生成 AI サービスに関する個人情報保護委員会からの注意喚起と実務への影響

2023 年 6 月 5 日

弁護士　中井　杏

＜目次＞

1. 生成 AI サービスの利用に関する注意喚起

2023 年 6 月 2 日、個人情報保護委員会が生成 AI サービスの利用に関する注意喚起等を行ったことが公表されました。

本注意喚起は、あくまでも個人情報を取り扱う際の注意喚起が行われているものであり、具体的な法違反が指摘されているわけではありませんが、生成 AI サービスを利用する企業や、機械学習を行う企業が留意すべき点が指摘されています。

本ニューズレターでは、本注意喚起の概要と実務への影響について述べます。

2. 生成サービス利用時における注意点

(1)利用目的の範囲内で利用すること

本注意喚起では、生成サービス利用者に対し以下の注意喚起がなされています。

「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。」

生成 AI サービスに個人情報を含むプロンプトを入力し、個人情報としての回答を得る場合、利用目的を特定する必要があります（個人情報保護法（以下「法」といいます。）17 条 1 項）。また、既に取得した個人情報をプロンプトとして入力する場合、取得時に特定された利用目的の達成に必要な範囲でなければなりません。本注意喚起では、このことが確認的に指摘されています。

個人情報をプロンプトとして入力する目的が、利用目的の範囲外の場合は、仮名加工情報制度を用いて利用目的を変更することも考えられます。仮名加工情報制度を活用する方法については、「ChatGPT と仮名加工情報・個人情報」をご参照ください。

(2)生成 AI サービス提供事業者が機械学習に利用しないことの確認

生成 AI サービス提供事業者におけるプロンプトの利用態様に関し以下の注意喚起がなされています。

「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。」

個人情報保護法のいずれの規定に違反することとなるかは明らかにされていませんが、少なくとも第三者提供の規制（法 27 条）、外国にある第三者への提供の制限（法 28 条）を念頭においた注意喚起だと考えられます。

個人情報保護法上「提供」とは、個人データ等を自己以外のものが利用可能な状態に置くことをいうとされております（通則ガイドライン 2-17）。

したがって、本注意喚起の記載を踏まえると、少なくとも、AI サービス提供事業者が、プロンプトとして入力された個人データを学習用データセットに加工して機械学習に利用している場合には、サービス利用者から AI サービス提供事業者への個人データの「提供」と評価される可能性が高いと考えられます。そこで、AI サービス提供事業者がプロンプトとして入力された個人データを機械学習のために利用しないような設定を行っているか、改めて確認しておくことが重要です。

AI サービス提供事業者へ個人データを「提供」していることとなった場合、Chat-GPT は米国 OpenAI 社が提供するサービスであるため、①法 28 条に基づき本人の同意を取得するか、②法 27 条 5 項 1 号の委託と法 28 条の基準適合体制（※）に関する対応（基準適合体制の確保や情報提供等）を行うことが考えられます。

ただし、「個人データ」を提供していない場合であっても、安全管理措置（法 23 条）として外的環境の把握を行う義務が生じます。

詳細については、「ChatGPT の利用について法務が検討すべき 3 つのポイント」をご参照ください。

※個人データの取扱いについて個人情報保護法第 4 章第 2 節（法 17 条～40 条）の規定により個人情報取扱事業者が講ずべきこととされている措置に相当する措置を継続的に講ずるために必要なものとして個人情報保護委員会規則で定める基準に適合する体制を整備していること

3. 機械学習を行う場合への示唆

生成 AI サービス提供事業者に対しては、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ないことが注意喚起されています。

また、機械学習のために情報を収集する際、「①収集する情報に要配慮個人情報が含まれないように必要な取り組みを行うこと、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」等が指摘されています。

要配慮個人情報を取得する場合、法 20 条 2 項各号の例外に当たる場合を除き、あらかじめ本人の同意を得る必要があります（法 20 条 2 項）。要配慮個人情報の取得が問題となる場合としては、機械学習のための情報をクローリングにより収集する場合や、機械学習のために生成 AI サービスにプロンプトとして入力された情報を用いる場合など、収集する情報をコントロールできない場合が考えられます。

個人情報を含む情報がインターネット等により公にされている場合については、当該情報を単に画面上で閲覧する場合は、個人情報を取得したとは解されませんが、当該情報を転記の上、検索可能な状態にしている場合や、当該情報が含まれるファイルをダウンロードしてデータベース化する場合は個人情報を取得したと解し得るとされています（「個人情報の保護に関する法律についてのガイドライン」に関する Q&A4-4）。

本注意喚起では、収集する情報に要配慮個人情報が含まれないように必要な取り組みを行ったうえ、少なくとも学習用データセットに加工する前までに、要配慮個人情報を削除するか、特定の個人を識別することができないようにすることが求められています。

この点は、生成 AI サービス提供事業者のみならず、機械学習のための情報を収集し学習用データセットを作

成する事業者においても留意する必要があると考えられます。

また、本注意喚起では、生成 AI サービス提供事業者に対し、利用者及び利用者以外の者を本人とする個人情報について、日本語で利用目的を通知又は公表することを求めています。個人情報保護委員会が生成 AI サービス事業者に対し、どのような利用目的を特定することを求めているかは、今後も注目する必要があります。

関連セミナー

U&P リーガルセミナー「ChatGPT の利用について法務が検討すべきこと」（2023 年 5 月 19 日&アーカイブ配信）

関連記事

ニューズレター「ChatGPT をはじめとする生成 AI を利用する際の法的論点」
特集記事「ChatGPT の利用について法務が検討すべき 3 つのポイント」
特集記事「ChatGPT と仮名加工情報・個人情報」

以 上