Tech News Daily

2026-06-29

MORNING DISPATCH / Vibe Coder Bootcamp Tech News

今朝のホットな話題

1. Anthropic 公式が Fable 5 / Mythos 5 の復旧へ ― Mythos 5 は「信頼できる100超機関」に解禁、Fable 5 は来週にも一般復帰の見込み
2. Anthropic 輸出規制の空白をアジア勢が奪う ― 中国 360 が Mythos 対抗「Yitian Tulong（屠龙）」、Sakana の Fugu も export-control-free を前面に
3. npm サプライチェーン攻撃が新段階へ ― worm「Miasma/Hades」が Go 圏へ波及し AIコーディングrepo起点で起動、「Shai Hulud」は8ヶ月・自己増殖の全容 post-mortem

6トピックを整理。

TEKION Group

TEKION Group

Tech News Daily

2026-06-29

1. Anthropic 公式が Fable 5 / Mythos 5 の復旧へ ― Mythos 5 は「信頼できる100超機関」に解禁、Fable 5 は来週にも一般復帰の見込み

Anthropic公式 / Axios

♡ 236

何が起きた？

6/12 以降止まっていた Anthropic の Fable 5 / Mythos 5 について、米政府がアクセス復旧を進めていることを Anthropic が公式に確認。商務省が金曜にまず最強サイバーモデル Mythos 5 を「信頼できる100超の米国機関」へ解禁。Lutnick 商務長官は書簡でリスク対処を認めた。一般ユーザー向け Fable 5 も早ければ来週に復帰する見込み。

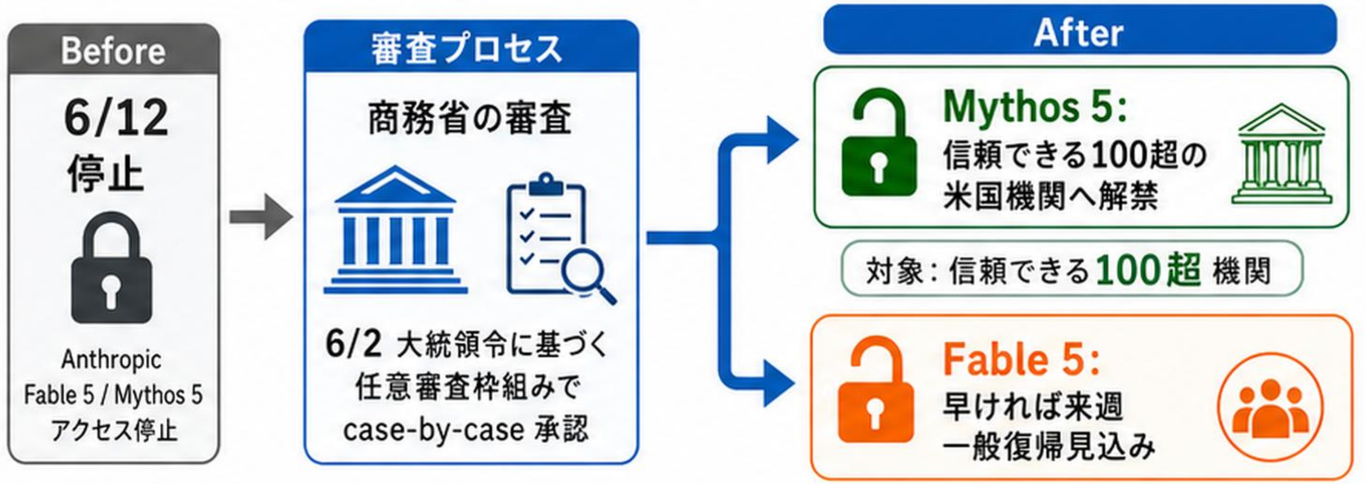
主な変更点

- **Mythos 5:** 商務省が「信頼できる100超の米国機関」限定で解禁。Lutnick 商務長官が「リスクに対処した」と明記
- **Fable 5:** 15日間の停止を経て「早ければ来週」一般復帰の方向。ただし国防総省・NSA の承認は未了
- **背景:** 6/2 大統領令の任意審査枠組みで case-by-case 承認。Hegseth 国防長官が Anthropic を「安全保障上のサプライチェーンリスク」と名指しした対立から雪解け局面

なぜ重要？

- **未確定:** サブスク向け Fable の無料枠が戻るか、追加課金/本人確認付きになるかは未発表
- Anthropic / OpenAI は審査プロセスの制度化を政府に要望中
- 停止の影響で、企業は中国製を含む安価な代替へ乗り換え（GLM 5.2 等）が進んでいた

アクセス復旧の流れ（Before / After）



数字で見るポイント

100超 機関	15日間 停止
6/2 大統領令	6/12 停止

リスク・承認状況

- 国防総省・NSA 承認未了
- 無料枠 / 追加課金 / 本人確認は未発表

市場への影響

- 代替へ乗り換え：GLM 5.2 等
- 代替サービス

x.com/Anthropic/... / axios.com

TEKION Group

2. Anthropic 輸出規制の空白をアジア勢が奪う ― 中国 360 が Mythos 対抗「Yitian Tulong（屠龙）」、Sakana の Fugu も export-control-free を前面に

何が起きた？

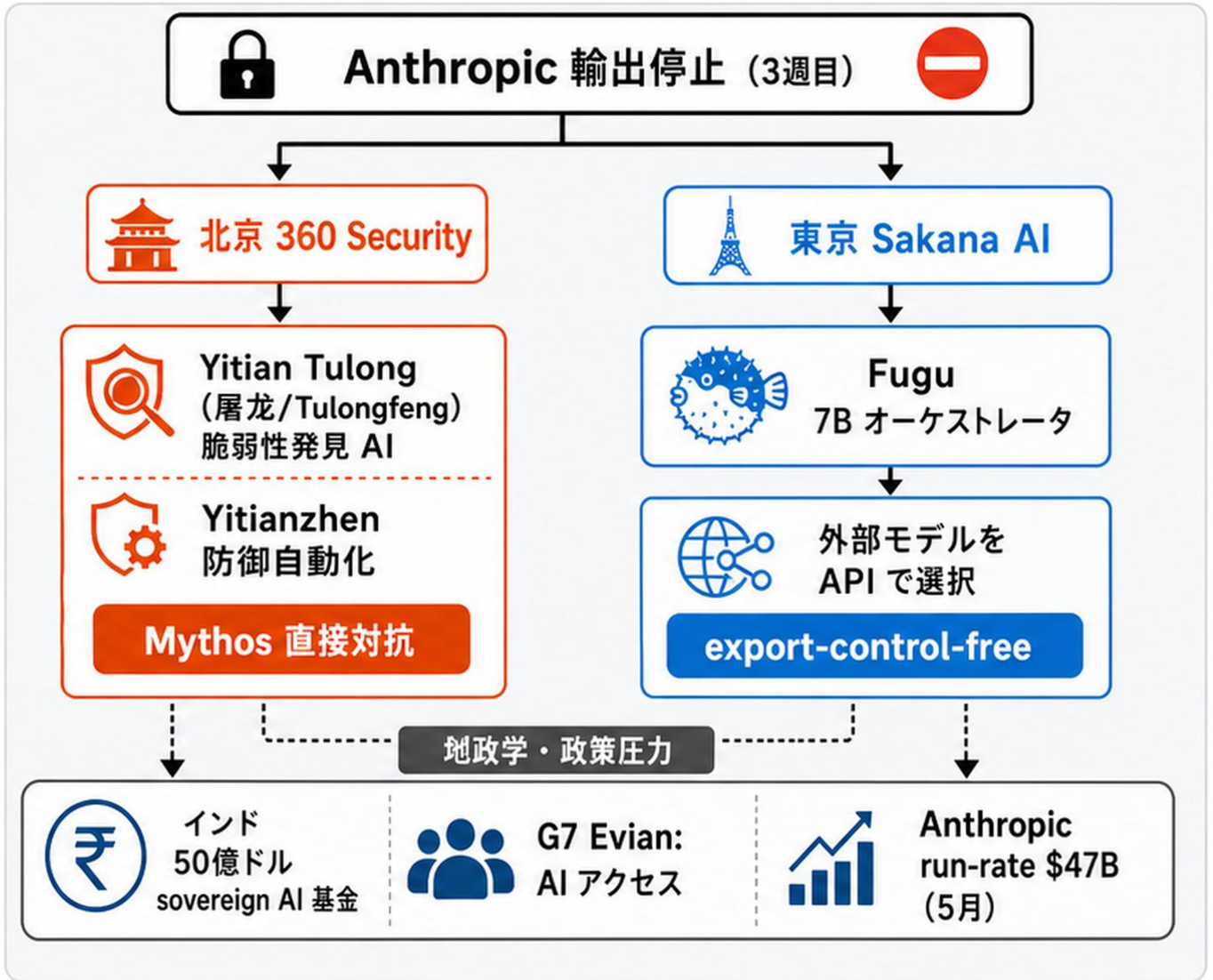
Anthropic の輸出停止が3週目に入る中、アジアの2社が代替を打ち出した。北京の 360 Security は ISC AI 2026 で、Mythos に対抗する脆弱性発見 AI『Yitian Tulong（屠龙/Tulongfeng）』と防御自動化『Yitianzhen』を発表。東京の Sakana AI は外部モデルを束ねる7B オーケストレータ『Fugu』を Fable 5 / Mythos 級と位置づけ、サイトで『輸出規制のリスクなしにフロンティア能力を』と訴求。

主な変更点

- **360（創業者 周鴻禕）：**脆弱性発見 AI を『国家戦略資産』と表現。自国だけが他国ソフトを精査できる『one-way transparency』に警鐘。Mythos 直接対抗を明言。
- **Sakana Fugu:** 新フロンティアを一から訓練せず、タスクに最適な外部モデルを API 経由で選ぶ7B『オーケストレータ』。元 Google 研究者 Llion Jones らが2023設立。
- Sakana は launch timing を『全くの偶然』としつつ、サイトで export-control-free を売りに。Ren Ito は『米モデルは依然重要』と全面置換は否定。

なぜ重要？

地政学: インドは50億ドルのソブリン AI 基金を議論、G7（Evian）でも AI アクセスが主要議題に。Anthropic の run-rate 売上は5月に $47B 到達。アジア企業依存度は非開示だが、停止の隙に現地最適化モデルが空白を埋めつつある。



3. npm サプライチェーン攻撃が新段階へ — worm「Miasma/Hades」がGo 圏へ波及しAIコーディングrepo起点で起動、「Shai Hulud」は8ヶ月・自己増殖の全容 post-mortem

何が起きた？

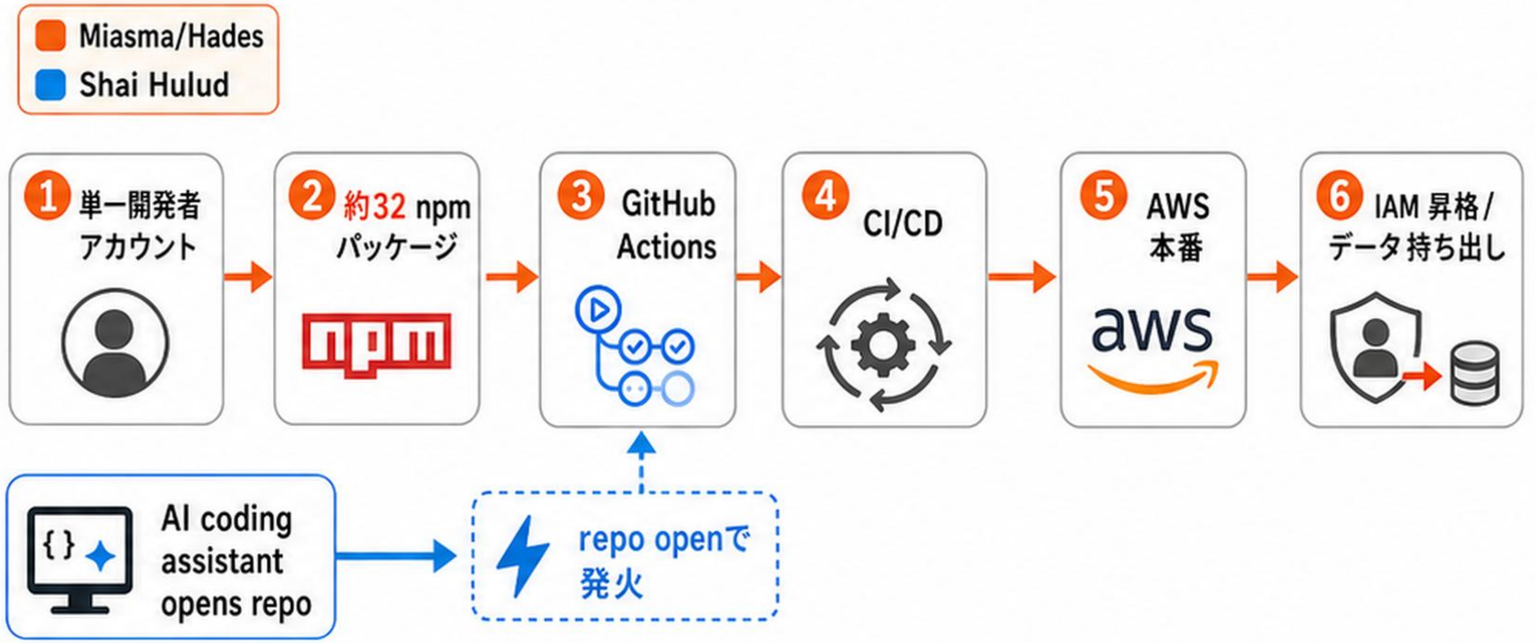
npm を狙うサプライチェーン worm が新フェーズに入った。
「Miasma/Hades」は npm に加え GitHub Actions を侵害して資格情報を収集し、Go エコシステムへ波及。
AI コーディングアシスタントが対象 repo を開いた瞬間にトリガーする挙動が報告されている。

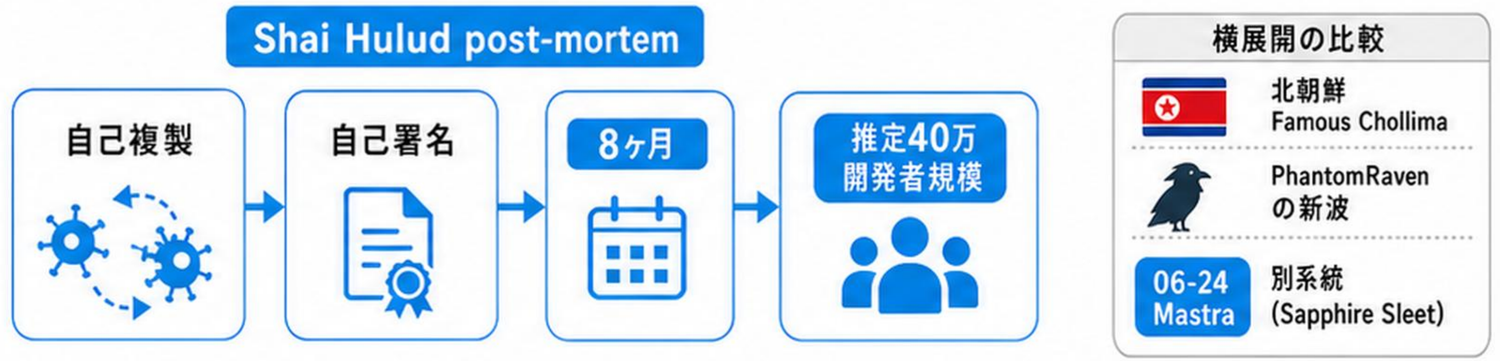
主な変更点

- Miasma/Hades: 単一開発者アカウント経由で約32 npm パッケージを侵害 → GitHub Actions で伝播
- CI/CD から AWS 本番へ橋渡しし IAM 昇格・データ持ち出しの観測も
- 起動トリガー: AI コーディングアシスタントが対象 repo を開くと発火
- Shai Hulud: 自己複製し成果物に自己署名。8ヶ月の長期キャンペーン post-mortem（推定40万開発者規模）
- 横展開: 北朝鮮 Famous Chollima、PhantomRaven の新波、06-24 の Mastra(Sapphire Sleet) とは別系統

なぜ重要？

エージェント前提の開発フローが新たな攻撃面に。依存ツリー監査、lockfile 固定、install スクリプト無効化、資格情報 rotate が必須対応。





4.「リポジトリ全体を毎回読み直す」トークン浪費を断つ MCP サーバ — コードベースをミリ秒で地図化してエージェントへ渡す（MIT・9,900★級）

要点

多くのコーディングエージェントは質問のたびにリポジトリ全体を読み直してトークンを浪費する。これを解消する MCP サーバが注目を集めている。コードベース全体の構造マップをミリ秒で生成してエージェントに渡す。

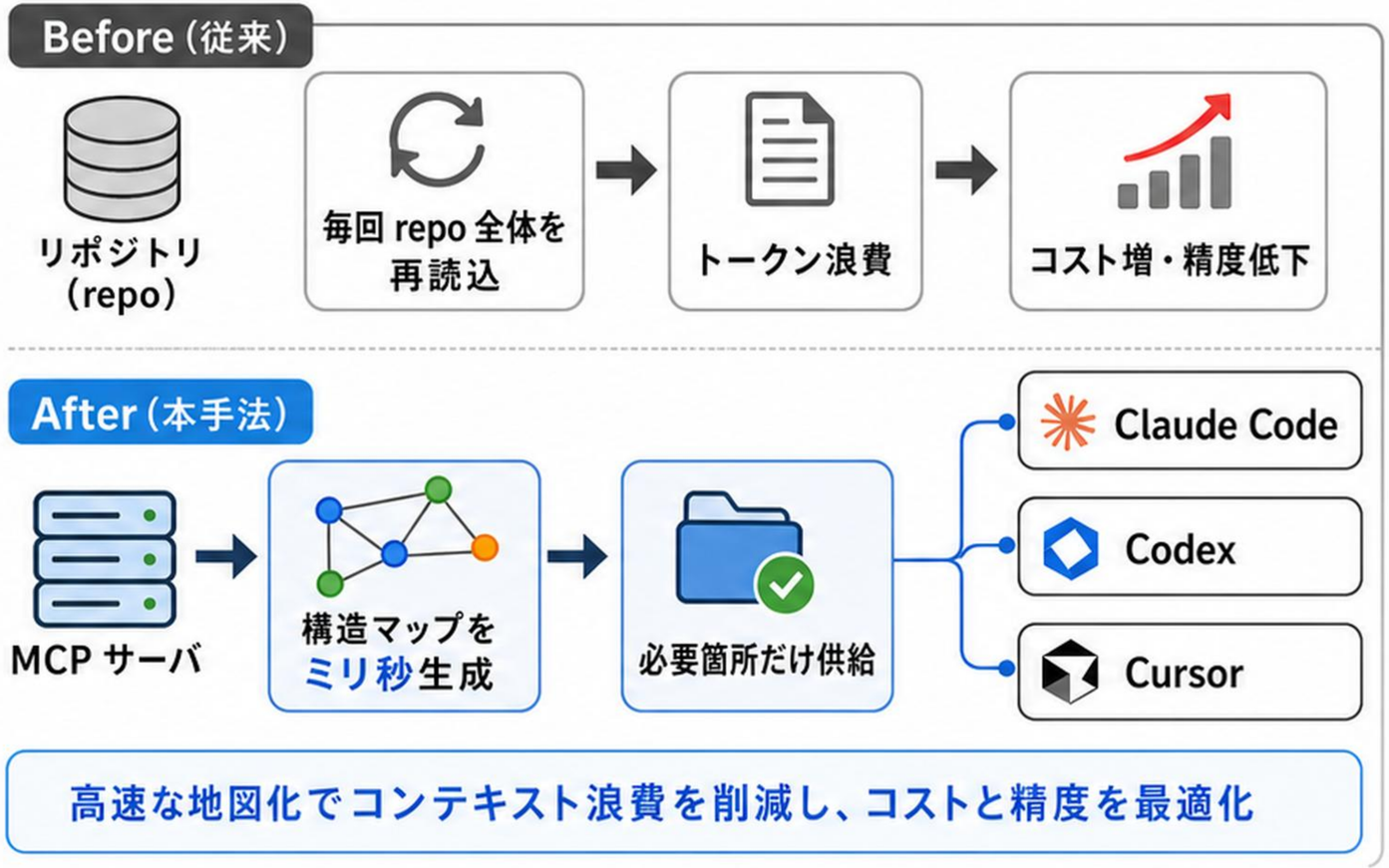
具体的な手法 / 使いどころ

- **課題：**エージェントが毎回 repo 全体を再読込 → コンテキスト浪費とコスト増・精度低下を招く
- **解決：**コードベースを高速に『地図化』し、必要箇所だけをエージェントに供給する MCP サーバ
- **対応：**Claude Code / Codex / Cursor 等の主要エージェントから利用可、OSS（MIT, 約9,900★）

なぜ刺さるか / 学び

フロンティア API がコスト変動・規制で揺れる中、
『手元の効率化でトークンを節約する』実務 Tips。

MIT　約9,900★　ミリ秒



5. オンデバイス LLM が実用速度域に ― OpenBMB「MiniCPM5-1B」が iPhone 17 Pro 上で 66.8 tok/s（Apple Core AI 経由）

何が起きた？

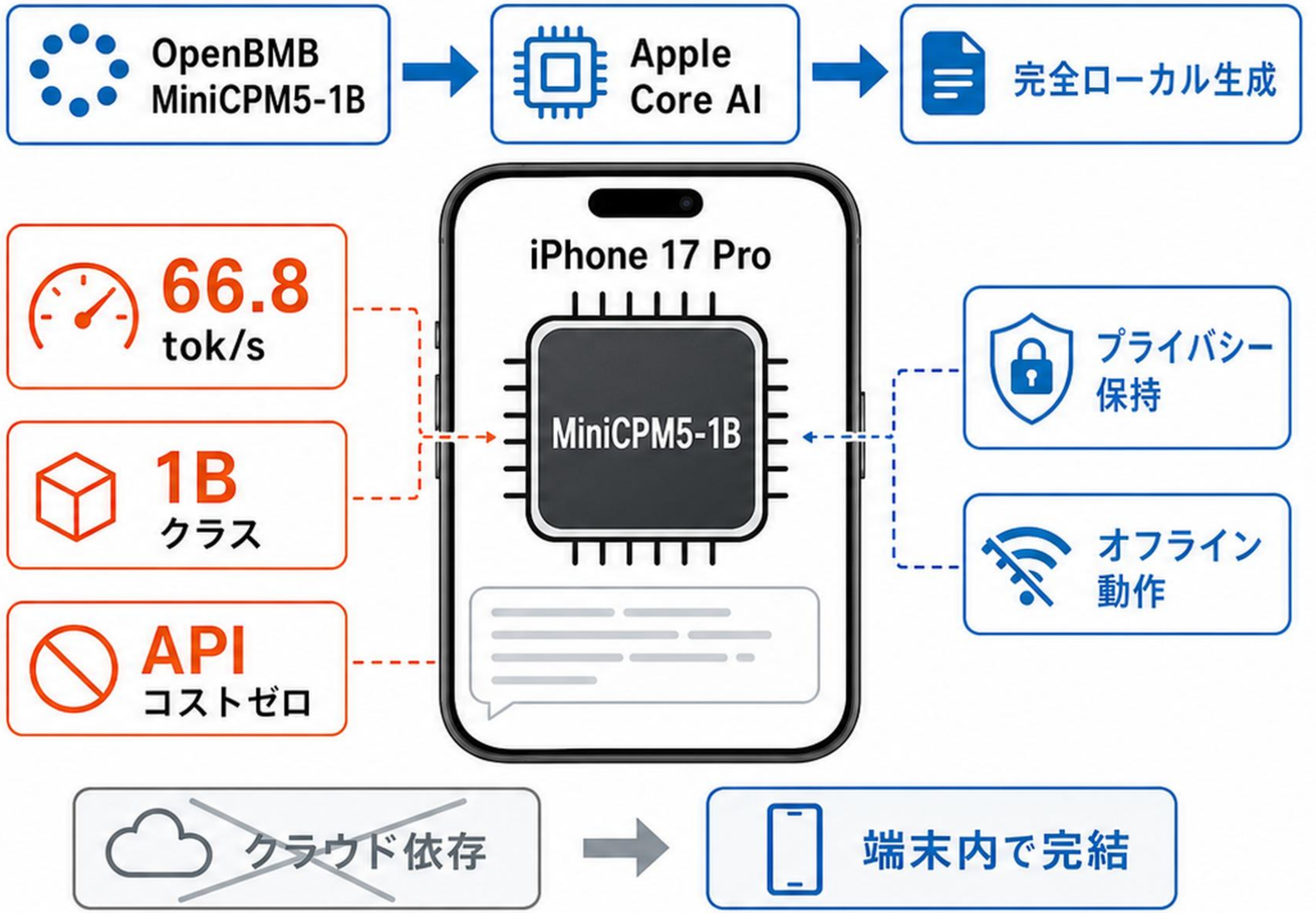
OpenBMB の1Bクラス・オンデバイス特化 LLM『MiniCPM5-1B』が、Apple Core AI 経由で iPhone 17 Pro 上で完全ローカル動作し、66.8 tok/s を記録したと実機報告。

主な変更点

- **モデル：** OpenBMB MiniCPM5-1B（1Bクラス、on-device SOTA を主張）
- **速度：** iPhone 17 Pro で 66.8 tok/s、完全ローカル（Apple Core AI 経由）
- **意味：** 端末内で完結＝プライバシー保持・オフライン動作・API コストゼロ
- **文脈：** フロンティアが規制/コストで揺れる中、エッジ/オンデバイスの実用度が着実に上昇

なぜ重要？

クラウド非依存・低コストで動く小型モデルが、スマホ単体で実用的な生成速度に達しつつある。



6. オープンソースの MCP ペンテスト基盤「HexStrike AI」公開 — 150超のセキュリティツールを AI から自動オーケストレーション

🔎 何が起きた？

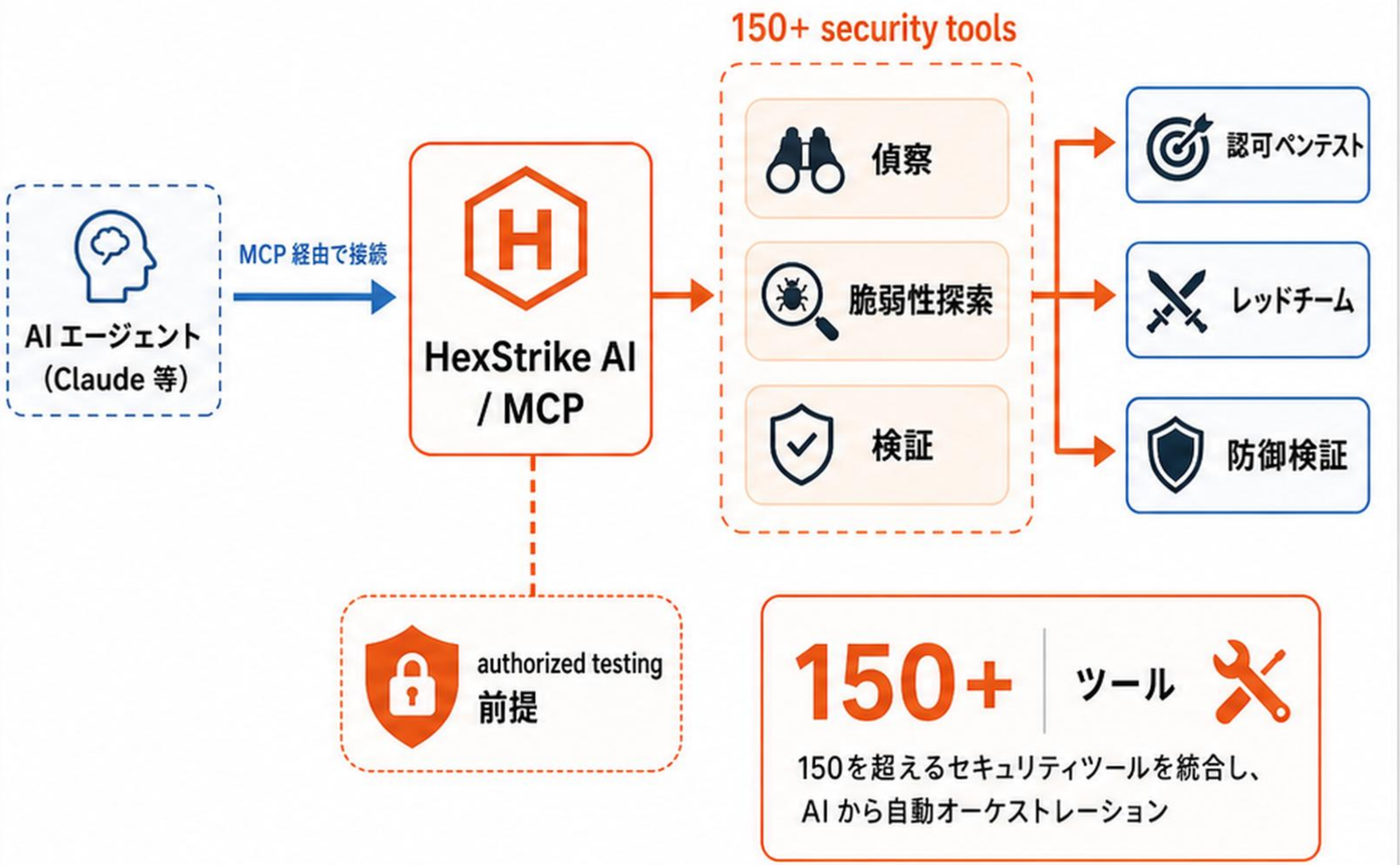
150を超えるセキュリティツールを束ね、AI から自動で
ペネトレーションテストを駆動するオープンソースの MCP 基盤
「HexStrike AI」が公開された。Claude などの AI エージェントを
MCP 経由で接続し、偵察・脆弱性探索・検証のワークフローを
自動化する、認可されたレッドチーム/防御向けプラットフォーム。

📌 主な変更点

- **中身:** 150+ のセキュリティツールを統合した
  OSS の MCP サイバーセキュリティ自動化基盤
- **接続:** AI エージェント（Claude 等）を MCP 経由でつなぎ、
  ツール群をオーケストレーション
- **用途:** 認可された範囲でのペンテスト/レッドチーム・
  脆弱性探索の自動化（authorized testing 前提）
- **文脈:** 攻撃側（topic 3 の worm 等）が高度化する中、
  防御/検証側でも AI×MCP の自動化が進む

💡 なぜ重要？

攻撃側の自動化に対抗するため、防御・検証側も AI と MCP で
ツール実行をつなぎ、調査から検証までを高速化する流れを
示している。



github.com/0x4m4/hexstrike-ai

本日のトピック一覧

1. Anthropic 公式が Fable 5 / Mythos 5 の復旧へ ―

Mythos 5 は「信頼できる100超機関」に解禁、Fable 5 は来週にも一般復帰の見込み

2. Anthropic 輸出規制の空白をアジア勢が奪う ―

中国 360 が Mythos 対抗「Yitian Tulong（屠龙）」、
Sakana の Fugu も export-control-free を前面に

3. npm サプライチェーン攻撃が新段階へ ―

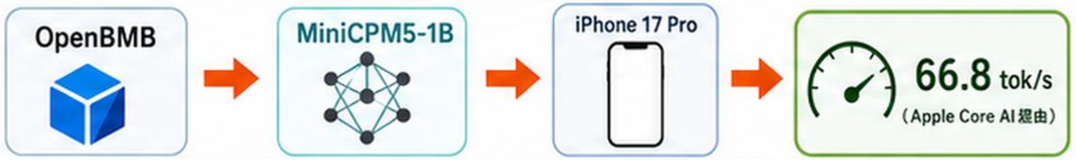
worm「Miasma/Hades」が Go 圏へ波及しAIコーディングrepo起点で起動、
「Shai Hulud」は8ヶ月・自己増殖の全容 post-mortem

4.「リポジトリ全体を毎回読み直す」トークン浪費を断つ

MCP サーバ ― コードベースをミリ秒で地図化して
エージェントへ渡す（MIT・9,900★級）

5. オンデバイス LLM が実用速度域に ―

OpenBMB「MiniCPM5-1B」が iPhone 17 Pro 上で
66.8 tok/s（Apple Core AI 経由）



6. オープンソースの MCP ペンテスト基盤「HexStrike AI」公開 ―

150超のセキュリティツールを AI から自動オーケストレーション

Sources: OpenAI | Anthropic | Google

TEKION Group