公司代码：688651　　公司简称：盛邦安全　　公告号：2024-012

# 远江盛邦安全科技集团股份有限公司

# 2024 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 http://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阐述公司在经营过程中可能面临的各种风险和应对措施，本年度关于业绩大幅下滑的主要原因请查阅本报告第三节“管理层讨论与分析”第四项“风险因素”中“（二）业绩大幅下滑或亏损的风险。

**3、 本公司董事会、监事会及董事、监事、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、 信永中和会计师事务所（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**

公司 2024年度利润分配方案为不派发现金红利，不进行资本公积金转增股本，不送红股。

**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 | 盛邦安全 | 688651 | / |

### 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 | 袁先登 | 杨烨琨 |
| 联系地址 | 北京市海淀区上地九街9号9号2层209号 | 北京市海淀区上地九街9号9号2层209号 |
| 电话 | 010-62966096 | 010-62966096 |
| 传真 | 010-82730576 | 010-82730576 |
| 电子信箱 | ir_public@webray.com.cn | ir_public@webray.com.cn |

## 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

报告期内，公司主营业务分为以下产品和服务体系：

1、网络安全产品及服务

网络安全整体围绕 TCP/IP 协议进行设计，根据 TCP/IP 协议，计算机网络体系结构分为四层，分别为链路层、网络层、传输层、应用层，网络安全行业的产品及服务也能够根据上述四层协议进行划分。随着近年网络安全行业朝着攻防实战化方向演变，应用层承受了绝大多数的网络攻击，针对应用层的攻击威胁复杂程度也远超其他类型，应用安全的重要性日益显著。

随着入侵检测、病毒防御、漏洞扫描、Web 防护等安全技术的不断成熟，应用安全产业逐渐形成了安全检测（查）、安全防御（防）和安全管理（管）三大基础能力，公司针对“查”、“防”、“管”三大基础核心能力，开发了包括安全检测、应用安全防御、安全管理与溯源分析、安全审计为核心的网络安全产品。同时为满足不同行业的业务场景化需求，公司形成了面向电力能源的电力安全分析室和网络挂图作战指挥系统，面向金融科技的风险管控平台（RayCOM）和金融机构业务连续性管理系统，面向教育行业的智慧校园安全治理解决方案，面向运营商行业的物联网安全监测解决方案，面向公共领域的网络威胁情报攻击阻断系统（RayTI）、多源威胁情报融合分析系统（RayTBD）、网络安全单兵自动化检测系统（RayBox）、多接入网关系统（RaySDT）等多样化的安全产品及解决方案。

公司实现了核心产品的云化部署，基于网络空间地图数据、脆弱性检测与管理系统漏洞库、Web 攻击防御库、工控漏洞检测规则库和威胁情报库等数据，形成了 SaaS 化的监控预警、网络空间资产测绘分析、应用安全防御等能力。用户通过多租户的订阅模式，可以根据个性化需求按需选配、灵活调度，对其网络资产或服务进行 7*24 小时的持续风险监测、防御及管理。网络安全服务包含远程安全监测预警服务、暴露面/攻击面监测服务等 SaaS 服务，以及安全咨询服务、基于红蓝对抗的安全保障服务、网络安全评估服务等网络安全专家服务。

2. 网络空间地图：

公司网络空间地图类产品包含网络空间地图映射分析系统（RayMap），网络空间资产测绘系统（RaySpace）、网络空间资产治理系统（RayGate）、网络攻击面管理系统（RayASM）、网络空间开源信息监测预警系统（RaySIN）、反测绘检测与防御系统（RaySDS）、互联网空间资产探测平台(DayDayMap)等。

互联网空间资产探测平台(DayDayMap)是一款集产学研用于一体、聚焦空间测绘科研领域的全球网络空间资产测绘平台，让网络空间资产可感知、易定位、更有价值。DayDayMap 致力打造最具科研属性的网络空间资产测绘平台，通过无状态防溯源探测、高性能端口扫描等技术、大规模分布式扫描引擎资源，覆盖 60 亿+IPv6 数据，在业界处于领先地位。同时能够进行多维度数据关联融合分析，精确识别资产归属与行业等信息，智能关联分析资产的归属单位，发现未知或未监控资产、服务和数据。

3、卫星互联网安全业务

近年来进入卫星互联网的快速发展期，公司针对卫星互联网安全的不同场景，推出如卫星互联网仿真平台、卫星互联网测绘系统、卫星安全漏洞检测系统、卫星 SAT-WAN 安全组网系统、卫星 SD-VLAN 智能微网系统、卫星通讯加密系统等多款卫星互联网安全产品，并形成了如低空无人飞行安全防护等针对不同场景的卫星互联网安全解决方案。

公司具体产品体系如下图所示：

## 2.2 主要经营模式

公司拥有完备的网络安全产品和创新的网络安全服务，拥有完善的盈利、研发、采购、生产和销售模式。

1. 盈利模式

公司的盈利主要来源于自主研发的网络安全软硬件产品的销售以及为客户提供网络安全服务。公司研发并销售的网络安全产品包括网络安全产品与服务、网络空间地图类产品、卫星互联网安全类产品等。

2. 研发模式

公司研发以创新驱动、市场需求为导向，遵守“客户第一”的原则，坚持“两精一深”的研发理念，坚持自主研发、快速迭代的总体思路，实现产品的加速落地和市场转化。公司采取“基

座+能力模型+业务模型”的类积木形式研发模型。“基座”为公司自主研发的统一操作系统平台 RayOS，通过建立适配国产化、云化及虚拟化的通用基础操作系统，可运用于不同的应用场景。基于 RayOS 平台，公司将网络安全共性能力模块化/组件化，针对不同市场需求以“搭积木”的方式快速形成差异化产品，提高研发成果复用性，缩短研发工时，提高研发效率。“能力模型”是以漏洞为核心的六大检测能力，及以模块化引擎和一体化策略为核心的高速数据包转发处理能力。“业务模型”是针对不同行业、不同客户的业务需求，建立不同场景化的模型。采用该研发模型能够应对市场需求变化，对现有技术进行快速迭代并迅速形成标准产品，为公司业务“深入行业”提供技术保障。

3. 采购模式

公司对外采购包括以下三大类：（1）网络安全产品使用的工控机、服务器、数据授权及相关配件；（2）网络安全解决方案相关的第三方软硬件；（3）技术服务。按照行业定制化产品和通用化标准产品的不同，公司分别实行订单驱动式采购和季度预测式采购。公司建立了《采购管理制度》规范采购行为，由供应链管理部负责公司采购的执行，按供应商分类建立供应商台账。为满足公司网络安全产品和服务的质量要求，公司由采购部门牵头，根据供应商的供货能力、质量、价格、付款方式、售后服务及供应商的信誉度等对候选供应商进行综合评定，按照对比择优的原则，选择最佳合作供应商。

4. 生产模式

公司网络安全产品主要形态是软件或软硬件一体化产品。硬件为服务器、工控机、计算机、网络设备等，通过对外采购方式获得。公司采用季度预测式和订单驱动式生产模式，直接向客户交付软件产品或将自主研发的软件灌装入硬件设备中，经拷机测试、产品质量检验、入库等环节完成生产交付。

5. 服务模式

安全服务包括 SaaS 服务及专家服务两大类，公司根据客户的实际需求，为客户提供云监测、技术咨询及安全保障等服务。公司与客户洽谈、沟通达成合作意向后，成立安全服务项目小组开展前期调研、制定服务方案及组织服务实施等工作。

6. 销售模式

公司产品及服务的销售采用直接销售与渠道销售相结合的模式，其中以直销模式为主。直销模式主要包括终端用户销售、技术能力输出、嵌入式集成销售等几种方式，渠道合作模式主要有签约渠道和项目合作渠道两种形式。

## 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

2024 年，在随着人工智能、5G、卫星互联网、量子计算等新一代信息技术的推动下，全球范围内的数字化转型呈现跃进式发展，世界开启万物互联的新时代。在数字化转型加速的背景下，网络安全已成为企业与组织发展的关键要素。2024 年 7 月，公安部、国家互联网信息办公室联合发布《国家网络身份认证公共服务管理办法（征求意见稿）》，切实推动网络可信身份战略的落地实施，稳步推进国家网络身份认证公共服务建设；同月，公安部等三部门发布《低空无人机安全管理规定》建立无人机实名登记、空域管控、数据安全传输等制度，防范无人机黑飞和数据泄露

风险；2024 年 9 月，国务院发布《网络数据安全管理条例》，推动政企建立数据安全治理体系，相关市场规模大幅增长。政策的出台进一步推动了新质生产力的规范发展，数据作为关键生产要素进入生产过程，网络安全则成为保障数据价值实现的重要前提。无处不在的数字组织及其创建的海量数据的安全需求为网络安全行业带来更多技术挑战及发展机遇，实战化和场景化逐渐成为核心要求，对网络空间地图构建与卫星通信安全保护的迫切需求，更成为行业发展的新方向。

目前网络安全行业的基本特点有：

（1）国际形势复杂严峻，公共领域安全需求强烈。

近年国际形势发生了复杂深刻的变化，伴随着物理世界国家间对抗的增加，网络世界的数字争端也在不断加剧。面对着常态化的网络空间对抗，各国政府对网络战的认识不断加深，网信办、公安等国家公共领域的网络安全的重要性被提升到了新的高度。俄乌战争为我们带来了三点重要启示：①网络攻击成为现代战争的一部分，呈现规模化、组织化的特征，持续时间长；②战争中关键信息基础设施是被攻击的重点对象；③关键信息基础设施安全防御体系的建设将促使网络安全行业的重大升级。常态化对抗的国际形势充分凸显出网信办、公安等公共安全领域的重要性。未来，围绕公共安全领域开展检测、防御、态势预警等网络安全体系化建设必将成为我国网络安全市场发展趋势。2023 年《信息安全技术关键信息基础设施安全保护要求》开始正式实施，这是《关键信息基础设施安全保护条例》发布后，首个正式发布的关键信息基础设施安全保护标准。该标准提供了更好的、更具体的操作指引，以帮助关键信息基础设施管理者更好地开展安全保护工作，进而推动和指导关键信息基础设施的关基保护落地。

（2）“新基建”加速数字化转型，网络空间地图重要性凸显。5G、人工智能、互联网等领域的“新基建”充分带动了数据的流动和集中。随着社会数字化转型的进程加快，数据跨界流转的速度越来越快，数据总量以指数级增长。海量数据为数字资产的管理带来巨大挑战，国家、监管部门、乃至各行各业都因数字化转型迸发出大量资产测绘、分类和管理等需求，网络空间地图能够通过资产测绘、网络映射、资产管理等功能，维护网络世界中数字资产的秩序，为“新基建”建设提供数字底座。伴随着数字化转型深入各行业，物联网终端、5G 新技术终端、云平台、SD-WAN 等新业态衍生出了安全行业的新形势、新需求，驱动安全界限不断向网络物理融合空间延伸。例如网络空间的 5G 远程手术、车联网、卫星导航等遭到攻击，会直接影响到物理世界的生命安全及社会安全。在此背景下，通过网络空间地图将物理世界的资产在虚拟空间中完成映射，并对数字资产进行全生命周期的主动化、智能化的实时安全防御至关重要。据 IDC《中国网络空间地图市场洞察，2023 生成式 AI 加持》报告预测，到 2027 年，中国 40%的企业将使用量化模型为网络风险进行金额量化。为了响应这一需求，企业将寻找网络风险量化供应商，以计算其遭受攻击的概率和金额损失。网络空间地图相关技术可以很好地支撑上述需求，并成为构建数字世界的必备基础技术能力。

（3）实战化攻防演练促进技术创新发展，智能化、主动化产品成为新趋势。实战化网络攻防演练行动成为推动安全技术和产品在新场景发展的重要动力，智能化、主动化能力成为产品技术竞争力关键所在。通过攻防演练，能够发现传统网络安全技术存在攻防能力不对等及不能及时适应新场景安全需求的问题。攻防能力不对等是指网络安全攻击方能够通过智能学习模仿、实施高级可持续威胁攻击等方式进行攻击，增加攻击发现和溯源难度，导致防御方基于已有规则特征的被动静态应对失效，难以发现攻击背后的联动风险，难以应对未知威胁和蛰伏攻击，防御产品亟

需迎来技术升级。此外，5G、物联网、工业互联网等新场景衍生出了特殊的安全需求，为在广域覆盖、资源受限场景下的威胁应对提出了更高的技术要求。在此背景下，智能化、主动化安全技术成为了行业发展的新趋势，该技术不仅可实现安全威胁的快速感知、主动捕获、关联预测、动态对抗，还支持轻量化、场景定制化、全局安全联动部署。随着攻防态势演变和新场景安全需求迸发，智能主动安全类产品将迎来规模化应用，在网络攻防对抗与核心资产业务防护中凸显重要价值。

（4）工业互联网市场增速明显，推动网络安全需求的快速升级。工业互联网是新一代信息通信技术与工业经济深度融合的新型基础设施、应用模式和工业生态，为工业乃至产业数字化、网络化、智能化发展提供了实现途径，是工业 4.0 的重要基石。2018 年以来，针对制造、通信、能源等关键信息基础领域的攻击事件频频发生，受到攻击的行业领域不断扩大，造成后果也愈加严重，工业互联网安全的市场关注度随之提升。近年来，随着我国智能制造和工业互联网推进政策的不断出台，政府及企业开始逐步重视对工业互联网安全的投入，工业互联网市场呈现快速增长的趋势。根据工信部发布的《“十四五”信息化和工业化深度融合发展规划》要求，“到 2025 年，我国工业互联网平台普及率达 45%，系统解决方案服务能力明显增强，形成平台企业赋能、大中小企业融通发展新格局”。目前，我国工业互联网产业规模已达到万亿级别，工业互联网庞大的市场规模及高速的发展态势也将进一步推动对工业互联网安全保障需求的快速升级。

**(2)．公司所处的行业地位分析及其变化情况**

公司作为全国领先的网络安全产品提供商，十几年来坚持核心技术研发投入，不断提升公司的自主创新能力和研发水平，公司核心产品和技术始终处于行业领先地位。

公司是国家级专精特新“小巨人”企业，被中国网络安全产业联盟（CCIA）评为“网络资产测绘技术领域典型企业”，连续 5 年入选“中国网安产业竞争力 50 强”，排名逐年上升。公司荣获 2023 年度北京市科学技术进步奖，同时入选“2024 信创 500 强”。公司是 CNCERT 网络安全应急服务支撑单位（甲级）（全国共 13 家），国家网络与信息安全信息通报机制技术支持单位、获 CNVD 满星评价，荣获“年原创漏洞发现贡献单位”、“年度漏洞治理合作最具贡献单位”；荣获 CCTGA 协同防御试点优秀成员单位三项大奖；连续三年入选工信部 CAPPVD 漏洞库技术支撑单位；入选工信部 2024 年网络安全技术应用典型案例、CITVID 信创政务产品安全漏洞专业库技术支撑单位、工业和信息化部移动互联网 APP 产品安全漏洞库（CAPPVD）技术支撑单位。公司的产品入选信通院《数字安全护航技术能力全景图》8 大类 23 个细分领域；入选 2024 中国金融行业网络安全研究报告并上榜多个领域。公司的烽火台实验室入选世界互联网大会首批智库合作计划；创新方案入选工信部《网络安全保险典型服务方案目录》；卫星互联网安全解决方案斩获雄安大赛唯一卫星应用获奖项目；100G 超高速低时延链路密码机荣获“网络安全优秀创新成果大赛”优胜奖；API 安全治理方案荣获 “金帽子”年度优秀行业解决方案奖；电力行业方案荣获 2024 年度电力行业数据安全保护解决方案优秀奖。

公司主要产品近年市场份额持续位居行业前列，市场份额及行业认可如下表所示：

| 产品类别 | 产品名称 | 市场份额与排名 | 数据来源 |
| --- | --- | --- | --- |
| 安全检测类 | 漏洞扫描评估系统 | 最新发布报告显示，2023 年市场占比 8.1%，排名第 3。 | IDC |

| | | | |
|---|---|---|---|
| 安全防御类 | Web 应用防护系统（硬件 WAF） | 最新发布报告显示，2023 年度市场占比 5.9%，排名第 5；2022 年度市场占比 5.7%，排名第 5。 | IDC |
| 网络空间地图 | 资产管理与网络空间地图体系 | 2021 年、2022 年、2023 年连续入选 IDC《中国网络空间地图市场洞察》研究报告主要技术提供商。 | IDC |

作为国内网络安全行业，尤其是网络空间地图领域的领军企业，在进行研发创新和市场开拓的同时，公司积极承担国家信息安全产业发展的社会责任，受邀参与了包括网络脆弱性扫描产品安全技术要求和测试评价方法、网络安全威胁信息格式规范、网络安全态势感知通用技术要求、网络安全审计产品技术规范、政务网站系统安全指南、信息安全服务分类与代码、网络安全信息报送指南、信息安全控制评估指南等多项国家与行业标准的制定。公司共参与 14 项国家/团体标准制定，已发布 12 项。

**(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**

随着国内和国际局势日益严峻，网络安全事件频发，诸如数据泄漏、勒索软件、黑客攻击等层出不穷，网络安全风险持续增加，围绕公共安全领域开展检测、防御、态势预警等网络安全体系化建设，开展常态化攻防演练对国家信息安全至关重要。网络安全事件，特别是突发性的、造成较大范围影响的安全事件推动了各行业对网络安全的需求，促使各行业，尤其是对于社会安全稳定至关重要的网信办、公安等公共安全领域加大网络安全投入，为网络安全行业发展带来了更多机遇。

伴随 5G 基站的建设、IPv6 网络带来的流量增长，区块链、物联网、云计算、智能制造、AI、VR、AR 等新技术、新业态、新应用的涌现，各行业的数字化转型进程不断加速，对网络信息安全提出了新的要求。以云计算和物联网为例，云计算与传统计算方式不同，采用分布式计算的方式，使用虚拟化技术突破了时间、空间的界限，使 IT 基础架构发生了根本性的变化。这也使得云计算相较于传统计算方式面临更多的网络风险，例如云端数据泄漏、针对虚拟化技术 hypervisor 组件的安全漏洞等。而物联网的快速发展，使得入网设备数量快速增长，且这些入网设备通常不具备安全防护能力，容易遭受外部攻击者的攻击和利用，使物联网面临更多的安全风险。应用环境变化而不断产生的新的需求为网络信息安全行业产品和服务的升级与拓展带来了新的增长点。

当前，以 5G、大数据、物联网、人工智能等新技术为代表的新型基础设施建设是国家经济复苏的关键举措之一，网络安全作为保障“新基建”安全的重要基石，与“新基建”相互共生、相互依存。各行业信息化建设的加速让网络安全产业得到更多蓬勃发展的新机遇。

## 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

| | 2024年 | 2023年 | 本年比上年增减(%) | 2022年 |
|---|---|---|---|---|
| 总资产 | 1,181,922,645.66 | 1,140,755,800.32 | 3.61 | 368,913,205.09 |

| | | | | |
|---|---|---|---|---|
| 归属于上市公司股东的净资产 | 981,662,633.09 | 1,002,906,634.26 | -2.12 | 268,920,798.59 |
| 营业收入 | 293,533,599.00 | 290,833,046.16 | 0.93 | 236,124,720.93 |
| 归属于上市公司股东的净利润 | 1,628,506.74 | 42,508,631.53 | -96.17 | 46,186,018.53 |
| 归属于上市公司股东的扣除非经常性损益的净利润 | -7,206,850.81 | 34,559,245.89 | -120.85 | 42,474,519.07 |
| 经营活动产生的现金流量净额 | -63,386,705.83 | -10,682,187.62 | -493.39 | 13,249,620.80 |
| 加权平均净资产收益率（%） | 0.16 | 7.43 | 减少7.27个百分点 | 18.71 |
| 基本每股收益（元／股） | 0.02 | 0.66 | -96.97 | 0.82 |
| 稀释每股收益（元／股） | 0.02 | 0.66 | -96.97 | 0.82 |
| 研发投入占营业收入的比例（%） | 25.21 | 19.15 | 增加6.06个百分点 | 20.20 |

## 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 | 42,211,542.03 | 52,867,677.75 | 48,119,966.22 | 150,334,413.00 |
| 归属于上市公司股东的净利润 | -10,088,621.92 | -8,601,025.84 | -16,162,856.46 | 36,481,010.96 |
| 归属于上市公司股东的扣除非经常性损益后的净利润 | -14,346,289.69 | -10,222,632.08 | -18,887,702.82 | 36,249,773.78 |
| 经营活动产生的现金流量净额 | -20,322,651.28 | -18,856,126.77 | -19,425,702.62 | -4,782,225.16 |

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) | 3,382 |
| 年度报告披露日前上一月末的普通股股东总数(户) | 3,553 |
| 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 | |
| 权晓文 | 0 | 18,424,712 | 24.44 | 18,424,712 | 无 | / | 境内自然人 |
| 北京远江星图网络科技有限公司 | 0 | 6,110,000 | 8.1 | 6,110,000 | 无 | / | 境内非国有法人 |
| 刘晓薇 | 0 | 6,076,510 | 8.06 | 6,076,510 | 无 | / | 境内自然人 |
| 韩卫东 | 0 | 3,531,335 | 4.68 | 3,531,335 | 无 | / | 境内自然人 |
| 北京远江高科股权投资合伙企业（有限合伙） | 0 | 2,390,439 | 3.17 | 2,390,439 | 无 | / | 境内非国有法人 |
| 新余盛邦网云科技服务合伙企业（有限合伙） | 0 | 1,790,000 | 2.37 | 1,790,000 | 无 | / | 境内非国有法人 |
| 王润合 | 0 | 1,408,886 | 1.87 | 1,408,886 | 无 | / | 境内自然人 |
| 陈四强 | 0 | 1,312,692 | 1.74 | 1,312,692 | 无 | / | 境内自然人 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 魏春梅 | -51,529 | 1,202,000 | 1.59 | 0 | 无 | / | 境内自然人 |
| 周华金 | -258,106 | 1,157,062 | 1.53 | 0 | 无 | / | 境内自然人 |
| 上述股东关联关系或一致行动的说明 | | | 权晓文与刘晓薇、王润合为一致行动人关系；远江星图、远江高科、新余网云同为控股股东、实际控制人权晓文控制的企业。 | | | | |
| 表决权恢复的优先股股东及持股数量的说明 | | | 公司不存在优先股情况 | | | | |

**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**

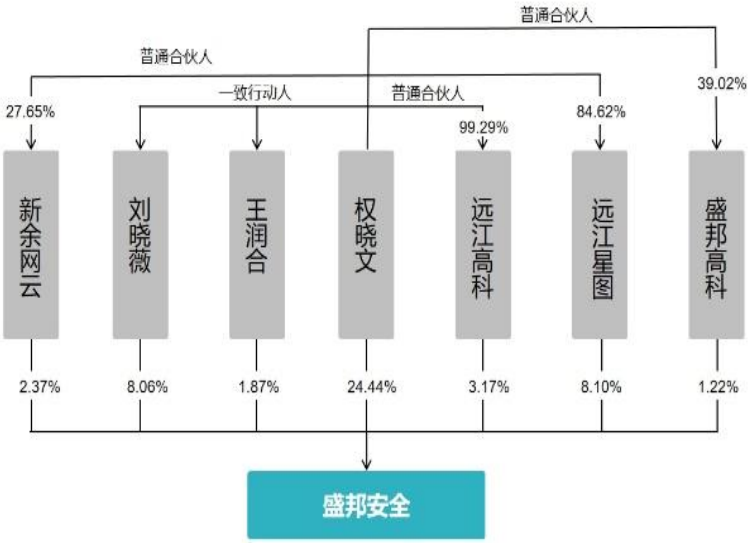
√适用 □不适用

单位:股

| 序号 | 股东名称 | 持股数量 | | 表决权数量 | 表决权比例 | 报告期内表决权增减 | 表决权受到限制的情况 |
|---|---|---|---|---|---|---|---|
| | | 普通股 | 特别表决权股份 | | | | |
| 1 | 权晓文 | 18,424,712 | 0 | 18,424,712 | 24.48 | 0 | / |
| 2 | 北京远江星图网络科技有限公司 | 6,110,000 | 0 | 6,110,000 | 8.12 | 0 | / |
| 3 | 刘晓薇 | 6,076,510 | 0 | 6,076,510 | 8.07 | 0 | / |
| 4 | 韩卫东 | 3,531,335 | 0 | 3,531,335 | 4.69 | 0 | / |
| 5 | 北京远江高科股权投资合伙企业（有限合伙） | 2,390,439 | 0 | 2,390,439 | 3.18 | 0 | / |
| 6 | 新余盛邦网云科技服务合伙企业（有限合伙） | 1,790,000 | 0 | 1,790,000 | 2.38 | 0 | / |
| 7 | 王润合 | 1,408,886 | 0 | 1,408,886 | 1.87 | 0 | / |
| 8 | 陈四强 | 1,312,692 | 0 | 1,312,692 | 1.74 | 0 | / |
| 9 | 魏春梅 | 1,202,000 | 0 | 1,202,000 | 1.60 | 0 | / |
| 10 | 周华金 | 1,157,062 | 0 | 1,157,062 | 1.54 | 0 | / |
| 合计 | / | 43,403,636 | 0 | 43,403,636 | / | / | / |

**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。

报告期内，公司实现营业总收入 29,353.36 万元，比上年同期增长 0.93%；实现归属于上市公司股东的净利润 162.85 万元，归属于上市公司股东的扣除非经常性损益后的净利润-720.69 万元。

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