由 Codex 自动生成

# AI前沿发展日报 | 2026-05-02（Asia）

日期：2026-05-02｜覆盖窗口：2026-05-01 00:00 - 2026-05-02 i）

## 今日总览

今天的高信号不在单一模型发布，而在 AI 进入“可控部署”的硬约束阶段。美国防务系统把 OpenAI、Google、Microsoft、AWS、NVIDIA、SpaceX 和 Re络，说明 frontier AI 正从通用生产力工具进入国家安全基础设施。企业侧，Microsof Agent 365 在 2026-05-01 GA，进一步确认 agent 的竞争焦点正在从“能不转向“能不能被观察、授权、审计和处置”。中国方向，Huawei AI 芯片收入预期大幅增长，显示本土算力替代已经从政策口号进入采购和收入兑现。OpenAI-Musk 庭审则提醒，AI 公司的治理结构会直接影响融资、IPO、政府合同和企业客户信任。

## 今日三条结论

1. Frontier AI 正在被纳入国家级关键系统，模型供应商的政治可信度、安全边界和部署架构会变成商业资产。
2. Agent 的企业化不是“更聪明的机器人”，而是新的身份与权限治理对象；没有控制平面的 agent 平台会很难进入核心流程。
3. 中国 AI 算力链开始出现可量化替代，NVIDIA 在中国市场的优势仍强，但 Huawei、mbricon 等本土供应商的收入和采购份额正在改变谈判结构。

## 今日 Top 5 大事件

### 1. 美国防务部门与 7 家 AI / 基础设施公司达成高密级网络部署协议，Anthropic 缺席

发生了什么： 美国防务部门在 2026-05-01 宣布与 SpaceX、OpenAI、Google Reflection、Microsoft 和 Amazon Web Services 达成协议，把到 Impact Level 6 和 Impact Level 7 等高密级网络环境，用于合法作战运营场景。报道还提到，GenAI.mil 平台上线 5 个月已覆盖超过 130 万名防务人员，产生数千万次 prompts，并部署数十万个 agents。Anthropic 未在名单中，背景是其部门围绕自主武器、国内大规模监控等使用边界发生争议。

为什么重要： 这是 AI 产业的边界事件。模型、云、芯片和通信公司同时进入高密级防务网络，意味着 AI 供应链已经被国家安全系统视为一体化能力，而不是单个软件采购。NVI

DIA 的出现说明硬件栈同样被纳入战略体系；SpaceX 的出现说明网络连接和边缘通信也在 AI 部署版图内。

对商业世界意味着什么： 大客户采购 AI 时会更重视“可在受限环境运行”的能力：私有部署、审计、访问控制、数据隔离、安全工程团队和政策承诺。对模型公司而言，是否能服务政府和高监管行业，会影响估值和收入质量；对企业客户而言，供应商的政治与合规风险也会进入采购评分表。

可信来源： Breaking Defense（https://breakingdefense.c
ars-7-tech-firms-to-deploy-their-ai-on-its-classi
（https://techcrunch.com/2026/05/01/pentagon-inks-
-and-aws-to-deploy-ai-on-classified-networks/）、PY
m/artificial-intelligence-2/2026/pentagon-links-w
opic-dispute/）

## 2. Microsoft Agent 365 正式 GA，企业 agent 控制平段

发生了什么： Microsoft Agent 365 于 2026-05-01 正式 GA，可作为
soft 365 计划的一部分或单独购买。Microsoft 将其定位为企业 agent 的 co
ne，能力包括 agent inventory、registry、agents map、生命周期管
uardrails、least privilege access、日志、审计、数据安全风险报告和威
rosoft 安全博客此前披露，Agent 365 定价为每用户每月 15 美元；包含 Copil
nt 365、Entra Suite 和 Microsoft 365 E5 安全能力的 Micro
零售价每用户每月 99 美元。

为什么重要： 这把 agent 从“业务部门试用工具”推入 IT 和安全预算。过去企业买 Co
pilot 是买个人生产力，现在买 Agent 365 是买 agent 的可见性、权限、合规和运
险管理。Microsoft 的优势在于它控制 Entra、Defender、Purview、Off
SharePoint 等企业身份与数据入口。

对商业世界意味着什么： Agent 平台的采购标准会被 Microsoft 重新定义：能否自动发现 agents、绑定 owner、最小权限、记录行为、检测 prompt manipulatio
ased attack chains。独立 agent 创业公司若不能接入 Entra / Okt
企业控制面，会被限制在低风险场景。

可信来源： Microsoft Agent 365 产品页（https://www.micros
oft-agent-365）、Microsoft Security Blog（https://w
rity/blog/2026/03/09/secure-agentic-ai-for-your-f
icrosoft Adoption（https://adoption.microsoft.com
agent-365/）

## ３． Ｈｕａｗｅｉ 预计 ＡＩ 芯片收入今年至少增长 ６０%，中国算力替代进入收入兑现期

发生了什么： Ｒｅｕｔｅｒｓ 引述 Ｆｉｎａｎｃｉａｌ Ｔｉｍｅｓ 报道称，Ｈｕａｗｅｉ 预计其 ２６ 年至少增长 ６０%，受中国企业对本土 ＡＩ 芯片需求推动。同期，中国本土 ＡＩ 芯片供应商已在国内服务器市场获得更高份额；此前 Ｒｅｕｔｅｒｓ 报道的 ＩＤＣ 数据显示，中国芯片厂商 ２０２５ 年交付约 １６５ 万颗 ＡＩ ＧＰＵ，在国内 ＡＩ 服务器市场占 ４１%，Ｈｕａｗｅ商中的最大交付方。

为什么重要： 这不是单纯的“国产替代”叙事，而是供应链议价权变化。美国对高端芯片出口的政策摆动，使中国云厂商和模型公司必须为长期可用性设计备用路线。Ｈｕａｗｅｉ、Ｃａｍｂｒｉｃｏｎ 等公司的增长，说明本土栈即便性能和生态仍有差距，也已经足以承接部分训练和推理需求。

对商业世界意味着什么： 中国企业的 ＡＩ 成本、模型选型和云采购会更受芯片可得性影响。跨国企业在中国部署 ＡＩ，要考虑 ＮＶＩＤＩＡ、Ｈｕａｗｅｉ、云厂商自研芯片之间的兼容性、供应稳定性和合规边界。对应用公司来说，能否在多种芯片后端上稳定运行，会成为产品化能力。

可信来源： Ｒｅｕｔｅｒｓ / Ｉｎｖｅｓｔｉｎｇ．ｃｏｍ（ｈｔｔｐｓ：//ｗｗｗ．ｉｎｖｅｓｔ-ｎｅｗｓ/ｈｕａｗｅｉ-ｅｘｐｅｃｔｓ-ａｉ-ｃｈｉｐ-ｒｅｖｅｎｕｅ-ｔｏ-ｊｕｍｐ-ａｔｒｔｓ-４６５１８３９）、Ｔｏｍ's Ｈａｒｄｗａｒｅ 引述 ＳＣＭＰ 与 ＩＤＣ 数据（ｈｔｔｃｏｍ/ｔｅｃｈ-ｉｎｄｕｓｔｒｙ/ｃａｍｂｒｉｃｏｎｓ-ｑ１-ｒｅｖｅｎｕｅ-ｈｉｔｓ-４２３-ａｉ-ｃｈｉｐ-ｍａｒｋｅｔ-ａｃｃｅｌｅｒａｔｅｓ）

## ４． ｘＡＩ 推出 Ｇｒｏｋ ４．３，低价 ＡＰＩ 与 ａｇｅｎｔ 性能成为竞争重

发生了什么： Ａｒｔｉｆｉｃｉａｌ Ａｎａｌｙｓｉｓ 报道称，ｘＡＩ 发布 Ｇｒｏｋ ４．３，并将ｇｅｎｔｉｃ ｐｅｒｆｏｒｍａｎｃｅ 与更低 ＡＰＩ 价格的模型。报道显示，Ｇｒｏｋ ４．３ 在其Ｉｎｄｅｘ 上较 Ｇｒｏｋ ４．２０ 提升 ４ 分，位于 Ｍｕｓｅ Ｓｐａｒｋ 和 Ｃｌａｕｄｅ开价格为每百万 ｉｎｐｕｔ ｔｏｋｅｎｓ １．２５ 美元、每百万 ｏｕｔｐｕｔ ｔｏｋｅｎｓ ２．Ｂｅａｔ 转载信息也称，新版 Ｇｒｏｋ 同步强化语音克隆套件和 ＡＰＩ 可用性，但仍未达到 ＯｐｅＡＩ、Ａｎｔｈｒｏｐｉｃ 顶级模型的整体状态。

为什么重要： 这说明 ｘＡＩ 的打法不是只追逐最高 ｂｅｎｃｈｍａｒｋ，而是在用价格、Ｘ 数据入口和实时分发争夺开发者。低价模型对大规模 ａｇｅｎｔ、客服、社媒分析、内容生成和中低风险自动化很敏感，因为这些场景的 ｔｏｋｅｎ 消耗比单次模型质量更能决定 ＲＯＩ。

对商业世界意味着什么： 企业会开始按任务层级路由模型：高风险推理用顶级模型，批量执行和长上下文清洗用更便宜模型。模型公司之间的竞争会更像云资源竞价，价格、速率、上下文、工具调用稳定性和部署地区会共同决定客户留存。

可信来源： Ａｒｔｉｆｉｃｉａｌ Ａｎａｌｙｓｉｓ（ｈｔｔｐｓ：//ａｒｔｉｆｉｃｉａｌａｎａｌ

unches-grok-4-3-with-improved-agentic-performance
Cloud 转引 VentureBeat (https://www.dataandcloud.co

### 5. Musk 连续三天在 OpenAI 转营利诉讼中作证，AI 公司治理成为产业

发生了什么： Reuters 报道，Elon Musk 本周在加州 Oakland 的 OpenA
讼中作证超过 7 小时，称其诉讼是在维护慈善机构制度，并围绕 OpenAI 是否偏离创立使
命、是否可转向营利结构展开争议。庭审还涉及 AI 灭绝风险专家证词是否应被采纳等问
题。OpenAI 方面则继续主张 Musk 的诉讼缺乏依据，并与其竞争利益相关。

为什么重要： 这场诉讼不只是创始人冲突。OpenAI 正在面对大规模融资、云合同、政府
合作、潜在 IPO 和企业客户依赖，其治理结构会影响投资者对控制权、利润分配、使命约
束和监管风险的判断。若法院对 AI nonprofit-to-for-profit 转换设置更高门
AI 实验室和公益结构创业公司都会受影响。

对商业世界意味着什么： 企业采购 AI 平台时，治理稳定性会成为尽调项。客户不只要问
模型是否先进，还要问供应商是否可能因诉讼、控制权争议、监管审查或使命条款被迫改变
产品路线。AI 公司越接近基础设施，治理问题越会从“法律背景噪音”变成商业连续性风
险。

可信来源： Reuters / Investing.com (https://www.invest
et-news/key-takeaways-from-musks-testimony-at-ope
ttps://www.axios.com/2026/04/30/musk-openai-safet
景 (https://www.investing.com/news/stock-market-ne
s-forprofit-conversion-can-head-to-trial-us-judge

## 商业与应用解读

大模型公司：政府和高监管行业会把“可控部署”放到模型能力之前。 美国防务高密级网
络部署说明，未来 frontier lab 的护城河不只是模型分数，还包括合规承诺、安全工程
、私有环境部署、模型行为边界和本地化支持能力。Anthropic 的缺席尤其值得跟踪：安
全原则会增强品牌信任，但也可能在特定政府收入场景中形成摩擦。

Agent / coding / workflow：Agent 365 把 agent 管理变成标
要进企业核心流程，必须具备身份、权限、工具注册、审计日志、异常检测、数据泄露防护
和撤销机制。Microsoft 和 Okta 连续推进 agent identity，意味着下一阶
“谁的 agent 更聪明”转向“谁能让安全团队批准上线”。

中国企业与内容服务场景：算力国产化会推动模型和应用更深绑定本土云。 Huawei AI 芯
片收入增长意味着中国 AI 应用公司需要更早考虑部署栈选择。内容生成、营销 agent、
客服自动化和电商运营工具如果要服务大客户，将被要求证明可在国内合规云和国产芯片栈
上运行。

模型价格战：低价模型会打开“高频低风险 agent”市场。 Grok 4.3 的价格信号说明，模型公司正在用 API 成本换取开发者工作负载。对企业来说，合理架构不是押注单一最强模型，而是建立模型路由：高价值决策用强模型，批量处理用低价模型，敏感数据用私有模型。

## X 平台高信号观点

### 1. 防务部门 CTO 账号将 7 家 AI 公司协议称为 AI-first ma分

类型：已验证事实 + 趋势信号。 多家媒体转引美国防务部门 CTO 账号在 X 上的表述：防务部门与 7 家 frontier AI model and infrastructure co力部署到 classified networks。事实主体已由 Breaking Defense、NTS 报道验证。

商业判断： X 上的官方表述显示，政府并不把这看成单次采购，而是“AI-first”组织转型的一部分。对大型企业也是同理：AI adoption 一旦进入核心流程，就会牵动架构、权限、组织流程和供应商组合。

来源： PYMNTS 转引官方 X 与新闻稿（https://www.pymnts.com/ar ence-2/2026/pentagon-links-with-7-ai-giants-after ing Defense（https://breakingdefense.com/2026/05/ s-to-deploy-their-ai-on-its-classified-networks/）

### 2. Agent 365 社区讨论集中在“agent sprawl”和 Entra

类型：趋势信号，事实部分由 Microsoft 官方验证。 Microsoft 页面说明，通过 M oft 365 渠道发布并注册 Entra Agent ID 的 agents 会自动出现在 Ag ry 中；外部 agents 需要额外注册。Reddit 和 Microsoft 365 管理员社也集中在 GA 后的 SKU、旧 Entra agent registry 迁移和治理复杂度。

商业判断： 这说明企业不缺 agent demo，缺的是统一盘点和控制面。未来 agent 项目成败会越来越取决于 admin experience，而不只是最终用户体验。

来源： Microsoft Agent 365（https://www.microsoft.co 65）、Microsoft Community Hub（https://techcommunit 365-blog/save-the-date-for-agent-365-live-ama/451 （https://www.reddit.com/r/sysadmin/comments/1t0pr hanges_a_quick_summary/）

### 3. Grok 4.3 讨论的焦点不是 SOTA，而是“便宜、快、接近可用”

类型：趋势信号，部分已由 Artificial Analysis 验证。 X / Reddit /

绕 Grok 4.3 的讨论集中在价格下降、agentic performance、上下文和实时数
时也有用户反馈视频模型稳定性仍有问题。Artificial Analysis 已验证其相对上一版的
评分提升和价格信息，但用户体验仍需继续观察。

商业判断： 开发者对“足够好 + 便宜”的关注在上升。模型市场将出现更明确的分层：
顶级模型承担复杂推理和高价值工作，低价模型吞吐大量边缘任务。

来源： Artificial Analysis (https://artificialanalys
es-grok-4-3-with-improved-agentic-performance-and
用户反馈 (https://www.reddit.com/r/grok/comments/1t0j
is_still_completely_broken/)

### 4. OpenAI-Musk 庭审让“AI 公司是否能转营利”成为公开治理议题

类型：已验证事实 + 观点信号。 Reuters 已确认 Musk 于 2026-04-28 至
在 Oakland 庭审中作证。X 和科技媒体讨论从“个人恩怨”扩展到 nonprofit cor
公益使命、AGI 收益分配和潜在 IPO。

商业判断： AI 公司越接近关键基础设施，治理结构越会被客户、政府和资本市场放大审
视。企业客户需要把供应商法律风险纳入业务连续性评估。

来源： Reuters / Investing.com (https://www.investin
ews/key-takeaways-from-musks-testimony-at-openai-
://www.axios.com/2026/04/30/musk-openai-safety-gr

## 前沿研究速递

### 1. LaST-R1：把 VLA 机器人的“物理推理”也纳入强化学习优化

做了什么： LaST-R1 提出面向 Vision-Language-Action 模型的统一框架
前引入连续 latent Chain-of-Thought 物理推理，并用 Latent-to-A
mization 同时优化推理过程和动作生成。论文报告，在 LIBERO benchmark 上只
upervised warm-up 即达到 99.8% 平均成功率；真实部署中，LAPO post
个复杂任务上较初始 warm-up policy 最高提升 44%。

新在哪里： 过去很多 VLA 强化学习只优化动作空间，推理过程仍是静态或间接的。LaST-
R1 把“想多久、如何想物理动态”也纳入可训练对象，并让推理 horizon 随任务复杂度
自适应。

应用方向： 工业机械臂、仓储操作、家庭机器人、双臂协作、需要接触和动态调整的具身
agent。

判断： 机器人 agent 的下一步不是会说更多，而是把物理推理变成可优化的控制变量。

来源： arXiv:2604.28192 （https://arxiv.org/abs/2604.

## 2． OmniRobotHome：48 个同步 RGB 摄像头构建真实家庭多人与多互平台

做了什么： OmniRobotHome 搭建了一个房间级住宅实验平台，用 48 个硬件同步 RGB 像头进行 markerless、抗遮挡、实时 3D 人和物体追踪，并与两台 Franka 机械臂在世界坐标中协同。论文关注多人、多机器人、物体在真实家庭空间中同时行动的 multiadic interaction，而不是传统的一人一机或顺序任务。

新在哪里： 真实家庭环境的核心难点是遮挡、多人并发、快速状态变化和长时行为记忆。该平台把大范围感知、实时追踪、机器人执行和长期轨迹积累放进同一系统，为安全协作和预判式辅助提供实验基座。

应用方向： 家庭服务机器人、养老辅助、厨房与清洁机器人、安全协作、长期行为建模。

判断： 具身智能要进入家庭，先要解决“多人同时在场”的感知和安全问题，而不是只在干净桌面上抓取物体。

来源： arXiv:2604.28197 （https://arxiv.org/abs/2604.

## 3． GenWildSplat：用稀疏、无位姿互联网图像实时重建户外 3D 场景

做了什么： GenWildSplat 提出一个 feed-forward 稀疏视角户外 3D 重建 scene-specific optimization。给定无位姿、光照变化、包含临时遮挡的互联网 模型预测深度、相机参数和 canonical space 中的 3D Gaussians，并用 a apter 和语义分割处理光照变化和临时对象。

新在哪里： 许多 3D reconstruction 方法依赖每个场景单独优化，在稀疏、真实互联网 图片条件下泛化差。GenWildSplat 的重点是从合成和真实数据课程学习中获得几何先验，实现无需 test-time optimization 的实时推理。

应用方向： 城市数字孪生、地图重建、旅游与地产 3D 展示、机器人导航、AR 场景理解。

判断： 如果 3D 内容生产要规模化，关键能力是从“不完美的真实图片”直接生成可用场景，而不是依赖专业采集流程。

来源： arXiv:2604.28193 （https://arxiv.org/abs/2604.