由 Codex 自动生成

AI前沿发展日报 | 2026-07-02（Asia）

日期：2026-07-02；覆盖窗口：2026-07-02 00:00-23:59（Asia/Sh
窗口内完成公开确认、进入执行节点或形成新增变量的官方发布、一级媒体报道、研究预印本与高信号公开讨论。

今日要点

今天最值得看的不是单个新模型，而是平台边界在收紧：OpenAI 的自助微调在 7 月 2 日进入第二个收口节点，未在过去 60 天运行过微调模型推理的组织失去创建新微调任务的资格。基础设施侧，Meta 被报道计划把过剩 AI 算力和模型访问包装成云业务，资本市场把“AI 资本开支能否变现”作为新的定价变量。应用侧，Xero 把财务数据、MCP、CLI、AI 代理和行业基准数据连在一起，说明垂直 SaaS 正在从记录系统走向行动系统。政策侧，美国 6 月 2 日 AI 网络安全行政令的首批 30 天动作在今天到期，监管重点从抽象原则转向联邦系统防御、漏洞清理和前沿模型测试通道。

今日结论

1. AI 平台正在从“开放试用”转向“活跃用户保留、低活跃用户退出、老能力迁移”的生命周期管理；企业不能把模型微调、评测平台和旧接口当作永久资产。

2. AI 基础设施的竞争从“谁买到 GPU”进入“谁能把闲置或峰谷容量商业化”；Meta 若正式入局，会压低新兴 AI 云厂商的稀缺性溢价。

3. 垂直 SaaS 的 AI 护城河会更多来自专有工作流数据、审计记录和可执行连接器，而不是聊天入口本身。

AI 产品与应用

OpenAI 自助微调进入 7 月 2 日收口节点。 OpenAI API 文档显示，7 月 2 60 天没有运行过微调模型推理的组织将不能再创建新的微调任务；现有微调模型推理仍可用，直到对应基础模型退役；活跃客户创建新微调任务的最终截止日是 2027 年 1 月 6 日。对企业来说，这不是简单的“功能下线”，而是把低活跃定制能力从平台供给中清出去。已经依赖微调做分类、风格控制、行业术语或低延迟任务的团队，应马上确认最近 60 天推理记录、导出训练数据、准备迁移到 RAG、提示模板、评测驱动优化或第三方可控训练方案。来源：OpenAI API Deprecations（https://developer/deprecations）。

Xero 把 AI 代理入口前移到开发者工具和中小企业财务决策。 Xero Developer 页了面向 Xero API 的 Agentic SDK、开源 MCP Server、CLI、Prom

例；Xero 产品页同时强调 JAX 的审计轨迹、JAX Assure 验证、4.6 millio
rs，以及“数据不用于训练外部 AI 模型”。另据 AFR 7 月 2 日报道，Xero 正以新的
icrosoft AI 合作回应股价与战略质疑。新增变量是：财务 SaaS 不再只把 AI 放在自
记账或问答层，而是把代理、连接器、审计和办公入口合并成可执行工作流。来源：Xero
AI Toolkit（https://developer.xero.com/ai）、Xero A
ero.com/ai-in-accounting/）、AFR（https://www.afr.c
gs-off-14b-rout-with-new-microsoft-ai-pact-202606

Google AI Mode 调整食谱查询的来源呈现，内容平台仍在争夺 AI 搜索分发权。 The
ge 报道称，Google AI Mode 会在烹饪类查询顶部更突出地直接链接原始食谱来源，并显
示图片、评分和食材数量，但 AI 生成食谱仍在下方展示，部分创作者仍担心来源不透明
和错误步骤。这个产品变化的重要性在于，它把“AI 摘要是否抢走流量”转成更细的界面
分配问题：哪些来源获得首屏可见性、哪些内容被 AI 重写、错误责任由谁承担。来源：T
he Verge（https://www.theverge.com/tech/960082/go
inal-recipe-links-more-prominent）。

模型与技术进展

研究侧今天更偏“让 agent 可长期运行、可审计、可低成本训练”。 AutoMem 把文件系
统操作提升为 agent 的一等记忆动作，让模型学习何时写入、检索和组织长期记忆；Theo
ria 把答案验证拆成带证据许可的状态转移；单层 RL 论文则显示，大模型强化学习收益
可能集中在少数中间层。这三条共同指向一个方向：下一阶段的模型工程不只靠更大参数，
而靠记忆、验证和训练预算的结构化分配。来源：AutoMem（https://arxiv.org/
7.01224）、Theoria（https://arxiv.org/abs/2607.0122
//arxiv.org/abs/2607.01232）。

OpenAI 的微调收口让“后训练能力”变成平台策略问题。 微调本身仍有价值，但 7 月 2
日的限制说明，平台正在减少长尾低活跃训练负担，并把客户推向更新模型、标准化工具链
和可维护迁移路径。技术团队不能只比较微调后准确率，还要比较模型可续训性、训练数据
可携带性、基础模型退役风险和替代方案的回归测试成本。来源：OpenAI API Deprecati
ns（https://developers.openai.com/api/docs/deprec

Xero 的 MCP 与 CLI 组合说明垂直 agent 需要“系统接口”，不是只要一个聊天框。
ro 将 MCP Server 描述为让 LLM 安全连接 Xero 数据的方式，CLI 则包装
服务自治系统。这对企业软件开发者的启发很直接：如果 AI 要执行财务、采购、客服或
运营动作，产品必须把权限、数据读取、动作提交、审计和回滚做成稳定接口。来源：Xer
o AI Toolkit（https://developer.xero.com/ai）。

投融资与商业动态

Meta 被报道计划推出 AI 云业务，资本市场把 AI 算力从成本项重新看成可售资产。 Blo
omberg News / Reuters 报道称，Meta 正在规划出售过剩 AI 计算能力的云

括模型访问和原始算力租赁；Meta 尚未正式确认该计划。报道称 Zuckerberg 5 月曾表示，若出现过剩供给，出售算力“definitely on the table”；市场反应强烈，Met一度上涨约 9%-10%，CoreWeave、Nebius 等 AI 云相关股票承压。商业含义是：台把内部算力商品化，新兴 AI 云厂商的定价权会被重新评估。来源：Reuters via Investing.com（https://www.investing.com/news/stock-mass-ai-computing-capacity-via-cloud-business-bloom、The Information（https://www.theinformation.com/ud-business-push）、MarketWatch（https://www.marketebius-shares-tumble-as-meta-stands-to-become-a-frc3616）。

Xero 用行业基准数据和 Microsoft 合作对冲“AI 会不会吃掉财务软件”的疑问。 Xe6 月 29 日宣布 Industry Benchmarks in Xero Analytics，客户数据转成行业和地区 peer comparison，并用 AI 生成行动优先级；7 月 2 日报道其 CEO 以新的 Microsoft AI pact 解释公司在 AI 时代的位置。这里的商：垂直 SaaS 正在把客户数据资产产品化，既提高留存，也把会计师和小企业主的咨询对话锁回平台。来源：Xero media release（https://www.xero.comxero-introduces-industry-benchmarking-intelligenFR（https://www.afr.com/technology/xero-ceo-shrugrosoft-ai-pact-20260629-p60av3）。

OpenAI 的微调退役路径会带出一批迁移服务和替代训练需求。 7 月 2 日的资格收紧意味着一部分企业会突然发现“还能推理，但不能继续迭代”。这会利好三类供应商：能做评测与回归测试的工具、能把微调任务迁到开源或专有小模型的训练平台，以及能把微调需求替换成检索、规则和提示编排的实施服务。来源：OpenAI API Deprecations（helopers.openai.com/api/docs/deprecations）。

政策、伦理与安全

美国 AI 网络安全行政令首批 30 天任务在 7 月 2 日到期。 白宫 6 月 2 日 ExeOrder 14409 要求，在 30 天内推进国家安全系统、国防系统和民用联邦系统的 AI 网络防御；CISA 需发布 Binding Operational Directives 或其他指导，御、扩展 AI 防御工具，并便利关键基础设施获得网络安全工具和必要时的前沿模型能力；财政部还需组建 AI cybersecurity clearinghouse，协调漏洞扫描、验证丁分发。今天的新增意义是：政策从“是否允许前沿模型”转向“如何把模型接入国家级防御流程”。来源：White House EO 14409（https://www.whiteho-actions/2026/06/promoting-advanced-artificial-iecurity/）。

OpenAI 微调限制也有治理含义：平台正在主动清理不可持续的长尾能力。 对模型平台而言，老模型、老评测、老微调任务和低活跃客户都会形成安全、维护和合规负担。7 月 2

日节点说明，能力下线会越来越像云服务生命周期管理，而不是消费者软件的功能更新。采购方需要把“可训练多久、可迁移什么、下线通知多长、是否能买 dedicated capacity”写进技术和商业评估。来源：OpenAI API Deprecations（https://dev
om/api/docs/deprecations）。

Google AI Mode 的来源呈现调整继续暴露 AI 搜索的责任边界。 食谱查询看似轻量，但它同时涉及创作者流量、用户安全、错误步骤和来源署名。Google 更突出原始来源链接，是对出版方压力的产品回应；但只要 AI 生成内容仍占据同一页面，平台就必须解释推荐、引用、错误纠正和责任分担。来源：The Verge（https://www.theverge.
082/google-ai-mode-is-making-original-recipe-link

X 平台高信号

1. 信号标题：OpenAI 自助微调 7 月 2 日资格收紧

类型：平台访问 / 产品生命周期

来源或链接：https://developers.openai.com/api/docs/depr

核心观点：今天的新增变量是，未在过去 60 天运行过微调模型推理的组织，从 2026-07-02 起不能再创建新的微调任务；现有推理继续可用，直到基础模型退役。

为什么重要：这把微调从“随时可回来的功能”变成“需要持续活跃才能保留迭代权”的平台资源。

影响：企业要立刻核查微调模型调用记录和训练数据归档，并为 2027-01-06 的最终新建任务截止日准备迁移方案。

验证状态：已由 OpenAI 官方 API deprecations 页面验证。

2. 信号标题：Meta 被报道计划出售过剩 AI 算力

类型：基础设施商业化 / 云竞争

来源或链接：https://www.investing.com/news/stock-market
ess-ai-computing-capacity-via-cloud-business-bloc
；https://www.theinformation.com/briefings/meta-pl

核心观点：Reuters 引述 Bloomberg 称 Meta 正规划云业务出售过剩 AI 计算
Information 也报道了相关计划；Meta 尚未正式确认。

为什么重要：如果 Meta 把内部算力外售，AI 云市场会从“GPU 稀缺”进入“超大平台闲置容量再分配”的竞争。

影响：CoreWeave、Nebius、Runpod 等 AI 云供应商会面对更强的价格和信用对手

公司则可能获得更多短期算力选择。

验证状态：已由 Reuters 转述 Bloomberg 与 The Information 报道
方确认仍待观察。

3. 信号标题：美国 AI 网络安全行政令首批 30 天动作到期

类型：政策执行 / 网络安全

来源或链接：https://www.whitehouse.gov/presidential-act
-advanced-artificial-intelligence-innovation-and-

核心观点：Executive Order 14409 要求 CISA、财政部、国防与国家安全相关部
天内推进联邦系统防御、AI 防御工具、关键基础设施接入和漏洞清理协同；以 6 月 2 日
签署日计算，今天是首批期限。

为什么重要：这让前沿模型安全从发布前评估，进一步进入政府网络防御和漏洞修复流程。

影响：安全厂商、关键基础设施运营商和前沿模型公司会被拉进更具体的协作链条，采购与
合规会更关注模型是否能服务防御任务。

验证状态：已由白宫行政令原文验证；各部门具体执行文件需继续跟踪。

4. 信号标题：Xero 将财务 SaaS 数据接入 MCP 与 AI 代理工具链

类型：垂直应用 / 开发者平台

来源或链接：https://developer.xero.com/ai；https://www.x
ing/

核心观点：Xero 面向开发者提供 Agentic SDK、MCP Server、CLI 和提示样
产品页强调 JAX 的审计、验证和数据保护。

为什么重要：财务软件的 AI 化正在从“自动录入和问答”走向“可执行、可审计、可连
接第三方工具”的代理入口。

影响：会计、税务、现金流和应收应付场景会成为垂直 agent 的高价值试验田，但权限控
制和操作留痕会决定企业接受度。

验证状态：已由 Xero 官方开发者页面和产品页面验证。

5. 信号标题：Xero 用行业基准数据强化 AI 分析入口

类型：数据产品 / 垂直 SaaS

来源或链接：https://www.xero.com/us/media-releases/xero

enchmarking-intelligence-for-small-businesses/

核心观点：Xero 的 Industry Benchmarks 把匿名聚合的小企业数据转成行业和地
指标，并用 AI 生成行动优先级。

为什么重要：这类功能把 SaaS 历史数据变成决策产品，竞争点不只是模型能力，而是平
台能否提供同行参照和可执行建议。

影响：中小企业软件会更频繁地把“数据网络效应”包装成 AI 决策能力；独立工具若没
有数据规模，会更难复制同类洞察。

验证状态：已由 Xero 官方新闻稿验证。

6. 信号标题：Google AI Mode 调整食谱来源链接展示

类型：搜索分发 / 内容生态

来源或链接：https://www.theverge.com/tech/960082/google
ginal-recipe-links-more-prominent

核心观点：Google AI Mode 将在烹饪查询顶部更突出地直接链接原始食谱来源，但仍保留
AI 生成食谱内容。

为什么重要：这说明 AI 搜索平台正在用界面位置来回应出版方和创作者对流量流失的压
力。

影响：品牌、媒体和内容站需要重新优化可被 AI 搜索引用的结构化内容，同时继续监控
AI 摘要错误带来的责任风险。

验证状态：已由 The Verge 报道验证；Google 后续是否扩展到更多垂直类目需继续跟踪
。

前沿研究速递

1. AutoMem：把长期记忆管理训练成 agent 的独立技能

做了什么：论文把文件系统操作提升为 agent 的一等记忆动作，让模型自己决定写什么、
何时检索、如何组织记忆；再用强模型审查完整轨迹并迭代记忆结构，同时从好的记忆决策
中训练模型。来源：arXiv:2607.01224 （https://arxiv.org/abs/

新在哪里：它把“记忆”从手写 prompt 和外部插件，变成可优化、可训练的认知技能；
在 Crafter、MiniHack、NetHack 上，仅优化记忆就让基础 agent 表现提升

潜在应用方向：长周期软件开发 agent、研究助理、企业流程 agent、游戏和仿真环境中
的持续任务执行。

一句话判断：长期 agent 的瓶颈不是记得更多，而是学会何时记、何时忘、如何把记忆变成行动优势。

2. Theoria：把非形式化推理答案拆成可审计状态转移

做了什么：论文提出 Theoria，把候选解答重写成一串带类型的状态转移，每一步必须由引用、计算或题目事实授权；任何连续状态差异都要被解释。来源：arXiv:2607.01223（https://arxiv.org/abs/2607.01223）。

新在哪里：它试图补上形式化证明覆盖不足和 LLM judge 不透明之间的空白；在 HLE-Verified Gold 上认证 105 题，strict precision 为 91.4%，并在对式 judge 更擅长抓隐藏前提和虚构引用。

潜在应用方向：高风险问答、法律和科研论证审查、代码变更解释、企业知识库答案验真。

一句话判断：可信 AI 不一定每次都要完整形式化，但必须让关键推理步骤能被独立挑战。

3. 单层 RL：大模型后训练收益可能集中在少数中间层

做了什么：论文系统研究 RL 后训练在 Transformer 层间的分布，发现只训练单个层就能恢复大部分全参数 RL 收益，有时甚至超过全参数训练。来源：arXiv:2607.01232（https://arxiv.org/abs/2607.01232）。

新在哪里：结果跨 Qwen3、Qwen2.5、三种 RL 算法和数学、代码、agent 决策等任务稳定，并显示高贡献层集中在模型中部。

潜在应用方向：低成本后训练、企业私有模型适配、快速任务对齐、资源受限环境中的 agent 微调。

一句话判断：如果结论经更多模型验证，RL 后训练的成本结构会被重写，企业不必默认全参数更新才有价值。