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

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 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2024年12月31日，公司母公司报表中期末未分配利润为人民币166,617,529.44元，2024年度公司归属于上市公司股东的净利润为人民币8,482,212.34元。经董事会决议，公司2024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，如在实施权益分派的股权登记日前公司总股本发生变动，公司拟维持分配总额不变，相应调整每股分配比例。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0.50元（含税）。截至2024年12月31日，公司总股本102,234,195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101,515,258股，以此计算合计拟派发现金红利5,075,762.90元（含税），占2024年度实现归属于上市公司股东的净利润的比例为59.84%。

（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12月31日，公司总股本102,234,195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101,515,258股，以此计算合计转增48,727,324股，转增后公司总股本增加至150,961,519股（具体以中国证券登记结算

有限责任公司登记为准）。

公司2024年度利润分配及资本公积金转增股本方案已经公司第四届董事会第四次会议审议通过，尚需公司2024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

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

二、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、主营业务基本情况

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，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。公司在人工智能、数据要素、工业控制、关键信息基础设施保护等领域发挥重要作用。

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、安全防护与管控等产品和服务。

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风险趋于“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”。

“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。

（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，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）一等奖和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。

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测试评估产品、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测试评估、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

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”，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，我国针对网络和数据安全相继出台了《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》等一系列的法律法规，我国网络和数据安全法律架构日趋完善，网络空间安全治理根基持续夯实。

2024 年以来，监管部门持续对现有网络和数据安全政策体系进行完善，扎实推进相关领域立法工作，法律架构日趋完备。《工业领域数据安全能力提升实施方案（2024-2026 年）》《促进和规范数据跨境流动规定》《人工智能安全治理框架》《网络数据安全管理条例》《关于促进数据产业高质量发展的指导意见》等聚焦更加细分领域突出问题，规范行业健康高质量发展的政策条例持续发布，对相关制度规定进行了细化、补充和完善，进一步奠定了我国数字经济高质量发展基石。同时，国家级产业基金、科技创新专项、重点产业园区以及一系列支持网信企业做大做强、优化完善产业生态的政策举措逐步落地实施。

（2）常态化测试评估成为保障 AI“数字健康”的关键

随着以大模型为代表的 AI 等新技术在各行业的广泛落地，数据安全、隐私保护、伦理道德、知识产权等挑战日益显现，安全风险与能力评估的需求也不断攀升。面对日益严峻的安全风险，各国纷纷出台相关政策法规，规范行业健康、有序、高质量发展。

2023 年 8 月，我国《生成式人工智能服务管理暂行办法》正式施行，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；2023 年 10 月，美国发布首个生成式 AI 监管规定，要求大模型产品正式发布前要进行安全评估，上报测试结果；2024 年 3 月，我国《生成式人工智能服务安全基本要求》正式发布，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；2024 年 4 月，世界数字技术院发布的全球大模型安全领域首个国际标准《生成式人工智能应用安全测试标准》，也提出要注重生成内容安全，为生成式人工智能应用的安全测试提供了指导。

可见，全球范围内，生成式人工智能服务的安全建设都是一个复杂且重要的议题。如何能建立起一套多层次的防范机制和评估体系，已经成为保障 AI“数字健康”的关键！

（3）政企用户“实质”安全需求愈发迫切

随着数字经济的高速发展，政企用户在网络和数据安全建设方面面临三大挑战：

①法律法规的密集出台，在实施措施上采取了“处罚”、“强制”等影响安全结果导向的管理方式，处罚力度大幅增加。

②勒索病毒等新型攻击不断涌现，成为政企用户网络和数据安全持续面临的高危安全威胁。

③国际形势风云变化，长期隐密存在的高烈度特种攻击成为新常态，实质性加强网络和数据安全迫在眉睫。

在此情势下，政企客户对网络和数据安全的需求已经由“形式合规”向“实质合规”加强，

各行业领域均积极从业务视角出发，建立以保障业务连续性和高可用性为目标的安全防护和运营体系，积极开展网络和数据安全测试评估，验证防范化解安全风险，以筑牢数字安全和经营安全防线，保障“数字健康”。

（4）网络靶场持续助力各行业安全能力提升

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。通过网络靶场建设，可为国家关键信息基础设施运营单位安全体系建设提供分析、设计、研发、集成、测试、评估、运维等全生命周期保障服务，解决无法在真实环境中对复杂大规模异构网络和用户进行逼真的模拟、测试，以及风险评估等问题，实现各行业网络空间安全能力的整体跃升。

当下我国网络靶场行业正处于快速发展期，国家部委及主管部门持续出台各类政策支撑行业持续、高质量发展。2023 年 1 月，国家能源局综合司印发《2023 年电力安全监管重点任务》，面向全国电力单位，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。2023 年 5 月，《信息安全技术 关键信息基础设施安全保护要求》正式实施，明确提出“应在关键信息基础设施建设、改造、升级等环节，实现网络安全技术措施与关键信息基础设施主体工程同步规划、同步建设、同步使用，并采取测试、评审、攻防演练等多种形式验证。必要时，可建设关键业务的仿真验证环境予以验证。”2024 年 5 月，国家能源局印发实施《电力网络安全事件应急预案》，持续推动国家级电力网络安全靶场建设。

随着国家和社会不断加大对网络靶场的投入及数字经济的快速发展，贵阳启动大数据网络安全靶场建设、鹏城实验室成立、公司网络靶场技术荣获国家科学技术进步奖二等奖和北京市科学技术奖（科学技术进步奖）一等奖，以及“强网杯”“网鼎杯”“护网杯”等国家级重要赛事的成功举办，将持续推动网络靶场行业保持较快发展态势。

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，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。“数字风洞”产品体系荣获中国职工技术协会 2024 年职工技术创

新成果奖特等奖；在中国网络安全产业联盟主办的 2024 年网络安全优秀创新成果大赛中，春秋 AI 大模型测评“数字风洞”平台荣获网络安全创新产品优胜奖；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、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；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，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；参股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；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”，2024 年白皮书以“安全测试评估”为主题，提升人才“发现问题-分析问题-解决问题”的能力，广泛拓宽行业应用基础；组织和支撑超过 750 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”产品体系将持续满足政企用户“实质”安全需求

随着社会经济网络化、数字化、智能化进程的加速推进，政企用户面临的网络与数据安全防护形势愈加严峻，对于以勒索病毒、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，传统的安全防范措施难以有效应对，网络和数据安全行业由“形式合规”向“实质合规”加强趋势得到进一步强化。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）“原生安全”助力 AI 应用安全、高效落地

随着 DeepSeek 等开源技术推动基础模型能力突破，企业级私有化部署成本显著降低，私有化成为众多企业进行模型部署的理想选择。DeepSeek 大模型一体机作为开箱即用的私有化部署方案，在实现快速部署 AI 大模型的同时，能够满足对于公民信息、关键业务数据等数据安全保障的需求，满足企业数据安全及合规需求，且相对更低的部署成本，能够帮助政企用户快速决策、灵活部署、高效应用，市场规模有望快速放量。

2025 年 3 月 3 日，深圳印发《深圳市加快推进人工智能终端产业发展行动计划（2025—2026 年）》，明确提出要抢抓大模型开源化机遇，加快推出开箱即用训推一体机和推理一体机等产品，服务企业和政务领域定制化、轻量化需求。重点围绕智慧金融、智慧医疗、智能办公等场景，提供私有化部署、行业场景定制、高效安全合规的端到端解决方案。同月，泉州市出台《深度求索（DeepSeek）赋能政务提效与产业升级工作方案》，明确以“试点—示范—推广”三阶段推进，重点整合政务云算力资源，支持本地化部署 DeepSeek 大模型及算力一体机。

值得注意的是，用户在完成 AI 私有化部署后，虽然数据不出域，但私有化部署并不意味着安全。2025 年 3 月，国家网络安全通报中心通报，开源跨平台大模型工具 Ollama 默认配置存在未授权访问与模型窃取等安全隐患。鉴于目前 DeepSeek 等大模型的研究部署和应用非常广泛，多数用户使用 Ollama 私有化部署且未修改默认配置，存在数据泄露、算力盗取、服务中断等安全风险，极易引发网络和数据安全事件。因此，私有化部署大模型固然越来越简单便捷，但是这些应用与

生俱来的安全缺陷有可能让使用者和二次开发人员暴露在巨大的网络和数据安全风险之中。

针对上述风险，通过构建 AI 大模型的原生安全能力，将安全融入模型的全生命周期，才是应对安全风险的关键所在。基于这一理念，公司依托在“数字风洞”测试评估、安全攻防以及在 AI 大模型研究等多个领域深厚的技术沉淀和实践积累，以原生安全为核心，发布基础版、专业版和大师版“元方”原生安全大模型一体机和原生安全行业大模型（量身定制）产品及方案，持续为企业提供从私有化部署到垂直场景应用的 AI 智能体建设方案。

（3）新质生产力带来的新型安全需求持续增加

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，以机器人、低空经济、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，随着机器人的广泛应用，机器人在网络安全上，易被黑客攻击致通信中断、指令被恶意篡改，数据层面也存在被窃取、篡改、泄露风险，影响用户权益与运行决策，同时在系统安全上，若发生软件漏洞、非法访问，则会破坏系统，威胁机器人运行及应用安全；低空经济作为一种新兴的经济形态，以无人机、低空飞行器等为核心，涉及到空域管理、通信导航、飞行控制等多个环节，低空飞行器的通信系统若遭受干扰或攻击，可能会导致飞行事故，威胁到地面人员和财产的安全；智能驾驶产业的发展更是对网络安全提出了极高的要求，智能汽车通过车载网络、传感器、通信模块等实现了自动驾驶、车联网等功能，但也面临着黑客攻击、恶意软件入侵等安全威胁，一旦智能驾驶系统被攻击，可能会导致车辆失控、引发交通事故等严重后果，危及乘客和行人的生命安全和财产安全。

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，支撑机器人、低空经济、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，可以为机器人、低空经济、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”。

三、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

	2024年	2023年	本年比上年	2022年

			增减(%)	调整后	调整前
总资产	121,953.02	124,786.84	-2.27	118,010.57	118,010.18
归属于上市公司股东的净资产	102,652.06	106,652.11	-3.75	105,087.00	105,086.61
营业收入	35,632.63	39,586.55	-9.99	33,066.03	33,066.03
归属于上市公司股东的净利润	848.22	3,110.54	-72.73	5,080.64	5,080.31
归属于上市公司股东的扣除非经常性损益的净利润	-205.77	1,103.04	-118.65	3,985.15	3,984.83
经营活动产生的现金流量净额	-4,630.06	-1,855.52	不适用	-1,753.82	-1,753.82
加权平均净资产收益率（%）	0.82	2.94	减少2.12个百分点	8.42	8.41
基本每股收益（元／股）	0.08	0.30	-73.33	0.63	0.93
稀释每股收益（元／股）	0.08	0.30	-73.33	0.63	0.93
研发投入占营业收入的比例（%）	26.01	21.24	增加4.77个百分点	19.11	19.11

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	2,944.73	7,071.37	7,278.02	18,338.51
归属于上市公司股东的净利润	-1,996.60	149.89	-1,311.54	4,006.47
归属于上市公司股东的扣除非经常性损益后的净利润	-2,157.53	-200.31	-1,507.70	3,659.77
经营活动产生的现金流量净额	-4,842.05	-1,947.04	-1,620.04	3,779.07

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

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)	2,960
年度报告披露日前上一月末的普通股股东总数(户)	3,815
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	11,556,077	35,631,237	34.85	35,631,237	无	0	境内自然人
陈俊	5,334,393	16,447,713	16.09	16,447,713	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）	3,841,797	11,907,797	11.65	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	3,245,175	4,597,148	4.50	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）	316,164	2,374,923	2.32	0	无	0	其他
北京启明星辰信息安全技术有限公司	-11,341	2,102,099	2.06	0	无	0	国有法人
交通银行股份有限公司－博时新兴成长混合型证券投资基金	1,004,210	1,160,939	1.14	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）	355,200	1,095,200	1.07	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	-1,044,297	688,460	0.67	0	无	0	其他
北京信安春秋科技合伙企业（有限合伙）	217,383	670,263	0.66	670,263	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 34.85%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 16.09%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

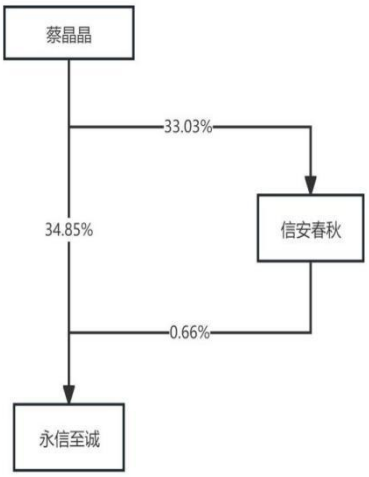
□适用 √不适用

截至报告期末表决权数量前十名股东情况表

□适用 √不适用

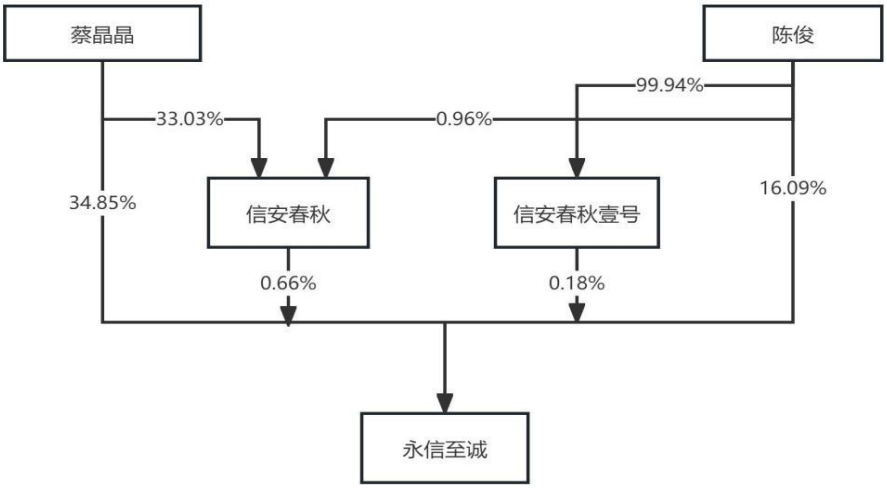
4.2 公司与控股股东之间的产权及控制关系的方框图

√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 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 35,632.63 万元，同比减少 9.99%；实现归属于上市公司股东的净利润 848.22 万元，同比减少 72.73%；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 -205.77 万元，同比减少 118.65%。

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