【社内・代理店限】

情報セキュリティ

生成AIの利用に関する
コンプライアンス上の注意点

【研修について】

・本研修の目安時間は、１５分間です。
・講師の指示に従って、本資料を読み進めてください。
（勝手に本資料を読み進めないでください。）

【本研修の目的】

・隣の人や、後ろの人と**意見交換をしながら**、学ぶことを
目的としています。積極的に発言しましょう。

当資料は、2023年8月時点の情報をもとに記載しています。

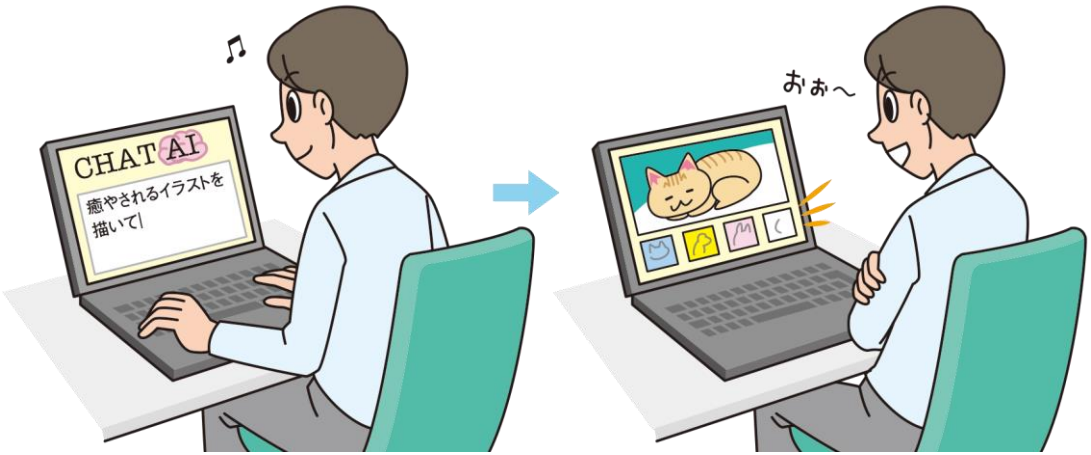
生成AIとは

「生成AI」とは、「質問や作業指示等に応え、画像や文章、音楽、映像、プログラム等の多様なコンテンツを生成するAI※」のことをいいます。

※:「生成AIの活用について」（地上放送課 衛星・地域放送課：総務省webサイト）

■生成AIの代表的なサービス

- ChatGPT（文章生成AI）
- DALL-E（画像生成AI）



生成AIの大きな特徴は、日常会話のような平易な言葉で指示ができる点です。プログラミングなどの専門知識がなくても、生成AIでコンテンツを生み出すことができます。今後はOS、オフィスソフト、検索エンジンにも組み込まれる見通しで、より身近な存在になっていくことが考えられます。

生成AIを業務で利用する際のリスクは？

広告部のAさんは、未発表の新商品に関するプレゼンテーション資料を作成することになりました。Aさんは、生成AIを使って資料を作成しようと思い、利用する上で「手軽に使えて便利そうだけど、何か注意点はあるのかな」と、考えました。

Q1 生成AIを業務で利用するにあたっては、どのようなリスクがあるでしょうか？

A 1

生成AIを利用するにあたってのリスクには、次のようなものがあります。

① 情報が漏えいするリスク

② 誤情報が出力されるリスク

③ 生成された成果物が他者の著作権を侵害するリスク

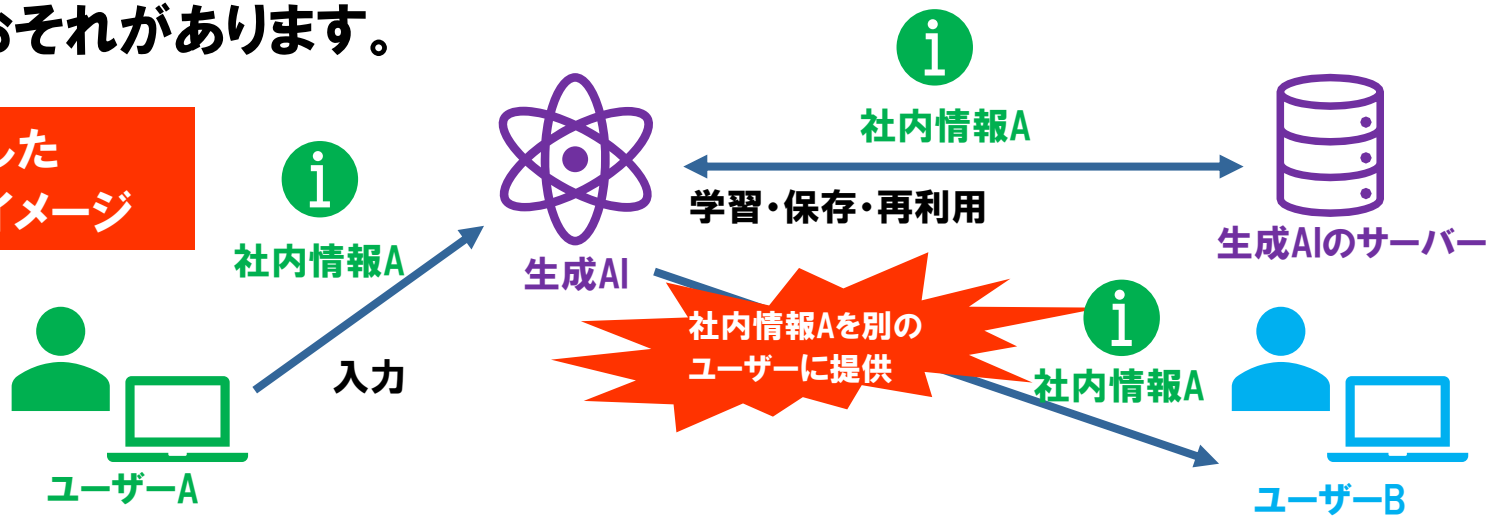
これらの点に十分注意して利用しましょう。

【社内・代理店限】

リスク①：情報が漏えいするリスク

たとえばChatGPTの場合、アプリ以外から入力された情報はサービスの開発や改善に使用される可能性があることが利用規約に明記されています。特に、機密情報や顧客情報を入力し、それが漏えいすれば、社内の問題にとどまらない大きな問題になるおそれがあります。

生成AIに入力した情報の漏えいイメージ



■情報漏えいに関する事例

ある企業の従業員がChatGPTに社外秘情報をアップロードしたことが発覚。データは外部サーバーに保存されるため回収・削除が難しく、他のユーザーに開示されてしまうおそれがあるとされている。同社は、生成AIの利用を原則禁止とした。

【社内・代理店限】

リスク②：誤情報が出力されるリスク

生成AIによる出力情報には、誤情報が含まれることが指摘されています（2023年10月時点）。したがって、情報の正確性を検証する必要があります。

■誤情報の出力例

質問	生成AIによる回答
日本の下請法における「買いたたき」について教えてください。	日本の下請法（特定労働者派遣事業における派遣労働者の待遇の向上等に関する法律）における「買いたたき」は、派遣先の企業が派遣労働者の労働条件を適正に保護し、搾取を防ぐための規定です。（後略）

下請法の正式名称は「下請代金支払遅延等防止法」です。また、「特定労働者派遣事業における派遣労働者の待遇の向上等に関する法律」という法律は存在しません。しかし、情報はもっともらしく提供されるため、事実を知らなければ信じてしまうかもしれません。

■誤情報の出力に関する事例

米国の弁護士が裁判所に提出した書類に実在しない判例が含まれていた。弁護士は、ChatGPTで判例を調べており、ChatGPTが誤情報を生成するとは思わなかったと語った。裁判所は、弁護士が文書の正確性についての責任を放棄したと判断し、5000ドル（約72万円）の支払いを命じた。

リスク③：生成された成果物が他者の著作権を侵害するリスク

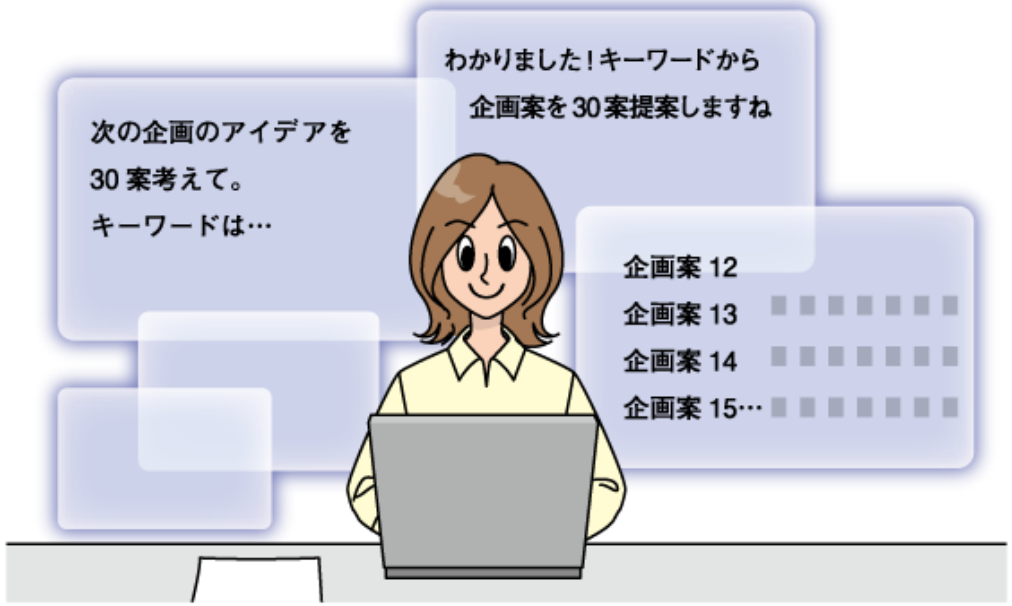
生成された文章や画像が他者の著作物に類似している場合、著作権法上の問題が生じるおそれがあります（著作権侵害となるか否かは、人がAIを利用せず絵を描いた場合などの、通常の場合と同様に「類似性」および「依拠性」によって判断されます）。
AIに生成させた著作物は参考するにとどめ、公表する著作物は人間の手で作成しましょう。

■参考
生成AIが生成したものの著作権については議論されている最中です。
文化庁は2023年6月時点での見解を公表しています。
「ＡＩと著作権」（文化庁）
https://www.bunka.go.jp/seisaku/chosakuken/pdf/93903601_01.pdf

生成AIは利用しない方がいい？

生成AIの利用には、情報漏えい、誤情報の出力、著作権侵害等のリスクが存在する一方で、業務の質や効率を向上させるという大きな可能性があり、利用する価値は十分にあります。たとえば、次のような用途で利用してみましょう。

- アイデアの提案
- 文章の校正
- メール文の文案作成
- ドキュメントの下書き作成



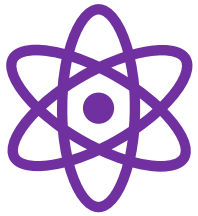
生成AIに求めている情報を出力してもらうには

生成AIに指示を入力しても、求めている情報が出力されないケースが数多くあります。そのため生成AIは役に立たないと考えてしまいがちですが、多くの場合、原因は指示が不十分なことにあります。指示内容を明確にし、必要情報を提供しましょう（情報漏えいにならないよう注意）。

不明確な指示の例

新製品のチョコレートのキャッチコピーを考えてください

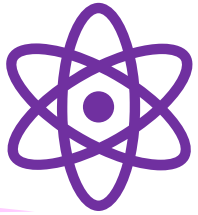
（精度の低い回答）



明確な指示の例

新製品のチョコレートのキャッチコピーを考えてください。
#文字数：80文字以内
#文体：ターゲット層に好まれるようなやわらかい文体
#商品の特徴：~~~
#ターゲット：~~~

（精度の高い回答）



指示を出す際のポイント

指示をする際には、次のような点を明確にしましょう。

- 条件を明確に指定する（例：文字数、ページ数など）
- 出力形式を具体的に指定する（例：メール文、箇条書き、テスト問題など）
- AIが文章生成に使う資料や素材などを提供する（ただし、情報漏えいを避けるために既知の情報を使う。例：会社の経営理念、公的な資料、公表済みの情報など）
- より精度の高い回答に必要な指示・要素を、AI自身に聞いてみる

生成AIは便利ですが、作業を丸投げしないよう注意しましょう。情報に価値を持たせるのは人間の役目です。

会社と働く人たち、その家族を守るのは
あなたのコンプライアンス行動です。

お疲れ様でした。