知財生成AI・SaaS導入における社内承認・アーキテクチャ評価報告書

TOKKYO.AI / Summaria / Genzo AI における コンプライアンス要件と導入ロードマップ

Target Audience: 経営層・情報システム部・法務部・知財部

エグゼクティブ・サマリー：導入推奨ステータス

01

[本命] ○

Summaria

- 最も社内承認に載せやすい有力候補。
- ISMS認証取得済、AWS保存の明示。
- 外部送信先が明示されており、稟議通過の透明性が極めて高い。

02

[条件付] ○

TOKKYO.AI

- 検索・ドラフトの一体運用に優れる。
- 利用規約上のAzure/OpenAI API送信条件のクリアが必須。
- リージョン未指定部分の契約交渉が前提となる。

03

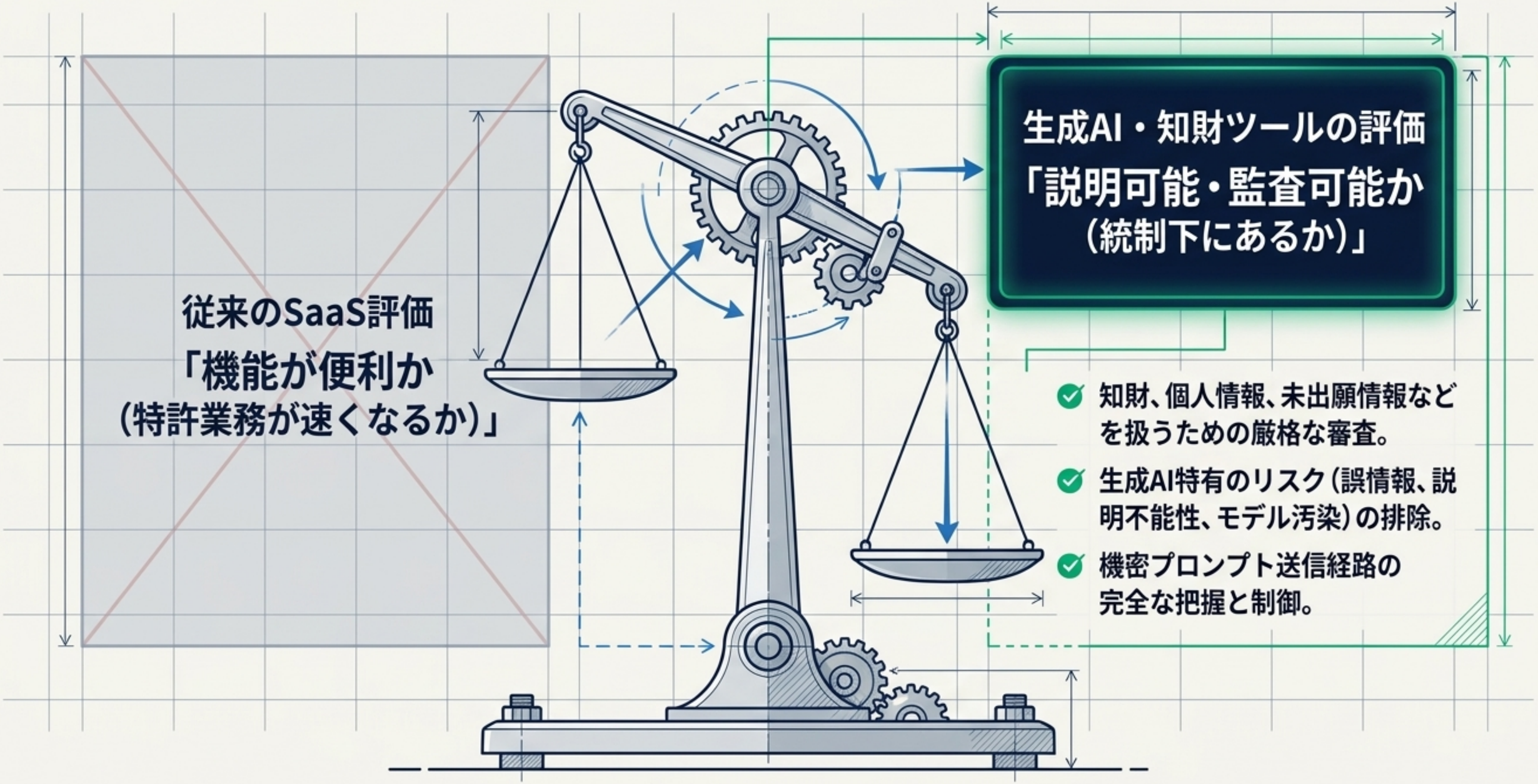
[PoC向け] ○

Genzo AI

- 国内完結・運営者アクセス不可の最強設計思想。
- 公開コンプライアンス資料が現時点では未成熟。
- 現段階では限定的なPoC検証が妥当。

「機能の良し悪し」ではなく「説明可能性と監査可能性」が導入の成否を決める。

知財AI導入における「真のハードル」

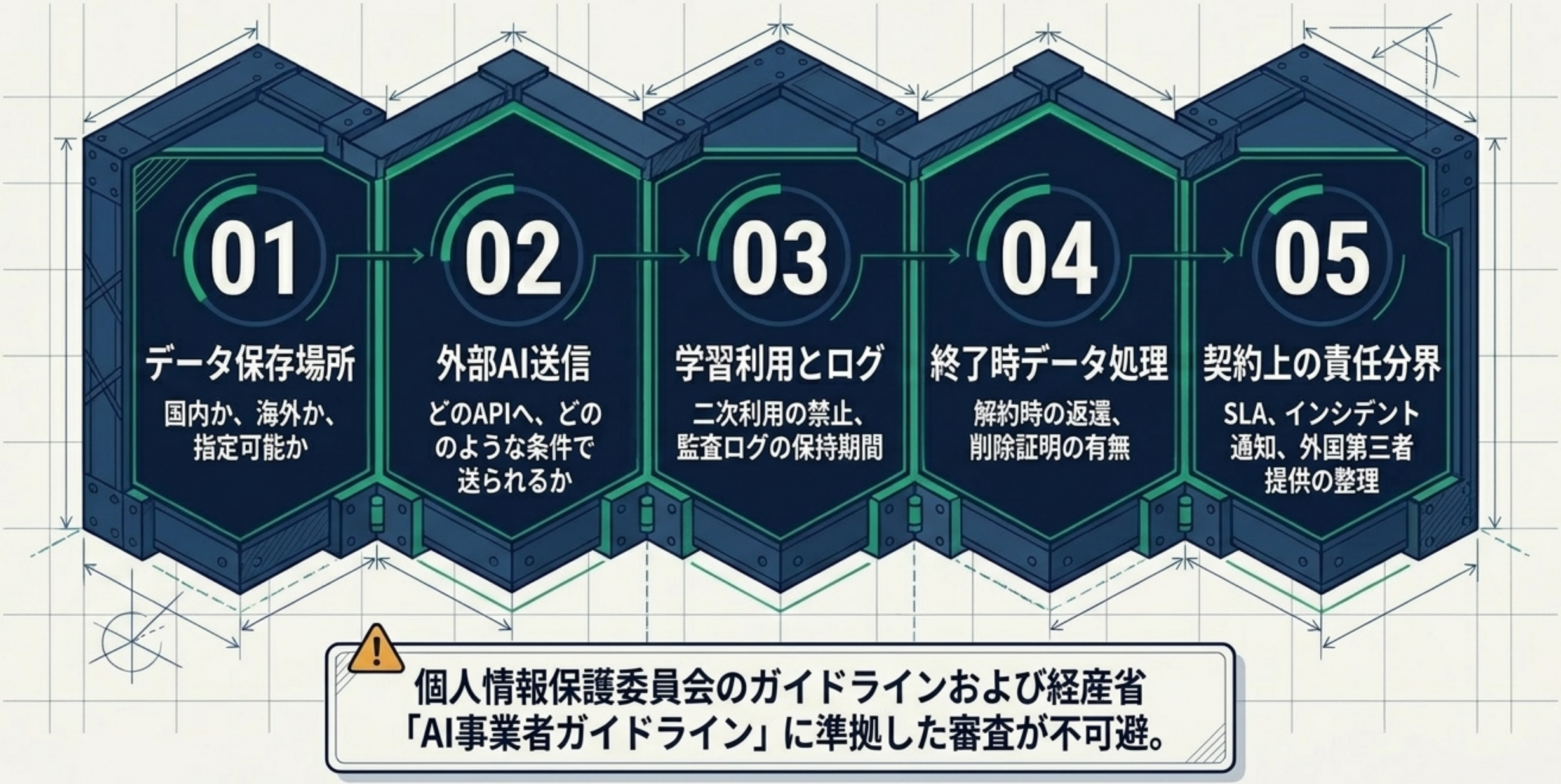


従来のSaaS評価
「機能が便利か
（特許業務が速くなるか）」

生成AI・知財ツールの評価
「説明可能・監査可能か
（統制下にあるか）」

- 知財、個人情報、未出願情報などを扱うための厳格な審査。
- 生成AI特有のリスク（誤情報、説明不能性、モデル汚染）の排除。
- 機密プロンプト送信経路の完全な把握と制御。

稟議通過のための「5つの承認基準」



⚠ 個人情報保護委員会のガイドラインおよび経産省「AI事業者ガイドライン」に準拠した審査が不可避。

【診断マトリクス】3製品の総合評価

製品名	主用途	データ取扱いの要点	セキュリティ認証	コスト要因	推奨度
TOKKYO.AI	検索・ドラフト	専用環境内保持・監査ログ有・API送信可	ポリシーのみ公開	1ID 2万円/月	条件付き
Summaria	読解・拒絶対応	AWS保存・ユーザ識別情報非送信	ISMS(ISO27001)取得済	プラン課金＋指示追加購入	最優先
Genzo AI	知財業務全般・FTO	国内AWS・運営者アクセス不可設計	公開資料不足	年額100万～1,500万円	PoC推奨

アーキテクチャ評価: TOKKYO.AI (1/2) - 評価と要点

Core Value

知財検索・生成AIの一体運用

(ChatTokkyo / 生成AI Plus)

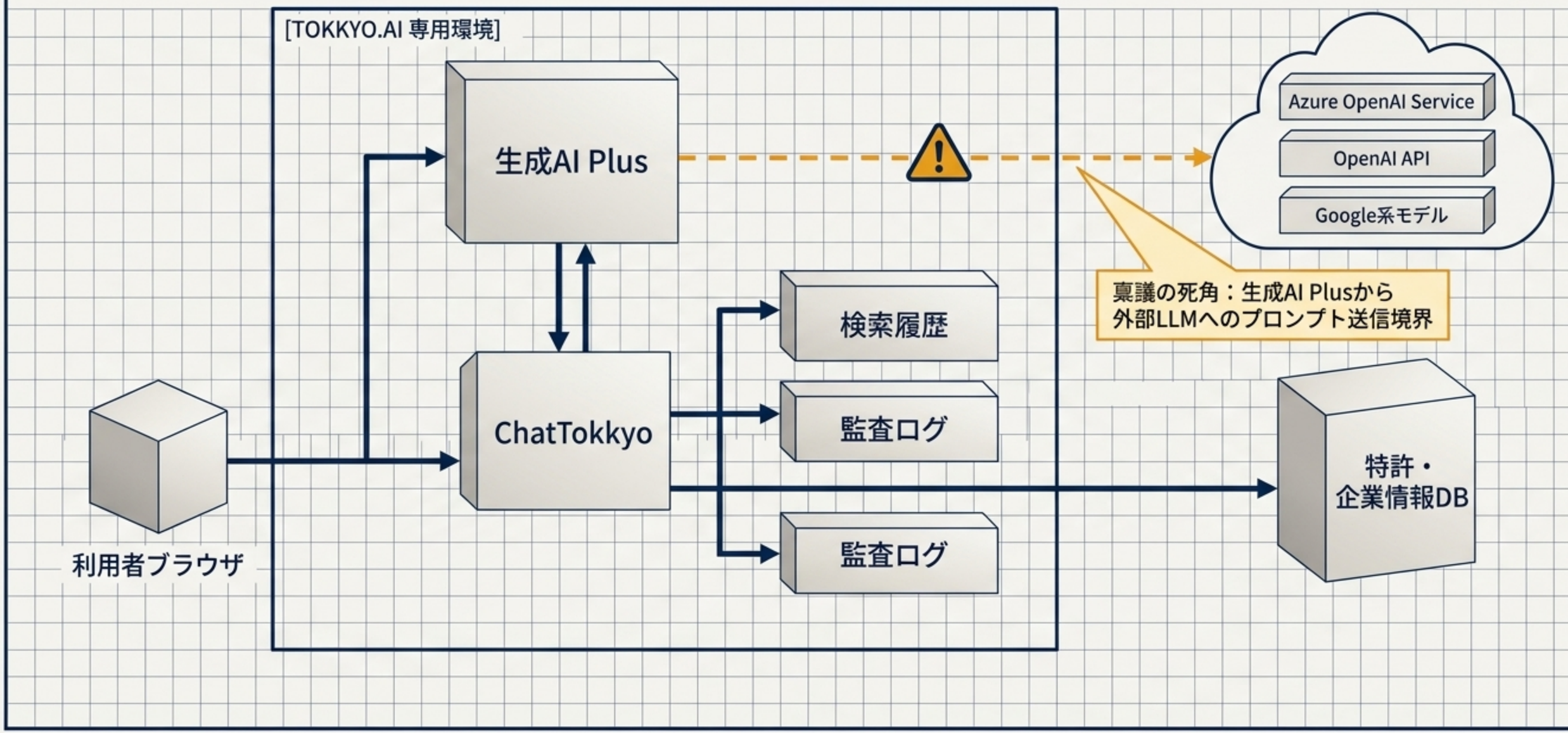
強み

- 専用環境での提供
- 検索履歴の専用環境内保持（社外持ち出し抑制）
- 明確な監査ログ

承認上の懸念点

- 利用規約にてプロンプト情報を「Azure OpenAI Service または OpenAI API等」へ提供できると定めている点。
- 保存リージョンや暗号化詳細が公開資料上「未指定」である点。

TOKKYO.AI (2/2) - データフロー・アーキテクチャ



アーキテクチャ評価: Summaria (1/2) - 評価と要点

Core Value

特許文書の読解支援・拒絶理由対応

(Claude 3.7 Sonnet等の最新モデル活用)

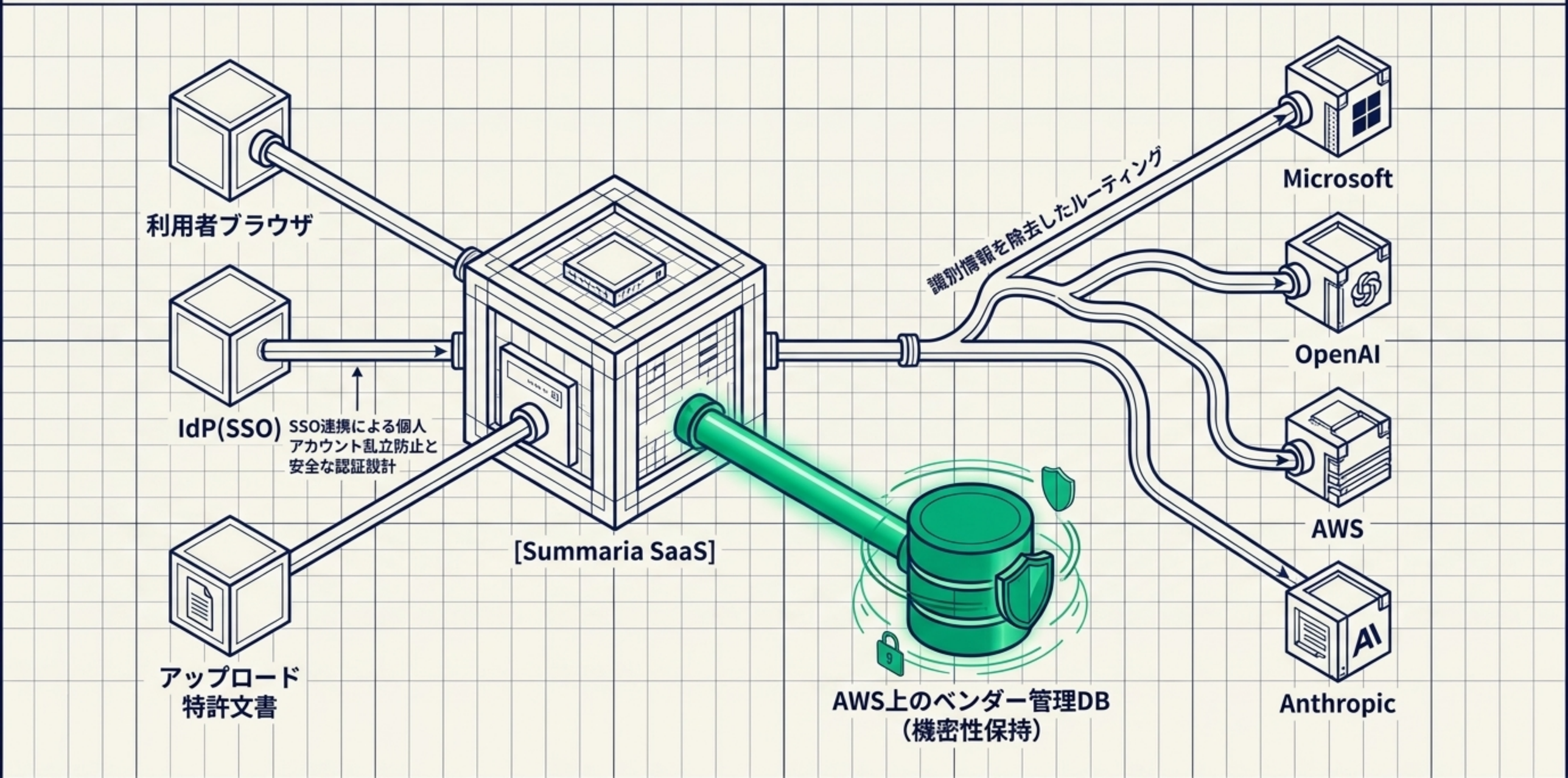
強み

- AWS保存とSSL通信の明記
- ISMS（ISO27001）取得済
- SSO（シングルサインオン）対応
- ユーザ識別情報の外部非送信

承認上の懸念点

- 外部送信先が複数（Microsoft / OpenAI / AWS / Anthropic）に及ぶため、基盤ベンダー側とSaaS側の責任分界およびログ保持期間の確認が必要。

Summaria (2/2) - データフロー・アーキテクチャ



アーキテクチャ評価: Genzo AI (1/2)　- 評価と要点

Core Value

知財業務全体の自動化

（発明提案からFTOまで）

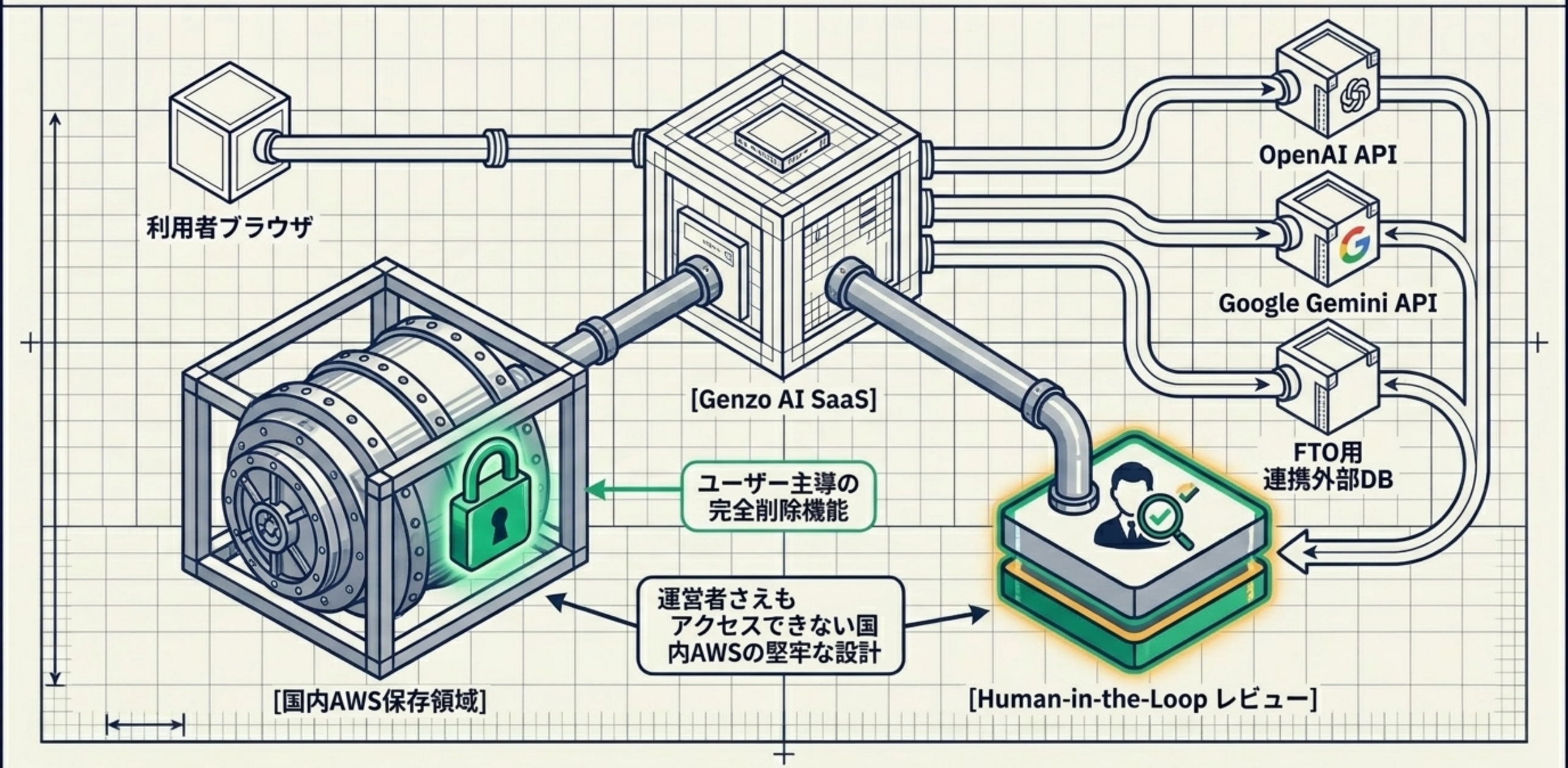
強み

- 国内AWS保存領域で完結
- 運営者アクセス不可設計
- ユーザー主導での完全削除（復元不能）

承認上の懸念点

- プライバシーポリシー、DPA、ISO/SOC、SLA等の公開資料が未成熟（2026年春インフラ増強段階）。

Genzo AI (2/2) - データフロー・アーキテクチャ



コンプライアンス上の死角と緩和策

Threat Box	Shield
外国移転・外部委託リスク	契約による利用プロバイダ・リージョンの固定、サブプロセッサ一覧の取得。
AI特有のハルシネーション（誤情報）	出力をそのまま提出物にしない「人間レビュー（Human-in-the-Loop）」の業務フロー必須化。
ベンダーロックイン・データ流出	エクスポートの定期実施、削除証明、終了時データ返還条項の明確化。

運用ガバナンスの前提条件（ルール設計）

権限統制

- [x] 管理者権限を厳密に限定し、共用IDでの利用を禁止する。

APPROVAL

データ区分ルール

- [x] 高機密・個人情報・共同研究先情報の投入基準（ホワイトリスト/ブラックリスト）を制定する。

APPROVAL

最終確認責任

- [x] AIの出力（論点抽出・叩き台）をそのまま外部提出せず、必ず人間の知財担当者・弁理士がレビューする。

APPROVAL

監査と棚卸し

- [x] 監査ログの保全期を設定し、定期的なエクスポートと棚卸しを定例化する。

APPROVAL

稟議添付用：必須取得ドキュメント・チェックリスト

TOKKYO.AI 向け要求

- ☐ DPA（データ処理契約）
- ☐ Azure/OpenAIのリージョン指定
- ☐ 監査ログの仕様
- ☐ 終了時データ返還条件

Summaria 向け要求

- ☐ 上流AIベンダーごとのログ保持期間表
- ☐ 削除条件
- ☐ SLA
- ☐ サブプロセッサー一覧

Genzo AI 向け要求

- ☐ MSA（基本契約書）
- ☐ プライバシーポリシー
- ☐ DPA
- ☐ セキュリティ認証証跡
- ☐ バックアップ/DR仕様

推奨ロードマップ（結論）

【Step 1】Immediate ●

本命による実務導入

公開証跡が揃う Summaria を最優先導入し、読解・拒絶対応の効率化と安全確保を即時実現する。

【Step 2】Parallel ●

条件付き並行評価

検索・ドラフトの一体化を狙い、TOKKYO.AI の契約条件（外部送信・データ所在）を詰めた上で並行評価する。

【Step 3】Future ○

将来像の限定PoC

業務全般の自動化を見据え、Genzo AI の認証資料が揃うのを待ち、低機密データによる限定PoC検証を行う。

この段階的アプローチが「現場の効率化」と「経営の要求する統制」のズレを最小化する最適解である。