公司代码：688030　　公司简称：山石网科

山石网科通信技术股份有限公司

2025 年年度报告摘要

第一节 重要提示

1、 本年度报告摘要来自年度报告全文，为全面了解本公司的经营成果、财务状况及未来发展规划，投资者应当到 www.sse.com.cn 网站仔细阅读年度报告全文。

2、 重大风险提示

公司已在本报告中详细说明公司在经营过程中可能面临的各种风险，敬请查阅本报告第三节“管理层讨论与分析”。

3、 本公司董事会及董事、高级管理人员保证年度报告内容的真实性、准确性、完整性，不存在虚假记载、误导性陈述或重大遗漏，并承担个别和连带的法律责任。

4、 公司全体董事出席董事会会议。

5、 致同会计师事务所（特殊普通合伙）为本公司出具了标准无保留意见的审计报告。

6、 公司上市时未盈利且尚未实现盈利

□是 √否

7、 董事会决议通过的本报告期利润分配预案或公积金转增股本预案

经公司第三届董事会第十一次会议决议，截至2025年12月31日，母公司期末可供分配利润为-256,263,947.37元，根据《上市公司监管指引第3号——上市公司现金分红》《山石网科通信技术股份有限公司章程》等相关规定，不满足利润分配条件，综合考虑公司未来经营计划和资金需求，公司2025年度拟不进行利润分配，也不进行资本公积转增股本和其他形式的分配。

上述利润分配方案需经公司2025年年度股东会审议通过后实施。

母公司存在未弥补亏损

√适用 □不适用

截至2025年12月31日，母公司期末可供分配利润为-256,263,947.37元，存在累计未弥补亏损，根据《中华人民共和国公司法》《上市公司监管指引第3号——上市公司现金分红》《山石网科通信技术股份有限公司章程》等相关规定，公司目前不满足实施现金分红的前提条件。敬请广大投资者注意相关投资风险。

公司将严格按照相关法律法规和《公司章程》等规定，为中小股东参与现金分红决策提供便利。同时公司将积极提升发展质量，做好主责主业，改善盈利能力，努力为投资者创造并提供稳

定、长效的回报。

8、 是否存在公司治理特殊安排等重要事项

□适用 √不适用

第二节 公司基本情况

1、 公司简介

1.1 公司股票简况

√适用 □不适用

公司股票简况				
股票种类	股票上市交易所及板块	股票简称	股票代码	变更前股票简称
A股	上海证券交易所科创板	山石网科	688030	无

1.2 公司存托凭证简况

□适用 √不适用

1.3 联系人和联系方式

	董事会秘书	证券事务代表
姓名	尚喜鹤	何远涛
联系地址	苏州高新区景润路181号	苏州高新区景润路181号
电话	0512-66806591	0512-66806591
传真	0512-66806591	0512-66806591
电子信箱	ir@hillstonenet.com	ir@hillstonenet.com

2、 报告期公司主要业务简介

2.1 主要业务、主要产品或服务情况

2025 年，公司聚焦网络安全主业，坚定推进以自研 ASIC 安全专用芯片和 AI 技术为核心的“双 A 战略”，通过硬件与智能技术的深度融合构建全域安全防护体系。全年实现了 ASIC 芯片核心技术研发落地和 AI 核心能力持续突破，业务已覆盖基础设施安全、云安全、数据安全、应用安全、安全运营、工业互联网安全、信息技术应用创新、AI 安全、安全服务、安全教育等 10 大类产品及服务，形成 50 余个行业场景解决方案。2026 年，公司将把 ASIC 芯片与 AI 能力全面融入全系产品，重塑国产化安全矩阵，实现产品性能跃升，为千行百业交付“芯片定义安全、AI 驱动智能”的全栈安全解决方案与服务。

1、公司主要业务及产品

2、报告期内公司主要业务及产品进展情况

（1）边界安全

公司以“双 A 战略”为核心持续深耕边界安全领域，完善产品组合与功能模块，形成多场景、多层级、多形态的防护解决方案，首批集成自研 ASIC 芯片的防火墙产品成功发布，显著提升国产替代和信创市场竞争力。

精准布局信创市场：发布涵盖 4G 至 60G 全档位的多款盒式信创防火墙，推出支持国密 SM1 算法的产品型号，满足党政、金融等行业合规与性能双重需求；逐渐推出 30G~200G 档位信创防火墙型号，凭借 ASIC 芯片的高性能、低时延优势，成为金融、政务、能源等高安全要求场景的国产化防护屏障。IDPS 产品完成 v5.5、v6.1 两大主线版本迭代，新增 4 款国产化型号，匹配中小用户对中低端国产化型号的性能诉求，并从威胁检测、运维管理、国产化适配等维度全面提升能力，强化国产替代领域核心竞争力。

深度下沉商用市场：推出多款 2G 档位桌面型及机架型防火墙，全面覆盖政府、医疗、企业、教育等行业基层机构与中小企业的轻量化边界防护需求，完善商用市场产品布局。

核心系统迭代升级：发布 StoneOS v5.5R12 版本，围绕“开放融合、AI 赋能、智慧运维”完成 335 项功能特性升级，推动产品从工具型系统向智能安全中枢演进，打造一体化安全能力底座。

报告期内，公司边界安全产品与服务实现营业收入 67,396.75 万元，同比下降 9.94%。

（2）云安全

公司聚焦打造“云安全原子级防护能力”，推进云工作负载全方位防护平台建设，优化云安全管理体系，形成全栈式、可扩展、可定制的云计算安全解决方案，广泛兼容私有云、公有云、多云及混合云架构，无缝适配物理服务器、虚拟机、容器等多种工作负载形态，全面覆盖各类云环境安全需求。2025 年云安全核心产品能力、生态合作与行业落地均实现提升：

山石云·界：基于 StoneOS 5.5R12 版本完成策略增强、高级威胁防护、ZTNA（零信任网络访问）能力提升等数百项功能升级，产品稳定性、兼容性与易用性大幅提升，成功支撑多个大型政企客户云边界的高效部署与运维。

山石云铠主机安全防护平台（CNAPP）正式发布 v1.0R5 版本及多款 R5P 版本，平台新增网络入侵防护、应用实时防护（RASP）、主机入侵行为检测等多项威胁防护能力；核心微隔离功能进一步优化升级，精细化管控水平显著提高，同时新增配置预提交机制。此外，平台溯源分析能力得到优化，新增案件调查与病毒采样功能，为安全事件的深度处置提供强有力支撑。商业模式方面，采用功能模块拆分授权模式，能够灵活适配不同场景下客户的安全建设需求。

报告期内，公司山石云·格、山石云·池等云安全产品也进行了功能升级或版本迭代。

报告期内，公司云安全产品与服务实现营业收入 7,945.80 万元，同比增长 56.56%。

（3）其他安全

I.数据安全

报告期内，公司从产品、服务、技术赋能多维度升级数据安全治理能力：发布《数据安全治理白皮书 v4.0》《数据安全解码手册 v3.0》，夯实数据安全治理理论与实践基础；完善人工智能数据安全服务体系，形成 AI 环境安全、智能体开发、提示词测试、大模型算法备案 4 项核心服务；AI 技术持续赋能数据安全治理，依托山石灵岩大模型应用平台，实现海量数据的自动化扫描、识别、标签化处理，精准判定数据类别及安全等级，大幅提升数据治理效率；创新推出数据安全产品租赁服务，降低企业前期一次性资金投入与整体治理成本；发布 API 安全 2.0，强化访问控制、HTTPS 代理及多功能安全插件能力，实现数据共享场景下 API 安全风险的深度加固与全域防护。

II.安全服务

报告期内，安全服务业务规模实现大幅增长，构建起以安全评估、安全咨询、安全运营为核心的全流程综合安全服务体系，具备从问题发现、建设整改到持续运营的一体化服务能力。安全评估引入并优化网站监测、攻击面管理、托管渗透等在线交付服务，与技术专家服务形成互补，提升服务交付标准与质量；安全咨询在银行、期货、高校、半导体、制药等多细分行业，成功交付网络安全、数据安全及 AI 安全领域规划咨询标杆案例，其中数据安全治理服务成为数据安全业务的核心增长点；安全运营组建 7×24 小时专家团队，依托自研 AI 智能体辅助开展服务，实现安全运营的标准化、智能化与高质量交付。同时围绕体系建设、能力提升、交付管理开展多项专项工作，在数据安全、安全运营的业务拓展与服务交付上取得积极成果，夯实综合服务能力。

III.应用安全

应用交付（ADC）：围绕金融、能源等重点行业核心需求推进产品迭代，推出 3 大主线版本及 1 款高端国产化型号，从性能、稳定性、运维管理、国产化适配率等维度实现全方位升级，加速对国外产品的替代进程。核心强化加密流量编排（SSLO）能力，优化同类产品脚本兼容能力以提升替换落地效率，完善全局负载均衡（GSLB）场景化功能，升级集群能力以适配大型银行等客户业务需求，全面兼容国密/非国密加速卡，实现各应用场景下的性能大幅提升。

WAF：完成两大主线版本迭代及操作系统向 R12 主线版本的升级，为后续 ASIC 平台导入打好技术基础；推出 iWAF（极速 · 智御）全新产品理念，融合 ASIC/FPGA 芯片加速技术与智能算法，实现主干网全域串联式防护，依托自识别自防御能力及 GenAI 技术，精准识别网络威胁、化解资产暴露隐患，破解企业资产检测难、高流量负荷承压的行业痛点；同步发布 iWAF 首款高端型号，并推出高校专属解决方案，针对性解决高校大流量瓶颈、资产检测困难等问题，拓宽产品应用场景。

大模型应用防火墙（MAF）：发布专为大模型应用场景打造的 MAF 产品，部署于智能应用与模型服务之间，具备请求保护、响应保护双重防护机制及 Web 安全防护能力，可抵御提示词注入、恶意 URL 等威胁，把控内容安全与数据库操作规范，为大模型全生态应用提供全流程 AI 运行时与 Web 安全防护。目前已推出两款高性能国产化型号及虚拟化型号，可灵活适配各类部署场景，支持外接检测模型提升检测能力，满足不同场景下大模型安全防护需求。

IV.安全运营及端点安全

Open XDR：以山石智源平台为核心联动 NGFW、EDR 等多元安全能力，实现威胁检测、处

置、响应闭环的一体化安全运营。2025年发布智源63A系列4款新品及V2.0R14主线版本，63A系列以高可靠架构实现性能全面升级；V2.0R14版本优化北向数据开放与应用中心联动能力，新增AI助手、案件调查智能体等功能提升运营效率，升级威胁态势概览与案件调查体系，强化智慧运维，进一步巩固XDR领域领先地位。

EDR：发布山石智铠v5.0R6及多款R6P版本，完成多维度功能升级并优化终端安全管理与防护效能；持续坚守“ZTNA+EPP+EDR+DLP”四重防护策略，从零信任访问、终端防护等多维度，为用户构建更立体、可靠的终端安全。

V.综合实训平台

网络安全综合仿真靶场围绕核心理念完成产品迭代，具备直播、AI智能体、AI赛、沙盒攻防赛等功能，丰富实训与攻防演练场景；全面响应国产化与实战化需求，完成国产芯片与操作系统的适配并正式发布，进一步提升平台的国产化适配能力与实战化水平。

VI.工控安全

报告期内，对工业防火墙、工控安全监测审计、工业入侵检测三大核心产品开展技术迭代与能力升级。核心产品均完成版本迭代，发布国产化及全国产型号，实现国产芯片与操作系统的全面适配，全面响应国产化替代与实战化防护需求；工业防火墙具备多种工业协议深度解析、HA高可用及零信任ZTNA能力，融入XDR整体解决方案，实现从协议防护到纵深防御的升级；工控安全监测审计产品支持百余种工业协议解析与数千种恶意代码识别，提升工控系统威胁可见性与合规效率；工业入侵检测产品特征库超万条，支持协议基线自学习与异常行为检测，强化跨域攻击与高级威胁的精准识别和实时响应。

报告期内，公司其他安全产品与服务实现营业收入15,587.43万元，同比下降17.39%。

2.2 主要经营模式

1、销售模式

报告期内，公司采用直销和渠道代理销售相结合的模式，并以渠道代理为主。

（1）直销模式

基于部分电信运营商、金融机构及大型企业对于采购成本、服务质量的严苛要求，公司对此类重要客户主要采取直销模式，便于公司安排专业销售及技术人员为客户提供更好的服务。此外，

公司以直接供应商身份参与国家重点行业集中采购并入围集中采购名录，是对公司技术、实力的一项重要认可，有利于打造公司品牌形象。

公司通过参与招投标、邀标谈判的方式获取直销客户。直销模式下，公司严格履行客户的招投标程序，公司定价以市场竞争为原则，根据客户对产品性能需求、预算和市场竞争情况确定投标价格和谈判的报价。一般情况下，公司根据直销客户招投标或邀标的要求、客户合同模板约定、客户内部建设项目竣工验收安排等因素确定信用期，通过电汇、银承、商承结算。

（2）渠道代理模式

报告期内，公司渠道代理商分为总代理商、白金和金牌、认证代理商。其中，总代理商可以直接向公司进行采购。一般情况下，白金、金牌、认证代理商直接与总代理商签订订单合同，并通过总代理商下单提货。

报告期内，公司采用直销和渠道代理销售相结合并以渠道代理为主的销售模式，降低了企业的资金风险，加大了对终端用户的覆盖面，公司将延续现有的经营模式，并不断加强渠道建设工作。

2、采购模式

公司物料采购可以分为生产性物料采购和非生产性物料采购，其中生产性物料包括委托加工类和直采类。公司采购的主要物料包括自主研发的硬件平台（委托加工模式）、工控机、服务器、硬盘、电源、光模块、包装材料等。公司拥有独立的供应链体系，物料采购主要由采购部门执行，工程部、计划部、质量部、生产运营部等进行必要协助，确保采购的产品和服务持续满足公司客户的要求，并通过持续稳定的供应链体系支持公司整个业务发展的需求。

3、生产模式

公司主要销售的网络安全硬件设备和软件由公司自主研发设计，经过严格缜密的组装灌装，并最终交付给客户。公司硬件设备主要采取代工模式生产，产品全部在公司认证的专线完成电子线路板生产，统一经过严苛的设备组装、生产测试、预装软件、烤机、检测包装等环节。部分产品下线后安装公司自主研发安全软件并由公司质量部门进行检验，检验通过后采取直运模式交付给终端客户或渠道代理商。同时，为满足不同重要客户的需求，公司少量产品由代工厂组装后交付至公司质量部门检验，检验通过后交付给公司自有车间进行定制生产，保证了该部分产品的特殊性及保密性。

公司产品主要采取标准化生产模式，根据不同部署场景及性能需求，公司提供多种性能层级的标准化的安全解决方案。

4、研发模式

公司的产品研发设计，以技术创新为导向，将客户需求及反馈融入到产品规划、设计、研发和服务的全过程中，研发工作通过“规划—设计—交付—反馈—升级”的良性循环，不断加强产品能力并提升用户体验。

公司的产品研发采用矩阵模式进行，除产品研发团队外，市场部门、销售部门、运营部门也有指定资源全程参与，从而保证产品在设计研发的所有阶段，可以充分考虑市场需求和客户反馈。产品在交付后，确保可以迅速实现大规模生产和销售。

公司的研发部门主要由苏州、北京、美国硅谷三地研发团队构成。研发阶段主要分为需求阶段、设计阶段、开发阶段及测试阶段 4 个阶段。随着公司产品品类的不断丰富和市场变化逐渐加快，公司在瀑布式开发模式的基础上，引入了敏捷开发模式，针对不同特点的产品采用不同的开发方式。

报告期内，公司主要经营模式未发生重大变化。

2.3 所处行业情况

(1). 行业的发展阶段、基本特点、主要技术门槛

2025 年，网络安全行业仍未出现明显复苏，下游需求疲软，市场竞争加剧。面对宏观经济承压与行业的阶段性调整，安全厂商如何摆脱“碎片化、低质量、重复化”的低效竞争，通过技术创新与业务模式创新提升运营效率，进而构建可持续盈利能力，成为行业新方向。同时，AI 技术的大规模应用成为网络安全市场竞争的新变量，如何实现 AI 对技术与产品的赋能、利用 AI 提升服务效率与内部运营质量、把握 AI 带来的新兴安全市场机会，也成为行业内重点探索方向。2025 年，新修订的《网络安全法》审议通过，并于 2026 年 1 月 1 日起施行，修订以“强化责任、适配 AI、衔接多法”为核心，成为行业发展重要法规指引。

2025 年，《中共中央关于制定国民经济和社会发展第十五个五年规划的建议》（以下简称“《建议》”）发布。《建议》明确提出“加快高水平科技自立自强，引领发展新质生产力”“构建大安全格局，筑牢国家安全屏障”，将网络安全提升至国家战略核心层级。《建议》首次将网络安全与经济发展、科技自立自强、社会稳定置于同等战略高度，强调“强化网络安全、数据安全、关键信

息基础设施安全保障”，要求网络安全从“被动防御”转向“主动护航”，为数字经济筑牢“安全底座”。《建议》为网络安全产业划定了“自主、智能、合规、场景、生态”的发展蓝图，网络安全已成为数字经济发展不可或缺的关键基础能力，顶层立法与政策导向为行业长期发展注入强劲动力，也推动网络安全厂商加快核心技术突破与综合服务能力提升，以适配政策与市场需求。

根据 IDC《2025 年第二季度中国安全硬件市场预测报告》数据，2024 年中国安全硬件市场营收 210.2 亿元，同比下降 6.5%；2025 年上半年安全硬件市场规模 70.96 亿元，同比下降 3.2%。IDC 预测，2024-2029 年安全硬件市场复合增速 4.4%，2029 年有望达到 257 亿元。根据 IDC《2025 年第二季度中国安全硬件市场预测报告》数据，2024 年防火墙整体市场规模 143 亿元，为安全硬件里面不可或缺的、占据主流地位的单品市场，占比连续 5 年提升；放眼未来，IDC 预测 2024-2029 年防火墙整体市场五年复合增速 4.9%，2029 年有望达到 178 亿元。山石网科依托自研 ASIC 安全芯片核心技术，搭载 ASIC 芯片的防火墙产品在时延、吞吐等关键性能指标处于行业领先水平，聚焦金融、运营商、能源、教育等重点行业，持续提升防火墙市场份额。

根据 IDC《中国 IT 安全软件市场跟踪报告，2025H1》，2024 年信息与数据安全软件市场规模 71 亿元，同比增长 6.14%；2025 年上半年市场规模 25.62 亿元，同比增长 4.5%。IDC 预测 2024-2029 年信息与数据安全软件年复合增速 11.6%，2029 年将达到 112 亿元。山石网科将数据安全及服务打造为第二增长曲线，通过数据安全治理与安全服务介入客户顶层设计，提升单一客户价值与合作粘性。相关业务近年保持高速增长，在重点行业客户持续落地标杆案例，并以“咨询-部署-运营-应急”一站式服务带动产品销售，逐步释放市场回报。

从下游市场看，信创领域具备长期增长动力。《建议》反复强调“加强重点领域关键核心技术攻关取得决定性突破”，明确将芯片、基础软件、安全算法等纳入攻关重点，要求网络安全产业实现“从单一产品国产化”向“芯片-软件-生态全链条自主可控”升级，防范供应链安全风险，保障安全体系独立性。山石网科已搭建完整国产化安全产品矩阵与解决方案，深度适配国产软硬件生态，并于 2025 年完成 ASIC 安全芯片研发，实现国产化安全芯片核心技术突破，构建覆盖信创安全的完整技术体系。

在 AI 安全治理方面，新修订的《网络安全法》增设人工智能专门条款，《人工智能生成合成内容标识办法》《网络安全技术 生成式人工智能服务安全基本要求》《网络安全标准实践指南——生成式人工智能服务安全应急响应指南》等规则密集出台。国务院发布的《关于深入实施“人工智能+”行动的意见》中，专门对提升人工智能安全能力水平作出部署，强调“推动模型算法、

数据资源、基础设施、应用系统等安全能力建设”，防范模型黑箱、算法歧视等各类风险，同时明确要求加快构建“动态敏捷、多元协同的人工智能治理格局”，为我国人工智能安全治理确立了发展与安全并重的基本原则。山石网科聚焦大模型面临的提示注入、敏感信息泄露、供应链风险、模型滥用及内容合规等安全威胁，不断建设和推出系统性 AI 安全防护解决方案。

(2)．公司所处的行业地位分析及其变化情况

2025 年 1 月，公司数据安全治理平台产品入选 Gartner®《中国市场：“数据安全平台市场指南”》报告，首次发布便入选，被评为代表厂商。

2025 年 3 月，公司零信任解决方案入选 Forrester《零信任平台市场格局（2025Q1）》报告，被评为代表厂商。

2025 年 4 月，公司网络威胁检测与响应产品入选 Gartner®《网络检测与响应（NDR）实施架构设计》报告，被评为代表厂商。

2025 年 6 月，公司运维安全网关产品入选 Gartner®《中国特权访问管理市场指南》报告，首次发布便入选，被评为代表厂商。

2025 年 6 月，公司云防火墙产品入选 Gartner®《云防火墙市场指南》报告，首次发布便入选，被评为代表厂商。

2025 年 7 月，公司入选 Gartner®《2025 年中国网络安全成熟度曲线》报告，并在数据安全平台技术领域被列为代表厂商，这也是山石网科连续第四年入选此报告。

2025 年 7 月，在 2025 中国科创领袖大会上，山石网科凭借“双 A 战略”的硬核突破，获评“2025 年最具创新力科创板上市公司”称号。

2025 年 7 月，IDC 发布的《中国安全智能体市场概览，2025：东风已至，未来可期》报告显示，山石网科入选了“安全运营智能体，安全检测智能体”2 个分类。

2025 年 7 月，IDC 发布的《中国大模型安全保护市场概览，2025：全方位安全检测与防护构建可信 AI》报告显示，山石网科入选了全部“大模型输入内容控制，大模型输出内容控制，大模型访问控制，保护大模型接口，大模型可用性检测，构建安全大模型，保护大模型数据存储”7 个二级分类。

2025 年 8 月，IDC 发布《中国 GenAI 赋能的混合部署防火墙平台报告，2025》，山石网科作

为代表性厂商入围。

2025 年 8 月，山石网科入围 IDC《中国统一终端安全技术评估，2025》报告。

2025 年 9 月，公司零信任访问解决方案入选 Gartner®《中国零信任网络访问市场指南》报告，被评为代表厂商，这也是山石网科连续第二年入选此报告。

2025 年 9 月，山石网科在安全牛发布的《私有云泛主机安全技术与应用研究 2025》报告中被推荐为特色厂商，山石云铠主机安全防护平台（CNAPP）获得认可。

2025 年 10 月，公司网络威胁检测与响应产品 NDR 入选 Gartner® Peer Insights™《网络检测与响应（NDR）》客户之声报告，连续 3 年获“强劲表现者”称号。

2025 年 10 月，IDC 发布的《2025 年第二季度中国安全硬件市场跟踪报告》显示，2025 年上半年，山石网科在中国统一威胁管理（UTM）硬件市场主要厂商市场份额中排名第三，产品能力和技术创新体系获得市场高度认可。

2025 年 11 月，公司数据防泄漏产品入选 Gartner®《数据防泄漏市场指南——中国篇》报告，首次发布便入选，被评为代表厂商。

2025 年 11 月，安全牛发布《AI 时代勒索软件威胁与防护技术应用指南》，山石网科作为特色厂商入围，山石智铠统一终端安全管理系统（EDR）获得认可。

(3)．报告期内新技术、新产业、新业态、新模式的发展情况和未来发展趋势

（1）人工智能技术发展趋势

全球人工智能技术与网络安全软硬件产品深度融合成为行业核心发展趋势，呈现硬件高性能化、软件智能化、服务自动化的显著特征，网络安全产品也从传统单点防御，逐步演进为以智能安全运营平台为核心的体系化防御模式，可融合多源安全数据开展 AI 深度关联分析与自动化响应，推动安全防护从“被动防御”向“主动应对”转变。山石网科以“双 A 战略”为核心，实现硬件层 ASIC 芯片构建性能底座与软件层 AI 大模型智能赋能的深度融合，战略上兼顾“用 AI 做安全”与“为 AI 做安全”，通过 OpenXDR（开放式扩展检测与响应）安全运营平台等实现安全能力自动化运营，降低对人工专家的依赖；行业竞争也从单一产品竞争转向以开放平台为核心的生态能力竞争，技术融合的最终目标聚焦解决各行业场景化的安全与效率问题，实现网络安全从合规满足到业务价值守护的跨越。

（2）后量子密码技术发展趋势

后量子密码与网络安全软硬件产品结合成为全球网络安全行业重要发展方向，受量子计算带来的安全威胁影响，国际和国内的关键行业也将布局量子抗性建设，而后量子密码算法计算复杂度高、密钥尺寸大的特点，对硬件性能提出更高要求。山石网科自研的 ASIC 安全芯片可实现后量子密码运算的硬件加速，还可与可信平台模块 TPM 技术结合构建硬件信任根，从源头增强系统安全性；应用层面，后量子密码技术将分层融入 IPsec/SSL VPN 等核心安全协议、数据加密存储传输、身份认证等环节，其引入带来的密钥管理、性能监控等复杂度问题，可通过 AI 智能体与安全运营平台实现自动化监控、智能分析与响应。后量子密码技术发展属于系统工程，当前，后量子密码算法能力与山石网科硬件的融合正在研发进程中，公司也将通过与行业伙伴开展战略合作补齐技术能力，分阶段、分层级将后量子密码技术融入全栈产品与解决方案，依托“双 A 战略”实现芯片级性能支撑与智能化运营管理的协同，为后量子时代网络安全建设奠定基础。

3、 公司主要会计数据和财务指标

3.1 近 3 年的主要会计数据和财务指标

单位：元　币种：人民币

	2025年	2024年	本年比上年增减(%)	2023年
总资产	1,963,288,075.63	1,985,452,032.75	-1.12	1,852,071,698.16
归属于上市公司股东的净资产	731,391,609.79	922,498,947.25	-20.72	1,078,942,643.90
营业收入	911,405,334.74	996,589,519.06	-8.55	901,040,067.77
扣除与主营业务无关的业务收入和不具备商业实质的收入后的营业收入	909,299,795.52	987,777,507.78	-7.94	890,664,719.34
利润总额	-204,955,231.85	-144,123,072.96	不适用	-260,327,464.13
归属于上市公司股东的净利润	-193,542,956.50	-137,208,201.10	不适用	-239,811,522.01
归属于上市公司股东的扣除非经常性损益的净利润	-196,560,576.86	-151,005,942.88	不适用	-248,593,008.86
经营活动产生的现金流量净额	-109,738,305.28	-90,212,983.42	不适用	-58,254,382.32
加权平均净资产收益率（%）	-23.41	-13.69	减少9.72个百分点	-20.01
基本每股收益（元／股）	-1.0738	-0.7613	不适用	-1.3306
稀释每股收益（元／股）	-1.0738	-0.7613	不适用	-1.3306

研发投入占营业收入的比例（%）	37.36	39.71	减少2.35个百分点	41.58

3.2 报告期分季度的主要会计数据

单位：元　币种：人民币

	第一季度（1-3 月份）	第二季度（4-6 月份）	第三季度（7-9 月份）	第四季度（10-12 月份）
营业收入	158,002,030.06	258,813,752.33	301,828,293.50	192,761,258.85
归属于上市公司股东的净利润	-74,409,215.90	-2,147,957.79	3,721,713.12	-120,707,495.93
归属于上市公司股东的扣除非经常性损益后的净利润	-74,645,724.72	-1,948,087.74	3,830,619.75	-123,797,384.15
经营活动产生的现金流量净额	-119,152,473.46	-6,827,543.94	-29,031,217.62	45,272,929.74

季度数据与已披露定期报告数据差异说明

□适用　√不适用

4、 股东情况

4.1 普通股股东总数、表决权恢复的优先股股东总数和持有特别表决权股份的股东总数及前 10 名股东情况

单位: 股

截至报告期末普通股股东总数(户)	7,653
年度报告披露日前上一月末的普通股股东总数(户)	8,388
截至报告期末表决权恢复的优先股股东总数（户）	0
年度报告披露日前上一月末表决权恢复的优先股股东总数（户）	0
截至报告期末持有特别表决权股份的股东总数（户）	0
年度报告披露日前上一月末持有特别表决权股份的股东总数（户）	0

前十名股东持股情况（不含通过转融通出借股份）

股东名称（全称）	报告期内增减	期末持股数量	比例(%)	持有有限售条件股份数量	质押、标记或冻结情况		股东性质
					股份状态	数量	
神州云科（北京）科技有限公司		23,357,932	12.96	0	无	0	境内非国有法人
三六零数字安全科技集团有限公司		12,604,505	6.99	0	无	0	境内非国有法人
田涛		11,603,662	6.44	0	无	0	境外自然人
宜兴光控投资有限公司		10,964,397	6.08	0	无	0	境内非国有法人

国创开元股权投资基金（有限合伙）	-1,345,173	9,011,636	4.99991	0	无	0	境内非国有法人
越超高科技有限公司		8,985,850	4.99	0	无	0	境外法人
北京奇虎科技有限公司		5,406,698	3.00	0	无	0	境内非国有法人
卞伟		4,414,568	2.45	0	无	0	境内自然人
LUO DONGPING		4,329,835	2.40	0	无	0	境外自然人
苏州工业园区元禾重元并购股权投资基金合伙企业（有限合伙）	-5,194,917	3,576,692	1.98	0	无	0	境内非国有法人
上述股东关联关系或一致行动的说明			1、苏州元禾控股股份有限公司为苏州工业园区元禾重元并购股权投资基金合伙企业（有限合伙）的有限合伙人（出资比例为 33%），同时苏州元禾控股股份有限公司亦为国创开元股权投资基金（有限合伙）的有限合伙人（出资比例为 10%）。2、三六零数字安全科技集团有限公司和北京奇虎科技有限公司均为三六零安全科技股份有限公司全资子公司，属于受同一主体控制，根据《上市公司收购管理办法》第八十三条的规定，三六零数字安全科技集团有限公司和北京奇虎科技有限公司之间构成一致行动关系。除上述说明外，公司未接到上述股东有存在关联关系或一致行动协议的说明。				
表决权恢复的优先股股东及持股数量的说明			不适用				

注：截至 2025 年 12 月 31 日，公司股东卞伟通过普通证券账户持有公司股份 38,614 股，通过证券公司客户信用交易担保证券账户持有公司股份 4,375,954 股，合计持有公司股份 4,414,568 股。

存托凭证持有人情况

□适用 √不适用

截至报告期末表决权数量前十名股东情况表

□适用 √不适用

4.2 公司与控股股东之间的产权及控制关系的方框图

□适用 √不适用

4.3 公司与实际控制人之间的产权及控制关系的方框图

□适用 √不适用

4.4 报告期末公司优先股股东总数及前 10 名股东情况

□适用 √不适用

5、 公司债券情况

□适用 √不适用

第三节 重要事项

1、 公司应当根据重要性原则，披露报告期内公司经营情况的重大变化，以及报告期内发生的对公司经营情况有重大影响和预计未来会有重大影响的事项。

2025 年度，公司实现营业收入 91,140.53 万元，同比下降 8.55%；实现归属于母公司所有者的净利润-19,354.30 万元，同比亏损扩大 41.06 %；实现归属于母公司所有者的扣除非经常性损益的净利润-19,656.06 万元，同比亏损扩大 30.17%。

2、 公司年度报告披露后存在退市风险警示或终止上市情形的，应当披露导致退市风险警示或终止上市情形的原因。

□适用 √不适用