

A I 前沿发展日报 | 2026 - 08 - 03 (A s i a)

日期：2026 - 08 - 03；覆盖窗口：2026 - 08 - 02 07:00 至 2026 - 08 - 03 a i)，并纳入经官方资料核实于 2026 - 08 - 03 生效或完成部署的产品、权限与监管变化。

今日要点

- 今天没有需要追逐的新前沿模型，真正值得处理的是三个“默认值”变化：团队 A I 从私聊工具变成 S l a c k 频道成员，数据平台的既有授权开始实际生效，欧盟 A I 素养义务进入可监督、可执法阶段。
- A n t h r o p i c 的 C l a u d e T a g 在迁移节点上把 A I 的工作上下文、长期任务和主进共享频道；入口价值上升的同时，频道边界、工具权限、t o k e n 预算和操作日志也变成部署前置条件。
- G o o g l e M e e t 与 D a t a b r i c k s 的变化都提示企业：A I 工作流的风险常藏在管值和历史授权里，而不是模型本身。一次产品更新就可能让原本无效的权限变得有效，或为未来自动记录会议预先打开开关。
- 资本侧没有达到入选门槛的新大型融资交易；当天更清晰的信号来自 A b u D h a b i 的 H u b 7 1 + A I 招募截止，现金、服务资源与创始人长期落地被打包成同一笔区域产业政策交易。

今日结论

- 1 . 企业 A I 正从“个人调用一个助手”转向“团队共享一个有记忆、可异步执行的主体”；采购重点应随之从席位数转向身份隔离、工具最小权限、预算上限与可追责日志。
- 2 . 管理后台里的旧授权和默认开关已经是 A I 风险面。组织必须把产品发布说明纳入持续权限审计，否则今天看似无效的授权，可能在供应商改动语义后自动获得删除、转移所有权或自动记录数据的能力。
- 3 . A I 合规正在进入可证明阶段：培训过员工并不等于完成义务，企业需要能说明谁使用何种 A I、面对什么风险、接受过什么针对性指导，以及如何持续更新这些措施。

A I 产品与应用

C l a u d e T a g 接替旧版 S l a c k 应用，团队 A I 从被动问答转为共享执

A n t h r o p i c 已将 C l a u d e T a g 作为 C l a u d e E n t e r p r i s e 与 T e 理员为不同频道配置独立身份、工具和访问，成员可在频道内共同委派任务；C l a u d e 能积累经授权的频道上下文、异步执行数小时或数天的任务，并在启用 a m b i e n t b e h a v i o r 后主动跟进未完成事项。A n t h r o p i c 的官方发布说明称，C l a u d e T a g 将替代旧版 C l

in Slack 应用；关于 8 月 3 日自动迁移节点，目前可由产品报道交叉确认。Anthropic 官方发布 (<https://www.anthropic.com/news/introducing-ld>) (<https://www.computerworld.com/article/4189055-to-turn-workplace-ai-from-a-personal-assistant-i>)

重要变化不是多了一个聊天入口，而是同一个 AI 身份开始服务多人、读取持续上下文并调用真实工具。企业上线前至少要完成三件事：按业务域拆分 Claude 身份，给频道设置月度 token 上限，并验证管理员日志能把每次行动追溯到具体请求者。共享记忆若没有权限隔离，会把“效率工具”迅速变成跨团队数据泄漏面。

模型与技术进展

WIDE 把动态剪枝下沉到每个 token，兼顾 prefill 与 decoding

WIDE (<https://arxiv.org/abs/2607.28418>) 提出 token n 自行选择注意力头组与 FFN 通道组，并通过 mask 重排、block 跳过和定制 kernel 细粒度稀疏真正转成推理加速。论文报告，在 50% 稀疏度下，相比当时最强动态深度剪枝提升 55.1%；kernel 级加速最高达到 prefill 1.98 倍、decoding 4 别达到 1.68 倍和 1.55 倍。

这条路线比单纯减少模型层数更贴近生产负载：不同 token 可以获得不同计算预算，同时覆盖输入处理与逐 token 生成两个阶段。若结果能在更多模型、批量大小和硬件上复现，服务商可在不更换基础模型的情况下压低延迟和单位推理成本；当前数字仍是论文环境结果，不能直接等同于云端账单降幅。

投融资与商业动态

Hub71+ AI Cohort 20 截止：资金、生态资源与长期落地绑定

Abu Dhabi 的 Hub71+ AI 于 8 月 2 日结束 Cohort 20 的当期申请计划于 2027 年 2 月启动。官方资料显示，入选公司可获得 25 万迪拉姆现金（通过 SAFE 换取股权）和 25 万迪拉姆灵活服务资源；表现优秀且持续扎根 Abu Dhabi 的公司还可再获得最高 25 万迪拉姆、对应额外股权的追加支持。至少一名创始人需长期迁入并在当地组建团队。Hub71 项目说明 (<https://www.hub71.com/program/hub71>) 官方 FAQ (<https://www.hub71.com/index.php/faqs>)

这不是一笔单纯的加速器补贴，而是“资本 + 云与算力伙伴 + 监管通道 + 区域总部”组合。对早期 AI 公司，实际代价是 SAFE 稀释、迁移成本和区域经营承诺；对 Abu Dhabi，现金只是获客成本，目标是把模型应用、人才和后续融资活动留在本地。当天未发现可由官方或一级媒体确认、且重要性更高的新大型 AI 融资交易。

政策、伦理与安全

欧盟 AI 素养义务从 8 月 3 日进入监督与执法期

欧盟委员会最新问答确认，《AI Act》Article 4 自 2025 年 2 月 2 日起已要求系统提供者与部署者采取措施提升员工及代表其操作 AI 人员的 AI 素养；监督和执法规则从 2026 年 8 月 3 日起适用。7 月生效的 Digital Omnibus 修订保留了要求达到某个统一、明确的“充分”水平。欧盟委员会 AI literacy 问答 (<https://digital-strategy.ec.europa.eu/en/faqs/ai-literacy-questions>)

今天的新增变量不是企业突然需要开一门通识课，而是监管者可以开始检查措施是否与人员经验、业务场景、AI 系统风险及受影响群体相称。通用在线课程只能作为底座；客服、招聘、信贷、内容发布和高权限 agent 应分别保存角色清单、培训记录、场景化测试、更新频率与纠错流程。可审计的能力建设记录将比一张结业证更有价值。

X 平台高信号

1. Claude Tag 的迁移节点把共享 AI 身份推入正式运营

信号标题：旧版 Claude in Slack 被团队型 Claude Tag 接替
类型：产品入口变化 / 企业协作

来源或链接：Anthropic 官方发布 (<https://www.anthropic.com/news/claude-tag>)；Computerworld 迁移日期报道 ([https://www.computerworld.com/article/4189055/anthropics-claude-tag-aims-to-turn-workplace-stant-into-a-teammate.html](https://www.computerworld.com/article/4189055/anthropics-claude-tag-aims-to-turn-workplace-ai-stant-into-a-teammate.html))

核心观点：8 月 3 日的变化是迁移节点到达；新入口不只回应 @ 提及，还能在授权频道中积累上下文、运行长期任务，并在开启主动行为后跟进未解决事项。

为什么重要：同一个 AI 身份开始被多人共同使用，权限、记忆和责任不再天然属于单一用户。

影响：管理员应按部门拆分身份与连接器，限制频道预算，并确认每个动作都能关联到请求者；敏感频道不应沿用宽泛的旧版 Slack 应用权限。

验证状态：产品能力和替代关系由 Anthropic 一手发布确认；8 月 3 日自动迁移日期来自 Computerworld 产品报道，Anthropic 可公开检索页面未单独列出该绝对日期，属于经二级来源交叉确认。

2. Databricks 历史 MANAGE 授权开始实际生效

信号标题：MANAGE 不再要求对象本身的 USE 权限
类型：平台权限变化 / 数据治理

来源或链接：Databricks 官方发布说明 (<https://docs.databricks.com/se-notes/whats-coming>)

核心观点：从 8 月 3 日起，持有 catalog 的 MANAGE 即可管理该 catalog，ma 时只需父 catalog 的 USE CATALOG 加该 schema 的 MANAGE，USE SCHEMA。父容器权限仍然保留。

为什么重要：过去因缺少 USE 而未发挥作用的历史 MANAGE 授权会自动变成有效管理能力。

影响：权限持有人可能立即获得修改授权、转移所有权或删除对象的能力；运行 RAG、agent 数据与 MLflow 资产的组织应当盘点 MANAGE grants，而不是只检查查询权限。

验证状态：生效日期、权限矩阵、不变项和官方审计建议均由 Databricks 一手发布说明确认。

3. Google Meet 的 AI 会议记录默认值新增“三人以上”选项

信号标题：自动 AI 记笔记管理员设置到达预计全量部署日

类型：默认设置变化 / 会议数据

来源或链接：Google Workspace 官方更新 (<https://workspaceupdates.google.com/2026/07/>)

核心观点：Google 预计在 8 月 3 日前完成新的管理员设置部署，允许只对三人及以上会议预设自动启用 Take notes for me；Business Standard 与 Plus、Frontline Plus 与教育相关版本默认关闭。

为什么重要：虽然终端用户体验要到 9 月 21 日以后才受影响，但今天起管理员已经可以看到并决定未来的自动记录默认值。

影响：组织应在 9 月生效前明确哪些会议允许生成转录和摘要，并把客户通话、HR 面谈、法律讨论及跨境会议的同意要求写进设置策略。

验证状态：设置范围、版本差异、8 月 3 日完成日期及“9 月 21 日前不影响用户”的边界均由 Google Workspace 一手更新确认。

4. Hub71 把逾期申请自动顺延到下一批次

信号标题：Cohort 20 截止后申请不会被拒绝，而是转入后续批次

类型：资本准入变化 / 区域落地

来源或链接：Hub71+ AI 官方项目页 (<https://www.hub71.com/program/>)；Hub71 官方 FAQ (<https://www.hub71.com/index.php/frequently-asked-questions/>)

核心观点：Cohort 20 的 8 月 2 日截止已经过去；官方明确，截止后提交的申请仍会被接收，但会进入下一批次，而非参与计划于 2027 年 2 月启动的本批项目。

为什么重要：这改变的是获得现金、服务资源和当地合作伙伴支持的时间，而不是申请资格本身。

影响：需要短期进入 UAE 市场的 AI 创业公司不能把逾期申请当作本轮融资替代；应单独安排 runway、签证和客户试点，并评估最高 75 万迪拉姆支持对应的股权与迁移承诺。

验证状态：截止日期、项目启动时间、逾期处理方式、现金与服务资源金额均由 Hub71 官方页面确认。

5. 欧盟 AI 素养执法不要求统一合格线

信号标题：Article 4 可执法，但企业措施仍按具体风险判断

类型：监管执法 / 人员能力

来源或链接：欧盟委员会官方问答 (<https://digital-strategy.ec.europa.eu/en/ai-literacy-questions-answers>)

核心观点：8 月 3 日开始适用监督与执法规则；7 月修订后的新事实是义务继续存在，但法律不规定单一或统一的“充分”素养等级。

为什么重要：没有统一考试并不等于无需证明。监管判断会回到人员经验、使用环境、系统风险和受影响对象。

影响：企业应按角色保存培训、场景测试与更新证据；高权限 agent 操作员、招聘人员和面向公众的内容团队不能只依赖同一套入门课程。

验证状态：执法起始日、义务沿革及修订后的适用边界均由欧盟委员会一手问答确认。

前沿研究速递

OSReward：先评估“评委”，再训练电脑操作 agent

做了什么：OSReward (<https://arxiv.org/abs/2607.28609>) 操作轨迹评测视觉语言模型能否正确判断 agent 是否完成任务，并发布 OSReward-Hard OSReward-Multi、10 万条带推理标注的 OS-Shepherd-100K，以及 9B reward model。

新在哪里：研究发现前沿 VLM 评委普遍存在宽松偏差，容易把失败运行判为成功；可靠的商业模型成本过高，开放模型则明显落后。作者训练的 OS-Shepherd 报告称，可用比前沿商业评委低 30%—60% 的成本提供相近判断质量。

潜在应用方向：GUI agent 评测、轨迹数据清洗、强化学习奖励、企业自动化验收与失败回放。

一句话判断：电脑操作 agent 的扩张瓶颈不只是“会不会做”，还包括“能否低成本确认真的做成”；论文标注为 work in progress，成本与可靠性结论仍需独立复现。

PAC-MAN：只用头戴相机，让人形机器人做全身动态避障

做了什么：PAC-MAN (<https://arxiv.org/abs/2607.28623>) 将学习和部署时可获得的头戴深度视觉结合，训练 Unitree G1 对飞来的球做全身躲避；训练阶段计算球到每个身体 link 的间距，部署时只输入分割后的深度图。

新在哪里：论文在真实机器人上零样本部署轻量 Link-CBF 策略，并报告在其受控投球测试中成功率为 95%；同时说明更精细的 Joint-CBF 在球状态准确时最好，但固定相机观测不足时会退化，凸显安全控制必须受可观测性约束。

潜在应用方向：仓储与工厂人形机器人、动态避碰、近人作业、受限传感器条件下的安全策略训练。

一句话判断：安全先验只有在机器人真正看得见相关变量时才有用；95% 来自特定装置与

任务，距离通用工业安全认证仍有很长路径。

SCOPE：把供应链多个部门的决策联成一个端到端策略

做了什么：SCOPE (<https://arxiv.org/abs/2607.28488>) 将商品送请求表示为 token，用共享运营表示依次决定选品、供货来源、补货频率和配送路径，并以最终系统级效用共同评价整套计划。

新在哪里：它不再分别优化库存、补货和路线后再拼接，而是让每一步读取前序形成的部分计划。作者在叮咚买菜与京东的真实运营数据上报告，跨阶段联合策略持续优于分段优化和常用业务基线。

潜在应用方向：生鲜零售补货、城市配送、库存与运力协同、跨部门运营 agent、情景模拟。

一句话判断：agent 在企业里的高价值可能来自联动原本分散的决策权，而不只是自动执行单个任务；论文尚未给出足以外推到其他供应链的公开长期线上结果。