MORNING DISPATCH

2026-11-04

1. Anthropic、上場申請書類の修正版で7〜9月期の売上170億ドルを開示…
2. Claude にログインするだけで MCP サーバーに自動接続する「auto-connect…
3. Claude Code 2.1.317、アカウントのメールアドレスをネットに送る操作の前に確認…

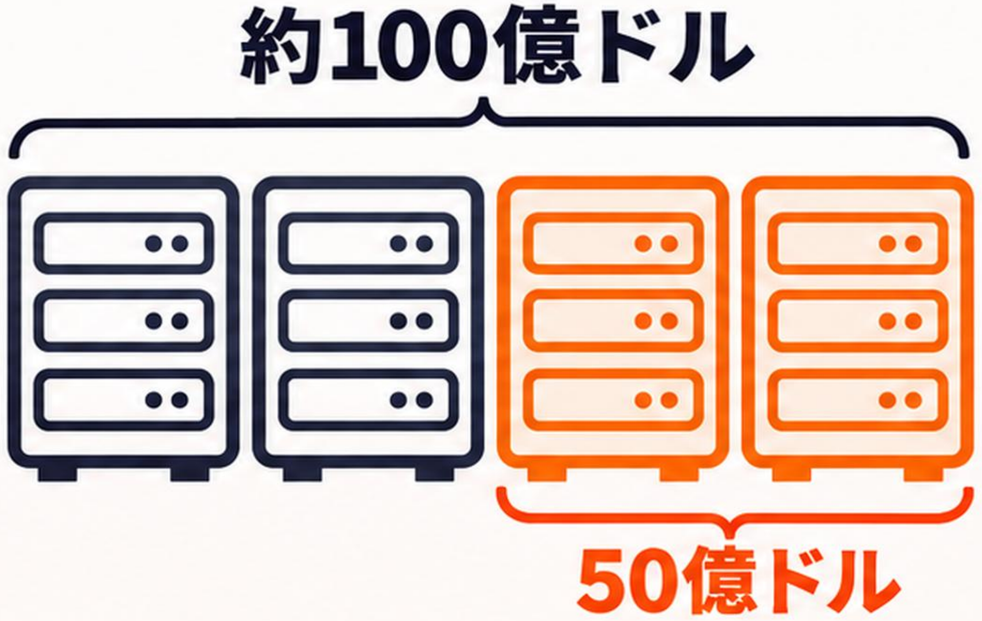
注目3件

TEKION Group

Anthropic、上場申請書類の修正版で7〜9月期の売上170億ドルを開示…

Anthropic が11月2日（米国時間）に提出した上場申請書類の修正版（S-1/A）で、9月30日までの四半期の業績が新たに開示されました。

- 四半期の計算資源の費用は約100億ドル。そのうち50億ドルは短期契約で調達した分で…
- 計算資源1ドルあたりの売上は、前の四半期の2倍強から1.72倍に下がった。需要に追いつくため…
- TechCrunch によると、SpaceX に月12.5億ドルを計算資源の代金として払っているほか、Nscale・Akamai・Volta…



Claude の需要の伸びに計算資源の調達が追いつかず、高い短期契約で埋めている様子が数字で見えました。

techcrunch.com

Claude にログインするだけで MCP サーバーに自動接続する「auto-connect」がベータに…

Claude にログインすると、Claude を信頼できる発行元として受け入れる MCP サーバーのプラグインに、メンバーが一人ずつ認可しなくても自動でつながる「auto-connect」がベータになりました。

- 対象は Claude Team / Enterprise で、Claude の管理者が有効にする。Supabase 側は SSO を設定済みの Team /…
- Claude は「組織の現メンバーか」と「Claude アカウントのメールアドレス」を確かめて…
- IdP でのサインインや多要素認証は確かめない。IdP でメンバーを無効にしてもアクセスは止まらないので…

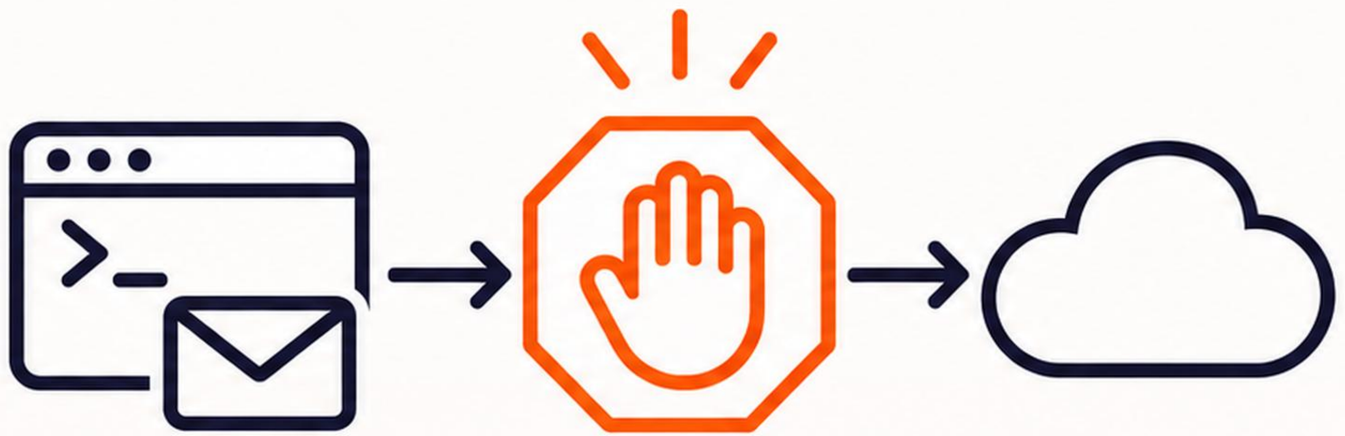


社内で MCP を使うときの「メンバー一人ひとりが接続して認可する」手間がなくなります。

Claude Code 2.1.317、アカウントのメールアドレスをネットに送る操作の前に確認…

Claude Code 2.1.317 では、Web やシェルのツール呼び出しが自分のアカウントのメールアドレスをネットワークに送ろうとすると、実行前に確認を求めるようになりました。

- Agent SDK のフックのコールバックに `onFailure: "block" を追加。コールバックが失敗したら…
- Claude apps gateway の管理 API に、過去の支出を期間ごとに合計・開発者別・日別・IdP グループ別で読める…
- OTel のメトリクス・イベント・スパンに `anthropic.plan`、`anthropic.seat_type`、`anthropic.provider`…



エージェントが知らないうちに個人の情報を外へ送る、余計な接続を付けたまま予約タスクが動く、といった事故を防ぐ方向の変更です。

github.com

TEKION Group

Vercel Security Review がパブリックベータ。push のたびに AI が脆弱性をレビューし…

Vercel が、接続した GitHub リポジトリへの push のたびにコードの脆弱性を自動でレビューする「Security Review」を、Pro / Enterprise 向けにパブリックベータで公開しました。

- プルリクエストではなく push をきっかけに動くので、本番ブランチへの直接の push や force push…
- コミットごとに GitHub のチェックを追加し、プルリクエストがあればレビューコメントで指摘する…
- 「Fix with Vercel Agent」で修正のプルリクエストを作る（承認するまでマージされない）。CLI 65.10.0 以降の…



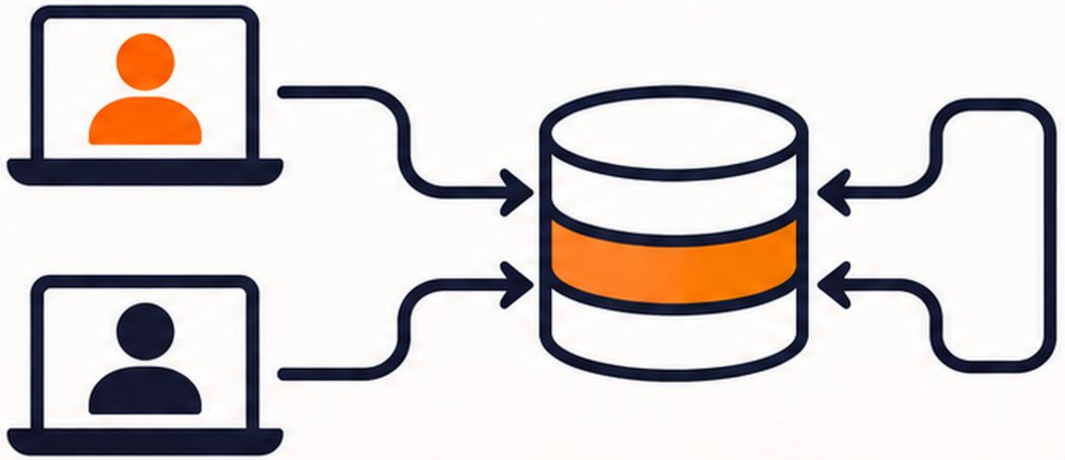
AI によるセキュリティレビューが、デプロイ基盤の機能として push のたびに走る形になりました。

vercel.com

Next.js 16.4.5 / 15.5.29、`'use cache'` でほかの利用者のデータが見えてしまう問題など…

Next.js がセキュリティ修正版の 16.4.5 と 15.5.29 を公開しました。

- 16.4.5 だけの4件はキャッシュ関連。
  `unstable_cache` 経由で呼んだ `'use cache'` …
- 16.4.5 と 15.5.29 の両方で直った3件:
  セルフホストで取得したレスポンスをそのまま返すと
  別のクライアントに….
- 深刻度はすべて Moderate。各アドバイザリの詳細は
  リリースノートからたどれる



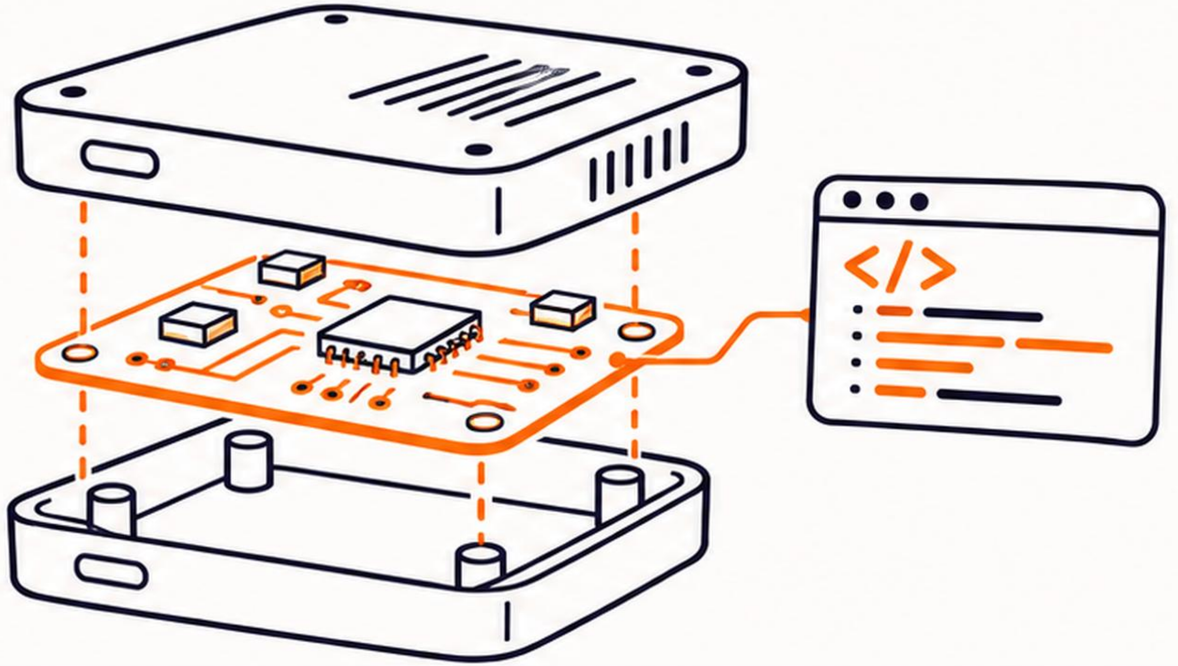
**Cache Components や `'use cache'` を使っている 16 系のアプリは、
ログインした利用者ごとに違うデータを返す画面でキャッシュが混ざると情報漏えいになります。**

github.com

OpenAI、GPT-6 Astra が人の手で直さずに筐体・基板・ファームウェアまで設計した試作機を…

OpenAI が、機械設計・電気設計・シミュレーションなど、物をつくるエンジニアリングでのモデルの活用状況を公開しました。

- 試作機は2人が副業的に1週間足らずで設計し、委託先の工場が1か月足らずで少数を製造した
- 量産に向けては、工場の製造上の制約や公差、組み立てに必要な細部を Astra が十分に考慮できず…
- 社内のハードウェア部門でのモデル利用（トークン量）は2月から23倍。CAD モデルの作成・修正、製造図面…

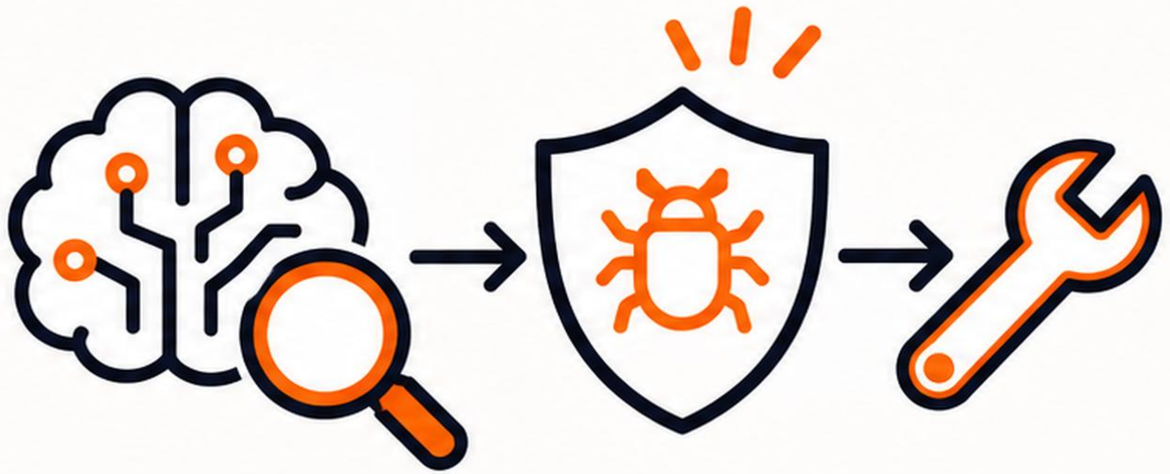


コーディングエージェントの次の対象が、CAD やシミュレーションのような専門ソフトを使う物づくりに広がりつつあります。

OpenAI、外部の研究者と組んで次の社内セキュリティ集中期間を計画…

OpenAI が、自社のモデルを使って自社システムの弱点を探して直す、社内のセキュリティ集中期間（セキュリティスプリント）を再び行うと発表しました。

- 前回のスプリントでは、プロダクトエンジニアの25%を弱点探しと修正に充てた。Codex で指摘を調べ…
- 報奨金は、中・高・重大の報酬帯の中央値を平均で4倍以上に引き上げ。ChatGPT・Codex・API Platform…
- 防御側向けの「Daybreak」で最も高性能なモデルを提供し、重要インフラを守る人たち向けに6か月で10億ドル分の…



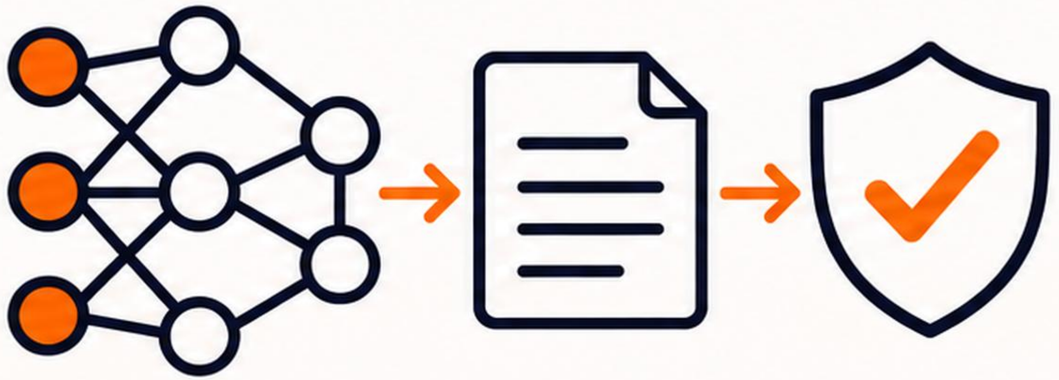
AI で脆弱性が見つかる速さが上がる中、攻撃者より先に自分のシステムに AI を当てて穴を探す、という考え方を OpenAI 自身が人員の規模で実行している例です。

openai.com

Anthropic、AIの応答が「本当にそのモデルから出たか」を暗号で証明する「FlashProve…

Anthropicが、利用者が受け取った応答が、開発者がうたう特定のモデルから本当に生成されたものかを確かめられる仕組み「FlashProve」を、研究の途中経過として公開しました。

- 4bit量子化した400BパラメータのLlama 4 Maverickで、H100 1枚あたり約110トークン/秒で証明を作れる…
- それでも、モデルをvLLMで動かすときのGPU時間の約70〜95倍かかる。検証する側は、重みを持たずに普通の…
- Claudeが設計した部分は判断の良し悪しを評価しにくいため、安全性の主張を形式検証言語Lean…



APIの向こうで本当にどのモデルが動いているかを、提供元を信じるのではなく証明で確かめる方向の研究です。

anthropic.com

本日のトピック一覧

1. Anthropic、上場申請書類の修正版で7〜9月期の売上170億ドルを開示…
2. Claude にログインするだけで MCP サーバーに自動接続する「auto-connect…
3. Claude Code 2.1.317、アカウントのメールアドレスをネットに送る操作の前に確認…
4. Vercel Security Review がパブリックベータ。push のたびに AI…
5. Next.js 16.4.5 / 15.5.29、`'use cache'` でほかの利用者のデータが見えてしまう…
6. OpenAI、GPT-6 Astra が人の手で直さずに筐体・基板…
7. OpenAI、外部の研究者と組んで次の社内セキュリティ集中期間を計画…
8. Anthropic、AI の応答が「本当にそのモデルから出たか…

2026-11-04