参考資料WG20－３

「デジタル空間における情報流通の健全性確保の在り方に関する検討会」

ワーキンググループ（第１２回）

１　日時　令和６年４月５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、石井構成員、落合構成員、水谷構成員、森構成員、

山本（健）構成員

（２）オブザーバー団体

一般社団法人安心ネットづくり促進協議会、一般社団法人新経済連盟、一般社団法人セーファーインターネット協会、一般社団法人ソーシャルメディア利用環境整備機構、一般社団法人デジタル広告品質認証機構、一般社団法人テレコムサービス協会、一般社団法人電気通信事業者協会、一般社団法人日本インターネットプロバイダー協会、一般社団法人日本ケーブルテレビ連盟、一般社団法人日本新聞協会、日本放送協会、一般社団法人MyData Japan、一般財団法人マルチメディア振興センター

（３）オブザーバー省庁

内閣官房、内閣府、警察庁、消費者庁、デジタル庁、文部科学省、経済産業省

（４）総務省

湯本大臣官房総括審議官、西泉大臣官房審議官、田邊情報通信政策課長、

大澤情報流通振興課長、恩賀情報流通適正化推進室長、内藤情報流通適正化推進室課長補佐、

上原情報流通適正化推進室課長補佐

（５）ヒアリング関係者

株式会社野村総合研究所　齋藤氏　尾張氏

4　議事

(1) デジタル空間における情報流通の健全性確保に向けた国内外の検討状況

(2) 意見交換

(3) その他

【山本（龍）主査】　それでは、「デジタル空間における情報流通の健全性確保の在り方に関する検討会」ワーキンググループ第１２回会合を開催いたします。

本日は御多忙の中、当会合に御出席いただきまして、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。

【髙橋係長】　事務局でございます。

まず、本日の会議は公開とさせていただきますので、その点、御了承ください。

次に、事務局よりウェブ会議による開催上の注意事項について案内いたします。本日の会議につきましては、構成員及び傍聴はウェブ会議システムにて実施させていただいております。本日の会合の傍聴につきましては、ウェブ会議システムによる音声及び資料投影のみでの傍聴とさせていただいております。事務局において傍聴者は発言ができない設定とさせていただいておりますので、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、本体資料として、資料WG１２－１－１から資料WG１２－２までの３点を用意しております。万が一お手元に届いていない場合がございましたら事務局までお申しつけください。また、傍聴の方につきましては、本WGのホームページ上に資料が公開されておりますので、そちらから閲覧ください。

なお、本日は、曽我部構成員が御欠席予定と伺っております。

事務局からは以上です。

【山本（龍）主査】　ありがとうございます。

本日の議事でございますけれども、デジタル空間における情報流通の健全性確保に向けた国内外の検討状況といたしまして、株式会社野村総合研究所様から御説明をいただき、その後、構成員から御発表いただいて、それぞれの後に質疑の時間を設けるという形で進めさせていただきたいと思います。

それでは、早速議事に入らせていただきます。

まず、ＥＵにおける災害時等危機対応メカニズムにつきまして、野村総合研究所、齋藤様、それから、尾張様より御発表をお願いいたします。御準備のほうはいかがでしょうか。

【野村総合研究所（齋藤氏）】　ＮＲＩ、齋藤です。ありがとうございます。

【山本（龍）主査】　よろしくお願いいたします。

【野村総合研究所（齋藤氏）】　では、資料のほうを投影させていただければと思います。少々お待ちください。

では、発表のほうを進めさせていただければと思います。

改めて、お時間いただきありがとうございます。弊社のほうから、まずはＥＵにおける災害時等の特例という形で御説明をさせていただければと思います。

一応第８回のＷＧで御説明させていただいたＤＳＡの内容ですとか、行動規範の内容等も、重複しますけれども、改めて振り返りつつ、災害時等の特例について御説明させていただければと思っております。

まず、こちらが以前もお示しした資料ですけれども、ＥＵの偽情報に関する政策の全体像といった形で、まずは左上のオレンジの部分、２０１８年の偽情報に関する行動規範のところからスタートしたというところですけれども、それに対する２０２０年の行動規範に対する欧州委員会からの評価と、それに基づく欧州民主主義行動計画、さらには、それを踏まえた偽情報に関する行動規範の強化に係るガイダンスというものを踏まえて、偽情報に関する行動規範の２０２２年版というのが、欧州委員会との共同規制として公表されたといったところと、デジタルサービス法というものが２０２８年から一部ＶＬＯＰ・ＶＬＯＳＥに適用され、今年の２月から全面適用となってきたといった枠組みの中で、全体の政策が仕組みづけられているといったところでございます。

このデジタルサービスアクトと、このガイダンス、さらには偽情報に関する行動規範の中で、危機ないしは災害というものがどういう位置づけになっているのかというのを整理しているのが次のページになっております。

まず一番最初は「デジタルサービス法」で、次が「行動規範強化に関するガイダンス」、さらに、下が「２０２２年版行動規範」といった形になっておりますけれども、まず結論として申し上げますと、危機というものに関する言及は、いずれにおいてもされているといったところであります。

ただし、災害というものに関して言いますと、ＤＳＡの中での前文の中で、危機の具体例の一つとして言及されているといったものにとどまっているというのが、全体の中での言及の度合いといった形になっております。

それぞれの中でどのような位置づけ、言及がされているのかというのは、この後、見ていければというところですけれども、ＤＳＡの中では、大きく第３６条と４８条という、ＶＬＯＰとＶＬＯＳＥに対する追加義務の中で、この危機というものが言及されているといったところが大きなところでございます。

この３６条、４８条といったところが、危機対応措置要求が第３６条、自主的な危機プロトコルの作成開始が４８条というところですけれども、これがどのように危機発生時に権

限が発動されてアクションされていくのかというのを簡単に示したのが４ページのものとなっております。

一番大きなところは、欧州デジタルサービス会議というところのＤＳＡの第６１条に基づき設置される独立諮問機関が、この３６条と４８条に対する勧告をするとなっているといったところでございまして、その勧告に基づいて、欧州委員会が自主的な危機プロトコルの作成を開始する、ないしは危機対応措置要求を取るといったことになっております。

この３６条に基づく要求というのが、ＶＬＯＰ・ＶＬＯＳＥに係るところといったところでございまして、自主的な危機プロトコルを作成するとなった場合には、その協力を要請することができるといったところで、ＶＬＯＰ・ＶＬＯＳＥは、要請に対して応える義務が付されているといったところでございます。

さらに、行動規範の中で規定されている部分を青色で書いているところですけれども、行動規範の中では、常設のタスクフォースというものを持つこととされておりますけれども、その中でリスク評価手法と危機対応システムの確立というのが、コミットメント３７の２項で示されておりますけれども、その内容を踏まえた連携をして危機対応を図っていくというのが大きな枠組みにはなっているところでございます。

それぞれの中でどういった内容が書かれているかといったところを、関連条文を抜粋しているところでございますけれども、その内容を踏まえて書かせていただいているのが次のページ以降になりますけれども、まず危機についての言及については、３６条と４８条にて定義されているところでございます。

危機については、３６条２項の中で、「危機は、連邦内またはその重要な地域において、公共の安全または公衆衛生に対する重大な脅威をもたらす異常事態が発生した場合に発生したものとされる」とされているといったところでございます。

さらには、前文９１の中で、「このような危機は」というところ以降になりますけれども、「武力紛争やテロ行為、地震やハリケーンなどの自然災害、パンデミックや公衆衛生に対する国境を越えたその他の深刻な脅威から生じる可能性がある」といったことが言及されているところでありまして、先ほど申し上げたとおり、危機の中の具体例として自然災害というものが想起されているところでございます。

先ほど申し上げた３６条については、参照になりますけれども、ロシアのウクライナ侵攻に伴い追加された規定であるといったところで、その内容について、一部市民団体からの批判と抗議も踏まえながら、危機対応の期間等が設定される中で、最終的な最終文書が承認さ

れたところが大きな流れになっているといったところでございます。

先ほど３６条の危機対応措置要求と自主的な危機対応プロトコルが第４８条で規定されているといったところでありますけれども、現時点では、これが施行または検討された事例というのは確認されていないところでございます。

欧州委員会のウェブページで公開されているＶＬＯＰないしはＶＬＯＳＥの監視施行に関する情報というところで言いますと、第６６条に基づく情報提供要請が主となっているところであります。

一部、ＭｅｔａとＴｉｋＴｏｋに対して、危機の具体例に当てはまるハマスのテロについての情報要求も出されているところですけれども、これも第３６条に基づく危機対応措置の要求ですとか、第４８条に基づく危機プロトコルの協力要請までは至っていないところでして、あくまで第６６条に基づく情報提供要請にとどまっているといったところであります。

さらには、ＤＳＡに基づいて公開されている透明性レポートが、最新のものですと２０２３年１０月末に公表されておりますけれども、いずれも第１５条、第２４条、第４２条で規定されている内容のみの記載にとどまるというところでして、危機対応措置に関する記載はないような状況になっております。

先ほど申し上げたとおり、この３６条と４８条というのは、欧州デジタルサービス会議の勧告に基づいて行われるというふうに規定されているところでございまして、この欧州デジタルサービス会議というのは、下に概要を示しておりますけれども、第４７条に基づいて設立される独立した諮問機関で、各国の執行機関であるＤＳＣでデジタルサービスコーディネーターと、さらには欧州委員会で構成されるといったところでありますけれども、この会合自体は、これまで２月１９日と３月１５日の２回行われたのみというところで、こちらの会合内容について、公表されている資料ベースですと、３６条、４８条に関連する議論がされた景色はないといったところでありまして、４月にも会合は予定されておりますけれども、今後、ここで議論されるということがあれば、それに基づいた勧告等で具体的な動きが出てくることが想定されるかなといったところでございますけれども、直近の３月時点までというところで言いますと、３６条、４８条の危機対応メカニズムというのが施行または検討された事例というのはないといったところでございます。

以降は、それぞれの逐語訳となっておりますので、御参照いただければというところになります。

ここから行動規範強化に関するガイダンスになりますけれども、こちら、先ほど言及したとおりですけれども、冒頭及びユーザーのエンパワーメントに関わる内容において「危機」についての言及があるというところですけれども、「災害」に関する言及はないといったところになっております。

こちら、詳細は割愛させていただいて、こちらのガイダンスを踏まえて２０２２年版の行動規範が更新されておりますので、そちらの内容に移らせていただければと思います。

行動規範においても、ガイダンスと同様に、「災害」に関して言及されているというコミットメントはなく、「危機」に関して言及されているコミットメントというところで言いますと、具体的には４つあるといったところでございます。

１つが、ユーザーのエンパワーメントの中で、関連署名団体が、公共や社会が特に関心を持つ話題や危機的状況において、利用者を権威ある情報源に導くような製品や機能を設計し、適用するといったことが言及されているところと、コミットメント３５の措置４、透明性センターに関する項目の中で、危機的状況において、署名団体は透明性センターを利用し、危機に関連して講じられた具体的な緩和措置に関する情報を公表するといったことが示されているといったところ。常設タスクフォースに関する部分では、コミットメント３７の中で、選挙や危機というような並列する形で、特殊な状況下といったものが例示されているといったところ。同様に、監視体制の強化、コミットメント４２の中では、選挙や危機のような特別な状況といった形で、並列される形で示されているといった形になっております。

この行動規範については、半年に一度、透明性レポートが署名団体から提出されているといったところでありまして、この具体的な透明性レポートの構成というのは、下記のとおりになっております。

この中で、今申し上げた具体的な危機に関するコミットメントに対してもレポートがあるというところでありますけれども、コミットメント２２と４２については、対応状況への記載に加えて、具体的な対応状況についての各社の具体的な記述があるというところで、それを抜粋してまとめているといったところと、さらには、付録の中で、危機対応状況という形でCrisis Responseという項目が設けられておりまして、その中で各社が具体的にどのような対応を行ったのかというのが記載されておりますので、そちらについても抜粋をしております。

ただ、こちらは、災害に対する言及というのはこれまでないところで、２０２３年７月までのレポートの中では、Ｃｏｖｉｄ－１９のパンデミックへの対応と、ウクライナ戦争に関

する対応が記載されているといったところが、この危機対応状況になっております。

こちらが主なプラットフォーム事業者の関連するコミットメントへのコミットメント状況といったところでありますけれども、Ｔｗｉｔｔｅｒ（現X）については、昨年の５月に離脱をしておりますので、レポートは、提出されていた１月時点でのレポートのコミットメント内容を記しているところになっております。

その具体的な記述があるコミットメント２２の措置７（危機的状況に対応したＵＩ設計）と、欧州委員会への情報・データの提供というコミットメント４２に関する部分を抜粋しているといったところになります。

こちらは、それぞれの事業者の主な内容を抜粋しているところになりますけれども、まずコミットメント２２の措置７というところで言いますと、権威ある情報ないしは信頼性の高い情報に対しての誘導ですとか、それを目的としたパネルですとかアラートの表示といったものが、ＧｏｏｇｌｅですとかＭｉｃｒｏｓｏｆｔ、さらにはＴｉｋＴｏｋのほうからレポートの中に記載されているといったところであります。

欧州委員会への情報・データの提供というコミットメント４２については、報告期間に行った具体的な実施策ですとか、今後の見通しといったものが示されているといったところや、ないしは、サブグループへの情報提供やその他協力に対する姿勢を積極的に行うといったものは、Ｍｉｃｒｏｓｏｆｔ等から示されているところになっております。

各社の詳細については、以降のページに記しておりますので、御参照いただければというところになります。

もう一つ、透明性レポートの中で、先ほど申し上げました付録の部分で、危機対応状況という形で、Crisis Responseへの記載内容が記載されているといったところですけれども、重ねてになりますけれども、Ｃｏｖｉｄ－１９とウクライナ戦争のみに関するものというところで、自然災害に対する言及はなかったといったところになります。

それぞれＣｏｖｉｄ－１９に関しましては、偽誤情報ですとか、それに関連するコンテンツを削除したですとか、不正アカウントの特定・削除をしたといったものが主な取組として記載されているといったもの、ウクライナ戦争については、ロシア関連の広告の一時停止ですとか、ジャーナリストの支援、ないしはファクトチェック団体・プログラムへの投資といったもの等が各社からそれぞれ言及されていたといったところになっております。

こちらも各社のＣｏｖｉｄ－１９とウクライナ戦争それぞれに対する具体の取組については、以降のページに抜粋をしておりますので、御参照いただければといったところになり

ます。各社、この２つについては、基本的に言及をしているといった形になっております。

透明性レポートについては、２０２４年3月２６日、直近に最新版、２４年１月までのレポートという形で各署名団体の透明性レポートが公表されているといった形になります。今回が、去年の１月、７月に続く３回目のレポート公表となっているところであります。

こちらのレポートのそれぞれの概要は、後ほど説明させていただきますリスク評価のところで、それぞれのところについて抜粋させていただければと思いますけれども、フォーカス自体が、６月に予定されている欧州議会選挙に焦点を当てているといったところで、選挙の公正な実施を担保するために、どういった対策をしてきたのか、さらには、進めていく方針なのかといったことが主眼に置かれているところでありまして、過去のレポートと同様に、災害に関する言及はないといったところで、危機全般に関してで言いますと、イスラエル関連のものについての取組が少しCrisis Responseに言及されているといった程度でございまして、自然災害という観点で言いますと、このレポートについても言及はなかったといったところになります。

こちらのプレスリリースからコメントを抜粋しておりますけれども、それぞれ、左側のコメントで言いますと、各プラットフォームが現在行っている対策の概要を説明する中で、選挙期間中に外国による情報操作や偽情報の脅威に備え、迅速に対応するため、取組を強化するよう強く求めるといった形で、この年に行われる選挙に対しての対策をちゃんとしていくことというのに強化が行われているといったところでございます。

まずは、危機対応時の特例といったところで御説明させていただきました。

以上となります。

【山本（龍）主査】　ありがとうございます。

それでは、今の御発表につきまして御質問、御意見のある方は、挙手機能またはチャットで御発言の希望の旨を御連絡ください。大体１５分程度、質疑応答の時間とさせていただきたいと思います。よろしくお願いいたします。

特に今のところないようですので、私のほうから、時間稼ぎというところで１点お願いしたいんですけれども、危機対応の最長期間を設定したというお話がありましたけれども、この辺りの背景について、少し詳しくお話しいただければと思います。いかがでしょうか。

【野村総合研究所（齋藤氏）】　こちら、弊社の尾張さんのほうから答えられますか。

【野村総合研究所（尾張氏）】　承知いたしました。先ほどの参照ということで飛ばしてしまったスライドを見せていただけますか。こちらですね。

こちら、先ほどは飛ばしてしまったんですが、まずそもそも、これ、最初のほうに検討の中にはなかった条項でして、ただ、ロシアのウクライナ侵攻という異常な事態が起きたので、必要なのではないかというところで、急遽入れられたというふうに報道では出ております。

関連するロシア系のメディアを禁止するだとか、そういった中の一つの取組として行われております。

ただ、やはりこれ、結構拙速だったというところで、かなり市民団体が表現の自由に対する制約になるのではないかというところで、いろいろな署名活動といいますか、世論的な意味で巻き起こってしまったところがあったので、それに対応してというところになりますけれども、最終的な調整の中で、やはり欧州委員会に無限の権限を与えるのはよくないというところで、もしこういう特別な危機対応という制度をつくったとしても、最長で何日とか何週間以内のみでしか使えないということで、条文の中にしっかりと書くということで、行政の権力を少し制約するという形で少し落ち着かせたというふうに解釈されております。

【山本（龍）主査】　ありがとうございます。

一つ重要なところかなと思いましたので、御質問させていただきました。ありがとうございます。

ちなみに、これは最長期間３か月に設定ということですけれども、この辺りは延長とかもあり得るということなんでしょうか。

【野村総合研究所（尾張氏）】　条文上は、特に延長の可能性があるというところは記載はしておりませんでして、あくまで司法機関や裁判所が基本的に本当にそれが必要かどうかというところは決めるというところも、一応検討にはあるとは思うんですけれど、ただ、条文上は、そこまでしっかり深く踏み込んでいるわけではなく、あくまで最長のみの設定という形で妥協している。

【山本（龍）主査】　分かりました。ありがとうございます。

それでは、質問が今チャットで出ているようですので、そちらのほうに移りたいと思いますが、まずは生貝さん、よろしくお願いいたします。

【生貝構成員】　ありがとうございました。

御質問ではなく、簡単な関連情報提供というところなのですけれども。

今回、様々、特に危機対応における自然災害の位置づけということについても御検討をいただいたところでございますけれども。このデジタルサービス法のほかに、昨年末採択されて今年の１月に官報に掲載されたデータアクトという法律が存在しており、この法律自体

は、データの活用に関わる包括的な枠組みを定めたものでございますけれども、その中の第５章に、ＢｔｏＧデータ共有、特に公共の緊急事態等における民間部門保有データに対する政府の共有要請といったものを包括的に定めた規定が置かれているところです。

その中では、公共の緊急事態、パブリックエマージェンシーの中に、特に自然災害、具体的な表現で言いますと、an emergency resulting from natural disasterという言葉も直接的に入っているところでございまして、こういった条項といったようなものも、もしかすると今後深掘りして、よく考えていく価値もあるのかなと感じたところでございます。

差し当たり、以上です。

【山本（龍）主査】　ありがとうございます。

それでは、次に、山本健人さん、お願いいたします。

【山本（健）構成員】　山本です。ありがとうございました。

私のほうからは、初歩的な確認なのかもしれないんですけれど、このＤＳＡの危機プロトコルについてなんですけれど、これ、基本的に危機的な事態が生じた後に要請を受けて作るというのが想定されているような感じはするんですけれど、策定にそれなりに時間もかかるのではないかとか、そんな感じもしていて、ある程度事前にひな形というか、典型パートみたいなのが準備されているような仕組みになっているのかとか、どういうスピード感で作ることが想定されているのかみたいな点について、もし御存じであれば教えていただきたいなと思いました。

以上です。

【山本（龍）主査】　ありがとうございます。

それでは、次に、山本健人さん、お願いいたします。

【山本（健）構成員】　北九州市立大学の山本です。ご報告ありがとうございました。

私からは、初歩的な確認なのかもしれませんが、ＤＳＡの危機プロトコルについて質問です。基本的に危機的な事態が生じた後に要請を受けて作成するというのが想定されていると思うのですが、策定にはそれなりに時間もかかるのではないかと思います。ある程度事前にひな形というか、典型例みたいものが準備されているような仕組みになっているのかとか、どういうスピード感で作ることが想定されているのかといった点について、もし御存じであれば教えて頂きたいと思います。

以上です。

【山本（龍）主査】　ありがとうございます。

では、この点は齋藤さんからお答えいただければと思いますが。お願いいたします。

【野村総合研究所（齋藤氏）】　これ、プロトコルのところは、我々も見ているところではあるんですけれども、具体的なところには、今、山本先生のおっしゃっていただいたところまでは言及されていないといったところでして、翻って、日本の災害対応なんかを踏まえると、やっぱり事前に作り込んでおくのが通常みたいな感覚なのかなと思うんですけれども、そこが割と異なる部分かなというところではございまして、ここは勧告が来た後に策定をするというところまでしか書かれていないというのが、条文ですとか公開資料から読み取れる部分となっております。

【山本（健）構成員】　なるほど、分かりました。ありがとうございます。

【山本（龍）主査】　ありがとうございます。

この辺りは、例えば、先ほどの行動規範の話とはリンクしてくるんですかね。それとも、ここはまた別のものになるんでしょうか。行動規範でコミットメントがいろいろと示されているところがあると思いますけれども、こういうことがプロトコルの内容と一部重複してくるようなところというのがあったりというのは、まだ分からないということですか。

【野村総合研究所（齋藤氏）】　そうですね。コミットメント４２の中で、関連することは書かれているんですが、プロトコルに関するところまでは言及されていないといったところですので、その具体なところまでは読み取れないかなというところですね。

【山本（龍）主査】　分かりました。ありがとうございます。

それでは、石井さん、お願いいたします。

【石井構成員】　ありがとうございました。大変精緻におまとめいただき、勉強させていただいております。

私のほうからも簡単な確認になりますが、危機の範囲、これ、ＤＳＡの中では、前文９１項で具体的な例として挙げられているので、危機の中で自然災害は含み得るという解釈は可能であると。他方、行動規範強化のほうでは、災害に関する直接的な言及はないということですが、そうはいっても排除しているわけではないという認識でよろしいですよね。地域的に危機がどういうものかというのは、それぞれ想定するものが変わってくると思うので、その違いによって、ガイダンスでは災害に関する言及が特段ないといいますか、プライオリティ的にそこまで高くないのかもしれないのですが、問題が生じ得る状況の種類が違うことによるものだという認識でよろしいかという点について、お考えをお聞かせいただければということですけれど、よろしくお願いいたします。

【山本（龍）主査】　　よろしくお願いいたします。

【野村総合研究所（齋藤氏）】　　基本、先生におっしゃっていただいたとおりかなと思っております。ここに書いているＤＳＡの中では、危機の中で自然災害が例示の一つとしてされていまして、行動規範並びにガイダンスの中では、危機の中で自然災害について具体の例示はないというところですけれども、排除しているわけではないというふうには思っておりまして、ただ、地域特性上、やはり武力紛争ですとか、パンデミックのほうが上位に来るかなというところではありますけれども、排除されているものではないというふうには認識しております。

【石井構成員】　　ありがとうございます。

【山本（龍）主査】　　ありがとうございます。

それでは、森さん、お願いいたします。

【森構成員】　　御説明ありがとうございました。大変興味深く拝聴いたしました。

１つは意見で、１つが質問なんですけれども。以前から私、ヒアリングのときも、偽情報が投稿として来る場合と、広告で来る場合と両方ありますよねというお話はさせていただいていたんですけれども、今回の資料を拝見すると、広告についてこういう対応をしましたということは非常に具体的に書かれていまして、例えば、２７ページのＭｉｃｒｏｓｏｆｔの対応とか、ほかにも何か所もそういうことが出てきていて、すみません、ページ数はあれなんですけれども、いろいろ資料内検索をしたりしたところ、たくさん出てきていまして、やっぱりちゃんといろんなことをしていただいているんだなというふうなことが分かりました。それがよかったです。

もう一つは質問なんですけれども、お話の中で、Ｘが行動規範から脱退しましたということがありましたけれども、その影響といいますか、Ｘが行動規範から脱退したことについて、政府側とか市民社会側からどんな反応があったかというのを教えていただければと思います。よろしくお願いします。

【山本（龍）主査】　　お願いします。

【野村総合研究所（齋藤氏）】　　こちらは弊社の尾張のほうから簡単にコメントさせていただければと思いますけれども、いかがでしょうか。

【野村総合研究所（尾張氏）】　　Ｘの脱退については、Ｘがやめますと言ったというよりは、Ｘが行動規範に示されている義務を守り切れていないので、行動規範側のほうから、このまま守れていない人たちを入れるのはどうかという形で、追い出されたといいますか、ど

ちらかというと、Xが主体的に出たという認識とは少し違っていると思います。

これを受けての反応というところで、市民側はどうこうというところは把握できていないものの、欧州委員会のほうはすごく残念だというふうにはっきりとスピーチはしておりまして、復帰は願っているみたいな形のスタンスではいたと思います。

【森構成員】　なるほど。分かりました。ありがとうございました。

【山本（龍）主査】　ありがとうございます。

森さん、よろしいですか。

【森構成員】　はい。

【山本（龍）主査】　では、水谷さん、よろしくお願いします。

【水谷構成員】　御報告ありがとうございました。

私からも、ちょっと基礎的な部分になるかもしれないんですけれども、欧州デジタルサービス会議の位置づけについてお伺いしたいと思います。

スライドの４ページ目等の危機発生時の各ステークホルダーの行動と関係性というのからすると、まずこのデジタルサービス会議が危機対応の勧告をして、そこから欧州委員会がプロトコルを作成したり、危機対応措置要求をしたりというので動き出すということになっていて、まずこの欧州デジタルサービス会議というのを一つ挟むという、直接欧州委員会が最初から動くのではなくて、ここがまず勧告を出すという仕組みになったという点について、なぜこういう形になったかというのをちょっと詳しくお聞きしたいなというのが１点です。

もう１点は、御説明の中で、この会議体は６１条に基づいて、独立した諮問機関であるというふうに書かれているところなんですけれども、スライドの１２ページとか１３ページに欧州デジタルサービス会議の条文が逐語訳されているわけなんですけれども、これを見ていると、会議の議長は欧州委員会が務めるというふうになっているわけですね。６２条の構成のところで、そうなっていると。投票権はどうもないみたいですけれども、メンバー的には各国の加盟国の高官がメンバーになるという形かなと思うので、ここでいう独立というのは何を意味しているのかというのをちょっとお伺いできればと思います。

以上です。

【野村総合研究所（齋藤氏）】　ありがとうございます。

その独立が何を意味するかというのは、この条文からだけだとなかなか解釈が難しいかなというところと、まだ会合は２回しか開かれていないというところですけれども、今後そ

こは見ていく必要があるところなのかなというのは正直なところではあります。

ただ、ＤＳＡの考え方として、欧州デジタルサービス会議と欧州委員会とＤＳＣ、各国のＤＳＡの監督執行を有する機関の三位一体となってマネジメントしていくといったところが鮮明になっているところでして、その欧州委員会とＤＳＣの代表で構成されるのが欧州デジタルサービス会議といったところになっておりますので、欧州委員会だけではなくて、ＤＳＣも含めた中で、この危機対応をしていくといった文脈の中で、欧州デジタルサービス会議が勧告をしていくといったような形になっているのかなとは推測されるところかなと思っております。

【水谷構成員】　ありがとうございます。

独立の観点について、もし今後分かったこととかありましたら、また御教示いただければと思います。ありがとうございます。

【山本（龍）主査】　ありがとうございます。

それでは、落合さん、よろしくお願いいたします。

【落合構成員】　どうも御説明ありがとうございます。非常に詳細であって、大変参考になりました。

その中で、一つ気になりましたのが、危機対応から若干外れる部分はあるようには思いますが、主要な事業者の取組例についてもまとめていただいております。その中で、各事業者とも、広告に対する対応ですとか、偽情報等に関連するようなマネタイズに対する対策を打たれているという部分はあるように見受けられます。

これが、もちろんＣｏｖｉｄですとか、ロシア・ウクライナの関係では、各事業者でそれぞれ方法は違うと思いますが、それぞれ対応する事項の中心的なもののうちの一部を構成しているようにも思われます。こういった危機局面以外の場合での偽情報ですとか、そういう場合の対策は行われているのかどうかはいかがでしょうか。それとも、これは危機時ですとか、それに関連するので、特により厳しく対応しているような状態になっているのかどうかがもしお分かりになれば、その辺り教えていただければと思います。

【山本（龍）主査】　よろしくお願いします。

【野村総合研究所（齋藤氏）】　ありがとうございます。

こちらについては、基本、危機に絞るというわけではないですけれども、今回、危機に対応するところを抜粋しているというところで、こういう言及にはなっております。先ほど行動規範の透明性レポートのところも、コミットメント全体を書いておりますけれども、この

中で、それぞれに対しての言及は書かれているといったところではありますけれども、ただ、このCrisis Responseというところの危機対応状況という付録に関しては、危機しかないというところで、そこは特出しされている観点、項目というところかなと思っております。

【落合構成員】　ありがとうございます。位置づけ、よく分かりました。また今後、一般的な対応をするに当たっては、整理をして、どういう対応を求めているのかを理解すること自体は改めて重要かなとは思いました。

どうもありがとうございます。

【山本（龍）主査】　ありがとうございます。

確かに、その差分というんですか、一般的な状況と危機的な状況、あるいは、災害というところとの差分、当然、一般的な状況においても偽情報に対する対策というのは講じるというふうに行動規範等々でなっていると思いますけれども、それがどれぐらい危機的状況において上乗せされていくのかという、その差分については、もう少し詳しく今後も見ていかなければいけないのかなと思いました。ありがとうございます。

ほかの方はいかがでしょうか。

それでは、ちょうど時間ですので、次のトピックに入りたいと思います。

次ですけれども、リスク評価・軽減措置等につきまして、引き続き野村総合研究所、齋藤様、尾張様より御発表をお願いいたします。同様に２０分間でお願いいたします。

【野村総合研究所（齋藤氏）】　では、続きまして、お時間いただきまして、リスク評価の概要という形で、引き続きＥＵの事例と、さらには、英国の中でもオンラインセーフティ安全法という中で、一部リスク評価についても提示されている部分がありますので、そちらについても簡単に御説明させていただければと思います。

まずＥＵ全体のＤＳＡと、さらには、行動規範を含めても、リスク評価というのがどのように枠づけられているかというところを簡単に御説明させていただければと思います。

こちらがＤＳＡの全体構成という形で、以前のWGでもお示しさせていただいたものになっておりますけれども、この中で、リスク評価は、具体的には第３４条に書かれているといったところで、そのリスク評価をした上でのリスク軽減措置というのが第３５条になってくるというところでございます。

こちらはＤＳＡ全体の中で言うと、第５節の中に位置づけられておりまして、こちらの第５節の対象というのは、超大規模オンライン・プラットフォーム（ＶＬＯＰ）及び超大規模オンライン検索エンジン（ＶＬＯＳＥ）に対して課される追加義務となっておりますので、

ＤＳＡの中でリスク評価とリスクの軽減の具体対象となるのは、ＶＬＯＰとＶＬＯＳＥのみに課されているというところがまず大きなところといったところであります。

先ほどもお示ししたものになりますけれども、少し抜粋して言いますけれども、偽情報に関する行動規範とデジタルサービス法が、関連してＶＬＯＰ／ＶＬＯＳＥのリスク軽減に対する枠組みを位置づけているといったところではありまして、具体的には、この行動規範に参加するということが、ＶＬＯＰとＶＬＯＳＥのリスク軽減義務の一環に位置づけられているといった形が大きな枠組みとなっているというところでございます。

以後、３４条と３５条、さらには、それを踏まえて監査する第３７条について、それぞれ御説明をしているところになります。それぞれの条文の内容については、６ページから８ページに示しているところでございますけれども、それを踏まえて、全体がどういった流れになっているかというのをまとめているのが９ページになっております。

申し上げたとおり、ＶＬＯＰ・ＶＬＯＳＥに指定される事業者というのは、リスク評価を含めたＤＳＡと、さらには、行動規範それぞれの遵守状況について独立機関から監査を受ける必要があるといったところでございます。

独立監査の流れというのを下のほうで記しているところでございますけれども、大きく４つのステップに分かれているといったところであります。

まずＶＬＯＰ・ＶＬＯＳＥに該当する事業者というのは、１番目にシステミックリスクの識別・分析・評価といったところで、まずリスク評価をするというのが第３４条で書かれているところであります。評価は年に１回以上行う必要があるということで、具体的には、市民言説・選挙等への悪影響リスクですとか、基本権に関する悪影響リスク、違法コンテンツの拡散リスク等、評価をすることが１番目。

２番目が、合理的・比例的かつ有効な軽減措置という形で、①の評価内容を踏まえて措置を行うといったところで、具体的には、サービス設計・機能等の工夫、さらには、利用規約の工夫ですとか、コンテンツモデレーション手続の工夫、さらには、軽減措置を講じる約束を定めた行動規範の策定といったものまで含めて、具体的な有効な軽減措置を取ることというのが定められているところになります。

この①と②の遵守状況を監査するというのが、③の監査の実施という形で、こちらがＤＳＡの第３７条に書かれていることと、関連する内容として、偽情報に関する行動規範のコミットメント４４にも内容が書かれているところであります。

具体的な監査対象となるのが、３４条、３５条を含めたＤＳＡ上の義務と、行動規範を通

じて自主的にコミットメントした事項に対する制約の状況といったことを守っているかといったところであります。

この監査の意見は3段階で、「肯定的」以外の意見の場合については、ＶＬＯＰ・ＶＬＯＳＥに対して報告書の作成が求めているといったところであります。

「コメント付き肯定的」、部分的肯定的という話と、「否定的」といった場合には、左側の④に返ってきまして、監査を踏まえた取組報告書の作成が求められるといったところであります。

こちら、２３年８月から先行してＶＬＯＰ・ＶＬＯＳＥにＤＳＡの適用が開始されたところですけれども、最初の独立監査というのは１年以内ということですので、最初の独立監査が２４年８月までに行われるというところが見込みでありまして、その中で、この「コメント付き肯定的」ですとか「否定的」といったものが出された場合には、３７条に基づいた監査を踏まえた取組報告書の作成に進むものと思われるといったところであります。

ただ、この３月時点では、リスク評価に関する具体の資料等はまだ公表されていないところですので、最初の独立監査を待って、どのように実際リスク評価が行われているのかというのを把握していくことになるのかなと思っております。

以降、３４条から３７条に関連する部分のところを逐語を載せておりますので、適宜御参照いただければというところになります。

ですので、先ほど申し上げたとおり、ＤＳＡの中でリスク評価とリスク軽減をして、それを独立監査を受けるといったところが大きくリスク評価の枠組みというところですけれども、その枠組み自体は、申し上げたとおりで、最初の独立監査がこの８月までにされるといったところになっております。

一方で、行動規範の中で、透明性レポートにおいて主要プラットフォーム事業者がどのようなコミットメントをしていたかというところと、その内容についてのレポートといった形の抜粋が１６ページになっておりまして、こちらが先ほど申し上げた特記のレポートで出された内容が、２４年１月までのレポートで、どういったところが書かれていたかというのを簡単に抜粋しているものが１６ページになっております。

先ほど申し上げたとおり、選挙に関するところに注力していくというところがフォーカスされていたところですので、各社のサマリーの中でも、その内容についての言及が中心になっていたところでございます。

特に４のサービスの完全性のところで言いますと、選挙に先立って、生成ＡＩコンテンツ

が与え得るリスクに対抗したアプローチ計画ですとか、ガイダンスの発表、さらには、原則への誓約等が行われているといったところでありますし、５のユーザーのエンパワーメントというところで言いますと、選挙に関連した偽誤情報に対抗するために、音声・画像・動画の出所や作成元などの情報を開示するといったところで、ユーザーに対する透明性を高める動きが各社から報告されていたといったところであります。

さらには、ファクトチェック団体等のエンパワーメントで言いますと、ファクトチェック団体への助成ですとか、サミットの開催等に対しても言及されているということと、一部事業者については、自社のファクトチェックプログラムでファクトチェック団体の認証の受入れを開始予定といったことまで言及されていたところになっております。

ここまでが、行動規範の中でリスク評価という、ここまで記載している項目を踏まえて、今後ＤＳＡの枠組みの中での独立監査がされていくといったものになるかなと思われますけれども、各社のコミットメントの中では、各社の具体的な取組について記しているところになっております。

以降、１７ページ以降が、直近の最新の行動規範に関する透明性レポートの中で、各社の取組について、主なものを抜粋しているところになっております。

一部、前回までの２３年７月のレポートまでと内容が重複するものについては、括弧で追加項目なしといった形で、後段の２３年７月までの内容を御参照いただければといったところになっております。

なお、先ほど申し上げたとおりですけれども、X社については、２３年５月に脱退しておりますので、この１月のレポートについては、もちろん提出はしていないところですので、Ｘについては除外させていただいております。

２２ページは、こちら御参考になりますけれども、以前のWGでも示させていただいた過去の２３年７月までの各項目に対する各社のサマリーの内容となっておりますので、こちらも必要に応じて適宜御参照いただければというところになります。

ここまでが、まず一旦、ＥＵにおけるリスク評価とリスク軽減の枠組みといったところで、ＤＳＡにおいてどのような位置づけにされているかと、それに対する監査の枠組みと、行動規範の中でどういった内容が書かれているかというところを簡単に御紹介させていただいたところになります。

続いて、英国のオンライン安全法におけるリスク評価の考え方というところで、こちらも、オンライン安全法については、第８回のWGの中で御説明させていただいた内容も重複し

ますけれども、改めて簡単に振り返りつつ、その中でリスク評価がどのように定義されているのかというところを簡単に御説明させていただければと思います。

振り返りますと、この英国オンライン安全法（Online Safety Act）は、２０２３年１０月２６日に制定されたところで、違法または子供に有害なコンテンツですとか、それによるリスクを特定・軽減・管理する義務をオンラインサービスの提供者に課し、個人にとってより安全なオンラインサービスの提供を確保することを目的としているといったような法律になっているところであります。

大きな法律の構成自体は２９ページに示しているところでありますけれども、それに対して、具体なガイダンス等がＯＦＣＯＭのほうから提示されていくといったような流れになっているところであります。

法律の概要については、詳細は割愛させていただければと思いますけれども、対象事業者としては、大きくユーザー間サービスというところで、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サービスということで、いわゆるソーシャルメディアですとか、写真・ビデオの溶融デバイスサービスといったものが対象になるというところと、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検索サービスという、大きく２つに分けて課される義務等を規定しているというのが特徴となっております。

このオンライン上における偽誤情報の位置づけは、参照までになりますけれども、偽誤情報自体は、オンライン安全法の中では定義をされていないといったところでして、オンライン安全法については、違法コンテンツというのを定義しているところでして、その中では偽情報というのは含まれていないといったところであります。

この法律の中で偽誤情報に関連する項目としては、大きく３つあるというところで、一番大きなものとしては、偽誤情報のアドバイザリー委員会の設置というのが書かれているといったところでございます。

このアドバイザリー委員会については、前回も簡単に御紹介させていただきましたけれども、同法の１５２条において、偽誤情報のアドバイザリー委員会の設置が義務づけられているといったところであります。

こちらはまだガイダンス策定中ですけれども、具体の要件自体は法律の中にこのように書かれているところでありまして、実際に設置された場合には、１８か月以内に報告書を公表することが義務づけられているといったところと、その後の定期的な報告書の公表が義務づけられているといったところであります。

事業者に課される義務・違反時の罰則等も、前回の御説明と重複する部分はありますので、割愛させていただければと思いますけれども、違反時の罰則としては、１，８００万ポンド、ないしは全世界売上高の１０％のいずれか高い額を上限とする制裁金が課される可能性があるといったことになっているところであります。

こちらの具体の執行に向けたスケジュールで言いますと、大きく３つのフェーズに分けて進められる。今が第１フェーズで、フェーズ１に当たるところで、全般のillegal harmsに対するガイダンスと具体の行動規範がＯＦＣＯＭのほうから提示されていたといったところで、このパブコメ自体が２月２３日まで行われていまして、現状は、そのパブコメのコメントを精査中といったような状況になっているところであります。

そのＯＦＣＯＭから出ていたコンサルテーション、“Protecting people from illegal harms online”は、大きく６章構成になっていたところですけれども、その３つ目の項目で、オンライン上のリスクの評価方法といった形で、ＯＦＣＯＭからの案が提示されていたといったところになっております。

このオンライン安全法の中で、どのようにリスク評価をしていくかというところは、ＯＦＣＯＭからの提示案としては、４つのステップに分けて実施してくださいというのが提唱されているといったところです。

１つ目のステップとしては、危険性の理解といったところで、ＯＦＣＯＭが提示するリスクプロファイルに沿ってリスク要因を考慮した上で、評価が必要な違法な危険性を認識するといったところで、具体的には、１５種類の法律の中で対象となる違法な危害についての理解を深めることというのが示されております。

それを理解した上で、ステップ２で、リスクの評価をしていくといったところで、各種の違法な危害の可能性とその影響を評価して、具体の危害のリスクレベルを割り当てるというのが具体的な内容になっております。

ですので、この１５種の危害それぞれに対するリスクを自社のサービスに対して割り当てるといったところがアウトカムになってくる。それに基づいて、対策の実行と記録をしていくというのがステップ３になってくるといったところであります。

さらには、ステップ４で、レポートとリスク評価の監視と更新といったところで、リスク評価と対策について報告をしていくといったところと、効果をモニタリングするとともに、リスク評価へのレビューを行うといった形で、具体には年に一度のレビューを提示することというのがＯＦＣＯＭ案としては示されているところになっております。

申し上げました１５種類の違法な危害については、テロリズムに関連するものから、外国干渉罪までの１５項というのが具体的に提示されているといったところになっております。

リスク評価の概要のところは、先ほど説明した内容と重複しますけれども、こちらはＯＦＣＯＭからの資料を少し抜粋する形ですけれども、事業者に対しては、現状ではリスク評価の義務はまだないというところですけれども、ガイダンスの最終版が公表されてから３か月以内にリスク評価を行うことが課されているところであります。ですので、事前から内容を把握してくださいといったような周知がＯＦＣＯＭからされているところであります。

リスクを認識して評価するというところに対して、リスクプロファイルというのがＯＦＣＯＭから提示されているといったところです。リスク評価自体は各事業者が行うこととしておりますけれども、ガイドとしてリスクプロファイルというのを提示しているといったところであります。

大きくユーザー間サービスというものと検索サービスのそれぞれのサービスに対して、評価項目リストというのを提示しておりまして、それに沿ってリスクを評価してくださいということが言われております。

まずサービス特性の評価といったところで、ユーザー間サービスと検索サービスの中で、それぞれが具体にどういうサービスなのかと。ユーザー間サービスの中で、例えば、Social1メディアに当てはまるのかですとか、ゲーミングサービスに当たるのかですとか、具体のサービスタイプを特定していくといったところが１つ目。

今、特定のリスク要因への評価といった形で、そのサービスタイプに起因するリスク要因というのを評価していくといったところで、それぞれについて、自社のサービスが該当するサービス特性を踏まえてリスク要因を評価していくといったことが２番目。

３番目は、サービスタイプにかかわらず、共通する一般的なリスク要因への評価といった形で、ユーザーの人口構成ですとか、ビジネスモデルですとか、サービス・ビジネスの成熟度といったものに応じてリスクを評価するといったものが課されているところであります。

今申し上げたリスクプロファイルの１番目と２番目の例というところでありますけれども、ユーザー間サービスに向けたリスクプロファイルから一部抜粋をしているといったところでありますけれども、サービス特性の評価のところは、クエスチョンシートみたいなものがＯＦＣＯＭのほうから提示されているといったところで、それに対して事業者のほうで答えていくといったことが想定されております。

例えば、例示になりますけれども、この中で自社のサービスがソーシャルメディアサービ

スに当てはまるのかどうかといったところで、これに当てはまる場合ですと、右側になりますけれども、特定のリスク要因の評価という形で、ソーシャルメディアサービスがどういった特性なのかといった形と、どういったリスクを含むのかということを例示した上で、その上でリスク評価をするということがガイドされているといった形になっております。

ソーシャルメディアサービスの場合ですと、広範なサービスになりますため、先ほどの１５種の違法な危害については全てに該当する危険性があるといったことが示されているということと、リスク要因の中で、偽情報を拡散するキャンペーンとして、ソーシャルメディアサービスが利用される可能性についても言及されているといったところであります。

一般的なリスク要因、サービスタイプにかかわらず共通するものについては、ユーザー構成とビジネスモデルとサービス・ビジネスの成熟度となっているところです。

特にユーザー構成については、年代等に加えて、人種ですとか、宗教ですとか、年齢といった特定の属性を踏まえてリスク評価を行うといったもの、さらには、ビジネスモデルについて、広告ターゲティングを行っているようなものですと、有害な活動を助長する可能性があるといったことまで言及されているといったものと、サービス・ビジネスの成熟度というところで言いますと、アーリーステージのビジネスというのはリソース等が限定的であるというところですので、違法危害の可能性が高まるといったところ、ないしは、利用者数が急成長する、ビジネスの規模が急成長するようなフェーズにあるような場合には、リスク源が変化し得るといったことを認識した上でリスク評価を行ってくださいといったことまでが言及されているといったところになっております。

ここまでが英国の例というところですけれども、まだガイダンスの案といったところで、今後パブコメを踏まえて更新されていくものと思われますけれども、大きく４つのステップ等で行われていくといったところ等が、英国におけるオンライン安全法のリスク評価の特徴でございます。

以上、ＥＵ全体と英国におけるリスク評価の概要というところで御説明をさせていただきました。

以上となります。ありがとうございました。

【山本（龍）主査】　ありがとうございました。

リスク評価の概要が明らかになってきたのかなと思いますけれども、皆さん、いかがでしょうか。大体１１時１５分ぐらいまで質疑の時間にしたいと思います。積極的に御質問、コメントいただければと思います。よろしくお願いいたします。

また時間を稼ぐというところで、２点ほど教えていただきたいんですけれども、１点は、スライドの３０ページだと思いますが、ここのまず１点目は、やはりリスク評価というのが、基本的に、この一番上にあるように、違法コンテンツに関するリスク評価の義務ということだと思うんですね。

先ほど偽情報に関しては、別の考え方が、例えば、アドバイザリー委員会を設置してとか、別のルートでの対応を考えている、つまり、リスク評価に関して、この偽情報というのが含まれているのか、それとも、偽情報に関しては、アドバイザリー委員会ですとかＯＦＣＯＭがもろもろ今後助言などを出していくという話がありましたけれども、別ものと考えているのか、リスク評価にはやはり偽情報のリスクというのも含まれるというふうに理解されているのか。この点、まずいかがでしょうか。

【野村総合研究所（齋藤氏）】　ありがとうございます。

大きく別物になっているというふうに理解しております。

まず、違法コンテンツというものに対しては、偽情報は含まれていないといった形になっておりますので、基本的に、先ほど申し上げたリスク評価というのは、この１５個の違法コンテンツ・違法危害に対してリスク評価を行うといったことが示されておりますので、偽情報に対しては、この中で厳密に評価をするということになっていないというふうに理解しております。

ただ、先ほど申し上げたとおり、ソーシャルメディアの中では、偽情報を拡散するキャンペーン等が含まれることも踏まえてサービスの評価を行うことといったものは言及されておりますので、偽情報が完全に除外されているわけではないといったところでありますけれども、具体的なリスク評価を行って、その後、行動規範でのリスク軽減措置を取っていくという枠組みの中では、１５種の違法危害というのがまず想定されておりますので、その中には偽情報は含まれていないというふうになっております。

【山本（龍）主査】　ありがとうございます。

２点目なんですけれども、３番目の特定のカテゴリーのサービスに対しての追加義務なんですが、聞き逃している可能性もあるのですが、この特定のカテゴリーが何かと。私は、このユーザーエンパワーメントに関する義務というのは重要かなと。これは英国の安全法の一つのポイントかなとも思います。ユーザーのコントローラビリティを高めていくというところですけれども、別途定められる予定の規則と、この規則の位置づけというのがどういうものなのかということを教えていただければと思います。

よろしくお願いいたします。

【野村総合研究所（齋藤氏）】　ありがとうございます。

この特定のカテゴリーに対して具体の規則というのが、ＯＦＣＯＭのほうから示されるガイダンスのことを指しておりまして、こちらが３４ページになりますけれども、ＯＦＣＯＭの中で、今申し上げたカテゴライズされたサービスに対する義務というのはフェーズ３に当たるといったところになりまして、こちらについてのコンサルテーションは、今年度の中盤以降に想定されているといったところですので、具体的にどういったカテゴライズするか、ないしは、具体の対応を検討してもらうのかといったところの案というのは、この後のフェーズに沿って示されていくことが想定されていると。

ただ、まだフェーズ２のChild safety duty and pornographyというところもまだ示されていないところですので、その後の対応になるということですので、もう少し期間的な猶予というところでは、先延ばしになっているのかと思っております。

【山本（龍）主査】　ありがとうございます。

それでは、森さん、よろしくお願いいたします。

【森構成員】　御説明ありがとうございました。すごい勉強になりましたし、山本先生もおっしゃっていましたけど、リスク評価の具体的なイメージがつかめて、なるほど、これはなかなかいい制度だなというふうに感じました。

私の御質問も山本先生と同じなんですけれども、偽情報は１５種類の違法な危害に入っていないというお話だったんですが、それはそうなんでしょうか。というのは、我々の行っている偽情報は、例えば、ここで挙げていただいている５番目のhate offenceとか、あと、テロももしかしたら関係するかもしれませんし、近時話題になっている１４番の詐欺・金融サービス犯罪とか、こっちは違法化されているのかもしれませんけど、日欧の違法情報の範囲が違うので、違うカテゴリーになっていますが、偽情報の一部の顕著なものがこっちに入っているのではないかなというふうに、御説明を伺っていて感じたんですけれども。

例えば、ヘイトスピーチみたいなことですよね。それって全然事実ではなかったりとかするわけですし、あと、テロに関することもそうで、陰謀論みたいなことを伝えてテロを擁護したり批判したりするというアプローチがあると思いますので、１５番の外国干渉罪なんて、何となくイメージすると、まさにそうなのかなという気がするんですけれども、それはいかがでしょうか。我々的には偽情報としてカテゴリーしているけれども、向こうだと違法になっているから違法なのかなというふうに伺ったということです。

以上です。

【山本（龍）主査】　お願いします。

【野村総合研究所（齋藤氏）】　ありがとうございます。

そういった意味で、私が先ほど説明させていただいた理解の中で言いますと、まずこの１５種の中には、偽情報というのが具体的にカテゴライズされているわけではないといったところと、あとは、この具体の１５種の違法危害というのは、このオンラインセーフティアクトの中で定義されているものではなくて、それぞれ関連する法案を参照するというふうになっているといったところであります。それぞれテロリズムに関する法律ですとか、児童の虐待に関する法律ですとか、そういったものからそれぞれ引用するような形で、このオンラインセーフティアクトの中では定義されているといったところでありますので、今、先生に添付いただいたように、それぞれの中で、例えば、５番の憎悪に関するもの等の中では、一部偽情報を含むようなもの、スピーチもhate offenceに含まれるといったこともあり得るというか、想定されるかなといったところではありますけれども、このオンラインセーフティアクトの中で、その中に偽情報が含まれるといったような定義はしていないといったことになります。

【森構成員】　分かりました。ありがとうございました。

【山本（龍）主査】　ありがとうございます。

すみません。今の点、もう少し確認したいんですけれども、要するに、ＤＳＡの３４条、スライドでいくと１０ページを見ると、ＤＳＡの場合には、リスク評価に小見出しとして一番上のところに、偽情報の拡散を含むリスクの特定が義務づけられているというようにつけていただいていて、条文上は、しかし、その偽情報というのは、３４条の条文には含まれていないということですかね。そうすると、ここの偽情報の拡散を含むリスクの特定が義務づけられているという、ここの小見出しの根拠は、どこにあるのか。前文とかにあるんでしたっけ。

【野村総合研究所（齋藤）】　今おっしゃっていただいているのは。

【山本（龍）主査】　スライドの一番上のところに見出しをつけていただいていて、ＶＬＯＰ／ＶＬＯＳＥは第３４条で偽情報の拡散を含むリスクの特定が義務づけられているとお書きいただいています。これはＤＳＡの場合には、明確に偽情報リスクの評価を含むという理解のようにさっき伺っていたんですけれども、ただ、条文上は、偽情報という言葉はたしかない。

【野村総合研究所（齋藤氏）】　そうですね。ここは、なので、前文のところで関連するもので、偽情報に関する前文の１０４項等を踏まえて書いているといったところですかね。

【山本（龍）主査】　なるほど。確かに、条文の書き方で言えば、ＤＳＡの３４条のほうが、かなり基本的な権利、いわゆる基本権に対するシステミックリスクということで、かなり広くある種捉えているように見えるわけですけれど、これに対して、英国のオンライン安全法は、さっき森さんの御指摘にあるように、やっぱり違法コンテンツというのをかなり強調されているようなところがあるので、確かに、そこに偽情報を読み込むということは解釈上可能なような気もしますけれども、やっぱり法律上の意図としては何か限定するようなイメージが多少あるのですけれども、この辺はもうちょっと深掘りしていかなければいけないと思うんですが、そのような理解なんでしょうか。

要するに、偽情報のリスクを排除しているわけではないけれども、やはり違法コンテンツというものを条文上明確に、違法コンテンツに関するリスクの評価なんだと言っているというところは、ＤＳＡの３４条に比べれば狭いというふうな理解になるんですかね。

【野村総合研究所（齋藤氏）】　そうですね。そこは御指摘のとおり、もう少し具体のＯＦＣＯＭの提示するガイダンス等も見ていく必要があるかなといったところでありますけれども、英国の中でも、この中でファクトチェック団体のフルファクトは、オンライン安全法の中で利用規約がどういう内容を盛り込むかですとか、さらには、偽誤情報の拡散を防ぐための内容というのは十分ではないといったような意見が表明されていたりというところもありますけれども、割とスペシフィックに、ちゃんと違法コンテンツを特定して、その中に対する具体の義務を課していくと。さらには、重きを置かれているのは、やはり青少年に対する安全をいかに確保するかといったところが重きを置かれているところですので、偽情報に関するところだと、ＤＳＡに比べても、やはり少しコントラストが薄いのかなといったところではあります。

【山本（龍）主査】　ありがとうございます。

森さん、この辺いかがでしょうか。何かコメントがあればと思います。ちょっと割り込んでしまって申し訳ありません。

【森構成員】　いや、でも、確かに、伺っていますと、結局、文脈によっては、表現の自由との関係で問題があるという指摘を受けるわけですから、もしかしたら限定的なアプローチを取っているのかなというふうにも思いましたが。

我々の立場と比べて考えれば、我々はそもそも違法情報の範囲というのをかなり限定し

たアプローチを取っている。先ほどの１５のカテゴリーを見ていただくと分かるとおり、向こうではしっかり違法というふうになっています。例えば、薬物なんかに関するものは、日本でも広く違法になっていますけれども、ヘイトとか、テロも、そういうのは多分ないと思うんですよね。なので、我々とＥＵの違法情報の定義の違いというのを前提にして学ぶことが必要なのかなと、山本さんのお話を聞いていて思いました。

【山本（龍）主査】　そうですね。ありがとうございます。この辺は今後もしっかり検討していかなければいけないところかなと思いました。ありがとうございます。

それでは、山本健人さん、お待たせしました。お願いいたします。

【山本（健）構成員】　北九州市立大学の山本です。

ＤＳＡと行動規範に関する部分の質問です。もしかしたら私が、聞き逃したのかもしれないのですが、独立監査主体がどういう組織になるのかというところが若干気になっております。たとえば、日本でもし同じような仕組みを作るのだとしたら、独立行政法人みたいな形で、一定程度国が関わってくるような、ある程度そんな仕組みが考えられそうなのですが、DSAでは純粋に民間的な団体で考えられているのかとか、現にある組織が想定されているのかとか、そういった点で、もし何かお分かりのことがあれば、お教え頂ければと思います。

【野村総合研究所（齋藤氏）】　ありがとうございます。

この独立監査主体については、要件は明記されているといったところで、ＶＬＯＰ・ＶＬＯＳＥと独立していて、利益相反しないこと、リスク管理等の専門知識を持つこと、さらには、客観性、職業倫理の遵守をすることといったことが書かれているところですので、ここを満たせる団体になるかなといったところですけれども、それが具体的にどこになっているのかといったところと、これが各ＶＬＯＰごとに設定しているのかというところを含めて、まだ公開されていないところですので、それ以上の情報は現状ではないといったところなんですけれども、今年中には独立監査が出されるかなというところですので、それをどこがしているのかということを含めて、確認が必要だというふうに認識しております。

【山本（健）構成員】　なるほど。ありがとうございます。

感覚的な印象ではあるのですが、規定を見てみると、基本的にこの監査自体の費用はＶＬＯＰとかＶＬＯＳＥ持ちという形になっていますので、監査主体の規模が小さいと、独立がどこまで維持できるのかといった問題が、見えない形で生じる可能性もあるかなと思いまして、若干気になったということでした。

ありがとうございます。

【山本（龍）主査】　ありがとうございます。

この辺りは本当に重要なところかなと思いますので、今後いろいろ明らかになってくるところがあると思いますけれども、引き続きフォローいただければと思いました。

それでは、落合さん、お願いいたします。

【落合構成員】　ありがとうございます。

私のほうも、実は先ほど森さんが議論されていたオンライン安全法の定義をお伺いしようかなと思っておりましたが、そこは座長も含めて議論されて、かなり明確になってきたところがあると思います。

もう一つ、お聞きしたいと思っていたのが、9ページのＶＬＯＰ・ＶＬＯＳＥの偽誤情報を含むリスクの特定の義務づけという部分です。この中で、３４条の中で、特にどの部分を指して偽情報の拡散というふうにタイトルのほうでつけられていたのかを、明確に示していただければと思いました。いかがでしょうか。

【山本（龍）主査】　ありがとうございます。

先ほどは前文を参照していただいたとは思いますが、改めて、そういうことで。

【野村総合研究所（齋藤氏）】　先ほど山本先生にもいただいたところでありますけれども、３４条の中では、偽情報の拡散というところは書かれていないところですけれども、前文の中で、偽情報を含む情報の増幅を目的とした協調的な操作というところが書かれているところですので、そこを踏まえて書かせていただいているといったところになっております。ですので、３４条の中で具体的に書かれているというわけではないというところです。

【落合構成員】　ありがとうございます。

一方で、繰り返しになっていたところ自体はそうですが、ただ、イギリスのほうと似ているところは、先ほどの森さんとの議論と似ているところがあると思っておりました。その中で、例えば、公衆衛生の保護などが書いてあるですとか、治安に及ぼすとかということが１項のＣでは書かれています。また、基本的権利の関係で言われている部分があるので、この辺りの内容が、やはり英国と同じで、もともと保護の対象とされるような権利・利益が日本よりもやや広いような様子が、欧州についてもあるかとは思っています。一方で、やはりＤＳＡのほうも、基本的には何かの関係で違法であること自体を条文そのものでは正面から書いているので、そこでは表現の自由といった権利との調整に当たっては、無限定に偽情報というような形の言葉は使わず、守られるべき権利・利益の侵害の範囲をある程度日本よりは広く取って定めた上で、その条項の関係で違法性があるものとしています。これが日本

で言っている違法と完全に同じなのかどうかもやや分からないようにも思いますが、そう整理しているようにも思ったのですが、いかがでしょうか。御感触か何かをいただければと思います。

【山本（龍）主査】　今の点に関して、森さんからチャットが入っておりますので、森さん、この点、ちょっと口頭で補足いただけますでしょうか。

【森構成員】　はい。すみません。先ほどヘイトが違法ではないとはっきり言ってしまったんですけれども、そんなことはなくて、ヘイトスピーチ解消法がありますので、必ずしも違法ではないとは言えない。公法上は違法であると思いますが、誹謗中傷とかプライバシー侵害とかとは違う扱いになっているかと思います。

そこだけちょっと訂正をさせていただいて、ただ、私が申し上げたかった全般的な違法指定が狭いのではないかということは、ほかのカテゴリー、１番とか４番とか、１番がテロで、４番がハラスメント・ストーキング・脅迫みたいなこと、脅迫は犯罪ですけれども、それから１５番の外国干渉、そういうものはあまり聞かないなと思っていまして、なので、全般的に違法指定が狭いということは言えるのかなと思いましたので、ちょっと補足をさせていただきました。

すみません。以上です。

【山本（龍）主査】　ありがとうございます。

それでは、まだいろいろと全容が明らかになっていないところで、答えにくいかもしれませんけれども、現状で御理解いただいているところで、ＮＲＩ様から、今の落合さんからの御質問に関してお答えいただければと思いますが、いかがでしょうか。

【野村総合研究所（齋藤氏）】　ちょっと全容が、今後具体的なガイダンス等を含めて、さらにフェーズ３を含めて、カテゴライズされたサービスまで含めて見えてくるのかなとは思っておりますけれども、今後追っていく中で、そもそものスコープとしている範囲ですとか考え方のところを踏まえて、整理・調査をしていきたいなと思っております。

ありがとうございます。

【山本（龍）主査】　ありがとうございます。

それでは、やや時間が押しておりますので、ＮＲＩ様からのプレゼンテーションに関しましてはここまでにさせていただきまして、ありがとうございます。

続きまして、生貝さんから御発表をお願いいたします。同様に、２０分間の時間厳守でお願いできればと思います。よろしくお願いいたします。

【生貝構成員】　今、資料を共有いたします。

それでは、私のほうからは、特に今ＤＳＡ等についてお話しいただきましたけれども、もう一つの切り口であるところのＡＩ規制という観点から、ＥＵにおける偽・誤情報対策というのを御紹介してまいりたいと思います。

基本的に内容としては、もう官報にもそろそろ載るＡＩ法案がメインになるんですけれども、少しデジタルサービス法の観点についても、特にＡＩに関わる部分を御紹介した上で、最後に、それらの相互補完関係というところも含めて、幾つかの論点を挙げるという形にさせていただきたいと思います。

さて、まずＡＩ法案につきましては、これはもう既に皆様もよく御存じのとおりのことが多いかと思いますけれども、もともと２０２１年４月に欧州委員会から提案されて、現在、段階としては、３月１３日に欧州議会の総会で採択されまして、この後、corrigendum、言語あるいは法律的な観点からのテクニカルなチェック、修正というところを経て、最後にＥＵ理事会から最終的な承認を得た形で、もう近日中には官報に掲載されて発行する、そして、ある程度の期間を取って適用開始といったような段階にございます。

今回の御説明におきましては、３月１３日に欧州議会総会で採択されたテキストというものをベースにしているという形になるところです。

そして、その概略といたしましては、御案内のとおり、ＡＩシステムを、基本的にリスクに応じて、禁止されるＡＩ行為、ハイリスクＡＩシステム、そして、特定のＡＩシステムに適用される透明性の義務、最後に、これは非常に幅広いですが、拘束性のないものとして、自主的な行動規範というような形が設けられているという、このことは、当初提案の頃から大きな枠組み自体は変わっておりません。

なんですけれども、今回少し見ていくとおり、内容はかなり当初の提案の当時からいろいろなものが加わっていたりするということがあることに加えて、何よりも大きなこととして、ここ１年程度の生成ＡＩの非常に大きな影響力の拡大というものを受けまして、この４類型とは基本的には別のものとして、生成ＡＩを含む汎用目的ＡＩといったようなものに対する規律の枠組みが別途設けられたという形になるわけであります。

それぞれにおきまして、まず少し禁止されるＡＩ行為というところについても見ておきたいと思います。これも当初段階からかなり様々なものが加わっているところであるのですけれども、基本的には、やはり極めて悪質性の高い、あるいは、基本権に対する悪影響というものが極めて大きいといったようなものを指定しているところでございますけれども、

これらについては、基本的に、御覧のとおり、どちらかというと、プロファイリングですとか、そういったことに関わる、ＧＤＰＲの上乗せ規律的なものが中心にはなっているところではあります。

そのため、特に偽・誤情報に対して、直接的にそれを規律するといったようなものはこの中には含まれていないわけでありますけれども、しかし、例えば、この２番目にあるような脆弱性の悪用というもの、これはそういったものを悪用して、特定の個人ですとか集団なんかに非常に大きな悪影響を与える、与え得るといったようなものを指定しているわけでございますけれども、限定的ではあるかと思いますけれども、場合によっては、そういうことも今回の議論とも関わり得るのかなということで、仮に挙げさせていただいているところでございます。

そして、続きまして、これがやはり我が国の注目としても非常に中心になってまいりましたハイリスクＡＩというところでございます。ハイリスクＡＩのカテゴリー自体は、これは上にございますもともとの、まさに安全確保するといったようなもののカテゴリー、そして、新たな指定と書いてあるところで、これは様々な観点がありますけれども、特にプロファイリング等のリスクというものを個別の領域に合わせてしっかりと上乗せ的な規制を課していくといったような側面が多いカテゴリーかなと思います。

バイオメトリクスが広く拡がったりといったようなことはあったりするのですけれども、しかし、このカテゴリー全体も大きくは動いてはいないところであります。

しかし、その中で一つ、幾つかの議論がされたことを少し付言しますと、審議プロセスの中で、デジタルサービス法のＶＬＯＰ／ＶＬＯＳＥが用いるレコメンダーシステムを、そのままハイリスクＡＩとして指定しよう、このＡＩ法でも規制しようといったような提案が欧州議会から出されたりしたこともあったんですけれども、それはＤＳＡですとか、あるいは、一部ＤＭＡによって規律されているということもあり、これ、最終的には、直接的にそれを含むことはしなかったといったようなことがございます。

でありますので、コンテンツモデレーションですとか偽・誤情報に本当に関係がないかといいますと、しかし、この司法または民主主義プロセスといったようなところが、これは最初の提案版ではなかった８の（ｂ）というのが付属文書Ⅲの中に追加されているところでございまして、特に選挙や国民投票の結果、または選挙や国民投票における自然人の投票行動に影響を与えるために使用されることを意図したＡＩシステムといったようなものを、ハイリスクＡＩとして最終的に指定することになった。この具体的な範囲でありますとか、そ

ういったことについては、まだ詳しい情報は出てきていないところなのですけれども、こういったことというのは、やはりこの議論とも関わりが出てき得るところかなと思います。

要求事項は大きくは変わっておりません。整合規格を通じて具体化していく共同プロセスといったようなところもございます。

そして、これも最後の段階では明確に含まれることになったハイリスクＡＩを配備するもの、これは、その権限に基づいてそのＡＩシステムを使用したりする人たちのことを指すわけでございますけれども、そうしたときに、基本権影響評価、つまり、どういった人たちにどういう影響を与え得るのかということをちゃんと評価して、当局への提出というものもしなければならなくなった。御承知のとおり、この基本権というところはかなり幅広いものでございますから、やはり大きなリスクが様々なことに生じ得る場合といったようなところにも対応しようとしているのかなと思います。

次に、特定のＡＩシステムの透明性義務というところでございます。このことについても、上の２つは少なくともいわゆる偽・誤情報といったところには関わることが多いかどうかはさておいても重要なところではありますが、今日は割愛させていただきたいと思います。

３つ目のところ、これも御案内のとおり、最初の段階からございましたけれども、このディープフェイク生成ＡＩシステムの配備者、それを使用する者というのは、当該コンテンツが人為的に作られたものであるということをちゃんと開示しなければならないということがある。

それに加えて、さらに新しく追加されたものとして、汎用目的ＡＩを含むコンテンツ生成ＡＩ提供者といったようなものは、これは提供者ですから、開発したり、開発させたりする側といったようなことになりますけれども、ＡＩシステムの出力がマシンリーダブルな形でマークされて、人為的に生成・操作されたことを検出できることを保証する。これを開発側でしっかりやらなければならないという義務が課されたわけでございます。

このことは何かと申しますと、まさにそれに対応する前文の１２０をここで引いておりますが、これはまさに今お話しいただいたデジタルサービス法のまさにシステミックリスク軽減のような義務というものを、効果的な実施を促進するために特に関連するとされている。これはやはりインターネット上で非常に様々なＡＩ生成コンテンツ、特にプラットフォーム上で流通する蓋然性というのがこれから高まる中で、彼らがしっかりとそれを機械的に検出して、しっかりとユーザーに伝えることができる、あるいは、彼らのコンテンツモデレーションポリシーに従った上で、削除等の対応を行うことも比較的容易にするといっ

たようなことと非常に深く関わる規律だと考えていただけるとよいのかと思います。

そして、こちらのスライドが、まさに汎用目的ＡＩの規律枠組みといったような形で、非常に大きな新しいカテゴリーとして設けられたものであります。

ここで特に特筆すべきは、汎用目的ＡＩモデル全般と、それの中でもまさにＥＵデジタルサービス法のＶＬＯＰ等のように、システミックリスクを有するような汎用目的ＡＩモデル、これはＦＬＯＰｓ等で一旦閾値を設けていますけれども、これは欧州委員会が後でより詳しい条件というものをつくったりすることが想定されています。この２つに分けられているのが特徴的なところです。

そして、この汎用目的ＡＩモデル提供者全般としては、設計や学習等の技術文書を当局に提供したり、あるいは、それを使用して具体的なＡＩシステムに落とし込む人たちが、ちゃんとこのＡＩ法を守れるような形の情報開示というものをしなければならない。さらに、これも別途様々議論されているとおり、特に著作権ですとか学習データに関わる情報の開示や遵守措置というのも非常に広く設けられているところ。

それに加えまして、特にシステミックリスクに関して、これはまさにＶＬＯＰのシステミックリスク枠組みというものを流用しているというところでございまして、しっかりとそれを特定して、軽減するためのレッドチームテストを実施したり、その文書化を含むモデル評価というものをちゃんと行うこと。そして、広く評価・軽減といったようなことを、まさにＤＳＡ同様に求めるに至っているといったようなこと。

そのほか、様々な規定と幾つかの義務というところもございますけれども、このことも、基本的にＡＩ法案側は、最終的なことは、これはCENとCENELECが中心になってつくる整合規格によって具体化するということを企図しているわけでございますけれども、しかし、やはりこちらの側でも、このＤＳＡと同じようなcode of practiceといったようなものは極めて重視されているところで、それにより様々な具体化が行われてくるといったような共同規制プロセスが想定されているのかなと思います。

そうしたときに、システミックリスク、この中で定義がされています。この特有のリスクであって、影響範囲の広さにより市場に重大な影響を及ぼし、公衆衛生、安全、治安、基本権もしくは社会全体に対する悪影響といったような形で想定されているわけでございますけれども、この中身がどういったものかといったようなことについては、例えば、前文の１１０に、こういった汎用目的ＡＩモデルといったようなものが、違法、虚偽、または差別的なコンテンツの流布を含むが、これらに限定されないシステミックリスクをもたらす可

能性があるということで、まさに偽・誤情報といったようなものが、そのシステミックリスクとして具体的に想定されているのかと思います。

そして、こういったときに、それをどうやってリスク軽減していくかといったような、これ、具体的に先ほど申し上げた義務との関わりでございますけれども、ミスインフォメーションですとか、大規模なマニピュレーション等のリスクを引き起こす可能性がある。そうしたときに、しっかりと先ほどのような機械が読み取り可能な形式で表示するといったようなことが、これ、例えば、いろんなレイヤーでそういうものを、これＡＩで作られたコンテンツですから気をつけてくださいねといったようなことをプラットフォーム側ですとか、あるいは、様々なブラウジングのレベルでも行ったりするといったようなことが想定されていると。ここでもまさに誤情報といったことが明示されているわけであります。

そして、一旦ここまでがＥＵのＡＩ法なんですけれども、これは既に私のほうも親会で一回御紹介しておりまして、今既に詳しく御紹介もいただいているところですけれども、デジタルサービス法も、ＡＩ規制というところから少しおさらいをしておきたいと思います。

このページというのは、もうよくよく御存じのとおりのことばかりですけれども、わけても、要点として挙げた３つそれぞれというのが、やはりＡＩにも深く関わるものであるということ。まず、このコンテンツモデレーションの規律といったようなことは、これはやはり透明性、アカウンタビリティといったような観点から極めて重要である。しかし、御案内のとおり、アルゴリズムによる意思決定、人間によるレビューの重要性といったようなことは、コンテンツモデレーションのプロセスの中でも極めて重要になっているところ、そのことをしっかり開示しなければならない。あるいは、それがどのぐらいエラーを起こすのか、そして、しっかりとそういったＡＩによる判断だということが分かった上で、本人が異議を申し立てることができるために理由の説明と内部苦情処理システム、裁判外紛争処理の利用といったような形で、これもまさしくＡＩによる判断、そして、それに対する人間の保護といったような側面が多いところ。

２番目のこちらのプロファイリング規制についても繰り返しになっているところでありますけれども、ターゲティング広告、パラメータ、レコメンダーシステム、まさに先ほどＡＩ法案に含むかということが直接的な議論の対象にもなった。それに加えまして、やはり特別カテゴリー、あるいは、未成年個人データのプロファイリング広告利用禁止といったようなことというのも、まさにＡＩの規律というところに深く関わるのであろう。

他方で、別の表現で言えば、既に御案内いただきましたとおり、こういったコンテンツモ

デレーションでありますとか、あるいは、プロファイリング広告といったところに関わることというのは、直接的にはＡＩ法のほうで規律するという形にはせず、やはりこちらのほうでプラットフォームレイヤーに関わる部分というのは基本的には委ねる、そういう判断というものが法制全体の中では行われていると見ることもできるのかなと思います。

そして、既に今回詳しく御紹介もいただきましたＶＬＯＰ／ＶＬＯＳＥのリスク軽減義務といったようなことがあるわけでございます。このことというのが、大きな枠組みとして、ＡＩ法の中でも取り入れられたということになったわけでございますけれども、次のページで、関係性というものが果たしてどうなっているのかということについて、前文の１１８というところを引いてきております。

このことは少し読み方が難しく、僕自身も、このＡＩ法案最新版を少し解析中の部分が多いところであるのですけれども、これは具体的に何かというふうに申しますと、この規則は、ＡＩシステム及びモデルを規制するものである。そういった、まさに汎用目的ＡＩモデルといったようなことがＶＬＯＰやＶＬＯＳＥに組み込まれた場合には、それはまさにデジタルサービス法に規定されたリスク特定軽減の枠組みの対象になると。

なので、やはり多くの場合、この汎用目的ＡＩ、生成ＡＩのようなものって、しばしばＶＬＯＰのようなものの中に組み込んで使われることというのが恐らく圧倒的に多くなってくるのだと思います。それだけではもちろんございませんけれど。そうしたときに、まずそのことはしっかりそちらでやっていただく。そして、デジタルサービス法が想定していないような重大なシステミックリスクが出現していたりといったようなことがない限りは、デジタルサービス法の枠組みによってしっかりその義務が果たされていると推定されるべきであるといったようなことも書かれているところでございます。

まさにこういった２つの法の関係性といったようなことが、これから具体的な運用の中でも非常に重要な論点にはなってくるのかなと思います。

最後に、幾つかの論点をまとめの代わりという形で挙げさせていただきました。

まずＡＩ法案、これはやはりＡＩを作ったり、作らせたり、あるいは、それを使用する様々な人たちの義務といったようなものを基本的には規律している。

そして、焦点として挙げている、対象としているリスクというのは、非常に大きく言うと、この３つなのだろう。

ＡＩシステム全般に関わる製品安全、これ自体は、恐らくそんなに今回の偽・誤情報、健全な情報流通というところにはさほど関わってこないかもしれない。

他方で、やはりプロファイリングといったようなところに関しては、これはコンテンツモデレーション、広告、あるいは、レコメンダーといったようなところとの関わりでも、様々な影響というものがもしかすると出てくるかもしれない。しかし、デジタルプラットフォームに関わる部分というのは、基本的にはデジタルサービス法のほうの規律に委ねているといったようなことはある。

そして、やはり汎用目的ＡＩというところに関することについては、今日申し上げたとおり、まさに偽・誤情報、そして、それにとどまらないマニピュレーションですとかディセプティブ行為全体というものを、ちゃんと開発、つまり、提供者の側でしっかり守っていただく、そういった形になっているといったようなこと。

例えば、まさしく今日本でも様々議論がされているＡＩセーフティインスティテュート等によるリスクの管理といったことは、ＥＵでは欧州委員会と、まさしくそれに付随する様々な各国当局が協力して対応するということになっているところでありますけれども、そういったことと併せて、そして、他方で、デジタルサービス法は、まさにプラットフォームレイヤーにおけるＡＩがもたらし得る情報流通へのリスクを非常に広くカバーしているといったような対応関係になるのだろう。ＡＩ、コンテンツモデレーション、レコメンダー、プロファイリングの透明性ですとか、利用者保護というものをしっかり規律する。

その上で、まさにＡＩ法との補完関係というものも意識しながら、ＡＩ生成コンテンツ流通への対応というのを、御紹介いただいたような行動規範ですとか、危機対応プロトコルといったようなところを含めて、しっかり対応していく。そういうつくりになっているのかと思います。

そして、重要なのは、やはりこの２つというのは、非常に深い相互補完関係にあるということであります。非常に様々なものがあると思うのですけれども、少なくとも挙げられることとしては、繰り返しにはなりますけれども、ＡＩ法案の側で、ちゃんとＡＩ生成コンテンツというものを、マシンリーダブルな形も含めて、しっかり検出可能にしていただいたりする。よくウォーターマーキングというふうに言われたりしますけれども、そういうものもある種活用しながら、デジタルプラットフォーム側でも、システミックリスク軽減の一環としたりして、しっかりとその対応をしていくといったようなことが一つは挙げられましょうし、また、もう一つは、やはりいずれの側にも存在するシステミックリスク軽減義務といったようなことが、まさにデジタルプラットフォームに組み込まれた場合は、しっかりとそういうところも見てやっていく。他方で、それに含まれないような場合というのは、まさにＡ

Ｉ法案がしっかりとした対応をしていく。

こういった、まさに我が国においても、ＡＩレイヤーとデジタルサービスプラットフォームレイヤーの議論というのが、この文脈でも様々進んでいく上での参考になる部分というのは多いのかなと思います。

私から以上でございます。

【山本（龍）主査】　ありがとうございます。時間を守っていただいて、大変助かりました。ありがとうございます。

それでは、今の御説明、プレゼンに関しまして、御意見、御質問がございます方は、挙手機能またはチャットで発言希望の旨を御連絡ください。大体残り２０分ぐらいでしょうか。よろしくお願いいたします。

私のほうから、２点伺えればと思います。

最後の話で、ＡＩレイヤーとプラットフォームレイヤーの規律の相互補完関係が重要だというお話で、これはＥＵが参考になるのではないかというお話でした。日本の場合に、どちらも今現状においては立法がない状態ではあると思います。特にＡＩレイヤーについて、今、我々はプラットフォームレイヤーについて主に検討しているわけですが、そのＡＩレイヤーについて、現状は事業者ガイドライン等がありますけれども、さっきのウォーターマークの義務づけみたいな話とか、やはりそういった形で、相互補完的ではないと逆にプラットフォームレイヤーも機能しないみたいなところがあるのかどうか。そうすると、今の参考になるとおっしゃっていただいたところが何を含むのかというところかなと思うんですけれども、もし何か現状においてお考えがあれば教えていただきたいというのが１点目です。もう一つが、スライドの３ページ、ハイリスクＡＩ配備者の義務で、基本権影響評価の実施と当局への提出というところがあるんですが、この基本権影響評価の具体的な内容というか、システミックリスクとの違いというんですか、その辺り、少し伺えればと思いました。

すみません。２点、お願いいたします。

【生貝構成員】　ありがとうございます。

まず１点目につきましては、まさしくＧ７などで合意された枠組みに基づいて、それをソフトローでやるのか、ハードローでやるのかということが、我が国も含めた様々な議論になっているところ。

一つは、やはりまさに御言及いただいた事業者ガイドラインにおいても、拘束力というのはＥＵとの違いというのもあるところでございますけれども、しっかりとまさにここで挙

げたような、ここのデジタルプラットフォームレイヤーでの問題として重要となること、あるいは、まさにＡＩレイヤーで独立にしっかりやっていただかなければならないこと、これは例えば脆弱性を悪用するような働きかけというのは基本的にやるべきではないよねでありますとか、場合によっては、選挙等、民主的プロセスに関わるようなことというのは、プラットフォーム側の規律だけでどうにかするといったようなことは、これはまたなかなかできない部分でもあるのだろう。そうしたようなことをしっかりとああいったガイドラインの今後の発展の中でも考えていく価値があるのだろうといったこととともに、まさしく我が国でも、特にＥＵ法でいうところの汎用目的ＡＩ、特に巨大なものについては、一定の体制整備等の規律が必要なのではないかといったようなハードロー側の議論なんかも出てきているところ。しっかりこういったプラットフォームレイヤーの議論と、そういった新たな施策の整合性を意識することが、やはりまずは示唆として挙げられるのかと思いました。

それから、２つ目といたしまして、この基本権影響評価といったようなところは、これはやはり条文上もＧＤＰＲのインパクトアセスメントを補完するものという形で位置づけられているところであります。当然、システミックリスク特定評価のような非常に詳細な、そして、それを具体的に頑張って軽減するという義務までは設けないのだけれども、やはりどういうリスクがあり得るのかということをしっかりとチェックをした上で、ちゃんと特定をして、当局とも共有していこう。近い部分はあると思うのですけれども、やはり相対的にはライトな義務だというのが一つの観点としては言えるのかなと思います。

取りあえず以上です。

【山本（龍）主査】　ありがとうございます。

１点目のところで、これは私の感想めいたことですけど、やっぱりＥＵのＡＩ関連、ＤＳＡも含む法制度というのが、基本権保障を究極の目的とした、ある種の体系性というものをつくってきていて、その中でのシナジーですとか相互補完関係が体系的につくられてきている部分があるのかなと思いました。その相互補完性というのは、今後はやはり非常に重要になってくるのかなと、今コメントを伺って思いました。ありがとうございます。

【生貝構成員】　ありがとうございます。

非常におっしゃるとおりかと思っており、基本権という基本的な背骨があり、しかし、またそれと同時に、やっぱり体系性といったようなことが、いろいろな意味で拡がってきている、複雑化してきている。今日ＡＩ法案とＤＳＡの相関関係だけを挙げましたが、例えば、ＧＤＰＲとの補完関係というのもそれぞれ極めて複雑ですし、またさらに、今日は挙げなか

ったんですけれども、別途最終段階に入っている女性への暴力撲滅指令案という中では、そういった特に問題のあるディープフェイクに関して、直接的な禁止の対象とするといったような形での、ある種のバーチカルの規制といったようなところも別途設けられていたりするところでございます。まさに様々な制度枠組み同士の相互補完、その体系というのを我々も考えていく必要があるんだろうなと感じているところです。

【山本（龍）主査】　ありがとうございます。

それでは、石井さん、よろしくお願いいたします。

【石井構成員】　ありがとうございます。法制度の相互補完関係、非常に重要な論点だと思って伺っておりました。

それに関係するところではありますが、プロファイリングに関する規律がいろいろなところで出てきているというところで、とりわけＡＩ法の中でも禁止されるＡＩ行為として、非常に問題のあるものが挙げられているという中で、プロファイリングという観点から見たときに、日本の法的なアプローチとして、どういう対応が望ましいのか。先ほどレイヤーごとの御説明もあったところですが、日本における現状の法制度を基にしたときに、どういう規律の在り方が望ましいのか。非常に漠然とした御質問ですが、お考えがあればお聞かせいただきたいということが１つ。

それから、ＡＩ法案の中で、禁止されるＡＩ行為、これ、非常に問題があるのだという認識ですが、どのようにそれを見つけて執行していくのかが疑問としてありまして、運用方法の課題というのはやはりあるのかなと。この点についても、お考えがあればお聞かせいただければと。

最後に、今日御紹介いただいた法令以外にも、例えば、ダークパターンですと、消費者保護関係の不公正取引方法指令の規制対象になり得るという話で、さらに関係する法令の広がりもあるのではないかとなると、内容が混乱しそうだということが、全体的な印象としてはあるということでして、この辺りも、もし研究される中で問題意識等あれば教えていただければと思います。お願いします。

【生貝構成員】　ありがとうございます。

ダークパターンの部分、申し訳ございません。ほかの分野というと。

【石井構成員】　不公正取引方法指令。

【生貝構成員】　まさしくおっしゃるとおりです。ありがとうございます。

それでは、まず１点目といたしましては、まさしく我が国の法体系上、プロファイリング

をどのように位置づけていくのかというのは、極めて難しい問題でございまして、御案内のとおり、ＥＵ法のようなプロファイリング規制というのは、我が国の個人情報保護法本法の中には設けられていないといいましたときに、１つは、私自身の考えとしては、個情法のほうでもベースラインとしての立法の在り方というものをそろそろ本格的に考える余地はあるのだろうとは考えておりますが、それは少しここのスコープからは離れるといたしましても、しかし、やはりＥＵの法体系といたしましても、例えば、プラットフォーム上でも生じ得る特別なプロファイリングのリスク、あるいは、ＡＩで生じる特別なプロファイリングリスクといったようなものは、しっかりと特定をして、ちゃんとした規律をＧＤＰＲ本法とは関連しつつも、また別途規律するといったようなことをやってきているところ。

我が国としても、ハードロー、ソフトロー、いろいろな方法論はあると思うのですけれども、こういった重要なＡＩですとか、プラットフォームですとか、そういった事ごとにおける、特にやはり規律の対象とすべき類型というものをしっかり議論した上で、ちゃんとした枠組みの在り方を考えていくというのが重要なのかというのがまず１点目であります。

２つ目といたしまして、執行については、これ、非常に難しいところかなというところも出てくると思います。まさに当局としては、各国の執行当局を含めて、非常にリソースをこれから割いていくことになるかとは思うのですけれども、やはりこれ全体を通じて、例えば、このハイリスクの場合ですとか、そういったところについては、しっかりと情報の開示ということもしていかなければならないといったような情報提供の義務というのも、今日、あまり深くは触れられていないのですけれども、含まれている。それをやはり本人も、そして当局側もしっかりと把握していくことができるような透明性の在り方というのが大変重要なのかなと思います。

最後に、ダークパターンについては、おっしゃるとおり、やっぱり消費者保護系の各種の指令などでも様々扱われているところ。しかし、これはＧＤＰＲとこういったＡＩ提供者等に対する規律の補完関係というところの最たるものでもありますが、やはり被害が起こって初めて救済することができるといったタイプの規律枠組み、また、それとは他方で、ＡＩ法やデジタルサービス法が規定しているのは、事業者として、しっかりとサービス提供段階で、こういった安全措置を取らないといけないんですよという意味での、まさに事業者規制、体制整備、そういったことの補完関係というのは、こういった枠組みの中でも重視されているのかなと感じるところでございます。

【石井構成員】　よく分かりました。ありがとうございました。

【山本（龍）主査】　ありがとうございます。

それでは、次、水谷さんからお願いいたします。

【水谷構成員】　ありがとうございます。

私も、このＡＩ法案とＤＳＡの関係性どうなっているんだろうというのはすごく興味を持っていたので、今日の先生のＡＩレイヤーとプラットフォームレイヤーで整理できるというような最後のまとめを伺っていて、なるほどと思いました。

それで、私の頭の中がこんがらがっていて、整理ができていない部分があるかもしれないんですが、今日の先生のお話について、私の理解ですと、プラットフォームレイヤーでコンテンツモデレーションがレコメンダー、プロファイリング、あと、生成ＡＩもそうですけれども、それらについては、ＤＳＡがきちんと規律をすると。しかしながら、ＡＩ法案が、それこそ偽・誤情報も含む、民主主義のプロセス等のリスクがあるものと関係ないかというと、やっぱりそうではなくて、ハイリスクＡＩの中に、レコメンダーの仕組みは外されたけれども、一応大枠としては関係するものは入っているという立てつけだったと思うんですね。レコメンダーの部分は入らなかったけれども、司法とか民主的プロセスに関連するという大枠の部分は押さえているみたいな感じだったと思うんです。

そう考えると、特に選挙とかに絡むものだと思いますけど、プラットフォームレイヤーの部分において、ＤＳＡで規律をされていないけれども、ＡＩ法案の部分で、こういう民主主義プロセスに関連する規律を受ける、ＡＩリスクとして規律を受けるＡＩというのは、どういうものがあり得るのかなという、役割分担というか、規律の分担の部分について、もし先生のほうで考えているという部分があれば、ちょっとお伺いしたいなと思います。

以上です。

【生貝構成員】　ありがとうございます。

やっぱりデジタルサービス法が偽・誤情報で対象にできているのは、あくまでＶＬＯＰである。そして、他方で、やはりこのＡＩレイヤーですと、ＶＬＯＰ以外にも様々な形で波及することがある。あるいは、そういった独立した事業者さんなんかも別途存在するといったときに、例えば、禁止ＡＩの中にあるような、こういった脆弱性の悪用というのが、もしかするとそういった民主主義に関わるところにも影響してくる可能性はあるかということのほかに、やはり特に個人的に着目したものは、最終的に（ｂ）が丸ごと追加された司法及び民主的プロセスの、特に選挙、国民投票といったようなところでございますね。

もともとの条文ですと、いわゆる裁判で使われるようなＡＩだけが（ａ）として含まれて

いたところ、こういった形で含まれたことによって、やはりこのＡＩ法独特の規律の在り方というのもこれから具体化されてくるのかなと思います。

お答えになっているか、大丈夫でしょうか。

【水谷構成員】　ありがとうございます。

やっぱり、今表示されている付属文書の８の（ｂ）のところが重要なんだろうなと思います。私の中でも、どういうものがそれに当たるだろうと考えたときに、実際にＡＩ法でこれが当たるかどうか分からないですけど、それこそ、最近日本でもちょくちょく出てきていますが、政党マッチング、つまり、アンケートとかに答えると、自分の考えと近いような政党とか投票先をマッチングしてくれる仕組みってありますよね。もちろん、あれは現状だとＡＩというほど高度ではないわけですけれども、あれをもっと高度にしたものなんかがこういうものには入ってくるのかなというのを何となくイメージとして浮かんでいたので、影響を与えるという意味で、どこまで対象に入るのかがちょっと分からないですけれども、結構広く射程に含まれるのかなと思いながら、今の先生の御回答を聞いておりました。

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す。

【山本（龍）主査】　ありがとうございます。

私の進行の不手際で、ちょっと時間が押してまいりましたので、この後、御質問、御回答はなるべく簡潔にお願いできればと思います。

それでは、落合さん、お願いいたします。

【落合構成員】　ありがとうございます。そうしましたら、手短にとは思います。気づいた点を幾つか申し上げますので、可能な範囲でお答えいただければと思います。

１つが、モデレーションの点について、御発表の中で御指摘いただきましたが、米国等の論文を最近ちょっと読む機会があって、見ていますと、個別のモデレーションだけではなく、プラットフォームのアーキテクチャであったりですとか、例えば、そもそもの表示や、警告のつけ方など、個別のモデレーションに限らず、アーキテクチャのようなところ自体も誤った情報拡散を進めたりすることもあるように思われます。これに対して働きかけをするということ自体も、個別のコンテンツのモデレーションだけではなく、こういったプラットフォーム規制の中において考慮するということが、現実的な解としては重要な部分もあるのではないかと思っております。この点について、欧州のほうでどう見られているか、もし何かお気づきのところがあればということがあります。

第２点が、ＡＩの関係ですが、プラットフォームのモデレーションとの関係では、結局、自動的にモデレートしているものと、人がモデレートしているもので、全く違う結果が出るようなこともあるように思っております。かなり機械的にというか、必ずしも別にＡＩに限らなくてもいいとは思いますが、アルゴリズムではじくという場合には、機微的な判断は基本的にあまりできずというか、間違った判断を下手すると繰り返すということで、人が関与しているかしていないかで、かなり結論が変わってくる部分もあると思います。

ただ、一方で、米国の論文などを見ておりますと、人が見てしまうと、例えば、１時間に数万件の問題があったときに、それに人が対応することはできないであろうと。そうすると、もちろんアルゴリズムというか、ＡＩの側に対応してもらったからこそできることもあると思われるところはあいます。一方で、人が関与しないとまたおかしいことが出てしまう可能性もあります。この辺りについて、欧州の場合は、ＡＩ規則ですとか、ＧＤＰＲのプロファイリングにかかる部分も、かなり人の関与というのを言っておりますが、このコンテンツモデレーションの関係での人の関与について、どういう議論があるか御存じのところがあれば教えていただきたいということがあります。

最後は本当に気づいた点ではありますが、意思決定を誤らせることや、もしくは、何か誤った働きかけを欺瞞的に行っていくことは、やはりかなり重要なプロセスのように思っております。米国の場合ですと、ＦＴＣ法を中心に、そちらのほうを主に取り締まっているような感じもいたしますが、この点について、欧州側でどう評価しているかわかることがあれば、教えていただければと思いました。

すみません。もう本当に時間はないと思うので、可能な範囲でと思います。【生貝構成員】

ありがとうございました。では、３つ、簡単に。

まず１つ目のアーキテクチャ等への着目というのは、デジタルサービス法がまさにシステミックリスクの特定軽減義務というものを導入したことによって、様々な法体系の中でも非常に包括的に初めてそれを扱うことができるようになった。私自身、まさにシステミックリスク条項はそこに着眼しているという認識でいるというのがまず１点目です。

それから、２つ目として、やはりモデレーションにおいても、ＡＩに相当程度頼らなければ絶対にモデレーションはできませんし、そのことは極めて重要であり、しかし、やはり人間の役割は重要である。どう関わっていくか。そして、どれだけの人間を、ＡＩで、例えば、１００億をさばきながら、１００分の１が落ちてくるだけでも、毎日１億必要なのですよね。といったようなときに、人的体制整備をどのようにしていくかというのが大変重要であり、

であるから、デジタルサービス法の透明性レポートの中でも、人的リソースといったようなものの開示を大変重要視しているという部分がある。

３点目に、まさに意思決定、欺瞞的行為というのは極めて重要である。このことは、やはり欧州のほうも、消費者保護法制の中で様々存在するのですけれども、今回、まさにＡＩ法の中でも、かなり消費者保護といったようなところに対して着目した記述というのが、様々な形で出てくるわけでございます。まさにＡＩ法、事業者、あるいは開発者規律でなければできない利用者保護の在り方という両面からしっかり考えていく必要があると認識されているんだと思います。

以上です。

【落合構成員】　ありがとうございます。

【山本（龍）主査】　ありがとうございます。

それでは、森さん、お願いいたします。

【森構成員】　ありがとうございます。大変勉強になりましたし、頭も整理されました。

私は意見なんですけれども、親会の下で私、プレゼンをさせていただいたのは、かつてのプラ研が持っていた課題が、誹謗中傷と偽情報とデータ保護で、それに対する対応のアプローチ、これは横積みで書いたんですけれども、それがリテラシーとＡＩとプラットフォームだということを書きました。

その趣旨は、それぞれの課題に対応する、特にＡＩとかプラットフォームというのはコントロールポイントだと思うんですけれども、行けるところまで行こうと。あまり概念的な体系的な議論をせずに、行けるところがやろうという、現実的になろうという御提案だったわけですけれども、今、落合先生も、我々のような場合に、プラットフォームについての検討ということがあるわけだから、それは現実的なのではないかというお話がありました。私も全く賛成で、我々は偽・誤情報対策を担当していて、かつ、プラットフォームを見ているので、そこでできることをするというのが現実的なのではないかなというふうに感じました。

そのできることというのはどういうことかということですけれども、今日、生貝先生の御説明を聞いていて、本当にしみじみ思ったんですが、やっぱりプロファイリングですよね。生成ＡＩによって偽情報のコンテンツなりクリエーティブが増えるということと、もう一つは、これは生成系ではないですけれども、予測系だと思いますけれども、プロファイリングによって、刺さりそうな人を探し出して、そこに行くと。コンテンツとしてではなく、広告としてということになると思うんですけれども、そのプロファイリングの部分がもう非

常に緩くなっていて、プロファイリング天国となっているのではないかと思っていまして、１０ページのスライドでお示しいただいた、例えば、特別カテゴリーのプロファイリング広告利用禁止というようなことがありましたけれども、我が国では、データ保護法においては、プロファイリングというのはもう利用目的の特定ぐらいの話しかなくて、要配慮個人情報を生成することも取得に当たらないのではないかと。つまり、要配慮個人情報の取得として、本人の同意を要しないのではないかみたいな、そういう話になりつつありますので、そのプロファイリングのところがごっそり抜けている。それによって刺さりそうな人を探すとか、その人に対してだけメッセージを送信するということが全然可能になっていて、それがひいてはマインドハッキング等が民主主義への脅威につながるのではないかということがあろうかと思いますので、やはりその点、プロファイリングのところを考えていくということが、健全性の検討会、あるいはこのWGでも重要なのではないかなと思いました。

以上です。

【山本（龍）主査】　ありがとうございます。

生貝さんから一言だけ、何か今の点にコメントがあればと思いますが。

【生貝構成員】　ありがとうございます。

全体的に、特に、まずしっかりプロファイリングに取り組んでいくことの重要性、私も全くおっしゃるとおりだと思います。

【山本（龍）主査】　ありがとうございます。

山本健人さんから、お時間があればお願いしますということなんですが、大変申し訳ありません。お時間はもうないということになりますので、メールで事務局を経由して御質問をいただければと思います。山本健人さん、大変申し訳ありません。

構成員の皆様、オブザーバの皆様、それから、聴講いただいている皆様に関しましても、時間が予定より超過しております。大変申し訳ありません。

それでは、本日ですけれども、今日は本来、自由な意見交換もと思いましたけれども、かなり情報量も多くて、おなかいっぱいというところかもしれませんけれども、ここまでにさせていただいて、インプットいただいた情報というのは、今後しっかり整理をして、日本ではどのような取組が必要かという具体的な議論へとつなげていきたいと思います。

それでは、本日はここまでにさせていただいて、最後に、事務局から何か連絡事項はございますでしょうか。

【髙橋係長】　ありがとうございます。次回ワーキンググループ第１３回会合につきまし

ては、来週４月８日月曜日、１３時から検討会第１６回会合との合同開催を予定しております。議事等詳細につきましては、別途事務局より御案内させていただきます。

以上です。

【山本（龍）主査】　ありがとうございます。

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健全性確保の在り方に関する検討会」ワーキンググループ第１２回会合を閉会いたします。本日はありがとうございました。