MORNING DISPATCH

2026-10-31

Cursor の拡張機能ストアに、偽の「Claude Code」拡張。SSH…

Claude Code 2.1.314、作業フォルダの外への書き込みを一律で禁止できる設定。VS…

Claude の Max プランが「Max」と「Ultra」に。Ultra…

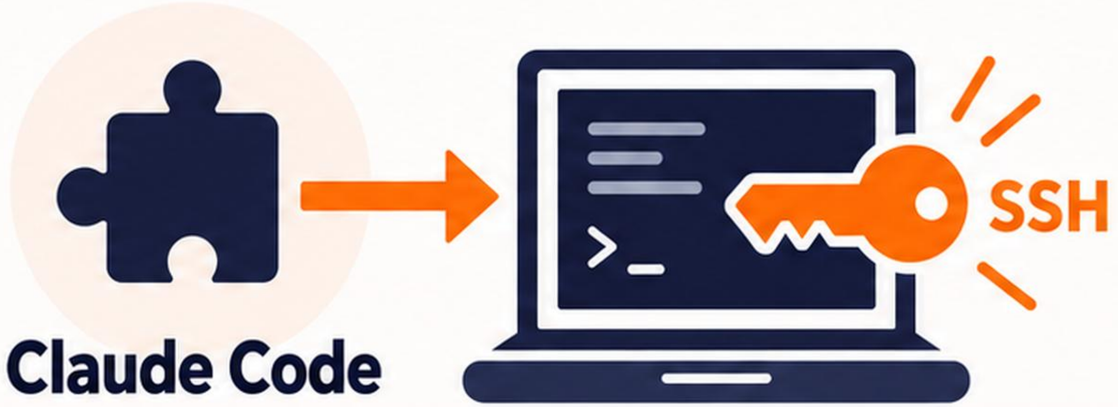
注目3件

TEKION Group

Cursorの拡張機能ストアに、偽の「Claude Code」拡張。SSHの裏口を仕掛ける版が最大5,000人に

Cursorが、自社のVS Code拡張機能マーケットプレイスで、Anthropicの「Claude Code」拡張を装った改ざん版（2.1.312と2.1.313、macOSとWindows向け）が配布されていたと公表しました。

- 配布されていたのは米国太平洋時間10月29日の午前2時27分～午後1時35分（日本時間10月29日18時27分～30日5時35…
- 送られたのはホスト名・ユーザー名・OS・ホームフォルダ・環境変数の名前・Gitのメールアドレス・グローバルIPなど
- `~/.ssh/authorized_keys` に `svc-telemetry` という鍵があれば感染。macOSは `grep -qs svc-telemetry…



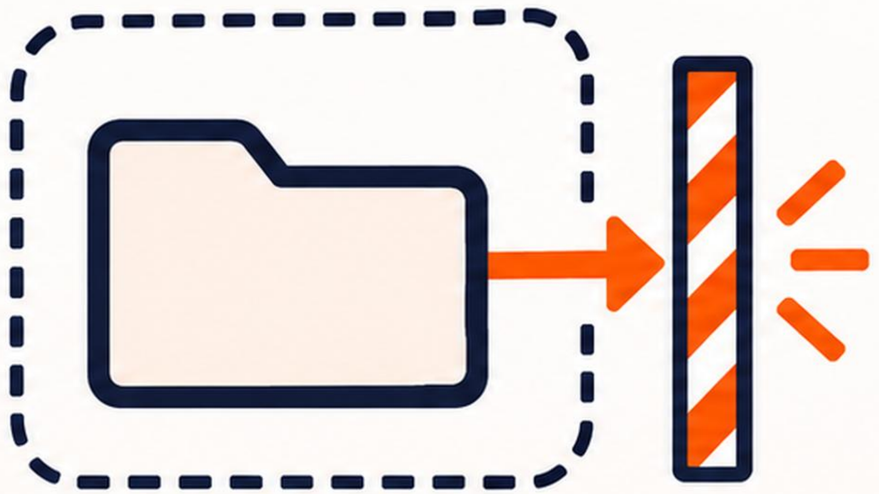
AIコーディングツールの拡張機能は、手元のファイルやシェルに広い権限を持ちます。

cursor.com

Claude Code 2.1.314、作業フォルダの外への書き込みを一律で禁止できる設定。VS Code…

Claude Codeの2.1.314が公開されました。

- `permissions.blockWritesOutsideWorkingDirectories`：Write・Edit・NotebookEditが、作業フォルダの外のパスを拒否する
- idle compaction：20万トークン以上の会話を放置すると要約しておき…
- 管理者がモデルのeffortに上限を設けた組織で「Invalid effort level」が続く不具合を修正…



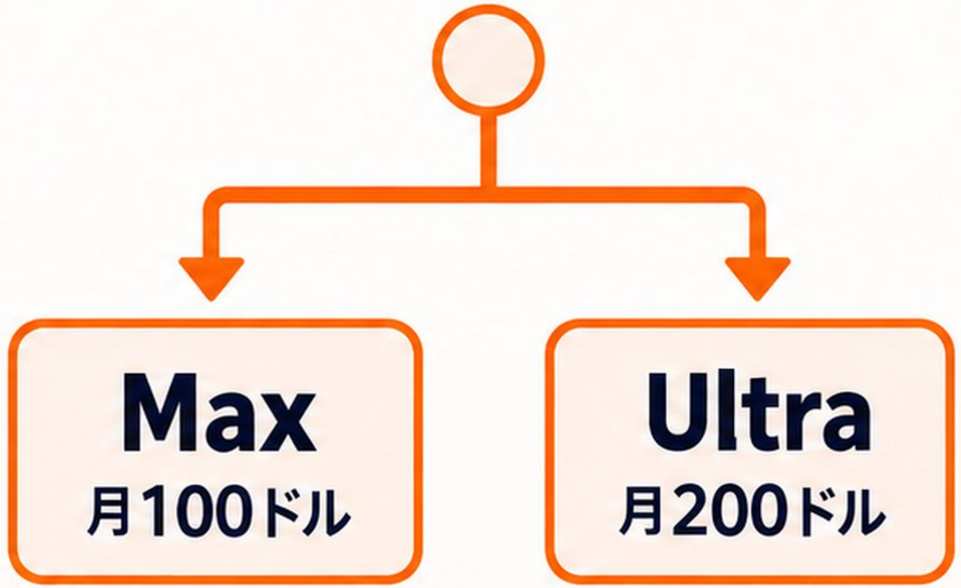
エージェントに広い権限を任せるほど、「作業フォルダの外は触らせない」という線引きが効いてきます。

github.com

ClaudeのMaxプランが「Max」と「Ultra」に。Ultraは本人確認済みなら5時間ごとの利用…

Anthropicが、Claudeの上位プランの名前を変えました。

- Maxは月100ドル、Ultraは月200ドルのまま。
  週ごとの利用上限は変わらない
- 新しいアカウントは、不正利用を防ぐため本人確認が
  済むまで一時的に5時間制限が残る。制限が外れると
  メールで知らせる
- 料金ページでは、Ultraの利用量は「Proの10倍／週」。
  Claude Platform（API）のクレジットがMaxに月100ドル分…



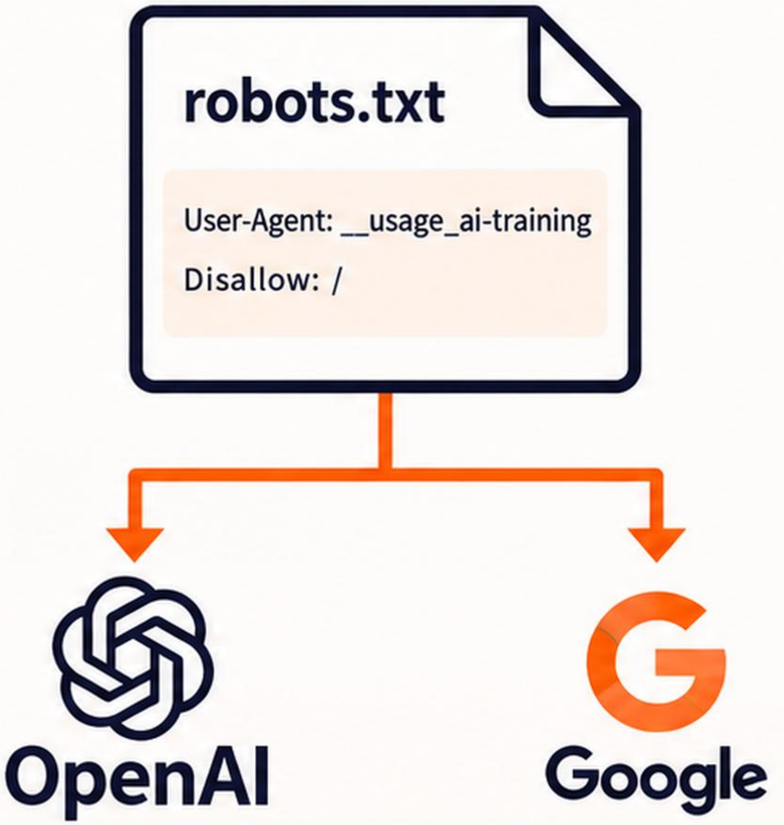
Claude Codeなどを長時間回す人にとって、5時間ごとに止まらないのは大きな変化です。

x.com

OpenAIとGoogle、robots.txtの共通の合図で「AIの学習に使わないで…

OpenAIとGoogleが、ウェブサイトのrobots.txtに書く「AI学習についての共通の合図」を尊重すると発表しました。

- 書き方は `User-Agent: __usage_ai-training` のグループに `Disallow: /` などを書く形…
- `User-Agent: *` の指定はこの合図に当てはまらない扱い。合図のグループがなければ「意思表示なし」とみなす
- Googleは、この合図で学習を拒否していてGoogle-Extendedの指定がない場合、Google-Extendedを拒否したものとして扱う方針



自分のブログやサービスの文章をAIの学習に使われたくないとき、1か所の指定で複数社に意思を示せるようになります。

openai.com

VercelのData CacheがRuntime Cacheに統合。Next.js…

Vercelが、Next.jsのfetchキャッシュなどに使われてきた「Data Cache」を、
フレームワークを問わず使える「Runtime Cache」に一本化すると発表しました。

- 料金は読み取り100万ユニットあたり0.40ドル、書き込み100万ユニットあたり4.00ドルから（地域で変わる）…
- Proはプロジェクト・環境ごとに、以前のチーム全体の容量の8倍。Enterpriseは以前の10倍…
- Hobbyのチームは2026年11月29日に自動で移行。Proには移行日を個別に通知する…



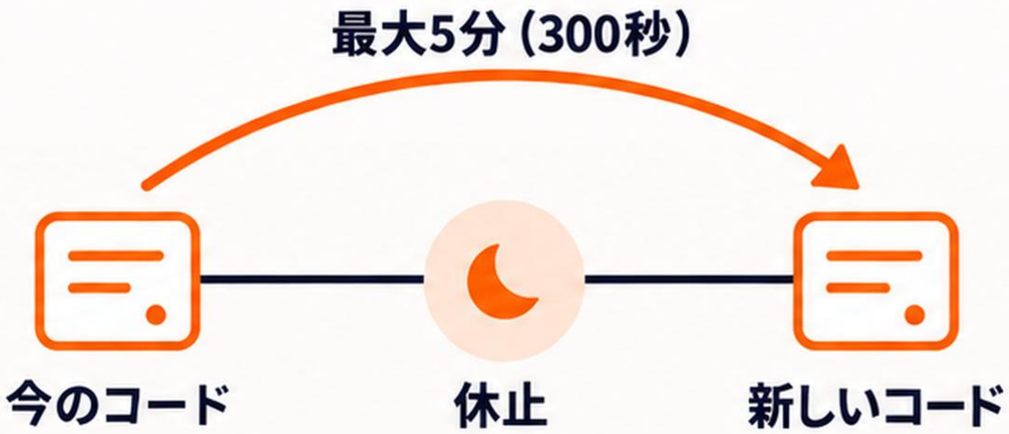
Next.jsのアプリをVercelに置いている人は、何もしなくても請求が変わる可能性があります。

vercel.com

Cloudflare Durable Objects、デプロイ時の新しいコードへの切り替えを既定で最大5分待つ…

CloudflareのDurable Objectsは、長時間動くエージェントやWebSocketの接続を保ったまま、状態を持って動かせる仕組みです。

- 動作中のオブジェクトは、最大5分（300秒）待つあいだ今のコードで動き、休止（hibernate…
- Hibernation APIを使ったWebSocket接続は、休止を経て新しいコードに切り替わっても切れない
- 待ち時間内に休止しなかった場合や、即時切り替え（immediate）を選んだ場合は、リセットして新しいコードになる



エージェントを本番で動かすと、「デプロイのたびに途中の仕事が消える」問題にぶつかります。

OpenAI、企業向けのデータ保護をまとめた「Private Intelligence」を発表…

OpenAIが、企業が機密性の高い仕事に最新モデルを使うためのデータ保護の取り組みを「OpenAI Private Intelligence」としてまとめて発表しました。

- Private Safety Processingは、OpenAIの社員が顧客の内容を見ずに、自動の仕組みで悪用の兆候を調べる方式…
- Private Inferenceはプレビューの段階で、機密計算と検証できる管理の仕組みを組み合わせる…
- 対象になる条件や、Private Inferenceの一般提供の時期は、確認できた範囲では示されていない

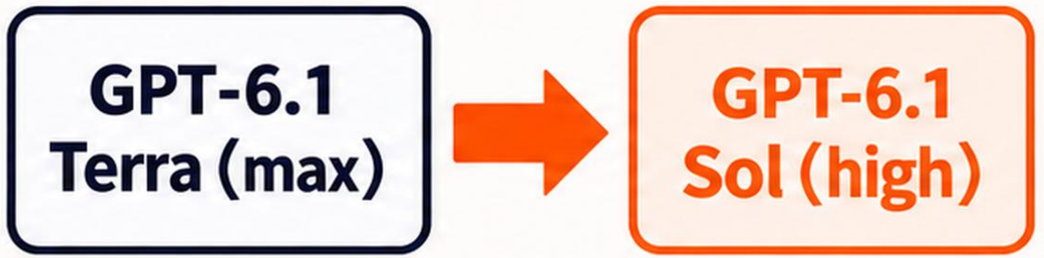


企業がAIの導入をためらう大きな理由は「データを誰が見られるのか」です。

〈知見〉GPT-6.1 Terra を推論量 max で回すより、GPT-6.1 Sol の high の方が割安…

金のニワトリ（@gosrum）さんが、Codexの利用枠がリセットされたタイミングで、GPT-6.1 Terraを推論量（effort）maxで追加検証した結果を公開しました。

- 結論は「GPT-6.1 Terra（max）を使うくらいなら、GPT-6.1 Sol（high）を使おう」
- Terra（max）はTerra（xhigh）より性能は上だが、費用は3倍以上
- 続く投稿では、GPT-6.1 Solのxhighやmediumも、費用あたりの性能が最も良い部類だと補足



推論量を最大にすると、性能は伸びてもトークンの消費が急に増えます。

本日のトピック一覧

1. Cursor の拡張機能ストアに、偽の「Claude Code」拡張。SSH…
2. Claude Code 2.1.314、作業フォルダの外への書き込みを一律で禁止できる設定。VS…
3. Claude の Max プランが「Max」と「Ultra」に。Ultra…
4. OpenAI と Google、robots.txt の共通の合図で「AIの学習に使わないで…
5. Vercel の Data Cache が Runtime Cache に統合。Next.js…
6. Cloudflare Durable Objects、デプロイ時の新しいコードへの切り替えを既定で最大…
7. OpenAI、企業向けのデータ保護をまとめた「Private Intelligence」を発表…
8. 〈知見〉GPT-6.1 Terra を推論量 max で回すより、GPT-6.1 Sol の high…