2026年3月末 正式公開予定

AI事業者ガイドライン 第1.2版改訂

生成AI利用者企業が知るべき影響と対応策

Manus

今回の改訂が「利用者企業」にも無関係ではない理由

これまでのガイドラインは「開発者」や「提供者」が主役でした。
しかし、第1.2版では**「AIエージェント」**が新たに規制対象となります。

Impact 単にChatGPTやClaudeを業務で利用するだけの企業も、業務プロセスの見直しや体制整備が求められます。

Risk 罰則はありませんが、対応を怠れば**取引先からの信頼失墜**や**ブランド毀損**のリスクに直結します。

日本のAI規制の3本柱

柱	名称	状況
法律	AI推進法 基本法（罰則なし）	施行済
国家計画	人工知能基本計画 閣議決定	決定済
ガイドライン	**AI事業者ガイドライン** ソフトロー（任意）	2026/3末

第1.2版の4大変更点：利用者企業への影響は大きい

01 AI概念の範囲拡大

「AIエージェント」と「フィジカルAI」が新たに定義・規制対象化。

> **影響:** 自社利用AIが意図せず「AIエージェント」に該当し、義務が発生するリスク。

02 Human-in-the-Loop (HITL) 必須化

AIが外部に影響を与える操作を行う前に、人間の承認プロセスを挟む仕組みが必須に。

> **影響:** 自動化フローの見直しと、承認プロセスの追加が必要。

03 ガバナンスの位置づけ転換

「守り（リスク管理）」から「攻め（イノベーション促進）」へ再定義。

> **影響:** ガバナンス体制構築が、企業の信頼性向上への戦略的投資となる。

04 責任範囲の拡大

RAG構築やファインチューニングを行う場合、「開発者」としての責任が発生。

> **影響:** 「使っているだけ」では済まされず、高度な説明責任が求められる。

「AIエージェント」とは何か：利用者企業が特に注意すべき新概念

DEFINITION

目標を与えられると自ら計画を立て、複数のツールを連携させながらタスクを自律的に実行するAI

用途	具体例	該当リスク
業務自動化	メール自動返信・仕分け・送信	誤送信・情報漏洩
情報収集	Web情報収集 → レポート自動生成	著作権侵害・誤情報拡散
社内支援	社内DBを参照した自動回答	機密情報漏洩
購買・発注	在庫状況に応じた自動発注	誤発注・不正操作

Human-in-the-Loop（HITL）の必須化：業務フローが変わる

具体的な業務フローの変化

業務例	現在のフロー		v1.2対応後のフロー
見積書作成・送付	AI生成 → 自動送信	→	AI生成 → **担当者が内容確認** → 送信
顧客問い合わせ対応	AI自動返信	→	AI下書き → **人間が修正・承認** → 返信
発注・購買処理	在庫連動で自動発注	→	発注案作成 → **購買担当者承認** → 発注

システム対応：HITLの実現には「誰が・いつ・何を承認したか」を記録する**監査ログ**の取得も必須となります。

利用者企業への4つの具体的影響：コストと体制変更を見込む

業務プロセスへの影響

- 自動化フローに**承認ステップ**が追加
- 業務リードタイムの長期化
- 承認者の業務負担が増加
- 一方でミスや不正の防止機能が強化される

システム対応の必要性

- HITL実現のための既存システム改修
- 承認ワークフロー管理システムの新規導入
- **監査ログ**（誰がいつ承認したか）の取得・保存

新たなリスクへの対応

- AIエージェント特有の機密情報漏洩リスク
- **プロンプトインジェクション**攻撃への対策
- 誤動作による不正操作の防止

体制構築・教育コスト

- 全社的なAIガバナンス体制の構築
- 従業員への**リテラシー教育**
- 法務・IT部門との連携体制整備
- 組織的な対応コストの発生

対応策 Step 1：現状把握とリスク評価から始める

「自社のAI利用状況を正確に把握する」ことがすべての出発点です。
IT部門が把握していない**「シャドーAI」**の発見も重要課題となります。

01 AI利用状況の棚卸し

社内のどの部署で、どのAIツール（ChatGPT・Claude・自社開発AI等）が、何の目的で使われているかをリストアップします。

02 「AIエージェント」該当性の確認

棚卸ししたAIの中に、**自律的に外部への操作**（メール送信・データ書き込み・外部API呼び出し等）を行うものがないかを確認します。

⚠ 該当する場合は優先的に対応が必要です

03 ギャップ分析の実施

ガイドラインv1.2の原則（特に**Human-in-the-Loop**）と自社の現状を照らし合わせ、リスクの高い業務から優先順位をつけて対応計画を策定します。

対応策 Step 2：社内体制の整備で「ガバナンスの骨格」を作る

AIガバナンス体制の構築

経営層・法務・IT・事業部門による**部門横断的な委員会**を設置。

全社的な方針決定とリスク管理の責任を一元化し、現場任せにしない体制を作る。

業務フローの再設計（HITL）

「AIに任せる範囲」と「人間が判断する範囲」を明確に定義。

特に**外部への影響が大きい業務**（発注・契約等）は、人間の承認プロセスを必須化する。

従業員教育の実施

全従業員を対象に、ガイドラインやリスク（情報漏洩・著作権等）に関する**リテラシー教育**を実施。

管理職と一般社員で内容を分け、実効性を高める。

対応策 Step 3：社内ガイドラインの策定・更新で「ルールを明文化」する

基本方針

AI活用の目的と「人間中心」「公平性」「透明性」等の**基本原則**を定義する。

出力物の利用ルール

AI生成物は必ず人間が**ファクトチェック**を実施。著作権リスクにも留意する。

データ入力ルール

個人情報・顧客秘密情報・未公開財務情報等の**機密データの入力**を原則禁止する。

責任の所在

問題発生時の最終責任はAIではなく、利用・承認した**人間・組織**が負うことを明記。

禁止用途

人命に関わる判断・差別助長・非倫理的コンテンツ生成等を**明確に禁止**する。

相談窓口

疑問・懸念が生じた際の相談先（IT部門・法務部門等）を設置し、**全社に周知**する。

ガイドラインは策定して終わりではなく、技術進化に合わせて定期的に見直す仕組みが重要です。

まとめ：ガイドライン改訂を「攻め」の好機と捉えよ

ガイドライン改訂を単なる「規制」ではなく、
自社のAI活用を加速させる「戦略的投資」の機会と捉える。

STEP 1

現状把握と リスク評価

・AI利用状況の棚卸し
・AIエージェント該当性確認
・ギャップ分析

STEP 2

社内体制の 整備

・部門横断委員会の設置
・HITL業務フロー再設計
・従業員リテラシー教育

STEP 3

社内ガイドライン 策定・更新

・ルールの明文化
・相談窓口の設置
・定期的な見直し

戦略的に取り組むことが、これからの時代を勝ち抜く鍵となる

出典：総務省 AI事業者ガイドライン検討会（第29回、2026年2月16日）