

AIを組み込むときの確認表

『WordPressプラグイン開発の教科書 4』付録A。AIに組み込みのコードを書かせたら、上から順に確かめてください。

仕組みを選ぶ（第2章）

- ☐ 返事をまとめて受け取れば足りる機能なら、コアのAIクライアントを使っている
- ☐ `function_exists` と `wp_supports_ai()` で、AIを使えるサイトかを確認している
- ☐ `is_supported_for_text_generation()` で、使える接続先があるかを確認している
- ☐ 7.0以降が必要なら、プラグインヘッダーに `Requires at least: 7.0` を書いた
- ☐ 使う理由の無い設定（ばらつきの設定など）を足していない

受け口と上限（第5章）

- ☐ 受け口で、Nonceと権限（または公開する理由）を確認している
- ☐ 送る前の確かめ（長さ、不正の対策、回数）を、1か所にまとめている
- ☐ 回数の上限を、時刻で区切ったキーで数えている
- ☐ 利用者のIPを、信頼できる経路のときだけヘッダーから読んでいる
- ☐ 月の上限で、費用の歯止めをかけている
- ☐ 答えを使い回すなら、同じ聞き方のときだけにしている

APIキー（第3章）

- ☐ キーは、できるだけコネクタに任せ、プラグインで持たない
- ☐ 持つなら、画面の入力欄の `value` にキーを入れない
- ☐ キーをURLのクエリに入れていない
- ☐ キーをJavaScriptに渡していない
- ☐ キーや利用者の入力を、ログに書いていない

少しずつ返す（第6章）

- ☐ 少しずつ返す受け口でも、まとめて返す受け口と同じ確かめを通して
- ☐ サーバーの貯め込み対策（詰め物、ヘッダー）を入れ、実際の環境で測った
- ☐ 途中で失敗したときに、まとめて返す受け口へ切り替えられる

呼び出し（第4章）

- ☐ 待ち時間の上限（`timeout`）を、AIの返事に合わせて長くしている
- ☐ 返事の長さの上限に、考える過程の分の余裕がある
- ☐ 失敗を、認証・回数の上限・提供元の不調などに分け、画面の言葉に直している
- ☐ 返事の形をJSONで決め、読み取れないときの扱いがある

出力（第7章）

- ☐ AIの返事を、形・長さを確認、サニタイズしてから使っている
- ☐ 画面に出す直前に、エスケープしている
- ☐ 根拠を渡して答えさせ、答えられないときの道がある
- ☐ AIの出力で、保存・公開・削除などの強い操作をしていない
- ☐ 会話を記録するなら、期限を決めて消し、記録と外部への送信を知らせている

移行と公開（第8章、3巻）

- ☐ 移す範囲を、AIを呼ぶところと設定に絞った
- ☐ 保存済みの古い設定が、新しい作りとぶつからない
- ☐ 古いAPIキーを消す手順を用意した
- ☐ 公式ディレクトリに出すなら、`readme.txt`に外部サービスへの送信と規約へのリンクを書いた