Tech News Daily

2026-06-24

MORNING DISPATCH / Vibe Coder Bootcamp Tech News

今朝のホットな話題

1. JetBrains の AI コーディングエージェント「Junie」が正式版（GA）に — IDE のデバッガで自律デバッグ
2. Mastra npm サプライチェーン攻撃の全貌 — 北朝鮮 Sapphire Sleet が 88 分で 144 パッケージを汚染
3. 中島聡 「Vibe Crafting」— Vibe Coding はまだ序の口、本丸は一人のためにその場で作るソフトウェア

7 トピックを整理。

TEKION Group

1. JetBrains の AI コーディングエージェント「Junie」が正式版（GA）に — IDE のデバッガで自律デバッグ

何が起きた？

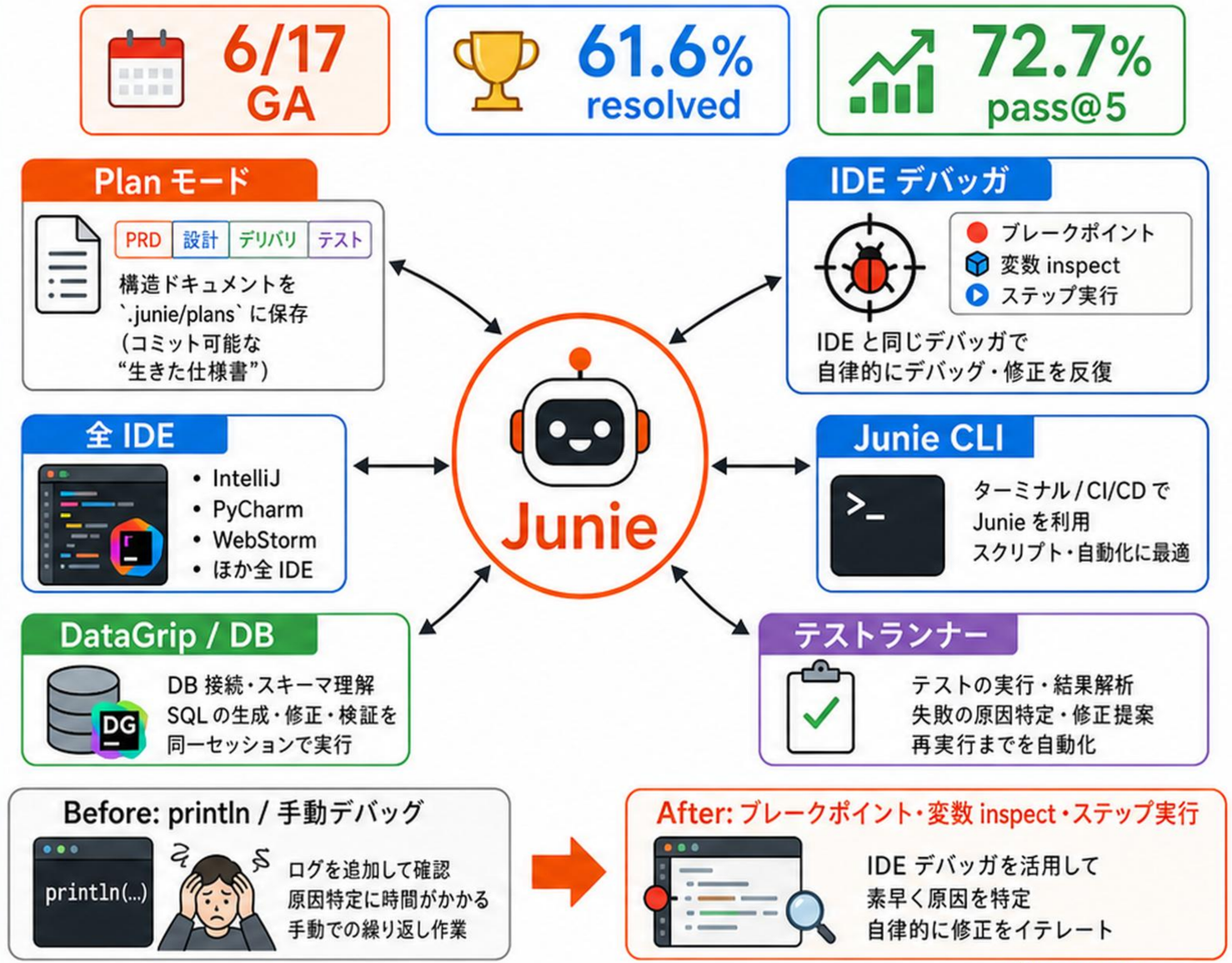
JetBrains は AI コーディングエージェント Junie を 6/17 に正式版（GA）化。IntelliJ・PyCharm・WebStorm 等の全 IDE と Junie CLI（ターミナル/CI/CD）で動く。IDE 連携を ACP(Agent Communication Protocol) で作り直した。

主な変更点

- **Plan モード:** 生成前に PRD/技術設計/デリバリ段階/テスト戦略をタブ化した構造ドキュメントを `.junie/plans` に保存（コミット可能な“生きた仕様書”）
- **自律デバッグ:** println でなく IDE と同じデバッガでブレークポイント・変数 inspect・ステップ実行して修正をイテレート
- **深い IDE 統合:** セマンティックインデックス/ビルド設定/テストランナー/DB(DataGrip) を流用し、SQL の生成・修正・検証も同一セッションで
- SWE-Rebench で coding agent 首位（resolved 61.6% / pass@5 72.7%）
- LLM 非依存・BYOK はプロバイダ料金のみ（JetBrains 上乗せなし）。中国では当面非提供

なぜ重要？

コード生成、仕様書、デバッグ、DB 操作、テスト検証が IDE と CLI をまたいで 1 セッション化。AI エージェントが実開発環境の文脈を使って自律的に修正できる。



2. Mastra npm サプライチェーン攻撃の全貌 — 北朝鮮 Sapphire Sleet が 88 分で 144 パッケージを汚染

何が起きた？

AI エージェント構築フレームワーク Mastra（@mastra スコープ）の npm パッケージ 144 個が乗っ取られ、インストール時に自動実行される postinstall フックでマルウェアを仕込む攻撃が起きた。Microsoft は北朝鮮系 Sapphire Sleet の犯行と高確度で帰属。

主な変更点

- 起点はメンテナアカウント(ehindero)乗っ取り。LinkedIn 経由のソーシャルエンジニアリングと npm の token bypass 設定の隙。
- dayjs の typosquat「easy-day-js」を注入。無害版 1.11.21 → postinstall 付き 1.11.22、^1.11.21 の SemVer 自動解決で新規インストールが汚染版に。
- 01:12–02:39 UTC の 88 分で 142 パッケージを自動再公開。import の有無に関係なく install/update で発火。
- ペイロードは TLS 検証を無効化 → C2 から二段目取得。160+ の暗号ウォレット拡張やブラウザ履歴を窃取し Win/macOS/Linux に永続化。

なぜ重要？

npm v12 が install スクリプトをデフォルト無効化した背景にある実例。コードで import していなくても npm install した瞬間に発火する怖さを示す。

対策 npm install --ignore-scripts / lockfile・依存ツリー監査 / バージョン固定 / メンテナ MFA 徹底 / token bypass 廃止

1. LinkedIn ソーシャルエンジニアリング
2. ehindero 侵害
3. npm token bypass
4. @mastra 144 パッケージ汚染
5. postinstall 発火
6. TLS 無効化 → C2 二段目
7. ウォレット拡張 160+・履歴窃取
8. Win / macOS / Linux 永続化

- 88 分
- 144 パッケージ
- 142 再公開
- 160+ ウォレット拡張
- 1.11.21 → 1.11.22

easy-day-js の Before / After

前日: 1.11.21	翌日: 1.11.22
無害	postinstall 付き

3. 中島聡「Vibe Crafting」— Vibe Coding はまだ序の口、本丸は"一人のためにその場で作るソフトウェア"

要点

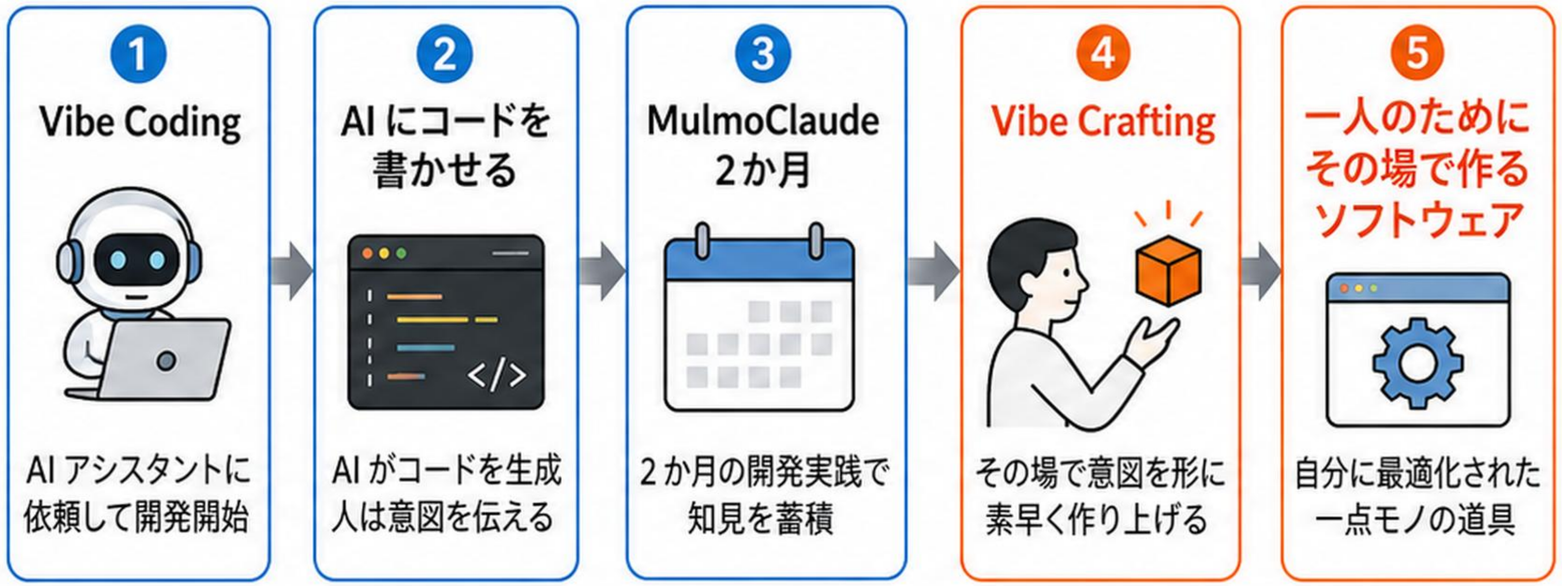
著名エンジニア中島聡が、Vibe Coding（AI にコードを書かせる開発スタイル）はまだ序の口で本丸はその先だと提起した。

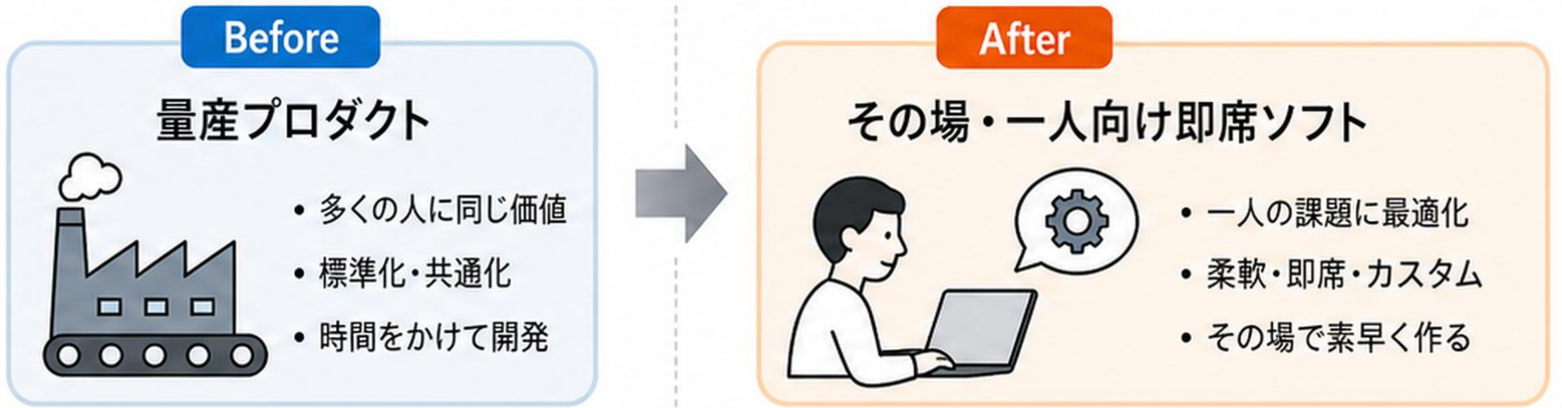
具体的な手法 / 使いどころ

- 「Vibe Coding の次」を Vibe Crafting と命名して提示
- 2 か月の MulmoClaude 開発実践から得た知見

なぜ刺さるか / 学び

量産プロダクトではなく"その場・一人向け"の即席ソフトが当たり前になる、という発想転換。





🔍 何が起きた？

Vibe coding で公開したアプリに SQL インジェクション・認証なし DB 公開・AI エージェントによる本番 DB 削除などの事故が相次いでいると The Verge が報道。実務エンジニアが本番リリース前の具体チェックリストを共有している。

📌 主な事故類型

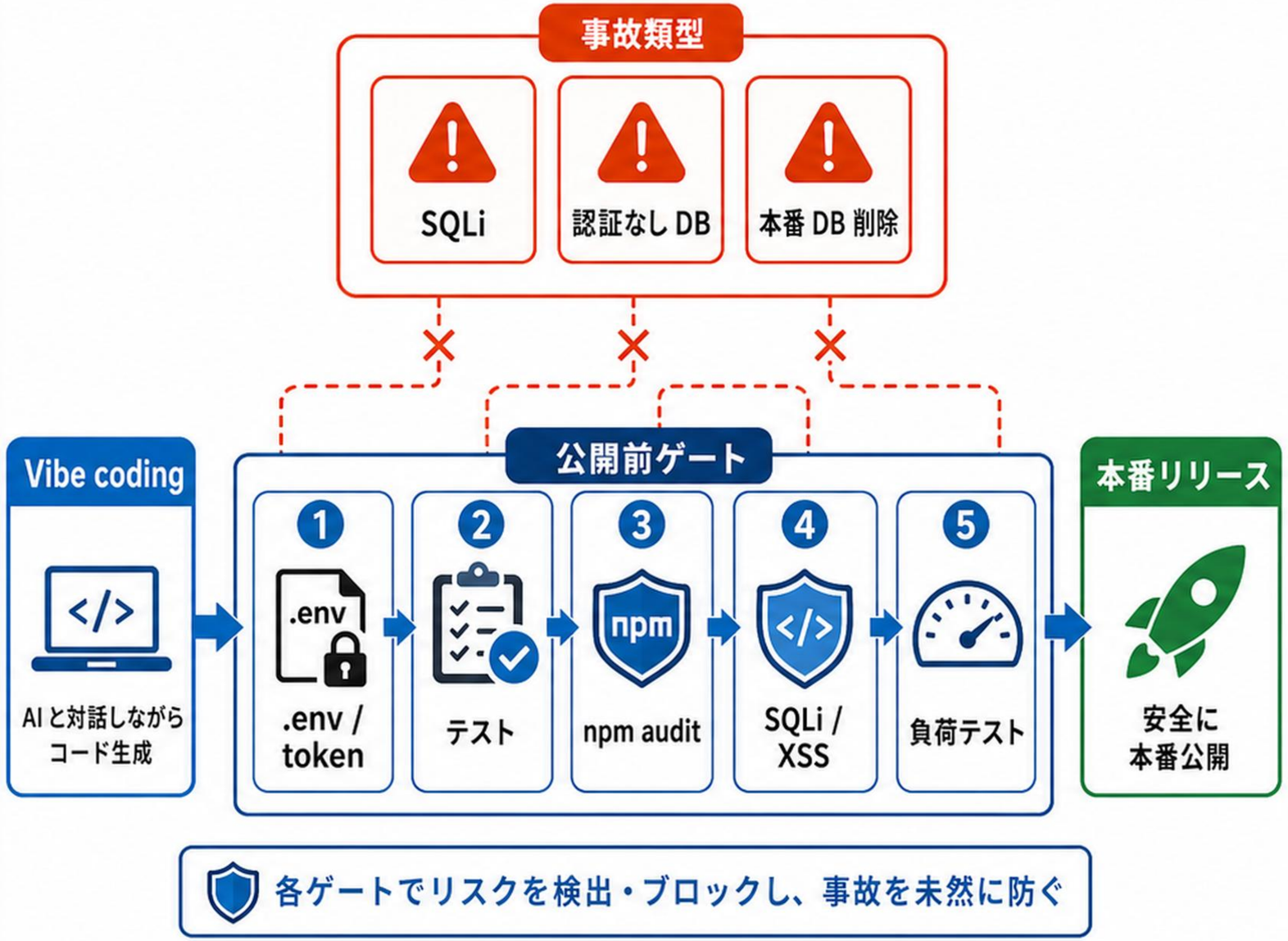
- SQLインジェクション
- 認証なしで DB を公開
- AI が本番 DB を削除

🛠️ 本番前チェック

- 生成コードに .env・認証トークンが混入してないか確認
- AI のコードは『自信満々に間違える』のでテスト必須
- npm audit で依存の脆弱性確認
- SQLi・XSS 対策を必ず入れる
- 本番想定量のシードデータで負荷テスト

💡 なぜ重要？

『動く』までが速い分、本番スケールでの挙動を想像する時間が削られやすいのが事故の温床。ローカル少数データだと N+1 等を見逃す。



5. Codeburn — Claude/Codex/Cursor/Copilot+28 ツールの AI コーディング支出をローカルで一元可視化

要点

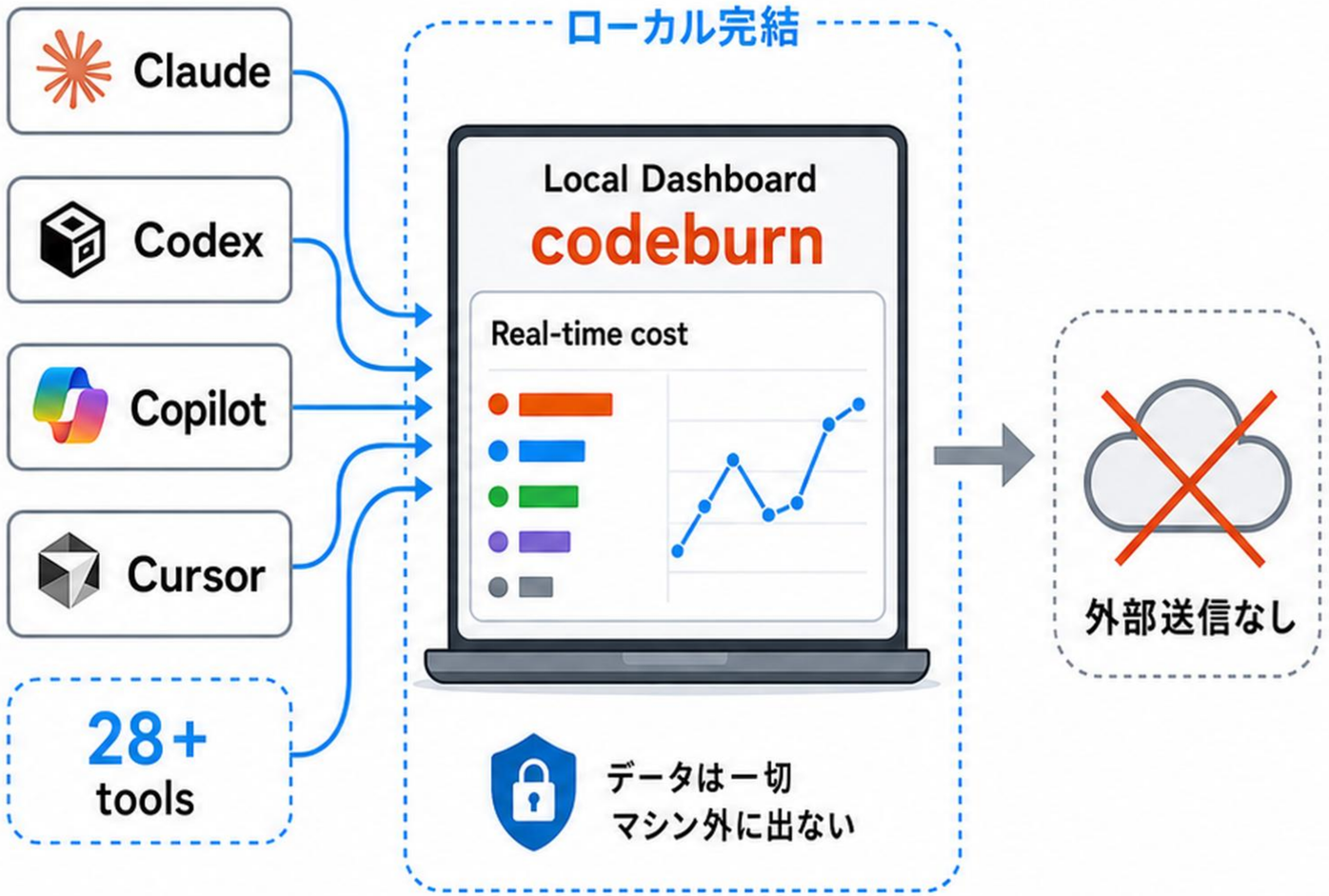
`npx codeburn web` だけで、Claude・Codex・Copilot・Cursor など 28+ の AI コーディングツールの利用コストをローカルのダッシュボードでリアルタイム集計。データは一切マシン外に出ない。

具体的な手法 / 使いどころ

- 28+ の AI コーディングツール横断でコストをライブ集計
- `npx codeburn web` で起動、ローカル完結（プライバシー）
- Claude・Codex・Copilot・Cursor などを併用するチームの支出確認に使える

なぜ刺さるか / 学び

複数エージェント併用で“課金が見えない”問題への回答。AI コーディングの利用が広がるほど、ツール別ではなく横断の可視化が重要になる。



6. Cline を完全ローカル・オフラインで動かす — Atomic Chat が open-weight モデルで実行

🔍 何が起きた？

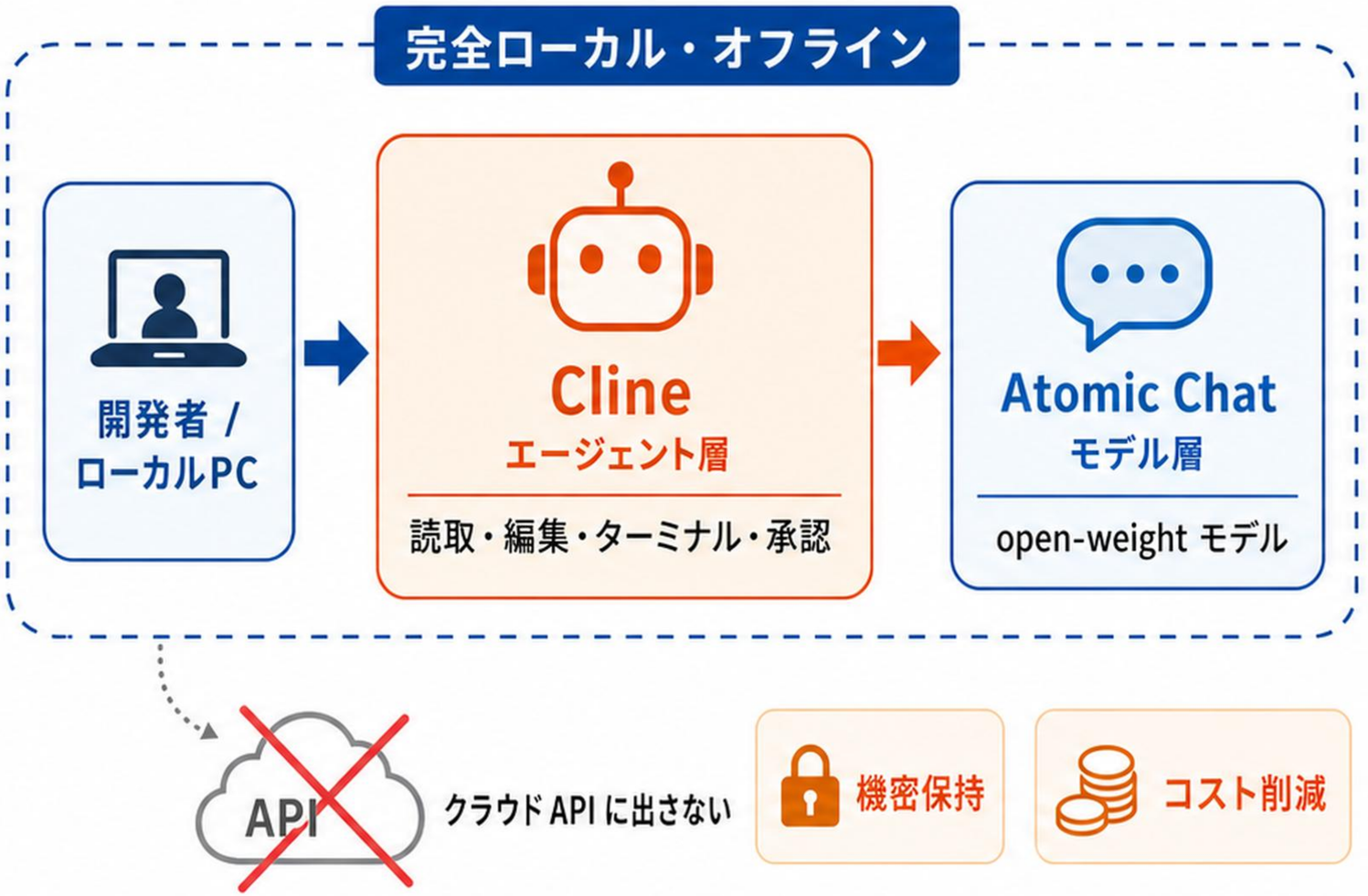
コーディングエージェント Cline を、Atomic Chat のローカル open-weight モデル上で完全オフライン実行できるようにした構成が公開された。

📌 主な変更点

- Cline = エージェント層：ファイル読み書き・コマンド実行・エラー調査・アクション前の承認
- Atomic Chat = モデル層：open-weight モデルをオフライン・ローカルで実行
- クラウド API に出さずローカル完結（機密保持・コスト削減）

💡 なぜ重要？

開発支援エージェントの実行基盤をクラウド依存から切り離し、機密コードやコストを気にせずローカル環境で試せる構成として注目。



7. Cursor 共同創業者 Truell「5 つのエージェントを切り替えるのは未来じゃない」— 数日かけ完成品を返すエージェント像

💡 要点

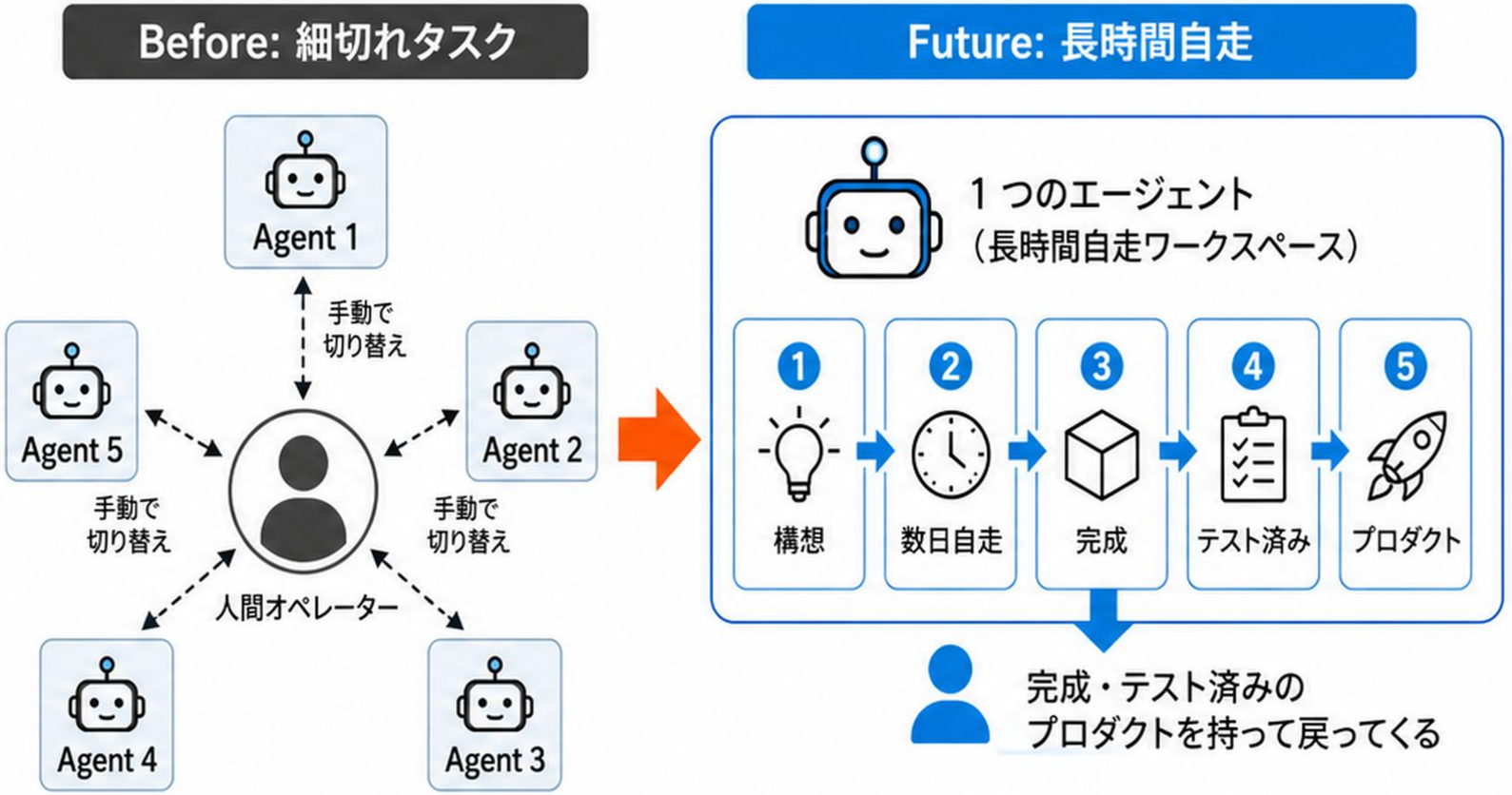
Cursor 共同創業者 Michael Truell が、細切れタスクのために 5 つのエージェントを切り替える今のやり方はコーディングの未来ではない、と述べた。

🛠️ 具体的な手法 / 使いどころ

ラフな構想を渡す → エージェントが数日姿を消す → 完成・テスト済みのプロダクトを持って戻ってくる。

🌱 なぜ刺さるか / 学び

複数エージェントを手動で切り替える現状を「過渡期」と位置づけ。目指す姿は、長時間自走して完成・テスト済み成果物を返すエージェント。



> 5 つのエージェントを切り替えるのは未来じゃない
>
> — Michael Truell

TEKION Slide Generator v5

TEKION Group

今日のまとめ

本日のトピック一覧

1 JetBrains の AI コーディングエージェント「Junie」が正式版（GA）に — IDE のデバッガで自律デバッグ

GA

Junie が IDE のデバッガと統合し、コード理解から再現・原因特定・修正検証までを自律実行。

2 Mastra npm サプライチェーン攻撃の全貌 — 北朝鮮 Sapphire Sleet が 88 分で 144 パッケージを汚染

88 分　144 パッケージ

Sapphire Sleet が Mastra の信頼を悪用し、短時間で多数パッケージにマルウェアを混入。

3 中島聡「Vibe Crafting」 — Vibe Coding はまだ序の口、本丸は「一人のためにその場で作るソフトウェア」

Vibe Coding を超え、個人の文脈と目的に最適化したソフトをその場で創る未来を提示。

4 Vibe coding で本番に出す前の必須チェック — 事故報道（The Verge）と実践チェックリスト

The Verge の事故報道を踏まえ、本番前に確認すべき実践チェックリストを整理。

5 Codeburn — Claude/Codex/Cursor/Copilot+28 ツールの AI コーディング支出をローカルで一元可視化

+28 ツール

複数 AI ツールの利用・支出をローカルで集約し、コストと利用状況を一元可視化。

6 Cline を完全ローカル・オフラインで動かす — Atomic Chat が open-weight モデルで実行

完全ローカル

Cline を外部依存なしにローカル環境で稼働。プライバシーとセキュリティを確保。

7 Cursor 共同創業者 Truell「5 つのエージェントを切り替えるのは未来じゃない」 — 数日かけ完成品を返すエージェント像

5 つ　数日

多くのエージェントを使い分ける時代は終わり。数日かけて完成品を届けるエージェントへ。

出典サマリ: OpenAI　Anthropic　Google　JetBrains　The Verge　npm

TEKION Group
TEKION Slide Generator v5