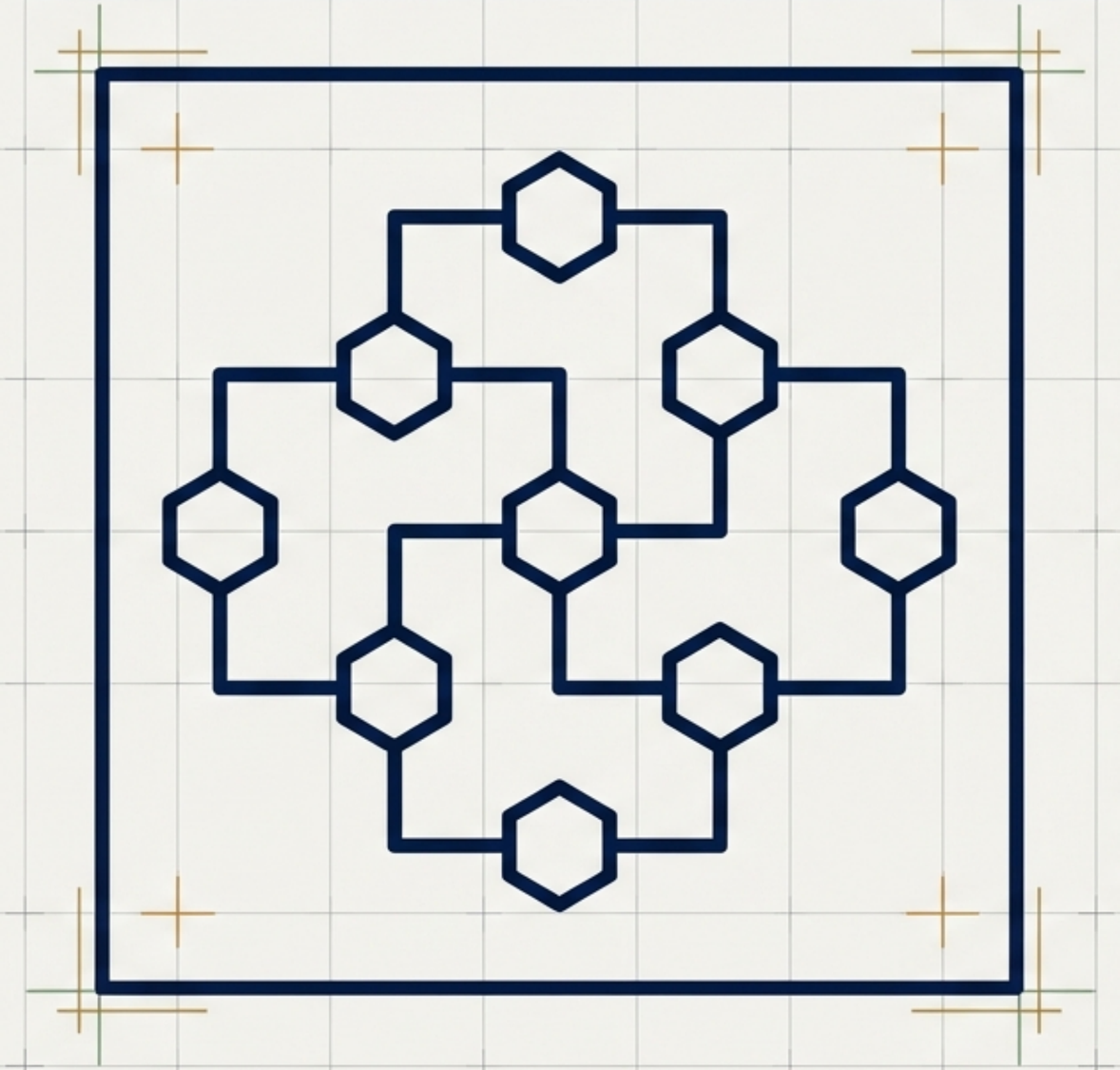


Perplexity Computerと知財 業務の未来

自律型エージェント時代における法的リスク・ガバナンス設計と導入ロードマップ

エグゼクティブサマリ：単なるIT導入からの脱却

進化 (Evolution)

手作業や単発チャットから、「数時間〜数か月に及ぶ自律型ワークフロー」へのパラダイムシフト。知財の調査・抽出プロセスが根底から覆る。

課題 (Challenges)

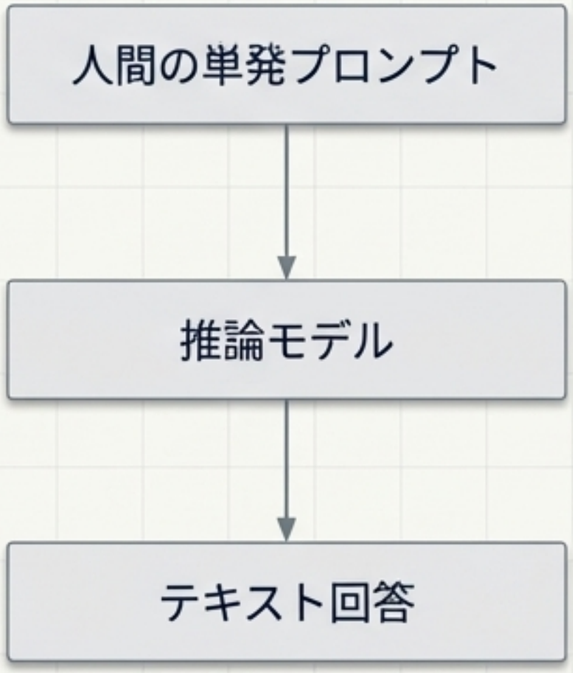
秘密情報、生成物の著作権、発明者性（DABUS問題）が複雑に絡む。　これはIT施策ではなく「全社的ガバナンス施策」である。

要件 (Requirements)

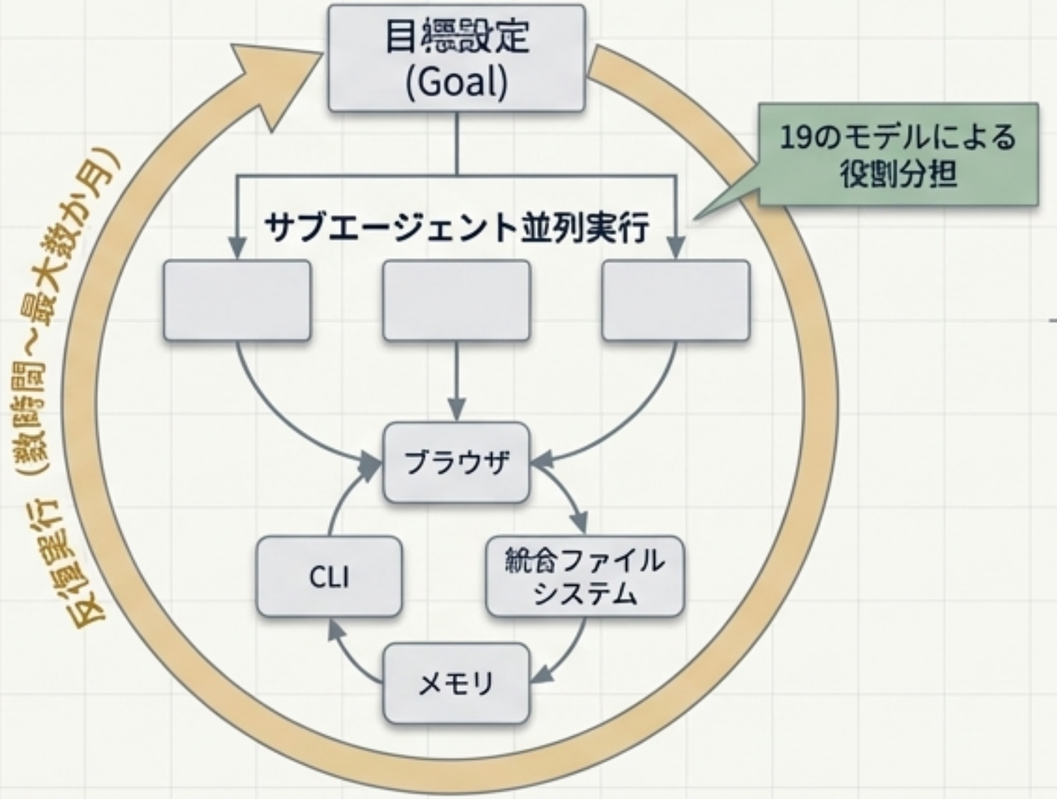
人間の「創作的寄与」の確実な記録保存、著作権法30条の4の射程限界の理解、および厳格な監査ログ統制が導入の絶対条件。

パラダイムシフト：「単発チャット」から「自律型業務遂行」へ

従来の生成AI (Traditional GenAI)



Perplexity Computer

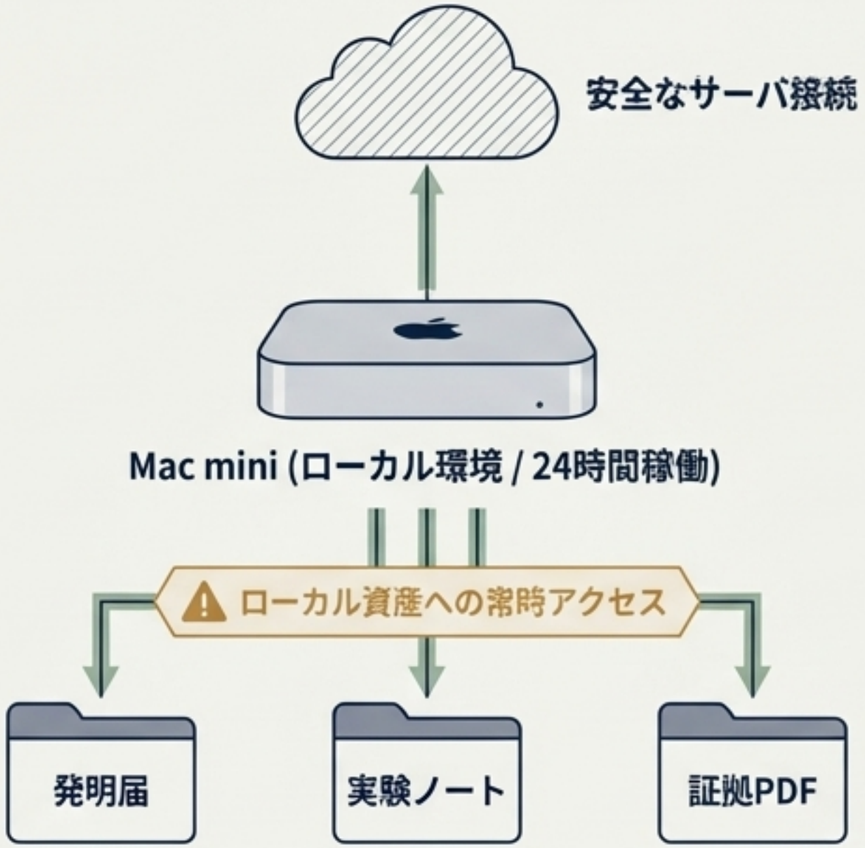


Computerは単なる回答エンジンではない。目標分解・並列実行・ファイル操作を自律的に反復する「実行エージェント」である。

Personal Computer：究極のデジタル代理人とその危うさ

アーキテクチャ

24時間365日稼働する専用端末とローカルアプリのハイブリッド構成。圧倒的効率化を生む。



知財への脅威

常時接続を前提とするため、アクセス制御が甘いと構造的に深刻な情報漏洩事故に直結する。

必須の安全装置

- センシティブ操作時の人間の承認 (HITL)
- 完全な監査証跡の取得
- 即時停止用のキルスイッチ

Enterpriseプランのガバナンス要件（知財投入の絶対条件）

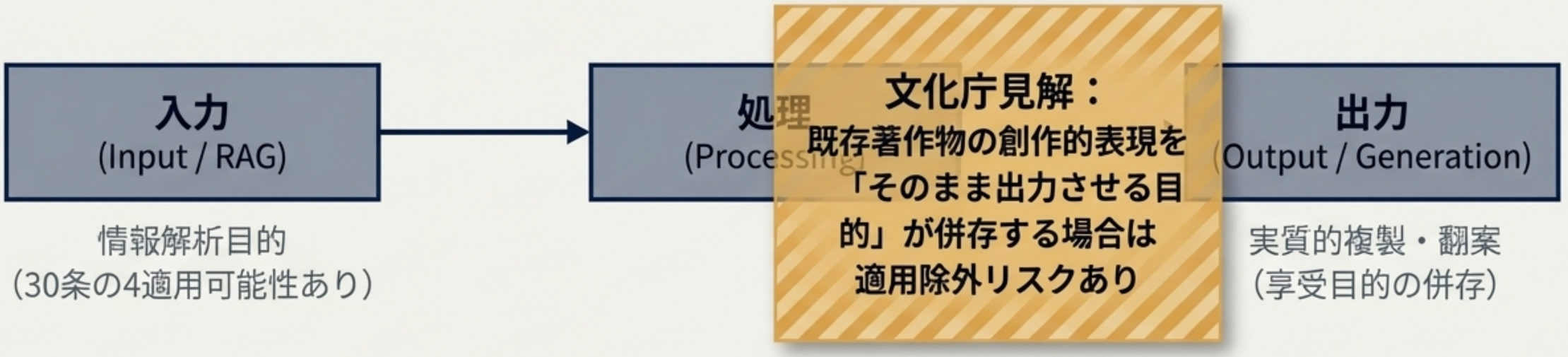
	Free / Pro / Max	Enterprise
AI学習用データ	デフォルト有効（過去分削除不可）	学習・ファインチューニング不使用 用（サードパーティ含む）
データ保持期間	ユーザー制御（制限あり）	スレッド添付分は原則7日で自動削除 （期間制御可能）
監査ログ・証拠性	不十分	入力から回答まで捕捉しWebhookでリアルタイム配送

結論：学習不使用＋監査ログ＋保持期間制御がない環境へ、発明情報や契約資料を投入することは「原則NG」。

知財法規別インパクト①：特許（発明者性の担保と証拠化）

法的要件	日本の特許法および東京地裁（DABUS事案）に基づき、「発明者は自然人に限る」のが大前提。
⚠ リスク	AIが抽出した発明候補をそのまま出願すると、人間による「創作的寄与」が不明瞭になり、冒認や無効リスクが生じる。
実務対策	「いつ・誰が・AIのどの出力を採用し、課題と解決手段を確定したか」を監査ログと案件IDで紐付けて強力に保全する。

知財法規別インパクト②：著作権（30条の4の限界とRAG出力）



RAGの罠

調査メモや報告書へのAI要約出力が、原文の実質的複製（享受目的）とみなされる危険性がある。

必須対策（4ステップ）

- ① 原典URL・公報番号の強制付与
- ② 引用の最小限化
- ③ 類似表現のシステム検出
- ④ 外部提出物の厳格な法務レビュー

知財法規別インパクト③：営業秘密・個人情報・商標・DB権

営業秘密（Trade Secrets）

不正競争防止法。AIへの無秩序な入力による「秘密管理性」の喪失リスク。

対策：機微情報の入力統制とEnterprise環境の強制。

個人情報（PII）

個情委（PPC）からの警告。目的外利用と無断学習のリスク。

対策：DPA締結、データのマスキング、越境移転要件のクリア。

商標（Trademarks）

自動ネーミング生成に伴う、既存の著名商標との混同および識別力低下リスク。

対策：最終的なJ-PlatPat等でのクリアランス維持。

データベース権（DB Rights）

EUにおける投資保護（sui generis権）とTDMオプトアウト（DSM指令）の抵触。

対策：海外DB収集における技術的統制とスクレイピング制限。

グローバル規制・判例動向と知財業務への波及

日本 (Japan)

2025年AI基本法。柔軟な権利制限（30条の4）と、その適用限界を巡る文化庁の継続的整理。

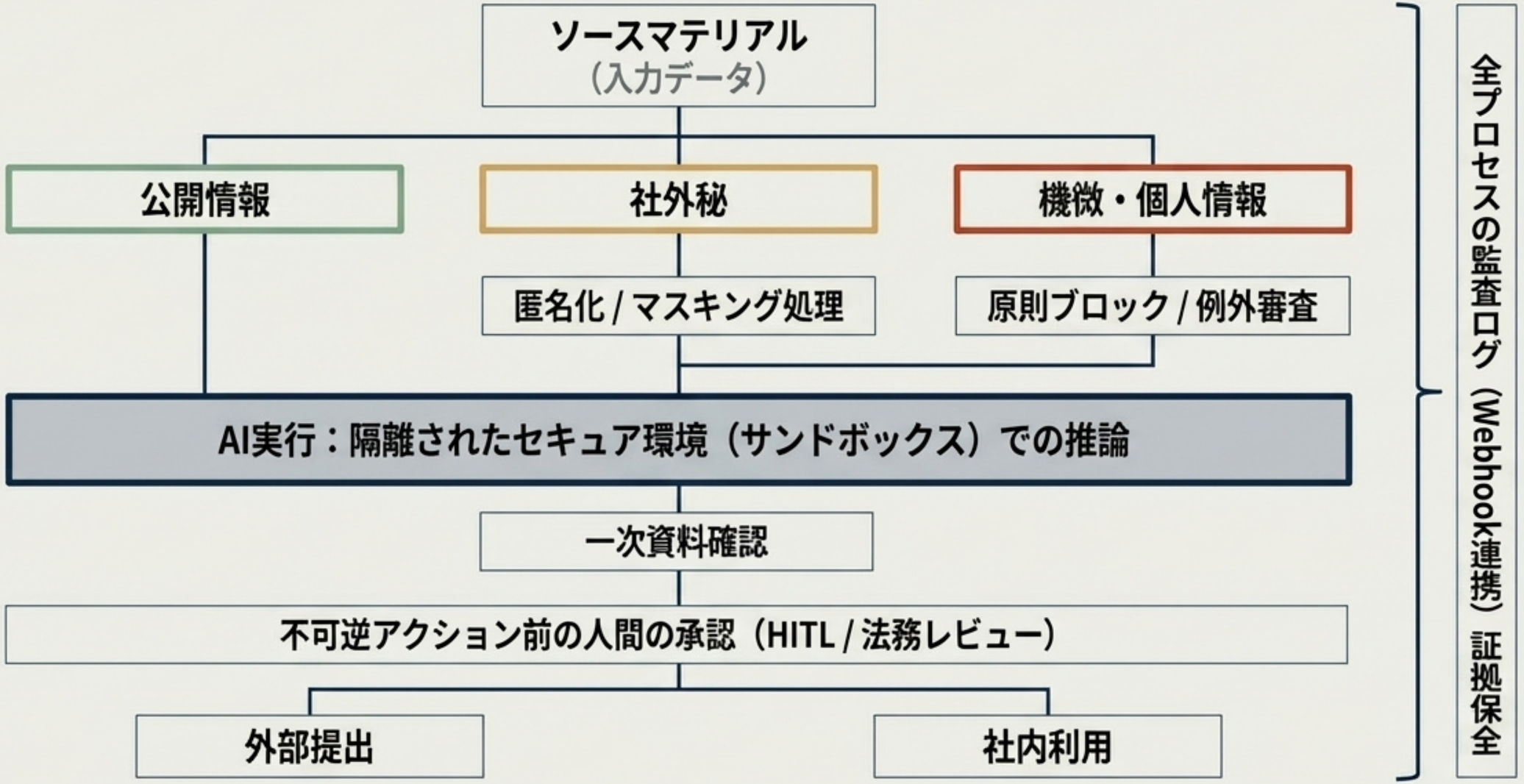
EU

AI Actに基づく透明性義務・ラベリング。DSM指令によるデータ取得統制とオプトアウトの尊重義務。

米国 (US)

著作権局のスタンス（著作物性に人間の表現決定が必須）。Reuters v. Ross等に見る学習利用とフェアユースの最新判例。

【シンセシス】知財データの入力・処理ワークフロー（意思決定ツリー）



リスク・コントロール・マトリクス（RCM）：全体像の把握

典型シナリオ	主要な法的論点	推奨対策	残余リスク
発明届ドラフトの投入	秘密管理性の毀損	Enterprise強制 ＋ 禁止区分策定	内部不正・端末リスク
発明者情報の投入	個情委(PPC)警告・目的外利用	匿名化投入とログ監査	ハルシネーション出力
論文表現のレポート混入	著作権侵害・30条の4の限界	原典URL付与・類似表現検出	事後的な類似性判断のブレ
AI提案の直接出願	発明者認定トラブル(DABUS)	AI利用欄の設置・案件ID紐付けログ	寄与度の線引き問題
AIエージェントの誤操作	管理責任・自律実行リスク	人間の承認(HITL) ＋ キルスイッチ	承認者の形骸化・見落とし

コンプライアンス・契約・証拠保全要件（ベンダーチェックリスト）

Contractual & DPA

- 「データの学習・ファインチューニング利用禁止」の明文化
- サードパーティ（他社AIモデル等）への学習データ提供禁止の担保
- 知財侵害・情報漏洩発生時の責任分界点の明確化

Technical Specifications

- 監査ログのWebhookによるリアルタイム配送と改ざん防止機能
- ファイル自動削除（原則7日）等の保持期間制御と社内DMS連携
- 隔離環境（サンドボックス・FUSE）での実行と内製システム連携API

導入ロードマップ（Phase 1: 短期 1〜3ヶ月）— ガバナンス確立と統制つきPoC

Month 1 | Month 2 | Month 3

ルール策定・契約合意

- 入力禁止ルール（機微情報・個人データ等）の明確化。DPA（学習不使用）の合意。

証拠保全インフラ構築

- 監査ログのWebhook連携による自社内での証拠保全化。

統制つきPoCの実施

- 公開情報限定の「先行技術調査」、マスキング前提の「契約レビュー補助」。一次資料確認の必須化。

導入ロードマップ（Phase 2/3: 中長期 3〜24ヶ月） ― 業務定着から自律運用へ

Months 3-12 (定着化)

プロンプト標準化と最小権限

指示の標準化、コネクタ権限の最小化（Least Privilege）の徹底。

社内規程の改訂

発明届への「AI関与記録欄」追加による発明者認定の防衛。

Months 12-24 (拡張・自律化)

知財業務OSとのシステム統合

Agent APIを活用した自社システムとの直接連携。

高度な証拠保全スキーマ

WORM（Write Once Read Many）やデジタル署名を用いた、訴訟に耐えうる記録保全。

サマリー：知財部門が直視すべき3つのネクストアクション

1

「学習不使用」と「ログ保全」を大前提とする

Enterprise環境での導入を必須とし、入力統制と監査ログの自社保全なしに機微情報を投入させない。

2

人間の役割を「作業者」から「監査者・法的判断者」へシフトする

AIが長期間の自律ワークフローを担う時代、知財部門のコア価値は「出力の適法性検証（HITL）」と「創作的寄与の証明」に完全移行する。

3

ガバナンスを「ブレーキ」ではなく「権利を守る武器」とする

厳格なプロセス設計と証拠保全こそが、DABUS問題や著作権リスクから自社の知的財産を防衛する最大の盾となる。