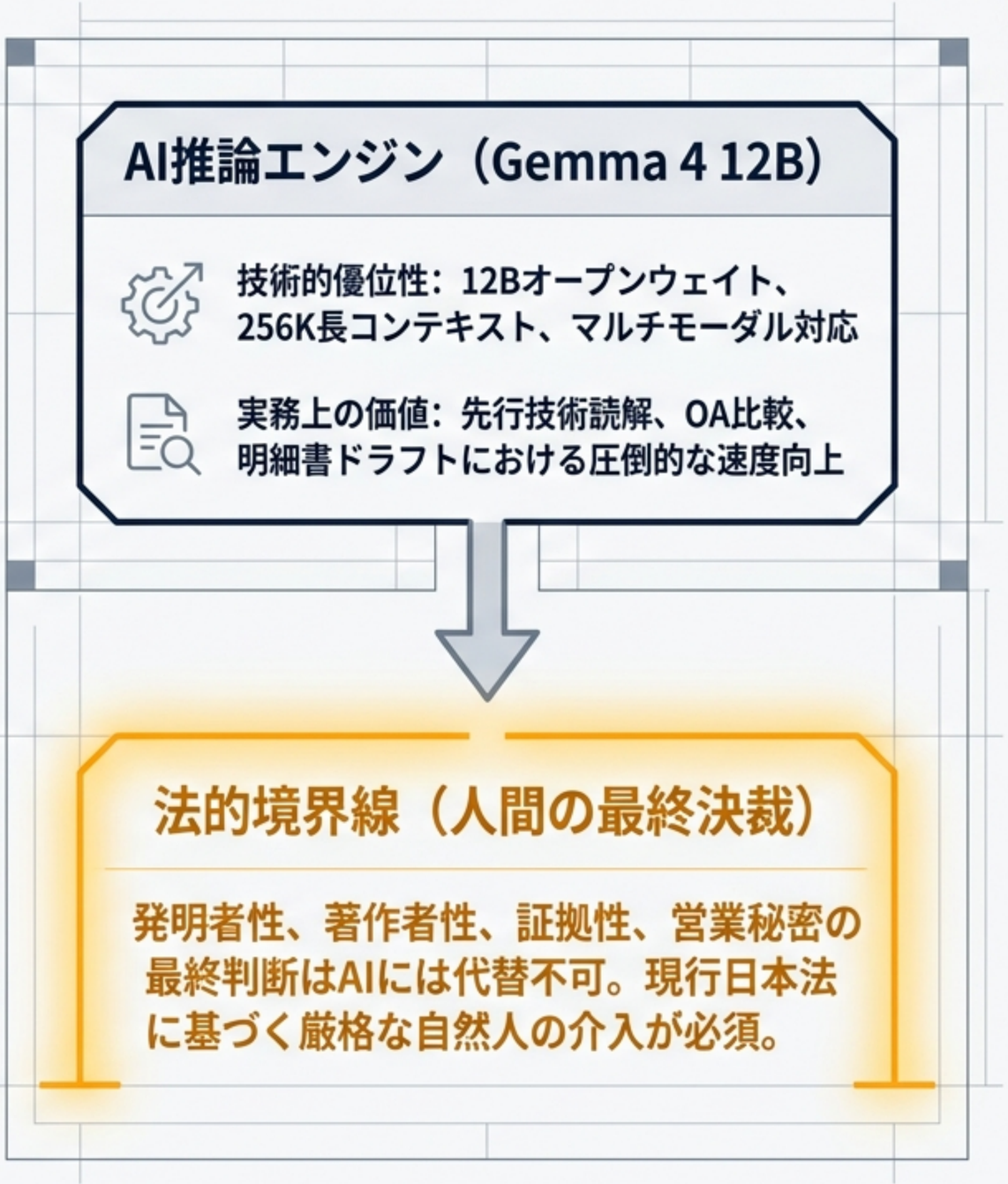
Gemma 4 12Bの知財実務への実装戦略

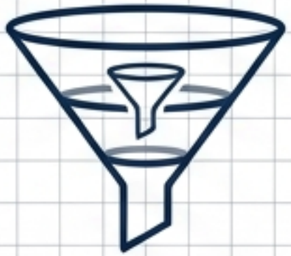
高機密情報をローカルで処理する次世代の起案・分析基盤。法的評価の最終決裁は「人」に委ねる、知財法務のためアーキテクチャ設計。



技術特性と知財実務の価値変換マトリクス

256K長コンテキスト & マルチモーダル

単一のデコーダーでテキスト、画像、PDF、図表を同時に長文処理



審査履歴の一括読解と相違点抽出

大量のOA履歴、特許図面、請求項を横断的に読み込み、瞬時に相違点表を生成。

12B オープンウェイト設計

ローカル環境で実行可能な軽量アーキテクチャ・Apache 2.0準拠

営業秘密と個人情報の完全保護

外部SaaS APIをバイパスし、不正競争防止法上の秘密管理性と個人情報保護法を遵守。

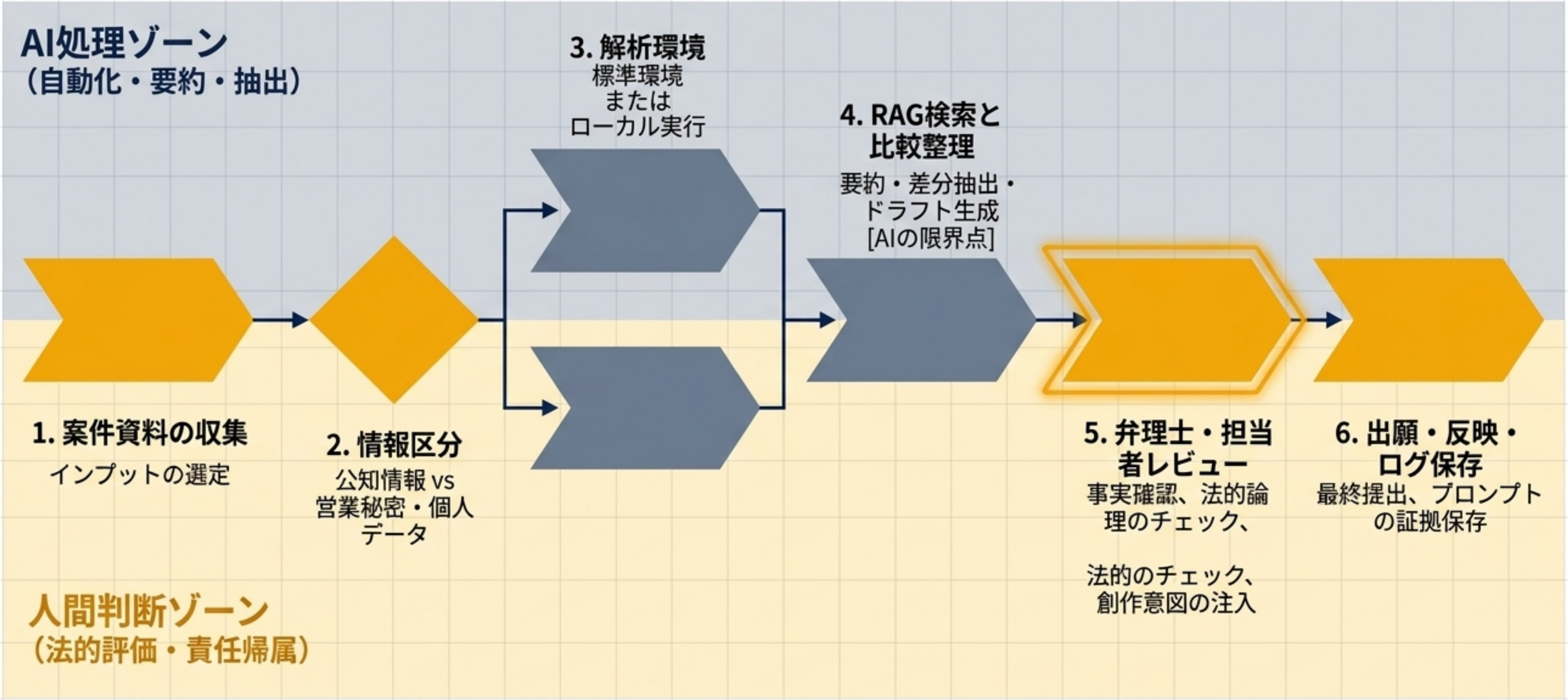
AIの限界（2025年1月カットオフ）

知識の陳腐化および幻覚（ハルシネーション）の不可避なリスク

RAG統合と人間による検証の必須化

J-PlatPatや社内DBとのRAG連携を前提とし、致命的な法的エラーを防ぐための人間によるファクトチェックが必須。

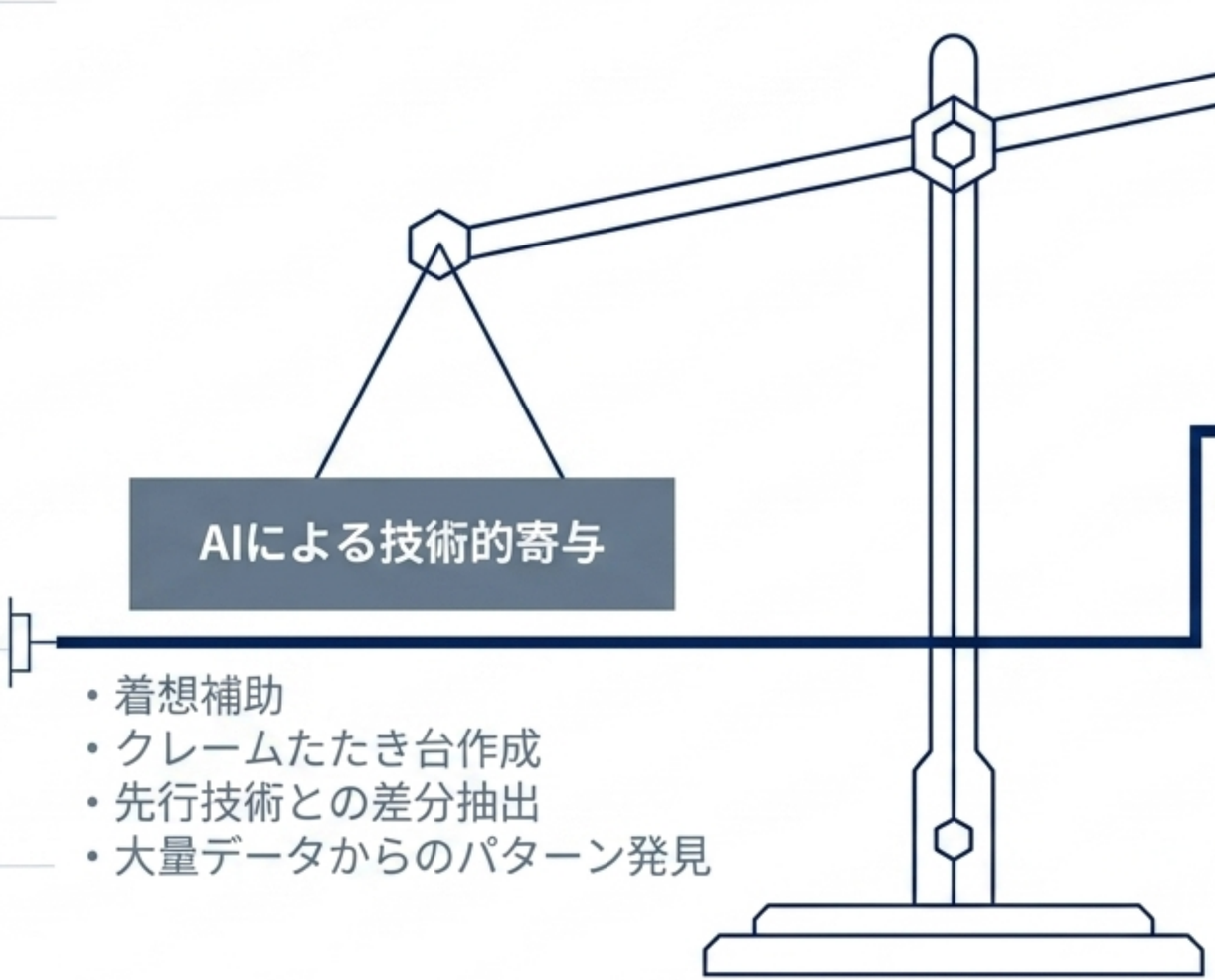
生成AIを組み込んだ次世代知財ワークフロー



知財分野別：効果・リスク・実装ルールの統括マトリクス

知財分野	主な効果	主要リスク	実務上の整理
特許出願・審査	長文比較、差分抽出、OA要約、ドラフト高速化	幻覚、法的評価の飛躍	起案補助まで。最終的な判断・法解釈は人が行う
著作権	下書き・翻案補助、表現案探索	類似性・依拠性、著作物性の誤認	創作意図と寄与を記録し、既存著作物の侵害を確認する
営業秘密	ローカル処理による漏えいの抑制	外部SaaSでの学習利用、秘密管理性の低下	高機密データは原則オンプレミスまたは閉域ネットワークで処理
商標	ネーミング候補生成、整理、説明文案作成	先行商標との類似、識別力不足	J-PlatPat検索を前提とし、人間が候補を削減する
訴訟・証拠	証拠束の整理、論点表、年表の自動作成	出所不明、証拠の再現性不足	元資料・出力・プロンプトのログ保存を必須とする

法的深掘り1：特許と発明者性（DABUS判決の教訓）



AIによる技術的寄与

- 着想補助
- クレームたたき台作成
- 先行技術との差分抽出
- 大量データからのパターン発見

人間の法的発明者性

絶対原則： 現行特許法上、発明者は「自然人」に限られる。

判例基準： DABUS事件　知財高裁　令和7年1月30日判決。AIを発明者として記載する出願は不適法。

実務要件： AIを使用した場合でも、誰が人間として「創作的寄与」を行ったかの記録・立証が実務上決定的となる。

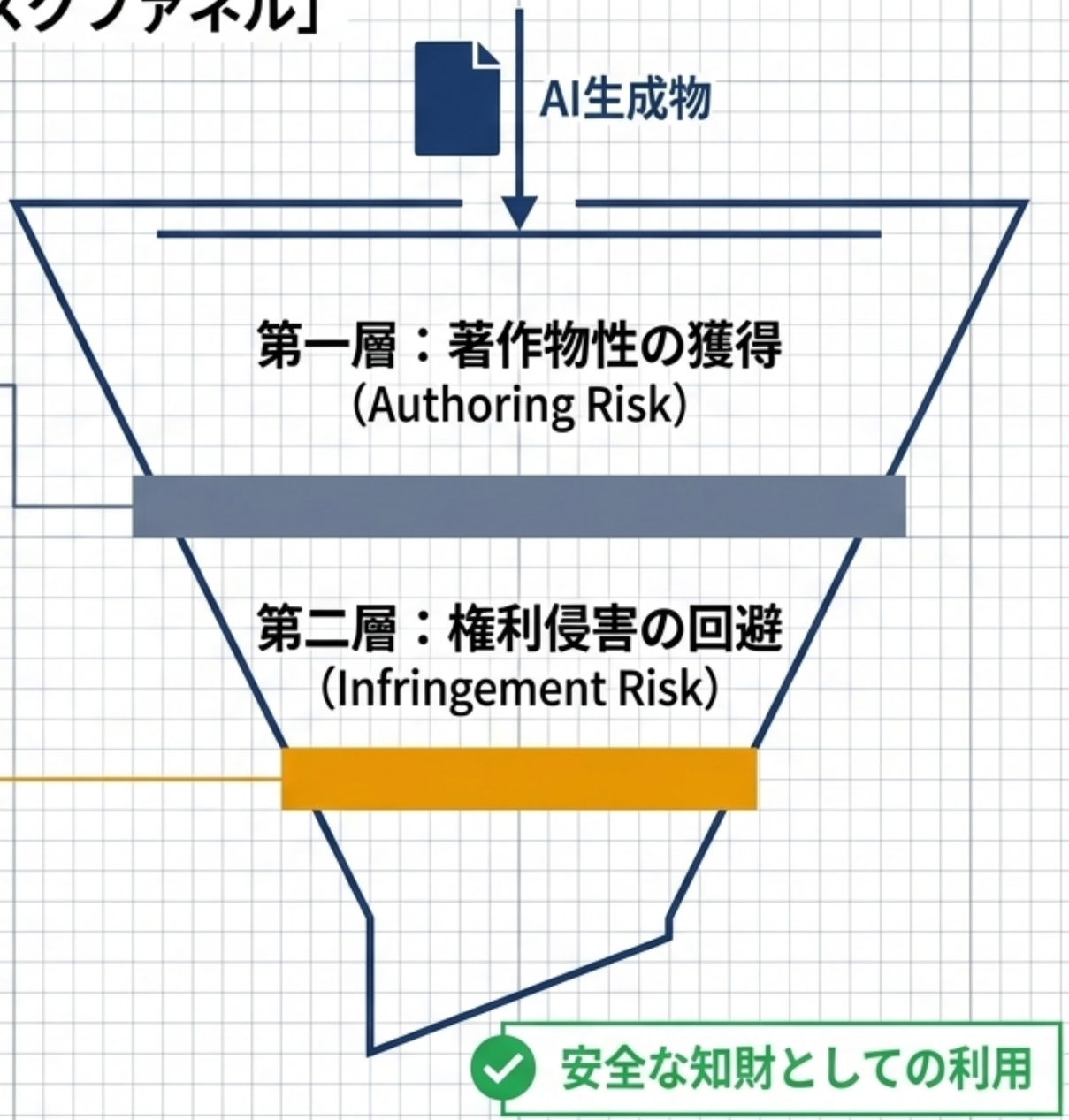
法的深掘り2：著作権における「二層のリスクファネル」

AI自律生成物は原則として著作物非該当。文化庁の指針に基づき、AIを「道具としての利用」に留めること。

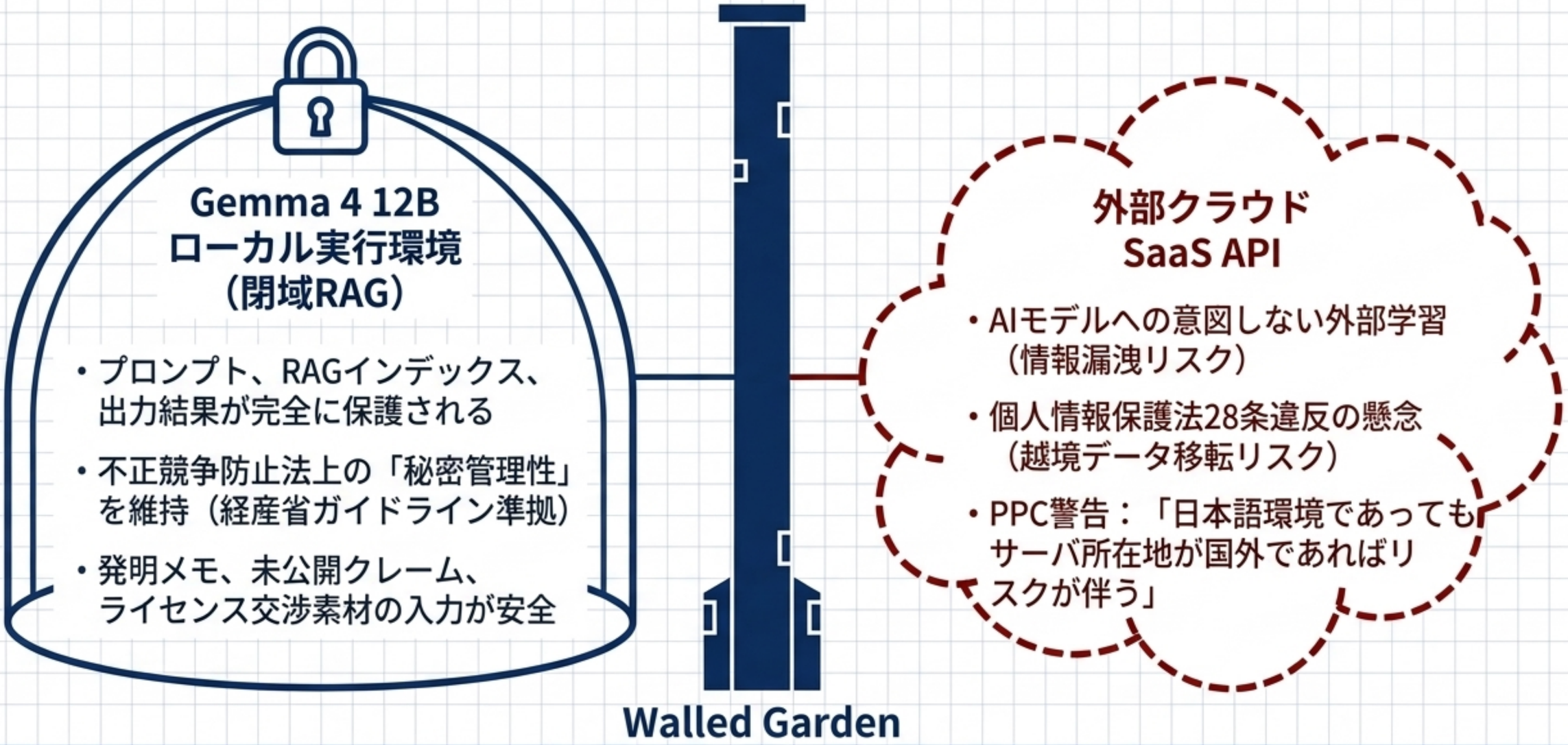
- 要件：詳細な指示、反復修正による「創作意図」と「創作的寄与」のドキュメント化が必須。

自社で著作物性を獲得しても、他者への侵害リスクは残存する。

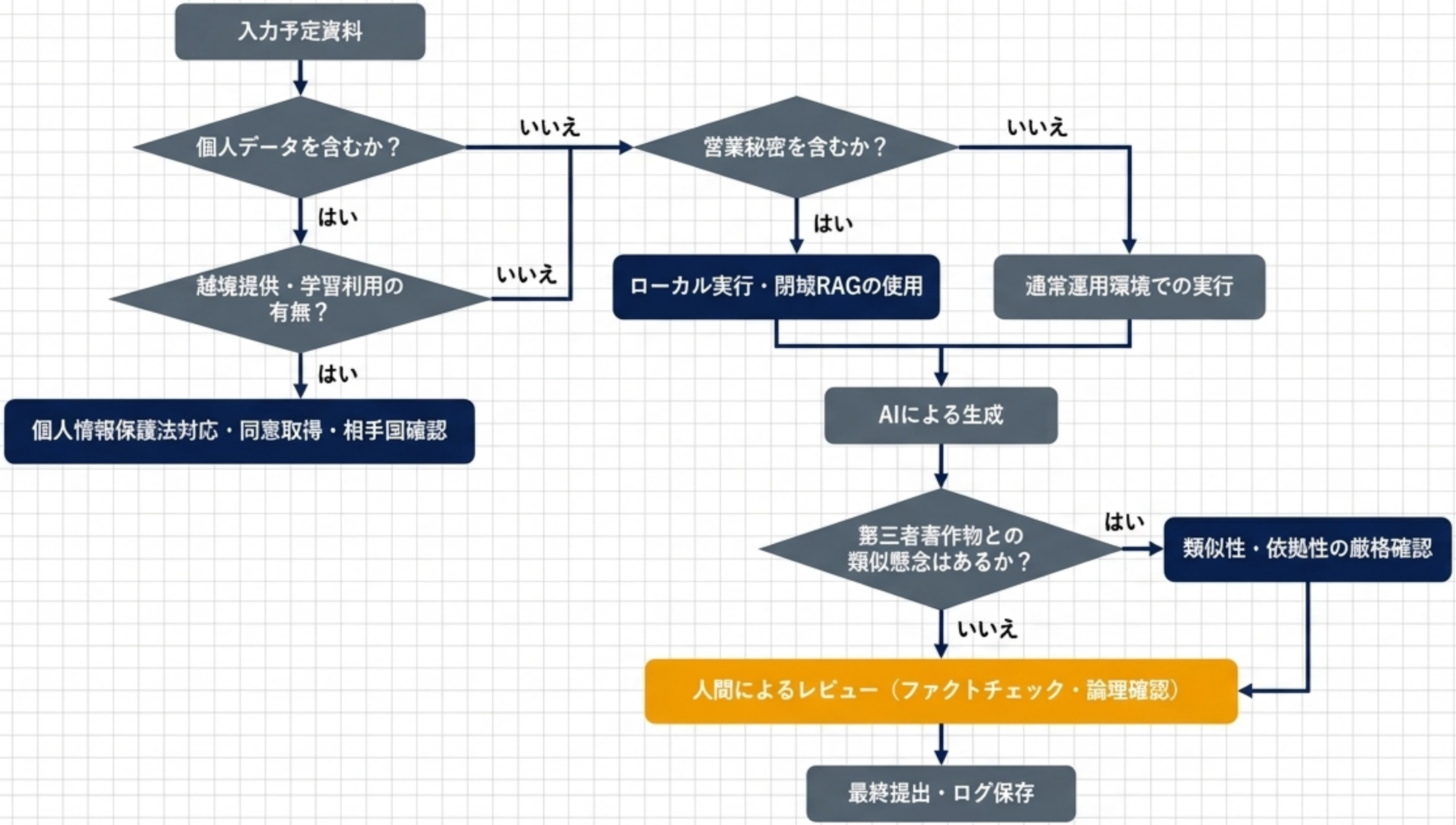
- 要件：既存の著作物との「類似性」および「依拠性」の厳密な確認。
- 特記事項：30条の4に基づく学習利用は「非享受目的」に限定。内部ファインチューニングの際は目的混在を徹底排除。



法的深掘り3：営業秘密・個人情報保護（ローカル実行の優位性）



実務執行デシジョンツリー（安全なAI運用フロー）



全社AIガバナンスの4本柱（METI・PPC・文化庁 準拠）

知財・法務における安全なAI運用アーキテクチャ

入力統制 (Input)

- データの機密分類の定義（個人データ、営業秘密、未公開発明）
- 高機密データに対する閉域・ローカル処理の義務化

出力統制 (Output)

- **外部配布前の人間による出典確認の義務化 [人間による判断]**
- 著作権類似性、商標重複、名誉毀損のスクリーニング

記録統制 (Traceability)

- 「証拠説明可能性」を担保するためのログ保存
- プロンプト、出力結果、参照元、レビュー履歴の完全保持

契約統制 (Contract)

- ベンダー契約における学習利用権限の明文化
- 監査権の確保および越境データ移転ルールの標準化

契約・ベンダーガイドライン（METI AI契約チェックリスト対応）

1. 入力データ利用制限

ベンダーによる汎用的なモデル学習、第三者提供、モデル改善、公開ベンチマーク生成を明示的に禁止する。一切の利用には事前の書面同意を要する。

2. 出力利用と非侵害の開示

ベンダーは非侵害を保証しないが、知財部門がリスクを正確に評価できるよう、AIモデルの生成条件および学習データの概要を開示する義務を負う。

3. ログ保存・監査対応

セキュリティ事故調査のために、認証ログ、アクセスログ、管理者操作ログ、生成ログの保存を義務付ける。また、必要に応じた監査要請に応じる体制を確保する。

4. 個人データ越境移転

サーバ所在地、再委託先、個人情報保護措置を事前開示すること。変更が生じた場合は遅滞なく通知する義務を負わせ、APPI（個人情報保護法）違反を未然に防ぐ。

実装ロードマップと重要KPI

実装フェーズ（Gantt Timeline）

短期

高機密案件向け閉鎖PoC、入力区分ルールの整備、
ローカル実行環境の確保、ログ保存設計の確立

中期

2025年1月のカットオフを補完する
J-PlatPat・法令DBとのRAG連携、
利用規約ひな型の改定、レビュー教育

長期

出願・係争の統合ナレッジ基盤化、
ファインチューニングのガバナンス構築

重要KPIダッシュボード

一次レビュー時間 XX分	OA比較表作成時間 XX分
出願ドラフト初稿時間 XX日	誤答訂正率 XX%
機密入力違反件数 0件	ログ保存率 100%

参照文献・規制トレーサビリティ

開発元仕様	・Google DeepMind Gemma 4 Model Card	・Apache 2.0 License	・Intended / Prohibited Use Policies
著作権・特許規制	・文化庁：AIと著作権に関する考え方、30条の4解説	・特許庁：発明者等の表示示について	・知財高裁：DABUS控訴審判決（令和7年1月30日）
ガバナンス・セキュリティ	・経済産業省：AI事業者ガイドライン 第1.2版	・経済産業省：AI契約チェックリスト、営業秘密管理指針	・個人情報保護委員会：生成AIサービスの利用に関する注意喚起等