

第2回 基礎研修 / 2026.07.29 WED AM

プロンプトと セキュリティ判断

株式会社 法研システムズ 御中 選抜 10～15名

第2回 入れてよい情報の線引きと構造化プロンプト

2026年7月29日（水）10:00 - 13:00 ／ 対面

講師 **安田 光喜**（Givery）



講師紹介 / INSTRUCTOR

安田 光喜 Mitsuki Yasuda

Givery メイン講師 / 生成AIエバンジェリスト

- 公立はこだて未来大学 修士課程修了（AI・デザイン領域）
- デザイン会社・デジタル教育会社の設立と運営を経験
- 生成AI事業を設立・運営、企業研修の設計と登壇を担当
- 非エンジニア向けの入門研修を数多く担当

第1回に続いての伴走です。今日も専門用語はできるだけ使わずに進めます。詰まったらいつでも手を挙げてください。

本日3時間のゴール

第1回で触れたGeminiを、自分の部署の仕事にどう入れるかを設計します。今日は計画を1枚形にする日です。

- ☑ 入れてよい情報・だめな情報を、自分で判断できる
- ☑ やむを得ないとき、渡す前に加工（マスキング）できる
- ☑ 5要素で依頼文を組み立て、狙った回答を引き出せる
- ☑ 自部署AI活用計画書v1を、1枚作りきる

今日の目標は**完璧な計画を作ることではありません**。粗くてもv1を1枚作りきり、上長と話せる状態にして持ち帰ることです。

今日の流れ

区分	セッション	形式	持ち帰るもの
導入	前回振り返り	共有	深掘りする論点
講義	セキュリティとデータ取扱い	講義＋デモ	入れる/入れないと加工の型
実践	プロンプト実践	ハンズオン	5要素プロンプト2本
実践	自部署計画	デモ＋ハンズオン	計画書v1

計 [180min]。発表やグループワークはありません。各自で進め、詰まったら手を挙げてください。

SESSION 01 / 共有 [15min]

前回振り返り

第1回の宿題（業務でGeminiを使った結果）を一言だけ共有し、前回作った業務×AI活用マップを開いて再確認します。

第1回の到達点と本日の位置づけ

回	テーマ	到達点
第1回	完全入門編	触ってみる / 業務×AI活用マップ作成
第2回（本日）	基礎研修	自部署にどう適用するかを設計 / 計画書v1
第3回	エンジニア向け	開発タスク体験 / ワークフロー×AI

第1回は触れてみる回でした。本日は一歩進めて、**自分の部署の仕事にどう入れるか**を設計します。第3回はさらに開発寄りの体験に進みます。

SESSION 02 / 講義・デモ [55min]

セキュリティとデータ取扱い

正しく怖がって正しく使うための時間です。公的指針の現在地を確認し、入れる/入れないの判断とマスキング加工を、デモを挟みながら押さえます。

公的指針の現在地 2026

AI事業者ガイドライン 第1.2版

- 2026年3月31日公表（総務省・経済産業省）
- 追加＝AIエージェント・フィジカルAIのリスク整理
- リスクベースアプローチの具体化
- AIガバナンスの具体化

日本のAI法

- 2025年9月1日 全面施行（2025年6月4日公布）
- 内閣にAI戦略本部を設置、AI基本計画を策定
- 実態調査・情報提供要請・指導など
- 理念法で罰則規定はなし

日本は**罰則で縛る規制ではなく、理念と体制で進める**段階です。だからこそ現場の判断基準を各社で持つ必要があります。

海外規制の最新更新

- ◆ **EU AI Act**は2026年8月2日に、ガバナンス構造とGPAI（汎用AI）の執行権限が発効します
- ◆ GPAIモデルの義務は2025年8月2日から適用済み、AI Officeの本格執行（制裁金等）が2026年8月2日から
- ◆ **最新更新** Digital Omnibus暫定合意（2026年5月7日）で、Annex III高リスク義務（採用・与信・生体認証など）の適用が**2026年8月2日→2027年12月2日へ延期**

高リスク義務の延期は**直近の更新**です。海外の規制は動き続けているので、日付とともに追う癖をつけてください。

AI利用者が押さえる責務

- ◆ **契約確認** 使うツールが学習に使うか、データがどこへ行くかを契約で確認する
- ◆ **機微性管理** 機密・個人・要配慮の情報は、そもそも渡さない前提で扱う
- ◆ **出力レビュー** AIの出力は必ず人間が確認してから使う
- ◆ **利用ログ** 誰が何に使ったかを追える状態にしておく
- ◆ **提供者制約** ツール側の利用規約・制限を守る
- ◆ **教育** 現場が判断できるよう学ぶ機会を持つ
- ◆ **HITL（人間の関与）** 採用・与信などの意思決定はAI任せにしない

社内規程では、**採用・与信などの意思決定をAIに委ねることを明文で禁止するのが安全側の運用です。**

データ取扱い 3環境×情報種別 早見表

データの種別	無料版のGemini	個人の有料プラン	会社アカウント(Workspace)
入力が学習に使われるか	使われることあり(設定でオフ可)	無料版と同じ(オフ可)	契約上 使われない
機密情報(社外秘・契約など)	原則 入れない	原則 入れない	原則 入れない(必要時マスキング)
個人情報(氏名・顧客データ)	入れない	入れない	入れない(必要時マスキング)
要配慮情報(健康・医療など)	入れない	入れない	原則NG(承認＋マスキング)

会社アカウント(Workspace)は入力が**学習に使われない**設計です。それでも機密・個人情報は『**念のため入れない**』。**迷ったら入れない**、やむを得なければマスキングが原則です。

出典 [Google Workspace 生成AI プライバシー](#) [Gemini Apps プライバシーハブ](#)

自分がどの環境かを判別する

- ◆ ログイン中のメールアドレスの**末尾ドメイン**で、会社アカウントか個人・研修用かを見分ける
- ◆ 会社ドメイン（例 @houken-...）なら会社アカウント（Workspace）
- ◆ @gmail.com など個人アドレスなら個人プラン扱い
- ◆ 個人系を使う場合は、設定で**学習オフ**にしておく

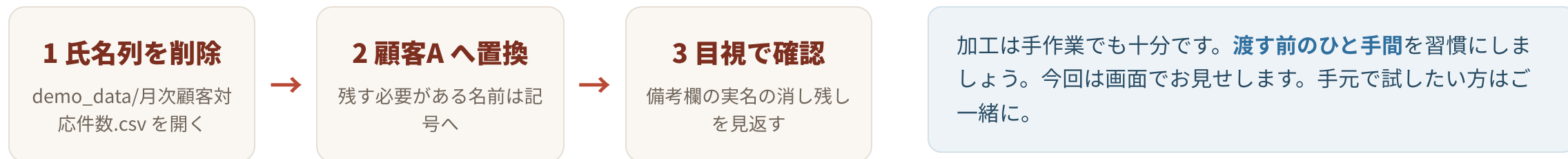
画面右上のアカウント表示で、いまどのアカウントで使っているかを毎回確認する癖をつけてください。**最終判断は自社ガイドライン**に従います。

マスキングの型 4手法

方法	どうする	例
ダミー置換	名前や社名を記号に置き換える	田中花子 → 顧客A、〇〇商事 → A社
列ごと削除	表の氏名・電話・住所の列を丸ごと消す	CSVの個人情報列を削除
一般化	粒度を粗くして特定できなくする	37歳 → 30代、住所 → 都道府県だけ
仮名化	元に戻せる/戻せない形で記号化	DUMMY-0001 のような通し番号

ダミーが最初から『顧客A』なのは、**実務でも氏名や契約番号をこう加工してから渡す**ためです。まずは全員『原則そのままは入れない』から始めてください。

渡す前に加工する工程



- ◆ **ゆらさない** 同じ名前は必ず同じ記号へ
- ◆ **迷う列は消す** 塗るより削除が確実
- ◆ **備考を見返す** 実名は備考欄に紛れがち

シャドーAI対策

約5人に1人

業務利用者のシャドーAI該当

56%

世界のシャドーAI利用

- ◆ シャドーAI＝会社が把握していないAI利用
- ◆ 国内は約5人に1人（エルテス 2026年1月調査）
- ◆ 世界では56%が業務でシャドーAIを利用（IDC）

- ◆ 承認済みツールを明示 使ってよいものを先に示す
- ◆ 軽い申請 使いたいツールは申請1本で
- ◆ 初回違反は教育優先 罰でなく学ぶ機会に
- ◆ インシデント報告ライン 起きたらすぐ相談できる窓口

禁止一辺倒だと、隠れて使うシャドーAIが増えます。使ってよい道を用意する方が安全です。

出典 [エルテス シャドーAI実態調査 2026年1月](#)

SESSION 03 / ハンズオン [55min]

プロンプト実践

5要素のフレームが主役です。曖昧な依頼を構造化する演習を2本、自分の手で書きます。導入と比較講評を挟みつつ55分で進めます。

プロンプト5要素と4原則



- ◆ **ロールは事実問題に効かない** 難問の正答率は上がらない (Wharton 2025)
- ◆ **Few-shotは2~5件** 例は多すぎず少なすぎず
- ◆ **否定形は誤読される** 『~するな』より『~してください』
- ◆ **1ターン完結を求めない** 追いプロンプトで磨く前提で

5要素を埋めると回答が化けます。ただし**ロール付与は事実確認には効かない**など、効く場面と効かない場面があります。統計は調査時期を添えて扱ってください。

演習1 構造化プロンプトを書く

- ◆ 曖昧な1回依頼を、**5要素（役割・タスク・状況・出力形式・制約）**へ書き換える
- ◆ Step1 まず曖昧な1回依頼を投げる / Step2 5要素で書き直す
- ◆ Step3 両方をGeminiに投げ、回答の差を見る
- ◆ Step4 `hints/step01_markdown_prompt_hint.md` と型紙を並べる
- ◆ 題材＝ `templates/プロンプト型紙_5要素.md`
- ◆ 第1回デモ『1回の依頼 vs 状況を渡した依頼』の受講者体験版
- ◆ **OK基準** 5要素が全て埋まり、1回依頼より具体的な回答が返る

先に型紙をコピーせず、**まず曖昧な1回依頼から**始めてください。差を自分の目で見るのが体験になります。

演習2 議事録要約

- ◆ ダミー議事録を、**要点・決定事項・宿題（担当と期限）**に構造化して要約させる
- ◆ 題材 = `templates/議事録ダミー.md`
- ◆ Step4 `hints/step02_minutes_summary_hint.md` で抜けを確認
- ◆ **OK基準** 要点・決定事項・宿題（担当と期限）が構造化されて返る

依頼例（答え合わせで開く）

あなたは会議の書記です。次の議事録を、
1) 要点 2) 決定事項 3) 宿題（担当と期限）
の3見出しで整理してください。
決定事項と宿題は箇条書きで。

配布のダミーは**実名なし**で、AIに渡してよい前提で作った素材です。実務では渡す前に必ず加工の判断を挟んでください。

発展課題 任意

発展	内容	題材・hint
A メール推敲	文面のトーンと要素を整える	hints/step03_mail_polish_hint.md
B 2文書の差分抽出	改訂前後の変更点と意図を出す	demo_data/改訂前・改訂後_社内規程.txt ／ step04
C 表データ集計	部門別集計と外れ値を出す	demo_data/月次顧客対応件数.csv ／ step05

必須は演習1・2までです。**手元に余裕がある方だけ**、上の発展課題に進んでください。hintは配布フォルダに残してあります。

SESSION 04 / デモ+ハンズオン [45min]

自部署計画

前半でNotebookLMとGemを画面でお見せし、後半で自部署AI活用計画書v1を作ります。設計する時間です。

NotebookLM 自分の資料だけで答えるAI

- ◆ 渡した資料**だけ**を根拠に答える（RAG）ツール
- ◆ バックエンドは**Gemini 3**（2025年12月に切替）
- ◆ ソース上限＝無料50 / Plus100 / Pro300 / Ultra500～600
- ◆ 1ソース最大**50万語**、アップロード資料は学習に不使用
- ◆ **社内マニュアル・規程集**を入れて社内FAQに
- ◆ **100ページ超のPDF**に直接質問して該当箇所を探す
- ◆ **Audio Overview（音声概要）**で耳から学ぶ（無料版は1日3回）
- ◆ 誤りが減るのは、ネット全体でなく手元資料に絞るから

『この資料の中身を正確に知りたい』場面に強いツールです。全員が使えるとは限らないため、今回は画面でお見せします。

出典 [NotebookLM プラン比較（公式）](#) [NotebookLM Enterprise 概要](#)

後半デモ NotebookLM と Gem

1 資料を追加

social_faq → 社内
FAQ_NotebookLM素材.md をアッ
プ



2 要約

『この資料を3行で要約して』と聞
く



3 Audio Overview

音声概要を生成して雰囲気を知る



4 Gem 紹介

よく使う役割を保存する Gem の位
置づけを説明

全員必須のハンズオンにはしません。無料版やプランで使えない・上限が違うことがあるため、まずは画面でご覧ください。手元で試せる方は一緒に。

Gemini とコーディングエージェントの今

- ◆ **Gemini 3.5 Flash**が消費者向けGeminiアプリの標準モデルに（一般提供済み）
- ◆ **Gemini 3.5 Pro**は2026年7月に一般提供をロールアウト中
- ◆ 基本は**対話型のGemini**で十分。まずここを使いこなす
- ◆ **コーディングエージェント**（Copilot / Cursor / Claude Code）は**興味喚起の紹介どまり**
- ◆ Claude Codeのモデルは**Claude Sonnet 5**（2026年6月30日）
- ◆ 非エンジニアの実務は対話型Geminiで進める、が今日の前提

開発向けのツールは『**こういう世界がある**』の紹介にとどめます。第3回で開発タスクを体験する方向けの予告です。

演習3 自部署AI活用計画書v1

- ◆ 第1回の業務×AI活用マップを起点に、対象業務を**1～2件**選ぶ
- ◆ 題材＝ `templates/自部署AI活用計画書_テンプレート.md`
- ◆ Step4 `hints/step07_dept_plan_hint.md` で埋め方を確認
- ◆ リスク・上長コメントは末尾の**任意欄**へ（今日は無理に埋めない）

セクション	書くこと
1 サマリー	何をどう変えるかを2～3行で
2 現状	対象業務のいまの手順と時間
3 AI適用方針	どこをAIに任せるか
4 データ取扱い判断	入れる/入れない・加工の可否
5 4週スケジュール	週ごとに試すこと
6 成功基準	数値で測れる目標

OK基準＝対象業務1～2件・データ取扱い判断・成功基準の数値・4週スケジュールが埋まること。完璧主義は封印して、**粗くてもv1を作りきってください**。

振り返り

- ☒ 対象業務として選んだのは何か
- ☒ 成功基準の数値を、どこに置いたか
- ☒ 計画の中で、一番ハードルが高いと感じた点はどこか

3点を**クラス共有シート（または各自メモ）**に記入してください。30秒の口頭共有は任意です。書かれた気づきを、講師が匿名でいくつか紹介します（お名前
は出しません）。

宿題と第3回へ

本日以降

計画書v1を上長へ共有してください。第3回を受講する方は計画のアップデートを続け、対象外の方は1ヶ月後に振り返りをしてみてください。

回	テーマ	到達点
第1回	完全入門編	業務で1件AIを使えた成功体験
第2回（本日）	基礎研修	自部署AI活用計画書v1
第3回	エンジニア向け	Geminiでの開発タスク体験

第3回はGeminiでの開発タスク体験に進みます。コーディングエージェントはデモ紹介にとどめます。3時間お疲れさまでした。