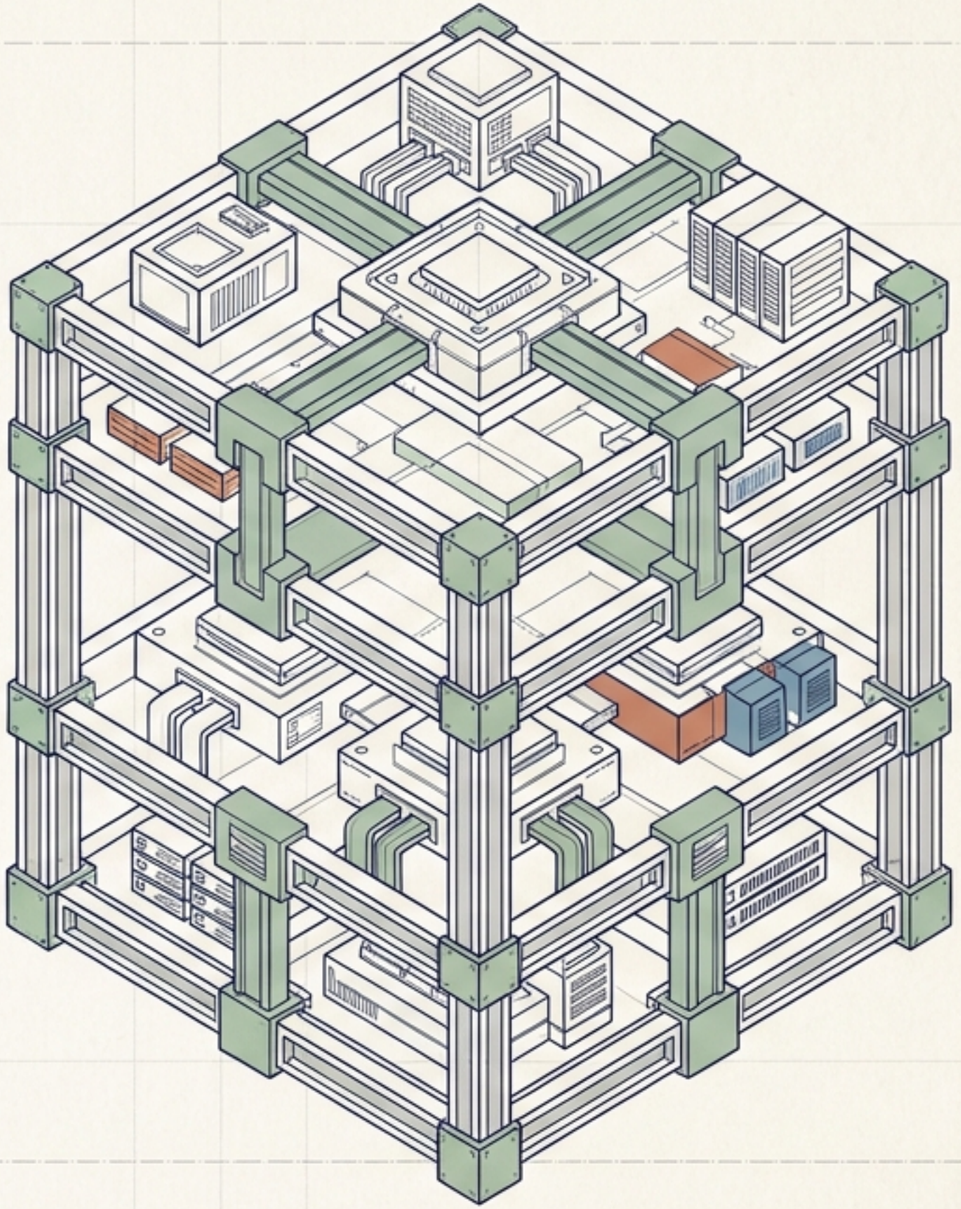
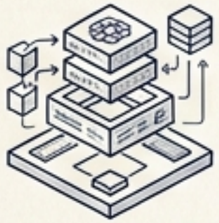
自律型AIエージェント基盤競争と知財業務の未来

「最強モデル」から「多層的ガバナンス」へ：2026-2030年の戦略的プレイブック

FOR CIPO, LEGAL STRATEGISTS, AND IT ARCHITECTS

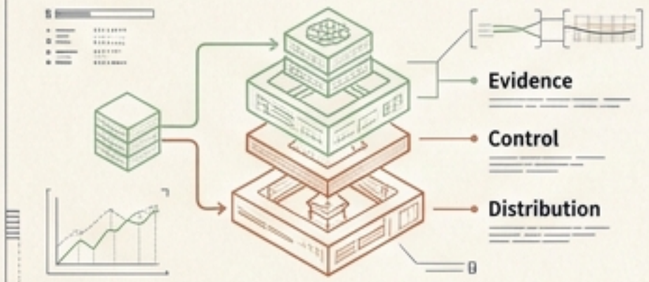


EXECUTIVE SUMMARY



「最強モデル」の探求は終わった。

勝負は単一モデルの性能ではなく、NVIDIA、Google、Microsoft、OpenAI、Anthropicが展開する「証拠性・統制・分配」を含めたレイヤーの覇権競争へ移行した。

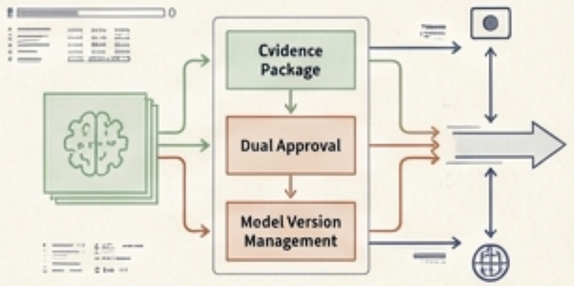


知財業務の最適解は「多層配置」

単一ベンダーへの集中（ロックイン）はリスク。探索、社内文脈、高機密（営業秘密）など、業務の機密区分に応じたベンダーの使い分けが必須となる。

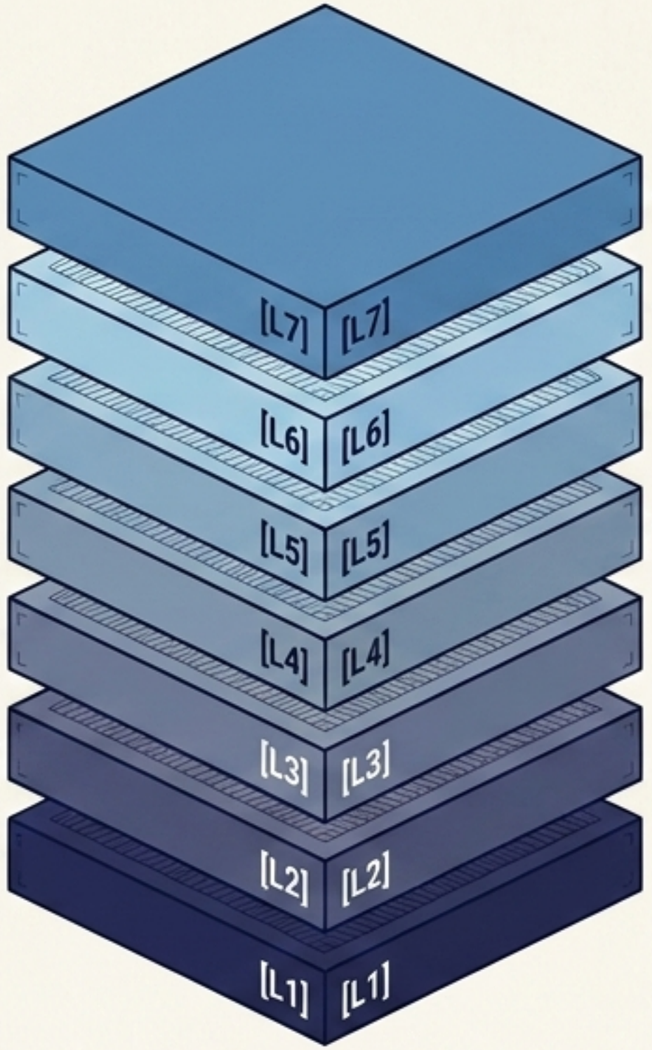
AIを選ぶ前に、統制を設計せよ。

日・米・欧の法規制の違いを踏まえ、モデルの導入より先に「証拠パッケージ」「二重承認」「モデル版管理」の責任体系（ガバナンス）を構築した企業が勝者となる。



覇権を決定づける「7つの技術レイヤー」

主権性・原価・再現性の支配



実行基盤
Foundry, NIM, Agents SDK等

モデル層
Gemini, GPT, Claude, Llama等の推論コア

チップ・計算資源
GPU, TPU, Azure等の物理インフラ

標準・相互運用（MCP, A2A）：
ID・権限・承認ワークフローの統合面

分配力・ユーザーベース：
M365, Workspace, ChatGPT等、最終接点

デスクトップ／作業面：
OS統合、Agent UI。業務の"既定面"化

管理・観測・統制：Copilot Control System, Agent Gateway等のログ管理

定着率・組織的ロックインの支配

MCP/A2Aの普及によりプロトコルの差異は消滅する。
最終的な勝者は、標準の上で「作業面」と「ガバナンス」を握る企業である。

ビッグテック5社の戦略アーキテクチャと知財適性

企業	制圧レイヤーの強み	知財第一適性
Microsoft	L4(管理・統制) / L5(デスクトップ) / L6(分配)	出願ドラフト、OA応答、社内ナレッジ接続。監査証跡が必要な本番運用。
Google	L2(モデル) / L4(管理・統制) / L6(分配)	公知情報・技術文書・図表を跨ぐ先行技術・無効資料の横断調査。
OpenAI	L2(モデル) / L3(実行基盤) / L6(接点)	迅速なPoC、独自エージェント実装、外部検索自動化。
NVIDIA	L1(計算資源) / L3(実行基盤)	営業秘密・訴訟準備・オンプレRAGなど「主権型運用・専用環境」。
Anthropic	L2(モデル) / L7(標準/MCP)	長文比較、契約差分、長時間推論タスク。

インサイト:
M365やWorkspaceが「業務の開始点」を押さえているため、Microsoft / Googleが統制の基盤となりやすい。

知財AI配備の「4つの帯（The 4 Bands）」

第2帯：探索帯（Exploration）

先行技術・競合探索。
公開情報の多段要約や図表理解。

推奨: Google, OpenAI, Anthropic

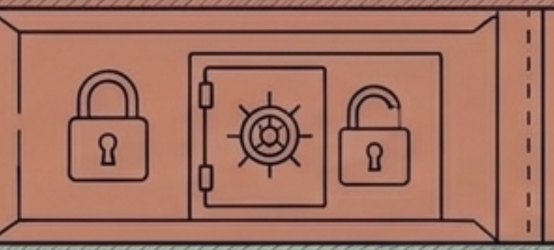
第3帯：社内文脈帯 (Internal Context)

出願・OA・契約。
社内会議、メール、ナレッジへの権限付き接続。

推奨: Microsoft (M365), Google (Workspace)

第4帯：高機密帯 (High-Secrecy)

侵害調査・営業秘密。データ越境や
学習利用を完全に遮断する閉域環境。



推奨: NVIDIA (オンプレ),
OpenAI (Reserved Capacity)

第1帯：証拠帯 (Base Layer)

全AI利用の必須基盤。
元ソース、引用片、ツール呼出し、承認ログの保存。

対象: 全ベンダー / SIEM連携必須

プロセス・ディープダイブ [1]: 探索と文脈の結合

パネル1: 発明発掘 & 先行技術調査 (Exploration Band)

最適解

Google (Deep Researchによる技術・図表横断)、
Anthropic (MCP接続による多段探索)。

潜在リスク

出典欠落、API変更による調査の「再現不能」、
非発明の幻覚。

推奨アクション

検索結果のURL、取得日時、スナップショットを
必ず保存（証拠化）。

パネル2: 特許出願 & 審査対応 (Internal Context Band)

最適解

Microsoft (Foundry IQ / M365統合による
ドラフト運用現実化)。

潜在リスク

人間発明者性・人間寄与の記録不足、
クレームの広すぎ/狭すぎ。

推奨アクション

「骨子作成はAI、最終クレームは人間」の原則化。
発明者面談記録と構成要件表を人間の介入証拠として保全。

プロセス・ディープダイブ [2]: 権利行使と高機密の隔離

パネル1: 権利行使 & 侵害調査

最適解：NVIDIA（閉域でのClaim Chart内製），Anthropic（長大契約比較）。

潜在リスク：誤検知による不当警告、UI自動操作（Computer Use）の暴走。

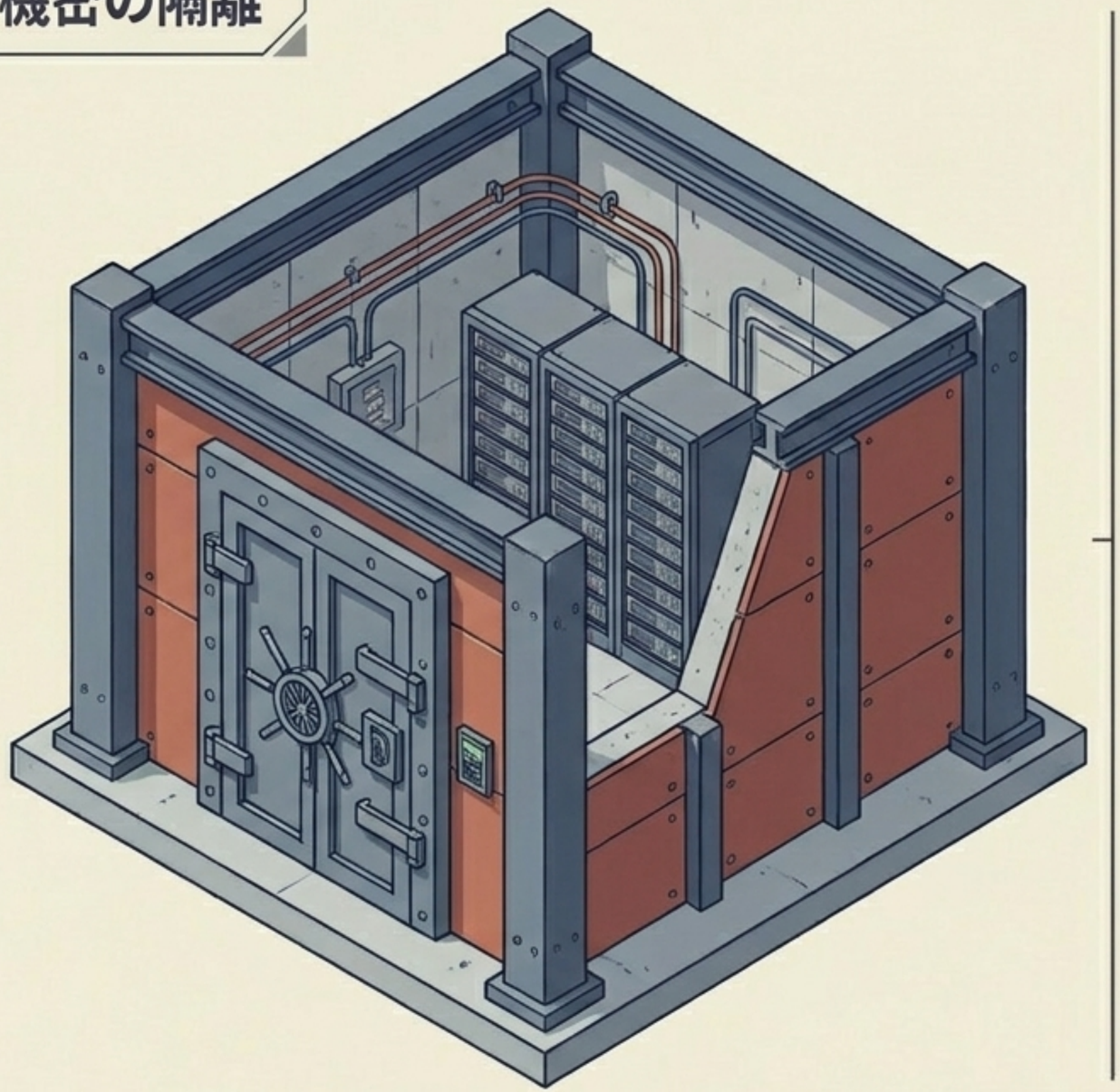
アクション：警告書送付前は「人間の専門家レビュー（二重承認）」を必須とする。

パネル2: 営業秘密管理 (High-Secrecy Band)

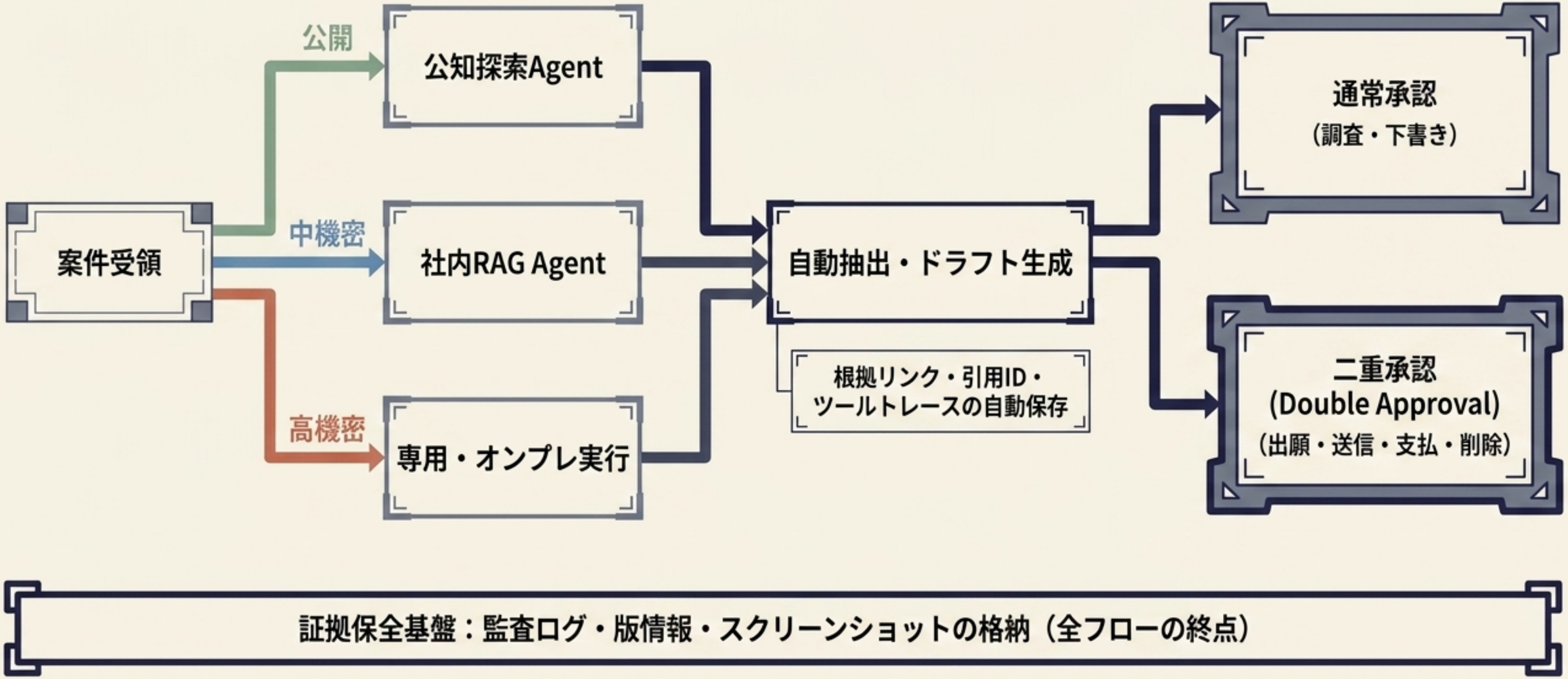
最適解：NVIDIA (AI Enterprise等のエアギャップ志向のオンプレ実装)。

潜在リスク：クラウド越境転送、シャドーAI利用、ログ欠落。

アクション：個人向けUIを禁止。高機密データは専用環境または版固定のReserved Capacityへ物理的分離。

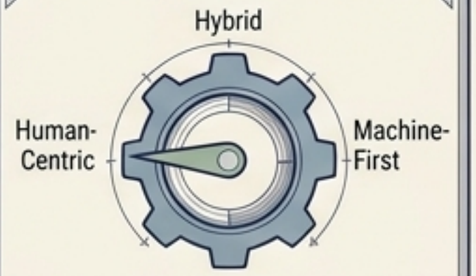


ワークフロー・アーキテクチャ：機密レベル別「承認ゲート」設計



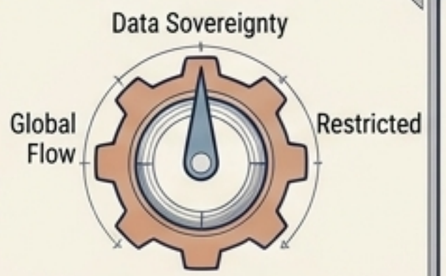
グローバル法規制マップ：法域ごとの知財実務への影響

米国 (USA)



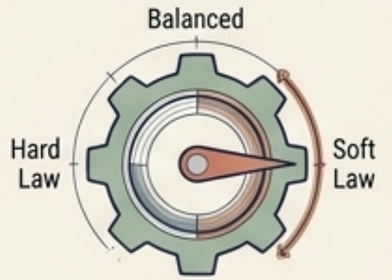
重心：人間中心 (Human-Centric)。発明者は自然人に限定。出願時の人間の重大な寄与と訓練データの適法性記録が不可欠。

欧州 (EU)



重心：データ主権・透明性。EU AI Act適用。リージョン固定、サブプロセッサ変更、ログ保存の合法的根拠が必須条件。

日本 (Japan)



重心：ソフトロー・社内統制。著作権は柔軟。ベンダー約款より社内の自主規程が法務リスクの差に直結。

「証拠パッケージ」要件（The Evidence Imperative）

「説明できないが正しい」は不可。
出力結果よりもプロセス証跡化がAI利用原則。

1. ソース証明

出典URL、取得日時、引用元のスニペット（引用片）。

2. トレーサビリティ

ツールの呼び出し履歴、検索クエリのログ。

3. モデル固定証跡

使用したモデル名、正確なバージョン（版情報）。

AI Evidence Package

4. 画面保全

承認画面やツールトレース画面のスクリーンショット（またはPDF）保全。

5. 人間介在証明

編集履歴、レビュー・承認者のID（誰が最終判断したか）。

知財部門の戦略オプション比較

[Option 1] 単一ベンダー集中

- コスト: 中
- 実現性: 高
- リスク: 高

ロックイン、法域対応の片寄り。初速は出るが長期的な交渉力が低下する。

[Option 2] 複数ベンダー併用 (推奨解)

- コスト: 中〜高
- 実現性: 中
- リスク: 低

設計・責任分界の複雑化。探索・統制・高機密を明確に分離可能（総合推奨）。

[Option 3] 自社オンプレ／エッジ実装

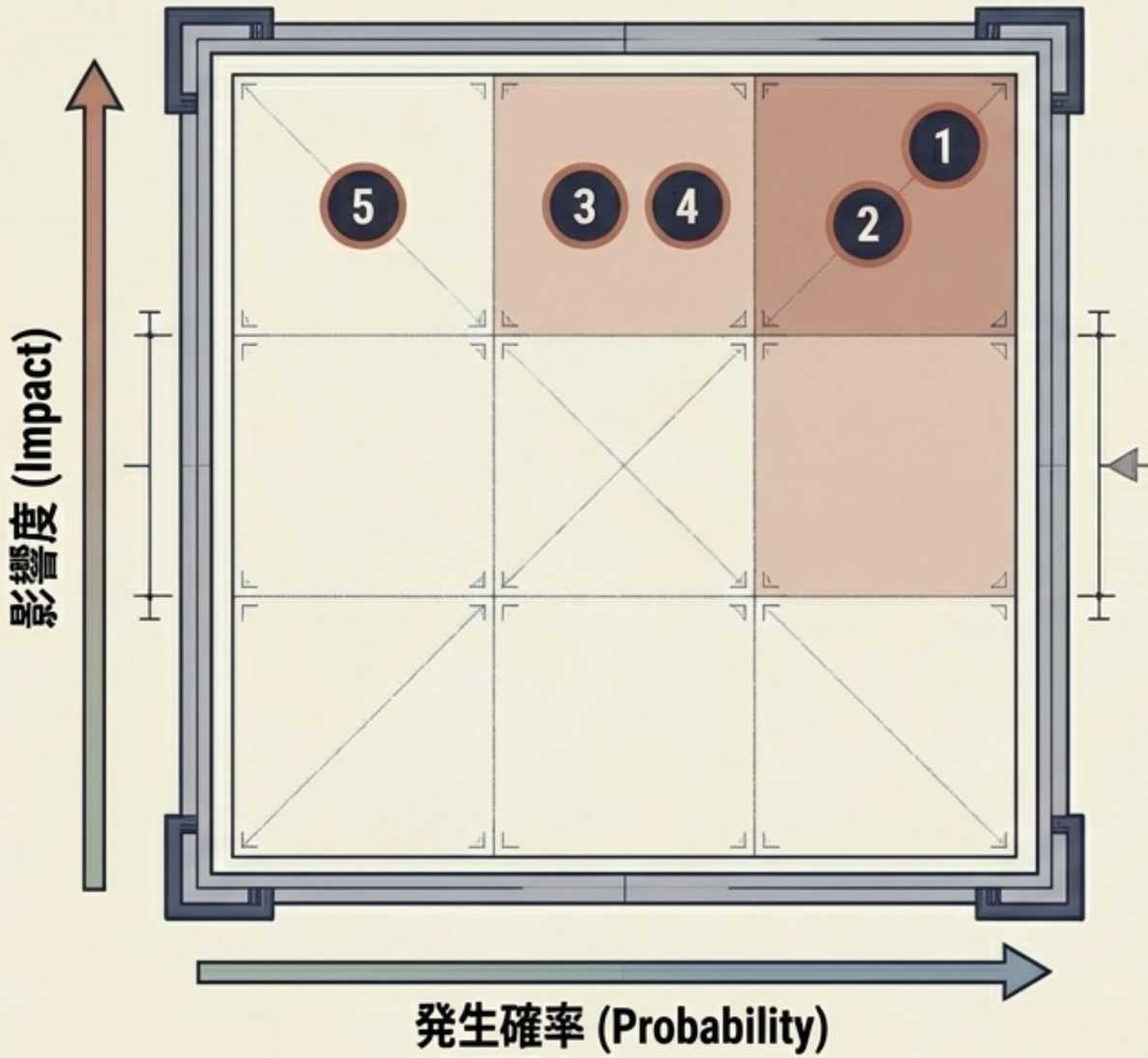
- コスト: 高
- 実現性: 低
- リスク: 低

運用負荷増大、業務UIの弱さ。全社一律には不向きだが「高機密帯」では最有力。

インサイト

業務UIはMicrosoft/Googleで固め、モデル層は交換可能にし、最高機密はNVIDIA等の専用レーンに逃がす「多層設計」が法的耐性とコストの最適解。

リスク・プロファイルと緩和マトリクス



1. ログ欠落・再現不能

原因: シャドーAI利用。
対策: SIEM連携、スクリーンショット保全義務。

2. モデル更新・廃止

原因: API Sunset、性能ドリフト。
対策: Reserved Capacity等の「版固定」、回帰評価。

3. データ越境・主権侵害

原因: 未固定リージョン。
対策: Region Pinning、高機密専用環境の分離。

4. 誤引用・幻覚

原因: 要約のみの転記。
対策: URL・引用片・取得日時・再実行結果の必須化。

5. UI自動操作の暴走

原因: Computer Useの誤操作。
対策: 高リスク操作の手動承認、Isolated VMの利用。

Implementation Roadmap: 2026-2030

1. 2026 (基盤統制期)

MCP/A2A採用。PoCから「本番統制」へ移行。証拠パッケージ様準の制定と、公開/高機密の2レーン分離。

2. 2027 (法規制順応期)

EU AI Act本格適用。監査ログ・版固定・データ越境管理の実務組み込み必須化。

3. 2028 (高機密隔離期)

権利行使・営業秘密の「専用実行環境化」が進展。二重承認の標準化。

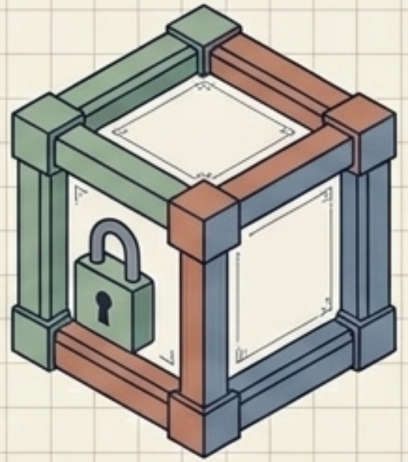
4. 2029 (評価基盤内製期)

特定ベンダー脱却。モデル切替とルーティング基盤の内製化が競争力のコアに。

5. 2030 (二層構造完成期)

「AIによる探索」+「人間責任による判断」の二層構造完成。交換可能なモデル層を持つ企業が覇者へ。

Conclusion: The Architecture of Responsibility



真の勝者は「最も多くのAIを使った企業」ではない。
「AIの出力を、いつ、どのモデルで、どの根拠に基づき、誰が承認したかを説明できる企業」である。

1. AUDIT	全知財業務プロセスを棚卸しし、「機密区分」と「人間承認点（ゲート）」を即座に定義せよ。
2. SEGMENT	業務UI面とモデル層、高機密専用レーンを切り離す「多層設計」をPoC段階から組み込め。
3. STANDARDIZE	ベンダー約款に依存せず、ログ輸出権を含む自社独自の「証拠・契約テンプレート」を確立せよ。