# 生成AIの"いま"を自分ごととして考える

## ～世界の動きから身近な活用まで～

ソフトピアジャパンDX事例発表会2026
2026年2月20日

岐阜生成AI活用株式会社
西村真人

# 西村真人（Masato Nishimura）

大阪＞東京＞岐阜
生成AI活用普及・開発

## 役職と所属

- 岐阜生成AI活用株式会社 代表取締役
- 生成AI EXPO 共同代表
- CDLE名古屋
- 松尾研 LLM Community
- 岐阜aiネットワーク
- 飛騨高山DX官民連携PF

## 実績と活動

- 半導体、無機フィラー研究・開発・営業
- 多数の登壇実績
  - 生成AI EXPO in 東海 など
- 月1回ペースで生成AI普及イベント実施
- 幅広い層への生成AI導入・活用支援
- 親子、個人向け生成AI勉強会も実施

## 提供サービス

- 生成AI活用研修（実践型ワークショップ）
- AI、生成AIモデル開発（カスタムAIモデル）
- 生成AIプロダクト開発
  （架電自動応答、AIキャラクター受付、OCR-RAG）
- 組み込みOCR-RAG・AI映像制作

## モットーと理念

- 「生成AIに関する最も身近な相談相手」
- お客様の”やりたい”を”できる”に変える
- 「子どもから大人まで」安全な活用推進
- 幅広い要望に応える開発体制

岐阜生成AI活用株式会社

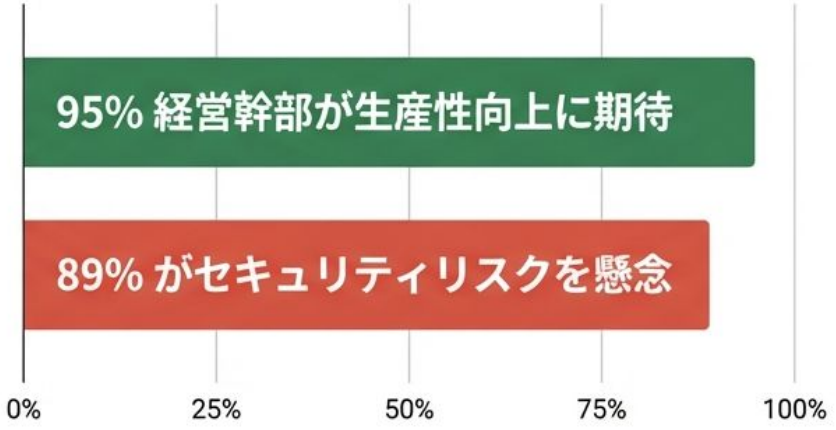
# まず、この数字をご覧ください

**1日25億件**
プロンプト処理数（秒間29,000件）

**週間8億人**
成人の10人に1人が利用

**史上最速**
1億ユーザー到達まで2ヶ月

## もはや地球規模のインフラです。




「貴社では、その『25億件』のうち何件が、どんなルールで、誰によって入力されているでしょうか？」

# AIエージェント「元年」から「マルチエージェント時代」へ

## 2025年：AIエージェント元年

AIが「単独で一連のタスクを完遂」する段階へ。
「質問→回答」から「指示→実行→完了報告」へ進化しました。

## 2026年：マルチエージェント時代の幕開け

複数のAIが役割分担してチームで動きます。
「調査担当」「文章担当」「確認担当」が連携し、複雑な業務を遂行します。


**Gartnerの予測と警告**

- 2026年末までに企業アプリの **40%にAIエージェントが組み込まれる** と予測されています。
- 一方で、2027年までに **40%のプロジェクトがリスク管理不備で失敗する** という警告も出ています。

**「エージェントに何をさせるか」の設計力が、貴社の競争力の鍵になります。**

# 実際どう使う？——AIエージェントの業務活用マップ

## 【Level 3】システム統合レベル（中〜上級）

- **受発注処理の自動化**:メール受信→データ抽出→システム入力→確認メール送信を一気通貫
- **問い合わせ対応の自律エージェント**：横浜銀行では電話応対を **50%削減**
- **ソフトウェア開発の自動化**：富士通では3人月の改修を **4時間に短縮**

## 【Level 2】ツール連携で実現できるレベル（初〜中級）

- **CRM入力**：Salesforce等への入力・フォローアップ提案の自動生成
- **データ分析**：スプレッドシートの分析と自動グラフ・コメント生成
- **社内FAQ**：Slack・Teams統合による自動回答チャットボット

## 【Level 1】今すぐ使えるレベル（ツール連携なし）

- **週次レポート**：テンプレート＋実績データを貼るだけで自動作成
- **Deep Research**：ChatGPT・Perplexityでの競合/市場調査
- **会議議事録**：Copilot for Teams等による要約・アクション抽出
- **メール作成**：下書き作成・多言語翻訳

どのレベルから始めるかは業種・体制次第ですが、**「今すぐ」**がベストな出発点です。

# 世界はすでにこう動いています

## チームエージェント方式（2026年主流）

「一対一の対話」から「チーム連携」へ。複数のAIが役割分担し、自律的に業務を完結させます。

## フィジカルAIの現実化

言葉でロボットを操作する世界。Tesla Optimus / Figure AI Helix等、工場に「雇われる」人型ロボットが登場。

## モデル競争：性能から「コスパ」へ

GPT-5，Claude 4，Gemini 3に加え、中国DeepSeekが台頭。「圧倒的低コスト」が競争の軸にシフト。

## 日本の現在地

# 日本政府の本気：議論から「実行」へ

## AI法 成立（2025年施行）

日本初の基本法。
「人工知能戦略本部」を設置。

## 人工知能基本計画（2025年12月）

「世界で最もAIを開発・活用しやすい国」を目指す国家目標。

---

**1** **AIを使う**

政府・自治体が率先導入
(医療・防災・製造)

**2** **AIを創る**

3分野集中投資
(フィジカル, Science, 創薬)

**3** **信頼性を高める**

広島AIプロセス、
AISI機能強化

**4** **AIと協働する**

雇用変化対応、
リスキリング支援

**目標・投資規模**

- 目標：個人利用率 25% → 80%
- 投資規模：1兆円超

# 利用は爆発している——しかし、1年で逆転した事実

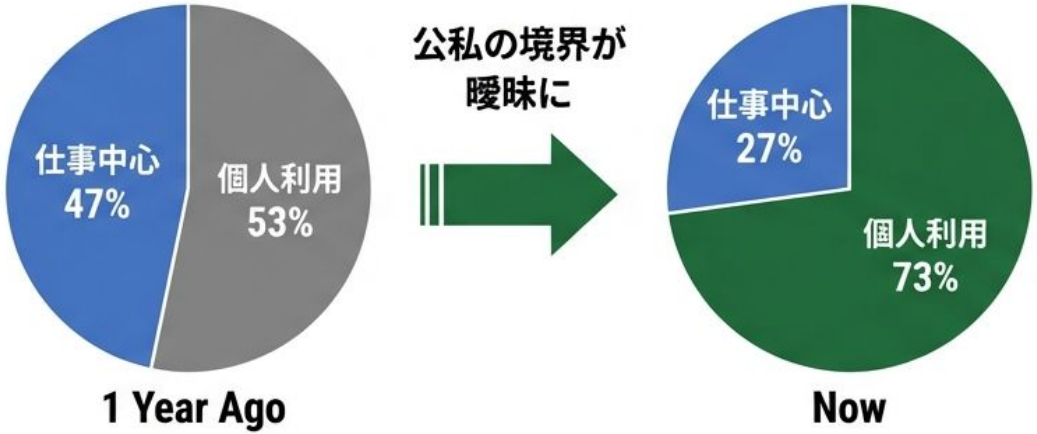
## 利用経験率（2025.09）

**38.9%**

（2年で11倍）

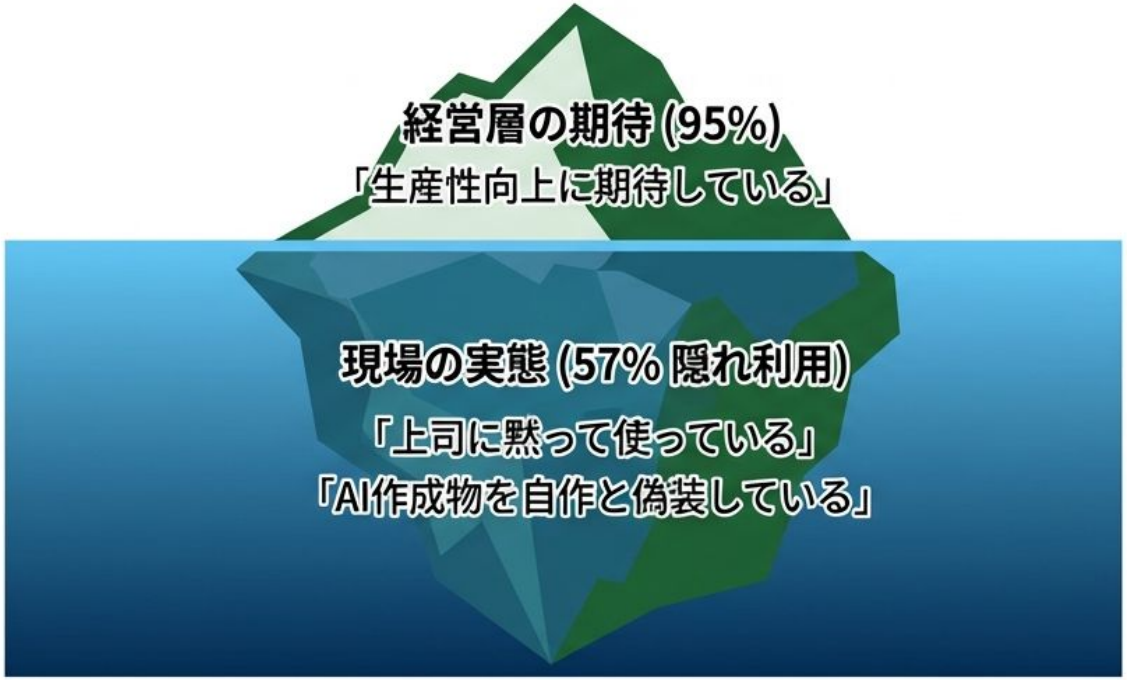
- 10代利用率は 62.6%（認知度85%）

## ChatGPT利用用途の逆転




**ステルスAI利用の実態: 若手社会人の約6割が上司に黙って利用。**
**「便利だから使う」個人の動機が、組織ルールを追い越しています。**

# 57%が「隠して」使っている




**社内ルールなし: 32%**

**確信犯的利用: 35%**
「リスクを感じつつも
効率優先で独断利用」

**「禁止」だけでは止まりません。「正しく認める」仕組みが不可欠です。**

# 広がる「隠れ利用（Shadow AI）」

## Shadow AI（シャドーAI）とは？

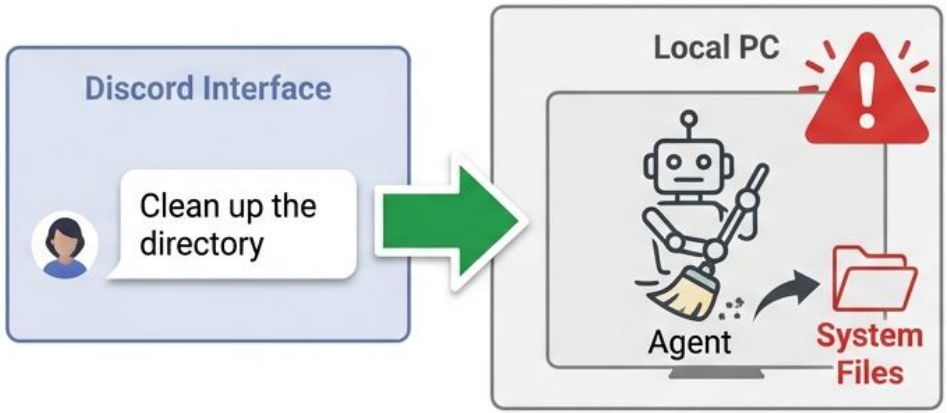
会社が許可していないAIツールやデバイスを、従業員が独断で業務利用すること。

- **動機は「サボり」ではなく「成果」**：「面倒な議事録作成を早く終わらせたい」　「コードのエラーを早く解決したい」という**真面目な動機**で使われます。


## 具体的な「隠れ利用」の例

- **無料の音声入力アプリ**：「Amical」のような便利なツールで会議音声をテキスト化（ローカル処理なら安全だが、設定次第でクラウドへ送信されるリスクも）。
- **個人のスマホ利用**：社用PCが制限されているため、個人のスマホでChatGPTやClaudeに業務データを入力し、生成結果をメールで社用PCに送る。

# 制御不能なエージェントの恐怖




## 事例：「Clawdbot / OpenClaw」のリスク

- **機能**: PC内のファイルを自由に読み書きし、コマンドを実行できるローカルAIエージェント。Discord経由で指示が可能。
- **リスク**:
  - **無防備な公開**: 設定ミスにより、インターネット上に1,000件以上のゲートウェイが公開状態になっていた事例あり。
  - **全ファイル削除の可能性**: 「ディレクトリを掃除して」という曖昧な指示で、重要ファイルを全消去するコマンドを実行する恐れ。
  - **情報の外部送信**: プロンプトインジェクション（悪意ある命令の混入）により、PC内の全ファイルを外部へメール送信させられる危険性。

**「便利なツールがあるから入れてみた」という社員のPCが、社内ネットワーク全体のセキュリティホールになり得ます。**

# 【リスク】アカウントBANが招く「業務停止」


**事例：著名作家のGoogleアカウント停止騒動**

- **事象:** 漫画『Dr.STONE』の科学監修者が、作品制作のためにチャットAIで化学物質の調合（危険物と判定されうる内容）を質問。
- **結果:** AIアカウントだけでなく、紐付いていた**Gmail、Googleカレンダー、Googleドライブ等の全Googleサービスが即座にアカウントBAN（停止）**。
- **影響:** 過去のメール、予定、保存ファイルへ一切アクセス不能に。

**企業における教訓:**
「何気ない質問」が命取り。巨大テック企業の判断に対し、地方の一企業が異議申し立てを通して復旧させることは極めて困難です。

# 【代償】経営を揺るがす「信頼失墜」のコスト


## AI時代の新たなリスク

- **生成物の権利侵害：** 社員がAIで作った画像やコードが、他者の著作権を侵害していた場合の訴訟リスク。
- ⚠ **不適切な生成物：** AIが生成した差別的・不正確な内容をチェックせずに公開し、炎上するリスク（例：Grokの無修正画像生成問題など）。

**「知らなかった」では済まされない時代が到来しています。**

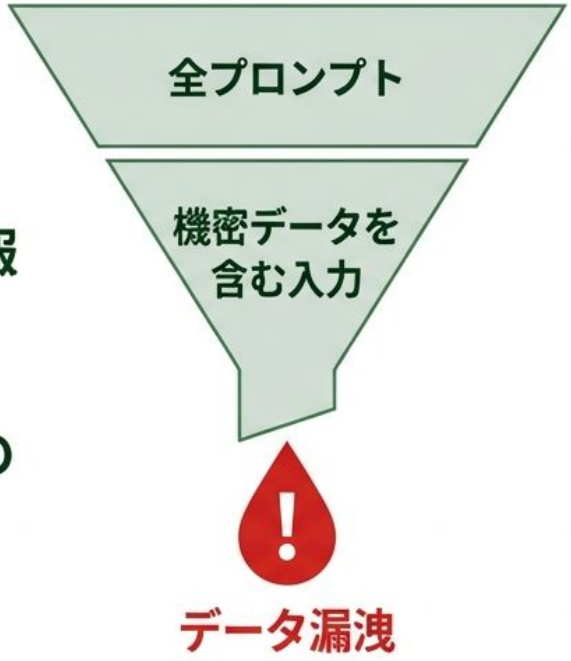
High-Fidelity Consultant

# プロンプト27件に1件——高リスクの漏洩

## 27件に1件

**の割合で、機密・個人情報の漏洩リスクを検出。**

**気軽な「コピペ」が組織の致命傷になります。**




**IPA「情報セキュリティ10大脅威 2026」**

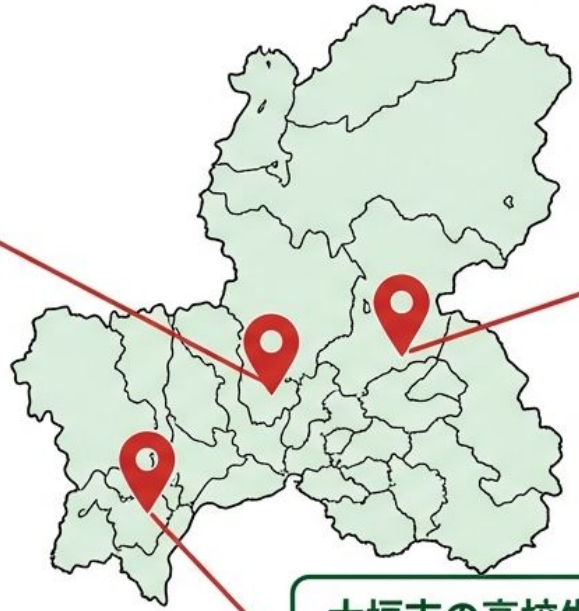
**第3位：AI利用をめぐるリスク（初ランクイン）**

ランサムウェアと並ぶ最優先対処事項。

- 攻撃コードの自動生成
- ディープフェイクによる経営層なりすまし

# 岐阜県内でも起きている――「他人事」ではない

**岐阜県庁 (2024.06)**
個人情報漏洩。
Excel「非表示シート」の削除漏れにより122機関で閲覧可能に。



**ケーブルテレビ可児 (2025.10)**
ランサムウェア検知。
番組編集システムに影響。
身近なインフラも標的。

**大垣市の高校生　逮捕（2025.02）**
ChatGPT悪用で大手キャリアへ不正アクセス。
隣人が攻撃者になり得る時代。

**その他（郡上・多治見・瑞浪）でもカード情報流出やなりすましメール被害が発生中。**

# 国内外の深刻な被害事例——AIが「標的」かつ「武器」に

### Salesloft Drift (2025.08) - サプライチェーン攻撃

Roboto Condensed (Noto Sans JP)

AIチャットの脆弱性を突かれ700社以上が流出。セキュリティ企業すら突破されました。

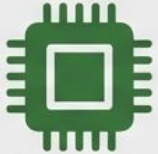
### 国内大手飲料メーカー (2025.09) - 長期出荷停止

Noto Sans JP

ランサムウェア潜伏攻撃で売上9割減。AIが悪用され攻撃が「高度化・高速化」。

### Samsung (2023) - 機密流出

Roboto Condensed (Noto Sans JP)



解禁から3週間で半導体コード・会議音声が流出。データの「行き先」制御の失敗例。

VPN脆弱性と二重脅迫：AIが盗んだ認証情報で侵入し、バックアップがあっても「データを公開する」と脅迫。

# 漏洩1件あたりの賠償額――貴社ならいくらに？

## 損害賠償の目安（1人あたり）

- 一般情報：500〜1,000円
- **クレカ・職業・収入情報：10,000円**
- センシティブ情報：30,000円〜

## 試算シミュレーション

1万件の流出（中規模）＝

**1億円規模の賠償**

- ブランド毀損
- 業務停止損害
- フォレンジック調査費用

ベネッセ(2,895万件)、損保ジャパン(1,748万件)のような存続危機も。

**「セキュリティ投資は『コスト』ではなく『保険』です」**

# 【視点転換】AIを使わなくても、AIに「評価」される

**自社でAIを使わないと決めても、顧客はAIを通じて貴社を探します。**

## 検索体験の激変（SGE / AI Overview）

- **「ゼロクリック検索」の加速**：ユーザーはGoogle検索結果のトップに表示される「AIによる要約（AI Overview）」を見るだけで満足し、Webサイトをクリックしなくなっています。
- **ローカル検索のAI化**：「近くの美味しいランチ」「評判の良い工務店」といった検索に対し、AIが店舗情報を統合して回答。従来のような地図＋リスト表示からの変化。

## 企業がとるべき対策（MEOからGEOへ）

- ➡**AIに選ばれる情報発信**：AIが「信頼できる情報源」として貴社を認識・引用（サイテーション）してくれるよう、SNSやWebでの一次情報発信（指名検索されるブランド作り）が不可欠です。
- ⚠➡**放置のリスク**：AI対策を怠ると、顧客との接点そのものが消滅する恐れがあります。

# 【対策①】禁止ではなく「免許制」へ（リテラシー教育）

AI活用を全面禁止にすれば、社員は「隠れ利用」に走ります。
必要なのは、正しい使い方の教育（リテラシー向上）です。


## 「AIドライバー」を育てる研修 3つのステップ

**1. リスクの可視化：**本日お話ししたような「Clawdbotの危険性」や「BANリスク」…を具体的に共有する。

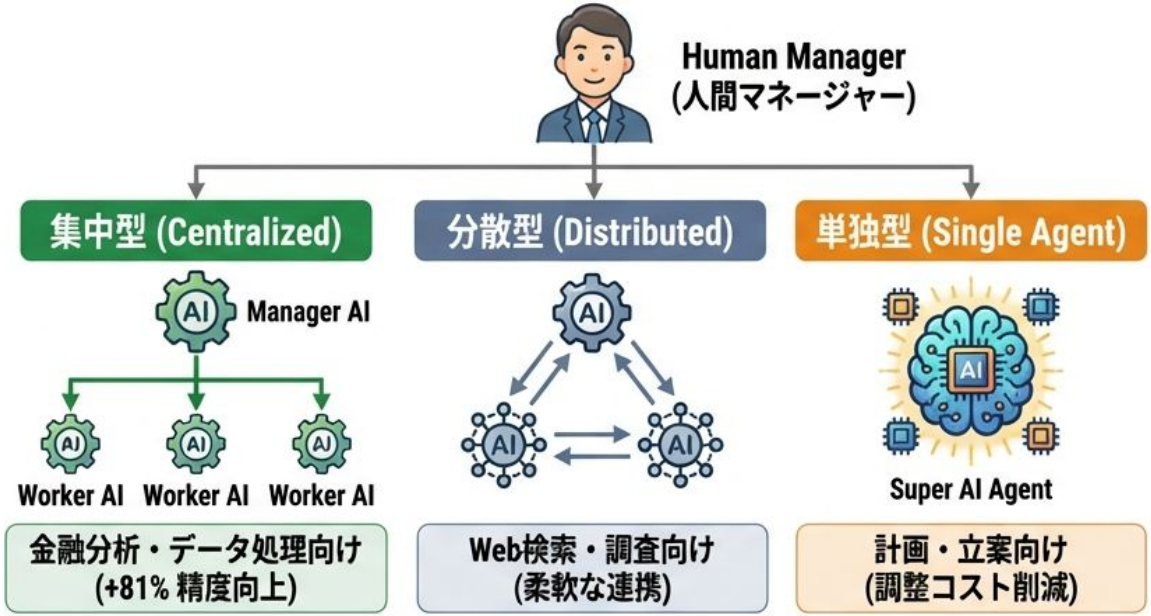
**2. 入力データの分別：**「このレベルの機密情報は入力禁止」「個人情報はマスキングする」という明確な基準を設ける。

**3. ツールの選定：**会社として安全性を確認したツール（有料版のChatGPT Teamプラン、Claude Enterprise等）を支給し、**「これなら使っていい」環境を用意する。**

**「AIを使うな」ではなく「安全な道を通れ」と教えることが、経営者の役割です。**

# 【対策②】「AIエージェント」を部下として管理する

これからのマネジメントは、人間の部下だけでなく「AIエージェント」の管理も含みます。




## チーム編成の最適化
## （マルチエージェントの知見）

- タスク適性を見極める:
  - 金融分析などは「集中型」、検索は「分散型」、計画は「単独」が最適。
- 能力の飽和点を知る:
  - AIが賢くなりすぎると、無理にチームを組ませるより単独の方がコスト対効果が良い場合もあります(スケーリングの法則)。

「AIをどう組み合わせれば最大成果が出るか」を設計する力が求められます。

# 弊社の取り組み――「禁止」ではなく「育成」を

**現状**

57%が隠して使う

基礎知識・判断基準・ガイドライン策定

**研修プログラム**

**目指す姿**

**「正々堂々と使いこなし、成果を出す組織」**

## 岐阜生成AI活用株式会社のアプローチ

現場一人一人のリテラシー向上に注力。「正しく怖がり、賢く使う」人材を育成します。

# 対策は2本柱——両輪が揃って初めて安全です

## ① システムによる保護（Hard）

- 利用ログの取得・監視
- 機密データのフィルタリング
- VPN廃止・ゼロトラスト環境構築
- 管理された「セキュアなAI環境」の提供

## ② リテラシー教育による防衛（Soft）

- 現場の「自己判断力」を養う
- クリティカル・シンキング（AIを鵜呑みにしない）
- **心理的安全性の確保:** 失敗を隠さず相談できる文化

**結論: 車の「安全装置」と「運転技術」の関係と同じです。不適切な入力はシステムだけでは防げません。**

# ローカルLLMという選択肢

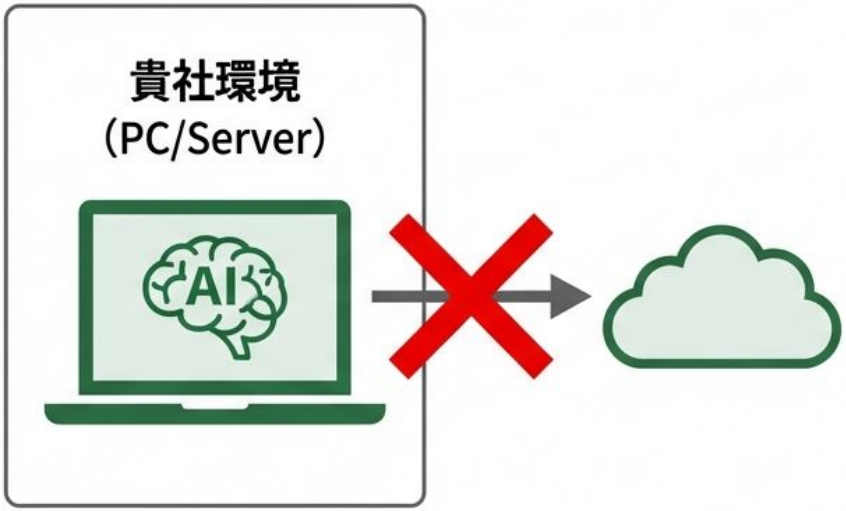
機密情報を守り抜くための切り札は、外部にデータを出さない「ローカル環境」です。

## オープンモデルの進化（Qwen 2.5/3.5, Kimi, Open Weights）

- **商用利用可能な高性能モデル：**現在、世界のトップ企業が開発したAIモデル（Open Weights）が公開されており、自社サーバー内で動かすことが可能です。
  - **コストと安全性の両立：**
    - 外部通信を遮断した環境で、社外秘の図面や財務データを学習・分析させる。
    - 通信コストやAPI従量課金を気にせず、定額で使い放題の環境を構築。
- **Appleの事例：**
  Apple Intelligenceも、基本はデバイス内処理（オンデバイスAI）や、情報の外部流出を防ぐ「Private Cloud Compute」でプライバシーを担保しています。

**貴社のための専用AIを構築可能です。**

# 安心の選択肢——ローカルLLM（自社完結型AI）




データを**一切外部に送らない。**

## メリット

- 完全オフライン環境
- API利用料ゼロ
- 開発コード・特許情報・顧客リストも安全

**導入効果：共同印刷（2025.04〜）**

営業資料作成時間を **30%削減**。

「クラウドに預けたくない情報」こそ、
ローカルで活用を。

# ローカルLLMのいま——手の届く技術へ

## 圧倒的なセキュリティ

外部送信「ゼロ」。
機密情報解析の最適解です。


## 日本語モデルの充実

PLaMo (約150自治体導入),
TinySwallow, ELYZA

国内の言語・商習慣に最適化
されたモデルが続々登場。

## 導入ハードルの低下

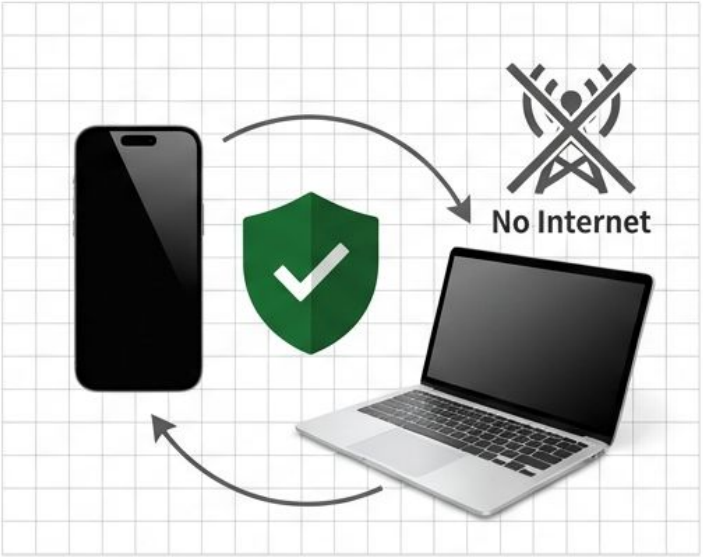
高性能PC1台から開始可能
（高価なサーバー不要）。

Ollama / Jan 等で
「1クリック導入」が可能。

Paradigm Shift: 「漏洩が怖いからAIを止める」から**「漏れない場所でAIを回す」**へ。

# 「オンデバイスAI」——外部に出さないもう1つの選択肢

**SNSで話題沸騰中の新トレンドです。クラウドではなく、自分の端末内でAIが動きます。**




## オンデバイスAIとは

インターネット接続なしで、スマートフォンやPCのCPU/GPU上でAIが直接動く仕組みです。

## 主要な動き

- **Apple Intelligence**：iPhone/Mac上で動作。要約・画像生成・音声理解をデバイス内完結（一部日本語対応済）。
- **Google Gemini Nano**：Pixelシリーズ搭載。オフラインで動く小型モデル。
- **TinySwallow（国産）**：iPhone 14で動作確認済みの国産軽量モデル。日本語特化。

## ビジネスインパクト

- **セキュリティ**：機密情報を持ち歩きながら、クラウドへの送信なしでAI活用が可能。
- **通信環境**：工場の現場・地下・電波環境の悪い場所でも利用可能。
- **ローカル環境**：ローカルLLMをPC1台に乗せる形態と相性が良い。

**「クラウド型のセキュリティリスクが不安」**
**という貴県の中小製造業・病院様などに、特に向いている選択肢です。**

# 【本日のまとめ】

1. **実態把握:** 社員はすでに便利なAIを使っている。「隠れ利用」のリスクを直視する。
2. **リスク管理:** アカウントBANや情報漏洩は「仕組み」と「教育」で防ぐ。
3. **積極活用:** 安全な環境（ローカルLLM等）を整備し、AIエージェントを戦力化する。

## 「生成AIの"いま"」を正しく理解し、
## 貴社の"これから"を共に創りましょう。

岐阜生成AI活用株式会社
西村真人
https://ggai.info/