东兴证券 DONGXING SECURITIES

等保2.0出台在即 网安央企大力度混改

——“安全可靠工程半月谈”第一期

2019 年 05 月 13 日

看好/维持

国防军工 | 周期报告

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

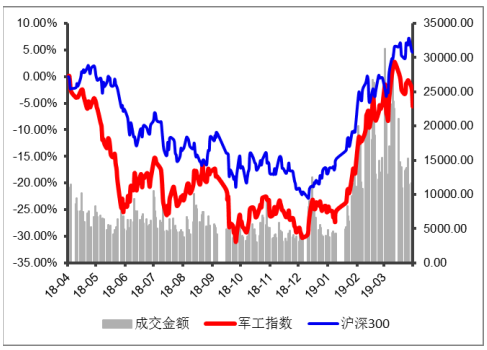
010-66554018 Zhangzq_yjs@dxzq.net.cn

执业证书编号: S1480117080010

细分行业	评级	动态
密码行业	看好	维持

行业基本资料		占比%
股票家数	53	1.46%
重点公司家数	3	
行业市值	8325.13 亿元	1.32%
流通市值	544.01 亿元	1.09%
行业平均市盈率	89.51	/
市场平均市盈率	16.54	/

行业指数走势图



资料来源：东兴证券研究所

相关研究报告

投资摘要：

中国电子 6.9 倍 PS 入股奇安信，中国电科网安公司混改值得关注。中国电子以 37.31 亿元持有奇安信 22.59%股份，接替三六零成为奇安信第二大股东，PS 估值 6.9 倍，PE 估值 100 倍。按照网络安全行业平均 PS 8.25 倍来看，叠加网络安全央企身份，未来奇安信有望冲击 300 亿市值。此次混改体现了中国电子发力网络安全业务的决心，也为下一步信息安全领域混改释放积极信号。中国电子战略入股奇安信是战略投资，是国企与民企共同推动网络安全产业做大做强的一次重要实践。此前，中国电科整合下属 30 所、33 所等资产成立中国电子科技网络信息安全公司，一直以网安领域“国家队”的形象出现。在中国电子并购民营网安龙头公司后，中国电科网安公司的混改举动也值得关注。

等保 2.0 将于 5 月 13 日出台。有媒体报道称，我国将于 5 月 13 日发布网络安全等级保护技术 2.0 版本。等保 2.0 的管辖范围将大幅扩张，除个人及家庭自建自用的网络外其他都在管辖范围内，另外还新增了云计算、大数据、物联网、工控等新兴领域，整体市场规模经前瞻研究院预测到 2022 年约为 1157 亿，市场空间大大增加。同时，等保 2.0 还从网络安全保护、涉密网络系统安全防护、密码管理等层面用法律的形式确立了要求。等保 2.0 也带动了新兴领域和新技术应用的需求，威胁情报、态势感知等主动防御领域受益最大。

“PK 体系”不断扩大朋友圈，多家企业携手共建生态圈。中国电子举办现代数字城市“生态合作伙伴之夜”活动，重磅发布了多款基于飞腾 2000+CPU 的服务器产品，以及多项基于“PK 体系”的现代数字城市科技创新成果。随着对于国产核心技术关注度的增加，国产架构在不断扩大“朋友圈”，与越来越多的企业携手建设“生态圈”。

投资建议：CEC 入股奇安信完善了 PK 体系中网络安全板块，对 CEC 旗下**中国长城**开展安全可控业务有很大助益；等保 2.0 中对密码应用的要求利好网络攻防和密码龙头**卫士通**。

风险提示：

等保 2.0 落地速度不及预期，网络安全行业发展不及预期，自主可控业务发展不达预期。

行业重点公司盈利预测

简称	EPS（元）			PE			PB	评级
	18A	19E	20E	18A	19E	20E		
卫士通	0.19	0.65	0.96	156	45	31	5.63	强烈推荐
中国长城	0.34	0.44	0.56	27	21	16	4.35	强烈推荐

目录

表格目录

插图目录

1. CEC 战略入股奇安信，打造世界一流网络安全企业

中国电子入股奇安信，打造网络安全国家队。奇安信集团是中国最大的网络安全公司之一，专门为政府、军队、企业，教育、金融等机构和组织提供企业级网络安全技术、产品和服务，已覆盖 90%以上的中央政府部门、中央企业和大型银行，已在印度尼西亚、新加坡、加拿大、中国香港等国家和地区开展了安全业务。根据协议，中国电子以人民币 37.31 亿元持有奇安信 22.59%股份，接替三六零成为奇安信第二大股东，目前已经完成工商登记。这是近年来网络安全领域央企入股“民企”金额最高，也是规模最大的一次混改。此次混改将成为中国电子打造网络安全国家队的重要战略落地，同时也为下一步信息安全领域混改释放积极信号。

从三六零年报中可知，奇安信营业收入 24 亿，净利润 1.58 亿，净资产 54.85 亿，从此次入股情况可以推算出奇安信整体估值 165 亿左右，PS6.85，PE104。而与当前 A 股已上市网络安全公司进行横向比较，行业平均 PS 为 8.25，公司估值有望进一步提升。如果按照与之定位相同，且也是网络安全央企身份的卫士通的估值，其 PS 为 11.35，奇安信市值有望朝 300 亿进发。

表 1： A 股网络安全公司市值和估值情况

证券代码	证券简称	总市值	PE（TTM）	PS（TTM）
300659. SZ	中孚信息	47. 4479	123. 6380	12. 3785
002268. SZ	卫士通	221. 6560	174. 9826	11. 3570
002197. SZ	证通电子	48. 0126	-19. 9011	3. 6976
002912. SZ	中新赛克	102. 6540	52. 4771	14. 6943
300546. SZ	雄帝科技	37. 0409	30. 5683	5. 6673
300188. SZ	美亚柏科	136. 7907	48. 2094	8. 2279
603039. SH	泛微网络	99. 4851	83. 0510	9. 4554
300229. SZ	拓尔思	52. 7054	79. 2606	5. 9107
300579. SZ	数字认证	47. 4720	54. 5838	6. 8087
603232. SH	格尔软件	31. 3076	45. 8189	10. 0958
300369. SZ	绿盟科技	105. 6698	61. 3578	7. 7063
002439. SZ	启明星辰	239. 5066	46. 7679	9. 2964
300352. SZ	北信源	73. 0711	75. 6443	12. 2578
601360. SH	三六零	1, 440. 7438	38. 8934	11. 0149
300297. SZ	蓝盾股份	83. 4541	20. 8117	3. 8248
300333. SZ	兆日科技	33. 3648	275. 1225	15. 3725
300386. SZ	飞天诚信	47. 9915	36. 0039	4. 3243
300311. SZ	任子行	49. 0506	35. 3220	4. 1021
A 股行业平均			69	8. 25

数据来源：Wind

中国电子战略入股奇安信，不是简单的财务投资，而是战略投资。中国电子与奇安信分别在本质安全和过程安全领域具有较大优势。奇安信在漏洞处理技术等过程安全领域储备了深厚技术和人才；中国电子则在国产 CPU 市场占据一半的份额，双方合计占据 90%以上的国产操作系统市场。本质安全和过程安全深度融合是中国网络安全发展刻不容缓的课题。中国电子董事长、党组书记芮晓武表示，入股奇安信是战略性投资。一方面将带动奇安信跻身“国家队”行列，增强奇安信服务网络强国建设的战略定力，同时，有利于双方强化网络安全核心能力，加快迈向世界一流网信企业行列，全面提升服务网络强国建设的战略支撑力。

中国电子战略入股奇安信是国企与民企共同推动网络安全产业做大做强的一次重要实践。国企与民企的强强联合，有益于放大国有资本功能，释放民营企业的创新活力，实现国企与民企的取长补短、相互促进、共同发展。奇安信董事长齐向东表示，这次最核心的意义，就是让奇安信成为了正式的网络安全国家队。网络安全是个特殊的行业，一方面，漏洞技术是伴随着互联网发展的，核心技术主要掌握在民营的互联网安全公司手中；另一方面是特殊人才，网络攻防不走寻常路，是逆向思维，很多漏洞高手普遍学历不高，有强烈的个人特色，这样的特殊人才或被体制的高门槛拒之门外，或在体制内生存比较困难，因此有一句话叫“高手在民间”。如何在保障安全可控的基础上充分利用和调动民间力量，也成为建立我国信息安全防御体系的关键所在。

入股后双方将加强合作，争取领跑网络安全领域。随着我国面临日益严峻的国际网络空间形势，我们必须要全面提升防御和对抗能力。中国电子战略入股奇安信以后，将在技术创新、资源整合、重大项目建设等方面进行紧密深入的合作，把网络安全防御能力与操作系统等底层应用紧密结合，在网络安全非对称、颠覆性技术上集中攻关，尽快取得新的重大突破，争取实现‘领跑’，共同构筑更强大的网络安全防线。

2. CEC 亮相第二届数字中国建设峰会，与会企业携手共建“PK 体系”生态圈

2.1“PK 体系”不断扩大朋友圈，多家企业携手共建生态圈

一枝独放不是春，百花齐放春满园。5 月 8 日，第二届数字中国建设峰会在福州海峡国际会展中心落幕，本届展会上，中国电子联合来自国内电子信息行业的 70 余家企业，共同在三坊七巷郭柏荫故居举办现代数字城市 “生态合作伙伴之夜” 活动，重磅发布了多款基于飞腾 2000+ CPU 的服务器产品，以及多项基于 “PK 体系” 的现代数字城市科技创新成果。中国电子党组成员、副总经理陈锡明表示，目前以“飞腾 CPU+麒麟操作系统”为基础的“PK 体系”，尽管还与世界顶尖水平存在一定差距，但随着大家对于国产核心技术关注度的增加，国产架构在不断扩大“朋友圈”，与越来越多的企业携手建设“生态圈”。

图 1：“PK 体系”生态树

资料来源：搜狐网，东兴证券研究所

“PK 体系”不断发展完善，已有 400 余家企业融入。由飞腾 CPU 和银河麒麟 OS 联手打造的“PK 体系” 是国内最完整、最先进、最富有朝气的计算机基础软硬件架构。包括以 CPU、操作系统、BIOS、桥片等基础关键产品为代表的“基础生态”，以数据库、开发工具、驱动等系统软件为代表的“系统生态”，以办公应用系统、业务系统、安全系统、游戏应用为代表的“应用生态”。目前，已有 400 余家国内企业和单位融入 PK 体系，极大的推动了我国自主信息体系的建设步伐。

2.2 FT-2000+服务器产品群发布，擎天 DF720 整机性能表现优异

FT-2000+服务器产品群发布，另有多款基于飞腾平台的国产软硬件产品和解决方案一并发布，共同助力数字中国建设。FT-2000+/64 处理器芯片集成 64 个自主开发的 ARMv8 指令集兼容处理器内核 FTC662，采用片上并行系统（PSoC）体系结构。通过集成高效处理器核心、基于数据亲和的大规模一性存储架构、层次式二维 Mesh 互连网络，优化存储访问延时，提供业界领先的计算性能、访存带宽和 IO 扩展能力。在 ARMv8 指令集兼容的现有产品中，FT-2000+/64 在单核计算能力、单芯片并行性能、单芯片 cache 一致性规模、访存带宽等指标上处于国际先进水平。FT-2000+/64 主要应用于高性能、高吞吐率服务器领域，如对处理能力和吞吐能力要求很高的行业大型业务主机、高性能服务器系统和大型互联网数据中心等。

图 2：FT-2000+/64 主要技术指标

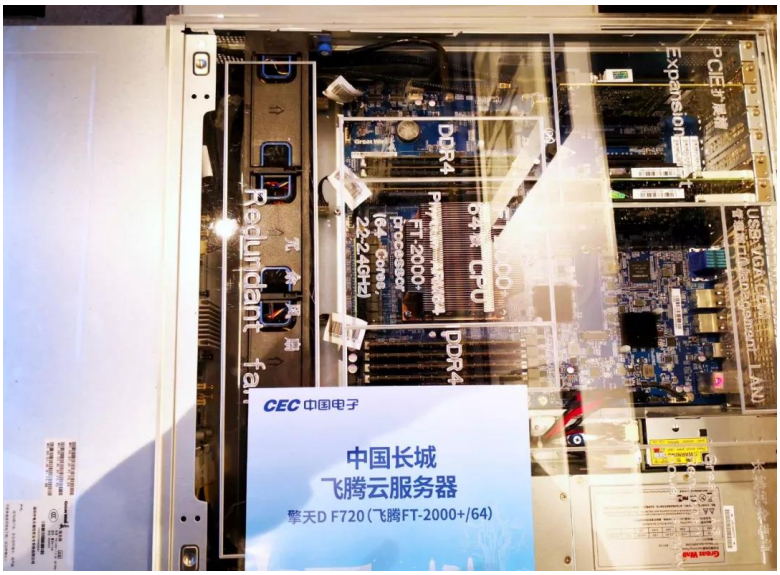
类别	参数
工艺特征	16nm工艺
核心	集成64个FTC662处理器核
主频	工作主频2.2GHz~2.4GHz
缓存	集成32MB二级cache
存储器接口	集成8个DDR4存储控制器，可提供204.8GB/s访存带宽
PCIE接口	集成33个PCIE3.0接口
功耗	典型功耗100W
封装	FCBGA封装，引脚个数3576

资料来源：公司官网，东兴证券研究所

本次活动中，包括联想、浪潮、紫光、航天科工、中国长城在内的多家国内顶尖服务器厂商发布了基于飞腾 2000+ CPU 的国产高性能服务器产品。阿里云发布了基于中国电子飞腾 1500A 和 2000+构建的阿里专有云安可敏捷标准云计算平台，该云平台已经在全国的一些省市进行实际部署和应用。腾讯云发布了基于飞腾硬件平台的腾讯云 TStack。过去的 20 年里，腾讯在海量数据处理、大流量接入、高性能高并发的处理模型，以及大规模服务器运营上积累了丰富经验。今天与中国电子发布腾讯云 TStack，就是希望把腾讯多年的积累经验输出到中国自主研发的芯片和操作系统中，让国产电子信息技术能力快速发展，结出丰硕果实。此次活动中，还有来自奇安信、同有、冠捷、启明星辰、金山、绿盟、用友、金蝶等合作伙伴的多款基于飞腾平台的国产软硬件产品和解决方案一并发布，共同助力数字中国建设。

中国长城擎天 DF720 整机性能表现优异，能够满足多种应用场景需求。中国长城展出的擎天 DF720 服务器，是基于飞腾 FT-2000+高性能处理器、中文化 BIOS 和银河麒麟操作系统的通用机架式服务器。支持 8 通道 DDR4，12 个 3.5 寸热插拔硬盘，具备多个 USB、VGA、SATA、PCIE 等类型数据接口，支持远程管控，KVM Over IP 等功能。与上一代产品相比，擎天 DF720 采用 64 核，最高主频达到 2.4GHz，整体性能是原先的 5.8 倍，内存总容量可扩展到 512GB，整体存储容量可以达到 168TB，能够很好的满足现代数字城市和数据中心建设多样化扩展和存储需求。不仅如此，擎天 DF720 的整机能效也表现优异，相对于同等算力的 X86 平台，能耗降低 20%~40%，能大幅降低客户的 TCO。擎天 DF720 服务器主要面向政务、金融、医疗、交通、电力、档案、教育等国家重点行业信息系统和业务系统应用需求，适用于包含 ERP、数据库、云计算、虚拟化、分布式存储、业务处理等多种应用场景。

图 3：擎天 DF720



资料来源：公司官网，东兴证券研究所

2.3“PK 体系”助力实现“现代数字城市”，长城产品备受关注

CEC 提出“现代数字城市”理念，“PK 体系”产品及解决方案广受认可。峰会期间中国电子在 6 号馆用 400 多平米的参展最大展位，以“现代数字城市”为主题，从高安全信息基础设施、高安全数据平台、高安全数字应用三个“基础维度”，以及让政府管理更高效、让产业动能更强劲、让人民生活更美好三个“应用维度”，展出现代数字城市的理念和建设成果。在“现代数字城市”理念的支撑下，“PK 体系”产品及解决方案赢得了行业内的高度认可，已经成为企业合作的首选体系。数字中国峰会期间，中国建设银行宣布基于 PK 体系的商密自动化办公系统全面上线。该系统基于飞腾 CPU 和银河麒麟 OS 为核心的自主安全可控平台，率先在国内金融业中实现了办公自动化系统的软硬件全国产化替代。作为金融系统国产化替代的探索者，建行后续将持续优化升级，并探索依托“建行公有云”对外开放服务，提供行业办公自动化解决方案。中国联通宣布采用“PK 体系”实现自有系统的改造升级，未来将同中国电子共同为用户提供更加安全的网络基础设施服务，助力现代数字城市建设。另外，中国电子与中国联通、人民网、中国互联网投资基金，天津麒麟与中国金融电子化公司分别签署了战略合作协议，共同打造基于“PK 体系”的现代数字城市产品及解决方案，推动“PK 体系”用于通信行业信息技术创新、媒体融合发展以及互联网关键技术设施、国家金融安全等。

基于中国长城整机的现代数字城市解决方案备受关注。中国长城带来的产品与展示方案有中国长城飞腾云服务器擎天 DF720（飞腾 FT-2000+/64）、中国长城电竞专用机、中国长城档案信息一体化管理平台、公安交通智能管控集成应用平台、智能配用电大数据应用平台、智慧医疗平台。此外，中国长城还为本次峰会中国电子展位提供了台式机、一体机、笔记本、服务器等设备。

图 4：中国长城档案信息一体化管理平台

资料来源：公司官网，东兴证券研究所

中国长城档案信息一体化管理平台：该平台面向档案行业数字化建设，依照档案业务收、管、存、用四大方向，为档案馆（室）电子档案数据可信管理和安全存储提供技术支撑的一体化控制平台。主要包括：共性应用基础支撑平台、数字档案室系统、数字档案馆系统、电子档案长期保存库管理系统、电子档案综合利用系统和相关的应用支撑工具等。

图 5：公安交通智能管控集成应用平台

资料来源：公司官网，东兴证券研究所

公安交通智能管控集成应用平台：基于 PK 体系，采用人工智能技术实现车辆违法识

别，建立公安交通指挥、缉查布控智慧大脑，为公安交警执法推送实时、精准稽查布控信息，准确率达到 98%。包括黑名单车辆、无牌车、套牌车稽查，区间超速等车辆违法信息，极大地提升了公安交警缉查布控指挥调度行政执法质量和效率。

图 6：智能配用电大数据系统

资料来源：公司官网，东兴证券研究所

智能配用电大数据系统：基于 PK 体系，采用大数据和人工智能技术，对居民、工农业用电等信息深度挖掘，实现用电查询、分析，节电、用电预测和错峰调度等智能应用和数据服务，实现资源优化配置。

3. 等保 2.0 的前生今世

3.1 网络安全等级保护制度发展历程

我国于 1994 年确立计算机信息系统实行安全等级保护制度，并逐渐发展成熟，有力地保障了国家信息安全。2017 年 6 月 1 日开始实施《中华人民共和国网络安全法》，明确地将国家网络安全等级保护制度上升为法律要求。2018 年 6 月 27 日，《网络安全等级保护条例（征求意见稿）》的颁布和征求意见，既是健全完善相关法律规范体系的需要，也为解决等级保护现实问题提供契机，成为等级保护创新发展的驱动力，作为《网络安全法》重要配套制度的网络安全等级保护制度初现轮廓。

等级保护制度发展的三个阶段

随着云计算、大数据、人工智能等新技术、应用的发展，数据资产快速泛在化，传统安全防御边界被打破，信息资产安全面临前所未有的威胁。与此同时，等级保护工作持续健康发展，成为国家信息安全保护的基本制度。回顾我国等级保护制度的发展，大致可分为以下三个阶段。

- **第一阶段：等级保护确立和探索（1994~2006）。**该阶段从 1994 年确立计算机信息系统实行安全等级保护制度开始，到 2003 年等级保护从一项计算机信息系统安全保护制度提升至国家信息安全保障基本制度。2004 年至 2006 年，公安部联合

四部委开展了涉及 6 万余家单位，共 11 万余信息系统的等级保护基础调查和等级保护试点工作。通过摸底调查和试点，探索开展等级保护工作领导、组织、协调的模式和办法，营造等级保护工作的政策环境，为全面开展等级保护工作奠定了坚实的基础。

- **第二阶段：等级保护全面实施（2007~2017）。**2007 年正式启动实施等级保护工作，陆续出台等级保护基本要求、安全设计和测评要求等一系列标准，实现了完善测评体系、开展三级以上系统测评、建设整改等有关等级保护工作的阶段性目标。2010 年以后，金融、电力、教育、医疗、交通等行业监管部门和企事业单位陆续配套相关制度，全面贯彻执行等级保护工作，标志着我国信息安全等级保护工作全面展开，等级保护工作进入规模化推进阶段。

- **第三阶段：等级保护创新发展（2017 至今）。**2017 年 6 月 1 日，《中华人民共和国网络安全法》正式实施，明确将国家网络安全等级保护制度从我国的基本国策和基本制度上升为国家法律。网络安全等级保护的保护对象也发生了较大变化，原有的“信息系统”扩展成更广范围的“等级保护对象”，包括网络基础设施、信息系统、云计算平台、大数据、物联网和工业控制系统等。建立更为完善的等级保护体系，包括政策体系、标准体系、测评体系、技术体系、服务体系、关键技术研究体系、教育训练体系等。以等级保护为核心，构建包括安全监测、通报预警、快速处置、态势感知、安全防范、精确打击等为一体的国家关键信息基础设施安全保卫体系。

表 2：网络安全等级保护制度发展历程

时间	事件
1994 年	国务院颁布《中华人民共和国计算机信息系统安全保护条例》（国务院令 147 号），首次提出“计算机信息系统实行安全等级保护”概念
2003 年	中办、国办转发《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27 号）
2007 年	公安部会同国家保密局、国家密码管理局、国务院信息化工作办公室等四部委发布了《信息安全等级保护管理办法》，将信息安全等级保护工作写入法规中
2007 年	浙江省发布了《浙江省信息安全等级保护管理办法》，细化信息安全等级保护工作要求
2008 年	发布《GB/T22239-2008 信息安全技术 信息系统安全等级保护基本要求》，简称为等保 1.0，明确对于各等级信息系统的安全保护基本要求
2015 年	发布《公共安全业务连续性管理体系指南》，针对企业实施业务连续性管理体系中的方法和步骤给出了详细的指导
2016 年	全国人民代表大会常务委员发布《中华人民共和国网络安全法》，标志着网络空间安全治理方面从此有法可依
2017 年	信息安全等级保护制度改为网络安全等级保护制度
2018 年 6 月	公安部向社会发布了《网络安全等级保护条例（征求意见稿）》公开征求意见

资料来源：东兴证券研究所

网络安全等级保护制度是国家网络安全领域的基本国策、基本制度和基本方法。随着信息技术的发展和网络安全形势的变化，等级保护制度 2.0 在 1.0 的基础上，更加注重主动防御、动态防御、整体防控和精准防护，实现了对云计算、大数据、物联网、移动互联和工业控制信息系统等保护对象全覆盖，以及除个人及家庭自建网络之外的领域全覆盖。网络安全等级保护制度 2.0 国家标准的发布，对加强我国网络安全保障工作，提升网络安全保护能力具有重要意义。

图 7：等保 2.0 政策时间线

资料来源：东兴证券研究所

等级保护 2.0 的时代特征是要确保关键信息基础设施安全，重点对云计算、移动互联、物联网、工业控制以及大数据安全等进行全面安全防护，主要分为三个层面。一是，法律支撑，将我国的计算机系统等级保护条例提升为国家基础性法律制度，即“网络安全法”中的网络安全等级保护制度；二是，科学技术层面，由分层被动防护发展到了科学安全框架下的主动免疫防护；三是，工程应用层面，由传统的计算机系统防护转向了新型计算环境下的网络空间主动防护体系建设。

表 3：网络安全等级保护新标准具有三个特点

序号	特点
一	等级保护的基本要求、测评要求和设计技术要求框架统一，安全管理中心下的三重防护结构框架
二	通用安全要求+新型应用安全扩展要求,将云计算、移动互联、物联网、工业控制系统列入标准规范
三	把可信验证列入各级别和各环节的主要功能要求。

资料来源：东兴证券研究所

主管、监管部门：中央网络安全和信息化领导机构统一领导网络安全等级保护工作。国家网信部门负责网络安全等级保护工作的统筹协调。国务院公安部门主管网络安全等级保护工作，负责网络安全等级保护工作的监督管理，依法组织开展网络安全保卫。国家保密行政管理部门主管涉密网络分级保护工作，负责网络安全等级保护工作中有关保密工作的监督管理。国家密码管理部门负责网络安全等级保护工作中有关密码管理工作的监督管理。国务院其他有关部门依照有关法律法规的规定，在各自职责范围内开展网络安全等级保护相关工作。县级以上地方人民政府依照本条例和有关法律法规规定，开展网络安全等级保护工作。

3.2 等保 2.0 VS 等保 1.0

3.2.1 等保 2.0 具有法律效力

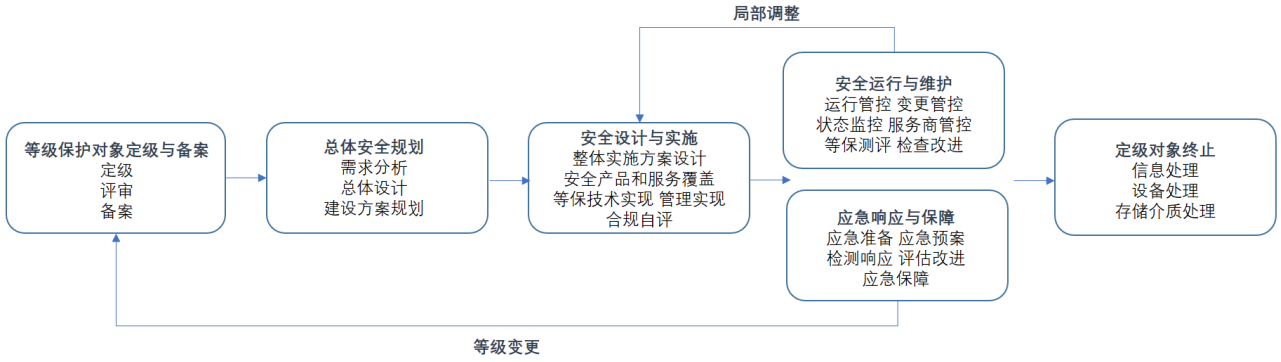
在自身法律效力和法律依据的效力位阶方面，等保 2.0 均优于等保 1.0。《等保办法》由公安部、国家保密局、国家密码管理局、国务院信息工作办公室共同发布，是等保 1.0 体系的核心规定，其法律效力为部门规范性文件。且根据《等保办法》第一条规定，其制定依据为国务院行政法规《计算机信息系统安全保护条例》。《等保条例》第一条规定了其制定依据为《网安法》与《保守国家秘密法》。根据《行政法规制定程序条例》第五条，行政法规的名称一般称“条例”，国务院各部门和地方人民政府制定的规章不得称“条例”，因此，《等保条例》应当属于行政法规范畴。综上可知，《等

保办法》为依据行政法规制定的部门规范性文件，而《等保条例》则属于依据国家法律制定的行政法规。

3.2.2 等级保护的工作内容和步骤的变动

等保 1.0 时代，等级保护工作由五个规定动作组成，定级、备案、建设整改、等级测评和监督检查。而在等保 2.0 时代，除了满足以上五个步骤，还把风险评估、安全监测、通报预警，案事件调查、数据防护、自主可控、供应链安全、效果评价、综治考核等方面的工作纳入到等级保护的范围之内。

图 8：等保 2.0 工作流程图



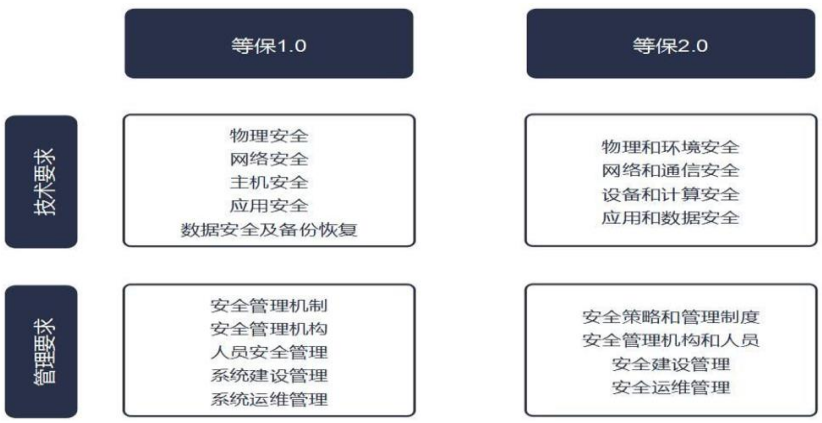
资料来源：e 安在线网站、东兴证券研究所

等保 1.0 偏重对于防护的要求，而随着当前网络安全形势的变化，等保 2.0 标准结合《网络安全法》中对于持续监测、威胁情报、快速响应类的要求提出了更加具体的措施。

3.2.3 技术要求和管理要求上的变动

等保 2.0 控制措施由旧标准的 10 个分类合并为 8 个分类，**技术部分：物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全；管理部分：安全策略和管理制度、安全管理机构和人员、安全建设管理、安全运维管理。**

图 9：等保 2.0 与等保 1.0 的技术要求和管理要求区分



资料来源：东兴证券研究所

此外，等保 2.0 在控制点要求上并没有明显增加，通过合并整合后相对旧标准略有缩减。

图 10：等保 2.0 与等保 1.0 控制点变化对比

旧标准	控制类	二级	三级	四级
技术要求	物理安全	10	10	10
	网络安全	6	7	7
	主机安全	6	7	9
	应用安全	7	9	11
	数据安全及备份恢复	3	3	3
管理要求	安全管理制度	3	3	3
	安全管理机构	5	5	5
	人员安全管理	5	5	5
	系统建设管理	9	11	11
	系统运维管理	12	13	13
合计	/	66	73	77
级差	/	/	7	4

等保2.0	控制类	二级	三级	四级
技术要求	物理和环境安全	10	10	10
	网络和通信安全	6	8	8
	设备和计算安全	6	6	6
	应用和数据安全	9	10	10
管理要求	安全策略和管理制度	4	4	4
	安全管理机构和人员	9	9	9
	安全建设管理	10	10	10
	安全运维管理	14	14	14
合计	/	68	71	71
级差	/	/	3	/

资料来源：深信服公司官网，东兴证券研究所

图 11：等保 2.0 与等保 1.0 要求项变化对比

方面	控制类	二级	三级	四级
技术要求	物理安全	19	32	33
	网络安全	18	33	32
	主机安全	19	32	36
	应用安全	19	31	36
	数据安全及备份恢复	4	8	11
管理要求	安全管理制度	7	11	14
	安全管理机构	9	20	20
	人员安全管理	11	16	18
	系统建设管理	28	45	48
	系统运维管理	42	62	70
合计	/	175	290	318
级差	/	/	115	28

方面	控制类	二级	三级	四级
技术要求	物理和环境安全	15	22	24
	网络和通信安全	16	33	35
	设备和计算安全	17	26	27
	应用和数据安全	22	34	38
管理要求	安全策略和管理制度	6	7	7
	安全管理机构和人员	16	26	29
	安全建设管理	25	34	35
	安全运维管理	31	49	51
合计	/	148	231	246
级差	/	/	83	15

资料来源：深信服公司官网，东兴证券研究所

4. 等保 2.0 条例解读与政策前瞻

等保 2.0 的诞生源自网络安全等级保护制度等立法层级不高、执行强制性差的现实情况。针对网络安全职能部门行政执法支撑不足等问题，中央领导同志就网络安全等级保护立法工作多次作出批示，要求加强等级保护立法工作，健全完善以保护国家关键信息基础设施安全为重点的网络安全等级保护制度。根据政策文件和中央领导指示精神，为落实《网络安全法》的规定，公安部牵头《网络安全等级保护条例（征求意见稿）》起草工作，共八章七十三条。按照工作惯例和工作职责，其中第三章“涉密网

络的安全保护”由国家保密局负责起草，第四章“密码管理”由国家密码管理局负责起草。主要内容包括：网络的安全保护、涉密网络的安全保护、密码管理。

4.1 网络的安全保护

《条例》第三章中规定了网络安全等级保护制度体系的基本框架、具体内容、要求和相关主体的责任义务。

一是，明确了网络运营者依法落实网络安全等级保护制度。按照《条例》规定开展网络定级、备案、测评、整改、自查工作，公安机关对网络分级监督管理的职责及其在备案审核、服务机构管理、事件调查、执法检查中的职责。《条例》中的内容与《关键信息基础设施保护条例（征求意见稿）》有关内容进行了协调衔接。

二是，规定了网络的定级和备案要求。根据网络在国家安全、经济建设、社会生活中的重要程度，以及其一旦遭到破坏、丧失功能或者数据被篡改、泄露、丢失、损毁后，对国家安全、社会秩序、公共利益以及相关公民、法人和其他组织的合法权益的危害程度等因素，网络分为五个安全保护等级。

表 4：安全保护等级划分

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第三级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

资料来源：《网络安全等级保护条例（征求意见稿）》

网络运营者或主管部门应参考 GA/T 1389-2017《信息安全技术 网络安全等级保护定级指南》的要求，梳理出定级对象并合理确定其所属网络的安全保护等级、确定其安全责任单位和具体责任人。需注意：网络运营者应当在规划设计阶段确定网络的安全保护等级；当网络功能、服务范围、服务对象和处理的数据等发生重大变化时，网络运营者应当依法变更网络的安全保护等级；网络定级应按照网络运营者拟定网络等级、专家评审、主管部门核准、公安机关审核的流程进行。对于基础网络、云计算平台和大数据平台等起支撑作用的网络系统，应根据其承载或将要承载的等级保护对象的重要程度确定其安全保护等级，原则上应不低于其承载的等级保护对象的安全保护等级。原则上大数据的安全等级不低于第三级。

三是，《条例》在《网络安全法》规定的网络运营者安全保护义务的基础上，对不同安全保护等级网络的运营者的安全保护义务做了明确、细化的要求。第二十条规定了网络运营者应当依法履行的 11 项一般性安全保护义务，包括落实责任制，建立并落实安全管理和技术保护制度，制定并落实机房安全管理、设备和介质安全管理等操作规范和工作流程，落实身份识别、防范恶意代码感染传播和网络入侵攻击的管理和技术措施，落实监测、记录网络运行状态、网络安全事件、违法犯罪活动的管理和技术措施，相关网络日志留存以及落实数据分类、重要数据备份和加密、个人信息保护措施，对网络中发生的案事件应当向属地公安机关报告等网络安全保护义务。第三级以

上网络的运营者，除履行上述网络安全保护义务之外，根据第二十二条规定，还应当履行的其他 8 项安全保护义务包括：强化网络安全管理机构的职责，重大事项逐级审批，网络安全管理负责人和关键岗位的人员安全背景审查，采取网络安全态势感知监测预警措施进行动态监测分析以及落实备份和恢复措施、定期开展等级测评等网络安全保护义务，突出强化了国家对关键信息基础设施和其他重要网络的重点保护和管理。

四是，规定了第三级以上网络运营者在开展技术维护、监测预警、信息通报、应急处置以及数据信息安全等工作时应当履行的责任义务。同时，《条例》中就测评服务、安全监测、运维、数据应用等其安全服务机构管理提出了明确的管理要求，提出了新技术新应用的风险管控规定。

4.2 关于涉密网络系统的安全保护

《条例》第四章中提出了涉密网络安全保密总体要求，以及涉密网络分级保护要求和涉密网络使用管理要求，明确了涉密网络全过程管理，规定了涉密网络密级确定、方案论证、建设实施、测评审查、风险评估、重大变化以及废止等环节的保密管理要求。

《条例》将涉密网络按照存储、处理、传输国家秘密的最高密级分为绝密级、机密级和秘密级。涉密网络运营者应当依法确定涉密网络的密级，通过本单位保密委员会（领导小组）的审定，并向同级保密行政管理部门备案。

对于涉密网络中使用的信息设备，应当从国家有关主管部门发布的涉密专用信息设备名录中选择；未纳入名录的，应选择政府采购目录中的产品。确需选用进口产品的，应当进行安全保密检测。

涉密网络运营者不得选用国家保密行政管理部门禁止使用或者政府采购主管部门禁止采购的产品。

涉密网络中使用的安全保密产品，应当通过国家保密行政管理部门设立的检测机构检测。计算机病毒防护产品应当选用取得计算机信息系统安全专用产品销售许可证的可靠产品，密码产品应当选用国家密码管理部门批准的产品。

4.3 密码管理

《条例》第五章中明确提出了密码配备使用、管理和应用安全性评估的有关要求，对网络的密码保护做出规定。其中，对涉密网络，明确密码检测、装备、采购、使用以及系统设计、运行维护、日常管理等要求；对非涉及国家秘密网络、第三级以上网络提出密码保护要求，明确规定网络运营者应在网络规划、建设和运行阶段委托专业测评机构开展密码应用安全性评估，并对评估结果备案提出了要求。

非涉密网络应当按照国家密码管理法律法规和标准的要求，使用密码技术、产品和服务。第三级以上网络应当采用密码保护，并使用国家密码管理部门认可的密码技术、产品和服务。

第三级以上网络运营者应在网络规划、建设和运行阶段，按照密码应用安全性评估管理办法和相关标准，委托密码应用安全性测评机构开展密码应用安全性评估。网络通

过评估后，方可上线运行，并在投入运行后，每年至少组织一次评估。密码应用安全性评估结果应当报受理备案的公安机关和所在地设区市的密码管理部门备案。

密码安全管理责任：网络运营者应当按照国家密码管理法规和相关管理要求，履行密码安全管理职责，加强密码安全制度建设，完善密码安全管理措施，规范密码使用行为。任何单位和个人不得利用密码从事危害国家安全、社会公共利益的活动，或者从事其他违法犯罪活动。

密码法草案、关键信息基础设施安全保护条例。5 月 11 日，国务院办公厅发布《国务院 2019 年立法工作计划》（以下简称“计划”），计划中明确的与网络安全相关的立法项目有：密码法草案（密码局起草）、未成年人网络保护条例（网信办起草）、公共安全视频图像信息系统管理条例（公安部起草）、关键信息基础设施安全保护条例（网信办、工业和信息化部、公安部起草）等。

5. 等保 2.0 带动新技术、新应用需求

5.1 等保 2.0 带动新兴领域安全需求

由于等保 2.0 较等保 1.0 范围更广、力度更大且对新兴领域安全提出要求，有望带动信息安全整体市场需求增加，其中受益最大的是威胁情报、态势感知、SOC 等主动防御领域、云安全、数据安全和工控安全等新兴安全领域和安全服务领域。

等级保护已经从原有的规定上升到了法律层面，等保 2.0 的执行力度和强制力度将加大。考虑到信息安全行业受政策影响大，等保 2.0 的推出将提高大家在信息安全投入的积极性，长期带动信息安全需求增加。等级保护首次加入“未知攻击”的检测、SOC 等主动防御的要求。以前信息安全以防火墙、杀病毒、IDS 等被动防御为主，随着安全威胁的升级，等保制度积极响应，提出主动防御上的要求，将有望带动威胁情报、态势感知、APT 攻击检测与防护和 SOC 等主动防御产品的需求增加。

信息系统除了需满足通用要求，还需满足云计算、移动互联、大数据、工业控制等领域的扩展要求。由于等保 2.0 相比于 1.0 保护对象范围进一步扩大，新增了移动互联、云计算、大数据、物联网和工业控制等新兴安全领域的内容和要求，相应的新兴安全领域需求将受政策出台推动带来需求增加。

等保 2.0 增加了外包运维管理的管理要求，侧面体现了等保 2.0 对安全服务的认可，预计政策也将带动安全服务的加速发展。

- 威胁情报：根据安全牛的估算，2017 年威胁情报的各种形态带来的收入为 5 亿到 8 亿元，约占整个安全市场的 1.25%到 2%。预计到 2020 年，威胁情报市场的规模有可能超过 12 亿元，复合增速在 24%左右。360 企业安全、思科、绿盟等厂商市场份额领先。

图 12：威胁情报细分领域矩阵

资料来源：安全牛、东兴证券研究所

图 13：态势感知细分领域矩阵

资料来源：安全牛、东兴证券研究所

- 态势感知：根据安全牛的统计，2017 年国内态势感知市场规模约计 20 亿人民币，占整个安全市场的 5%左右，预计到 2020 年，态势感知市场将达到 50 亿元左右，复合增速高达 36%。360 企业安全、安恒信息、华为、绿盟等厂商竞争力靠前。

- 云安全：根据 CCDI 的报告，2014-2016 年我国云安全市场规模分别为 9.8 亿元、12.8 亿元和 18.2 亿元，同比增速分别为 21.3%、30.6%和 42.2%，行业呈现爆发式增长趋势。阿里云、华为、腾讯云、360 企业安全等厂商竞争力靠前。

- 数据安全：数据安全起步较早，2016 年数据安全市场规模达 18.1 亿元，同比增长 21%，随着大数据产业的快速发展将催生数据安全需求不断增加，预计数据安全未来还将保持 20%以上增速增长。竞争格局方面，启明星辰、绿盟科技、天融信、神州泰岳和时代亿信等企业市场份额排名靠前。

- 工控安全：根据工信部发布的《工业控制系统信息安全行动计划(2018-2020 年)》的统计分析，预计 2018 年国内市场工控安全市场将达到 4.4 亿元，占全国信息安全市场规模的比重仅为 1%左右，仍处于市场导入期。考虑到全球工控安全占整体市场规模的 10%左右，随着未来几年在国家政策的持续推动，我国工控安全市场逐步升温，并有望在未来 3~5 年进入快速成长期。根据国家工业信息安全发展研究中心预计，5 年后，我国工控安全市场规模将达到约 20 亿~30 亿元,占信息安全市场规模的比重将达到 5%~6%左右。工控安全领域启明星辰、360 企业安全等企业布局领先。

5.2 等保 2.0 对新技术和新应用的要求标准

等保 2.0 在制定之初就充分考虑移动互联、云计算、物联网和工业控制等新技术和新应用，从应用领域到保护对象等各方面都进行了扩展。同时为了配合《中华人民共和国网络安全法》的实施，等保 2.0 针对共性安全保护需求提出安全通用要求；针对移

动互联、云计算、物联网和工业控制等新技术、新应用领域的个性安全保护需求提出安全扩展要求，以此形成新的网络安全等级保护基本要求标准。

5.2.1 云计算

云计算系统是等级保护重点要关注的一个领域。需要对云计算环境中的安全责任进行明确，不同的服务模式下，不同责任主体的责任也是不同的。云服务商，云租户的责任划分需要明晰。数据安全防护，无论 IaaS、PaaS 到 SaaS，对于云租户来讲，是始终要面对的一个很重要的问题。

图 14：三种服务模式下责任划分情况

资料来源：深信服公司官网，东兴证券研究所

- IaaS 服务下，云服务方责任硬件及虚拟化层的防护；虚拟化以上的客户机的安全防护，数据库防护以及中间件和应用及数据的防护，这都是租户需要去面对的问题。
- PaaS 服务模式下，客户虚拟机的安全防护责任交给了云服务商，云租户关心的是在这之上的，如软件开发平台中间件以及应用和数据本身的安全防护。
- SaaS 服务模式下，进一步上移，这个时候作为租户来讲他需要关心的其实就是跟一些应用的简单的安全配置相关了，以及数据安全的防护，这都是租户需要考虑的内容了。

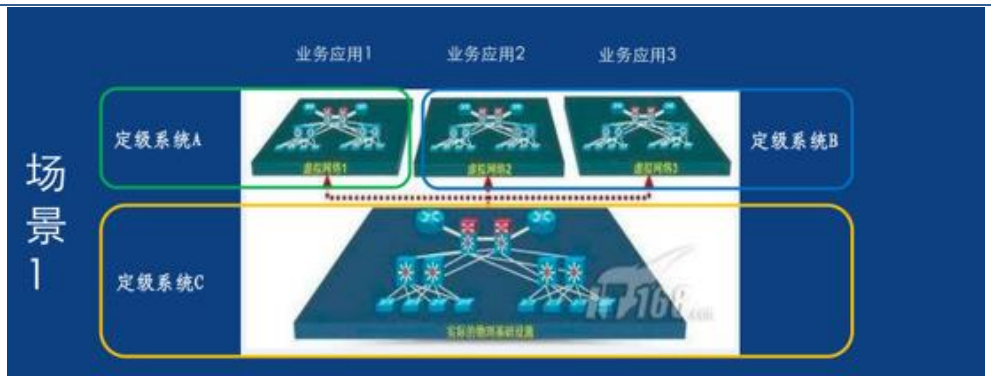
（1）系统的定级

云的环境下，把虚拟边界作为系统定级的变界。定级需要从业务应用的角度出发，梳理不同业务应用及对应的模块。传统的信息系统，强调分区分域、纵深防御，网络架构伴随业务变化而变化，系统各组件能与硬件紧耦合。信息系统的系统划分其实是以

物理网络/安全设备为边界的硬件设备的划分。而云计算系统网络架构具有扁平化的特征，业务应用系统与硬平台松耦合。信息系统的系统划分，单纯的以物理网络/安全设备为边界的划分方法无法体现出业务应用系统的逻辑关系，无法体现对业务信息安全和系统服务安全。有两种常见场景：

场景 1：若每种应用都需要使用物理基础支撑平台，业务应用系统则可不包含基础支撑的物理硬件部分。根据业务应用的关联性，进行切分定级。许多公共云就是这种状态，如果定级系统 C 的运行主体是云服务商的话，上面就是云租户的业务应用系统。

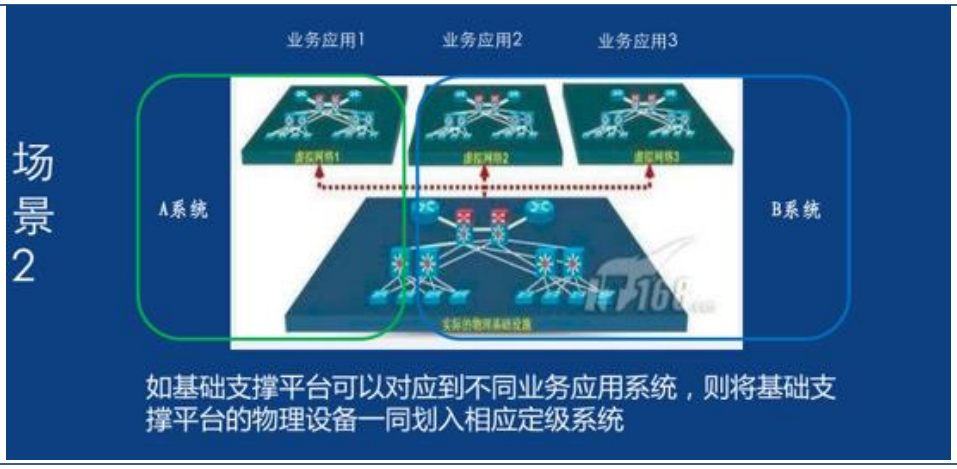
图 15：云环境下常见场景 1



资料来源：REEBUF，东兴证券研究所

场景 2：若基础支撑平台可以对应到不同业务应用系统，则将基础支撑平台的物理设备一同划入相应定级系统。业务应用可以与硬件平台有对应关系，比如某个应用固定的使用一堆的硬件服务器，独立成一个平台，则可以将其视作一个单独的定级系统。也可以在定级系统 B 向下切分，成为另一朵小云。下面是云平台，上面是承载的业务应用系统，就是云租户的系统。

图 16：云环境下常见场景 2



资料来源：REEBUF，东兴证券研究所

（2）备案

由于传统的系统的 IT 基础设施、运维地点、工商注册地基本上都是一致的，因此可以直接去所在地市局、网安或者是分局去备案。但是云服务商的工商注册地、办公地点大都不同。如阿里云，注册地在北京，运维地点在杭州，机房遍布全国各地。因此对于云上的系统，不管是云平台还是云租户，均以运维人员的所在地为备案地点，方便监管、证据固定、数据采集。

（3）建设整改

- 统一思维去考量，统一认证、统一账户管理、统一授权，统一安全审计。其中关于安全审计方面，标准条款里有明确要求，主机的安全审计、网络的审计、数据库的安全审计都必不可少。
- 侧重动态监测预警、快速应急响应能力建设以及服务安全产品合规，如果想自己搭一个私有云的话，那么建议一定要有这样的能力。
- 重点保护的就是业务数据安全和用户的隐私安全。数据安全这块真的是很重要。我们在安全扩展里有明确要求，一个是数据库的安全审计。要求云服务商开放第三方接口，支持第三方的安全审计的产品接入；还有一个就是对于云租户，同样要求要有自己的审计。在做云租户的系统检查或者测评的时候，一样要看你有没有做安全审计。

5.2.2 物联网

随着物联网的发展，安全问题日益突出。物联网是近年来快速发展的新技术之一。车联网、智慧城市、安防监控、共享单车、能源电力、远程抄表等各个行业，都有物联网应用。为了简化，将物联网分为感知层、平台层、应用层和网络层。物联网的各个层次，都有对应的安全威胁。

图 17：物联网各层次安全威胁

资料来源：安全牛，东兴证券研究所

等保 2.0 物联网部分主要扩展了感知层的安全要求。物联网的定义，就是由各种感知设备组成的网络。等保 2.0 物联网部分在物理和环境安全、网络和通讯安全、设备和计算安全，以及应用和数据安全做了扩展要求。

表 5：等保 2.0 物联网扩展要求

类别	子类	第一级	第二级	第三级	第四级
物理和环境安全	感知节点设备物理防护	增加	增加	增加	增加
网络和通讯安全	入侵防范		增加	增加	增加
	接入控制	增加	增加	增加	增加
设备和计算安全	感知节点设备安全			增加	增加
	网关节点设备安全			增加	增加
应用和数据安全	抗数据重放			增加	增加
	数据融合处理			增加	增加

资料来源：安全牛，东兴证券研究所

表 6：物联网扩展要求细则

感知节点设备物理防护	感知节点设备所处的物理环境应不对感知节点设备造成物理破坏，如挤压、强振动；
	感知节点设备在工作状态所处物理环境应能正确反映环境状态（如温湿度传感器不能装在阳光直射区域）；
	感知节点设备在工作状态所处物理环境应不对感知节点设备的正常工作造成影响，如强干扰、阻挡屏蔽等；
	关键感知节点设备应具有可供长时间工作的电力供应（关键网关节点设备应具有持久的，稳定的电力供应能力）
入侵防范	应能够限制与感知节点通信的目标地址，以避免对陌生地址的攻击
	应能够限制与网关节点通信的目标地址，以避免对陌生地址的攻击行为
	应确保只有授权的感知节点可以接入
感知节点设备安全	应保证只有授权的用户可以对感知节点设备上的软件应用进行配置或变更
	应具有对其连接的网关节点设备（包括读卡器）设备进行身份标识和鉴别的能力
	应具有对其连接的其他感知节点设备（包括路由节点）进行身份标识和鉴别的能力
网关节点设备安全	应设置最大并发连接数
	应具备对合法连接设备（包括终端节点、路由节点、数据处理中心）进行标识和鉴别的能力
	应具有过滤非法节点和伪造节点所发送的数据的能力
	授权用户应能够在设备使用过程中对关键密钥进行在线更新
	授权用户应能够在设备使用过程中对关键配置参数进行在线更新
抗数据重放	应能够鉴别数据的新鲜性，避免历史数据的重放攻击
	应能够鉴别历史数据的非法修改，避免数据的修改重放攻击
数据融合处理	应对来自传感网的数据进行数据融合处理，使不同种类的数据可以在同一个平台被使用
	应对不同数据之间的依赖关系和制约关系等进行智能处理，如一类数据达到某个门限

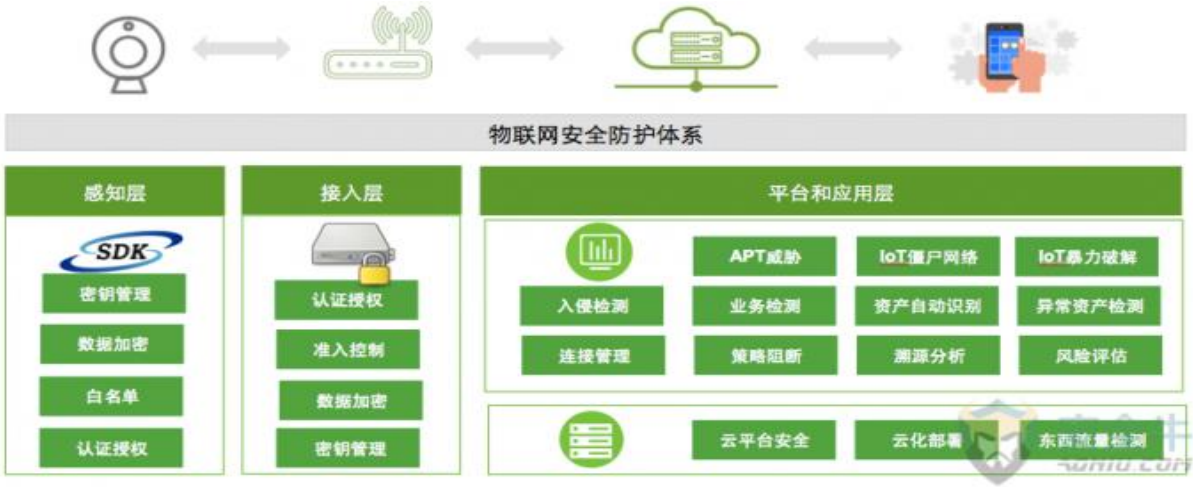
时可以影响对另一类数据采集终端的管理指令。

资料来源：安全牛，东兴证券研究所

等保 2.0 物联网扩展要求，大部分条款是针对感知节点，然而，标准强调物联网系统定级的整体性，“物联网应作为一个整体对象定级”。因此，物联网安全需要体系化建设，需要涵盖物联网的感知层、平台层、应用层和网络层。物联网安全防护体系，既包括等保 2.0 中所要求的传统安全，也能涵盖扩展后对感知设备层面的安全要求。

绿盟科技物联网安全解决方案，包括感知设备的威胁防护，持续的漏洞评估，以及安全态势，特别针对等保 2.0 物联网扩展要求，对物联网感知设备漏洞和威胁全面防护的整体安全解决方案。

图 18：物联网安全防护体系



资料来源：安全牛、东兴证券研究所

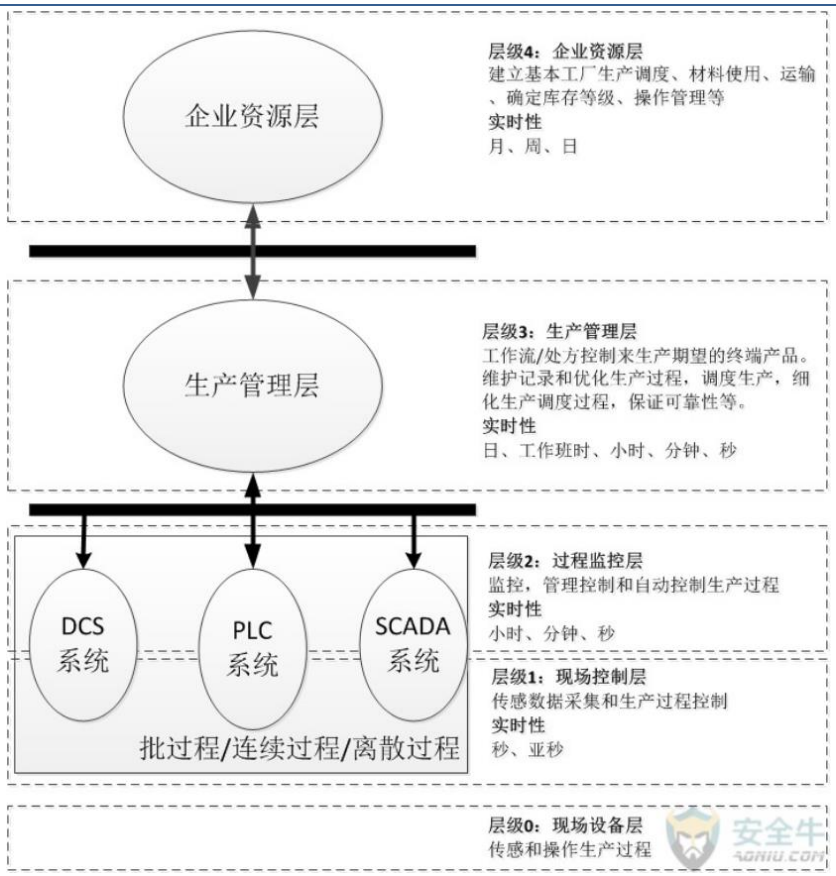
5.2.3 工业控制

工业控制系统（ICS）是几种类型控制系统的总称，包括数据采集与监视控制系统（SCADA）系统、集散控制系统（DCS）和其它控制系统，如在工业部门和关键基础设施中经常使用的可编程逻辑控制器（PLC）。工业控制系统通常用于诸如电力、水和污水处理、石油和天然气、化工、交通运输、制药、纸浆和造纸、食品和饮料以及离散制造（如汽车、航空航天和耐用品）等行业。工业控制系统主要由过程级、操作级以及各级之间和内部的通信网络构成，对于大规模的控制系统，也包括管理级。过程级包括被控对象、现场控制设备和测量仪表等，操作级包括工程师和操作员站、人机界面和组态软件、控制服务器等，管理级包括生产管理系统和企业资源系统等，通信网络包括商用以太网、工业以太网、现场总线等。

该标准参考 IEC 62264-1 的层次结构模型划分，同时将 SCADA 系统、DCS 系统和 PLC 系统等模型的共性进行抽象，形成了分层架构模型，从上到下共分为 5 个层级，依次为企业资源层、生产管理层、过程监控层、现场控制层和现场设备层，不同层级的实时性要求不同。

- 企业资源层主要包括 ERP 系统功能单元，用于为企业决策层员工提供决策运行手段；
- 生产管理层主要包括 MES 系统功能单元，用于对生产过程进行管理，如制造数据管理、生产调度管理等；
- 过程监控层主要包括监控服务器与 HMI 系统功能单元，用于对生产过程数据进行采集与监控，并利用 HMI 系统实现人机交互；
- 现场控制层主要包括各类控制器单元，如 PLC、DCS 控制单元等，用于对各执行设备进行控制；
- 现场设备层主要包括各类过程传感设备与执行设备单元，用于对生产过程进行感知与操作。

图 19：工业控制系统典型分层架构模型



资料来源：安全牛，东兴证券研究所

根据工业控制系统的架构模型不同层次的业务应用、实时性要求以及不同层次之间的通信协议不同，需要部署的工控安全产品或解决方案有所差异，尤其是涉及工控协议通信的边界需要部署工控安全产品进行防护，不仅支持对工控协议细粒度的访问控制，同时满足各层次对实时性的要求。

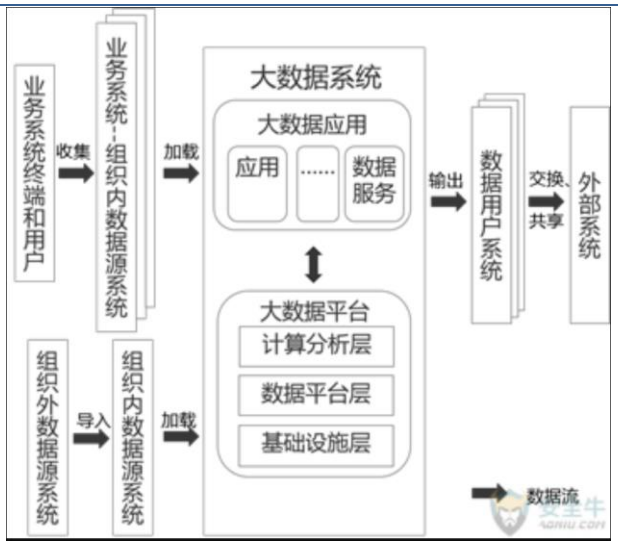
工业控制系统安全扩展要求：

- **物理和环境安全：**增加了对室外控制设备的安全防护要求，如放置控制设备的箱体或装置以及控制设备周围的环境；
- **网络和通信安全：**增加了适配于工业控制系统网络环境的网络架构安全防护要求、通信传输要求以及访问控制要求，增加了拨号使用控制和无线使用控制的要求；
- **设备和计算安全：**增加了对控制设备的安全要求，控制设备主要是应用到工业控制系统当中执行控制逻辑和数据采集功能的实时控制器设备，如 PLC、DCS 控制器等；
- **安全建设管理：**增加了产品采购和使用和软件外包方面的要求，主要针对工控设备和工控专用信息安全产品的要求，以及工业控制系统软件外包时有关保密和专业性的要求；
- **安全运维管理：**调整了漏洞和风险管理、恶意代码防范管理和安全事件处置方面的需求，更加适配工业场景应用和工业控制系统。

5.2.4 大数据

大数据系统通常由大数据平台和大数据应用构成。大数据平台为其支撑的大数据应用提供资源和服务的支撑集成环境。其中，基础设施层提供物理或虚拟的计算、网络和存储能力；数据平台层提供结构化和非结构化数据的物理存储、逻辑存储能力；计算分析层提供处理大量、高速、多样和多变数据的分析计算能力。大数据应用完成数据采集、处理、存储、分析和展示功能，运用综合知识为数据创造价值。

图 20：大数据系统



资料来源：安全牛，东兴证券研究所

大数据的采集、应用、传输等过程涉及到组织内、外其他的业务系统，这些业务系统包括为大数据系统提供原始数据的数据源系统，也包括数据用户系统，为保证在数据全生命周期中提供全程一致的数据安全保护。

大数据数据集合的特征是体量大、种类多、聚合快、价值高，受到破坏、泄露或篡改会对国家安全、社会秩序或公共利益造成影响，因此大数据安全保护的原则以数据为核心，提出针对不同安全保护等级大数据及其支撑系统安全保护扩展要求。

表 7：等保 2.0 对大数据应用安全的扩展要求

类别	子类	第一级	第二级	第三级	第四级
物理和环境安全	物理访问控制	/	增加	增加	增加
网络和通信安全	网络架构	/	/	增加	增加
设备和计算安全	访问控制	/	增加	增加	增加
	入侵防范	/	增加	增加	增加
	资源控制	/	增加	增加	增加
应用和数据要求	身份鉴别	增加	增加	增加	增加
	访问控制	/	增加	增加	增加
	安全审计	/	增加	增加	增加
	数据应用	增加	增加	增加	增加
	数据保密性	/	/	增加	增加
	数据完整性	增加	增加	增加	增加
	数据备份恢复	增加	增加	增加	
	数据溯源	/	/	增加	增加
	剩余信息保护	/	增加	增加	增加

资料来源：安全牛、东兴证券研究所

- **物理和环境安全对物理访问加以控制。**要求大数据存储设备必须在中国境内；数据分析设备必须在中国境内；数据清除或销毁必须在中国境内。
- **网络和通信安全对网络架构做出要求。**以保证大数据平台的管理流量与系统业务流量分离
- **设备和计算安全对访问控制、入侵防范、资源控制加以限制。**要求大数据平台应具备授权控制和数据分类分级功能；大数据应用对数据资源必须做授权，及分类分级保护。分布式系统完整性检测，提供告警和恢复；数据副本完整性检测，提供告警和恢复；自动识别检测仿造的虚假节点。集中管控平台——计算和存储资源使用状况；对数据资源的隔离与控制；对资源运维过程不能影响正常业务运行。
- **应用和数据要求。**数据采集、导出实施**身份鉴别**。大数据平台提供细粒度的访问控制策略，采用技术包括：分类分级、数据标记；控制对象包括：实施数据、调用接口；控制行为包括：采集、处理、关联。**安全审计，**时钟同步——保证审计的正确性；集中审计、隔离存放——降低失窃风险；大数据应用应能审计到大数据平台对其资源的操作。**数据应用，**包括鉴别数据、重要业务数据、重要个人信息。**数据保密性，**采集终端留存的重要个人信息的保密性。**数据完整性，**整体数据迁移，并保

证完整性。**数据备份恢复**，数据一致性：与原数据、多副本数据；数据可用性：备份的重要业务数据；异地实时备份。**数据溯源**，溯源数据完整性、合规性、真实性、保密性、可重现。**剩余信息保护**，在数据整体迁移的过程中，应杜绝数据残留。

6. 重点推荐：卫士通

6.1 深耕密码主业，打造党政军信息安全服务商

卫士通的主业是密码，具有国家资质核心竞争力，是公司最重要的护城河。信息安全基本是两类产品，一类是网络安全，本质是隔离，防止信息泄露。业务发展逻辑是动态的攻防过程，需要不断的技术迭代，是一个 know-how 的过程，此类厂商是启明星辰、深信服、360 等；另一类是信息被加密，即使泄露也无法读取，这类就是密码学，由国家指定，最核心的竞争力是资质，而卫士通恰恰具备这一资质，是上市公司中唯一的信息安全国家队。

6.1.1 央企安全运维

密码技术自主可控，基本形成网络信息安全产业链。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。 2015 年，卫士通收购了三零盛安、三零瑞通和三零嘉微，基本形成从芯片、产品到系统和应用的完整网络信息安全产业链，进一步增强市场竞争能力。从安全产品提供商到安全服务整体解决方案提供商，改变原有产品交付模式，提升整体防护水平的同时，运营管理费使收入更加平滑，有效提高毛利率水平。随着传统优质央企需求的转变，公司有望迎来新一轮增长。

卫士通打造“创新模式”“央企网络信息安全整体保障服务”，将网络信息安全规划、安全评估、安全设计、建设实施、安全运维、安全培训及人才培养等全生命周期安全保障过程统一纳入到安全服务范畴，为央企构建网络安全管控、安全防护、安全服务三大体系化的网络信息安全保障能力，提供“全托管”、“一站式”网络信息安全服务。

图 21：央企安全运维模型

资料来源：公司官网，东兴证券研究所

以电子政务市场为例，2018 年市场规模将超过 3000 亿，按照其中 IT 服务占总体投入的 30%的历史经验，其政务 IT 类服务的市场规模将达到千亿规模。凭借公司信息安全国家队的资质，公司有望在千亿级市场中取得不俗的市场份额。

公司完成央企网络安全总体方案，已经为招商局集团、中远海运等央企提供安全运维整体解决方案。仅考虑央企安全运维市场，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。

2019 年目标：招商局项目样板做完，人员到位，队伍经过锻炼，新董事长到位，今年计划做 10 家央企。按照招商局项目时间推算，19 年推广的十家央企能做完 70%，就有约 14 亿收入，20 年推广的 15 家央企能做完 70%，将有 23 亿收入。

6.1.2 网安飞天云

近年来我国政务云市场增长迅猛，超过工业、金融、互联网等其他行业，达到 292.6 亿元规模，预计未来几年政府会保持稳定投入，到 2021 年市场规模将达到 813.2 亿。**卫士通提出了政务云密码应用总体架构，采用国产商用密码在各个环节保证数据的完整性、机密性、不可抵赖和真实性，为政务云安全稳定运行提供全方位密码保障支撑。**

国内第一公有云平台与信息安全国家队第一品牌的强强联合。2018 年 5 月，公司控股股东中国网安与阿里云计算有限公司签署战略合作协议，携手打造国际先进、国内领先的“网安飞天”安全云平台品牌，构建国产自主可控安全云平台生态链。

网安飞天云是针对党政军、国有企业、大型民营企业的高安全私有云。在 2018 年获得试点订单，目前已调试完毕， 2019 年预计新增 5 处试点，利润率较高。党政军上云规模预计不低于 5000 朵云，按照安全服务 300 万的价格，市场规模将达到 150 亿。未来党政军自主可控安全云平台中取得更大市场份额，成为公司未来成长支柱之一。

与阿里云合作卡位安全云，成为党政军自主可控安全云平台生态链中优势地位。公司具备信息安全国家队资质优势以及在央企中网络安全先进的运维经验，有望结合阿里云的技术优势，在未来党政军自主可控安全云平台中取得更大市场份额。历史来看，公司于 2014 年安全集成服务从 1.65 亿跃升为 6.96 亿，与阿里云强强联合，有望在安全集成领域掀起另一轮高增长态势。党政军上云规模预计不低于 5000 朵云，如果安全服务按照 300 万的价格，其市场规模将达到 150 亿，助力公司新一轮业绩飞跃。

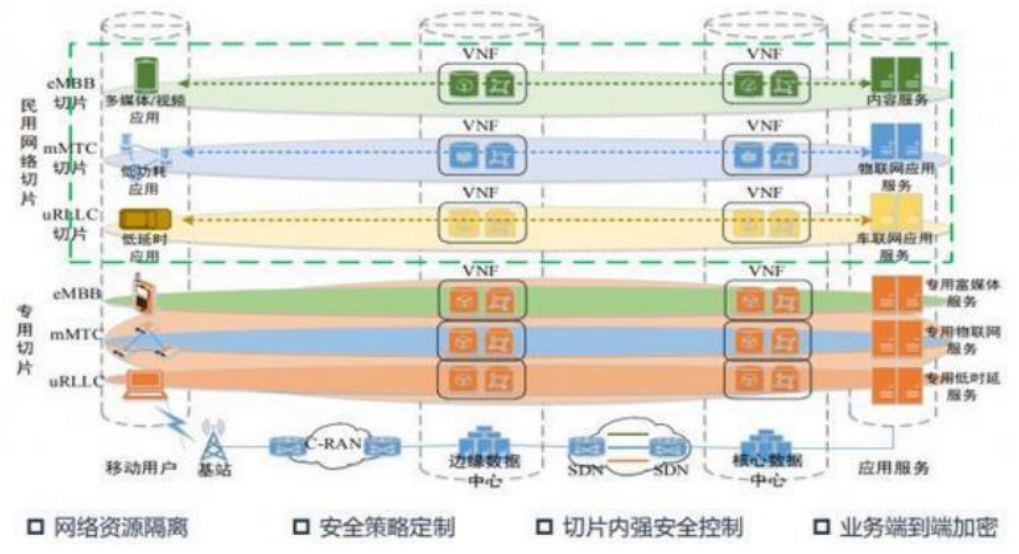
图 22：卫士云

资料来源：公司官网，东兴证券研究所

6.1.3 5G 专网

卫士通也是 5G 军用标准制定者，有望成为 5G 军用通信运营商，成功卡位未来网战主力。卫士通提前进行技术战略卡位，成立 5G 安全专项推进组，重点开展 5G 密码应用等研发，依托于密码技术这一核心优势，确立以密码为基础的统一信任体系，构建多元分立的数据防护模型,建立整体性的安全服务基础设施,形成面向垂直行业的 5G 安全解决方案，未来无疑会给企业带来积极影响。

图 23：5G 安全专网建设



资料来源：互联网，东兴证券研究所

6.2 等保 2.0 强化密码应用要求，卫士通拥抱新兴应用场景机遇

等保 2.0 强化了对自主可控的国产化商用密码应用的要求，并对新的应用场景做了更明确的安全要求。公司将努力抓住机遇，努力进入更多新行业，培育新的业务增长点；公司专注于政务云安全、政务云密码市场，参与了部分标准和指南的编制，争取更多的政务云应用落地。

7. 重点推荐：中国长城

7.1 金融领域自主可控趋势已成，公司具备先发优势并积极布局。

金融领域作为我国经济命脉主体，其 IT 国产化渗透率低，存在隐患。公司是金融信息化领域的重要供应商，金融智能网点解决方案国内市场占有率第一，是我国金融自助发卡机行业标准的制定者和引领者，区域银行市场订单实现翻倍增长，积极布局“3+2”海外业务，在保险、证券和政务行业领域取得突破。公司在金融领域成功实现基于 PK 架构产品的软件适配迁移，金融自助终端及其解决方案强化了安全可靠能力建设，基于国产硬件平台研发的跨端驱动平台和跨端应用平台，实现了驱动平台跨 Windows、Android 版本的开发与应用，支持现金、自助、发卡、回单、存单通用业务，并在多个项目上推广。未来基于飞腾的自主可控整机有望大规模进入金融领域，公司有望提供软硬件相关生态构建金融领域 IT 长城。

7.2 十三五计划剩余两年军工订单有望爆发，高新电子将充分受益。

高新电子业务专注于军事通信、海洋信息安全产业及军用计算机及网络等领域，是我军国防信息化系统解决方案和装备的重要提供商及服务商，陆军通信领域市占率高；海洋监测领域中高可靠大功率水声数字功放技术、阵列零浮力技术、深海阵列技术等多项技术实现突破，子公司圣非凡与株洲市政府和天易集团合作海洋信息安全产业基地，并且在一季度公司获得国家 3000 万补贴；在安全可靠网络交换、显示和国产化计算等领域，掌握“基于国产软硬件平台的网络交换”、“多网融合实时以太网交换”、“新一代机载图卡显示”、“液晶屏光学绑定”及“基于飞腾系列平台的核心计算主板研制”等关键及核心技术。十三五计划中，前两年由于军改拖累多个军工订单落地，圣非凡也因军改影响没有完成业绩对赌，但今明两年将是军工订单爆发年，公司也修改募投项目方向到智能单兵综合信息系统项目，看好公司军工业务后续发展。且公司入选国企改革“双百行动”名单，期待公司后续行动。

7.3 PK 体系坚定推动者，多点布局同时自身往美超微方向转型。

公司力争打造网络安全与信息化综合解决方案服务商，开展了与生态链龙头厂商的合作，在人工智能、大数据、云计算领域，率先形成 PK 体系（飞腾 CPU+麒麟 OS）的应用平台，与中国软件、百度、金蝶、科大讯飞、奔图等多家行业龙头企业展开生态合作完善 PK 体系应用，并形成行业信息化解决方案，基于飞腾平台的终端和服务器产品在国家某重点升级替代项目中占有率均为第一；，在金融、医疗等多个关键行业成功实现基于 PK 架构产品的软件适配迁移；成功打造多个精品工程项目，以 ERP 等复杂系统、大型系统以及融合云计算、大数据、人工智能等前沿技术的创新应用为核心的产业发展生态圈建设。倾力引进外部团队，打造自研 BIOS 和 BMC 固件能力，此举可以认为是为以后专注为飞腾做好主板业务，转型成飞腾的美超微，快速提升飞腾在我国自主可控领域的市占率，全力推广 PK 体系。且 CEC 已经入股奇安信，补足了 PK 生态体系中网络安全方面的短板。

8. 风险提示

等保 2.0 落地速度不及预期，网络安全行业发展不及预期，自主可控业务发展不达预期。

表 8：重点跟踪公司

公司名称	盈利预测				PE 估值			
	2017A	2018A	2019E	2020E	2017A	2018A	2019E	2020E
卫士通	0.20	0.19	0.65	0.96	148	156	45	31
中国长城	0.20	0.34	0.44	0.56	46	27	21	16

资料来源：东兴证券研究所

分析师简介

单击此处输入文字。

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，4 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。

单击此处输入文字。

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，市场有风险，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。