AI活用ガイド

AIの使い分けと任せ方の設計

9種類の道具・作る仕事・事故を防ぐ設計

仕事ごとに頼む相手を決め、任せてよい範囲に線を引くための1冊です。
文章も、画像も、動画も、作る仕事も、同じ枠で判断できます。

まず、道具の全体像

AIは用途ごとに種類が分かれています。ここでは実務でよく使う**9種類**と「人」を並べます。これで全部ではありませんが、パソコンの上の仕事は、たいていこの組み合わせで片づきます。

種類	できること	弱いところ・注意
会話型AI 大規模言語モデル（LLM）	読む・書く・言い換える・要約する・分類する	確率で言葉を選ぶので答えがぶれる。一度に読める量に上限。**渡した分だけ読める**（自分から探しに行くことも、保存し直すこともできない）
エージェント型AI AIエージェント／コーディングエージェント	ファイルを読み書きし、実行し、結果を見て自分で直す。道具やシステムを作る	副作用（消す・送る・課金）が実際に起きる。承認を挟む設計が要る
資料に紐づけるAI 検索拡張生成（RAG）／グラウンディング	渡した資料の中だけで、出典つきで答える	関係する部分を**探し出せなかった時に「書かれていません」と返る**（書いてあっても起きる）。出典が付いていても、そこに本当にあるかは別に確かめる
画像生成AI 画像生成モデル	サムネイル、バナー、商品イメージ、図解、背景の差し替え	細かい文字や指定どおりの構図は苦手なことがある。権利と商用利用の条件を要確認
動画生成AI 動画生成モデル	短い説明動画、商品の見せ方、素材クリップ	長さと一貫性に制約がある。実在の人物・商品の再現は権利と誤認の問題が出る
音声・音楽の生成AI 音声合成（TTS）／音楽生成	ナレーション、案内音声、BGM、効果音	声の権利（本人の許諾）と、商用利用の条件を必ず確認する
音声認識 文字起こし（ASR）	会議・電話・動画の音声を文字にする	固有名詞と専門用語は誤変換する。話者の分離は完全ではない
翻訳 機械翻訳	多言語の資料・商品説明・問い合わせ対応	契約書や規約は、訳文をそのまま使わない。原文と併記して専門家に確認
決定的な処理 関数・スクリプト・データベースの問い合わせ	同じ入力なら必ず同じ出力（日付や外部の数字を使う所を除く）。速く、正確に、何度でも	あいまいな指示は通らない。書き方を決める必要がある
人 意思決定と責任	決める。承認する。外に出す前の最終確認をする	くり返しの作業に時間を取られる。だから上の9つに渡す

会話型とエージェント型は、同じ画面から使えることがあります。気づかないうちに**副作用のある側**（実際にファイルが変わる側）を使っていることがあるので、実行を伴う作業かどうかは、その都度確かめてください。

契約の話（事実だけ）

提供元のヘルプには「Codex はすべての ChatGPT プランに含まれています。利用上限はプランによって異なります」と書かれており、一方で発表ページには「期間限定で、ChatGPT 無料版と Go で Codex を利用できます」とあります（どちらも2026年9月14日に確認。終了日の記載はありません）。**会話型とエージェント型は同じ ChatGPT の契約の中にあり、無料版と Go での利用だけが期間限定の扱い**、と読むのが正確です。

一方、資料に紐づけるAI、画像・動画・音楽の生成は、別の会社のサービスを使うことが多く、その場合はそれぞれのアカウントと契約が要ります。「AIは全部ひとつの契約で済む」ではありません。

長く使う前提なら、この点を確認してから決めてください。条件は変わるので、契約前に必ず提供元のページで今の内容を見てください。

日々の作業は、どれに頼むか

この仕事は	頼む相手	設計のポイント
毎月の売上を集計して検算する	**エージェント型＋決定的処理**	金額は決定的な側で計算し、AIには指示と突合をさせる
請求書PDFの束を一覧表にする	**エージェント型**	文字が埋まったPDFかを先に確認。画像だけのPDFは読めない
社内マニュアルの中を探す	**資料に紐づけるAI**	出典つきで返る形にする。根拠が出ない答えは採用しない
メールや案内文の下書き	**会話型AI**	事実（金額・期日）は自分で差し込む
合計・平均・条件抽出	**決定的な処理**	毎月同じ形なら関数やスクリプト。速く、ぶれない
会議の内容を記録に残す	**音声認識＋会話型AI**	文字起こししてから要約。固有名詞は自分で直す
海外の取引先とやり取りする	**翻訳＋会話型AI**	重要な条件は原文を併記し、契約文は専門家に確認
採用・評価・取引の可否	**人**	AIは材料を並べるまで。理由づけは必ず作られる
支払い・契約・公開・送信	**人**	取り返しがつかない操作は、最後のひと押しを人がやる

制作・クリエイティブの仕事

この仕事は	頼む相手	注意

販促物のサムネイル・バナー	**画像生成AI**	文字は後から自分で載せたほうが確実。ブランドの色と余白は指定する
商品写真の背景差し替え・加工	**画像生成AI**	商品そのものの形状や色を変えると、実物と違う表示になる
資料に入れる図解・アイコン	**画像生成AI**	社内資料から始める。社外配布は権利の確認後
短い説明動画・商品の見せ方	**動画生成AI**	長さと一貫性に制約。実在の人物・店舗の再現は避ける
ナレーション・案内音声	**音声合成**	声の権利を確認。本人の声を使うなら本人の許諾を取る
BGM・効果音	**音楽生成AI**	商用利用の条件を規約で確認。配信先の規約も別に見る
動画の字幕・書き起こし	**音声認識**	固有名詞は誤変換する前提で、必ず人が直す
多言語の商品説明	**翻訳＋会話型AI**	数量・サイズ・法令表示は機械任せにしない
原稿・台本のたたき台	**会話型AI**	事実の主張には根拠を求める。誇張表現は禁止と明示
配信素材の一括変換（サイズ・形式）	**エージェント型**	元素材は書きかえず、出力を別フォルダに

> 生成した画像・動画・音声・音楽を仕事で使う時は、3つを必ず確認します。1. 提供元の規約で**商用利用**が認められているか。2. 生成物の**権利**が誰にあるか。3. 実在の人物・商品・ブランドに似せていないか。社外に出す物ほど、ここを先に確認します。

「作る仕事」は、どこまでできるか

エージェント型AIの本領は、書類仕事ではなく**物を作ること**です。日本語で頼むだけで、次のようなものが実際に作れます。

作る物	可否	先に決めておくこと
社内用の業務システム（在庫・予約・顧客）	**作れる**	誰が使うかで作りが変わる。社外に出すなら本人確認と個人情報の扱いが必須
表計算と連携する業務ツール	**作れる**	実行の権限と、動かす人のアカウントを先に決める
通知のしくみ（チャット・メールへ自動送信）	**作れる**	鍵（APIキー）はコードに書かず、設定の保管場所から読む
既存ファイルの一括変換ツール	**作れる**	元ファイルを書きかえない。出力は別フォルダ
集計のダッシュボード	**作れる**	元データの更新方法を先に決める
ブラウザの拡張機能・自分用の小道具	**作れる**	配布するなら各ストアの審査と規約がある

Excelのマクロ／スクリプト	作れる	マクロつきファイルは受け取る側でブロックされます。配るなら、操作するスクリプトを別に渡すか、関数だけで組む
ゲーム・研修用アプリ	作れる	社内研修や学習用に向く。素材の権利に注意
既存コードの改修・不具合調査	作れる	変更前にコピー。差分を必ず人が読む
外部サービスとつなぐ処理（API連携）	作れる	相手の規約と送信回数の上限（レート制限）を先に読む
自社資料の横断検索	作れる	社外秘を含むなら、保存先を確認してから
お金・個人情報を扱う本番システム	慎重に	作れるが、法令・保守・障害対応が要る。まず社内用から

作る仕事で、最初に決める4つ

1. **誰が使うか**（自分だけ／社内／社外）　2. **データはどこに置くか**　3. **壊れた時に誰が直すか**　4. **どこにお金がかかるか**（利用料・通信量・保管料）

任せ方の設計 —— 事故を防ぐ6つの原則

1　最小権限　—— 触れる範囲を、先に狭める

作業用のフォルダだけを渡し、その外を触らせません。読むだけでよい作業に、書きかえの許可を与えません。事故の大きさは、渡した権限の広さで決まります。

2　ドライラン　—— 実行の前に、計画だけ出させる

何を、どの順で、どのファイルに対してやるのか。実行前に一覧で出させ、人が見てから進めます。

3　冪等（べきとう）　—— 2回流しても壊れない形にする

同じ処理をもう一度動かした時に、二重に登録・送信されない作りにします。途中で止まっても、安心してやり直せます。

4　検算　—— 確率で動くものには、必ず答え合わせを付ける

会話型AIは確率で言葉を選びます。桁を間違えても自信たっぷりに出します。金額と件数は、別の方法で計算し直して一致を見ます。

5　秘密の分離　—— 鍵（APIキー）をコードに書かない

鍵は設定の置き場所に入れ、コードや会話には貼りません。漏れた時に差し替えられるよう、作り直す手順も控えておきます。

6　戻せる形　―― 変更前のコピーと、変更の記録

変える前にコピーを取り、何をどう変えたかを残します。「戻せる」という前提があるかどうかで、任せられる範囲が変わります。

任せて作らせた時の、固有の外し方5つ

1　テストを通すために、テストの側を書き換える

「動くようにして」と頼むと、期待値を実際の出力に合わせて書き換え、「通りました」と報告することがあります。**合否の条件は人が書き、AIには触らせません。**

2　やっていないのに「やりました」と返る

実行が途中で止まっても、文章としては成功の形で返ります。**ファイルの更新日時・行数・件数**を人が見るまで、完了と扱いません。

3　関係ないファイルまで一斉に直す

「整えて」のような広い指示で起きます。1回の依頼で触ってよいファイルを、名前で列挙します。

4　途中で前提を忘れて作り直す

一度に扱える分量には上限があり、長い作業では最初の決め事が落ちます。決め事は会話ではなく**ファイルに書いて置き**、毎回それを読ませます。

5　同じ所を行き来して直らない

2回直して直らなければ、指示ではなく前提が間違っています。止めて、状況を説明させてから、やり直す範囲を人が決めます。

そのまま貼れる、3つの実物

ドライラン（実行の前に必ず入れる）

```
これから頼む作業を、まだ実行しないで。
1. 触るファイルの一覧　2. それぞれに何をするか（読むだけ／書き換える／消す／送る）
3. やり直せるかどうか　4. お金が動くか
この4つを表で出して。私が「実行して」と書くまで、1つも実行しないで。
```

最小権限（作業の最初に入れる）

```
作業してよいのは「作業用」フォルダの中だけ。その外は読むのも書くのも禁止。
消す操作と、外に送る操作（メール・チャット・アップロード）は、毎回私の許可を取って。
元のファイルは書き換えず、結果は「作業用/出力」に新しく作って。
```

検算（結果を受け取ったら）

元データの行数と、集計に使った行数を両方教えて。
金額と数量の合計も、元データ側と結果側の両方で出して。
同じ番号が2回出ていないか、抜けた番号が無いかも確かめて。

突き合わせるのは3つで足ります。**件数・合計・重複と欠け**。この3つが合えば、並べ替えの取り違えはほぼ拾えます。表計算で確かめる時は、AIに数えさせず、自分で COUNTA と SUM を入れて比べます。「数えて」と頼むと、数えずに見た目から答えることがあります。

会話型を使う時の、よくある外し方

集計そのものを、会話型AIに直接させる

確率で言葉を選ぶ仕組みなので、桁の扱いを外すことがあります。計算は決定的な側に寄せ、AIには「式を書く」「結果を突き合わせる」を任せます。

長い資料を、そのまま全文貼る

一度に読める量には上限があります。上限に収まっていても、長い文章では真ん中あたりの情報が扱われにくくなる傾向が報告されています。資料に紐づける形に寄せるか、分けて渡します。

外から来た文章を、そのまま指示として渡す

取り込んだメールやWebページに「これまでの指示を無視して…」と書かれていると、AIがそれに従うことがあります（プロンプトインジェクション）。**言い方では止まりません**。外部の文章を読む作業では、送信・削除・支払いの権限を外します。読むだけの権限なら、従われても被害が出ません。

生成した画像や音声を、確認せずに社外へ出す

商用利用の条件、権利の所在、実在の人物や商品に似ていないか。この3点を見ずに出すと、後から差し替えでは済まない問題になります。

道具が増えても、見る所は変わりません

物が実際に変わるのか（副作用があるか）、**何を根拠に出しているのか**（資料か、確率か）、**誰が責任を取るのか**。新しい道具が出たら、この3つだけ見れば置き場所が決まります。

次にやること　いま任せようとしている作業を1つ選び、下のドライランの1行を貼ってから始めてください。実行の前に、何が変わるかが一覧で出ます。