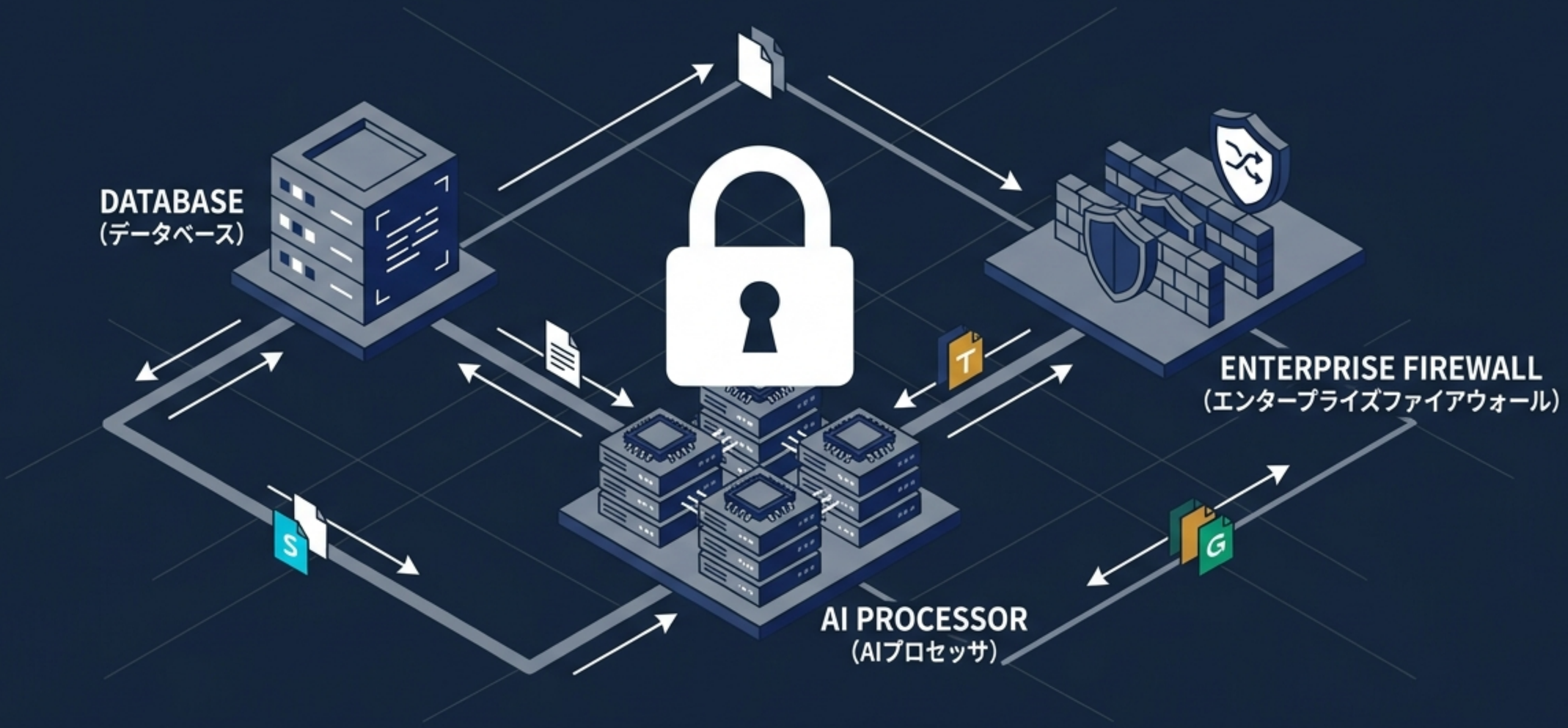
次世代知財AIアーキテクチャ設計および情報セキュリティ評価報告書

生成AIの社内導入における新規性喪失リスクの排除と、エンタープライズITガバナンスへの適合性評価



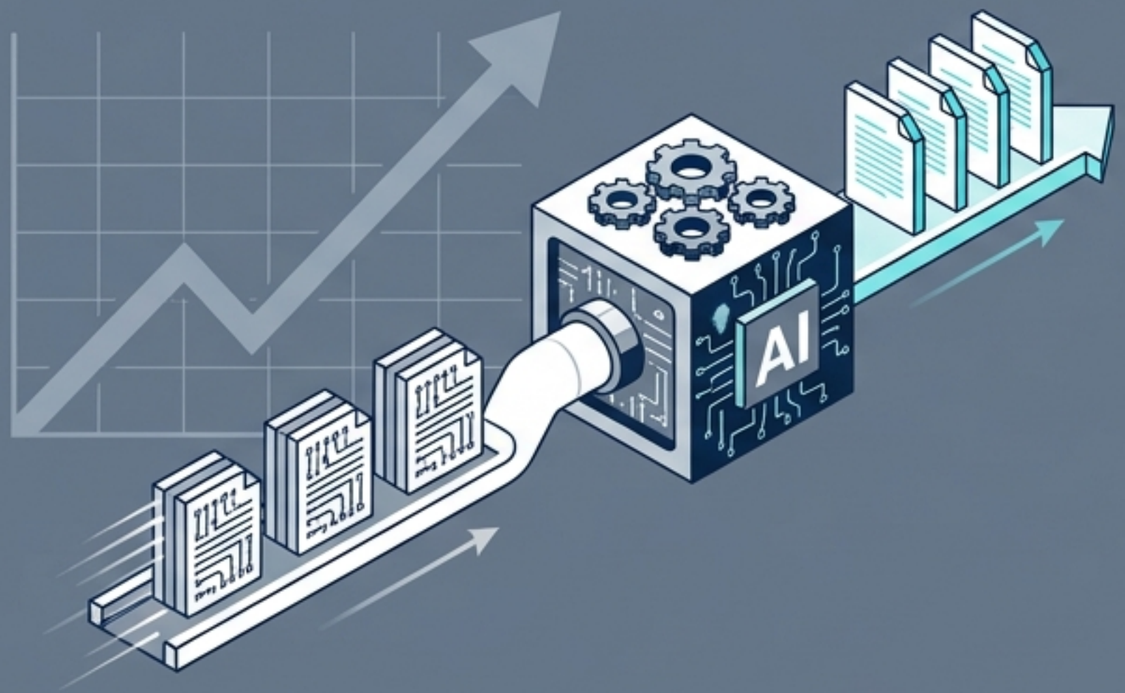
対象ツール：TOKKYO.AI / Summaria / Genzo AI

提出先：情報システム部門・セキュリティ監査委員会

知財管理のパラダイムシフトと、情報システム部門が直面するジレンマ

事業部門の要請 - アジリティ

生成AIによる知財業務の劇的な効率化（特許明細書のドラフティング、先行技術調査、非構造化データからの発明抽出）。



情報システム部門の懸念 - ガバナンス

知的財産（最重要機密）のパブリックSaaS入力による「新規性の喪失」および「モデル再学習を通じた競合への情報漏洩」リスク。

結論：厳格なコンプライアンス要件と事業アジリティを両立する「セキュア・アーキテクチャ」の証明が必須である。

パブリックSaaS環境における未公開知財データの流出ベクトル（リスク可視化）

Input (企業環境):
未出願の発明概要（Trade Secrets）を入力。

Transmission (パブリッククラウド):
API/Web経由で送信。

Risk Point A (Data Persistence):
プロバイダー側のサーバーにプロンプト履歴として永続保存される（標的型攻撃の的）。

Risk Point B (Model Retraining):
LLMの継続的学習・ファインチューニングデータセットとして吸収される。

Catastrophic Output (競合他社):
他社の類似プロンプトに対し、自社の機密情報が出力される（特許法上の「公知」となり新規性喪失）。

一般的な業務効率化ツールとは異なり、知財業務においては「交差汚染 (Cross-contamination)の完全な排除がシステムレベルで求められる。

情報システム部門が要求する「知財AIセキュリティ・ベースライン」4要件

Secure IP AI

Zero Data Retention（データ学習の完全なオプトアウト）

バックエンドLLM（OpenAI, Azure, AWS, Anthropic等）のエンタープライズAPI契約に基づく、学習利用の技術的・法的ブロック。

Logical Isolation（マルチテナント環境の論理的分離）

データベースレベルでの専用インスタンス化、または他の顧客データとの完全な隔離（交差汚染ベクトルの遮断）。

PII Stripping（匿名化処理とデータプロキシ）

外部API送信前のサーバーサイドでの個人識別情報（ユーザーID等）の事前ストリッピング機構。

Ephemeral Storage（データの揮発性とライフサイクル管理）

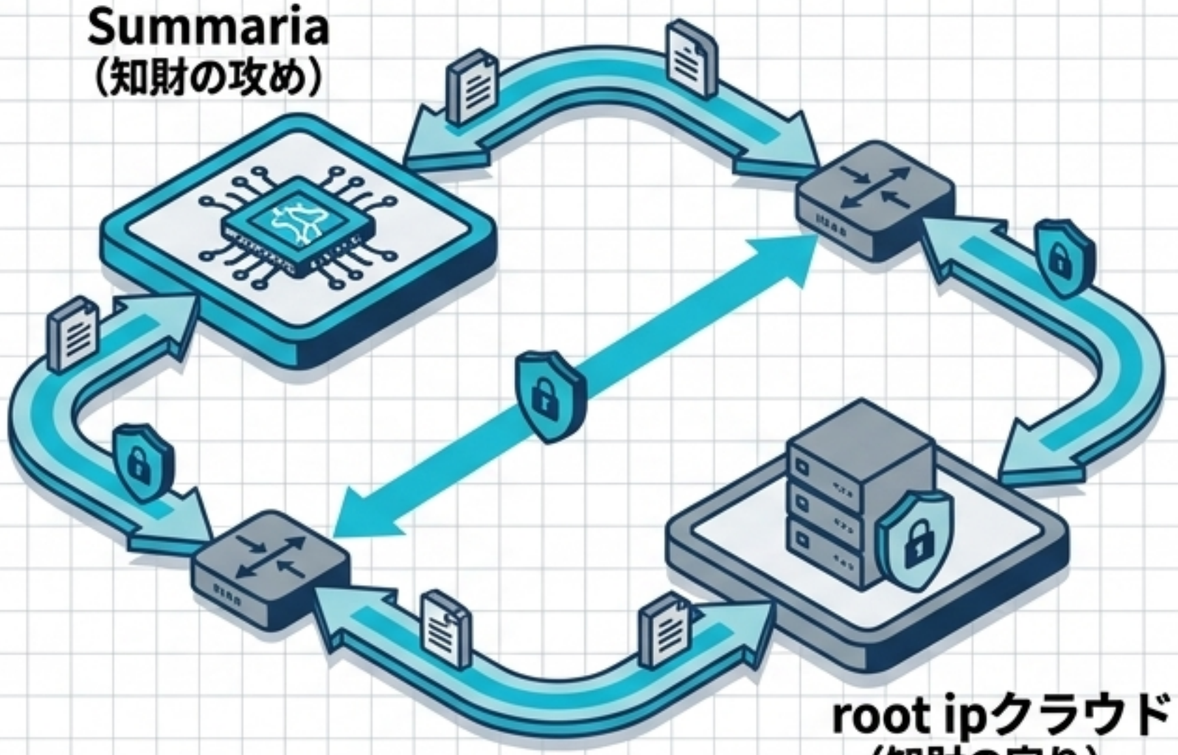
クラウド上のデータ永続化を防ぐ、セッション終終了時や一定期間経過後の自動破棄（時限消去）メカニズム。

Summaria：実務家の知見から生まれた「特許文書読解支援」特化型AI

Core Profile

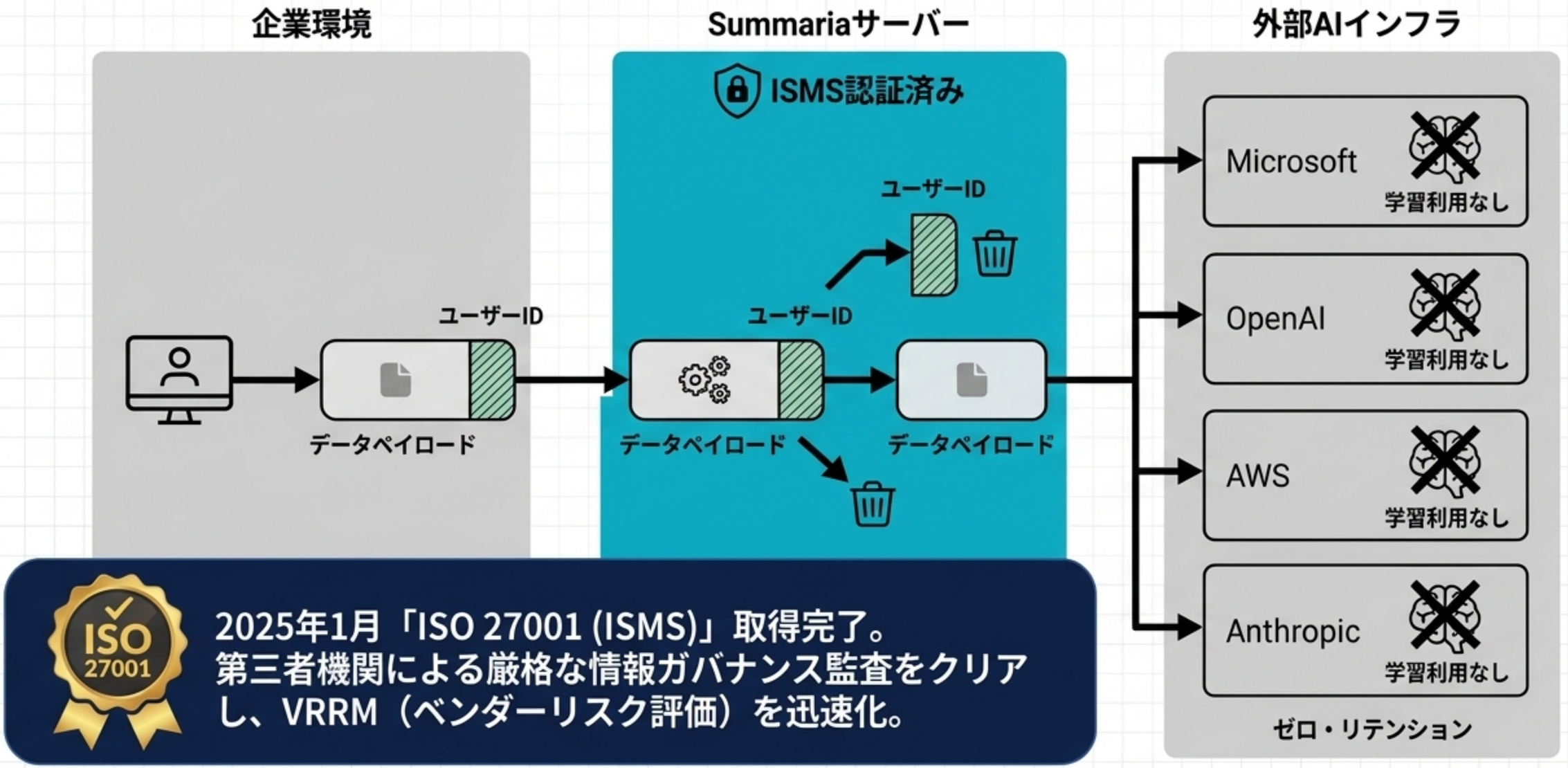
開発元:
パテント・インテグレーション株式会社（代表は受講生2,743人を抱える現役弁理士）。

設計思想:
長大な明細書からの実施例抽出、クレーム（請求項）解析、技術的範囲の特定など、研究者・知財担当者の「読解アシスト」に特化。



既存の知財管理システムとのセキュアなAPI連携を実現。IT資産のサイロ化を防ぎ、特許権取得から維持管理までを一気通貫で効率化。

Summaria アーキテクチャ：マルチLLMルーティングと匿名化プロキシ機構



ISO 27001

2025年1月「ISO 27001 (ISMS)」取得完了。
第三者機関による厳格な情報ガバナンス監査をクリアし、VRRM（ベンダーリスク評価）を迅速化。

TOKKYO.AI (Private版) ：出願準備から類似検索までを網羅する統合型プラットフォーム

プラットフォーム概要: リーガルテック株式会社（2012年設立）が提供する、法務・知財向けエンタープライズ統合システム。

主要機能群（Core Functions）

機能（Feature）	詳細（Detail）
ChatTokkyo（AIチャット）	GPT-4o等活用、発明のライフサイクル加速
AIテキスト検索 / 類似特許	文章入力による文脈分析・無制限検索
生成AIドラフティング	特許明細書のたたき台作成
AIイメージ商標検索	アップロード画像に基づくロゴ検索
知財判断蓄積・育成支援	出願・維持判断のプロセス可視化（2026年3月提供開始）

特許データ収録範囲（Data Coverage）

対象国・地域（Region）	収録期間（Coverage）
日本（Japan）	1989年以降
米国（United States）	2005年以降
欧州（Europe）	1978年以降
中国（China）	1985年以降
韓国（South Korea）	1968年以降
国際出願（PCT）	1978年以降

TOKKYO.AI アーキテクチャ：専用プライベート環境とハイブリッドAI基盤

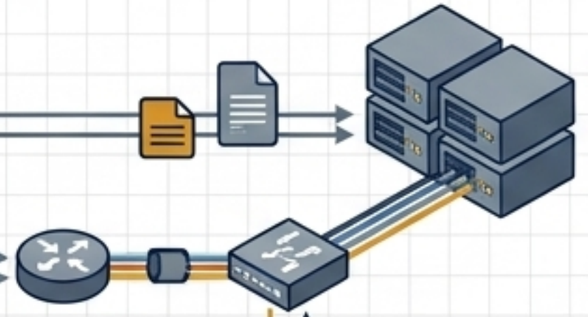
Public SaaS Risk（交差汚染リスク）

共用環境におけるデータ混在と外部流出の懸念

Private Tenant Vault（専用テナント&AI基盤）

1. The Vault（専用テナント）

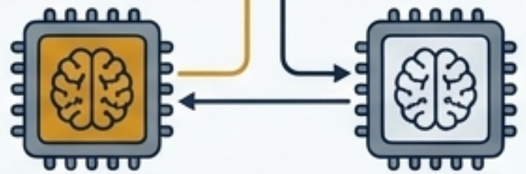
導入企業ごとに論理的に分離された完全なプライベート環境。検索クエリ、プロンプト履歴、アップロード文書の外部流出ベクトルを物理的・論理的に遮断。



2. The Engine（Xシステム）

膨大なグローバル特許データをリアルタイム処理する独自ビッグデータ基盤。高いスケーラビリティを担保。

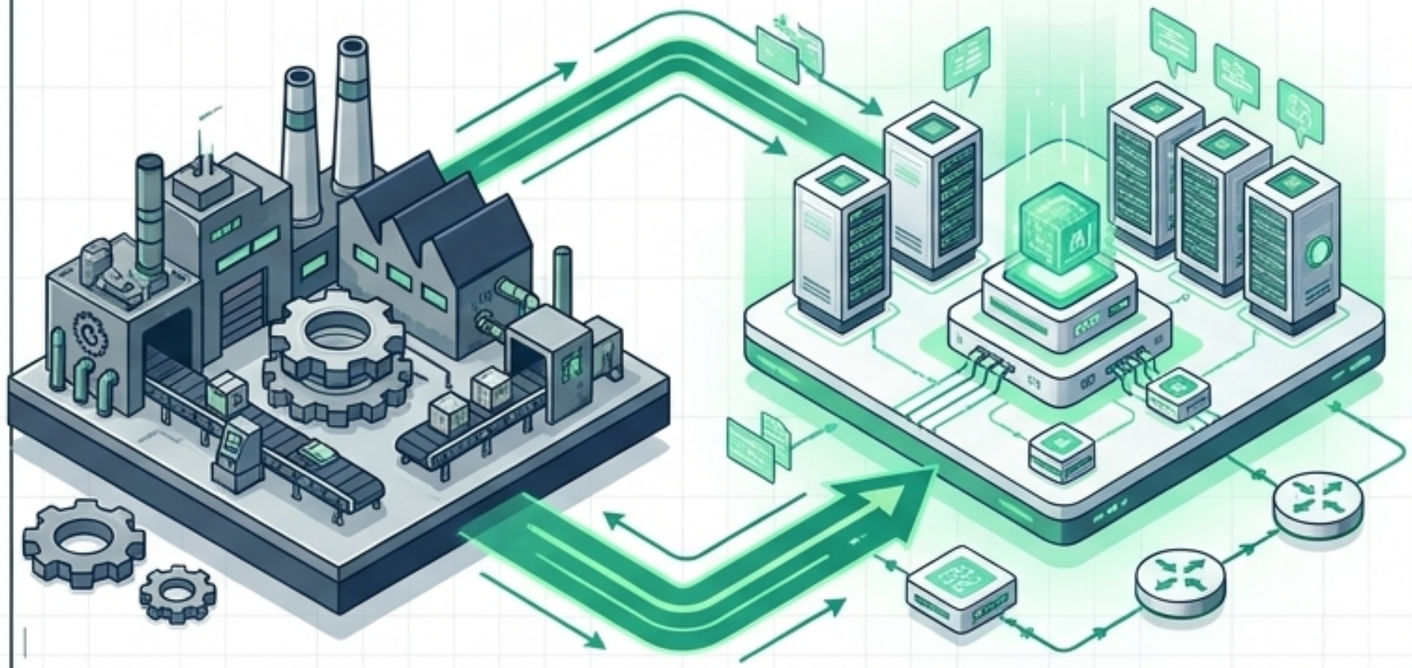
3. Hybrid AI Core（ハイブリッドAI）



タスクに応じ、GPT-4o（複雑な推論）とGemma（軽量高速なオープンウェイトモデル）を動的に使い分け、精度とコストを最適化。

Governance Note: 運営元の「情報セキュリティポリシー」（2025年10月策定）に基づく定期監査と全社統制を実施。

Genzo AI：島津製作所の本番運用から生まれた「実業発」の知財AI



産業基盤（島津製作所工場）

AI知財基盤（Genzo AI）

Origin Story Panel

2026年4月、株式会社島津製作所と株式会社IP Agentのジョイントベンチャーにより設立（名称は創業者・島津源蔵氏に由来）。

単なるSaaS開発ではなく、巨大グローバル製造業が自社の「知財担当者不足・属人化・外部委託費高騰」を解決するために内製・実運用してきたシステムを外販化。

Hard ROI Proof Panel

年間 8,000万円

島津製作所社内での本番運用（2025年度）において実証された外部委託コストの削減効果。PoCレベルではない、エンタープライズ環境での明確な投資対効果の証明。

Target: 2030年度までに320社導入、売上高15億円の事業目標を掲げる堅牢なインフラ。

Genzo AI アーキテクチャ：RAGマイニングと厳格な時限消去メカニズム

Phase 1: Ingestion
(非構造化データの直接投入)

仕様書、実験データ、会議議事録など、フォーマット化されていない開発現場の生データ（Trade Secrets）を直接システムへアップロード。

Phase 2: RAG Engine
(自律的発明抽出)

高度なRAG（検索拡張生成）システムがデータを解析し、研究者が意識していない潜在的な「特許性のあるアイデア」を能動的にマイニング。

Phase 3: Ephemeral Storage
(データライフサイクル管理・時限消去)

クラウド上のデータ残留リスク（Data Persistence Risk）を排除するため、元データ、中間ファイル、プロンプト履歴を「一定期間で自動的に完全削除」するよう詳細なチューニングが可能。自社の機密レベル（例：24時間以内の論理削除）に合わせた厳格なガバナンスを実現。

セキュリティ・ベースライン監査結果：全ツールにおけるコンプライアンス適合証明

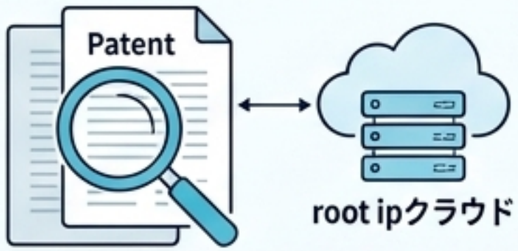
	Summaria	TOKKYO.AI	Genzo AI
Zero Data Retention	✓ 各LLM API規約による保証	✓ 専用環境内での遮断	✓ エンタープライズSLA準拠
Logical Isolation	✓ 独立したセッション管理	✓ 完全な専用プライベートテナント	✓ 企業別データ分離
PII Stripping	✓ 独自プロキシによる物理的除去	✓ ローカルUI制御	✓ セキュアな認証基盤
Ephemeral Storage	✓ セッション揮発	✓ 顧客管理の閉域保存	✓ 厳格な時限自動消去設定

IS Conclusion: 3システム全てにおいて、特許法上の新規性喪失リスクおよびデータ二次利用リスクはアーキテクチャレベルで排除されている。

アーキテクチャ特性と機能ケーパビリティの比較

Summaria

- **コア設計:** 弁理士視点の「読解支援特化」
- **得意領域:** 既存特許の解析、クレーム読解・要約
- **対象データ:** 既存の公開特許文献
- **連携性:** root ipクラウド等の外部知財システム連携

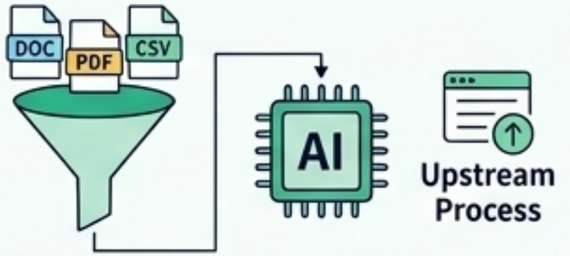


TOKKYO.AI

- **コア設計:** 総合型プラットフォームの構築
- **得意領域:** ドラフティング、AI類似検索、商標画像検索
- **対象データ:** アイデア概要、検索クエリ
- **連携性:** 単一UI内で完結するエコシステム

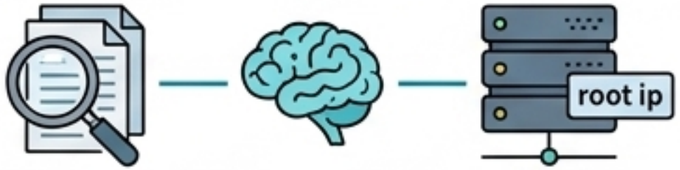
Genzo AI

- **コア設計:** 製造業実務発の発明マイニング・自動化
- **得意領域:** 開発資料からの自律発明抽出、翻訳、契約確認
- **対象データ:** 社内の未整理な開発資料（非構造化データ）
- **連携性:** 開発上流プロセスへの直接介入

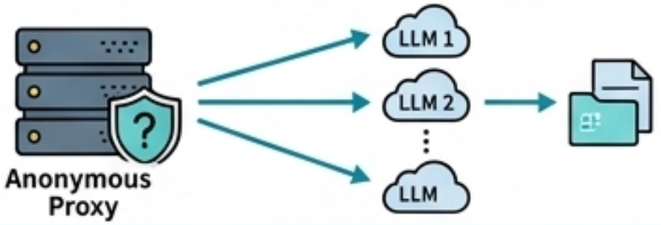


組織課題とアーキテクチャ適合性に基づくユースケース・マッピング

Condition: 既存の知財管理システム（root ip等）を活かしつつ、研究者・知財担当者の「読解効率」を最大化したい。

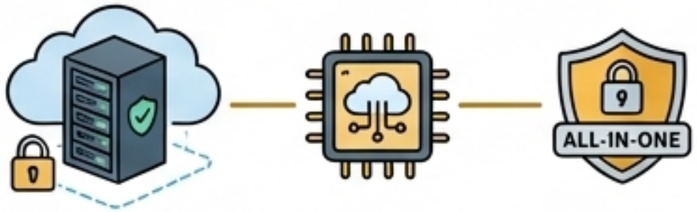


Recommendation: Summaria ヘルーティング。匿名化プロキシ経由で複数LLMの強みを適材適所で活用可能。



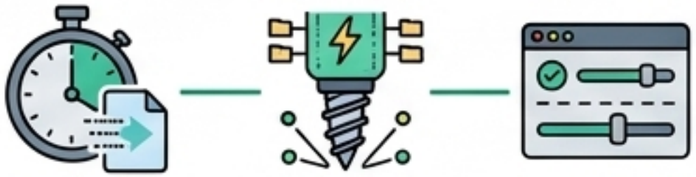
Condition: 全社的な知財業務を単一のUIに統合し、SaaSでありながら「オンプレミスに近い完全隔離環境」を構築したい。

Recommendation: TOKKYO.AI ヘルーティング。専用プライベートテナントとハイブリッドAIがセキュアなオールインワン環境を提供。



Condition: R&D部門の非構造化データ（生資料）を直接投入し、潜在的発明を「攻めの姿勢」で発掘したい。

Recommendation: Genzo AI ヘルーティング。情報残留リスクを「時限消去機能」でコントロールしつつ、強力なRAGマイニングを実行。



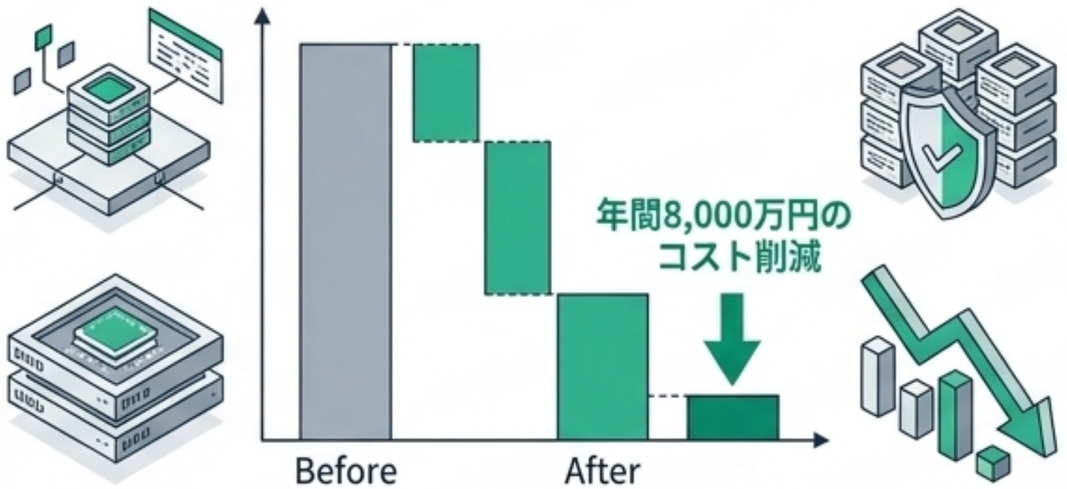
予算策定に向けたコスト・スケーラビリティと投資対効果（ROI）の証明

Model A : TOKKYO.AI（サブスクリプションの透明性）

- 初期費用0円。1ユーザーID月額35,000円。

Analysis: Xシステム（独自ビッグデータ基盤）の効率化による競争力のある価格設定。機能制限なし（生成AI回数制限等を除く）、全社展開時のボリュームディスカウントも可能でIT予算の予見性が高い。

Model B：Genzo AI（実績ベースのコスト削減）



- 年間8,000万円のコスト削減（島津製作所 2025年度実績）。

Analysis: 外部の特許事務所への依頼費用等、知財・R&D部門における初期連携コストと時間を劇的に削減。PoC不要レベルでの確実なROIが実証済み。

総括：情報漏洩リスクの完全なコントロールと、PoC（概念実証）への移行勧告

次世代知財AIは、学習オプトアウト、テナント隔離、PIIストリッピング、時限消去という最新のエンタープライズ・アーキテクチャによって、新規性喪失・データ流出のボトルネックを完全に克服している。これらは単なる効率化ツールではなく、企業の無形資産価値を最大化する戦略的インフラである。

1. Select

ユースケース・マッピングに基づき、自社の既存インフラに最適化されたツールを1〜2つ選定する。

2. Audit Validate

ISMS（ISO 27001）等の認証証明書およびプロバイダーAPI規約を社内セキュリティ基準へ最終照合する。

3. Execute PoC

特定のR&D部門または知財チームにおいて、実務データを（時限消去設定下で）用いたスモールスタートの概念実証を開始する。

リスクの回避から、リスクをコントロールした上での競争力強化へ。