【経営】広報パンフレット「生成 AI サービスの利用に関する注意喚起」を掲載

個人情報保護委員会から、広報パンフレット「生成 AI サービスの利用に関する注意喚起」を掲載したとのお知らせがありました。現在、生成 AI サービスが普及し、利用者が急増しています。生成 AI サービスは、誰でも手軽に使うことができ、様々な情報を入手できるようになる一方で、気付かないうちに個人情報保護法に違反してしまう可能性があります。このパンフレットでは、利用者（個人情報取扱事業者及び行政機関等）にどのような規律が課されるのかなどが紹介されています。

■生成 AI サービスの利用に関する注意喚起
－個人情報が AI の学習データとして利用されていませんか？－

現在、生成 AI サービスが普及し、利用者が急増しています。生成 AI サービスは、誰でも手軽に使うことができ、様々な情報を入手できるようになる一方で、気付かないうちに個人情報保護法に違反してしまう可能性があります。

入力する情報が、生成 AI サービスの提供者において AI の学習データとして利用されることが予定されている場合には、利用者（個人情報取扱事業者及び行政機関等）には以下の規律が課されます。このため、利用規約を確認するなどした上でサービスを利用するようにしてください。

〇個人情報取扱事業者（個人情報データベース等を事業の用に供している者）に対する規律
個人データを第三者に提供する場合は、原則として、あらかじめ本人の同意を得なければなりません（個人情報保護法第 27 条、第 28 条）。

〇行政機関等に対する規律
保有個人情報を利用、提供する場合は、原則として、特定された利用目的のために利用、提供しなければなりません（個人情報保護法第 69 条）。

※生成 AI サービスの利用者が入力した情報について、生成 AI サービスの提供者が自らの AI の精度向上等のために学習データとして利用することとしている場合に、利用者が個人データもしくは保有個人情報を入力すると、利用者から提供者に対し、個人データもしくは保有個人情報を提供したことになります。

※生成 AI サービスを利用する際には、上記の点以外にも、特定された利用目的の達成に必要な範囲内で個人情報を取り扱う等、個人情報保護法の規律に従って、個人情報を適正に取り扱っていただく必要があります。詳しくは、個人情報保護委員会 HP「生成 AI サービスの利用に関する注意喚起等について」（ https://www.ppc.go.jp/news/careful_information/230602_AI_utilize_alert/ ）を確認してください。

■生成 AI サービスの利用に関する注意喚起等について
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
https://www.ppc.go.jp/files/pdf/230602_alert_generative_AI_service.pdf

【下記は抜粋です】
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。

※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。

【別添２】OpenAI に対する注意喚起の概要
https://www.ppc.go.jp/files/pdf/230602_alert_AI_utilize.pdf

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。

詳しくは、こちらをご覧ください。

参照ホームページ[個人情報保護委員会]
https://www.kaiketsu-j.com/compliance/5207/