Gemini 3.5 Flash「Computer Use」が知財実務にもたらすパラダイムシフト

エージェント型AIの法的リスクと次世代ガバナンスの設計図

効率化の代償：生成AIは「文案作成ツール」から「実行主体」へ

RPAの上位互換

- ✅・Gemini 3.5 Flashの「Computer Use」は自律的エージェント能力を保持。
- ✅・SaaS、DMS、特許庁サイトを横断し、人間と同様に画面を閲覧・操作・取得。
- ✅・先行技術調査や権利化補助の効率を劇的に向上。

制御不能な法的債務

- ⚠️・単なるチャット利用とは次元が異なるリスク。
- ⚠️・無制限なアクセスによる営業秘密の流出。
- ⚠️・意図せぬ著作権侵害と、AIによる勝手な「法的同意」の発生。

結論：知財部門におけるAIの価値は、「どこまで自動化するか」ではなく、「何を自動化しないか」を制度化できるかで決まる。

アーキテクチャの根本的差異：API連携とGUI自動化の違い

従来のAPI連携 (データ構造に基づく制御)

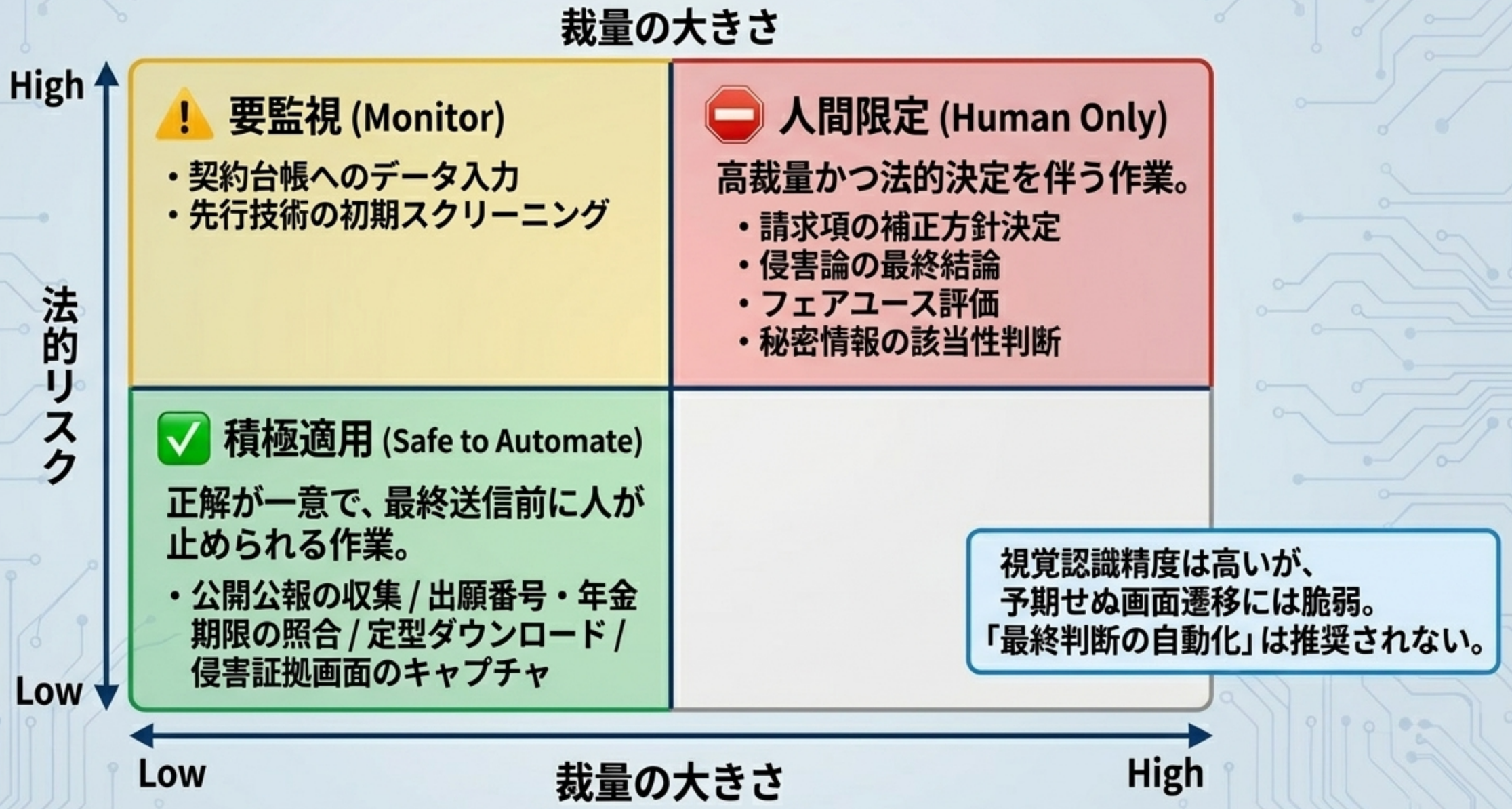
許可されたデータのみが送受信され、
既存のDLP機能が有効に機能する。

Computer Use (視覚と行動のループ)

入力要素：テキスト+直近のスクリーンショット+行動履歴。
Gemini 2.5の仕様に依拠し、Webブラウザ操作に最適化。

⚠ [SYSTEM WARNING]: GUI上に表示された秘密情報・個人情報・著作物は、意図せずとも「スクリーンショット」としてモデルの処理対象（入力）となる。これが知財・法務リスクの根本原因である。

知財業務における自動化適性マトリクス



エージェント型AIが引き起こす4つの法的脅威

特許
(Patents)

Threat

- AIは発明者になれない。自律探索が増えるほど人間の「着想」との境界が曖昧化。

Mitigation

- 人間の「創作的寄与」を証明するプロセスログの保持。

著作権
(Copyright)

Threat

- 画面読取りに伴う複製・送信。享受目的があれば法30条の4適用外。

Mitigation

- API連携の優先、または正規ライセンスの取得。

営業秘密
(Trade Secrets)

Threat

- 既存DLPの死角。画面を直接読み取り「秘密管理性」を破壊。

Mitigation

- 専用IDの使用、ワークスペース分離、システム的なダウンロード禁止。

コンプライアンス

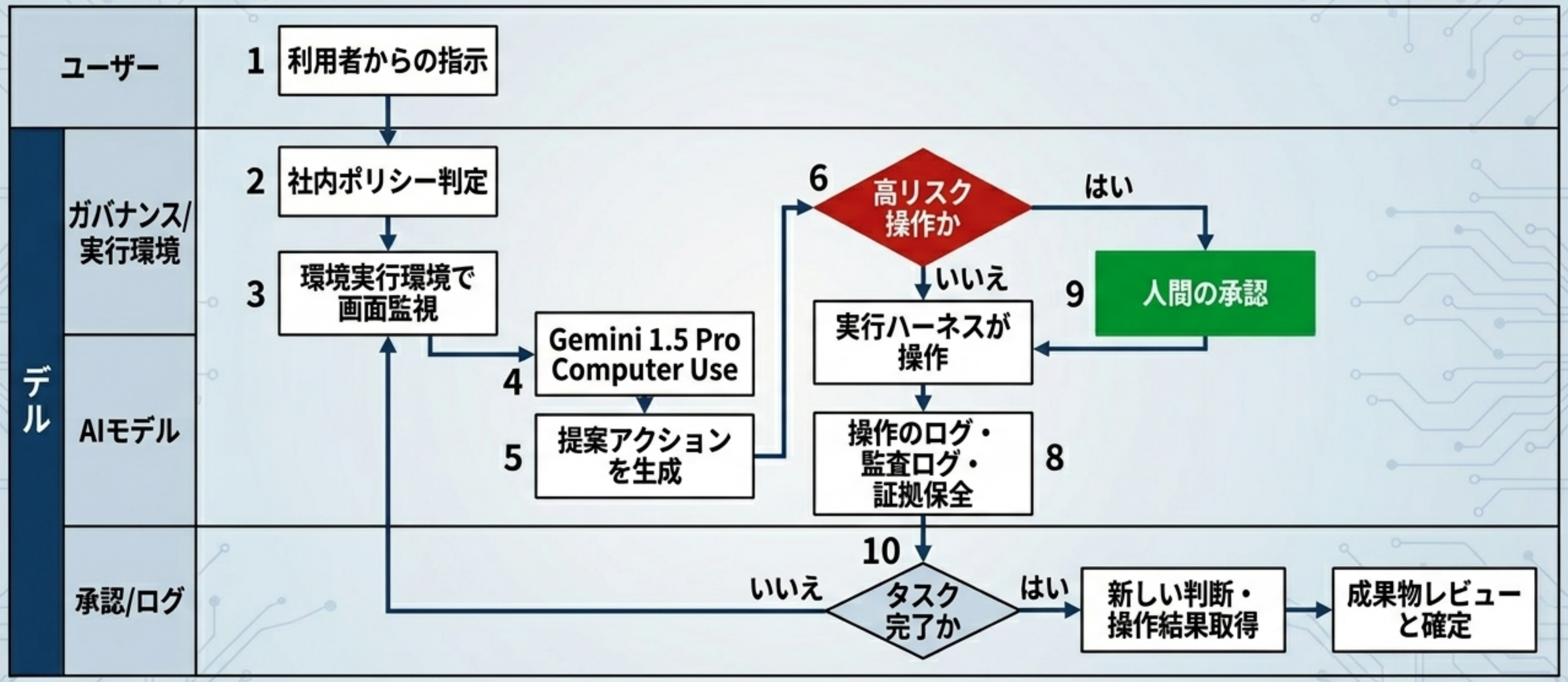
Threat

- AIによる勝手な「同意」「送信」。GDPRやAI Act違反の誘発。

Mitigation

- 高リスク操作に対する確実な「Human-in-the-Loop」の強制。

次世代ガバナンス設計：Human-in-the-Loop (HITL) アーキテクチャ



モデルに直接権限を与えず、企業側ハーネスが仲介し、送信系操作には必ず人間を介在させる。

証拠性のギャップ：監査ログを「法的証拠」に昇華させる要件

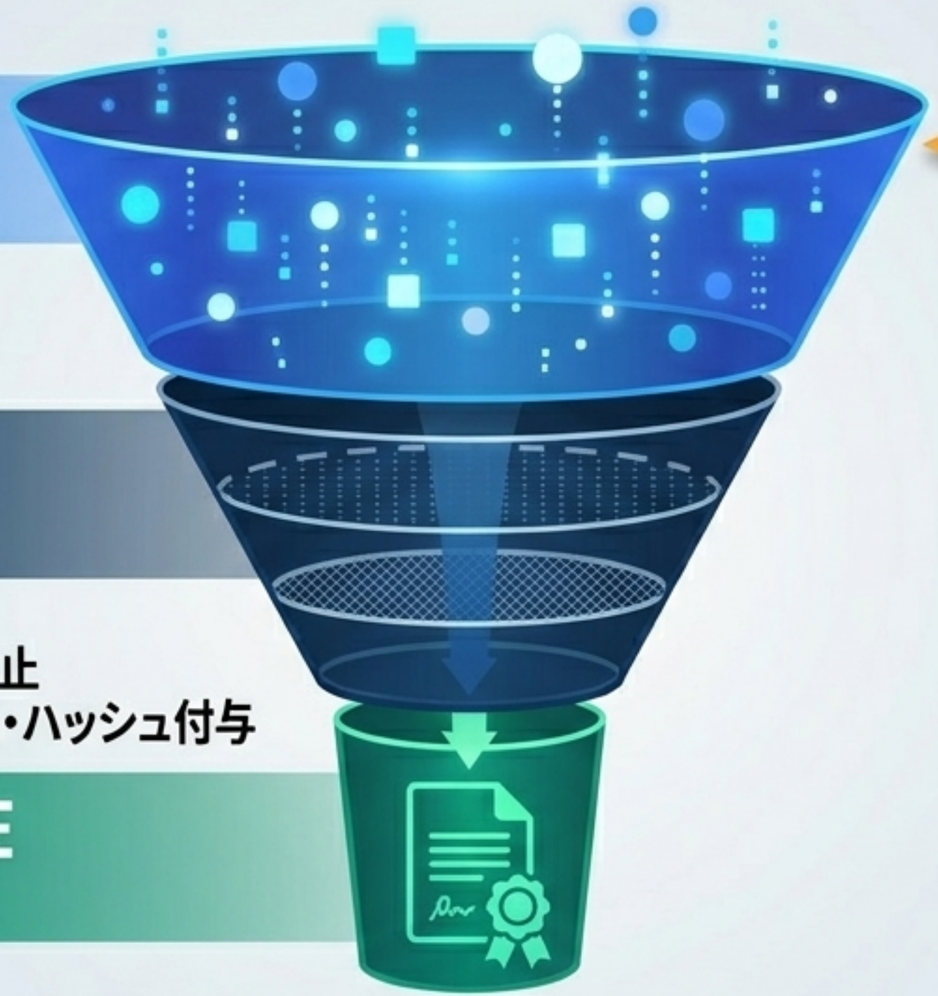
RAW DATA
(Google Cloud 基盤)

Cloud Audit Logs &
Agent Observability

THE FILTERS
(企業側の保全設計)

- SIEMへの転送
- WORMストレージでの改ざん防止
- 案件ID紐付け・担当者電子署名・ハッシュ付与

LEGAL EVIDENCE
(法的証拠)



⚠ Data Accessログは
「明示的有効化」が必須。
デフォルトでは不十分。

真正性・完全性・時系列の一貫性が担保された証拠。

「AIが勝手にやった」という抗弁を無効化し、訴訟でのDiscoveryに耐えうる設計。

エンタープライズ・アクセス制御と権限分離

NG: 危険な運用パターン

- 従業員の個人端末（ローカルPC）での直接実行
- 既存の「知財担当者」IDでの自動化実行
- 共有アカウントでの複数部門による使い回し
- 無制限なファイルダウンロードとルートアクセス

OK: 推奨されるアクセス統制

- 専用ID分離：「自動化用サービスアカウント」と「レビュー権限者」を完全分離
- 専用環境：案件別の独立ワークスペースでの実行
- 機能制限：ファイルダウンロード禁止、ターミナルアクセスの無効化
- 監査権限：Private Logs Viewerの厳格な割り当て

規程に「使ってよい」と書くだけではガバナンスは成立しない。IAMロールとハードな実行環境の分離が必須。

エージェント型AI ベンダー別リスク&ガバナンス評価

	Google (Gemini 3.5)	Anthropic (Claude)	OpenAI	Microsoft (Copilot Studio)
法的リスク (Risk)	3.5詳細仕様の公開不足による責任分界の曖昧さ。	Client-side実行により、証拠保全責任が100%ユーザ企業側に。	送信等、高リスク行為の確認が明記されている。	資格情報共有による権限濫用、なりすましリスクが突出。
ガバナンス (Governance)	Cloud Audit Logs等のエンタープライズ統合は強力。	自社統制を組みやすいがゼロからの設計が必要。	承認フロー (Confirmation semantics) が最も詳細に文書化。	Power Platform統合により現場実装は容易だが暴走リスク大。
推奨方針 (Recommendation)	契約での仕様補完、Web GUI限定での導入。	自社保全を活かし、厳格な隔離環境を構築。	高リスク画面はallow listとtakeoverを併用。	現場主導の自動化は非推奨。エンドユーザ資格情報の強制。

組織実装へのロードマップ：責任所在の再設計

短期（最初の90日）- 制御の確立

- デフォルト利用の原則禁止と許可リストの策定
- 専用実行環境の分離とData Accessログの有効化
- 「送信・決裁」操作に対するHuman-in-the-Loopの強制

中期 - 制度化と防衛

- ベンダー契約の改定（学習不使用、データ保存先）
- 知財SOPの改訂と監査・法務・情シスの三者レビュー
- エージェントのログを「訴訟ホールド」対象へ組み込む

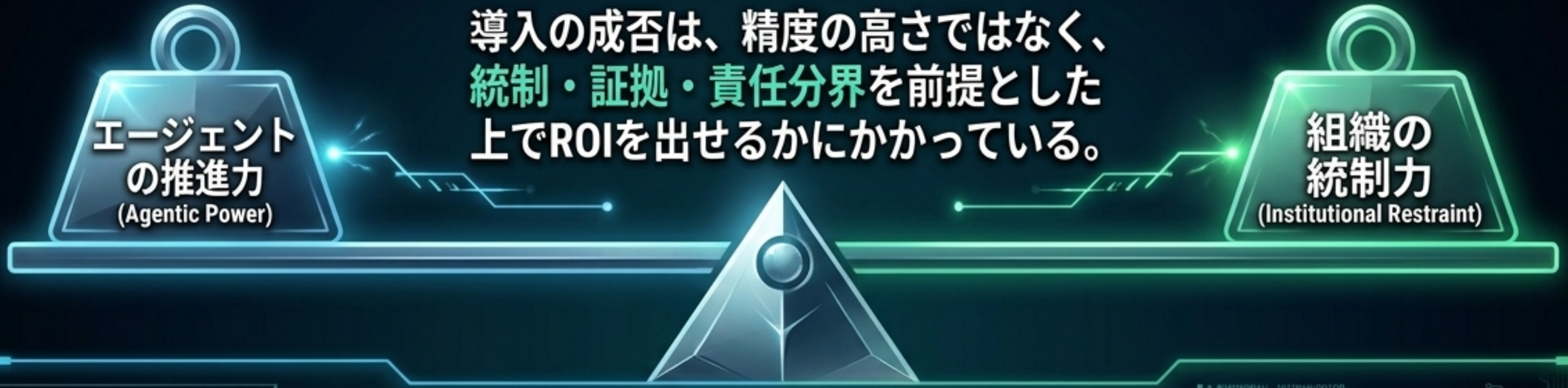
長期 - 持続可能なアーキテクチャ

- 「API-first, GUI-second」原則の徹底
- ユースケースごとのDPIA（データ保護影響評価）実施
- 社内証拠保全基盤のWORM化

START — 3 MONTHS — 6 MONTHS — 1 YEAR

結論とPoC 優先調査チェックリスト

導入の成否は、精度の高さではなく、
統制・証拠・責任分界を前提とした
上でROIを出せるかにかかっている。



- ☐ 画面上の情報に、**個人データ・営業秘密・訴訟保留文書**が含まれていないか？
- ☐ Google Cloud上で**Data Accessログが有効化**され、案件IDで追跡可能か？
- ☐ 発明創出支援において、後日**「人間の創作的寄与」を証明できるログ**が残るか？
- ☐ 規約上、**画面の大量抽出が許容**されているか？（不可ならAPIへ）
- ☐ 送信・同意を伴う**高リスク操作**の直前に、**人間の承認ゲート**が機能しているか？