資料３－３

ChatGPT 等の生成 AI の業務利用に関する申合せ（第２版）（案）

2023 年（令和 5 年）X 月 XX 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ため、関係省庁における生成 AI の業務利用に関し、2023 年（令和５年）５月８日に申し合わせた。

これまでの AI 戦略会議及び AI 戦略チームでの議論を踏まえ、各府省庁のセキュリティポリシーに従って個別にリスク管理を行っていることを前提とした上で、次のとおり申し合わせを変更する。なお、政府における検討等今後の取組や利用状況に応じ、適宜見直しを行うものとする。

（１）約款型クラウド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、定型約款や規約等への同意のみで利用可能となるクラウドサービス」(以下「約款型クラウドサービス」という。)に該当する。

約款型クラウドサービスでは、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、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、個々の利用に当たっては、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クラウド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 は約款型クラウドサービスに区分されるサービスであること

[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５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。

・約款型クラウドサービスでは、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、利用に当たっては、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。

なお、各府省庁のセキュリティポリシーに従って個別にリスク管理が行なわれていることを考慮し、要機密情報を含まない情報の取扱いを前提とした、約款型クラウドサービスに該当する生成 AI の利用に当たっては、組織の規程に則り利用承認を得た上で、「AI 戦略チーム」への報告を不要とする。

（2）約款型クラウド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、約款型クラウドサービスの形態ではなく、個別契約等に基づく生成 AI の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、「クラウドサービス（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、約款型クラウドサービスの形態ではなく、個別契約等に基づく生成 AI の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。

また、関係省庁においては、

・サービスにおいて生成 AI を利用していることの明示
・生成 AI の出力結果を二次利用する場合の責任の明確化
・当初は行政職員、自治体職員など対象となる利用者層を限定
・学習に利用するデータ、入力され得るプロンプト、出力結果の社会的影響に係るリスク評価の実施
・入力されたプロンプト及び出力結果のロギングを行った上で、必ず利用者からフィードバックを受ける仕組みを設けること
・一般利用者を対象とする場合は検証段階であることの明示とテスト参加の同意の取得
・上記項目について対応済である旨を、利用計画書に記載し、AI 戦略チームへ提出

について対応し、「AI 戦略チーム」の了解を得ることを前提に、組織の規程に則り利用承認を得た上で、適切なリスク分析を行った一部の機密性２情報まで取り扱うことができるものとする。

なお、各府省庁のセキュリティポリシーに従って個別にリスク管理が行なわれていることを考慮し、要機密情報を含まない情報の取扱いを前提とした、クラウドサービス（約款型クラウドサービスを除く。）に該当する生成 AI の利用に当たっては、組織の規程に則り利用承認を得た上で、「AI 戦略チーム」への報告を不要とする。

（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５年度版）（抜粋）

4.2 クラウドサービス

4.2.1 クラウドサービスの選定（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、定型約款や規約等への同意のみで利用可能となるクラウドサービスでは、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ため、4.2.3「クラウドサービスの選定・利用（要機密情報を取り扱わない場合）」の規定を遵守する必要がある。

4.2.3 クラウドサービスの選定・利用（要機密情報を取り扱わない場合）

遵守事項

(1) 要機密情報を取り扱わない場合のクラウドサービスの利用に係る運用規程の整備

(a) 統括情報セキュリティ責任者は、以下を全て含むクラウドサービス（要機密情報を取り扱わない場合）の利用に関する運用規程を整備すること。

（ア）クラウドサービスを利用可能な業務の範囲

（イ）クラウドサービスの利用申請の許可権限者と利用手続

（ウ）クラウドサービス管理者の指名とクラウドサービスの利用状況の管理

（エ）クラウドサービスの利用の運用規程

(2) 要機密情報を取り扱わない場合のクラウドサービスの利用における対策の実施

(a) 職員等は、要機密情報を取り扱わないことを前提としたクラウドサービスを利用する場合、利用するサービスの定型約款、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利用申請の許可権限者へ要機密情報を取り扱わない場合のクラウドサービスの利用を申請すること。

(b) 利用申請の許可権限者は、職員等による利用するクラウドサービスの定型約款、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の確認結果を踏まえて、クラウド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。

(c) 利用申請の許可権限者は、要機密情報を取り扱わないクラウドサービスの利用申請を承認した場合は、クラウドサービス管理者を指名し、承認したクラウドサービ

スを記録すること。

(d) クラウドサービス管理者は、要機密情報を取り扱わないクラウドサービスを安全に利用するための適切な措置を講ずること。

（様式）利用計画書

報告番号	
報告主体	
初回報告日	
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	
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	

要機密情報の取り扱いに関する確認事項への対応	（はい・いいえ）
・サービスにおいて生成 AI を利用していることの明示 ・生成 AI の出力結果を二次利用する場合の責任の明確化 ・当初は行政職員、自治体職員など対象となる利用者層を限定 ・学習に利用するデータ、入力され得るプロンプト、出力結果の社会影響に係るリスク評価の実施 ・入力されたプロンプト及び出力結果のロギングを行った上で、必ず利用者からフィードバックを受ける仕組みを設けること ・一般利用者を対象とする場合は検証段階であることの明示とテスト参加の同意の取得	
（自由記述欄）	