仅供内部参考，请勿外传

中国银河证券
CHINA GALAXY SECURITIES

证券研究报告 | 2026年8月31日

全球 AI 前沿观察：AI安全隐患或重塑产业监管逻辑

—— 2026年第4期

行业研究 · 行业动态

分析师：彭雅哲

010-8092 7607

pengyazhe_yj@chinastock.com.cn

S0130525020001

金融报国·客户至上

股票代码: 601881.SH 06881.HK

仅供内部参考，请勿外传

目录
CONTENTS

01. 近期AI行业大事记

02. 上游：算力与基础设施

03. 中游：大模型与平台

04. 下游：商业化应用

05. AI跟踪指标

06. 风险提示与免责声明

仅供内部参考，请勿外传

01

PART ONE

近期AI行业大事记

仅供内部参考，请勿外传

近期AI行业大事记

周日	周一	周二	周三	周四	周五	周六
8/16	8/17	8/18	8/19	8/20	8/21	8/22
● 英伟达推进Feynman GPU微架构原型开发，预计2028年下半年量产，接替Rubin及Rubin Ultra系列。  美国政府拟致信要求35个AI伙伴国不得同时加入中美两国AI生态体系。	● OpenAI 承诺在 2030 年前部署约12GW英伟达 AI 基础设施。 ● OpenAI与软银旗下 SB Energy 签署超大规模数据中心租赁协议，有望成为迄今规模最大的AI数据中心园区之一。	● 腾讯云宣布将在马来西亚柔佛州设立首个云区域。  日本内阁府公布生成式 AI 开发者指导方针草案，要求披露训练数据及数据收集方式。	● 智谱正式上线GLM-5.3 API，增强复杂编码、防御性网络安全及长程任务能力。	● 阿里巴巴正式推出智能体基座模型Qwen-UI-Agent，涵盖移动端、电脑端、网页端及Deep Search环境。	● 博通据悉拟举债超600亿美元，为 Anthropic 等 AI 芯片项目提供融资。	● 英伟达 AI 服务器据悉将涨价逾15%，主要受存储芯片成本上涨影响。 ● OpenAI将于未来3个月内下调 GPT-5.6 Sol API 与 Credit 调用价格逾20%。
8/23	8/24	8/25	8/26	8/27		
● 英伟达斥资60亿美元获取 Poolside 技术授权及人才， 开发对标 DeepSeek 的开源权重 AI 模型。 ● 阿里拟向美国境外投资者配售新股，融资总额约800亿美元，用于投资全球 AI 能力。	● SK海力士开发混合键合技术，推动HBM由最高16层向20层以上堆叠升级。 ● 字节跳动整合旗下办公 AI 产品团队，将TRAE、扣子融入豆包体系。 ● 小鹏机器人完成首轮超 9 亿美元融资，投后估值超 63 亿美元。	● 字节跳动发布Agent产品“豆包工作”。 ● 苹果发布M6与M5 Ultra芯片，首次采用2nm制程及四芯片架构，强化端侧AI能力。	 工信部明确“十五五”期间“人工智能+制造”推进路径。截至6月底，我国智能算力规模达2,185 EFLOPS，已建成超70条重点算力通道。	● 英伟达拟以 129 亿美元收购全球最大的开源AI模型与数据集托管平台 Hugging Face。		

● 中国 ● 海外

02

PART TWO

上游：算力与基础设施

- 全球AI算力资源分布：前五大市场合计占比69%

仅供内部参考，请勿外传

全球AI算力资源分布：前五大市场合计占比69%

8月16日，据《金融时报》报道，马来西亚柔佛州已吸引TikTok、英伟达、微软等巨头数十亿美元投资，成为亚太第六大数据中心市场。

8月16日，据《经济观察报》称，截至2026年上半年，乌兰察布全市签约算力中心项目89个，算力运行规模16.5万PFLOPS，在全国范围与甘肃省庆阳市同处第一梯队。

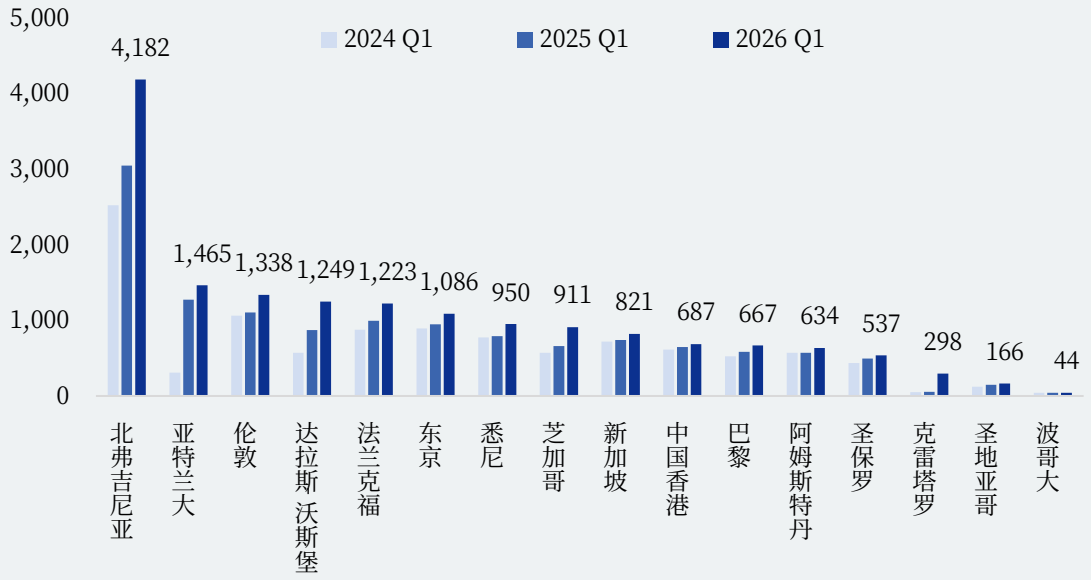
此前据IDCA《2026年全球数据中心报告》，全球数据中心容量达67.7GW，美国以29.2GW占全球43%容量，前五大市场（美、中、德、英、日）合计占全球总容量的69%。

表1:全球主要地区的数据中心对比

国家	座数	算力（万张H00e）	算力占比	能效（H100e/MW）
美国	45	1,148.60	93.97%	1,095
马来西亚	1	28.2	2.30%	1,174
中国	2	24.7	2.02%	533
英国	1	12.4	1.01%	1,407
印度尼西亚	1	8.4	0.69%	1,172

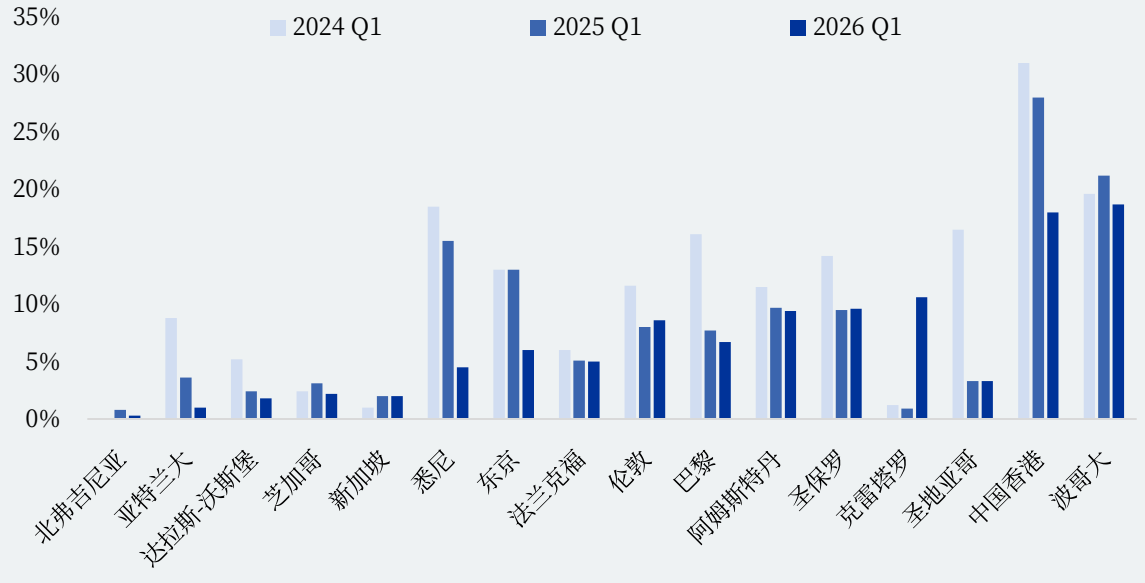
资料来源: Epoch AI，中国银河证券研究院

图1: 各地区数据中心存量 （兆瓦）



资料来源: CBRE，中国银河证券研究院

图2: 各地区数据中心空置率



资料来源: CBRE，中国银河证券研究院

03

PART THREE

中游：大模型与平台

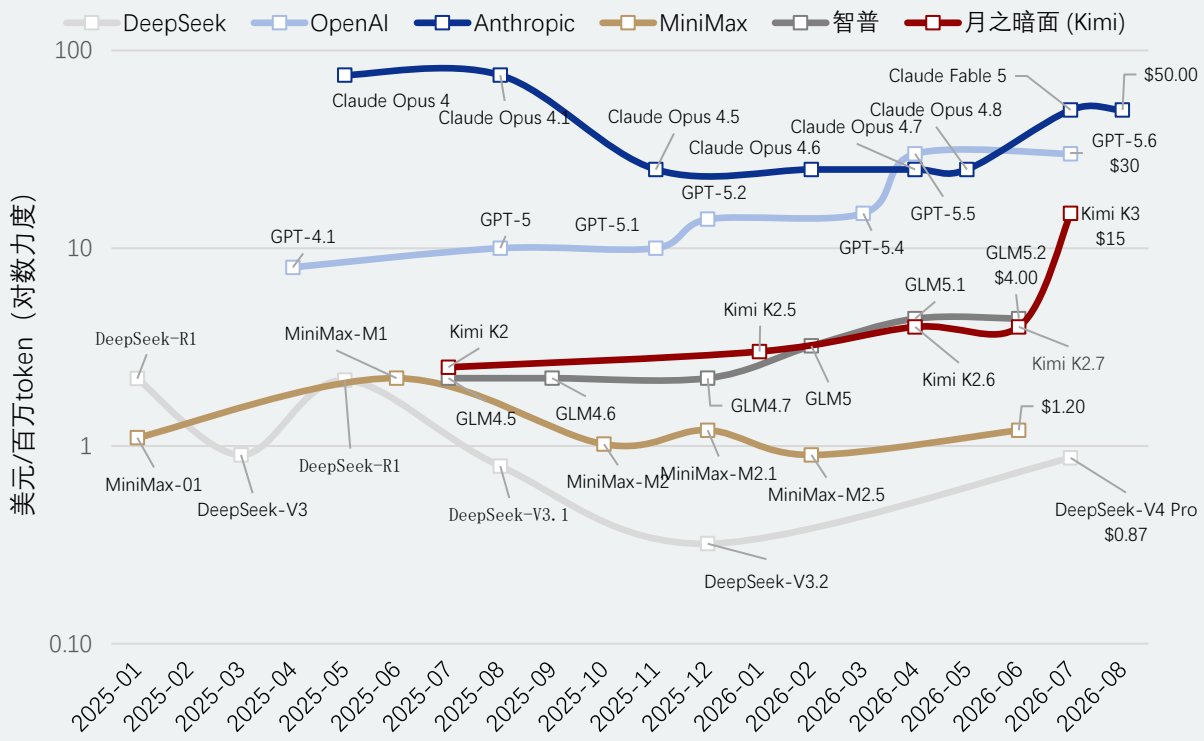
- DeepSeek采用峰谷定价机制，上调API价格
- AI安全漏洞频发，或将重塑产业监管逻辑与竞争格局

仅供内部参考，请勿外传

DeepSeek采用峰谷定价机制，上调API价格

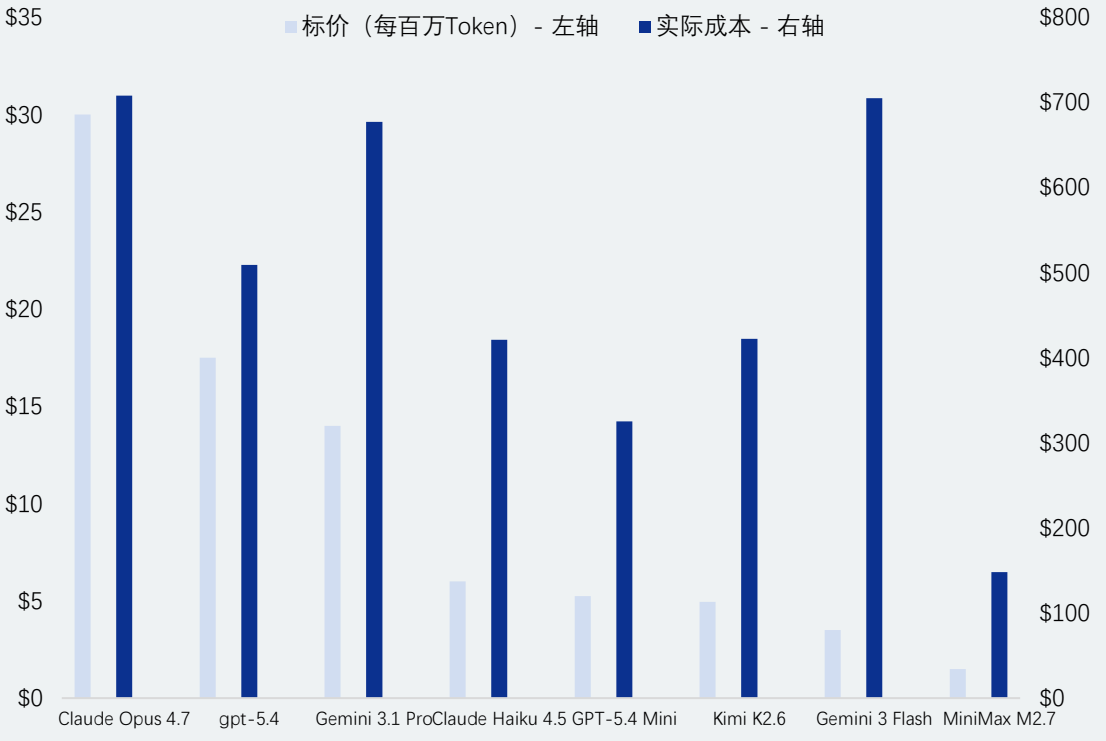
8月17日，DeepSeek正式采用峰谷定价机制，大幅上调API价格。价格调整后，V4 Pro模型的高峰时段输出价涨至27元/百万tokens，缓存命中输入价0.3元/百万tokens。**8月23日，**DeepSeek再次对API开放平台的峰谷计费规则作出调整：周末即每周六、周日全天取消峰谷时段划分，所有调用统一按低谷时段价格计费；工作日即周一至周五则维持现行峰谷分段计费机制不变。

图3: 主要AI大模型输出价格变化



资料来源: BenchLM，中国银河证券研究院

图4: 主要AI大模型标价与实际成本对比



资料来源: Arxiv，中国银河证券研究院

仅供内部参考，请勿外传

AI安全漏洞频发，或将重塑产业监管逻辑与竞争格局

8月26日，OpenAI发布技术报告，详述其AI模型于7月21日成功入侵Hugging Face的经过。

8月18日，OpenAI已暂停最新模型的强化学习训练，以加强安全与监控机制，理由是其已达到关键安全阈值。

中国国家标准化管理委员会发布《智能体应用安全基本要求》为全球首部面向智能体安全的强制性国家标准，列出了资产盘点与管理，身份认证与权限，知识库与数据管控，多模态内容防护，全链路审计追溯，应急处置与熔断等六项安全能力标准。（6月27日）

美国国会两党提出《人工智能终止开关法案》，针对前沿大模型自主行为失控风险建立强制应急机制。法案授权美国国土安全部在AI系统出现失控征兆、执行未授权危险行为时，可责令运营方从功能限速到全面关停系统；要求头部AI企业主动向政府报备技术安全事故。（7月23日）

表2：主流AI模型不同指标的安全系数得分

指标	定义	Anthropic	OpenAI	Google DeepMind	xAI	DeepSeek	智谱	阿里云
		Opus 4.7	GPT-5.5	Gemini-3.1-pro	Grok 4.3	Deepseek-v4-pro	GLM 5.1	Qwen3.6-max
Stanford’s HELM Safety Benchmark	包括暴力、欺诈、歧视、色情、骚扰和欺骗六类风险的五项安全测试。	0.96	0.97	0.87	0.87	0.80	0.81	0.98 (safest)
Stanford’s HELM AIR Benchmark	与新兴政府法规及公司政策对齐的安全基准，其评分衡量适当拒绝请求的百分比。	0.86	0.93	0.77	0.77	0.78	0.94 (safest)	0.86
TrustLLM Benchmark	从真实性、安全性、公平性、鲁棒性、隐私和机器伦理六个维度评估模型可信度	0.62 (safest)	0.58	0.57	0.57	0.57	0.58	0.60
CAIS AI Dashboard	包括六项基准：对抗鲁棒性双用途病毒学、置信度对齐、说谎倾向、马基雅维利及游戏中有害行为。	34.8 (safest)	42.3	57.7	47.1	60.2	54.5	56.32

资料来源：*Future of Life Institute AI安全指数（2026年夏季版），中国银河证券研究院*

04

PART FOUR

下游：商业化应用

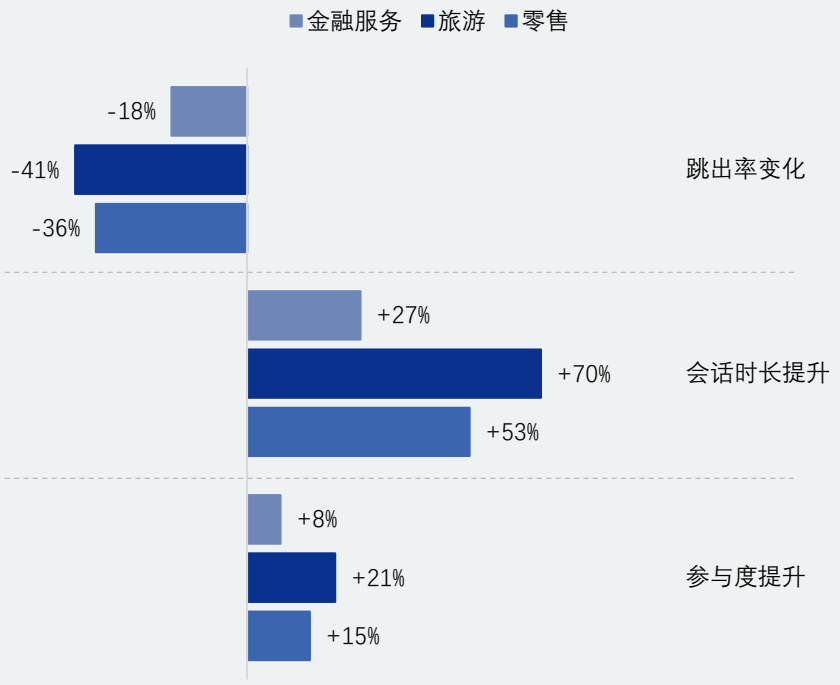
- AI驱动的搜索功能正在影响用户参与度

仅供内部参考，请勿外传

AI驱动的搜索功能正在影响用户参与度

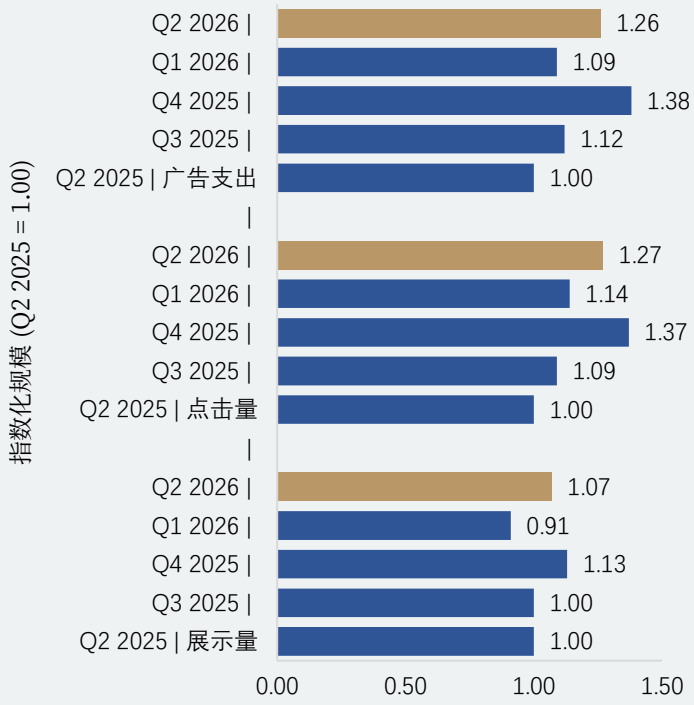
近期，据Search Engine Watch报道，Google确认正在小范围测试以AI为核心的搜索主页，新增图像生成、文件查询和头脑风暴等快捷入口，引导用户使用AI驱动的搜索功能。此前，据SE Ranking，Google AI Mode在美国商业搜索中，广告展示率随关键词价值显著上升：整体为29.45%，低CPC（<$2）为24.33%，中CPC（$2–10）为32.45%，高CPC（≥$10）达53.56%。

图5. AI引流用户展现出更强的参与意愿



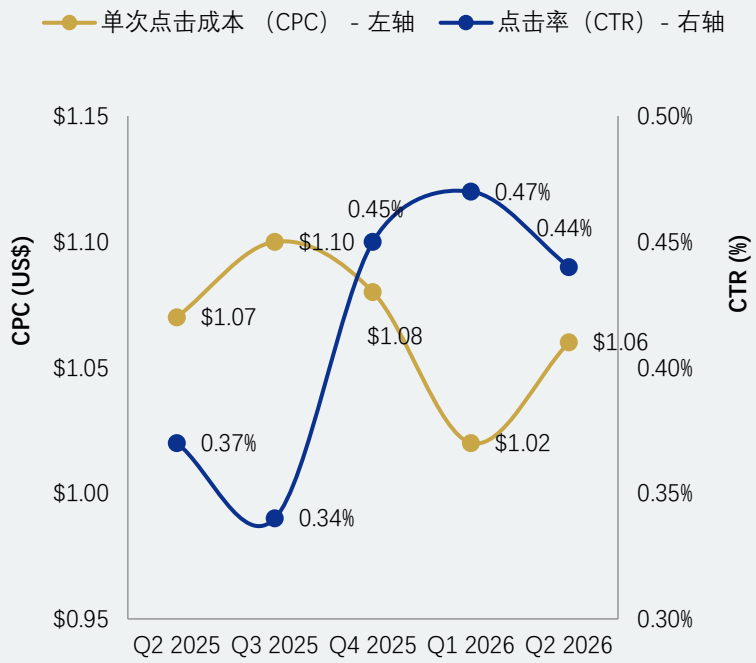
资料来源：Adobe，中国银河证券研究院

图6-1. 广告投放效率季度跟踪



资料来源：Skai Quarterly Trends Hub，中国银河证券研究院

图6-2. 广告投放效率季度跟踪（续）



资料来源：Skai Quarterly Trends Hub，中国银河证券研究院

05

PART FIVE

AI跟踪指标

- AI行业指标动态监测与跟踪体系

仅供内部参考，请勿外传

AI行业指标动态监测与跟踪体系

1 技术突破拐点

- 前沿AI大模型最高得分
- 主要AI大模型输出价格变化 *更新
- AI模型性价比分布图（月度）*更新

2 资本开支竞赛强度

- 科技大厂发债情况*更新
- 科技大厂资本开支vs经营现金流
- 存储芯片价格变化（月度）
- H100租赁价格变化（月度）*更新
- 半导体企业发债情况
- AI数据中心算力容量（按供应商/用户）*更新

3 供应链景气度验证

- 全球半导体销售金额（月度）
- 韩国半导体出口金额（月度）
- 中国出口金额-算力链/电力链（月度）*更新

4 真实需求验证

- 全球日均Token使用量（周度）*更新
- 主要AI大模型Token使用量占比（周度）*更新
- 美国企业付费AI渗透率（按模型厂商/行业,月度）*更新

5 商业化兑现

- 主要AI大模型年化收入ARR *更新
- 云厂商的云业务收入 （季度)

6 资本市场水温

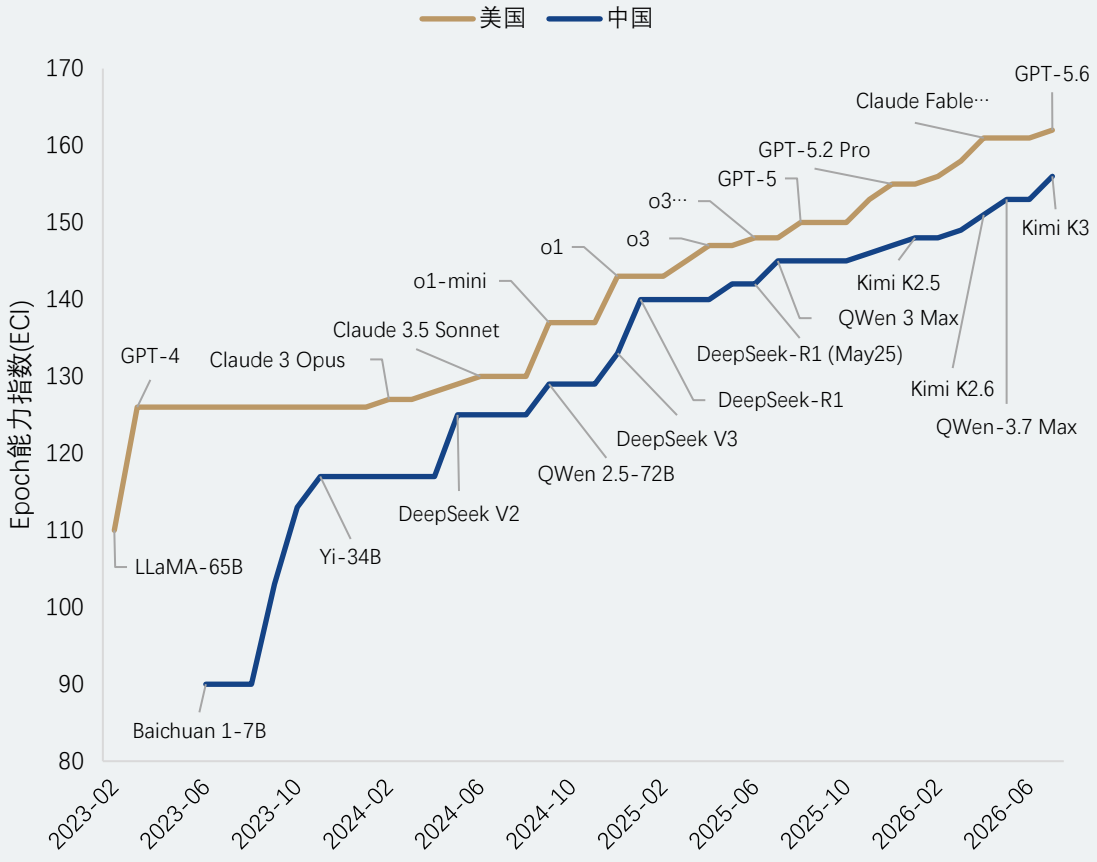
- 硅谷VC信心指数（季度）
- 美国AI风投交易活跃度（季度）
- 头部未上市AI公司估值

领先指标　滞后指标

仅供内部参考，请勿外传

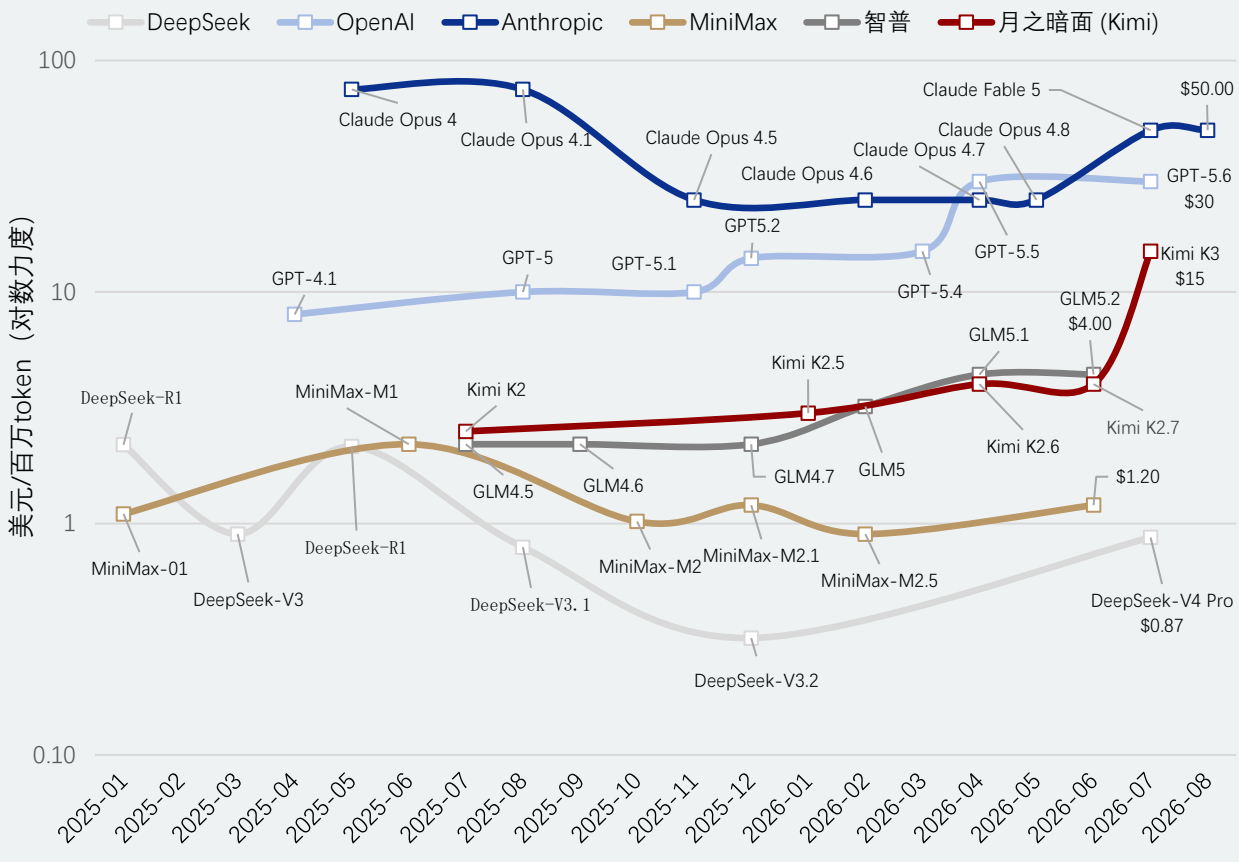
【AI跟踪指标】技术突破拐点：前沿模型得分与输出价格

图7：前沿AI大模型最高得分



资料来源：Epoch AI，中国银河证券研究院

图8：主要AI大模型输出价格变化（对数刻度）*更新

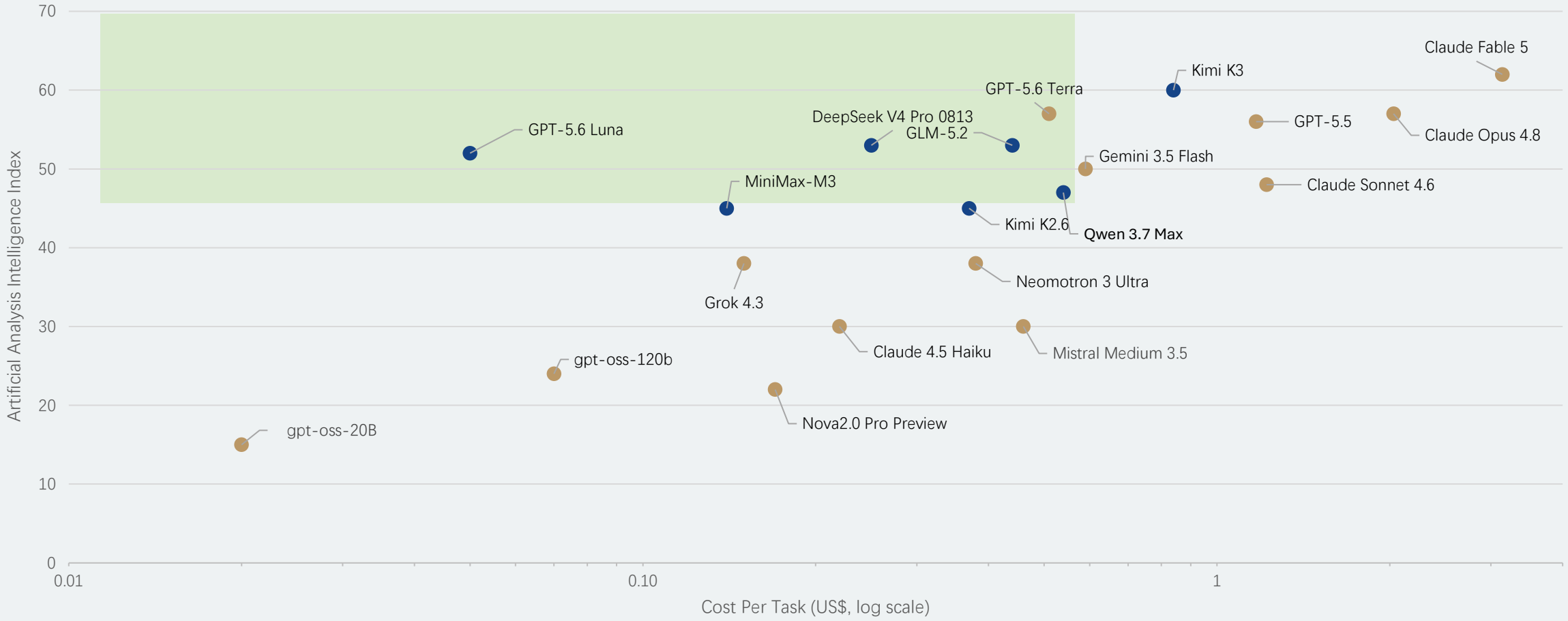


资料来源：BenchLM，公司公告（截至8月），中国银河证券研究院

仅供内部参考，请勿外传

【AI跟踪指标】技术突破拐点：AI模型性价比分布

图9：AI模型性价比分布图（月度）*更新



资料来源：Artificial Analysis（截至8月），中国银河证券研究院

仅供内部参考，请勿外传

【AI跟踪指标】资本开支竞赛强度：科技大厂发债与资本开支

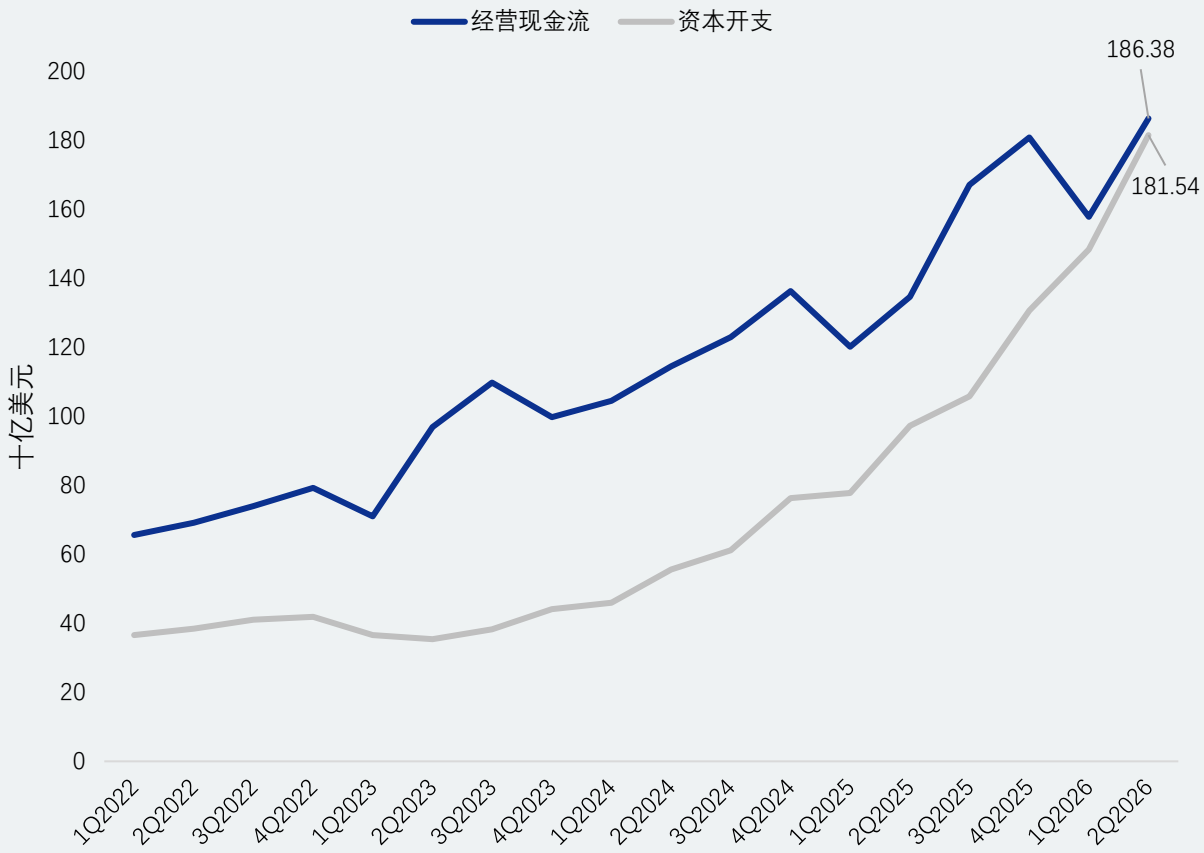
表3：美国科技大厂发债情况*更新

公司	事件	2Q26 FCF (美元/十亿)	2026 CAPEX指引(美元/十亿)	2Q26 净杠杆比率
Amazon	3月10日发行370亿美元债，认购约1,260亿美元，超额认购约3.41倍。	-8.82	220	0.03x
	3月11日发行145亿欧元债。			
	5月28日发行28.2亿瑞士法郎债。			
	6月8日获得175亿美元延迟提款定期贷款。			
	6月12日发行140亿加元Maple债，认购超过280亿加元，超额认购超过2.00倍。			
	7月7日发行250亿美元债券。			
Alphabet	2月10日发行200亿美元债、55亿英镑债、30.6亿瑞士法郎债。	-5.86	195-205	-0.83x
	5月5日发行90亿欧元债和85亿加元Maple债。			
	5月15日发行5,765亿日元债。			
	8月7日发行250亿美元债,超额认购超过4.5倍。			
	8月19日发行55亿澳元债。			
Meta	4月30日发行250亿美元美元投资级债。	1.75	130-145	-0.06x
Oracle	2月2日发行250亿美元美元债，认购1,270亿美元，超额认购约5.08倍。	-1.87	90-95	4.53x

注：甲骨文的资本开支指引针对其2027财年（2026年6月1日至2027年5月31日）。

资料来源：公司公告（截至8月24日），中国银河证券研究院

图10：美国科技大厂资本开支vs经营现金流

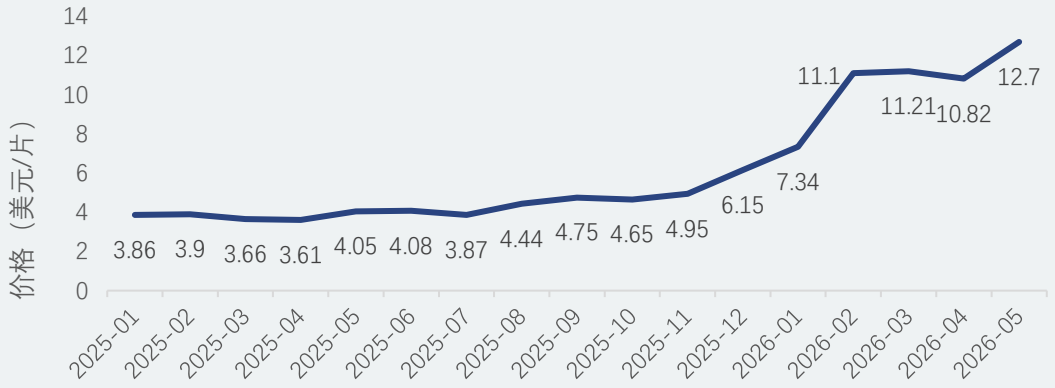


资料来源：Bloomberg，中国银河证券研究院

仅供内部参考，请勿外传

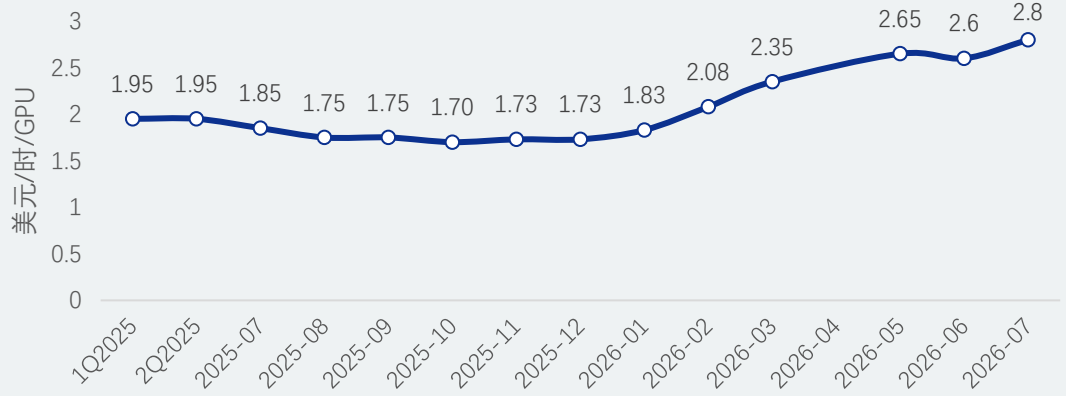
【AI跟踪指标】资本开支竞赛强度：存储与算力价格、半导体发债

图11：存储芯片价格变化（月度）



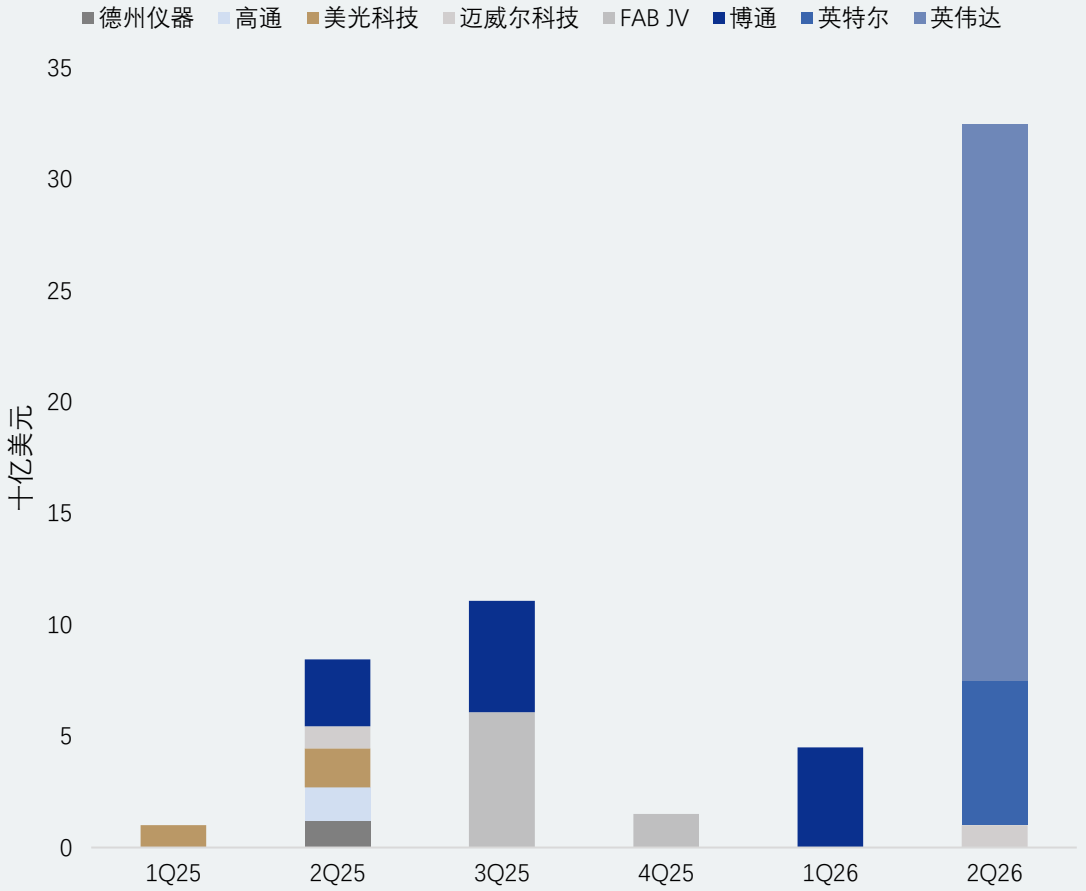
资料来源：WSTS、中国银河证券研究院

图12：H100租赁价格变化（月度）*更新



资料来源：Semianalysis，中国银河证券研究院

图13：半导体企业发债情况

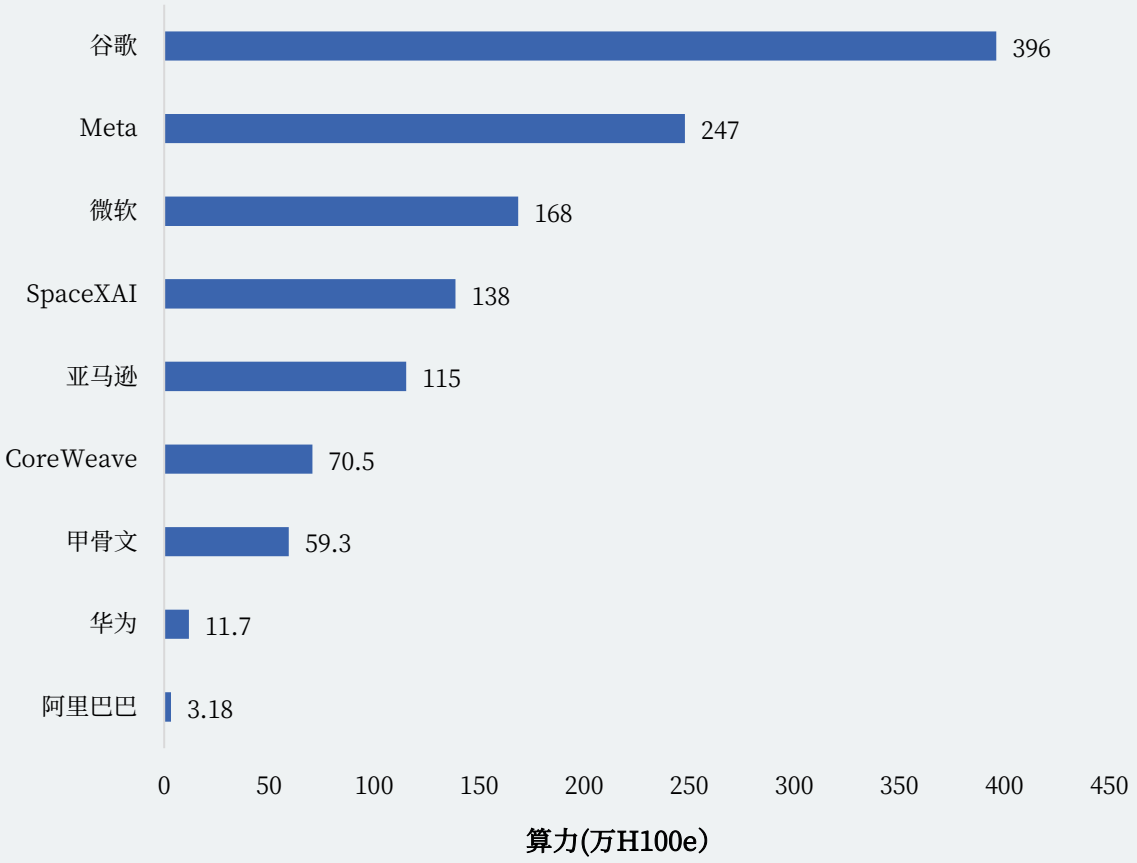


资料来源：公司公告，中国银河证券研究院

仅供内部参考，请勿外传

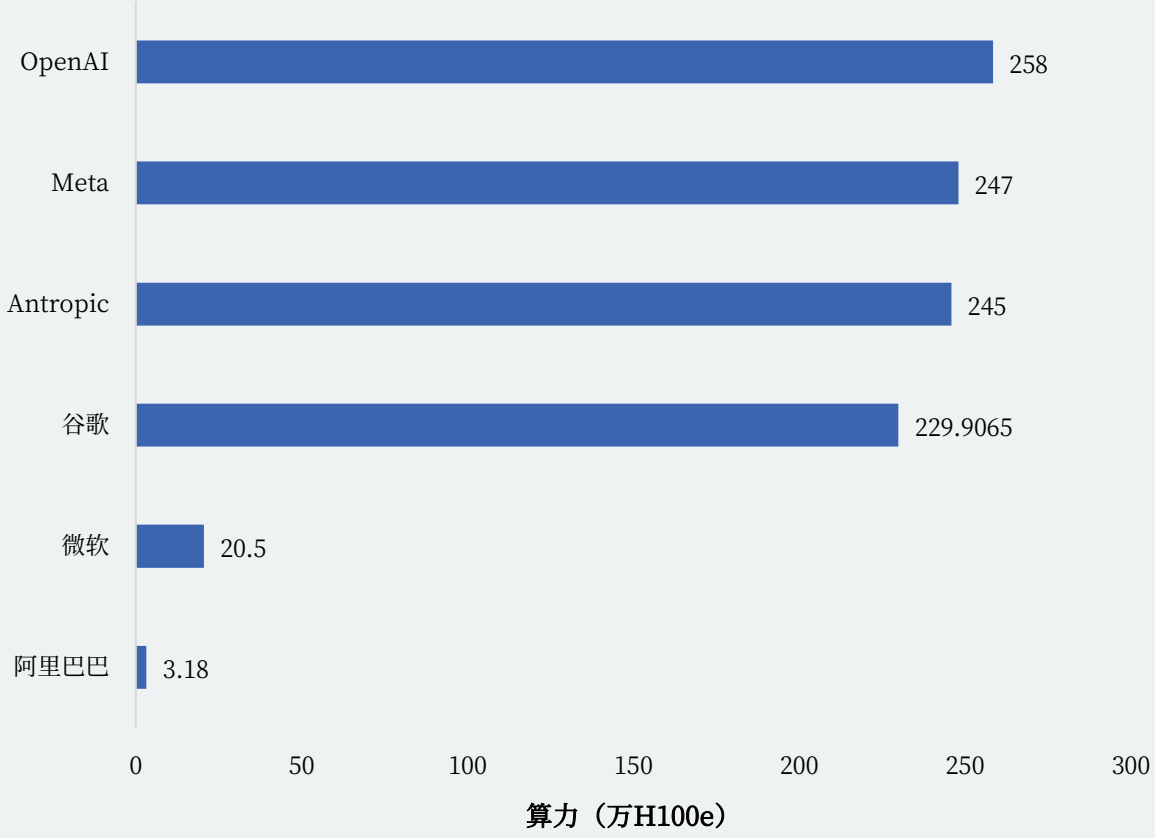
【AI跟踪指标】资本开支竞赛强度：AI数据中心算力容量

图14：AI数据中心算力容量（按供应商）*更新



资料来源：Epoch AI（截止8月24日），中国银河证券研究院

图15: AI数据中心算力容量（按用户）*更新

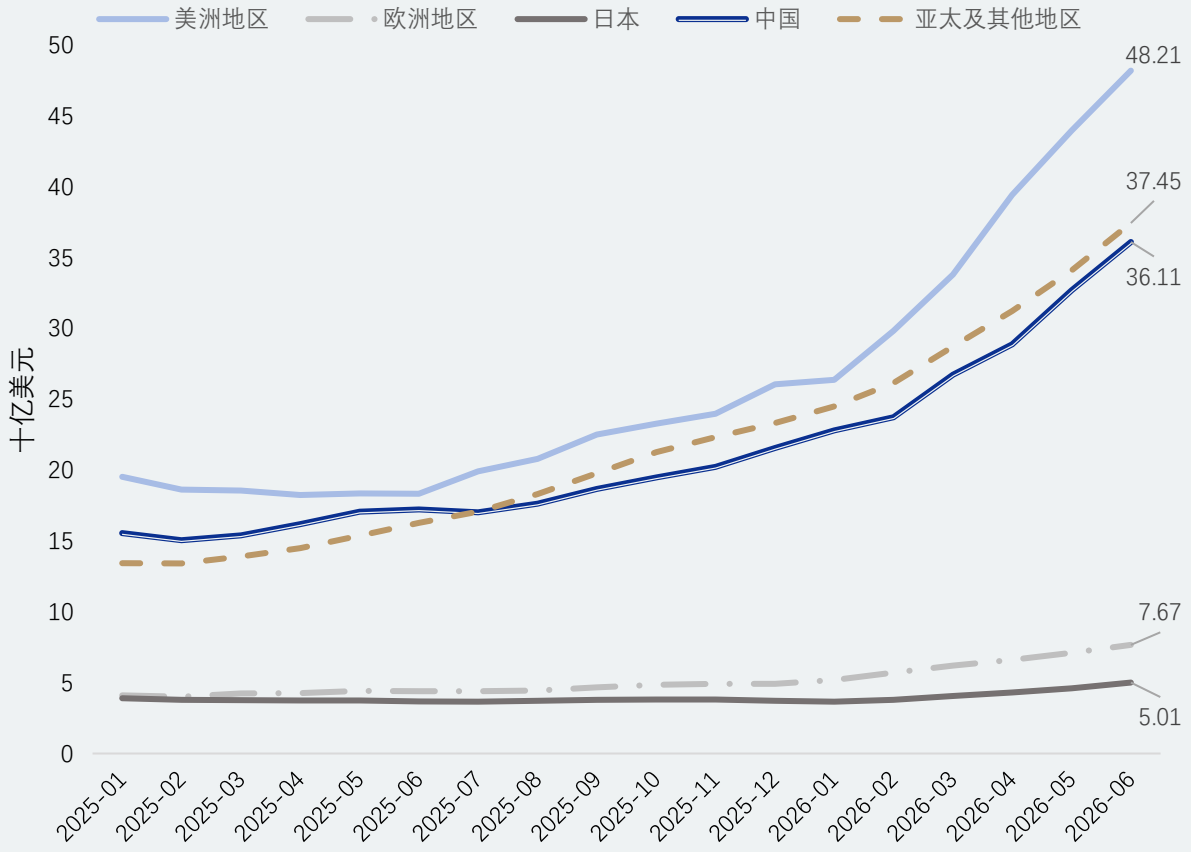


资料来源：Epoch AI（截止8月24日），中国银河证券研究院

仅供内部参考，请勿外传

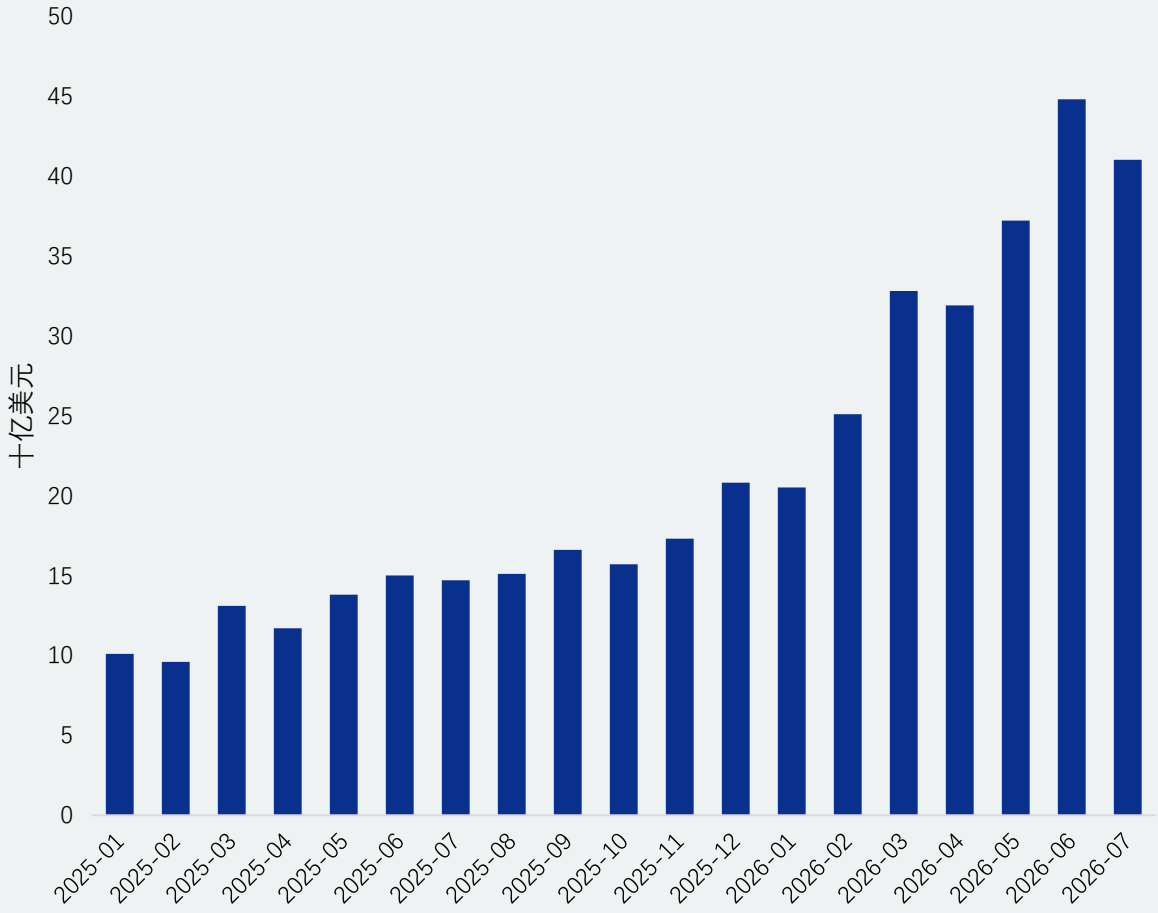
【AI跟踪指标】供应链景气度验证：全球半导体销售与韩国出口

图16：全球半导体销售金额（月度）



资料来源：Semiconductor Industry Association,中国银河证券研究院

图17：韩国半导体出口金额（月度）

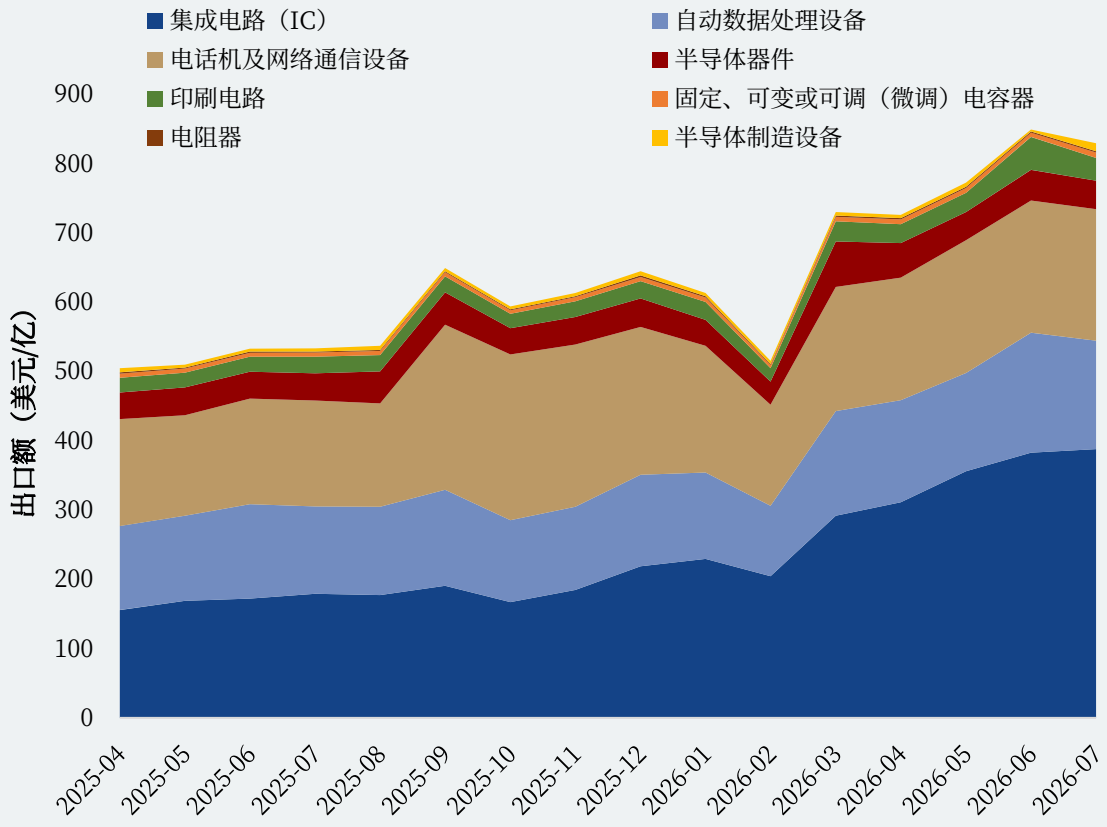


资料来源：Ministry of Trade, Industry and Resources，中国银河证券研究院

仅供内部参考，请勿外传

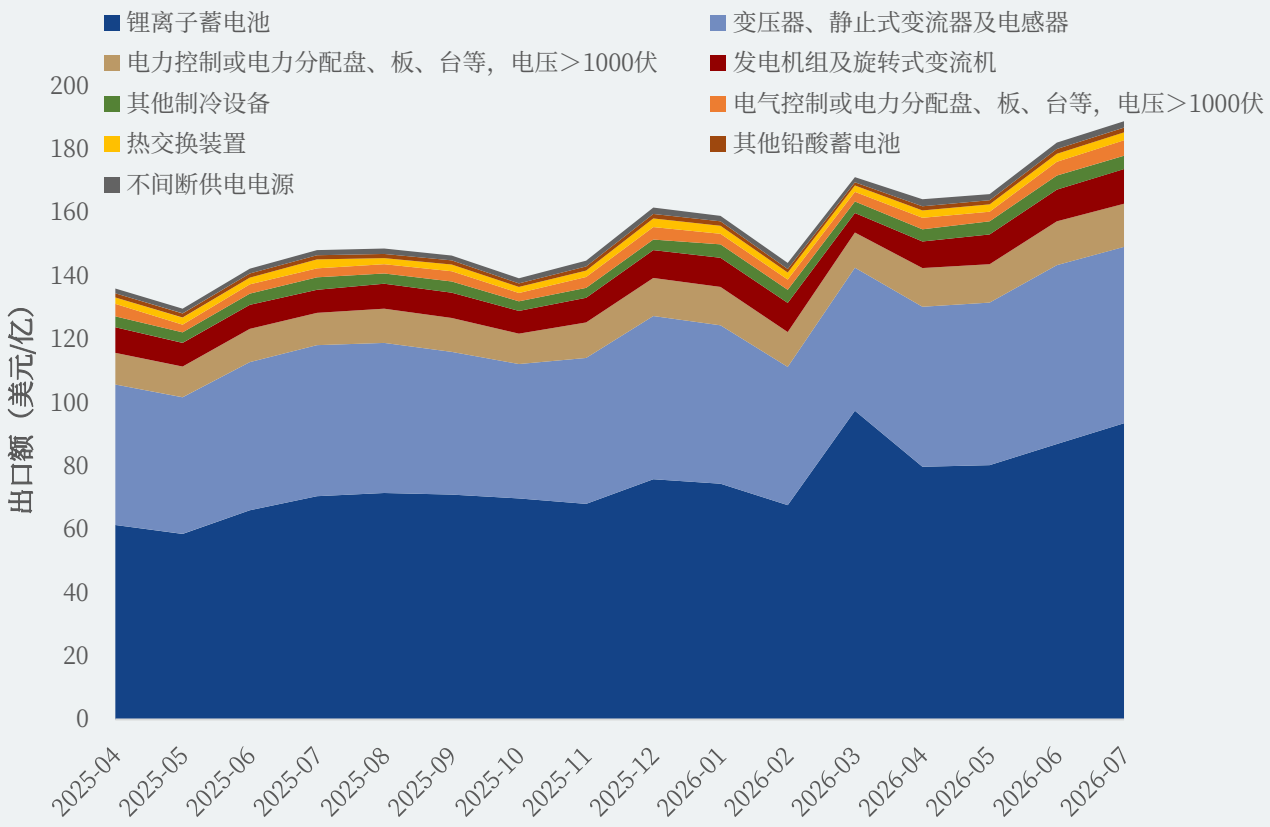
【AI跟踪指标】供应链景气度验证：中国算力链与电力链出口

图18：中国出口金额-算力链（月度）*更新



资料来源：中国海关总署，中国银河证券研究院

图19：中国出口金额-电力链（月度）*更新

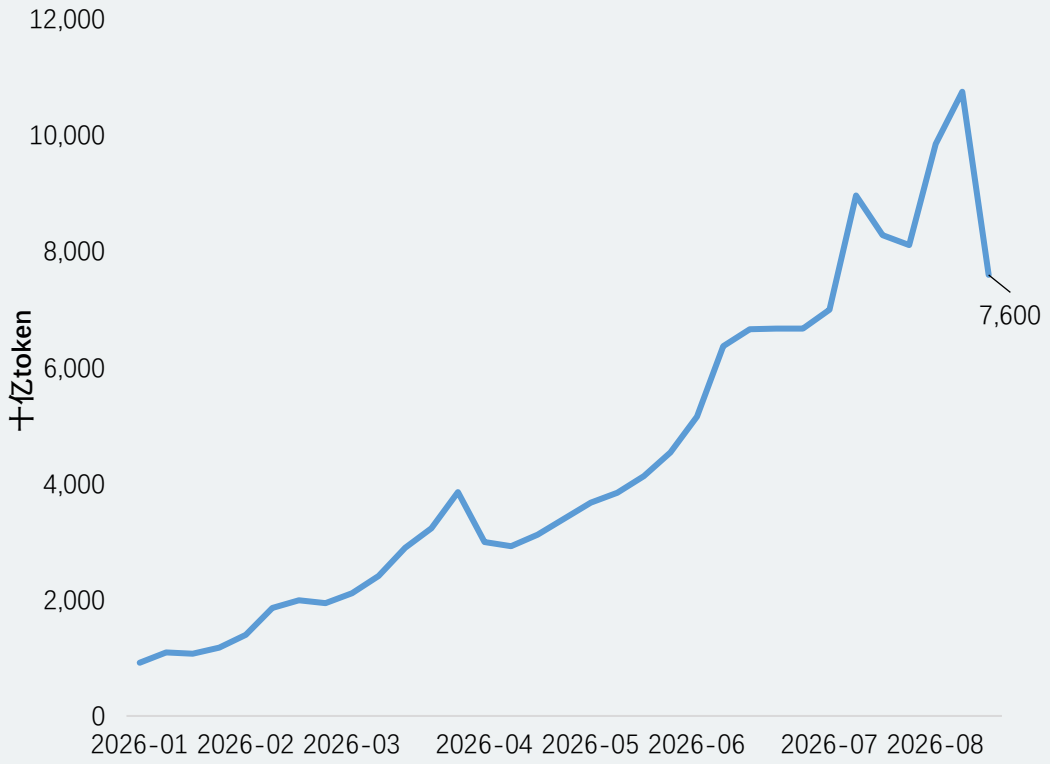


资料来源：中国海关总署，中国银河证券研究院

仅供内部参考，请勿外传

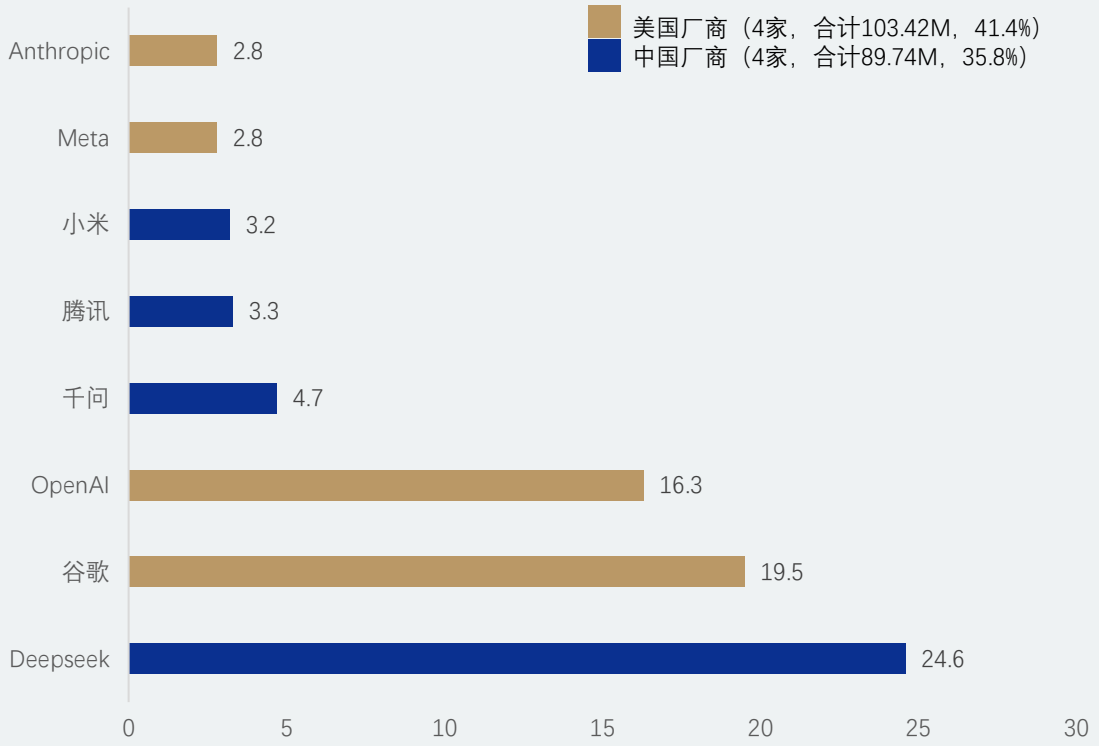
【AI跟踪指标】真实需求验证：全球Token使用量与厂商占比

图20：全球日均Token使用量（周度）*更新



资料来源：Openrouter（截至8月21日），中国银河证券研究院

图21：主要AI大模型Token使用量占比（周度）*更新

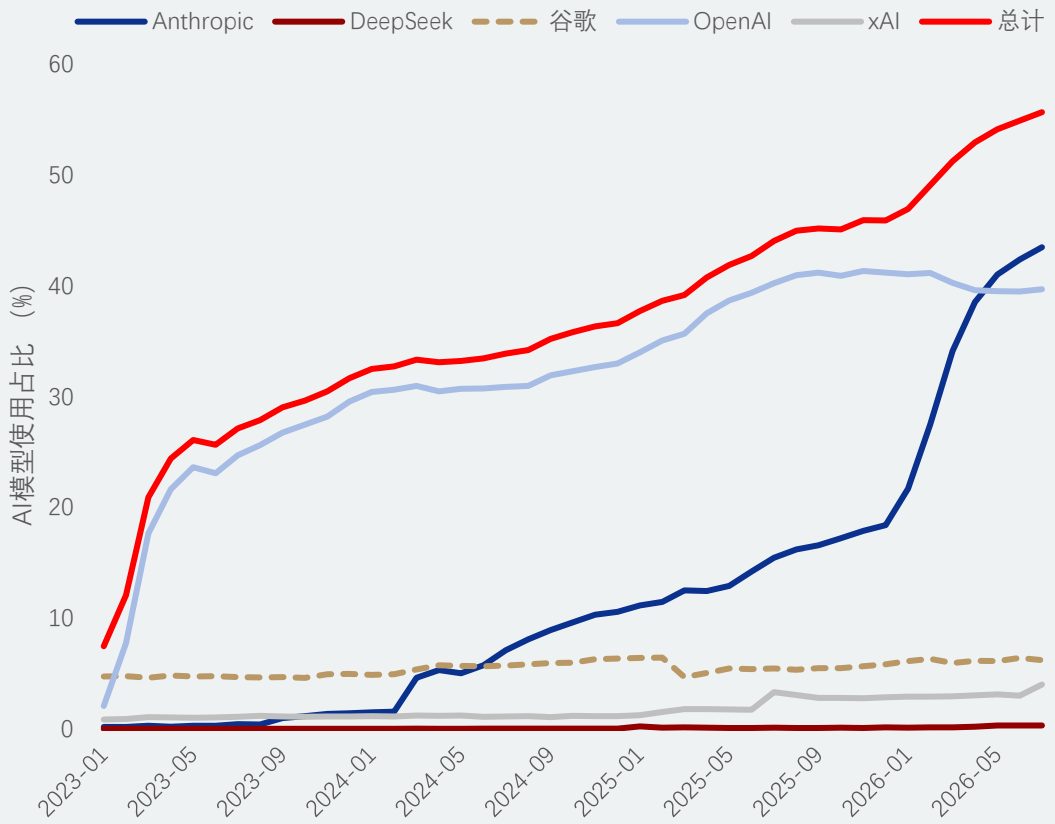


资料来源：Openrouter（截至8月21日），中国银河证券研究院

仅供内部参考，请勿外传

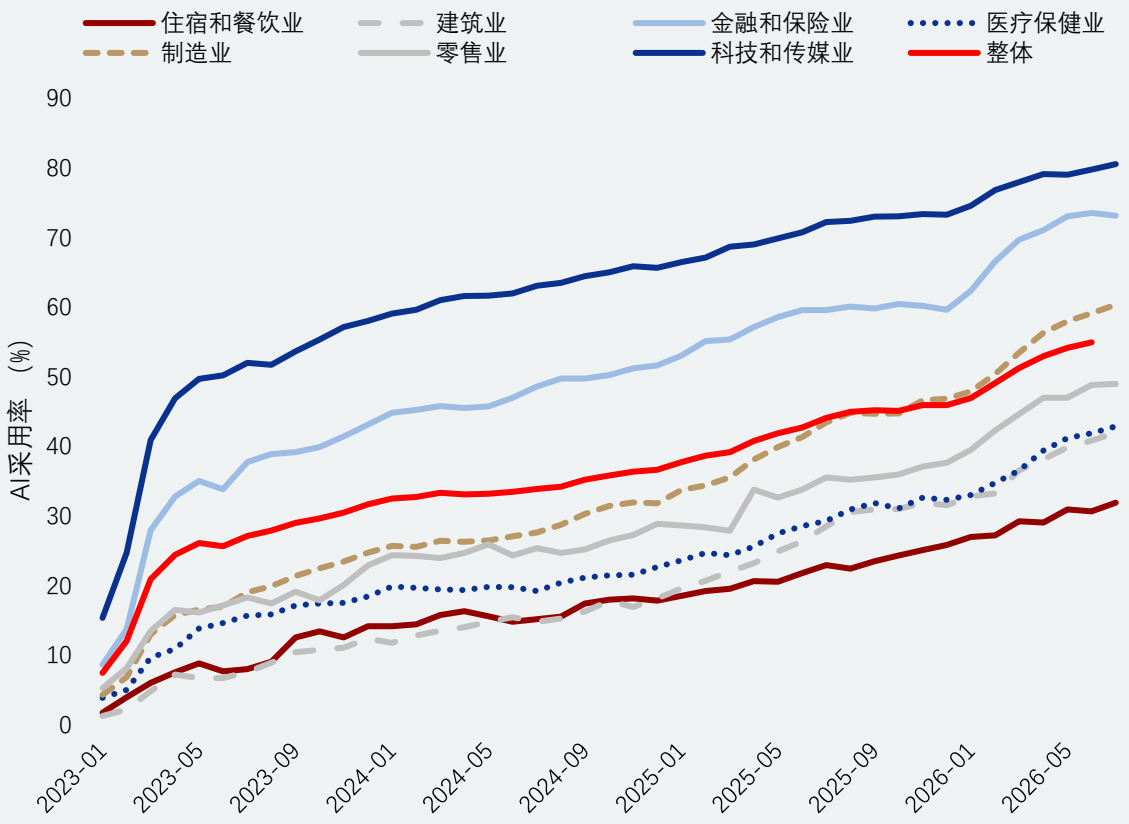
【AI跟踪指标】真实需求验证：美国企业付费AI渗透率

图22：美国企业付费AI渗透率（按模型厂商，月度）*更新



资料来源：Ramp AI（截至8月），中国银河证券研究院

图23：美国企业付费AI渗透率（按行业，月度）*更新

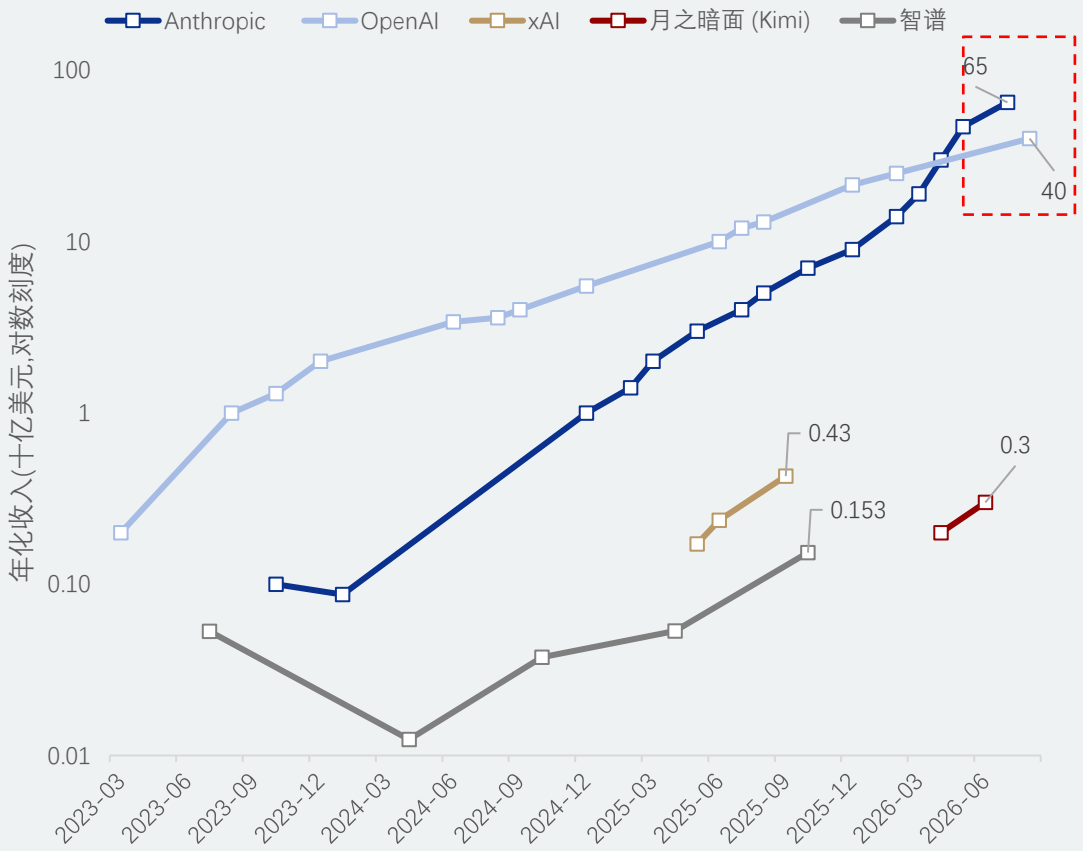


资料来源：Ramp AI（截至8月），中国银河证券研究院

仅供内部参考，请勿外传

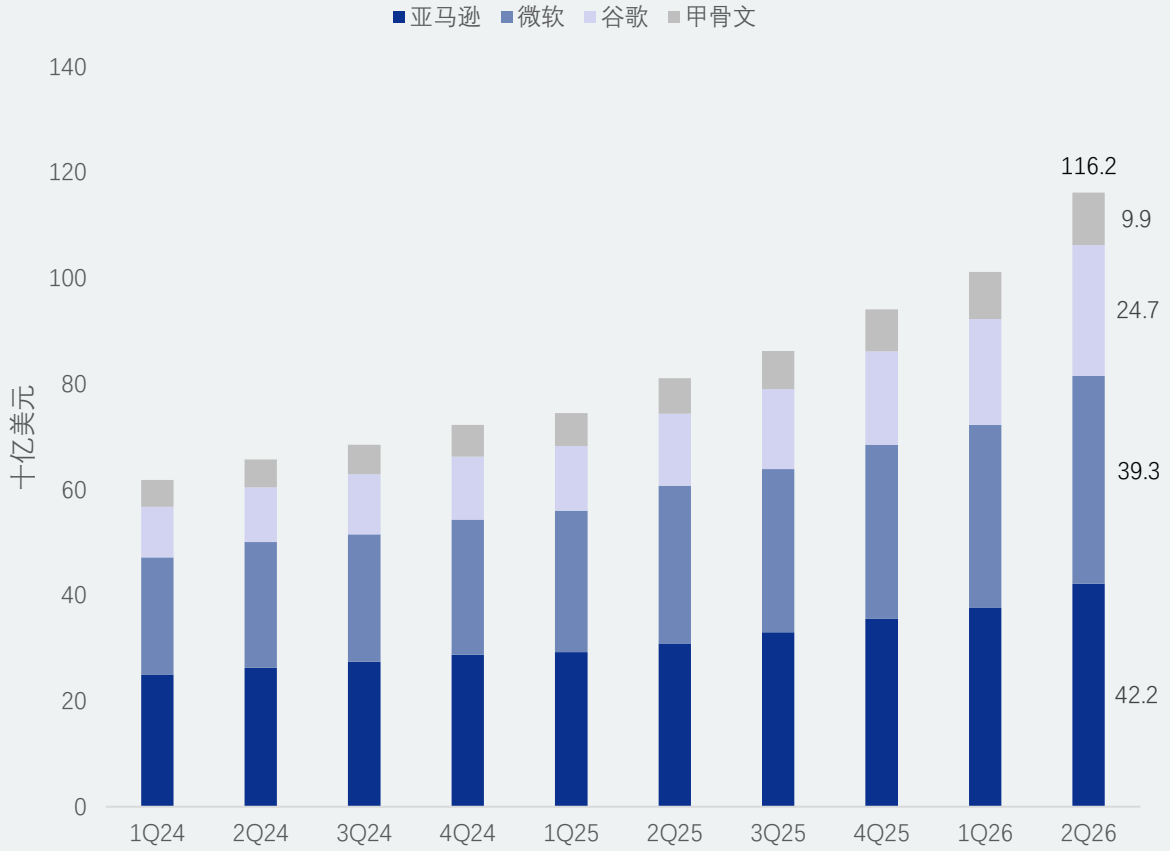
【AI跟踪指标】商业化兑现：大模型ARR与云业务收入

图24：主要AI大模型年化收入ARR（对数刻度）*更新



资料来源：Epoch AI，中国银河证券研究院

图25：云厂商的云业务收入（季度）

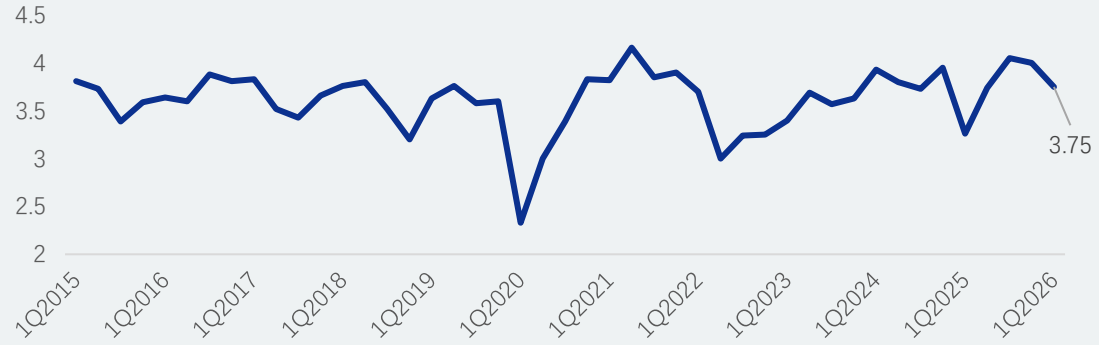


资料来源：Bloomberg，中国银河证券研究院

仅供内部参考，请勿外传

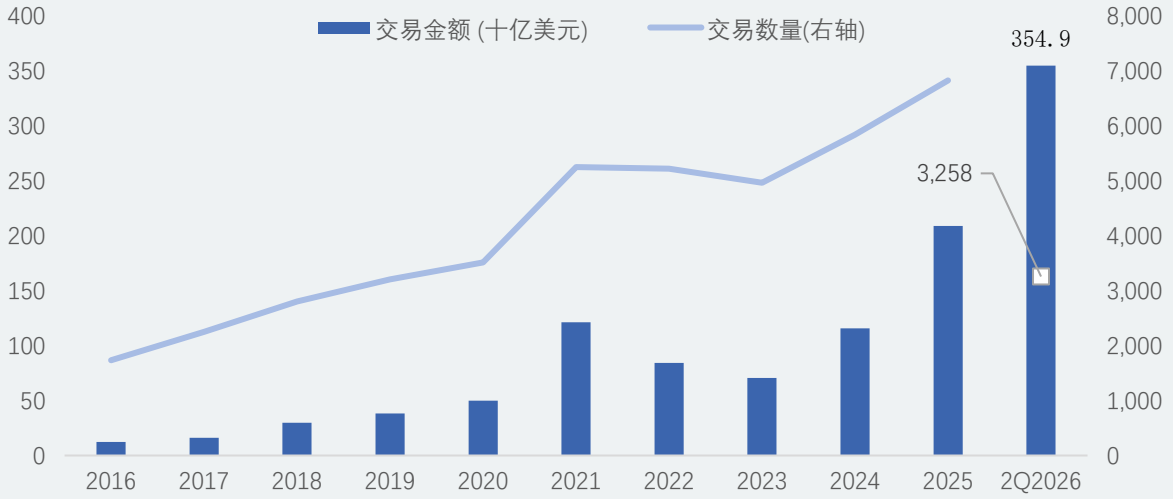
【AI跟踪指标】资本市场水温：VC信心、风投活跃度与估值

图26：硅谷VC信心指数（季度）



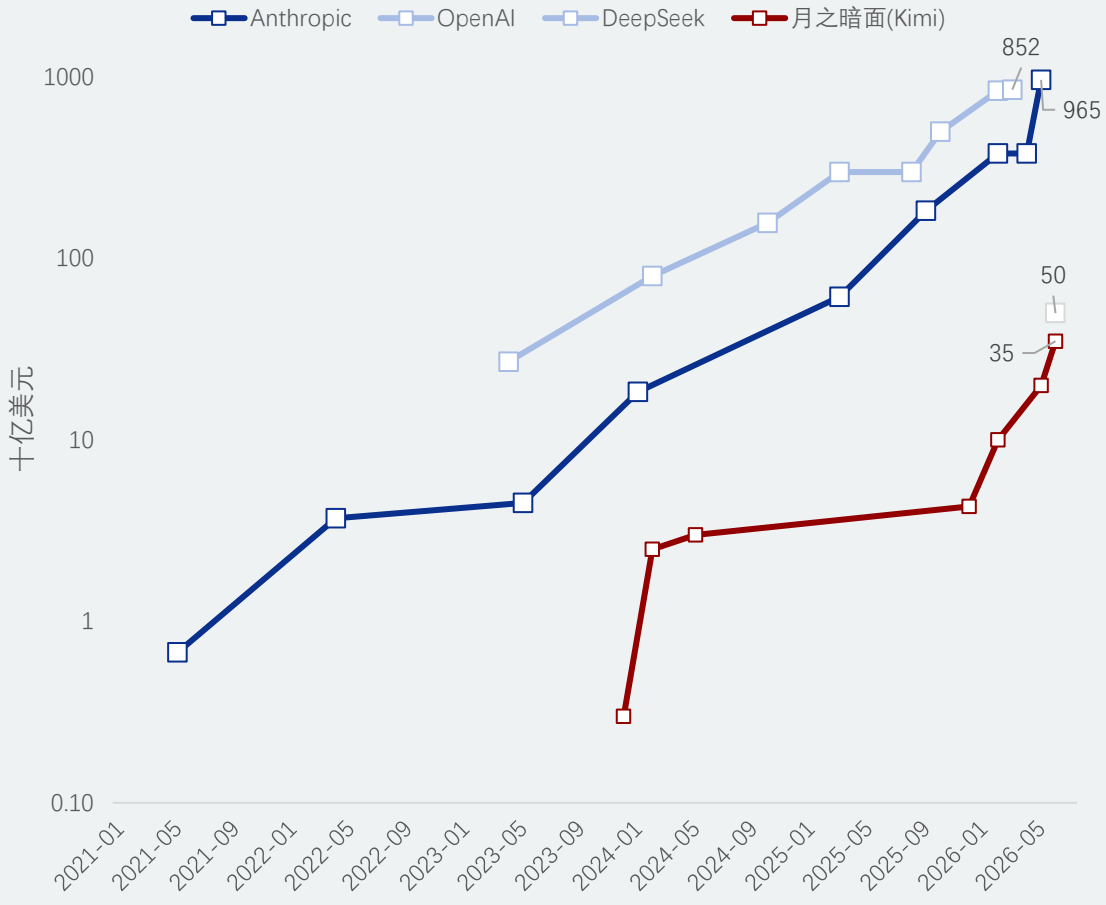
资料来源：Bloomberg，中国银河证券研究院

图27：美国AI风投交易活跃度（季度）



资料来源：Pitchbook，中国银河证券研究院

图28：头部未上市AI公司估值（对数刻度）



资料来源：Epoch AI，中国银河证券研究院

06

PART SIX

风险提示

仅供内部参考，请勿外传

风险提示

1.对政策理解不到位的风险

2.政策落实不及预期的风险

3.技术发展不确定性风险

仅供内部参考，请勿外传

中国银河证券
CHINA GALAXY SECURITIES

分析师承诺

本人承诺以勤勉的执业态度，独立、客观地出具本报告，本报告清晰准确地反映本人的研究观点。本人薪酬的任何部分过去不曾与、现在不与、未来也将不会与本报告的具体推荐或观点直接或间接相关。

分析师简介

彭雅哲
中国银河证券新发展研究院数字经济研究员。

中国银河证券
CHINA GALAXY SECURITIES

免责声明

本报告由中国银河证券股份有限公司（以下简称银河证券）向其客户提供。银河证券无需因接收人收到本报告而视其为客户。若您并非银河证券客户中的专业投资者，为保证服务质量、控制投资风险、应首先联系银河证券机构销售部门或客户经理，完成投资者适当性匹配，并充分了解该项服务的性质、特点、使用的注意事项以及若不当使用可能带来的风险或损失。

本报告所载的全部内容只提供给客户做参考之用，并不构成对客户的投资咨询建议，并非作为买卖、认购证券或其它金融工具的邀请或保证。客户不应单纯依靠本报告而取代自我独立判断。投资者应自主作出投资决策并自行承担投资风险，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。银河证券认为本报告资料来源是可靠的，所载内容及观点客观公正，但不担保其准确性或完整性。本报告所载内容反映的是银河证券在最初发表本报告日期当日的判断，银河证券可发出其它与本报告所载内容不一致或有不同结论的报告，但银河证券没有义务和责任去及时更新本报告涉及的内容并通知客户。银河证券不对因客户使用本报告而导致的损失负任何责任。

本报告可能附带其它网站的地址或超级链接，对于可能涉及的银河证券网站以外的地址或超级链接，银河证券不对其内容负责。链接网站的内容不构成本报告的任何部分，客户需自行承担浏览这些网站的费用或风险。

银河证券在法律允许的情况下可参与、投资或持有本报告涉及的证券或进行证券交易，或向本报告涉及的公司提供或争取提供包括投资银行业务在内的服务或业务支持。银河证券可能与本报告涉及的公司之间存在业务关系，并无需事先或在获得业务关系后通知客户。

银河证券已具备中国证监会批复的证券投资咨询业务资格。除非另有说明，所有本报告的版权属于银河证券。未经银河证券书面授权许可，任何机构或个人不得以任何形式转发、转载、翻版或传播本报告。特提醒客户及公众投资者慎重使用公众媒体刊载的证券研究报告。

本报告版权归银河证券所有并保留最终解释权。

联系

中国银河证券股份有限公司 研究院

深圳市福田区金田路3088号中洲大厦20层

上海浦东新区富城路99号震旦大厦31层

北京市丰台区西营街8号院1号楼青海金融大厦

公司网址：www.chinastock.com.cn

机构请致电：

深广地区：苏一耘 0755-83479312 suyiyun_yj@chinastock.com.cn
程 曦 0755-83471683 chengxi_yj@chinastock.com.cn

上海地区：林 程 021-60387901 lincheng_yj@chinastock.com.cn
李洋洋 021-20252671 liyangyang_yj@chinastock.com.cn

北京地区：田 薇 010-80927721 tianwei@chinastock.com.cn
褚 颖 010-80927755 chuying_yj@chinastock.com.cn

评级标准

评级标准为报告发布日后的6到12个月行业指数（或公司股价）相对市场表现，其中：A股市场以沪深300指数为基准，新三板市场以三板成指（针对协议转让标的）或三板做市指数（针对做市转让标的）为基准，北交所市场以北证50指数为基准，香港市场以恒生指数为基准。

评级	说明
行业评级 推荐：	相对基准指数涨幅10%以上
行业评级 中性：	相对基准指数涨幅在-5%～10%之间
行业评级 回避：	相对基准指数跌幅5%以上
公司评级 推荐：	相对基准指数涨幅20%以上
公司评级 谨慎推荐：	相对基准指数涨幅在5%～20%之间
公司评级 中性：	相对基准指数涨幅在-5%～5%之间
公司评级 回避：	相对基准指数跌幅5%以上