機密性２　政府機関等職員限り

ChatGPT 等の生成 AI の業務利用に関する申合せに関する Q&A

2023 年（令和 5 年）6 月 5 日
AI 戦略チーム事務局

「ChatGPT 等の生成 AI の業務利用に関する申合せ」（以下、「申合せ」という。）に基づく関係省庁における対応を円滑に行うため、申合せの運用に関する関係省庁向けの Q&A を作成する。

今後の運用状況を踏まえ、逐次、本 Q&A を更新することとする。

Ｑ１　生成ＡＩとは何か

Ａ．明確な定義が存在する訳ではないが、「データから学習し、独創的かつ現実的な新しい成果物を生成するＡＩ」といった見解が示されており、例えば、画像を生成できるＡＩの「Stable Diffusion」や、テキストを生成できるＡＩの「ChatGPT」、機械的翻訳を行うＡＩの「DeepL」が該当すると考えられる。明確な定義が存在する訳ではないものの、機械学習や信号処理技術を用いていても、以下のような場合は、生成ＡＩには該当しないと考えられる。

- 予測値等の数値情報しか出力できない場合
- 文章分類等の事前定義されたカテゴリやラベルしか出力できない場合
- 形態素解析や固有表現抽出のような元の文章の一部分を抽出したものしか出力できない場合
- 工場ロボットの運動制御等、デジタル信号を制御するために用いられる場合

Ｑ２　ＡＩ戦略チームに対する報告や了解を求めている趣旨如何

Ａ．昨今のChatGPT等の生成ＡＩを巡る技術革新は、さまざまな利点をもたらす一方、プライバシーや著作権の侵害などの新たな課題が生じるとの見方もある。生成ＡＩを巡る様々な課題や規制の在り方に関しては、国際的にも議論が行われているところ、政府としては、そうした議論の動向を見極めつつ、関係省庁が連携して生成ＡＩに関する実態の把握に努め、適切な措置を講じていく必要がある。

Ｑ２－１　所管の独立行政法人等の取組についても報告や了解の対象となるのか

Ａ．　「政府機関等のサイバーセキュリティ対策のための統一基準」（令和３年度版）（以下「政府統一基準」という。）※の対象となる独立行政法人等についても、申合せの趣旨を踏まえた適切な対応が求められる。ＡＩ戦略チームに対する報告については、例えば、ある独立行政法人における利活用が、所管省庁における対応と同じ範囲であれば、各独法分に関する個別案件毎の一律での報告や了解は不要な場合もあると考える。所管省庁が活用せず、所管の独立行政法人のみが活用する場合など、判断に迷う場合は、個別に相談されたい。

※政府統一基準に係る問合せについては、内閣サイバーセキュリティセンター宛てに相談されたい。

Ｑ３　生成AI機能を有するサービスを業務利用する場合、全て報告を求めるのか

Ａ．今回の申合せは、生成AIの固有のリスクを踏まえ、関係省庁が連携して生成AIに関する実態の把握に努め、適切な措置を講じていくためのものである。そのため、生成AIを業務において活用することで、どのようなリスクが発生するのかを把握し、適切なリスク軽減策を講じることが必要。例えば、関係省庁において、文書生成AIを用いて関係省庁の名において公表する文書を作成する場合は、当該文書の信頼性の確保等の観点から、関係省庁が連携して適切な対応（生成AIの利用状況や、信頼性確保のために講じる措置に係る対外的な説明等）を取ることが必要であり、報告や了解の対象となる。その一方で、例えば、ウェブ会議ツールに用いられるノイズキャンセラー機能については、一般的に、利用者側は実装方式の詳細までは意識しないものの、実装方法によっては、生成AIではないとは言い切ることは困難ではあるが、当該機能を活用して業務を行ったとしても、生成AI固有のリスクは想定しえないことから、報告や了解を求めるものではない。その他にも、例えば、生成AI機能を搭載する「検索エンジン」を業務利用する場合において、報告が必要か否かについても、同様に、生成AI固有のリスクが発生しているか否かの観点から判断していくことになる（現状、Microsoft Bingでは、タブ選択によりチャット機能の利用が可能となっているが、当該機能を利用する場合は報告が必要と考えられる）。なお、申合せに基づく報告の要否に関わらず、当然、政府統一基準に基づく関係省庁における適切な対応は必要。

個別の報告の要否については、本Q&Aを更新することにより、明らかにしていくため、判断に迷う場合は、事務局まで相談されたい。

Ｑ３－１　民間事業者に対する委託事業において、委託事業者が委託事業とは別に、自らの環境下で生成AIの実証を行う場合は報告が必要か

Ａ．報告は不要。なお、行政機関職員が業務として利用する場合、利用を開始する前に報告を求める。

Ｑ４　どの時点で報告が必要なのか

Ａ．申合せに記載の通り、関係省庁におかれては、①約款型外部サービスについては、「利用するにあたって」報告いただきたい。具体的には、関係省庁において、実際に業務において利用する前に報告されたい。②個別契約等、約款型外部サービスでない形態での生成AI利用を検討する場合には、その検討状況を報告いただきたい。組織内の承認（許可等を含む）は、AI戦略チームへの報告の前か否かは問わない。

Ｑ５　具体的な報告方法を教えてほしい

Ａ．以下の方法でAI戦略チーム宛に報告されたい。

１．報告内容

（１）外部サービスの名称、外部サービス提供者の名称、利用目的（業務内容）、取り扱う情報の機密性、利用期間、利用者の範囲、利用申請の許可権限者等。

様式については、関係省庁において、政府統一基準に基づく省内の申請・届出を行う際に用いた書類やファイルを提出いただくことを想定。

（２）生成AIに係る固有のリスクやセキュリティ懸念への対応

関係省庁における申請・届出の際に用いられた様式内に記載されている場合はそれをもって確認。記載されていない場合は、必要に応じて追加説明を求める。

２．報告先

AI戦略チーム事務局

【内閣府CSTI】

担当：根本参事官、河村・鈴木・神野・中村

【デジタル庁】

担当：野崎参事官、上田・磐田・嶋寸・古本

【連絡先】

[redacted]

３．報告期限

毎週金曜日12:00。AI戦略チーム事務局において、とりまとめ、翌週のAI戦略チームに報告し、必要に応じて了解を取る。※必要に応じてAI戦略チームへの出席・説明をお願いする可能性あり。

Ｑ６　これまでの報告事例について、共有して欲しい

Ａ．個別の報告事例における共有可否については、報告を行った関係省庁における判断となる。個別に事務局宛に相談いただきたい。

Ｑ７　今後も、個別の利用毎に報告は必要なのか

Ａ．Ｑ３で記載の通り、今回の申合せは、生成ＡＩの固有のリスクを踏まえ、関係省庁が連携して生成ＡＩに関する実態の把握に努め、適切な措置を講じていくためのもの。そのため、申合せに関する運用状況を踏まえ、本Ｑ&Ａにおいて、個別報告不要な類型を示す等、具体的な報告内容や方法については、随時見直しを行っていく。

Ｑ８　報告内容はＡＩ戦略チームにおいてどのように扱われるのか

Ａ．Ｑ５に記載の通り、毎週金曜日 12:00〆でとりまとめ、ＡＩ戦略チーム事務局において、とりまとめ、翌週のＡＩ戦略チームに報告し、必要に応じて了解を取る。

Ｑ９　報告内容は公表されるのか

Ａ．ＡＩ戦略チームとしては、現時点において、報告内容自体を直ちに公表することは想定していない。そのため、公表有無については、関係省庁において適切に判断されたい。なお、報告があった省庁名については、当該報告をＡＩ戦略チームに行った後に、公表する可能性がある。その場合においても、公表可否については、報告があった省庁に確認を取るものとする。