



いけともch 「注目AIニュース19選」 から
2026.10.12

今週のAIニュース 7選

原石工房

隠れた才能に気づき、花開く

10月5日～11日の7つ



原石工房

守りの話が3つ、道具と仕組みの話が4つ。出典は各面の小見出しから開けます

- 1 顧客情報の流出が相次ぐ
- 2 GLM-5.3、重みを公開
- 3 バイブコーディングの穴
- 4 Claude Haiku 5.5
- 5 Claude Cowork、クラウドへ
- 6 企業向けのGemini agent
- 7 Personal Agent Protocol

① 顧客情報の流出が相次ぐ

出典：GMOリサーチ&AIのお知らせ（押すと開きます）

何があったか

GMO・ミスターマックス・焼肉キング・タイムズなどが流出を公表。タイムズは免許証の情報も漏れた

なぜ大きいのか

都道府県によっては免許証の再発行を案内するほどの規模。AIが使われたかは、どの発表にも書かれていない

② GLM-5.3、重みを公開



原石工房

出典：Z.aiのブログ（押すと開きます）

米国の非公開のモデル

提供する会社のクラウドで動く

悪用を提供側で止められる

GLM-5.3（重みを公開）

手元に落として動かせる

悪用を止める仕組みが弱い

穴を見つける力はMythos並み

③ バイブコーディングの穴



原石工房

出典：ITmedia NEWS（押すと開きます）

調べた公開アプリ

200件

バイブコーディング製

脆弱性があった割合

91%

ほぼすべてに穴

失敗の型

8つ

記憶・目標・知識

④ Claude Haiku 5.5



原石工房

出典：Anthropic（押すと開きます）

値段

GPT-6と同じ値段。
Claudeの安いモデルの
割高さが消えた

賢さ

同じ値段で、多くの試
験でGPT-6を上回る

効く場面

サブエージェントや
APIで、数をこなす仕
事

⑤ Claude Cowork、クラウドへ



原石工房

出典：Claudeのヘルプセンター（押すと開きます）

これまで

手元のPCで処理する

ファイルはPCの中

手元で動かすならCowork



これから

クラウドで処理する

一度コピーし、終われば消す

手元で動かすならClaude Code

⑥ 企業向けのGemini agent



原石工房

出典：Google Cloudのブログ（押すと開きます）

いま（自分のアカウントで動かす）

人とAIの作業が見分けられない

AIの権限が自分と同じになる

Gemini agent（エージェントに専用ID）

専用のメールとIDで記録が残る

任せる範囲を絞って渡せる

⑦ Personal Agent Protocol



原石工房

出典：Sierraのブログ（押すと開きます）

使う人が決めること

見るだけか、書き込むか

ログインまで任せるか

企業が決めること

AIにどこまで見せるか

応じ方は画面・API・会話



出典：いけともch「注目AIニュース19選」（押すと開きます）

コロナでリモートワークが広がったように、
セキュリティ危機で、守る側にも
エージェントが要る時代が来る

— 池田朋弘さん（いけともch、2026年10月11日の動画より要約）

あなたの会社は、どれから備えますか



原石工房

隠れた才能に気づき、花開く