

「AIの勝負はモデルでは終わらない」 深掘り調査レポート：Gensparkが示す「次のAIサービス」の競争軸

エグゼクティブサマリー

2026年8月30日にYahoo!ニュースで配信された「AIの勝負はモデルでは終わらない、Genspark創業者が描く『次のAIサービス』の条件」は、Forbes JAPAN編集部・安井克至氏による同日10時30分公開の記事である。本レポートでは、Yahoo!ニュース配信ページに対応するForbes JAPAN公式原文を一次的な記事本文として照合した。記事の中心命題は、**基盤モデルの性能向上そのものより、「モデルをユーザーの仕事の完了へ変換するシステム層」がAIサービスの主要な競争領域になる**というものだ。記事が挙げる条件は、モデル選択の抽象化、継続的な文脈・記憶、ツール実行、現実世界からの情報取得、そして非専門家でも使えるUXに集約できる。 ①

Yahoo!ニュース配信URL：

<https://news.yahoo.co.jp/articles/bfde0325786588fe3ba4f650d0505ec046cad97c>

Forbes JAPAN原文：

<https://forbesjapan.com/articles/detail/103707>

公開：2026年8月30日 10:30、著者：安井克至 | Forbes JAPAN編集部。 ②

本調査の結論は、記事の方向性にはかなり強い根拠がある一方、「**モデルが重要でなくなる**」と解釈すると誤りだ、というものである。2026年の実務的な競争単位は「モデル」対「アプリ」ではなく、**モデル × コンテキスト × データ × ツール × 実行環境 × 評価 × セキュリティ × UX × 流通**の積である。Genspark自身も2026年8月、企業エージェントでは一つの長い処理に多数の推論・ツール呼び出し・サブエージェントが含まれ、それぞれがコスト、遅延、失敗確率を増やすため、「最良のモデル」ではなく**成功タスク当たりコスト**やモデル・ルーティングを重視すべきだと論じている。 ③

Gensparkはこの考えを製品構造にも反映している。2026年7月公開の「AI Workspace 6.0」は、**SecondBrain=記憶、Super Agent=知能、Build/Office/Content Suites=実行ツール、GenTeam=人間・エージェント協業**という四層構造を明示する。これは、LLMを最終製品ではなく「部品」として扱う典型的なシステム設計である。 ④

事業面でもGensparkは急速に拡大した。Reutersによれば、2026年6月のSeries B延長ラウンドで1億ドルを調達し、評価額は**26億ドル**、Series B総額は**4.85億ドル**となった。会社発表ベースでBusiness顧客は6カ月で6,000社超、2025年4月以降のARR 1億ドルに加えて2026年第1四半期に1.5億ドルを積み増したとしている。共同創業者Wen SangはLinkedInで総調達額6.45億ドル、6,400社超、ARR 2.5億ドル超と述べている。ただしARR・顧客数は監査済み財務情報ではなく、**企業側の自己申告値として扱うべき**である。 ⑤

一方、最大のリスクは「記憶+行動能力」が高まるほど、データ漏えい、権限逸脱、プロンプトインジェクション、誤った自動実行、録音同意、法的責任、推論費用も同時に拡大することだ。AgentDojoは、外部ツールから返るデータに埋め込まれた命令によってエージェントが乗っ取られ得ることを実証しており、OWASPもPrompt Injectionを主要LLMリスク、さらに2026年にはAgentic Skills特有のリスクを整理している。 ⑥

したがって次世代AIサービスで長期的な堀になりやすいのは「モデルを何個載せているか」ではなく、**企業固有コンテキストの品質、評価・改善ループ、権限付きツール実行基盤、失敗回復、監査可能性、利用習慣への埋め込み、顧客データから学習する運用組織**である。これはGensparkの論点を支持する一方、Microsoft、Google、OpenAI、Anthropic、Gleanなどもまさに同じレイヤーへ進出しており、Gensparkの優位が自動的に持続するわけではない。 ⁷

評価項目	本調査の判断
「モデル以外が重要になる」	強く支持 。モデル性能差より、実際のタスク成功率・統合・UX・コストが事業価値を左右する領域が拡大。 ⁸
「モデル自体は差別化でなくなる」	言い過ぎ 。長期タスクではモデル・ハーネスの選択で性能差がなお大きい。 ⁹
永続メモリは重要か	非常に重要。ただし諸刃の剣 。価値とプライバシー・権限・鮮度問題が比例して増える。 ¹⁰
マルチモデル戦略	合理的 。性能・価格・障害・供給者依存を分散できる。ただしルーティング評価自体がコア技術になる。 ³
Gensparkの最大の機会	「AIを使う」から「AIに仕事を終わらせてもらう」への市場転換。
Gensparkの最大の脅威	Microsoft/Google/OpenAI等が同じ「文脈+実行+エージェント」層をOS・Office・Workspaceレベルから囲い込むこと。 ¹¹

記事の主要主張と重要引用

記事の論理は、おおむね六段階で構成されている。第一に、ChatGPT、Gemini、Claudeなど基盤モデルは急速に賢くなった一方、**人間の仕事の流れそのものは同じ速度では変化していない**。第二に、企業利用者が本当に買いたいのは「最強モデル」ではなく「仕事がどこまで終わるか」である。第三に、モデルを使い分ける負担そのものをサービス側で吸収すべきだとする。第四に、そのためにはメール、会議、チャット、資料、過去プロジェクトをまたぐ持続的な文脈が必要になる。第五に、画面内のテキストだけでなく会議や対面会話など物理世界もコンテキスト化する。第六に、それらをAI専門家以外にも使えるUXへ落とし込むことが次の競争になる、という構成である。 ¹

記事の主張	正確な要約	分析
モデル性能だけでは不十分	モデルの文章・調査・コード・画像能力が上がっても、実務フローが自動的に変わるわけではない。 ²	「能力」と「業務成果」の間に、データ接続、ワークフロー、権限、検証、UIという巨大な中間層がある。
成果中心のAI	企業はモデルのベンチマークより、資料作成、メール処理、会議後タスクなどが実際に完了することを重視する。 ¹²	SaaSの価値指標が「席数・質問数」から「完了タスク・時間削減・成果」へ移る可能性を示す。
モデルを抽象化	Gensparkは複数モデルを内部で使い分け、利用者がモデル選択を意識しない方向を志向する。 ¹³	クラウド時代のCPU・DB抽象化に近い。「モデル・ルータ」が差別化レイヤーになる。
永続コンテキスト	SecondBrainでメール、会議、チャット、文書、アプリ、プロジェクト履歴を横断する。 ¹⁴	「毎回ゼロから説明するAI」から「過去を踏まえるAI」への転換。ただし機密情報の集中点にもなる。

記事の主張	正確な要約	分析
物理世界へ拡張	録音機器SecondBrain Note等を使い、対面会議などをAIの作業コンテキストにする。 15	AIサービスが「アプリ」から人間の仕事環境を観測するambient computingへ接近する。
人間中心UX	ユーザーがモデル名やツール構成を学ばず、目的を自然言語で示せばよい世界を目指す。 16	普及障壁をプロンプト技術から「意図確認・例外処理・信頼設計」へ移す。

重要引用。 著作権上、原文の引用は必要最小限の短い抜粋に限定する。

「彼らが作っているのはエンジンだ。」

Wen SangによるOpenAI・Anthropicとの役割分担の比喻で、後半ではGenspark自身を「車」を作る側として位置づける。つまりモデルメーカーを倒すのではなく、その知能を利用者が目的地へ到達できる製品へ変えるという整理である。出典：Forbes JAPAN、2026年8月30日。 12

URL：[Forbes JAPAN原文](#)

「人間中心であるべきだ」

Wen Sangが、モデルやツールの構成ではなく、人間の仕事の連続性をUXの中心に据えるべきだと説明した箇所である。出典：Forbes JAPAN、2026年8月30日。 16

URL：[Forbes JAPAN原文](#)

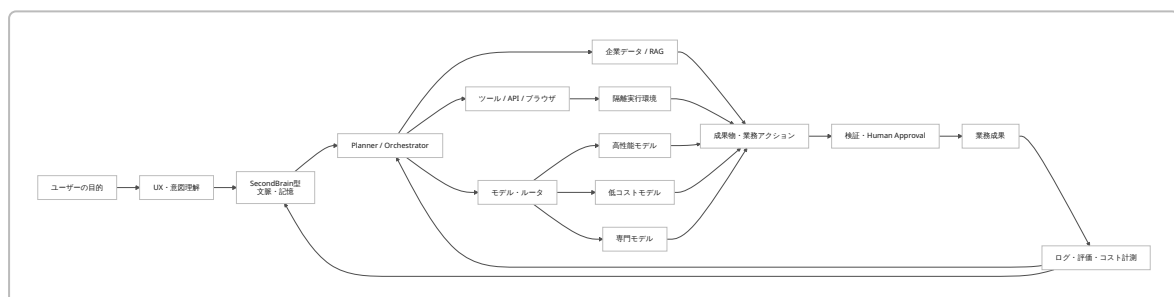
「Googleが使える人なら、Gensparkも使えるべきだ」

記事がGensparkの狙いを最も簡潔に表す言葉として紹介している。高度なAIを「プロンプト専門家向けの道具」のままにしないという思想である。出典：Forbes JAPAN、2026年8月30日。 16

URL：[Forbes JAPAN原文](#)

記事中には、GensparkがOpenAI等のフロンティアラボと密接に協力し、未公開モデルへの早期アクセスとフィードバックの関係を持つとの記述もある。ただし、**アクセス契約の相手、範囲、期間、独占性、具体的な未公開モデル名は未指定**であり、公開一次資料から契約条件までは確認できない。Reutersは2026年6月時点でOpenAI、Anthropic、Microsoft、AWSとの提携関係を報じている。 17

記事の最も重要な概念をシステム構造へ翻訳すると、次のようになる。Genspark 6.0の四層構造と、Kay Zhuが論じる「成功タスク当たりのコスト」という考え方を一般化した図である。 18



ここで本当の競争力は一つの箱ではなく、このループ全体がどの程度速く、安全に、低コストに改善され続けるかにある。

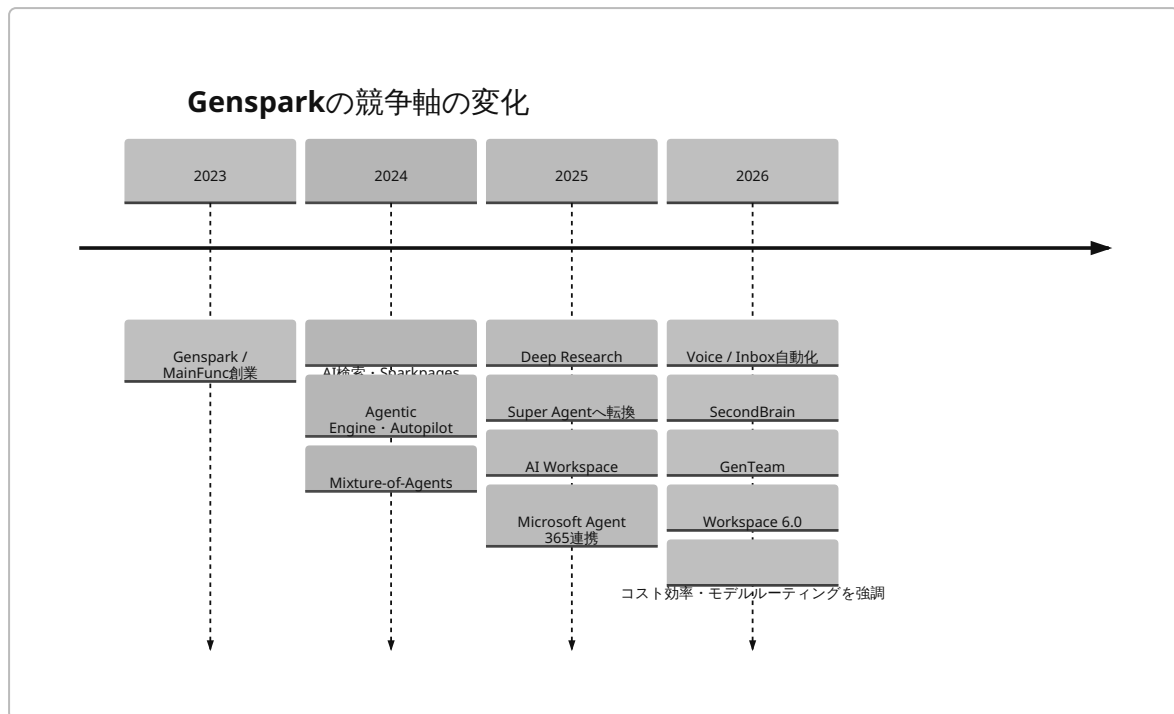
Genspark創業者・企業情報と思想の系譜

Gensparkは2023年末にパロアルトで設立された。創業メンバーについて、Forbes JAPANおよび投資家 Emergence Capitalの資料では、**Eric Jing (CEO)**、**Kay Zhu (CTO)**、**Wen Sang (COO)** が共同創業者として前面に出ている。一方、LinkedIn等ではLenjoy LinもCo-founderとして表記される資料があり、公開資料間で創業者一覧が完全には統一されていない。したがって、**正式な創業者総数・創業時の持分構成は未指定**として扱うのが妥当である。 ¹⁹

人物	公開経歴・役割	本テーマとの関係	情報の性質
Eric Jing	共同創業者・CEO。本人／Genspark公式によれば2006年にMicrosoftへソフトウェア開発者として参加し、Bing立ち上げチームに所属。その後Baidu系AI・音声デバイス事業を率いた経歴を持つ。Reutersも元Baidu幹部、Xiaoduを率いた人物として報じている。 ²⁰	「検索」から「エージェント」「仕事の完了」へ市場を再定義する事業思想を主に語る。	Microsoft/Baidu部分は独立報道でも一定確認。40M台等の実績値は本人・会社発表色が強い。
Kay Zhu	共同創業者・CTO。本人LinkedInとEmergence Capitalは、Googleのproduction searchで初期のdeep-neural ranking modelを立ち上げた経歴などを紹介する。 ²¹	マルチモデル、モデル・ルーティング、推論コスト、評価システムという技術戦略の中心人物。	LinkedIn・投資家資料。
Wen Sang	共同創業者・COO。Emergenceは、YC/Khosla支援のenterprise SaaS企業を創業しexitした経歴を紹介。本人LinkedInではSmarking等の経歴を確認できる。 ²²	「エンジン対車」「人間中心」「非専門家でも使えるAI」など、GTM・製品哲学を説明する役割が大きい。 ²³	一次プロフィール＋投資家資料。
Lenjoy Lin	LinkedIn上ではGenspark co-founderを名乗り、Google、TikTok、Pinterest等での技術経歴を記載。 ²⁴	製品・技術組織との関係。	Forbes記事では創業者三者ほど詳細に扱われていないため、創業時役割の詳細は 未指定 。

Eric Jingは2025年のGenspark公式投稿で、長年検索、AI、チャットボット、AIハードウェアに携わってきた経歴を説明しており、Gensparkの出発点が「新しい検索エンジンを作る」ことだったのは偶然ではない。2024年6月のReuters報道では、GensparkはAI検索サービスとして始まり、LlamaやGPTなど複数モデルを使用する20人規模の企業で、6,000万ドルのSeedを2.6億ドル評価で調達していた。 ²⁰

しかし検索だけでは「答え」で止まる。Genspark公式ブログの履歴では、2024年のAgentic Engine、非同期Autopilot、Mixture-of-Agents、2025年のDeep Researchを経て、2025年4月にSuper Agentへ大きく軸足を移し、2025年11月にはAI Workspaceを発表した。さらに2026年7月のWorkspace 6.0でSecondBrain、Super Agent、Suites、GenTeamの四層へ再編した。これは**検索→回答生成→エージェント→ワークスペース→継続的コンテキストOS**という一貫した上位レイヤー化である。 ²⁵



この変遷は「基盤モデル以外が価値になる」という主張が、今回の記事のために新しく作られたマーケティングメッセージではないことを示す。2025年7月にEric Jingは公式ブログで、将来は一つの完璧なモデルではなく、専門化した複数モデルと複数エージェントを組み合わせる方向だと論じ、その本当のブレークスルーは**オーケストレーション、エージェント間コミュニケーション、引き継ぎ、反復**にあると説明していた。同時に、モデル企業がAPIを閉じる可能性という戦略リスクにも触れている。 ²⁶

2026年8月6日のKay Zhuの公式投稿ではこの思想がさらに経済学へ進む。企業エージェントは検索、ツール呼び出し、サブエージェント、文書・ソフトウェア生成、自己検証、エラー回復を繰り返すため、一問一答型チャットより推論量が大きく、各ステップが遅延と失敗の機会を増やす。そのため、単純なtoken単価より**Cost per Successful Task=成功タスク当たり総費用**を管理し、タスクごとに適切なモデルを選択することが重要だとする。これは記事の「モデルを隠して仕事を終わらせる」という主張を、技術・財務レベルで裏づける過去発言である。 ²⁷

企業規模は極めて急速に拡大している。2025年11月には2.75億ドルのSeries B、12.5億ドルpost-money評価を公式発表。2026年6月にはReutersが1億ドルのSeries B extension、26億ドル評価、Series B総額4.85億ドルを報じた。既往のSeed・Series Aを含めると、Wen Sangが公表した総調達6.45億ドルとも整合する。 ²⁸

時点	資金・事業イベント	出典
2024年6月	Seed \$60M 、評価額 \$260M 。当時はAI検索中心。	Reuters ²⁹
2025年2-3月	Series A \$100M 、報道評価額 \$530M 。	Reuters / Genspark公式 ³⁰
2025年11月	Series B \$275M 、post-money \$1.25B 。	Genspark公式 ³¹
2026年6月	Series B extension \$100M 、評価額 \$2.6B 、Series B累計 \$485M 。	Reuters ¹⁷

時点	資金・事業イベント	出典
2026年6月	Wen Sang公表値：総調達 \$645M、6,400+ business clients、\$250M+ ARR。	LinkedIn ³²

なお、顧客数・ARRは企業発表であり監査財務諸表ではない。Reutersも「the company said」として会社側の数値として扱っている。したがって評価には実績として利用しつつ、独立検証済み売上高とは区別する必要がある。 ¹⁷

「モデル以外の差別化要因」と国内外の実装・成功・失敗事例

モデルが容易にAPIから調達できる世界では、単純なモデルアクセスは徐々に希少資源でなくなる。ただし「モデルがコモディティになる」と「サービスがコモディティになる」ことは同じではない。むしろ、モデルを利用して**再現可能な業務成果を安全・低コストに出す周辺システム**の重要性が増す。Genspark自身も70以上のAIモデル、150以上のツール、20以上のデータセットを企業向けページで公称しており、競争単位をモデル単体ではなくシステムへ置いている。 ³³

差別化要因	定義	具体的な実装	成功／失敗・教訓	代表的参考URL
UX / Intent Interface	AIの内部構造を見せず、ユーザーの「目的」を仕事へ変換する層。	Gensparkは自然言語、Speakly音声入力、AI Inbox等を統合。Workspace 2.0はメール処理ルールを自然言語から自動ワークフローへ変換する。 ³⁴	成功・国内: Panasonic Connectは社内生成AIでFY2025に約78.8万時間の削減効果、361万回利用、月次ユニーク利用率61%を会社発表。逆にMETRのRCTでは、経験豊富なOSS開発者が当時のAIツールを使うと平均19%遅くなり、「AIを置くだけ＝生産性向上」ではないことを示した。 ³⁵	Panasonic Connect / METR
データパイプライン / RAG	社内・外部データを収集、権限確認、正規化、索引化し、必要な時に正しい情報をAIへ供給する機構。	LY CorporationのSeekAIは部署別の社内文書をRAGで検索・回答する仕組みを展開。Genspark SecondBrainはメール、会議、チャット、文書、アプリ等を継続コンテキスト化する。 ³⁶	成功・国内: LINEヤフーは社内情報検索を業務効率化の基盤として展開。 失敗リスク: 長いコンテキストなら自動的に正しく使えるわけではなく、「Lost in the Middle」は情報位置によって検索・QA性能が大きく低下し得ることを示す。 ³⁷	LY Corp. / TACL論文

差別化要因	定義	具体的な実装	成功／失敗・教訓	代表的参考URL
インフラ / 実行環境	コード、ブラウザ、ファイル、外部APIなどを安全に実行する計算基盤。	E2BはGenspark Super Agentに隔離VMを提供し、コード実行やウェブ操作をサンドボックス化していると説明。 ³⁸	成功条件は「回答生成」ではなく、安全にside effectを実行できること。長いagent loopでは推論量・遅延・失敗箇所が増加するため、timeout、checkpoint、retry、idempotencyが必要。 ³	E2B × Genspark
運用 / Evals / Observability	本番タスクの成功率、失敗原因、モデル・プロンプト・ツール変更を継続評価する仕組み。	Gensparkはワークフロー別にモデル能力と経済性を評価し、モデルを使い分ける思想を明示。Microsoft Agent 365はagent activity/healthを集中監視するcontrol planeを提供。 ³⁹	失敗例: 現行agent benchmarkでは長期タスクになるほど性能が劣化し、ある2026年評価ではモデルだけでなくharness変更で最大18ポイント差が生じた。つまり「モデル評価」だけでは不十分。 ⁴⁰	Microsoft Agent 365 Docs
セキュリティ / Identity	誰が何を読めるか、AIが何を実行できるか、実行履歴をどう監査するかを制御する層。	GensparkはSOC 2 Type II、ISO 27001:2022認証、SSO、暗号化、Enterpriseのagent-level permissions、dedicated VPC等を公表。 ⁴¹	失敗リスク: AgentDojoは外部ツールから取得した悪意あるデータによる間接Prompt Injectionを実証。OWASPもPrompt Injectionや過剰なagencyを重大リスクとする。 ⁴²	Genspark Business / OWASP
法務 / コンプライアンス	個人情報、著作権、録音同意、出力責任、データ越境、契約責任を設計段階から扱う機能。	Genspark自身もSecondBrain Noteで医療、法務、HR等の機微な場面では録音許可を慎重に確認し、同意がなければ録音しないよう案内。 ⁴³	失敗・海外: Air Canadaはチャットボットが誤った弔事運賃情報を提示した件で責任を問われた。企業は「AIが言った」ことで責任を切り離せない。 ⁴⁴	ABA解説
ビジネスモデル	価値の回収方法。seat、usage、task、outcome、API等の課金設計。	Genspark Teamは\$30/seat/月、12,000 credits、Enterprise価格は営業問い合わせて 具体価格未指定 。 ⁴⁵	seatだけでは大量agent利用時の原価を吸収できない可能性があり、seat + credits/usageのハイブリッドが合理的。Genspark CTO自身が「成功タスク当たりコスト」を重要指標とする。 ³	Genspark Team/ Enterprise

差別化要因	定義	具体的な実装	成功／失敗・教訓	代表的参考URL
エコシステム / Distribution	Office、Slack、CRM、ブラウザ等、既存業務環境への接続と外部開発者・パートナー網。	GensparkはMicrosoft Agent 365 launch partnerとしてMicrosoft 365エコシステムと連携。Microsoft側は外部製agentもAgent 365で管理可能としている。 ⁴⁶	成功すれば流通を急拡大できる一方、OS/Officeベンダー自身が同等agentを提供するとプラットフォーム依存が競争リスクになる。	Microsoft Agent 365
カスタマイズ性	業種、会社、部署、個人のワークフロー・権限・出力様式に適応する能力。	Genspark AgentBase、GenTeam、Enterpriseのagent-level permissions。Notionも2026年にCustom Agentsを導入し、定期実行・trigger型業務を可能にした。 ⁴⁷	ノーコード化は普及に効くが、過度な自由度は「shadow agent」を生む。Genspark Teamではconnectorの一部ユーザーのみ有効化が現在できず組織全体単位であるなど、細粒度管理には制約も残る。 ⁴⁵	Genspark 6.0
コスト構造 / Model Routing	モデル・推論・検索・sandbox・人間レビューを含む一件当たり原価を最小化する仕組み。	高性能モデルを全ステップに使わず、分類・検索・生成・検証ごとに適切なモデルをroutingする。 ³	「安いtoken」を使っても失敗→再試行が増えれば総費用は上昇するため、 cost/tokenではなくcost/successful-task が適切。長期agentほど重要になる。 ⁴⁸	Genspark: AI Efficiency Frontier

この表から見える最大の変化は、AIサービスの「品質」が一つの数字ではなくなることである。たとえばモデルの推論能力が95点でも、retrieval 90%、正しい権限設定98%、tool execution 95%、verification 95%という複数段階を全部通過しなければならない長期タスクでは、全体成功率は各工程の掛け算になる。したがって、**ステップ数が増えるほど局所的な1~2%の改善にも大きな価値が生まれる**。Gensparkがモデル研究そのものよりオーケストレーション、評価、コストへ焦点を移しているのは、この「複合システム問題」への回答と解釈できる。これは本レポートによるシステム工学的推論であり、Gensparkの公式数値ではない。

また、データに関するGensparkの公開情報には重要な区別がある。企業向けでは「顧客データをモデル学習に利用しない」、サブプロセッサについてZDRを適用する場合があること、SOC 2 Type II/ISO 27001認証、データ所在地の選択等を説明している。⁴¹ 一方、一般向けPrivacy Policyでは、ユーザーがpromptに含めた個人情報が回答生成のためOpenAIやAnthropic等に送信され得ること、データがMicrosoft Azureに保存されること、米国で保存・処理され得ること、アカウントデータは退会後30日以内に削除すると説明している。⁴⁹

これは矛盾とは限らない。**Consumer、Team、Enterpriseでは契約条件・データ処理条件が異なるためである**。ただし企業導入時は「Zero Data Retention」というマーケティング文句だけではなく、DPA、subprocessor一覧、バックアップ保持、地域、ログ保持、法的hold、モデルprovider別ZDR適用状況を契約書で個別確認すべきである。Genspark Help Centerによればバックアップ保持は削除後90日で、GDPR

compliance programは現時点で「in progress」とされる。また詳細SOC 2 reportはEnterprise顧客向けNDA下で提供される。 45

競合分析と差別化マトリクス

Gensparkが直面する競争は、従来の「Perplexity対Google」のようなAI検索競争より広い。2026年時点でOpenAIはChatGPT Workspace Agents、AnthropicはClaude Cowork/Managed Agents、MicrosoftはAgent 365、GoogleはWorkspace Studio、GleanはWork AI platform、PerplexityはComputer、NotionはCustom Agentsへ進んでおり、主要各社が「回答」から**組織コンテキスト+ワークフロー実行**へ移動している。 50

以下の○○△は公開機能に基づく**定性的比較**であり、統一ベンチマークによる**性能順位**ではない。「未指定」は公開資料から十分に確認できない項目を示す。

サービス	独自基盤モデル	マルチモデル	永続的組織コンテキスト	自律ツール実行	Office/既存SaaS統合	Agentガバナンス	主な差別化
Genspark 6.0	△ 基盤モデル自体よりsystem層	◎ 70+公称	◎ SecondBrain	◎ Super Agent	○ M365等	○～◎ Enterprise	複数モデルを隠し、「完成した成果物」まで一体提供。 51
OpenAI ChatGPT Workspace Agents	◎	△ 主にOpenAI stack	○～◎ workspace knowledge/memory	◎	◎ connected apps、Slack	◎	世界有数のモデル能力とChatGPT distributionを同一製品に保持。Workspace agentsは共有、scheduled run、connected appsをサポート。 52

サービス	独自基 盤モデル	マルチモ デル	永続的組織コ ンテキスト	自律ツール 実行	Office/既存 SaaS統合	Agentガバ ナンス	主な差別化
Anthropic Claude / Cowork / Managed Agents	◎	△	○	◎	○～◎	◎	高性能 Claudeと業 務別agent template。 Financeでは KYC、 pitchbook、 month-end close等を package 化。SMB版 では送信・ 投稿・支払 前のhuman approvalを 明示する。 53
Microsoft Copilot / Agent 365	○ パー トナー モデル 含む	◎ platform として外 部agent 対応	◎ Microsoft Graph/M365	◎	◎	◎	最大の強み はEntra、 Purview、 Defenderと 結合した identity- first control plane 。外 部製agentも 管理対象に できる。 54
Google Workspace Studio / Gemini	◎ Gemini	△	◎ Gmail/ Drive/Docs/ Chat	◎	◎ Workspace native	◎	既存 Workspace の利用面と agent builderが直 結。自然言 語でflowを 作成・共有 できる。 55

サービス	独自基盤モデル	マルチモデル	永続的組織コンテキスト	自律ツール実行	Office/既存SaaS統合	Agentガバナンス	主な差別化
Glean	○ 外部 LLM 活用	◎ 複数 LLM	◎	◎	◎ 企業 connector 群	◎	permission-aware enterprise knowledge/context が強み。Glean は 250 以上の connector と複数 LLM 対応を公表する。 ⁵⁶
Perplexity Enterprise / Computer	○	○	○	◎ web/ browser 中心	○	○～◎	検索・根拠提示から browser/ action へ拡張。Computer for Enterprise は connector、credits、管理機能を提供。 ⁵⁷
Notion Custom Agents	△	△～○	◎ Notion workspace	○～◎	○	○	既に文書・project data が存在する Notion 内で、scheduled/ trigger agents を作れる点が強い。 ⁵⁸
Manus	△	○	△～○	◎	○	公開情報では一部未指定	汎用「action agent」として、成果物・操作完了に重点。Microsoft Agent 365 ecosystem にも参加。 ⁵⁹

ここからGensparkの真の競争相手は「同じようなAIスタートアップ」だけでなく、**仕事のコンテキストを既に所有するMicrosoft、Google、Notion、Glean**であることがわかる。GensparkのSecondBrain戦略は、メール・会議・資料・アプリを横断してユーザーのコンテキストを新しく集約する発想だが、MicrosoftやGoogleは最初からメール、文書、予定、アイデンティティ、権限を持っている。この点ではincumbentに構造的優位がある。 60

逆にGensparkには、既存スイートへの忠誠が比較的弱いため、**OpenAI、Anthropic、Google等のモデルを性能・価格に応じて横断利用できる「中立オーケストレーター」になれる可能性**がある。これはクラウド時代のマルチクラウド・データプラットフォームに近いポジションである。ただし、その価値は各モデル企業が十分開かれたAPIを提供し続けることを前提とする。Eric Jing自身も2025年にモデル企業がAPIを閉じる可能性をリスクとして認識していた。 26

さらに、GensparkはMicrosoftと単純競合だけの関係ではない。Microsoft Agent 365のlaunch partnerでもある。これは重要な戦略で、Gensparkが「Officeそのものを置き換える」のではなく、Microsoftのidentity/security/distributionを利用しながら、その上にエージェント・オーケストレーションを置く余地を残す。 46

したがって、競争の勝敗を決める指標はモデルbenchmarkではなく、以下に近づく。

実用AI優位性 $\approx$ **Task Success** $\times$ **Context Quality** $\times$ **Integration Coverage** $\times$ **Trust** $\times$ **Adoption** $\div$ (**Latency** $\times$ **Cost** $\times$ **Operational Complexity**)

これは本レポートの分析式である。重要なのは、どれか一つがゼロに近ければ、最高性能モデルを使用しても実務価値が消える点である。

技術・事業課題、批判的評価、リスクとロードマップ

記事の主張は全体として妥当だが、最も注意すべき点は「モデル以外が重要になる」から「モデルは代替可能で重要ではない」へ論理を飛躍させないことである。2026年の長期agent benchmarkでは、最良構成でも完全な信頼性には遠く、ある実験では同じモデルでもagent harnessの違いで最大18ポイントの性能差が生じた。これは二つのことを同時に示す。**モデル差はまだ大きい。そしてモデル以外のシステム差も同じくらい大きい。** 40

METRの研究も、AIが処理できる長時間タスクの時間幅が歴史的に急速に伸びている一方、その指標は「一定成功確率で何時間相当の人間タスクを完了できるか」を測るものであり、無限に長い業務を完全自律で処理できることを意味しない。2026年現在も長期タスクの信頼性評価自体が重要研究領域である。 61

記事の論点	批判的評価	主リスク	必要な対策
モデル選択をユーザーから隠す	妥当。専門知識を要求しない。	Routerが誤ったモデルを選ぶと、ユーザーには原因が見えない。	task-level eval、fallback、confidence、モデル選択口グ。
永続メモリ	競争力になり得る最大要素の一つ。	古い情報、誤情報、権限変更後の情報、個人情報が長期残存。	TTL、freshness score、source lineage、permission-aware retrieval、forget/delete機能。

記事の論点	批判的評価	主リスク	必要な対策
マルチモデル	供給者・価格 リスクの分散 に有効。	provider障害、API変更、出力形式差、データ移転、contract fragmentation。	abstraction layer、provider-specific eval、multi-region、contract inventory。
物理世界からのcapture	強力だが高リスク。	録音同意、営業秘密、HR、医療・法務情報。Genspark自身も機微場面での録音回避を案内。 43	明示的consent、録音LED/通知、purpose limitation、local redaction。
Agentの自律実行	最大の価値源 かつ最大の security risk。	Prompt Injection、権限逸脱、誤送信・誤購入・データ削除。AgentDojo/OWASPが問題を実証。 62	least privilege、transaction limits、sandbox、human approval、two-phase commit。
All-in-one workspace	導入容易性では強い。	Microsoft/Google等との機能重複、feature sprawl。	horizontal platform + 高ROI vertical workflowの二層戦略。
モデルを大量に組み合わせる	性能・コスト最適化に有効。	observability、billing、debuggingが複雑化。	cost/successful-task、trace、replay、A/B router eval。
成果主義のAI	最も重要な記事の洞察。	「作業量削減」が「事業成果」に直結するとは限らない。METRの19% slowdown事例が警告。 63	ROIを時間だけでなく売上、品質、cycle time、error rateまで測る。

セキュリティ面では「persistent memory」と「autonomous action」を組み合わせるほど脅威モデルが変わる。従来型チャットボットの誤回答は画面上の間違いで終わる場合が多いが、エージェントがメール、CRM、カレンダー、支払、コード実行へアクセスすれば、悪意ある外部文書が実行命令へ変換され得る。AgentDojoはメール、銀行、旅行予約など現実的タスクを含む97タスク・629 security test casesでこの問題を評価している。
64

したがって「回答前に安全性を確認する」だけでは足りない。設計は原則として、

read権限 ≠ write権限 ≠ send権限 ≠ money-moving権限

と分離すべきである。たとえばAnthropicのSmall Business向けagentsが、送信・投稿・支払いの前に人間承認を置く設計を明示しているのは合理的なパターンである。
65 Microsoft Agent 365もEntraによるagent identity、Purviewによるデータ統制、Defenderによるsecurityを統合する方向を採っている。
66

法規制について、日本では「人工知能関連技術の研究開発及び活用の推進に関する法律」が2025年6月4日に公布され、2025年9月1日に全面施行された。2026年3月には経産省・総務省の「AI事業者ガイドライン」が第1.2版となり、2026年7月には第II期人工知能基本計画も閣議決定されている。
67 個人情報保護委員会も生成AI利用に際する個人情報の入力・取扱いについて注意喚起しているため、SecondBrain型サービスでは個人情報保護法対応が「付加機能」ではなく基礎設計となる。
68

EUではAI Actが2024年8月1日に発効し、規定は段階的に適用されている。欧州委員会は2026年8月2日にも適用段階の更新を案内しており、EUで展開するagent serviceではAI Act、GDPR、業種規制を統合したcompliance-by-designが必要になる。
69 Gensparkの現行Help CenterはSOC 2 Type IIとISO 27001:2022を

certifiedとする一方、GDPR compliance programを「in progress」と記載しているため、EUの高規制顧客は個別DPA・data residency・subprocessor条件を確認する必要がある。 45

NISTのAI RMFとGenerative AI Profileは、こうしたリスクを単発のsecurity reviewではなく、AI lifecycle全体でGovern、Map、Measure、Manageしていく方向を示している。次世代AIサービスの差別化は、認証マークの有無だけではなく、**評価・インシデント対応・変更管理・監査証跡を日常運用へ落とせるか**に移る。 70

ロードマップ試算。 以下はGenspark自身の投資計画ではなく、「**自社でフロンティア基盤モデルを訓練せず、複数モデルAPIを用いて100～1,000席規模の企業向けagent serviceを構築する事業者**」を想定した本レポート独自の概算である。対象業種・既存システム・海外展開範囲はユーザー指定がないため**未指定**であり、予算には幅を持たせている。フロンティアモデル自社訓練費用は含まない。

期間	重点施策	必要人材の目安	投資規模概算	主要KPI
短期：0-6カ月	2～3の高頻度・低不可逆性workflowを選定。baseline測定。RAG/connector、SSO、audit log、model router、sandbox、human approval、offline evalを構築。	8-12 FTE：Product 1、Agent/ML 3-4、Platform/SRE 2、Data 1、Security 1、UX 1、Domain/CS 1-2	1.5～3億円	Task Success >80%、critical error <1%、Time-to-Outcome ▲30%以上、cost/successful-task、WAU/eligible users、human override率
中期：6-18カ月	Persistent context、permission-aware retrieval、workflow builder、model A/B routing、SLA/SOC運用、部署展開、vertical templates。	20-35 FTE：上記にEval、Security/Compliance、Data Eng、FinOps、Forward Deployed Eng、Customer Successを追加	累積6～15億円	Task Success >90%、p95 latency、cost/successful-task ▲30～50%、30/90日 retention、seat activation >70%、重大 security incident 0
長期：18-36カ月	Enterprise-grade agent platform、地域別data residency、agent marketplace、partner API、継続学習・policy engine、業種別compliance、国際展開。	40-70 FTE	累積20～50億円	gross margin、NRR >120%目標、workflow expansion、agent-created business value、SLA >99.9%、false-action率、regulatory incidents 0

この試算では、完全雇用コストを一人当たり年1,500万～2,500万円程度と置き、API/cloud/sandbox/observability/security/compliance/GTMを追加する。これは**市場平均値を断定するものではなく投資計画用の仮定**であり、API使用量や人間レビューが多いサービスではインフラ原価が大きく上振れする。

最重要KPIは「プロンプト数」でも「token数」でもない。Genspark CTOの議論を一段拡張すると、次の指標体系が妥当である。 3

Cost per Successful Task =
$$\frac{\text{Model API} + \text{Search/Data} + \text{Sandbox/Compute} + \text{Human Review} + \text{Retry Cost}}{\text{成功判定された業務タスク数}}$$

さらに事業KPIは、

Net AI Value = 削減労働費 + 増分売上 + 品質改善価値 + Cycle Time削減価値 - AI総運用費 - Review/Review

で測るべきである。「何時間短縮したか」だけでは、METRのように実際には作業者を遅くするケースや、品質低下による後工程コストを捕捉できない。 63

本レポートが特に重要と考えるKPIは、**task success rate、critical-error rate、human-intervention rate、cost per successful task、time-to-outcome、first-pass acceptance rate、security-policy violation、data-freshness failure、30/90-day retained users、workflow expansion、gross margin**である。

推奨アクションと最終評価

事業者向け。記事から「複数の最新モデルを載せれば勝てる」と読むべきではない。最初にするべきなのはモデルrouterより、**どの業務を「完了」と定義するかを機械判定できる評価基盤**である。たとえば営業提案なら「スライドを作った」で終わらず、必要データの網羅、引用の正確性、ブランドテンプレート、数値一致、承認、CRM更新までを成功条件にする。その成功判定がなければ、最適モデルもコスト最適化も学習できない。長期agentの信頼性がまだ未解決であるという研究結果からも、この順序が重要である。 71

次に、モデルは交換可能に設計する一方、**企業固有のコンテキスト層、権限グラフ、評価データ、ユーザー修正履歴は自社資産として蓄積**すべきである。基盤モデルの能力が毎年上がるほど、モデルそのものへの独自投資より「新モデルを一週間で安全に評価・切替できる能力」の価値が上がる。Gensparkのマルチモデル思想はこの点で合理的だが、本当の堀はモデル数ではなく、そのrouterを改善する評価データと運用ループである。 3

第三に、**read → draft → recommend → execute → irreversible action**の順に自律性を段階開放すべきである。メール要約と銀行振込を同じagent permission modelで扱ってはいけない。Prompt Injectionや過剰agencyが既知の問題である以上、高リスク操作にはhuman-in-the-loop、最小権限、一回限りtoken、金額制限、二段階commit、完全audit trailを設けるべきである。 62

さらにSecondBrain型の製品を作るなら、「記憶量最大化」を目標にすべきではない。**正しく忘れる能力**もプロダクト機能である。保存目的、TTL、削除、source attribution、権限失効時の再index、個人情報redaction、データ所在地を最初から設計する必要がある。Gensparkの公開Privacy Policy自身が、prompt経由の情報を外部AI providerへ送る場合や米国処理の可能性を明示している。 49

投資家向け。次世代AIアプリを評価するとき、モデルbenchmarkやデモ動画より、次の三つを見るべきである。第一は、**一回使った後も蓄積する資産が何か**。評価データ、permissioned context graph、domain workflow、integration、network effectsがなければ、新しい基盤モデルの機能追加で差別化が消える。第二は、**AI原価を含めたgross marginとcost/successful-taskの改善速度**。agentが長時間動くほど売上と同時に推論費も伸びるため、ARRだけでは質を評価できない。第三は、**distribution**である。GensparkがMicrosoft Agent 365へ参加するのは、モデル優位より流通・企業導入経路が重要だからと解釈できる。 72

Gensparkについては、26億ドル評価、6.45億ドル総調達、ARR 2.5億ドル超という公表値は非常に強いtractionを示す一方、少なくとも公開資料上はARRの監査方法、cohort別retention、gross margin、credit消費に対する推論原価、enterprise/consumer revenue mix、顧客集中度は**未指定**である。これらは投資判断では顧客数そのものより重要である。 5

特にDDでは、「**モデルAPI価格が2倍になった場合**」「**主要providerがAPIアクセス条件を変更した場合**」「**Microsoft/Googleが同等agentをbundleした場合**」の三つの**stress test**を行うべきである。Eric Jing自身がmodel providerによるAPI閉鎖リスクを以前から認識しているため、これは仮想的すぎる論点ではない。

研究者向け。「モデル性能」だけでなく、agentic system全体の科学へ研究対象を広げるべきである。特に不足しているのは、長時間・確率的・状態変更を伴う仕事の評価である。AgentDojoはsecurity、METRIはtask horizon、SentinelBenchはreaction timeとresource use、2026年の長期benchmark群はharness差を含む信頼性を測り始めている。 ⁷³

今後重要になる研究課題は、**長期タスクのreliability science、permission-aware memory、agent identity、prompt-injection耐性、model-router learning、uncertainty calibration、cost-aware planning、human-agent handoff、multi-agent coordination、忘却・データ最小化**である。これらこそ「モデル以外の差別化」を学術的な測定可能概念へ変える領域である。

記事に対する最終評価は、「方向として正しいが、『モデルの後』ではなく『モデルの上』に新しい競争が形成される、と表現した方が正確」である。

モデル競争は終わらない。OpenAI、Anthropic、Google等がモデルを改善すれば、agent serviceの可能な仕事範囲そのものが広がる。実際、長期タスク能力は今もモデル世代によって大きく動いている。 ⁷⁴ しかしモデルが高度化するほど、人間は「どのモデルを選ぶか」を考えなくなり、代わりに**AIが自分の状況を理解しているか、正しいデータを見ているか、仕事を最後まで実行できるか、誤った時に止まれるか、価格に見合うか**を見るようになる。

その意味でGenspark創業者たちの「エンジンではなく車を作る」という発想の本質は、単なる製品比喻ではない。AI産業の価値移動を、

- Intelligence as a Model
- Intelligence as a Product
- Intelligence as a Workflow
- Intelligence as an Operating System for Work

と捉える戦略である。Genspark 6.0のSecondBrain、Super Agent、Suites、GenTeamという構造は、その「仕事のOS」仮説をかなり明示的に具現化している。 ⁴

ただし最終的に勝つのは、最も多くのモデルを束ねた会社でも、最も大きなcontext windowを持つ会社でもない可能性が高い。**ユーザーの意図から安全で検証可能な業務成果までを、最小の認知負荷・最小の成功タスク原価で閉ループ化できる会社**が強い。

そして、その閉ループの中で最も模倣困難なのはモデルAPIそのものではなく、**顧客固有の文脈、ワークフロー、権限関係、失敗データ、評価体系、改善運用、信頼、distributionの蓄積**である。ここまで含めて読むことで、2026年8月30日のForbes JAPAN／Yahoo!ニュース記事が提示した「AIの勝負はモデルでは終わらない」という命題は、単なる「UXが大事」という話ではなく、**AIの競争単位が単体モデルから社会技術的な業務システム全体へ移行している**という、より強い産業構造上の主張として理解できる。 ⁷⁵

主要一次・準一次資料

資料	公開日	URL
Forbes JAPAN「AIの勝負はモデルでは終わらない…」	2026-08-30	Forbes JAPAN ²
Yahoo!ニュース配信ページ	2026-08-30	Yahoo!ニュース
Genspark AI Workspace 6.0	2026-07-20	Genspark公式 ⁴

資料	公開日	URL
The AI Efficiency Frontier	2026-08-06	Genspark公式 3
Genspark Privacy Policy	2026年7月24日版	Genspark公式 49
Genspark Team & Enterprise Plans	現行	Genspark Help Center 45
Genspark Series B / Workspace	2025-11-20	Genspark公式 31
Genspark \$2.6B valuation	2026-06-17	Reuters 17
OpenAI Workspace Agents	2026-04-22	OpenAI公式 76
Anthropic Finance Agents	2026-05-05	Anthropic公式 77
Microsoft Agent 365	現行	Microsoft公式 78
Google Workspace Studio	2025-12-04	Google公式 79
NIST AI RMF / GenAI Profile	2024-07-26	NIST 80
AI事業者ガイドライン第1.2版	2026-03-31	経済産業省 81
日本AI法	2025-06-04公布、同年09-01全面施行	内閣府 82
AgentDojo	2024	arXiv 64
METR Task-Completion Time Horizons	更新版 2026	METR 83
Lost in the Middle	TACL 2024	ACL Anthology 84

1 2 19 75 AIの勝負はモデルでは終わらない、Genspark創業者が描く「次のAIサービス」の条件 | Forbes JAPAN 公式サイト（フォーブス ジャパン）

<https://forbesjapan.com/articles/detail/103707>

3 8 27 39 48 72 The AI Efficiency Frontier: How Enterprises Scale Agentic AI Without Letting Cost Outrun Value

<https://www.genspark.ai/blog/the-ai-efficiency-frontier>

4 10 14 18 47 51 Introducing Genspark AI Workspace 6.0

<https://www.genspark.ai/blog/genspark-ai-workspace-6>

5 17 AI startup Genspark valued at \$2.6 billion in latest funding round | Reuters

<https://www.reuters.com/technology/gensparkai-valued-26-billion-latest-funding-round-2026-06-17/>

6 42 62 64 73 AgentDojo: A Dynamic Environment to Evaluate Prompt Injection Attacks and Defenses for LLM Agents

https://arxiv.org/abs/2406.13352?utm_source=chatgpt.com

7 11 50 52 76 Introducing workspace agents in ChatGPT

https://openai.com/index/introducing-workspace-agents-in-chatgpt/?utm_source=chatgpt.com

9 40 71 A Benchmark for Real-World, Long-Horizon Agent Evaluation

https://arxiv.org/html/2605.10912v1?utm_source=chatgpt.com

- 12 13 23 AIの勝負はモデルでは終わらない、Genspark創業者が描く「次のAIサービス」の条件 | Forbes JAPAN 公式サイト (フォーブス ジャパン)
<https://forbesjapan.com/articles/detail/103707/page2>
- 15 16 AIの勝負はモデルでは終わらない、Genspark創業者が描く「次のAIサービス」の条件 | Forbes JAPAN 公式サイト (フォーブス ジャパン)
<https://forbesjapan.com/articles/detail/103707/page3>
- 20 Seeing AGI
https://www.genspark.ai/blog/seeing-agi-impact?utm_source=chatgpt.com
- 21 Kay Zhu - Co-founder & CTO @ Genspark | AI
https://www.linkedin.com/in/kay-zhu-522b275?utm_source=chatgpt.com
- 22 Genspark: The Ultimate System of Context
https://www.emcap.com/thoughts/genspark-the-ultimate-system-of-context?utm_source=chatgpt.com
- 24 Lenjoy Lin - Co-Founder at Genspark.ai, ex-Google/TikTok ...
https://www.linkedin.com/in/lenjoy?utm_source=chatgpt.com
- 25 Blog
https://www.genspark.ai/blog?utm_source=chatgpt.com
- 26 Seeing AGI (5): Multi-Model and Multi-Agent is the Future
<https://www.genspark.ai/blog/seeing-agi-impact5>
- 28 31 Genspark AI Workspace: Where Your Work Gets Finished ...
https://www.genspark.ai/blog/genspark-ai-workspace-and-series-b-funding?utm_source=chatgpt.com
- 29 AI search startup Genspark raises \$60 million in seed round to challenge Google
https://www.reuters.com/technology/artificial-intelligence/ai-search-startup-genspark-raises-60-million-seed-round-challenge-google-2024-06-18/?utm_source=chatgpt.com
- 30 AI startup Genspark raises \$100 million to compete with Google, source says
https://www.reuters.com/technology/artificial-intelligence/ai-startup-genspark-raises-100-million-compete-with-google-source-says-2025-02-21/?utm_source=chatgpt.com
- 32 Genspark Valuation Surpasses \$2.6B with \$645M Raised | Wen S. posted on the topic | LinkedIn
https://www.linkedin.com/posts/wen-sang_genspark-ai-seriesb-activity-7473078893994876928-19TT
- 33 41 Genspark for Business | Team & Enterprise AI Workspace
https://www.genspark.ai/business?utm_source=chatgpt.com
- 34 Genspark AI Workspace 2.0: Don't Type, Just Speak, Work ...
https://www.genspark.ai/blog/genspark-ai-workspace-2?utm_source=chatgpt.com
- 35 パナソニック コネクト、AI活用で総労働時間の3.4%削減 ...
https://news.panasonic.com/jp/press/jn260729-1?utm_source=chatgpt.com
- 36 LINEヤフー、RAG技術を活用した独自業務効率化ツール ...
https://www.lycorp.co.jp/ja/news/release/008806/?utm_source=chatgpt.com
- 37 Lost in the Middle: How Language Models Use Long Contexts
https://arxiv.org/abs/2307.03172?utm_source=chatgpt.com
- 38 How Genspark Uses E2B to Run a General-Purpose AI ...
https://e2b.dev/blog/genspark?utm_source=chatgpt.com

- 43 **SecondBrain Note | Genspark Help Center**
https://www.genspark.ai/helpcenter/secondbrain-note?utm_source=chatgpt.com
- 44 **BC Tribunal Confirms Companies Remain Liable for ...**
https://www.americanbar.org/groups/business_law/resources/business-law-today/2024-february/bc-tribunal-confirms-companies-remain-liable-information-provided-ai-chatbot/?utm_source=chatgpt.com
- 45 **Team & Enterprise Plans | Genspark Help Center**
https://www.genspark.ai/helpcenter/team-enterprise-plans?utm_source=chatgpt.com
- 46 **A Strategic Collaboration with Microsoft to Bring AI Agents ...**
https://www.genspark.ai/blog/genspark-microsoft-agent365?utm_source=chatgpt.com
- 49 **Privacy Policy - Genspark**
<https://www.genspark.ai/privacy>
- 53 77 **Agents for financial services**
https://www.anthropic.com/news/finance-agents?utm_source=chatgpt.com
- 54 60 66 78 **Microsoft Agent 365: The Control Plane for Agents**
https://www.microsoft.com/en-us/microsoft-agent-365?utm_source=chatgpt.com
- 55 79 **Introducing Google Workspace Studio to automate ...**
https://workspace.google.com/blog/product-announcements/introducing-google-workspace-studio-agents-for-everyday-work?utm_source=chatgpt.com
- 56 **Glean – Enterprise AI that Works | Agents, Assistant & Search**
https://www.glean.com/?utm_source=chatgpt.com
- 57 **Perplexity Enterprise**
https://www.perplexity.ai/enterprise?utm_source=chatgpt.com
- 58 **February 24, 2026 – Notion 3.3: Custom Agents**
https://www.notion.com/releases/2026-02-24?utm_source=chatgpt.com
- 59 **Manus: Hands On AI**
https://manus.im/?utm_source=chatgpt.com
- 61 **Measuring AI Ability to Complete Long Software Tasks**
https://metr.org/blog/2025-03-19-measuring-ai-ability-to-complete-long-tasks/?utm_source=chatgpt.com
- 63 **Measuring the Impact of Early-2025 AI on Experienced ...**
https://metr.org/blog/2025-07-10-early-2025-ai-experienced-os-dev-study/?utm_source=chatgpt.com
- 65 **Introducing Claude for Small Business**
https://www.anthropic.com/news/claude-for-small-business?utm_source=chatgpt.com
- 67 82 **人工知能関連技術の研究開発及び活用の推進に関する法律 ...**
https://www8.cao.go.jp/cstp/ai/ai_act/ai_act.html?utm_source=chatgpt.com
- 68 **生成AIサービスの利用に関する注意喚起等について**
https://www.ppc.go.jp/news/careful_information/230602_AI_utilize_alert/?utm_source=chatgpt.com
- 69 **AI Act enters into force - European Commission - Europa.eu**
https://commission.europa.eu/news-and-media/news/ai-act-enters-force-2024-08-01_en?utm_source=chatgpt.com
- 70 80 **AI Risk Management Framework**
https://www.nist.gov/itl/ai-risk-management-framework?utm_source=chatgpt.com

74 83 Task-Completion Time Horizons of Frontier AI Models

https://metr.org/time-horizons/?utm_source=chatgpt.com

81 AI事業者ガイドライン

https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/20260331_report.html?utm_source=chatgpt.com

84 Lost in the Middle: How Language Models Use Long ...

https://aclanthology.org/2024.tacl-1.9/?utm_source=chatgpt.com