DXお悩み相談室

第4回 「生成AIのリスク」のお悩み

仕事で使うなら法人契約を。リスクを知って活用しよう

Dさん（経営者）： ビジネスに欠かせないツールといわれる生成AIですが、当社でもみんな使い始めているようです。情報収集や資料作成、企画立案などに幅広く使っている人もおり、確かに便利なのだと思いますが、セキュリティ面などのリスクがあるとも聞きます。従業員が自由に使う状態にしておいて大丈夫でしょうか？

柴山： おっしゃるとおり、生成AIを仕事で使う場合には、いくつか知っておくべきリスクがあります。その対策をおろそかにすると、機密情報の漏洩や訴訟問題など、会社にとって重大な事態を招く恐れがあります。

Dさん： やはりそうなんですね。じゃあ、仕事では使わないようにと言ったほうがいいですかね。

柴山： いえいえ、それは「事故を起こす可能性があるから車は使用禁止」と言うのと同じで、今の時代にはもうありえない選択肢だと思ってください。従業員の皆さんには、押さえるべきリスクをしっかり伝えたうえでどんどん活用してもらうことが、業務の効率化や会社の発展につながると思いますよ。

Dさん： どこに気を付けたらいいのでしょう。

柴山： まず前提として確認したいのですが、Dさんの会社で従業員の皆さんが使っている生成AIは、法人契約したものか、無料版か、どちらでしょうか？

Dさん： えーっと、そういう違いがあることも、私はあまり把握できていませんでした。IT担当者に確認してみます。

柴山： もし「無料版の生成AIをウェブ経由で使っている」というような状態でしたら、法人契約への切替をおすすめします。それだけでもリスクをかなり低減させることができます。そのうえで気を付けてほしい3大リスクがあります。1つめが情報漏洩です。まずは、「機密情報は生成AIに入力厳禁」ということを社内に徹底させてください。機密情報というのは、会社の財務情報や顧客情報はもちろん、企画内容や商品情報など社外に未発表の情報全てです。

Dさん： 生成AIに入力した情報は、漏洩リスクがあるのですか？

柴山： 無料版の場合は特に、生成AIに入力した情報は学習に使われるものと思ってください。例えば、御社で新製品のアイデアを生成AIに入力した場合、そのアイデアが競合他社で生成AIの回答として出力されてしまう、というようなことも起こりえます。実際過去には、サムスン電子のエンジニアが社内の機密ソースコードをチャットGPTに入力し、外部に情報流出した事例もあります。

Dさん： うわ、それは怖いですね。法人契約なら大丈夫ですか？

柴山： 漏洩リスクは低くはなりますが、外部サービスを利用している時点でリスクはゼロにはならないので、どんな場合でも「機密情報は入力しない」と徹底したほうがいいです。

Dさん： すぐにみんなに伝えます。

柴山： 2つめは、生成AIの回答は間違っている可能性があることです。ハルシネーション（幻覚）といって、AIが事実ではない情報や根拠のない内容をもっともらしく生成してしまう場合があります。生成AIの大規模言語モデル（LLM）は学習データに基づいて結果を導き出すため、データが偏っていたり誤っていたりすると、回答が不完全だったり間違っていたりします。また、ユーザーの問いに対して適切な回答が見つけられない場合にも、LLMは「わかりません」とは回答せずに、ユーザーが好むような文章を生成して回答として提示してしまうという特性があります。最近はハルシネーションの問題もだいぶ改善されてきたと言われていますが、それでも、回答を鵜呑みにせず、「間違っているかもしれない」という意識を常に持つことは大切です。

Dさん： 顧客に出す書類に生成AIの回答を使って、その内容が間違っていても、生成AIは責任を取ってくれないですからね。

柴山： そのとおりです。やはりそこは人間が、責任を持ってチェックする必要がありますし、事業戦略など業務のコア部分に関わる判断は、生成AIに任せてはいけないと思います。そして3つめは、著作権などの法的な問題です。生成AIは既存の著作物を学習しているため、生成されたコンテンツが既存の著作物と類似している場合、著作権侵害と判断される可能性があります。生成AIで作成したイラストを自社商品のデザインや広告に使うといったことは、避けたほうがいいですね。

Dさん： なるほど。リスクを把握できると、立てるべき対策も見えてきた気がします。私も使ってみながら、社内での使用ルールを早急につくりたいと思います。

知っトク！ 生成AIの使い道おすすめ5選

生成AIを「仕事で使ったことがない」「何に使っていいのかわからない」という場合、3大リスクに留意したうえで、次のようなところから試してみてください。

1 議事録作成をAIにお任せ
生成AIは、会議の音声データから議事録を生成することができます。要点を整理してくれるので、社員の負担軽減になり情報共有もスムーズに。

2 SNSの投稿内容をスタッフの代わりに
季節のイベントや商品紹介など、SNS用の文章を生成AIに指示して作成。トーンやターゲットに合わせて調整も可能。

3 採用活動のサポート役に
求人票の文章や面接質問の作成、応募者対応メールの下書きなど、採用業務の効率化に生成AIは有効。人材採用を検討している企業におすすめ。

4 社内マニュアルの作成をラクに
業務手順や社内ルールの骨子を生成AIに整理してもらえば、マニュアル作成がスピーディに。

5 企画構想の補助に
新商品やサービスの企画段階で、生成AIに「こんなテーマでアイデアを出して」と頼むと、意外な発想が得られることも。ブレストの補助に最適。

回答者

柴山 治
（しばやま・おさむ）
デジタル戦略プランナー／株式会社YOHACK CEO

米国ワシントン大学 経営学修士課程（Global Executive MBA）修了。ITベンチャー、コンサルティングファーム、外資系生命保険会社等を経て、現在は株式会社YOHACK代表。
企業の成長フェーズや課題に応じた、テーラーメイドの支援を提供している。著書に『日本型デジタル戦略』等がある。

※DXに関するお悩みは、どんなことでもお気軽にご相談ください。