制作：王敬涛 电话：010-83251716 E—mail：zqrb9@zqrb.sina.net
证券日报

证券代码：688201 证券简称：信安世纪 公告编号：2026-009

北京信安世纪科技股份有限公司关于续聘会计师事务所的公告

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：

● 拟续聘2026年度审计机构（会计师事务所）名称：容诚会计师事务所（特殊普通合伙）

北京信安世纪科技股份有限公司（以下简称“公司”）于2026年4月26日召开第三届董事会第十七次会议审议通过了《关于续聘会计师事务所的议案》，拟继续聘任容诚会计师事务所（特殊普通合伙）（以下简称“容诚”）为公司2026年度审计机构。该议案尚需提交公司股东会审议。现将相关事项公告如下：

一、拟续聘会计师事务所的基本情况

（一）机构信息

1、基本信息

容诚会计师事务所由原华普天健会计师事务所（特殊普通合伙）更名而来，初始成立于1988年8月，2013年12月10日改制为特殊普通合伙企业，是国内最早获准从事证券服务业务的会计师事务所之一，长期从事证券服务业务。注册地址为北京市西城区阜成门外大街22号1幢10层1001-1至1001-26，首席合伙人刘维。

2、人员信息

截至2025年12月31日，容诚会计师事务所共有合伙人233人，共有注册会计师1507人，其中856人签署过证券服务业务审计报告。

3、业务规模

容诚会计师事务所经审计的2024年度收入总额为251,025.80万元，其中审计业务收入234,862.94万元，证券期货业务收入123,764.58万元。

容诚会计师事务所共承担518家上市公司2024年年报审计业务，审计收费总额62,047.52万元，客户主要集中在制造业、信息传输、软件和信息技术服务业、批发和零售业、科学研究和技术服务业、建筑业、水利、环境和公共设施管理业等多个行业。容诚会计师事务所对北京信安世纪科技股份有限公司所在的相同行业上市公司审计客户家数为42家。

4、投资者保护能力

容诚会计师事务所已购买注册会计师职业责任保险，职业保险累计赔偿限额不低于2.5亿元，职业保险购买符合相关规定。

近三年在执业中相关民事诉讼承担民事责任的情况：

2023年9月21日，北京金融法院就乐视网信息技术（北京）股份有限公司（以下简称乐视网）证券虚假陈述责任纠纷案[（2021）京74民初111号]作出判决，判决华普天健咨询（北京）有限公司（以下简称“华普天健咨询”）和容诚会计师事务所共同就2011年3月17日（含）之后曾买入过乐视网股票的原告投资者的损失，在1%范围内与被告乐视网承担连带赔偿责任。华普天健咨询及容诚会计师事务所收到判决后已提起上诉，截至目前，本案尚在二审诉讼程序中。

5、诚信记录

容诚会计师事务所近三年（最近三个完整自然年度及当年）因执业行为受到刑事处罚0次、行政处罚1次、监督管理措施12次、自律监管措施13次、纪律处分4次、自律处分1次。

101名从业人员近三年（最近三个完整自然年度及当年）因执业行为受到刑事处罚0次、行政处罚4次（共2个项目）、监督管理措施20次、自律监管措施9次、纪律处分10次、自律处分1次。

根据相关法律法规的规定，前述监督管理措施和自律监管措施及自律处分不影响容诚会计师事务所继续承接或执行证券服务业务和其他业务。

（二）项目成员信息

1、基本信息

容诚会计师事务所承做公司2025年度财务报表及内部控制审计项目的项目合伙人、签字注册会计师和项目质量控制复核人的基本信息如下：

项目合伙人及签字注册会计师：李成林，2012年成为中国注册会计师，2010年开始从事上市公司审计业务，2010年开始在容诚会计师事务所执业，曾于2017年至2019年为公司提供审计服务，并于2023年开始继续为公司提供服务，至今已连续服务3年；近三年签署过多家上市公司审计报告。

项目签字会计师：李春燕，2016年成为中国注册会计师，2013年开始从事上市公司审计业务，2013年开始在容诚会计师事务所执业，2024年开始为公司提供审计服务，至今已连续服务2年；近三年签署过3家上市公司审计报告。

项目质量复核人：姚瑞，2019年成为中国注册会计师，2024年开始在容诚会计师事务所执业，2025年开始为公司提供审计服务。近三年签署或复核过9家上市公司审计报告。

2、诚信记录情况。

项目合伙人李成林、签字注册会计师李春燕近三年内未曾因执业行为受到刑事处罚、行政处罚、监督管理措施和自律监管措施、纪律处分。

项目质量复核人近三年因执业行为受到刑事处罚，受到证监会及其派出机构、行业主管部门等的行政处罚、监督管理措施，受到证券交易所、行业协会等自律组织的自律监管措施、纪律处分的具体情况，详见下表：

姓名	处理处罚日期	处理处罚类型	实施单位	情况
姚瑞	2025年4月2日	行政监管措施	中国证券监督管理委员会重庆监管局	纽米科技2021-2023年年报审计项目；出具警示函
姚瑞	2026年1月19日	行政监管措施	中国证券监督管理委员会安徽监管局	润建股份2024年年报审计项目；出具警示函

容诚会计师事务所及上述人员不存在违反《中国注册会计师职业道德守则》对独立性要求的情形。

3、独立性

容诚会计师事务所及上述人员不存在违反《中国注册会计师职业道德守则》对独立性要求的情形。

4、审计收费

2025年度财务审计费用为140万元，内控审计费用为20万元，合计160万元。2024年度财务审计费用为120万元，内控审计费用为20万元，合计140万元。2025年度审计费用和内控审计费用合计同比增加14.29%。

公司2026年度审计收费根据本公司的业务规模、所处行业和会计处理复杂程度等多方面因素，并根据公司年报审计需配备的审计人员情况和投入的工作量以及事务所的收费标准确定最终的审计收费。

二、拟续聘会计师事务所履行的程序

（一）审计委员会履职情况

公司于2026年4月26日召开第三届董事会审计委员会第十三次会议，经对容诚会计师事务所的专业资质、业务能力、诚信状况、独立性、过往审计工作情况及其执业质量等进行了严格核查和评价，认为：容诚会计师事务所具备为公司提供审计工作的资质和专业能力，能够满足公司审计工作的要求。同意聘任容诚会计师事务所为公司2026年度审计机构及内部控制审计机构，并提交公司董事会审议。

（二）董事会的审议和表决情况

本事项经2026年4月26日召开的公司第三届董事会第十七次会议以7票同意，0票反对，0票弃权的表决结果审议通过。董事会同意续聘容诚会计师事务所（特殊普通合伙）为公司2026年度财务审计机构，同时提请股东会授权管理层根据2026年公司审计工作量和市场价格情况与容诚会计师事务所（特殊普通合伙）协商确定2026年度审计费用及签署相关服务协议等事项。

（三）生效日期

本次续聘会计师事务所事项尚需提交公司2025年年度股东会审议，并自公司股东会审议通过之日起生效。

特此公告。

北京信安世纪科技股份有限公司董事会
2026年4月28日

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 2025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https://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、本公司董事会及董事、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

2026年4月26日，公司于第三届董事会第十七次会议审议通过了《关于<2025年度利润分配预案>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。具体如下：

根据容诚会计师事务所出具的审计报告，截至2025年12月31日，公司单体报表未分配利润为223,993,479.98元，合并报表未分配利润为309,399,255.64元，按照单体和合并报表未分配利润取孰低原则，可供分配利润为223,993,479.98元。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，预案如下：

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0.25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2026年4月26日，公司总股本317,153,816股，回购专用证券账户中股份总数为2,195,000股，以此计算合计拟派发现金红利7,873,970.40元（含税），占公司2025年度合并报表归属于上市公司股东净利润的比例为38.33%。不送红股。

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/出售回购股份等致使公司总股本扣减回购专用证券账户中股份发生变动的，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。如后续总股本发生变化，将另行公告具体调整情况。

提请股东会授权公司董事会具体执行上述利润分配预案，根据实施结果适时变更注册资本、修订《公司章程》相关条款并办理相关工商变更登记手续。

母公司存在未弥补亏损

□适用 √不适用

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

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
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

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	丁纯	李明霞
联系地址	北京市海淀区建枫路（南延）6号院2号楼1层101	北京市海淀区建枫路（南延）6号院2号楼1层101
电话	010-68025518	010-68025518
传真	010-68025519	010-68025519
电子信箱	ir@infosec.com.cn	ir@infosec.com.cn

2、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

公司以密码技术为核心，网络安全技术为基础支撑，致力于解决多种网络环境中的身份安全、数据安全和通信安全等信息安全问题，为各行业业务系统提供安全产品和解决方案。

在产品体系方面，公司围绕密码安全、网络安全、数据安全与保密安全，构建了纵深一体化的产品与解决方案体系，形成覆盖多层级、多场景的安全能力布局。公司通过多产品线协同发展与持续技术创新，已形成体系化、平台化与高性能优势突出的安全产品与解决方案能力，为金融、政府及军队等关键行业信息系统提供稳定可靠的安全保障。

1、密码安全

在密码安全领域，公司具备深厚的技术积累与产品化能力，产品谱系涵盖各类密码模块、密码整机及密码服务系统，全面支撑多类应用场景需求。公司率先推出国内首款达到安全三级标准的数字签名服务器、SSL应用安全网关及视频安全网关等创新产品，有效满足高安全等级业务场景对密码能力的严苛要求，持续引领行业技术发展方向。具体包含：

产品线	产品名称	产品介绍
身份安全	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控，具备高级别安全机制及完善的管理、配置策略。
	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，实现了用户口令的“一次一密”特性，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。支持实体令牌、小程序令牌及短信令牌等多种形态动态令牌。
	统一身份认证管理系统（NetAuth）	提供单点登录、统一身份管理、统一身份认证、统一授权、集中安全审计等功能。适用于单位业务系统较多，需要提升IT管理员对业务系统帐号的管理效率，增强业务系统帐号的安全性，提供人员便捷的业务系统访问体验及等保、信创替代、密评、零信任等场景。
	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的安全认证、网络隐身、动态授权、应用层动态脱敏和虚拟门户等安全功能，适用于零信任安全、旁路认证、移动安全办公等场景，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。
	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，以及通信消息的完整性、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。
数据安全	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，并提供相关认证交易信息溯源验证。
	电子签章系统（NetSeal）	结合传统印章与电子签名技术，通过采用组件技术、PKI技术、图像处理技术等对电子文档签名并加盖签章。在保留了用户印章使用和管理习惯的同时提供了电子文档的完整性、真实性和抗抵赖性保护，为电子政务、企业办公、电子交易提供了安全与合规保障。
	可信时间戳服务器（NetTSA）	将经过时间戳服务器签名的一个可信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防抵赖提供基础服务。
	密码模块软件（iSec）	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。
	视频安全网关（NetVSG）	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，帮助用户以较低的投入、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）	是一种保护数据隐私的安全计算技术方案，以多方安全计算为基础，综合运用同态加密、混淆电路、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，拓宽了风控、营销和政企互联的覆盖能力，提升挖掘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SM1/2/3/4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，提高系统整体安全防护能力。
移动安全	移动统一认证安全管理平台（MAuth）	采用密钥分割、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、安全传输及抗抵赖性等安全需求，迅速提升移动互联网应用的信息安全防护能力。
	移动安全中间件（MAuth SDK）	采用密钥分割技术、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，解决了加密硬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PC操作系统（Windows、Linux）或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、私密性等的需求。
云安全	云服务器密码机（CCypher-HSM）	保障云计算密码功能需求研发的高性能密码设备，通过虚拟化技术，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物理设备资源、密码运算资源等部件的共享与安全隔离，提供SM2、SM3、SM4等多种密码算法，满足应用系统数据的签名/验证、加密/解密的要求，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，保障信息的机密性、完整性和有效性。
	密码应用一体化系统（CCypher）	采用密码超融合技术实现的新一代密码基础设施专用一体机。产品配备高性能通用计算单元与专用密码运算单元，内嵌虚拟化管理系统与密钥管理机制，支持计算虚拟化、网络虚拟化、密码虚拟化等功能，单台设备可同时运行数字签名、电子签章、动态口令、SSL VPN等多种虚拟化密码应用。
	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、租户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	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；信安CSSP全密码安全服务平台结合客户自身业务发展的需要和监管方面的要求，从前台的业务接入到中台的统一调度到后台的密码设备统一管理以及整个业务运行状况的展示，为客户提供了全方位的密码安全服务。
	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。
	密码应用监管平台（CASP）	利用平台化技术实现商用密码应用的统一监管与合规治理，构建覆盖备案、监测、核查的全流程密码安全生态。以“分级部署、统一监管”架构为核心，通过联动应用核查前置机实时分析、动态监测密码应用态势；基于自动化处理技术集成密评备案全流程，并依托可视化态势展示强化决策支持，实现同时支持国家、省、市多级资源协同管理，并联动iCET密评工具箱生成差距分析报告，显著提升监管效率并降低合规成本。
	密评工具箱系统（iCET）	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。

2、网络安全

在网络安全领域，公司以高性能架构设计为核心竞争优势，国产化负载均衡及零信任安全网关产品在大规模并发场景下具备突出的稳定性与处理能力。其中，信创零信任网关单设备可支持数万级并发用户访问，在性能与可靠性方面处于行业领先水平，能够满足大型复杂网络环境下的安全接入需求。具体包含：

产品线	产品名称	产品介绍
通信安全	应用安全网关（NSAE）	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。
	应用交付系统（APV）	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高速缓存等功能的专业硬件设备，打造网络安全资源池，实现设备与流量的统一调度，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，保证交易数据的安全传输。
	安全接入网关（AG）	基于IPSec和SSL技术实现远程接入、跨区域组网的综合安全VPN平台。支持SSL加速、AAA认证、IPSec组网、虚拟站点、单点登录等功能，适用于远程办公、移动办公、多分支机构组网等场景，可为用户提供安全、高效、快速、稳定的远程接入方式，实现随时随地的安全访问。
	动态应用防护系统（ASF-动态防护）	针对自动化攻击、恶意爬虫、中间人劫持、0day等高级威胁，采用动态封装、动态混淆、动态验证、动态令牌等自适应安全技术，实时打乱攻击路径，使威胁行为无法预测、无法重放、无法批量化利用；实现多引擎相互协同抵御攻击，促使攻击成本指数级提升，构建覆盖Web、API、APP、小程序等全业务形态的全域智能防御网络。
	应用安全防火墙（ASF）	采用先进的64位SpeedCore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。集负向WAF和正向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，通过客户端源认证提高攻击识别精度。

3、数据治理

在数据安全领域，公司构建“1+2+N”的完整产品与解决方案体系，覆盖数据资产发现、分类分级、数据脱敏与加密以及数据安全治理全流程。相关产品深度融合人工智能技术，实现数据识别、风险分析与策略执行的智能化与自动化，显著提升数据安全管理效率与精细化水平。具体包含：

产品线	产品名称	产品介绍
态势感知	数据安全态势感知平台（DSecDSA）	以安全风险管理为核心的综合性平台，利用多维度的量化指标，精准描绘数据资产分布及数据安全实时风险。平台通过数据安全分析引擎实现对数据风险的主动发现、精准定位、智能研判、协同处置以及严格审计，进而助力用户构建数据安全运营中心，实现数据安全保护工作的闭环处置。
管控平台	数据安全管控平台（DSecDGP）	数据资产梳理、数据脱敏、数据审计等各类数据安全子系统的统一管理中心。平台通过标准化的管理接口实时获取全域数据资产分布情况及安全防护状态，并将数据分类分级标签作为策略联动基础，为安全管理人员提供流程化、自动化的数据安全策略管理能力，进而支撑用户高效开展常态化、合规化的数据安全治理工作。
	数据安全流转管控平台（DSecDFC）	将“流程表单”与“数据安全”技术深度融合，面向数据共享外发场景提供工作流审批、数据保护、数据溯源等综合安全能力。平台支持自定义数据审批工作流，对数据访问全流程进行灵活管控与审计；同时基于数据分类分级标签按需实现加密及脱敏；结合明暗水印技术，进一步实现数据文件及数据集的精准溯源。
治理系统	数据安全分类分级系统（DSecDAC）	以全数据梳理为核心目标的智能化产品。采用静态网络扫描和动态流量识别相结合的方式，建立精准可靠的数据资产台账，形成完整的数据分类分级清单，自动绘制全方位的数据资产地图以及动态监测数据资产状态，帮助用户一站式解决组织内数据资产的管理、使用、统计、合规问题，并为数据安全防护提供基础策略支撑。
	数据加解密服务系统（NetEDS）	基于商用密码算法与技术实现的高性能数据安全产品，拥有“强安全”“多场景”“高性能”三重优势，提供统一密钥管理、通用数据加解密、数据库加解密及凭据管理等安全服务，能够对敏感数据和重要信息等进行加密保护，有效降低因数据泄露带来的安全风险，帮助用户切实履行《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规要求的数据保护义务。
	大数据集成与脱敏系统（DSecDMS-SDM）	是一款高性能、高兼容、智能化、全场景的数据仿真产品。系统支持抑制、泛化、扰乱和随机四大类脱敏技术共计数十种算法和策略，使脱敏后数据具备“保真性”“关联性”“可逆性”“可重复性”“时效性”“安全性”等特性，满足测试、开发、数据分析等不同场景的安全与合规要求。
	大数据动态脱敏系统（DSecDMS-DDM）	完全满足用户对数据库安全管控的需求，充分解决了运维人员、业务人员及第三方人员访问时的权限管控与数据脱敏问题。产品依据用户的角色、职责和其他IT身份特征，动态对生产数据库返回的数据进行专门的屏蔽、加密、隐藏和审计，实现在业务系统无改造情况下用户身份的可信和访问内容的可控，有效防止敏感数据的越权访问及泄露。
	数据库运维管控系统（DSecDMC）	针对敏感资产及敏感操作，提供数据库访问的最小化权限访问控制能力，解决数据库运维侧安全问题。系统将事前审批、事中控制、事后溯源贯穿整个运维过程，支持数据库准入控制、访问控制、运维审批、动态脱敏、全程审计、结果统计等核心功能。实现数据库运维侧多元化管理，解决敏感数据泄露、越权操作、高危风险操作等各类数据安全问题。
	数据库防火墙系统（DSecDBF）	以数据资产为防护核心，聚焦业务侧入侵风险防护，防止数据库由于应用程序逻辑漏洞或缺陷导致的数据安全问题。系统基于数据库协议解析与访问控制技术，提供虚拟补丁、访问控制、双白名单、三层关联等功能，使数据库免受漏洞攻击、恶意操作、SQL注入等威胁，全方面保障数据库安全，同时帮助用户满足法律法规的要求。
	数据库审计系统（DSecDBA）	信安数据库审计系统是一款对数据库访问行为进行记录、监控、跟踪溯源的安全产品。基于数据库协议解析分析技术，实现细粒度的双向审计、精准化行为回溯、用户行为风险分析、灵活报表模板、全方位风险告警等多重安全能力。帮助用户构建全面的数据安全防护体系，降低数据泄露和滥用的风险，确保数据资产的安全性。
	API安全风险监测系统（DSecASM）	基于流量分析技术实现的应用层安全审计产品，提供API资产梳理、API访问记录、API风险监测、API敏感数据发现等功能。产品具有检索性能极高、风险模型丰富、行为审计粒度细等特点，能够帮助用户在海量流量中精准发现隐藏的API资产、动态监测API的敏感数据访问情况、标记API异常访问行为，真正实现API可视化安全管理。
	数据安全协同运营平台（DSecCOP）	数据安全协同运营平台以“协同”为核心，构建一体化安全运营体系。平台将“数据敏感度、数据流动行为、策略基线”等信息进行多维监测分析，从数据资产、安全风险、合规差距、安全状态等多个视角呈现数据安全运营态势。配合流程工单及数据安全知识库，推动数据安全滚动治理，实现常态化数据安全运营。
	API安全监测与防护系统（DSecASG）	以API生命周期管理为核心，对API及传输数据进行监控、管理和保护。系统支持流动监测、访问控制、数据加密等安全机制，统一管理和保护接口数据安全。对外统一提供规范接口、认证授权，对内实现负载均衡，流量控制，确保API使用过程的高性能、高可用与安全性。

4、保密安全

在保密安全领域，公司持续强化国产化适配能力与高等级安全合规能力，相关跨网交换与保密综合管理产品较早通过行业主管部门认证，并在军队等高安全等级场景实现规模化部署应用，具备良好的实践基础与应用验证。具体包含：

产品线	产品名称	产品介绍
跨网隔离交换	科云光盘安全隔离与信息单向导入系统	针对两个物理隔离网络之间数据跨网传输的需求，采用模拟人手工操作光盘方式，实现由外部网络到内部网络数据自动单向无反馈传输。
	科云影像摆渡单向导入系统	通过显示屏和摄像头模拟人眼观察目标的单向信息传递模式实现物理隔离，采用先进的二维码及纠错技术，发送端和接收端无物理介质连接形态，实现由外部网络到内部网络数据自动单向无反馈传输。
	科云网络安全隔离与信息单向导入系统	光纤型：采用标准“2+1”架构设计，采用单向光纤传输通道，通过协议剥离、私有协议转换等隔离技术，实现由外部网络到内部网络数据自动单向无反馈传输。
		大气激光型：采用特制的空气隔离装置，通过空气传输单向光信号实现物理隔离，实现由外部网络到内部网络数据自动单向无反馈传输，具备更好的安全隔离性。
	“科云”网络安全隔离与信息交换系统	通过协议剥离、私有协议转换等隔离技术，在保持逻辑隔离的状态下实现双向交互式应用数据的代理转发。
	“科云”数据跨网交换一体化设备	依据跨网GJB标准中的安全保密建设体系要求设计，将标准中各区域需要的安全软硬件和单向导入系统以独立板卡的形式集成到一个设备内部署，采用标准机架式设计，既极大的解决了跨网设备占用空间大、部署维护难等问题，又兼顾了纵深防御路线。
	“科云”数据交换网关	对进行跨网传输的用户、应用和设备进行安全核查和身份认证，确保安全合法实体的接入，实施加密保护和完整性保护，对交换数据进行各项安全检查，并按转发范围转发从隔离器接收的数据。
	“科云”互联缓冲代理网关	采用标准机架式设备，配有千兆网络电口和可扩展光口，具备数据审核、设备调度、转发控制、设备互认证、日志审计和系统管理等功能，用于强化对两网跨网数据的检查，作为数据安全交换代理网关的一个补充。
	“科云”接入控制网关	对进行跨网传输的用户、应用和设备进行安全核查和身份认证，确保安全合法实体的接入。
	“科云”数据安全交换代理网关	对跨网传输数据添加标识，实施加密保护和完整性保护，实现跨网数据的安全引接；对交换数据进行各项安全检查，根据配置调度相应隔离器进行数据传输，并按转发范围转发从隔离器接收的数据。
	“科云”业务协议代理网关	采用标准机架式设备，配有千兆网络电口和可扩展光口，具备业务协议代理、设备互认证、日志审计和系统管理等功能，该网关用于交互式双向应用协议向双单向协议的转换，即双向交互式应用才需要业务协议代理网关。
	“科云”交换管控与审计网关	对跨网交换的基础设施设备和交换应用、用户实施统一的运行监控和管理，对跨网跨域数据交换行为进行全流程审计，进行相关统计分析，并及时发出告警，支持对历史跨网交换行为进行全流程回溯、还原。
	“科云”跨网个人文件同步系统	针对内网用户导入外部文件数据需求，实现在两个网络隔离的条件下，与跨网传输系统结合，用户通过电脑、手机上传数据，跨网数据导入系统将数据导入到内网，实现数据的自动导入，信息及时全面的共享。
	“科云”UTM安全网关	针对网络访问控制、深度报文检测、入侵检测、防病毒、抗DDos攻击、应用防护和拓扑隐藏等多种防护功能，实现对网络流量的监控，阻止未经授权的访问和攻击，保护网络免受病毒、木马、恶意软件等网络威胁的侵害。
	“科云”攻击诱捕蜜罐系统	能够提供诱骗环境仿真、攻击欺骗与转移、入侵行为监控、快速发现告警等多项功能，实现延缓攻击者对实际业务网络的攻击，保护真实信息资产。
	“科云”威胁检测沙箱	通过镜像流量来检测外部黑客发起的钓鱼邮件攻击、或在内部网络中传播的恶意软件，利用软件虚拟运行、沙箱逃逸对抗等技术对恶意软件的真实意图进行深度剖析，能够发现常规手段无法检测的APT攻击等高级威胁，并能与防火墙等设备进行安全联动，阻断威胁的进一步蔓延，为企业或组织机构的网络安全保驾护航。
	“科云”多功能导入装置（外接式）	可以将U盘数据单向的导入到计算机中，单向数据传输采用光模块进行，利用光的单向性原理，保证U盘和主机之间的数据传输单向性，即实现了U盘和主机之间的数据传输又保证了U盘和主机之间的物理隔离。
	“科云”外设共享切换器	实现两台主机共享一台显示器和一套键盘鼠标，显示器和键盘鼠标与两台主机之间采用光收发管进行单向传输隔离。
	“科云”涉密专用移动存储介质	专用移动存储介质由认证处理器、主控、存储单元等部件构成，采用专用数据接口通过多功能导入装置与SM计算机进行双向数据交互。
终端安全	“科云”保密综合管理系统	具有对计算机终端安全管控、涉密电子文件全生命周期的可追溯和审计、电子信息集中加密存储、纸质文件打印复印输出、电子文件刻录复制外带等行为严格管控和审计等能力，全方位保护计算机终端运行环境和涉密数据的安全可控。
	“科云”主机监控与审计系统	针对涉密领域或安全等级较高行业用户终端安全保护需求，实现终端准入控制、合规检查、网络访问控制、桌面行为管理、外设及接口管理、移动磁盘管理和终端安全加固，对违规行为可实施断网、锁定、关机等处理手段。
	“科云”集中管控系统	采用保密管理的操作流程，针对“终端不存密”的安全保密要求开发设计，在终端操作系统环境中创建出一个受保护的、可控的相对封闭的安全隔离工作环境，对单位日常办公中产生的涉密电子信息实施集中存储、加密保护，并通过严格的身份认证、授权访问控制和全程审计等安全机制，实现用户对文件的所有操作均可控可查和文档生成、编辑、保存、输出全过程保护。
	“科云”打印刻录复印安全监控与审计系统	针对文印输出介质全生命周期管理而设计，以集中文印输出管理方式实现打印、复印、刻录输出的全流程管理与审计，并通过建立安全的文件输出机制，实现文印管理、业务审批、内容监控、身份认证、权限管理和标识嵌入、输出文件回收等功能。
	“科云”光盘刻录保密自监管系统	深度对接密级标志系统实现全流程标识联动，采用光盘高强度加解密技术筑牢数据访问防线，依托违规外联检测与联网监管平台构建一体化安全态势感知与防控体系，全面覆盖光盘刻录、流转、归档、销毁全生命周期闭环管理。
	“科云”文印交互终端	针对集中文印系统用户在文印室或文印点现场操作需求设计，实现集中文印系统输出时的身份认证和任务管理功能。
	“科云”光盘打印刻录一体机	采用机电一体化设计，提供光盘刻录输出的同时实现盘面信息自动打印及载体信息记录。具有涉密载体标识条码以及图片、文字等多种类型信息的盘面打印功能，可有效支持涉密载体追溯。
	“科云”文件自助回收柜	将载体的自动化回收和涉密文件柜相结合，通过与集中文印系统或载体管理系统对接，实现对纸质文件、光盘、磁介质、半导体四类常用办公涉密介质的自助回收。支持人脸识别、指纹、IC/ID刷卡等多种身份认证方式，有效消除涉密载体回收的安全性和效率之间的矛盾。
	“科云”安全保密套件	聚焦涉密网络场景，搭建统一终端安全基座，以统一管控、统一接口、统一数据为核心，整合原有三合一、身份鉴别、接入控制、主机审计等各类终端安全能力，实现终端一体化管控与数据统一采集，形成终端安全数据底座，以支撑涉密网络智能自监管、分析与闭环处置，构建集防护、检查、测评、监管、运维于一体的标准化、体系化、智能化涉密网络综合防护体系。
载体管控	“科云”离线文件单向导入系统	离线文件单向导入系统部署在敏感网络边界处，用于实现将移动存储介质内的文件数据安全、高效的导入至敏感网络。该产品可保证移动存储介质与敏感网络之间的具备物理隔离强度，有效防止敏感网络内的数据反向泄露。针对单体巨大文件，支持断点续传功能，极大的提高了数据导入的易用性、可用性。
	“科云”RFID智能交换柜	基于RFID射频识别技术完成涉密载体识别，结合指纹、人脸生物识别完成交换双方身份核验，以类丰巢快递柜模式，实现涉密载体非接触式安全交换与全程留痕追溯，有效解决传统接触式交换登记繁琐、交接不清、行踪难追等痛点，满足涉密场所跨岗位、跨部门的载体便捷交换需求，助力单位落实涉密载体全流程管控要求，堵塞交换环节保密管理漏洞。
	“科云”涉密载体管控系统	涉密载体管控系统针对涉密载体在产生、存储、交接、出入等流转过程中的安全管控需求而设计，通过智能化技术实现载体流转的全程可追溯、权限精细化控制及异常行为实时告警。系统以RFID智能交换/存储柜、通道门等设备为核心，对载体的存取、交接、出入等流转操作进行动态监控，确保载体在授权范围内有序流转，杜绝泄密风险。
	“科云”自助输出一体机	自助输出一体机将身份认证与输出控制、光盘刻录和纸质文件打印等功能集于一身，与集中文印系统部署在同一网络协同工作，为用户提供文印输出的7×24小时一站式自助服务，适用于文印室、楼道、大厅等公共服务场景。
	“科云”RFID智能存储/交换柜	是一款基于超高频RFID技术设计，配合“科云”涉密载体管控系统，提供涉密载体安全存储/交换的同时，实现载体在位的实时监控及自动盘点，补全了涉密载体全生命周期中存储环节的管理功能，且能够智能识别判断异常的用户存取行为，并及时进行预警，适用于军队、军工、党政、公安等涉密办公领域中。
	“科云”RFID智能通道门	采用软硬一体化设计，具备吊顶式与立式两种型号，内置高增益天线组，高性能读写器，采用红外、雷达触发读取模式，大大延长读写器的使用寿命，可快速检测进出通道的涉密载体RFID标签，并对非法进出载体进行声光报警，适用于军队、军工、党政、公安等涉密办公领域中。
备份归档	“科云”数据归档蓝光阵列	针对数据长期保存、永久保存需求而设计，采用磁盘缓存与蓝光光盘相结合的混合存储架构，利用蓝光存储介质和自动化光盘库的优势，结合数据备份归档系统软件，通过高速磁盘缓存技术及多台光驱并发工作原理，实现海量数据长期安全存储、快速查询与下载，统计分析等数据管理需求。

5、服务

公司具有信息安全服务资质，包括风险评估、安全运维、安全开发、安全应急、安全集成，目前向客户提供自有产品的运维服务、安全技术咨询和风险评估、定制开发服务等。

2.2 主要经营模式

公司主营业务为信息安全产品的研发、生产及销售，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、提供自有产品的服务，保障在多种网络环境下的身份安全、数据安全和通信安全。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增效降本，提升经营效率。

1.研发模式

公司坚持“前沿技术+业务需求”的双轮驱动创新机制，以技术创新为驱动、市场需求为导向进行新产品规划。在软件成熟度模型CMMI L5、TSM可信研发运营安全能力成熟度评估和ISO 9001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，从产品需求、设计、编码、测试到发布的各环节进行产品的全生命周期管理，保证产品质量。

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，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。公司定期对供应商就资质、供货质量、规模和交货期等进行评估，并要求符合环保、工序变动通知等要求，建立稳定的商务合作关系。对重要物料进行招标以保证质量。公司采购计划以库存预警式为主，订单驱动式为辅，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。

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，按生产工序划分区域，设置明显标识，建立独立的局域网，与外网隔绝，以防病毒和恶意软件攻击。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，采用数字化系统管理严格管控，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。建立重点行业销售团队，深刻理解行业需求和特点，应用中心节点的顶端优势，打造行业典型解决方案；建立北京总部和华北、华东、华南、华中、西南、西北、东北等七个大区及各省级办事处，积极和各地合作伙伴合作，拓展业务局面。

5.方案和交付模式

公司在北京总部和各大区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，结合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。服务交付中心遵循ISO质量管理、信息安全管理、IT服务管理标准体系理念，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，并对重点行业、重点客户提供的全天候安全保障、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。

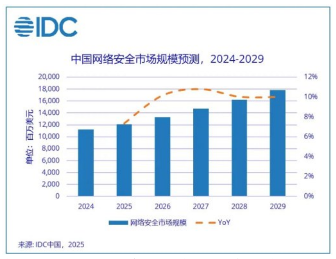
2.3 所处行业情况

(1). 行业的发展阶段、基本特点、主要技术门槛

（1）行业发展阶段

随着数字化进程的开展，商用密码技术在不断发展，零信任、隐私计算、数据安全、后量子密码、智能威胁检测、云计算等新技术的发展，带来了基础架构升级，推动安全技术创新，拓宽安全边界，促使安全防御向自动化、智能化转型，网络安全行业进入了动态积极防御阶段，导致网络安全乃至商用密码市场需求增加。另外，网络安全与低空经济、卫星互联网等新兴领域融合趋势明显，带动了网络安全边界的扩展，进而增加了网络安全的需求。

安全合规、技术迭代及市场需求形成双重驱动，促进了网络安全及商用密a码的健康发展。据国际数据公司（IDC）发布的《全球网络安全支出指南》，中国网络安全市场从终端用户的投资来看，政府、金融服务、电信是网络安全支出前三的行业，2024年支出占比分别为25.4%、16.8%和15.4%，市场规模从2024年的112亿美元增长至2029年的178亿美元，五年复合增长率为9.7%。其中，网络安全软件市场五年复合增长率为13.7%，成为中国网络安全市场中增长最快的子市场。



中国网络安全市场规模预测，2024-2029

来源：IDC中国，2025

在数字化时代，数据价值的提升也伴生更多风险，企业对数据保护的重视程度不断提高，更加注重确保数据的机密性、完整性和可用性，增加了在数据安全软件领域的投资。聚焦终端设备安全，随着多终端接入模式的深化与远程办公场景的普及，企业需要应对分散化、复杂化的安全威胁，提高了对终端设备安全的需求，也将促进该市场的迅速发展。

《网络安全法》修正草案明确关键信息基础设施运营者义务及法律责任，形成系统性网络安全治理框架。政府、金融服务与电信等行业因数据敏感性，在网络安全方面有更迫切的需求，更需要构建多层次安全防护体系，近六成网络安全支出来自于这些终端用户。

工信部办公厅发布《2025年护航新型工业化网络安全专项行动方案》，提出了建立完善工业领域网络安全防护重点企业清单，深入实施工业互联网安全分类分级管理，开展网络安全贯标达标试点和工业控制系统网络安全评估，推动了制造业网络安全市场的发展。制造业相关细分行业中，高科技与电子产品（High Tech and Electronics）行业的投资增长较为迅速。数字技术的渗透增加使得互联设备增多，数据安全与知识产权的保护需求也推动了该细分行业安全投入的增长，IDC预测，高科技与电子产品行业五年复合增长率将达到12.5%。

（2）行业基本特点

从网络安全产业链看，上游为设备、系统等供应商，如芯片、内存、操作系统、引擎等；中游为不同细分领域的网络安全产品和服务厂商，如安全软件或运维、安全服务等；下游为应用领域，如金融、政府、军工等相关领域。行业具有以下特点：

行业特点一：政策鼓励和合规监管的强力驱动

近年来，国家高度重视网络空间安全及密码安全领域，发布《中华人民共和国密码法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《关键信息基础设施安全保护条例》，“三法一条例”的立法框架构建促使国家在网络安全、数据安全、个人信息保护等方面的政策法规不断完善。2025年，国家和相关部委继续出台了多个政策，涉及密码安全、网络安全、数据安全的相关信息安全法律法规体系逐步完善，为筑牢网络与信息安全防线，维护国家安全、社会公共利益以及保护公民合法权益提供了坚实有力的法治保障。

2025年5月，中国人民银行发布《中国人民银行业务领域数据安全管理办法》，首次明确“谁管业务，谁管业务数据，谁管数据安全”的核心原则，将央行业务领域数据（涵盖货币信贷、跨境人民币、支付清算、征信等）细分为一般数据、重要数据、核心数据三级，并要求金融机构建立“全流程数据安全管理制度”，为金融数据流通与安全划定了更清晰的合规边界。

2025年6月，国家密码管理局、国家网信办、公安部联合发布了《关键信息基础设施商用密码使用管理规定》，明确划分密码管理部门、网信部门、公安机关以及保护工作部门、运营者的职权义务，明确规划、建设、运行等各阶段的规范要求，明确制度、人员、经费等方面的保障措施，将关键信息基础设施商用密码使用管理各方面、各环节的要求以法定形式固化下来。

2025年8月，国务院印发《关于深入实施“人工智能+”行动的意见》，强调“提升安全能力水平”，要求推动算法、数据、基础设施等安全建设，防范模型黑箱、歧视等风险，并明确提出要“加快形成动态敏捷、多元协同的人工智能治理格局”。这为AI安全治理定下了“发展与安全并重”的总基调。

2025年10月，全国人民代表大会常务委员会修订《中华人民共和国网络安全法》，积极应对数字技术的飞速变革，以全面适应新发展格局下的安全要求；显著提高违法行为的处罚力度，将法律责任与网络安全事件造成的实际危害后果直接挂钩，系统性强化了网络安全责任的可追责性和法律威慑力，为推进网络强国战略构筑坚实的法治根基。另外，嵌入人工智能发展与安全框架，明确加强安全风险监测评估，推动我国AI安全治理加速迈入法治轨道。

此外，细分行业发布《银行卡清算机构管理办法》《中国人民银行业务领域数据安全管理办法》《国家发展改革委国家能源局关于加快推进虚拟电厂发展的指导意见》《电力监控系统安全防护规定》《商务部印发<关于加快推进服务业扩大开放综合试点工作方案>的通知》《市场监管总局等部门关于加快推进质量认证数字化发展的指导意见》《国家网络身份认证公共服务管理办法》《关于印发<终端设备直连卫星服务管理规定>的通知》等规定和意见，推动商用密码和数据安全产品、方案在各行业的应用。

行业特点二：信息安全技术的快速发展

随着量子计算、区块链、AI等技术的快速发展，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深度融合，如后量子密码、数据治理、人工智能AI等，形成综合技术结合的密码及网络安全产品。

行业特点三：新兴应用领域不断涌现

随着数字化中国的推进，信息安全应用领域从金融、财政、交通、通信、政务等重要应用领域向外拓展，向能源、医疗、教育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、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。

行业特点四：国产化和信创的占比快速提升

信创产业以自主可控为根基，依托政策驱动和技术创新，在多行业场景中加速落地，同时通过产业链协同和安全保障构建核心竞争力，成为推动国家数字化转型和信息安全的关键力量。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。国产化和信创的占比快速提升。

（3）行业主要技术门槛

信息安全行业涉及网络、密码、人工智能等多领域技术，需要有专业的学习和研究能力，持续研发投入和技术积累才能掌握。产品需要结合区块链、大数据、人工智能、安全多方计算、同态加密、可搜索加密、隐私计算、轻量算法等多种计算机及安全技术，在近年后量子密码技术快速推进的形势下，要利用技术积淀和技术创新能力来快速理解后量子密码技术并落地产品；产品需要和相关硬件、网络环境相结合，才具有较强性能指标；同时还适应云计算、移动互联网、物联网、车联网、工业互联网、低空等多种业态，需具有对多个行业的探索、积累、理解的机会和经验，了解和贴近行业应用，才具备行业应用能力。以上各类能力高度交叉复合，更新迭代快，具有一定技术门槛。

(2). 公司所处的行业地位分析及其变化情况

公司是行业领先的安全产品和解决方案提供商，致力于解决多种网络环境中的身份安全、数据安全和通信安全等信息安全问题，服务于金融、政府、企业和军队军工等重要领域。

（1）公司研发实力

公司已获软件成熟度模型CMMI-Level5最高级别认证及“TSM可信研发运营安全能力成熟度评估—增强级”的评估，标志着公司具备高水平的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。报告期内，公司获得24项软件著作权证书，12项发明专利，累计获得351项软件著作权证书；227项专利授权（其中发明专利222项）。

公司在信息安全行业已经深耕二十余载，具有深厚的技术积淀，产品链持续延长，在信息安全版图中占有越来越多的位置。报告期内，产品进入多项行业评选：

行业全景图	公司产品进入类别	发布单位
《数字安全护航技术能力全景图（第三期）》	14大类79小类	中国信息通信研究院
《2025金融量子安全迁移与协同生态全景图》	9大类	金电研究院
《2025网络安全产业图谱》	6大类别26项细分领域	嘶吼研究院
《中国网络安全行业全景图（第十二版）》	7大领域13细分领域	安全牛
《2026年中国密评密改产业全景图》	供给侧4个维度全部入选	金电
ISC.AI 2025创新百强	身份认证	ISC

（2）行业解决方案能力

公司持续深入行业，具有较强的产品和解决方案能力和行业应用结合的能力，公司继续深耕金融、军队军工、运营商、交通等传统优势行业，加大对地方政务云、医疗疾控、税务、应急管理等行业的拓展，起到引领作用，获得了相关机构的认可。报告期内，凭借《金融控股集团数据安全流通与联合应用方案》荣获安全牛《2025数据流通安全技术应用指南》优秀案例奖，凭借《隐私计算方案》荣获嘶吼研究院颁发的《2025中国网络安全金融行业优秀解决方案》奖，政务云密码安全项目荣获2025网络安全“金帽子”年度优秀典型案例，《CMMI赋能信安世纪四大安全能力质效提升》案例被收录至《CMMI中国2025年度优秀实践案例集》，5个方案入选《甲方安全建设精品采购指南》。

（3）公司综合实力

公司建立了完善的创新机制，提升产品先进性，加强产品和解决方案向市场的推出能力，提升综合竞争能力，在市场获得认可。

奖项	发布单位
数世咨询2025年新质·中国数字安全百强-综合领域领军者	数世咨询
数世咨询2025中国数据安全50强-综合实力榜	数世咨询
嘶吼2025网络安全产业图谱-密码安全领域TOP1优秀安全企业	嘶吼
《2025数字化转型推动企业100强》	互联网周刊
2025Q3IDC中国市场应用交付Tracker-第七	IDC
2025年度IDC中国金融IT中坚力量榜单	IDC
数说安全-2025年中国网络安全市场100强	数说安全
嘶吼2025中国网络安全产业势能榜	嘶吼

报告期内，公司积极开展前沿技术研究，牵头或参与55项国家和行业的技术标准制订工作，参与编撰《低空智联网环境下的安全管控技术与应用（2025版）》《后量子密码安全能力构建技术指南（2025版）》《2025数据流通安全技术应用指南》《2025数据安全市场研究报告》《中国数字安全产业年度报告（2025）》《可信数据空间下隐私计算技术应用实践与价值研究（2025版）》，为细分行业发展提供安全支持。

(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

报告期内，信安世纪实现从合规驱动向价值驱动的转型。在新技术方面，公司重点突破后量子密码（PQC），完成关键算法研究并实现多款核心产品对PQC算法的支持，在金融、运营商等客户中成功试点迁移；同时依托信创服务器（如华为鲲鹏）实现基于可信执行环境（TEE）的机密计算产品化，获得商用密码产品二级认证，解决了数据使用过程中的保护难题。此外，公司大力推进AI与密码技术的融合，对内利用大模型实现智能配置、流量分析与日志运维，提升研发与运营效率，对外打造AI应用的安全防护方案，推动密码产品向“AI+密码”的智能化方向演进。在新产业与新业态方面，信安世纪紧跟低空经济、车联网、卫星互联网等战略性新兴产业，推出无人机数据全生命周期加密方案、车联网V2X安全中间件以及卫星互联网密码应用方案，并在多个行业实现落地示范。在新模式方面，产业正从“合规驱动”向“风险驱动”加速转型，数据安全治理从单点防护走向全生命周期智能运营，公司建立了“1+2+N”数据安全治理框架，推出密码应用监管平台（CASP），从提供单一密码产品转向提供“监测-核查-监管”的全流程服务，助力客户实现密码建设的可视、可管、可控。未来，信安世纪将持续聚焦网络安全、商用密码以及数据安全的基础理论与应用，重点跟踪零知识证明（ZKP）、可信执行环境（TEE）和全同态加密（FHE）等技术以及网络安全、商用密码、数据安全与AI的融合发展，实现AI原生安全以及AI应用的安全防护研究并推出相关安全防护解决方案，重点推进关键信息基础设施（关基）的密码改造、提升信创原生密码安全防护能力，致力于构建下一代可信AI与国产化密码安全体系。

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

	2025年	2024年	本年比上年增减(%)	2023年
总资产	1,594,342,188.16	1,514,702,960.44	5.26	1,585,547,276.30
归属于上市公司股东的净资产	1,309,149,973.06	1,284,512,803.65	1.92	1,378,711,115.63
营业收入	541,926,391.27	500,562,915.06	8.26	549,226,850.31
利润总额	23,163,837.98	-38,626,517.36	-	630,255.55
归属于上市公司股东的净利润	20,540,594.17	-47,817,571.62	-	11,222,676.59
归属于上市公司股东的扣除非经常性损益的净利润	15,101,218.46	-50,038,233.34	-	9,466,995.69
经营活动产生的现金流量净额	34,898,128.34	11,771,108.51	196.47	40,168,032.39
加权平均净资产收益率（%）	1.59	-3.60	增加5.19个百分点	1.95
基本每股收益（元／股）	0.0648	-0.1515	-	0.036
稀释每股收益（元／股）	0.0645	-0.1515	-	0.036
研发投入占营业收入的比例（%）	27.88	34.49	减少6.61个百分点	35.3

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	75,161,832.96	122,934,947.23	120,043,306.17	223,786,304.91
归属于上市公司股东的净利润	-24,896,341.64	1,409,700.02	-11,896,741.52	55,923,977.31
归属于上市公司股东的扣除非经常性损益后的净利润	-27,316,955.39	907,721.36	-12,481,667.70	53,992,120.19
经营活动产生的现金流量净额	-48,282,081.59	3,687,326.46	-37,189,471.78	116,682,355.25

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）	13,796
年度报告披露日前上一月末的普通股股东总数（户）	12,375
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	
李伟		75,857,933	23.92		无	0	境内自然人
丁纯		28,203,590	8.89		无	0	境内自然人
王翊心	-6,689,586	21,514,004	6.78		无	0	境内自然人
宁波恒世顺安企业管理合伙企业（有限合伙）	-5,366,328	14,084,424	4.44		无	0	其他
毛捍东		10,704,864	3.38	10,704,864	无	0	境内自然人
财通创新投资有限公司		4,553,330	1.44		无	0	国有法人
缪嘉嘉		3,142,941	0.99	3,142,941	无	0	境内自然人
中国建设银行股份有限公司－华宝中证金融科技主题交易型开放式指数证券投资基金	1,414,032	2,778,069	0.88		无	0	其他
刘巍建	1,140,753	2,231,507	0.7		无	0	境内自然人
北京信安世纪科技股份有限公司回购专用证券账户		2,195,000	0.69		无	0	境内非国有法人
上述股东关联关系或一致行动的说明			李伟、丁纯、王翊心为一致行动人				
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

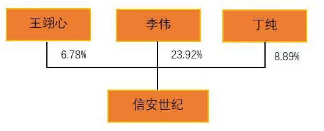
□适用 √不适用

截至报告期末表决权数量前十名股东情况表

□适用 √不适用

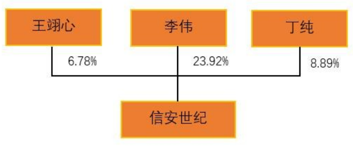
4.2 公司与控股股东之间的产权及控制关系的方框图

√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

5、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54,192.64万元，与上年同期相比增长8.26%；实现归属于母公司所有者的净利润2,054.06万元，与上年同期相比增长142.96%；实现归属于母公司所有者的扣除非经常性损益的净利润1,510.12万元，与上年同期相比增长130.18%。

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

北京信安世纪科技股份有限公司董事会关于公司2025年度否定意见内控审计报告涉及事项的专项说明

容诚会计师事务所（特殊普通合伙）（以下简称“容诚”）对北京信安世纪科技股份有限公司（以下简称“公司”）2025年度内部控制有效性进行了审计，出具了否定意见的内控审计报告（容诚审字[2026]100Z2628号），公司董事会对上述涉及事项专项说明如下：

一、否定意见内控审计报告涉及事项的基本情况

公司于2026年4月18日发布了《关于前期会计差错更正、定期报告更正及2025年度业绩预告暨业绩快报更正的公告》，对2025年研发投入资本化的会计处理进行了调整，导致对已发布的2025年各期报告及2025年年度业绩预告和2025年度业绩快报公告的相关财务数据及披露信息进行了会计差错更正。上述事项表明公司在2025年研发费用会计核算与资本化相关的内部控制存在重大缺陷。

二、董事会对上述涉及事项的意见

公司董事会认为，容诚对公司2025年度内部控制出具了否定意见内控审计报告，是根据中国注册会计师审计准则要求及审计职业判断出具的，依据和理由符合有关规定。公司董事会尊重会计师事务所依据其独立性作出的相关报告。董事会已组织公司董事、高级管理人员等积极采取有效措施，完成上述事项整改，以消除上述所涉及事项的不良影响，以保证公司持续稳定健康发展。董事会将持续关注并监督公司管理层采取相应的措施，尽快解决所涉及的相关事项，及时、准确、充分的履行信披义务，切实维护好公司和广大投资者的利益。

三、消除该事项及其影响的具体措施

针对上述导致公司形成否定意见内控审计报告的涉及事项，公司董事会和管理层高度重视，已组织开展全面自查整改，系统梳理并优化研发项目全流程管理，强化对《企业会计准则第6号—无形资产》的理解与实务应用，采取如下措施，解决上述事项以消除对公司的影响，切实保护投资者合法权益。具体措施如下：

1、公司进一步完善开发阶段专项评审制度，建立软件行业外部咨询专家库，引入外部专家参与评审及第三方机构原型测评机制，联审通过后书面确认资本化起始时点，已全部整改完毕。

2、公司于2026年4月17日召开第三届董事会第十六次会议，审议通过了《关于前期会计差错更正及定期报告更正的议案》，根据相关法律法规、规范性文件的规定，对前期会计差错及相关定期报告进行更正，并于2026年4月18日在上海证券交易所披露了《关于前期会计差错更正、定期报告更正及2025年度业绩预告暨业绩快报更正的公告》。

3、根据《上海证券交易所科创板股票上市规则（2025年4月修订）》第12.9.7条的相关规定，公司股票因第12.9.1条第一款第三项规定情形被实施其他风险警示后，公司内部控制缺陷整改完成，内控有效运行，申请撤销对其股票实施的其他风险警示的，应当披露会计师事务所对其最近一个会计年度财务报告出具的标准无保留意见的内部控制审计报告。公司持续优化内控，满足条件后，及时申请撤销对公司股票实施的其他风险警示。

特此说明。

北京信安世纪科技股份有限公司董事会
2026年4月26日

证券代码：688201 证券简称：信安世纪 公告编号：2026-011

北京信安世纪科技股份有限公司关于作废2025年限制性股票激励计划部分已授予尚未归属的限制性股票的公告

本公司董事会及全体董事保证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。

北京信安世纪科技股份有限公司（以下简称“公司”）于2026年4月26日召开的第三届董事会第十七次会议，审议通过《关于作废2025年限制性股票激励计划部分已授予尚未归属的限制性股票的议案》。现将有关事项说明如下：

一、本次激励计划已履行的相关审批程序

（一）2025年3月28日，公司第三届董事会第九次会议审议通过了《关于公司<2025年限制性股票激励计划（草案）>及其摘要的议案》《关于公司<2025年限制性股票激励计划实施考核管理办法>的议案》及《关于提请股东大会授权董事会办理公司2025年限制性股票激励计划相关事宜的议案》。

（二）2025年3月28日，公司第三届监事会第七次会议审议通过了《关于公司<2025年限制性股票激励计划（草案）>及其摘要的议案》《关于公司<2025年限制性股票激励计划实施考核管理办法>的议案》及《关于核实公司<2025年限制性股票激励计划激励对象名单>的议案》。公司监事会对本激励计划相关事项进行核实并出具了相关核查意见。

（三）2025年3月29日，公司披露了《关于独立董事公开征集委托投票权的公告》，根据公司其他独立董事的委托，独立董事马运弢先生作为征集人就2025年第一次临时股东大会审议的本次激励计划相关议案向公司全体股东征集投票权。

（四）2025年3月29日至2025年4月7日，在公司内部对激励对象的姓名和职务进行了公示。在公示的期限内，没有任何组织或个人提出异议或不良反映，无反馈记录。2025年4月10日，公司披露了《监事会关于公司2025年限制性股票激励计划激励对象名单的审核意见及公示情况说明》，监事会对本激励计划激励对象名单进行了核查并对公示情况进行了说明。

（五）2025年4月15日，公司召开2025年第一次临时股东大会，审议通过了《关于公司<2025年限制性股票激励计划（草案）>及其摘要的议案》《关于公司<2025年限制性股票激励计划实施考核管理办法>的议案》及《关于提请股东大会授权董事会办理公司2025年限制性股票激励计划相关事宜的议案》。同时，公司就内幕信息知情人在公司《2025年限制性股票激励计划（草案）》公告前6个月买卖公司股票的情况进行了自查，未发现利用内幕信息进行股票交易的情形。2025年4月16日，公司披露了《关于2025年限制性股票激励计划内幕信息知情人买卖公司股票情况的自查报告》。

（六）2025年4月15日，公司召开第三届董事会第十次会议和第三届监事会第八次会议，审议通过了《关于向激励对象授予限制性股票的议案》。公司监事会对激励对象名单进行了核实并发表了同意的意见。

（七）2026年4月26日，公司召开第三届董事会第十七次会议，审议通过了《关于作废2025年限制性股票激励计划部分已授予尚未归属的限制性股票的议案》。公司董事会薪酬与考核委员会发表了核查意见。

二、本次作废限制性股票的具体情况

（一）激励对象离职

根据公司《2025年限制性股票激励计划（草案）》（以下简称《激励计划（草案）》）的相关规定，公司2025年限制性股票激励计划的激励对象中有8人已经离职，不再符合激励资格，对应已授予尚未归属的17万股限制性股票不得归属，由公司作废。

（二）公司层面业绩考核未达标

根据公司《激励计划（草案）》的相关规定，第一个归属期公司层面业绩考核需满足下列两个条件之一：以2024年营业收入为基数，2025年营业收入增长率不低于15%；2025年净利润达到4,500万元。公司未满足上述业绩考核目标的，相应归属期内，激励对象当期计划归属的限制性股票不得归属，并作废失效。

根据容诚会计师事务所（特殊普通合伙）出具的《北京信安世纪科技股份有限公司审计报告》（容诚审字[2026]100Z2627号），公司2025年度营业收入增长率与净利润均未达标，激励对象对应已授予尚未归属的320.50万股限制性股票不得归属，由公司作废。

综上，公司本次作废已授予尚未归属的限制性股票合计337.50万股。

根据公司2025年第一次临时股东大会的授权，本激励计划限制性股票作废事项经董事会审议通过即可，无需再次提交股东会审议。

三、本次作废部分限制性股票对公司的影响

本次限制性股票作废事项不会对公司的财务状况和经营成果产生重大影响，不会影响公司核心团队的稳定性，不会影响公司股权激励计划的继续实施。

四、董事会薪酬与考核委员会意见

董事会薪酬与考核委员会认为：根据《上市公司股权激励管理办法》等相关法律法规及公司《2025年限制性股票激励计划（草案）》的有关规定，鉴于公司2025年限制性股票激励计划部分激励对象已离职、第一个归属期公司层面业绩考核未达标，对应已授予尚未归属的限制性股票共计337.50万股不得归属，由公司作废。公司本次作废部分已授予尚未归属的限制性股票符合《上市公司股权激励管理办法》等相关法律法规及公司《2025年限制性股票激励计划（草案）》的相关规定，不存在损害公司股东利益的情况。

五、法律意见书的结论性意见

北京市通商律师事务所律师认为：截至本《法律意见书》出具之日，公司本次作废已经取得了现阶段必要的批准和授权；本次激励计划部分已获授但尚未归属的限制性股票作废的情况符合《股权激励管理办法》等法律、法规、规范性文件和《激励计划》的相关规定，合法、有效。

六、独立财务顾问的结论性意见

深圳市他山企业管理咨询有限公司认为：截至本独立财务顾问报告出具日，公司2025年限制性股票激励计划作废部分限制性股票事项已经履行必要的审议程序和信息披露义务，符合《管理办法》和《激励计划（草案）》的相关规定，不存在损害上市公司及全体股东利益的情形。

七、上网公告附件

1、北京市通商律师事务所关于北京信安世纪科技股份有限公司作废2025年限制性股票激励计划部分已授予尚未归属的限制性股票事项之法律意见书；

2、深圳市他山企业管理咨询有限公司关于北京信安世纪科技股份有限公司2025年限制性股票激励计划作废部分限制性股票事项的独立财务顾问报告。

特此公告。

北京信安世纪科技股份有限公司
董事会
2026年4月28日