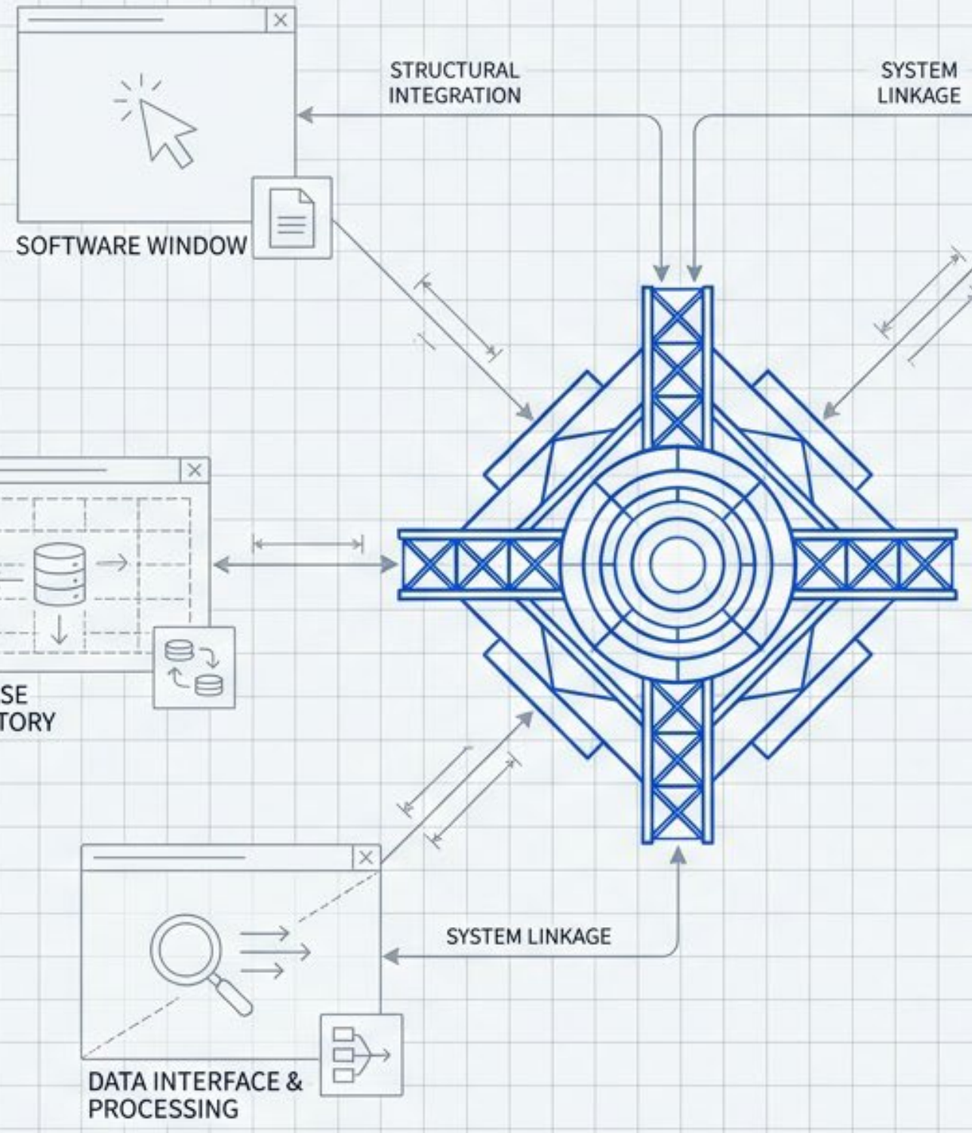


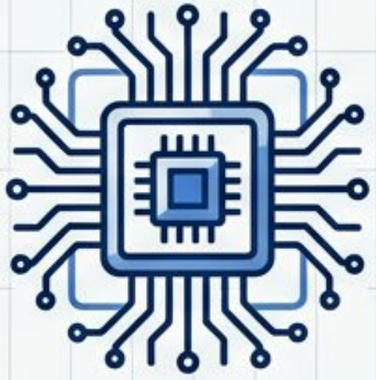
知財業務におけるAgentic AIの夜明け

Gemini 3.5 Flash「Computer Use」機能がもたらす構造的変革と戦略的実装アプローチ

リード・知財DXアーキテクト

2026年6月27日

エグゼクティブ・サマリー：3つのパラダイムシフト



技術的飛躍
(The Tech Shift)

API非依存の完全統合。単一のAIモデルが、人間と全く同じように画面を視覚的に認識し、文脈を推論し、自律的に操作を実行する「Computer Use」の標準搭載。

実務的価値
(The Operational Value)

単純なデータ転記から、非定型・推論を伴う知識労働への移行。クライアント別ポータル連携、引例PDFの知的格納、明細書の継続的品質監査などの複雑なGUI業務を完全自動化。

厳格なコンプライアンス
(The Strict Compliance Mandate)

知財特有の機密性を守るためのアーキテクチャ設計。Vertex AI環境における「Zero Data Retention (ZDR)」の確実な達成と、日本弁理士会（JPAA）ガイドラインに準拠した人間の関与（Human-in-the-loop）の実装。

知財DXのボトルネック：従来型RPAの構造的限界

固定座標への依存が、メンテナンスコストの増大とエラーを引き起こす。

The Rigid Line
(従来型RPA)

- UI変更への極端な脆弱性（数ピクセルのズレで停止）
- 例外処理能力の欠如（予期せぬポップアップによる誤動作）
- 非構造化データ（特許明細書・通知書）の推論不可

The Semantic Target
(Agentic AI)

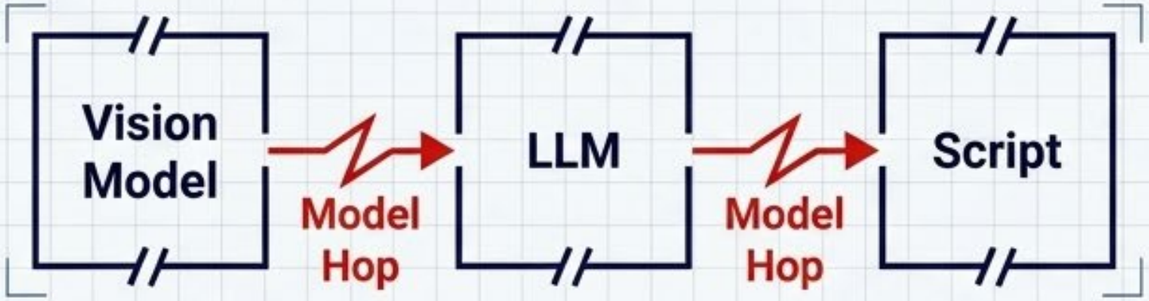
Gemini 3.5 Flashは「絶対座標」ではなく「意味論的構造」を理解し、人間のようにUIの文脈を解釈する。

診断マトリックス：従来型RPA vs. Agentic AI

比較項目	従来型RPA	✧ Gemini 3.5 Flash
UI変更への耐性	低い (固定座標/DOM依存)	極めて高い (視覚情報と文脈から推論)
対応可能なタスク	定型的な繰り返し作業 (データ転記)	非定型・推論を伴う作業 (要約、比較、動的判断)
例外処理・エラー回復	事前設定外の事象で停止	画面状態を再評価し自律的に回避
開発インターフェース	シナリオ構築ツール	自然言語による目標指示 (Prompt)
API非依存のGUI操作	可能（ただし脆い）	可能 (人間の視覚・操作を模倣し堅牢)

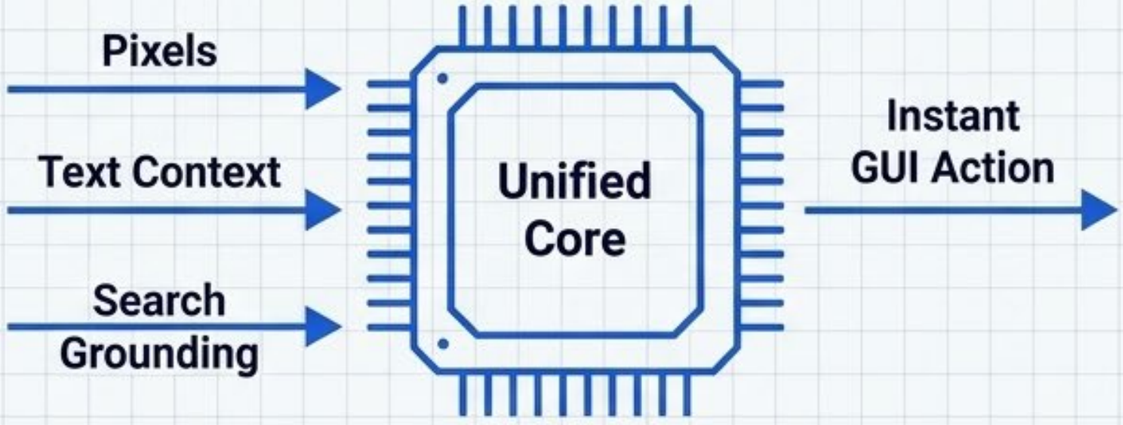
技術的革新：「モデルホップ」の排除によるリアルタイム制御

パイプライン構成 - 過去のアーキテクチャ



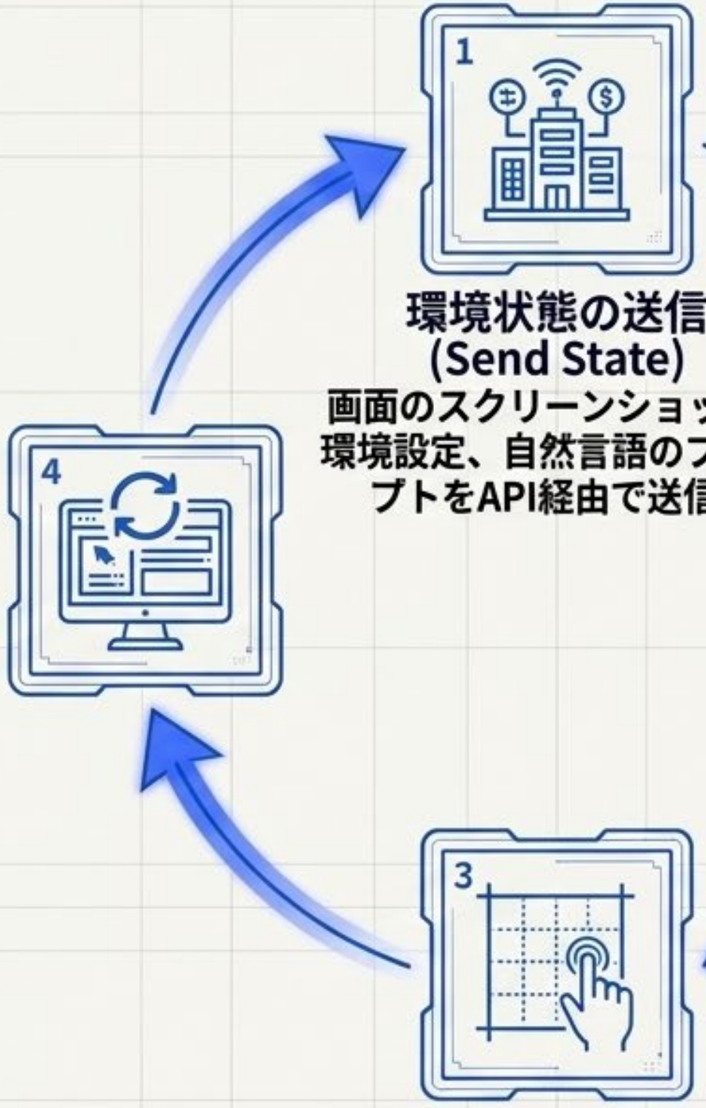
マルチモデル間の受け渡しによる遅延（レイテンシ）と微細な情報の欠落。

ネイティブ統合 - Gemini 3.5 Flash



- **単一の推論パス** (Single Inference Pass)
- **視覚認識、言語処理、リアルタイム検索**（Grounding）**、ツール操作が単一モデルに直接統合。文脈の断絶が完全に排除され、エンタープライズ水準の実行速度と信頼性を獲得。**

エージェントループ：視覚認識と行動の反復プロセス



環境状態の送信
(Send State)
画面のスクリーンショット、環境設定、
自然言語のプロンプトをAPI経由で送信。

推論と意図の生成
(Reason & Generate Intent)
次のアクションを決定し、自身の論理的推論（intent: 意図）を可視化出力。
ブラックボックス化を防止。

座標の非正規化と実行
(De-normalize & Act)
モデルが認識した「1000×1000の正規化グリッド」を、
実際のディスプレイ解像度（ピクセル座標）に変換
（非正規化）し、物理的なクリック・入力を実行。

状態の再評価
(Re-evaluate)
アクション後の新たな画面を
キャプチャし、タスク完了まで
ループを継続。

環境状態の送信
(Send State)
画面のスクリーンショット、
環境設定、自然言語のプロンプトをAPI経由で送信。

多層防御（Defense-in-depth）：エンタープライズ向けの堅牢なセーフガード

オプトイン型インジェクション検知 (Opt-in Injection Detection)

隠された敵対的な命令（間接的プロンプトインジェクション）をスキャンし、検知時にタスクを自動停止。

敵対的訓練 (Targeted Adversarial Training)

不適切な操作要求やシステムを欺こうとするプロンプトに対する、モデルレベルでの根本的な耐性強化。

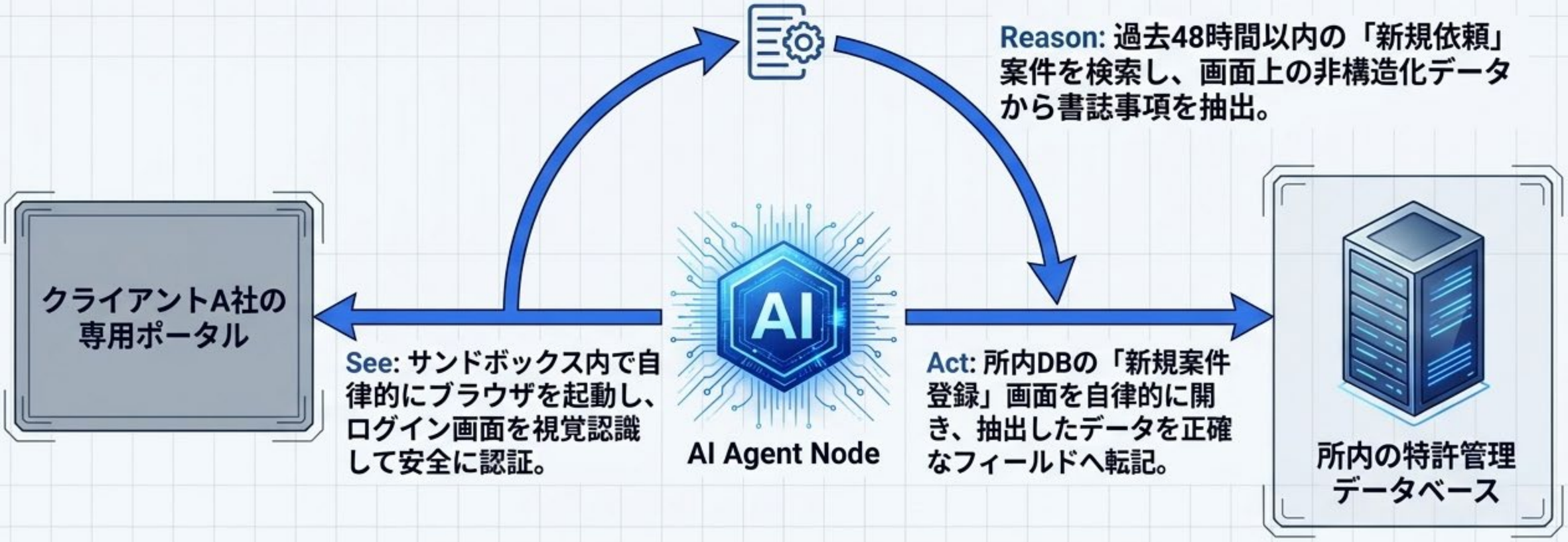
明示的なユーザー確認 (Explicit User Confirmation)

企業ポリシーに応じ、重要操作の直前でシステムを一時停止させ、人間の承認 (Require_confirmation) を強制する機能。

推奨構成: サンドボックス環境での隔離実行（仮想マシン/Docker等）の併用が強く推奨される。

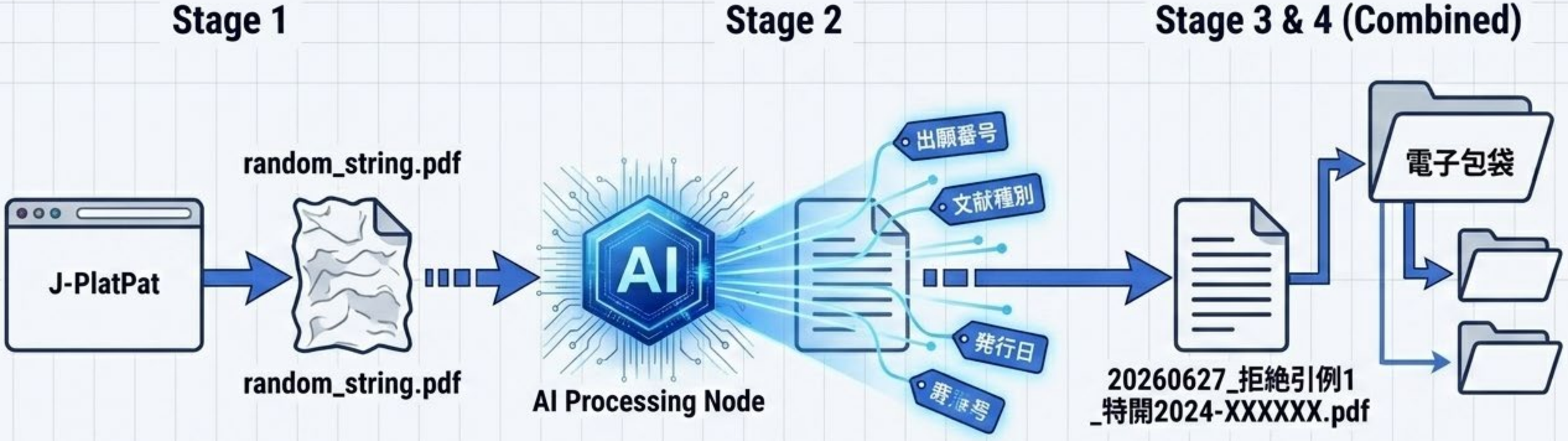
知財ユースケース 1: 閉鎖的システム間の自律的連携

API接続が提供されていないクライアント専用ポータルと所内システム間のデータ転記業務。



Key Insight: UIの軽微な変更に惑わされることなく、人間同様の柔軟なシステム間連携を実現。

知財ユースケース 2: 引例PDFの自律的取得と電子的知財格納



取得: 各国特許庁DBに自律アクセスし、該当PDFのリンクを特定してダウンロード。

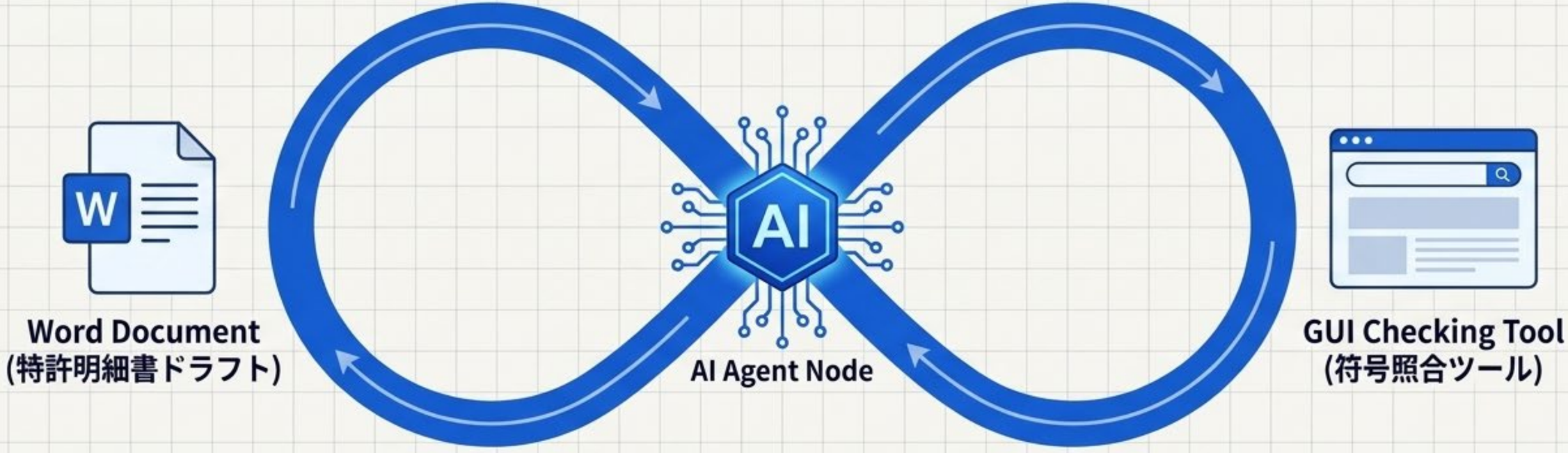
意味的解析: ダウンロード直後にLLMのテキスト処理能力でPDF内容を解析し、書誌情報を読み取る。

知的格納: 事務所の厳格な命名規則に合致するようファイル名を自動リネームし、該当案件の電子包袋フォルダへ正確に移動。

知財ユースケース 3: AIによる明細書の継続的品質監査

ソフトウェア開発における「Continuous Testing」を知財実務へ応用。

取得・入力: ドラフトテキストを全選択・コピーし、
外部ツールのフォームに貼り付けて照合実行。



Word Document
(特許明細書ドラフト)

AI Agent Node

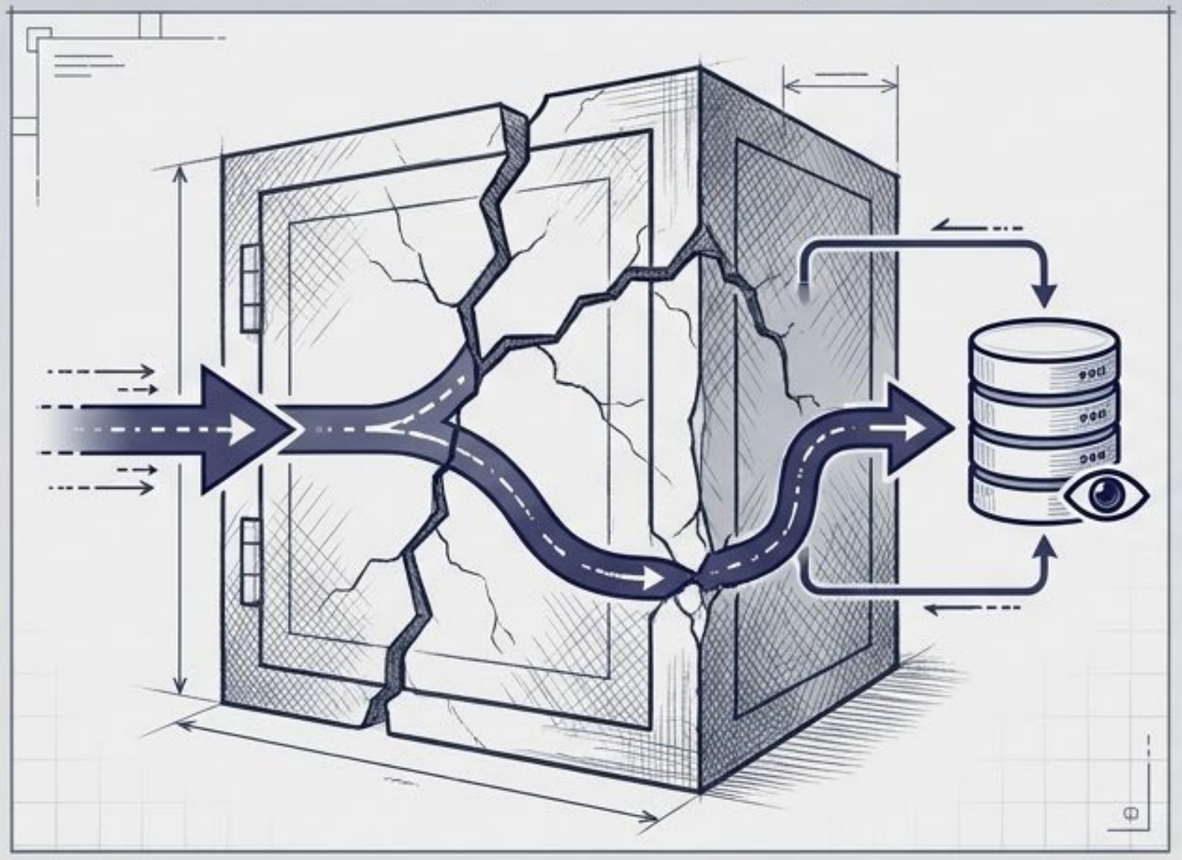
GUI Checking Tool
(符号照合ツール)

フィードバック: ツールが出力した整合性エラーを画面から読み取り、
元のWord文書末尾に品質チェックレポートとして追記。

Result: 人間の目視チェックに依存しない、バックグラウンドでの絶え間ない品質向上。

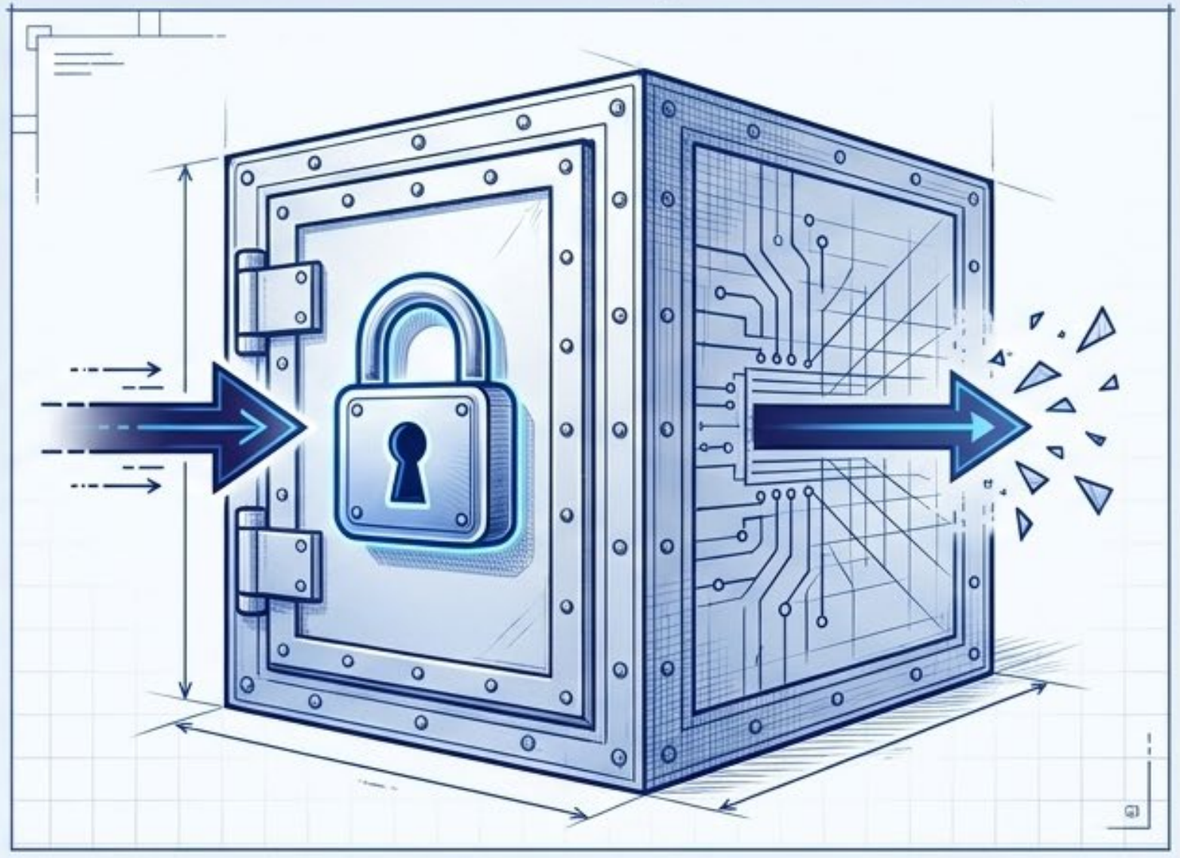
ガバナンスの絶対条件：「学習利用なし」と「保持ゼロ」の致命的差異

Standard Training Restriction (学習制限のみ)



プロンプトに入力した未公開情報が、乱用監視等の目的で一時保存される。営業秘密の漏洩・新規性喪失リスクが残存。「AIの学習に利用されない」という規約だけでは、実務上極めて不十分。

Zero Data Retention (データ保持ゼロ)



プロンプトデータが外部サーバー上に一切残存しない。知財実務において求められるのは、この「ZDR」の確実な達成である。

ZDR達成へのコンフィギュレーション・ロードマップ

Gemini API (Vertex AI) 利用開始

データキャッシング設定

無効化 (Disable)

レスポンス高速化のためのデフォルト24時間保存を、プロジェクトレベルで明示的にオフにする。

Abuse Monitoring (乱用監視ロギング)

ZDRオプトアウトリクエスト提出・承認

デフォルトの最長60日間の保存をを完全に回避するため、Googleへ公式申請を行い承認を得る。

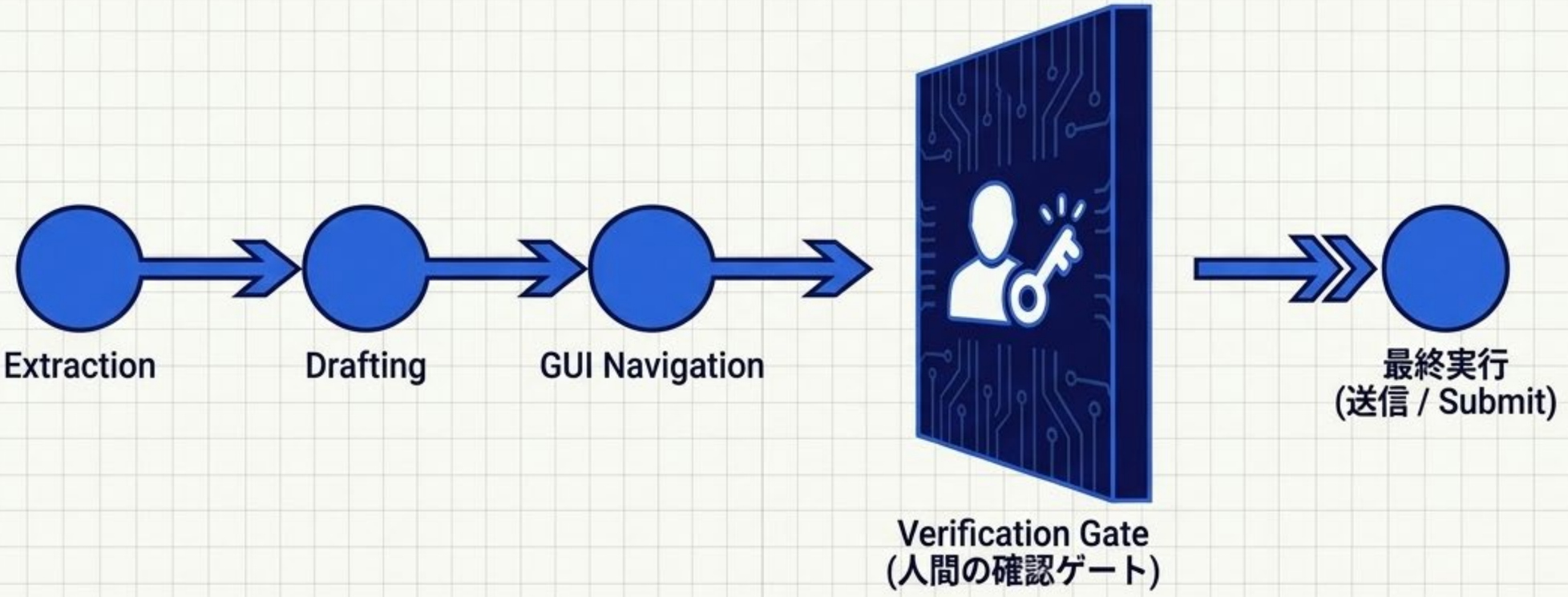
Grounding機能 (Google Search/Maps)

機密業務では利用を回避 (30日間保存のため)

事実確認ツールは強力だが、規約上30日間のデータ保存が回避不可であるため意図的に使用を避ける。

Zero Data Retention 達成 (知財業務への適用可)

JPAAガイドラインとHuman-in-the-loopの法的実装



Principle 1: ファクトチェックの義務と最終責任

日本弁理士会（JPAA）ガイドラインに基づき、AIが実行したシステム上のステータス変更や技術的解釈の妥当性は、必ず人間（弁理士等）が検証・担保しなければならない。

Principle 2: 強制的な確認プロセスの設計 (Explicit User Confirmation)

完全無人化ではなく、不可逆な操作（特許庁への送信、DBの致命的書き換え）の直前にAIを一時停止させ、人間の承認を要求するセーフティポリシーをワークフローの中核に組み込む。

個人情報保護法における法的整理：クラウド例外と委託構成

個人情報のプロンプト入力
（発明者・顧客情報）

クラウド例外（Cloud Exception）

契約および技術的担保により、事業者側で個人データへのアクセスが行われない状態を構築（第三者提供に非該当）。

委託構成（Delegation Structure）

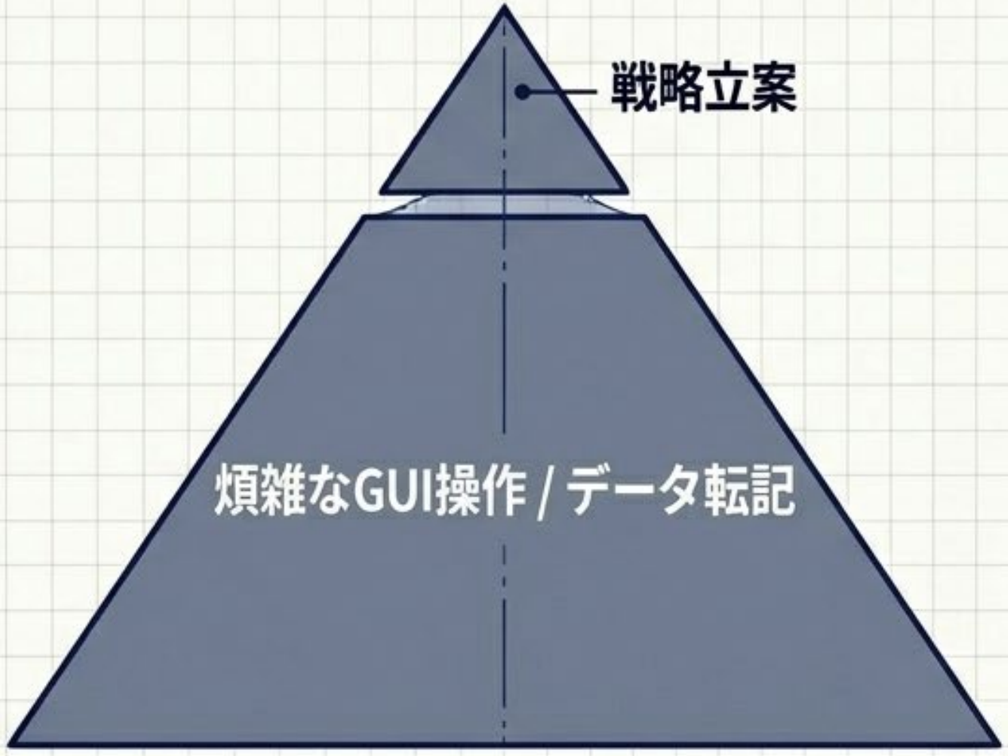
「委託」の例外規定を適用。ただし、事業者のAI学習目的での利用が規約で許可されている場合は委託範囲の逸脱となる。

Vertex AI Enterprise Agreement（エンタープライズ契約）

モデル学習への利用拒否（Training restriction）が明示され、自社データのコントロール権を技術的・契約的に担保できる環境の選択が法令遵守の大前提となる。

知財パラダイムの転換：AI協働による高付加価値業務への回帰

従来の実務構造



AI協働時代

Gemini 3.5 Flash「Computer Use」の真の価値は、自動化そのものではなく、知財専門家から「作業」を奪い、「思考」の時間を返還することにある。ZDRの技術的担保とHuman-in-the-loopの倫理的運用を両立させた堅牢なアーキテクチャの下で、弁理士は人間の創造性が不可欠な高度な高度な専門業務へとリソースを集中させる。真の知財DXが、ここから始まる。