2026年 AI事業者ガイドライン改訂の要点：AIエージェント時代の「人間の介在（HITL）」

2026年3月予定の改訂（v1.2）では、対象が「AIエージェント」と「フィジカルAI」へ拡大。「Human-in-the-Loop」が必須となります。

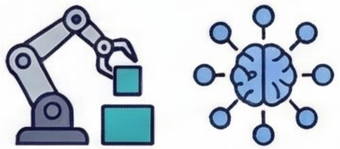
ガイドラインv1.2：対象拡大と「人間の介在」の義務化

現行版 (v1.1)

Web上の生成AI中心

改定版 (v1.2)

対象が「AIエージェント」と「フィジカルAI」へ拡大



「Human-in-the-Loop (HITL)」の必須化

自律的に計画・実行し、物理的なデバイスを操作するAIが正式に規制対象。外部への影響や重要変更の前に、必ず人間の承認を挟むプロセスを構築。

ガバナンスは「イノベーションの加速装置」

規制による禁止ではなく、適切なガードレールを設けることで安全な活用を促進。

項目	現行版 (v1.1)	改定版 (v1.2)
AIの範囲	 Web上の生成AI中心	AIエージェント、フィジカルAIを追加
自律的な判断	 明確な規定なし	 人間の判断（HITL）を明記
ガバナンス	 リスク管理の一環	 イノベーションの「加速装置」

企業が直面するリスクと必須アクション

自律型AIに伴う新たなリスク要因

不正操作

ハルシネーション アクセス

物理的損害

安全事故への備え

HITLを組み込んだ業務プロセスの再設計

承認フローのシステム化、最小権限の適用、監査ログの自動取得体制を構築。

社内規定の策定と従業員教育

- 入力ルールの厳格化
- 禁止用途の定義
- 人間によるファクトチェックの義務化を徹底。