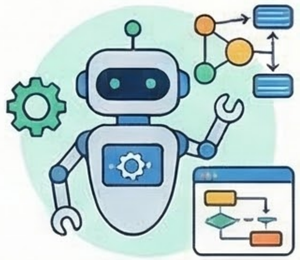
2026年「AI事業者ガイドライン」改訂：企業に求められる新ルールと3ステップの対応策

2026年3月のガイドライン改訂（第1.2版）により、生成AIの単なる「利用者」であっても、AIエージェントの活用や独自データの利用（RAG等）に応じて、開発者と同等の重い責任とガバナンス体制が求められるようになります。

ガイドライン改訂による3つの主要な変化

Human-in-the-Loop（HITL）の事実上必須化

AIの判断に対し、人間が必ず監視・承認を行うプロセスの構築が求められます。



「AIエージェント」が新たに規制対象へ

自律的にタスクを遂行するAIも対象となり、意図しない活的機能が生じる可能性があります。

利用者から「開発者」への責任拡大

RAGやカスタマイズを行う企業は、より高度なリスク管理と説明責任を問われます。

現行版（v1.1）と改訂版（v1.2）における定義と責任の比較

項目	現行版（v1.1）	改訂版（v1.2）
対象AI	主にチャット型AI	AIエージェント・フィジカルAI
承認プロセス	明確な規定なし	HITL（人間の介在）が必須
ガバナンス	「守り」のリスク管理	信頼性を高める「攻め」の投資

今すぐ着手すべき「3ステップ」の対応策

Step 1：現状把握とギャップ分析

社内のAI利用状況を棚卸しし、新基準との乖離やリスクを正確に評価します。

Step 2：ガバナンス体制とフローの再設計

部門横断の委員会を設置し、人間が最終判断を下す承認フローを構築します。

Step 3：社内ルールの明文化と教育

禁止事項や責任所在を明記したガイドラインを策定し、全社員へ教育を実施します。