AI 事業者ガイドライン第 1.2 版改訂：生成 AI 利用者企業が知るべき影響と具体的な対応策

Manus

はじめに

2026 年 3 月末に、総務省および経済産業省が策定する「AI 事業者ガイドライン」の第 1.2 版が公開される予定です。今回の改訂は、AI 開発者や提供者だけでなく、単に生成 AI を業務で利用するだけの「利用者企業」にも、これまで以上に大きな影響を及ぼす内容となっています。特に、自律的にタスクを遂行する「AI エージェント」が新たに規制対象となることで、多くの企業で業務プロセスの見直しや新たなリスクへの対応が不可避となります。

本レポートでは、今回のガイドライン改訂の核心的なポイントを解説し、利用者企業にどのような影響が及ぶのか、そして具体的にどのような対応を講じるべきかを、ステップ・バイ・ステップで詳述します。

1. 何が変わるのか？AI 事業者ガイドライン第 1.2 版の 4 つの主要変更点

今回の改訂で特に重要なのは、以下の 4 つのポイントです。これらは、AI 利用のあり方を根本から変える可能性を秘めています。

変更点	現行版（v1.1）との違い	利用者企業への影響
1. AI 概念の範囲拡大	主にチャットボットのような対話型 AI が念頭に置かれていたが、新たに**「AI エージェント」と「フィジカル AI」**が定義され、規制対象として明記された。	自社で利用中の AI が、意図せず「AI エージェント」に該当し、新たな義務が発生する可能性がある。

変更点	現行版（v1.1）との違い	利用者企業への影響
2. 人間の介在の必須化	AIの自律的な判断・行動に関する明確な規定はなかったが、**「Human-in-the-Loop（HITL）」**の仕組みが事実上必須とされた。	AIが外部に影響を与える操作（例：顧客へのメール送信、発注）を行う前に、必ず人間の承認プロセスを挟む必要が出てくる。
3. ガバナンスの位置づけ	リスク管理の一環という「守り」の側面が強かったが、イノベーションを促進するための**「アクセル（加速装置）」**として再定義された。	ガバナンス体制の構築が、単なるコストではなく、企業の信頼性を高め、より積極的なAI活用を可能にする「攻め」の投資と位置づけられる。
4. 責任範囲の拡大	主にAIサービスの「利用者」としての責任が問われていたが、社内データを用いたRAGシステムの構築やファインチューニングを行うことで、**「開発者」としての責任**を問われる可能性が明示された。	「AIを使っているだけ」という認識では不十分となり、より高度なリスク管理と説明責任が求められるようになる。

> *【用語解説】*
>
> - **AIエージェント**: 特定の目標達成のため、自ら計画を立て、複数のツールやアプリを連携させながらタスクを自律的に実行するAI。
> - **フィジカルAI**: AIの判断をロボットやドローンなどの物理的なデバイスの動作に直接結びつけ、現実世界でタスクを実行するAI。
> - **Human-in-the-Loop (HITL)**: AIの処理プロセスや意思決定の要所に人間が介在し、監視、承認、修正を行う仕組み。

2. 利用者企業への具体的な影響

今回の改訂は、利用者企業に以下のような具体的な影響を及ぼします。

- **業務プロセスの変更**: これまでAIで自動化していた業務フローに、人間の承認ステップを組み込む必要が生じます。これにより、業務のリードタイムが長期化したり、承認者の負担が増加したりする可能性があります。例えば、AIによる見積書作成・送付プロセスは、「AIが作成 → 人間が承認 → 送信」というフローへの変更が求められます。

- **システム対応の必要性**: Human-in-the-Loop を実現するためには、既存システムの改修や、承認ワークフローを管理する新たなシステムの導入が必要になる場合があります。また、誰が、いつ、何を承認したのかを記録する監査ログの取得も必須となるため、そのためのシステム的な手当ても欠かせません。
- **新たなリスクへの対応**: AI エージェントは自律的に動作するため、これまでの生成 AI にはなかった新たなリスクをもたらします。例えば、AI エージェントが社内データベースを参照する過程で機密情報を外部に漏洩させたり、プロンプトインジェクション攻撃によって乗っ取られ、不正な操作を行ったりするリスクです。これらのリスクに対する技術的・組織的な対策が新たに求められます。
- **体制構築と教育コストの発生**: 全社的な AI ガバナンス体制の構築、従業員へのリテラシー教育、法務・IT 部門と連携した相談窓口の設置など、新たな組織体制の構築とそれに伴う教育コストが発生します。

3. 今すぐ始めるべき具体的な対応策：3 つのステップ

ガイドラインの正式公開は 2026 年 3 月末ですが、影響の大きさを鑑みると、今から準備に着手することが賢明です。以下に、企業が取るべき具体的な対応策を 3 つのステップで示します。

Step 1: 現状把握とリスク評価

まず、自社の AI 利用状況を正確に把握することから始めます。

1. **AI 利用状況の棚卸し**: 現在、社内のどの部署で、どのような AI ツール（ChatGPT、Claude、自社開発 AI など）が、何の目的（顧客対応、業務効率化、製品開発など）で利用されているかをリストアップします。
2. **「AI エージェント」該当性の確認**: 棚卸しした AI の中に、自律的に外部への操作を行うなど、「AI エージェント」や「フィジカル AI」に該当する可能性のあるものがないかを確認します。
3. **ギャップ分析**: ガイドライン v1.2 で示された原則（特に Human-in-the-Loop）と、自社の現状との間にどのようなギャップがあるかを分析し、潜在的なリスクを評価します。

Step 2: 社内体制の整備

次に、リスクを管理し、AI を安全に活用するための組織体制を構築します。

4. **AI ガバナンス体制の構築**: 経営層、法務・コンプライアンス部門、IT 部門、そして実際に AI を利用する事業部門の担当者からなる、部門横断的な AI ガバナンス委員会を設置します。この委員会が、全社的な方針決定やリスク管理の責任を担います。
5. **業務フローの再設計**: Human-in-the-Loop の原則に基づき、既存の業務プロセスを見直します。「AI に任せる範囲」と「人間が最終判断を下すべき範囲」を明確に定義し、承認フローを具体的に設計します。
6. **従業員教育の実施**: 全従業員を対象に、新しいガイドラインの内容、社内ルール、AI 利用に伴うリスク（情報漏洩、著作権侵害、ハルシネーションなど）に関するリテラシー教育を実施し、安全な AI 活用の意識を醸成します。

Step 3: 社内ガイドラインの策定・更新

最後に、体制やルールを明文化し、全社に周知徹底します。

7. **基本方針の策定**: 自社が AI を活用する目的、そして「人間中心」「公平性」「透明性」といった遵守すべき基本原則を定義します。
8. **具体的な利用ルールの策定**: 以下のような具体的なルールを盛り込んだ、実用的な社内ガイドラインを作成または更新します。
    - **データ入力のルール**: 個人情報、顧客の秘密情報、未公開の財務情報など、機密性の高い情報を AI に入力することを原則禁止する。
    - **禁止用途の明確化**: 人命に関わる判断、差別を助長する可能性のある業務、非倫理的なコンテンツ生成など、AI の利用を明確に禁止する用途を定める。
    - **出力物の利用ルール**: AI の生成物は必ず人間がファクトチェックを行い、必要に応じて加筆・修正を加えてから利用することを義務付ける。特に、著作権侵害のリスクに留意する。

    - **責任の所在の明確化**: AI の利用によって問題が発生した場合、その最終的な責任は AI ではなく、それを利用・承認した人間および組織が負うことを明記する。
9. **相談窓口の設置**: AI の利用に関する疑問や懸念が生じた際に、従業員が気軽に相談できる窓口（例：IT 部門や法務部門）を設置し、その存在を周知します。

まとめ

2026 年 3 月末に予定されている「AI 事業者ガイドライン」第 1.2 版の改訂は、単なる努力義務の追加ではありません。これは、企業が AI とどう向き合い、その恩恵を享受しながらリスクを管理していくかという、AI 時代の新たな「事業の OS」を定義するものです。罰則がないからといって対応を軽視すれば、取引先からの信頼失墜、ブランドイメージの毀損、そして将来的には国際競争からの脱落といった、より大きな代償を払うことになりかねません。

本レポートで示したステップを参考に、ぜひ早期に自社の AI ガバナンス体制の見直しに着手してください。ガイドライン改訂を単なる「規制」と捉えるのではなく、自社の AI 活用を加速させる「好機」と捉え、戦略的に取り組むことが、これからの時代を勝ち抜く鍵となるでしょう。

参考資料

- 【2026 年 3 月最新】AI 事業者ガイドライン改定とは？AI エージェント時代に企業が押さえるべき新ルール | MIRAINA ブログ
- 2026 年 AI 事業者ガイドライン改訂は、生成 AI 利用者にどう影響するか？ | Felo AI
- AI 事業者ガイドライン改定案（第 1.2 版）の深堀分析 | Perplexity
- 【2026 年最新】生成 AI 規制 日本の現状｜企業が今すべき 5 つの対応 | 株式会社 Uravation
- AI 事業者ガイドライン検討会 | 総務省