证券代码：688561　　证券简称：奇安信

奇安信科技集团股份有限公司
投资者关系活动记录表

编号：2026-001

投资者关系活动类别	☐ 特定对象调研　☐分析师会议　☐媒体采访　☐现场参观 ☑ 业绩说明会　☐路演活动　☐一对一沟通 ☐新闻发布会　☐其他
参与单位及人员	本次参会机构共 69 家，参会人员 77 人，具体名单详见文后附录。
时间	2026 年 4 月 30 日 11 点 00 分-12 点 00 分
方式	线上会议
接待人员	**董事长齐向东；董事、总经理吴云坤；** **董事会秘书徐文杰；财务经理郑静**
投资者交流主要内容介绍	**本次业绩说明会主要包含两部分，第一部分由公司管理层介绍公司 2025 年年度及 2026 年第一季度经营情况，第二部分由公司管理层与投资者互动问答。** **第一部分由公司管理层介绍公司 2025 年年度及 2026 年第一季度经营情况：** **1、2025 年度核心财务指标** 2025 年，公司秉持高质量发展的理念，现金流水平实现历史性突破，为上市以来最佳，其持续向好的势头也显示了企业造血能力的显著增强。2025 年，公司实现营业收入 43.92 亿元，同比增长 0.97%；归母净利润-12.87 亿元，同比改善 6.68%；扣非净利润-15.26 亿元，同比改善 5.34%；销售回款 51.39 亿元，同比增长 8.00%，经营性现金流净额-0.61 亿元，同比改善 2.81 亿元；人均创收 59.19 万元，同比增长超过 3%。 **2、产品及研发方面，“AI+安全”领跑市场** 在 IDC 最新发布的“AI+安全”系列市场报告中，公司分别入选中国大模型安全市场的 6 大能力方向和中国安全智能体市场的 7 大核心领域，凭借覆盖范围之广、能力维度之多的优势，持续领跑“AI+安全”赛道。公司持续锻造 AI 能力，系统性地打造了以 AI 为核心的研发质量与效率提升体系。2025 年，在 AI 新产品方面，“智能安全”（Security for AI）和“安全智能”（AI for Security）”两线开花： 1）AISOC 斩获了新能源、汽车、有色、金融等行业的一批头部客户项目；

2）AI+代码卫士将能源、特种、运营商、金融、制造等行业一批知名客户的项目收入囊中；

3）大模型卫士在信息技术、政府、能源、金融等行业实现重要突破。

此外，公司的大模型卫士系统获得了公安部第三研究所颁发的《大模型安全防护围栏产品认证（增强级）》证书，在安全能力上得到了顶尖权威机构的认可。

3、市场销售侧，强化核心大客户战略

2025 年，公司聚焦资源投入，优化过程运营，屡次斩获千万级大单：

金融行业，中标某大型商业银行国产化 NDR 项目，金额达千万级；中标某国有银行国产化智慧防火墙项目以及某国有银行零信任项目；中标某头部证券公司 AISOC 项目。运营商行业，以 60%排名第一的份额占比，中标某运营商集团的防病毒软件集采项目，金额达千万级。能源行业，中标某大型电网企业千万级年度项目；接连中标国家管网集团多个省级工业安全大单，累计金额达千万级；中标某能源科技企业两千万元级全国产化工控安全项目。制造业，中标某家电巨头终端安全软件集采项目，以 EDR 等产品为主；中标轨交装备行业某头部企业安全集采项目，金额达千万级。消费品行业，中标某知名白酒企业网安体系、管理平台以及零信任项目，金额达千万级；接连中标中国烟草多个省公司项目，总金额达千万级。政府行业，中标某地大数据管理中心项目，金额近千万元；中标华南某中心城市网络靶场项目，金额达千万级。

收入结构方面，企业级客户持续成为公司收入端的主要引擎。2025 年，企业级客户、政府客户、公检法司分别占主营业务收入比为 76.23%、15.66%、8.11%。能源、金融、运营商、特种、制造业和信息技术六大行业合计占公司主营业务收入比重超过 66%。收入同比增速方面，运营商、制造业、特种、信息技术收入同比增速分别为 8%、38%、35%和 17%。从收入的体量分布上看，百万级以上客户占收入比重超过 73%，尤其是公司最坚实的“基本盘”——500 万级以上的关基行业大客户，贡献了约 50%的整体收入比重。

4、超短期融资券发行成功

今年 4 月，公司 2026 年度第一期超短期融资券发行成功，发行规模 3 亿元，利率 2.5%，期限 270 日。公司成为网安行业首家发行超短期融资券的企业，是继 2020 年 IPO 登陆股权市场后，在债券市场完成的新突破，标志着公司的资本市场多元化融资体系逐步完善，融资能力与市场认可度获得进一步提升。

5、革新产研架构，组建四大战区

2025 年末，公司在产研体系以“客户价值”为中心，进行了重建产品供给方式的深层次改革与组织升级，全新打造了“4+1”产研架构：即由 4 个面向客户的“产品市场 BG”和 1 个统一研发的“产研 BG”所组成的全新体系。

其中，产品市场 BG 的定位是“前线作战部队”，直接面向客户，深入需求场景理解业务痛点，基于标准化产品及定制开发能力输出有针对性的端到端解决方案，聚焦价值交付和业绩达成。产研 BG 则扮演“后方武器基地”的角色，承担公司级技术架构设

	计、标准产品研发、产品间的整合协同以及产品质量保证，负责产品长期竞争力的打造以及版本维护等“基础设施”工作，以长期主义为导向，确保产品核心竞争力领先。 2026 年，公司将围绕上述新成立的 4 个产品市场 BG，将销售、安服、交付等“军种”力量集结在其周围，组建成立“四大战区”，在战区内形成目标与考核的共同体，落地“战区资源协同、军种目标主责、总部指挥协调”的协同作战体系。 **6、财务管理方面** 在费用支出方面，公司进一步执行了严格的费用管控，报告期内三费总金额较去年同期降低 5.59 亿元，三费费用率同比下降 13.48 个百分点。在现金流管理方面，公司成立了回款专项管理组织，系统性地运营回款，通过识别不同类型的回款问题形成工作流，采取更有针对性的回款举措，以多种手段推动实现回款的“应收尽收”。 **7、2026 年第一季度经营情况** 2026 年第一季度，公司实现营业收入 7.17 亿元，同比增长 4.44%；归母净利润-3.88 亿，同比改善 7.08%；扣非净利润-3.61 亿元，同比改善 12.07%；经营性现金流净额-4.95 亿元，同比改善 35.22%；销售回款 7.83 亿元，同比增长 25.72%。归母净利润、扣非净利润、经营性现金流净额在绝对金额上均创上市以来 Q1 单季度最佳水平，实现新年开门红！ **第二部分由公司管理层与投资者进行问答互动：** **问题一、作为一家在“AI+安全”领域核心竞争力突出的企业，公司如何看待未来如“龙虾”和 Mythos 等新技术对网络安全行业的影响？** **答：**毫无疑问，“AI+安全”未来将成为领跑市场的核心竞争力。AI 已经成为一种革命的力量，开始改造我们的千行百业。这一轮 AI 对千行百业的改造，或者说是“人工智能+千行百业”，它和以往的信息化、数字化转型对我们业务的影响是完全不一样的，数字化转型和 IT 信息化系统的影响都是缓慢的，但人工智能的影响是断崖式的，影响非常直接，直截了当，立竿见影。 2026 年 3 月，以 OpenClaw（“龙虾”）为代表的 AI Agent（智能体）突然爆火，一边带来了生产力突破，一边也“炸”出了安全隐患——权限乱套、高危漏洞、Skills 投毒、数据外泄等风险集中爆发，许多企业刚用上 AI 就踩坑，有些行业的协会、学会、主管部门都发出了使用“龙虾”的风险告警，有些单位甚至直接喊出“龙虾太危险，暂时不能用”。 就在行业犹豫观望、客户“想用又不敢用”时，3 月 16 日，奇安信果断出击，成为业内率先一批站出来直面龙虾风险的团队，当时定的龙虾安全策略就九个字：“看得清、管得住、用得好”。围绕这九个字，公司推出一系列动作：1）发布《政企版龙虾（OpenClaw）安全使用指南》，让广大客户心中有谱，敢上“龙虾”，白皮书一经发布，反响非常热烈；2）发布“龙虾安全伴侣”，端、网、云三层联动，让企业敢用、能用、用得放心；3）天擎、椒图、网络准入、防火墙等拳头产品全线升级，给客户提供全面的“龙虾”私有

	化部署安全方案，彻底解决客户的后顾之忧。这次行动让很多政府和企业客户改变了对“龙虾”的看法，愿意使用“龙虾”或者类似的自主智能体来改造自己的业务，提高质量和效率。 2026 年 4 月，Anthropic 公司的 Mythos 发布，又引发了行业恐慌。Mythos 展示的 AI 漏洞挖掘能力，震惊行业。网络攻击从“手工化”时代跨入“工业化”阶段。全球主要国家及国际组织纷纷紧急研究对策，国内政企客户更是感觉很无助，觉得怎么防都防不住。这时如果没有人站出来把 Mythos 讲清讲透，恐慌就有可能会变成崩溃。所以，4 月 22 日，奇安信又作为业内第一家发布应对白皮书——《Mythos 事件白皮书》，核心观点包括： 1）正视现实。过去那种“发现漏洞、打补丁、再发现、再打补丁”的老办法，在 AI 批量化发动网络攻击的今天已经行不通了。我们必须承认漏洞永远修不完，必须学会“带洞防护” ——带着漏洞也能把系统守住、把业务保住。 2）尽快构建一套“高位、中位、低位”三位一体的内生安全体系，形成具备韧性、能应对极端情况的纵深防御。低位补盲区、中位提效率、高位做加固。允许局部失守，但绝不允许单点失守演化为系统性沦陷。 3）给出了一个完整的建设闭环——“AI 体检-AI 运营-AI 预见-AI 红队”，推动“以 AI 对抗 AI”真正落地。 白皮书发布后，很多客户跟我们说：看完之后踏实了，也知道自己该怎么干了，心里有底了！ 面对这些 AI 大事件，奇安信之所以能够第一时间提供专业和系统的应对方案，要归功于 2026 年 2 月我们专门成立的人工智能子公司。新的人工智能子公司聚合了三支队伍——科学家搞模型、攻防专家攻实战、产品工程师做落地，并且 All in 三大方向：网络安全垂类大模型与 AI 智能体、安全智能（AI for Security）、智能安全（Security for AI）。我们认为，未来的安全对抗，本质就是“以 AI 对抗 AI”，光靠堆人是扛不住 AI 攻击的，也就是说“手工化”对付不了“工业化”，所以我们必须要把安全能力智能化、智能化能力体系化，这是我们未来的起点。 俗话说，没有金刚钻，不揽瓷器活。奇安信能做到比友商快一步，靠的是四大核心优势，即深厚的技术积累、顶尖的攻防队伍、强大的漏洞挖掘能力，以及服务政府、央企、金融等头部客户多年所积累的广泛实战场景： 1）我们拥有先进的人工智能安全研究院，数据与知识储备业界领先；2）我们有国内领先的网络攻击渗透测试队伍，长期开展高强度实战演练，持续保持对前沿攻击手法的敏锐感知；3）我们的威胁情报中心每天研判全球海量的高疑似恶意对象，还发布威胁情报 MCP 服务，深度融合了安全大模型和多维度情报数据。4）长期应对头部客户最艰巨、最复杂的安全需求，持续在实战中磨炼，构成了公司独特的竞争壁垒。 关于市场前景，奇安信有这样一个判断：Mythos 事件不仅是技术里程碑，更是市场爆发点，即所谓的“奇点”。网络安全产业的逻辑彻底改变了。过去是“低频合规”——买个盒子、应付检查、不出事就行；现在是“高频实战”——攻击时刻在发生，合

	规已经远远不够了。一旦防御变成“保命”的刚需，市场就会迎来爆发。而且在高频的网络攻击实战面前，攻击的后果立等可现。同时，因为人工智能的广泛应用和数字化水平的提高，网络被攻击导致的破坏性后果也出现了“奇点式”变化。所有这些变化都会推动中国网络安全产业向着非常健康的方向发展。 参考 IDC 数据，目前中国网络安全市场规模和美国相比，存在 10 倍以上的差距，这个差距在中美两国所有行业对比中都是极其罕见的，也是不利于企业在数字化和人工智能化时代生存与可持续发展、不利于政府提高运行效率和质量、不利于国家数据安全的。所以我们认为，这 10 倍的差距恰恰是未来 10 倍的增长空间。随着攻击“工业化”趋势的加速，中国网络安全市场将迎来爆发式扩容，中美网络安全市场之间的差距会显著缩小。这是一个窗口期，我们要力争牢牢抓住！ **问题二、从战略视角看，公司进行产研架构改革，包括组建“四大战区”，其背后的原因是什么？这将为公司后续发展起到什么样的作用？** **答：**1）我们为什么要改？公司从成立那天起，技术就在行业里打出了口碑。攻防能力强、漏洞挖得深、产品线全，客户一提奇安信会竖起大拇指——技术好、靠得住。但是在公司内部我们经常讲一句话：技术好归技术好，咱们得算账，得赚钱。 过去十多年，我们有一个结构性的矛盾始终没解决好：标品和定制化服务混在一块卖。前端销售面对客户的时候，搞不清楚什么时候该卖标品，什么时候该承诺定制服务。结果就是要么卖了标品的钱，赔了定制化服务的成本——单子签回来了，一算账，没怎么赚钱；要么是重要客户的大项目只顾着上定制化开发，把标品的规模化销售给耽误了。标品和定制化服务这两者搅在一起，卖了一份钱，背了两份成本。 导致的结果就是叫好不叫座。行业里认可奇安信技术领先，然而从财报角度看，企业的盈利能力并不理想。这个问题如果不解决，技术再强也难持续。所以我们下决心，必须把标品和定制化服务拆开——标品归标品，服务归服务，各自算账，各自体现价值。 2）怎么改，也就是成立战区的核心逻辑。这次我们成立四大战区，核心逻辑就八个字：标品打底、场景增量。 首先，标品不会被取代。标准化的网络安全产品是公司的基本盘，成本可控、毛利率高、交付快，这块市场不但不会丢，还要继续做大。我们签的一些千万级大单——某大型商业银行的国产化 NDR、某运营商集团的防病毒软件集采、某家电巨头的终端安全集采——这些都是在标品赛道上的强有力证明。 然而，光有标品并不够。我们发现，央企、军工、金融这些高端客户，有两个新的需求正在爆发：一个是行业批量化定制——不是给某一家定制，而是整个行业有共性需求，我们可以做小批量、高定价的定制开发，交付简单、利润率好；另一个是订阅式运营服务——客户买了标品以后，愿意付年费，让我们持续帮他运营，确保产品真正跑起来、发挥作用。 这两块就是我们说的“双增量”。战区要干的，就是让我们的技术专家、市场 BG 跟

	销售体系绑在一起，直接走到客户的场景里去，把这两个增量挖出来、做深做透。 3）公司的核心策略是什么？就是靠“三位一体”纵深防御来拉动。我们把整个防御体系分成了三个位阶：低位是标品工具，防火墙、EDR、NDR 这些标准化的安全产品是基础武器；中位和高位是我们战区主抓的事，即订阅服务和行业定制。这里有个关键逻辑：中高位做起来后，可以直接拉动低位标品销售。客户上了我们的运营服务，用了我们的定制方案，他对标品工具的依赖和采购意愿会更强。所以我们提了一个概念，叫“三位一体”纵深防御——低位铺工具、中高位做运营和定制，三层联动形成一个闭环，让客户从“买盒子应付检查”变成“建体系持续对抗”。而且这个逻辑在 AI 时代更加成立。大模型解决不了所有问题，必须跟具体业务场景结合。我们战区的技术专家在客户那里，能够把智能体、MCP、Skills 等新技术跟客户的真实需求对接起来，把 AI 的能力真正落到场景里。我们签的几个 AI 大单，例如某头部证券公司的 AISOC 项目，就是战区逻辑落地的典型证明。 总结一下，这次战区调整，本质上是要把过去搅在一起的“标品”和“服务”彻底分开，让标品继续规模化地往上走，让场景化增量服务创造新的利润增长点。用一句话说就是：技术好，也要让技术卖出好价钱，叫好的同时更得叫座。未来我们经营业绩改善的预期，要依托于这个逻辑。希望未来让大家能够看到，奇安信不仅技术强，赚钱的能力也很强。 最后，再说一下战区的结构，其中包括产品市场 BG、交付团队、安服团队、若干营销组织。这四块组成一个战区，他们所有的工作都在封闭的一个战区里，不管是产品市场 BG、交付、服务还是营销组织都不能到战区之外去“打粮食”，一切收入都来自于这个战区。上述四个组织的业绩考核目标是完全绑定在一起的，从而极大地释放了生产力。以前一个销售面对一个客户的产品组合需求，要和后方几十个产品去打交道，这对销售是非常困难的。战区改革之后，销售在面对客户时，无论其需要什么样的产品组合，都只和 BG 的技术专家、产品专家去打交道，从而节约时间，降低成本，提高效率，提高质量。 战区架构在今年一季度已经产生了较为明显的效果，公司归母净利润、扣非净利润和经营性现金流净额这三大财务指标均创造了上市以来最佳水平，这与战区机制的推进是分不开的。我们也期待在 2026 年，在战区机制改革的推动下，公司业绩能够取得更好的成绩。 **问题三、以 AI 对抗 AI，安全厂商和模型厂商的能力区别之处在哪里？价值分配是怎样的？** **答：**对于“AI+安全”，主要的利益都还在安全厂商。人工智能大模型在安全领域的应用和在其他数字化领域里的应用，在模式上没有根本性的差别。以自主智能体在我们业务领域中的应用来做个比喻，基本是三层结构：下面是 AI 大模型，中间是自主智能体，上层是各类工具应用。 对安全也是一样，结合“三位一体”纵深防御体系，可以这样看：

	智能体连接的工具就是我们说的低位的安全能力，包括上百种安全产品，涵盖边界、终端、服务器安全、云安全、身份认证、API 等。这些安全产品在“AI+安全”时代下，变成了智能体的工具。如果没有工具，智能体是无法去做复杂任务的，这在其他行业也是一样的。工具又分为复杂工具和简单工具，其中的简单工具通过 Skill 就能完成，而复杂工具往往则需要场景化。 对于中间层，刚才说到的自主智能体就包括我们的 AISOC、AI 天眼等拳头产品，以及 AI 资产管理运营平台、AI 的 API 运营平台等，需要和 AI 深度融合，具体方式有两种：一种是用安全的需求把原来运营中心的平台和 AI 深度融合，变成一个较为复杂的智能体或者智能体+运营平台。第二种是用安全技术来训练安全垂域大模型，这类大模型多数是在本地部署的。因此，参照上述架构，AISOC 完全是安全厂商自研的，即智能体这一层是安全厂商自研的，智能体所连接的工具也都是安全厂商自己的，操作和设计“AI+安全”的也是安全公司做的。 在高位能力上，例如威胁情报以及对安全问题的发现和定位，才需要用到大模型的技术。而大模型的技术因为涉及安全的特殊性，因此多数情况下会用安全厂商自己训练的安全垂域大模型。使用通用大模型的服务，只占我们对外使用资源的一部分。从利益分配角度来说，大模型厂商拿走的那部分，体量上会小于其他行业大模型参与的利益分配。 总结一下，“AI+安全”为整个安全行业带来了巨大的利好：用 AI 改造之后的中位安全能力和高位安全能力可以给客户提供订阅服务从而创收。有了中位和高位安全能力的智能化，又能发现低位工具类安全产品数量和质量的不足，因此市场规模会被放大。目前许多客户部署低位安全工具的数量都严重不足，把数量补足本身就是扩容。同时，客户使用智能体运营安全工具时，会发现安全工具的效果有差别，采购安全工具时有望“以质定价”，从而推动好用的安全工具价格往上走。 **问题四、Mythos 出来后，客户和监管等方面的反应是什么样的？** **答：**客户方面，在“三位一体”的纵深管理体系中，三个层面的预算都会增加。低位能力层面，一是原来买便宜的工具，现在买质量好的、价格高的工具；二是原来买的工具数量不够，现在要补充数量。中位能力层面，原来买 SOC 就可以，现在 SOC 要与 AI 相融合，虽然看上去不用增加人力了，但是算力投入会增加，所以客户在这方面的预算也会提升。高位能力层面，要么用更高的价格购买安全公司的威胁情报，要么就自己投入资金，在安全公司指导下，外购威胁情报和自建威胁情报相结合，这些都需要安全预算大幅度的提升。目前我们已经看到了“补数量”和“提质量”的强烈要求，这些要求往往都是从头部企业反映出来的，尤其是大型制造业企业，和人工智能的结合度相对更紧密。政府和国有企业在预算上还需要一个过程。 监管方面也在发生明显的变化。过去攻击或攻击事故是小概率事件，因此监管的方式以检查为主。但是当攻击和网络安全事件变成大概率事件时，监管方式则会发生变化： 中国对网络安全的监管主要依托于“三法两条例”等重要的法律法规，包括《网络

	安全法》《数据安全法》《个人信息保护法》，以及《计算机等级保护条例》和《关键信息基础设施保护条例》等。尤其上述两个条例，是落地的最强监管手段。大家熟知的“等保合规”，是一个静态的底线标准，例如某单位建一套计算机等级保护系统，通过第三方评估，得到一张符合计算机等级保护规定的证书，有效期一到三年不等。《关键信息基础设施保护条例》中强调的不再是静态，而是“三化六防”，强调动态防御，只符合规定还不够，最终要确保不出问题，要实现动态的防护。但是，各单位的计算机体系是否符合动态防御，是否符合“三化六防”，以前尚未作为监管部门的重要监管事项，也没有足够有效的验证方法。因为安全体系是不是纵深化，是不是符合实战化，实际上要靠市场来检验。 Mythos 事件发生后，奇安信作为厂商代表，参与过监管部门的一些讨论会，能够明显感受到监管部门在评判政企单位的网络安全建设是否合规时，逐渐将责任重心由“检查-评估-发证”的体系转移到政府和企业客户自身，要求各单位真正做到“三化六防”。一旦宣称已经做到了“三化六防”，出现事故后，追究责任的力度是不一样的。这也促使了政府和企业在建立“三化六防”纵深防御体系时自主积极性的提高。小概率事件还可以凭运气，当网络攻击变成大概率事件，靠运气躲不过去时，未按照“三化六防”建立防御体系的单位，责任往往难以说清。同时根据这段时间与客户的沟通，客户对我们的“三位一体”纵深防御体系架构非常认同。我们已经启动了一批紧急项目，以安全改造的形式，帮助客户在“十五五”期间把他们现有的安全体系改造成为符合“三化六防”要求的纵深防御体系，这也是一个业务增量。 **问题五、以 AI 对抗 AI，有什么具体步骤么？** **答：**第一步，是中位能力 AI 化，没有中位能力就检验不出低位安全产品是否有效，通过 0-Day 漏洞打进来的东西发现不了。所以首先要把中位能力 AI 化。 第二步，低位的安全产品要补全化。通常在一个集团层面的网络架构中，各个出口、各个终端、各个网络单元都部署了合适的安全工具且数量足够。然而在二级单位、三级单位、四级单位却没有足额数量的部署。现在 AI 时代下，只要有一个地方形成“口子”，AI 攻击的洪流就能够把整个网络体系冲垮。所以第二步，是补数量。 第三步，提质量，通过更换一些不合格的安全产品和安全工具，让体系更加健壮。 我们说纵深防御体系，比如终端没有防住，攻击就进去了。进去以后可能会找服务器，到了服务器如果还没有防住，后面可能会去找云。如果云也没有防住，在云上大概率就会去找数据。假设账号密码失窃，数据系统这关也没防住，攻击者就可能对数据进行敏感操作。这些全都没有防住的话，整个信息系统就彻底崩掉了。所以对于一个攻击来说，安全厂商至少有七八种乃至更多的安全品类有机会发现进入到内网里的攻击。关键是把发现的这些线索，能够用一个非常聪明的 AISOC 进行联动式的威胁发现计算，并把攻击截断在路上，从而保证我们的系统的安全。 最后总结下，第一步是先把运营 AI 化，第二步把数量不全的安全工具补全，第三步把不合格的安全工具替换成合格的。

问题六、随着 AI 和自动攻防的发展，安全运营及人力方面的需求会不会减少？

答：网络安全运营的人员并不会减少，反而还会再增加。因为实际情况是，目前人力的数量尚且不够，以至于只能处理 1%-2%的告警信息。对于安全运营 AI 化，即处理全量告警信息，机器是能够发挥决定性作用的。但与此同时，依然需要大量的人工去梳理并判断一些敏感的结果。因此，网络安全运营因 AI 的引入导致从业人员失业的风险并不大，相反人工需求可能还会因此提升。

——结束——

附件清单（参会机构人员单位、姓名）

附：线上参会机构名单，按所在机构拼音首字母排序。

机构名称	参会者姓名
北京和信金创投资管理有限公司	黄庆铭
北京泾谷私募基金管理有限公司	蒋海
北京久阳润泉资本管理中心	赵炜
北京朗辉信泽投资管理有限公司	陈明波
北京微村智科基金管理有限公司	赵培恩
北京禹田资本管理有限公司	赵玮玮
北京中泽控股集团有限公司	刘军洁
创金合信基金管理有限公司	李晗
重庆渝汇投资(集团)有限公司	李树平
东北证券股份有限公司	马宗铠
东方证券股份有限公司	浦俊懿
东吴证券股份有限公司	黄诗涛
东吴证券股份有限公司	戴晨
福建金牛投资管理股份有限公司	梁敏忠
富瑞金融集团香港有限公司	张朗铭
光大证券股份有限公司	刘勇
广东邦政资产管理有限公司	熊政
广发证券股份有限公司	李婉云
国海证券股份有限公司	伍海量
国金证券股份有限公司	李忠宇
国盛证券有限责任公司	李可夫
国泰海通证券股份有限公司	楼剑雄
国投证券股份有限公司	王永彬
国信弘盛创业投资有限公司	杨嘉
国信证券股份有限公司	库宏垚
国元证券股份有限公司	耿军军
果行育德管理咨询有限公司	宋海亮
杭州致道投资有限公司	刘福杰
合方创新基金管理有限公司	任熠
鸿运私募基金管理有限公司	张丽青
鸿运私募基金管理有限公司	舒殷
湖南潇湘资本投资管理有限公司	陈靓璇

华安证券股份有限公司	来祚豪
华创证券有限责任公司	胡昕安
华福证券股份有限公司	魏征宇
华泰证券股份有限公司	范昳蕊
汇丰前海证券有限责任公司	刘逸然
美银证券	庄亚林
美银证券	李慧群
青榕资产管理有限公司	唐明
全天候基金投资管理合伙企业	胡聪玲
瑞银资产管理(香港)有限公司	丁宁
赛伯乐投资集团有限公司	程凯
上海国理投资有限公司	岳政
上海合道资产管理有限公司	严思宏
上海环懿私募基金管理有限公司	杨伟
上海加盛投资管理有限公司	陈科
上海金恩投资有限公司	林仁兴
上海君璞投资咨询有限公司	高翔
上海联视投资管理有限公司	周申力
上海秋阳予梁投资管理有限公司	郑捷
上海润桂投资管理有限公司	金勇
上海远海私募基金管理有限公司	邵万琦
上海匀升投资管理有限公司	饶欣莹
上海肇万资产管理有限公司	崔磊
上海致君资产管理有限公司	王鸣飞
深圳丞毅投资有限公司	胡亚男
深圳市尚诚资产管理有限公司	黄向前
深圳中天汇富基金管理有限公司	古道和
西部利得基金管理有限公司	冯皓琪
西部证券股份有限公司	周成
兴业证券股份有限公司	蒋佳霖
玄卜投资(上海)有限公司	李苗苗
浙江壁虎投资管理有限公司	张小东
浙商证券股份有限公司	刘雯蜀
中国国际金融股份有限公司	梁善晴
中国国际金融股份有限公司	于钟海
中国国际金融股份有限公司	韩蕊
中国国际金融股份有限公司	李铭妯
中信证券股份有限公司	潘儒琛
中信证券股份有限公司	王盛乾
中银基金管理有限公司	张令泓
中邮证券有限责任公司	王思
中邮证券有限责任公司	孙鹏
中邮资本管理有限公司	仇振洋
Global Telecom Capital	Li Yiming
TOPAZ FAMILY OFFICE LIMITED	范志鹏

本次活动是否涉及应当披露重大信息	否
日期	2026 年 4 月 30 日