中国工业信息安全产业发展白皮书

(2019-2020)

工业信息安全产业发展联盟
National Industrial Security Industry Alliance

前 言

近年来，全球制造业数字化转型进程加速，以大数据、云计算、人工智能等为代表的新一代信息技术向制造领域全面渗透，工业生产过程开放程度逐步加深。工业信息安全作为网络安全的重要组成部分，泛指工业运行过程中的信息安全。当前，在中央大力部署推进5G、工业互联网等新型基础设施建设的大背景下，加快构建工业信息安全技术产业生态是支撑服务制造业数字化转型，保障数字经济健康发展的重要基础。

回顾2019年，我国工业信息安全政策标准日益完善，垂直行业工业信息安全建设提速，工业企业安全意识显著增强，工业信息安全保障技术水平大幅提升，推动了工业信息安全产业的蓬勃发展。在新一轮产业数字化转型的大背景下，工业互联网建设将全面加速，安全保障仍是工业互联网的重点工作，产业内生需求有望进一步被激发，我国工业信息安全产业未来前景可期。经综合研判，预计2020年我国工业信息安全市场增长率将达23.13%，市场整体规模将增长至122.81亿元。

此次白皮书是工业信息安全产业发展联盟连续第三年发布的工业信息安全产业研究成果，由国家工业信息安全发展研究中心联合启明星辰、天融信、绿盟科技、安恒信息、

恒安嘉新、威努特、烽台科技、珞安科技、六方云、国家能源集团信息公司网安中心共同编制完成。白皮书延续了对国内外工业信息安全产业进展的跟踪研判，重点围绕产业规模结构、政策环境、技术演进、行业应用、市场竞争格局等产业要素进行梳理分析，深度剖析了现阶段我国工业信息安全产业发展面临的挑战，对产业发展趋势进行了科学预测。

由于时间关系，报告尚有不足之处，恳请批评指正。

工业信息安全产业发展白皮书编写组

2020 年 12 月

目 录

一、全球工业信息安全产业年度概况

近年来，各国地缘政治博弈已经超越了实体空间限制，延伸到网络空间，能源、制造业和其他关键基础设施领域的工业控制系统正成为网络空间对抗的主战场。2019 年，工业信息安全得到全球主要经济体的高度重视，各国陆续采取政策措施完善产业发展环境，行业用户安全意识稳步提高，技术创新演进持续深入，市场竞争合作日益激烈，全球工业信息安全产业进入蓬勃发展阶段。

（一）全球工业信息安全产业规模稳中有增

据市场研究公司 Verified Market Research 分析，2019 年全球工业信息安全市场规模达 164.01 亿美元，预计到 2026 年增长至 297.6 亿美元，年复合增长率为 8.83%。其中，运营技术（OT）安全仍然是增速最快的细分市场。据 Gartner 预测，2019 年全球 OT 安全支出达 3.8 亿美元，年增长率达 52%。另据市场研究公司 Market Watch 分析，预计到 2025 年，全球 OT 安全市场规模将增长至 35.31 亿美元。

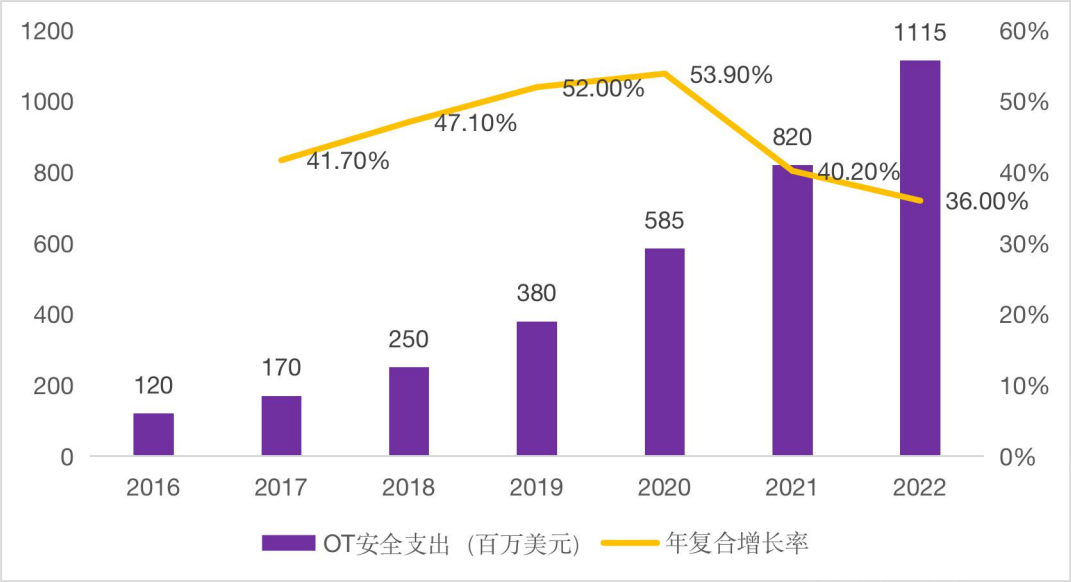

图 1 OT 安全年支出预测和增长率（单位：百万美元）

资料来源：Gartner 公司，工业信息安全产业发展联盟综合分析

区域分布方面，据 Verified Market Research 的数据显示，2019 年北美地区工业信息安全市场增势稳定，市场规模达 79.38 亿美元，占全球市场份额近 50%。由于针对能源和制造业网络攻击数量的快速增长，欧洲工业信息安全市场规模持续扩大，达 35.03 亿美元。随着中国、日本和印度等国家城市化和工业化不断深入，亚太地区工业信息安全市场增速加快，市场规模达 31.12 亿美元。在工控安全领域，北美地区在政策监管、市场供给和技术应用等方面优势显著，市场规模稳居首位；中东和非洲地区关键基础设施部门安全意识显著增强，工控安全市场增速仍保持领先。

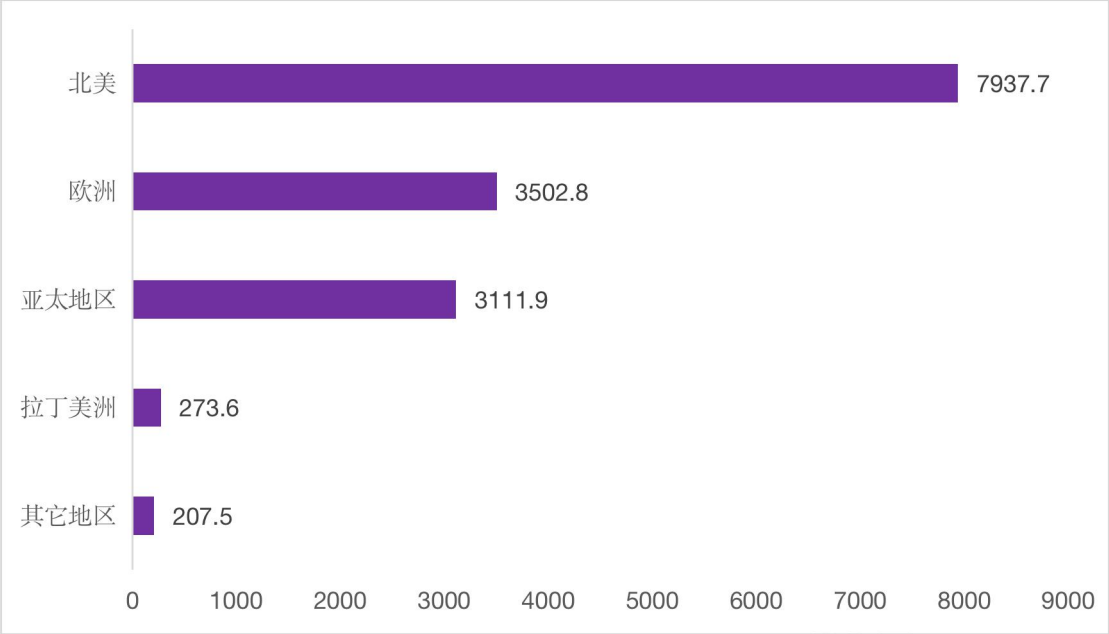

图 2 2019 年全球主要地区工业信息安全市场规模（单位：百万美元）

资料来源：Verified Market Research，工业信息安全产业发展联盟综合分析

行业应用方面，Verified Market Research 的数据表明，能源和公用事业（市政）领域仍然是工业信息安全的“主战场”，2019 年市场规模达 52.32 亿美元。由于控制系统和物联网设备的广泛应用，交通运输行业工业信息安全需求显著增强，成为 2019 年增速最快的垂直行业，市场规模达 31.87 亿美元。化工和制造业工业信息安全市场增速小幅放缓，市场规模达 23.18 亿美元。其中，由于制造业间谍活动等网络威胁加剧，预计未来增速将进一步加快。

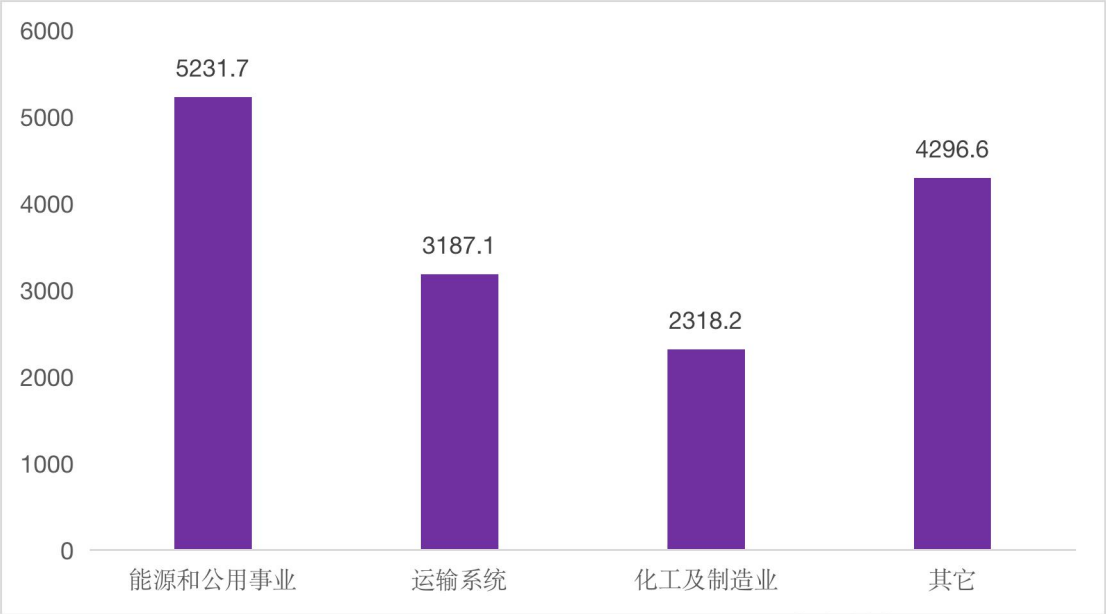

图 3 2019 年全球工业信息安全应用行业市场规模（百万美元）

资料来源：Verified Market Research，工业信息安全产业发展联盟综合分析

产业结构方面，随着联网工控系统和设备数量的快速增长和频繁曝出的安全漏洞，加密解决方案需求旺盛，成为 2019 年增速最快的工业信息安全细分领域，年复合增长率达 8.59%。此外，事件应急响应、安全运营等风险管理服务市场发展迅猛，预计未来将成为工业信息安全增速最快的服务类市场。

（二）主要国家和地区政策环境不断完善

当前，国际网络空间安全形势日趋复杂多变，关键基础设施领域网络攻防对抗愈发激烈。2019 年，全球主要国家和地区陆续采取措施强化工业信息安全，持续完善产业发展环境。

1. 美国加大工业信息安全保障力度

美国长期以来高度重视关键基础设施领域的工业信息安全，从工作机制、资金预算、技术手段、产业协作等多个方面不断提升工业信息安全保障能力。

工作机制方面，为进一步加强关键基础设施领域的网络安全，2018 年 11 月，美国众议院正式批准将美国国土安全部（DHS）的国家保护和计划局（NPPD）重组为网络安全和基础设施安全局（CISA），负责关键基础设施的网络和物理安全。2019 年，CISA 明确将工控安全作为主要任务之一。4 月，CISA 发布了 55 个国家关键职能清单，强调关键系统和制造业工控安全防护的重要性，为开展关键基础设施领域的风险评估提供了依据。

资金预算方面，美国在工业信息安全方面的投入持续走高。白官发布的 2020 年联邦预算中近 110 亿美元被要求用于网络安全，关键基础设施保护仍然是预算投入重点。其中，国土安全部（DHS）为工控安全增加了 1140 万美元的预算，用于加强工控安全培训、恶意软件分析、工控系统脆弱性分析、事件响应以及新兴行业和细分领域的安全评估。能源部（DOE）的网络安全、能源安全和应急响应办公室（CESER）将新增预算 1.56 亿美元，用于提升美国电网安全性和弹性的早期研究项目。

技术手段方面，国土安全部坚持技术理念与实践应用并重，近年来向美国使用工控系统的工业企业用户提供了包括

漏洞扫描、网络攻击监测与事件响应、恶意软件分析、漏洞披露等在内的安全工具和资源。2019 年，CISA 强调将着力开发针对工控系统的新型检测响应技术和解决方案，以及将网络供给链理念和纵深防御理念应用于工控系统，降低工控安全领域的网络攻击和安全风险。11 月，CISA 还发布了网络安全评估工具（CSET）的 9.2 版，通过使用公认的政府和行业的标准和建议，指导资产所有者和运营者对控制系统网络进行合规性评估。

产业协作方面，美国工业信息安全领域的各主管部门加强了与行业用户的协作。为了加强跨行业的协作和沟通，美国国会引入了《2019 年网络安全咨询委员会授权法案》，建立由 35 个来自包括制造业、能源、化工、运输等行业的网络安全专业人员组成的咨询委员会，为国土安全部提供网络安全政策建议和规则制定的指导。2019 年，CISA 多次表示，未来将持续加强与美国其他政府机构和关键基础设施领域私营部门在工控安全方面的协作。能源部也就如何加强电力、管道等能源行业基础设施安全等议题，积极征求产业界建议，加快能源领域工业信息安全保障建设。

2. 欧盟强化工业信息安全能力整合

为提升欧盟各成员国工业信息安全的防护能力和产业发展水平，欧盟近年来强化网络安全资源整合，聚焦产业多方协同。2019 年 1 月，联合国欧洲经济委员会（UNECE）

明确将工业信息安全领域最广泛应用的 ISA/IEC62443 系列标准纳入《网络安全共同监管框架（CRF）》，作为联合国对欧洲政策立场的正式声明。2 月，欧盟宣布为“地平线 2020”的四个试点项目投入 6350 万欧元，汇集 26 个成员国的 160 多家大、中小型企业、高校和网络安全研究机构，启动网络安全能力建设计划。5 月，欧盟网络与信息安全局（ENISA）发布了《工业 4.0 网络安全挑战和建议》，指出了工业 4.0 和工业物联网面临的主要安全挑战，为产业各方开展工业信息安全工作和实践应用提供建议。

欧洲地区还通过组织开展网络安全演习、建立跨国网络防御项目等方式，积极推动工业信息安全领域的国际合作。2019 年，北约分别组织了代号为“锁盾（Locked Shields）”“十字剑（Crossed Swords）”“网络联盟（Cyber Coalition）”等大型网络安全实战演习活动，促进各成员国提升工业信息安全综合防御能力。“锁盾 2019”演习聚焦与当前国家关系最密切的网络威胁，设置了包含净水系统、电网、海上感知能力在内的多个关键基础设施。“十字剑 2019”演习为提高网络红队成员在预防、检测和应对全面网络运营方面的技能，加入了大量工业控制系统、物理安全系统、无人机和海上监控系统的挑战场景。此外，为加强在能源基础设施方面的网络安全防御能力，立陶宛、拉脱维亚和爱沙尼亚等波罗的海诸国与美国能源部达成战略合作，保护波罗的海的能源网免受

网络攻击。

3. 德国、新加坡等发达国家加快政策布局

作为工业 4.0 的发源地，德国政府不断加强工业信息安全管理体系建设。德国联邦信息安全局（BSI）自 2013 年发布《工业控制系统信息安全（以下简称“工控安全”）手册》以来，陆续出台多份工控安全实施建议文件。2019 年 2 月，BSI 发布《2019 年工业控制系统安全面临的十大威胁和反制措施》指导工业控制系统运营商、制造商和集成商做好工业信息安全防护工作。德国联邦教育与研究部（BMBF）也将工业信息安全领域的技术研究和创新作为优先任务，提升德国在工业关键基础设施领域安全防护水平。

2019 年，新加坡政府也强化了工业信息安全顶层设计。10 月，新加坡网络安全局（CSA）发布《运营技术（OT）网络安全总体规划》，主要面向能源、水处理、交通等领域的关键信息基础设施运营者，通过扩大人才库，加强政府部门与私营部门的信息共享等方式提高 OT 系统安全防御能力和网络弹性。

（三）行业用户安全意识稳步提升

1. 合规需求推动能源领域工业信息安全发展加速

能源领域作为各国国民经济发展的支柱型产业，近年来已成为工业网络攻击的重点目标。2019 年 3 月，委内瑞拉爆

发由古里水电站引起的大规模停电，美国西部地区电网运营商遭受了分布式拒绝服务（DDoS）攻击，以电力行业为代表的能源领域的安全性再次引发全球广泛关注。

为加强能源部门的工业信息安全，美国多个联邦机构纷纷采取措施。2019 年 2 月，一家美国能源公司因违反近 130 条关键基础设施保护（CIP）标准，被北美电力可靠性公司（NERC）罚款 1000 万美元，这也是 NERC 截至目前为止最高的罚款记录。6 月，美国能源部以电力行业为基础发布了网络安全能力成熟度模型 2.0 版（C2M2），对 1.0 版的技术、实践和环境因素进行了调整，为工业企业提供用于评估其网络安全能力的工具。9 月，美国国家标准与技术研究院（NIST）发布了《能源行业网络安全指南》，提供了有关能源组织如何识别和管理 OT 资产及检测与这些资产相关的网络安全风险的详细步骤。NIST 下属的美国国家网络安全卓越中心（NCCoE）还建立了实验室环境，重点展示能源企业如何运用现有的安全能力来加强 OT 资产管理实践。

此外，美国能源部门还高度重视工业信息安全技术的创新研究人才培养工作。10 月，CESER 发布了近 700 万美元的奖金，支持研究、开发和演示用于增强能源输送系统的网络安全下一代工具和技术。11 月，第五届 Cyber Force 竞赛在 DOE 的十个国家实验室举办，丰富美国能源行业的工业信息安全专业人员培养形式。

2. 制造业工业信息安全意识有所提升

随着物联网、云计算、人工智能等新一代信息技术的广泛应用，制造业在加快数字化转型的同时也面临了激增的工业信息安全风险。2019 年 3 月，全球最大的铝生产商之一，挪威金属和能源巨头 Norsk Hydro 受到勒索软件攻击; 10 月，全球最大的自动化产品供应商德国皮尔兹（Pilz）公司遭受严重网络攻击，导致网络瘫痪，订单系统无法访问。

相较于电力、石油化工等流程型行业，制造业企业在工业设计和生产工艺方面独特的知识产权（IP）、生产和运营数据等的巨大经济价值，都使其成为网络间谍活动的主要目标。据 IT 服务提供商 Wipro 的研究显示，在暗网提供的全部关键资源或资产中，有 14%来自制造业。另据英国制造业研究机构 MAKE 的报告，2019 年，60%的英国制造业企业曾遭受网络攻击，其中 1/3 遭受了经济损失或业务中断。

为应对制造业不断升级的工业信息安全风险，2019 年 9 月，CISA 发布了《关键制造业内部威胁项目实施指南》，强调必须对威胁进行连续、主动的监测，以确保关键操作的安全。据 Marsh 和微软联合开展的 2019 网络风险感知调查显示，2019 年全球制造业企业安全意识有较大提升，超过 3/4（76%）的制造业企业将网络风险列为组织最关注的五大问题，其中，22%的制造业代表将网络风险列为组织的头号风险关注点。

3. 交通、市政等重点领域投入仍显不足

数字时代的到来和通信技术的迅猛发展，推动了海运、航空、地面运输、城市轨道、管道等交通运输领域的加速变革。据 IBM 公司的 X-Force 威胁情报数据显示，交通运输行业已成为网络攻击的第二大优先目标。与持续攀升的安全风险相比，交通运输行业在网络安全领域长期缺乏政策监管和实践指导，工业信息安全意识水平普遍较低。2019 年 12 月，美国一港口设施遭受 Ryuk 勒索软件攻击，导致港口运行瘫痪 30 多小时；同月，美国 RavnAir 航空公司遭到网络攻击，最终导致飞机维修等关键系统关闭。

水处理、供热、供水、供气等市政公用事业部门也是工业信息安全的主要应用部门之一。据西门子与波蒙研究院的调查显示，56%的市政企业每年至少经历一次网络攻击，并造成业务关停或运行数据丢失。另据 ABI Research 的报告预测，市政部门每年将投入 140 亿美元用于智能设备等数字基础设施领域，但与之相对应的工业信息安全投入增速仅为 55%，到 2023 年，工业信息安全投入仅为 80 亿美元。

（四）技术创新持续演进深化

近年来，随着 IT 与 OT 加速融合一体化，大数据、云计算、人工智能、区块链、5G、边缘计算等新技术在工业互联网领域快速应用。2019 年，工业信息安全技术在传统信息安

全技术的影响和自身的发展下开始进入转型期，从被动防御向主动防御发展，逐渐进入落地阶段。

2019 年，ARC 更新了工业/OT 网络安全成熟度模型（图 4），将企业工业信息安全项目建设分解为单个设备安全防护、外部攻击防御、访问控制（恶意软件等）、网络监测和入侵检测及主动威胁管理等一系列阶段。该模型明确了被动防御（蓝色）和主动防御（橙色）的安全成熟度级别和所需的人员、流程和技术，为企业建立和管理工业信息安全项目提供参考。

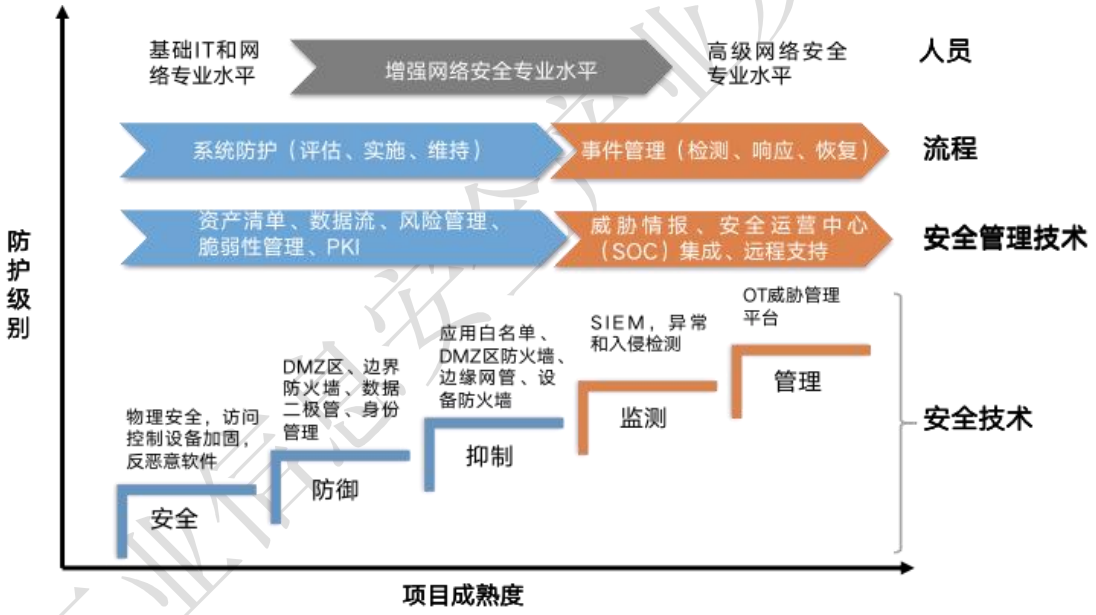

图 4 ARC 工业信息安全成熟度模型 2.0 版

资料来源：ARC，工业信息安全产业发展联盟综合分析

据安全研究机构 SANS 的调查报告显示（见图 5），2019 年，访问控制、网络分区、安全意识、端点安全等基本的工业信息安全被动防护技术已经被用户广泛使用。OT 网络监测和异常检测、软件定义网络（SDN）分区、适用于 OT 的

安全操作中心、工业数据防泄露等主动防御技术将在未来 18 个月被广泛采用。

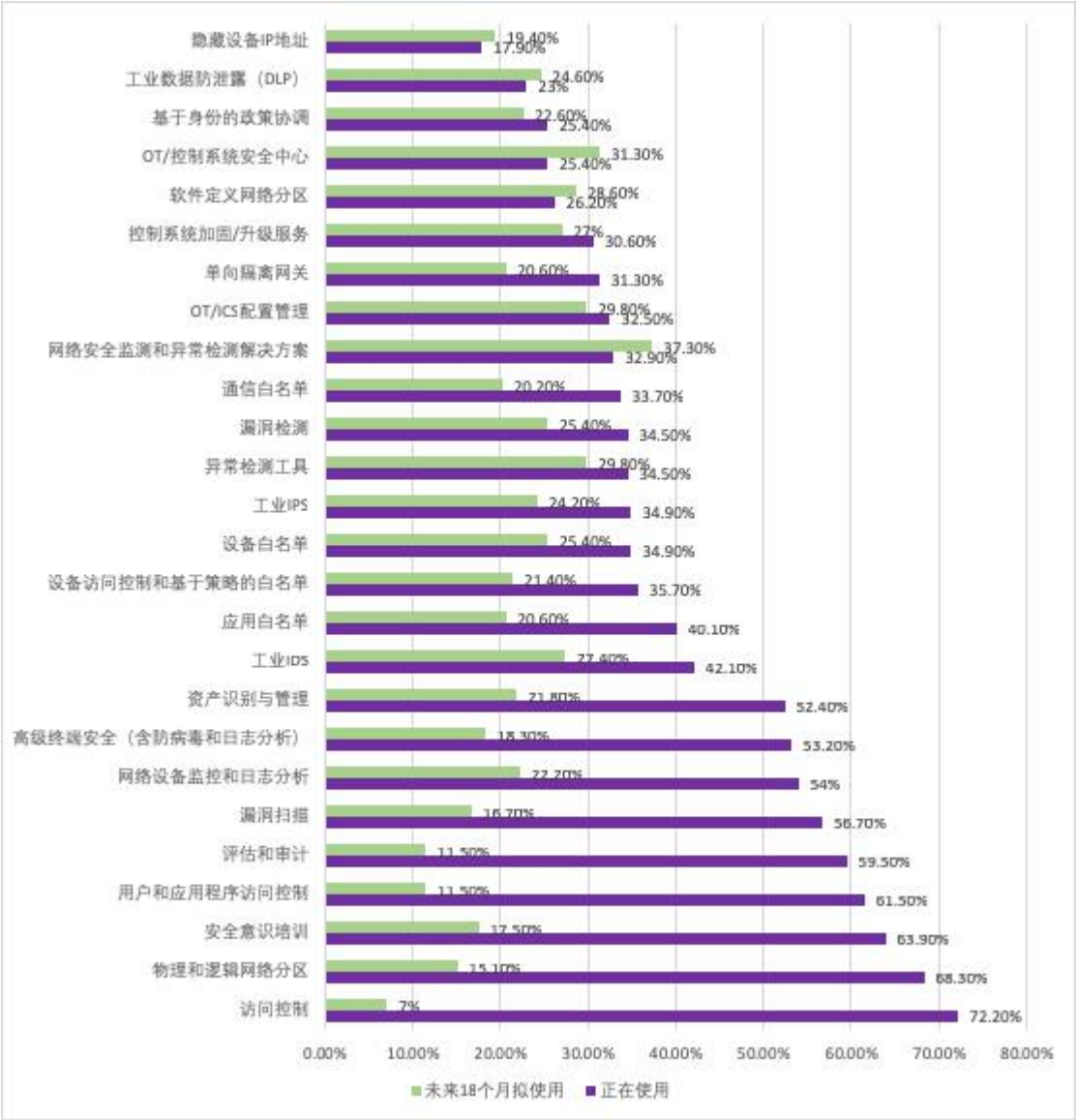

图 5 用户正在使用和未来 18 个月拟采用的技术和解决方案分布

资料来源：SANS，工业信息安全产业发展联盟综合分析

（五）市场竞争合作逐步升级

近年来，全球工业信息安全产品和服务市场持续发展壮大，获得资本市场的广泛青睐。2019 年，传统信息安全企业、国际自动化企业、工业信息安全初创企业、国际咨询机构、

垂直行业龙头等工业信息安全产业链上下游企业共同发力，加快资本整合和战略合作步伐。

传统信息安全企业方面，2019 年 6 月，思科公司宣布收购工业信息安全厂商 Sentryo，提高在 OT 安全资产发现、网络分区和 OT 安全运营方面的能力。12 月，全球知名漏洞管理网络安全公司 Tenable 宣布以 7800 万美元现金收购了以色列领先的 OT 安全解决方案提供商 Indegy。此次收购将充分融合双方在 IT 和 OT 方面的技术优势，为工业企业用户提供 IT/OT 安全风险的综合管理平台。此外，信息安全龙头企业派拓网络（Palo Alto Networks）也通过与 Radiflow、Cyber X 等初创企业的合作，将新型工业信息安全技术应用集成到其安全运营平台（Cortex）中。

自动化企业方面，西门子、霍尼韦尔等国际自动化巨头近年来不断完善工业信息安全领域的布局，依托自身庞大的工业客户基础，通过提供安全托管和安全咨询等服务进入安全市场。2019 年，罗克韦尔宣布在其工业控制系统相关产品中加入安全功能，并在工业信息安全服务方面取得 ISA/IEC 62443-2-4 的认证。ABB 也联合 Cylance、Checkpoint 及微软等厂商建立了运行技术网络安全联盟（OTCSA），促进 IT 和 OT 运营者与行业领先解决方案公司之间的合作，进一步完善工业信息安全生态圈建设。

工业信息安全初创企业方面，以 Claroty、Dragos、Nozomi

Networks 等为代表的初创企业陆续凭借技术的持续创新性，在日益白热化的市场竞争中脱颖而出。同时，专注垂直行业工业信息安全应用的厂商也开始发挥行业知识和市场策略优势，引发资本市场关注。专注铁路工业信息安全的以色列厂商 Cylus 于 2019 年 6 月获得由 Magma Venture Partners 和 Vertex Ventures 共同领投的 1200 万美元 A 轮融资；10 月，工业信息安全公司 FoxGuard Solutions 宣布被国际核能系统和设备供应商 Framatome 收购，并将增强 Framatome 在能源行业的工业信息安全产品和解决方案。

表 1 2019 年全球工业信息安全市场企业融资概况

序号	时间	厂商	融资额/万美元	融资阶段	国家
1	1 月	Xage Security	400	A+轮	美国
2	3 月	Mocana	1500	E+轮	美国
3	3 月	NexDefense（收购方：Dragos）	—	收购	美国
4	3 月	Cyber X	1800	战略	以色列
5	6 月	Sentryo（收购方：思科）	—	收购	法国
6	6 月	Cylus	1200	A 轮	以色

					列
7	10 月	FoxGuard Solutions（收购方：Framatome）	—	收购	美国
8	12 月	Indegy（收购方：Tenable）	7800	收购	以色列

资料来源：工业信息安全产业发展联盟综合分析

二、我国工业信息安全产业年度概况

（一）我国工业信息安全政策体系不断完善

随着信息技术与制造业的不断融合，云计算、物联网、5G 等新一代信息技术日益成熟，工业领域的网络安全风险增多，如漏洞高发、安全事件频发，工业信息安全成为国家和企业高度关注议题。近年来，为切实保障“两个强国”战略的实施，促进工业信息安全工作有效落实，我国不断加强工业信息安全顶层设计，在政策法规、标准工作等多方面完善工业信息安全政策体系建设。

2019 年，工业和信息化部（以下简称“工信部”）、公安部、国家能源局、水利部等国家工业信息安全主管部门和行业监管部门密集出台了多项与工业信息安全相关的政策文件（见表 2），指导开展工控安全标准体系建设和工业互联网安全保障工作。

表 2 2019 年我国工业信息安全相关政策汇总

月份	部门	法规
1 月	工信部	《工业互联网网络建设及推广指南》
3 月	工信部、国家标准化管理委员会	《工业互联网综合标准化体系建设指南》
5 月	国家市场监督管理总局、国家标	网络安全等级保护制度 2.0 标准:《信息安全技术网络安全等级保护基

	准化管理委员会	本要求》、《信息安全技术网络安全等级保护测评要求》、《信息安全技术网络安全等级保护安全设计技术要求》等国家标准
6 月	工信部、北京市人民政府	《国家网络安全产业发展规划》
8 月	水利部	《水利网络安全管理办法（试行）》
8 月	工信部、教育部等十部门	《关于印发加强工业互联网安全工作的指导意见的通知》
9 月	工信部等部门	《关于促进网络安全产业发展的指导意见（征求意见稿）》
10 月	全国人大常委会	《密码法》
12 月	工信部	《工业互联网企业网络安全分类分级指南（试行）》（征求意见稿）

资料来源：工业信息安全产业发展联盟综合分析

1. 聚焦工业互联网安全，引导效应凸显

2019 年，工信部陆续发布《加强工业互联网安全工作的指导意见》《工业互联网企业网络安全分类分级指南（试行）》《工业互联网综合标准化体系建设指南》等多项政策文件，明确了工业互联网安全要求，为我国工业互联网安全保障体系建设提供了强有力的政策支撑。

3 月，工信部、国家标准化管理委员会联合印发的《工

业互联网综合标准化体系建设指南》正式发布，强调安全体系是工业互联网的保障，提出从防护对象、防护措施及防护管理三个维度构建工业互联网安全标准体系，明确了设备安全、控制系统安全、网络安全、数据安全、平台安全、应用程序安全、安全管理等七项工业互联网安全重点标准化建设领域及方向。

8 月，由工信部等十部门联合发布了《加强工业互联网安全工作的指导意见》（以下简称《意见》），从企业主体责任、政府监管责任出发，围绕设备、控制、网络、平台、数据安全等方面，以健全制度机制、建设技术手段、促进产业发展、强化人才培育为基本内容，实现工业互联网安全的全面管理。《意见》进一步明确了工业互联网安全保障体系初步建立的近期目标和远期目标，也为工业互联网安全建设向法治化、制度化、专业化发展打下基础。

12 月，工信部发布《工业互联网企业网络安全分类分级指南（试行）》（征求意见稿），切实落实《意见》要求，指导企业开展分类分级工作，提高工业互联网企业网络安全防范能力和水平，促进企业落实网络安全主体责任。

2. 强化应用牵引，激发创新潜能

2019 年 5 月，工信部启动“2019 年工业互联网创新发展工程项目”，组织开展项目招标工作。工业互联网安全方向涵盖了开发测试基础共性服务平台、网络信任支撑平台、网

络安全公共服务平台等共14个项目，支持企事业单位开展工业互联网安全态势感知、安全综合防护、平台数据安全监测与服务等建设。同时，2019年的创新发展工程首次开展了“面向工业企业、工业互联网平台企业等的网络安全解决方案供应商项目”招标工作，对于加快安全企业实施推广工业信息安全解决方案，培育工业信息安全产业生态起到了巨大促进作用。

11月，为推动工业互联网创新发展，工信部开展2019年工业互联网试点示范项目推荐工作。在2020年2月公布的试点示范项目名单（见表3）中，共有17个安全方向项目入围。通过遴选一批标杆企业、样板工程，试点示范项目有利于探索面向垂直领域的工业互联网安全方向应用场景，形成一批可复制、可推广的路径模式，促进工业互联网安全应用推广。

表3 2019年工业互联网试点示范项目名单（安全方向）

序号	项目名称	申报单位	推荐单位
1	工业嵌入式软件信息安全测试及仿真验证平台	上海工业控制安全创新科技有限公司	上海市经济和信息化委员会
2	南京地铁宁高城际禄高段工程信号系统信息安防护平台	上海三零卫士信息安全有限公司	上海市经济和信息化委员会

3	企业级工业互联网安全监测与态势感知平台	恒安嘉新（北京）科技股份公司	北京市通信管理局
4	基于异质协议数据融合的工业控制安全监控预警平台	北京安天网络安全技术有限公司	北京市经济和信息化局
5	华能新能源辽宁分公司风电场安全集中管控系统	北京天地和兴科技有限公司	北京市经济和信息化局
6	面向城市轨道交通的工业互联网平台安全防护系统	深信服科技股份有限公司	深圳市工业和信息化局
7	面向装备制造行业生产控制系统的安全防护解决方案	中国电子科技网络信息安全有限公司	四川省经济和信息化厅
8	基于商密算法的车联网 5G-V2X 通信安全认证防护平台	国汽（北京）智能网联汽车研究院有限公司	北京市经济和信息化局
9	上汽乘用车工业互联网安全态势感知平台	上海工业自动化仪表研究院有限公司	上海市经济和信息化委员会

10	面向智能制造行业的工业安全态势感知与监测预警平台	北京圣博润高新技术股份有限公司	北京市经济和信息化局
11	面向混合云的工业数据安全防护系统	合肥城市云数据中心股份有限公司	安徽省通信管理局
12	企业级工业互联网安全运营平台	烽台科技（北京）有限公司	北京市经济和信息化局
13	贵州工业互联网平台安全监测与防护系统	贵州航天云网科技有限公司	贵州省工业和信息化厅
14	电力监控系统端点恶意代码防御系统	哈尔滨安天科技集团股份有限公司	黑龙江省工业和信息化厅
15	基于工业资产全息画像的工业互联网安全监测平台	南京中新赛克科技有限责任公司	江苏省通信管理局
16	工业互联网数据持续保护与预警防御平台	南京壹进制信息科技有限公司	江苏省工业和信息化厅
17	面向新材料行业的工业互联网平台安	新疆众和股份有限公司	新疆维吾尔自治区工业和信息化

	全综合防护系统		厅

资料来源：工业信息安全产业发展联盟综合整理

3. 开启“等保 2.0”时代，提升工控安全要求

2019 年 5 月，国家市场监督管理总局、国家标准化管理委员会正式发布网络安全等级保护技术 2.0 版本（以下简称“等保 2.0”）系列核心标准，正式宣告等保进入 2.0 时代。相较于“等保 1.0”，即《GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求》，等保 2.0 正式将工业控制系统作为五大新技术与重要应用之一，列出了扩展要求。随着等保 2.0 的发布，我国工业控制系统信息安全建设进程将大幅加快。同时，工控安全等级保护工作的落地实施，也将有效提升国内工业企业在工控安全方面的综合防护能力。

（二）我国工业信息安全产业规模增势强劲

当前，由于国内外缺乏对工业信息安全产业的公认界定，产业相关数据的统计口径也尚未建立，国家工业信息安全发展研究中心依托对国内外工业信息安全产业长期的跟踪调研，对我国工业信息安全产业规模的统计口径进行了调整，涵盖工业领域 IT 安全、OT 安全、IT/OT 融合安全，同时还包括含有内嵌信息安全功能的工业自动化、信息化和网络基础设施等。

2017 年以来，我国工控安全、工业互联网安全政策标准

日益完善，垂直行业工业信息安全建设提速，工业企业安全意识全面增强，工业信息安全保障技术水平显著提升，推动了工业信息安全产业的全面发展。2019 年，我国工业信息安全产业规模保持了快速上升之势。据调研结果统计[1]显示（见图 6），我国工业信息安全产业规模为 99.74 亿元，市场增长率达 41.84%；其中，工业互联网安全产业[2]规模为 38.3 亿元，较 2018 年同比增长 51.62%。

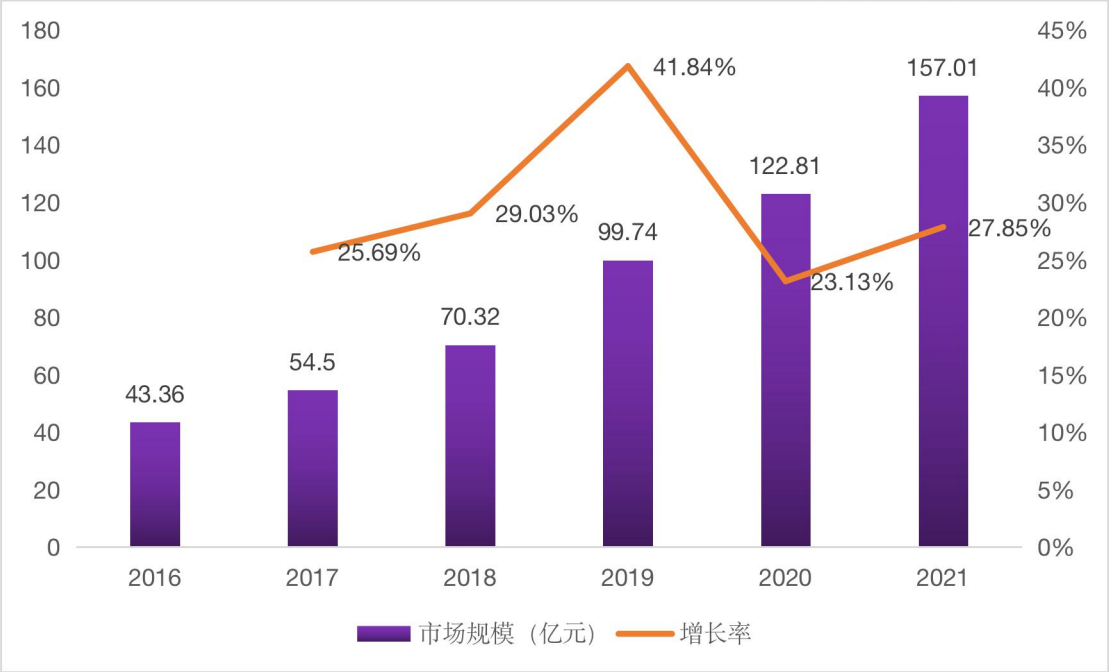

图 6 2016—2021 年我国工业信息安全市场规模及增长率

资料来源：工业信息安全产业发展联盟综合分析

在新一轮产业数字化转型的大背景下，工业互联网建设将全面加速，安全保障仍是工业互联网的重点工作，产业内生需求有望进一步被激发，我国工业信息安全产业未来前景

[1] 工业信息安全产业发展联盟对国内典型工业信息安全厂商 2019 年业绩进行了调研，结合国内工业信息安全市场公开招标情况、企业年报、其他相关产业报告等材料，对我国工业信息安全产业进行综合分析和预测。

[2] 不包含工业领域 IT 安全投入。

可期。与此同时，受 2020 年年初新型冠状肺炎疫情影响，我国工业信息安全产业发展也面临巨大的考验。经综合研判，预计 2020 年我国工业信息安全市场增长率将达 23.13%，市场整体规模将增长至 122.81 亿元。

（三）我国工业信息安全产业结构加速调整

从产业结构[3]来看，据《中国工业信息安全产业发展白皮书（2017）》，以外建安全为主的工业信息安全依据市场应用可以分为产品和服务两大类（见图 7）。

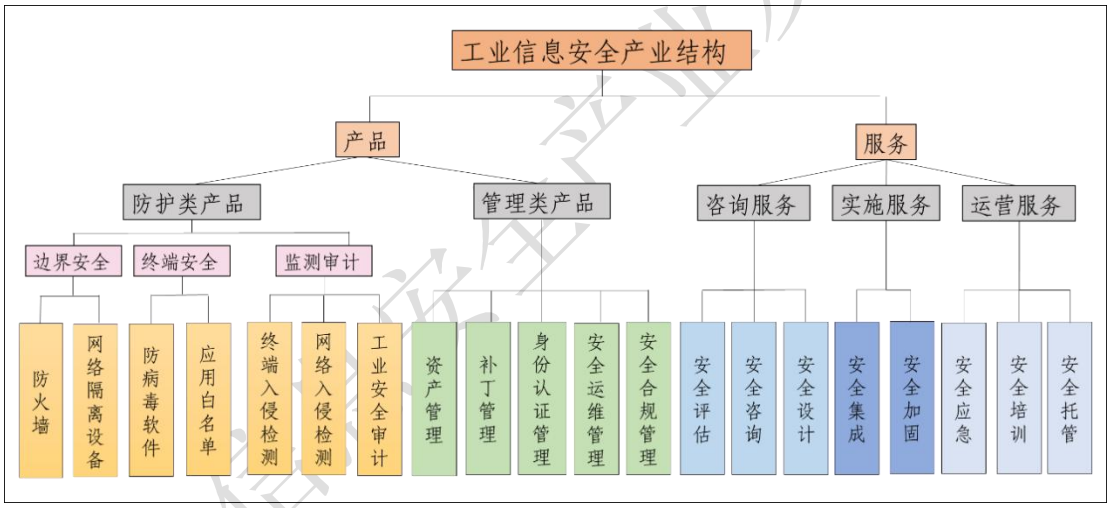

图 7 工业信息安全产业结构图

资料来源：《中国工业信息安全产业发展白皮书（2017）》

当前，随着工业信息安全技术的逐渐成熟，我国工业信息安全产品和服务已陆续从研究探索走向实践应用。2019 年，我国工业信息安全产品类市场规模达 30.303 亿元，占市场总额的 79%(见图 8)。其中，防护类产品市场规模达 10.125

[3] 由于工业信息安全产业测算口径的调整，此处工业信息安全产业结构主要指应用于工业互联网外建安全的产品和服务。

亿元，占市场总额的 26%。与过去两年相比，防护类产品市场增速有所放缓。**一方面**，防护类产品的部署大多由合规需求驱动，与政策推进情况密切相关；**另一方面**，安全意识的提升和日趋复杂的工业现场环境，直接影响了用户在工业信息安全项目建设上的采购决策，单纯的工业防火墙、工业网闸、应用白名单等边界安全和终端安全产品已不能完全满足安全防护需求。随着等保 2.0 的正式实施，防护类产品将作为整体解决方案中必备的基础安全措施，推动该类市场规模稳定增长。

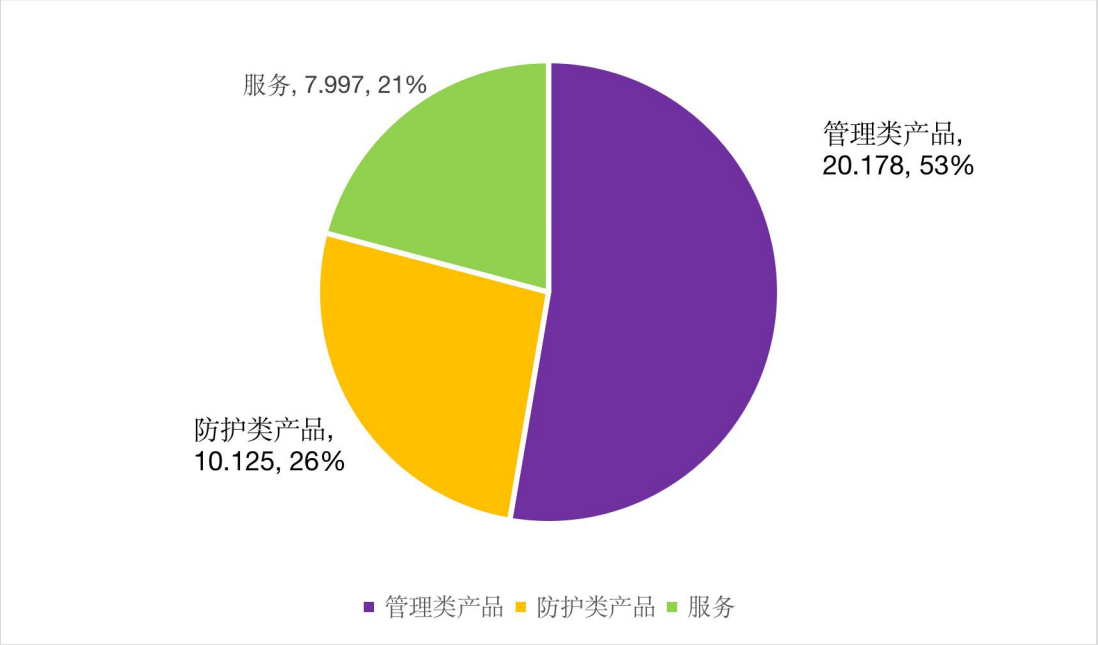

图 8 2019 年我国工业信息安全产业结构概览

资料来源：工业信息安全产业发展联盟采集整理

2019 年，我国工业信息安全管理类产品市场规模约为 20.178 亿元，占市场总额的 53%。我国工业信息安全管理类产品主要分布于态势感知、合规管理、安全运维管理等领域。

2019 年，国家、地方和垂直行业涌现了大量的新增态势感知项目，其中，企业侧态势感知产品的部署和运营是该类市场快速增长的重要因素。未来在合规需求和内生需求的双重推动下，该类产品市场规模将进一步扩大。

我国工业信息安全服务类市场在 2019 年继续快速增长，市场规模近 7.997 亿元，占市场总额的 21%。其中，安全评估、安全应急和安全培训服务是推动该类市场增长的主要驱动力。随着国家针对关键信息基础设施的网络安全演习扩大到电力、石油石化等诸多工业领域，工业企业用户的渗透测试、攻防演习等应急类安全保障支撑服务需求明显增多。同时，等保 2.0 出台后，工业安全评估体系逐渐完善，测评类评估需求将更为明确，带动市场规模进一步扩大。此外，工业信息安全人才短缺的问题已逐渐凸显，促使高校、科研院所等加大在工业信息安全培训方面的投入，带动了安全培训服务和实训类产品的快速增长。

（四）我国工业信息安全行业应用显著增强

2019 年，我国电力、智能制造、水利、交通等关键信息基础设施的重点行业开始积极行动，纷纷在工业信息安全领域加大投入，行业应用格局发生了较大的变化。

地方政府及科研机构在工业信息安全领域的投入稳中有增，达 2.97 亿元，占市场总额的 8%（见图 9）。国家层

面工业信息安全相关政策的陆续出台，引起了地方政府和科研机构的高度重视。同时，2019 年工业互联网创新发展工程的发布实施和工业互联网安全方向试点示范项目的遴选，也极大地提高了地方政府和科研机构在工业信息安全工程化应用和产业化推广的投入力度。

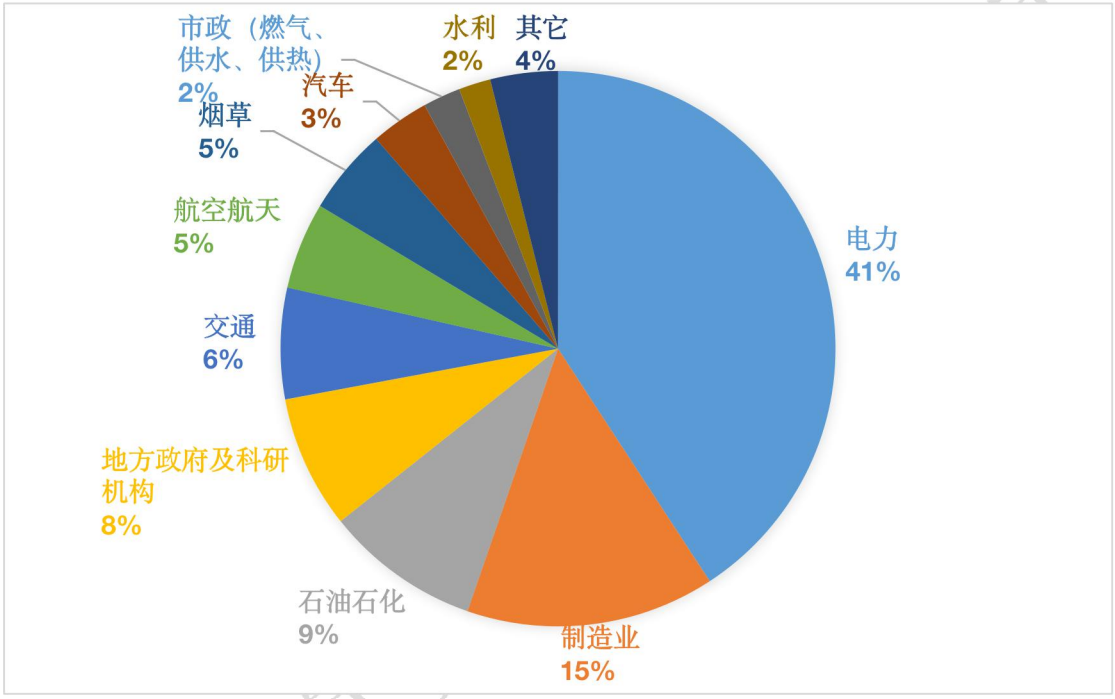

图 9 2019 年我国工业信息安全行业应用情况

资料来源：工业信息安全产业发展联盟综合分析

2019 年电力行业工业信息安全投入仍保持高位，市场规模达 15.62 亿元，市场占比达 41%，稳居榜首。电力行业是我国目前工业信息安全建设成熟度最高的行业，尤其是电网侧在安全防护类产品方面投入非常稳定。2019 年 1 月，国家电网明确打造“三型两网”战略目标，提出加快推进泛在物联网建设。该战略在开启新一轮电力信息化建设高潮的同时，也带动了安全防护相关建设工作，进一步推进电网侧工

业信息安全应用从基础防护向可信互联、综合防御等方向演进。2019 年 7 月，《电力信息系统安全等级保护实施指南》正式实施，在依据国家标准并结合电力行业实际的基础上，提出了电力信息系统安全等级保护实施工作的标准，为电力行业工业信息安全应用的深化起到了重要指导作用。

伴随工业互联网纵深发展，离散制造业的工业信息安全应用取得高速发展。2019 年，机械加工、装备等高端制造业工业信息安全市场规模达 5.55 亿元，市场占有率达 15%，跃居第二位。与电力、石油石化等典型流程行业不同，离散制造业工业信息安全应用主要集中于工业互联网平台安全和数据安全防护，产品类型仍通过对传统信息安全产品的改进来实现。

石油石化行业 2019 年工业信息安全市场规模达 3.46 亿元，市场占有率为 9%，位居第三。相较过去两年的快速增长，石油石化行业工业信息安全应用进入战略调整阶段。由于缺乏明确的行业应用指导，石油石化行业工业信息安全项目建设较为零散，安全防护需求目前仍集中于边界隔离和安全加固，行业应用以防护类产品为主。

此外，2019 年交通、水利等部门工业信息安全市场增速加快。2019 年 8 月，中国城市轨道交通协会团体标准《智慧城市轨道交通信息技术架构及网络安全规范》正式发布，强化行业建设规范，为城市轨道交通工业信息安全建设提供了

重要参考。同月，水利部印发《2019 年水利网信工作要点》，明确提出要全面构建网络安全防线，并通过开展水利关键信息基础设施网络安全态势感知示范工程，推动行业加快工业信息安全建设。

（五）我国工业信息安全市场竞合加快

伴随着现代制造业数字化、智能化、网络化的快速发展和政策体系的完善，2019 年国内工业信息安全赛道涌现了一批新玩家及跨界选手，市场竞争日益加剧。总体来看，国内的工控系统厂商、传统信息安全厂商及系统集成商都将一定的研发力量投入了工业信息安全的研究及产品研发领域，并力争在工业信息安全领域获得先发优势。

据统计，2019 年约 266 家国内企业涉工业信息安全业务，较 2018 年增长 50%。其中，传统信息安全背景厂商最多，占总体数量的 55%；专注工控安全厂商数量和系统集成商数量几乎持平，行业整体集中度有所下降。

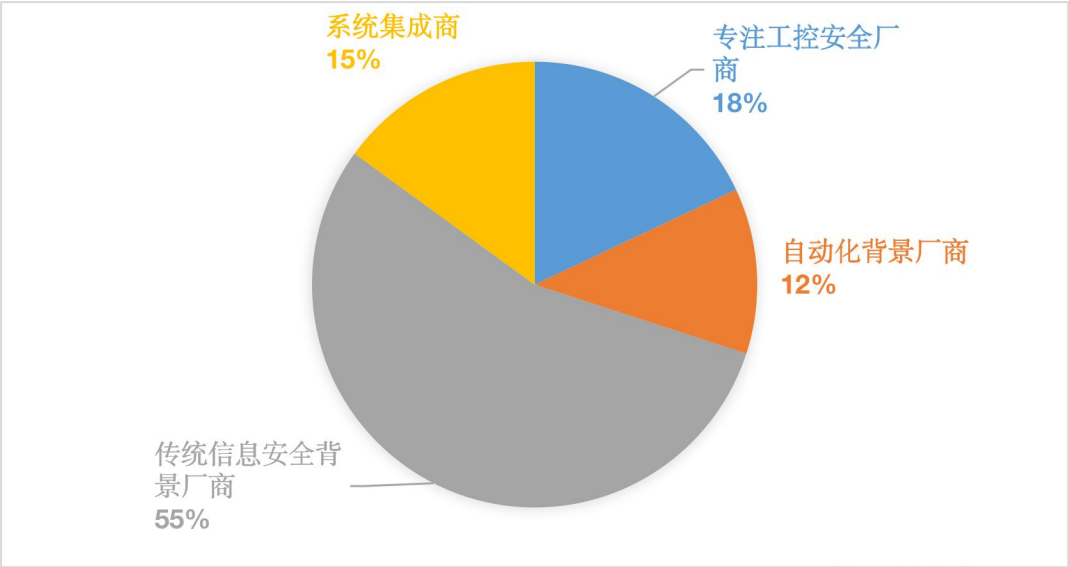

图 10 2019 年我国工业信息安全行业应用情况

资料来源：工业信息安全产业发展联盟分析整理

与 2018 年相比，2019 年工业信息安全市场的竞争格局主要呈现以下变化趋势：**一是**国家队入局工业信息安全行业。中国电科相继入股绿盟科技、南洋股份，与中国网安、卫士通一起构成了网络安全领域的“集团军”。中国电子投资奇安信，结合原有的 PK 体系，提出了内生安全的理念。这也意味着，国家资本针对工业信息安全产业布局趋向纵深发展，一方面彰显了其看好网络安全市场前景，另一方面也为安全企业的发展提供重要资源支持，将有力推动我国网络安全产业做大做强。

二是集成商中工业互联网平台供应商数量显著增多，海尔、华为、阿里巴巴等产业巨头公司纷纷入局，通过在现有的工业互联网平台中集成安全功能，强化在工业信息安全领域的竞争优势。同时，由于平台型厂商的客户资源优势，系

统集成商与安全厂商间也形成了更错综复杂的竞合关系。

三是科创板开启新兴安全厂商的上市通道。2019 年国内融资并购总金额达 108.3 亿元，工控安全是重要领域。科创板的推出极大提升了工业信息安全初创企业和资本方的信心。以安恒信息为代表的科创板新贵也正积极布局工控安全及工业互联网安全产品升级等项目，继续深耕工业信息安全领域。

四是工控安全初创公司融资捷报频传。2019 年年初，工业互联网安全、云安全服务商六方云完成由上海盛宇领投的数千万融资。作为国内领先的专注工业信息安全服务的初创企业，烽台科技在 2019 年上半年连续完成贵阳创投的千万级天使轮融资和由启明星辰的战略投资，正式成为启明星辰在工业信息安全领域的重要生态合作伙伴。此外，成立于 2018 年的融安网络也于 6 月获得有君盛投资的数千万 A 轮融资。进入 2019 年下半年，工业信息安全赛道上的资本角力更为激烈。10 月，工业互联网安全企业长扬科技宣布完成由基石基金、合创资本等 4 家机构投资的数千万 Pre-B 轮融资。同期，天地和兴再创融资新高，完成由毅达资本领投，广州国资黄埔智造基金跟投的 C 轮和战略投资方中兴、松禾资本的 C+轮，融资规模近 2 亿元。

表 4 2019 年我国工业信息安全初创企业融资情况

序	企业名称	时间	投资机构	轮次	金额

号					
1	六方云	2018-12-11	盛宇投资	战略投资	数千万元
2	烽台科技	2019-02-19	贵阳创投	天使轮	—
		2019-05-16	启明星辰	Pre-A轮	—
3	长扬科技	2019-03-11	合创智能基金	A+轮	数千万元
		2019-10-15	合创资本 杭州汉京西成股权投资合伙企业（有限合伙） 基石基金 深圳丰厚尚德创业投资中心	Pre-B轮	数千万元
4	融安网络	2019-06-21	同威资本 君盛投资	A 轮	数千万元
5	天地和兴	2019-10-25	松禾资本 中兴创投 毅达资本	C 轮	近 2 亿元

			广州国资黄埔智造基金		
6	珞安科技	2019-11-12	加盛巢生壹号基金 同创伟业 三一集团有限公司	A 轮	数千万元
7	博智安全	2019-12-20	中科科创等	C 轮	1.5 亿元

资料来源：工业信息安全产业发展联盟分析整理

三、我国工业信息安全产业发展面临的挑战

（一）产业发展仍由合规需求主导

合规需求是过去几年推动我国工业信息安全建设和产业发展的主要动因。在政策合规驱动下，工业企业用户的安全投入以单点、分散式采购为主，缺少体系化的安全规划和布局。随着各类实战化网络攻防演习行动的逐年增多，单纯依靠合规驱动的工业企业用户往往需要采取临时协调、突击建设等方式来应对，安全投入不足、主体责任落实不到位等问题仍然突出，产业内生需求有待进一步培育壮大。

（二）安全建设仍处于初级阶段

根据 ARC 工业信息安全成熟度模型，我国工业信息安全建设目前以技术应用和产品部署为主，在安全策略、制度、流程等方面普遍考虑不足。由于缺少与安全技术相匹配的人员、流程和管理手段，工业企业用户往往无法实现对安全产品效能和服务质量的有效评估，只能依赖市场上各类资质不一、能力参差不齐的安全厂商，工业企业自身的安全建设水平和保障能力亟待提升。

（三）产品同质化现象日益加剧

当前，工业信息安全技术发展进入一定瓶颈期，厂商的安全技术水平市场认可度不高。部分厂商的防护类产品和管

理类产品与工业业务场景结合程度不高，在产品形态和功能上与传统信息安全产品差异有限，产品线和解决方案趋同情况严重，应急处置、攻防演练等安全服务的价值也尚未得到有效体现。

（四）市场集中度提升空间较大

近年来，随着产业的快速发展，涉足工业信息安全业务的厂商数量在短时间内激增，市场竞争格局呈现高度分散的特点。与此同时，工业信息安全产业规模整体尚处于低位，产业集聚效应不明显，不同背景的工业信息安全厂商在相对有限的市场空间中竞争激烈，市场份额增长缓慢，企业规模经济效应难以快速实现。

四、我国工业信息安全产业发展趋势展望

（一）政策环境持续优化

工业信息安全作为国家安全的重要领域，是我国实施制造强国和网络强国战略的重要保障，也是落实总体国家安全观的重要抓手。在5G、工业互联网等新基建加速发展的大背景下，统筹发展和安全将成为我国新时期制造业数字化转型的主旋律，国家和地方有望进一步加大财政支持，工业信息安全法律、政策、标准体系将逐步完善，产业内需将加速释放。

（二）用户意识持续提升

在工业互联网创新发展工程、网络安全试点示范等工作的持续开展和带动下，工业企业安全意识显著提升，安全技术应用和防护能力建设已经由试点探索逐渐向产业化推进，电力（发电侧）、轨道交通等行业已陆续出现了区域级的规模化部署和应用。随着越来越多的工业信息安全产品和解决方案走向成熟，工业信息安全建设进程也将加快，未来有望迎来更大规模的行业级部署和应用。

（三）技术创新持续升级

随着针对工业领域的实战化网络攻防演习行动的增多，产业发展将从单纯合规驱动逐步转向合规与防护效果双轮

驱动，安全产品和服务效能将逐步受到重视，工业信息安全技术将从被动防御加快向动态防护、精准防护、整体防控等主动防御升级。更为多元化的工业企业用户安全需求也将推动安全厂商加快技术创新，不断丰富安全产品类型，积极提升安全服务质量。

（四）市场竞争持续加剧

未来，工业信息安全市场整体竞争将更为激烈，各类市场玩家将发挥各自技术、市场和资源优势加速布局，聚焦行业痛点问题，将技术突破、模式创新与产业实际需求相结合，形成更多面向特定场景、具有更大价值的行业解决方案。同时，工业企业、工控系统厂商、安全企业、研究机构、行业主管部门等产业链相关方将继续深化合作，逐步形成政府引导、用户主导、厂商参与和资本推动的良性产业生态。