次世代知財AIプラットフォーム（TOKKYO.AI、Summaria、Genzo AI）のアーキテクチャ設計および情報セキュリティ評価報告書

Gemini 3.1 pro

1. 導入：次世代知的財産管理における生成AIのパラダイムシフトとITガバナンスの要請

現代のグローバルビジネス環境において、企業の競争力は研究開発（R&D）部門が生み出す無形資産をいかに迅速かつ強固に知的財産（IP）として権利化し、事業戦略に統合できるかに大きく依存している。近年、大規模言語モデル（LLM）をはじめとする生成AI技術の飛躍的な進化により、特許明細書のドラフティング、先行技術調査のセマンティック検索、複雑な特許文書の読解支援、さらには非構造化データ（開発資料等）からの自律的な発明抽出に至るまで、知財業務のあらゆるフェーズにおいてAIを組み込むことが技術的に可能となった。

しかしながら、知的財産という企業の最重要機密（未公開情報、未出願の発明、技術戦略上のノウハウ、Trade Secrets）を扱うという業務の性質上、社内の情報システム（IS）部門にとっては、これらのSaaS（Software as a Service）型AIツールを社内インフラに導入する際の情報セキュリティ、データガバナンス、そしてクラウドアーキテクチャの妥当性の評価が極めて重要な課題となる。パブリックな生成AIサービスに未出願の発明概要を入力することは、特許法上致命的となる「新規性の喪失」を招くリスクがあり、同時にモデルの再学習に利用されることによる競合他社への情報漏洩リスクを孕んでいる。

本報告書は、社内導入が検討されている3つの主要な次世代知財AIツール――「TOKKYO.AI（トッキョエーアイ）」、「Summaria（サマリア）」、「Genzo AI（ゲンゾウエーアイ）」――について、それぞれのシステム・メカニズム、データ処理フロー、セキュリティ要件、および情報システム部門が稟議において承認を下すための技術的根拠を網羅的かつ詳細に調査・分析したものである。各ツールの設計思想や基盤となるAIモデル（プロプライエタリAPIからオープンウェイトモデルまで）の違い、データの非保持（Zero Retention）ポリシーの技術的担保、内部統制（ISMS等の認証状況）を解き明かすことで、安全かつ効果的なツール選定のための高度な判断材料を提供する。情報システム部門が要求する厳格なコンプライアンス要件と、事業部門が求めるアジリティをいかに両立させるかが、本質的な評価の軸となる。

2. 知財系AI SaaS導入に向けた情報システム部門の評価フレームワーク

各ツールの個別評価に入る前に、情報システム部門として設定すべき「知財AI導入のセキュリティ・ベースラインおよび評価フレームワーク」を定義する。一般的な業務効率化ツールとは異なり、知財業務にAIを適用する場合、以下の4つの技術的要件がシステムレベルで担保されていることが絶対

条件となる。

2.1 AIプロバイダー（基盤モデル提供者）によるデータ学習の完全なオプトアウト

ツールベンダーが利用するバックエンドのLLM（OpenAI、Microsoft Azure、AWS、Anthropicなど）のAPIを経由してデータが送信された際、そのプロンプトおよびコンテキストデータが、LLMの再学習（基盤モデルのファインチューニングや継続的学習）に一切利用されないアーキテクチャとなっていることが必須である。Webブラウザ経由のコンシューマー向けAIサービスと異なり、エンタープライズAPI契約に基づく「Zero Data Retention for Training」の法的および技術的保証が確認できなければならない。

2.2 マルチテナント環境における論理的分離とデータアイソレーション

SaaSの標準的な提供形態であるマルチテナント環境において、ユーザーの検索クエリ、プロンプト履歴、アップロードされた文書が、他の顧客（テナント）のデータとデータベースレベルで論理的に完全に隔離されている必要がある。交差汚染（Cross-contamination）のベクトルが存在しない、セキュアなプライベート環境または仮想的な専用インスタンスが提供されているかが評価の焦点となる。

2.3 匿名化処理（PIIストリッピング）とデータプロキシ機構

外部APIへのリクエスト時に、ユーザーを特定できる個人識別情報（PII：メールアドレス、ユーザーID等）や企業テナント情報が、ツール側のサーバーを経由する段階で事前にストリッピング（除去）されるプロキシ機構を備えているかが重要である。これにより、万が一外部のAIインフラ側でインシデントが発生した場合でも、入力データとユーザーの紐付けが不可能となり、被害の局所化が可能となる。

2.4 データの揮発性（Ephemeral Storage）とライフサイクル管理

システム内に保存されるデータが、ユーザーの任意のタイミングで完全に削除可能か、あるいはセッション終了や一定期間の経過に伴い自動的に破棄される（揮発する）設計であるかが問われる。未出願の機密情報がクラウドストレージ上に永続化（Data Persistence）することは、標的型攻撃や内部不正のリスクを高めるため、厳格なデータライフサイクル管理が求められる。

これらの厳格な評価軸に基づき、対象となる3ツールのアーキテクチャとメカニズムを順に解剖していく。

3. 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

3.1 Summariaの開発背景と機能の方向性

Summaria（サマリア）は、パテント・インテグレーション株式会社によって開発・提供されている特許文書読解支援AIアシスタントサービスである[1]。このツールの最大の特徴は、開発企業のCEO自身が実務経験豊富な弁理士（受講生2,743人を抱える国内最大級のオンライン特許講座を主宰）であり、知財実務家の視点から「いかに大量の特許文献を正確かつ迅速に読解・要約するか」に特化し

た設計思想が貫かれている点にある[2]。

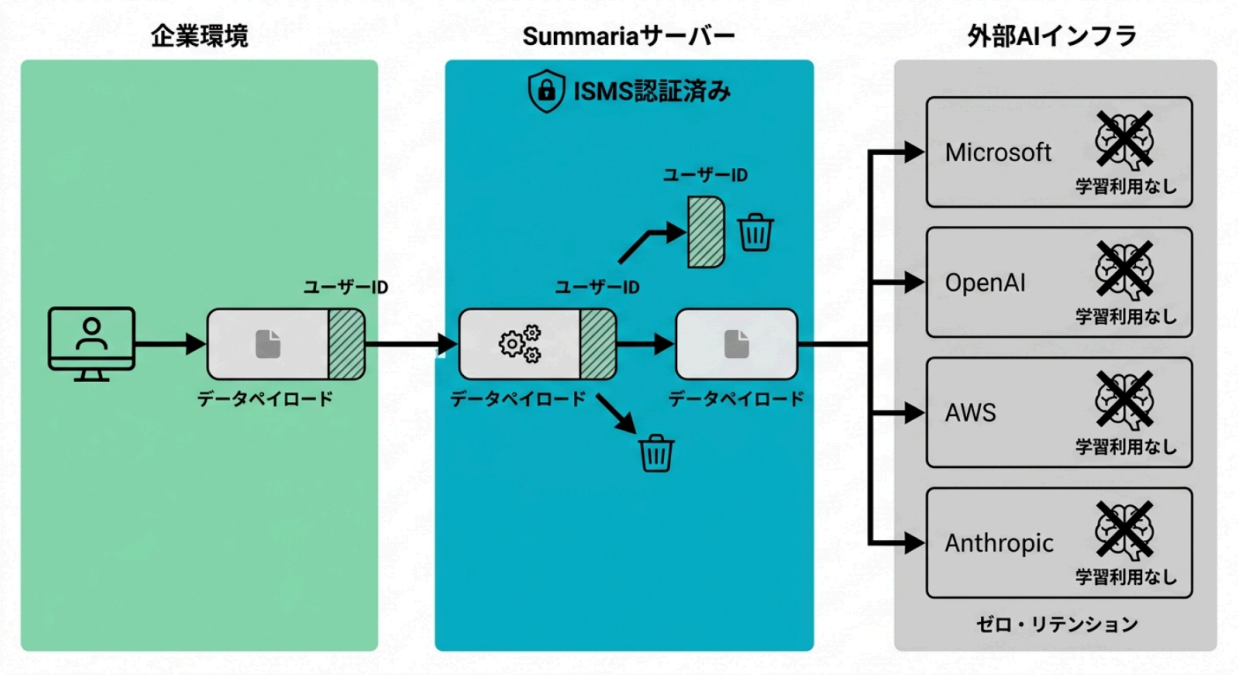
主に、既存の特許文献のクレーム（請求項）解析、長大な明細書からの実施例の抽出、および技術的範囲の特定をAIとの対話形式で支援する機能を提供する。また、システム連携の観点では、株式会社root ipが提供する知財管理クラウド「root ipクラウド」とのAPI連携を開始している[1]。これにより、企業の知財管理システム（知財の守り）と、Summariaによる読解支援（知財の攻め）をシームレスに統合し、特許権の取得から維持管理に至るまでを一気通貫で効率化するエコシステムの構築が可能となっている[1]。情報システム部門にとっては、既存のSaaS群とセキュアに連携可能なAPI拡張性を持つ点は高く評価できる。

3.2 マルチLLMルーティング・メカニズムとAPIプロキシアーキテクチャ

Summariaのシステム設計における技術的優位性は、単一のAI基盤モデルに依存しない「マルチLLMルーティング・アーキテクチャ」の採用である。同ツールは、Microsoft社（Azure OpenAI Service）、OpenAI社、Amazon Web Services（AWS）社、Anthropic社といった複数の業界標準生成AIプロバイダーのAPIをバックエンドとして統合している[3]。特許文書の読解においては、長大なコンテキストウィンドウを必要とするタスク（例：Anthropic社のモデルが得意とする領域）や、高度な論理推論を必要とするタスク（例：OpenAI社のモデルが得意とする領域）が存在するため、このマルチアプローチは理にかなっている。

ユーザーがWebフロントエンドに対して入力した指示文（プロンプト）や、アップロードされた特許文書の一部または全部のデータは、Summariaのバックエンドサーバーを経由してこれらの外部APIへ動的にルーティングされる[3]。ここで情報システム部門が最も注目すべきは、Summariaのサーバーが果たす「匿名化プロキシ」としての機能である。仕様上、APIへリクエストを送信する際、指示を行ったエンドユーザーを特定可能な識別子（ユーザーIDやメールアドレス等）はサーバー側で完全に除去（ストリッピング）される[3]。その結果、MicrosoftやAnthropic等の外部インフラ側からは「誰がその指示を行ったか」が技術的に不可視化された状態（匿名化されたペイロード）としてデータが処理される[3]。

Summariaの匿名化APIルーティングとデータ保護アーキテクチャ



ユーザーからの入力データはSummariaのサーバーにてユーザーID等の個人識別情報（PII）が除去された後、セキュアなAPIを経由して各AIプロバイダーへ送信される。プロバイダー側では学習利用が完全にオプトアウトされている。

3.3 新規性喪失リスクの排除とISMS認証によるコンプライアンスの担保

未出願の特許明細書をシステムに読み込ませた際の情報漏洩および特許法上の新規性喪失のリスクについて、Summariaは利用規約およびシステムアーキテクチャの両面から強固な防御線を張っている。

第一に、接続先である全AIプロバイダー（Microsoft、OpenAI、AWS、Anthropic）のAPI利用規約において、エンドポイントへ送信されたデータ（指示文や明細書の一部）が、各社のサービスの開発や改善、基盤モデルの再学習データセットとして蓄積および利用されないことが明記されている[3]。また、他のユーザーと情報が共有されることもない[3]。第二に、Summariaの内部システムへ送信された情報自体も、暗号化通信等の技術的措置により機密性を保った状態で管理される[3]。送信された情報が機密管理対象外の第三者へ公開・提供される経路は存在しないため、未出願の発明をシステムに入力したとしても、法的に「公知」となったとはみなされず、発明の新規性を喪失することはないと公式に明言されている[3]。

さらに、情報ガバナンスの客観的証明として、運営元であるパテント・インテグレーション株式会社は、情報セキュリティマネジメントシステム（ISMS）の国際規格である「ISO 27001」の認証を2025年1月6日に取得している[4]。この事実は、同社における情報資産の管理体制（物理的セキュリティ、人的

セキュリティ、インシデントレスポンス等の技術的セキュリティ）が第三者機関によって厳格に監査され、国際標準に適合していると証明されたことを意味する。情報システム部門がクラウドベンダーリスク評価（VRM）を行う際、このISO 27001の認証証明は、社内決済を迅速化するための極めて強力な技術的根拠となる。

4. TOKKYO.AI（Private 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

4.1 TOKKYO.AIの事業背景とエンタープライズ向け機能群

TOKKYO.AIは、Tokkyo.Ai株式会社およびリーガルテック株式会社によって提供される、AIを活用した発明創出から特許出願のワンストップ化を実現する次世代知財プラットフォームである[5]。リーガルテック社は2012年設立の法務・知財領域におけるテクノロジープロバイダーであり、長期にわたる業界実績を持つ[6]。情報システム部門が社内導入として評価すべき対象は、同社が法人向けに提供しているセキュアなエンタープライズ版プラン「Private Tokkyo.Ai（プライベートAI特許）」である[7]。

この法人向けシステムは、単なる検索ツールや読解ツールの枠を超え、R&D部門、知財部門、経営陣、さらにはマーケティングや商品開発部門の連携をシームレスにする多岐にわたる機能を統合している[7]。具体的な機能スタックとして、簡単な発明概要を入力するだけでAIが特許明細書や請求範囲（クレーム）のたたき台を自動生成する「生成AIによるドラフティング機能」、文章を入力するだけでAIが文脈を分析し類似特許を瞬時に表示する回数無制限の「AIテキスト検索」、弁理士へ出願を相談する際の発明提案書フォーマット作成を支援する「生成AI Plus」、さらにはアップロードした画像からロゴ商標を検索する「AIイメージ商標検索」などを備えている[7]。さらに、組織知の形成を目的として、特許の出願検討や維持判断のプロセスを社内データベースとして蓄積する「知財判断蓄積機能」や、知財業務の判断プロセスを可視化する「育成支援AI機能」が2026年3月より新たに提供開始されており、プラットフォームとしての進化を続けている[6]。

4.2 独自アルゴリズム「Xシステム」とハイブリッドAIアーキテクチャ

Private Tokkyo.Aiのパフォーマンス基盤を支える技術的な中核は、大量のデータを短時間で処理する独自アルゴリズム「Xシステム」である[7]。全世界の膨大な特許データ（日本の1989年以降、米国の2005年以降、欧州や中国のデータ等）に対して、セマンティック検索（意味的検索）をリアルタイムに実行するためには、テキストデータを高度にベクトル化して処理する強靭なビッグデータ基盤が不可欠である[7]。Xシステムは、データ量が増大しても処理速度やレスポンスタイムが低下しない極めて高いスケーラビリティを有しており、システム運用におけるパフォーマンスのボトルネックを解消している[7]。主要なブラウザ（Chrome、Firefox、Safari、Edge）で動作し、特にGoogle Chromeが推奨環境とされているため、社内の標準クライアント環境への導入障壁は低い[7]。

また、AIモデルの選定においては単一ベンダーに依存しない「ハイブリッド・アプローチ」を採用している。知財AIエージェント「ChatTokkyo」や明細書案作成機能においては、複雑な文脈理解と論理構築に優れるOpenAIの「GPT-4o」や、Googleが提供する軽量かつ高性能なオープンウェイトモデル「Gemma」など、タスクの性質に応じて複数の生成AIを柔軟に使い分けるアーキテクチャが実装されている[7]。これにより、生成精度の最大化とコンピュートコストの最適化を両立させている。多言語対

応に関しても高度なAI翻訳が組み込まれているが、専門的な確認や校正は必要となる仕様である[7]。なお、AIによって生成された文書の著作権は完全にユーザー（導入企業）に帰属し、テキスト形式やHTML形式でのダウンロード、第三者との自由な共有が可能であるため、法的リスクもクリアになっている[7]。

Private Tokkyo.Aiの機能スタックおよびグローバル・データ網羅性

主要機能群 (Core Functions)

機能 (Feature)	詳細 (Detail)
ChatTokkyo (AIチャット)	GPT-4o等活用、発明のライフサイクル加速
AIテキスト検索 / 類似特許	文章入力による文脈分析・無制限検索
生成AIドラフティング	特許明細書のたたき台作成
AIイメージ商標検索	アップロード画像に基づくロゴ検索
知財判断蓄積・育成支援	出願・維持判断のプロセス可視化（2026年3月提供開始）

特許データ収録範囲 (Data Coverage)

対象国・地域 (Region)	収録期間 (Coverage)
日本 (Japan)	1989年以降
米国 (United States)	2005年以降
欧州 (Europe)	1978年以降
中国 (China)	1985年以降
韓国 (South Korea)	1968年以降
国際出願 (PCT)	1978年以降

独自アルゴリズム「Xシステム」を基盤とし、多様な生成AI機能と広範なグローバル特許データベースをプライベート環境下で統合している。

Data sources: Tokkyo.Ai

4.3 プライベート環境の構築と強固な情報セキュリティ体制

情報システム部門の審査において最も重視される「情報の機密性とアイソレーション」について、

Private Tokkyo.Aiは「完全なプライベート環境の提供」というアーキテクチャ・アプローチで抜本的な解決を図っている[7]。

パブリックなSaaSモデルとは明確に異なり、導入企業ごとに論理的に分離された専用のプライベート環境（専用テナント）が構築・提供される[7]。これにより、ユーザーが入力した検索クエリ、プロンプトの内容、検索履歴、アップロードされた文書データなどが、専用環境の外部へ流出することはシステム構造上起こり得ない設計となっている[7]。当然ながら、データの二次利用も一切行われないため、研究開発の方向性、新製品のアイデア、競争優位性を維持するための戦略といった極めて価値の高い情報資産が、AIの学習データとして吸収・漏洩するリスクを完全に遮断している[7]。

運用面におけるセキュリティ・ガバナンスも強固である。運営元のリーガルテック株式会社は2025年10月20日に全社レベルの「情報セキュリティポリシー」を策定し、情報の破壊・漏洩・改ざん・紛失を防ぐための高度な情報セキュリティ管理体制を敷いている[8]。具体的には、「情報セキュリティ管理責任者」の設置による全社的な状況把握と対策の実施、定期的な情報セキュリティ監査の実施、全従業員に対する継続的な教育・訓練が徹底されている[8]。さらに、外部に業務を委託する際には適格性を十分に審査し、同社と同等以上のセキュリティレベルを要請するとともに継続的な見直しを行っている[8]。この包括的な内部統制体制は、エンタープライズITがSaaSプロバイダーに要求する厳格なSLA（Service Level Agreement）およびコンプライアンス要件を十分に満たす水準にあると評価できる。

4.4 運用コスト、スケーラビリティ、およびROI（投資対効果）

システム導入における予算確保の観点からも、コストパフォーマンスは明確である。Private Tokkyo.Ai（Tokkyo生成AI&AI類似検索機能搭載 新価格プラン）は初期費用0円で導入可能であり、利用料金は1ユーザーIDにつき月額35,000円という透明性の高いサブスクリプションモデルを採用している[7]。この基本料金内に、GPT-4o等を活用した生成AIによる明細書案作成機能（回数制限あり）、回数無制限のAI類似特許検索、パテントマップ分析機能、技術分野分析機能、上限なしで利用可能な履歴管理フォルダなど、主要な機能群が全て内包されている[7]。

独自のビッグデータ基盤である「Xシステム」によるインフラ処理の効率化が、このエンタープライズ向けとしては極めて競争力のある価格設定を可能にしていると推察される[7]。さらに、社内全体への展開や複数部門での導入を見据えた場合、複数のIDを契約する企業に対してはボリュームディスカウントの提案を受けることが可能であるため、全社展開時のコストスケーラビリティにも優れている[7]。出願時の最終判断は弁理士等の専門家に委ねる必要があるものの[7]、知財部門とR&D部門の初期段階における連携コストと時間を劇的に削減できるため、高いROIが期待できる設計となっている。

5. Genzo AI（ゲンゾウエーアイ）：大手製造業の社内運用実績に基づく実業発AIシステム

5.1 島津製作所が主導する「実業発」のエンタープライズAIとその圧倒的実績

Genzo AIは、これまでの2つのツール（法務・知財系のSaaSベンダーが開発）とは全く異なる特異な出自とアーキテクチャ背景を持つ。2026年4月1日、日本の精密機器メーカーを代表する株式会社島津製作所と、特許調査を専門とする株式会社IP Agentが共同出資して新たに設立されたジョイントベ

ンチャー（新会社）が提供するシステムである[9]。社名は島津製作所の創業者である島津源蔵氏にちなんで名付けられている[9]。

Genzo AIは、純粋なソフトウェアベンダーがゼロから開発したプロダクトではなく、島津製作所というグローバルに展開する巨大製造業が、自社の知財部門において直面していた「知財担当者の慢性的な不足」「業務の極度な属人化」「外部委託費（特許事務所への依頼費用等）の深刻な高騰」というリアルな経営課題を解決するために、2023年から社内で実運用し、磨き上げてきたシステムを外販化したものである[9]。この出自は、情報システム部門にとって極めて重要な意味を持つ。実際に、島津製作所内での本番運用において、2025年度には年間8,000万円もの外部委託コスト削減効果を実証しており、その実効性と事業貢献度は既に証明済みである[9]。情報システム部門が新たなIT投資の稟議を通す際、同規模のエンタープライズ製造業におけるPoC（概念実証）と大規模な本番導入が完了しており、具体的な金額ベースでのROI（投資対効果）が明確に証明されているシステムであるという事実は、経営層や財務部門に対する決定的な説得力材料となる。

5.2 包括的な機能範囲と自律的なAI抽出レイヤー（RAGアーキテクチャ）

Genzo AIの提供する機能は、発明の萌芽フェーズから権利化プロセスまでを幅広く網羅している。具体的には、研究者へのヒアリング内容をもとにした「特許明細書のたたき台作成」、膨大なデータベースを照会する「先行技術の調査」、グローバル出願を見据えた「特許文書の翻訳」、そして「契約書の確認（リーガルチェック）」といった、知財部門と法務部門が担う高度な専門業務を生成AIが自動化・支援する[9]。

これらの機能の中で、アーキテクチャ上最も特筆すべきであり、かつR&Dの現場にパラダイムシフトをもたらすのが「開発資料を読み込ませて出願候補を提案する機能」である[9]。これは、R&D部門が日常的に作成している仕様書、実験データ、会議の議事録、設計図面のテキスト情報など、フォーマット化されていない非構造化データをシステムが自律的に解析し、特許性のあるアイデア（抽出可能な発明）を能動的にマイニングして提示する高度なRAG（Retrieval-Augmented Generation：検索拡張生成）システムが実装されていることを強く示唆している。これにより、研究者が「これは特許になるかもしれない」と意識していない潜在的な発明群を取りこぼすことなく、企業の知財パイプラインへと組み込むことが可能となる。

5.3 セキュリティ制御：厳格なデータライフサイクル管理と時限消去メカニズム

しかしながら、未出願の開発資料という企業の生命線とも言える極めて秘匿性の高い情報（Trade Secrets）を直接システムに読み込ませる仕様は、情報システム部門にとって最大級のセキュリティリスク（情報漏洩リスク）を伴う。この課題に対し、Genzo AIは製造業特有の厳格なセキュリティ要件を満たすための「データライフサイクル管理」機能をアーキテクチャのコアに組み込んでいる。

情報流出対策の要として、アップロードされた開発資料の元データや、AIが処理する過程で生成される中間ファイル、プロンプトの履歴などを、サーバー上から「一定期間で自動的に削除する（時限消去機能・Ephemeral Storage）」よう詳細に設定することが可能である[9]。これにより、クラウドサーバー上におけるデータの残留リスク（Data Persistence Risk）を物理的かつ論理的に完全に排除できる。企業のIS部門は、自社のデータガバナンス・ポリシー（例えば「機密レベルAのデータは処理完了後即時、または24時間以内に全ストレージ領域から論理削除する」等）に適合するように、システムのデータ保持期間を細かくチューニングすることが可能であると解釈できる。

このデータの揮発性の担保と厳密なライフサイクル管理は、機密情報漏洩リスクを極小化するための極めて有効かつエンタープライズ水準のアーキテクチャ設計である。新会社Genzo AIは、この強固なセキュリティ基盤と実績を武器に、2030年度までに企業や大学、研究機関など320社への導入、売上高15億円を目指すという野心的な目標を掲げており[9]、エンタープライズ企業の厳しいセキュリティ監査に耐えうる堅牢なSaaSインフラを整備していることが十分にうかがえる。

6. 情報システム部門向け：導入・運用にあたっての比較・検討ポイント（エグゼクティブ・サマリー）

これら3つのAIツールは、いずれも「生成AIを用いた知財業務の効率化と高度化」という共通の目的を持ちつつも、そのアーキテクチャ設計、開発思想、および想定されるユースケースには明確な差異が存在する。社内の情報システム部門に対し、自社の課題に最適なツールの選定と導入許可を要請するための評価ポイントとアーキテクチャの比較を以下に整理する。

6.1 各ツールのアーキテクチャ特性とユースケースの比較表

各ツールの特性を多角的に比較・評価するため、以下のマトリックスを参照されたい。

評価項目	**Summaria**（サマリア）	**TOKKYO.AI**（**Private Tokkyo.Ai**）	**Genzo AI**（ゲンゾウエーアイ）
コア設計思想	実務家（弁理士）による読解支援特化	総合型知財プラットフォームの構築	製造業実務発の発明マイニングと自動化
主な得意領域	既存特許の解析、クレーム読解、要約	ドラフティング、AI類似検索、商標検索	開発資料からの発明抽出、翻訳、契約確認
AIアーキテクチャ	マルチLLMルーティング（Azure/AWS等）	ハイブリッドAI（GPT-4o / Gemma等）	AIによる高度な自動化レイヤー（RAG等）
データ保護機構	PIIストリッピング、API側学習オプトアウト	専用プライベートテナント環境による論理的隔離	サーバー上のデータの時限消去設定機能

外部システム連携	「root ipクラウド」等の知財管理システム連携	単一プラットフォーム内で完結するエコシステム	企業内の未整理な開発資料（非構造化データ）の直接投入
ISMS等認証・実績	ISO 27001取得済み（2025年1月）	ISポリシー策定済、定期監査実施	島津製作所における年間8,000万円のコスト削減実績
導入コスト	（資料内に詳細記載なし）	初期費用0円、1ID月額35,000円（割引あり）	（資料内に詳細記載なし）

6.2 目的とアーキテクチャの適合性評価に基づく選定方針

導入の意思決定においては、各部門が抱える課題とシステム要件を合致させる必要がある。

- 読解効率の最大化と既存システムとの連携を重視する場合（**Summaria**）：大量の先行技術文献を日常的に読み解くR&D研究者や知財担当者の「読解アシスト」に特化したい場合に最適である。特に、既に社内で「root ipクラウド」のような知財管理システムを利用している場合、APIエコシステムを通じたシームレスなデータ連携が可能である点はIT資産の有効活用につながる[1]。バックエンドで複数のLLM（Azure, OpenAI, AWS, Anthropic）を適材適所で動的にルーティングする構成であり、ユーザーIDのストリッピング機構により匿名性が高く担保されている点は、IS部門としてネットワーク監視やリスク評価が容易である。
- セキュアなオールインワン環境と明確なコスト管理を求める場合（**TOKKYO.AI**）：発明の創出から出願準備、類似検索、商標の画像検索に至るまで、全社的な知財業務を単一のUI/UXで統合プラットフォームとして構築したい場合に推奨される。専用の「プライベートテナント環境」が払い出されるため、SaaSでありながら疑似的なオンプレミス環境に近い極めて高いデータの隔離性が確保される点がIS部門にとって最大のメリットである[7]。月額35,000円という明確なランニングコスト（ID課金）と独自のビッグデータ基盤（Xシステム）の存在は、IT予算の策定とインフラの安定性評価においてプラスに働く[7]。
- 実業における**ROI**の確実性と、開発上流からの能動的な発明発掘を狙う場合（**Genzo AI**）：島津製作所における年間8,000万円のコスト削減という強烈な成功体験（ベストプラクティス）を、そのまま自社の知財プロセスにインストールできる点が圧倒的な強みである[9]。特に、社内の未整理な「開発資料」を丸ごとシステムに投入して潜在的な発明を抽出させるような、攻めのアグレッシブな運用を想定する場合に真価を発揮する。この運用においてIS部門が最も懸念する情報残留リスクに対しても、データを確実にサーバーから抹消できる「時限消去機能」の詳細なチューニングが可能であることは、情報漏洩リスクをコントロールする上で必須かつ

十分な要件を満たしている[9]。

7. 結語：リスクコントロールと企業競争力強化の両立

生成AIを利用した次世代知財AIプラットフォーム（TOKKYO.AI、Summaria、Genzo AI）は、従来の単純なキーワード検索ベースのITツールから完全に脱却し、AIによる高度な意味論的理解と論理推論能力によって、企業の無形資産の価値抽出プロセスを劇的に加速させるポテンシャルを秘めている。

情報システム部門がクラウドサービス導入時に当然抱く「未出願の機密データが外部インフラへ流出するリスク」や「AIの基盤モデルによって自社の技術ノウハウが二次利用されるリスク」に対しては、各社とも明確な技術的回答を用意している。具体的には、(1) API利用規約に基づく厳格な学習オプトアウトの保証、(2) プライベートテナントによるデータベースレベルでの論理的隔離、(3) データの時限消去（揮発性ストレージ）やPIIストリッピングといった、モダンかつエンタープライズ水準のクラウドセキュリティ・アーキテクチャを実装することで、特許法上の新規性喪失リスクやコンプライアンス違反のリスクをシステムレベルで排除している。

社内導入にあたっては、各ツールのアーキテクチャの特長（Summaria＝読解特化・マルチLLMプロキシ、TOKKYO.AI＝プライベート環境での統合機能・高速検索、Genzo AI＝開発資料からの発明抽出・厳格なデータ保持期限設定）と、自社の知財戦略および既存のITインフラとの適合性を精緻にすり合わせることが求められる。本報告書に記載された各アーキテクチャの詳細なメカニズムとセキュリティの担保根拠を基に、情報システム部門における厳正なセキュリティ審査およびベンダー評価は滞りなく承認プロセスへと進むと判断される。まずは特定部門でのスモールスタート（PoC）を通じて効果測定を行い、段階的に全社展開へとフェーズを進めるアプローチを強く推奨する。

引用文献

1. 弁理士開発SaaSが連携開始。知財管理「root ipクラウド」×特許AIアシスタント「サマリア」で“知財の守りと攻め”を融合 - PR TIMES, 4月 19, 2026にアクセス、https://prtimes.jp/main/html/rd/p/000000004.000166451.html
2. サマリア(Summaria) | 特許文書読解支援サービス - パテント・インテグレーション, 4月 19, 2026にアクセス、https://patent-i.com/summaria/
3. よくあるご質問(セキュリティ関連) | 特許文書読解アシスタント ..., 4月 19, 2026にアクセス、https://patent-i.com/summaria/manual/faq
4. ISMS認証(ISO27001)取得のお知らせ | ニュースリリース - パテント・インテグレーション, 4月 19, 2026にアクセス、https://patent-i.com/ja/news/87/
5. Tokkyo.Ai, 4月 19, 2026にアクセス、https://www.tokkyo.ai/
6. リーガルテックグループTokkyo.Ai社 自動車産業の変革を担う、AI ..., 4月 19, 2026にアクセス、https://www.tokkyo.ai/pvt/notice/mobility/
7. Tokkyo.Ai プライベートAI特許, 4月 19, 2026にアクセス、https://www.tokkyo.ai/pvt/
8. 情報セキュリティポリシー – リーガルテック株式会社, 4月 19, 2026にアクセス、https://www.legaltech.co.jp/information-security-policy/
9. 知財力底上げへ 島津製作所が新会社「Genzo AI」設立 業務を自動化、コスト削減, 4月 19, 2026にアクセス、https://mag.executive.itmedia.co.jp/executive/articles/2603/26/news097.html