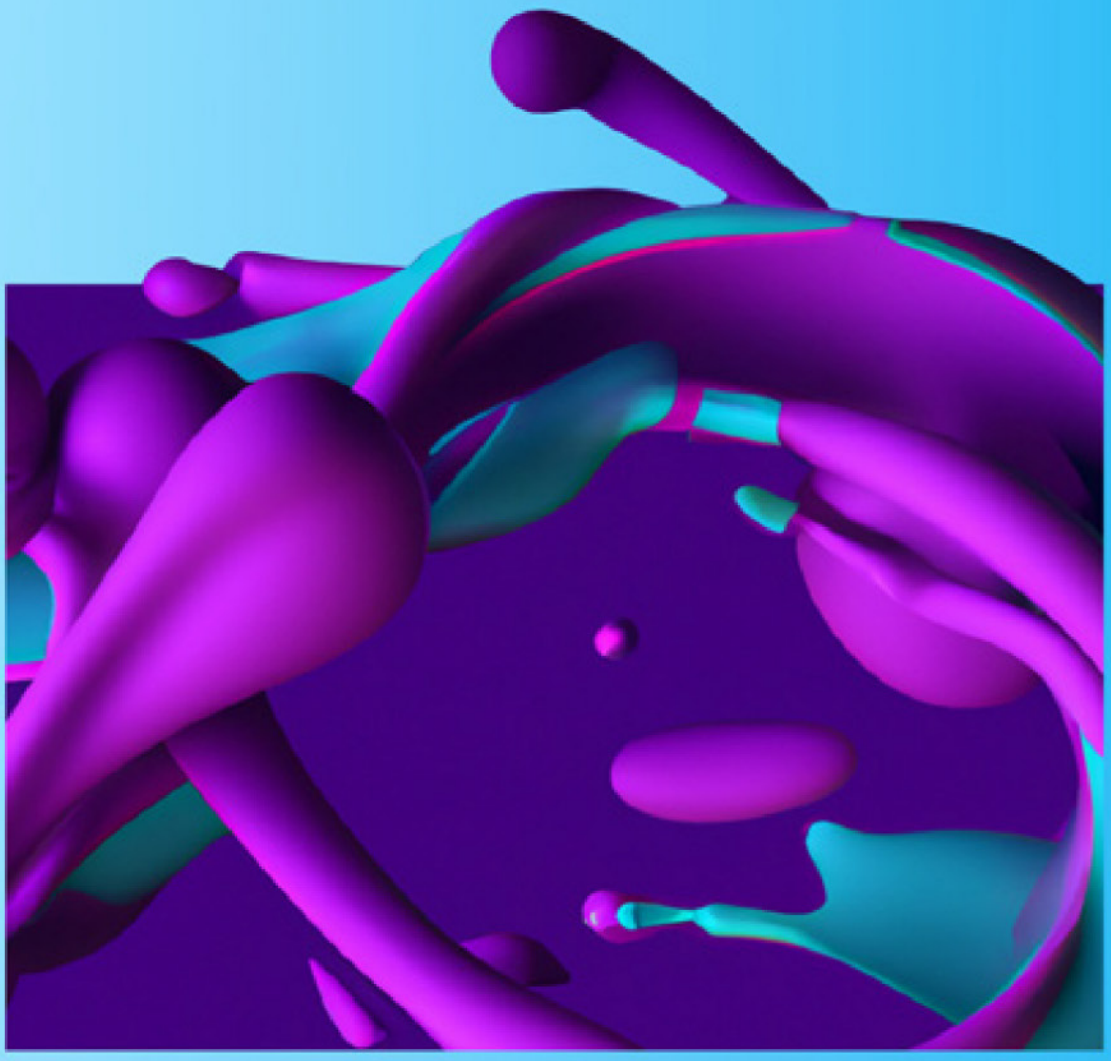
KPMG

生成AIモデル：ビジネスにおけるリスクおよび潜在的なリターン

ChatGPT、DALL·E2、Bard等の出現は組織にどのような影響を与えるか



Lisa Heneghan
Global Chief Digital Officer
KPMGインターナショナル

生成AIモデルは、テクノロジーの力を際立たせます。
これらのモデルによって、より生産的になり、また何かをより簡単に行うことができる可能性があります。
しかし、これらのモデルには、すべての組織と個人が認識すべきリスクが伴います。それでも、これらのモデルは私たちの私生活や仕事の一部として急速に普及しており、無視することはできません。私たちは、それらをどのように安全に受け入れるかを判断する必要があります。

本レポートに掲載の画像は、テキスト記述に基づいて画像を生成するAIアートジェネレーターである「DALL·E2」を使用してデザインされました。

表紙画像のプロンプトは、流体的な抽象画、青と紫の波状の柱、水しぶき、水滴、紫の背景でした。

DALL·E2は魅力的で視覚的なコンテンツを生成しますが、KPMGのブランドガイドラインに基づいてトレーニングされているわけではありません。また、KPMGのブランドポジショニングを理解するための人間の専門知識や独創性も持ち合わせていません。そのため、これらの画像はオフブランドとみなされ、KPMGのブランドマネジメント部門の特別な許可のもと、説明用のみに使用されています。

目次

エグゼクティブサマリー 04

市場概況 05

生成AIモデルとは？ 06

生成AIモデルの仕組み 06

潜在的な機会とユースケース 07

現在の検討事項 10

未来には何が起こるのか？ 13

KPMGによる支援 14

01 エグゼクティブサマリー

生成型人工知能（生成AI）モデルが、前例のない速度と効率で特定のタスクを自動化および実行することにより、ビジネスが大きく変革されようとしています。特に、人間の専門知識と独創性が、これらのプログラムの使用方法と、その能力を効果的に活用するための深い理解と組み合わされた場合に、その傾向が顕著になります。

しかしながら、責任ある、信頼できる、そして安全な方法でこれらのプログラムの可能性を最大限に引き出すには、時間と人間の専門知識が必要です。

生成AIの使用を検討している場合は、組織内のすべての人が従うための一連の内部プロセスと統制を確立することが重要です。

本レポートでは、潜在的なユースケースと機会、そして組織内でChatGPTなどの生成AIアプリケーションの使用を検討する際に考慮すべき事項について取り上げます。

生成AIについて知っておくべき10のこと

1. 最も一般的な生成AIソリューションは、大まかに次の5つのカテゴリに分類されます。コンテンツ生成、情報抽出、スマートチャットボット、言語翻訳、コード生成です。
2. 生成AIモデルは、記事の要約、メールの下書き、画像や動画の作成が可能です。人間によって訓練された一部の生成AIモデルは、追加の質問に答える、間違いを認める、不正確な仮説に異議を唱える、不適切な要求をフィルタリングまたは拒否するなどの会話スキルを備えています。
3. ChatGPTは、人間の指示に基づいて訓練されたチャットボットです。GPT-3.5はインターネットに接続されておらず、2021年9月までのデータで学習されました。OpenAI社の新しい大規模マルチモーダルモデルであるGPT-4は、以前の大規模言語モデルから進化したものです。
4. 生成AIモデルは、IT、人事、オペレーション、財務、監査、法務、マーケティングなどのさまざまなビジネス機能で使用できます。適切な応用例には、提案書の作成、コードの開発とテスト、複雑な情報の抽出と要約が含まれます。
5. 生成AIはデータ入力またはパラメータを受け取り、学習して知識を構築します。明示的にアプリケーションプロバイダーに制限をかけない限り、そのデータは他の誰かからのプロンプトに答えるために使用される可能性があり、結果的に組織の独自情報が一般に公開される恐れがあります。アプリケーションによっては、著作権を譲渡することになる場合もあります。利用者が入力したデータがどのように扱われるかは、それぞれの利用規約を確認することで把握できます。
6. 生成AIを使用する目的と実装方法によっては、知的財産や営業秘密を露出し、組織を不正リスクにさらす危険性があります。組織に適用される法律（プライバシー法を含む）、顧客との契約、または専門基準に違反するような形でAIを使用していないことを確認するために、注意深い監視が重要です。
7. AIによって生成された情報やコードを成果物や製品にコピーすることで、著作権や他の知的財産権を侵害する可能性があります。これにより、組織が法的または風評上の損害を被るリスクがあります。
8. KPMGは、オープンソース版とブティック版の生成AIが、インターネットブラウザからクラウドベースのソフトウェアやインスタントメッセージングプログラムなど、組織がライセンスを供与するAIと連携した技術まで、多くの一般的なアプリケーション、システム、プロセスに統合され続けると予測しています。
9. 組織内で安全な使用ガイドラインを作成することは、生成AIアプリケーションを適切かつ効果的に使用するうえで重要です。また、人間がかかわることでのみ得られる独自の洞察力や理解力を、生成AI単独では再現できないため、組織は自社の人材をスキルアップする必要があります。
10. KPMGは、安全で信頼性があり、倫理的な方法でAIシステムを設計、構築、展開する責任あるアプローチを取っています。このアプローチにより、企業が消費者、組織、社会に対する価値を高めることを支援します。

02 市場概況

調査・コンサルティング企業のGartner社によると、2025年までに、大企業から送信されるメッセージの30%が合成的に生成されると予想されています[1]。2022年9月にKPMG米国が実施したAIリスク調査レポートでは、回答者の85%がAIと予測分析モデルの利用増加を予測しています。また、2022年のKPMG米国のテクノロジー調査では、回答者の半数がAI技術への投資からROIを実感していると回答しています。

2022年夏、AIが生成した画像がアートコンテストで優勝したことで、生成AIモデルが注目を集めました[2]。その後、11月にはChatGPTがリリースされ、再び注目されました。さらに、2023年1月の世界経済フォーラムで、Microsoft社のチェアマン兼CEOであるSatya Nadella氏が「AIの黄金時代が始まった」と発言したことで[3]、ChatGPTに対する関心が高まり、KPMGの各ファームのクライアントから多くの質問が寄せられました。

これらのモデルを学習するには、莫大なベンチャーキャピタル、人的労力、コンピューティングパワーが必要です。ChatGPTを開発したOpenAI社は、Microsoft社から10億米ドルを受け取り[4]、2023年初めに同社からさらに数十億米ドルの投資を受けました[5]。Google[6]やMeta[7]も独自の生成AIモデルを作成しています。さまざまな応用範囲が考えられることから、生成AIモデルを活用した新しい産業が形成されつつあります。

生成AIアプリケーションは、コンテンツ生成、情報抽出、スマートチャットボット、言語翻訳、コード生成の5つに大別されます：

- **コンテンツ生成：**事前学習済みのTransformerツールがブログ投稿、メール、ソーシャルメディア投稿、画像、ウェブコンテンツや広告などを生成します。
- **情報抽出：**ニュース記事、ブログ投稿、法的文書などの短文または長文の要約を作成できます。一部の企業はこれらを使用して法的文書を策定および分析しています。
- **スマートチャットボット：**企業は、スマートチャットボットを消費者のアシスタントとして使用することが増えています。チャットボットは会話形式で対話し、追加の質問に答え、間違いを認め、不確かなアイデアに異議を唱え、不適切な要求を拒否できます。
- **言語翻訳：**多くの言語を翻訳することができる多言語ツールです。翻訳サイトを含むウェブサイト全体のインターフェースを構築できる可能性があります。
- **コード生成：**生成AIモデルは、自然なテキスト入力をコードスニペットやアプリケーションに変換することができます。基本的な説明や小さなプログラム関数の入力があれば、これらのモデルはさまざまなプログラミング言語のコードを生成し、バグを特定して修正することができます。

1 Gartner, 7 Technology Disruptions That Will Completely Change Sales , October 10, 2022. https://www.gartner.com/en/articles/7-technology-disruptions-that-will-completely-change-sales. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.
2 https://www.smithsonianmag.com/smart-news/artificial-intelligence-art-wins-colorado-state-fair-180980703/
3 https://www.weforum.org/press/2023/01/satya-nadella-says-ai-golden-age-is-here-and-it-s-good-for-humanity
4 https://openai.com/blog/microsoft-invests-in-and-partners-with-openai
5 https://blogs.microsoft.com/blog/2023/01/23/microsoftandopenaiextendpartnership/
6 https://blog.google/technology/ai/bard-google-ai-search-updates/
7 https://ai.facebook.com/

03 生成AIモデルとは？

生成AIは、既存のデータを単に分析または処理するのではなく、コンテンツを生成できる人工知能を指します。

GPT-4などの生成AIモデルは、収集されたデータセットで構築および学習が行われます。これらのモデルは、事前定義されたデータコレクションに基づいてジェネラリストやスペシャリストにもなることができ、人間が指示した特定の要求に従って出力を生成するように設計されています。

たとえば、一部のモデルは、前のフレーズに基づいて次の単語を予測したり、前の画像の説明に基づいて次の画像を予測したりすることができます。

この学習により、テキスト、画像、動画、コードなどのオリジナルコンテンツを素早く生成できます。必要な人的リソースが低減されることにより、一部の企業は、より速く、低コストでコンテンツを作成できることを期待し、以前はコストや時間がかかりすぎていた新しい種類のコンテンツを作成する機会が得られるようになると考えています。これは人間と機械の相互作用を根本的に変え、多数のユースケースの可能性を広げることになります。

この予測能力により、入力されたテキストで説明されたトピックに関する文書を特定するなど、モデルによる分析を行うことができます。

04 生成AIモデルの仕組み

生成AIモデルは、明確な入力とルールに基づいてコンテンツを生成するように設計されています。

最近、最も話題になっている生成AIモデルのアプリケーションは、米国サンフランシスコの研究・開発企業であるOpenAI社が作成した、人間の指示に基づいて学習されたチャットボット「ChatGPT」です[8]。2023年3月14日時点でChatGPT Plusの契約者は、画像とテキストの両方の入力を受け付け、テキスト出力を生成する大規模マルチモーダルモデル（LMM）であるGPT-4を使用することができるようになりました[9]。また、2023年3月23日には、OpenAI社が独自のウェブブラウザのプラグインを含むChatGPT専用のプラグインを発表しました。これにより、ChatGPTは特定のサードパーティのソースやデータベースへのアクセスが可能となりました[10]。

ChatGPTは、**C**hat（conversation-based：会話ベースの）**G**（generative：生成する）**P**（pretrained：事前学習された）**T**（transformer：自然言語処理（NLP）タスクで使用される深層学習モデルの一種）を表しています。人間のフィードバックから強化学習を使用して微調整され、人間らしい音声を出力し、望ましくない応答を防止し、幻覚（事実を作り上げること）を回避するために、人間の嗜好を表す報酬モデルが学習されました。

ChatGPTは、大規模言語モデル（LLM）として作成され、その後、大規模マルチモーダル生成AIアプリケーションに進化しました。

これは、ChatGPTが以前はテキスト入力のみであったのに対し、画像とテキストの両方を受け付けられるようになったことを意味します。加えて、教師なし学習によって結果を予測するニューラルネットワークモデルを組み合わせることで、このタイプの生成モデルは、最も可能性の高い言語パターンと、すでに学習済みのコンテンツ間の関係性を判断できます。

「大規模」とは、モデル自体の大きさだけでなく、モデルのベースとなるデータ量のことを指します。これには、大量の公開電子文書のコレクションを使用してモデルを学習することも含まれます。

ChatGPTは最初に、WikipediaやThe New York Timesなどから100万以上のデータセットまたは5,000億トークン（単語の断片）で学習されました。これをわかりやすくすると、人間が一生で話す言葉の平均は8億6,030万語であり[11]、このコレクション（AI用語では「コーパス」と呼ばれる）は語彙量としておよそ300年分に相当します。

8 https://www.forbes.com/sites/cindygordon/2023/02/02/chatgpt-is-the-fastest-growing-ap-in-the-history-of-web-applications/?sh=7510d916678c
9 https://openai.com/research/gpt-4
10 ChatGPT plugins (openai.com)
11 https://openlibrary.org/books/OL3502128M/The_joy_of_lex

ChatGPTの基本バージョンはインターネットに接続されておらず、2021年9月までのオンライン教材を基に学習しているため、その知識は最新ではありません。Bingの検索エンジンのプラグインのように[12]、一部のプレミアム開発者向けにリリースされた新しい実装はインターネットに接続され、より最近のコンテンツを含んでいます。

ChatGPTは特化型人工知能（ANI）の一例です。ANIシステムは、訓練された1つのタスクを実行することに適しています。たとえば、画像を生成するように設計されたANIシステムは、数学の問題を解決することはできないでしょう。

OpenAI社によると、GPT-4は前身であるGPT-3.5に比べてより信頼性が高く、微妙な指示を扱うことができるとされていますが、まだ完全に信頼性があるわけではありません。最も重要なことは、GPT-4が模擬司法試験で、トップ10%の受験者に匹敵するスコアを獲得したことです。一方、同じ模擬試験でのGPT-3.5のスコアは下位10%でした。OpenAI社は、GPT-3.5の限界は、事実の幻覚化や、推論の誤りを犯すといった点でGPTの先行モデルと同様であると指摘しています[13]。

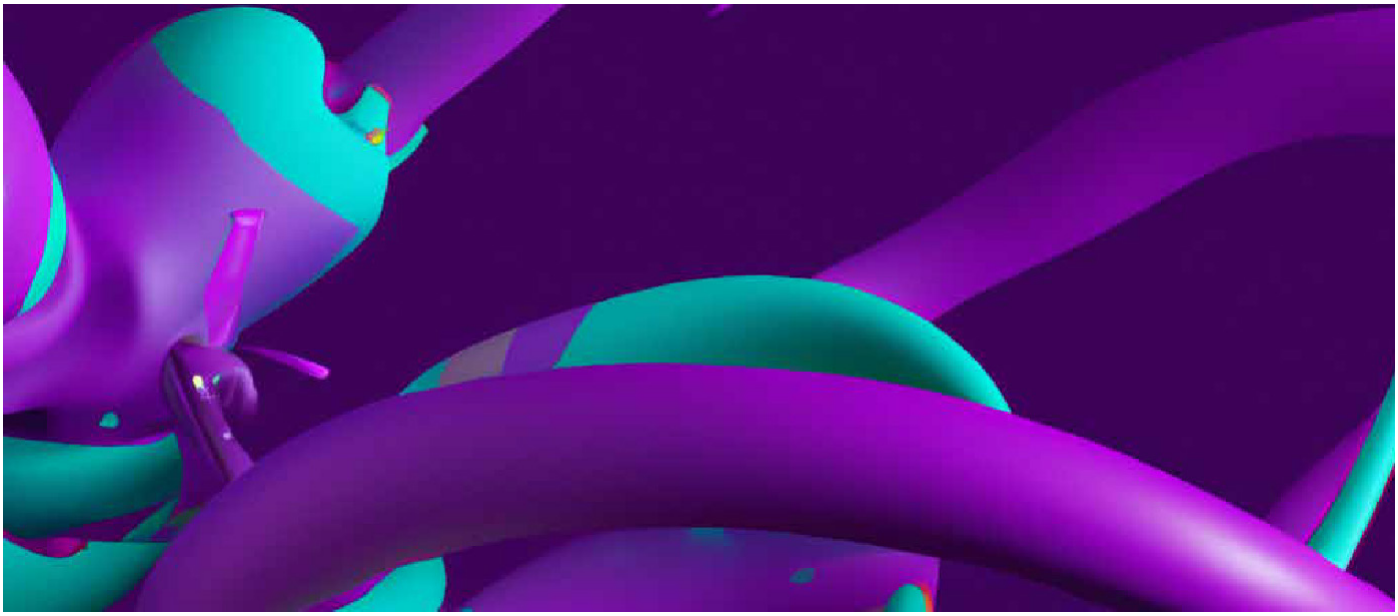
05 潜在的な機会とユースケース

ChatGPTが急速に人気を博している理由の1つは、技術的なバックグラウンドを持たない人でも利用できるということです。2023年2月時点で、ユーザー数が1億人に達したことは[14]、人々がこの技術を利用したいという熱意の表れです。そして、チャットボットのユーザー数が多いほど、その基盤となるAIの学習が進むことになります。

ChatGPTは、言語に基づくタスクを前例のない速度と効率で自動化して実行することにより、ビジネスを変革する可能性を秘めています。大規模マルチモーダルモデル（LMM）は、さまざまなタスクに対応するために展開することができます。法的文書の要約や分類、消費者からの質問への回答、専門家へのアドバイス、エンジニアリングや建築図面の作成などに利用できます。

生成AIモデルは、人間のインスピレーションの出発点として機能し、新鮮で創造的な考えに変換できるアイデアを提供することができます。そのため、ビジネスレポート、マーケティングプレゼンテーション、ソフトウェアアプリケーションのコード生成に適しています。

生成AIモデルには、IT、監査、人事、オペレーションなど、ビジネス機能全般においても応用できる可能性があります。これらのユースケースを検討する際、生成AIが多くの機会をもたらす一方で、リスクが伴う危険性に留意する必要があります。



12 https://www.bing.com/new
13 https://openai.com/research/gpt-4
14 https://www.theguardian.com/technology/2023/feb/02/chatgpt-100-million-users-open-ai-fastest-growing-app

IT運用の現場では、以下のように使用できます：

大規模マルチモーダルモデル（LMM）ベースのナレッジマネジメントシステム
さまざまなデータソースフォーマットからの情報収集に使用できます。この情報は、特定のアイテムを検索するためにクエリされます。

セルフサービス型ITサポート
会話型AIチャットボットによって生成されたサポート手順によって、従業員によるITシステムのエラー解決を支援します。

コーディングまたはコードのテスト
コードを別の機能に変換すること、たとえばSQLからPythonへの変換、またはコードの動作確認テストを行うことができます。

監査・コンプライアンスにおいては、以下のようなことに役立つかもしれません：

監査レビューの自動化
クエリ形式に基づき、提出された監査報告の事実収集および詳細な監査レビューを自動化することができます。

独立性要件の評価
監査関与の独立性要件を評価し、独立性を認定するための承認プロセスを簡素化することに役立ちます。

人事分野における活用の可能性は以下のとおりです：

候補者選定
仕事内容や関連スキルのデータを基に生成AIモデルを学習させ、適切な候補者の特定を支援します。

セルフサービスアプリケーション
人的な方法で知識を共有し、人事に関する問合せの解決が可能なチャットボットを展開できます。

オペレーション面では、以下のようなことに役立ちます：

サステナビリティとESGの報告
ESGデータを文脈化し、ESGの取組み概要をわかりやすく説明した文書の作成など、報告業務をサポートすることができます。

バーチャルイベント運営
招待状の作成、セッションのスケジュール調整、参加者の質問対応など、イベント運営をコーディネートします。

ビジネスオペレーションの簡素化
電子メールの作成や提案依頼書の準備から競合分析の実施、市場調査まで、さまざまな業務において活用できます。

財務・ロジスティクスの分野では、以下のようなサポートが考えられます:

支払いの分類と検証
膨大なデータを整理することで、組織の税金納付の公開を支援します。

契約条項の作成・見直し
契約書の見直し、潜在的な利益相反条項の指摘、契約プロセスを早めるための条項や条件を起草します。

法的および組織的なガバナンスには、以下のような選択肢があります：

投資に関する独立性を保った個別提案
独立性に関する問合せに対して、チャットボットでパーソナライズされた回答を提供することができます。

法的引用と出所の提示
関連する法的判例や事例を検索し、信頼できる情報源を特定することで、法的引用や出所を提示することができます。

マーケティングにおいて想定される活用方法は以下のとおりです：

キャンペーン文言の簡略化
さまざまな言語で適切に翻訳される代替語候補を見つけることができます。

大規模なマーケティングコミュニケーションのローカライズ
モデルと現地の会話データを共有することにより、グローバルキャンペーンのローカライズを支援します。

複雑な情報の抽出
たとえば、財務デューデリジェンスの基礎を学び、コンテンツを理解し構造化することで、強力なマーケティングキャンペーンを構築するための支援を行います。

KPMGは、AI、機械学習、データ＆アナリティクスなどの新興技術に関するリスクに対し、深い専門知識を有しています。また、企業のAIおよび機械学習技術における倫理、ガバナンス、およびセキュリティの評価を支援することができます。

KPMGの各ファームは、長年にわたり新しいテクノロジーの探求と活用を推進しており、生成AIの応用が組織の成長にどのように役立つかについて、提言が可能です。

06 現在の検討事項

ここまで、生成AIモデルが消費者の助けとなり、組織プロセスを効率化し、従業員がより高い付加価値のある業務に時間を充てられるようになる可能性をみてきました。しかし、生成AIの使用には多くの制限や潜在的な問題があります。

セクション4で述べたように、ChatGPTの初期の基盤となる大規模言語モデル（LLM）であるGPT-3.5は、2021年9月までの教材を基に学習し、インターネットには接続されていませんでした。OpenAI社は、ChatGPTが特定のケースでインターネットを閲覧できるようにしたとはいえ、生成AIの使用プロセスには人間のレビューや専門知識が組み込まれることが重要です。生成AIモデルはAIアプリケーションの中核となり得ますが、問題を解決するためには、追加の分析、技術、人間の関与が必要です。

本セクションでは、顧客や企業の機密性、従業員の不正使用やフィッシングなど、生成AIモデルやアプリケーションを使用することのリスクとその管理方法について説明します。

ChatGPTのような大規模マルチモーダルモデル（LMM）は人間らしい応答を生成しますが、人間らしい推論力を持ちません。これらのモデルが信頼を得るためには、ユーザーが責任をもって適切なユースケースにAI機能を適用し、組織は従業員にこのようなプログラムの使用方法を教育する必要があります。同様に、開発者は信頼できるデータセットを使用してAIモデルを学習させ、関連するバイアスやコンテンツフィルターを適用しなければなりません。

リスクマネジメント

生成AIの人気の高まりは、組織が誤用から自社を保護するために、責任ある方法でAIを開発・導入することを推奨する理由の1つです。生成AIモデルのリスク管理上の課題として、以下が挙げられます。

内部リスクと考慮事項

機密性や知的財産の侵害

多くの生成AIモデルは、ユーザーが入力したデータを吸収して基盤となるモデルを時間の経過とともに改善するように構築されています。つまり、学習と知識の蓄積を手助けするものです。そのデータは、代わりに他の誰かのプロンプトに答えるために使用される可能性があり、公衆に個人情報や独自の情報が公開される恐れがあります。この技術を使用するほど、機密性の高い情報が他人にアクセスされるリスクが高くなります。したがって、組織は生成AIアプリケーションの利点を享受しながら、知的財産を保護する方法を模索する必要があります。

従業員の誤使用や不正確性

生成AIの正当な使用にもリスクが伴います。これらのモデルは入力に基づいて回答を生成するため、虚偽または悪意のあるコンテンツを提供する可能性があります。従業員が使用する際には、慎重を期して品質保証に重点を置き、AIが生成したコンテンツを注意深く確認することが求められます。

生成AIのコンテンツに誤りが含まれていても検出されない場合、ビジネスの成果に影響を与えたり、責任問題を引き起こしかねません。たとえば、Meta社の生成AIボットであるGalacticaは、科学情報を簡略化し、学者や研究者が論文や研究を迅速に見つけることを支援するために作成されました。しかし、Galacticaは著名な科学者を誤って引用し、膨大な量の誤情報を作り出したのです[15]。また、BlenderBot3というMeta社の別のボットは、2022年8月のリリース直後に虚偽の誤った主張を行っていることが判明しました[16]。さらに、Google社のチャットボットBardは、最初のデモで不正確な情報を共有したことにより、親会社のAlphabetは市場価値にして1,000億米ドル以上を失いました[17]。ChatGPTが事実を歪曲することもよく文献化されており[18,19]、開発者のOpenAI社もその継続的な不備を認めています[20]。

生成AIに関するその他のリスクには、個人データなどの機密情報の生成が考えられること、その情報を用いて個人情報の盗難やプライバシー侵害の恐れがあること、不満を持つ従業員や怒った顧客が企業や従業員、役員の評判を傷つけるために偽の情報を生成させる可能性があることなどが挙げられます。

生成AIの進化

AIに対する世界の理解が進むなか、すでに世界的な規制の強化がみられます。意図的に生成AIを使用する予定がない場合でも、これらの規制について常に最新情報を把握することが重要です。

KPMGは、インターネットブラウザから組織がライセンスを供与するAIと連携した技術まで、生成AIが多くの一般的なアプリケーション、システム、プロセスに統合され続けると予測しています。したがって、AIを仕事上で使用する際には、適用される法律（プライバシー法を含む）、顧客との契約、または専門基準に違反するような方法で使用しないように注意深く監視し、遵守していくことが重要です。

15 https://gizmodo.com/meta-ai-bot-galactica-1849813665
16 https://www.cnn.com/2022/08/11/tech/meta-chatbot-blenderbot/index.html
17 https://www.npr.org/2023/02/09/1155650909/google-chatbot--error-bard-shares
18 https://www.npr.org/2023/03/17/1164383826/heres-what-the-latest-version-of-chatgpt-gets-right-and-wrong
19 https://news.yahoo.com/factual-errors-inflated-bios-aside-100209244.html
20 https://openai.com/research/gpt-4

考えるべき質問：

1. 生成AIモデルを使いながら、機密性と正確性を確保するにはどうすればよいのでしょうか？
2. 生成AIモデルを、拡大するグローバル規制に確実に対応させるにはどうすればよいのでしょうか？
3. コンプライアンスポリシーの見直しや管理を自動化するにはどうすればよいのでしょうか？
4. 従業員は、リスクと利点の観点から、生成AIについてどのようなことを知っておく必要があるのでしょうか？

従業員への影響

高品質で専門的なアウトプットは、高品質で専門的なクエリを用いてのみ達成できます。したがって、組織はクエリの文脈を理解して適切なプロンプトを提供するために、従業員のスキルアップと独自の知識を維持する必要があります。たとえば、KPMGでは「Digital and Data Foundations」プログラムを通じて、全社員に対して生成AIのトレーニングを提供しています。このプログラムは、AIの進化や信頼できるAIの構築、実装、および関与方法についての基礎的な内容を提供しています。

専門家は、単に問題解決のために生成AIを使用するだけでなく、それをトレーニングして進化させていることを認識する必要があります。

生成AIの将来における専門家の役割は、問題解決から問題定義へと移行し、チームが機械と一緒になって新しいアプローチを生み出すことが予想されます。生成AIツールはインターフェースであり、神のお告げではありません。

新しいアプローチを生み出すループのなかで人間は、生成AIだけでは再現できないプロセスに、独自の洞察力と理解をもたらします。人間が重要なフィードバックを提供することで、時間の経過とともにモデルを改善し、精度を高め、公正で、目的に沿った出力を実現します。

人間とテクノロジーの調和により素晴らしいことが起こる可能性があり、人間の創造力なしには持続的な変化は起こり得ないと私たちは強く信じています。

外部リスクと考慮事項

誤情報、偏見、差別

先に述べたように、大規模言語モデル（LLM）や大規模マルチモーダルモデル（LMM）は、誤った、時代遅れの、差別的な情報を共有することがありますが、非常に説得力のある主張をするため、最も懐疑的な読者でさえ騙される可能性があります。

生成AIは、ディープフェイク画像や動画を作成するために使用されることがあります（映像コンテンツが改変され、誰かが何かを言ったかのようにみせかけること）。これらの画像や動画は、非常にリアルにみえることが多く、編集されたデジタルメディアに痕跡が残らないため、人間や機械でさえも検出することが困難です[21]。

著作権

生成AIアプリケーションを通じて実行されたコンテンツの所有者は誰かという疑問は多々ありますが、答えは1つではありません。ツールごとに利用規約が異なることや、素材の使用方法も重要な要素となります。

他者が著作権を有する文章からコピー＆ペーストし、ほとんど変更されないまま使用した場合は、盗作とみなされる可能性があります。生成AIツールを通じて得られた情報を、どこまで変えれば正当に自分のものと言えるのか、断定はできません。

AIが生成したコンテンツを自分のものと主張することは、多くの倫理的問題を引き起こすかもしれません。まず、このような行動は責任も信頼もなく、もしそれが明るみに出れば、クライアントや消費者は、あらゆる面であなたの組織の誠実さを疑うことになるでしょう。さらに、もし単にAIが生成した情報を伝えているだけだと判明した場合、クライアントや消費者は同様に生成AIを利用すればよいと考え、あなたの組織を不要とみなすかもしれません。

財務、ブランド、風評上のリスク

もし、あなたやあなたの組織の誰かがAIによって生成された情報やコードを成果物や製品に使用した場合、それは著作権または他の知的財産権の侵害となる可能性があります。これは、あなたの組織に法的損害や風評被害を与える恐れがあります。

これらのツールの多くは、クライアントの機密情報を入力しないよう明確に指示していますが、トレーニングや理解が不十分なユーザーは、不注意から、知的財産や企業秘密を一般ユーザーや競合他社にさらす危険性があります。これは訴訟につながる可能性があり、現在または将来のクライアントや消費者が、自社の機密情報を任せられるかどうか疑問を抱く懸念があり、自社の収益に悪影響を及ぼしかねません。

生成AIコンテンツを使用する際の透明性の欠如は、風評上の問題を引き起こすことも予想されます。技術系出版社のCNETは、“アイデア出しから出版まで”編集者チームがコンテンツに関与しているとウェブサイトで述べているにもかかわらず、2022年11月から70本以上の記事を書くためにこの技術をひそかに使用しており、その一部には誤りが含まれていると批判されました[22]。

考えるべき質問：

1. 規制に準拠していないことによる財務的なペナルティを避けるために、生成AIアプリケーションを効果的に管理するにはどうすればよいでしょうか？
2. あなたの組織が使うアプリケーションには信頼性があるでしょうか?
3. どのようにしてアプリケーションを積極的に管理し、偏見や差別の可能性を認識し、監視することができるでしょうか？
4. 生成AIアプリケーションを使用することは、あなたの組織の倫理、価値観、ブランドに合っているでしょうか？

21 https://www.propertycasualty360.com/2021/09/14/deepfakes-an-insurance-industry-threat/
22 https://gizmodo.com/cnet-artificial-intelligence-writing-scandal-1850031292

サイバーセキュリティ

サイバー犯罪者は、生成AIを使用して、より現実的で洗練されたフィッシング詐欺やシステムに侵入するための認証情報を作成することができます。さらに、AIアルゴリズムは、その基盤となるトレーニングデータセットを保護することはできません。データが匿名化され、スクラビングされたとしても、アルゴリズムが個人のアイデンティティを識別できることが研究で示されています[23]。

その他の生成AIのサイバーセキュリティリスクとしては、モデルの学習に使用するデータが操作されるデータポイズニングや、生成AIのモデルに悪意のある入力を与えて騙そうとする敵対的攻撃などがあります。

ChatGPTやその他の生成AIアプリケーションのユースケースを検討する際には、サイバーチームとリスクチームが安全な実装ガイドラインと規制を設定することを推奨します。これには、各企業の状況に合わせてChatGPTやその他のソリューションを使用する際の期待値を設定すること、生成AIアプリケーションを使用するメリットとリスクについて従業員を教育すること、適切なサイバーセキュリティ制御を実施することが含まれます。

考えるべき質問：

1. あなたの組織が使用している生成AIアプリケーションは、サイバー攻撃、悪意のある行為、内部者の脅威からどの程度保護されていますか？
2. あなたの組織のセキュリティ制御は機能していますか？　改善できる点はありますか？
3. あなたの組織が使用しているアプリケーションは、誰かのプライバシーを侵害していませんか？

敵対的攻撃

許容範囲内で動作するように訓練されていても、生成AIモデルは、他の分析モデルと同様に、巧妙な外部ユーザーによる意図的な操作に対して脆弱であることが証明されています。あなたの組織が生成AIソリューションの使用を計画している場合、それが一般に公開されたときに、このようなことが起こり得ることを認識しておく必要があります。

考えるべき質問：

1. 使用している技術の基本的な既知の敵対的脆弱性は何でしょうか？
2. 想定される攻撃のテストと、既存および新規のソリューションの強化により、攻撃に備えるにはどうすればよいでしょうか？
3. 敵対的攻撃を特定するために、どのような監視を行っていますか？

適切な生成AIの活用支援

KPMGは、生成AIアプリケーションを適切かつ効果的に使用するために、組織において安全な使用ガイドラインを作成することを推奨します。ガイドラインには、生成AIを使用したい従業員全員にトレーニングを受けさせ、どのように使用すべきか、使用しないべきかを示すことが含まれます。また、組織は生成AIを他のテクノロジーソリューションと同様に扱い、すでに存在する関連ポリシー（使用許諾ポリシーや情報セキュリティポリシーなど）に従うよう従業員に要求する必要があります。

消費者、従業員、社会の人々、企業とのやりとりに最先端のAIを活用するには、まだやるべきことがあるとKPMGでは考えています。責任あるAIプログラムを導入することで、組織は生成AIの使用にまつわるプロセスや手順の開発を進めることができます。

23　https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/

07 未来には何が起こるのか？

生成AIに関してテクノロジー企業が探究していることをみると、この領域が今後どこへ向かうかのヒントが得られます。

ソフトウェア開発・保守

生成AIは、ソフトウェア開発全体のプロセスを進歩させ、より信頼性の高いソフトウェア製品やサービスをより速く提供できるようにする可能性を示しています。コード生成、保守、バグ修正などのプロセスを完全に自動化できる未来がくると予想されています。

映像制作とバーチャルリアリティ

生成AIは、没入感のあるビデオゲーム環境を作ったり、動画をデザインしたり、あるいはeコマースサイトの商品動画をパーソナライズしたりすることができます。将来的には、企業がバーチャルアシスタントや、ライブ映像に自動的にキャプションを付けるようなライブストリーミングアプリケーションに活用することも可能です。

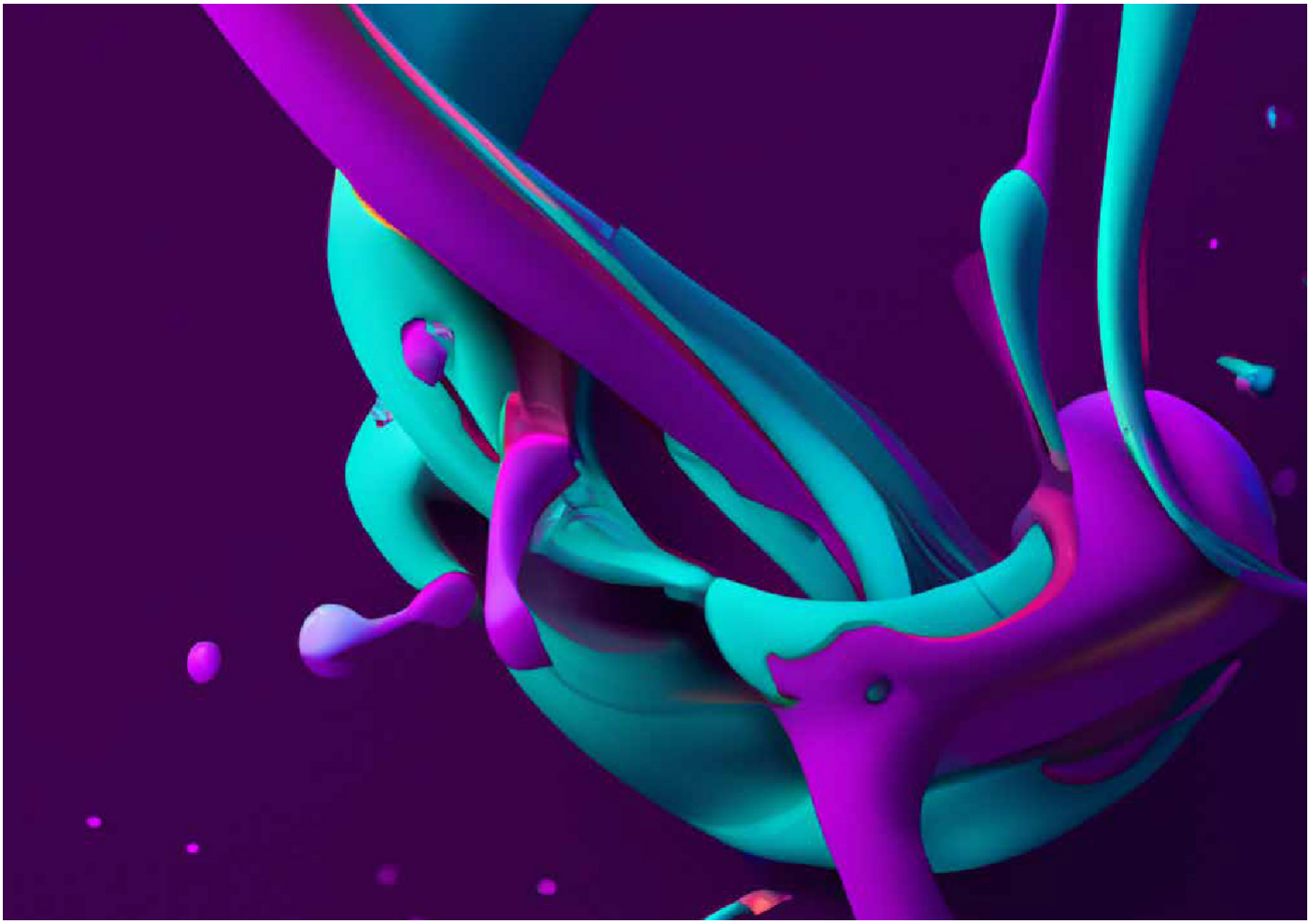
この分野の多くの企業は、現在、企業向けビジネスに焦点を移しています。

メタバース

メタバースでのリアルな3Dアセットを作成するには費用と時間がかかります。生成AIは、テキストから画像や音声に変換した3Dアセットの生成、2D画像からの3Dシーンの生成、あるいは効果音の生成が可能です。また、人間の顔を生成し、メタバースのアバターによりリアルな特徴を与えることもできます。

情報セキュリティの向上

生成AIは、ある脆弱性がどのような重要リスクとなるかを個人に教え、適切なスクリプトの生成や、脅威行為者の攻撃方法を理解することを支援します。



08 KPMGの支援

KPMGは、150年以上にわたって先端テクノロジーの探求と活用を推進し、それらの実装に向けた保証業務の提供とディレクションの役割を果たしています。

KPMG Lighthouseは、データ＆アナリティクス、AI、エマージングテクノロジーのスペシャリスト15,000人以上からなるKPMGの世界的ネットワークで、南北アメリカ、アジア太平洋、ヨーロッパの37ヵ国に拠点を置いています。私たちは、責任あるAIがビジネス、規制、技術の面で複雑な課題であることを理解しています。KPMG LighthouseとKPMGのネットワークを通じて、私たちは企業が責任あるAIを実現することを支援しています。

責任ある生成AIの活用

KPMG Lighthouseは、組織が責任ある、信頼できる、安全なAIソリューションを構築することを支援します。さらにKPMGは、企業のAIおよび機械学習技術における倫理、ガバナンス、セキュリティを評価する責任あるアプローチを取っています。一連のフレームワーク、コントロール、プロセス、ツールのセットは、企業がAIの力を利用し、安全で信頼性があり、倫理的な方法でAIシステムを設計、構築、展開することで、消費者、組織、社会に対して価値を高めるようサポートします。

KPMGの責任あるAIアプローチには以下が含まれます：

1. **公平性：**モデルが公平で、偏見がないことを保証する。
2. **説明可能性：**AIが理解され、文書化され、レビューのためにオープンであることを確実にする。
3. **説明責任：**AIのライフサイクル全体で責任を果たすための仕組みが整っていることを確実にする。
4. **データの完全性：**データ品質、ガバナンス、および信頼性を強化するための手順を実装する。
5. **信頼性：**AIシステムが望ましいレベルの精度と一貫性を持って動作することを確実にする。
6. **セキュリティ：**不正なアクセス、破壊、攻撃から保護する。
7. **プライバシー：**データプライバシー規制と消費者データの使用に関するコンプライアンスを遵守する。
8. **安全性：**AIが人間、知的財産、環境に悪影響を与えないようにする。

お問合せ先

KPMGコンサルティング株式会社

T : 03-3548-5111
E : kc@jp.kpmg.com

kpmg.com/jp/kc

kpmg.com/socialmedia

本冊子で紹介するサービスは、公認会計士法、独立性規則及び利益相反等の観点から、提供できる企業や提供できる業務の範囲等に一定の制限がかかる場合があります。詳しくはKPMGコンサルティング株式会社までお問い合わせください。

Publication name: Generative AI models — the risks and potential rewards in business | Publication number: 138647-G | Publication date: April 2023