

平台限制第三方智能体访问，系统执行边界更受关注

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 10 月 18 日

摘要

人工智能产业最新的分歧，已经从模型能否完成任务，延伸至任务能否获得外部系统的合法授权。10 月 17 日，《The Verge》集中报道 Yelp、达美航空及美国金融机构针对第三方智能体访问设置的限制；在深圳举办的 GOSIM 开源创新大会当日议程中，智能体执行框架工程、边缘长上下文处理与开放模型基础设施成为多个独立技术议题；Anthropic 联合创始人 Jack Clark 在国际货币基金组织与世界银行年会期间提出，模型推动科研进步的同时，也要求更有力的跨国安全治理。产品侧，英伟达新一代支持本地 AI 的 Windows 设备已进入实机评测，计算能力、软件兼容和成本之间的矛盾开始有了具体数据。模型能回答问题还不够；访问权限、工具调用、运行环境与交付结果也得逐项检验。

Contents

一、网站主动限制第三方智能体：线上服务重新定义自动化访问权	2
二、深圳开源大会聚焦智能体执行框架：工具编排成为独立工程领域	2
三、端侧长上下文技术进入专题讨论：推理成本仍是应用架构约束	3
四、Anthropic 联合创始人警示进步与监管脱节：内部经济模型不等于宏观预测	3
趋势观察	4
参考资料	4

一、网站主动限制第三方智能体：线上服务重新定义自动化访问权

10 月 17 日,《The Verge》报道,多家线上平台已经或正在限制第三方 AI 智能体代用户访问其服务。Yelp 表示只允许通过付费数据许可途径接入的智能体;达美航空不允许第三方智能体代客直接完成机票预订;摩根大通和嘉信理财确认,出于账户安全考虑限制 AI 智能体访问客户账户。报道还梳理了亚马逊与 Perplexity 围绕智能体购物展开的诉讼争议。这里的新进展是媒体对平台具体访问规则的集中核实,不能把上述限制全部表述为 10 月 17 日同日出台的新政策。[1]

这些限制划出了一条边界:用户授权代理处理事务,并不自动意味着第三方网站已经允许程序化访问其数据库、交易和风控系统。旅行预订涉及座位库存和支付确认,金融服务则需要反欺诈、身份认证和责任认定。如果模型使用浏览器模仿人工点击,而服务方缺乏授权接口、速率控制和撤销机制,规模化使用就容易造成纠纷。企业开发者应把“网站许可—用户授权—工具权限—最终确认”设计成可验证的四层控制链,而非将网页能打开当作接口已获授权。

二、深圳开源大会聚焦智能体执行框架：工具编排成为独立工程领域

GOSIM 深圳 2026 大会的官方议程显示,10 月 17 日的“Agentic AI Summit”和“Agentic OS & App”分论坛安排了《State of Harness Engineering》以及《Agentic Harness Engineering: Observability-Driven Automatic Evolution of Coding-Agent Harnesses》等专题,由 Thoughtworks 等机构和开发者参与。大会列明的是议程与演讲主题,不能据此宣称演讲者现场发布了经独立测试的新产品。[2]

Harness 要管的不只是函数连接，还包括任务状态、工具调用、文件变更、失败重试、运行日志和预算。同一模型在不同执行框架下，可能因提示词装载、上下文裁剪、权限配置和错误恢复方式不同，而产生明显不同的端到端成功率。开发者工具选型应把任务完成率与调用次数、失败恢复、可复现日志一并测试。企业不能用单次基准分数代替真实持续运行质量。

三、端侧长上下文技术进入专题讨论：推理成本仍是应用架构约束

同一大会 10 月 17 日 “Agentic AI on Edge” 分论坛安排了 Pleias 开发者关于《How Do You Read a Million Tokens on Your Laptop? You Don't.》的报告，“Open Source Models & Infra” 分论坛还讨论模型残差连接与算力扩展。会议议程反映出小团队和开源研究者对长上下文读取、模型组织及端侧推理效率的持续关注。[2]

百万 Token 上下文并不是必须一次性全部送进模型的理由。对于长期工作的研发智能体，本地索引、分层摘要、按需检索、文件指纹及任务状态存储往往比直接扩大输入窗口更经济；真正难点在于信息检索不足时遗漏关键证据，或错误摘要使后续决策偏离原始材料。技术团队应建立固定任务集，同时测量信息召回率、首 Token 延迟、显存峰值、推理费用和引用溯源。大会主题可作为选型观察，但并非任何方案已经获得工业级长期运行证明。

四、Anthropic 联合创始人警示进步与监管脱节：内部经济模型不等于宏观预测

路透社 10 月 17 日报道，Anthropic 联合创始人 Jack Clark 在曼谷国际货币基金组织、世界银行年会期间表示，AI 能力发展可能显著加快科

研与产业创新，但生物领域滥用、网络安全及人类监督能力不足也要求跨国协调。他提到公司内部模型在特定前提下估算，美国 2030 年经济总量可能达到 44 万亿美元，而当前约为 30 万亿美元；这一数字是高度条件化的内部情景推演，不是 IMF 官方预测，更不是确定会实现的增长。[3]

讲话中的宏观数字有条件限制；科研复核、安全评估和部署治理更值得单独讨论。科学发现需要实验复核、学术可追溯和数据来源审查；高度自主的代理任务还需要可撤销授权、沙箱隔离及独立监控。科研用途与生产级执行应设置不同的风险级别，避免把演示能力误当成可无人监督运行的条件。

趋势观察

本期四条进展分别来自平台规则、开源执行框架、端侧系统研究和国际安全讨论。模型能力、用户意愿和服务方许可是三件事，不能互相替代。下一阶段真正具备竞争力的 AI 系统，应在不增加无谓推理成本的前提下，持续完成合法、可控、可追踪的真实任务。

参考资料

1. The Verge | 《Websites are closing their doors to AI agents》 | 2026-10-17 | 用途：核验 Yelp、达美航空、摩根大通、嘉信理财等平台对智能体的访问限制及争议背景。

<https://www.theverge.com/ai-artificial-intelligence/1013195/ai-agents-blocked-web>

2. GOSIM 深圳 2026 大会官网 | 《Schedule —Day 2, October 17》 | 会议日 2026-10-17 | 用途：核验 Harness 工程、端侧长上下文与开源模型的实际议程及报告人员。

<https://shenzhen2026.gosim.org/schedule/>

3. Reuters | 《AI rapidly improving, could vastly boost US GDP, Anthropic's Clark tells policymakers》 | 2026-10-17 | 用途: 核验 Jack Clark 演讲、风险警示及内部情景预测的限定条件。
<https://www.reuters.com/world/china/anthropics-clark-say-s-ais-impact-accelerating-quickly-could-vastly-boost-us-gdp-2026-10-17/>
4. NVIDIA 官方新闻室 | 《NVIDIA RTX Spark PCs Available Today》 | 2026-10-16, 技术背景 | 用途: 核验支持本地模型的 PC 实际上市与厂商公布的统一内存配置。
<https://nvidianews.nvidia.com/news/nvidia-rtx-spark-pcs-available-today-a-new-beginning-for-windows-pcs>
5. The Verge | 《A week with RTX Spark: everything we've learned using Nvidia's new laptops》 | 2026-10-16, 独立评测背景 | 用途: 区分厂商宣称的本地算力能力与实际设备价格、应用兼容情况。
<https://www.theverge.com/tech/1012748/nvidia-rtx-spark-windows-arm-laptops-asus-hp-lenovo-impressions>
6. GOSIM 深圳 2026 大会官网 | 《The New Developer Ecosystem in Agentic Era》 | 会议日 2026-10-17 | 用途: 佐证智能体开发者生态专题; 仅表示会议议程。
<https://shenzhen2026.gosim.org/schedule/>
7. GOSIM 深圳 2026 大会官网 | 《Agentic Harness Engineering: Observability-Driven Automatic Evolution of Coding-Agent Harnesses》 | 会议日 2026-10-17 | 用途: 佐证可观测性驱动的执行框架研究议题。

<https://shenzhen2026.gosim.org/schedule/>

联系我们，请扫描二维码



新质生产力工作委员会
官方公众号



工业智能算网
gyznsw.cn

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。

网站地址：<https://gyznsw.cn>