

信号機ルール：AIに入れていい情報・いけない情報

組織でAIを使い始めるときの最初のルール（たたき台）

更新日：2026-10-03（2026年10月時点の情報） | HUMAC 伊藤晴通

AIを使い始めるとき、最初に決めるべきは「どの道具を使うか」ではなく「何を入れてよいか」。ルールがないのは悪いことではない。今日決めればいい。

信号機ルール（たたき台）

区分	例	扱い
● 青	公的資料（統計・制度の公募要領）、公開されている業界情報、自社のチラシ・告知文の文案、一般的な質問	無料版でもOK
● 黄	業種・規模だけにした相談内容、事業計画の骨子、社名や個人名を伏せた議事録	有料版で「学習に使わない」設定を確認してから
● 赤	決算書・申告書、個人名・住所・電話番号、借入や取引の状況、マイナンバー、健康情報	組織契約とルール整備が済むまで入れない

あわせて決めておく5つのこと

1. 使ってよいサービスとプラン（個人の無料アカウントで業務をしない、など）
2. 学習利用の設定（有料版でも「学習に使わない」設定を全員が確認する）
3. 出力の確認責任（AIの回答は必ず人が確認し、出典を開く）
4. 送信・公開は人が押す（AIエージェントに任せても、外に出る操作は人が承認する）
5. 困ったときの相談先（入れてしまった、漏れたかもしれない、をすぐ言える窓口）

よくある落とし穴

👍👎 ボタン

個人アカウントのGemini Notebookで評価ボタンを押すと、その会話と資料が人の確認に回り、最長3年保存される。業務の会話では押さない。

低価格プラン

ChatGPTの無料版・Goは、初期設定で入力学習対象。設定を変えるか、業務では使わない。

鍵の管理

AIを使うための鍵（APIキー・パスワード）を資料やチャットに書かない。講師自身、鍵の漏えいで約6万8千円の不正請求を受けた。

便利さと事故は、同じ入口から来る

AIエージェントは自分で動く分、「頼んでいない相手にメールを送る」「見せるべきでない情報にアクセスする」といった権限のはみ出しが起きやすい。任せる範囲と、人が止める場所（ガードレール）を先に決める。