知財系 AI ツール導入に関する情報システム部門向け Q&A

Manus

本資料は、知財系 AI ツール（TOKKYO.AI、Summaria、Genzo AI）の社内導入にあたり、情報システム部門から想定されるセキュリティ関連の質問と、その回答（Q&A）をまとめたものです。

---

1. AI モデルの学習利用に関する懸念

Q1. 社内の機密情報（未公開の特許情報など）を入力した場合、外部の AI モデル（ChatGPT など）の学習データとして利用され、他社に漏洩するリスクはありませんか？

A1.3 ツールすべてにおいて、入力データが AI モデルの学習や改善に使用されることはありません。
各ツールは API 経由で AI モデルを利用しており、API 提供元（OpenAI、Google、Microsoft 等）の規約により学習利用が明示的に禁止されています。また、各ツールの利用規約や契約上でも「二次利用しない」「モデル改善等に一切使用しない」ことが保証されています [1] [2] [3]。

Q2. 未出願の特許明細書をアップロードしても、特許法上の「新規性」は喪失しませんか？

A2.新規性を喪失することはありません。
例えば Summaria では、公式 FAQ にて「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」ことが明記されています [2]。TOKKYO.AI はユーザー専用のプライベート環境で完結するため外部漏洩リスクがなく [1]、Genzo AI もコンシューマー向けサービスから完全に切り離されたセキュアな環境で処理されます [3]。

2. データの保存場所と管理体制

Q3. 入力したデータや検索履歴はどこに保存されますか？海外のサーバーに保存されることによる法的リスク（海外データ移転）はありませんか？

A3. 3 ツールすべてにおいて、データは**国内**で管理されます。

- **TOKKYO.AI**: リーガルテック社が管理するユーザー専用のプライベート環境内に保存されます [1]。
- **Summaria**: パテント・インテグレーション社が管理する国内 AWS サーバーに保存されます [2]。
- **Genzo AI**: AWS の国内リージョンサーバーに保存されます [3]。
  いずれも海外サーバーへのデータ移転リスクは極めて低く設計されています。

Q4. サービス提供者（運営会社の担当者）が、当社の入力データや検索履歴を閲覧することは可能ですか？

A4. 運営側からの閲覧は技術的または運用的に制限されています。

- **Summaria / Genzo AI**: AWS の権限設計等により、運営担当者であっても顧客データにアクセスできない「技術的な遮断」が行われています [2] [3]。
- **TOKKYO.AI**: 監査ログ機能が備わっており、「いつ・誰が・何にアクセスしたか」が完全に記録されるため、不正アクセスの抑止と事後追跡が可能なガバナンス設計となっています [4]。

3. システム要件と運用管理

Q5. 導入にあたり、社内ネットワークやインフラの改修、専用サーバーの構築は必要ですか？

A5.不要です。
3 ツールともクラウドベースの SaaS（Software as a Service）として提供されるため、社内サーバーの構築や大規模なシステム改修は必要ありません。社内ネットワークから各サービスの URL へのアクセス（HTTPS 通信）を許可するだけで利用開始が可能です。

Q6. 退会時や不要になったデータの削除は完全に実施されますか？

A6.はい、可能です。
各ツールともユーザー主導でのデータ削除機能を提供しており、特に Genzo AI では「ユーザー主導で完全削除可能（復元不可）」であることが明記されています [3]。TOKKYO.AI も専用環境内でのデータ管理となるため、確実な破棄が可能です [1]。

Q7. 各ツールの運営会社は、情報セキュリティに関する第三者認証や明確なポリシーを持っていますか？

A7. はい、各社とも厳格なセキュリティ体制を構築しています。

- **TOKKYO.AI (リーガルテック社)**: 情報セキュリティポリシーを策定・公開し、定期監査を実施しています [5]。
- **Summaria (パテント・インテグレーション社)**: ISMS（情報セキュリティマネジメントシステム）認証を取得しています [6]。
- **Genzo AI (株式会社 Genzo AI)**: 島津製作所の子会社として、同グループの厳格なセキュリティ基準に準拠しています [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] 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/)
[6] 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)