公司代码：688244 **公司简称：永信至诚**

永信至诚科技集团股份有限公司

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阐述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”中“风险因素”相关的内容。

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、 天健会计师事务所（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2025年度拟不进行利润分配，不以资本公积金转增股本。上述利润分配方案已经第四届董事会第九次会议审议通过，该议案尚需提交公司2025年年度股东会审议。

母公司存在未弥补亏损

□适用 √不适用

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	永信至诚	688244	/

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	张恒	丁一凡
联系地址	北京市海淀区丰豪东路9号院6号楼103	北京市海淀区丰豪东路9号院6号楼103
电话	010-50866160	010-50866160
传真	010-50866153	010-50866153
电子信箱	yxzc@integritytech.com.cn	yxzc@integritytech.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

（1）主要业务情况

永信至诚（688244.SH）是数字安全测试评估赛道领跑者，网络靶场和人才建设领军者，AI原生安全倡导者，国家级专精特新“小巨人”企业。公司自主研发的网络靶场核心技术，获北京市科技进步奖一等奖、国家科技进步奖二等奖，属网络空间安全领域的硬科技。公司首创“数字风洞”测试评估产品技术体系，为用户在数字化、智能化转型中面临的网络安全、数据安全等问题提供了切实有效的解决方案。

公司秉承“人是安全的核心”主导思想和“产品乘服务”创新理念，为政企用户提供专业的数字安全测试评估、网络靶场及运营、AI安全测评与管理、安全防护与管控等系列产品与服务。助力政企用户解决数字化进程中安全防御效能难度量、仿真环境缺失、人员实战能力不足和主动防护能力缺乏等问题。

（2）主要产品或服务情况

①数字风洞及运营

数字风洞是借鉴航空风洞的理念，围绕政企用户数字化、智能化转型过程中的数字系统及应用等数字资产，构建的全生命周期健康管理平台。该平台以系统的开发者、建设者、使用者为服务对象，以测试评估为手段，以数字资产全生命周期健康管理为主线，以风险趋于“证无”为目标，通过风洞时光机的多轮测试和迭代进行数字资产的安全能力度量，形成安全验证和整改的全流程闭环，确保数字化、智能化转型的安全性、合规性和业务稳定性。围绕AI大模型等新兴技术的应用，创新打造春秋AI大模型测评“数字风洞”，以模测模，以模强模，对目标模型在智能度、安全度、匹配度和一致度方面的能力进行动态验证和科学评估，保障大模型基因健康、系统健康、数据健康和业务健康。

公司基于“数字健康”创新理念，以“家庭医生”“网络安全秘书”身份，为政企用户提供“数字风洞”产品体系等“产品乘服务”解决方案，全面助力网络和数据安全工作实现合规的保障、风险的预控、标准的践行和投入的回报，保障“数字健康”。

②网络靶场及运营

春秋云境网络靶场平台基于永信至诚多年研发实践的平行仿真技术体系构建而成，平台融合了多种前沿技术，具有大规模、多层次、高仿真、高柔性和全场景的特点。实验和测试过程安全可控，数据采集准确详实，效能展示科学直观。经过多年持续迭代和运营，春秋云境网络靶场平台已实现竞赛演训、人才实战、攻防演练、AI实训与科研、人机对抗、人工智能攻防、5G网络仿真、智慧城市安全测试、工业场景仿真、综合应急演练及复杂业务安全推演等应用场景落地，经多位院士、专家评审，该平台具有大规模、多层次、高仿真、高柔性和全场景的特点。“基于平行仿真的大规模网络靶场构建技术及应用”项目荣获北京市科学技术奖一等奖；参与申报的“超大规模多领域融合联邦靶场（鹏城网络靶场）关键技术及系统”项目，荣获国家科学技术进步奖二等奖。

公司春秋云境网络靶场平台是网络安全竞赛和网络安全人才培养的重要支撑平台。公司网络安全竞赛运营服务包括竞赛平台开发、竞赛题目定制开发、竞赛效果呈现、赛事组织管理、竞赛裁判服务、赛事方案设计等。同时，公司构建了完整的网络安全人才培养体系，通过i春秋实训平台以及开设线下安全培训班等形式满足不同层次学员培训需求，助力学员网络安全技能的全方位提升。

③安全防护与管控

公司安全防护与管控类产品主要包括春秋云阵新一代蜜网平台、春秋云势网络安全态势感知与处置平台、蜜罐及态势感知整合安全管控、安全工具类产品、安全防护系列服务等。

2.2 主要经营模式

（1）盈利模式

公司盈利主要来源于向政府、企事业单位销售自主研发的数字风洞及运营产品、网络靶场及运营产品、安全防护与管控产品，并提供相应服务。上述产品和服务形成了公司网络安全产品服务体系生态链条，在业务上既可独立销售，又相互补充、相互促进、相互带动，在技术上同根同源、模块共用、交互迭代。

（2）研发模式

公司采取的是“标品化研发+定向二次研发”的模式，公司始终坚持自主研发的研发模式，核心产品、核心技术通过自主研发取得。公司产品的底层技术为网络空间平行仿真技术、网络攻防对抗技术、多循环数字风洞测试评估技术和基于对抗生成的多维大模型安全测试评估技术，公司自建研发体系持续进行网络空间平行仿真、网络攻防对抗、多循环数字风洞测试评估和基于对抗生成的多维大模型安全测试评估等技术的研发，形成了标准化的产品体系和功能模块，并取得了相关的发明专利、软件著作权等自主知识产权。

公司产品研发以客户为中心，以市场需求为导向，公司主要产品线均有相应的研发团队支持，确保了研发方向符合客户和市场需求。通过研发部门、销售部门、质量部门、市场部门的整体协作，形成了技术储备、产品定义、技术攻关、验收测试、推广应用、产品迭代的全生命周期的研发架构。

公司在重大的产品研发控制上采用项目管理开发模式，利用项目生命周期方法论，结合公司项目执行的实际情况，从项目的启动过程、计划过程、执行过程、控制过程以及收尾过程出发，以项目各过程组的成果输出为导向，制定了《项目管理规范》，并持续运行、迭代。公司在研发团队内部推行IPD开发模式，明确地划分为概念、计划、开发、验证、发布、生命周期管理等六个阶段，并且在流程中有定义清晰的决策评审点，立足于产品的市场定位及盈利情况，动态调整产品开发策略。研制过程中，结合公司内部的项目管理流程，从项目的启动、计划、执行、控制以及收尾等维度保障产品价值的持续输出，在保证产品成果交付质量的同时，运用各种工具和激励策略，实现整个产品研发过程的可视化和精准可控。

（3）采购模式

公司对外采购范围包括硬件、软件、服务三大类。对外采购的硬件主要用于公司软件的载体，包括服务器、计算机、网络设备等。对外采购的软件主要包含操作系统、数据库及专用软件产品等项目中非公司核心技术的软件。对外采购的服务主要用于为客户提供公司非关键岗位和环节的相关服务。

公司制定了采购相关管理制度等规范采购行为，需求部门提出采购申请后，由商务部负责采购的执行。商务部负责建立合格供应商名录，定期对供应商的货物品质、交货期限、价格、服务、信誉等进行评价，为公司采购业务优选供应商。最终公司主要通过招标、询比价、议价谈判等市场化方式进行采购。针对部分项目采购，如果客户有明确要求，则会根据客户的要求进行采购。

（4）生产模式

公司网络安全产品主要形态是纯软件或软硬件结合产品。硬件为服务器、计算机、网络设备等，通过对外采购方式获得。软件分为标准化软件产品和定制开发软件产品。公司软件产品生产的具体情况如下：

①标准化软件产品

公司市场部门根据市场中的热点方向，以及在为客户服务过程中发现新的客户需求，形成市场需求报告。研发部门在此基础上判断技术可行性。如技术上可行，则形成内部业务需求，经公司管理层审核通过后，确定产品研发需求，并对研发部门提出研发任务。研发部门则根据产品需求文档和设计文档进行产品研发，并最终形成标准化软件产品。

②定制化软件产品

公司在开发客户或服务客户过程中，如果客户对公司现有产品提出新的技术要求或功能要求的，业务部门则根据客户需求形成业务需求，经公司管理层审批后，由研发部门实施。实施过程中，研发部门、业务部门与客户不断进行沟通和互动，获得及时反馈，并不断对产品进行优化，最终形成定制化软件产品。公司在定制化产品研发过程中，加强与客户的沟通和互动，获得及时反馈，把控定制化产品需求和目标，控制需求变更和可能发生的各类风险。

（5）销售模式

公司产品销售和服务以直销为主，非直接销售为辅，非直接销售指通过集成商等销售给终端用户，集成商通过招投标、竞争性谈判或单一来源等方式获取最终客户的商业机会后，向公司采购安全产品或服务并交付给终端用户。

公司将客户按行业分布及地域分布进行分类，公司总部或各地子公司、分支机构，通过销售人员直接接触客户，了解客户需求，根据客户实际情况引导和推荐相应解决方案，为客户直接提供产品或服务。

公司主要通过“军团制”的管理模式为客户提供数字风洞及运营、网络靶场及运营、安全防护与管控等产品和服务，针对重点领域及重点区域的客户进行军团化作战，不断提升客户的产品使用体验和合作粘性，确保客户合作的稳定、可持续。

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

①国家政策持续助力行业健康、高质量发展，安全监管全面升级

我国高度重视网络和数据安全，党的十九大报告指出，网络安全等非传统安全是人类面临的共同挑战之一，要坚持总体国家安全观，加强国家安全能力建设，坚决维护国家主权、安全、发展利益；党的二十大报告明确指出要“加快建设网络强国和数字中国”；“十五五”规划纲要明确提出要提升网络安全保障能力，网络强国、数字中国、智慧社会等建设为网络和数据安全发展创造了宝贵机遇。在国家数据安全总体战略布局下，我国持续推进网络安全顶层架构建设，相继出台了《网络安全法》《数据安全法》《个人信息保护法》《关键信息基础设施安全保护条例》《信息安全技术关键信息基础设施安全保护要求》《网络安全等级保护制度2.0标准》等一系列的法律法规，多措并举推动我国网络和数据安全产业高质量发展，夯实我国网络空间安全治理根基。

2025年10月28日，十四届全国人大常委会第十八次会议表决通过了关于修改《中华人民共和国网络安全法》的决定。修改后的《网络安全法》已于2026年1月1日起正式施行。此次修改对原有安全监管体系进行了全面的升级，首次将人工智能治理纳入法治轨道，并强化了主体责任与处罚力度，是一次立足当下、面向未来的系统性升级，也向政企机构清晰地传递出一个信号：合规不再只是监管要求，而是企业赢得市场信任与持续发展的基石。

②“实质合规”驱动，客户“数字健康”管理需求持续释放

没有网络安全就没有国家安全，受国际博弈形势紧张、全球经济增速放缓、企业安全建设薄弱、AI技术赋能等多重因素影响，全球勒索病毒及特种攻击事件呈持续高发态势，从而驱动政企用户“实质合规”意识不断提升。2025年全球勒索攻击持续恶化，勒索攻击愈发高频化，勒索手段愈发多样化，勒索组织愈发专业化，制造业、互联网、医疗保健、金融等业务连续性强、资产规模庞大、数据价值高且敏感的行业成为勒索病毒攻击的重灾区，企业运营和财务遭受严重后果。美国区块链分析公司Chainalysis发布《2026年加密货币犯罪报告》，指出2025年勒索攻击的受害者数量同比增长约50%，达到历史最高水平，勒索攻击态势进一步加剧。尤其是随着AI技术的快速迭代发展，攻击者可借助AI加速代码生成、社会工程攻击，使传统检测手段失效，难以有效应对，构建智能化、体系化的防御体系迫在眉睫。

根据国家安全机关披露，近年来，以美国国家安全局为首的间谍情报机关，持续对我国实施网攻活动，入侵控制关键基础设施，窃取重要情报，监听重点人员，肆意侵犯我国网络主权和个人隐私，严重危害全球网络空间安全。自2022年3月起，该机构持续对我国国家授时中心实施重大网络攻击活动，攻击手段呈现递进式、体系化特点，企图掌握我国时间频率基准的核心数据并

实施破坏。

随着上述威胁愈演愈烈，如何通过构建主动防御体系规避勒索病毒与特种攻击威胁，已经成为政企用户保障网络和数据安全能力建设的重中之重，用户“数字健康”管理需求持续释放。

③网络安全产业挑战与机遇并存，新质生产力为行业发展注入新增量

当下，我国网络安全产业正处于挑战与机遇交织的关键时间点。受市场环境变化等因素影响，下游重点行业客户安全投入意愿减弱，网络安全行业规模增速承压进一步强化行业由“形式合规”向“实质合规”加强趋势，网络安全产业由追求规模扩张，转向追求高质量、可持续发展的新阶段。同时，每一轮科技革命迅猛发展都离不开安全在背后的保驾护航，随着我国在AI、具身智能、低空经济、卫星互联网、智能驾驶等新兴领域的持续突破，新兴产业应用场景的不断涌现和持续扩容也为网络安全市场规模的扩张带来更多增量机会。根据IDC《中国IT安全市场预测，2025-2029》显示，在政策法规持续强化、企业安全投入意愿提升以及新技术应用加速的共同作用下，中国网络安全市场保持稳健增长。IDC预计到2026年，整体市场规模有望突破800亿元人民币，2024—2029年年复合增长率达到8.9%。网络安全已成为数字经济发展中不可或缺的关键基础能力。

④前沿技术加速网络安全产业革新

当前，全球数字化进程正以前所未有的速度推进，网络空间已成为继陆、海、空、天之后的“第五疆域”。在数字经济与前沿技术的飞速发展下，人工智能、量子计算等前沿技术正加速与网络安全产业进行融合，重构网络安全产业生态与发展边界。以人工智能为例，AI大模型技术正系统性重塑网络安全攻防逻辑，加速网络安全产业革新，其通过智能分析过滤海量安全日志与流量数据，能够精准提炼攻击行为特征与威胁模式，可大幅缩短应急响应时间，提升未知威胁的检测效率，有效缓解传统基于规则引擎的滞后性与响应速度慢等问题，并推动网络安全产品形态由传统工具向智能平台的跃迁，从而构建了一个更加智能、安全、高效的新型网络安全体系，推动网络安全产业发展实现质的飞跃。未来，唯有推动技术创新与产业应用深度融合，才能提升防护能力，让前沿技术成为产业革新核心引擎。

（2）公司所处的行业地位分析及其变化情况

近年来，我国网络和数据安全市场参与厂商众多，不同的细分领域存在不同的优势厂商。永信至诚是数字安全测试评估赛道领跑者，网络靶场和人才建设领军者，AI原生安全倡导者，国家级专精特新“小巨人”企业。

在测试评估领域，公司战略发布“数字风洞”产品体系，以中立的生态位置，开启并领跑数字安全测试评估专业赛道发展。公司荣获中国计算机行业协会网络和数据安全专业委员会颁发的

“2025年度卓越贡献奖”;“数字风洞”产品体系荣获中国职工技术协会职工技术创新成果奖特等奖；公司自主研发的“AI大模型安全测评数字风洞平台”入选北京市新技术新产品支持项目；深度参编《人工智能安全风险测评（2025年）》白皮书，为其提供关键技术与实践支撑；在中国网络安全产业联盟主办的2025年网络安全优秀创新成果大赛中，“基于‘数字风洞’的AI大模型测评解决方案”凭借突出的技术创新能力与行业应用价值，荣获“人工智能与机器人安全专题赛”优胜奖；面向数字资产的数字健康管理解决方案入选“十四五”全国金融创新优秀案例；作为香港重点引进的内地网络和数据安全企业，先后与香港数码港、香港引进重点企业办公室、香港物流及供应链多元技术研发中心签署战略合作协议；建设并运营香港“数字风洞”测评中心、北京“数字风洞”测评中心；先后成为海南、福建等多个省市网络安全技术支撑单位;“数字风洞”安全测试评估产品凭借在测试评估领域的专业及领跑优势，入选等级保护测评主办的“十大明星产品”评选。

在网络靶场领域，根据IDC《中国IT安全服务市场追踪报告—网络靶场，2024H2》研究报告显示，永信至诚凭借领先的靶场产品竞争力，以14.3%的市场份额位居中国网络靶场市场第一；2025年全年累计交付和运营超150个国家级、行业级网络靶场建设项目；根据数世咨询发布的《数字靶场能力点阵图2022》显示，永信至诚春秋云境网络靶场在应用创新力和市场执行力维度均位列行业第一；春秋云境网络靶场荣获中国网络安全审查技术与认证中心颁发的首个网络靶场类IT产品信息安全认证证书，也是国内网络靶场产品第一个国家权威认证证书;“基于平行仿真的大规模网络靶场构建技术及应用”项目，荣获北京市科学技术奖（科学技术进步奖）一等奖；参与申报的“超大规模多领域融合联邦靶场（鹏城网络靶场）关键技术及系统”项目，获得国家科学技术进步奖二等奖；支撑国家级电力网络安全靶场建设；落地香港首个国产网络靶场；深度参与多项网络靶场行业标准制定，持续引领产业发展。

在人才建设领域，根据IDC《中国IT安全服务市场跟踪报告，2024H2》报告显示，永信至诚以13.7%市场份额稳居中国企业级培训服务市场第一，并已蝉联八年；i春秋实训平台拥有注册网安实战学习者超过80万名；深度参与2025国家网络安全宣传周系列活动，支撑全国近20省市、地区开展网络安全意识教育；连续三年在国家网安周发布“网络安全人才实战能力白皮书”；组织和支撑超过850场重点赛事演练和实网测试评估演练，持续推动我国各领域网络安全人才选拔、训练、评价体系的建立。

公司行业地位连续多年处于领先水平，预计未来一段时间，公司行业地位仍不会发生重大变化。

（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“数字风洞”将持续满足政企用户“数字健康”管理需求

随着修订后《网络安全法》的正式实施，以及以勒索病毒、特种攻击为代表的具备智能化、高隐蔽性、高渗透性等特征的新型攻击手段持续高发态势。网络和数据安全行业由“形式合规”向“实质合规”加强趋势持续得到强化。在此背景下，安全测试评估已经成为政企用户安全感建设中必不可少的首要环节，用户需转变传统的由“合规导向”的被动防御思维，转向建立前瞻性的安全思维，重视“数字健康”，注重实质安全能力提升。

数字风洞是借鉴航空风洞的理念，围绕政企用户数字化、智能化转型过程中的数字系统及应用等数字资产，构建的全生命周期健康管理平台。通过数字风洞产品体系及其构建的数字健康管理范式，打造智能安全的“检验场”和智能化转型的“安全基座”，全面满足政企用户“数字健康”管理需求，保障国家网络安全、数字安全、智能安全。

②AI**大模型驱动网络靶场智能化演进**

网络靶场作为国家网络安全体系建设的关键基础设施，在提升网络安全实战能力、培养专业人才以及验证安全性能方面发挥着重要作用。然而，随着网络攻击手段正加速向复杂化、智能化和自动化方向演进，传统网络靶场在仿真逼真度、场景动态性、演练效率和智能化水平等方面的局限性愈发凸显，难以完全满足日益复杂化、智能化网络威胁对抗的需求，亟须技术革新提升核心能力。

AI大模型的快速发展为网络靶场的智能化演进提供了关键突破口，AI大模型通过实现从静态脚本到动态智能的场景仿真革新、构建高逼真网络流量环境、赋能自主化的智能攻防博弈以及重塑个性化实战人才培养体系四大维度为网络靶场革新注入新动能，从而显著提升网络靶场的实战化水平与运营效率。

不过，AI大模型作为一把双刃剑，在推动网络靶场革新过程中不可避免会面临诸多技术、应用层面的挑战，以及不容忽视的伦理和安全风险，对此需要在AI赋能靶场的建设和应用中积极践行“负责任的AI”原则，包括确保系统的透明度、可解释性、可问责性、安全性、公平性和隐私保护。建立健全严格的安全可控评估机制，围绕大模型全生命周期的数据安全、内容安全、运行安全展开多维度、多层面的评估，识别并消除安全隐患。

③新质生产力带来的新型安全需求将持续释放

网络安全是加快培育新质生产力，推动新质生产力实现大规模应用落地的重要保障。近年来，以AI、具身智能、低空经济、卫星互联网、智能驾驶等为代表的新质生产力的蓬勃发展不断带动网络安全技术的创新和安全边界的拓宽，新兴应用场景的持续扩容也为网络安全市场规模的扩张

带来更多增量机会。例如，随着大语言模型的飞速发展，AI系统在应用层面临漏洞与基础设施攻击风险，数据层存在数据投毒、隐私泄露隐患，网络层开放API易遭未授权访问，供应链层开源组件隐患可扩散至全产业生态，多重风险叠加，尤其是伴随着全球范围内OpenClaw部署热潮，其部署风险更是给所有AI使用者敲响警钟；具身智能在感知、决策、执行、交互各环节的失误，已不再只是数据层面的偏差，而会直接引发现实世界的安全风险，感知层受环境干扰或对抗欺骗可能导致认知偏差，决策层因大模型的不确定性可能引发错误甚至失范决策，执行层的控制系统或通信链路一旦失守，将直接影响设备行动安全，交互层的隐私泄露与欺骗行为则会削弱人机互信基础。

在此背景下，公司的核心技术网络空间平行仿真技术是数字化新一代关键技术的基座，可以模拟与各种现实网络空间相对应的场景模型，构建高仿真业务环境，支撑 AI、具身智能、低空经济、卫星互联网、智能驾驶等新兴产业进行网络空间的测试、演练、实训、推演、研判、指挥、防御、实战等综合性仿真业务和安全业务开展；同时，公司“数字风洞”产品体系是为数字化建设提供安全测试评估的基础设施，可以为 AI、具身智能、低空经济、卫星互联网、智能驾驶等场景下的网络和数据环境提供全周期的数字安全测试评估，保障“数字健康”。

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：万元　币种：人民币

	2025年	2024年	本年比上年增减(%)	2023年
总资产	111,922.62	121,953.02	-8.22	124,786.84
归属于上市公司股东的净资产	97,192.69	102,652.06	-5.32	106,652.11
营业收入	27,634.02	35,632.63	-22.45	39,586.55
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	27,634.02	35,632.63	-22.45	39,586.55
利润总额	-4,981.06	197.25	-2,625.23	3,210.74
归属于上市公司股东的净利润	-4,898.67	848.22	-677.52	3,110.54
归属于上市公司股东的扣除非经常性损益的净利润	-5,727.82	-205.77	不适用	1,103.04
经营活动产生的现金流量净额	-225.01	-4,630.06	不适用	-1,855.52
加权平均净资产收益率（%）	-4.90	0.82	减少5.72个百分点	2.94
基本每股收益（元／股）	-0.32	0.05	-740.00	0.20
稀释每股收益（元／股）	-0.32	0.05	-740.00	0.20
研发投入占营业收入的比例（%）	31.63	26.01	增加5.62个百分点	21.24

3.2 报告期分季度的主要会计数据

单位：万元　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	3,008.50	5,519.51	5,701.34	13,404.67
归属于上市公司股东的净利润	-2,397.43	-1,807.83	-1,280.01	586.60
归属于上市公司股东的扣除非经常性损益后的净利润	-2,459.14	-2,112.73	-1,353.20	197.25
经营活动产生的现金流量净额	-3,596.13	-733.62	-511.50	4,616.23

注：数据若有尾数差，为四舍五入所致。

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十名股东情况

单位：股

截至报告期末普通股股东总数(户)	7,540
年度报告披露日前上一月末的普通股股东总数(户)	7,299
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	
蔡晶晶	17,102,994	52,734,231	34.93	0	无	0	境内自然人
陈俊	7,894,902	24,342,615	16.13	0	无	0	境内自然人
奇安（北京）投资管理有限公司－北京奇安创业投资合伙企业（有限合伙）	-4,359,662	7,548,135	5.00	0	无	0	其他
北京熙诚金睿股权投资基金管理有限公司－北京新动力股权投资基金（有限合伙）	-299,161	2,075,762	1.38	0	无	0	其他
北京启明星辰信息安全技术有限公司	-311,740	1,790,359	1.19	0	无	0	国有法人
孙绪隆	1,681,604	1,681,604	1.11	0	无	0	境内自然人
丁来英	1,369,969	1,369,969	0.91	0	无	0	境内自然人
郑君	1,217,550	1,217,550	0.81	0	无	0	境内自然人

北京信安春秋科技合伙企业（有限合伙）	321,726	991,989	0.66	0	无	0	其他
众安在线财产保险股份有限公司－自有资金	842,379	842,379	0.56	0	无	0	其他
上述股东关联关系或一致行动的说明	1、截至本报告披露之日，公司前十名股东中，蔡晶晶与陈俊为一致行动人，蔡晶晶直接持有公司34.93%股份，通过信安春秋支配公司 0.66%股份，通过《一致行动人协议书》与陈俊一起支配公司 16.13%股份。 2、公司未知其他股东之间是否存在关联关系或一致行动。						
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

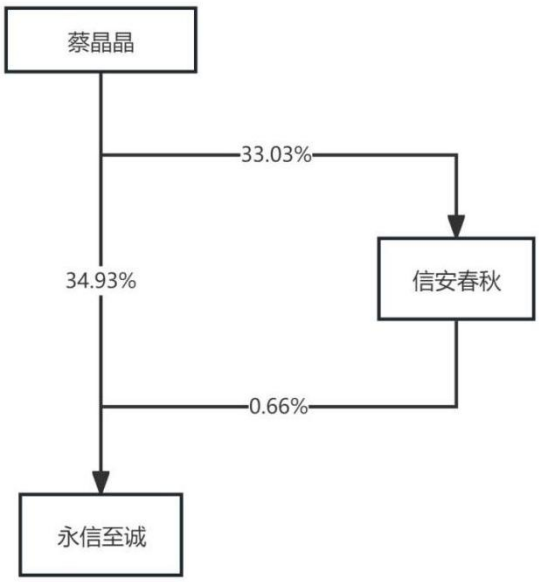
□适用 √不适用

截至报告期末表决权数量前十名股东情况表

□适用 √不适用

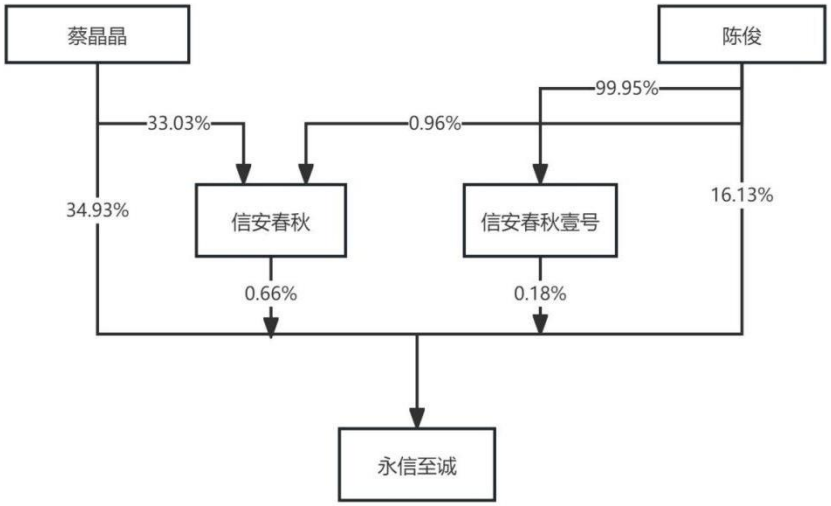
4.2 公司与控股股东之间的产权及控制关系的方框图

√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十名股东情况

□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，公司实现营业收入 27,634.02 万元，同比减少 22.45%；实现归属于上市公司股东的净利润-4,898.67 万元;实现归属于上市公司股东的扣除非经常性损益后的净利润-5,727.82 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