

ちょっと
待って！

その情報、AIに入れて大丈夫？ AIを使う前に知っておくべきリスク

生成AIは、文章の作成や要約、アイデア出しなど、日々の業務に欠かせないツールとなりつつありますが、業務効率を大幅に高めてくれる一方で、使い方を誤ると情報漏えいや思わぬトラブルにつながるリスクも潜んでいます。

実際、情報処理推進機構（IPA）が発表した「情報セキュリティ10大脅威 2026」では、「AIの利用をめぐるサイバーリスク」が組織向け脅威の第3位に初めて選ばれました。AIの不適切な利用による情報漏えいや、生成された情報を十分に確認せず鵜呑みにすることなどがリスクとして挙げられています。

今回は、生成AIを仕事で安全に使いこなすために、現場で意識しておきたいポイントを整理して解説します。

AIへの入力は「社外への情報送信」と同じ

生成AIに質問や指示を出す際、私たちは文章やファイルを外部のAIサービスへ送信しています。入力データが学習に利用されるかどうかはサービスによって異なりますが、「AIの中だから大丈夫」と軽率に入力してしまうのは危険です。送信ボタンを押す前に、「この情報を社外のサービスに送信しても問題ないだろうか？」と一度確認する習慣をつけましょう。

例えば、「このメール文面を読みやすく書き直して」「この会議資料を3行でまとめて」「このExcelデータから課題を抽出して」といった使い方は非常に効率的です。しかし、その資料の中に顧客名や売上データ、未公開のプロジェクト計画などが含まれていないかを常に意識する必要があります。

具体的に避けるべき情報は、主に「個人情報」「会社の機密情報」「認証情報」の3つです。

- ・個人情報は氏名、電話番号、メールアドレス、住所など。問合せメールは氏名や会社名を伏せて入力しましょう。
- ・会社の機密情報は未発表資料、売上・原価、見積金額、取引条件、仕様書などが該当します。
- PDFやExcelはそのまま送らず、必要部分だけ抜き出し、具体的な名称や数字をぼかしましょう。
- ・ID、パスワード、APIキー等の認証情報も要注意。設定ファイルを貼る前に必ず確認してください。



安全に業務に活かすための工夫

制限ばかりではAIの良さを活かせません。大切なのは「使わない」ことではなく「情報を整理して使う」ことです。文章のたたき台作成であれば、「商品の発送が遅れる際のお詫び文面案を作成して」のように、具体的な名称を出さずに一般論として依頼すればリスクはありません。

また、「社内研修で使えるテーマ案を10個あげて」といったアイデア出しや、「Windowsのこの機能について分かりやすく説明して」などの公開情報の整理・要約も、機密情報を入力せずに安全に活用できる領域です。なお、「石川県で3店舗を運営している従業員30人ほどの〇〇業です。採用向けの会社紹介文を作ってください」のように会社を特定できる情報を入れすぎると、名称を伏せていても会社が特定されてしまう可能性があるため注意が必要です。

もう一つ重要なのが、AIは間違った情報をもっともらしく回答することがあるという点です。生成AIは文章を自然につなぐことが得意な反面、事実とは異なる情報や存在しない制度を正解のように提示してしまうことがあります。特に金額や数値データ、日付・スケジュール、法律や公的制度、セキュリティ設定や製品の仕様といった項目については、AIの回答を鵜呑みにせず、必ず公式サイトや元の資料で事実確認を行ってください。

AIは「絶対に正しい答えを出してくれる検索ツール」ではなく、「作業を手伝ってくれるアシスタント」として位置づけ、最後の確認は人間が行うのが最も安全です。



AIが作ったものにも「権利」の問題がある

AIで作成した文章や画像も、自由に使えるとは限りません。AIが作ったか人が作ったかにかかわらず、完成物が第三者の著作権を侵害していれば問題になります。生成物が既存のWebサイトや書籍、キャラクターやデザインに酷似している場合は注意が必要です。

特に、Webサイトや広告など社外公開物にAI生成物を使う場合、「AIが作ったから著作権を気にしなくてよい」と考えるのは禁物です。既存作品を模倣する指示は避け、生成内容が第三者の著作物に似すぎていないか確認しましょう。

もう一つの注意点は、AI生成物自体の著作権です。人が創作した文章や画像は、創作性があれば通常その人の著作物となります。一方、AIへの簡単な指示だけで自動生成させた場合、著作権が認められない可能性があります。表現や構成を細かく指示したり、生成後に創作的修正を加えたりしていれば、著作物として認められやすくなります。

つまり、「AIで作ったから自由に使える」「自分の著作物になる」とは単純に考えられません。社外公開や商用利用の際は、第三者の権利を侵害していないか確認し、AIサービスの規約も確認しておきましょう。



利用前の5つのセルフチェック！！

AIに指示を送信したり、回答を確認するときに、以下の5項目をチェックしてみてください。

- 1 個人情報を送信していないか
- 2 社外に出て困る情報を送信していないか
- 3 パスワードや認証情報を送信していないか
- 4 返ってきた回答をそのまま鵜呑みにしていないか
- 5 AIが作った文章や画像が第三者の権利を侵害していないか



開発室から



最近、一人でドライブしている時に「ChatGPT」とおしゃべりを楽しむことがあります。でも「近くの観光地を教えて」と言うと、位置情報までは取得できてないみたいで、どこにいるか教えてと言われます。でも、こちらからドライブ中の現在地を教え、「明日〇〇があるよ」と最新のイベント情報まで詳しく教えてくれました。その情報のおかげで二日続けて同じところへドライブに行っちゃいました。



小規模・中小企業向け
クラウド販売管理システム



簡単、便利、使いやすい！

「もうかります！」の基本機能や使いやすさはそのままに、
クラウドバージョンの登場です！

日々の販売業務の効率化に役立ちます！面倒な設定なしで手軽にスタートできます。



**無料トライアルの
お申込みはこちら！**

クレジットカードの登録なしで、簡単にお試しいただけます。



moucla 公式ページ

無料トライアルのお申込み、
moucla の機能詳細は
こちらから！

mouclaの特徴

01. 販売管理に必要な機能がひとつに！
02. 操作しやすく、シンプルな画面
03. 業種や業務の流れに合わせて、機能を追加できます！
04. 追加費用無し！安心のサポート対応
05. クラウド型で導入が早くて安い！
06. 情報共有が簡単、災害時も安心

PCだけでなく、タブレットでもお使いいただけます！

主な機能一覧

- ・見積書の作成
- ・受注管理、注文請書の作成
- ・売上計上、納品書の作成
- ・請求書の作成
- ・入金、売掛管理
- ・発注管理、注文書の作成
- ・仕入、支払、買掛管理
- ・在庫管理
- ・売上や粗利集計、実績管理
- ・請求書、見積書のメール送信

※軽減税率や適格請求書（インボイス）に対応しています。

料金

初期費用	50,000 円（税別）
月額費用	月額 3,000 円（税別）～

販売管理機能を1ユーザーでご利用の場合は、月額 3,000 円（税別）です。

販売管理＋仕入在庫管理機能を1ユーザーでご利用の場合は、月額 5,000 円（税別）です。

※月額費用は、ご利用の機能とユーザー数により変動します。

※カスタマイズした場合は料金が異なります。

moucla 導入の流れ

01 無料トライアルのご提案

お客様専用のアカウントをご用意いたします。
サンプルデータと操作ガイドが用意されており、
すぐにお使いいただけます。

電話、メール、WEBなどでサポートいたします。
業務に合わせてカスタマイズのご提案もいたします。

02 ご契約

ご利用の機能とユーザー数を決めていただきます。
カスタマイズが必要な場合は御見積後のご契約と
なります。

03 システムの運用開始

無料トライアルで入力したデータをお使いいただく
ことも可能です。

電話、メール、WEBなどでサポートいたします。
導入後のカスタマイズも可能です。

「もうかります！」シリーズを お使いのお客様へ

販売管理パッケージソフト「もうかります！」
シリーズをご利用いただき、誠にありがとうございます。

クラウドの販売管理システムをお探しであれば、
ぜひこの機会に「moucla」の無料トライアルをお
試してください！

無料トライアル後にそのままご購入される場合、
「もうかります！」のデータを引き継ぐことが
できます。