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

# 2023 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、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 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**

经天健会计师事务所（特殊普通合伙）审计，截至 2023 年 12 月 31 日，公司母公司报表中期末未分配利润为人民币 173,901,566.26 元，2023 年度公司归属于上市公司股东的净利润为人民币 31,105,410.29 元。经董事会决议，公司 2023 年度拟以实施权益分派股权登记日登记的总股本扣除公司回购专户中的股份数为基数分配利润、转增股本。本次利润分配及资本公积金转增股本方案如下：

（1）拟向全体股东每 10 股派发现金红利 2.26 元（含税）。截至 2024 年 4 月 26 日，公司总股本 69,310,328 股，扣除回购专用证券账户中股份数 718,937 股后的剩余股份总数为 68,591,391 股，以此计算合计拟派发现金红利 15,501,654.37 元（含税），占 2023 年度实现归属于上市公司股东的净利润的比例为 49.84%。

（2）拟向全体股东以资本公积金每 10 股转增 4.8 股。截至 2024 年 4 月 26 日，公司总股本 69,310,328 股，扣除回购专用证券账户中股份数 718,937 股后的剩余股份总数为 68,591,391 股，

以此计算合计转增 32,923,867 股，转增后公司总股本增加至 102,234,195 股（具体以中国证券登记结算有限责任公司登记为准）。

在实施权益分派的股权登记日前公司总股本扣减公司回购专用证券账户中的股份数发生变动的，公司拟维持分配总额、转增总额不变，相应调整每股分配比例和每股转增比例，并将另行公告具体调整情况。

公司 2023 年度利润分配及资本公积金转增股本方案已经公司第三届董事会第二十次会议审议通过，尚需公司 2023 年年度股东大会审议通过。

**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 | 永信至诚 | 688244 | / |

**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 | 张恒 | 丁一凡 |
| 办公地址 | 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 |
| 电子信箱 | yxzc@integritytech.com.cn | yxzc@integritytech.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

#### 1、主营业务基本情况

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，国家级专精特新“小巨人”企业。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“数字风洞”测试评估、网络靶场及运营、安全防护与管控、网络安全竞赛服务以及其他服务，其他服务主要包括线上线下培训服务。

目前，公司已经帮助上千家政企用户解决数字化进程中安全有效性验证和仿真环境缺失、人员实战能力不足、政企用户主动防护能力缺乏等问题。公司致力于成为网络空间与数字时代安全基础设施关键建设者，保障“数字健康”，带给世界安全感！

**2、主要产品和服务**

**（1）“数字风洞”测试评估**

数字风洞是为数字化建设提供安全测试评估的基础设施，基于永信至诚独创的安全趋于“证无”理念，以“3×3×3×（产品×服务）”（第一个 3 指三类用户：城市、行业、单位；第二个 3 指三类场景：人、系统、数据；第三个 3 指业务周期的三个阶段：规划、运营、处置）安全感公式为方法论构建而成，通过在指定场景里对城市、行业、单位、人、系统、数据等各要素进行系统性风险验证，度量安全效果，提升综合防护能力。公司以“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×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”。

“数字风洞”产品体系具有如下特点：

①风洞时光机：独创风洞时光机系统，实现各类测评任务整体封装、快速重放、风险复测。基于公司十年打磨全自研专有云平台，构建高逼真业务环境和高拟真数据交互的沉浸式安全测评环境，结合多循环激励模式及全维度数据可视化，不断迭代安全风险。

②威胁激励+全维数据采集：插件化的智能风险载荷控制，渐进式安全威胁激励和被试体全维响应采集，为被试体提供科学的全方位“风洞”测试，为迭代优化提供数据和平台支持。

③多循环激励响应：提供多类智能评估模型，结合多循环激励响应控制，科学评价被试体迭代成效。

④热修复方案：提供与风险载荷配套的热修复方案，利用系统化防护手段解决在系统迭代优化空窗期的安全保障难题，指导系统快速完成风险控制与修复处置。

⑤合规留痕：被试体测试评估和优化迭代全生命周期立体化数字留痕，助力被试体合规审查要求。

⑥全场景应用：满足“人、系统、数据”的各类测试评估需求。

报告期内，“数字风洞”产品体系助力政府部门、能源、电力、电信、民营企业等关键行业安全趋于“证无”；落地了数字政府安全测试评估、数据安全测试评估、系统安全测试评估、人员能力检验与评价、人工智能安全测试评估以及关键行业安全测试评估六大典型应用场景；在等级保护测评主办的“2023 年网络安全优秀评选”活动中，公司“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“十大明星产品”。

**（2）网络靶场及运营**

网络靶场是数字化建设过程中安全性测试的重要基础设施，是检验和评估安全防御体系有效性的重要技术系统，是国家对重大网络安全风险和趋势进行推演和论证研判的重要科学装置，是防范化解重大网络安全风险的重要手段，也是政企、院校、科研机构等单位网络安全人才培养的重要支撑平台。

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，该平台融合了主机虚拟化、网络虚拟化、软件定义网络、多维数据采集、3D 展示引擎和高可用云端架构等多种前沿技术，支持多种角色以不同权限和资源访问能力在同一靶场场景中进行联合交互和测试。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。同时，通过理解和分析客户的靶场应用场景，公司可以帮助客户分析和发现利用靶场各功能系统帮助客户实现最佳实践的方案，并结合客户痛点提供优质的运营服务，以靶场产品为核心帮助客户进行意识教育、人才培训及选拔、实网安全演练及测评、复杂业务模拟、安全对抗复盘等活动。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，荣获北京市科学技术奖（科学技术进步奖）一等奖。公司通过春秋云境网络靶场平台连续三届为“网鼎杯”网络安全大赛提供专业支持，持续在大赛规则、赛制赛题设计、技术平台支持、赛事运营保障等方面树立国家级竞赛标准。

报告期内，公司网络靶场领军地位稳固，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；支撑了国家多个部委主办的数十场网络安全演练活动及多个行业的靶场建设工程；赛事演练、人才培养、智慧城市安全测试、案件线索追踪实战、业务模拟仿真、人工智能攻防、复杂业务安全推演及综合应用等“7+1”应用场景持续运营，发展态势持续向好。

**（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罐系统、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。

①春秋云阵新一代蜜罐系统

春秋云阵新一代蜜罐系统基于“欺骗式防御”理念，利用永信至诚特有的平行仿真技术和全量行为捕获技术，构建高甜度的蜜罐环境，诱捕攻击者进入仿真网络环境中，大大延缓攻击者对实际业务网络的攻击。同时，不再依赖特征库对流量层的威胁行为进行甄别，“触碰蜜罐即报警”“深入蜜罐即攻击”，保证蜜罐系统对所有攻击的“零误报”特征。全程记录攻击轨迹和攻击行为，实现了对攻击者的快速取证和溯源。在不影响现有网络的安全架构下，利用其高甜度、易部署、零误报的特性，简化网络安全运维工作的复杂程度，有效增强实际业务网络的安全防护能力。该平台已获评数说安全“中国网络安全蜜罐顶级供应商”。

该产品主要用户为政府部门、能源、电力、交通等国家关键信息基础设施运营单位。

②春秋云势网络安全态势感知与处置平台

春秋云势态势感知平台是基于大数据技术框架，综合全维度安全因素，从整体上动态监管网络安全状况，提升风险发现、决策分析、响应处置能力的网络空间安全综合治理体系。该体系具有“精准预警、高效处置”的特点，能够合理调配安全专家，在预定义的处置场景下，及时、高效处置网络安全事件，从而帮助监管部门和重点用户从总体把握网络安全态势，研判网络安全趋势和解决网络安全问题，最终实现“可感知、可研判、可处置”的网络态势安全闭环。

态势感知主要面向政府部门、行业主管机构、关键信息基础设施运营单位等用户。

③蜜罐及态势感知整合安全管控

蜜罐及态势感知系统可以组合使用，也可以分别单独使用。组合使用，可以发挥良好的协同效应，达成产品的最佳效能，对网络空间环境形成整体的安全管控。蜜罐主要部署于边界安全产品之后，其主要部署在被保护网络内部，与内部网络形成一体。态势感知平台利用其卓越的大数据汇聚、存储和分析处理能力，形成对非法入侵等网络威胁的感知能力，并依托公司网络安全处置能力，协助管理部门处置各类安全事件，为用户实现了全场景、高精度、高处置的“全天候、全方位感知网络安全态势”能力。

④安全工具类产品

随着国家政策法规对网络安全要求的提升以及信息技术的高速发展，国家监管部门在新的业务场景和垂直领域中的需求不断更新，公司开发并快速迭代了一系列行业创新应用类产品，满足监管部门的特定需求，维护国家网络安全。安全工具类产品包括：流量监测类产品、数据分析类产品、情报管理类产品、安全攻防类产品等。

⑤安全防护系列服务

随着网络安全形势愈发严峻，政府、企业用户对网络安全保障需求不断提升，我国网络安全市场正从产品市场不断向服务市场扩展，安全服务是网络安全市场一个重要分支。网络安全相关法规对政府、企业等关键信息基础设施运营单位明确提出了开展安全检测、安全测评、安全演练的相关要求，规定了等级保护制度安全措施的基线要求并赋予强制力。随着法规和标准的实施，网络安全服务市场快速增长，成为网络安全产业中一个重要的细分领域。

公司基于自身对网络攻防和各行业网络安全风险场景的深刻理解，以高效、实效提升用户安全防御水平为目标，向用户提供安全检测与评估、安全咨询、安全运维与分析处置以及安全能力建设与评估等方面服务。

**（4）网络安全竞赛服务**

网络安全技术是一项注重实战的技术，在国家数字化转型的关键时期，各行各业在享受数字化红利的同时也面临勒索病毒、特种攻击、数据泄露、系统中断等巨大安全风险，各行业具有网络安全实践能力的人才培养及选拔，以及实战能力的有效测评成为急需解决的问题，关系到我国各行业数字化转型的战略实现。2019 年 5 月，美国总统签署了一项行政令，要求举办新总统杯网络安全竞赛，为政府选拔出国家顶级网络安全人才。根据教育部《网络安全人才实战能力白皮书》数据显示，到 2027 年，我国网络安全人员缺口将达 327 万，诸多行业将面临网络安全人才缺失的困境。近年来我国相关部门也出台了有关政策，支持和规范网络安全竞赛健康发展。

永信至诚自 2014 年开始一直致力于国内网络安全赛事运营，打造了知名的网络安全赛事专业品牌春秋 GAME，推动了安全赛事从小到大，从企业到集团，从集团到行业，从地区到全国，从单一到多元的发展，并带动不同产业网络安全人才选拔、训练、评价体系的建立。公司春秋 GAME 网络安全赛事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；竞赛平台包括线上竞赛平台和线下竞赛平台，支持个人赛和团体赛，除了支持目前国际主流的夺旗赛（CTF）、攻防赛（AWD）外，并开创性发展了靶场赛（ISW）、人工智能网络安全竞赛（RHG）、共同防御、实景防御赛（RDG）等多种竞技模式，随着对数字化进程中数字安全的深刻思考和大量实践，创新构建以安全风险修复为导向的“ZHWU 证无”赛制。这些赛事竞赛系统、竞技模式及规则和标准影响了我国各行业各领域网络安全竞赛实践。

随着公司多年来对国家主管单位和各部委进行的网络安全赛事市场普及教育和推广，自 2019 年起，网络安全赛事从一个网络安全盛会中可有可无的配套活动，变成了重大网络安全活动中的重点项目，行业人才培养、选拔、评价的重要手段，高校学科教育和人才评价的重要配套，以及地方政府招商引资、产业建设的重点工程。公司为全国各地、各行业打造了包括网鼎杯、强网杯、

春秋杯等在内的数十个知名赛事品牌，成为行业及地方网络安全名片。

**（5）其他服务**

其他服务主要包括线上安全培训、线下安全培训。

①线上安全培训

公司线上安全培训服务主要通过 i 春秋实训平台开展，该平台是自主研发的服务平台。i 春秋实训平台以互联网门户网站形式展现，目前注册网安实战学习者超过 80 万名，课程超过 300 门，在线实验场景超过 3,000 个。此外，平台建立了包含百度、阿里、腾讯、京东等八十多家互联网公司入驻的自有品牌 SRC 部落，形成了国内有重要影响力的网络安全社区，提升了公司在网络安全领域的影响力、知名度。

②线下安全培训

线下安全培训分为线下培训就业班、线下培训定制班和国家网络安全技术认证班三种类型。线下培训就业班以渗透测试工程和网络安全攻防工程师培训为主。线下培训定制班主要服务于政府部门、各大企事业单位、学校等，针对于网络安全技术和网络安全大赛技术为主要培训方向。网络安全技术认证班主要以培训及考取国家网络安全技术人员认证为主，是中国信息安全测评中心、网络安全技术审查与认证中心和公安部授权的培训机构。

## （二） 主要经营模式

1、盈利模式

公司盈利主要来源于向客户销售自主研发的网络安全产品，以及向客户提供网络安全服务。“数字风洞”测试评估、网络靶场及运营、安全防护与管控、网络安全竞赛服务主要面向政企类客户，线上线下培训服务主要面向个人和企事业单位。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、网络攻防对抗技术和多循环数字风洞测试评估技术，公司自建研发体系持续进行网络空间平行仿真、网络攻防对抗和多循环数字风洞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。通过销售部门、市场部门、研发部门、质量部门的整体协作，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。由于公司业务一般体现为项目制特征，公司采购通常亦是跟随不同项目的具体需求进行采购。

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，由研发部门进行实施。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。

（3）安全服务

公司安全服务部门从技术和业务需求两个生产维度设定安全防护类服务的产品设计。首先依托对攻防技术的积累，根据网络空间安全的技术类型设定和市场共性需求，初步设计出安全防护类服务的服务类型；在为客户提供服务的过程中，根据行业客户的共性需求和自身技术积累，提交需求说明，进行产品设计优化，进行细分服务类型的二次开发和升级；在服务实施过程中，收集客户反馈和建议，对于服务质量和流程进行管控。在安全防护类服务的生产过程中，公司始终以客户需求为核心，以自身技术优势为基础，打造有市场、高能效的安全服务产品。

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。

公司通常以“项目制”形式为客户提供产品和服务，公司主要通过参与客户组织的招投标、竞争性谈判或客户的单一来源采购等方式取得项目合同，公司获取项目合同后实施合同，经客户验收通过后出具验收文件。此外，为进一步拓展新客户和新市场，对于部分成熟产品，公司还采用试用推广模式，即先将成熟产品提供给最终客户试用，通过产品试用发展新客户。

## （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

（1）全球网络安全行业发展概况

①全球网络安全形势复杂严峻，发达国家加速网络安全战略布局

近年来，全球重大网络安全事件频繁发生，严重威胁各国的经济发展和社会的安全稳定，“棱镜门”、RSA 后门、Intel 芯片安全漏洞、WannaCry 勒索软件、Facebook 用户数据泄漏等安全事件引起了全球各界对网络安全的高度重视。此外，随着网络空间安全形势快速变化以及人工智能技术的快速发展，国家级博弈更为突出、攻防对抗更为激烈、数字经济安全保障要求不断提升。

为应对层出不穷的网络安全威胁，主要发达国家均加大网络安全领域的投入力度、细化和调整网络安全相关政策和法规要求，在网络空间主导权、话语权方面争夺更加激烈。2017 年，根据美国总统指示，美国国防部将网络司令部升级为一级联合作战司令部，成为美军第十个联合作战司令部，地位与美国中央司令部等主要作战司令部持平。2018 年以来，美国在国土安全部设立一个新的网络安全机构“网络安全与基础设施保护局”，将网络安全预算大幅增加至 300 亿美元。

2023 年以来，美国政府先后发布了《国家网络安全战略》《2023 年国防部网络战略》《美国政府关键和新兴技术国家标准战略》《国家网络安全战略实施计划》等一系列政策文件，旨在进一步加速完善美国网络安全总体布局，增强美国在网络安全、关键信息基础设施安全、数据安全等领域的安全防御能力，确保国家安全、经济繁荣、国家关键基础设施、公民隐私免受网络安全威胁的攻击。

面对日益严峻的网络安全形势，欧盟也在 2023 年加速网络和数据安全领域相关法律法规的颁布与实施，先后出台了《关于在欧盟全境实现高度统一网络安全措施的指令》（NIS 2 指令）、《关于 GDPR 下的个人数据泄露通知的第 9/2022 号指南》《网络团结法案》等法律法规，2024 年 1 月 7 日，欧盟《网络安全条例》正式生效，该条例规定了欧盟内实体内部网络安全风险管理、治理和控制框架的具体措施。

②全球各国网络靶场建设情况

根据 2015 年 4 月人民网转发的中国军网的文章《美国网络“曼哈顿计划”》，早在 2008 年，美军就启动了被称为新世纪网络安全“曼哈顿计划”的国家网络靶场建设，为美国国防部模拟真实的网络攻防作战提供虚拟环境。

2021 年 7 月，据美国国防部网站消息，美国已授权价值 24.10 亿美元的网络靶场相关合同。在未来的 10 年中，赢得订单的公司将为军方网络任务部队提供事件规划和执行、场地安全、信息技术管理以及靶场现代化和作战支持，同时通过测试、规划和系列活动来支持国家网络靶场综合设施的运行。总体上，该合同的主要目标是为其国家网络靶场综合设施提供 IT 服务。2023 年，美国第 2 届网络空间日光浴委员会发布的《2023 年实施报告》指出美国政府在网络空间建设方面有明确的战略规划和实施进度，网络靶场作为其中的重要支撑手段，得到了相应的政策支持和资

源倾斜。

美国建设国家网络靶场引起了各国高度重视。英、德、俄、日、韩等国借鉴美国经验，建设了同类项目，作为支撑网络空间安全技术演示验证、网络武器装备研制试验的重要工具。

（2）我国网络安全行业发展概况

①我国网络安全市场规模稳步增长

根据 IDC 发布的《全球网络安全支出指南》（2024 年 V1 版）预测，中国网络安全市场规模预计将从 2022 年的 123.5 亿美元快速增长至 2027 年的 233.2 亿美元，期间年复合增长率为 13.5%，高于全球平均水平。

中国网络安全产业联盟在《中国网络安全产业分析报告（2023 年）》中指出，展望未来三年，网络安全产业发展顶层设计更加完善，促进行业发展的政策基础愈加稳固，数字经济加速发展等正向激励将给网络安全产业注入新动力，产业结构调整逐步深化，更多网络安全板块将涌现出来。

根据工信部发布《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》中提出，到 2023 年，电信等重点行业网络安全投入占信息化投入比例达 10%。2023 年网络安全产业规模超过 2,500 亿元。

②勒索病毒与特种攻击威胁升级

没有网络安全就没有国家安全，随着各种新型攻击手段的不断出现以及大国竞争的持续深化，政企用户面临的网络安全形势越来越复杂严峻，网络安全牵一发而动全身。一方面，以勒索病毒为代表的网络安全威胁事件呈不断上升趋势，并呈现出勒索攻击逐渐产业链化、勒索方式多元化、勒索赎金规模化的发展特征，2023 年以来，包括英国皇家邮政、波音、米高梅以及国内某大型银行在美全资子公司等一大批国内外知名单位先后遭受到勒索病毒攻击，勒索病毒已经成为危害政企用户网络安全的头号威胁，上述勒索事件给企业正常运营带来了严重的负面影响，同时也给政企用户如何构建主动防御体系保护网络和数据安全敲响了警钟。

另一方面，2023 年 9 月，中国国家安全部在官方微信公众号发文指出，美国情报部门凭借其强大的网络攻击武器库，对包括中国在内的全球多国实施监控、窃密和网络攻击，并多次对我国进行体系化、平台化攻击，试图窃取我国重要数据资源。2023 年 7 月 26 日，武汉市应急管理局地震监测中心部分地震速报数据前端台站采集点网络设备遭受境外组织的网络攻击，攻击手段符合美国情报机构特征，目标是窃取地震监测相关数据，具有明显的军事侦察目的。这是继 2022 年 6 月西北工业大学遭受境外网络攻击后又一具体案例，受全球经济增速放缓、地缘政治冲突的升级以及能源危机等因素影响，我国关键信息基础设施已经成为境外网络攻击重点关注和首要打

击对象，未来或将持续暴露在境外特种攻击威胁之下。

③我国网络靶场建设情况

我国互联网规模和用户规模均居世界第一，但核心技术与关键资源依赖国外产品情况严重，勒索病毒、网络攻击、信息窃取等事件呈多发态势，我国面临的境外网络攻击和威胁越发严重，网络靶场是保障网络安全的重要基础设施。在国家网络靶场建设方面，无论从靶场基础理论研究、关键技术和产品研发，还是网络空间安全风险评估研究，与欧美国家相比，我国都还存在着一定差距。

2023 年 1 月 30 日，国家能源局综合司印发《2023 年电力安全监管重点任务》（以下简称“重点任务”），面向全国电力单位，对 2023 年度电力安全工作进行详细部署，旨在确保电力系统安全稳定运行和电力可靠供应。在重点任务中，明确要求“推进国家级电力网络安全靶场建设”，并强调安全风险评估、攻防演练、教育培训等内容。

随着国家和社会不断加大对网络靶场的投入，贵阳启动大数据网络安全靶场建设、鹏城实验室成立、公司作为第一完成人的“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 2019 年度北京市科学技术奖（科学技术进步奖）一等奖，以及“网鼎杯”“强网杯”等国家级重要赛事的持续成功举办，推动网络靶场行业迅速发展。

**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行业市场增长较快，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，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；与国家工业信息安全发展研究中心（工业和信息化部电子第一研究所）签署战略合作协议，共同建设并运营“工业安全数字风洞测试评估基地”；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签署战略合作协议，建设并运营“香港数字风洞测评中心”；“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《中国网络安全实训演练测试平台市场份额，2021：高歌猛进，快速发展》研究报告显示，永信至诚凭借春秋云境网络靶场产品，以 20.4%的市场份额位居第一名；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；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，公司连续第七年稳居中国 IT 安全企业级培训服务市场第一；i 春秋实训平台拥有注册网安实战学习者超过 80 万名；荣获“2023 年中国产学研合作创新奖”，成为网络和数据安全领域唯一获奖企业；子公司天健网安负责管理运营的网络安全科技馆入选由中央网信办等 13 个部门认定的全民数字素养与技能培训基地；作为主编单位之一发布国内首部聚焦网络安全人才评价的白皮书—《网络安全人才实战能力白皮书-人才评价篇》；组织和支撑超过 610+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**

没有网络安全就没有国家安全，网络和数据安全与国家经济运行、社会治理、公共服务等方面密切相关，保障网络和数据安全已成为事关国家安全与经济社会发展的重大问题。近年来，随着《网络安全法》《数据安全法》《个人信息保护法》《密码法》《网络安全审查办法》《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》《数据出境安全评估办法》等网络和数据安全相关法律法规相继出台、实施，以《网络安全法》和《数据安全法》为基础的网络和数据安全立法体系基本完成，网络和数据安全行业顶层设计愈发完善，政策驱动行业长期发展格局向好。2024 年 2 月，工信部印发《工业领域数据安全能力提升实施方案（2024-2026 年）》，为工信领域数据安全监管和保护工作提供了指导和依据。

（1）网络和数据安全行业趋势由“形式合规”向“实质合规”加强

随着数字经济的高速发展，网络和数据安全作为经济发展的关键基座，迎来了前所未见的机遇与挑战。一方面，近年来我国网络安全、数据安全相关法律法规陆续推出，对网络和数据安全建设工作提出了诸多标准和要求；另一方面，勒索病毒、特种攻击等网络安全威胁层出不穷，严重威胁国家安全和社会经济发展。在此背景下，网络和数据安全行业开始由“形式合规”向“实质合规”加强，永信至诚战略发布“数字风洞”产品体系，开启并领跑数字安全测试评估专业赛道。

数字风洞是为数字化建设提供安全测试评估的基础设施，基于永信至诚独创的安全趋于“证

无”理念，以“3×3×3×（产品×服务）”安全感公式为方法论构建而成。通过在指定场景里对城市、行业、单位、人、系统、数据等各要素进行系统性风险验证，度量安全效果，提升综合防护能力。公司以“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×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”。

公司将持续助力网络和数据安全行业由“形式合规”向“实质合规”加强，进一步夯实永信至诚网络靶场和人才建设领域的领军地位，跃迁式创新推动安全测试评估专业赛道发展，为公司整体迈入规模化发展奠定坚实基础。公司致力于成为中国网络空间与数字时代安全基础设施关键建设者，为我国数字经济安全稳健发展保驾护航。

（2）AI 大模型急需常态化测试评估

以 ChatGPT 为代表的 AI 大模型新技术、新应用的快速发展给行业发展带来新的增量机会，打开了网络攻防对抗新局面，AI 在赋能网络和数据安全行业发展的同时，一些实际存在的 AI 大模型安全问题引发公众的深切担忧，一是 AI 大模型作为复杂的软件系统，面临基础设施和软件安全风险，如系统漏洞、数据泄露、模型篡改等；二是 AI 大模型虽然提高了内容产出质量，但同时生成的内容可能包含误导信息或偏见内容，被用于不良目的，如钓鱼邮件和恶意软件的编写，降低网络攻击等犯罪门槛。

2023 年 8 月 15 日，由国家网信办联合国家发展改革委、教育部、科技部、工业和信息化部、公安部、广电总局发布《生成式人工智能服务管理暂行办法》（以下简称“《办法》”）正式施行。《办法》明确要求提供具有舆论属性或者社会动员能力的生成式人工智能服务的，应当按照国家有关规定开展安全评估。

2024 年 3 月 1 日，全国网络安全标准化技术委员会发布 TC260-003《生成式人工智能服务安全基本要求》（以下简称“《要求》”），《要求》给出了生成式人工智能服务在安全方面的基本要求，包括语料安全、模型安全、安全措施、安全评估等，进一步明确要求提供者在向相关主管部门提出生成式人工智能服务上线的备案申请前，应按照《要求》中各项要求逐条进行安全性评估，并将评估结果以及证明材料在备案时提交。

公司网络靶场系列产品和“数字风洞”产品体系均是人工智能安全测试评估的基础设施平台，具备对人工智能相关产品和风险进行安全测试评估的能力。AI 大模型安全测评“数字风洞”协同 AI 春秋大模型，可以实现对大模型基础设施安全和内容安全风险进行持续性检查，支撑 AI 大模型常态化安全测试评估，为 AI 技术在各行业的安全应用保驾护航，保障 AI“数字健康”。

## 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：万元　币种：人民币

| | 2023年 | 2022年 | | 本年比上年增减(%) | 2021年 | |
|---|---|---|---|---|---|---|
| | | 调整后 | 调整前 | | 调整后 | 调整前 |
| 总资产 | 124,786.84 | 118,010.57 | 118,010.18 | 5.74 | 61,180.39 | 61,180.33 |
| 归属于上市公司股东的净资产 | 106,652.11 | 105,087.00 | 105,086.61 | 1.49 | 49,401.00 | 49,400.93 |
| 营业收入 | 39,586.55 | 33,066.03 | 33,066.03 | 19.72 | 32,016.59 | 32,016.59 |
| 归属于上市公司股东的净利润 | 3,110.54 | 5,080.64 | 5,080.31 | -38.78 | 4,707.21 | 4,707.15 |
| 归属于上市公司股东的扣除非经常性损益的净利润 | 1,103.04 | 3,985.15 | 3,984.83 | -72.32 | 3,656.68 | 3,656.61 |
| 经营活动产生的现金流量净额 | -1,855.52 | -1,753.82 | -1,753.82 | 不适用 | 1,033.57 | 1,033.57 |
| 加权平均净资产收益率（%） | 2.94 | 8.42 | 8.41 | 减少5.48个百分点 | 10.00 | 10.00 |
| 基本每股收益（元／股） | 0.45 | 0.93 | 1.37 | -51.61 | 0.91 | 1.34 |
| 稀释每股收益（元／股） | 0.45 | 0.93 | 1.37 | -51.61 | 0.91 | 1.34 |
| 研发投入占营业收入的比例（%） | 21.24 | 19.11 | 19.11 | 增加2.13个百分点 | 15.60 | 15.60 |

### （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 | 26,610,651.68 | 57,926,957.56 | 86,195,146.76 | 225,132,744.06 |
| 归属于上市公司股东的净利润 | -16,468,200.36 | -10,315,199.46 | -3,707,520.02 | 61,596,330.13 |
| 归属于上市公司股东的扣除非经常性损益后的净利润 | -18,356,639.94 | -15,882,132.81 | -14,556,724.87 | 59,825,852.72 |
| 经营活动产生的现金流量净额 | -37,415,638.16 | -10,524,546.96 | -17,363,121.19 | 46,748,142.31 |

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) | 3,183 |
| 年度报告披露日前上一月末的普通股股东总数(户) | 1,947 |
| 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

| 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 | 7,808,160 | 24,075,160 | 34.74 | 24,075,160 | 无 | 0 | 境内自然人 |
| 陈俊 | 3,604,320 | 11,113,320 | 16.03 | 11,113,320 | 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） | 2,616,000 | 8,066,000 | 11.64 | 0 | 无 | 0 | 其他 |
| 北京启明星辰信息安全技术有限公司 | 685,440 | 2,113,440 | 3.05 | 0 | 无 | 0 | 境内非国有法人 |
| 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） | 592,699 | 2,058,759 | 2.97 | 0 | 无 | 0 | 其他 |
| 国信证券－招商银行－国信证券永信至诚员工参与战略配售集合资产管理计划 | 561,975 | 1,732,757 | 2.50 | 0 | 无 | 0 | 其他 |
| 中国建设银行股份有限公司－博时军工主题股票型证券投资基金 | 809,565 | 1,351,973 | 1.95 | 0 | 无 | 0 | 其他 |
| 浙江赛智伯乐股权投资管理有限公司－杭州同心众创投资合伙企业（有限合伙） | 240,000 | 740,000 | 1.07 | 0 | 无 | 0 | 其他 |
| 冯亚 | -62,588 | 674,694 | 0.97 | 0 | 无 | 0 | 境内自然人 |
| 国信资本有限责任公司 | 103,987 | 599,478 | 0.86 | 599,478 | 无 | 0 | 国有法人 |

| | |
|---|---|
| 上述股东关联关系或一致行动的说明 | 截至本报告披露日，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34.74%股份，通过信安春秋支配公司0.65%股份，通过《一致行动人协议书》与陈俊一起支配公司16.03%股份；除此之外，公司未知上述股东间存在其他关联关系或一致行动。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。 |
| 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**

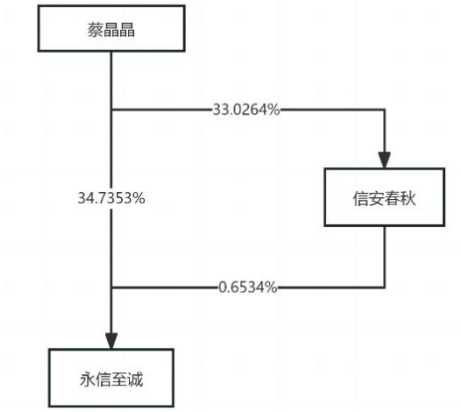
□适用 √不适用

**截至报告期末表决权数量前十名股东情况表**

□适用 √不适用

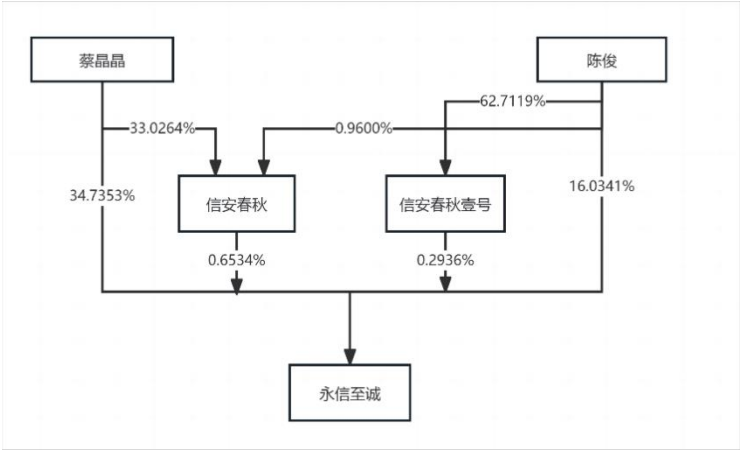
**（二）公司与控股股东之间的产权及控制关系的方框图**

√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。

报告期内，公司实现营业收入 39,586.55 万元，比上年同期增长 19.72%；实现归属于上市公司股东的净利润 3,110.54 万元，比上年同期下降 38.78%；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 1,103.04 万元，比上年同期下降 72.32%。

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