

2026.05.24

MORNING DISPATCH / Vibe Coder Bootcamp Tech News

今朝のホットな話題

7 トピック
を整理。

【Content Data】

1. OpenAI Codex Thursday — ロック中Macもスマホから操作可能に
2. Anthropic Project Glasswing — Claudeが重大脆弱性10,000件超を発見
3. Cursor SDK 独自エージェントをPython/TSで構築



1. OpenAI Codex Thursday — ロック中Macもスマホから操作可能に



🔍 何が起きた？

OpenAIが「Codex Thursday」と称してCodexアプリの大型アップデートを連発。最大の目玉は、Macが画面ロック・スクリーンオフのままでもスマホからCodex経由でMacのアプリを安全に操作操作できる機能。

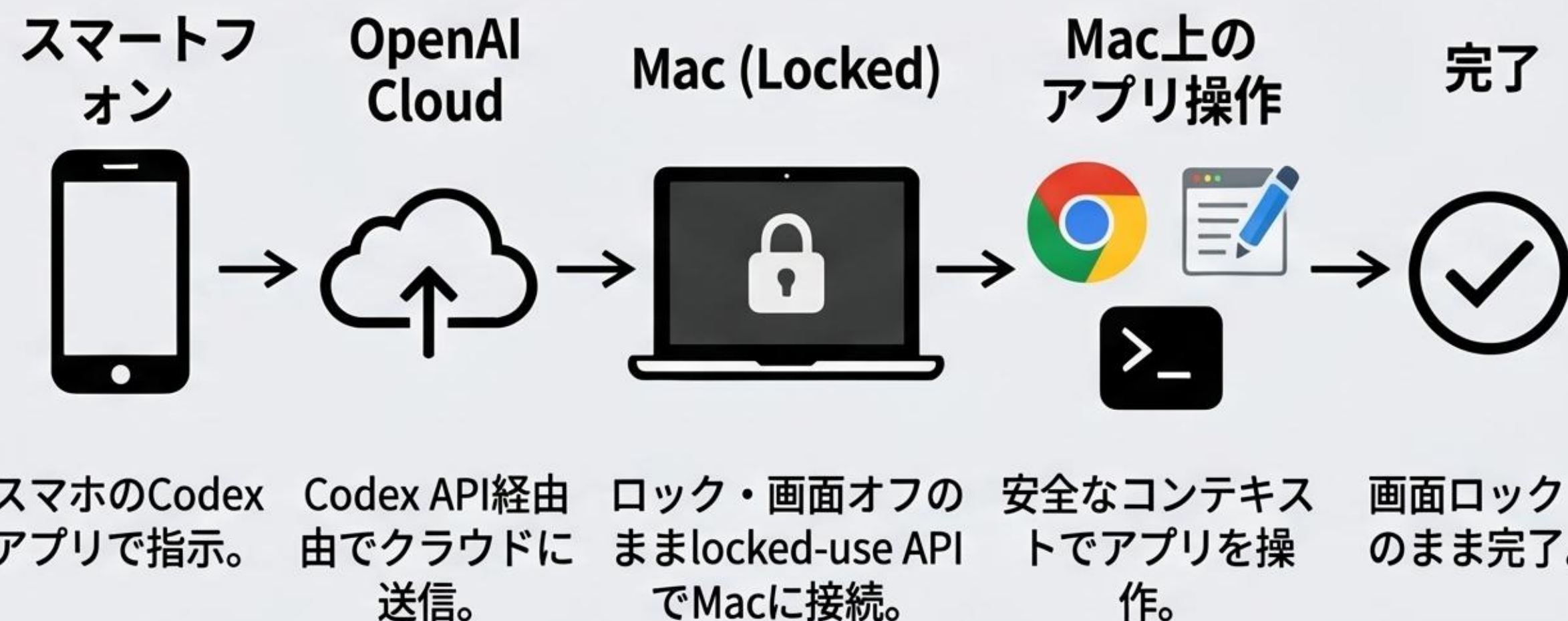
📌 主な変更点

- Mac unlock不要のリモート操作可能 (locked-use API)
- 作業中アプリのコンテキストを丸ごと渡せる「Appshots」
- 差分マーカ―設定機能
- 法人向けanalytics拡充

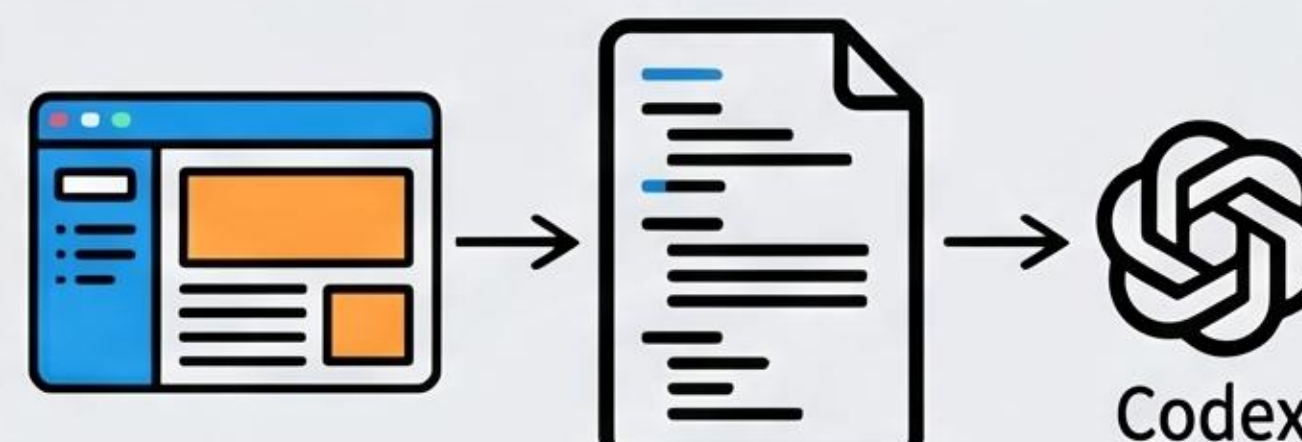
💡 なぜ重要？

セキュリティを保ちつつ、Macがロック状態でもスマートフォンからリモートでPCアプリを安全かつ便利に操作できる (locked-use API)。また、「Appshots」によるコンテキスト継承でより高度なAIアシストが可能になる。

Remote Operation Flow



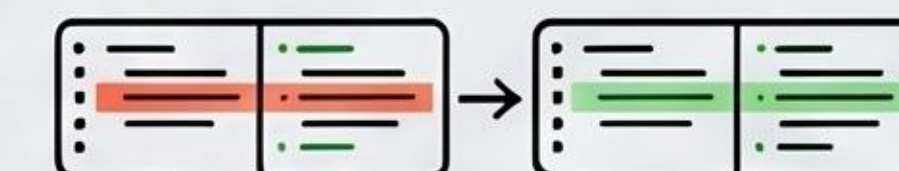
「Appshots」でコンテキスト共有



作業中アプリの状態と全データを丸ごとCodexに渡す。

その他アップデート

差分マーカ―



法人向けanalytics



2. Anthropic Project Glasswing — Claudeが重大脆弱性10,000件超を発見

🔍 何が起きた？

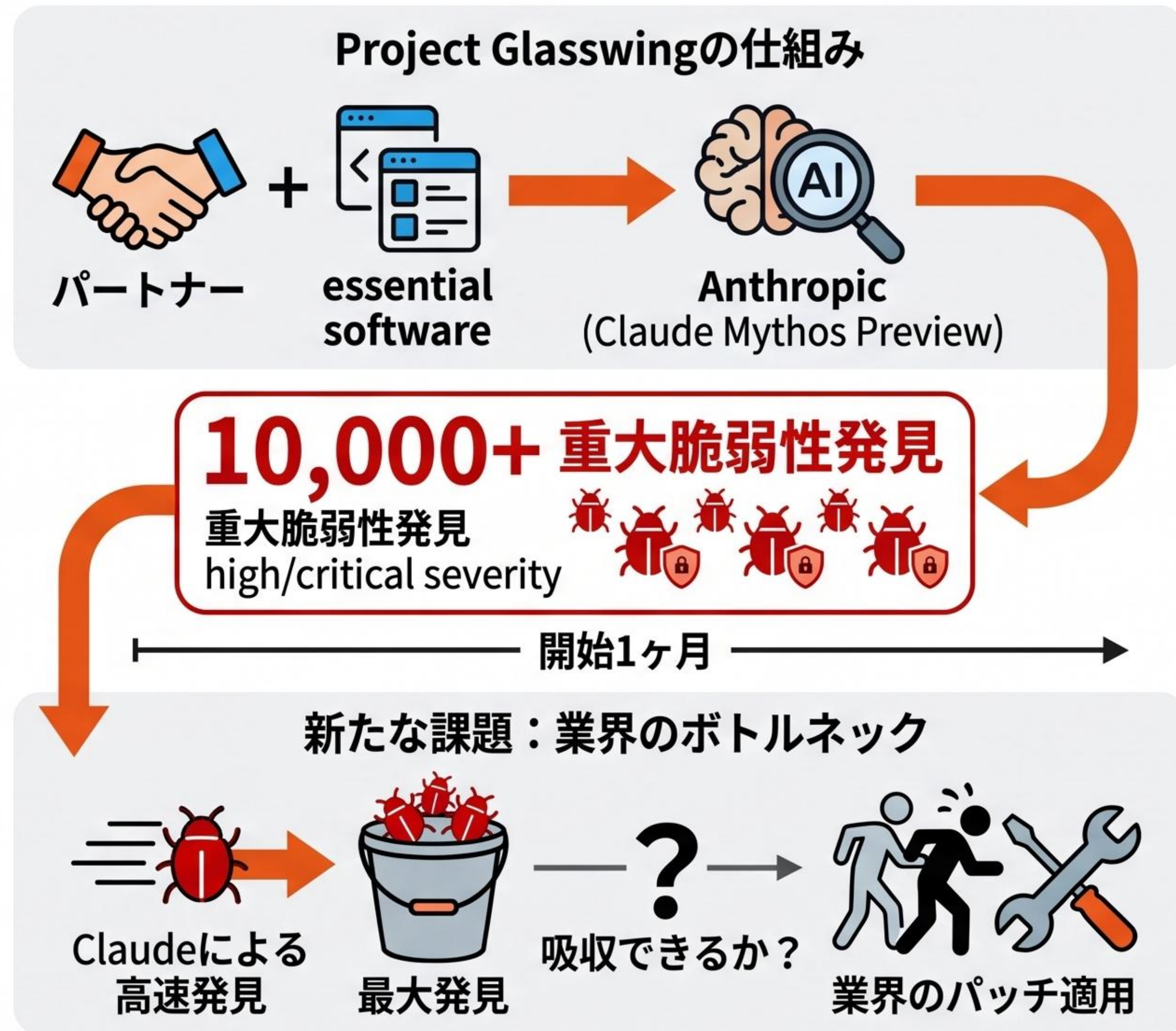
Anthropicが2026-04に立ち上げた共同サイバーセキュリティ・イニシアチブ（Project Glasswing）が、開始1ヶ月で重要ソフトウェアからhigh/critical severityの脆弱性を10,000件以上と発見したと初回レポート。

📌 主な変更点

- パートナーと共同で essential software をスキャン
- 新世代モデル「Claude Mythos Preview」級が発見を担当。

💡 なぜ重要？

発見される脆弱性の量を、業界がパッチで吸収できるかが新たな課題となる。



3. Cursor SDK + Composer 2.5 — 独自エージェントをPython/TSで構築



🔍 何が起きた？

Cursor SDK一般提供開始。Cursor内蔵のCoding agent (Composer 2.5)と同じランタイムを利用可能に。

📌 主な変更点

- Python / TypeScriptから叩いて独自エージェントを構築
- 連休限定：SDK経由のComposer利用が90% OFF

💡 なぜ重要？

デベロッパーはCursorの強力なCoding agent機能を自社のアプリやカスタムツールに直接統合でき、高度な自律型開発エージェントを構築可能になる。

CURSOR SDKエコシステムと独自エージェント構築フロー

YOUR CODE
(Python/TS)

```
1 SnpedLeere=>(  
2 ud("composer511(s)=  
3 pethl ="#ndae1/aest")  
4 patn: "ComposerialeComporri3")  
5 return (  
6 text: "code-saierInome")  
7 taatie: "composerIneINcope")  
8 )  
9 }  
10 def main() + {  
11 deosouer = ircate( agent()  
12 for x == 4:  
13 if s wcoivenss("come")  
14 ndsch.ezipsfr.r++  
15 return oxett  
16 ))
```

YOUR CODE
(Python/TS)

CURSOR SDK



← CUSTOM AGENT



CUSTOM AGENT

CURSOR INTERNAL RUNTIME
(Composer 2.5 Engine)

✨ 連休限定オファー

90% OFF

SDK経由のComposer利用



4. Gemini Omni — フルマルチモーダル、動画をネイティブ編集

📰 何が起きた？

Ethan Mollickが解説：Gemini Omniは他社の動画AIと違って fully multimodal で動画をネイティブ編集可能。

📌 主な変更点

1896年の "train" 映像にLEGO・新幹線・タイムトラベラー・ムカデ・マペットを追加するデモが拡散。反射光まで自然に整合する。

💡 なぜ重要？

text / image / audio / video を1モデルで in/out できる Omni 設計。

Native Fully Multimodal Model



動画ネイティブ編集デモ (Before/After)

Before: 1896年 'train' 映像
(オリジナル)



After: ネイティブ編集後



💡 要点

Karpathyが「クエリの最後に 'structure your response as X' を必ず付ける」だけで品質が劇的に上がると投稿。

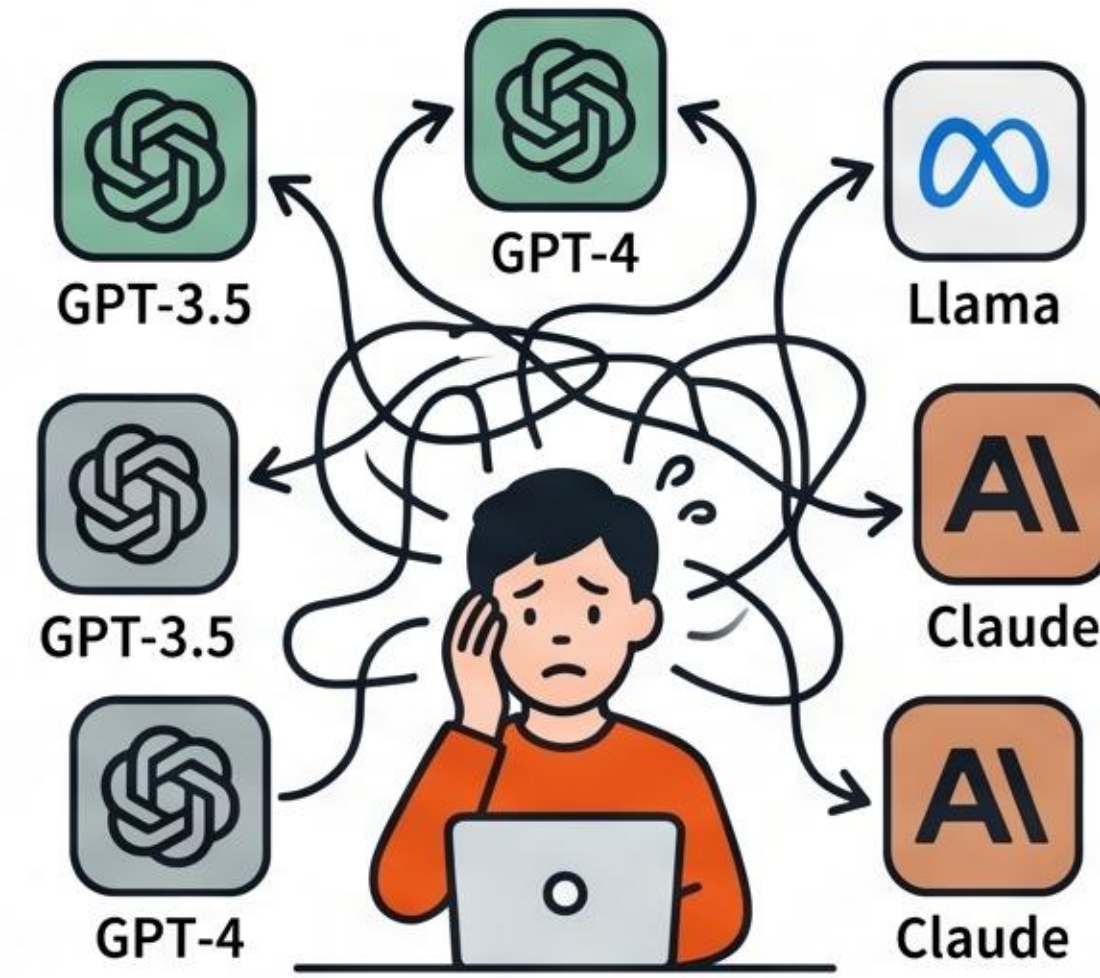
🔧 具体的な手法 / 使いどころ

- 毎クエリ末尾に 'structure as ...' を追加する。
- 「強いモデル」より「良い要求の構造化」を優先すべきと拡散。
- AYiの続報：過去半年のAIワークフローを全否定したと衝撃。

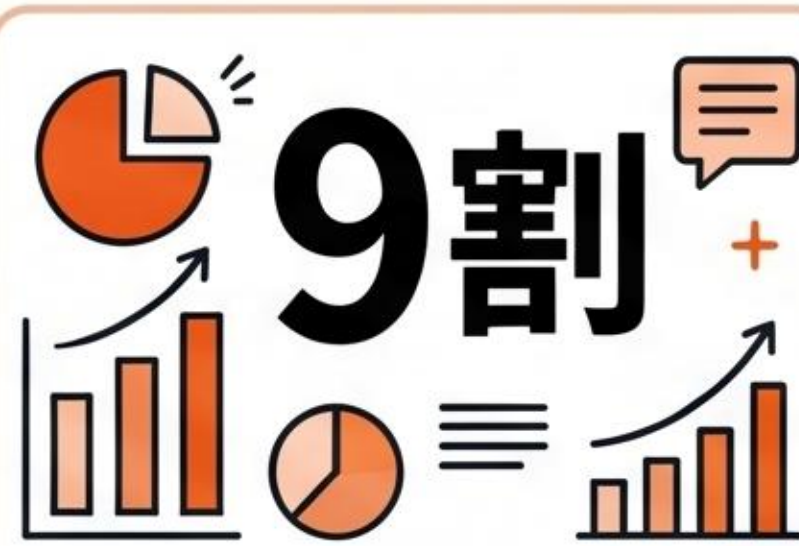
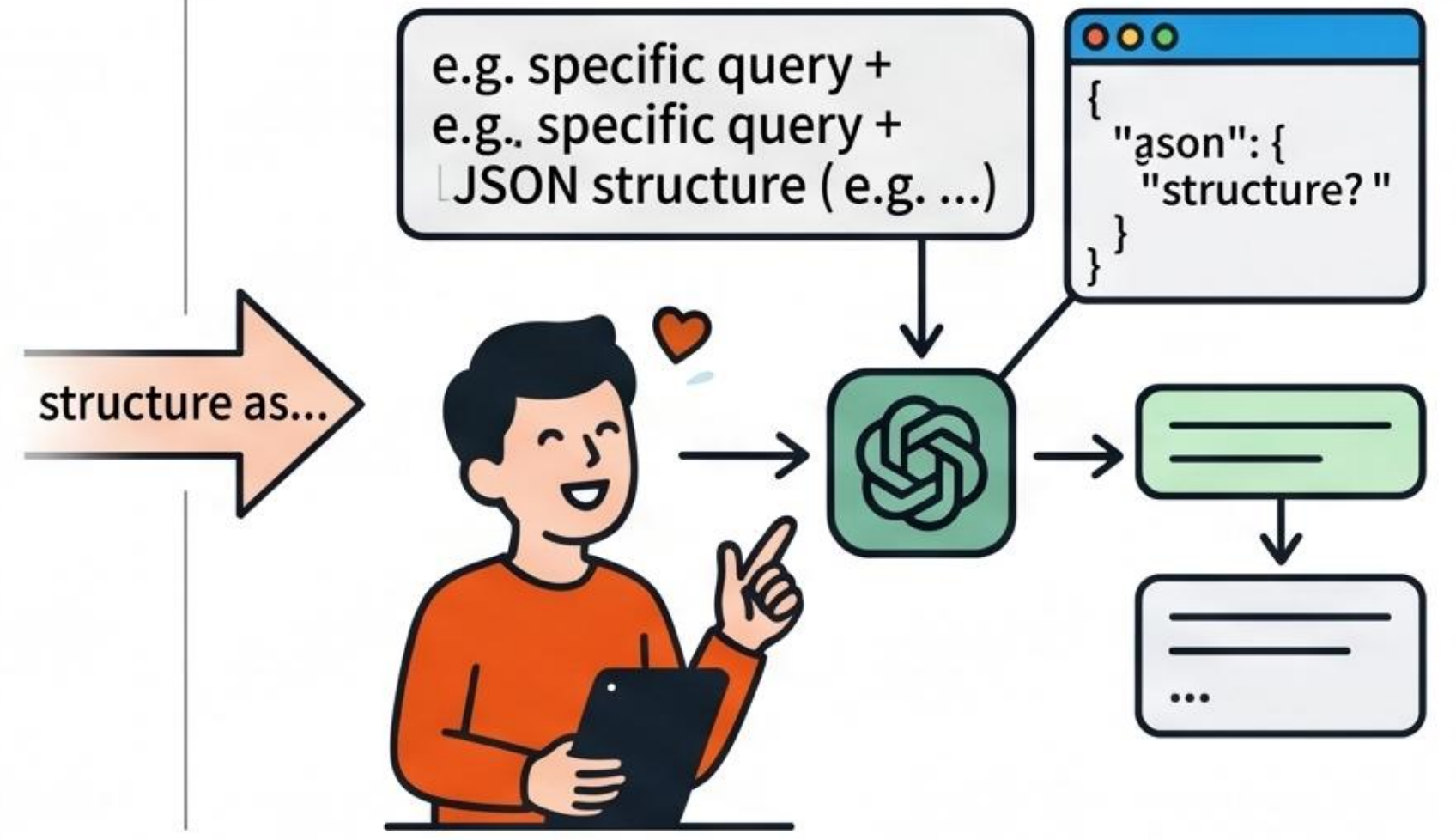
🌱 なぜ刺さるか / 学び

LLM性能を引き出す根本的な転換。「単に問いかける」から「出力形式を規定して制御する」へ。

旧：強いモデルを求めて彷徨う



新：「良い構造化要求」で即品質向上



LLM 📈 活用の「構造化要求」という概義

Karpathyの主張：
LLM活用は「構造化要求」が9割

Xでの反応：AYi
「Karpathyのこのスレッドが過去半年の自分のAIワークフローを全否定した」
拡散：要求の構造化を優先すべき

6. Greg Brockman: "the model alone is no longer the product"

何が起きた？

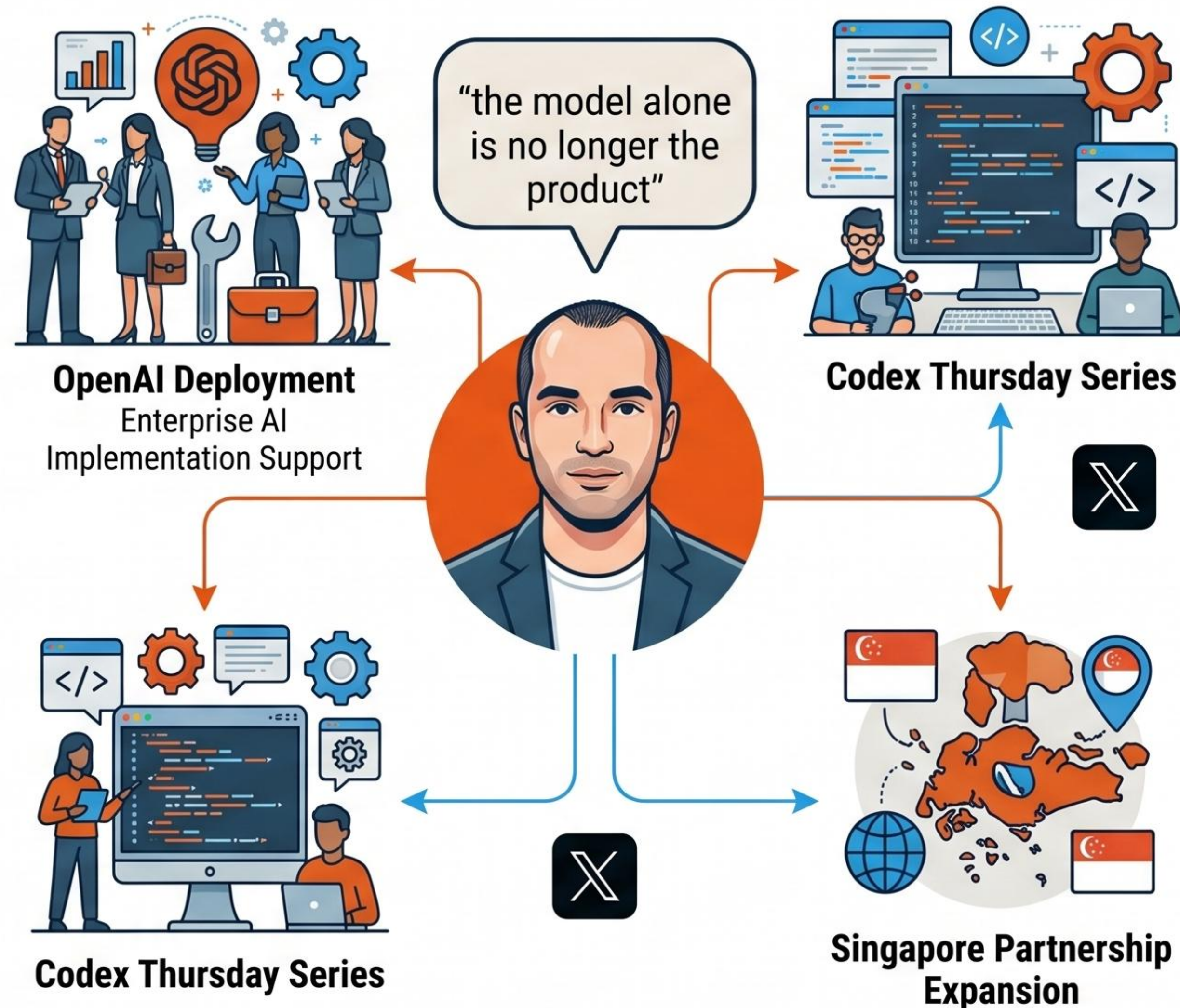
- Greg Brockman made a single-sentence post: 「the model alone is no longer the product」 .
- This declaration made a chain of concurrent announcements from OpenAI on the same day.

主な変更点

- Literal from the Content Data:
- **Greg Brockman's post**
- Concurrent moves: OpenAI Deployment Company announcement, Codex Thursday series-, Singapore partnership expansion.
- **OpenAI Deployment Company** (-enterprise AI implementation support).

なぜ重要？

The statement reflects a strategic shift by OpenAI beyond building models towards **deployment, enterprise services**, and global expansion. .Just just the 'model' to practical applications and ecosystem support based on the content.



🔍 何が起きた？

チームみらい・安野貴博氏が党首討論にて、政治家はAIの影響を過小評価せず、トップ自らAIを使い倒すべきと提言。

📌 提言の要点

- トップのAI活用不足への警鐘
- シンガポール・ヴィヴィアン外相のNanoClaw活用例を紹介
- 総理からAI活用と家庭教師依頼の応答を得る

💡 なぜ重要？

意思決定者の“AI素振り”不足が政治の論点へ。国全体の発展を左右する重要課題として認識された。

日本のトップがAIを『使い倒す』未来

効率的な政策判断

政治の政策の判断を評価し、効率的な政策判を判断

データドリブンな政治

データドリブンな政治や、イタリオーゾンな政術

迅速な意思決定

総理にコラボレートな迅速化を給み、迅速な意思決定



効率的な政策判断

政治誤策は、AIを充満してリーマントを決断

データドリブンな政治

データドリブンな政治し、ベータをタンレングな決定

迅速な意思決定

迅速なご自作に政策判断を効率的なる政策決定

事例紹介：シンガポール



NanoClaw ヴィヴィアン外相
NanoClaw（オープンソース）活用
自作AIエージェント業務活用

党首討論の成果



政治家のAI素振りを

「AIを使い倒さなければ
発展はない」
「家庭教師お願いしたい」



AI活用が政治課題に

本日のトピック一覧

- 1. OpenAI Codex Thursday**
— ロック中Macもスマホから操作可能に
- 2. Anthropic Project Glasswing**
— Claudeが重大脆弱性10,000件超を発見
- 3. Cursor SDK + Composer 2.5**
— 独自エージェントをPython/TSで構築
- 4. Gemini Omni**
— フルマルチモーダル、動画をネイティブ編集
- 5. Karpathy: LLM活用は「構造化要求」が9割**
— プロンプトエンジニアリングを徹底的に解説
- 6. Greg Brockman: 'the model alone is no longer the product'**
— 独自の商品を作るために必要な付加価値
- 7. 党首討論：日本のトップにAIを使い倒すよう提言（安野貴博）**
— 党首討論アドバイザーに就任、提言へ

