公司代码:688201　　公司简称:信安世纪

北京信安世纪科技股份有限公司

【2023】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https://www.sse.com.cn网站仔细阅读年度报告全文。

2重大风险提示

业绩大幅下滑的风险

1、业绩大幅下滑的具体原因

报告期内,公司在深耕现有金融、烟草、交通、人社等传统优势行业的基础上,加大对教育、医疗等行业的拓展,积极探索无人机等领域的新应用,并加强产品在IPV6网络环境下的实现,但受宏观经济等因素影响,部分客户采购节奏延缓,订单签订、项目交付、验收等环节出现不同程度的延期,公司实现营业收入54,922.69万元,同比降低16.54%。为保证高质量长远发展,公司持续研发、技术、市场等方面的人才储备,员工人数及薪酬同比增长,公司实现归属于母公司所有者的净利润1,122.27万元,同比降低93.15%。

2、主营业务、核心竞争力及所处行业景气情况

近年来,国际、国内重大网络安全事故频发,我国对网络信息安全的重视程度不断提高,金融、政府及大型企业对网络安全产品的需求不断提升。同时,商用密码的应用领域亦从金融、财政、烟草、交通、通信、政务等重要应用领域向医疗、教育、农业等新的应用领域拓展。随着云计算、移动互联网、物联网、车联网、工业互联网等新业态、新应用、新场景的不断涌现,针对新技术环境下的数据安全和隐私保护等问题,都对网络安全和密码安全提出了新需求。网络安全和商用密码市场仍将保持快速发展态势。报告期内,公司主营业务、核心竞争力均未发生重大不利变化,与网络安全和商用密码行业整体趋势一致。

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,敬请查阅本报告第四节“经营情况讨论与分析”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容诚会计师事务所(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

2024年4月25日,公司于第三届董事会第三次会议审议通过了《关于〈2023年度利润分配及资本公积金转增股本预案〉的议案》,拟实施权益分派股权登记日登记的总股本扣减公司回购专用证券账户中股份为基数,分配利润/转增股本。具体如下:

1、公司拟以实施权益分派股权登记日登记的总股本扣减公司回购专用证券账户中股份为基数分配利润,拟向全体股东每10股派发现金红利0.3元(含税)。根据《上市公司股份回购规则》等有关规定,上市公司回购专用账户中的股份,不享有利润分配的权利,因此本公司回购专用证券账户中的股份将不参与公司本次利润分配。截至2024年4月25日,公司总股本215,005,011股,回购专用证券账户中股份总数为1,921,983股,以此计算合计拟派发现金红利6,392,490.84元(含税),占公司2023年度合并报表归属于上市公司股东净利润的比例为56.96%。不送红股。

2、公司拟以实施权益分派股权登记日登记的总股本扣减公司回购专用证券账户中股份为基数,以资本公积金向全体股东每10股转增4.8股。截至2024年4月25日,公司总股本215,005,011股,回购专用证券账户中股份总数为1,921,983股,以此计算合计转增102,279,853股,转增后公司总股本增加至317,284,864股。

3、如在本次董事会起至实施权益分派股权登记日期间,因可转债转股/回购股份/股权激励授予股份归属/重大资产重组股份回购注销等致使公司总股本发生变动的,公司拟维持每股现金分红金额不变,相应调整现金分红总额。同时维持每股转增股数不变,调整转增股本总额。

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

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
人民币普通股(A股)	上海证券交易所科创板	信安世纪	688201	不适用

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	丁炜	李明澜
办公地址	北京市海淀区建枫路(南延)9号院2号楼1层101	北京市海淀区建枫路(南延)9号院2号楼1层101
电话	010-68025518	010-68025518
电子信箱	ir@infosec.com.cn	ir@infosec.com.cn

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

系列名称	系列简介	名称	简介
身份安全产品系列	身份安全系列产品提供用户的身份信息和认证凭证的全生命周期管理、统一身份认证、单点登录功能,以及系统内硬件设备的安全管理和运维审计,满足各种应用系统对强身份认证及认证授权目标一管理、统一审计等的安全需求。	数字证书认证系统(NetCert)	是公钥密码基础设施解决方案的基础支撑系统,由CA数字证书认证系统、RA证书注册系统、KM密钥管理系统、OCSP服务器等组成,能够提供数字证书全生命周期的管理功能,支持X.509 V3/V4标准规范,采用安全的架构设计和权限管理,具备高级别安全机制及完善的管理、配置策略。
		车联网安全认证管理系统(V2X SCMS)	综合采用数字证书、数字签名、匿名化等技术手段,有效保障车载设备(OBU)、路侧设备(RSU)等V2X通信节点的身份合法性、认证的高效性、机密性抗抵赖性、防篡改和隐私保护。可以为各类V2X终端设备签发符合相关标准的证书及全生命周期管理,提供制作各类BSM及SPDU消息的API,并提供全方位的安全监控及预警功能。
		统一身份认证管理系统(NetAuth)	提供统一身份管理、统一身份认证、单点登录和统一安全审计,实现在一个平台对人员信息、组织信息、应用信息、账号信息的高效统一管理,支持多种身份认证方式,支持单点登录(SSO)实现一次授权可访问所有应用,满足隐私保护条例等法律法规要求,满足多维度实时审计要求。
		动态密码系统(NetPass)	基于代表身份的密钥,结合时间、事件或挑战信息,生成每隔一段时间变化一次的动态密码(口令),避免静态口令泄漏带来的安全隐患。为用户的合法身份认证提供了简捷、有效的认证手段。
		安全认证网关(NetIAG)	以安全、合规为原则,融合零信任架构理念,提供基于商用密码技术实现的安全认证、网络隐身、动态授权和虚拟门户等安全服务,在全面保障企业应用访问安全性的同时,最大程度简化接入过程,提升企业生产效率。
		统一安全管理及运维审计平台(NetPort)	是集用户管理、授权管理、认证管理和综合审计于一体的集中运维管理平台系统。该平台系统能够为客户提供集中的管理平台,提供全面的用户和资源管理,通过制定严格的资源访问策略,采用强身份认证手段,全面保障系统资源的安全;详细记录用户对资源的访问及操作,达到对运维操作行为全面审计的需要。
通信安全产品系列	通信安全系列产品是供数据传输过程中的访问控制、安全代理加解密,及性能优化、虚拟私有网络的远程安全接入、WEB通道的安全构建等功能,可以为应用系统打造一个安全、高性能的专属通信空间,提高系统整体的安全性。	应用安全网关(NISAE)	支持基于证书的服务器和客户端身份认证。提供数据在传输过程中的机密性和完整性保护。全面支持SSL/TLS协议,配合产品自带的负载均衡、防火墙、HTTP压缩等功能,为应用系统提供全方位的安全代理和应用加速服务。
		安全互联网关(NetSafe)	基于SSL安全协议实现的安全加密认证通信客户端硬件产品。集成身份认证、SSL安全链接、数字签名、验证签名、日志审计等功能,保证关键数据的数据安全,实现关键数据的防篡改、抗抵赖和数据提供方身份的真实性验证,为企业内部网络和银行、互联网电子商务等应用服务器之间构建安全的Web通道,保证业务数据的安全传输。
		应用安付系统(NetApv)	具备服务器负载均衡、链路负载均衡、全局负载均衡功能,HTTP压缩和WEB高速缓存等功能为专业级设备,打造网络安全防御墙,实现设备与业务的最优统一调度,满足了个性化、差异化的安全流量编排需求,帮助用户提高业务应用稳定性和质量,避免服务器宕机或链路故障对业务应用的影响,确保用户的业务应用能够快速、安全、可靠地交付以及按需扩展。
		安全接入网关(AG)	基于SSL安全协议的VPN设备,集成了身份认证、访问控制和资源管理等功能;提供用户接入控制和流量传输的加/解密功能,具备强大的访问控制权限管理,细粒度的审计和日志记录等功能,为用户提供安全、高效、快速、稳定的远程接入方式,实现随时随地的安全访问。
		应用安全防火墙(ASF)	采用先进的4层Speed Core多核处理架构,为关键业务应用提供全面的攻击和威胁的检测与防护。集合传WAF和正传WAF模型于一身,不仅能够检测和防范最新的已知安全攻击和漏洞,还能有效地防范“零日”攻击。可提供精细化的攻击防护控制,支持自动学习和动态防护模板刷新,通过客户端跟认证提高攻击识别精度。
数据安全产品系列	数据安全系列产品用于对电子数据和文档提供数字签名/签章,签名验证,可信时间戳等功能,使得诸如网上交易、公文审批、互联网+政务等需要经办人签名签章才可认办理业务的系统,可以确助于数字签名/签章技术得以在信息系统上开展,并且与传统手写盖章具有同等法律效力。同时用于解决不同密级网络之间的跨网隔离交换问题,支持数据从分散状态走向集中和融合,解决传统计算机的行为授权、数据授权和监管审计问题,确保高效于合规和受控状态;解决数据证移和长期保存管理问题,保证数据的可靠存储和有序管理。	签名验签服务器(NetSign)	能够对各类电子信息数据、电子文档等提供基于数字证书的数字签名服务,并对签名数据验证其签名真实性和有效性;支持不同CA的用户证书验证,提供CRL/OCSP等多种方式的证书有效性验证,满足用户在网络行为中不可否认、信息完整性、私密性等需求,并提供相关认证安易信息溯源验证。
		电子签章系统(NetSeal)	将传统印章与电子签名技术完美结合,通过采用哈希技术、PKI技术、图像处理技术等对电子文档签名并加盖签章,用于辨识电子文档签署者身份,保护文档完整性,防止对文档未经授权的篡改,确保签名行为的不可否认,并实现数字签名的可视化展现。
		可信时间戳服务器(NetTSA)	将以过时间戳服务器签名的一个可验赖的日期和时间与特定电子数据绑定在一起,对外提供精确可信的时间戳服务,通过采用精确的时间源,高强度高标准的安全机制,以确认系统处理数据在某一时间的存在性和相关操作的相对时间顺序,为信息系统中的时间戳提供基础服务。
		数据加解密服务系统(NetEDS)	是基于商用密码算法与技术实现的高性能数据安全产品,该产品可提供统一密钥管理、通用数据加解密、数据库加解密等安全服务。用户在业务系统、数据库、云基础设施等通过集成SDK或标准协议,即可为该产品对接,实现敏感数据、重要信息的加密保护,从而降低非授权访问或数据泄露带来的安全风险。
		密码模块软件(Ikec)	是符合国密相关标准的软件密码模块产品,支持SM2、SM3、SM4商用密码算法及常见国际密码算法,可提供加解密、签名验签名、证书解析等基础密码运算功能,同时可提供TLS/TLCP等安全协议处理能力。
		密码应用一体化系统(视频安全(CCypher-VSS))	将网络协议解析技术与数字签名技术深度融合,为数据中心的视频监控系统提供透明、免改造的视频数据完整性保护服务,帮忙用户以较低的投入,快速满足“密评”关于视频监控的相关合规要求。
		隐私计算平台(NetPEC)	是一种数据隐私的安全计算技术方案,语方案以NetPEC隐私计算平台为核心,以多方安全计算为基础,结合运用同态加密、差商电路、不经意传输、秘密共享等技术,提供数据加密、安全计算、数据共享、数据授权等多种服务,在满足数据隐私、安全、合规的前提下,实现多机构的联合协同计算,数据融合与联合建模,极大地拓宽了风控、营销和政企互联的覆盖能力,提升控制和使用数据要素所蕴含的巨大价值能力,解决数据孤岛和数据隐私保护两大问题,助力金融、保险、政务等领域的数据安全融合与共享流通。
		服务器密码机(UCypher)	能够为各类应用系统提供高性能、多任务并行处理的密码基础运算,支持SM1、SM2、SM3、SM4等多种国产密码算法,可以满足应用系统数据的签名/验证、加密/解密的需求,保证传输信息的机密性、完整性和有效性,同时提供安全、完善的密钥管理机制,提高系统整体安全的护能力。
		跨网隔离交换系统	隔离传输设备(隔离器)和安全把关网关组成。隔离传输设备保证两端网络物理处于相互隔离状态,主要包括光盘摆渡系统、单向摆渡系统、安全隔离与信息单向导入系统、安全隔离与信息单向导出系统等产品。安全把关网关针对跨网网络建设规范的安全防护要求,通过多种功能类型设备之间的相互联动,达到跨网系统整体风险防御效果,主要包括涉外协议代理网关、接入控制网关、数据安全交换代理网关、互联网协代理网关等产品。
		终端安全管控系统	解信息安全的护与保密管理标准要求,对用户内网终端、数据、业务流程进行全方位管控,由终端安全管控软件和文印专用外设组成。终端安全管控软件包括主机监控与审计、身份鉴别、数据集中管控、文印管控等产品,文印专用外设包括文印交互终端、刻录打印一体机、文件目录印刷收取等产品。
		数据安全归档系统	支持结构化与非结构化的数据采集与回迁,针对文档、图片、视频等不同类型数据提供了丰富的数据查询检索与统计分析功能,由数据归档软件、归档控制器和蓝光光盘库组成。蓝光光盘库内置大容量蓝光光盘作为数据存储介质,具有超长存储寿命、防电磁辐射、数据防篡改、环保节能等特点。
移动安全产品系列	移动安全系列产品构建从移动终端-管道-云的全方位移动安全防护体系,从移动终端客户数据的输入、数据显示、数据存储、数据传递、数据验证等数据全流程进行保护,有效解决移动互联网中身份认证、业务数据完整性、安全性等、防抵赖等问题。	移动统一认证安全管理平台(MAuth)	采用密钥分散、协同签名、大数据分析感知等一系列技术,为移动端提供移动数字证书全生命周期管理及基于移动数字证书的协同签名服务,对移动应用服务提供签名数据验证其签名真实性和有效性,满足移动应用的基于数字证书的强身份认证、安全传输及抵赖性等安全需求,迅速提升移动互联网应用的信息安全的护能力。
		移动安全中间件(MAuth SDK)	采用密钥分散技术、移动隔离技术、与移动安全认证系统协同,实现在移动终端的密钥、数字证书全生命周期管理及密码运算,解决了加密软件在移动端使用不便或无法与移动端结合的问题,提升了移动安全解决方案的兼容性和易用性。
		移动安全认证客户端(MAuth APP)	利用移动安全中间件构建的移动安全应用,能够通过“扫一扫”实现Android、iOS、Linux以及PC上各类应用的用户安全登录,为移动应用开发者和企业管理者提供简单快捷的基于数字证书的双因子认证解决方案;对各类移动应用的电子信息数据、电子文档等提供基于数字证书的协同签名服务,满足移动应用对信息不可否认、信息完整性、私密性等的要求。
云安全产品系列	云安全系列产品以密码技术为核心,将密码应用与云计算技术深度融合,对虚拟化资源池进行统一管理,并实现平台日动化的运维。	密码应用一体化系统(CCypher)	采用密码超融合架构将虚拟化计算、网络、密码整合到同一个系统平台,通过网络设备虚拟化技术和密码卡虚拟化技术,在一台硬件密码设备上实现同时运行多个虚拟化的密码安全设备和安全系统,与云计算管理系统无缝对接,提供云计算环境中身份、数据、通信安全所需IaaS、PaaS以及SaaS级别的密码应用服务。
		云服务器密码机(CCypher-HSM)	采用基于内核的安全隔离技术和密码硬件虚拟化技术,可支持多个虚拟服务器密码机同时提供服务,并保持各个虚拟服务器密码机之间密钥隔离、权限隔离、网络隔离、运行隔离,提供SM1、SM2、SM3、SM4等多种国产密码算法,能够为各类业务系统提供高性能、多任务并行处理的密码运算,保证信息的机密性、完整性和有效性。
		密码安全服务管理平台(CSSP-Cloud)	以“密码即服务”为核心理念,在安全、合规的原则基础上,实现密码设备资源池的弹性调度管理,典型密码应用服务的发布与管理,和产化管理与计费等功能的一体化密码云管理平台,可全面覆盖公有云模式、混合云模式、多云架构模式等复杂场景,完美解决用户在业务上云、数据上云过程中所面临的密码应用安全性合规难题。
平台安全产品系列	平台安全系列产品将业务系统所需的各种密码服务进行集中管理,将后台密码资源进行抽象包装整合,转化为前台友好的可复用共享的核心密码能力,同时运用自动感知技术实现系统运行情况的全景展示、监控及预警。	密码安全可视化监管系统(NetCVM)	采用B/S架构方式,提供统一、集中的密码应用设备集中监管服务,帮助用户实时监控密码应用设备的状态、密码服务的状态以及代理状态的监控以及密码应用日志的集中审计。
		全密码安全服务平台(CSSP)	利用平台化技术手段实现识别、沉淀和复用密码服务,构建密码服务生态,提供标准化统一的密码服务和管理服务,有效支撑业务系统的快速创新;同时,针对海量安全数据可提供采集、存储、计算、分析等功能,实现对业务、安全中台、设备、系统的全景运行态势展现。
		密评工具箱(iCBT)	是商用密码应用安全性评估工作的一体化专业便携装备,具有测评流程引导和管理、测评工具调用、测评结果分析和报告展示等功能;为测评机构提供了流程引导、数字化管理、以及专业的检测及分析工具。提高了密评工作整体的标准化、合规性和专业性。
服务			公司目有产品的运维服务、安全技术咨询和风险评估、定制开发服务等。

(二)主要经营模式

公司为客户的数字化环境和网络应用提供安全产品和解决方案,保障在多种网络环境下的身份安全、数据安全和通信安全,同时向客户提供自有产品的服务。公司具有完善的研发、采购、生产、销售、服务模式和流程,实现对经营各环节的降本增效,提升经营效率。

1. 研发模式

公司坚持“前沿技术驱动创新+业务需求驱动创新”的双线创新机制,以技术创新为驱动、市场需求为导向进行产品研发。公司设有信息安全研究院、产品部门、研发中心等三大研发机构,在软件成熟度模型CMMI L5、TSM可信研发运营安全能体系和ISO9000质量管理体系的规范指引下,公司建立了完善的研发制度和管理流程。

信息安全研究院:致力于前沿技术预研、创新业务探索。公司联合园区设立博士站,邀请院校教授,开展专题课题研究。

产品部门:对公司产品的全生命周期进行管理。根据市场调研结合技术发展,开展需求分析以确定产品方向;把控产品研发的质量和时间节点,通过评审等机制确定产品发布;根据技术发展水平和新需求提出新版本或新产品规划。

研发中心:确定了不同规模等级的研发项目的开发过程要求,经过概要设计、系统设计、编码实现等研发流程,实现产品需求;通过集成测试、自动化测试、安全攻防等系列测试手段保证产品质量;公司通过对研发过程的监督检查,保证了开发全过程的严格把控。

2. 采购模式

公司采购的主要物料为软硬一体机产品所需的各类硬件设备和配件,包括服务器、加密卡、加速卡等硬件,由供应中心负责公司供应链的管理。公

司建立了独立、完整的供应链体系,包括供应商管理、重要物料招标和采购等环节。

公司定期对供应商进行评估、走访,对供应商资质、供货质量、供货规模和交货期等进行评估,并要求供应商符合环保要求,执行RoHS标准,就工序变动通知(PCN)达成一致,符合要求的供应商进入供应商名录,建立稳定的商务合作关系,签订合作框架协议。

为进一步降低成本,公司对用量较大的物料进行年度招标。公司邀请相关供应商就产品性能、供货速度和价格等内容进行投标,并提交相关型号的产品进行测试,组织评审会,对相关指标打分和评审,确认入围价格和年供货量基准,确定建立稳定的供应关系,持续支持公司业务发展。

公司采购计划以库存预警式为主,订单驱动式为辅。确定批次采购后,通过签订订单、跟踪交期、检验入库、给付货款等环节,来保证供应链正常进行,对不合格物料进行退换货处理,或要求供应商进行整改,直到质量过关恢复供货。

3. 生产模式

公司的产品形态主要为软硬一体机,需要将自主研发的软件灌装至硬件设备。

生产环境恒温恒湿,全部铺设防静电地胶,按检验区、组装区、包装区和库房划分区域,设置明显标识,生产区域建立了独立的局域网,与外网隔绝,以防病毒和恶意软件攻击。

生产组装工作按生产工序拆分,进行流水作业,并定制了数字化的企业需求系统和生产决策系统,设有仓储条码系统,通过SN条码来定位设备和配件,具有防呆,防错料和防混料功能,使组装工作过程更精准。

公司建立了包括原材料质量管理、生产过程控制、产成品出入库等方面的全过程质量管理,严格管控生产组装全过程。公司遵照GB/T2828.1进行来料质量控制;严格按照NPI流程及制程控制软件灌装、组装、调试工序作业,保证规范操作;进行过程检验、对产成品检验,合格后方可进入产成品库房。确保产品的质量符合规定要求,保质保量交付至下游客户,公司顺利通过国内龙头企业的供应商认证,制程能力获得高端客户的认可。

4. 营销模式

公司采取“纵向深耕行业,横向拓展区域”的矩阵式销售模式,建立了全国性营销网络。建立了金融、交通、医疗、教育等重点行业销售及技术团队,深刻理解行业需求和特点,为客户提供贴身服务,针对性地提出行业解决方案,纵向深耕行业;同时建立了北京总部和华北、华东、华南、华中、西南、西北、东北等七个大区、二十七个省级办事处,为客户提供快速响应服务。

公司充分发挥行业代表性客户、网络应用中心节点的顶端优势,打造行业典型应用案例,快速向全国各大区各办事处拓展,形成覆盖全面、突出行业的营销态势。公司积极联合各细分行业的独立软件开发商(ISV),开展业务合作,建设行业生态圈,拓展细分行业的应用安全业务。公司积极和各地合作伙伴合作,寻求安全机会,快速打开当地业务局面。

公司建立了客户关系数字化管理系统,精准管理客户和销售环节。通过项目立项、技术交流、合同评审与签订、项目实施、交付与验收等一系列活动,及时记录项目进度、接收和处理客户反馈信息,保证对营销活动全周期的良性管理。

5. 方案和交付模式

公司在北京总部和七大区、二十七个省级办事处均设立了产品方案中心和服务交付中心,由多年形成的专业化信息安全队伍提供标准化服务,形成了覆盖全国的营销服务网络。

公司的产品方案中心依据信息安全相关技术标准、网络安全等级保护等相关法律法规的规定,结合客户系统的商用密码应用安全性评估情况,凭借对行业应用的丰富案例经验和对该地区的数字化进展的发展程度,针对客户的安全需求和痛点,向客户提供完整先进、贴合应用的产品和解决方案。

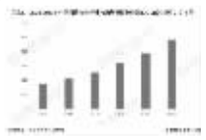
公司的服务交付中心遵循ISO9000质量管理、ISO20000IT服务管理标准以及ISO27000信息安全管理体系理念,向客户提供产品交付、质量保障、运行维护等专业化的标准安全服务。根据客户的具体情况,制定各等级的《技术服务标准》,对重点行业、重点客户提供7*24小时的全天候安全保障、关键时段值守、重点保障、应急处理等金牌安全服务,保证客户业务系统的安全性和连续性。

(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)行业发展阶段

IDC数据显示,2021年中国网络安全相关支出为122.0亿美元左右。初步统计,2022年中国网络安全相关支出为137.6亿美元;预计到2026年,中国网络安全支出规模将达318.0亿美元,预测期内将以23.3%左右的年复合增长率增长;按此增速,预计到2028年,网络安全行业整体市场规模为484亿美元。



(2)行业基本特点

应用领域和适配场景不断增加

随着数字化中国的推进,商用密码的应用领域从金融、财政、烟草、交通、通信、政务等重要应用领域向外拓展,向医疗、教育、农业等新的应用领域拓展,并有一些像低空领域等新的细分领域不断出现;随着云计算、移动互联网、物联网、车联网、工业互联网等新业态、新应用、新场景的不断涌现,针对新技术环境下的数据安全和隐私保护等问题,都对网络安全和密码安全提出了新需求。

对密码及安全的技术要求不断提升

随着数据要素和大数据时代的来临,数据资产面临的网络环境和攻击手段日趋复杂,现有的密码技术和数据安全技术需要和多种新技术的结合,如后量子密码、安全多方计算、同态加密、可搜索加密、隐私计算等,对网络安全和密码安全提出了新的技术要求。

国产化和信创的占比不断加大

网络安全作为国家战略的一部分,在国产密码算法及国产化技术已经成熟的条件下,基于国产商用密码算法的产品和各类国产硬件平台、国产操作系统、国产数据库和中间件等相关国产软硬件的结合已经成为趋势。发展信创是国家战略,解决本质安全的问题。信创产业发展已经成为经济数字化转型、提升产业链发展的关键。

政策鼓励和合规监管的驱动不断加强

近年来,国家高度重视网络空间安全及密码安全领域,国家和相关部委出台了多个政策,以密码为核心的信息安全相关法律法规体系逐步完善。政策鼓励和合规监管的驱动,推动了密评工作,也给安全行业带来机会。

序号	名称	发文单位	发布时间
1	国务院办公厅关于深入推进跨部门综合监管的指导意见	国务院办公厅	2023-02-17
2	商用密码管理条例	国务院	2023-03-14
3	国务院办公厅关于印发《政务服务电子文件归档和电子档案管理办法》的通知	国务院办公厅	2023-08-22
4	交通运输部关于推进公路数字化转型加快智慧公路建设发展的意见	交通运输部	2023-09-20
5	商用密码检测机构管理办法	国家密码管理局	2023-09-26
6	商用密码应用安全性评估管理办法	国家密码管理局	2023-09-26
7	电子政务电子认证服务管理办法(征求意见稿)	国家密码管理局	2023-10-17
8	国家数据局等部门关于印发《“数据要素×”三年行动计划(2024—2026年)》的通知	发改委国家数据局	2023-12-31

(3)主要技术门槛

技术交叉复合性门槛

密码安全技术不属于计算机及信息行业的通用技术,需要有专业的学习和研究能力才能掌握;在后量子密码技术快速推进的形势下,快速理解后量子密码技术并落地产品,需要技术积淀和技术创新能力;信息安全产品需要和其他软件或密码相关硬件相结合,了解有较强的软硬件适配能力和性能指标;信息安全产品需要适应云计算、移动互联网、物联网、车联网、工业互联网等多种业态;在技术上要结合区块链、大数据、人工智能等技术,以及安全多方计算、同态加密、可搜索加密、隐私计算等多种密码安全技术;产品和解决方案需要了解和贴近行业的应用,才能有效地解决应用的基础安全问题,需要有多个对行业的探索、积累和理解的机会和经验,具备行业应用能力。以上各类能力高度交叉复合,具有一定门槛。

产品资质门槛

根据《密码法》的第二十五条规定,“国家推进商用密码检测认证体系建设,制定商用密码检测认证技术规范、规则,鼓励商用密码从业单位自愿接受商用密码检测认证,提升市场竞争力”。商用密码生产单位应根据产品确认证各类,并向具备资格的机构提交密码模块等级的申请,经过资料审查、型式试验、工厂检查等过程,确认产品的安全性和持续生产保障能力,方可获得产品认证资格,在获证的五年有效期内,应接受管理部门的不定时证后监督检查。

根据《计算机信息系统安全专用产品检测和销售许可证管理办法》第三条的规定,“中华人民共和国境内的安全专用产品进入市场销售,实行销售许可证制度。安全专用产品的生产者在其产品进入市场销售之前,必须申领《计算机信息系统安全专用产品销售许可证》(以下简称销售许可证)”申请单位将样品送指定检测机构进行检测,检测合格后,按规定提交证书申请的相关材料,经审批通过后,方可获得相关产品的销售许可证。

2.公司所处的行业地位分析及其变化情况

作为国内较早从事密码研究并形成密码和网络安全产品和解决方案研究、生产和销售的公司,公司在科研、研发、市场等方面持续投入,不断提升经营业绩和企业影响力,推动行业发展,成为行业领先者。

(1)科研地位

公司已累计牵头或参与了《信息安全技术 大数据服务安全能力要求》《工业互联网平台身份鉴别密码应用指南》等16项国家标准的编写工作,其中11项已公开发布。

公司已累计牵头或参与了《数据安全密码技术应用指南(制定)》《政务信息系统密码应用实施指南》等68项行业标准的编写工作,其中34项已公开发布。

公司积极推进后量子密码算法研究、迁移及行业落地工作,已成功将部分后量子算法融入公司产品当中,为面对未来的后量子攻击风险提供安全保障;综合设计后量子密码的迁移规划及落地实践,助力各行业从传统密码体系平滑过渡到后量子密码体系;已与多家具有创新能力的机构建立联合,共同开展后量子密码实验课题的研究。

(2)研发能力

公司已获得美国软件工程学会(Software Engineering Institute,SEI)软件成熟度模型CMMI-Level5最高级别认证,在报告期内获得“TSM可信研发运营安全能力成熟度评估一增强级”的评估,标志着公司提升了软件应用服务全生命周期的研发运营安全管理能力,可有效控制进度偏差、提升开发效率、控制开发成本、提升产品质量和客户满意度。

公司拥有自主创新的独立知识产权,已获得308项软件著作权书和197项专利授权(其中发明专利177项)。公司的密码产品均取得了商用密码产品认证证书,并全系列通过信创适配,满足国产化要求。

(3)市场地位

入榜ISC“数字安全创新能力百强”,位列密码领域九强;

入榜CCIA中国网络安全产业联盟的“中国网安产业竞争力50强”;

入榜安全牛发布的“中国网络安全企业综合能力100强”、企业经营十强;

入榜数世咨询发布的“中国数字安全100强中坚企业”;

入榜嘶吼研究院“2023中国网络安全产业势能榜”-金融行业综合型

NetEDS数据加解密系统荣获2023鼎新信息安全先锋榜奖;

信创载方案荣获2023“金鼎奖”优秀金融科技解决方案奖;

公司荣获“金数奖-2023优秀数字化解决方案提供商”;

软件密码模块应用方案荣获“堡垒计划-安全技术应用标杆奖”;

公司在北京商用密码协会、湖北商用密码协会等四个商用密码协会担任副会长职务,并在国家密码行业标准化技术委员会和全国信息安全标准化技术委员等机构担任专家、组长职务,合力推动密码事业的发展。

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

商用密码已广泛应用于能源、交通、金融、公共服务、电子政务等关键信息基础设施领域,为维护国家安全,促进经济发展,保护人民群众利益发挥了重要作用。

报告期内,受益于国家对信息系统安全的日益重视以及安全相关政策的驱动。特别是2023年《商用密码管理条例》正式颁布,进一步落实了《密码法》的管理要求.明确了国家支持网络产品和服务使用商用密码提升安全性,支持并规范商用密码在信息领域新技术、新业态、新模式中的应用.条例的出台将加快密码技术与密码产品创新,促进我国商用密码行业规模不断扩大。2023年11月1日《商用密码应用安全性评估管理办法》正式施行,密评工作正式上升为具有强制力的国家规范,密评“强制性”执行阶段正式到来。商用密码的应用广度和深度将迎来进一步促进,密码需求将得到充分释放。商用密码的应用将焕发出更强的生命力和活力,也将持续推动密码应用快速发展。

同时伴随着信创市场进一步发展,使得基础软硬件生态体系趋于成熟和完善,使得信息技术应用创新与国产密码应用融合进一步深化,使操作系统、通用处理器、数据库、中间件等基础软硬件产品逐步具备内生密码能力,形成了支持密码应用的良好产业生态。

在需求侧,商用密码与业务融合发展也不断推动密码科技创新,云计算推动密码算法设计理论进入全同态时代,物联网发展促进了轻量级密码的设计与应用,数据要素市场化方向下,数据安全成为刚需,密码技术作为保护数据安全的核心技术和基础支撑,贯穿数据全生命周期,是重要的网络空间战略资源。为应对量子计算技术发展对密码的安全性构成的威胁,加快后量子密码发展,已积极布局后量子密码算法、协议、方案、基础设施迁移工作。

综合以上因素,商用密码领域企业需要持续的进行人才投入和研发投入,不断通过加强密码技术与其他行业的融合创新,加大研发规模投入,强化技术壁垒,提升行业内的竞争优势,保持和巩固竞争地位。

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

	2023年	2022年	本年比上年增减(%)	2021年
总资产	1,589,547,276.30	1,329,770,448.71	19.52	1,208,653,633.15
归属于上市公司股东的净资产	1,378,711,115.63	1,152,821,656.32	19.59	1,026,425,727.79
营业收入	549,226,850.31	658,076,109.27	-16.54	524,604,415.42
归属于上市公司股东的净利润	11,222,676.59	163,924,540.37	-93.15	154,126,856.05
归属于上市公司股东的扣除非经常性损益的净利润	9,466,986.69	156,548,322.01	-93.91	142,967,479.91
经营活动产生的现金流量净额	40,168,032.39	72,870,758.88	-44.88	93,935,530.17
加权平均净资产收益率(%)	1.96	15.88	减少13.93个百分点	17.98
基本每股收益(元/股)	0.0532	0.8036	-93.38	1.2199
稀释每股收益(元/股)	0.0532	0.8029	-93.37	1.2199
研发投入占营业收入的比例(%)	35.30	20.32	增加14.98个百分点	19.15

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	51,666,460.77	126,212,530.10	164,773,436.49	206,574,422.95
归属于上市公司股东的净利润	-32,571,787.33	4,781,082.03	15,529,683.06	23,473,698.83
归属于上市公司股东的扣除非经常性损益后的净利润	-32,792,248.47	5,091,177.68	15,083,749.22	22,084,317.26
经营活动产生的现金流量净额	-42,821,093.72	-12,049,770.47	-16,949,325.01	111,988,221.59

(下转B090版)

证券代码:688201　　证券简称:信安世纪

北京信安世纪科技股份有限公司

【2024】第一季度报告

本公司董事会及全体董事保证本公告内容不存在任何虚假记载、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。

重要内容提示

公司董事会、监事会及董事、监事、高级管理人员保证季度报告内容的真实、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。

公司负责人、主管会计工作负责人及会计机构负责人(会计主管人员)保证季度报告中财务信息的真实、准确、完整。

第一季度财务报表是否经审计

□是 √否

一、主要财务数据

(一)主要会计数据和财务指标

单位:元　币种:人民币

项目	本报告期		本报告期比上年同期增减变动幅度(%)
营业收入	70,611,358.39		36.67
归属于上市公司股东的净利润	-29,766,280.60		8.61
归属于上市公司股东的扣除非经常性损益的净利润	-30,364,340.23		7.43
经营活动产生的现金流量净额	-39,751,078.47		7.17
基本每股收益(元/股)	-0.1384		41.43
稀释每股收益(元/股)	-0.1384		41.38
加权平均净资产收益率(%)	-2.18		增加0.21个百分点
研发投入合计	46,951,951.55		13.34
研发投入占营业收入的比例(%)	66.48		减少13.39个百分点
	本报告期末	上年度末	本报告期末比上年度末增减变动幅度(%)
总资产	1,620,000,319.94	1,589,547,276.30	-4.13
归属于上市公司股东的所有者权益	1,333,156,570.82	1,378,711,115.63	-3.30