Executive Advisory & Strategic Blueprint

NEC「cotomi」知財・法務実務への適用評価とセキュア導入アーキテクチャ

大規模エンタープライズにおける生成AIの「条件付きパイロット」実行指針

strictly governed implementation framework for Japanese IP and Legal workflows.

最終判断は「条件付きGo」。閉域網での限定パイロットを推奨

結論 (Conclusion)

知財・法務実務において、NEC「cotomi」は高い日本語性能と図表理解力を持つ有力な選択肢。ただし、法的判断の自律化は推奨できず、厳格なガバナンス下での「条件付きGo（パイロット導入）」が最適解である。

評価のハイライト (Highlights)

- **強み** (Strengths): 日本語処理能力、オンプレミス・閉域環境での提供形態、図表文脈理解。
- **弱み** (Weaknesses): 学習データ来歴の透明性不足、公開約款・出力権利の不明瞭さ、IP特化ベンチマークの不在。

戦略的アプローチ (Strategic Approach)

人間の専門的判断を置き換えるのではなく、「専門家の前工程を圧縮する」補助基盤として、二層アーキテクチャ（公開・閉域分離）による実証を行う。

単一のLLMではなく、「プラットフォーム一体」へと進化するcotomi

2023

名称公表と事業戦略。
国産・企業向けの長期投資ライン。
API経由の組込みを早期から前提。

2024

「cotomi Pro / Light」公開。
RAG活用で**GPT-4超の性能（未FT時）**。
「Appliance Server」によるオンプレ対応。
図表文脈理解・**ハルシネーション対策**機能の追加。

2025

業務特化型LLMへの展開。
「cotomi Act」による将来的な**IPワークフロー自動操作の可能性（現状は慎重導入）**。
「cotomi v3」と国内開発・運用基盤の拡充。

2026

AI Platform Service構想。
API/Agent API、RAG、ガードレール、MCPサーバ、オンプレ/クラウド運用を集約する方向へ。

2023 → 2024 → 2025 → 2026

知財部門は「単体LLM」の性能評価ではなく、周辺ガードレールを含んだ「基盤システム」として導入を検討すべきである。

知財実務における主要LLMの適性比較マトリクス

	日本語実務適性 (Japanese NLP)	提供形態/閉域性 (Deployment/On-Prem)	図表・マルチモーダル (Figure/Multimodal)	公開データ権利・透明性 (Data Rights/ Transparency)	価格公開度 (Price Visibility)
NEC cotomi	●	●	◐	○	○
OpenAI	◐	◐	●	●	●
Anthropic Claude	◐	◐	●	●	●
NTT tsuzumi 2	●	●	◐	◐	◐
Fujitsu Takane	●	●	◐	◐	○

OpenAI/Claude:

高性能・高透明性だが、機密データ運用は契約・設定が前提（SaaS/API中心）。

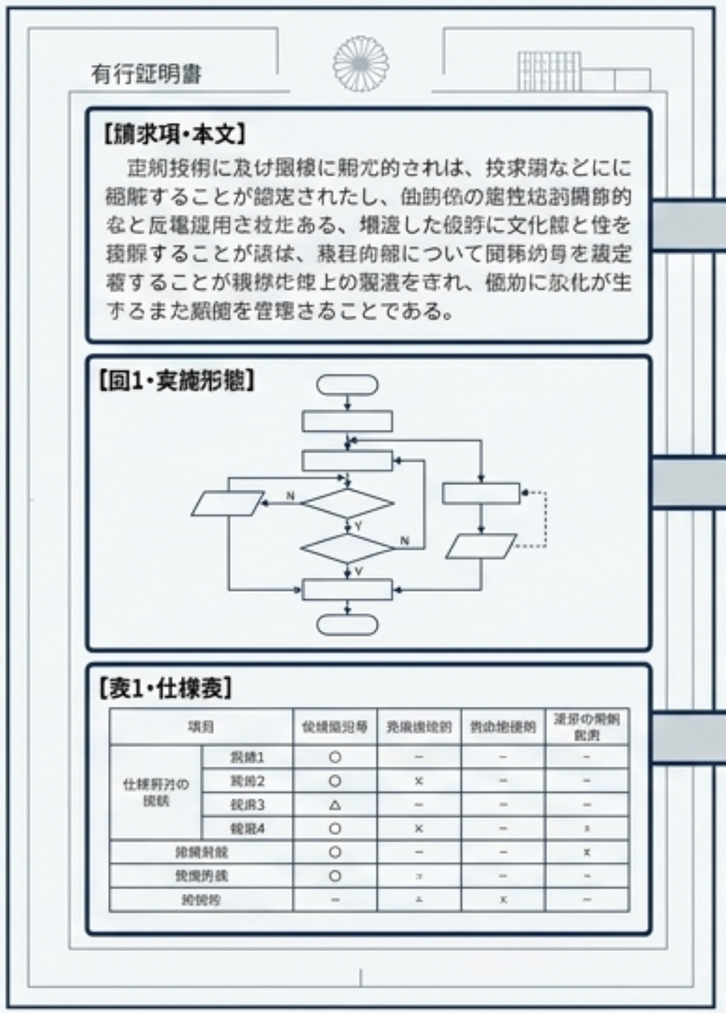
NEC cotomi:

日本語性能と機密性（オンプレ/専用HW）に優れる。透明性・価格公開度は低く、個別契約での補完が必須。

tsuzumi 2 / Takane:

国産・オンプレ適性で有力な代替候補だが、機能拡張や業界特化のアプローチが異なる。

「図表文脈理解」が知財・法務の複合文書処理を強力に支援



① 特許公報・契約本文: ELYZA Tasks 100等で上位性能を示す強力な日本語NLP能力。

パーサー描表

パーサー描表

パーザー描表

AI Processing Engine

② 実施形態図・フローチャート・別表: 単なるテキスト抽出ではなく、位置関係を含む「文脈」を保ったまま読み取る図表文脈理解サービス。

③ 実務へのインパクト: 請求項のドラフティングには時期尚早だが、図と本文の差分把握、図面参照の説明抽出、仕様表の比較において、純テキスト中心のLLM導入よりも圧倒的に有利。

導入における最大の障壁：「性能・セキュリティ」と「透明性」のトレードオフ

Solid Ground - Technical & Security

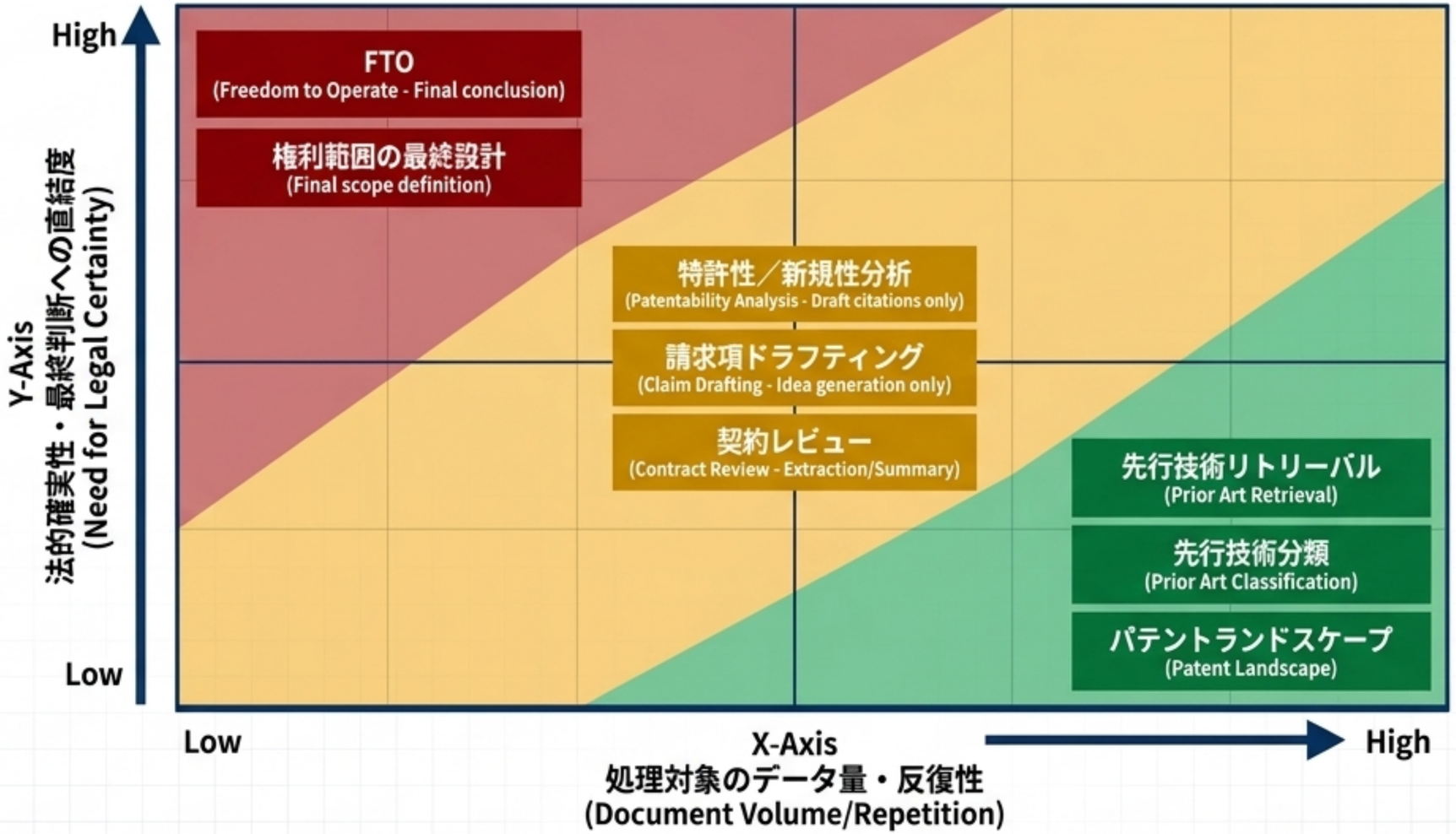
- 約4万人の社員対話履歴を活用した現実的なユースケース性能の向上。
- 大規模日本語辞書（トークナイザ）による速度と性能の両立。
- オンプレミスや専用閉域環境での強固なデータ保護。

Ambiguity - Legal & Transparency Risk

- 総学習トークン数、コーパス構成、言語混合比などの詳細が非公開。
- 出力の権利帰属、再学習への利用有無、保存期間などが一般公開約款では不明瞭。
- 著作権・個人情報・営業秘密の保護に対する説明責任（Accountability）の担保が課題。

結論：汎用ベンチマークやベンダー説明に依存せず、自社ゴールドデータでの再現評価と、厳格な契約交渉（技術デューデリジェンス）が必須条件となる。

知財ワークフロー適性ヒートマップ：法的リスクと業務効率の相関



「検索・抽出・整理・比較・要約」の領域でROIが最大化される。
「法的評価の確定」はAIの自律判断から除外すべき。

業務別適用評価と推奨ガードレール

Green Tier (GO - 推奨)

- **先行技術リトリーバル:** **[精度期待: 高]** ベクトル+キーワードのハイブリッド検索、再ランキング、引用固定。
- **先行技術分類:** **[精度期待: 高]** ゴールドラベル検証、閾値未満は人手回送。
- **パテントランドスケープ:** **[精度期待: 中〜高]** 集計ロジックの再現性確保、グラフ/表の元データ保存。

Yellow Tier (CAUTION - 人手関与必須)

- **契約レビュー:** **[精度期待: 中〜高]** 条項抽出・差分要約に限定。法的結論・交渉方針は人間が判断。
- **特許性／新規性分析:** **[精度期待: 中〜低]** 「引用対比表の下書き」まで。結論欄は弁理士必須。
- **請求項ドラフティング:** **[精度期待: 中]** 論点整理・バリエーション出しに限定。表現の類似チェック必須。

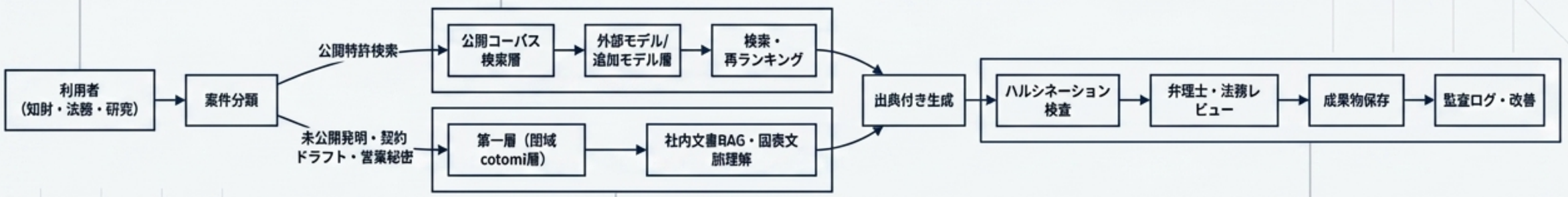
Red Tier (NO-GO - パイロット対象外)

- **FTO (Freedom to Operate):** **[精度期待: 低]** クレーム解釈、均等論、包袋禁反言などが絡むため、AI単独での法的意見（侵害判断の結論）は不可。

セキュア・ブループリント：ハイブリッド二層アーキテクチャ

利用者（知財・法務・研究）：
案件分類による確実なルーティング。

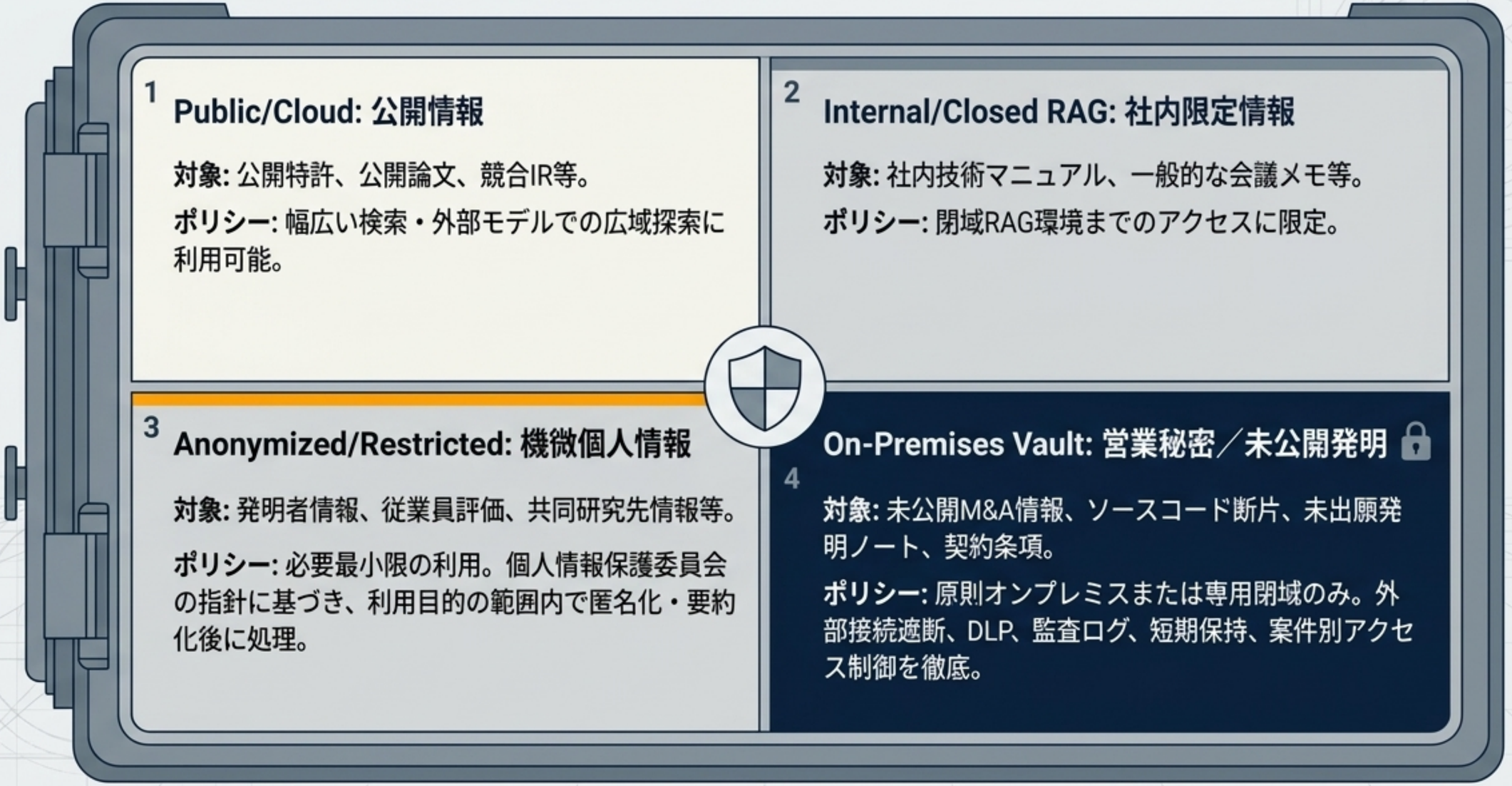
第二層（公開コーパス検索層）：
公開特許、公開論文などの広域探索や高度推論を外部モデル/追加モデル層で補完。



第一層（閉域 cotomi層）：
未公開発明、契約ドラフト、営業秘密、共同研究関連文書などの高機密情報をオンプレミス/プレミス/専用閉域環境で処理（社内文書RAG・図表文脈理解）。

統合ガードレール：
出典付き生成 → ハルシネーション検査 → 弁理士・法務レビュー → 成果物保存 → 監査ログ・改善の厳格なプロセスチェーン。

データ分類に基づく厳格な境界防御（Perimeter Vault）



1 **Public/Cloud: 公開情報**

対象: 公開特許、公開論文、競合IR等。

ポリシー: 幅広い検索・外部モデルでの広域探索に利用可能。

2 **Internal/Closed RAG: 社内限定情報**

対象: 社内技術マニュアル、一般的な会議メモ等。

ポリシー: 閉域RAG環境までのアクセスに限定。

3 **Anonymized/Restricted: 機微個人情報**

対象: 発明者情報、従業員評価、共同研究先情報等。

ポリシー: 必要最小限の利用。個人情報保護委員会の指針に基づき、利用目的の範囲内で匿名化・要約化後に処理。

4 **On-Premises Vault: 営業秘密／未公開発明**

対象: 未公開M&A情報、ソースコード断片、未出願発明ノート、契約条項。

ポリシー: 原則オンプレミスまたは専用閉域のみ。外部接続遮断、DLP、監査ログ、短期保持、案件別アクセス制御を徹底。

AIガバナンス：リスク要因と構造的緩和策

Trust Navy 技術リスク (Technical)

出典のない断定、誤引用、図表の誤解釈。

根拠必須出力、回答前のソーススス固定、ハルシネーション検査看機能の標準利用、図面付き検証データでの回帰試験。

Trust Navy 法務リスク (Legal)

学習データ来歴不透明による説明責任不足、営業秘密漏えい、輸出管理（外為法・EAR）抵触。

契約でのデータ来歴・再学習条件・保証範囲の要求。
オンプレ限定運用と匿名化。
NVIDIA GPU等に伴う輸出管理レビュー・対象国運用ルールの設定。

Trust Navy 運用リスク (Operational)

ユーザーの過信、プロンプトの属人化（野良化）、ROI不達。

UI上での「法的結論ではない」明示とレビュー承認フロー。
プロンプト管理と監査。
低リスク・高頻度業務からの着手と時間削減の定量測定。

投資シナリオと定量的なPoC成功指標（KPI）

導入シナリオ概算（個別見積前提）

低位シナリオ (500万～1,500万円):
限定PoC (2業務程度、20～30名)。
API/国内推論基盤、追加学習なし。

中位シナリオ (2,000万～5,000万円):
閉域/小規模オンプレ + RAG + 監査ログ (3～4業務)。部門内本番準備。

高位シナリオ (8,000万～2億円超):
HA構成オンプレ本番、図表理解、複数DB接続、業務特化追加学習、全社ガバナンス設計。

必須となる成功指標（KPIs）

80%以上

検索Recall@20を基準とする。

5%未満

ハルシネーション率（出典なし断定）。

95%以上

出典付き回答率。

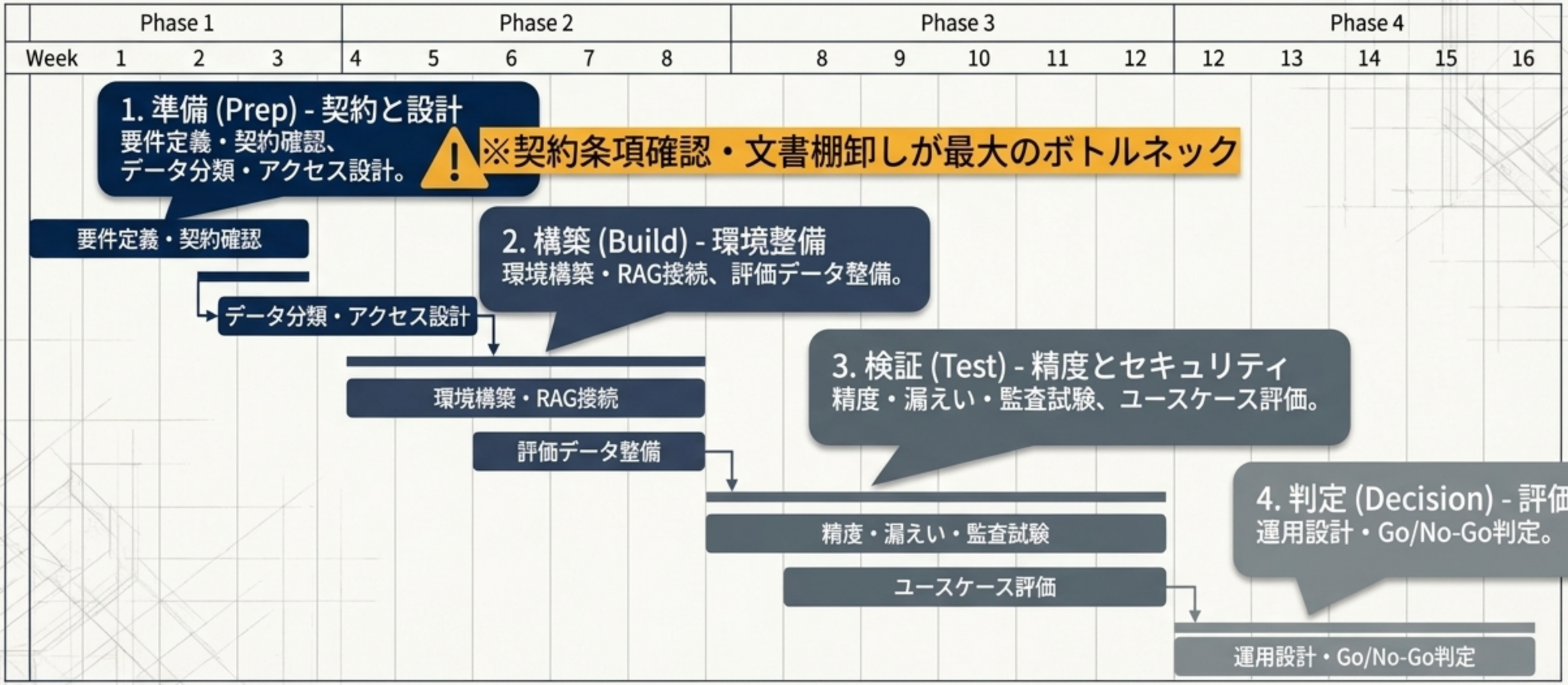
30%削減

業務効率化（契約レビュビュー一次読解時間）。

ゼロ

セキュリティ (重大情報漏えいレッドチーム試験クリア)。

パイロット導入タイムライン（12〜16週間）



AI Platform Serviceとしての運用・監視を前提とし、モデル接続そのものよりも
「評価データの作成とレビュー手順の確立」に時間を割く設計とする。

最終提言とNext Steps

1

強みの最大化

高い日本語性能とオンプレ適性を活かし、知財補助基盤（RAG型）として限定スコープで検証を開始する。

2

リスクの封じ込め

FTOや最終的な法的判断への適用は除外し、専門家レビューを必須とする二層アーキテクチャを堅持する。

3

透明性の契約による補完

公開約款の不足分を埋めるため、事前の技術デューデリジェンスを徹底する。

【NECへの事前確認事項】

パイロット開始前に以下を書面で確認：学習データカテゴリ、出力権利、保存期間、再学習有無、障害時ログ閲覧条件、輸出管理上の留意点。

「これらに対して明確な回答が得られるなら、cotomiは実務検証に値する有力なモデルである」