次世代知財AIプラットフォーム
アーキテクチャ・セキュリティ評価報告

情報システム部門向け 導入要件およびシステム構造解説

情報システム部門のセキュリティ評価フレームワーク

1. データ学習の完全なオプトアウト

API経由のデータが、LLMプロバイダー（OpenAI, Azure等）の基盤モデル再学習に一切利用されないアーキテクチャ設計。

2. マルチテナント環境における論理的分離

クエリやアップロード文書が、他テナントのデータとデータベースレベルで完全に隔離（アイソレーション）された環境。

3. 匿名化処理（PIIストリッピング）

外部APIへのリクエスト時、ユーザー識別情報（メールアドレス等）がサーバー側で事前に除去されるプロキシ機構。

4. データの揮発性（Ephemeral Storage）

Summaria (サマリア)

マルチLLMアーキテクチャと匿名化プロキシによる読解特化型支援

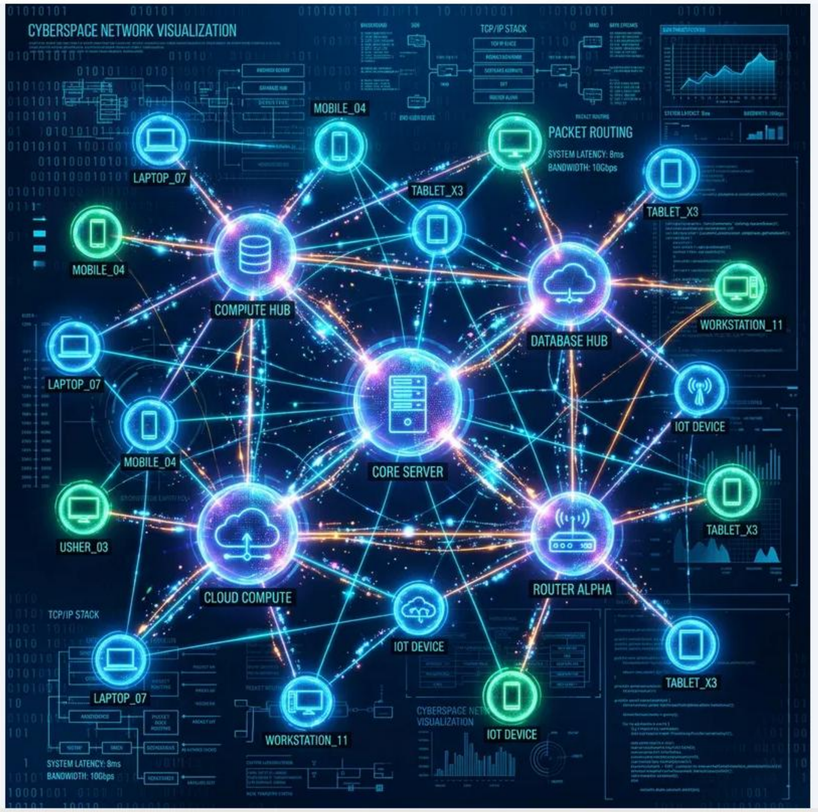
Summaria: システムアーキテクチャ

マルチLLMと匿名化プロキシ

Summariaは単一の基盤モデルに依存せず、Microsoft Azure、OpenAI、AWS、Anthropic等のAPIを動的に使い分ける**マルチLLMルーティング**を採用しています。

特筆すべきは、情報システム部門の懸念事項である「個人の特定」を防ぐ仕組みです。ユーザーからの指示や特許データは、Summariaのサーバーを経由する際、ユーザーIDなどの識別情報が完全に除去（ストリッピング）されます。

この**匿名化プロキシ**により、外部インフラからは「誰が実行したか」が完全に不可視化され、被害の局所化が可能となります。



Summaria: コンプライアンスと連携

新規性喪失リスクの排除

未出願の特許明細書を入力した場合の漏洩リスクに対処するため、接続先の全AIプロバイダーのAPI利用規約において、送信データが開発や再学習データセットとして利用されないことが明記されています。

システム内の通信も暗号化されており、法的に「公知」とならず発明の新規性を喪失することはありません。

ISMS認証と既存SaaS連携

運営元は2025年1月に情報セキュリティマネジメントシステム（ISMS）の国際規格「ISO 27001」を取得完了。第三者機関による厳格な監査をクリアしています。

また、「root ipクラウド」などの社内知財管理システムとAPI連携が可能であり、セキュアなエコシステム拡張に対応します。

TOKKYO.AI

ハイブリッドAIと独自ビッグデータ基盤による統合型プラットフォーム

独自基盤とハイブリッドAI

TOKKYO.AIの中核は、全世界の膨大な特許データを高速でベクトル処理する独自アルゴリズム**「Xシステム」**です。これにより検索レスポンスの低下を防ぎます。

また、GPT-4oやGoogleのオープンウェイトモデル「Gemma」などをタスクに応じて柔軟に使い分ける**ハイブリッド・アプローチ**を採用し、高精度な生成と計算コストの最適化を両立しています。

TOKKYO.AI: エンタープライズ向けセキュリティ

プライベート環境構築

パブリックSaaSとは異なり、導入企業ごとに論理的に分離された「専用テナント」が提供されます。クエリや文書が外部流出する構造的リスクを遮断します。

情報セキュリティ体制

運営元にて全社レベルの「情報セキュリティポリシー」を策定。管理責任者の設置、定期監査、外部委託先の審査など、厳格なSLA・内部統制要件を満たします。

高いスケーラビリティ

独自基盤により初期費用0円、1ID月額定額で主要機能が使い放題。全社展開時のボリュームディスカウントもあり、予測可能なコスト運用が可能です。

Genzo AI (ゲンゾウエーアイ)

大手製造業の実運用に基づく自律型RAGと厳格なデータ管理

Genzo AI: 開発資料からの自律的発明抽出

Genzo AIは、島津製作所が自社の知財課題解決のために実運用し、年間8,000万円の外部委託費削減を実証した「実業発」のエンタープライズシステムです。

最大の特長は、仕様書や実験データなど未整理の非構造化データを直接システムに読み込ませ、潜在的な発明を自律的に抽出する**高度なRAGアーキテクチャ**にあります。

これにより、現場の研究者が気付いていない特許の種をマイニングし、企業の知財パイプラインへ自動的に組み込むことが可能となります。

Genzo AI: 究極の情報漏洩対策

0

データ残留リスク

時限消去メカニズム (Ephemeral Storage)

未出願の開発資料を読み込ませる際のIS部門最大の懸念である情報漏洩に対し、Genzo AIは
「データライフサイクル管理」をコアに実装しています。

アップロードされた元データ、中間ファイル、プロンプト履歴などを、サーバー上から「一定期間で自動的に論理削除」するよう詳細なチューニングが可能です。

自社のデータガバナンス・ポリシーに適合させ、クラウドストレージにおける情報残留を物理的・論理的にゼロ化します。

アーキテクチャおよびセキュリティ要件比較

ツール名	コア技術・アーキテクチャ	データ保護・セキュリティ機構	実績・コンプライアンス認証
Summaria	マルチLLMルーティング (Azure, AWS, OpenAI, Anthropic等)	PIIストリッピング（匿名化プロキシ） API側学習の完全オプトアウト	ISO 27001取得済（2025年1月）
TOKKYO.AI	独自DB（Xシステム） + ハイブリッド生成AI	導入企業ごとの専用テナント提供 （論理的なデータベース隔離）	全社セキュリティポリシー策定済 定期監査の実施
Genzo AI	開発資料を解析する 高度な自律型RAGレイヤー	サーバー上データの時限消去設定 （揮発性ストレージ管理）	島津製作所にて本番運用実績 （年間8000万円コスト削減）

ご提案のまとめと次のステップ

各システムはいずれも、エンタープライズ水準の
高度なセキュリティアーキテクチャを実装しています。

特定部門でのスモールスタート（PoC）実施に向けて、
セキュリティ審査の承認をお願い申し上げます。

Image Sources

https://media.easy-peasy.ai/3fbf64bf-39db-4859-820c-3910a4ed939f/6edf30fe-b03e-4204-9ff1-8fb6618e5331_medium.webp

Source: easy-peasy.ai

https://media.istockphoto.com/id/2230807736/photo/futuristic-ai-data-center-interior.jpg?s=612x612&w=0&k=20&c=E2s9c_8IA4fBpNmX4gzn2qLnne4mXW1jhYOf9Essem8=

Source: www.istockphoto.com

https://cdmoworld.com/wp-content/uploads/2026/04/Untitled-design-33.png

Source: cdmoworld.com