TOKKYO.AI、Summaria、Genzo AI セキュリティ詳細比較表

Manus

本資料は、社内導入を検討中の知財系 AI ツール（TOKKYO.AI、Summaria、Genzo AI）について、情報システム部門への説明用にセキュリティ仕様を詳細に比較したものです。

1. セキュリティ仕様 詳細比較表

比較項目	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 [1]	国内 AWS サーバー [2]	国内 AWS サーバー [3]
AI モデルの学習利用	二次利用なし（専用環境外に出さない） [1]	利用規約で禁止（API 経由のため学習利用なし） [2]	契約上禁止（モデル改善等に一切使用されない） [3]
運営側のアクセス権限	監査ログ機能あり（いつ誰がアクセスしたか保存） [4]	運営側からも閲覧不可 [2]	運営担当者もアクセス不可（AWS 権限設計による） [3]
通信・データの暗号化	堅牢なセキュリティ技術（リーガルテック社基盤） [4]	SSL による暗号化通信 [5]	国内 AWS の標準的な暗号化に準拠 [3]
未公開情報の安全性	プライベート環境のため外部漏洩リスクなし [1]	未出願明細書をアップロードしても新規性喪失なし [2]	コンシューマーサービスから完全切り離し [3]
バックエンド AI	独自 AI＋ChatGPT API 等（詳細非公開）	Azure OpenAI, OpenAI, Bedrock, Claude API [2]	OpenAI API, Google Gemini API [3]

比較項目	TOKKYO.AI	Summaria	Genzo AI
データの削除	ユーザー専用環境内で管理 [1]	ユーザーによる削除可能	ユーザー主導で完全削除可能（復元不可） [3]
情報セキュリティ体制	情報セキュリティポリシー策定済み [6]	ISMS 認証取得 [7]	島津製作所子会社としての厳格な基準 [3]

2. 情報システム部門への説明ポイント（ツール別）

TOKKYO.AI

TOKKYO.AI は、リーガルテック株式会社が提供する「プライベート AI 特許」環境が最大の特徴です。
ユーザー専用の環境が提供されるため、検索履歴や入力データが専用環境外に出ることはなく、AI の二次利用も行われません [1]。また、いつ誰がアクセスしたかを記録する監査ログ機能が備わっており、社内のガバナンス要件を満たしやすい設計となっています [4]。

Summaria

Summaria は、パテント・インテグレーション株式会社が提供するツールで、国内 AWS サーバーを基盤としています [5]。
入力データは機密性を保った状態で保存され、他のユーザーや運営側からも閲覧できない仕組みになっています [2]。また、未出願の特許明細書をアップロードしても新規性を喪失しないことが明記されており、研究開発の初期段階から安全に利用可能です [2]。

Genzo AI

Genzo AI は、株式会社 Genzo AI（島津製作所子会社）が提供するツールで、こちらも国内 AWS サーバーでデータを管理しています [3]。
OpenAI や Google の API を利用していますが、契約上 AI モデルの学習や二次利用が明確に禁止されています [3]。また、AWS のアクセス権限設計により、運営担当者

であっても顧客データにアクセスできない「ゼロトラスト」に近い設計が採用されています [3]。

参考文献

[1] TOKKYO.AI よくある質問: "Q. このツールのデータのセキュリティはどうなっていますか？ A. ユーザー専用の環境で提供しており、検索履歴などのデータは専用環境外に出さず、また、二次利用もいたしません。" (https://www.tokkyo.ai/pvt/support/faq/)

[2] Summaria よくあるご質問(セキュリティ関連): "入力した情報は、AWS 上の弊社が管理するデータベースに機密性を保った状態で保存されます。他のユーザや弊社側も閲覧できません。" (https://patent-i.com/summaria/manual/faq)

[3] Genzo AI データ保護の取り組み: "お客様のデータはすべて、国内の AWS サーバー上で管理されます。運営担当者であっても、お客様のデータにアクセスできない設計を採用しています。" (https://www.genzo-ai.co.jp/security.html)

[4] TOKKYO.AI AI 検索機能: "リーガルテックで培ったセキュリティ技術で堅牢な知財データアクセスを実現。監査ログが残るため、いつ誰がアクセスしたかが明確に保存されます。" (https://www.tokkyo.ai/pvt/function/)

[5] Summaria 公式サイト: "SSL による暗号化通信。基盤インフラとして、AWS を利用。" (https://patent-i.com/summaria/)

[6] リーガルテック株式会社 情報セキュリティポリシー: "情報の適切な管理を重要な経営課題であると認識し、情報セキュリティの確保を目的として「情報セキュリティポリシー」を策定しました。" (https://www.legaltech.co.jp/information-security-policy/)

[7] 知財系生成 AI サービスの比較: "ISMS 認証取得、データ暗号化、GCP でのデータ保存" (https://yorozuipsc.com/uploads/1/3/2/5/132566344/e177e1a5a744e71be65f.pdf)