北京北信源软件股份有限公司
向特定对象发行股票募集资金使用的
可行性分析报告

二〇二〇年七月

目录

释义表

一、普通名词释义

发行人、北信源、公司、本公司	指	北京北信源软件股份有限公司
本次向特定对象发行、本次发行	指	北京北信源软件股份有限公司以向特定对象方式向特定对象发行股票的行为
华为鲲鹏	指	华为在 2019 年 1 月向业界发布的高性能数据中心处理器
龙芯	指	中国科学院计算所自主研发的通用 CPU
飞腾	指	为“天河”系列计算机量身定制的由国防科大研制的 CPU
申威	指	申威处理器或申威 CPU，简称 “SW 处理器”
统信	指	统信软件技术有限公司
中兴	指	中兴通讯股份有限公司
华为	指	华为技术有限公司
中科方德	指	中科方德软件有限公司
致远互联	指	北京致远互联软件股份有限公司
泛微网络	指	上海泛微网络科技股份有限公司
腾讯	指	深圳市腾讯计算机系统有限公司
阿里巴巴	指	阿里巴巴网络技术有限公司
谷歌	指	Google，谷歌公司
Facebook	指	脸书或者脸谱网，是美国的一个社交网络服务网站
亚马逊	指	亚马逊公司，是美国最大的一家网络电子商务公司
Twitter	指	推特，是一家美国社交网络及微博客服务的网站，是全球互联网上访问量最大的十个网站之一

盖洛普	指	盖洛普咨询公司
蓝凌	指	深圳市蓝凌软件股份有限公司
赛迪顾问	指	赛迪顾问股份有限公司
北京市科委	指	北京市科学技术委员会
国务院	指	中华人民共和国国务院
中央网信办	指	中共中央网络安全和信息化委员会办公室
国家发改委	指	中华人民共和国国家发展和改革委员会
工信部	指	中华人民共和国工业和信息化部
新基建	指	新型基础设施建设，是以新发展理念为引领，以技术创新为驱动，以信息网络为基础，面向高质量发展需要，提供数字转型、智能升级、融合创新等服务的基础设施体系
《网络安全法》	指	《中华人民共和国网络安全法》
《公司章程》	指	北京北信源软件股份有限公司公司章程
股东大会	指	北京北信源软件股份有限公司股东大会
董事会	指	北京北信源软件股份有限公司董事会
元、万元、亿元	指	人民币元、人民币万元、人民币亿元

二、专业名词释义

信源豆豆、Linkdood	指	北信源即时通信系统、相关开发平台及应用生态圈
黑客	指	利用安全漏洞对网络或系统进行攻击破坏或窃取资料的人
终端安全管理	指	一种保护网络安全的策略式方法，它需要终端设备在得到访问网络资源的许可之前遵从特定的标准
信息安全等级保护	指	信息安全等级保护是指对国家秘密信息、法人和其他组织及公民的专有信息以及公开信息和存储、传输、处理这些信息的信息系统分等级实行安全保护，对信息系统中使用的信息安全产品实行按等级管理，对信息系统中发生的信息安全事件分等级响应、处置。

安全审计	指	对网络上发生的事件进行记载、分析和报告的操作
安全管理平台	指	通过对网络中的安全设备、网络设备、服务器系统、终端系统的日志事件信息进行统一收集、过滤、归并和关联性分析，实现对重要信息资产和业务系统的安全状态监控、安全风险管理和安全态势感知，并及时进行安全预警、安全响应和管理控制的信息安全产品
身份认证	指	包括实现数字签名、身份验证和数字证明等技术的软硬件产品
中标麒麟	指	中标麒麟操作系统
银河麒麟	指	由国防科技大学研制的开源服务器操作系统
飞书	指	字节跳动于 2016 年自研的新一代一站式协作平台，是保障字节跳动全球五万人高效协作的办公工具
WeLink	指	源自华为 19 万员工的数字化办公实践，融合消息、邮件、会议、音视频、云空间、OA、小程序等服务，高效连接企业的团队、业务、知识、设备，为政企开启数字化办公新体验，助力企业数字化转型
5G	指	第五代移动通信技术，是最新一代蜂窝移动通信技术，也是继 4G（LTE-A、WiMax）、3G（UMTS、LTE）和 2G（GSM）系统之后的延伸
PC	指	英文“Personal Computer”的缩写，个人计算机
APP	指	安装在智能手机上的软件
双因子认证	指	结合密码以及实物（信用卡、SMS 手机、令牌或指纹等生物标志）两种条件对用户进行认证的方法
数字证书	指	在互联网通讯中标志通讯各方身份信息的一个数字认证，人们可以在网上用它来识别对方的身份
移动互联网	指	互联网的技术、平台、商业模式和应用与移动通信技术结合并实践的活动的总称
万物互联	指	将人，流程，数据和事物结合一起使得网络连接变得更加相关，更有价值
系统集成	指	将软件、硬件与通信技术组合起来为用户解决信息处理问题的业务
GandCrab	指	一种计算机勒索病毒
AI	指	英文“Artificial Intelligence”的缩写，即人工智能

单点故障	指	系统中一点失效，就会让整个系统无法运作的部件，换句话说，单点故障即会整体故障
开源	指	全称为开放源代码。就是要用户利用源代码在其基础上修改和学习的，但开源系统同样也有版权，同样也受到法律保护
漏洞扫描	指	基于漏洞数据库，通过扫描等手段对指定的远程或者本地计算机系统的安全脆弱性进行检测，发现可利用漏洞的一种安全检测（渗透攻击）行为
恶意代码	指	没有作用却会带来危险的代码，一个最安全的定义是把所有不必要的代码都看作是恶意的，不必要代码比恶意代码具有更宽泛的含义，包括所有可能与某个组织安全策略相冲突的软件
大数据	指	无法在一定时间范围内用常规软件工具进行捕捉、管理和处理的数据集合，是需要新处理模式才能具有更强的决策力、洞察发现力和流程优化能力的海量、高增长率和多样化的信息资产
防火墙	指	设置在不同网络或网络安全域之间的一系列部件的组合。可通过监测、限制、更改跨越防火墙的数据流，尽可能地对外部屏蔽网络内部的信息、结构和运行状况，以此来实现网络的安全保护
API	指	英文“Application Programming Interface”的缩写，应用程序接口，是一些预先定义的函数，或指软件系统不同组成部分衔接的约定
网络准入控制	指	其宗旨是防止病毒和蠕虫等新兴黑客技术对企业安全造成危害，客户可以只允许合法的、值得信任的终端设备接入网络，而不允许其它设备接入
移动存储介质安全管理系统	指	数据安全有较高需求的单位用以对数据进行防护、防止数据通过 U 盘和移动硬盘、移动硬盘等被泄露的系统
Wintel	指	Microsoft（微软）与 Intel（英特尔）的商业联盟
区块链	指	是一种共享数据库，存储于其中的数据或信息，具有“不可伪造”“全程留痕”“可以追溯”“公开透明”“集体维护”等特征。 基于这些特征，区块链技术奠定了坚实的“信任“基础，创造了可靠 的“合作”机制
信创	指	信息化应用创新的简称
等保 1.0	指	网络安全等级保护 1.0 制度
等保 2.0	指	网络安全等级保护 2.0 制度,是我国网络安全领域的基本国策、基本制度
云服务	指	基于互联网的相关服务的增加、使用和交互模式，通常涉及通过互联网来提供动态易扩展且经常是虚拟化的资源
云计算	指	基于互联网的相关服务的增加、使用和交付模式，通常涉及通过互联网来提供动态易扩展且经常是虚拟化的资源

公有云	指	通过虚拟化技术把硬件资源抽象成的资源池，由第三方提供商为用户提供的能够使用的云。用户可通过互联网使用，其核心属性是共享资源服务。用户对云资源只有使用权而没有拥有权
私有云	指	用户基于数据安全及服务质量的有效管控而单独构建的云。用户对基础设施拥有所属权并可以控制在此设施上部署应用程序的方式，私有云可部署在企业数据中心内，核心属性是专有资源
混合云	指	综合了数据安全性、成本效益、业务需求等多方面考虑，基于公有云及私有云构建的云
互联网+	指	创新 2.0 下的互联网发展的新业态,是知识社会创新 2.0 推动下的互联网形态演进及其催生的经济社会发展新形态
物联网	指	基于传感技术的物物相联、人物相联和人人相联的信息实时共享的网络
虚拟化	指	计算机元件在虚拟的基础上而不是真实的基础上运行，如服务器虚拟化、桌面虚拟化、存储虚拟化等
耦合度	指	对模块间关联程度的度量。耦合的强弱取决于模块间接口的复杂性、调用模块的方式以及通过界面传送数据的多少。
应用层协议	指	定义了运行在不同端系统上的应用程序进程如何相互传递报文
代理服务器	指	代理网络用户去取得网络信息的中转站，是个人网络和 Internet 服务商之间的中间代理机构，负责转发合法的网络信息，对转发进行控制和登记
沙箱	指	一个虚拟系统程序，允许你在沙盘环境中运行浏览器或其他程序，因此运行所产生的变化可以随后删除。它创造了一个类似沙盒的独立作业环境，在其内部运行的程序并不能对硬盘产生永久性的影响。 在网络安全中，沙箱指在隔离环境中，用以测试不受信任的文件或应用程序等行为的工具。
智能合约	指	是一种旨在以信息化方式传播、验证或执行合同的计算机协议。智能合约允许在没有第三方的情况下进行可信交易，这些交易可追踪且不可逆转
Web	指	现广泛被译作网络、互联网，表现为三种形式，即超文本（hypertext）、超媒体（hypermedia）、超文本传输协议（HTTP）等
ROOT	指	Android 和 iOS 移动设备系统中的唯一的超级用户，因其可对根目录执行读写和执行操作而得名，其具有系统中的最高权限，如启动或停止一个进程，删除或增加用户，增加或者禁用硬件，添加文件或删除所有文件等等

TCP	指	英文“Transmission Control Protocol/Internet Protocol”的缩写，即传输控制协议，是一种面向连接的、可靠的、基于字节流的传输层通信协议
SDK	指	英文“Software Development Kit”的缩写，即软件开发工具包
哈希	指	“Hash”的音译，是把任意长度的输入（又叫做预映射 pre-image）通过散列算法变换成固定长度的输出，该输出就是散列值
APT 攻击	指	高级可持续威胁攻击,也称为定向威胁攻击，指某组织对特定对象展开的持续有效的攻击活动。
SNMP	指	专门设计用于在 IP 网络管理网络节点（服务器、工作站、路由器、交换机及 HUBS 等）的一种标准协议，它是一种应用层协议
VLAN	指	英文“Virtual Local Area Network”的缩写，即虚拟局域网，是一组逻辑上的设备和用户，这些设备和用户并不受物理位置的限制，可以根据功能、部门及应用等因素将它们组织起来，相互之间的通信就好像它们在同一个网段中一样，由此得名虚拟局域网
Linux	指	全称 GNU/Linux，是一套免费使用和自由传播的类 UNIX 操作系统
HOOK	指	Windows 中提供的一种用以替换 DOS 下“中断”的系统机制
Rootkit	指	一种特殊的恶意软件，它的功能是在安装目标上隐藏自身及指定的文件、进程和网络链接等信息
SaaS	指	英文“Software-as-a-Service”的缩写，即通过网络提供软件服务
CMMI	指	即软件成熟度模型集成（Capability Maturity Model Integration），由美国卡耐基梅隆大学软件工程学院发布，是一个可以改进系统工程和软件工程的整合模式，能够降低项目的成本，提高项目质量与按期完成率，在世界各地得到了广泛的推广与接受
CUDA	指	英文“Compute Unified Device Architecture”的缩写，是显卡厂商 NVIDIA 推出的运算平台
GPU	指	英文“Graphics Processing Unit”的缩写，即图形处理器
CPU	指	英文“Central Processing Unit”的缩写，即中央处理器,是计算机系统的运算和控制核心，是信息处理、程序运行的最终执行单元
UOS	指	由包括中国电子集团（CEC）、武汉深之度科技有限公司、南京诚迈科技、中兴新支点在内的多家国内操作系统核心企业自愿发起“UOS(Unity Operating System)统一操作系统筹备组”共同打造的中文国产操作系统
CDN	指	英文“Content Delivery Network”的缩写，即内容分发网络，是构建在现有网络基础之上的智能虚拟网络

一、本次向特定对象发行股票募集资金的使用计划

本次向特定对象发行股票募集资金总额（含发行费用）不超过 88,158 万元，扣除发行费用后拟用于如下项目：

序号	项目名称	建设内容	拟投资总额（万元）	募集资金拟投入金额（万元）
1	大数据和AI驱动的信创终端主动防御平台研发项目	信创平台新一代终端安全防护系统	11,707.24	11,707.24
		信创平台端点检测与响应系统	10,240.42	10,240.42
小计			21,947.66	21,947.66
2	基于私有服务器的安全移动办公平台	移动办公系统	17,003.77	17,003.77
		视频会议系统	11,301.49	11,301.49
		商业秘密沟通系统	11,602.41	11,602.41
小计			39,907.67	39,907.67
3	补充流动资金	-	26,302.67	26,302.67
合计			88,158.00	88,158.00

本次发行的募集资金到位前，公司可根据市场情况利用自筹资金对募集资金投资项目进行先期投入，并在募集资金到位后予以置换。在上述募集资金项目范围内，公司可根据项目的实际需求情况，按照相关法律、法规的规定对上述单个或多个项目的募集投入金额进行适当调整。

若实际募集资金净额低于上述募集资金投资项目拟投入金额，公司股东大会将授权董事会（或董事会授权人士）根据实际募集资金净额，按照项目的轻重缓急等情况，调整并最终决定募集资金投入的优先顺序及各项目的具体投资金额等使用安排，募集资金不足部分由公司自筹解决。

二、本次募集资金投资项目基本情况及可行性分析

（一）大数据和AI驱动的信创终端主动防御平台研发项目

1．项目整体概况

本项目是因应国家信息技术产业创新的战略要求，结合北信源在信息安全领域的传统优势，通过开发信创平台新一代终端安全防护平台、信创平台端点检测

与响应平台，进一步丰富和完善信创平台信息安全产品体系。

项目总投资额为 21,947.66 万元，拟使用募集资金 21,947.66 万元，详见下表：

序号	名称	金额（万元）	比例	拟使用募集资金（万元）
1	建设投资	5,482.85	24.98%	5,482.85
1.1	建筑安装工程费用	887.85	4.05%	887.85
1.2	设备及软硬件购置费用	4,595.00	20.94%	4,595.00
2	基本预备费	164.49	0.75%	164.49
3	项目实施费	14,089.97	64.20%	14,089.97
3.1	租赁费用	1,099.97	5.01%	1,099.97
3.2	人员工资	12,020.00	54.77%	12,020.00
3.3	测试费用	970.00	4.42%	970.00
4	铺底流动资金	2,210.36	10.07%	2,210.36
5	**合计**	21,947.66	100.00%	21,947.66

2．项目建设的背景

（1）信息安全事件频发，内生安全需求激增

随着信息技术的发展，互联网、移动互联网的普及应用，网络信息安全事件频发。2018 年国家互联网应急中心共处置网络安全事件约 10.6 万起，捕获勒索软件近 14 万个，全年整体呈增长趋势，更新频率和威胁广度都大幅提升，勒索软件 GandCrab 全年出现了约 19 个版本，持续快速更新迭代[1]。2018 年全球因网络犯罪造成的损失达 15,000 亿美元，较 2014 年的 4,450 亿美元增长了 237%[2]。

网络信息安全事件频发，对制造、通信、能源、市政设施等关键基础设施的攻击事件也频繁发生，受到攻击的行业领域不断扩大，造成的后果也愈发严重，各界对网络信息安全的关注度随之提升。随着各界对网络信息安全的关注度逐步提升，网络信息安全行业将迎来新的发展机遇。

[1] 中国银河证券，《信息安全行业深度研究报告：解码信息安全七大细分领域，剖析未来重点关注方向》，2020 年 04 月 02 日

[2] 东方证券，《网络安全系列报告之二：行业成长趋势不改，新兴安全及服务成为增长风口》，2020 年 05 月 06 日

（2）政策大力支持，为产业发展注入强劲动力

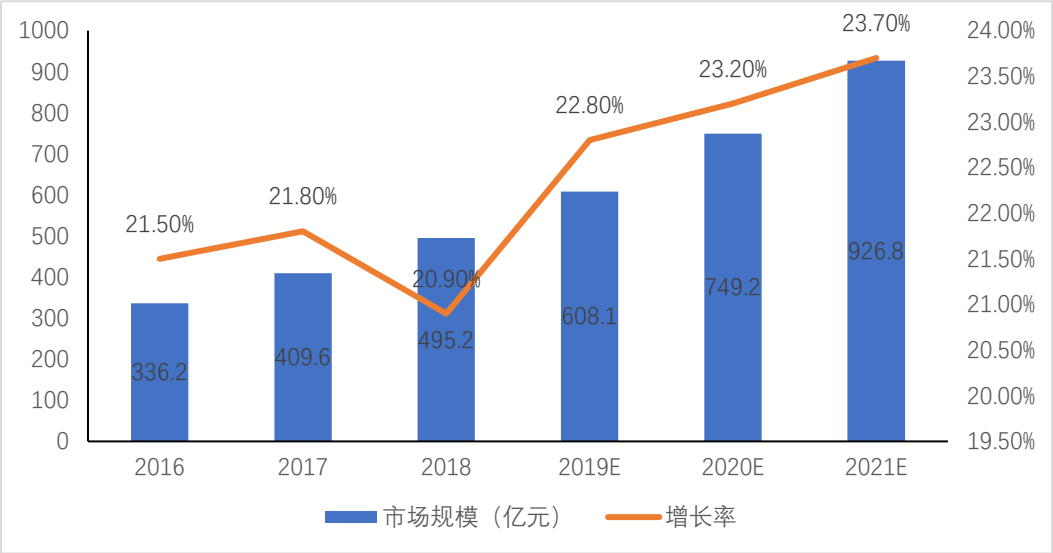
党中央高度重视网络信息安全。“棱镜门”事件爆发之后，信息安全的战略地位越来越高。十八届三中全会决定成立国家安全委员会，将国家安全提高到前所未有的地位。2014 年 2 月，中央网络安全和信息化领导小组成立，标志着信息安全已经上升到国家战略。2016 年 10 月 9 日，习近平总书记在中共中央政治局第三十六次集体学习时提出，“构建安全可控的信息技术体系”“实施网络信息领域核心技术设备攻坚战略”[3]。2017 年 6 月《中华人民共和国网络安全法》开始实施，把网络安全工作以法律形式提高到了国家安全战略的高度。相关政策与法律的实施将长期利好信息安全行业。

（3）技术驱动拓宽市场边界，诞生增量市场

信息技术的不断演进，催生了新的安全威胁，也为信息安全行业的发展带来了机遇。从信息技术的演进过程来看，大致经历了从 PC 互联网时代、移动互联网时代到现在的万物互联时代。信息安全也从传统的 PC 时代的反病毒逐渐向边界防护、数据安全和整体安全持续进化。当今的信息安全已经不仅仅局限于网络信息安全，而是拓展到了现实世界的每一个角落、社会生活的方方面面，成为人类社会的基本需求。当物与物之间互联越来越紧密，数据的价值越来越高，业务的组织形式以围绕数据进行，将会出现围绕企业业务场景的安全服务，同时用户与服务器直接联系也越来越紧密。2019 年 5 月 13 日，国家市场监督管理总局、国家标准化管理委员会发布《信息安全技术网络信息安全等级保护基本要求》国家标准，于 2019 年 12 月 1 日正式实施，标志着“等保 2.0”时代正式到来。对比“等保 1.0”，“等保 2.0”将定级备案的对象从信息系统增加到关键信息基础设施这一网络空间层面，新纳入云计算平台、工业控制系统、大数据中心、大型互联网企业、移动互联网和物联网系统等对象，并从被动防御的安全体系向事前防御、事中响应、事后审计的动态保障体系转变。新的安全要求，将极大催生新的市场需求。根据赛迪顾问预测，我国网络信息安全市场规模到 2021 年将达到 926.8 亿元。[4]

2016-2021 年中国网络信息安全市场规模与增长趋势图

[3] 网信办，构建安全可控的信息技术体系，http://www.cac.gov.cn/2018-05/11/c_1122777589.htm
[4] 赛迪顾问，《2019 中国网络安全发展白皮书》，2019 年 02 月。

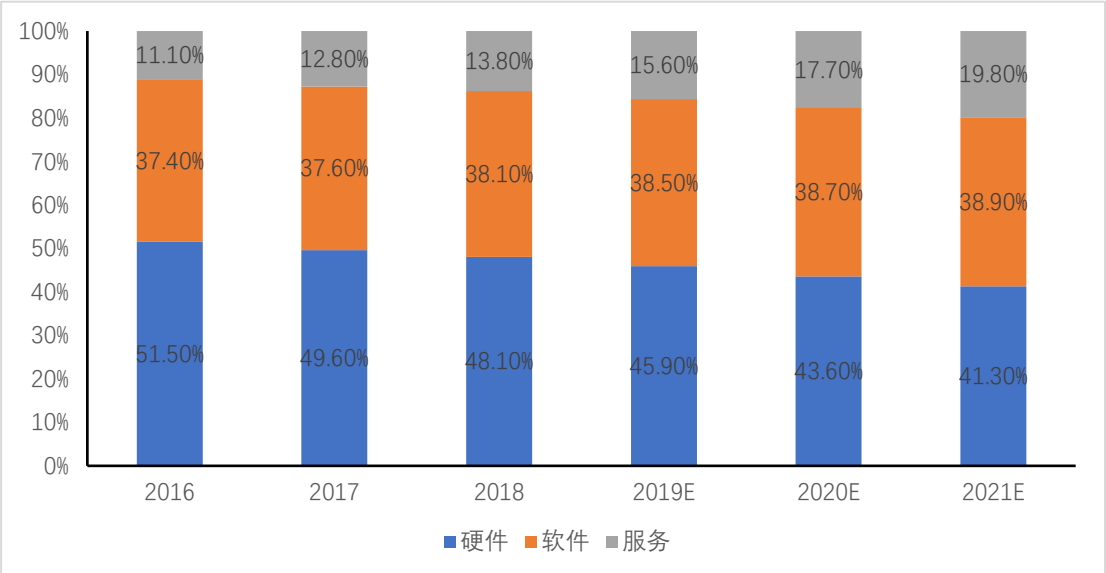


数据来源：赛迪顾问

（4）中国网络信息安全市场逐步向服务化转型

网络安全产业的发展主要受政策、技术及特定事件的影响。近年来，网络信息安全事件频发，各方开始把网络信息安全视为一项重要的风险，并看重网络信息安全服务的持续性。随着“等保 2.0”的实施、虚拟化及云服务理念的渗透，我国网络安全市场结构逐步由软硬件产品为主向软硬件产品及服务均衡发展的态势。

2016-2021 年中国网络信息安全市场规模与增长



数据来源：赛迪顾问

3．项目实施的必要性

（1）实施本项目是响应国家发展战略的需要

随着《网络安全法》的颁布实施，国家相关部委相继发文，强力推进我国信息技术应用创新的发展进程。2016 年 12 月，国务院发布《“十三五”国家信息化规划》提出“强化网络安全顶层设计、构建关键信息基础设施安全保障体系、加强全天候全方位感知网络安全态势能力建设以及强化网络安全科技创新能力[5]。”2016 年 12 月，国家互联网信息办公室发布《国家网络空间安全战略》指出“网络安全是国家安全的核心，核心技术装备应安全可控，建立实施网络安全审查制度，提高产品和服务的安全性和可控性”。由此可见，信息技术创新应用和国家网络安全紧密相关，是中国信息化产业发展的必经之路，也是国家安全战略的必然要求[6]。

网络安全保护是信息系统不可或缺的一部分，基于信创产业平台的网络安全产品更是今后网络安全保护的标配。随着我国信创基础软硬件产品的逐步成熟，以龙芯、飞腾、兆芯、申威为代表的 CPU，以及以麒麟、统信、普华为代表的操作系统，已经由基本可用实现了到可媲美“WIntel”体系产品的跨越。基于信创产业平台对安全产品进行全面适配，是响应国家信创产业发展战略的重要举措。

本项目与国家网络空间安全战略高度一致，是落实国家网络空间安全战略的具体举措，也与国家《网络空间安全战略》《网络安全法》《网络安全等级保护技术 2.0 版本》的具体技术要求相吻合。本项目的实施紧贴信创产业发展进程，将为信创平台终端与信息系统的安全保驾护航。

（2）实施本项目是顺应行业发展趋势的需要

随着 5G、云计算、大数据、物联网、人工智能、区块链等新兴技术的发展，企业信息化程度持续提升，新技术的应用导致企业业务场景发生变化的同时，新的网络安全问题也将伴随着发生。

近年来，中兴事件、华为事件暴露了我国在网络信息领域的供应链风险和安全风险。与此同时，面对日益复杂的网络安全环境以及新一代网络安全威胁，传

[5] 中国政府网，http://www.gov.cn/zhengce/content/2016-12/27/content_5153411.htm
[6] 中央网信办，http://www.cac.gov.cn/2016-12/27/c_1120195926.htm

统的安全手段已经无法有效满足社会各界的安全需求。随着大数据分析、人工智能、安全情报收集等技术的逐渐成熟和发展，安全检测技术对安全态势的分析、预警和预测越来越准确，具备数据分析、安全运营和情报收集等能力的中高位安全产品不断涌现，网络安全防御体系逐渐从被动防御体系向具有自动响应、追查、威胁诱捕等功能的主动防御体系转变。在信息技术应用创新的背景下，构建主动安全防御体系成为我国信息技术行业的重要发展趋势。

本项目与我国网络安全行业构建主动安全防御体系的发展趋势高度吻合。信创平台端点检测与响应系统项目基于信创平台，强调安全防护能力的提升，特别是从网络攻防对抗的角度，通过端点检测与响应，以大数据和 AI（人工智能）驱动，能够有效抵御未知威胁和高级可持续性威胁。

（3）实施本项目是实现公司发展战略目标的需要

公司作为专业从事网络安全的国家级高新技术企业，为政府机关、军工、金融和能源等国家重点行业及企事业单位提供网络安全产品和整体解决方案。公司将以网络安全为基础，依循“信息技术应用创新”这一国家安全的核心发展方向，坚持技术创新，力求为客户提供优质的产品及服务。

随着我国“信息技术应用创新”战略的逐步推进，基于信创平台的各类软硬件产品逐渐在各领域、各行业渗透，不断扩大其应用领域，也对网络安全产品提出了全新的要求。面对信创平台的多样化及其安全需求，公司现有基于“Wintel”体系的网络安全产品将面临着一定程度的投入高、被替代的风险。

因此，为了抓住网络安全行业良好的发展机遇和扩张空间，巩固公司在技术门槛、行业资源以及市场等方面建立起来的优势，进一步提升公司在国内网络安全行业的市场地位和市场份额，公司有必要进行信创平台研发项目的实施。

4．项目实施的可行性

（1）公司具有强大的研发能力

公司长期在网络安全领域精耕细作，始终秉承专业、专注的态度致力于前瞻科技，不断提升产品性能和服务品质，持续加大研发投入和技术创新，经过多年积累，公司具备提供网络安全领域的软件设计开发、技术咨询、关键设备研发、系统集成服务、大数据、移动互联等应用业务的较强业务能力。

公司在网络安全技术相关领域拥有较高的市场地位，曾承担过多项国家发改委、北京市经济和信息化局及北京市科委的科研与产业化项目；公司持续深化与国内外科研院校的长期战略合作，积极开展产学研合作和上下游技术攻关。截至2020年3月31日，公司及子公司取得软件著作权证书219项，授权专利104项，其中发明专利90项，外观设计专利10项，实用新型专利4项，已申请取得商标123项，涵盖了信息安全、大数据、移动互联应用领域等诸多技术，形成了较全面并具有前瞻性的专利体系。

因此，公司具有实施本项目的研发能力，确保项目的顺利实施。

（2）公司具有实施本项目的相应积累

①技术积累

公司已研发了与本项目相关的终端安全管理技术、体系化的信创平台终端安全技术、大数据与人工智能驱动的安全分析技术、基于零信任策略的动态自适应访问控制技术、基于微服务架构的统一终端安全框架等技术，此外，公司70余项专利、60余项软件著作权能够为本项目提供技术支撑。公司的技术积累为实施本项目提供了有力的技术支撑。

②资质积累

公司是国家规划布局重点软件企业、国家网络与信息安全通报中心技术支持单位、北京市关键信息基础设施网络安全检查工作技术支撑单位、商用密码产品生产定点单位；通过CMMI-DEV-ML-3认证、信息安全等级保护安全建设服务机构能力评估认证、ISO9001:2015质量管理体系认证、信息安全管理体系认证；拥有近百项计算机信息系统安全专用产品销售许可证、涉密信息系统产品检测证书、军用信息安全产品认证证书、商用密码产品销售许可证、涉密信息系统集成甲级资质证书、装备承制单位注册证书等权威机构颁发的产品及企业资质。众多资质积累，为本项目顺利实施且顺利投向市场提供了资质保障。

③良好的经验及合作关系积累

公司与中标麒麟、银河麒麟等操作系统厂商建立战略合作关系，不断将原有领先的终端安全技术向信创平台迁移，主动适配不同型号的信创平台计算机，开发包括主机监控审计、网络准入控制、终端安全登录和电子文档安全管理等满足信创平台安全需求的终端安全管理技术和产品。针对信创平台的合作关系及开发

经验积累，为本次项目成功实施打下坚实的基础。

④优质的客户资源积累

公司凭借在信息安全领域多年的积累，依靠自身过硬的产品和领先的技术实力，赢得了众多用户的信赖，产品被广泛应用于政府、军队、军工、能源和金融等重要行业领域的优质客户，其信息系统绝大多数是需要进行信息技术应用创新的国家关键信息基础设施。

随着我国信息产业技术创新进程的推进，将给本项目系列产品的推广、部署和应用，带来非常积极的效果。公司将以现有客户群体为基础，推广基于信创平台的信息安全产品，在原有安全产品、服务的基础上进一步为客户提供自主可控的安全防护技术、产品和服务，优质的客户资源积累，为本次项目成功实施奠定了客户基础。

（3）公司拥有覆盖面广泛的营销服务体系

公司拥有专业的信息安全研发、咨询与服务人员，目前在北京设有总部技术支持中心。总部技术支持中心采取“一站式”服务结构体系，统一服务窗口。公司现已构建了覆盖全国七大区、近三十个省市的营销与服务网络，具有较强的跨区域经营能力，可为全国的用户进行本地化的现场技术服务。同时，公司依托多年积累的成熟经销商体系，可以快速实现新产品在中小企业客户中的推广，提高市场推广和技术支持能力。公司凭借这一广覆盖、快响应的营销服务体系，能够帮助客户快速了解产品的功能和使用方法，降低新产品推广的难度，为本项目的顺利实施提供了良好的市场渠道保障。

5．项目实施的具体内容

（1）信创平台新一代终端安全防护系统

①平台简介

信创平台新一代终端安全防护平台是面向装配华为鲲鹏 CPU 或统一操作系统 UOS 的信创平台环境，基于防护监管一体化安全策略，根据国家网络安全等级保护和信息系统分级保护相关国家标准，从网络接入控制、操作系统安全加固、基线安全管理、应用与数据安全、用户实体行为分析和恶意代码检测等多个维度与层次，而打造的具有网络接入控制、主机监控审计与补丁分发、终端身份鉴别、专用服务器审计、电子文档安全管理、数据防泄漏、终端保密安全检测评估、移

动存储介质安全管理、打印刻录监控与审计和网络防病毒等安全功能的系列安全产品。利用该平台可构建面向信创平台终端的一体化安全解决方案，系统性地解决信创平台终端的网络安全问题，为信息技术创新应用进程安全护航。该平台适用于鲲鹏 CPU 或 UOS 新型操作系统构建的信创平台终端环境，包括服务器、桌面终端主机和笔记本电脑；客户端代理的主机 CPU、内存和网络带宽资源峰值占用率≤10%，平均占用率≤5%。

②系统结构

信创平台新一代终端安全防护平台专门针对新出现的具有较强市场竞争力的华为鲲鹏 CPU 及统一操作系统 UOS 信创平台环境，通过移植适配、技术升级、模块更新和功能拓展而开发的系列终端安全防护产品，由网络准入控制系统、主机监控审计与补丁分发系统、终端安全登录系统、专用服务器审计系统、电子文档安全管理系统、数据防泄漏系统、终端安全保密检测评估系统、移动存储介质安全管理系统、打印刻录监控与审计系统和网络防病毒系统等 10 余款产品组成。这些产品既可以独立运行，也能够组合在一起形成终端安全整体解决方案。除了网络准入控制系统由客户端、准入控制网关和服务端组成之外，其余系统均由客户端和服务端组成，支持分布式集中统一安全管理，支持大数据和人工智能驱动，系统结构如下图所示：

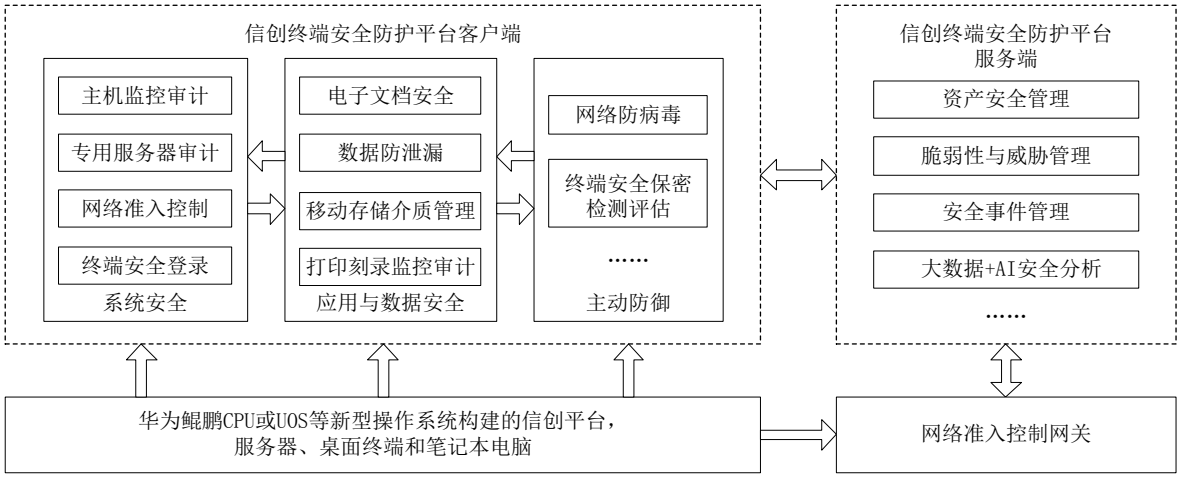


图 信创平台新一代终端安全防护平台结构

③关键技术

该平台面向信创平台终端环境创新发展了基于微服务架构的统一安全管理框架、内核级驱动拦截、基于零信任策略的动态自适应网络准入控制、基于网络流量模型的协同数据防泄漏检测、基于国密算法的透明加解密、大数据网络安全

态势感知和基于数据指纹的数据库防泄漏检测等技术，保证了产品的技术先进性。

A．基于微服务架构的统一安全管理框架

基于微服务架构，为终端安全管理提供统一的服务端与客户端框架，为上层安全管理应用开发提供统一的 API 接口、通用基础服务、数据存储和物理资源等支持，使上层应用只需关注自己的功能实现，实现插件化，从而大幅提高服务端和客户端的性能和开发效率。该架构分为物理资源层、支撑框架层、基础服务层、业务服务层和应用层五个层次。物理资源层为上层服务提供计算和存储资源；基础服务层为各类终端安全管理应用提供通用的基础服务，例如配置服务、升级服务和日志服务；业务服务层则针对边界安全、内网安全和数据安全，以低耦合度为目标，实现具体不同的安全管理服务；应用层负责适配各类终端主机，提供管理接口和用户接口。

B．内核级驱动拦截

基于防护监管一体化策略，以内核层 HOOK 系统调用为根本，以规范化的数据接口和控制接口为基础，创新融合基于哈希的账号弱口令快速识别算法、基于 Rootkit 的主机安全监控、基于 Linux 的软件非法卸载防护、基于内核层的驱动级透明加解密、基于文件访问驱动过滤与沙箱的可信行为智能识别、基于语义特征与用户行为分析的数据防泄漏检测、基于大数据的终端检测与响应等多种技术，以相对独立的模块组件嵌入到统一安全管理框架，实现对信创平台终端从操作系统行为监控、应用安全、数据安全到恶意代码防御的全方位安全管理，具备大数据采集、资产管理、行为监控、基线配置核查、补丁管理、强身份鉴别、恶意代码防御和安全审计等功能。信创平台终端成为大数据网络感知和执行安全策略的关键节点。

C．基于零信任策略的动态自适应网络准入控制

以终端安全为网络准入的唯一依据，在终端、接入交换机和网络准入控制网关上进行三重控制，基于设备身份、用户身份和终端安全，实现动态的自适应网络准入控制，同时设定访问权限，确保接入网络的终端安全可信。它监控并评估终端使其一直处于安全状态中，一旦终端被评估为不安全就将被置于隔离修复区，仅有有限的访问权限，直至被修复变成安全状态才能准入。该技术包含定性与定量相结合的主机安全评估，基于流量重定向的自动准入管理，以及策略路由、旁路干扰、VLAN 与 SNMP 协同等准入控制技术，以适应不同的信创终端应用场景。

D．大数据网络态势感知

基于开源的大数据技术和平台，以前端大数据采集、后端大数据分析和展示

为核心，通过网络和终端数据采集以及大数据分析模型，构建“数据采集、数据分析、决策支持、行动”闭环，实现基于大数据和深度学习的网络安全态势感知、威胁情报获取、业务应用性能分析、网络安全管理和安全运维管理。数据采集代理与终端安全管理代理融合，执行基于策略的数据定向采集和预处理，采集策略与大数据分析模型相关联，实现多维度、多层次的全要素数据采集。不同的应用需求具有不同的大数据分析模型，例如面向业务情景的数据盗取行为检测、APT攻击检测、用户实体行为分析、异常流量分析、业务应用性能分析、面向网络舆情监测的大数据衍生处理等模型。大数据分析模型对采集的大数据进行分析，同时又指导大数据的精准采集。基于搜索引擎技术的大规模数据存储与检索，以及内存索引方式，实现对新鲜数据的准实时查询和TB级硬盘数据的秒级查询。

E．基于网络流量模型的协同数据防泄漏检测

该技术通过采集主机产生的网络流量数据，结合数据防泄漏策略，建立并训练敏感数据模型；终端捕获主机产生的网络流量数据并将其重定向发送至最优接入节点；接入节点根据该网络流量数据决定是否与目标地址建立加密通信链路；接入节点根据当前检测节点运行状态与其他参考数据选择合适的检测节点并下发检测任务；检测节点结合检测策略与所述敏感数据模型实时识别敏感数据并反馈至接入节点；接入节点结合反馈结果与管控策略决定是否对该网络流量数据进行管控。通过该技术，能够识别并及时管控敏感外传数据，提高数据防泄漏系统对数据的安全防护能力。

F．基于数据指纹的数据库防泄漏检测

该技术针对数据库的访问进行检测，当有数据通过网络或文件进行传输时，截获传输数据，对传输数据进行分段解析，得到分段后的传输数据；根据传输数据总数据量和预先设定的允许误差率，通过基于用户指定的数据库预先建立得到的过滤器计算得到需要生成的数据指纹个数；根据需要生成的数据指纹个数，对分段后的传输数据进行哈希计算，得到数据指纹；通过过滤器进行数据指纹匹配，实现数据防泄漏。通过本技术生成的指纹信息，只占常规哈希算法指纹数据的四分之一，从而有效地解决了海量数据库的指纹存储问题；同时，由于利用了过滤器的位操作特性，极大地提高了查询速度。

④系统建设进度安排

时间（季） 项目/	2021年				2022年				2023年
	1	2	3	4	1	2	3	4	1~4

子项目									
信创平台终端安全防护平台	网络准入控制系统	需求、设计	关键技术研究	关键技术研究、编码		编码	测试、完善	发布	市场推广、升级更新
	主机监控审计与补丁分发系统	需求、设计	关键技术研究	关键技术研究、编码		测试、完善	发布	市场推广、升级更新	
	终端安全登录系统	需求、设计	关键技术研究	编码	测试、完善	发布	市场推广、升级更新		
	专用服务器审计系统	需求、设计	关键技术研究	编码		测试、完善	发布	市场推广、升级更新	
	电子文档安全管理系统	需求、设计	关键技术研究		编码		测试、完善	发布	市场推广、升级更新
	数据防泄漏系统	需求、设计	关键技术研究		编码		测试、完善	发布	市场推广、升级更新
	终端安全保密检测评估系统	需求、设计	关键技术研究		编码		测试、完善	发布	市场推广、升级更新
	移动存储介质安全管理系统	需求、设计	关键技术研究	编码	测试、完善	发布	市场推广、升级更新		
	打印刻录监控与审计系统	需求、设计	关键技术研究	编码	测试、完善	发布	市场推广、升级更新		
	网络防病毒系统	需求、设计	关键技术研究		编码		测试、完善	发布	市场推广、升级更新

（2）信创平台端点检测与响应系统

①平台简介

信创平台端点检测与响应平台利用终端威胁检测和基线安全漏洞扫描技术，实时检测资产配置信息、安全漏洞和未知安全威胁，并快速进行响应。基于多源数据的大数据安全分析，云端和终端协同，形成事前预警、事中监控、事后分析取证；高级威胁识别能力后移，从终端到云端，终端基于先验知识（特征为快速、

资源占用低）快速识别已知威胁和部分未知威胁，云端利用大数据和人工智能手段进行行为识别，发现各类安全威胁特别是未知威胁。专门针对中标麒麟、银河麒麟、中科方德和 UOS 等各类典型的信创操作系统平台，支持服务器、终端桌面主机和笔记本电脑，全面适用于私有云、公有云和混合云等不同的终端安全应用场景，满足各种规模和 IT 架构的企业或组织安全需求，大大提升了用户的网络安全防护水平以及对未知安全威胁/高级可持续性威胁的抵御能力。

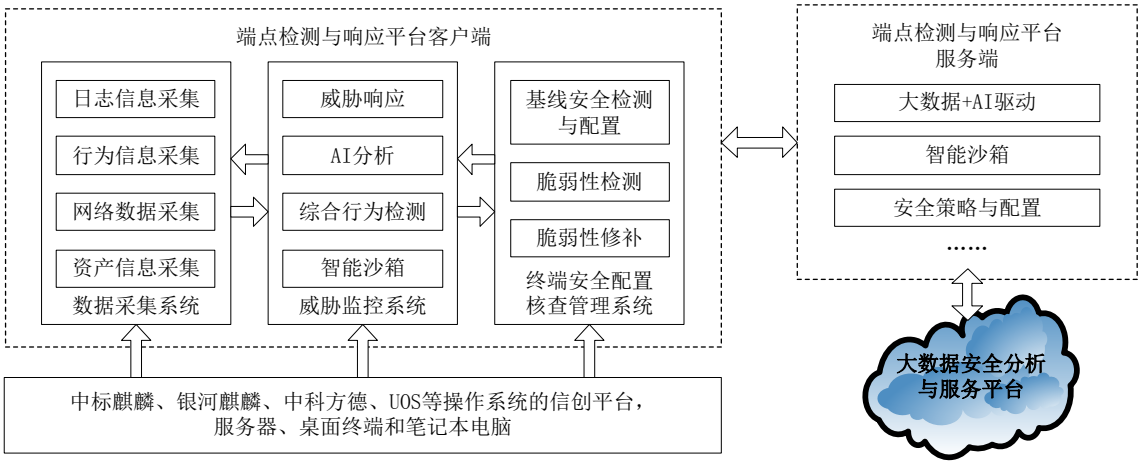
②系统结构

信创平台端点检测与响应平台包括数据采集系统、终端安全配置核查管理系统、威胁监控系统三个系统。其中，数据采集系统用于实现多维度的资产信息收集、自动与人工辅助的资产信息收集和安全相关数据采集，为大数据安全分析与服务平台提供基础数据；终端安全配置核查管理系统通过基线安全检测与配置、脆弱性检测、脆弱性修补等手段，确保终端处于基线安全状态；威胁监控系统基于行为分析和机器学习技术，通过大数据和人工智能驱动，本地检测与云端检测相结合，识别未知安全威胁和高级可持续性威胁。

该平台基于人工智能和大数据分析技术，对主机、网络、文件和用户等信息，进行深层次挖掘和多维度分析，结合云端优质威胁情报，将威胁进行可视化，并通过场景化和全局性的威胁追捕，对事件进行深度剖析，识别黑客/威胁意图，追踪威胁的扩散轨迹，评估威胁影响面，从而协同端点防护平台 EPP、网络安全管理平台 SOC、防火墙等安全产品，进行快速自动化的联动响应，将单次响应转化为安全策略，控制威胁蔓延，进行持续遏制，全面提升企业终端安全防护能力。按照全域覆盖、自主决策、主动防御的设计理念，技术和管理并重、可靠和好用兼顾、安全防护和信息系统一体，全力打造态势全网感知、设备协同联动、结构动态捷变、技术高效融合的动态安全防御体系。

信创平台端点检测与响应平台由客户端代理和服务端组成，采用分布式体系结构，客户端代理运行在信创平台的服务器、桌面终端主机和笔记本电脑上，服务端既可独立部署，安装在专门的服务器上，与客户端代理构建完整的产品运行架构，并与大数据安全分析与服务平台联动，也可与大数据安全分析与服务平台融为一体，成为其大安全体系下的一个组成部分。

端点检测与响应平台系统结构如下图所示：



③关键技术

信创平台端点检测与响应平台综合采用智能沙箱、机器学习、大数据关联分析、APT 攻击分析和计算机取证等技术，实现对已知或未知网络安全威胁的检测、遏制和调查，形成完整的全局安全威胁视图，并针对信创终端进行系统修复。

A．智能沙箱

智能沙箱技术既在客户端实现，也在云端（服务端）实现，只是实现的类型和程度不同。它是针对可疑代码进行动态行为分析的关键技术，通过模拟各类虚拟资源，创建严格受控和高度隔离的程序运行环境，运行并提取可疑代码运行过程中的行为信息，实现对未知恶意代码的快速识别。通过重定向技术来支撑智能沙箱隔离，在可疑代码样本的地址空间中拦截相关操作，并将可能导致的更改重定位到虚拟资源上，比如虚拟文件系统、虚拟硬件系统、虚拟注册表系统、虚拟化句柄。这样，通过重定向技术使得恶意代码的任何修改都不会破坏到真实的用户系统。智能沙箱的检测包括静态分析、动态分析以及相应智能数据解析几个过程，最终形成输出报告，判定可疑代码的安全属性。

B．机器学习

机器学习技术是人工智能的核心，在大规模数据处理中，可以自动分析获得规律，然后利用这些规律预测未知的数据。机器学习一般有两个步骤：分类器训练和模型检测。首先利用训练集文件的向量模型及其类别标记生成分类器，其次利用分类模型对待检测数据进行分类检测，通过将分类结果与真实样本数据进行比对，评估分类器的效果，最后根据结果进一步完善分类器。在端点检测与响应

中，机器学习主要应用于端点用户和软件的正常行为和异常行为的提取，通过捕获大量的端点静态和动态的用户和软件行为特征向量，采用机器学习的方法进行端点用户和软件行为的训练建模和分类检测，得出该使用场景下用户和软件的正常和异常行为知识库，而利用知识库可以更加高效地检测出端点的异常行为。

C．大数据关联分析

端点采集的系统日志、进程线程启停信息、文件系统访问信息和网络流量等各类安全相关数据是终端安全中防御、检测和响应的重要依据。对海量终端安全数据进行自动智能化的关联分析，追溯其攻击过程，寻找漏洞源和威胁源，是有效防御和确保终端安全的重要途径和方法。大数据关联分析的主要目标是不丢失终端安全相关的重要信息，并通过分析原始终端安全数据而形成缜密连贯的全局攻击视图。为了应对 APT 攻击的极强持续性和阶段性，关联分析过程中应尽量收集各层面、各阶段的全方位信息，同时适量将时间窗口拉大，通过宽时间域数据分析提取具有内在关联的若干属性，识别出攻击发生的时间、地点、攻击类型和强度等信息。

D．APT 攻击分析

通过对攻击者一次完整的攻击行为所采用的攻击步骤进行关联分析，根据检测到的攻击发生的时间序列，将该次完整的攻击的每一步攻击步骤以图形的形式重新表示出来，进行攻击场景的重构。攻击场景重构通过对关联规则及知识的形式化表述，将庞杂、无序的安全数据流转换为结构化、易于理解的攻击场景，将反映攻击过程和意图的场景图呈现出来，发现攻击者的攻击策略和目的，甚至推测漏报的告警和预测下一步可能的攻击行为，以协助管理员人员获取更有价值的网络安全信息，以便于安全管理员做出及时有效的应急响应。

E．计算机取证

计算机取证是端点检测与响应的重要工作过程，需要对具有足够可靠和有说服力的，存在于计算机、网络、电子设备等数字设备中的数字证据，进行确认、保护、提取和归档，形成完整的威胁情报信息。计算机取证要适应各种终端应用场景，能够进行云计算环境取证、智能终端取证和大数据取证等，自动定位和采集端点入侵电子证据，降低取证分析的技术门槛，提高取证效率及其分析结果的准确性，为端点安全事件调查、打击网络犯罪提供技术支持。

④**系统建设进度安排**

<table>
<tr><td colspan="2" rowspan="2">时间（季）
项目/子项目</td><td colspan="4">2021 年</td><td colspan="4">2022 年</td><td>2023 年</td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>1</td><td>2</td><td>3</td><td>4</td><td>1~4</td></tr>
<tr><td rowspan="3">信创平台端点检测与响应平台</td><td>数据采集系统</td><td>需求、设计</td><td colspan="2">关键技术研究、编码</td><td>编码</td><td>测试、完善</td><td>发布</td><td colspan="3">市场推广、升级更新</td></tr>
<tr><td>终端安全配置核查管理系统</td><td>需求、设计</td><td colspan="2">关键技术研究、编码</td><td>编码</td><td>测试、完善</td><td>发布</td><td colspan="3">市场推广、升级更新</td></tr>
<tr><td>威胁监控系统</td><td>需求、设计</td><td>关键技术研究</td><td colspan="2">关键技术研究、编码</td><td>编码</td><td>测试、完善</td><td>发布</td><td colspan="2">市场推广、升级更新</td></tr>
</table>

6．项目实施主体

本项目由北信源负责实施。

7．项目效益情况

本项目中信创平台新一代终端安全防护系统、信创平台端点检测与响应系统，是对公司现有产品进行的升级、更新、扩展，无法单独核算因本次募集资金使用而产生的效益。根据公司现有竞争优势、技术积累以及行业发展趋势，预期本项目实施后，将对公司收入、利润产生积极影响。

8．项目备案与批准情况

（1）本项目拟利用现有及租赁相关办公场地，不涉及土地购置事项。

（2）本项目相关备案正在办理中。

（3）本项目为软件研发类项目，非生产型项目，不产生废气、废水、固体废弃物等污染物，根据生态环境部《建设项目环境影响评价分类管理名录》及北京市生态环境局《〈建设项目环境影响评价分类管理名录〉北京市实施细化规定（2019 年本）》，不属于需要编制环境影响报告书、环境影响报告表或者填报环境影响登记表的情形。

（二）基于私有服务器的安全移动办公平台项目

1．项目概述

基于私有服务器的安全移动办公平台（以下简称“移动办公平台”）为公司因应办公智能化、移动化的发展趋势，依托在信息安全市场多年的技术和经验积累，依据公司在业绩提出的私有化移动办公理念，通过在互联网或专网上构建安全的办公基础设施，为客户提供个性化的办公平台。本次移动办公平台项目拟重点建设移动办公系统、视频会议系统、商业秘密沟通系统，保障用户对办公数据、安全性和服务质量的有效控制，实现移动办公的开放性和安全性之间的平衡。

项目总投资额为 39,907.67 万元，拟使用募集资金 39,907.67 万元，详见下表：

序号	名称	金额（万元）	比例	拟使用募集资金（万元）
1	建设投资	18,002.50	45.11%	18,002.50
1.1	工程费用	18,002.50	45.11%	18,002.50
1.1.1	建筑安装工程费用	1,252.50	3.14%	1,252.50
1.1.2	设备及软件购置费用	16,750.00	41.97%	16,750.00
2	基本预备费	540.08	1.35%	540.08
3	项目实施费	16,499.97	41.35%	16,499.97
3.1	租赁费用	1,099.97	2.76%	1,099.97
3.2	人员工资	15,100.00	37.84%	15,100.00
3.3	测试费用	300.00	0.75%	300.00
4	铺底流动资金	4,865.11	12.19%	4,865.11
5	**合计**	39,907.67	100.00%	39,907.67

2．项目建设的背景

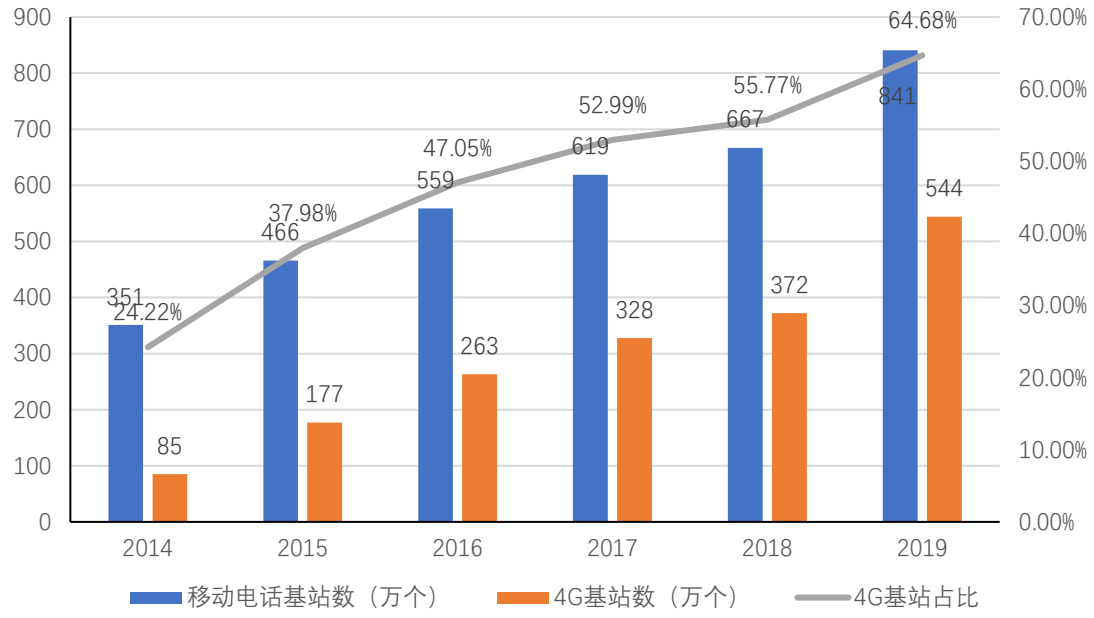
（1）移动通信环境持续优化，移动办公条件日益成熟

高速移动互联网的普及为移动办公创造了必要的发展条件。近年来，我国持续加大移动通信基站的建设力度，并逐步提高 4G 基站比例。2019 年，全国净增移动电话基站 174 万个，总数达 841 万个。其中 4G 基站总数达到 544 万个，5G 网络建设稳步推进。移动电话基站连年增长的同时，4G 基站占比也逐年上升，2019 年达到 64.68%[7]，4G 基站的普及及 5G 的大力建设，保障了移动网速的高

[7] 工业和信息化部，《2019 年通信业统计公报》，http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057511/n3057518/c7696204/content.html。

速传递，为移动办公提供了基础设施保障。

2014-2019 年我国移动基站建设情况[8]



数据来源：工业和信息化部

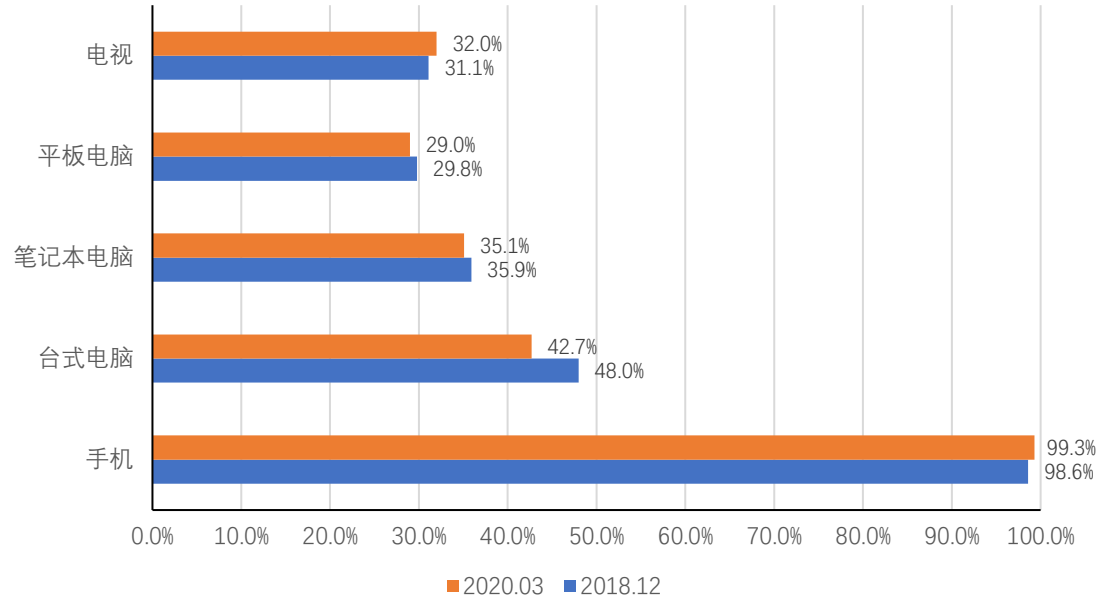
移动办公与当下互联网设备轻量化需求相契合，上网工具渐渐由电脑转向智能手机等移动设备。截至 2020 年 3 月，我国网民使用手机上网比例高达 99.3%，较 2018 年底提升 0.7 个百分点，使用台式电脑、笔记本电脑上网比例分别为 42.7% 和 35.1%[9]，台式电脑使用比例下降明显。随着科技的进步，智能手机等移动设备的功能越来越完善，办公需求就是其中之一。现代人对移动终端存在高度依赖，开发移动办公应用更加适应新型管理方式。

我国网民上网接入设备统计情况[10]

[8] 工业和信息化部，《2019 年通信业统计公报》，http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057511/n3057518/c7696204/content.html。

[9] 中国互联网信息中心，第 45 次《中国互联网络发展状况统计报告》

[10] 中国互联网信息中心，第 45 次《中国互联网络发展状况统计报告》



数据来源：中国互联网信息中心

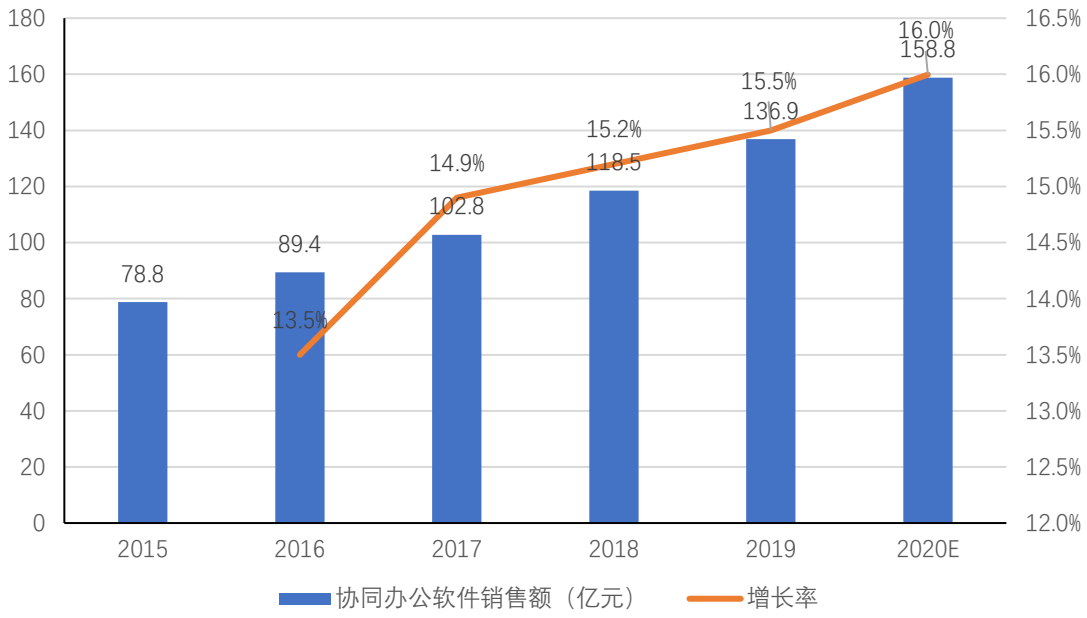
（2）企业数量稳定增长，移动办公市场潜力巨大

我国企业数量逐年增加，信息化转型需求迫切，市场规模潜力巨大。近些年，国家经济迅猛发展，市场经济展现出充足的活力。在过去十年间我国企业数量快速增长，由 1,136 万户增长为 3,858 万户，年复合增长率为 14.55%[11]。

目前尚未有权威数据对整个移动办公行业进行统计，但专业的协同办公软件市场规模正在不断变大。根据中国软件行业协会发布的《2019 中国软件与信息服务业发展报告》显示，协同办公软件销售总额 2019 年达到 136.9 亿元，同比增长 15.5%，2020 年预计达到 158.8 亿元[12]。

2016-2020 年我国协同办公软件市场规模情况[13]

[11] 市场监督管理总局，《全国市场主体发展基本情况》，http://www.samr.gov.cn/zhghs/tjsj/。
[12] 中国软件行业协会，《2019 中国软件与信息服务业发展报告》。
[13] 中国软件行业协会，《2019 中国软件与信息服务业发展报告》。



数据来源：中国软件行业协会

协同办公软件市场的快速增长，吸引越来越多厂商开始参与市场竞争。随着云计算和移动互联网的普及，以阿里钉钉和腾讯企业微信为代表的互联网厂商以免费或低价的策略，凭借自身技术、流量、品牌、资金等方面优势，迅速抢占市场。互联网厂商初期产品以简洁轻便为主，主要集中于中小企业。截至 2020 年 3 月底，钉钉用户数超过 3 亿，企业组织数超过 1500 万家[14]。企业微信 2020 年 5 月宣布，其已为数百万企业提供服务[15]。随着市场开发进度深入，移动办公普及，越来越多科技企业开始布局移动办公市场。

（3）突发疫情推动行业爆发，移动办公行业市场需求旺盛

新冠疫情影响之下，远程办公需求短期迅速增加。为抢占市场，各大厂商纷纷对旗下产品进行免费推广体验，移动办公软件下载量和用户量迎来暴增。2020 年 2 月 5 日，阿里巴巴旗下移动办公软件“钉钉”在苹果应用商店下载量首次超过微信，排行第一，这也是苹果应用商店首次出现办公类软件排行第一[16]。其他移动办公类软件下载量也突飞猛进，因疫情造成交通阻隔，视频会议能较好的解

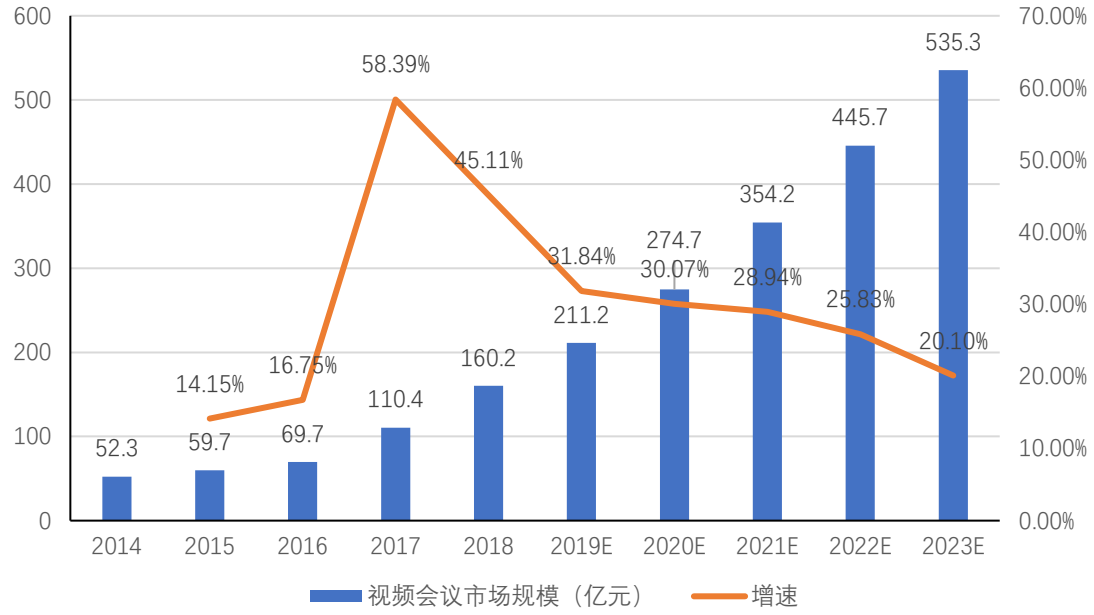
[14] 钉钉官方，《2020 钉钉春夏新品发布会》，https://36kr.com/p/711945636665864?spm=a213l2.14527612.3134967900.1.4bde687aMdGAED&acm=lb-zebra-656835-8252898.1003.4.7789753&scm=1003.4.lb-zebra-656835-8252898.OTHER_15814735234031_7789753。

[15] 环球网，《企业微信：5 个月服务微信用户数从 6000 万至 2.5 亿》，https://tech.huanqiu.com/article/3yI4cgExvjX。

[16] IT 之家，《钉钉首次超过微信，跃居苹果应用商店排行榜第一》，2020 年 2 月 5 日，https://www.ithome.com/0/471/633.htm。

决办公、沟通等问题，给企业带来直观的服务体验。本次突发的疫情，短期内提升了企业使用视频会议的意愿，通过时间培育，使用户养成视频会议的习惯，后期通过高效便捷的服务和相对低廉的成本，使免费客户转化为付费客户，提高行业渗透率。根据 Frost & Sullivan 数据统计，基于硬件的传统视频会议市场逐渐萎缩，新兴的软件视频会议和云视频会议迅速发展，我国视频会议市场 2018 年达到 160.2 亿元，预计市场将于 2019 年至 2023 年间实现高达 26.2%的年均复合增长，于 2023 年达到 535.3 亿元规模[17]。

2014-2023 年我国视频会议市场规模[18]



数据来源：Frost & Sullivan

3．项目建设必要性

（1）顺应全球办公移动化趋势发展的迫切需要

移动办公是当今高速发展的通信业与 IT 业交融的产物，它将通信业在沟通上的便捷、用户上的规模，与 IT 业在软件应用上的成熟、业务内容上的丰富完美地结合到了一起，使之成为了继无纸化办公、互联网远程化办公之后的新一代办公模式。移动办公借助移动设备的便利性，摆脱了传统办公场所、设备等地理位置限制，为电子政务、企业协同、商务沟通提供了高效迅捷的工作平台，对于

[17] Frost & Sullivan，《中国视频通信行业概览》，2019 年 4 月。
[18] Frost & Sullivan，《中国视频通信行业概览》，2019 年 4 月。

突发性事件的处理、应急性事件的部署有极为重要的意义，对于企业的核心竞争力也有着日益重要的影响，成为全球最流行的办公模式。据美国 ABC 新闻网统计，2019 年全球约有 2,000 万人远程工作，占比世界人口约为 0.3%[19]。

新冠疫情在全球的爆发，进一步加速了移动办公的渗透率。华为指出疫情爆发后我国远程办公人数从 500 万增长到 3 亿，远程教育由 2.32 亿增长至 4.32 亿[20]，远程办公成为新冠疫情下的大型社会实践，移动办公规模进一步提升。全球范围内各大企业也在积极倡导员工远程办公，谷歌和 Facebook 要求员工在家办公，并将这一政策延长至 2021 年；亚马逊要求西雅图总部 5 万多名员工在家远程工作，并将政策至少延长至 2020 年 10 月份；Twitter 从 3 月 11 日起强制员工在家办公，并声明最早 2020 年 9 月份重启现场办公[21]。根据盖洛普预测，到 2028 年，全球将有 73%的工作交付将远程处理[22]。移动办公作为远程办公的主要应用形式，在本次疫情中扮演重要角色，成为众企业争相使用的应用。鉴于办公移动化的全球趋势，公司有必要尽快实施移动办公项目，以抢占移动办公市场和企业服务入口。

（2）市场对高安全性移动办公产品的迫切需求

移动办公运行需要一个覆盖“云、管、端”的完整互联网信息系统，移动办公应用在提升办公效率的同时，也面临着网络安全的风险。移动办公应用传输和存储着企业的核心数据和商业机密，对安全的要求更为苛刻。从移动办公的设备、通道和终端三个方面来看，移动办公应用面临风险主要分为三类：移动应用 APP 安全风险，移动应用通信安全风险，移动应用服务端安全风险[23]。、

移动应用安全风险是指智能设备端的 APP 面临信息泄露、应用仿冒、用户身份冒用、个人隐私侵犯等四类主要安全风险；移动应用通信安全风险是指在移动数据传输过程中，面临的信息泄露和非法篡改等风险；移动应用服务端安全风险是指数据存储端，包括 Web 服务器、应用服务器、数据库服务器、数据存储

[19] 中金公司，《主题研究：数字化办公，疫情如何改变我们的工作习惯》，2020 年 5 月 27 日。
[20] 华为《科技抗疫： 运营商网络洞察和实践白皮书》，https://carrier.huawei.com/cn/technical-topics/fixed-network/Anti-epidemic-technology。
[21] 每日经济新闻，《深度：推特允许部分员工永久在家办公》，http://www.nbd.com.cn/articles/2020-05-18/1435469.html。
[22] 中金公司，《主题研究：数字化办公，疫情如何改变我们的工作习惯》，2020 年 5 月 27 日。
[23] 中国网络安全产业联盟，《移动办公及业务应用安全保障白皮书》，2020 年 3 月。

设备等面临包括拒绝服务、入侵攻击、恶意代码、越权操作、以及单点故障等风险。这些风险长期存在于网络环境中，威胁着移动办公数据的真实性、完整性、机密性和可用性。

目前市场上存在众多移动办公产品，既有传统协同办公的泛微网络、致远互联和蓝凌等，也有互联网巨头旗下的钉钉、企业微信、飞书、WeLink 等。传统协同办公软件主要客户集中在大中型企业和特殊机构等，协同办公技术储备雄厚，但均非安全行业出身。互联网厂商主打中小微企业，对信息安全的重视程度较高，但因服务对象较多，很难做到企业信息的独立维护和存储。市场缺乏主打安全防护的移动办公产品。政府、军工、能源、金融等机构和组织对互联网应用产品的安全性更为看重，市场存在较大缺口。安全稳定的运行环境是移动办公的基础条件和必要前提，市场对高安全性移动办公应用存在迫切需求。

（3）完善公司战略发展与产品创新布局的迫切需求

公司积极响应国家“新基建”发展战略，顺应信息化技术的发展浪潮，按照国家信息产业相关发展规划，适应国家政策指引下产业结构战略调整趋势，为进一步满足国家党政机关、企事业单位及互联网用户的互联网应用环境及移动办公应用需求，在全面分析国内外移动办公行业竞争情况和竞争优势的前提下，深度剖析把握移动办公产业发展的规律，以既有的即时通信、信息安全、大数据等相关的软硬件技术为基础，以提供高效、便捷、安全的移动办公平台及相关应用生态为核心目标，建设移动办公项目，开启办公应用场景化、应用移动化、工具服务化的移动办公之路。该项目将依托“信源豆豆”体系，以办公高效、通信安全、应用丰富为目标，针对移动办公数据流转、应用协作、隐私保护、应急调度等问题，为用户提供更优质的移动办公服务。

为此，公司将紧密围绕自身的发展战略，深度整合移动通信和信息安全领域的核心技术、研发力量和市场能力等资源，以本次项目增发为契机，通过利用募集资金开展移动办公项目的建设，增强公司的软件开发能力及自主创新能力，使公司移动办公主营产品和服务得以本质性提升，成为全球领先的移动办公产品和解决方案提供商。

4．项目建设的可行性

（1）国家政策支持信息化产业发展

长期以来，国家一直在努力推进企业的信息化进程，并多次出台相关产业政策，鼓励企业加速办公智能化、协同化和云端化。

2015 年，国务院印发《关于积极推进“互联网+”行动计划的指导意见》[24]，鼓励建立网络化、智能化、服务化、协同化的“互联网+”产业生态体系；2016 年网信办通过《移动互联网应用程序信息服务管理规定》[25]对移动互联网应用提出监管要求，对其进行规范管理，并建立健全网络用户信息安全保障体制；2017 年工信部印发《关于进一步推进中小企业信息化的指导意见》[26]的通知，鼓励和支持中小企业充分利用云计算、大数据、移动互联网等信息技术，获得以租代建、支持核心业务发展、覆盖企业经营管理链条的便捷信息化服务，降低信息化应用的成本和门槛；2018 年工信部印发《推动企业上云实施指南（2018-2020 年）》[27]，稳妥有序推进企业上云，强化政策支持，积极发展协同办公、生产管理、财务管理、营销管理、人力资源管理等各类 SaaS 服务，为上云企业提供业务支撑。

2018 年 12 月召开的中央经济工作会议，首次提出“加快 5G 商用步伐，加强人工智能、工业互联网、物联网等新型基础设施建设”[28]，“新型基础设施建设”的提法由此产生。随后“加强新一代信息基础设施建设”被列入 2019 年政府工作报告。2020 年 3 月 4 日，中共中央政治局常务委员会召开会议指出，加快推进国家规划已明确的重大工程和基础设施建设，加快 5G 网络、数据中心等新型基础设施建设进度[29]。“新基建”更着眼于“新”，有着更多科技内涵，其聚焦的领域比如 5G、物联网、工业互联网、智能制造等都是面向未来的“硬核科技”，符合产业升级需要，也代表着中国经济高质量发展的方向。工业互联网、车联网、

[24] 国务院，《国务院关于积极推进“互联网＋”行动的指导意见》国发〔2015〕40 号，http://www.gov.cn/zhengce/content/2015-07/04/content_10002.htm。

[25] 互联网信息办公室，《移动互联网应用程序信息服务管理规定》，http://www.cac.gov.cn/2016-06/28/c_1119122192.htm。

[26] 工信部，《关于进一步推进中小企业信息化的指导意见》工信部企业〔2016〕445 号，http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757016/c5475728/content.html。

[27] 工信部，《工业和信息化部关于印发推动企业上云实施指南（2018-2020 年）的通知》工信部信软〔2018〕135 号，http://www.gov.cn/xinwen/2018-08/12/content_5313305.htm。

[28] 央视网，中央经济工作会议，2018 年 12 月 21 日，http://news.cctv.com/2018/12/21/ARTI93Cwl0GAzC5dJpsxF9Aj181221.shtml?spm=C94212.PZmRfaLbDrpt.S83334.1。

[29] 新华网，中共中央政治局常务委员会召开会议，2020 年 3 月 4 日，http://m.xinhuanet.com/2020-03/04/c_1125663518.htm。

企业上云、远程医疗、远程办公、人工智能等是 “新基建”的主要应用领域，移动办公作为企业上云和远程办公的重要实现路径，在疫情的催发下，成为“新基建”的优先爆发应用场景。

密集发布的产业指导政策，充分体现政府对企业信息化、企业上云的大力支持。移动办公基于移动设备、移动通信和云端服务，使办公信息化和云端化，提高工作效率，降低运营成本，符合国家政策指引，是国家大力提倡的办公新趋势。

（二）公司拥有雄厚的技术积累

公司长期深耕信息安全领域，持续注重研发投入，保证安全技术的可靠性和领先性。经过多年积累，公司在信息安全、大数据和即时通信领域有了长足的发展。移动办公平台涉及移动互联、云计算、即时通信、信息安全、图形图像处理等领域的一系列关键技术，在这些技术领域和应用公司已经积累雄厚的技术基础。

在传统信息安全领域，经过多年积累，公司具备提供网络安全领域的软件设计开发、技术咨询、关键设备研发、系统集成服务、大数据、移动互联等应用业务的较强业务能力，随着信息技术应用创新的进一步落地，公司产品技术竞争力将得到进一步释放。公司在网络安全技术相关领域拥有高度的话语权和市场地位，曾获得国家科技进步二等奖及多项省部级科技进步一等奖，承担多项大型国家科研项目，同时积极开展产学研合作和上下游技术攻关，成果颇为丰硕。

在安全通信应用领域，公司全力打造的“新一代安全通信聚合平台-信源豆豆”是以“安全连接，智慧聚合”为核心理念，以私有服务器为载体，以即时通信为基础的安全可信聚合平台，有效满足万物互联时代的安全即时通信需求。“信源豆豆”具备高安全性，支持服务器、通信链路到客户端全程加密，对通信、存储、访问和使用模式进行四维安全防护,提供了丰富的即时通信功能和独特的安全远程办公功能，同时还提供开放结构，支持第三方的多类型应用。公司组建了高水平的区块链团队，依托“信源豆豆”，展开了数据存证、健康医疗、社区管理等方面的应用研发，并为进一步开拓海内外市场做好了基础性铺垫。

公司在信息安全领域和移动应用开发领域积累的技术，为本项目的顺利实施提供了切实保障。

5. 项目的具体内容

（1）移动办公系统

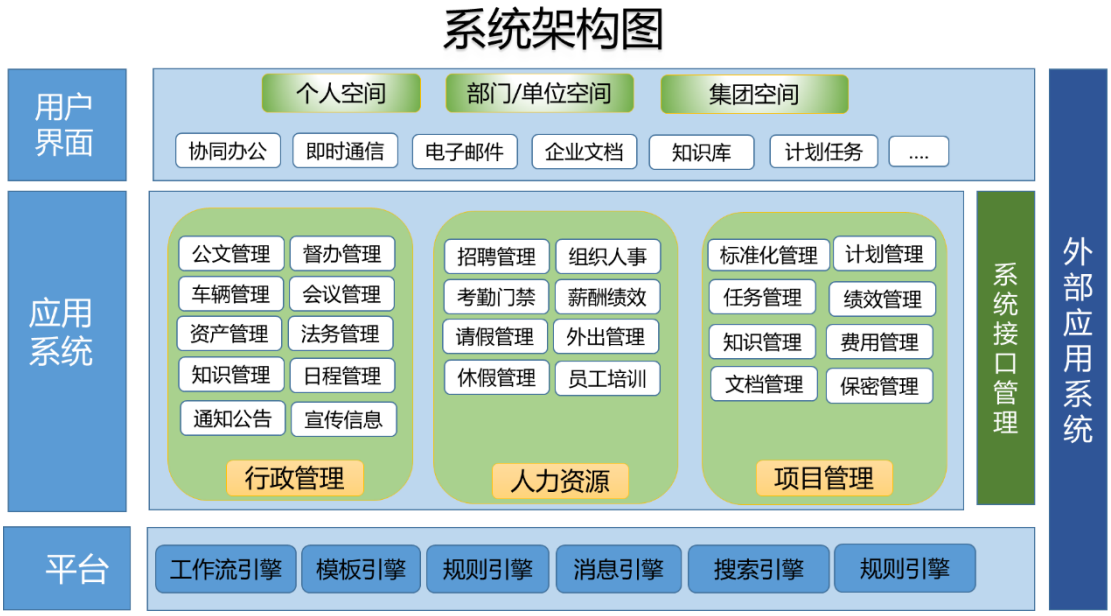
①系统概述

移动办公的研究与开发的目标是构建一套全生命周期内强化安全防护的协同办公环境，即从终端数据的产生、加工、流转、存储、共享与输出等每一个办公业务处理环节，通过将多种安全防护技术和自动化办公技术有机结合，实现安全的在线移动办公。

②系统方案

A．系统架构

移动办公中的组件分为基础组件、应用组件两个部分，具体技术架构如下如所示：



本项目此次研发，主要提供对移动办公运行所必须的各项基础功能体系的构建、管理和调试等功能。本次研发方向移动办公组件主要包含：

序号	组件名称	功能概述
1	前端框架组件	前端界面公共组件库。
2	业务生成组件	应用管理的核心组件之一，涉及到业务生成所必须的各种设计器和功能组件。如模块编辑器、表单设计器、视图设计器、报表设计器等等。
3	工作流引擎	应用管理的核心组件之一，涉及到业务生成中审批流程

		有关的组件，如图形化工作流程设计器、流程建模、流程实例管理等。
4	模板引擎	采用模板框架技术，负责服务器后台文本处理和预处理 Web 页面数据（后台渲染）等。
5	规则引擎	以规则引擎为基础，规则 API 满足 JSR-94 规范，对系统业务逻辑提供描述、规则设定和规则解释等。
6	消息引擎	负责系统内部消息（如逻辑状态生成与监控、日志），用户消息（如 IM、邮件、通知、提醒等）的统一设计和管理。
7	搜索引擎	分为全文搜索引擎和字段搜索引擎。为办公类业务加入特定的权限控制所构成。字段搜索引擎则提供基于关系型数据表的查询、汇总、呈现的有关逻辑。
8	权限引擎	满足 RBAC 规范，为系统内的全部资源（如菜单、视图、数据项、操作等）提供统一的权限模型和权限管理。

B．系统终端安全技术

移动终端安全管理涉及移动设备管控、数据保护和网络访问控制等方面，具体为：

移动设备管控，具有移动终端管控能力，实现覆盖移动终端的注册、部署、使用、淘汰等环节的全生命周期管理，保证终端丢失或被盗后的终端查找和数据防护，可远程擦除数据、远程锁定终端等，最大限度的保护数据安全；移动终端管控包含设备管理、安全策略管理、文档下发管理、应用安装管理等。

数据保护，在进入移动安全门户的安全沙箱应用时，终端安全运行环境进行安全自检，检测网络是否正常连接至专网，同时合规策略检查是否有无关应用在后台启动运行，防止数据泄露隐患，同时检测终端有无被 ROOT，一旦异常则触发告警，防止数据泄露；在退出移动安全门户之后，移动终端将业务应用使用的内存空间进行释放清除，防止通过内存访问泄露数据；对于安全沙箱内产生的业务数据进行用户无感的自动加密处理，保证数据自动加密存储，自动解密阅读，保护数据安全；同时沙箱应用及文件策略支持禁用截屏、添加水印，禁用复制粘贴等功能，避免用户泄露数据信息。在移动终端清退、淘汰使用或者更换使用时，可以直接卸载安全沙箱，同时将安全沙箱内所有应用数据擦除，防止淘汰终端时数据泄露隐患。

网络访问控制，通过移动终端安全管理系统，控制移动终端利用无线局域网和移动通信网络的网络访问。

本项目涉及移动终端安全管理技术主要为：

a．隐写溯源技术

系统通过隐写溯源技术,可以对打印输出的文档进行溯源追踪，在文档泄漏的情况下，能够有效锁定文档所有者，并对文档的泄漏进行责任认定,从而实现文档全生命周期管理，保障密级文档的安全。系统对泄密后的打印纸质文档扫描、拍照及电子文档显示截图、拍照等数字化图像或残存的部分图像数据导入本系统，即可高精度提取识别事先隐藏的安全信息标识，从而进行文件泄密源头的追溯。

b．与电子文档密标管理系统的无缝集成技术

移动应用服务区各模块通过与电子文档密标管理系统的结合,实现保障密级标志文档不可被非授权查阅、复制以及编辑，实现对密级文档从预定密、定密、签发、流转、使用、审计。

c．移动终端身份认证技术

移动终端的接入访问支持基于口令、生物特征方式的认证，结合信任服务系统数字证书认证，可实现双因子认证；通过设备合规准入策略实现访问控制，可保障接入系统终端的合规性，避免异常设备接入。此外，针对涉密应用可设置应用锁，在移动终端使用时需进行二次密码验证，保证安全性。

d．移动终端单点登录访问控制

终端管理系统用户中心对接与单位业务网用户身份认证，实现用户同步及用户信息获取。支持办公应用集成实现单点登录，登录移动安全门户即可访问移动门户网站、在线交流系统、移动办公业务系统等应用，无需再次输入密码，用户方便快捷地使用办公应用。访问控制功能，可通过终端管理系统对用户进行授权，设定用户所能安装访问的应用及移动终端接收的安全策略。

e．区块链技术

通过区块链的智能合约技术将原本属于不同业务领域的处理流程有机的衔接起来，实现协同办公自动化的升级，通过建立跨业务的信任链、用智能合约编织起整个自动化办公网。

③系统建设时间进度安排

时间（季） 项目/子项目	2021 年				2022 年				2023 年	
	1	2	3	4	1	2	3	4	1~2	3~4

移动办公	底层工作引擎	需求、设计	关键技术研究	关键技术研究、编码		编码	测试、完善	发布	
	前端应用框架	需求、设计	关键技术研究	关键技术研究、编码		测试、完善	发布		
	行政管理系统		需求分析	方案设计	关键技术研究	编码		测试与完善	发布	市场推广与升级更新
	人力资源系统		需求分析	方案设计	关键技术研究	编码		测试与完善	发布	市场推广与升级更新
	项目管理系统		需求分析	方案设计	关键技术研究	编码		测试与完善	发布	市场推广与升级更新

（2）视频会议系统

视频会议系统分为硬件层、功能层两个方面。体系架构如下图所示：

①功能层—专业视频会议及会控系统

A．实现多种专业会议模式

主持人管理会议秩序、提升助理管理人员维持会议秩序、参会人员麦克状态控制，参会人员摄像头状态控制，支持多种会议类型，将会议进行分类，使会议更贴合与用户使用场景。主要分为：讨论模式、讲座模式、直播模式等。

讨论模式：最多允许开启 9 路摄像头，默认麦克风开启，摄像头关闭，适用于 16 人以内的群组讨论等会议场景；

讲座模式：最多允许开启 9 路摄像头，默认麦克风关闭，摄像头关闭，适用于 50 人以内的培训、讲座等会议场景；

直播模式：最多允许开启 3 路摄像头，默认麦克风禁用，摄像头禁用，适用于 50 人以上的直播场景。

B．具备多种发起形式

群内发起：会议房间按群内事件进行划分，讨论中可以快速的使用群会议来发起会议进行沟通；

预约会议：会议可提前预订好，到达指定时间自动发起；

微会议(小程序)自由发起：无限制的发起会议，可选择联系人，组织机构，群中的成员自由地创建音视频会议房间开会。

C．丰富的会议功能

屏幕共享：可共享当前屏幕、正在运行的应用、共享分屏；

会议文档共享：在会议中可添加文档和其他会议人员分享会议相关资料；

会议聊天：会议期间可通过会议聊天，进行一些纪要性的沟通或讨论，不打扰主讲人或讨论双方的对话；

会议半屏及会议全屏预览：放大视频区域，可以满足便携设备能够更清晰的看到对方分享的视频内容。

D．其它扩展功能

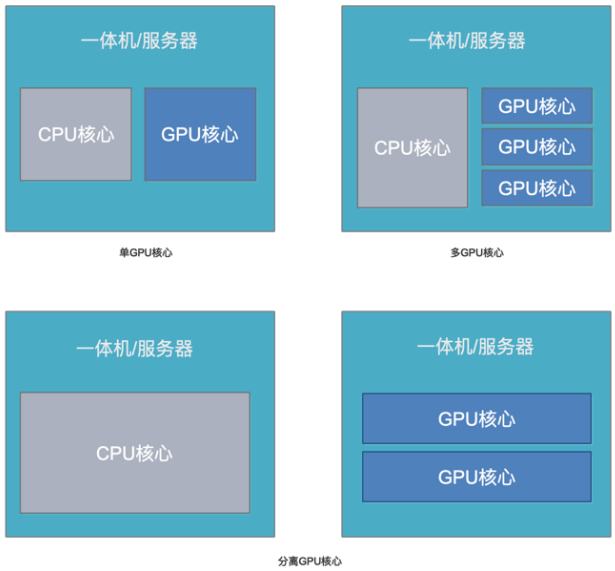
专用会议应用：所有会议可通过该应用进行统一参与和管理；

视频会议 SDK 二次开发包-视频会议开放集成系统：利用现有的视频会议组件，研究一套可扩展集成的标准，通过标准使其他厂商的应用 APP 可以集成北信源视频会议的 SDK，此系统使得视频会议更加自由和更强可扩展性。

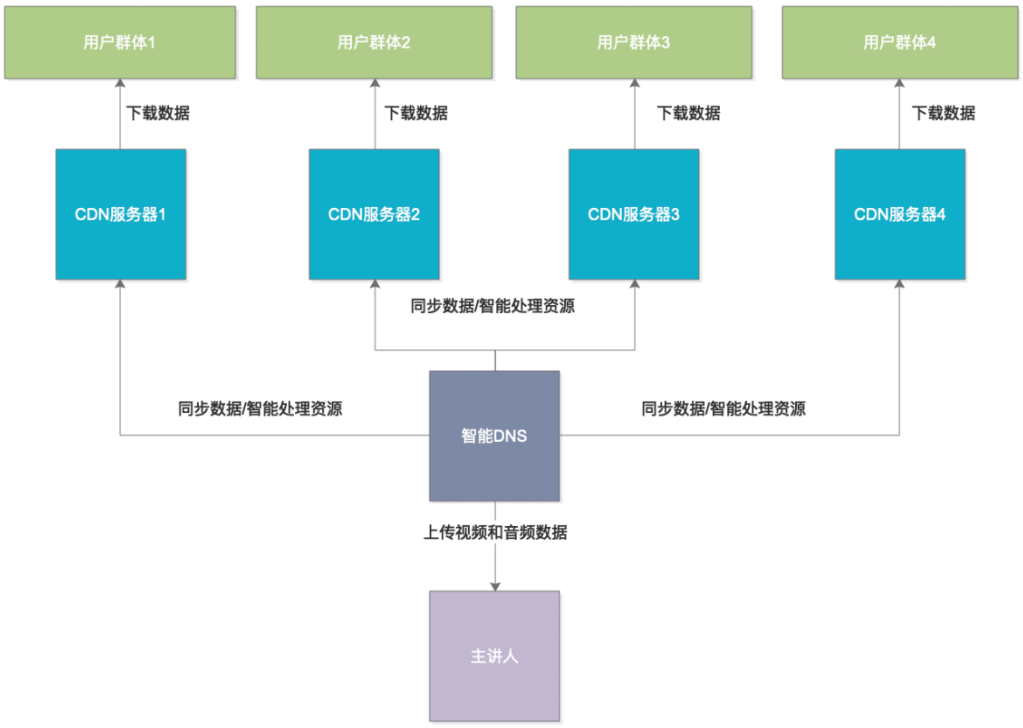
②硬件层—专用混流加速套件

在 GPU 流处理器架构下用 CUDA 技术实现编码并行化,并针对流处理器架构特点进行内存读写等方面的优化，合理划分 CPU 和 GPU 之间的资源分配，使之可以最大化的利用性能，防止资源浪费。

GPU 核心的部署方案：



通过 CDN 技术架构，搭建安全的 CDN 服务体系，使用户实现更高性能的直播会议。



③系统建设时间进度安排

时间（季） 项目/子项目		2021 年				2022 年				2023 年	
		1	2	3	4	1	2	3	4	1~2	3~4
视	硬件层	需求、	关键	关键技术研		测	发布				

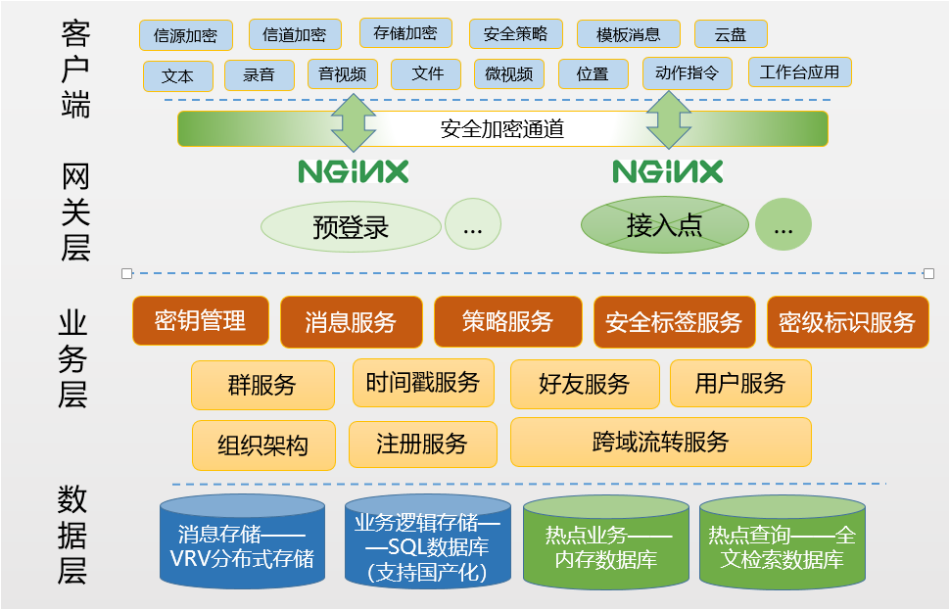
频会议	与操作系统层	设计	技术研究	究、编码		试、完善				
	信令协商与媒体交换层	需求、设计	关键技术研究	关键技术研究、编码		测试、完善	发布			
	媒体处理层	需求、设计	关键技术研究	方案设计 关键技术研究		编码		测试与完善	发布	
	SDK 层		需求分析	方案设计	关键技术研究	编码		测试与完善	发布	
	用户层		需求分析	方案设计	关键技术研究	编码		测试与完善	发布	市场推广与升级更新

（3）商业秘密沟通系统

①系统概述

商业秘密一旦泄露将可能损失经济利益，影响运营安全和竞争优势。因商业秘密的安全性，对应的信息沟通也要保证在安全的情况下进行。为了加强商业密码沟通的安全性，需从多个角度，全链路的考虑信息沟通和交流的安全保护。在传统的对信息加密措施和消息通道的 https 处理之外，我们又考虑了多种措施保证信息的安全，防止被监听、被伪造、被篡改，主要包括：端到端加密、通信代理、消息通道加密和独立对象标识及存储。

商业秘密沟通系统的架构图如下图所示：



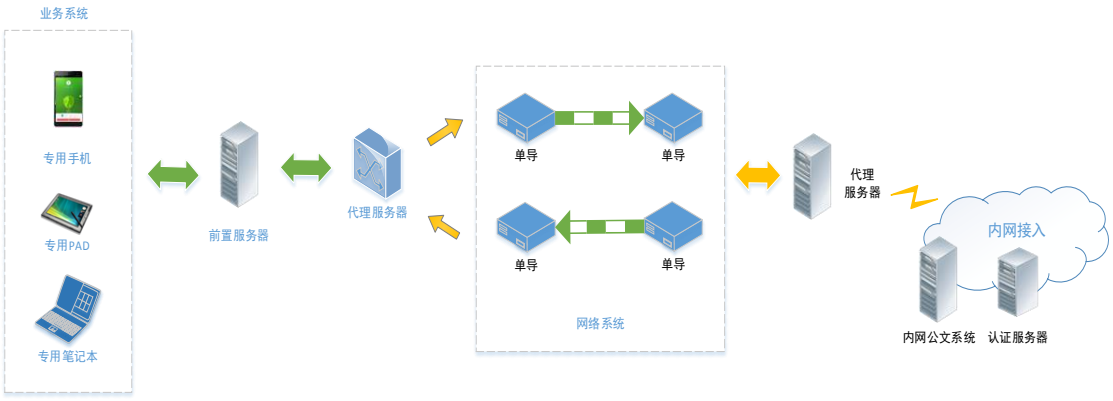
②系统技术与功能

A．端到端加密

消息以端到端的信源加密为保护的基础手段，在终端之间的消息传递采用端到端加密方式，在会话建立之初进行端到端密钥协商，随后的会话中密钥不断的在更换，服务器在整个生命周期中不知道任何用户的密钥，并且实现一条消息一个密钥，密钥不重复，保证消息不会被截获破解，从而实现了安全的端到端加密。

B．通信代理

通信代理的整体思路为代理服务器在网络的两端，负责解决不同网络协议的差异，把内外网的数据经过代理服务器的转码、封装和处理，并提供给对方业务系统可识别的接口。对业务系统来说，网络访问的接口一致，统一而规范，数据只要传输给通信代理服务器后，由通信代理服务器保证通信的准确性和及时性，并屏蔽网络协议的细节对业务系统的影响。通信代理的功能架构如下图所示：



TCP 协议代理的方式实现代理服务器之间的通讯，TCP 协议代理屏蔽了应用层协议的差异（可适配多种网络）；在代理服务器中配置一个唯一的端口和 IP 地址的映射，客户端将访问地址配置为代理服务器的地址和对应的端口，客户端通过 IP 和端口访问标准的代理服务器通信服务接口。

C．消息通道加密

消息通道加密是指通过一定技术手段对通信信道进行加密，是一种通过保护信源信息明文或对代表明文的电信号进行加密，使消息不被非法截获或破译的保密方式。

信道加密采用链路和网络加密技术为各通信节点间传输的群路信息进行加密，支持国密、商密以及自定义加密方式。为了适应客户场景业务变化的需求，增加对加密算法可配置化，插件方式进行选择和适配的功能。

D、独立对象标识及存储

通过给对象增加标识，即一个对象一个标识，标识内容包括级别，所属信息，权限范围等，同时对对象进行加包和拆包操作，就算获取文件，没有读写中间件也无法访问。依据文件的标识级别，进行不同的分级化存储，不同标识级别的数据进行不同的存储策略，原则上高级别的对象有更高的安全性，更多的存储空间，更安全的备份恢复策略等。

系统投资概算

③系统建设时间进度安排

<table>
<tr><td colspan="2" rowspan="2">时间（季）
项目/子项目</td><td colspan="4">2021 年</td><td colspan="4">2022 年</td><td colspan="2">2023 年</td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td><td>1</td><td>2</td><td>3</td><td>4</td><td>1~2</td><td>3~4</td></tr>
<tr><td rowspan="4">商业秘密沟通</td><td>数据存储层</td><td>需求、设计</td><td>关键技术研究</td><td colspan="2">关键技术研究、编码</td><td>测试、完善</td><td>发布</td><td></td><td colspan="3"></td></tr>
<tr><td>通信业务逻辑层</td><td>需求、设计</td><td>方案设计</td><td colspan="2">关键技术研究</td><td colspan="2">编码</td><td colspan="2">测试与完善</td><td>发布</td><td></td></tr>
<tr><td>通信网关层</td><td>需求、设计</td><td>关键技术研究</td><td colspan="2">方案设计
关键技术研究</td><td colspan="2">编码</td><td colspan="2">测试与完善</td><td>发布</td><td></td></tr>
<tr><td>客户端</td><td></td><td>需求分析</td><td>方案设计</td><td colspan="3">关键技术研究与编码</td><td colspan="2">测试与完善</td><td>发布</td><td>市场推广与升级更新</td></tr>
</table>

6．项目实施主体

本项目由北信源负责实施。

7．项目效益情况

本项目是公司在现有产品基础上进行的升级、拓展，研发升级后的产品实现的效益是公司对该产品历史累计投入的结果，无法单独核算因本次募集资金使用而产生的效益。根据公司现有竞争优势、技术积累以及行业发展趋势，预期本项目实施后，将对公司收入、利润产生积极影响。

8、项目备案与批准情况

（1）本项目拟利用现有及租赁相关办公场地，不涉及土地购置事项。

（2）本项目相关备案正在办理中。

（3）本项目为软件研发类项目，非生产型项目，不产生废气、废水、固体废弃物等污染物，根据生态环境部《建设项目环境影响评价分类管理名录》及北京市生态环境局《〈建设项目环境影响评价分类管理名录〉北京市实施细化规定（2019 年本）》，不属于需要编制环境影响报告书、环境影响报告表或者填报环境影响登记表的情形。

三、本次募集资金使用对公司经营管理、财务状况的影响

（一）对公司经营管理的影响

本次发行募集资金拟投资的项目符合国家相关的产业政策以及公司未来的发展方向，具有良好的发展前景和综合效益，有助于巩固和夯实公司的研发优势，提升公司的核心竞争力，增强公司的综合实力。

（二）对公司财务状况的影响

本次发行募集资金到位后，公司的总资产和净资产规模将有所增长，资产负债率水平得到降低，资金实力将有效提升，整体实力得到增强。

本次发行募集资金拟投资的项目围绕公司战略和主营业务开展，募集资金项目顺利实施后，公司在相关领域的研发优势将进一步得以提升，公司的相关产品将得到有效优化，从而能够更好地满足快速增长的市场需求。但由于公司募集资金投资项目所涉及产品的经营效益需要一定的时间才能体现，因此短期内不排除公司每股收益被摊薄的可能性。

四、可行性分析结论

本次发行的募集资金投向符合国家产业政策及行业发展方向，募集资金投资项目具有良好的发展前景和综合效益，有利于有效推进公司的发展战略，有助于巩固和夯实公司的研发优势，提升公司的核心竞争力，增强公司的综合实力，符合公司及全体股东的利益。

北京北信源软件股份有限公司

董事会

二〇二〇年七月十五日