを通報できるシステムやプロセスを用いてサービスを運営するよう義務付け。

コンテンツ報告・苦情受付の意味

- コンテンツ報告：ユーザーが違法・有害と思うコンテンツをプロバイダに報告すること
- 苦情受付：プロバイダが義務を果たしていないと思ったり、プロバイダにより自身のコンテンツが削除・制限等されたりしたユーザーからの苦情を受け付け、必要に応じて対応すること。

区分	ユーザー間サービス【第20条・第21条】
コンテンツ報告	【第20条】 ユーザーや影響を受ける人*が、以下に定める種類のコンテンツと思われるものを容易に報告できるようなシステムやプロセスを用いてサービスを運営する義務。 • 違法コンテンツ • 子供がアクセス可能なサービスの一部に存在する、子供にとって有害なコンテンツ
苦情受付	【第21条】 以下のような苦情を受け付ける手続きを、容易で、（子供も含めて）使いやすく、透明性があるように運用すること。また、苦情の処理および解決を規定する方針およびプロセスを、（子供を含めて）容易にアクセスできる条項として利用規約に含めること。 • サービスが違法コンテンツ、子供に有害なコンテンツやその他の義務に対応していないことへの苦情 • プロバイダにより（プロアクティブ技術によることを含む）削除や制限をかけられたコンテンツを生成、アップロード、共有したユーザーからの苦情

*影響を受ける人とは、当該サービスの利用者以外の者であって、英国内にあり、かつ、以下のいずれかに該当する者をいう。
(a) コンテンツの対象である
(b) コンテンツが対象とする特定の特性を有する人々のクラスまたはグループの一員である
(c) サービスの利用者またはコンテンツの対象者である子供の親、または子供に責任を持つその他の成人
(d) 他の成人がサービスの利用者またはコンテンツの対象者である場合、そのような支援を必要とする他の成人にサービスを利用する際の支援を提供する成人

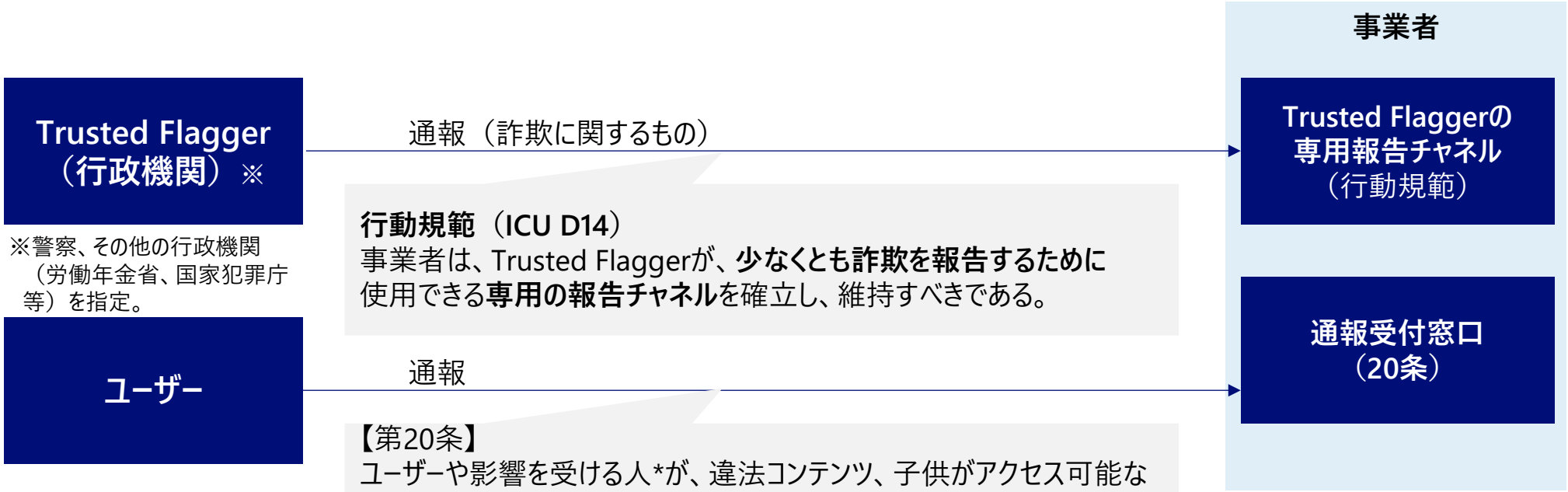
行動規範の内容

ユーザー間サービス【第20条・第21条】に関する行動規範の概要

第10条と同様の行動規範のうち、第20条・第21条は主に「報告・苦情」の項目において、14の小項目に分けて推奨される措置が提示されている。
具体的には、例えば、苦情を受領した際には、「苦情を決定するための目安の期間」を、苦情の申立人に提供すべきであること等が示されている。

OSAは事業者に対して、ユーザー等からの違法コンテンツ通報受付、苦情処理手続きの運用を義務付けるともに、行動規範においてTrusted Flaggerからの専用報告チャネルの設置を推奨

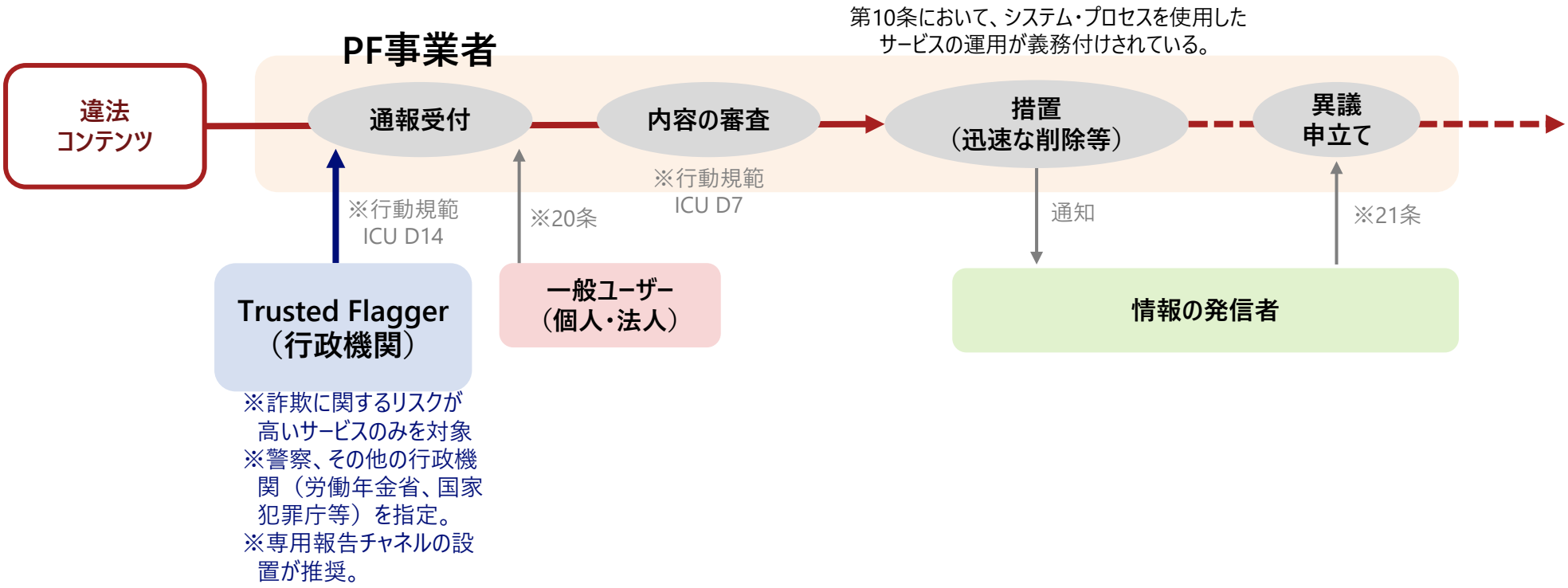
OSAにおける窓口整備義務の概観



出所）OSA条文Online Safety Act 2023等よりNRI作成

OSAでは、事業者に対して、ユーザー等からの違法コンテンツ通報受付や苦情処理手続きの運用を義務付け。また、OSAに基づきOfcomが策定を義務付けられている行動規範において、Trusted Flaggerからの専用報告チャネルの設置を推奨している

OSAにおける事業者の対応義務の概観



出所）OSA条文Online Safety Act 2023等よりNRI作成

Ofcomは、「違法コンテンツ判断ガイダンス」を発行。優先犯罪（およびその他の犯罪）ごとに、違法コンテンツの判断方法を提示している

■ Ofcomは2024年のステートメントの中で、「違法コンテンツ判断ガイダンス（“Illegal Content Judgements Guidance (ICJG)”）」を発行。**優先犯罪（テロ・CSEA・ハラスメント等）ごとに、違法コンテンツの判断方法を提示している。**

ガイダンスの章構成

導入	1. Introduction
優先犯罪ごとの判断方法	2. テロ：Terrorism 3. 脅迫・虐待・ハラスメントThreats, abuse and harassment (including hate) 4. 子供の性的虐待・搾取Child sexual exploitation and abuse (CSEA) 5. 詐欺・金融サービス犯罪：Fraud and other financial offences 6. ドラッグ：Drugs and psychoactive substances 7. 銃器・武器：Firearms and other weapons 8. 成人の性的搾取：Sexual exploitation of adults 9. 画像に基づく成人向け性的犯罪：Image-based adult sexual offences 10. 人身売買：Human trafficking 11. 不法移民：Unlawful immigration 12. 自殺ほう助：Encouraging or assisting suicide 13. 外国干渉罪：Foreign interference 14. 動物虐待：Animal cruelty
その他の犯罪の判断方法	15. その他の犯罪：Non-priority offences and relevant non-priority offences (‘other’ offences)

出所）Illegal Content Judgements Guidance (ICJG)よりNRI作成

ガイダンスで、サービス提供者は、英国刑法に則り、コンテンツの違法性を判断すべきとされている（すべての優先犯罪・その他の犯罪に共通の内容）

■ Ofcomは「違法コンテンツ判断ガイダンス」の中で、英国の刑法では、すべての犯罪は以下の3つの要素で構成されているとしている。

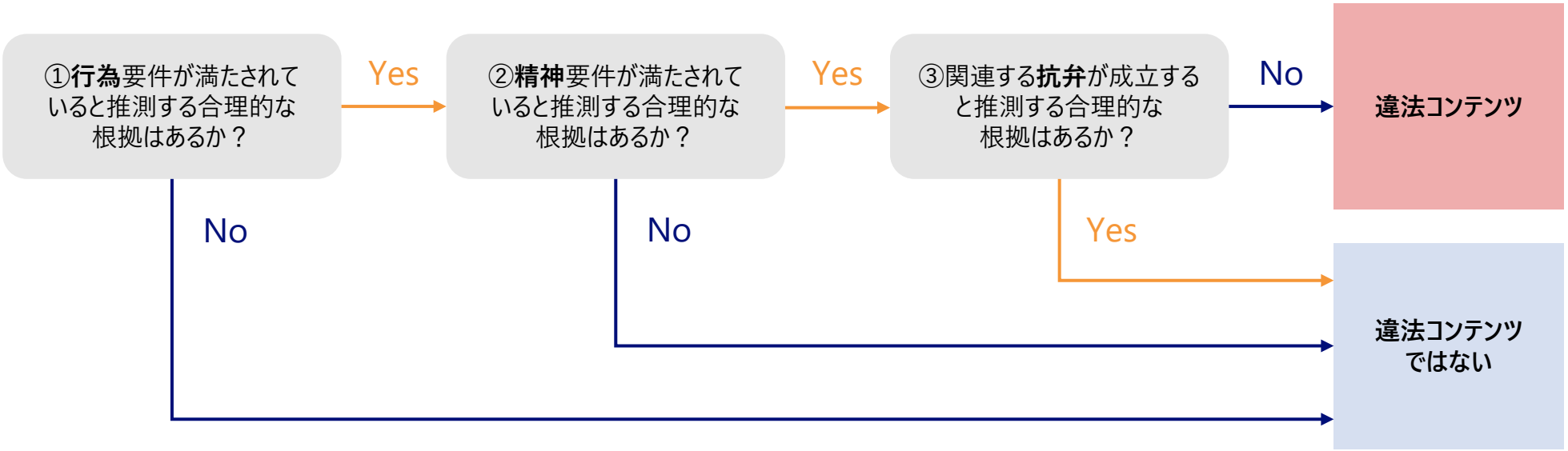
① **違法な行為**またはその要素（actus reus）

② **違法な精神状態**またはその要素（mens rea）

③ **関連する抗弁**（OSAにおいては、関連する抗弁があると合理的に推論できる場合は、当該コンテンツは違法コンテンツではない）

■ コンテンツが違法コンテンツか否かの判断にあたっても、それぞれの要素がユーザーとの関係性の中で考慮すべきとされている。

違法コンテンツの判断にあたっての考え方（すべての優先犯罪・その他の犯罪に共通の内容）



出所）Illegal Content Judgements Guidance (ICJG)よりNRI作成

（参考） OSAにおける特定の違法情報に係る特別な対応

Ofcomは、テロおよびCSEAコンテンツの場合に限り、暗号化された通信を解読する技術などの認定技術を用いて、コンテンツを特定し、削除等の措置の実施を要求することが可能

- **Ofcomは、必要かつ適切であると判断した場合、**ユーザー間サービスまたは検索サービスの提供者に対し、**テロコンテンツやCSEA（子供の性的搾取・虐待）コンテンツへの対処通知が可能（121条）。**
  - **2025年2月時点で、執行事例は確認できていない。**
- なお、通知を行う前に、熟練者（skilled person）からのレポートを入手することが、Ofcomに義務付けられている（122条）。

Ofcomが発出可能な通知

通知対象	通知内容	条文
ユーザー間サービス	• 以下のいずれか、またはすべてを実施すること。 a. 認定技術を使用して、サービス上で発信されるテロコンテンツを特定し、迅速に削除すること b. 認定技術を使用して、サービス上で発信されるテロコンテンツへの接触を防止すること c. 認定技術を使用して、サービス上で公私問わず発信されるCSEAコンテンツを特定し、迅速に削除すること d. 認定技術を使用して、サービス上で公私問わず発信されるCSEAコンテンツへの接触を防止すること	121条2項(a)
	• 以下の要件を満たす技術を開発または調達する努力を最大限行うこと。 1. 上記cまたはdの目的を達成すること。 2. 国務大臣が公表する基準を満たすこと。	121条2項(b)
検索サービス	• 以下のいずれか、またはすべてを実施すること。 a. 認定技術を使用して、サービスの検索結果内のテロコンテンツを特定し、可能な限り迅速に検索結果からそのコンテンツを排除する措置を講じること。 b. 認定技術を使用して、サービスの検索結果内のCSEAコンテンツを特定し、可能な限り迅速に検索結果からそのコンテンツを排除する措置を講じること。	121条3項(a)
	• 以下の要件を満たす技術を開発または調達する努力を最大限行うこと。 1. 上記bの目的を達成すること 2. 国務大臣が公表する基準を満たすこと	121条3項(b)

出所）Online Safety Act 2023　等よりNRI作成

（参考）OSAにおける特定の違法情報に係る特別な対応

前述の121条義務には、セキュリティやプライバシーの観点から懸念が上がっている

121条義務に対する、ステークホルダーからの懸念

■ 121条義務は、テロコンテンツ・CSEAコンテンツに絞っている一方で、暗号化された通信を解読する技術などの**認定技術を用いてのコンテンツの特定**等を設けていることから、セキュリティやプライバシーの観点から懸念が上がっている。

懸念	具体の内容（主体）
セキュリティ	• オンラインサービスに認定技術の使用を命じるOfcomの権限は、すべてのユーザーの権利を危険にさらす。セキュリティの専門家やNGOは反対意見を表明してきたが、OSAの内容には反映されなかった。（米非営利組織・Electronic Frontier Foundation）
プライバシー	• 政府がサービスプロバイダーに対してコンテンツの事前スキャンを要求できることを定めたものであり、個人のプライバシーが脅かされる可能性がある。（英メディア・New Statesman） • エンドツーエンド暗号化メッセージングサービスでは、サービスに内在するユーザープライバシーの原則と対立しするため、OSAの要件を満たすことができないのではないか。（英法律事務所・Cooley） • エンドツーエンド暗号化メッセージングサービスでは、サービスに内在するユーザープライバシーの原則と対立しするため、OSAの要件を満たすことができないのではないか。（英法律事務所・Cooley）

出所）The UK Online Safety Bill Attacks Free Speech and Encryption | Electronic Frontier Foundation、The Online Safety Bill is finally law – it says a lot about our broken politics - New Statesman、Balancing Act: Navigating Privacy Challenges Under UK's Online Safety Act 2023 - cyber/data/privacy insights、UK Online Safety Bill passes with encryption-busting clause • The Register、End-to-end encryption and child safety - GOV.UK　等よりNRI作成

（参考）OSAにおける特定の違法情報に係る特別な対応

Ofcomは、先進的な企業でも、エンドツーエンド暗号化との両立を実現する技術は開発中であることから、実現性は2023年9月時点では担保されていないと推察されると声明を発表。英技術大臣は、121条義務の行使は「最後の手段」であるとコメントしている。

Ofcomによる声明

- Ofcomは2023年9月、「**エンドツーエンド暗号化と子供の安全**」と題した声明を発表。
- Metaやその他のSNS運営企業に対して、エンドツーエンド暗号化とオンラインでの子供の保護を両立するための、技術的解決策を開発することを要求しているとした。
- 一方で、Metaのような先進的な企業でも、エンドツーエンド暗号化との両立を実現する技術は開発中であることから、**実現性は2023年9月時点では担保されていない**と推察される。

英技術大臣のコメント

- 英国のMichelle Donelan 技術大臣は、BBCの取材に対し、政府はサービスの暗号化に反対しているわけではなく、アクセス権限の要求は最後の手段（"a last resort"）としてのみ行われるとコメントしている。

出所）UK defends plan to demand access to encrypted messages to protect children | Reuters等よりNRI作成

３．違法情報の発信を抑止するための方策（本人確認制度）

3．違法情報の発信を抑止するための方策（英国・韓国）

	英国	韓国	
法律名	**OSA（オンライン安全法）**	**情報通信網法**	**公職選挙法**
背景	匿名での人種差別や誹謗中傷等に対する懸念の高まり	2000年代に韓国ではインターネット上での匿名性を原因とする誹謗中傷や名誉毀損が社会問題となり、著名人が標的となる事案が多発し、被害者が自殺に追い込まれる事態も発生	2002年大統領選挙における政党や候補者へのネガティブキャンペーンが問題視され、対応策として法制度化
義務内容	成人ユーザー向けの本人確認のオプション提供義務 （本人確認を義務付けているわけではない）	民間・公的機関のオンライン掲示板利用者向けの本人確認の義務付け	インターネット報道機関の掲示板やチャットページにおける選挙期間中選挙に関する投稿を対象に実名認証と認証表示を義務付け
現状	施行に向けて準備中 （Ofcomに策定義務が課せられているガイダンスは未公開※2025年1月現在）	憲法裁判所において違憲判決 民間事業者向けの本人確認義務規定については削除	憲法裁判所において違憲判決 本人確認義務規定については削除

本人確認義務の立法背景として、匿名での誹謗中傷等をOfcomは挙げている。サービス提供者は、成人ユーザーに本人確認のオプションを提供する必要がある。Ofcomは、義務遵守支援のためのガイダンスの策定が義務付けられている

立法背景と本人確認義務の趣旨

- Ofcomは、本人確認のオプション提供義務の背景として、**匿名での誹謗中傷**を挙げている。（サッカー欧州選手権後の選手への人種差別や、女性議員へのレイプ・殺害予告など）
- 本人確認の認証オプションを提供し、同時に未認証ユーザーからのメッセージやリプライを受け取らないよう設定できるツールを提供する義務を課すことで、ユーザーが**交流するユーザーを自由に選択できる**（匿名ユーザーと交流しないことを選択できる）措置だと説明している。

本人確認に係る義務規定（同法64条・65条）

- カテゴリ1サービスの提供者に対して、**成人ユーザーへの本人確認のオプション提供を義務付けている（本人確認を義務付けているわけではない）**。

	義務規定	条文
サービス提供者に対する本人確認義務	• サービス提供者は、**サービスの成人ユーザー全員に対し、本人確認を行うオプションを提供しなければならない。**（本人確認のプロセスは任意の方法で実施できる）	64条(1)(2)
	• サービス提供者は、本人確認プロセスがどのように機能するかについて、**明瞭でわかりやすい規定を利用規約に含めなければならない。**	64条(3)
	• 本人確認義務は、以下の範囲にのみ適用される。 **(a)ユーザー間の交流機能を持つサービス部分　かつ、** **(b)英国におけるサービス**	64条(7)
Ofcomに対するガイダンス作成義務	• Ofcomは、サービス提供者が本人確認オプション提供義務を遵守するのを支援するため、**ガイダンス**（注）**を作成しなければならない。**	65条(1)
	• ガイダンスを作成する際には、年齢や障がい等のため支援が必要な**社会的弱者**（**vulnerable adult users**）**が利用できる形態となるよう考慮しなければならない。**	65条(2)
	• ガイダンスを作成する前に、以下の関係者と協議しなければならない。 (a)情報コミッショナー（ICO） (b)技術的専門知識を有すると考えられる者 (c)サービスの社会的弱者ユーザーの利益を代表すると考えられる者 (d)Ofcomが適切と判断するその他の者	65条(3)

出所）Online Safety Act 2023、Call for evidence: Third phase of online safety regulation　等よりNRI作成
注）2025年2月6日現在では、ガイダンスは公開されていない。

議会では、本人確認義務が立法化される過程で、無料提供・ガイダンスでの原則策定・認証ユーザーの可視化等が議論された

本人確認義務が立法化される過程で、議員から提示された修正案及び当該修正案に対する採否と理由

議員から提示された修正案	採否と理由
無料提供の明確化 ：本人確認義務等を「無料」で提供することを明確化するべき	• 政府答弁で、「有料では全ユーザーへの提供が不可能になるため、結果として無料で提供せざるを得ない」とされ、**明文化修正は不要として退けられた**
ガイダンスでの原則の策定義務 ：Ofcomは、ガイダンスの中で最低基準や原則を定めるべき	• 政府答弁で、「Ofcomにはすでに一般消費者の利益を図る義務などがあり、ガイダンス内容は専門家や関係者と協議して柔軟に決めるべき」とされ、**採用は見送られた**
PF上での認証ユーザーの表示義務 ：サービス上で、他のユーザーが認証済みか否かの表示を義務付けるべき	• 政府答弁で、「一部のユーザーの安全性を高める可能性はあるものの、正当な理由で匿名性を維持する必要がある脆弱なユーザー(vulnerable users)(※)にとっては不利益となるため、利用者が本人確認済みか否かの表示を義務付けることは適切ではない」とされ、**退けられた** (※) 例えば、ハラスメントや差別等の理由で匿名性を保持する必要のある者を含む、オンライン上で特に被害を受けやすい利用者。 • この点は、人権団体（Open Rights Group等）からも指摘されていた点であり、政府はこれらに配慮したと考えられる

出所）New plans to protect people from anonymous trolls online - GOV.UK、Our submission to Ofcom's call for evidence on its "third phase of online safety regulation"、Online Safety Bill - Hansard - UK Parliament、The Online Safety Bill and Government crackdown on anonymity will punish victims | Open Rights Group、Online Safety Bill - Hansard - UK Parliament 等よりNRI作成

（参考）ステークホルダーからの意見

ステークホルダーからの、本人確認義務への意見

主体	意見（主体）
議員	• プラットフォーム任せだった匿名利用対策に対して歯止めがかけられる。（与党） • 方針は支持するが、高齢者や障がい者にも利用しやすい確認方法を提示すべき。（野党）
事業者・業界団体	• 既に認証バッジなど、アカウント認証サービスの提供を進めている。（X） • ユーザー情報のプライバシー保護等課題が山積している。（teckUK）
プライバシー・人権団体	• インターネットを二層化し、匿名性に頼って自身を守っている人々を事実上差別することになる。（Open Rights Group）
表現の自由擁護団体・インターネットの自由擁護団体	• 匿名の表現は健全な民主主義社会の構成要素であり、過度な自己検閲を生まないよう保証されるべき。（Index on Censorship）
青少年保護団体・被害者支援団体	• 匿名の陰に隠れて行われるネットいじめや性的勧誘から青少年を守るには、プラットフォーム側で年齢確認や本人確認を促進することが重要。（NSPCC）

出所）New plans to protect people from anonymous trolls online - GOV.UK、Our submission to Ofcom's call for evidence on its "third phase of online safety regulation"、Online Safety Bill - Hansard - UK Parliament、The Online Safety Bill and Government crackdown on anonymity will punish victims | Open Rights Group等よりNRI作成

匿名での誹謗中傷が社会問題となり、掲示板やコメント機能を提供する大規模なサイトの運営事業者に対し、利用者の実名よる本人確認が導入された

■ 2008年6月改正の情報通信網法では、44条の5（掲示板利用者の本人確認）が追加され、**インターネット上の誹謗中傷や違法コンテンツを抑制**するため、1日の平均訪問者数が10万人以上の**掲示板やコメント機能を提供するサイト**の運営事業者について、利用者の本人確認措置が義務付けられた（いわゆる「実名制」）。

- 立法背景として、2000年代に韓国ではインターネット上での**匿名性を原因とする誹謗中傷や名誉毀損が社会問題**となり、著名人が標的となる事案が多発し、被害者が自殺に追い込まれる事態も発生した。
- 適用対象は民間事業者が運営するポータルサイト等に加え、コメント機能を提供する公営サイトも含まれた。
- 具体的には、**ユーザー登録時の本人確認後**、事業者側で実名情報を保存し、**当局の要請に応じて情報を提供**。ユーザーが初めて**投稿する際に事業者が再度本人確認**を実施した場合には、IDや**ニックネーム表示で投稿が可能**。

運営者	カテゴリ	対象サイトの例
民間事業者	ポータルサイト	Naver、Daum
	ソーシャルメディア・コミュニティサイト	Cyworld、Nate
	動画共有サイト	Pandora TV、AfreecaTV
	オンライン掲示板・フォーラム	DC Inside、Clien
	ECサイト	Gmarket、Auction
	ニュースサイト	Yonhap News（聯合ニュース）、Chosun Ilbo（朝鮮日報）
行政機関	韓国政府のウェブサイト	大統領府の公式サイト、政府ポータルサイト（Gov.kr）
	地方自治体のウェブサイト	ソウル市の公式サイト、釜山市の公式サイト

出所）情報通信網法（정보통신망법）2008年6月改正 https://elaw.klri.re.kr/eng_service/lawView.do?lang=ENG&hseq=7288（英訳）
2014年5月改正 https://elaw.klri.re.kr/eng_service/lawView.do?lang=ENG&hseq=32543（英訳）
法律新聞（법률신문）「インターネット実名制違憲判決の意義と展望」 https://www.lawtimes.co.kr/news/105055 ※韓国語のみ

業界団体からは運用コストの増加、表現の自由への影響などの懸念が表明された。実名による本人確認は過度に制限的であるとして違憲判決により法改正で削除された

- 実名制の導入に際し、韓国インターネット企業協会や韓国コンテンツ振興協会等、多くの業界団体から懸念が表明され、主に以下が指摘された。
  - 運用コストの増加：本人確認のシステムを構築・運用するコストがかかり、中小規模のサイトの運営事業者に負荷が大きい。
  - 個人情報漏えいのリスク：本人確認のための個人情報の収集・管理に伴い、漏えいの可能性が高まる。
  - インターネット上の表現の自由への影響：匿名性が失われ、ユーザーが意見交換や創造的な活動を控える可能性がある。
  - 国際競争力の低下：海外プラットフォームは対象外であり、韓国企業のみ対象となるために競争上不利となる可能性がある。
  - 実効性への疑問：VPNや海外プラットフォームを利用すれば実名制を回避可能であり、匿名での誹謗中傷を防げない。
- 2012年8月の**憲法裁判所の違憲判決**を受け、2014年5月改正で民間事業者向け規定（1条2項）が**削除**された。
  - 判決では、**実名制は過度に制限的**であり、掲示板利用者の表現の自由と自己情報決定権、提供事業者の言論の自由などの基本権を侵害するものと判断された。
    - 被害者救済は同法の他規定（違法情報の削除、流通禁止など）や事後の損害賠償等で可能
    - 違法行為の可能性がない閲覧者も本人確認の対象に含まれるため、適用対象の事業者を恣意的に解釈可能
    - 本人確認情報は情報の掲示終了後6か月間保管されるため、情報を削除しない限り無期限に保管される
    - 国内利用者の海外サイトへの回避、海外事業者への執行困難、適用対象外となるSNSの登場
  - 公営サイトでの（実名を公表しない形での）本人確認そのものは否定せず、特定の目的（行政サービスの提供、不正防止）に限定すれば表現の自由を侵害しないと判断された。
- 実名制の廃止後、2019年には誹謗中傷による著名人の自殺事件を受け、再導入を求める意見が増加した。

出所）情報通信網法（정보통신망법）2008年6月改正 https://elaw.klri.re.kr/eng_service/lawView.do?lang=ENG&hseq=7288（英訳）
2014年5月改正 https://elaw.klri.re.kr/eng_service/lawView.do?lang=ENG&hseq=32543（英訳）
法律新聞（법률신문）「インターネット実名制違憲判決の意義と展望」 https://www.lawtimes.co.kr/news/105055 ※韓国語のみ
聯合ニュース https://jp.yna.co.kr/view/AJP20191016003900882

公職選挙法ではネガティブキャンペーン防止のために実名認証が導入されたが、表現の自由への過度な制約であるとして違憲判決が出され、同規定は削除された

- 2005年8月改正の公職選挙法では、82条の6（インターネット報道機関の掲示板やチャットページにおける実名認証の表示）が追加され、**選挙期間中の選挙関連の投稿について実名認証が必須化**された。
  - 背景として、2002年大統領選挙における政党や候補者に対するネガティブキャンペーンが問題視され、対応策として実名制が導入された。
  - 具体的には、運営事業者はユーザー登録において、行政安全部と中央選挙管理委員会が提供する住民登録番号*を用いた認証システムや、個人信用評価会社（信用機関）の照合サービスを利用して本人確認を実施していた。
  - 導入後も世論の反発は強く、2008年、2010年に違憲訴訟が提起され、一部改正されてきた（いずれも合憲判断）。
- 2015年7月の**憲法裁判所の違憲判決**を受け、以後、同条は適用が中止され、2023年の改正で**同条は削除**された。
  - 判決では、匿名による政治的表現への規制は、民主主義社会における自由な世論形成を妨げる可能性があるうえ、選挙期間中のネガティブキャンペーンは匿名性以外の要因によっても生じるため、すべての匿名表現を事前かつ包括的に規制することは、表現の自由を過度に制限すると判断された。
- 情報通信網法に比べ、選挙の公正性という公共の利益に関係しているうえ、選挙期間かつ選挙関連の投稿のみに対象が限定されていたことから、本人確認制の廃止の時期が遅くなったと考えらえる。

*政府が17歳以上の国民に対して割り振る13桁の番号。行政サービスや銀行口座の開設等に利用される。

出所）公職選挙法（공직선거법）　2005年8月改正 https://elaw.klri.re.kr/kor_service/lawView.do?lang=KOR&hseq=229（英訳）
現行法 https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B3%B5%EC%A7%81%EC%84%A0%EA%B1%B0%EB%B2%95　※韓国語
韓国法制処　「公職選挙法82条の6の1項公等違憲確認等」 https://www.law.go.kr/detcInfoP.do?mode=1&detcSeq=163493&vSct=2018%ED%97%8C%EB%A7%88456　※韓国語のみ
行政安全部・中央選挙管理委員会　「実名確認サービス利用マニュアル」 https://www.nec.go.kr/files/1/4/1_4_151_20120217214253_1.pdf　※韓国語のみ
柳 文殊　「韓国におけるインターネット実名制の施行と効果」 https://www.jstage.jst.go.jp/article/ssi/2/1/2_KJ00008760308/_pdf/-char/ja

（参考）情報通信網法　44条の5

44条の5　掲示板利用者の本人確認

赤字：2014年5月改正時に削除

1　次の各号のいずれかに該当する者は、掲示板を設置し、運用しようとする場合には、掲示板の利用者の本人確認の方法及び手順を整備する等、大統領令で定める必要な措置（以下「本人確認措置」という）を講じなければならない。

1. 国の機関、地方公共団体、公営企業・・・（中略）・・・地方政府公営企業

2. 大統領令で定める基準に該当する情報通信サービス提供者であって、提供する各種情報通信サービスの平均利用者数が1日当たり10万人以上に達する者。

2　韓国通信委員会は、1項2号の基準に該当する情報通信サービスの提供者が本人確認措置を講じない場合、当該措置を講じるよう命じることができる。

3　政府は、1項に基づく本人確認に向けて、より安全かつ信頼性の高いシステムを開発するための方針を定めなければならない。

4　公共機関または情報通信サービス提供者は、善良な管理者の注意をもって1項の本人確認措置を講じたときは、第三者による不正利用による損害賠償責任を軽減、または免除することができる。

情報通信網法施行令（大統領令）　22条の2

第 22 条の 2 （本人確認措置）

法律第 44 条の 5 第 1 項各号以外の部分で「大統領令の定める必要な措置」と言うのは、次の各号のすべてを言う。

1　「電子署名法」第 2 条第 10 号による公認認証機関その他の本人確認サービスを提供する第三者または行政機関に依頼することや、コピー送信・対面確認などを通じて、掲示板利用者が本人であることを確認することができる手段を用意すること

2.本人確認手続き及び本人確認情報保管の時、本人確認情報流出を防止することができる技術を用意すること

3.利用者が掲示板に情報を掲示した時から 6 ヶ月間、第 22 条の 4 による情報を保管すること

出所）情報通信網法（정보통신망법）2008年6月改正 https://elaw.klri.re.kr/eng_service/lawView.do?lang=ENG&hseq=7288（英訳）
2014年5月改正 https://elaw.klri.re.kr/eng_service/lawView.do?lang=ENG&hseq=32543（英訳）
公職選挙法（공직선거법）　2005年8月改正 https://elaw.klri.re.kr/kor_service/lawView.do?lang=KOR&hseq=229（英訳）
現行法 https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B3%B5%EC%A7%81%EC%84%A0%EA%B1%B0%EB%B2%95　※韓国語

（参考）公職選挙法　82条の6

82条の6　インターネット報道機関の掲示板やチャットページにおける実名表示　（抜粋）　**※2023年改正時に条ごと削除**

1　インターネット報道機関が選挙運動期間中、当該インターネットホームページの掲示板やチャットルーム等に、政党の候補者に対する支持や反対の文字・音声・画像又は動画等の情報（以下、本条で「情報等」という。）を掲示できるようにする場合には、行政安全部長官又は「信用情報の利用及び保護に関する法律」2条5号による個人信用評価会社（以下、本条で「個人信用評価会社」という。）が提供する実名認証方法*で実名を確認させる技術的措置を講じなければならない。ただし、インターネット報道機関が「情報通信網利用促進及び情報保護などに関する法律」44条の5による本人確認措置を行った場合には、その実名を確認されるような技術的措置を行ったものとみなす。

2　政党又は候補者が、その開設・運営するインターネットホームページの掲示板及びチャットページに、その政党又は候補者に対する支持又は反対の情報等を掲示できるようにする場合においては、その政党又は候補者は、1項の規定による技術的措置を講ずることができる。

3　行政安全部長官及び個人信用評価会社は、1項及び2項の規定により提供した実名認証資料を実名認証を受けた者及びインターネットホームページ別に管理しなければならず、中央選挙管理委員会がその実名認証資料の提出を要求する場合には、遅滞なくこれに応じなければならない。

4　インターネット報道機関は、1項の規定により実名認証を受けた者が情報等を掲示した場合、当該インターネットホームページの掲示板・チャットルーム等に「実名認証」表示が表示されるように技術的な措置を講じなければならない。

5　インターネット報道機関は、当該インターネットホームページの掲示板・チャットルーム等で情報等を掲示しようとする者に住民登録番号を記載することを要求してはならない。

6　インターネット報道機関は、当該インターネットホームページの掲示板・チャットルームなどに「実名認証」の表示がない政党や候補者に対する支持・反対の情報などが掲載された場合には、遅滞なくこれを削除しなければならない。

7　インターネット報道機関は、政党・候補者及び各級選挙管理委員会が6項の規定による情報等の削除を要求した場合には、遅滞なくこれに従わなければならない。

*行政安全部と中央選挙管理委員会は住民登録情報を利用した認証システムを事業者向けに提供している。
「実名確認サービス利用マニュアル」　https://www.nec.go.kr/files/1/4/1_4_151_20120217214253_1.pdf　※韓国語のみ

出所）公職選挙法（공직선거법）　2005年8月改正 https://elaw.klri.re.kr/kor_service/lawView.do?lang=KOR&hseq=229（英訳）
現行法 https://www.law.go.kr/%EB%B2%95%EB%A0%B9/%EA%B3%B5%EC%A7%81%EC%84%A0%EA%B1%B0%EB%B2%95　※韓国語