

第4回 安心安全なAIの使い方

- ・ PayPay購買データの利用を見直す
- ・ AIにこの質問はしない
- ・ 最新のAI脅威をご紹介

2026年9月26日（土） 10:30–11:30
主催：小林 正和



安全
設定

生成

防御

本日のテーマ

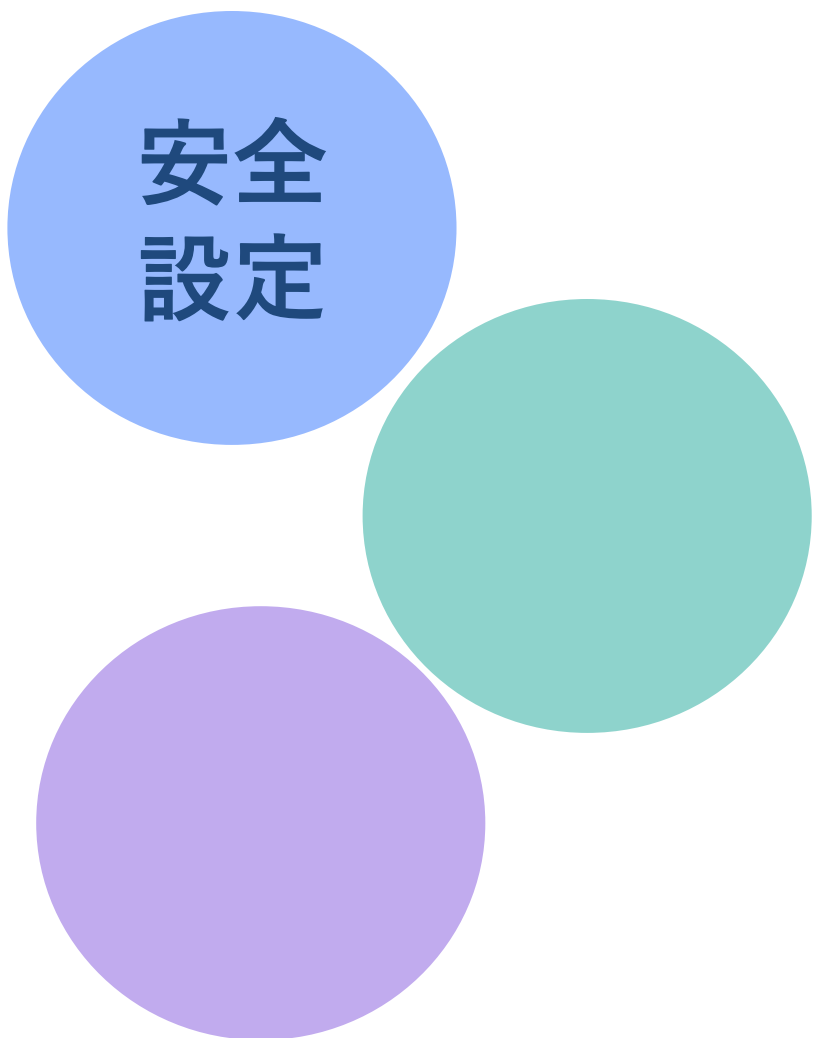
- 1 **PayPay購買データの提供設定を見直す** 買い物履歴、AIに分析されている？
- 2 **AIにこの質問はしない** 通常チャットとの違いについて
- 3 **最新のAI脅威をご紹介します** 国内外で流行している新しい手法を紹介
- 4 **質問コーナー** 便利な使い方をみんなで共有

難しい専門用語よりも「その場でできる設定」と「安全な使い方」を優先します。

1. 安全設定

PayPay購買データの 提供設定を見直す

— 買い物履歴、AIに分析されている？ —

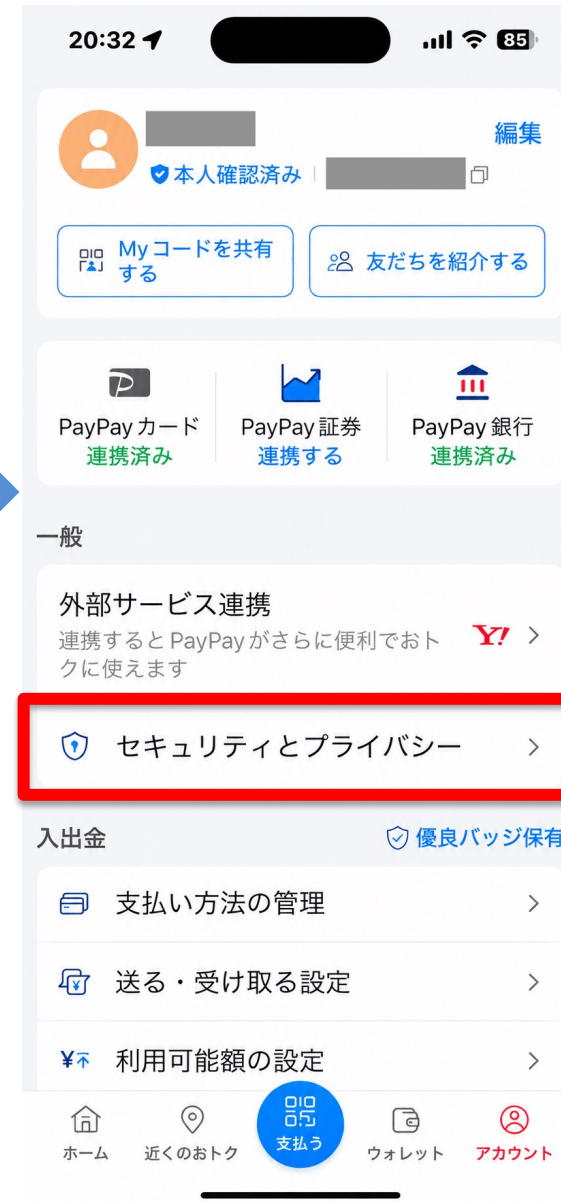
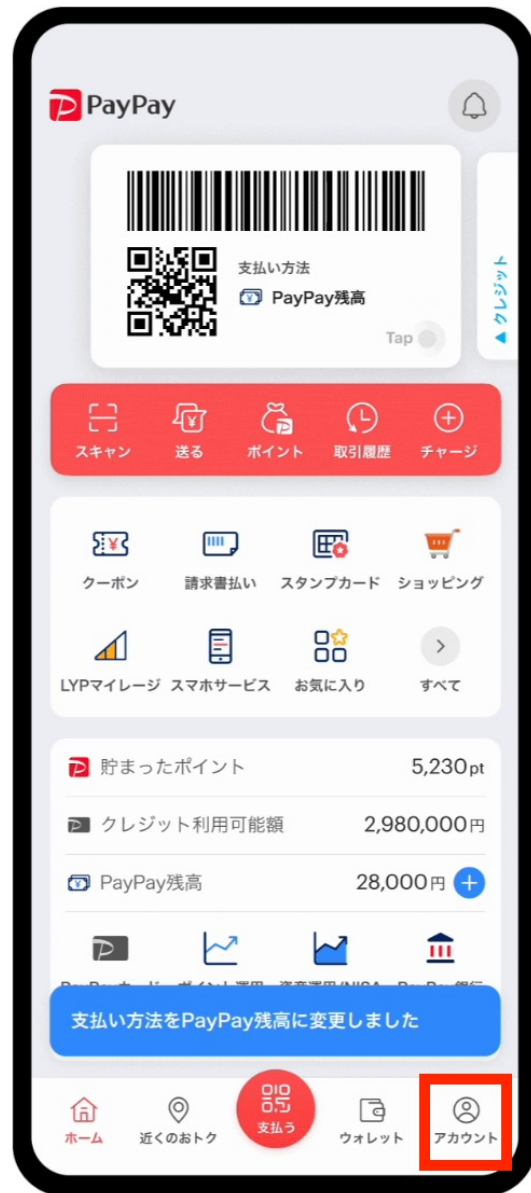


安全
設定

PayPay購買データの利用を見直す



実際に設定してみましよう！①



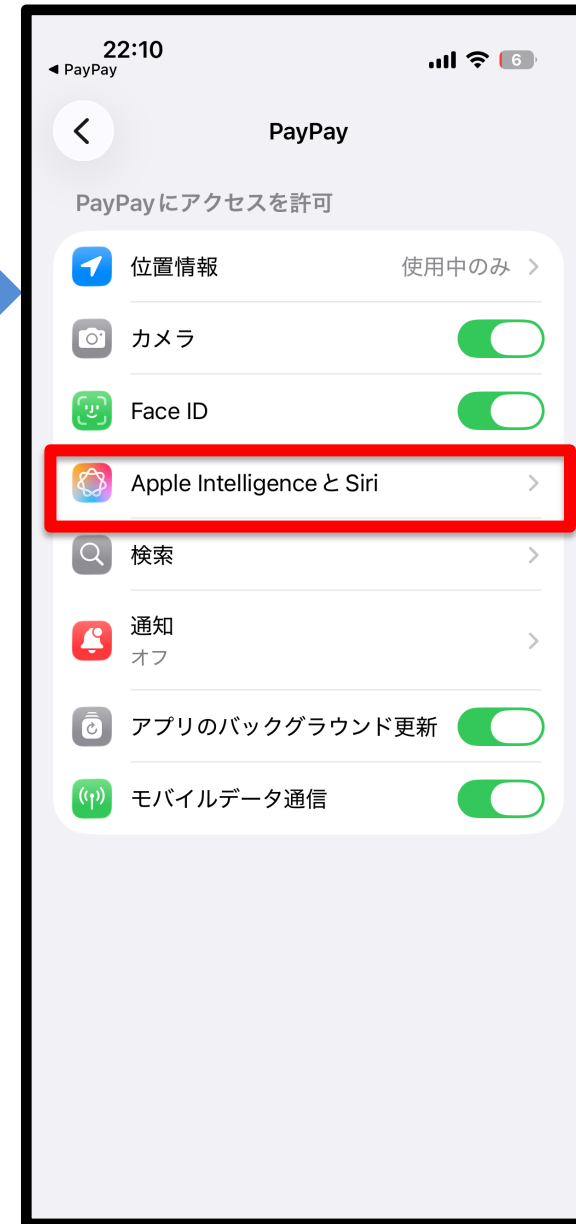
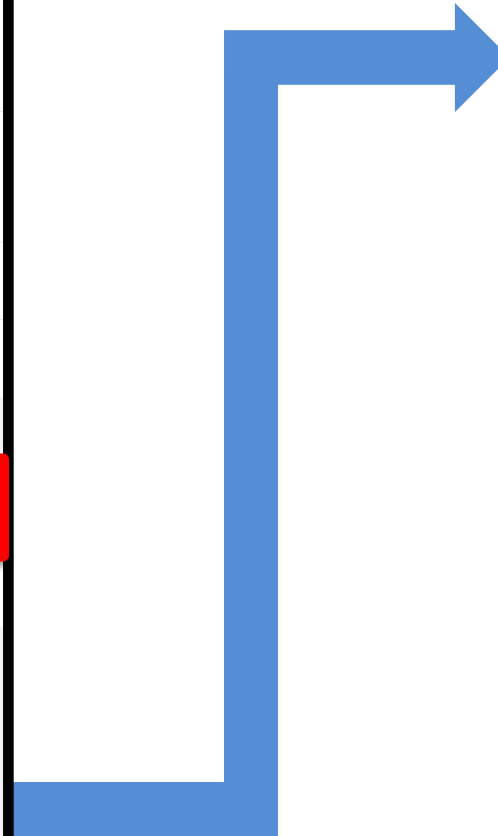
実際に設定してみよう！②



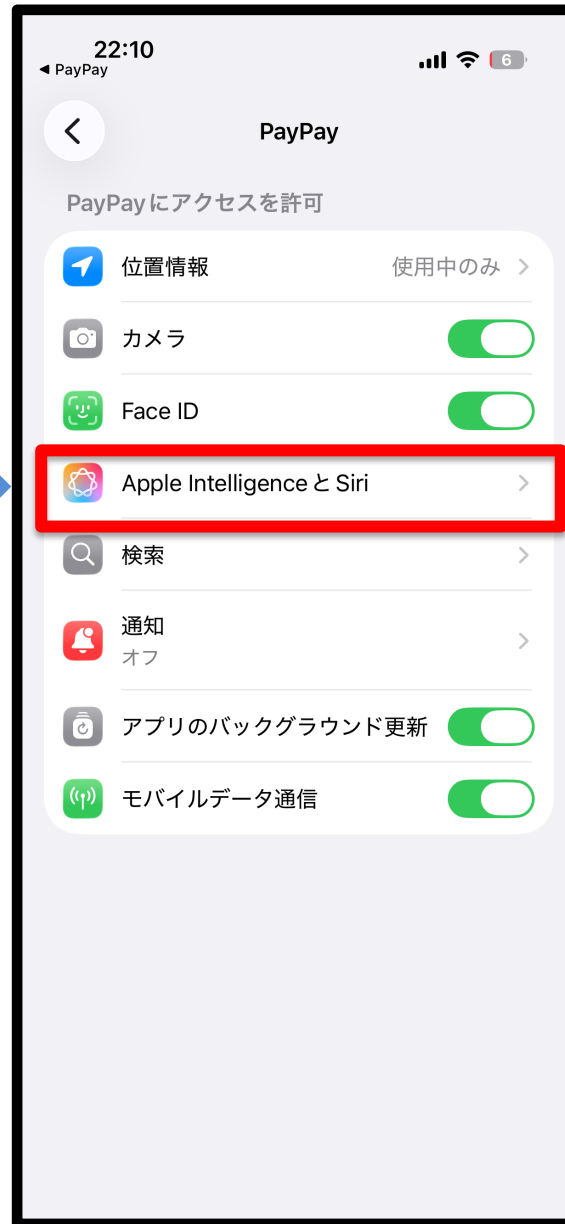
実際に設定してみましょう！③



実際に設定してみましょう！④



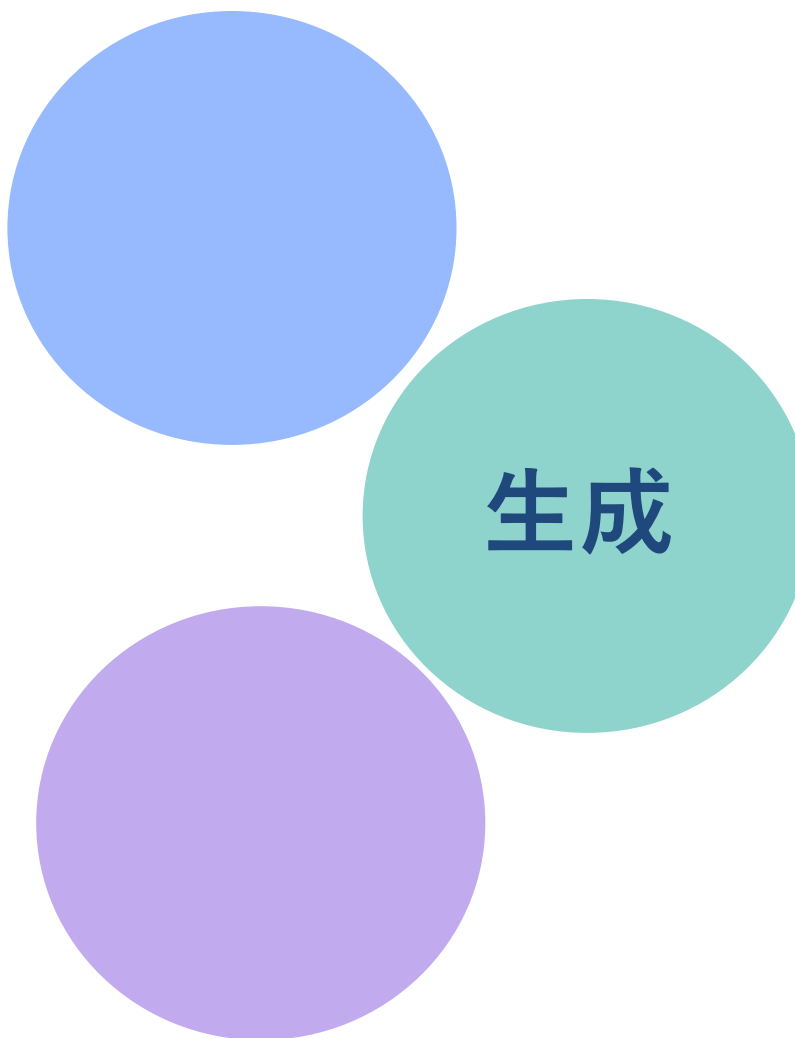
実際に設定してみましょう！⑤



2. 生成

AIにこの質問はしない

—重要判断は必ずご自身で。AIは責任を取らない—



生成

AIは“判断材料係”として使う



ポイント

AIは『最終判断する先生』ではなく、『考える材料を並べる助手』として使う。

AIに任せてよいこと／任せないこと

任せてよいこと

情報の整理や要約
選択肢を挙げさせる
専門家に聞く質問を作成
メリット・デメリットの比較
文章を分かりやすく言い換える

AIだけに任せないこと

診断・治療判断
法的な結論
投資の売買判断
税務申告の最終確定
高額契約・緊急時の判断

例1：医療相談 — 診断ではなく準備に使う

危険な聞き方

胸が痛いけど病院に行かなくて大丈夫？
この薬を飲んでも絶対安全？
この症状は何の病気？

安全な聞き方

病院で説明するために、症状を整理して
医師に聞くべき質問を作って
一般的な副作用を調べる時の確認点を教えて

ポイント 症状の最終判断は医師へ。AIは“受診前のメモ作り”に使う。

例2：法律・税金・投資 — 断定回答に注意

法律

契約書は絶対安全？

→ 確認すべき条項を整理

税金

税額は絶対この金額？

→ 必要書類と確認項目を整理

投資

この株を買うべき？

→ 判断材料とリスクを整理

共通ルール AIは『資料整理・質問づくり』まで。最終判断は人間と専門家で行う。

クイズ：AIに聞いてよい？ 決めさせてよい？

風邪薬の一般的な副作用を教えて

OK：一般情報

胸が痛いけど病院へ行かなくて大丈夫？

NG：緊急判断

契約書の難しい言葉をやさしく説明して

OK：要約

この契約は絶対に安全？

NG：法的結論

この株の決算資料を要約して

OK：整理

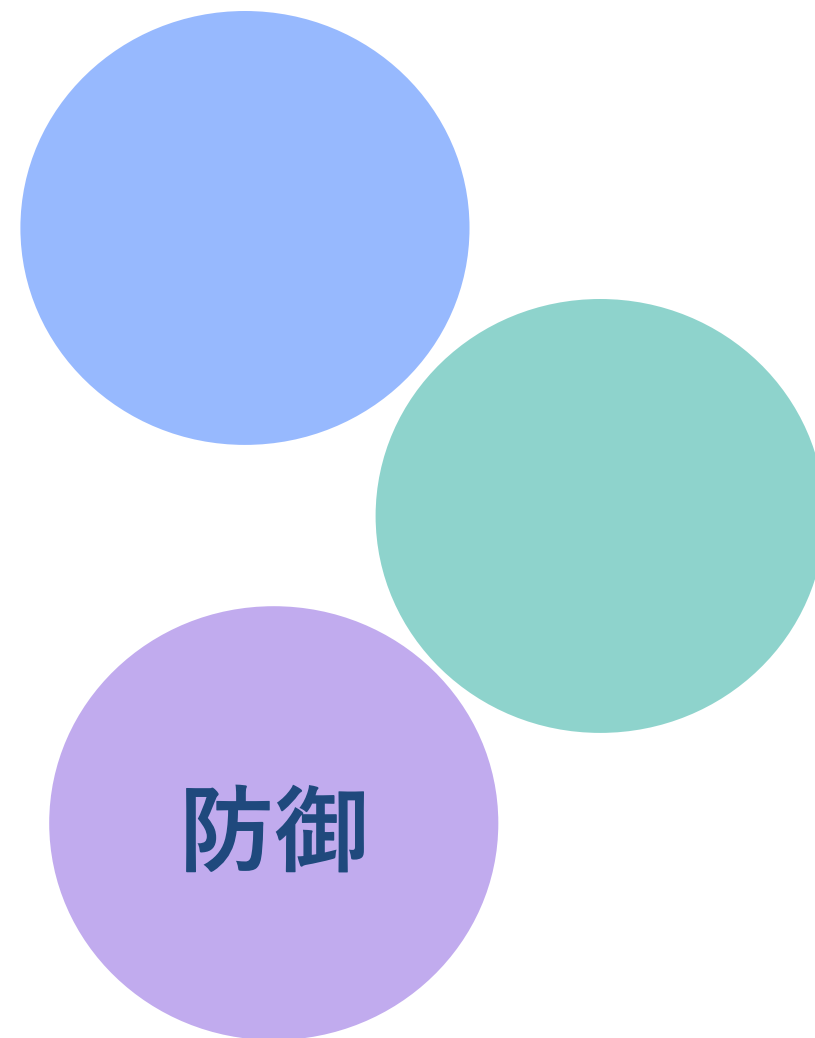
明日100万円分買うべき？

NG：投資判断

2. 防御

最新のAI脅威をご紹介します

—国内外で流行している新しい手法を紹介—



本人になりすましたAIが株式会社KOWROの面接を受けにきた事例



質問コーナー

今日の内容で不安なこと・AIへの聞き方・設定の詳細について
遠慮なくご質問ください。

参考資料

- OpenAI Help Center : ChatGPT can make mistakes / Data Controls / Projects
- Google Help : Gemini Apps Privacy / Activity / Connected apps
- Microsoft Support : Copilot privacy and conversation history
- 消費者庁・金融庁・国税庁などの公式情報は、実際の判断時に確認してください
- ※ 本資料は初心者向け講習用に、重要判断をAIだけに任せないための考え方に絞って説明しています。