今話題のChatGPT等 生成系AI利用時の注意点

損害保険ジャパン株式会社
ＳＯＭＰＯひまわり生命保険株式会社

０．生成系AIとは？

生成系ＡＩとは、音声入力やテキスト入力等をＡＩが認識して、あたかも人間を相手にしているかのように文章等を生成して応答するテクノロジーのことを指します。
生成系ＡＩは、インターネット上にある膨大なデータを基に回答を行うため、高い精度の回答をすることが可能であり、文章やプログラムの作成に要する時間を驚くほど短縮することができます。

【生成系AIの種類】
テキスト生成系：ChatGPT、BingAI、Bard
画像生成系：Midjourney、Stable Diffusion
動画生成系：Gen-2　　など

便利な反面、**注意を怠ると法的なトラブルや情報漏えい等の問題が生じる可能性があります。**
下記のリスクを確認のうえ、安全・適切な利用を心掛けてください。

１．情報漏えいのリスク

個人情報や会社の機密情報等の入力は厳禁！！

ChatGPT等の生成系ＡＩは、入力された内容を学習データとして蓄積・活用します。そのため、個人情報や機密情報を入力した場合、その内容が第三者の質問の回答に利用される可能性があります。
無断で個人情報を入力することは、個人情報の第三者提供にあたり、個人情報保護法違反や個人情報漏えいに繋がる危険性があります。
また、Google翻訳などの自動翻訳サービスやSNS利用時においても、同様のリスクが発生する可能性があるため、注意が必要です。

【ご参考】個人情報取扱事業者等が生成AIサービスを利用する際の個人情報の取扱いに関する注意事項が記載されています。
・一般社団法人日本ディープラーニング協会
　生成AIの利用ガイドライン
・個人情報保護委員会　令和5年6月2日付　注意情報
　生成AIサービスの利用に関する注意喚起等

２．正確性・適切性のリスク

回答内容の正確性や適切性の確認が必要です！！

生成系ＡＩは、回答内容の正確性については保証されていません。ＡＩが利用する情報が最新でない場合や、誤った情報を利用している場合があります。また、質問の仕方で回答が異なったり、事実と異なる回答をする場合があります。
そのため、生成系ＡＩの回答内容をそのまま鵜呑みにせず、**自分自身で情報の正確性や適切性を確認することが不可欠です**。

３．法令違反等のリスク

法令や利用規約の確認・遵守が必要です！！

生成系ＡＩの多くは、インターネット上のデータを基に文章やプログラムを生成するため、意図せず他人の著作物を模倣してしまい、生成された文章が盗作と見做されるリスクがあります。また、１．にあるような個人情報の入力に起因するプライバシー侵害のリスクもあり、**場合によっては、法令違反（個人情報保護法、著作権保護法、知的財産権やプライバシーの侵害等）となり、罰せられる可能性があります。**
そのため、対象の生成系ＡＩの利用規約を利用前にしっかりと理解するとともに、各種法令に則ったうえで、正しく利用してください。

生成系 ＡＩに限らず 、無料で利用できる Web サービスに関しては、利用者がそのリスクや注意点を理解して利用することが求められています。
便利なテクノロジーが生み出され生活が豊かになる一方で、利用する我々が注意しなければならない点も増えるということを理解しておく必要があります。

【Web サービス例】

Web 検索 ：Google 、Bing、Yahoo！
翻訳ツール ：DeepL、Google 翻訳
音声アシスタント ：Alexa、Siri、Cortana
開発支援 ：GitHub、GitHub Copilot　　など