MORNING DISPATCH

2026-10-26

Claude Code、Monitorが全経路で利用可能に

Cloudflare、Brotli脆弱性にWAF規則

英国、AIで生物の脅威に備える研究所

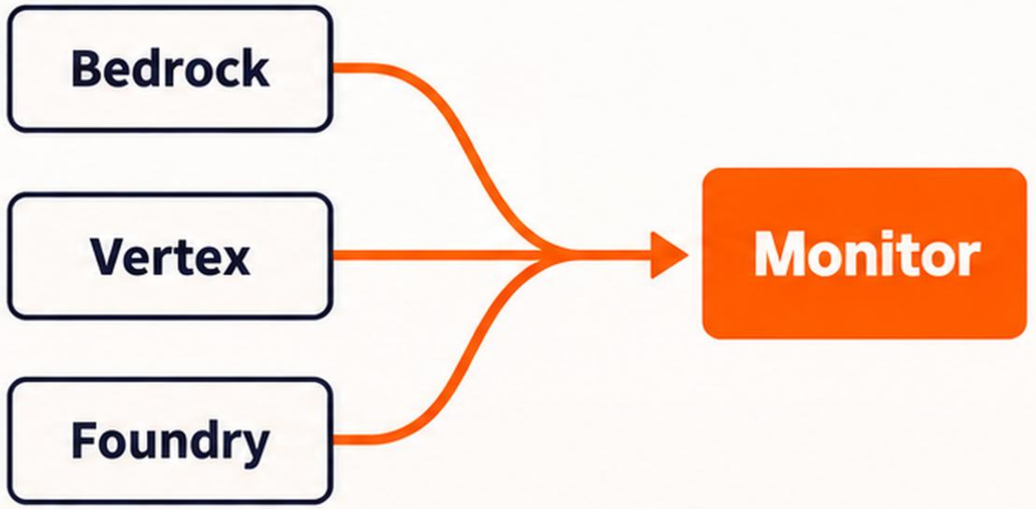
注目3件

TEKION Group

Claude Code、Monitorが全経路で利用可能に

Claude Code 2.1.310が公開されました。

- Monitorツールとプラグインのモニターが、Bedrock・Vertex・Foundry経由と…
- ゲートウェイや互換サーバーが `effort-2025-11-24` のベータ値や会話途中のシステムメッセージを拒んで失敗す…
- `cleanupPeriodDays` をとても大きな値にしたとき、貼り付けた画像など最近のファイルまで掃除で消える不具合を修正



社内のゲートウェイやクラウド事業者経由でClaude Codeを使っている環境では、Anthropicに直接つないだときと動きがそろっていない部分がありました。

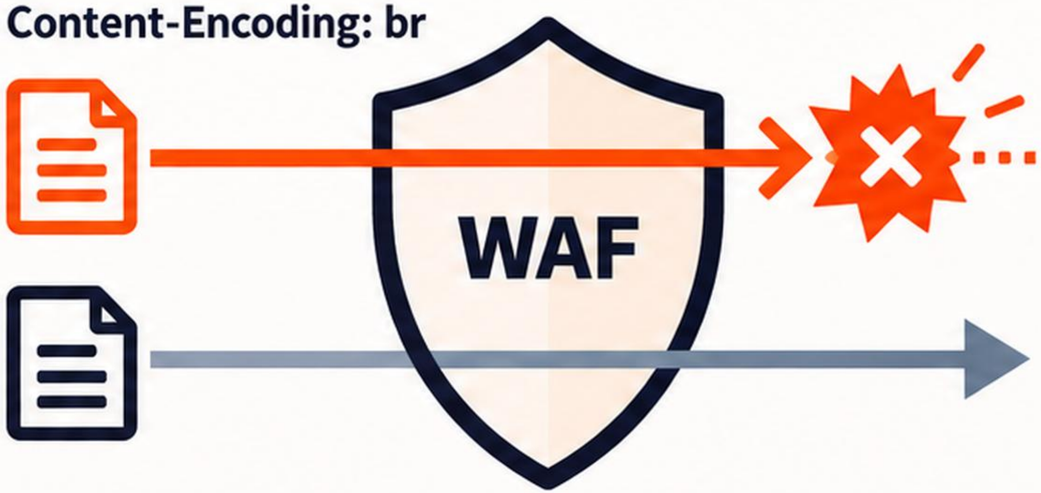
github.com

TEKION Group

Cloudflare、Brotli脆弱性にWAF規則

Cloudflareは、圧縮形式Brotliの脆弱性（CVE-2026-111497）に関係する2つの検知ルールを、Cloudflare Managed Rulesetに緊急で追加しました。

- 対象はBrotliの脆弱性CVE-2026-111497。10月25日公開の緊急リリース
- Brotliのルールは、リクエスト本文に`Content-Encoding: br`を付けた通信だけが対象。`Accept-Encoding: br`…
- Next.jsのルールは`/_next/image`へのリクエストが対象。正規の画像最適化の通信にも当たるため…



10月25日に取り上げたBrotliの脆弱性に対して、CDNの側でも守りが始まりました。

英国、AIで生物の脅威に備える研究所

英国政府は、AIを使って感染症などの生物学的な脅威を早く見つけ、ワクチンや治療薬の開発を速める「AI Biosecurity Lab（AIBL）」を設立すると発表しました。

- 新設の「National AI Biosecurity Initiative」に1億6,500万ポンド。うちAIBLに1億ポンド…
- AIBLは、OpenAIとAnthropicから最大2億ポンド分のAIモデル利用枠の提供を受け、Google…
- AI Security Instituteに1億2,000万ポンドを追加し、新しいAIシステムの試験と技術標準づくりを続ける



AIが脆弱性や脅威を人より速く見つける時代に向けて、国がAIを守りの側で使う体制に具体的な予算を付けた例です。

gov.uk

TEKION Group

llama.cpp、DeepSeek V4.1 Flashに対応

ローカルでLLMを動かす定番ソフトllama.cppが、ビルドb11870でDeepSeek-V4.1-Flashに対応しました。

- 対応したのはビルド b11870（10月25日 11:15 JST公開）
- 新しいモデル種別 `deepseek41` を追加
- Engramのテーブルを BF16 に変換し、MXFP8 形式は外した。Engramの行の取り出しもグラフの中で行う



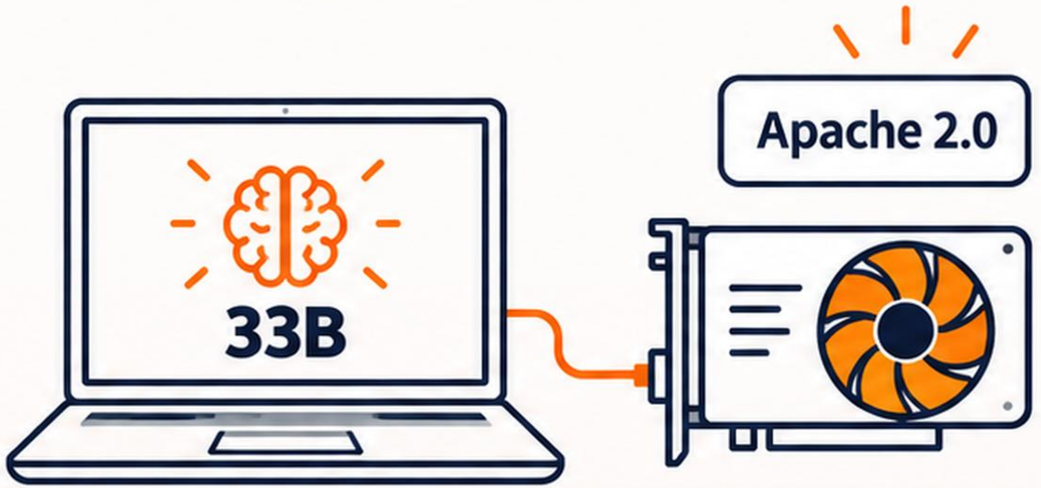
DeepSeekのAPIを通さずに、V4.1 Flashを手元のマシンで動かす道が開けました。

github.com

Nanbeige、エージェント向け33Bを公開

中国のNanbeige LLM Labが、33Bパラメータの公開重みモデル「Nanbeige4.3-33B」を、商用利用もできるApache 2.0ライセンスでHugging Faceに公開しました。

- 33B、ライセンスはApache 2.0。事前学習だけのベースモデル「Nanbeige4.3-33B-Base」も同時に公開
- Nanbeigeの比較では、Terminal-Bench 2.1が80.9（Qwen3.8-27Bは73.0）、DeepSWEが65.5（同42.5）
- SWE-Bench Proは60.3で、Qwen3.8-27Bの61.7をわずかに下回る。GPQA DiamondではGemma4-31B（91.3）が上



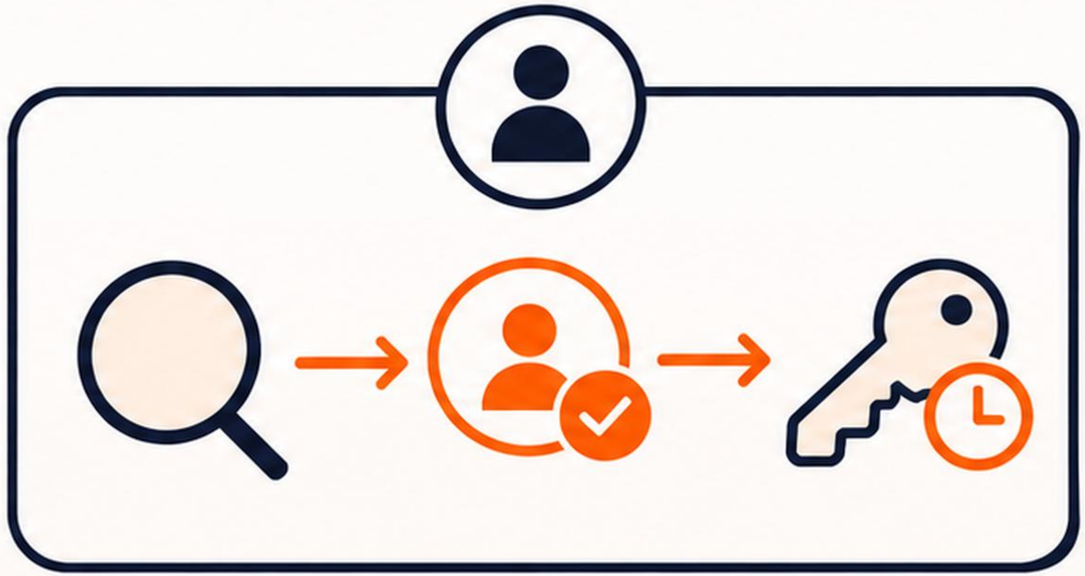
30B前後は、メモリの多いMacやGPU 1枚で手元実行を狙える大きさです。

huggingface.co

〈知見〉Vercel流、エージェントの権限設計

Vercelが、自社のVercel Agentに本番環境を安全に操作させるための権限設計を解説しました。

- 調査は`read:´で始まる読み取り専用の権限だけで自動で進める。それを超える権限を求める計画は、計画ごと承認を待つ
- 承認しても、ユーザー自身が持っていない権限はエージェントに渡らない
- 承認後は、読み取りの基本権限に承認した分を足した、期限付きのトークンが用意される…



「エージェントにどこまで任せるか」を、権限の粒度と承認のタイミングで設計する具体例です。

〈知見〉ECCをCodexに入れる前に

Claude CodeやCodexに、計画・テスト・レビュー・記憶の仕組みをまとめて足すオープンソースの道具集「ECC」が、Xで「Codexに入れるべき」と紹介されて広く読まれています。

- ECCは「計画 → テスト → 実装 → レビュー → 検証 → 記憶 → 改善」の流れを…
- 中身は71エージェント・311スキル・97コマンドと、フック・ルール・記憶・AgentShield（プロンプト、フック…
- Codexでは、`codex plugin marketplace add affaan-m/ECC` と `codex plugin add ecc@ecc` …



スキルやエージェントを大量に入れると、読み込む文脈が増えて動きが重くなることもあります。

本日のトピック一覧

1. Claude Code、Monitorが全経路で利用可能に
2. Cloudflare、Brotli脆弱性にWAF規則
3. 英国、AIで生物の脅威に備える研究所
4. llama.cpp、DeepSeek V4.1 Flashに対応
5. Nanbeige、エージェント向け33Bを公開
6. 〈知見〉Vercel流、エージェントの権限設計
7. 〈知見〉ECCをCodexに入れる前に