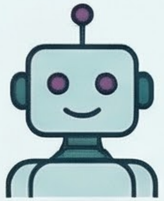
2026年 AI事業者ガイドライン改訂：企業が守るべき「AIエージェント」運用の新ルール

2026年、日本のAIガバナンスは「試験導入」から「本格運用」へ移行。最新ガイドライン（第1.2版）で自律的な「AIエージェント」が規制対象となり、システム設計や契約実務に根本的変更を要求。

自律型AIに求められる「人間による承認ゲート」

AIエージェント



フィジカルAI

AIエージェントとフィジカルAIが規制対象に

自律的に計画・実行するAIや、物理空間を制御するAIが明文化されました。

人間の判断必須（Human-in-the-Loop）の義務化

外部への送金、投稿、機器操作の前に必ず人間の承認が必要です。

AIによる完全自動化（STP）

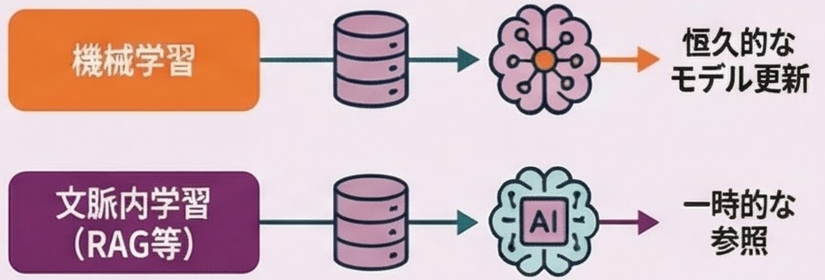
HITL型業務フロー

自動化かる「HITL型」業務フローへの転換

日本とEUのAI規制アプローチの決定的な違い

比較項目	日本（AI推進法＋ガイドライン）	欧州連合（EU AI Act）
法的性質	ソフトロー中心（柔軟な運用）	ハードロー（強行法規・厳罰）
主な制裁	行政指導・実名公表（信用失墜）	巨額の制裁金（売上高の最大7%）
規制対象	利用者の行動指針を提示	AIシステムをリスク則に分類

データ戦略と法的リスクの新基準

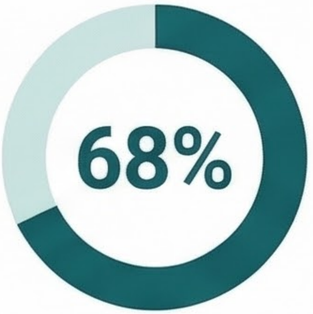


「機械学習」と「文脈内学習（RAG等）」の厳密な区別

恒久的なモデル更新と、一時的な参照を契約上で明確に分ける必要があります。

実名公表（ネーム・アンド・シェイム）のリスク

直接の罰則はなくとも、ガイドライン違反による実名公表は社会的死を意味します。



68%の事業者がエージェント活用を視野に

多くの企業が導入を検討する中、高度なガバナンス構築が競争力の源泉となります。