食品サークル AIセミナー 基調講演

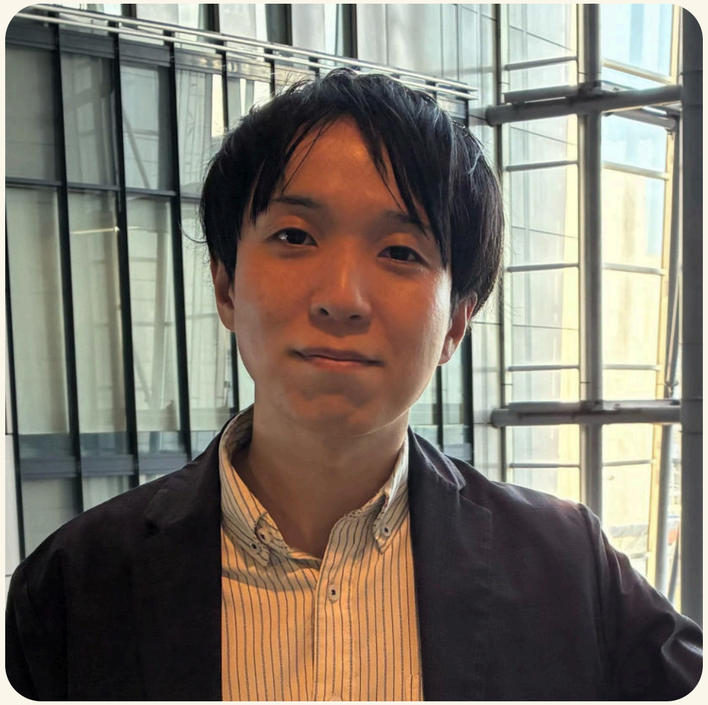
AIに聞くだけに終わっていませんか？

食品の現場で“使い倒す”ための次の一手



講師 伊藤 一樹（工学博士／特定非営利活動法人ＡＩかけこみ寺 理事長）

11/20(金) ｜ 吹上ホール



はじめに

伊藤 一樹

工学博士／特定非営利活動法人AIかけこみ寺 理事長

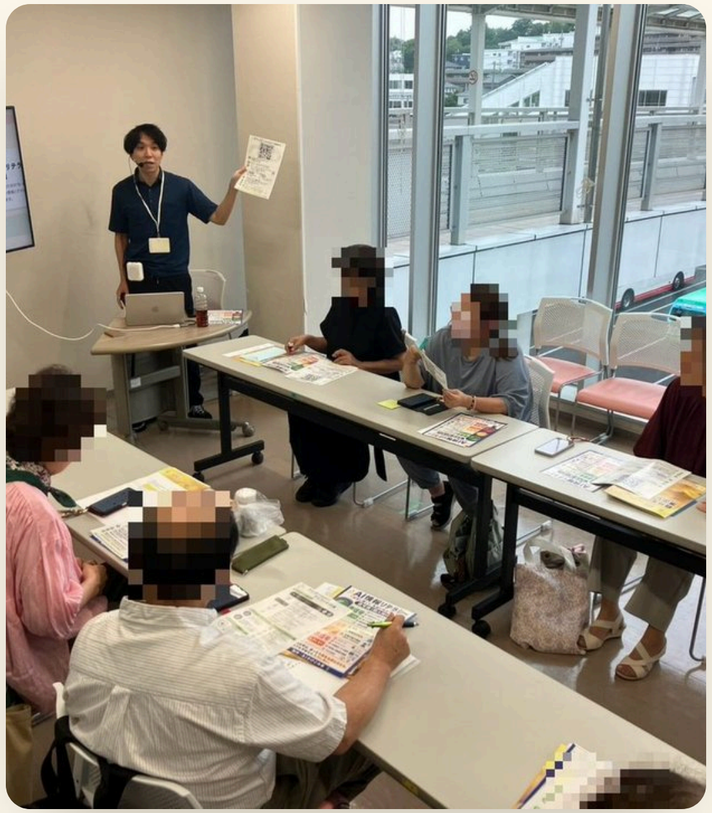
本業 半導体メーカーのエンジニア

活動 本業のかたわら無料のAI教室を
ボランティアで開催

はじめに

こんな活動をしています







地域の生涯学習センターなどで無料のAI教室を開いています

はじめに

AIかけこみ寺のこれまで

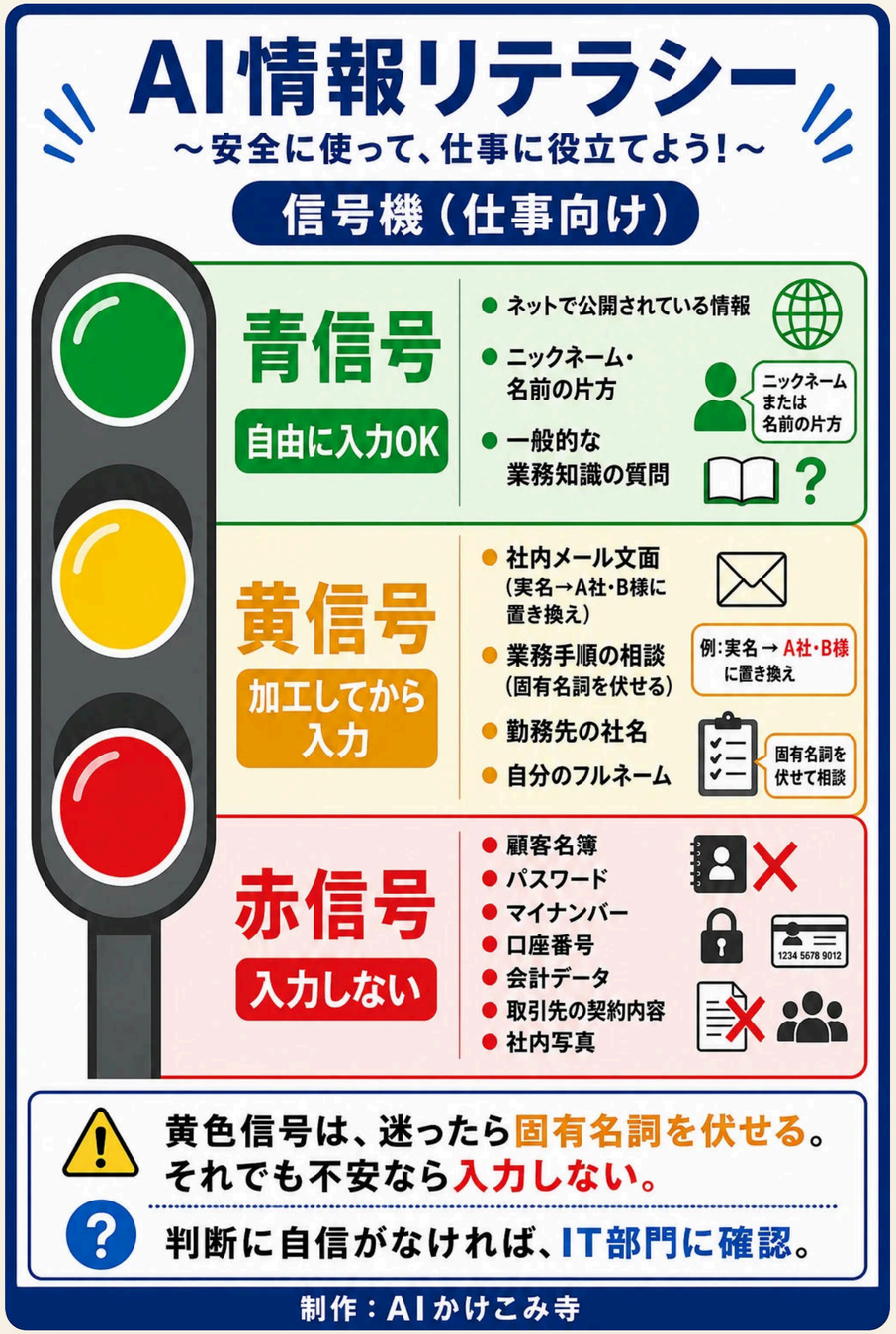
13回	198名	90%	約90名
開催回数	のべ参加者	満足度	ボランティア

- **2026年10月にNPO法人化**
  名古屋で無料のAI教室を続け来年は東京・福島（会津）でも計画中
- **身近な困りごとからアプリを作成**
  バス座席表メーカー・ひとり親ライフプランシミュレータ・食品表示ラベルメーカー

1

AIリテラシーの基本

AIリテラシー信号機


AI情報リテラシー
～安全に使って、仕事に役立てよう！～
信号機（仕事向け）
青信号
自由に入力OK
ネットで公開されている情報
ニックネーム・名前の片方
一般的な業務知識の質問
ニックネームまたは名前の片方
黄信号
加工してから入力
社内メール文面（実名→A社・B様に置き換え）
業務手順の相談（固有名詞を伏せる）
勤務先の社名
自分のフルネーム
例：実名 → A社・B様に置き換え
固有名詞を伏せて相談
赤信号
入力しない
顧客名簿
パスワード
マイナンバー
口座番号
会計データ
取引先の契約内容
社内写真
1234 5678 9012
黄色信号は、迷ったら固有名詞を伏せる。
それでも不安なら入力しない。
判断に自信がなければ、IT部門に確認。
制作：AIかけこみ寺

仕事で使う前に会社のルールを確かめる

AIの答えと社内ルールが違ったら社内ルールに従う

使ってよいAIは？

例: 会社の Copilot はよい
個人の ChatGPT はだめ

入れてよい情報は？

例: 取引先名や配合は入れない
信号機の線を会社の基準で

AIエージェントは？

Claude Code・Codex など
ファイルを読み書きできる分リスクも大きい

使用量と料金は？

誰の費用で月いくらまでか
回数の上限

情報漏洩のリスク

- **会話は普段ほかの人には見えない**
  鍵のかかった部屋のようなもの
- **ただし見られてしまうこともある**
  パスワードが盗まれたとき
  AIの運営会社がハッキングされたとき
- **見られて困る情報は入れない**
  どこまで入れてよいかは信号機が目安



2

2026年のAIの地図

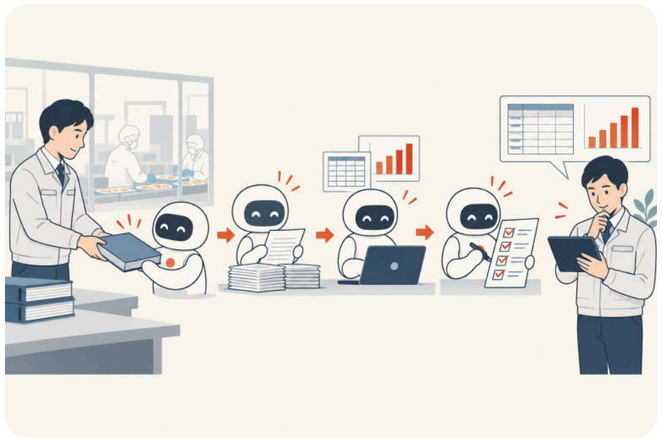
AIは3つの型に分かれてきた



チャット型

1回ずつ聞いて答えを受け取る

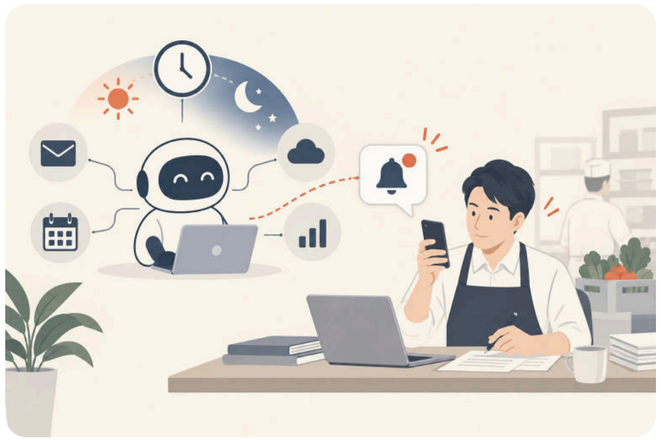
人は毎回読んで判断する



AIエージェント型

作業フォルダごと渡して指示を出す

人はできたものを確かめる



常時稼働型

裏で動き続けAIのほうから声をかけてくる

人は任せる範囲と許可を決める

2 2026年のAIの地図

チャット型 聞いて答えを受け取る

人 質問する → AI 答えを返す → 人 読んで判断する → 人 次の質問へ（くり返す）

得意

- 長い文章の要約
- 言い換え・下書き
- 考えを整理する相談
- 翻訳

苦手

- 最新の法令や基準
- 正確な計算
- 社内の事情
- 何十ものファイルをまとめて扱う

食品の現場の例

- 規格書のPDFの要点をつかむ
- クレームへの返信の下書き
- 英語の規格書を訳す
- 表示基準の質問（必ず元の資料で確かめる）

主なもの ChatGPT Claude Gemini Microsoft Copilot

2 2026年のAIの地図

AIエージェント型
作業フォルダごと渡して任せる

人 作業フォルダごと渡す → 人 指示を出す → AI 計画を立てる → AI 読む・作る・調べる → AI 確かめて報告 → 人 最終確認

食品の現場の例

- 取引先から届いた規格書20件から比較表（Excel）を作る
- 製造日報1か月分から異常の傾向をグラフにする
- 新旧の手順書から変更点の一覧を作る

得意

- たくさんのファイルの読み込みと集計
- 会議の録音から議事録を作る
- 動画や音声の編集
- プログラミング（ツール作り・自動化）

主なもの

Claude
Cowork（チャットと統合）

ChatGPT
Work

Claude Code・Codex
開発者向け

AIエージェントの始め方

1. **使ってよいかルールを確かめる**
   仕事のファイルを渡す前に
2. **有料版に入る**
   Claude は Pro（月20ドル）から
3. **デスクトップアプリを入れる**
   Claude・ChatGPT のアプリ
4. **作業フォルダを指定する**
   渡してよいファイルだけを入れたフォルダを作る
5. **頼みごとをする**
   例: このフォルダの規格書20件から比較表をExcelで作って

2 2026年のAIの地図

常時稼働型 自律して動きAIから話しかけてくる

人 目標と任せる範囲を決める → AI 自分で動き続ける → AI 気づいたら知らせる → 人 判断して許可する → AI 実行する

何が違うか

- 目標を一度伝えれば24時間動き続ける
- 連携したメール・予定・アプリからやりたいことを汲み取る
- 判断が必要なところはAIの方から聞いてくる
- たとえばネットショッピング
  美容室や映画館の予約

⚠ 注意

- パスワードを預かり
  いろいろなアカウントにログインして操作できる
- 権限が広い
  乗っ取られたら何をされるかわからない
- 出たばかりの最先端
  （Muse・Dots・Duet はここ2か月ほどで登場）
- 今年は仕事で使うのをおすすめしません

主なもの

Muse	Dots	Claude Duet	Grok Bot	OpenClaw
Meta・2026年9月8日	OpenAI・2026年9月29日	Anthropic・2026年10月21日	xAI・ベータ版	オープンソース・2025年末

モデルの違いは価格と性能の兼ね合い

	速い・安い			賢い・高い
ChatGPT	Luna 無料でも使える	Terra 有料	Sol 有料	
Claude	Haiku 無料でも使える	Sonnet 無料でも使える	Opus 有料	Fable 有料

普段のお仕事

迷ったら真ん中くらいを選ぶ

難しいこと

ひとつ上のモデルを試す

個人版と法人版の大きな違いはセキュリティ

	個人版（無料・有料）	法人版
入力が学習に使われるか	設定しだい。ChatGPT の無料版・Plus は初期設定がオン（オフにできる）	**初めから使われない**
誰が管理するか	本人だけ	**会社の管理者が利用者と設定を管理できる**
人が辞めたら	会話やファイルは本人のアカウントに残る	**会社がアカウントを止められる**
主なもの	ChatGPT Plus ／ Claude Pro ／ Google AI Pro	**ChatGPT Business・Enterprise ／ Claude Team・Enterprise ／ Gemini（Google Workspace）／ Microsoft 365 Copilot**

AIエージェントで変わったこと

聞くだけ

答えを受け取り
作業は自分でする

任せる

作業を進めてもらい
人は目的を決めて確認する

今日の話も
来年には古くなります

AIはそれだけ速く進歩しています

安全な範囲を確かめたうえで個人で最新のAIを試して動きを追うことを

おすすめします

3

AIのリスク

AIのリスクは大きく3つ

1

AIの嘘

もっともらしい間違いを
自信満々に言う

2

人の手抜きと間違い

AIの答えをそのまま使う・
会社の情報をうっかり
入れてしまう

3

サイバー攻撃

犯罪者のAIエージェントが
自動で大規模に
攻撃してくる時代になった

AIの嘘を前提にして使う

よくある嘘

- 実在しない条文や出典をそれらしく作る
- 古い基準を今のもののように言う
- 数字や単位を取り違える

対策

- AIに根拠の出どころ（法令・規格・社内文書）を出させる
- 原文は人が読んで確かめる
- 間違っていたらAIに指摘する。直してくれることが多い

ちなみに 高い有料モデルほど嘘は減る。でもゼロにはならない

AIに任せきりにする手抜き

- **AIの答えをそのまま信じる**

  考えるのをAIに任せきりにする

- **AIが作ったものをそのまま人に見せる**

  AIっぽい言い回しや「—」「**」が混ざり、読めばすぐわかる

  AI時代のマナー違反

対策

納得いくまでAIに何度もダメ出しする

伊藤は、この資料を作るのに50回はAIにダメ出ししました

3 AIのリスク ② 人の間違い

シャドーAI 会社の情報を個人のAIに入れてしまう

会社が把握・許可していないAIを仕事に使うこと

よくある場面

- 取引先のメールや規格書を私用スマホのAIに貼って要約
- 検索のつもりでGoogleのAIモードに社内の数字を入れる
- 自宅のパソコンで会社の資料をAIに読ませる

なぜ危ないか

- 個人向けは入力内容が学習に使われる設定のことがある
- 誰が何を入れたか会社にはわからない
- 共有ボタンで会話が検索に出ることも（2025年・ChatGPT）

対策

- 会社が許可したAIだけを使う
- 迷ったら入れない
- 判断に迷ったらIT部門に確認

3 AIのリスク ③ サイバー攻撃

AIでサイバー攻撃は自動化・大規模化した

2025年11月	作業の大半をAIエージェントが担うサイバー攻撃が発覚。約30の組織が標的に
2026年4月～	**Claude Mythos**　攻撃の能力が高すぎるため一般には公開せず、世界中のソフトの弱点をふさぐために使われている
2026年7月	WordPress 本体の弱点がAIを使った調査で見つかり、修正後に実際の攻撃に悪用された
2026年9月	誰でも入手できるAIでも、攻撃の能力が最先端の数か月遅れまで迫った
2026年10月	**PHP の弱点**　ホームページの約7割が使う仕組みに、ログインなしで乗っ取れる弱点。過去10年ほどのほぼ全バージョンが対象。見つけたのはAIを使うセキュリティ会社

3 AIのリスク ③ サイバー攻撃

ここ数か月で深刻な情報漏洩が相次ぐ

2026年9月

タイムズカー（パーク24）

Webシステムの弱点を突かれ、約663万件の個人情報が流出。
運転免許証などの画像も約146万件

2026年10月

GMOリサーチ&AI

アンケートサイトに不正アクセス。最大約95万人分の個人情報。
ポイントの不正交換も

2026年10月

お名前.com デスクトップクラウド（GMOインターネット）

不正アクセスで利用者の情報が流出。攻撃者を名乗る人物が公開を宣言

2026年10月

GMOトラスト・ログイン

保存場所の設定不備で2,492社・45,030人の情報が見える状態に

中小企業にとって情報管理がとても難しい時代

3 AIのリスク ③ サイバー攻撃

中小企業がいま備えること

ホームページ

PHP や WordPress が古くないか制作会社に
確かめる。何年も放置しているページは、
点検できないなら一旦止める手も

更新

パソコン・ソフト・ホームページの更新（アップデート）
を後回しにしない

アカウント

二段階認証を入れる。パスワードを使い回さない

怪しいメール

AIで文面が自然になった。リンクや添付は送り主に
別の手段で確かめる

個人情報

不要な個人情報は持たない。使い終わったら破棄する。持つなら暗号化する。持っていなければ漏れることもない

4

今日からできるAIのコツ

プロンプト① 記憶して

プロンプト

私は食品メーカーで品質保証を担当しています。
配合や取引先の情報は、社内ルールで入力禁止です。
記憶して。

- **次の会話からも覚えている**
  毎回説明しなくてよい
- **入れてはいけない情報を先に伝えておく**
  AIのほうから求めてこなくなる

プロンプト② 検索して

プロンプト

食品表示基準の最近の改正を検索して、
施行日と出典のURLを一覧にしてください。

- **AIの知識は少し古い**
  検索させると最新の情報が出る
- **出典のURLも出させる**
  裏取りがすぐできる

4 今日からできるAIのコツ

プロンプト③ PDFで出して

プロンプト

いまの内容を、社内で回覧するA4 1枚にまとめて、
PDFで出して。

食品の現場は紙とPDF

プロンプト④ 愚痴のつもりで相談

プロンプト

ケーキのアルミホイルにフォークが触れると
酸っぱい味がする。でも木やプラスチックのフォークは
好きじゃないんだよね。なんとかならない？

答え AIが「チタンのフォークにすればよい」と提案してくれた！

できないと思い込まずに、まず聞いてみるのが大事

まずは個人の有料プランで試してみる

1. 月3,000円くらいの有料プランを1か月だけ契約する
2. AIに「AIチャレンジカレンダー」を作ってもらう
3. カレンダーどおりに毎日1つずつ試す
4. 効果を感じたら続ける・感じなければやめてよい

プロンプトの例

これから1か月、有料版のAIの機能を毎日1つずつ試したい。テーマは健康と趣味。
1日10分でできるチャレンジカレンダーを作って。

4 今日からできるAIのコツ

AIエージェントに指示を出す

PC › ドキュメント › **AIエージェント用** › **クレーム記録**

名前	更新日時	種類
クレーム記録_7月.xlsx	2026/7/30	Excel
クレーム記録_8月.xlsx	2026/8/30	Excel
クレーム記録_9月.xlsx	2026/9/30	Excel
お客様相談の電話メモ_9月.pdf	2026/9/30	PDF

プロンプト

このフォルダのクレーム記録を読んで、内容で分類し、件数の表をExcelで作って。

データはすべて架空です

demo-claims.xlsx　シート「分類別の件数」（クレーム記録 17件・架空データ）

分類	件数	割合	主な内容（例）
味・品質	4	24%	いつもより固く、焼きすぎのように感じた
異物混入	3	18%	髪の毛のようなものが入っていた
表示	3	18%	アレルギー表示に卵の記載が見当たらない
包装	3	18%	開け口が切れにくい
配送・数量	2	12%	注文より1袋少なかった
問い合わせ	2	12%	原料の産地を知りたい
合計	**17**	**100%**	

PDCAサイクルとは？


Plan
目標とやり方を決める
Do
実行する
Check
計画と結果を比べる
Act
改善点を探す
何度も回す
Act のあとは次の Plan へ

AIでPDCAを速く回す



5

食品の現場で使い倒す

5 食品の現場で使い倒す

プログラミングの知識がなくてもアプリが作れる

AIエージェントはプログラミングが得意

5 食品の現場で使い倒す

食品表示ラベルメーカー



主催の食品サークルさんに
困りごとを伺って作りました

ai-kakekomi.com/apps/food-label

5 食品の現場で使い倒す

使ったプロンプト

Claude Code（月100ドルのプラン）／ Claude Fable

食品表示ラベルメーカーをHTMLとJavaScriptで作って。マニュアルもつけて。
根拠となる法令をもとに自動チェックできるように。栄養成分表示も
つけられるようにして。いろんな食品メーカーさんが使えるように、自社の
社内ルールを追加できるようにして。

そのあと　最初の案は数十分で完成・そこから何度も修正を指示

5 食品の現場で使い倒す

AIエージェントも完璧ではない

最も賢いモデル（Claude Fable）で作っても最新のアレルゲンが抜けていた

カシューナッツ

特定原材料（義務）に追加

ピスタチオ

準ずるもの（推奨）に追加

令和8年（2026年）4月1日 消費者庁 事務連絡。カシューナッツは2028年3月末までの経過措置

だから AIの知識の遅れは人の専門知識で補う

6

今日からできるチャレンジ

今日からできるチャレンジ（個人で）

- [ ] **個人の有料プランを1か月だけ試してみる**
  AIにチャレンジカレンダーを作ってもらい毎日1つ試す
- [ ] **「記憶して」「検索して」「PDFで出して」と入力して試す**
- [ ] **うまくいかないことを愚痴のつもりでAIに相談する**
- [ ] **健康や趣味の目標でAIとPDCAを回してみる**
  AIと計画を立てて自分で実行し結果を報告する
- [ ] **AIの答えは元の資料で確かめる**

今日からできるチャレンジ（会社で）

- [ ] 会社で許可されているAIと利用上限を確かめる
- [ ] AIエージェント（Claude Code・Codex など）が使えるか確かめる
- [ ] 使えるなら読ませてよいExcelやPDFをフォルダごと渡して指示する
- [ ] 毎日の定型業務を1つ選び自動化できないかAIエージェントに相談する
- [ ] 自社のITセキュリティを制作会社に確かめる
  PHP・WordPress など

まとめ

今日のまとめ

1 **AIリテラシーの基本**
社内ルールが最優先。信号機で入れてよい情報を決める

2 **2026年のAIの地図**
チャット型・AIエージェント型・常時稼働型。モデルは迷ったら真ん中

3 **AIのリスク**
AIの嘘・人の手抜きと間違い・サイバー攻撃。中小企業も備える

4 **今日からできるAIのコツ**
記憶して・検索して・PDFで出して。AIでPDCAを速く回す

5 **食品の現場で使い倒す**
知識がなくてもアプリは作れる。最後は人の専門知識で補う

今日いちばん伝えたいこと

AIに聞くだけで終わらず
任せて確かめる

AIと一緒に考え、人間は現実世界で実行する。何度でも回して、仕事を変えていきましょう

6 今日からできるチャレンジ

AIかけこみ寺 LINE公式

無料AI教室の日程・講演や教室のご相談は
LINEから

LINE公式アカウント

AIかけこみ寺

ありがとうございました

ai-kakekomi.com