

AI 技术每日分析：MCP 转向无状态架构，智能体基础设施进入协议化扩展阶段

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 7 月 29 日星期三

摘要

本期 AI 技术动态集中在协议基础设施、模型分发、软件供应链和评测时效性四个方向。Model Context Protocol 发布 2026 年 7 月 28 日版规范，将核心通信机制改为无状态架构，降低智能体工具服务器的横向扩展成本；GitHub 同步把 Grok 4.5 接入 Copilot，模型竞争继续向开发工具入口和并行工具调用延伸。智能体自动编写代码、调用依赖和运行持续集成流程后，软件供应链风险也随之扩大。GitHub 开始对可疑 workflow 实施执行前审批，并扩大恶意软件包告警范围。与此同时，一项针对 40 篇生成式 AI 评测研究的审计显示，论文发表时所测试的模型往往已经被新版本替代，AI 评测需要从“论文发布时间”转向“模型版本和测试时间”管理。

目录

一、MCP 转向无状态架构，智能体工具协议开始按照互联网方式扩展	2
二、Grok 4.5 进入 GitHub Copilot，模型分发继续向开发工具集中	2
三、GitHub 加固 npm 和 Actions，供应链安全从扫描转向阻断	3

四、AI 评测出现 “证据半衰期”，论文发表时模型可能已经过时	4
趋势判断	4
参考资料	5

一、MCP 转向无状态架构，智能体工具协议开始按照互联网方式扩展

Model Context Protocol 于 7 月 28 日发布新版规范。核心变化是将协议调整为无状态架构，使 MCP 服务器可以像普通 HTTP 服务一样被缓存、路由和横向扩展，不再要求基础设施持续保存客户端会话。Cloudflare、AWS、Google Cloud、微软等平台已宣布支持或参与新版规范。

此前的 MCP 实现通常包含会话初始化、连接状态和后端存储。当大量智能体并发调用同一组工具时，开发者需要维护会话数据库、连接粘性和故障恢复机制。新版规范移除了会话与 initialize 流程，客户端还可以并行完成连接握手。GitHub MCP Server 升级后取消了 Redis 会话读写，减少了每次工具调用前的数据库访问。

新版协议还引入扩展机制，支持 MCP 应用、企业统一授权和长时间运行任务。MCP 由“模型连接工具的接口”逐渐演变为智能体基础设施协议，后续竞争重点将包括身份管理、审批流程、任务状态、审计日志和跨平台兼容性。

二、Grok 4.5 进入 GitHub Copilot，模型分发继续向开发工具集中

GitHub 宣布 Grok 4.5 开始进入 Copilot 模型选择器。该模型提供最高 50 万 Token 上下文，支持文字和图像输入，并允许开发者选择低、中、高三档推理强度。GitHub 称，其内部测试中，Grok 4.5 在终端编程、并行分发工具和多步骤任务方面表现较强。

Grok 4.5 将陆续进入 Visual Studio Code、Visual Studio、Copilot CLI、云端编程智能体、JetBrains、Xcode 和 Eclipse 等入口。对于企业版和商业版用户，管理员需要主动启用相关模型策略，默认状态下并不会自动开

放。

这一变化说明，开发者不再需要在不同模型网站之间切换，而是在同一个编程平台内根据任务类型选择模型。模型厂商获得用户的关键方式，也从独立聊天产品转向 IDE、代码仓库、命令行和云端任务代理。

三、GitHub 加固 npm 和 Actions，供应链安全从扫描转向阻断

GitHub 总结了近期针对 npm 和 GitHub Actions 供应链攻击的防护措施。此类攻击通常先窃取维护者账户或利用不安全的持续集成工作流，再获取发布凭据、篡改软件包，并通过依赖关系向更多项目传播。GitHub 认为，供应链攻击由多个薄弱环节连接形成，单一安全功能无法完整阻断。

针对高影响力 npm 账户，用户修改邮箱或使用双重认证恢复码后，账户会进入 72 小时只读状态。GitHub 还限制低信任工作流修改共享缓存，并允许企业控制哪些用户和事件可以触发 Actions 流程。

7 月 28 日上线的两项新功能进一步把防护前移：Dependabot 开始接收 OpenSSF 恶意软件包数据库的信息，扩大对 npm、PyPI 等生态的恶意依赖告警；GitHub Actions 会自动识别部分可疑工作流，并要求具有写入权限的协作者审核后才能执行。

编程智能体能够自动安装依赖、修改工作流和发布软件后，企业不能只检查智能体生成的代码，还需要控制依赖来源、密钥权限、构建网络和发布流程。

四、AI 评测出现“证据半衰期”，论文发表时模型可能已经过时

一项 7 月 27 日发布的预印本审计了 40 篇生成式 AI 实证研究。样本中，论文或报告出现时，所测试的最新模型中位年龄达到 281 天；35 篇研究至少包含一个已经出现后续版本的模型家族，只有 7 篇给出了精确的模型快照或日期标识，明确更新过模型证据的研究仅有 3 篇。

不同发表渠道之间也存在明显差异：该样本中，期刊论文测试模型的中位年龄为 395 天，预印本为 56 天。不过，作者特别说明，该研究采用目的性样本，不能代表整个 AI 研究领域的统计分布。

问题的关键不只是模型发布日期。相同模型名称背后，还可能发生路由、推理预算、工具、搜索、记忆和系统提示变化。企业和研究机构需要记录模型精确版本、测试时间、工具配置及调用路径，并在模型发生重大升级后补充敏感性测试。

趋势判断

第一，智能体基础设施开始从应用层向协议层下沉。MCP 无状态化之后，服务器部署、负载均衡和跨云运行将更接近成熟互联网服务。

第二，模型竞争继续向渠道竞争转移。IDE、代码仓库和命令行正在成为模型获取高价值用户的重要入口。

第三，智能体安全必须覆盖完整的软件生产链。代码审查、依赖检测、 workflow 审批、密钥管理和发布控制需要形成连续防线。

第四，AI 评测结果的有效期正在缩短。今后的模型研究不能只公布评分，还需要公布测试日期、后端版本、工具配置和后续模型更新情况。

参考资料

- Model Context Protocol Blog: 《The 2026-07-28 Specification》; 2026 年 7 月 28 日。用于核实 MCP 无状态架构、扩展机制及云平台支持情况。
<https://blog.modelcontextprotocol.io/posts/2026-07-28/>
- GitHub Changelog: 《GitHub MCP Server supports the next MCP specification》; 2026 年 7 月 23 日。用于核实会话移除、并行握手和兼容性设计。
<https://github.blog/changelog/2026-07-23-github-mcp-server-supports-the-next-mcp-specification/>
- GitHub Changelog: 《Grok 4.5 is now available in GitHub Copilot》; 2026 年 7 月 28 日。用于核实上下文长度、输入模态和工具调用能力。
<https://github.blog/changelog/2026-07-28-grok-4-5-is-now-available-in-github-copilot/>
- GitHub Blog: 《Disrupting supply chain attacks on npm and GitHub Actions》; 2026 年 7 月 28 日。用于分析软件供应链攻击链及综合防护措施。
<https://github.blog/security/supply-chain-security/disrupting-supply-chain-attacks-on-npm-and-github-actions/>
- GitHub Changelog: 《Dependabot alerts on malicious packages across more ecosystems》; 2026 年 7 月 28 日。用于核实恶意软件包告警范围扩大。
<https://github.blog/changelog/2026-07-28-dependabot-alerts-on-malicious-packages-across-more-ecosystems/>
- GitHub Changelog: 《GitHub Actions holds potentially malicious workflows for approval》; 2026 年 7 月 28 日。用于核实可疑 workflow 执行前审

批机制。

<https://github.blog/changelog/2026-07-28-github-actions-holds-potentially-malicious-workflows-for-approval/>

- arXiv: 《The Half-Lives of Generative-AI Evidence》; 2026 年 7 月 27 日。用于分析模型评测证据的时效性问题。

<https://arxiv.org/abs/2607.24032>

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>