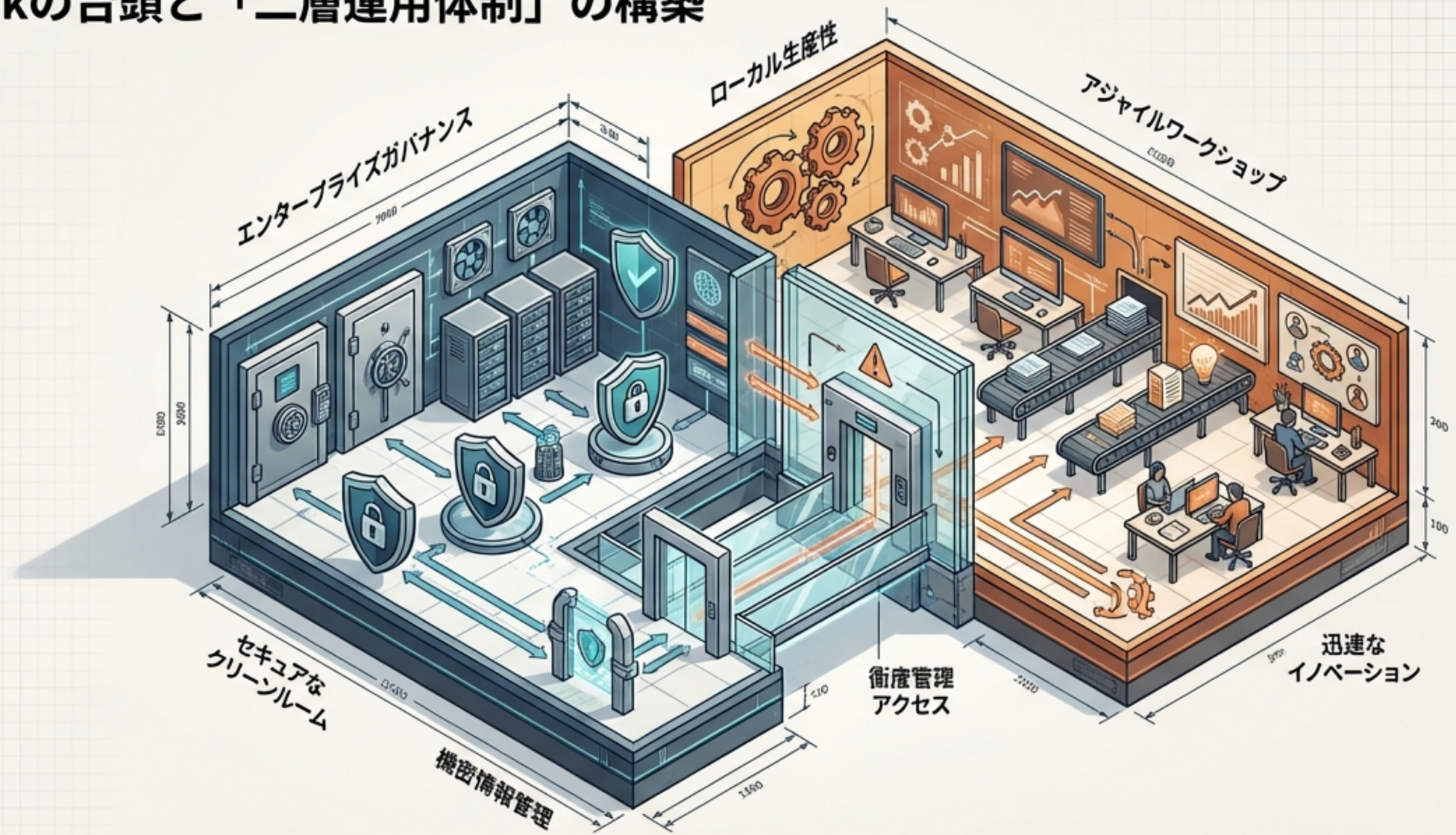
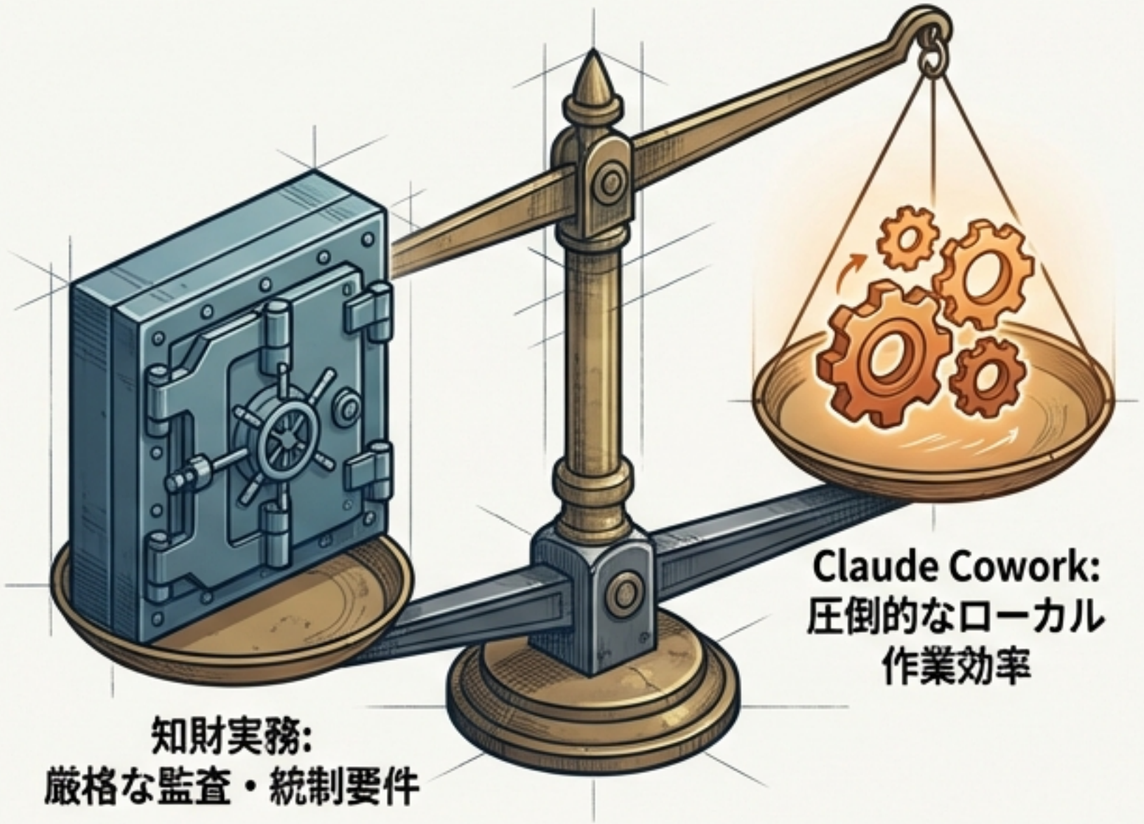
知財業務における生成AIのアーキテクチャ設計

Claude Coworkの台頭と「二層運用体制」の構築



エグゼクティブサマリ：生産性と監査証跡のジレンマ



Claude Coworkはローカル環境で自律的に稼働する強力なエージェントですが、監査ログやCompliance APIに非対応です。公式ドキュメントでも「規制対応や厳格な監査証跡が必要な業務には不適」と明記されています。

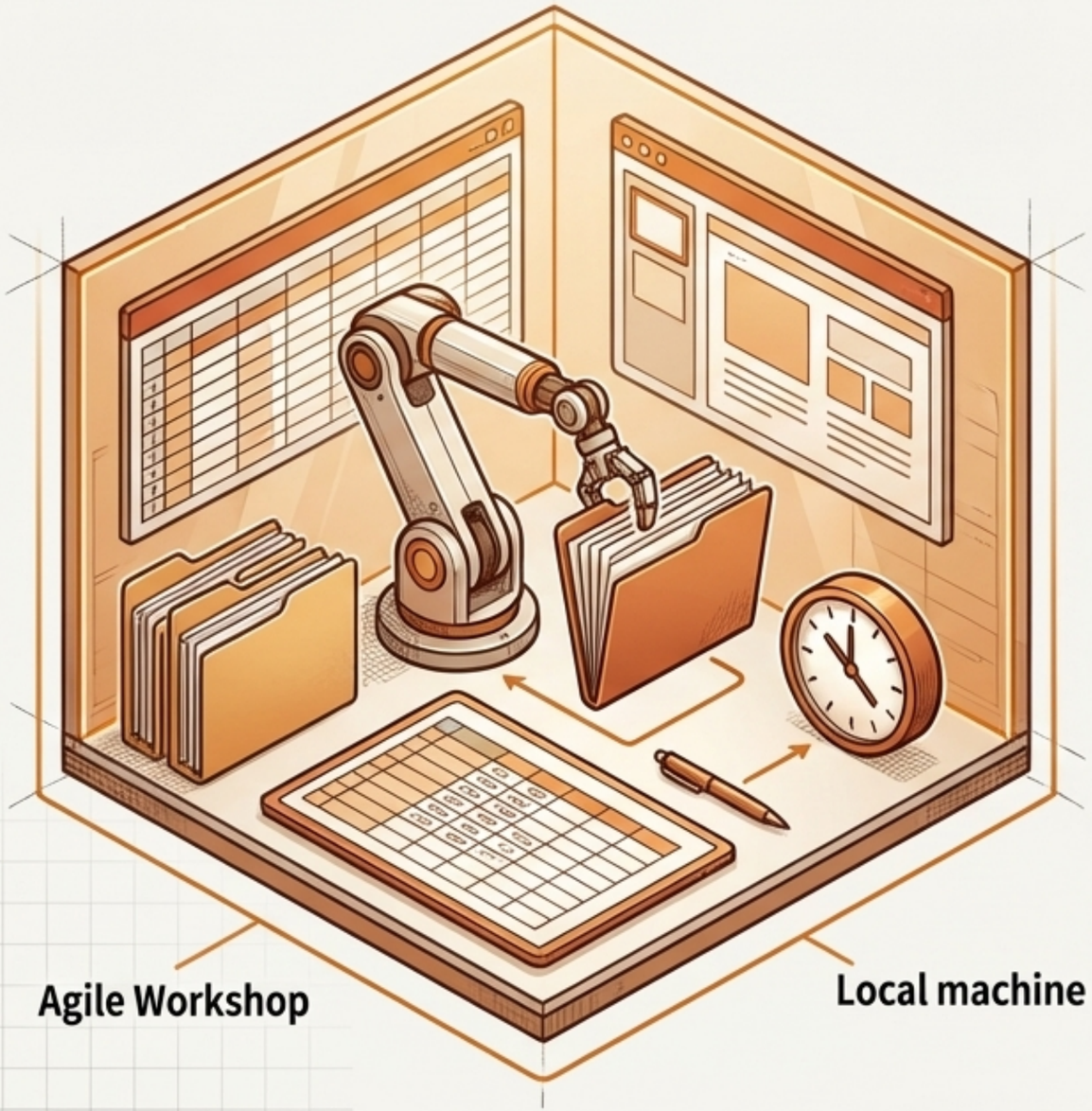
本レポートの結論：

知財部門においては、AIを単一のツールとして導入するのではなく、用途別に環境を分離する**「二層運用体制」**が不可欠です。

1. 統制型基盤（Microsoft/Google/OpenAI等）
＝ 機密案件・証跡必須業務

2. Claude Cowork（ローカル隔離環境）
＝ 汎用的な資料整形・ドラフト作成

Claude Coworkの正体：「端末内」で完結する自律型エージェント



従来の「チャット型AI」から、ローカルツールを直接操作する「エージェント型」へ進化。

中核機能：

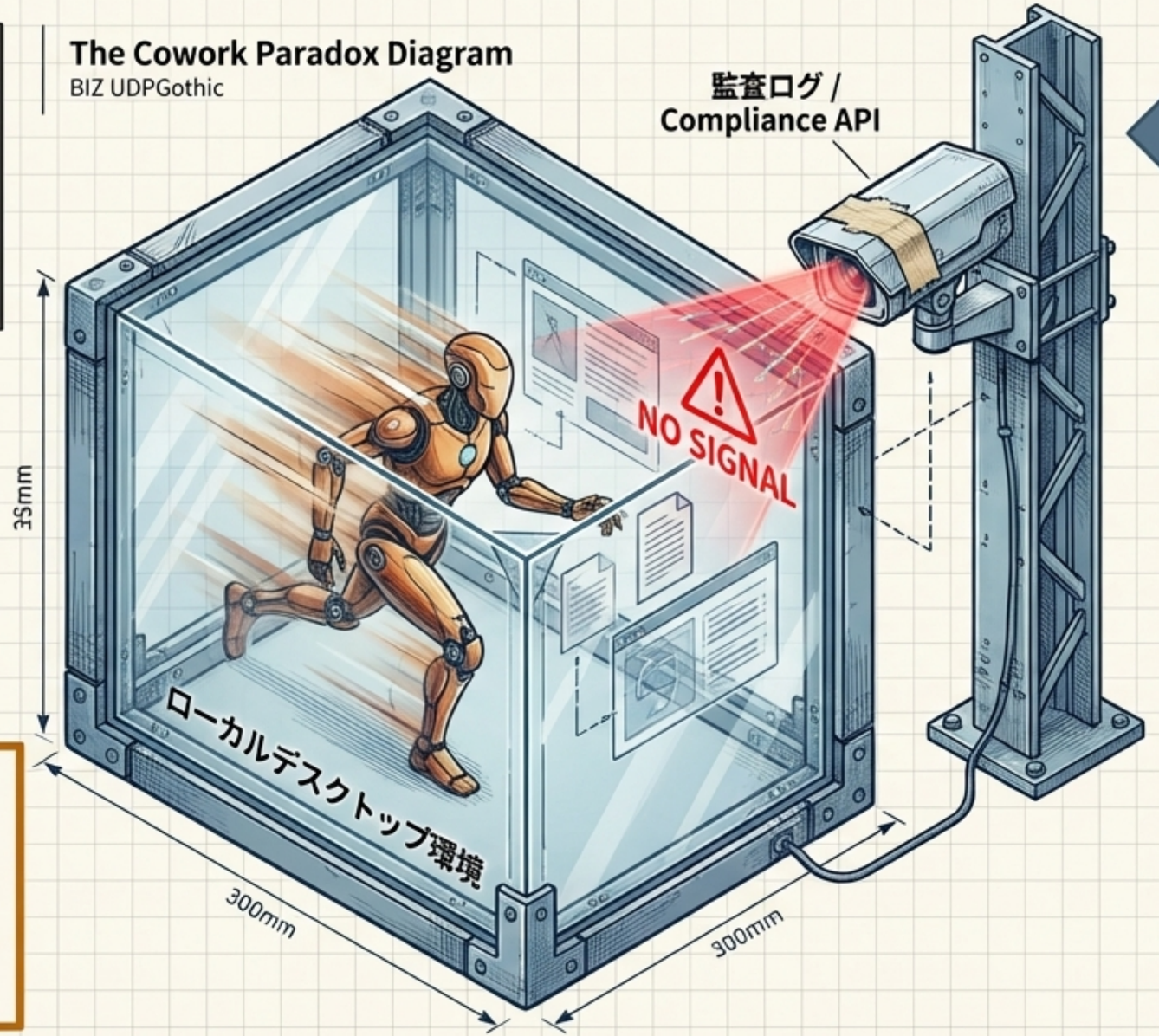
- ローカルファイル直接アクセス：端末内のExcelやPowerPointを直接読み書きし、成果物を生成。
- 長時間タスクの実行：会話のタイムアウトに阻まれず、複数サブエージェントが協調して作業を継続。
- スケジュール実行：指定時間 (/schedule) での自動起動とバッチ処理 (※PC起動・アプリ展開時のみ)。

知財業務での強み：膨大な先行技術文献のローカルフォルダ内での比較表化や、明細書構成案の高速ドラフト作成。

知財コンプライアンスの空白：見えない作業者（Invisible Worker）

致命的な制約:

Coworkの活動は、エンタープライズ水準の監視網から完全に抜け落ちます。



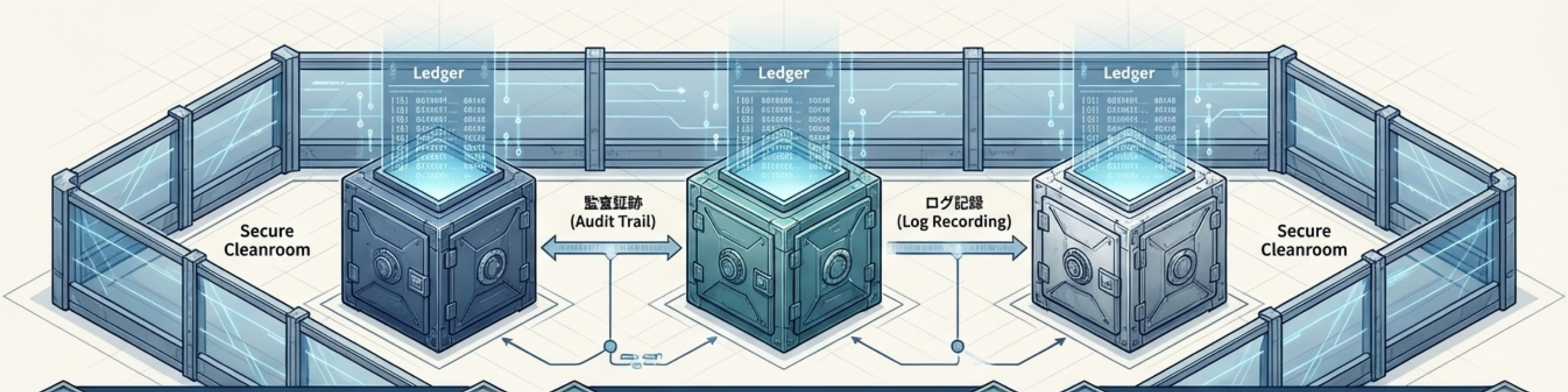
公式の警告:

会話履歴は端末ローカルにのみ保存され、データエクスポートや監査ログには記録されません。

知財実務への影響:

侵害評価や拒絶理由対応など、「後日、判断根拠を説明できること（説明責任）」が求められる業務において、証跡を残せない環境での作業は、、コンプライアンス上の重大なリスクとなります。

エンタープライズAIの対策：統制と証跡を担保するクラウド環境



Microsoft 365 Copilot

既存のテナント境界とPurview（感度ラベル/暗号化）を完全に継承。180日間の監査ログ保持と非蓄積型のデータ統合（フェデレーション）を提供。

Microsoft

Google Gemini (Workspace)

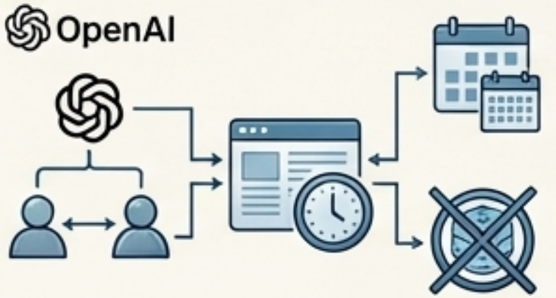
DLP/IRM等の既存保護を前提に動作。管理コンソールからのログイベント参照とReporting APIによる監査機能。

Google Workspace

ChatGPT Business / Enterprise

セキュアな共有ワークスペースとSAML SSO。Compliance Logs Platformを通じた最大30日のログ保持とAPI追跡。業務データの学習利用を原則除外。

OpenAI



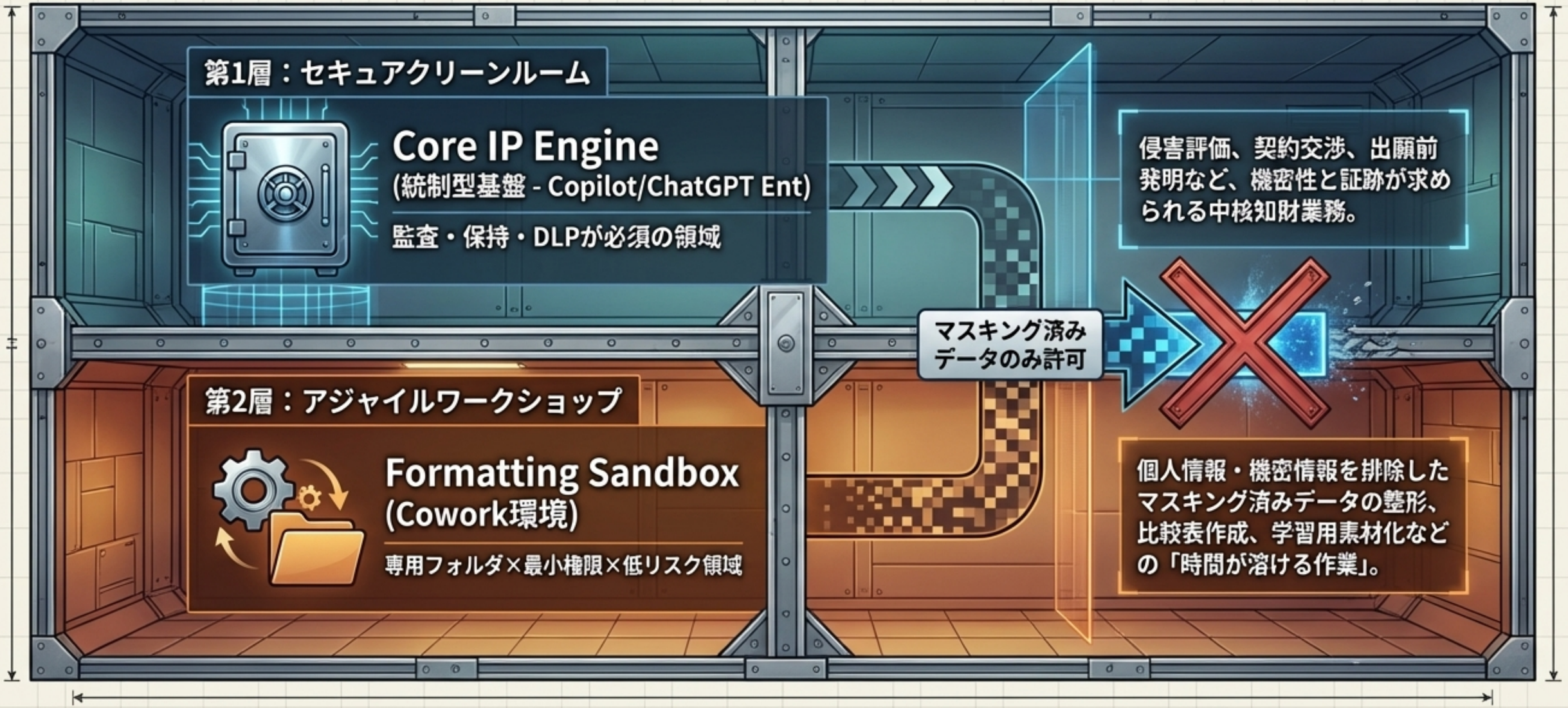
ガバナンス＆機能 比較マトリクス

ツール	データ主権と監査ログ	既存権限の継承・アクセス制御	コラボレーション環境	拡張性リスクの低さ
Claude Cowork	○	◐ Local only	○ Local desktop	○ Unvetted MCPs
MS 365 Copilot	●	● Purview	● M365	◔ Managed Connectors
Google Gemini	◔	● Workspace	● Docs/Drive	◔
ChatGPT Enterprise	● API	◐ SSO/Roles	◔ Workspace	◐ Internal connections

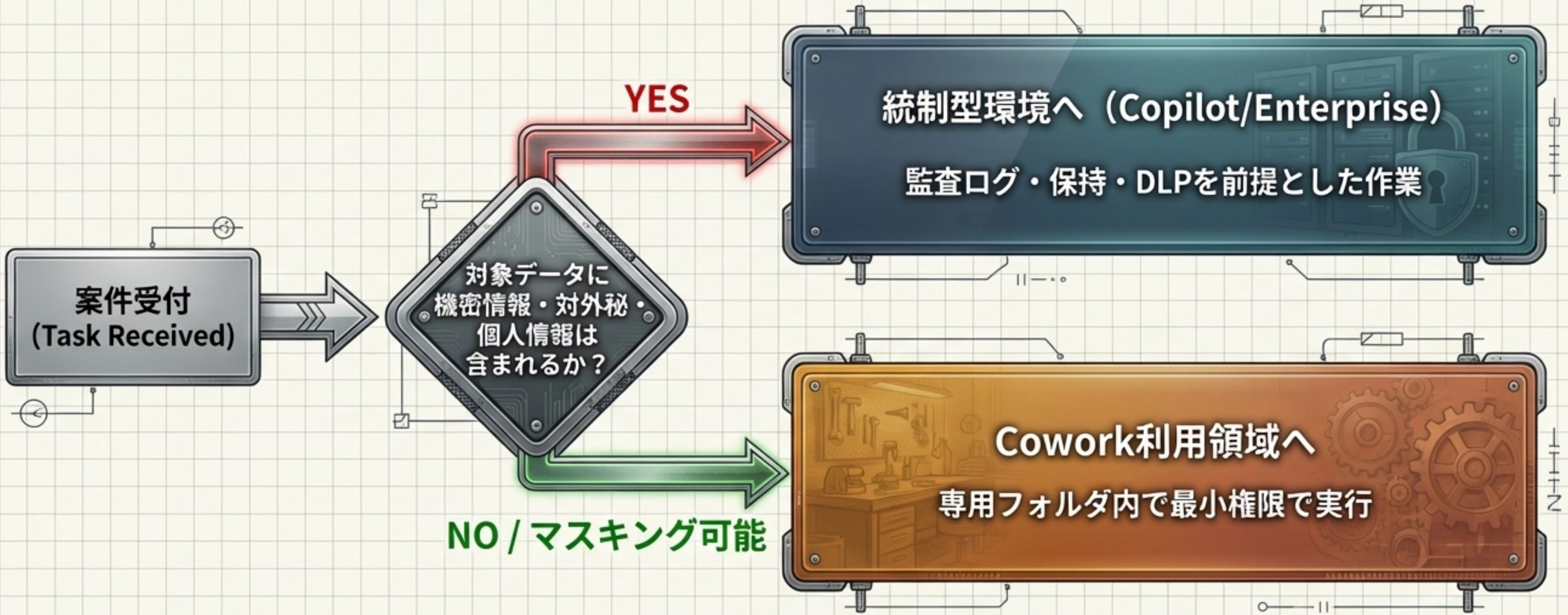
Coworkは「ローカル編集能力」で突出する反面、
「監査と統制」においてエンタープライズ要件を満たしません。

結論のアーキテクチャ：「二層運用体制」の構築

生産性と安全性を両立させる最適解は、用途に応じてAI環境を切り替える「二層運用」です。



知財タスク・ルーティング・フローチャート



デジタル庁のガイドラインが示す通り、「利活用促進とリスク管理は一体で進める」必要があります。
実行前にデータの感度を判定し、適切な処理環境へルーティングするプロセスを標準化します。

Cowork適用領域：アジャイル・ワークショップ（低〜中リスク）

1. 特許調査 / 先行技術調査 (一部) :

統制環境で取得した原文を、Coworkの専用フォルダで比較表（発明特徴×文献）に高速整形。

2. 明細書作成支援（構成案）:

機密情報を含まない既存メモやマスキング済み実験記録からのたたき台作成。

3. ナレッジ共有・教育資料化:

承認済み資料のみをコーパス化し、Coworkで大量ドキュメントを体系化・FAQ生成。

FAQ

絶対ルール: 常に「専用作業フォルダ」を用意し、CoworkにPC全体の読み取り権限を与えないこと。

エンタープライズ専任領域：セキュア・クリーンルーム（高リスク）

1. FTO / 侵害分析：

誤った法解釈や監査証跡不足が致命傷になるため、原則としてログが取れる統制型環境で実行。

2. クレーム草案作成：

過度な広狭や禁反言のリスク。プロンプトの固定化と証跡保存が必須。

3. 契約書レビュー：

交渉方針の漏洩や相手方秘密情報の再利用を防ぐため、監査ログとDLPが効く環境に限定。

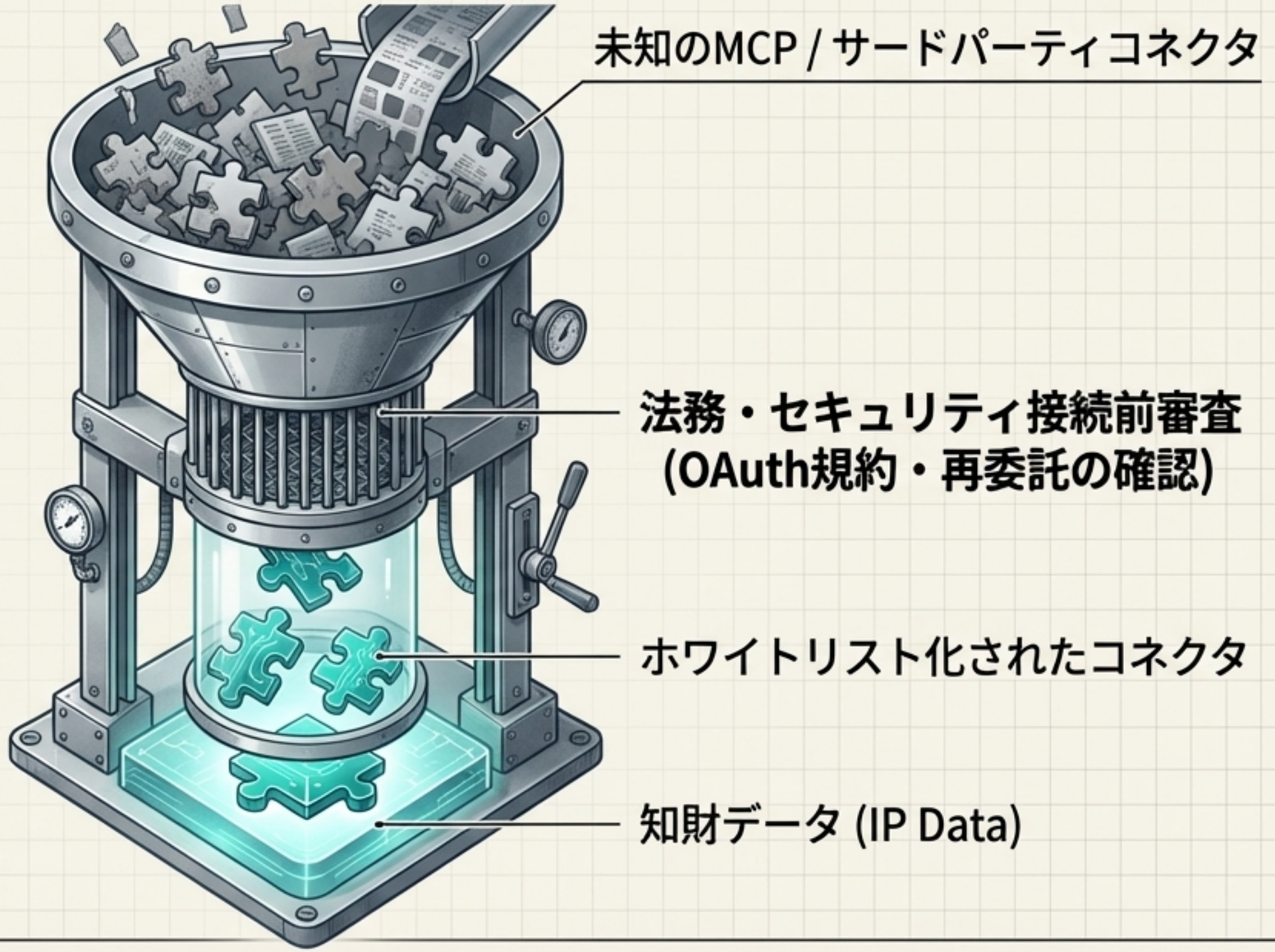
絶対ルール：係争、契約、出願前詳細など「後からプロセスを証明すべき業務」は、いかにCoworkが便利でも決して投入しない。

サードパーティ連携のリスク：MCP / プラグイン脅威モデル

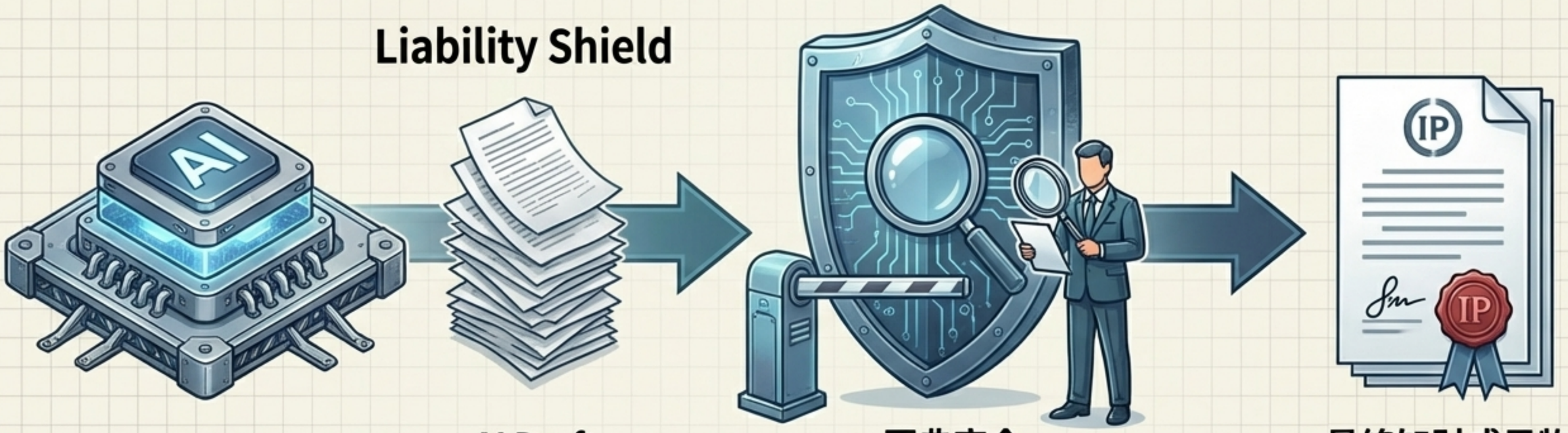
Coworkの強力な拡張性（skills/connectors）は、同時に最大の攻撃面（アタックサーフェス）となります。

コネクタは第三者が実装しており、OAuth接続時に各社のプライバシーポリシーが適用されます。

実務対策: Anthropicのディレクトリに掲載されているからといって安全とは限りません。知財部門では「接続申請 → 法務審査 → 許可リスト化」のプロセスを実質必須とする必要があります。



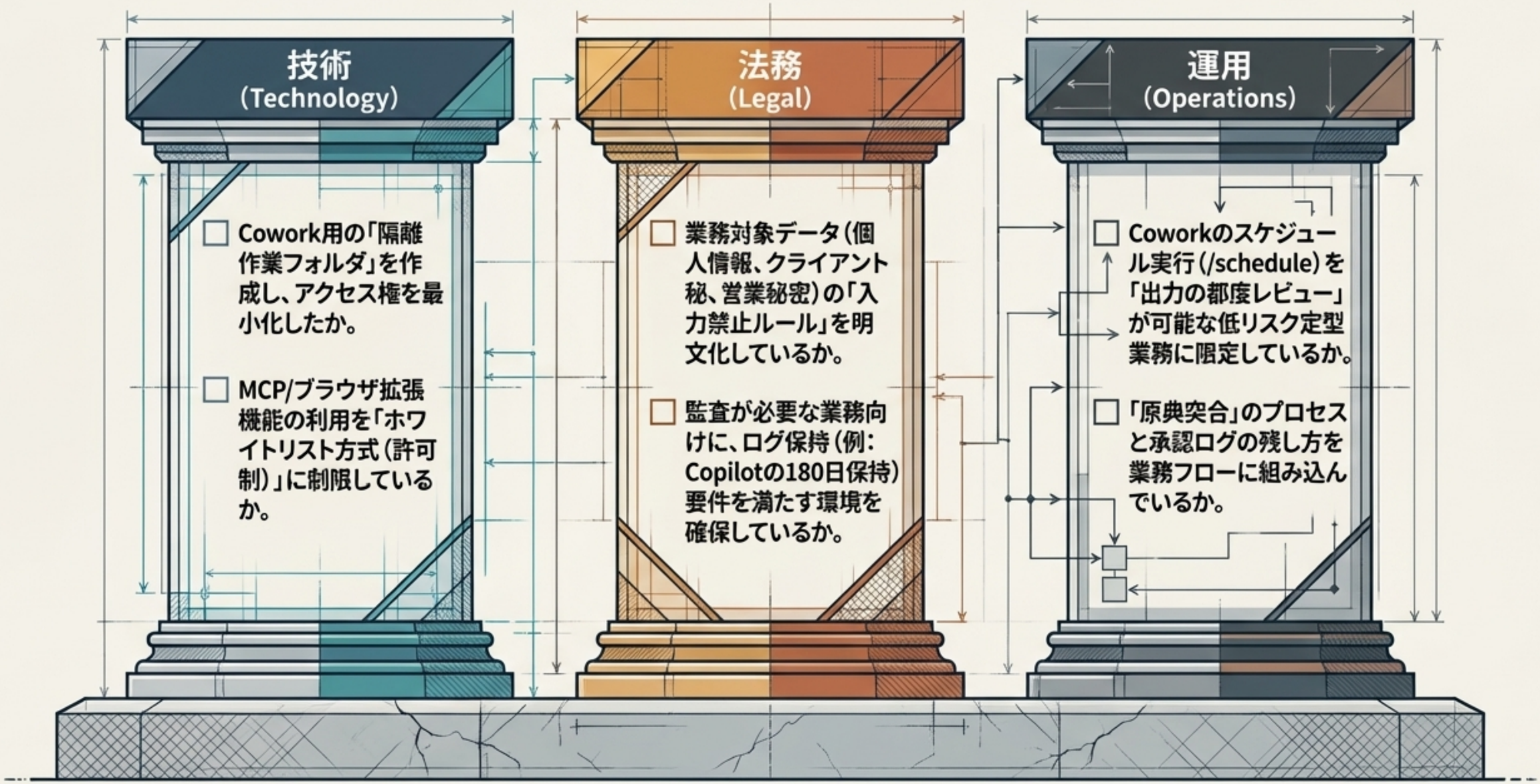
最終防衛線（Human-in-the-Loop）：弁理士の法的責任と検証ゲート



日本弁理士会のガイドライン:「生成AIの出力は正確性が保証されず、最終責任は弁理士が負う。検証なしの提供は善管注意義務違反のおそれがある。」

検証の義務化: 特に特許調査や明細書作成において、AIが出力した引用番号や文献内容は必ず「原典へのアクセスと突合」を経なければ、対外的な知財成果物として登録・提出してはなりません。

知財部門向け AI導入・実装チェックリスト



結論：知財AIアーキテクチャ 3つの絶対原則