

Claude Haiku 5.5と 「全件AI処理」時代の知財戦略

企業知財のコスト構造破壊と、
セキュリティ・法務ガバナンスの実装プレイブック

「検索式による絞り込み」から「**AIによる
全件一次処理**」へのパラダイムシフトと、
それを支える3層マルチエージェント構造。

Executive Summary: 3つのパラダイムシフト



コスト構造の破壊

Haiku 5.5の入力単価（\$0.10/1M Tokens）により、従来の「検索式で絞り込む」アプローチから、数万件の特許や契約書を「全件AIに読ませる」アプローチへの移行が経済的に可能に。



品質評価の分離

「大量処理・一次分析」をHaiku 5.5が担い、「法的結論・最終判断」は上位モデル（Opus 5.5）や専門家が担う。AIの性能向上を法務品質の完全な代替と混同しない多段設計が必須。



専用統制の必須化

「学習に使われない」だけでは不十分。著作権、発明者適格性、データ保持期間（原則30日）、自律エージェントの操作権限に対応する、知財部門専用のAIゲートウェイと証跡保全が急務。

The Shift: 「検索式」からの脱却と全件処理の実現

30,000件特許スクリーニング API費用試算

Fable 5.1
(全文読み込み想定)

\$10,500

Opus 5.5
(全文読み込み想定)

\$4,200

Haiku 5.5
(一次処理想定)

\$22.5

0

\$00

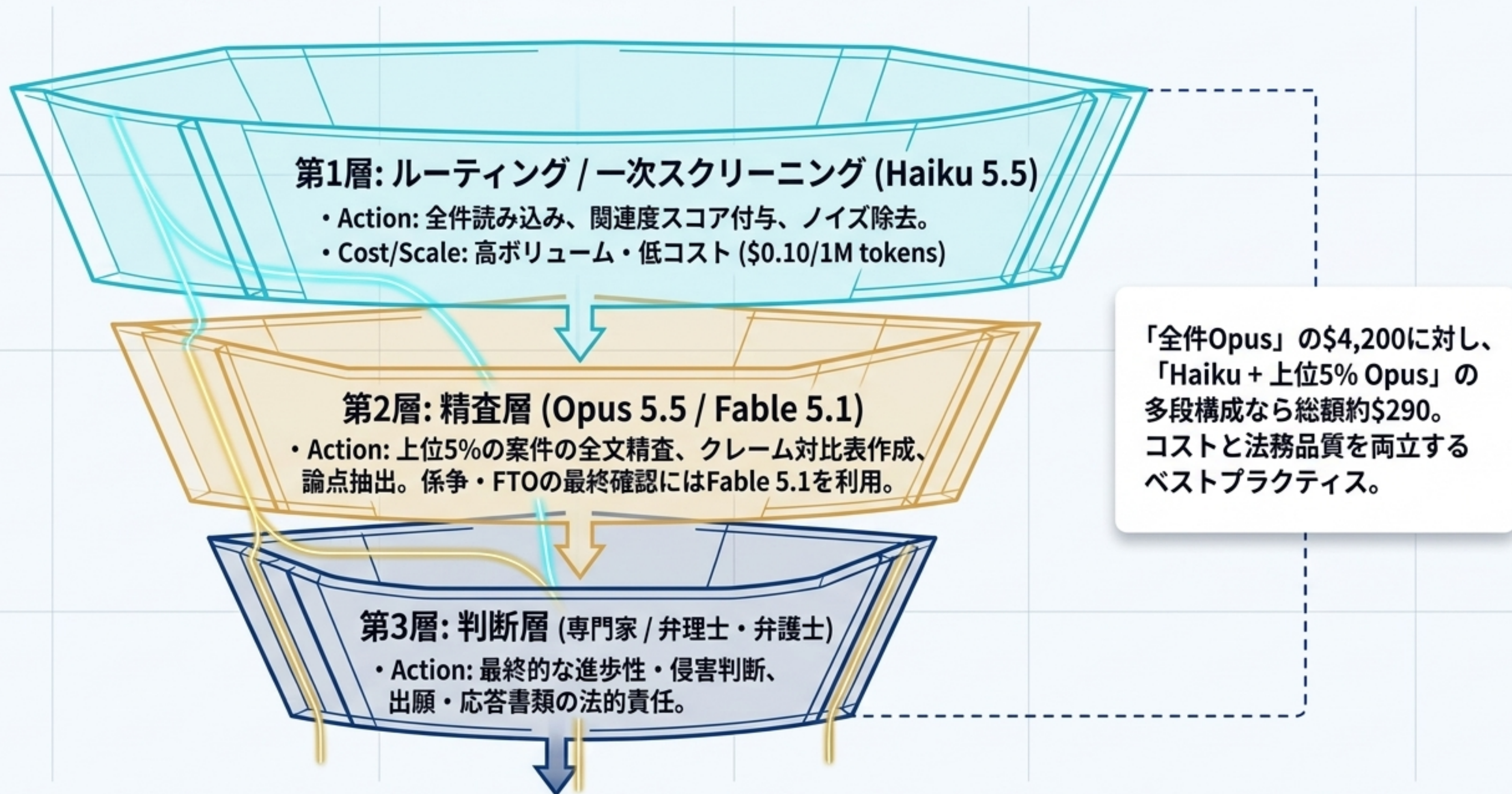
Insight: 調査コストの主戦場は「LLMの利用料」から「評価セットの構築と検証」へ移行した。
検索式の漏れ（再現率の不足）を、予算ではなく設計の問題として解決できる段階に到達。

Model Landscape: 知財リスクと性能の多目的最適化

評価軸	Haiku 5.5	GPT-4o	Llama 3
配備形態 (Deployment)	Managed / Cloud	Managed API	Self-host weights
データ保持 (Retention)	原則30日以内削除, ZDRは要審査	原則30日, 適格顧客にZDR	自社管理で 完全統制可能
著作権リスク (Copyright Risk)	Bartz訴訟の 判例史あり	別途権利確認必要	自社がOperatorとし ての直接責任
知財部向け評価 (IP Evaluation)	大量要約・抽出の 最有力	Legacy比較対象	最高機密向けの Architecture候補

モデル選定は能力ランキングではなく、「性能 × 機密性 × 契約 × 証拠保全」の多目的最適化方程式である。

Synthesis: 3層マルチエージェント・アーキテクチャ



Task Mapping: 知財業務別のAI／人間 境界線

知財タスク (IP Tasks)

先行技術調査

発明提案・明細書

契約・M&A DD

Haiku 5.5 (自動化・一次処理)

ノイズ除去、構成要件の
「記載あり/なし」候補抽出

定型項目への整理、
類似既出願の候補提示、
用語の揺れ検出

Change of Controlや
ライセンス条項の抽出、
データルームの一次分類

Opus / Human (判断・責任)

対比表の作成、
新規性・進歩性の法的評価

発明の把握、権利化方針、
実施可能要件の実質判断

Materiality (重要性) の評価、
リスク交渉方針の策定

Note: Haiku 5.5はJune 2026が知識カットオフ。最新の公開特許・判例はRAG（外部検索）連携が必須。

Legal Reality 1: 著作権と「出所 (Provenance)」の管理

The Reality

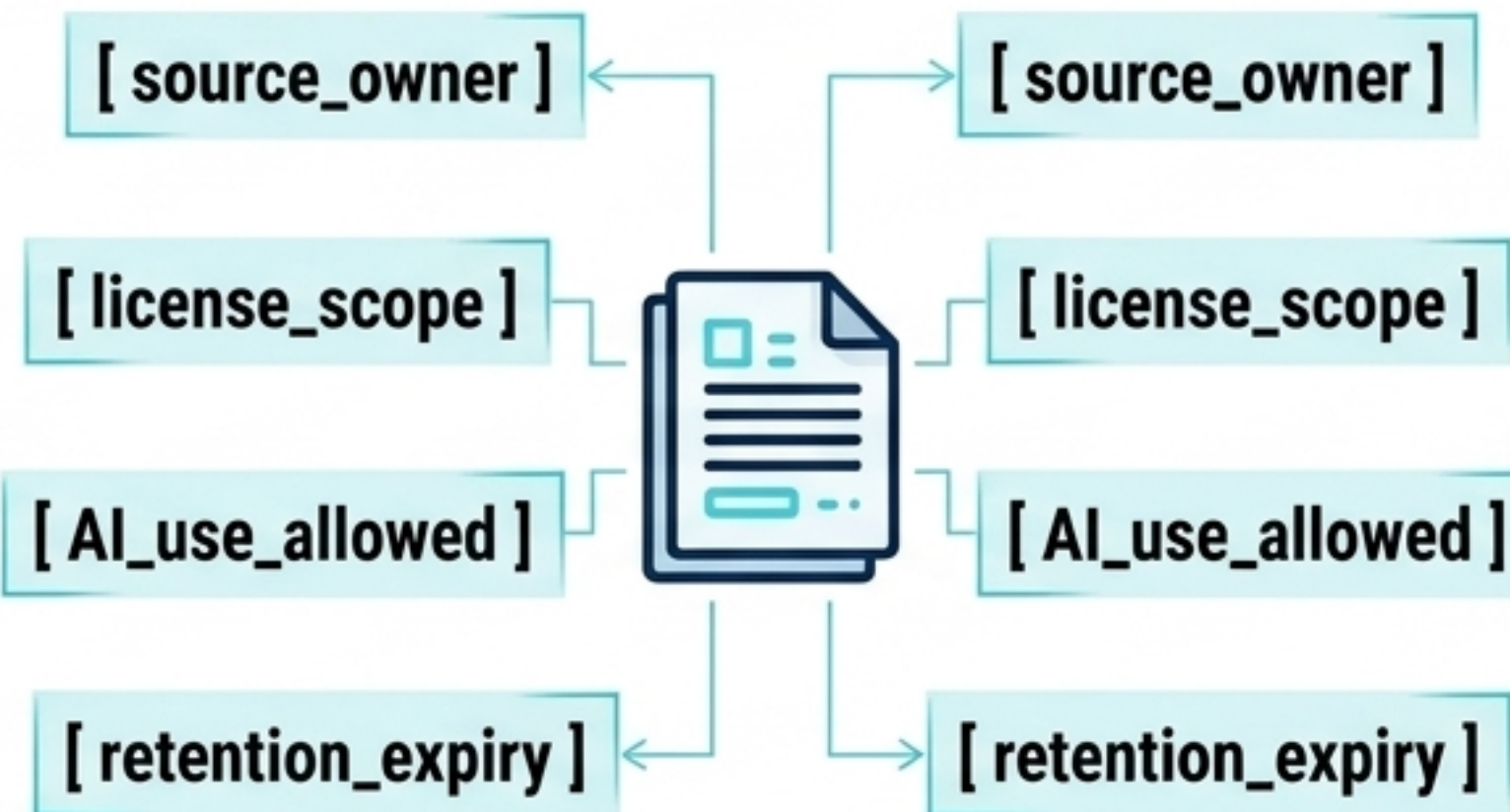


Bartz v. Anthropic (2025-2026)

訓練目的の特定コピーはFair Useとされた一方、海賊版サイトからの恒久ライブラリ構築は別問題とされ、15億ドルの和解が成立。

教訓: 「AIで処理するから元データの取得権原は問われない」という考え方は極めて危険。

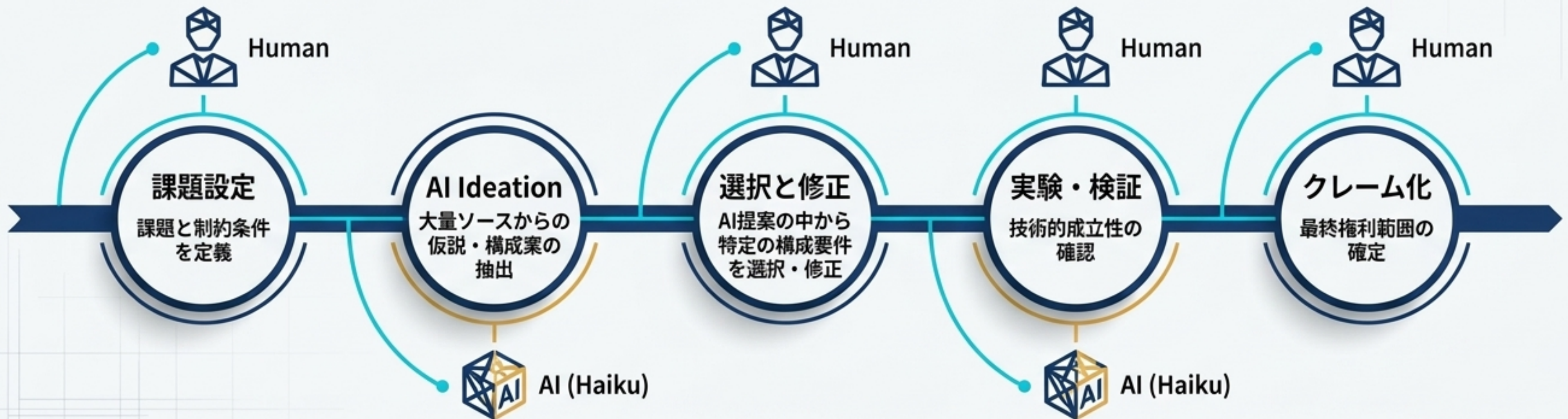
The Solution: RAG Metadata Schema



Takeaway: 人間が閲覧できる契約と、LLMへ全文投入・複製できる契約は同一ではない。

日本知財高裁（DABUS事件 / 2025年1月判決）および米国USPTOガイダンスは、「人間の寄与（Human Contribution）」を発明者認定の必須要件として維持している。

発明創出プロセス



Highlight: AIが「10案出し、案7を採用した」という事実だけでは不十分。誰が、どの段階で、どう寄与したかの「発明寄与ログ（Human-contribution log）」を再構成できる証拠保全が必要。

機密性リスク = 外部送信 × 保持期間 × アクセス可能者
サブプロセッサ × ツール転送 × 契約条件

Anthropic Reality Check

No Training

商用サービスでは顧客データを訓練に使用しない。しかし...

Retention Period

標準APIの入出力は「原則30日以内に削除」。Files APIやAbuse monitoring等の例外が存在。

Subprocessors

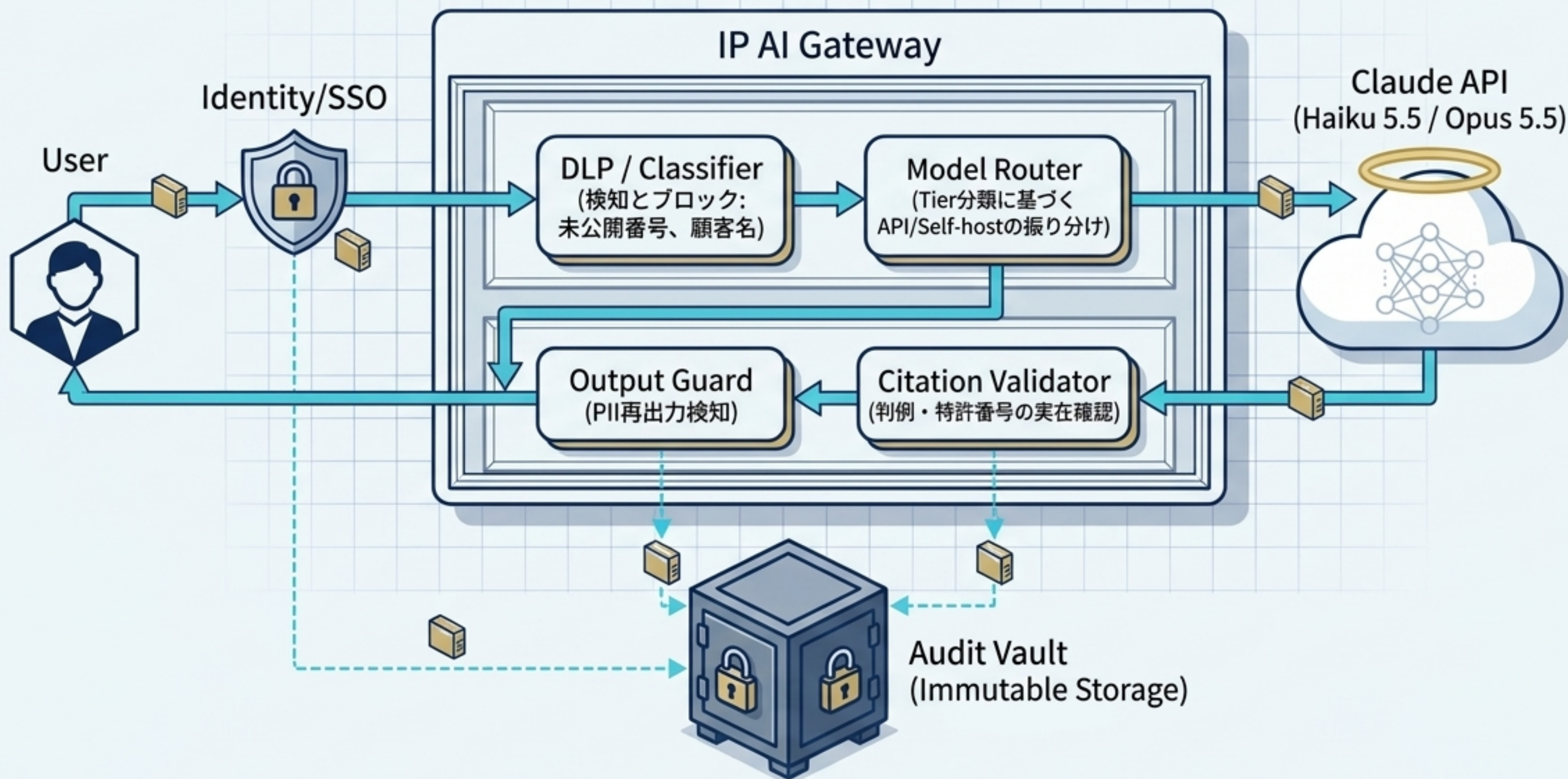
AWS/GCP/Azure経由の場合、プラットフォーム側のデータ保持条件も重畳適用される。

Conclusion: 未出願発明やM&A資料において「学習に使われないから安全」は誤り。
保持期間（ZDR要件）を含めた総合的な統制が必須。

Governance 1: 4軸（データ・タスク・権限・法的効果）のリスク分類

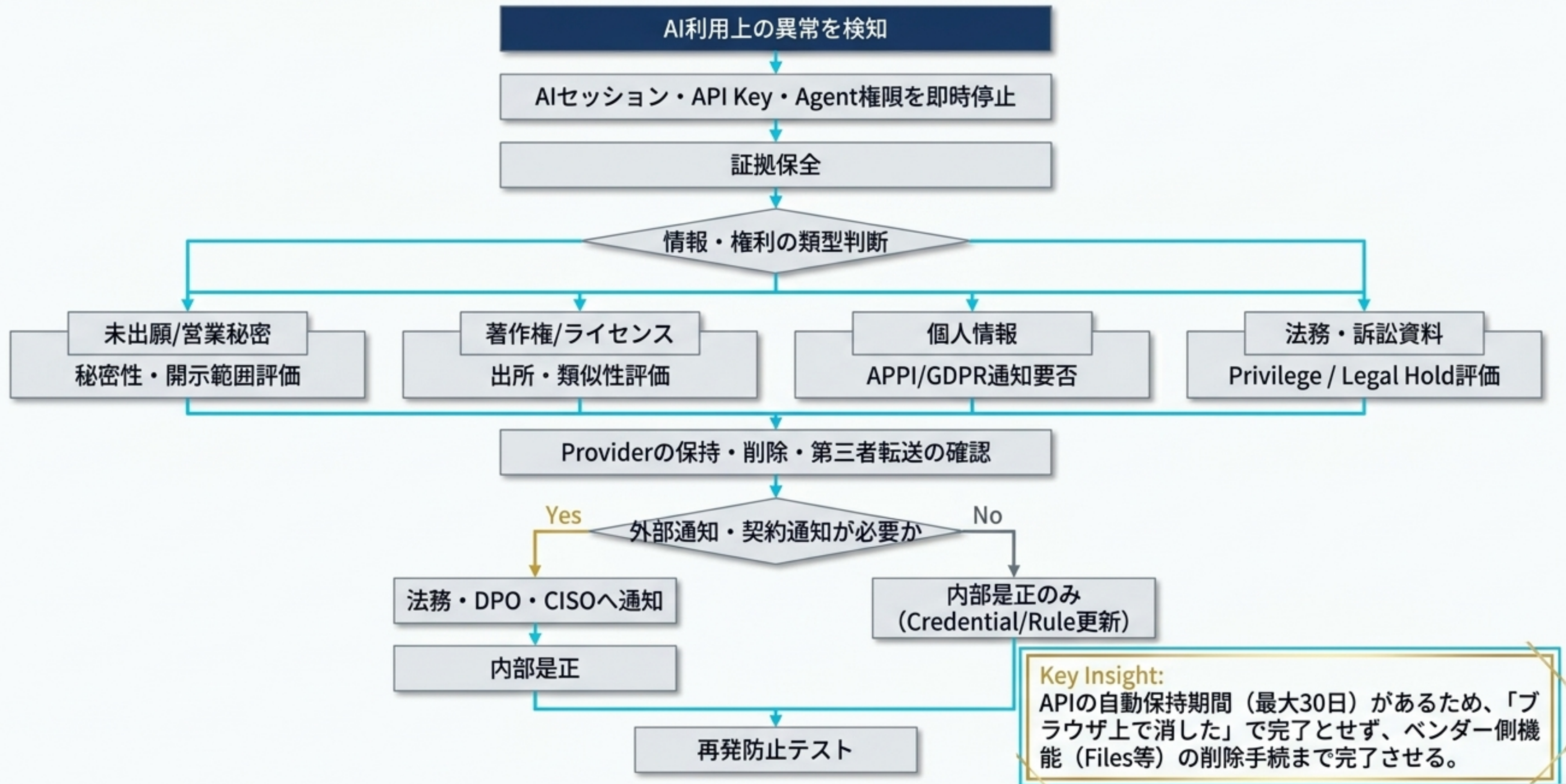
リスクレベル (Risk Tier)	対象データ例 (Examples)	Haiku 5.5利用可否	必須統制 (Controls)
 Green (低リスク)	公開特許要約、 公開法令分類	原則可	通常の事実確認
 Amber (中リスク)	社内契約、既出願R&D、 非公開台帳	Enterprise/API 限定	DPA、No-training確認、 アクセス制御、 人間レビュー
 Red (高リスク)	未出願Core Invention、 M&Aクリーンチーム、 重要ソースコード	原則個別承認	ZDR (ゼロデータ保持) 必須、 専用ゲートウェイ、 最小化、監査ログ
 Restricted (極秘)	輸出規制対象、 外部提供禁止データ	クラウドAI禁止	Self-hostモデル (Llama 3等) または完全人手対応

Governance 2: 知財専用AIゲートウェイの構造設計



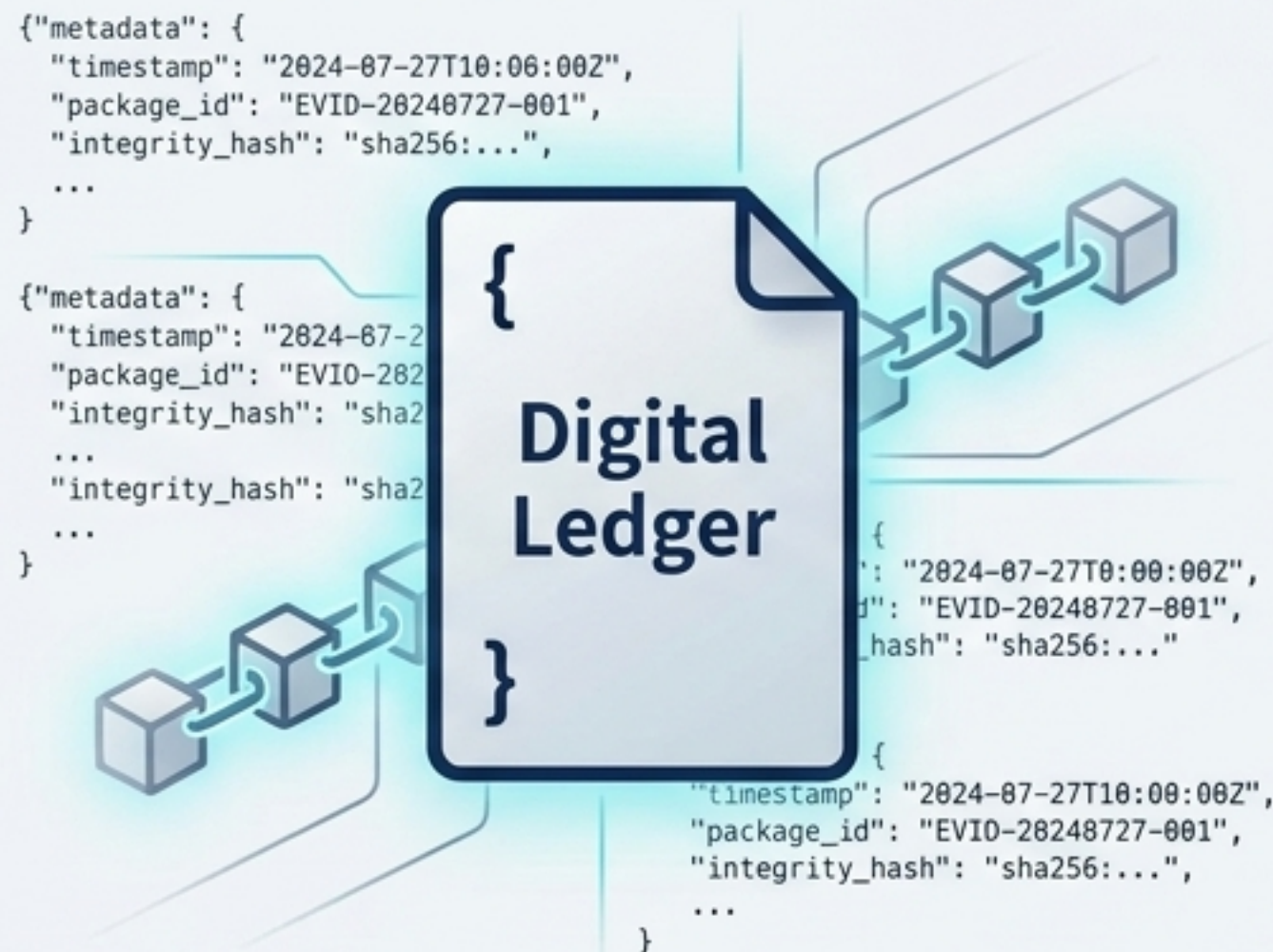
Note: Anthropic側のSafety Classifier (stop_reason: "refusal") に依存せず、自社特有のルール（「Project Xは入力禁止」等）をGateway側で実装することが要諦。

Incident Response: AI異常検知時の対応デシジョンツリー



Evidence Package: 訴訟・監査に耐えるAI証跡保全

「プロンプト履歴」だけでは不十分。知財の権利保護には以下のパッケージ化が必須。



- ✓ [Model ID] [Parameter / Effort]:
将来の再現性確保（Haiku 5.5は適応的思考により Effort設定が結果を左右する）
- ✓ [Source Hash] [Retrieval Results]:
どの版の原資料を解析し、どの根拠を引用したか
- ✓ [Tool Calls]: Agentによる外部アクセス（検索、リポジトリ参照）の証拠
- ✓ [Human Edits] [Reviewer]:
AI出力と人間による創作（修正）の切り分け、法的責任の所在



Warning: 証跡を増やすほどAI本体より監視基盤が漏洩源になりやすい。機密プロンプト本体は分離し、アクセス制限されたEvidence Vaultへ保管する。

Policy & Contracts: ベンダー契約と社内規程のアップデート

AI Vendor Contracts (Anthropic / Cloud Providers)

- Data Use: 商用データの「学習非利用」に加え、再委託先 (Subprocessors) も含めた適用を明文化。
- Retention: 単なる「30日以内」ではなく、Logs, Legal Hold, Abuse Monitoringなどの例外範囲の特定と、技術的に可能な限りのZDR (Zero Data Retention) 構成の要求。
- Model Changes: モデルの退役・変更 (Deprecation) に関する事前通知義務 (再現性の担保)。

External Partners (Law Firms, Patent Attorneys)

- Clause: 外部の法律事務所や翻訳会社との契約において、「顧客資料を生成AIへ投入する際の事前承認・環境指定」を明記。自社内部を統制しても外部経由で漏洩するリスクを遮断する。

Internal AI Policy (社内規程)

- Clause: AI出力は法的結論 (特許性、侵害性) として扱わず、人間による実質的レビューを必須とする。Agent化 (自動出願、自動送信) には事前承認を義務付け。

Execution Roadmap: 導入への3ステップと最終評価

Message: 自社の競争力を決めるのは「どのLLMが一番賢いか」ではない。
「正しい原資料を渡せるか」「機密を分離できるか」「人間の寄与と証拠を復元できるか」である。
正しく統制されたHaiku 5.5は、知財部門のコスト構造を根本から変革する強力なエンジンとなる。

Phase 3: 長期（18ヶ月～） - 二層型アーキテクチャと価値管理

- Haiku 5.5 (Managed) と Llama 3 (Self-host) を情報分類に応じて使い分ける二層構造の確立。
- AIの評価軸を「時短」から「拒絶対応品質、DD Red-flag発見率」へ移行。

Phase 2: 中期（6～18ヶ月） - ゲートウェイとRAGの実装

- DLP、モデルルーティングを備えた知財AIゲートウェイの構築。
- 引用 (Citation) を必須化したRAG基盤の整備。EU AI ActのRole Mapping確認。

Phase 1: 短期（即時） - 無管理の停止と可視化

- AI Inventoryの作成（利用実態把握）。
- 未出願発明の一般Consumer AIへの入力停止。知財用途をEnterprise/APIへ限定。