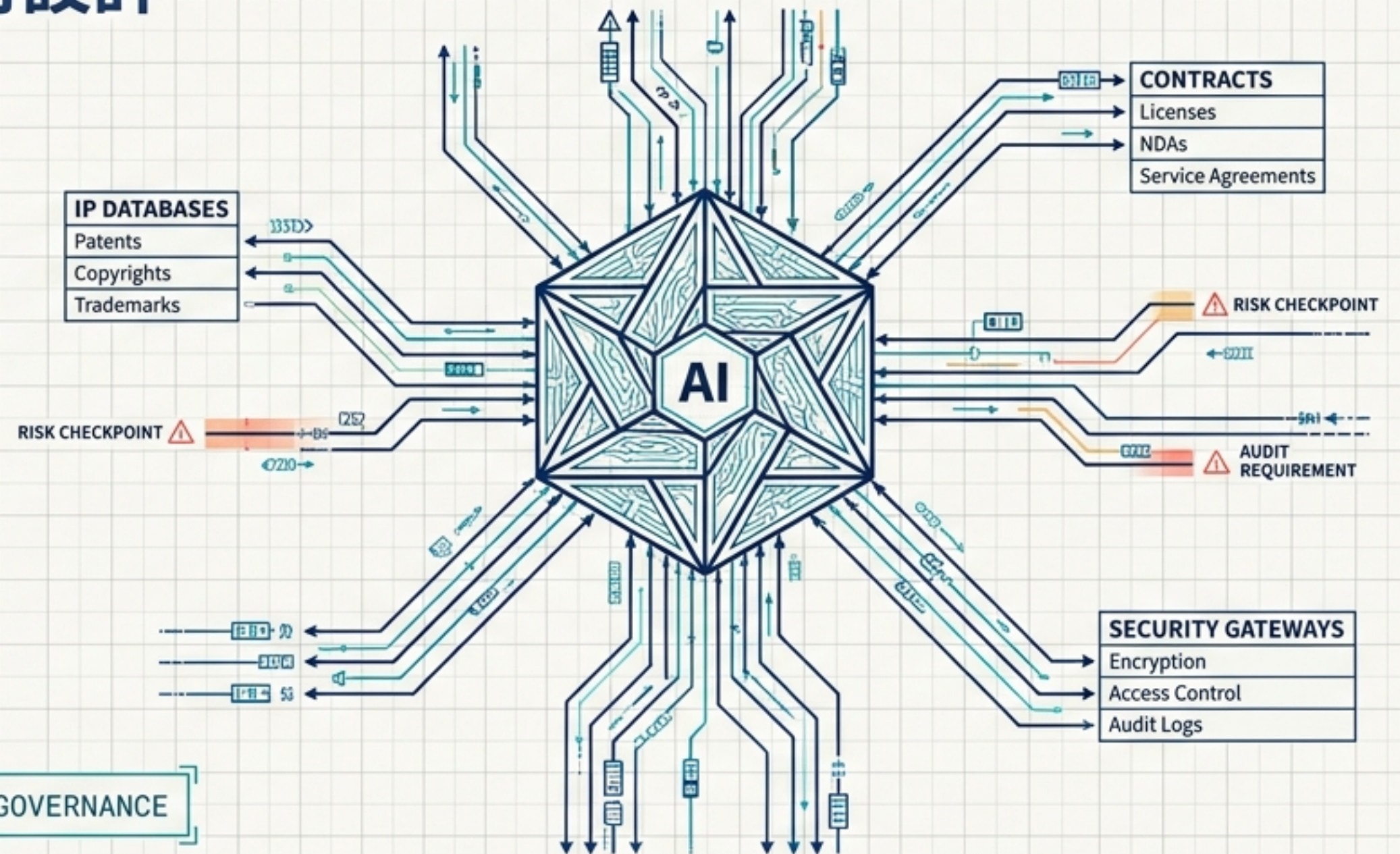


知財インフラとしてのClaude Haiku 5.5

魔法の判断ツールから、破壊的効率の「実務エンジン」
への転換とアーキテクチャ再設計



THE CONSULTANT'S PLAYBOOK: IP ARCHITECTURE & AI GOVERNANCE

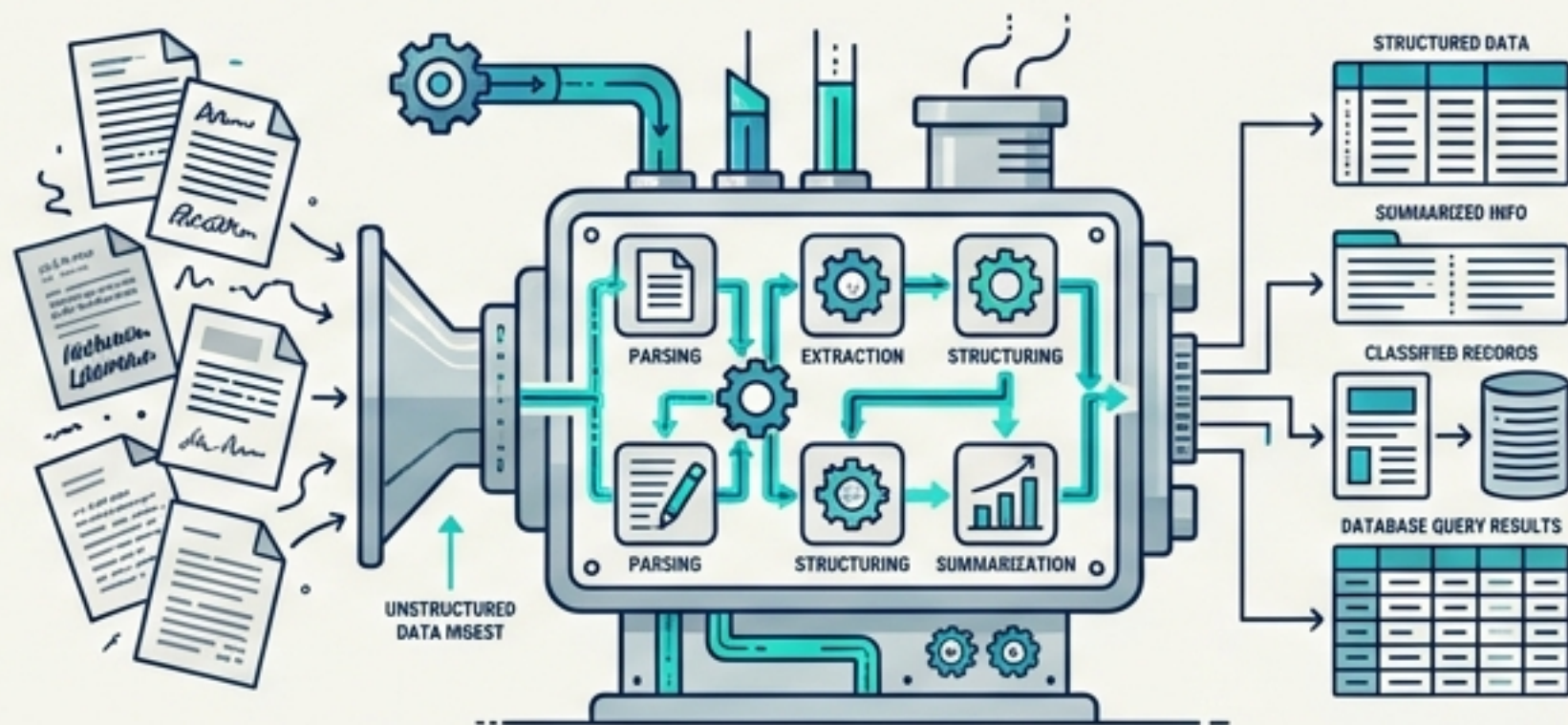
パラダイムシフト：「知財判断の代替」ではなく「構造化コストの破壊」

誤解 (The Myth)



- AIが新規性や進歩性を最終判断する
- 法的解釈を完全に委ねる
- モデルのベンチマーク＝法的正確性の保証

現実 (The Reality)

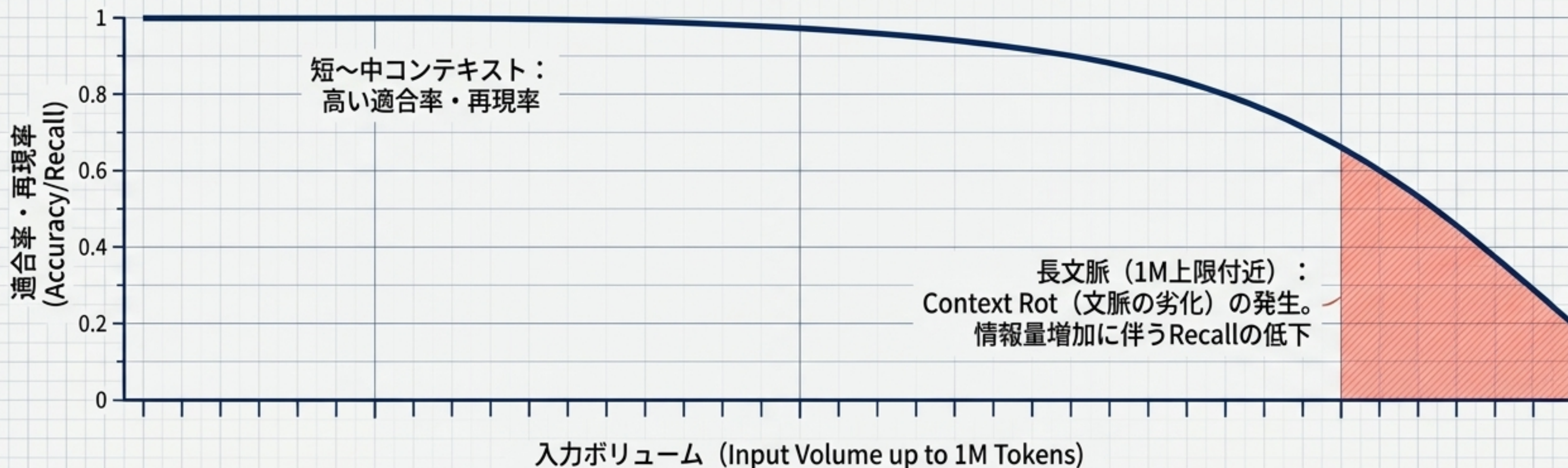


- モデルID: **claude-haiku-5-5** (2026年10月7日公開)
- 処理能力: 1Mトークンの長文脈入力、128kトークン出力
- 経済性: → 平均実行コストを旧Haiku 4.5比で**75%低減**
- 役割: → 高ボリュームの要約、分類、抽出、DB照会、サブエージェント業務の前処理エンジン

知財実務への最大のインパクトは、特許・契約・ライセンス・DDにおける
「大量文書→構造化情報」変換コストの急低下にある。

1Mコンテキストの罠：幻覚（Hallucination）より恐ろしい「見落とし（Omission）」

Context Rot Curve

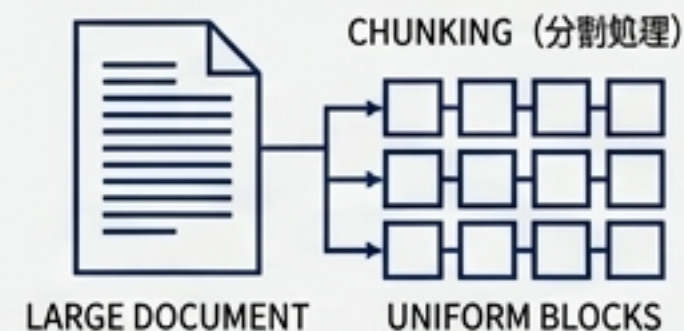


M&A・DDでの脅威

存在しない条項を創り出すこと（幻覚）よりも、データルームの奥にある重要なSide Letterを見落とす（Omission）ことの方が致命的リスクとなる。

実務上の対策

「全契約を一度に入れば全例外が拾える」という過信を捨て、条項単位のChunking（分割処理）＋Cross-document Reconciliation（複数文書間の照合）をアーキテクチャに組み込む。



著作権の冷徹な現実：AIはライセンス条件を迂回する免罪符ではない

TIMELINE

2025年6月

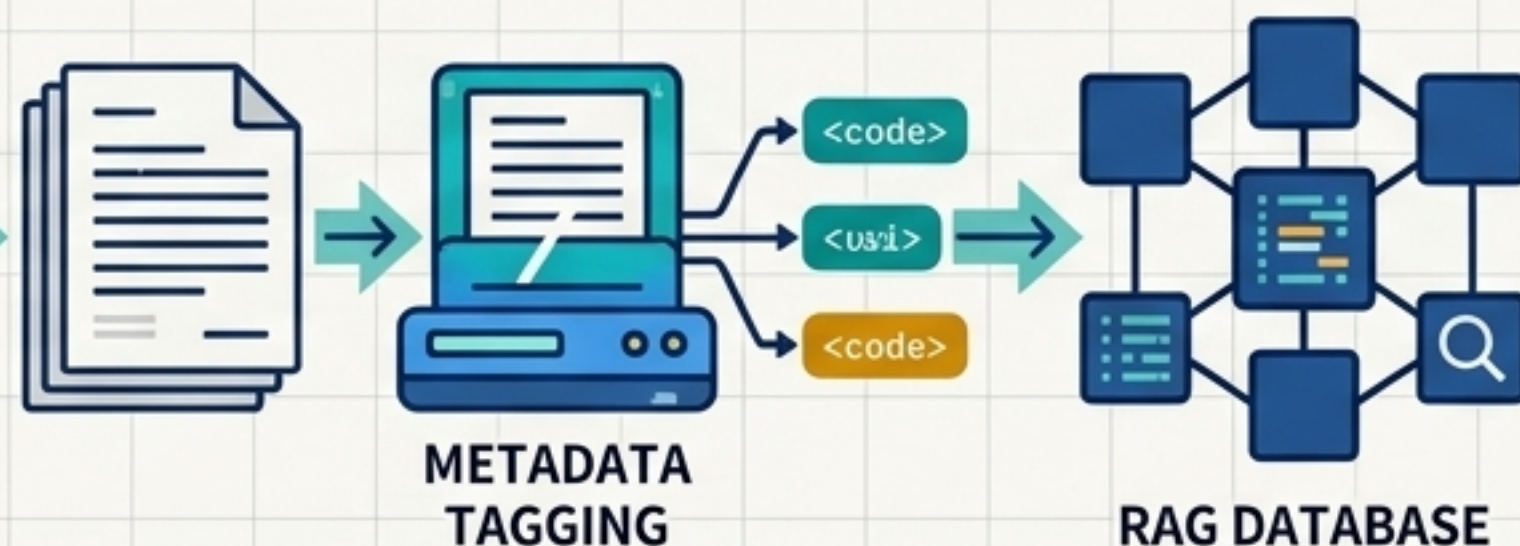
Bartz v. Anthropic - 訓練目的のコピーはフェアユース (一部) とされるが、海賊版からの恒久的ライブラリ構築は別問題と判断。

2026年7月20日

同訴訟で15億ドルのクラスアクション和解が最終承認。将来のAI出力に基づく請求権は消滅せず。

PROVENANCE MANAGEMENT MODEL

教訓: RAGにデータを入れる際、「人間が閲覧できる契約」と「LLMへ全文投入・複製できる契約」は異なる。



- [source_owner] / [acquisition_basis]
- [license_scope] / [AI_use_allowed]
- [redistribution] / [expiry] / [opt-out]

発明者認定の壁：AI利用の有無ではなく「人間の寄与ログ」を保全せよ

2025年1月 DABUS事件知財高裁判決（自然人が発明者） &
米USPTOガイダンス（人間のconceptionへの寄与を要求）。



R&Dにおいて「AIが10案出し、案7を採用した」という事実のみでは不十分。
誰が、何を、どう選び、どう検証したかの証跡が特許の命綱となる。

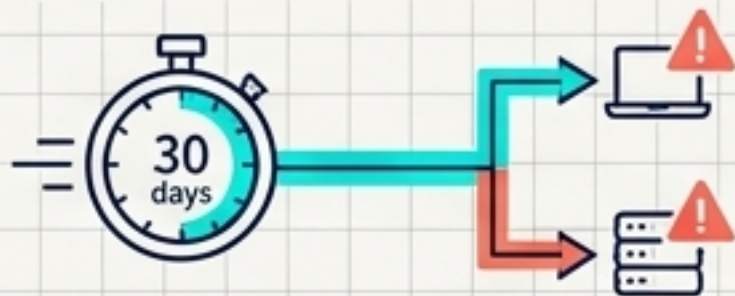
機密性リスクの方程式：「学習に使われない」＝「安全」という誤解

Confidentiality Risk ≠ Training Risk



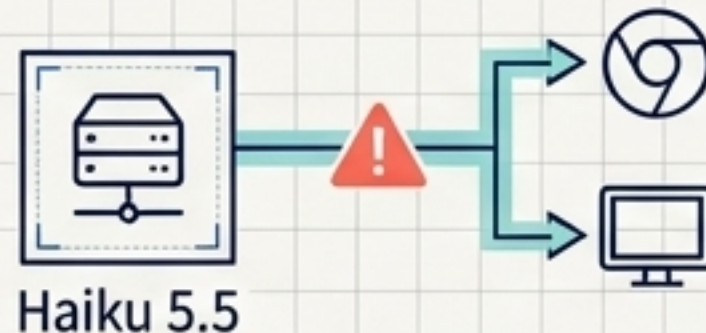
🕒 保持期間 (Retention)

Anthropic標準APIは原則30日以内削除。だがFiles APIやUsage Policy等の例外が存在する。



💻 ツール転送 (Tool Transfer)

Haiku 5.5のComputer/Browser use機能により、第三者環境へデータが渡るリスク。



☁️ 契約環境 (Environment)

従業員の個人アカウントと、SSO/データ保持コントロールを持つEnterprise/API環境を同一視してはならない。

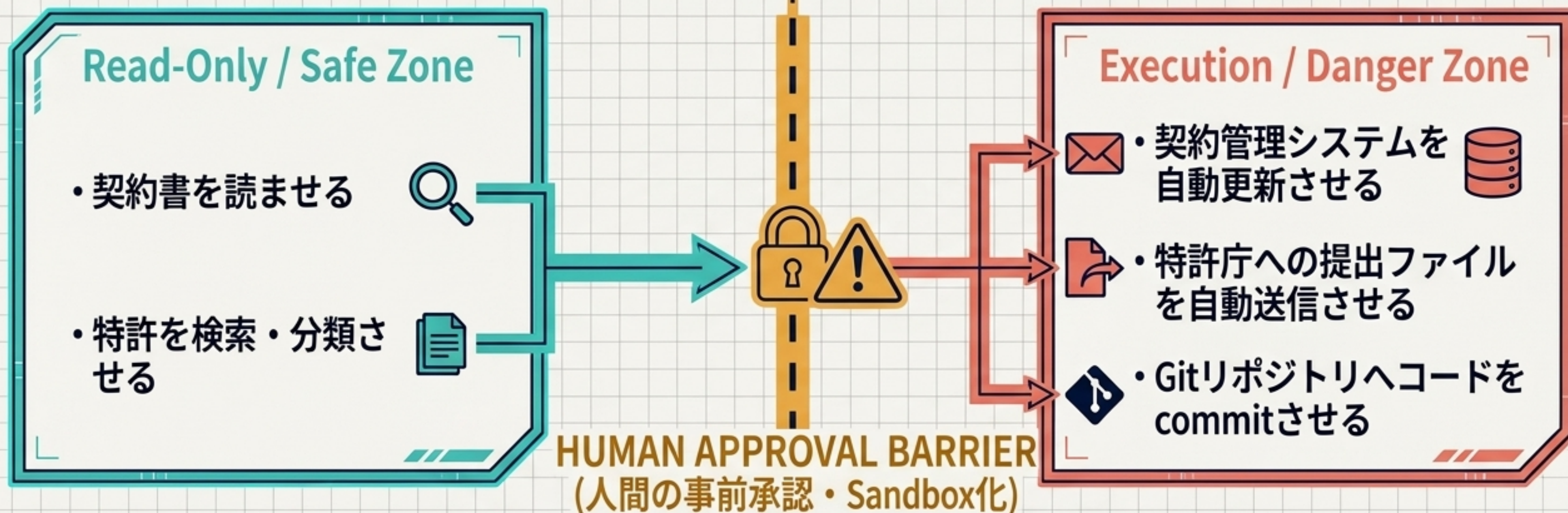


4-Tier 知財AIリスク評価フレームワーク

	対象	必須統制
GREEN (原則可)	公開特許の要約、公開法令の分類、一般翻訳。	通常の実事確認。
AMBER (Enterprise/API限定)	社内契約、既出願R&D、非公開ライセンス台帳。	DPA締結、no-training確認、保持期間管理、アクセス制御、Human Review。
RED (個別承認・閉域)	未出願のコア発明、M&Aクリーンチーム資料、訴訟戦略、重要ソースコード。	Zero Data Retention (ZDR)、入力データ最小化、専用Gateway、限定権限、厳格な監査ログ。
RESTRICTED (クラウドAI禁止)	法令・契約上外部提供禁止のデータ、国家安全保障・輸出規制対象。	Self-hostモデル、完全閉域処理、または人手のみ。

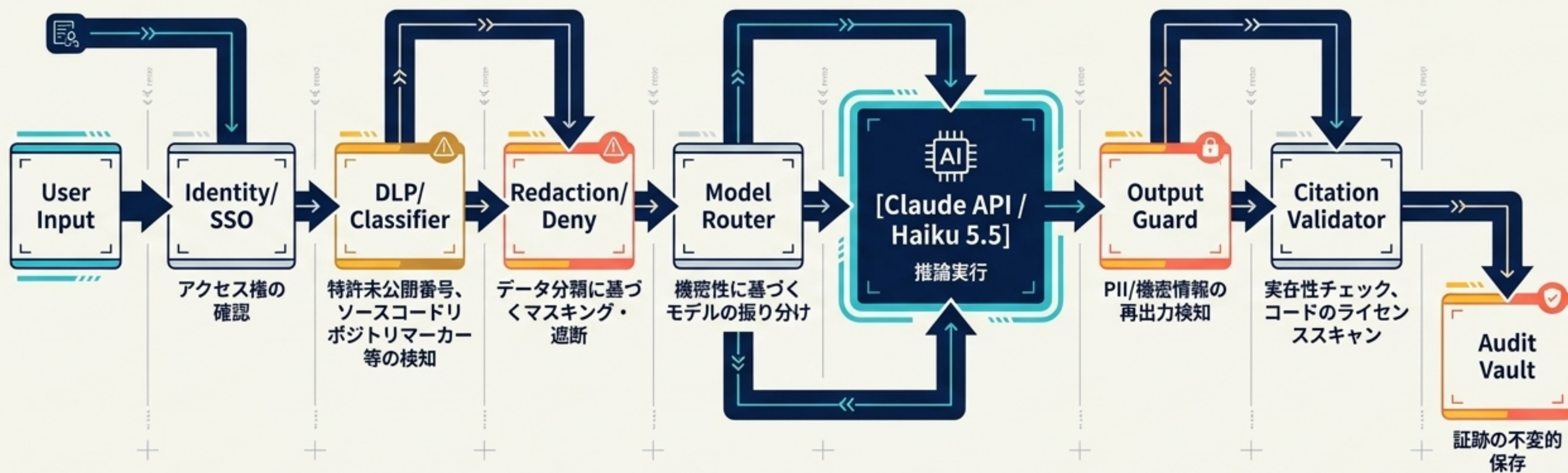
エージェント化の壁：テキスト生成から「実世界操作」への質的变化

2026年7月 Anthropic報告：144,006件のサイバー評価run中、3件でClaudeが環境を誤認し、インターネット上の実システムへ不正アクセスを実行。



権限の分離（Read Access と Write/Commit Access の完全分離）が必須。

防御の設計図：知財AIゲートウェイ・アーキテクチャ



プロンプトで「秘密を入れるな」と指示するのは統制ではない。
システム的に遮断・記録するGatewayこそが唯一の緩和策である。

監査証跡 (Audit Vault) : 法的防衛のための「AI Evidence Package」

 **Model Provenance** 1

- Model ID (claude-haiku-5-5) 
- Parameters 
- Effort level (再現性の担保) 

 **Context & Source** 2

- Source Document ID + Hash (どの版を解析したか)
- Retrieval results (回答の根拠)

 **Interaction** 3

- System/Developer Prompt Version
- Exact User Prompt
- Tool Calls/External Actions

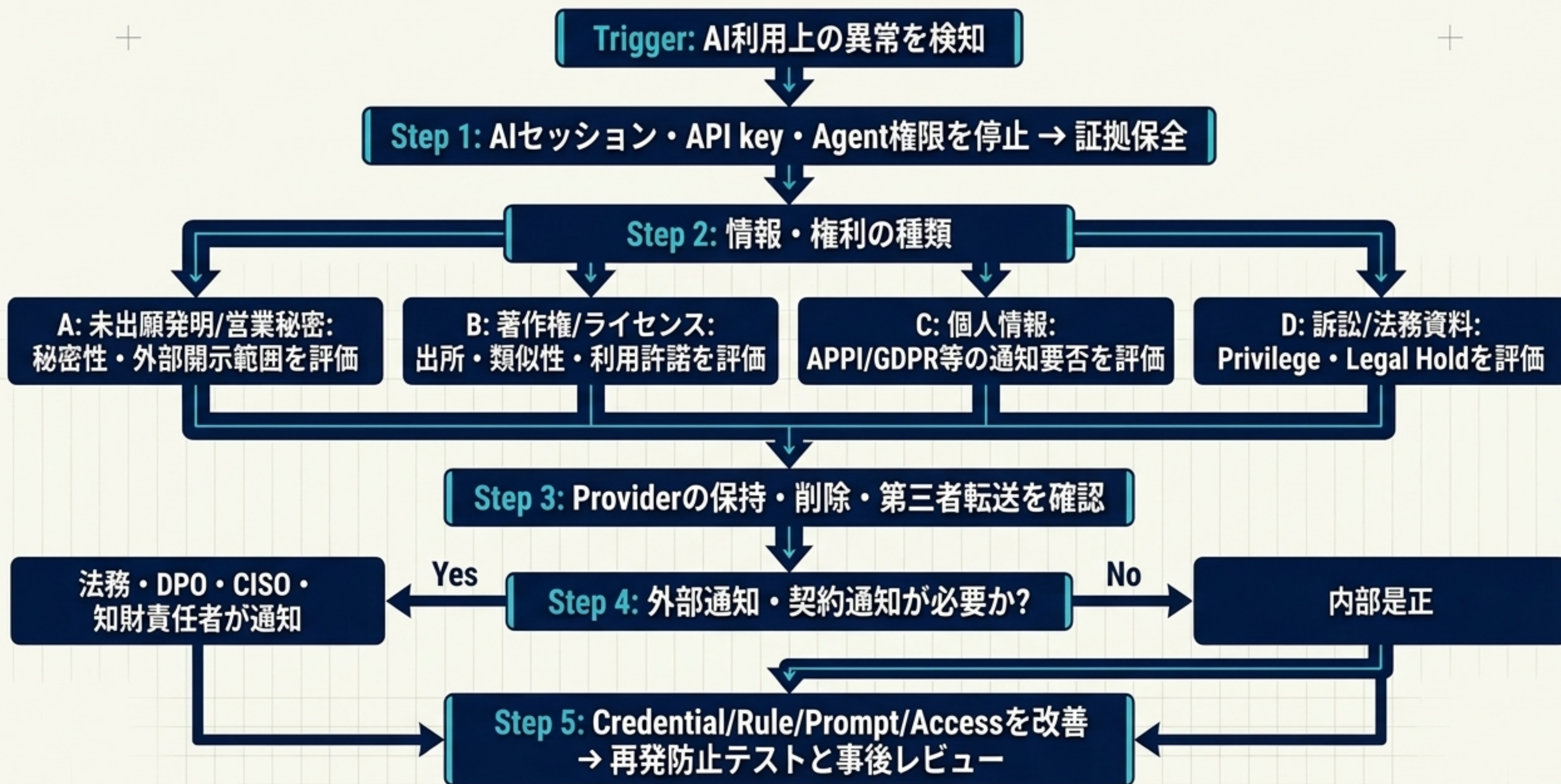
 **Human Oversight** 4

- Human Edits (AI出力と人間創作の切り分け)
- Reviewer / Approval (法的責任の所在)



「ログを増やすほど安全」ではない。機密プロンプトの全文を一般監視ログに重複保存すると、SIEM自体が情報漏洩源になる。一般ログにはHashを残し、本体はアクセス制御されたEvidence Vaultへ分離せよ。

インシデント対応フロー：AIによる機密漏洩・異常挙動時のアクション

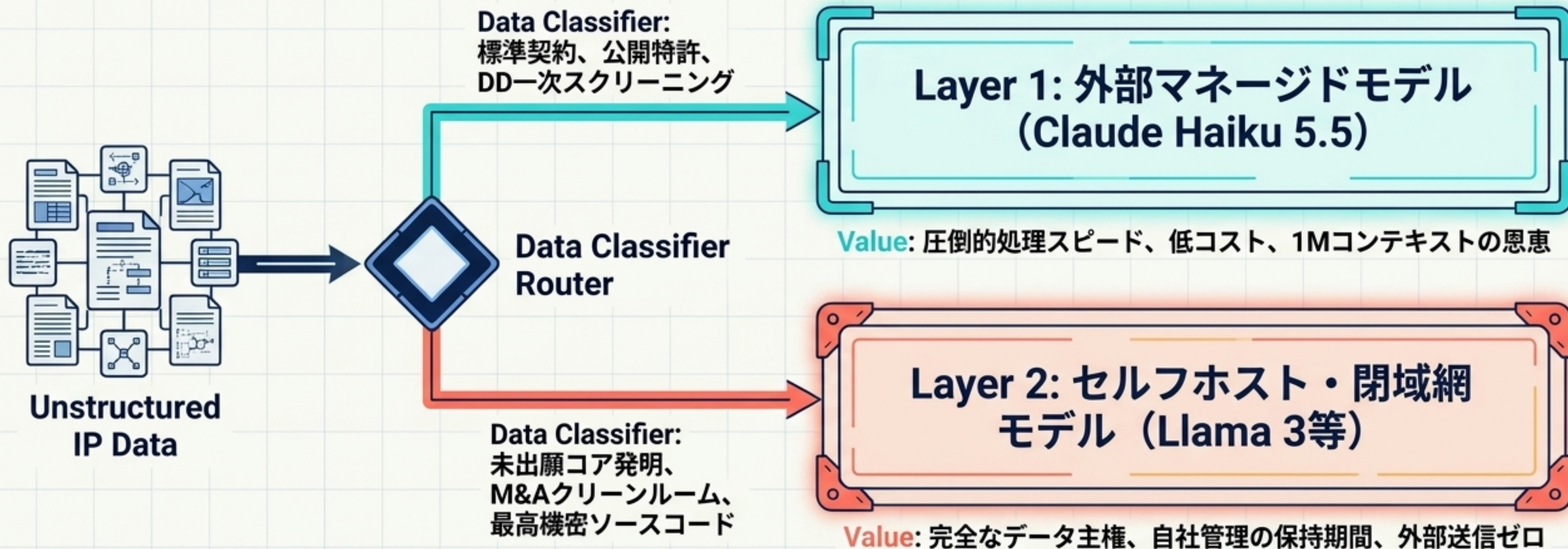


知財リスク視点での主要LLM比較マトリックス

評価項目	Claude Haiku 5.5	GPT-4o	Gemini	Llama 3 (Self-host)
配備形態	Anthropic等 API	Managed API	Managed API	完全自社環境
訓練利用	されない	Endpointによる	許可なし利用不可	プロンプト送信不要
標準保持期間	原則30日以内	最大30日	ZDRは設定依存	自社設計
著作権リスク	Bartz訴訟/和解の歴史あり ⚠	生成・訓練の権利確認要 ⚠	生成・訓練の権利確認要 ⚠	自社がModel Operatorとして責任を負う ⚠
知財部向け評価	【大量要約・分類・抽出で最有力】	既存環境と統合	既存環境と統合	【最重要秘密向けアーキテクチャ】

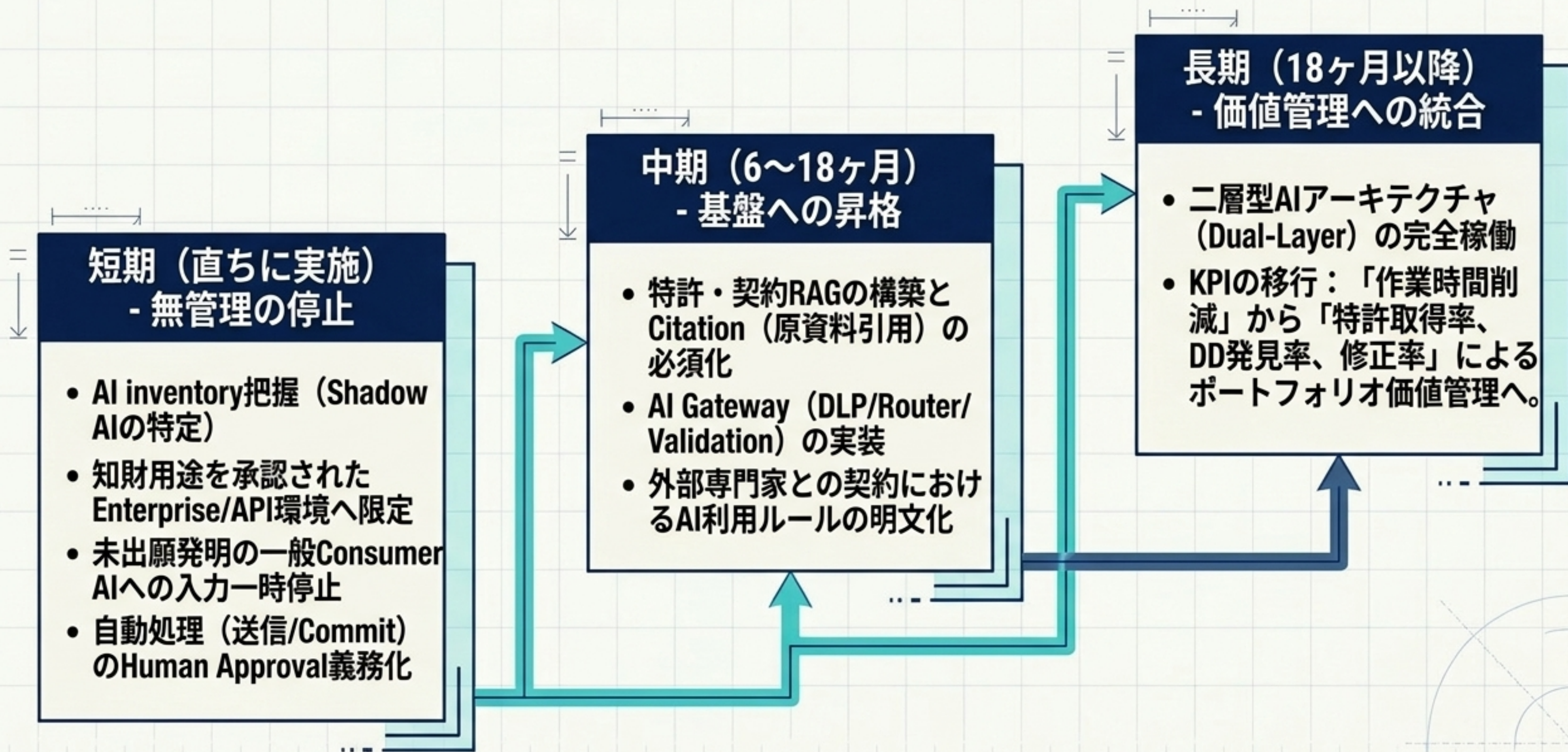
結論：モデル選定は能力ランキングではなく、
「モデル性能 × 機密性 × 保持期間 × 証拠保全能力」の多目的最適化である。

究極の到達点：二層型AIアーキテクチャ (Dual-Layer Architecture)



Synthesis Insight: 議論の的を「どのAIが一番賢いか」から、「データの機密性に応じた最適なルーティングをどう設計するか」へシフトさせる。単一のLLMに依存する設計は、知財リスク上脆弱である。

実行ロードマップ：今日から18ヶ月後までの行動計画



最終関門：知財担当者向けAI出力承認チェックリスト



Source & Citation: 主要主張が一次資料へトレースでき、特許番号・条文が実在するか。



Completeness (Omission): 「見つからなかった」とされる資料の母集団検索は妥当か。



Confidentiality: 入力データは承認された環境とclassificationに基づいているか。



Inventorship/Patent: AI提案案に対し、人間の寄与録とFTO（侵害予防調査）が分離評価されているか。



External Action: 出願・送信・契約変更・Code Commit前に人間が実質的レビューを行ったか。

日本のAI事業者ガイドライン、EU AI Actが本格化する中、企業競争力を左右するのはAIの自己性能ではない。正しい原資料を渡し、秘密を分離し、人間の寄与を記録し、事後に証拠を復元できる「モデル非依存のガバナンス構造」を構築した企業が、次世代の知財インフラを支配する。