デジタル空間における情報流通の諸課題への対処に関する検討会

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）

１　日時　令和７年２月28日（金）10時00分～12時00分

２　場所　オンライン開催

３　出席者

（１）構成員

山本（龍）主査、生貝構成員、上沼構成員、高口構成員、森構成員、山本（健）構成員

（２）オブザーバー

警察庁刑事局、警察庁サイバー警察局、法務省人権擁護局、

一般社団法人ソーシャルメディア利用環境整備機構

（３）総務省

玉田大臣官房総括審議官、下仲大臣官房審議官、田邊情報通信政策課長、

大澤情報流通振興課長、入江情報流通適正化推進室長、吉田情報流通振興課企画官、

武田情報流通適正化推進室課長補佐、菅野情報流通適正化推進室課長補佐

（４）発表者

株式会社野村総合研究所　齋藤氏、尾張氏

４　議事

（１）オブザーバーの追加

（２）今後の検討スケジュールについて

（３）諸外国の制度整備の動向について

（４）意見交換

（５）その他

【山本主査】　定刻になりましたので、デジタル空間における情報流通の諸課題への対処に関する検討会「デジタル空間における情報流通に関わるワーキンググループ」第２回会合を開催いたします。本日も御多忙の中、当会合に御出席いただき、誠にありがとうございます。

まず、議事に入る前に、事務局から連絡事項の説明をお願いします。

【菅野補佐】　事務局です。本日の会議は公開となりますので、その点ご了承いただきますようお願いいたします。

次に、WEB会議による開催上の注意事項についてご案内します。本日の会議はWEB会議システムにて実施しております。会合の傍聴は、WEB会議システムによる音声及び資料等へのみの傍聴となっています。また、事務局において傍聴者は発言できない設定としていますので、音声設定を変更しないようお願いいたします。

次に、本日の資料は本体資料として資料２－１から資料２－３までの計３点となります。万が一、お手元に届いていない場合は事務局までお申しつけください。傍聴の方は、ホームページ上の公開資料をご覧いただきますようお願いいたします。

なお、増田構成員は本日ご欠席の旨を伺っております。事務局からは以上です。

【山本主査】　ありがとうございました。本日の議事は、冒頭にオブザーバーの追加及び今後の検討スケジュールについてご確認いただいた後、株式会社 野村総合研究所（NRI）様からの説明及び質疑の時間を設けています。その後、最後に意見交換の時間を取る形で進めていきます。

それでは、早速議事に入ります。（１）オブザーバーの追加になりますが、開催要項４の（６）「主査は必要に応じ本ワーキンググループの構成員又はオブザーバーを追加することができる」との規定に基づき、資料２－１のとおり、新たにご内諾をいただいた警察庁刑事局、一般社団法人ソーシャルメディア利用環境整備機構にオブザーバーとしてご参画いただきたいと思っております。構成員の皆様、いかがでしょうか。

【一同】　異議なし。

【山本主査】　ありがとうございます。異議なしとのことから、オブザーバーとして両者にご参画いただくことにいたします。

続いて、議事（２）に移ります。今後の検討スケジュールを資料２－２に基づき、事務局から説明願います。

【菅野補佐】　それでは、資料２－２に基づき、今後の検討スケジュールについて説明い

たします。第１回の制度ワーキングにおいて今後のスケジュールを示しましたが、今後の検討に当たり、諸外国制度については制度の内容だけでなく、その実態も深掘りしながら把握をしてまいります。そのため、当初は１回のみの実施予定でしたが、２回に分ける形で実施する予定でございます。今回の第２回制度ワーキングについては、違法情報に関する制度の概要を議題とし、次回の第３回制度ワーキングを諸外国制度の報告２回目として、違法情報・有害情報に共通する対策である軽減措置やエンフォースメント特定の場面に着目した対応について議題とすることを予定しております。また、これに伴い、当初３月の実施予定としていた事業者ヒアリングを４月に実施し、その後、事業者ヒアリングの総括及び論点整理を５月、６月にかけて実施し、夏頃の方向性の整理を目指すという形で進めていく予定です。事務局からは以上になります。

【山本主査】　ありがとうございました。

それでは、議事（３）に移ります。諸外国の制度整備の動向について、野村総合研究所の齋藤様からご発表いただきます。それでは、よろしくお願いいたします。

【NRI_齋藤氏】　ただいま紹介いただきました野村総合研究所の齋藤です。本日は、弊社から違法情報に関する諸外国の対応状況について説明いたします。

タイトルは、資料２－３にあるとおり「違法情報に関する諸外国の対応状況」となります。右上に未定稿とありますが、まさに本日取り上げるDSA・OSAともに施行状況を含めて動いている状況となります。現状版の意味合いとしてご理解ください。

本日の報告は大きく分けて三つです。最初に各国制度の概要という形で、EUにおけるDSA（Digital Services Act）、英国におけるOSA（Online Safety Act）についてそれぞれ説明いたします。その後、違法情報に関する制度及び事業者の対応として、DSA・OSAそれぞれの説明を行います。

まず、３ページの各国制度の概要です。左がDSA、右がOSAになります。最初にDSAから説明します。概要についてはご承知の方も多いと思いますが、２０２４年２月にEU加盟国内で全面適用を開始されています。対象事業者の欄にも書いていますが、SNS等のオンラインプラットフォームサービス事業者、検索サービス事業者等の仲介サービスを提供する事業者が対象となります。違法コンテンツへの対応として、具体的には行政当局への応答や削除申出への遅滞ない応答・通知等が義務づけられています。更には、その運用状況の公表等も義務づけに加え、一般的にVLOP、VLOSEと言われる大規模事業者については、上乗せでリスクを評価・軽減することが義務づけられています。後ほど説明しますが、対象とする違法情報

については、DSAの中ではEU法に反している情報、又はEU法に準拠している加盟国の法律に反している情報としており、DSAの中では定められていません。

次に、OSAになります。こちらは２０２３年１０月に英国において成立しました。３段階に分けての施行となっており、第一の施行で制度面を去年１０月に確定しています。こちらの対象事業者は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となっており、違法コンテンツへの対応として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、更にはその運用状況の透明性報告書の作成を義務づけられています。そのほか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・軽減することも義務づけられています。こちらが対象とする違法情報ですが、テロリズムコンテンツとCSEA（子供の性的搾取・虐待）コンテンツがまず挙げられます。その他、優先犯罪に関するコンテンツも具体的に定義されています。さらに、上記いずれにも該当しないものの、法に触れ個人に被害を与えるコンテンツも対象違法情報として含まれます。

それでは、今申し上げたそれぞれの概要について、５ページで詳しく説明します。まずDSAです。対象事業者についてはこれまでの弊社資料でも説明しているとおりですが、大きく仲介サービスの枠内として、ホスティングサービスにクラウドストレージサービスやSNS、ECサイト、アプリストア、掲示板が含められます。その中で、オンラインプラットフォームサービスにSNS、ECサイト、アプリストアが含まれています。そうした中で、EU域内で利用者が４，５００万人以上、域内人口の１０％以上のサービスについてはVLOP（Very Large Online Platform）として指定を受けています。さらに、下のオンライン検索サービスエンジンサービスについては、いわゆる一般的な検索エンジンが含まれます。こちらも域内人口の１０％以上のサービスについては、VLOSE（Very Large Online Search Engine）という形で指定事業者となっています。

６ページです。先ほど申し上げたDSAにおける対象違法情報ですが、ほかのEU法や加盟国の国内法に委ねているのがDSAの中での定義です。DSAの中では、前文の中での例示にとどまっているところです。こちらの真ん中に前文１２項を抜粋しています。その中で、「例えば」以降に記載あるとおり、児童の性的虐待を描写した画像の共有や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等が具体例として示されています。

７ページです。DSAの各事業者カテゴリに係る規定については、ご参照いただければと思いますが、一番右側のVLOP・VLOSEについては全ての義務が課されているという特徴です。

続いて、英国におけるOSAの概要になります。９ページです。OSAの対象事業者については、ユーザー間サービスのSNS、動画共有サービスと検索エンジンサービスが大きく対象になっています。その中で、大規模なユーザー間サービス事業者についてはカテゴリ１サービスとして定められます。こちらは、まだ基準の閾値が確定していないものの、英国人口の約５０％に相当する３，４００万人以上のユーザーを有するコンテンツレコメンドシステム、もしくは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、レコメンドシステムを有し、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といった閾値が現在提案されています。下の違法コンテンツについては、次のページに詳細を載せています。

１０ページです。オンライン安全法の中では、あらゆる種類の違法コンテンツを対象としていますが、テロ等の優先犯罪を設定し、そちらに関わるものを優先違法コンテンツとしています。そちらについては区別して把握し、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ます。資料の下側に１７項目で示しているものが優先犯罪（Priority offences）の定義です。ここに係るコンテンツが優先違法コンテンツとして定められています。これらの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など、よりプロアクティブな措置がその他の違法コンテンツよりも求められています。

１１ページです。OSAにおけるOfcomの行動規範やガイダンスの発行義務になります。先ほど申し上げたとおり、Ofcomの各種義務は３段階に分けて施行する予定になっています。Ofcomには各段階に応じて行動規範及びガイダンスの発行が義務づけられています。フェーズ１の全てのサービスに課される義務ですが、去年１２月に行動規範とガイダンスが確定されており、今年３月１７日から事業者がリスク軽減措置を講じる義務を負うことになっています。フェーズ２は、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となります。こちらは、去年に行動規範やガイダンスに関するパブリックコメントが公表されており、今年４月から６月をめどにガイダンスが確定予定となっています。フェーズ３は、先ほどのカテゴリ１の大規模サービスに課される義務ですが、こちらについては、現状まだ行動規範・ガイダンス作成のためのエビデンスを募集している段階です。今後、パブリックコメントが今年１月から３月頃までに出る予定となっています。現状ではまだ出ていない状況ですが、今年の終わりに、それを受けて行動規範・ガイダンスが確定予定となっています。本日、主に説明するのはフェーズ１の全てのサービスに課される義務が対象になっているところですけれども、最後に説明する本人確認義務については、フェーズ３の大規模サービ

スのみに課される義務となります。

１２ページは参考です。先ほどのカテゴリ１サービスという大規模サービスについては、追加の義務が課されていることに加え、それ以外のカテゴリ２サービス、その他全般のサービスに係る義務との対照表になっています。ここまでが概要となります。次から２番目の違法情報に関する制度及び事業者の対応について説明します。

１４ページです。違法情報に関する制度については、大きく四つの観点から整理しています。①窓口の設置義務、②違法情報の判断基準、③違法情報の措置方法、④異議申立て方法という形で整理しています。それぞれに後のページで説明していますが、まずポイントを概要として申し上げます。DSAの窓口については、サービス利用者からの連絡を受ける窓口、司法行政当局からの窓口、更にはトラステッドフラッガーからの窓口という三つがDSAの規定上に義務づけられているものです。違法情報の判断基準については、判断に係る具体的な基準は定めていません。これは、そもそも違法コンテンツの定義自体も他のEU法や加盟国の国内法に委ねており、それに伴い判断基準についても国内法に委ねていると推察されます。違法情報の措置方法については、違法コンテンツに対して個人又は団体が容易かつ電子的に報告できる仕組み（メカニズム）を導入し、報告された情報について決定を遅滞なく報告者に通知することや、措置を講じる際に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が義務づけられています。ただ、削除等の具体的な措置方法については指定されていません。さらに、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も義務づけられています。

次に右側のOSAになりますが、サービス利用者からの窓口を設置することが義務づけられています。トラステッドフラッガーについては法律上の規定はないものの、Ofcomから出されている行動規範において、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が推奨されています。後ほどご説明しますが、OSAはDSAのトラステッドフラッガーに指定されている事業者と性格が少し異なります。警察やその他の行政機関について指定されている点がOSAのトラステッドフラッガーの特徴です。違法情報の判断基準については、違法コンテンツのうち、テロや児童の性的搾取・虐待の優先犯罪に係るコンテンツについて、違法コンテンツ判断ガイダンスをOfcomが示し、判断方法のガイドを行っています。違法情報の措置方法は、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、もしくは認識した場合は迅速に削除することを目的とし、設計されたシステム・プロセスを使用したサービス運用が義務づけられています。さらに、優先違法コンテンツにつ

いては存在する期間を最小限にする等の適切なシステム・プロセス運用が義務づけられています。異議申立て方法については、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が義務づけられています。以降、先ほど同様にDSAとOSAにおけるポイントを絞って説明します。

１６ページです。DSAにおいて、先ほど申し上げた通知と行動の仕組みが具体的に１６条と１７条に書かれています。詳細は割愛しますが、ホスティングサービス提供者に対し、利用者が違法なコンテンツの通報を行った場合、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と１６条の中で義務づけられています。

１７ページです。１７条の中で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が義務づけられています。

１８ページです。内部苦情処理体制については、第２０条の中で、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と義務づけられています。

１９ページです。こちらは、DSAにおける命令・通知の窓口整備義務をもう少し分かりやすく整理したものとなります。DSAの方は三つからの連絡窓口を設定することになっています。一番上が加盟国の司法・行政当局からの措置命令・情報提供命令に対応する窓口です。こちらについて、１１条の中で加盟国の当局・欧州委・欧州デジタルサービス会議との連絡窓口を設置することが定められています。トラステッドフラッガーについても、２２条の中でトラステッドフラッガーから来た通知に対し、優先的に不当な遅延なく対応することが定められています。更には一般ユーザーからの通知の対応に対する窓口も設置することが義務づけられています。

２０ページです。こちらは、先ほどご説明した窓口も含め、具体的に違法コンテンツに対する通知や措置命令が出たときのフローを簡単に整理しています。トラステッドフラッガーや当局からの措置命令が来るとプラットフォーム事業者は特定、かつ判断をして措置する形になります。措置をした場合には、情報の発信者に対して、それを行った理由等を通知することが１７条で義務づけられています。そして、情報の発信者については、それに対する異議申立てが２０条を基に可能となっています。

２１ページです。こちらは例になります。当局からの法的根拠に基づく措置命令に対して専用窓口を設けることで優先的に対応を義務づけられている点は先ほど申し上げたとおり

ですが、トラステッドフラッガーからの通知をどの窓口で受けるかというのは、事業者で運用が少し異なっています。例えば左のGoogleの例では、DSA関連窓口を設定しています。ここで、司法・行政当局からの措置命令とトラステッドフラッガーからの通知を受ける形になっています。右はXの例です。司法・行政当局からは法的請求提出サイトで受ける一方、トラステッドフラッガーと一般ユーザーからはヘルプセンターで通知を受けます。このように、運用は事業者によって少し異なります。

２２ページです。こちらは参考になります。TikTokの例ですが、当局からの措置命令の種類を表頭に示し、縦に国を並べています。これまでの傾向としては、ドイツやフランス当局からの措置命令が多いです。また、情報の種類から見るとテロ犯罪に関するものが多いと公開情報のレポートから読み取れます。

２３ページです。次に、DSAの中のトラステッドフラッガー制度です。トラステッドフラッガー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がDSAの中で求められています。具体的には、DSAの２２条の中で今申し上げたことが規定されています。

２４ページです。トラステッドフラッガーの具体的な審査基準については、２２条を踏まえ、今後欧州委員会がガイドラインを公表予定です。現状はまだ公表されていません。ただ、一部の国では先行してガイドラインを策定し、任命されています。下側に青いハッチの部分で示しているものが、アイルランドのDSCが提供するトラステッドフラッガーに関するガイドラインです。こちらの中では、対象となり得る組織や対象となる違法コンテンツリストが定義されています。

２５ページです。もう一つの例になります。フィンランドのDSCの中でもガイドラインが示されています。こちらは、先ほど申し上げたDSA２２条に基づき、専門性、独立性、中立・客観性についてそれぞれもう少し具体的なガイドが示されています。

２６ページです。設置状況ですが、２０２４年５月以降に任命が始まっています。これまで２月上旬時点において１６団体がトラステッドフラッガーに任命されています。

２７ページです。その中身を詳細に見たものがこちらになります。大半はNPOなどの市民団体になっています。主な財政基盤に記していますが、公的機関から資金を調達している団体も含まれています。

２８ページです。こちらは一つの例となります。オーストラリアのトラステッドフラッガーの場合は、プラットフォーム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は全体の４６％ほどを占めています。

２９ページです。トラステッドフラッガーは去年から運用開始された段階ですが、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ます。こちらは去年１１月に行われたウェビナーでの意見交換等の内容を少し抜粋したものですが、リソースの制約に関しては、市民団体が多い点からリソース面での大きな制約に直面しており、資金調達のメカニズム等が必要である、更には人的リソースが確保できない点が言及されています。世間の誤った認識においては、トラステッドフラッガーが違法コンテンツではなく、自分たち又は行政当局等によって不都合なコンテンツを処理しているといった懐疑的な見方が出回っているといった懸念になります。普及率の低さとしては、参加の障壁として負担の大きい要件や明確なプロセスがまだ提示されていない、更には、トラステッドフラッガーになることの具体的なメリットの不明瞭さ等が指摘をされています。

３０ページです。こちらは例になります。簡単に述べますが、欧州議会においてトラステッドフラッガーの任命におけるDSCの政治的な選好の影響について質問が出されています。欧州委からの回答としては、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されます。

３１ページです。更に、ドイツの「Respect!」というトラステッドフラッガーの公的資金への依存に関して中立性の観点から質問が出されています。それに対し、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の回答を出しています。

３２ページです。こちらも参考になります。ドイツの「Respect!」が認可された際の根拠をドイツのDSC認可資料から抜粋しています。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・実績が評価をされ、独立性の根拠はプラットフォーム等事業者との金銭的なやり取りがないことが挙げられています。

３３ページです。先ほど申し上げたとおり、トラステッドフラッガーの運用はまだ始まったばかりであることとレポートの共有時期も相まって、公表情報から読み取れる限りでは、トラステッドフラッガーから各プラットフォーム事業者への通知は多くはありません。

３４ページです。２番目の違法情報の判断基準については、DSAの中で申し上げたとおり、具体的なプロセスは義務づけられていません。事業者は、自社ポリシーに基づいてコンテンツを評価し、違反がなければEU法・各国法に基づき評価を実施するといった大きなフローで行っています。ただ、このフローの中で具体的にどのように行っているかは、事業者によって若干対応が異なるところです。また、その具体的な内容については公開されていませ

ん。

３５ページです。参考ですが、窓口に通知を受けた際の違法性の根拠は、各事業者のポリシーによるものとEU法・各国法に基づくものの割合はサービス事業者によって異なっています。

３６ページです。先ほどの措置方法については、繰り返しになりますが、DSAの中では違法コンテンツに関して削除等の具体的な措置方法は定めていません。

３７ページです。事業者が実施した措置に対して異議申立てを受け付ける仕組みの導入が義務づけられています。具体的に異議申立てをどの程度受け、どれだけ撤回したかで言うと、その割合はプラットフォーム事業者によって若干異なっており、２割から６割程度とばらつきがあります。

続いて、英国における違法情報に関する制度及び事業者へ対応です。３９ページです。こちらは、OSAにおける全般的な安全義務が第１０条の中で定められています。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、設計されたシステム・プロセスを使用してサービス運用することが義務づけられています。先ほど申し上げたとおり、優先違法コンテンツについてはプロアクティブな義務が課されています。その具体的な内容については、下に記載する違法コンテンツに関する行動規範がOfcomから示されており、そこでコンテンツモデレーション等に関して推奨される対策が提示されています。具体的にコンテンツモデレーションについても１０個の項目に分けて軽減措置・行動規範のガイドにされています。

４０ページです。違法コンテンツの報告・苦情受付義務になります。まず、コンテンツの報告については第２０条の中で義務づけられており、苦情受付については第２１条の中で規定されています。こちらも、先ほどの第１０条の安全義務と同様に、その具体的な内容についても行動規範の中で示されています。具体的には、先ほど申し上げたガイドラインのガイダンス、具体の中で報告・苦情という項目において１４の小項目に分けて推奨される措置が提示されています。例として、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等とガイドで示されています。

４１ページです。OSAも窓口の設置義務等についてポイントを絞って説明します。まずユーザーからの通報の受付窓口を設置することがOSA上で義務づけられています。トラステッドフラッガーについてはOSA上で定められていませんが、行動規範の中で、少なくとも詐欺を報告するために使用できる専用の報告チャネルを確立して維持すべきと推奨されていま

す。

４２ページです。こちらは、オンライン安全における今まで申し上げてきたものを含めた違法コンテンツの対応フローになります。大きく一般ユーザーからの受付義務が２０条で課されていることと、トラステッドフラッガーについては行動規範の中で詐欺に関するリスクの高いものについて、警察やその他の行政機関等のトラステッドフラッガーからの通報を受けることが推奨されています。異議申立てに関して情報発信者に対する設置が２１条で義務づけられています。

４３ページです。違法性の判断方法については、違法コンテンツの判断ガイダンスをOfcomが発行しています。右側にガイダンスの章構成を載せており、先ほど紹介した優先犯罪ごとに違法コンテンツの判断方法が提示されています。

４４ページです。ガイダンスの具体なフレームワークについては、一般的な英国刑法にのっとり、コンテンツの違法性を判断すべきとされています。大きく三つ、違法な行為又はその要素があるかどうか、違法な精神状態又はその要素に該当するか、それに関連した抗弁が成立と推測する合理的な根拠があるかをフローにしたがって判断すべきとされています。これについて、具体に優先犯罪ごとのガイドが示されています。

４５ページです。OSAにおける特定の違法情報に関わる特別な対応の内容がこちらです。具体的には、OSAの１２１条の中でテロ及びCSEA（子供の性的搾取・虐待）コンテンツに限り、暗号化された通信を解読する技術等、認定技術を用いてコンテンツについて特定し、削除等の措置の実施を要求することが可能と規定されています。こちらは、現時点で執行事例は確認できていません。

４６ページです。こちらの１２１条の義務については、セキュリティーやプライバシーの観点からの懸念が上がっています。コンテンツの対象は絞っているものの、一方で暗号化された通信を解読する技術等、認定技術を用いた特定であり全てのユーザーの権利を危険にさらす、プライバシーの観点でも危険性があるといった懸念を示されています。

４７ページです。こちらについては、Ofcomが先進的な企業でもエンドツーエンドの暗号化との両立を実現する技術は開発中ですが、２０２３年９月時点では担保されていないと推察される声明が発表されている状況です。更には英国技術大臣のコメントとしても、１２１条を基にしたアクセス権の要求は最後の手段としてのみ行われると発言されています。

最後に、３番目の違法情報の発信を抑止するための方策（本人確認制度）になります。

４９ページです。こちらについては、これまで説明してきた英国OSAの中における本人確認の内容、更には韓国における情報通信網法と公職選挙法の下での本人確認に関連する事象を申し上げます。まずポイントになりますが、英国の背景として、匿名での人種差別や誹謗中傷等に対する懸念の高まりがありました。それに対し、成人ユーザー向けの本人確認のオプションの提供義務が課されています。これは、本人確認の義務づけてはなく、本人確認のオプションを提供することが義務づけられています。こちらは施行に向けて準備中です。ガイダンスをOfcomが策定すると義務づけられていますが、先月の時点でまだ公開されていません。

韓国の例になります。まず情報通信網法ですが、２０００年代に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ったことを受け、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を義務づけると規定されました。現状のステータスは、憲法裁判所において違憲判決を受けたというところで、民間公的機関のオンライン掲示板での本人確認の義務づけに関して、民間事業者向けの本人確認義務規定は削除されています。右側の公職選挙法ですが、こちらは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社会問題となり、その対応策として法制度化されたものです。具体的な義務としては、インターネット報道機関の掲示板やでチャットページにおける選挙期間中の選挙に関する投稿を対象に、実名認証と認証表示を義務づけるというものになります。こちらも、ステータスとしては憲法裁判所において違憲判決を受け、本人確認の義務規定については現在削除されています。

５０ページです。今申し上げたものの補足となります。まずOSAにおける本人確認義務について、こちらは対象となるサービスが非常に大規模なサービスになっています。いわゆるカテゴリ―1サービスになっている点が一つのポイントです。更には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に設定できるツールの提供を義務づけるということで、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オプションの措置と説明されています。

５１ページです。こちらは、本人確認義務が立法化される過程で無料提供にすべきか否かの明確化を求めるといった話やガイダンスの原則策定、認証ユーザーの可視化等が議論されました。無料提供については、結果として無料で提供せざるを得ないため、明文化は不要となっています。また、ガイダンスの原則の策定義務においては、一定程度の柔軟性を基に

して決めるべきとのことから採用が見送られました。更にはプラットフォーム上での認証ユーザーの可視化義務において、プロフィールに未認証と烙印を押すようなことは、正当な理由で本人確認できない人々をネット上で階層化するおそれがあるとのことから退けられました。

５２ページです。参考ですが、ステークホルダーからの意見として、議員、事業者・業界団体、プライバシー・人権団体といったそれぞれの趣旨の団体等から、各立場を基にした意見が上げられています。

５３ページです。続いて韓国の例になります。まず情報通信網法ですが、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サイト運営事業者に対して、利用者の実名による本人確認が導入されたものです。具体的には、ユーザー登録時の本人確認後に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します。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、IDやニックネーム表示で投稿が可能になるといったものが義務化されました。具体的な民間事業者としては、Naver、Pandora TV等が指定されています。

５４ページです。こちらに対する世論の反応と結果としての違憲判決になります。まず、業界団体等から、この義務が課されて運用コストが増加する、更には表現の自由に対する懸念が表明されました。２０１２年８月の憲法裁判所の違憲判決を受け、２０１４年５月改正で民間業者向けの規定は削除されています。判決の中では、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して判断されています。

５５ページです。続いて、公職選挙法の違憲判決になります。背景としては、特定の候補に対するネガティブキャンペーンを防止するため実名認証が導入されました。具体的には、運営事業者がユーザー登録において行政安全部や選挙管理委員会が提供する住民登録番号用いた認証システム、更には信用機関の照合サービスを利用し、本人確認を実施していたところです。ただ、導入後の世論の反発は強く、違憲訴訟を起こされる中で、一部改正されていきました。最終的には２０１５年７月の憲法裁判所の違憲判決を受け、同条は無効化され、２０２１年の改正により削除されました。判決の中では、匿名による政治的表現の規制は、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。その上で、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ことから、全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ています。弊社か

らの説明は以上です。ありがとうございました。

【山本主査】　詳細なご説明をありがとうございました。それでは、ただいまの説明に対する質問・意見を受け付けます。皆様、いかがでしょうか。

それでは、私から少し確認いたします。まず１点目ですが、本日DSAと英国におけるOSAの両方を説明いただきました。どちらも偽・誤情報を正面から取り扱っているというよりも、違法情報又は違法コンテンツかどうかという観点から対応を枠づけているといった理解でよろしいでしょうか。

また、２点目として、どちらも違法情報又は違法コンテンツとされるものについて第三者が削除を要請するものではない。あるいは、事業者としては削除を義務づけられるものではなく何らかの対応を取る。OSAについては、また異なる対応だと思いますが、どちらの場合も削除義務までは設けられていないという解釈で正しいでしょうか。

最後に本人確認義務になりますが、OSAについては本人確認義務を求めるものではなく、本人確認のオプション提供義務を課している。それについても議論が様々あるといったステータスとの理解で合っていますか。これら３点について確認いたします。

【NRI_齋藤氏】　ありがとうございます。まず１点目ですが、ご認識のとおりと我々も理解しています。違法情報について、DSA・OSAの中でそれぞれ対象にしており、その定義についてはDSA・OSAの中で異なっています。偽・誤情報を含むような有害情報がこの制度の中でターゲットになっているわけではありません。

２点目についても、違法コンテンツについて削除を義務づけるものではなく、利用規約又は通知を基に、それぞれの判断をもって適当な対処を取ることを義務づけられていると理解しています。

３点目についても、まさにご説明いただいたとおりです。OSAの中における本人確認というのも、本人確認を義務づけるものではなく、本人確認のオプションを提供するものとなります。それをもって、本人確認をしていない匿名のユーザーとは交流しないことを選べるなど、そうしたオプションの提供となっています。それに対する懸念を含め、種々議論が行われています。

【山本主査】　ありがとうございます。最後のところで１点確認します。本人確認のオプション提供ですが、要は本人確認を自ら行った人のインセンティブをつくっていく、なるべく本人確認を行っていただく方向でインセンティブづくりができないかといった議論になっているという理解でしょうか。

【NRI_齋藤氏】　おっしゃるとおりです。未認証ユーザーからのメッセージやリプライについて、受け取らないように設定できるツール提供義務を課すことになっているため、そうした形のインセンティブが設けられると理解しています。

【山本主査】　現状、インセンティブをどうするかまではOSA上で規定されていないものの、今後どのようなインセンティブを設定していくかはオープンになっているのですか。

【NRI_齋藤氏】　本人確認のオプションについても、Ofcomからガイダンスを策定することが義務づけられているものの、こちらについては現状公開をされていません。その中で、具体の内容や、それに対するものやパブリックコメントが今後課されると理解しています。

【山本主査】　ありがとうございました。それでは、高口構成員お願いします。

【高口構成員】　資料の確認になりますが、スライド３５で窓口から各プラットフォームに通知何件という内容が示されています。ここでYouTube２３万件からX２５万件の措置の全件数が並んでいる一方、スライド３７の異議申立ての対応の件数が書いてあります。これを比較すると、措置の全件数よりもはるかに多い異議申立ての全件数がデータ上に見られます。措置に対する異議申立てが措置件数より大きい点は、窓口に通知が来ておらず、事業者が自主的に措置したものも含めた異議申立ての件数として理解すればよいでしょうか。

【NRI_齋藤氏】　ありがとうございます。これは我々の中でもう少し確認する必要があると認識した上で、基本的にはおっしゃるとおり、事業者の方で判断したものも含めてのレポートの開示になっていると理解しています。

【高口構成員】　承知しました。ありがとうございます。

【山本主査】　それでは、森構成員お願いします。

【森構成員】　ご説明を伺い大変勉強になった次第です。ありがとうございました。同じ問題意識に基づき、我々がイメージするような法制度を二つ作成されている改めて強く感じています。

その上で、スライド１０の優先犯罪に関して伺います。これは非常に重要な指摘であり、共感できる部分も多々ありました。２番目の子供の性的搾取・虐待ですが、日本で言うと児童ポルノに当たるものだと思います。これは日本側のネーミング及び構成要件もおかしいといいますか、本来は２番のように性的搾取・虐待に関する情報をすべきだったものが、なぜかポルノになっていると思うところです。また、もう一つは１２番の親密画像の悪用（inmate image abuse）ですが、これは日本法で言うリベンジポルノになると思います。これら二つのイメージは大体合っているでしょうか。

次に、スライド１７になります。異議申立てにおいて、表題にもあるとおり、発信者に対して明確かつ具体的に説明することを義務づけるとなっています。これは、先ほどの数的な問題もありますが、非常に大変だと思うところで、手間暇的にはどのように実効性を確保されているのかを教えてください。

【NRI_齋藤氏】　ありがとうございます。違法コンテンツに関して、２番と１２番についてはご認識のとおりです。このようなものが義務づけられたときに事業者の方でどのように対応されているかは、あくまでもレポートの方から読み取れる部分になりますが、各事業者が非常に大きなリソースや工数をかけて取り組んでいることが示されています。具体的な内容や対応フローについては公表されていませんが、その対応についてどの程度の工数をかけたか、レポートの作成を含め、この程度の時間をかけたというものは各社の中から示されており、多大なリソースをかけて対応していることはスタンスも含めて説明されていると理解しています。

【森構成員】　承知しました。ありがとうございます。

【山本主査】　それでは、上沼構成員お願いします。

【上沼構成員】　ありがとうございました。非常に大量な情報を整理していただき、大変勉強になります。私からは、行政機関やトラステッドフラッガーなどの命令、申出の効果について確認させてもらいたいと思います。スライド２０のフローのイメージ図に関してです。違法コンテンツのところにトラステッドフラッガーは載っています。先ほどの話では、行政機関からの措置命令はその命令に関して対処する義務ということで、必ずしも削除義務ではないとのことでした。そうすると、結局は自主的な判断に乗ってくるということになろうかと思います。トラステッドフラッガーよりもう少し優先なものが右側にあるのか、左側にあるのかは分かりませんが、トラステッドフラッガーからの通知も、そのような自主的な判断のフロー上に乗ってくるという理解でよろしいでしょうか。

また、そうすると、この判断を仮に誤った場合にはどうなるのか――これはエンフォースメントかもしれませんので、もしかしたら次回とも思いますが。スライド１６では通報内容が明確であり違法性を特定できる場合には違法性を認識したものとみなされるといった記載があります。これは、判断を誤った場合に、事業者自体の責任の根拠となるという趣旨だと思いますが、これも同じような流れになるのでしょうか。それから、関連して同じフローになりますが、もしこのようになると、異議申立ての対象に例えば行政機関やトラステッドフラッガーが該当するのか。少しこのあたりが気になりました。

もう一点は別な観点になります。スライド４４ですが、違法コンテンツの判断基準の中に「責任要件が満たされている」というものが含まれています。犯罪の構成要件としてはそのとおりだと思いますが、これですと、ネット上に流れている情報について、形式的に違法だけれども、上げた人の責任能力がないと対処されないような疑問を持ちました。以上の点についてよろしくお願いします。

【山本主査】　大きく２点のご質問をいただきました。齋藤様、いかがでしょうか。

【NRI_齋藤氏】　ありがとうございます。まずスライド２０に関連する質問への回答になります。１点目の措置のところが事業者の対応であり、トラステッドフラッガー等も事業者判断に基づくものではないかという点では、基本的にご説明いただいたとおりと我々も理解しています。

それから２点目の判断を誤った場合について、当局又はトラステッドフラッガーが誤った場合の対応という理解でよろしいでしょうか。

【上沼構成員】　その逆となります。本来対応するべきところを、自主的な判断の結果、対応を不要と判断した場合という趣旨です。

【NRI_齋藤氏】　それについては、一般ユーザーからの異議申立てがあるというのは説明したとおりです。トラステッドフラッガーと当局からも異議申立てがあるか否かというのは、今の議論だとあるように思いますが、その内容については改めて確認したく思います。

【上沼構成員】　ありがとうございます。エンフォースメントにも絡むものと思いますので、もし次回お分かりになれば、お願いいたします。

【NRI_齋藤氏】　ありがとうございます。それでは２点目への回答に移ります。違法コンテンツの判断ガイダンスにおいて、２番目の違法な精神状態又はその要素における解釈ですが、こちらは今いただいたとおりと思うものの、もう少しガイダンスの中身に具体的にどのように書かれているかを含めてフォローしたく思います。

【上沼構成員】　ありがとうございます。よろしくお願いします。

【山本主査】　今の点と関連して、私の方から伺います。結局、削除義務までは負っていないということで、第三者から要請があったとしても一定の裁量といいますか、判断の余地が事業者側にあるものと理解します。そうしたときに、その後、異議申立てが発信者から来て、ある種責任が問われる可能性もあります。例えばトラステッドフラッガーや行政から削除をするようにと言われ、削除した場合の事業者の責任はどのように扱われるのか。それに従って削除をした場合には免責されるような形になっているのか。それとも、事業者側に判

断の余地があることにより、事業者側が責任を負う形になるのか。その点は、非常に事業者にとって悩ましいと思いますが、いかがでしょうか。

【NRI_齋藤氏】　ありがとうございます。そこは、我々も公開されている情報からだけでは読み取れないところです。一般的に措置命令にしたがって対処した場合には免責になると思うものの、明確にそのような記載はされていません。そこは、どのように対応をしているかを含め、公開情報で取れるものがあるかは少し調査をしたいとは思います。

【山本主査】　ありがとうございます。ここはエンフォースメントを考えていく上で重要です。行政当局から要請があったときにすぐに消すといった対応になると、ある意味での検閲リスクが高まる一方、判断の余地を認めると一定程度の検閲リスクを抑えられるといいますか、事業者がそこでもう一回判断をすることで抑えられる。しかし、事業者の負担が非常に大きくなる。ある種のジレンマが考えられますね。行政から言われたらすぐに消すことは、よい点もあれば検閲の問題もある。大変悩ましいところですが、このあたりはそのような課題があるという理解でよいですか。

【NRI_齋藤氏】　事業者のレポート等からは、非常にリソースをかけて対応していることは既に明示されています。今おっしゃられたとおり、一定のジレンマが発生している点は、VLOP等の実際の透明性レポートからの対応を見ても読み取れ、まず自分たちのガイドラインやポリシーにのっとって判断をしていると考えられます。その上で、違反が認められた場合には社内弁護士や法律・顧問等に相談を実施し、EU法・各国法に基づく判断を行うフローになっています。先ほどの話に切り替えると、一定程度の検閲に対する距離感は置きつつも、その上での判断を求められる点では非常に負担が大きいものにはなっているという理解です。

【山本主査】　ありがとうございます。後ほどの意見交換、又は今後のWG等でもこの点は議論になると考えます。更に詳細が分かれば、またご報告いただければと思います。それでは、生貝構成員お願いします。

【生貝構成員】　大変丁寧な調査とご説明をありがとうございました。私の方からは３点ほど伺います。また、可能であればこの後も詳しくお調べいただきたく思います。

全てOSAに関するものですが、まず１点目は、先ほど山本龍彦主査からもあった偽・誤情報への対策がスコープにどの程度入っているかに関して、本日ご紹介いただいていなかった部分になりますが、OSAにおいて、１７９条でそれ以降に様々な新しい犯罪の類型が作られています。その中に、１７９条でいわゆる虚偽通信罪、他人に深刻、non-trivialな危害

を与えるような虚偽の情報を、それと知りながら発信することについて犯罪と位置づける改正が行われています。去年の夏の英国の暴動でも、プラットフォームの義務が施行される前であるため、発信者自身に対してとなりますが、実際に適用される例も生じています。私も犯罪の詳細に関して十分に把握しているわけではありませんが、１７９条と世界的に、あるいはここで議論されている偽・誤情報の問題がどの程度重なってくるのかをご存じであれば教えてください。

それから２点目ですが、スライド３８以降、OSAの違法情報に対する様々な義務の１０条以降を詳しく扱われています。その前置きとして、第９条においてオンラインサービスの提供者が違法なコンテンツに関するリスクアセスメントを行う必要がある。そして去年１２月にOfcomからこのリスクアセスメントについてのガイダンスが出され、今年３月までに各サービスプロバイダーはそのリスク評価を完了しなければならないとされています。この第９条と第１０条以降の義務の関係について、もしご存じのことがあれば教えてください。

それから３点目ですが、こちらは少し各論となります。先ほど森構成員から挙げられたリベンジポルノやディープフェイクに関して、OSAの中で１８８条に親密な画像の共有についての新しい犯罪が設けられています。その中では、そういった行為を行っていると見えるようなものを含むような形で非常に広めの定義に見えます。恐らく生成AI等を使ったディープフェイクの問題にも一定程度対応しようとされていると思いますが、この定義というものが、果たして日本の児童ポルノ防止法などと比べてどの程度の差異があるのか。この点も先ほどの論点との関係では重要になってくると感じます。以上３点となります。

【山本主査】　ありがとうございます。今の段階でお分かりの部分を回答いただきたく思います。

【NRI_齋藤氏】　ありがとうございます。まず１点目の１７９条で追加されている点は把握していますが、その内容と偽・誤情報がどこまで重なっているのかは、もう少し我々の方でも追加調査を行い、次回ご報告できればと思います。１５４条の中で偽情報に関するコミッティを設けること等も規定されていたと思いますので、そのあたりとの関連も含めて把握できればと思います。

そして、２点目についてはおっしゃるとおりです。その内容については次回ご報告しますが、まずOSAは、前提として自分たちのサービスとそのリスクを特定することが義務づけられています。それに伴い、しかるべき軽減措置を講じることが大前提となっているところで、

そのフローや具体的にどのような軽減措置に関しては、本日一部コンテンツモデレーションなど報告について例示しましたが、１２月に出されたガイダンスの内容を含め、具体的なステップ、リスク評価の方法についてご説明できればと思っています。

それから３点目の日本の児童ポルノとの差異ですが、この点はまだ見切れていないため、次回に向けて見ていきたく思います。ありがとうございました。

【生貝構成員】　ありがとうございました。私も勉強したく思います。それから追加で１点伺います。先ほど上沼構成員から上げられた削除義務に関して、これは国内法マターになってくるため複雑なところもありますが、例えばドイツのSNS対策法などでは、まさに国内法の中である種の違法コンテンツに対する削除を義務づけるという形で規定していると思います。その削除の義務づけに関しても、国内法との相互関係を併せてDSAの方で特に見ていく必要があると思いました。以上です。

【山本主査】　ありがとうございました。それでは、山本健人構成員お願いします。

【山本健人構成員】　ありがとうございます。大変勉強になりました。トラステッドフラッガーに関するDSAとOSAの立てつけについて１点お伺いします。DSAでは、行政機関とトラステッドフラッガーが分かれている仕組みになっているのに対し、OSAはトラステッドフラッガーとして行政機関を指定していると理解しました。OSAにおいては基本的には行政機関をトラステッドフラッガーという形で指定していくという仕組みにしているのでしょうか。それとも、今後はDSAのように行政機関以外もトラステッドフラッガーに指定する運用になっていくのでしょうか。行政機関とトラステッドフラッガーを分けるか否かでその後の対応義務に差を設けるなど、様々な制度上の立てつけのアレンジが可能な印象も持っています。もう少しこの点についてご教示いただけると助かります。

【NRI_齋藤氏】　ありがとうございます。まずトラステッドフラッガーについては、ここを行政当局と設定しているというよりも、あくまでも警察やその他の行政機関で、英国家犯罪対策庁等が含まれています。かつ対象を詐欺に関するリスクについて絞っており、非常に限定的といいますか、特定なものについてのトラステッドフラッガーとして設定されています。また、OSA上の条文ではなく、行動規範上でそれに対する窓口を設置すると推奨されています。その位置づけを含め、DSAとは異なるところです。これを増やしていくことは現状においては、あまり読み取れないものと思っています。

【山本健人構成員】　ありがとうございます。そうすると、OSAとDSAでトラステッドフラッガーという同じ言葉を使っていても位置づけはだいぶ異なるという理解でよいでしょう

か。

【NRI_齋藤氏】　そのように理解しています。

【山本健人構成員】　ありがとうございました。

【山本主査】　それでは、森構成員お願いします。

【森構成員】　質問というよりも感想に近いと思いますが、少し申し上げます。先ほど山本龍彦主査が上げられた免責の話は非常に重要だと思います。情報空間型ではないマッチング型、取引型の方ですが、DPF消費者保護法では内閣総理大臣の削除要請に対する免責、削除した場合の民事免責は規定されていたと思います。そういうものがあってよいかというのは難しい話だと感じますが、正直なところ、私はDPF消費者保護法のような免責規定があるべきものとは思えませんので、その点については慎重に考えていく必要があると思います。まず削除要請を受けたときに、当然ながらプラットフォームとしてはその情報について知るわけです。法的な考え方をすれば、その時点からもしかしたらプラットフォーム自体に削除義務が生じるというパターンもあると考えます。一方、今度は言われるままに削除をした場合、誤った検閲にならないかという方ですが、これも行政機関、トラステッドフラッガーが真面目に要請をしているため、違法情報であることに自信を持っていると思うものの、右から左にとなれば一定の危険はあると思いました。

それから２点目は、全体に戻りますが、本日ご説明いただいた中で留意すべき点として重要と思うものを四つほど申し上げます。一つ目は、DSAにおいて違法情報の違法性は他の法令に委ねられているとの説明でした。スライド６や１４だったと思いますが、これは我々もそのように考えているわけで、そういう考え方でよいと改めて確認できたと思います。二つ目は、先ほど少し申し上げた優先犯罪というものが列挙されているところで、優先犯罪という和訳で正しいかは不明ですが、これも重要なポイントだと思いました。三つ目は、DSAもOSAもトラステッドフラッガーのみならず、司法・行政窓口がしっかりとある点で、もちろん検閲等の問題はありますが、違法情報、特に公法上の権利侵害情報ではないものがあってもそういう窓口があるべきで、その迅速化・透明化の要請があることを改めて教えてくれたものと思います。四つ目は、トラステッドフラッガーの独立性です。スライド３１、３２で公的資金が投入される場合の独立性の話がありましたけれども、これは日本でもファクトチェック等の関係で問題になっていたことです。これもバランスの取れた考え方をしないといけませんが、あまりに厳しく行うとどこも機能しなくなる問題もあります。そうした点で示唆を与えてくれるものでした。この四つは、私としては留意事項と思いながら伺ってい

た次第です。ありがとうございました。

【山本主査】　ありがとうございます。我々として深堀りしていくべき事項についてご示唆をいただきました。今の森構成員の留意事項について、齋藤様から何か付け加えるものはありますか。

【NRI_齋藤氏】　ご指摘いただいた点は非常に重要なものとして我々も理解しています。特に１点目の免責に関しては、次回のテーマに直接的にかかるものです。執行の部分の中でどのように運用されているかを深掘りし、情報の精査を行いたいと思います。ありがとうございました。

【山本主査】　ありがとうございます。

【森構成員】　ありがとうございました。追加になりますが、検閲との関係する余談になりますけれども、インターネットホットラインセンターで公法上の違法について削除の対応要請をする場合、これは警察庁の受託事業ということで検閲問題になります。しかし、非常にシビアな判断の下で行っており、かつて私が手伝っていた頃の運用としては、削除要請の文言の中に、「消すことについて違法情報かどうか不安を感じられるかもしれませんが、これは専門的判断を経たものであり、異議申立てがあった際には、ホットラインセンターからの削除要請に基づいて対応したことが一定の抗弁になるはずです」という旨を書いてお送りしていました。現在という話ではありませんが、よいかどうかは別として、そのようなことを行っていた次第です。以上になります。

【山本主査】　非常に重要な追加情報をいただきました。ありがとうございます。それでは、生貝構成員お願いします。

【生貝構成員】　今のところに関連して申し上げます。誤った削除あるいは削除しない判断をした際の異議申立てを含む手続に関して、DSAなどではスライド１７に記載ある説明と次のスライド１８にある内部苦情処理体制の提供にて説明いただいていますが、その後の２１条に内部苦情処理システムの判断でも不服があった場合には、いわゆる裁判外紛争処理のシステムを利用できるようにしなければならない義務が定められています。実際に裁判外紛争処理機関について複数の認定をされ、欧州委員会のホームページにも公表されています。もしかすると、この法律の立てつけではそういった手続まで含めた免責の在り方を評価する必要があるように少し感じた次第です。

【山本主査】　ありがとうございます。責任の問題において、行政機関も要請をするとなった際に、行政機関の責任がどうなるのか。あるいはトラステッドフラッガーの責任も含

めて考えていくのか。一方、あまりにも責任を重くし過ぎると萎縮する面も考えられます。表現の自由を保障する関係で、このバランスをどのように取っていくのかも非常に重要です。今後お調べいただくことがあれば、ぜひよろしくお願いいたします。

それでは、齋藤様からの報告に対する質問は一回りしましたので、（４）の意見交換に進みます。引き続き、齋藤様も参加されますので、先ほどの発表を踏まえ、皆様からご意見等をお願いできればと思いますが、まず私の方から少し確認をお願いします。第三者がプラットフォーム事業者に対して要請ができるとなっていますが、そもそもDSAの行政当局というのは一体誰なのか。例えば、行政当局のところですが、ある法令に違反していることについて判断する適格性がない、全く専門的な知識がない行政機関がプラットフォーム事業者に対して強く要請できるとなれば、濫用される可能性もあります。そうした点で、要請できる行政当局がどのように絞り込まれているのかを伺います。

それから２点目は、トラステッドフラッガーの信頼問題として、先ほどから様々な議論が出てきているところです。トラステッドフラッガーに対する信頼をどのように担保しているかに関わるのですけれども、DSAの場合、DSCがトラステッドフラッガーを指定する立てつけになっていたと思います。そうした際に、トラステッドフラッガーを指名するDSCがどのような存在なのかは重要だと思います。特に政府との距離感、あるいは政府からの独立性ですが、Ofcomのようなものがだとすれば、一定の独立性が担保された組織がトラステッドフラッガーを指定していると思うところで、このDSCという存在について少し教えてください。

それから、OSAに関しても、先ほど山本健人構成員からあったように、トラステッドフラッガーは性質が異なるものでありながらも存在している点で、これについてどのように指定がなされるのかを伺います。

最後に、トラステッドフラッガーをモニタリングする仕組みがあるのか。何かそうした仕組みとして用意されている、あるいはトラステッドフラッガーと一旦指定をしたものの、あまり信頼できないという存在に対しては指定を撤回・取消しするといったものがあるかを教えてください。長くなりましたが、以上です。

【NRI_齋藤氏】　ありがとうございます。まず１点目の行政当局とはどのようなところかですが、通知を実際にどこから受けたかというのは公表上のレポートからは読み取れません。スライド２２のTikTokの例になりますが、どの国の当局からどのような種類の情報を受けたかというのは出ているものの、それが具体にどの当局だったのかは出ておりません。こ

れは推察ですが、ドイツとフランスが多いというのは、ドイツであれば、もともとあったネットワーク執行法が置き換えられているため、それを所轄していた当局からの通知が多いのかなと思われます。さらに、フランスについてもAvia法のところでARCOMやCSAからの監査を設定するとされているため、そうした当局からの指定が多いと考えますが、具体的にどの当局からの措置命令が多いのかまでは公表されていません。

次に２点目のDSCについて、本日の資料には含めていませんが、基本的に各国で通信系の行政当局が指定されている場合が多いです。ドイツの例だと先ほどのところですが、連邦ネットワーク庁がDSCになっており、フランスの場合もARCOMが設定されています。その距離感は国によって若干異なりますが、そのような機関がDSCを担っている場合が多いです。

次に３点目のトラステッドフラッガーの監視制度について、現状そこまでは読み取れません。モニタリングをする仕組みがあるかは追加で調査を行いたいと思います。

【NRI_尾張氏】　補足いたします。DSAの中に条項があり、トラステッドフラッガーからは少なくとも年に１回報告書を公表するというものがあります。その中で彼らの働きぶりについてある程度の透明性を確保できると思います。一度DSCからトラステッドフラッガーの地位を付与されたとしても、場合によっては取り消すことも可能ではあるようです。一度付与をされたから万全というものではなく、働きぶりを見られた上で、場合によっては取り消される可能性もある点を申し上げます。以上です。

【山本主査】　大変よく分かりました。ありがとうございます。私が当局のところで少し気になったのは、例えば景品表示法に違反していることに対し、消費者庁が削除等を要請することは想像できます。一方、極端な話として、景品表示法違反について仮に外務省から削除要請があった場合には、プラットフォーム事業者としてはなぜだろうかという話になります。その要請は、的確な情報を所掌する当局からの要請とは違うと思います。これを全部当局として広く認めてしまえば政治的な介入も考えられます。表現の自由に配慮し過ぎかもしれませんが、そうした懸念は持った方がよいと思い伺った次第です。このあたりも、今後何か分かればお教えください。いろいろと大変勉強になりました。それでは、高口構成員お願いします。

【高口構成員】　当局、トラステッドフラッガー、事業者という三つの主体について少しコメントをします。DSAは今１年、OSAは現在進行中で制度整備とのことで、その期間が短いことから今後いろいろと動く前提はあるものの、まず当局について申し上げると、山本龍彦主査が言われた点と少し関連しますが、スライド２２を見ると、国によって措置命令をして

いる分野に非常に偏りがあります。例えばイタリアでは画像の非同意共有で多く措置が出ており、フィンランドだと違法商品に多く措置が出ているというように、国によってどの分野で措置を多く出しているかが結構違います。当然ながら、その国でそういう特徴のある違法情報が多いという見方もできますが、もう一方の見方としては当局の各部局のリソース、スタンスによってどの分野の措置が多くなるかは違うようにも考えられます。ルーマニアであれば、嫌がらせ・脅迫に対しては非常に多く措置が出ているように、こういう制度を日本でも展開する際に、当局側の体制やリソースにも少し留意しておかないと、特定の分野においては非常正確に当局が措置命令を出せるものの、ある分野では手が回らないといった形になればもったいないです。そういう当局側の体制も、このような制度には留意が必要という感想を持ちました。

次にトラステッドフラッガーですが、もちろん始まったばかりであるものの、スライド３３を見ると、一つのTikTokの例ですが通知数はまだ少ないです。通知数が少ないことは問題がないという見方もできますが、一般ユーザーと比較をするともう少し通知があってもよいという印象です。トラステッドフラッガーは非常に有効な仕組みだと思いますが、当然その仕組みを整備するコストがどうしてもかかります。もし日本で検討をするなら、それに見合うような展開ができる制度を考えていかなければいけないと思いました。

最後に事業者ですが、これは資料の読み方を間違えていたらご指摘をお願いします。資料説明を受ける前は、前回の議論において、健全性検討会で「事業者は自分で正誤をあまり検証することができないため、不可能を求めてはいけない」との意見が出されたと論点整理されました。それを頭に入れながら伺っていると、特にDSAに対して、しっかりと事業者が一応判断をしていると感じました。それほど不可能ではない、意外とやれるのではないかと思いつつも、例えばスライド３５を見ると、通知に対する措置の割合が事業者で大幅に違います。Xが９割、Googleも大体８割弱が通知に対して措置を取っている一方、TikTokは通知に対して２割しか措置をしていません。つまり８割は通知が誤り、又は措置する必要がないと判断をされたことになります。これも、一つの見方としては、XやGoogleに通知する人というのは非常にポリシーや法律に精通しており正しく通知しているため、YouTubeやXはそれらにほぼ対応して措置を取っている。一方、TikTokに通知する人というのは全く分かっていないため、TikTok側で検討をした結果措置はしない判断したという見方もできますが、本当にそうなのだろうかと思うわけです。事業者が、どこまでルールで求められる中で実際に正しく措置できているのか。事業者によって通知に対する措置の割合が全く違うため、そのあ

たりは実効性の有無において、今後もう少し見ていくべきです。

あわせまして、スライド３７を見ると、先ほど判断の誤りやエンフォースメントの議論も少しありましたが、今度は異議申立てが来たときに実際に撤回しているかを見ると、これも事業者で相当違います。Instagramは１７％であるため、逆に言えば８割以上は撤回をしていません。その一方、YouTubeは半分以上を撤回しています。その撤回というのは、改めて検討をした結果、最初の措置は少し違う可能性のある判断を行ったと私は受け取ります。そうすると、事業者によって結構対応が違うというのは、当初の措置における正確性が違うという解釈になるのか。あるいは事業者によってスタンスがあり、例えばGoogleは８割通知があれば取りあえず措置をするとし、異議申立てがあればそれは全て撤回するといったスタンス的な問題が影響しているのか。そうしたところが、ルールとしてはDSAがありつつも、実際どの程度理念どおりに正しく事業者が運用できているかは少し見ていく必要性を感じました。このあたりは、今後ヒアリング等もあるかもしれませんので、実際のところをしっかりと見た上でルールを考えていくべきと思います。長くなりましたが、以上です。

【山本主査】　ありがとうございます。今のご指摘は非常に重要なものです。健全性検討会のときから運用が始まったこともあり、深掘りは必要となります。特に実効性や執行の複雑なメカニズムではあると思いますが、そのあたりはしっかりと議論をしなければいけません。高口構成員のご発言について、齋藤様から何かありますか。

【NRI_齋藤氏】　おっしゃるとおりで、議論として重要なポイントであることは理解をした上で、レポート上ではなかなかそこまで読み取るのは難しいところもあります。しかしながら、いただいた論点は重要と認識しますので、少しご示唆となるものがあるかについて我々の方で精査を進めます。

【山本主査】　ありがとうございます。それでは、森構成員お願いします。

【森構成員】　今の高口構成員が指摘された点は、ごもっともだと思います。例えば権利侵害情報が一番顕著だと思うのですが、何かを要請した際に、プラットフォームが対応をしてくれるかどうかはそれぞれ違い、訴訟でなければ受けないといった対応のところもあるわけです。それを違法情報全体に一般化できるかどうかは分かりませんが、当然のことながらトラステッドフラッガーも信頼できるものでないといけませんし、山本龍彦主査が指摘されたように、行政機関も当該法令の所管及びしっかりとバックグラウンドを持ったところからの要請でなければいけません。その間口は絞られるわけですが、一定程度合理的に絞られているという前提であれば、それはある程度ビビットに対応していただかないと、国民

としては困ります。つまり、違法情報・権利侵害情報の弊害が放置されることになるため、ある程度対応をしていただくことが適切と思います。また、今度は反対に、その対応に対して異議を出された場合に最もコストをかけずに済ますのは、そういうものに原則として対応しないといことが楽なわけです。しかし、それは様々な趣旨に反するわけですから、来たものに対しては一旦確認をする。そうすると、どうしても一定の割合で前の判断は少し違っていたというものが出てきます。それにより、ある程度の撤回率も出てくることが望ましい姿だと前提にしつつ、透明化をされていると思います。また、こちらからのコンテンツモデレーションの要請に対して反応が一定以上低い、異議申立てに対して反応が一定以上低いのはなぜかという観点で我々も見ることになると思います。逆に言えば、それを通じて削除要請に対して一定程度しっかりと対応していただく、異議申立てについてもしっかりとした対応を希望しつつ、その透明化が図られているのではないかと思った次第です。

もう一つは、本日あまり議論に上がらなかった点ですが、匿名表現の問題がありました。これも難しい問題ですが、かつては匿名性が非常に違法情報の大きな温床であったことに間違いありません。今でもそういう状況は大きく変わっていないのかもしれませんが、現状で非常に問題の大きなものとして、例えば闇バイトの募集、犯罪集団募集、犯罪実行者募集というものが匿名に隠れてやっているというよりは、本人確認をされたアカウントで譲り受けてやっているわけです。匿名性を奪うことが、あまり違法情報対策として効いていないという問題意識が非常に出てきていると思います。韓国の裁判所の言っていることを見ても、果たして本人確認をすることで強い効果があるのかというのも示されています。そうした意味では、オプションを提供するというのはよいと思いますが、本人確認義務といった話になると韓国の裁判所の判断と同じような結論になるように考えます。以上です。

【山本主査】　ありがとうございます。貴重なご指摘をいただいきました。齋藤様からは何かありますか。

【NRI_齋藤氏】　ありがとうございます。おっしゃるとおり、本人確認のところもオプションとするのかどうかという点で、見解を含め非常に対応が分かれると思い、今回の英国と韓国の例を比較する意味でも示唆になると考えます。

【山本主査】　ありがとうございます。森構成員が言われた透明性の観点も非常に重要だと思います。何かこういう形の立てつけをした場合、それが適正に運用されているかどうかをチェックするといったときには透明性が鍵になっていきます。他方で気をつけなければならないのは、どれぐらい対応をしたのか、あるいは異議申立てにどの程度対応されたかと

いう数字や件数が透明化されても、今まで我々がそれにあまり関心を持ってこなかったのではないかという点です。ですから、透明化されても、それが事業者に対するある種のプレッシャーにつながらず、非常に形式的に透明性が確保されてきた部分があるように思います。その意味では、リテラシーも含め、そういう数字をしっかりと評価する仕組みと言うべきか、社会全体がそういうものに関心を持っていくことをどのようにつくり出すのか。それも同時に重要だと感じた次第です。

ほかにいかがでしょうか。それでは、上沼構成員お願いします。

【上沼構成員】　ご説明を伺っていて思ったのですが、トラステッドフラッガーに独立性を要求するというのは、トラステッドフラッガーが何に対して要請をするのかとも関係してくると思います。トラステッドフラッガーに関する世間の誤った認識が多く書かれており、どこも同じような状況と思いましたが、政府に都合のよいものを削除しているのではないかといった内容が出るのなら、そこに関するものは独立性が強く求められると考えるのですけれども、優先犯罪のような特定のものであれば、そこまで独立性が要求されることもないのだと思います。そうした意味で、構成を考えるときには、なぜその独立性が要るのか、何からの独立性なのかを対象情報と一緒にマトリックスにして考えていく必要があるように思いました。コメントになりますが、以上です。

【山本主査】　ありがとうございます。大変重要なご指摘です。トラステッドフラッガー制度を仮に導入するとしても、先ほどから議論があるように、そのトラステッドフラッガーをどのように信頼できるかという問題は非常に重要です。独立性というものも、ここでは事業者からの独立性とありますが、上沼構成員が言われたように政府からの独立性も重要である一方、事項によって党派性がないような領域については別の観点も重要になってくると思います。全体で適切性を担保する上で、このあたりの議論も不可欠だと感じた次第です。適宜、齋藤様からも何かあればよろしくお願いいたします。

【NRI_齋藤氏】　ありがとうございます。今の点もおっしゃるとおりで、独立性を事業者から、更には政府からも取ろうとするとそれはそれで独立するのですが、一方でリソースの観点であるとか、どのように持続可能なものにしていくのかといったバランスも求められます。条件として、専門性が求められているところで、本当にプラットフォーム事業者からも独立し、トラステッドフラッガーの条件を満たすような専門性を持つ団体はどれだけ該当するのかを含め、運用と照らし合わせると非常にこのバランスのところが悩ましい問題と認識しています。

【山本主査】　ありがとうございます。それでは、山本健人構成員お願いします。

【山本健人構成員】　２点申し上げます。まず１点目は透明性に関するもので、既に出たところとも重なると思いますが、やはり透明性をどのように設計するかは非常に重要な問題です。DSAやOSAの仕組みでは、まさに行政当局やトラステッドフラッガー自体の透明性も必要になる一方、権利侵害情報の申請プロセスに関する透明性も必要のように感じました。どのような情報を権利侵害情報として申請したのかについて透明化をし過ぎると、それにより二次被害が起こり得ます。そのため、そのような被害が出ない範囲で、申請自体が適切であることを透明にしていくといった方向性が必要と感じます。そうした申請プロセス上の透明化のようなものが考えられているのであればご教示いただければと思います。また、透明性において、数字自体の公表は非常に重要ですが、事後的にプラットフォーム事業者の違法性の判断などが適当であったかを評価できる透明性の仕組みを設けることもあり得ると思います。件数自体が非常に多くなると思われるため、個別に検証することは厳しい作業のように思いますが、研究者又は研究機関、あるいは第三者機関などに情報のアクセス権を付与し、判断の適当性・エラー率、判断体制の適正性を確認できる仕組みも有効だと思います。こうした点についても何か議論があればご教示ください。

２点目は、先ほどのトラステッドフラッガーの独立性に関するコメントです。DSAでは事業者からの独立性が強調されている一方、政府からの独立性は特に言われていない印象です。それは持続可能性の観点を懸念しているという理解でしょうか。トラステッドフラッガーの資金問題やリソース問題も指摘されていたと思いますが、持続可能な形でワークしていくために今考えられている問題や、政府からの資金援助がどの程度必要と考えられているのか。これらの点でもし把握されているものがあればご教示ください。特に、今回は偽・誤情報対策というフレームからの検討ではなく、違法情報対策というフレームのため、そうであれば政府から独立性はそこまで意識しなくてもいいように感じた次第です。

【山本主査】　ありがとうございます。意見交換としながらも質問が続いてしまい恐縮ですが、齋藤様の方で把握されているものがあれば、お願いいたします。

【NRI_齋藤氏】　ありがとうございます。プロセスの適格性がどのように担保されているかは、DSA上において現状理解としてはそこまで明らかになっていない認識です。もう少し深堀りしたく思います。一方、OSAの方では、先ほど申し上げたコンテンツモデレーションを含めたガイダンスの中で常にプライバシーに配慮することが明示されています。その上でどのように軽減措置を取るのかを示されているものがOfcomのガイダンスです。そういっ

た意味で、利用者の中での判断も当然生まれる部分がありますけれども、その両面を配慮した措置を行うことはOfcomのガイダンスから読み取れます。

２点目については、もう一度ご質問を伺ってもよろしいでしょうか。

【山本健人構成員】　お聞きしたかったのは、トラステッドフラッガーの持続可能性について現在どのような議論を行われているかです。特に政府援助がある程度必要になると考えられているのかという点です。

【NRI_齋藤氏】　ありがとうございます。このあたりは、単純に欧州と日本の状況を比較するのも難しいところですが、実際に公的資金が入っているような団体が複数任命されていることを含め、あくまでもDSAの中では事業者からの独立性に非常に重きを置かれています。その上で、運用において判断の適切な客観性・専門性を保てることがトラステッドフラッガーの任命条件だと欧州委からも答弁されています。そういった意味では政府及び行政機関からの独立性は、そこまで強固に求められていないのではという認識です。

【山本健人構成員】　分かりました。ありがとうございます。

【山本主査】　時間が少なくなってきましたが、そのほかいかがでしょうか。

それでは、私から伺います。EUや英国の仕組みに対して、この前のバンス米国副大統領の安全保障会議での発言は、偽誤情報対策は検閲的なもので表現の自由を制限しているのではないかといった含みがありました。そうした声も世界的に一定程度出てきている状況だと思います。EUは本日お話があったような仕組みを様々積み上げられてここまできているという中、昨今の状況で、こういった動きに対する評価は変わってきているでしょうか。非常に難しい質問ですので今回でなくとも構いません。また、定性的なものであり答えにくいところもあると思いますが、把握しているものがあれば伺いたく思いました。

それからコメントになりますが、本日の議論で大分解像度が高まったと思います。本当にNRI様及び事務局の皆様に感謝を申し上げます。他方で、本日あまり議論できなかったのは、EUや英国と日本との制度的な違い、文化的な違いになります。例えばDSCのような存在が日本の場合にどこに当たるのか。また、リソースの問題も違いますし、トラステッドフラッガーについても、実証・検証は行っていないものの、日本の場合は市民社会・市民団体の存在感が小さいと考えた際に、日本では誰がトラステッドフラッガーになるのかといった問題もある。こうした文化的な違いも考慮しないと実効性は確保できないように感じます。今後このあたりはしっかり議論を行いたく思います。齋藤様、非常に政治状況に左右される部分があると思いますが、何かお分かりのものがあれば教えてください。

【NRI_齋藤氏】　定性的な内容になりますが、欧州では、フランスと等も含め青少年関連の話がこの文脈で言えば非常に多くなってきています。一方、米国等は大統領が代わって以降、ファクトチェックに対する立場が事業者の中で変わってくるなど、立場や風向きは少し変化しつつあります。その点は、２点目も含め、この関連で取り巻く状況は各国で少し異なるものと理解しています。その点をはじめ、制度的な比較も含めて示唆になるものを少しインプットできるよう進めていきたく思います。

【山本主査】　ありがとうございました。ちょうど時間になりましたが、本日これだけは発言しておきたいといった内容、あるいは、もう一度海外調査のご報告をいただきますので、この点を少しお調べいただきたいといった事項があればお願いいたします。それでは、森構成員お願いします。

【森構成員】　ありがとうございます。一言だけ申し上げます。山本龍彦主査の話にあった市民社会について、日欧で状況は全く違うと思います。トラステッドフラッガーに多分そのようなものが入ってきていると思いますけれども、少しそのあたりに注目していただき、市民社会・消費者団体というものの実態、規模、取組がもしお分かりであれば教えていただきたく思います。よろしくお願いします。

【山本主査】　それでは、生貝構成員お願いします。

【生貝構成員】　ありがとうございます。可能な範囲でお願いできればと思いますが、一つは先ほど少しドイツの例を挙げたように、国内法とのインタラクションになります。ここは違法コンテンツへの具体的な対応において重要なところも出てくると考えます。もう一つは、EUと英国ともにオンラインプラットフォームにおける違法、有害、偽・誤情報に関する制度として時々言及されるものが、いわゆる視聴覚メディア・サービス指令及び英国におけるAVMS規制、２０１８年にもともと対象外だったオンラインビデオ共有プラットフォームが対象に含まれており、その中で、特定の違法コンテンツや人種差別、ヘイトといったものに関する安全措置をプラットフォーム提供者に求めています。これがある種DSAを補完する制度の一つだと言及されることはありますが、あまり深堀りする必要はないものの、見ておく価値があると思いました。以上です。

【山本主査】　ありがとうございます。我々がこの日本で議論を進めていく際に必要な情報があれば、ぜひ今後も提供いただくとともに、可能な限りで本日いただいた意見及びコメント等にフィードバックをいただければ幸いです。本日は本当にありがとうございました。

それでは、最後に（５）その他として、事務局から連絡事項をお願いします。

【菅野補佐】　ありがとうございます。次回の第３回会合については、別途事務局よりご案内を差し上げます。以上です。

【山本主査】　ありがとうございました。詳細な調査をいただいたNRI様に改めて感謝を申し上げます。引き続きどうぞよろしくお願いいたします。

それでは、以上をもちまして、デジタル空間における情報流通の諸課題への対処に関する検討会「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回会合を閉会いたします。本日もどうもありがとうございました。

【終了】