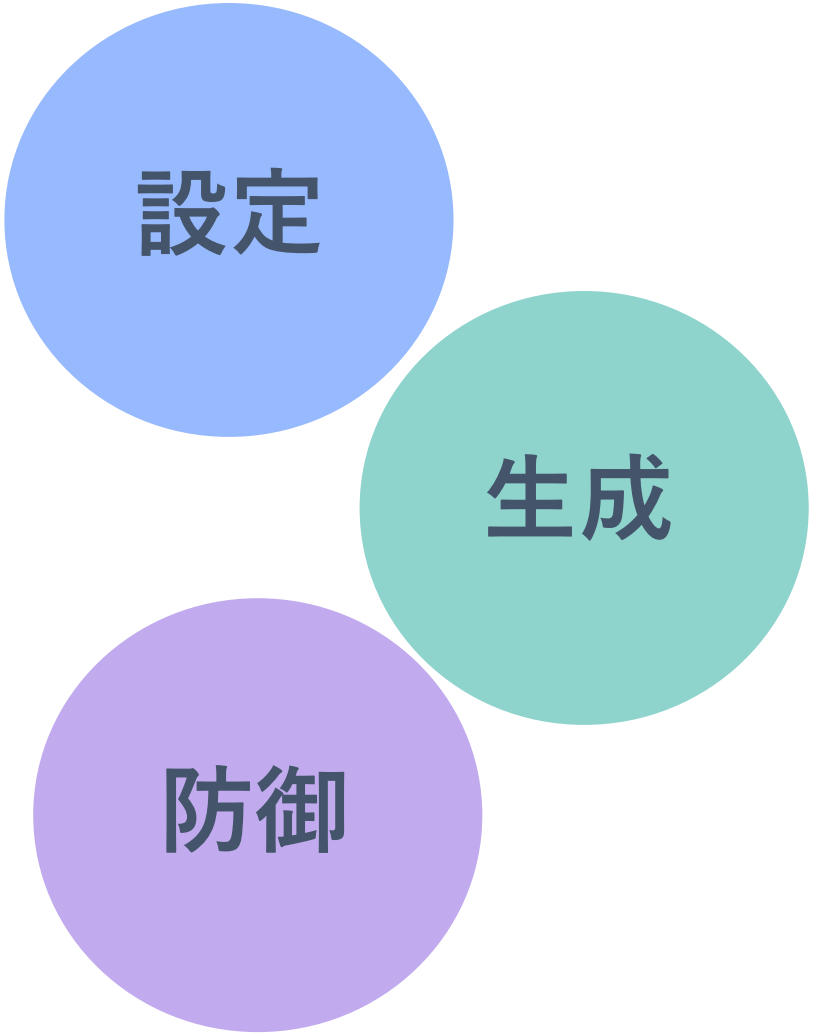
第２回
安心安全なAIの使い方

Google新設定・AI記事生成・最新フィッシングから身を守る



2026年7月19日（日）10:30–11:30
主催：小林 正和

本日の流れ

1. **Googleのセキュリティ設定** — Google新設定とAI学習項目
2. **好きなジャンルの記事をAIで自動生成** — エージェント監視機能の体験作成
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。

今日のゴール

設定

Google・AIアプリの学習利用を確認

活用

ご趣味の情報を自動で集める

防御

AIフィッシングにだまされない

本日のテーマ

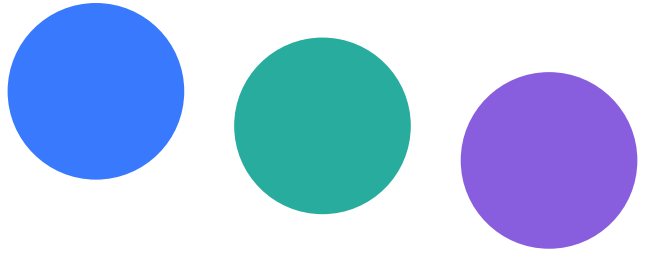
✓ 7月30日までに確認したいGoogle新設定を理解する

✓ AIを安全に使って、趣味の記事収集を自動化する

✓ 最新のAIフィッシングで狙われるポイントを見抜く

1. セキュリティ設定

Googleのセキュリティ設定



Googleの新しいポリシーの回避方法

GoogleがユーザーのAIへ学習利用

スマホを一緒に確認し、個人情報を学習させない準備をします

Googleが取得する履歴内容

・検索サービス
・メディア検索
・個別化設定を見ます。

AIアプリ設定も復習
ChatGPT・Geminiなどで、履歴・学習利用・連携を確認します。

合言葉：入力前に「消す・ぼかす・置き換える」

7月30日までに必要に応じて設定を変更します。
不要な保存・学習利用を避ける設定を行います。

Google新設定：何を確認する？

「Google検索」と「Google画像検索」を中心に設定します

STEP 1

Google検索
テキスト検索履歴
画像検索履歴
Maps・翻訳

STEP 2

Google Drive
メディア保存
画像・音声・動画
・ファイル

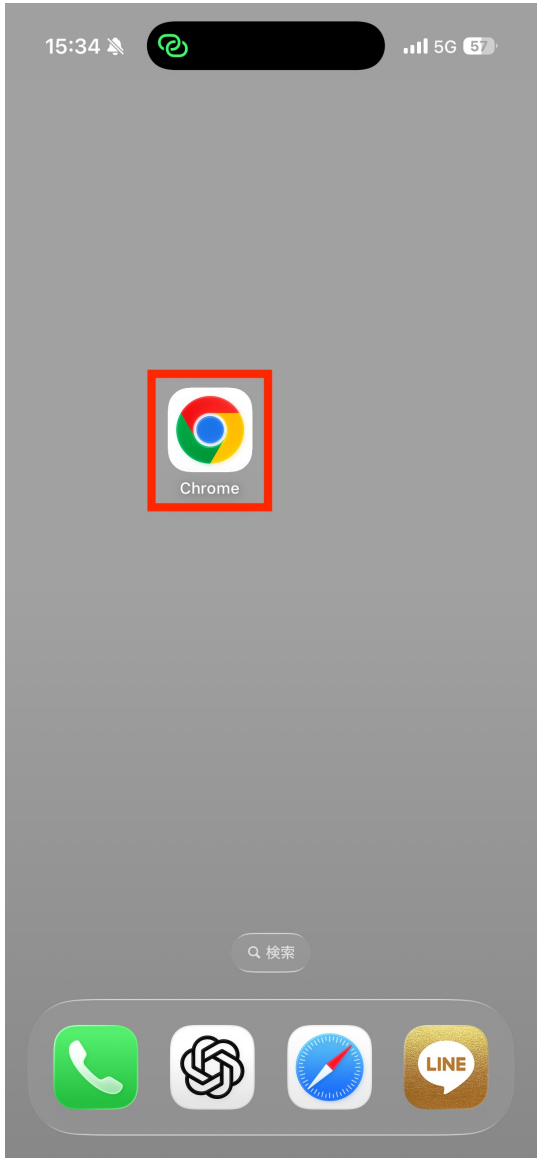
STEP 3

Gemini
生成AIとの
やり取り

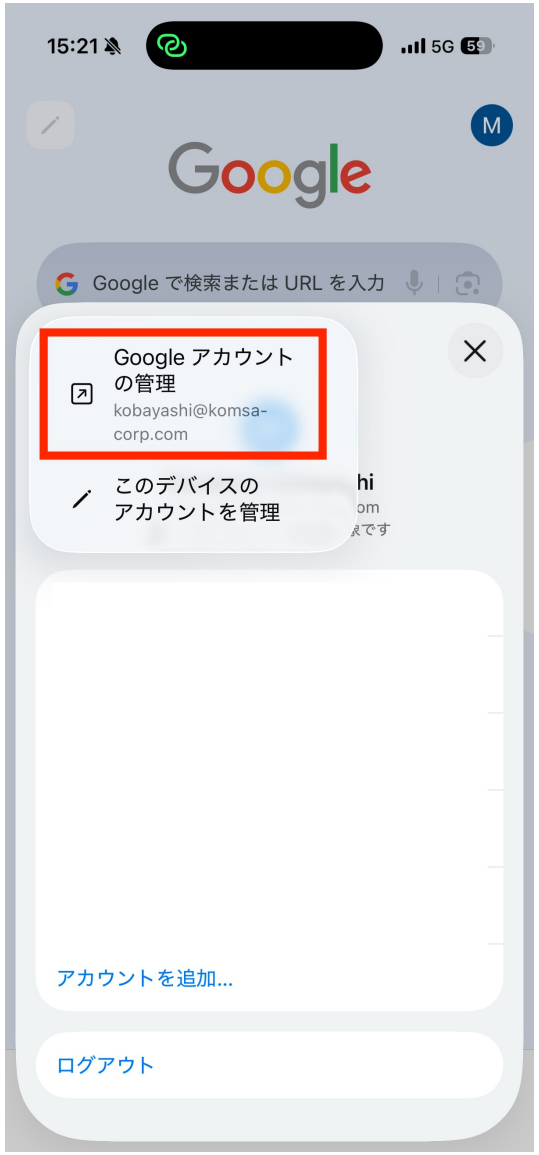
設定するかどうかの考え方：便利さを取るか、保存・学習利用を抑えるかを選ぶ。

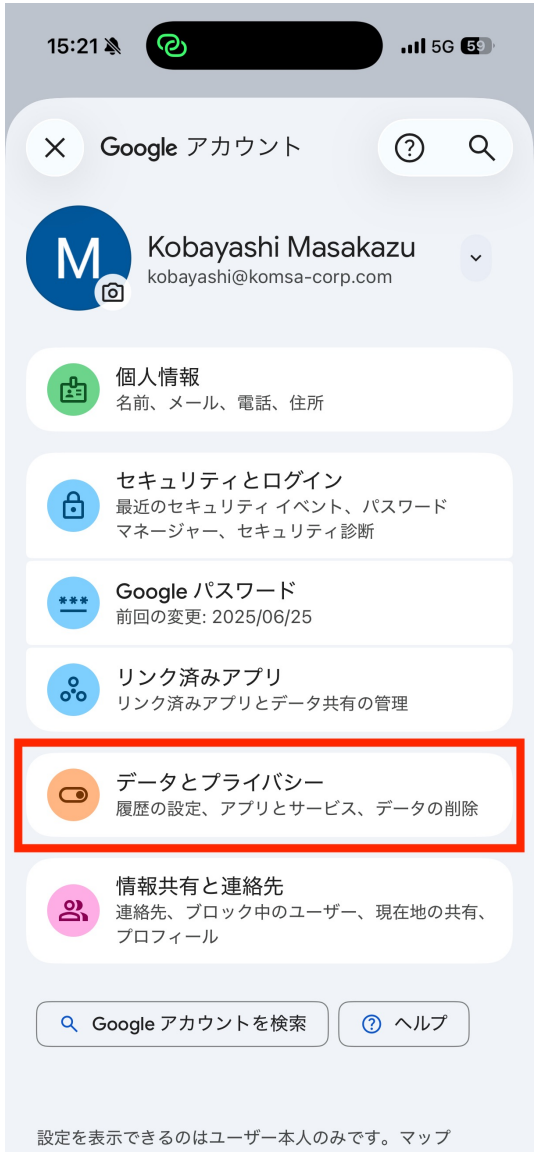
第一回学び：AIに入力する情報は、個人情報を「消す・ぼかす・置き換える」

実際に設定していきましょう①（Chrome）

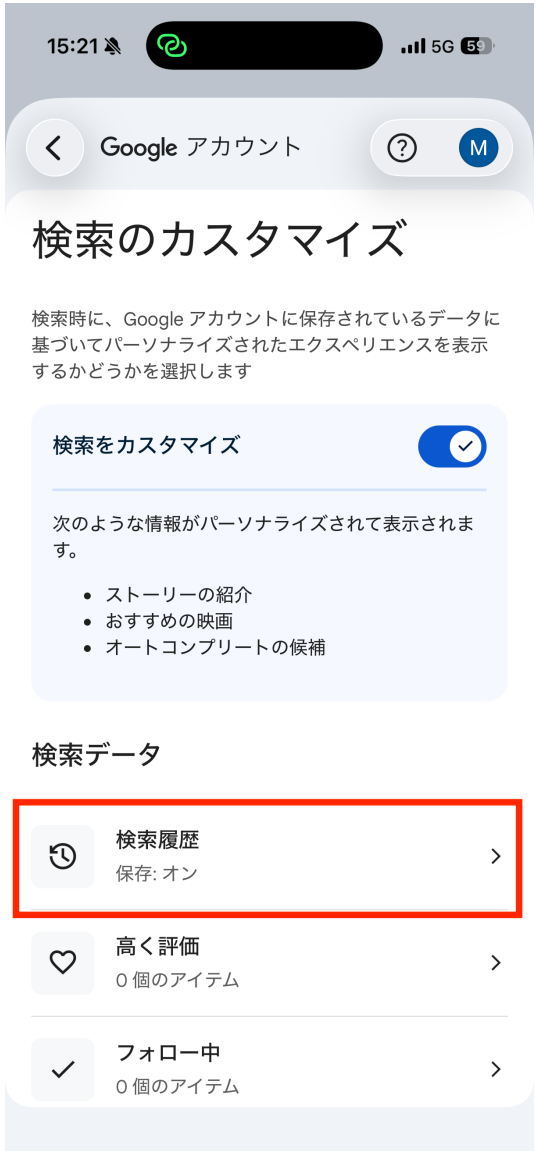


実際に設定していきましょう②（Chrome）

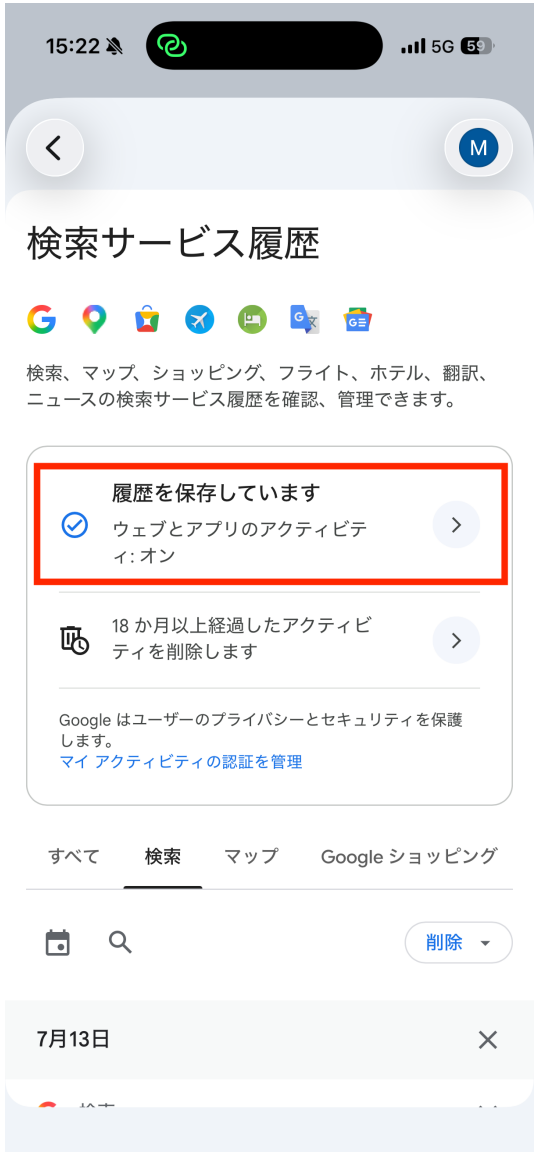




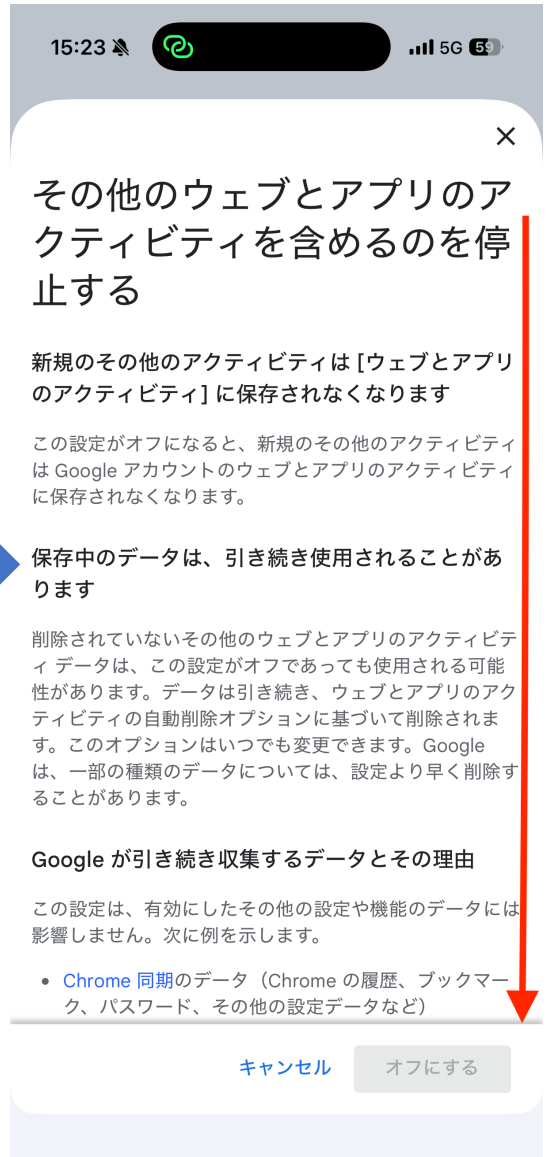
実際に設定していきましょう③（Chrome）



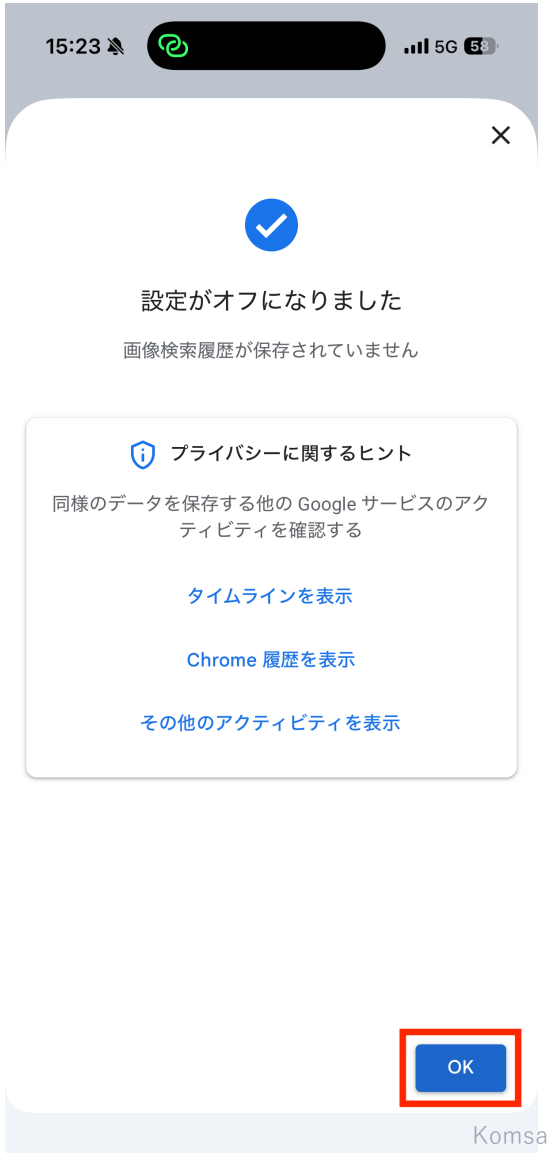
実際に設定していきましょう④（Chrome）



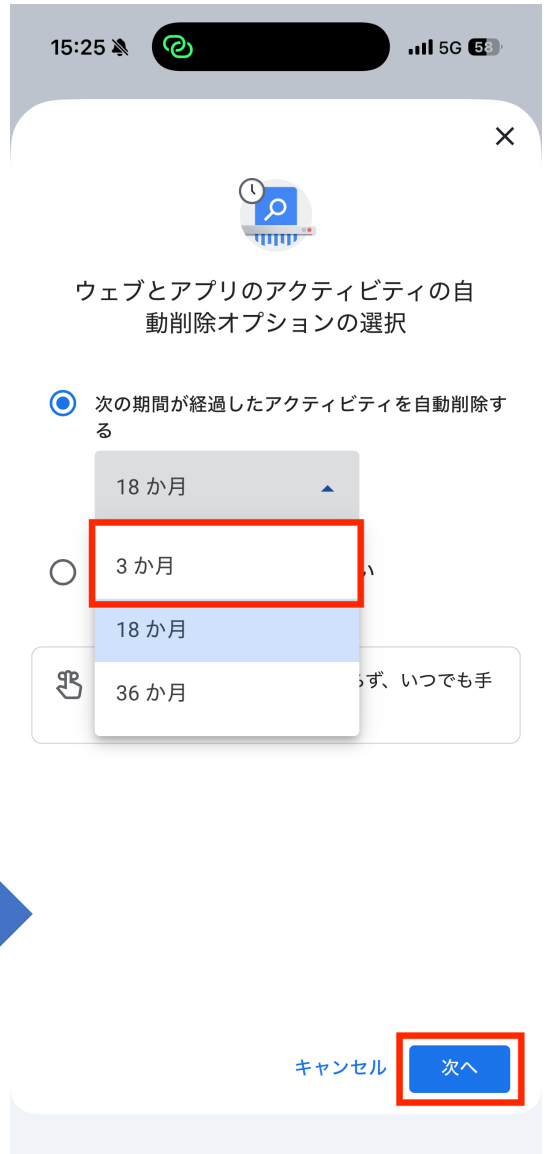
実際に設定していきましょう⑤（Chrome）

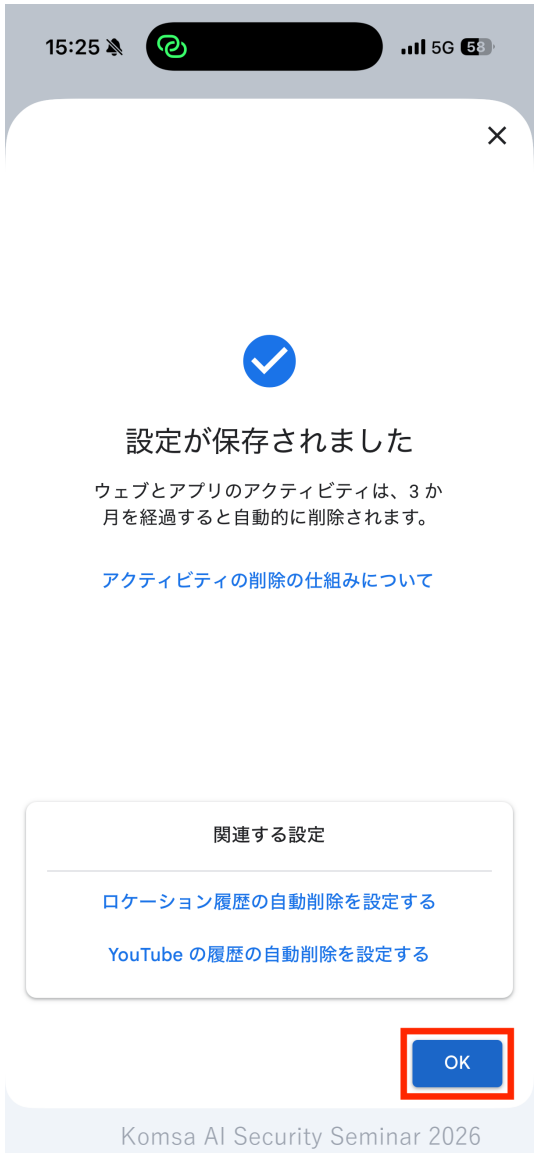


実際に設定していきましょう⑤（Chrome）



実際に設定していきましょう⑤（Chrome）





2. AI記事生成

AIで好きなジャンルの記事を自動生成

趣味や関心ごとの記事収集を安全に自動化します

AIで好きなジャンルの記事を自動生成

世界中の**公開情報**を集めて、まとめて報告。

例：航空券の価格・不動産情報・野球ニュース・株式ニュース・Amazon価格・地域イベント

テーマ	収集	要約	保存
何を知りたいか	公開情報を自動検索	比較要約	毎日・毎週の習慣化

安全ポイント：AIに「住所・勤務先・個人情報」を渡さず、公開情報だけを集める設計にします。

エージェント監視機能

「毎回自分で検索する」を、AIに手伝ってもらいます

1

テーマ登録
趣味関心を決める

2

時間を指定
何時に報告して
欲しい？

3

要約生成
報告文は詳細に？
短く整理？

4

報告方式
重複した情報は
どうする？

基本プロンプト例：「〇〇について、過去24時間の新しい公開情報を3件に絞り、
毎朝7時に要約して毎日報告してください。」

安全な記事生成のコツ

AIに任せる範囲と、入れない情報を分けます

指示内容の情報
- ✓ 趣味のジャンル
- ✓ 知りたい地域やテーマ
- ✓ 読みたい分量
- ✓ 要約の形式

入れない情報
- ✓ 自宅住所・電話番号
- ✓ 勤務先の内部情報
- ✓ 家族や顧客の情報
- ✓ ログイン情報・認証コード

ログインIDやパスワードは指示内容とセキュリティを考慮し推奨しません。
公開情報に絞り、個人情報を混ぜない設計が重要です。

ワーク：自分の「読みたい記事」を作る

テーマを1つ選び、AIに指示文を作ってもらいます

① テーマを決定

例：イベント／買い物価格／投資ニュース／ポイ活情報

② 条件を決定

毎日・7時・トップ3件・短く要約

③ AIに指示文を作成

公開情報だけを使う／個人情報やログインは使わない

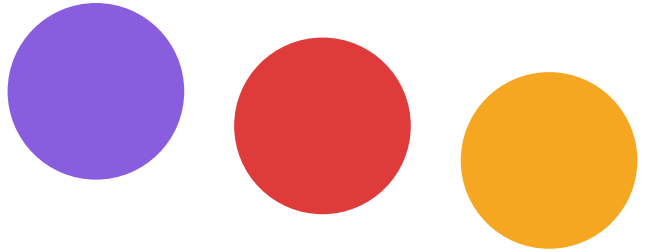
④ 出力を確認

信頼できるソースか、誤りがないか確認

完成形：あなた専用の「趣味ニュースまとめ」プロンプト

3. 最新AIフィッシング

最新AIフィッシング手法



自然な日本語・個別化・認証狙いに注意します

最新AIフィッシング手法

AIにより「日本語が自然」「大量に作れる」「個別化できる」時代です

自然な日本語
翻訳精度が上がり、見抜きにくい

個別化
名前・趣味・仕事に合わせた会話内容

音声・動画
声や顔で信じさせる

認証狙い
コード・ログイン許可・OAuthを狙う

見分けるより大切：リンクを押さない・立ち止まる・公式サイトを確認

AIフィッシングの流れ

典型的な詐欺の一例

STEP 1	STEP 2	STEP 3	STEP 4	STEP 5
偽メッセージ 宅配・銀行・ 市役所	偽サイト 本物そっくり	情報入力 ID・PW	認証要求 確認コード・ 許可	乗っ取り 不正ログイン

手を止める場所：リンクを押す前、情報を入れる前、認証コードを入力する前

危険なキーワードに反応する

詐欺は、あなたを急がせて判断力を下げます

「今すぐ」
期限切れ・停止・凍結

「秘密にして」
家族や職場に相談させない

「コードを入力」
認証コード・ログイン許可

「この電話を切らないで」
公式番号へ確認させない

この4つが出たら、話を進めず「一度止まる」

怪しい連絡が来た時の返し方

その場で決めず、別ルートで確認します

電話の場合（警察・税務署など）
「確認しますので、一度切ります。
こちらから掛け直します。」

メール・SMSの場合（宅配荷物など）
リンクは開かず、公式アプリから確認

家族・知人を名乗る場合
家族しか知らない情報を言ってもらう
電話番号やLINEで連絡して確認

職場・上司を名乗る場合
「社内の正式ルートで確認して対応」

質問タイム

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

※ 本資料は初心者向け講習用に、防御方法と設定確認に絞って説明しています。