卫士通(002268)

网络安全国家旗舰，腾飞在即

买入(维持)

2017 年 09 月 13 日

盈利预测与估值	2016	2017E	2018E	2019E
营业收入（百万元）	1,799	2,496	3,543	5,127
同比（%）	12.2%	38.7%	42.0%	44.7%
净利润（百万元）	155.75	204.88	299.98	418.48
同比（%）	4.7%	31.5%	46.4%	39.5%
毛利率（%）	34.4%	32.5%	32.9%	32.3%
ROE（%）	10.5%	4.7%	6.4%	8.3%
每股收益（元）	0.36	0.24	0.36	0.50
P/E	58	91	61	44
P/B	6	4	4	4

投资要点

■ **网络空间成为新战场，卫士通作为中国网安上市平台持续整合打造完整产业链：**美国网军不断升级，网络空间成为国家间新的战场，中国电科顺应时代潮流组建专业网络安全子集团，卫士通成为网安子集团的上市平台。此前集团已将三十所旗下的三家公司注入卫士通，为公司的战略整合指明发展方向。未来在电科集团资产证券化比例提升的趋势下，我们预计卫士通有望进一步通过整合完善产业链布局，打造网安旗舰上市平台。

■ **安全服务模式转型大步推进，市场份额有望提升：**大数据分析、云模式以及需求升级的三重推动，网安行业有望从当前的产品采购模式逐步向安全运维模式过渡，高壁垒决定了行业竞争格局走向集中。目前国内央企有 98 家，假定一家央企的网安运维平均投入 1 亿/年，则仅央企范围的安全运维市场可达 100 亿。若加上成规模的地方国企，则市场保守估计可达 200 亿。目前中国网安已签订远洋海运等标杆客户，全年有望突破 10 家。

■ **电子政务内网需求有望拉动加密业务快速发展：**国务院办公厅印发的《政务信息系统整合共享实施方案》提出 2018 年 6 月底前，实现国务院各部门整合后的政务系统统一接入国家数据共享交换平台。电子政务内网建设市场可达百亿级别，我们预计省级招标今年有望启动，涉密网对厂商资质要求较高，卫士通作为专业加密龙头有望获得较大份额。

■ **安全手机标准已经立项，放量可期：**8 月底中国手机网络安全高峰论坛上，沈昌祥院士表示国家安全标准委已对安全手机标准立项，意在研究制定手机安全标准，其中将包括关键硬件、软件信息基础设施的网络安全防护能力，系统安全等级，APP 权限限定等。如果标准出台进展顺利，公司的安全手机有望在明年开始放量。根据我们的推算，安全手机中加密部分每年潜在市场空间达百亿，卫士通作为央企竞争优势明显。推广初期假定每年 100 万人的推广速度，则核心加密部分有望为公司带来 3.96 亿收入。

■ **维持“买入”评级：**我们预计 2017/2018/2019 年净利润分别为 2.05/3.00/4.18 亿元，EPS 分别为 0.24/0.36/0.50 元，对应 91/61/44 倍 PE。公司近 5 年历史估值水平大部分处于 78 倍-140 倍之间，目前处于历史估值中下水平，考虑到公司作为网安央企平台的地位，维持“买入”评级。

■ 风险提示：信息安全市场低于预期；安全手机项目低于预期。

证券分析师郝彪
执业证书编号：S0600516030001
021-60199781
haob@dwzq.com.cn
研究助理陈晨
021-60199793
chenchen@dwzq.com.cn

股价走势

市场数据

收盘价（元）	22.05
一年最低/最高价	13.22/36.00
市净率（倍）	4.62
流通 A 股市值（百万元）	12158.6

基础数据

每股净资产（元）	4.77
资本负债率（%）	19.45
总股本（百万股）	838
流通 A 股(百万股）	551

相关研究

1. **卫士通：收入稳健增长，业绩承压不改长期增长逻辑-20170824**
2. **卫士通：业绩稳健布局完整，安全手机有望爆发-20170427**
3. **卫士通：增发顺利完成，构筑信息安全核心竞争力-20170322**
4. **卫士通：投入增加拖累业绩，自主可控大步迈进-20170305**
5. **卫士通：第三季度业绩优秀，增发助安全布局完善-20161027**

目录

图表目录

1 投资结论

网络空间成为新战场，卫士通作为中国网安上市平台持续整合打造完整产业链：美国网军不断升级，网络空间成为国家间博弈新的战场，中国电科顺应时代潮流组建专业网络安全子集团，卫士通成为网安子集团的上市平台。此前集团已将三十所旗下的三零嘉微、三零瑞通和三零盛安注入卫士通，为公司的战略整合指明发展方向。未来在电科集团资产证券化比例提升的趋势下，我们预计卫士通有望进一步通过整合完善产业链布局，打造网安旗舰上市平台。

从安全产品到安全服务模式转型大步推进，市场份额有望提升：大数据分析、云模式以及需求升级的三重推动，网安行业有望从当前的产品采购模式逐步向安全运维模式过渡，高壁垒决定了行业竞争格局走向集中。目前国内央企数量 98 家，假定一家央企的网安运维平均投入 1 亿/年，则仅央企范围的安全运维市场可达 100 亿。若加上成规模的地方国企，则市场保守估计可达 200 亿。目前中国网安已签订远洋海运等标杆客户，全年有望突破 10 家。作为中国网安的核心成员企业，并且中国网安的集成业务主要在卫士通，我们预计卫士通将主导安全运维业务的推进。

电子政务内网需求有望拉动加密业务快速发展：国务院办公厅印发的《政务信息系统整合共享实施方案》提出 2018 年 6 月底前，实现国务院各部门整合后的政务系统统一接入国家数据共享交换平台。电子政务内网建设市场可达百亿级别，我们预计省级招标今年有望启动，涉密网对厂商资质要求较高，卫士通作为专业加密龙头有望获得较大份额。

安全手机标准已经立项，放量可期：8 月底中国手机网络安全高峰论坛上，沈昌祥院士表示国家安全标准委已对安全手机标准立项，意在研究制定手机安全标准，其中将包括关键硬件、软件信息基础设施的网络安全防护能力，系统安全等级，APP 权限限定等。如果标准出台进展顺利，公司的安全手机有望在明年开始放量。根据我们的推算，安全手机中加密部分每年潜在市场空间达百亿，卫士通作为央企竞争优势明显。推广初期假定每年 100 万人的推广速度，则核心加密部分有望为公司带来 3.96 亿收入。

盈利预测与估值：我们预计 2017/2018/2019 年净利润分别为 2.05/3.00/4.18 亿元。EPS 分别为 0.24/0.36/0.50 元，对应 91/61/44 倍 PE，考虑到公司网安国家队的平台地位，维持“买入”评级。

风险提示：信息安全市场低于预期；安全手机项目低于预期。资产注入存在较大不确定性。

2 电科网络安全平台持续完善产业链，安全服务转型可期

2.1 网络安全成为新战场，成立中国网安打造专业子集团

2.1.1 网络安全成为新战场，美国网军不断升级

网络安全成为国家安全新战场，保卫网络疆域迫在眉睫。早在 2013 年，斯诺登曝光 NSA 的棱镜计划，棱镜计划是一项由美国国家安全局实施的绝密电子监听计划，该计划曝光后引发了美国民众对于隐私权的恐慌，曝光者斯诺登遭到刑事调查。在 2016 年的美国总统大选中，由维基解密曝光的希拉里邮件门引发了美国联邦调查局对希拉里的调查，并在很大程度上影响了大选结果。而 2017 年的 CIA 泄密事件相比前两者后果更加严重，在于其性质为黑客泄密，机密黑客工具一旦泄露，可迅速在几秒钟之内传遍全球，局面很难控制。从这些影响广泛的网络安全事件中不难看出，网络安全已经成为了国家安全的新战场，对于各国政府和国家领导来说，保卫自身的网络疆域迫在眉睫。

美国升级网军司令部凸显网络空间国防的重要性：美军网络司令部成立于 2009 年，曾隶属于美国战略司令部。2010 年正式启动后，该司令部开始统管全军网络安全和网络作战指挥。根据新华网，[1]美国总统特朗普 8 月 18 日宣布美军网络司令部升级。网络司令部升级后将成为美军第十个联合作战司令部，地位与美国中央司令部等主要作战司令部持平。网络司令部升级体现了美国抵御网络威胁的决心，并对敌人形成威慑。同时，国防部长马蒂斯正在审查网络司令部脱离国家安全局的可能性。美军网络司令部的成立与升级，意味着网络战成为国家层面的顶级进攻性战略作战方式，凸显了全球范围内对于网络空间安全之于国家安全的重要性的共识。

图表 1：美国网络空间国防发展轨迹

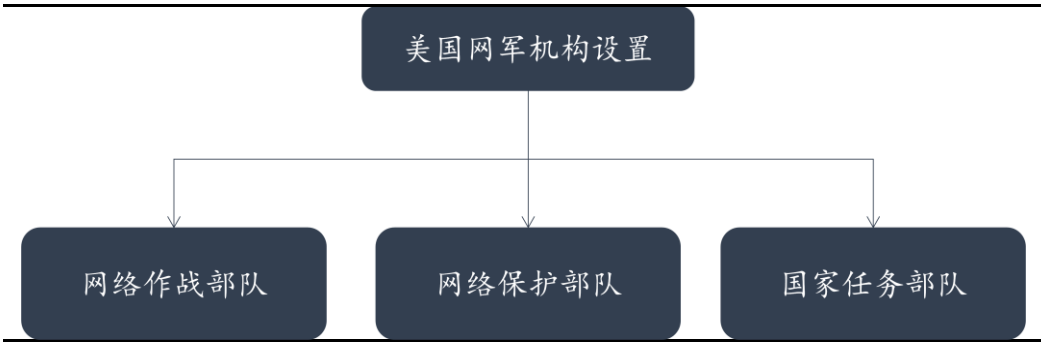
时间	事件	影响
2017.8	网络战司令部升级	升级后将成为美军第十个联合作战司令部，地位与美国中央司令部等主要作战司令部持平。网络战成为顶级战略作战方式。
2016	举行“网络卫士”演习	提高在联合作战中实际运用网络战的能力
2015	国防部发布最新网络空间安全战略	提供网络安全综合能力，支持军事行动和紧急计划；建设并维护网络安全力量，为网络行动做好准备。
2014	发布《四年防务审查报告》	将网络战列为 7 种作战能力之首，位于导弹防御、核威慑等能力之前；提出到 2019 年前，建设 108 个不同军种网络防护部队。
2011	发布《网络空间国际战略》	引发国际间网络军备竞赛
2009	组建网络战司令部	计划招聘 4000 名黑客，组建特种部队，统一协调保障美军网络安全和开展网络战等军事行动 。
2008	《国家网络安全综合计划(CNCI)》	美国首次提出网域安全国家战略，信息安全战略地位提升。
2007	棱镜计划	对即时通信和既存资料进行深度的监听
2004-今	爱因斯坦计划 2	部署基于签名的传感器，检测出试图非法进入联邦网络系统的互联网流量和恶意内容，形成入侵检测系统(IDS) 。
2004-今	爱因斯坦计划 3	识别和描述恶意网络流量，增强网络安全分析、态势感知和安全响应能力，形成入侵防御系统（IPS） 。

资料来源：中国军网，东吴证券研究所

[1] http://news.xinhuanet.com/2017-08/19/c_1121507713.htm

美国网络空间国防预算近千亿人民币，未来国内有望诞生千亿产业。据 2016 年新华网[2]的报道，美军从 2013 年年初开始组建网络部队，迄今已建成 123 支，总人数为 4990；未来的目标是在 2018 年建成 133 支具有全面作战能力的网络部队，总人数达 6187 人。美国网军包括网络作战部队、网络保护部队、国家任务部队三大机构。2016 年美国用于国防的网络安全预算已达 140 亿美元左右[3]，2016 年初我国成立战略支援部队，下设网络战部队，如果对照美国的投入，则网络空间国防有望催生千亿产业。

图表 2：美国网军机构设置



资料来源：新华网，东吴证券研究所

2.1.2 中国电科组建网络安全专业子集团

网络安全上升为国家战略，中电科组建网络安全产业子集团。2013 年底，国家成立中央网络安全和信息化领导小组，由习近平同志担任组长，标志着网络信息安全上升为国家战略。中国电科作为电子信息产业领域的科技型央企，在国家网络安全领域肩负着重要的使命和责任。为了在网络安全领域加强布局，同时加快整合集团内部资源，2015 年 5 月，经国务院批准，中国电科组建了国内规模最大的网络安全产业子集团——中国电科网络信息安全有限公司，以支撑国家网络安全战略实施，打造国家网络空间安全的核心力量，捍卫国家网络空间安全。

三十所和三十三所分别深耕加密和电磁安全业务。中国网安的核心是深耕信息安全和物理安全领域的中国电科第三十研究所、第三十三研究所。三十研究所以信息安全和保密为核心，以通信网络和信息系统为主体，以信息服务和信息工程为支撑，向社会提供全方位信息安全保密产品、通信网络软硬件产品并提供全方位信息服务，定位主要在于信息安全及保密，是网安构成的核心研究所。三十三研究所成立于 1958 年，是专门从事综合电磁安全防护技术的国家一类研究所，国家电磁防护专业技术组成员单位，主要研究方向为电磁安全防护技术、磁应用技术、电子信息系统集成技术、轨道交通测控技术等，在电磁防御领域具有较强实力。

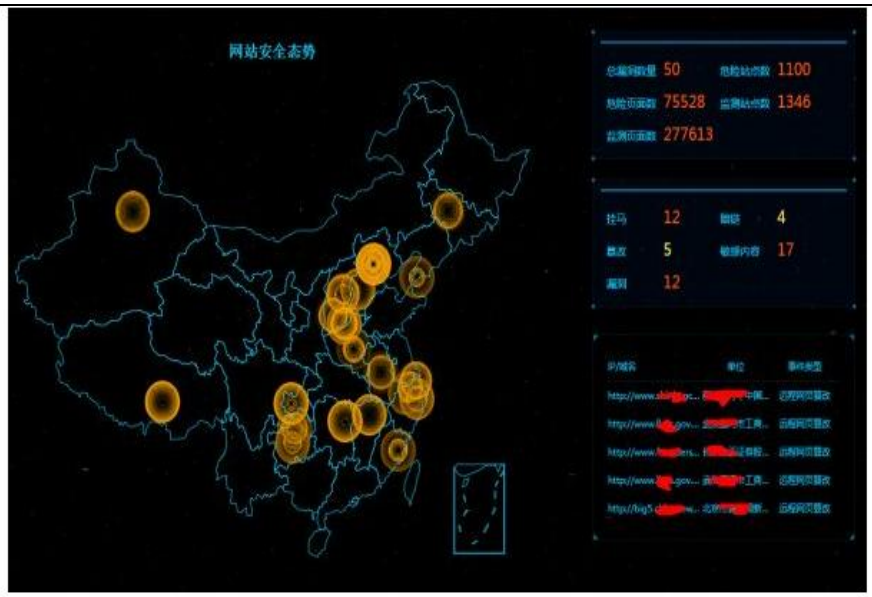
2.1.3 网安子集团发力全产业链布局，开启全新发展空间

态势感知成为网安发展方向和国家“十三五”信息规划重点内容。态势感知的概念源于军事需求，上世纪末被引入网络安全领域，其中最成熟的应用，是美国的爱因斯坦计划。爱因斯坦计划始于 2003 年，目的是让“系统能够自动地收集、关联、分析和共享美国联邦国内政府之间的计算机安全信息，从而使得各联邦机构能够接近实时地感知其网络基础设施面临的威胁。”现阶段“态势感知”要做到的除了检测和告警外，还包

[2] http://news.xinhuanet.com/tech/2016-04/06/c_1118541011.htm
[3] http://money.163.com/16/0219/05/BG5NOBA000253B0H.html

括指导决策，和动态监测。2016 年 12 月 27 日，国务院全文刊发了《“十三五”国家信息化规划》[4]，重点强调了态势感知的重要性。“十大任务”中的最后一项，是健全网络安全保障体系，并提出“全天候全方位感知网络安全态势”，为“态势感知”在未来五年的良好发展奠定基调。2017 年，四川省已正式启动了网络安全态势感知平台，目前，该平台已为 249 家重点单位超过 450 个关键信息基础设施，提供全方位不间断的网络威胁动态感知和通报预警。平台通过专用手机 APP，实现和提升了全省公安网安部门扫描监测、快速发现、问题通报、跟踪督办及整改复核等多项网络安全服务保障能力。未来，网络安全态势感知平台有望在更多省级项目实现落地，带来可观的市场空间。目前阶段的态势感知包括防火墙、漏洞扫描系统等多种产品和服务，但未来可能包括人机交互、人工智能等多个领域，多领域的发展有望为行业带来快速发展。

图表 3：网络态势感知示意图



资料来源：天极网，东吴证券研究所

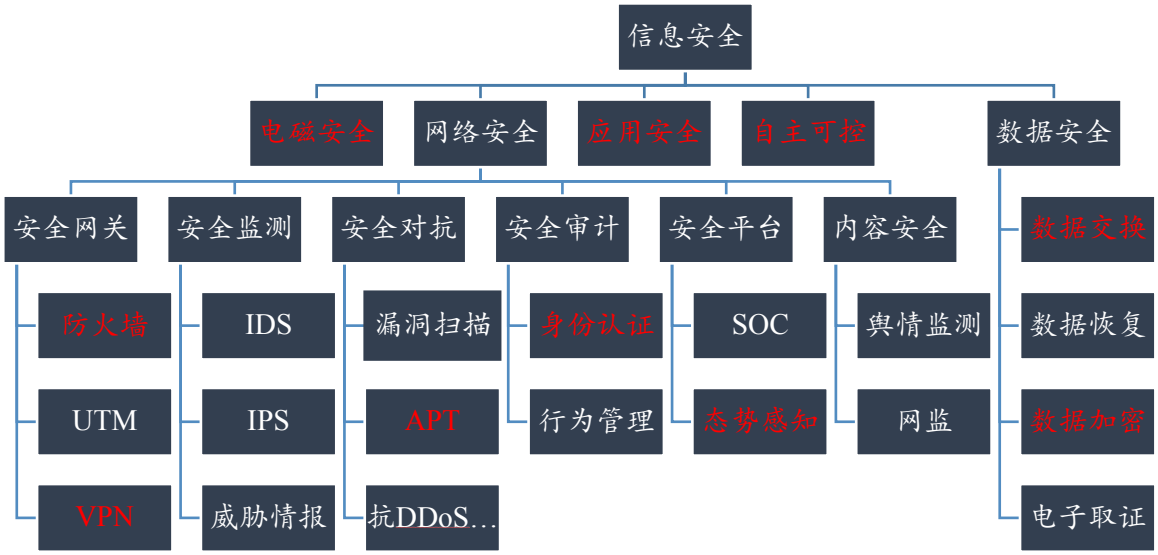
产学研结合抢占态势感知制高点。早在 2015 年底，中国网安就曾和西南交通大学签订有关“态势感知”的战略协议[5]，双方以本次签订战略合作框架协议为契机，在工业控制系统安全、密码算法设计与协议分析、网络安全态势感知、大数据安全存储、智慧城市网络安全架构等领域开展全方位的战略合作。近年来，中国网安在态势感知领域不断布局，后续有望在态势监测、工控安全、大数据安全等多领域实现突破。卫士通作为中国网安旗下的子公司，有望在态势感知领域走在前列，把握未来网络安全发展的新动态。

整合深思科技和新欣神风，应对 APT 和电磁安全[6]：2017 年 3 月上旬，中国网安完成对成都深思科技有限公司（以下简称深思科技）的战略性投资，深思科技正式成为中国网安旗下控股公司。这是继 2016 年 6 月控股成都新欣神风科技有限公司之后，中国网安在产业资源整合工作中的又一战略布局。在网络安全检测、取证、分析、防护和对抗领域构建了完备的产品体系，覆盖了从桌面、智能终端到服务器、网络设备和生产系统（如工控系统）的多个层级，形成了数个颇具影响力的系统。是在国内最早研究并跟

[4]http://www.miit.gov.cn/n1146290/n1146392/c5444529/content.html
[5]http://www.cbdio.com/BigData/2016-01/07/content_4450441.htm
[6] http://cetcsc.cetc.com.cn/wa/335070/335046/468379/index.html

踪高级可持续攻击（APT）的网络安全公司之一，也是极少数具有国家级网络入侵检测发现和对抗能力的公司。

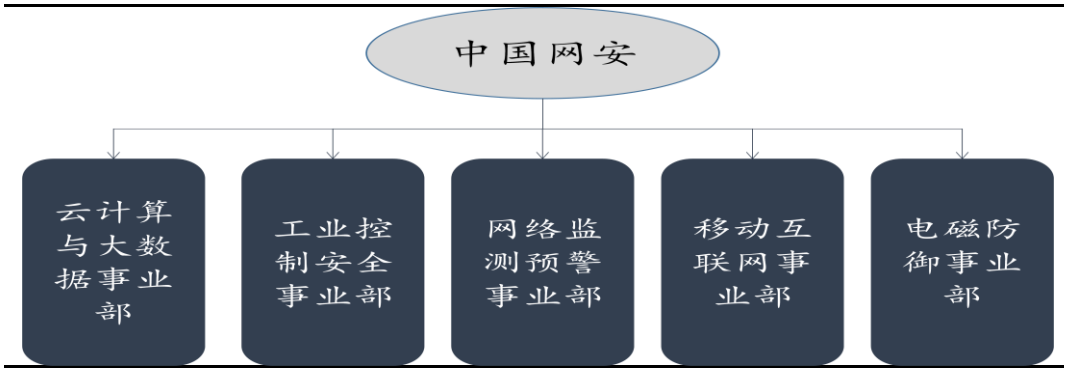
图表 4：信息安全产业的产品结构和中国网安的布局情况（红色）



资料来源：中国网安，东吴证券研究所

中国网安逐步打造完整信息安全产业链。组建后的中国网安子集团与成都市签署战略合作协议，斥资 100 多亿元在蓉建设国家示范网络信息安全产业园，目前已成立云计算与大数据事业部、工业控制安全事业部、网络监测预警事业部、移动互联网事业部和电磁防御事业部等五个事业部。此外，子集团通过合作和收购，逐步完成涵盖“芯片—软件—平台—整机—系统”的信息安全完整产业链布局，打造了包括卫士通、深思科技等在内的多个信息安全企业。

图表 5：中国网安成立五大事业部



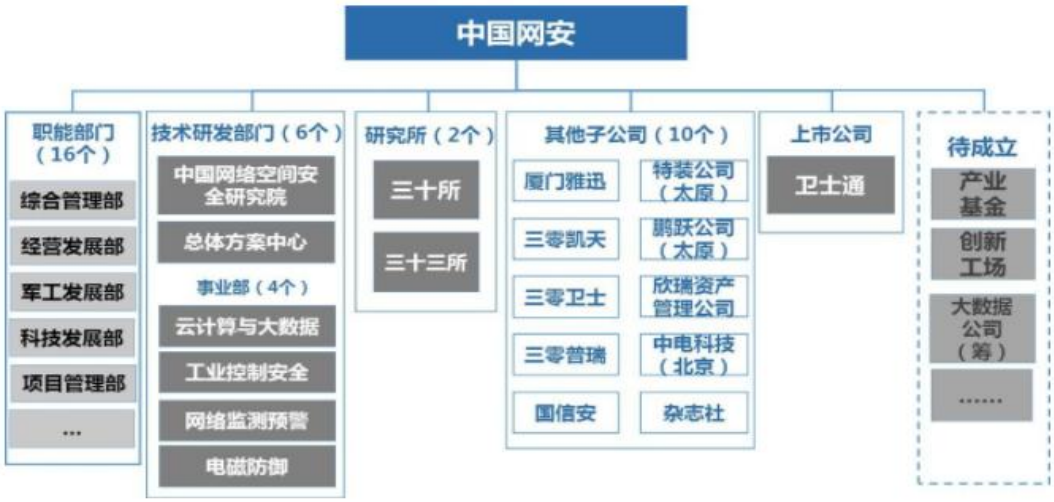
资料来源：卫士通公司公告，东吴证券研究所

2.2 定增整合，打造网络安全上市旗舰平台

2.2.1 中国网安的整合窗口，平台价值凸显

卫士通是中国网安的唯一上市平台。卫士通作为中国电科网络信息安全板块的上市公司，2014 年 12 月通过发行股份购买资产的方式整合了三十所下属的三家公司股权及北京房产。经过 2015 年的股份无偿划转后，中国网安成为卫士通的直接股东，能够充分利用上市公司平台，开展相关业务的战略布局、资源整合和业务协同。

图表 6：卫士通是中国网安旗下唯一的上市平台



资料来源：中国网安官网，东吴证券研究所

公司有望成为子集团的资源整合窗口。卫士通作为中国电科集团全资控股的中国网安旗下唯一的上市公司，未来有望成为其资产整合窗口，提升平台价值。此前卫士通已收购了三十所旗下的三零嘉微、三零瑞通和三零盛安，为公司未来的战略整合指明发展道路。未来，在电科集团资产证券化比例提升的趋势下，结合网安公司的板块布局规划，我们预计卫士通有望进一步整合中国网安下属其他优质资产，成为资源整合平台，不断扩充和完善全产业链，快速转型综合性服务厂商。

图表 7：三十所旗下信息安全企业

公司	主营业务	状态
三零嘉微	信息安全与通信保密系统相关芯片产品开发、测试、销售与服务	已收购
三零瑞通	安全保密手机，公众移动通信系统和专用移动通信系统的通信和网络安全服务。	已收购
三零盛安	信息系统集成、涉密系统建设、信息安全产品研发、行业应用软件开发、信息安全服务及 IT 外包服务。	已收购
厦门雅迅	卫星导航定位、车载终端及服务中心软硬件一体化解决方案及运营服务提供商	未收购
凯天	网络互动媒体、综合智能安方监控系统	未收购

资料来源：中国网安，卫士通，东吴证券研究所

2.2.2 定增完成，大股东参与彰显发展信心

募投项目完善安全布局，核心竞争力大幅增强。我国信息安全企业主要分布在北京、广深、四川、上海等地，其中北京地区拥有的信息安全企业数量较多，信息安全企业的

聚集效应也十分明显。公司目前的主要客户是政府、军工、金融、能源、运营商等重点行业及领域大中型企业。公司 2017 年 2 月底完成定向增发，本次增发募投资金主要用于投资密码系列产品、安全智能移动终端、国产自主高安全专用终端、面向工业控制系统和物联网的系列安全芯片项目、行业安全解决方案创新中心项目等公司重点战略布局项目，在行业用户方面进行深入布局，大力发展自主可控移动终端产品并在北京建立创新中心。本次募投项目实施后，公司将逐步完善从商用密码、芯片、板卡、设备、平台、系统，到方案、集成、服务的完整产业链，紧密围绕商用密码技术、网络安全、终端安全、数据安全、应用安全、内容安全和管理安全，努力构建技术先进、功能完善、种类丰富的齐套产品线，进一步提升公司在安全信息领域的行业地位，增强公司的核心竞争力。

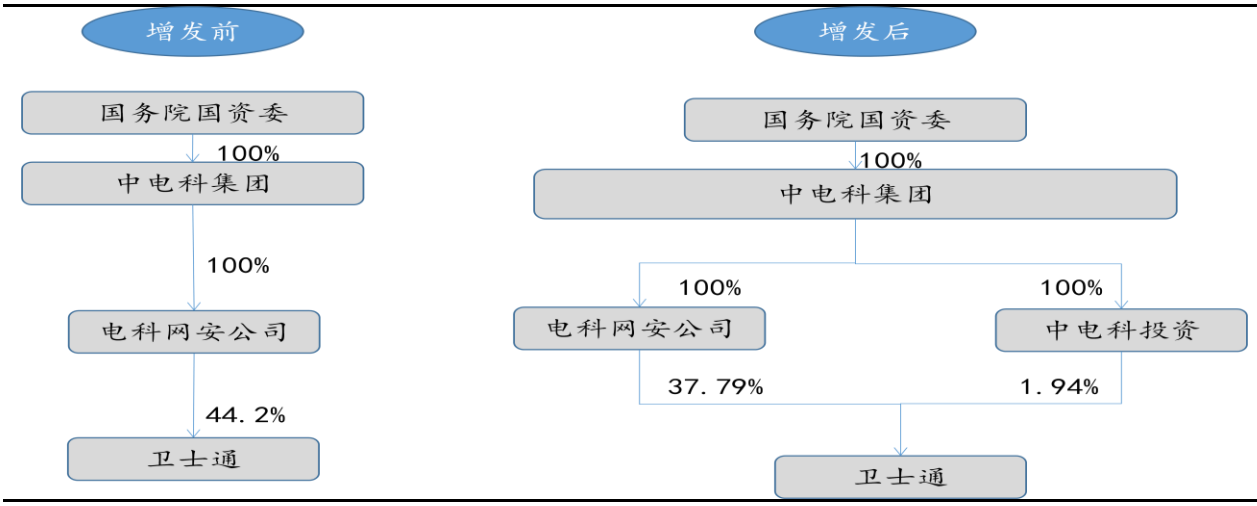
图表 8：公司募投项目

项目名称	项目投资总额	募集资金投入额	自筹资金投入额
新型商用密码系列产品产业化及国际化项目	75,628	68,628	7,000
安全智能移动终端及应用服务产业化项目	66,350	59,350	7,000
国产自主高安全专用终端项目	34,228	32,228	2,000
面向工业控制系统和物联网的系列安全芯片项目	59,250	51,250	8,000
行业安全解决方案创新中心项目	64,825	57,825	7,000

资料来源：卫士通公告，东吴证券研究所

大股东参与定增，彰显发展信心。本次非公开发行股票共计 9143.67 万股，募资金额 26.92 亿元，发行对象为包括中国网安、中电科投资在内不超过十名特定对象。中国网安、中电科投资分别承诺拟认购金额为 2 亿元、3 亿元。目前公司定增已经完成，完成后中国网安将持有公司 37.79%股权，中电科投资将持有公司 1.94%股权，中国网安仍为公司的控股股东，大股东参与定增充分彰显公司未来发展信心。

图表 9：卫士通增发前后股权结构对比



资料来源：卫士通公告，东吴证券研究所

2.3 从产品走向运维服务，卫士通作为央企份额有望扩大

安全平台大数据分析技术推动网安行业市场走向集中。由于网安大数据和安全平台技术出现较晚，此前国内企业的网安体系构建缺少整体性，主要是不同产品拼凑组合，各部门和产品之间互相独立缺少联动交互，同时主要以满足等保政策要求为主，网络安全厂商并不对安全防护的结果负责。这一模式不仅造成了行业产品结构零散和市场份额分散的局面，同时不能实现安全防护的根本目标。随着安全平台和大数据分析技术的成熟，以及人工智能深度学习的兴起，我们判断，未来网络安全的防护策略会变成涵盖云-网-端立体式一体化的策略，并且网络安全行业会逐步发展成为结果买单的服务模式，这样仅提供单个产品而不能提供整体策略和服务的中小公司将会被逐步淘汰，市场份额将向龙头公司集中。

云计算模式进一步加速行业走向集中。过去企业的 IT 网络是信息中心的模式，未来将变为云计算的模式。政府及大型企业在本地化到云端的迁移过程中，对于安全问题会更加敏感。我们认为在云计算场景中，将云平台服务和云安全服务分离的模式更有利于保障客户的数据安全，第三方安全厂商的地位会逐渐稳固和提升。随着政务网的互联互通，自上而下的一体化安全服务推广模式成为可能，导致市场份额也将进一步向龙头集中。我们认为 PPP 或政府采购服务有望成为未来政企领域云安全可能的付费方式，一方面将大幅改善行业的季节性，另一方面统一的安全服务商可以获得立体的安全数据，从而为下游提供更好的安全分析和安全保障。除政府层面的安全保障外，我们预计未来一段时间内，大型央企的安全运维工作也有望迎来增长。

首个央企网安运维落地，公司有望从安全设备提供商转型安全运维服务商。目前中国网安已经与中远海运集团签订了央企的安全运维“第一单”[7]，标志着中国网安将从传统的安全设备提供商向安全运维服务转变。中远海运集团将委托中国网安提供全系统、全方位、全天候的网络信息安全整体保障服务。中国网安将采用全新模式，为中远海运集团提供网络信息安全整体保障，建立安全管控、安全防护和安全服务三大体系。双方本次的合作，创新了网络信息安全保障的模式，改变了单一、静态、被动的信息系统防护方式，提升为全方位、全过程、全覆盖的全生命周期安全保障服务。通过对网络信息

[7] http://sichuan.scol.com.cn/ggxw/201708/55964020.html

安全整体保障模式的探索，力争达到“整体安全，全面保障”的信息化发展目标。实现关键信息基础设施和数据资产从局部单一防护向整体综合防护转变、从静态被动防御向主动防御转变、从事后处置整改向事前预警监测转变、从基础合规性要求向系统性本质安全转变，实现全方位的信息系统保障态势。本次合作有望打造央企安全运维标杆案例，未来央企网络安全从产品采购模式转向安全运维模式大势所趋。作为中国网安的核心成员企业，并且中国网安的集成业务主要在卫士通，我们预计卫士通将主导安全运维业务的推进，实现从设备商向安全运维商的转型。

安全运维市场有望达到 200 亿。目前国内央企数量为 98 家[8]，根据产业链调研，我们预计一家央企每年在网安领域的平均运维投入在 5000 万-2 亿之间，为谨慎起见，我们取 1 亿元的平均值，则仅央企范围的安全运维市场空间在 100 亿左右。地方国企数量过万家，成规模的国企数量逾千家，考虑到推广力度，我们谨慎预估地方性国有企业市场空间基本与央企安全运维市场空间齐平，则仅安全运维的市场空间即达到 200 亿以上。

央企龙头在行业走向集中的时期优势明显。卫士通背靠中电科，直属中国网安，是目前中国网络安全领域较为少见的央企平台。目前政府和央企业务占据公司收入大部分，我们预计未来随着政府及大型企业的逐步上云，同时随着自主可控的要求逐步加强，卫士通作为网安旗下唯一的上市平台，有望在市场份额不断提升的条件下占据更大的市场份额。

[8] http://news.163.com/17/0830/20/CT45PH2S00018AOQ.html

3 网络安全重中之重，加密领域加速发展

3.1 加密是网络安全体系的核心环节，卫士通龙头中地位突出

3.1.1 加密是网络安全中的重要一环，保护数据安全

加密产品是网络安全中的重要一环，作用在于保护用户的数据安全。网络安全从层次角度来看，可以大体上分为物理安全、逻辑安全、系统安全和联网安全。从防护的区域来讲，可以分为边界安全与主机安全。过去的网路安全发展过程中，边界安全得以不断加强，但主机安全的发展却有所落后。主机安全的主要功能是保证主机在数据存储的保密性，它包括硬件、固件、系统软件的自身安全以及一系列安全软件和技术。加密技术是数据安全的核心技术，尤其是在当今的电子商务、数字货币、网络银行等各种网络业务的快速的兴起时代。如何保护数据安全使之不被窃取、不被篡改或破坏等问题越来越受到人们的重视，而解决这些问题的关键就是数据加密技术。在加密技术中，密钥是必不可少的，密钥是使密码算法按照一种特定方式运行并产生特定密文的值。

3.1.2 加密技术主要分为对称加密和非对称加密

加密与解密的关系可以用公式简洁地表示。C=EK1(P)表示用加密密钥 K1 通过加密方法 E 对明文 P 进行加密得到密文 C。P=DK2(C)表示用解密密钥 K2 通过解密方法 D 对密文 C 进行解密得到明文 P。DK2(EK1(P))=P 由上面两个式子可以得到这个式子。由此可见，实际上，密码算法 E 和 D 都是数学函数。在典型的密码系统中，入侵者分为两类，一类是被动入侵者，即只监听消息而不改变消息内容，产生一个消息分叉；而第二类则为主动入侵者，不仅监听消息，还会将消息截断进行篡改，最后传递出错误的密码信息导致对于最终明文的误读。

对称密码算法与非对称密码算法。密码学发展至今，已经产生了大量优秀的密码算法，通常分为两类：对称密码算法和非对称密码算法。对称密码算法是指有了加密密钥就可以推算出解密密钥，有了解密密钥就可以推算出加密密钥的的算法。对称密码算法的特点是加密者指定一个密钥后，必须得想方设法把密钥分发出去给解密者，同时还得小心翼翼确保密钥不被泄露。在这种情况下，非对称密码显得至关重要，非对称密码算法的特点是加密密钥和解密密钥不相同，而且从加密密钥推算出解密密钥极其困难，因此也被称为公钥密码算法。

对称密码应用广泛，优缺点各有千秋。对称密码通常分为两类，一类是分组密码，另一类是序列密码。分组密码也称块密码，就是将明文划分成固定位的数据组，各组分别在密钥的控制下变换成等长度的密文分组，优点是对插入和修改具有免疫性，而缺点则是加密速度较慢以及错误容易扩散。序列密码也称流密码，是将明文逐位转换成密文，序列密码算法的安全性依赖于简单的异或运算和一次一密密码。序列密码体制的保密性取决于密钥的随机性，算法的优点是转换速度快，错误传播率低。对称密码主要包括 DES、IDEA、AES 等多种加密算法，在性能上各有千秋，近年来 AES 逐渐成为主流算法。

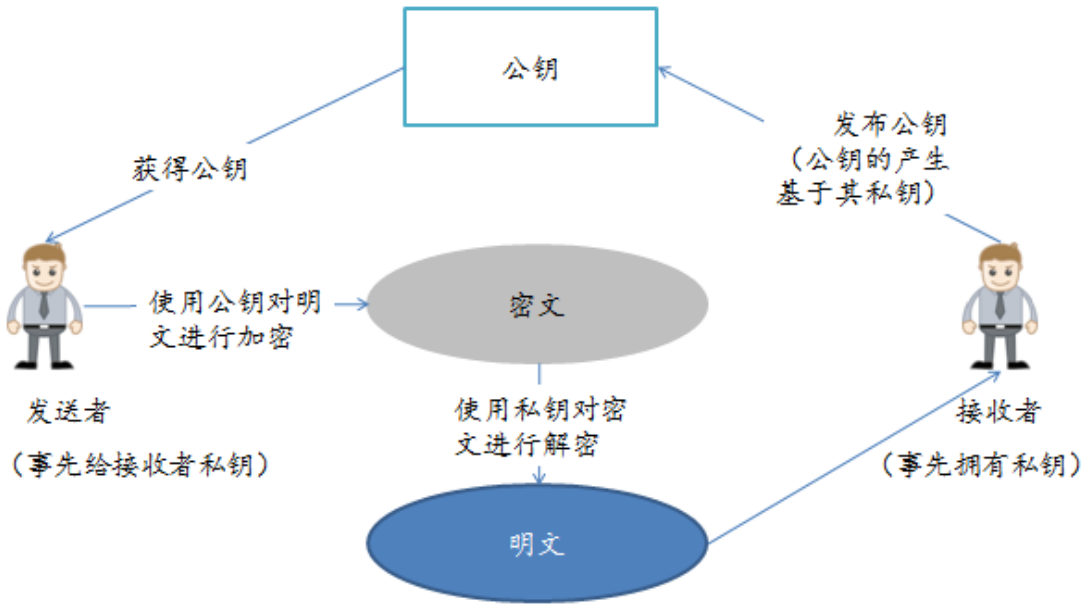
图表 10：几种商用加密算法特性比较

算法	密钥位数	循环次数	应用
DES	56 位	16	SET，Kerberos
IDEA	128 位	8	PGP
Blowfish	可变，至多 448 位	16	
三重 DES	112 或 168 位	48	财务密钥管理，PGP
LOKI	64 位	176	
RC5	可变，至多 2048 位	可变，至多 255	
CAST-128	40-128 位	16	PGP

资料来源：知网相关论文，东吴证券研究所

非对称密码主要用于数字签名领域。公开密钥加密简称公钥加密，属于不对称加密系统，其实现过程是使用一对密钥：公钥 PK 和私钥 SK，公钥和加密/解密算法是公开的，而密钥是保密的。一般用公钥加密，私钥解密，反之亦可，复杂度在于根据公钥估算出私钥是困难的，加密速度比 DES 要慢得多。RSA 是非对称加密算法中最常见的算法，其基本原理是：解密者拥有私钥，并且将由私钥计算生成的公钥发布给加密者。加密都使用公钥进行加密，并将密文发送到解密者，解密者用私钥解密将密文解码为明文。以甲要把信息发给乙为例，首先确定角色：甲为加密者，乙为解密者。首先由乙随机确定一个 KEY，称之为密钥，将这个 KEY 始终保存在机器 B 中而不发出来；然后，由这个 KEY 计算出另一个 KEY，称之为公钥。这个公钥的特性是几乎不可能通过它自身计算出生成它的私钥。接下来通过网络把这个公钥传给甲，甲收到公钥后，利用公钥对信息加密，并把密文通过网络发送到乙，最后乙利用已知的私钥，就对密文进行解码了。

图表 11：RSA 加密算法的基本流程



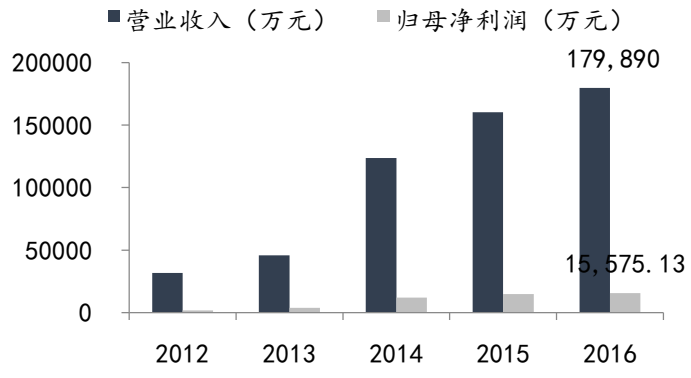
资料来源：知网论文整理，东吴证券研究所

3.1.3 加密业务历史悠久，密码领域绝对龙头

卫士通是国内加密领域绝对龙头。公司是国内唯一一家同时拥有涉密，商密领域最高级别资质信息安全企业，也是目前国内以密码为核心的信息安全设备的最大供应商。

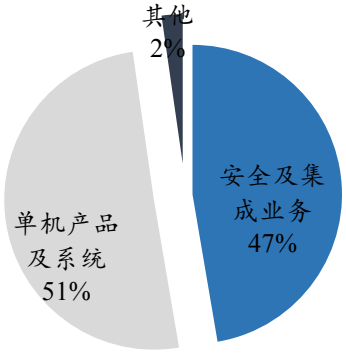
截至 2016 年底，公司实现营业收入 17.99 亿元，在收入层面实现大幅增长，由于投入较大，实现归母净利润 1.56 亿元。公司业务占比中，密码单机产品占比 51%左右，安全集成业务占比 47%。

图表 12：公司收入和净利润稳步提升



资料来源：Wind，东吴证券研究所

图表 13：密码及安全产品业务占比



资料来源：Wind，东吴证券研究所

密码系列产品涵盖芯片、系统、模块、设备全产业链。公司作为密码企业老牌龙头公司，产品类别涵盖芯片、系统、模块及设备等四个环节，产品包括密码卡、认证装置、安全模块、签名认证服务器等具体产品。密码产品在公司收入中占比很重，公司客户包括融、社保、电力、公交、证券等多行业领域，为企业及个人的加密业务提供强力保障。除传统密码产品之外，公司还拥有包括安全网关、安全专用平板等基于加密技术的信息安全产品，以及基于数字签名技术的电子文档安全管理系统等。

图表 14：密码产品系列

板块	产品
芯片	高速商用 PCI-E 密码卡
	商用 PCI-E 密码卡
系统	电力系统专用纵向加密认证装置
	金融 IC 卡密钥管理系统
	统一密码服务系统
	数字证书认证系统
	USBKEY 安全模块
	密钥管理系统
	金融 IC 卡数据准备系统
模块	USBKEY 安全模块
设备	签名认证服务器
	金融数据密码机
	服务器密码机

资料来源：卫士通公司网站，东吴证券研究所

3.2 信息安全加速发展，商密空间有望打开

3.2.1 信息安全三等级，商密市场空间最大

国家信息安全三个等级，其中核密最高。我们国家将信息安全划分为三个等级：核密、普密和商密。其中核密最高，普密次之，商密最低。核密指国家党政领导人及绝密单位的安全级别，此领域不存在任何商务行为。普密是指国家党政军机关的信息安全级别，此领域安全设备由国家指定的五家研究机构负责研制工作，商密用于保护企业级的商业秘密，技术上不一定比普密低，但商密产品的管理程度不如普密，应用产品多，应用面广（如 VPN）。国家规定商密禁止操作任何国家秘密以上的安全信息。

图表 15：国内加密等级及说明

信息安全等级	安全程度	内容描述	资质情况
核密	最高	国家党政领导人及绝密单位的安全级别。	无商业行为。
普密	次之	国家党政军机关的信息安全级别。普密可用于保护一定范围的国家安全信息，对国家秘密保护的强度包括它的手段和技术。因保护国家秘密信息的时候所采用的密码必须是普密级以上的，普密设备从管理上要求对普密产品、设备的管理非常严格。	国家指定五家研究机构负责研制：电子工业集团 30 研究所（卫士通）、原邮电部数据通信研究所（数据所）、总参 56 所（江南所）、中船 722 所、空三所。
商密	最低	用于保护企业级的商业秘密，技术上不一定比普密低，但商密产品的管理程度低于普密，应用产品多，应用面广（如 VPN）。	卫士通（国内唯一一家同时拥有涉密，商密领域最高级别资质信息安全企业）、立思辰、蓝盾股份等。

资料来源：卫士通官网，东吴证券研究所

普密及商密是具备市场空间的加密领域。普密级别中具有市场实力的只有三家：电子工业集团 30 研究所、原邮电部数据通信研究所、总参 56 所。普密和商密这两种信息的保护要求不一样，普密可以用于保护一定范围的国家安全信息，对国家秘密保护的强度包括它的手段和技术。从密码角度来说保护国家秘密信息的时候所采用的密码必须是普密级以上的，普密设备从管理上要求对普密产品、设备（包括研制、生产、销售普密产品的企业）的管理非常严格，应用范围相对较小。而商密的市场相对公开，管理程度低于普密，但应用产品多，应用面较广。

3.2.2 商用密码领域市场发展加速

商用密码产业链完整，销售额达到百亿级以上。商用密码是指对不涉及国家秘密内容的信息进行加密保护或者安全认证所需要使用的密码技术和密码产品，是商用密码技术和商用密码产品的总称。我国密码技术体系基本形成，在某些领域上的研究深度达到了国际水平，如 SM4 分组密码算法、TCM 密码芯片、PKI/CA 等技术。目前，商用密码产品已经形成了从芯片、办卡、整机到软件、系统和密码服务的完整产业链，而且密码产品更加实用。根据北京市密码管理局局长介绍，截至 2016 年底，北京市商用密码

产品销售额达到 70 亿元，占全国商用密码产品总销售额的 60%，处于领先地位[9]。以此推算，全国商用密码产品的销售额为 120 亿元左右，在信息安全产业总规模市场中占比接近 20%。未来商用密码市场在信息安全产业中占比有望提升，增速获得进一步提高。

图表 16：商密产品按照功能分类

类别	解释	典型产品
密码算法类	构成密码应用基础的能提供密码运算功能的产品	密码算法实现软件、密码算法芯片等产品
数据加解密类	提供数据加解密功能的产品	加密机、加密卡、智能密码钥匙等产品
认证鉴别类	提供身份认证、密码鉴别功能的产品	动态口令系统、身份认证系统等产品
证书管理类	提供数字证书的产生、分发、管理功能的产品	数字证书管理系统等产品
密钥管理类	提供密钥的产生、分发、更新、归档和恢复等功能的产品	密钥管理系统等产品
密码防伪类	提供密码防伪验证功能的产品	电子印章系统、支付密码器、数字水印等产品
综合类	提供上述两种或两种以上功能的产品	电子商务安全平台等产品

资料来源：中孚信息公告，东吴证券研究所

商用密码功能完整，形态多样。商用密码产品按功能可分为密码算法类、数据加解密类、认证鉴别类、证书管理类、密钥管理类、密码防伪类和综合类。商用密码产品按照形态可分为密码软件类、密码芯片类、密码模块类、密码板卡类、密码整机类和密码系统类。

图表 17：商密产品按照形态分类

类别	解释	典型产品
密码软件类	提供纯软件形态出现的密码产品	信息加密软件、密码算法实现软件等产品
密码芯片类	指以集成电路芯片形态出现的密码产品	密码算法芯片、密码 SOC 芯片等产品
密码模块类	指以多芯片组装的背板形态出现，具备专用密码功能，但本身不能完成完整的密码功能的产品	加解密模块、安全控制模块等产品
密码板卡类	指以板卡形态出现，具备完整密码功能的产品	USB 密码钥匙、PCI 密码卡等产品
密码整机类	指以整机形态出现，具备完整密码功能的产品	VPN、网络密码机、服务器密码机、签名验证服务器等产品
密码系统类	指以系统形态出现，由密码功能支撑的产品	安全认证系统、秘钥管理系统等产品

资料来源：中孚信息公告，东吴证券研究所

[9]http://bj.people.com.cn/n2/2017/0212/c82839-29702880.html

各行业密码管理规范不断加强，需求进一步释放。近年来，为了保障各个重要行业的数据安全，加强密码管理，国家在密码管理规范上不断加强，在金融、电力等多个领域均发布重磅规范及政策。政策规范之下，重点行业企业的密码需求有望得到进一步释放。

图表 18 ： 加密领域行业政策法规

时间	政策	主要内容
2012、2013 年	国家发展与改革委员会启动“下一代互联网高性能 IPSECVPN”和“移动互联网安全接入网关-高性能 SSLVPN”专项	对国产商用高性能 VPN 的产业化进行了资金和政策上的大力支持
2014 年	国家密码管理局于 2014 年发布了最新的《IPSECVPN 技术规范》、《IPSECVPN 网关产品规范》、《SSLVPN 技术规范》、《SSLVPN 网关产品规范》等行业技术标准	对国产商用 VPN 的发展进行了规范
2014 年 2 月	国务院发布《国务院办公厅转发密码局等部门关于金融领域密码应用指导意见的通知》	明确提出在金融领域要用我国自主研制的系列商用密码技术（包含算法、协议和产品）替换原用的国外密码技术，并在时间进度要求方面、加快产业升级改造方面、强化基础设施支撑方面以及稳步推进密码应用发展方面明确了目标及工作内容。
2014 年 8 月	国家发展与改革委员会于 2014 年发布了 14 号令—电力监控系统安全防护规定	加强电力监控系统的信息安全管理，防范黑客及恶意代码等对电力监控系统的攻击及侵害，保障电力系统的安全稳定运行
2015 年 2 月	国家能源局印发《电力监控系统安全防护总体方案》等安全防护方案和评估规范的通知，	对发电、输变电、配电、电力调度等各大环节及各级电力单位提出了建设完善的电力监控系统安全防护体系的要求，并明确提出了在纵向边界防护和数据远程传输方面采用专用的纵向加密认证装置或加密认证网关（电力专用 VPN 的两种产品形态）实现身份认证、安全接入和数据加密，实现数据传输的机密性、完整性保护

资料来源：国务院，国家密码管理局等，东吴证券研究所

3.3 多重因素发酵，传统加密市场有望加大

3.3.1 密码算法国产化趋势显著，增量市场有望释放

目前，我过的密码体系仍普遍采用 RSA 算法。根据格尔软件的招股说明书，目前我国密码体系仍然普遍使用 RSA 算法。RSA 密码算法是三位美国麻省理工学院教授提出的，后来这三名教授还联合成立了同名的 RSA 公司，中国的三大运营商及不少银行、制造业企业也都是它的客户。国内很多企业和网站甚至完全采用国外密码体系和产品，这具有很大的安全隐患。

全面采用国产通用算法是商用密码产业发展的重大机遇。目前全面采用国产通用算法是国家信息安全战略的内在要求，也是商用密码发展的必由之路。从产业基础上看，国产通用算法的推广已经具备了一些基础，包括基础设施产品、安全应用产品、应用中间件、标准规范、密码芯片、智能 IC 卡、智能密码钥匙、密码卡和服务器密码机等相关市场。我们预计随着国产密码算法的逐步推广和标准的逐步成熟，密码行业有望迎来全新国产替代的增量空间。

硬件国产化也有望为密码产品带来增量市场。由于我国整个 IT 产业的起步比国际落后几十年，技术水平有不小差距。在实现自主可控的道路上，先后出现了三种不同的模式：自主研发，以 CEC 集团（中国电子信息集团产业公司）为代表；开放合作，以华胜天成和 IBM 的合作为代表；国际并购，以紫光集团的海外并购为代表。开放合作主要是在高端计算领域，海外并购则主要是在移动端芯片、服务器方面，目前看起来，自主研发已经逐步搭建自身生态实现产业化，开放合作和国际并购的效果尚待验证。底层硬件技术逐渐成熟，16 年以来信息安全相关事件频出，政策层面来看硬件国产化空间亟待释放，第二期自主可控招标即将大规模启动。伴随着硬件国产化空间的逐步释放，未来配套的密码产品将会迎来大规模更新需求，增量市场有望随着自主可控的招标而逐步打开。

图表 19：16 年以来国内主要信息安全事件凸显自主可控的重要性

时间	政策事件
2012.12.28	全国人大常委会通过《关于加强网络信息保护的决定》
2013.6.8	中美将在战略安全对话框架内设网络安全工作小组
2013.6.14	外交部设立网络实物办公室
2013.11.12	中央决定成立国家安全委员会
2014.2.27	中央网络安全和信息化领导小组成立
2015.7.1	《国家安全法》公布施行
2016.3.25	中国网络空间安全协会成立
2016.4.19	习近平在网络安全和信息化工作座谈会上发表 419 重要讲话
2016.8.22	中央网信领导小组发布《关于加强国家网络安全标准化工作的若干意见》
2016.10.17	工信部印发《工业控制系统信息安全防护指南》
2016.12.27	国家网信办发布《国家网络空间安全战略》
2017.3.1	外交部和国家网信办发布《网络空间国际合作战略》
2017.6.1	《网络安全法》正式实施
2017.6.9	国家网信办、公安部、工信部等四部委发布《网络关键设备和网络安全专用产品目录（第一批）》

资料来源：工信部，网信办等，东吴证券研究所

3.3.2 电子政务市场发展如火如荼，密码法有望出台

电子政务内网提出对私有密钥的需求，强化网络安全。2002 年 7 月，国家信息化领导小组就推出了《关于我国电子政务建设的指导意见》（17 号文件），文件中提出要建设政务内网和政务外网。电子政务网络由政务内网和政务外网构成，两网之间物理隔离，政务外网和互联网之间逻辑隔离。政务内网主要是副省级以上政务部门的办公网，与副省级以下的政务部门的办公网物理隔离。此后 2006 年又推出了 18 号文，明确定义了电子政务网络。政务内网有自己的政府局域网、城域网和广域网，政务外网也有自己的政府局域网、城域网和广域网。党委、政府、人大、政协、纪委五套班子统一建网，政务内网的网络要提供报文加密能力，网络加密设备除提供标准加密算法和 128 位以上加密

密钥支持外，需具备对私有密钥的支持能力，强化网络安全。

政务内网由垂直部门走向互通，如若进展顺利则更大市场空间凸显。国务院办公厅印发《政务信息系统整合共享实施方案》，提出 2017 年 12 月底前，基本完成国务院部门内部政务信息系统整合工作；2018 年 6 月底前，实现国务院各部门整合后的政务系统统一接入国家数据共享交换平台，初步实现国务院部门和地方政府信息系统互联互通。本次《方案》对完成节点和各主要责任方做了具体安排，有望保障方案的顺利进行。我们预计今年省份的招标有望启动，传统的机要网建设向涉密级网络转变，一旦政务内网的建设进展顺利，将有望为卫士通带来机会。政务信息共享平台的建设，将原先垂直部门进行打通，各类信息系统的数据平台建设和运维市场空间有望达到百亿级别，带来更大的市场空间。

国密局密码法征求意见稿发布，密码法有望颁布。2017 年 4 月，国家密码局对公众发布了《中华人民共和国密码法（草案征求意见稿）》[10]，草案征求意见稿在密码应用、密码安全、密码发展促进等多个领域给予了具体规范和指导，违者将承担法律责任。草案内容中的关键一点是，国家将对关键信息基础设施的密码应用安全性进行分类分级评估，按照国家安全审查的要求对影响或者可能影响国家安全的密码产品、密码相关服务和密码保障系统进行安全审查。对于密码产品的全国性检查一经展开的话，我们预计将很快对企业及单位的密码产品及服务采取强制配备措施。这样一来，企业在密码产品使用方面的需求将逐步由自愿转为强制，市场规模将得到大规模提升。此外，《意见稿》还指出，任何组织或者个人不得非法攻击他人的加密信息或者密码保障系统，将攻击密码保障系统正式确立为犯罪行为，将大大加强密码产品使用的权威性和安全性。我们预计，《密码法》有望于今年出第二版征求意见稿，安全性核查有望逐步展开，带来密码行业进展的进一步加速。

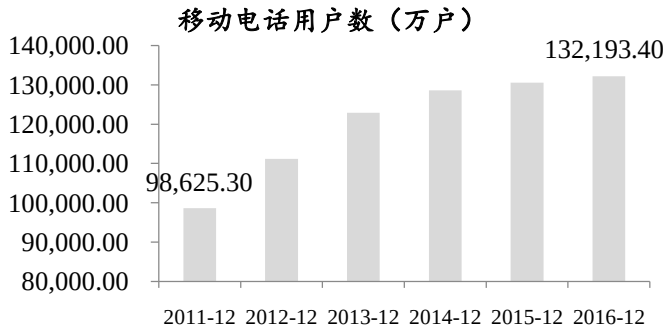
[10]http://mt.sohu.com/business/d20170414/133995419_498774.shtml

4 安全手机打开加密应用新空间

4.1 移动终端的安全及自主可控重要性逐渐显现

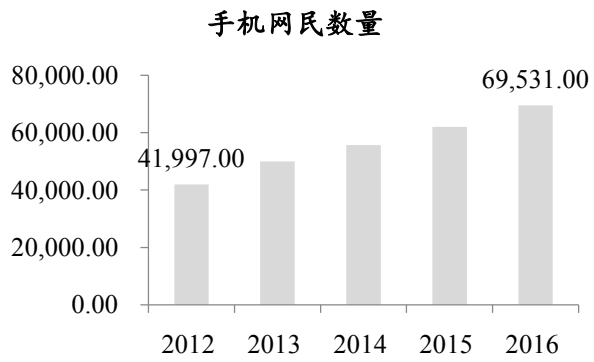
移动终端用户需求不断提升。随着新型智能移动终端的发布，我国智能移动终端用户呈现井喷式增长趋势，智能移动终端的需求不断攀升。根据工信部发布的数据显示，我国移动电话的用户数由 2011 年底的不到 10 亿人，快速增长至 2016 年底的过 13 亿人。同时，根据中国互联网络信息中心的数据统计，我国手机网民的数量于 2016 年底已经增加至 6.95 亿人，在所有网民中占比达到 69.53%。

图表 20：移动电话用户数逐年递增



资料来源：Wind，东吴证券研究所

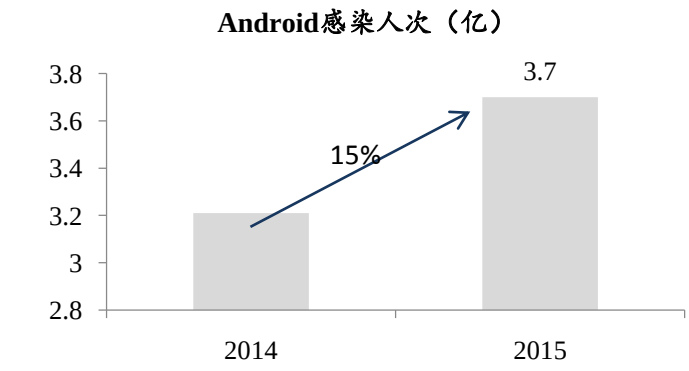
图表 21：手机网民数量



资料来源：Wind，东吴证券研究所

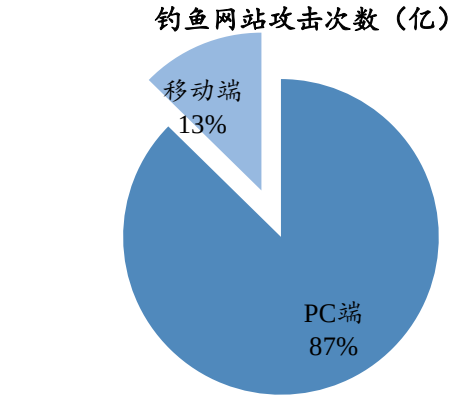
移动终端安全问题日渐严重。根据 360 发布的《2015 年中国互联网安全报告》[11]，2015 年移动端累计监测到 Android 用户感染恶意程序 3.7 亿人次，较 2014 年增长了 15.0%，移动端恶意程序类型中资费消耗占比高达 73.6%；其次为恶意扣费（21.5%）和隐私窃取（4.1%），手机恶意程序趋利性极为明显。在拦截的钓鱼网站中，手机端为 48.0 亿次，占比 12.6%。手机端拦截的总攻击次数和在总拦截量中的占比，均创历史新高。手机端被骗用户的虚假兼职、虚假中奖及账号被盗占比达到 50.5%，而社交工具在诈骗案例中的占比达到 59.3%，是实施诈骗最主要的途径。终端信息安全形势的日益严峻使得政企、个人用户更加注重网络安全，未来移动终端市场有望成为信息安全厂商的争夺重点。

图表 22：Android 用户感染恶意程序 3.7 亿人次



资料来源：中国互联网安全报告，东吴证券研究所

图表 23：黑客利用软件漏洞制造了输油管道爆炸



资料来源：中国互联网安全报告，东吴证券研究所

[11]http://zt.360.cn/1101061855.php?dtid=1101062370&did=1101654296

4.2 安全手机业务放量可期

安全手机标准的制定有望拉动行业快速发展。根据经济参考报[12]，国家安全标准委已对安全手机标准立项，意在研究制定手机安全标准，其中将包括关键硬件、软件信息基础设施的网络安全防护能力，系统安全等级，APP 权限限定等。16 年以来，我国在网络安全、自主可控领域的政策频出，此前 2016 年 7 月已经发布了关键行业基础设施的检查要求，而《网络安全法》于 2016 年 11 月得以颁布，并于今年 6 月 1 日起正式施行，不断推动安全行业的发展。但目前为止相关基础设施及网络安全的要求主要停留在 PC 层面的安全，对于移动端暂时未提出具体要求。本次手机安全标准的立项，有望推动基础设施及网络安全向移动端转移，有望对于安全手机硬件、网络安全软件防护、系统安全等级等方面做出具体规定。标准一旦颁布，未来对于移动端的安全产品与服务的投入将有望大幅增加，目前华为、中兴等手机厂商也在安全手机领域进行抢滩。我们预计，未来手机安全行业在硬件端有望迎来更高增速，基于硬件防护设置及保密通信的安全手机有望成为热点；另一方面，相较于个人信息泄露的危害而言，企业级移动安全更为牵动人心，关键部门及国家关键行业央企从业人员的移动手机涉及更多国家关键信息，一旦泄露危害很大。

安全手机成熟，有望实现快速放量。公司自 2015 年就开展国产自主高安全专用终端的研发，针对政府、军工、金融、能源等重点行业用户的安全需求，自主设计元器件、核心模块、整机、操作系统及基础软件，为重点行业用户提供国产自主高安全专用终端。同时旗下天津网安专注于移动安全中间件、移动安全管理平台/运营中心、行业移动安全应用等软件产品的研发与推广，为公司构建持续的安全运营能力，推动公司的可持续发展。目前，卫士通已经发布龙御系列自主可控计算机、卫士通中华卫士系列自主可控安全交换机等基于国产芯片的产品，与华为合作的安全手机集成了移动 OA，从此前的通话安全扩展到办公安全和数据安全，17 年有望开始放量。

图表 24：卫士通安全手机

资料来源：卫士通公司网站，东吴证券研究所

公司从产品走向运营，有望拓展移动支付安全服务。目前，卫士通与华为合作的安

[12]http://jjckb.xinhuanet.com/2017-08/30/c_136566684.htm

全手机集成了移动 OA，从此前的通话安全扩展到办公安全和数据安全，目前已经安装 10 个左右 APP。公司作为安全手机标准制定的参与者之一，未来在安全手机的市场中有望分得更大蛋糕。同时，随着移动支付的高速增长，2016 年非银行支付机构累计发生网络支付业务 1639.02 亿笔，金额 99.27 万亿元，同比分别增长 99.53%和 100.65%，二季度人均损失金额高达 17582 元。在移动互联网端网民数量剧增、信息泄露、恶意攻击等恶性攻击事件频出的背景下，我们预计手机网络安全市场空间有望实现快速拓展，有望从目前约 100 亿元左右规模扩张至千亿元以上。随着从安全手机硬件向办公软件、支付安全软件等不断拓展的过程中，公司自身也不断实现从产品到运营的转变。我们预计未来公司有望在移动支付和支付安全领域进行更多布局和优势积累。

4.3 安全手机每年潜在市场空间达百亿

安全智能终端市场空间广阔。公司的安全智能移动终端客户主要面向政府、事业单位、金融、能源等领域对具有高安全性的智能移动终端需求迫切的政企行业用户和高端商务人士，目标市场可划分为专用市场，商用政企行业市场，以及金融、能源等大中型企业和高端商务人士市场；其中专用市场和商用政企行业市场为最主要的目标市场。从商业模式上看，除了安全手机硬件销售利润之外，公司和中国移动合作的产品还包括秘钥管理平台，公司有望在给运营商提供安全平台服务的过程中参与增值服务分成。

公务人员体系庞大，安全手机每年潜在市场空间达百亿。根据人社部发布的《2016 年度人力资源和社会保障事业发展统计公报》，截止 2016 年底，全国共有公务员 719 万人。按照每台安全手机售价 3000 元，若假设公务员人手一台安全手机，仅考虑公务员的安全手机整机市场规模约为 215 亿元。如果按照全部财政供养人数 5000 万左右计算[13]，则市场空间约为公务员人数的 6.95 倍，整机市场空间近 1500 亿元。根据产业链调研，按照每部手机约有 300 元左右的加密硬件费，每部手机每个月 20 块的加密服务费（其中卫士通分成 8 元），全年加密服务费为 96 元。假定一部手机使用三年，则年化潜在市场空间 98 亿。我们预计，在业务推广初期，如果能够实现 100 万人每年的安全手机推进速度，则安全手机给公司带来的收入约为 3.96 亿元。

卫士通在安全智能手机厂商中竞争优势突出：目前，商业智能安全手机领域由于资质门槛较低同时安全机制有所不同，所以市场上参与者众多，主要分为三类：第一类是运营商，当前主要是电信和中移动；2、第二类是手机厂商，主要有酷派、华为、中兴等；3、加密厂商，主要有卫士通和国家保密局保密技术研究所。同时，合作共赢的趋势愈加显著。而军品加密手机除技术门槛较高外，对资质要求严格，当前仅公司（军工集团旗下企业）和江南计算机技术研究所（总参 56 所）具备军品安全手机相关资质，未来增加可能性小，属有限竞争市场。在商业智能安全手机领域，公司和中移动、华为深度合作，推出 Mate8/Mate9 系列安全手机，华为智能手机的市占率目前已达到全国第一[14]，在国内的智能手机市场上竞争力超群，加之中国移动是我国最大的运营商，品牌和渠道最优，我们预计未来卫士通推出的安全手机有望抢占 30%以上的市场份额。如果按照每年 100 万部手机的推进速度，则每年安全手机硬件及运营业务带来的收入将达到 1.02 亿元。短期内，我们预计公务员 719 万人有望在 4-5 年内更换完毕，2017 年下半年刚开始推进，所以预期 2017 年推广数量为 50 万台，2018 年随着需求逐步释放市场有望

[13]http://politics.people.com.cn/n1/2016/0621/c1001-28464163.html
[14] http://android.tgbus.com/news/bd/201607/549964.shtml

翻倍，2019 年继续大幅增长。

图表 25：移动终端市场空间和卫士通营收测算

智能安全手机市场空间	单价（元）	2017	2018	2019
销量（万台）		50	100	200
市场空间（亿元）	3000	15	30	60
卫士通收入空间	单品（元）	收入（万元）		
假设：市占率 30%		2017E	2018E	2019E
硬件	300	5000	10000	20000
加密服务	8	120	240	480
总额		5120	10240	20480

资料来源：东吴证券研究所

安全手机有望拓展到其他国产自主可控安全终端市场广阔。根据人社部的公报，我国有约 719 万在编公务员，按每人配置一台终端计算机进行概算，涉及更换的终端计算机约 720 万台套。参考目前的市场价格，则仅政府市场空间将在 420 亿元以上。随着金融、能源等重点行业非公务员序列的自主安全终端更换需求被陆续唤醒，国产自主安全终端市场规模将超千亿元。

5 盈利预测与估值

5.1 核心假设与盈利预测

中国网安唯一上市公司平台，有望成为资源整合窗口。卫士通作为中国电科集团全资控股的中国网安旗下上市平台，是网安子集团资产的整合窗口。此前集团已将三十所旗下的三零嘉微、三零瑞通和三零盛安注入卫士通，为公司的战略整合指明发展道路。未来，在电科集团资产证券化比例提升的趋势下，结合网安公司的板块布局规划，我们预计卫士通有望不断扩充和完善全产业链，打造网安旗舰平台。

核心假设：

1 假设公司传统加密业务 2017 年维持 20%左右的收入增速，后续电子政务内网加速实现增速维持 30%;

2 假设安全运维今年实现 10 个央企的运维，并确认 35%收入;

3 假设安全手机今年放量 50 万台，未来 2 年增速 100%，公司市场份额 30%。

图表 26：卫士通营收测算

卫士通收入（亿元）	2017	2018	2019
传统业务	21	27.3	35.5
安全运维	3.5	7	14
安全手机	0.45	0.9	1.8
总收入（取整数）	25	35	51

资料来源：东吴证券研究所

盈利预测：考虑到公司 2017-2019 年处于新业务不断拓展的阶段，投入有所增加。我们预计 2017/2018/2019 年净利润分别为 2.05/3.00/4.18 亿元。

5.2 估值与评级

与可比公司估值对比：卫士通是网安央企平台，可比标的一种是计算机行业平台公司，比如用友网络，一种是其它央企军工信息化平台如中电广通、杰赛科技， 一种是央企混改平台如四维图新。这四家公司 2017 年平均估值 120 倍，2018 年平均估值 94 倍，卫士通 2017 年估值 91 倍，2018 年估值 61 倍，与这些可比公司相比，公司估值处于合理范围。

图表 27：可比公司估值情况

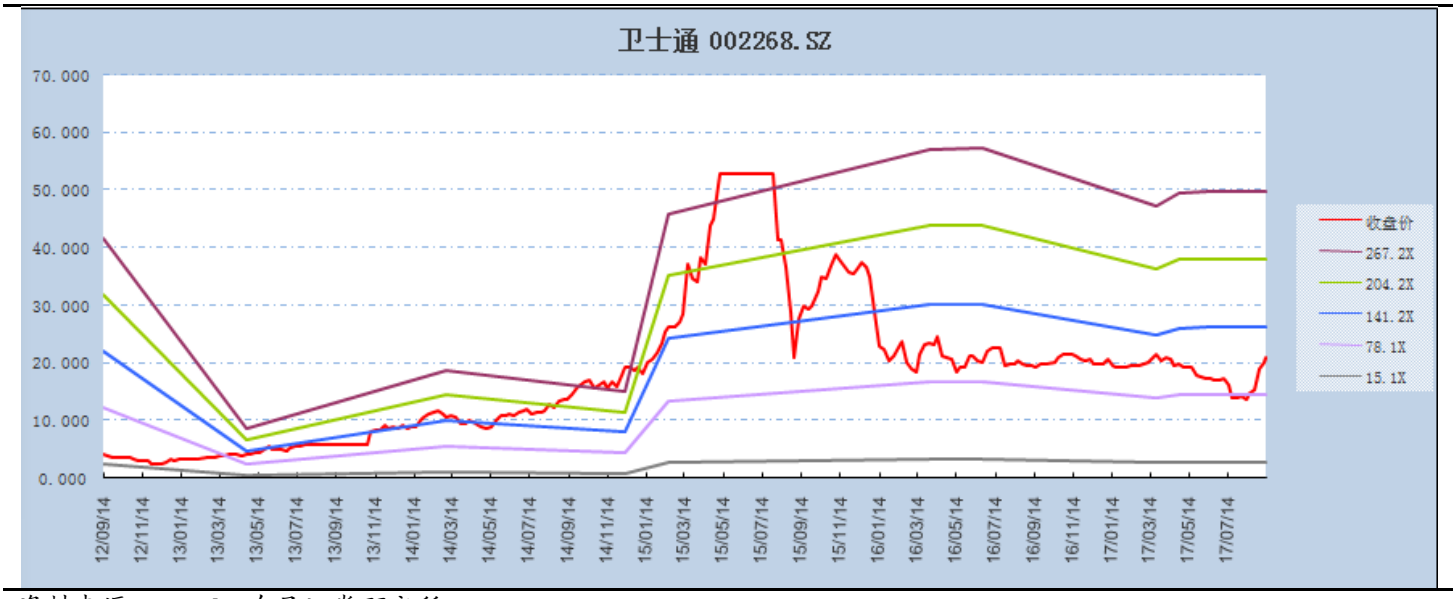
代码	公司名称	市值（亿元）	收盘价	EPS 2016	EPS 2017E	EPS 2018E	PE 2016	PE 2017	PE 2018	评级
002544.SZ	杰赛科技	110.11	21.35	0.21	0.41	0.5	101.67	52.07	42.7	买入
600764.SH	中电广通	129.85	39.38	0.02	0.16	0.19	1790	246.13	207.26	买入
002405.SZ	四维图新	358.88	27.98	0.15	0.3	0.39	187.66	93.52	71.74	未评级
600588.SH	用友网络	356.68	24.36	0.14	0.27	0.44	174	90.22	55.36	买入

资料来源：Wind，东吴证券研究所，未评级公司取 Wind 一致预期

与历史估值相比：我们考察了公司的历史估值水平，根据 Wind 统计的 PE-band 显

示，近 5 年以来，公司历史估值水平大部分处于 78-140 倍之间，目前估值处于历史估值中下水平。

图表 28：卫士通历史估值数据



资料来源：Wind，东吴证券研究所

维持“买入”评级。我们预计 2017/2018/2019 年净利润分别为 2.05/3.00/4.18 亿元。EPS 分别为 0.24/0.36/0.50 元，对应 91/61/44 倍 PE，考虑到公司网安国家队的平台地位，维持“买入”评级。

风险提示：信息安全市场低于预期；安全手机项目低于预期。

卫士通三大财务预测表

资产负债表（百万元）	2016	2017E	2018E	2019E
流动资产	**2140.3**	**4433.3**	**5432.6**	**6736.5**
现金	523.5	2670.3	2802.8	3018.7
应收款项	1340.2	1394.4	2099.0	2951.1
存货	192.5	285.6	400.9	587.5
其他	84.1	83.0	129.9	179.2
非流动资产	**1509.2**	**1541.8**	**1546.1**	**1554.3**
长期股权投资	25.0	25.0	25.0	25.0
固定资产	1391.1	1424.0	1428.7	1437.2
无形资产	10.5	10.1	9.8	9.4
其他	82.6	82.6	82.6	82.6
资产总计	**3649.5**	**5975.1**	**6978.8**	**8290.7**
流动负债	**2026.4**	**1461.4**	**2178.1**	**3091.7**
短期借款	828.6	0.0	0.0	0.0
应付账款	801.8	921.4	1369.6	1951.1
其他	396.0	540.0	808.5	1140.6
非流动负债	**50.2**	**55.2**	**60.2**	**65.2**
长期借款	0.0	0.0	0.0	0.0
其他	50.2	55.2	60.2	65.2
负债总计	**2076.6**	**1516.7**	**2238.3**	**3156.9**
少数股东权益	83.8	83.8	83.8	83.8
归属母公司股东权益	1489.1	4374.7	4656.6	5050.0
负债和股东权益总计	**3649.5**	**5975.1**	**6978.8**	**8290.7**

现金流量表（百万元）	2016	2017E	2018E	2019E
经营活动现金流	-137.2	340.4	234.4	336.8
投资活动现金流	-634.1	-45.8	-83.9	-95.8
筹资活动现金流	733.3	1852.1	-18.0	-25.1
现金净增加额	-38.1	2146.8	132.5	215.9
企业自由现金流	-748.7	230.5	76.5	139.0

利润表（百万元）	2016	2017E	2018E	2019E
营业收入	**1798.9**	**2495.7**	**3542.6**	**5126.7**
营业成本	1164.8	1659.3	2340.2	3421.3
营业税金及附加	15.5	25.0	35.4	51.3
营业费用	177.3	249.6	354.3	512.7
管理费用	274.9	387.2	542.4	769.4
财务费用	5.6	-14.4	-41.3	-72.8
投资净收益	1.9	0.0	0.0	0.0
其他	-43.3	-14.7	-14.7	-14.7
营业利润	**119.5**	**174.5**	**297.1**	**430.2**
营业外净收支	76.5	55.8	40.0	40.0
利润总额	**196.1**	**230.2**	**337.1**	**470.2**
所得税费用	23.1	25.3	37.1	51.7
少数股东损益	17.2	0.0	0.0	0.0
归属母公司净利润	**155.8**	**204.9**	**300.0**	**418.5**
EBIT	170.7	175.0	270.8	372.4
EBITDA	200.0	220.6	335.4	445.1

重要财务与估值指标	2016	2017E	2018E	2019E
摊薄每股收益(元)	0.36	0.24	0.36	0.50
每股净资产(元)	3.44	5.22	5.56	6.03
发行在外股份(百万股)	432.5	837.6	837.6	837.6
ROIC(%)	7.9%	6.6%	10.3%	13.2%
ROE(%)	10.5%	4.7%	6.4%	8.3%
毛利率(%)	34.4%	32.5%	32.9%	32.3%
EBIT Margin(%)	9.5%	7.0%	7.6%	7.3%
销售净利率(%)	8.7%	8.2%	8.5%	8.2%
资产负债率(%)	56.9%	25.4%	32.1%	38.1%
收入增长率(%)	12.2%	38.7%	42.0%	44.7%
净利润增长率(%)	4.7%	31.5%	46.4%	39.5%

数据来源：Wind，东吴证券研究所

免责声明

东吴证券股份有限公司经中国证券监督管理委员会批准，已具备证券投资咨询业务资格。

本研究报告仅供东吴证券股份有限公司（以下简称“本公司”）的客户使用。本公司不会因接收人收到本报告而视其为客户。在任何情况下，本报告中的信息或所表述的意见并不构成对任何人的投资建议，本公司不对任何人因使用本报告中的内容所导致的损失负任何责任。在法律许可的情况下，东吴证券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并进行交易，还可能为这些公司提供投资银行服务或其他服务。

市场有风险，投资需谨慎。本报告是基于本公司分析师认为可靠且已公开的信息，本公司力求但不保证这些信息的准确性和完整性，也不保证文中观点或陈述不会发生任何变更，在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的报告。

东吴证券投资评级标准:

公司投资评级:

买入：预期未来 6 个月个股涨跌幅相对大盘在 15%以上;

增持：预期未来 6 个月个股涨跌幅相对大盘介于 5%与 15%之间;

中性：预期未来 6 个月个股涨跌幅相对大盘介于-5%与 5%之间;

减持：预期未来 6 个月个股涨跌幅相对大盘介于-15%与-5%之间;

卖出：预期未来 6 个月个股涨跌幅相对大盘在-15%以下。

行业投资评级:

增持：预期未来 6 个月内，行业指数相对强于大盘 5%以上;

中性：预期未来 6 个月内，行业指数相对大盘-5%与 5%;

减持：预期未来 6 个月内，行业指数相对弱于大盘 5%以上。

东吴证券研究所
苏州工业园区星阳街 5 号
邮政编码：215021
传真：（0512）62938527
公司网址：http://www.dwzq.com.cn