证券代码：300768　　证券简称：迪普科技

杭州迪普科技股份有限公司

（杭州市滨江区通和路 68 号中财大厦 6 楼）

2020 年度向特定对象发行股票并在创业板上市

募集说明书

（申报稿）

保荐人（主承销商）

中信建投证券股份有限公司
CHINA SECURITIES CO.,LTD.

二〇二〇年十月

公司声明

1、本募集说明书按照《公司法》、《证券法》、《创业板上市公司证券发行注册管理办法（试行）》、《公开发行证券的公司信息披露内容与格式准则第36 号——创业板上市公司向特定对象发行证券募集说明书和发行情况报告书（2020 年修订）》、《公开发行证券的公司信息披露内容与格式准则第 37 号——创业板上市公司发行证券申请文件（2020 年修订）》等要求编制。

2、公司及董事会全体成员保证本募集说明书内容真实、准确、完整，确认不存在虚假记载、误导性陈述或重大遗漏，并对其内容的真实性、准确性、完整性承担个别和连带的法律责任。

3、本次发行完成后，公司经营与收益的变化，由公司自行负责；因本次发行引致的投资风险，由投资者自行负责。

4、本募集说明书是公司董事会对本次发行的说明，任何与之相反的声明均属不实陈述。

5、投资者如有任何疑问，应咨询自己的股票经纪人、律师、专业会计师或其他专业顾问。

6、本募集说明书所述事项并不代表审批机关对于本次发行相关事项的实质性判断、确认、批准或核准，本募集说明书所述本次发行相关事项的生效和完成尚需经深圳证券交易所审核通过并经中国证监会同意注册。

特别提示

1、本次向特定对象发行股票事宜已经公司第二届董事会第三次会议及 2020 年第一次临时股东大会审议通过。根据有关法律法规规定，本次发行尚需经深圳证券交易所审核通过并经中国证监会同意注册。

2、本次向特定对象发行股票的发行对象不超过 35 名（含 35 名），为符合中国证监会规定条件的法人、自然人或其他合法投资组织；证券投资基金管理公司、证券公司、合格境外机构投资者、人民币合格境外机构投资者以其管理的二只以上产品认购的，视为一个发行对象；信托公司作为发行对象，只能以自有资金认购。

最终发行对象由公司股东大会授权董事会在本次发行申请经深圳证券交易所审核通过并经中国证监会同意注册后，按照中国证监会、深圳证券交易所的相关规定，根据竞价结果与保荐机构（主承销商）协商确定。所有投资者均以现金认购公司本次发行的股份。若国家法律、法规对此有新的规定，公司将按新的规定进行调整。

3、本次发行采用竞价方式，本次发行的定价基准日为发行期首日。发行价格为不低于定价基准日前二十个交易日公司股票交易均价的 80%（定价基准日前二十个交易日股票交易均价=定价基准日前二十个交易日股票交易总额/定价基准日前二十个交易日股票交易总量）。

本次发行的最终发行价格将在公司本次发行申请经深圳证券交易所审核通过并经中国证监会同意注册后，由公司董事会与保荐机构（主承销商）按照相关法律、法规、规章和规范性文件的规定，以竞价方式确定。若国家法律、法规对此有新的规定，公司将按新的规定进行调整。

若公司股票在定价基准日至发行日期间发生派息、送股、资本公积转增股本等除权除息事项，本次发行底价将作相应调整。

4、本次发行股票数量按照募集资金总额除以发行价格确定，同时本次发行股票数量不超过 40,000,000 股（含），未超过本次发行前公司总股本的 10%。最终发行数量将在本次发行申请经深圳证券交易所审核通过并经中国证监会同意

注册后，由公司董事会根据公司股东大会的授权及发行时的实际情况，与本次发行的保荐机构（主承销商）协商确定。若本次发行的股份总数因监管政策变化或根据发行审批文件的要求予以调整的，则本次发行的股票数量届时将相应调整。

在本次发行董事会决议公告日至发行日期间，若公司发生派息、送股、资本公积转增股本等除权除息事项，本次发行股票数量的上限将作相应调整。

5、本次发行对象认购的股份自发行结束之日起六个月内不得转让。法律法规、规范性文件对限售期另有规定的，依其规定。

本次发行对象因由本次发行取得的公司股份在锁定期届满后减持还需遵守《公司法》、《证券法》、《深圳证券交易所创业板股票上市规则》等法律法规、规章、规范性文件、交易所相关规则以及公司《公司章程》的相关规定。本次发行结束后，由于公司送股、资本公积转增股本等原因增加的公司股份，亦应遵守上述限售期安排。

6、本次发行拟募集资金总额不超过 101,500.00 万元（含），募集资金扣除发行费用后的净额用于下述项目：

单位：万元

序号	项目名称	项目总投资	拟投入募集资金
1	新一代IT基础设施平台研发项目	63,265.07	45,354.00
2	智能测试、验证及试制基地建设项目	67,269.25	56,146.00
合计		**130,534.32**	**101,500.00**

注：项目名称系以经政府有关部门正式备案的名称为准。

若实际募集资金不能满足上述募集资金用途需要，公司将根据实际募集资金净额，按照轻重缓急的原则，调整并最终决定募集资金投入优先顺序及各项目具体投资额等使用安排，募集资金不足部分由公司自筹资金解决。

本次发行募集资金到位前，公司将根据市场情况及自身实际情况以自有或自筹资金择机先行投入募集资金投资项目。募集资金到位后，依照相关法律法规要求和程序置换先期投入。

7、本次发行完成后，公司在本次发行前滚存的截至本次发行完成时的未分配利润将由本次发行完成后的新老股东按发行后的持股比例共同享有。

8、本次发行不会导致公司控股股东、实际控制人发生变化，亦不会导致公

司股权分布不具备上市条件。

9、公司重视对投资者的持续回报，公司现行有效的《公司章程》符合中国证监会《关于进一步落实上市公司现金分红有关事项的通知》（证监发[2012]37号）和《上市公司监管指引第 3 号—上市公司现金分红》（证监会公告[2013]43号）的相关要求。同时，公司制定了《杭州迪普科技股份有限公司未来三年（2020-2022 年）股东分红回报规划》，该规划已经公司第二届董事会第三次会议及 2020 年第一次临时股东大会审议通过。

10、根据《国务院关于进一步促进资本市场健康发展的若干意见》（国发[2014]17 号）、《国务院办公厅关于进一步加强资本市场中小投资者合法权益保护工作的意见》（国办发[2013]110 号）和《关于首发及再融资、重大资产重组摊薄即期回报有关事项的指导意见》（中国证监会公告[2015]31 号）要求，为保障中小投资者利益，公司制定了本次发行后填补被摊薄即期回报的措施，公司控股股东、实际控制人、董事、高级管理人员对公司填补回报措施能够得到切实履行作出了承诺，相关措施及承诺事项等议案已经公司第二届董事会第三次会议及 2020 年第一次临时股东大会审议通过。

本次发行后填补被摊薄即期回报的措施及相关承诺请参见本募集说明书“第六节 与本次发行相关的声明”。公司制定填补回报措施不等于对公司未来利润作出保证，投资者不应据此进行投资决策，投资者据此进行投资决策造成损失的，公司不承担赔偿责任，提请广大投资者注意。

11、本次向特定对象发行股票方案最终能否取得深圳证券交易所审核通过并经中国证监会同意注册及其他有关部门的审核通过尚存在较大的不确定性，提醒投资者注意相关风险。

目 录

释 义

本募集说明书中，除非另有说明，下列词语或简称具有如下特定含义：

一、一般名词释义

迪普科技、发行人、公司、本公司	指	杭州迪普科技股份有限公司
本次发行、本次向特定对象发行股票	指	杭州迪普科技股份有限公司 2020 年向特定对象发行股票的行为
本募集说明书	指	《杭州迪普科技股份有限公司 2020 年度向特定对象发行股票并在创业板上市募集说明书（申报稿）》
股东大会	指	杭州迪普科技股份有限公司股东大会
董事会	指	杭州迪普科技股份有限公司董事会
监事会	指	杭州迪普科技股份有限公司监事会
公司章程	指	《杭州迪普科技股份有限公司章程》
思道惟诚	指	杭州思道惟诚投资管理合伙企业（有限合伙）
经略即远	指	杭州经略即远投资管理合伙企业（有限合伙）
格物致慧	指	杭州格物致慧投资管理合伙企业（有限合伙）
闻涛岭潮	指	杭州闻涛岭潮投资管理合伙企业（有限合伙）
中移创新	指	中移创新产业基金（深圳）合伙企业（有限合伙）
方广创投	指	苏州方广创业投资合伙企业（有限合伙）
杭州哲创	指	杭州哲创投资合伙企业（有限合伙）
迪普信息	指	杭州迪普信息技术有限公司，公司的全资子公司
中国移动	指	中国移动通信集团有限公司总部、各分公司及受其控制的子公司
中国联通	指	中国联合网络通信有限公司总部、各分公司及受其控制的子公司
中国电信	指	中国电信集团有限公司总部、各分公司及受其控制的子公司
三大运营商	指	中国移动、中国联通和中国电信
全国人大常委会	指	全国人民代表大会常务委员会
国家发展改革委	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
公安部	指	中华人民共和国公安部
中央网信办	指	中共中央网络安全和信息化领导小组办公室
国家网信办	指	中华人民共和国互联网信息办公室
中央保密办	指	中共中央保密委员会办公室
国家保密局	指	中华人民共和国国家保密局

中央密码办	指	中共中央密码工作领导小组办公室
国家密码局	指	中华人民共和国国家密码管理局
IDC	指	International Data Corporation，国际数据公司
Frost & Sullivan	指	弗若斯特沙利文咨询公司
启明星辰	指	北京启明星辰信息技术股份有限公司（002439.SZ）
绿盟科技	指	北京神州绿盟信息安全科技股份有限公司（300369.SZ）
北信源	指	北京北信源软件股份有限公司（300352.SZ）
任子行	指	任子行网络技术股份有限公司（300311.SZ）
天融信	指	北京天融信科技有限公司
深信服	指	深信服科技股份有限公司（300454.SZ）
F5 网络（美国）	指	F5 Networks,Inc. （FFIV.O）
星网锐捷	指	福建星网锐捷通讯股份有限公司（002396.SZ）
东土科技	指	北京东土科技股份有限公司（300353.SZ）
安恒信息	指	杭州安恒信息技术股份有限公司（688023.SH）
山石网科	指	山石网科通信技术股份有限公司（688030.SH）
奇安信	指	奇安信科技集团股份有限公司（688561.SH）
《公司法》	指	《中华人民共和国公司法》
《证券法》	指	《中华人民共和国证券法》
定价基准日	指	发行期首日
报告期	指	2017 年、2018 年、2019 年及 2020 年 1-6 月
报告期各期末	指	2017 年末、2018 年末、2019 年末及 2020 年 6 月末
最近三年	指	2017年、2018年及2019年
A 股	指	境内上市的人民币普通股股票
中国证监会、证监会	指	中国证券监督管理委员会
深交所	指	深圳证券交易所
上交所	指	上海证券交易所
元、万元、亿元	指	人民币元、人民币万元、人民币亿元

二、专业名词或术语释义

FW	指	Firewall，防火墙
IPS	指	Intrusion Prevention System，入侵防御系统
WAF	指	Web Application Firewall，Web 应用防火墙
Guard	指	迪普科技异常流量清洗产品

Probe	指	迪普科技异常流量检测产品
DAC	指	迪普科技物联网设备应用控制系统产品
DPI	指	Deep Packet Inspection，深度包检测
ADX	指	迪普科技应用交付平台产品
UAG	指	迪普科技上网行为管理及流控系统产品
DeepCache	指	迪普科技高速缓存加速系统产品
UMC	指	迪普科技统一管理中心产品
DPX	指	迪普科技深度业务路由交换网关产品
LSW	指	迪普科技盒式交换机产品
WLAN	指	Wireless Local Area Networks，无线局域网
AC	指	Access Controller，无线接入控制器
AP	指	Access Point，无线访问接入点
XR	指	迪普科技路由器产品
UTM	指	Unified Threat Management，统一威胁管理
ConPlat	指	迪普科技 L2~7 融合操作系统
APP-X	指	迪普科技高性能硬件架构
APP-ID	指	迪普科技应用识别与威胁特征库
VSM	指	Virtual Switching Matrix，虚拟交换矩阵
FPGA	指	Field Programmable Gate Array，即现场可编程门阵列
Web	指	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
IPv6	指	Internet Protocol version 6，互联网协议第六版
L2~7	指	网络系统结构的二层至七层。网络系统结构的七层参考模型将整个网络通信的功能划分为七个层次，由低到高分别是物理层、数据链路层、网络层、传输层、会话层、表示层、应用层。每层完成一定的功能，每层都直接为其上层提供服务，并且所有层次都互相支持。四层到七层主要负责互操作性，而一层到三层则用于创造两个网络设备间的物理连接
漏洞	指	在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，使攻击者能够在未授权的情况下访问或破坏系统
病毒	指	编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码
蠕虫	指	通过网络和电子邮件进行复制和传播的计算机病毒
间谍软件	指	从计算机上搜集信息，并在未得到该计算机用户许可时便将信息传递到第三方的软件
僵尸网络	指	一组被植入恶意程序的可控主机以及若干控制它们的主机所组成的网络，攻击者可以用来发动 DDoS 攻击、发送垃圾邮件或窃取用户信息等

网页挂马	指	把恶意代码嵌入到正常的网页中，使 PC 终端中木马，达到盗取用户信息、控制 PC 等非法目的
跨站脚本	指	利用网站漏洞把恶意的脚本代码注入到网页之中，当其他用户浏览这些网页时，就会执行其中的恶意代码，对受害用户可能采取 Cookie 资料窃取、会话劫持、钓鱼欺骗等各种攻击
SQL 注入	指	通过把 SQL 命令插入到 Web 表单递交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意 SQL 命令的攻击手段
DDoS 攻击	指	分布式拒绝服务（Distributed Denial of Service）攻击，借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动攻击，使计算机或网络无法提供正常的服务
APT 攻击	指	高级持续性威胁（Advanced Persistent Threat）攻击，利用先进的攻击手段对特定目标进行长期持续性网络攻击
黑客	指	Hacker，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
负载均衡	指	Load Balance，将工作任务分摊到多个网络设备和服务器，增加吞吐量、加强网络数据处理能力
VPN	指	Virtual Private Network，虚拟专用网络
SSL	指	Secure Sockets Layer，安全套接层协议层
MRP	指	Material Requirement Planning，物料需求计划，根据生产计划及库存情况，逐步推导出产品所需要的零部件、原材料等的采购方式
PCBA	指	PCB Assembly，将各种电子元器件通过表面封装工艺组装在印制电路板上
“交钥匙”工程	指	通过完备的产品线、以及针对各行业特点设计的完善的解决方案体系，为用户交付可以完整满足需求并可直接使用的整个网络，而不再需要用户自己进行复杂的网络设计与实施工作，可以有效降低用户工作复杂度
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
工业互联网	指	工业系统与高级计算、分析、感应技术以及互联网连接融合，通过智能机器间的连接及人机连接，结合硬件、软件、大数据、人工智能等新技术，升级关键的工业领域，重构全球工业、激发生产力
人工智能	指	是研究、开发用于模拟、延伸和扩展人的智能的理论、方法、技术及应用系统的一门新的技术科学
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
物联网	指	是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
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
5G	指	第五代移动电话行动通信标准，也称第五代移动通信技术，外语缩写：5G

本募集说明书中，除特别说明外，所有数值保留两位小数，若出现总数与各分项数值之和尾数不符的情况，均为四舍五入原因造成。

第一节 发行人基本情况

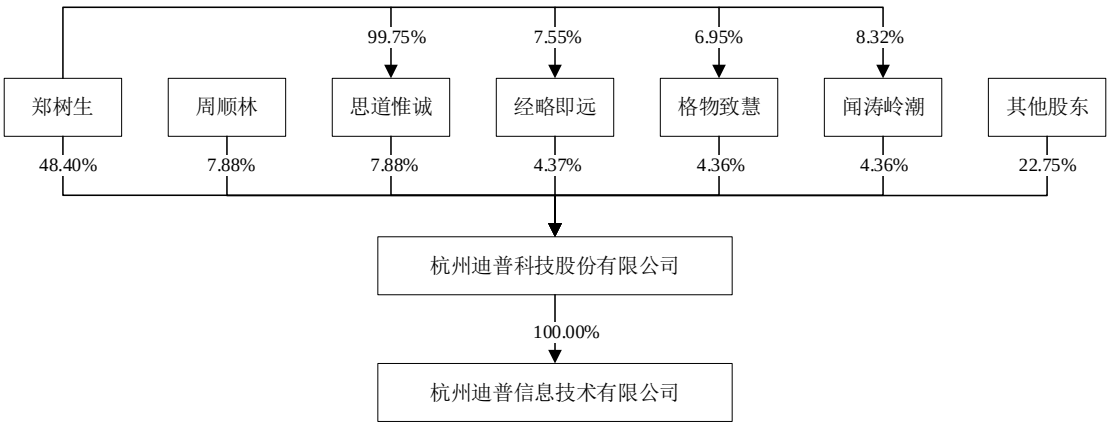
一、发行人基本情况概要

公司名称：	杭州迪普科技股份有限公司
英文名称：	Hangzhou DPtech Technologies Co., Ltd.
注册资本：	400,010,000 元
法定代表人：	郑树生
成立日期：	2008 年 5 月 28 日
上市日期	2019 年 4 月 12 日
股票简称：	迪普科技
股票代码：	300768
董事会秘书：	邹禧典
注册地址：	杭州市滨江区通和路 68 号中财大厦 6 楼
办公地址：	杭州市滨江区通和路 68 号中财大厦
邮政编码：	310051
电话号码：	0571-2828 1966
传真号码：	0571-2828 0900
公司网址：	http://www.dptech.com/
电子信箱：	public@dptech.com
经营范围：	一般项目：网络与信息安全软件开发；信息安全设备制造；计算机软硬件及外围设备制造；网络设备制造；信息安全设备销售；网络设备销售；软件销售；互联网安全服务；信息系统运行维护服务；信息技术咨询服务（除依法须经批准的项目外，凭营业执照依法自主开展经营活动）。 许可项目：商用密码产品销售；计算机信息系统安全专用产品销售；货物进出口（依法须经批准的项目，经相关部门批准后方可开展经营活动，具体经营项目以审批结果为准）。

二、股权结构、控股股东及实际控制人情况

（一）公司股权结构

截至 2020 年 6 月末，公司股权结构如下：



（二）前十大股东持股情况

截至 2020 年 6 月末，公司前十大股东持股情况如下：

序号	股东姓名/名称	持股数量（股）	持股比例	持有有限售条件股份数量（股）
1	郑树生	193,611,490	48.40%	193,611,490
2	周顺林	31,535,715	7.88%	31,535,715
3	思道惟诚	31,535,715	7.88%	31,535,715
4	经略即远	17,498,180	4.37%	-
5	格物致慧	17,432,728	4.36%	-
6	闻涛岭潮	17,432,728	4.36%	-
7	中移创新	13,788,699	3.45%	-
8	方广创投	6,792,282	1.70%	-
9	邹禧典	6,306,758	1.58%	4,730,068
10	杭州哲创	4,182,618	1.05%	-
合　计		**340,116,913**	**85.03%**	**261,412,988**

（三）控股股东及实际控制人情况

截至本募集说明书签署日，公司控股股东、实际控制人为郑树生，其直接持有公司 48.40%的股份，通过思道惟诚间接控制公司 7.88%的股份，合计控制公司 56.29%的股份，为公司控股股东及实际控制人。

此外，郑树生通过非控制的经略即远、格物致慧和闻涛岭潮间接持有公司的股份，截至本募集说明书签署日，郑树生直接和间接共持有公司 57.26%的股份。

公司控股股东及实际控制人郑树生的基本情况如下：

郑树生先生，1966 年出生，中国国籍，无境外永久居留权，身份证号码为

3301061966********。1993 年毕业于浙江大学通信与电子专业，获博士学位。1993 年至 2003 年，任职于华为技术有限公司，历任研发项目经理、中试部总监、生产部总监、技术支持部总监、交换事业部总裁、国内营销管理办公室主任、公司常务副总裁；2003 年至 2012 年，任杭州华三通信技术有限公司总裁；2013 年至 2016 年，任杭州迈尚股权投资有限公司（已注销）董事长；2012 年起，任职于本公司，历任执行董事，2016 年至今，任本公司董事长兼总经理。现兼任杭州宏杉科技股份有限公司董事长、苏州光格设备有限公司董事。

三、所处行业的主要特点及行业竞争情况

依据国家统计局《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”。依据证监会《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”。

按照公司主营业务的产品和服务的领域，公司属于信息安全行业。

（一）行业主管部门、监管体制以及主要法律法规政策

1、行业主管部门和行业监管体制

信息安全行业主要受信息产业及安全主管部门的监管，具体如下：

主管部门	主要职能
工信部	负责产业政策的研究制定、产业标准的制定、信息化建设的政府推动、国家产业扶持基金的管理和软件产品认证以及软件企业、系统集成资质认证、电子认证服务资质等企业资质评估等工作。
公安部	负责公共信息网络的安全监察工作、信息安全及等级保护的监督管理工作和信息安全产品的销售许可工作等。
国家发展改革委	综合分析高技术产业及产业技术的发展态势，组织拟订高技术产业发展、产业技术进步的战略、规划和重大政策；统筹信息化的发展规划与国民经济和社会发展规划、计划的衔接平衡；组织推动技术创新和产学研联合等。
中央网信办 国家网信办	着眼国家安全和长远发展，统筹协调涉及经济、政治、文化、社会及军事等各个领域的网络安全和信息化重大问题；研究制定网络安全和信息化发展战略、宏观规划和重大政策；推动国家网络安全和信息化法治建设，不断增强安全保障能力。
中央保密办 国家保密局	管理和指导保密技术工作，负责办公自动化和计算机信息系统的保密管理，指导保密技术产品的研制和开发应用，对从事涉密信息系统集成的企业资质进行认定。
中央密码办 国家密码局	拟订密码工作发展规划，起草密码工作法规并负责密码法规的解释，组织拟订密码相关标准；依法履行密码行政管理职能，管理密码科研、生产、装备(销售)，测评认证及使用,查处密码失泄密事件和违法违规研制、使用密码行为，负责有关密码的涉外事宜；对密码工作部门实施业务领导；负责网络与信息系统中密码保障体系的规划和管理，规划、建设和管理国家密码基础设施。

主管部门	主要职能
国家市场监督管理总局	直属单位中国网络安全审查技术与认证中心（原中国信息安全认证中心），依据《网络安全法》《网络安全审查办法》及国家有关强制性产品认证法律法规，承担网络安全审查技术支撑和认证工作；在批准范围内开展与网络安全相关的产品、管理体系、服务、人员认证和培训等工作；同时设有国家信息安全产品质量监督检验中心（北京）。授权机构中国信息安全测评中心，专门从事信息技术安全测试和风险评估等。
全国信息安全标准化技术委员会	负责组织开展国内信息安全有关的安全技术、安全机制、安全服务、安全管理、安全评估等领域的标准化技术工作。

2、行业主要法律法规政策

公司所处行业的主要法律法规政策如下：

发布时间	发文单位	文件名称	内容概要
2020 年 4 月	国家网信办、国家发展改革委、工信部、公安部、国家安全部、财政部、商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、国家保密局、国家密码局	《网络安全审查办法》	为了确保关键信息基础设施供应链安全，维护国家安全，关键信息基础设施运营者采购网络产品和服务，影响或可能影响国家安全的，应当进行网络安全审查。网络安全审查坚持防范网络安全风险与促进先进技术应用相结合、过程公正透明与知识产权保护相结合、事前审查与持续监管相结合、企业承诺与社会监督相结合，从产品和服务安全性、可能带来的国家安全风险等方面进行审查。
2019 年 10 月	全国人大常委会	《中华人民共和国密码法》	规范密码应用和管理，促进密码事业发展，保障网络与信息安全，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益。
2019 年 8 月	国家市场监督管理总局、国家标准化管理委员会	《信息安全技术 大数据安全管理指南》	提出了大数据安全管理基本原则，规定了大数据安全需求、数据分类分级、大数据活动的安全要求、评估大数据安全风险，适用于各类组织进行数据安全管理。
2019 年 5 月	国家市场监督管理总局、国家标准化管理委员会	《信息安全技术 网络安全等级保护基本要求》、《信息安全技术 网络安全等级保护测评要求》、《信息安全技术 网络安全等级保护安全设计技术要求》	指导网络运营者、网络安全企业、网络安全服务机构开展网络安全等级保护安全技术方案的设计和实施，指导测评机构更加规范化和标准化地开展等级测评工作，进而全面提升网络运营者的网络安全防护能力。
2018 年 9 月	公安部	《公安机关互联网安全监督检查规定》	规范公安机关互联网安全监督检查工作，预防网络违法犯罪，维护网络安全，保护公民、法人和其他组织合法权益。
2018 年 7 月	工信部、国家发展改革委	《扩大和升级信息消费三年行动计划（2018-2020 年）》	大力推动信息消费向纵深发展，壮大经济发展内生动力，在更高水平、更高层次、更深程度实现供需新平衡，优化经济结构，普惠社会民生。
2018 年 7 月	工信部	《推动企业上云实施指南（2018-2020 年）》	推动企业利用云计算加快数字化、网络化、智能化转型，推进互联网、大数据、人工智能与实体经济深度融合。

发布时间	发文单位	文件名称	内容概要
2018 年 6 月	工信部	《工业互联网发展行动计划（2018-2020 年）》	深入实施工业互联网创新发展战略，推动实体经济与数字经济深度融合。
2018 年 4 月	中央网信办、中国证监会	《关于推动资本市场服务网络强国建设的指导意见》	充分发挥资本市场在资源配置中的重要作用，规范和促进网信企业创新发展，推进网络强国、数字中国建设。
2017 年 12 月	工信部	《工业控制系统信息安全行动计划（2018-2020 年）》	建成全国在线监测网络，应急资源库，仿真测试、信息共享、信息通报平台（一网一库三平台），态势感知、安全防护、应急处置能力显著提升。
2017 年 11 月	国务院	《关于深化“互联网+先进制造业”发展工业互联网的指导意见》	以全面支撑制造强国和网络强国建设为目标，围绕推动互联网和实体经济深度融合，构建网络、平台、安全三大功能体系，持续提升我国工业互联网发展水平，深入推进“互联网+”。
2017 年 11 月	工信部	《公共互联网网络安全突发事件应急预案》	建立健全公共互联网网络安全突发事件应急组织体系和工作机制，提高网络安全突发事件综合应对能力，确保及时有效地控制、减轻和消除网络安全突发事件造成的社会危害和损失。
2017 年 9 月	工信部	《公共互联网网络安全威胁监测与处置办法》	积极应对严峻复杂的网络安全形势，进一步健全公共互联网网络安全威胁监测与处置机制，维护公民、法人和其他组织的合法权益。
2017 年 8 月	工信部	《工业控制系统信息安全防护能力评估工作管理办法》	规范工业控制系统信息安全防护能力评估工作，切实提升工控安全防护水平。
2017 年 6 月	工信部	《工业控制系统信息安全事件应急管理工作指南》	加强工控安全应急工作管理，建立健全工控安全应急工作机制，提高应对工控安全事件的组织协调和应急处置能力，预防和减少工控安全事件造成的损失和危害，保障工业生产正常运行。
2017 年 6 月	国家网信办、工信部、公安部、国家认证认可监督管理委员会	《网络关键设备和网络安全专用产品目录（第一批）》	列入《网络关键设备和网络安全专用产品目录》的设备和产品，应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供
2017 年 5 月	国家网信办	《网络产品和服务安全审查办法（试行）》	关系国家安全的网络和信息系统采购的重要网络产品和服务，应当经过网络安全审查。
2017 年 3 月	工信部	《云计算发展三年行动计划（2017-2019 年）》	支持软件和信息技术服务企业基于开发测试平台发展产品、服务和解决方案，加速向云计算转型。
2017 年 1 月	中央网信办	《国家网络安全事件应急预案》	建立健全国家网络安全事件应急工作机制，提高应对网络安全事件能力，预防和减少网络安全事件造成的损失和危害，保护公众利益，维护国家安全、公共安全和社会秩序。
2017 年 1 月	工信部	《信息通信网络与信息安全规划（2016-2020 年）》	紧扣“十三五”期间行业网络与信息安全工作面临的重大问题，对“十三五”期间行业网络与信息安全工作进行统一谋划、设计和部署。
2017 年 1 月	工信部	《软件和信息技术服务业发展规划（2016－2020 年）》	发展信息安全产业，支持面向“云管端”环境下的基础类、网络与边界安全类、终端与数字内容安全类、安全管理类等信息安全产品研发和产业化。创新云计算应用和服务。支持发展云计算产品、服务和解决方案，推动各行业领域信息系统向云平台迁移，促进基于云计算的业务模式和商业模式创新。

发布时间	发文单位	文件名称	内容概要
2017 年 1 月	工信部	《大数据产业发展规划（2016-2020 年）》	围绕实施国家大数据战略，以强化大数据产业创新发展能力为核心，以推动数据开放与共享、加强技术产品研发、深化应用创新为重点，以完善发展环境和提升安全保障能力为支撑，打造数据、技术、应用与安全协同发展的自主产业生态体系，全面提升我国大数据的资源掌控能力、技术支撑能力和价值挖掘能力，加快建设数据强国，有力支撑制造强国和网络强国建设。
2016 年 12 月	国家网信办	《国家网络空间安全战略》	贯彻落实推进全球互联网治理体系变革的“四项原则”和构建网络空间命运共同体的“五点主张”，阐明中国关于网络空间发展和安全的重大立场，指导中国网络安全工作，维护国家在网络空间的主权、安全、发展利益。
2016 年 12 月	国务院	《“十三五”国家信息化规划》	组织实施信息安全专项，建立关键信息基础设施安全防护平台，支持关键基础设施和重要信息系统，整体提升安全防御能力。提升云计算自主创新能力。培育发展一批具有国际竞争力的云计算骨干企业，发挥企业创新主体作用，增强云计算技术原始创新能力，尽快在云计算平台大规模资源管理与调度、运行监控与安全保障、大数据挖掘分析等关键技术和核心软硬件上取得突破。
2016 年 11 月	全国人大常委会	《中华人民共和国网络安全法》	为保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展制定。
2016 年 9 月	工信部	《互联网信息安全管理系统使用及运行维护管理办法（试行）》	规范做好互联网信息安全管理系统的使用与运行维护管理工作；保障各单位系统安全可靠运行，有效发挥系统作用。
2016 年 8 月	中央网信办、国家质量监督检验检疫总局、国家标准化管理委员会	《关于加强国家网络安全标准化工作的若干意见》	建立网络安全统筹协调、分工协作的工作机制；加强网络安全标准体系建设；提升标准质量和基础能力；强化网络安全标准宣传实施；加强国际网络安全标准化工作；抓好标准化人才队伍建设；做好资金保障。
2015 年 9 月	国务院	《促进大数据发展行动纲要》	培育高端智能、新兴繁荣的产业发展新生态。推动大数据与云计算、物联网、移动互联网等新一代信息技术融合发展，探索大数据与传统产业协同发展的新业态、新模式，促进传统产业转型升级和新兴产业发展，培育新的经济增长点。
2015 年 7 月	国务院	《国务院关于积极推进“互联网+”行动的指导意见》	推动互联网由消费领域向生产领域拓展，加速提升产业发展水平，增强各行业创新能力，构筑经济社会发展新优势和新动能。坚持改革创新和市场需求导向，突出企业的主体作用，大力拓展互联网与经济社会各领域融合的广度和深度。
2015 年 7 月	全国人大常委会	《中华人民共和国国家安全法》	确立了中央国家安全领导体制和总体国家安全观的指导地位，明确了维护国家安全的各项任务，建立了维护国家安全的各项制度，对当前和今后一个时期维护国家安全的主要任务和措施保障作出了综合性、全局性、基础性安排。
2015 年 1 月	国务院	《关于促进云计算创新发展培育信息产业新业态的意	完善发展环境，培育骨干企业，创新服务模式，扩展应用领域，强化技术支撑，保障信息安全，优化设施布局，促进云计算创新发展，培育信息

发布时间	发文单位	文件名称	内容概要
		见》	产业新业态。
2014 年 8 月	工信部	《关于加强电信和互联网行业网络安全工作的指导意见》	加大对基础电信企业的网络安全监督检查和考核力度，加强对互联网域名注册管理和服务机构以及增值电信企业的网络安全监管，推动建立电信和互联网行业网络安全认证体系。
2012 年 12 月	全国人大常委会	《关于加强网络信息保护的决定》	网络服务提供者应当加强对其用户发布的信息的管理，发现法律、法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，保存有关记录，并向有关主管部门报告。
2012 年 7 月	国务院	《关于大力推进信息化发展和切实保障信息安全的若干意见》	加快建设下一代信息基础设施，推动信息化和工业化深度融合，构建现代信息技术产业体系，全面提高经济社会信息化发展水平。健全信息安全保障体系，切实增强信息安全保障能力。
2011 年 1 月	国务院	《计算机信息网络国际联网安全保护管理办法（2011 年修订）》	对中国境内的计算机信息网络国际联网安全保护管理的相关问题做出了相关规定。
2011 年 1 月	国务院	《进一步鼓励软件产业和集成电路产业发展的若干政策》	继续实施软件增值税优惠政策。进一步落实和完善相关营业税优惠政策，对符合条件的软件企业和集成电路设计企业从事软件开发与测试、信息系统集成、咨询和运营维护、集成电路设计等业务，免征营业税，并简化相关程序。
2010 年 1 月	工信部	《通信网络安全防护管理办法》	加强对通信网络安全的管理，提高通信网络安全防护能力，保障通信网络安全畅通。
2009 年 4 月	工信部	《互联网网络安全信息通报实施办法》	规范通信行业互联网网络安全信息通报工作，促进网络安全信息共享，提高网络安全预警、防范和应急水平。
2007 年 6 月	公安部、国家保密局、国家密码局、国务院信息化工作办公室	《信息安全等级保护管理办法》	国家通过制定统一的信息安全等级保护管理规范和技术标准，组织公民、法人和其他组织对信息系统分等级实行安全保护，对等级保护工作的实施进行监督、管理。

（二）信息安全行业概况

1、信息安全行业发展概况

（1）全球信息安全行业发展概况

当前，世界各国信息化快速发展，信息技术的应用促进了全球资源的优化配置和发展模式的创新，互联网对政治、经济、社会和文化的影响更加深刻，信息化渗透到国民生活的各个领域，网络和信息系统已经成为关键基础设施乃至整个经济社会的神经中枢，围绕信息获取、利用和控制的国际竞争日趋激烈，保障信息安全成为各国重要议题。

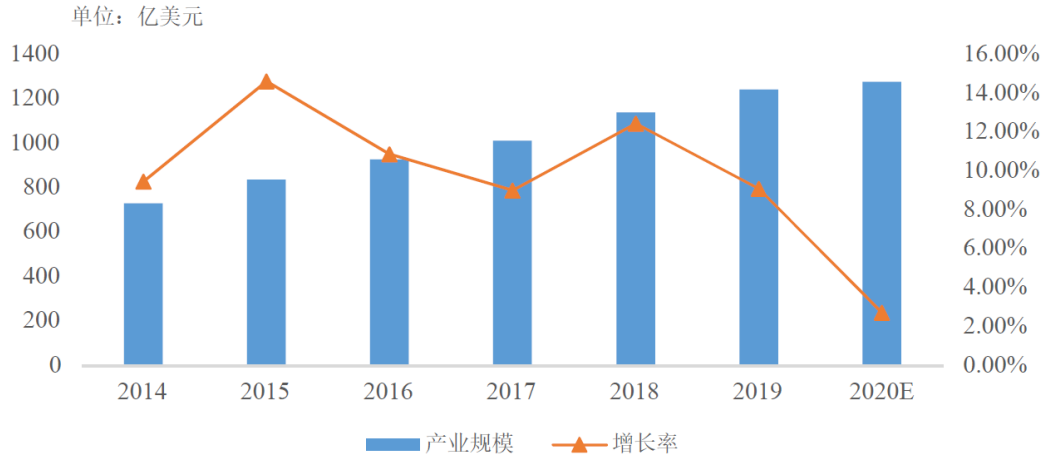
近年来，全球频现重大安全事件，仅 2019 年就曝光了万豪酒店 5 亿客户数据泄露、亚马逊云平台遭到黑客 DDos 攻击服务中断 8 小时、委内瑞拉遭遇网络

攻击全国停电 6 天等引起各界广泛关注的热点事件。网络攻击从最初的自发式、分散式的攻击转向专业化的有组织行为，呈现出攻击工具专业化、目的商业化、行为组织化的特点。随着获利成为网络攻击活动的核心，许多信息网络漏洞和攻击工具被不法分子和组织商品化，以此来牟取暴利，从而使信息安全威胁的范围加速扩散。个人信息及敏感信息泄露的信息安全事件，可能引发严重的网络诈骗、电信诈骗、财务勒索等犯罪案件，并最终导致严重的经济损失；而政府机构、工业控制系统、互联网服务器遭受攻击破坏、发生重大安全事件，将导致能源、交通、通信、金融等基础设施瘫痪，造成灾难性后果，严重危害国家经济安全和公共利益。全球整体网络安全形势不容乐观，国际间网络空间竞争形势日益紧张。

面对日益严峻的网络空间安全威胁，美国、德国、英国、法国等世界主要发达国家纷纷出台了国家网络安全战略，明确网络空间战略地位，并提出将采取包括外交、军事、经济等在内的多种手段保障网络空间安全。2011 年 4 月，美国发布了《网络空间可信身份国家战略》，首次将网络空间的身份管理上升到国家战略的高度，并着手构建网络身份生态系统。这一战略的出台表明美国已高度认识到网络身份安全在保障网络空间安全中的重要战略地位。从各国的战略规划的内容来看，一方面政府希望通过顶层安全战略的制定来引导本国安全产业的发展，另一方面对于网络空间的保护逐渐上升到和传统疆域保卫同等的地位上来，通过成立网络安全部队以加速军队信息安全攻防的研发，积极应对未来有可能发生的网络战争。

严峻的网络安全形势驱动安全市场的快速增长。根据中国信息通信研究院的数据，2019 年全球网络安全产业规模达到 1,244.01 亿美元，较 2018 年增长 9.11%。数字化企业的多个要素日益推动全球关注信息安全，尤其是云计算、移动计算和物联网等，而错综复杂、影响重大的高级针对性攻击同样起到了推动作用。

2014-2020 年全球网络安全产业规模及增速



数据来源：中国信息通信研究院

（2）我国信息安全行业发展概况

①信息安全成为我国国家战略的重要组成部分

我国一直高度重视信息安全产业的发展，早在 2003 年，中共中央办公厅、国务院办公厅转发了《国家信息化领导小组关于加强信息安全保障工作的意见》，党的十六届四中全会将信息安全上升到国家安全的战略层面，明确提出“确保国家的政治安全、经济安全、文化安全和信息安全”。面对日益复杂的全球信息安全形势和国内信息安全现状，2012 年，党的十八大报告中强调，要高度关注网络空间安全，并将网络空间安全、海洋安全、太空安全置于同一战略高度。2013 年，党的十八届三中全会也再次指出，“加大依法管理网络力度，加快完善互联网管理领导体制，确保国家网络和信息安全”。2014 年，中央网络安全和信息化领导小组成立，中共中央总书记、国家主席、中央军委主席习近平亲自担任组长，充分体现了国家对信息安全的重视程度。2015 年 7 月，全国人民代表大会常务委员会通过《中华人民共和国国家安全法》，并于 2015 年 7 月 1 日开始实施，首次将网络空间正式上升成为我国继陆、海、空、天后的第五疆域。2015 年 10 月，《中共中央关于制定国民经济和社会发展第十三个五年规划的建议》指出“实施网络强国战略，加快构建高速、移动、安全、泛在的新一代信息基础设施”。2016 年 4 月，习近平总书记主持召开网络安全和信息化工作座谈会并发表重要讲话，强调“加快构建关键信息基础设施安全保障体系”、“增强网络空间安全防御能力”。2016 年 11 月，全国人民代表大会常务委员会通过《中华

人民共和国网络安全法》，并于 2017 年 6 月 1 日开始实施，提出“国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序”，强调了金融、能源、交通、电子政务等行业在网络安全等级保护制度的建设。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》，是我国第一次向全世界系统、明确地宣示和阐述对于网络空间发展和安全的立场和主张。2017 年 1 月，工信部制定印发了《软件和信息技术服务业发展规划（2016-2020 年）》，对信息安全产品明确提出了到 2020 年收入达到 2,000 亿元，年均 20%以上增速的目标。2017 年 1 月，工信部制定印发了《信息通信网络与信息安全规划（2016-2020 年）》，紧扣“十三五”期间行业网络与信息安全工作面临的重大问题，对“十三五”期间行业网络与信息安全工作进行统一谋划、设计和部署。2017 年 7 月，国家互联网信息办公室起草《关键信息基础设施安全保护条例（征求意见稿）》，提出顶层设计、整体防护，统筹协调、分工负责的原则，充分发挥运营主体作用，社会各方积极参与，共同保护关键信息基础设施安全。2019 年 5 月，国家市场监督管理总局、国家标准化管理委员会召开新闻发布会，《信息安全技术网络安全等级保护基本要求》、《信息安全技术网络安全等级保护测评要求》、《信息安全技术网络安全等级保护安全设计技术要求》三大“网络安全等级保护 2.0 制度”核心国家标准正式发布，进一步推进了我国网络安全制度建设的进程，也再次推动我国网络安全成为政府和企业级用户信息化、数字化建设的刚需。信息安全产业作为信息安全技术、产品和服务提供者和实施者，承担着国家信息安全防御和保障的历史使命。发展壮大网络安全产业已经成为维护国家网络空间主权、安全和发展利益的战略选择。

②信息安全产品国产化替代趋势日益显著

近年来，国内信息安全厂商快速发展，依托本地布局的产品和研发团队，对用户需求理解更为透彻，对新需求的响应更为迅速，产品性价比更高，部分功能特性已超过国外厂商，但在高端产品市场的竞争力仍相对较弱。

“十三五”时期，我国将大力实施网络强国战略，要求网络与信息安全有足够的保障手段和能力，通过切实推进自主可控和国产化替代，政策化培养和市场化发展双向结合，信息安全市场国产化脚步逐步加快。拥有自主可控的标准、技

术、产品的信息安全厂商，将在对公业务，为政府、行业服务的大背景下，充分应用包括云计算、大数据等技术，把握产业发展机遇，不断扩大市场份额，实现对国外信息安全产品的规模性替代，在核心应用领域和国内产业转型升级的变革中发挥重要作用，在国家网络信息安全领域中担当核心角色。

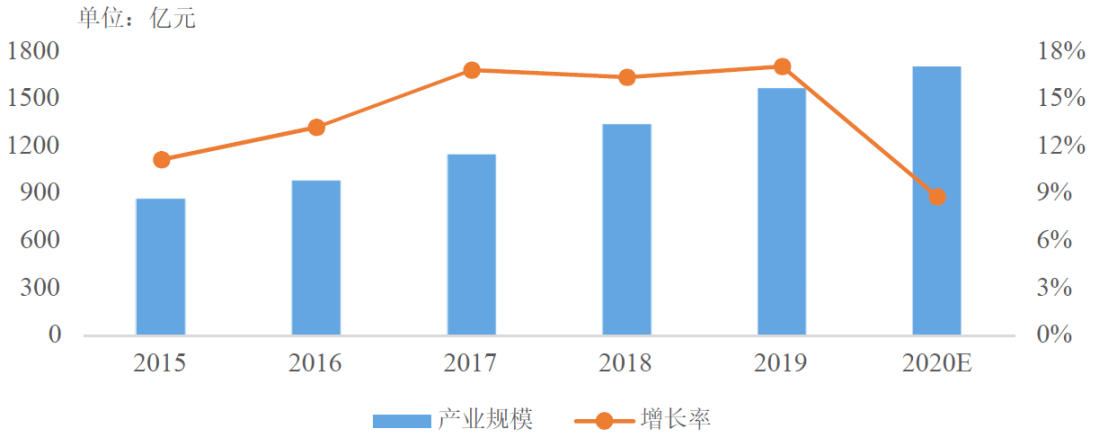
③我国网络安全事件多有发生

随着我国不断完善网络安全保障措施，网络安全防护和网络安全事件应急响应水平进一步提升，网络安全国际合作进一步加强。但随着互联网应用的深化、网络空间战略地位的日益提升，网络空间已经成为国家或地区安全博弈的新战场。国家互联网应急中心报告，2019 年，我国面临的安全问题日益复杂，敲诈勒索病毒盛行，分布式拒绝服务攻击事件峰值流量持续突破新高，联网智能设备面临的安全威胁加剧，工业控制系统安全风险在加大，网络攻击“武器库”泄露给网络空间安全造成严重的潜在安全威胁，APT 攻击组织依然活跃等问题，对我国实现建设成为网络强国目标不断提出新的挑战。日益复杂严峻的网络安全形势、国家网络强国战略推进建设迫切要求创新安全技术、增强综合安全保障能力。

④我国信息安全产业规模快速增长

根据中国信息通信研究院《中国网络安全产业白皮书（2020 年）》，2019 年我国网络安全产业规模达到 1,563.59 亿元，同比增长 17.1%，预计 2020 年产业规模约为 1,702 亿元，增速约为 8.85%。

2015-2020 年我国网络安全产业规模增长情况



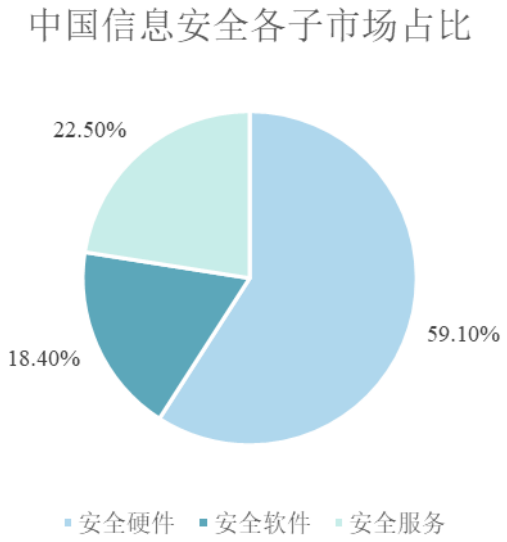
数据来源：中国信息通信研究院

根据 IDC《全球网络安全支出指南》预测，未来 3 年中国信息安全市场将继

续保持快速增长，2018-2022 年的预测年均复合增长率约为 25%，远超全球平均的 9%，预计 2022 年市场规模将增至 137.7 亿美元。

⑤国内信息安全市场以硬件产品为主

根据 IDC《全球网络安全支出指南》，2020 年在中国整体网络安全支出中安全硬件将继续占主导地位，占比高达 59.1%，安全软件和安全服务支出比例则分别为 18.4%和 22.5%。



数据来源：IDC

我国安全硬件前三大细分子市场依次为 UTM 防火墙（UTM Firewall）、统一威胁管理（Unified Threat Management）、安全内容管理（Security Content Management），三者总和占中国整体安全硬件市场比例超过 80%。其中统一威胁管理是中国市场增长最快的安全硬件市场，在 2019-2023 年的预测期间内，年均复合增长率将达到 25.6%。等保 2.0 等法律法规的合规性建设、5G 等新技术对于网络安全的需求将进一步推动硬件市场的发展。

与此同时，一方面，我国云计算、大数据、物联网等新系统的大量部署与应用使得客户逐渐认识到主动安全防御体系建设的重要性，安全可感、可视、可维护成为客户的具体需求，态势感知、威胁情报、云安全等产品的进一步发展也将成为软件市场高速增长的新动能。另一方面，我国网络安全专业人才数量缺失严重，企业亟需网络安全服务商提供专业的安全集成、安全运维、安全咨询、安全教育与培训等服务，从而帮助企业及时应对各种潜在的、突发的网络安全事件，保障企业业务的健康、稳定运行，因此“人机”共智、自动化响应与安全服务相

结合的网络安全解决方案也将成为未来网络安全的主要发展趋势。安全软件、安全服务市场前景十分广阔。

⑥信息安全投入有待提高

与美国、日本等发达国家相比，我国信息安全投入的绝对数量以及相对 IT 总投入的占比都明显偏小。国内安全投入占信息产业总规模较低的占比说明国内信息安全发展程度与发达国家相比尚存在差距。这与国内信息安全产业起步较晚，普遍重视程度不够有关系。而根据经验，随着发展阶段的变化，对于信息安全的投入会从产品为主逐渐过渡到服务为主。目前国内处在信息安全发展较为初级的阶段，国内信息安全产品偏高的占比也体现了这点。信息安全产业的快速发展将逐渐降低国内外信息安全领域投入的差距，国内逐渐增长的信息安全投入也将成为信息安全厂商发展的原动力。

2、行业发展的影响因素及趋势

（1）信息安全行业发展影响因素

我国信息安全行业近年来快速发展的主要驱动因素有以下几个方面：

①基础信息网络和重要信息系统设备国产自主水平关乎国家网络安全形势，信息安全设备自主可控和国产化替代是大势所趋。随着国家对信息安全愈加重视而上升到国家战略层面，国产化替代不可逆转，随着技术能力提升及政策推动，我国信息基础设备会沿着外围到核心、从党政军企特殊市场到消费者市场，国产替代率会逐渐提高。

②信息安全需求的提升是推动行业快速发展的根本因素。随着我国整体信息化水平持续提升，经济和社会对信息化的依赖程度日益提高，一旦数据泄露、遭到破坏或者丧失功能可能严重危害国家安全、公共利益，而随着身份盗用、交易诈骗、资源滥用、网络钓鱼等安全事件频繁发生，政府、企业、个人对信息安全的关注程度日益增强，社会对信息安全的需求与日俱增，政府部门、重点行业在信息安全产品和服务上的投入也不断增加，促进了信息安全行业的持续增长。

③国家政策支持是信息安全行业发展的重要因素。近年来，国家有关部门相继出台了一系列法律法规和鼓励行业发展的产业政策，为信息安全行业的发展营造了良好的政策环境。我国的信息安全工作提高到国家战略高度。信息安全形势

日益严峻，国家对信息安全产业的重视程度日益提高，政府及行业政策法规的推动，促使我国信息安全市场空间日益扩大。

④信息安全标准化工作的推进促进了信息安全行业的发展。近年来，我国相继制定了一系列信息安全国家标准，进一步规范了行业的发展，为信息安全产品的选用和研发提供了标准和依据，对信息安全行业的发展起到了积极的引导作用。

⑤信息技术不断发展革新。近年来，云计算、大数据、移动以及社交网络的快速发展给信息系统架构带来了巨大变化，信息安全也随之迎来挑战。例如云计算技术，使得数据中心的基础设施由原来的各业务系统独立建设模式转变为资源池建设模式，服务器、存储、网络设备的部署方式相应改变。基础架构的变化要求信息安全建设能够适应新的 IT 基础架构，从而满足新的安全需求，这同时为信息安全建设带来了新的发展空间。

（2）信息安全行业发展趋势

①安全威胁态势智能感知将成为一个重要方向

目前各种各样的安全产品被用于检测网络中的攻击威胁，维护网络的安全运行。但这些安全手段一般只能在一定范围内发挥特定的作用，互相之间缺乏有效的数据融合和协同管理机制。面对众多分散的信息，用户无法全面直观地了解系统安全脆弱点、整体攻击状况以及安全防护效果，无法满足预判系统安全脆弱点并提前实施防御措施的需求，另一方面，随着攻击手段的不断变化，目前部分高级攻击隐蔽性很强，通过单独的安全产品很难检测和防护，需要汇总用户网络中所有安全事件信息、威胁信息以及相关数据，结合知识库和网络情报库，快速准确地发现网络异常和高级威胁，同时通过通知用户或与网络中安全设备进行联动，实现针对高级威胁进行智能检测与防护的目的。

安全威胁态势感知平台可以有效解决以上问题，其融合了基于大数据的安全分析技术、威胁情报和可视化技术，可以更加系统地分析整体漏洞和风险，呈现整体安全状态，同时能够实现针对攻击风险的预判和预防，并且可以与传统网络安全产品一起联动配合，整体形成网络安全威胁“全局可视、提前预判、主动预警、立体防护”的全新安全解决方案，有效提升安全防护效果和客户体验，因此

将成为未来几年安全建设的重要方向。

②云安全和物联网安全市场将会成为下一个高速增长点

随着云计算的普及，大量数据和业务都集中在云计算数据中心中，云计算数据中心面临着巨大的安全风险，其对安全的需求达到了全新的高度，安全在云计算领域将成为与计算、存储、网络并列的四大基础设施之一，云计算的快速发展给网络安全行业带来了巨大的市场空间和商业价值。

另外近几年来，物联网发展也非常迅猛，物联网技术不仅仅在家庭及消费级设备上取得发展，还在制造业、物流、矿业、石油、公用设施和农业等拥有大型资产的行业也开始大量得到应用。但是物联网的安全性非常薄弱，各类物联网终端很容易成了被入侵和控制的对象，黑客通过入侵物联网设备，再逐步渗透到整个网络，窃取大量机密信息，甚至通过操控物联网设备对企业、国家产生直接攻击和威胁。近几年来物联网安全事故频发，物联网的安全问题正在被日益重视，后续几年物联网安全市场将会取得快速发展。

③应用交付市场将持续快速发展

随着各类互联网业务的高速发展，网络应用不断增多，各类网络应用的安全和质量管理也日益复杂，同时用户业务随着访问用户量、业务流量的逐渐增大，链路、服务器的负载均衡以及按需平滑扩容变得非常重要，并且由于服务器宕机、链路故障、应用程序故障时有发生，故障智能检测与自愈也迫在眉睫。用户急需一类能智能识别应用，让网络中各应用可视可控，同时能智能检测各类故障并平滑自愈，支持业务处理能力按需平滑扩容，确保各应用安全高效交付的智能产品和解决方案。

基于以上需求，信息安全行业衍生了一个新型的应用交付领域，目前该领域需求旺盛，存在较大的市场空间和商业价值，并且随着用户需求的日益强烈，在未来几年也将会持续快速发展。

④高端产品需求快速增长

随着各行各业信息化和各类互联网应用的蓬勃发展，尤其视频、游戏、移动互联网的快速发展，网络流量急剧增长，用户对网络安全产品的性能需求将会快速提高，市场对高端产品的需求将会快速增长。

⑤安全产品向多功能融合方向发展

业界现有的信息安全和应用交付类设备通常组网能力较弱，需要与网络设备一起配合部署，并且基本上每一种业务功能都是单一品类，例如防火墙、IPS 入侵防御设备、WEB 防火墙、DDoS 防护设备、流控审计设备等，导致用户网络中设备种类繁多，配置和维护工作都比较复杂。用户急需一类能融合所有功能、开启全部功能后仍然保持较高性能的产品，从而有效降低用户运维管理的复杂度。因此多功能融合的安全产品需求日益强烈，相关产品将会加速发展。

⑥网络安全由“注重防外”向“内外兼顾”转变

过去业界认为网络攻击通常来自于外网，而内网相对比较安全，因此网络安全产品通常部署在网络出口和重要区域边界，对内网攻击却疏于防护，但近些年由内网发起的攻击日益增多，例如各类蠕虫病毒一旦感染某台主机后，就会在局域网内部快速扩散攻击全网，从而给用户造成重大损失，另外从内网非法窃取数据资料的行为时有发生，尤其随着云计算多租户模式的快速发展，内网云租户之间的安全防护不可或缺，因此，内网安全防护变得日益重要。用户不仅需要重视外部安全，更要对内网安全做配套建设，对接入用户、网络应用、用户行为、网络异常流量进行严格管控，做到“内外兼顾、立体防护”，才能实现真正意义上的安全。

⑦整体解决方案能力将变得日益重要

目前安全产品可分为防火墙、IPS、DDoS 防护、Web 应用防火墙、上网行为管理与审计、漏洞扫描等产品，各类产品配置方法和监控日志形式各异，运维管理非常复杂，另外，随着网络安全的威胁来源和攻击手段不断变化，仅采购和部署几类安全产品无法完全保障网络长期、系统的安全，而对网络进行系统规划、构建全面的安全防护体系、制定完善的安全管理策略、落实日常专业的安全管理显得尤为重要。但是大量中小企业安全技术人员匮乏，并不具备这样的能力，另外随着信息安全环境日益复杂，即使是大型企业和机构也越来越难以独自应对，用户普遍期望安全厂商能够提供全面应对各类安全威胁的整体解决方案，从而降低用户安全管理复杂度。所以在未来的安全市场中，整体解决方案能力将变得日益重要。

（三）行业技术水平和特点

1、行业技术水平

目前全球范围内，信息安全产业发展水平较高的国家主要有美国、英国、法国、以色列等。从安全体系研究以及攻防技术研究等领域来看，我国信息安全产业在这些领域的技术水平与国际保持同步。其中在攻防对抗技术领域（包括漏洞挖掘和分析、拒绝服务攻击防护、异常行为发现与防御等方面），以及安全服务领域（包括信息安全风险评估、系统规划与安全加固、安全运维与应急响应等方面），国内厂商已经具备了较高水平，在部分领域已经形成了特有的专项技术。在产品研发方面，国内主流厂商已能够规模化开展攻防技术的体系化研究和产品化开发，相关产品已经具备较强竞争力。

但是，我国在硬件的研发及制造方面较美国等发达国家尚有较大差距，这些领域包括芯片制造、超大规模集成电路规模生产等。目前我国在计算机 CPU、交换芯片、专用芯片等硬件产品的制造方面，从功耗、性能、性价比等指标来看，尚不能做到完全替代国外产品。

2、行业技术特点

（1）软硬件技术协同发展

一方面，信息安全的防护需覆盖信息系统的各个方面，完善的防护体系是综合的解决方案，这就需要厂商对安全体系、知识库储备、威胁分析与建模等方面具备相应的技术积累，并跟踪行业的发展状况进行技术投入。

另一方面，安全产品的运行离不开支撑其运行的硬件环境。这需要信息安全领域的技术呈现一定的广度特点，能够针对市场需求在产品的硬件平台技术上投入精力发展，以使得产品能够满足在性能、可靠性方面的要求。

（2）行业技术门槛较高

对于行业内厂商而言，由于需要在软件及硬件领域有足够的积累。同时，由于 IT 行业技术发展迅速，所以具有较高的行业准入门槛。

软件方面具体体现在威胁对抗技术的积累上。信息安全领域的发展是随着威胁对抗技术的发展而不断成长，从最早基于特征的攻击检测和防御，到现今异常

行为模式以及信誉库机制，这些都需要针对新兴威胁持续保持跟踪，并形成安全相关的各类知识库，包括漏洞库、攻击手法库、Web 信誉库等，这些知识是厂商需要具备的基本技术积累。

硬件方面，主要体现在对网络协议的理解和对设备硬件架构、性能、可靠性的把握能力上。由于安全硬件设备必须部署在网络中才能发挥作用，随着云计算、物联网等新技术的迅猛发展，新的 IT 网络对安全设备的组网能力、性能、可靠性等指标有了新的要求，这就需要厂商必须具备相当的硬件方面的技术积累，才能使产品满足未来的部署需求。

（3）技术发展日新月异

随着信息化应用的极大丰富，安全威胁的种类和数量暴增。安全的攻与防技术就是典型的交替上升关系，各种威胁为了规避安全产品的封杀，也加快了攻击威胁的变化速度。例如，目前网站被感染了恶意代码之后的存活周期从以往的几天下降到几小时。这就要求安全厂商掌握的安全技术能够迅速发现和响应这些威胁，并在第一时间保证安全产品的知识库得到升级，才能确保对新型威胁的有效防护和阻断。

（四）行业竞争格局及市场化程度

1、信息安全业务市场竞争格局

在信息安全产品方面，得益于国内信息安全市场的快速增长，国内提供信息安全产品的企业数量众多，市场竞争激烈，信息安全产品市场总体的市场集中度相对较低。

在信息安全服务方面，安全咨询及运维服务行业总体上处于从初创期转向快速发展期的过渡阶段，当前市场的参与主体较多，模式尚不统一，竞争较为激烈。

目前信息安全行业内兼并整合较为活跃，具有技术、资质、品牌、人才和资金优势的厂商通过并购扩充产品业务线以提升整体解决方案能力。未来随着市场竞争进一步加剧，缺乏技术创新、服务能力和独特商业应用模式的企业将逐步被淘汰，竞争实力较弱的中小厂商数量将大幅减少，行业集中度将进一步提高。

2、应用交付业务市场竞争格局

目前国内应用交付市场中活跃的产品提供商可以划分为全球厂商和本土厂商两大类。全球厂商，以 F5 网络（美国）等企业为代表，由于起步较早，产品在成熟度、品牌和用户认知度方面具备一定优势。而以本公司、深信服为代表的本土厂商则在本地化能力、服务与支持优势、自主可控合规等方面形成独特竞争力。

（五）行业内主要企业情况

行业内主要竞争对手简要情况如下：

1、网络安全产品主要竞争对手

启明星辰：北京启明星辰信息技术股份有限公司，成立于 1996 年，2010 年在深交所中小板上市，证券代码：002439。启明星辰是网络安全产品、可信安全管理平台、安全服务与解决方案的综合提供商，产品覆盖防火墙/UTM、入侵检测管理、网络审计、终端管理、加密认证等技术领域，在政府、军队/军工、电信、金融、能源、交通、制造等行业的企业级用户中有一定市场占有率。

绿盟科技：北京神州绿盟信息安全科技股份有限公司，成立于 2000 年，2014 年在深交所创业板上市，证券代码：300369。绿盟科技是企业级网络安全解决方案供应商，向用户提供安全评估类、检测防御类、安全监管类等信息安全产品和专业安全服务，主要服务于政府、电信运营商、金融、能源、互联网等领域的企业级用户。

天融信：北京天融信科技有限公司，成立于 1995 年，是广东南洋电缆集团股份有限公司（证券代码：002212）的全资子公司。天融信业务覆盖政府、军队、金融、电信、教育、医疗、制造等行业，向客户提供安全防护、安全接入、安全检测、数据安全、云安全、大数据、安全服务、安全云服务和安全集成等 9 大类安全产品或安全业务，建立了以北京为中心覆盖全国三十多个省市的支撑服务平台。

任子行：任子行网络技术股份有限公司，成立于 2000 年，2012 年在深交所创业板上市，证券代码：300311。任子行是网络内容与行为审计和监管整体解决方案提供商，主要从事网络内容与行为审计和监管产品的研发、生产和销售，并

提供安全集成、安全审计相关服务，形成从计算机终端到网络在线分析等全面的网络内容与行为审计产品线，以及网络游戏软件的开发、销售、维护。主要产品为网络内容与行为审计系列产品、网络内容与行为监管系列产品、网络游戏软件。网络内容和行为审计监管产品覆盖国内外军工、教育、医疗、金融、企业、文化、能源、运营商等领域客户。

北信源：北京北信源软件股份有限公司，成立于 1996 年，2012 年在深交所创业板上市，证券代码：300352。北信源是国内信息安全领域的解决方案提供商，主营业务为信息安全软件产品的研发、生产、销售及提供技术服务，产品覆盖国产终端安全、虚拟终端安全、大数据应用、移动化管理、数据安全、边界安全等，用户涉及政府、军队军工、公安、金融、能源、通信、交通等重要行业。

深信服：深信服科技股份有限公司，成立于 2000 年，2018 年在深交所创业板上市，证券代码：300454。深信服是安全与云计算解决方案供应商，其产品线包括应用交付、上网行为管理、防火墙、VPN、企业移动管理、广域网优化、云安全、云计算等。深信服主要向金融机构、政府、运营商、教育机构、企业等提供产品或解决方案。深信服在网络安全产品及应用交付产品均与公司存在一定的竞争。

安恒信息：杭州安恒信息技术股份有限公司，成立于 2007 年，2019 年在上交所科创板上市，证券代码：688023。安恒信息的产品及服务涉及应用安全、云安全、大数据安全、物联网安全、智慧城市安全和工业互联网安全等领域，围绕事前、事中、事后几个维度已形成覆盖网络信息安全生命全周期的产品体系，包括网络信息安全基础产品、网络信息安全平台以及网络信息安全服务，各产品线在行业中均形成了较强的竞争力。

山石网科：山石网科通信技术股份有限公司，成立于 2011 年，2019 年在上交所科创板上市，证券代码：688030。山石网科专注于企业级网络安全产品的研发与创新，产品线涵盖边界安全、云安全、Web 安全、内网安全、数据安全、应用交付、态势感知等领域，构建了“安全产品+安全服务”模式，将产品与服务深度融合形成合力。

奇安信：奇安信科技集团股份有限公司，成立于 2014 年，2020 年在上交所

科创板上市，证券代码：688561。奇安信专注于网络空间安全市场，针对云计算、大数据、物联网、移动互联网、工业互联网和 5G 等新技术下产生的新业态、新业务和新场景，为政府与企业等机构客户提供全面、有效的网络安全解决方案。

思科：Cisco Systems, Inc.，成立于 1984 年，总部位于美国加利福尼亚州圣何塞，于 1994 年进驻中国。思科是全球领先的网络解决方案供应商，产品覆盖交换机、路由器、无线、安全、服务器、云和系统管理、统一通信、协作终端和电话等。

瞻博：Juniper Networks, Inc.，成立于 1996 年，总部位于美国加利福尼亚州桑尼维尔。瞻博是网络通讯设备公司，提供广泛的产品组合，涵盖了路由、交换、安全、应用加速、身份识别策略和控制以及管理等方面。

迈克菲：McAfee, LLC.，成立于 1987 年，总部位于美国加利福尼亚州圣克拉拉，于 1998 年进驻中国。迈克菲是全球领先的独立网络安全企业，产品和解决方案涵盖数据保护和加密、数据库安全、终端保护、网络安全、安全分析、安全管理、安全信息和事件管理、服务器安全、Web 安全、云数据据安全等。

2、应用交付产品主要竞争对手

F5 网络（美国）：F5 Networks, Inc.，成立于 1996 年，总部位于美国华盛顿州西雅图，于 2000 年进驻中国。F5 网络（美国）是全球应用交付领导者，主要提供文件存储虚拟化产品、SSL VPN、BIG-IP 企业管理器、VIPRION 威普龙应用交付控制器、WANJet 广域网加速器、Web 应用加速器等产品。

3、基础网络产品主要竞争对手

星网锐捷：福建星网锐捷通讯股份有限公司，成立于 1996 年，2010 年在深交所中小板上市，证券代码：002396。星网锐捷是国内领先的企业级网络、通讯、终端设备、视频应用产品及系统解决方案供应商，在网络通讯、交换机、云计算终端、瘦客户机、支付 POS、桌面云、无线接入、宽带接入、统一通信、视频信息应用、减灾防灾信息化等各产品领域均有一定的领先优势，同时也致力于在移动互联网、云计算、物联网、下一代网络、智慧园区、大数据等新兴应用领域为客户带来前瞻的应用解决方案。

东土科技：北京东土科技股份有限公司，成立于 2000 年，2012 年在深交所

创业板上市，证券代码：300353。东土科技致力于网络化工业控制整体解决方案的研究实践，主要研究、开发、生产和销售工业以太网交换机，并提供工业控制系统数据传输解决方案，产品广泛应用于智能电网、核电、风电、石油化工、轨道交通、城市智能交通和船舶等行业的国家重点工程和全球项目。

（六）行业特有的经营模式

我国信息安全行业特有的经营模式包括：

第一，信息安全行业的用户大部分属于运营商、政府、金融、电力能源、教育、医疗等领域。这些用户通常采用招投标的方式进行信息安全产品与服务的集中采购。

第二，作为知识密集型的新兴行业，信息安全行业与资本、劳动密集型的传统产业有显著的不同，知识和人才发挥着重要作用、技术资本和人力资本是行业内企业的核心竞争力。因此，信息安全行业的企业固定资产占总资产的比例普遍较小，具有“轻资产”的特征。

第三，我国信息安全行业在现阶段具有较为明显的季节性特征，主要因为上述用户通常实行预算管理制度和集中采购制度，在上半年审批当年的年度预算和固定资产投资计划，在年中或下半年安排设备招标采购，设备交货、安装、调试和验收则集中在下半年尤其是第四季度。因此，本行业存在明显的季节性销售特征。

第四，信息安全行业一般采用渠道销售为主，直签销售为辅的方式进行销售。由于行业资质、技术能力限制和产品服务支持的需要，各厂商一般会直接面对用户，为用户提供技术咨询、方案设计、产品实施、技术服务等过程内容。

四、主要业务模式、产品或服务的主要内容

（一）主营业务

公司主营业务为从事企业级网络通信产品的研发、生产、销售以及为用户提供相关专业服务，主要产品包括网络安全产品、应用交付产品及基础网络产品。公司提供基于创新的统一软件平台和高性能硬件平台下，以网络安全为核心，融合企业通信领域中网络安全、应用交付、基础网络各功能模块的整体解决方案。

公司主营业务产品均属于通讯设备领域，用于各系统间交换数据并保证数据安全可靠传输交换，其中基础网络产品是实现各类 IT 基础设备互联互通的基础，网络安全产品用于保护各类 IT 基础设备之间相互通信的安全性，应用交付产品主要用于提高各类 IT 基础设备之间相互通信的质量和可靠性。三类产品协同配合，可有效满足用户需要在各类 IT 基础设备之间实现安全、高速、可靠、有效的数据通信的需求。公司研发了一套集网络、安全、应用交付三大功能于一体的软硬件平台，融合了基础网络设备的各类功能特性，与应用层信息的安全与应用交付处理能力，可向用户提供整网解决方案。

公司产品主要部署在用户网络出口处、服务器前端或路由交换核心、网络汇聚或核心节点等场景。如部署在用户网络出口处时，公司产品主要会涉及防火墙、入侵防御系统、应用交付、上网行为管理及流控等，其中防火墙产品用于实现用户内网与外网的隔离，入侵防御系统产品用于防御系统漏洞攻击、病毒蠕虫入侵，应用交付产品可根据不同运营商实时的流量状况选择最佳通讯链路，上网行为管理及流控产品用于管理用户上网行为，保障网络安全。

（二）产品和服务的主要内容

公司以“让网络更简单、智能、安全”为愿景，专注于企业级网络通信领域，致力于为用户提供完备的产品和解决方案。通过持续的研发与创新，公司推出了全面覆盖企业级网络通信主要应用领域的共十余类上百款产品，形成了有较强竞争力的完备产品线。主要产品和服务如下表所示：

业务分类	具体产品和服务		简要说明
网络安全产品	安全防护产品	应用防火墙（FW）	实现网络边界安全防护，对进、出不同网络安全域的数据访问行为进行安全控制，确保网络访问的合法性。
		入侵防御系统（IPS）	深度检测与智能防御系统漏洞攻击、病毒蠕虫、DDoS 攻击、网页篡改、间谍软件、恶意攻击、流量异常等网络应用层威胁。
		Web 应用防火墙（WAF）	为 Web 应用提供保护，对来自 Web 客户端的各类请求进行检测和验证，对非法的请求和内容予以实时阻断，防护 SQL 注入、跨站脚本、网页挂马等常见 Web 攻击。
		异常流量清洗系统（Guard、Probe）	Probe 用于实时检测 DDoS 攻击，Guard 用于对 DDoS 攻击流量进行实时阻断，配合形成异常流量清洗系统，自动发现网络中的 DDoS 攻击并进行实时阻断。
		物联网应用安全控制系统（DAC）	对物联网、视频监控网等场景使用的白名单准入控制及应用控制，实现对物联网全网范围内前端 IP 设备和传输的流量进行精确管控，防范非法私接、设备仿冒、非法扫描、DDoS 攻击等。

业务分类	具体产品和服务		简要说明
		工控防火墙（IFW）	除具备包过滤、状态检测等功能外，同时支持对工业协议的精确识别，从指令、指令地址、取值范围等方面进行深度解析过滤，对工业控制系统进行专业的安全保护。
	安全分析产品	DPI 流量分析设备	对网络中的流量进行采集，同时针对流量中的业务应用以及报文内容进行深度识别与分析，与第三方应用系统配合，实现网络流量分析、网络优化及安全管控。
	安全审计产品	运维审计管理平台	提供账号管理、身份认证、单点登录、资源授权、访问控制和操作审计能力，对 IT 资产的运维操作过程进行有效的运维审计。
		日志审计分析平台	以大数据、机器学习技术为核心，快速全面的收集各类网络设备、安全设备、主机服务器、中间件、数据库以及业务系统的日志信息，实时进行安全事件的分析、溯源，协助用户进行安全分析及合规审计。
		数据库审计管理平台	提供完整的数据库审计分析、泄密轨迹分析、数据库攻击威胁分析等安全能力，有效帮助用户实现事件追根溯源，全面保护数据资产安全。
		运维一体机	集运维审计、日志审计、数据库审计、基线核查和漏洞扫描等丰富功能，帮助企业实现了安全统一管理、风险精准定位、运维高效便捷、等保合规建设。
	网络安全风险管控平台		以安全大数据分析技术为基础，通过主动探测机制，依托可视化技术实现网络安全风险的预警及信息通报，落实网络安全监管主体责任，实现网络安全管理闭环。
	网络安全威胁感知大数据平台		提供发现 APT 攻击、失陷主机、僵木蠕传播等安全威胁的能力，帮助客户进行威胁精准溯源及应急处置，实现安全事件可视化、全网威胁可视化、全网流量可视化、资产及脆弱性可视化。
	慧眼安全检测平台		及时发现网络设备、主机、应用等系统的漏洞隐患，快速摸排资产、精准定位风险隐患，及时响应通报并推动整改；可作为行业化关键信息基础设施的管理和监控平台，结合安全事件，帮助用户进行资产梳理，评估漏洞影响，快速处置，形成安全管理闭环。
应用交付产品	应用交付平台（ADX）		提高用户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。
	上网行为管理及流控（UAG）		对网络中的用户上网行为进行分析控制，保障网络资源合理使用，保证关键应用和关键用户的网络服务质量。
	高速缓存加速系统（DeepCache）		网络内容的自动缓存与访问加速，将高速缓存加速系统部署到局域网中，自动缓存用户频繁访问的网络内容，后续访问时通过局域网提供，提升用户访问速度、改进上网体验，有效节约出口带宽，降低带宽成本。
	统一管理中心（UMC）		对网络中各类安全设备、网络设备的统一管理，对网络日志事件信息的统一收集、过滤、归并和关联性分析，实现对整网用户上网行为、应用访问行为、流量应用组成、网络及应用质量、安全和攻击状态等全方位的监控，为用户直观呈现网络运行中各维度的实时状态和历史状态。
基础网络产品	深度业务路由交换网关（DPX）		公司各产品线通用的多业务核心平台，采用分布式高性能的框式架构，提供与业界主流核心交换机相匹敌

业务分类	具体产品和服务	简要说明
		的网络功能和大容量交换能力，可作为高端交换机使用，也可单独插入各类安全和应用交付业务板，作为高端安全产品和应用交付产品使用，也支持一起插入多类安全和应用交付业务板，作为融合网络、安全以及应用交付等各类业务功能于一体的高性能综合网关使用。
	盒式交换机（LSW）	针对企业级园区网、数据中心、工业网络等网络场景使用的网络接入交换机，在提供完善的传统网络特性和数据中心特性的同时，在网络接入边缘加强了对接入用户和接入流量的安全管控。
	WLAN 产品（AC、AP）	在公共场所、校园、酒店、写字楼等各类需要无线覆盖的场景提供 WIFI 无线网络的信号覆盖与控制，为用户提供无线上网功能。
	路由器产品（XR）	城域网、企业广域网、企业园区互联和数据中心网络出口等广域网络场景使用的互联互通设备。
服务类业务	安全服务	通过为用户提供安全技术服务，帮助用户完善信息系统安全防护能力，提升安全运维水平。服务内容包含安全风险评估、渗透测试、等保差距分析、安全技术体系规划、安全管理咨询、等保差距整改、安全巡检、安全加固、安全应急响应、安全通告、安全攻防演练等。
	维保服务	远程及现场技术支持、软件升级、备件先行更换、网络运行管理支持，帮助用户维护安全、高效、稳定的 IT 环境，提高网络生产力。

（三）主要业务模式

1、研发模式

公司产品研发以市场需求为导向，结合对相关领域技术发展趋势的研究和预测而开展。公司采用产品线管理团队的模式进行组织，产品线管理团队由市场产品部和研发产品部共同组成，市场产品部负责需求信息收集和产品定义，研发产品部负责需求细化和技术分析，共同讨论决策形成最终的产品规划，之后由研发产品部组织研发力量进行开发并最终交付。通过市场与研发的衔接，确保研发输出符合市场需求的高质量产品。

公司研发中心分为平台类部门和产品类部门。平台类部门主要负责关键技术的攻关和创新研究、基础平台以及各产品公共特性的开发与维护，为各产品部门提供软硬件基础平台和公共框架，主要包括硬件开发部、驱动开发部、软件开发部等；产品类部门主要负责与市场接口、进行产品规划、利用平台类部门提供的软硬件平台和公共框架进行产品个性化功能的开发，并对产品的开发过程进行整体控制，为产品的质量和竞争力负责，主要包括安全防护产品研发部、网络与应

用交付产品研发部、安全检测与服务产品研发部等。通过各产品最大限度的共用平台，提高产品开发效率，同时由平台部门对核心技术进行持续积累，确保技术的先进性。

公司产品研发管理流程主要分为概念计划、开发、验证以及交付四个阶段。通过周期性地跟踪项目计划的各项任务目标，如工作产品的规模、工作量、成本、进度、风险等，不断地了解项目的进展情况，当项目实际进展偏离项目计划时及时监控并采取纠正措施，从而实现对产品研发过程的监控与管理。主要流程如下图所示：

2、生产模式

公司产品生产严格遵循研发设计定型的硬件图纸与工艺说明，将各类电子元器件及其辅料组装，并将自主研发的软件灌装到硬件设备中，经过一系列生产流程控制，严格的质量检验，最终交付客户合格的产品。

公司主要产品的生产流程为物料分拣、PCBA、装配、测试、老化、老化后测试、包装等环节。其中 PCBA 环节为外协加工环节。PCBA 环节中生产设备、

工艺参数、生产与检验人员均经过公司严格认证，外协厂为配合公司业务采用了定人定线方式，保证了公司产品的质量与供应弹性。组装、测试、老化、包装等环节公司根据产品的销量也进行了部分产品的外协生产。

公司生产排产采用了预测加订单的混合模式，计划部门根据历史销售数据，销售人员预估，产品的生产周期等预计各个产品的销售量，采购与生产根据实际订单的波动进行动态库存的调整，有效的满足客户及时交付需求并实现总体库存控制。

公司大多数产品均采用上述自主研发设计，外协 PCBA 方式，少数非公司核心竞争力的产品采用了外购硬件设备自主开发软件的方式，外购硬件（服务器）属于充分竞争的成熟市场。

3、采购模式

公司采购通过战略性供应商选择、采购执行、供应商管理三大流程的运作，构建一个高效的采购运作系统，为公司获取及时与优质的产品及服务，同时对市场变化提供灵活的应变能力，保证具有竞争力的成本，达成采购竞争优势与全流程安全可控的采购运作。

公司采购依据行业或工艺（生产）相关性的特点，划分对应于不同行业的物料族，建立若干采购专家团队。采购专家团队作为供应商选择与认证的唯一责任中心，基于统一的流程与 IT 系统，制定采购策略，细分供应商，建立并逐步优化供应商资源，具体流程如下图所示：

依据完整的供应商认证体系产生合格供应商名录，公司所有原材料向已认证的合格供应商实施采购。公司采用 MRP 采购需求和高低库存采购需求相结合的

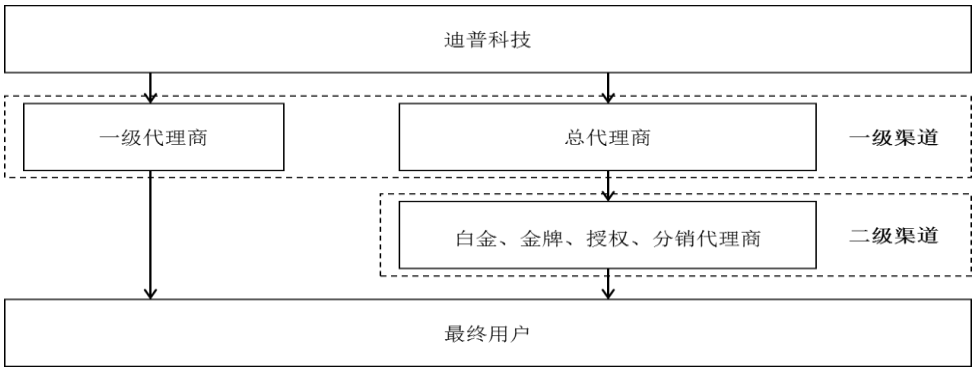
触发方式生成采购订单。对于大部分原材料，采用 MRP 实施采购，根据销售预测情况，汇总产品需求，运行 MRP 后，得到初步原材料申购清单，经市场、计划、采购等部门评审确认后，由采购部统一执行采购实施和到货。对于价值较低，需求持续的常用原材料，采用高低库存法实施采购，以规避原材料短缺造成的断货风险和多次分散采购导致的效率低下，并定期评审和回顾这些原材料的最低库存阈值和最高库存阈值，确保其合理性。采购部平日监控原材料的库存水平，根据库存实际数量和阈值，随时检查库存，当库存下降到最低库存阈值时，确定采购订单采购数量和到货时间，发出订单指令并跟踪到货。

4、销售模式

公司的产品销售采用渠道销售和直签销售相结合的方式，并以渠道销售为主。

（1）渠道销售

报告期内，公司销售渠道分为一级渠道代理商和二级渠道代理商。其中，一级渠道代理商可以直接向迪普科技进行采购，包括总代理商和一级代理商。公司的渠道体系如下图所示：



总代理商一般不参与终端用户的招投标，利用其物流、资金、集成商/代理商管理能力，负责物流运输、商务资金流，配合 IT 厂商提供支持服务，获得稳定的采销价差率。

一级代理商直接参与终端用户的招投标，一般为全国性的规模较大的系统集成商，具有范围较广的销售、服务渠道，具有较强的综合实力，直接面对最终用户，承担物流运输、商务资金流，负责用户及市场拓展销售、产品安装、售后服务等。

二级渠道代理商直接参与终端用户的招投标，具备一定特定行业、特定区域的客户资源、服务能力，直接向最终用户销售迪普科技产品，参与项目招投标，负责用户及市场拓展销售、产品安装、售后服务等。二级渠道代理商按其销售额、综合能力等指标，分为白金代理商、金牌代理商、授权代理商及分销代理商，白金、金牌、授权、分销代理商之间不存在隶属关系，均直接向总代理商采购公司产品。

公司代理商的分级、类别、认证原则、职责分工情况如下表所示：

代理商级别	代理商类别	认证原则	职责分工
一级渠道代理商	总代理商	工作性质：主要承接迪普物流和资金管理工作	总代理主要承接与迪普科技订单执行相关的物流和资金流管理工作，并配合迪普科技实施对各类别代理商的服务、支持和拓展工作
	一级代理商	①行业市场 ②年度目标任务金额	①一级代理商是有意愿和迪普科技合作，并通过迪普科技一级代理商标准认证的代理商 ②一级代理商应在特定或多个行业具有较强的行业背景、优势和资源，具有广泛影响力，业务覆盖国内多个省份，具备较强的迪普科技产品和解决方案营销及服务能力
二级渠道代理商		①行业及中小企业市场 ②年度及季度目标任务金额	①有意愿和迪普科技合作，并通过迪普科技代理商标准认证的代理商 ②应在区域/行业市场具有背景和资源，与迪普科技的合作紧密程度和配合度较高，具备迪普科技产品和解决方案营销及服务能力

报告期内，公司渠道销售按用户行业主要集中在政府、公共事业（电力能源、教育、医疗）、电信运营商、金融等行业，用户较为分散，行业覆盖广泛。

（2）直签销售

对于电信运营商等重点客户，公司一般采取直签销售的模式。该类重点客户业务需求量大，为降低采购成本，运营商主要采取集中采购模式，且运营商对售前售后技术服务要求高，公司安排专业的销售及业务人员可以更好地为其提供优质的服务。同时，产品能够入围电信运营商集中采购往往被业内作为供应商的实力认可的一项重要指标，公司参与运营商集中采购利于打造品牌。

（四）公司在行业中的竞争地位

1、公司产品和服务的市场地位

公司已经成为国内网络安全领域国家级重大技术专项的重要承担者之一。公司高性能高可靠的下一代应用防火墙、面向云计算的高性能入侵防御系统、面向云计算和大数据应用的高性能异常流量检测和清洗产品入选国家发展改革委国

家信息安全专项，基于下一代互联网的高性能入侵防御系统入选科技部国家重点新产品计划项目，自主可控核心交换机入选 2019 年度浙江省重点研发计划项目。

作为践行国家网络信息安全战略的重要先行者，公司是北京“APEC 峰会”、杭州“G20 峰会”、乌镇“世界互联网大会”、厦门“金砖国家峰会”、南宁“中国-东盟商务与投资峰会”、青岛“上海合作组织峰会”、上海“中国国际进口博览会”的网络安全保障和应急响应工作的技术支撑单位。

公司是信息安全产品的国产化替代的生力军。在信息安全产品国产化政策的背景下，国内企业在安全市场的份额逐渐增加，但国外品牌安全产品如 Cisco（思科）和 Juniper（瞻博）的防火墙产品、Cisco（思科）和 McAfee（迈克菲）的入侵防御产品，在国内的运营商、电力、金融等高端使用场景仍占据重要地位，公司相关产品在运营商、电力集中采购市场已实现连续多年入围，在金融行业亦取得突破，打破了国外厂商在高端使用场景的垄断地位。应用交付产品因技术复杂、研发难度高，过去市场一直由 F5 网络（美国）等国外企业主导，公司应用交付产品已规模化运用于三大运营商，市场排名稳居前列。

公司凭借先进的技术实力和完备的产品体系，通过持续不懈的市场及服务体系组织建设、客户及渠道拓展以及公司品牌建设，实现了市场的快速增长。公司最终用户覆盖了中央部委、省市级政府单位、三大运营商及广电网络运营商、各大电力能源、教育、医疗、金融机构，以及多家交通、水利、钢铁、汽车、制药、食品领域的大型企业。公司部分主要用户如下表所示：

行业	用户
运营商	中国移动、中国联通、中国电信、中国广电、歌华有线、华数传媒、长城宽带、鹏博士等
政府	国家信息中心、国家发展改革委、国务院国资委、公安部、财政部、商务部、环保部、海关总署、国家税务总局、国家工商总局、国家体育总局、国家广播电视总局、国家知识产权局、中国气象局、中国地震局、最高人民检察院、河南省信息中心、吉林省公安厅、辽宁省财政厅、山东省财政厅、浙江省税务局、湖南省税务局等
电力能源	国家电网、南方电网、华能集团、大唐集团、华电集团、国家电投、中广核、中国石油、中国石化、神华集团、阳煤集团等
教育	中国科学院、北京大学、清华大学、复旦大学、上海交通大学、浙江大学、哈尔滨工业大学、山东大学、北京交通大学、北京工业大学、北京工商大学、北京中医药大学、天津理工大学、西北工业大学、中南财经政法大学、南京邮电大学、湖南大学、吉林大学、贵州大学、新疆大学、云南大学、西北大学、武汉科技大学、国家超级计算广州中心等
医疗	解放军第 117 医院、上海市第一人民医院、上海市第六人民医院、辽宁省肿瘤医院、中国医科大学附属第一医院、重庆医科大学附属第一医院、浙江省人民

行业	用户
	医院、浙江大学附属第二医院、贵州省人民医院、新疆医科大学第五附属医院、新疆医科大学第一附属医院等
金融	中国人民银行、中国建设银行、中国银行、中国进出口银行、中国邮政储蓄银行、交通银行、恒丰银行、浦发银行、广发银行、北京银行、九江银行、郑州银行、齐商银行、赣州银行、平顶山银行、晋中银行、阜新银行、兰州银行、华融湘江银行、鞍山银行、吉林银行、江西银行、东北证券、国泰君安证券、方正证券、浙商保险等
其他	中国兵器集团、中国船舶重工集团、中国电子科技集团、中国交通建设集团、中粮集团、三峡集团、第一汽车集团、华晨汽车集团、宝武集团、太钢集团、哈药集团、国药集团、茅台集团、五粮液集团、长虹集团、大唐电信集团等

在运营商用户中，公司的防火墙、入侵防御、异常流量清洗、应用交付平台等产品多年入围三大运营商的集中采购名单，并且多次在多个标段中位列第一，公司产品已经规模应用于三大运营商包括城域网、无线互联网出口、数据中心等核心节点在内的全国网络中。

在政府用户中，公司是国家信息中心在电子政务安全领域的战略合作伙伴，也是全国首条量子通信光纤链路（京沪干线）等国家级重大项目的安全产品提供商。公司产品已经全面服务多个国家部委及金税工程、金关工程等“金”字工程，并在各省市电子政务工程中得到广泛应用。

在电力能源行业用户中，公司的防火墙和入侵防御产品均连续 5 年入围国家电网集采，应用交付产品也已成功入围，相关产品广泛应用于国家电网总部以及各省分公司；公司已经成为电力能源行业主要的网络安全和应用交付产品供应商之一。

在金融行业用户中，公司应用交付平台产品中标中国工商银行全行网络及网络安全设备项目（网络负载均衡设备项），并实现了在交通银行总行数据中心的突破；公司防火墙产品应用于中国银行北京数据中心、上海数据中心以及超过 20 个一级分行；从 2015 年开始，公司防火墙产品规模应用于恒丰银行多个数据中心及分行。

公司已经建立起了良好口碑和品牌，拥有以各大行业高端优质用户为主的用户群，并长期保持着深入稳定的合作关系，同时在各大行业均建立了数量众多的高端样板点，可以对各行各业更大范围的用户起到较好的辐射和示范效应。公司获得了中国高科技产业化研究会和品牌战略专家工作委员会联合颁发的“2015 中国计算机信息安全产品创新 质量创优 消费者放心品牌”。

2、公司的技术水平及特点

（1）公司的技术水平

公司拥有一支技术积累深厚、创新能力强的研发团队，其中核心技术团队在企业级网络通信领域拥有丰富的研发、管理经验，尤其是在高性能硬件架构、FPGA 系统设计、大型软件平台技术、信息安全和应用交付领域核心算法等方面在业界具有明显优势。2017 年，公司获得美国软件工程学会软件能力成熟度模型集成最高等级认证（CMMI 5 级），标志着公司在软件开发过程的改善能力、质量管理水平、软件开发的整体成熟度居于行业前列。通过持续的技术创新，形成了一系列具有自主知识产权的核心技术。截至 2020 年 9 月 11 日，公司拥有已获授权的境内专利 615 项（其中发明专利 523 项）、境外专利 6 项（其中发明专利 6 项）、已登记的软件著作权 51 项，并以这些核心技术为基础，推出了全面覆盖企业级网络通信主要应用领域的共十几大类上百款产品，形成了有较强竞争力的完备产品线。

此外，公司在安全研究和安全服务方面也具备业内领先的技术实力。在安全研究方面，公司拥有独立安全攻防实验室及一流的安全研究团队，团队核心成员具有 CISSP、ITIL、COBIT5、CISP、PMP 等信息安全人员资质认证，通过跟踪最新安全攻防技术，持续进行漏洞分析与挖掘、APT 攻击分析、攻击工具分析、黑客行为画像、僵尸网络分析等前沿安全技术研究，并将研究成果迅速转化为产品能力，持续提升公司安全产品的防护能力，确保公司在市场竞争中保持技术的领先性。在安全服务方面，公司具有信息安全服务资质认证（信息安全应急处理一级）、信息安全服务资质认证（信息安全风险评估一级）、信息安全服务资质（安全工程类二级）、中国通信企业协会通信网络安全服务能力评定（通信网络安全服务风险评估一级）、信息安全等级保护安全建设服务机构能力评估合格证书等安全服务资质，可以为用户提供安全评估、安全规划、安全运维、安全培训等完善覆盖 IT 系统全生命周期安全需求的专业安全服务。

公司研发中心被浙江省政府批准认定为浙江省级企业技术中心；公司被浙江省经济和信息化委员会评为 2017 年及 2018 年“浙江省电子信息 50 家成长性特色企业”；2017 年 8 月，公司“浙江省迪普网络信息安全研究院”被浙江省科学技术厅、浙江省发展和改革委员会和浙江省经济和信息化委员会认定为省级企

业研究院；2019 年 12 月，公司被国家知识产权局认定为“国家知识产权示范企业”；2020 年 1 月，公司被浙江省经信厅认定为“浙江省隐形冠军企业”；2020 年 3 月，公司被浙江省科技厅认定为“浙江省创新型领军企业培育企业”；2020 年 3 月，浙江省市场监督管理局发布 2019 年全省知识产权统计情况，公司位列 2019 年发明专利授权数全省企业第二位；2020 年 4 月，浙江省市场监督管理局发布浙江省创造力百强企业，公司位列全省第十。公司“转发与控制分离技术及应用”获 2016 年浙江省技术发明一等奖，“转发与控制分离网络件技术与产业化应用”获 2017 年教育部科学技术进步奖（推广类）二等奖，“一种用户态与内核态共享内存的管理方法和装置”获国家知识产权局“第二十届中国专利优秀奖”，“自安全白名单”物联网解决方案获得由中国电子信息产业发展研究院、中国计算机用户协会、《网络安全和信息化》杂志社联合颁发的“2016 年度中国信息技术创新样板工程奖（杭州交警视频专用网络安全建设示范工程）”，DPX17000 产品荣获由中国计算机用户协会网络应用分会颁发的 2016 年度“产品创新奖”。以上成果和荣誉，标志着公司研发实力得到了业界的广泛认可，整体技术水平处于业界领先水平。

（2）公司的技术特点

随着各行各业信息化和各类互联网应用的蓬勃发展，移动互联网、云计算、物联网等新型网络形态的快速兴起，信息交互的日益便捷，以及网络威胁来源和攻击手段的不断演变，网络安全行业迎来了全新的挑战。一方面，万物互联为黑客提供更多入侵目标及手段，渗透目标由传统终端设备、服务器扩展至移动终端、视频设备、智能穿戴设备、物联网、工控网络、交通工具等，信息入口庞杂，入侵手段隐蔽多样，攻击检测和防护手段需要进一步革新。另一方面，网络安全产品由于自身业务处理的复杂性，通常采用 CPU 作为业务处理单元，与采用 ASIC、NP 等专用硬件的网络设备相比性能不在同等量级，随着视频、游戏、移动互联网的快速发展，网络流量急剧增长，网络安全产品已成为制约网络性能的主要瓶颈。为了提升单台设备的处理性能，在安全产品设计时，通常会将每一类产品的功能设计得比较单一，在现网部署时需要网络产品和各类安全产品相互配合使用，随着攻击和防护手段的不断增多，对应的安全产品变得种类繁多，尤其是在流量较大的网络中，即使同一类安全产品也需要叠加多台设备来提升性能，网络

的部署和运维变得非常复杂。网络安全产品需要向着更高性能、更易部署的方向变革。此外，随着各类互联网业务的高速发展，网络应用不断增多，各类网络应用的安全和质量管理也日益复杂，用户急需一类能智能识别应用，让网络中各应用可视可控，确保各应用安全高效交付的智能产品和解决方案。基于对以上网络安全发展趋势及用户需求的深刻理解，公司的研发与创新一直紧紧围绕“让网络更简单、智能、安全”的主要目标展开，通过高性能硬件平台，融合网络、安全、应用交付功能于一体的软件平台，FPGA 系统设计、信息安全和应用交付领域相关核心技术等方面的一系列创新，形成了颇具特色的产品和解决方案，与业界同类产品相比具有比较明显的差异化竞争优势。

3、公司的竞争优势与劣势

（1）公司的竞争优势

①领先的技术

公司具有一支业界领先的研发队伍，并通过一系列有效的聘用、培训和激励机制保障团队稳定。截至 2020 年 6 月末，公司在北京和杭州设有研发中心，一共拥有研发员工 507 名，占公司员工总数的 40.82%，其中核心技术团队在企业级网络通信领域拥有丰富的研发、管理经验，尤其是在高性能硬件架构、FPGA 系统设计、大型软件平台技术、信息安全和应用交付领域核心算法、安全研究和安全服务相关技术等方面具有深厚积累。公司拥有专业的安全攻防实验室、一流的安全研究团队以及各类业界高等级的安全服务资质，相关研究成果能够迅速转化为产品能力，为持续提升公司安全产品的防护能力、确保公司在市场竞争中保持技术领先性提供了有力保障。

通过持续的技术创新，公司形成了一系列具有自主知识产权的核心技术。截至 2020 年 9 月 11 日，公司拥有已获授权的境内专利 615 项（其中发明专利 523 项）、境外专利 6 项（其中发明专利 6 项）、已登记的软件著作权 51 项，并以这些核心技术为基础，推出了全面覆盖企业级网络通信主要应用领域的共十几大类上百款产品，形成了有较强竞争力的完备产品线。

围绕“让网络更简单、智能、安全”的核心目标，公司在相关产品和解决方案上已经形成鲜明技术特点和领先技术优势，同时，通过完备的产品布局和系统

的安全服务能力，可以为用户提供完善的整网解决方案，真正实现“交钥匙”工程。目前公司相关产品和解决方案已经在众多行业获得广泛应用，较好地满足了用户需求，受到用户的广泛认可。

②客户与行业经验的积累

通过持续的市场拓展，目前公司产品及服务已经进入了包括运营商、政府、电力能源、金融、教育、医疗、交通等在内的众多行业，积累了大量客户，并长期保持着深入稳定的合作关系，这些客户自身具有雄厚的实力并在业界拥有良好的信誉，极大降低了公司的经营风险和财务风险。

公司通过在上述行业的长期耕耘与积累，与行业内的大量客户达成了紧密合作，积累信息化建设及信息安全建设项目的实施经验，完善产品功能，满足客户信息化业务的发展规划及建设思路，动态把握主要领域客户对于信息化建设的技术需求及发展趋势，可以进一步提高公司产品、解决方案及服务的竞争力。此外，公司已经在各大行业建立了数量众多的样板点，可以对更大范围的用户起到较好的辐射和示范效应，为公司实现持续快速发展、进一步扩大领先优势打下了坚实基础。

③业内知名的品牌

公司产品和服务的用户已经遍及全国各个省份以及众多行业，通过优质的产品质量、领先的解决方案以及专业的服务，公司在客户中树立了良好的企业形象，并且建立起了良好口碑和品牌。

公司获得了 Frost & Sullivan 颁发的“2016 中国区网络安全技术领导奖”、中国高科技产业化研究会和品牌战略专家工作委员会联合颁发的“2015 中国计算机信息安全产品创新•质量创优•消费者放心品牌”。除此之外，公司还是由中国信息安全测评中心认定的国家信息安全漏洞库技术支撑单位、国家互联网应急中心和中国互联网协会联合认定的中国互联网网络安全威胁治理联盟首批成员单位、以及中国网络安全产业联盟理事单位、中国保密协会会员单位和中国网络空间安全协会会员单位。在北京“APEC 峰会”、杭州“G20 峰会”、乌镇“世界互联网大会”、厦门“金砖国家峰会”、南宁“中国-东盟商务与投资峰会”、青岛“上海合作组织峰会”、上海“中国国际进口博览会”等重大国际会议和展

览活动期间，公司都是重要的网络安全保障单位。广大用户、行业同仁以及国家相关部门对公司的认可，体现出公司在信息安全行业的品牌已得到广泛认可。

④营销和服务体系

公司在营销体系方面的竞争力主要体现在建立了全国性的营销团队和技术支持中心，以及广泛的渠道体系两个方面。

公司在全国设有 27 个办事处，通过持续的市场拓展，公司已建立起覆盖全国的市场销售与技术支援体系，公司对行业价值客户的信息化建设和网络安全需求的理解和把握能力，使公司针对价值客户所提供的产品及服务赢得了广泛认同。公司拥有专业的安全服务与研究团队，能够自行挖掘安全漏洞，提供安全评估、安全应急等服务；具有本地化服务能力，能保证对用户突发事件的及时响应。

公司广泛发展渠道合作伙伴，现拥有 1,900 余家认证代理商，公司已经建立了覆盖一定细分行业市场的营销和服务渠道体系。目前，公司的办事处、售后服务机构与渠道合作伙伴之间形成了良好的互动，使得公司的产品和服务能得到快速推广。

（2）公司的竞争劣势

①公司规模仍然偏小，发展资金不足

公司目前仍处于业务快速发展期，但规模仍然较小，资金实力较弱，面对市场的快速增长，全国快速拓展的模式和手段单一。随着信息技术飞速发展，新产业、新模式不断出现，公司需要对前瞻性技术研究、产品升级换代、服务能力优化等关系公司核心竞争力的重点领域加大投入，以保持和提升公司在行业的领先地位。

②高端人才储备尚待进一步提升

信息安全行业作为知识密集型的高技术行业，高端人才的储备是企业竞争力的关键。目前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。公司当前在技术研发、产品规划、方案咨询等方面的高端人才储备尚待进一步提升，公司未来将通过加大培训投入、加强员工培养、引进高端人才，进一步加强公司高端人才储备。

五、现有业务发展安排及未来发展战略

（一）公司未来发展战略

公司以“让网络更简单、智能、安全”为愿景，坚持产品和技术的创新，采取“以科技创新赢得未来，以产品质量赢得市场”的发展方式，致力于成为一家具有优秀企业文化、可持续发展的企业级网络通信领域领军企业。

未来，公司除了保持已有的鲜明技术特点和领先技术优势之外，将抓住企业级网络通信市场的发展机遇，凭借公司在行业方面的核心技术优势、丰富的专家资源、多年沉积的专业化解决方案，依托公司自主研发的集网络、安全及应用交付功能于一体的软硬件平台，紧跟企业级网络通信领域的用户需求与发展趋势，加大研发力度，研发出能更好的满足用户需求、更具竞争力的产品和解决方案。同时公司将不断扩大产业链深度和广度、发挥规模化经营效应、加强品牌建设力度、拓展客户及营销渠道，大力提升公司核心竞争力，成为企业级网络通信领域的领导者。

（二）现有业务发展安排

1、专注主业持续技术创新

公司紧跟用户需求，专注于提供完善的企业级网络通信领域的产品及解决方案，通过持续的研发投入和技术创新服务于用户。公司基于自主研发的高性能软硬件平台而推出的高端网络、安全及应用交付产品，已广泛应用于运营商、政府、电力、金融、教育、医疗等行业，并建立起了良好口碑和品牌，拥有以各大行业高端优质用户为主的用户群体，可以对各行各业更大范围的用户起到较好的辐射和示范效应。公司将进一步保持在企业级网络通信领域的研发、管理经验，尤其是在高性能硬件架构、FPGA 系统设计、大型软件平台技术、信息安全和应用交付领域核心算法等方面的技术优势，不断巩固公司在高端网络、安全及应用交付市场的市场地位。

2、通过新技术应用构建闭环的网络安全产品体系

在“事前预警、事中防御、事后处置”的安全闭环的理论体系的指引下，随着新技术的不断推动，信息安全行业的不断发展，行业内各细分领域的协同将是行业新的发展趋势。为此，公司在保持安全防护领域的技术优势的同时，将加大

对安全检测、安全分析、及安全风险管控领域的投入。目前，公司已推出包括以安全大数据+AI 智能分析技术为核心，结合主被动检测、威胁情报等技术，实现安全可视化的网络安全威胁感知大数据平台产品；以安全大数据分析技术为基础，通过主动探测机制，依托可视化技术实现网络安全风险的预警及信息通报的网络安全风险管控平台产品；以公司多年渗透测试实战积累，集成大量的行业化安全漏洞库，提升用户安全风险事前检测能力的慧眼安全检测平台产品。公司将进一步加大这一领域的投入和市场推广力度，构建闭环的网络安全产品体系。

3、进一步聚焦价值行业的长期耕耘

公司凭借先进的技术实力和完备的产品体系，通过持续不懈的市场及服务体系组织建设、客户及渠道拓展以及公司品牌建设，实现了市场的快速增长。服务了政府、电信运营商、金融、能源、互联网等领域的企业级用户。公司已经建立起了良好口碑和品牌，拥有以各大行业高端优质用户为主的用户群，并长期保持着深入稳定的合作关系，同时在各大行业均建立了数量众多的高端样板点，可以对各行各业更大范围的用户起到较好的辐射和示范效应。未来，公司将进一步聚焦价值行业的长期耕耘，以不断开发贴近行业需求的解决方案为落脚点，持续服务价值行业，并以此为基础开拓各行各业市场。

4、优化人才结构，提升公司治理水平

人才是企业发展重要的战略性资源，公司坚持“创新、诚信、贡献&分享”的价值观，持续完善人才引进机制、优化人才激励措施、完善薪酬考核体系等，为员工提供广阔平台，拓宽员工成长空间，实现企业与员工共同成长。公司持续完善法人治理、优化组织结构、提高运营效率，不断增强公司的竞争力。

第二节 本次证券发行概要

一、本次发行的背景和目的

（一）本次发行的背景

1、信息安全产业已成为国家重点发展的产业之一，政策的大力支持为行业的发展创造了良好的政策环境和发展机遇

近年来，随着数字化技术及应用的快速发展，网络信息安全态势日趋严峻，我国政府对网络信息安全的重视程度不断提高，信息安全已上升为国家战略，政府在制度和法规层面强化了对信息安全的要求，大力支持网络信息安全产业的发展，为行业的发展创造了良好的政策环境和发展机遇。

2017 年 1 月，《信息通信网络与信息安全规划（2016-2020）》正式发布，该规划提出了建立健全网络与信息安全法律法规制度、构建新型网络与信息安全治理体系、全面提升网络与信息安全技术保障水平、加快构建网络基础设施安全保障体系、大力强化网络数据和用户信息保护、推动网络安全服务市场发展等 9 个方面的重点任务；2017 年 6 月，《中华人民共和国网络安全法》正式施行，该法明确了保障网络安全的基本要求和主要目标，提出了重点领域的网络安全政策、工作任务和措施，提出了对关键信息基础设施实施重点保护的要求；2019 年 9 月，工信部会同有关部门起草了《关于促进网络安全产业发展的指导意见（征求意见稿）》，该指导意见提出突破网络安全关键技术、积极创新网络安全服务模式、合力打造网络安全产业生态、大力推广网络安全技术应用、加快构建网络安全基础设施等主要任务；2019 年 12 月，《信息安全技术网络安全等级保护基本要求》、《信息安全技术网络安全等级保护测评要求》、《信息安全技术网络安全等级保护安全设计技术要求》等国家标准正式执行，网络安全等级保护进入 2.0 时代，在传统的基础信息网络基础上，针对移动互联、云计算、大数据、物联网和工业控制等新技术、新应用领域的安全保护提出了要求，极大扩展了网络安全保护的广度和深度。

网络安全投入与网络安全保障需求密切相关，电信、能源、金融、政府等关键信息基础设施领域，承载大量关系国计民生的信息系统和网络数据，是网络安

全工作的重中之重，也将是未来网络安全投入力度最大、创新安全技术容纳能力最强的领域，将对产业发展起到重要带动作用。随着国家信息安全战略规划以及相关政策的稳步推进落实，网络安全市场涌现爆发式增长需求，网络安全行业迎来巨大政策性红利和发展契机。

2、信息技术被广泛应用，数字化转型趋势日益明显，IT 基础设施市场快速发展，带动网络安全产业高速增长

一方面，我国经济当前正处在转变发展方式、优化经济结构、转换增长动力的攻关期，用更高效率提供更具高附加值的生产和服务是各行业努力的方向，信息技术是经济转型和产业升级中不可或缺的支柱和先导力量。信息技术已广泛应用于各个领域，并向更深层次应用渗透，各行各业都处于数字化转型浪潮中，包括网络安全产品在内的 IT 基础设施作为各行各业数字化转型的基础，取得了快速发展。

另一方面，随着 IT 基础设施的快速发展以及与社会各方面的深入融合，近年来网络安全问题频发并呈现愈加复杂的趋势。DDoS 攻击呈现高发频发态势，攻击组织性和目的性更加凸显；APT 攻击逐步向各重要行业领域渗透，在重大活动和敏感时期更加猖獗；事件型漏洞和高危零日漏洞数量上升，信息系统面临的漏洞威胁形势更加严峻；数据安全形势严峻，大规模数据泄露事件频发；“灰色”恶意应用程序大量出现，针对重要行业安全威胁更加明显；恶意注册、网络赌博、勒索病毒、挖矿病毒等依然活跃，高强度技术对抗更加激烈；工业控制系统产品安全问题依然突出，终端和智能设备的泛在互联逐渐瓦解传统安全边界，云计算、移动互联网、物联网、工业互联网等新产业的发展更是对网络安全提出了更高要求。

网络安全产品作为 IT 基础设施不可或缺的组成部分，在 IT 基础设施市场快速发展和网络安全严峻形势的驱动下，我国网络安全产业市场规模不断提升。根据中国信息通信研究院《中国网络安全产业白皮书（2020 年）》，2019 年我国网络安全产业规模达到 1,563.59 亿元，同比增长 17.1%，预计 2020 年产业规模约为 1,702 亿元，增速约为 8.85%。

3、公司专注于网络安全、应用交付、基础网络等 IT 基础设施领域，持续的研发和产业化投入有利于保持公司核心竞争力

自成立以来，公司专注于网络安全、应用交付、基础网络等 IT 基础设施领域，以“让网络更简单、智能、安全”为愿景，公司重视研发投入，始终以用户需求为指导，紧跟行业技术发展趋势，持续进行研发创新，不断进行产品及解决方案的优化迭代，孵化培育新产品和升级现有产品及服务。通过持续的研发与创新，公司推出了全面覆盖 IT 基础设施领域的共十余类上百款产品，形成了有较强竞争力的完备产品线。

随着移动互联网、云计算、大数据、物联网和工业互联网等技术的快速发展和逐步成熟，包括政府、运营商、电力能源、医疗教育等在内的行业用户也逐步意识到内部的 IT 架构和系统除了对业务形成支撑外，还可以大幅提升企业内外部的效率和企业核心竞争力，众多行业掀起了信息化建设和数字化转型的浪潮。基于此，公司始终坚持以行业用户的 IT 建设需求为中心，聚焦网络安全、应用交付、基础网络等 IT 基础设施相关领域的产品和解决方案等核心业务，向用户交付比过去更简单、更智能、更安全的产品和解决方案。

随着业务规模的不断扩大，公司将通过继续加大研发投入，吸引更多优秀人才，提升公司技术能力和应对趋势变化的能力，不断优化现有产品，研发满足用户需求的新产品，升级产品测试、验证及试制的能力，提升公司产品产业化转化的能力，从而不断提升公司产品及服务的市场竞争力，保持公司核心竞争力。

（二）本次发行的目的

1、以客户需求为导向，加大对新一代 IT 基础设施相关产品的研发投入，实现产品升级和完善，提升公司核心竞争力

在信息技术不断发展及国家政策大力支持的背景下，网络信息安全行业迎来了良好的政策环境和发展机遇，公司自成立以来便专注于网络安全、应用交付及基础网络等 IT 基础设施领域，通过十几年的发展，公司构建了一支业界领先的研发队伍，形成了一系列具有自主知识产权的核心技术，建立了良好的市场口碑、客户资源和营销服务体系，公司主营业务发展良好。IT 基础设施领域是技术密集型行业，核心技术研发能力是企业保持市场竞争力与行业地位的关键，因此只

有持续的研发投入，根据行业发展趋势和客户需求变化不断优化升级产品，推出新的产品及解决方案，才能够保持公司的核心竞争力。

本次募投项目“新一代 IT 基础设施平台研发项目”是公司在已有网络安全、应用交付及基础网络等 IT 基础设施领域的相关技术和产品的基础上，对下一代高性能软硬件平台、工业互联网安全相关产品、数据安全相关产品等在内的新一代 IT 基础设施平台及产品进行研发，从而实现对原有 IT 基础设施相关产品的升级，以顺应目前 IT 技术的发展趋势和市场需求，满足客户对新一代 IT 基础设施产品的需求。

本次募投项目实施后，将推动公司主营业务产品升级，进一步完善公司的产品结构，促进公司的研发成果产业化，并提升公司的核心竞争力。

2、建设智能测试、验证及试制基地，满足公司日益增长及提高的场地需求，提升运营管理效率

受行业政策环境、国产替代趋势以及公司在技术和市场方面的不断积累，公司经营状况持续向好，主营业务收入保持快速增长，最近三年公司主营业务规模持续扩大，实现营业收入分别为 61,696.30 万元、70,405.56 万元和 80,383.92 万元，年均复合增长率为 14.14%。随着公司经营规模的不断增长，公司对测试、验证、试制和仓储的场地需求也在不断增长。同时，随着近年来信息技术的不断发展，用户对网络安全、应用交付等 IT 基础设施的性能要求不断提高，对相关产品的测试和验证的要求也相应有所提高。目前公司主要通过租赁的方式实现上述测试、验证、试制和仓储的场地需求，而租赁场所从使用面积、管理效率、质量控制以及升级改造条件和成本等方面已无法满足公司日益增长的客观需求。

基于此，通过本次募投项目“智能测试、验证及试制基地建设项目”的建设，公司拟通过自建测试、验证及试制基地的方式，扩大测试、验证及试制的场地面积，升级改造测试、验证及试制的软硬件环境，实现测试、验证及试制的智能化，提高公司测试和验证的稳定性和可靠性，实现集中化管理，从而提高公司运营管理效率，提升公司响应用户需求的能力，促进公司的长期稳定发展。

3、提升公司资金实力，促进公司可持续发展

本次向特定对象发行股票募集资金到位后，将进一步提升公司的资金实力，

为公司的经营发展提供有力的资金支持，进一步满足公司核心业务增长与业务战略布局需要，促进公司可持续发展。此外，募集资金到账后，公司抵御全球经济扰动及意外风险的能力也将相应提升。

二、发行对象及与发行人的关系

本次向特定对象发行股票的发行对象不超过 35 名（含 35 名），为符合中国证监会规定条件的法人、自然人或其他合法投资组织；证券投资基金管理公司、证券公司、合格境外机构投资者、人民币合格境外机构投资者以其管理的二只以上产品认购的，视为一个发行对象；信托公司作为发行对象，只能以自有资金认购。

最终发行对象由公司股东大会授权董事会在本次发行申请经深圳证券交易所审核通过并经中国证监会同意注册后，按照中国证监会、深圳证券交易所的相关规定，根据竞价结果与保荐机构（主承销商）协商确定。所有投资者均以现金认购公司本次发行的股份。若国家法律、法规对此有新的规定，公司将按新的规定进行调整。

截至本募集说明书签署日，本次发行尚未确定具体发行对象，因而无法确定发行对象与公司的关系。具体发行对象与公司之间的关系将在本次发行结束后公告的发行情况报告书中予以披露。

三、本次发行方案概要

（一）发行股票的种类和面值

本次发行的股票种类为境内上市人民币普通股（A 股），每股面值为人民币 1.00 元。

（二）发行方式及发行时间

本次发行采取向特定对象发行股票的方式，公司将在获得中国证监会关于同意注册批复文件的有效期内选择适当时机实施。

（三）发行对象及认购方式

本次向特定对象发行股票的发行对象不超过 35 名（含 35 名），为符合中国证监会规定条件的法人、自然人或其他合法投资组织；证券投资基金管理公司、

证券公司、合格境外机构投资者、人民币合格境外机构投资者以其管理的二只以上产品认购的，视为一个发行对象；信托公司作为发行对象，只能以自有资金认购。

最终发行对象由公司股东大会授权董事会在本次发行申请经深圳证券交易所审核通过并经中国证监会同意注册后，按照中国证监会、深圳证券交易所的相关规定，根据竞价结果与保荐机构（主承销商）协商确定。所有投资者均以现金认购公司本次发行的股份。若国家法律、法规对此有新的规定，公司将按新的规定进行调整。

（四）定价原则及发行价格

本次发行采用竞价方式，本次发行的定价基准日为发行期首日。发行价格为不低于定价基准日前二十个交易日公司股票交易均价的 80%（定价基准日前二十个交易日股票交易均价=定价基准日前二十个交易日股票交易总额/定价基准日前二十个交易日股票交易总量）。

本次发行的最终发行价格将在公司本次发行申请经深圳证券交易所审核通过并经中国证监会同意注册后，由公司董事会与保荐机构（主承销商）按照相关法律、法规、规章和规范性文件的规定，以竞价方式确定。若国家法律、法规对此有新的规定，公司将按新的规定进行调整。

若公司股票在定价基准日至发行日期间发生派息、送股、资本公积转增股本等除权除息事项，本次发行底价将按以下办法作相应调整。调整公式为：

派发现金股利：P1=P0-D

送红股或转增股本：P1=P0/（1+N）

派发现金同时送红股或转增股本：P1=（P0-D）/（1+N）

其中：P0 为调整前发行底价，D 为每股派发现金股利，N 为每股送红股或转增股本数，P1 为调整后发行底价。

（五）发行数量

本次发行股票数量按照募集资金总额除以发行价格确定，同时本次发行股票数量不超过 40,000,000 股（含），未超过本次发行前公司总股本的 10%。最终发

行数量将在本次发行申请经深圳证券交易所审核通过并经中国证监会同意注册后，由公司董事会根据公司股东大会的授权及发行时的实际情况，与本次发行的保荐机构（主承销商）协商确定。若本次发行的股份总数因监管政策变化或根据发行审批文件的要求予以调整的，则本次发行的股票数量届时将相应调整。

在本次发行董事会决议公告日至发行日期间，若公司发生派息、送股、资本公积转增股本等除权除息事项，本次发行股票数量的上限将作相应调整。调整公式为：

Q1=Q0×（1+n）

其中：Q0 为调整前的本次发行股票数量的上限；n 为每股的送股、资本公积转增股本的比率（即每股股票经送股、转增后增加的股票数量）；Q1 为调整后的本次发行股票数量的上限。

（六）限售期

本次发行对象认购的股份自发行结束之日起六个月内不得转让。法律法规、规范性文件对限售期另有规定的，依其规定。

本次发行对象因由本次发行取得的公司股份在锁定期届满后减持还需遵守《公司法》、《证券法》、《深圳证券交易所创业板股票上市规则》等法律法规、规章、规范性文件、交易所相关规则以及公司《公司章程》的相关规定。本次发行结束后，由于公司送股、资本公积转增股本等原因增加的公司股份，亦应遵守上述限售期安排。

（七）募集资金数量及用途

本次发行拟募集资金总额不超过 101,500.00 万元（含），募集资金扣除发行费用后的净额用于下述项目：

单位：万元

序号	项目名称	项目总投资	拟投入募集资金
1	新一代IT基础设施平台研发项目	63,265.07	45,354.00
2	智能测试、验证及试制基地建设项目	67,269.25	56,146.00
合计		**130,534.32**	**101,500.00**

注：项目名称系以经政府有关部门正式备案的名称为准。

若实际募集资金不能满足上述募集资金用途需要，公司将根据实际募集资金

净额，按照轻重缓急的原则，调整并最终决定募集资金投入优先顺序及各项目具体投资额等使用安排，募集资金不足部分由公司自筹资金解决。

本次发行募集资金到位前，公司将根据市场情况及自身实际情况以自有或自筹资金择机先行投入募集资金投资项目。募集资金到位后，依照相关法律法规要求和程序置换先期投入。

（八）公司滚存利润分配的安排

本次发行完成后，公司在本次发行前滚存的截至本次发行完成时的未分配利润将由本次发行完成后的新老股东按发行后的持股比例共同享有。

（九）上市地点

本次发行的股票将申请在深圳证券交易所创业板上市交易。

（十）决议有效期

本次发行决议的有效期为自公司股东大会审议通过之日起 12 个月。

四、本次发行是否构成关联交易

截至本募集说明书签署日，公司本次发行尚未确定具体的发行对象，最终是否存在因关联方认购公司本次发行股票构成关联交易的情形，将在发行结束后公告的发行情况报告书中披露。

五、本次发行是否导致公司控制权发生变化

截至本募集说明书签署日，公司控股股东、实际控制人为郑树生，其直接持有公司 193,611,490 股股票，占公司总股本的 48.40%，并通过思道惟诚间接控制公司 31,535,715 股股票，占公司总股本的 7.88%，郑树生通过直接和间接方式合计控制公司 56.29%的股份，为公司实际控制人。此外，郑树生通过非控制的经略即远、格物致慧和闻涛岭潮间接持有公司的部分股份，截至本募集说明书签署日，郑树生直接和间接共持有公司 57.26%的股份。

按照本次发行的发行数量上限 4,000 万股测算，本次发行完成后，郑树生直接持有公司 44.00%的股份，通过直接和间接方式合计控制公司 51.17%的股份，仍为公司的控股股东、实际控制人。本次发行不会导致公司控制权发生变化。

六、本次发行是否导致股权分布不具备上市条件

按照本次发行的发行数量上限测算，本次发行完成后，公司社会公众股东合计持股比例将不低于公司总股本的 10%，满足《公司法》、《证券法》及《深圳证券交易所创业板股票上市规则》等法律法规规定的股票上市条件。本次发行不会导致公司的股权分布不具备上市条件。

七、本次发行已经取得批准的情况以及尚需呈报批准的程序

本次发行已经公司第二届董事会第三次会议及 2020 年第一次临时股东大会审议通过。根据有关法律法规规定，本次向特定对象发行股票尚需经深圳证券交易所审核通过并经中国证监会同意注册。

在经深圳证券交易所审核通过并经中国证监会同意注册后，公司将向深圳证券交易所和中国证券登记结算有限责任公司申请办理股票发行、登记和上市事宜，完成本次发行相关的全部呈报批准程序。

第三节 董事会关于本次募集资金使用的可行性分析

一、本次募集资金使用计划

本次发行拟募集资金总额不超过 101,500.00 万元（含），募集资金扣除发行费用后的净额用于下述项目：

单位：万元

序号	项目名称	项目总投资	拟投入募集资金
1	新一代IT基础设施平台研发项目	63,265.07	45,354.00
2	智能测试、验证及试制基地建设项目	67,269.25	56,146.00
合计		**130,534.32**	**101,500.00**

注：项目名称系以经政府有关部门正式备案的名称为准。

若实际募集资金不能满足上述募集资金用途需要，公司将根据实际募集资金净额，按照轻重缓急的原则，调整并最终决定募集资金投入优先顺序及各项目具体投资额等使用安排，募集资金不足部分由公司自筹资金解决。

截至本次发行董事会决议日，募集资金投资项目尚未投入资金。本次发行募集资金到位前，公司将根据市场情况及自身实际情况以自有或自筹资金择机先行投入募集资金投资项目。募集资金到位后，依照相关法律法规要求和程序置换先期投入。

二、本次募集资金投资项目实施的必要性和可行性

（一）项目实施的必要性

1、把握新型基础设施建设的发展契机，满足各行各业信息化建设中对新一代 IT 基础设备的需求

近年来，我国加速数字经济转型，持续密集部署新型基础设施，包括 5G 基建、特高压、城际高速铁路和城市轨道交通、新能源汽车充电桩、大数据中心、人工智能、工业互联网等领域的新型基础设施建设持续推进，同时对高性能、高并发、高新建、海量用户的场景提出了新的建设要求，包括物联网、工业互联网、大数据、5G、电网建设、人工智能等在内的应用领域对于网络安全设备等 IT 基础设施的需求规模巨大。

推进 IT 基础设施建设不仅仅是落实国家战略的重要行动，更逐步成为推动

当地经济发展的重要抓手之一，在此背景下，各地政府也不断出台政策并投入资金进行相关信息化建设，IT 基础设施产品在党政军和金融、电信、能源、电力、医疗、教育、交通、公共事业等各行业中的需求量持续增长。随着未来各生态体系在 IT 基础设施领域的产品、服务、运维、资金、资源等全方位的投入加大，将有效拉动 IT 基础设施需求和投资，这也就意味着新一代 IT 基础设施领域的网络、应用交付、安全防护、安全检测等方面的需求也会随着投资的增加而不断扩大。

随着新型基础设施建设的不断深入，各行各业信息化建设的不断增加，未来市场对新一代 IT 基础设施的需求将迎来显著增长。本次募投项目“新一代 IT 基础设施平台研发项目”将对新一代 IT 基础设施平台及产品进行研发，有利于公司把握新型基础设施建设的发展契机，满足客户对新一代 IT 基础设备的需求。

2、建设新一代高性能软硬件平台有利于满足 5G、云计算以及云原生应用的发展需要

目前，全球 5G 研发和产业化进程加速推进，我国 5G 正式进入商用部署期，5G 网络的快速投建为网络安全产品、服务和解决方案带来了巨大的市场空间，进一步带动网络安全产业结构升级和容量扩张。5G 应用具有低时延、高并发、高可靠等特性，网络中模糊的设备安全边界、开放的端口、集中的控制器和边缘部署节点等都在不断激发新的安全需求，对新一代 IT 基础设施的软硬件平台提出了更高的要求。

云计算作为信息技术发展和服务模式创新的集中体现，是推动互联网、大数据、人工智能与实体经济深度融合的基石。近年来，云计算技术和应用均得到快速发展，公司的“云安全、硬实力”持续为此类应用场景提供着优质的产品及落地解决方案，也得到了相关行业的认可。随着新的云原生应用场景的逐渐发展，也催生了一系列新的安全需求、新的应用交付使用场景。为了使得公司“云安全、硬实力”系列解决方案在这类场景中更有竞争力地为客户去解决实际的问题，开发新一代的软硬件平台的解决方案变得尤为重要。

本次募投项目“新一代 IT 基础设施平台研发项目”中对新一代高性能软硬件平台的建设，有利于公司满足 5G、云计算以及云原生应用的发展需要。

3、工业互联网安全问题凸显，我国工业互联网安全行业有望快速增长

随着工业互联网的快速发展和制造业企业的转型升级，越来越多的工厂和重要设施接入互联网，工业互联网在极大扩展网络空间的边界和功能的同时，也打破了工业控制系统传统的封闭和强调高可靠性的格局，使工业信息安全问题大量暴露出来。

一方面，自 2015 年以来，全球每年发生的大型工业网络安全事件更是进入高发阶段，每年数量都超过 300 起，攻击手段也在快速演变，网络渗透、PLC 程序病毒扩散、工控协议漏洞攻击等新型攻击手段层出不穷。另一方面，党的十九大以来，国家将发展先进制造业，建设制造强国和网络强国上升到国家战略。为保障“两个强国”战略顺利实施，加强工业信息安全建设、完善工业信息安全保障体系，党中央、国务院陆续出台了一系列政策，为我国工业信息安全发展提供了良好产业环境。

根据中国信息通信研究数据，2019 年我国工业互联网产业经济总体规模为 2.13 万亿，同比实际增长 47.3%，预计 2020 年将达到 3.1 万亿元，同比实际增长约为 47.9%，工业互联网产业高速发展持续带动安全细分领域增长。此外，根据工信部数据，2019 年，我国工业互联网安全产业存量规模为 27.2 亿元，2017-2019 年复合年均增长率达 42.3%，在工业互联网核心产业中占比仅为 0.5%。

在市场需求不断增长和一系列政策推动持续落地的背景下，随着企业安全意识逐步加强，工业互联网安全市场有望快速增长。公司需要加强技术研发和产业布局，解决工业互联网场景下的安全问题。

本次募投项目“新一代 IT 基础设施平台研发项目”中对工业互联网安全相关产品的研究，有利于公司加强对工业互联网安全技术的布局，解决工业互联网场景下的安全问题，有利于公司满足日益增长的工业互联网安全需求。

4、各类数据迅猛增长，数据已成为重要资产，保护数据安全已是政府、企事业单位乃至个人刻不容缓的基本需求

随着信息技术和人类生活的交融，以及云计算、大数据等新兴技术突飞猛进的发展，各类数据迅猛增长，数据逐渐成为企事业乃至政府最重要的资产之一，2015 年 9 月国务院印发的《促进大数据发展行动纲要》指出“数据已成为国家

基础性战略资源”。数据应用场景和参与主体日益多样化，促使数据安全的外延不断扩展。对个人而言，大数据收集处理技术和开放共享的要求，弱化了用户对个人信息的自决权力，多源数据汇聚降低了用户隐私被恶意滥用的门槛，数据安全治理成为加强个人数据保护的基本要求。对企业而言，大数据是重要的商业资源和生产要素，数据安全治理能力已成为企业的重要竞争力。

经济全球化推动世界各国经济贸易与技术交流不断扩大，大量数据日益频繁地在全球范围跨境流动。跨境数据流动引发的安全风险不仅影响商业利益获取，也影响国家安全和国家竞争力。加强数据安全治理已经成为维护国家安全的战略需要。我国政府高度重视数据在新常态中推动国家现代化建设的基础性、战略性作用，数据安全已成为贯彻国家发展战略的现实要求。2017 年《中华人民共和国网络安全法》正式实施，对数据提出了“安全可控”的核心要求，并强制要求等级保护工作；2019 年网络安全等级保护制度 2.0 标准颁布实施，数据安全建设成为建设的核心内容之一，对数据访问的审计、访问控制、加密、脱敏和溯源都有了明确的要求；2020 年《中华人民共和国数据安全法（草案）》面向社会公开征求意见，明确提出保障数据安全，促进数据开发利用，保护公民、组织的合法权益，维护国家主权、安全和发展利益等核心要求，标志着我国将数据治理的政策要求，通过法律文本的形式予以明确和强化。

本次募投项目“新一代 IT 基础设施平台研发项目”中对数据安全相关产品的研究，将有利于公司把握数据安全市场的发展机会。

5、信息安全行业是技术密集型行业，核心技术研发能力是信息安全企业保持核心竞争力、维持行业地位以及获得长足发展的关键

新技术新业态不断涌现，伴生新的安全风险和挑战。伴随新一代信息通信技术在更广范围、更深层次、更高水平与实体经济融合，网络安全风险和挑战也不断渗透、扩散、放大，亟需在工业互联网、区块链、5G、IPv6、物联网、大数据等领域加大安全研究力度，提早谋划，预先布局，有效防范不断变化的安全风险。新兴技术与网络安全融合创新，驱动安全防御能力不断演进升级；而新兴技术的恶意利用和滥用，也倒逼安全防护能力提升。面对更为严峻的攻防对抗形势，安全防护理念、思路和技术实现路径也需动态调整、适配，以提高安全决策智能性、协同性和运营效率，搭建更加敏捷和开放的防护架构、实现更加广泛的防护体系

协同。持续提升自身技术研发能力已成为信息安全企业竞争的关键点。

本次募投项目“新一代 IT 基础设施平台研发项目”的实施，公司通过对下一代高性能软硬件平台、工业互联网安全相关产品、数据安全相关产品等新一代 IT 基础设施平台及产品进行研发，将实现对公司主营业务产品的技术升级，有利于加强公司的核心技术研发能力，保持公司的核心竞争力。

6、有利于满足公司不断提高的测试、验证、试制和仓储的场所需求，促进公司核心技术产业化落地

公司是在企业级网络通信领域集研发、生产、销售于一体的高科技企业，提供基于创新的统一软件平台和高性能硬件平台下，以网络安全为核心，融合企业通信领域中网络安全、应用交付、基础网络各功能模块的整体解决方案。在公司规模不断扩大、产品类型日益增多以及信息安全行业保持持续快速发展的背景下，一方面，公司目前用于测试、验证、试制和仓储的租赁场地已逐渐无法继续满足业务扩展的需要，租赁地理位置较为分散给公司业务带来了诸多不便，货物长途运输周转增加了产品损坏的风险；另一方面，公司主营业务产品主要应用于运营商等对产品性能要求较高的企事业单位的信息化基础设施建设，随着信息技术的持续发展，客户对产品性能要求也在不断提高，对公司测试及验证的软硬件环境提出了更高要求，公司亟需对各项测试、验证的环节进行升级和改造，但升级改造对场地的软硬件要求较高，且资金投入成本较大，从经济和技术角度，租赁场地均难以满足升级改造需要。

基于上述情况，公司拟通过本次募投项目“智能测试、验证及试制基地建设项目”的建设，新建智能测试、验证、试制和仓储基地，以升级公司测试、验证、试制和仓储的软硬件环境，实现测试、验证、试制及仓储的智能化和集中化管理，提升公司测试、验证及试制的稳定性和可靠性，满足公司现有业务及未来业务发展带来的经营场地需求，优化公司核心技术产业化布局，满足公司长期发展的战略需求。

（二）项目实施的可行性

1、信息安全产业发展政策环境持续优化，市场空间广阔

信息安全产业作为信息安全技术、产品和服务提供者和实施者，承担着国家

信息安全防御和保障的历史使命，发展壮大网络安全产业已经成为维护国家网络空间主权、安全和发展利益的战略选择。

网络安全相关立法计划稳步推进。2017 年 6 月，《中华人民共和国网络安全法》施行，为我国有效应对网络安全威胁和风险、全方位保障网络安全提供了法律依据；2018 年 6 月，《网络安全等级保护条例（征求意见稿）》发布，深入推进实施国家网络安全等级保护制度；2020 年 1 月，《中华人民共和国密码法》施行，旨在规范密码应用和管理，促进密码事业发展，保障网络与信息安全；2020 年 6 月，由中央网信办、工信部、公安部负责起草的《关键信息基础设施安全保护条例》列入国务院 2020 年立法计划；2020 年 7 月，《中华人民共和国数据安全法（草案）》全文在中国人大网公开征求意见，立法直面数据这一非传统领域的国家安全风险与挑战，勾勒数据安全保护管理各项基本制度，强化国家数据安全保障能力。

工业互联网、车联网、电力等重要行业领域网络安全顶层设计密集出台。2018 年 9 月，国家能源局发布《关于加强电力行业网络安全工作的指导意见》，提出加强全方位网络安全管理、强化关键信息基础设施安全保护、提高网络安全态势感知、预警及应急处置能力等电力行业网络安全工作重点。2018 年 12 月，工信部印发《车联网（智能网联汽车）产业发展行动计划》，将“强化管理、保障安全”作为基本要求，提出了“产业安全管理体系初步形成，安全管理制度与安全防护机制落地实施，安全技术及产品研发取得阶段性成果，安全技术支撑手段建设初见成效，安全保障和服务能力逐步完善”的阶段性发展目标。2019 年 9 月，工信部会同九部门联合印发《加强工业互联网安全工作的指导意见》，要求“加快构建工业互联网安全保障体系，形成覆盖工业互联网全生命周期的事前防范、事中监测和事后应急能力”。

金融科技、区块链、IPv6 等新兴技术领域安全发展目标和要求更为明确。2019 年 1 月，国家互联网信息办公室发布《区块链信息服务管理规定》，明确区块链信息服务提供者的信息安全管理责任，规范和促进区块链技术及相关服务健康发展，规避区块链信息服务安全风险，为区块链信息服务的提供、使用、管理等提供有效的法律依据。2019 年 4 月，工信部印发《关于开展 2019 年 IPv6 网络就绪专项行动的通知》，提出“完善网络安全管理制度体系，同步升级防火

墙/WAF、IDS/IPS、4A 系统等 IPv6 网络安全防护手段”等一系列增加网络安全保障的措施。2019 年 8 月，中国人民银行印发《金融科技（FinTech）发展规划（2019-2021 年）》，围绕大数据、云计算、人工智能等新兴技术在金融领域安全应用以及金融网络安全风险管控等提出细化措施。

随着信息安全行业政策红利持续释放，产业发展顶层设计加强，产业发展重点和方向更为明确，网络信息安全需求持续增强，持续激活产业动能，助力拓展市场空间，信息安全行业市场空间广阔。

2、公司重视研发投入，坚持技术创新，具备扎实的人才储备及技术积累

信息安全行业属于知识密集型行业，技术、知识的更新换代迅速，自成立以来，公司在网络安全产品、应用交付产品及基础网络产品等 IT 基础设施领域持续进行研发投入，坚持技术创新，建立了扎实的人才储备和技术积累。

在人才储备方面，公司具有一支业界领先的研发队伍，并通过一系列有效的聘用、培训和激励机制保障团队稳定。截至 2020 年 6 月末，公司在北京和杭州设有研发中心，一共拥有研发员工 507 名，占公司员工总数的 40.82%，其中核心技术团队在 IT 基础设施领域拥有丰富的研发、管理经验，尤其是在高性能硬件架构、FPGA 系统设计、大型软件平台技术、信息安全和应用交付领域核心算法、安全研究和安全服务相关技术等方面具有深厚积累。公司拥有专业的安全攻防实验室、一流的安全研究团队以及各类业界高等级的安全服务资质，相关研究成果能够迅速转化为产品能力，为持续提升公司安全产品的防护能力、确保公司在市场竞争中保持技术领先性提供了有力保障。

在技术积累方面，自成立以来，公司以“让网络更简单、智能、安全”为愿景，持续进行研发创新，并自主开发了基于多核 CPU、FPGA 芯片以及分布式转发技术的高性能硬件平台“APP-X”，全面融合网络、安全、应用交付功能的 L2~7 融合操作系统“ConPlat”，将应用特征库、攻击特征库以及病毒库三库合一的应用识别与威胁特征库“APP-ID”。在此基础上，依托于安全研究团队十多年以来在攻防研究、漏洞挖掘、威胁情报分析、安全事件响应等技术积累，公司开发了具有自主知识产权的安全大数据处理引擎与 AI 智能分析引擎，结合主/被动安全检测、威胁情报、攻击建模等先进技术。公司形成了一系列具有自主知

识产权的核心技术，截至 2020 年 9 月 11 日，公司拥有已获授权的境内专利 615 项（其中发明专利 523 项）、境外专利 6 项（其中发明专利 6 项）、已登记的软件著作权 51 项，在技术成果转化成为实际生产力方面有足够的储备和能力，公司以这些核心技术为基础，推出了涉及网络安全、应用交付、基础网络等 IT 基础设施主要应用领域的共十几大类上百款产品，形成了有较强竞争力的完备产品线。围绕“让网络更简单、智能、安全”的核心目标，公司在相关产品和解决方案上已经形成鲜明技术特点和领先技术优势，同时，通过完备的产品布局和系统的安全服务能力，可以为用户提供完善的整网解决方案，真正实现“交钥匙”工程。

公司在网络安全产品、应用交付产品及基础网络产品等 IT 基础设备领域的人才储备和技术积累将有助于本次发行募集资金投资项目有效实施。

3、公司深耕信息安全行业，具备良好的客户资源、品牌口碑和营销服务体系

自成立以来，基于对网络信息安全发展趋势及用户需求的深刻理解，公司以“让网络更简单、智能、安全”为愿景，一直专注于企业级网络通信产品的研发、生产、销售以及为用户提供相关专业服务，形成了良好的客户资源、品牌口碑和营销服务体系。

在客户资源方面，通过持续的市场拓展，目前公司产品及服务已经进入了包括运营商、政府、电力能源、金融、教育、医疗、交通等在内的众多行业，积累了大量客户，并长期保持着深入稳定的合作关系，这些客户自身具有雄厚的实力并在业界拥有良好的信誉，极大降低了公司的经营风险和财务风险。公司通过在上述行业的长期耕耘与积累，与行业内的大量客户达成了紧密合作，积累信息化建设及信息安全建设项目的实施经验，完善产品功能，满足客户信息化业务的发展规划及建设思路，动态把握主要领域客户对于信息化建设的技术需求及发展趋势，可以进一步提高公司产品、解决方案及服务的竞争力。此外，公司已经在各大行业建立了数量众多的样板点，可以对更大范围的用户起到较好的辐射和示范效应，为公司实现持续快速发展、进一步扩大领先优势打下了坚实基础。

在品牌口碑方面，公司产品和服务的用户已经遍及全国各个省份以及众多行

业，通过优质的产品质量、领先的解决方案以及专业的服务，公司在客户中树立了良好的企业形象，并且建立起了良好口碑和品牌。作为国内信息安全产业的重要厂商之一，公司是“国家信息安全漏洞库一级技术支撑单位”、“信息安全标准化技术委员会成员单位”、“中国网络安全产业联盟常务理事单位”。同时，公司还获得了“国家知识产权示范企业”、“国家重点软件企业”、“国家高新技术企业”等多项荣誉。广大用户、行业同仁以及国家相关部门对公司的认可，体现出公司在信息安全行业的品牌已得到广泛认可。

在营销服务体系方面，公司在全国设有 27 个办事处，通过持续的市场拓展，公司已建立起覆盖全国的市场销售与技术支援体系，公司对行业价值客户的信息化建设和网络安全需求的理解和把握能力，使公司针对价值客户所提供的产品及服务赢得了广泛认同。公司拥有专业的安全服务与研究团队，能够自行挖掘安全漏洞，提供安全评估、安全应急等服务；具有本地化服务能力，能保证对用户突发事件的及时响应。公司广泛发展渠道合作伙伴，现拥有 1,900 余家认证代理商，公司已经建立了覆盖众多细分行业市场的完备的营销和服务渠道体系。目前，公司的办事处、售后服务机构与渠道合作伙伴之间形成了良好的互动，使得公司的产品和服务能得到快速推广。

4、公司法人治理结构完善，内控体系健全

公司已按照上市公司的治理标准建立了以法人治理结构为核心的现代企业制度，健全了各项规章制度和内控制度，并在日常经营过程中不断地改进和完善，形成了较为规范的公司治理体系和完善的内部控制环境。在募集资金管理方面，公司制定了《募集资金管理制度》，对募集资金的存储、使用进行了明确规定。健全的治理体系、内控制度和募集资金管理制度，能够促进募投项目的顺利实施，保证募集资金合理规范使用。

三、本次募集资金投资项目的基本情况

（一）新一代 IT 基础设施平台研发项目

1、项目基本情况和经营前景

本项目实施主体为迪普科技及其全资子公司，拟通过购进先进软硬件设备，增加研发人员投入，对下一代高性能软硬件平台、工业互联网安全相关产品、数

据安全相关产品等在内的新一代 IT 基础设施平台及产品进行持续研发，对新一代 IT 基础设施平台相关的产品进行升级和延伸。具体建设内容如下：

（1）下一代高性能软硬件平台研发。以公司原有 IT 基础设施产品为基础，升级开发新一代的 IT 基础设施产品，覆盖公司安全防护产品、应用交付产品、交换机产品等；升级开发高端高性能的硬件架构和软件平台，以支持 5G 低延时、高并发、高新建、海量终端的安全防护应用场景；升级开发支持云安全产品及平台，完善公司新一代 IT 基础设施产品的整体解决方案，提升相关解决方案在 5G、云安全中的竞争力。

具体项目	主要研发内容	预计研发成果
新一代安全防护产品	研发新一代的安全防护产品； 研究机器学习、AI 等新技术在防护产品中的应用和产品化； 研究新一代安全防护产品平台的 VSM 技术； 研发面向高并发、高新建、海量用户的 5G、物联网、大数据应用场景的高端安全防护产品	发布新一代安全防护产品； 满足 5G、物联网、大数据等场景对高端安全防护设备的需求； 满足安全防护产品等级保护建设需求； 完善新行业新领域行业化解决方案。
新一代应用交付产品	研发新一代应用交付产品； 研究高性能的国密芯片在运营商领域以及金融领域的应用； 推动应用交付和应用加速技术在 5G、物联网、大数据平台场景下的产业化和应用。	发布新一代高性能应用交付产品； 发布大数据、物联网、5G 等场景化解决方案。
新一代交换机产品	研究新一代交换芯片的交换机设计和开发。	发布新一代接入级交换机、数据中心级交换机以及骨干网交换机。
云计算安全防护平台	升级并更新换代网络功能虚拟化软件和平台； 研究容器安全、微隔离等云安全技术。	发布网络安全功能虚拟化软件； 发布容器安全、微隔离等解决方案和产品。
云管理平台以及运维管理平台	研究云管理平台云资源管理和编排等技术； 研究新一代运维管理和自动安全事件处置技术； 研究机器学习、AI 等技术在日志分析以及智能事件处置方面的应用。	完成新的云管理平台的开发，发布新一代云管理平台； 提供更智能的自动化运维和安全事件智能处置解决方案。
云原生应用防护产品	研究云原生应用防护相关产品，包含容器安全、镜像安全、开发安全等环节产品； 研究云原生应用防护管理平台。	完成云原生应用防护相关技术的研究，开发云原生应用防护产品设计； 完善云原生应用防护领域产品解决方案。

（2）工业互联网安全相关产品研发。围绕工业企业控制安全、网络安全、接入安全、主机安全、安全管理、安全可视化等主要安全需求，利用工业协议深

度解析、工控网络流量检测、行为基线建模、深度学习威胁识别、资产指纹匹配识别、工控主机防护、大数据流式处理、工控恶意代码检测、工控漏洞风险关联匹配、工控数据库审计、非法外联检测等关键技术，研发工控防火墙、工控监测审计系统、工控入侵检测系统、工控漏洞检测平台、工控安全管理平台、工控主机防护系统、工控态势感知等工业互联网安全产品，形成具备防攻击、防病毒、防入侵、防控制等能力的工业互联网安全解决方案。

具体项目	主要研发内容	预计研发成果
工控防火墙	研发升级工业协议库、工业协议深度过滤功能，丰富工业协议种类，适应更多场景。	实现对工业协议库、工业协议深度解析数量和质量方面的研发提升； 引入新的硬件平台，丰富工控防火墙产品档次。
工控监测审计系统	研发升级工控资产被动识别、本地化可视化分析、工控指令监测、行为基线建模等功能。	实现对工控流量监测、工控指令监测、行为基线建模等数量和质量方面的研发提升； 引入新的硬件平台，丰富工控监测审计产品档次。
工控入侵检测系统	研发工控漏洞利用检测、工业协议深度检测、ARP 攻击检测、DDOS 攻击检测、安全事件管理及分析、自定义语义检测等功能；	实现工控 IDS 引擎、工控安全事件库、自定义检测引擎等功能的研发； 发布多档次的工控入侵检测产品。
工控漏洞检测平台	研发工控资产无损识别、无损漏洞检测、资产扫描报告、交互式安全检测报告、可视化风险监控分析功能；	实现工控资产指纹库、资产识别引擎、工控漏洞库、漏洞关联匹配引擎等功能的研发； 发布便携式、机架式形态的工控漏洞检测产品。
工控安全管理平台	研发资产管理、拓扑管理、设备管理、策略管理、安全监测分析、日志管理等功能；	实现工控安全设备管理、资产拓扑管理、集中策略管控等功能的研发； 发布软件版、硬件版两种形态产品。
工控主机防护系统	研发应用程序白名单、脚本白名单、网络白名单、移动存储管控等功能；	发布具备多种白名单、移动存储管控等功能的工控主机防护产品。
工控态势感知	研发工控态势感知（风险趋势、攻击态势、漏洞态势、资产态势）、工控安全分析（事件聚合、关联分析、流量异常、设备画像、行为分析；支持攻击路径、影响主机、事件取证）、预警处置、报告管理、工控知识库。	发布具备 AI、大数据等技术能力，覆盖工控威胁态势、工控安全分析、预警处置等功能的工控态势感知产品。

（3）数据安全相关产品研发。以大数据处理引擎为基础，利用数据资产识别、敏感数据识别、数据流转监控、数据脱敏、数据水印等关键技术，开发为用户提供数据安全运营能力、数据安全管控能力、数据安全监控能力的综合性数据

安全治理平台。

具体项目	主要研发内容	预计研发成果
大数据分析平台	研究大数据存储技术、实时分析技术、离线分析技术和大数据情况下数据安全事件分析技术； 研究深度学习技术、关联分析技术、事件建模技术在数据风险分析方面的应用； 研究数据资产流转关系梳理技术、数据资产血缘关系分析技术在数据资产领域的应用。	发布基于大数据和人工智能技术的数据安全治理平台； 完善数据安全管控治理解决方案。
全流量分析系统	研究网络协议分析技术在数据流转接口方面的应用； 研究通过网络流量提取技术在敏感信息识别方面的应用； 研究全流量存储技术在敏感信息事件溯源方面的应用。	发布全流量分析系统； 完善数据安全治理平台的主动采集能力。
主动探测采集系统	研究主动扫描技术在数据资产识别方面的应用； 研究基于语义分析技术在敏感数据识别方面的应用； 研究图像识别技术在非格式化数据的敏感数据识别。	发布主动探测采集系统； 完善数据安全治理平台的主动采集能力。

本项目有利于公司把握新型基础设施建设的发展契机，满足各行各业信息化建设中对新一代 IT 基础设备的需求，解决 5G、云计算以及云原生应用等场景下的安全问题，加强对工业互联网安全技术的布局，把握数据安全市场的发展机会，具有良好的经营前景。

2、项目与现有业务或发展战略的关系

本项目紧密围绕公司主营业务展开，是公司依据市场需求和技术趋势对相关产品进行的升级研发，是对公司现有产品及解决方案体系的进一步升级与扩充，旨在增强公司技术实力，提升公司企业级网络通信领域相关产品及解决方案的竞争力。本项目与公司现有业务或发展战略的关系具体如下：

（1）下一代高性能软硬件平台研发

具体项目	与公司现有业务或发展战略的关系
新一代安全防护产品	以新一代高性能云计算数据中心安全平台为基础，融合公司在网络及应用软件等方面的技术，对公司现有产品进行升级： 1、发布新的盒式 VSM 特性，在公司原有产品的框式 VSM 技术基础上开发，提升盒式竞争力； 2、通过机器学习、AI 等新技术的应用，增强原有产品的防护能力； 3、优化原有产品的性能，满足 5G、物联网、大数据等应用场景的高性能安全防护设备的需求；

具体项目	与公司现有业务或发展战略的关系
	4、利用国产化硬件，开发新一代的安全防护产品，满足国内国产化安全防护产品的需求。
新一代应用交付产品	以新一代高性能应用交付平台为基础，融合公司在网络及应用软件等方面的技术，对公司现有产品进行升级： 1、可编程脚本语言：新增事件入口，扩展脚本语言适应范围，从网络层到应用层均支持脚本介入处理；对各种不同应用提供模式引导，简化用户配置；采用新的脚本编译引擎，提升负载脚本语句性能； 2、高可用集群：对现有产品进行升级，实现大规模应用集群；简化配置，增加大量容错机制降低用户学习和使用成本； 3、应用交付云平台：使用全新云平台接口，全面提升云平台对应用交付产品配置效率；升级应用交付产品多用户管理模式，提升产品支持的云平台用户规格； 4、智能化运维和配置：引入了多种智能化配置和运维工具。支持多种规则处理批量添加、修改、删除和查询服务器的各种配置和状态。新增对服务器多维度的运维信息收集，异常分析以及故障处理机制。引入了多种业务模拟功能，便于用户进行业务验证。
新一代交换机产品	在现有 DPX19000 产品基础上，新开发 DPX29000 产品系列核心交换机，推出高密度 100G 接口板卡和更高性能交换网板；同时推出全系列国产化交换机。
云计算安全防护平台	在现有虚拟化软件产品基础上，研发 SDN 引流技术的对接，虚拟化与第三方云平台的对接，例如 OpenStack 平台的接口、插件的开发，第三方云平台的策略功能对接，引入容器安全和微隔离产品及解决方案： 1、研究容器安全，为后续的容器安全解决方案做技术储备； 2、研究微隔离技术和方案，将虚拟化软件系列产品用于微隔离场景，开发微隔离用的微隔离平台。
云管理平台以及运维管理平台	1、在原有的管理平台等技术平台的基础上，研究和开发 AI 日志分析、AI 辅助攻击处置等新特性； 2、研究和开发云管理平台，完善云安全环境的安全防护能力编排技术和解决方案。
云原生应用防护产品	1、全新的研究性项目，研究和储备新的研究方向和技术，研究云原生应用场景，以及对应的安全问题； 2、改进原有产品，使之适配云原生应用场景的防护； 3、储备云原生安全相关技术，研究新的技术开发方向，为后续产品做储备。

（2）工业互联网安全相关产品研发

具体项目	与公司现有业务或发展战略的关系
工控防火墙	引入专用于工业应用环境的防火墙产品，包含工业协议智能识别、工业协议深度过滤等功能，应对工业控制系统网络安全防护的需求。
工控监测审计系统	引入专用于工业应用环境的安全审计产品，包含行为基线建模、本地可视化分析等功能，应对工业控制系统网络安全审计的需求。
工控入侵检测系统	引入专用于工业应用环境的入侵检测产品，包含工控漏洞利用检测、安全事件管理等功能，应对工业控制系统网络入侵检测的需求。
工控漏洞检测平台	引入专用于工业应用环境的工控漏洞检测产品，包含工控资产无损识别、无损漏洞检测等功能，应对工业控制系统网络脆弱性检测的需求。
工控安全管理平台	引入专用于工业应用环境的工控安全管理平台产品，对部署的工控防火墙、工控监测审计、工控入侵检测、工控漏洞检测等产品进行

具体项目	与公司现有业务或发展战略的关系
	集中管控，应对工业控制系统网络安全集中管理的需求。
工控主机防护系统	引入专用于工业应用环境的工控主机防护产品，对工业现场工作站、服务器等系统进行终端安全防护。
工控态势感知	引入专用于工业应用环境的工控态势感知产品，基于 AI，大数据等技术对采集的工业安全数据进行挖掘利用，并与工业安全防护设备形成处置联动，提升工业企业的安全监测及应急处置能力。

（3）数据安全相关产品研发

具体项目	与公司现有业务或发展战略的关系
大数据分析平台	基于大数据、机器学习和事件建模关联分析，实现数据安全的资产管理，监控数据安全事件，掌握数据安全风险。
全流量分析系统	基于全流量识别技术，发现数据接口，并通过对流量监控发现数据安全风险。
主动探测采集系统	基于数据扫描和特征识别技术，发现数据资产，并监控数据资产的涉敏情况，流转情况等。

3、项目投资计划

本项目计划总投资 63,265.07 万元，拟投入募集资金 45,354.00 万元，项目具体投资内容如下：

单位：万元

项目	投资金额	拟投入募集资金
研发费用	35,656.70	30,400.00
设备投资	14,904.00	14,904.00
软件投资	50.00	50.00
预备费	745.20	-
市场推广费用	6,157.80	-
铺底流动资金	5,751.37	-
合计	**63,265.07**	**45,354.00**

4、项目预计实施时间和整体进度安排

本项目建设期预计约为 3 年，整体进度安排如下：

实施阶段	建设期（月）											
	3	6	9	12	15	18	21	24	27	30	33	36
硬件设计、软件需求分析												
硬件测试、软件特性开发												
验证												
试产												

实施阶段	建设期（月）											
	3	6	9	12	15	18	21	24	27	30	33	36
市场推广、产品更新												

5、项目经济效益

本项目是对公司现有产品进行的升级研发，研发升级后的产品实现的效益是公司对相关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。

6、项目审批、备案情况

本项目拟在租赁办公场地或自有办公场地开展，不涉及土地购置事项。

本项目已取得杭州市滨江区发展和改革局《杭州高新区（滨江）企业投资项目备案通知书》（滨发改金融[2020]028 号），本项目已在建设项目环境影响登记表备案系统（浙江省）完成备案（备案号：202033010800000182）。

本项目实施前不涉及其他尚需履行的程序，项目实施不存在重大不确定性。

（二）智能测试、验证及试制基地建设项目

1、项目基本情况和经营前景

本项目实施主体为迪普科技及其全资子公司，公司拟通过购进先进软硬件设备，以自建方式新建智能厂验中心、可靠性测试中心、硬件鉴定中心、新产品试制中心、智能制造中心、智能仓储中心等与公司主营业务产品相关的测试、验证、试制和仓储等场地及相关基础配套用房，实现测试、验证、试制及仓储的智能化和集中化管理，提升公司测试、验证及试制的稳定性和可靠性，提高公司经营管理能力和效率。具体建设内容如下：

具体项目	主要建设内容
智能厂验中心	建设全面系统的一站式厂验中心，根据客户需求提出的厂验，按照项目配置将不同产品模拟组网测试，根据客户关心功能，配置并运行设备，经过长时间稳定测试筛选出配合有异常的产品或者模块，验证客户的网络方案中设备和技术方案的可靠性、可行性，检验产品及组网架构能否符合客户的商业和技术目标、是否存在潜在的技术隐患等。
可靠性测试中心	建设满足中国合格评定国家认可委员会（CNAS）标准的测试实验室：电磁兼容性（EMC）实验室测试设备或系统在其电磁环境中符合要求运行并不对其环境中的任何设备产生无法忍受的电磁干扰的能力；安规实验室对产品的安

具体项目	主要建设内容
	规摸底测试与验证测试；机械实验室验证产品的机械强度是否满足设计要求；失效分析实验室考虑采用物理切片研磨的方法发现器件焊点等失效的根本原因针对原因找出失效解决方案；高加速应力筛选（HASS）、环境应力筛选（ESS）等通过提高产品运行环境的压力等手段提前暴露产品早期失效提升产品的最终质量。
硬件鉴定中心	建设新产品导入过程中验证器件的离散性对信号级别影响的鉴定中心，在小批量试产后随即抽取合适数量产品重新进行信号级别测试，对比研发阶段测试报告，发现差异找出问题并回归解决，保障生产环节严格复制研发定型产品。
新产品试制中心	建设区别于量产产品的车间用于进行新产品的装配测试，通过各种异常模拟制造环节可能发生的各种异常情况，验证产品是否满足所有情况下的可制造性、可测试性、可维修性，实现从研发原型机到量产整机。
智能制造中心	建设基于制造执行系统（MES）的智能制造车间，正向制造完成整机的装配测试老化业务，逆向制造完成整机的拆解、剔除不达标部件、完成整机的装配测试老化等业务。
智能仓储中心	建设新的仓储中心和管理信息化系统平台，协调各个环节的运作，保证及时准确的进出库作业和实时透明的库存控制作业，合理配置仓库资源、优化仓库布局和提升仓库作业，节约劳动力和库存空间，降低运营成本。
基地配套用房	建设基地配套的会议室、培训室、员工宿舍及食堂。

本项目有利于进一步促进公司核心技术产业化落地，具有良好的经营前景。

2、项目与现有业务或发展战略的关系

本项目为新建公司主营业务产品的智能测试、验证、试制和仓储基地，涉及的业务环节既包含了部分将公司在研产品由研发导入生产阶段的过度性技术环节，也包含了公司产品生产、销售中的必须环节，本项目的建设实施将满足公司现有业务及未来业务发展带来的经营场地需求，提高产品质量、加快用户需求响应、加速研发转化，预计建设完成后对公司业务或发展战略的促进作用具体如下：

具体环节	预计建设完成后对公司业务或发展战略的促进作用
厂验	提供全面系统的一站式验证服务，优化厂验服务流程，显著降低返工、外部失败成本、业务流失成本等非一致性成本，有效缩短客户项目建设周期、减少项目建设人员投入。
可靠性测试	充分暴露研发设计过程中与加工制造过程中影响产品可靠性的因素，通过产品优化变更使其满足设计规格需求，有效加快公司新产品的认证进度，降低认证费用，助力快速推向市场，早一步抢占市场先机。
硬件鉴定	最小化生产销售产品的设计缺陷，进一步加快公司核心知识产权落地，保证公司产品稳定一致。
新产品试制	进一步完善公司新产品试制，通过研发与制造工程师不断的磨合修改达到效率与质量最优，在保证质量的前提下快速完成新品导入量产。
正向与逆向制造	完成公司智能化设计与改造，减少产品质量对工人个人技术水平的依赖性，提高设备产出效率，提升产品质量。
仓储	通过信息化、物联网和机电一体化，提高准确性和实时性，减少人工操作，从而降低仓储成本，提升仓储管理能力，提高交付响应速度。

3、项目投资计划

本项目计划总投资 67,269.25 万元，拟投入募集资金 56,146.00 万元，项目具体投资内容如下：

单位：万元

项目	投资金额	拟投入募集资金
建设工程投资	32,649.00	32,649.00
设备投资	20,812.00	20,812.00
土地投资	2,100.00	2,100.00
软件投资	585.00	585.00
预备费	2,680.30	
铺底流动资金	8,442.95	
合计	**67,269.25**	**56,146.00**

4、项目预计实施时间和整体进度安排

本项目建设期预计约为 3 年，整体进度安排如下：

实施阶段	建设期（月）											
	3	6	9	12	15	18	21	24	27	30	33	36
初步设计												
施工图设计												
厂房建造及装修												
设备招投标订货												
设备到货安装												
劳动培训与试产												
竣工验收												

5、项目经济效益

本项目为新建公司主营业务产品的智能测试、验证、试制和仓储基地，以加快用户需求响应、加速研发转化、提高产品质量，本项目无法单独核算因本次募集资金使用而产生的效益。本项目建设完后，将显著提高公司测试、验证、试制和仓储的办公场地软硬件水平，提升公司的经营实力与运营管理效率，有利于公司长期稳定发展。

6、项目审批、备案情况

本项目实施地点为杭州高新区（滨江），拟以出让方式取得约 20,000 平方米工业用地用于项目建设。公司已与杭州高新开发区（滨江）经济和信息化局签署《建设项目投资意向书》，明确了相关用地意向，该项目用地正在按照正常流程进行报批。

本项目已取得杭州市滨江区发展和改革局《杭州高新区（滨江）企业投资项目备案通知书》（滨发改金融[2020]029 号），本项目已在建设项目环境影响登记表备案系统（浙江省）完成备案（备案号：202033010800000183）。

本项目后续需履行的其他行政审批事项属于建筑工程类项目需履行的一般行政审批事项，不存在无法取得相关行政审批而导致项目无法顺利实施的重大风险，项目实施不存在重大不确定性。

四、本次发行对公司经营管理、财务状况等的影响

（一）对公司经营业务的影响

本次发行的募集资金投资项目符合国家相关的产业政策以及公司整体战略发展方向，募投项目的实施有利于公司进一步提高研发能力，提高公司测试和验证的稳定性和可靠性，强化公司主营业务的优势，提升公司的核心竞争力和可持续发展能力，增强公司的综合实力。

（二）对公司财务状况的影响

本次发行完成后，公司的资金实力将得到有效提升，公司总资产和净资产规模将有所增加，资产负债率将有所下降，资金实力将有效提升，财务结构将更加稳健合理，经营抗风险能力将进一步加强。

五、可行性分析结论

综上，本次发行是公司把握市场机遇，实现可持续发展的重要举措。本次发行的募集资金投向符合国家产业政策以及公司的战略发展规划，有利于提升公司整体研发实力，进一步加强公司主营业务优势，提升公司的核心竞争力和可持续发展能力。本次募集资金投资项目的实施，将优化公司资本结构，提升公司的综合竞争实力和可持续发展能力，符合全体股东的利益。本次募集资金投资项目是可行的、必要的。

第四节 董事会关于本次发行对公司影响的讨论与分析

一、本次发行完成后，公司的业务及资产的变动或整合计划

本次发行募集资金投资项目均围绕公司主营业务开展，符合国家有关产业政策以及未来公司整体战略发展方向。本次发行完成后，公司的主营业务保持不变，不涉及资产或股权认购事项，不会导致公司业务和资产的整合情况。

二、本次发行完成后，公司控制权结构的变化

截至本募集说明书签署日，公司控股股东、实际控制人为郑树生，其直接持有公司 193,611,490 股股票，占公司总股本的 48.40%，并通过思道惟诚间接控制公司 31,535,715 股股票，占公司总股本的 7.88%，郑树生通过直接和间接方式合计控制公司 56.29%的股份，为公司实际控制人。此外，郑树生通过非控制的经略即远、格物致慧和闻涛岭潮间接持有公司的部分股份，截至本募集说明书签署日，郑树生直接和间接共持有公司 57.26%的股份。

按照本次发行的发行数量上限 4,000 万股测算，本次发行完成后，郑树生直接持有公司 44.00%的股份，通过直接和间接方式合计控制公司 51.17%的股份，仍为公司的控股股东、实际控制人。本次发行不会导致公司控制权发生变化。

三、本次发行完成后，公司与发行对象及发行对象的控股股东和实际控制人从事的业务存在同业竞争或潜在的同业竞争的情况

截至本募集说明书签署日，本次发行尚未确定发行对象，最终是否存在公司与发行对象及发行对象的控股股东和实际控制人从事的业务存在同业竞争或潜在的同业竞争的情况，将在本次发行结束后公告的发行情况报告书中予以披露。

四、本次发行完成后，公司与发行对象及发行对象的控股股东和实际控制人可能存在的关联交易的情况

截至本募集说明书签署日，本次发行尚未确定具体发行对象，最终是否存在公司与发行对象及发行对象的控股股东和实际控制人存在关联交易的情况，将在本次发行结束后公告的发行情况报告书中予以披露。

第五节 与本次发行相关的风险因素

投资者在评价公司本次向特定对象发行股票时，除本募集说明书提供的其他各项资料外，应特别认真考虑下述各项风险因素：

一、对公司核心竞争力、经营稳定性及未来发展可能产生重大不利影响的因素

（一）技术创新风险

公司所处的行业在技术与产品上更新换代很快，企业需要随时判断行业发展方向，预测技术发展趋势，并根据判断及预测的结果不断调整相应的研发和创新，然后将研发和创新成果转换为成熟产品推向市场，才能够使自身的产品贴合市场需求，并保持持续的竞争力和领先优势。

虽然公司拥有研发创新能力，在研发方向的选择上也是基于长期行业实践积累的经验以及对市场需求充分调研的基础上综合决定的，但是由于行业发展趋势的不确定性，可能会导致公司选择及投入的研发方向、创新成果与未来的行业发展趋势存在差异，使公司新产品无法满足未来的行业需求，从而降低公司产品体系的整体竞争力。另外，各种原因造成的研发创新及相应产品转化的进度拖延，也有可能造成公司未来新产品无法及时投放市场，对公司未来的市场竞争造成不利影响。

（二）技术失密和核心技术人员流失风险

公司主营产品科技含量较高且在核心关键技术上拥有自主知识产权，技术研发与创新依赖于所拥有的核心技术以及培养、积累的核心技术人员。当前公司多项产品和技术处于研发阶段，因此核心技术人员稳定及核心技术保密对公司的发展尤为重要。如果在技术和人才的市场竞争中，出现技术外泄或者核心技术人员流失的情况，可能会在一定程度上影响公司的技术创新能力。

（三）原材料采购风险

公司产品生产所用的芯片、内存条、光模块等原材料，其高端款型的核心技术垄断，市场集中度较高，主要由美国、韩国、中国台湾等国家或地区的知名厂

商生产，最终供应商采取渠道销售模式，授权专业代理商向 IT 基础设备厂商销售。公司研发和生产部门选定产品所需原材料原厂品牌后，采购部门向交付迅速、价格具有竞争优势、能够满足公司相应采购需求的贸易供应商采购该等原材料。报告期内，该等原材料供给较充分，价格总体趋势相对稳定。同时，随着国内电子元器件厂商的发展，国产电子元器件的竞争力不断增强，公司对该等原材料的国产替代产品进行了较深入的技术研究，已经部分实现产品化，并计划持续加大采用替代原材料产品的比重。然而公司目前芯片、内存条、光模块等原材料的高端款型的采购，在整体上仍存在一定进口供应风险。若国际市场供需变化导致进口原材料价格波动，或因为国际贸易环境变化导致进口原材料供应限制，而公司不能采取有效应对措施，短期内公司可能会遇到生产成本升高、客户供货紧张等问题，将会对公司的产品生产、销售及经营业绩产生一定的不利影响。

（四）外协加工风险

出于购置焊接机等生产设备利用率较低且投资回报期长、焊接及装配等环节委外加工模式在业内较为成熟等因素考虑，公司将产品生产的 PCBA 阶段全部外协加工，装配与测试阶段根据业务量弹性外协加工，公司自身负责原材料采购、部分产品的组装、软件灌装、整机测试、高温老化、验证测试等环节的加工或控制。随着未来公司生产规模的扩大，外协加工的规模必然随之增长，如果现有外协厂商出现加工任务饱和、加工能力下降或是公司出现突发大额订单等情况，有可能会影响公司产品生产进度，从而影响产品及时供货，导致客户满意度下降，甚至存在丢失客户和订单的风险。另外，如果外协加工厂加工的产品存在重大质量问题，并且因为产品质量问题引致丢失客户、纠纷、索赔或诉讼，均将对公司的市场信誉、市场地位甚至对公司销售造成重大不利影响。

（五）产品销售风险

由于信息安全行业最终用户分散、用户具体需求各有差异，报告期内，公司的产品销售采用渠道销售和直签销售相结合的方式，并以渠道销售为主。公司产品通过代理商渠道销售的最终用户大部分属于运营商、政府、金融、电力能源、教育、医疗等领域。基于行业特性，公司业务主要以解决方案提供商的模式进行，并以项目招投标的方式实现销售，招投标过程通常受公司不能控制的若干因素影响，包括市场情况、客户招投标计划、招投标条件、标书所规定的竞标者的资质

及其他竞标者所提供的条款等，因此，公司销售情况受到项目招投标结果的直接影响。若未来年度公司主要客户招投标竞争激烈而公司不能中标、中标份额下降或入围产品价格较大幅度下降，或招投标计划调整而项目规模、数量、时间等情况发生较大变化，将影响公司当年或下一年度的销售情况，可能存在公司向主要客户销售收入波动或经营业绩下滑的风险。

（六）市场竞争风险

国内信息安全行业厂商众多，市场竞争较为激烈，随着信息安全市场空间进一步拓展，公司与行业内具有技术、品牌、人才和资金优势的厂商之间的竞争可能进一步加剧。在应用交付市场，公司与国外竞争对手相比在品牌影响力、资金实力、专业人才水平、产品技术积累等方面仍存有差距，随着未来国内应用交付企业的不断崛起与发展，公司也可能会面临来自国内企业的挑战与竞争。

（七）管理风险

报告期内，公司的资产规模持续扩大。随着募集资金投资项目的实施，公司资产规模、人员规模将有一定的增长，需要公司在资源整合、市场开拓、产品研发与质量管理、财务管理、内部控制等诸多方面进行调整，对各部门工作的协调性、严密性、连续性也提出了更高的要求。如果公司管理层素质及管理水平不能适应公司规模扩张的需要，组织模式和管理制度未能随着公司规模的扩大而及时调整、完善，公司的市场竞争力将因此受到削弱。

（八）财税政策风险

根据国家有关税收的法律法规，报告期内，公司享受的税收优惠主要包括增值税退税和企业所得税优惠。如果国家税收优惠政策发生不利变化，或如果公司以后年度不能被认定为“国家规划布局内重点软件企业”或“高新技术企业”，公司需按 25%的税率缴纳企业所得税，将对公司的经营成果产生不利影响。公司存在税收优惠政策变化风险。

（九）主营业务收入增速下滑风险

报告期内，公司的主营业务收入分别为 61,555.34 万元、70,369.43 万元、80,278.93 万元和 31,619.79 万元，最近三年同比增长 15.77%、14.32%和 14.08%，持续增长，但增长态势趋于平缓。尽管目前公司主营业务所属行业的国家政策、

发展状况、技术前沿，公司的销售、经营和管理模式，均未发生较大的变化。但是，如果未来出现行业竞争加剧、市场需求萎缩、重要客户流失或经营成本上升等不利因素，或者公司出现不能巩固和提升市场竞争优势、跟不上产品技术更新换代的速度、市场开拓能力不足、募集资金投资项目的实施达不到预期效果等情形，公司业绩增长速度将可能会有所降低，亦可能出现业绩下滑。

（十）经营业绩季节性波动风险

公司的营业收入有一定的季节性，主要原因是公司业务的下游用户群体主要来源于运营商、政府、公共事业（电力能源、教育、医疗）等领域，这些用户大多在上半年对全年的投资和采购进行规划，下半年再进行项目招标、项目验收和项目结算。因此，公司下半年（尤其是第四季度）的业务收入显著高于上半年（或其他季度），使得公司整体的销售收入在上、下半年呈现不均衡性。

2017-2019 年，公司营业收入和净利润按季度分布情况如下：

项目	2019 年度		2018 年度		2017 年度	
	当期营业收入占比	当期净利润占比	当期营业收入占比	当期净利润占比	当期营业收入占比	当期净利润占比
第一季度	20.17%	18.59%	20.12%	18.44%	19.82%	17.43%
第二季度	22.59%	18.07%	23.35%	19.83%	22.89%	23.07%
上半年小计	**42.76%**	**36.66%**	**43.47%**	**38.27%**	**42.70%**	**40.49%**
第三季度	24.70%	25.75%	24.72%	27.73%	24.32%	27.13%
第四季度	32.53%	37.59%	31.82%	34.01%	32.98%	32.38%
下半年小计	**57.24%**	**63.34%**	**56.53%**	**61.73%**	**57.30%**	**59.51%**
合计	**100.00%**	**100.00%**	**100.00%**	**100.00%**	**100.00%**	**100.00%**

注：各季度收入和利润数据未经审计。

从公司各季度营业收入和净利润占全年的比重来看，2017-2019 年，公司下半年营业收入占比均显著高于上半年，公司的营业收入呈现的季节性特征导致公司利润也呈季节性分布。公司营业收入在全年实现的不均衡性，可能对公司生产经营活动造成一定不利影响。由于费用在年度内较为均衡的发生，而收入主要集中在下半年，因此可能造成上半年净利润低于全年的 50%的情况。公司收入和盈利有一定的季节性波动，投资者不宜以半年度或者季度报告的数据推测全年盈利情况。

（十一）应收账款金额较大及发生坏账的风险

报告期各期末，公司应收账款账面价值分别为 8,592.35 万元、7,813.75 万元、6,848.05 万元和 6,829.94 万元，应收账款金额较大。

项目	2020-06-30	2019-12-31	2018-12-31	2017-12-31
账面价值（万元）	6,829.94	6,848.05	7,813.75	8,592.35
账面价值较上期末增长	-0.26%	-12.36%	-9.06%	-21.08%
占期末总资产比例	3.22%	3.20%	5.77%	7.90%
应收账款周转率（次）	4.54	10.38	7.91	6.04
应收账款余额前 5 名之和占比	97.65%	95.28%	89.49%	94.64%

报告期各期末，公司应收账款占期末总资产的比例分别 7.90%、5.77%、3.20%和 3.22%，应收账款周转率分别为 6.04、7.91、10.38 和 4.54。报告期各期末，应收账款余额前五名之和占比分别为 94.64%、89.49%、95.28%和 97.65%。

公司应收账款主要以政府事业单位，以及运营商、电力能源、金融等领域的企业客户为主。虽然客户资信状况良好，应收账款较少发生坏账，应收账款总体状况良好，但随着公司经营规模的扩大，应收账款金额较大，如出现客户信用发生变化等情况，公司存在应收账款坏账损失增大的风险。

（十二）期间费用较高的风险

报告期内，公司期间费用主要由销售费用、研发费用和管理费用组成。2017-2019 年及 2020 年 1-6 月，公司销售费用、研发费用和管理费用的合计发生额分别为 33,932.80 万元、36,622.92 万元、41,301.56 万元和 19,458.56 万元，占同期营业收入的比例分别为 55.01%、52.01%、51.39%和 61.50%。销售费用、研发费用和管理费用的投入，推动了市场渠道的建设，巩固、提高了公司的行业地位，培养了研发人才、管理团队，为公司持续发展提供了动力。

未来几年内，为了进一步巩固公司的行业地位和竞争优势，公司将继续增加研发和销售等投入，相关期间费用可能持续增加。这些投入给公司技术创新能力、品牌价值和新产品开发能力所带来的提升效应将会在未来一定时间内逐步显现。期间费用投入与效益产生之间会有时间差，若短期内大规模投入未能产生预期效益，公司的经营业绩将会受到不利影响。

（十三）经营活动产生的现金流量净额波动风险

2017-2019 年及 2020 年 1-6 月，公司经营活动产生的现金流量净额分别为 17,567.08 万元、22,244.95 万元、32,086.37 万元和-832.24 万元。2017-2019 年，公司经营活动产生的现金流量净额为正，2020 年 1-6 月，公司经营活动现金净额为负主要系受季节性、疫情影响，部分下游用户的 IT 系统建设项目的采购和项目建设进度有所延缓，以及原材料战略备货和员工薪酬增加所致。未来，随着公司业务规模的不断增长，资金支出与销售回款之间存在一定的时间差异，从而影响经营活动产生的现金流量净额，导致资产流动性风险。

二、可能导致本次发行失败或募集资金不足的因素

（一）审批风险

本次向特定对象发行股票尚需经深圳证券交易所审核通过并经中国证监会同意注册，能否通过深圳证券交易所审核并完成发行注册程序，以及最终通过审核及完成注册时间存在不确定性。因此，公司本次向特定对象发行股票事项存在未能通过审核或完成注册的风险。

（二）发行风险

公司本次向特定对象发行股票的发行结果将受到证券市场整体情况、公司股票价格走势、投资者对本次发行方案的认可程度等多种内外部因素的影响。因此，公司本次向特定对象发行股票存在发行募集资金不足甚至发行失败的风险。

三、对本次募投项目的实施过程或实施效果可能产生重大不利影响的因素

（一）募投项目实施风险

本次募集资金拟投资的项目的可行性分析是基于目前的国家产业政策、国内外市场条件作出的，若国家产业政策发生变化或随着时间的推移，在项目实施时如果募集资金不能及时到位，或因市场环境突变、行业竞争加剧、项目建设过程中管理不善导致募集资金投资项目不能如期实施，都将会导致项目不能如期完成。

本次募集资金拟投资的新一代 IT 基础设施平台研发项目，是在公司原有技

术基础上的进一步开发和升级，公司在相关项目中对诸多关键技术难点进行了预研和攻关，有效降低了项目整体风险。但技术的升级开发具有不确定性，如未能按期完成研发计划，可能会导致新产品推出时间延后、新技术开发进度不达预期、研发遭遇技术瓶颈甚至失败，将对公司进一步提升产品竞争力带来不利影响。

此外，本次募投项目实施完成后每年将新增折旧摊销费用，在一定程度上影响公司的盈利水平，从而使公司面临盈利能力下降的风险。

（二）募投项目用地风险

本次募集资金拟投资的智能测试、验证及试制基地建设项目，实施地点为杭州高新区（滨江），拟以出让方式取得约 20,000 平方米工业用地用于项目建设。公司已与杭州高新开发区（滨江）经济和信息化局签署《建设项目投资意向书》，明确了相关用地意向，该项目用地正在按照正常流程进行报批。截至本募集说明书签署日，公司尚未就募投项目用地签署《国有建设用地使用权出让合同》，公司最终能否取得募投项目用地仍存在一定的不确定性。如公司未能如期取得募投项目用地的土地使用权，可能会对募投项目的实施产生一定影响。

四、与本次发行相关的其他风险因素

（一）股市价格波动风险

股票市场收益与风险并存。股票价格的波动不仅受到公司业绩及行业发展的影响，还受到宏观经济、监管政策、市场交易及投资者心理预期等多种因素影响。因此即使在公司经营状况稳定的情况下，公司的股票价格仍可能出现较大幅度的波动，有可能给投资者造成损失，存在一定的股价波动风险。

（二）即期回报被摊薄的风险

本次向特定对象发行股票募集资金到位后，公司净资产规模和总股本相应增加，故若经营效率未能在短期内得到有效提升，在公司总股本和净资产均增加的情况下，公司的每股收益、加权平均净资产收益率等财务指标短期内存在下降的风险，即本次向特定对象发行股票存在摊薄每股收益的风险。

（三）股东分红减少、表决权被摊薄的风险

本次发行将在一定程度上增加公司总股本和归属母公司股东所有者权益等

指标，股东回报短期内仍主要以现有业务的收益实现，因此公司原股东面临分红因总股本增加而减少的风险。同时，由于总股本的增加，公司原股东在股东大会上所享有的表决权会相应被摊薄，从而存在表决权被摊薄的风险。

（四）新冠肺炎疫情等重大不确定因素影响的风险

新冠肺炎疫情的发展和后续对社会、经济环境的影响，会对公司市场业务开拓、经营生产产生干扰，存在影响公司未来业绩目标实现的风险。影响程度取决于疫情防控的进展情况、持续时间以及各地防控政策的实施情况和后续影响情况。尽管公司持续密切关注新冠肺炎疫情的发展情况，并评估和积极应对其对公司财务状况、经营成果等方面的影响情况，公司未来业务经营仍存在受新冠肺炎疫情等重大不确定因素影响的风险。

第六节 与本次发行相关的声明

一、发行人及全体董事、监事、高级管理人员声明

本公司及全体董事、监事、高级管理人员承诺本募集说明书内容真实、准确、完整，不存在虚假记载、误导性陈述或重大遗漏，按照诚信原则履行承诺，并承担相应的法律责任。

公司全体董事签名：

郑树生	周顺林	邹禧典
李 强	钱雪彪	黄海波
张龙平	肖 冰	王 匡

公司全体监事签名：

关 巍	陈忠良	黄 成

公司全体非董事高级管理人员签名：

陈瑾瑾	康 亮	李 治

杭州迪普科技股份有限公司

2023年 10月 22日

二、发行人控股股东、实际控制人声明

本人承诺本募集说明书内容真实、准确、完整，不存在虚假记载、误导性陈述或重大遗漏，按照诚信原则履行承诺，并承担相应的法律责任。

公司控股股东、实际控制人签名：

郑树生

2020 年 10 月 22 日

三、保荐人（主承销商）声明

本公司已对募集说明书进行了核查，确认本募集说明书内容真实、准确、完整，不存在虚假记载、误导性陈述或重大遗漏，并承担相应的法律责任。

项目协办人：

寨新华

保荐代表人：

吴继平 赵润璋

法定代表人：

王常青

中信建投证券股份有限公司

2020年10月20日

声明

本人已认真阅读杭州迪普科技股份有限公司募集说明书的全部内容，确认募集说明书不存在虚假记载、误导性陈述或者重大遗漏，并对募集说明书真实性、准确性、完整性承担相应法律责任。

保荐机构总经理：

李格平

保荐机构董事长：

王常青

中信建投证券股份有限公司

2025年 10 月 22 日

四、律师事务所声明

本所及经办律师已阅读募集说明书，确认募集说明书内容与本所出具的法律意见书不存在矛盾。本所及经办律师对发行人在募集说明书中引用的法律意见书的内容无异议，确认募集说明书不因引用上述内容而出现虚假记载、误导性陈述或重大遗漏，并承担相应的法律责任。

上海市锦天城律师事务所

负责人：_____
顾功耘

经办律师：_____
李 波

经办律师：_____
张灵芝

经办律师：_____
李 青

2020年 10 月 22 日

五、会计师事务所声明

本所及签字注册会计师已阅读募集说明书，确认募集说明书内容与本所出具的审计报告等文件不存在矛盾。本所及签字注册会计师对发行人在募集说明书中引用的审计报告等文件的内容无异议，确认募集说明书不因引用上述内容而出现虚假记载、误导性陈述或重大遗漏，并承担相应的法律责任。

经办注册会计师：

孙 峰　　吕爱珍

会计师事务所负责人：

杨志国

立信会计师事务所（特殊普通合伙）

2020 年 10 月 22 日

六、发行人董事会声明

（一）未来十二个月内是否有其他股权融资计划的声明

除本次发行外，公司未来十二个月将根据业务发展情况确定是否实施其他股权融资计划。若未来公司根据业务发展需要及资产负债状况需安排股权融资时，将按照相关法律法规履行相关审议程序和信息披露义务。

（二）本次发行摊薄即期回报的有关事项

根据《国务院办公厅关于进一步加强资本市场中小投资者合法权益保护工作的意见》（国办发[2013]110 号）、《国务院关于进一步促进资本市场健康发展的若干意见》（国发[2014]17 号）以及《关于首发及再融资、重大资产重组摊薄即期回报有关事项的指导意见》（证监会公告[2015]31 号）等法律、法规、规章及其他规范性文件的要求，为保障中小投资者知情权、维护中小投资者利益，公司就本次向特定对象发行股票摊薄即期回报对公司主要财务指标的影响进行了认真、审慎、客观的分析并提出了填补回报的措施，具体如下：

1、本次向特定对象发行股票摊薄即期回报对公司主要财务指标的影响

（1）主要假设和前提条件

以下假设仅为测算本次向特定对象发行股票摊薄即期回报对公司主要财务指标的影响，不代表公司对 2020 年经营情况及趋势的判断，亦不构成盈利预测。投资者不应据此进行投资决策，投资者据此进行投资决策造成损失的，公司不承担赔偿责任。

本次发行完成后，公司净资产和总股本将有一定幅度的增加。本次向特定对象发行股票摊薄即期回报对公司主要财务指标的影响的基本情况和假设前提如下：

（1）假设国内外宏观经济环境、产业政策、行业发展状况、市场情况、公司经营环境等方面没有且在可预见的未来也不会发生重大不利变化；

（2）假设本次发行于 2020 年 11 月 30 日实施完毕（前述完成时间仅用于分析本次发行摊薄即期回报对公司主要财务指标的影响，最终以深圳证券交易所审核通过并报中国证监会同意注册后实际发行完成时间为准）；

（3）在预测公司本次发行后总股本时，以本次发行前总股本 400,010,000 股为基数，仅考虑本次向特定对象发行股票的影响，不考虑其他因素（如资本公积金转增股本、股权激励、股票回购注销等）导致股本发生变化的情况，同时不考虑相关发行费用，本次向特定对象发行股票募集资金总额为 101,500.00 万元。本次发行完成后，公司总股本将由 400,010,000 股增至 440,010,000 股（上述募集资金总额、发行股份数量仅为估计值，仅用于计算本次向特定对象发行股票摊薄即期回报对主要财务指标的影响，不代表最终募集资金总额、发行股票数量；实际到账的募集资金规模将根据监管部门审核、发行认购情况以及发行费用等情况最终确定，最终发行股票数量以深圳证券交易所审核通过并报中国证监会同意注册的数量为准）；

（4）根据公司 2019 年年度报告，公司 2019 年归属于上市公司股东的净利润、扣除非经常性损益后归属于上市公司股东的净利润分别为 25,246.88 万元、23,413.35 万元。假设 2020 年全年扣除非经常性损益后净利润的增长率与净利润增长率相同。2020 年度，公司将归属于上市公司股东的净利润、扣除非经常性损益后归属于上市公司股东的净利润在 2019 年的基础上按照增长 20%、持平、减少 20%三种情况分别测算。上述测算不代表对公司 2020 年度盈利的预测，投资者不应据此进行投资决策，投资者据此进行投资决策造成损失的，公司不承担赔偿责任；

（5）未考虑本次发行募集资金到账后，对公司生产经营、财务状况（如财务费用、投资收益）等的影响；

（6）未考虑可能存在的分红情况，该假设仅用于测算本次向特定对象发行股票摊薄即期回报对公司主要财务指标的影响，实际分红情况以公司公告为准。

（2）对公司主要财务指标的影响

基于上述假设，公司测算了本次向特定对象发行股票对公司的每股收益等主要财务指标的影响，具体如下：

项目	2019 年度/年末	2020 年度	
		本次发行前	本次发行后
总股本（万股）	40,001.00	40,001.00	44,001.00

项目	2019 年度/年末	2020 年度	
		本次发行前	本次发行后
本次发行预计完成时间	2020 年 11 月 30 日		
假设情形 1：公司 2020 年度归属于上市公司股东的净利润与 2019 年度持平			
归属于上市公司股东的净利润（万元）	25,246.88	25,246.88	25,246.88
归属于上市公司股东的扣除非经常性损益后的净利润（万元）	23,413.35	23,413.35	23,413.35
基本每股收益（元/股）	0.65	0.63	0.63
稀释每股收益（元/股）	0.65	0.63	0.63
扣除非经常性损益后的基本每股收益（元/股）	0.61	0.59	0.58
扣除非经常性损益后的稀释每股收益（元/股）	0.61	0.59	0.58
假设情形 2：公司 2020 年度归属于上市公司股东的净利润较 2019 年度增长 20%			
归属于上市公司股东的净利润（万元）	25,246.88	30,296.25	30,296.25
归属于上市公司股东的扣除非经常性损益后的净利润（万元）	23,413.35	28,096.03	28,096.03
基本每股收益（元/股）	0.65	0.76	0.75
稀释每股收益（元/股）	0.65	0.76	0.75
扣除非经常性损益后的基本每股收益（元/股）	0.61	0.70	0.70
扣除非经常性损益后的稀释每股收益（元/股）	0.61	0.70	0.70
假设情形 3：公司 2020 年度归属于上市公司股东的净利润较 2019 年度减少 20%			
归属于上市公司股东的净利润（万元）	25,246.88	20,197.50	20,197.50
归属于上市公司股东的扣除非经常性损益后的净利润（万元）	23,413.35	18,730.68	18,730.68
基本每股收益（元/股）	0.65	0.50	0.50
稀释每股收益（元/股）	0.65	0.50	0.50
扣除非经常性损益后的基本每股收益（元/股）	0.61	0.47	0.46
扣除非经常性损益后的稀释每股收益（元/股）	0.61	0.47	0.46

注：基本每股收益、稀释每股收益系按照《公开发行证券的公司信息披露编报规则第 9 号—净资产收益率和每股收益的计算及披露》的规定测算。

经测算，本次发行后，公司扣除非经常性损益后的基本每股收益、稀释每股收益存在低于 2019 年的可能，本次募集资金到位当年公司的即期回报存在短期内被摊薄的风险。

2、关于摊薄即期回报的风险提示

本次向特定对象发行股票募集资金到位后，公司净资产规模和总股本相应增加，故若经营效率未能在短期内得到有效提升，在公司总股本和净资产均增加的

情况下，公司的每股收益、加权平均净资产收益率等财务指标短期内存在下降的风险。特此提醒投资者关注本次向特定对象发行股票可能摊薄每股收益的风险。

同时，在测算本次发行对即期回报的摊薄影响过程中，公司对 2020 年归属于母公司所有者的净利润的假设分析并非公司的盈利预测，为应对即期回报被摊薄风险而制定的填补回报具体措施不等于对公司未来利润做出保证，投资者不应据此进行投资决策，投资者据此进行投资决策造成损失的，公司不承担赔偿责任。提请广大投资者注意。

3、本次向特定对象发行股票的必要性和合理性

本次向特定对象发行股票的募集资金投向符合国家产业政策以及公司的战略发展规划。本次募集资金投资项目的实施，有利于提升公司整体研发实力，进一步加强公司主营业务优势，提升公司的综合竞争实力和可持续发展能力，巩固和加强公司的行业地位，符合公司及公司全体股东的利益。因此，本次募集资金投资项目具有必要性和合理性。

关于本次募集资金投资项目的必要性和合理性分析，详见本募集说明书“第三节 董事会关于本次募集资金使用的可行性分析”。

4、募集资金投资项目与公司现有业务的关系，公司从事募集资金投资项目在人员、技术、市场等方面的储备情况

（1）本次发行募集资金投资项目与公司现有业务的关系

公司主营业务为从事企业级网络通信产品的研发、生产、销售以及为用户提供相关专业服务，主要产品包括网络安全产品、应用交付产品及基础网络产品。公司提供基于创新的统一软件平台和高性能硬件平台下，以网络安全为核心，融合企业通信领域中网络安全、应用交付、基础网络各功能模块的整体解决方案。

本次向特定对象发行股票的募集资金投资项目紧密围绕公司主营业务展开，符合国家相关的产业政策以及公司整体战略发展方向，有利于公司进一步提高研发能力，提高公司测试和验证的稳定性和可靠性，强化公司主营业务的优势，提升公司的核心竞争力和可持续发展能力。本次发行不会导致公司的主营业务发生变化。

（2）公司从事募集资金投资项目在人员、技术、市场等方面的储备情况

公司本次募集资金投资项目的实施具备人员、技术、市场等方面的基础，关于本次募集资金投资项目在上述方面的储备情况分析，详见本募集说明书“第三节 董事会关于本次募集资金使用的可行性分析”。

5、公司采取的填补即期回报的具体措施

为保证本次募集资金有效使用、有效防范股东即期回报被摊薄的风险、增强对股东利益的回报，公司拟采取以下措施填补即期回报：

（1）强化对募集资金的管理，确保募集资金充分使用

本次向特定对象发行股票完成后，募集资金的到位可在一定程度上满足公司经营资金需求，提升公司研发实力、资本实力和核心竞争力。为规范募集资金的管理与使用，确保本次向特定对象发行股票募集资金专项用于募集资金投资项目，公司将按照《公司法》、《证券法》和《深圳证券交易所创业板股票上市规则》等法律、法规、规范性文件及公司章程的要求管理和使用本次募集资金，确保募集资金被存放于董事会指定的募集资金专项账户中并建立募集资金三方监管制度，合理防范募集资金使用风险，使募集资金得以充分、有效利用。

（2）全面提升公司管理水平，完善员工激励机制

本次向特定对象发行股票募集资金到位后，公司将继续围绕现有业务及产品，着力提升内部运营管理水平，进一步优化业务流程，加强对采购、生产、销售等各环节的信息化管理，持续加强市场开拓，完善投资决策程序，提升资金使用效率，加强费用控制，全面有效地控制公司的经营风险。此外，公司还将进一步完善员工薪酬和激励机制，充分挖掘员工创造力和潜在动力，引进优秀人才，进而促进公司业务发展。

（3）不断完善公司治理，为公司发展提供制度保障

公司已建立、健全了法人治理结构，有完善的股东大会、董事会、监事会和管理层的独立运行机制，设置了与公司生产经营相适应的的组织职能机构。公司已形成了一套较为合理、完整、有效的公司治理与经营管理框架。公司将继续严格遵守《公司法》、《证券法》、《上市公司治理准则》等法律、法规和规范性

文件的规定，不断完善公司治理结构，切实保护投资者尤其是中小投资者权益，为公司发展提供制度保障。

（4）严格执行公司既定的分红政策，保证公司股东的利益回报

公司现行《公司章程》中关于利润分配政策尤其是现金分红的具体条件、比例、期间间隔和股票股利分配条件的规定，符合中国证监会发布的《关于进一步落实上市公司现金分红有关事项的通知》（证监发[2012]37 号）及《上市公司监管指引第 3 号——上市公司现金分红》（中国证监会公告[2013]43 号）的要求和公司实际情况。本次向特定对象发行股票完成后，公司将按照法律法规、《公司章程》、《未来三年（2020-2022 年）股东分红回报规划》的规定，在符合利润分配条件的前提下，实施积极的利润分配政策，并注重保持连续性和稳定性，以提高公司对投资者的回报能力，切实维护投资者合法权益，并保障公司股东利益，有效降低原股东即期回报被摊薄的风险。

6、公司董事、高级管理人员对公司本次向特定对象发行股票摊薄即期回报采取填补措施的承诺

为维护公司和全体股东合法权益，提高公司未来的回报能力，并防范即期回报被摊薄的风险，公司全体董事、高级管理人员作出如下承诺：

“（一）本人承诺不无偿或以不公平条件向其他单位或者个人输送利益，也不采用其他方式损害公司利益；

（二）本人承诺对本人的职务消费行为进行约束；

（三）本人承诺不动用公司资产从事与履行职责无关的投资、消费活动；

（四）本人承诺在自身职责和权限范围内，全力促使由董事会或薪酬委员会制定的薪酬制度与公司填补回报措施的执行情况相挂钩；

（五）如未来公司实施股权激励，本人承诺在自身职责和权限范围内，全力促使公司股权激励计划的行权条件与公司填补回报措施的执行情况相挂钩；

（六）本承诺公告日后至公司本次向特定对象发行股票实施完毕前，若中国证监会作出关于填补回报措施及其承诺的其他新的监管规定，且上述承诺不能满足中国证监会该等规定时，本人承诺届时将按照中国证监会的最新规定出具补充

承诺；

（七）本人承诺切实履行公司制定的有关填补回报措施以及本人对此作出的任何有关填补回报措施的承诺，若本人违反该等承诺并给公司或者投资者造成损失的，本人愿意依法承担对公司或者投资者的补偿责任；

作为填补被摊薄即期回报措施相关责任主体之一，若违反上述承诺或拒不履行上述承诺，本人同意按照中国证监会和深圳证券交易所等证券监管机构制定或发布的有关规定、规则，对本人作出相关处罚或采取相关监管措施。”

7、公司控股股东、实际控制人对公司本次向特定对象发行股票摊薄即期回报采取填补措施的承诺

为确保公司填补回报措施能够得到切实履行，公司控股股东及实际控制人郑树生作出如下承诺：

“（一）本人承诺不无偿或以不公平条件向其他单位或者个人输送利益，也不采用其他方式损害公司利益，不越权干预公司经营管理活动；

（二）本人承诺不动用公司资产从事与履行职责无关的投资、消费活动；

（三）自本承诺出具日至公司本次向特定对象发行股票实施完毕前，若中国证监会作出关于填补回报措施及其承诺的其他新的监管规定，且上述承诺不能满足中国证监会该等规定时，本人承诺届时将按照中国证监会的最新规定出具补充承诺；

（四）本人承诺切实履行公司制定的有关填补回报措施以及本人对此作出的任何有关填补回报措施的承诺，若本人违反该等承诺并给公司或者投资者造成损失的，本人愿意依法承担对公司或者投资者的补偿责任；

作为填补回报措施相关责任主体之一，若违反上述承诺或拒不履行上述承诺，本人同意按照中国证监会和深圳证券交易所等证券监管机构制定或发布的有关规定、规则，对本人作出相关处罚或采取相关监管措施。”

（以下无正文）

（本页无正文，为《杭州迪普科技股份有限公司 2020 年度向特定对象发行股票并在创业板上市募集说明书发行人董事会声明》之盖章页）

杭州迪普科技股份有限公司

董事会

2020年10月22日