万联证券 WANLIAN SECURITIES

智能体终端管理规范落地，安全治理同步完善

——计算机行业跟踪报告

同步大市(维持)

2026 年 11 月 09 日

行业核心观点：

上周，沪深300上涨1.73%，创业板指上涨2.14%，申万计算机行业指数上涨6.85%，分别跑赢沪深300和创业板指5.13和4.71个百分点，在申万各一级行业中排名第4位。上周，工业和信息化部发布《关于加强智能体终端设备进网管理的通知》（以下简称《通知》），围绕加强智能体与终端适配、改进进网管理、强化现网升级和健全智能体分发管理机制四方面明确工作任务。我们认为，《通知》提出开展智能体和终端适配及改进进网管理，为智能体终端提供规范框架，加强了终端厂商和应用开发者安全责任，有助于推动新一代智能终端创新发展同时提升用户信任，为产业协同提供支撑。建议关注AI终端、智能体应用及终端安全管理相关机会。OpenAI发布网络安全专用模型GPT-6 Cyber，面向经授权的漏洞发现、利用验证、渗透测试和安全修复任务，官方评测显示其网络安全能力较前代提升，并同步建立分级访问与使用管控机制。我们认为，GPT-6 Cyber的发布反映出高能力模型进入网络安全等专业场景后，治理重点正由模型输出审核延伸至用户身份、授权范围、工具权限和运行过程管控。分级开放有助于在支持专业防御任务的同时控制滥用风险，也意味着模型服务商需要将安全能力嵌入产品部署和持续运营环节。随着智能体进一步接入企业系统，相关配套将影响高能力模型在安全行业的商业化应用。建议关注智能体安全、身份权限管理方向。**中长期视角下，**继续聚焦AI产业、数据产业两大投资主线。

投资要点：

产业动态：（1）人工智能：11 月 6 日，工业和信息化部对外发布《关于加强智能体终端设备进网管理的通知》。**（2）AI 大模型：**11 月 4 日，腾讯混元发布新一代大语言模型 Hy4。**（3）AI 大模型**：OpenAI 宣布推出发布网络安全专用模型 GPT-6 Cyber。

行业估值：从估值情况来看，申万计算机行业 2026 年 11 月 6 日 PE-TTM 为 105.79 倍，低于 2023-2025 年历史 PE-TTM 的均值 158.58 倍。

风险提示：中美科技摩擦；地缘政治风险；产业生态建设不及预期；应用落地不及预期；数据隐私安全风险；市场竞争加剧。

行业相对沪深 300 指数表现



数据来源：聚源，万联证券研究所

相关研究

我国人工智能推理数据量首超训练数据量，AI 产业需求重心正向应用推理延伸

从 Anthropic 招股书看 AI 大模型商业化进程及算力需求

政策推动 AI 向产业基础研发与产品智能化延伸

分析师： 夏清莹
执业证书编号：S0270520050001
电话：(0755) 8322 3620
邮箱：xiaqy1@wlzq.com.cn
研究助理： 梁源源
电话：13242092258
邮箱：liangyy@wlzq.com.cn

正文目录

1 行业周观点.....3
2 市场行情回顾.....3
3 产业动态.....4
3.1 人工智能：工业和信息化部办公厅关于加强智能体终端设备进网管理的通知.....4
3.2 AI 大模型：腾讯混元发布 Hy4，跻身开源最强，实测四大实用场景.....5
3.3 AI 大模型：OpenAI 最强网安 AI 模型 GPT-6 Cyber 登场，性能提高 51%、发现火狐 Firefox 浏览器 81 个新漏洞.....7
4 风险提示.....7

图表 1： 沪深 300、创业板指、申万一级行业指数涨跌幅（%）（上周）.....3
图表 2： 沪深 300、创业板指、申万一级行业指数涨跌幅（%）（2026 年初至 2026 年 11 月 6 日）.....4
图表 3： 申万计算机行业估值情况（PE-TTM，单位：倍）.....4

1 行业周观点

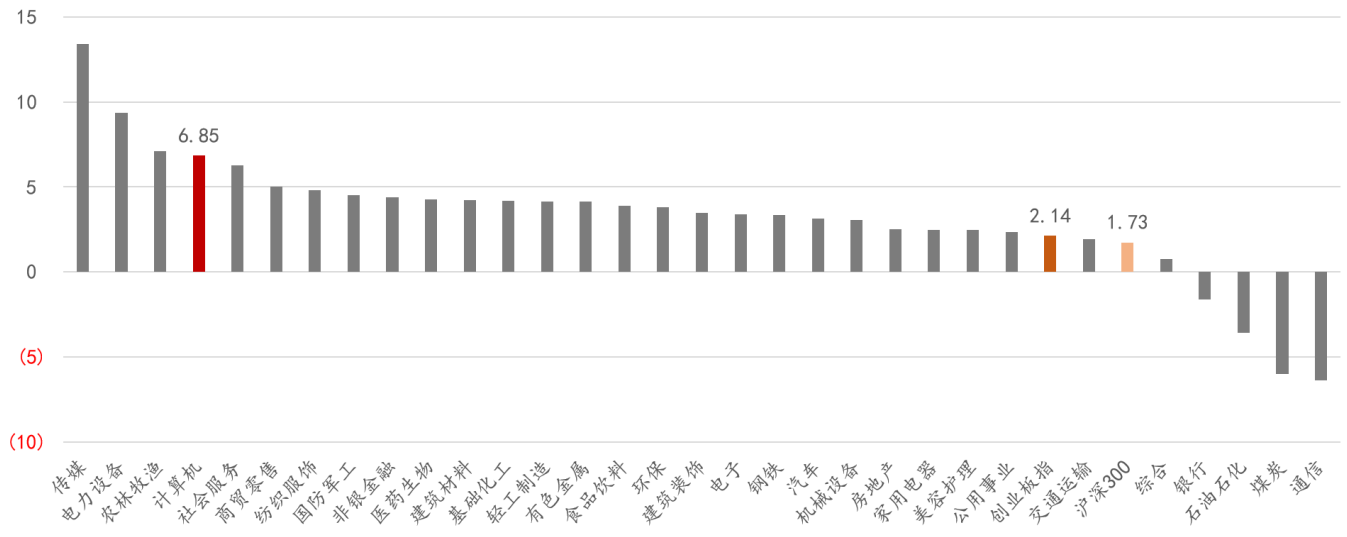
上周，工业和信息化部发布《关于加强智能体终端设备进网管理的通知》（以下简称《通知》），围绕加强智能体与终端适配、改进进网管理、强化现网升级和健全智能体分发管理机制四方面明确工作任务。我们认为，《通知》提出开展智能体和终端适配及改进进网管理，为智能体终端提供规范框架，加强了终端厂商和应用开发者安全责任，有助于推动新一代智能终端创新发展同时提升用户信任，为产业协同提供支撑。建议关注AI终端、智能体应用及终端安全管理相关机会。OpenAI发布网络安全专用模型GPT-6 Cyber，面向经授权的漏洞发现、利用验证、渗透测试和安全修复任务，官方评测显示其网络安全能力较前代提升，并同步建立分级访问与使用管控机制。我们认为，GPT-6 Cyber的发布反映出高能力模型进入网络安全等专业场景后，治理重点正由模型输出审核延伸至用户身份、授权范围、工具权限和运行过程管控。分级开放有助于在支持专业防御任务的同时控制滥用风险，也意味着模型服务商需要将安全能力嵌入产品部署和持续运营环节。随着智能体进一步接入企业系统，相关配套将影响高能力模型在安全行业的商业化应用。建议关注智能体安全、身份权限管理方向。

中长期视角下，继续聚焦AI产业、数据产业两大投资主线。1）AI产业：主要关注国内AI大模型的技术升级和产品迭代、头部AI大模型厂商的生态建设、智能驾驶、具身智能等新型智能终端及智能体的应用落地进程，以及人工智能治理的生态建设。2）数据产业：主要关注数据基础设施建设、高质量数据集等数据要素资源的开发利用、数据要素的价值释放及应用落地以及数据隐私安全。

2 市场行情回顾

申万计算机行业跑赢沪深300和创业板指，周涨跌幅位于申万31个一级行业的第4名。上周，沪深300上涨1.73%，创业板指上涨2.14%，申万计算机行业指数上涨6.85%，分别跑赢沪深300和创业板指5.13和4.71个百分点，在申万各一级行业中排名第4位。

图表1：沪深300、创业板指、申万一级行业指数涨跌幅（%）（上周）

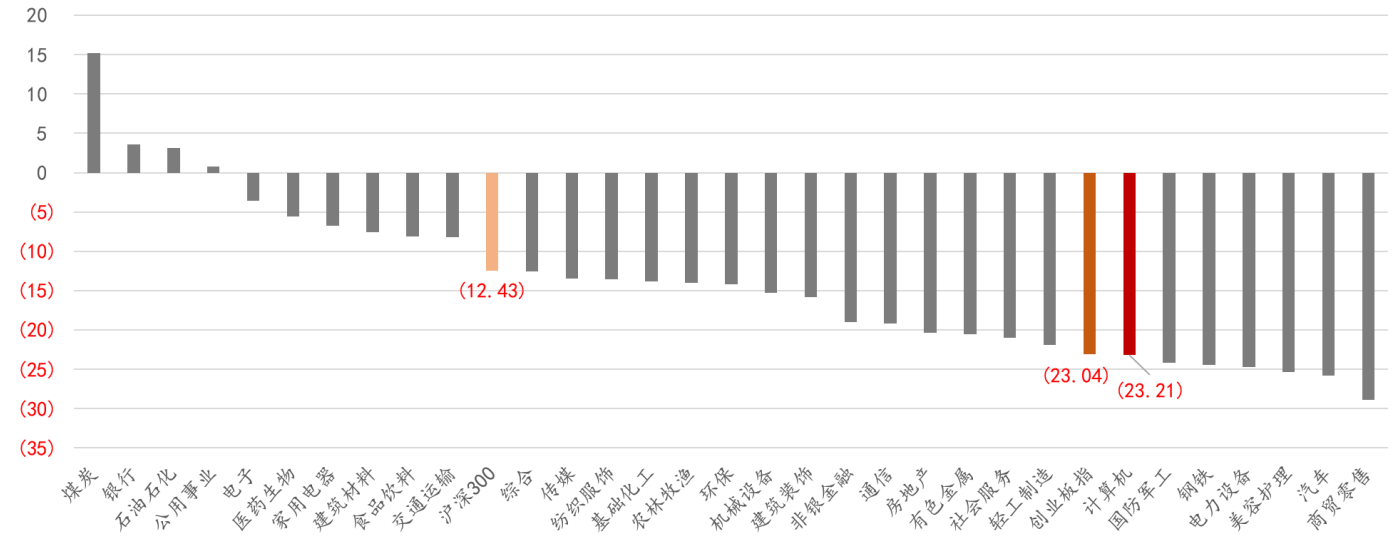


资料来源：iFinD，万联证券研究所

申万计算机行业2026年初至11月6日累计下跌23.21%，位于申万31个一级行业的第25名。2026年初至11月6日，沪深300下跌12.43%，创业板指下跌23.04%，申万计算机行

业指数下跌23.21%，分别跑输沪深300和创业板指10.78和0.17个百分点，在申万各一级行业中排名第25位。

图表2：沪深300、创业板指、申万一级行业指数涨跌幅（%）（2026年初至2026年11月6日）



资料来源：iFinD，万联证券研究所

行业估值水平低于历史中枢水平。从估值情况来看，申万计算机行业2026年11月6日PE-TTM为105.79倍，低于2023-2025年历史PE-TTM的均值158.58倍。

图表3：申万计算机行业估值情况（PE-TTM，单位：倍）



资料来源：iFinD，万联证券研究所

3 产业动态

3.1 人工智能：工业和信息化部办公厅关于加强智能体终端设备进网管理的通知

各相关单位：

智能体终端是指预置安装智能体的手机、平板、可穿戴设备等电信终端设备。为深入贯彻党的二十大和二十届历次全会精神，统筹发展和安全，促进智能体终端健康有序发展，切实维护用户合法权益，依据《中华人民共和国网络安全法》《中华人民共和

国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国反电信网络诈骗法》《中华人民共和国电信条例》《电信设备进网管理办法》等相关法律法规规章，现就有关事项通知如下。

一、工作任务

（一）开展智能体和终端适配。智能体是具备自主感知、记忆、决策、交互与执行能力的智能系统。智能体开发者应加强与终端设备的适配验证，强化权限调用、通信能力、网络与数据安全、用户权益和任务执行等方面管理，确保符合监管要求和用户预期，保障智能体兼容稳定运行。智能体开发者应规范智能体信息管理，在产品设置页面向用户公示适配验证列表，列明已完成适配的终端型号以及操作系统信息，保障用户知情权和选择权。智能体在应用分发平台上架前，其开发者应向应用分发平台提交适配验证情况。

（二）改进智能体终端进网管理。开展风险评估，完善电信设备进网检测机制，细化特别规定事项要求。预置智能体的手机、平板、可穿戴设备等智能体终端，须在进网检测中依据有关标准开展智能体适配验证；依法开展智能体终端涉诈风险安全评估和反诈能力前置性评测，落实重要通信工作要求。终端上使用的智能体应参考智能体互联系列国家标准配备唯一身份码。终端生产企业应当保证智能体终端获得进网许可证前后的一致性。智能体终端发生重大变化的，终端生产企业应当向工业和信息化部报备，并按要求开展进网检测。

（三）强化智能体现网升级管理。终端生产企业通过在线升级推送（OTA）等方式开展智能体现网升级的，应向工业和信息化部提交现网升级方案，明确现网升级时间、规模、用户群体、业务场景、服务内容、业务经营模式、网络和数据安全措施、反电信网络诈骗措施等内容，并同步做好重要通信工作。终端生产企业现网升级结束后，向工业和信息化部提交现网升级报告，经工业和信息化部组织专家评估、征求意见后方可正式向用户提供服务。

（四）健全智能体分发管理机制。应用分发平台应推动应用程序开发者，通过电子签名主动声明是否同意智能体调用，未经声明同意的，智能体不得强制调用调取应用。应用分发平台应在分发页面向用户公示智能体适配验证列表，不得为用户提供不兼容设备型号的智能体下载和安装服务。应用分发平台应加强在架智能体适配验证情况巡查，对未完成适配验证的智能体应采取限期整改、下架处置等措施。

二、工作要求

（一）加强市场监管。工业和信息化部以及各省、自治区、直辖市通信管理局加强组织协调和监督检查，建立日常与专项检查机制，做好政策解读，畅通投诉举报渠道，依法处置产品违规上市等行为，切实维护用户合法权益。

（二）强化责任落实。各相关单位主体要切实履行主体责任，严格落实本通知各项工作任务，认真组织开展智能体终端进网检测、适配验证、现网升级、分发管理等工作。细化任务分工，明确工作目标，强化内部管理和技术支撑，确保各环节落实到位。

（三）夯实能力建设。工业和信息化部组织中国信息通信研究院等相关机构持续深化智能体终端技术研究，夯实新技术分析与测试验证、事件监测与分析、问题研判与处置、场景研究与应用等能力。组织建设智能体版本和终端型号适配库，加快推进适配验证相关标准研制，加快智能体可信身份体系和管理平台建设，不断提升终端技术和创新水平。（资料来源：工业和信息化部）

3.2 AI 大模型：腾讯混元发布 Hy4，跻身开源最强，实测四大实用场景

11月4日，腾讯混元正式发布新一代大语言模型Hy4。相比此前的Hy4 preview，新模型进一步扩大预训练和后训练规模，首次引入视觉理解能力，并重点强化指令遵循、长文本理解、长程Agent及真实生产力任务表现。Hy4总参数规模为770B，采用混合专家架构，并首次支持电脑操作（Computer Use），能够结合命令行与图形界面执行复杂任务。

从评测结果来看，Hy4已跻身全球第一梯队开源模型行列，模型权重也将于近期开源。混元团队表示，尽管Hy4已经是目前最强的开源模型之一，但与顶尖闭源模型仍然存在较大差距。混元将持续稳健地扩展预训练和后训练规模，努力缩小和顶尖闭源模型的差距。针对模型在网络和生物等方面潜在的安全风险，混元以更负责任的方式进行训练、开源与发布。

在视觉理解方面，Hy4能够识别图像中的细节，分析复杂图表，并结合推理能力完成视觉数学任务。首次引入的Computer Use能力，让模型可以操作图形界面和命令行。针对Blender、CAD等专业软件，以及需要跨应用协作的长程任务，腾讯混元开展了专项训练。

与此同时，腾讯正在通过模型与产品深度协同设计（Co-Design），提升模型在真实工作中的表现。

专业金融分析是另一项重点升级。腾讯针对基金研究、证券分析和量化策略等场景，构建了数千个工作空间和上万个高质量训练任务。在213位金融专家参与、覆盖579项真实任务的众测中，Hy4获得3.04分，高于同场比较的Kimi K3.1 Pro（2.68分）、GLM-5.3（2.68分）和DeepSeek-V4.1-Flash-1017（2.97分）。针对金融等场景对信息准确性的要求，混元还开展了时效检索、多源信息整合和事实一致性校验的专项优化。

在前端和游戏开发上，Hy4进一步提升了复杂交互、业务逻辑和状态管理能力，并强化了对UE、Unity、Godot等主流游戏引擎的适配。相比preview版，GameDev和GameLogic评测成绩分别提升19.1%和9.8%。

在科学研究领域，Hy4进一步结合复杂推理、科学编程和长程任务执行能力。在覆盖7大学科、123项可执行研究任务的TenureTrail内部评测中，模型在数学构造、物理建模、地球环境和系统工程等方向展现了较强的任务处理能力。更值得关注的是，Hy4开始参与AI模型自身的研发。腾讯混元正在为递归自我改进（RSI，Recursive Self-Improvement）做准备，利用Hy4与Hyra 2.0研发框架协同优化小模型的预训练基础设施，并自动完成模型训练。混元还开源了由这一体系辅助研发的单细胞表征基础模型HyCell和物理场基础模型HyPDE，尝试将AI辅助科研的能力转化为可复用的工具。

网络安全方面，Hy4在训练中仅纳入与PoC生成、漏洞修复相关的防守性网络安全数据，同时剔除漏洞利用、逆向、渗透等攻击性训练内容，力求避免潜在进攻性能力的提升。混元组织来自腾讯玄武和科恩实验室的安全专家，围绕密码分析、逆向工程、漏洞利用等方向进行了审计，结果表明：Hy4在加密算法的逆向求解、对抗二进制混淆、漏洞利用等进攻性能力上未展现出突出风险。

生物安全方面，Hy4的开放式实验设计能力与前沿模型存在明显差距（Hy-BioExperimentBench：30.4/100）。混元组织了内部专家对轨迹进行审计，发现模型基础生物知识的掌握能力较强，但将知识转化为可执行实验方案的能力仍然有限，尚未发现其能够显著降低实施生物化学危害行为的门槛。

腾讯混元以“模型实用性”为核心原则，在不断追求智能上限的同时，为用户提供高性价比服务。（资料来源：“腾讯科技”公众号）

3.3 AI 大模型：OpenAI 最强网安 AI 模型 GPT-6 Cyber 登场，性能提高 51%、发现火狐 Firefox 浏览器 81 个新漏洞

11月6日消息，OpenAI发布博文，宣布推出发布网络安全专用模型GPT-6 Cyber，官方宣称在发现、验证和修复软件漏洞方面，比上一代GPT-5.6 Cyber实现显著提升，在ExploitGym测试中跑分相对提升51%。

ExploitGym基准主要检验模型能否利用指定远程漏洞，GPT-6 Cyber得分为48.5%，较GPT-5.6 Cyber的32.1%相对提升约51%。OpenAI还称，该模型在无部署安全提示时，99.93%的测试避免攻击授权范围外的服务；启用提示后，这一比例达到100%。

实际成效方面，OpenAI研究人员利用GPT-6 Cyber复现了1,724个Linux内核漏洞，并为其中948个开发出可用的权限提升利用程序；同时，该模型在Firefox中发现81个此前未知的高危漏洞，并向Mozilla提交证据、可复现测试和候选补丁，Mozilla已开始发布修复。

OpenAI将GPT-6 Cyber在其“准备框架”下的网络安全风险等级定为Critical（关键），高于上一代的High。公司强调，该模型初期仅向经批准的Daybreak Red客户开放，并配套滥用监测、凭据保护、沙箱、人工监督及针对关键基础设施的高风险行为拦截等安全机制。

OpenAI表示，前沿模型正进入“用AI保护软件”的关键窗口期，未来将扩大Daybreak计划覆盖面，帮助各类组织、独立研究人员和开源维护者开展漏洞研究、代码审查与补丁开发。（资料来源：IT之家）

4 风险提示

中美科技摩擦；地缘政治风险；产业生态建设不及预期；应用落地不及预期；数据隐私安全风险；市场竞争加剧。

行业投资评级

强于大市：未来6个月内行业指数相对大盘涨幅10％以上；
同步大市：未来6个月内行业指数相对大盘涨幅10％至-10％之间；
弱于大市：未来6个月内行业指数相对大盘跌幅10％以上。

公司投资评级

买入：未来6个月内公司相对大盘涨幅15％以上；
增持：未来6个月内公司相对大盘涨幅5％至15％；
观望：未来6个月内公司相对大盘涨幅-5％至5％；
卖出：未来6个月内公司相对大盘跌幅5％以上。
基准指数 ： 沪深300指数

风险提示

我们在此提醒您，不同证券研究机构采用不同的评级术语及评级标准。我们采用的是相对评级体系，表示投资的相对比重建议；投资者买入或者卖出证券的决定取决于个人的实际情况，比如当前的持仓结构以及其他需要考虑的因素。投资者应阅读整篇报告，以获取比较完整的观点与信息，不应仅仅依靠投资评级来推断结论。

证券分析师承诺

本人具有中国证券业协会授予的证券投资咨询执业资格并登记为证券分析师，以勤勉的执业态度，独立、客观地出具本报告。本报告清晰准确地反映了本人的研究观点。本人不曾因，不因，也将不会因本报告中的具体推荐意见或观点而直接或间接收到任何形式的补偿。

免责条款

万联证券股份有限公司（以下简称“本公司”）是一家覆盖证券经纪、投资银行、投资管理和证券咨询等多项业务的全国性综合类证券公司。本公司具有中国证监会许可的证券投资咨询业务资格。
本报告仅供本公司的客户使用。本公司不会因接收人收到本报告而视其为客户。在任何情况下，本报告中的信息或所表述的意见并不构成对任何人的投资建议。本报告中的信息或所表述的意见并未考虑到个别投资者的具体投资目的、财务状况以及特定需求。客户应自主作出投资决策并自行承担投资风险。本公司不对任何人因使用本报告中的内容所导致的损失负任何责任。在法律许可情况下，本公司或其关联机构可能会持有报告中提到的公司所发行的证券头寸并进行交易，还可能为这些公司提供或争取提供投资银行、财务顾问或类似的金融服务。
市场有风险，投资需谨慎。本报告是基于本公司认为可靠且已公开的信息撰写，本公司力求但不保证这些信息的准确性及完整性，也不保证文中的观点或陈述不会发生任何变更。在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的报告。分析师任何形式的分享证券投资收益或者分担证券投资损失的书面或口头承诺均为无效。
本报告的版权仅为本公司所有，未经书面许可任何机构和个人不得以任何形式翻版、复制、刊登、发表和引用。未经我方许可而引用、刊发或转载的引起法律后果和造成我公司经济损失的概由对方承担，我公司保留追究的权利。

万联证券股份有限公司 研究所
上海浦东新区世纪大道 1528 号陆家嘴基金大厦
北京西城区平安里西大街 28 号中海国际中心
深圳福田区深南大道 2007 号金地中心
广州天河区珠江东路 11 号高德置地广场