DeepSeek 等の生成 AI の業務利用に関する注意喚起（事務連絡）

令和７年２月６日
デジタル社会推進会議幹事会事務局

１．令和７年２月３日付で個人情報保護委員会事務局より、DeepSeek 社[1]による生成 AI サービスに関し、同社が公表するプライバシーポリシーについて、中国語及び英語表記のみであることを踏まえ、以下の情報提供が行われております。

① 当該サービスの利用に伴い DeepSeek 社が取得した個人情報を含むデータは、中華人民共和国に所在するサーバに保存されること

② 当該データについては、中華人民共和国の法令が適用されること

＜DeepSeek に関する情報提供＞（令和７年２月３日 個人情報保護委員会事務局）
https://www.ppc.go.jp/news/careful_information/250203_alert_deepseek/

２．生成 AI の業務利用については、「ChatGPT 等の生成 AI の業務利用に関する申合せ」を行っております。

当該申合せにおいては、約款型サービスに関し、原則として要機密情報を取り扱うことはできない旨、明記しております。また、機密情報を取り扱わない場合であっても、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とされています。（別添１）

＜ChatGPT 等の生成 AI の業務利用に関する申合せ（第２版）＞
（2023 年（令和 5 年）9 月 15 日デジタル社会推進会議幹事会申合せ）
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/c64badc7-6f43-406a-b6ed-63f91e0bc7cf/e2fe5e16/20230915_meeting_executive_outline_03.pdf

３．さらに、「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群」においては、要機密情報を取り扱わない場合であっても、例えば、国外にサーバ装置を設置している場合は、現地の法令が適用され、現地の政府等による検閲や接収を受ける可能性があることなどが、利用の可否を判断する際に考慮すべきリスクとして例示されています。（別添２）

[1] Hangzhou DeepSeek Artificial Intelligence Co., Ltd., Beijing DeepSeek Artificial Intelligence Co., Ltd. 及び関連会社

＜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群＞

https://www.nisc.go.jp/policy/group/general/kijun.html

４．加えて、「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」（以下「IT 調達申合せ」という。）においては、政府機関等による情報システム・機器・役務等に関する調達手続に関し、「サプライチェーン・リスクの観点から必要な場合において、内閣サイバーセキュリティセンター及びデジタル庁に対して、講ずべき必要な措置について、原則、助言を求めるものとする」とされており、生成 AI についても IT 調達申合せの対象となります。（別添３）

＜IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ＞

https://www.nisc.go.jp/pdf/policy/kihon-2/IT_moushiawase.pdf

5．各政府機関等におかれては、DeepSeek 等の生成 AI の業務利用に当たっては、調達行為を伴わない場合であってもサービスの利用によって生じるリスクを十分認識の上、IT 調達申合せ等の趣旨も踏まえ、内閣サイバーセキュリティセンター及びデジタル庁に助言を求めた上で適切に判断いただきますようお願いいたします。

（別添１）ChatGPT 等の生成 AI の業務利用に関する申合せ（第２版）＜抜粋＞

2023 年（令和 5 年）9 月 15 日 デジタル社会推進会議幹事会申合せ

（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
- 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。

（別添２）政府機関等の対策基準策定のためのガイドライン（令和５年度版）＜抜粋＞

【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　より抜粋】

○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。

【（解説）遵守事項 4.2.3(1)(a)(ア)「利用可能な業務の範囲」について　より抜粋】

○クラウドサービスの利用において、要機密情報を取り扱わない場合であっても考慮すべきリスクの例には、以下のようなものがある。統括情報セキュリティ責任者は、以下を例とするリスクを受容するか又は低減するための措置を講ずることが可能であるかを十分検討した上で、許可する業務の範囲を決定する必要がある。

- クラウドサービス提供者は、保存された情報を自由に利用することが可能である。また、定型約款、利用規約等でその旨を条件として明示していない場合がある。加えて、クラウドサービス提供者は、利用者から収集した種々の情報を分析し、利用者の関心事項を把握し得る立場にある。
- 政府が利用等することで結果的に国民一般に、安全・安心なサービスであるとして推奨していると受け取られることがある。
- クラウドサービス提供者が国外のデータセンター等にサーバ装置を設置してサービスを提供している場合は、当該サーバ装置に保存されている情報に対し、現地の法令等が適用され、現地の政府等による検閲や接収を受ける可能性がある。
- 情報が改ざんされた場合でも、利用形態によってはクラウドサービス提供者が一切の責任を負わない場合がある。
- 突然サービス停止に陥ることがある。また、その際に預けた情報の取扱いは保証されず、損害賠償も行われない場合がある。定型約款の条項は一般的にサービス提供者に不利益が生じないようになっており、このような利用条件に合意せざるを得ない。また、サービスの復旧についても保証されない場合が多い。
- 保存された情報が誤って消去又は破壊されてしまった場合に、サービス提供者が情報の復元に応じない可能性がある。また、復元に応じる場合でも復旧に時間がかかることがある。
- 情報セキュリティインシデントが発生した際に、機関等に対し必要十分な報告がなされないことがある。
- 定型約款及び利用規約の内容が、クラウドサービス提供者側の都合で利用開始後においても定型約款の変更をすることにより、変更後の定型約款の条項について合意があったものとみなし、個別に相手方と合意をすることなく契約の内容を変更することができる場合がある。
- 情報の取扱いが保証されず、一旦記録された情報の確実な消去は困難である。

・ 利用上の不都合、不利益等が発生しても、サービス提供者が個別の対応には応じない場合が多く、万が一対応を承諾された場合でも、その対応には時間を要することが多い。

（別添３）

IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ＜抜粋＞
（平成 30 年 12 月 10 日 関係省庁申合せ）

１．目的

複雑化・巧妙化しているサイバー攻撃に対して、政府機関等におけるサイバーセキュリティ対策を一層向上させるためには、従来行われている取組に加え、より一層サプライチェーン・リスクに対応するなど、国の行政機関・独立行政法人・サイバーセキュリティ基本法に定める指定法人（以下「政府機関等」という。）の重要業務に係る情報システム・機器・役務等の調達におけるサイバーセキュリティ上の深刻な悪影響を軽減するための新たな取組が必要である。そのため、政府機関等において特に防護すべき情報システム・機器・役務等に関する調達の基本的な方針及び手続について、次のとおり関係省庁で申し合わせ、講ずべき必要な措置について明確化を図る。

２．対象とする調達

別紙１に掲げる政府機関等において、別紙２に掲げる情報システム・機器・役務等の調達のうち、別紙３に掲げる重要性の観点から、より一層サプライチェーン・リスクに対応することが必要であると判断されるものについては、内閣サイバーセキュリティセンター及びデジタル庁と協議のうえ、本申合せに基づき必要な措置を講じる対象とする。なお、別紙２の役務には、別紙３に掲げるシステムの開発、保守・運用、及び当該システムで扱われるデータの管理・処理の外部委託等が含まれる。

（略）

５．調達手続

政府機関等は、第２項で特定した調達を実施する際は、各政府機関等が遵守すべき調達に関する法令等に基づき契約手続を進めるに当たり、調達する情報システム・機器・役務等の提供事業者及びその製品並びに役務について、サイバーセキュリティ確保の観点から、仕様条件の決定、製品及び役務を提供する事業者の選定のために必要な情報を、Request for Information（RFI）及び Request for Proposal（RFP）等により取得することとする。なお、再委託先等の情報についても取得の対象に含まれる。

政府機関等は、調達手続のうち、サプライチェーン・リスクの観点から必要な場合において、内閣サイバーセキュリティセンター及びデジタル庁に対して、講ずべき必要な措置について、原則、助言を求めるものとする。

（略）