AI 技术每日分析：DeepMind 用 AlphaProof Code 验证 Signal 部分密码学实现

中国高技术产业发展促进会新质生产力工作委员会

博雅云创 & 中科创新驱动

2026 年 11 月 11 日

摘要

11 月 10 日的几条 AI 消息，关注点逐渐落到任务能否完成、结果能否核验。Google DeepMind 介绍 AlphaProof Code：智能体生成证明，再交给形式语言与机器核验；Google 开放 Gemini 4 Carbon，并发布面向视觉知识工作的 MKA 基准。OpenAI 推出 Businesses in ChatGPT 及 Business Agent 相关功能，还与 Upwork 发布自由职业市场研究。另有微调数据污染研究提示，训练与交付环节的安全检查不能省。

Contents

1. DeepMind 以 AlphaProof Code 验证 Signal 关键密码学实现 2
2. Gemini 4 Carbon 开放，长任务与协作智能体受到关注 2
3. MKA 基准测试智能体能否交付可用文件 3
4. OpenAI 让企业资料进入 ChatGPT 对话 3
5. 自由职业市场变化与微调数据风险 4
趋势观察 4
参考资料 4

1. DeepMind 以 AlphaProof Code 验证 Signal 关键密码学实现

Google DeepMind 在 11 月 10 日介绍 AlphaProof Code 研究。人类专家先审定形式化安全规范，多个 AI 智能体随后生成 Lean 证明，由 Lean 内核做机器检查。研究对象是 Signal 协议参考实现 libsignal 的一部分代码: 团队把协议层的安全性质与 AArch64 机器代码接起来, 针对 PQXDH 握手和 Triple Ratchet 验证前向保密、身份认证、密钥泄露后的安全恢复等指定性质。团队报告，四周集中攻关生成约 650 万行 Lean 证明代码; 他们还重新引入两处曾修复的缺陷，测试机制能否辨识。

这项工作没有证明 Signal 整个应用程序无条件安全，更不能保证软件今后没有漏洞。它的实际价值在于：对边界明确的安全性质，工程团队可以反复检查证明, 同时把更多精力用在规范是否准确、编译目标是否对应、可信计算基础是否可控上。工业控制、能源、医疗系统若采用类似方法，可以先从通信协议、权限检查或固件升级链路等模块做起。

2. Gemini 4 Carbon 开放，长任务与协作智能体受到关注

Google 在 11 月 10 日宣布，Gemini 4 Carbon 面向开发者、企业和部分订阅用户提供，重点放在复杂编码、调试、科学研究、网络安全及持续多步骤任务。Antigravity 开发平台预览/swarm 功能可把任务分给多个协作智能体，让它们在平行工作区进行架构设计、执行和反向核验。官方列出的限时公开 API 价格是每百万输入 token 2 美元、每百万输出 token 10 美元，并注明 11 月 30 日后公开版本价格将调整；实际使用仍要看当期服务条款。

协作智能体可分担接口设计、迁移测试和安全审计。每个环节都能记录使用的工具、任务上下文、产物和交叉检查结果。企业可按任务完成率、

成本、日志和版本记录评估协作效果。

3. MKA 基准测试智能体能否交付可用文件

Google 与 Artificial Analysis 在 11 月 10 日推出 Multimodal Knowledge Agent（MKA）评测，测试模型处理图像、复杂排版、表格和不同文件格式的知识任务。代理需要调用工具，读取并生成实际交付文件。公告称正式评测集有 200 项私有任务、10 项公开样例；自动评分器会打开文件、渲染页面、检查电子表格公式，再按专家标准评判，官方报告的人类专家与自动评分一致率为 96%。Google 称，在该次测试中 Carbon 的质量位列被测模型第二，单位任务平均费用比最高分模型低六倍以上；这是该公司介绍的测试结果。

企业可以用表格公式、图纸尺寸、图例和版本差异检验文件交付质量。工业知识还分布在 PDF、CAD 导出图、试验记录和异构表格里，评测时应看可用成果、工程约束以及人工复核成本。

4. OpenAI 让企业资料进入 ChatGPT 对话

OpenAI 于 11 月 10 日公布 Businesses in ChatGPT 测试版。企业可在 Business Hub 认领并核验身份，维护基本信息、产品价格和供应情况，查看聚合层面的被提及与网站点击数据。部分美国电商和在线服务企业还可建立 Business Agent，让用户基于企业资料进一步了解产品与服务。公告区分代理对话与独立模型回答，企业提供的信息及工具受平台政策约束；聚合分析不向企业提供用户私人对话。

企业由此多了一个展示和解释产品的对话入口，首批面向特定商业类别。工业设备或企业服务供应商可以提前整理技术参数、配置边界和服务记录；工业设备和企业服务商可先把技术参数、配置边界和服务记录整理成结构化资料。

5. 自由职业市场变化与微调数据风险

OpenAI 与 Upwork 在 11 月 10 日发布自由职业市场研究，观察不同服务门类的需求、项目预算及 AI 相关技能组合。报告指出，部分传统服务的份额有变化，AI 相关工作也在与原有专业技能重新组合。企业购买服务时，开始更多地关注围绕业务目标完成整段交付的能力。

同一天，Anthropic 及合作研究者公开微调数据污染研究：在特定小模型和构造数据集条件下，少量有害训练样本经过“稀释”，反而可能表现出更强的后门效果。企业需要审计训练数据来源、评测数据与模型更新过程。

工业智能体与专业人员可在工程流程中分工，人员负责物理约束和结果核对。平台订单呈现服务需求变化，受控实验为模型更新审计提供了具体样本。

趋势观察

今天的消息涵盖证明核验、协作开发、文件交付和企业服务。证明要对上代码，协作智能体要留痕，生成文件要能打开并接受检查；企业对话入口和模型更新还涉及信息边界与安全审计。工程团队可以从具体任务开始，连接工具、产物和复核记录。

参考资料

1. deepmind.google ｜ DeepMind 以 AlphaProof Code 验证 Signal 关键密码学实现｜ 2026-11-10 ｜相关资料
   `https://deepmind.google/blog/introducing-alphaproof-code/`
2. google-deepmind.github.io ｜ DeepMind 以 AlphaProof Code 验证 Signal 关键密码学实现｜ 2026-11-10 ｜相关资料
   `https://google-deepmind.github.io/code-verification/`

3. blog.google ｜ Gemini 4 Carbon 开放，长任务与协作智能体受到关注 ｜ 2026-11-10 ｜相关资料
https://blog.google/innovation-and-ai/models-and-research/gemini-models/gemini-4-carbon-now-available/

4. blog.google ｜ MKA 基准测试智能体能否交付可用文件｜ 2026-11-10 ｜相关资料
https://blog.google/innovation-and-ai/models-and-research/gemini-models/multimodal-knowledge-agent-benchmark/

5. openai.com ｜ OpenAI 让企业资料进入 ChatGPT 对话｜ 2026-11-10 ｜相关资料
https://openai.com/index/introducing-businesses-chatgpt/

6. openai.com ｜自由职业市场变化与微调数据风险｜ 2026-11-10 ｜相关资料
https://openai.com/index/ai-effect-on-freelance-work/

7. alignment.anthropic.com ｜自由职业市场变化与微调数据风险｜ 2026-11-10 ｜相关资料
https://alignment.anthropic.com/2026/homeopathic-learning/

机构介绍与关注

新质生产力工作委员会

中国高技术产业发展促进会新质生产力工作委员会，专注于推动工业人工智能、智能制造、数字化转型等前沿技术发展，为企业提供政策解读、技术咨询和产业对接服务。

工业智能算网

专注于工业人工智能、新质生产力、工业软件 CAE、智能制造等前沿技术。提供每日动态分析、技术趋势解读、解决方案分享，推动工业智能化转型。

关注高促会新质生产力工委会公众号

关注工业智能算网平台

https://gyznsw.cn