知財業務の高度化に向けたAI支援ツールの導入について

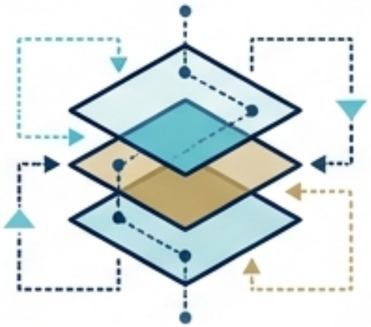
情報システム部門向け
セキュリティ・システム要件設計書

知的財産部門・研究開発部門

エグゼクティブ・サマリー

導入の目的

- 知財業務（特許調査・明細書作成）の**飛躍的効率化**
- コア業務へのリソース集中
- 年間数千万円規模のコスト削減



提案内容

- 知財プロセスに特化した3つのSaaS型AIツールの導入
  - TOKKYO.AI
  - Summaria
  - Genzo AI

セキュリティの確約

- AI学習への二次利用完全排除
- 国内データ保存の徹底
- 強固なアクセス制御（運営側アクセス不可）
- エンタープライズ要件を完全クリア

背景と課題解決のアプローチ

知財・R&D部門の要求

膨大な特許文献の迅速な処理と、類似特許の高精度な検出が必要（生成AIの活用が不可避）

情報システム部門の懸念

未公開の特許情報やR&D機密の漏洩、AIモデルへの学習利用（二次利用）リスクは絶対に許容できない

最新の実務特化型AIツールは、このトレードオフを技術的に解決している。

導入予定ツール・ポートフォリオ（相互補完の関係性）

Phase 1: 調査・検索

TOKKYO.AI

特許専用AIエージェントによる直感的な類似特許検索とビッグデータ処理（Xシステム搭載）。

Phase 2: 読解・分析

Summaria

弁理士開発。高度なプロンプトエンジニアリングによる難解な特許文書の要約・用語抽出。

Phase 3: 実務・統合管理

Genzo AI

島津製作所の知財ノウハウを実装。出願・翻訳・FTO等、AIと人が協働する次世代プラットフォーム。

Zero-Leakage Architecture

エンタープライズ知財AIの3大セキュリティ原則

Shield 1: Opt-Out（学習の完全遮断）

すべてのツールはAPI通信を利用しており、入力データがLLM（ChatGPT, Claude等）の学習に二次利用されることは規約および契約上、完全に禁止されている。

Shield 2: Domestic Storage（国内データ主権）

プロジェクトデータおよび処理結果は、国内のセキュアなAWS環境等に限定して保存され、国外へ流出しない。

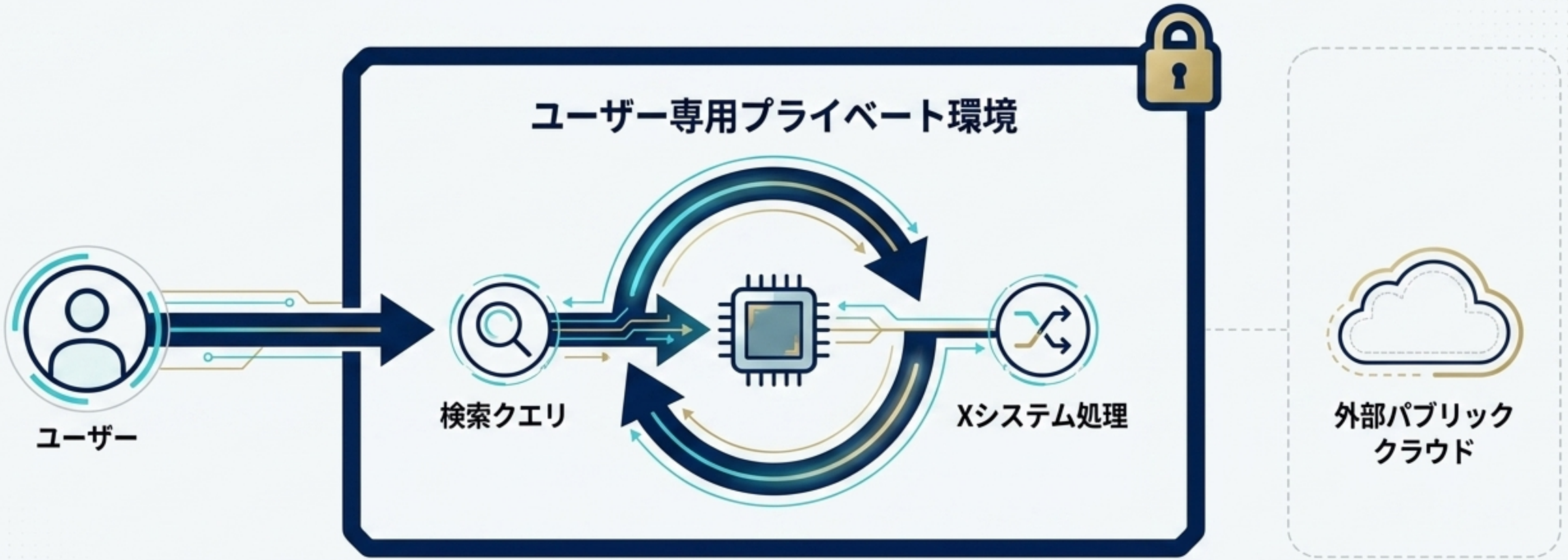
Shield 3: Zero-Access（運営者アクセスの排除）

専用環境の分離やAWSの厳格なIAM権限設計により、各ツールベンダーの運営担当者であっても顧客の機密データにはアクセスできない。

情報システム部門向け
ツール別セキュリティ評価マトリクス

評価項目	TOKKYO.AI	Summaria	Genzo AI
データ保存場所	ユーザー専用のプライベート環境	国内AWSサーバー	国内AWSサーバー
AI学習への利用	二次利用なし	利用規約により学習禁止	契約上禁止（学習・二次利用不可）
運営者のアクセス	専用環境により制限	運営側からの閲覧不可	AWS権限設計によりアクセス不可
データ削除	専用環境内で管理	ユーザー操作による削除可能	ユーザー主導で完全削除可能
検索クエリの扱い	社外流出しない設計	API送信時に匿名化	国内AWS保存、外部AIへは一時送信のみ

「プライベートAI特許」によるクローズド・アーキテクチャ

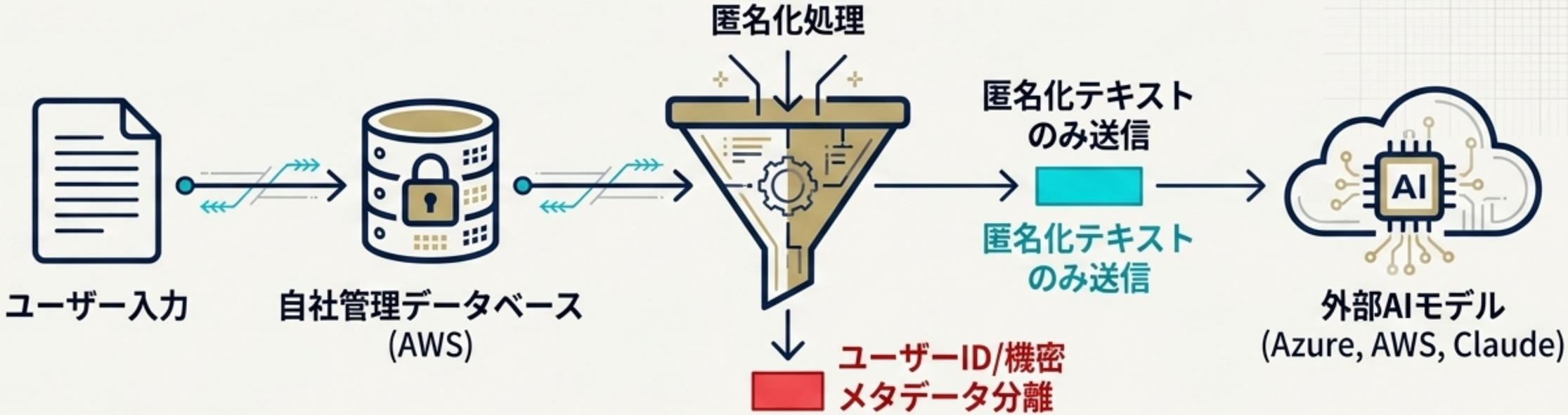


ユーザー専用の閉じた環境を構築。研究開発の方向性やアイデアを含む極めて機密性の高い検索クエリが環境外へ流出しない。

バックエンドを活用しつつも、入力データや検索履歴は専用環境内で保護・管理され、根本的な漏洩リスクを排除。

アーキテクチャ深掘り (2) Summaria

API通信時の厳格な匿名化パイプライン

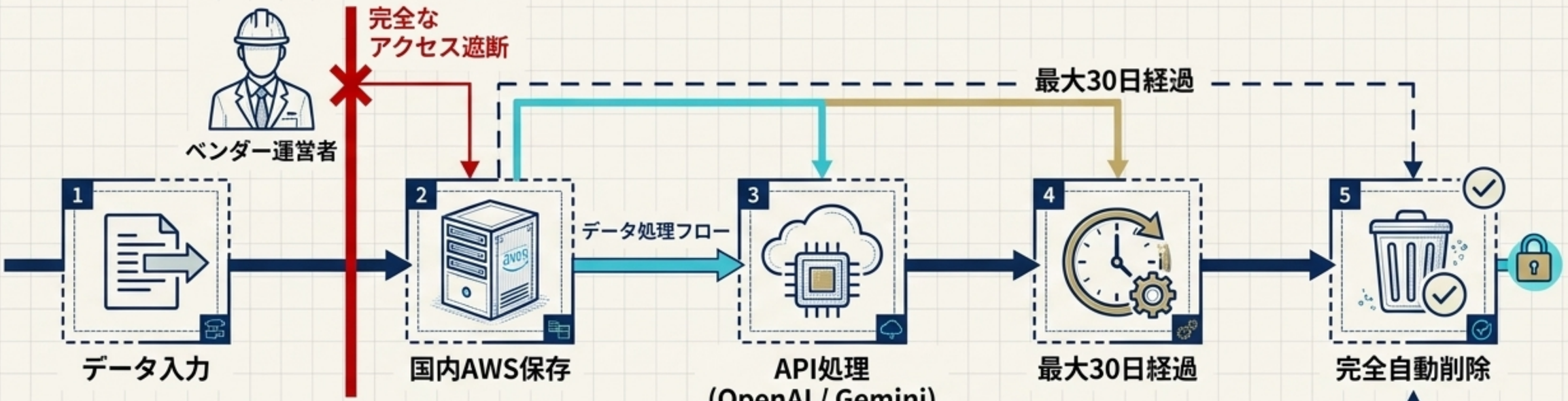


1. 入力データはAWS上の自社管理データベースに機密を保持して保存。

2. 外部AIへの送信時、ユーザー特定情報（ID等）をシステム側で完全に分離（マスキング）。

3. 匿名化されたデータのみが送信され、学習非利用規約の下で処理されるため、未出願明細書でも新規性喪失のリスクはゼロ。

島津製作所品質のデータライフサイクル管理



1 **完全なアクセス遮断:**

AWSの厳格な権限設計により、開発・運営元の担当者であっても顧客データへのアクセスは不可能。

2 **自動データパージ:**

不正利用防止のためのログ保持は最大30日間に制限され、その後システムによって自動的かつ不可逆的に削除される。

3 **学習利用の契約的禁止:**

APIプロバイダとの直接契約により、いかなる二次利用も排除。

導入メリットと投資対効果（Business Impact）

導入メリットと投資対効果（Business Impact）

コア業務へのリソース集中

従来手作業であった先行技術調査や明細書ドラフト作成時間を劇的に短縮。

調査精度の圧倒的向上

高度な自然言語処理により、キーワード検索での見落としリスクを文脈ベースの検出で低減。

年間8,000万円のコスト削減

外部委託費用や調査人件費の削減（Genzo AIベースシステムにおける島津製作所等での実績）。

情報システム部門へのご依頼事項（ネクストステップ）

Action Required

- [ ] **クラウドサービス利用許可の承認**
  各ツールが使用するドメインおよびAPIエンドポイントに対する、社内ネットワークからのアクセス制限の解除。
- [ ] **セキュリティ評価・ポリシー適合の確認**
  本資料で提示したアーキテクチャに基づく、当社情報セキュリティポリシーとの適合性評価の実施。
- [ ] **社内利用ガイドラインの策定支援**
  機密情報の取り扱い・入力に関する社内ルールの策定、およびユーザー向けセキュリティ教育への技術的知見からのご協力。