

## 第3回 先進的 AI 利活用アドバイザーボード

### ■ 資料及び議事要旨の公開について

本検討会の資料の一部については、関係者による闊達な議論につなげる観点から非公表とし、議事については議事要旨として公開する。

### ■ 概要

- 日時：令和8年3月10日（火）9：30－11：30
- 場所：デジタル庁 20F 庁議室・オンライン開催
- 議事次第
  1. 開会
  2. 議事
    - (1) 各府省庁生成 AI システム定期報告概要
    - (2) 我が国及び諸外国における生成 AI に係る動向
    - (3) 行政の進化と革新のための生成 AI の調達・利活用に係るガイドライン充実に向けた改定案
  3. 閉会

### ● 資料

#### 議事次第

資料1：各府省庁生成 AI システム定期報告概要

資料2：我が国及び諸外国における生成 AI に係る動向

資料3：行政の進化と革新のための生成 AI の調達・利活用に係るガイドライン充実に向けた改定案

参考資料1：「行政の進化と革新のための生成 AI の調達・利活用に係るガイドライン」改定案

参考資料2：知的財産権等対策参考シート（案）（非公開）

参考資料3：国民向け生成 AI システム 利用規約作成時の留意事項（案）（非公開）

### ■ 出席者

#### (1) 構成員

門林座長、岡田構成員、北村構成員、柴山構成員、鳥澤構成員、永沼構成員、生田目構成員、吉永構成員

#### (2) デジタル庁

松本デジタル大臣、川崎デジタル大臣政務官、浅沼参与、伊藤参与、三角デジタル監、富安デジタル審議官、荻原統括官、蓮井統括官、森田総括審議官、井幡審議官、奥田審議官、北間審議官、内藤参事官、橋本参事官、山口参事官

### ■ 議事

冒頭、川崎デジタル大臣政務官から、ロボティクスやステーブルコイン等の登場により AI エージェント等の利用シーンが増えていく中で、「AI 基本計画」に基づいてガイドラインを充実させていく本会議の重要性について発言があった。

## <（１）各府省庁生成 AI システム定期報告概要>

事務局より、各府省庁による生成 AI の利活用状況の分析結果について資料 1 により報告した。

### <質疑及び意見>

出席者の主な質疑、意見等は、以下のとおり。

- （生田目構成員）定期報告について、取組が各府省庁において実用化が進み、定性・定量の成果も見えているという状況を理解した。定量的な成果目標として整理できる部分も見えてきていると考えられる。今後中長期的な視点で見た場合に、各府省庁にて、AI の導入によってどのような成果を得られたか、国民向けに共有するような取組も有効と考える。各府省庁の効率的な業務運営に貢献するような取組になるといいのではないかと。民間企業においても、AI の導入により業務時間が削減できたことも確認しているが、組織の中で浮いた時間が吸収されてしまうことがある。その結果人員を減らせたということではなく、単に夜 8 時まで残業していたのが夕方 5 時までで終わるだけで業務実態は変わらないといったケースもある。このように可視化されていく課題が、各府省庁における業務効率化の検討には重要と考える。
  - （事務局）成果目標については、本年度から AI 利活用を進め始めたところであり、まずはどのくらい業務効率化ができるかということを見つ、指標を立てている。実際の利活用が進み、成果目標がどのように達成できるか等は今後も注視していきたい。民間と同様に、AI を活用しても業務時間が削減されないというケースは我々でも観測している。役所だけで解決できない状況もあると考えられるため、民間の中でも良いマネジメントのスキームがあれば参考にしていきたい。
  - （事務局）AI の成果を客観的に評価し、どのような形で示していくかというのはこれからも検討していかないといけない。利用促進という意味では、客観的な指標から見えてくるメリットを広く共有するのが大事。そういったことを心がけ、どのように指標を設定するか、どのように成果目標を示していくか引き続き検討する。
- （吉永構成員）AI は業務効率等の政府職員のベネフィットをもたらすものでなくてはならないため、成果を可視化するのには意義があり、良い取組だと考える。また、利用目的によってリスクは異なる。例えば、対国民向けのシステムは特にリスクが高くなる。今後各府省庁内で生成 AI が政策立案・形成に活用される場合は、間違った情報に基づいて判断しないように注意する必要がある。利用目的に関する情報を今後収集していく必要があると考える。単なる情報収集なのか、あるいは政策立案に活用されているのか等も含めて、利用目的の詳細を示していくことをお願いしたい。
  - （事務局）利用目的に関しても報告頂いているところ、どのような分類ができるか等を引き続き整理し、各府省庁への共有も検討していきたい。
- （柴山構成員）資料 1 の 5 ページにて、機密性 2 情報を参照した AI の利用が増えていると記載があるが、ひとえにデジタル庁の取組の成果だと考える。こういった利用について、例えば政府職員が議事録用に AI を使いたいといったケースにおいて、前例があるか、どのようなサービスをどのような条件で使っているかといった照会や問い合わせがデジタル庁宛てに来た場合に、照会に応じる仕組みや体制はあるのか。先日、個人的に国立の法人から相談を受けた際、前例が具体的にどのようなものがあるのか、前例があったら心強いという話があった。具体的な前例の有無や内容を政府内で共有できる仕組みはあるか。
  - （事務局）デジタル庁事務局として AI 相談窓口を開設しており、そちらを各府省庁担当部局に連携する仕組みを運用している。まだユースケースの蓄積は途上ではあるものの、現段階でも相談内容に応じて利活用事例の共有等は可能である。
  - （柴山構成員）ある程度、使っているサービス等の具体的な情報も照会に応じているのか。

- （事務局）おっしゃるとおり。案件によっては、具体的な案件内容のヒアリングをすることもしており、ヒアリングを通して具体的な情報も収集している。
- （鳥澤構成員）定期報告概要は、情報の粒度が粗く、今後どのような施策を打つべきなのかイメージが湧かない。より詳細な情報収集をしようとするれば各府省庁の負担になるため難しいかもしれないが、利用目的やどういったシステムであるかの情報等を概略的にでも集められるとよいと思う。各府省庁での利用推進は理解できたため、数だけ集計する段階を脱して分析する段階になるとよいと考える。
  - （事務局）必要な情報は状況に応じて変わってくると考えているため、各府省庁のニーズを踏まえつつ分析内容を検討していきたい。特に利用用途や、どのようなシステムやモデルを使われているか等の情報は、引き続き検討していきたい。

## <（2）我が国及び諸外国における生成 AI に係る動向>

事務局より、我が国及び諸外国における生成 AI に係る動向について資料 2 により報告した。

### <質疑及び意見>

出席者の主な質疑、意見等は、以下のとおり。

- （生田目構成員）AISI の「AI インシデントレスポンス・アプローチブック」には、可視化（観測性）と封じ込め（制御性）が重要であるとの記載があるがそのとおり。可視化というのは一体誰がどのように実施するのかというのが疑問。シンガポールの「エージェント型 AI のためのモデル AI ガバナンスフレームワーク」では、人間が責任を持つべきであると記載があり、人間が可視化するというプロセスをどのように行うかが重要と考えている。デジタル庁としてどのようなフレームワークを考えているか、各府省庁でどのような取組をしているかお聞きしたい。
  - （事務局）可視化（観測性）の部分については、「AI インシデントレスポンス・アプローチブック」ではセキュリティ面での可視化を意図している側面が強く、ガイドライン上ではログ等をもって検証可能にするという対応事項を資料 3 にも記載している。アカウントビリティについては、AI 事業者ガイドラインで人間中心に関する記載があり、AI 調達利活用ガイドラインにおいても説明責任の記載がある。行政として、一義的に説明責任を負わねばならないということは明らかにしている。「AI インシデントレスポンス・アプローチブック」の可視化について、北村構成員より補足はあるか。
  - （北村構成員）事務局からの説明のとおり、「AI インシデントレスポンス・アプローチブック」のフレームワークは、まずはサイバーセキュリティに重きを置いている。隔離ゾーンと呼んでいるが、AI エージェント等の利用中にインシデントが発生した場合に、しっかりと AI を隔離し、安心安全に使い続けるということが重要である。AISI からは今月中に CAIO に関する実務的なガイドブックも公開予定。一度作った規程やガイドラインを、今後の動向を踏まえてどのようにアップデートしていくかの検討は重要と考えている。
- （吉永構成員）シンガポールの Agentic AI に関するモデル AI ガバナンスフレームワークの他に、OECD からも AI Agent/Agentic AI に関する定義等に関するレポートも出たため、参照いただくと良いと考える。米国 NIST からも AI エージェントの技術標準策定の取り組みが発表されているため、ご参照いただきたい。
  - （事務局）OECD の Agentic AI の定義は、AI 事業者ガイドラインの改定案でも言及されているが、まだ検討中の内容であるため、暫定的なものとなっている。AI 事業者ガイドラインが確定した場合は、そちらの定義を注釈等で参照することを検討している。
- （岡田構成員）資料 1 を見ていると、国内ではどちらかというと効率化やコストダウンのために AI を使っているところが多いと思う。一方で、資料 2 の諸外国動向では、効率化と、安全に使うことが強調されている。ドイツの「行動共

通基盤としての価値観に基づく指導原則」では、「チャンス志向」というポジティブな言葉が使われている。この「チャンス志向」というのは、付加価値を増大させる使い方や、新しいアウトカムを発見するような使い方が想定されているのか、あるいは単なる効率化のみなのかを調べていただきたい。その情報を参考に、我が国でのポジティブな使い方について検討していただきたい。

- （事務局）AI を使うこと自体が目的になりつつあるという懸念もある。利用率だけを見るのではなく、AI を使う目的と、使うことによってどういったことが実現できるかを含めて検討する必要があると考えている。IT の失敗事例からも見られる傾向だが、IT を使うこと自体が目的となってしまった事例もあった。「チャンス志向」についてもそういった観点と関係があると考えため、しっかりと調査を進めつつ引き続き検討したい。
- （門林座長）議題 1 及び 2 の議論を通して、AI の利用目的と観測性は深掘りする余地があるため、引き続き産官学でベストプラクティスを見ていき、現状把握の方法を検討していきたいと考えている。

### <（3）行政の進化と革新のための生成 AI の調達・利活用に係るガイドライン充実に向けた改定案>

事務局より、ガイドライン充実に向けた改定案について資料 3 により報告した。

#### <質疑及び意見>

出席者の主な質疑、意見等は、以下のとおり。

- （永沼構成員）第 2 回アドバイザーボードで経団連関連企業のヒアリング結果を説明したが、今回の改定案に関して、4 点申し上げたい。1 点目に、ガイドラインの対象 AI に関して、音声及び画像出力を伴う生成 AI を含むスコープ拡充の方向性には賛成。民間企業においても、実務における活用が進んでおり、官民双方の利活用の実態に即したものであると考える。2 点目に、リスク判定ロジックについて今回アップデートがあったが、セキュリティ設計の考え方に基いており、民間企業の実務感覚とも整合している点で評価をしている。一方で、運用の段階において、重大な影響の該当の判断を個々の CAIO に委ねすぎると、府省庁間や案件間でばらつきが生じるのではないかと懸念している。3 点目に、調達チェックシートに関して、対策例や裏付けとなる情報の例、ベンチマーク例等の充実化により、透明性及び説明責任の向上に繋がると考える。対策例の部分について、「可能な限り」と記載があるが、学習データやモデルの内部、セキュリティの部分等は、競争的な関係からも現実的な要求事項となるようご議論いただきたい。その中でも、知的財産権等に係る部分を特にご議論いただくとありがたい。また、前回のアンケートの結果にもあった件として、個別案件ごとに詳細なチェックが行われるとのことだったが、一定の要件に関しては、外部認証等の既存の仕組みとの組み合わせも示していただくことで、民間企業の参入に繋がると考える。4 点目に、現行の運用では、複数のガイドラインを相互に参照する必要がある。一本化することは難しいと考えられるものの、クロスリファレンスをつけていただくことで民間も優先付けをして参照できるのではないかと考える。
- （事務局）2 点目のリスクロジックに関して、高リスクの案件はまだ少ない。今後運用が進めば増えるのではないかと想定もしているが、具体例を踏まえた詳細化は今後の検討課題と考えている。AI 相談窓口で各府省庁から相談を受けており、運用上は各府省庁での判断の差異が大きくなり過ぎないようにしている。3 点目に関連する内容として、学習方法について、資料 3 の 24 ページに観測性の記載があるが、最低限「主要性能指標情報等の情報を取得する」等、AI を使う上で当然知っておくべき内容を記載している。その上で、「リスク分析やリスク対応の検討のために合理的な範囲で」としており、生成 AI 開発上の営業秘密に係る部分は、必要な範囲での要求とならないように努めている。調達チェックシートの要求事項が過度ではないかという観点については、今後の意見募集の結果も踏まえ、検討をしてみたい。外部の認証の活用については、現時点では活用はしないこととしているが、実際の導入状況を見ながら検討すること

としてまいりたい。4 点目について、関連する政府内や AISI のガイドライン等のクロスリファレンスをしつつ、調達・利活用の観点で必要な内容をガイドラインに取り込んでいる。調達チェックシート上に関連ガイドラインを記載しており、少なくとも調達・利活用の場面では網羅的な把握ができるようなものになっている。

- （吉永構成員）14 ページの「6.5 政府における生成 AI システムの提供者の対応事項」の改定箇所について質問がある。「利用者が高度なタスクを実行できる AI エージェントなどを作成できる生成 AI システムにおいて、出力結果の適切さの判断を行わずにタスクを実行するものを作成した場合には、提供者又は AI 統括責任者（CAIO）に報告させることが求められる。」の記載について、AI システム提供者が提供する利用範囲を超えて利用しないということは利用規約にも書かれると考えるが、具体的にはどのような事象を想定されているか。
  - （事務局）AI エージェントのような、様々なアプリケーションと連携し、何らかのアクションを自動でできるようなものを想定している。アプリ連携を設定すると、メールの返信等を自動的にを行い、場合によっては人の目を介さずに返信がされる可能性がある。大手のサービスではこのようなサービスが利用可能になっている状況。これを府省庁内でどこまで利用できるかというのは現実的な課題となっており、Human in the loop から抜けてしまう部分はリスクが高くなる。このため、そういったシステムを提供可能にする場合には事前に申告・リスク判定をするようにしている。
  - （吉永構成員）システム提供者にも報告する必要があるのかどうか気になっている。全てを CAIO に報告することも CAIO の負担になると考えるが、リスク管理の観点からこのような記載となっているのか確認したい。
  - （事務局）提供者に対して報告するかどうかは任意としている。ただ、提供者に報告があった場合でも、CAIO に報告することとしている。
  - （門林座長）該当箇所について、書きぶりの改善を含め、事務局で検討する。
- （鳥澤構成員）意見募集（パブリックコメント）を介して調達チェックシートを改善していくとおっしゃっていたが、国産 LLM を開発している事業者は多くないため、事業者と直接議論をしていただいた方が良いと考える。パブリックコメントだけではニュアンスを拾いきれない懸念がある。また、調達チェックシートにあるチェック項目の要求事項が実際に満たせるかどうかの議論もした方がいい。今回、「源内」で国産 LLM が 7 社選定されたとのことだが、そのあたりの事業者との相談も検討されると良いと考える。
  - （事務局）事務局としても、パブリックコメントと並行して、事業者との意見交換を行っていく想定。
  - （門林座長）私もこのあたり気になっている。LLM や AI エージェント等のクリエイターと密に調整が必要と理解した。事務局の方で別途そのような場を調整いただけるということか。
  - （事務局）そのように取り組んでまいりたい。
- （生田目構成員）永沼構成員からも、知的財産権等の改定に関して強調されていたが、同感であり、こちらに関して明確な記載が拡充された点には賛成である。米国では AI に関する訴訟が常態化しているが、一番多いのが著作権侵害のケースである。その上で、著作権侵害の保護に関する記載に関しては、他者の知的財産権等の侵害等を起こさないことを起点に記載されていると理解している。各府省庁において知的財産権等を保有しているケースもあると思うが、第三者が悪意を持って政府内データにアクセスし、著作権侵害を行うケース等もあると考えられる。こういったケースに対してどのような対応や注意喚起を行っているか伺いたい。
  - （事務局）政府がホームページ等で公開している情報は、オープンデータ等として提供されているものが多いと想定している。そういった情報については、生成 AI 以前から、オープンデータに関する規約を整備している。オープンデータに AI システムがアクセスする場合も、基本的には既に整備されている規約の範疇である

と想定している。基本的に府省庁が公開しているデータを使用する場合は、出典を記載する等していただければ使用いただいて問題ない。

- （生田目構成員）既存の規程でカバーできると理解した。その上で、生成 AI ではフェイク生成や改変を行う等、悪意を持った使用も考えられるため、生成 AI に対する政府データの活用については、一定の注意喚起の発出等を考えられると良いと考える。
- （事務局）政府以外の事例も踏まえながら検討してまいりたい。
- （北村構成員）AI を取り巻く環境は急速に変化しており、従来のように半年～1年単位で規程やガイドラインを改訂する方式には限界がある。そのため、変更点や更新内容を随時公表する仕組みとして、いわゆるリリースノートのような形など、内容をより機動的に更新できる方法を取り入れるとともに、その運用にあたっては日本の強みを活かした形での運用の在り方を検討することが重要である。
  - （事務局）今回のガイドラインも、幹の部分は変えずに、枝葉の部分をアップデートしやすくという形を考慮して進めていた。例えば、対策例詳細は現時点でも参考情報という位置づけだが、いずれはガイドラインから切り離すことも考えられる。改定案の留意事項①（4）に、CAIO に対する注意喚起に関して記載を追記しており、実務においては CAIO 連絡会も開催している。ガイドライン本体の改定だけでなく、こういった CAIO 連絡会等の場を使いながら、ガイドラインだけでは補えない運用面での情報等を共有してまいりたい。
  - （北村構成員）おっしゃるとおりの進め方が良いと考える。2025 年は AI エージェントの年、2026 年はフィジカル AI の年と呼ばれている。米国においては、第一四半期から第二四半期で、事業実証を見据えた AI エージェントに係る体系的なアプローチが出てくると想定されるため、動きを注視していく必要がある。また、資料 2 のドイツの「連邦行政における人工知能利用ガイドライン」における「チャンス志向」の意味を理解するための継続的な動向調査の参考情報として、昨年度にドイツの研究機関や大学を訪問した際の状況を共有したい。訪問時の意見交換では、ドイツでは DX および AI の活用を通じて産業競争力の強化を図り、国力の向上につなげていくとの認識が示されていた。また、その際には品質保証など自国の強みを活かした取組の重要性についても言及があった。品質保証は日本にとっても強みであるため、ドイツの動向は今後の検討において参考になると考えられる。
  - （事務局）ドイツの例等も今後の参考にしてみたい。
- （岡田構成員）本ガイドラインは、そもそも生成 AI が使われていない状態を前提として、どのように利活用を推進するかという考え方がベースになっている。そのため、このガイドラインを人間が読み、人間が理解をしたうえで使われる形であると想定している。今後そういった前提が変わってきて、本ガイドラインを生成 AI に読み込ませて活用するという流れとなると考える。ガイドラインの対象である府省庁においても生成 AI に内容を読み込ませ、質問しながらガイドラインを活用するケース等も考えられるが、ガイドラインの使い方が変わることで、新たなリスクが生まれる可能性も考えられる。このあたりについてどのような検討や議論を進めているか。
  - （事務局）現行の調達チェックシートに基づき、調達仕様書が適合しているかについてのチェック等も「源内」を使って実施できており、現行のガイドラインでも生成 AI により適切に活用できるものとなっている。一方、生成 AI を活用する上でハルシネーションのリスクがゼロにならない点は懸念として当然残るため、しっかりと人間の目で確認することは必須である。今後も、機械可読性を意識し、そのような活用方法に対しフレンドリーな形で提供したいと考えている。
  - （岡田構成員）現在は、出力結果に対し人間が責任を持つ整理が明確だが、今後の進展を踏まえて責任が曖昧になる可能性もあるため、引き続き検討いただきたい。

- （北村構成員）国内外における AI の進展は急速であり、生成 AI は「導入段階」から「社会全体で広く活用される段階」へ移行しつつあるとともに、技術の均一化も進みつつある。このような AI 利用のフェーズの変化を踏まえると、従来の導入期を前提とした対応だけでは不十分であり、広範な利用を前提とした新たなフェーズに適したアプローチを検討していくことが重要である。
- （永沼構成員）民間でも同様の課題があるが、CAIO の業務が膨大になる懸念がある。グローバルなシンクタンク等では AI エージェントのガバナンスに関する議論が進んでいるが、今までの AI ガバナンスからリスク統制の方法等も変わってくる認識である。CAIO が見なければならぬものが変わっていく中で、CAIO の意識変革のための取組等は、府省庁内でも今後検討されるのか。
  - （事務局）CAIO 連絡会では、ガイドラインの改定内容や知見の共有を行っている。本日の傍聴でも CAIO が参加しており、こういった CAIO と、CAIO を支える部門がアドバイザリーボードへ参加することにより、キャッチアップをいただいている。AI エージェントのガバナンスについて、政府内でも報告の対象とするだけでなく、あるべき規律の形は諸外国や民間を参考にしていきたい。AI エージェントの活用を進めている府省庁のベストプラクティス等も踏まえながら、適宜府省庁への展開も検討していきたい。
  - （北村構成員）AISI では AI エージェントに関する調査事業を加速しており、来年には AI エージェントに関する評価観点ガイドを公表する予定である。
- （川崎デジタル大臣政務官）資料 1、2とも共通するが、生成 AI のリスクを人間が見る運用が膨大になり、運用が困難になる懸念がある。「源内」を府省庁にカスタマイズして展開していくにあたり、各府省庁の利用実態にあわせ、ガイドラインの記載粒度を高めることが必要になってくるのではないかと。今後、人がガイドラインのルールを全量対応することが負担になるとも考える。例えば、利活用ルールひな形の「要機密情報をプロンプトに入力しない」の件に関しては、最初からプロンプト規制をシステム上で実装するようなことも検討が必要になってくる。デジタル庁が先進的な取組を行っていく必要がある。
  - （鳥澤構成員）いずれは資料 1 の定期報告概要も全自動で作成できるかもしれない。そういった方向も検討してみると良いと思う。
  - （門林座長）説明可能性や可読性向上のため、本会議体での議論を踏まえ、来年度以降の改定で検討していくとよいと考える。
- （柴山構成員）調達チェックシートや契約チェックシートについては事前にコメントした内容も反映いただきありがたい。ガイドラインの容量も膨大であり、現場でのチェック作業も大変だと考える。こうしたチェックの場面で最も参考になるのは過去の前例であると考えため、ユースケースの横展開や情報共有体制をより一層整備できるとよい。
- （門林座長）これにて意見交換を終了する。本日の議論を受けて修正が必要な箇所がある場合は、デジタル庁や、必要に応じて個別の構成員と相談しつつ、座長である私に修正を一任いただきたい。修正の必要があれば、私の方で修正を行い、皆様に修正内容を報告する形で進めさせていただく。

閉会にあたり、松本デジタル大臣より、世界で最も AI 利活用しやすい国を目指して、行政でバランスの取れた AI 利活用のため、ガイドライン改定及び各府省庁での「源内」利活用促進を全速力で進めたい旨の発言があった。

以上