## 公司简称:亚信安全 亚信安全科技股份有限公司 2023 年年度报告摘要

()900 信息披露

投近有巡过式》 WWI-2020 2 重大风险提示 公司已在报告中详细描述可能存在的相关风险,敬请查阅《2023年年度报告》第三节管理层讨论

公司已在报告中详细描述引能存在的相关风险, 或可查阅(2023 年半度报告)第二节管理层可论与分析"四、风险因素"部分内容。
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 致同会计师事务所(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

21/平巳经公司第二届董事会; 8 是否存在公司治理特殊安排等重要事项 门适用 V不适用 V不适用 第二节 公司基本情况 1 公司简介 公司服要库尔 分配方案已经公司第二届董事会第八次会议和第二届监事会第六次会议审议通过,尚

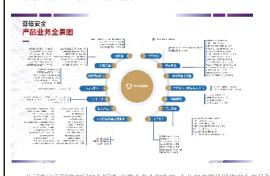
司股票简况 □不适用

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	亚信安全	688225	/				
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	王震	李宝	
办公地址	北京经济技术开发区科谷一街 10 号院 11 号楼 13 层	北京经济技术开发区科谷一街 10 号院 11 号楼 13 层	
电话	010-57550972	010-57550972	
电子信箱	ir@asiainfo-sec.com	ir@asiainfo-sec.com	
<ul><li>4 但生期八司十西川</li></ul>	. 72 YE A		

(一) 主要业务、主要产品或服务情况



公司专注于网络空间安全领域,主营业务为向政府、企业客户提供网络安全产品和服务。客户广泛分布于电信运营商、金融、政府、制造业、能源、医疗、交通等关键信息基础设施行业。公司是中国网络安全软件领域的领距者、作为"懂网、横云"的安全公司、致力于护航产业互联网、成为在56云网时代、守护云、网、边、端的安全智能平台企业。公司提出了"安全定义边界"的发展型。从身份安全为基础,以云网安全和端点安全为重心,以安全中台为枢纽、以威胁情报为支撑、构建"云化、联动、智能"的产品技术战略、颠储企业在56时代的数字化安全运营能力。报告期内、公司主营业务包括网络安全产品、网络安全服务、云网旗取化二大部分。其中网络安全产品包括数字信任及身份安全产品体系、端点安全产品体系、云风边安全产品体系。

安全产品体系、云网边安全产品体系。
1、网络安全产品体系。
1、网络安全产品体系
1、网络安全产品体系
数字信任及身份安全产品体系
数字信任及身份安全产品体系以身份识别与访问控制、数据安全相关的产品为主,为用户提供与
数字身份相关的账号管理,接入认证。权限控制、访问过程审计以及数据安全管控等功能、保障用户以
可信的数字身份接入网络或系统。在授权的范围内操作系统、访问和使用资源、同时能够对用户访问
记录和使用数据情况进行监控分析,从人口和出口两个方向为政企用户的系统和数据提供安全防护,
为用户打造可信任的数字化应用体系。
产品主要解决客户在数字身份及数据资产管理的网络安全建设方面需求、如确保具备权限的用
户才能访问网络、签录系统、访问资源和执行业务操作;对用户访问系统和数据的记录进行审计分析,
防止敏感数据泄露等。该体系产品主要应用于电信运营商、政府、金融、能源等中大型企业。
(2)端点安全产品体系

(2)端点安全产品体系 端点安全产品体系以终端安全、云安全、高级威胁治理和边界安全产品为主,通过在不同的位置

電点安全产品体系以終電安全、云安全、高级威财治理和以界安全产品为主,通过在不同时宜直 部署该体系产品,可以为用户的 IT系统、资源,除继设备提供多方面的安全防护;通过在内网和外网 的边界处部署高级威胁治理和边界安全产品,可以对进出组织的网络流量进行深度识别和分析,阻断 带有一般恶意程序,和高级威胁的流量进入内网;通过在终端设备上部署产品,可以有效发现和查杀人 侵终端设备的恶意程序,保障终端设备的正常运转;通过在云主机、云计算服务器等介质上部署产品, 可以增强云端资源抵调恶意程序攻击的能力。 该产品主要解决客户在终端、网络节点和云上的网络安全建设方面需求,该体系产品广泛应用于 政府,但信运营商、金融、能源、医疗、制造业等各行业客户。 (3)云网边安全产品体系

(3)云网边安全产品体系主要聚焦在5G技术发展体系和云网融合的网络架构演进趋势下,利用威胁情极及全产品体系主要聚焦在5G技术发展体系和云网融合的网络架构演进趋势下,利用威胁情极及大数据技术,提供智能化的态势感知分析,安全事件仍环管理及综合性网络安全管理能力。云网边安全产品体系着重于从用户进行安全运营及网络管理的全局视射出发,解决网络空间资产及网络设备管理、安全事件及威胁情报的关联分析及决策响应、安全管理及运营自动化、基础网络运维管理等问题。综合采集处理多测数据、实现对安全对象的主动管理、安全空间内外部威胁与行为的实时 监测,威胁事件智能分析和通报处置,联合威胁情报狩猎追踪,精密编排自动响应准确检测及制止威

那次。 该产品主要解决客户在安全管理及网络管理的建设方面需求,如通过建设态势感知平台,联动其 他安全设备能力,实现客户全天候,全方位的网络威胁识别,预警和处理能力;通过建设域名解析及网 络准人系统,为运营者提供越名解析,安全的护,数据分析,安全监管等网络管理能力。该体系产品主 要应用于电信运营商,政府,金融,能源,制造业等中大型客户。

弱点分析、风险评估和安全培训服务等多项业务,通过这些服务,能够有效提高客户的安全意识,增强

客户抵御网络安全威胁的能力。 网络安全服务主要解决客户在网络安全服务方面的需求,主要应用于电信运营商、金融、能源、政

府等中大型客户。该体系产品的主要交付形式为根据客户需求,通过专家团队及能力中心为客户提供 网络安全咨询等一系列服务。

3.云网虚拟化 为满足项有客户提出的云化转型及安全合规的需求、公司拓展与云基础架构领导厂商的业务合作,共同推进运营商及行业客户云网基础设施和云化管理运维方案的落地,以及和公司现有安全产品服务结合的探索。用户通过将该产品安装在通用的物理服务器上,将计算、存储、网络等功能与物理服务器进行解解,虚拟成可灵活调用的云端计算,存储和调信资源,增起其17条线的灵活性和可拓展性。云网虚拟化产品主要解决客户在云计算虚拟化基础设施建设方面需求。

公司盈利主要来源于网络安全产品的销售,以及为客户提供专业的网络安全解决方案和安全服公司采取直销与渠道代理销售相结合的方式,对于电信运营商、金融、能源等领域的头部大型客 公司一般采用直销的方式,安排专门的销售及业务团队为其进行服务。对于其他客户,公司一般采

公元宗则條以、公司宗帥的主要内容为两大类;(1)服务器、U盘、产品包装物及第三方软硬件等产品;(2)技术服务。公司制定了(采购管理制度)(供应商管理制度)及(招标管理制度)规范采购行为。需求部门提出采购申请后,由使必整管理集程公司市能采购的,所有货物进行营业的市场调研、明确不同供应商可能供应的材料的质量、价格及供应商的供货能力、制定采购策略并为 公司提供决策依据。负责建立供应商管理档案,定期对供应商的货物品质、交货期限、价格、服务、信誉等进行分析,为公司采购优选供应商。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指定采购。

司的研发遵循统一的流程架构,同时对于网络安全产品和网络安全解决方案的不同特点和要

公司的研发連確統一的流程架构,同时对于网络安全产品和网络安全解决万案的不同特点和要求实行等是化的管理方式。 (1)统一流程架构 公司研发流程主要分为需求阶段、设计阶段、开发阶段、测试阶段及交付阶段。 1)需求阶段、公司的市场营销团队和售前团队主动调研客户的痛点和需求、作为设计产品和解决 方案的基础。同时基于公司管理层与研发团队对于未来网络安全行业前沿技术发展的调研、理解与预 测量44年24年的《证件》等

2)设计阶段:基于前沿的网络安全技术与发展趋势,并结合客户和市场的需求,由研发团队进行

需求与技术整合、完成规划方案,架构师根据规划方案进行架构设计。 3)开发阶段。由各研发团队相互配合、根据设计方案进行架构设计。 整体交互、原型、视觉、页面效果设计、优化、开发工作、确保产品方案的可用性、易用性及美观性。 4)测试阶段:测试和了在产品方案开发完成后、对产品进行测试、保障产品方案的安全性相质量。

5)交付阶段:公司根据产品方案的实施难易程度,进行发货或派遣人员至客户现场实施安装适配

(2)网络安全产品 公司在产品开发过程中,广泛采用持续集成,自动化测试、敏捷开发与瀑布开发相结合的方式,同时在部分产品开发中积极推进 DevOps 实践,以有效地提升研发效率,缩短产品的发布周期。公司遵循产品质量和安全是不能逾越的红线原则,对于产品研发有着一套严格的过程管理和质量控制机制,所有产品在发布前,需会过产品经理。安全测试团队。第二方模块评审委员会。Q和 团队和技术支持团队的层层把关,只有符合发布标准的产品才会被推向市场,以保障产品交付版本的质量和安全性。

的层层代大,只有行音及中称信的"临力会数值向印动。以称吗?" "高文勺成本的则面课件安全性。 (3) 网络安全解决方案。 公司采用"产品研发以技术为驱动,负责统一框架。核心功能、标准化方案等的研发工作;系统开发以 行业为驱动,负责行业场景方案设计,接口开发,方案交付等工作;专业服务以客户为驱动,负责客户 分率为驱动,负责行业场景方案设计,接口开发,方案交付等工作;专业服务以客户为驱动,负责客户 关系,项目管理、项目实施、项目节点测试以及客户需求和反馈的收集。三个团队、紧密配合,有力地保 障了公司提供网络安全解决方案的过程组织能力、研发能力和质量管理能力。

公司的产品生产主要包括纯软件模式和软件灌装模式,纯软件模式由公司根据合同约定向客户交付软件;软件灌装模式是由硬件设备供应商将软件产品灌装到外购的硬件设备(工控机、服务器等),再交付给客户。硬件设备作为安全软件的硬件载体,方便客户部署和应用,使客户无需准备软件

(2)安全服务模式

(2)安全服务模式 公司根据客户的实际需求,为客户提供的技术、咨询及安全保障等服务,包括咨询与规划、评估与测试、分析与响应,情报与运营等。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的实施工作。 5.盈利模式 公司的盈利模式分为三类,具体如下; (1)销售产品:主要系公司基于用户采购需求,向其销售产品,以产品销售方式与用户签署购销合 同,产品的增值部分职分公司的盈利来源。 (2)提供解决方案:主要系针对各户需求,公司综合自身各个产品线和服务能力,为客户提供一揽 子解决方案。公司盈利来源主要为项目收入与成本费用之间的差额。 (3)提供网络安全服务:根据用户需求,提供网络安全相关服务。公司盈利来源为网络安全服务收 人和成人员应本及项目申取后的差额。 入扣减人员成本及项目费用后的差额。 (三) 所处行业情况

(三) 所处行业情况
1. 行业的发展阶段,基本特点,主要技术门艦
(1) 网络安全行业驱动力加速转向业务刚需,中国网络安全市场增速继续领跑全球。
在地缘政治冲突升级、供应链挑战加剧等多重冲击下,作为社会发展的基础性和战略性科技领域、网络安全产业发展面临的国际涉替依然复杂严峻、网络安全成为大国角力和科技竞争主办方向的趋势更加明显。与此同时,随着社会各领域向数字化、校对化、智能化的加速发展,千行百业逐渐加大对信息化建设与数字化转型的投入已成为共识,组织的信息系统及交互环境日趋多变复杂。业务场景发生较大变化、伴随的网络安全风险日趋严峻、安全能力建设从台规型转变为符合业务发展需要,抵货工程中不少。由地位的周绝对方值。 网络安全企业积极应对市场需求,技术快速进代中和创新,从云安全到 加真实安全威胁的刚需型方向。网络安全企业积极应对市场需求,技术快速迭代和创新,从云安全到数据安全到人工智能的应用,前沿技术为网络安全领域注入了新的活力,从长期看网络安全产业仍处

丁和公叶均及限周别。 从全球网络安全市场来看,随着数字化、智能化的快速渗透,网络安全需求持续增长。根据 IDC 《全球网络安全支出指南》最新预测, 2022 年至 2027 年,全球网络安全 IT 总投资五年复合增长率 (CAGR)为 11.7%;中国网络安全市场规模五年复合增长率为 13.5%,高于全球平均水平。从国内网络 安全市场来看。2023年中国网络安全市场面临宏观经济波动与产业生态调整的双重挑战,行业需求增速短期内继续放缓。但中国网络安全市场近年来基于数字化转型、业务内生安全的需求日趋强烈,对 是成例/948-50.03念。但中国/947女王中/920上不感了 84-71(74至,至为/9王女王的馬尔口曼班然, 70 定制化釋此方案能力, 内生安全能力及与数字业务的探读协同等方面提出了更高要求,需求空间正在逐渐释放,未来将引导网络安全产业的长期增长趋势。中国网络安全市场增长的核心逻辑并没有变化,随着下游行业需求日新复苏,中国网络安全市场仍将保持快速增长。 (2)网络安全法治体系日臻完善,新技术加速迭代升级,持续扩张行业发展机遇。 2023年中国网络安全法律法规,政策发布呈现高密度特征,引起行业高度关注的政策达 50 余项。

数据安全领域。个人信息保护和数据跨境安全成为关注的热点。分别有7项。6项。6项的策围终这些 数据安全领域。个人信息保护和数据跨壤安全成为关注的热点。分别有7项.6项。6项版策围绕这些
汉题展开、数字中国和行业安全类别的政策都突出了数据安全的重要性、反映了当前推动数据资源转
化为经济新优势的大背原下。数据安全正在从传统网络安全中逐渐独立出来的趋势。同时、传统网络
安全领域的重要性愈加凸显。以网络安全为核心的政策数量达到12项,而涉及行业安全的政策更是
高达13项、位居首位。这要拥将网络安全与业务融合,并通过安全促进发展的现金已经获得了更广泛
的认可。此外、密码安全和人工智能成为2023年网络安全政策的两个重点领域。数字中国领域也推出
了多项重要政策、均滤盖了网络数据安全保管体系建设的内容、强调建立可信赖的数字安全防线。近
年来、随着关键信息基础设施安全保护、网络安全审查、数据安全管理、个人信息保护等领域的一系列
法律法规相继出合。不仅表明国家对网络安全行业监管呈现检查、趋细的态势、也为相关企业提供了 明确的指导和规范,行业健康发展得以有据可依、有法可循,有力地保障了网络安全行业的持续繁荣

<sup>录及 展。</sup> 全球各国加大对新兴技术的投研力度,零信任、生成式人工智能、隐私计算等网络安全新技术的 与创新,这为网络安全行业带来新的发展机遇。同时,随着"一带一路"倡议的深人推进,这一重要经济 框架为相关国家的网络安全意识提升和网络安全市场拓展提供了契机,有助于推动我国网络安全行 业的进一步发展壮大,中国网络安全公司古兹加快布局全球化业务,抢抓出海机遇 (3)大国博弈加剧网络空间竞争烈度,产业供应链风险提升,网络攻击技术快速演进升级,网络安

全挑战复杂多变。 2022 年以来,国家间网络攻防、供应链攻击、勒索软件、数据泄露、黑客攻击等安全事件层出不穷,

2022年以来,国家间网络攻防、供应链攻击、勒索软件、数插油露、黑客攻击等安全事件层出不穷, 危害性更强、大国竞争趋势更加明显。急加地缘政治中平等负面影响,网络空间安全成为大国对抗的 重要战场。2023年、80%以上的国家颁布了网络安全战略或法规,140多个国家设立了网络安全事务协 调机构、110多个国家出台个人数据与隐私保护法规。60%以上的国家通过外资审查、市场许可证等方 式管理网络安全产品准人、对跨国企业的合规运营产生一定的影响。同时,供应链攻击已成为主要的 络攻击手段、供应链条较长的产业将面临更加严峻的供应链安全风险。全球安全态势的不确定性将对 中国网络空间安全防护、供应链的安全稳定提出更大的挑战。 随着新兴技术的迅猛发展和广泛应用,新型攻击者也层出不穷,生成式人工智能新威胁崭露头

随着新兴技术的迅猛发展和广泛应用,新型攻击者也层出不穷,生成式人工智能新威胁崭露头 用、勤索软件仍为主要攻击方式,网络攻击的重点行业主要集中在政府、医疗、通讯、金融、能源、汽车 等重要领域。这使得网络安全形势更加复杂和严峻。新技术、新应用的涌现带来愈来愈多的网络安全 风险积据战。需要政府和企业不断更新安全理念,形成合力、资车网络安全的线。 综上野站、我国网络安全产业发展面临的形势依然复杂严峻、战有政策法规的细化深入、数字经 济赋能、技术迭代创新等发展机遇、也面临大国博弈激烈、网络攻击复杂多元、行业需求阶段性趋弱等 诸多挑战、网络安全行业将在高度不确定性的环境中探索前行。 2. 公司所处的行业地位分析及其变化情况。 公司的核心产品与技术以及公司整体市场影响力获得了国内外市场研究机构的广泛认可,在数 学信任与身份安全软件。将谐安全被引导响应(NDR)、云安全、数据安全、安全服务等 领域均位于市场领先地位、奠定了亚信安全在中国网络安全软件市场的领先地位。 目前,在第三方研究机构最近时期的评处,

(1)身份安全、数字身份治理与管理代表厂商 2023年1月在安全年(数字身份治理和管理(IGA)应用实践指南)、公司荣获代表厂商; (2)身份安全统产与价管理》,市场价额位度第一 2023年7月在IDC(中国统?身份管理平台市场份额,2022;安全建设身份先行)、公司的身份安全

(司) 的伊姆山尼岛一: (3) 身份安全: 市场份额排名第二 2023年 ID 月在 IDC(2023 年上半年中国 IT 安全软件市场跟踪报告)中,公司的身份和访问管理 品市场份额排名第二: (4) 终端安全: 市场份额排名第二 2023年 ID 月在 IDC(2023年上半年中国 IT 安全软件市场跟踪报告》中,公司的终端安全产品连

续多年位居第二; (5)云工作负载安全:私有云市场份额位居第三

2023年7月在IDC《中国私有云云工作负载安全市场份额,2022》中,公司的云主机安全产品市场 份额位居第三; (6)云工作负载安全:公有云市场份额位居第五

2023年7月在IDC《中国公有云云工作负载安全市场份额,2022》中,公司的云主机安全产品市场 位居第五: (7)网络威胁检测与响应:市场份额排名第五 2023年8月在IDC《中国:给威胁检测与响应市场份额,2022》中,公司的NDR产品市场份额排名

1; (8)中国网络安全软件:市场份额排名第三 2023 年 8 月在 IDC(中国?络安全软件市场份额,2022)中,公司七大安全软件产品市场份额排名

(9)杰势感知:位居领导者象限 2023年7月在IDC《IDC MarketScape:中国态势感知解决方案市场 2023年厂商评估》中,公司的

(10)《中国王:汉本八及》同 2023 年 7月在 IDC(IDC Technology Assessment:中国零信任网络访问解决方案技术评估 , 2023》 公司的零信任产品 SDP 人围技术代表厂商; (11)零信年 代表性厂商 公司的零信由:"命 5DF (ALBIXANIA PRO 1994) (11)零信任:代表性厂商 2023年9月在 Gartner 《Market Guide for Zero Trust Network Access, China》中,公司的零信任

产品人围代表性厂商; (12)云工作负载、云安全资源池:模范厂商 2023年10月在Gartner《Hype Cycle for Security in China, 2023》中,公司的云安全资源池、云工

2023年10月在Gartner(Hype Cycle for Security in China, 2023)中、公司的云安全资源池、云工作负载、总选技术领域的 Sample Vendor(模范厂商),再次证明技术创新与市场实践能力; (13)防勒索治理:防勒索领域代表厂商,2023年10月在1DC(中国热点威胁安全检测与防护解决方案。2023)中,亚信安全「方舟」勒索治理体系解决方案获评防动等领域代表厂商,TustOne 对攻击面管理等新兴技术的创新应用,进一步推动勒索治理理念革新,助力勘索治理能力再升级; (14)云安全生态建设代表厂商。2023年1月存1DC(中国云安全生态市场洞察。2023)中、公司凭借完整的云安全能力、云安全生态的持续建设、以产品+服务的发展模式,与云厂商一起推动云安全的升级发展,荣获云安全生态建设代表厂商。

代表「商; (15)终端安全,新一代终端安全代表「商 2023年12月在IDC(中国新一代终端安全市场洞察,2023——安全防御的"最前线"》中,正式定 义了"中国新一代终端安全 的技术概念,技术演述和技术特点,公司的终端安全产品 TrustOne 凭借领 先的技术能力,成为该领域优表「商、其优秀行业实践成为唯一人选案例; (16)数据安全,技术深耕型企业

、101%355至:347心本对至近型 2023年12月在CSA(《数据安全平台神兽企业报告(2023版)》中,公司的数据安全平台产品凭借 核心竞争力,技术研发实力强,产品成熟度高,并且有良好的市场占有率,荣获"技术深耕型企业"; (17)攻击面管理:技术代表厂商

(17)攻击面管理:技术代表厂商 2023年12月在安全牛《攻击面管理技术应用指南》中,公司的攻击面管理产品人围技术代表厂 (18)安全运营:电信行业代表厂商 2023年11月在数说安全《2023年中国网络安全运营市场研究报告》中,公司的安全运营人围

2013年11月在數说安全(2023年中国网络安全运营市场研究报告》中,公司的安全运营人围2018-2022电信户业TOP10安全运营服务师。(19)2023年12月,在安全半(中国网络安全企业100强)中,公司连续多年凭借综合能力人围综合能力十强,以及技术创新十强,行业应用十强、信创能力十强;(20)新一代终端安全 TrustOne :CAS 安全餐石奖 2023年12月,公司的新一代终端安全产品 TrustOne 凭借前瞻性理念和突出技术能力,引领中国新一代终端安全、荣获 CSA 2023 最高荣誉奖项——安全磐石奖 3.报告期内新技术、新产业、新业宏、新模式的发展情况和未来发展趋势(1)安全大模型的应用与大模型自身的安全正在深刻影响着网络安全行业从安全防御视角来看,AI 大模型带来的安全产品形态的改变,产品能力与响应效率的提升将带来竞争格局的改善。海外国际大厂 AI +安全已初步形成生产力,以 Microsoft Security Copilot 和 Crowdstrike Charlotte AI 为代表,生成式 AI 技术广泛应用于安全产品与平台中,改善产品形态和功能、聚焦的功能主要在安全监控、成财检测、资产风险、创建报告等,能够辅助安全管理人员提升安全运营的自动化水平。国内众多网络安全企业推出安全大模型,尚处于探索与测试阶段,应用方向领域相对有限,尚未真正形成生产力。

运营的自动化水平。国内众多网络安全企业推出安全大模型,尚处于探索与测试阶段,应用方向领域相对有限,尚未真正形战生产力。 AI 自身的安全也成为业内关注的热点。网络攻击的方式和手段,在人工智能技术的推动下也在不断演变,呈现出分布式,智能化和自动化的特点,同时,人工智能训练和应用过程中,会遇到数据非法获取,数据滥用,算法偏见与歧视以及敏感数据泄露等安全问题,进而带来行业总需求的提升,这将为网络安全厂商带来新的市场机遇。
(2)数据安全继续保持高热度,数据共享流通的安全成为焦点
2022年12月,中共中央、国务院发布了构建数据基础制度体系"数据二十条",通过数据基础建设大力推进数据要素发展。随后数据要来发展进程明型加速。数据安全相关法律,法规和标准,规范也密集出台,针对数据安全的专项检查,监管和处罚明显增加。2023年10月25日,国家数据局正式挂牌,主要职责是负责协调推进数据基础制度建设,统筹数据资源整合共享和开发利用,统筹推进数字中显 教字经济、教学社会规划取错设备。至此、图家在数据经验的原规的设计与基本成型。2023年

王安联切定以即的调性比较熔整轴前限建设,统券效納函效器管产环平机厂农利用,统筹推出级子干 國教学经济 教学社会规划和键设等。至此、国家在数据领达行民规划的设计已经基本成建。2023年 是数据聚素发展和数据安全的主要目标是完成固层规划设计、2024年将全面进入落地行动阶段。在数据聚素加速形成生享的新形势下,隐私计算正成为支撑数据服素流通的板心技术基础设施、该领域的技术如联邦学习、多方安全计算。可信执行环境等,在确保数据不泄漏。限定数据处理目的方面具有原生的优势。未来数据流通交易。数据安全保护等市场将版起新一轮扶漏。因此,如何实现数据的共享交易流通,如何建立起名行业的跨域数据安全保护等市场将版起新一轮扶漏。因此,如何实现数据的共享交易流通,如何建立起名行业的跨域数据安全保护特制制以及如何以持续运营的思路开展数据 的共享交易流通、如何建立起各行! 安全治理工作等将成为未来的重点

面具有原生的优势。未来数据流通交易、数据安全保护等市场将板起影一轮热潮。因此、如何实规数据安全冷理工作等将成为未来的重点。
(3) 云原生安全发展迅速,注重云环境安全可信随着工作等将成为未来的重点。
(3) 云原生安全发展迅速,注重云环境安全可信随着工作等将成为未来的重点。
(3) 云原生安全发展迅速,注重云环境安全可信随着工作算水件每到更广泛的采用,越来越多的企业根据不同业务系统的特性选择多云或混合云的模式进行部署,更多敏感数据会存储到云端,但大部分组织缺乏云安全实时评估能力,云数据泄露事件高发。AP 安全成为云计算应用特型工烧建。同时,云原生块大的敏捷性。可观察性,性结效率和可移植性等技术优势,以及成本优势促使数学化模型中的企业积极拥抱云原生。云原生安全技术将持续发展并成为云安全领域的重要趋势,容器安全和微隔离安全等云原生安全技术将得到更广泛的应用部署。AI 和机器学习技术在云安全领域的后用更加深入,实现更高效的威胁检测与响应机制,云安全技术向自动化方向演进,全面的云安全的形方索将成为主流。因此,云安全仿将是未来企业安全与风险管理支出中增长最快的领域之一。
(4)终端安全轻强化、一体化、智能化助力降本增效数字化等型带来安全边界泛化、终端面临钓鱼攻击,无文件恶意软件、勒索软件、零日攻击,加密数持等众全经强化、一体化、智能化助力降本增效数字化转型带来安全边界泛化、终端面临钓鱼攻击,无文件恶意软件、勒索软件、零日攻击,加密数许等企会全球战,参加级各个经常安全处外种类多、管理难度加大、黑产积极利用 AI 技术提高供给效率,这对终端安全的护技术提出更高要求。因此,新一代终端安全的登量化、一体化、智能化发展,通过融合指数多等设计,然后任果取村转流通进根据中国信通院《2023 年零信任发展研究报告》、零信任能力涵盖六大领域、数字身份是基础组件、是核心、联合网络水坡安全的产生要解决用户身份不统一以及梁构中所有对象数字身份缺失,不合法等问题。并对身份基础较及不是全级大量、的国和工作分量全的交全的交全的关键控制面,因此,LAA 在组织安全中的作用越来越大,身份安全优先建设、由被动识明由过效多量的多级的发生,更同的网络攻防对抗成为必要的战争手段之一,且地致政治中安的聚场全势被发生成为,APT的护带派、作为一种计对转度目标的复杂、隐藏和特别接近,由于对防路等。从2022 年的成岛战争到 2023 年的巴以战争,国家间的网络攻防对抗成为必要的战争。是大战的发生,由被政力出于最后的绝互外无动。从市场对场接近的正常高的线级发出于更多,高级特殊性的重点的不是不是不是一种的影响下、网络见用国

温酮%。 该領域要求网络安全厂商具各全网安全大数据。威胁情报、攻防知识库以及具备实战化攻防能力 的安全专家等,能够进行零日漏洞的挖掘、储备、漏洞利用程序的研究、分析等,帮助客户建立完备的 响应机制和预察。204亿险频率的扩方家及专业化安全服务支撑。

响应机制和预案。立体化绘测和的护方案及专业化安全服务支撑。
(7)安全建设的平台化、集约化特征进一步凸显
随着连接数量的增加以及 Saa3 和云应用的普及,组织机构面对的攻击面在不断扩大,因此需要
随着连接数量的增加以及 Saa3 和云应用的普及,组织机构面对的攻击面在不断扩大,因此需要
提高可见性和打造中心化平台,持续地感测多类威胁与暴露面情况。组织机构在连续多年的安全建设
对海量的告警及处理高级威胁事件,因此推进安全供应商的整合,安全产品的融合平台化势在必行,原来碎片化的安全能力开始向集纷化、整合化、平台化转炮。安全产品的融合平台化势在必行,核测与响应、智运维等优势能力将极大地提高客户的安全能力,通过平台的搭建、标复散、碎片的安全能
力最小化组件化集成于平台之中,更好地匹配业务逻辑和特性,真正实现安全能力整合的要求。
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 市种:人民币

	2023年	2022年	本年比上年 增减(%)	2021年
总资产	3,400,977,486.04	3,682,656,570.16	-7.65	2,489,526,807.56
归属于上市公司股东的净 资产	2,117,938,483.39	2,647,146,253.85	-19.99	1,458,075,252.77
营业收入	1,608,088,384.17	1,720,951,997.61	-6.56	1,667,467,958.09
扣除与主营业务无关的业 务收人和不具备商业实质 的收入后的营业收入	1,607,032,330.10	1,720,457,133.33	-6.59	1,667,083,818.17
归属于上市公司股东的净 利润	-291,075,848.53	98,483,055.93	-395.56	178,685,242.30
归属于上市公司股东的扣 除非经常性损益的净利润	-324,941,753.06	15,774,329.48	-2,159.94	94,995,540.59
经营活动产生的现金流量 净额	-379,335,701.16	-260,712,946.69	不适用	143,648,403.06
加权平均净资产收益率(%)	-12.03	3.88	减少 15.91 个百分点	13.29
基本每股收益(元/股)	-0.7302	0.2483	-394.08	0.4963
稀释每股收益(元/股)	-	-	-	-
研发投入占营业收入的比例(%)			增加 9.04 个百分点	

	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	236,212,569.11	327,012,162.53	428,631,503.98	616,232,148.55
归属于上市公司股东的净利润	-94,897,763.93	-76,456,114.71	-39,871,689.60	-79,850,280.29
归属于上市公司股东的扣除非经常 性损益后的净利润	-112,748,669.93	-79,335,952.27	-51,408,861.49	-81,448,269.37
经营活动产生的现金流量净额	-304,829,575.00	-91,592,802.23	-212,760,038.12	229,846,714.19
季度数据与已披露定期报	2告数据差异说5	A		

√不适用 4 股东情况

截至报告期末普通股股东总数(户)

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

年度报告披露日前上一月末的普通股股东总数(户)					7,793					
截至报告期末表决权恢复的优先股股东总数(户)										
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)							
截至报告期末持有特别表决核	又股份的股东总	数(户)								
年度报告披露日前上一月末	寺有特别表决权	【股份的股东总数	次(户)							
前十名股东持股情况										
股东名称	报告期内增	期末持股数	11.00		持有有限售		质押、标记 况	巴或冻结情	股东	
(全称)	減	量	比例	(%)	条件股份数量		股份状态	数量	性质	
亚信信远(南京)企业管理有 限公司		80,948,488	20.24	ı	80,948,488		无	0	境内非国 有法人	
南京亚信融信企业管理中心 (有限合伙)		62,013,649	15.50	)	62,013,649		无	0	其他	
天津亚信信合经济信息咨询 有限公司		30,656,621	7.66		30,656,621		无	0	境内非国 有法人	
先进制造产业投资基金 (有限合伙)		19,328,859	4.83				无	0	其他	
南京安職企业管理合伙企业 (有限合伙)	-206,803	11,259,494	2.81				无	0	其他	
北京亚信融创咨询中心 (有限合伙)		11,073,117	2.77		11,073,117		无	0	其他	
广州亚信信安投资中心 (有 限合伙)	-6,611,614	10,301,138	2.58				无	0	其他	
广州亚信铭安投资中心 (有 限合伙)	-157,564	10,159,154	2.54				无	0	其他	
中国互联网投资基金管理有 限公司-中国互联网投资基 金(有限合伙)		10,147,655	2.54				无	0	其他	
南京安宸企业管理合伙企业 (有限合伙)	-2,074,434	9,380,250	2.54				无	0	其他	
上述股东关联关系或一致行						、亚信铭安 为一致行动		人均为公司	司董事长何	
表决权恢复的优先股股东及持股数量的说明 /										

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

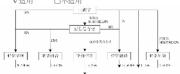
羊	单位:股								
序号	股东名称	持股数量		表决权数量	表决权比例	报告期内表决	表决权受到限		
P. S	双水石桥	普通股	特别表决 权股份	农伏权奴里	20.00.00.00	权增减	制的情况		
1	亚信信远(南京)企业管理有限 公司	80,948,488		80,948,488	20.24%		/		
2	南京亚信融信企业管理中心 (有限合伙)	62,013,649		62,013,649	15.50%		/		
3	天津亚信信合经济信息咨询有 限公司	30,656,621		30,656,621	7.66%		/		
4	先进制造产业投资基金 (有限 合伙)	19,328,859		19,328,859	4.83%		/		
5	南京安融企业管理合伙企业 (有限合伙)	11,259,494		11,259,494	2.81%	-206,803	/		
6	北京亚信融创咨询中心 (有限 合伙)	11,073,117		11,073,117	2.77%		/		
7	广州亚信信安投资中心 (有限 合伙)	10,301,138		10,301,138	2.58%	-6,611,614	/		
8	广州亚信铭安投资中心 (有限 合伙)	10,159,154		10,159,154	2.54%	-157,564	/		
9	中国互联网投资基金管理有限 公司-中国互联网投资基金(有 限合伙)	10,147,655		10,147,655	2.54%		/		
10	南京安宸企业管理合伙企业 (有限合伙)	9,380,250		9,380,250	2.35%	-2,074,434	/		
合计	/	255,268,425		255,268,425	/	/	/		

4.2 公司与控股股东之间的产权及控制关系的方框图 □不适用

亚信信远 (南京) 企业管理有限公司 20.2366%

业信安全科技股份有限公司

4.3 公司与实际控制人之间的产权及控制关系的方框图



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

√不适用 □适用 √不遠 第三节 重要事项

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

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16.08 亿元、较上年同期减少6.56%。整体毛利率略有下降,从52.79%降至47.82%。公司销售渠道体系建设趋于完善、销售费用较上年同期降低0.34%。同时持续加大研发投入,研发费用较上年同期增加38.54%。报告期内国质于母公司所有者的争利润-29.107.58 万元、较上年同期下降395.56%;归属于母公司所有者的补利海-32.494.18 万元,较上年同期减少2,159.94%。 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。

## 亚信安全科技股份有限公司 关于 2024 年度日常关联交易预计的公告 本公司董事会及董事会全体成员保证公告内容不存在虚假记载、误导性陈述或者重大遗漏,并对其内容的真实性、准确性和完整性依法承担法律责任。

★ 日常关联交易对上市公司的影响:本次关联交易属于公司日常性关联交易,是公司正常生产 联股东利益的情形

日堂羊群交易其木情况 一)日常关联交易履行的审议程序 (1) 由予切水 20個 109甲以程即7 亚信安全科技股份有限公司(以下简称"公司")于 2024 年 4 月 26 日召开了第二届董事会第八次 会议和第二届监事会第六次会议,审议通过了(关于 2023 年度日常关联交易执行情况及 2024 年度日 常关联交易预计的议案),本次日常关联交易预计金额合计为人民币 13,600 万元。关联董事陆光明,吴

强, 黄海波, 刘东红同避表决, 出席会议的非关联董事一致同意该议案, 审议程序符合相关法律法规的 规定。本次日常关联交易额度的确认及预计事项尚需提交公司 2023 年年度股东大会审议,关联股东 监事会认为:公司与关联方的关联交易遵循公允、公平、公正的原则进行,对公司未来的财务状况

以及经营成果有积极而长远的影响。没有损害公司及其他中小股东的利益,上述关联交易对公司独立性没有影响,公司的主营业务不会因此类交易而对关联方形成依赖。 公司于 2024年4月15日召开第二届董事会独立董事 2024年第四次专门会议,审议通过了《关 公司,2024年9月13日台开第二曲里事至無公里事 2024年時代《专门宏议、审议通过》(《专 于 2023年度日常美联交易执行情况及 2024年度日常关联交易预计的议案),独立董事认为:公司 关联方签署协议并进行日常交易具有合理性与必要性,相关交易具有真实背景。日常关联交易定价政 策和定价依据遵照公开、公平、公正的原则,双方交易价格按照市场价格结算,不会对公司及公司财务 状况、经营成果产生不利影响,不存在损害公司及全体股东特别是中小股东利益的行为

《从几点音级录》 三个个原本则、个件任项库之间及主体放弃行列定于广政来利益的引力,公司主旨显示 多不会因上述交易而对关联方形成依赖,没有影响公司的独立性。全体独立董事一致同意 2024 年度 日常关联交易预计,并同意将该议案提交公司第二届董事会第八次会议。审议通过了《关于<2023 年 度可常关联交易执行情况及 2024 年度日常关联交易预计。的预验。董事会审计委员会认为,公司及 子公司 2024 年度日常关联交易预计事项均按照公开、公平、公正的原则进行,为正常生产经营所需。 符合公司日常业务发展的需要,关联交易价格定价合理公允、程序合规,没有损害公司和其他股东尤 甘县山小朋生的和经

股东的利益。 )2024年度日常关联交易预计金额及类别

关联交易 类别	关联方集团	本年預计金額	占 2023 年度 同类业务比 例(%)	本年初至 2024 年3月末与关联 方累计已发生的 交易金额	2023 年度实际发生额	占 2023 年 度 同 类 业 务比例(%)	本额 5 年 3 年 3 年 5 年 5 年 5 年 5 年 5 年 5 年 5 年
	亚信科技控股有限公司及 其附属企业	5,000.00	3.1086	14.36	615.76	0.3828	
	亚信创新技术(南京)有限 公司	1,000.00	0.6217	0.34	1.36	0.0008	
	宁夏西云算力科技有限公司	600.00	0.3730	-	-	0.0000	
关联方销	上海富数科技有限公司	500.00	0.3109	-	-	0.0000	
售	恒安嘉新(北京)科技股份 有限公司	200.00	0.1243	-	-	0.0000	
	北京深演智能科技股份有限公司	100.00	0.0622	-	20.75	0.0129	
	北京天润融通科技股份有限公司	100.00	0.0622	1.41	2.58	0.0016	
	北京中科视云科技有限公司	50.00	0.0311	-	-	0.0000	根据公司并
	亚信科技控股有限公司及 其附属企业	2,500.00	5.1224	8.55	175.37	0.3593	按照实验的提供的证据的证据的证据的证据的证据的证据的证据的证据的证据的证据的证据的证据的证据的
	亚信创新技术(南京)有限 公司	1,000.00	2.0489	-	888.30	1.8201	
	宁夏西云算力科技有限公司	900.00	1.8440	1.00	-	0.0000	
关联方采	上海富数科技有限公司	600.00	1.2294	-	109.27	0.2239	
购	恒安嘉新(北京)科技股份 公司	500.00	1.0245	-	159.76	0.3273	
	北京信书科技发展有限公司	250.00	0.5122	-	-	0.0000	
	北京中科视云科技有限公司	150.00	0.3073	-	-	0.0000	
	亚信远航软件(北京)有限 公司	100.00	0.2049	-	6.93	0.0142	1
关联方租 赁	亚信科技控股有限公司及 其附属企业	50.00	1.1393	-	16.61	0.3786	-

注1.本年初全2024年3月末与关联方累计已发生的交易金额未经审计; 注2.在上述关联交易企额和范围入公司及子公司可以根据实际情况在同一控制下的不同关联 方人之间的关联交易金额可实现内部调剂(包括不同关联交易类型间的调剂)。

(三)2023年度日常关联交易的预计和执行情况 单位:万元 币种:人民币

关联交易 类别	关联方集团	2023 年度預计 金额	2023 年度实际 金額	预计金额与实际发生金额的 异较大的原因
	亚信科技控股有限公司及其附属企业	2,000.00	615.76	
	亚信创新技术(南京)有限公司	1,000.00	1.36	
	上海富数科技有限公司	500.00	-	
关联方销	广东明日联合数字科技有限公司	300.00	-	
售	恒安嘉新(北京)科技股份有限公司	200.00	-	
	北京中科视云科技有限公司	50.00	-	公司在进行 2023 年度关键 交易預计时,系基于当时 场需求,以与关联方可能 生业务的上限金额进行
	北京深演智能科技股份有限公司	-	20.75	计,但因市场与双方需求 化等影响,公司关联交易 计与实际发生情况存在
	北京天洞職通科技股份有限公司	-	2.58	异,属于正常的经营行为
	亚信科技控股有限公司及其附属企业	2,500.00	175.37	
	亚信创新技术(南京)有限公司	3,000.00	888.30	
	上海富数科技有限公司	600.00	109.27	
关联方采	恒安嘉新(北京)科技股份公司	500.00	159.76	
购	北京信书科技发展有限公司	250.00	-	
	北京中科视云科技有限公司	150.00	-	
	亚信运航软件(北京)有限公司	100.00	6.93	
	宁夏西云算力科技有限公司(原名"宁夏天云网络科技有限公司")	30.00	-	
关联方租 赁	亚信科技控股有限公司及其附属企业	50.00	16.61	

1、亚信科技能股有限公司(AsiaInfo Technologies Limited)注册资本:10,000元港币 企业类型:于英属维尔京群岛注册成立的国际商业公司 主册地址:Craigmuir Chambers Road Town Tortola, VG1110 British Virgin Islands

法定代表人:田溯宁 成立日期:2003年7月15日

成立日列記2003年7月18日 主要股东:Skipper Investment Limited 持股 22.87%等 经营范围、软件产品及相关服务 关联关系:公司实际控制人田溯宁先生同时担任亚信科技控股有限公司主席兼执行董事

关联关系。公司实际控制人田湖宁先生同时担任亚信料 2.北京中科被云科技有限公司 注册资本;1,000 万元人民币 企业类型,其他有限责任公司 注册他批。北京市海淀区中关村大街 11 号 10 层 1061A 法定代表人、黄正

法定代表人,黄正成立日期;2014年6月11日 主要股东:北京中科海力技术有限公司持股 21.00%、北京中科智网科技有限公司持股 20.00%、北京东声致远科技有限公司持股 20.00%、中科信息安全共性技术国家工程研究中心有限公司持股 20.00%。受替范围,技术开发,技术服务,技术转让,技术咨询;计算机系统服务,销售自行开发的产品,机械设备,通讯设备;产品设计。(除电子产品,服装等实体店)市场主体依法自主选择经营项目,开展经营活动,依法现经常批准的项目。经相关部门批准后依批准的内容开展经营活动;不得从事国家和本市产业政策基止和限制类项目的经营活动。 关联关系,公司子公司亚信科技(成都)有限公司持有北京中科视云科技有限公司 19%股权,公司董事刘东红女士同时担任北京中科视云科技有限公司董事刘东红女士同时担任北京中科视云科技有限公司董事刘东红女士同时担任北京中科视云科技有限公司董事刘东红女士同时担任北京中科视云科技有限公司连册资本,7981.4466万元

注册资本:7.981.4466 万元 企业类型:其他股份有限公司(非上市) 注册地址:北京市海淀区北三环西路 25 号 27 号楼五层 5002 室

注册地址:北京市海淀区北三环西路 25 号 27 号楼五层 5002 室 注定代表人:金红 成立日期:2008 年 8 月 7 日 主要股东:金红持股 23.0989%,启明星辰信息技术集团股份有限公司持股 13.3573%、北京红杉盛 德股权投资中心(有限合伙)持股 10.8657%等 经营范围:技术服务,技术开发,技术各询,技术交流,技术转让、技术推广;数据处理和存储支持服务,信息系统集成服务,软件开发,计算机及通讯设备租赁,计算机系统服务;计算机软硬件及辅助设备程度,计算机系统服务;计算机系统服务;计算机软硬件及辅助设备器售,生产高销售,机械收备销售,安全技术的药系统设计施工服务,信息安全设备销售,专业设计服务;货物进出口,技术进出口;进出口代理。(除依法须经批准的项目外、凭营业执照依法自主开展经营活动)(不得从事国家和本市产业政策禁止和限制类项目的经营活动) 140。 / 关联关系:公司董事黄海波先生同时担任恒安嘉新(北京)科技股份有限公司董事

大耿大东:公中重申真傳放分生印刷包比世安嘉朝(北京) 4.上海富数拌技有限公司 注册资本:1,042,7296 万元人民币 企业类型:有限责任公司(自然人投资或控股) 注册地址:上海市静安区悬园路 246 寿 10 号 4 层 417 室 法定代表人;賠光明 动立日期;2016 年 4 月 90 日

成立可辨:2014年4月29日 主要股东:2014年4月29日 主要股东:此机金顺归科技有限公司持股18.0068%,成都最山股权投资基金合伙企业(有限合伙) 持股9.7234%。上海聚增仁科技合伙企业(有限合伙)持股9.2961%。上海三律企业管理合伙企业(有限 合伙)持股8.9908%。北京最山创业投资基金合伙企业(有限合伙)持股8.3665%,亚信安全科技股份有 限公司持股 8.3665%等 问行成 6.3003%等 经营范围:从事计算机软件技术、环保技术、通信技术领域内的技术开发、技术转让、技术服务、技 木咨询、计算机服务(除互联网上网服务)、电子商务、不得从事增值电信。金融业务)、企业管理分询、网络科技(不得从事科技中介),市场信息咨询与调查(不得从事社会调查、社会调研、民意调查、民意调查、大学机、软件及辅助设备的销售。(依法须经批准的项目、经相关部门批准后方可开展经营活

关联关系:公司持有上海富数科技有限公司8.3665%股权,公司董事陆光明先生同时担任上海富

注册资本:1,000 万美元 企业类型:有限责任公司(外国法人独资)

注册地址:南京市雨花台区花神大道 98 号 1 栋 203 室 法定代表人:徐猛 成立日期:2018年6月7日 主要股东: ASIAINFO INTERNATIONAL PTE.LTD.持股 100%

主要版系; ASIAINYO INICHAI IONAL PLALID: // (河区) UNP 宏宫范围: 计算机软件及网络技术开发, 技术咨询, 技术转让, 技术服务; 数据处理; 设计、制作、代理、发布广告。企业管理咨询, 白营和代理货物和技术的进出口(国家限定经营或禁止进出口的货物和技术除外(依注源纸批准的项围, 经相关部 [] 批准后方可开展经营活动) 关联关系; 公司实际控制人田测宁先生为亚信创新技术(南京) 有限公司实际控制人

6、亚信远航软件(北京)有限公司 注册资本:4,000万美元 企业类型:有限责任公司(台港澳法人独资) 注册地址:北京市海淀区西北旺东路 10 号院东区亚信联创全球总部研发中心大楼 4 层 A 座 A1

区 法定代表人: 张纯 成立日期: 2015 年 11 月 2 日 主要股东: 亚信科技国际(香港)有限公司持股 100% 经营范围: 计算机软件及网络技术开发, 技术各询, 技术转让, 技术服务; 货物进出口, 技术进出口, 代理进出口, 数据处理; 设计、制作,代理, 发布广告; 企业管理咨询, 销售计算机, 软件及辅助设备(依法须经批准的项目, 经相关部门批准后依批准的内容开展经营活动)。 关联关系: 公司实际控制人 日朔宁先生为亚信远航软件(北京)有限公司实际控制人 7. 北京信书科技及属有限公司 注册容本: 850 万元人民币

注册资本:850万元人民币 企业类型:有限责任公司(自然人投资或控股)

法定代表人:田劃宁 成立日期:2022年8月11日 主要股东:田劃宁特股 94.1176%。张纯特股 5.8824% 经营范围一般项目:技术服务,技术开发,技术咨询,技术交流,技术转让,技术推广;软件开发; 软件销售;企业管理咨询;计算机系统服务:图文设计制作;电子产品销售;计算机软硬件及辅助设备 零售;通讯设备销售;广告发布;广告设计,代理;广告制作;货物进出口;技术进出口;进出口代理。(除 法法统举批准的项目外,凭营业执照依法自主开展经营活动)(不得从事国家和本市产业政策禁止和 即组长第四日份系统法公)

关联关系:公司实际控制人田溯宁先生为北京信书科技发展有限公司实际控制人 8、宁夏西云算力科技有限公司(原名:宁夏天云网络科技有限公司) 注册资本:29,040.01 万元人民币

8、丁夏巴公异八种权名中枢公司原元;丁夏大云网络种权有限公司)
注册资本:2904001 万元人民币
企业类型;有限责任公司自然人投资或控股)
注册地址;宁夏回陆度治区中卫市沙坡头区中关村科技产业园中卫云中心 A 座 306 室
注定代表人;庄宁
成立日明:2016 年 1 月 5 日
主要股东;宁夏诚贝创业投资各询有限公司持股 89.5764%。宁夏云聚企业管理咨询合伙企业(有
限合伙/持股 10.2858%。田溯宁持股 0.1377%
经营范围;许可项目,基础电信业务;第一类增值电信业务;至联网信息服
务(依法须经批准的项目,经相关部门批准后方可开展经营活动)一般经营范围;计算机系统服务;软件开发;软件销售;技术服务,技术产资间,技术会词,技术资间级济上设计算机系统服务;实计算机交通代资金制设,是以网数据服务;数据处理服务。图文设计制作。数字文化创意软件开发;计算机软硬件及辅助设备批发;计算机软硬件及辅助设备各批发;计算机软硬件及辅助设备和发,计算机及通讯设备租赁;对外承包工程;会议及展览服务、除许可业务外,可自主依法经营法律法规申禁业或规则的项目) 关联关系。公司实际控制人田溯宁先生为宁夏西云算力科技有限公司实际控制人
9、北京深演智能科技股份有限公司
注册资本。8.391.5175 万元人民币
企业类型,科技股份有限公司
注册资本。8.391.5175 万元人民币
企业类型,科技股份有限公司
注册于水。8.391.5175 万元人民币
企业类型,科技股份有限公司
注册于水。8.391.5175 万元人民币

主要股东、黄晓南结股 20.3%。 经营产品 技术标》,设计、制作、代理、发布广告、组织文化艺术交流活动(不含演出);会议及展览服务;经济贸易咨询;计算机技术培训,软件开发;计算机系统服务,基础软件服务;应用软件服务(不含医用软件);产品设计;企业管理咨询;数据处理 数据处理 数据处理的银行卡中心、PUE 值在 1.5以上的云计算数据中心缘外);互联网信息服务。 (市场主体改法自主选择经营项目,开展经营活动,互联网信息服务以及依法须经批准的项目、经相关部门批准后依批准的内容开展经营活动,不得从审国家和本市产业政策禁止和限制类项目的经营活动。) 关联关系、公司董事资流波自 20 10 北京天洞縣通科技股份有限公司董事10 北京天洞縣通科技股份有限公司董事12 出席水、5.166 万元 从民币

注册资本:5,166 万元人民币 企业类型:科技股份有限公司

注册地址:北京市北京经济技术开发区荣华南路2号院1号楼2901

注册地址:北京市北京经济技术开发区荣华南路 2 号院 1 号楼 2901 注定代表人,吴墨 成立日期:2006年2 月23日 主要股东;吴强特股40.7589% 经营范围:一般项目:技术服务,技术开发,技术咨询,技术交流,技术转让,技术推广;软件开发; 人工智能应用软件开发;互联网数据服务,计算机较硬件及辅助设备零售;电子产品销售,通讯设备销售;企业征信业务。(除依法须经批准的项目外,凭营业执照依法自主开展经营活动)许可项目第一次增值电信业务,第二类增值电信业务。(依法须经批准的项目、参相关部门批准后方可开展经营活动,具体经营项目以相关部门批准文件或许可证件为准)(不得从事国家和本市产业政策禁止和限制类项目的经营运动。)

目的经营活动。) 关联关系:公司董事吴强担任北京天润融通科技股份有限公司法定代表人

(二)履约能力分析 上述关联方均系依法注册成立、依法存续并持续经营的法人主体、生产经营稳定、财务状况良好、 具有良好的服约能力过往发生的交易能正常实施并结算。公司将就上述交易与相关关联方签署合同 或协议并严格按照约定执行、履约具有法律保障。 三、日常性关联交易主要内容 (一)关联交易主要内容 公司及子公司与相关关联方 2024年度的预计日常关联交易主要为向关联方销售商品、采购设 备。提供劳务、接受劳务、租赁场地等、公司及子公司与各关联方之间的业务往来将遵循公允、公平、公 正的原则进行之募价格按照市场公价格和合理的收费标准确定。公司及子公司将在每次交易前与 各关联方签署具体的单项协议、对公司及子公司与各关联方(包括各关联方直接或间接控股公司)之 间的口常关联交易表效至及身位所原则等予以约定。 (二)关联交易标义签署情况

(二) 未实免债的条件,以为是的条件,以为是的条件,以为是的企业,但为实验的,是是不是的。 为维护双方利益。公司及于公司与上述关联方将根据业务开展情况签订具体合同或协议,届时公司将严格按照合同约定条款行使相关权利。履行相关义务。 四、日常性关联交易目的和对公司的影响

四、日常性关策交易目的东时公司的影响
(一)关联交易的必要性
上述关联交易是的双子公司的影响
(一)关联交易的必要性
上述关联交易是的双子公司业务发展及生产经营的正常经营活动需要,属于正常性业务,符合公司和全体股东的到益,具有公理性。
公司与关联交易是你的公允性。结算时间和方式的合理性
公司与关联方的关联交易遵循公允、公平公正的原则进行、交易价格按照市场公允价格和合理的收费标准确定,没有损害公司及其他中小股东的利益,上述关联交易对公司独立性没有影响,公司的主营业务不会因此等交易而对关联方形成依赖。
(三)关联交易的持续性
在公司业务稳定发展的情况下,公司与上述关联方之间的关联交易将持续存在。
五、保孝和助战办意识
经核查、保养和助认为。上述关于预计 2024 年度日常关联交易事项已经公司董事会,监事会独立董事专门会议及董事会审计委员会审议通过,相关关联董事已对关联交易事项回避表决。上述事项简需提受股东大会审议、符合相关法律、法规及《公司章相》的规定。公司上述预计日常关营统功所需,未被重生为公司部上关联及易事项印鑑表决。上述事项简常提受股东大会审议、符合相关法律、法规及《公司章相》的规定。公司上述预计日常关联交易事项均为公司开展日常经营运动所需,未被重生市公司和非关联股东的和益、不会对上市公司如生性产生影响,上市公司亦不会因此类交易而对关联方产生依赖。
综上所述、保孝和规对公司预计 2024 年度日常关联交易事项无异议。六、上网公告部件

六、上网公告附件 (一)《亚信安全科技股份有限公司第二届董事会独立董事 2024 年第四次专门会议决议》 (二)《中国国际金融股份有限公司关于亚信安全科技股份有限公司预计 2024 年度日常关联交易

亚信安全科技股份有限公司董事会 2024年4月27日