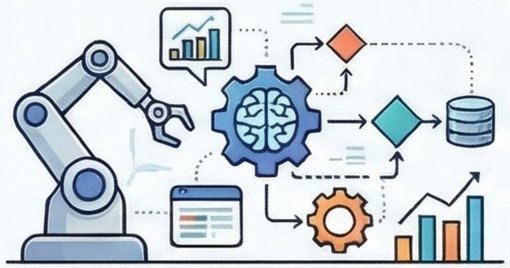
2026年AI事業者ガイドライン改訂：生成AI利用者に求められる「実務対応」の要点

2026年のガイドライン改訂案では、AIエージェントやフィジカルAIといった「自律型AI」が明確に対象に含まれます。
利用者は単に結果を確認するだけでなく、ガバナンス（統制設計）を業務フローに組み込むことが「前提」として求められるようになります。

ガイドライン改訂に伴う「3つの本質的変化」

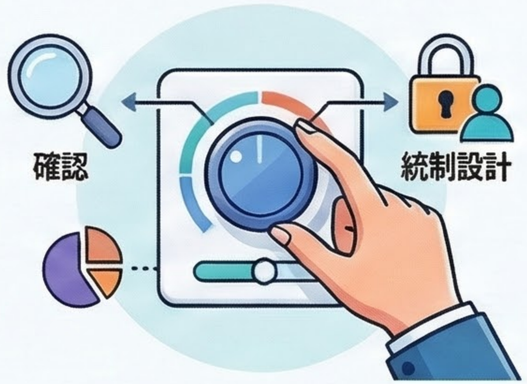


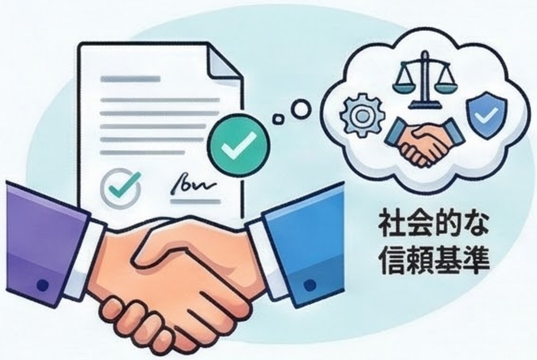
自律型AI（エージェント・フィジカルAI）への適用拡大

業務フローに組み込まれた自律性の高いAIの統制が不可欠となります。

「確認」から「統制設計」へのパラダイムシフト

人間の判断の介在、ログ記録、最小権限の設定が運用の前提となります。





“共通言語”の更新による期待水準の向上

法的罰則よりも、調達や監査における社会的な信頼基準がアップデートされます。

実務担当者が取り組むべき優先アクション

ユースケースの棚卸しと役割の明確化

自社が「利用者」か「提供者」かを再定義し、責任分界点を明確にします。

入力データの統制と学習利用設定の確認

個人情報・機密情報の入力制限と、ベンダーの学習利用設定の点検を行います。

人間の判断を介在させる「レビュー工程」の設計

特に重要領域では、AIの出力を人間が最終確認するフローを標準化します。

主要な生成AI提供者のデータ取扱い方針（利用者側の確認ポイント）

提供者	学習利用（企業向け）	ログ保持の例
OpenAI	既定で学習に使わない	API乱用監視ログ：最大30日
Microsoft	基盤モデル学習に使用しない	商用Copilotでのデータ保護を明示
AWS (Bedrock)	プロンプト等を学習に使わない	組織単位でのオプトアウトが可能