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４回）

１　日時　令和７年４月３日（木）17 時 00 分～19 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
警察庁サイバー警察局、警察庁刑事局、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、
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
京都大学大学院法学研究科　曽我部教授

４　議事
（１）情報流通プラットフォーム対処法の施行について
（２）諸外国の制度整備の動向について
（３）有識者ヒアリング
（４）意見交換
（５）その他

【山本主査】　それでは、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 WG 第 4 回会合」を開催いたします。本日もご多忙の中、ご出席いただき誠にありがとうございます。

議事に入る前に、事務局から連絡事項の説明をお願いいたします。

【事務局】　事務局からご連絡いたします。本日の会議は公開とさせていただいておりますので、ご了承ください。次に、Web 会議による開催上の注意事項についてご案内いたします。本会議は Web 会議システムにて実施しております。傍聴についても同様に Web 会議システムを通じて行われており、傍聴者は発言ができない設定となっております。音声設定を変更しないようお願いいたします。

本日の資料は資料 4-1 から資料 4-3 まで、計 3 点をご用意しております。万が一、お手元に届いていない場合は、事務局までお知らせください。また、冒頭の資料につきましてはホームページ上にも公開しておりますので、そちらからもご確認いただけます。

以上、事務局からのご連絡でした。

【山本主査】　本日の議事についてですが、まず冒頭、事務局より情報流通プラットフォーム対処法の施行についてご説明いただき、その後、諸外国の制度整備の動向について、最後に有識者ヒアリングとして発表と質疑応答の時間を設ける、3 部構成で進めてまいります。

それでは、まず情報流通プラットフォーム対処法の施行について、事務局からご説明をお願いいたします。

【木村補佐】　総務省情報流通適正化推進室の木村です。先生方には日頃よりお世話になっております。

本日は冒頭の時間をお借りして、一昨日 4 月 1 日に施行された令和 6 年改正プロバイダ責任制限法についてご報告いたします。資料をご覧ください。

改正法の内容は既に有識者の皆様にご案内のとおりかと存じますので、簡単にご説明いたします。改正法では、インターネット上の違法・有害情報に対処するため、大規模プラットフォーム事業者に対し、削除対応の迅速化や運用状況の透明化に関する措置を義務付けています。

この改正に伴い、法律の通称も変更され、従来の「プロバイダ責任制限法」から「情報流通プラットフォーム対処法」と改称し、新たなスタートを切ることとなりました。

施行日は、令和 6 年 5 月 17 日から起算して 1 年を超えない範囲内の政令で定める日とされておりましたが、先月 3 月 11 日、施行日を令和 7 年 4 月 1 日とする政令が閣議決定され、4 月 1 日に正式に施行されました。

改正法の施行に際し、省令及びガイドラインの策定を行いました。省令では、大規模特定電気通信役務提供者の指定要件、削除申出に対する判断・通知までの一定期間、運用状況の公表に関する具体的な項目等が規定されています。

併せて、2 種類のガイドラインも公表しております。1 つ目は法律の解釈を示したガイドライン、2 つ目はいわゆる「違法情報ガイドライン」で、どのような情報を流通させること

が権利侵害や法令違反に該当するかを明確化しています。これらのガイドラインには法的拘束力はありませんが、指定対象事業者が本法に基づく対応を進める上で参考となるよう作成しております。また、これらのガイドラインは広く公開されており、指定対象外の中小事業者においても、サービス上の違法・有害情報への対応の参考にしていただける内容となっております。昨年 11 月に開催された本検討会において、有識者の先生方より多くの示唆に富んだご意見を頂戴しました。これらはガイドラインや省令の随所に反映しております。この場をお借りして、改めて深く御礼申し上げます。

今後とも、有識者の皆様のご指導ご鞭撻を賜りますようお願い申し上げます。以上、ご報告を終わります。ありがとうございました。

【山本主査】　本件はご報告事項となりますので、議事を先に進めたいと思います。次に、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よりご説明をお願いいたします。

【NRI 齋藤氏】　野村総合研究所の齋藤でございます。資料 4-2 をご覧ください。第 2 回、第 3 回に引き続き、現時点で整理した違法・有害情報に関する諸外国の対応状況を発表いたします。

まず、違法・有害情報に関するその他の措置で、レコメンダシステムに関する対応です。具体的には DSA と OSA を中心に大きく、背景・目的と制度の概要をまとめています。

DSA の中ではプラットフォーム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等、一定の対応を義務付けています。具体的には利用規約に「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が義務付けられています（27 条）。

また、レコメンダシステムを使用している VLOP・VLOSE には上記に加えプロファイリングに基づかない選択肢の提供を義務付けています（38 条）。さらに、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」が挙げられております（35 条 1 項（ｄ））。詳細は資料をご確認ください。レコメンダシステムが DSA に盛り込まれた背景として、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」において、DSA 及び「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ところです。この声明の中では、市民によるニュースの消費、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て、レコメンダシステムの悪用による偽情報の拡散が問題視されています。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が目指されております。

この背景には 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ます。特に「ケンブリッジ・

アナリティカ事件」等を受けた議論の高まりを踏まえたものと考えられます。

資料では、27 条・38 条を踏まえて事業者がどのような取組をしているかを例として抜粋しています。TikTok ではおすすめフィードの中で書かれている情報が記載されており、具体的にコンテンツがレコメンドされる仕組みに関する主な要素として「ユーザーのリアクション」、「コンテンツ情報」及び「ユーザー情報」が示され、またさらにおすすめする方法に影響を与える他の要素も示されております。

TikTok に表示される内容をコントロールする方法としては、「興味がない」、「フィード更新」、「動画キーワードのフィルター」の機能を使用することが示されております。行政機関の制度の執行状況について、27 条・38 条違反に関する調査状況です。欧州委員会は、SNS のプラットフォームとは異なりますが、AliExpress（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）の 27 条・38 条を含む違反の調査を始めております。

具体的にはレコメンダシステムで主に使用されるパラメータの公開（27 条）、プロファイリングに基づかない選択肢（38 条）の 2 つが提供されていないことが疑われております。DSA の執行支援機関として、欧州アルゴリズム透明センター（ECAT）といわれるアルゴリズム関係のセンターがスペインに 2023 年 4 月設立され、プラットフォームの調査・分析や、科学的研究と将来展望、ネットワーキングとコミュニティ形成につき、DG CONNECT と緊密に連携して活動しております。

続いて OSA のレコメンダシステムに関する対応です。OSA は 3 段階のフェーズに分けて施行する予定となっており、行動規範、ガイダンスの整備がされております。

前回、9 条 10 条でリスク評価と軽減措置、安全義務の中で示していた 10 条 4 項の 1 つとしてサービス機能、安全設計に関する措置を組み込むことを義務付けており、「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時の推奨措置について規定されています。

具体的には安全性指標の作成、安全性指標の内容、テストの環境整備、記録保持、記録の活用です。OSA のレコメンダシステムに関する制度の議論の背景として、主に 2 つ。2019 年 3 月オンライン危害に関する白書での記載されており、エコチェンバー・フィルターバブルの発生が言及されています。これは、ユーザーが反対意見を持つ他の情報源を見ないことで情報が偏る可能性や、特定のストーリーが実際よりも広く認識されることを示しています。

もう 1 つの背景は、法案が提出された後の議論において、2022 年 3 月に下院の修正議論が延期された点です。この中で、レコメンダシステムのメリットがユーザーにとっての利点として研究され、一方で有害コンテンツが増幅されるという点についても言及されています。特に、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がリスクを生み出すコンテンツの増幅につながる可能性があることが指摘されています。

また、2018 年には YouTube 上で視聴された動画の 70%以上がレコメンドに応じて視聴されていると懸念しています。

さらに、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（いわゆるパブコメ）では、レコメンダシステムに関する懸念点が寄せられています。ここでは、大きく主体別に整理しており、事業者からはリスク評価義務との関係性や安全性指標の収集頻度、さらに遵守に伴うコストに関するコメントが挙げられています。

また、データ保護機関からは個人情報の取り扱いについての意見、学術機関からは有害性の証拠不足に関する指摘が寄せられています。

レコメンダシステムに関連する内容として、オーストラリアとニュージーランドの偽情報対策に関する行動規範にも記載があります。こちらのページには、コメントシステムの透明性に関係するコメントコミットメントが抜粋されています。

オーストラリアにおいては、利用者がレコメンダシステムに関する一般情報にアクセスできることや、コンテンツに関する選択肢を持つことが成果として記載されています。ニュージーランドについても大まかな法制、内容はオーストラリア同様です。

続いて、収益化停止に関する対応についてご説明いたします。

DSA では、プラットフォーム事業者に対してユーザーに対する収益化の停止措置は義務づけられていません。一方、違法コンテンツや利用規約に反するコンテンツについては、プラットフォーム事業者が収益化停止措置を講じた場合、その内容についてユーザーに通知することが制度上義務付けられています。

こちらの事業者に関する内容を抜粋いたします。YouTube で提供されているガイドラインでは、不適切な言語や暴力等の具体例を挙げており、収益化停止基準を示しています。同様に、X についても抜粋しており、行動基準とコンテンツ基準に分けて、収益化停止の基準に関する記載が公開されています。

参考として、先ほど紹介したオーストラリアやニュージーランドの行動規範に加え、前回触れた欧州の偽情報に関する行動規範も、行動規範レベルで偽情報の流通防止を目的としており、ユーザーの収益化や広告活動に対する事前審査の強化をコミットメントの中で推奨しています。

次に、ユーザーエンパワーメントに関する対応について報告いたします。

まず、DSA において、プラットフォーム事業者はサービスを利用するユーザーが、表示されるコンテンツや広告について自主的に管理できる機能を提供することが義務付けられています。関連条文として、利用規約（14 条）、レコメンダシステムの透明性確保義務（27 条）、広告透明性確保義務（26 条）、AI 生成物等へのラベリング機能の提供に関する 35 条 1 項が示されています。

なお、先ほど紹介した欧州の偽情報に関する行動規範では、ユーザーに対する偽情報の識別支援やメディアリテラシー向上、レコメンダシステムの透明性についてコミットメントが記されています。例えば、生成 AI に関するユーザーエンパワーメントの観点では、YouTube 投稿者に AI ツールを用いて作成したコンテンツを申告させるシステムを設けており、また AI 生成コンテンツを自動的に識別するシステムを Instagram や TikTok が展開している例が

あります。また、X のコミュニティノートを用いてユーザーによる監視や TikTok でのファクトチェック団体による監視も行われています。

続いて、OSA におけるユーザーエンパワーメントに関する規定です。

ユーザーエンパワーメント評価に関する規定は、具体的には 14 条から 15 条にかけて僅かに定められています。対象は第 2 回で説明した、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 サービスとしており、その事業者に対して 14 条義務がかかってきます。このカテゴリー1 サービスは、フェーズ 3 の中で順を追って行動規範やガイダンスが整備されていきます。概要としては、成人ユーザーに関し、ユーザー層の実態や特定コンテンツ、接触の可能性を評価することが義務付けられ、さらにユーザーエンパワーメントに関する機能として特定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をサービスに含めることを義務付けています。

次に、情報発信・流通に態様に着目した対応ついて、具体的にはコンテンツの不正利用に対する規定として、DSA ではプラットフォーム事業者に対し、内容を繰り返し発信し、根拠のない通知や異議申し立てを行うユーザーには事前警告を行った上でサービスを停止することが義務付けられています。これに関する詳細は 23 条 1 項・2 項に記されており、利用規約には不正利用に関する方針を明記することが求められます(23 条 4 項)。YouTube(Google)の具体例としては、動画スパムや何度も投稿される繰り返しコメントに関するポリシーがあり、コミュニティガイドラインにおいて警告の管理についても明記されています。

ファーストストライク、セカンドストライク、ハードストライクといった警告システムがあり、それぞれ期間が設けられています。その他の事業者についても例を挙げて説明させていただいておりますので、ご参照ください。

また、DSA におけるリスク評価や軽減措置に関連して、システミックリスクがもたらす悪影響の例示として bot を利用した情報の流通・拡散についても触れられています(前文 84 項・104 項)。

続いて、特定の場面、具体的には災害やテロに限定された特別対応に関する EU における DSA の対応についてです。

制度の概要として、48 条と 36 条の 2 つの重要な規定が存在します。48 条は、欧州デジタルサービス会議が欧州委員会に対して、危機的状況に関する危機対応プロトコルの作成を開始するよう勧告できることを定めています。

一方、36 条では、危機が発生した場合に、欧州委員会が欧州デジタルサービス会議の勧告に基づき、VLOP・VLOSE に対して深刻な脅威を防止するための適切かつ効果的な措置を講じるよう要求することができると定められています。

この定義については、後ほど改めて紹介いたしますが、48 条と 36 条は、いわゆる危機対応メカニズムに関するものであり、特に 36 条は VLOP・VLOSE に対する規定として理解できます。危機の具体的な定義は示されていませんが、DSA では武力紛争、テロ行為、自然災害、パンデミック等が危機の例として挙げられています。危機の発生及び危機的状況について

は、公共の安全または公衆衛生に対する異常事態を指すことが、36 条 2 項及び 48 条に記されています。

また、DSA においては、VLOP・VLOSE の監督・執行を基本的に欧州委員会が担い、その他の事業者については DSC が監督・執行を担うことが定められています。欧州デジタルサービス会議は独立した諮問機関として、その議長と構成員から成り立っており、48 条についての詳細は、46 ページに記載されています。この内容としては、欧州デジタルサービス会議が欧州委員会に対して危機プロトコルの作成開始を勧告することができます。次のページでも、36 条について同様に欧州委員会は VLOP・VLOSE に対して危機対応の措置要求を行うことができるとされています。簡単なフロー図として整理したものは、次の 48 ページに記載されています。このフロー図では、欧州デジタルサービス会議からの勧告に基づく判断が行われ、欧州委員会が VLOP・VLOSE に対して具体的な措置を要求する流れが示されています。VLOP・VLOSE はその要求を受け、自社サービスが危機に及ぼす影響の評価を行い、その評価に基づいた特定措置を実施することが義務付けられています。

また、欧州委員会に対してその評価・報告を行う必要があります。この報告を受けて、特定措置に関する評価・協議は欧州デジタルサービス会議と欧州委員会の間で行われ、危機対応の期間となる 3 ヶ月以内に評価・報告を行い、必要に応じて延長や内容変更、終了の判断が行われる流れになります。

この特定の場面に限った特別対応の導入経緯としては、ロシアによるウクライナ侵攻に伴い、情報操作への懸念が高まったことが背景となっています。市民団体から、欧州委員会は危機対応を何年も維持する権限が与えられているとの批判を受け、最長期間を 3 ヶ月に設定しました。

執行状況については、2025 年 2 月時点ではこのメカニズムが実際に施行された事例は確認されていない状況です。前述の通り、勧告自体は、欧州デジタルサービス会議の勧告に基づいて行われており、2025 年 2 月末までの各閣僚会議において、36 条及び 48 条に関連する議題は確認されていない状況です。

参考として、先ほどまで説明していた「偽情報に関する欧州の行動規範」の中では、コミットメントに署名した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ます。

次に、法制度の執行権限体制について、DSA と OSA の部分を整理して説明します。過去 2 回の説明と重複する部分がありますので、一部を割愛しながらご説明します。

まず、DSA の執行権限体制について、規定においては 49 条以降に具体的な内容が示されています。規定のフローは、各条項の関係と共に 56 ページに記載されています。

具体的に VLOP・VLOSE に関する部分では、欧州委員会が中心となっており、DSA 違反の疑いがある場合には、欧州委員会が事前調査を開始することが定められています。DSC の協力を得て、事業者に対する強力な調査権限を行使し、最終的には違反が決定されるという流れが支持されています。各国の DSC はそれぞれ任命されており、2025 年 2 月現在で 27 カ国中

25 カ国が任命機関を公表しています。先ほどのフローで使用した各規定についての具体的な概要は、58 ページ以降にまとめられていますので、併せてご参照ください。VLOP・VLOSE に関するシステム管理の義務について、欧州委員会が監督及び執行の権限を有し、DSC と協力して調査権限を行使できることが示されています。具体的な条文、49 条から 51 条や 53 条も 60 ページに抜粋されていますので、こちらもご覧ください。

続いて、DSA の執行に関して、欧州委員会担当の DG CONNECT にヒアリングした内容を報告いたします。組織体制と人員配置についてですが、欧州委員会では DSA の監督と執行に特化した 3 つのユニットが設置されています。

1 つ目は規則遵守の監督・調整を担当するユニットで、約 30 人が所属しています。

2 つ目は DSA の執行を担当するユニットで、約 60 人が従事しています。

3 つ目に経済・技術評価ユニットがあり、これも約 30 人の人員で構成されています。

さらに、2025 年末までに職員数を 200 人まで増員する計画があることも言及されていました。ECAT 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するところで、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を調査、成果を提供しています。

組織の構成については、VLOP・VLOSE ごと、水平的な問題（未成年者保護やオンライン犯罪、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を決定しています。執行のためにアルゴリズム分析、法務、経済分析、法律、ポリシー、経済、データ分析の各分野における専門的な人材を組織として有しています。

事前調査の端緒に関して、定期的なモニタリングにおいては、違法コンテンツ、選挙の完全性や未成年者保護、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されています。特に選挙の完全性に関しては、偽情報が組織的に流通・拡散され、それにより選挙の完全性が危険にさらされていないか等のモニタリングを行っています。

DSA の規則に対する遵守状況の監視には、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)として設けているチャネルを活用しています。また、市民団体からの定期的な報告を活用している状況です。

例えば、フランスの団体が報告した情報を基に調査を開始した事例もあり、このように市民団体の持つ知識は、DG CONNECT の専門知識や活動を補完することができるため、これらの団体との連携は非常に重要です。

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 の下では禁止であり、実際のところ不可能なため、プラットフォーム事業者、ユーザー、市民社会等の利害関係者の間で、オンラインの安全性を強化する責任を分散させることが目的の 1 つとされています。

調査方法に関して 68 条 1 項で示されているインタビューの実施をされることもありますが、現時点ではいずれのインタビューも行われていないとのことです。

調査・分析の対象は大きく 3 つに分けられます。

第1に、通知メカニズムが適切に機能しているかどうかの評価、システミックリスクの評価及び軽減の報告書の内容が適切かどうかの評価、及び対策が行われているかを分析しています。さらに研究者の調査が妨げられていないかどうかの監視と必要に応じた調査が行われます。

執行に関しては、制裁を課すことが目的ではなく、サービスの安全性を高め、利用者の基本的権利を保護することを目的として、欧州委員会がプラットフォーム事業者との対話に関与することが基本的な考えです。欧州委員会が常時監視を行っているといわれますが、これは事実ではないということと、プラットフォーム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やシステム、手順を実施しているかどうか評価していると言及していました。また、個々の違法情報を特定しモニタリングするようなものではないとのことです。

さらに、欧州委員会はデータ分析能力を有するECATと協力し、関連するトピックについてはAPIなど全てにアクセスすることが規定されていますが、異議申し立ても可能とされています。リスク評価に関する執行については、DSAの34条において、有害情報から生じるリスクに対処する一方で、偽情報そのものが必ずしも問題でないことが記されており、条文上は偽情報について明示的に言及はしていません。特に偽情報に対する懸念としては選挙の完全性や公共の安全、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ります。偽情報の拡散が選挙の完全性を損なう場合には評価を行い、軽減措置を講じることが求められます。この一環として、昨年の欧州議会選挙に先立って選挙の完全性に関するベストプラクティスを概説したガイドラインが公表されています。

リスク軽減措置に関する執行では、各種行動規範の遵守がリスク軽減措置の担保に考慮されることに加え、事業者から受け取る監査レポートや市民団体からの証拠を基に対策が不足していることが明らかであれば調査を開始します。

リスク評価・軽減措置義務の違反の評価では、事業者間での対応を比較し、不足している部分が無いかを確認します。その上で、特定の事業者だけが取り組んでいない場合には違反の可能性を判断することもあります。

具体的には、その対策が合理的かどうかや、プラットフォーム事業者の規模に見合ったものか、または効果的にリスクに対処しているかといった観点からの評価が行われます。DSA上では、プラットフォーム事業者が取るべき具体的な対策は規定されていませんが、これは事業者のシステムの変化に対応する必要があるためであり、重要な焦点は、この変化に対して適切に対応しているかどうかであり、この技術の進歩により、コンテンツモデレーションにかかる工数やリソースも大きく変化しています。そのため、特定のルールや方法を指定するアプローチではなく、取られた措置の有効性に焦点を当てるのがDSAのスタンスと言及されています。

さらに、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ことが求められます。欧州委員会が下した決定については、プラットフォーム事業者による異議

申し立てが欧州裁判所で行われる可能性もあると言われています。

Trusted Flagger について第 2 回でも報告したとおり前提として、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ります。また、欧州内での地位・活動は新しいものではなく、DSA が実施される以前から多くのプラットフォーム事業者が市民社会組織や団体と協力して取り組みを行ってきており、その経験に基づき DSA は現在の法的枠組みを提供しています。Trusted Flagger のガイドラインについては 2025 年第 2 四半期に発表予定です。また、昨年下半期に初めて Trusted Flagger の認定を受けたため、今後 Trusted Flagger からの通知が増えていく可能性があるとの意見が担当者から示されています。

最後に、英国における OSA の執行権限・体制について簡単に触れます。

こちらは規定上、91 条から 166 条にわたり規定されています。ここでは、Ofcom が独立した規制当局として役割を担っています。具体的には、政府や議会との関係性の中で対象となるプロバイダに対する執行監督を行うこととなっています。

OSA 違反の疑いが生じた場合、Ofcom が調査を開始します。その後、違反仮通知を発出し、サービス提供者からの意見陳述を経て義務違反と判断される場合には、その違反が確定されるという流れになっています。

情報収集権限については、100 条から 114 条に記載されており、その概要は【資料 4-2】72 ページに示されています。130 条で定められている違反仮通知発出権限について、その具体的内容が 131 条にて規定されています。131 条には、違反仮通知を発することができる OSA 上の条項の抜粋が示されています。

また、133 条では確認決定としてサービス提供者に対して措置要請が可能となり、受け取った場合にはサービス提供者がそれに従う義務を負うことが明記されています。

長くなりまして恐縮ですが、以上が弊社から本日の発表事項の概要となります。ありがとうございました。

【山本主査】　多くの情報があり、EU やイギリスの制度的な仕組みが非常に包括的であり、制度的な資源も豊富で、これらが複雑に絡み合っている様子を感じることができました。ありがとうございます。それでは、予定より少し時間を要しておりますが、30 分程度の質疑応答の時間を設け、その後、曽我部教授からご報告があります。

まず、単純な質問となりますが、制度的な資源が非常に豊富で、さまざまに配置されている状況ですが、この ECAT について、現在どれくらいの人数が働いているのか、そしてその属性について具体的な情報があればお伺いしたいと思います。

【NRI 齋藤氏】　ありがとうございます。こちらのヒアリングの中での言及はなかったのですが、公開情報によれば、30～40 名の職員がいるようです。具体的な能力は、技術的な分析ができる人材が多く在籍していると推測されますので、その中の過半数はそういった分析業務に従事しているのではないかと考えています。

【山本主査】　ありがとうございます。この機関は、欧州委員会の DG CONNECT の 1 機関と

して属しているのか、あるいはある程度独立した形で設置されているのでしょうか。
【NRI 齋藤氏】　ここでは、明確な言及がなかったのですが、1 つ確かなのは、DG CONNECT と緊密に連携して活動しているという点です。その上で、この組織が DG CONNECT の下に位置するのか、独立しているのかについては、確認が必要です。
【山本主査】　ありがとうございます。それでは、いくつかの質問をいただいていますので、森構成員、最初にお願いいたします。
【森構成員】　ご説明ありがとうございました。大変勉強になりました。3 点ほどお尋ねしたいのですが、レコメンダシステムに関して主なパラメータがいくつか 4 ページ等で示されていました。その主なパラメータが何かについて、8 ページを拝見しますと、TikTok のコンテンツがレコメンドされる仕組みについて記載があり、ユーザーのリアクションやコンテンツの情報、ユーザーの情報に基づいているとのことでしたが、これが主なパラメータという理解でしょうか。

それは私の認識は少し異なりまして、データのソースの問題ではなく、ユーザーの属性、つまり性別や年齢、住所等がどのようにプロファイリングされているのかという点がここでのパラメータではないかと考えています。

それはターゲティング時に広告主が性別や年齢、興味をもとに設定するわけで、さらには「ケンブリッジ・アナリティカ事件」があり、メッセージや広告を出す際には怒りに流されるや陰謀論に弱いといったメタな属性が悪用されてしまうことから、提示された情報がパラメータに該当すると認識しておりませんでしたが、主なパラメータについて教えていただければと思います。これが 1 点目です。

2 点目は、6 ページの義務の内容について 27 条 2 項 a の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について記載がありますが、この基準はパラメータとイコールという理解でよろしいでしょうか。

3 点目に、7 ページに関してですが、欧州民主主義行動計画に関する記述があり、SNS のレコメンダシステムが異なる意見を持つユーザー間の対立を深め、世論の分断を助長するという問題意識が示されています。この記述は行動計画やそれに関する声明文のものでしょうか、それとも NRI の分析結果としての記述でしょうか。この点について教えていただきたいと思います。以上です。
【山本主査】　ありがとうございます。それでは NRI 齋藤様、お願いいたします。
【NRI 齋藤氏】　コメントや質問をありがとうございます。まず 1 点目に関してですが、パラメータの部分について、TikTok の例においてはユーザー情報を用いていると記されていますので、ユーザー属性等を活用していることは推測できます。

ただ、その具体的な使用方法については、森構成員がおっしゃる通り、我々が調査した範囲内では把握できていないという状況です。

また、6 ページの 27 条 2 項 a、b に関しても、規定上示さなければならない点については理解していますが、公開情報を見た限りでは、この重要な基準に関しては主要な事業者が示

していることは確認できておりません。調査を進める中で、事業者からDSAにおけるレコメンダシステムに関する基準が明確にされていないという研究も存在しますので、具体的にどう示していくのかについては今後議論、定められていくと推測されることと考えています。

最後に、7ページに関する記述について申し上げますが、行動計画の文面は示されている一方で、上記の背景以降の内容については我々の理解のもとで記載いたしておりますので、欧州委員会の文書等の中で「ケンブリッジ・アナリティカ事件」についての言及があるわけではない旨を申し添えておきます。

【森構成員】　ありがとうございます。先ほどの6ページの27条2項aについてですが、「基準」とありますけど、この「パラメータ」と同義でしょうか。

【NRI齋藤氏】　はい、その認識です。

【森構成員】　わかりました。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。それでは、高口構成員、お願いいたします。

【高口構成員】　ありがとうございます。ご丁寧な説明をいただき、勉強になりました。確認のために、少々細かい点について質問させていただきたいと思います。

現在表示されているスライド番号6、レコメンダシステムに関するVLOPに課されている38条の義務ですが、レコメンダシステムは少なくとも1つの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という内容ですが、このときの「選択肢」というのは、レコメンド方法を複数提示する際に、その中の1つがプロファイルに基づかないレコメンド方法というレコメンド方法の意味なのか、あるいはどのレコメンド方法を選択した場合でも、ユーザーに対して情報を順位付けて提案する際に、プロファイリングに基づかない結果という最後に提示する情報での選択肢での意味、どちらでしょうか。前者のように感じますが、教えていただけると幸いです。

【山本主査】　NRI齋藤様、お願いいたします。

【NRI齋藤氏】　基本的には、我々も前者と理解しています。

【高口構成員】　わかりました、ありがとうございます。

【山本主査】　それでは、山本健人構成員お願いいたします。

【山本健人構成員】　ご報告ありがとうございました。大変勉強になりました。私からは2点質問させていただきます。いずれもDG CONNECTに関連する部分ですので、お答え可能でしたらお願いできればと思います。

まず1つ目は、61ページ目において人員がかなり強化されているという話があり、これ自体は非常に興味深い内容ですが、増強の根拠や理由、具体的にどういった人材が増えているのかについて、もし情報があれば教えていただきたいです。ECATとの連携を考えると、経済技術評価ユニットの役割も含めて、DG CONNECT内にも技術的な知見を持つ人材が増えている印象があり、そういった背景でどのような方々が採用されているのか気になります。

2点目は66ページあたりのリスク軽減措置の全体執行に関する部分ですが、リスク軽減

措置の全体執行について、基本的には柔軟性を持たせて、技術的変化にも早期に対応できるような枠組みを採用していると思います。しかし、事業者がどのような措置をどの程度行えば有効性な措置といえるのか、また執行機関が当該措置の有効性や合理性の評価をどのように行うのかといった点で、十分な明確性が欠けているのではないかという印象があります。そのあたりについての見解や、企業からの反応についてご存知のことがあれば教えていただきたいと思います。以上、2点についてよろしくお願いいたします。

【山本主査】　齋藤様、お願いいたします。

【NRI 齋藤氏】　ありがとうございます。まず、人員や組織体制に関する点ですが、200人までの増強がどのような根拠に基づいているのかについては、ヒアリングの中で具体的には言及されていませんでした。増やしていく人材の具体的な内容についても明言されていないという状況ですが、括弧書きの部分で示しているように、法的サポートや他の専門家を除外した数字としての増強ということになります。そこから類推すると、分析や執行に必要な能力を確保するために人員が増やされるという形が想定されると考えています。

2点目の執行に関するところでは、おっしゃる通り、非常に柔軟性を持たせた枠組みになっています。現在、比較を用いて評価を行っているとのことですが、その基準が明確かというと必ずしもそうではないと思います。ヒアリングの場でも、プラットフォーム事業者からDSA上の明確な基準が書かれていないことという指摘が多数あり、やはりケースバイケースで運用されている一方で、基準が不明確だという不満が寄せられている実態が見受けられます。

【山本健人構成員】　ありがとうございます。特に2点目について、日本で制度を設計する際には柔軟性が必要な一方で、明確性がなければ難しいという点について、どのようにバランスを取るかが重要で気になっていました。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。特に2点目のご質問は、日本で制度を考えていく上で非常に重要なご指摘だったと思います。それでは森構成員お願いいたします。

【森構成員】　ありがとうございます。手短に2回目の発言をさせていただきます。今度は意見としてお話ししますが、皆様方のご意見とも重なる部分があります。6ページに出ていたレコメンダシステムにおけるプロファイリングに基づかない選択肢の提供について、38条に記載されている点が非常に重要だと考えました。ユーザーにこうした選択肢を確保することは、今のさまざまな問題を考える際にも非常に重要です。

2点目は、山本健人構成員からの指摘にもあったECATの執行支援についてですが、この非常に困難なレコメンダシステムの問題を解決するためには、官単独では行えない性質のものだと思います。したがって、特に民間の市民団体や技術者と連携して、しっかりとしたリソースを投入することが重要です。

3点目は、山本健人構成員のご指摘を繰り返す必要はないと思いますが、本当におっしゃる通りだと感じています。以上です。

【山本主査】　ありがとうございます。まだ生貝構成員、上沼構成員からご質問があります

が、私も今触れたレコメンダシステムの件について述べさせていただきます。情報をどう受け取っていくのか、またどのような情報を得るのかということに関して、ユーザーの主体性をどのように確保していくのかは、憲法上でもいわゆる知る自由のような権利とも関連してくる重要なテーマと考えています。これが1点目です。

そして2点目として、ECATのような仕組みは今後さらに重要になると私も感じていますが、リソースをどのように確保していくのかがとても難しい点だと思っております。この点に関して、官民の連携が必要かもしれませんし、公正取引委員会も競争法の観点からアルゴリズムの調査を行うことになるでしょうし、そうした意味で政府が1つの機関を持ち、それを各省庁が共有していく形も考えられるのではないかと思います。これはかなり省庁横断的な取り組みになると思いますが、そのような点についても考慮する必要があると感じています。それでは生貝構成員、お願いいたします。

【生貝構成員】　ありがとうございます。私からは全体的なコメントという形でお話しします。これまでの議論にも出てきた点も含めて、コンプリートな調査をしていただいたことに感謝いたします。このようなテーマを深く研究することは重要であり、3点ほど、日本の制度のあり方について考えた内容を述べさせていただきます。

まず1つ目ですが、前回も少し触れましたが、デジタルプラットフォーム及びその情報空間に関する様々なリスクに対して過不足なく対応するためには、ワンサイズ・フィッツ・オールのアプローチでは不十分です。事業者自身がサービスに適した形でリスクを常に評価し、様々なプレイヤーと協力しながら軽減していく枠組みが非常に重要だと思います。この意味では、デジタルサービス法におけるシステミックリスクのような、広範なアプローチが理想的ではないかと考えています。

他方で、我が国の法制度にしっかりと接合させるためには、ある種の具体化、あるいは細分化を検討する必要があると思います。これまでの発言とも関連する部分ですが、大きく2つの方向性が考えられます。1つは、様々なリスクの中で国としてどれを特に重視し、立法事実としてのリスクと認識するのかを特定し、オンラインサービス法等を参考にリスク評価することです。具体的には、深刻な違法情報への取り組み（接触回避、流通の抑制）や青少年の保護、さらには災害への対応等にリスク評価を具体的に行い、軽減策を講じる方向性が1つです。

2つ目は、このような大きな枠組みであっても、OSAの具体的な行動規範に表れているとおり何を求めているのかは、システムやアーキテクチャ等の対応でかなり明確に特定されている認識であり、それは、レコメンダシステムや収益停止といった行動規範をしっかりと制度の中に落とし込むことで、より明確な制度のあり方を考えることができると思います。このように、両方の方向性が同時に進められるべきだと考えています。

ちなみに、前半のシステミックリスクやリスク評価のアプローチに関しては、先ほど山本健人構成員からいただいたご質問にもあったように、その具体化が必要とされる文脈において、どの制度を参考にするかという観点が重要です。1つの可能性として、日本国内のア

セスメント制度がありますし、さらには、例えば個人情報保護法における安全管理措置や不適正利用に関する規律といった比較的抽象的な文言も参考にする道があるのではないかと感じています。また、労働法の文脈も、こうしたアプローチにおいて近い位置にあるかもしれません。

さらにもう2点、簡潔に述べさせていただきます。前回も申し上げましたが、山本主査のご発言とも深く重なるところですが、こうした制度全体の中でユーザーのエンパワーメントを中心に据える基本的な発想が、DSAやOSAにおいてあるのだと思います。レコメンダシステムやプロファイリングの透明性、変更可能性、ラベリング等、ユーザーの自律的判断を手助けするアーキテクチャを法制度の助けによって実現していくことが求められます。さらに、解決できない部分については、もっとパターナリスティックな対応も検討する必要があるのだろうと思います。

3点目として、ユーザーだけでは透明性と理解、そしてリスク評価が難しい部分において、ECAT のような組織が重要だと考えます。私が知る限り、欧州委員会の中にはジョイントリサーチセンターという、政策に対して独立的な立場から科学的な助言を行う専門の組織があります。この組織は全体で2000人以上の科学者等も含めて雇用しているようですが、その一部を参考にして、日本の現行制度にあてはめる場合、IIPC（International Internet Preservation Consortium）というよりNICT（国立研究開発法人情報通信研究機構）が近いと考えられるかもしれません。このように、政府内部だけでなく、外部の研究機関との連携を如何にして強化し、分析能力を高めていくのかが、山本主査もおっしゃっていた日本版DMAの施行にあたっては公正取引委員会も組織内外に人員含め補強をしておりますが、重要な課題だと思います。

近い将来、日本版DSMやDMAにおいても、同様の協力体制を構築する必要があるかもしれません。それに加え、調査研究機関のみならず、外部の第三者のエンパワーメント、例えば研究者によるデータアクセスや、以前議論したTrusted Flaggerのような仕組みも重要です。制度全体を通じて、ユーザー及び様々な外部の第三者のエンパワーメントをどのように考えていくのかを重視しながら検討を進めることが重要ではないかと思います。以上です。

【山本主査】　非常に重要なご指摘をいただいたと思います。これからの議論においても、ぜひとも参考にさせていただければと思います。ありがとうございました。それでは上沼構成員お願いいたします。

【上沼構成員】　今の生貝構成員の包括的なコメントの後に、前提的な質問となり、これを今頃質問するのは遅かったと少し後悔しています。

まず1つ目ですが、収益停止に関する質問です。20ページには収益化停止措置を義務づける制度はないと記載されていますが、23ページにEUの偽情報に関する行動規範があるとのことで、義務付けはされていないものの、行動規範によって進められると理解しています。そうすると、収益停止措置を取るかどうかは事業者が包括的に決定するが、収益停止措置を

取った場合にはさらに義務が生じるというやや複雑な状況になっているということでよろしいでしょうか。制度に関する非常にプリミティブな質問で恐縮です。

2 つ目は、ユーザーエンパワーメントに関する OSA についてですが、33 ページに記載されている内容に基づきます。成人ユーザーに対するユーザーエンパワーメントについて、有害コンテンツに関わるものの評価を義務づけるとのことですが、特に「特定の特性を持つユーザーへの影響の有無」に関しては、それぞれのユーザーの情報を取得した上で影響評価を行うということになるとかなり踏み込んだ内容になると思われますが、その理解で間違いないでしょうか。

あと、成人ユーザーに対するユーザーエンパワーメント義務の部分で、そのサービスに含める義務や利用可能な機能については、端的に言えば「a.フィルタリング」と「b.警告する」ことかと思います。これは、ユーザー側で機能を選択できるのか、それとも事業者が選ぶのかという点についての確認です。

以上 3 点についてご質問させていただきます。特に成人ユーザーに対する有害コンテンツに関連する部分について非常に興味深く感じております。

【山本主査】　ありがとうございます。それでは齋藤様、お答えいただけますでしょうか。

【NRI 齋藤氏】　ご質問いただきありがとうございます。まず 1 点目の収益停止に関する件についてですが、ご理解いただいている通り、基本的に収益停止措置は義務づけてはいないです。基本的には、利用規約に基づいた対応が必要で、利用規約に違反する場合には、対応説明を通知することが義務付けられています。

また、偽情報に関する行動規範において、流通・拡散防止のために収益化の停止や広告規制に関する事前審査の強化がコミットメントとして記載されており、取り組みとしては推奨されています。これに従った対応を取ることで適切なリスク評価及び軽減措置が講じられるという理解でよいかと思います。

2 点目に、ユーザーエンパワーメントに関する OSA の規定についてですが、こちらはもう少し確認が必要だと考えています。前提として、このカテゴリー1 サービスはまだ施行されていないため、具体的な条項を受けた行動規範やガイダンスが今後出される予定です。それによって、いただいたご質問に対する理解がより深まるのではないかと思っております。

また、特定コンテンツにおけるユーザーへの影響の有無の評価に関しては、特定の特性を持つユーザーへの影響を評価する必要があると記載されています。このことから、本規定は踏み込んだものと考えます。このカテゴリー1 サービスは英国人口の 50%以上を利用する大規模サービスかつコンテンツレコメンダシステムを持つ事業者が対象となっており、その影響力が大きい事業者のみが対象となる前提のもと詳細な規定が設けられていると思っています。

3 点目に関しても、基本的には事業者が提供する内容が中心になると思いますが、ここについてもまだ我々の理解が明確ではありませんが、行動規範等を通じて明確にしていく必要があると考えています。

【上沼構成員】　ありがとうございます。施行がまだ先という理解で承知しました。
【山本主査】　一通りご質問ご意見いただいたかと思います。時間の都合もありますのでここまでとさせていただきます。
それでは、議事の 3 として、有識者ヒアリングとして曽我部教授にご発表をお願いしたいと思います。よろしくお願いいたします。
【曽我部教授】　ありがとうございます。「匿名表現の自由」についてお話しさせていただきます。どうぞよろしくお願いいたします。
前半は匿名表現というものでそのようなものが存在するのかといったものも含めて、歴史をひも解くと、匿名表現は多くの国において当然のものとして認められてきていることをいくつかの視点からご紹介したいと思います。時間が限られていますので、急ぎ足で進めさせていただきます。
まず、現在表示されている内容は、「世界を変えた匿名表現」と題された部分です。歴史的な文書はしばしば匿名・偽名で発表されるということを示しています。また、各国の判例においても、匿名表現が当然認められていることもお伝えしたいと思います。例えば、アメリカの連邦最高裁判所やヨーロッパ人権裁判所の判断から、その匿名性が特にインターネット上において意見を表明する自由な流れを促進する重要な手段という点が述べられています。もちろん、匿名性が大切だとされながらも、譲歩が必要な場合もあるとされています。
次に、日本の憲法学説においても、多くの文献が明示的に言及している訳ではないが匿名表現が表現の自由の一環とされる文献も当然ながら存在します。最近発行された教科書にも、表現の自由は匿名表現にも及ぶと明確に記載されています。
日本の判例では、大阪市のヘイトスピーチ規制条例に関する地裁判決があり、ここでは匿名表現の自由が憲法 21 条 1 項によって保障されていると明言されています。
同じ事件に関する最高裁の判断では、ヘイトスピーチにあたるという市長の認識に関する公表について、表現活動を行った者の氏名や名称を特定するために法的強制力を持つ手段は存在しないという判断が下されました。また、取材源の秘匿も手厚く保護されていると最高裁の判例でも認められています。このほか、市の政策に反対の署名をした市民に対して職員が接触を図るという行為があり、このような戸別訪問は表現者に対する萎縮効果をもたらすことから違法とされた事例があります。
以上が、判例や裁判例に関する部分です。ここから、法規定についても匿名表現に関わるものをいくつか紹介いたします。
まず、政治資金規正法において、22 条の 6 で本人名義の寄附は匿名で政治活動を行うことを禁じています。つまり、匿名での政治献金は許されていないが、この政治献金は政治参加の一環として表現の自由に関わるものだと捉えられます。国会審議においても匿名寄付の禁止に関する質問が出ており、匿名の自由とともに透明性が重要であることが議論されています。ただし、収支報告については一定額以下の少額なものを除き、個々の献金の収支は公開することとされています。それは最低限匿名での献金も認められるべきとの考えが

前提となっていると思います。

次に、公職選挙法における選挙運動の規律についてお話しします。インターネットを利用した選挙運動に関しては、ウェブサイト等を通じて配布される文書には、電子メールアドレスやその他の連絡先を表示することが必要とされています。

また、電子メールで選挙運動を行う場合も、送信者の氏名や名称を表示しなければならないといった規定があります。国会審議でも議論があり、表示義務の違反が表現を萎縮させる恐れがあるため、あえて罰則は設けられていないという説明されています。これは、表現の自由を重んじつつも、責任ある情報発信を求めるという 2 つの価値観のバランスを取るための規制だと理解されます。つまり、表示義務は課せられているものの、罰則は存在しないという形で、このバランスが取られていることがうかがえます。逆に言えば、一定の匿名性の保護が必要とされているという認識も伺えます。

次に、情報流通プラットフォーム対処法の「発信者情報開示」に関する部分にも触れたいと思います。これは、発信者情報が開示されるためには、権利侵害の明白性、また正当な理由が求められています。この趣旨に関しては、総務省の逐条解説等でも匿名表現の保護が挙げられています。

匿名表現は日本の現行法においても一定程度保護または考慮されていることが確認されるというお話をしました。以下は憲法論に関する簡単な説明です。匿名表現の自由には、ある論者が提言するように、発言が本音を言いやすくする効果や、過去の見解と矛盾した表現を行うことが可能なこと、また、発言者の人格を反映しない形での表現ができること等があります。

例えば、女性の発言が真剣に受け止められない傾向がある場合、匿名や変名を用いることでそのバイアスを回避することが想定されます。

続いて、匿名表現に対する制約の合憲性評価について、小向太郎先生の教科書を参考にし、制約のパターンをいくつか示します。

1 つ目は、端的に実名表示を義務づけるという匿名表現の禁止されるもの、2 つ目に、匿名で表現しようとした者が自分に関する情報を開示されるというもの、3 つ目に、匿名で表現する手段が禁止されるようなツールの規制があります。

これらが合憲性の判断をどのように行うかという点について、1 つ目は規制が必要不可欠と考えられるかなり厳格な判断が必要であり、2 つ目は、発信者情報開示の要件を参照し、その必要性を個別に検討し、手続的保障も考慮しなければならないことが挙げられます。3 つ目については、それぞれのケースにおいて個別に検討する必要があります。

最後に個別の場面について、SNS における本人確認と匿名表現との関連性についてです。匿名での書き込みを禁止することが 1 つ目のポイントに該当するのですが、これは韓国において違憲とされている事例もあります。同様に、日本でも基本的にはこの見解が妥当するだろうと考えられます。

また、アカウント作成時に本人確認を義務付けるものの、個別の投稿に関しては匿名また

はアカウント名で良いという形が許容されることについても考慮する必要があります。

匿名表現の自由は直接には侵害されないものの、SNS 事業者による情報開示があれば、匿名性が剥奪される場合があり、この開示が法的手続に基づく場合、違憲とは言えない可能性があります。ただし、アカウントには長期的な発言が紐づくため、アカウント作成は重要な行為となります。

さらに、情報漏洩等のリスクや、漠然とした不安を考えれば、アカウント作成時に本人確認を求めることによる萎縮効果は小さくないだろうと考えられます。

したがって、最小限の確認に留めるべきであり、冗長性を確保しつつもメールアドレスや電話番号の確認にとどまり、例えばマイナンバーカードの確認等、過度の負担は避けるべきと提言します。

さらに、本人確認を行うことで複数のアカウント保有に制約がかかる場合、それを許容できるかどうかも重要な論点となりますが、時間が経過しているため、ここまでで締めさせていただきます。御清聴ありがとうございました。

【山本主査】　それでは、残りの時間を利用し、曽我部教授のプレゼンテーションに対するご質問やコメントを受け付けたいと思います。

まず、私から質問させていただきます。スライドの 5 ページ後半部分について、曽我部教授のお考えはよく理解できました。ただ、「身元を明かさないこと」が誰に対して向けられているのかをもう少し整理する必要があるのではないかと思います。

元々、フェデラリスト・ペーパーズや政治的な古典が匿名だったというお話をされましたが、その際にはパブリックに対しては匿名でも、パブリッシャーに対しては著者は明らかであったのではないかと思います。本が売れたときにはお金を払わなければなりませんし、パブリッシャーは著者が誰なのか把握していたと思うのです。

この意味で、匿名の自由はパブリックに対するものであり、パブリッシャーや媒介者に対しての匿名性は、この段階ではさほど考慮されていなかったのではないかと感じます。この観点から、プラットフォームに対して本人確認を求めることが、匿名表現への直接的な制約ではなく、萎縮効果の問題に留まるのではないかという理解で良いのか、教えていただければと思います。

【曽我部教授】　まず 1 つ、萎縮効果の問題と匿名表現の自由の関係性について考えを述べたいと思います。私は比較的素朴に、両者は同じものを異なる方向から見るものだと理解しています。

つまり、私個人の見解としては、匿名表現の自由が存在するというよりは、萎縮効果によって何かしらの制約がかかるために匿名性が重要だという考え方を持っています。

また、誰に対する匿名という点も当然重要ですが、萎縮効果に基づいて考えれば、連続的な問題で 3 つ考えられます。

パブリッシャーに対しては匿名性がなくても、公権力や公衆に対しては匿名性が確保されるべきだと私は考えています。出版の場合、基本的にはパブリッシャーに対して匿名では

ないものの、権力や公権力に対しては匿名である状況といえます。

後半のアカウント作成に関する本人確認義務についてはパブリッシャーに対しては匿名ではありませんが、公権力や公衆に対しては匿名である状況でそれも匿名表現の問題として扱えると考えます。

【山本主査】　ありがとうございました。私自身のコメントもありますが、先に他の構成員の皆様からご質問を受けたいと思います。森構成員、お願いいたします。

【森構成員】　大変勉強になりました。私が言語化できていなかった部分もすっきりと説明され、全く異なる意見はなく、納得して伺っておりました。些細なコメントですが、最近の話題として、誹謗中傷を想定した発信者情報の開示についてのアナロジーが窺えますが、さらに犯罪実行者募集広告のような深刻な情報も出てきており、広告主の確認等の問題もあるかと思います。

この文脈で匿名表現をこのまま維持してもよいのかという議論があると承知しているのですが、犯罪実行者募集のような場合には、本人確認がなされたアカウントが多いことから、あまり規制効果がないのではないかと思っています。

また、本日の説明の外の話ではありますが、この話から匿名性が破られても仕方がないことという見解が最近の議論においては見受けられる気がしますので、改めて表明しておきます。ありがとうございました。

【山本主査】　今の森構成員のコメントに関して、何かお答えしたいことはありますか。

【曽我部教授】　十分には理解できませんでしたが、広告の文脈では本人確認をせよといった話が広告 WG でもあったと記憶していますが、その問題や違法な広告については、匿名性を確保しなくても良いというご指摘だったのでしょうか。

【森構成員】　広告の文脈では本人確認の要請がかなり強いと思っています。違法かどうかとは別に、憲法に関する専門家の方々の話かと思いますが、広告の性質上、民主主義の維持に関係する程度は低いのかもしれません。広告コンテンツの性質上、本人確認等に基づいて、責任ある広告の発信が求められ、プラットフォームにはその責任ある広告発信と広告主の確認が課せられるべきだと考えています。

それと別に、最近の議論では、有害な情報発信が増えており、例えば犯罪を募る広告でなくても、先鋭的な政治的言論や差別主義的言論等を発信している時にその匿名性によって助長されているといった主張がありますが、これに対しては本人確認済みのアカウントが多く利用されていることが多く、こうした規制が果たして効果があるのか疑問が残ります。

したがって広告に限った話ではなく、最近行われている匿名性が果たしてこのまま維持されて良いのかというこうした議論の中には正確さを欠いているものが含まれていると感じています。

【曽我部教授】　ありがとうございます。まだ少々理解しきれない部分がありますが、今のコメントについてリプライさせていただきます。結局、表現内容と匿名性の保護がどう関係してくるのかという問題が今のコメントに含まれていると思いました。

1つは、そもそも表現の内容が保護領域の外にある場合、匿名性は必要ないのではないかという理屈が成り立つ可能性があると考えます。もう一方で、どんなに常識的に見て有害なものであっても、それが表現の自由の範囲に含まれる限り、内容に関わらず、その匿名性は保障されるべきだと思います。

広告については、元々、内容規制に関しては広告が異なる扱いを受けているため、広告の匿名性は一定制限され、本人確認を求めても大きな問題がないという整理はできるのではないかと思います。

【森構成員】　ありがとうございます。

【山本主査】　今の森構成員の意見についてですが、結局、本人確認義務を求めたところで、有害な投稿が減少しないのではないかという指摘について、何らかのデータが存在するのでしょうか。

【森構成員】　いえ、特にそういったデータはありません。あくまで印象論ですが、曽我部教授のお話からも、誹謗中傷の程度がひどくなってきているのは事実で、そのような状況を前提にして、現在の議論がどう進展しているのかという点については全くおっしゃる通りだと思います。ただ最近は、以前と方向性が変わってきており、例えば日弁連等が匿名性に対する意見を変えて、ある程度の制限がやむを得ないと考える人たちが出てきていることから、状況の変化が彼らに影響を与えているのではないかと思い、そう述べた次第です。データがある話ではないです。

【山本主査】　重要な指摘だと思います。曽我部教授は先ほど、パブリックや公権力に対する匿名性と、パブリッシャーやプラットフォームに対する匿名性は、基本的に萎縮効果という観点から必ずしも区別する必要はないというお話をされていたと思いますが、私は多少違うのかなと感じています。パブリックに対して実名を強制されることは、かなり萎縮効果があると思います。対して、パブリックに対して匿名性が保障されることは、一種の萎縮効果を軽減する要素があると感じます。

もちろん、パブリッシャーやプラットフォームに対する匿名性についても、依然として萎縮効果が見られると思うので、その程度がどのくらいなのかを実証的に考える必要があると感じます。また、森構成員が言われたように、本人確認義務を設けた際にその効果が薄い場合、憲法上違憲とされる可能性もあるため、その点についても実証的な考察が必要だと思います。

【曽我部教授】　今の山本主査のご発言には私も全く同感です。萎縮効果という量的な観点から、パブリッシャーに対する匿名性と一般公衆に対する匿名性は、当然萎縮効果の程度の差はあるかもしれませんが、あくまでも量的な問題として連続的に語ることができると思います。

【山本主査】　ありがとうございます。

【曽我部教授】　つまり、森構成員の言及された効果の問題について、韓国で特に実名制を実施した際にあまり誹謗中傷が減らなかったということを以前読んだ記憶があります。

ただ、やはり現在は場合によっては発信者情報開示をしても辿れないこともありますので、事後的な責任追及が本人確認を通じて促進されるという側面は確実にあるのではないかと思います。以上です。

【山本主査】　ありがとうございます。森構成員、すみませんが、この韓国の事例は、パブリックに対する実名制の強制でしょうか。

【森構成員】　これはパブリックに対するものではなく、特定のユーザーが一定数以上のプラットフォームに対してのことです。

【山本主査】　確認していただいてありがとうございます。それでは、上沼構成員お願いいたします。

【上沼構成員】　実際に詐欺等の問題に関しては曽我部教授が述べたように、「表現の自由の外側」で、その行為を行うためにSNSを用いているという前提があると思います。

そうした場合、責任追及や対応のために、実名登録を義務付ける必要があるという議論が出ているのだと思います。そこで、森構成員が言うように、その点には関係がないというお話であれば、そこで議論は終了するのですが、関係しているかどうかについてのデータが出てこないとなると、対策としうる可能性を否定するのが難しいです。

確かに、SNS内で実名登録が義務づけられると、表現の自由の範囲内での表現に対しても萎縮効果が生じる可能性があるため、それをどう解決するかというジレンマがあるのだと思います。その点についてどうアプローチするかが課題だと考えます。

例えば、プラットフォーム事業者が実名制を採用するという表明をすること自体は問題ないと思いますが、その場合、実名制を採用していないSNSでは、匿名が故に信頼性が低下するという認識が広がることも考えられます。そうした課題についての調整が可能なのかどうか、私は疑問に思いながら聞いていました。そのジレンマのあたりをどう調整すべきかと思っています。ちなみに、話は変わりますが、私自身は複数アカウントの運用をぜひ希望しています。相手によって、見せる顔が異なるのは当然であり、複数アカウントは、これを担保するものだと個人的には感じています。

【山本主査】　ありがとうございます。複数アカウントで表現することは、特にパブリックに対する匿名表現の自由として保障されるべきものであり、自己実現においても大切な要素だと思います。上沼構成員のご発言に対し、森構成員いかがでしょうか。

【森構成員】　ありがとうございます。まさにそのジレンマについては、その通りです。表現の自由の外側にいる人々には、匿名性も保障されていませんし、表現の自由の範囲内にいる人には匿名表現の自由が保障されています。しかし、その一方で、外側にいる人々が混じっているために、全員から一定程度匿名性を剥奪することが許されるのかということが議論されています。また、プラットフォームへの確認が必要になった場合、その信頼性、つまり、プラットフォームが秘密を守ってくれるのか、利用者の情報を不用意に漏らさないのかといった問題も残ります。この観点からも、ジレンマのせめぎ合いのところをこれまでの議論から匿名性を制限する方向に進んでいくのは、私は適切だとは思っていません。

【曽我部教授】　今の話の一部は、現在映っている資料の２つ目の詐欺目的でアカウントを作成する人なんてものは分からない訳で、結局、そうした人々が混ざっている場合、個別の比較を経ずに匿名性を特別に剥奪することになってしまいます。したがって、やはり保護の方向に判断が傾かざるを得なくなるのではないかと思います。
【山本主査】　ありがとうございます。他の方はいかがでしょうか。もし他に意見が出ないようでしたら、少しおさらいをしようと思いますが、今、野村総研の齋藤さんは残っていますでしょうか。本人確認を義務付けてはいないが、本人確認をすることによって得られる特典、インセンティブ設計、ディスインセンティブ設計について、諸外国での議論があったと記憶しています。そのあたりを改めて共有していただくことは可能でしょうか。突然のお願いで難しいかもしれませんが。
【NRI 齋藤氏】　少しお時間をいただいてもよろしいでしょうか。
【山本主査】　ありがとうございます。
【曽我部教授】　今の点については、私が飛ばしたスライドに少しだけ書いてあります。
【山本主査】　そうですか。それでは、曽我部教授から少しお話しいただければと思います。
【曽我部教授】　本人確認を行うオプション機能をユーザーに提供することが義務付けられる法律については、OSA が念頭にあると思いますが、これは結局どういう目的で、どのような機能を提供するかという問題が関わっていると思います。重要な機能を本人確認なしでは使用できないとなると、それは実質的に本人確認の義務付けと同じことになります。したがって、一概には語れないのではないかと思います。どのような目的でそういった規制を設けるのか、もう少し詳細を詰めないと、議論は進みにくいと思います。要するに分からないということです。生貝構成員からご発言があるようです。
【生貝構成員】　ありがとうございます。簡単に感想を述べさせていただきます。まず１つ目は、このページに記載されている本人確認オプション機能の提供義務についてですが、これは別の文脈において、山本龍彦主査たちと議論している青少年保護のための年齢確認義務、すなわちユーザーベリフィケーションに関わっています。アメリカでも年齢を確認するための機能が義務付けられている例がありますので、そうした事例を考慮に入れる必要があると思います。
２つ目は、パブリックではなくプラットフォーマーに対する情報の提供を義務づけるという文脈についてです。これは直接的な関係ではありませんが、ヨーロッパのデータリテンションに関連する規制とも関わりがあると思います。無差別に保存する ID 情報を含め、犯罪訴追の目的のみに使うというような目的の制限についての制度上の問題があった事件も考えられますので、私自身ももう少し勉強しておかなければならないと感じています。
【山本主査】　ありがとうございます。それでは、山本健人さんからコメントをいただき、その後に齋藤さんからの一言をお願いし、最後に曽我部教授からまとめ的なコメントをいただければと思います。山本健人さん、お願いいたします。
【山本健人構成員】　私からは事業者の自由の制約の観点について簡単にお聞きできれば

と思います。オプションではなく、一般的に法律で本人確認が義務付けるが、匿名での書き込みを禁止しないときに事業者の自由の観点がどういう形で出てくるのかという点も気になります。曽我部教授のお考えをお聞きできればと思います。また、義務化が進むと事業者は自由の観点だけでなく、個人情報の管理に関する負担も増えるのではないかと思うので、この点の評価についてもお聞きできればと思います。よろしくお願いいたします。

【山本主査】　ありがとうございます。曽我部教授にお答えいただく前に、先ほどの重要な指摘について補足させていただきます。このインセンティブに関して、本質的なサービスが本人確認をしないと使えないという状況になると、実質的には本人確認を義務付けているのと同じことになります。NRI 齋藤さん、具体的にはどの辺りが議論されているのか、何かあれば教えていただけると助かります。

【NRI 齋藤氏】　第 2 回の議論では、我々の方から、今、曽我部教授からご報告いただいた英国の本人確認制度についてのところをお話ししました。また、韓国の事例も紹介しましたが、英国の制度は本人確認の義務付けではなく、オプションとして提供されているという点での議論がありました。このオプションとして提供されていることが、大きな論点として整理されている認識です。韓国では、一時は認められた部分もありましたが、最終的には違憲判決が出たため、今は義務化されていないとのことです。本人確認の義務づけは確かに難しい議論という理解です。OSA の特徴としてはオプションとして提示していることが大きな特徴というところが比較からも見えてきました。

【山本主査】　ありがとうございます。曽我部さんのご質問は、オプションとして本人確認を望んだ人は何ができるのか、逆に本人確認のオプションを望まなかった人は何ができないのか、その内容によって議論の方向性が変わるのではないかということでしたが、そのあたりについて具体的な議論はできているのでしょうか。

【NRI 齋藤氏】　OSA の中では、ユーザーが本人確認をした人とのみ交流することを選択できる仕組みになっています。つまり、匿名ユーザーと交流しないことを選ぶことができるという説明がされています。

【山本主査】　なるほど、わかりました。ありがとうございます。大変勉強になりました。重要な指摘をいただいたと思います。現在の内容を踏まえ、山本健人さんからのご質問や生貝さんからの包括的なコメント、齋藤さんからのご指摘を踏まえて、最後に何か一言お聞きできればと思います。

【曽我部教授】　ありがとうございます。生貝構成員の指摘について、私から十分に咀嚼できなかった部分があるのですが、開示を行う際に目的によって制御することは当然ありうると思いますので、1 つの着眼点だと考えています。山本健人構成員のご指摘については、オプション機能として本人確認を提供するというスライドには、確かに事業者の自由に関する言及があるのに、本人確認の本体については触れられていないという指摘だと思います。

趣旨として、本人確認を行う以上、事業者には負担が生じますので、事業者の自由という

観点や負担についても考慮しなければならないと思います。その際に重要なのは、本人確認との関係が問題ない場合に次のステップとして事業者の自由の問題が出てくるということです。もし本人確認の問題が大きな論点であれば、事業者の負担の話は影に隠れてしまうことになるので、そのあたりも明記されていなかったのかもしれません。

また、事業者の自由は対策を検討するにあたり常に考慮する必要があります。オプション機能についても、以前議論した偽情報の問題では、著名人に対して本人確認機能を使ってもらうことで、なりすましの発信を防止する等の対策が考えられます。そういった理由から、本人確認機能の提供を義務付けることには有効性があると思います。

ただし、先ほど齋藤さんがご説明されたように、ユーザー間の交流を制限するという点になると、一般ユーザーにとっては本人確認をしないと使いにくくなるという状況が出てくる可能性がありそうです。そのため、私が申し上げたような著名人がなりすましを防ぐための機能提供とは異なり、少し制約度の高い使い方になるのではないかという感想を持ちました。以上です。

【山本主査】　ありがとうございました。すでに定刻になってしまいましたが、特にこの場で何かコメントしておきたいことがなければ、今日の議論はここまでとさせていただきたいと思いますが、いかがでしょうか。

はい、ありがとうございます。それでは、今日はここまでとさせていただきます。最後に事務局からご連絡事項をお願いいたします。

【事務局】　ありがとうございます。事務局でございます。次回の会合につきましては、別途事務局よりご案内を差し上げます。以上でございます。

【山本主査】　はい、ありがとうございます。制度に関しては、本当にNRI様から詳細な報告をいただいたと思います。それを受けて、構成員の皆さんからさまざまなご質問やご意見をいただいたかと思いますので、制度WGの単独での会合が今後いつになるかはまだ決まっていないところですが、大変お手数ですが、事務局の方でコメント等を整理しておいていただけると、次の議論につながるかなと思いますので、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WG第4回会合を閉会いたします。本日もありがとうございました。

【終了】