HITACHI

信頼できるAIエージェント活用コンサルティング

安全かつ適切な活用で、AIエージェントを信頼できるビジネスパートナーへ

生成AIから発展した「AIエージェント」が注目を集めています。これは、AIエージェントがより人に近い業務を遂行できるだけでなく、人では困難であった業務も実現できる可能性があるためです。例えば、人手では数十時間を要したWeb情報に基づくレポートを数分で作成したり、数千件のビジネス取引の処理を短時間で完了したりすることも可能です。

このように、AIエージェントは人を超える新たなリソースとしてビジネスを根本から変革する可能性を秘めている一方、自律性とそれに伴う自動化に起因して誤判断や倫理的問題、データ漏えいを発生させるといったリスクもはらんでいるため、活用に向けては信頼性を高める必要があります。

日立コンサルティングは、これまでAIガバナンスの構築や生成AIのガイドライン作成など、AI活用の信頼性確保を一貫して支援してきましたが、その支援範囲をAIエージェントまで拡大します。

日立グループにおけるAIエージェントビジネスの展開支援、国や公的機関のプロジェクトにおけるELSI※の研究などの経験とノウハウを生かし、貴社のAIエージェントとの信頼できるパートナーシップの形成を総合的に支援。AIエージェントの信頼性を確保し、ビジネスイノベーションの創出に貢献します。

※ Ethical, Legal and Social Implications/Issues

AIエージェントと生成AIの違い

人が使うことが前提の生成AIに対し、AIエージェントは人に代替するという点で大きく異なります。また生成AIの機能を拡張する形で発展していることから、代替できる業務もより高度なものになり、生産性の飛躍的な向上に期待が寄せられています。

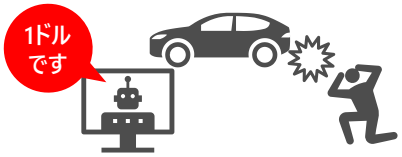
	生成AI	AIエージェント
稼働のきっかけ	プロンプトの入力	目標やプロセスの設定で自律的に稼働
業務での活用	特定の業務データを活用したRAG等の活用	業務システムを直接操作する想定
複合的なタスクへの対応	対話を通して段階的にタスクを実行	目標やプロセスの設定で複合的なタスクを実行
データ活用	学習データやRAG等の外付けデータを活用	インターネットや業務システムにあるデータを活用

RAG：Retrieval-Augmented Generation

AIエージェントのリスク

AIエージェントと生成AIは、その違いから発生リスクも異なります。AIエージェントは、自律性やそれに伴う自動化から、さまざまなリスクを生じさせる可能性があります。

Case 1 ある自動車販売会社で、自動応答のチャットボットが1ドルで自動車を販売しかける事態が発生



Case 2 AIエージェントがメールやクラウド内のデータを自動的にシステム内に読み込んで処理するという特性を狙ったサイバー攻撃が発生

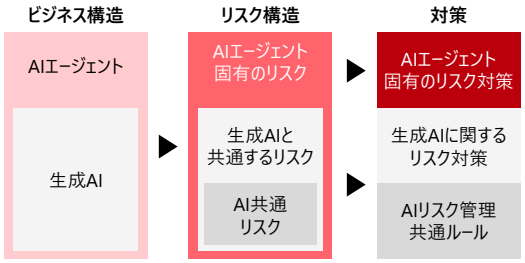
株式会社 日立コンサルティング

こんなお客さまにお勧めします

- ☑ 生成AIの活用を検討し始めたところだが、AIエージェントも含めて安全な活用環境を整備したい。
- ☑ すでに活用している生成AIに加え、今後はAIエージェントも活用したいがリスク面で不安がある。
- ☑ AIエージェントの活用を機に自社のAIガバナンスを見直したい。
- ☑ すでに使い始めているAIエージェントをさらに高度化してマルチエージェントなどの利用を計画しているので、信頼性等の課題を検討したい。

AIエージェントのリスクの考え方

AI、生成AI、AIエージェントに関するリスクの構造は、AI共通、生成AI共通、AIエージェント固有に分かれます。AIガバナンスに関するコンサルティングを提供している当社は、AI共通、生成AIと共通、AIエージェント固有の全てのリスクを考慮した支援はもちろん、生成AIの利用ガイドライン等を整備済みの場合は、AIエージェント固有のリスクを扱う支援のみを提供することも可能です。貴社の状況と要望に合わせ、安全な活用を促すルールの策定で、AIエージェントの信頼性の確保に貢献します。



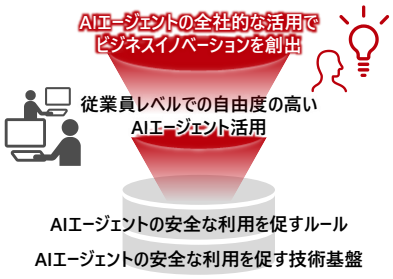
検討プロセス

日々進化しているAIエージェントを取り巻く技術は日々進展していることから、その導入には、段階的な推進と探究的なアプローチが必要です。また、AIエージェントの信頼性を担保するために技術と制度の両面からの対策、エンドユーザーがAIエージェントを作成する可能性への考慮も不可欠です。当社では、探究的なアプローチを含め、活用の検討から普及・啓発に必要な組織の整備まで一貫した支援を提供できます。

活用の検討	ガバナンスの確認	IT環境の確認	ルールの整備	普及・啓発
● AIエージェントのイメージ形成 ● 想定ユースケースの整理	● AIおよび生成AIのルール確認 ● 関連規則等の確認	● 生成AIを含む社内のITインフラおよびセキュリティの確認	● AIエージェントの開発要件検討 ● AIエージェント利用者のルール整備	● 要件に基づいた開発支援 ● ルールに関する研修の開催支援

信頼できるAIエージェントのめざすべき姿

従業員がAIエージェントを自由度高く活用するためには、ルールはもちろん、制度や組織の整備も欠かせません。AIエージェントが貴社のビジネスパートナーとなり、全社的にビジネスイノベーションを創出できるよう、一貫した支援を提供します。



コンサルティング事例

団体A

お客さまの課題	医療機関等における働き方改革を推進するために、医療現場で生成AIの活用を促したいが、セキュリティをはじめとするさまざまなリスクから利用が進まない。
支援内容	医療現場で生成AIを安心して使えるよう、医療分野における法制度、セキュリティ規則等を考慮した上で、生成AIガイドラインの作成を実施。

企業B

お客さまの課題	社内業務を効率化するため、生成AIに加え、AIエージェントの活用を検討しているが、社内システムへのアクセス、自動的な業務処理に懸念がある。
支援内容	想定されるAIエージェントのユースケースを策定し、それに基づくリスクと対策を整理。生成AIのガイドラインに追加する形でドキュメント化。

株式会社 日立コンサルティング

〒102-0083 東京都千代田区麹町2-4-1 麹町大通りビル11F　電話番号(代表)：03-6779-5500
https://www.hitachiconsulting.co.jp/