

MORNING DISPATCH

2026-10-15

GitHub Actions、実行する依存コードをロック

Copilot、複数モデルの検査を深めるMaxを追加

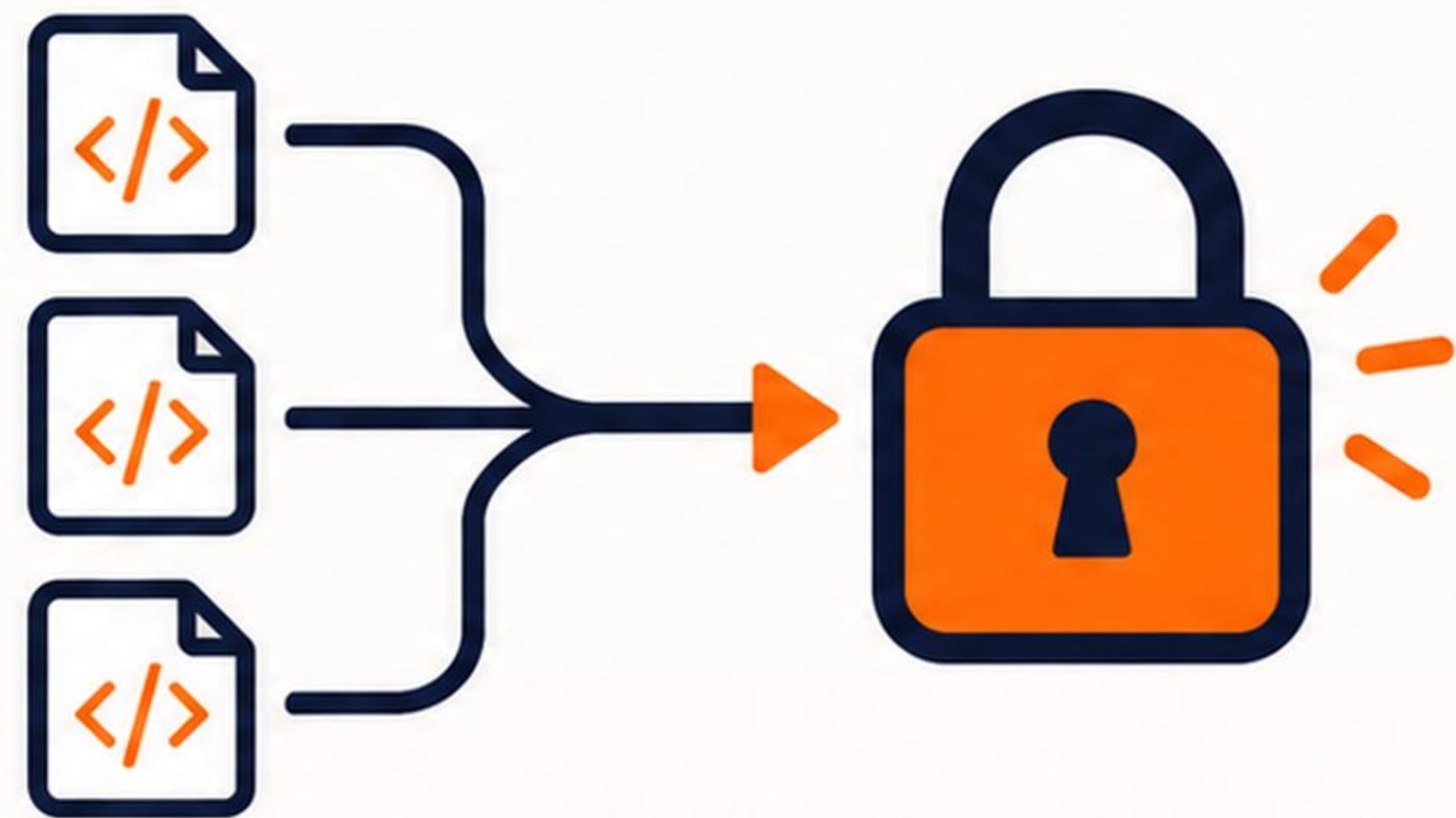
Claude Code、放置中の長い会話を自動圧縮

注目3件

GitHub Actions、実行する依存コードをロック

GitHub Actionsに、ワークフローが使うアクションを特定のコミットに固定するロックファイルがプレビューで入りました。

- `gh actions-lock`で依存関係のロックを生成
- 推移的依存と再利用ワークフローも対象
- Dependabotが更新PRでロックも更新

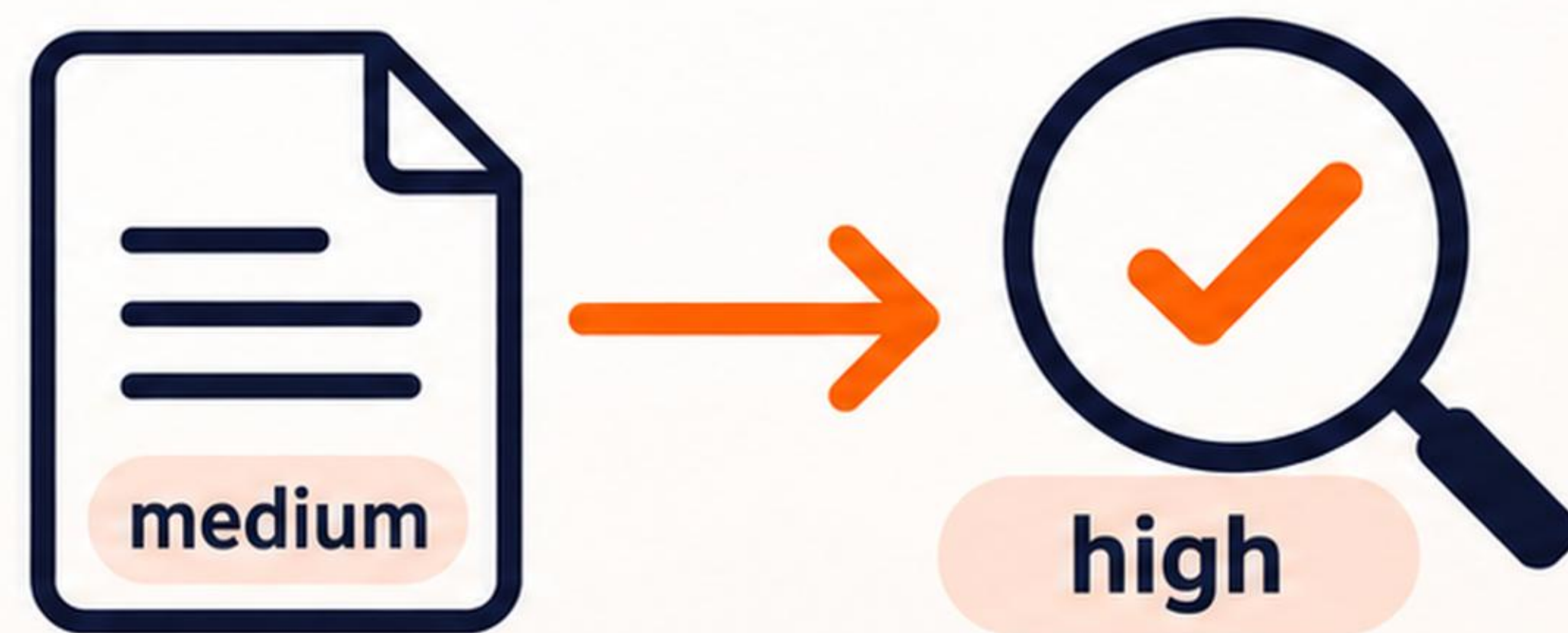


タグの差し替えでCIの実行内容が変わるリスクを減らせます。

Copilot、複数モデルの検査を深めるMaxを追加

GitHub CopilotのHydraFusionに、難しい作業向けのMaxが追加されました。

- Opus 5.5、GPT-6 Astra、Sol、Lunaをプールに追加
- 下書きはmedium、レビューはhighで処理
- VS Code・Copilotアプリ・CLIで研究プレビュー

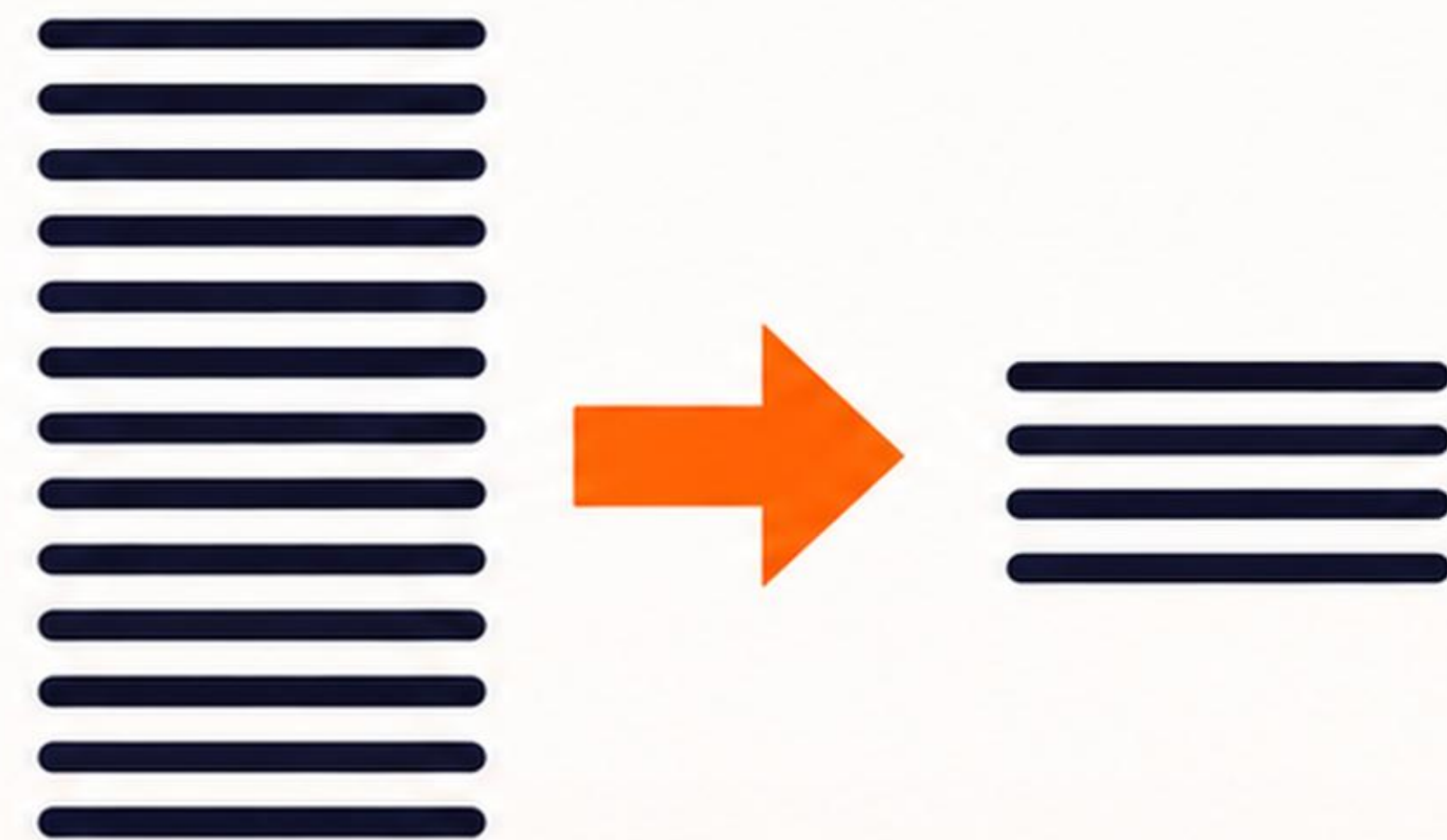


作成と検査に異なるモデルを使う仕組みを、開発ツール側が担います。

Claude Code、放置中の長い会話を自動圧縮

Claude Code 2.1.299は、大きな会話を放置している間に圧縮する機能を追加しました。

- 20万トークン以上の会話を約54分の待機後に圧縮
- 1時間キャッシュの期限切れ前に処理
- 設定で無効化や最低トークン数の変更が可能

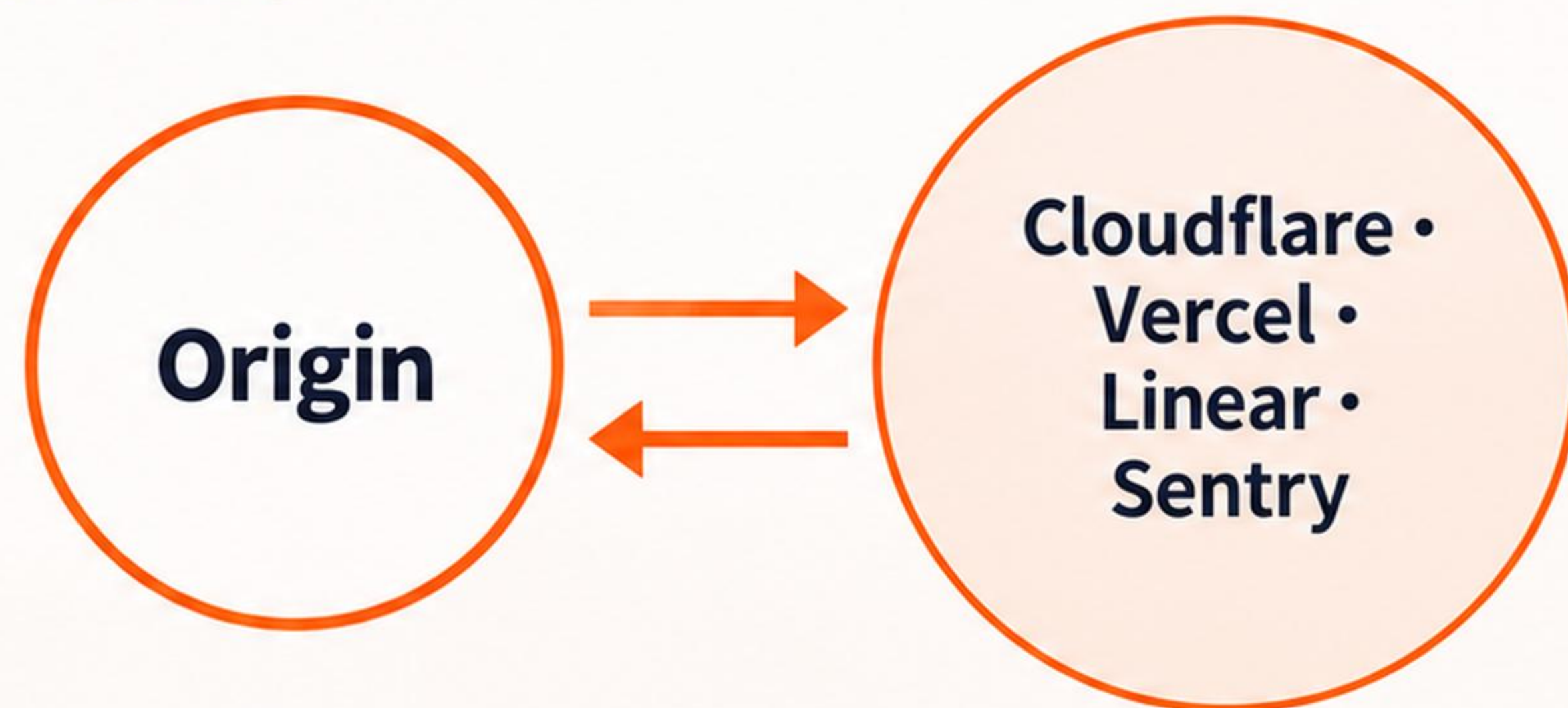


長い作業を中断した後、次の入力で全履歴を処理し直す負担を抑えます。

Cursor Origin、20以上のアプリと連携

Cursorのソース管理基盤Originに、デプロイやCI、コードレビューなど20以上のアプリが集まるマーケットプレイスができました。

- Cloudflare・Vercel・Linear・Sentryなどが参加
- アプリはJWTとインストールトークンで認証
- webhookからチェック結果やレビューを書き戻せる

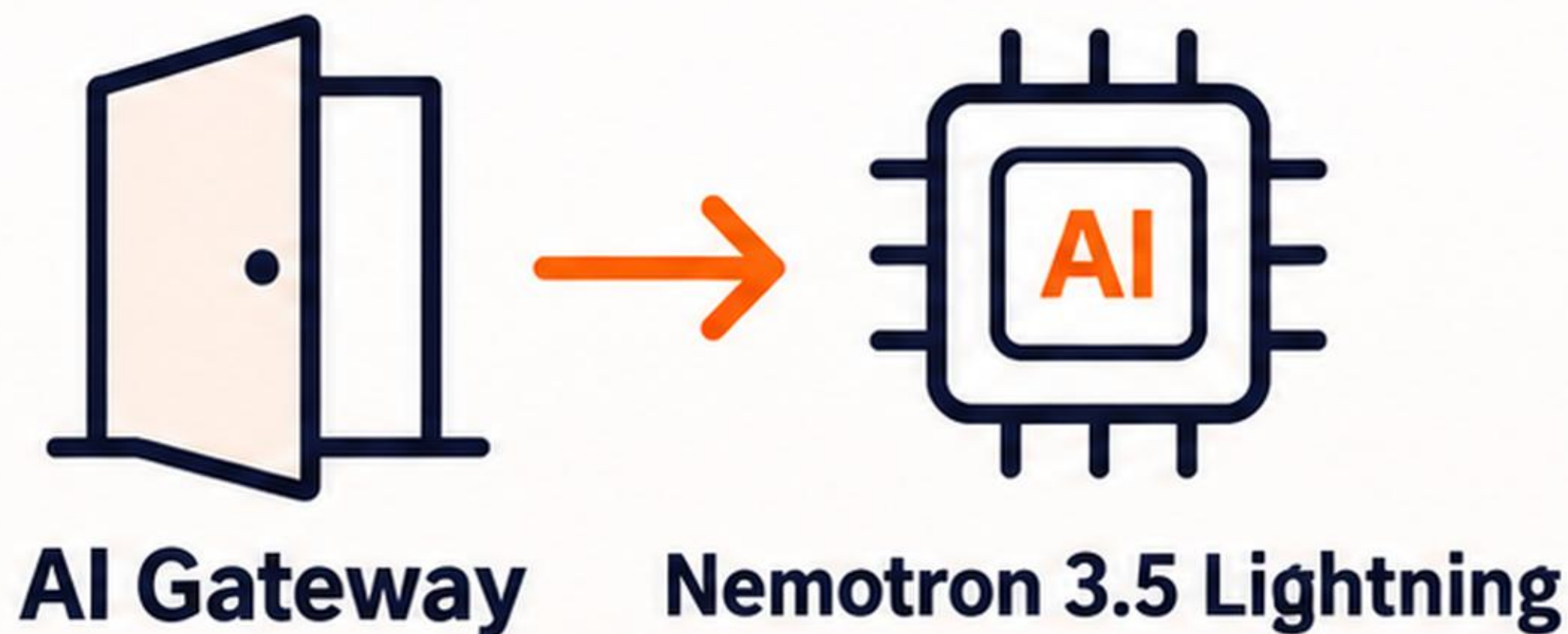


Originを使うチームが既存の開発工程を接続しやすくなります。

Nemotron 3.5 Lightningを AI Gatewayで無料提供

Vercel AI Gatewayで、NVIDIAが提供するNemotron 3.5 Lightningの無料枠が使えるようになりました。

- モデルIDはnvidia/nemotron-3.5-lightning-free
- 100万トークンのコンテキストに対応
- 総30B、トークンごとに3Bが動く設計

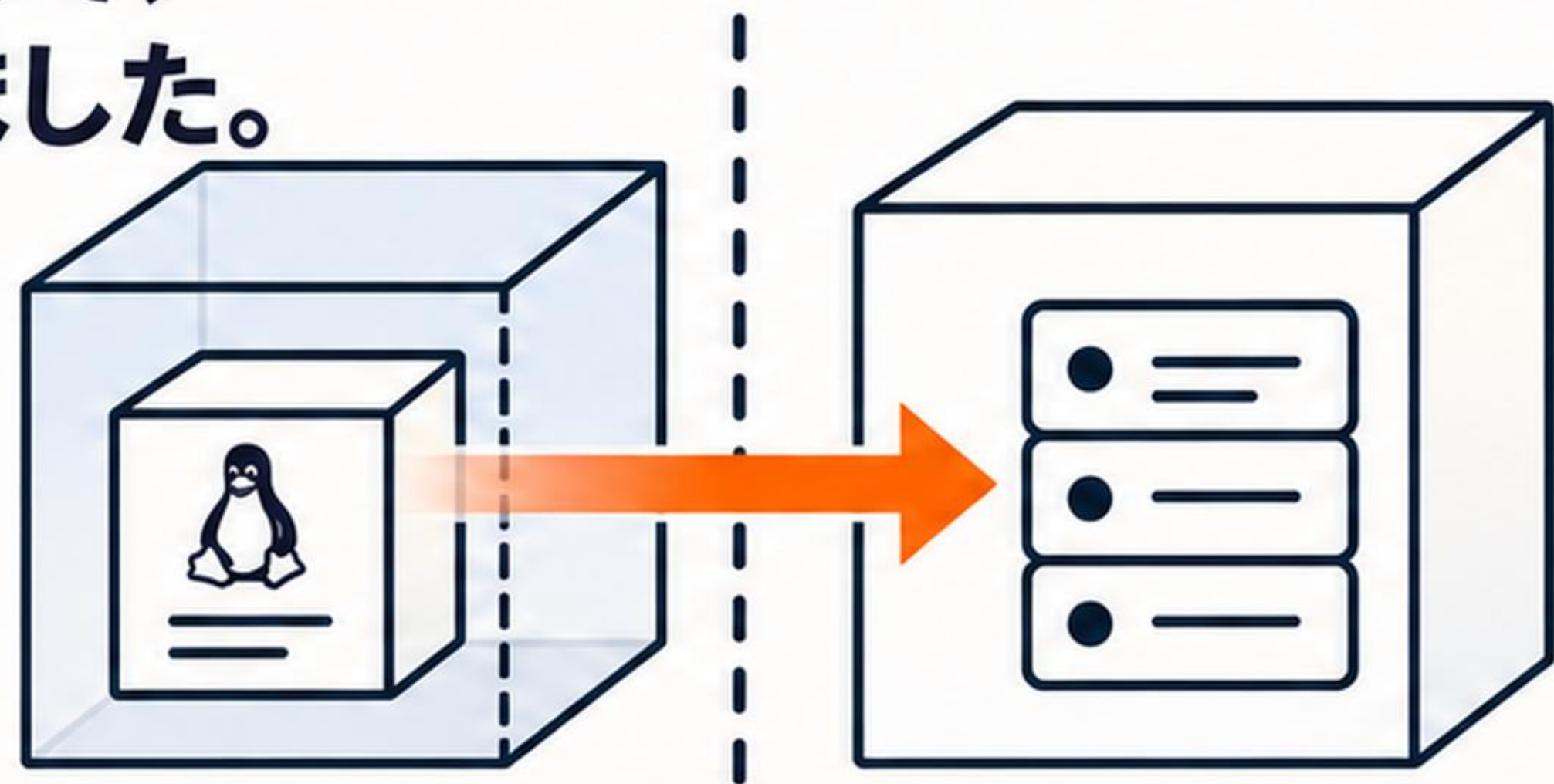


下書きや公開情報の整理を試す選択肢になります。

Vercel Sandboxの検証でLinuxの欠陥を発見

VercelはSandbox脱出チャレンジの結果として、Linuxカーネルの未公開の欠陥などを報告しました。

- 2週間で1,285件の報告、報奨金は24万2,000ドル
- 修正は非公開レビュー中でCVEは未発行
- 各microVMは専用のゲストカーネルを持つ



仮想マシンで分離していても、ホスト側の処理に欠陥があれば境界を越える場合があります。

Gemmaで詐欺を検知、 会話を端末内で処理

Google DeepMindとシンガポールのGovTechは、
現地の詐欺会話で調整したGemmaの検知モデルを開発しました。

- 軽量な分類器とGemmaの会話分析を組み合わせる
- 学習には匿名化された報告・情報データを利用
- 展開後も政府やGoogleが会話を取得しない設計



小型モデルを地域のデータで調整し、外部に送れない情報を端末内で扱う実例です。

本日のトピック一覧

1. **GitHub Actions、実行する依存コードをロック**
2. **Copilot、複数モデルの検査を深めるMaxを追加**
3. **Claude Code、放置中の長い会話を自動圧縮**
4. **Cursor Origin、20以上のアプリと連携**
5. **Nemotron 3.5 LightningをAI Gatewayで無料提供**
6. **Vercel Sandboxの検証でLinuxの欠陥を発見**
7. **Gemmaで詐欺を検知、会話を端末内で処理**