参考資料WG5－3

※参考資料９－２再掲

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（第７回）・
ワーキンググループ（第１回）

１　日時　令和６年１月25日（木）15時00分～17時00分

２　場所　オンライン開催

３　出席者

（１）構成員

宍戸座長、山本（龍）座長代理、生貝構成員、石井構成員、越前構成員、江間構成員、奥村構成員、落合構成員、クロサカ構成員、後藤構成員、澁谷構成員、曽我部構成員、田中構成員、増田構成員、水谷構成員、森構成員、安野構成員、山口構成員、山本（健）構成員、脇浜構成員

（２）オブザーバー

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）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専門職

４　議事

（１）　ワーキンググループについて

（２）　基本的な考え方について

（３）　意見交換

（４）　今後の進め方

（５）　その他

【宍戸座長】　それでは、定刻でございますので、「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」の第７回会合と、前回の会合で設置をお認めいただきましたワーキンググループの第１回の会合、これは合同会議ということになりますけれども、開催をさせていただきます。本日も御多忙のところ、会合に御出席をいただき、誠にありがとうございます。

議事に入る前に、事務局より連絡事項の説明をお願いいたします。

【内藤補佐】　本日事務局を務めます、総務省の内藤です。

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、議事次第のとおり、資料７－１－１から参考資料７－３までの１１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、傍聴者の方につきましては、本検討会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、越前構成員、田中構成員は会議途中から御出席予定、曽我部構成員は会議途中で御退席予定と伺っております。

事務局からは以上でございます。

【宍戸座長】　ありがとうございます。

それでは、まず冒頭、本日の議事の進め方につきまして、私より御説明を申し上げます。

まず（１）といたしまして、先ほど申し上げましたとおり、前回、設置について御了承をいただきましたワーキンググループについてでございます。この件につきましては、前回の会合で主査として指名をさせていただきました山本龍彦構成員、それから私、そして事務局に御一任をいただいておりましたけれども、このたび設置の運びになりましたということで、事務局より御説明いただきたいと思っております。

続きまして、（２）、それから（３）といたしまして、この会合における、デジタル空間における情報流通の健全性に関する「基本的な考え方」の議論・検討に向けまして、本日は、まず後藤構成員より御発表をいただき、質疑の時間を設けたいと思っております。

そして、前回会合におきまして、私より、これまでの議論で見えてきた部分、それから深掘りしていく部分を踏まえて、デジタル空間における情報流通の健全性について、基本理念、それからステークホルダーに期待される役割を、これまでのこの検討会の会合で構成員の皆様からいただきました様々なインプットも踏まえて、一度整理をするよう事務局に依頼いたしました。そこで、事務局において作成されました「これまでの主な御意見・全体像・基本理念・ステークホルダーの役割」につきまして御説明をいただき、「基本的な考え方」について構成員の皆様から議論をいただきたいと考えております。

最後に（４）でございますが、「今後の進め方」についてお諮りをしたいと思います。

以上が本日の進行の予定でございます。お聞きいただいてお分かりいただけますとおり、本日も大変盛りだくさんでございますので、議事進行にどうぞ御協力をお願いいたします。

それでは、早速議事に入らせていただきます。

（１）でございますが、ワーキンググループの設置について、事務局より資料に基づいて御説明をいただければと思います。

【内藤補佐】　承知いたしました。事務局でございます。まず、資料７－１－１を御覧ください。画面共有をお願いできますか。ありがとうございます。こちら、ワーキンググループの開催要綱案となります。

ポイントを御紹介いたします。

まず、「３　検討事項」について、（１）事業者の取組に関する透明性の確保の在り方、（２）事業者のビジネスモデルに起因する課題への対応の在り方などを記載してございます。

次に、「４　構成及び運営」につきまして、（２）のとおり、構成員は、別紙のとおりとされております。また、（４）におきまして、主査は、主査代理を指名することができるとされております。こちらに基づき、本日、主査代理につきましては、事前に曽我部構成員に御内諾いただいていると承知しております。続きまして、（６）において、主査は、構成員又はオブザーバーを追加できるとされております。また、（７）において、主査は、構成員以外の出席を求め、その意見を聴くことができるとされております。

続きまして、「５　議事・資料等の扱い」につきまして、（１）において、本ワーキンググループは、原則として公開とすること、（２）において、資料及び議事概要は、原則として公開することとしてございます。

続きまして、資料７－１－２を御覧ください。こちら、本検討会の開催要綱となります。昨年の本検討会第１回会合で御了承いただきました資料１－１の開催要綱からの更新箇所

を御説明いたします。

２ページを御覧ください。まず、ワーキンググループの設置に伴いまして、曽我部構成員及び山本健人構成員を構成員名簿に追記しております。また、事務的な修正となりますが、第１回会合で座長及び座長代理について既に御了承されておりますので、このタイミングとはなりますが、座長及び座長代理の記載について更新しております。

事務局からは以上でございます。

【宍戸座長】　ありがとうございました。ただいま御説明いただきましたワーキンググループ及び検討会の開催要綱それぞれにつきまして、案のとおり、構成員の皆様、御了承いただけますでしょうか。

（「異議なし」の声あり）

【宍戸座長】　ありがとうございます。チャット欄でもいただいております。ありがとうございます。

それでは、これは親会、そしてワーキンググループいずれについても御了承いただいたものとしたいと思います。

つきましては、ワーキンググループ主査をお務めいただきます山本龍彦構成員、それに今回からこの親会、それからワーキンググループに加わっていただきます、ワーキンググループ主査代理の曽我部構成員、それから山本健人構成員、それぞれから一言ずつ御挨拶いただければと思います。

まず、山本龍彦先生、お願いいたします。

【山本（龍）構成員】　主査を拝命いたしました山本でございます。大変重要な使命を負っていると認識しておりますので、表現の自由にも配慮しながら、有効な偽情報等の対策を具体的に検討できればと思っております。どうぞよろしくお願いします。

【宍戸座長】　ありがとうございます。

それでは、曽我部先生、お願いいたします。

【曽我部座長代理】　ありがとうございます。京都大学の曽我部と申します。このたび親会のほうの構成員、それからワーキンググループのほうでは主査代理ということで仰せつかっております。

私、専門は憲法でございまして、憲法の観点から、インターネットにまつわる様々な問題を研究してまいりました。今回の検討会、それからワーキンググループのテーマであります デジタル空間における情報流通の健全性確保というのは大変重要な問題でございまして、

この検討に参加できるということは大変光栄に思っております。

途中からの参加ということで、まずはキャッチアップをさせていただき、何らかの貢献ができますよう努めたいと思いますので、どうぞよろしくお願い申し上げます。

【宍戸座長】　よろしくお願いいたします。

それでは、山本健人先生、お願いいたします。

【山本（健）構成員】　北九州市立大学の山本健人と申します。私も専門は憲法学でして、この分野ではデジタル立憲主義と言われる議論を検討しております。その他、偽・誤情報について言えば、カナダでの対策の状況についても若干ですが勉強したことがあります。

新参者で、かつ若輩者ではありますが、こういった機会をいただきまして大変光栄に思っております。ぜひ貢献したいと思いますので、よろしくお願いいたします。

【宍戸座長】　よろしくお願いします。

３先生に加えまして、既に親会のメンバーであります生貝先生、石井先生、落合先生、水谷先生、森先生にお加わりいただいてワーキンググループを運営していただき、専門的に論点を深掘りしていただくということで、合わせて８人の先生方には、改めまして私からもどうぞお願いを差し上げたいと思います。ありがとうございました。

それでは続きまして、議事（２）に移ります。「基本的な考え方」について、構成員の皆様から御発表いただき、議論を深めていくというラウンドが続いておりますけれども、本日は後藤構成員から御発表をいただきたいと思います。資料７－２－１ですね。どうぞよろしくお願いいたします。

【後藤構成員】　後藤でございます。御紹介ありがとうございます。

早速ですが、資料を共有させていただいて、お話をしたいと思います。私はサイバーセキュリティ実務に近い立場におりますので、今日は、その観点から一言話をさせていただきます。

最初の１ページ目、それから２ページ目は、初回の検討会にて自己紹介を兼ねてお話をしたものです。私としては、偽情報・誤情報の問題、非常に大きく難しい問題だという意味で、継続的な取組をどうやっていくかが課題だなと感じました。特に、多角的かつスパイラル的に取組を継続するための仕組み、これが大事だなと。今、サイバーセキュリティ対策では、悪戦苦闘しながら継続的に取り組んでいるわけでして、偽情報・誤情報対策も同じく長期戦になるなと覚悟をしたところです。

今日のお話ですが、主にサイバーセキュリティ確保の観点から、それと偽情報・誤情報対

策を、サイバーセキュリティ確保と対比させながら、見ていきたいと思います。私がこの委員会の場で勉強させていただいたことも含めて、私の理解で書いておりますので、間違い等があったら遠慮なく御指摘をいただきたいと思います。

最初に皆様と視線を共有するために、サプライチェーンのサイバーリスクを中心に御紹介した後、本論に入りたいと思います。

これは私がよく使っている図ですけど、いわゆるフィジカル空間、サイバー空間、ここでいろいろなものが動きつつある。ＩｏＴサービスや、重要インフラ、クラウド、ＡＩ、いろいろなサービスが動いているわけですが、この中にはいろいろなサプライチェーンがあると。例えば普通の製品のライフサイクルの全体のサプライチェーンですね。自動車は典型です。作ってから利用し最後に廃棄するまでつながります。それ以外にも、今日の主題ですが、ソフトウェアのサプライチェーンがあります。それからクラウドのサプライチェーンもあれば、複合サービスのサプライチェーン、個人向けサービスもあります。今後は、ＡＩとかロボットのサプライチェーンもいろいろ出てくる。多様なサプライチェーン全体にわたって、いろいろなステークホルダーが絡んでいる中でサイバーセキュリティ確保をどのように進めていくか、これが最近の私の主な仕事ということになります。

ここで取り上げるソフトウェアのサプライチェーンは、今、大きな問題となっております。といいますのは、この三、四年でソフトウェアのサプライチェーンのセキュリティリスクが非常に高まっていて、2020年から2023年までにインシデントが７倍増と、急増しています。

いろいろな要因があります。大きなポイントは、非常に有用で、かつ広く使われておりますオープンソースソフトウェア（ＯＳＳ）です。ＯＳＳは有用で、いろいろなところでたくさん使われています。多くのソフトウェアシステムの共通の部品として使われていることが一番のポイントですね。このようなＯＳＳ部品にも脆弱性が残ってしまうので、そこを攻撃されてしまうと、世界中の何億というＩｏＴやスマホなどが一斉に攻撃されてしまうことも起こり得るということです。

実際にある調査では、世の中のコンピューターとか制御機器で動いているソフトウェアコードの９６％は何らかの部品として、オープンソースソフトウェアを使っているとのことです。一番の典型例は、ＴＣＰ／ＩＰスタックです。

ソフトウェアサプライチェーンの問題が顕著になったのは、２０２０年のソーラーウィンズという事案からですが、この事案以降、ソフトウェアのサプライチェーン全体にはセキュリティの透明性の向上が必須であるということが言われ出しました。それを正面切って

言い出したのが今のバイデン政権による、２０２１年の大統領令です。この中で、連邦政府を挙げてソフトウェアの透明性に取り組みなさいという指令が出ました。

いろいろな機関がガイドラインを作っていますが、その中で昨今注目されているのが、ＳＢＯＭ、Software Bill of Materialsです。ＳＢＯＭは米商務省のアラン・フリードマンさんという人が中心になって立ち上げたソフトウェアの透明性向上のための成分表です。食品の成分表と同じです。ソフトウェアの成分表として、ソフトウェアの開発の履歴、今回の偽情報・誤情報でいうと、来歴管理情報に相当するものが記録されたものと思っていただきたいと思います。今、米国連邦政府は、ソフトウェアシステムのユーザー（省庁等の調達者）がベンダーにＳＢＯＭ情報の提供を求めることを義務化しようとしています。つまりＳＢＯＭはベンダーの責務だと。

一方、ベンダーにとってＳＢＯＭの提供にはコストがかかって、管理コストも高いわけです。ここで議論になるのが、ＳＢＯＭを頑張って用意して提供する価値と、コスト負担の問題で、今、米国でもけんけんがくがくの状況です。日本でもＳＢＯＭをどのように生かせるか、経産省さんや総務省さんでいろいろな実証実験が行われていますが、どこまで責任があり、どこまでコスト負担、どうしていくのかというところは大きな課題となっています。

以上のとおり、私としては、ソフトウェアのセキュリティの透明性確保のために、ＳＢＯＭをサプライチェーン全体で取り組むためには、いろいろな観点が要ると考え、その解決に取り組んでいるという状況です。これはソフトウェアだけではなく、ハードウェア、それからクラウド、今後はＡＩやロボットに関しても同じです。それぞれがどのようにできているかという透明性をいかに担保していくか、それを法制度、社会的観点、システム技術、経済の観点から、どうしていくのかというのがポイントだと思います。

これを、ソフトウェアのセキュリティの透明性ではなくて、コンテンツや情報の透明性と置き換えたのが、今回の検討会の議論と理解しています。

そこで、ソフトウェアサプライチェーンの観点のサイバーセキュリティ確保と偽情報・誤情報対策を私なりに比較して並べてみたらどのようになるかです。

まず、リスクと背景です。右側がサイバーセキュリティ確保、特にソフトウェアサプライチェーン対策における対象、社会的なリスク、アクター、裏コミュニティ、背景課題等です。

対応する偽情報・誤情報が左側です。今回の委員会で私も勉強させていただきましたが、こちらは、コンピューターやネットワークではなく、人間の認知機能に直接攻撃するという意味で、深刻な問題だと改めて思いました。また、先生方からの御指導で理解しましたが、

アテンション・エコノミーが背景課題にある。一方、アクターとか裏コミュニティの分析は必要と思いました。ちなみに、昨日の別の委員会で勉強したんですが、生成ＡＩの悪用では、既に裏ビジネスができているとのことです。

２つ目は、対策技術や対策手段です。右側はサイバーセキュリティ確保のための取組、左側は偽情報です。サイバーセキュリティ確保ではいろいろなチェック手段やソフトウェアサプライチェーンにおいてもいろいろな取組をしておりますが、１００％ではなく、過検知、誤検知があることは覚悟の上で、いろいろ取り組んでいる状況です。ＳＢＯＭは、デザイン時またはデフォルトとして透明性を求めるための取組です。それから確保主体は誰か。その確保手段はサプライチェーンにおける委託契約など。また、業界の促進策や、ガイドラインもあります。左側には私が検討会で勉強させていただいた偽情報・誤情報に関するものを記しています。

まさに今日も始まる議論だと思いますが、ガイドライン等をどうしていくのかというところも課題だと思います。

３つ目が、法的な枠組みです。右側、私どもが取り組んでいるサイバーセキュリティ確保では、サイバーセキュリティ基本法が上にあって、そこで目的や理念が明示されています。多様な主体と連携によるセキュリティの対応が必要であり、その中で、国や地方、それから重要インフラ、サイバー関連事業者の責務、それから努力義務が述べられています。この基本法に基づいてサイバーセキュリティ戦略を戦略本部が担っています。

関連法制度もありますし、国際的な取組もありますが、偽情報・誤情報対策において対応する法的な枠組みはどうあるべきなのかというところがポイントになると思います。

これが、今日からスタートする専門の先生方によるワーキンググループで議論されるものだと思いますが、サイバーセキュリティ確保の取り組みは、偽情報・誤情報の観点でも参考になることが多くあると思っています。例として、検知のための努力について御紹介します。これはＮＯＴＩＣＥと呼んでいるもので、管理が不十分なＩｏＴデバイスがあったときに、それが攻撃者によってＤＤＯＳ攻撃に悪用されてしまうことがあります。２０１６年に出たＭｉｒａｉというマルウェアの問題が一番有名で、世界中のインフラや社会システムが攻撃される事態が起こりました。

これをきっかけに、日本で使われている管理不十分なＩｏＴ機器をＮＩＣＴが中心となって見つけ出し、それをＩＳＰ、通信事業者と共有して、実際の利用者・所有者に注意喚起する。また、ＮＯＴＩＣＥセンターが、利用者が適切に対応できるようにサポートする。そ

ういう仕組みです。

これに関しましては、ＮＩＣＴ法の改正という形で制度的にサポートされてきましたが、昨年１２月の国会においてさらに改正がされ、この調査を延長すること、加えて対象を、ソフトウェアの脆弱性にも拡大することが法律として認められました。これによって今後も続くことになりますが、ポイントは、いろいろな事業者が情報共有して、協働で啓発活動等を進めるというところですので、今回の偽情報・誤情報でも十分参考になると思っています。

次は研究と実務の相互連携と継続性の観点でお話をしたいと思います。

１５ページはサイバーセキュリティの研究と実務の相互連携を表現したものです。左側には研究開発プロジェクトがいろいろあります、右側は、サイバーセキュリティ確保に関わる企業活動または社会活動のエコシステムです。

ここでのポイントは、真ん中にある脆弱性のデータベース、インシデントのデータベース、または評価技術・ツール、ベンチマーク、悪性サイトのURL、そういうものが研究プロジェクト間で共有されることによって、研究プロジェクト同士が協力し合ってデータベースを作りながら、新たな対策技術を研究できる、そういう仕組みが少しずつできてまいりました。

さらに、それらの情報を、セキュリティベンダーや、ＩＳＰ、通信事業者が行っている実務と共有し合って、実際の対策を継続できる。また、逆に実務から研究にデータベースの情報のフィードバックもあるという形で動きつつあります。

また、一般企業においてはインシデントへの対応がポイントですが、それを支援するコミュニティの取組があります。そのアドバイスを受けて、企業は、ＣＳＩＲＴ、工場のＦＳＩＲＴ、またはプロダクトのＰＳＩＲＴを構成して、インシデント対応ノウハウを蓄積して、実務に当たっています。

これを偽情報・誤情報対策について書いたものが16ページです。活動や連携がはっきりしないところはグレーや点線になっています。偽情報・誤情報に取り組む研究では、コグニティブセキュリティとＡＩの脅威対策に対する研究が多分メジャーと考えます。右側では今後は対策の実務のエコシステムが回っていくと思っています。

そのときに、研究プロジェクト間の、例えば偽情報・誤情報のデータベースであったり、それを評価する技術または普及活動、そういう活動が現状では不十分ではないかと心配です。

ＡＩに関しては、海外で事故事例のデータベースが少し作られるという動きが出てきているようです。

また、右側の実務サイドでは、今、ファクトチェックセンターが動き出しているとのことですが、実際の企業とかメディア企業において偽情報や誤情報に関するインシデントが起きてしまったときに、対応チームはどう組織され、どう動くべきなのかと。そのようなインシデント対応の仕組みに関する検討はまだまだ不十分ではないかと思っています。先ほど申し上げた法制度も今後期待されることです。

この辺り、サイバーセキュリティ確保の取り組みでも全てがうまくいっているわけではありませんが、サイバーセキュリティの関係者がみんなで苦労して、データベースや共有の仕組み作りに取り組んでいることに関しましては、偽情報・誤情報対策においても参考になるところは多いと思います。

最後、３つ目でございます。実際の対策技術を研究する立場、またはそれを実運用する立場として、大規模データ基盤やＡＩの大規模学習モデルが必要になってくるというお話です。

偽情報分析の研究や、ファクトチェックの前処理の中で使われる偽情報の検知では、高信頼のデータ基盤が非常に大事になるだろうと思います。

なぜかというと、偽情報の分析のためには、多様なステークホルダー、また、ＳＮＳからの公開情報を準リアルタイムに収集・検知・評価する仕組みが要るだろう。そのときに、コンテンツの種類にもよりますので、いろいろな契約条件の下でデータを入手し、その制約において処理をするため、処理をする土台自体が十分に高信頼であり、法的にも安全な、倫理的にも安全なものが求められることになります。

ＡＩの分析基盤も同じですが、我が国に、このような基盤があるんだろうかという心配です。

実際、分析基盤の能力限界が出た事例です。2020年の米国大統領選挙において、SocialBot（偽情報を拡散しやすいロボット）を分析する論文が発表されましたが、処理能力が足りなくて、サンプリングでしか分析できなかったとのことです。つまり、まだまだデータの量に比べて処理できる基盤が十分できていない。これは米国の研究者の例ですが、まして日本では、と心配です。

今、このような検知技術、評価技術の研究が盛んになってきています。私の大学でも取り組み始めている人間がおりますが、分析対象の規模に今の設備では負けてしまうのが現状です。

このような基盤は、研究開発だけではなくて、それを実務に展開する場合にも重要です。

また、サイバーセキュリティの研究開発にとっても重要であるため共有できるかもしれません。

今、いろいろな研究チームが盛んに動き出していますが、土台として使う基盤がまだまだ不十分であり、国の施策としてもしっかり対応していく、準備することが、日本全体にとって大事ではないかと思います。

今回、サイバーセキュリティ確保の取組と偽情報の取組を並べて比較してみました。多様な取組が必要ですが、法制度については新設のWGでしっかり取り組んでいただけることを、うれしく思いますが、同時に、いろいろな情報を収集して共有する仕組みも要るだろうと思います。その観点からは、ＮＯＴＩＣＥの取組は参考になると思います。

また、研究と実務の相互連携・継続性も重要です。この辺りはなかなか日本では評価されにくいところもあるので、しっかり国とか公的な機関がサポートし、今後は増えてくるであろう実被害への対応方法をサポートする取組も必要だと思います。

また、データ基盤も必要で、ここはぜひ国としては大きな投資をしていくべきと考えています。

以上でございます。

【宍戸座長】　後藤先生、ありがとうございました。

それでは、ここから質疑応答とさせていただきます。チャット欄で私にお知らせいただければと思いますが、事前に１６時頃から途中参加される田中先生から御質問をお預かりしておりますので、私から代読をさせていただきます。

資料を拝読し、サイバーセキュリティ領域における広い視野と多様な観点を学ばせていただきました。ありがとうございました。できれば後藤先生の発表を直接拝聴したかったのですが、授業の都合で遅れて参加することになってしまい、大変恐縮ですが、資料を拝読した時点での御質問をさせていただければ幸いです。

この一番、今ちょうど触れていただいた「データ基盤と大規模ＬＬM基盤の必要性」についてが田中先生からの御質問でございます。そこにおける「ＳＮＳからの公開情報の（準）リアルタイム収集・検知・評価」という点に関して、そこにテキストメッセージが含まれるとして、英語に加えて日本語の情報を収集・検知・評価を継続的・安定的に行うことの現状の課題や今後の課題があれば御教示いただけませんでしょうか。

というのも、誤情報が認知に及ぼす影響に関する研究の多くは、英語のＳＮＳメッセージを実験材料として、英語圏の参加者を対象に行われているという現状があります。そうしま

すと、例えば米国における誤情報が研究での「partisanship」のように、果たして日本への影響を予測する主要因子になるかどうかという要因が予測モデルに入ることもあります。

特定の国における誤情報の影響を予測するモデルに依存して日本での対策を講じてしまうと、コグニティブセキュリティに関する日本独自の脆弱性を見過ごすリスクや、逆に、日本ではそこまで発生しにくい海外の特定の脆弱性対策に過剰なコストをかけてしまうリスクにつながることが考えられます。このようなリスクに備えるためには、英語圏の研究や動向を参考にしつつも、日本語・日本文化圏での研究も必要で、そのためには日本語での情報をどのように研究や技術開発に利活用できるかが重要になってくるように思います。

このような関心から御質問させていただきました、ということでございます。

それでは、後藤先生、何かお気づきの点があれば、お願いをいたします。

【後藤構成員】　非常に大事なポイントです。逆に私からどうしたら良いかと田中先生にお伺いしたいのが本音です。

まず、田中先生おっしゃったように、日本語での研究は大事だと思っていますし、偽情報・誤情報は、まだ分かっていませんが、近くにいるＡＩの先生方は皆さんＡＩの学習自体も、日本語の文章をしっかり読み込ませられるようにしないといけないとおっしゃいます。

関連して申し上げると、日本語での分析の研究を充実させるためには、幾つかポイントがあると思います。１つは、先ほど申し上げたように、共有する努力、これに関して、例えば学会等でも共有の活動へ高い評価をするとか、国の研究ファンディングでサポートする取組があるべきと思います。

日本語のフィッシングのメール文等の分析をやっていますが、メール文中には、個人情報や、プライバシーに係るものが入っているため機微な情報として、法令に基づいて処理、クレンジングをする作業に多大な手間がかかります。その処理のためのツール作りも、試行錯誤でやっていますが、どのような前処理をするとどのような情報がつくれるか自体を１つの研究の成果として情報交換するような場も必要なのではないかと思います。そういうことによって、この研究のアクティビティーも活性化できるようになると思っています。

大規模という観点では、サイバーセキュリティのためのＯＳＩＮＴ（Open Source Intelligence）として、広く発信されている公開情報を集めて分析するために、リアルタイム処理を進めています。

それに関しましては大分ノウハウがたまってまいりましたので、多様な情報を扱うときの仕組みをどうすればいいかに関しては、セキュリティのチームと偽情報・誤情報チームが

協力し合うことが有益と思います。

ただし、新たに必要となる法的な配慮または倫理的な配慮があるはずなので、そこに関しては新たな仕組みが必要と思っています。

取りあえず私がお答えできる範囲では、以上でございます。

【宍戸座長】　ありがとうございます。

この後、森先生、それから澁谷先生から御発言の御希望がありますので、そこまでとさせていただければと思います。

まず、森先生、お願いします。

【森構成員】　後藤先生、御説明ありがとうございました。大変勉強になりました。

私は、多分サイバーって、偽情報・誤情報全般の中で一歩先を歩いている領域ではないかと思っていまして、先日のアプローチのところにも書かせていただいたんですけれども、例えばサポート詐欺というんでしょうか、ウイルスに感染しましたとかウイルスが検出されましたとか、画面にばばばっと出て、単に閉じればいいわけなんですけども、電話をかけろとか、そういうアプローチがあると思うんですが、そういうのに対して、ＩＰＡが体験サイトですか、ちょっと試しに体験してみてくださいとか、あると思いますし、あと分かりやすいところでは、ベンダーさんが標的型攻撃メールの訓練とか、そういうサービスを提供されていると思うんですけども、ああいうことは結構、偽情報・誤情報一般の対策として使えるのではないかと。ユーザーに認知能力の限界を知ってもらって、リテラシーを上げて、さらには認知能力を上げるということについて、偽情報・誤情報一般でも、そういうものに接したときにやっちゃいけない対応ってあるわけでして、それは電話をかけるとかそういうことではないかもしれませんけど、例えばすっかり信じて拡散するとか、すぐに信じて怒って興奮するとか、そういうのは偽情報とか誤情報に対する対応としては駄目なわけですけれども、そういう駄目な対応をしないで正しく対応しましょうねということを、体験サイトみたいなものとか、あるいはベンダーさんの攻撃メールの訓練みたいなこと、もちろんかなりモディファイはしないといけないと思うんですが、そういうことを通じて何か応用できないかなとはちょっと思っておりましたが、いかがでございましょうかということでございます。よろしくお願いします。

【後藤構成員】　森先生のおっしゃるとおりだと思います。今、幅広く、いろいろな観点で、基本的なマナーや基本知識を身につけるために、一般の人が経験する、体験するための取組はいろいろ行われております。ＩＰＡがやっているものも有名ですし、最近は中学とか

高校に出向いて特別講座を開き、スマホを利用する上での注意点を学んでもらう機会も増えてまいりました。このような活動は本当に草の根的に、やればやるほど価値が出るので、偽情報・誤情報でも十分やっていくべきだと思います。

もちろん、それだけで全てが解決されるわけではないので、プラットフォーマーの取組とうまく抱き合わせで相乗効果を出していくべきなんだろうと思います。

最近はアニメや漫画のキャラクターを使っての啓発ノウハウはたまってきています。私の周りでもアニメを使った学習コンテンツをつくる研究をしている人間もおります。そのノウハウは偽情報・誤情報にも十分活用できると思っています。大賛成です。

【森構成員】　ありがとうございます。

【宍戸座長】　ありがとうございます。

それでは、澁谷先生、お願いいたします。

【澁谷構成員】　澁谷です。よろしくお願いいたします。大変貴重な御発表ありがとうございました。とても勉強になりました。

最後のところでおっしゃっておられた、研究と実務の継続性の観点とか、それから分析基盤の能力の限界というところは特に共感いたしまして、やはり現在ですと、特定のケースですとか特定の言語のみを対象とした分析が主流で、もちろんそういったものの積み重ねで全体像を見ていくということもあると思うんですが、俯瞰的な研究に限りがあります。しかし、例えば能登半島地震を見てみましても、言語だけに限ってみても、閲覧数を伸ばすためだけに、いろいろな言語のユーザー、海外の人と思われる方の投稿も偽・誤情報系でもたくさん見られました。本来は広い視野で、理想的には複数のプラットフォーム間の相互作用を含めた広い視野での効果検証とか、偽・誤情報のリスクの特定とか、あるいはプラットフォームの取組の、第三者としての評価や分析ができる基盤づくりが課題と感じました。

それに関しまして、スライドの１５ページ、１６ページで、サイバーセキュリティの研究と実務というところで御紹介いただいておりますが、日本国内で努力するということはもちろんですけど、やはりサイバーセキュリティでも、海外からの影響というのもあると思うんですが、例えば１５ページのところでお示しいただいたものとかで、海外との連携とか、あるいは日本独自の考え方とか、その辺の何かノウハウとか御知見があったらぜひお伺いして、この偽・誤情報のところへどうつなげていけばいいのか、考えたいなと思いました。よろしくお願いいたします。

【後藤構成員】　ありがとうございます。海外との連携は非常に大事です。ここに表れて

いるところで言いますと、例えば脆弱性情報の最初のＣＶＥでは米国の有名なシンクタンクＭＩＴＲＥが中心となって世界から情報をためています。それを補足する形で、日本ではＪＰＣＥＲＴやＩＰＡが日本のバージョンをつくっています。

また、インシデント対応チームのコミュニティに関しましても、ＦＩＲＳＴという世界的な取組があって、それに貢献しつつ、日本ＣＳＩＲＴ協会（ＮＣＡ）が中心となって、日本の企業組織向けにＣＳＩＲＴに関する情報、つくり方、組織の仕方を共有しています。このように、海外と日本の両方の活動が必要ですし、それぞれにて海外と日本の間の連携も進めています。

この促進には、政府レベルの２国間協議等で、政府同士がしっかり握手しておいていただくことが、民間レベル、または学術レベルの連携に結びつくと思います。

ひとつ残念な現状を申し上げますと、いろいろな情報に関しましては、日本は輸入超過です。日本で情報収集して、それを海外に貢献する量に比べて、世界、特に米国からデータを買ってくる、輸入超過の状況になっているのが現状です。

そういう意味で、サイバーセキュリティにおいても、日本としても頑張らなければいけないと思います。まず政府間でいろいろ握手をしていただく。あとは民間レベルでもしっかりと実務を進めていくというところに関しましては、偽情報・誤情報に関するものも同じだと思います。

物によっては一緒にやると良いものもたくさんあると思います。インシデントのチームは、偽情報・誤情報に関するインシデントも一緒に扱ってもいいのかもしれないなという気がしております。

以上です。

【澁谷構成員】　ありがとうございます。

【宍戸座長】　ありがとうございます。

この後、まだ御質問、御発言の御希望あろうかと思いますけれども、後の議論とも関連するものもあろうかと思いますので、そちらでお願いできればと思います。

後藤構成員、御報告、また、質疑への御対応、どうもありがとうございました。

【後藤構成員】　ありがとうございました。

【宍戸座長】　それでは次に、先ほども申し上げましたけれども、「これまでの主な御意見・全体像・基本理念・ステークホルダーの役割」につきまして、資料７－２－２、７－２－３、７－２－４に基づき、事務局から御説明をいただければと思います。よろしくお願いい

たします。

【上原専門職】　事務局でございます。事務局より御説明いたします。

まず、資料７－２－２、ワードの資料を御覧ください。こちらの資料は、本検討会の第１回から第５回までの会合において構成員の皆様からお寄せいただいた御意見を、事務局において、大きく、デジタル空間における情報流通の「健全性」の考え方、デジタル空間における情報流通に関する現在の課題、そしてその課題に対処する上で健全性の考え方を踏まえて各ステークホルダーが果たすべき役割・責務の３つに分類し、取りまとめたものになります。

第１回から第３回までの会合における御意見については、昨年末の１２月２５日開催の第５回会合において資料５－２－１として既に御紹介したところでございますけれども、第５回会合での落合構成員による「デジタル空間における情報伝達の全体像のたたき台」の発表、それから前回第６回会合における石井構成員、山本龍彦構成員からの「基本的な考え方について」の御発表などを踏まえまして、「健全性」の考え方や課題に関する御意見の分類を整理し直しております。また、第４回・第５回会合で構成員の皆様からいただいた御意見、つまり、前回の資料との差分については、イエローハイライトを付しております。

これらの御意見を踏まえ、デジタル空間における情報流通と、情報流通に関する課題の全体像の可視化を試みたのが、資料７－２－３のパワーポイントの資料となります。こちら、御覧ください。

こちらの資料は、第５回会合で落合構成員に御作成・御発表いただきました「全体像のたたき台」、資料５－２－１ですね、こちらをベースに、事務局にて一つの案として用意させていただきました。

まず、表紙をめくっていただいて１ページ目、こちらは落合構成員の案と同様、情報流通の各過程、すなわち発信、伝送、受信を左から右へと配置し、情報の流れを矢印で示しております。矢印の色は伝送経路の違いを表しておりまして、放送波や紙媒体を通じて受信者に受信される情報は水色、インターネットを通じて送受信される情報は緑色、また、その中でもプラットフォーム事業者・サービスによるモデレーション、プロミネンスなどを経て受信される情報は赤色としております。また、ファクトチェック機関・ファクトチェック関連団体を、ほかの発信者とは別枠で、上のほうに配置させていただきました。こうしたファクトチェック機関は、ほかの発信者から発信された情報を、直接あるいはプラットフォームを通じて受信・収集し、ファクトチェック記事などの情報を自らのメディアで、またはプラット

フォームを通じて発信しているものと考えられることから、そのような情報の受信・発信過程については点線で表しております。

次に、２ページ目を御覧ください。２ページ目から４ページ目までは、情報そのものではなく、これも落合構成員の案に基づきまして、情報流通の裏側にあるお金などの交換財の流れ、エコシステムを表現したスライドとなります。

２ページ目は、放送や新聞といった伝統メディアを通じた情報流通に関わるエコシステムをごく簡単に示しております。落合構成員からも御発表がありましたとおり、伝統メディアのうち公共放送や新聞等のメディアについては、利用者から直接受信料・購読料を受け取り、その対価としてコンテンツを直接届けている関係である一方、新聞等は同時に、また、民間放送もそうですけれども、広告主から広告料を受け取って、その対価として広告枠を提供し、広告主を通じて広告つきのコンテンツを利用者に届けている。利用者は、特に民間放送については受信料を支払わずに視聴可能ですけれども、その代わりに広告を視聴しているという関係があるという指摘がございます。

次に、３ページ目を御覧ください。こちらは、自社のサービス上に広告を配信するプラットフォーム事業者・サービスを通じた情報流通に関わるエコシステムを示しております。

この場合の広告主は、プラットフォーム事業者に広告料を支払い、対価としてプラットフォームサービス上の広告枠を提供してもらっているという関係になります。一方で、プラットフォーム事業者・サービスは、伝統メディアであったり、その他の制作主体、必ずしもここに挙げたものだけではないと思われますが、多様な発信主体が発信するコンテンツをプラットフォーム上に掲載し、広告つきで利用者に届けている。他方で、利用者が対価としてプラットフォーム事業者・サービスに何を支払っているのかであったり、また、プラットフォーム事業者・サービスがコンテンツの対価として発信主体に何をどのような基準で支払っているのか、さらに、そうした対価の流れがプラットフォーム事業者・サービスから利用者に向けて伸びるコンテンツの伝送のされ方にどのように影響しているのかといった部分は、まだ不透明さが残っているという御指摘が構成員の皆様からございましたので、「はてな」を付しているところでございます。

次に、４ページ目を御覧ください。こちらは、先ほどと異なり、他社のサービス、つまり、ウェブサイト、アプリなどの上に広告を配信するプラットフォームを通じた情報流通に関わるエコシステムを表現したものになります。

この場合も広告主はプラットフォーム事業者・サービスに広告料を支払いますが、それに

対して、プラットフォーム事業者サービスが提供するのは、他社のサービス上の広告枠ということになります。その広告枠は、ここではネットメディア・個人などのその他の制作主体というところをハイライトしておりますが、それに限らず、様々なメディア・媒体社と呼ばれるものがプラットフォームを通じて販売しているということになります。媒体社は、多数のインターネット利用者に自社メディアを訪問してもらって広告効果を上げられるように、いろいろコンテンツを広告つきで発信しているということになります。他方で、３ページ目と同様ですけれども、では、インターネット利用者が対価として何を支払っているのか、また、プラットフォーム事業者・サービスが媒体社である発信主体に対して何を支払っているのか。基本的には広告収入を分配していることになろうと思われますが、どういう基準で分配しているのかといったところは不透明であるという御指摘がございますので、「はてな」をつけているところでございます。

最後に、５ページ目を御覧ください。こちらは、「デジタル空間における情報流通の健全性を巡る課題」の例として構成員の皆様にお寄せいただいたものを挙げております。こちらに記載の課題例は、先ほど御覧いただいた資料７－２－２のワード資料内の整理に従っております。いずれの課題も、厳密にはデジタル空間におけるほぼ全てのステークホルダーが連携・協力しながら対処していくべきものであるという御意見もございますので、配置がなかなか難しい面もございますが、あくまで主として、この段階のこのステークホルダーに関係するとの御指摘があるという観点から、関係する情報流通の段階あるいはステークホルダーにかぶさるような形で配置をしているところです。

まずは、そもそもこうした整理の目的として、前回第６回会合で宍戸座長より御指示いただいたように、「健全性確保に向けた基本理念や各ステークホルダーに期待される役割・責務の在り方」の検討というものがございますので、これを赤枠で一番上に置かせていただきました。

その下の「デジタル空間の情報流通に関するガバナンスの在り方」、「ステークホルダー同士の連携・協力の在り方」といったところは、全てのステークホルダーに関わるものとして、横長に配置しております。「国際連携・協力の在り方」も、これは一番左の外国政府や国際機関とも連携・協力しながら、やはり全てのステークホルダーが検討・対処していくものとして、横長に配置しております。

一番下のほう、「緊急事態（災害、サイバー攻撃など）への対応の在り方」や「技術・研究開発の在り方」も、これらは国・自治体や重要インフラ事業者をはじめとする企業あるい

は研究機関が中心的に関係するところではありますが、やはり多様なステークホルダーが連携・協力しながら対応していくものという御意見がございますので、横長に配置しております。

なお、「技術・研究開発の在り方」の一部分ということになろうと思いますが、プラットフォーム事業者などの事業者から研究機関等に対するデータ提供等の形で連携ができるといいといった御意見があったところですので、これを「研究機関等との連携・協力の在り方」という形で表現しております。

左側、「生成ＡＩ・ディープフェイク技術の進展に伴うリスクへの対応の在り方」については、まずは生成ＡＩなどの技術を用いて生成された情報が発信されることによる問題があるという観点からの御意見がございましたので、発信段階に配置させていただいておりますが、他方で、伝送段階でも、検知技術など対処の在り方が問題になり得るという御指摘もございましたので、伝送段階にも同じ文言を配置しております。これも広い範囲のステークホルダーが関係する課題と言うことができようと存じます。

次に、主として発信段階、とりわけ伝統メディアの役割に関連して複数の構成員から御指摘いただいたものとして、左側上部に、「発信情報の信頼性を得るためのコスト増への対応の在り方」、例えば発信主体の真正性や信頼性を確保・向上するためにどのような方策が打てるのかといった課題でありましたり、「発信力強化のためのガバナンスの在り方」といった課題を記載させていただいております。

また、上のほう、「持続可能なファクトチェック推進のための仕組みの在り方」、資金面であったり、効果的な訂正情報の届け方といった観点も含め、これも主として発信段階に関係する課題でありますけれども、伝送段階でも問題になり得るものとして指摘されておりますので、この位置に配置させていただいております。

主として伝送段階に関係する課題としては、根本にある構造的な課題として複数の構成員の皆様から挙げていただいた、「アテンション・エコノミーが引き起こす課題（フィルターバブル、エコーチェンバーを含む）への対応の在り方」というものを中心に置かせていただいております。

そしてこの周辺に、これらもアテンション・エコノミーが引き起こす課題の一部分と言えるかもしれませんけれども、「偽・誤情報の拡散への対応の在り方」、「広告を巡る課題への対応の在り方」、さらにこれらをもう少し具体化したものとして、「事業者の取組の透明性・アカウンタビリティ確保の在り方」といったところも複数の構成員の皆様から御指摘いた

だいたところでございます。

ここでの「事業者の取組」としては、例えば利用者へのコンテンツ伝送の過程に主として関連する「コンテンツモデレーションの方針・体制・実施状況、プロミネンスなど」の透明化という話と、発信主体や広告主との間に関係する「レコメンド、データ取扱い、広告収入の発信者への分配など」の透明化という話、どちらも構成員の皆様から御指摘いただいたところかと存じます。

最後に、右側、主として受信段階に関わる課題としては、やはり「認知的・社会的バイアスを前提としたリテラシー向上策の在り方」というところが多く御意見いただいたところでした。これは利用者そのものだけではなく、一番下の研究機関・教育機関・普及啓発機関といったところにも関わるところであるとの御意見を踏まえ、縦長に配置させていただいております。

そして、一部重複するところでありますけれども、下のほう、「発信・拡散主体となり得る受信者側のガバナンス・リテラシー向上策の在り方」については、単なる情報の受け手ではなく、受信後に発信者に回って情報を拡大再生産していく主体としての利用者について、例えば偽・誤情報などを拡大再生産してしまうような事態に対してどのように対応すべきか、そういった意味でのガバナンスないしリテラシー向上策が必要なのではないかという御指摘を踏まえ、記載したものになります。正確に表現するならば、左側の発信段階にもつながる課題ということになろうと思いますが、見やすさの観点から、ここに配置させていただきました。

こうした課題があるとの御意見をいただいた一方で、これらに対処する上で考慮すべき基本理念としては、構成員の皆様の御意見を踏まえると、このようなものが挙げられるのではないかという例を記載したのが、資料７－２－４のパワーポイント資料になります。

こちらの表紙をめくって、１ページ目を御覧ください。これらは構成員の皆様からのこれまでの御意見、あるいは事務局において情報収集を行った、デジタル空間の情報流通に関連する国内外の各種法政策領域における「原則」であるとか「基本理念」などの議論状況、これらについては２ページ目以降に参考資料として添付させていただいておりますので、併せて御参照ください。これらを踏まえまして、事務局にて例として提示させていただいたものでして、健全性の在り方に関する考え方はこれら９つに限られるものではないと考えておりますが、いずれにしましても、過不足等の御指摘ございましたら、ぜひ頂戴できますと幸いです。

一つ一つ御説明しますと、まずは、やはり「表現の自由・知る権利」が重要ではないかという御意見がありました。発信者の表現の自由、伝送者の表現の自由、それぞれを考慮すべきという御意見であったり、その裏側としての受信者の知る権利（知る自由）というものが重要であるという御意見もございました。

それから、２の「多様性・包摂性」を重視すべきという議論もございます。これも知る権利と密接に関連するところですけれども、前回第６回会合での山本龍彦構成員からの御発表では、「情報的健康」の考え方を通じて、多様な情報へのアクセスが保障され、知る権利の実質的な保障がなされることが重要であるとのお話があったところでございます。

それから、３の「法の支配・民主主義」、例えばルールにのっとった民主的なガバナンスがデジタル空間において確立されるべきではないかという御意見。

それから、４の「公平性・公正性」については、情報の伝送過程で不当な偏りが発生しないようにすべきである、あるいは、ＡＩガバナンスに関連して、バイアスが発生しないようにすべきといった議論もここに含まれるかと存じます。

５の「真正性・信頼性」については、信頼性の高いコンテンツの流通にインセンティブを付与すべきという構造的な議論であったり、受信者の判断能力の向上支援、例えばリテラシー向上あるいは関連する概念としてのデジタル・シティズンシップ教育などもここに含まれるものと思われます。

６の「安心・安全」については、例えば児童・青少年の保護や、より社会的な文脈でのコスト・リスクの増加の抑制、さらに、災害発生等の社会的混乱の抑止といった観点も御提示いただいているところでございます。あるいは、情報セキュリティの保護といった観点、サイバーセキュリティの確保といった観点も「安全」には含まれるものと思われます。

７の「オープン・透明性・アカウンタビリティ」については、発信主体・受信主体それぞれから見た事業者による取組の透明性・アカウンタビリティ、あるいは、事業者だけでなく、行政機関の行為についての透明性・アカウンタビリティ確保も重要だというお話がございました。

８の「プライバシー保護」については、前回第６回会合での石井構成員の御発表で、個人の認知領域の保護というものが広い意味でここに含まれるのではないかという御指摘がございました。

それから、９の「グローバル・国際性」についても、やはり国際的に調和のとれたルールづくりや国際連携の促進が重要であるという御意見があったところでございます。

事務局からは以上となります。

【宍戸座長】　ありがとうございました。

それでは、御質問・御意見のある方は、チャット欄で私にお知らせをいただければと思います。特に、これまで構成員の皆様から御発言・御議論いただいた内容が、ただいま御説明いただきました事務局作成資料に反映されているかの御確認でありますとか、資料に反映すべき新たな課題・論点などがあれば、ぜひこの機会に御議論いただければと思っております。どこからでも御自由に御発言の希望をお知らせいただければと思いますが、いかがでございましょうか。

まず、曽我部先生、お願いいたします。

【曽我部座長代理】　ありがとうございます。すみません、私、これまで議論に参加させていただいておりませんので、ちょっと的外れかもしれませんが、途中で退席させていただきます関係で、先にお願いできればと思います。

２点あるんですけれども、１つは、資料７－２－３の全体像（案）というところの様々な図なんですが、ここでの広告の扱いというところが若干気になりまして、申し上げたいと思います。図の中に、お金の流れの話があり、広告主というのが、これはステークホルダーという位置づけなのか分かりませんが、出てくるということなんですが、広告も、プラットフォームというのがあったり、あるいは広告代理店というものがあったり、ステークホルダーとして取り込むべき主体があるのではないかと思われ、お金の流れが重要だということの反映で、こういった広告にまつわるアクターも、今回の全体像の議論の中で何らか取り込むべきではないかなと思いましたので、その旨、一つ申し上げたいと思います。「広告を巡る課題への対応の在り方」というのはあるので、その中に入るのか分かりませんが、図の中にステークホルダーとしてそういったものを入れていただくのがいいのではないかというのが１点でございます。

２点目は、もう一つの資料の基本理念なんですが、全体として表現の自由というのが強調されているわけですが、他方で、やっぱり責任ある発信ということも言わないと、表現の自由を一方的に強調するということになると、やや趣旨としてずれてくるのではないかなという感じがいたしますので、そこを入れていただく必要がやはりあるのだろうと。５のところで、受信者のリテラシー、デジタル・シティズンシップというのがあるわけですけれども、発信主体のリテラシー、シティズンシップというのも言っていく必要があるのではないかと思います。

それから、２番目の「多様性・包摂性」は、結局表現の自由を保障すれば実現する話なので、２のところの意味というのは私はよく分からなかったところで、ついでに気になったということで申し上げますが、主には広告の話と、責任ある発信というところも入れていただくのがいいのかなという点でございます。

以上です。

【宍戸座長】　ありがとうございました。今日はいろいろなところから御議論いただくということで、事務局が一つ一つ回答するということではないと思いますけれども、今、曽我部先生がおっしゃったこととの関係で、私が申し上げますと、一つは広告について、そういう形でより解像度を上げて議論すべきである、様々なプレーヤーがいるということとの関係について、さすが曽我部先生という、蒙を啓かれる思いで御意見を伺っておりましたので、今後、ヒアリング等も含めて、あるいは事務局の調査も含めて、深掘りをしていきたいと思います。

また、基本理念のときの表現の自由というときに、まさに発信者の責任の問題でございますね。これは、本検討会がまずは情報流通ということで広く捉えるという観点から見たときに、情報発信者固有の問題をどういうふうに分析していくかという話もちょっと悩んできたところでございますけれども、御指摘を踏まえて、まさに伝統的なメディアは特に自ら責任ある行動ということでやってこられたわけでございますので、今後のデジタル空間の中で、伝統メディアあるいはそれ以外の広い人々の発信の責任の問題を、どういうふうに考えていくか。先ほどおっしゃいましたように、１であるとか４であるとか５、あるいは「安心・安全」とか、７のアカウンタビリティのところにも関わるかと思いますので、少し整理をさせていただきたいと思います。ありがとうございます。

それでは続きまして、この調子で私がしゃべっていると時間がなくなりますので、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２点ほどなんですけれども、まず１つは、情報流通の全体像に関しまして、前回、以前言及した広告についても詳しく取り上げていただいて、ありがとうございます。まさに曽我部先生おっしゃっていただいた点含めて、重要な点を詰めていけるとよいのかなと思いました。

そうしたときに、やはりこういった重要な整理ですと、あれもこれもと申し上げたくなることになってくるんですけれども、大きな一固まりだけで申し上げますと、伝統メディアと言ったときに、恐らくほかにも、例えば書籍であるとか出版物といったようなものがあるん

だろうなと思います。そうしたときに、例えばファクトをチェックしたり、信頼できる情報を得たりするときに、もちろん放送や新聞といったようなものは見てほしいのですけど、やはり大学教員としては、本を読んでほしいなと思うわけでございます。

例えばそれが電子書籍であれ、あるいはアナログの活字であれ、やはり様々なファクトチェックで頼られる出版物といったようなものをどのように考えていくのかといったようなこと、そして、それと深く関わる情報流通の主体として、いわゆる図書館と呼ばれる主体がございます。そのことというのは、もちろん伝統的には出版物をある種伝達・流通させるメディアとしての役割を果たしてきたわけでもありますけれども、他方で、やはり現代においてはデジタルアーカイブという言葉に象徴されるような、そういった図書館やその他のアーカイブ機関自身が、信頼できる知識の蓄積というものをデジタル空間に供給する上で、非常に重要な役割を果たしているわけでございます。

例えば国立国会図書館が公表しているデジタルアーカイブといったようなもの、これは具体の例を挙げると、ウィキペディア、あれは典拠主義でございますけれども、ああいった中で、じゃあ、典拠、アクセシブルなものはどこにあるのかといったとき、それはしばしばああいったデジタルアーカイブが参照されることも多いわけでございます。それは恐らくこれからのファクトチェックにおいても同様かなと思います。

そうしたときに、私たち、しばしばストックの情報とフローの情報という分け方をする。ここでは主として情報流通といったときに、フローの情報を取り上げていただいていると思うのですけれども、ストックの情報というものを果たしてどう考えていくのか。そのストックというのは、デジタルに存在するストックもそうであるし、あるいは、それ自体がデジタルで流通するわけではないのだが、しかし、そのデジタルに流通する情報の信頼性を担保するために、アナログに存在している情報というものをどのように考えるかといった点。

そういう点を含めまして、特に、いわゆる出版物ですとかデジタルアーカイブに関しましては、今、内閣府でもずっと僕も議論に参加させていただいているところですけれども、ちょうど１２年前に総務省の情報流通振興課様が主催した知のデジタルアーカイブに関する研究会が重要な提言を出されていまして、これ、我々、しばしば今でも参照することがあるのでございますけれども、まさにああいった蓄積というものも参照しながら、そういった論点を深めていくことも考え得るのかなと考えましたのが、まず大きな一固まりでございます。

それからもう一つは、基本理念というところに関してでございます。こちら、非常に重要

な理念をまとめていただいている中で、個人的に強いて特に強調するという点を挙げるとしたら、まず一つは、まさにこの基本理念というところで、マルチステークホルダーといったような概念をやはり大きく重視する必要性というのは高いのかなと思います。

そのことというのは、やはり健全な情報流通、情報流通の健全性というものを誰か、ある一つの立場というものが断定的に決めるものではない。そのコンセプト自体をまさに継続的にマルチステークホルダーで考え続けていくこと自体が、このプロセスの中で極めて重要な役割を果たすのだろうというのが１点目。

そしてもう一つは、やはりこれ、包摂性、インクルージョンの中に含まれるのかと思うのですけれども、脆弱な個人、それは青少年であったり、あるいは障害者・高齢者といったような方々、そういった方々がいかにこの健全な情報流通に参加していくのかという観点は、特に強調してもよいのかなと思いました。

差し当たり、私からは以上でございます。

【宍戸座長】　ありがとうございます。いずれも、今、念頭に置かれている外側、デジタル空間の外側にある全ての情報をむしろデジタルにするというやり方もあるでしょう。ここでは、情報流通のプロセスに普通に、言わばネットを使える人、参画できる主体を考えていますけど、そこに参画しにくい主体の問題も考えていかなければいけないということで、非常に問題の視野を広げていただいたかと思います。ありがとうございます。

それで、本日、残り３０分ほど御議論いただきたいと思っておりますが、現時点で９人の方から手が挙がっておりますので、大体１人３分ぐらいをめどに、意識しながら御発言いただけると大変助かります。

それでは、水谷構成員、お願いいたします。

【水谷構成員】　よろしくお願いします。私からは、全体像の１の部分、もっといえば全部に関わるところでもあると思うんですけども、さきほど広告主の解像度の話がありましたが、プラットフォーム事業者・サービスの解像度の部分についても、少し検討を入れなければいけないところがあるんじゃないかなと思いました。

これはもしかすると以前にも言ったかもしれませんが、アプリケーションストアは、同じプラットフォーム事業者の中でもすごく強力な地位にあるというようなことがアメリカとかでも議論になっていたりします。特にアメリカのトランプさんがアカウント凍結されたときに、支持者の人たちが逃げ込んだ先のＰａｒｌｅｒというSNSが、アプリケーションストアからポリシー違反で排除されたというような案件がありまして、もちろんアプリケー

ションストア側も悪意でやっているわけではない、アプリケーションのセキュリティ面を考慮して行っていると思うんですけれども、ゲートキーパーのさらにゲートキーパーのような存在になっているところというのは、少しプラットフォーム事業者の中でも分けて考えていく必要があるのではないかなと思いました。

私からは以上でございます。

【宍戸座長】　ありがとうございます。

それでは、落合構成員、お願いします。

落合先生、難しいようであれば、また後で御指名をさせていただければと思います。

江間先生、お願いできますでしょうか。

【江間構成員】　江間でございます。短く１点だけ、コメントに近いかもしれないんですが、基本理念の項目のところなんですけれども、６項目目に「安心・安全」とあります。いろいろ参照されているのが国内のものもあれば海外のものもありというところなんですが、もしこれを国際的な展開とか連携とかしていく場合に、国内では安心・安全というんですけども、なかなかこれ、日本的な書き方で、海外発信するものだと、結構安全とセキュリティという言葉を使っていて、しかもそれは別項目になっていることが多いのではないかなと思っています。

日本でも、ＡＩに関しては海外と足並みをそろえてのセーフティ・インスティテュートをつくるというような考え方はございます。けれども、セーフティというのとセキュリティというのは考え方も難しいなと思ってます。今日の冒頭にサイバーセキュリティのお話がございましたけれども、ある意味、セーフティというのは、事故や事件という、何かリスクがあること一般をセーフティのようなイメージで、セキュリティというのは、ある種、明確な他者からの攻撃があることというか、そういうようなことに使うことが多いのではないかなと思っています。そういう整理をしたときに、対策の取り方、それからどういうアクターが関わってくるのかということが、若干セーフティとセキュリティでも重なるところはあると思うんですが、変わるところもあると思います。ですので、言葉遣いという非常にささいなことではあるんですけれども、本当にこれでいいのかということはちょっと御議論いただいてもいいのかなと思ったというコメントでございます。

【宍戸座長】　ありがとうございます。伝統的にインターネットでは安全・安心と言ってきたんですよね。ただ、今御指摘いただいたように、より広く、ＡＩも普及してきて、サイバー空間とフィジカル空間が融合してくる中で、デジタル空間の安全と安心は、そもそも何

についての安全とか安心と我々が言っているのか、もう一度きっちり整理しなければいけないということを、御指摘を踏まえて、改めて考えさせられました。ありがとうございます。

それでは、落合構成員、お願いできますでしょうか。

【落合構成員】　先ほどは失礼いたしました。私のほうから３つほどございます。１つが、コメントで書かせていただきましたが、後藤先生の発表をお伺いしておりまして、情報連携をどういうふうにこの偽情報対策の関係で行っていくのかを考察していくことは、非常に重要ではないかと思いました。どういう対策をしていくかにもよるとは思いますが、情報連携の枠組み自体を整備する可能性を念頭に置いておいたほうがいいかと思います。

また、セキュリティの関係で、後藤先生に触発されたところもございますが、江間先生もおっしゃられていましたが、やはり今回の対策の中では、一つ、サイバー攻撃という部分も重要な論点になってくるのかなと思います。独立して１つの項目になっていてもいいのではないかという論点だと思いました。

２点目としましては、先ほど曽我部先生や水谷先生からコメントいただきました、広告であったりですとかプラットフォームに関する分析の部分です。私の前回の発表でもあまりそこに突っ込み切れなかったところがございまして、それで、その際にも、アドフラウドですとかディープフェイク、または政治的言論、サイバー攻撃などもそうですけれど、それぞれの場面で各アクターがどう動いており、それがそれぞれどう影響し合っているのかは、この全体像だけではなく、さらに場面ごとに深掘っていくことによって、誰にどういう対策を求めていくこよが合理的なのかが見えてくるかと思います。この点については、全体像とは別にということなのかなとも思っておりますが、さらに分析をすることは必須であろうと思っております。

最後、第３点ですが、こちらについても、今、「表現の自由・知る権利」が１番に挙がってございます。一方で、この検討については、やはり民主主義自体に影響を及ぼすような偽情報というのが、各選挙などの関係での、特に欧米で見えてきている問題があるのではないかという部分に対する対策であったりですとか、昨今の地震における生命・身体の保護にも直結するような、重大な権利侵害につながるおそれがあるような事態の招来も考えられる中で議論をしていくということでもあります。そのために、恐らく表現の自由ということで特に尊重をしてきていて、そこについては触れないような形で整理していた部分について、修正をしていくという部分もあろうかと思います。いずれについても非常に重要な、表現の自由と、それぞれ重要な権利、利益であり、民主主義という制度であろうかと思いますが、

これらを対比しながら議論することが必要です。一方的に表現の自由を侵害するというようなものであってはならないことは間違いがない部分ではございますが、一方で、そういった対立する権利、利益を保護していく部分もあろうかと思います。そこの並べ方といいますか、整理の仕方は、表現の自由の保護のほうに偏り過ぎないような形で少し調整していただければと思いました。

私のほうでは以上でございます。

【宍戸座長】　ありがとうございます。項目で１、２、３と書いてあるのは、別に圧倒的な優先順位があって、表現の自由と残りが全部対立しているというものではなくて、もう少し多次元的な利益衡量といいますか、あるいは、そもそも表現の自由を実効化することを現代社会において考えたときに、こういった項目がむしろ必要ではないかということで、ここについては必ずしも表現の自由対何か、しかも表現の自由のほうが圧倒的に上ということで議論してきたつもりでもないですけど、改めて御注意いただいたと思います。

そもそも表現の自由の捉え方自体が、このデジタル社会においてどうなっていくのかということが一つ課題かなと思いますし、そういう観点からも御報告いただいていると思います。ありがとうございます。

それでは次に、クロサカ構成員、お願いいたします。

【クロサカ構成員】　クロサカです。私からも３点ほどコメントをさせていただきます。

先ほど曽我部先生から広告についての御指摘がありました。私も非常に重要な御指摘だと思っております。その上でぜひ御留意いただきたいのは、伝統メディアの広告の世界とデジタルメディアの広告の世界が、ほぼ全く別物と言えるほど大きく異なるということです。同じ広告という言葉でくくられていること自体が、実は産業論的にはかなり違和感があるぐらい、別物だと考えていただいていいと思っています。

まず、プレーヤーが違いますし、サプライチェーンも当然違う。プロセスごとの責任分界の領域も違えば、デジタル広告は、プロセス間のエアポケット、つまり責任が消えてしまう領域が多い。逆に、伝統メディアは、広告代理店やパブリッシャーと呼ばれるメディア側の配慮も含めて、かなり手厚く対応しており、大きく異なるものでもあります。

また、広告主の立場も全然違うということが実はありまして、この辺り、専門家に話を聞いて、より解像度を上げていく、議論の詳細な理解を深めていくということがここではかなり重要になると思いましたので、御一考いただければというのが１つ目です。

あと、基本理念の項目について、いずれも異存はございません。一方で、整理はもう少し

してもいいのかなと。今、少し大まかにくくられているところが、もう少し分解されてもいいものもあるかと思います。例えば真正性と信頼性を１つのものとしていいのか。あるいは、透明性とアカウンタビリティは１つでいいのか。グローバルと国際は１つでいいのか。これは一度、もう少しばらして議論をした上で、再整理・再集約するということが検討のプロセスとしてあっていいかなと思いました。御一考いただけるとありがたいと思っています。

あと追加すべきこととして、先ほどの落合構成員や後藤先生のご指摘とも重複するのですが、サイバー攻撃、特にフィジカル側に影響がしみ出してくる、直接的に出てくるものについては、特出ししてもいいのかもしれないなと思っています。

これは、２０１３年・１４年のクリミアにおいて、既にツイッター上で、クリミアに対して攻撃を仕掛けたかった勢力が、言論操作的にこれをうまくやってしまった、つまり、様々な手段を使って、言論をかなりつくり上げてしまった。それによってクリミアの市民に影響を与えたということもあります。あと、ケンブリッジ・アナリティカというのは、まさしく説明無用かと思います。

このように考えていきますと、サイバーの中で閉じているだけではなく、フィジカルなところにしみ出していくことの影響の大きさということが、災害対応もそうですけれども、非常に大きな問題になっているかと思いますので、ここは少し特出しして議論を深めて、整理がまたできるようであれば、全体に混ぜていくということでもいいのかなと思いますので、ここも御一考いただければと思います。

私からは以上です。

【宍戸座長】　ありがとうございます。

この後、６人の構成員から御発言をいただきたいと思います。ずっとこれまでと同じように、大体３分をめどに御発言いただければと思います。

森構成員、お願いします。

【森構成員】　ありがとうございます。時間厳守で頑張ります。３点申し上げます。

１点目は、曽我部先生に賛成です。クロサカさんもおっしゃっていましたけど、まず、ステークホルダーとして広告というものを、広告事業者ですね、広告主のみならず、広告事業者を７－２－３の資料のほうで正面から把握していただいたほうがいいかなと思います。プラットフォーム事業者ももちろん広告事業者であるわけなんですけれども、プラットフォーム事業者以外のプレーヤーもいますし、その人たちが広告主と媒体をつないでいるというところがありますので、これを入れていただくと。

それから、私は、責任ある発信ということもどこかに、抽象的でいいと思うんですけども、書いていただくと、今後の議論に資するところがあると思うんですよね。やっぱり偽情報・誤情報の場合、悪意のある発信主体というのも結構いるわけでして、それとどう向き合っていくかという問題もある。先ほど落合先生、クロサカさんからありましたけれども、重大な結果を引き起こしているわけですよね。ですので、そこは抽象的にでもお書きいただいたほうがいいのかなと思いました。

２点目です。先ほどの広告事業者を把握すべきであるということとも関係しますけれども、やはり７－２－３の５ページ目のスライドの、課題のどこかに、ユーザーデータの保護ということ、プライバシーということを入れていただいたほうがいいんじゃないかなと思います。というのは、真ん中のところに「アテンションエコノミーが引き起こす課題（フィルターバブル、エコーチェンバーを含む）への対応の在り方」というのがありますけども、御案内のとおりですが、フィルターバブルとかエコーチェンバーというのは、これはユーザーの特徴を把握するデータベースの存在が前提になっていて、言ってみればそれの濫用であるということです。それから、アテンションエコノミーそのものもそうですよね。ユーザーの特徴を把握した上でコンテンツを見せるということなわけですので。

それから、その右側、偽・誤情報、これは拡散ですね、失礼しました。どこかに偽・誤情報発信の問題というのがあると思うんですけども、これもやはり受信者に対して選択的に偽・誤情報をつけていくということが、先ほどのケンブリッジ・アナリティカなんかでは見られたわけですし、今でもそういう広告手法というのがあるわけですので、やはりユーザーデータということをこの課題の表のどこかに入れていただくべきではないかと思います。

３点目ですが、同じことです、資料７－２－４の論点の一覧表ですけれども、こちらには８番、「プライバシー保護」と書いていただいているんですが、個人の認知領域の保護ということで石井先生からお話がありましたが、これはプライバシーの問題だということですね。その下ですが、「個人情報の適正な取扱いなど」とありますけれども、「など」があるのでいいですが、今申し上げたデータベース、ＤＭＢのデータベースは、ここで使われるデータベースは個人情報でないことがしばしばです。ですので、やはりそれはここに、個人情報でないデータもあるということをお書きいただいていいんじゃないかと思いますし、それはプラ研では通信関連プライバシーと呼ばれるものであったということです。

もともと電気通信事業法は、個人情報ではない通信の秘密を保護してきましたけれども、それと同じような形で、外部送信によって獲得されるデータベースの扱われ方、情報の獲得

のされ方も含めて、それを通信関連プライバシーとして保護してきましたので、個人情報でない、そういったものも保護していくということをはっきりとこの８番目にお書きいただくのがいいんじゃないかと思います。

以上です。

【宍戸座長】　ありがとうございます。

脇浜構成員、お願いします。

【脇浜構成員】　ありがとうございます。この会は情報流通の健全性がテーマですので、もしかしたらスコープから外れているかもしれないんですが、１点気になりましたのは、全体像の中で、発信・伝送・受信という３つのフェーズでお書きいただいているんですけれども、発信の手前の情報コンテンツの部分は気にしなくてもいいのかなというところが気になりました。

偽・誤情報に対抗するには、そもそもそれを上回る真実性・信頼性、それから見てもらうことができる情報が流通していないとなかなか対抗できないのかなと思いまして、そうした情報コンテンツをつくるためには、テーマを見つけ出して、リサーチして、取材して、編集して、表現して、しかも人に面白いといって見てもらえる形につくり上げるということが必要になってきまして、この辺り、先ほどからワードとして出て（音声途切れ）伝統メディアに期待されているのかもしれないんですが、伝統メディアに勤めていたことのある者からしますと、なかなか丸投げされてもつらいなというところがあって、アメリカでニュース砂漠が広がっていて、なかなか地域に記者ですとかつくり手が減っているという状況も言われておりますので、日本においても、やはり情報をつくり出す人間、健全な情報をつくり出す人間が足りていないし、その教育の機関というのもないんじゃないかなと思っておりますので、流通だけということであればいいのかもしれませんが、そうした流通以前の、制作の部分にも少し、何か気を向けてもいいのではないかなと思いました。

以上です。

【宍戸座長】　ありがとうございます。私自身の理解では、情報流通と言う場合には、伝送の真ん中の部分だけじゃなく、発信・受信を含む。そこで言う発信とは多分、受信との対比で発信と言っているだけであります。おっしゃいましたような取材であるとか編集であるとか編成を含む制作全体を、私は当然含むものと思っておりますので、引き続き御指摘・御意見いただければと思っております。ありがとうございます。

【脇浜構成員】　ありがとうございます。

【宍戸座長】　それでは次に、山本健人構成員、お願いします。

【山本（健）構成員】　山本健人です。私は本日からの参加ですので、的外れでしたら申し訳ないのですが、２点ほどコメントさせていただければと思います。

１点目は、情報流通の健全性に関する基本理念に関してです。現在、９つの項目が基本理念として挙がっています。また、先ほどのクロサカ先生のお話によると、これらがさらに分解される可能性があるということですが、この基本理念の全体像を対外的に見せるときには、多くの項目を横並びで並べておくスタイルでは、逆に全体像が見えづらくなるという問題が起こるのではないかという懸念を持っています。場合によっては、各基本理念の相互関係の整理や、階層制を設けるなどの工夫をして、全体像がきれいに見えるような形で整理するという方向性も必要なのではないかなと感じています。デジタル立憲主義を勉強した経験から、基本理念の位置づけや見え方がとくに気になったということでもあります。

２点目は、「グローバル・国際性」の項目に関してです。この項目では、やはり他国との連携が念頭にあるような印象を受けましたが、現在の情報流通環境を踏まえると、グルーバル性を有しているプラットフォームとの関係性というもかなり重要になってくるのではないかと思いました。実際に情報空間の健全性を実現するという段階を考えると、プラットフォームとどのような関係を築くべきか、という点を考えざるを得ないように思いますので、この点を強調しておくことも重要なのかなと思いました。

手短ですが、以上２点です。

【宍戸座長】　ありがとうございます。今の段階は、要素を抽出して、その関係をこれから議論する段階ですので、最後、どうやって整理していくかという点では、まさに山本健人先生のような理論家のお力をいただければと思っております。

国際と言ったときに、国と国の関係だけじゃなくて、国とプラットフォームあるいは国々とプラットフォームの関係は非常に重要な視点かと思います。ありがとうございました。

それでは続きまして、奥村構成員、お願いいたします。

【奥村構成員】　お願いします。ありがとうございます。ファクトチェック機関の位置づけとファクトチェックのことについて若干の違和感がありますので、そのことについて皆さんと共有しておきたいと思います。

さはさりとて、と申し上げたら、どうすればいいのかということについて、実は妙案がございませんので、ぜひ皆さんのアイデアを拝借して、よりよいエコシステムができるような方向に行けたらいいなと思って申し上げます。

１つはまず、ファクトチェック機関というようなものですけれども、ファクトチェックというのは、できるだけたくさんの人が同じようなスキルを共有できるような方向に社会がなっていくほうがいいわけで、ファクトチェック機関にファクトチェックを任せっきりになっているという社会ではやっぱりいけないということになりますと、一般の人たちにどうやって広めていくかということ、それから例えばＯＳＩＮＴや何かの分野で言いますと、実は一般の人たちのいろいろな知見をもらってファクトチェックをしなければいけないような場面が増えてきているとなると、集合知をどうやって活用するかというようなことも出てきています。

何かそれをリテラシーとか教育とかというふうにまとめてしまうとすごく陳腐になってしまうので、ただ、一般の人たちにそれをどうやって裾野を広げていくかということは、一つ大きな課題です。

あと３点申し上げます。

もう一つは、もっとファクトチェックってリアクティブなもので、例えば伝統メディアのメッセージや何かも、もしかするとファクトチェックをする対象にならなければいけないかもしれないということです。非常にまれですし、それからカニバリズムだといって批判する方もいるんですけれども、やっぱりその可能性は排除しちゃいけないとなると、もっとファクトチェックはリアクティブなところにあるものかなという気もしているということです。

それから、ファクトチェック機関が、これ、独立していますけれども、独立したファクトチェック機関は、世界的に資金難で、相当困難に直面しています。最近ではＧｏｏｇｌｅとＭＥＴＡの資金が枯渇してきているということで、独立したファクトチェック機関の人員などが整理され出したりして、すごくファクトチェックが世界的に危機に瀕しています。

ですので、独立したファクトチェック機関がこれからサステーナブルにやっていけるかということになると、それはとても難しいことではないだろうかと。そうすると代替の何か組織みたいなものを考えていかなければならないと。

例えば韓国にSNU（ソウル大学）ファクトチェックセンターというのがあって、大学に設けられたファクトチェック機関が出したファクトチェックの情報を各メディアが自由に使えるようにする、というようなものもありましたが、これもサステーナブルじゃなくて、やっぱりお金を出していたメディアがどんどん引いていって、今、ちょっと引き潮状況にあると。

その反面、例えばフランスとかブラジルの選挙や何かだと、メディア全部で集まろうという動きにもなっているとなると、伝統メディアやほかの人たちを全部合わせたような裾野で、新たなファクトチェックの何か連合体みたいなものができていくようなものが望ましいのではないかと思われるような側面もあります。

ただ、それは誰が中心になってどういうふうに音頭をとるのかと。特にこの会議は政府中心の会議ですので、政府がそれをリコメンしたりリーダーシップをとるのかというかなり微妙な問題もあるということですので、政策としてどのように書き込むかというのはあるわけですけれども、一応そのような課題というようなものがぼわっと見えているということで、この表の中にうまくそれが表現できていないなというのが非常に気になったということを申し上げておきます。ありがとうございます。

【宍戸座長】　ありがとうございます。この場はまさに政府の検討会でありますけれども、まずもって、デジタル空間における情報流通の全体像を１回認識し切らないと、次の話が進まないし、そのことによって、では、民間で我々どうしようという御議論が盛り上がっていただくことが大事だと思っておりますので、図としてはしっかり、今いただいた御指摘を把握したいと思います。

その上で、今１ページに書いていただいているのは、まさに現状でございますので、現状日本だとこんな感じというところがあります。例えば５ページの、課題として見たときに、「持続可能なファクトチェック推進のための仕組みの在り方」という論点が、何かファクトチェック機関とプラットフォームなどの真ん中の伝送の部分だけというよりは、幅広く、右側の利用者あるいは左側の発信者を含めて、社会全体でこのファクトチェックの作用をつくり出し、支える。また、それを現実に具体的に担う主体がある場合もあれば、全体で作用するという場合もあるでしょうし、そこら辺は少し書き方を工夫させていただきたいと思います。よろしいでしょうか。

【奥村構成員】　ありがとうございました。

【宍戸座長】　ありがとうございます。

それでは、安野構成員、お願いいたします。

【安野構成員】　中央大学の安野です。大変丁寧な取りまとめ、どうもありがとうございました。先生方と指摘がかぶったら辞退すると申し上げて、微妙にかぶったりかぶらなかったりなので、一旦申し上げることをお許しください。

まず大きく分けて３点なんですが、１点目は、資料７－２－４の基本理念のところですね、

こちらをベースで、このような文言を入れていただければという御提案をしておきたいと思います。

まず一つは、先ほど奥村先生の御指摘と関連しているんですが、利用者のリテラシーのことですね、これを何らかの形で、陳腐かもしれないんですけど、入れていただけると、例えば情報に関するリテラシー教材との関連なども明確になってよろしいのではないかと考えました。

それからもう一つは、アテンションエコノミー、こちら、資料７－２－３の５枚目の全体像には入っているんですけれども、７－２－４の基本理念のところからこのアテンションエコノミーにどう立ち向かうかということ、背景に下がっているように思いますので、３ページ目以降ですかね、実質的なところにはこのキーワード、何度か出てくるんですけれども、取りまとめのところにも入れていただけると、以前、落合先生、それから森先生の御報告にもあったように、システムとして、ここにやっぱりどうしてもこういった誤情報や虚偽情報のインセンティブが出てしまうということに何らかの形で言及していただけると、個人的にはいいなと思いました。

ただ、それについてどうしようもないので外すということであれば、仕方がないかもしれないんですけれども。すみません、以上が１点目です。

２点目は、こちらは半分質問になるんですけれども、人権保護ですね、例えば誹謗中傷ですとかに対する対応とかは、これはどこに入るのかなということです。６か８かどっちかなのか、あるいは別途立てるのか、よく分からないんですが、例えば権利侵害の情報なのかもしれないんですけれども、具体的にはどこに入るのかなというところを明確にしていただけるとありがたいと考えました。

３点目は、最初に曽我部先生が御指摘されたこととも関係しているんですが、発信の責任ですね、これは森先生も御指摘されていましたけど、非常に重要だと思うんですけれども、あえて付け加えるとしますと、例えばＡＩの時代になりますと、責任が明確でない形での誤情報・虚偽情報が流れかねないということですね。こういう場合にどうするのか。何か意図がある虚偽情報・誤情報の問題もありますけれども、結果的に流れている何か虚偽情報・誤情報、これについても検討していく必要があるのかなと考えました。

以上、３点です。ありがとうございます。

【宍戸座長】　ありがとうございます。いずれも重要な御指摘をいただいたと思います。

２点目の御質問でいただいた誹謗中傷等は、私自身の認識では、まさに御指摘のとおり、

６の「安心・安全」の権利侵害情報の中の最たるものとして、名誉毀損であるとか名誉感情の侵害であるとか、その他、人格的利益の侵害ということで、プラットフォームサービス研究会でずっと議論してきた問題でもあるのですけど、その点は明確にしたいと思います。

また、昨今ですと、３点目に関わりますけれども、ＡＩを利用してコンテンツをつくって流通させるんだったら、ＡＩを使ったと書くことによって、人々がそういう向き合い方をするといったことは、ＡＩの規律の在り方の問題としても議論されてきており、それがまたアカウンタビリティの、先ほど出てきた話ということにも当然関わっているんだろうと思います。

この発信の責任あるいは発信されたコンテンツについての説明の問題、世の中が理解できるような問題を少し考えたいと思います。ありがとうございました。

それでは、石井構成員、お願いいたします。

【石井構成員】　資料７－２－４の今開いていただいているページの中の、８の「プライバシー保護」について、項目に入れていただき、ありがとうございます。

前回、プライバシー侵害と認知領域の保護についての御報告を差し上げた中で、いわゆる侵襲行為について御報告申し上げたところでありますが、同じ資料の中で、参考資料に挙げていただいている原則の例というものは、基本的には個人情報の取扱いに関する原則であるという点で、私の御説明した侵襲行為を全てカバーしているわけではないところを意識した上で、今後どのようなルール形成が必要かということを議論したほうがいいかと思いました。いわゆるプライバシー保護の観点と個人情報保護の関係を意識しながら、今後、ワーキンググループで議論していく必要があると。

認知領域に関するプライバシー保護を議論する上では、今のところの私自身の考えとしては、２点重要な視点があるかなと思っていまして、１つは、認知に働きかけられる段階で、どうすればその点に気づくことができるのか。働きかける行為にどういう歯止めがかけられるのか、非常に難しい論点になりますけど、１つ目はその観点になるかと思います。

２つ目は、意思決定を個人が行う段階で、どのようにすれば自律性が保障されるのか。すなわち意思決定がゆがまないようにするためには、どのようなルール形成があり得るのか。

認知領域に関するプライバシー保護を議論する上では、今の２つの視点は重要性を持つのかではないかと思いました。

既に存在するＯＥＣＤプライバシーガイドラインや個人情報の取扱いに関する原則でカバーされる部分なども当然あるのですが、それを超えたところをどのように考えていくの

かという課題に取り組むのがこの検討会であると考えております。もちろん参考資料の形で挙げていただいてはいるのですが、先ほど申し上げた点は今後議論する上での視点として重要な観点になるかと思いました。プライバシー保護の観点から、意識しておく点があるかと思いまして、念のためコメントさせていただきました。

以上になります。

【宍戸座長】　ありがとうございます。

それでは最後、山口構成員、手短にお願いいたします。

【山口構成員】　御説明いただき、ありがとうございました。また、お時間いただき、ありがとうございます。私も、今表示されております基本理念のところで少しだけコメントさせていただければと思います。

まず、何人かのほかの先生方から階層性という話題が出たと思うんですけど、それはこれからやるということを重々理解した上で、その観点で言うと、私、今これ、有事の話と平時の話って結構違うと思っているんですが、それが並列で書かれているというところで、今感じているところです。

その中で、有事という観点でお話しさせていただきますと、ほかの構成員からも御指摘のあったとおり、サイバー攻撃という話もありましたけども、情報流通の健全性というような文脈で、安全保障という観点が、キーワードが出てこないというのは、これを見た方は違和感があるんじゃないかなと思った次第です。

担当省庁が違うとか、様々なことはあるかと思うんですけども、その影響力工作など、様々話題としてある中で、サイバー攻撃に対する対抗というところはやはり重要かなと思いますし、近隣諸国での戦争状態とか、そういった中で一気に状況が変わることもあり得ますので、そういったことを少し強調するというか、特出しするのも必要なんじゃないかなと感じた次第です。

関連してもう一つ、有事というところで申しますと、「法の支配・民主主義」というところで、選挙という話が出てきていないというところですね。キーワードとして出てきていないという話です。当然頭にはあると思うんですけども、参考資料の中には選挙というものについて言及しているものも多いかと、下についている参考資料ですね、には多くて、例えば「情報的健康」の話だって、選挙モードなどの話をしていますし、ＥＵなどでの選挙という話が出てきますし、また、選挙時だけ法律が違う、選挙時に関してだけ、この情報公開に関して特別の法律を持っているというような国も結構あります。という中で、やはりこれも強

調していいんじゃないかなというふうに、つまり、選挙というキーワードを出したほうがいいんじゃないかなと思った次第です。

最後に、国際連携というようなキーワードが出てきていて、これもほかの構成員の方と少し話がかぶりますけども、さんざんステークホルダー間の連携が重要であるということを言ってきたところですし、また、総務省としても言ってきたところですので、プラットフォーム事業者とか、あるいはファクトチェック組織とか業界団体などなど、あるいはアカデミアとの連携というところも一行加えてもよろしいんじゃないかなと思った次第です。

私からは以上です。

【宍戸座長】　ありがとうございました。

お話全体を伺っていて、なかなか基本理念は書くのは大変だなとは思いながら、伺っておりました。今、事務局のほうでは、私もそうであったのですけれども、ひとまずは、これまでのインターネット、デジタル空間あるいは社会全体におけるいろいろな局面での基本理念として、いわば汎用的な概念を挙げてみて、御議論いただいてみようと思ったわけですけれども、一つには、包括性・網羅性が足りていない部分があるんじゃないか。それから少しとっ散らかっている、並立になっている部分がある。何よりもここで問題にしている情報流通の健全性という、固有のドメインの問題に合わせて、しかし、基本理念をきっちり、さらに具体像をもって書き起こしていくための、非常に重要な御指摘・御議論を本日いただいたかと思います。引き続き御意見、御指導いただければと思っております。ありがとうございました。

それでは、残り時間で議事の（４）、（５）についてやらせていただければと思います。

まず議事の（４）今後の進め方につきまして、資料７－３－１、７－３－２に基づき、事務局より御説明をお願いいたします。

【内藤補佐】　ありがとうございます。事務局でございます。

資料７－３－１を御覧ください。これまでの検討会について、第１回から第６回までの会合の主な概要は、資料の左側に簡単に記載してございます。

そして今後のスケジュールとなりますが、まず本検討会については、本日、第７回会合を開催した後、４月頃までプラットフォーム事業者などのヒアリングを、ワーキンググループとの合同開催で進めるとしてございます。また、併せて基本的な考え方や具体的な方策を御議論いただくこととしております。その後、取りまとめ骨子案、取りまとめ案を作成し、１か月程度の意見募集を行い、７月頃に取りまとめを作成することとしております。

ワーキンググループにつきましては、資料下側の緑の丸で記載しておりますが、本日が第１回会合となりまして、今後は適宜会合を開催し、検討会に報告するという進め方としております。

続きまして、資料７－３－３「「偽情報対策に係る取組集Ｖｅｒ．１．０」の更新について」を御覧ください。

まず、１にこれまでの御議論を整理してございます。昨年３月、プラットフォームサービスに関する研究会において、プラットフォーム事業者等のステークホルダーによる偽情報対策に係る取組について、関係者間で参照しやすくし、プラクティスの促進に資することを目的として、取組集Ｖｅｒ．１．０が作成・公表されました。

この取組集につきまして、昨年１２月に当研究会の大谷構成員より、収録する範囲を広げて取組集を更新するべきであるとの御提案がございまして、この御提案を踏まえて、本検討会第５回、同じく昨年の１２月に、プラットフォーム事業者などのヒアリングのアウトプットも踏まえ、取組集をアップデートすることについて御了解をいただきました。

続きまして、２のこの取組集の今後の進め方（案）について、まず１ポツ目、プラットフォーム事業者やファクトチェック関係団体等以外も含めた幅広いステークホルダーによる取組、例えばステークホルダー間の連携・協力、リテラシー・人材育成・普及啓発、ファクトチェック、研究・開発・実証、国際連携・協力等の取組につきまして、本年２月上旬から３月上旬の期間に意見募集を実施してはどうかとしております。

２ポツ目、この意見募集においては、国内のステークホルダーによる取組に限らず、今後の取組の参考となる、海外における取組も対象とした上で、サービス、技術、イベント、文献なども広く対象としてはどうかとしております。

続いて３ポツ目、この募集により提出された取組とヒアリングの結果を合わせて、本検討会での御議論を経て、本年春頃、例えば国際ファクトチェックデーである４月２日にあわせて公表してはどうかとしてございます。

最後に、４ポツ目となりますけれども、この取組集を英訳して公表することで、日本における取組を国際的に情報発信するとともに、国際的な議論への貢献等を通じて国際的な連携・協力を積極的に推進してはどうかとしてございます。

２ページ目からは参考資料となりますけれども、２ページは、昨年３月に取りまとめられた取組集Ｖｅｒ．１．０の概要となります。３ページ目から５ページ目は、検討会第５回の国際動向に関する資料５－１－２からの再掲となります。

簡単でございますが、事務局からは以上でございます。

【宍戸座長】　ありがとうございます。

構成員の皆様から特に御異論がなければ、今後、親会、ワーキンググループ、それから取組集の更新について、今、事務局から御説明ありましたように進めさせていただきたいと思いますが、いかがでございましょうか。

（「異議なし」の声あり）

【宍戸座長】　異議ありませんといただいております。ありがとうございます。

それでは、今御説明いただいたように進めさせていただきたいと思いますが、特に最後の偽情報対策に関する取組集の更新につきましては、今説明がありましたように、かなり対象を広げて、また、この間、国内外で議論が進んできたこと、あるいは課題も見えてきつつあるということを踏まえて更新をしていく関係で、構成員の皆様、また、構成員の皆様がそれぞれ知っておられるとか、関わっておられるプロジェクトとか、御研究とか、こういう人がいるよとかいう情報は、ぜひどしどし事務局のほうにお寄せいただければと思います。これ、事務局と何の打合せもなく私申し上げていますので、事務局が大量の情報提供でかえって溺れる可能性もございますけれども、これは、私、非常に重要なことだと思っておりますので、ぜひ構成員の皆様、情報提供等いただければと思います。よろしくお願いいたします。

それでは最後、議事の（５）でございます。全体を通じて構成員の皆様から、何かこの機に御注意いただく点ございますでしょうか。よろしゅうございますでしょうか。

森先生、どうぞお願いいたします。

【森構成員】　すみません、時間がないところ。１点だけですが、これからヒアリングをお進めいただくに当たって、プラ研では海外プラットフォームのヒアリングで時間が足らないということがしばしばありましたので、その点について御配慮いただければと思います。よろしくお願いします。

【宍戸座長】　ありがとうございます。この点、私も前回も申しましたし、また、プラットフォームサービス研究会での反省といいますか、何度も森先生にお叱りをいただいたという経験も踏まえまして、本当に聞きたいことが聞けるように、事前にきっちりとした項目を示してすり合せをすること、また、やり方も趣旨をきちんとお伝えをしているところでございます。この場で改めてこのことは申し上げて、また事務局でも確認していただきたいと思いますが、事務局、よろしいですか。

【内藤補佐】　事務局でございます。今、宍戸座長からいただいた御指摘について、承知

いたしました。

【宍戸座長】　ありがとうございます。森先生もありがとうございました。

【森構成員】　ありがとうございました。

【宍戸座長】　事務局からほかに何か、この機に連絡事項等ございますでしょうか。

【内藤補佐】　ありがとうございます。次回会合の詳細につきましては、別途、事務局から御連絡さし上げるとともに、総務省ホームページに開催案内を掲載いたします。

以上でございます。

【宍戸座長】　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」の第７回会合兼「ワーキンググループ」の第１回会合の合同会合を閉会とさせていただきます。

本日も誠にお忙しいところ御参集いただき、また、短い時間の中で活発な御議論をいただき、ありがとうございました。これにて閉会といたします。