技術トレンド

TREND INFORMATION

# 生成AI時代を生きる ～ChatGPT活用のリスクと可能性～

応用技術課　植村 亮太

**2022年11月30日にChatGPTが公開され、生成AIは大きな注目を集めています。日本の民間企業や行政機関においても事業の高度化・効率化を目指し、ツールとしての生成AIの導入や実証実験の取組が始まっています。生成AIは生産性や付加価値を高めるための道具になり得ますが、一方で、使い方を誤ると包丁や自動車のように取り返しのつかない事故につながるかもしれません。ChatGPTを題材にリスクと活用場面について紹介します。**

## 注意すべきリスク

生成AIを使うリスクにはどのようなものがあるでしょうか。「入力する情報に対するリスク」と「出力された情報を利用するリスク」の2つの観点から整理してみましょう。

生成AIから回答を得るためにはプロンプト（指示・質問）を入力する必要があります。人間同士のコミュニケーションでは具体的で詳しい指示や質問を与えた方が良い働きや回答が得られることが多いですが、生成AIでもそれは同様と考えられます。一方で入力した情報が漏洩する可能性は否定できません。例えば、生成AIはやり取りを学習するため、他者とのやり取りの中で情報が現れる可能性もありますし（ChatGPTでは学習させない設定可能）、不正アクセスによる情報漏洩の危険性もあります。つまり、企業秘密や守秘義務のある機密情報等の入力の制限は必要になると考えられます。業務として生成AIを使う場合は安全性と利便性のバランスを考慮した組織内ガイドラインや環境を整備する必要があるでしょう。

出力された情報をどのように使うかは使う者が責任をもって判断しなくてはなりません。生成AIは事実に基づかない不正確な情報を出力する場合がありますが、誤った情報を信じてしまったために起きたトラブルの責任は人間にあります。その業務では情報が真実である必要があるのか、そうであれば真実であるという裏付けや判断をどのように行うか考える必要があります。また、生成AIはインターネット上の膨大な学習データを元に回答を生成しているため、その情報を元に何かを発信する際には誰かの著作権を侵害していないか、倫理的に不適切な表現が含まれていないか等への細心の注意が必要となります。

## 活用できそうな場面

上述のリスクを踏まえて、業務のどのような場面でどのように生成AIを活用できる可能性がありそうか検討してみました。その中から3つほど活用場面をご紹介します。

当センターでは日々企業からの技術相談を受けており、この業務の高度化・効率化は重要な課題です。ところが、個々の技術相談内容は絶対に漏洩できない機密情報であり、個別具体的な情報を生成AIに入力することはご法度です。例えば、「〇〇工場で作った食品△△から発見された異物の原因究明」の相談があったとします。当然この情報はそのまま入力できません。個別具体的な情報を一般的な情報に置き換えることで情報漏洩のリスクを解消しつつ、それなりに有用な情報を得ることはできないでしょうか。そこで「食品中に異物が発生する現象について原因究明方法と対策方法」を示すようにChatGPTに入力してみます。そうすると、どのような分析手法で検証できるか、どのような対策が必要になるか、一般的な答えが示され、「専門家の助言を得ることも重要です」と締めくくられました。一般的な質問に対するChatGPTの回答は、その分野の専門家にとっては当たり前のことが並ぶように感じますが、検証項目の洗い出しや整理の段階では有用な回答が得られる印象です。それでも現時点ではまだまだ当センターの職員は、専門家として適切な助言ができるように個別具体的な状況を検証・考察しながら課題解決につなげる力を磨かなくてはならないようです。

会議事務局の準備の要点など一般的なビジネススキルの確認においては、ChatGPTは教科書のような回答を示してくれます。また、生成AI使用者はその回答をそのまま使うのではなく、生成AIが教えてくれたコツやノウハウを参考に業務を組み立てることになりますので、たとえ不正確な情報が含まれていたとしてもそれほど大きな問題はなさそうです。その意味で生成AIを初めて使ってみる題材としてビジネススキルの確認はオススメです。意外と世間一般で効果的に使われているビジネススキルを職場で教えてもらえる機会は少ないものですので、色々な気づきを得るきっかけにできそうです。

文章の要約や校正、想定読者層に合わせた表現変換などを効率的に行うことができます。ただし、未発表の文章は機密情報にあたるとも考えられますので、どのような文章であれば入力しても支障がないか組織内でルール整備が必要です。

## 生成AIのこれから

この記事を執筆した8月時点から出版された10月、お読みいただいている現在までの間にも生成AIは急速に進歩していることでしょう。自動車、PC、スマホを使うのが当たり前になったように生成AIを当たり前に使う時代は近いかもしれません。

飛躍的に進歩する技術を捉え、変化をいとわず学び続けるマインドを持ちながら、生成AIをどう使うか、生成AIが発達しても人間に求められることは何かを問うことがこれからの時代に必要なことであるように思います。

●お問い合わせ先／ 京都府中小企業技術センター 応用技術課 食品バイオ係　TEL：075-315-8634　E-mail：ouyou@kptc.jp