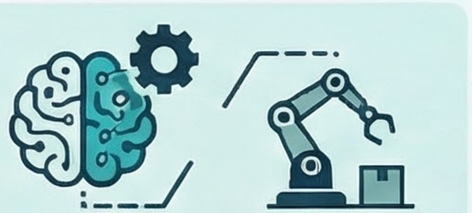
2026年 AI事業者ガイドライン改訂：生成AI利用者が知っておくべき「新ルール」

2026年3月のガイドライン改訂（v1.2）による主要な変更点と、企業が取るべき具体的アクションを簡潔に伝える。
AIのビジネス利用が本格運用フェーズに入り、新たな基準が示されています。

ガイドライン改訂（v1.2）の3大重要ポイント



「AIエージェント」と「フィジカルAI」の定義

自律的にタスクを遂行するシステムや物理動作を伴うAIが新たに規制対象となります。

「Human-in-the-Loop（人間の介在）」の必須化

クリティカルな意思決定には必ず人間の承認を介在させることが求められます。

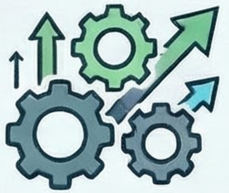
日本のAI規制「三本柱」の現状

柱	名称	現状
法律	AI推進法	2025年9月に全面施行済み
国家計画	人工知能基本計画	2025年12月に閣議決定済み
ガイドライン	AI事業者ガイドライン	2026年3月末にv1.2公開予定

「利用者」から「開発者」への責任拡大

RAGや追加学習を行う利用者は、モデルの安全性確保に対する重い責任を負います。

生成AI利用者が今すぐ取り組むべき3つのアクション

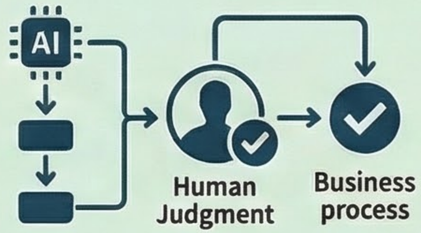


AI利用状況の棚卸しとリスク評価

社内のAI活用状況をリスト化し、ハルシネーションや情報識漏のリスクを洗い出します。

AI利用ポリシーの策定・更新

入力データの制限や出力結果の検証プロセスを明記した社内ルールを整備します。



「人間の判断」を組み込む業務フロー設計

AIエージェント導入時、人間が最終確認を行うタイミングを業務フローに設計します。