

ChatGPT・Gemini・Gemini Notebook・Claude 比較表

4つのAIの性格・得意なこと・無料でできること／有料でできること

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

覚え方のコツ：バージョン番号ではなく「性格」で覚える

AIのモデル名や番号は数ヶ月ごとに変わります（たとえば2026年9月には、OpenAIがGPT-6のAstra・Sol・Lunaを、GoogleがGemini 3.8 Flashを出しました。10月7日にはAnthropicが小型のClaude Haiku 5.5、OpenAIもChatGPTにGPT-6を広げ、無料版・GoはLuna、有料版はSolが使われます）。どのAIが「どんな仕事」が得意な同僚かをつかんでおけば、名前が変わっても迷いません。

スマホでQRを読み取ると、そのままAIが開きます（ログインはご自身のGoogleアカウント等で）



ChatGPT

chatgpt.com



Gemini

gemini.google.com



Gemini Notebook

notebook.google.com



Claude

claude.ai

アプリ版（App Store／Google Play）を入れておくと、次からはアプリで開けます。

4つのAIの性格

ChatGPT

OpenAI 総合職

何でもこなす優秀な総合職。利用者が最も多い。壁打ち、文章のたたき台、画像づくり、音声会話が得意。

Gemini

Google 調べものの係

Googleに詳しい調べものの係。検索と一体の調査、Gmail・Googleドライブ・ドキュメントとの連携が強み。

Gemini Notebook

（旧NotebookLM）

Google 資料室の司書

渡した資料だけを根拠に答える司書。出典付きで答え、音声解説・動画解説・マインドマップ・レポートも作る。2026年7月に改名。

Claude

Anthropic

書記役+エージェント

筋道の通った文章と長文読解が得意。会話の中でファイル操作・スキル・定期実行ができ（2026年9月に旧Coworkと統合）、Claude Codeで本格的な自動化まで任せられる。

比較表：特徴と、無料／有料でできること

	ChatGPT	Gemini	Gemini Notebook	Claude
一番の得意	何でも一通り・画像	検索・Google連携	資料に基づく回答（RAG）	長文読解・文章・エージェント
答えの根拠	学習した知識＋Web検索	学習した知識＋Google検索	登録した資料だけ（出典付き）	学習した知識＋Web検索＋渡した資料
無料でできること	会話・Web検索・画像生成・ファイル読み込み（回数制限が強い）	会話・画像・Deep Research・Canvas（使用量で上限）	100ノート・1ノート50資料・1日50質問・音声解説	会話・Web検索・ファイル作成・スキル・プロジェクト5個
有料で増えること	上位モデル、Deep Research本格利用、エージェント	上限2～4倍、エージェント機能、Notebook上限5倍	500ノート・300資料・1日500質問（Google AI Pro）	Claude Code、会話でのスキル・定期実行（旧Cowork）、Research、プロジェクト無制限
個人の有料版	Go 約1,200円／Plus 約3,000円	AI Plus 725～1,450円（公式ページで表示が異なる）／AI Pro 2,900円	Google AI Proに含まれる	Pro 約3,000円（\$20）
入力データの学習利用	無料・Goは初期設定で学習対象（設定でオフ可）	設定で管理（アクティビティ）	資料は学習に使わない。👍👍を押すと人の確認に回る（個人アカウント）	設定で学習オフ可
こんな時に	まず相談したい、たたき台がほしい	Googleで仕事をしている、調べたい	マニュアル・規程・議事録・公的資料を根拠に答えさせたい	長い資料を読み込む、業務を任せて自動化したい

料金は2026年9月時点の目安（ドル建ては為替で変動）。無料版の上限は各社とも「使用量」で決まり、回数は固定されていない。

迷ったらこう選ぶ

やりたいこと	まず使うAI
文章のたたき台・チラシ案・壁打ち	ChatGPT か Gemini（好きな方でよい）
最新情報を調べてレポートにしたい	各社の Deep Research（→ B3）
社内資料・公的資料を根拠に答えさせたい	Gemini Notebook （→ B1b）
毎回同じ手順の仕事を任せたい・自動化したい	Claude（旧Cowork） ／ Claude Code （→ A3）
Google Workspace で仕事をしている組織	Gemini（Workspaceならデータ保護も強い）

出典（2026年9月確認）

- Google Gemini サブスクリプション (<https://gemini.google/subscriptions/>)
- Claude 料金プラン (<https://claude.com/pricing>)
- ChatGPTの有料プラン比較（2026年9月） (<https://tech-camp.in/ai-navi/chatgpt-paid/>)（二次情報）
- NotebookLM is now Gemini Notebook（Google） (<https://blog.google/innovation-and-ai/products/gemini-notebook/notebooklm-gemini-notebook/>)
- Gemini Notebook のプライバシー（Googleヘルプ） (<https://support.google.com/gemininotebook/answer/17004255?hl=en>)

無料版・有料版・組織契約の違い

料金と「入力データの扱い」の差。仕事で有料版を使うべき理由

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

たとえ：無料版は「試食」、有料版は「業務用の仕入れ契約」

味は同じでも、量・品質・取引条件（データの扱い）が違う。専門職が無料版だけで業務をするのは、試食品で弁当を作って売のようなもの。

3つの段階の違い

観点	無料版	有料版（個人）	組織契約（Team／Business／Workspace）
使える量	すぐ上限に当たる	実務で困らない程度	同左＋利用者ごとに管理
AIの賢さ	軽量なモデルが中心	最上位モデル	同左
長い資料	途中で止まりやすい	長いマニュアルや制度の文書を丸ごと読める	同左
調査機能（Deep Research）	ごく少数回／使えない	実用的に使える	同左
エージェント機能	ほぼ使えない	使える	同左
入力データの学習利用	初期設定で学習対象のものがある	設定でオフにできる	原則として学習に使わない契約
管理・監査	なし	なし	管理者が利用状況を管理できる

料金の目安（2026年10月時点・月額）

サービス	無料	個人の有料版	組織向け
ChatGPT	0円	Go 約1,200円（広告あり・Deep Research不可） Plus 約3,000円 Pro 約15,000円～（100・200・500ドルの3段）	Business 約3,800円～／人
Gemini／Gemini Notebook	0円	Google AI Plus 725～1,450円（公式ページで表示が異なる） Google AI Pro 2,900円 Ultra 14,500円～	Google Workspace のプランに含まれる

サービス	無料	個人の有料版	組織向け
Claude	0円	Pro 約3,000円 (\$20) Max 約15,000円～ (\$100～)	Team 約3,000円～／席 (年払い)

ドル建ては為替で変動。価格・プラン名は頻繁に変わるため、契約前に各社の公式ページで確認すること（Gemini・Claudeの数字は2026年10月3日に公式ページで確認。Google AI Plus は、Gemini のページでは725円、Google One のページでは1,450円と表示が異なる。ChatGPT は公式が取得できず、二次情報）。

2026年9月末から出た「常時稼働型のエージェント」は、上位プランに含まれる：ChatGPT の dots は Pro・Business Premium、Gemini Spark は Google AI Ultra 向け、Claude のクラウド実行は Pro 以上（→ A3）。

おすすめの始め方

1

2人で1ヶ月試す
個人の有料版を2人が別々のサービスで契約

2

同じ業務で比べる
市場調査・長い資料の読み込みなど、実際の業務で1回ずつ

3

効果を測る
かかった時間・品質・使いやすさを記録

4

組織契約へ
顧客・取引先の情報を扱う前に、ルールと組織契約を整える

「安いプラン」の落とし穴

ChatGPT Go のような低価格プランは、入力データが初期設定で学習対象であり、調査機能やエージェントも使えない。業務で使うなら、データの扱いを確認できるプランを選ぶ。

出典（2026年9月確認）

- Google Gemini サブスクリプション (<https://gemini.google/subscriptions/>)
- Claude 料金プラン (<https://claude.com/pricing>)
- ChatGPTの有料プラン比較（2026年9月） (<https://tech-camp.in/ai-navi/chatgpt-paid/>)（二次情報）

AIエージェント入門：Claude Code と Claude（旧 Cowork）

スキル化と自動化を担うAIエージェントの機能と、各社の勢力図

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

対象ツール：Claude Code

この資料は、**Claude** と **Claude Code** を中心に説明します。実習・合宿で使うのは**Claude Code**です。OpenAI や Google などのエージェントは、**動向**として紹介しています（画面・設定は、それぞれ異なります）。

対象の方：開発者ではない方（経営者・事務・現場の担当者）。プログラミングは不要です。**コードは書かず、AIエージェントに頼んで、自分の業務アプリをつくる**ところまでを、順に進めます（ターミナルの黒い画面は、使わない形で書いています）。

AIエージェントとは

「質問に答える辞書」ではなく、**目的を伝え、自分で手順を考え、調べ、資料を読み、書類を作り、結果を報告してくる「任せられる部下」**。人の役割は「作業する人」から「任せて、確認し、承認する人」に変わる。

Claude の2つのエージェント

Claude（旧 Claude Cowork）

事務職・非エンジニア向け 画面で操作

Claudeのデスクトップアプリの中で使う。黒い画面（ターミナル）は不要。フォルダを指定して「この資料を整理して報告書にして」と頼むだけ。2026年9月時点で、Web・スマホからも使える。

Claude Code（クロード・コード）

本格派 AIエージェントの先頭

もともとはプログラマー向け。ファイル操作・手順の実行・外部ツール連携まで何でもできる。業務手順を「スキル」として覚えさせる考え方を広めた。

2026年9月16日：Cowork とチャットがひとつの「Claude」に統合

以前は「チャット」と「Cowork（作業用）」を使い分ける必要があったが、統合後はClaudeが依頼の大きさを見て自動で判断する。スキル・コネクタ・定期実行・ファイル操作は、ふつうの会話の中で使える。**Pro・Maxプランから数週間かけて順次**、Team・Freelは後日。あわせて Claude Docs・Claude Slides（ベータ）も登場。

どちらも**Claudeの有料版（Pro 以上）**で使える。まずは Claude の会話でスキルを作り、物足りなくなったら Claude Code へ進むのが近道。

2026年秋の新しい動き：エージェントが「常時稼働」になった

2026年9月末～10月、3社がそろって「PCを閉じても、クラウドで働き続けるエージェント」を出した。質問したら答えるAIから、こちらが寝ている間も仕事を進めるAIへ。

会社	名前	中身	使えるプラン（2026年10月時点）	確認
OpenAI	dots（ドッツ）	自分専用のクラウドPCとブラウザを持ち、ChatGPT・Slack・Teams・電話で話しかけられる。メールやGoogleドライブなどをつないで、会話の合間も作業を進める。判断が要るときだけ連絡してくる。2026年9月29日発表	ChatGPT Pro（100・200・500ドル）、Business Premium、Enterprise（管理者が有効化）。無料・Go・Plusは対象外。段階的に提供中	公式で確認
Google	Gemini Spark（スパーク）	Gmail・カレンダー・ドキュメントを見ながら、クラウドで動き続ける個人向けエージェント。Windows版Geminiからも作業を任せられる	Google AI Ultra向けと報じられている	公式は言及のみ、詳細は報道
Anthropic	Claude（旧Cowork）	10月6日から、ProとMax（Team・Enterpriseも）の新しいタスクは、すべてクラウドで実行。設定の「自分のコンピュータのみ」は廃止。すでに始めたタスクは、そのまま	Pro・Max・Team・Enterprise	公式で確認

常時稼働ほど、「関所」が大事になる

3社とも、安全のために「読むだけ・下書きまで」「人の許可が要る操作」を設けている。それでも、**自分の知らないうちにエージェントが動く**ようになるため、何を任せ、どこで止めるかを自分で決めておくことが前よりも重要になる（→ E2 ハーネス）。

機能表：何ができて、仕事ではどう使えるか

機能	ひとことで	事務・総務・営業の仕事なら	Claude (旧Cowork)	Code
ファイルを読む・作る	指定したフォルダの資料を読み、Word・Excel・PDFなどの成果物を作って保存する	取引先から届いた見積書PDFを読み、比較表（Excel）と確認メール（Word）を作る	○	○
スキル	業務手順書をAIに覚えさせる。「あれやって」の一言で同じ手順・同じ品質で仕上がる	「月次の請求チェックをやって」で、不備の一覧・修正依頼文・集計表の3点が下書きで出る	○	○

機能	ひとことで	事務・総務・営業の仕事なら	Claude (旧Cowork)	Code
スキルをAIと作る	「この仕事をスキルにしたい」と話しかけると、手順書そのものをAIが書き起こす	ベテランのやり方を言葉にして残す（引き継ぎ・属人化の解消）	○	○
定期実行	決まった時間に自動で動く。クラウドで動くので、PCを閉じていても実行される（2026年10月6日から、ProとMaxの新しいタスクはすべてクラウド実行）	毎週月曜の朝に、先週の問い合わせの要約と未対応の一覧を下書きしておく	○	○
コネクタ（外部ツール連携）	Gmail・カレンダー・Googleドライブ・Slackなどをつなぐ（MCPという共通規格）	メールの問い合わせを読んで返信の下書きを作る（送信は人が押す）	○	○
プラグイン	スキルや連携をまとめたセット。一度作れば職場で配れる	「経理チェックセット」を全社員で共有	○	○
分身（サブエージェント）	大きな仕事を、調べ係・まとめ係・チェック係に分けて並行して進める	複数の取引先の見積を同時に比較する	△	○
プログラム・アプリ作成	集計の仕組みや小さな業務アプリまで作れる	案件台帳の集計表、社内向け検索ページ	△	○
人の承認（ガードレール）	危ない操作の前に止まって確認を求める。任せる範囲を設定できる	「送信ボタンは人が押す」を仕組みで守る	○	○

自動化までの4段階（例：月次の請求チェック）

1

学ぶ
Gemini Notebookに取引条件や社内ルールを入れ、根拠付きで答えさせる（RAGの体験）

2

型にする
「①不備の一覧 ②修正依頼文 ③集計表」と手順を言葉にする（→F1）

3

スキル化
Claudeに手順をスキルとして覚えさせる。以後は一言で3点が下書きで出る

4

自動化
「PDFを置いたら」「毎週月曜」で自動実行。人は確認して送信ボタンだけ押す

講師（伊藤）自身の運用例

- 毎月の請求書業務：「請求書業務やって」の一言で、金額の照合から請求書作成・メール下書きまで。**送信は自分で押す。**
- 毎朝、予定とやるべきことのまとめが自動で届く。
- どちらも最初は「毎回AIに頼んでいたこと」。それを手順書にし、スキルにし、最後に自動化した。

各社の勢力図：Claude Code が先頭、OpenAI・Google が猛追

会社	エージェント	開発者の利用率（2026年5～7月）	状況
Anthropic	Claude Code／Claude（旧 Cowork）	39%（米国47%）	先頭。スキルの考え方を広めた
OpenAI	Codex（コーデックス）	16%	1月の3%から約5倍に急伸。週500万人以上が利用
Google	Antigravity（アンチグラビティ）ほか	6%	知名度は急上昇（47%）。Gemini Notebookとの連携も進む

数字はプロの開発者1.5万人超への調査（JetBrains、2026年5～7月）。事務職の利用率ではない。9月末にOpenAIの dots が出たので、次の調査では変わる可能性がある。

製品名より「考え方」を身につける

競争の軸は「どのAIが賢いか」から「どのAIエージェントが仕事を任せられるか」に移った。大事なのは「業務手順を言葉にしてAIに覚えさせる力」。これさえあれば、どの会社が伸びても乗り換えられる。

出典（2026年9月確認）

- Claude Cowork and chat are now one Claude（Anthropic, 2026年9月16日）（<https://claude.com/blog/cowork-is-now-claude>）
- Get started with Claude Cowork（Claude Help Center）（<https://support.claude.com/en/articles/13345190-get-started-with-claude-cowork>）
- Claude's scheduled tasks（XDA）（<https://www.xda-developers.com/claude-scheduled-tasks-feature/>）
- Claude Code Guide 2026（MarkTechPost）（<https://www.marktechpost.com/2026/06/14/claude-code-guide-2026-25-features-with-example-s-demo/>）
- AI Coding Agents: Adoption Trends（JetBrains, 2026年8月）（<https://blog.jetbrains.com/research/2026/08/ai-coding-agent-adoption-2026/>）
- Claude 料金プラン（<https://claude.com/pricing>）
- dots について（OpenAI公式ドキュメント）（<https://learn.chatgpt.com/docs/dots>）
- OpenAI launches Dots（9to5Google・2026年9月29日）（<https://9to5google.com/2026/09/29/openai-dots-agent/>）（報道）
- The latest AI news we announced in September 2026（Google）（<https://blog.google/innovation-and-ai/technology/ai/google-ai-updates-september-2026/>）
- Google launches Gemini Spark（TNW）（<https://thenextweb.com/news/google-gemini-spark-agentic-assistant-gmail-io-2026>）（報道）

Claudeの契約と、デスクトップアプリの最初の設定 (Windows・Mac)

Pro以上の契約（ブラウザで）、アプリのインストール、Codeタブ、最低限の設定3つ（権限モード・モデル・プライバシー）、WindowsとMacの違い、つまりき、動作確認

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

対象ツール：Claude Code

この資料は、**Claude Code**（Anthropic のAIエージェント。Claudeのデスクトップアプリの「Code」タブ）を前提に書いています。ほかのAIエージェント（OpenAI のCodex、Google のエージェントなど）は、**画面・用語・ファイル名・設定が異なります**。

対象の方：開発者ではない方（経営者・事務・現場の担当者）。プログラミングは不要です。**コードは書かず、AIエージェントに頼んで、自分の業務アプリをつくる**ところまでを、順に進めます（ターミナルの黒い画面は、使わない形で書いています）。

3ステップで、使い始められる：契約 → アプリ → 最初の設定

AIエージェント（Claude Code）を使うには、**Claudeの有料プラン（Pro以上）**と、**デスクトップアプリ**が要る。難しい操作はない。**Windows と Mac のどちらでも**、この順に進めればよい。所要は、約30～45分。

この資料の画面の名称は、アプリの版で変わることがある。**見つからないときは、画面の写真を添えて、講師に相談してください**。

1. 先に決める：どのプランか

プラン	料金（公式の料金ページ）	Claude Code（Codeタブ）	向く人
Free	無料	使えない	チャットを試すだけ
Pro	月額20ドル（年払いは、月あたり17ドル）	使える	まず、ここから 。合宿・講座の標準
Max	月額100ドルから	使える（利用量が、Proの5倍または20倍）	毎日、長時間使う人
Team・Enterprise	席ごとの月額	使える	会社として、複数人で使う

- **利用量の枠は、ChatのClaudeと、Claude Codeで共有される（公式）**。Codeで使いすぎると、チャットの分も減る。
- 枠を使い切ったときの選択肢：**リセットまで待つ**／**Maxに上げる**／**追加の利用量（クレジット）を有効にする**。残りが少なくなると、警告が出る（公式）。
- 料金は、為替で変わる。ドル建てで、日本円では、約3,000円（Pro）が目安（→ A2）。

2. 契約する（Windows・Mac共通。ブラウザで）

1

1 アカウントを作る・ログイン

ブラウザで claude.ai を開き、アカウントを作る（すでにあればログイン）

2

2 Proに申し込む

claude.ai/upgrade から、Pro を選ぶ

3

3 支払い

クレジットカードまたはデビットカード（公式のヘルプ）。自動で更新される

4

4 契約を確認

画面の左下の名前をクリック → 「Settings（設定）」で、プランが Pro になっているか確認

契約は、スマホのアプリではなく、ブラウザがおすすめ

iPhoneやAndroidのアプリの中で契約すると、その契約は、AppleやGoogleのものになる。**解約や変更が、App Store／Google Play の画面になり、分かりにくくなる。**パソコンのブラウザで契約すると、設定の画面で、まとめて管理できる。

解約・更新

- 自動で更新される。やめるときは、**設定（Settings）の「Billing（請求）」から「Cancel（解約）」**。次の請求日の**24時間前まで**に行う。解約しても、いまの請求期間の終わりまでは、使える（公式のヘルプ）。
- 合宿・講座のために入る人は、**解約の予定日を、カレンダーに入れておく**と、安心。

3. デスクトップアプリを入れる

手順	Mac	Windows
ダウンロード	Mac版（Intel・Apple Silicon共通）	Windows版（x64）。ARM版のパソコンは、ARM64版
入れる	ダウンロードしたファイルを開き、案内に従ってインストールする	ダウンロードしたインストーラーを実行する
起動	「アプリケーション」フォルダの Claude を開く	スタートメニューの Claude を開く
サインイン	Claude のアカウント（契約したもの）でログインする。ブラウザが開いたら、ログインを完了して、アプリに戻る（戻らないときは、アプリを再起動する）	
更新の確認	メニューの「Claude」→「Check for Updates（アップデートを確認）」	メニューの「Help」→「Check for Updates」

- デスクトップアプリには、**Claude Code が含まれている**。Node.js や、ターミナルの導入は、要らない（公式）。
- Windows の ARM64 かどうかは、「設定」→「システム」→「バージョン情報」の「システムの種類」で分かる。迷ったら、x64を入れて、動かなければ、ARM64を入れる。
- 新しい機能を使うために、**アプリは、ときどき更新**する。

公式のはじめかた：[Get started with the desktop app](#)（ダウンロードのリンクと、最初のセッションの手順）。

4. 最初の画面：Code タブで、フォルダを選んで話しかける

1

1 「Code」 タブを開く
画面の上の中央。「アップグレード」と出たら、契約が済んでいない（7章）

2

2 「Local」 を選ぶ
自分のパソコンの中のパイルで動かす

3

3 「Select folder」 でフォルダを選ぶ
仕事のフォルダ（E1）。最初は、空の練習用フォルダでよい

4

4 モデルと権限モードを確認
入力欄の横にある、2つの選択（5章）

5

5 話しかける
8章の「最初の一言」を、入力して、Enter

5. 最低限の設定：画面で、3つだけ

設定	どこで	どうする
① 権限モード	入力欄の、送信ボタンの横にある選択	「Manual（確認あり）」を選ぶ。Claudeがファイルを書き換える前に、変更の内容（差分）が出て、「承認」か「却下」を選べる。慣れるまで、これで使う（E1）。選んだモードは、フォルダごとに、記憶される
② モデル	入力欄の、送信ボタンの横にある選択	Pro のはじめは、初期の設定のままでよい（公式の既定は、Opus 5.5）。一部のモデル（Fable）は、プランによって、追加の利用量（クレジット）が必要。迷ったら、変えない
③ プライバシー	左下の名前 → 「Settings（設定）」 → 「Privacy（プライバシー）」	「Help improve our AI models」（AIモデルの改善に協力する）のオン・オフを、自分で決める。オフにすると、今後の新しいチャットとコーディングのセッションが、モデルの学習に使われなくなる（すでに学習されたものは、そのまま）。お客様や仕事の情報を扱うなら、オフを検討する（D1）

この3つ以外は、最初は、触らなくてよい

設定の項目は、たくさんあるが、はじめは、上の3つで十分。ほかの設定（作業コピーの置き場所、通知など）は、使いながら、必要になったときに調べる。

6. Windows と Mac の違い（まとめ）

項目	Mac	Windows
新しいセッション	Cmd + N	Ctrl + N
ショートカットの一覧	Cmd + /	Ctrl + /
アプリの更新	「Claude」メニュー → Check for Updates	「Help」メニュー → Check for Updates
Git の準備（E4）	ほとんどのMacに、最初から入っている。無ければ、開発者ツールの案内に従う	Git for Windows を入れる

項目	Mac	Windows
貼り付け・コピー	Cmd + V / Cmd + C	Ctrl + V / Ctrl + C
フォルダの場所の書き方	/Users/名前/Projects/…	C:\Users\名前\Projects\…
アプリの場所	「アプリケーション」フォルダ	スタートメニュー

7. つまづいたとき

こんなとき	こうする
Codeタブを開くと、「アップグレード」と出る	Pro以上の契約が、済んでいない（または、反映前）。2章で契約を確認し、アプリを、いったん終了して、開き直す
「ブラウザでログインしてください」と出る	ブラウザで、ログインを完了し、アプリを再起動する
「403」などの認証のエラー	公式のトラブルシューティングを見る。画面の写真を添えて、講師に相談
契約しているのに、従量課金になる？	パソコンに ANTHROPIC_API_KEY という環境変数（鍵）が設定されていると、Claude Codeは、 契約の枠ではなく、従量のAPI課金で動く （公式）。心当たりがあれば、Claudeに「ANTHROPIC_API_KEY が設定されているか、値は表示せずに確認して」と頼む（E6）
利用量の上限に達した	リセットまで待つ／Maxに上げる／追加の利用量（クレジット）を有効にする（公式）。チャットとCodeで、枠は共有
Gitの確認でつまづく	Claudeに「Gitの状態を確認して、使えなければ、手順を教えて」と頼む（E4）。公式も、Gitの問題は、Claudeに相談することを勧めている

8. 最初の一言：動作の確認（安全なテスト）

空の練習用フォルダを選んで、次のように話しかける。**確認あり（Manual）**のモードなら、書き込みの前に、確認が出る。

コピーして使う

このフォルダに、「こんにちは.txt」というファイルを作って、「はじめてのClaude Code」と1行だけ書いてください。作る前に、何をするか教えてください。

- Claudeが、「ファイルを作ります」と説明する。
- 確認の画面（変更の差分）が出る。**内容を読んで、「承認」を押す。**
- フォルダに、ファイルができていれば、成功。

これができれば、準備は完了。次は、E4（Git）と、E1（フォルダの作り方）へ。

9. 準備完了のチェックリスト

☐	確認すること
☐	Claudeの有料プラン（Pro以上）に入っている（設定で、プランを確認した）
☐	デスクトップアプリを入れ、ログインできた
☐	「Code」タブが開く（「アップグレード」と出ない）
☐	権限モードは「Manual（確認あり）」
☐	プライバシーの設定（モデル改善への協力）を、自分で決めた
☐	練習用のフォルダで、「こんにちは.txt」を作れた
☐	解約の予定日を、カレンダーに入れた（必要な人）
☐	パソコンに ANTHROPIC_API_KEY が設定されていないことを、確認した

関連資料

- A2 無料版・有料版・組織契約の違い／A3 AIエージェント入門
- E4 Gitの導入と設定／E1 フォルダ構成と管理／G3 合宿の事前準備ガイド

出典（2026年10月確認）

- Get started with the desktop app（Anthropic 公式）（<https://code.claude.com/docs/en/desktop-quickstart>）：インストール、Code タブ、フォルダの選択、Pro以上が必要、Node.js不要
- Use Claude Code Desktop（Anthropic 公式）（<https://code.claude.com/docs/en/desktop>）：権限モード、新しいセッション、更新の確認、ショートカット
- Using Claude Code with your Pro or Max plan（Claude ヘルプ）（<https://support.claude.com/en/articles/11145838-using-claude-code-with-your-pro-or-max-plan>）：利用量の共有、上限に達したとき、ANTHROPIC_API_KEY
- How do I change my model improvement privacy settings?（Claude プライバシー）（<https://privacy.claude.com/en/articles/12109829-how-do-i-change-my-model-improvement-privacy-settings>）：Help improve our AI models
- Cancel your Pro or Max subscription（Claude ヘルプ）（<https://support.claude.com/en/articles/8325617-cancel-your-pro-or-max-subscription>）：解約の手順、請求日の24時間前
- Claude 料金プラン（<https://claude.com/pricing>）
- Model configuration（Anthropic 公式）（<https://code.claude.com/docs/en/model-config>）：Proの既定のモデル

AIへの頼み方の基本

初級：頼み方の4要素と、仕事で使える例文集

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

このページの位置づけ

AIへの頼み方の基本（初級）：ChatGPT・Gemini・Claude のどれでも使える頼み方。続きは B1b RAG：資料を根拠に答えさせる（中級）。

スマホでQRを読み取ると、そのままAIが開きます（ログインはご自身のGoogleアカウント等で）



ChatGPT
chatgpt.com



Gemini
gemini.google.com



Gemini Notebook
notebook.google.com



Claude
claude.ai

アプリ版（App Store／Google Play）を入れておくと、次からはアプリで開けます。

1. 一言で頼むと、一般論が返ってくる

AIは、あなたの仕事も、お店も、お客様も知らない。状況を伝えるほど、答えは「自分ごと」になる。

一言だけ

コピーして使う

チラシの文章を考えて

→ どこのお店にも使える、ありきたりな文章が返ってくる

状況を伝える

コピーして使う

桑名市で米屋を営んでいます。新商品の玄米5kgを紹介するチラシの文章を、年配のお客様にも読みやすい言葉で、150文字程度で考えてください。

→ そのまま使える文章に近づく

2. 頼み方の4要素

要素	書くこと	例
① 誰が	業種・立場	工務店の事務担当です／飲食店の店主です

要素	書くこと	例
② 何のために	目的	お客様に新しいメニューを案内したい
③ 誰に向けて	読む人・相手	パソコンが苦手な年配の経営者に
④ どんな条件で	文字数・トーン・形式	やさしい言葉で、300文字以内、箇条書き3つ

コピーして使う

私は〔①業種・立場〕です。〔②目的〕のために、〔③相手〕に向けた〔作ってほしいもの〕を作ってください。
〔④条件：文字数・トーン・形式〕をお願いします。

3. 一発で決めなくていい：返ってきたら直してもらう

AIとのやりとりは「注文」ではなく「打ち合わせ」。返ってきた答えに、続けて一言足すだけで良くなる。

こうしたいとき	続けて頼む一言
長い・硬い	「半分の長さに」「もっとやわらかい言葉で」
選びたい	「違う切り口で3案出して」
相手に合わせたい	「70代の方にも伝わるように」「若い人向けに」
理由を知りたい	「なぜその書き方にしたのか教えて」
足りないものを知りたい	「この文章に足りない情報があれば、質問して」

4. 仕事で使える例文（コピーして〔 〕を埋める）

案内文・お知らせ

コピーして使う

私は〔会社の担当者〕です。〔イベント名・日時・場所・対象〕のお知らせ文を、〔お客様・取引先〕向けに、
200文字程度のやさしい言葉で作ってください。最後に申込み方法を1行で入れてください。

メールの返信

コピーして使う

次のお客様のメールに、丁寧に返信する文章を作ってください。〔伝えたいこと：例〕日程変更を了承する、資料は後日送る〕を入れてください。

（ここにお客様のメールを貼る。お名前・連絡先は伏せる）

要約・議事録

コピーして使う

次のメモから、①話し合ったこと②決まったこと③次までにやること（担当・期限つき）の3つに分けて、議事録を作ってください。

（ここにメモを貼る）

写真の表を読み取って集計（スマホで撮影して添付）

コピーして使う

添付した写真の表を読み取って、項目ごとの合計を計算してください。読み取れない文字があれば、推測せずに「読めない」と書いてください。

やさしく言い換える

コピーして使う

次の文章を、専門用語を使わずに、中学生にも分かる言葉で言い換えてください。

（ここに文章を貼る）

アイデア出し・壁打ち

コピーして使う

〔業種〕の小さなお店が、〔目的：例〕平日の昼の来店を増やす〕ためにできることを、お金をかけない順に5つ挙げてください。それぞれの良い点と注意点も書いてください。

頼むときの2つの約束

- お客様の名前・連絡先・決算の数字は入れない（伏せて頼む）。入れてよい情報は D1 信号機ルール
- 数字・日付・制度の中身は、必ず自分で確かめる。AIはもっともらしく間違えることがある。この「間違い」を減らすのが、B1b RAG

RAG：資料を根拠に答えさせる

中級：AIに「資料室」を持たせ、資料を根拠に答えさせる（Gemini Notebook）

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

このページの位置づけ

RAG（中級）：頼み方に「根拠にする資料」を足すと、AIは資料を指さしながら答えるようになる。頼み方の基本は B1a AIへの頼み方の基本（初級）。

スマホでQRを読み取ると、そのままAIが開きます（ログインはご自身のGoogleアカウント等で）



ChatGPT
chatgpt.com



Gemini
gemini.google.com



Gemini Notebook
notebook.google.com



Claude
claude.ai

アプリ版（App Store／Google Play）を入れておくと、次からはアプリで開けます。

1. RAG（ラグ）とは

RAG＝検索拡張生成（Retrieval-Augmented Generation）。AIに「資料室」を持たせ、答える前に資料を調べ、その内容を根拠に答えさせる仕組み。

ふつうのAI＝記憶で答える物知りな人

- インターネット全体から学んだ記憶で答える
- 知らないことも、もっともらしく答えてしまう（ハルシネーション）
- あなたの会社の規程・取引先との取り決め・最新の制度は知らない

RAG＝棚から資料を出して答える司書

- 登録した資料だけを調べて答える
- 「どの資料の、どこに書いてあるか」を指さして示す（出典）
- 資料にないことは「書いていない」と答える

RAGの価値は「答えないこと」にある

制度・契約・社内ルールのように「**根拠はどこか**」が問われる仕事では、それらしい作り話は致命的。棚にない本を「ない」と言える司書こそ、専門職の相棒になる。

2. Gemini Notebook（旧NotebookLM）で体験する

プログラムなしで、誰でもRAGを体験できる道具。Googleアカウントがあれば無料で使える。

1

ノートブックを作る

notebook.google.com（旧 notebooklm.google.com）から自動で移動。Geminiアプリからも開ける）

2

資料を入れる

PDF・Word・Webページ・音声・動画など（無料で1ノート50資料）。スマホは「共有」から追加できる（→7）

3

質問する

答えの中の番号をクリックすると、根拠の箇所が開く

4

共有する

職場の仲間に共有すれば、全員が同じ根拠で答えられる

3. 例：資料室の「〇〇係」をつくる

自社の資料（就業規則・マニュアル・取扱説明書・見積書の雛形など）で作るのが本番。ここでは、誰でも手に入る公開資料として**補助金の公募要領**で体験する（どの業種の会社も対象になりうる制度で、内容が長く、根拠探しの練習に向いている）。

入れる資料：最新の公募要領、よくある質問集、申請様式、（あれば）過去の公募要領

試しに使える資料：小規模事業者持続化補助金＜一般型 通常枠＞第20回（商工会地区）



スマホで読み取ると
PDFが開きます

公募要領（第8版・PDF）をダウンロード

2026年7月21日版・約1.6MB

申請・公募要領のページ

新旧対照表・様式もここから

よくあるご質問

Webページのまま追加できる

出典：小規模事業者持続化補助金事務局（商工会地区）。商工会議所地区の方は 商工会議所地区の事務局サイト から。公募ごとに版が変わるので、使う前に最新版が確かめてください。

スマホなら「共有」から、そのまま Gemini Notebook に入れられる

Gemini Notebook のアプリ（iPhone・Android）を入れておくと、PDF・Webページ・YouTube をダウンロードしてパソコンに移さなくても、スマホの「共有」ボタンからソースとして追加できる。

1

アプリを入れる

App Store／Google Play で「Gemini Notebook」。
Googleアカウントでログイン

2

資料を開く

上の「公募要領をダウンロード」を押すか、紙ならQRを読み取ってPDFを開く（Webページのままでもよい）

3

共有 → Gemini Notebook

画面の共有ボタン（□に↑、または<）を押し、一覧から Gemini Notebook を選ぶ

4

ノートを選ぶ

「新しいノートブック」を作るか、既存のノートを選んで追加。すぐ質問できる

パソコンなら

PDFをダウンロードして、Gemini Notebookの「ソースを追加」にドラッグする。または「ウェブサイト」を選んで、上のページのURLを貼り付ける（PDFを保存しなくても追加できる）。

コピーして使う

この補助金の「補助対象経費」と「対象外経費」を一覧表にしてください。それぞれ根拠となる記載箇所も示してください。

コピーして使う

前回の公募要領から変わった点を、自社への影響が大きい順に5つ挙げてください。

自社の計画が補助対象になりそうか、一次確認する

コピーして使う

次の取り組みを考えています。この補助金の対象経費になりそうか、根拠となる記載と一緒に答えてください。判断できない場合は「資料からは判断できない」と答えてください。
取り組み：店舗の看板を新しくして、集客を増やしたい。

試してみる例	見どころ
店舗の看板を新しくしたい	対象になりうる経費の区分と条件が、根拠付きで出るか
ネット販売用のホームページを作りたい	上限や条件（割合の制限など）まで拾えるか
中古の軽トラックを買いたい	対象外の可能性を、根拠付きで答えられるか（汎用品・車両の扱い）

最終判断は人がする

AIは「根拠のページを素早く探す係」。迷うものは公募要領の本文と、事務局・専門家に確認する。公募回ごとに要領は変わるので、**ノートブックの資料は必ず最新版に入れ替える**。

4. RAGの限界：Gemini Notebookは「調べて答える」まで

- 自分から仕事を始めない（毎回、人が質問しに行く）
- 書類を作ってフォルダに保存したり、メールの下書きを作って次の作業に渡したりはしない

「決まった手順の仕事を、毎回同じ品質で、できれば自動で」こなすには、AIエージェント（A3）の出番になる。**まずGemini NotebookでRAGを体で理解し、業務によってはAIエージェントまで使いこなす**——これが仕組み化の道筋。

データの扱い（個人アカウントの注意）

Gemini Notebookは登録した資料をAIの学習に使わない。ただし**個人のGoogleアカウントで回答に👍👏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**。お客様・取引先の情報を入れるなら、Google Workspace のアカウントで使う（→ D1）。会社の共有ドライブを資料室にする方法は、W2 の5章。

出典（2026年9月確認）

- NotebookLM is now Gemini Notebook（Google）（<https://blog.google/innovation-and-ai/products/gemini-notebook/notebooklm-gemini-notebook/>）
- Privacy and Terms of Use in Gemini Notebook（Googleヘルプ）（<https://support.google.com/gemininotebook/answer/17004255?hl=en>）
- How to Use Gemini Notebook: 2026 Guide（<https://aiweekly.co/learning-ai/generative-ai/how-to-use-notebooklm>）（無料枠の数値）
- Gemini Notebook モバイルアプリの使い方（Googleヘルプ）（<https://support.google.com/gemininotebook/answer/16296687?hl=ja>）（共有からのソース追加）
- 小規模事業者持続化補助金事務局（商工会地区）申請ページ（<https://official.jizokukanb.com/shinsei>）

AIはデータなくして語れない：データ管理の型

何を集め、どこに置き、どう名付け、いつ更新するか

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

AIの答えの質は「賢いAIか」より「何を読ませたか」で決まる

どんなに賢いAIでも、あなたの会社の規程・取引先との取り決め・最新の制度は知らない。**データを整えた人が、AIを使いこなす。** ChatGPTでもGeminiでもClaudeでも、これは同じ。

データ管理の5つの型

1

集める

AIに読ませたい資料を決める

2

置く

決まった場所に、決まった分け方で

3

名付ける

日付・種類・版がわかる名前

4

色を付ける

信号機で、AIに入れてよいか

5

更新する

古い版を入れ替える日を決める

1. 集める：まず「繰り返し見に行く資料」から

- 毎回探しに行く資料（マニュアル・規程・様式・見積書の雛形）
- 毎回同じ説明をしている内容（よくある質問と答え）
- ベテランの頭の中にしかない判断基準 → 言葉にして文書化する（これ自体がAI活用の最大の成果になる）

2. 置く：フォルダは「業務」で分ける

フォルダの形

■ 総務

■ 規程

就業規則_2026-04改定.pdf

■ 様式

■ 営業

■ 見積書の雛形

■ よくある質問

■ 経理

■ 月次チェック手順

■ 公的資料

統計・補助金の公募要領

このフォルダ構成が、そのまま Gemini Notebook の「ノートブック」の単位や、AIエージェントの「スキル」が参照する場所になる。

3. 名付ける：日付と版を必ず入れる

悪い例	良い例	理由
就業規則.pdf	就業規則_2026-04改定.pdf	AIも人も、どれが最新か判断できる
最新版（修正）2.docx	FAQ_お客様対応_v3_2026-09.docx	「最新」は時間が経つと嘘になる

4. 色を付ける：信号機ルール

● 公開情報 ● 匿名化した相談内容 ● 個人情報・決算書など。詳しくは D1。

5. 更新する：古い資料はAIを間違えさせる

- 制度や規程が改定されたら、**ノートブックの資料を差し替える**（古い版は削除か「旧版」フォルダへ）
- 更新日を決める（例：毎月第1月曜に見直す）。これ自体をAIエージェントに自動化させることもできる

道具ごとの「データの持たせ方」

道具	データの持たせ方	向いている使い方
Gemini Notebook	ノートブックに資料を登録（RAG）	資料を根拠に質問に答える・要約する・共有する
ChatGPT／Claude のプロジェクト	プロジェクトに指示文と資料を置く	毎回同じ前提で相談する（スキルの手前の「型」）
Claude（旧Cowork）／Claude Code	フォルダを指定し、スキル（手順書）に資料の場所を書く	資料を読んで書類を作り、保存し、次に渡す（自動化）

道具	データの持たせ方	向いている使い方
Deep Research	データを持たせるのではなく、Webから集めてくる	集めた結果を、上の道具に入れて使う (→ B3)

データ整備は「AIのため」だけではない

資料の置き場所と名前が揃うと、人の引き継ぎも楽になる。属人化の解消、新人教育、異動への備え——AI活用の準備は、そのまま組織の足腰を強くする。

Deep Research で市場・業界調査

問いの立て方の型と、Gemini Notebookで裏取りする流れ

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

Deep Research（ディープリサーチ）とは

AIが数分～数十分かけて数十のWebページを自分で読み、出典付きのレポートにまとめる調査機能。ChatGPT・Gemini・Claude の各社が持っている。以前は半日～1日かかった下調べが、待っている間に終わる。

サービス	無料版	有料版
Gemini	使える（使用量で上限）	上限が大きい（AI Pro）
ChatGPT	ごく少数	Plus以上で本格利用
Claude（Research）	使えない	Pro以上

問いの立て方の型：「何を調べて」より「何に使うか」

要素	書くこと	例
① 目的	調査結果を何に使うか	新サービスの企画書の「市場動向」欄に書くため
② 対象	業種・地域・規模	地方の観光地にある、従業員3名の飲食店
③ 知りたいこと	市場規模・動向・競合・追い風／向かい風	テイクアウト需要の動向、観光客数の推移
④ 範囲と質	期間・情報源の条件	直近3年、公的統計や業界団体の資料を優先
⑤ 出力形式	形と分量	見出し付き、各主張に出典URL、最後に300字の要約

コピーして使う

【目的】新しいテイクアウトサービスの企画書の「市場動向」欄を書くための下調べです。

【対象】地方の観光地で営業する、従業員3名の飲食店。テイクアウト販売を強化したい。

【知りたいこと】①全国と地方のテイクアウト・中食市場の規模と動向 ②観光客の飲食消費の傾向 ③小規模飲食店にとっての追い風・向かい風

【条件】直近3年の情報。政府統計・業界団体・信頼できる調査会社の資料を優先。推測と事実を分けて書く。

【出力】見出し付きのレポート。すべての数字と主張に出典URLを付ける。最後に企画書向けの300字要約。

調べっぱなしにしない：裏取りまでの流れ

1

Deep Researchで下調べ

出典付きレポートを作らせる

2

公的データを人が足す

AIが拾いにくい一次情報（B4）。どの統計を当てるかは専門職の腕の見せ所

3

Gemini Notebookで裏取り

レポートと公的資料をまとめて入れ、矛盾を点検させる

4

本人の言葉に直す

自分たちの強みや想いを、自分の言葉で足す

コピーして使う

（Gemini Notebookで）登録した調査レポートの中で、公的統計の資料と食い違っている数字や記述はありますか？食い違いがあれば、両方の出典を並べて示してください。

コピーして使う

（Gemini Notebookで）この事業の市場動向を300字でまとめてください。各文の根拠となる資料を示し、公的統計を優先してください。

ポイント：AIの調査結果を、RAGで裏取りする

Deep Researchは広く集めるのが得意、Gemini Notebookは資料に忠実に答えるのが得意。「広く集める → 資料に閉じて確かめる」の2段構えが、根拠の厚い提案・企画の型になる。

注意

- Deep Researchの出典は必ず開いて確認する（出典があっても、読み間違えていることがある）
- 数字は年度と定義（売上か出荷額か等）をそろえる
- そのまま企画書・申請書に貼らない（補助金の申請なら → D2）

市場調査に使える公的データ一覧

AIが拾いにくい一次情報の入手先

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

Deep Researchは便利だが、公的統計の細かい表や地域別のデータは拾いきれないことが多い。「どの統計を当たるべきか」を知っていることが、専門職の価値になる。ここで集めたPDFやグラフを、Gemini Notebookに入れて裏取りに使う（→ B3）。

全国・業種の統計

データ源	わかること	使いどころ
e-Stat（政府統計の総合窓口）	国勢調査・経済センサス・家計調査・商業動態統計など、政府統計のほぼすべて	市場規模、事業所数、消費支出の推移
jSTAT MAP（地図で見る統計）	指定した範囲（半径〇kmなど）の人口・世帯・事業所	商圈分析
中小企業白書・小規模企業白書	中小企業の経営動向、課題、施策	業界の追い風・向かい風の裏付け
日本政策金融公庫「小企業の経営指標調査」	業種別の利益率・生産性などの平均値	自社の数字を同業平均と比べる
日本政策金融公庫 調査結果一覧	新規開業実態調査、景況調査など	創業計画、業界の景況感

地域のデータ

データ源	わかること	使いどころ
RESAS（地域経済分析システム）	人口・産業構造・観光・消費を地図とグラフで。2026年6月に「クレジットカード消費額分析」「地域経済総合分析」などを追加	地域の強み・弱み、観光客の動き
RESAS Portal	RESASの使い方・活用事例	初めて使うときの引き
都道府県・市町村の統計ページ	地域の人口推計、観光入込客数、事業所統計	「地元では」を数字で語る
観光協会・商工団体の調査	地域のイベント来場者数、消費動向	観光関連の申請

集めるときのコツ

- PDFやグラフの画像は、日付を付けたファイル名で保存する（→ B2）
- 表はそのままGemini Notebookに入れてよい（公開情報なので● 青）
- 「全国」「県」「市町村」の3段で数字をそろえると、説得力のある市場動向になる

出典（2026年9月確認）

- RESASをアップデートしました（経済産業省、2026年6月18日） (<https://www.meti.go.jp/press/2026/06/20260618002/20260618002.html>)
- 小企業の経営指標調査（日本政策金融公庫） (https://www.jfc.go.jp/n/findings/shihyou_ekka_m_index.html)

AIサロン桑名 AI活用事例集

地域の事業者18名が持ち寄った、AI活用の現在地

更新日：2026-09-30（2026年10月時点の情報） | HUMAC 伊藤晴通

AIサロン桑名とは

講師の伊藤が長年、毎月開催している勉強会（2026年にICTサロン桑名から改称）。地元の事業者・個人事業主・専門家が集まり、**エンジニアではない普通の事業者が、自分の仕事にAIをどう使っているかを持ち寄る場**。2026年9月の回は18名が参加して「AI活用事例の交換会」を行った。その実践から、地域のAI活用の現在地がわかる。

※参加者のお名前は伏せ、業種のみで紹介しています。

見えてきた3つの傾向

道具の使い分けが定着

記録・要約はGemini
Notebook、プログラムや複雑な処理はClaude、壁打ちやコピーはChatGPT、デザインはCanva。目的で選ぶのが当たり前。

「デジタル化」から「仕組みづくり」へ

紙やホワイトボードをデジタルにする段階から、自社の課題を解くオリジナルの仕組みを作る段階へ進む人が増えている。

浮いた時間を人の仕事に

単純作業や文章づくりをAIに任せ、本音を引き出す対話・現場の判断・対面の信頼関係づくりに時間を使う。

業種別の事例

「段階」は4段階（①相談相手 ②資料室=RAG ③スキル化 ④自動化）のどこにいるかの目安。

業種	取り組み	主な道具	段階
生命保険代理店・FP	面談音声を文字にしてPDFのまとめを作成。契約理由・お客様の意向の整理、LINEやメールの返信文案も	Gemini Notebook	②
ライター	「書かないライター」。取材音声を要約・対話を抽出し、コピーはAIで。人は本音を引き出すことに集中	Gemini Notebook・ChatGPT	②
中小企業診断士	経営支援・AIの実運用・伴走支援の視点から助言。支援の専門家自身がAIを学びに来ている	—	—
サッシ・窓の施工業	案件の進捗・施工事例・予定を全社で共有する仕組み。75インチの大型モニターで、ITが苦手なスタッフにも見える化。バックアップと復元手順も整備	自作システム	③

業種	取り組み	主な道具	段階
看板業	磁石のホワイトボードの予定・配車管理を、PC・スマホで見られる仕組みに。天気情報との連携や入力ミス防止も検討	自作システム	③
工務店・建設業	社内のGoogleドライブの情報をAIに読ませて対話し、業務の標準化・マニュアル化	AI＋ドライブ	②
NPO事務・Web制作	スマホ講座の事務・月次集計を、月末に「よろしくね」の一言で全部終わる仕組みに。 事務担当者がAIエージェントでスキル化・自動化	Claude Code	④
コワーキング管理・商品開発	店頭ポップやLPを短時間で作り、どちらが効くか比べるテスト（ABテスト）まで	Claude Code	③
パソコン教室講師	空き地をスマホで撮ると、広さや雑草の高さから除草の見積もりを出すWebアプリを開発中	AI＋自作アプリ	③
ネット通販・CAD設計・農業	相続登記の書類作成。4年分の栽培環境データ（気温・湿度・気圧）で出荷予測をする構想	Claude	①～ ③
ショート動画制作	企画・シナリオをAIと壁打ちし、秒単位の構成を設計。生成画像を動画生成AIへ	各種生成AI	①
Webコンテンツ・サイネージ制作	人物音声の合成、背景合わせ、企画書作成。空室管理とカメラデータの掛け合わせに関心	各種生成AI	①
観光農園	広いハウスの巡回（1日約4万歩）や天候対応を、カメラとAIの自動判断・予約の自動化で減らしたい	検討中	—
民泊経営	監視カメラ映像からAIが火災や異常を検知し、すぐ通知する仕組みを相談中	検討中	—
コーヒー豆販売	AI初心者。ChatGPTでブランドロゴを作ったところから業務活用を学び始めた	ChatGPT	①
学術論文の活用・研究	AIで論文の要約・構造理解・分析・読解	各種AI	①～ ②

先進事例

講師（伊藤）の「任せるAI」運用

- 細かく指示する使い方から、仕事を丸ごと任せて結果だけ確認・承認する使い方へ
- 情報漏えいに備え、自社のPC・サーバーで動くAI（ローカルAI）も活用。人が指示を出すPCと、24時間動くPCの2台体制
- 過去にAIの鍵（APIキー）が漏れ、約6万8千円の不正請求を受けた経験から、鍵は専用の金庫で管理

創業約180年の老舗：「数億円級の仕組みを約10万円で」

- 検索キーワード、HPの滞在時間、予約ボタンの履歴、電話の要約、注文内容など、バラバラのデータをつないで売上・顧客の予測に
- 「考える仕事」はAI、「確実な集計」は普通のプログラムと役割分担し、AIに読ませる量を大幅に削減
- 教訓：小さな事業者でも、データをつなぎ役割分担させれば強力な仕組みが作れる

地域の現在地

Gemini Notebookで記録・要約する段階の人から、AIエージェントで業務を自動化する段階の人まで、**すでに同じ地域にいる**。支援する側より、相談に来る事業者のほうがAIに詳しい——そんな場面がこれから増えていく。

支援機関・各種団体の業務別AI活用（職員研修向け）

会員企業はAIを学び始めている。経営指導・補助金支援・事務のどこにAIを使うか、会員企業に勧められる形まで

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

会員企業は、もうAIを使い始めている

帝国データバンクの調査（2026年3月・約1万社）では、**企業の34.5%が生成AIを業務で活用**している（大企業46.5%、小さい企業でも28.0%）。支援を仕事にする専門家にも広がっていて、中小企業診断士は約7割が「仕事で使ったことがある」と答えた（2023年12月・124名の調査）。社労士は、全国の連合会が2024年に「生成AI活用ガイドブック」を公開している。

一方で、顧客の個人情報を扱う士業や支援機関は、守秘義務の観点から使い方に慎重になる事務所が多い、と指摘されている。だから差がつくのは「使うか使わないか」より、**情報の扱いのルール（D1）を決めて、安全に使い始められるか**。ルールのない組織は、動き出した会員に追い越される。

研修は「いつか」ではなく、いま始めるものになっている。

支援機関・各種団体の職員が、日々の業務にAIをどう使えるかの一覧（職員研修用）。「聞けば済む仕事」はGemini Notebookや普通のAI、「毎回同じ手順で書類を作って次に渡す仕事」はAIエージェント、という見分け方が基本。

業務別の活用例

業務	AIでどう変わるか	道具	段階の目安	信号
制度・補助金の資料の読み込み	制度ごとのノートブックで「資料係」をつくり、根拠付きで回答。組織内で共有	Gemini Notebook	②	●
相談内容が制度の対象かの一次確認	相談内容を入れて、対象になりそうかを根拠のページ付きで確認。最終判断は職員	Gemini Notebook	②	●
制度の更新対応・会員への案内	新しい資料が出たら、変更点まとめ・早見表・案内文の3点を一言で下書き。定期実行も	Claude	③→④	●
市場・業界調査	Deep Researchで下調べ → 公的データを足す → Gemini Notebookで裏取り	Deep Research + Gemini Notebook	②→③	●
経営計画づくりの壁打ち	事業者の強み・課題を引き出す質問リストをAIと作る。計画書はあくまで事業者本人の言葉で	ChatGPT / Claude	①	●

業務	AIでどう変わるか	道具	段階の目安	信号
巡回・窓口相談の記録	面談メモや録音から記録の下書きを作る	Gemini Notebook ／Claude	②→③	●
理事会・部会の議事録	録音から議事録と「次回までにやること」を作る	Gemini Notebook	②	●
セミナー告知文・会報・チラシ	たたき台を作り、職員が仕上げる。過去の会報をノートブックに入れると文体がそろふ	ChatGPT／ Gemini	①→②	●
記帳・税務・労務のよくある質問	組織内のFAQをノートブックにし、新人でも同じ根拠で答えられるように	Gemini Notebook	②	●
事業承継・創業相談のヒアリング準備	業種別の論点整理、質問リスト、公的データの下調べ	Deep Research／ Claude	①	●
決算書の分析	数字の推移や同業比較の整理	組織契約のAIで	①	●

段階：①相談相手 ②資料室（RAG）③スキル化 ④自動化。信号：● 公開情報中心 ● 匿名化すれば可 ● 組織契約とルール整備が前提（→ D1）

職員研修の最初の一步におすすめの3つ

1. 制度資料のノートブック

無料で今日から。制度を1つ選び、公募要領・FAQ・様式を入れて組織内で共有する（→ B1b）。

2. 更新対応のスキル

有料版で。変更点・早見表・案内文を一言で下書きするスキルを作る。慣れたら定期実行へ（→ F1）。

3. 市場調査の型

Deep Research → 公的データ → 裏取り、の流れを1件やってみて、手順を組織内で共有する（→ B3）。

会員企業に勧めるなら

この資料集は、業種を問わず会員企業の経営者・社員がそのまま使えるように書いてある。職員が使ってみて「これは勧めたい」と思った資料を、そのまま渡せる。

何から始めるか

A1 比較表・B1a 頼み方の基本・D1 信号機ルール

社員に使わせたい

D1 信号機ルール・A2 無料・有料・組織契約

自社の仕事に当てはめる

F1 業務の棚卸しと仕組み化・B2 データ管理の型

勉強会として開く

6コース（初級・中級・上級）や集中講座を、会員向けの勉強会として開けます。

支援の質の「標準」が上がっている

申請や経営の支援を仕事にする専門家にも、AIの活用が広がっている。競争ではなく、会員が期待する支援の水準が上がったということ。**地域の事情を知る職員×AIの速さ**は、とても強い組み合わせになる。

出典（2026年10月確認）

- 生成AIに関する企業の動向調査（2026年3月）（帝国データバンク）（<https://www.tdb.co.jp/report/economic/20260514-genai/>）：調査期間2026年3月17～31日、有効回答10,312社
- 生成AIを使いこなす中小企業診断士が急増（ハッシュタグ）（<https://prtimes.jp/main/html/rd/p/000000002.000125484.html>）：2023年12月、124名。調査は小規模で、当時のAI環境（Bing AIなど）での結果
- 社会保険労務士向け生成AI活用ガイドブック（全国社会保険労務士会連合会・2024年公開）（<https://cir.nii.ac.jp/crid/1520301919370285056>）
- 土業のAI活用：守秘義務の条文と事務所の環境・ルール（コプラス）（<https://coplus-one.jp/shigyo-ai/>）（二次情報）

事例：この資料集のスキル化・自動化

セミナー準備を「資料室→スキル化→自動化」で仕組みにした実例。人がやるのは方針・確認・公開だけ

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

対象ツール：Claude Code

考え方は、どのAIエージェントにも共通です。ただし、**ファイル名・画面・設定・コマンドは、Claude Code**（Claudeのデスクトップアプリの「Code」タブ）の場合です。ほかのAIエージェントでは、読み替えが必要です。

対象の方：開発者ではない方（経営者・事務・現場の担当者）。プログラミングは不要です。**コードは書かず、AIエージェントに頼んで、自分の業務アプリをつくる**ところまでを、順に進めます（ターミナルの黒い画面は、使わない形で書いています）。

いま見ているこの資料集そのものが、スキル化・自動化の実例です

「セミナーのたびに資料を作り直す」「AIの情報が古くなる」という講師自身の困りごとを、**資料室（RAG）→スキル化→自動化**の順で仕組みにした。人がやるのは「方針を決める」「確かめる」「公開ボタンを押す」の3つだけ。

全体の流れ

1

主催者と面談

人：面談シートで対象・人数・困りごとを聞く

2

「セミナー構成考えます。」

AI：級とコースを提案、音声解説の原稿と配布資料を作る

3

確かめる

人：内容・読み・レイアウトを確認

4

当日

音声解説→ヒアリング→コース→アンケート（QR）

5

毎週の点検

AI：最新情報の変化を検知して知らせる

4段階のどこで何をしているか

段階	この仕組みでの実物	担当
② 資料室（RAG）	この資料集（18本）と「AIの現在地」の記録。出典と「〇年〇月時点」を必ず付ける	クラウドのAIが作り、人が確認

段階	この仕組みでの実物	担当
③ スキル化	合言葉「 セミナー構成考えます。 」：現在地の確認 → 音声解説の原稿（Gemini Notebook用） → コース決定 → 配布資料（A4・2枚）まで同じ手順で作る 合言葉「 AIの現在地更新して 」：最新情報をWebで確かめ、古くなった資料を直してプレビューに出す	クラウドのAI（Claude Code）
④ 自動化	毎週土曜10時（米国の1週間の発表が出そろった後）、社内の24時間PCでローカルLLMが公式ページの変化・ニュース・リンク切れを調べ、変化の大きさの目安を付けてメールで知らせる	ローカルLLM（社内PC）
関所（人）	ホームページへの公開、資料の書き換えの確定、配布資料の印刷	講師

自動で作られるもの

配布資料（A4・2枚）

級（初級・中級・上級）とコースを指定するだけで、ヒアリングの質問・コースの時間割・資料QR・アンケートQRが入った配布資料ができる。**QRは作った後に読み取り直して、中身が正しいか自動で検証する。**

音声解説の原稿

「AIの現在地」の最新記録から、対象者に合わせた原稿とプロンプトを作る。組織名を読ませない、講師の呼び方など、過去の失敗をルールとして組み込み済み。

受講後アンケートの集計

アンケートは1つのフォームを使い回し、セミナーIDで回ごとに集計。研修や個別相談の希望が来たときだけ講師に通知。

実際に役立った場面

週次チェックの初回で「大きな変化」を検知

自動点検を動かした初日、ローカルLLMが公式の料金ページの変化を拾い、「**Claude Cowork がチャットと統合されてひとつの Claude になった（2026年9月16日）**」ことが分かった。資料のうち古くなっていた5本と配布資料を、その日のうちに直せた。

同時に分かった限界

同じ試験で、ローカルLLMは別の差分を読み違えた要約も出した。だから**ローカルLLMの役目は「見つけて知らせる」**まで。要約には根拠の原文を必ず引用させ、資料を直す判断と公開は人が行う（→ E2・E3）。

この事例から持ち帰れること

1. 自分の困りごとから始める：いちばん繰り返している仕事が、最初のスキル化の候補
2. 先に「資料室」を整える：出典と日付のそろった資料があれば、AIは毎回同じ品質で組み立てられる
3. 役割を分ける：賢さが要る仕事はクラウドのAI、毎週の見張りはローカルLLM、最後の確認と公開は人
4. 失敗をルールに変える：読み間違い・古い知識・勝手な公開——起きたことを1つずつ手順書に書き足していく

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、初期設定で入力が学習対象。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、鍵の漏れいで約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。

補助金申請とAI：使い方の注意

AIに書かせた計画書が不利になる理由と、申請する側・支援する側それぞれの正しい使い方

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

このページの読み方

補助金を**自社で申請する企業**にも、**申請を支援する側（支援機関・専門家）**にも当てはまる。どちらの立場でも、AIは「代わりに書く道具」ではなく「根拠をそろえる道具」。

AIに丸投げした計画書が増えている

補助金申請の世界では、AIで作った似たような構成・言い回しの計画書が大量に出ていると、申請支援の専門家が相次いで指摘している。汎用的な文章は、その会社ならではの計画に見えず、審査で不利になりうる。

公募要領で確認すべきこと（例：小規模事業者持続化補助金。ほかの補助金でも同じ観点で確認する）

項目	第20回（一般型・通常枠）の内容
公募要領	第20回・第8版（2026年7月21日）
申請受付	2026年11月5日～12月15日 17:00
様式4（事業支援計画書）の発行	12月4日まで（商工会・商工会議所が発行）
補助上限・補助率	通常50万円（特例の併用で最大250万円）／2/3（赤字事業者は3/4）
生成AIの利用	公募要領に「生成AI」という言葉は出てこない（禁止も許可も書かれていない）
事業者自身の検討	「事業者自らが検討しているような記載が見られない場合や、自らが検討していなかったことが発覚した場合、評価に関わらず不採択・交付決定取消」（注意事項）。AIに丸投げした計画書が危ない一番の根拠
第三者からの支援	「商工会・商工会議所を除く第三者からのアドバイスの有無」を様式2で申告。有償・無償を問わず、相手方と金額（着手金・成功報酬など）を書かないと虚偽として不採択・交付決定取消。商工会・商工会議所の支援は申告の対象外

内容は公募要領（第20回・第8版）の本文で確認済み（2026年9月30日）。**公募回・版ごとに変わるので、申請支援の前に必ず最新版で確認すること。**公募要領そのものをGemini Notebookに入れて確認するのが確実（→ B1b）。

AIの正しい位置づけ

× 代わりに書く道具

「この事業の計画書を書いて」と丸投げする。どの事業者でも似た文章になり、本人も説明できない計画になる。

○ 頭の中を引き出し、根拠をそろえる道具

ヒアリングの質問を考える、市場の根拠を集める、公募要領との整合を点検する、本人の言葉を読みやすく整える。

場面別：AIの使いどころ

場面	AIに任せてよいこと	人がやること
ヒアリング前	業種別の論点・質問リストの下準備	（支援する側）事業者と会って強みと想いを聞く／（申請する側）自社の強みと想いを言葉にする
市場動向	Deep Researchでの下調べ、公的データとの裏取り（B3）	どの数字を使うか選び、事業者を確認する
対象経費の確認	公募要領ノートブックで根拠のページを探す	最終判断。迷えば事務局に確認
計画書の点検	公募要領・審査項目と照らした抜け漏れチェック、表記の統一	内容の正しさ、事業者本人の言葉になっているか

コピーして使う

（Gemini Notebookに公募要領と計画書の下書きを入れて）この計画書の下書きを、公募要領の審査項目と照らして点検してください。記載が足りない項目、公募要領と食い違う記述があれば、根拠となる箇所と一緒に指摘してください。文章の書き直しはしないでください。

強みや想いは、本人の言葉でしか書けない

AIの速さで根拠をそろえ、浮いた時間を、自社を考える時間に（支援する側なら、事業者との対話に）使う。それが、AI時代の申請と支援の価値になる。

出典（2026年9月確認）

- 小規模事業者持続化補助金＜一般型 通常枠＞第20回 公募要領（第8版）（事務局・商工会地区）（<https://official.jizokukanb.com/s hinsei>）
- 小規模事業者持続化補助金（第20回）公募要領の公開（中小企業庁）（<https://www.chusho.meti.go.jp/koukai/hojyokin/kobo/2026/260527002.html>）
- 第20回 公募要領まとめ（行政書士潮海事務所）（<https://shiomi-gyosei.com/%E8%A3%9C%E5%8A%A9%E9%87%91%E3%83%BB%E5%8A%A9%E6%88%90%E9%87%91%E3%81%AB%E3%81%A4%E3%81%84%E3%81%A6/smallsub2026/>）（二次情報）

- 「AIで書いた申請書」が採択されない理由（ジャイロ総合コンサルティング）(<https://jairo.co.jp/blog/ai-de-kaita-shinseisho-saitakuriyu/>)

会社のAI利用ガイドラインとガバナンス：小さな会社の最小セット

A4 1枚のガイドライン・役割と手順・事故のときの動き方・台帳。建設・リフォーム業の線引き例と、公的な土台つき

更新日：2026-10-08（2026年10月時点の情報） | HUMAC 伊藤晴通

D1の「信号機ルール」は、**何を入れてよいか**を決める最初の一步です。会社として使い続けるには、その先の「誰が決めるのか」「事故が起きたらどうするのか」「どう見直すのか」も要ります。この資料は、**従業員が数名～数十名の会社**が、A4で2枚と台帳1枚から始められる形にしました（2026年10月時点）。

1. 3つの層で考える

層	決めること	分量の目安
① 方針	なぜAIを使うのか。何を大切にするのか（お客様の信頼、社員の働き方など）。社長の言葉で	数行
② ガイドライン	現場のルール。何を入れてよいか、誰が確認するか、してはいけないこと	A4 1枚（次の2章）
③ ガバナンス	運用の仕組み。誰が決め、誰が見て、事故のときにどう動き、どう直すか	A4 1枚＋台帳（3章・6章）

最初から完璧を目指しません。**A4で2枚＋台帳1枚で始めて、半年ごとに直す**のが現実的です。ルールが先で、道具が後。

2. 利用ガイドライン：A4 1枚のひな形

〔 〕を自社の言葉で埋めてください。

項目	書くこと（例）
1. 目的	〔お客様への提案の質を上げ、事務を減らすため〕にAIを使う。
2. 対象	〔社員・パート・協力会社〕が業務で使うすべてのAI。
3. 使ってよいサービス	許可リストに載せたものだけ。 個人の無料アカウントで業務をしない （個人のスマホでも同じ）。
4. 入れてよい情報・いけない情報	信号機ルール（D1）に従う。青＝入れてよい／黄＝条件つき／赤＝入れない。
5. 学習の設定	入力が学習に使われる設定を、許可リストの各サービスで オフ にする。確認するのは〔AI窓口〕。

項目	書くこと（例）
6. 出力の確認	AIの回答は必ず人が確認する。数字・法律・工法・価格は出典を開いて確かめる。お客様に出す前に〔上長〕が見る。
7. 著作権・他者の権利	他社の文章・画像・写真をそのまま入れて加工しない。AIが作った画像や文章が既存のものに似ていないか確認してから使う。
8. 個人情報	お客様の個人情報は、赤として扱う。入れる必要があるときは〔AI窓口〕に相談し、利用目的の範囲内か、学習に使われない設定かを確認してから。
9. 外に出る操作は人が承認	メール送信・公開・発注・支払いは、AIに任せきりにしない。最後は人が押す。
10. 困ったとき	入れてしまった／漏れたかもしれない、はすぐ〔AI窓口〕へ。早く言った人を責めない。
11. 見直し	〔半年〕ごと、またはサービスの料金・規約が変わったとき。

3. ガバナンス：役割・手順・記録

役割

役割	やること
経営者	方針を決める。ルールを承認する。最終責任を持つ
AI窓口（担当1名＋代理1名）	許可リストと台帳の管理／設定の確認／相談の受付／年2回の見直し／事故のときの連絡の中心
利用者	ルールを守る。迷ったら聞く。事故は早く報告する
協力会社	AIに入れてよい情報の範囲を、契約や覚書で合わせる（現場写真・図面・見積など）

新しいツールを使いたいときの5つの確認

1. 誰が運営しているか（会社名・所在地・連絡先が確認できるか）
2. 入力データの扱い（学習に使われるか。使われない設定があるか。A2参照）
3. 契約の形（個人か、組織か。退会したときデータはどうなるか）
4. 料金の上限（使った分だけ請求される形のときは、上限を決める）
5. 誰が使うか（全員か、担当者だけか）

確認が済んだら許可リストに載せ、台帳に1行足します（6章）。

事故が起きたときの手順

1. 止める：その場の入力をやめる。会話や共有を削除できるなら削除する（削除しても相手側に残る場合があります）。
2. AI窓口へ連絡：何を、どのサービスに、いつ入れたかを伝える。
3. 影響を確認：個人情報・取引先の情報・社外秘が含まれていたか。
4. 必要な連絡：お客様・取引先への連絡が要るか。個人情報の場合は、専門家や関係機関への相談も検討する。
5. 再発防止：ルールか設定か教育を直す。責める場ではなく、直す場にする。

教育と見直し

- **入社時と年1回**：ルールの説明は10～15分でよいので、**実際の失敗例**を使う。
- **半年ごと**：許可リスト・台帳・ルールを見直す。無料・有料の条件や学習設定は、予告なく変わることがあります。

AIエージェントを使うときは、権限を絞る

AIエージェントは、自分で調べて、操作して、送信まで進められます。**権限は必要な範囲だけにして、外に出る操作は人が承認し、操作の履歴を定期的に確認**します。国の「AI事業者ガイドライン」も、エージェントについて、権限の適切な設定・人の判断の介在・操作履歴の確認といった考え方を整理しています（5章）。

4. 業種別の線引き例：建設・リフォーム業

D1の信号機ルールを、建設・リフォーム業に当てはめたたたき台です。自社の仕事に合わせて直してください。

区分	例	扱い
● 青	一般的な工法・設備・制度の質問、公開済みのホームページやチラシの文案、お客様がよく調べそうなことの下調べ（例：水回りの一般的な悩み）	無料版でもOK
● 黄	施主名・住所を伏せた現場の状況説明、見積の考え方（単価は伏せる）、社名・個人名を伏せた議事録、現場写真（個人や場所が特定されないよう処理したもの）	許可リストのサービスで、学習オフを確認してから
● 赤	施主の氏名・住所・電話・家族の情報、図面や現場写真で施主が特定できるもの、見積単価・原価・協力業者との取引条件、契約書の原本、従業員の個人情報	入れない（必要なら、AI窓口が条件を決めてから）

現場写真の注意：表札・車のナンバー・人の顔・書類が写り込んでいないか、入れる前に確認します。

5. 公的な土台（この資料の根拠）

- **AI事業者ガイドライン（第1.2版）**：総務省・経済産業省、2026年3月31日公表。AIを使う側の事業者も対象。第1.2版では、AIエージェントについて、権限の適切な設定、人の判断の適切な介在、操作履歴の定期的な確認といった留意点が整理されています。経済産業省の検討会ページ
- **生成AIサービスの利用に関する注意喚起**：個人情報保護委員会、2023年6月2日。個人情報を含む入力、特定した利用目的の範囲内か確認し、事業者が入力データを機械学習に使わないことを確認する、という考え方が示されています。個人情報保護委員会（PDF）
- **AIと著作権に関する考え方について**：文化庁、2024年3月15日。生成物が既存の著作物に似ていないか（類似性）、既存の著作物に依拠していないか（依拠性）が、利用段階の判断の柱です。文化庁
- **生成AIの利用ガイドライン（ひな形）**：日本ディープラーニング協会（JDLA）、第1.1版（2023年10月）。条項のみ・簡易解説つき・画像編があり、無料でダウンロードできます。**自社のガイドラインは、このひな形を土台にして、本資料の役割・手順・業種別の線引きを足すと早い**です。JDLA 資料室

※ 上記は2026年10月時点の公表内容です。ガイドラインは改定されます。使う前に各ページで最新版をご確認ください。この資料は法的助言ではありません。個別の判断が必要なときは、弁護士などの専門家に相談してください。

6. 台帳のひな形（A4 1枚）

ツール	用途	プラン・契約	学習設定	使う人	確認日
〔例：Gemini（会社の契約）〕	〔文案づくり・調べもの〕	〔組織契約／有料〕	〔オフを確認〕	〔全員〕	〔 年 月 日〕
〔 〕	〔 〕	〔 〕	〔 〕	〔 〕	〔 〕
〔 〕	〔 〕	〔 〕	〔 〕	〔 〕	〔 〕

はじめてのAIエージェント：フォルダの置き場所・分け方・管理

先にここで、手を動かす。置き場所（クラウド同期は避ける）、顧客・アプリ・案件の分け方、AIに頼んで自分の事業に合わせる方法、指示書・現在地・決定ログ、完成の基準、会話の区切り方、戻せる仕組み、最初の30分

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

対象ツール：Claude Code

この資料は、**Claude Code**（Anthropic のAIエージェント。Claudeのデスクトップアプリの「Code」タブ）を前提に書いています。ほかのAIエージェント（OpenAI のCodex、Google のエージェントなど）は、**画面・用語・ファイル名・設定が異なります**。

対象の方：開発者ではない方（経営者・事務・現場の担当者）。プログラミングは不要です。**コードは書かず、AIエージェントに頼んで、自分の業務アプリをつくる**ところまでを、順に進めます（ターミナルの黒い画面は、使わない形で書いています）。

AIエージェントを使う前に、まず「場所」を決める

AIエージェントは、開いたフォルダの中を「自分の職場」として働く。資料があちこちに散らばっていると、AIも人も迷う。最初にやるのは、頼み方の工夫ではなく「**場所づくり**」。**1つの仕事=1つのフォルダ**にして、その中に「指示書」「現在地」「決めたこと」を置くと、別の日・別の人・別のPCでも、同じ品質で続きができる。

E1とE2は、セットで使う：先にここ（E1）で、手を動かす

このページ（E1）は「**置き場所と進め方**（どこに・どうやって）」。**先に、ここで、手を動かして、フォルダを作る**。続けてE2 ハーネスエンジニアリング入門（**考え方と6つの部品：なぜ・何を**）を読むと、「なぜ、そうするのか」が、腑に落ちる。勉強会・サロンでは、**E1（手を動かす）→ E2（考え方）**の順に使う。

1. 先に知っておく、2つの制約

このページのルールは、すべて次の2つから来ている（Claude Code の公式ドキュメントと、Anthropic の技術解説による）。

① AIは、毎回「白紙」から始まる

新しく会話を始めるたびに、AIは前回のことを覚えていない。**前回の続きを引き継ぐ唯一の方法は、ファイルに書いておくこと**。だから「指示書」「現在地」「決定ログ」が要る。

② 作業机（文脈）は小さく、いっぱいになるほど鈍る

会話・読んだ資料・実行結果は、すべて「作業机」に載る。机がいっぱいになると、**前の指示を忘れたり、間違いが増える**（「context rot」と呼ばれる）。だから「整理して、小さく保つ」「話題ごとに区切る」ことが、最も大事な習慣になる。

2. どこに置くか：クラウド同期フォルダは、避ける

仕事のフォルダ（AIに開かせるフォルダ）は、**パソコンの中（ローカル）**に置く。Google ドライブ・iCloud Drive・OneDrive・Dropbox のような**クラウド同期のフォルダの中には、置かないのが、おすすめ。**

置き場所	作業フォルダ	ひとつこと
パソコンの中 Mac：~/Projects Windows：C:\Users\名前\Projects	◎	ホーム（ユーザー）フォルダの直下に、Projects を作る。「デスクトップ」「書類」の中には、作らない（下の注意）
Google ドライブ（Drive for desktop）	×	資料の保管・共有には、向いている
iCloud Drive	×	Macの「デスクトップと書類フォルダ」の同期がオンだと、デスクトップ・書類の中身が iCloud Drive に保存される（Apple 公式）
OneDrive	×	「フォルダーのバックアップ」をオンにしていると、デスクトップ・ドキュメントなどが、同期の対象になる（設定による）
Dropbox など	×	同じ理由

なぜ、避けるのか（5つの理由）

理由	起きること
① Gitの管理ファイルが壊れる	同期サービスが、同時に変わったファイルを、「main 2」のような 番号つきの複製 にしまい、fatal: bad object というエラーで、保存・送信ができなくなる報告がある（iCloud Drive での事例）。直すのは、難しい
② 小さなファイルが大量で、同期が止まる	Gitや、AIが作る一時ファイルは、数千個になる。OneDrive が応答しなくなった報告があり、 OpenAI の Codex でも、「クラウド同期フォルダでの作業に、警告を出してほしい」という課題 が記録されている
③ 「オンラインのみ」のファイル	OneDrive の「オンラインのみ」のファイルは、 開くたびにダウンロード される（Microsoft 公式）。Google ドライブの「ストリーミング」も、ファイルは主にクラウドにあり、開いたときにダウンロードされる（Google 公式）。AIが、大量のファイルを読むと、遅くなる・失敗する
④ 鍵や実データが、自動でクラウドに上がる	知らないうちに、クラウドにコピーされる（D1・E6）
⑤ 同時に書き換えて、衝突する	AIが、多数のファイルを、短時間に書き換える。同期と衝突し、複製ファイルが増える

「必ず壊れる」わけではない。個人のメモ用途で、問題なく使っている人もいる。ただし、壊れたときに直すのは難しく、非開発者には、**避けるのが安全。**

最善の提案：3つの役割に分ける

1

① 作業場所＝パソコンの中

Projects（ホーム直下）。AIが開く・Gitがある場所

2

② バックアップ＝Git → GitHub（非公開）

仕事の履歴と、控え（E4）。加えて、パソコン全体のバックアップ

3

③ 受け渡し・共有・保管＝クラウドストレージ

完成した資料の共有、会社の資料室（Google 共有ドライブ。W2）

やりたいこと	やり方
クラウドにある資料を、AIに読ませたい	必要なものを、ローカルの inputs/ にコピーしてから読ませる（コピーも、AIに頼める）
できた成果物を、お客様・社内に共有したい	完成版を、クラウドの共有フォルダに、コピーする（仕事のフォルダは、そのまま、ローカルに置く）
複数のパソコンで、同じ仕事を続けたい	クラウド同期ではなく、GitHubで同期する（保存して送る／取り込む。E4）
会社として、資料をAIの根拠にしたい	共有ドライブを資料室にして、Gemini Notebook に入れる（W2）。ここは、同期ではなく、資料の置き場所

どうしても、クラウドの中で作業するなら（最低限の条件）

- Git を使わない、資料中心のフォルダに限る（.git を、同期の中に置かない）。
- Google ドライブは、「ストリーミング」ではなく、「ミラーリング」（ファイルを、常に、パソコンとクラウドの両方に持つ）にする。OneDrive は、そのフォルダを「常にこのデバイスに保持」にする。
- AIに、大量のファイルを作らせない。鍵・実データを置かない。

自分のフォルダが、同期の中にないかを、AIに確認してもらう（コピーして使う）：

コピーして使う

いま選んでいるフォルダの場所（パス）を調べて、iCloud Drive・OneDrive・Google ドライブ・Dropbox などの「同期フォルダ」の中ではないか、確認してください。中だった場合は、ホーム（ユーザー）フォルダ直下の Projects への、移動の手順を提案してください。移動・削除は、私の承認を得てからにしてください。

講師の実例

作業フォルダ（Projects）は、パソコンの中に置き、iCloud の同期の対象外にしている。バックアップは、GitHub の非公開の金庫。お客様の書類の保管・共有は、Google ドライブ。「作業場所」と「保管・共有」を分けるのが、基本の考え方。

3. 何の単位で分けるか：顧客ごと？ アプリごと？ 案件ごと？

「1仕事＝1フォルダ」の、「仕事」を、どう切るか。正解は、事業ごとに違う。ここでは、決めるための「基準」と「型」を示す。そのうえで、自分の事業に合わせて決める（AIと一緒に決める方法は、後半）。

切り方は、4つ

切り方	向く仕事	メリット	注意
顧客ごと	継続して関わる（顧問・保守・士業・コンサル）	顧客共通のルール・用語・担当者・守秘を、1か所に書ける	案件が混ざる。 顧客の中を、案件で、さらに分ける
案件ごと	期限と成果物がある（見積～納品、申請、イベント）	終わったら、まるごと退避（_archive）できる	同じ顧客の案件が、散らばらないように、顧客の下にまとめる
アプリごと	つくって、育てていく（社内アプリ、顧客向けアプリ）	Gitの単位=アプリ 。履歴・共有・引き継ぎが、アプリごとにきれい	顧客が複数のアプリを持つなら、顧客の下に、アプリを置く
業務ごと	自社の仕事を良くする（月次の請求チェック、問い合わせ返信など）	「F1の棚卸し」の単位と、そろう	部署が違っていると、見せてよい範囲が違う。部門で束ねる

迷ったら：5つの質問（上から順に）

#	質問	答えの使い方
1	AIに見せてよい範囲が、同じか？（守秘の境界。D1）	最優先 。別の顧客・別の部署・信号の色が違う情報は、 同じフォルダに入れない （AIが取り違える・漏らす）
2	AIに渡す、資料・ルール・言葉が、同じか？	同じなら、同じフォルダ。違うなら、分ける
3	引き継ぐ相手（担当者）が、同じか？	担当が変わる単位で、切ると、引き継ぎが楽
4	終わりがあるか？	案件＝あり（終わったら退避）。アプリ・業務＝なし（育てる）
5	契約・請求の単位は？	顧客か案件の単位と、そろえると、あとで整理しやすい

指示書は、3層に重ねられる（親のフォルダの指示書も、効く）

Claude Code は、作業フォルダの CLAUDE.md だけでなく、**その上のフォルダの CLAUDE.md も、連結して読む**（公式）。これを使うと、「顧客共通のルール」を、1回だけ書ける。

フォルダの形

Projects

clients … 顧客ごと

tanaka-sekkei … 顧客A

CLAUDE.md … ②顧客共通（守秘・用語・担当者・連絡の作法）

2026-monthly-check … 案件・業務 ◀ AIを開くのは、ここ

CLAUDE.md / STATUS.md / docs/ … ③この案件だけのルールと現在地

2026-booking-app … 同じ顧客の、別の案件

apps … 自社のアプリ（1アプリ＝1フォルダ）

work … 自社の業務（月次の請求チェックなど）

（全体の指示書 ~/.claude/CLAUDE.md … ①全部の仕事に共通）

- AIに開かせるのは、いちばん下（案件・アプリ・業務）のフォルダ。顧客フォルダを開くと、同じ顧客の別の案件の資料も、AIの範囲に入る。
- 顧客共通のルールは、顧客フォルダの CLAUDE.md に1回だけ書き、各案件には、案件だけの内容を書く。

事業のタイプ別：型の例

事業のタイプ	おすすめの切り方	フォルダの例
顧問・士業・コンサル（顧客に継続して関わる）	顧客 → 案件。顧客共通の指示書＋案件ごとの指示書	clients/顧客略称/2026-案件名/
受託でアプリをつくる	顧客 → アプリ。Git の単位は、アプリ	clients/顧客略称/アプリ名/
自社のアプリを育てる	アプリごと	apps/アプリ名/
店舗・製造・事務（自社の業務を良くする）	業務ごと。部署で束ねる	work/経理/月次請求チェック/
セミナー・発信・学習	テーマごと／開催ごと	seminar/2026-10-17-主催名/

Git・GitHub との関係

- 1つのフォルダ（Gitの単位）＝共有・引き継ぎの単位。顧客Aと顧客Bを、同じ保存先（リポジトリ）に入れない。
- お客様と共有する場合は、案件・アプリの単位で、共有する（顧客フォルダ全体を共有しない）。

名前の付け方

- 顧客：半角の英小文字とハイフンの略称（例：tanaka-sekkei）。会社名の変更があっても、フォルダ名は、変えない。
- 案件：西暦-内容（例：2026-monthly-check）。アプリ：アプリの名前。
- 日本語の説明は、フォルダの中の文書（運用ルール.md など）に書く。

自分の事業に合わせて、決める手順

1

1 仕事を書き出す

思いつく順に、10個。F1のステップ1

2

2 まとめる

「同じ資料・同じルール・同じ相手」で、グループにする

3

3 線を引く

AIに見せてよい範囲（守秘）が違うところで、必ず分ける

4

4 名前の規則を決める

顧客・案件・アプリの付け方

5

5 3か月使って、見直す

はじめから、完璧にしない。変えるのは、普通

AIに頼んで、決める（コピーして使う）

一般論ではなく、**自分の事業の言葉**で、AIに質問してもらいながら決める。

コピーして使う

私の事業は、〔業種・人数・何をしているか〕です。

仕事の例：〔月次の請求チェック／顧客Aの保守／新しいアプリの開発 など、思いつく限り〕

AIに見せてはいけない情報：〔個人情報・決算書・他のお客様の情報 など〕

仕事用のフォルダの構成案を、3つ出してください。それぞれ、①フォルダの例（図）、②向く理由、③取り違い・情報漏れのリスク、④3か月後に困りそうなこと、を比べてください。

いきなり決めずに、先に私に質問してください（1回3問まで）。フォルダを作る前に、必ず、私の承認を得てください。

いまのフォルダが散らかっているとき（提案だけ。移動はしない）

コピーして使う

〔いまのフォルダ〕の中身を調べて、仕事ごと・顧客ごとの整理案を出してください。ファイルの移動・削除・名前の変更は、しないでください（提案だけ）。案には、①新しいフォルダの構成、②どのファイルを、どこへ移すか（一覧）、③迷うもの（私に確認が必要なもの）、④消さずに退避するもの（_archive）を、入れてください。

顧客共通の指示書を作る

コピーして使う

顧客〔略称〕のフォルダに置く、顧客共通の CLAUDE.md を作りたいです。いきなり書かずに、先に私に質問してください（守秘のルール、用語、担当者、連絡の作法、やってはいけないこと、使う資料の置き場所など）。聞き終えたら、200行以内で、箇条書きで書いてください。個別の案件の内容は、書かないでください。

見直しのサイン

AIが、**別の案件・別のお客様の話を、持ち出す**／同じ説明を、何度もしている／探しものが多い／1つのフォルダで、共有する相手が違う。→ 分け方を、見直すタイミング。フォルダの移動は、**Git の履歴が切れる**ので、早めに。

4. 基本の構成：1仕事＝1フォルダ

「仕事のフォルダ」は、1か所にまとめる（デスクトップや書類フォルダにばらまかない）。名前は半角の英小文字とハイフンにすると、扱いやすい。

最初はこれだけ（軽量版）

フォルダの形

Projects … 仕事のフォルダは、すべてここ

monthly-invoice-check … 1つの仕事=1フォルダ

CLAUDE.md … ①指示書（AIが最初に読む。薄く）

STATUS.md … ⑤現在地（今どこまで・次にやること）

docs

決定ログ.md … ⑤決めたことと理由

inputs … 材料（請求書PDFなど。AIは読むだけ）

outputs … AIが作ったもの（下書き・集計表）

_archive … 退避（消さずに、ここへ移す）

慣れたら足す（フル版）

フォルダの形

monthly-invoice-check

CLAUDE.md / STATUS.md

RAID.md … ⑥気がかり帳（リスク・課題・前提・依存）

docs

運用ルール.md … この仕事の真実源（詳しい決まり）

決定ログ.md / 用語集.md

.claude

skills … ②スキル（この仕事の手順書）

settings.json … ③権限・④関所の設定

data … 実データ（⚠ 共有・保存の対象から外す）

.gitignore … 鍵（.env）・実データを、保存の対象から外す

AIは「開いたフォルダ」の中で働く

これは便利さであり、安全装置でもある。フォルダの外は、AIに触らせない（権限の範囲）。別の仕事の資料が同じフォルダにあると、AIがそちらを参照して取り違える。2つの仕事を、1つのフォルダで進めない。

5. 各ファイルの役割（E2の6部品との対応）

E2の部品	置き場所	役割	書き方のコツ	更新のタイミング
① 指示書	CLAUDE .md	AIが毎回最初に読む。この仕事の目的、置き場所、禁止事項	短く。目安は200行以内。「消してもAIが間違えない行」は消す（E2の4）	同じ訂正を2度したとき

E2の部品	置き場所	役割	書き方のコツ	更新のタイミング
② スキル	.claude/skills/	この仕事の手順書。呼んだときだけ読まれる	手順は指示書ではなく、スキルへ（F1の手順書）	手順が固まったとき
③ 権限	.claude/settings.json、フォルダの範囲、.gitignore	どこを読み、どこに書き、何を実行してよいか	最初は確認あり。安全と分かった操作だけ許可リストへ	新しい道具を使うとき
④ 関所	承認の設定、outputs/、_archive/	送信・公開・削除・支払いの前に、人が確認する	「書き込み先は outputs だけ」「消さずに _archive へ」と決めておく	外に出る操作を足すとき
⑤ 記憶	STATUS.md、docs/決定ログ.md	現在地と、決めたことの理由。次の会話に持ち越す	STATUS は「済んだこと／次の一手／待っていること」だけ。決定ログは、日付・決めたこと・理由・却下した案	毎回の作業の最後
⑥ 点検	RAID.md、週1回の点検	ルールと実態のずれ、残っている課題を確かめる	R（リスク）A（前提）I（課題）D（依存）で分け、閉じたら消す	週1回

6. 最初の30分：手を動かして、フォルダを作る

勉強会・サロンでは、ここを実際にやる。まず、小さくて、失敗しても取り返しがつく仕事を1つ選ぶ（例：毎月の請求書チェック、問い合わせメールの下書き）。

1

1 フォルダを作る
Projects の中に、仕事の名前（英小文字とハイフン）で。inputs・outputs・_archive も作る

2

2 AIに、質問させる
いきなり指示書を書かない。AIに「聞き取って」もらい、答えながら作る

3

3 指示書と現在地を作る
CLAUDE.md と STATUS.md を、AIに書かせる。人が読んで直す

4

4 関所を決める
送信・公開・削除は、人が押す。書き込み先は outputs だけ

5

5 小さな仕事で試す
1件だけ頼む。結果を人が確認し、直すところを指示書へ

6

6 保存して終える
STATUS に今日の到達点を書き、変更を保存する（Gitの準備はE4）

手順2：AIに「聞き取って」もらう（コピーして使う）

コピーして使う

この仕事（[仕事の名前]）の指示書（CLAUDE.md）を作りたい。いきなり書かずに、まず私に質問してください。

聞いてほしいこと：目的、出来上がりの形、使う資料と置き場所、やってはいけないこと、言葉づかい、迷ったときの判断。

1回に聞くのは3問まで。聞き終えたら、200行以内で、箇条書きで CLAUDE.md を書いてください。書いたら、足りないところを私に確認してください。

手順3：現在地ファイルを作る

コピーして使う

STATUS.md を作ってください。見出しは「済んだこと」「次の一手」「待っていること」「決めたこと（日付つき）」の4つだけ。今日の作業を反映して、次に私が開いたときに、これだけ読めば続きができる状態にしてください。

終わるときの合言葉（毎回）

コピーして使う

今日の作業を締めます。STATUS.md を更新し、決めたことと理由を docs/決定ログ.md に追記して、変更を保存してください。次回の最初にやることを、STATUS の先頭に書いてください。

「変更を保存してください」は、Git（E4）の準備ができていれば、そのまま動く。まだなら、この一文を除いて使う。

7. 仕事の進め方の型

公式ドキュメントと、長時間働くエージェントの設計（Anthropicの技術解説）に共通する、うまくいく進め方。

コマンドの名前は、覚えなくてよい

この資料は、Claudeのデスクトップアプリ（Codeタブ）の画面のボタンと、Claudeへの頼み方だけで進められるように書いてある。ターミナル（黒い画面）は開かなくてよい。コマンドは、慣れた人向けの「参考」として、小さく添えるだけにする。

① 先に調べて、計画してから、実行する

1

探索

読むだけ。何も変更しない
（プランモード）

2

計画

何をどの順で行うか、案を出させる。人が直す

3

実行

計画に沿って進める

4

確認・保存

結果を確かめて、変更を保存する

いきなり実行させると、「間違った問題を解く」ことがある。ただし、**1文で説明できるほど小さな変更**（誤字の修正など）は、計画を飛ばしてよい。

② 「完成の基準」を先に渡す

AIは「できたように見えた」ところで止まる。**確かめる方法が無いと、人が毎回、間違いを見つける係になる。**次のように、確認の手段を一緒に渡す。

曖昧な頼み方	完成の基準を付けた頼み方
請求書をチェックして	請求書PDF 30件を読み、金額・税率・日付を表にして。取引先リストと一致しないものを一覧にして。 最後に、件数の合計が合っているか確かめて、結果を見せて
メールを書いて	お客様への見積案内メールを下書きして。条件：です・ます調、200字以内、金額は見積書の数字をそのまま写す。 書いたあと、条件を1つずつ満たしているか確認して

- 「できました」という言葉ではなく、**確認した結果（数字・実行結果・画面）を見せて、**と頼む。証拠を見るほうが速い。
- 作った本人（AI）が、そのまま採点しない。**別の会話・別のAIに、「抜けがないか」を見てもらうと、**思い込みが入りにくい（作る人と見る人を分ける）。ただし、見る係に「問題を探して」と頼むと、必ず何か指摘する。**正確さと要件に関わる指摘だけ、**と範囲を決める。

③ 1度に1つ。終わったら確認して、保存する

長い仕事を一気に頼むと、AIは「全部できた」と早く宣言したり、途中で作業机がいっぱいになって中途半端に終わる、という失敗が起きやすい。Anthropicの設計では、次の工夫で防いでいる。

起きること	対策
「全部できた」と早く宣言する	やることの一覧 （チェックリスト）を最初に作る。人が確認してから、チェックを付ける
確認が足りないのに、完了にする	確認が終わったものだけ、完了にする
前の作業の続きが分からなくなる	進捗のメモ（STATUS）と、変更の保存を、1つ終わるごとに残す
やり方が毎回変わる	起動や実行の手順を、1か所（スキルやスクリプト）にまとめる

④ 会話は区切る：1つの仕事=1つのセッション

Claudeのデスクトップアプリでは、1つの会話を「セッション」と呼ぶ。左のサイドバーに一覧が並び、いつでも開き直せる。**仕事が変わったら、新しいセッションにする**（サイドバーの「+ 新しいセッション」。MacはCmd+N、WindowsはCtrl+N）。

状況	やること
別の仕事の話に移る	新しいセッションを始める。関係ない話が混ざると、精度が落ちる
同じことを2回直しても直らない	新しいセッションで、学んだことを入れた、より具体的な頼み方で、やり直す。直し続けるより、早い
会話が長くなった・今日は終わりにする	「終わりの合言葉」 （6章）で、STATUS.md と決定ログに書いてもらう。次は、新しいセッションで、STATUS を読ませて始める

状況	やること
続きを別の日にやる	サイドバーのセッション一覧から開き直す。または、新しいセッションで、STATUS.md を読ませる。セッションの名前は、上のタイトルをクリックして、分かりやすく付け直せる
調べものが大量になる	調べる役を「別の担当（サブエージェント）」に任せるよう頼む。結果の要約だけが戻るので、作業机が汚れない

講師のやり方：「会話を整理する」より「ファイルに書いて、新しく始める」

講師自身は、会話の要約（/compact）や、会話の消去（/clear）のコマンドは、ほとんど使っていない。作業の最後に、「締めます」の一言で、**STATUS・決定ログ・保存まで書き出し**、次は新しいセッションで、続きから始める。覚えておくことは、**会話の中ではなく、ファイルの中に置く**。これなら、コマンドを覚えなくても、毎回、同じ品質で続けられる。

参考（慣れた人向け）：会話を要約して縮める /compact、会話を消して新しく始める /clear、前の会話を選んで再開する --resume。ただし、要約すると、会話の中だけで伝えた指示は失われやすい。残したいことは、ファイルに書く。

⑤ いつでも戻せるようにする

- **変更は、確認してから受け入れる**：最初は「確認あり（Manual）」のモードにしておくと、Claudeがファイルを書き換える前に、**何がどう変わるか（差分）を画面で見え、**「承認」か「却下」を選べる。受け入れたあとも、変更のあった行数（例「+12 -1」）をクリックすると、変更の一覧を、あとから見直せる。
- **取り消したいとき**：「さっきの変更を、取り消してください」と頼む。ただし、AIの巻き戻し機能で戻せるのは、**AIが直接編集したファイルだけ**。コマンドで消したものや、外部への操作は戻せない。バックアップの代わりにはならない。
- **変更履歴（Git）が本命**：フォルダごと履歴で管理すると、「昨日の状態に戻す」ができる。難しい操作は不要で、Claudeに「保存して」と頼めばよい。**導入と設定は E4 Gitの導入と設定**（ターミナルなしで進められる）。
- **消さずに退避する**：不要に見えるファイルも、_archive へ移すだけにする。消すのは、最後に人が決める（E2の事故の実例）。

⑥ 同じフォルダで、2つのセッションを同時に動かさない

同じファイルを、2つのセッションが同時に書き換えると、衝突する。並行して進めるなら、**作業用のコピー（ワークツリー）**か、別のフォルダに分ける。デスクトップアプリでは、新しいセッションを作るときに、ブランチ名の横の「worktree」を選ぶと、そのセッション専用の独立したコピーで動く（Gitが必要。→ E4）。初めは「1フォルダ・1セッション」で十分。

8. 安全な置き場所の設計（E2の「権限」「関所」とつなぐ）

置き場所	AIの権限	信号
inputs/	読むだけ	● ～ ● 公開情報／匿名化した資料
outputs/	書いてよい（下書きまで）。送信・公開は人	●
_archive/	移すだけ。消さない	—

置き場所	AIの権限	信号
data/（実データ）	必要なときだけ、人が許可。保存・共有の対象から外す	● 個人情報・決算書など（D1）
鍵・パスワード	ファイルに書かない。専用の金庫（Vault）に置く（→ E6）。AIに、鍵のファイルを読ませない設定も入れる	●

- 「必ず守らせたい」ことは、指示書に書くだけでなく、**仕組みで止める**：指示書はAIへの「お願い」で、強制ではない。権限の設定や、決まった場面で自動で動くチェック（フック）で止める（E2の4-1）。
- **最初は「確認あり（Manual）」で始める**：入力欄の横のモード選択で選べる。Claudeがファイルを書き換えたり、コマンドを実行したりする前に、確認が出る。慣れて、安全と分かった操作だけ、許可する範囲を広げる。確認ボタンを、読まずに押し続けるようになったら、設定を見直すサイン。

9. 名前と整理のルール

- **日付と版を名前に入れる**：「最新版（修正）2.docx」は、すぐ嘘になる（→ B2）。
- **日本語のファイル名もよい**：「運用ルール.md」「決定ログ.md」は、見た瞬間に中身が分かる。勉強会で説明なしに伝わる、という利点もある。
- **真実源は1か所**：同じ内容を2か所に書かない。指示書には「詳しくは docs/運用ルール.md」と案内だけを書く。
- **他のAIツールと共用するなら**：多くのAIツール（20以上、OpenAI の Codex など）は、「AGENTS.md」という共通の指示書を読む。Claude は、CLAUDE.md が無いときだけ AGENTS.md を読む。両方使うときは、CLAUDE.md の中から取り込む。

10. フォルダを「育てる」：週1回の点検

最初から完璧なフォルダは作れない。失敗を1つずつ、ファイルに書き足して育てる。

こんなとき	やること
同じ間違いを、2度された	指示書に1行足す（具体的に、守れたか確かめられる形で）
同じ説明を、また入力した	指示書が決定ログに書く
指示書が長くなってきた	手順はスキルへ、一部の場所だけのルールは近くのファイルへ（E2の4-5）
AIが、指示を守らなくなった	指示書が長すぎて埋もれていないか、指示が食い違っていないかを見る。1行だけ強調してもよい

コピーして使う

（週1回の点検用）

このフォルダを点検してください。①CLAUDE.md が200行以内か、古い指示・食い違いがないか
②STATUS.md が最新か ③RAID.md の閉じられる項目 ④_archive に移したほうがよいファイル ⑤鍵や実データが、保存の対象に入っていないか。結果を表で報告してください。直す前に、私の確認を取ってください。

11. よくある失敗と、直し方

何でも1つの会話でやる

別の話が混ざり、作業机が散らかる。話題ごとに会話を新しくする。

直し続ける

2回直して直らなければ、新しい会話で、具体的な頼み方からやり直す。

指示書が長すぎる

半分は読まれない。「消しても間違えない行」は消す。手順はスキルへ。

確認の手段が無い

「もっともらしい」結果をそのまま使ってしまう。完成の基準と、結果の証拠を求める。

範囲を決めずに調べさせる

大量の資料を読み、作業机がいっぱいになる。範囲を絞るか、別の担当に任せる。

混ぜる

2つの仕事を1つのフォルダで進めると、別の資料を参照して取り違える。1仕事1フォルダ。

鍵を書いてしまう

共有やバックアップで漏れる。鍵は金庫に置き、保存の対象から外す。

「最新版」だらけ

日付と版を名前に入れる。古い版は `_archive` へ。

12. はじめての日のチェックリスト

- ☐ 確認すること
- ☐ 仕事を1つ選んだ（小さく、失敗しても取り返しがつく）
- ☐ 1仕事=1フォルダを作り、`inputs`・`outputs`・`_archive`を用意した
- ☐ AIに質問させて、`CLAUDE.md`を作り、200行以内で、人が読み直した
- ☐ `STATUS.md`を作った（済んだこと／次の一手／待っていること）
- ☐ 送信・公開・削除は人が押す、と決めた（書き込み先は `outputs` だけ）
- ☐ 鍵や実データを、フォルダに置かない、または保存の対象から外した
- ☐ 1件だけ試して、完成の基準で確かめた
- ☐ 変更履歴（Git）の準備ができた（→ E4）。まだなら、次回までの宿題にする
- ☐ 終わるときに、`STATUS`を更新し、変更を保存した
- ☐ 次回の最初にやることを、`STATUS`の先頭に書いた

勉強会・サロンでの使い方（E1とE2をセットで）

1. **E1（60分）**：まず、置き場所（2章）と、分け方（3章）を、自分の事業で決める。そして、6章の「最初の30分」を、全員で実際にやる。各自の仕事を1つ選び、フォルダ・指示書・STATUSを作り、1件だけ試す。
2. **E2（30分）**：手を動かしたあとで、「なぜ、そうするのか」。ハーネスとは何か、6つの部品、mdファイルの役割と行数の限界、事故から生まれたルール。
3. **E4（事前または当日に別枠で）**：Git と GitHub の導入と設定（①②を実際にやる）。ターミナルは使わない。
4. **宿題**：1週間、終わりの合言葉で STATUS を更新する。翌回に、「2度された間違い」を指示書に足した例を持ち寄る。

関連資料

- E2 ハーネスエンジニアリング入門 … 考え方と6つの部品。mdファイルの行数の限界
- E4 Gitの導入と設定 … 変更履歴という「保存の金庫」。ターミナルなしで進められる
- F1 業務の棚卸しと仕組み化 … 手順書の書き方（スキルの材料）
- B2 データ管理の型 … 資料の置き方・名付け方
- D1 信号機ルール … 入れてよい情報・いけない情報
- G1 1日集中合宿 / G2 2日集中合宿

出典（2026年10月確認）

- Best practices for Claude Code（Anthropic 公式）（<https://code.claude.com/docs/en/best-practices>）：文脈の制約、完成の基準、探索→計画→実装、会話の区切り方、巻き戻し、並行作業、よくある失敗
- How Claude remembers your project（Anthropic 公式）（<https://code.claude.com/docs/en/memory>）：CLAUDE.md・自動メモリ・AGENTS.md の扱い
- Effective harnesses for long-running agents（Anthropic）（<https://www.anthropic.com/engineering/effective-harnesses-for-long-running-agents>）：進捗ファイル、機能リスト、変更の保存、1度に1つ、確認してから完了にする
- Effective context engineering for AI agents（Anthropic）（<https://www.anthropic.com/engineering/effective-context-engineering-for-ai-agents>）：文脈は有限の資源、外部ノート、サブエージェント、必要なときに取り込む
- AGENTS.md（オープンな指示書の形式）（<https://agents.md/>）

ハーネスエンジニアリング入門

考え方と6つの部品（E1のあとに読む）。mdファイル（指示書・メモリ・スキル）の使い方と行数の限界、ルールを置く場所の決め方、採点表、事故から生まれたルール、10の確認

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

対象ツール：Claude Code

考え方は、どのAIエージェントにも共通です。ただし、**ファイル名・画面・設定・コマンドは、Claude Code**（Claudeのデスクトップアプリの「Code」タブ）の場合です。ほかのAIエージェントでは、読み替えが必要です。

対象の方：開発者ではない方（経営者・事務・現場の担当者）。プログラミングは不要です。**コードは書かず、AIエージェントに頼んで、自分の業務アプリをつくる**ところまでを、順に進めます（ターミナルの黒い画面は、使わない形で書いています）。

先に E1（フォルダの作り方）で、手を動かすと、読みやすい

このページは「考え方」（なぜ・何を）。E1で、**仕事のフォルダ・指示書・現在地を、実際に作ってから読む**と、各部品が、自分のフォルダのどこにあたるか、すぐ分かる。

ハーネスとは「馬具」のこと

AIエージェントは力の強い馬。放っておくと、頼んでいない相手にメールを送ったり、消してはいけないファイルを消したりする。**手綱と装具（ハーネス）を付けて、決めた道を安全に走らせる仕組みづくり**が「ハーネスエンジニアリング」。AIを賢くするより、**AIが間違えても事故にならない形**を作ることが仕事の中心になる。

1. まず1枚の絵：エンジンと車体

AIモデル＝エンジン

ChatGPT・Gemini・Claude の「頭脳」にあたる部分。とても高性能だが、エンジンだけでは走れない。

ハーネス＝車体まわり一式

ハンドル・ブレーキ・ナビ・シートベルト。エンジンを「目的地まで安全に走れる車」にする仕組み。私たちが普段さわっているのは、実はこちら。

NVIDIAのジェンスン・フアンCEOは2026年5月、エージェントは言語モデルの上で直接動くのではなく、その手前に挟まる「**安全に管理されたソフトウェア層**」の上で動くと説明した。この層が担うのは、考えて道具を使う手順の繰り返し、外部システムの呼び出し、モデルの使い分け、記憶と文脈の管理、そして暴走の停止や行動の記録。

「賢いAI」と「使えるAI」は別物

質問して答えをもらうだけなら、ハーネスは薄くてよい。しかし「AIが自分でメールを送る・データを更新する・複数のシステムをまたいで作業する」ようになると、**何を許すか・どこで止めるか・何を記録するか**の設計が要る。同じモデルでも、ハーネスの出来で「使い物になるか」が決まる。

2. なぜ今、大事なのか

- **モデルの差が縮まった**：どの会社のAIも、一定以上に賢い。差がつくのは「どう仕事につなぐか」の側になった。
- **人間の統制は、機械の速度に間に合わない**：人の担当者なら、権限・承認・監査で管理できた。AIは人間よりずっと速く複数のシステムを動かすので、別の設計が要る。
- **失敗の多くはモデルではなくハーネス側にある**：権限が広すぎた、資料が古かった、止める条件がなかった。「もっと賢いAIにすれば解決する」とは限らない。

3. ハーネスの6つの部品

部品	たとえ	中身	Claude での実体	これが無いと
① 指示書	新人に渡す「職場のルールブック」	この仕事の目的、置き場所、やってはいけないこと、言葉づかい	プロジェクトごとの CLAUDE.md	毎回、同じ説明をする。人によって結果が違う
② スキル	業務ごとの手順書	「この仕事はこの順で、この資料を見て、この形で仕上げる」	スキル（合言葉で呼び出す）	毎回ゼロから頼む。品質がばらつく
③ 権限	渡す鍵の範囲	読んでよい場所・書いてよい場所・使ってよい道具	許可設定（ファイル・コマンド・外部サービスごと）	触ってはいけないものに触れてしまう
④ 関所（承認）	判子が要る書類	送信・公開・削除・支払いの前は、必ず人が確認する	承認の確認画面、フック（自動チェック）	取り返しのつかない操作が、人の知らないうちに実行される
⑤ 記憶	引き継ぎノート	前回の失敗・決まったこと・好みを次回に持ち越す	メモリ、決定ログ、STATUS	同じ失敗と説明を、何度も繰り返す
⑥ 点検	定期監査	ルールと実態がずれていないか、定期的に確かめる	週次の自動点検（定期実行）	ルールが古くなり、いつの間にか守られなくなる

6つの部品は、フォルダの中のどこに置くか

① 指示書＝CLAUDE.md／② スキル＝.claude/skills/／③ 権限＝.claude/settings.jsonとフォルダの範囲／④ 関所＝承認の設定と、書き込み先（outputs/）・退避（_archive/）／⑤ 記憶＝STATUS.mdと決定ログ.md／⑥ 点検＝RAID.mdと週1回の点検。実際の作り方と進め方は E1 はじめてのAIエージェント：フォルダ構成と管理。

4. mdファイル：ハーネスの本体は「文章」

Claude Code のハーネスは、プログラムではなく、**人が読める普通の文章ファイル（Markdown＝「.md」）**で作る部分が多い。AIは会話のたびに「白紙」から始まるので、**前回の学びと、守ってほしいルールを持ち越す手段は、mdファイルしかない**。ここを理解すると、プログラムが書けなくても、AIの振る舞いを設計できる。

4-1 3種類のmdファイルと、それぞれの役割

ファイル	誰が書く	いつ読まれる	一言でいうと
CLAUDE.md（指示書）	人	セッションの開始時に、毎回	「このルールで働け」
メモリ（MEMORY.md + 個別のメモ）	Claude が自分で書く	目次（MEMORY.md）は毎回。個別のメモは必要になったとき	「前に教わったこと」
SKILL.md（スキル）	人（Claude と一緒に作ってもよい）	呼んだとき、または必要と判断されたとき	「この仕事のやり方」

mdは「お願い」であって、「強制」ではない

CLAUDE.md は、Claude に渡される**文脈**で、設定のように強制されるものではない。曖昧な指示や、食い違う指示は、守られないことがある。**必ず守らせたいこと（送信・削除・公開の前の確認など）は、md に書くだけでなく、権限の設定やフック（決まった場面で自動で動くチェック）で、仕組みとして止める（→④関所）。**

4-2 置き場所＝効く範囲

置き場所	効く範囲	向く内容
組織の管理者が置く場所（OSごとに決まった場所）	その組織のすべての利用者	会社の規程、セキュリティの方針
~/ .claude/CLAUDE.md	自分の全セッション	言語、秘密情報のルール、共通の作法
案件のフォルダ/CLAUDE.md（または .claude/CLAUDE.md）	その案件のセッション。共有できる	案件の目的、置き場所、ルール、依頼例
CLAUDE.local.md	その案件・自分だけ（共有しない）	個人の作業メモ
サブフォルダの CLAUDE.md	そのフォルダのファイルを読んだときだけ	部分的なルール
.claude/rules/ のmd	パスを指定すると、該当するファイルのときだけ。指定なしは毎回	テーマごとに分けたルール

- **上書きではなく、連結される**：見つかったすべての CLAUDE.md が、文脈に並べて読み込まれる。広い範囲のものが先、作業フォルダに近いものが後。食い違うときは、近いほうが優先されやすい。
- **どこで開いたかで、読まれるものが決まる**：案件のフォルダで開けば、その案件の CLAUDE.md とメモリが載る。全案件に効かせたいことは、全体用に昇格させる。

4-3 行数・サイズの限界（2026年10月時点・公式の数字）

対象	限界・目安	超えとどうなるか
CLAUDE.md（1ファイル）	200行以内が目安。それより長くしない	文脈を多く使い、守られにくくなる。長いと、起動時などに警告が出る。4MiBを超えると、そもそも読み込まれない
メモリの目次（MEMORY.md）	起動時に読まれるのは、先頭200行、または25KBの、先に来たほうまで	それ以降は読み込まれない（書き込み自体はできる）。1記憶1行、詳細は個別のメモに分ける
メモリの個別ファイル	起動時には読まれない	必要になったとき、Claude が読みに行く
SKILL.md（本体）	500行以内が目安。詳細は別ファイルへ	呼ぶたびに全部が文脈に載るので、長いほど毎回のコストが増える
スキルの説明文（description）	説明文＋使う場面の合計で1,536文字まで（一覧に載る分）	それ以降は一覧で切れる。「いつ使うか」を先頭に書く
@で読み込む別ファイル（import）	入れ子は最大4段まで	整理には役立つが、読み込む量は減らない（起動時にすべて読む）
.claude/rules/（パス指定なし）	起動時に毎回読まれる（CLAUDE.md と同じ扱い）	長くしたくなったら、パス指定で「該当するファイルのときだけ」にする

行数の限界は「機械的に切られる線」ではなく、「長いほど守られにくい」という目安（CLAUDE.md）と、「それ以降は読み込まれない」という線（メモリの目次）の2種類がある。長い文章の中ほどが見落とされやすいことは、研究でも知られている（→①）。

4-4 使い方の原則

- **書くタイミング**：「同じ間違いを2度された」「前回と同じ訂正を、また入力した」「新しく来た人にも同じ説明が要る」。毎回説明し直していることを、文章にする。
- **書くこと**：毎回必要な事実（ルール、置き場所、言葉づかい、「必ずこうする」）。**書かないこと**：複数の手順（→スキルへ）、一部の場所でしか要らないこと（→サブフォルダやパス指定へ）、ファイルを見れば分かること（古くなって嘘になる）。
- **確かめられる具体さで書く**：「ちゃんと書いて」は守りようがない。次のように、守れたかが分かる書き方にする。

曖昧な書き方	確かめられる書き方
丁寧な文章で	「です・ます調」で、1文は60字以内
資料は整理して置く	見積書は「営業/見積書」に、ファイル名は「会社名_日付_v番号」で保存する
メールは気をつけて	メールは下書きまで。送信はしない

- **見出しと箇条書きで整理する**：長い文章より、構造のあるほうが、AIも読みやすい。
- **食い違う指示を残さない**：矛盾があると、AIはどちらかを適当に選ぶ。追記を重ねたら、定期的に読み直して、古い指示や矛盾を消す。点検は、Claudeに頼めばよい（「CLAUDE.md を点検して。古い指示・存在しないファイル

への言及・食い違いを、一覧で報告して。直す前に、私に確認して」)。Claude Code には、同じ点検をする機能（/doctor prompt-audit）もある（新しいバージョンのみ）。

- **人間向けのメモは、コメントで書ける**：行頭のHTMLコメント（<!-- ... -->）は、AIに読み込まれず、文脈を使わない。
- **会話の中だけで伝えた指示は、消える**：長い会話を要約（コンパクト）したとき、案件の直下の CLAUDE.md は読み直されて残るが、会話の中で言っただけの指示は失われる。残したいことは、ファイルに書く。
- **他のAIツールとの共用**：他のツールが使う指示書（AGENTS.md）がある場合、CLAUDE.md が無いときだけ読まれる。両方使うなら、CLAUDE.md の中から取り込む。

4-5 長くなったときの直し方（優先順位）

1

1 自明なことを消す
ファイルを見れば分かること、古くなった情報

2

2 手順はスキルへ
複数のステップは、呼んだときだけ読まれるスキルに

3

3 場所で分ける
その案件だけ、そのフォルダだけのルールは、近くのパイルへ

4

4 詳細は別ファイル+案内だけ
本体には「詳しくはここ」だけ書く（※@で取り込むと、量は減らない）

コピーして使う

（行数の点検：ターミナルは使わず、Claudeに頼む）

このフォルダの CLAUDE.md と、全体用の CLAUDE.md の行数を数えて、200行を超えていないか教えてください。メモリの目次（MEMORY.md）も、行数とサイズ（KB）を教えてください。

4-6 確認のしかた：コマンドより、Claudeへの頼み方

ターミナルが苦手でも大丈夫。やりたいことを、そのままClaudeに頼めばよい。コマンド（右の列）は、慣れた人向けの参考で、デスクトップアプリでは、使えないものもある。

やりたいこと	Claudeへの頼み方	（参考）コマンド
読み込まれている指示書・メモリの確認。「書いたのに効かない」ときは、まずこれ	「いま読み込んでいる指示書とメモリを、ファイル名と行数で一覧にして」	/context、/memory
指示書のひな形を作る	「この仕事の CLAUDE.md を作って。書く前に、私に質問して」（コードの無い案件は、先に議論してから作るほうがよい）	/init

やりたいこと	Claudeへの頼み方	(参考) コマンド
指示書の点検	「CLAUDE.md を点検して。長すぎる所、古い所、食い違いを報告して。直す前に確認して」	/doctor
覚えさせたいことを、ファイルに残す	「これを CLAUDE.md に追記して」(自動メモリに残したいときは「覚えておいて」)	/memory

講師の実例

- 全体用の CLAUDE.md は約70行、案件用は約40行。毎回読まれるものは、短く保つ。
- 詳しいルールは別ファイル（真実源）に置き、指示書には「どこを見るか」だけを書く。
- スキルの一覧は指示書に書かない。各スキルの説明文が自動で読まれるので、二重管理を避ける。
- メモリには、教訓だけを1行ずつ。長くなったら整理する（上の「限界」の表）。

5. 部品を、もう一段くわしく

① 指示書：短く、判断を書く

- **毎回読み込まれる**ので、長いほど損をする（目安は200行以内。くわしくは上の「4. mdファイル」）。コストがかかるうえ、肝心のルールが埋もれる（長い文章の真ん中は、見落とされやすいことが研究で知られている）。
- **書くこと**：目的／置き場所／やってはいけないこと／言葉づかい／「ここを見れば分かる」という場所。**書かないこと**：フォルダー一覧の丸写しなど、ファイルを見れば分かること（すぐ古くなって嘘になる）。
- **置き場所＝効く範囲**：全員共通のルールは全体用に、案件ごとのルールは案件のフォルダに。詳しい規則は別ファイルに置き、指示書にはそこへの案内だけ書く（真実源を1か所にする）。
- **矛盾する指示を同居させない**：「記録を必ず残す」と「メモは書かない」が両方あると、AIは迷う。
- **一律の禁止より、判断の軸**：Anthropicは2026年7月、最新のモデルは「周囲に合わせて」と判断を渡すほうが、細かい一律ルールで縛るより良く働く、と整理している。
- **秘密（パスワード・鍵）は絶対に書かない**。指示書はコピーされ、チャットにも読み込まれる。

コピーして使う

【この仕事の目的】 お客様への見積案内メールの下書きを作る

【置き場所】 見積書の雛形は「営業/見積書の雛形」。過去の案内文は「営業/案内文」

【言葉づかい】 丁寧語。「させていただく」は使いすぎない

【やってはいけないこと】

- 送信しない（下書きまで）
- お客様の個人情報を、AIに入力する文章に含めない
- 金額は、見積書の数字を写す（計算し直さない）

【迷ったら】 作らずに、私に質問する

② スキル：必要なときだけ呼ぶ手順書

- 指示書は「常に読まれる」、スキルは「呼んだときだけ読まれる」。手順は、指示書ではなくスキルに入れると、軽く保てる（段階的に開く、という考え方）。
- スキルの中身は、F1の手順書の5項目（出来上がり・材料・手順・人が確認するところ・例外と目安）。
- 置き場所で効く範囲が決まる。どのフォルダからでも使うなら全体用、その案件だけなら案件のフォルダ。

③ 権限：必要な分だけ、渡す

鍵は仕事に必要な最小限だけ渡す。「念のため全部」は事故のもと。

区分	考え方	例
● 自由にしてよい	読むだけ、元に戻せる、社内で完結	資料を読む、下書きファイルを作る
● 確認してから	元に戻しにくい、または外に影響する	既存ファイルの上書き、決まった手順以外のコマンド
● させない（できなくする）	事故になる、取り返しがつかない	メール送信・公開・削除・支払い、本番データの書き換え

④ 関所：ルールを「どこに置くか」はリスクで決める

ここが一番大事。指示書に「やらないでね」と書くだけでは足りない。AIは確率で動くので、ルールを「ほぼ」守るが、「必ず」ではない。長い文章の中で忘れる、外から紛れ込んだ文章に上書きされる、解釈を間違える、という理由がある。

破られたときの影響	ルールを置く場所	例
致命的でない	指示書（お願い）	文体、言葉づかい
業務が回らなくなる	スキル（手順として組み込む）	請求書チェックの手順
事故になる	関所・権限（AIの外側で、できなくする）	個人情報の外部送信、メールの自動送信、ファイルの削除

原則：「信頼して検証する」ではなく、「できないようにする」

ウェブの世界で、入力チェックを画面側だけでなく、サーバー側でも行うのと同じ考え方。AIが何を考えていても、外側の仕組みが止める。事故になる種類は、「お願い」ではなく仕組みで止める。

⑤ 記憶：4種類を使い分ける

プリンストン大学の研究者が提案した整理（CoALA）では、AIエージェントの記憶は4種類。

種類	役割	Claude での実体
作業中の記憶	今この瞬間の作業（会話・直近のデータ）。セッションが終わると消える	会話の中身
知っていること	事実・規約・制約。常に読み込まれる	指示書（CLAUDE.md）

種類	役割	Claude での実体
やり方	実行手順。必要なときだけ呼ばれる	スキル
経験	過去のやりとり・決定・結果から得た教訓	メモリ、決定ログ

- **経験は「蒸留」して残す**：生のやりとり全部ではなく、教訓だけを残す（例：45分の会話ではなく、「作業を始める前に、必ず対象の環境を確認する」の1行）。
- **忘れる仕組みも要る**：状況が変われば、古い教訓は捨てる。何を捨てるかが、使い勝手の質を決める。
- **記憶は、置き場所で効く範囲が決まる**：案件ごとの記憶は、その案件を開いたときだけ載る。全部の案件に効かせたいことは、全体用の指示書へ昇格させる。

⑥ 点検：1回で終わらせず、回し続ける

型	起動	止まり方	向く仕事
対話型	人が頼むたび	1往復ごとに人が判断	日常の相談・下書き
ゴール型	完了条件を決めて頼む	条件を満たしたら止まる	1つの作業を仕上げる
時間型	毎週・毎日など、決めた時間	実行が終わったら止まる	週次の点検、定期レポート
自律型	きっかけがあれば人の関与なしに起動	AIの判断	最も自律的。関所の設計が最重要

- **点検は、未解決を翌週に持ち越す**：指摘して終わりにせず、台帳（簡単なメモでよい）に残して、「先週の指摘は直ったか」を次の点検で確かめる。
- **AIが直して、AIが確認して、人が見ない**、という並びは避ける。自動で直した箇所は、次の点検で再検証する。
- 点検は、「新しく長持ちするものを作る」仕事ではなく、「調べて報告する」仕事に向く。

6. 「採点表」を持つ（評価）

動かして終わりではなく、「**良い仕事**」の基準を数字にして、測る。Microsoftのサティア・ナデラCEOは2026年6月、企業の「自分たちのAI」を、基盤モデル＋ハーネス＋**自社専用の採点表（private eval）**と説明した。一般的なAIの賢さの比較ではなく、**自社の仕事で、何を価値とし、何を許されない失敗とするかを決めるもの**。

例：問い合わせ返信の下書きAI	目標の例
直さずにそのまま使えた割合	7割以上
事実と違うことを書いた件数	ゼロ（1件でもルールを見直す）
人の確認が必要な案件を、見逃さなかった割合	ほぼ100%
自社の言葉づかいに合っているか（人が5段階で評価）	平均4以上

モデルを乗り換えても、この採点表で良い結果が出続けるなら、**主導権は自社にある**。特定のAIに依存しないと成果が出ないなら、主導権は提供会社側にある。事故になる種類は、測って減点するより、④の関所で**止める**。

7. 事故から生まれたルール（講師の実例）

ハーネスは机上で考えるより、小さな事故を1つずつルールに変えていくと強くなる。

起きたこと	ルールにしたこと	部品
AIを使うための鍵（APIキー）が公開の場所に出て、約6万8千円の不正請求	鍵はコードにもチャットにも書かない。鍵は専用の金庫に集め、プログラムは金庫から読む（→ E6）	①③
鍵や秘密を確認しようとして、中身をそのまま表示させてしまい、会話の記録に残った	秘密の中身は表示しない。確認は「存在するか」だけ。試験用の使い捨てを使う。漏れたら、すぐ入れ替える	③④
AIが「不要」と判断した経理書類を消してしまった	AIの判断で消さない。疑わしいものは「退避フォルダ」へ移し、最後は人が消す	③④
クライアントのブログを、確認前に公開しかけた	公開ボタンはクライアント本人が押す。AIは下書きまで	④
AIが古い知識で製品名を「訂正」して間違えた	製品名・料金は、直す前に必ずWebで確認する	①⑤
同じ説明を何度もさせられた	一度決めたことは記憶に残し、蒸し返さない	⑤

8. 作り方の手順

1 仕事を1つ選ぶ 毎回同じ手順で、失敗しても取り返しがつくもの	2 指示書を書く 目的・置き場所・禁止事項を1枚に。長くしない	3 関所を決める 「外に出る操作」と「消す操作」は必ず人が押す	4 スキルにする 手順を言葉にし、合言葉で呼べるようにする
5 点検を回す 週1回、ルールと実態のずれを確かめ、事故はルールに変える			

小さく始める1週間

日	やること
1日目	仕事を1つ選ぶ。何が出来上がればよいか、1行で書く
2日目	指示書を1枚書く（上の例を参考に）。禁止事項は3つまで
3日目	関所を決める。送信・公開・削除・支払いのうち、この仕事に関わるものを書き出す
4～5日目	実際に頼んでみる。うまくいかなかった点を、指示書かスキルに1行ずつ足す
6日目	手順をスキルにする（F1のステップ4・5）
7日目	点検：事故やヒヤリとした点はなかったか。あればルールにする。なければ、翌週も同じ

9. AIに仕事を任せる前の10の確認

□ 確認すること

- 目的と、出来上がりの形が、1行で書けている
- 使う資料の置き場所と、最新かどうかの見分け方が決まっている（B2）
- 入れてよい情報・いけない情報が決まっている（D1）
- 渡す権限が、仕事に必要な最小限になっている
- 送信・公開・削除・支払いは、人が押す関所になっている
- 鍵・パスワードが、指示書にもチャットにも書かれていない
- 間違えたとき、元に戻せる（退避フォルダ・履歴）
- 何をしたかの記録が残る
- 最終的な責任者が、1人決まっている
- 点検の頻度と担当が決まっている

10. よくある失敗

指示書が長大になる

全部書こうとして、肝心のルールが埋もれる。短く、案内だけにする。

ルールが矛盾している

追記を重ねて、前の指示と食い違う。点検のときに読み直す。

権限が広すぎる

「念のため全部」を渡す。便利さと事故は同じ入口から来る。

お願いで済ませる

事故になる種類を、「やらないでね」と書いて終わりにする。仕組みで止める。

記憶が増えるだけ

古い教訓を捨てない。状況が変われば、捨てる・直す。

点検しない

作って満足し、半年後にルールと実態がずれている。週1回、短くてよい。

任せるほど、関所が大事になる

AIエージェントが自分で動くようになるほど、「権限のはみ出し」が起きやすくなる。便利さと事故は同じ入口から来る。**最初に決めるのは「何をさせるか」ではなく「どこで止めるか」。**

関連資料

- F1 業務の棚卸しと仕組み化 … 手順書の書き方（スキルの材料）
- E1 はじめてのAIエージェント：フォルダ構成と管理 … **セットで使う**。置き場所と進め方、最初の30分の手順

- E4 Gitの導入と設定 … 変更履歴という「保存の金庫」。ターミナルなしで進められる
- E5 SupabaseとCloudflare … 作ったものの置き場所。RLSと無料枠
- E6 APIキー（秘密）の扱い … .env に頼らず、Vault に置く
- E7 VPSサーバー … 自分のサーバーに、Webアプリを設置するとき
- E3 ローカルLLMと「情報を外に出さない」設計
- C3 事例：この資料ライブラリの自動化・スキル化 … ハーネスの実物
- D1 信号機ルール

出典（2026年10月確認）

- GPU数から「トークン経済性」へ Dellが示したAIインフラ競争の新基準（AI新聞・2026年5月20日）(<https://community.exawizards.com/aishinbun/news-05-20-2026/>)：NVIDIAのハーネスの定義
- チャットボットを「自律型AI」に変える鍵、『4つの記憶とガードレール』（ITmedia・2026年5月）(<https://blogs.itmedia.co.jp/osono/2026/05/ai4.html>)：記憶4種（CoALA）、ガードレール、ルールを置く場所
- Claude 5世代のコンテキストエンジニアリング（@IT・Anthropic原文の解説）(<https://atmarkit.itmedia.co.jp/ait/articles/2609/03/news040.html>)：指示書は軽く、判断を渡す、手順は段階的に
- 「最強モデル」はもう無意味 ナデラCEOが語る「学習ループ」（@IT・2026年6月）(<https://atmarkit.itmedia.co.jp/ait/spv/2606/25/news016.html>)
- 全ての企業が「自分たちのAI」を構築する時代＝Microsoftのサティア・ナデラ氏（AI新聞・2026年6月5日）(<https://aishinbun.com/>)：モデル＋ハーネス＋自社専用の採点表
- Claude Code 公式ドキュメント：メモリ（CLAUDE.md・自動メモリ）(<https://code.claude.com/docs/en/memory>)：200行、25KB、4MiB、@importの4段、置き場所と読み込み順（2026年10月3日確認）
- Claude Code 公式ドキュメント：スキル（SKILL.md）(<https://code.claude.com/docs/en/skills>)：500行、説明文1,536文字

ローカルLLMと「情報を外に出さない」設計

社内PCで動かすAIの向き・不向きと、クラウドのAIとの使い分け

更新日：2026-09-30（2026年10月時点の情報） | HUMAC 伊藤晴通

ローカルLLMとは

インターネットの向こうの会社のAIではなく、**自社のPC・サーバーの中で動かすAI**。入力した情報が社外に出ず、使うたびにお金がかかる仕組み（従量課金）でもない。その代わりに、性能・設備・手間の見きわめが必要になる。

クラウドのAIとの違い

観点	クラウドのAI（ChatGPT・Gemini・Claude）	ローカルLLM
賢さ	最先端	一段落ちる（要約・分類・下書きは十分）
情報の行き先	社外のサーバーに送られる（契約で保護）	社内から出ない
費用	月額または使った分だけ	最初に機械代、あとは電気代
Web検索	できる	そのままではできない（決まったページを取りに行くことはできる）
手間	契約するだけ	設置・更新・故障対応が要る
向いている仕事	調査、長文の読解、難しい判断、アプリづくり	毎日の定型処理、社外に出せない情報の要約・分類、夜間の自動処理

「使い分け」が正解：講師の2台体制

人が指示するPC

クラウドのAI（Claude Code など）で、設計・調査・資料づくり・アプリ開発。賢さが要る仕事はこちら。

24時間動くPC（GPU搭載）

ローカルLLM・資料室（RAG）・定時の自動処理。夜中や休日も、PCを閉じていても動く。秘密は専用の金庫から読み、コードに書かない。

ローカルLLMに任せている定型の仕事（例）

仕事	頻度	ローカルLLMがやること	人がやること
朝のまとめ（予定・タスク）	毎朝	集めて整えてメールで届ける	読む

仕事	頻度	ローカルLLMがやること	人がやること
経理書類の仕分け	毎日	スキャンした書類を読み、種類を判定して分類・名前付け	迷った書類の最終判断（AIは消さない）
AIの現在地チェック（この資料ライブラリ）	毎週土曜	公式ページの変化とニュースを要約し、【大】【小】の目安を付けて知らせる	原文で確かめ、資料を直すかを決める（→ C3）

ローカルLLMは「知らせる係」から始める

中型のローカルLLMは、判定を読み違えることがある。実際、資料ライブラリの週次チェックでも、差分を誤読した要約が出た。**最初は「見つけて知らせる」まで**を任せ、書き換え・公開・削除は人（またはクラウドの高性能AI＋人の確認）が行う。慣れてきたら範囲を広げる。

始めるときの目安

- **機械**：GPU（画像処理用の部品）を積んだPC。中型のモデル（140億～320億パラメータ級）で、日本語の要約・分類が実用になる
- **道具**：モデルを動かすソフト（Ollama など）＋資料室（RAGエンジン）＋窓口になる小さなサーバー
- **最初の一步**：社外に出せない定型の仕事を1つ選び、「要約してメールで知らせる」だけを自動化する
- **情報の扱い**：ローカルでも、鍵の管理と権限の絞り込み（→ E2）は同じように必要

Gitの導入と設定：変更履歴という「保存の金庫」

非開発者向け。ターミナルなしで進める：Gitの確認・設定、GitHub（非公開）、保存と戻し方、確認画面で見るべき言葉、守るルール

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

対象ツール：Claude Code

Git と GitHub は、**どのAIエージェントでも共通**です。「Claudeに頼む」「Codeタブ」などの操作は、**Claude Code**（Claudeのデスクトップアプリの「Code」タブ）の場合です。

対象の方：開発者ではない方（経営者・事務・現場の担当者）。プログラミングは不要です。**コードは書かず、AIエージェントに頼んで、自分の業務アプリをつくる**ところまでを、順に進めます（ターミナルの黒い画面は、使わない形で書いています）。

Gitとは、「セーブポイント」付きの保存機能

ゲームのセーブポイントのように、**仕事のフォルダの「ある時点の状態」を、何度でも保存**できる仕組み。あとから「昨日の状態に戻す」「いつ、何を变えたか見る」ができる。そして、保存したものを**インターネット上の「貸金庫」（GitHub）**にも預けておけば、パソコンが壊れても、別のパソコンでも、続きができる。

難しい操作は要らない。**ターミナル（黒い画面）は、開かなくてよい**。この資料は、Claudeに頼むか、画面のボタンだけで進められる形で書いてある。E1で作った仕事のフォルダを、ここで「保存できる状態」にする。

1. なぜ、AIエージェントにGitが要するのか

AIが壊しても、戻せる

AIは、ファイルを書き換えたり、消したりする。**保存した時点には、いつでも戻れる**。安心して任せられる。

「いつ・何を」が分かる

AIが何を变えたかを、履歴で確認できる。引き継ぎや、あとからの確認にも使える。

バックアップになる

貸金庫（GitHub）に預けておけば、パソコンの故障や紛失から守れる。別のPCにも、そのまま移せる。

並行して作業できる

Claudeのデスクトップアプリで、複数のセッションを、それぞれ独立した作業コピーで動かすには、Gitが必要（公式）。

AIの「巻き戻し」機能は、Gitの代わりにならない

Claude Code にも、AIの編集を取り消す機能（チェックポイント）がある。ただし戻せるのは、AIが直接編集したファイルだけ。コマンドで消したファイルや、外部への操作は戻せず、保存期間も限られる（約30日）。長く残す履歴は、Gitで持つ（公式の説明）。

2. 3つの段階：まずは①だけでもよい

段階	できること	用意するもの	目安	ターミナル
① PCの中に保存する	昨日の状態に戻せる。履歴が残る	Git	約15分	不要（Claudeに頼む）
② 貸金庫（GitHub）に預ける	バックアップ。別のPCで続きができる	GitHubのアカウント、GitHub Desktop	+約20分	不要（ボタンで操作）
③ 「保存して、金庫に送って」と頼めるようにする	終わりの合言葉に、保存と送信まで含められる	GitHub CLI（gh）でのログイン	+約10分	任意（Claudeに頼めば、操作は案内される）

おすすめは、①と②。③は、慣れてから。勉強会・サロンでは、①②を実際にやる。

3. 準備の手順

手順1：Gitが入っているか確認する（①）

ClaudeのデスクトップアプリのCodeタブで（まだなら、先に A4：契約と最初の設定）、仕事のフォルダを選び、次のように頼む。

コピーして使う

このパソコンで、Git が使える状態か確認してください。使えなければ、私のパソコン（MacかWindowsか）に合わせて、入れ方を1手順ずつ、やさしく教えてください。

パソコン	入れ方（Gitの公式の案内）
Mac	ほとんどのMacには、最初から入っている（Claudeの公式ドキュメントの説明）。入っていないときは、Macが「開発者ツールをインストールしますか」と案内を出すので、「インストール」を押して、終わるまで待つ（Gitの公式が、いちばん簡単な方法として案内している）
Windows	Gitの公式サイト（git-scm.com）から、「Git for Windows」のインストーラーをダウンロードして実行する。迷ったら、設定は初期のまま「Next」で進めてよい

手順2：最初の設定（名前とメールアドレス）

Gitは、保存のたびに「誰が保存したか」を記録する。最初に、名前とメールアドレスを1回だけ設定する。

コピーして使う

Git の最初の設定をしてください。名前は〔あなたの名前〕、メールアドレスは〔使っているメールアドレス〕です。設定したあと、設定が合っているか確認して、結果を見せてください。

参考：Claudeがやっていること

Gitの最初の設定は、`git config --global user.name "名前"` と `git config --global user.email メールアドレス` の2つ（Gitの公式の手順）。自分で打ちたい人は、この2行をターミナルに入れてもよい。名前とメールは、保存の履歴に載る。**だから、保存先は必ず非公開にする**（後述）。

手順3：仕事のフォルダを、Gitで保存できる状態にする（①）

先に、「入れてはいけないもの」を決める。鍵・パスワード・実データ・個人情報は、保存の対象から外す（D1）。この除外リストが「.gitignore」というファイル。

コピーして使う

この仕事のフォルダを、Git で保存できる状態にしてください。
先に .gitignore を作ってください。次のものは、保存の対象から外します：鍵・パスワード（.env など）、data フォルダ（実データ）、パソコンが勝手に作る不要なファイル（.DS_Store など）。
作ったら、保存の対象になっているファイルの一覧を見せてください。私が確認してから、最初の保存をします。

.gitignore に入れる例	理由
.env .env.* *.key *.pem	鍵・パスワード。入れると、金庫から漏れる
data/	実データ（個人情報・決算書など）
.DS_Store Thumbs.db	パソコンが自動で作る不要なファイル
動画・大きな画像のフォルダ	大きなファイルは、金庫に向かない

手順4：最初の保存（①）

コピーして使う

いまのフォルダの状態を、最初の保存として記録してください。保存の説明は「最初の保存：指示書と現在地ファイル」にしてください。保存したあと、保存の履歴を見せてください。

これで、「セーブポイント」が1つできた。**以後は、「保存して」と頼むだけ**。保存の説明（コミットメッセージ）は、日本語でよい。「何を変えたか」を一言で書く。

手順5：貸金庫（GitHub）を用意する（②）

1

アカウントを作る

github.com で、無料のアカウントを作る。二段階認証を有効にしておくで安心

2

GitHub Desktop を入れる

desktop.github.com から入れる（無料。ボタンで操作できるアプリ）。「Sign into GitHub.com」でログイン

3

フォルダを追加する

メニュー「File」→「Add local repository」で、仕事のフォルダを選ぶ（ドラッグでも追加できる）

4

金庫に預ける（公開）

画面の「Publish repository」から、GitHubに作る。**必ず「非公開（Private）」を選ぶ**

いちばん大事：必ず「非公開」にする

「公開」にすると、世界中の誰でも中身を見られる。**仕事のフォルダは、すべて非公開**。預ける前に、画面の「非公開（Private）」の選択を、毎回、目で確認する（ボタンの名前は、アプリの版で変わることがある）。

預けたあとは、GitHub Desktop の画面に、変更されたファイルの一覧が出る。**保存は「Commit」ボタン、金庫に送るのは「Push origin」ボタン**。まずは、この2つのボタンだけ覚えればよい。

手順6（任意）：Claudeに「保存して、金庫に送って」と頼めるようにする（③）

慣れたら、Claudeが金庫への送信までやれるようにできる。GitHubの公式コマンドラインツール「gh」を入れて、1回だけログインする。

コピーして使う

GitHub CLI (gh) が使える状態か確認してください。入っていないければ、私のパソコンに合う入れ方を1手順ずつ教えてください。入ったら、GitHub へのログインを、ブラウザで行う方法で案内してください。ログインが終わったら、ログイン状態を確認してください。

- ログインは、ブラウザが自動で開き、GitHubのアカウントで認証する形（GitHubの公式の説明）。認証の情報は、パソコンの安全な保管場所に残るので、以後は、毎回のログインは要らない。
- パスワードやトークンを、チャットに書かない。ログインは、必ずブラウザの画面で行う。

4. 毎日の使い方：終わりの合言葉に入れる

E1の「終わりの合言葉」に、保存を入れる。これで、毎回の作業の最後に、現在地・決めたこと・保存が、まとめて残る。

コピーして使う

今日の作業を締めます。STATUS.md を更新し、決めたことと理由を docs/決定ログ.md に追記してください。そのあと、変更を保存してください（保存の説明は、今日やったことを一言で）。保存した内容の一覧を見せてください。

（③まで設定した人は、最後に「金庫にも送ってください」を足す。②だけの人は、GitHub Desktop の「Push origin」を押す。）

5. 戻りたいとき：「見る」→「戻す」の順で

いきなり戻さない。先に、何が変わるかを見てから、戻す。

やりたいこと	Claudeへの頼み方
AIがさっき直した所を、取り消したい	「さっきの変更を、すべて取り消してください。取り消す前に、どのファイルがどう変わるか教えてください」
昨日の状態を、見たい	「保存の履歴を、新しい順に10件、日付と説明で見せてください」→「〇日の保存のときの、〔ファイル名〕の中身を見せてください」（見るだけで、何も変えない）
昨日の状態に、戻したい	「いまの状態を、先に保存してください」→「〇日の保存の状態に戻したい。戻す前に、変わるファイルの一覧を見せてください。私が確認するまで、実行しないでください」
消してしまったファイルを、復活したい	「保存の履歴から、〔ファイル名〕を探して、元の場所に復元してください」

GitHub Desktop の「History」タブでも、保存の履歴を一覧で見られる。

6. Claudeの確認画面で、見るべき言葉

Claudeがコマンドを実行する前に、実行する内容が確認画面に出る（最初の設定の「確認あり」のとき）。**コマンドの意味は、読めなくてよい。ただし、次の言葉があったら、承認せず、「これは何をしますものですか？本当に必要ですか？」と聞く。**

確認画面の言葉	意味	どうする
rm、delete、clean	ファイルを消す	消す対象を聞く。消さずに、退避フォルダへ（E1）
--force、-f	確認を飛ばして、強引に実行する	原則、承認しない。理由を聞く
reset --hard、checkout .、restore .	保存していない変更を、捨てて戻す	捨てられる内容を、先に確認する
push と --force の組み合わせ	金庫の履歴を、書き換える	承認しない
public（公開）	金庫を、世界に公開する	承認しない。必ず非公開

7. 守るルール（E2の「関所」）

1. 金庫は、必ず非公開。
2. 鍵・パスワード・個人情報・実データは、保存しない（.gitignore で除外。鍵の置き場所は E6）。間違えて入れてしまったら、履歴から消すだけでは足りない。**その鍵を、すぐ無効にして、新しいものに入れ替える**（講師の約6万8千円の事故の教訓。E2）。
3. 履歴を書き換える・消す操作は、AIに任せない（上の表）。迷ったら、人が判断する。
4. 保存の前に、中身を見る。「何が保存の対象になっているか」の一覧を、毎回、軽く眺める。
5. 大きなファイル（動画など）は、入れない。

8. 用語のやさしい説明

用語	やさしく言うと
Git	変更履歴を残す仕組み（セーブ機能）。自分のパソコンの中で動く
GitHub	Gitで保存したものを預ける、インターネット上の貸金庫
リポジトリ	Gitで管理しているフォルダ（保存の履歴つきの仕事フォルダ）
コミット（保存）	セーブポイントを1つ作ること。説明を添える
プッシュ（金庫に送る）	保存したものを、GitHubに預けること
プル（金庫から取る）	GitHubにある最新の状態を、自分のパソコンに取り込むこと
ブランチ	履歴の枝分かれ。最初は、1本（main）だけで十分
ワークツリー	同じ仕事フォルダの、独立した作業コピー。複数のセッションを並行して動かすとき
.gitignore	「保存の対象にしないもの」の除外リスト

9. ターミナルを使う場面のまとめ

場面	ターミナル	代わりの方法
Gitの確認・設定・保存・履歴の確認・戻す	不要	Claudeに頼む
金庫に預ける、変更を送る	不要	GitHub Desktop のボタン
Claudeに、金庫への送信まで頼む（③）	任意	Claudeに、ghの導入とログインを案内してもらう（ログインはブラウザ）

ターミナルの操作に慣れた人向けの確認方法として、`git --version`（Gitが入っているか）、`git status`（いまの状態）、`git log --oneline`（保存の履歴）がある。

講師の実例

- 設定ファイル・手順書（スキル）・記憶のファイルを、非公開の金庫に、毎日自動で保存している。
- 保存の対象は「入れるものだけを許可する」形の除外リストにして、鍵や会話の記録が入らないようにしている。
- 作業の最後は「締めます」の一言で、記録・保存・バックアップまで、まとめて行う。
- Git はもともと開発者の道具だが、「保存して」「金庫に送って」と頼むだけで、非開発者でも使える。

10. はじめての日のチェックリスト

☐	確認すること
☐	Gitが使える状態になった（Claudeに確認してもらった）
☐	名前とメールアドレスを設定した
☐	.gitignore を作り、鍵・実データが除外されている
☐	最初の保存ができた。履歴に1件出ている
☐	GitHubのアカウントを作った（二段階認証つき）
☐	金庫に預けた。 非公開（Private） になっている
☐	終わりの合言葉に、保存を入れた
☐	「見る→戻す」の順を、1回練習した（ファイルを1つ直して、取り消してもらう）

関連資料

- E1 はじめてのAIエージェント：フォルダ構成と管理 … 仕事のフォルダの作り方と、終わりの合言葉
- E2 ハーネスエンジニアリング入門 … 関所と事故から生まれたルール
- D1 信号機ルール … 入れてよい情報・いけない情報

出典（2026年10月確認）

- Git 公式：ダウンロード（Mac・Windows）（<https://git-scm.com/downloads>）
- Git 公式：最初の設定（First-Time Git Setup）（<https://git-scm.com/book/en/v2/Getting-Started-First-Time-Git-Setup>）
- GitHub Docs：リポジトリの作成（<https://docs.github.com/en/repositories/creating-and-managing-repositories/quickstart-for-repositories>）
- GitHub Docs：GitHub Desktop をはじめる（<https://docs.github.com/en/desktop/overview/getting-started-with-github-desktop>）
- GitHub Docs：自分のフォルダを GitHub Desktop に追加する（<https://docs.github.com/en/desktop/adding-and-cloning-repositories/adding-a-repository-from-your-local-computer-to-github-desktop>）
- GitHub CLI：gh auth login（ブラウザでのログイン）（https://cli.github.com/manual/gh_auth_login）
- Claude Code 公式：デスクトップアプリ（セッション、作業コピーにGitが必要）（<https://code.claude.com/docs/en/desktop>）
- Claude Code 公式：チェックポイント（Gitの代わりにならない）（<https://code.claude.com/docs/en/checkpointing>）

SupabaseとCloudflare：AIエージェントで作ったものの置き場所

いつ必要になるか、無料枠と落とし穴（一時停止）、RLS、AIとつながときの注意（MCP）、公開前の確認とDNSの扱い

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

対象ツール：Claude Code

考え方は、どのAIエージェントにも共通です。ただし、**ファイル名・画面・設定・コマンドは、Claude Code**（Claudeのデスクトップアプリの「Code」タブ）の場合です。ほかのAIエージェントでは、読み替えが必要です。

対象の方：開発者ではない方（経営者・事務・現場の担当者）。プログラミングは不要です。**コードは書かず、AIエージェントに頼んで、自分の業務アプリをつくる**ところまでを、順に進めます（ターミナルの黒い画面は、使わない形で書いています）。

AIエージェントで「動くもの」を作ると、置き場所が要る

AIエージェントに、台帳アプリや予約の仕組みを作ってもらくと、必ず「データをどこに置くか」「どうやって公開するか」が問題になる。その定番の置き場所が、**Supabase（スーパベース）**と**Cloudflare（クラウドフレア）**。

たとえるなら、**Supabase＝「倉庫と受付」**（データをしまい、ログインを受け付ける）、**Cloudflare＝「店舗の入口と看板」**（世界に公開し、配信する）。どちらも、無料から始められる。

1. いつ、必要になるのか

作りたいもの	必要なもの
自分のパソコンの中だけで使う集計・資料づくり	どちらも不要（E1のフォルダと、E4の保存で足りる）
ホームページ・案内ページ（見せるだけ）	Cloudflare（公開と配信）
台帳・予約・顧客管理（データを貯めて、複数人で使う）	Supabase（データ）＋Cloudflare（公開）
ログインして使う社内アプリ	Supabase（ログインとデータ）＋Cloudflare（公開）
AIの鍵（APIキー）を、安全にしまいたい	SupabaseのVault（→E6）

2. それぞれ、何ができるのか

Supabase：データの置き場所

機能	ひとことで
データベース	表の形でデータをしまう（PostgreSQL）。台帳・顧客・売上など
ログイン（Auth）	メールアドレスなどでのログインを受け付ける
ファイル保存（Storage）	写真やPDFをしまう
Edge Functions	小さなサーバー処理（決まったときに動くプログラム）
Vault	鍵・パスワードを、暗号化してしまう（→ E6）

Cloudflare：公開と配信の置き場所

機能	ひとことで
Workers	小さなプログラムや、ページを、世界中から高速に配信する。Cloudflare が、新しいプロジェクトに最初に勧める基盤（公式）
Pages	ホームページなどの「出来上がったファイル」を公開する。引き続き使えるが、新規はWorkersから始めるのが公式の推奨
保存先（KV・D1・R2）	KV=キーと値の保存、D1=軽いSQLデータベース、R2=ファイル保存
Secrets	鍵を、使う場所に直接しまう。保存後は、値を画面で見られない（→ E6）
ドメイン・DNS	ホームページのアドレスと、メールの宛先を、決める設定
Access	自作のWebアプリに、ログインの関所を付ける仕組み（条件は公式で確認）

3. 無料枠と、落とし穴（2026年10月時点・公式）

	無料枠	落とし穴
Supabase	プロジェクト2つまで／データベース500MB ／ファイル1GB／月間利用者5万人／Edge Functions 月50万回	1週間アクセスがないと、自動で一時停止する。 止まると、そのプロジェクトのデータにも、鍵にも届かない。 有料（Pro）は月25ドルから
Cloudflare Workers	1日10万リクエスト／1回の処理のCPU時間 10ミリ秒／1回のサブリクエスト50まで	人気が出ると、1日10万を超えて止まる。重い処理は、 無料枠に収まらない
Cloudflare Pages	ビルド月500回／プロジェクト100／ファイ ル2万個まで（1つ25MiBまで）	新規はWorkersが推奨（公式）

Supabaseの「一時停止」に注意

無料のプロジェクトは、1週間まったく使われないと止まる。試作のうちは問題ないが、**本番で毎日使うものは、止まると業務が止まる**。長く使うものは、有料プランにするか、止まっても困らない作りにする。鍵の置き場所に使う場合は、特に注意（→ E6）。

4. 最初の一步：AIエージェントに頼む

アカウントを作り（どちらも無料）、最初は「試作用」のプロジェクトで練習する。本番のデータは、入れない。

コピーして使う

〔作りたいもの：例「お客様の予約台帳」〕を、Supabase にデータを置いて、Cloudflare で公開する形で作りたいです。

いきなり作らず、先に私に質問してください（誰が使うか、何人か、個人情報を扱うか、ログインは要るか）。そのうえで、①必要な表、②ログインの有無、③置き場所の構成を、図と短い説明で提案してください。私が確認してから、作り始めてください。

条件：Supabase の表には、必ず「行ごとのアクセス制限（RLS）」を付けてください。鍵は、チャットにもファイルにも書かないでください。

- AIには、Supabaseと「つなぐ道具」（MCP）を渡せる。ただし、後述のとおり、最初は試作用に限る。
- 作ったものは、E1のフォルダに置き、E4の方法で保存する。
- 無料枠に収まらない・特別なソフトや24時間の処理が要る場合は、**自分専用のサーバー（VPS）**を借りる選択肢がある（→ E7）。

5. 安全に使う：AIが作ったアプリで、いちばん多い事故

Supabase：「RLS」を必ず付ける

Supabaseは、データベースを、インターネット経由のAPIとして公開する仕組み。そのため、公式が次のように警告している：「行ごとのアクセス制限（RLS）が無い表は、権限を持つ誰でも、読み書きできる」。AIが作った表に、RLSが付いていないと、お客様のデータが、誰にでも見える・書き換えられる状態になる。

鍵の種類	使う場所	ルール
公開用の鍵（publishable／anon）	ブラウザ・スマホのアプリ	見えても大丈夫な、最小限の権限。RLSで守られていることが前提
秘密の鍵（secret／service_role）	サーバー側だけ	RLSを無視して、すべてを操作できる。ブラウザやスマホに、絶対に出さない（公式）

コピーして使う

この Supabase のプロジェクトを点検してください。①RLS が無効なテーブルを一覧にしてください ②各テーブルに、誰が何をできるかのポリシーがあるか ③秘密の鍵（service_role）が、ブラウザ側のコードや公開ファイルに入っていないか。結果を表で報告し、直す前に、私の確認を取ってください。値（鍵そのもの）は、表示しないでください。

AIとSupabaseをつなぐとき（MCP）

Supabase の公式は、AIをデータベースにつなぐ危険性を、はっきり書いている。お客様が入力した文章の中に、悪意のある命令が紛れていると、AIがそれに従って、データを読み出したり、消したりしかねない（プロンプトインジェクション）。公式の推奨は次のとおり。

- 本番のデータには、必要なときだけつなぐ。プロジェクトを指定し、読み取り専用にする。
- 道具を呼ぶたびの承認を、残しておく（自動承認にしない）。
- 使う機能を、必要なものだけに絞る。
- 試すときは、本番ではなく、開発用の枝（ブランチ）で。
- AIの出力は、実行する前に、人が確認する。

AIの画面に、鍵や個人情報が出ると、会話の記録に残る

AIに「データを見せて」と頼んで、表の中身（個人情報や鍵）が表示されると、それは会話の記録に残り、モデルの提供会社にも送られる。本番のデータや鍵は、AIに表示させない（赤の情報。D1）。講師は、鍵を表示させた事故の教訓から、「鍵は見ない・表示させない」をルールにしている（→ E2、E6）。

Cloudflare：公開前の確認と、DNSの扱い

- 公開する前に、中身を確認する：ホームページなどを公開する操作は、人が押す（関所。E2）。まず、確認用のURL（プレビュー）に出して、人が見てから、本番にする。
- 鍵は、Secrets に入れる：Workers の Secrets は、保存すると、画面でも、コマンドでも、値を読み出せない（置き換えるだけ）。環境変数に、鍵を平文で置かない（公式）。
- ドメイン・DNS・メールの設定は、慎重に：ドメインの設定を間違えると、ホームページだけでなく、メールが止まることもある。変更の前に、いまの設定を記録し、AIに任せきりにせず、人が確認する。特に、メールの宛先（MXレコード）には触らない。
- ログインを付けたいときは、Cloudflare Accessのような「関所」の仕組みがある。

6. どちらを使うか、迷ったら

1

Q1 データを貯める？

はい→Supabase。いいえ→Q2へ

2

Q2 公開する？

はい→Cloudflare（新規はWorkers から）

3

Q3 ログインが要る？

はい→Supabase の Auth、または Cloudflare Access

4

Q4 個人情報を扱う？

はい→RLS必須。本番は有料プランも検討。まずD1

7. はじめての日のチェックリスト

☐	確認すること
☐	作りたいものに、データベース・公開が本当に必要か、先にAIに質問してもらった
☐	試作用のプロジェクトで始め、本番データは入れていない
☐	すべての表に、RLS が付いている（AIに点検してもらった）
☐	秘密の鍵が、ブラウザ側・公開ファイル・チャットに出ていない

□	確認すること
□	AIをSupabaseにつなぐときは、試作用・読み取り専用・承認あり
□	公開は、プレビューで確認してから、人が押した
□	無料枠の上限と、「一時停止」の条件を、理解した
□	鍵の置き場所を決めた（→ E6）

関連資料

- E6 APIキー（秘密）の扱い… .env に頼らず、Vault に置く
- E1 はじめてのAIエージェント：フォルダ構成と管理
- E4 Gitの導入と設定
- D1 信号機ルール／E2 ハーネスエンジニアリング入門

出典（2026年10月確認）

- Supabase 料金（無料枠・一時停止・Pro） (<https://supabase.com/pricing>)
- Supabase Docs：Row Level Security (<https://supabase.com/docs/guides/database/postgres/row-level-security>)
- Supabase Docs：MCP（セキュリティ上の注意） (<https://supabase.com/docs/guides/getting-started/mcp>)
- Cloudflare Workers：制限（無料プラン） (<https://developers.cloudflare.com/workers/platform/limits/>)
- Cloudflare Pages：制限 (<https://developers.cloudflare.com/pages/platform/limits/>)
- Cloudflare Pages（新規はWorkersを推奨） (<https://developers.cloudflare.com/pages/>)
- Cloudflare Workers：保存先の選択肢 (<https://developers.cloudflare.com/workers/platform/storage-options/>)
- Cloudflare Workers：Secrets (<https://developers.cloudflare.com/workers/configuration/secrets/>)
- Cloudflare Access：自作アプリの認証 (<https://developers.cloudflare.com/cloudflare-one/applications/configure-apps/self-hosted-public-app/>)

APIキー（秘密）の扱い：.envに頼らず、Vaultに置く

.envが推奨されなくなってきた理由（根拠つき）、鍵をAIに読ませない設定、講師のVault方式、始め方、漏れたときの手順

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

対象ツール：Claude Code

考え方は、どのAIエージェントにも共通です。ただし、ファイル名・画面・設定・コマンドは、Claude Code（Claudeのデスクトップアプリの「Code」タブ）の場合です。ほかのAIエージェントでは、読み替えが必要です。

対象の方：開発者ではない方（経営者・事務・現場の担当者）。プログラミングは不要です。コードは書かず、AIエージェントに頼んで、自分の業務アプリをつくるところまでを、順に進めます（ターミナルの黒い画面は、使わない形で書いています）。

結論：鍵は、AIが読めるファイルに置かない。置き場所は「金庫」

AIを使うアプリを作ると、「APIキー」（AIや外部サービスを使うための鍵）が必要になる。鍵は、仕事のフォルダのファイルに、平文で書かない。専用の「金庫」に入れ、値は、AIの目に触れさせない。講師は、SupabaseのVaultに一元化している。この資料は、その考え方と、始め方。

1. 鍵が漏れると、何が起きるか（講師の実例）

講師は、AIを使うための鍵が公開の場所に出てしまい、約6万8千円の不正請求を受けた。鍵は、「財布の暗証番号つきカード」のようなもの。持っている人は誰でも、あなたの名前で、お金のかかる操作ができる。そのため、鍵の扱いは、AI活用の中で最も慎重にする項目になる（→ E2）。

2. 「.envに鍵を書く」は、なぜ推奨されなくなってきたか

.env（ドット・エンブ）は、鍵などの設定を、1つのファイルにまとめて書く、長年の定番の方法。これまでは、「.gitignoreで保存の対象から外せば安全」と言われてきた。しかし、AIエージェントの登場で、前提が変わった。

わかっていること	出典
AIエージェントは、作業フォルダの中のファイルを読む。 .envも、読む対象になりうる 。読んだ内容は、会話の文脈に入り、 モデルの提供会社のサーバーに送られる	セキュリティ各社の指摘（Knostic、Infisical など）
2026年1月、「Claude Codeが、.claudeignoreや.gitignoreで除外したはずの.envを読んでしまう」という報道があった。Anthropicはコメントしなかった	The Register（2026年1月28日）
Claude Codeの公式ドキュメントは、読ませたくないファイルは、 設定の「Readの拒否ルール」 で指定すると書いている。そして、 .claudeignoreは効果がないと明記している	Claude Code 公式（権限）

わかっていること	出典
拒否ルールが止められるのは、AIの標準の道具と、認識できるコマンドだけ。 AIが書いたスクリプトが、間接的にファイルを読む場合は止められない 。確実に止めるには、OSレベルの制限（サンドボックス）が要る	Claude Code 公式（権限）

「.env が禁止になった」のではない

正確には、「AIが動く作業フォルダに、平文の鍵を置く運用」が、推奨されなくなってきた。.env が必要な場面は、まだある（自分のパソコンで試すときなど）。だから、「鍵を、AIの手の届かない所に置く」のが、新しい基本になる。

3. 守りの3段階（鍵をどこに置くか）

段階	やること	向く場面
① 最低限	.gitignore で保存の対象から外す + AIに 読ませない設定 （Read の拒否ルール）。使い終わったら、.env を消す	自分のパソコンで、ちょっと試すとき
② 鍵を、作業フォルダの外へ	使う場所に、直接しまう（Cloudflare の Secrets、Supabase の Edge Functions の Secrets）。保存後は、画面で値を読み出せない	小さなアプリが1つ、1か所で動くとき
③ 金庫に一元化（Vault）	すべての鍵を、1つの金庫に集める。アプリやサーバーは、起動時に、金庫から取り出す	複数のアプリ・パソコン・顧客で、鍵を使い回すとき。棚卸しと入れ替えを一元化したいとき

段階①：AIに、鍵のファイルを読ませない設定

仕事のフォルダの設定ファイル（.claude/settings.json）に、読ませないファイルを書く。ターミナルは使わず、Claudeに頼む。

コピーして使う

このフォルダの Claude Code の設定（.claude/settings.json）に、次のファイルを「読ませない」設定を追加してください：.env、.env.*、secrets フォルダの中。

追加したら、実際に .env を読ませようとして、拒否されることを確認して、結果を見せてください（中身は表示しないでください）。

設定の書き方（公式）：`"permissions": { "deny": ["Read(.env)", "Read(.env.*)", "Read(secrets/**)"] }`。「拒否ルール」が効いているかは、必ず試して確認する。AIが書いたスクリプトが間接的に読む場合は止められないので、確実に守るなら、サンドボックス（公式）も併用する。

4. 講師の方式：Supabase の Vault に一元化する

Vaultは、Supabase に付いている「暗号化して鍵をしまう」機能。秘密は、暗号化されて保存される。復号するための鍵は、データベースの外の、保護された場所で管理される（公式）。講師は、**自社用も、顧客の業務用も、すべての鍵を、1つの金庫に集めている**。

1

1 人が、値を入れる

管理画面の、パスワード欄から。チャットや、ファイルには書かない

2

2 Vault に、暗号化して保存

名前と、用途の説明を付けて

3

3 取り出し口は、1か所

取り出すための関数を1つだけ作り、サーバーだけが呼べるようにする

4

4 アプリは、起動時に取り出す

メモリの中だけで使う。ファイルに書かない

設計のルール

- **値は、AIの目に触れさせない。** 値の入力は、人が、管理画面です。AIは「入れ物」と「取り出し口」を作るだけで、値は見ない。
- **ブラウザ・スマホのアプリから、直接取り出さない。** 取り出せるのは、サーバー側（秘密の鍵を持つ処理）だけ。
- **取り出し口は、許可リスト方式：**「どのプログラムが、どの鍵を取れるか」を、決めておく。
- **名前の付け方を決める：**自分用は サービス名_用途（例：GEMINI_API_KEY）、顧客の業務用は CLIENT_顧客の略称_サービス名_用途。
- **説明（description）は必須：**用途・発行日・権限の範囲・誰宛か。
- **棚卸し：**半年ごとに、6か月以上更新していない鍵を確認する。使っていない鍵は、無効にする。
- **鍵ごとに、権限を最小にして発行する：**使い道だけに絞った鍵にする。

最後に残る、1本の鍵

金庫から取り出すためには、「金庫の鍵」が要る。この1本だけは、どうしても、そのパソコン（サーバー）の環境に置く（鶏と卵の問題）。講師は、これを、パソコンの暗号化（ディスク全体の暗号化）で守り、他の鍵は、すべて金庫に入れている。環境に残る秘密が、1本だけなら、守りも棚卸しも、簡単になる。

金庫の中身を、AIに「見せて」と頼まない

金庫の鍵を、データベースの問い合わせ（SELECT）で表示させると、画面に出た値が、会話の記録に残る。講師は、これで実際に事故を起こし、鍵を入れ替えた。確認してよいのは、「鍵が存在するか」「いつ更新したか」だけ。値は見ない。試験には、使い捨てのダミーの鍵を使う。

5. 始め方（Claudeに頼む）

1

1 鍵の置き場所を作る

Supabase に、鍵専用のプロジェクトを1つ作る（試すだけなら無料でよい。業務で使うなら、下の注意を読む）

2

2 取り出し口を作る

Claudeに頼む。許可リスト方式で

3

3 ダミーで試す

使い捨ての値で、取り出せるか、権限が効くか確認

4

4 本物は、人が入れる

管理画面で。チャットに書かない

コピーして使う

Supabase の Vault を使って、APIキーを安全に管理する仕組みを作りたいです。次の条件で、設計を提案してください。作る前に、私の確認を取ってください。

- ・鍵の値は、私が管理画面で入れます。あなたは、値を見ません。チャットにも、ファイルにも、書かないでください。
- ・鍵を取り出す関数を1つだけ作り、サーバー側（service_role）だけが呼べるようにしてください。ブラウザ側の鍵（anon）からは、呼べないようにしてください。
- ・「どの呼び出し元が、どの鍵を取れるか」の許可リストを持たせてください。
- ・動作の確認は、使い捨てのダミーの鍵で行ってください。確認のとき、鍵の値は表示しないでください。
- ・名前の付け方は「サービス名_用途」。説明（description）を必須にしてください。

無料プランの「一時停止」に注意

Supabase の無料プロジェクトは、**1週間アクセスがないと、自動で一時停止する（公式）**。金庫が止まると、**アプリが起動時に鍵を取り出せず、動かなくなる**。毎日使うアプリが取りに来ていれば、止まらないが、**業務で使うなら、有料プラン（月25ドルから）を検討する**。無料のプロジェクトは2つまで（公式）なので、1つを鍵専用にすると、余裕が少なくなる点も、あらかじめ知っておく。

6. 日常の運用

場面	やること
新しい鍵を使い始める	管理画面で、名前と説明を付けて入れる。使うアプリの許可リストに足す
半年ごと	棚卸し。更新していない鍵、使っていない鍵を確認して、無効にする
鍵を入れ替える	発行元で新しい鍵を作り、金庫の値を置き換え、古い鍵を無効にする。アプリは、再起動して取り直す
鍵が漏れたかもしれない	① すぐ、発行元でその鍵を無効にする ②新しい鍵に入れ替える ③使われた形跡（請求・利用履歴）を確認する。 保存の履歴から消すだけでは足りない （一度公開されたものは、取り戻せない）

7. 鍵の置き場所：どれを選ぶか

方法	向く場面	注意
.env（ファイル）	自分のパソコンで試すだけ	.gitignore + AIに読ませない設定。使い終わったら消す。仕事のフォルダには、置きっぱなしにしない
Cloudflare Workers の Secrets	Cloudflare で動かす小さなアプリ1つ	保存後は、値を読み出せない（置き換えるだけ）。平文の環境変数には、鍵を置かない（公式）
Supabase Edge Functions の Secrets	Supabase の関数1つ	設定のとき、一時的に .env を使うことがある。使い終わったら消す。鍵の名前は SUPABASE_ で始められない（公式）

方法	向く場面	注意
Supabase Vault（講師方式）	複数のアプリ・パソコン・顧客で、 鍵を使い回す。棚卸し・入れ替えを 一元化したい	取り出し口の設計が必要。無料の一時停止に注 意

8. よくある失敗

鍵を、チャットに貼る 会話の記録に残り、提供会社にも送られる。値は、管理画面にだけ入れる。	.env を置きっぱなし AIがいつでも読める状態になる。使い終わったら消すか、金庫に移す。	鍵を表示させて確認する 確認するのは「存在するか」だけ。値は見ない。
ブラウザ側に、秘密の鍵を入れる 画面のソースから、誰でも見られる。サーバー側だけで使う。	権限が広い鍵を使う 漏れたときの被害が大きい。使い道だけに絞った鍵にする。	入れ替えない・棚卸ししない 古い鍵が残り続ける。半年ごとに確認する。

9. 鍵を扱う前のチェックリスト

☐ 確認すること
☐ 鍵が、仕事のフォルダの、ファイル・指示書・チャットに書かれていない
☐ .env を使う場合は、.gitignore と、AIに読ませない設定がある（試して確認した）
☐ 鍵の置き場所を決めた（試すだけ／Secrets／Vault）
☐ 値は、人が、管理画面で入れる。AIは、値を見ない
☐ 鍵の権限を、最小にしてある。名前と説明が付いている
☐ ブラウザ・スマホ側には、秘密の鍵が無い
☐ 漏れたときの手順（無効化→入れ替え→確認）を知っている
☐ 半年ごとの棚卸しを、予定に入れた

関連資料

- E5 SupabaseとCloudflare … 動かす場所と、RLS・無料枠
- E2 ハーネスエンジニアリング入門 … 権限・関所と、事故から生まれたルール
- E4 Gitの導入と設定 … 鍵を保存の対象から外す（.gitignore）
- D1 信号機ルール

出典（2026年10月確認）

- Claude Code 公式：権限（Read の拒否ルール、.claudeignore は効果なし、サンドボックス） (<https://code.claude.com/docs/en/permissions>)
- Claude Code's prying AIs read off-limits secret files（The Register • 2026年1月28日） (https://www.theregister.com/2026/01/28/claude_code_ai_secrets_files/)（報道）
- Your AI Coding Agent is Reading Your .env File（Infisical） (<https://infisical.com/blog/your-ai-coding-agent-is-reading-your-env-file>)（セキュリティ会社の解説）
- From .env to Leakage（Knostic） (<https://www.knostic.ai/blog/claude-cursor-env-file-secret-leakage>)（セキュリティ会社の解説）
- Supabase Docs：Vault (<https://supabase.com/docs/guides/database/vault>)
- Supabase Docs：Edge Functions の Secrets (<https://supabase.com/docs/guides/functions/secrets>)
- Cloudflare Workers：Secrets (<https://developers.cloudflare.com/workers/configuration/secrets/>)
- Supabase 料金（無料枠・一時停止） (<https://supabase.com/pricing>)

VPSサーバー（Xserver VPS）：Webアプリを自分のサーバーで動かすとき

VPSが必要なとき、Xserver VPSの現状（新規受付の一時停止）と、いま申し込めるVPSクラウドの料金・オプション・構成例（公式カタログ）、見落としやすい注意、防犯の初期設定、設置の流れ、取次店のお申し込みフォーム（広告表示つき）

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

対象ツール：Claude Code

考え方は、どのAIエージェントにも共通です。ただし、**ファイル名・画面・設定・コマンドは、Claude Code**（Claudeのデスクトップアプリの「Code」タブ）の場合です。ほかのAIエージェントでは、読み替えが必要です。

対象の方：開発者ではない方（経営者・事務・現場の担当者）。プログラミングは不要です。**コードは書かず、AIエージェントに頼んで、自分の業務アプリをつくる**ところまでを、順に進めます（ターミナルの黒い画面は、使わない形で書いています）。

広告（取次店）と、受付状況についてのお知らせ（2026年10月3日時点）

- **広告**：講師（株式会社ヒューマック 伊藤）は、エックスサーバーの**取次店**です。この資料の8章には、講師の「申し込みフォーム」のリンクが載っています。このリンクからお申し込みいただくと、講師に、取次の報酬（紹介料・手数料など）が支払われる場合があります。資料の内容は、公式の情報にもとづいて書いています。このリンクを使わずに、エックスサーバーに直接申し込むこともできます。
- **受付状況**：エックスサーバーの公式のお知らせによると、「**XServer VPS**」は、**全プランで、2026年9月17日から新規の受付を一時停止**しています。**再開は、2026年11月中の予定**です（既存の契約者は、追加の申し込みができます）。代わりに、新しいサービス「**XServer VPS クラウド**」（2026年8月31日開始）が案内されています。**VPS クラウドは、講師の取次店のお申し込みフォームの対象外で、エックスサーバーに直接お申し込みいただく形になります**（講師への報酬は、この資料のリンクからは生じません）。受付の状況は、変わることがあるので、申し込みの前に、公式のお知らせで必ず確認してください。

VPSは、「自分専用の小さなサーバー」を借りること

AIエージェントに作ってもらったWebアプリは、まず、E5の Supabase と Cloudflare で動かせるか、考える。それで足りない場合に、**VPS（仮想専用サーバー）**を借りて、自分でアプリを設置する。借りるのは「サーバーという建物の、1フロア」。鍵（管理者の権限）は、**すべて自分が持つ**代わりに、**OSの更新・防犯・バックアップも、自分の責任**になる。

1. VPSが必要になるのは、どんなとき？

やりたいこと	Cloudflare・Supabase（E5）で足りる？	VPSが向く？
ホームページ・案内ページを公開する	足りる	不要
台帳・予約などの、データを貯めるアプリ	足りることが多い（Supabase）	特別な事情があるとき
24時間動き続ける処理（定期実行・通知・連携）を、自由に作りたい	無料枠の制限（処理時間・回数）に当たることがある	向く
特定のソフト・言語・OS・ポートが必要	対応できないことがある	向く
既存のWebアプリ（PHPなど）を、そのまま移したい	作り直しが要ることがある	向く
外部のサービスと、決まった接続先（固定のIP）でつなぎたい	難しいことがある	向く

VPS と、「レンタルサーバー」の違い

レンタルサーバー（共用）は、事業者がOSや防犯を管理してくれる、決まった型の貸し部屋。VPSは、**OSの管理者（root）権限を持つ、自分専用の環境**で、自由度が高い。そのかわり、**設定・更新・防犯を、自分でやる**。自信がなければ、まずE5のサービスか、レンタルサーバーを検討する。

2. Xserver VPS の、サービスの種類（公式の情報・2026年10月時点）

	XServer VPS（従来）	XServer VPS クラウド（新サービス）
受付	新規受付は一時停止中（2026年9月17日～、再開は11月中の予定）	受付中（2026年8月31日開始）
向き	1台構成（Web・開発・ゲームなど）	1台から、複数台構成まで。サーバー同士をつなぐ私設ネットワーク、データベースサーバー、ロードバランサーなどを足せる
料金（4GBの例）	公式の料金一覧で確認（受付の再開後）	4GB（50GB）：月額2,480円（1か月契約）／2,068円（12か月契約）、税込 。通信量や時間の従量課金は無し（3章の表）
バックアップ	自動バックアップは、標準では付かない（オプションなど。公式で確認）	日次の自動バックアップが標準 （最大7日分）
ビジネスプラン（法人向け）	稼働率保証（SLA）・自動バックアップが付く、法人向けのプラン（受付停止の対象に含まれる）	—
API（自動操作）	—	未提供（今後の予定）

料金・キャンペーン・受付状況は、頻繁に変わる。申し込み画面と、公式のお知らせで必ず確認する。ビジネスプランの内容は、販売パートナーの解説にもとづく（公式ページで確認）。

3. XServer VPS クラウドの料金・オプション・構成例（公式カタログ・2026年8月31日更新版・税込）

いま申し込める「XServer VPS クラウド」の内容。料金は、VPSは12か月契約時の月額換算で、ほかのオプションは1か月契約の月額。当月分は日割りになる（カタログの注記）。

VPS（ストレージの違う2タイプから選ぶ）

メモリ	vCPU	NVMe SSD と 月額（12か月契約時）
4GB	4コア	50GB：2,068円～／200GB：3,100円～
8GB	8コア	100GB：3,784円～／400GB：5,676円～
16GB	12コア	100GB：8,167円～／800GB：12,250円～
32GB	18コア	100GB：20,475円～／1,600GB：30,713円～
64GB	32コア	100GB：40,950円～／2,400GB：61,425円～
128GB	48コア	100GB：81,900円～／3,200GB：122,850円～

小さなWebアプリなら、まず4GBで十分なことが多い。1か月契約の4GB（50GB）は、月額2,480円（公式サイト）。

有料オプション

オプション	ひとことで	月額の例
DBサーバー	PostgreSQL または MariaDB の、データベース専用のサーバー。 OSなどは、エックスサーバーが管理（rootは付かない）	10GB：1,441円／30GB：2,480円／60GB：4,961円～
DBの自動バックアップ	日次・最大7日分	10GB：220円／30GB：660円～
L4ロードバランサー	アクセスを、複数のサーバーに振り分ける	スタンダード 3,300円／ハイスペック 6,600円
NFS	サーバー間で共有する、保存場所	30GB：1,790円／100GB：5,951円～
追加IPアドレス	IPv4アドレスを足す	400円／1個
ネットワーク帯域拡張	通信の太さを広げる	300Mbps 5,500円／500Mbps 8,800円
イメージ保存容量の追加	VPSのイメージ（まるごとの保存）を置く容量。50GBは標準で付く	1,650円／500GBあたり

「おまとめ自動セットアップ」：構成を選ぶだけ（月額が目安）

構成	中身	向く用途	月額が目安
小規模・検証用	VPS 4GB 1台+DB 10GB	WordPress、データの管理、小さなアプリ	3,509円
機能ごとの分離	VPS 4GB 2台	アプリ用・バッチ用・管理用など	4,136円
標準的なサイト	VPS 2台+DB+ロードバランサー	Webサーバー・APIサーバー	8,877円
ファイルのバックアップ	VPS+NFS 100GB	データのバックアップ、ログ集計	8,019円
本番とテスト環境	VPS 3台+DB+ロードバランサー	修正を、テスト環境で試してから、本番へ	10,945円
安全なファイル共有	VPS 2台（VPN用）+NFS 100GB	社内ファイルサーバー	10,087円
セキュリティ重視	VPS 3台+DB+ロードバランサー+NFS（運営者専用のVPN経路）	基幹業務システム、ECサイト	16,896円
負荷耐性重視	VPS 2台+DB+ロードバランサー+NFS	画像・メディアの配信	14,828円

構成例は、最小の注文内容。はじめての方は、「小規模・検証用」か、VPS1台から始めて、必要に応じて足す。

標準で付く機能

- **管理者（root）の権限**：VPSには、全プランで付く（DBサーバー・NFS・ロードバランサーには付かない）。
- **通信量は無制限**：従量課金や維持調整費は無い。ただし、回線は共有で、1契約あたり最大100Mbps（オプションで拡張）。
- **自動バックアップ**：VPSのデータを、1日1回、最大7日分。復元は、管理画面（コントロールパネル）の操作で行える。
- **イメージ保存**：その時点のVPSを、まるごと保存できる（50GBまで無料）。
- **防犯の機能**：パケットフィルター（ポートの開閉、接続元の制限）、SSH鍵（秘密鍵と公開鍵。申し込み時に自動生成できる）、管理画面の二段階認証。
- **操作**：ブラウザからのコンソール（リモート接続できないときも、管理画面から直接操作できる）。独自ドメインのDNS設定。無料のサブドメイン（example.xvps.jp のようなURL）で、すぐにテスト公開できる。
- **OS・アプリのひな形**：OSイメージと、セットアップスクリプト（Docker、WordPress、KUSANAGIなど）から選べる。
- **支払い**：クレジットカード、あと払い（ペイディ）、プリペイド決済。
- **サポート**：メールは24時間365日。電話は平日10時～18時。

はじめての人が、見落とししやすい点（カタログの注記）

- DBサーバーの設定・保存データ・バックアップは、お客様の管理。自動バックアップは、有料のオプション（上の表）。付けない場合、自分で取る。
- NFS（共有の保存場所）には、お客様が任意に復元できるバックアップ機能がない。大事なデータの、唯一の置き場にしない。
- プランの変更は、「ストレージが、いまと同じか、大きいプラン」にだけできる（小さくはできない）。最初に大きすぎるタイプを選ぶと、戻せない。
- 料金は、12か月契約時の月額換算で表示されている。月ごとの契約より、年間の契約のほうが、月額は安い。期間の縛りがある。
- 「大手のクラウド（IaaS）のように、部品を自由に組み合わせる」ものではなく、導入の速さと、費用の分かりやすさを重視したサービス（エックスサーバーの説明）。

4. 契約する前の確認

□ 確認すること

- E5（Cloudflare・Supabase）では、本当に足りないか、AIに確認してもらった
- OSの更新・防犯・バックアップを、自分（または担当者）が続けられるか
- 個人情報・お客様のデータを置くか（置くなら、法人向け・バックアップ・SLAを検討）
- 独自ドメインを、どこで管理しているか（DNSの変更の権限）
- メモリの量（まず4GB程度）と、ストレージの量（あとで小さくはできない）
- DBを使う場合、バックアップをどうするか決めた（有料オプション、または自分で取る）
- 支払い方法（カード・あと払い・プリペイド）と、契約の期間（1か月／12か月）を決めた
- 公式のお知らせで、受付状況を確認した
- 鍵の置き場所を決めた（E6）

5. 契約直後に、必ずやること：防犯の初期設定

VPSは、入り口（ポート）を開けた瞬間から、世界中の攻撃の対象になる（エックスサーバーの公式の解説）。契約直後の設定が、最も大切。公式の手順は、次の3つ。

1

1 OSとソフトを、最新にする

古いままだと、すでに知られている弱点を、突かれる

2

2 安全に、遠隔操作できるようにする

管理用の一般ユーザーを作る／パスワードではなく、鍵（公開鍵認証）で入る／管理者（root）での直接のログインを禁止

3

3 ファイアウォール（パケットフィルター）

必要なポートだけを開ける（遠隔操作、Webの公開用）。契約直後は、すべての接続を拒否する設定

「パスワードで入れる」「rootで入れる」状態を、放置しない

サーバーの乗っ取り（データの流出、暗号資産の採掘への悪用、他者への攻撃の踏み台）は、**初期設定の甘さ**から起きる。作ったサーバーが乗っ取られると、**お客様への信頼と、業務のすべてを失う**。AIに任せるにしても、上の3つは、**人が、設定されたことを確認する**（関所。E2）。

6. Webアプリを設置する流れ

1

1 契約・OSの選択

公式が用意するOS・アプリのひな形から選ぶ（Ubuntuなど）

2

2 防犯の初期設定

4章

3

3 アプリを置く

手元で動いたものを、サーバーに置く。まず、確認用の環境で

4

4 ドメインとHTTPS

ドメインを向ける（DNS）。通信を暗号化する

5

5 バックアップ・見守り

データの保存先、更新の予定、動いているかの確認

AIエージェントに、設置を手伝ってもらうとき（コピーして使う）

コピーして使う

「作ったWebアプリ」を、VPS（Ubuntu）に設置したいです。いきなり操作せず、まず手順を提案してください。

条件：

- ・サーバーに入るのは、私がするか、1コマンドずつ内容を説明して、私の承認を得てからにしてください。
- ・管理者（root）で作業しない。管理用の一般ユーザーと、公開鍵認証にしてください。パスワードでのログインと、rootでのログインは、禁止にしてください。
- ・ファイアウォールは、必要なポート（遠隔操作・Web）だけを開けてください。
- ・鍵・パスワードは、チャットにも、ファイルにも書かない。保管の方法を提案してください（金庫を使う）。
- ・消す操作、権限を変える操作、設定ファイルの書き換えは、実行前に、何がかわるかを説明してください。
- ・作業の前に、サーバーの状態（バックアップがあるか）を確認してください。

AIに渡してはいけないもの

- ・ **秘密鍵（サーバーに入るための鍵）**と、パスワード。チャットに貼らない（E6）。
- ・ サーバーの管理者（root）の権限。必要な操作だけ、1つずつ、人が承認する。
- ・ お客様の実データ（赤の情報。D1）。

7. 動かし始めたあとの運用

頻度	やること
毎月	OS・ソフトの更新を適用する。動作を確認する

頻度	やること
毎週	バックアップが取れているか確認する。ディスクの空き、動いているかを確認する
半年ごと	使っていないポート・ユーザー・鍵を、整理する。鍵の棚卸し（E6）
異常があったとき	慌てて操作を重ねず、状況を記録する。必要なら、サーバーをいったん止め、鍵を入れ替える（E6）

8. お申し込み：エックスサーバー VPS（取次店のお申し込みフォーム）

講師の紹介リンクから、お申し込みの場合（広告）

下のリンクは、エックスサーバーの申し込みページです。講師は、エックスサーバーの**取次店**で、この「申し込みフォーム」のリンクを使ってお申し込みいただくと、**講師に、取次の報酬（紹介料・手数料など）が支払われる場合があります**。お客様への特典の有無・内容は、お申し込みの画面で、エックスサーバーの案内を確認してください。

XServer VPS（標準プラン）のお申し込みフォーム

広告。新規受付は一時停止中（再開は11月中の予定）

XServer VPS（ビジネスプラン・法人向け）のお申し込みフォーム

広告。新規受付は一時停止中（再開は11月中の予定）

公式のお知らせ（受付状況の確認）

再開の日付は、[ここで確認](#)

XServer VPS クラウド（公式・直接お申し込み）

いま受付中。広告ではありません（講師の取次店フォームの対象外）

受付停止の間は、上の2つの申し込みページを開いても、お申し込みができない場合があります。いま申し込めるのは、**VPS クラウド（直接のお申し込み）**です。取次店のリンクを使うかどうかは、自由です。

関連資料

- E5 SupabaseとCloudflare … まず、ここで足りるか確認する
- E6 APIキー（秘密）の扱い … 鍵をサーバーに置かない・金庫に置く
- E2 ハーネスエンジニアリング入門 … 関所と事故から生まれたルール
- E4 Gitの導入と設定／D1 信号機ルール

出典（2026年10月確認）

- 『XServer VPS』新規受付の一時停止のお知らせ（エックスサーバー・2026年9月17日）(https://vps.xserver.ne.jp/support/news_detail.php?view_id=19471)：全プラン、再開は11月中の予定
- XServer VPS クラウド（エックスサーバー）(<https://vpscloud.xserver.ne.jp/>)：料金、日次自動バックアップ、複数台構成
- XServer VPS Cloud開始（VPSニュース・2026年8月31日）(<https://vpshikaku.com/news/vps/vps-2026-08-31-xserver-vps-cloud-launch/>)：従来のVPSとの違い、APIは未提供（二次情報）

- XServer VPSの契約直後に対応すべきセキュリティ対策（エックスサーバー） (<https://vps.xserver.ne.jp/vps-media/initial-security/>) : OS更新、公開鍵認証、root禁止、パケットフィルター
- XServer VPS クラウド 料金（エックスサーバー） (<https://vpscloud.xserver.ne.jp/price/>) : 3章の料金・オプション・構成例（カタログ 2026年8月31日更新版にもとづく）
- XServer VPS クラウド 対応OS一覧（エックスサーバー） (https://vpscloud.xserver.ne.jp/functions/os_images/)
- XServer VPS（エックスサーバー） (<https://vps.xserver.ne.jp/>)
- XServer VPSの「ビジネスプラン」を徹底解説（販売パートナー） (<https://sabameijin.com/xserver-vps-business/>)（ビジネスプランの内容。二次情報）

1日集中合宿：アプリを1本持ち帰る

9:00～19:00。接続チェック→共通課題（午前に前倒し）→各自のアプリ→発表

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

対象ツール：Claude Code

この資料は、**Claude Code**（Anthropic のAIエージェント。Claudeのデスクトップアプリの「Code」タブ）を前提に書いています。ほかのAIエージェント（OpenAI のCodex、Google のエージェントなど）は、**画面・用語・ファイル名・設定が異なります**。

対象の方：開発者ではない方（経営者・事務・現場の担当者）。プログラミングは不要です。**コードは書かず、AIエージェントに頼んで、自分の業務アプリをつくる**ところまでを、順に進めます（ターミナルの黒い画面は、使わない形で書いています）。

ゴール：自分の仕事の困りごとを1つ、「動くアプリ」にして持ち帰る

プログラミング経験は不要。Claude Code（または Claude）に、日本語で頼みながら作る。**座学で終わらせず、1日で「怖くない・楽しい・できた」を全員に届ける**のがこの合宿の型。AIサロン桑名での合宿（2日間・約11時間）の手応えをもとに、1日（約10時間）に圧縮した。

対象と条件

こんな方	ChatGPT や Gemini Notebook は使っているが、自分でアプリを作ったことはない。仕事に「これが何とかなれば」という困りごとがある
定員の目安	6～10名／講師2名（似たテーマ同士の2グループに分け、講師が1人ずつ伴走）
事前に必須	約50分・3つだけ（G3）：①Claudeの有料版（Pro）の契約とデスクトップアプリのインストール（A4：Windows・Mac）②GitHubのアカウント作成（無料）③「作りたいもの」を3行のメモに。 読み物の予習はなし （フォルダ・指示書・Gitの設定は当日、一緒に）。ノートPCと電源は持参
その後	翌週の定例勉強会で作ったアプリを発表（「作って終わり」にしない）

1日の流れ（9:00～19:00）

座学を減らし、**共通課題を午前の早い時間に前倒し**する。フォルダ・指示書・鍵・保存は、読ませず、共通課題の中で「必要になった瞬間」に教える。

時間	内容	資料
9:00	ご挨拶・音声解説「AIの現在地」（短縮）・全員の「作りたいもの」を1分ずつ共有・ 鍵の3原則 （鍵はチャットに貼らない／ファイルに書かない／決まった1か所にだけ置く）	D1

時間	内容	資料
9:30	フォルダのミニ講義 （10分）：置き場所（ホーム直下の作業フォルダ）・同期フォルダを避ける・1仕事=1フォルダ。続けて 接続チェック ：配布した「ひな形」を複製してアプリ名に変え、Gitの設定とGitHub Desktopの導入を、Claudeに頼んで進める。事前準備が済んでいない人もここで吸収（ただしClaudeの契約は事前に必須）。 入れてよい情報・いけない情報 を口頭説明（個人情報・鍵は入れない）	E1・E4・D1
10:00	共通課題 ：全員で同じ小さなアプリ「ひとことメモ台帳」を、 各自のデータベース（Supabase）に保存して公開（Cloudflare） まで作る（練習用なので個人情報は書かない）。「作る→直す→見せる」を1周体験。この中で、フォルダ、指示書（CLAUDE.md）、鍵を書かずにつなぐ方法、変更履歴の保存を、必要になった瞬間に教える。外部サービスのAPIを使いたい人だけ、終わった人から別卓で組み込みへ	E1・E5
11:45	振り返り （15分）：1アプリ=1フォルダ／指示書／戻せる保存、の3つを、いま作ったものを見ながら整理	E1・E2
12:00	昼食	
13:00	アプリ依頼シート ：AIに質問してもらい、「作りたいもの」を1枚にまとめる → 各自のアプリづくり① ：最初の画面を出す（グループ内で見せ合い）	B1a・F1
15:00	休憩・つまずき共有（同じところで止まっている人を講師がまとめて説明）	
15:20	各自のアプリづくり② ：データ（仮のデータ）を入れて実際に使ってみる → 直したいところを頼み直す	
17:30	仕上げ ：スマホで開けるようにする、使い方を1枚にまとめる、変更履歴を保存	E1
18:15	発表 （1人3分）：困りごと → 作ったもの → この先どう育てるか	
18:50	まとめ・受講後アンケート・次の発表会の案内	

実績：2026-10-17 AIサロン桑名 特別回

この型を、各自のアカウントでデータベースと公開先まで作る構成に具体化して実施予定（講師2名・定員10名）。依頼があれば、この実績の進め方と本資料を組み合わせ、依頼先に合わせて組み直す。

作るものの例（申込み時の困りごとから）

予定・台帳をスマホで

ホワイトボードや紙の予定・配車・案件台帳を、誰でもスマホで見直せるように。

記録を探せるように

面談・接客・点検の記録をまとめて、すぐ検索できるように。

集計を一言で

毎月の集計作業を「よろしく」の一言で終わらせる。

写真から見積もり

写真やセンサーのデータから、見積もりや予測を出す。

成功させるコツ（過去の合宿から）

- 共通課題を先にやる：全員が同じ土台で1回作ると、連帯感と安心感が生まれ、午後の個別課題で止まりにくい
- 資料の作り込みより、その場で一緒に作る：凝ったスライドは使い切れない。画面を見せながら一緒に進める
- 作りたいものを事前に集める：当日考え始めると午前が消える
- 「完璧より、動くもの」：1日目のゴールは「使える最初の版」。育てるのはその後
- 発表の場を先に決めておく：人に見せる予定があると、最後まで仕上がる

企業向けの応用

会社でAI活用を始めるときも、最初にこの「集中キックスタート」を行うと定着率が大きく変わる。土台を作ってから、日々の伴走に入る。

2日集中合宿：アプリからスキル化・自動化まで

1日目で動くアプリ、2日目で資料室・スキル・関所・定期実行をつなげて仕組みにする

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

対象ツール：Claude Code

この資料は、**Claude Code**（Anthropic のAIエージェント。Claudeのデスクトップアプリの「Code」タブ）を前提に書いています。ほかのAIエージェント（OpenAI のCodex、Google のエージェントなど）は、**画面・用語・ファイル名・設定が異なります**。

対象の方：開発者ではない方（経営者・事務・現場の担当者）。プログラミングは不要です。**コードは書かず、AIエージェントに頼んで、自分の業務アプリをつくる**ところまでを、順に進めます（ターミナルの黒い画面は、使わない形で書いています）。

ゴール：アプリを1本作り、さらに「スキル化・自動化」まで持ち帰る

1日目で動くアプリを作り、2日目でそれを**仕事の仕組み**にする（スキル化・定期実行・安全の関所・引き継げるフォルダ）。AIサロン桑名で実施した1泊2日の合宿（レクチャー2時間＋ハンズオン9時間）の型がもとになっている。合宿の翌月の発表会には17名が集まった。

対象と条件

こんな方	アプリを作るだけでなく、自分や職場の業務を「一言で回る仕組み」にしたい方。1日合宿（G1）の経験者、または ChatGPT や Gemini Notebook を日常的に使っている方
定員の目安	6～10名／講師2名
事前に必須	G1と同じ（作りたいもの・Claude有料版・デスクトップアプリ・ノートPC・Git と GitHub の準備＝E4）

1日目：動くアプリを1本（9:00～18:30）

時間	内容	資料
9:00	ご挨拶・音声解説「AIの現在地」・作りたいものの共有	
9:45	レクチャー（2時間） ：フォルダ設計と指示書／AIへの頼み方（依頼テンプレ）／MCPファースト（鍵を書かずに外部サービスとつなぐ）／鍵の安全な扱い／AIの使い分け	E1・ E2・A1
11:45	共通課題：全員で同じ小さなアプリを作って公開まで	
12:45	昼食	
13:30	各自のアプリづくり（グループで伴走）	
16:30	中間発表（1人2分）：できたこと・詰まっていること	

時間	内容	資料
17:00	仕上げ・変更履歴の保存・STATUS.mdに「今日の到達点と明日やること」を書く	E1
18:30	1日目終了（懇親会）	

2日目：仕組みにする（9:00～17:00）

時間	内容	資料
9:00	前日のふり返り（STATUS.mdを読むところから再開＝引き継ぎの体験）	E1
9:30	資料室（RAG）をつなぐ：自分の業務資料を Gemini Notebook やアプリに持たせ、根拠付きで答えさせる	B1・B2
10:30	スキル化：いつもの作業の手順を言葉にし、合言葉で呼べるスキルにする	A3
11:30	ハーネス：関所（送信・公開・削除は人が押す）、権限の絞り込み、事故をルールに変える練習	E2
12:15	昼食	
13:00	自動化：定期実行を1つ設定（例：毎週月曜に集計して報告）。ローカルLLMの話（希望者）	A3・E3
14:30	仕上げ：使い方1枚・運用ルール・引き継ぎ用の決定ログ	E1
15:30	発表（1人5分）：困りごと → アプリ → スキル・自動化 → 次の一手	
16:40	まとめ・受講後アンケート・発表会の案内	

持ち帰るもの

動くアプリ1本 スマホで開ける、自分の困りごとを解くアプリ。	スキル1つ＋定期実行1つ 合言葉で呼べる業務手順と、自動で動く仕組み。	引き継げるフォルダ 指示書・現在地・決定ログがそろった、別の日・別の人でも続けられる形。
--	---	--

1日合宿（G1）との違い

	1日合宿（G1）	2日合宿（G2）
ゴール	動くアプリを1本	アプリ＋スキル化・自動化・引き継げる形
レクチャー	約1時間45分（要点に絞る）	約2時間＋2日目に各30～60分
向いている人	まず作ってみたい	職場の仕組みにしたい

集中講座の事前準備：3つだけ（約50分）

事前は、Claudeの契約とアプリ、GitHubのアカウント、作りたいもののメモ、の3つだけ。読み物はなし

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

事前準備は、3つだけ。約50分です

集中講座では、当日の時間を**アプリをつくるために使う**ため、事前をお願いすることを、最小限に絞っています。**読み物の予習はありません**。フォルダの作り方やGit（変更履歴の保存）の設定は、当日、講師と一緒に手を動かして進めます。

事前に済ませるのは、**当日に始めると時間が読めなくなる**ことだけです。

事前をお願いする3つ

1

1 約30分

Claudeの有料プラン（Pro）の契約と、デスクトップアプリのインストール

2

2 約10分

GitHub（作ったものを預けるクラウド上のバックアップ置き場）のアカウントを作る（無料）

3

3 約10分

「作りたいもの」を、3行くらいのメモにする

1の画面つきの手順は A4 Claudeの契約と、デスクトップアプリの最初の設定 にあります。

当日に、一緒にやること

- Gitの設定と、GitHub Desktopの導入
- 仕事のフォルダと、指示書（CLAUDE.md）の作成
- 入れてよい情報・いけない情報（D1 信号機ルール）、鍵の安全な扱い
- 共通課題（小さなアプリを作って公開まで）と、各自のアプリづくり

お申し込みの方へ

お申し込みの方には、期限・つまりいたときの相談方法・チェックリスト・当日の準備物一式（ひな形）を、メールで個別にご案内します。

関連資料

- G1 1日集中合宿（時間割）／G2 2日集中合宿
- A4 Claudeの契約と最初の設定

ワークシート：業務の棚卸しと仕組み化

自分たちの業務を書き出し、4段階に仕分けて、最初の3つを選び、手順を言葉にして仕組みにする

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

対象ツール：Claude Code

考え方は、どのAIエージェントにも共通です。ただし、**ファイル名・画面・設定・コマンドは、Claude Code**（Claudeのデスクトップアプリの「Code」タブ）の場合です。ほかのAIエージェントでは、読み替えが必要です。

対象の方：開発者ではない方（経営者・事務・現場の担当者）。プログラミングは不要です。**コードは書かず、AIエージェントに頼んで、自分の業務アプリをつくる**ところまでを、順に進めます（ターミナルの黒い画面は、使わない形で書いています）。

このワークシートでやること

書き出す → 仕分ける → 最初の3つを選ぶ → 手順を言葉にする（仕組み化） → 試す。業種や職種は問いません。自分の仕事を材料に、紙に書きながら進めます。

「**仕組み化**」とは：その仕事のやり方を、新人に引き継げる手順書にして、AIに同じ手順・同じ品質で任せられる形にすること（段階③スキル化・④自動化）。

AI活用の4段階

段階	道具	たとえ	向いている仕事
① 相談相手	ChatGPT・Gemini・Claude	物知りの同僚に聞く	たたき台、壁打ち
② 資料室（RAG）	Gemini Notebook（職場で共有）	司書のいる資料室	資料を根拠に答える、要約する
③ スキル化	AIエージェント（Claude／Claude Code）	仕事を型ごと新人に引き継ぐ	毎回同じ手順で書類を作る
④ 自動化	AIエージェント＋定期実行	任せた部下が報告書を持ってくる	決まったきっかけで毎回やる仕事

見分け方：「聞けば済む仕事」→①② / 「毎回同じ手順で書類を作って次に渡す仕事」→③④

1

Q1 聞けば済む？
はい → ① 相談相手

2

Q2 手元の資料を根拠に
答えさせたい？
はい → ② 資料室（RAG）

3

Q3 毎回ほぼ同じ手順
で、書類やメールの下
書きを作る？
はい → ③ スキル化

4

Q4 「毎週月曜」「ファ
イルが届いたら」と、
きっかけが決まってい
る？
はい → ④ 自動化

ステップ1：業務を書き出す

付箋1枚に1業務。まず思いつく順に、5〜10個書く。完璧でなくてよい。

業務名	頻度	1回の時間	使う資料	出来上がるもの	信号
例：請求書の月次チェック	毎月	3時間	取引先の請求書PDF	不備の一覧・修正依頼文	黄
例：お客様の問い合わせへの返信	毎日	1時間	過去の返信・よくある質問	返信メールの下書き	黄

頻度：毎日／毎週／毎月／時期もの。信号：● 青 公開情報 ● 黄 匿名化すれば可 ● 赤 個人情報・決算書など（D1）

書き出すときのコツ：「誰かに頼むなら、どう説明するか」で考える。説明できる仕事は、AIにも説明できる。

ステップ2：4段階に仕分ける

書き出した業務を、上のQ1〜Q4で、①〜④のどれに当たるか仕分ける。迷ったら、手前の段階から始める。

① 相談相手	② 資料室（RAG）	③ スキル化	④ 自動化
例：案内文のたたき台	例：就業規則を根拠に答える	例：請求書チェックの手順	例：毎週月曜に未対応の一覧

ステップ3：最初の3つを選ぶ

評価の軸は2つだけ：効果（頻度×時間）と始めやすさ（信号が青〜黄）。それぞれ1〜3点で付け、合計の高いものから3つ。

#	業務	効果（1～3）	始めやすさ（1～3）	目指す段階	最初の一步
1					
2					
3					

効果3＝毎日・毎週で時間がかかる。始めやすさ3＝信号が青で、資料がそろっている。赤の情報が中心の業務は、いまは選ばない。

ステップ4：仕組み化する（手順を言葉にする）

③④に進む業務は、「手順書」を書くところから始まる。AIに任せる前に、人が「どこまでやるか」を決めておく。手順書は、次の5つを埋めれば完成。

項目	書くこと	例：請求書の月次チェック
① 出来上がり	何が、どんな形でできればよいか	不備の一覧（Excel）、取引先への修正依頼文（メールの下書き）、件数の集計
② 材料	使う資料と、置き場所・名前のルール（B2）	フォルダ「請求書／2026-10」の請求書PDF、取引先リスト、前月分
③ 手順	1・2・3の順に。判断のポイントも書く	1 PDFから取引先名・日付・金額・税区分を表にする／2 取引先リストと照合する／3 前月と大きく違うものに印を付ける／4 不備がある取引先ごとに修正依頼文を作る
④ 人が確認するところ	AIに任せず、人が見る・押す所（E2の「関所」）	金額は人が最終確認／メールは下書きまで、送信は人が押す／口座番号などの赤の情報は入れない
⑤ 例外と目安	うまくいかないケースと、成功の目安	手書きの請求書は人が処理／3時間 → 30分、見落としゼロ

あなたの業務の手順書（ステップ3で選んだ1つ目）

項目	書く
業務名	
① 出来上がり	
② 材料	
③ 手順	

項目	書く
④ 人が確認するところ	
⑤ 例外と目安	

ステップ5：試す → 直す → 定着させる

いきなり自動化しない。手で一度やってから、手順書にして、スキルにして、最後に自動化する。手順書は、使いながら直して育てる。

1

1回目：毎回AIに頼む

(①)

手順を言葉にしながら実際にやる。うまくいった頼み方をメモする

2

2回目：手順書にする

ステップ4の5項目を埋める。
引き継げる文章になったかを
確認

3

3回目：スキルにする

(③)

手順書をClaudeに渡して
「スキルにして」と頼む。以
後は一言で同じ品質

4

4回目：自動化する

(④)

きっかけ（毎週月曜・ファイ
ルが届いたら）を決める。確
認は人

コピーして使う

次の手順書を、毎回同じ手順・同じ品質で実行できる「スキル」にしてください。「人が確認するところ」は、必ず私の確認を待ってから先に進むようにしてください。

（ここにステップ4の手順書を貼る）

仕組み化でつまづく3つのポイント

- 手順が頭の中にある：やりながら書く。書けないところが、属人化している所
- 最初から全部やろうとする：1つの業務の、1つの工程だけから始める
- 確認を外してしまう：送信・公開・削除は、慣れても人が押す。口座番号など赤の情報は入れない

明日からの3手

1. 信号機ルールを職場で確認し、● 赤の情報は今日から入れない
2. 手元の資料を1つ選び（就業規則・マニュアル・取扱説明書、または補助金の公募要領など）、Gemini Notebookでノートブックを作って職場で共有する（無料で可）
3. 有料版を1ヶ月試し、選んだ業務を1つ、ステップ4の手順書に書いてスキル化してみる

Google Workspace と Google One の違い

個人・家族向けと、仕事向け。3種類のアカウント、違いの一覧（資料室RAGを含む）、個人アカウントで仕事を続けると起きること、どちらを選ぶか

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

Google One は「自宅の物置」、Google Workspace は「管理人付きの事務所」

同じ「Google」でも、**個人で使うもの**と**仕事で使うもの**は、作りが違う。Google One は、写真や書類をしまう**個人・家族向けの保管場所**。Google Workspace は、会社・団体・個人事業主の**仕事のための事務所**で、独自のメールアドレス、管理者による管理、組織のデータ保護が付く。

この資料では、3つの違いをはっきりさせる。そのうえで、「**自分の仕事に、Workspace は必要か**」を判断できるようにする。

1. 「Googleのアカウント」は、3種類ある

① 個人のGoogleアカウント

誰でも無料で作れる。Gmail（〇〇@gmail.com）、ドライブ、フォトなど。保存容量は、Gmail・ドライブ・フォトを合わせて**15GB**。

② Google One

個人のアカウントに、**保存容量やAI機能を足す、有料の個人向けプラン**。最大5人で、容量を共有できる（家族向け）。

③ Google Workspace

法人・団体・個人事業主向け。独自ドメインのメール、管理者機能、組織のデータ保護。ユーザーごとに月額。

2. 違いの一覧

観点	個人のアカウント／Google One	Google Workspace
想定する使い方	プライベート・家族	仕事（会社・団体・個人事業主）
メールアドレス	〇〇@gmail.com で固定	独自ドメイン （〇〇@自社名.co.jp など）
料金	無料／Basic 月290円（100GB）／Google AI Plus・Pro など（Google Oneのページの表示）	ユーザーごとに月額（Starter 800円～、税別。→ W2）
保存容量	無料15GB。有料プランで100GB～5TB（最大5人で共有）	プランにより、 1ユーザーあたり30GB～5TB
管理者による管理	なし（本人がすべて管理する）	管理コンソール で、ユーザーの追加・停止、権限、セキュリティ設定を一括管理

観点	個人のアカウント／Google One	Google Workspace
データの持ち主	個人	組織（退職者のデータも、組織に残せる）
会社の資料を、AIの根拠にする（RAG）	個人のドライブの資料を、個人で使う形になる	共有ドライブの資料を、全員で共有して、権限のとおりに使える。ドライブを直すと、AIの資料も自動で更新（→ W2）
AI（Gemini）に入力した内容	設定により、会話が改善に使われ、人の確認に回ることがある（設定で管理）	学習には使われず、顧客の許可なく人が確認することもない（Google の公式説明。→ W2）
Meet（会議）の参加人数	—	プランにより100～1,000人（→ W2）

個人アカウントとWorkspaceの管理・データの所有に関する違いは、販売パートナー各社の解説にも共通する内容。契約前に、Google の公式の説明で確認すること（出典欄）。

3. 個人のアカウントで仕事を続けると、起きること

場面	起きること
従業員が辞めた	仕事のメール・資料が、 本人の個人アカウントに残る 。組織で回収できない
誰かがパスワードを忘れた・乗っ取られた	組織としては、止める・リセットする手段がない
取引先に、メールを送る	「@gmail.com」では、会社の信頼感や、なりすまし対策の面で、不利になりやすい
AIを使う	入力した内容の扱いが、個人の設定に任される。 お客様の情報を入れてよいか、組織として保証できない （→ D1）
複数人で資料を共有する	個人のドライブ同士の共有になり、持ち主が抜けると、資料が消えたり、見えなくなったりする

4. あなたは、どちらを選ぶ？

1 Q1 仕事でお客様とメールをする？ はい→ 独自ドメインのメールが要る → Workspace	2 Q2 2人以上で、資料を共有する？ はい→ 管理と共有の仕組みが要る → Workspace	3 Q3 AIに、仕事の情報を入れる？ はい→ 組織としてのデータ保護が要る → Workspace	4 Q4 全部「いいえ」？ 写真・個人の書類の保管だけなら、Google One で足りる
--	---	---	--

目安

- Google One で足りる：プライベートの写真・書類の保管、家族との共有。
- Workspace が向く：1人でも、お客様とやりとりする個人事業主は、独自ドメインと組織としてのデータ保護の利点がある。従業員がいる、または、資料を共有する組織は、ほぼ、Workspace。

5. Workspace に含まれる主なもの

サービス	ひとことで
Gmail	独自ドメインのメール
ドライブ	資料の保管と共有。組織の共有ドライブも使える
ドキュメント・スプレッドシート・スライド	文書・表・資料を、複数人で同時に編集
Meet	オンライン会議（人数の上限はプランにより異なる）
カレンダー・チャット	予定の共有、社内の連絡
Gemini・Gemini Notebook	AIの相談相手と、資料を根拠に答える司書。 共有ドライブの資料を土台に、会社の「資料室」（RAG）になる（→ W2の5章、B1b）
管理コンソール	ユーザーの追加・停止、セキュリティ設定（2段階認証など）、AIのオン・オフ

関連資料

- W2 Google Workspaceのプランと、AI・情報の守り方
- W3 導入の進め方と、お申し込み（ご紹介）
- A2 無料版・有料版・組織契約の違い／D1 信号機ルール

出典（2026年10月確認）

- Google One プランと料金（Google）（<https://one.google.com/about/plans?hl=ja>）：無料15GB、Basic、Google AI Plus・Pro、最大5人で共有
- Google Workspace 料金（Google）（<https://workspace.google.com/intl/ja/pricing.html>）：プラン、ストレージ、Meetの参加人数
- Generative AI in Google Workspace Privacy Hub（Google）（<https://knowledge.workspace.google.com/admin/generative-ai/generative-ai-in-google-workspace-privacy-hub>）：Geminiのデータの扱い
- Google Workspace と個人向け Google サービスとの違い（販売パートナー）（<https://www.g-workspace.jp/comparison-googleworkspace-gmailcom/>）（独自ドメイン・管理者機能・データの所有）
- 個人用のGoogleアカウントとGoogle Workspaceの違い（KDDIウェブコミュニケーションズ）（<https://academy.kddi-web.com/beginner/google-account-comparison>）（二次情報）

Google Workspace のプランと、AI・情報の守り方

プランと料金（公式）、月額が目安、選び方、Geminiの入力データの扱い、共有ドライブ×Gemini Notebookで作る会社の資料室（RAG）、契約前の確認

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

プランは「人数 × 月額」。選ぶ軸は、容量・会議の規模・AIの範囲

Google Workspace は、ユーザー（アカウント）1人ごとの月額。人数が増えれば、その分が増える。プランの違いは、おもに、**保存容量・会議（Meet）の参加人数・使えるAI機能の範囲**。そして、仕事でAIを使う人にとって、もう1つ大事なのが、**入力した情報の扱い**。

1. プランと料金（2026年10月時点・Google公式の料金ページの表示）

	Business Starter	Business Standard	Business Plus	Enterprise
月額（1ユーザー・税別）	800円	1,600円	2,500円	営業担当に問い合わせ
保存容量（1ユーザー）	30GB	2TB	5TB	5TB（追加可）
Meet の参加人数	100人	150人	500人	1,000人
AI（Gemini）	各プランに、Gmail の Gemini が搭載。上位のプランほど、ドキュメント・スプレッドシート・Meet のAI機能が充実			—

新規のお客様向けの割引（公式料金ページの表示）

Business Starter：3か月間 20%オフ（640円）、Business Standard：3か月間 50%オフ（800円）、Business Plus：3か月間 50%オフ（1,250円）。キャンペーンの内容・期間・対象は、変わることがあるので、お申し込みの画面で確認すること。紹介リンクからの特典は、W3。

年間契約か月ごとの契約かで、金額や条件が変わる場合がある。料金は、契約前に、公式の料金ページで必ず確認する。セキュリティ・管理機能の違いも、公式の比較表で確認する。

2. 月額の目安（税別・通常料金）

人数	Starter（800円）	Standard（1,600円）	Plus（2,500円）
1人	800円	1,600円	2,500円
3人	2,400円	4,800円	7,500円
5人	4,000円	8,000円	12,500円

人数	Starter (800円)	Standard (1,600円)	Plus (2,500円)
10人	8,000円	16,000円	25,000円

3. どのプランを選ぶか

1

メールと、書類・表の共有が中心
→ Business Starter。容量は1人30GB。写真や動画を大量に置かないなら足りる

2

大きなファイルや、会議が多い
→ Business Standard。1人2TBの容量。Meet 150人

3

大規模な会議、より多くの容量
→ Business Plus。1人5TB。Meet 500人

4

迷ったら
→ まず Starter か Standard。あとからプランは変えられる（条件は、契約時に確認）

4. AI（Gemini・Gemini Notebook）と、情報の守り方

仕事でAIを使うときの最大の悩みは、「お客様の情報を入れて、大丈夫か」。Workspace のGeminiについて、Google は、公式に次のように説明している。

項目	Google Workspace のGemini（公式の説明）	個人のアカウントのGemini
入力の内容を、モデルの学習に使うか	使わない（顧客の事前の許可なく、学習・微調整に使わないことを、利用規約で約束）	設定により、会話が、サービスの改善に使われることがある
人が、内容を確認するか	顧客の許可なく、人が確認することはない	評価（👍👎）などで、人の確認に回ることがある（→ B1b）
会話の保存期間	管理者が決める（Gemini in Workspace：90日～無期限、Geminiアプリ：最大36か月）	本人の設定
管理者の制御	Geminiのオン・オフ、保存期間、対象サービスの選択、ユーザーの権限	なし

「安全」は、契約しただけでは、完成しない

Workspace にすると、データの扱いは、組織の契約で守られる。しかし、「何を入れてよいか」を決めるのは、組織。D1 信号機ルール（入れてよい情報・いけない情報）を、導入と同時に決める。また、管理者は、AI のオン・オフや、保存期間を、最初に設定する。

Workspace × 他のAI

- **Gemini Notebook**：お客様の情報を入れるなら、Workspace のアカウントで使う（B1b）。
- **ChatGPT・Claude などの、他社のAI**：Workspace の契約とは別。それぞれの契約（個人・組織）と、データの扱いを確認する（A2）。
- **情報を外に出したくない業務**は、社内のPCで動くAI（ローカルLLM）という選択肢もある（E3）。

5. Workspace × AI：会社の「資料室」(RAG)をつくる

Workspace の本当の強みは、ドメインで組織として管理され、資料を会社として共有できること。ここにAIを組み合わせると、「会社の資料を根拠に答えるAI」=RAG (→ B1b) が、会社の全員で使えるようになる。個人のアカウントでは、こうはいかない。

Workspace にあるもの	RAG で、なぜ効くのか
独自ドメインの、組織のアカウント	全員が、同じ組織の一員として、同じ資料室を使える。入社・退職で、アカウントを管理者が追加・停止できる
共有ドライブ（組織の資料置き場）	資料が、個人ではなく、 会社のもの になる。退職者がいても残る。資料室の「棚」になる
アクセス権（誰が何を見られるか）	Gemini は、 ユーザー本人と同じ範囲 でしか、 Workspace のデータにアクセスしない （Google 公式）。権限のない資料は、AIの答えにも出てこない。ただし、ファイルの持ち主がダウンロード・コピー・印刷を禁止しているものは、Gemini も使えない
Gemini Notebook × ドライブ	ドライブのドキュメント・スプレッドシート・スライドを、資料として登録できる。 ドライブ側を直すと、ノートブックの内容も自動で更新される （2026年5月から順次）。権限が取り消されると、その資料は使えなくなる
管理者の設定	AIのオン・オフ、会話の保存期間、 組織の外への共有の可否 （ドメイン・部署・グループ単位）を、管理者が決められる
入力データの保護	入力した内容は、学習に使われず、顧客の許可なく人が確認することもない（4章）。お客様に関わる資料も、ルールを決めれば扱える（D1）

資料室ができるまで

1

1 資料を、共有ドライブに整理
置く場所・名前・更新のルールを決める（B2）

2

2 フォルダごとに、権限を決める
全社に見せるもの／部署だけ／人事・給与など限定

3

3 Gemini Notebookに、ドライブの資料を入れる
就業規則・マニュアル・FAQ・見積のルールなど

4

4 全員が、質問する
根拠のページ付きで答える。新人でも、同じ根拠で

5

5 更新は、ドライブ側で
直すと、自動で反映。古い資料は、削除か「旧版」へ

資料室の前に、「権限の設計」が先

- RAG は、権限を回避しない。しかし、**権限が広すぎると、AIを通じて、見せたくない資料まで、見える範囲が広がる**。人事・給与・契約書などは、別のフォルダにして、見られる人を限定する。
- **古い資料を残すと、AIが古い内容で答える**。更新日を決めて、差し替える（B2）。
- 自動の更新の対象は、ドキュメント・スプレッドシート・スライド。**PDFなどは、手で入れ直す**。
- RAG の限界（調べて答えるまで。仕事を自動で進めるのは、AIエージェント）は、B1b・A3。

これが、「Workspace を契約する理由」の、もう1つの柱：メール・共有の土台に、AIと資料室（RAG）が、安全に乗る。

6. 契約する前の確認（Workspace を検討する人へ）

☐	確認すること
☐	何人が使うか（いまの人数と、半年後の人数）
☐	独自ドメインは、すでに持っているか（持っていなければ、取得が要る）
☐	いまのメールは、どこで運用しているか。切り替えの計画があるか（→ W3）
☐	ファイルの量は、1人30GBで足りるか
☐	Meet は、何人規模の会議があるか
☐	AIに入れてよい情報を、決める人と、ルールがあるか（D1）
☐	会社の資料室にしたい資料（規程・マニュアル・FAQ）と、見られる人の範囲を、洗い出したか（5章）
☐	管理者を、だれが、どう引き継ぐか

関連資料

- W1 Google Workspace と Google One の違い
- W3 導入の進め方と、お申し込み（ご紹介）
- A2 無料版・有料版・組織契約の違い／D1 信号機ルール／B1b RAG

出典（2026年10月確認）

- Google Workspace 料金（Google）（<https://workspace.google.com/intl/ja/pricing.html>）：プラン、月額（税別）、ストレージ、Meet、新規割引
- Generative AI in Google Workspace Privacy Hub（Google）（<https://knowledge.workspace.google.com/admin/generative-ai/generative-ai-in-google-workspace-privacy-hub>）：学習に使わない、人が確認しない、保存期間、管理者の制御
- Google One プランと料金（Google）（<https://one.google.com/about/plans?hl=ja>）
- What controls Gemini's access to Workspace data（Google）（<https://support.google.com/a/users/answer/17010577?hl=en>）：Gemini は、ユーザーと同じ権限で、データにアクセスする
- Drive の自動同期（Google Workspace Updates・2026年5月）（<https://workspaceupdates.googleblog.com/2026/05/keep-your-sources-up-to-date-with-automatic-Drive-syncing-in-NotebookLM.html>）：Docs・Sheets・Slides の更新が、ノートブックに自動反映
- Gemini Notebook の外部共有の管理（Google Workspace Updates・2026年9月）（<https://workspaceupdates.googleblog.com/2026/09/manage-external-sharing-for-gemini-notebook-in-the-Admin-console.html>）

Google Workspace 導入の進め方と、お申し込み（ご紹介）

導入の流れ、メールの切り替え（MX）の注意、最初の設定、よくある失敗、ご紹介リンク（広告表示つき）

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

広告（紹介料）についてのお知らせ

この資料の末尾（7章）には、講師（株式会社ヒューマック 伊藤）が参加している、**Google の「Google Workspace ご紹介プログラム」**の紹介リンクが載っています。このリンクからご契約いただくと、条件を満たした場合に、**Google から講師に紹介料が支払われます**。資料の内容（料金・違いの説明）は、公式の情報にもとづいて書いています。紹介リンクを使わずに、Google に直接申し込むこともできます。

1. 導入の流れ（全体像）

1

1 準備

人数・ドメイン・いまのメールの運用先を確認する（W2の確認表）

2

2 申し込み

管理者のアカウントを作る

3

3 ドメインの所有確認

そのドメインが自分のものだと、Googleに証明する

4

4 ユーザーを作る

一人ずつ、またはCSVで一括

5

5 メールの切り替え

最後に。ここで受信先が、Googleに変わる

順番が大事。「メールの切り替え」は、必ず、全員のアカウントを作り終えてから行う。

2. 事前に決めておくこと

項目	決めること・確認すること
独自ドメイン	すでに持っているドメイン（例：自社名.co.jp）を使うか、新しく取るか。ドメインを管理しているサービス（登録事業者）のログイン情報が、だれの手元にあるか
管理者	管理コンソールを操作する人。1人に集中させず、予備を決める（退職・不在のときに、困らないように）
ユーザー	全員の名前と、メールアドレス（〇〇@自社ドメイン）
いまのメール	現在、どのサービスで運用しているか。過去のメールを、新しい環境に移す必要があるか
AIのルール	入れてよい情報・いけない情報（D1）。Gemini のオン・オフ（W2）

3. メールの切り替え（MXレコード）で、いちばん注意すること

メールの宛先を決める設定を「MXレコード」と呼ぶ。Google の公式の説明では、次のとおり。

- 設定する値は、smtp.google.com（優先度 1）。
- 設定すると、受信メールが、Google に届くようになる。
- ほかのMXレコードは、すべて削除する。古い設定や誤った設定が残ると、メールが正しく届かなくなる。
- 反映には、最長で72時間ほどかかることがある。
- 設定の前に、ドメインの所有権を証明している必要がある。

メールが止まる事故を、防ぐ

- 切り替える前に、いまの設定（MXレコード）を、画面の写真や文字で、記録しておく。
- 切り替えは、取引先からの連絡が少ない日・時間帯に。反映の間、受信が不安定になることがある。
- ホームページのドメインと、メールのドメインが同じ場合、DNS（ドメインの設定）の変更で、ホームページまで止まることもある。変更は、設定を理解している人が、1つずつ確認しながら行う。AIに任せきりにしない（E5）。
- 切り替え後に、自分宛てに、テストメールを送って、受信できるか確認する。
- 古いメールサービスの解約は、新しい環境で、数日、問題なく動いてから。

4. 導入したあとの、最初の設定

設定	目的
2段階認証	パスワードが漏れても、乗っ取られにくくする。全員に、早い段階で
管理者の予備	管理者が不在でも、ユーザーの停止・パスワードのリセットができるように
共有ドライブ	仕事の資料を、個人ではなく、組織のものにする（退職者がいても、資料が残る）
Gemini の設定	オン・オフ、会話の保存期間、組織の外への共有の可否を決める（W2）
会社の資料室（RAG）	共有ドライブに規程・マニュアル・FAQ を整理し、権限を決めてから、Gemini Notebook に入れる（W2の5章）
AIの使い方のルール	信号機ルールを、全員に共有する（D1）

5. よくある失敗

ドメインの管理者が、分からない

以前の制作会社や、退職した人が登録している。申し込み前に、ログイン情報の持ち主を確認する。

全員を作る前に、メールを切り替える

作っていない人のメールが、届かなくなる。ユーザー作成が先。

古いMXレコードが残る

メールが届いたり、届かなかったりする。ほかのMXは、すべて消す（公式）。

管理者が1人きり

その人が不在だと、何もできない。予備を決める。

ルールを決めずに、AIを使い始める

「何を入れてよいか」は、組織が決める。信号機ルールを、導入と同時に。

個人のアカウントに、資料を残す

共有ドライブに移して、組織のデータにする。

6. ご契約を検討されている方へ

導入に不安がある方は、講師にご相談ください。上の確認表（W2）を埋めたうえで、**人数・ドメイン・いまのメールの運用先**をお伝えいただくと、話がスムーズです。

7. お申し込み：Google Workspace ご紹介リンク

講師の紹介リンクから、お申し込みの場合

講師は、Google の「Google Workspace ご紹介プログラム」に参加しています。**紹介リンクを経由してご契約いただいた方にも、特典があります。**特典の内容と条件（割引の率・期間・対象のプラン・新規のドメインが対象か、など）は、**お申し込みの画面で、Google の案内を、必ず確認してください。**公式の料金ページの新規割引（W2）との併用の可否も、お申し込みの画面で確認できます。



スマホで読み取ると
お申し込みのページが開きます

Google Workspace を申し込む（ご紹介リンク）

広告：紹介料が講師に支払われる場合があります

Google に直接申し込む（公式の料金ページ）

紹介リンクを使わずに申し込む場合

紹介リンクを使うかどうかは、自由です。特典の内容は、Google の都合で変わることがあります。

8. はじめての日のチェックリスト

- | | |
|--------------------------|-----------------------------------|
| ☐ | 確認すること |
| ☐ | 人数・ドメイン・いまのメールの運用先を、確認した |
| ☐ | ドメインの登録事業者に、ログインできる（持ち主を確認した） |
| ☐ | 管理者と、予備の管理者を決めた |
| ☐ | 全員分のアカウントを作った |
| ☐ | いまのMXレコードを、記録してから、切り替えた（ほかのMXは削除） |
| ☐ | テストメールで、受信を確認した |
| ☐ | 2段階認証を、全員に設定した |

□ 確認すること

- AIのルール（信号機ルール）と、Gemini の設定を決めた

関連資料

- W1 Google Workspace と Google One の違い／W2 プランと、AI・情報の守り方
- E5 SupabaseとCloudflare … ドメイン・DNSの扱い
- D1 信号機ルール

出典（2026年10月確認）

- Google Workspace 用の MX レコードの設定（Google）（<https://knowledge.workspace.google.com/admin/domains/set-up-mx-records-for-google-workspace?hl=ja>）：smtp.google.com、他のMXは削除、最長72時間
- Google Workspace 料金（Google）（<https://workspace.google.com/intl/ja/pricing.html>）
- Generative AI in Google Workspace Privacy Hub（Google）（<https://knowledge.workspace.google.com/admin/generative-ai/generative-ai-in-google-workspace-privacy-hub>）
- Google Workspace 初期設定ガイド（販売パートナー）（<https://googleworkspace.tscloud.co.jp/google-workspace/initial-setup>）（導入の流れ。二次情報）