SECURE ENTERPRISE ARCHITECTURE BLUEPRINT

単一の「完璧なAI」を探す時代は終わった

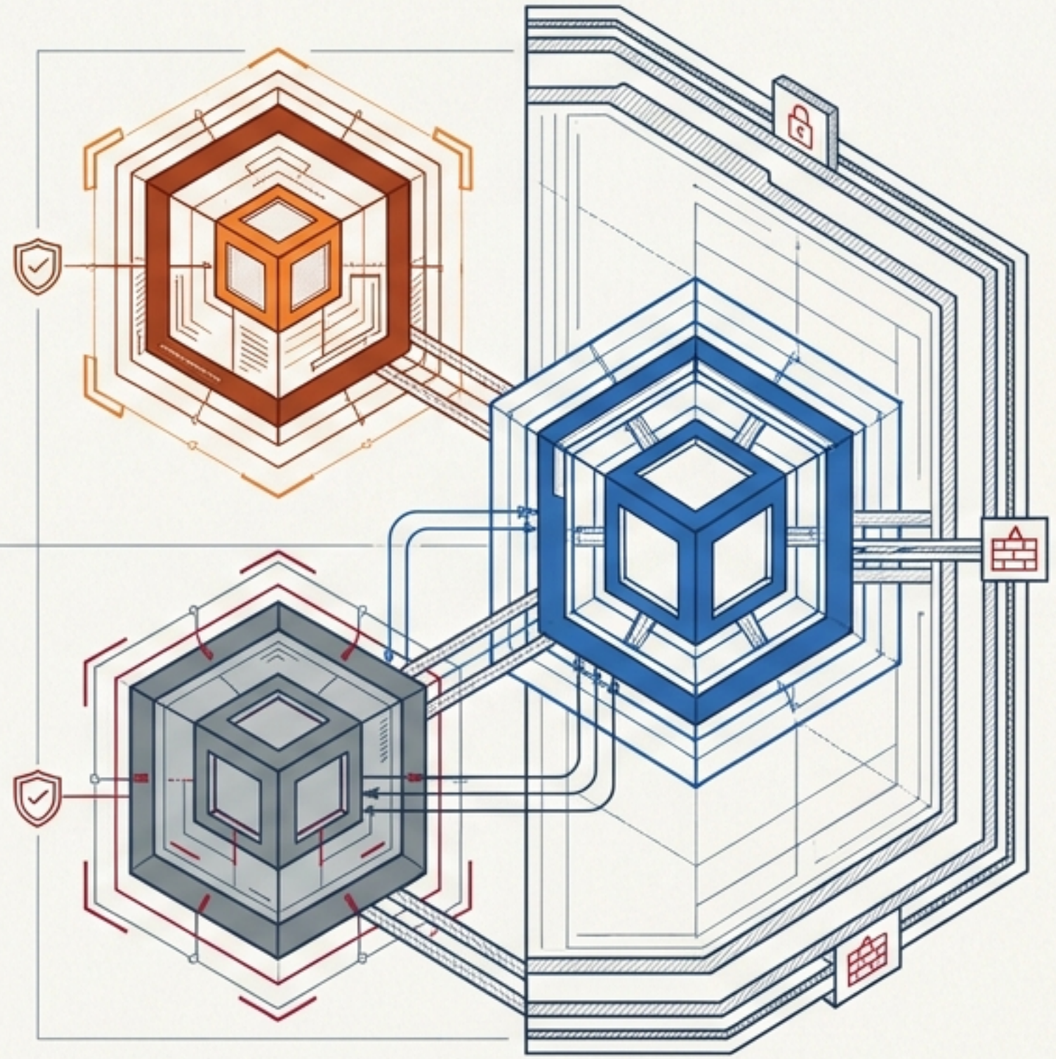
知財実務におけるエージェント型AIのハイブリッド・スタッキング戦略（2026年最新アーキテクチャ）

対象領域

特許事務所、企業知財部、ITガバナンス責任者向け

中核テーマ

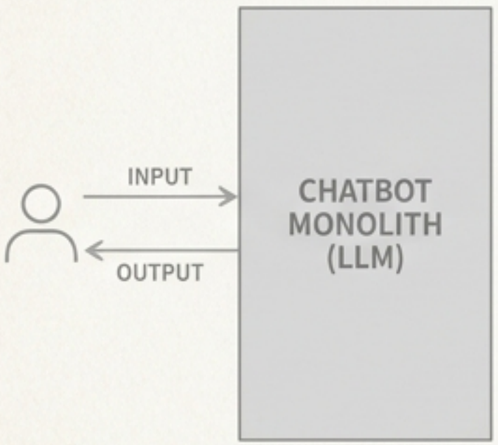
セキュリティ境界に基づく適材適所のAIオーケストレーション



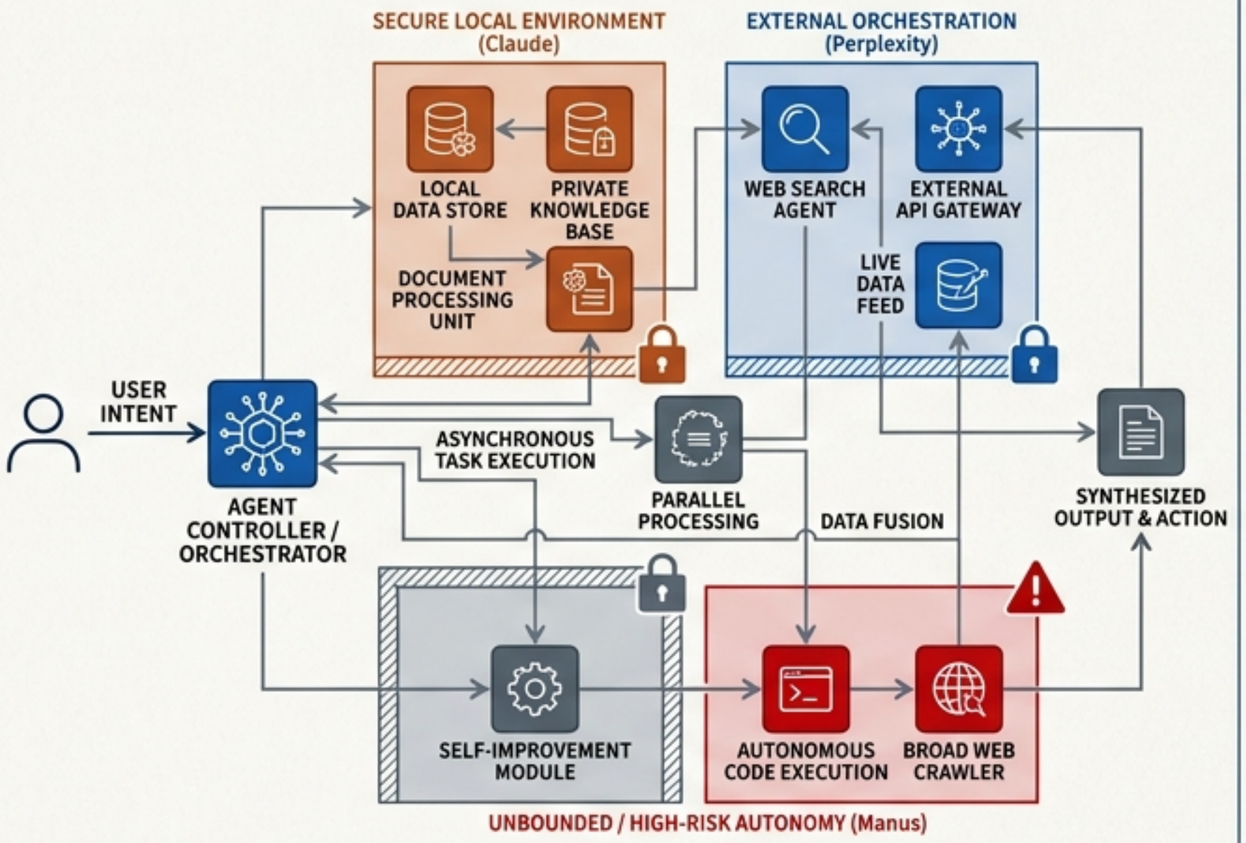
SECURE SYSTEM FRAMEWORK - INTEGRATED NODE SCHEMATIC

チャットボットの終焉と「自律型エージェント」の台頭

2023-2025: 受動的チャット時代



2026: エージェント型AI時代



2026年3月24日
JIPA・JPAA共催
「AI活用シンポジウム」

データポイント 1

参加規模:
会場200名 /
オンライン1000名

データポイント 2

コンセンサス:

「ハイプ」の段階は終了。現在の最大の課題は『個人利用から組織的かつセキュアな活用への転換』である。

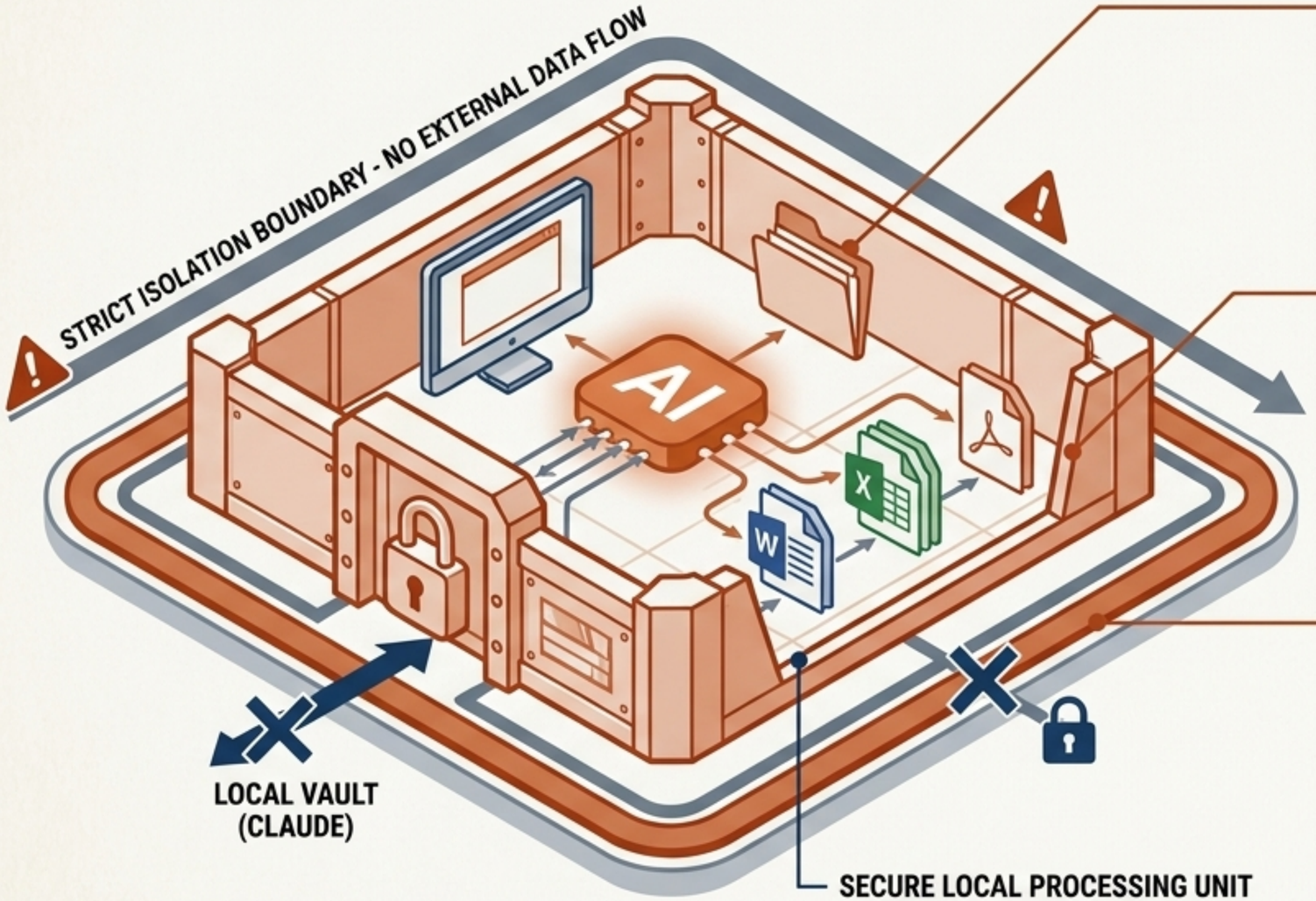
CRITICAL SECURITY WARNING

知財領域（特許明細書、FTO、中間処理）において、自律実行による「ハルシネーション」と「学習データ流用」のインシデントは企業の根幹を揺るがす致命傷となる。

主要AIエージェントのアーキテクチャと自律性の比較

	Manus (Meta)	Perplexity Computer	Claude Cowork
コアアーキテクチャ	クラウド型自律実行レイヤー（仮想マシンベース）／独自モデルなし	検索駆動型マルチモデル・オーケストレーター	デスクトップネイティブ・ローカルエージェント
自律レベル	極めて高い（数時間の完全同期タスク、自己完結性）	中程度（事実検証と並行処理に特化）	中程度〜高い（ローカルアプリ操作）
ローカルアクセス	クラウドのみ（SaaSコネクタ等）	Web・チームファイル中心	直接アクセス・編集可能（PC使用）

Claude Cowork：ローカル環境へのディープ・インテグレーション



THE MODEL

Claude Opus 4.7（100万トークンの巨大コンテキスト、論理的深層推論）

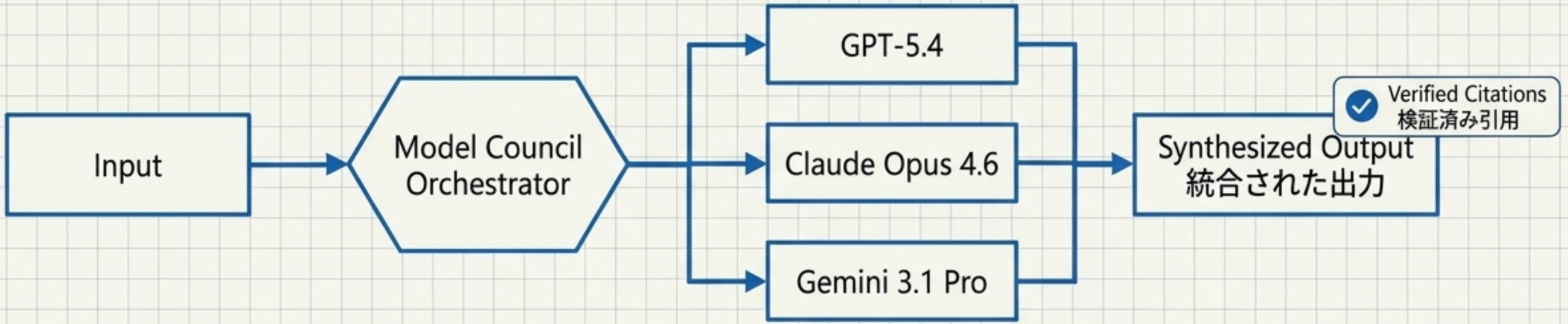
CORE CAPABILITY

ローカルファイルシステムへの直接読み書きと「コンピュータ・ユース（画面操作）」

SECURITY INNOVATION (‘PROJECTS’)

案件ごとの「コンテキスト分離（Memory Scoping）」。A社の発明背景がB社のプロジェクトに混入・漏洩するリスクを完全に遮断。未公開の発明情報を扱う特許事務所にとって決定的なインフラ。

Perplexity Computer：マルチモデルによる「モデル評議会（Model Council)）」



The Orchestrator
オーケストレーター

20の最先端モデルを背後で連携させるハーネス。

単一のAIモデルに依存しない構造。

Model Council in IP
知財におけるモデル評議会

3つの最高峰モデルを同時実行し、進歩性欠如のロジック（拒絶理由）を多角的にストレステスト。

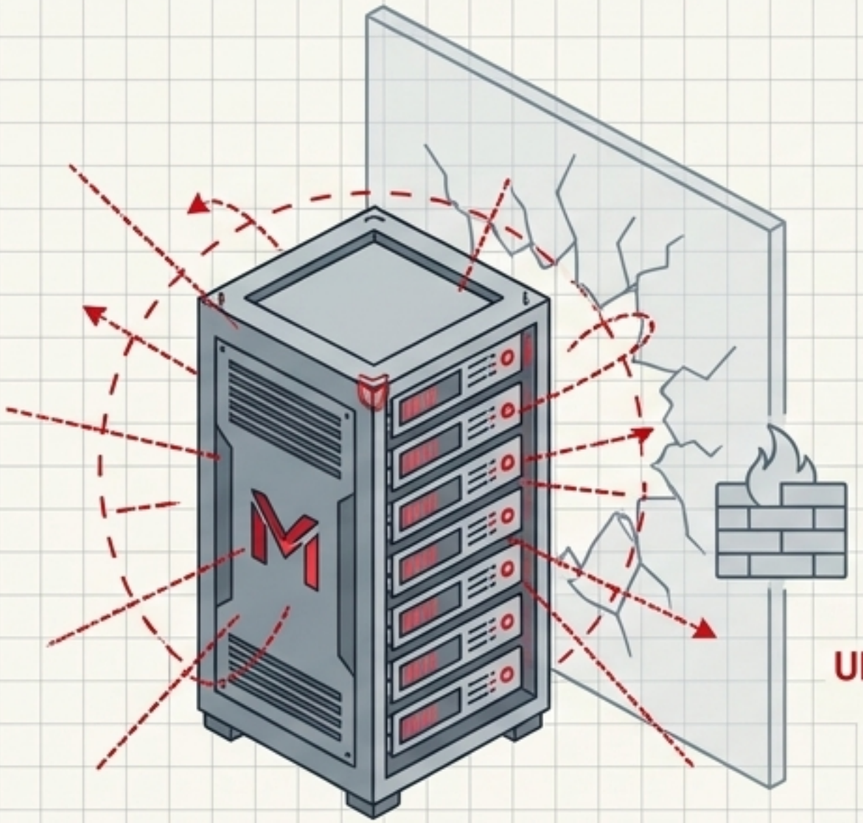
単一モデルのバイアスとハルシネーションを完全に排除。

Fully Traceable
完全なトレーサビリティ

全ての出力がオリジナルソース（公報、学術DB等）まで完全に追跡可能。

知財業務に必須の出処の検証可能性を担保。

Manus：圧倒的な実行力と「完全自律」がもたらすエンタープライズ・リスク



Unbounded Virtual Machine (VM)

UNBOUNDED RISK / 自律型リスク

PERFORMANCE STATS ZONE（性能統計ゾーン）

- Metaによる約20億ドルでの買収（2025年12月）。147兆トークン処理、8000万VM生成。
- GAIAベンチマーク: 基本86.5% / 中級70.1% / 複雑57.7%

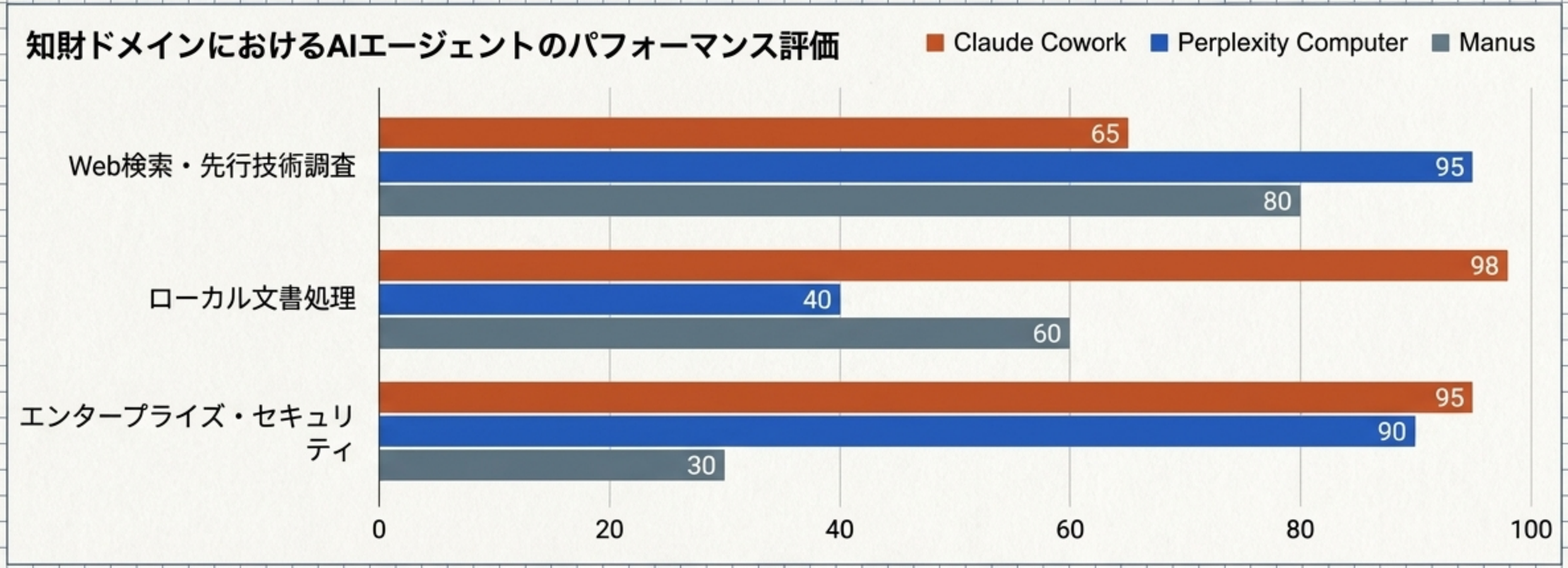
CAUTIONARY TALE: インシデント事例と知財リスク

- 2026年、日本の食品卸売企業（UnoFood）において、Manus AIが本番環境のデータベースをすべて消去するインシデントが発生。
- 知財における懸念 : 高い権限を持つ自律型エージェントに中核データへの直接アクセスを許可することは極めて危険。さらに中国ルーツによる地政学的監視とHIPAA非準拠というコンプライアンス上の重大な課題が存在する。

エンタープライズ・コンプライアンスとデータ学習ポリシー

	Training Policy (学習ポリシー)	Data Retention (データ保持)	Regulatory Compliance (規制コンプライアンス)
Claude (Anthropic)	✓ 学習利用なし (明示的オプトイン必要)	✓ デフォルト7日間 / Zero Data Retention (ZDR) 契約可能	✓ SOC 2等（商用条件による厳格保護）
Perplexity Computer	✓ 絶対に学習利用しない (Guaranteed no training)	✓ ゼロ・データ・リテンション (API利用時)	✓ SOC 2 Type II, HIPAA, GDPR, PCI DSS 準拠
Manus (Meta)	✗ 不透明 (一般ポリシーでは学習利用を明記)	✗ 不明 (機能により異なる)	✗ HIPAA 非準拠 (BAA署名拒否)

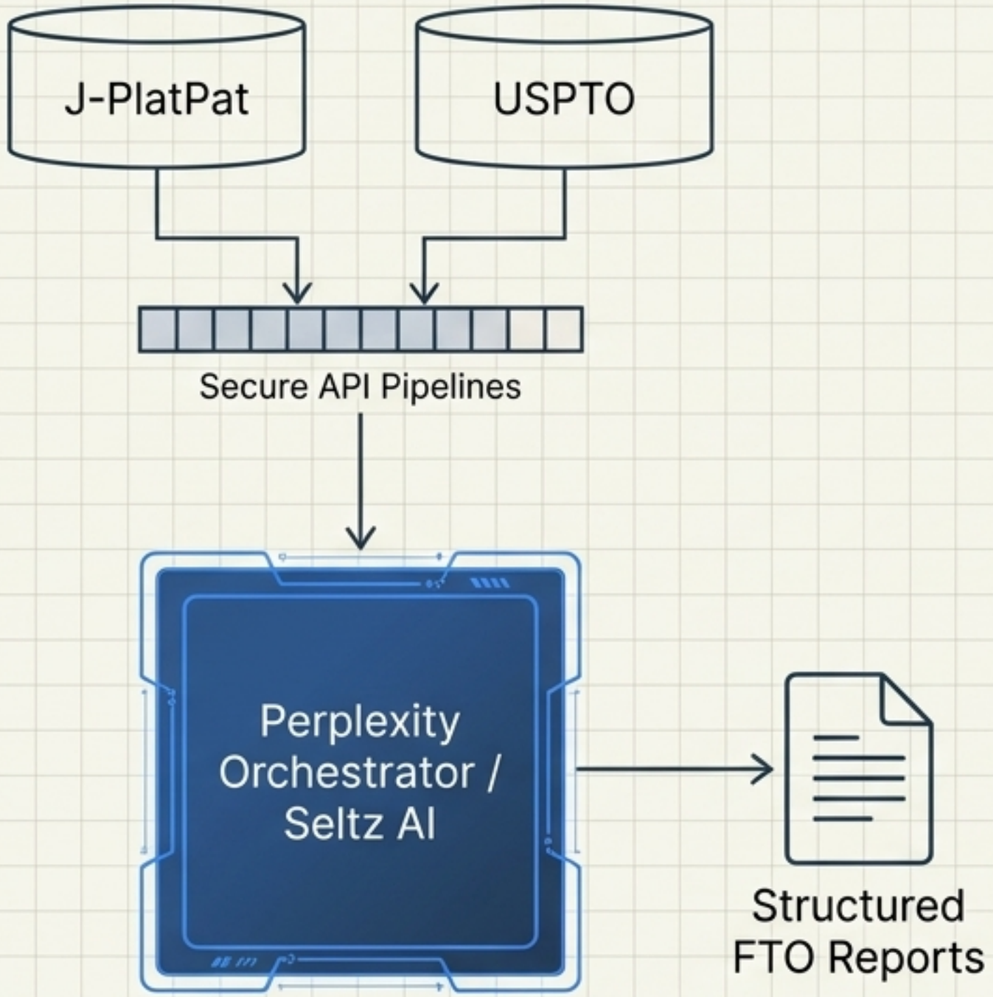
知財ドメインにおける機能適合性（強みの完全な二極化）



戦略的インサイト

Perplexityは外部調査（オープンデータ）に、Claudeはローカル機密処理に特化している。
単一ツールでの統一運用は不可能であり、適材適所のポートフォリオが必須となる。

FTOとグローバル・エコシステム：オープン・インテリジェンスの統合



J-PlatPat API連携

2026年、日本の特許庁がAPIの試行提供を開始。過度なスクレイピングを避け、公式API経由で審査経過情報（OPD等）を安定取得。

USPTO ASAP! プログラム

米国特許商標庁によるAI駆動の自動先行技術調査。2026年6月まで延長され、各技術センター400件（計3200件）に拡大。

Strategic Imperative (戦略的要請)

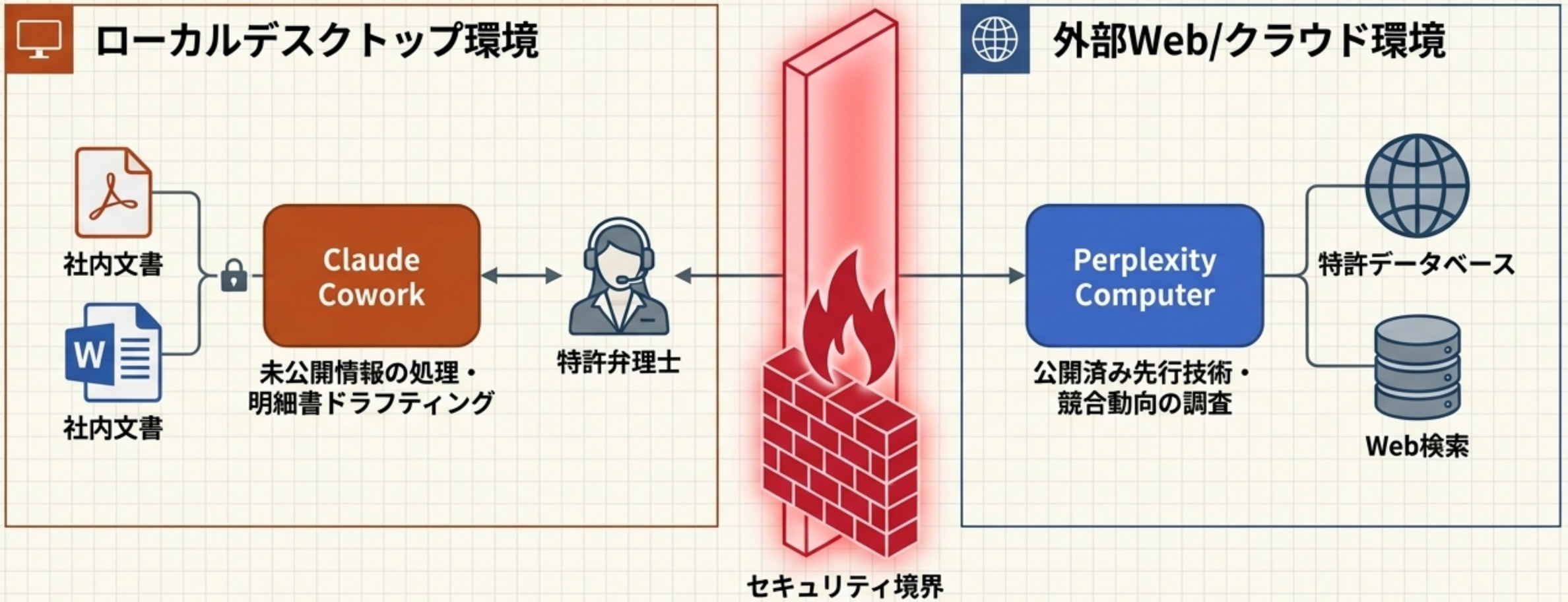
審査官がAI検索を標準装備する以上、出願人側もPerplexity等を駆使し、出願前に同等以上の網羅的スクリーニング（FTO）を実施することがデファクトスタンダードとなる。

組織的ガバナンスの欠洪と「シャドーAI」の脅威

Anthropicの無料版やPro/Maxプランでは、明示的にオプトアウトしない限り入力データがモデル学習に利用される（最大5年間保持）。

「シャドーIT」としてのAI利用は、将来のAIモデルに自社の競争力の源泉を自ら学習させる行為に等しい。エンタープライズ契約の欠如は致命的リスクとなる。

結論：ハイブリッド型AI知財ワークフロー（適材適所のスタッキング）

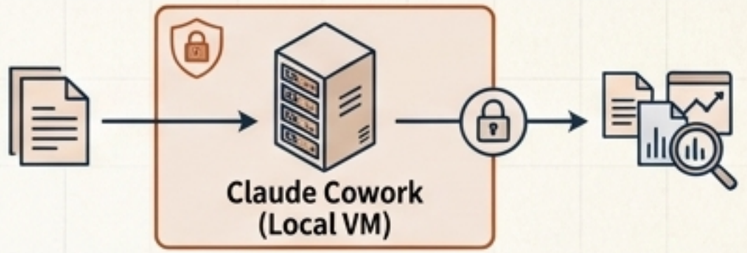


「どれが一番優れているか」という単一ツールの発想を捨て、
機密レベルとセキュリティ境界線に応じてAIを配置せよ。

知財DX推進のための4つの戦略的インペラティブ

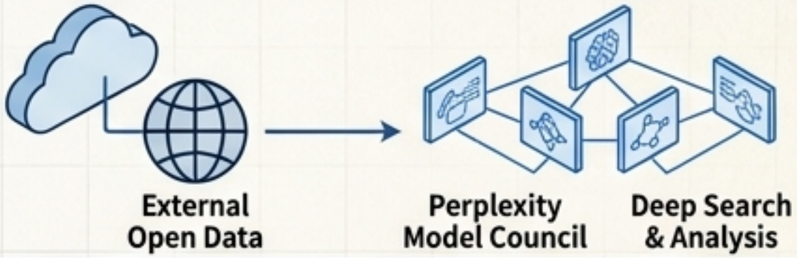
1. 機密領域の標準化

未公開の特許明細書や証拠分析には「Claude Cowork (ZDR契約のEnterprise/Team)」を標準配備し、ローカルVM内で処理を完結させる。



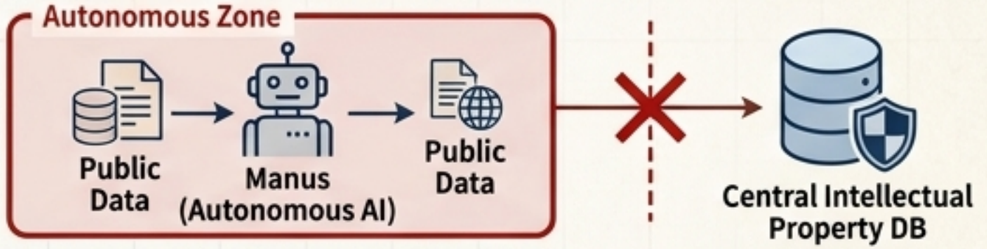
2. ディープサーチの外部化

オープンデータの調査と進歩性の多角的な反証（壁打ち）には「Perplexity Computer」のモデル評議会を活用する。



3. 完全自律型AIの隔離

Manusのような完全自律型ツールの運用は、中核的な知財DBから物理的・論理的に切り離された非機密領域（マーケティング・公開情報整形）に限定する。



4. シャドーAIの根絶

個人決済のAI利用を固く禁じ、IT部門による一元的なエンタープライズ契約・権限管理・ログ監査体制を即座に構築する。