非エンジニアのための

公開前チェックリスト 24項目

AIで作ったツールを、社内や外部に出す前に。
技術がわからなくても、上から順に答えていけば確認できます。

> **動くかどうかは、作った本人がわかります。**
> **公開していいかどうかは、本人にはわかりません。**

使い方

1. 上から順に読み、「はい」と言い切れる項目だけ □ にチェックを入れる
2. 各セクションの青い枠は、Claude Code にそのまま貼れる指示文です。迷ったら貼って確認する
3. ★ の7項目は、公開前に必ず塞ぐ。ここが空いていると、残りが完璧でも一晩でデータ流出か高額請求になる
4. 残りの17項目は、公開してから順番に直しても間に合う
5. チェックが埋まらない項目は、最後のページへ

発行：ソウゾウ合同会社

まず、データとキーが漏れる経路をふさぐ

① 他人のデータが見えないか

- [ ] ★ URLのIDを別の番号に変えても、他人のデータが表示されない
  例：/report/123 を /report/124 にして開く。自分のものでなければエラーになるか
- [ ] ★ APIを直接開いても、他人のデータが返らない
  例：/api/... のURLをブラウザに直接入れて、他人の分が出ないか
- [ ] ★ Supabase なら、Advisors → Security に RLS 無効のテーブルが1つもない
  AIにSQLを書かせて作ったテーブルには RLS が付かない。管理画面から無料で確認できる
- [ ] 一覧・検索・CSV出力など、まとめて取り出す機能も自分の分だけに絞られている
  1件ずつの画面は直っていても、一覧やエクスポートが抜けていることが多い

> **Claude Code に貼る**
> ログイン済みの利用者が、他人のデータにアクセスできる経路がないか、攻撃者の視点で監査してください。URLのIDを書き換えた場合と、APIを直接叩いた場合の両方を含めて、該当するファイル名と行を挙げてください

② APIキーが利用者側に出ていないか

- [ ] ★ ブラウザの「ページのソースを表示」に、キーやトークンが出てこない
  画面に見えなくても、ソースに書いてあれば誰でも読める
- [ ] ★ 利用者に配られる設定（Next.js の NEXT_PUBLIC_ など）にキーを入れていない
  名前の通りパブリック。ここに入れたものは全員に見える
- [ ] .env や鍵ファイルを GitHub に上げていない（.gitignore に入れてある）
  キーを探して巡回しているプログラムが常に動いている
- [ ] 一度でも公開の場所に出たキーは、作り直した
  非公開リポジトリに上げた場合も、漏れたものとして扱う

> **Claude Code に貼る**
> このリポジトリに、APIキーやトークンが直書きされていないか監査してください。そのうち、ブラウザ側に配信されるコードに含まれるものを、分けて報告してください

次に、権限とお金の上限を確かめる

③ 権限の確認が画面側だけになっていないか

- [ ] ★ 削除・更新・他人のデータ取得を、サーバー側でも「その権限があるか」確認している
  画面でボタンを隠すのは親切機能。鍵ではない
- [ ] 表示を消しているだけの操作が、他に残っていない
  管理メニュー、編集ボタン、金額の変更など
- [ ] 管理者用のURL（/admin など）を一般の利用者が直接開いても、中身が見えない
- [ ] ログインしていない状態で各URLを開くと、ログイン画面に戻る

> **Claude Code に貼る**
> 画面側で表示を消しているだけで、サーバー側で権限を確認していない操作を洗い出してください。削除、更新、他人のデータの取得を優先して見てください

④ お金の上限とアラート

- [ ] ★ AIに渡す1回の入力量に、上限がある
  小説一冊分を貼り付けられると、1回の送信で数百円かかる
- [ ] 1人あたりの実行回数に、制限がある
  反応がないと思った人が連打するだけで、回数は何倍にもなる
- [ ] AIの答えをまたAIに投げる処理に、回数の上限がある
  止まる条件がないと延々と回る。寝ている間に数万円になる
- [ ] 請求額のアラートを設定してある（例：5,000円を超えたらメール）
  気づくまでの時間が変わる。設定は数分で終わる

> **Claude Code に貼る**
> AIを呼び出している処理をすべて挙げて、1回あたりの入力量の上限、1人あたりの回数制限、繰り返し処理の回数上限が設定されているか確認してください。設定がない箇所は、どのファイルに何を追加すべきか具体的に書いてください

⑤ 想定外の入力でエラーが出ないか

- [ ] データが1件もない状態でも、画面が壊れない
  使い始めの人が最初に見るのが、この画面
- [ ] 極端に長い文字列・絵文字・空欄を入れても、保存でき、表示も崩れない
- [ ] 日をまたぐ時間帯に登録しても、正しい日付で記録・集計される
  23時に登録したものが翌日の集計に入る、はよくある
- [ ] 送信後の再読み込みや戻るボタンで、二重に登録されない

> **Claude Code に貼る**
> このアプリを、想定外の入力で壊してみてください。データが0件の状態、極端に長い文字列、絵文字、日付をまたぐ操作、送信後の戻るボタン。それぞれで何が起きるか、コードを読んで予測して報告してください

⑥ 気づける状態と、戻せる状態か

- [ ] 誰がいつ何をしたかの記録が残る
  記録がないと、漏れたかどうかすら証明できない
- [ ] その記録に、個人情報・パスワード・キーがそのまま出ていない
- [ ] エラーが起きたとき、自分に通知が届く
  利用者に言われて初めて知る、では遅い
- [ ] 1つ前の状態に戻す手順を、データベースの変更込みで確認してある
  画面は戻せても、テーブルの構造を変えていると戻らない

> **Claude Code に貼る**
> エラーが起きたときに記録が残るか、私に通知が来るか、直前の状態に戻せるかを確認してください。あわせて、記録に個人情報やキーがそのまま出力されている箇所があれば指摘してください

> **★ の7項目が埋まるまでは、公開しない。**

※ このチェックリストは一般的な確認の目安です。扱う情報の種類や規模によって、必要な対策は変わります。 発行：ソウゾウ合同会社