西部证券股份有限公司

关于

北京信安世纪科技股份有限公司

首次公开发行股票并在科创板上市

之

上市保荐书

保荐机构（主承销商）

西部证券股份有限公司

WESTERN SECURITIES CO.,LTD.

（陕西省西安市新城区东新街319号8幢10000室）

声明

保荐人及其保荐代表人已根据《中华人民共和国公司法》(以下简称《公司法》)、《中华人民共和国证券法》（以下简称《证券法》）等法律法规和中国证监会及上海证券交易所的有关规定，诚实守信，勤勉尽责,严格按照依法制定的业务规则和行业自律规范出具上市保荐书，并保证所出具文件真实、准确、完整。

如无特别说明，本上市保荐书中简称与《北京信安世纪科技股份有限公司首次公开发行股票并在科创板上市招股说明书（申报稿）》中具有相同含义。

上海证券交易所:

北京信安世纪科技股份有限公司（以下简称“信安世纪”、“发行人”“公司”）拟申请首次公开发行股票并在科创板上市。西部证券股份有限公司（以下简称“西部证券”、“保荐人”或“保荐机构”）认为发行人的上市符合《公司法》、《证券法》及《上海证券交易所科创板股票上市规则》的有关规定，特推荐其股票在贵所科创板上市交易。现将有关情况报告如下：

一、发行人概况

（一）发行人基本情况

公司名称：北京信安世纪科技股份有限公司

英文名称：Beijing Infosec Technologies Co.,Ltd.

注册资本：6,984.5817 万元

法定代表人：李伟

设立日期：2001 年 8 月 31 日

整体变更日期：2017 年 10 月 30 日

住所：北京市海淀区西三环北路 50 号院 6 号楼 11 层 1206-1

统一社会信用代码：911101086003810384

邮编：100052

电话：010-68025518

传真：010-68025519

互联网网址：www.infosec.com.cn

电子信箱：ir@infosec.com.cn

负责信息披露和投资者关系的部门：董事会办公室

负责人：丁纯

电话：010-68025518

经营范围：技术开发、技术推广、技术服务、技术咨询、技术转让；计算机系统服务；应用软件服务；计算机技术培训；生产、加工计算机软硬件；销售自产产品、计算机、软件及辅助设备、安全技术防范产品；货物进出口。（市场主体依法自主选择经营项目，开展经营活动；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；不得从事国家和本市产业政策禁止和限制类项目的经营活动。）

（二）主营业务

公司是国内领先的信息安全产品和解决方案提供商，以密码技术为基础支撑，致力于解决网络环境中的身份安全、通信安全和数据安全等信息安全问题。在信息技术互联网化、移动化和云化的发展趋势下，公司形成了身份安全、通信安全、数据安全、移动安全、云安全和平台安全六大产品系列。经过近二十年的自主研发和持续创新，公司已经成为行业内具有科技创新竞争力的企业。。

（三）发行人的技术与研发情况

1、公司核心技术情况

经过近二十年的行业技术和经验积累，公司掌握了多项具有自主知识产权的核心技术。目前，公司已经形成了移动互联网、大数据、物联网等新兴领域的一系列核心技术储备。截至本上市保荐书出具日，公司已经累计取得 62 项专利（其中发明专利 45 项）、138 项软件著作权。

（1）公司核心技术

公司主要产品中的核心技术、技术来源、技术特点和技术成熟度等方面的具体情况如下：

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	专利状态	相关产品与服务	所处阶段
1	网络密钥安全派生与协同签名技术	采用独创的移动端密钥防护和存储技术实现移动端派生密钥和数据安全存储，以及独创的算法和协议实现移动端派生密钥和服务端密钥的协同签名技术。	自主研发	原始创新	ZL201610183456.5	已授权	移动安全认证系统、云密码安全服务平台系统	成熟稳定成熟应用
					ZL201610987411.3			
					ZL201710694657.6			
					ZL201611194899.0	申请中		
					ZL201710694673.5			
					ZL201811147472.4			
					ZL201811148390.1			
2	基于人工智能的用户行为分析鉴别技术	通过用户行为大数据信息，利用机器深度学习，采用独创的学习算法和大数据快速分析技术实现用户身份鉴别与行为风险分析。	自主研发	原始创新	ZL201710358046.4	申请中	移动安全认证系统、云密码安全服务平台系统	成熟稳定成熟应用
					ZL201810439227.4			
3	网络传输加密与处理技术	通过独创的协议优化以及算法，对应用数据在网络传输和存储过程中进行加解密处理技术。	自主研发	原始创新	ZL201610648971.6	已授权	NSAE 应用安全网关、应用安全网关系统、NetOpti 应用交付系统、NetGate SSL VPN 网关、NetSafe 安全互联网关	成熟应用
					ZL200810101869.X			
					ZL201210343249.3			
					ZL201410575787.4			
					ZL201511029004.3			
					ZL201710832664.8	申请中		
					ZL201810273821.0			
					ZL201710592618.5			
					ZL201810736473.6			

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	专利状态	相关产品与服务	所处阶段
					ZL201810009255.2			
					ZL201910644205.6			
4	基于安全套接层协议特征的加速负载分发技术	独创的基于压缩、缓存、安全套接层协议优化在内的服务器加速负载分发技术。	自主研发	原始创新	ZL201510058710.4	已授权	NSAE 应用安全网关、应用安全网关系统、NetOpti 应用交付系统、NetGate SSL VPN 网关、NetSafe 安全互联网关	成熟稳定成熟应用
					ZL201910180888.4	申请中		
					ZL201911061545.2			
					ZL202010126110.8			
5	云架构密码分发与权限控制技术	采用独创的云架构虚拟化环境下密钥存储和权限控制技术实现云端密码管控。	自主研发	原始创新	ZL201510059803.9	已授权	移动安全认证系统、CCypher 云密码服务平台	成熟稳定成熟应用
					ZL201710117279.5	申请中		
					ZL201710630832.5			
					ZL201710694672.0			
					ZL201910350147.6			
					ZL201910148673.4			
					ZL201910967308.6			
6	数字证书与加密协议格式的快速解析和判定技术	通过独创的解析算法对数字证书以及签名加解密格式进行快速解析分析和判定。	自主研发	原始创新	ZL200910181164.8	已授权	NetCert 证书认证系统、NetPass 动态密码系	成熟稳定成熟应用

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	专利状态	相关产品与服务	所处阶段
							统、NetAuth 统一身份认证管理系统、NetSign 签名验签服务器、NetSeal 电子签章系统	
7	移动威胁态势感知技术	通过本技术提供的分析引擎和算法库，实现对移动操作系统漏洞、开放端口、黑客入侵、web 攻击、APP 攻击、威胁情报、企业安全舆情等全方位的监控，及时预警或预测威胁态势。	自主研发	原始创新	ZL201611199027.3	已授权	移动安全认证系统、CCypher 云密码服务平台	成熟稳定 成熟应用
					ZL201710829211.X	申请中		
					ZL201910967308.6	申请中		
8	高性能动态可配置的 API 网关技术	在 API 网关统一解决微服务集群的认证、鉴权、流量管控、熔断、灰度发布等问题，提升运维管控效率，在保障系统安全接入的基础上，构建高性能、高可靠稳定运行能力。	自主研发	原始创新	ZL201910498661.4	申请中	NetCert 证书认证系统、NetPass 动态密码系统、NetAuth 统一身份认证管理系统、NetSign 签名验签服务器、NetSeal 电子签章系统	成熟稳定 成熟应用
					ZL201910498047.8			
9	基于时序数据库分布式业务监控技术	采用特殊数据存储和索引方式，可以高效存储和快速处理海量时序大数据。相对于关系型数据库它的存储空间减半，查询速度极大的提高。时间序列函	自主研发	原始创新	ZL201910864869.3	申请中	CCypher 云密码服务平台	成熟稳定 成熟应用
					ZL201910281572.4			

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	专利状态	相关产品与服务	所处阶段
		数优越的查询性能远超过关系型数据库，非常适合在监控预警分析领域的应用。			ZL201910281587.0			
10	高效安全的容灾技术和集群技术	通过对硬件安全产品密钥运算主运算卡与多个待同步运算卡快速协同同步技术以及数据网络镜像技术，实现了运算卡密钥及安全配置数据等容灾和集群技术，同时保证产品的高性能、稳定性和可靠性。	自主研发	原始创新	ZL201610161906.0	已授权	NetCert 证书认证系统、NetPass 动态密码系统、NetAuth 统一身份认证管理系统、NetSign 签名验签服务器、NetSeal 电子签章系统	成熟稳定成熟应用
					ZL201610798638.3			
					ZL201610797724.2			
					ZL201610798642.X	申请中		
					ZL201810204031.7			
					ZL201910263030.4			
11	高性能网络产品架构技术	使用独创的 SpeedStackTM 专利技术，实现了快速 TCP/IP 协议栈、应用代理和智能应用协议分析器，保证产品的高性能、稳定性和可靠性。	自主研发	原始创新	ZL200910084745.X	已授权	NSAE 应用安全网关、应用安全网关系统、NetOpti 应用交付系统、NetGate SSL VPN 网关、NetSafe 安全互联网关	成熟稳定成熟应用
					ZL200810103457.X			
					ZL201210317104.6			
					ZL201210348315.6			
					ZL201210545948.6			
					ZL201310123660.4			
					ZL201310418949.9			
					ZL201910641832.4	申请中		
					ZL201910871217.2			
12	智能流量学习	利用智能流量学习和应用识别技术，对网络流量进	自主	原始创	ZL200810113016.8	已授权	NSAE 应用	成熟稳定

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	专利状态	相关产品与服务	所处阶段
	和应用识别技术	行分析建模，对各类网络应用进行识别，精准判断攻击流量，准确封堵攻击源头，为企业网络提供安全保障。	研发	新	ZL201210293426.1		安全网关	成熟应用
					ZL201711374503.5	申请中		
					ZL201410642928.X			
					ZL201710765544.0			
					ZL201810420673.0			
13	远程安全接入技术	通过独创的软件虚拟化技术和严格的逻辑隔离技术，使得单个硬件设备最大支持 256 个虚拟服务站点和最大 128,000 并发用户。	自主研发	原始创新	ZL200810102498.7	已授权	NetGate SSL VPN 网关	成熟稳定成熟应用
					ZL200810106321.4			
					ZL201110141389.8			
					ZL201210485032.6			
					ZL201911202379.3	申请中		
14	零信任边界安全保护技术	通过独创的 URL 和内容改写技术，无缝透明代理并保护后台的边界内应用。通过独创的 AAA 代理技术，为边界内的应用提供身份认证、预授权、集中审计的安全加固。	自主研发	原始创新	ZL200910092491.6	已授权	NetGate SSL VPN 网关、NetOpti 应用交付系统	成熟稳定成熟应用
					ZL201210425282.0			
					ZL201410043925.4			
					ZL201510960099.4	申请中		
15	网络设备虚拟化平台管理技术	使用自研的虚拟化管理技术，为各种不同种类的虚拟化网络设备提供统一的 NFP 平台，从而实现与云计算匹配的弹性网络配置，灵活资源管理，并提供高性能以及高可用性的网络虚拟化平台。可广泛用于各种私有云，公有云以及混合云的部署场景。	自主研发	原始创新	ZL201210241073.0	已授权	CCypher 云密码服务平台	成熟稳定成熟应用
					ZL201410281047.X	申请中		
					ZL201510714310.4			
					ZL201611175117.9			
					ZL201611238415.8			

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	专利状态	相关产品与服务	所处阶段
					ZL201911141172.X			
16	网络虚拟化平台的性能优化	在虚拟化平台中使用多种独创的网络性能优化技术，提升加解密运算和网络转发性能，从而解决传统云计算和 NFP 平台网络性能和加解密性能低的核心问题，实现大容量和高并发的网络虚拟化平台。	自主研发	原始创新	ZL201210585985.X	已授权	CCypher 云密码服务平台	成熟稳定成熟应用
					ZL201611238450.X	申请中		
					ZL201510551977.7			
					ZL201710063559.2			

（2）公司核心技术的先进性及具体表征

公司深耕信息安全行业近二十年，专注于以密码技术为基础支撑的信息安全产品的研发与创新。凭借优秀的技术研发团队和科技创新能力，截至本招股说明书签署日，公司共拥有 16 项核心技术，核心技术的先进性及具体表征如下：

1）网络密钥安全派生与协同签名技术

该技术创新性的提出了通过安全算法来保证用户密钥在移动终端的安全性，采用密码技术构建虚拟的安全边界，本技术总体思路：既然移动终端环境不安全，那么用户密钥在移动终端不存储，用户完整私钥数据在使用时也不完整在移动端出现。用户的完整私钥由移动终端、用户和服务端各自掌握一部分秘密信息，在使用时，移动端和服务端采用协同签名技术，移动端和服务端各自根据自己掌握的秘密信息派生各自的部分密钥，分段计算签名结果，最后组合各段签名结果为完整签名值。

该技术能够有效解决移动终端、物联网终端中的密钥安全保护和安全计算的问题。集成该技术的软件密码模块，已经通过了国家商用密码管理局的检测，获得了商用密码产品型号证书：SHM1705 移动安全中间件密码模块(证书编号：SXH2017265-1 号、SXH2017265-2 号)和 SHT1733 服务端协同签名平台(证书编号：SXH2017266-1 号、SXH2017266-2 号)，其中 SHM1705 移动安全中间件密码模块是达到安全等级第二级的密码软件模块产品，该技术处于国内先进水平。

基于该技术提供的安全解决方案相对于使用专用硬件认证设备的安全认证方案，降低了用户的成本，提高了用户的易用性。以极小的代价解决了移动互联网或物联网中的用户密钥安全管理及用户身份认证问题，可以帮助应用开发者快速接入移动安全或物联网安全解决方案，全方位保证开发者应用的安全性。

2）基于人工智能的用户行为分析鉴别技术

随着网上银行等电子商务应用的快速发展，用户对身份认证的便捷性要求越来越高。本技术利用终端设备内置传感器、加速度传感器、陀螺仪、方向传感器等等，多维度采集用户行为特征。行为特征进行识别的主要方法有：声音识别、笔迹识别、击键识别、用户站立、坐下以及其他运动行为特征，用户活动轨迹、时间节点活动特征、日常活动地点等信息。本技术在用户无感知的状态下持续深

度学习用户行为，持续多维度采集用户行为特征，为每个用户基于卷积神经网络和循环神经网络技术构建行为特征模型，并持续更新每个用户的行为特征库数据。在用户无感知的情况下对用户身份进行鉴别，将这一机制应用到大型业务系统中，分析用户的行为特征并利用大数据技术对用户行为特征进行细致研究，不断完善用户行为特征画像，提高身份鉴别的准确率。

该技术作为身份认证机制可以很好的提高设备的安全性，在实际应用中可操作性强，身份验证过程对用户透明，不干扰用户的正常使用操作，不需要增加额外的硬件开销。可以无缝的集成到现有的密码体系当中，实现对用户身份的二次认证，而基于触控滑动手势特征的身份识别，通过不断监听和收集用户手指与触摸屏交互产生的手势特征数据，实现对操作用户身份的持续性、动态性识别，确保智能手机中隐私数据的安全，弥补了传统静态身份识别方案仅在登录阶段认证的不足。

3）网络传输加密与处理技术

为了更好地适应互联网生态，网络传输加密产品需要尽可能少的影响已经建成的互联网生态，本技术采用目前业界比较通用的网络代理技术，支持标准的 HTTP 1.0、1.1、2.0 等协议标准，使用本技术后上不影响互联网业务，但获得了数据机密性、完整性保护，同时实现了用户对网站身份的认证。

本技术的特点：为应用系统提供多种应用安全方法支持，实现基于数字证书的身份鉴别和访问控制，可鉴别网站真实性和用户真实性；实现端到端的数据加密和数据完整性保护，能够有效防止用户隐私数据泄露；支持 SM2、SM3、SM4、RSA、AES、SHA2 等各类密码算法和多种网络协议；能够适应互联网生态的极致高性能需求并已在实际应用中得到验证。

采用该技术的网络安全加密产品已经通过了国家密码管理局商用密码检测中心的检测，获得了商用密码产品型号证书：SJJ1515 应用安全网关(证书编号：SXH2015087)。集成该技术的网络安全加密产品在“双十一”等各种高并发场景下经受了考验，已经证明能够满足用户对性能、稳定性及加解密等业务需求，因此该项技术具备一定的市场竞争优势。

4）基于安全套接层协议特征的加速负载分发技术

该技术创新性的提出了在不具备密码算法功能的负载均衡设备上实现对已经加密的流量进行分发的方法，本技术的总体思路：虽然加密流量难以分发，但加密流量不是凭空出现的，那么可以利用加密流量的上下文中的非加密流量的网络信息构建分发策略，再使用这些分发策略对后续的加密流量进行分发。

通过本技术的应用，负载均衡设备可以在不解密网络数据包的情况下实现对加密流量的分发，既能解决流量分发的问题，又无须增加使用加解密技术带来的成本增加、避免负载均衡产品复杂性的提升、降低负载均衡设备因增加加解密处理带来的性能损坏，可谓“一举多得”。发行人拥有该项技术的发明专利，了解相关技术实现细节，处于该技术竞争的国内领先地位。

发行人该技术已经应用于负载均衡产品中，能够有效的降低负载均衡产品使用密码运算部件的频率，在同等配置条件下获得更高的负载分发效率，使发行人的产品具有一定的竞争优势。

5）云架构密码分发与权限控制技术

随着云计算、大数据技术的迅猛发展，越来越多的机构采用云计算技术架构来建设数据中心和信息系统，如何在云计算架构下获得与非云计算架构等同或相近的安全特性，特别是密码安全特性，是一个重大的挑战。

该技术采用密码卡虚拟化技术，通过虚拟密码卡构建虚拟典型密码服务。虚拟密码卡是利用硬件虚拟化技术，将一块物理密码卡虚拟为多块（如 8 块、16 块等），同时实现这些虚拟密码卡的安全隔离，使得用户在使用虚拟密码卡时就像使用物理密码卡一样独占密钥管理权限，其他用户也不能发现别人的虚拟密码卡的存在，典型密码服务在使用时，也无须区分虚拟密码卡与物理密码卡，从而实现典型密码服务的无缝迁移和安全隔离。由于密码卡虚拟化的数量受物理条件的限制，在出厂时就已经限定了虚拟化的最大数目，为了更加灵活的使用密码卡的资源，在密码卡实现虚拟化基础上设计了一套完整的密钥分发和权限控制方案，从宿主机动态调度虚拟密码卡，实现密码资源的高效复用。

该技术作为云计算环境下密码虚拟化方案已经得到业内密码专家的认同，具有很强的可操作性，可以快速实现用户密码设备弹性扩展、按需使用，能够满足目前缺少既安全合规又适应云计算环境的密码解决方案的需求。

6）数字证书与加密协议格式的快速解析和判定技术

数字证书是公开密钥基础设施（PKI）技术的重要组成部分，所谓数字证书，实际上是一段数据，数字证书通常包括：所有者的公钥、所有者的名字、公钥的失效期、颁发机构的名称（发放数字证书的 CA）、数字证书的序列号、颁发机构的数字签名等。数字证书在编码时一般采用基本编码规则（BER）或非典型编码规则（DER）编码。

对于使用 ASN.1 进行编码的数字证书与加密协议格式，典型的处理方式都是按照 ASN.1 的定义，将数字证书或加密协议的数据进行逐层解析，直至将所有数据结构都处理完成，然后构造一个整体的数据结构供应用系统访问和处理。发行人的技术突破这种常规处理方法，采用“惰性”处理的思想，在进行 ASN.1 数据解析时，先对数字证书结构进行整体快速扫描后，依据实际解析需要，对于应用暂时不需要的数据域不进行解析，从而大大提高解析效率实现快速解析。

发行人该项技术能够有效提高数字证书、证书撤销列表和加密协议 ASN.1 的处理效率，减少程序处理时间、CPU 和内存占用，能够让发行人产品在同等配置条件下获得更好的性能，并已经成功应用于发行人产品中，使发行人产品具有一定的竞争优势。

7）移动威胁态势感知技术

本技术会采集与移动安全紧密关联的海量异构数据，包括移动设备动态信息、移动设备静态信息、移动运行环境信息、移动设备设置信息、移动设备安全信息、移动应用异常信息等移动终端安全信息；分布在用户网络中的公司现有设备搜集的与安全态势相关的信息与数据；业务服务器日志、业务告警数据、业务安全操作数据等业务类日志；IP 信誉库、恶意域名库、恶意 URL 库、恶意文件 Hash 等第三方威胁情报数据，并对这些数据进行归类存储，同时提供分析引擎和编程接口。

通过本技术提供的分析引擎和算法库，实现对移动操作系统漏洞、开放端口、黑客入侵、web 攻击、APP 攻击、威胁情报、企业安全舆情等全方位的监控，及时预警或预测威胁态势；通过机器学习等人工智能算法对海量样本进行自动化关联分析，确认攻击手段、攻击对象以及攻击目的；通过人工智能结合大数据知

识以及攻击者的多个维度特征还原出攻击者的全貌，包括程序形态，不同编码风格和不同攻击原理的同源木马程序，恶意服务器（C&C）等；通过全貌特征跟踪攻击者，做到攻击的精准预测和精准溯源。

通过本技术的利用，将原本碎片化的资产情况、网络情况、业务情况、威胁告警、异常行为告警等数据结构化，形成统一的可视化方案，以便于用户可以更直观地感知移动网络运行情况和安全态势。

8）高性能动态可配置的 API 网关技术

在多密码业务应用场景需求下，API 网关通过提供统一的 RESTFul API 来屏蔽密码硬件的差异，从而为客户应用系统提供统一的密码运算开发接口来集成密码安全服务。不同密码硬件的 API 接口形式不同，有的通过 SDK 提供 TCP 访问接口，有的提供 API 接口，即使是相同的接口，也存在接口参数不同的情况。针对这种情况，网关服务提供协议转换插件开放能力。由开发人员根据后端服务接口开发不同的 API 转换组件，通过管理中心发布即可动态生效。网关对于稳定性和性能要求非常高，不允许因个别 API 响应缓慢或者无法提供服务导致整个网关堵塞。本技术基于 Hystrix 自反馈调节熔断状态的算法原理，设计服务出错降级处理机制。当在一定时间段内 API 网关调用后端密码设备提供的服务的次数达到设定的阈值，并且出错比例达到设置的阈值，就会触发服务降级，由 API 内部执行本地降级策略，不再发起远程调用。而且 Hystrix 提供的熔断器具有自我反馈、自我恢复的功能，它会根据调用接口的情况，让熔断器在 closed、open、half-open 三种状态之间自动切换。这样就能够在某些服务故障时，网关自动降级，而当该服务恢复之后，系统能够恢复到正常状态。

本技术的特点：采用 API 转换组件动态加载的方法，为客户应用开发人员提供统一的 RESTFul 风格 API 接口，屏蔽不同设备接口多样性问题，显著提升应用集成开发速度。采用令牌桶的限流方案，在统一配置平台上配置 API 流量阈值，当流量超过阈值，新来的请求会被网关拦截，确保后端服务可以正常运行。通过服务出错熔断机制，显著降低分布式系统架构中多个系统之间远程 RPC 调用，当尾部应用发生故障导致连锁反应造成的雪崩现象，提升系统的运行稳定性和容错自恢复能力。

本技术在 API 网关统一解决微服务集群的认证、鉴权、流量管控、熔断、灰度发布等问题，提升运维管控效率，在保障系统安全接入的基础上，构建高性能、高可靠稳定运行能力。在网关层实现服务路由和协议转换，系统可以通过插件化方案适配后端不同接口服务，对于新设备的接入，可以动态发布插件支持，不同热插拔技术极大满足行业客户业务连续性要求。

9）基于时序数据库分布式业务监控技术

密码安全服务平台在运行时汇总和监控各种状态，实现平台大数据分析和预警。该应用需求会对大数据的存储和查询带来极大挑战，首先，平台数据需要存储海量数据。其次，监控系统对监控指标变化要求非常灵敏，需要支持在持续高并发入库的同时支持高频率查询。由于关系型数据库天生的劣势导致其无法进行高效的存储和查询。通过时序数据库使用特殊的存储方式，可以高效存储和快速处理海量时序大数据，是解决海量数据处理的一项重要技术。本技术采用特殊数据存储和索引方式，提高数据的处理能力。相对于关系型数据库它的存储空间减半，查询速度提高数倍。时间序列函数优越的查询性能远超过关系型数据库，适合在监控预警分析领域的应用。

时序数据会按照指定的时间粒度持续写入，支持实时、高并发写入，无须更新或删除操作。支持各种按照时间聚合函数操作，可以方便开发人员输出各种监控指标趋势和报表。

本技术支持海量监控指标数据高效存储，快速查询，支持 Grafana 报表平台对接，提供自定义报表开发接口。本技术可自定义告警规则和告警阈值，通过接口支持丰富的可视化统计报表。本技术支持基础资源监控，让用户全局掌控服务器、网络、存储资源和应用服务状态。支持多平台环境及主流服务器、存储、网络设备，实时采集与分析近千种性能指标。

10）高效安全的容灾技术和集群技术

业界对于硬件服务器容灾技术采用基于开源软件实现心跳服务和集群通信等技术，但对于安全产品，特别是加载安全硬件模块的安全产品，缺乏相应的安全防护机制来满足密钥安全性和业务的高效性。如何在硬件安全主机容灾和集群技术，保证稳定可靠地高性能安全数据传输是业界面临地挑战。

发行人通过对硬件安全产品密钥运算主运算卡与多个待同步运算卡快速协同同步技术以及数据网络镜像技术，实现了运算卡密钥及安全配置数据等容灾和集群技术，保证产品的高性能、稳定性和可靠性，能够有效解决业界面临的挑战。该技术难度高，复杂度大，对研发人员技术能力和创新能力要求极高，不仅需要对网络协议要深入了解细节，还要对包括硬件加密模块（HSM）在内的安全防护技术有全面深刻的理解，同时要对密钥安全管理业务需求有精准把握，这些都需要长期的技术积累才能完成。

不同于业界普遍采用的基于开源软件技术进行优化的做法，发行人自主研发的高性能网络产品系统底层架构技术在性能上，对加密运算卡进行性能和功能优化，同时采用智能同步多台设备上配置的安全数据，支持多种同步策略从而取得领先于业界同类产品的性能优势。同时因为是完全自主研发同步协议和机制，在容灾和集群功能时更加灵活和方便，不受制于开源软件，可以更加快速全面的满足客户日益增长的各种容灾和集群需求。

11）高性能网络产品架构技术

业界对于二层、三层网络设备普遍采用 ASIC、FPGA 或者网络处理器等专用硬件加速技术，但对于四层 TCP/UDP 协议和应用层 HTTP/HTTPS 协议，因为协议本身的复杂度和应用的灵活性，没有相应的专用硬件加速技术可以满足要求。业界普遍采用的是通用 CPU 硬件架构。如何在通用 CPU 架构上进行软件架构设计，保证稳定可靠地高性能数据传输是业界面临的挑战。

发行人通过独创的高性能网络产品架构技术，自行研发设计了具有自主知识产权的 TCP/IP 协议栈和应用层协议栈，保证产品的高性能、稳定性和可靠性，能够有效解决业界面临的挑战。不同于业界普遍采用的基于开源软件技术进行优化的做法，发行人集中研发力量深入研究各种网络协议规范，结合通用的多核 CPU 架构，完全自主研发了多核并行无锁化高速协议栈。该协议栈相比于开源软件和一般产品，性能有着大幅度的提升，达到了业界的领先水平。

与业界普遍采用的基于开源软件技术进行优化的做法相比，该技术在性能上可以完全发挥多核 CPU 硬件的潜力，从而取得领先于业界同类产品的性能优势。同时因为是完全自主研发的协议栈，在增加用户需要的各种功能时更加灵活和方

便，不会受制于开源软件固有架构，可以更加快速全面的满足客户日益增长的需求。在客户进行的产品比较测试中，因为使用了高性能网络产品架构技术，公司产品不仅满足了客户的各种功能需求，而且在性能上表现出了巨大的优势。

12）智能流量学习和应用识别技术

传统安全产品对基于流量的Flood攻击通常采用根据经验值进行手工阈值配置的方式，对于应用类型识别也常常手工进行配置，这需要用户有很强的专业知识和丰富的运维经验，给用户使用带来很多麻烦，同时容易产生错误。用户迫切希望安全产品能够对此进行改进，减少用户的人工操作，简化日常运维的复杂度。

发行人独创的智能流量学习和应用识别技术，通过集中研发力量深入研究各种流量模型和应用模型，提炼出了快速有效的核心识别算法。该算法创新性强，复杂度大，对研发人员技术能力和创新能力要求极高，不仅需要熟悉各种机器学习算法，还要对各种流量模型和应用模型有深入研究，同时要对网络协议和操作系统架构有全面深刻的理解，这都需要很深的技术积累才能完成。该技术显著降低了用户运维安全产品的复杂度，有效缓解了安全产品配置难，专业知识经验要求过高的问题。

发行人使用独创的智能流量学习和应用识别技术，自行研发设计了具有自主知识产权的机器学习软件模块，为安全产品提供了智能大脑。与传统安全产品相比，大大简化了运维人员的操作复杂度，降低了对运维人员专业技能和经验的苛刻要求，提升了运维的便利性和安全性。安全产品的运维是客户选购安全产品考虑的重要因素，该技术切实解决了客户痛点，受到了客户的广泛认可。

13）远程安全接入技术

远程安全接入是企业边界安全访问防护中的重要一环，企业的不同业务部门对安全接入的需求是不同的。在公司统一安全策略的前提下，各个部门希望能够独立管理本部门的特定安全访问策略，对接入的用户进行多维度的精细化管理。

安全接入网关通过独创的软件虚拟化技术，实现多个虚拟的安全服务站点。每个服务站点为一个业务部门或者一个用户群提供安全接入。通过严格的逻辑设计，保证每个虚拟服务站点相互独立，拥有独立的配置管理、接入策略、接入方法和内部资源。另外，为满足企业更高级别的安全要求，可根据每个用户其所属

位置、终端属性和所属角色等分配不同的安全访问策略。

安全接入网关单个硬件设备支持最大支持 256 个虚拟服务站点和最大 128,000 并发用户，支持传统的 PC 接入、移动终端接入和物联网设备等多种接入方式。不仅保证了安全还大大地提高了生产效率，该项技术在国内处于领先位置。

14）零信任边界安全保护技术

随着移动互联网、云计算和 IoT 等技术的不断发展，现代企业的数据和应用已经不再局限在企业内网，企业边界已经不复存在，传统的由防火墙实施物理边界防御和 VPN 创建安全传输隧道加密访问数据的安全方式已经无法适应企业的安全需求。新一代 Software Defined Perimeter（软件定义边界，即 SDP）的零信任安全模型已经越来越广泛地被接受，并成为近几年网络安全的热点。

该技术支持多因子身份认证、国密端到端加密和基于角色的精细化的动态访问控制，细粒度访问控制用户获得授权后，内网依然不可见，大大提高了安全性，满足了现代无边界企业对安全的新需求。通过与企业 IAM 联动和对各类 SSO 接口的支持，相比于传统 VPN，提供了更好的安全性、可维护性和可扩展性。该技术是安全网关产品区别于一般 IPsec VPN 和 SSL VPN 产品的一个重要方面。

发行人基于 SDP 安全模型打造了一体化的零信任边界安全网关功能，该功能将软件定义边界技术和公司业界领先高性能 SSL 处理平台软件相结合，通过端口映射和域名映射的方法实现了 Web 应用的安全发布，有效避免了对 Web 响应内 HTML 和 JavaScript 繁琐代码的解析，提高了 Web 应用的安全访问速度。零信任边界安全网关还可与大数据智能安全运营平台相结合，形成了新一代的边界防御解决方案。

15）网络设备虚拟化平台管理技术

云计算和虚拟化是近年来网络技术发展最为迅速的技术方向之一。其中，虚拟化以其可以提供弹性计算的能力，成为云计算的关键技术。网络虚拟化功能可以通过软硬件解耦及功能抽象，可以降低网络昂贵的设备成本，使网络资源可以充分灵活共享，实现新业务的快速开发和部署，弹性伸缩、故障隔离和自愈等。但是，对比已经很成熟的计算虚拟化和存储虚拟化技术，网络功能虚拟化技术进

展较为缓慢，因为网络功能虚拟化和计算资源虚拟化在技术实现和技术要求上有很大的不同，有其独特的技术难点需要克服，所以，如何使网络虚拟化技术得到实际应用是提升云计算的效率和自动部署的关键问题。

本技术以网络虚拟化技术作为基础，提出了独特的网络设备虚拟化平台(NFP 平台)。此平台可以实现与云计算匹配的弹性网络配置，资源管理灵活，并提供高性能以及高可用性的网络虚拟化平台。可广泛用于各种私有云、公有云以及混合云的部署场景。

使用此技术提供的 NFP 平台，不仅提供了成熟的网络虚拟化技术，更重要的是将平台上虚拟出的各种不同的网络设备有机的融合成为服务功能链进行管理。此技术可以在 NFP 平台和设备本身提供独特的两级高可靠性保证；可以与 SDN 等技术可以实现无缝对接，从而用于各种云环境的自动部署；整合了不同的网络设备，实现了服务功能链；通过这些独特优势，能够缩短网络运营的而业务创新周期，提升投放市场的速度，是云服务商或者使用者极大的减少网络成熟周期。

16）网络虚拟化平台的性能优化

网络设备最重要的特点是需要超高的数据包处理能力，而在虚拟化技术中，因为在虚拟化过程中对网卡进行了虚拟封装，所以数据包的处理速度受到严重影响。这也是影响网络虚拟化技术落地的最困难的因素。尤其是当前互联网上的流量中，使用 SSL 作为加密的流量越来越大，而 SSL 数据加解密的处理是当前传统专用网络设备中较难解决的课题之一。那么，使用通用服务器设备的虚拟化平台能否为 SSL 提供高处理性能变得非常关键。如果网络虚拟化产品无法提升在数据包转发和 SSL 流量处理上的性能，将会无法在需要处理海量数据的云计算环境中得到广泛使用。

本技术正是综合使用多种独创的网络性能优化技术，大幅度提高网络虚拟化平台上网络数据转发和 SSL 加解密的处理能力，达到了在虚拟平台上可以获得专有硬件设备相似的性能指标。同时，通过在平台上把 SSL 卡的资源进行虚拟化，提供给各种虚拟网络设备使用，可以把 SSL 的处理能力提升 5-10 倍以上。从而解决传统的网络虚拟化产品网络性能和加解密性能低的核心问题，实现大容

量和高并发的网络虚拟化平台设备。

通过提升网络数据转发性能和 SSL 数据处理性能，使 NFP 平台可以在云计算环境中替代传统的硬件设备得到广泛应用。从而能保证网络处理性能的情况下同时提升云计算的自动部署以及弹性资源扩展等能力，实现真正意义的全虚拟化自动部署。

（3）公司来源于核心技术的收入金额和占比情况

公司信息安全产品分为身份安全、数据安全、通信安全、移动安全、云安全和平台安全六大系列产品线，上述产品及相关技术服务的销售收入均来源于公司的核心技术。

报告期内，公司来源于核心技术的收入占营业收入比例如下表所示：

单位：万元、%

项目	2019 年度	2018 年度	2017 年度
来源于核心技术的销售收入	30,483.09	25,378.84	20,671.14
营业收入	31,783.90	26,934.15	22,044.13
占营业收入的比例	**95.91**	**94.23**	**93.77**

（3）核心技术保护措施

公司为保护核心技术和知识产权，防范核心技术人员流失，成立了安全管理委员会。负责建设公司信息安全体系，监督公司信息安全运行，同时也对核心技术人员提供有竞争力的薪酬待遇、股权激励等激励机制。

公司的安全管理委员会是由总经理为首、各安全事务归口负责人为辅、各部门负责人参与的安全管理组织，包括物理与环境、资产与系统建设、访问控制、操作安全和供应商安全管理，并持续关注信息安全事态和事件管理，保证信息安全制度的可用性和持续性。

公司具体技术保密措施：

1）所有员工入职时签订《劳动合同》、《知识产权及保密协议》，确定任职期间的知识产权归属，承诺保守公司的技术秘密或商业秘密信息。调离岗位时，必须移交其掌握的商业秘密、核心技术资料，工作电脑在信息安全小组的监督下做好清理工作；

2）核心技术人员在接受公司重要研发任务或客户的重大项目时，应根据需要签订《保密责任书》，明确应当承担的保密责任和应履行的保密义务；

3）公司的物理区域分为普通区域和安全区域。安全区域包括但不限于研发和生产区域，安装有独立的门禁系统，配置了视频监控系统等安全保障设备。

2、在研项目

目前公司正在从事的研发项目具体情况如下：

项目名称	研发子项目	所处阶段	项目人员	预算投入（万元）	预计达到的目标	研发项目及成果技术水平	研究领域
云安全服务密码关键技术研究项目	全同态加密算法应用技术	目前已初步完成已知同态密码算法研究与实现。	汪宗斌、秦体红等 5 人	400	完成基于国产密码算法的全同态密码算法实现，并根据实际应用场景完成全同态加密算法在数据加解密系统中的应用。	1、实现接入云端基于同态加密算法的快速加解密； 2、基于同态加密算法数据的快速索引； 3、实现国产密码算法替代。	云计算存储； 多行业数据加解密。
	云计算架构密钥存储与分发技术	已完成关键技术的研究，产品已投入市场，处于稳定开发优化阶段。	汪宗斌、刘金华、陈程等 30 人	1,405	实现 CCypher 云密码服务平台对密钥高安全性存储以及租户和业务系统密钥安全分发和使用。	1、通过 SR-IOV 技术，保障平台内虚拟化密码应用服务与传统物理设备性能的一致性和安全性 2、与主流 Openstack 框架云架构已完成对接； 3、配备独立的云密钥管理系统，具备身份认证、用户管理和监控等功能。	云计算密码服务应用领域。
物联网关键密码技术研究	物联网轻型密码算法应用技术	目前已完成对国产品算在物联网应用的优化阶段。	汪宗斌、马姚、刘金华等 20 人	1,360	实现基于国产密码算法改造的物联网轻型算法，该算法具备物联网感知层低端设备的安全存储与运算功能。	1、实现感知层国产密码算法的加密签名以及通道加密功能； 2、实现感知层基于硬件模组和密码模块的密钥数据的安全存储； 3、实现物联网海量感知层与物联网平台安全接入，接入速率<0.5 秒。	物联网终端领域。
	物联网高速安全传输技术	已完成关键技术的研究，产品已投入市场，处于稳定开发优化阶段。	汪宗斌等 10 人	930	优化已有的 NSAE 应用安全网关，实现客户端海量感知层数据与物联网平台的安全传输。	1、HTTP2.0、TLS1.3 协议支持 2、目前国密算法单台设备 SSL 连接 18KTPS； 3、对 GZIP、DEFLATE 进行高效压缩，实现 HTTP 报文的压缩和解压缩代理功能；	物联网平台接入领域。

项目名称	研发子项目	所处阶段	项目人员	预算投入（万元）	预计达到的目标	研发项目及成果技术水平	研究领域
						4、感知层终端 API 接口更易用，TLS 安全连接更快速。	
	物联网安全态势感知技术研究与应用	目前项目已初步完成相关模型与关键技术的研究，相关产品已投入市场，处于稳定开发优化阶段。	魏巍、孙波等 10 人	685	通过轻型算法适配更多物联网感知层终端安全接入；提高物联网终端接入威胁感知准确率；优化态势感知平台的数据模型何分析算法，提高威胁信息分析的准确度。	1、高效的基于端口与协议识别技术； 2、实现对加密流量恶意攻击行为智能研判，目前针对扫描探测、暴力破解、CC 攻击进行分钟级快速定位识别； 3、可实现在基于 IP 主动追踪溯源系统，精准溯源定位攻击者。	物联网态势感知领域。
工业控制密码关键技术研究项目	工业互联网软件平台安全接入	基础研究阶段	胡进、郑军等 15 人	1,340	完成工业互联网平台终端设备安全接入，应用商用密码在接入软件的类型识别、权限控制等认证管控与通讯加密传输。	1、实现对接入平台亿级终端快速识别； 2、实现对终端权限控制与访问控制； 3、平台实现 20KTP 终端快速安全接入，保障数据通信安全性。	工业互联网领域。
	工业互联网标识解析安全防护技术	基础研究阶段	刘金华、戴京川等 15 人	1,130	结合标识解析体系的树状结构，基于 CA 认证中的证书 链验证和数字签名/验签技术。实现父子节点系统的身份 验证、解析数据完整性校验。有效的防止子节点系统被 劫持冒用，解析数据被非法篡改的安全风险。	1、实现对标识解析数据上报的安全加密以及完整性保护； 2、实现上报数据基于数字签名技术的不可否认； 3、实现基于上报数据的安全通道加密。	工业互联网领域。
智能网联汽车身份认证体系研究	智能网联汽车身份认证体系	已完成关键技术的研究，产品已投入市场，处于稳定开发优化阶段	胡进、郑军等 15 人	1,305	建设智能网联汽车行业 V2X 安全认证防护体系，实现车车车路通讯信息完整性、真实性防护和隐私保护，并结合 V2X 通信的高移动性特点及低时延要求，实现 V2X 安全认证系统。	1、实现对车联网基于 IEEE1609.2 标准隐式证书支持 2、实现国产算替代； 3、实现多行业 CA 的管理 4、支持十亿级别证书与密钥存储。	智能网联汽车领域。
密码安全态	基于加密设	已完成关键技	魏巍、孙波	745	通过对安全设备的网络流量、脆弱	研发密码安全态势感知平台从用户	态势感知

项目名称	研发子项目	所处阶段	项目人员	预算投入（万元）	预计达到的目标	研发项目及成果技术水平	研究领域
势感知研究	备流量检测与态势预警平台	术的研究，产品已投入市场，处于稳定开发优化阶段	等 10 人		性、安全事件何威胁情报等数据，利用大数据何机器学习技术，分析网络行为及用户行为等因素构成的整个网络状态，研究和设计网络加密流量检测框架和关键技术，对网络空间面膜应用进行全面有效监控审计和管理；规避密码应用风险。	密码应用场景化需求出发，从终端自身系统进行防护、通道加密、数据安全防护和感知，基于多维度的原始终端数据，采用自适应的安全防护技术架构，可初步实现密码应用行为的全链条追溯、全态势的感知与管控。	领域。
	态势感知数据密码可视化技术	已完成关键技术的研究，产品已投入市场，处于稳定开发优化阶段	魏巍、孙波等 10 人	740	对密码应用安全数据进行深入的观察和分析。提供直觉的、可交互的和反应灵敏的可视化环境；降低用户的人工勘测成本，提升安全运维效率。	实现基于大屏多维度展现，实现多种格式报表内容展现与输出。	态势感知领域。
下一代 SSL 应用安全网关	下一代 SSL 应用安全网关	已完成关键技术的研究，产品已投入市场，处于稳定开发优化阶段	贝少峰，孙冬冬等 15 人	1,000	迁移到新硬件平台，实现多 CPU 并发调度处理，基于新的 CPU 和网络适配器虚拟化功能，升级多 CPU 软件架构，实现更高性能的 CPU 并发调度，并实现虚拟化场景下对不同租户使用的隔离机制，保证不同业务或租户之间的数据隔离。	1、实现算法与安全协议优化，对应用数据在网络传输和存储过程中进行加解密快速处理； 2、实现基于压缩、缓存、安全套接层协议优化在内的服务器加速负载分发技术。	信息安全 SSL 通讯传输领域。

3、研发投入情况

为保持技术领先优势，增强公司的核心竞争力，公司高度重视技术和新产品的研发工作。报告期内，公司研发支出分别 2,617.97 万元、2,940.11 万元、4,496.88 万元，占营业收入比例分别为 11.88%、10.92%、14.15%。

报告期内，公司研发费用的构成及占营业收入的比例如下：

单位：万元，%

项目	2019 年度	2018 年度	2017 年度
研发支出	4,496.88	2,940.11	2,617.97
营业收入	31,783.90	26,934.15	22,044.13
占比	14.15	10.92	11.88

4、研发人员和核心技术人员情况

（1）公司研发人员情况

截止 2019 年 12 月 31 日，公司拥有研发人员 260 人，占总人数 40.75%。公司主要研发人员具有丰富的专业理论知识和实践操作经验。报告期内主要研发人员未发生重大变动。

（2）核心技术人员情况

报告期内，公司的核心技术人员共 6 人，为王翊心、张庆勇、胡进、汪宗斌、刘金华、乔海权。报告期内，公司核心技术人员没有发生变化。

（3）核心技术人员取得的专业资质以及对公司研发的具体贡献情况

序号	姓名	参与专利情况
1	王翊心	一种网络交易认证系统和网络交易认证方法、一种基于 SM2 签名算法的复核签名方法和数字签名设备、一种网络交易数字签名方法和装置、一种基于安全套接层协议特征的负载分发方法、一种网络身份认证方法；一种保护网站的方法及装置、一种智能身份认证系统、一种程序文件验证方法及程序文件验证装置、一种防止重放攻击的技术、一种会话保持方法和装置、一种安全防护的方法及装置、一种访问认证方法及对应装置、一种证书吊销列表查询方法及装置、一种数据同步方法、装置和设备。
2	张庆勇	一种令牌种子的更新方法、装置和相关设备、一种网络协议数据包的安全处理方法和系统、数字证书同步方法、数字签名服务器及数字证书同步系统、数字证书同步方法、数字签名服务器及数字证书同步系统；一种智能身份认证系统、云存储安全网关及访问方法、在移动平台上快速打开信息安全设备应用的方法及系统、数字证书同步方法、数字签名服务器及数字证书同步系统、一种数据写入的方法及装置、一种会话保持方法和装置、一种客户端和服务端协作生成数字签名的方法、一种运算卡监控系统、方法及相关设备、

序号	姓名	参与专利情况
		基于应用系统的角色在统一认证平台反向授权方法及系统、一种安全防护的方法及装置、一种访问认证方法及对应装置、一种代理多后台认证识别的技术、一种门限密钥的管理、一种双方协作生成数字签名的方法、一种文件的签署方法、验证方法及装置、一种证书吊销列表查询方法及装置、一种数据同步方法、装置和设备、一种服务器日志分析的方法及装置、一种单点登录的方法、系统、装置及认证方法、一种 SSL-TLS 安全参数协商方法和系统、一种远程解锁安全设备的方法及装置、一种应用程序登录方法及装置、证书认证系统、证书认证系统的部署方法和证书认证方法、一种多方协同完成双向 SSL 认证的方法。
3	胡进	一种网络交易认证系统和网络交易认证方法、一种基于 SM2 签名算法的复核签名方法和数字签名设备、一种网络交易数字签名方法和装置、一种网络协议数据包的安全处理方法和系统、一种用户敏感信息的保护方法和系统、一种数字证书的申请方法、一种多功能认证设备、一种可充放电的认证设备；一种客户端和服务端协作生成数字签名的方法、一种门限密钥的管理、一种双方协作生成数字签名的方法、一种 SSL-TLS 安全参数协商方法和系统、一种基于 CSP 接口实现远端设备密码服务的方法和系统、一种多方协同完成双向 SSL 认证的方法、一种增强 SSL/TLS 协议中随机数随机性的方法、一种将移动端与客户端关联的方法。
4	汪宗斌	一种数字证书的快速处理方法、一种基于安全套接层协议特征的负载分发方法、一种网络身份认证方法、私钥的生成方法及装置；一种保护网站的方法及装置、一种智能身份认证系统、云存储安全网关及访问方法、基于应用系统的角色在统一认证平台反向授权方法及系统、一种服务器日志分析的方法及装置、基于 SM2 算法的协同签名的方法、装置及存储介质、双方协同生成 SM2 算法的签名方法、装置及存储介质、一种口令更新方法、装置及系统、跨浏览器的签名 license 控制方法、通信的方法、装置、路边设备、车辆和存储介质、通信的方法、装置、路边设备和存储介质。
5	刘金华	一种程序文件验证方法及程序文件验证装置、一种密钥保护方法及 PKI 系统、证书认证系统、证书认证系统的部署方法和证书认证方法。
6	乔海权	一种网络协议数据包的安全处理方法和系统、一种 SSL-TLS 安全参数协商方法和系统、一种基于 CSP 接口实现远端设备密码服务的方法和系统。

（4）核心技术人员实施的约束激励措施

核心技术人员均与公司签订了《劳动合同》、《知识产权及保密协议》，确定任职期间的知识产权归属，承诺保守公司的技术秘密或商业秘密信息。公司对核心技术人员实施了股权激励，核心技术人员直接持有或通过员工持股平台间接持有公司股份。

（四）近三年主要财务数据和财务指标

1、资产负债表主要数据

单位：万元

项目	2019 年 12 月 31 日	2018 年 12 月 31 日	2017 年 12 月 31 日
资产总计	55,862.70	39,981.88	27,575.53
其中：流动资产	39,741.30	33,558.69	22,933.83

项目	2019 年 12 月 31 日	2018 年 12 月 31 日	2017 年 12 月 31 日
固定资产	4,608.66	1,767.94	936.23
无形资产	1,809.55	228.44	259.24
负债总计	21,020.61	10,796.58	9,330.11
其中：流动负债	18,811.43	9,433.21	8,033.88
所有者权益	34,842.09	29,185.30	18,245.42
其中：归属母公司的所有者权益	34,762.72	29,185.30	18,245.42

2、利润表主要数据

单位：万元

项目	2019 年度	2018 年度	2017 年度
营业收入	31,783.90	26,934.15	22,044.13
营业利润	9,778.58	9,170.03	5,762.68
利润总额	9,867.20	8,841.91	5,394.30
净利润	9,158.07	7,809.56	4,742.65
其中：归属于发行人股东的净利润	9,034.80	7,809.56	4,746.69
扣除非经常性损益后归属于发行人股东的净利润	8,661.04	8,173.42	5,913.75

3、现金流量表主要数据

单位：万元

项目	2019 年	2018 年	2017 年
经营活动产生的现金流量净额	7,867.83	4,978.35	185.03
投资活动产生的现金流量净额	-1,138.59	-11,905.75	1,508.03
筹资活动产生的现金流量净额	-2,812.20	2,735.36	2,555.14
现金及现金等价物净增加额	3,916.76	-4,192.03	4,248.20

4、主要财务指标

财务指标	2019.12.31/ 2019 年度	2018.12.31/ 2018 年度	2017.12.31/ 2017 年度
流动比率（倍）	2.11	3.56	2.85
速动比率（倍）	1.77	3.03	2.19
资产负债率（合并）（%）	37.63	27.00	33.83
资产负债率（母公司）（%）	25.17	25.67	40.85
应收账款周转率（次/期）	1.92	2.35	3.31
存货周转率（次/期）	1.77	1.61	1.60

财务指标	2019.12.31/ 2019 年度	2018.12.31/ 2018 年度	2017.12.31/ 2017 年度
息税折旧摊销前利润（万元）	10,379.22	9,208.25	5,666.21
归属于公司普通股股东的净利润（万元）	9,034.80	7,809.56	4,746.69
扣除非经常损益后归属于公司普通股股东的净利润（万元）	8,661.04	8,173.42	5,913.75
研发投入占营业收入的比例	14.15%	10.92%	11.88%
每股经营活动产生的现金流量（元）	1.13	0.71	0.03
每股净现金流量（元）	0.56	-0.60	0.67
归属于公司普通股股东的每股净资产（元）	4.98	4.18	2.86

（五） 发行人存在的主要风险

1、产业政策风险

2013 年以来，国家相继发布了《国家安全法》、《网络安全法》和《密码法》等重要法律法规，将信息安全提升到国家战略层面；并制定了《“十三五”国家信息化规划》、《软件和信息技术服务业发展规划（2016－2020 年）》、《关于推动资本市场服务网络强国建设的指导意见》等多个产业政策，从多个层面促进国内信息安全产业的发展，一系列法律法规和鼓励行业发展的产业政策，为信息安全行业发展营造了良好的政策环境。如果未来国家产业政策发生重大不利变化，将会对公司业务发展和经营业绩产生一定的影响。

2、经营风险

（1）市场竞争风险

随着国家政策的大力支持，各行业应用领域的逐步深化以及移动互联网、云计算、大数据、工业互联网等新兴技术的不断发展，催生了新的信息安全需求，信息安全行业将迎来更加快速的增长。虽然公司在信息安全行业处于领先地位，并逐步形成了身份安全、通信安全、数据安全、移动安全、云安全和平台安全六大产品系列，但目前市场参与者较多，市场集中度较低，随着越来越多的企业参与到行业中，公司将面临更为严峻的市场竞争和挑战。

（2）经营业绩季节性波动风险

公司信息安全产品的主要用户为金融、政府、企业、电信运营商。受农历春

节假期、预算审批流程的影响，金融、政府、企业、电信运营商通常在每年的第一季度制定全年的信息安全产品采购计划并确定预算额，后续需经历采购方案制定、询价、确定供应商、合同签订、合同实施等步骤，因此信息安全产品的客户通常集中在下半年特别是第四季度完成产品的交付和验收。受此影响，公司的销售收入通常具有上半年尤其是第一季度较低、下半年尤其是第四季度较高的特点，而公司主营业务毛利率各季度变化相对稳定，管理费用、销售费用等各项费用在各季度相对均衡，因而公司的经营业绩存在较强的季节性波动风险。

（3）人力资源风险

信息安全行业作为知识密集型的高技术行业，对从业人员的综合素质和行业经验要求较高。随着行业应用领域的不断拓展、新业务模式的出现以及新产业形态带来的产业变革，对高端人才的需求持续增长，因此高端人才的储备是企业竞争力的关键。随着公司经营规模的扩大以及募集资金投资项目的建设，未来一段时间公司对于高素质人才的需求将持续增长。如果公司在技术研发、产品规划、方案咨询等方面的人才储备不能满足公司业务快速发展的需求，将对公司的经营带来不利影响。

（4）无法取得商用密码产品认证证书的风险

国家密码管理局、市场监督管理总局于 2019 年 12 月 30 日发布公告：根据《密码法》的规定，2020 年 1 月 1 日起不再受理商用密码产品品种和型号申请，停止发放《商用密码产品型号证书》；自 2020 年 7 月 1 日起，已发放的《商用密码产品型号证书》自动失效；对于有效期内的《商用密码产品型号证书》，持证单位可于 2020 年 6 月 30 日前，自愿申请转换国推商用密码产品认证证书，经认证机构审核符合认证要求后，直接换发认证证书。

就上述换发商用密码产品认证证书事宜，发行人已于规定时限按要求将相关申请材料邮寄至北京市密码管理局，目前正在等待北京市密码管理局的进一步通知。根据《密码法》及上述公告的规定，发行人已取得的《商用密码产品型号证书》将于 2020 年 7 月 1 日失效；发行人已提交相关申请材料，但亦存在发行人申请材料不符合要求或未通过转换认证而无法取得认证证书因而无法销售相关产品的风险。

3、技术风险

（1）产品研发风险

公司产品主要解决网络环境中的身份安全、通信安全和数据安全等信息安全问题。公司始终坚持自主研发和自主创新的策略，以技术创新为驱动、以市场需求为导向进行产品研发，并进行持续的研发投入。未来如果公司不能根据行业变化做出前瞻性判断、快速响应与精准把握市场，将会导致公司开发的产品不能适应市场的需求，对公司持续经营发展造成不利影响。

（2）核心人员流失及技术泄露风险

经过近二十年的技术积累，公司建立了国内信息安全领域具备较强实力的研发团队，其中核心技术人员均具有 10 年以上的行业经验，谙熟行业产品技术和应用的发展趋势。核心技术人员是公司的核心竞争力及未来持续发展的基础。

当前市场对于技术和人才竞争日益激烈，能否维持技术人员队伍的稳定，并不断吸收优秀研发人员的加入，是公司保持技术竞争优势的基础。如果未来公司出现核心人员大量流失或核心技术泄露的现象，可能会在一定程度上影响公司的市场竞争力和技术创新能力，从而对公司的经营发展产生一定不利影响。

（3）知识产权被侵害风险

公司是国内领先的信息安全产品和解决方案提供商，以密码技术为核心支撑，致力于解决网络环境中的身份安全、通信安全和数据安全等信息安全的基础性问题。截止本招股说明书出具日，公司拥有 48 项发明专利和 138 项软件著作权，这些知识产权对公司的未来业务发展发挥着关键作用。一方面，由于我国仍存在软件产品被盗版、专有技术流失或泄密等现象，公司知识产权存在被侵害的风险。另一方面，虽然公司一直坚持自主创新的研发策略，避免侵犯他人知识产权，但仍不能排除某些竞争对手采取恶意诉讼的市场策略，利用知识产品相关诉讼等拖延公司市场拓展的可能性。如果出现上述情况，可能对公司的业务开展产生一定不利影响。

（4）因最终客户发生数据泄密等安全事件时，公司承担罚款或赔偿的风险

当最终客户发生数据泄密及其他信息安全事件时，如相关部门认定最终客户

所采用的公司产品和服务违反了国家的相关法律法规，公司可能承担相应的法律责任，并可能需根据销售合同的约定向客户承担相应的赔偿责任，从而给公司的经营带来一定风险。

4、财务风险

（1）应收账款不能及时回收风险

随着信息安全市场的快速发展，公司业务规模迅速扩大，营业收入持续增长，盈利能力不断增强。报告期内公司应收账款随业务规模的扩大而持续增长；另外，公司营业收入具有季节性特征，销售集中在下半年尤其是第四季度，需要在次年进行收款，导致各年末的应收账款余额较大且增幅也较高。报告期各期末公司应收账款账面价值分别为 7,874.23 万元、13,214.47 万元和 17,430.14 万元，占同期末流动资产的比例分别为 34.33%、39.38%和 43.86%。

随着公司业务规模不断扩大，公司营业收入持续增长，应收账款余额仍可能保持在较高水平，将进一步加大公司的营运资金周转压力。如果公司主要客户的财务经营状况发生重大不利变化，将进一步加大本公司坏账损失的风险，进而对公司资产质量以及财务状况产生不利影响。

（2）人力成本上升风险

随着业务规模的不断扩大，公司在职人数整体呈上升趋势。报告期各期末，公司员工人数分别为 358 人、378 人和 638 人。同时为了避免人员流失，促进公司业务的快速发展，公司提高了员工的薪酬待遇水平，因此职工薪酬亦呈现增长态势，随着公司员工队伍的扩大和薪酬待遇水平的提高，如果公司人力成本增幅与营业收入增幅不匹配，将可能对公司经营业绩产生一定影响。

（3）存货减值风险

报告期各期末，公司存货的账面价值分别为 5,361.70 万元、4,990.95 万元和 6,422.44 万元，占流动资产比例分别为 23.38%、14.87%和 16.16%。公司建立了严格的存货管理制度，具有独立完整的供应链体系，根据实际业务经营需要合理控制需要采购的生产物料和服务。报告期内，本公司存货并未发生大额减值情形。如果未来公司产品发生严重滞销，或出现管理不善等情形，仍将可能存在存货减值的风险。

5、商誉减值风险

报告期末，公司合并报表商誉金额为 8,301.15 万元，占公司资产总额的比例为 14.86%，系公司收购神州融信、信安珞珈以及华耀科技产生。报告期内，公司每年对商誉及其相关的资产组或者资产组组合进行减值测试，经测试，公司收购神州融信、信安珞珈以及华耀科技产生的商誉及其相关的资产组或者资产组组合的可回收金额高于其账面价值，无需确认减值损失。但如果未来商誉所对应资产组或者资产组组合的经营情况不及预期，则可能导致商誉发生减值，从而对公司经营业绩产生较大影响。

6、增值税优惠政策变动风险

根据财政部、国家税务总局《关于软件产品增值税政策的通知》（财税[2011]100 号）的规定，增值税一般纳税人销售其自行开发生产的软件产品，按 17%（2018 年 5 月 1 日后税率为 16%，2019 年 4 月 1 日后税率为 13%）的法定税率征收增值税后，对增值税实际税负超过 3%的部分实行即征即退政策。

2017 年度、2018 年度和 2019 年度，公司收到的增值税退税款分别为 2,229.02 万元、2,111.03 万元和 1,564.07 万元，占利润总额的比例分别为 41.32%、23.88%和 15.85%。报告期内，公司收到的增值税退税额占当期利润总额比例较高，符合软件行业特点。但是，如果未来相关政策发生变动或者本公司不能持续符合享受增值税退税政策的条件，则公司将面临因不再享受相应税收优惠政策而导致利润总额下降的风险。

7、企业所得税优惠政策变动风险

（1）本公司于 2017 年 10 月 25 日通过复审取得编号为 GR201711002806 的《高新技术企业证书》，有效期为三年。根据财政部、国家税务总局《关于软件和集成电路产业企业所得税优惠政策有关问题的通知》（财税[2016]49 号）第四条规定，国家规划布局内的重点软件企业和集成电路设计企业，如当年未享受免税优惠的，可减按 10%的税率征收企业所得税。本公司 2019 年度、2018 年度和 2017 年度内满足相关条件，2018 年度和 2017 年度已享受减按 10%的税率征收企业所得税的税收优惠，2019 年度已申请重点软件企业企业所得税优惠备案，如备案通过，可以继续享受减按 10%的税率征收企业所得税的税收优惠。

（2）公司子公司信安珞珈于 2015 年 10 月 28 日被认定为高新技术企业，取得编号为 GR201542000499 的《高新技术企业证书》，有效期为三年，于 2018 年 11 月 30 日通过复审，取得编号为 GR201842002335 的《高新技术企业证书》，有效期为三年，信安珞珈 2019 年度、2018 年度和 2017 年度适用高新技术企业 15%的企业所得税率。

（3）本公司子公司华耀科技于 2017 年 8 月 6 日通过高新技术企业复审，取得编号为 GR201711007265 的《高新技术企业证书》，有效期为三年，依据《中华人民共和国企业所得税法》第二十八条、《中华人民共和国企业所得税实施条例》第九十三条规定，于 2019 年度、2018 年度和 2017 年度适用高新技术企业 15%的优惠税率。

如果国家对企业所得税优惠政策发生重大变动，或者公司不能及时办理相应的税收优惠证明，那么将对公司净利润产生一定影响。

8、毛利率波动的风险

报告期内，公司综合毛利率略有波动，分别为 63.03%、67.42%和 66.41%。随着业务规模的扩大和产品线的丰富，公司面临下游需求变化、市场竞争加剧和人力成本不断提高等因素而导致的毛利率波动风险。

9、管理风险

公司自成立以后，一直保持较快发展速度，资产和经营规模不断扩大。如果本次公开发行成功，公司的资产规模和经营规模将进一步扩大，这就对公司的内部管理水平提出了更高的要求。

近年来，公司不断完善法人治理结构，内部控制体系不断健全，积累了丰富的经营管理经验，形成了有效的约束机制及内部管理机制。随着公司的发展，如果公司管理层不能适时健全管理机制、调整组织模式，将由于公司规模的快速扩张而带来相应的管理风险。

10、募集资金投资风险

（1）募投项目达不到预期效益导致公司经营业绩受损的风险

公司本次计划募集资金 6.88 亿元，募投项目主要为公司重点产品与核心技

术的研发，募集资金重点投向为科技创新领域，项目建成投产后，将对本公司发展战略的实现、经营规模的扩大和业绩水平的提升具有重要意义。虽然公司对募集资金投资项目可行性进行了充分研究和论证，但是本次募集资金投资项目的建设能否按时完成、项目的实施效果能否达到预期等都存在一定的不确定性。同时，公司募投项目相关新产品不能满足客户的需求，或者由于宏观经济形势、产业政策、市场开拓情况、产品价格变动等方面发生不利变化导致产品销售未达预期目标，从而募集资金投资项目不能产生预期的经济效益，将对公司经营业绩带来较大不利影响。

（2）摊薄即期回报的风险

本次发行后，公司的净资产将有所增加。由于存在一定的建设周期，募集资金投资项目在短期内无法立即产生收益，公司的每股收益及净资产收益率可能会因此有所下降，从而导致公司的即期回报被摊薄。

11、净资产收益率下降的风险

报告期内，公司扣除非经常性损益后归属于普通股股东加权平均净资产收益率分别为 47.07%、34.41%和 26.86%。若本次发行成功且募集资金到位后，公司净资产规模将随之大幅增加，由于募集资金的投资项目需要一定的建设周期，且产生效益尚需一定的运行时间，无法在发行当年即产生预期效益。因此，在募集资金到位后的一段时间内，公司存在净资产收益率下降的风险。

12、新增固定资产折旧及研发支出导致公司利润下滑的风险

本次募投项目投资金额较大，募集资金投资项目达产后，公司的折旧费用及研发支出将大幅增加。如果未来募集资金投资项目不能达到预期收益，公司净利润存在下降的风险。

13、实际控制人不当控制风险

本次发行前，李伟、王翊心和丁纯三人通过直接和间接方式合计控制本公司 67.0047%股权。李伟、王翊心、丁纯为公司的实际控制人，三人为一致行动人。如果实际控制人利用其对本公司的控股地位或其他方式对公司经营和财务决策、人事安排、投资方向和利润分配等方面进行不当控制，可能存在给公司及其他中小股东利益带来一定损害的风险。

14、公司实际控制人可能履行对赌协议的风险

2019 年 4 至 5 月，信安世纪与李伟、王翊心、丁纯先后与方正投资、财通创新、珠海尚颀、金锦联城分别签署了《<股权转让协议>的补充协议》，其中含有实际控制人回购条款。该条款约定，若信安世纪未能在 2022 年 12 月 31 日之前完成在中国 A 股市场上市发行的，上述股东有权要求李伟、王翊心、丁纯对其所持有的公司股份进行回购。2020 年 5 月 18 日，信安世纪、李伟、王翊心、丁纯与方正投资、财通创新、珠海尚颀、金锦联城分别签署了《<股权转让协议>的补充协议（二）》，约定上述实际控制人回购股份的条款自信安世纪向中国证监会或者深圳证券交易所或者上海证券交易所递交首次公开发行股票并上市申请材料之日起自动失效，对各方不再具有法律效力；若中国证监会或者深圳证券交易所或者上海证券交易所否决信安世纪上市申请或信安世纪撤回申请材料，则该条款自申请材料撤回之日或上市申请被否决之日起恢复执行。

2015 年 7 月，李伟、王翊心、丁纯与南京捷奕、维思捷鼎、杭州维思签署了《<北京信安世纪科技有限公司投资框架协议>之补充协议》，约定若信安世纪有限不能在 2018 年 12 月 31 日前完成在中国 A 股市场的合格上市，则南京捷奕、维思捷鼎、杭州维思有权要求李伟、王翊心、丁纯回购其持有信安世纪有限的股权。2020 年 5 月，信安世纪、李伟、王翊心、丁纯与南京捷奕、杭州维思、维思捷鼎分别签署了《<北京信安世纪科技有限公司投资框架协议>之补充协议（二）》，将上述回购条款修改为，若信安世纪不能在 2022 年 12 月 31 日之前完成在中国 A 股市场上市发行的，南京捷奕、杭州维思、维思捷鼎有权要求实际控制人对其持有的股份进行回购；各方同意自信安世纪向中国证监会或者深圳证券交易所或者上海证券交易所递交首次公开发行股票并上市申请材料之日起，该条款自动失效，若中国证监会或上海证券交易所否决信安世纪上市申请或信安世纪撤回申请材料，则该条款自申请材料撤回之日或上市被否决之日起恢复执行。

因此，若公司未能在上述期限内完成发行上市，则存在公司实际控制人执行该协议并溢价回购公司股票的风险。

15、发行失败风险

公司拟首次公开发行股票并在科创板上市，尚需经上海证券交易所上市审核

和证监会同意公司首次公开发行股票注册。如果完成证监会注册程序，在发行中仍存在认购不足、发行时总市值未能达到预计市值上市条件从而导致发行失败的风险。

16、新冠肺炎疫情引发风险

受新冠肺炎疫情的影响，国内经济增速中短期内有所下滑，同时各地政府出台的延迟复工、限制人流、物流等防控政策，导致公司储备项目的落地及新增项目的拓展进度有所放缓。若本次新型肺炎疫情的影响在中短期内不能得到有效控制，则将对公司的经营发展产生一定不利影响。

17、诉讼风险

截至本保荐书出具日，公司存在 1 起尚未了结的行政诉讼。起因为飞天诚信曾于 2014 年起诉信安世纪有限专利侵权，北京知识产权法院于 2017 年 4 月裁定驳回飞天诚信的全部诉讼请求。在前述专利侵权案件审理过程中，信安世纪有限向专利复审委员会提出涉案专利无效宣告请求；2015 年 12 月专利复审委员会作出维持案涉发明专利权有效性的决定。针对该决定，信安世纪有限以专利复审委员会为被告、以飞天诚信为第三人向北京知识产权法院提起行政诉讼。2017 年 2 月 28 日，北京知识产权法院一审判决撤销专利复审委员会的审查决定并要求重新作出审查决定。飞天诚信不服前述行政一审判决，向北京市高级人民法院提起上诉。2018 年 6 月 20 日，北京市高级人民法院裁定撤销一审判决，发回北京知识产权法院重审。

截至本保荐书出具日，上述行政诉讼正在审理中。若信安世纪败诉，且案涉专利维持有效，则飞天诚信可能以信安世纪为被告提起专利侵权诉讼。

二、本次发行情况

股票种类	人民币普通股（A 股）		
每股面值	1.00 元		
发行股数	不超过 2,328.19 万股	占发行后总股本比例	不低于 25%
其中：发行新股数量	不超过 2,328.19 万股	占发行后总股本比例	不低于 25%
股东公开发售股份数量	-	占发行后总股本比例	-
发行后总股本	不超过 9,312.78 万股（行使超额配售选择权之前）		

每股发行价格	【】元/股		
发行市盈率	【】倍（按照【】年经审计的扣除非经常性损益前后孰低的归属于母公司股东的净利润除以本次发行前总股本计算）		
	【】倍（按照【】年经审计的扣除非经常性损益前后孰低的归属于母公司股东的净利润除以本次发行后总股本计算）		
发行前每股净资产	【】元/股（不含少数股东权益，以【】年【】月【】日经审计的净资产和发行前总股本计算）	发行前每股收益	【】元/股（按照 2019 年度经审计的扣除非经常性损益前后孰低的归属于母公司股东的净利润除以本次发行前总股本计算）
发行后每股净资产	【】元/股（不含少数股东权益，以【】年【】月【】日经的审计净资产加上预计募集资金净额和发行后总股本计算）	发行后每股收益	【】元/股（按照【】年度经审计的扣除非经常性损益前后孰低的归属于母公司股东的净利润除以本次发行前总股本计算）
发行市净率	【】倍（按照发行价格除以发行前每股净资产计算）		
	【】倍（按照发行价格除以发行后每股净资产计算）		
发行方式	采用网下向询价对象询价配售和网上资金申购定价发行相结合的方式，或采用中国证监会、上海证券交易所等监管部门认可的其他发行方式		
发行对象	本次发行对象为符合资格的询价对象和在上海证券交易所人民币普通股（A 股）证券账户上开通科创板股票交易权限的符合资格的自然人、法人及其他机构（国家法律、行政法规、所适用的其他规范性文件及公司须遵守的其他监管要求所禁止者除外），中国证监会或上海证券交易所另有规定的，按照其规定处理		
承销方式	余额包销		
拟公开发售股份股东名称	-		
发行费用的分摊原则	-		
募集资金总额	【】万元		
募集资金净额	【】万元		
募集资金投资项目	信息安全系列产品升级项目		
	新一代安全系列产品研发项目		
	面向新兴领域的技术研发项目		
	综合运营服务中心建设项目		
发行费用概算	保荐及承销费用【】万元 审计、验资及评估费用【】万元 律师费用【】万元 发行手续费用及其他费用等【】万元		

三、保荐代表人、项目协办人及项目其他组成员情况

本保荐机构指定苏华峰、史哲元作为本次发行的保荐代表人，指定高峰为发行人本次发行的项目协办人。保荐代表人、项目协办人和项目组人员相关情况如

下：

苏华峰：从业证书编号 S0800718010001。保荐代表人，注册会计师，曾参与了新疆火炬（603080）IPO 项目和重大资产购买项目；优博创（831400）及广盛小贷（833970）等公司新三板挂牌推荐项目。具有丰富的投资银行业务经验，执业记录良好。

史哲元：从业证书编号 S0800717050001。保荐代表人，注册会计师，国际注册内部审计师资格。具有十余年投资银行从业经历，负责完成了硕贝德创业板 IPO 项目、中能电气创业板 IPO 项目、农尚环境创业板 IPO 项目、中国核建股改、酒鬼酒 2011 年非公开发行项目、丽江旅游 2009 年非公开发行项目、中信银行非公开发行项目以及兴业银行非公开发行优先股等项目；并主持了太极集团重大资产重组、苏州中茵借壳 ST 天华财务顾问等项目。

高峰：证券执业证书编号 S0800114060014。准保荐代表人，注册会计师，经济学硕士。拥有多年会计师事务所及投资银行相关业务经验，主要负责了汇尔杰（835446）、六人游（摘牌）（872385）、恒丰达（873019）等新三板项目的推荐挂牌工作；并参与南新制药（688189）IPO 项目。

项目组其他成员：武文涛、颜丹、邹扬、韩星。

四、保荐人与发行人的关联关系、保荐人及其保荐代表人是否存在可能影响公正履行保荐责任情形的说明

保荐机构不存在下列可能影响其公正履行保荐职责的情形:

（一）保荐人或其控股股东、实际控制人、重要关联方持有或者通过参与本次发行战略配售持有发行人或其控股股东、实际控制人、重要关联方股份的情况；

（二）发行人或其控股股东、实际控制人、重要关联方持有保荐人或其控股股东、实际控制人、重要关联方股份的情况；

（三）保荐人的保荐代表人及其配偶，董事、监事、高级管理人员，持有发行人或其控股股东、实际控制人及重要关联方股份,以及在发行人或其控股股东、实际控制人及重要关联方任职的情况；

（四）保荐人的控股股东、实际控制人、重要关联方与发行人控股股东、实

际控制人、重要关联方相互提供担保或者融资等情况；

（五）保荐人与发行人之间的其他关联关系。

五、保荐人对发行人是否就本次证券发行上市履行相关决策程序的说明

（一）董事会

2020 年 5 月 12 日，公司召开第一届董事会第十七次会议，审议通过了公司申请首次公开发行股票并在科创板上市的相关议案。

（二）股东大会

2020 年 6 月 2 日，公司召开 2020 年第三次临时股东大会，审议通过了关于公司首次公开发行股票并在科创板上市的相关议案。

综上，本保荐人认为，发行人本次公开发行股票并在科创板上市已获得了必要的批准和授权，履行了必要的决策程序，决策程序合法有效。

六、保荐人对发行人是否符合科创板定位的专业判断

（一）公司符合科创板行业领域要求

公司主营业务为信息安全产品的研发、生产、销售及相关技术服务。根据证监会《上市公司行业分类指引》（2012 年修订），公司所处行业属于“I65 软件和信息技术服务业”；根据国家统计局《国民经济行业分类》（GB/T 4754-2017），公司所处行业属于“I65 软件和信息技术服务业”；根据国家统计局《战略性新兴产业分类（2018）》，公司所属行业为“新一代信息技术产业”。

公司所属行业符合《上海证券交易所科创板企业发行上市申报及推荐暂行规定》第三条（一）中规定的“新一代信息技术领域”行业领域。

（二）公司符合科创属性指标

（1）根据容诚会计师事务所（特殊普通合伙）（以下简称“容诚”）出具的审计报告（容诚审字[2020]100Z0316 号），公司最近三年累计研发投入为 10,054.97 万元，大于 6,000 万元；最近三年公司累计营业收入为 80,762.18 万元，研发累计投入占最近三年累计营业收入的比例为 12.45%；

（2）截至本保荐书出具日，公司拥有的形成主营业务收入的发明专利为 45 项；

（3）根据容诚出具的审计报告（容诚审字[2020]100Z0316 号），公司最近三年营业收入分别为 22,044.13 万元、26,934.15 万元和 31,783.90 万元，最近一年营业收入超过 3 亿元，且复合增长率为 20.08%。

保荐机构认为，公司符合《上海证券交易所科创板企业发行上市申报及推荐暂行规定》关于科创属性的指标要求。

七、保荐人对公司是否符合上市条件的说明

信安世纪股票上市符合《公司法》《证券法》和《上海证券交易所科创板股票上市规则》规定的上市条件：

（一）发行前公司股本总额为人民币 6,984.5817 万元，公司新股发行总数合计不超过 2,328.19 万股。本次发行后公司总股本不超过 9,312.78 万股；

（二）本次公开发行股份总数为不超过 2,328.19 万股，占发行后股份总数的 25.00%，公司公开发行的股份不低于本次发行后股份总数的 25.00%；

（三）市值及财务指标

1、市值结论

综合信安世纪报告期内外部股权融资估值、可比上市公司比较法、收益法得到的评估结果，信安世纪预计市值不低于 10 亿元。

2、财务指标

发行人 2017 年、2018 年、2019 年度扣除非经常性损益后的净利润为 5,913.75 万元、8,173.42 万元、8,661.04 万元，累计扣除非经常性损益后的净利润为 22,748.21 万元；公司 2019 年营业收入为 31,783.90 万元。

3、标准适用判定

依据《上海证券交易所科创板股票发行上市审核规则》《上海证券交易所科创板股票上市规则》等相关法律法规，发行人选择具体上市标准如下：（一）预计市值不低于人民币 10 亿元，最近两年净利润均为正且累计净利润不低于人民

币 5,000 万元，或者预计市值不低于人民币 10 亿元，最近一年净利润为正且营业收入不低于人民币 1 亿元。

综上所述，发行人满足所选择的上市标准。

本次股票发行申请尚需上海证券交易所审核并由中国证监会作出同意注册决定。

八、保荐人按照有关规定应当承诺的事项

（一）保荐人已按照法律法规和中国证监会及上海证券交易所的规定，对发行人及其控股股东、实际控制人进行了尽职调查、审慎核查,充分了解了发行人经营状况及其面临的风险和问题，履行了相应的内部审核程序，已具备相应的保荐工作底稿支持，同意推荐发行人证券发行并上市，并据此出具本上市保荐书。

（二）保荐人有充分理由确信发行人符合法律法规及中国证监会有关证券发行上市的相关规定。

（三）保荐人有充分理由确信发行人申请文件和信息披露资料不存在虚假记载、误导性陈述或者重大遗漏。

（四）保荐人有充分理由确信发行人及其董事在申请文件和信息披露资料中表达意见的依据充分合理。

（五）保荐人有充分理由确信申请文件和信息披露资料与证券服务机构发表的意见不存在实质性差异。

（六）保荐人保证所指定的保荐代表人及本保荐机构的相关人员已勤勉尽责，对发行人申请文件和信息披露资料进行了尽职调查、审慎核查。

（七）保荐人保证保荐书与履行保荐职责有关的其他文件不存在虚假记载、误导性陈述或者重大遗漏。

（八）保荐人保证对发行人提供的专业服务和出具的专业意见符合法律、行政法规、中国证监会的规定和行业规范。

（九）保荐人自愿接受中国证监会依照《证券发行上市保荐业务管理办法》采取的监管措施。

九、对公司持续督导期间的工作安排

事项	安排
（一）持续督导事项	在本次发行股票上市当年的剩余时间及以后 3 个完整会计年度内对发行人进行持续督导。
1、督导发行人有效执行并完善防止大股东、其他关联方违规占用发行人资源的制度	1、强化发行人严格执行中国证监会和上海证券交易所有关规定的意识，督导发行人有效执行并进一步完善已有的防止大股东、其他关联方违规占用发行人资源的制度； 2、与发行人建立经常性沟通机制，持续关注发行人上述制度的执行情况及履行信息披露义务的情况
2、督导发行人有效执行并完善防止高管人员利用职务之便损害发行人利益的内控制度	1、督导发行人有效执行并进一步完善已有的防止高管人员利用职务之便损害发行人利益的内控制度； 2、与发行人建立经常性沟通机制，持续关注发行人上述制度的执行情况及履行信息披露义务的情况。
3、督导发行人有效执行并完善保障关联交易公允性和合规性的制度，并对关联交易发表意见	1、督导发行人有效执行并进一步完善关联交易决策权限、表决程序、回避情形等工作规则； 2、督导发行人及时向保荐机构通报将进行的重大关联交易情况，保荐机构将对关联交易的公允性、合规性发表意见； 3、督导发行人严格执行有关关联交易的信息披露制度。
4、督导发行人履行信息披露的义务，审阅信息披露文件及向中国证监会、上海证券交易所提交的其他文件	1、督导发行人严格按照《公司法》《证券法》及《上海证券交易所科创板股票上市规则》等有关法律、法规及规范性文件的要求，履行信息披露义务； 2、在发行人发生须进行信息披露的事件后，审阅信息披露文件及向中国证监会、上海证券交易所提交的其他文件。
5、持续关注发行人募集资金的使用、投资项目的实施等承诺事项	1、督导发行人执行已制定的《募集资金管理制度》等规定，保证募集资金的安全性和专用性； 2、持续关注发行人募集资金的专户储存、投资项目的实施等承诺事项。
6、持续关注发行人为他人提供担保等事项，并发表意见	1、督导发行人严格按照中国证监会和上海证券交易所有关文件的要求规范发行人担保行为的决策程序； 2、要求发行人对所有担保行为与保荐人进行事前沟通。
（二）保荐协议对保荐人的权利、履行持续督导职责的其他主要约定	按照保荐制度有关规定积极行使保荐职责；严格履行保荐协议、建立通畅的沟通联系渠道。
（三）发行人和其他中介机构配合保荐人履行保荐职责的相关约定	会计师事务所、律师事务所持续对发行人进行关注，并进行相关业务的持续培训。
（四）其他安排	无

十、保荐人认为应当说明的其他事项

无其他需要说明的事项。

十一、保荐人对本次股票上市的推荐结论

西部证券作为信安世纪本次证券发行上市的保荐机构，遵循诚实守信、勤勉尽责的原则，根据法律、法规和中国证监会及上海证券交易所的有关规定，对发行人进行了充分的尽职调查。经过审慎核查，保荐机构认为，信安世纪申请其股票上市符合《公司法》《证券法》及《上海证券交易所科创板股票上市规则》等法律、法规及规范性文件的有关规定,其股票具备在上海证券交易所科创板上市的条件，同意推荐信安世纪的股票在上海证券交易所科创板上市交易，并承担相关保荐责任。

请予批准！

（以下无正文）

（此页无正文，为《西部证券股份有限公司关于北京信安世纪科技股份有限公司首次公开发行股票并在科创板上市之上市保荐书》之签字盖章页）

项目协办人：

高峰　　2020 年 6 月 22 日

保荐代表人：

苏华峰　　2020 年 6 月 22 日

史哲元　　2020 年 6 月 22 日

内核负责人：

倪晋武　　2020 年 6 月 22 日

保荐业务负责人：

范江峰　　2020 年 6 月 22 日

保荐机构总经理：

何　方　　2020 年 6 月 22 日

保荐机构董事长、法定代表人：

徐朝晖　　2020 年 6 月 22 日

西部证券股份有限公司

2020 年 6 月 22 日