2026年3月改訂「AI事業者ガイドライン」：生成AI利用企業に求められる新基準と対応策

2026年3月末に改訂予定の「AI事業者ガイドライン（第1.2版）」は、AIを自社開発しない「利用者企業」に対しても、実務上の期待水準を大きく引き上げます。
義務ではないものの、事故時の説明責任や取引先からの信頼を担保するための「合理的な注意」の参照点となります。

利用企業が守るべき「7つのコア要項（U-2〜U-7）」

「人間の介在（HITL）」の必須化

採用や与信などの重要判断にAIを使う際、人間の最終確認と説明責任が求められます。

入力データの厳格なガバナンス

プロンプトへの個人情報・機密情報の入力制限と、ベンダーの学習利用設定の確認が必要です。

透明性とステークホルダー対応

AI利用の有無を明示し、外部からの問い合わせや異議申し立てへの窓口設置が求められます。

短期（〜4週間）で優先すべき5つのアクション

入力禁止ルールと技術的ガードの設置

個人情報や営業秘密の入力を禁止し、技術的に検知・遮断する仕組みを導入します。

利用ケースの棚卸しとリスク分類

自社でのAI利用状況を可視化し、リスクの高さに応じた承認フローを構築します。

ベンダー契約・規約の再点検

AIベンダーがデータを学習利用していないか、保持期間や責任分担を再確認します。

リスク領域と求められる緩和策

リスク領域	具体的なリスクシナリオ	求められる緩和策
法的・個人情報	プロンプトへの個人情報入力による漏えい	入力禁止ルールの徹底と学習OFF設定
運用・ハルシネーション	AIの誤回答に基づく業務上の重大な誤判断	重要判断における人関承認（HITL）の義務化
レビュテーション	AI利用の非開示や差別的な出力の生成	利用表示のガイドライン化と問い合わせ窓口設置