公司代码：688023　　公司简称：安恒信息

杭州安恒信息技术股份有限公司

2022 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

报告期内，公司实现营业收入 198,001.24 万元，同比增长 8.77%，净利润为-25,344.57 万元，主要系报告期内:（1）受国内宏观经济增速放缓的不利影响，公司营业收入规模实现稳健增长但增速有所放缓，且为进一步提升公司产品竞争力，公司在数据安全、MSS、信创等领域持续保持创新研发及市场拓展投入；（2）公司人员基数较大，公司刚性人工成本仍呈增长趋势；（3）为吸引人才，公司实施多期股权激励计划，股份支付费用在激励计划实施过程中按照归属比例进行分期确认，报告期内公司的股份支付费用为 85,809,470.52 元。

报告期内，公司努力克服宏观经济增速明显放缓等外部影响，实现营业收入 198,001.24 万元，同比增长 8.77%，公司在数据安全、MSS、信创安全、密码安全等战略新方向的相关订单仍保持高速增长，同时公司的云安全、态势感知、安全服务等继续保持较好增速，因此公司整体营业收入规模仍保持增长态势。公司未来能否保持持续成长，受宏观经济、产业政策、行业竞争态势等宏观环境因素的影响，也取决于公司技术研发，产品市场推广及下游市场需求等因素。如果未来公司现有主要产品市场需求出现持续下滑、市场竞争加剧、技术研发失败或规模效应未按预期逐步显现，且公司未能及时拓展新的应用市场，公司营业收入、净利润将面临下降的风险。未来，公司将持续提升产品竞争力及管理能力等以应对上述可能出现的不利因素。

由于近年来国际、国内重大网络安全事故的频发，我国政府对网络信息安全的重视程度不断提高。随着网络安全政策法规持续的完善优化，网络安全市场规范性逐步提升，政企客户在网络安全产品和服务上的投入逐步增长。同时，随着云计算、大数据、物联网、5G 等技术的不断成熟和普遍应用，最终用户对网络安全产品和服务的需求也将持续提升，网络安全市场仍将保持快速发展态势。报告期内，公司主营业务、核心竞争力均未发生重大不利变化，与网络安全行业整体趋势一致。

公司在本报告第三节“管理层讨论与分析”之“四、风险因素”中详细阐述了公司在经营过程中可能面临的其他各种风险，敬请投资者关注相关内容。

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 立信会计师事务所（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

报告期内，公司实施了回购股份，合计回购公司股份333,232股，总成交金额为50,094,763.98元（不含交易费用）。根据中国证监会、上海证券交易所的相关规定，股份回购金额视同现金分红，纳入年度现金分红的相关比例计算。按此计算，2020年度至2022年度连续三年累计现金分红金额（含2022年度现金回购股份金额）符合《上市公司监管指引第3号——上市公司现金分》以及《公司章程》关于利润分配政策的有关规定。

公司2022年度归属于上市公司股东的净利润为负，2022年度拟不进行利润分配，不送红股，也不进行资本公积金转增股本，本议案已经公司第二届董事会第二十九次会议审议，尚需提交公司2022年度股东大会审议。

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

一、公司简介

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	安恒信息	688023	/

公司存托凭证简况

□适用 √不适用

联系人和联系方式

联系人和联系方式	董事会秘书（信息披露境内代表）	证券事务代表
姓名	楼晶	江姝婧
办公地址	浙江省杭州市滨江区西兴街道联慧街188号	浙江省杭州市滨江区西兴街道联慧街188号
电话	0571-28898076	0571-28898076
电子信箱	ahxx@dbappsecurity.com.cn	ahxx@dbappsecurity.com.cn

二、报告期公司主要业务简介

(一) 主要业务、主要产品或服务情况

公司自设立以来一直专注于网络信息安全领域，主营业务为网络信息安全产品的研发、生产及销售，并为客户提供专业的网络信息安全服务。公司的产品及服务涉及应用安全、云安全、大数据安全、物联网安全、智慧城市安全和工业互联网安全等领域。凭借强大的研发实力和持续的产品创新，公司围绕事前、事中、事后几个维度已形成覆盖网络信息安全生命全周期的产品体系，包括网络信息安全基础产品、网络信息安全平台以及网络信息安全服务，各产品线在行业中均形

成了较强的竞争力。

公司主要产品及服务情况如下：

分类	二级分类	主要产品	产品简介
网络信息安全基础产品	网络信息安全防护产品	Web 应用防火墙	明御®Web 应用防火墙（简称“WAF”）是一款专注为网站、APP 等 Web 应用提供安全防护的专业应用安全防护产品。能够对网站及 APP 业务流量进行多维度、深层次的安全检测和防护。系统内置五大安全引擎（包括语义分析引擎、机器学习引擎、威胁情报引擎、行为分析引擎、基础特征引擎），可通过主动防护与被动安全相结合的方式识别可疑、已知、未知安全威胁，有效保障网站及 APP 业务安全、可靠运行。
		综合日志审计系统	收集各类网络设备、安全设备、主机及业务系统的相关日志，通过对日志深度、精细化的解析，结合跨事件/设备的关联分析，识别网络环境和业务系统中存在的安全风险，同时日志审计系统可提供网络故障排查、基于日志的业务数据分析、内部审计等多种能力。归一化的日志和业务数据，可为第三方平台如态势感知、数据监管平台、安全管理中心、客户自建系统等提供出色的基础数据服务。
		数据库审计与风险控制系统	以全面审计和精确审计为基础，实时记录网络上的数据库活动，对数据库操作进行细粒度审计的合规性分析管理，对数据库遭受到的风险行为进行实时告警，如 SQL 注入攻击、高危操作等。同时产品支持本地、云上、混合等部署模式，并支持分布式集群管理、用户本次操作审计、TOPSQL 执行分析、日志归并分析等能力。
		运维审计与风险控制系统	明御®运维审计与风险控制系统（简称“DAS-USM”）是公司在多年运维安全管理的理论和实践经验积累的基础上，结合各类法律法规（如等级保护、赛班斯法案 SOX、PCI、企业内控管理、分级保护、ISO/IEC 27001 等）对运维审计的要求，采用 B/S 架构，集“身份认证（Authentication）、账户管理（Account）、控制权限（Authorization）、日志审计（Audit）”于一体，支持多种字符终端协议、文件传输协议、图形终端协议、远程应用协议的安全监控与历史查询，具备全方位运维风险控制能力的统一安全管理与审计产品。
		APT 攻击预警平台	明御®APT 攻击预警平台（简称“DAS-APT”）是一款集威胁检测、威胁分析、威胁态势、威胁响应和回溯取证分析于一体的网络流量检测类产品，该产品基于丰富的特征库、全面的检测策略、智能的机器学习、高效的沙箱动态分析、海量的威胁情报，能实时发现网络攻击行为，特别是新型网络攻击行为，结合产品中各类威胁分析视角和场景，帮助用户发现网络中发生的各种已知威胁和未知威胁，检测能力完整覆盖整个 APT 攻击链，能有效发现 APT 攻击、未知威胁及用户关心的网络安全事件。
		入侵检测系统	明御®入侵检测系统（简称“DAS-NTA”）以全面深入的网络流量解析为基础，通过智能语义分析、精准全面的检测规则、多角度分析模型、流量异常识别等技术，提供“可信、精准”的网络攻击和威胁事件发现、攻击源与攻击目标定位、攻击行为关联分析等能力，还原网络入侵事件，多维视角实时呈现全网安全态势，为用户网络安全保障工作提供有力支持。

分类	二级分类	主要产品	产品简介
	网络信息安全检测产品	Web 应用漏洞扫描系统	利用漏洞产生的原理和渗透测试的方法，对 Web 应用进行深度弱点探测，可帮助应用开发者和管理者了解应用系统存在的脆弱性，为改善并提高应用系统安全性提供依据，帮助用户建立安全可靠的 Web 应用服务。
		信息安全等级保护检查工具箱	等级保护主体单位、监管检查部门开展等级保护网络信息安全检查的一体化专用便携式监察装备，具有规范检查、工具调用、结果展示等功能，集成定制有专门的安全检查工具。
		明鉴漏洞扫描系统	提供 Web、数据库、基线配置核查、端口与服务识别等综合漏洞扫描功能，能够准确发现网络中各主机、设备、应用、数据库等存在的网络信息安全漏洞，完成整体系统的安全评估。
		网络安全事件应急处置工具箱	针对网络信息安全事件应急处置的一套专业装备，能够全程指导应急处置步骤，满足不同场景下对应急处置工具以及相关知识的需求，帮助实现网络信息安全事件的取证溯源并指导快速恢复。
		安恒资产脆弱性扫描与管理平台	安恒资产脆弱性扫描与管理平台是一套以资产为核心的漏洞生命周期管理平台，以攻击者视角出发对资产暴露面进行测绘，并进行持续安全巡检，结合威胁情报提前预警 0day 漏洞，利用 SOAR 自动化编排实现流程化和自动化。通过资产指纹级智能识别、资产脆弱性分析、供应链管理等技术手段自动的发现、清点、分类、排序和监控其攻击面并持续对其进行主动运营，从而减少黑客攻击成功的机会，帮助用户清洗攻击暴露面，实现攻击面管理。
		迷网系统	一种对攻击者进行欺骗的威胁检测防御系统，通过布置诱饵主机、网络服务，诱使攻击者实施攻击，对攻击行为进行捕获和分析，并通过技术和管理手段来增强实际系统的安全防护能力。
网络信息安全平台	云安全	安恒云-天池云安全管理平台	帮助行业私有云构建统一管理、弹性伸缩、协同防御、智能部署、满足等级保护安全能力需求的云安全资源池，能为用户提供一站式的云安全综合解决方案。
		安恒云-天池等保一体机	等保一体机是专门针对中小型客户等保合规需求的软硬一体机产品，通过集成等保所需的 9 类安全能力和特色的等保自测评功能，帮助用户快速、高效的完成等保建设。
	大数据态势感知	AiLPHA 大数据智能安全平台	运用大数据技术对用户全网安全数据进行采集、集中存储管理，通过人工智能技术提高已知安全威胁检测的准确度并实现未知安全威胁的智能发现。
		AiLPHA 安全编排与协同响应管理平台	AiLPHA 智能编排与协同响应平台是一款结合大数据技术和智能算法的安全运营系统，平台可通过智能灵活编排，把人、过程和技术整合起来，大幅提升安全运营工作效率，将分析人员从耗时且重复的分析工作中解放出来。支持拖拽式交互设计安全风险分析研判策略和联动响应剧本，支持多种策略编排动作，包括但不限于关联验证、告警聚合、联动、阻断。支持联动大量不同类型的安全设备，支持策略下发生成跟踪任务，任务执行过程中可加入安管人员控制环节。将人工分析经验沉淀为标准流程，不断优化响应流程，减少对人工的依赖。流程化完成事件管理，提高协作沟通效率。将响应时间从小时甚至天降低到分钟级别。

分类	二级分类	主要产品	产品简介
		网络安全态势感知预警平台	对用户重要信息系统、网络关键信息基础设施等 IT 资产，通过全要素的数据采集、数据治理、数据分析挖掘，结合威胁情报和管理需求。构建由被动到主动的实时网络威胁感知与预警响应能力，变被动防御为主动防御。该平台能够对网络安全威胁、隐患和事件进行通报预警和应急处置。帮助用户实时掌握网络安全态势，并开展预警通报、应急处置和管理工作。
		金融风险监测预警平台	集自有互联网大数据、行业监管数据和公安警务数据为一体的大数据分析平台。通过运用云计算、人工智能、情报挖掘等新一代信息技术，协助相关监管单位对金融风险进行全流程监测和预警。
		AXDR 高级威胁检测与分析平台	AXDR 是一款为高级威胁监测与攻防实战而量身打造的监测类产品。通过网+端的数据采集，实现网端数据的统一采集关联；通过原始告警-聚合告警-安全事件的三层聚合，使得告警噪音大大降低，告警更加精准；通过 22 类研判场景及攻击面展示等技术，将原始日志与原始告警通过不同维度呈现，帮助安全运维人员更好地对细分领域进行深入分析；同时，通过安全验证（BAS）将告警研判与处置紧密关联起来，即发现告警之后，可以立即通过 BAS 模块验证是否有安全设备出现策略设置缺失，实现安全闭环。
	物联网安全	物联网安全心	一款嵌入式物联网终端防护产品，对物联网终端系统进行内核防护、数据加密和实时审计；同时能与物联网安全态势感知与管控中心联动形成云+端联动的防护技术方案，实现物联网终端安全态势感知与可信管控。
		物联网安全监测平台	采用自主研发的 SUMAP 超级搜索引擎，实现物联终端设备快速识别、漏洞检测及非法接入监测，从而实现物联网终端安全状态实时监测，是物联网终端一站式安全评估平台。
		视频安全准入系统	基于内置主流视频监控指纹信息库、视频应用协议库以及网络安全防护能力，采用黑白名单双重机制，实现视频网摄像头终端接入行为识别与精准管控，实现授权终端安全接入，实时阻断非法接入、仿冒私接等行为，帮助用户构建一张终端接入全程可视、可管的视频网。
		物联网安全感知与管理平台	物联网安全感知与管理平台是基于安恒大数据分析技术和威胁建模技术的物联网安全运营系统，以“资产风险全生命周期展示和治理，未知安全威胁快速识别和处置”为产品理念；产品功能围绕“一心三能”展开，一心是以 IOT 资产为核心，能看见资产及资产风险，能溯源安全风险，找到安全告警和安全事件的源头，最后做到能处置，联动安全处置产品进行风险处置或者将风险预警/通报给对应的风险运维人员，从而实现全网资产集中管控、资产隐患实时监测、资产安全威胁实时感知。
	数据安全	AiSort 数据安全分级与风险评估系统	AiSort 基于网络嗅探技术，充分发现网络环境中存在的数据库资产，然后基于深度学习+条件随机场等 AI 识别模型算法，依据内置的法规、行业标准，对进行敏感数据识别和自动分类分级，生成数据资产目录。同时对数据库系统用户权限、弱口令、安全配置基线、安全漏洞和威胁等全方位梳理，进行风险评估。
		AiMask 数据脱敏	AiMask 采用独有的脱敏与水印溯源算法对敏感数据进行去标识化、匿

分类	二级分类	主要产品	产品简介
		系统	名化处理。支持固定值替换、置空、乱序、统计特征保留的脱敏算法和数据溯源算法。保证脱敏后的数据保留原有业务逻辑特征的同时保证数据的有效性和可用性，支持可回溯的脱敏算法，便于用户追溯泄漏源。所有敏感数据全部在内存中处理，可保证整个环节敏感数据不落地，使脱敏后的数据可以安全的应用于测试、开发、分析和第三方大数据分析等环境。
		AiGate 数据安全网关系统	AiGate 是公司在多年数据安全访问控制理论和实践经验积累的基础上，集访问控制、动态脱敏、漏洞防护、运维管控等多种功能一体的产品。有效防止未授权人员接触敏感数据，大大降低数据泄露的风险。
		AiThink 用户与实体行为分析系统	AiThink/UEBA 通过收集整合全方位多维度以及用户上下文等数据信息，全局关联，进行行为基线分析和群体异常分析，通过 AI 机器学习异常检测算法，可以更深层次的进行安全事件洞察，迅速识别异常事件。
		隐私计算（安全岛）	安全岛综合应用安全计算沙箱，联邦学习，MPC 等多种前沿技术，配合关键行为数字验签和区块链审计技术，实现共享数据的所有权和使用权分离，保障多方数据联合计算过程的可靠、可控和可溯。数据在传输、存储、加工过程中的安全性得到落地，避免了敏感数据在开放和共享过程中的泄露风险。
		AiTrust 零信任	AiTrust 秉持零信任安全理念，针对远程业务访问及数据开放共享场景下数据安全痛点，打造可信的数字身份体系，为用户的应用发布和数据开放共享提供持续化、动态化、自动化、精细化的访问控制及多项数据安全能力。
		数据安全管控平台	数据安全管控平台以数据和身份为中心，通过可视化技术展示数据资产详情、数据分类分级、敏感数据访问、数据流向、数据访问热度、数据风险及安全事件处置等内容。平台提供数据资产发现、敏感数据发现、数据账号权限发现、自动化数据分级分类、数据安全策略集中管理和下发、数据安全事件运营等能力，同时提供数据安全访问控制、风险监测实时告警、数据脱敏、全生命周期数据审计、异常行为分析及数据交换共享的合规性监控能力，从而实现数据安全管理、技术防护和安全运营的有效协同，构建深化数据安全风险模型和度量指标体系，完善数据安全态势场景覆盖面，形成专业化的数据安全管理解决方案。
	终端安全	明御终端安全及防病毒系统（EDR）	安恒 EDR 是一款集成了丰富的系统加固与防护、网络加固与防护等功能的主机安全产品，具备业界独有的入侵威胁防护模块， ATT&CK 框架覆盖率业界领先，能够精准识别未知威胁与攻击；通过自主研发的专利级文件诱饵引擎，有着业界领先的勒索专防专杀能力；通过内核级东西向流量隔离技术，实现网络隔离与防护；并具备网页防篡改与网站攻击防护等网页安全能力以及补丁修复、外设管控、文件审计、违规外联检测与阻断等主机安全能力。
		明御®云工作负载安全防护平台	CWPP 是一款集成了丰富的系统完整性监控与管理、容器防护、微隔离等功能的主机安全产品，以主机安全为核心，采用自适应安全架构，将主机监测、立体防御、威胁处理和安全响应能力融为一体，构建主

分类	二级分类	主要产品	产品简介
			机端的安全防护平台，并提供持续的安全监控、事件分析和危险处理能力，帮助用户在云原生架构体系的业务环境下，实现安全的统一策略管理，全方位保护企业数字资产的安全和业务的稳定运行。
		终端安全及管理系统（UES）	通过应用丰富的安全创新防御技术和简单易用的产品理念，研制的终端安全一体化产品，具备数据防泄露、主机监控审计、杀毒等功能模块，能对安全策略和安全事件进行集中、有效的管理，打破安全孤岛，使所有终端成为一个活的有机系统来抵御网络中的各种威胁。做到“集中监控、统一管理、全面分析快速响应”，融合多种安全策略为统一策略，最终为客户提供智能、全面、综合的防护方案。
网络信息安全服务	安全托管运营服务 MSS	安全托管运营服务 MSS	以用户资产全生命周期的安全需求为导向，参考 IPDRO 框架，将云端安全专家团队、标准化运营流程、云端智能化安全托管运营服务平台深度结合，从资产管理、攻击面管理、威胁检测与响应、威胁狩猎、应急响应等五大核心攻防对抗域持续开展安全活动，助力用户建立高性价比、7*24h*365 天、持续主动、有效闭环的安全运营体系。
	安恒云-在线订阅式 SaaS 服务	安恒云-在线订阅式 SaaS 服务	以 SaaS 化、集中化、智能化、生态化为主要特点的多云安全建设平台，实现多云统一纳管、统一门户、统一运维以及统一运营。通过对云安全环境态势分析及将云安全能力统一规划管理，满足客户安全合规需求。
	专家服务	专业安全服务	专业安全服务包括传统的安全检测服务、渗透测试服务、代码审计服务、移动 App 检测服务、风险评估服务、安全加固服务、驻场安全服务等，通过发现信息系统存在的各种安全隐患与漏洞，提出整改方案，协助客户进行安全加固，尽可能降低安全风险，抵御内外部安全攻击与入侵，保护信息资产的安全。
		可信众测服务	可信众测是公司推出的一款重点为金融、政府、运营商等高端用户量身定制的安全众测服务。可信众测选取了安恒信息认证的安全测试人员，对风险等级要求较高的网站采用众测的模式进行测试，用户可以按照测试的效果进行付费，而测试人员仍按照约定的保密要求进行服务，在不增加用户的测试风险的情况下，大幅度提高安全测试的效果，同时降低安全测试的成本。
		安全咨询服务	安全咨询服务包括信息系统等级保护咨询、云安全咨询、信息系统安全规划建设咨询、ISO27001 信息安全管理体系咨询、数据安全咨询以及安全开发生命周期咨询。随着信息安全等级保护工作进入 2.0 时代，公司通过专业和体系的安全咨询服务结合公司全产品线的优势，帮助客户开展符合等级保护 2.0 要求的信息系统安全保障体系的规划与建设。
		平台运营服务	为公司网络安全态势感知预警平台、AiLPHA 大数据智能安全平台及云平台用户提供的深度安全运营服务。通过深度数据分析，协助客户进行持续的安全威胁分析、安全检测、策略优化、实战演练和应急处理，建立积极防御体系。
		应急响应服务	应急响应服务包括 7*24 小时安全事件应急处置及应急演练两部分内容。其中公司应急演练服务包括应急预案制定、应急演练平台构建、红蓝对抗服务等全场景演练内容。应急响应服务结合公司应急响应工

分类	二级分类	主要产品	产品简介
			具箱和应急指挥平台，提供快速高效的处置能力。
		国家重大活动网络安保服务	国家重大活动网络安保服务是公司最具品牌影响力和知名度的综合安全服务，在国家重大活动期间为活动主办方、监管机构、政企单位提供整体网络安全保障计划、方案及能力，通过专业有效的安全平台、安全设备，结合全方位的安全保障服务，确保活动的顺利举办，有效降低网络攻击风险。国家重大活动网络安保服务均具有任务重、要求高、影响大的特点。公司凭借丰富的经验和一支融合专业技术精、素质高、有经验、能打持久战、能打胜仗的网络安保队伍，为每次重大活动网络安保提供坚实的护航力量。自 2008 年至今，公司共参与近百场国家重要活动/事件的网络安保，多次承担安保组长及中坚力量的职责，确保网络安保工作万无一失。
	智慧城市安全运营中心服务		以城市关键信息基础设施和重要信息系统为保障对象，聚焦全域网络安全统筹协调、预警防护、应急处置、智能防护工作能力提升，通过完善网络安全体系建设，构建安全运营服务平台、组建协同响应的服务团队，帮助客户构建一个集安全防护、态势感知、监测预警、情报共享、通报处置、应急指挥、协调联动、攻防演练、人才培养为一体的网络安全运营中心，中心可面向全市政府单位和企事业客户提供安全咨询、风险评估、监测预警、智能防护、事件处置、损失赔付等网络安全服务，降低客户的采购成本。
	网络安全人才培养服务		依托公司产品与服务经验，对产业资源、行业案例以及成熟的项目经验进行整理，并完成教育资源转化。公司开发了符合不同层次教学、应急演练和安全测试场景的攻防实验室平台、攻防演练平台和攻防靶场平台。 服务主要包括：协助在校学生、在职人员展开安全技能培训与国家认证培训；协助各企业构建网络安全人才队伍；提供在线的网络信息安全人才学习平台。负责给安恒及产业链提供优质人才供给。
商用密码产品	身份认证服务	协同签名系统	协同签名系统是我司结合门限算法和 SM2、SM3、SM4 国密算法自主研发的基于安全私钥分量托管的密码产品，在保证用户便利性的同时，为用户操作终端（PC 端、移动终端）提供安全合规的终端用户身份认证方案。
		国密身份认证系统	国密身份认证系一款基于国产密码而研制的身份认证产品，支持 USBKEY、国密验证码、扫码三种校验方式，帮助用户解决用户身份鉴别问题，满足商用密码应用安全性评估的要求。
	数据加解密服务	传输透明加密系统	传输透明加密系统是为防止 B/S 架构的 Web/H5 信息系统被非法人员登录和业务数据在网络传输中被窃取、篡改而研制的安全产品，可以提升业务系统数据传输的防护水平。
		数据库透明加密系统	基于国产密码的数据库加密系统，无需更改代码即可实现数据库加密，为用户提供安全合规、易部署的透明存储加密方案，产品通过国家密码管理局检测，具备《商用密码产品认证证书》，满足商用密码应用安全性评估要求。
		云密盾加密系统	云密盾加密系统是一款基于国密算法，为业务系统提供透明身份认证服务和数据加解密服务的产品。通过对终端用户、应用服务器的身份

分类	二级分类	主要产品	产品简介
			鉴别和密钥下发，实现数据的传输加密和存储加密。帮助各政企单位，在不改变原有办公流程和习惯的前提下，实现数据传输、存储的机密性，以及国密算法的合规性。
		服务器密码机	服务器密码机是 PKI 密钥管理系统的基础设备，为信息安全系统提供安全的应用层密码服务，包括密钥管理、消息验证、数据加解密、数字签名与验签等功能，解决数据从产生、传输、处理、存储整个过程的机密性、完整性等安全问题，为信息系统的安全提供支撑。
		云服务器密码机	云服务器密码机是一款面向电子政务、云计算等需求推出的高性能密码设备，满足云计算环境中数据加密保护、密钥管理及身份认证等安全需求。
	安全通道服务	SSL VPN 安全网关	SSL VPN 安全网关是为防止业务数据在网络传输中被窃取、篡改而研制的安全产品，具有采用国密标准的密码算法硬件、集认证以及传输加密于一体、同时支持点对网与网对网部署三大特点，为客户提供安全、可靠、易用的密码服务。
		IPSec VPN 网关	IPSec VPN 网关系统是为防止数据在传输过程中被第三方获取或修改的安全产品，IPSec VPN 网关在软件架构上主要有管理服务和应用服务组成，应用服务负责安全隧道的协商建立与维护、数据的加解密。管理服务负责整个系统的配置管理，IPSec VPN 管理后台为用户提供系统初始化及证书管理、基本策略（网络信息）配置、高级策略（安全策略）配置、授权终端管理、资源访问控制、日志管理、数据监控以及风险告警等功能。
	密钥管理服务	密钥管理服务器	密钥管理服务器是一款基于国产密码算法，提供密钥的生成、分发、存储、更新、归档、备份、恢复和销毁等全生命周期密钥管理和密码计算服务的安全密码产品，满足用户单位的业务系统对密钥管理的需求。
	密码服务平台		密码服务平台是面向多云、多机房、多租户场景，利用多类密码服务，为用户提供一站式密评综合解决方案的密码产品，根据负载动态调整基础密码设施的规模，实现密码运算资源的动态调整和灵活调度，为用户提供按需高效、弹性可扩展的密码服务，满足密评要求。
	专家服务		提供信息系统过密评的解决方案咨询服务，包括密码应用方案编制、密评问题答疑等，满足密码应用安全性评估对于密码应用方案评审的要求。 根据密评要求，协助梳理密码应用安全管理制度，建立操作流程与执行记录模版，制定应急处置办法并形成报告模版等。 提供信息系统过密评的应用开发指导服务，包括密评改造过程技术指导、标准接口对接、POC 测试等。

(二) 主要经营模式

1、 盈利模式

公司盈利主要来源于自主研发的网络信息安全产品的销售，以及为客户提供专业的网络信息安全服务。网络信息安全产品包括基础类产品（安全防护类产品、安全检测类产品）、平台类安全产品；网络信息安全服务，包括 SaaS 云安全服务、专家服务、智慧城市安全运营中心、国家重

大活动网络安保服务、网络信息安全人才培养服务。

2、 采购模式

公司采购的主要物料为相关产品、服务、解决方案所需的各类硬件设备及相关配件，采购的主要内容为以下三个方面：（1）网络信息安全产品使用的工控机、服务器及相关配件；（2）网络安全解决方案相关的第三方软硬件（3）第三方实施安装服务。

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。公司整体上建立《采购管理制度》规范采购行为，并设立采购部负责公司采购的执行，采购部根据需求部门提交的采购单，按供应商分类建立供应商台帐。

3、 生产模式

公司按照行业定制化产品和通用化标准产品的不同，分别实行订单驱动式生产和季度预测式生产。由于生产的产品形态主要为软硬件结合产品，公司采购相应软硬件原材料后进行组装调试，然后将自主研发的软件灌装入硬件设备中，最后经拷机测试、产品质量检验、入库等环节完成生产，并通过快递公司发货至下游客户。

4、 服务模式

公司基于自身在应用安全和数据安全方面深厚的技术背景和安全实践经验，具备为对网络信息安全服务存在需求的客户提供 SaaS 云安全服务、专家安全服务、国家重大活动网络安保服务、网络空间安全人才培养服务等能力。通常，公司通过项目投标或市场化销售等方式与客户签订相应的年度或单次服务合同，然后通过现场实施或远程服务的方式对客户特定网站、系统提供安全防护服务。

5、 销售模式

公司在产品销售上采用多级渠道经销和直接销售相结合的方式，并且充分依靠渠道销售等合作伙伴以最大程度实现市场覆盖。其中，渠道代理销售是指先将产品销售给渠道代理商，再由渠道代理商将产品销售给终端用户。直销模式是指直接将产品销售给终端用户。公司采取多级渠道经销和直接销售相结合的销售模式主要是因为公司产品的目标用户群多、用户的地域及行业分布广，采用该方式能够最大程度实现市场覆盖、最高效率为客户提供网络信息安全产品及服务。

(三) 所处行业情况

1. 行业的发展阶段、基本特点、主要技术门槛

网络信息安全是指网络系统（包括硬件、软件、基础设施等）中的数据受到保护，不会由于偶然的或者恶意的原因而遭受未经授权的访问、泄露、破坏、修改、审阅、检查、记录或销毁。一般而言，网络信息安全产品主要包括安全硬件、安全软件及安全服务。随着信息技术的迅速发展，特别是云计算、大数据、物联网和人工智能等新一代信息技术的飞速发展，网络信息安全风险全面泛化，种类和复杂度均显著增加。因此，网络信息安全产业范畴也得到不断延伸和拓展，产品与服务种类较传统分类不断得到充实与细化。

从产业链来看，网络信息安全行业的上游主要为工控机、服务器、存储器、芯片及操作系统、数据库等软硬件厂商。产业链上游市场竞争充分，主要参与者均为成熟的全球化厂商，产品更新快，产量充足，产品价格相对稳定，且产品性价比呈上升趋势。中游为提供安全产品、安全服务、安全集成的厂商，下游则是政府、金融、电信、能源等各行业的企业级用户。

随着近年来国际、国内重大网络安全事故的频发，我国政府对网络信息安全的重视程度不断提高。2022 年是《中华人民共和国网络安全法》正式施行的第五年，五年来，我国相继颁布《中华人民共和国密码法》《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》《关键信息基础设施安全保护条例》等法律法规，出台《网络安全审查办法》《云计算服务安全评估办法》等政策文件，建立等级保护、安全审查、密码测评、数据安全管理、个人信息保护等一批重要制

度，逐步形成了具有中国特色的网络安全政策体系，对促进网络安全产业及数字经济发展起到了重要作用。

2022 年，国家、各级政府及部分行业持续发布网络安全领域多项重要法律、政策文件，进一步提升了网络安全在信息化建设中的地位和作用,有效推动安全投入持续加大。其中，2022 年 1 月 12 日国务院发布《“十四五”数字经济发展规划》,《规划》部署了八项重点任务，在数字经济安全体系方面，提出了三个方向的要求，一是增强网络安全防护能力、二是提升数据安全保障水平、三是切实有效防范各类风险，并系统阐述了网络安全对于数字经济的独特作用及重要性；2022 年 2 月，国家互联网信息办公室等十三部门联合修订发布的《网络安全审查办法》正式施行；2022 年 3 月，工信部发布《车联网网络安全和数据安全标准体系建设指南》，提出到 2023 年底初步构建起车联网网络安全和数据安全标准体系，到 2025 年形成较为完善的车联网网络安全和数据安全标准体系；2022 年 3 月 5 日，发布《2022 年政府工作报告》，当中提到 2022 年重点工作，其中包含强化网络安全、数据安全和个人信息保护，这是自 2021 年政府工作报告以来，再次对数据安全和个人信息保护的强调，并指出建设数字信息基础设施，逐步构建全国一体化大数据中心体系，推进 5G 规模化应用，促进产业数字化转型，发展智慧城市、数字乡村；2022 年 9 月，十三届全国人大常委会第三十六次会议表决通过《中华人民共和国反电信网络诈骗法》，该法坚持以人民为中心，统筹发展和安全，立足各环节、全链条防范治理电信网络诈骗，精准发力，为反电信网络诈骗工作提供有力法律支撑，对金融、电信、互联网行业提出了建立统一监管标准的要求，互联网接入、网络代理、域名注册等服务提供者必须加强内部控制制度和安全制度，账号滥用、乱登记等乱象将得到有效解决；2022 年 11 月，国家标准 GB/T 39204-2022《信息安全技术 关键信息基础设施安全保护要求》正式发布；同月工信部会同银保监会发布了《关于促进网络安全保险规范健康发展的意见（征求意见稿）》，从建立健全网络安全保险政策标准体系、加强网络安全保险产品服务创新、强化网络安全技术赋能保险发展、促进网络安全产业需求释放、培育网络安全保险发展生态这五个方面提出了十点意见，网络安全保险为产业发展带来良机。2022 年 12 月，中共中央、国务院印发《关于构建数据基础制度更好发挥数据要素作用的意见》，从数据产权、流通交易、收益分配、安全治理四个方面提出 20 条政策举措，初步搭建了我国数据基础制度体系，激活数据要素潜能，做强做优做大数字经济，增强经济发展新动能，构筑国家竞争新优势。

近期，工信部与国家网信办联合十六部门印发《工业和信息化部等十六部门关于促进数据安全产业发展的指导意见》，提出到 2025 年，数据安全产业规模超过 1500 亿元，年复合增长率超过 30%，政策红利进一步支撑行业景气度。

在网络信息安全政策和新兴技术的驱动下，我国网络信息安全行业仍将保持较快的增长。随着网络安全政策法规持续的完善优化，网络安全市场规范性逐步提升，政企客户在网络安全产品和服务上的投入逐步增长。同时，随着云计算、大数据、物联网、5G 等技术的不断成熟和普遍应用，最终用户对网络安全产品和服务的需求也将持续提升，从而促进网络安全市场的快速发展。据 IDC 数据显示，中国网络安全 IT 支出预计在 2026 年将达到 318.6 亿美元，约占全球网安 IT 支出的 11.1%，五年 CAGR 将达到 21.2%，增速远高于全球平均水平。在 2022-2026 的五年预测期内，网络安全软件市场增速将继续领跑安全市场，五年 CAGR 将达到 25%，网络安全硬件市场五年 CAGR 将达 17%，2026 年市场规模将超百亿美元；此外，中国安全服务市场未来五年将保持稳定增长的态势，2026 年服务支出规模预计达 86.1 亿美元，五年 CAGR 约为 21.6%。

中国网络信息安全市场持续向服务化转型，与全球安全产业结构发展趋势保持一致。在网络信息安全产业发展过程中，大多数是由合规需求驱动的，而近年来的灾难性攻击表明网络风险是重大威胁，企业开始把安全视为一项重要的商业风险，并且更看重网络信息安全服务的持续性。随着虚拟化及云服务理念的渗透，我国网络安全技术趋势出现变化，正由以硬件交付安全产品，人工交付安全服务的形式，逐步向云化、SaaS 化方式交付技术和服务等形式转变。据 IDC《2023 年 V1 全球网络安全支出指南》显示，2022 年全球网络安全相关硬件、软件、服务总投资规模为

1955.1 亿美元，预计在 2026 年增至 2979.1 亿美元，五年复合增长率（CAGR）将达 11.9%。预计到 2026 年，中国网络安全支出规模将达到 288.6 亿美元，在 2022-2026 的五年预测期内，中国网络安全相关支出将以 18.8%的年复合增长率增长，增速位列全球第一。据《IDC 中国网络安全硬件市场预测，2022 上半年》《IDC 中国网络安全软件市场预测，2022 上半年》《IDC 中国安全服务市场预测，2022 上半年》报告显示，预计 2022 年，中国网络安全市场总投资规模为 123.4 亿美元，其中安全硬件市场投入达到 50.1 亿美元，占总体投入的 40.6%；安全软件市场投入达到 39.5 亿美元，占总体投入的 32%；安全服务市场投入达到 33.8 亿美元，占总体收入的 27.4%，中国网络安全市场格局中，安全硬件为最大的 IT 安全一级子市场。

2. 公司所处的行业地位分析及其变化情况

公司于 2007 年成立之初便以应用安全和数据安全作为切入点，推出市场首创性产品数据库审计与风险控制系统与 Web 应用防火墙产品，成功进入网络信息安全市场。目前，公司核心安全产品市场份额持续多年位居行业前列。此外，公司核心产品的前瞻性和影响力也获得了国内外权威机构认可。公司主要产品和服务排名及获得荣誉列举部分如下：

（1）在 IDC 发布的《中国运维安全管理硬件市场份额，2021：技术融合，场景适配》报告中，公司运维安全管理硬件产品市场份额排名第二；

（2）在 IDC 发布的《中国 Web 应用防火墙（硬件）市场份额，2021：技术融合，多形态发展》报告中，公司 Web 应用防火墙产品市场份额排名第二；

（3）在 IDC 发布的《中国 Web 应用防火墙（软件）市场份额，2021：云计算带动成熟产品的升级演变》报告中，公司 2021 年中国软件 WAF 市场份额排名第四；

（4）在 IDC 发布的《中国公有云托管安全服务市场份额，2021：责任共担，共筑云安全》报告中，公司公有云托管安全服务市场份额排名第三；

（5）在《IDC MarketScape:中国态势感知解决方案市场 2021，厂商评估》报告中，公司以突出的核心技术能力、丰富的行业实践以及领先的市场战略，继续成为中国态势感知解决方案领导者企业之一；

（6）在赛迪顾问发布的《中国工控安全市场发展白皮书（2021）》中，公司 2020 年工业安全管理平台和工控安全服务的竞争格局排名第一，工业安全态势感知系统和工控安全审计产品的竞争格局排名前二。

（7）公司密码服务平台获评首届全国商用密码应用优秀案例；

（8）公司获得“车联网专班优秀支撑单位”荣誉；

（9）公司 AiMask 数据脱敏系统获信创型号销售许可证；

（10）公司 AiSort 数据安全分级及风险管理平台获中国信息通信研究院数据安全能力评测基础级和进阶级认证；公司 AiGate 数据库安全网关通过中国信息通信研究院首批可信数安-数据安全网关评测；

（11）Frost & Sullivan 发布的《Asia Pacific (APAC) Managed and Professional Security Services Market》报告（以下简称《报告》）对中国地区安全托管服务(MSS)进行了深入研究。《报告》显示，公司凭借技术优势和专业服务，以 17.3%的市场份额位列 2021 年中国地区安全托管服务（Managed Security Services，MSS）第一名。

（12）公司凭借卓越的数据安全能力，“恒星实验室”、“HAC”两支团队分别荣获 2022 年首届数据安全大赛“数据安全大闯关”优胜奖，公司申报的《面向健康医疗数据的安全治理体系方案和应用》获 2022 年首届数据安全大赛“数据安全治理方案”银奖。

（13）在第六届世界浙商大会杭州专场活动——杭州民营经济发展论坛暨新生代企业家论坛上，公司分别获得“2022 杭州市民营企业服务业 50 强”和“2022 杭州市民营企业研发投入 50 强”荣誉。

（14）公司荣获工业和信息化部“铸网 2022”实网演练“优秀技术支撑单位”、“铸网 2022”车联网网络安全演练“优秀攻击队伍”。

（15）公司申报的“面向杭州亚运会等重大赛事的云安全服务保障平台”成功入选 2022 工业和信息化部网络安全技术应用试点示范项目。

（16）根据上海市经济和信息化委员会公布的《2022 年度上海市优质大数据服务供应商目录》，公司全资子公司上海安恒智慧城市安全技术有限公司成功入选该目录，标志着公司在金融行业的大数据服务能力得到了充分肯定与广泛认可。

（17）2022 年 7 月 22 日，科创板开市三周年，公司入选科创板创新力 30 强榜单。

公司始终坚持持续创新的发展战略，重视研发投入，同时紧跟全球信息技术发展趋势、贴近用户需求，不断更新迭代既有产品和解决方案，并孵化培育新兴产品及服务。自 2014 年开始，公司陆续推出了云安全、大数据安全、物联网安全、工业互联网安全和智慧城市安全等新兴安全领域相关产品和解决方案。凭借深厚的核心技术积累和对政企市场的深刻理解，公司在新兴领域取得了较好的发展成绩。在公有云安全领域，公司自 2015 年开始与阿里云合作，成为阿里云安全市场首批安全供应商，目前云安全产品已经上线包括阿里云、腾讯云、华为云、AWS 亚马逊、中国电信天翼云、中国联通沃云等在内的十余家国内主流公有云平台。

作为国内信息安全领域的领导者之一，在进行研发创新和市场开拓的同时，公司积极承担我国信息安全产业发展的社会责任，参与了众多国家与行业标准的制定。公司是我国“信息安全技术智慧城市安全体系框架”、“Java 语言源代码漏洞测试规范”、“信息安全技术移动智能终端应用软件安全技术要求和测试评价方法”等多项国家标准或国家标准计划的主要制定单位，并受邀参与制定“信息安全技术日志分析产品安全技术要求”、“信息安全技术数据库安全审计产品安全技术要求”、“信息安全技术网络型流量控制产品安全技术要求”等多项安全行业标准。

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

由于近年我国云计算、大数据、物联网等新技术的快速发展，在推动新兴技术市场不断增长的同时，也催生了新的安全需求和新的应用场景。新技术、新场景下，防护对象改变，企业网络边界逐渐消失，政府和企业网络信息安全防护理念发生较大变化，网络信息安全不再是被动修补模式，而是与信息系统建设同时规划。随着新的应用场景包括云计算、大数据、物联网和移动终端等的普及，企业信息化程度逐步提升，网络信息安全领域出现了三大变化：从传统 PC、服务器、网络边缘到云计算、大数据、泛终端、新边界；防护思想从“风险发现、查缺补漏”转变到“关口前移、系统规划”；核心技术升级从传统的围墙式防护到利用大数据等技术对安全威胁进行检测与响应。

三、 公司主要会计数据和财务指标

（一）近 3 年的主要会计数据和财务指标

单位：元 币种：人民币

	2022年	2021年	本年比上年增减(%)	2020年
总资产	5,014,299,977.34	4,851,766,480.11	3.35	2,463,122,943.30
归属于上市公司股东的净资产	2,907,377,433.38	3,091,465,764.24	-5.95	1,669,428,995.78
营业收入	1,980,012,417.18	1,820,328,069.14	8.77	1,322,972,681.79
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	1,971,098,060.44	1,811,553,816.19	8.81	1,315,658,894.69

归属于上市公司股东的净利润	-253,445,695.39	13,806,457.21	-1,935.70	134,115,510.40
归属于上市公司股东的扣除非经常性损益的净利润	-298,650,600.91	-79,594,601.00	不适用	120,756,955.19
经营活动产生的现金流量净额	-178,802,476.42	-61,298,568.17	不适用	279,993,869.41
加权平均净资产收益率（%）	-8.48	0.68	减少9.16个百分点	8.37
基本每股收益（元／股）	-3.23	0.18	-1,894.44	1.81
稀释每股收益（元／股）	-3.23	0.18	-1,894.44	1.81
研发投入占营业收入的比例（%）	32.62	29.42	增加3.20个百分点	23.56

（二）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	233,456,645.53	301,167,861.43	504,981,794.44	940,406,115.78
归属于上市公司股东的净利润	-190,153,052.03	-181,384,500.95	-85,399,439.96	203,491,297.55
归属于上市公司股东的扣除非经常性损益后的净利润	-195,707,485.24	-188,576,866.91	-94,018,611.63	179,652,362.87
经营活动产生的现金流量净额	-422,220,836.31	-93,186,597.55	-31,980,978.31	368,585,935.75

季度数据与已披露定期报告数据差异说明

□适用　√不适用

四、　股东情况

（一）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)	5,553
年度报告披露日前上一月末的普通股股东总数(户)	6,404
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	0

股东总数（户）								
前十名股东持股情况								
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	包含转融通借出股份的限售股份数量	质押、标记或冻结情况		股东性质
						股份状态	数量	
范渊	0	10,096,705	12.81	0	0	无	0	境内自然人
杭州阿里创业投资有限公司	0	8,008,337	10.16	0	0	无	0	境内非国有法人
交通银行股份有限公司－万家行业优选混合型证券投资基金（LOF）	-13,400	3,833,330	4.86	0	0	无	0	其他
嘉兴市安恒投资管理合伙企业（有限合伙）	-1,249,000	3,750,990	4.76	0	0	无	0	其他
全国社保基金四零六组合	1,532,672	3,408,998	4.32	0	0	无	0	其他
宁波安恒投资合伙企业（有限合伙）	-2,030,000	2,970,000	3.77	0	0	无	0	其他
UBS AG	765,150	2,119,681	2.69	0	0	无	0	境外法人
摩根资产管理（新加坡）有限公司－摩根中国 A 股市场机会基金		1,706,700	2.17	0	0	无	0	其他
中国电信集团投资有限公司	728,085	1,571,616	1.99	0	0	无	0	国有法人
高盛国际－自有资金		1,566,695	1.99	0	0	无	0	其他

上述股东关联关系或一致行动的说明	1、截止报告披露之日，公司前十名股东中，宁波安恒投资合伙企业（有限合伙）、嘉兴市安恒投资管理合伙企业（有限合伙）与实际控制人范渊先生签署了《一致行动协议》，除此之外，公司未接到上述股东有存在关联关系或一致行动协议的声明。2、公司未知无限售流通股股东之间是否存在关联关系或一致行动的说明。
表决权恢复的优先股股东及持股数量的说明	无

存托凭证持有人情况

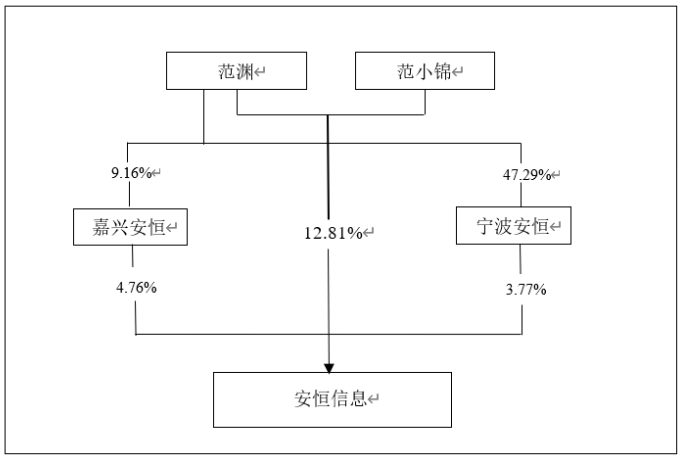
□适用 √不适用

截至报告期末表决权数量前十名股东情况表

□适用 √不适用

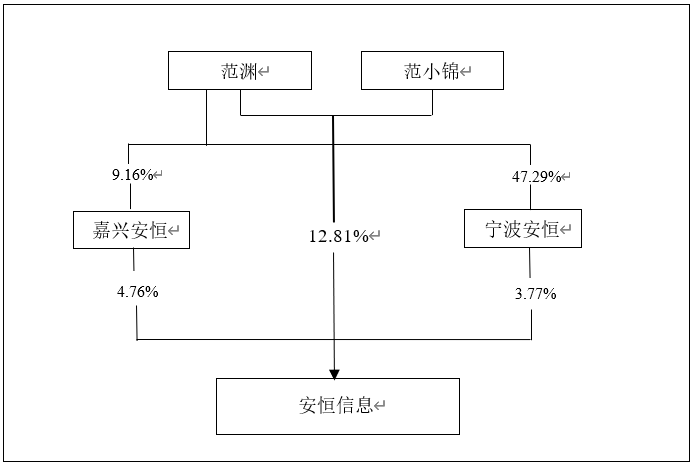
（二）公司与控股股东之间的产权及控制关系的方框图

√适用 □不适用



（三）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



（四）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

五、 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。

公司实现营业总收入 198,001.24 万元，比上年同期增长 8.77%；实现归属于上市公司股东的净利润-25,344.57 万元，比上年同期下降 1935.70%；归属于上市公司股东的扣除非经常性损益后的净利润-29,865.06 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