ChatGPT 等の生成 AI の業務利用に関する申合せ

2023 年（令和 5 年）5 月 8 日
デジタル社会推進会議幹事会申合せ

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。このため、関係省庁における生成 AI の業務利用に関し、次のとおり申し合わせる。

（Ⅰ）約款型外部サービスによる生成 AI の業務利用

生成 AI が現在の ChatGPT のようなサービス形態で提供される場合には、政府統一基準[1]でいうところの「不特定多数の利用者に対して提供する、画一的な約款や規約等への同意のみで利用可能となる外部サービス」（以下「約款型外部サービス」という。）に該当する。

約款型外部サービスでは、セキュリティ対策やデータの取扱いなどについて機関等[2]への特別な扱いを求めることができない場合が多く、必要十分なセキュリティ要件を満たすことが一般的に困難であることから、原則として要機密情報を取り扱うことはできない。

また、要機密情報を取り扱わない場合であっても、機関等においては、リスクを考慮した上で利用可能な業務の範囲をあらかじめ特定し、個々の利用にあたっては、利用手続に従って、利用目的（業務内容）や利用者の範囲などの利用者からの申請内容を許可権限者が審査した上で利用の可否を決定し、その利用状況について管理することが必要である。

組織の承認を得ずに職員等が外部サービスを利用する、いわゆる「シャドーIT」は、規程等に反していることに加えて、誰がどのように使用しているかなどの管理ができなくなるため、要機密情報の漏えい等のリスクを高めることになる。

これらを踏まえ、関係省庁においては、

- 現在の ChatGPT は約款型外部サービスに区分されるサービスであること
- 約款型外部サービスでは、原則として要機密情報を取り扱うことはできないこと
- 要機密情報を含まない場合であっても、利用にあたっては、組織の規程に則り承認を得る手続きが必要であること

について、職員等に対して周知することとする。

---

[1]「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）

[2]「政府機関等のサイバーセキュリティ対策のための統一規範」における「機関等」を指す。

また、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、関係省庁は、約款型外部サービスによる生成 AI を利用するにあたっては、「AI 戦略チーム」に報告することとする。

（２）約款型外部サービスでない形態による生成 AI の業務利用

機関等においては、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も考えられるが、その場合においても、「外部サービスの利用（政府統一基準 4.2 参照）」に係る関連規程に基づく対応が求められる。

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、関係省庁は、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「AI 戦略チーム」に報告し、了解を得ることとする。

（別添）

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）（抜粋）

4.2 外部サービスの利用

4.2.1 要機密情報を取り扱う場合

目的・趣旨

（略） なお、民間事業者等が不特定多数の利用者に対して提供する、画一的な約款や規約等への同意のみで利用可能となる外部サービスでは、セキュリティ対策やデータの取扱いなどについて機関等への特別な扱いを求めることができない場合が多く、要機密情報を取り扱う上で必要十分なセキュリティ要件を満たすことが一般的に困難であることから、原則として要機密情報を取り扱うことはできない。

4.2.2 要機密情報を取り扱わない場合

遵守事項

(1) 外部サービスの利用に係る規定の整備

(a) 統括情報セキュリティ責任者は、以下を含む外部サービス（要機密情報を取り扱わない場合）の利用に関する規定を整備すること。

（ア）外部サービスを利用可能な業務の範囲

（イ）外部サービスの利用申請の許可権限者と利用手続

（ウ）外部サービス管理者の指名と外部サービスの利用状況の管理

（エ）外部サービスの利用の運用手順

(2) 外部サービスの利用における対策の実施

(a) 職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で要機密情報を取り扱わない場合の外部サービスの利用を申請すること。また、承認時に指名された外部サービス管理者は、当該外部サービスの利用において適切な措置を講ずること。

(b) 利用申請の許可権限者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定すること。また、承認した外部サービスを記録すること。