MORNING DISPATCH

2026-10-22

PHPに重大な脆弱性、すぐ更新を

eMudhraの中間CA、秘密鍵が漏えい

Claude Duet、先回りして動く秘書アプリ

注目3件

TEKION Group

PHPに重大な脆弱性、すぐ更新を

PHPの開発チームは、認証なしで外部からプログラムを実行される恐れがある重大な脆弱性2件を修正した、PHP 8.5.12、8.4.27、8.3.36、8.2.35を公開しました。

- CVE-2026-109618（メモリ不足時の処理中断）と CVE-2026-109619（解放済みの状態が次のリクエストに残る）
- 対象はPHP-FPM・mod_php・php-cgi・FrankenPHP・LiteSpeedなど、Webを処理する全構成
- 8.1以前は公式更新なし。7.4・8.0・8.1向けに最小限のソース修正を特別に提供



WordPressなど、PHPで動くサイトを持つ人は今すぐ更新が必要です。

php.net

TEKION Group

eMudhraの中間CA、秘密鍵が漏えい

インドの認証局eMudhraが発行した中間CA証明書8件で、秘密鍵の漏えいが判明しました。

- Firefox・Chromeは10月17日、Appleは19日、Microsoftは20日から遮断
- 原因は認証局側の鍵生成の誤りで、2025年4月の作成時から鍵を割り出せた
- Node.js 22.23.4、Python certifi 2026.10.19、Go 1.27.3、Claude Code 2.1.303 などが修正版



ブラウザだけ更新しても、サーバーやエージェントが使うランタイムの証明書リストが古いままだと偽のサイトを信じてしまいます。

emudhra.we-have-a-problem.com

Claude Duet、先回りして動く秘書アプリ

Anthropicは、Claudeが自分から動くエージェントとして働く新しいアプリ「Claude Duet」の研究プレビューを始めました。

- iOS・Androidの単体アプリとclaude.aiで提供
- まず米国のPro・Max加入者から、順番待ちリスト制
- 利用上限は他のClaudeと共通で、裏での確認も消費する



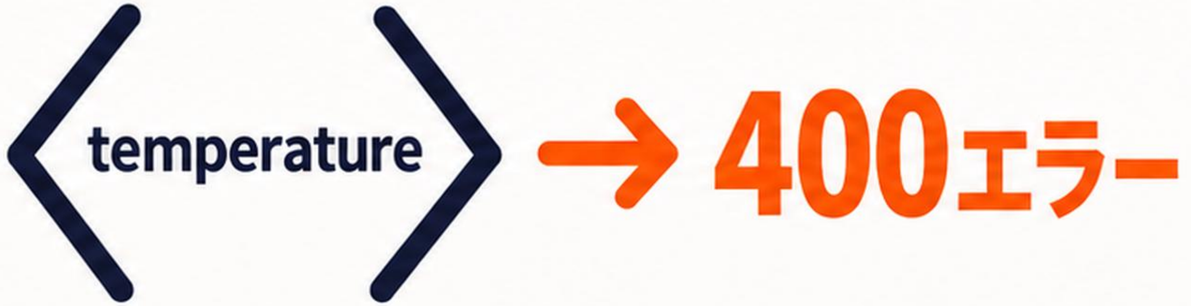
聞かれたら答えるAIから、状況を見て声をかけてくる秘書型のエージェントへ広がっています。

claude.com

Claude API、新版でtemperature廃止

Anthropicは、Claude APIの新しいバージョン「2026-10-21」を公開しました。

- temperature・top_p・top_k は削除され、送ると400エラー
- アシスタント側のメッセージに文書ブロックを直接入れると400エラー
- Python SDK 2.0.0、TypeScript SDK 1.0.0、Go SDK 2.0.0 などが新版を既定で送る



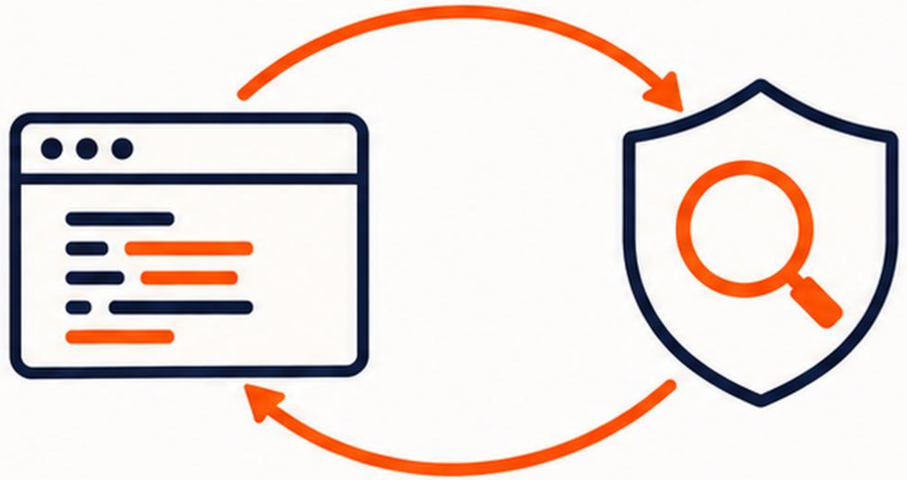
依存関係の自動更新でSDKのメジャー版が上がると、temperature を指定しているコードがエラーになります。

platform.claude.com

Claude Security、変更のたびに自動で再検査

Anthropicのセキュリティ診断ツールClaude Securityが、リポジトリをつなぐと最初に詳しく検査し、その後はコードの変更に合わせて継続的に再検査するようになりました。

- GitHubアプリ（GitHub Enterprise Server含む）か、GitLabなどのアクセストークンで接続
- プロジェクトごとに、デプロイ方法やセキュリティ方針を書く知識ベースを持てる
- Claude Enterprise向けのパブリックベータ

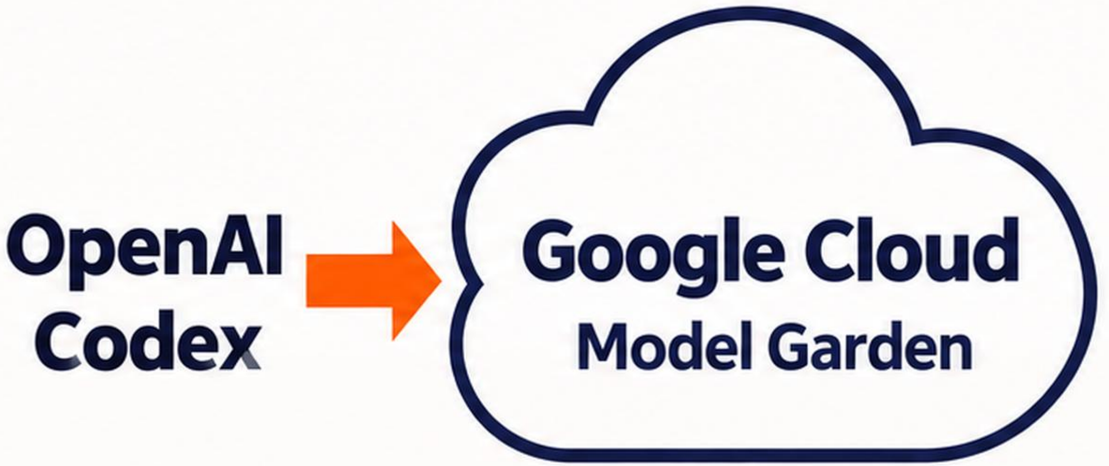


AIがコードを大量に書くほど、たまに検査するだけでは追いつきません。

OpenAIのモデル、Google Cloudに

OpenAIとGoogle Cloudが提携し、OpenAIのモデルとCodexをGoogle CloudのModel Gardenで使えるようにしました。

- 対象はGPT-6 Astra・GPT-6.1 Sol・GPT-6 Luna
- 現在は一部企業向けの限定プレビューで、利用は申し込み制
- 請求はGoogle Cloudにまとまり、利用額の約束（コミット）から充当できる



Google Cloudで社内の仕組みを作っている会社も、契約を増やさずにOpenAIのモデルを選べるようになります。

GitHub CLI、期限付きトークンを選択可能に

GitHub CLI（gh）で、有効期限付きで自動更新されるOAuthの認証情報を、パブリックプレビューとして選べるようになりました。



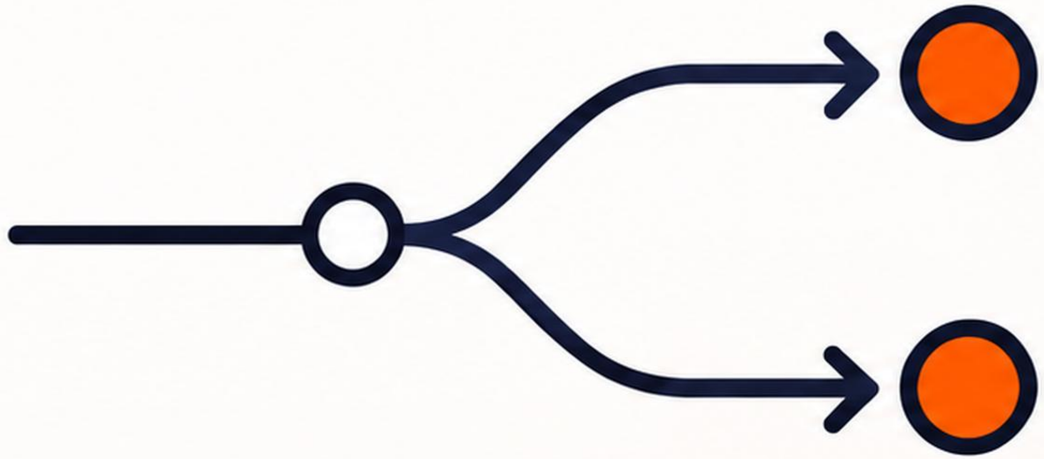
- v2.103.0以降で gh auth login --expiring
- 毎回使うなら gh config set expiring_credentials enabled
- gitで使うなら gh auth setup-git と git 2.46以降を強く推奨

AIエージェントにghを使わせる場面が増え、トークンが漏れたときの被害を小さくする設定です。

判定専用モデル、27日まで無料

Vercel AI Gatewayで、Basetenの判定専用モデルMammoth-1（27B）とElephant-1（9B）が10月27日まで無料で使えます。

- 無料期間は10月27日まで
- モデル名は baseten/mammoth-1 と baseten/elephant-1
- コンテキストは16kトークン



問い合わせの仕分けや承認の判断のように、選ぶだけの処理は大きなモデルでなくても回せます。

vercel.com

本日のトピック一覧

1. PHPに重大な脆弱性、すぐ更新を
2. eMudhraの中間CA、秘密鍵が漏えい
3. Claude Duet、先回りして動く秘書アプリ
4. Claude API、新版でtemperature廃止
5. Claude Security、変更のたびに自動で再検査
6. OpenAIのモデル、Google Cloudに
7. GitHub CLI、期限付きトークンを選択可能に
8. 判定専用モデル、27日まで無料