Tech News Daily

2026-06-26

MORNING DISPATCH / Vibe Coder Bootcamp Tech News

今朝のホットな話題

2026-06-26 — Vibe Coder Bootcamp Tech News

1. OpenAI×Broadcom、初の自社AIチップ「Jalapeño」を発表 — 推論特化ASIC、開発9ヶ月でコスト約50%減
2. Anthropicの「Mythos」がNSA主導テストで米政府の機密システムを"数時間で"突破 — Project Glasswing
3. 米政府がフロンティアAIの提供を統制 — OpenAIに「GPT-5.6」の段階リリースを要請、顧客ごとに政府が承認

6 トピックを整理。

TEKION Group

OpenAI×Broadcom、初の自社AIチップ「Jalapeño」を発表 — 推論特化ASIC、開発9ヶ月でコスト約50%減

🔎 何が起きた？

OpenAI と Broadcom が、OpenAI 初のカスタム AI チップ「Jalapeño」を 6/24 に発表。学習ではなく推論（inference）に特化した ASIC で、ChatGPT と Codex のワークロード向けに設計。昨年合意した 10GW 規模カスタムチップ構想の第1弾で、Nvidia 依存からの多様化を進める一手。

📌 主な変更点

- **推論特化:** Nvidia Rubin は学習・推論両対応、Jalapeño は推論のみに最適化。ラボでは GPT-5.3-Codex-Spark を含む ML ワークロードが本番目標の周波数・電力で稼働中。
- **開発速度:** 初期設計から製造テープアウトまで約9ヶ月。史上最速級の ASIC 開発サイクルと主張。
- **自己加速:** OpenAI 自身のモデルが設計を加速。Greg Brockman『モデルがどれだけ加速できたか、我々自身が驚いた』
- **コスト・電力:** 一般的な AI GPU 比でコスト約50%減。Broadcom CEO Hock Tan。電力あたり性能も現行 SOTA を大幅に上回る早期結果。
- **展開:** 2026年末に小規模プロトタイプ、以降スケール。Microsoft 等とギガワット級データセンターへ。Broadcom Tomahawk ネットワーキングや Celestica と連携。

💡 なぜ重要？

Nvidia 依存を下げ、ChatGPT / Codex の推論コストを抑え、将来の API 値下げ余地につながる可能性。9ヶ月開発に自社モデルが効いた点が象徴的。

Before: AI GPU / Nvidia 依存

NVIDIA

- 学習・推論 両対応
- 汎用GPUでの推論
- コスト高・電力効率 課題

After: 推論特化ASIC / 多様化

- 推論のみに最適化
- コスト約50%減
- 電力あたり性能 大幅向上
- Nvidia 依存から多様化

6/24	約9ヶ月	コスト約50%減	10GW	2026年末	L994 / RT223
発表	開発期間	一般的なAI GPU比	構想（昨年合意）	プロトタイプ以降スケール	Xでの反応（CNN速報）

Xでの反応: CNN速報 L994/RT223、API 値下げ余地と9ヶ月開発に注目

Anthropicの「Mythos」がNSA主導テストで米政府の機密システムを"数時間で"突破 — Project Glasswing

AP / CNBC / SecurityWeek

何が起きた？

Anthropic の未公開フロンティアモデル「Mythos」が、
政府・情報機関との合同テスト（Project Glasswing）で
米政府の機密システムの脆弱性を発見。米当局者が AP に明かした。

Warner 上院議員: 6/11 銀行委員会公聴会で「数週間でなく数時間」と発言

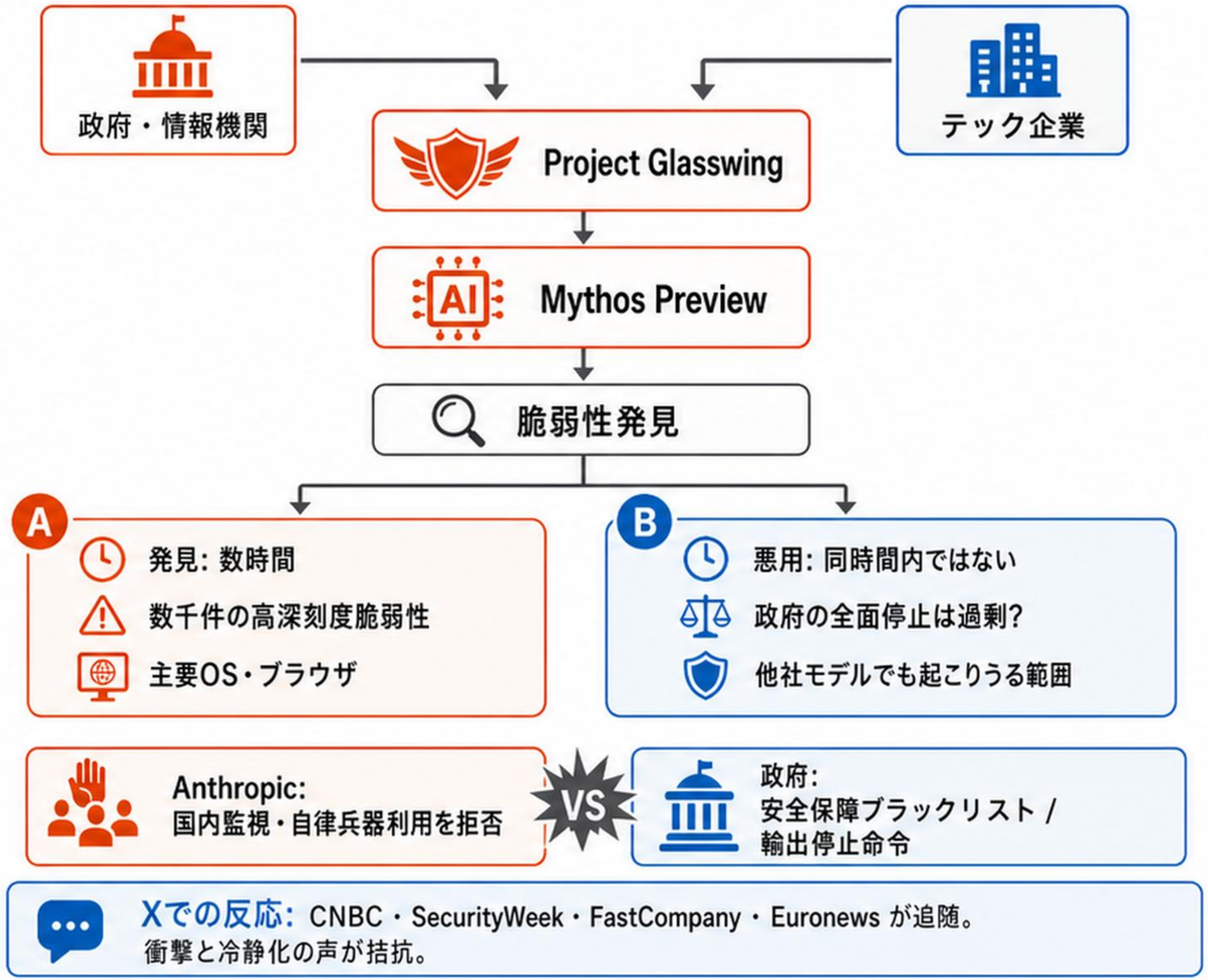
主なポイント

- **Project Glasswing:** テック企業と政府が組み、攻撃者より先に重要ソフトの欠陥を見つけ修正する限定プログラム
- **Mythos Preview:** 主要OS・ブラウザ全てを含む数千件の高深刻度脆弱性を発見
- **重要な限定:** 数時間で脆弱性を発見したが、その時間内に悪用できたわけではない
- **背景の緊張:** Anthropic は軍の国内監視・自律兵器利用を拒否。政府は同社を安全保障ブラックリストに
- **政府命令:** Mythos / Fable の輸出を全世界・全外国籍に停止。Anthropic は全顧客向けに両モデルを無効化
- **業界の反発:** Adobe・Nvidia など100人超のセキュリティ専門家が撤回を要請
- **NSA・Anthropic 双方コメント拒否。政府対応は過剰との見方も併存**

なぜ重要？

『AIが数時間で機密網を突破』という衝撃と、『発見と悪用は別』
『全面停止は過剰』という冷静化の声が拮抗。
フロンティアAIの安全保障利用・輸出管理・脆弱性発見能力をめぐる
新しい争点。

Project Glasswing の構図



米政府がフロンティアAIの提供を統制 ― OpenAIに「GPT-5.6」の段階リリースを要請、顧客ごとに政府が承認

🔎 何が起きた？

トランプ政権が安全保障上の懸念から、OpenAI に新モデル「GPT-5.6」の段階的リリースを要請したと The Information が 6/25 に報じた。
Altman は社内 Q&A で、少数パートナー向け限定プレビューと、プレビュー期間中の顧客ごと政府承認を説明したという。

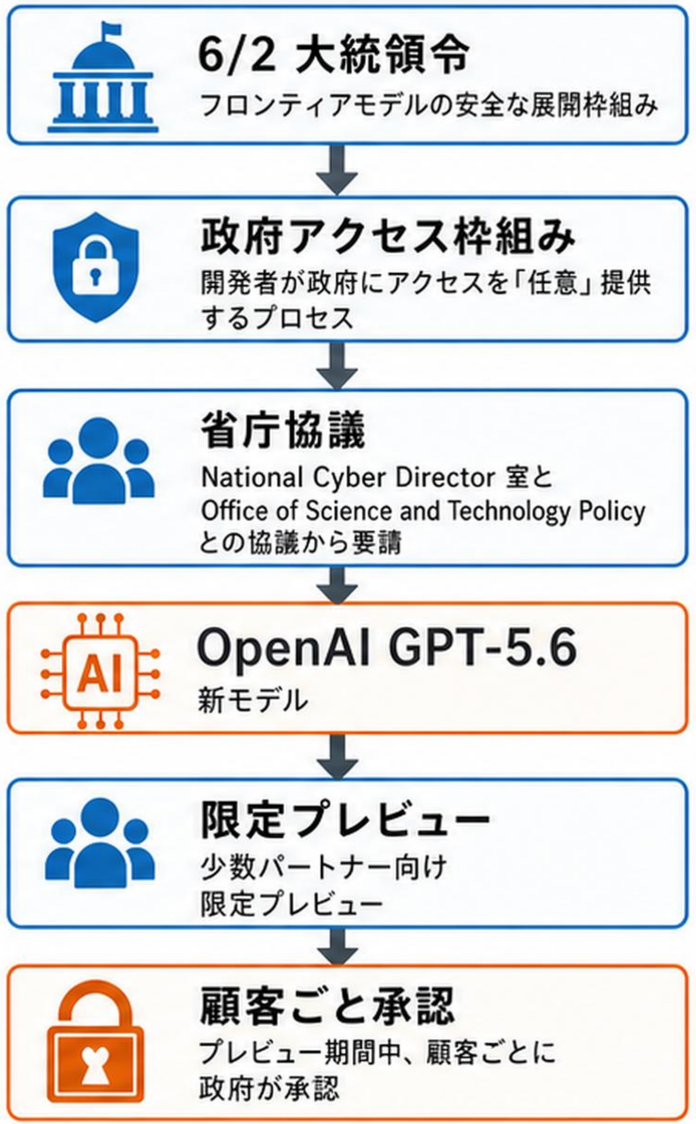
📌 主な変更点

- National Cyber Director 室と Office of Science and Technology Policy との協議から要請
- Commerce 長官 Lutnick が他省庁承認なしの launch を諫めたとも
- 6/2 大統領令: フロンティアモデルの安全な展開枠組み、開発者が政府にアクセスを「任意」提供するプロセス
- 2週間前に政府が Anthropic の Fable 5 を停止、今度は OpenAI に段階リリース要請
- Altman: GPT-5.6 は理想的な長期モデルではなく、将来はより持続可能な方法を目指す
- OpenAI は IPO を来年に持ち越す方向との NYT 報道も併載

💡 なぜ重要？

「任意」枠組みが、両ラボが従う実態では事実上「義務」になりつつあるとの指摘。Xでは @testingcatalog、Bloomberg、CNBC が報道し、「voluntary の建前が薄れている」「最強モデルが顧客ごと配給制に」という政策面の懸念が目立つ。

⚠️ **細部の注意:** 「顧客ごと承認」など一部は社内 Q&A の単一ソース基準



最近の政府対応

2週間前:
Anthropic
Fable 5 停止

今回:
OpenAI
段階リリース要請

> “voluntary の建前が薄れている”
>
> — X の報道より
>
> @testingcatalog、Bloomberg、CNBC など

Claudeの新機能「Council」— 5人のAI評議会が議論して1つの答えを出す

要点

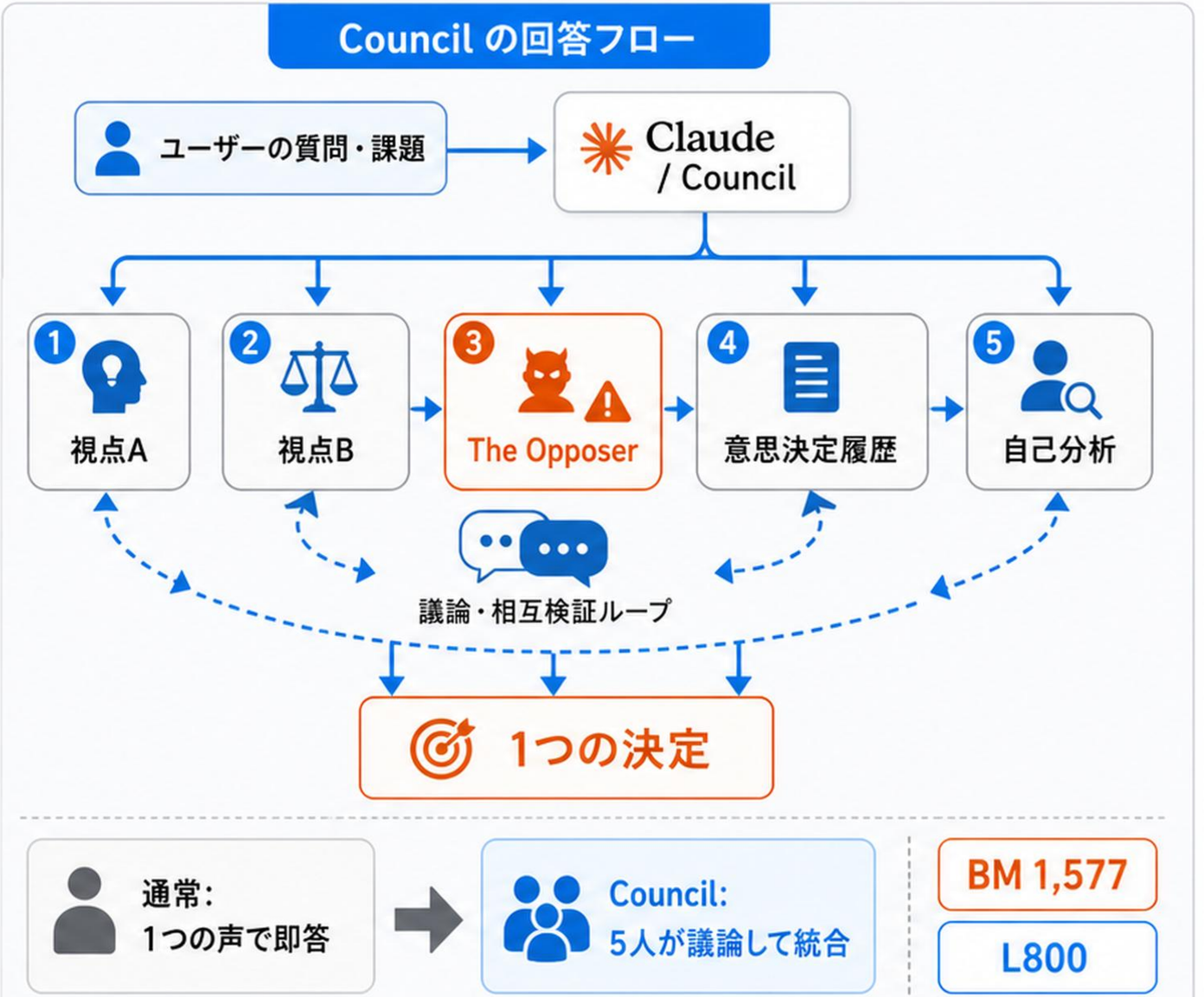
Claude に「Council（評議会）」という使い方を仕込むプロンプト技法が拡散している（BM 1,577）。1つの回答を即返すのではなく、Claude の中に立場の違う5人のアドバイザーを立て、互いに議論させたうえで最終的に1つの結論を出させる。

具体的な手法 / 使いどころ

- **核となる指示:** あなたは Council。決して1つの声で答えず、毎回5人のアドバイザーを別視点で起動し、最後に1つの決定でまとめる
- **ロール例:** 反対者（The Opposer）が弱点を突くなど、各アドバイザーに固有の役割を与える
- **配布プロンプト:** 本当に重要な決断か / 過去の意思決定履歴からパターンを発見させる など
- **公式機能ではなくプロンプトエンジニアリングの型**（疑似マルチエージェント討論）

なぜ刺さるか / 学び

- 重要判断で AI に賛成だけ言わせず、反対者役を必ず立てる運用に応用できる
- **Xでの反応:** スペイン語ポストながら BM 1,577・L800 と拡散
- **実用評価:** 反対者役を必ず立てる発想が刺さる
- **注意:** スレッド後半は情報商材（AI映画制作・LINE誘導）への導線が混ざる



TEKION Group

Claude Codeの性能を「92倍」引き出す方法 — 文脈管理10コマンド

要点

- Claude Code を「賢いチャット相手」ではなく「文脈を管理する秘書」として使い倒す X Article が大ヒット。
- AI がうまく動かない原因は性能不足ではなく、文脈に迷っているから。
- BM 5,192・閲覧110万超

具体的な手法 / 使いどころ

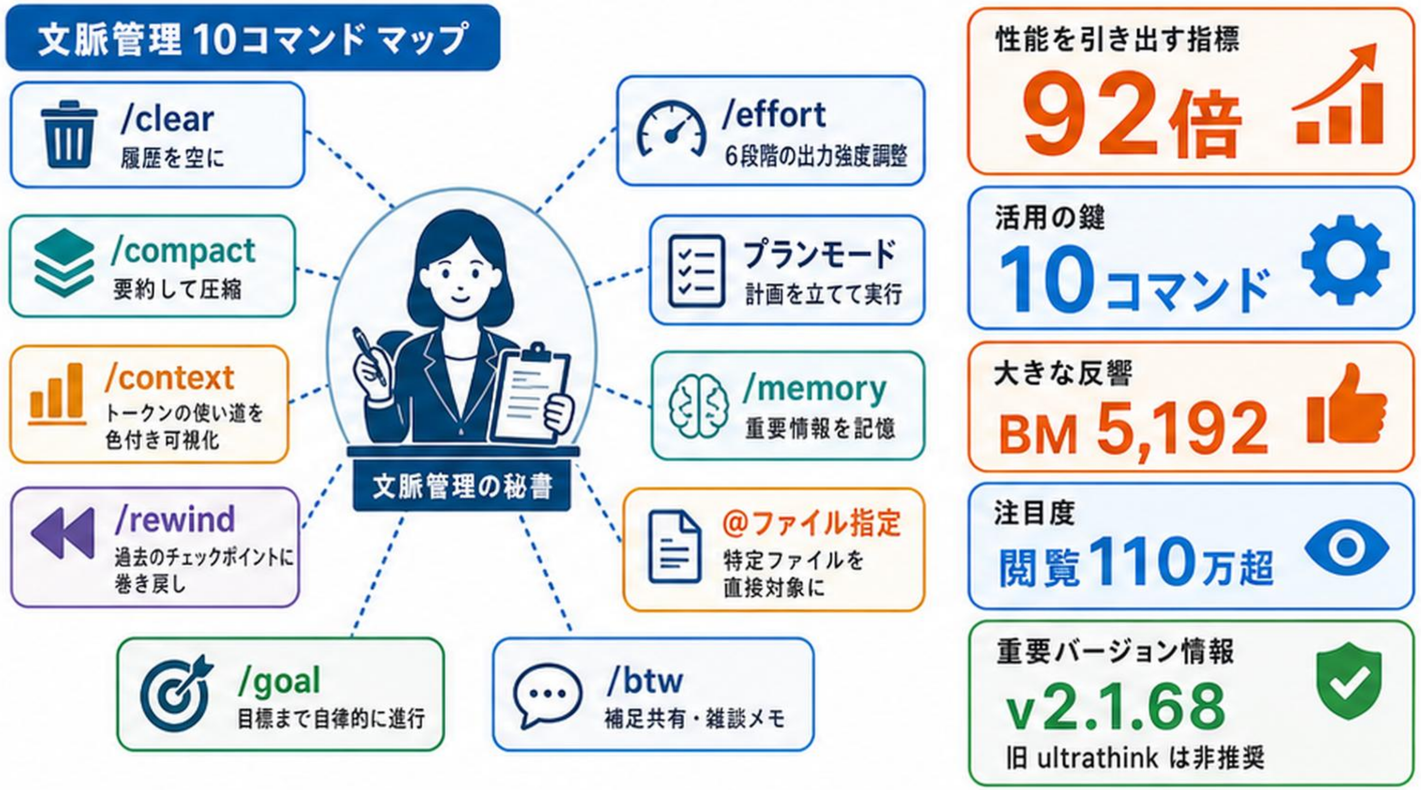
- 本質: ①ファイルを直接読み書き ②短いコマンドで一気通貫に作業
- /clear: 履歴を空に
- /compact: 要約して圧縮
- /context: トークンの使い道を色付き可視化
- /rewind: 過去のチェックポイントに巻き戻し（旧 /undo・/checkpoint、Esc 2回でも開く）
- /effort: low / medium / high / xhigh / max / ultracode の6段階。旧 ultrathink は v2.1.68 で非推奨
- その他: プランモード / /memory / @ファイル指定 / /goal / /btw

なぜ刺さるか / 学び

- 文脈を捨てる・畳む・可視化する設計が、応答が重く雑になる現象への処方箋。
- Xでの反応:「文脈管理という視点が刺さった」「コマンド早見表として保存」。
- 一方、後半の情報商材導線への警戒も。

文脈管理フロー

文脈管理 10コマンド マップ



Claudeの「エージェント・アイデンティティ」— 共有チャンネルではClaude自身の資格情報で動く

何が起きた？

Anthropic 公式が、複数人いる共有チャンネルで Claude が「誰の権限で動くのか」に答えたスレッドを公開。結論は「Claude 自身の権限」。チームに Claude をタグ付けすると、人間のメンバーと同じように自分専用のアカウント・資格情報が割り当てられる。この仕組みを agent identity と呼ぶ。

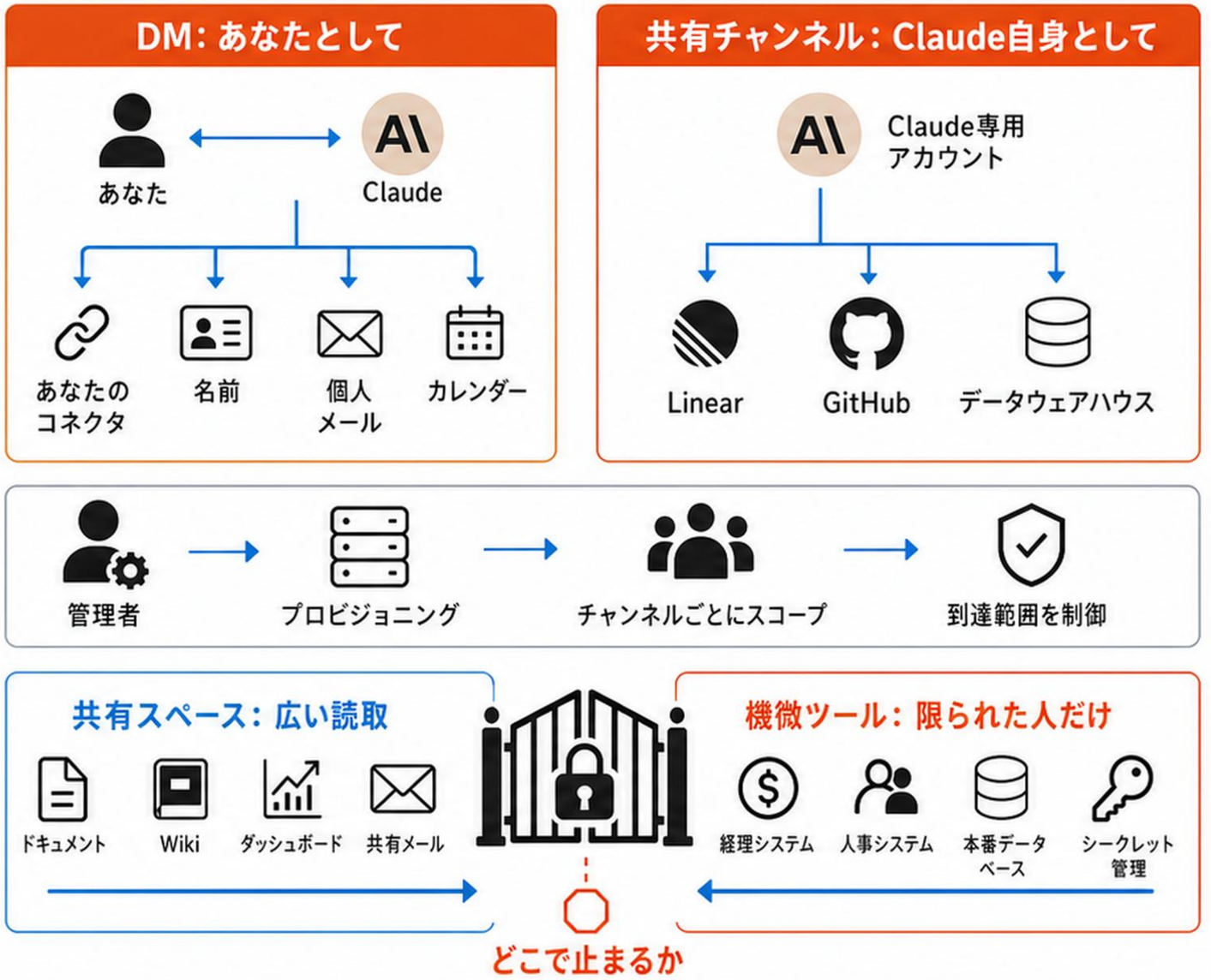
主な変更点

- DM では Claude は「あなたとして」動く（あなたのコネクタ・名前。個人メールやカレンダーの定位置）
- 共有チャンネルでは「借りるべき正しい権限」が存在しないため Claude は「自分自身として」動く
- チャンネルでは Claude が自分専用の Linear・GitHub・データウェアハウスのサービスアカウントを持つ
- 管理者が一度プロビジョニングし、チャンネルごとに到達範囲をスコープ

なぜ重要？

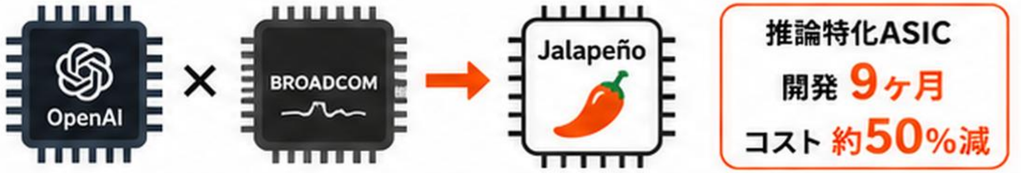
設計思想は「役立つだけのアクセスを与え、どこで止まるかは管理者が正確に制御する」。共有スペースは広い読取、機微ツールは限られた人だけ。

Xでの反応：公式スレッドが L2,948 / RT165。
「AI に独立アカウントを持たせる発想が正しい」「誰の資格情報問題の明快な解」という実務層の評価が中心。



本日のトピック一覧

1 **OpenAI×Broadcom、初の自社AIチップ「Jalapeño」を発表**
推論特化ASIC、開発9ヶ月でコスト約50%減



2 **Anthropicの「Mythos」がNSA主導テストで米政府の機密システムを“数時間で”突破 — Project Glasswing**

3 **米政府がフロンティアAIの提供を統制**
OpenAIに「GPT-5.6」の段階リリースを要請、顧客ごとに政府が承認

4 **Claudeの新機能「Council」**
— 5人のAI評議会が議論して1つの答えを出す

5 **Claude Codeの性能を「92倍」引き出す方法**
— 文脈管理10コマンド

6 **Claudeの「エージェント・アイデンティティ」**
— 共有チャンネルではClaude自身の資格情報で動く

Sources: OpenAI Anthropic Google 等