

2018年中国信息安全行业分析报告- 市场深度调研与发展前景研究

报告大纲

观研报告网

www.chinabaogao.com

一、报告简介

观研报告网发布的《2018年中国信息安全行业分析报告-市场深度调研与发展前景研究》涵盖行业最新数据，市场热点，政策规划，竞争情报，市场前景预测，投资策略等内容。更辅以大量直观的图表帮助本行业企业准确把握行业发展态势、市场商机动向、正确制定企业竞争战略和投资策略。本报告依据国家统计局、海关总署和国家信息中心等渠道发布的权威数据，以及我中心对本行业的实地调研，结合了行业所处的环境，从理论到实践、从宏观到微观等多个角度进行市场调研分析。

官网地址：<http://baogao.chinabaogao.com/xixinfuwu/328448328448.html>

报告价格：电子版: 7200元 纸介版：7200元 电子和纸介版: 7500

订购电话: 400-007-6266 010-86223221

电子邮箱: sale@chinabaogao.com

联系人: 客服

特别说明：本PDF目录为计算机程序生成，格式美观性可能有欠缺；实际报告排版规则、美观。

二、报告目录及图表目录

（一）行业技术状况

从技术角度来看，信息安全是对信息与信息系统固有属性的攻击与保护的过程。它围绕着信息系统、信息自身及信息利用的保密性、真实性、完整性、可靠性、可用性、不可否认性、可控性这七个核心安全属性，具体反映在物理安全、运行安全、数据安全、内容安全、信息内容对抗等五个层面上。

目前信息安全的主流安全技术包括信息系统自身的安全技术（物理安全和运行安全技术）、信息自身的安全技术（数据安全与内容安全技术）、信息利用的安全技术（信息对抗技术），具体如下：

图：目前信息安全的主流安全技术种类

（二）行业竞争格局

1、行业总体竞争格局

由于涉及国防安全和保密，国防网络信息安全行业进入壁垒较高，进而使得我国国防通讯和信息安全行业市场集中度较高。信息安全产品的提供方主要包括国家下属的科研院所、国有企业和少数民营企业，行业整体竞争程度相对较低。

（三）进入行业的主要壁垒

1、技术壁垒

军工技术取决于其可靠性，其次才是适用性和先进性。非军工企业进入军工行业，要对企业的生产设备、人员结构和管理方式进行相应的改进，实行国防网络标准和国家标准的双轨制。由于民用产品的技术指标和军品标准的差异，极易出现产品不符合要求的现象，一旦按照军品要求检验不合格，企业将承担相应的损失。

2、资质壁垒

国防网络信息安全产品因其应用领域的特殊性，出于保密技术安全的考虑，对承制单位实行生产许可管理。参与军品生产的企业必须获得“四证”，即武器装备科研生产许可证、装备承制单位注册证书、武器装备质量体系认证证书和保密资格单位证书。获得上述资质需要经过一套严格的审查程序，申请过程漫长，对于进入军品的民营企业是极大的挑战。业内参与产品研制的生产厂家主要是国内规模较大、实力雄厚的军工型科研院所、军工集团及少数具备军品供应资质的民营企业。

只有在完成自身体系、制度建设前提下，才有资格进行军工资质的申请，而且资格认证本身的长周期及先后顺序的规定与要求增加了认证的难度。因此，新进入者难以在短期内进入市场，参与竞争。

3、人才壁垒

国防网络信息安全行业属于技术密集型和知识密集型行业，只有掌握了其领域中的核心技术并拥有持续研究开发能力的技术团队，才能在该行业中处于有利地位。目前国内的军用

信息安全高端人才主要集中于大的安全厂商以及军队所属的研究机构，其共同特点是数量稀少、聘用成本较高、具有国防网络装备生产资质的企业普遍对其核心技术人员具有较强的管控能力。这使得新进入者在人才稀缺的情况下，无法在短期内突破研发领域中的技术难关，从而难以形成自身的技术或差异化优势。

（四）影响行业发展的有利和不利因素

1、有利因素

（1）信息安全已上升至国家战略的高度，行业面临良好政策环境，是行业快速成长的推动因素。

近年来，全球信息安全问题迭出，迫使政府和军队进一步重视网络信息安全问题，不断加大相关方面的投入。2013年6月，美国前中央情报局（CIA）雇员斯诺登披露了美国国家安全局（NSA）实施的“棱镜”项目，NSA和联邦调查局（FBI）直接进入美国网际网路公司的中心服务器里挖掘数据、收集情报。

该事件引爆国家、企业和个人对信息安全的重视。近年来，信息安全、云计算和大数据产业获得了国家战略层面的重视和支持。

2014年中共中央网络安全和信息化领导小组成立；2015年《网络安全法》发布，体现出网络安全对维护国家利益、推动信息化发展的重要作用，有助于提高全社会和各行业对网络安全的重视程度。信息安全对国家安全、经济发展的保障作用得到广泛认可，关键信息基础设施和政府信息系统普遍加强了网络安全防护体系的建设。面对日趋复杂的国际政治军事环境，国家和军队不断加大信息安全建设投入，这必将为国防网络通信和信息安全相关企业带来新的机遇、挑战和发展空间。

国家一直强调要健全信息安全保障体系，增强信息安全保障能力。2013年，《中共中央关于全面深化改革若干重大问题的决定》中提到了确保国家网络和信息安全。2015年8月，《国务院关于印发促进大数据发展行动纲要的通知》要求健全大数据安全保障体系，加强大数据环境下的网络安全问题研究和基于大数据的网络安全技术研究。本土信息安全行业在国家战略和相关政策的积极促进下，将迎来发展的重要契机与机遇。当前国家已经逐步出台一些可落实到操作层面上的政策，未来更多的细化政策有望出台，加速信息安全需求落地，全面利好产业发展。

（2）随着云计算和大数据技术不断发展，军队所面临的信息安全威胁不断演化，迫切需要安全防护体系和产品服务进行更新换代，市场空间可期。

随着军队的组织架构日趋完善，各种类型的安全设备、安全数据越来越多，传统的分析能力明显不足。为应对以高级持续威胁（APT）为代表的新型安全威胁，安全防护系统需要储存和分析更多的安全信息并且更加快速地做出判定和响应。这需要传统的安全防护体系做出变革，安全云和客户侧安全防护设备分工合作，在安全决策智能性、协同性和运营效率方面实现明显的提升。军事信息安全领域具备很强的对抗特征，安全防护体系、防护技术和产品、防护策略规则等都需要持续、及时升级换代，以应对高技术战争条件下进行信息化军事

斗争的需要。

(3) 军队信息化建设和信息战的发展，云计算、大数据、智能终端、移动通信等新信息技术的不断涌现，极大地推动数据流量的增长，带来新的网络安全产品需求，是驱动国防网络信息安全行业加速发展的基本因素。

信息化技术发展日新月异，云计算、大数据、智能终端、移动通信技术已广泛应用于国防信息化建设，随之而来的信息安全问题将更加突出，对信息安全产品提出了更为复杂的要求，催生云安全等新的信息安全应用领域。

中国军队的信息化建设正处于信息化全面发展的重要阶段。近年来，国防信息系统栅格化发展趋势明显，信息系统与指挥控制、武器平台及其他终端的融合不断加深。这一趋势对支持云计算、大数据的网络安全平台从功能上和性能上都提出了完全高于传统平台的新要求。

在国防领域，任何信息的传递都必须首先保证保密和安全，信息安全出现问题很可能导致严重的国家利益损失，因此，所有涉密网络都需要安全设备。此外，随着智能终端、移动通信设备功能性能的提升以及现代战争和军队办公对通信的机动性、实时性、便捷性提出更高要求，智能终端和移动通信设备在日常办公、作战指挥中的应用快速发展，其安全产品与技术应用具有很大的潜力和应用前景。

(4) 自主可控的安全保密平台需求不断增长以及国防网络信息安全产品核心软硬件国产化都推动了更新换代的新需求。

信息安全已成为左右国家政治命脉、经济发展、军事强弱和文化复兴的关键因素。构建完整、可靠的信息安全保障体系是一个复杂的系统工程，而自主可控的技术和产品则是信息安全的基石。

安全装备是军事网络安全和信息安全的核心环节，应用范围和数量呈逐年增长的态势。信息安全已上升到国家战略的高度，未来国家将通过政府采购或政策扶持等方式逐渐实现基础软硬件和重要IT 服务的国产化替代。军队也已明确要求军工安全产品必须采用国产芯片、软件，实现自主可控。因此，信息安全产品核心软硬件国产化将带来自主可控的信息安全装备平台的巨大需求。

(5) 国防和军队体制改革的不断深入，为民营军工企业的发展提供了巨大的发展空间。

随着科技产业革命和新军事变革的迅猛发展，国防经济与社会经济、军事技术与民用技术的界限趋于模糊，军民融合式发展已成为顺应世界新军事变革发展的大趋势。

新的“军改”政策下，部分科研院所也列入调整范围，这将意味着大量科研及装备生产任务将不再由军队承担，国防科研单位把工作重心放在了装备总体论证规划方面，大量装备的研制和生产交由地方工业部门和企业承担。

未来，随着军民融合的深度推进，具有强大研发实力、优秀管理团队、良好市场声誉的民营企业将迎来巨大的成长空间。我国政府正逐步有序向社会资本开放军工市场，这为我国

国防网络通信和信息安全相关企业带来了新的机遇和发展空间，整个行业面临较好的发展前景。

2、不利因素

不利因素

产业配套体系有待完善

虽然近几年我国信息安全市场快速发展，但与民用信息安全领域相比，国防网络信息安全领域产业链条不够完善。同时，由于信息安全产业整体发展程度有限，导致我国信息安全企业在高端人才吸引和新产品研发投入方面力度较为有限。因此，国防网络信息安全行业的发展在一定程度上依赖于产业链整体的发展和提升。

专业人才缺乏

信息安全产品的研制融合多学科的高精尖技术，对人员的技术要求高，人才培养周期长，导致了国内信息安全产品的研发人才队伍建设不能充分满足行业发展的需求，同时我国信息安全行业起步较晚，经验丰富、技术能力强的专业技术人才和管理人才较缺乏。随着国防建设的需要，国防网络信息安全产品市场规模稳步扩大增长，专业人才的缺乏问题矛盾将会更加突出。

（五）行业未来的发展趋势

移动互联网、物联网、云计算等技术的快速发展，一方面使得军事斗争所面临的信息安全形势愈发严峻，近年来频繁出现的信息安全事件给国家安全和军队的正常运作带来了大量的损失，信息安全愈发受到政府和军队的高度重视；另一方面，新技术也为维护国防网络信息安全提供了新的手段，从而也为国防网络信息安全行业带来了新的市场发展空间。

1、国防网络信息系统的合规及安全管理产品形成新的市场增长点，信息安全在国防网络信息系统中的核心战略地位和重要性日渐增强

随着国防和军队改革的逐步推进，与国防网络信息安全相关的政策和规范不断出台，国防网络信息系统对类似于检查评估、上网行为管理、安全审计等产品的需求持续增加。此外，在早期的安全加固、系统评估、值守呈现普遍化的情况下，国防网络信息系统在运行和维护过程中对于业务安全评估、安全度量、软件安全生命周期、SaaS（软件即服务）化安全的需求不断增强，形成了新的市场增长点。随着国家和行业政策、监管的不断加强，与国防网络信息系统相配套的合规和安全管理产品也会不断普及，从漏洞扫描延伸出的漏洞管理产品、基线核查产品和安全审计产品等都有较好的市场前景。

2、创新性的安全运维服务或云安全服务会成为国防网络信息安全领域的一个新兴增长点

单纯依靠产品无法彻底解决用户安全问题，用户更加关心厂商如何帮助他们解决问题。随着基于云计算的信息安全技术的发展，军队信息化建设所带来的信息安全意识的提升以及军工产品领域向民营企业的不断开放，未来安全运维服务以及云安全服务等创新性的服务会为军队用户提供更加完善、及时的服务。

3、信息安全产品向多功能化方向发展，集成的安全解决方案将成为用户首选

由于军队信息系统巨大的规模及其拓扑的复杂性，许多功能单一的信息安全产品越来越无法满足军队客户的信息安全保障需求。这将促使国防网络信息安全产品将向多功能化方向发展。

同时，由于国防网络信息系统待命时间长，担负的责任重大，因此需要尽量减少系统维护与调试的时间，对于持续性出现的新型安全威胁，军工客户普遍期望安全信息系统对于未来一段时期内可能出现的信息安全威胁提供一个预反应机制，以便能够全面解决军队所属组织机构安全管理、国防网络信息安全防护以及主动应对不断升级的威胁。

观研天下发布的《2018年中国信息安全行业分析报告-市场深度调研与发展前景研究》内容严谨、数据翔实，更辅以大量直观的图表帮助本行业企业准确把握行业发展动向、市场前景、正确制定企业竞争战略和投资策略。本报告依据国家统计局、海关总署和国家信息中心等渠道发布的权威数据，以及我中心对本行业的实地调研，结合了行业所处的环境，从理论到实践、从宏观到微观等多个角度进行市场调研分析。

它是业内企业、相关投资公司及政府部门准确把握行业发展趋势，洞悉行业竞争格局，规避经营和投资风险，制定正确竞争和投资战略决策的重要决策依据之一。本报告是全面了解行业以及对本行业进行投资不可或缺的重要工具。观研天下是国内知名的行业信息咨询机构，拥有资深的专家团队，多年来已经为上万家企业单位、咨询机构、金融机构、行业协会、个人投资者等提供了专业的行业分析报告，客户涵盖了华为、中国石油、中国电信、中国建筑、惠普、迪士尼等国内外行业领先企业，并得到了客户的广泛认可。

本研究报告数据主要采用国家统计局数据，海关总署，问卷调查数据，商务部采集数据等数据库。其中宏观经济数据主要来自国家统计局，部分行业统计数据主要来自国家统计局及市场调研数据，企业数据主要来自于国统计局规模企业统计数据库及信息安全交易所等，价格数据主要来自于各类市场监测数据库。本研究报告采用的行业分析方法包括波特五力模型分析法、SWOT分析法、信息安全T分析法，对行业进行全面的内外部环境分析，同时通过资深分析师对目前国家经济形势的走势以及市场发展趋势和当前行业热点分析，预测行业未来的发展方向、新兴热点、市场空间、技术趋势以及未来发展战略等。

【报告大纲】

第一章 2015-2017年中国信息安全行业发展概述

第一节 信息安全行业发展情况概述

- 一、信息安全行业相关定义
- 二、信息安全行业基本情况介绍
- 三、信息安全行业发展特点分析

第二节 中国信息安全行业上下游产业链分析

- 一、产业链模型原理介绍
- 二、信息安全行业产业链条分析
- 三、中国信息安全行业产业链环节分析
 - 1、上游产业
 - 2、下游产业

第三节 中国信息安全行业生命周期分析

- 一、信息安全行业生命周期理论概述
- 二、信息安全行业所属的生命周期分析

第四节 信息安全行业经济指标分析

- 一、信息安全行业的赢利性分析
- 二、信息安全行业的经济周期分析
- 三、信息安全行业附加值的提升空间分析

第五节 中国信息安全行业进入壁垒分析

- 一、信息安全行业资金壁垒分析
- 二、信息安全行业技术壁垒分析
- 三、信息安全行业人才壁垒分析
- 四、信息安全行业品牌壁垒分析
- 五、信息安全行业其他壁垒分析

第二章 2015-2017年全球信息安全行业市场发展现状分析

第一节 全球信息安全行业发展历程回顾

第二节 全球信息安全行业市场区域分布情况

第三节 亚洲信息安全行业地区市场分析

- 一、亚洲信息安全行业市场现状分析
- 二、亚洲信息安全行业市场规模与市场需求分析
- 三、亚洲信息安全行业市场前景分析

第四节 北美信息安全行业地区市场分析

- 一、北美信息安全行业市场现状分析
- 二、北美信息安全行业市场规模与市场需求分析
- 三、北美信息安全行业市场前景分析

第五节 欧盟信息安全行业地区市场分析

- 一、欧盟信息安全行业市场现状分析
- 二、欧盟信息安全行业市场规模与市场需求分析
- 三、欧盟信息安全行业市场前景分析

第六节 2018-2024年世界信息安全行业分布走势预测

第七节 2018-2024年全球信息安全行业市场规模预测

第三章 2015-2017年中国信息安全产业发展环境分析

第一节 我国宏观经济环境分析

一、中国GDP增长情况分析

二、工业经济发展形势分析

三、社会固定资产投资分析

四、全社会消费品零售总额

五、城乡居民收入增长分析

六、居民消费价格变化分析

七、对外贸易发展形势分析

第二节 中国信息安全行业政策环境分析

一、行业监管体制现状

二、行业主要政策法规

第三节 中国信息安全产业社会环境发展分析

一、人口环境分析

二、信息安全环境分析

三、文化环境分析

四、生态环境分析

五、消费观念分析

第四章 2015-2017年中国信息安全行业运行情况

第一节 中国信息安全行业发展状况情况介绍

一、行业发展历程回顾

二、行业创新情况分析

三、行业发展特点分析

第二节 中国信息安全行业市场规模分析

第三节 中国信息安全行业供应情况分析

第四节 中国信息安全行业需求情况分析

第五节 中国信息安全行业供需平衡分析

第六节 中国信息安全行业发展趋势分析

第五章 中国信息安全所属行业运行数据监测

第一节 中国信息安全所属行业总体规模分析

一、企业数量结构分析

二、行业资产规模分析

第二节 中国信息安全所属行业产销与费用分析

一、产成品分析

二、销售收入分析

三、负债分析

四、利润规模分析

五、产值分析

六、销售成本分析

七、销售费用分析

八、管理费用分析

九、财务费用分析

十、其他运营数据分析

第三节 中国信息安全所属行业财务指标分析

一、行业盈利能力分析

二、行业偿债能力分析

三、行业营运能力分析

四、行业发展能力分析

第六章 2015-2017年中国信息安全市场格局分析

第一节 中国信息安全行业竞争现状分析

一、中国信息安全行业竞争情况分析

二、中国信息安全行业主要品牌分析

第二节 中国信息安全行业集中度分析

一、中国信息安全行业市场集中度分析

二、中国信息安全行业企业集中度分析

第三节 中国信息安全行业存在的问题

第四节 中国信息安全行业解决问题的策略分析

第五节 中国信息安全行业竞争力分析

一、生产要素

二、需求条件

三、支援与相关产业

四、企业战略、结构与竞争状态

五、政府的作用

第七章 2015-2017年中国信息安全行业需求特点与价格走势分析

第一节 中国信息安全行业消费特点

第二节 中国信息安全行业消费偏好分析

一、需求偏好

二、价格偏好

三、品牌偏好

四、其他偏好

第二节 信息安全行业成本分析

第三节 信息安全行业价格影响因素分析

一、供需因素

二、成本因素

三、渠道因素

四、其他因素

第四节 中国信息安全行业价格现状分析

第五节 中国信息安全行业平均价格走势预测

一、中国信息安全行业价格影响因素

二、中国信息安全行业平均价格走势预测

三、中国信息安全行业平均价格增速预测

第八章 2015-2017年中国信息安全行业区域市场现状分析

第一节 中国信息安全行业区域市场规模分布

第二节 中国华东地信息安全市场分析

一、华东地区概述

二、华东地区经济环境分析

三、华东地区信息安全市场规模分析

四、华东地区信息安全市场规模预测

第三节 华中地区市场分析

一、华中地区概述

二、华中地区经济环境分析

三、华中地区信息安全市场规模分析

四、华中地区信息安全市场规模预测

第四节 华南地区市场分析

一、华南地区概述

二、华南地区经济环境分析

三、华南地区信息安全市场规模分析

第九章 2015-2017年中国信息安全行业竞争情况

第一节 中国信息安全行业竞争结构分析（波特五力模型）

- 一、现有企业间竞争
- 二、潜在进入者分析
- 三、替代品威胁分析
- 四、供应商议价能力
- 五、客户议价能力

第二节 中国信息安全行业SWOT分析

- 一、行业优势分析
- 二、行业劣势分析
- 三、行业机会分析
- 四、行业威胁分析

第三节 中国信息安全行业竞争环境分析（信息安全T）

- 一、政策环境
- 二、经济环境
- 三、社会环境
- 四、技术环境

第十章 信息安全行业企业分析（随数据更新有调整）

第一节 企业

- 一、企业概况
- 二、主营产品
- 三、运营情况
 - 1、主要经济指标情况
 - 2、企业盈利能力分析
 - 3、企业偿债能力分析
 - 4、企业运营能力分析
 - 5、企业成长能力分析
- 四、公司优劣势分析

第二节 企业

- 一、企业概况
- 二、主营产品
- 三、运营情况
 - 1、主要经济指标情况

2、企业盈利能力分析

3、企业偿债能力分析

4、企业运营能力分析

5、企业成长能力分析

四、公司优劣势分析

第三节 企业

一、企业概况

二、主营产品

三、运营情况

1、主要经济指标情况

2、企业盈利能力分析

3、企业偿债能力分析

4、企业运营能力分析

5、企业成长能力分析

四、公司优劣势分析

第四节 企业

一、企业概况

二、主营产品

三、运营情况

1、主要经济指标情况

2、企业盈利能力分析

3、企业偿债能力分析

4、企业运营能力分析

5、企业成长能力分析

四、公司优劣势分析

第五节 企业

一、企业概况

二、主营产品

三、运营情况

1、主要经济指标情况

2、企业盈利能力分析

3、企业偿债能力分析

4、企业运营能力分析

5、企业成长能力分析

四、公司优劣势分析

第十一章 2018-2024年中国信息安全行业发展前景分析与预测

第一节 中国信息安全行业未来发展前景分析

一、信息安全行业国内投资环境分析

二、中国信息安全行业市场机会分析

三、中国信息安全行业投资增速预测

第二节 中国信息安全行业未来发展趋势预测

第三节 中国信息安全行业市场发展预测

一、中国信息安全行业市场规模预测

二、中国信息安全行业市场规模增速预测

三、中国信息安全行业产值规模预测

四、中国信息安全行业产值增速预测

五、中国信息安全行业供需情况预测

第四节 中国信息安全行业盈利走势预测

一、中国信息安全行业毛利润同比增速预测

二、中国信息安全行业利润总额同比增速预测

第十二章 2018-2024年中国信息安全行业投资风险与营销分析

第一节 信息安全行业投资风险分析

一、信息安全行业政策风险分析

二、信息安全行业技术风险分析

三、信息安全行业竞争风险分析

四、信息安全行业其他风险分析

第二节 信息安全行业企业经营发展分析及建议

一、信息安全行业经营模式

二、信息安全行业销售模式

三、信息安全行业创新方向

第三节 信息安全行业应对策略

一、把握国家投资的契机

二、竞争性战略联盟的实施

三、企业自身应对策略

第十三章 2018-2024年中国信息安全行业发展策略及投资建议

第一节 中国信息安全行业品牌战略分析

一、信息安全企业品牌的重要性

二、信息安全企业实施品牌战略的意义

三、信息安全企业品牌的现状分析

四、信息安全企业的品牌战略

五、信息安全品牌战略管理的策略

第二节中国信息安全行业市场的重点客户战略实施

一、实施重点客户战略的必要性

二、合理确立重点客户

三、对重点客户的营销策略

四、强化重点客户的管理

五、实施重点客户战略要重点解决的问题

第三节中国信息安全行业战略综合规划分析

一、战略综合规划

二、技术开发战略

三、业务组合战略

四、区域战略规划

五、产业战略规划

六、营销品牌战略

七、竞争战略规划

第十四章 2018-2024年中国信息安全行业发展策略及投资建议

第一节中国信息安全行业产品策略分析

一、服务产品开发策略

二、市场细分策略

三、目标市场的选择

第二节中国信息安全行业定价策略分析

第二节中国信息安全行业营销渠道策略

一、信息安全行业渠道选择策略

二、信息安全行业营销策略

第三节中国信息安全行业价格策略

第四节 观研天下行业分析师投资建议

一、中国信息安全行业重点投资区域分析

二、中国信息安全行业重点投资产品分析

图表详见正文（GYWW）

详细请访问：<http://baogao.chinabaogao.com/xixinfuwu/328448328448.html>