

AIネットワーク社会推進会議（第20回）

AIガバナンス検討会（第16回）

合同会議

議事概要

1. 日時

令和4年2月8日（火）15:00～17:00

2. 場所

オンライン開催

3. 出席者

（1）構成員

【AIネットワーク社会推進会議】

須藤議長、岩本構成員、大田構成員、金井構成員、喜連川幹事、木村構成員、小塚構成員、近藤構成員、実積構成員、鈴木（晶）幹事、高橋構成員、谷崎構成員、田丸構成員、時田構成員（代理出席）、中川幹事、長田構成員、林構成員、東原構成員（代理出席）、福田構成員、藤田構成員、堀幹事、武藤構成員、村上構成員

【AIガバナンス検討会（平野座長以外のAIネットワーク社会推進会議構成員を除く。）】

平野座長、雨宮構成員、江間構成員、岡本構成員、落合構成員、河島構成員、三部構成員、鈴木（教）構成員（代理出席）、高木構成員、武田構成員

（2）オブザーバー

個人情報保護委員会事務局、消費者庁、文部科学省、経済産業省、情報通信研究機構、理化学研究所、産業技術総合研究所

（3）総務省

竹内総務審議官、佐々木総務審議官、鈴木官房総括審議官、竹村官房総括審議官、吉田情報流通行政局長、高地サイバーセキュリティ・情報化審議官、小野寺国際戦略局次長、藤野官房審議官、辺見官房審議官、飯田国際戦略局国際政策課情報通信政策総合研究官、大村情報流通行政局情報通信政策課長、尾川情報通信政策研究所調査研究部長、本間情報通信政策研究所情報通信政策総合研究官

4. 議事概要

（1）講演

田丸構成員より、資料1に基づき、『デジタルツインとメタバース』について講演が行われた。

(2) 講演

三部構成員より、資料2に基づき、『EUのAI規則案の概要と、欧州での反応について』講演が行われた。

(3) 事務局からの説明

事務局より、資料3に基づき、国内外の動向及び国際的な議論の動向について説明を行うとともに、資料4に基づき、AI開発ガイドライン及びAI利活用ガイドラインに関するレビューについて説明を行った。

(4) 質疑応答・意見交換

<議事(1)について>

【須藤議長】

- ・ HoloLens 3（複合現実（MR）ヘッドセットの次期モデル）の開発が昨年に中止され、今戦略の見直し中であるというような報道が先週にあったが、次の戦略はどのような方向に動いているのか。

【田丸構成員】

- ・ そこは話せない部分であるが、仮想現実世界にいか自然にアクセスできるようにするかということ考えたときに、必ずしも HoloLens だけではないと思う。様々な手法を考えていく上で、そのベースとなるのが、そもそも仮想空間、現実の世界での情報量をいかに高めていくかということとあり、HoloLens のチームをメタバースの方に投入して、そちらを加速させることになるかと思う。

【平野座長】

- ・ ソーラーパネルのシミュレーションのリアル感が素晴らしかったが、コンセプトとしては、実際の実務の事前の検証などに使うというアイデアであると思う。テーマパーク用のライドがパイロットの養成のシミュレーターに使えるということと同様に、今回のシミュレーションも、例えば、パイロットの養成において本当に飛んでいる実感を与えて訓練することなどにも使えると思うが、そのような可能性はあるか。

【田丸構成員】

- ・ どのような状況で、どのような操作をするのか、また、その時にどのような負荷がかかるのかということで、ソーラーパネルの例を紹介した。パイロットの育成というよりも、ある環境下において、どこでどのような不具合が起き得るのかといったことを仮想環境の中で検証することに重きを置いている。

【高木構成員】

- ・ ソーラーパネルについて、仮想のものをどのくらい現実に近づけるのかということが重要であると思うが、地形のデータは実際に収集したものを使っているのか。

【田丸構成員】

- ・ ジオデータに関しては実際のものを使っている。ソーラーパネルの場合、現実には隣の家の屋根が影になることがあるため、仮想空間の世界を実現するに当たっても、ジオグラフからのデータだけではなく近隣の建物の情報などもすべて含む形になる。

<議事（2）について>

【実積構成員】

- ・ EUの規制法案において、AIのどの段階で規制されるのか。例えば、ソーシャルスコアリング用のAIを開発しただけで規制するのか、それが実際に利活用される段階で規制するのか。
- ・ 認定制度については、リスクがあるAIを提供しようとしている企業が自らそのAIが安全であることを証明しようと提出するものだと思うが、隠れてリスクがあるAIが使われることに対して、そのAIの性質を調査するEUの機関というのは設定されるのか。
- ・ AIのアウトプットをEU域内に提供するものも規制対象になるとのことであったが、例えば、AIを使ってデザインした製品なども考えられる。かなり幅が広いと考えられるが、「AIを使った」というのは、どの程度の範囲なのか。
- ・ 規制のサンドボックスという話があったが、日本の特区のようなものが想定されているのか、あるいは、メタバースのようなものを使って、環境を用意するということが想定されているのか。

【三部構成員】

- ・ AIがどの段階で規制されるかということは、基本的にはそのAIを何らか提供するという場面と考えるとよい。市場に置く、サービスを開始するといった文言で区切られており、そのような活動をする段階で規制がかかることになる。ただし、システム自体が規制対象となるので、ある程度具体的に開発をしている段階からやらなければならないことがある。ハイリスクAIに該当するか否かについては、構想段階で考えておくことが重要である。
- ・ 認定制度に関連した調査については、具体的に加盟国との役割分担がどのようになるのかが未確定であるが、今のところ、加盟国において監督機関が選任され、その機関が動く形になっている。GDPR（EU一般データ保護規則）における各加盟国の機関に近いような形が想定されているのではないか。
- ・ アウトプットをEUに提供することについては、法案では「アウトプット」としか書かれていないため、今後の動きを見る必要がある。
- ・ サンドボックスについては、特区というより、個別プロジェクトごとに申請を受けて設定されると想定される。特定のプロジェクトについて、一定期間は規制を課さず、実証実験を認め、事業者から国に情報提供するようにして、規制の形を考えていくようなものになると想定される。ただし、各国で既に行っているサンドボックス制度との差異がどのようになるかについて、動向は注視していく必要がある。なお、AIに限ったものではないが、サンドボックス制度は、日本でも導入されている。

【実積構成員】

- ・ サンドボックスの対象はEUが直接認定する形になるのか。

【三部構成員】

- ・ サンドボックスについて定めている第 53 条では、加盟国所管機関又は欧州データ保護観察機関によって設置される A I の規制のサンドボックスとある。加盟国所管機関というのは、1 又は複数ということであり、1 つの国で置く場合もあれば複数の国で置くということも理論上はあり得るということになる。

【平野座長】

- ・ 英国は E U から離脱したため、E U 規則案は全く関係ないと思うが、親和性があるのか感触を伺いたい。

【三部構成員】

- ・ E U から離脱しているが、E U と非常に距離的にも近く、歴史的にはもっと近いとのことで、調査対象に加えることが適当であると判断した。また、規制法案において、域外適用がある点は日本と変わるものではなく、域外適用を受ける最も典型的な国として、その動向をウォッチすることは日本にとっても非常に重要である。そのため、英国のことを研究することも重要である。

【林構成員】

- ・ 4 つのリスク分類というのが、どれくらい世界標準になるのかという見通しを教えてください。E U のこの基準に対して、日本からも企業も政府も含めて意見表明するなどの積極的に関わっていく必要があると思う。
- ・ 加盟国政府による認証機関による審査について、ハイリスク A I に関しては、適合性評価手順を経る必要があるとのことであるが、規則案の記載が抽象的であるため、加盟国間でばらつきが生じる可能性があると思うが、見通しを伺いたい。

【三部構成員】

- ・ リスク分類に関する見通しは難しい。A I 規則案に記載されているハイリスク A I と許容できない A I の分類に関して、世界標準にまでなるかわからない。ただ、ある程度影響を及ぼすことについては、相応に考えていく必要がある。
- ・ 適合性評価については、検討すべきことが広範であり、完全に将来の課題である。

【中川幹事】

- ・ A I はデータに依存するところが大きく、データがサプライチェーンの中で非常に重要な要素になる。また、様々なデータが多様な形でつながったり、名寄せされたりと非常に複雑な構造になることが想定される。規則案において、その複雑な構造をコントロールしていくということがどの程度意識されているか。

【三部構成員】

- ・ データに関して定められている条文は、例えば、データガバナンス、ログの保存などがあり、その運用次第ということになる。技術的要件が明確にされていないため、今のところ、それ以上の情報

はない。規則案第3編第2章において、ハイリスクAIシステムの要件について、第40条や第41条に基づき今後定められることとなっている。その腹案がいつの段階で出てくるのかというのがポイントになってくる。

<議事(3)及び(4)について>

【高木構成員】

- ・ AI利活用ガイドラインを策定した際に、資料4の中にもある価値観の比較表を載せた。海外との議論においても有用であり、比較をしながらどこに違いを見出していくのかといった作業は非常に重要であると思っている。また、今後どのように実践的なものにしていくのかという点から、各原則間のバランスが重要であり、どのような状況において、何を重視しなければならないのか、トレードオフがあることも踏まえて、マルチステークホルダーの本会合で議論を深められるとよい。

【須藤議長】

- ・ AIについては、運用のフェーズに入ってきており、尊重すべき価値として、新しく抽出された「堅牢性」、「責任」、「追跡可能性」、「モニタリング・監査」、「ガバナンス」、「コスト」、「効果測定」というのは、運用フェーズにおけるガイドラインの観点であると思われる。これらの概念を打ち出していくことは重要である。
- ・ セキュリティの観点から、ガイドラインにおいて、ブロックチェーンをどのように位置付けることが適切であるのかを明確にしておくことも重要ではないかと思う。

【中川幹事】

- ・ ガバナンスということを考えるときに、AI自体をガバナンスするという考え方があるが、他方で、AIをツールとして社会や企業をガバナンスするという考え方もある。この2つの考え方をもう少し精密に分けて考えることが今後必要になってくるのではないかと思う。
- ・ セキュリティについて、外部からの侵入を完全に防ぐことは困難であり、むしろ、侵入されても被害を最小限にして、早く原状復帰にたどり着くレジリエンシー、システムとしてのセキュリティという考え方が重要になっている。
- ・ 現状においては、自動運転のように、AIは相互に通信し合いながら、つながって動いている。セキュリティを考えると、一部問題のあるAIがあった時に、他のAIに波及しないようにすることが重要であり、システムに対するレジリエンシーということが、今後AIが使われる社会において必要になるのではないか。
- ・ AIが使われる社会において、トラストの捉え方について、何らかの方向性があった方が、AIを開発する側にとっても指針として役立つものになると思う。

【須藤議長】

- ・ 中川幹事の御意見に賛成であり、リスクを最小限に抑え込むというリスクコントロールについて、どのようにアーキテクチャを作っていくのか、また、どのようにガイドラインに書き込むのかということが重要になってくる。

【事務局】

- ・ ガバナンスについて、今のところ、AIをツールとして社会や企業をガバナンスするという観点はないが、御意見を踏まえて、今後検討していきたい。
- ・ セキュリティにおいて、レジリエンシーの考え方には留意していきたいと思う。
- ・ AIが相互につながっているという御指摘については、本会合は「AIネットワーク社会」ということで十分に意識しており、現行のガイドラインにおいて、「連携の原則」の中で、ネットワーク化による便益やリスクの増幅の可能性に留意する旨が記載されている。今後の状況の変化を踏まえて、更に検討したい。
- ・ トラストについても、今後の検討を踏まえて、反映できるものがあれば、反映していきたい。

【中川幹事】

- ・ ネットワークの観点は、より強調すべき時代になってきたと思う。

【小塚構成員】

- ・ ブロックチェーンについて、CAHAI（欧州評議会 AIに関するアドホック会合）においてドキュメントが公表されることになっている。事務局でフォローしていただきたい。
- ・ 尊重すべき価値として、新たに抽出されたものがあるが、例えば、「追跡可能性」や「モニタリング・監査」というのは、「透明性」を確保するための手段であると考えられる。今後、新しい項目を拡張していくイメージなのか、基本価値と実現手段とに分けていくというイメージなのか、事務局の考えを伺いたい。

【事務局】

- ・ ブロックチェーンについては、事務局でフォローしたい。
- ・ 資料でお示ししたのは、形式的に用語の有無等で整理したものとなっており、現行のガイドラインにおいて、原則として盛り込まれていないものについては、新たに追加すべきという考え方もあるのではないと思う。他方で、例えば、「透明性の原則」において、追跡可能性といった概念は解説などで既に盛り込まれている面があり、新しく盛り込む必要はないという考え方もあると思う。事務局としては、構成員からの御意見を踏まえて、方向性を決めていきたいと考えている。

【落合構成員】

- ・ ブロックチェーンについて、セキュリティの関係で一番問題になっていたのが暗号資産の関係であると思うが、CGTF¹、JVCEA²などにヒアリングする方法が考えられる。また、内閣官房の旧IT総合戦略室と新経済連盟とで開催していた官民推進会合でレポートが公表されているので、参考になると思う。

¹ Cryptoassets Governance Task Force。セキュリティの専門家と仮想通貨交換業者の関係者で構成される研究会。

² Japan Virtual and Crypto assets Exchange Association（一般社団法人日本暗号資産取引業協会）。

- 中川幹事から御指摘があったA Iが連鎖する点について、分析が進んでいる分野として金融分野が挙げられる。システムリスクなどの関係で、B I S（国際決済銀行）、I O S C O（証券監督者国際機構）といった国際団体において検討されており、また、国内においても日本銀行金融研究所が検討している。
- 個別分野について言及したが、すべての個別分野を検討対象とすることは難しいため、全体にとってプラスになるようなところがあれば、ブラッシュアップの際に検討していただきたい。個別の分野特有の議論には踏み込み過ぎない方が、読み手にとってわかりやすい面があるという点は考慮していただくとよい。
- 例えば、プログラム医療機器の認証に関して、どのような形で法規制をしていくのかというところで薬機法³だけではなく、保険収載の評価などで国内でも制度のアップデートが繰り返されている。また、認証の方法についても、日本では個別の製品の認証、米国では体制認証というように異なっていることもある。ガバナンスの手法としての国際比較において、一般法ではなく、具体的な個別法レベルで分析するとアップデートによってプラスになる部分もあると思う。

以上

³ 医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律（昭和 35 年法律第 145 号）。