資料１－１

公表資料

個人情報保護委員会
Personal Information Protection Commission

News Release

生成 AI サービスの利用に関する注意喚起等について

令 和 ５ 年 ６ 月 ２ 日

我が国において、現在、生成 AI サービス（質問・作業指示（プロンプト入力）等に応えて文章・画像等を生成する AI を利用したサービス）が普及していることを踏まえ、当委員会として、別添１のとおり、生成 AI サービスの利用に関する注意喚起等を行うこととしました。

なお、生成 AI サービスである ChatGPT を開発・提供する OpenAI, L.L.C.及び OpenAI OpCo, LLC に対しては、別添２に記載の概要のとおり、注意喚起を行いました。

【別添１】生成 AI サービスの利用に関する注意喚起等
【別添２】OpenAI に対する注意喚起の概要

【連絡先】
個人情報保護委員会事務局
吉屋、松本、福本
電話：03-6457-9763

（別添１）

生成 AI サービスの利用に関する注意喚起等

令 和 ５ 年 ６ 月 ２ 日
個 人 情 報 保 護 委 員 会

生成 AI サービス（質問・作業指示（プロンプト入力）等に応えて文章・画像等を生成する AI を利用したサービス）については、「G7 広島首脳コミュニケ」（令和５年５月 20 日）において、「我々が共有する民主的価値観に沿った、信頼できる人工知能（AI）という共通のビジョンと目標を達成するために、包摂的な AI ガバナンス及び相互運用性に関する国際的な議論を進める。」、「国や分野を超えてますます顕著になっている生成 AI の機会及び課題について直ちに評価する必要性を認識し、（略）」とされているとおり、世界的な関心が高まるとともに、利活用の機会及び課題の両面からの評価が求められている。その一環として、例えば、個人情報の適正な取扱いやプライバシー保護の観点からの考慮の重要性も指摘されている。これらの経緯及び状況を踏まえ、各国において対応を検討する動きがある。

我が国においても、現在、生成 AI サービスが普及していることを踏まえ、当委員会として、個人情報の適正な取扱いによる個人の権利利益の確保の要請と、新たな技術に基づく公共的な利益（イノベーションの促進、生産性の向上、教育効果の向上、気候変動問題等の国際社会の課題の解決等を通じて、多様な社会的・経済的利益の増進に寄与する可能性）の要請とのバランスに留意しつつ、生成 AI サービスの利用に関する注意喚起等を行うこととした。

下記（１）及び（２）において、個人情報取扱事業者及び行政機関等[1]における生成 AI サービスの利用に際しての個人情報の取扱いに関する注意点を取りまとめたので、個人情報取扱事業者及び行政機関等において、生成 AI サービスを利用する際には、これらも参考に、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）の規律に従って、個人情報を適正に取り扱っていただきたい。

また、下記（３）において、一般の利用者における生成 AI サービスの利用に際しての個人情報の取扱いに関する留意点を取りまとめたので、参考としていただきた

[1] 行政機関、地方公共団体の機関（議会を除く。）、独立行政法人等（個人情報保護法別表第２に掲げる法人を除く。）及び地方独立行政法人（地方独立行政法人法第 21 条第１号に掲げる業務を主たる目的とするもの又は同条第２号若しくは第３号チに掲げる業務を目的とするものを除く。）をいう。以下、本文において同じ。

い。

なお、生成 AI サービスの利用に関する注意喚起等と併せて、生成 AI サービスである ChatGPT を開発・提供する OpenAI, L.L.C.及び OpenAI OpCo, LLC（以下、併せて「OpenAI」という。）に対しては、別添２のとおり、要配慮個人情報の取得及び利用目的の通知等についての注意喚起を行ったことに加え、今後、新たな懸念事項を認識した場合には、必要に応じ追加的な対応を行うとしたところである。

当委員会は、個人情報の適正な取扱いが確保され、個人の権利利益が保護されるよう、生成 AI サービスの開発・利用状況を引き続き注視していく予定であり、今後、追加の注意喚起等を実施する可能性もある点に留意されたい。

（１）　個人情報取扱事業者における注意点

① 個人情報取扱事業者が生成 AI サービスに個人情報を含むプロンプトを入力する場合には、特定された当該個人情報の利用目的を達成するために必要な範囲内であることを十分に確認すること。

② 個人情報取扱事業者が、あらかじめ本人の同意を得ることなく生成 AI サービスに個人データを含むプロンプトを入力し、当該個人データが当該プロンプトに対する応答結果の出力以外の目的で取り扱われる場合、当該個人情報取扱事業者は個人情報保護法の規定に違反することとなる可能性がある。そのため、このようなプロンプトの入力を行う場合には、当該生成 AI サービスを提供する事業者が、当該個人データを機械学習に利用しないこと等を十分に確認すること。

（２）　行政機関等における注意点

① 行政機関等が生成 AI サービスに個人情報を含むプロンプトを入力する場合には、特定された当該個人情報の利用目的のための必要最小限の利用又は提供であることを十分に確認すること。

② 行政機関等が、生成 AI サービスに保有個人情報を含むプロンプトを入力し、当該保有個人情報が当該プロンプトに対する応答結果の出力以外の目的で取り扱われる場合、当該行政機関等は個人情報保護法の規定に違反することとなる可能性がある。そのため、このようなプロンプトの入力を行う場合には、当該生成 AI サービスを提供する事業者が、当該保有個人情報を機械学習に利用しないこと等を十分に確認すること。

（３）　一般の利用者における留意点

① 生成 AI サービスでは、入力された個人情報が、生成 AI の機械学習に利用されることがあり、他の情報と統計的に結びついた上で、また、正確又は不正確な内容で、生成 AI サービスから出力されるリスクがある。そのため、生成 AI

サービスに個人情報を入力等する際には、このようなリスクを踏まえた上で適切に判断すること。

② 生成 AI サービスでは、入力されたプロンプトに対する応答結果に不正確な内容が含まれることがある。例えば、生成 AI サービスの中には、応答結果として自然な文章を出力することができるものもあるが、当該文章は確率的な相関関係に基づいて生成されるため、その応答結果には不正確な内容の個人情報が含まれるリスクがある。そのため、生成 AI サービスを利用して個人情報を取り扱う際には、このようなリスクを踏まえた上で適切に判断すること。

③ 生成 AI サービスの利用者においては、生成 AI サービスを提供する事業者の利用規約やプライバシーポリシー等を十分に確認し、入力する情報の内容等を踏まえ、生成 AI サービスの利用について適切に判断すること。

以　上

（別添２）

OpenAI に対する注意喚起の概要

令 和 ５ 年 ６ 月 ２ 日
個 人 情 報 保 護 委 員 会

当委員会は、令和５年６月１日付けで、OpenAI, L.L.C. 及び OpenAI OpCo, LLC に対し、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「法」という。）第 147 条の規定に基づき、下記概要のとおり、注意喚起を行った。

なお、本注意喚起は、当委員会が現時点で明確に認識した懸念事項を踏まえたものであり、今後新たな懸念事項を認識した場合には、必要に応じて、追加的な対応を行う可能性がある。

記

１　要配慮個人情報の取得

あらかじめ本人の同意を得ないで、ChatGPT の利用者（以下「利用者」という。）及び利用者以外の者を本人とする要配慮個人情報を取得しないこと（法第 20 条第２項各号に該当する場合を除く。）。

特に、以下の事項を遵守すること。

（１）機械学習のために情報を収集することに関して、以下の４点を実施すること。

①　収集する情報に要配慮個人情報が含まれないよう必要な取組を行うこと。

②　情報の収集後できる限り即時に、収集した情報に含まれ得る要配慮個人情報をできる限り減少させるための措置を講ずること。

③　上記①及び②の措置を講じてもなお収集した情報に要配慮個人情報が含まれていることが発覚した場合には、できる限り即時に、かつ、学習用データセットに加工する前に、当該要配慮個人情報を削除する又は特定の個人を識別できないようにするための措置を講ずること。

④　本人又は個人情報保護委員会等が、特定のサイト又は第三者から要配慮個人情報を収集しないよう要請又は指示した場合には、拒否する正当な理由がない限り、当該要請又は指示に従うこと。

（２）利用者が機械学習に利用されないことを選択してプロンプトに入力した要配慮個人情報について、正当な理由がない限り、取り扱わないこと。

２　利用目的の通知等

利用者及び利用者以外の者を本人とする個人情報の利用目的について、日本語

を用いて、利用者及び利用者以外の個人の双方に対して通知し又は公表すること。

以　上

個人情報の保護に関する法律（平成十五年法律第五十七号）（抜粋）

（１条　一　目的）

この法律は、デジタル社会の進展に伴い個人情報の利用が著しく拡大していることに鑑み、個人情報の適正な取扱いに関し、基本理念及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め、国及び地方公共団体の責務等を明らかにし、個人情報を取り扱う事業者及び行政機関等についてこれらの特性に応じて遵守すべき義務等を定めるとともに、個人情報保護委員会を設置することにより、行政機関等の事務及び事業の適正かつ円滑な運営を図り、並びに個人情報の適正かつ効果的な活用が新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の**個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的**とする。

（18 条 1 項　一　利用目的による制限）

個人情報取扱事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。

（20 条 2 項　一　要配慮個人情報の取得）

個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ**本人の同意を得ないで、要配慮個人情報を取得してはならない**。

一　法令に基づく場合

二　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

…（以下略）

（21 条 1 項　一　取得に際しての利用目的の通知等）

個人情報取扱事業者は、個人情報を**取得した場合**は、あらかじめその利用目的を公表している場合を除き、**速やかに、その利用目的を**、本人に通知し、又は**公表**しなければならない。

（27 条 1 項　一　第三者提供の制限）

個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。

一　法令に基づく場合

二　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

…（以下略）

（61 条 1 項　一　個人情報の保有の制限等）

行政機関等は、個人情報を保有するに当たっては、法令（条例を含む。…）の定める所掌事務又は業務を遂行するため必要な場合に限り、かつ、その利用目的をできる限り特定しなければならない。

（69 条 1 項・2 項　一　利用及び提供の制限）

行政機関の長等は、法令に基づく場合を除き、利用目的以外の目的のために保有個人情報を自ら利用し、又は提供してはならない。

2　前項の規定にかかわらず、行政機関の長等は、次の各号のいずれかに該当すると認めるときは、利用目的以外の目的のために保有個人情報を自ら利用し、又は提供することができる。ただし、保有個人情報を利用目的以外の目的のために自ら利用し、又は提供することによって、本人又は第三者の権利利益を不当に侵害するおそれがあると認められるときは、この限りでない。

一（以下略）

G7 データ保護・プライバシー機関ラウンドテーブル会合

生成 AI に関する声明

1. 我々、G7 データ保護・プライバシー機関（DPA）は、データ保護・プライバシーの観点から、生成 AI 技術の最近の動向及び課題について議論するために会合した。

2. 生成 AI 技術の急速な開発及び導入、世界中でその利用の広範な普及、並びに様々な分野での採用が進む中、我々は、生成 AI が適切に開発されて規制されなければ、プライバシー・データ保護、その他基本的人権に対してリスク及び潜在的な損害をもたらす可能性があるとの懸念が高まっていることを認識する。この点に関して、我々は、AI 関連の法、規則、政策及び基準が「人間中心であり、人権と基本的自由の保護、プライバシーと個人データの保護を含む民主的価値に基づくべきである」という立場を強化した 2023 年 4 月の G7 デジタル・技術閣僚宣言を歓迎する。

3. 我々は、様々な管轄区域が AI に特化した法律及び政策の開発を続けているが、現行法が生成 AI 製品及び利用に適用されることに留意する。

4. 我々は、生成 AI ツールに関連して、プライバシー・データ保護のリスクが生じる可能性のある主要な分野の懸念に注意を促すものとする。同分野には、以下が含まれるが、これらに限定されるものではない。
   - 以下の事項に関連した、個人情報の処理、特に、未成年者・子どもの個人情報の処理に関する法的権限
     - 生成 AI モデルの訓練、検証及びテストに利用されるデータセット
     - 個人による生成 AI ツールとの対話
     - 生成 AI ツールによって生成されたコンテンツ
   - 以下を目的とした脅威及び攻撃から保護するための安全保護措置
     - 生成 AI モデルを逆転させ、モデル訓練に利用されたデータセット内において当初処理された個人情報を抽出又は再現すること
     - 他のプライバシー・データ保護要件の遵守を促進するために設計された措置の効果を失わせること
   - 生成 AI ツールによって生成された個人情報が以下のとおりであることを確保するための軽減措置及びモニタリング措置

    - 正確、完全、かつ最新であること
    - 差別的、違法な、その他の不当な影響を受けないこと
- 生成 AI ツールの運用において、公開性・説明可能性を促進する透明性に関する措置、特に、当該ツールが個人に関する意思決定やその支援を行うために利用される場合の透明性に関する措置
- 生成 AI ツールのプライバシー・データ保護要件の遵守を評価するための、開発のライフサイクルを通じた技術文書の作成
- これらのシステムによる影響を受ける個人、又はこれらのシステムと対話を行う個人が、生成 AI ツールに関連して、以下に関する権利行使を確保するための技術的及び組織的措置
    - 自己の個人情報へのアクセス
    - 不正確な個人情報の修正
    - 自己の個人情報の削除
    - 重大な影響を及ぼす自動化された決定のみに従うことの拒否
- AI のサプライチェーンにおいて、主体間の適切な水準の責任を確保する説明責任の措置。特に、生成 AI モデルが相互に構築される場合の説明責任の措置
- 特定されたタスクを遂行するために必要な範囲にのみ、個人データの収集を制限すること

5. 我々は、G7 内の最近の動向に留意する。特に、我々は、イタリアのデータ保護機関（Garante)が、現在も継続中の調査活動の枠組みの中で、一般データ保護規則（GDPR）及びその国内法に違反する可能性があるため、生成 AI を利用するサービスをイタリア国内で一時的に停止したが、イタリア当局による命令に従って当該サービスに対する透明性及び個人の権利において改善が実施された後、その停止が解除されたことを想起する。我々は、テクノロジー企業が法的要件及び DPA のガイダンスに細心の注意を払い、適切な場合には、テクノロジー企業と DPA の間で緊密なコミュニケーションを図ることが、プライバシーその他基本的人権の認識・保護を確保するため、生成 AI の製品及びサービスに関する責任ある設計、開発及び導入に寄与することを強調する。さらに、以下のような G7 DPA による様々な継続中の行動に注目する。
    - 各国法制に基づいて生成 AI の調査を行うこと及び規制上の通知を発出すること
    - 専門のタスクフォースなどを通じ、あり得る執行活動に関する協力及び情報共有を促進すること

- データ保護・プライバシー遵守のためのベストプラクティスに関するガイダンスなど、AI に関する情報を提供すること
- 規制サンドボックスによることを含め、革新的な AI ベースのプロジェクト・主体を支援すること

6. 開発者・提供者は、「プライバシー・バイ・デザイン」の考えに基づき、生成 AI 技術を利用する新たな製品及びサービスに関する設計、構想、運用及び管理にプライバシーを組み込み、プライバシー影響評価において行った自らの選択と分析について文書化すべきである。特に、開発者・提供者は、既存の法を遵守しなければならず、また、データ最小化、データ内容、目的明確化、利用制限、安全保護措置、透明性、個人データの収集及び利用について情報の提供を受ける権利を含むデータ主体の権利、並びに、説明責任など、適用可能であり国際的に遵守されているデータ保護・プライバシーの主要原則を遵守すべきである。また、開発者・提供者は、そのシステムの導入者・採用者もデータ保護・プライバシーの義務を遵守することができるようにすることを確保するための措置を講じるべきである。

7. G7 DPA は、倫理的、法的、社会的及び技術的観点から、生成 AI に関連した個人データ保護の課題について、さらなる議論及び連携が必要であることに同意し、G7 DPA ラウンドテーブルの下、先端技術作業部会及び執行協力作業部会において、生成 AI に関連するプライバシー保護の最善の方法を引き続き探求する。また、我々は、他の国際フォーラムで行われる生成 AI に関する議論に貢献し、データ保護・プライバシーの課題に細心の注意を払う必要性を強調する。