

第3回 安心安全なAIの使い方

- ・ AIへの入力を避けるべき情報
- ・ ChatGPTプロジェクト機能
- ・ 最新フィッシングから身を守る

2026年8月16日（日） 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 AI入力とプライバシー

どこまでが個人情報？

2 ChatGPTのプロジェクト機能

通常チャットとの違いについて

3 最新AIフィッシング手法

国内外で流行している新しい手法を学ぶ

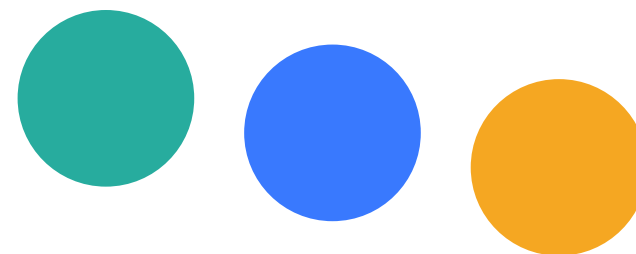
4 質問コーナー

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

AI入力とプライバシー



— PII・非PII・要配慮個人情報・組み合わせで特定される情報 —

AI入力とプライバシー

1

PIIとは何か？

2

非PII情報

3

組み合わせで特定される情報たち

**【AIに入力して良い情報・避けるべき情報・ぼかして入力すべき情報】
区別できるようになりましょう。**

個人情報的重要度ピラミッド

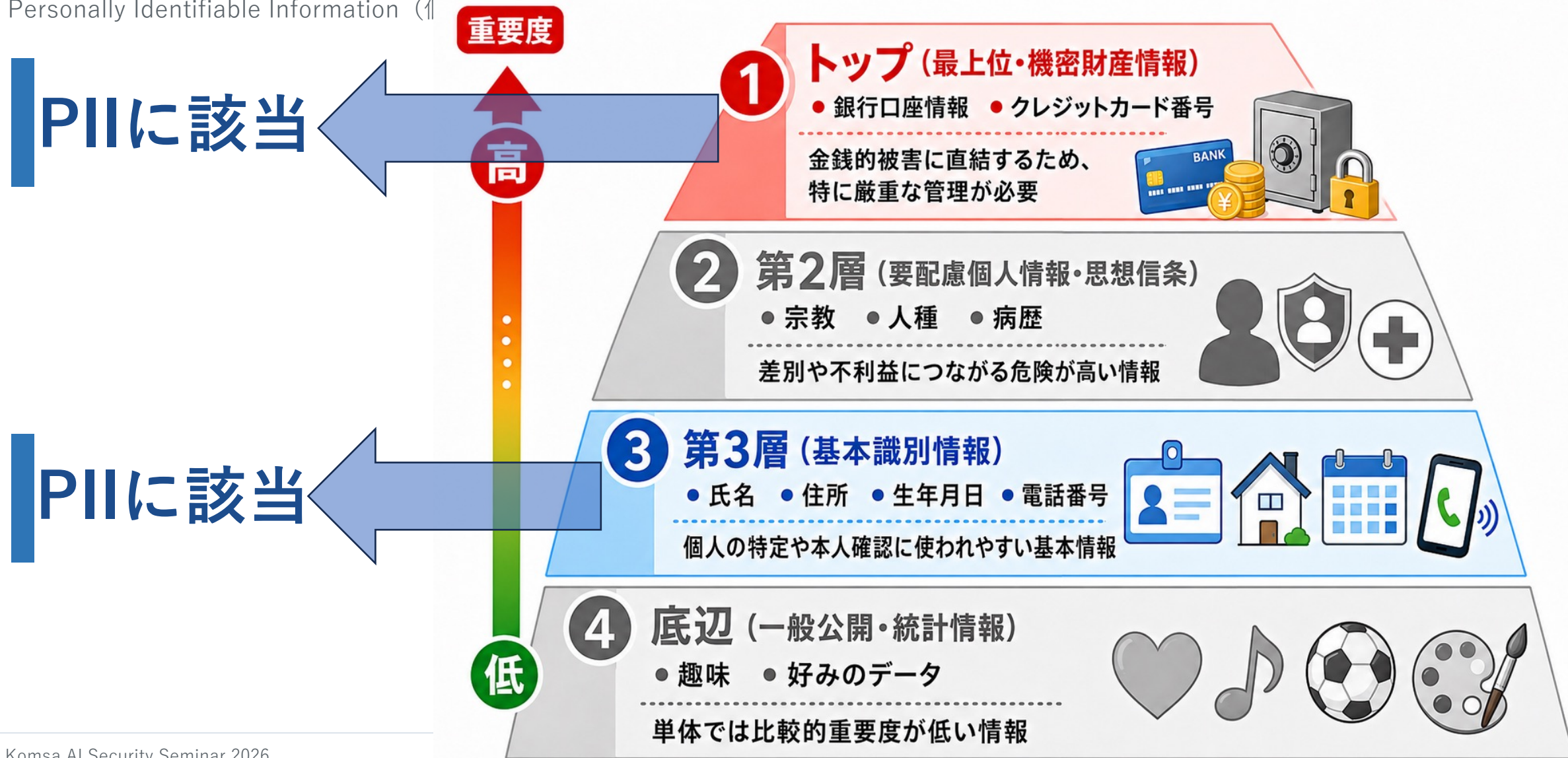
PIIとは何か？



AI入力とプライバシー

Personally Identifiable Information (PII)

個人情報的重要度ピラミッド



AI入力とプライバシー

Personally Identifiable Information (個人を識別できる情報)

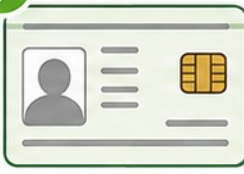
利便性と**セキュリティ**は反比例する



AI入力とプライバシー

Personally Identifiable Information (個人を識別できる情報)

AIに入力注意！ 個人情報の例

 1 氏名	 2 住所	 3 電話番号	 4 メールアドレス	 5 生年月日	 6 顔写真	 7 マイナンバー
 8 口座情報	 9 クレジットカード 情報	 10 ログインID	 11 パスワード	 12 認証コード	 13 本人確認書類	



そのまま入力せず、ぼかす・置き換える



AI入力とプライバシー

Personally Identifiable Information (個人を識別できる情報)

なりすまし・詐欺の材料になる

一度送ると完全に回収できない場合がある

AIサービスによっては、**会話履歴の保存、ログ、安全対策、サービス改善などのために入力情報が一定期間保持されることがあります**。各AIモデルで設定を推奨。(セミナー第一回資料を参照)

別の情報と結び付くと価値が高くなる

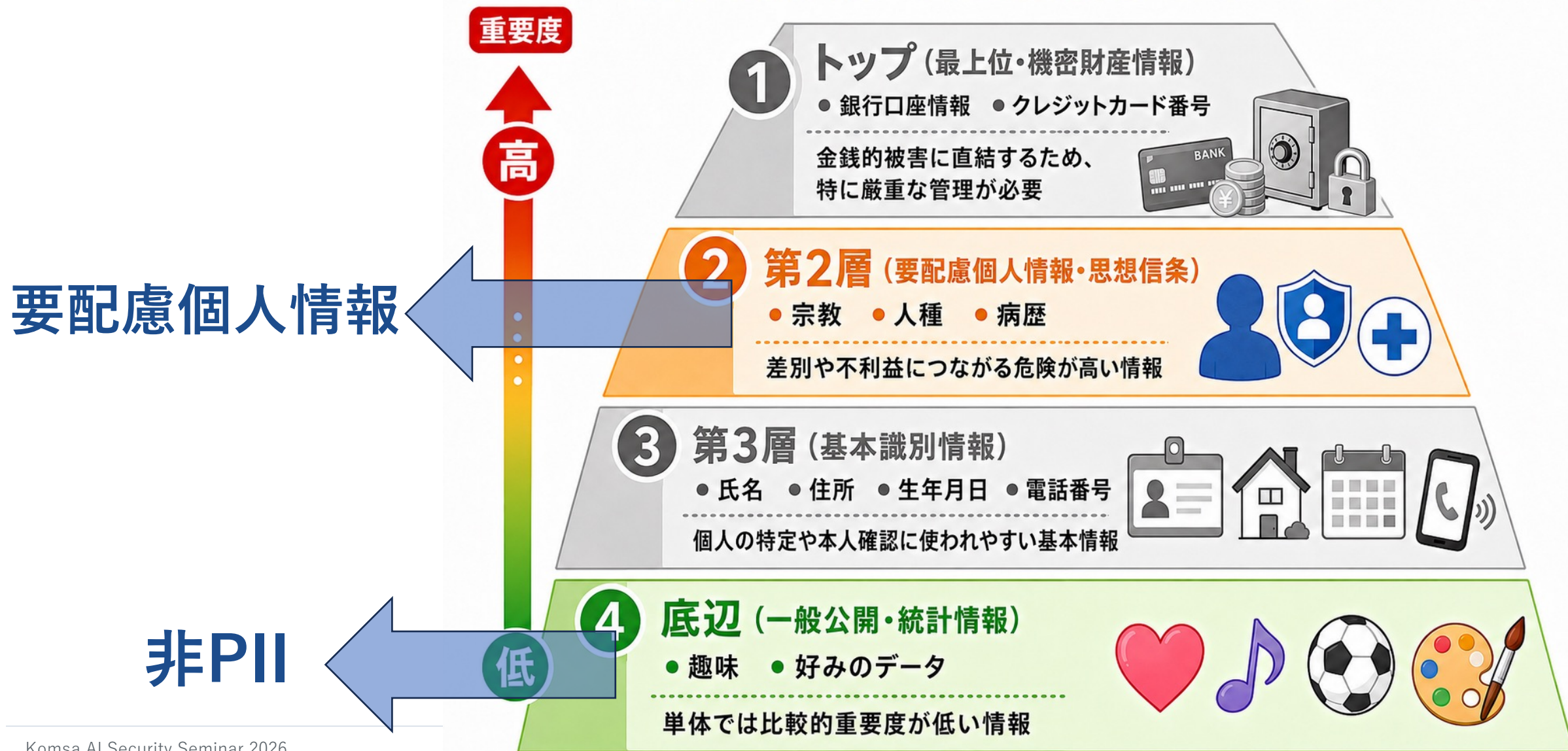
例) 氏名 + 生年月日 + 勤務先 + 最寄駅

自分だけでなく他人の情報まで漏らす可能性がある

例) 市役所に提出する書類

AIにメール、PDF、契約書、名簿などをそのまま貼り付けると、顧客、家族、同僚の氏名・住所・電話番号まで入力してしまうことがあります。

個人情報重要度ピラミッド



AI入力とプライバシー

単体では個人を特定しにくいですが、扱いに注意が必要です

安心して
AIに入力できる
情報の例



非PII (個人を特定できない情報) の代表的な例

単体では個人を特定できず、一般公開されているような情報

これらの情報は
単体では誰の情報か
特定できません



天気



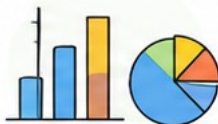
例: 今日の気温、
週間天気予報

ニュース・出来事



例: 世界のニュース、
スポーツの結果

統計・データ



例: 日本の人口、
経済成長率

知識・一般常識



例: 歴史の事実、
科学の原理

レシピ・料理方法



例: カレーの作り方、
パスタのレシピ

趣味に関する一般情報



例: サッカーのルール、
ギターの練習方法

製品の一般情報



例: PCのスペック比較、
スマホの機能紹介

場所の一般情報



例: 観光地の紹介、
地域の特徴

会社・組織の一般情報



例: 企業の沿革、
サービスの説明

利用規約・契約の一般情報



例: 利用規約の要点、
契約の一般的な仕組み

コード・プログラム(公開情報)



例: オープンソースのコード、
プログラミングの質問

学習・スキルに関する一般情報



例: 勉強のコツ、
タイムマネジメント方法

エンタメ・文化の一般情報



例: 映画のあらすじ、
音楽のジャンル解説

FAQ・ヘルプ情報



例: ソフトの使い方、
よくある質問

架空のシナリオ・例え話



例: もし〇〇だったら?
のシミュレーション

匿名・集合データ



例: アンケートの集計結果、
匿名化されたデータ

⚠ 注意ポイント

- 組み合わせると個人が特定できる可能性がある情報はPIIになる場合があります。
- 可能な限り、**具体的な固有名詞、日付、場所、数字**などは**ぼかして入力**しましょう。



非PIIの情報をうまく活用しよう!

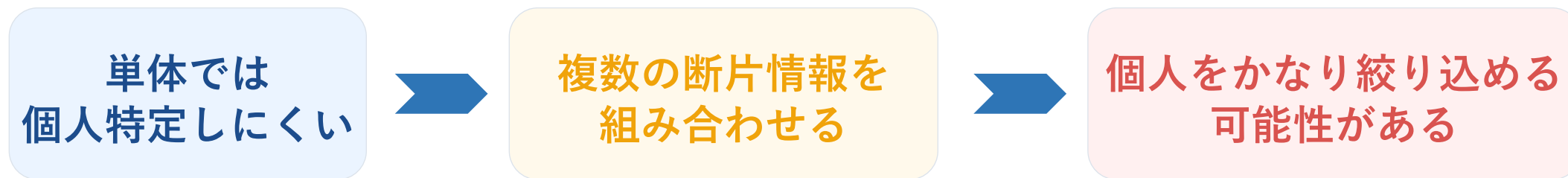
AI は、一般的な質問や知識提供、アイデア出し、情報整理などにとっても役立ちます。
安心して活用するために、入力する情報の性質を意識することが大切です。



AI入力とプライバシー

非PIIでも、複数そろえば『その人らしさ』が強くなります

組み合わせで個人を特定できる情報



ポイント：『直接PIIではない＝安全』ではありません。場所・行動・仕事・趣味などの断片は、つながると個人を指し示すことがあります。

AI入力とプライバシー

組み合わせ例：こんな断片でも個人に近づく

例1：場所の組み合わせ

自宅の最寄り駅
会社の最寄り駅
会社帰りによく寄る場所
→ 生活圏や通勤動線が見えやすくなる
→ 知人には『この人かも』と気づかれやすい

例2：仕事と生活の組み合わせ

勤務業界（例：医療、教育、IT）
勤務時間帯
住んでいるエリア
→ 対象者の候補がかなり絞られる
→ 詐欺師が自然な会話を作りやすくなる

例3：趣味と行動の組み合わせ

趣味・推し活の内容
よく行く店やイベント
SNSに載せた日時や頻度
→ 行動パターンが見えやすい
→ なりすましや勧誘に使われやすい

AI入力とプライバシー

① 絶対に入力しない

パスワード類、スマホに届く認証コード、クレジットカード番号、銀行口座番号、マイナンバー

② 原則として入力しない

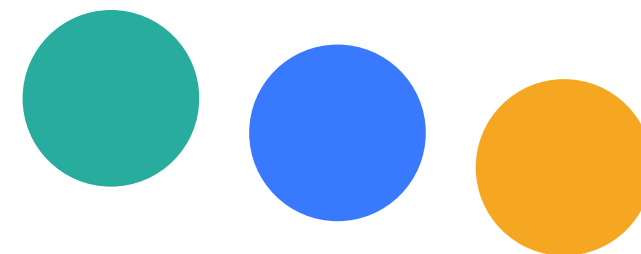
氏名、住所、電話番号、メール、生年月日、顔写真、本人確認書類

③ ぼかして入力する

最寄り駅、勤務先、居住地域、行動パターン、趣味、よく行く場所

2. 活用方法

ChatGPTのプロジェクト機能



その会話内容、将来的にも使いそう？

ChatGPTのプロジェクト機能



通常チャット

その場での会話・単発のやり取りに最適



- ちょっと質問したい時
- 単発の相談
- その場で終わる作業



- 会話ごとに分かれる
- テーマが混ざりやすい



- 毎回説明し直すことが多い



- 必要な時に都度アップロード



- 旅行の相談
- メール文章の作成
- 簡単な調べもの



使い分けのコツ

① すぐ終わる相談
→ 通常チャット

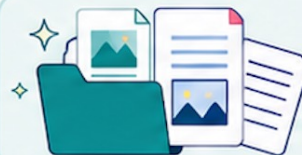
② 同じテーマを続ける
→ プロジェクト機能

③ 資料・メモ・会話を
まとめたい
→ プロジェクト機能



覚え方:

通常チャットはその場の会話、
プロジェクト機能はテーマごとの作業部屋



プロジェクト機能

◆ テーマごとの作業を整理・継続しやすい

- 長く続ける作業
- 同じテーマを深める作業
- 資料作成や企画の継続



- 関連チャットやファイルを1か所に整理
- テーマごとに管理しやすい



- プロジェクトの指示をまとめて持てる
- 毎回説明する手間を減らせる



- 参考資料や下書きをまとめて置ける



- セミナー準備
- 議事録の整理
- 学習ノート
- 長期の企画管理



ChatGPTのプロジェクト機能

関連するチャット・ファイル・指示を1か所にまとめる『作業スペース』



1. 文脈が続く

前回の続きから
始めやすい



2. 資料をまとめられる

PDF・画像・表を
一緒に使える



3. 指示を固定できる

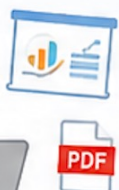
文体や目的を
ぶらさない



4. 繰り返し作業に強い

長期案件・
定例業務に向く

こんな場面で
役立つ！



講習資料づくり

スライド案・原稿・
参考資料をまとめて
効率的に作成



趣味の情報整理

調べた情報やメモを
整理して、自分だけの
知識ベースに



仕事の継続案件

議事録・資料・ToDoを
一元管理して、プロジェクト
をスムーズに推進

ChatGPTのプロジェクト機能

ChatGPT Plus

🔍 📄

📄 新しいチャット

📖 ライブラリ

🕒 スケジュール

🔗 プラグイン

⋮ さらに表示

📌 ピン留め

🕒 Top AI news: Karpathy joins /

🕒 AIセキュリティニュース配信

📁 プロジェクト ▾ ⋮ +

📁 横須賀・ライフスタイル

📄 レストランページ

📁 AI講習

📄 AI講習会予約ページ

📄 AI講習集客方法

 Masakazu Kobayashi
Plus

👤

ChatWork

🔄

今日は何をしましょうか？

+ ChatGPT に質問

高い ▾ 🎤 🎧

🕒 Alert me when material AI security stories break worldwide

🌈 やることを整理する

📧 フォローアップメールを下書き

ChatGPTのプロジェクト機能

プロジェクトを作成する

×

プロジェクト名

 横須賀観光ページ

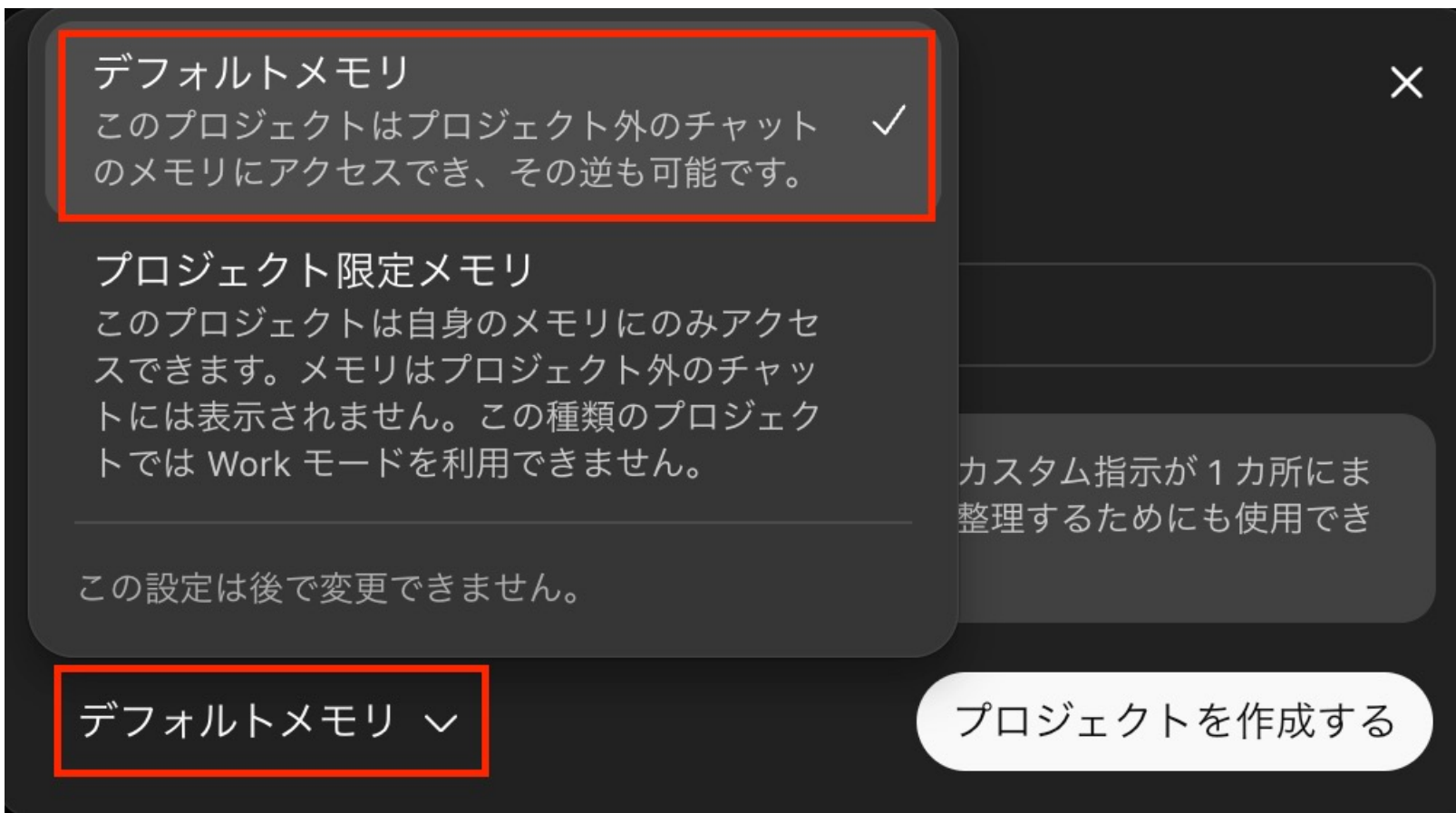


プロジェクトを使用すると、チャット、ファイル、カスタム指示が1カ所にまとまります。これは進行中の作業にも、単に物事を整理するためにも使用できます。

デフォルトメモリ ▼

プロジェクトを作成する

ChatGPTのプロジェクト機能



私がい実際に日常的に使用しているお題のご紹介

テーマを1つ選び、AIに相談します。

①毎日の献立・会社帰りの買い物リスト

家にある食材／調理方法／「今日何作る？」

②毎日のニュース整理

AIセキュリティ/AI/趣味など

③家電・家具の買い替え検討

予算/年式/欲しい機能/サイズ・容量

完成形：あなた専用の「趣味ニュースまとめ」プロンプト

📁 デフォルトメモリ と プロジェクト限定メモリの違い

💬 プロジェクトの情報を、どこまで他の会話とつなげるかの設定

デフォルトメモリ



- ✓ プロジェクト外のチャットや保存メモリも参照できる
- ✓ このプロジェクトの文脈が、外の会話にも活かることがある
- ✓ 過去の会話を活かして、横断的に使いたい人向け



たとえば：

家全体の資料を見ながら使う

“作業部屋”



プロジェクト限定メモリ



- ✓ このプロジェクト内の会話だけを参照する
- ✓ プロジェクト外のチャットにはアクセスしない
- ✓ 仕事・顧客案件・機密テーマを分けたい人向け



たとえば：

その部屋の資料だけで作業する

“独立した会議室”



使い分けの目安

おすすめ：デフォルトメモリ



学習ノート



趣味の情報整理



長期的な企画

おすすめ：プロジェクト限定メモリ



社内資料



顧客対応



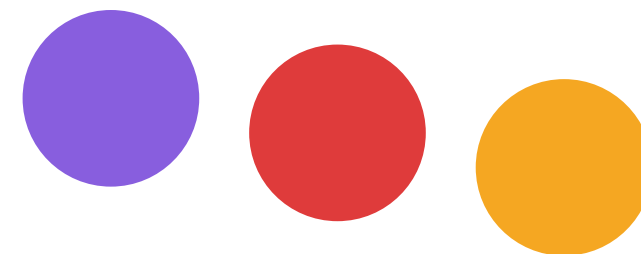
機密性の高い作業



※ この設定はプロジェクト作成後に変更できません

3. 最新AIフィッシング

最新AIフィッシング手法



自立型AI詐欺

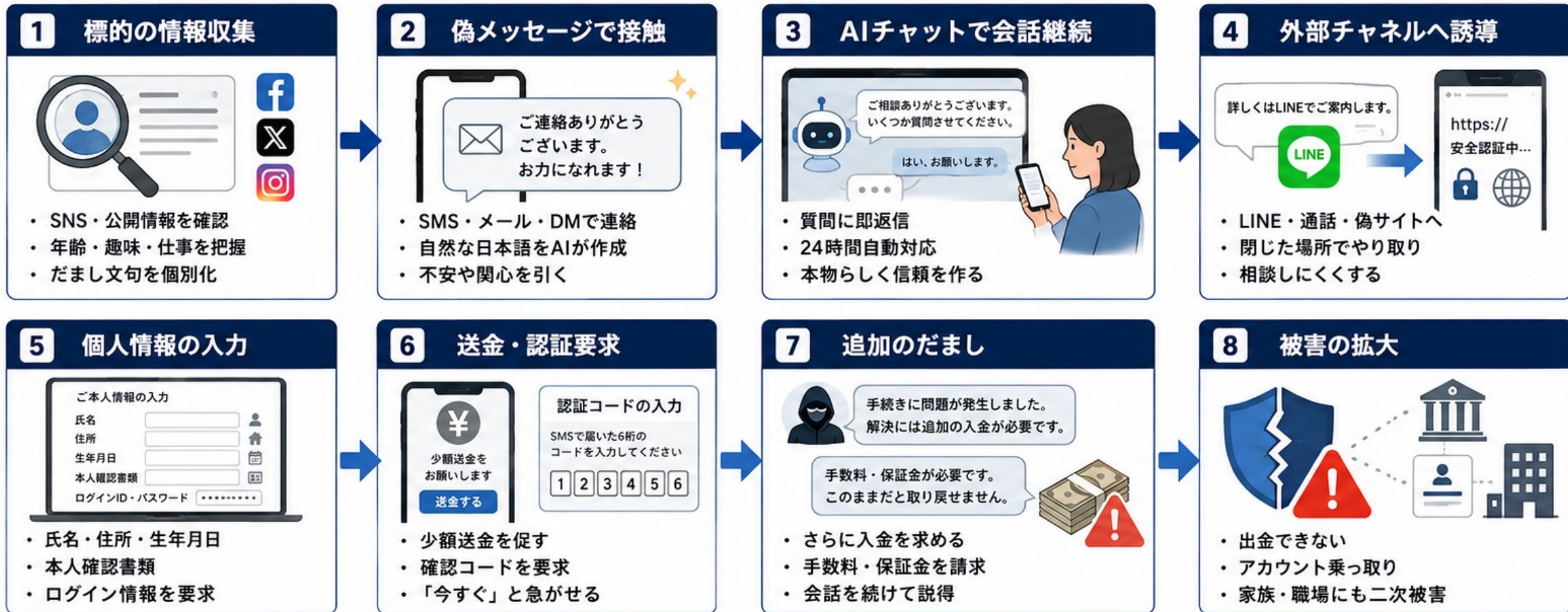
AI自動化された超個別狙いのフィッシング手法

最新AIフィッシング手法

令和時代はSNSで情報収集

Agentic Fraud (自律型AI詐欺)の流れ

AIが会話・誘導・なりすましを自動化する詐欺の典型パターン



Agentic Fraudの特徴

- AIが会話を自動化
- 相手ごとに内容を変える
- SNS・SMS・通話を連携
- 大量の相手に同時対応



対策のポイント

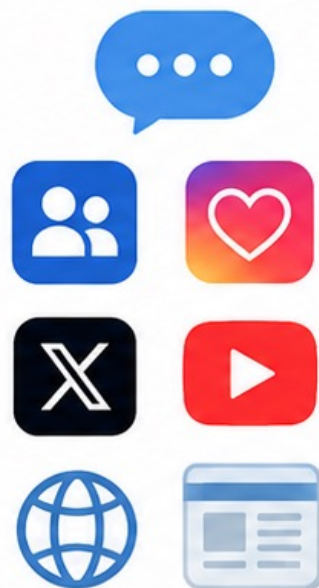
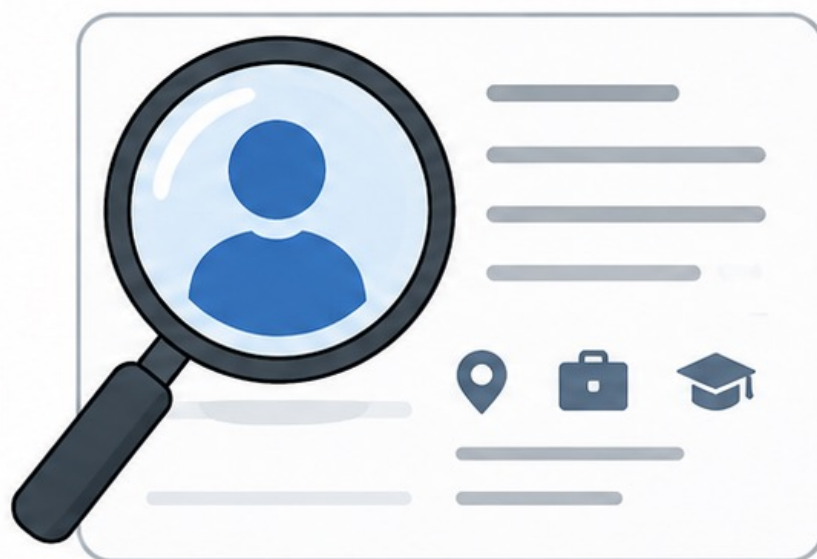
- リンクを押す前に公式確認
- 認証コードは教えない
- 送金を一人で決めない
- SNSの公開情報を見直す
- 二要素認証を使う
- 不安な時は家族・職場へ相談

Agentic Fraud (自律型AI詐欺)の流れ

AIが会話・誘導・なりすましを自動化する詐欺の典型パターン

STEP 1 / 8

1 標的の情報収集



- SNS・公開情報を確認
- 年齢・趣味・仕事を把握
- だまし文句を個別化



攻撃者はまず、公開情報やSNS投稿から相手の人物像を集めます。
ここで得た情報が、その後の自然な詐欺メッセージ作成に使われます。

Agentic Fraud (自律型AI詐欺) の流れ

AIが会話・誘導・なりすましを自動化する詐欺の典型パターン

STEP 2 / 8

2 偽メッセージで接触



- SMS・メール・DMで連絡
- 自然な日本語をAIが作成
- 不安や関心を引く



攻撃者は、AIで作った自然な文章を使って接触します。
相手に合わせた内容のため、本物らしく見えやすいのが特徴です。

Agentic Fraud (自律型AI詐欺) の流れ

AIが会話・誘導・なりすましを自動化する詐欺の典型パターン

STEP 3 / 8

3 AIチャットで会話継続



- 質問に即返信
- 24時間自動対応
- 本物らしく信頼を作る



返信があると、AIが会話を続けて相手の警戒心を下げます。
自然な受け答えにより、だまされやすい状況を作ります。

Agentic Fraud (自律型AI詐欺)の流れ

AIが会話・誘導・なりすましを自動化する詐欺の典型パターン

STEP 4 / 8

4 外部チャネルへ誘導



- LINE・通話・偽サイトへ
- 閉じた場所でやり取り
- 相談しにくくする



攻撃者は、LINEや通話、偽サイトなど外部チャネルに誘導します。
周囲に相談しにくい環境へ移すのが典型的な手口です。

Agentic Fraud（自律型AI詐欺）の流れ

AIが会話・誘導・なりすましを自動化する詐欺の典型パターン

STEP 5 / 8

5 個人情報を入力

ご本人情報の入力

氏名 

住所 

生年月日 

本人確認書類 

ログインID・パスワード

- 氏名・住所・生年月日
- 本人確認書類
- ログイン情報を要求



相手を信用させた後、個人情報や本人確認情報の入力を求めます。
この段階で、なりすましや二次被害の材料が集められます。

Agentic Fraud (自律型AI詐欺)の流れ

AIが会話・誘導・なりすましを自動化する詐欺の典型パターン

STEP 6 / 8

6 送金・認証要求



- 少額送金を促す
- 確認コードを要求
- 『今すぐ』と急がせる



攻撃者は、少額送金や認証コードの入力を求めて行動させます。
『今すぐ』『急いで』という言葉で冷静な判断を奪うのが特徴です。

Agentic Fraud (自律型AI詐欺)の流れ

AIが会話・誘導・なりすましを自動化する詐欺の典型パターン

STEP 7 / 8

7 追加のだまし



手続きに問題が発生しました。
解決には追加の入金が必要です。

手数料・保証金が必要です。
このままだと取り戻せません。



- さらに入金を求める
- 手数料・保証金を請求
- 会話を続けて説得



一度だまされると、手数料や保証金など別の理由で追加請求が続きます。
会話を継続して、被害を大きくするのがこの段階です。

Agentic Fraud (自律型AI詐欺)の流れ

AIが会話・誘導・なりすましを自動化する詐欺の典型パターン

STEP 8 / 8

8 被害の拡大



- 出金できない
- アカウント乗っ取り
- 家族・職場にも二次被害



最終的には、金銭被害だけでなくアカウント乗っ取りや二次被害に発展します。
被害は本人だけでなく、家族や職場へ広がる可能性があります。

質問コーナー

今日の内容で不安なこと・設定の詳細・AIの便利な使い方について
遠慮なくご質問ください。

参考資料

- Google Terms of Service : 2026年7月30日発効版
- Google Help : Search Services History & Save Media
- Google Account Help : Access & control activity in your account
- Google Gemini Apps Privacy Hub
- OpenAI Help Center : Data Controls / Privacy
- FBI IC3 : Kali365 Phishing-as-a-Service Kit
- Microsoft Learn : Device code flow / authentication security guidance

個人情報データの保存について

<https://support.microsoft.com/en-us/microsoft-copilot/privacy-faq-for-microsoft-copilot>

<https://support.microsoft.com/en-us/microsoft-copilot/conversation-history-in-microsoft-copilot>

<https://support.microsoft.com/en-us/microsoft-copilot/file-upload-in-microsoft-copilot>

<https://privacy.claude.com/en/articles/10023548-how-long-do-you-store-my-data>

<https://privacy.claude.com/en/articles/10023580-is-my-data-used-for-model-training>

<https://support.google.com/gemini/answer/13278892>

<https://support.google.com/gemini/answer/13594961>

<https://help.openai.com/en/articles/8983778-chat-and-file-retention-policies-in-chatgpt>

<https://help.openai.com/en/articles/7730893-data-controls-faq>

<https://help.openai.com/en/articles/8590148-memory-faq>