东兴证券 DONGXING SECURITIES

卫士通系列报告之二：安全可控助力央企安全运维，密码优势引领弯道超车

——卫士通（002268）深度报告

2018 年 11 月 12 日

强烈推荐/维持

卫士通 | 深度报告

报告摘要：

安全可控是我国网络基础设施可信的手段。自主是可控的有效手段，但不是唯一手段。自主可控解决了可信赖的根本问题。它是实现网络空间安全的手段，而且是捍卫者采用的唯一可信赖的手段。

央企安全可控市场空间巨大。随着网络攻击集团化专业化趋势增强，央企承载国家重要经济命脉，急需提升信息安全能力，网络安全“三同步”、检测评估、应急处置等细化要求将有效指导和规范关键信息基础设施保护实践。在两方面作用下，预计未来 1-2 年政府、电信、能源、交通、教育、医疗、工业等领域网络安全投入意愿将进一步增强，在网络威胁监测预警、网络安全态势感知、网络数据和用户信息保护、突发事件应急响应以及安全合规等方面需求迫切。

密码是网络空间的定海神针，自主可靠的密码技术是网络安全的聚点。据悉，密码法已列入国务院和全国人大 2018 年立法工作计划，合规使用密码不仅是政策和管理要求，更是法定责任。密码技术不仅是军民两用技术，也日益成为攻防双方正面交锋的利器，近年来比特币非法交易、暗网、勒索病毒等均利用加密技术实施犯罪活动。而卫士通是我国密码技术方面的龙头企业，拥有全国最多数量的密码专家，公司在密码产品多样性和密码算法高性能实现方面一直保持国内领先水平，多项商密产品达到国内首创、国际领先的水平。

网络安全行业新形势下卫士通有望受益。卫士通目前具备渠道和商业模式两方面的优势，推出行业首创的一站式央企网络安全服务解决方案，具备形成了“安全咨询、安全评估、安全建设、安全运维”为主要内容的信息系统全生命周期安全集成与服务能力。渠道方面，经过二十年的发展和布局，公司已建立起行业和区域相结合的矩阵式营销服务支撑体系，使公司具备完整的全国性本地化营销服务能力。商业模式方面，针对央企自身网络安全能力薄弱导致的网络安全能力需求，依托网络安全国家队优势，公司针对央企需求推出行业首创一站式央企网络安全服务解决方案，由单点防御向系统防御、被动防御向主动防御的转变，构建全方位的安全管控、安全防护、安全服务保障体系，构建起提升其网络安全防护水平和应对未知网络安全威胁的能力。

盈利预测与估值：结合目前宏观经济形式，央企服务业务受目前经济大环境影响较小，央企网络安全在 2017 年已经是一把手负责制，投入力度相比以前更高，且央企对网络安全从产品转向服务，卫士通为央企提供网络安全服务整机解决方案将是公司重大转折机遇，。云计算方面公司目前与阿里云合作，在云安全方面有望成为国内第一梯队；旗下三零瑞通的核心产品安全手机的

陆洲

010-66554142 luzhou@dxzq.net.cn

执业证书编号: S1480517080001

王习

010-66554034 Wangxi@dxzq.net.cn

执业证书编号: S1480518010001

研究助理：张卓琦

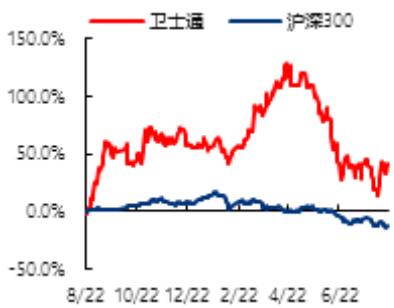
010-66554018 Zhangzq_yjs@dxzq.net.cn

执业证书编号: S1480117080010

交易数据

52 周股价区间（元）	11.00- 17.413
总市值（亿元）	243.98
流通市值（亿元）	1195
总股本/流通股（非限售）（百万股）	822.83/1689.63
流通 B 股/H 股（万股）	

52 周股价走势图



资料来源：东兴证券研究所

相关研究报告

1、《国防军工行业事件点评：混改东风一日起联通之后看军工》2017-08-16

2、《卫士通深度报告：密码资质构筑强力护城河，打造党政军综合信息安全服务商》2018-08-21

3、《卫士通深度报告：布局军用云计算，打造业务新成长极》2018-09-17

用户主要是国家涉密人员，如党政军人士等，有力保障通讯终端安全；公司以信息加密起家，母公司中国网安目前在量子加密方面走在世界前列，在数据加密方面将有力保障军队信息安全；公司所在的中电科集团中在电子干扰方面具备多年深厚背景，具备雄厚的技术积累，与卫士通共同打造军用综合信息安全体系。我们预计公司 2018 年、2019 年和 2020 年，收入分别为 27.15 亿元、52.27 亿元和 76.92 亿元，归母净利润分别为 1.60 亿元、5.47 亿元和 8.08 亿元，EPS 分别为 0.19 元、0.65 元和 0.96 元，维持公司“强烈推荐”评级。

风险提示：安全运维推广不达预期，政务云竞争激烈，5G 应用进度低于预期。

财务指标预测

指标	2016A	2017A	2018E	2019E	2020E
营业收入（百万元）	1,798.90	2,137.11	2,715.10	5,226.90	7,691.92
增长率（%）	12.21%	18.80%	27.05%	92.51%	47.16%
净利润（百万元）	155.75	169.05	160.30	547.30	807.85
增长率（%）	4.69%	8.54%	-5.18%	241.42%	47.61%
净资产收益率（%）	10.46%	3.94%	3.64%	11.44%	15.12%
每股收益(元)	0.36	0.21	0.19	0.65	0.96
PE	49.01	83.69	92.30	27.04	18.32
PB	5.13	3.44	3.36	3.09	2.77

资料来源：公司财报、东兴证券研究所

目 录

表格目录

插图目录

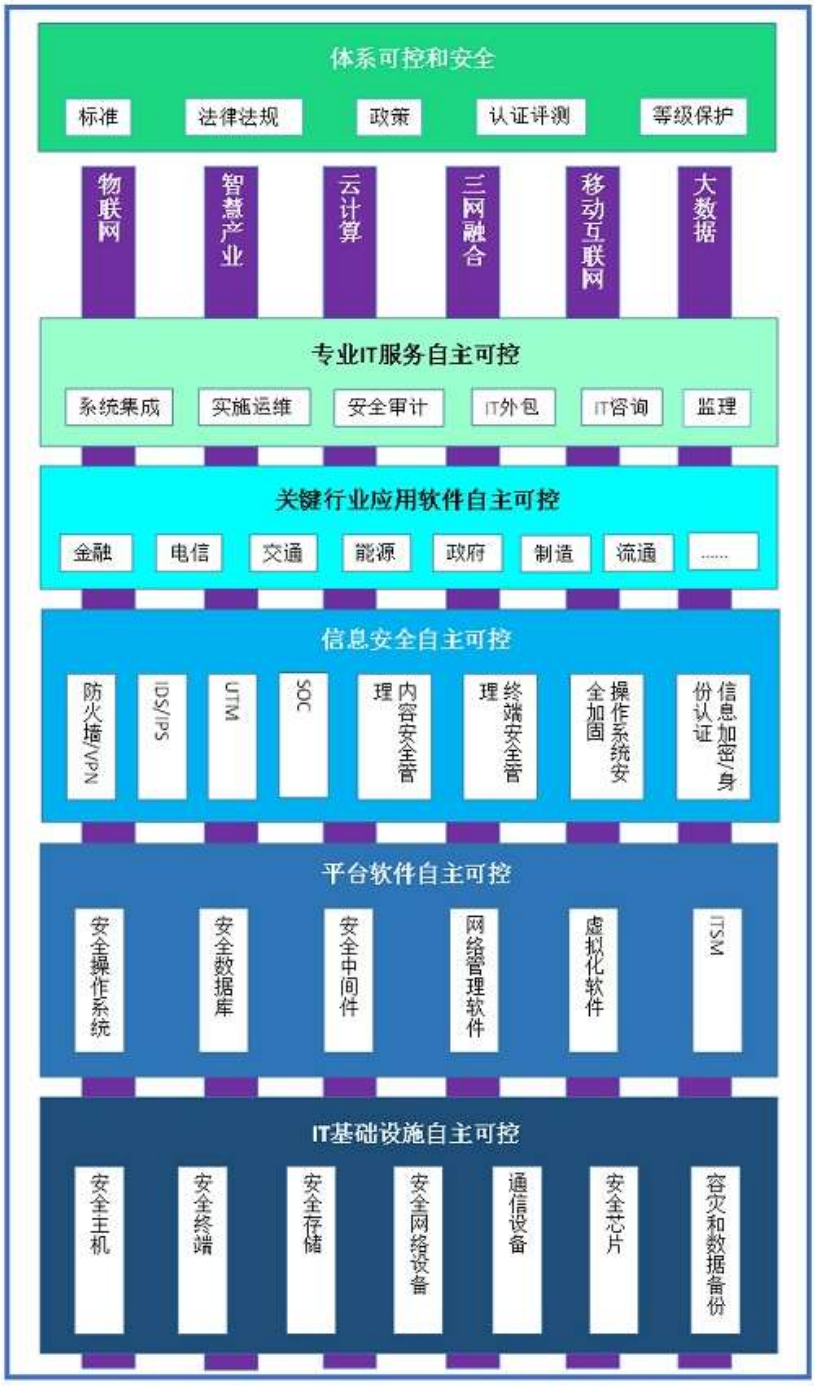
1. 安全可控是我国网络基础设施可信的手段

习近平总书记高度重视国家信息技术发展，围绕“突破互联网核心技术、实现信息技术产品安全可控”多次作出重要部署。在 2018 年 4 月召开的全国网络安全和信息化工作会议上，总书记提出，“核心技术是国之重器。要下定决心、保持恒心、找准重心，加速推动信息领域核心技术突破。要抓产业体系建设，在技术、产业、政策上共同发力。要遵循技术发展规律，做好体系化技术布局，优中选优、重点突破”。

1.1 自主可控全景图

自主可控全景图分为体系可控与安全、专业 IT 服务自主可控、关键行业应用软件自主可控、信息安全自主可控、平台软件自主可控、IT 基础设施自主可控等六部分。

图 1：中国 IT 系统自护可控全景图



资料来源：网络资料，东兴证券研究所

1.2 自主可控发展的方向就是安全可控

自主可控作为一个层面，安全可控作为另一个层面，这两个层面往往是因果关系。自主可控要事先进行评估，安全可控在应用场景里面对态势的变化，可能发生一些问题。所以要把自主可控和安全可控分开，至少在贯彻网络安全，同步推进的时候比较好操控。

自主是可控的有效手段，但不是唯一手段。自主可控只解决了可信赖的根本问题。它是实现网络空间安全的手段，而且是捍卫者采用的唯一可信赖的手段。

若把国家网络空间比喻为一座城池，产品比作守城的将领和士兵，那么自主可控产品就是守城死士，绝不会弃城而逃。但是，并不代表守城死士一定善于战斗并且确保城池安全。自主可控不代表安全能力出色，也不代表质量优良，但这恰恰是自主可控发展的方向：安全可靠。

网络空间没有绝对的安全，是因为自我安全性检测的方式、方法不全或复杂度导致不可实施，也就无法发现安全风险并修正。IT 产品的广义安全性包括环境安全性、结构安全性、信息安全保密能力等方面，可靠性指一定时间内、在一定条件下无故障地执行指定功能的能力或可能性。网络空间的构成产品“安全+可靠”是追求的目标。

当自主可控产品质量(功能性、可靠性、自身安全性等)等价于非自主可控产品质量时，一定使得网络空间更加安全可靠。因为它没有“潜伏者”。

1.3 我国信息安全可控技术政策环境良好

2014 年 2 月 27 日，中央网络安全和信息化领导小组第一次会议召开时，习近平总书记强调，网络安全和信息化对一个国家很多领域都是牵一发而动全身的，要认清我们面临的形势和任务，充分认识做好工作的重要性和紧迫性，因势而谋，应势而动，顺势而为。网络安全和信息化是一体之两翼、驱动之双轮，必须统一谋划、统一部署、统一推进、统一实施。做好网络安全和信息化工作，要处理好安全和发展的关系，做到协调一致、齐头并进，以安全保发展、以发展促安全，努力建久安之势、成长治之业。

国家加快制定出台相关法律法规，提出实现信息技术产品安全可控的明确要求。《国家安全法》第二十五条明确规定“加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控”；《网络安全法》第十六条明确要求“扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务”；《网络产品和服务安全审查办法》（试行）则明确提出是“为提高网络产品和服务安全可控水平”而制定的。

1.4 关键信息基础设施是自主安全可控重点领域

一方面，关键信息基础设施日益成为网络攻击的重点目标，安全防护能力建设需求迫切。美国防部，德核电站、印度外交部以及以色列电力局等关键信息基础设施的攻击事件层出不穷，造成严重危害后果，也为我国敲响警钟。特别是以社会工程为代表的攻击新理念，以网络武器为代表的供给新工具、以自动化为代表攻击新方式将极大改变攻防博弈格局，增强关键信息基础设施安全防护能力迫在眉睫。

网络安全“三同步”、检测评估、应急处置等细化要求将有效指导和规范关键信息基础设施保护实践。在两方面作用下，预计未来 1-2 年政府、电信、能源、交通、教育、医疗、工业等领域网络安全投入意愿将进一步增强，在网络威胁监测预警、网络安全态势感知、网络数据和用户信息保护、突发事件应急响应以及安全合规等方面需求迫切。

“金融、能源、电力、通信、交通等领域的关键信息基础设施是经济社会运行的神经

中枢，是网络安全的重中之重，也是可能遭到重点攻击的目标。‘物理隔离’防线可被跨网入侵，电力调配指令可被恶意篡改，金融交易信息可被窃取，这些都是重大风险隐患。不出问题则已，一出就可能导致交通中断、金融紊乱、电力瘫痪等问题，具有很大的破坏性和杀伤力。我们必须深入研究，采取有效措施，切实做好国家关键信息基础设施安全防护。”在2016年4月19日召开的网络安全和信息化工作座谈会上，习近平总书记对互联网管理提出明确要求。

1.5 为党政军和央企提供一站式网络安全服务解决方案

2016年3月4日，安全可靠技术和产业联盟成立。

联盟的业务工作范围是：一、开展我国安全可靠技术发展领域的战略及策略研究，支撑形成安全可靠软硬件发展的顶层设计；二、开展安全可靠关键技术、标准制定、发展路线等相关研究；三、组织开展安全可靠领域的人才培育、认证等相关工作；四、组织建立安全可靠领域的联合实验室，开展技术、产品、方案和安全等方面的技术研究工作，推进产品适配验证，系统优化改进；五、组织协调安全可靠领域的产学研用共同营造健康的安全可靠生态环境。

安全厂商（6家）包括：星网锐捷（通信、安全）、中孚信息（安全保密）、安宁创新（邮件、消息）、中安网脉（密码、存储）、海泰方圆（密码、安全）、卫士通（密码、芯片、系统）。

卫士通作为联盟成员，重点布局安全领域，并与其它自主可控公司一起打造全产业链自主可控生态体系。

卫士通公司以“密码国内第一、安全国内一流”为产品体系创新的目标，以商用密码产品为代表，研发和推出了一批在业界具有竞争力的拳头产品，其中多款产品处于国内首创、国际先进水平。为适应国家战略、技术趋势和产业形势，通过整合优势资源，重点打造了网络安全管控与态势感知、信任服务、网络安全、安全云运营平台、安全移动办公、安全终端、安全芯片、密码模块和自主可控系列产品。

公司5月份研制的中华卫士自主可控万兆交换产品，核心部件全部国产自主化，包括龙芯2H芯片、盛科交换芯片、CPLD等自主可控核心部件。

图 2：卫士通产品展示

资料来源：网络资料，东兴证券研究所

1.6 央企安全可控市场空间巨大

当前国际形势不明朗，外贸行情受影响较大，而且当前大众消费能力有所放缓，以及地方政府支出减少，相对来说央企业务稳定性强，卫士通为央企提供安全运维乃至网安飞天云等安全产品及服务，将具有相对好的安全边际。

金融、能源、电力、通信、交通等领域央企占主导地位，其关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重，关系整个国家的命脉。所以对安全要求高，也是国家重点关注领域，对国家网络安全要求执行力最强，是网安产业核心推动力。

目前卫士通已经与招商局集团、中远海运等央企已经提供安全运维整体解决方案，仅考虑到央企安全运维市场，央企共 97 家，估计每家平均 30 家分公司，每家分公司 750 万的合同额，将有 218.2 亿的市场，作为网络安全国家队，卫士通有望取得一半市场份额，也就是将近百亿级的收入级别，将极大提升公司业绩。

图 3：部分央企总人数

央企领域	数量
航空航天	10
船舶	3
能源	13
铁路	6
军工	3
通信	7
煤炭钢铁	7
石油化工	6
有色	7

电子	3
机械	3
电气	2
粮食	3
建筑	4
汽车	2
重点行业	6
其他行业	12
总计	97

资料来源：网络资料，东兴证券研究所

1.7 安全可控需要核心技术弯道超车

实现信息技术安全可控是摆脱受制于人的必由之路。2016 年 4 月 19 日，习近平总书记在网络安全和信息化工作座谈会上指出：“核心技术受制于人是我们最大的隐患。”习近平总书记多次强调，“市场换不来核心技术，有钱也买不来核心技术，必须靠自己研发、自己发展”。2018 年 4 月，美国针对中兴通讯的芯片制裁事件再次证明，核心技术受制于人存在巨大隐患，“打铁还需自身硬”。坚持关键信息技术安全可控是保证我国经济发展、社会稳定和国防安全的重要环节，是打破现有技术封锁、实现核心技术不受制于人的必要条件。

信息领域核心技术通常包括三类：一是基础技术、通用技术;二是非对称技术、“杀手锏”技术;三是前沿技术、颠覆性技术。

在自主可控的基础上，通过创新是大有前途的。现在像大数据、云计算、物联网、5G，量子计算机，特别是新一代人工智能的出现，新应用越来越多。我们在基础软硬件方面，如果能及早布局，赶上应用新浪潮，在前沿技术和颠覆性技术方面我们应该可以实现弯道超车和换道超车的。

1.8 前瞻布局，实现核心技术弯道超车---量子加密和人工智能

信息技术发展日新月异，新技术不断涌现，下一代信息技术革命已经呼之欲出。我们应着眼于未来，强化前瞻性布局，争取新一代信息技术发展的主导权。

一是扬长避短绕过技术鸿沟。针对当前互联网应用发展趋势，着力发展面向云计算、大数据和人工智能的 CPU、操作系统等核心技术，解决数据安全等关键问题，加速推进以云计算技术替代大型机的进程，避免陷入追赶西方高端芯片、大型机、高端数据库等技术路线的泥潭。

二是超前布局抢占未来先机，当前硅基信息技术已经面临发展瓶颈，我国应加强持续跟踪量子芯片、生物芯片等前沿技术发展方向，抢先布局下一代集成电路技术发展方向，抢占下一代信息技术发展至高点。

伴随人工智能技术的快速发展，国内厂商日益重视人工智能与网络安全的深度融合，积极推动机器学习、深度学习等人工智能技术在网络安全领域的落地应用，助力提升网络安全风险预测、攻击防御等全方位能力。

一方面，用户行为分析成为“人工智能+网络安全”落地的重点方向。人工智能技术

通过 IP、指纹、信誉库、历史行为等多维度关联分析，更为精准的对用户网络行为进行画像、评估风险点；应用知识图谱技术，将用户各类行为进行归类、聚合，筛选出某一共性的关联图，对未发生的威胁进行感知和预测；提供更为智能化的决策模式，突破了传统安全技术的局限。例如，腾讯利用人工智能技术强化网络运行、金融结算等特定场景中的用户行为分析，实现对恶意代码的检测与防御、网络谣言治理、有害信息鉴别等；安恒信息借助人工智能技术分析、跟踪并只能判定用户异常行为，实现对隐蔽威胁、未知攻击和 0day 攻击等网络攻击的检测和预警；观安信息基于机器学习和深度学习，通过无监督的异常检测算法对页面和用户进行快速检测，发现 Webshell、XSS 等异常页面和恶意扫描等异常行为。

图 4：AI 安全模型

资料来源：网络资料，东兴证券研究所

另一方面，人工智能技术对于数据分析实时性、准确性的提升，也激发了厂商在身份识别、数据保护等领域的应用探索。平安科技以深度学习为基础，结合数据挖掘、生物特征识别等技术，通过采集面部信息等生物特征识别用户身份；摩安科技利用机器学习算法，主动分析建立访问者信誉库，生成风险策略模型，提升对云安全威胁的感知力、防御力；墨云科技利用人工智能、机器学习等对用户数据进行持续性安全验证；赛貂腾龙利用人工智能技术，对用洗、存储和旺纳罗敏感数据进行发现、监控和保护。

整体来看，人工智能加快网络安全技术革新：

1）人工智能将加快信息和情报流动的闭环构建。

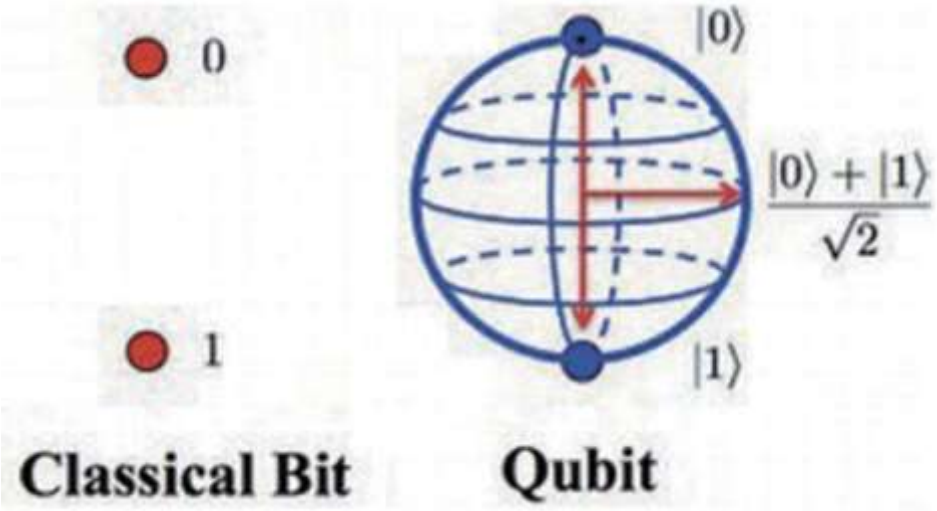
2）人工智能将推动未知威胁检测技术演进升级。

3）人工智能将推动对于复杂攻击识别由专家模型向智能模型转变。

量子计算机将引发密码革命。量子计算机利用量子特性来完成计算。由于量子叠加效应，n 比特的量子计算机可同时处于 2n 种状态，当量子计算终止时，2n 种状态因为测量而坍塌到一种确定的状态，从而完成计算。量子计算机的一次操作同时完成了对 2n 个数据的操作，相当于经典计算机完成了对 2n 个数据的并行处理。所以说，这种

叠加性让量子比特能够比比特编码处理多得多的信息，这就是量子计算机相对于经典计算机的优势。

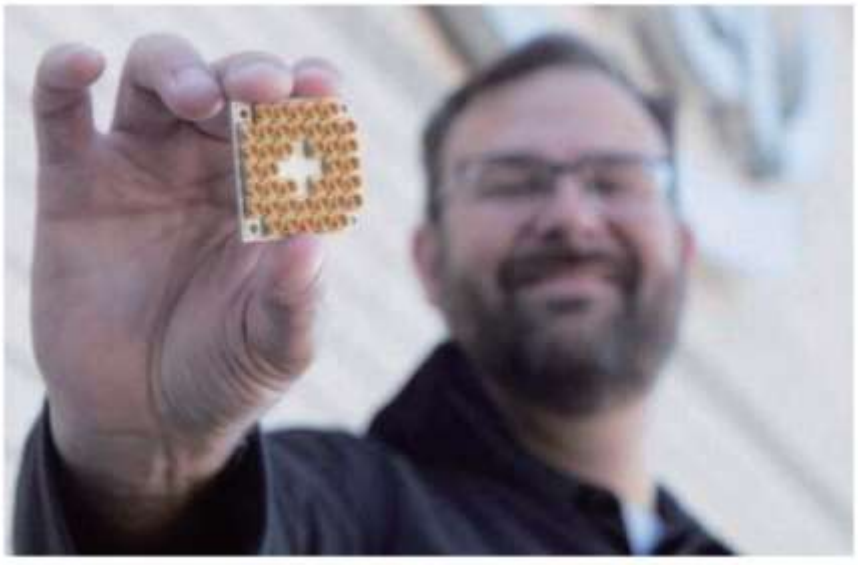
图 5：经典比特与量子比特



资料来源：网络资料，东兴证券研究所

2017 年 4 月份，Google 开发出具有 9 个量子位的计算芯片；2017 年 5 月，IBM 展示了首个包含 17 个量子位的芯片。2017 年 10 月 17 日 Intel 公司发布了包含 17 个量子位的超导测试芯片，同一天，IBM 宣布量子计算已经突破了 49 量子比特的障碍，2017 年 5 月，中国科技大学研究团队宣布通过电控可编程的光量子线路构建出可用于多光子“玻色取样”任务的光量子计算模拟机。

图 6：Intel 公司展示的 17 个量子位的超导测试芯片



资料来源：网络资料，东兴证券研究所

目前，各大科技公司的研究员都在开发包含 50 个量子位的芯片。这样的芯片计算能

力将超过当前所有超级计算机。

1994 年，Peter Shor 提出了一个能在多项式时间内分解给定整数的量子算法。这意味着，一个具有足够量子比特数的量子计算机可以破解 RSA 算法。RSA 算法是当前广泛使用的公钥密码体制之一，随着量子计算机能力的增强，此类公钥密码体制的安全性将受到严重威胁。

1.9 信息战与自主可控

实现信息技术安全可控是摆脱受制于人的必由之路。2013 年“棱镜门”事件充分体现了信息战的影响力，美国政府通过 9 家国际网络巨头对网络信息进行监控，其中美国在“棱镜门”期间利用网络信息对我国的攻击高 75%的成功率。因此我国必须重视即将展开的贸易战，以及未来有可能发生的信息战，而信息战中的关键在于自主可控。能自主可控意味着信息系统可以不断改进和修复漏洞，我国能自主控制系统安全而不被国外攻击；反之，不能自主可控，则意味着信息系统存在漏洞，受制于人，也难以对后门进行修补。自主可控要求核心技术、关键零部件、各类软件全部国产化，自己开发、自己制造。

未来战争中军队面临各方面的信息化打击，其中有几种最为致命：1. 瘫痪云基础设施；2. 通讯端泄密；3. 数据链乃至数据库遭到袭击；4. 电子干扰。任何一种打击成功，对军队的安全都将是致命的。

而卫士通作为 A 股唯一信息安全国家队，母公司中国网安目前在量子加密方面走在世界前列，在数据加密方面将有力保障军队信息安全；公司所在的中电科集团中在电子干扰方面具备多年深厚背景，具备雄厚的技术积累，与卫士通共同打造军用综合信息安全体系。

2. 密码是网络空间的定海神针，自主可靠的密码技术是网络安全的聚点

2.1 密码是网络安全的核心技术，是当前网络空间竞争的焦点

密码是网络安全基础性和核心的技术，构成网络空间安全的第一道防线，发挥着“保底”作用。这是因为不论是身份认证、信息来源认证，还是信息存储与传输安全都要用密码实现安全保护。可以说，密码技术是网络安全的基石，是信息系统内置的免疫基因，是解决网络安全最有效、最可靠、最经济的手段。

正因为如此，密码技术已成为各国在网络空间竞争的焦点。当前网络技术快速升级迭代，加快构建以密码技术为核心、多种技术相互融合、共同作用的新全安全体制，以密码基础设施为底层支撑的新安全环境，实现可信互联、开放共享的新安全文明，是网络安全面临的一项紧迫任务。

2.2 商用密码是我国自主网络安全技术的典型代表

据悉，密码法已列入国务院和全国人大 2018 年立法工作计划，合规使用密码不仅是政策和管理要求，更是法定责任。大力发展和严格管理商用密码，既是维护国家网络

安全的需要，也是保护各类经济组织的利益和安全，保护公民个人合法权益和安全的需要。

自 1999 年国务院颁布《商用密码管理条例》至今，近 20 年来我国商用密码取得了长足发展，基本形成了从密码芯片到密码服务的完全自主可控的产业链条，其种类丰富、链条完整、安全适用的商用密码产品体系和产业体系，在保障通信保密、信息和网络安全方面发挥了特殊的重要作用。

金融领域，商用密码已大规模应用于金融 IC 卡、网上银行、跨行交易等主流银行业务。93 家银行参与的密码应用示范工程，累计发行标准金融 IC 卡 2.34 亿张，完成 POS 终端升级 353 万台，ATM 机升级 58 万台，新发行网银设备 7977 万个。在重要领域，社保、能源、交通、广电、税务、公共安全等行业密码应用试点全面实施。应用商用密码的第二代居民身份证发放 15 亿张，杜绝了伪造、变造身份证违法行为；应用商用密码的智能电表超 4 亿只，输配电和调度系统全部应用商用密码，确保电网持续安全稳定运行；数字证书发放超 20 亿张，以电子认证服务体系为基础的网络信任体系逐步建立健全。中国密码“走出去”态势逐渐显现，在“一带一路”沿线国家的市场影响力和竞争力不断增强。

从发展的角度看，新型计算、网络攻防和密码技术的交替演变，一直是推进科技进步的重要因素。密码技术不仅是军民两用技术，也日益成为攻防双方正面交锋的利器，近年来比特币非法交易、暗网、勒索病毒等均利用加密技术实施犯罪活动。而卫士通是我国密码技术方面的龙头企业，拥有全国最多数量的密码专家，公司在密码产品多样性和密码算法高性能实现方面一直保持国内领先水平，多项商密产品达到国内首创、国际领先的水平。

2.2.2 卫士通走在密码算法领域最前沿，是我国密码安全自主可控主力军

在基础前沿创新方面，公司不断加大在密码算法分析与设计，量子密码、同态密码、区块链等基础和前沿技术领域的资源投入，组建专门团队，聘请外部专家，成立密码实验室，构建开放式创新平台,积极争取和承担国家科技领域重大专项、核高基项目等研究任务，牵头或深度参与国家、行业相关标准和技术规范的编写工作。

2.3 商用密码在金融领域具有非常重要的作用

信息化浪潮深刻影响着金融行业，虽然仍遵循着“客户 - 银行—清算银行—中央银行”这样多层级、中心化、相对稳定、可靠的架构。但是，随着互联网的普及、移动互联的深入应用以及大数据、云计算、物联网、区块链、人工智能等新技术的兴起和应用，给金融行业在产品服务、商业模式、经营理念带来了深刻变革和创新。

图 7：多应用安全金融信息系统框架

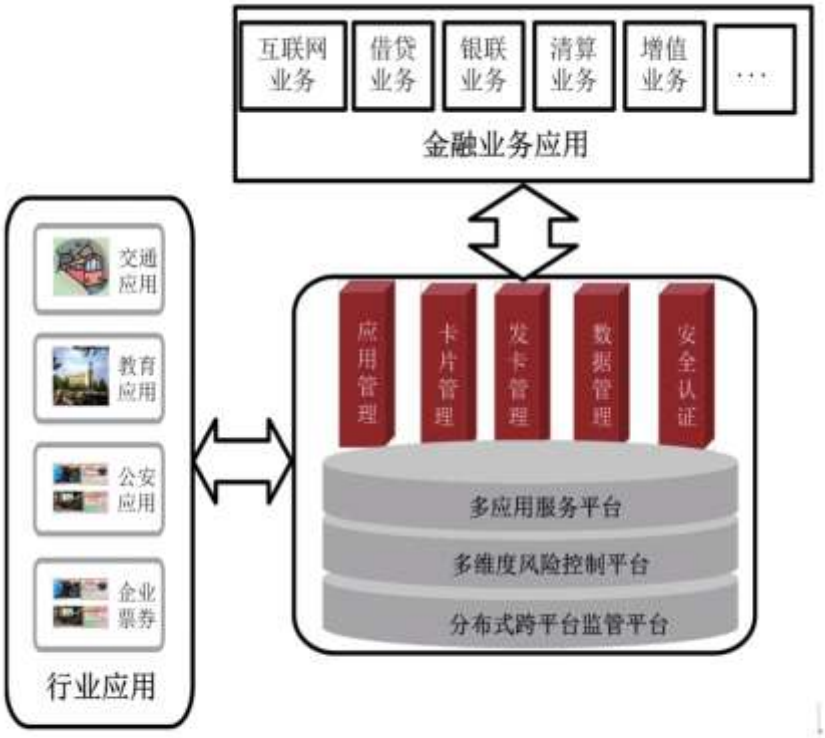


图 2 多应用安全金融信息系统框架

资料来源：网络资料，东兴证券研究所

当前出现了许多非传统的金融活动方式，如电子支付（支付宝、财付通）、互联网基金（余额宝）、P2P 等。信息化同时给金融信息安全带来了极大的威胁，APT 攻击、DNS 劫持、勒索软件、软件供应链攻击等也开始锁向金融领域，并且和传统的安全问题交织在一起，触及到了国家经济、金融安全的底线和命脉。

2.3.1 当前金融信息安全存在隐患

目前金融信息安全存在以下主要安全风险和局限性：

(1) 法律法规政策的滞后和不完善带来政策上的安全隐患；

(2) 智能移动终端的普及带来的安全新挑战；

(3) 以静态、被动防御为主，缺乏主动和弹性防御能力；缺乏多维度的风险控制和跨平台监管。

(4) 金融大数据的集中更容易成为网络攻击目标；

(5) 数据存储、骨干路由交换、主机等主要为国外产品，存在较大的被敌对势力控制和数据窃取风险；

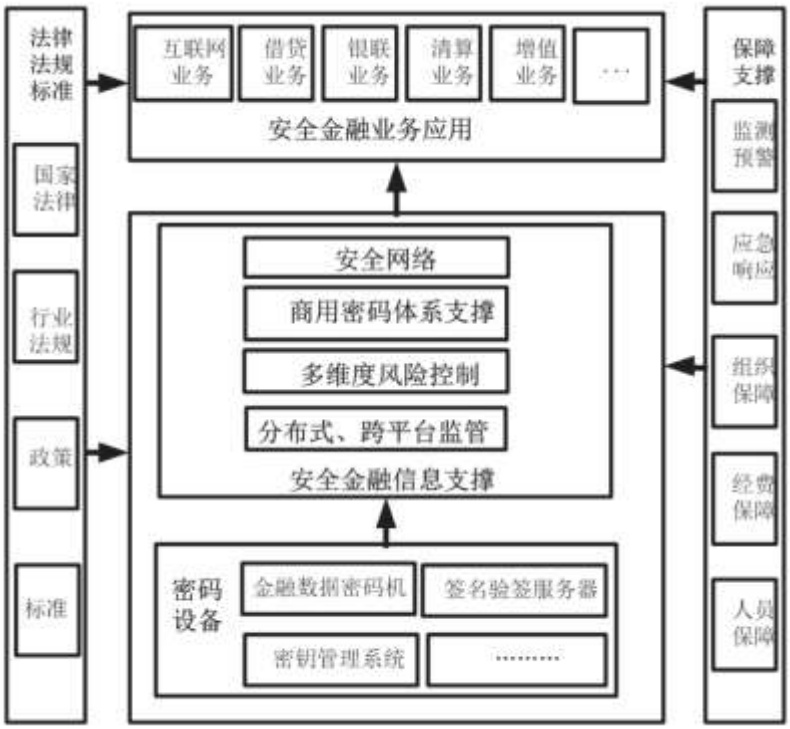
2.3.2 金融安全信息的四要素

安全金融信息四要素包括安全的网络、商用密码体系支撑、多维度风险控制和分布式、跨平台监管。

以密码设备、密码技术为基础，为安全网络、商用密码体系支撑、多维度分险控制、

分布式跨平台监管提供支撑；同时，在国家法律法规和标准的指引下，以监测预警、应急保障、组织保障等为支撑，为金融行业互联网业务、借贷业务、清算业务等应用提供安全保障。

图 8：安全金融信息密码保障框架



资料来源：网络资料，东兴证券研究所

安全网络：我国金融行业主要采用专网和一部分无线网络，其安全性占有绝对重要的地位，不安全的网络会造成金融信息被泄露、窃取等风险。

安全的网络一是要保证网络本身的安全，不存在被随意假冒、窃听的风险，即网络可信；二是网络的接入是可信的，防止不安全的接入危及网络安全。

采用可信网络和可信接入技术实现安全的网络，其核心是我国商用密码技术应用。由于金融活动的复杂性、密码技术的专业性，在金融网络安全中，怎样构建可信网络、可信接入，需要进行关键密码理论研究、技术突破、原型验证、示范应用和推广等。另外随着未来5G网络上线运营，相关5G专网通信也将需要专业的安全厂商来提供。

2.3.3 移动支付同样需要商用密码保护

目前政策和标准对于目前的互联网金融、金融科技、金融监管中的密码应用缺乏标准指导，如手机银行，在二级信息系统和三级信息系统中，终端平台安全的密码应用怎样和等级保护的具体目标有效结合？具体的有差异性的密码技术、密码算法配用、密钥管理、密码资源的管理、密码接口、密码服务、监管要求等，都需要进行细化。

智能终端应该有密码服务（或个性化密码机）、密钥管理模块、业务应用模块和个人风险控制模块（或个人风险控制器）。只有满足业务应用和个人风险控制（风险控制器）条件时，金融业务才能正常进行。

智能终端在高安全、大额度的交易应用需求中，必须采用数字签名、加密等措施，保护交易的安全性。一般性应用中，最低应该采用软密码模块（提供数字签名、加密等功能）方式，目前软密码模块遵循的主要标准是《密码模块技术要求》和《密码模块检测要求》，这两个标准是为硬件密码模块（加密卡、USBKEY）量身打造的，对于软件的密码模块，存在一些有待完善和不足的地方，软件密码模块缺乏硬件模块那样清新的安全边界，软件密码模块运行在一个不受控、不可信的环境中，采用的密钥保护措施、密码运算安全尤为重要。对于软模块中分组密码算法，一种有效的解决方法是采用白盒密码技术、辅以工程安全，如进程控制、代码混淆等。目前，对于白盒密码算法本身来说，缺乏安全标准、应用标准和检测标准。软模块中的公钥密码算法，一种是采用密钥分割的思想，即将客户端私钥分成两份，一份在客户端、一份在服务器端，通过两端的协同运算，实现客户端的签名运算。另一种可以采用基于同态密码方案，来实现客户端私钥运算的安全性。这些技术目前都没有标准化、不利于推广和应用，需要加强互联网金融终端安全密码应用、检测等标准的制定。

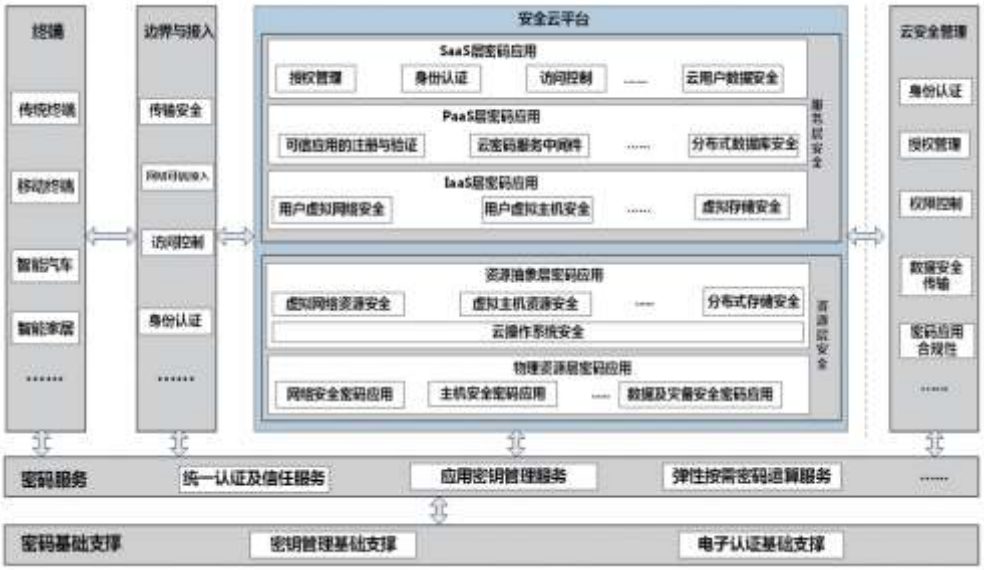
卫士通的子公司三零瑞通的核心产品加密手机的重要客户主要是国家涉密人员，如党政军人士等，拥有大约一百亿的市场空间。除党政军客户外，卫士通积极布局安全支付手机这一市场，2015 年 12 月 14 日，华为携手中国移动、卫士通在广州发布全球首款基于 VoLTE 通信加密解决方案的中国移动华为 Mate 8 VoLTE 安全手机。次年中国移动卫士通 4G VoLTE 安全手机(华为 Mate8 尊御版)”荣获“CITE2016 创新产品与应用奖”，2017 年包括与华为合作研发的 Mate 9 在内的 3 款安全手机已正式发布。

2.4 商用密码在云计算具有非常重要的作用

云计算作为信息化发展方向，为大数据应用、智能制造、人工智能、智慧城市等提供计算、网络、存储资源，已经广泛深入到我国政务、交通、能源等各个领域，出现了政务云、交通云、能源云等。云计算安全直接关系到我国关键信息基础设施的安全，因此，必须充分发挥密码在云计算安全中的核心支撑作用。

在云计算环境下，密码和云计算 IaaS 层、PaaS 层、SaaS 层中的云平台、各类云业务系统将深度融合，作为云计算中的“基因”嵌入各类云计算服务平台中，实现应用、安全、密码一体化。

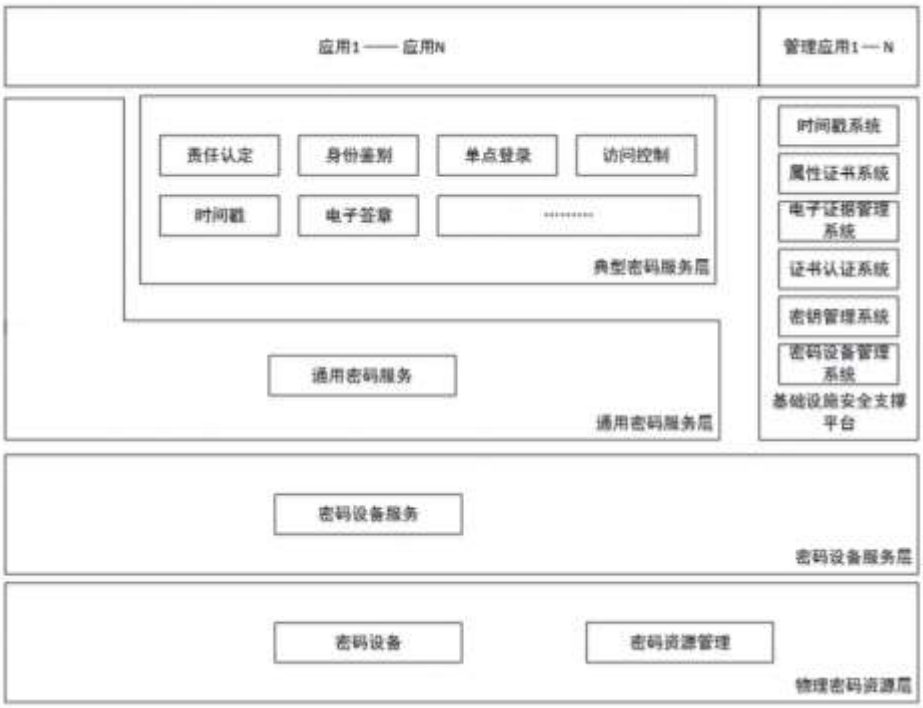
图 9：云计算密码应用体系



资料来源：网络资料，东兴证券研究所

对于云计算中计算资源虚拟化、软件自定义网络等特点，密码技术也应该从密码设备虚拟化、密码计算资源动态弹性按需调度等密码服务化方面进行适应。因此，云计算和大数据专线组成员单位共同提出了基于商用密码技术的云计算密码应用技术支撑框架，从云环境对密码技术需求角度，对云计算环境中使用的密码技术框架进行了设计。

图 10：云计算密码应用技术支撑框架



资料来源：网络资料，东兴证券研究所

该体系通过基于物理密码设备的虚拟化密码设备提供密码运算服务，通过证书认证系统、属性证书系统、时间戳系统、密钥管理系统等基础设施提供证书管理、时间戳管理和密钥管理等基础服务，以标准接口形式为应用系统提供统一的身份鉴别、单点登录、数据加解密、数字签名及验证等密码服务。

2.5 商用密码在电子政务具有非常重要的作用

财政部出台的《政务信息系统政府采购管理暂行办法》、发展改革委制定的智慧城市评价指标，切实写入了密码应用要求，实现密码应用与国家战略的融合发展，确保国家战略推进到哪里，密码就保障服务到哪里。加强密码应用与国家安全战略的统筹实施，在党政机关电子公文系统安全可靠应用、电子文件管理，以及政务信息资源共享等项目中落实密码应用要求。

2.5.1 政务云

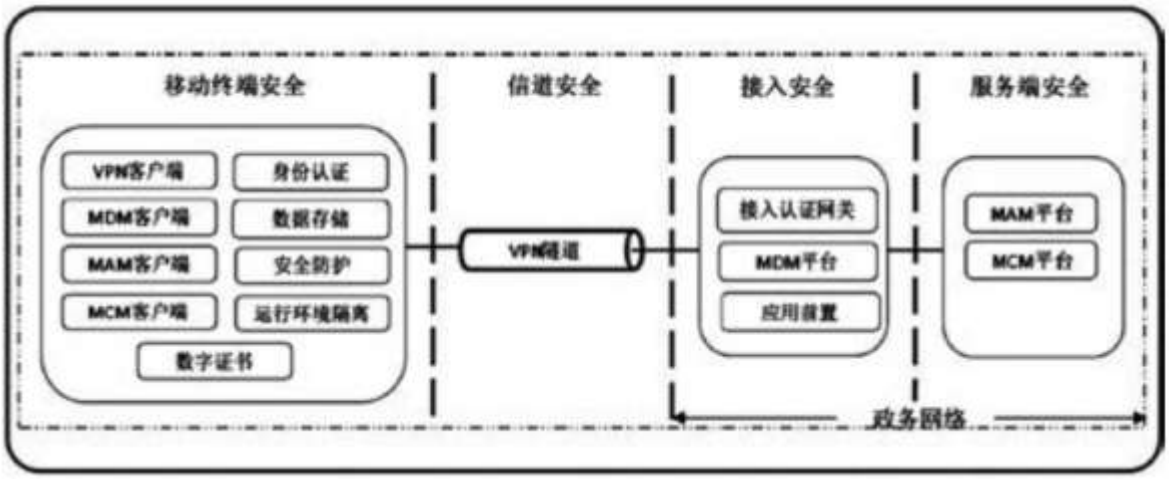
政务云安全通信网络密码应用是泛指用于保护用户与云平台之间、用户与用户之间、云平台不同数据中心之间的数据传输安全性的密码应用。

政务云业务平台密码应用应遵从《信息安全技术 网络安全等级保护基本要求 第 2 部分：云计算安全扩展要求》、《信息安全技术 网络安全等级保护安全设计技术要求 第 2 部分：云计算安全要求》及结合政务云平台的实际情况，从资源层、服务层、云业务平台密码应用（云计算环境安全）、云安全管理密码应用、政务云可信接入（区域边界）密码应用、安全通信网络、用户层安全密码应用、政务云灾备中心密码应用等几个层面分别对不同层次中的主机、网络、数据存储安全等进行考虑。
政务云中包括两种主要的应用场景，即各委办厅局接入单位终端用户密码应用、政务云同城备份中心密码应用以及政务云异地灾备中心密码应用。
1) 委办厅局接入单位终端用户密码应用：各委办厅局将业务应用迁移到政务云环境后，或各委办厅局直接访问云端统一的业务应用，均通过用户终端或瘦客户端访问政务云业务。在此种环境下其密码应用主要考虑委办厅局网络的边界安全、远程传输安全、终端保存的数据安全等。
2) 政务云同城备份中心密码应用：需要考备份中心数据和政务云交互时的远程传输安全、数据在备份中心存储时的数据保密性、完整性。
3) 政务云异地灾备中心密码应用：政务云灾备中心建设于异地，此场景下主要考灾备中心数据和政务云交互时的远程传输安全、数据在灾备中心存储时的数据保密性、完整性。
在依托商用密码支撑“互联网 + 政务服务”全面落地方面，一要依托商用密码实现民众企业可信身份的认证。民众企业网上办事最关键的就是身份可信，这直接关系到业务办理是否成功；二要依托商用密码实现个人信息的安全防护，“互联网 + 政务服务”的推进，不能以牺牲民众个人隐私为代价；三要依托商用密码实现电子材料的有效签名，民众和企业网上办事需要提交的各种文件需要确保真实性和有效性，同时要抗抵赖。

2.5.2 移动政务

移动办公人数呈现逐年增加的态势。预计到 2017 年，中国移动办公人数将达到 5 亿人，到 2018 年左右，移动办公人员的数量将与 2017 年微信用户 8.89 个亿的用户规模相当。

图 11：电子政务移动办公系统安全技术框架



资料来源：公开网络，东兴证券研究所

具有较强行业属性的政府单位，作为移动办公的重要用户，必然要考虑出台的国家相关法律法规、政策、标准和安全性保证等必要条件。另外，随着移动互联网技术日新月异的发展，移动办公的建设对于绝大多数政府用户往往是其现有信息系统的移动化改造，而非单纯的新建。

表 1：电子政务移动办公系统面临的主要安全风险

涉及对象	面临安全风险的要素	主要安全风险
移动终端	硬件、操作系统、应用软件及数据	非授权用户访问 授权用户恶意访问 恶意软件访问 互联网非授权实体的访问 移动终端丢失或被盗
通信信道	通信网络自身、信息传输过程	意外中断 传输信息被非法窃听、截获或修改 恶意攻击破坏
移动接入区	应用前置系统	非授权用户访问 授权用户恶意访问 恶意软件访问
服务端	业务应用系统和信息数据	非授权用户访问 授权用户恶意访问 恶意软件访问 信息泄露

资料来源：公开网络，东兴证券研究所

其中移动终端安全处于所有安全风险首位，必须实现芯片安全、终端操作系统安全、本地数据加密、运行环境隔离和设备防丢失、人员操作行为管控等需求；基于 TF 密

码卡和安全服务 SDK、安全沙箱、运行环境隔离和远程数据销毁等安全功能来保障移动终端的整体安全。

2.6 卫士通在密码方面的应用

卫士通在密码应用方面做了大量的研究工作，包括参与国家重大密码专项课题；组织完成海外多项应用，进行了我国商密产品应用、技术现状及存在问题的研究；开展了密码技术保障体系研究、重要信息系统领域密码保障基础设施发展规划、密码标准应用推广研究、商用密码科技创新发展战略研究等。同时，在生物识别技术如三维人脸识别技术、基于掌静脉识别积极研究密码应用的融合等密码国产软算法的替代和安全性研究。

在金融行业，以国密算法改造为切入点，积极开发满足用户需求的密码设备，在为用户提供密码产品的同时，为银行国密算法升级改造提供整体安全解决方案。

在电子政务领域，一方面以证书服务和身份认证服务为基础搭建服务于电子政务的信任服务平台，为用户提供资源管理、授权管理、可信时间等服务。另一方面，以电子文件密级标志产品为中心，围绕电子文件密标，综合终端安全产品、网络安全产品、文档安全管理产品、文档安全存储产品，打造新一代的数据安全防护体系。并且推出安全手机产品，满足政务移动安全办公需求。

在云计算领域，采用密码设备虚拟化技术，研发应用于云计算环境，能实现密码计算资源的集约利用、动态伸缩、迁移，并满足政府、企业、金融行业、云服务提供商等对于云数据加密保护、云内部安全管理、密钥管理及身份认证安全需求的云密码卡、云密码机和云密钥管理。

移动办公领域，卫士通公司按照国家等级保护 3 级规范要求及相关安全保密法规要求，研究推出了采用商密算法、商密 SSL VPN 传输技术、4A 技术、隔离交换技术、TF 密码卡安全套件技术、移动终端设备管控 MXM 技术、移动终端本地数据安全技术的高安全移动办公系统，可满足业务数据安全生命周期保护，产品从芯片到整机、到系统的一体化防护和多制式无线移动网络自适应切换等功能。

3. 网络安全行业新形势下卫士通有望受益

3.1 我国网络安全企业发展特点和趋势

1）联盟协作共同体相继成立，企业间合作紧密

从美国网络安全产业发展历史来看，美国各安全厂商通过建立联盟的形式共同推动信息安全产业发展。2011 年，美国各大信息安全厂商建立了反 APT 产业联盟，参与厂商有 Palo alto networks、Wildfire、Bit9、Virustota、Fireeye、Trustlook、VirtualThreat、Solera、Mandiant 等，形成了一个应对 APT 的产业资源体系和事实上的利益同盟。2014 年 10 月，赛门铁克、“火眼”、微软和思科等 10 家网络安全公司宣布成立联盟，共同对抗黑客攻击。

我国各 IT 大型厂商也开始推进安全联盟建设，打造协同联动的网络安全防御生态。2018 年 3UE 华为联合天融信、微步在线等厂商成立安全商业联盟，通过创新架构深度整合联盟伙伴优势产品，实现终端、网络、应用等层面协同构建全网协同立体防御

体系。8 月份腾讯携手卫士通、立思辰等 15 家上市企业，成立 P16 上市企业协作共同体，引领网络安全产业的发展和生态环境的构建。
而且云安全成为企业间合作的重点领域。浪潮与天融信、瑞星等安全企业携手共建云安全；卫士通与阿里云共同成立网安飞天安全云，结合双方优势为党政军和央企提供安全私有云服务。

2）军民融合进入深水区，军民联手维护国家网络安全

自主可控是网络安全的核心问题之一，也是军队和地方共同面临的重大挑战。集中军队和地方优势力量，加快推进自主可控事业发展，是网络安全军民深度融合的一项重点。
自 2015 年军民融合上升为国家战略以来，我国的网络安全领域军民融合路径日益明确，合作不断加深。截至目前，已有超过 30 家网络安全企业与军队有关部门开展了广泛而深入的合作，着眼军事需求打造“全自主”信息系统。我军正处在信息化建设加速发展的起始阶段，新一代指挥信息系统对自主可控的产品有着巨大的需求。

3）国家级网络安全产业园--中国电科网络信息安全产业园正加快建设

涉及网络信息安全、时频通导、电磁空间安全三个方面的中国电科网络信息安全产业园正在如火如荼建设中，该项目计划今年完成一批次主体工程建设，并启动二批次工程建设。据了解，这也是中国首个网络信息安全产业园，已被列入省“十三五”期间十大军民融合产业基地。

图 12：中电科成都网络信息安全产业园奠基仪式

资料来源：公开网络，东兴证券研究所

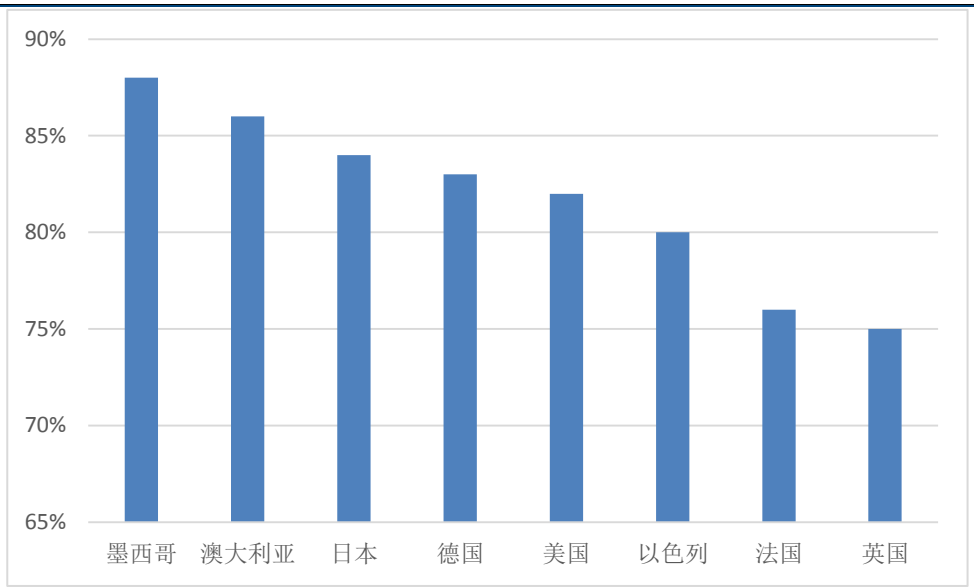
中国电科（成都）网络信息安全产业园已经于 2018 年 4 月获得增资，目前总投资将超过 500 亿元，增资将有助于进一步为大数据安全、云安全等新兴产业发展提供保障，同时加强网络安全产业合作。

3.2 人才仍旧是网络安全领域的核心竞争力

3.2.1 网络安全岗位需求快速增长，呈现全球范围短缺局面

从全球来看，网络安全岗位需求快速增加，人才短缺形势日益突出。国际咨询机构预测，2019 你网络安全岗位缺口将在 100-200 万，而到 2021 年缺口将达到 350 万。网络安全岗位需求增长加剧了网络安全人才短缺的趋势。针对信息领域调研显示，墨西哥、澳大利亚等国家 88%受访企业存在网络安全人才短缺，而美国、日本、法国等其他六个国家也均不低于 75%。在全球市场供不应求的环境下，围绕网络安全人才争夺将更趋全球化、白热化。

图 13：国际主要国家网络安全人才短缺程度



资料来源：信通院，东兴证券研究所

而且目前缺少的人才能力上，网络安全技术能力相较管理能力更难获取和提升，特别以入侵检测和安全软件开发技能最为稀缺，技术能力较管理能力更受重视。

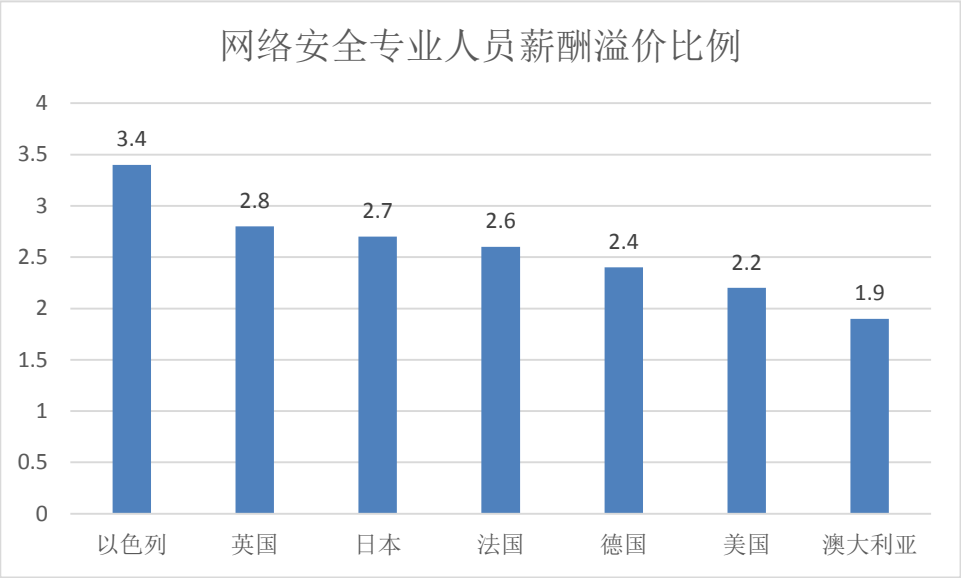
根据对美国、日本、英国、以色列等 8 个国家调查显示，入侵检测和安全软甲开发的技能最为稀缺，其中入侵检测平均稀缺程度达到了 75.8%，其次是安全软件开发 72.3%。综合来看，以入侵检测、软件开发、编程能力等技术能力相较于团队建设、沟通、协作等管理能力更加缺乏。这一方面表明技术能力是网络安全对抗的核心因素，掌握网络安全技能的从业人员更是行业稀缺资源，另一方面也揭示网络安全技术能力相较于管理能力更难与获取和提升。

3.2.2 网络安全从业人员薪酬持续走高，达平均工资 2.7 倍

网络安全人才的全球性大幅度短缺引发了网络安全职位薪酬的快速提升。根据 Robert

Walters 调查显示，2018 按网络安全从业人员薪资涨幅将达到 7%。同时网络安全岗位薪资水平远超其他 IT 岗位。根据对美国、日本、英国、以色列等 8 个国家调查显示，网络安全从业人员薪资约为企业平均工资的 2.7 倍。例如，美国网络安全从业人员薪资水平较其他 IT 岗位高出 6500 美元，溢价 9%，薪酬最高的岗位是网络安全架构师，年薪高达 23.3 万美元，高于首席信息安全官（CISO），这也侧面印证了网络安全技术能力相对管理更加稀缺。

图 14：网络安全专业人员的薪酬比例



资料来源：信通院，东兴证券研究所

3.2.3 网络安全人才培养进入深水区

1）美国：加大网络安全人才培养投入

美国国家标准与技术局（NIST）调查显示，美国网络安全职位缺口将近 35 万，政府担忧由于私营部门的网络安全人员待遇较高，会使得许多政府的高技能网络防御人才转向私营部门。为此美国政府在 2017 年投入 6200 万美元用于招聘和留住网络安全人才。该预算还被用来扩大 CyberCorps 计划，包括：为希望将来在政府部门从事网络安全工作的美国人，提供网络安全培训与奖金；为学术机构制定网络安全核心课程；加强国家网络安全中心提供网络安全解决方案的能力；为加入联邦政府的网络安全专家提供免息贷款；通过“全民计算机科学行动计划”等项目为网络安全教育提供投资。

2）英国：加强青少年和女性网络安全从业者培养

2017 年 2UE 由政府通信总部（GCHQ）组建的国家网络安全中心（NCSC）是英国网络安全人才培养工作牵头部门，该部门高度重视网络安全领域人才队伍建设，特别是注重对青少年和女性两个群体的发掘和培养。针对青少年启动网络学校计划，将投资 2000 万英镑选取青少年参与网络安全课程，计划 2021 年前培养至少 5700 名网络

安全人才。对于女性，该中心组织了 Cyber First Girls 比赛来选取女性人才，并为重返网络安全技术职位的女性提供生活保障。

3）中国：多渠道促进网络安全人才队伍建设

我国网络信息安全领域的核心技术水平与发达国家有一定的差距，关键在于高层次人才的稀缺。据不完全统计，截至 2014 年底，我国重要行业信息系统和信息基础设施对各类网络空间安全人才的需求为 70 万，预计到 2020 年对各类网络空间安全人才的需求将在 140 万人左右，而目前我国高等学校每年培养的信息安全相关人才不足 1.5 万人，远远无法满足网络空间安全的人才缺口。

自《关于加强网络安全学科建设和人才培养的意见》发布以来，各地政府积极响应，纷纷出台网络安全人才队伍建设文件，并且在各地举办多种网络安全竞赛以发掘网络安全人才。

一是武汉政府出台《关于支持国家网络安全人才与创新基地发展若干政策的通知》，文件对人才安居政策、生活住房补贴和建立人才奖励机制等方面做出明确规定，着力引进、培养网络安全领域高层次人才和团队。

二是成都市政府先后出台包括《信息安全专项资金补贴》在内的 10 余项网络安全人才培养支持政策，并与四川大学、电子科技大学、中国网安等知名校企合作开展复合型网络安全人才培养计划，增强网络安全科研人才队伍力量。

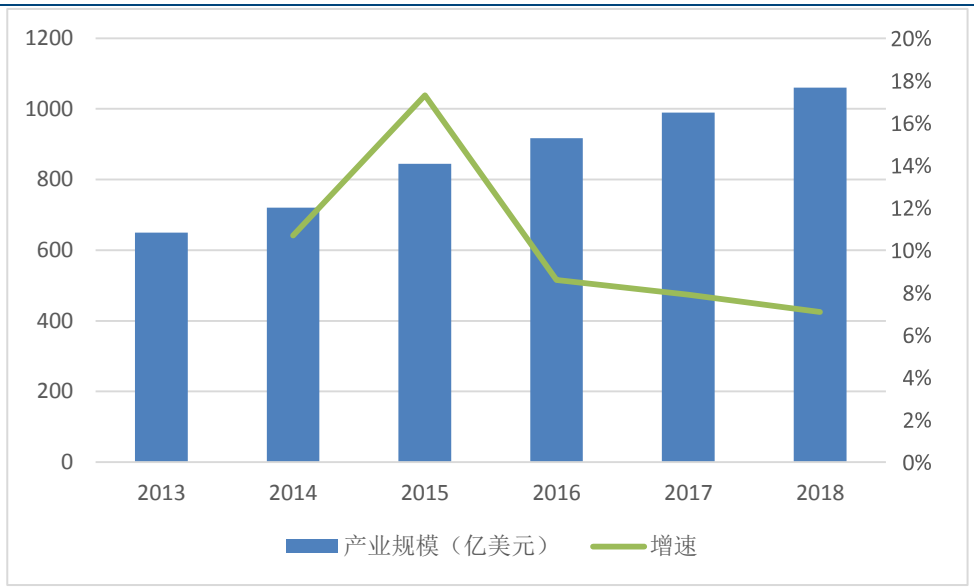
未来安全能力的输出方式很可能是“安全能力输出平台”+“专家型安全服务团队”的组合。卫士通公司非常重视高素质网络安全人才的培养和引进，确立了人才优先的发展战略，不断通过与高校合作、成立研究机构等形式，大力建设卫士通公司的网络安全人才队伍。目前公司技术人员占比超过 66%，拥有近百位研究员、高工、博士等信息安全领域专家，具有多年的信息安全系统软硬件技术开发经验。此外，公司是国家定点“博士后流动工作站”，并与国内知名高校长期合作，通过“客座教授”与硕士/博士生兼职实习等合作机制，从源头保证高端技术人才的持续输入。通过人才培养、行业合作，建立了快速将技术产品市场化的产学研一体化的可持续发展模式。

3.3 国际网络安全产业稳步增长，安全运维增长迅速

3.3.1 全球网络安全产业规模稳步增长

2017 年全球网络安全产业规模达到 989.86 亿美元，较 2016 年增长 7.9%，预计 2018 增长至 1060 亿美元。从增速来看，全球安全产业增速在 2015 年达到历史高位 17.3%，随后回落至逐年 8%的增长水平。

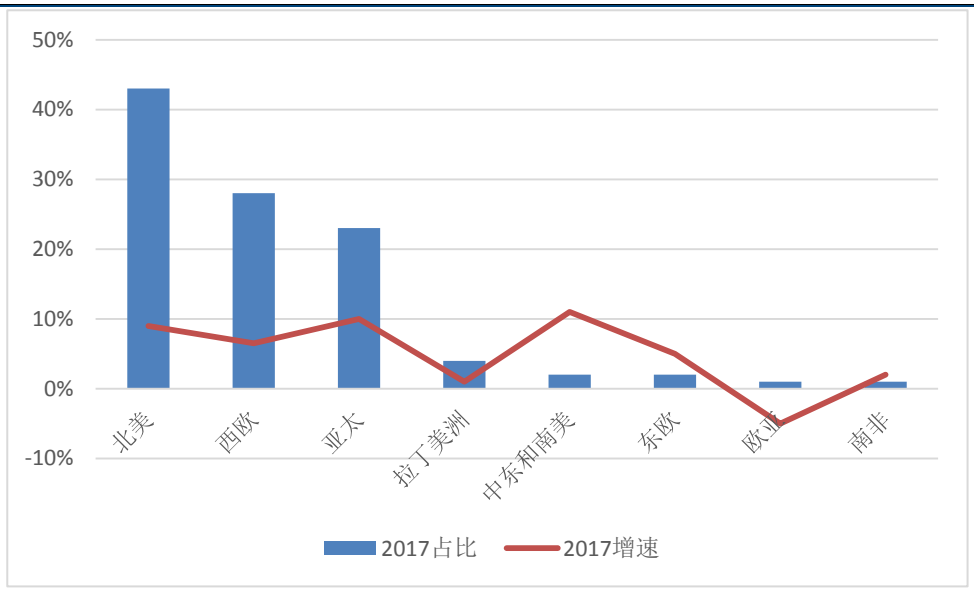
图 15：2013-2018 年全球安全产业增长情况



资料来源：信通院，东兴证券研究所

区域分布方面北美地区全球主导地位巩固，西欧地区保持稳定增长，规模位列全球第二，亚洲地区增速领先，规模位列第三。

图 16：全球安全产业区域分布和增长情况

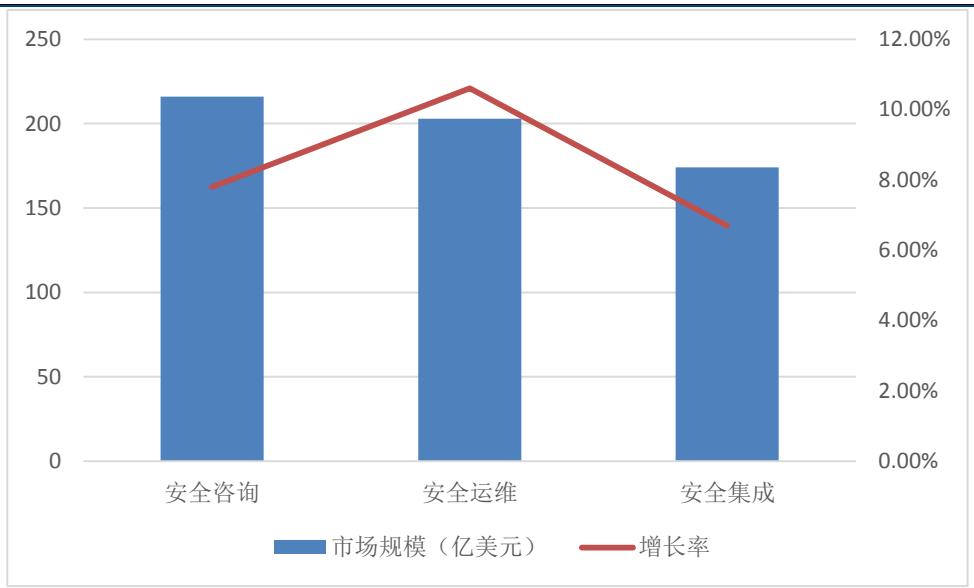


资料来源：信通院，东兴证券研究所

3.3.2 安全服务与产品市场格局总体稳定

安全服务市场与安全产品市场继续保持六四分格局，安全服务增长速度略占优势。2017 按安全服务市场规模达到 592 亿美元，较 2016lan 增长 8.3%。其中安全咨询、安全运维、安全集成三个细分市场份额分别为：21.8%、20.4%、17.6%。

图 17：安全服务产业市场规模和增长率



资料来源：信通院，东兴证券研究所

安全咨询服务市场规模达到 216 亿美元，相比 2016 年增长 7.8%。安全咨询服务将面向行业纵深发展，以行业特点为核心，从技术、运维、管理、策略等方面剔除更为针对性的安全技术与管理咨询服务，满足多样化的咨询服务需求。安全运维服务市场规模达到 203 美元，相比 2016 年增长 10.6%，成为安全服务产业的重要增长引擎。

从全球范围来看，安全运维服务发展迅速，全球已有超过 2 万家在行业领军企业和政府机构正在使用安全运维管理服务，特别是北美、欧洲等发达地区，安全运维服务市场已较为成熟。随着安全人才技能短缺、技术复杂性和威胁形势持续加深，安全运维服务市场规模增长有望持续。

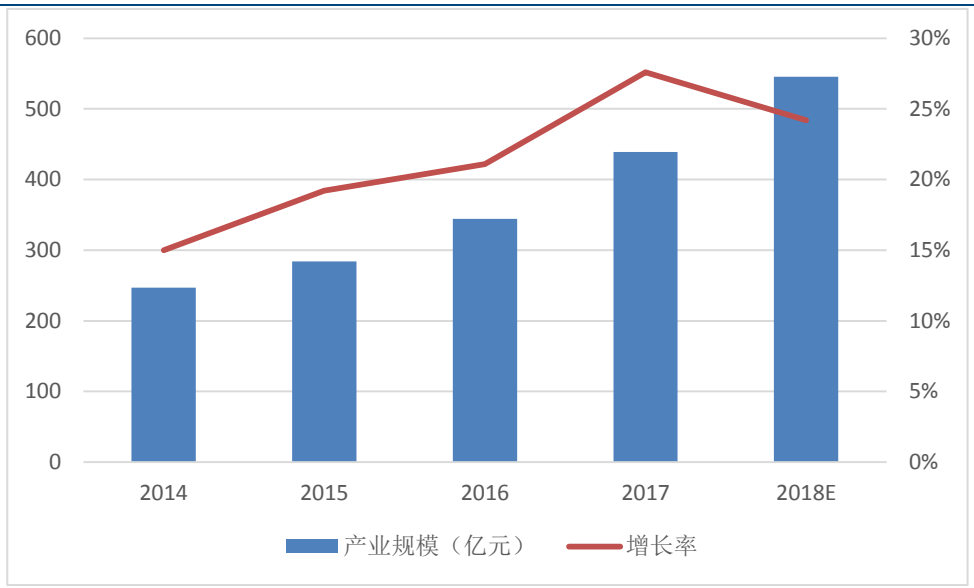
安全集成服务市场规模达到 174 亿美元，相比 2016 年增长 6.7%。美国、日本、欧盟占据了全球安全集成服务 80%的市场份额。

3.4 我国网络安全产业增速高于全球

我国网信工作持续发力，为网络安全技术创新、网络安全企业做大做强提供了宝贵机遇，也为网络安全产业发展创造了更为优越的政策环境，国内网络安全产业进入发展黄金期，近三年来产业增长率不断走高，产业规模迅速扩大。

根据中国信通院统计测算，2017 年我国网络安全产业规模达到 439.2 亿元，较 2016 年增长 27.6%，预计 2018 年达到 545.49 亿元。

图 18：我国网络安全产业规模增长情况



资料来源：信通院，东兴证券研究所

3.5 细分领域助力网络安全服务市场打开新局面

国际上安全服务连续多年占据安全市场的六成份额，而我国服务市场占比不足三成，“重产品轻服务”“劣币驱逐良币”等问题凸出，安全服务市场发展缓慢且艰难。近年来，随着网络安全事件频发和政策标准落地，应急服务、合规服务等服务市场发展态势逐步向好，为提升安全服务的价值认知、开辟服务市场空间起到一定助益作用。

1）事件调查、应急响应、溯源处置等服务推动对安全服务价值的认可。攻防是长期持续性对抗，本质是人与人之间的较量。在网络安全事件调查、应急处置等服务中，服务人员长期从事网络安全工作积累的对安全威胁的敏锐发现能力、对安全情报的分析利用能力、对安全事件的快速响应能力得以充分体现。从而让企业在解决燃眉之急的同时，更加认可安全服务的价值和采购安全服务的必要性。

2）合规性检查服务需求日益增多。等保 2.0 系列标准推动《网络安全法》中对于等级保护要求落地，企业自查和合规需求逐渐增多，合规性检查服务日渐兴起。有关行业组织、联盟等加大对检查服务机构、人员的管理，网络安全服务市场行为逐渐走向规范。

3.6 卫士通提供的一站式央企网络安全服务解决方案优势尽显

从国外安全服务市场市场规模超过安全产品，达 592 亿美元规模，而我国网络安全产业结构以安全产品为主，安全服务未来空间广阔。且目前国内安全服务领域有两个特点：

1）相对“远程服务”，国内更青睐“驻场运维”模式。目前大部分网络安全专业厂商均具备 7*24 小时运营中心，提供网络威胁检测、分析、响应、处置等能力，但主要为相应安全产品的增值性服务，以及提供威胁情报等。相对于国外安全产品、服务一揽子外包服务，国内市场普遍倾向于本地驻场的安全运维模式，依靠本地的安全网络

管理平台等产品和驻场运维人员，实现对本地网络设备、网络安全设备流量和日志的采集处理、深度分析和事件处置。

2）具备渠道优势的网络运营商提供的服务类型、服务深度仍有待拓展。例如中国电信推出的云堤高防是行业内标杆型产品，目前提供5000G运营商级DDoS防御能力，但除了高防产品外，电信的可管理安全服务仅仅覆盖反钓鱼、DNS 域名安全和 Web 网站安全等领域，服务类型有待进一步拓展。此外尚未推出类似国外安全运营中心提供的一体化的、基于用户侧网络设备和安全设备的安全运维模式，服务模式有待进一步创新。

而卫士通目前具备渠道和商业模式两方面的优势，推出行业首创的一站式央企网络安全服务解决方案，具备形成了“安全咨询、安全评估、安全建设、安全运维”为主要内容的信息系统全生命周期安全集成与服务能力。

渠道方面，经过二十年的发展和布局，公司已建立起行业和区域相结合的矩阵式营销服务支撑体系，通过北京、成都双总部，北方、西南、西北、华东、华南、四川六大区域营销服务中心，以及下设的 20 余个分公司、办事处和政府、金融、能源、央企、移动互联网等多个行业营销部门，向全国辐射建立了密集的销售和服务网络，使公司具备完整的全国性本地化营销服务能力。

商业模式方面，针对央企自身网络安全能力薄弱导致的网络安全能力需求，依托网络安全国家队优势，公司针对央企需求推出行业首创一站式央企网络安全服务解决方案，由单点防御向系统防御、被动防御向主动防御的转变，构建全方位的安全管控、安全防护、安全服务保障体系，构建起提升其网络安全防护水平和应对未知网络安全威胁的能力。

4. 盈利预测及估值

我们预计公司 2018 年、2019 年和 2020 年，收入分别为 27.15 亿元、52.27 亿元和 76.92 亿元，归母净利润分别为 1.60 亿元、5.47 亿元和 8.08 亿元，EPS 分别为 0.19 元、0.65 元和 0.96 元，维持公司“强烈推荐”评级。

5. 风险提示

安全运维推广不达预期，政务云竞争激烈，5G 应用进度低于预期。

表 2：公司盈利预测表

资产负债表				单位:百万元		利润表				单位:百万元	
	2016A	2017A	2018E	2019E	2020E		2016A	2017A	2018E	2019E	2020E
流动资产合计	2140	4067	5156	9778	14339	**营业收入**	1799	2137	2715	5227	7692
货币资金	524	1881	2389	4600	6769	**营业成本**	1165	1383	1776	3054	4393
应收账款	1088	1616	2053	3953	5817	营业税金及附加	15	20	9	17	25
其他应收款	59	67	85	163	240	营业费用	177	215	285	549	808
预付款项	55	68	85	114	156	管理费用	271	330	421	810	1192
存货	193	211	271	466	670	财务费用	6	-12	-9	80	232
其他流动资产	29	25	20	-5	-29	资产减值损失	47.47	74.60	74.60	74.60	74.60
非流动资产合计	1509	1686	1464	1300	1137	公允价值变动收益	0.00	0.00	0.00	0.00	0.00
长期股权投资	25	27	27	27	27	投资净收益	1.87	1.80	1.80	1.80	1.80
固定资产	268.05	265.66	1270.43	1113.41	956.39	**营业利润**	120	153	161	644	970
无形资产	10	71	63	57	51	营业外收入	76.69	50.75	50.75	50.75	50.75
其他非流动资产	0	55	55	55	55	营业外支出	0.16	0.74	0.74	0.74	0.74
资产总计	3649	5754	6620	11078	15477	**利润总额**	196	203	211	694	1020
流动负债合计	2026	1309	2057	6128	9961	所得税	23	26	42	139	204
短期借款	829	0	398	3440	6174	**净利润**	173	177	169	556	816
应付账款	759	980	1242	2136	3072	少数股东损益	17	8	8	8	8
预收款项	40	60	84	131	201	归属母公司净利润	156	169	160	547	808
一年内到期的非	0	0	0	0	0	EBITDA	161	238	315	888	1364
非流动负债合计	50	57	57	57	57	**EPS（元）**	0.36	0.21	0.19	0.65	0.96
长期借款	0	0	0	0	0	**主要财务比率**					
应付债券	0	0	0	0	0		2016A	2017A	2018E	2019E	2020E
负债合计	2077	1366	2113	6185	10018	**成长能力**					
少数股东权益	84	92	100	108	117	营业收入增长	12.21%	18.80%	27.05%	92.51%	47.16%
实收资本（或股	433	838	838	838	838	营业利润增长	-9.33%	28.11%	4.89%	301.18%	50.54%
资本公积	300	2558	2558	2558	2558	归属于母公司净利润	4.69%	8.54%	-5.18%	241.42%	47.61%
未分配利润	708	848	910	1121	1432	**获利能力**					
归属母公司股东	1489	4296	4406	4784	5342	毛利率(%)	34.57%	41.58%	42.89%	42.30%	43.14%
负债和所有者权	3649	5754	6620	11078	15477	净利率(%)	9.61%	8.29%	6.21%	10.63%	10.61%
现金流量表				单位:百万元		总资产净利润（%）		4.27%	2.94%	2.42%	4.94%
	2016A	2017A	2018E	2019E	2020E	ROE(%)	10.46%	3.94%	3.64%	11.44%	15.12%
经营活动现金流	-137	-51	165	-509	-10	**偿债能力**					
净利润	173	177	169	556	816	资产负债率(%)	57%	24%	32%	56%	65%
折旧摊销	35.55	97.30	0.00	157.02	157.02	流动比率	1.06	3.11	2.51	1.60	1.44
财务费用	6	-12	-9	80	232	速动比率	0.96	2.95	2.38	1.52	1.37
应收账款减少	0	0	-437	-1899	-1864	**营运能力**					
预收帐款增加	0	0	24	47	69	总资产周转率	0.57	0.45	0.44	0.59	0.58
投资活动现金流	-634	-181	-14	-73	-73	应收账款周转率	2	2	1	2	2
公允价值变动收	0	0	0	0	0	应付账款周转率	2.59	2.46	2.44	3.09	2.95
长期股权投资减	0	0	0	0	0	**每股指标（元）**					
投资收益	2	2	2	2	2	每股收益(最新摊薄)	0.36	0.21	0.19	0.65	0.96
筹资活动现金流	733	1579	358	2793	2252	每股净现金流(最新	-0.09	1.61	0.61	2.64	2.59
应付债券增加	0	0	0	0	0	每股净资产(最新摊	3.44	5.12	5.26	5.71	6.37
长期借款增加	0	0	0	0	0	**估值比率**					
普通股增加	0	406	0	0	0	P/E	49.01	83.69	92.30	27.04	18.32
资本公积增加	6	2258	0	0	0	P/B	5.13	3.44	3.36	3.09	2.77
现金净增加额	-38	1347	509	2210	2169	EV/EBITDA	49.42	54.21	40.62	15.36	10.41

资料来源：东兴证券研究所

分析师简介

陆洲

北京大学硕士，军工行业首席分析师。曾任中国证券报记者，历任光大证券、平安证券、国金证券研究所军工行业首席分析师，华商基金研究部工业品研究组组长，2017 年加盟东兴证券研究所。

王习

香港理工大学硕士，四年证券从业经验，曾任职于中航证券，长城证券，2017 年加入东兴证券军工组。

研究助理简介

张卓琦

清华大学工业工程博士，3 年大型国有军工企业运营管理培训、咨询经验，2017 年加盟东兴证券研究所，关注新三板、军工领域。

分析师承诺

负责本研究报告全部或部分内容的每一位证券分析师，在此申明，本报告的观点、逻辑和论据均为分析师本人研究成果，引用的相关信息和文字均已注明出处。本报告依据公开的信息来源，力求清晰、准确地反映分析师本人的研究观点。本人薪酬的任何部分过去不曾与、现在不与，未来也将不会与本报告中的具体推荐或观点直接或间接相关。

风险提示

本证券研究报告所载的信息、观点、结论等内容仅供投资者决策参考。在任何情况下，本公司证券研究报告均不构成对任何机构和个人的投资建议，市场有险，投资者在决定投资前，务必要审慎。投资者应自主作出投资决策，自行承担投资风险。

免责声明

本研究报告由东兴证券股份有限公司研究所撰写，东兴证券股份有限公司是具有合法证券投资咨询业务资格的机构。本研究报告中所引用信息均来源于公开资料，我公司对这些信息的准确性和完整性不作任何保证，也不保证所包含的信息和建议不会发生任何变更。我们已力求报告内容的客观、公正，但文中的观点、结论和建议仅供参考，报告中的信息或意见并不构成所述证券的买卖出价或征价，投资者据此做出的任何投资决策与本公司和作者无关。

我公司及其所属关联机构可能会持有报告中提到的公司所发行的证券头寸并进行交易，也可能为这些公司提供或者争取提供投资银行、财务顾问或者金融产品等相关服务。本报告版权仅为我公司所有，未经书面许可，任何机构和个人不得以任何形式翻版、复制和发布。如引用、刊发，需注明出处为东兴证券研究所，且不得对本报告进行有悖原意的引用、删节和修改。

本研究报告仅供东兴证券股份有限公司客户和经本公司授权刊载机构的客户使用，未经授权私自刊载研究报告的机构以及其阅读和使用者应慎重使用报告、防止被误导，本公司不承担由于非授权机构私自刊发和非授权客户使用该报告所产生的相关风险和责任。

行业评级体系

公司投资评级（以沪深 300 指数为基准指数）：

以报告日后的 6 个月内，公司股价相对于同期市场基准指数的表现为标准定义：

强烈推荐：相对强于市场基准指数收益率 15％以上；

推荐：相对强于市场基准指数收益率 5％～15％之间；

中性：相对于市场基准指数收益率介于-5％～+5％之间；

回避：相对弱于市场基准指数收益率 5％以上。

行业投资评级（以沪深 300 指数为基准指数）：

以报告日后的 6 个月内，行业指数相对于同期市场基准指数的表现为标准定义：

看好：相对强于市场基准指数收益率 5％以上；

中性：相对于市场基准指数收益率介于-5％～+5％之间；

看淡：相对弱于市场基准指数收益率 5％以上。