公司代码：688561　　公司简称：奇安信

奇安信科技集团股份有限公司

2020 年年度报告摘要

一 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，投资者应当到上海证券交易所网站等中国证监会指定媒体上仔细阅读年度报告全文。

2 重大风险提示

公司已在本报告“第四节 经营情况的讨论与分析”之“风险因素”中说明了可能对公司产生重大不利影响的风险因素，并提请投资者特别关注如下风险：

(一)尚未盈利的风险

网络安全产品及技术研发以及销售和服务网络的搭建完善需要大量投入。报告期内，公司净利润为-34,073.62 万元，亏损较上年同期减少 38.38%，归属于母公司所有者的净利润-33,436.61 万元，亏损较上年同期减少 32.44%，归属于上市公司股东的扣除非经常性损益后的净利润-53,926.84 万元，亏损较上年同期减少 21.63％。截止 2020 年末，公司累计未分配利润为-249,880.31 万元。公司持续亏损的主要原因是选择了高研发投入且人员快速扩张的发展模式，为建设研发平台、布局“新赛道”产品、提升攻防竞争力、建立全国应急响应中心而进行了大量投入。本报告期内，公司尚未盈利且存在累计未弥补亏损，预计未来仍可能持续亏损，无法保证短期内实现盈利或进行利润分配。

（二）业绩大幅下滑或亏损的风险

2020 年公司营业收入 41.61 亿元，同比增长 31.93%，尤其是布局的新赛道产品、主动防护类产品、服务营业收入高速增长。公司未来能否保持持续成长，受到宏观经济、产业政策、行业竞争态势等宏观环境等因素的影响，同时公司未来经营业绩也取决于公司技术研发，产品市场推广及销售等因素。市场规模的变化、细分领域的市场竞争加剧、产品更新换代、新市场需求的培育等因素均可能导致下游市场需求发生波动。如果未来公司现有主要产品市场需求出现持续下滑或市场竞争加剧，同时公司未能及时培育和拓展新的应用市场，将导致公司主营业务收入、净利润面临下降的风险。公司将持续在产品研发、市场推广及销售等方面进行投入，如公司收入未能按计划增长，或规模效应未按预期逐步显现，则可能导致亏损进一步增加。如果上述影响公司持续成长的因素发生不利变化，且公司未能及时采取措施积极应对，则不能保证收入按计划增长，公司存在持续亏损的风险，将导致公司存在成长性下降或者不能达到预期的风险。

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、准确、完整，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 信永中和会计师事务所（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 经董事会审议的报告期利润分配预案或公积金转增股本预案

公司 2020 年度利润分配预案为：不派发现金红利，不送红股，不以资本公积金转增股本。以上利润分配预案已经公司第一届董事会第十七次会议审议通过，尚需公司 2020 年年度股东大会审议。

7 是否存在公司治理特殊安排等重要事项

□适用 √不适用

二 公司基本情况

1 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	奇安信	688561	-

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	马勒思	
办公地址	北京市西城区西直门外南路26号院奇安信安全中心	
电话	010-56509199	
电子信箱	ir@qianxin.com	

2 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

公司专注于网络空间安全市场，主营业务为向政府、企业客户提供新一代企业级网络安全产品和服务。凭借持续的研发创新和以实战攻防为核心的安全能力，公司已发展成为国内领先的基于大数据、人工智能和安全运营技术的网络安全供应商。

公司面向新型基础设施建设、面向数字化业务，结合“内生安全”思想，将新一代网络安全框架作为顶层设计指导，以“数据驱动安全”为技术理念、以打造网络安全颠覆性和非对称性能力为目标，创建了面向万物互联时代的网络安全协同联动防御体系。公司针对云计算、大数据、物联网、移动互联网、工业互联网和 5G 等新技术下产生的新业态、新业务和新场景，为政府与企业等机构客户提供全面、体系化的网络安全解决方案。

报告期内，公司主营业务分为网络安全产品、网络安全服务、硬件以及其他。

1、网络安全产品

大数据智能安全检测与管控产品，采用大数据分析技术和人工智能方法针对威胁进行检测和响应，为客户提供针对威胁的全面检测、深度感知、关联分析、自动响应等能力闭环，包括新一代威胁态势感知与响应系统、政企态势感知与安全运营管理平台（NGSOC）、SaaS 智能安全防护、威胁情报平台等产品。

IT 设施安全防护产品（新一代 IT 基础设施防护产品），以泛终端、新边界、云计算、大数据为主要防护对象，包括泛终端安全防护、新边界安全防护、云计算基础设施安全防护、大数据基础设施安全防护等产品。

IT 架构安全防护产品（基础架构安全产品），围绕身份、行为和应用构建防御体系，包括以身份为中心进行动态访问控制的零信任安全产品、针对行为进行审计的日志与审计安全产品以及围绕应用开发的安全产品。

2、网络安全服务

安全服务系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，包括安全咨询与规划、评估与测试、分析与响应、订阅式威胁情报与远程托管式安全运营等。

3、硬件及其他

硬件及其他业务系公司在为客户提供体系化网络安全解决方案的过程中涉及到的政企客户信息化配套改造类项目，基于客户需求为客户外采第三方硬件产品并销售给对方的业务。

(二) 主要经营模式

1、研发模式

公司秉承“数据驱动安全”的技术理念，以市场需求为导向，坚持自主研发、自主创新，针对不同种类的产品和服务，针对不同客户的多样化需求，制定了独特的研发模式。

公司通过采用“产品（项目）开发+平台研发”的“横向”分层设置，覆盖公司业务开展中的研发场景，避免了通用性功能或模块在不同产品中的重复开发；通过委员会“纵向”技术管理组织，加强公司各类产品、安全平台、工程技术能力建设。两者形成“纵横”协同，保证了公司研发体系有序开展研发工作，能够极大地提高产品研发效率，缩短产品创新周期，降低产品成本，提高产品质量。

2、盈利模式

公司盈利主要来源于为政企客户体系化交付自主研发的网络安全产品，提供安全咨询规划、安全运营等各类安全服务，并满足政企客户在数字化转型过程中所遇到的各类网络安全建设需求。

3、采购模式

公司主要采购两大类软硬件设备，主要包括两大类：一类是公司自有产品所需的服务器、工控机等相关硬件设备；另一类是公司承接网络安全集成类业务所需的第三方软硬件产品及服务。

对于第一类物料的采购，公司建立了相关制度规范采购行为，由商务与供应链中心汇总项目及产品需求，合同订单和产品出货情况，综合考虑公司库存等因素，制定采购计划并实施采购。对于第二类物料的采购，公司主要通过招投标等市场化方式进行，如果客户有明确要求，则会根

据其要求进行指定采购。

4、生产模式

（1）安全产品生产模式

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。

（2）安全服务模式

安全服务是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、订阅式威胁情报与远程托管式安全运营等。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。

（3）安全集成模式

公司的安全集成业务主要为客户提供包含自有安全产品、安全服务、集成服务和第三方软硬件产品的销售及体系化交付。

5、销售模式

公司的产品和服务的销售采用直接销售与渠道销售相结合的模式。

（1）直接销售模式

对于大中型政企客户，如政府、公安、军队、金融、互联网以及能源、电力、运营商等央企和其他大型企业，公司一般采用直销的方式，安排专门的销售及技术团队为其服务，从而确保与客户持续、稳定的合作，为公司带来长期收益。

（2）渠道销售模式

对中小型客户，公司采取了区域与行业相结合的渠道销售模式，以便最大程度地覆盖更多的客户，提高市场占有率。区域经销体系是全国总经销商与各层级经销商相结合的多层次体系，各层级经销商在市场拓展、渠道建设等方面各有分工；行业渠道商主要覆盖政府、公检法司等重点行业客户，包括经销和项目合作两种模式。区域和行业渠道商根据需求采购公司产品，通常在采购后即交付给最终用户，因此项目合作伙伴的采购一般均有明确的最终用户需求。

(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

全球网络安全市场将持续保持高景气度，而中国网络安全行业则刚迈入高速发展阶段，产业规模与发达国家相比具备很大的成长空间，产业增速将持续领跑全球网络安全市场。具体而言，大数据、云计算、人工智能、5G、工业互联网、车联网等新技术新场景的快速发展，带来更多的安全需求；“十四五”规划中，强调加快推动数字产业化，培育壮大大数据、云计算、网络安全等新兴数字产业，又进一步扩大了需求侧；政企客户数字化转型、云化转型、智能化转型的加速，让网络安全从传统的本地网络零散式安全建设到覆盖更复杂业务场景全面型体系化安全建设方案转变，同样也为行业提供了新的商机。

目前，网络安全建设正在从“被动式、零散式”安全产品堆砌方案逐步发展为“全面型、体系化”的主动安全防御方案；以安全服务带动产品方案的销售模式将成为产业发展的新业态，托管式安全运营将成为未来的新安全运营模式，参考海外发达国家的安全产业特性，中国网络安全服务市场的快速发展将成为产业高速发展的重要助力。

一、行业宏观环境持续利好，网络安全支出有望大幅增长。

我国的网络安全市场增长潜力巨大。在国家刚刚发布的《“十四五”规划和 2035 年远景目标纲要》里，安全理念贯穿始终。规划中专门提出全面加强网络安全保障体系和能力建设，把网络安全与人工智能、大数据、区块链、云计算共同列为 5 大新兴数字产业，明确要求培育壮大，加快推动。

参考 Gartner 数据，2022 年，全球网络安全市场预计将达到 1704 亿美元，年复合增速在 9%左右；参考中国信息通信研究院《中国网络安全产业白皮书 2020》数据，2020 年中国网络安全产业规模约为 1702 亿人民币。

2021 年是“十四五”开局之年，为推动战略科技创新，确保产业链、供应链安全，国家将会在包括网络安全在内的科技领域继续加大投入。以扩大内需为目的的新型基础设施建设，也将促进对网络安全建设的巨大需求。

同时，个人隐私和信息泄露事件频发，也推动各国通过立法加强个人信息保护工作。企业面临的隐私保护合规压力不断增加，企业需要努力适应新的、更为严苛的数据隐私法规，这将有力地推动面向大数据应用的数据安全防护产业的发展。

二、网络安全行业的形势和技术发生了变化，取得先发优势并建立技术壁垒的企业将成为最大受益者。

从行业形势方面而言，“互联网+”和 5G 战略，推动大数据、云计算、工业互联网、物联网广泛应用，信息系统的安全也逐步改变之前围墙式、补丁式、形式合规式的业态，网络安全场景进入多元化发展期。

在技术方面，暴增的新应用、新场景需要网络安全的新技术和新体系，网络安全技术进入升级换代核心期。

在这个转折期，传统的碎片化防护方式虽然还在发挥作用，但面对已经模糊的网络边界、面对难以计数的接入终端，面对无处不在的攻击面，已经无法解决新技术、新场景和新业态下的安全问题。针对愈发复杂的攻防性的网络安全问题，需要建立协同联动的纵深防御体系，掌握基于大数据能力下的新一代网络安全技术，拥有高效全面的应急响应能力，才能真正阻断网络安全威胁，因此，取得先发优势并建立技术壁垒的网络安全企业将成为未来网络安全市场的最大受益者。

三、实战攻防演习的效果突现，显著推动实战化网络安全建设和安全服务行业的发展。

随着政企数字化转型的深入开展，网络攻击者的目标系统逐步转向核心业务数据和承载核心数据的业务应用。攻击者的角色也从普通的个人网络犯罪，到有组织的攻击甚至有境外背景的国家级对抗。攻击工具的武器化、攻击手段的战术化，均对政企用户的网络安全防御提出了更高要求。在此背景下，近年以来，国家主管部门主导的国家级网络安全实战攻防演习中，参与演习的行业更加广泛，参与演习的主体数量显著增加。实战攻防演习成为政企用户网络安全保护的常态化工作，也成为政企用户检验网络安全防御体系有效性、全面提升网络安全综合防护能力的重要手段，有效地推动了政企用户对实战化安全运行能力建设和安全人员能力建设的需求。

四、行业技术门槛较高、高端人才极其稀缺。

网络安全行业属于技术密集型行业，对产品研发和技术创新要求较高。一方面，网络安全技术和产品的创新能力是推动企业取得竞争优势的关键因素；另一方面，不同行业、不同政企用户对网络安全产品的技术需求也不尽相同，网络安全企业只有在充分了解用户需求的基础上，才能研发出匹配用户真实需求的产品和解决方案。此外，网络攻击和防御技术在对抗过程中会形成海量数据与知识库，如威胁情报数据库、漏洞库、病毒库等，这些知识库都需要专门的技术研究团队和产品应用团队长时间积累才能获得。

网络安全行业属于智力密集型行业，是一个高端人才极其稀缺的行业。目前国内的网络安全高端人才主要集中于国内外一些大的安全厂商以及研究机构，数量稀少，聘用成本较高且他们普遍与原单位签署了保密和竞业禁止协议，这使得市场新进入者短期内难以获得一批了解市场需求、掌握核心技术的人才团队，无法突破研发领域中的技术壁垒，从而难以形成自身的技术或差异化优势。

2. 公司所处的行业地位分析及其变化情况

公司是行业领先的企业级网络安全产品及服务提供商，持续为政企客户提供全面的网络安全软/硬件产品以及安全运营与实战化服务。报告期内，公司为国内首家在网络安全行业营业收入迈入 40 亿大关的网络安全公司，也是国内企业网络安全领域中体量最大、技术人员最多的网络安全公司。公司成为奥运会网络安全服务与杀毒软件官方赞助商，将为 2022 年北京冬奥会和冬残奥会提供系统的网络安全保障，公司的市场影响力、核心竞争力得到了进一步提升。

一、公司的安全理念及安全方法论继续引领行业发展

公司率先提出并成功实践“数据驱动安全”、“内生安全”等安全理念，这些安全理念成为国内安全产业发展的风向标；目前，内生安全框架已经纳入到近百家央企及重要行业客户的“十四五”规划中，获得了客户的良好反馈。2020 年 11 月 23 日，内生安全框架在世界互联网大会上，获得了“世界互联网领先科技成果”奖。

二、全面的产品布局，新赛道产品引领市场

公司是全领域覆盖的综合型网络安全厂商，具有全面的产品布局，根据 2020 年安全牛发布的第七版中国网络安全行业全景图，公司的产品线覆盖全部 15 个一级安全领域和 71 个二级细分领域，是入围该全景图细分领域最多的网络安全企业；公司在泛终端安全、态势感知、高级威胁检测、数据隐私保护、云安全、代码安全、SD-WAN、工业互联网安全、零信任身份安全、车联网安全、物联网安全等新领域、新赛道进行重点布局，针对信息化建设中的重点领域和风险领域，在网络安全市场未来发展的“主航道”中夺取先机。报告期内，公司在新领域、新赛道的产品营业收入占公司主营收入比例持续增加，市场竞争力显著提升。

三、应急响应和服务能力在实战攻防演习、重保、疫情期间网络安全防护中扮演中流砥柱的角色

公司打造了实战化的应急响应团队及安全服务体系，截至 2020 年末，公司已拥有超过 2,700 名技术支持及安全服务人员，建立了一支覆盖全国的应急响应团队和安全服务团队，在政企客户出现应急响应、重大安保和攻防演练需求时能够实时响应，有效解决客户安全问题，为公司赢得了品牌美誉度和用户信任。

2020 年国家级实战攻防演习中，公司承担众多的防守任务，实战攻防能力得到了主管机构、政企客户的广泛认可。2020 年在全国两会、中国国际服务贸易交易会、福建数字中国建设峰会、中国国际进出口博览会、世界互联网大会等国家级重大活动和会议上，公司都提供了网络安全方面的有力保障。

2020 年初疫情爆发后，以奇安信为代表的一批网络安全公司全力守护政府、医疗、交通、能源、物流等重要行业信息化系统的安全。公司向全国多家疫情防控单位提供了专业网络安全设备和服务，紧急成立疫情防控支援团，多名员工奔赴抗疫一线，为火神山、雷神山、北京小汤山等机构提供网络安全建设方案，为全国 600 家以上重要系统提供云端实时监测和防御，共发现多起 APT 组织的攻击事件，成功拦截网站 Web 应用攻击超过 150 万次。2020 年 12 月，公司被全国工商联评为“抗击新冠肺炎疫情先进民营企业”；“火神山小分队”队长魏雨露荣获国务院国资委抗疫“先进个人”殊荣。

四、公司核心技术能力受国内外权威机构认可

公司具有领先的安全攻防与对抗技术、终端安全防御技术、大数据与安全智能检测技术、安全运营与应急响应技术，在终端安全、安全管理、安全服务、云安全、威胁情报、态势感知领域市场占有率及技术先进性排名持续领先。

2020 年 4 月，凭借自主研发的新一代 QOWL 猫头鹰反病毒引擎和云安全引擎，以零误报、100%多样化样本检出率通过 VB100 测试，天擎反病毒能力再次获得权威评测机构-国际杀毒软件评测机构 Virus Bulletin 的检验和认可，标志着奇安信正式加入全球顶级反病毒厂商俱乐部。

2020 年 5 月，奇安信天擎终端安全管理系统（EDR）通过了国际知名第三方网络安全服务机构赛可达实验室威胁检测能力测试，并荣获“东方之星”证书。天擎 EDR 成为国内唯一通过该项测评的 EDR 产品。

2020 年 10 月 26 日，国际权威咨询机构 IDC 发布《IDC MarketScape:中国终端安全检测与响应市场 2020，厂商评估》报告。奇安信终端安全检测与响应（EDR）产品获得策略和市场份额双第一，位居领导者象限。

报告期内，公司核心产品在国内市场份额排名靠前：

年份	项目	排名	来源
2019	中国网络信息安全市场销售额	1	赛迪
	终端安全市场份额	1	赛迪
	安全管理平台市场份额	1	赛迪
	安全服务市场份额	1	赛迪
	云安全市场份额	1	赛迪
	Web 安全市场份额	2	赛迪
	UTM 市场份额	3	赛迪
	终端安全软件市场份额	1	IDC
	安全资源池市场份额	1	IDC
	终端安全检测与响应市场份额	1	IDC

	安全隔离与信息交换市场份额	2	IDC
	安全内容管理硬件市场份额	2	IDC
	UTM 市场份额	3	IDC
2020	安全分析和威胁情报市场份额	1	IDC
	终端安全软件市场份额	1	IDC

公司核心产品/解决方案上榜以下第三方机构报告：

年份	报告名称	品类	来源
2020	Magic Quadrant for Secure Web Gateways	SWG	Gartner
	Hype Cycle for ICT in China, 2020	云安全	Gartner
	Now Tech: Enterprise Firewalls, Q1 2020	UTM	Forrester
	Now Tech: Managed Security Services In Asia Pacific, Q4 2020	MSS	Forrester
	Now Tech: External Threat Intelligence Services, Q4 2020	威胁情报	Forrester
	新冠疫情下，IT 安全提供商如何保障企业业务稳定运行	数据安全	IDC
	CIO视角——中国智慧城市安全运营中心建设应用实践	智慧城市安全运营中心	IDC
	2020 网络安全态势感知应用指南	NGSOC/监管态势感知	安全牛

此外，报告期内，公司荣获以下第三方机构奖项：

年份	奖项名称	奖项授予	来源
2020	中国网络安全企业 100 强	奇安信集团	安全牛
	中国网络安全能力 100 强 - 领军者	奇安信集团	数世咨询
	中国十大网络安全企业	奇安信集团	等级保护测评
	中国威胁检测与响应市场领导奖	奇安信集团	沙利文
	安全服务企业服务奖	奇安信集团	艾瑞咨询
	中国十大网络安全明星产品	奇安信网神新一代安全感知系统	等级保护测评

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

面对大国之间日益严峻的网空对抗形势，面对“新冠”疫情后的经济重建、面对“十四五”规划及新基建的快速推进，网络安全在维护国家安全、支撑产业转型、促进社会发展、保障公众利益等方面的重要作用愈加凸显。2020 年 10 月，党的十九届五中全会明确了我国“十四五”期间发展的战略任务和 2035 年远景目标，强调要统筹发展和安全，全面加强网络安全保障体系和能力建设，网络安全已成为中国数字经济发展的底板。

从维护国家安全看，网络空间正在成为大国竞争博弈的新战场，极限施压、技术脱钩、技术民族主义等趋势对于信息技术产业链、供应链的负面影响上升，网络空间的地缘政治属性日益显现，未来万物互联的智慧社会对于网络安全防御技术能力的综合性、及时性的要求也将更高。

从支撑产业数字化转型看，产业转型升级引导网络互联互通，实现跨行业跨领域连接和海量数据采集汇聚，同时网络威胁也能直达生产一线，有效应对工业信息安全风险已经成为支撑产业转型升级的重要保障，亟需加强网络安全技术研发的前瞻性布局。

从维护社会稳定看，“新冠”疫情加速了信息化手段在城市建设和政务服务中的推广，城市治理和公共服务的泛在化、融合化、智能化水平日益提升。可以预见，各项城市公共服务和电子政务服务对于网络安全防护的需求与日俱增，构建体系化安全保障能力是必然趋势。

从保障人民利益看，“新冠”疫情期间，用户个人信息泄露和非法利用等风险正在增加，APP越权收集个人信息，个人隐私数据被暗网贩卖等各类网络违法犯罪行为层出不穷，数据安全与隐私保护领域需要全新的数据安全与隐私保护的创新型安全方案。

2020年复杂又严峻的网络安全形势，加速了网络安全新技术、新理念、新业态和新模式向落地实践的转化，具体而言：

（1）内生安全框架从顶层视角构建动态综合防御体系。新基建带来复杂的应用场景，对安全防护提出更高要求，内生安全框架应运而生，从“甲方视角、信息化视角、网络安全顶层视角”出发，构建了适应不同业务场景的网络安全整体防御能力分析模型，设计了复杂异构环境下的协同联动机制，形成了全生命周期的一体化安全体系。

（2）数据安全与隐私保护场景亟需技术突破。用户信息、隐私与数据保护作为互联网治理体系的重要组成部分，也是构建良好互联网秩序的重中之重，随着大数据技术的发展，数据的挖掘、收集、整合和交易越来越普遍便利，大数据开发利用中的信息安全问题凸显。在“数据不动程序动，数据可用不可见”技术理念的驱动下，新型的数据安全产品在数据安全和隐私保护方面将采用创新性的数据沙箱和安全分离学习技术，在数据需求方部署隐私保护的前提下，对多个数据源的全量数据进行充分的分析和挖掘，数据分析师只能带走不含敏感数据的分析模型文件和分析结果。

（3）零信任理念融入身份安全场景。大数据、物联网、云计算等技术的应用改变了传统身份管理和使用模式，传统身份管理无法满足数字化身份管理需求，疫情期间远程访问激增，身份安全风险尤为突出。零信任身份安全能力侧重于解决行业客户的大数据访问与身份安全问题，立足于信息化和网络安全双基础设施的定位，构建基于属性的身份管理与访问控制体系，全面纳管数字化身份，保障业务安全持续稳定运营。

（4）车联网的网络安全场景将成为客户关注的重要领域。随着5G的加速落地，智能驾驶技术的不断成熟，车联网已经成为未来智慧交通的重要应用场景，同时其带来的网络安全问题引起广泛关注，自动驾驶性能提升带来软件代码的激增，软件缺陷中隐含大量可能被利用的漏洞，这些程序漏洞可能导致软件系统的完整性受损。车联网安全防护需要结合车联网业务场景，采用多种防护技术协同联动，通过实时感知、及时反馈的安全防护方案，为自动驾驶落地提供安全保障。

（5）工业控制系统的网络安全防护成为重要方向。工业控制系统的网络安全防护与互联网有很大区别，很多联网工业设备设计之初未考虑到网络安全设计，而工业生产的可靠性、连续性要求较高，导致针对特定工业控制设备的定期更新升级通常很困难。随着工业互联网加快应用，未来主要的安全技术发展方向包括：威胁情报通过构建攻击知识库，使得针对网络威胁的响应更快；态势感知技术面向运营技术，对各种工控数据进行全面深入的安全智能分析；纵深防御通过设置多层重叠的安全防护系统，加强整体安全能力。

（6）实战化安全运行能力建设成为客户建设的重要领域。“实战化安全运行能力建设”是立足于业务架构衍生出安全架构的组织体系建设解决方案。通过识别业务架构中支撑“生产运行”的业务驱动力、组织构成和组织行为，设计对应“安全运行”的组织建设，最终实现“生产运行”与“安全

运行”的同步运行。

（7）攻防演习推动安全产品向实战化能力方向演进。为了提升国家及相关重点单位的网络安全防护水平，实战攻防演习成为了一种常态化的重要手段，通常以实际运行的信息系统作为演习目标，通过有监督的攻防对抗，最大限度地模拟真实的网络攻击，以检验信息系统的安全性和运行保障的有效性，进而推动了网络安全产品从功能趋同向防护效果差异化转变。因此，以“攻防”视角做安全的公司开始关注打造更多具备主动防御能力的产品及实战化防护效果的安全方案落地。

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 币种：人民币

	2020年	2019年	本年比上年增减(%)	2018年
总资产	12,424,319,146.93	7,154,857,102.78	73.65	6,782,262,297.69
营业收入	4,161,174,135.75	3,154,129,242.79	31.93	1,816,772,814.81
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	4,153,504,586.22	/	/	/
归属于上市公司股东的净利润	-334,366,055.61	-494,944,698.61	-32.44	-871,759,673.22
归属于上市公司股东的扣除非经常性损益的净利润	-539,268,446.84	-688,063,342.82	-21.63	-961,363,972.14
归属于上市公司股东的净资产	10,007,666,178.88	5,022,490,716.75	99.26	4,297,159,546.18
经营活动产生的现金流量净额	-688,556,343.32	-1,113,929,154.20	-38.19	-956,441,635.64
基本每股收益（元／股）	-0.54	-0.90	-40.00	-1.78
稀释每股收益（元／股）	-0.54	-0.90	-40.00	-1.78
加权平均净资产收益率（%）	-4.71	-12.11	增加7.40个百分点	-26.98
研发投入占营业收入的比例（%）	29.51	33.20	减少3.69个百分点	45.04

3.2 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	225,754,240.80	781,247,346.31	862,926,124.18	2,291,246,424.46
归属于上市公司股东的净利润	-543,908,524.83	-148,405,715.57	-315,047,703.28	672,995,888.07
归属于上市公司股东的扣除非经常性损益后的净利润	-548,886,982.12	-164,583,856.70	-337,687,231.89	511,889,623.87
经营活动产生的现金流量净额	-377,109,030.74	-519,310,653.80	-235,805,151.32	443,668,492.54

季度数据与已披露定期报告数据差异说明

□适用 √不适用

4 股本及股东情况

4.1 股东持股情况

单位：股

截止报告期末普通股股东总数(户)	15,409
年度报告披露日前上一月末的普通股股东总数(户)	14,956
截止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

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	质押或冻结情况		股东性质
						股份状态	数量	
齐向东	0	149,561,640	22.01	149,561,640	149,561,640	无	0	境内自然人

宁波梅山保税港区明洛投资管理合伙企业（有限合伙）	0	121,962,240	17.95	121,962,240	121,962,240	无	0	其他
宁波梅山保税港区安源创志股权投资合伙企业（有限合伙）	0	49,679,460	7.31	49,679,460	49,679,460	无	0	其他
天津奇安壹号科技合伙企业（有限合伙）	0	40,653,900	5.98	40,653,900	40,653,900	无	0	其他
北京金融街资本运营中心	1,960,784.00	24,208,244	3.56	24,208,244	24,208,244	无	0	国有法人
天津奇安叁号科技合伙企业（有限合伙）	0	22,247,460	3.27	22,247,460	22,247,460	无	0	其他
国投（上海）创业投资管理有限公司－国投（上海）科技成果转化创业投资基金企业（有限合伙）	0	20,852,100	3.07	20,852,100	20,852,100	无	0	其他
中电金投控股有限公司	15,721,925.00	15,721,925	2.31	15,721,925	15,721,925	无	0	国有法人

产业投资基金有限责任公司	0	12,558,140	1.85	12,558,140	12,558,140	无	0	国有法人
和谐成长二期（义乌）投资中心（有限合伙）	0	11,441,520	1.68	11,441,520	11,441,520	无	0	其他

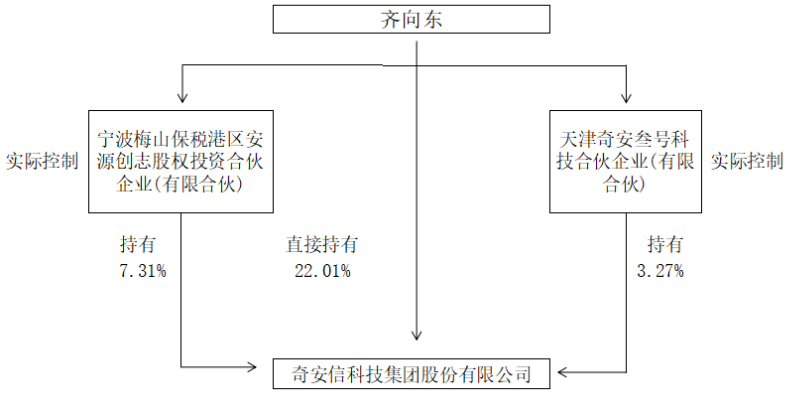
上述股东关联关系或一致行动的说明	1、齐向东先生与宁波梅山保税港区安源创志股权投资合伙企业（有限合伙）、天津奇安叁号科技合伙企业（有限合伙）为一致行动人；2、宁波梅山保税港区明洛投资管理合伙企业（有限合伙）与中电金投控股有限公司为一致行动人；3、天津奇安壹号科技合伙企业（有限合伙）和间接持有宁波梅山保税港区安源创志股权投资合伙企业（有限合伙）合伙企业份额的部分有限合伙人重合；4、和谐成长二期（义乌）投资中心（有限合伙）间接持有宁波梅山保税港区安源创志股权投资合伙企业（有限合伙）的部分合伙企业份额；5、国投（上海）科技成果转化创业投资基金企业（有限合伙）持有部分天津奇安叁号科技合伙企业（有限合伙）的合伙企业份额；6、中国电子信息产业集团有限公司为宁波梅山保税港区明洛投资管理合伙企业（有限合伙）、中电金投控股有限公司实际控制人，同时持有产业投资基金有限责任公司部分股权。除此之外，公司未知上述其他股东之间是否存在关联关系或属于一致行动人。
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

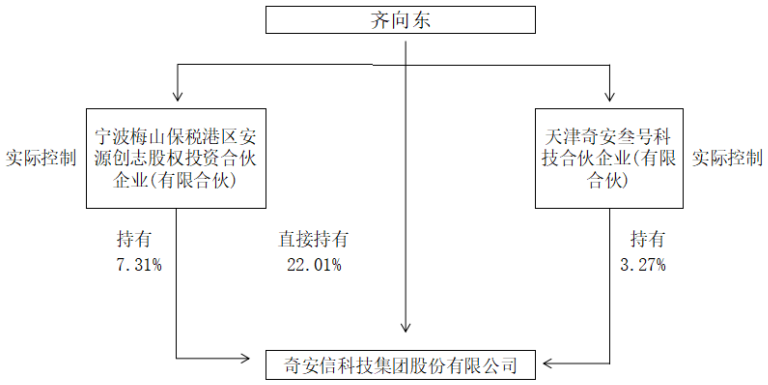
4.2 公司与控股股东之间的产权及控制关系的方框图

√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

5 公司债券情况

□适用 √不适用

三 经营情况讨论与分析

1 报告期内主要经营情况

报告期内，公司实现营业总收入 416,117.41 万元，比上年同期增长 31.93%，其中，安全产品业务 282,183.29 万元，较上年度增长 34.72%，安全服务业务 64,608.02 万元，较上年度增长 75.89%。公司毛利率由 2019 年度的 56.72%提升至 59.57%。

2 面临终止上市的情况和原因

□适用 √不适用

3　公司对会计政策、会计估计变更原因及影响的分析说明

√适用　□不适用

本报告期内涉及新收入准则的政策变更，详见本年报第十一节财务报告五、重要会计政策及会计估计 44、重要会计政策和会计估计的变更。

4　公司对重大会计差错更正原因及影响的分析说明

□适用　√不适用

5　与上年度财务报告相比，对财务报表合并范围发生变化的，公司应当作出具体说明。

√适用 □不适用

2020 年度纳入合并范围的子公司共 64 户，详见本附注九“在其他主体中的权益”。