

月刊AMCPレポート

AMCパートナーズ株式会社
AMCパートナーズ税理士事務所
〒541-0054 大阪市中央区南本町2-3-8
Tel:06-6262-2256 / Fax:06-6262-2257
【AMCPグループ】 <https://www.amcp.biz/>

経営 VOL.200

(令和7年12月26日発行)

2026年はAIが普及＝AIに“使われない”ためには？

前回、自身の意見を冷静に、かつ具体的に伝える手法としてSBIフレームをご紹介させて頂き、紙面の関係で今号にて詳細をお伝えするとご案内しておりましたが、複数の先生方から、「もう、AIで調べた！」というお声を頂きました。

確かに、最近、この先生方のようにChatGTPやCopilot、Gemini等の「生成AI」を活用し、ちょっとしたことであればこれで解決されている人が急増しており、今回のお声も、この潮流が刻々と進んでいる証左なのですが、ただ、先生方から「AIがこう言っていた」と教えて頂く内容の中には、少し考えれば分かるはずの誤った回答もあり、また、それを検証することなく、そのまま鵜呑みにする危うい傾向も見受けられます。

そこで、今号では、AMCPレポート発刊200号という大きな節目でもあり、また、AIが本格的に普及するであろう「AI普及元年」になると言われている2026年を前に、改めてAIのリスクや注意点等について整理したいと思います。

【生成AIの『活用』におけるリスク】

もう、使われている方は体感済みと存じますが、生成AIは生産性を飛躍的に向上させる「強力な助っ人」です。しかし、その恩恵を享受するには重大なリスクを理解し「最終的な責任は人間に帰属する」ことを理解しておく必要があります。

まず、活用上の重大な注意点(リスク)としては「ハルシネーション(誤情報生成)」が挙げられます。ハルシネーションとは、内容を理解せず「それらしい」回答をAIが生成し、誤った情報(ハルシネーション)を事実のように出力することです。

このような誤情報に基づき意思決定や判断を行ってしまうと取り返しのつかないことになる恐れもありますので、回答を鵜呑みにせず、徹底したファクトチェック:(特に数値、固有名詞、法律情報等)を行う必要があることを再認識しましょう。

次に考えられる重大な注意点(リスク)は「情報漏洩」です。多くの一般向け生成AIでは、ユーザーの入力データ(プロンプト)がAIモデルの学習に再利用される可能性があり、企業秘密、個人情報等が流出する危険があります。

従いまして、『機密情報(社外秘の情報等)は、原則として生成AIに入力しない』等の厳格なルールを設けるだけでなく、法人向けに、セキュリティが強固な環境を利用する等、「活用する環境を整える」ということも必要です。例えば、Gemini なら「Google Workspace 版」の法人プラン、ChatGPT なら「ChatGPT Enterprise」等が該当します。

さらに考えられる重大な注意点(リスク)は「著作権侵害による法的リスク」です。つまり、アウトプットを作成することがある場合において、AIが学習したデータに含まれる既存の著作物と酷似したコンテンツを出力した場合、著作権侵害と見なされる可能性がありますので、アウトプットをAIで作成する場合は、必ず「類似性の確認」を行って下さい。

加えて、生成AIの便利さから、ある業務を完全に任せることも出てくるかも知れませんが、その場合の重大な注意点(リスク)としては、業務継続性の危機(ロックイン)が考えられます。つまり、そのサービスが突然停止・終了したりすると、業務が完全に滞るということです。AIに任せながらも、常に複数の代替手段を検討し、特定のサービスに業務が過度に依存しない柔軟な仕組みを構築しておく必要があります。

【生成AIへの『過度な依存』がもたらすリスク】

これは、インターネットが普及してから囁かれていることですが、生成AIの普及により、今以上に頭脳として依存し過ぎると、人間の本質的な能力そのものが衰退・劣化するリスク、つまり、人間としての思考力・創造力が低下し「自分でゼロから考える」「試行錯誤する」という問題解決能力の根幹が失われ、複雑な問題に直面した際、AIに聞かなければ何も判断できなくなる、対処できなくなるというリスクがあります。

また、本質的な能力だけでなく、過度な依存は人間的スキルも衰退・劣化させてしまいます。つまり、依存によりプロンプトのスキルは上がるかも知れませんが、それにより、逆に、自力での文章校正能力、論理構成力、情報収集能力といった基本的なビジネススキルが身に付かず、生成AIが使えない状況下(会議や口頭で説明が必要なシーン等)で十分なパフォーマンスを発揮できなくなってしまいます。

従いまして、そうならないためにも、生成AIの回答を鵜呑みにせず、必ずそこから検証・深掘り・修正・独自視点の追加作業等を意識的にを行い、自分自身のスキルを意図的に維持・向上させる努力を怠らないようにしなければいけません。

【まとめ:生成AIに「使われる」のではなく、「使いこなす」】

今号にて、生成AIの便利さに依存するリスクとその対策をお伝えしましたが、まとめますと、生成AIを安全かつ効果的に使うには、最終的な判断と責任は人間が持つというリテラシーを持ち、誤情報対策(ファクトチェック)・情報漏洩対策(入力禁止ルール)・著作権対策(類似性確認)、そして、生成AIに使われないためのスキルアップが必要なのです。