

# 2024-2030年中国AI安全 产业发展现状与行业前景预测报告

## 报告目录及图表目录

北京迪索共研咨询有限公司

[www.cction.com](http://www.cction.com)

## 一、报告报价

《2024-2030年中国AI安全产业发展现状与行业前景预测报告》信息及时，资料详实，指导性强，具有独家，独到，独特的优势。旨在帮助客户掌握区域经济趋势，获得优质客户信息，准确、全面、迅速了解目前行业发展动向，从而提升工作效率和效果，是把握企业战略发展定位不可或缺的重要决策依据。

官方网站浏览地址：<http://www.cction.com/report/202404/452600.html>

报告价格：纸介版8000元 电子版8000元 纸介+电子8500元

北京迪索共研咨询有限公司

订购电话: 400-700-9228(免长话费) 010-69365838

海外报告销售: 010-69365838

Email: kefu@gonyn.com

联系人：李经理

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、说明、目录、图表目录

中企顾问网发布的《2024-2030年中国AI安全产业发展现状与行业前景预测报告》报告中的资料和数据来源于对行业公开信息的分析、对业内资深人士和相关企业高管的深度访谈，以及共研分析师综合以上内容作出的专业性判断和评价。分析内容中运用共研自主建立的产业分析模型，并结合市场分析、行业分析和厂商分析，能够反映当前市场现状，趋势和规律，是企业布局煤炭综采设备后市场服务行业的重要决策参考依据。

报告目录：第1章：AI安全行业综述及数据来源说明 1.1 AI定义与界定 1.1.1 人工智能定义 1.1.2 人工智能发展历程 1.2 AI安全定义与界定 1.2.1 AI安全定义 1.2.2 AI安全内涵 1.3 AI安全分类 1.3.1 AI安全分类概括 1.3.2 人工智能助力安全 1.3.3 人工智能内生安全 1.3.4 人工智能衍生安全 1.4 《国民经济行业分类与代码》中AI安全归属 1.5 AI安全专业术语说明 1.6 本报告研究范围界定说明 1.7 本报告数据来源及统计标准说明 1.7.1 本报告权威数据来源 1.7.2 本报告研究方法及统计标准说明 第2章：中国AI安全行业宏观环境分析（PEST） 2.1 中国AI安全行业政策（Policy）环境分析 2.1.1 行业监管体系及机构介绍 （1）中国AI安全行业主管部门 （2）中国AI安全行业自律组织 2.1.2 行业标准体系建设现状 （1）中国AI安全行业标准体系建设 （2）中国AI安全行业现行标准分析 1）中国AI安全行业现行标准汇总 2）中国AI安全行业现行标准分析 （3）中国AI安全行业即将实施标准 （4）中国AI安全行业重点标准解读 2.1.3 国家层面AI安全行业政策规划汇总及解读 （1）中国AI安全行业国家层面重点相关政策汇总 （2）中国AI安全行业国家层面重点相关规划汇总 2.1.4 国家层面重点政策对AI安全行业发展的影响分析 （1）《关于促进云网融合 加快中小城市信息基础设施建设的通知》 （2）《新一代人工智能伦理规范》 2.1.5 国家层面重点规划对AI安全行业发展的影响分析 （1）《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》 （2）《“双千兆”网络协同发展行动计划（2021-2023年）》 （3）《新一代人工智能发展规划》 2.1.6 中国AI安全行业区域政策热力图 2.1.7 中国AI安全产业各省市政策汇总及解读 （1）中国AI安全产业各省市重点政策汇总 （2）中国各省市AI安全行业发展目标解读 2.1.8 政策环境对行业发展的影响分析 2.2 中国AI安全行业经济（Economy）环境分析 2.2.1 中国宏观经济发展现状 （1）中国GDP及增长情况 （2）中国三次产业结构 （3）中国居民消费价格（CPI） （4）中国生产者价格指数（PPI） （5）中国第三产业增加值 2.2.2 中国宏观经济发展展望 （1）国际机构对中国GDP增速预测 （2）国内机构对中国宏观经济指标增速预测 2.2.3 中国AI安全行业发展与宏观经济相关性分析 2.3 中国AI安全行业社会（Society）环境分析 2.3.1 中国AI安全行业社会环境分析 （1）中国人口规模及增速 （2）中国城镇化水平变化 1）中国城镇化现状 2）中国城镇化趋势展望 （3）中国居民人均可支配收入 （4）中国居民人均消费支出及结构 1）中国居民人均消费支出 2）中国居民消费结构变化 （5）中国网民规模及互联网普及率 2.3.2 社会环境对AI

安全行业的影响总结 2.4 中国AI安全行业技术（Technology）环境分析 2.4.1 AI安全行业技术工艺及流程 2.4.2 AI安全行业关键技术/新兴技术分析 2.4.3 中国AI安全行业研发投入状况 2.4.4 中国AI安全行业研发创新成果 （1）中国AI安全行业专利申请公开 1）专利申请数量变化情况 2）专利公开数量变化情况 （2）中国AI安全行业热门专利申请人 （3）中国AI安全行业热门技术 2.4.5 技术环境对中国AI安全行业发展的影响总结 第3章：全球AI安全发展现状及市场 3.1 全球AI安全发展历程介绍 3.2 全球AI安全宏观环境背景 3.2.1 全球AI安全经济环境概况 （1）国际宏观经济现状 （2）主要地区宏观经济走势分析 1）美国宏观经济环境分析 2）欧元区宏观经济环境分析 3）日本宏观经济环境分析 （3）国际宏观经济预测 3.2.2 全球AI安全政法环境概况 （1）全球AI安全政策环境现状分析 （2）全球AI安全标准规范制定情况 3.2.3 全球AI安全技术环境概况 （1）全球AI安全技术发展概括 （2）全球AI安全技术发展成果 3.3 全球AI安全发展现状及市场规模情况分析 3.3.1 全球AI安全市场发展现状 3.3.2 全球AI安全市场规模情况 3.4 全球AI安全重点区域市场研究 3.4.1 北美地区AI安全发展状况 （1）北美地区AI安全发展背景 （2）北美地区AI安全发展现状 （3）北美地区AI安全发展前景 3.4.2 欧洲地区AI安全发展状况 （1）欧洲地区AI安全发展背景 （2）欧洲地区AI安全发展现状 （3）欧洲地区AI安全发展前景 3.4.3 亚太地区AI安全发展状况 （1）亚太地区AI安全发展背景 （2）亚太地区AI安全发展现状 （3）亚太地区AI安全发展前景 3.5 全球AI安全市场竞争格局及重点企业案例研究 3.5.1 全球AI安全市场竞争格局 （1）企业竞争格局 （2）地区竞争格局 3.5.2 全球AI安全企业兼并重组状况 3.5.3 全球AI安全重点企业案例 （1）IBM 1）企业发展历程及基本信息 2）企业运营状况 3）企业业务结构 4）企业销售网络 5）企业AI安全业务布局状况 （2）Meta Platforms, Inc 1）企业发展历程及基本信息 2）企业运营状况 3）企业业务结构 4）企业销售网络 5）企业AI安全业务布局状况 （3）DarkTrace 1）企业发展历程及基本信息 2）企业运营状况 3）企业业务结构 4）企业AI安全业务布局状况 5）企业AI安全业务销售状况 3.6 全球AI安全发展趋势预判及市场前景预测 3.6.1 全球AI安全发展趋势预判 3.6.2 全球AI安全市场前景预测 第4章：中国AI安全发展现状及市场痛点分析 4.1 中国AI安全形势 4.1.1 人工智能安全挑战 （1）基础设施面临安全挑战 （2）设计研发安全风险突出 （3）应用失控风险危害显著 （4）其他安全挑战 4.1.2 人工智能周期风险 4.2 中国AI安全威胁分析 4.2.1 新的攻击威胁 （1）攻击方法 （2）攻击影响 4.2.2 算法模型安全隐患 4.2.3 人工智能数据安全威胁 （1）人工智能自身面临的数据安全风险 （2）人工智能应用导致的数据安全风险 （3）人工智能应用加剧的数据治理挑战 4.2.4 基础设施安全隐患 4.2.5 应用安全隐患 4.2.6 人工智能滥用 4.3 中国AI安全市场特征 4.4 中国AI安全市场主体类型及入场方式 4.4.1 中国AI安全行业市场主体类型 4.4.2 中国AI安全行业企业入场方式 4.5 中国AI安全市场主体数量规模 4.6 中国AI安全事件汇总 4.7 中国AI安全能力分析 4.7.1 AI安全防御手段 4.7.2 AI安全攻防技术

(1) 闪避攻击防御技术 (2) 药饵攻击防御技术 (3) 后门攻击防御技术 (4) 模型/数据防窃取技术 4.8 中国AI安全布局现状 4.8.1 中国AI安全市场供给分析 4.8.2 中国AI安全市场需求状况 (1) 中国网络信息安全领域需求分析 1) 网络安全防护应用 2) 信息内容安全审查应用 3) 数据安全应用 (2) 中国社会公共安全应用领域需求分析 1) 智能安防应用 2) 金融风控应用 4.9 中国AI安全市场规模测算 第5章：中国AI安全竞争状况及市场格局解读 5.1 中国AI安全市场竞争格局分析 5.1.1 中国AI安全行业企业集群分布 5.1.2 中国AI安全行业企业竞争格局 5.2 中国AI安全投融资、兼并与重组状况 5.2.1 中国AI安全行业投融资分析 5.2.2 中国AI安全行业并购重组分析 第6章：中国AI安全产业链全景梳理及布局状况研究 6.1 中国AI安全产业结构属性(产业链)分析 6.1.1 中国AI安全产业链结构梳理 6.1.2 中国AI安全产业链生态图谱 6.2 中国AI安全体系架构 6.3 中国AI安全之“业务安全”市场布局状况 6.3.1 中国AI安全之“业务安全”业务合规性评估 6.3.2 中国AI安全之“业务安全”业务安全攻击监测 6.3.3 中国AI安全之“业务安全”业务安全机制 (1) 发展现状 (2) 企业布局 6.3.4 中国AI安全之“业务安全”业务恶意应用监测 6.4 中国AI安全之“算法安全”市场布局状况 6.4.1 中国AI安全之“算法安全”算法鲁棒性增强 6.4.2 中国AI安全之“算法安全”算法公平性保障 6.4.3 中国AI安全之“算法安全”算法可解释性提升 6.4.4 中国AI安全之“算法安全”算法知识产权保护 6.4.5 中国AI安全之“算法安全”算法安全评测 (1) 发展现状 (2) 企业布局 6.5 中国AI安全之“数据安全”市场布局状况 6.5.1 中国AI安全之“数据安全”数据隐私计算 (1) 发展现状 (2) 企业布局 6.5.2 中国AI安全之“数据安全”数据追踪溯源 (1) 发展现状 (2) 企业布局 6.5.3 中国AI安全之“数据安全”问题数据清洗 (1) 发展现状 (2) 企业布局 6.5.4 中国AI安全之“数据安全”数据公平性增强 (1) 发展现状 (2) 企业布局 6.5.5 中国AI安全之“数据安全”数据安全评测 6.6 中国AI安全之“平台安全”市场布局状况 6.6.1 中国AI安全之“平台安全”漏洞挖掘修复 (1) 发展现状 (2) 企业布局 6.6.2 中国AI安全之“平台安全”模型文件校验 (1) 发展现状 (2) 企业布局 6.6.3 中国AI安全之“平台安全”框架平台安全部署 (1) 发展现状 (2) 企业布局 6.7 中国AI安全“应用层”行业解决方案及案例分析 6.7.1 自动驾驶领域AI安全解决方案及案例分析 (1) 安全风险 1) 传感器数据干扰风险 2) 算法攻击安全风险 (2) 安全防护 1) 计算环境安全 2) AI算法安全防御 3) AI业务安全防御 4) 企业布局分析 6.7.2 信贷风控领域AI安全解决方案及案例分析 (1) 安全风险 (2) 安全防护 1) 安全防护措施分析 2) 企业布局分析 6.7.3 深度伪造领域AI安全解决方案及案例分析 (1) 安全风险 (2) 安全防护 1) 技术检测 2) 内容溯源 3) 企业布局分析 第7章：中国AI安全企业布局案

例研究 7.1 中国AI安全企业布局梳理 7.2 中国AI安全企业布局案例分析 7.2.1 阿里云计算有限公司 (1) 企业基本信息 (2) 企业生产经营基本情况 1) 企业整体经营状况 2) 企业整体业务架构 3) 企业销售布局情况 (3) 企业AI安全业务布局状况 (4) 企业AI安全技术能力 (5) 企业AI安全业务布局规划及最新动向追踪 1) 企业研发投入 2) 企业AI安全最新发展动向追踪 (6) 企业AI安全布局优劣势分析 7.2.2 绿盟科技集团股份有限公司 (1) 企业基本信息 (2) 企业业务架构及经营情况 1) 企业整体经营情况 2) 企业整体业务架构 3) 企业销售布局情况 (3) 企业AI安全行业业务布局及发展状况 1) AI安全产品 2) AI安全解决方案 (4) 企业应AI安全行业业务科研投入及创新成果追踪 1) 企业研发投入 2) 企业AI安全最新发展动向追踪 (5) 企业AI安全行业业务发展优劣势分析 7.2.3 深圳市腾讯计算机系统有限公司 (1) 企业基本信息介绍 (2) 企业业务架构及经营情况 1) 企业整体经营情况 2) 企业整体业务架构 3) 企业销售布局情况 (3) 企业AI安全业务布局及发展状况 1) 企业AI研究领域 2) 企业AI安全布局 (4) 企业AI安全业务最新发展动向追踪 1) 企业研发投入 2) 企业AI安全最新发展动向追踪 (5) 企业AI安全布局优劣势分析 7.2.4 苏州三六零智能安全科技有限公司 (1) 企业基本信息 (2) 企业业务架构及经营情况 1) 企业整体经营情况 2) 企业整体业务架构 3) 企业销售布局情况 (3) 企业AI安全行业业务布局及发展状况 (4) 企业应AI安全行业业务科研投入及创新成果追踪 (5) 企业AI安全行业业务发展优劣势分析 7.2.5 华为技术有限公司 (1) 企业发展历程及基本信息 (2) 企业生产经营基本情况 1) 企业整体经营数据 2) 企业整体业务架构 3) 企业销售布局情况 (3) 企业AI安全业务布局状况 1) 企业AI安全产品及服务 2) AI安全解决方案 (4) 企业AI安全技术能力 (5) 企业AI安全业务布局规划及最新发展动向追踪 (6) 企业AI安全布局优劣势分析 7.2.6 深信服科技股份有限公司 (1) 企业基本信息 (2) 企业业务架构及经营情况 1) 企业整体经营情况 2) 企业整体业务架构 3) 企业销售布局情况 (3) 企业AI安全行业业务布局及发展状况 (4) 企业应AI安全行业业务科研投入及创新成果追踪 1) 企业研发投入 2) 企业AI安全最新发展动向追踪 (5) 企业AI安全行业业务发展优劣势分析 7.2.7 上海依图网络科技有限公司 (1) 企业基本信息 (2) 企业业务架构及经营情况 1) 企业整体经营情况 2) 企业整体业务架构 3) 企业销售布局情况 (3) 企业AI安全业务布局状况 (4) 企业AI安全业务布局规划及最新发展动向追踪 1) 企业研发投入 2) 企业AI安全业务最新发展动向追踪 (5) 企业AI安全布局优劣势分析 7.2.8 北京瑞莱智慧科技有限公司 (1) 企业基本信息 (2) 企业业务架构 1) 企业整体业务架构 2) 企业主要客户情况 (3) 企业AI安全业务布局状况 (4) 企业AI安全技术能力 (5) 企业AI安全业务布局规划及最新发展动向追踪 (6) 企业AI安全布局优劣势分析 7.2.9 奇安信科技集团股份有限公司 (1) 企业基本信息 (2) 企业业务架构及经营情况 1) 企业整体经营情况 2) 企业整体业务架构 3) 企业销售布局情况 (3) 企业应AI安全行业业务科研投入及创新

成果追踪 1) 企业研发投入 2) 企业AI安全最新发展动向追踪 (4) 企业AI安全行业业务发展优劣势分析 7.2.10 慧安金科(北京)科技有限公司 (1) 企业基本信息 (2) 企业业务架构 1) 企业整体业务架构 2) 企业主要客户情况 (3) 企业AI安全业务布局状况 (4) 企业AI安全业务布局规划及最新动向追踪 (5) 企业AI安全布局优劣势分析 第8章：中国AI安全市场及战略布局策略建议 8.1 中国AI安全发展因素分析 8.1.1 行业驱动因素 8.1.2 行业制约因素 8.2 中国AI安全发展潜力评估 8.2.1 中国AI安全生命发展周期 8.2.2 中国AI安全发展潜力评估 8.3 中国AI安全发展前景预测 8.4 中国AI安全发展趋势预判 8.5 中国AI安全行业发展壁垒 8.6 中国AI安全投资风险预警 8.6.1 AI安全行业政策风险 8.6.2 AI安全行业技术风险 8.6.3 AI安全行业宏观经济波动风险 8.7 中国AI安全投资价值评估 8.8 中国AI安全投资机会分析 8.9 中国AI安全投资策略与建议 8.10 中国AI安全可持续发展建议 图表目录 图表1：人工智能定义的不同解读 图表2：人工智能行业的框架 图表3：人工智能发展历程 图表4：人工智能安全的界定 图表5：人工智能安全的内涵 图表6：AI安全分类 图表7：人工智能助力安全分析 图表8：AI安全的内生安全 图表9：AI安全的衍生安全 图表10：《国民经济行业分类与代码》中AI安全归属 图表11：AI安全专业术语说明 图表12：本报告研究范围界定 图表13：本报告权威数据资料来源汇总 图表14：本报告的主要研究方法 & 统计标准说明 图表15：中国AI安全行业监管体系构成 图表16：中国AI安全行业主管部门 图表17：中国AI安全行业自律组织 图表18：截至2022年中国AI安全行业标准体系建设(单位：项) 图表19：截至2022年中国AI安全行业的国家标准 图表20：截至2022年中国AI安全行业的行业标准 图表21：截至2022年中国AI安全行业的地方标准 图表22：截至2022年中国AI安全行业的企业标准 图表23：截至2022年中国AI安全行业的团体标准 图表24：截至2022年中国AI安全行业现行标准属性分布(单位：项，%) 图表25：截至2022年即将实行的AI安全行业标准汇总 图表26：中国AI安全行业重点标准解读 图表27：截至2022年中国AI安全行业国家层面重点相关政策汇总 图表28：截至2022年中国AI安全行业国家层面重点相关规划汇总 图表29：《关于促进云网融合 加快中小城市信息基础设施建设的通知》有关AI安全行业的指导内容 图表30：《新一代人工智能伦理规范》政策解读 图表31：《国家“十四五”规划》关于AI安全行业发展建设规划 图表32：《“双千兆”网络协同发展行动计划(2021-2023年)》有关AI安全行业发展建设规划 图表33：《新一代人工智能发展规划》政策解读 图表34：截至2022年中国AI安全行业区域政策热力图(单位：条) 图表35：中国AI安全产业主要政策汇总及解读 图表36：“十四五”期间中国各省份AI安全行业发展目标 图表37：政策环境对中国AI安全行业发展的影响总结 图表38：2010-2022年中国GDP增长走势图(单位：万亿元，%) 图表39：2010-2022年中国三次产业结构(单位：%) 图表40：2019-2022年中国CPI变化情况(单位：%) 图表41：2019-2022年中国PPI变化情况(单位：%) 图表42：2010-2022年中国第三产

业增加值及增速（单位：万亿元，%） 图表43：部分国际机构对2022-2023年中国GDP增速的预测（单位：%） 图表44：2022年中国宏观经济核心指标预测（单位：%） 图表45：2016-2021年中国GDP与AI安全行业营收规模相关性 图表46：2016-2021年中国固定资产投资额与AI安全行业营收规模相关性 图表47：2010-2021年中国人口规模及自然增长率（单位：万人，‰） 图表48：2010-2021年中国城镇人口规模及城镇化率（单位：万人，%） 图表49：中国城市化进程发展阶段 图表50：2010-2022年中国居民人均可支配收入（单位：元） 图表51：2010-2022年中国居民人均消费支出（单位：元） 图表52：2013-2022年中国居民人均消费支出结构（单位：%） 图表53：2016-2022年H1中国网民规模与普及率情况（单位：亿人，%） 图表54：社会环境对AI安全行业发展的影响分析 图表55：AI安全行业中的攻击与防御技术流程示意图 图表56：中国人工智能安全热点技术方向创新成果 图表57：2017-2021年中国AI安全行业上市公司研发投入情况（单位：亿元） 图表58：2015-2022年10月中国AI安全行业相关专利申请数量变化图（单位：项） 图表59：2015-2022年10月中国AI安全行业相关专利公开数量变化图（单位：项） 图表60：截至2022年10月中国AI安全企业专利排行榜（单位：项） 图表61：截至2022年10月中国AI安全行业热门技术 图表62：技术环境对中国AI安全行业发展的影响总结 图表63：全球AI安全的发展历程 图表64：2016-2021年世界及主要经济体GDP同比增长率（单位：%） 图表65：2016-2021年美国国内生产总值变化趋势图（单位：万亿美元，%） 图表66：2018-2021年欧盟GDP季度同比变化（单位：%） 图表67：2009-2021年日本GDP变化情况（单位：%） 图表68：2022-2023年全球主要经济体经济增速预测（单位：%） 图表69：全球AI安全政法环境现状 图表70：全球AI安全标准规范制定情况介绍 图表71：截至2021年底全球人工智能安全热点技术方向概括 图表72：截至2021年底全球AI安全技术发展成果 图表73：全球主要国家AI安全的关注重点 图表74：2017-2021年全球AI安全市场规模情况（单位：亿美元） 图表75：美国AI安全的发展背景 图表76：2017-2021年北美地区AI安全市场规模情况（单位：亿美元） 图表77：2022-2027年北美地区AI安全市场规模预测（单位：亿美元） 图表78：欧洲AI安全的发展背景 图表79：2018-2021年欧洲地区AI安全市场规模情况（单位：亿美元） 图表80：2022-2027年欧洲AI安全市场规模预测（单位：亿美元） 图表81：日本AI安全的发展背景 图表82：2017-2021年亚太地区AI安全市场规模情况（单位：亿美元） 图表83：2022-2027年亚太地区AI安全市场规模预测（单位：亿美元） 图表84：截至2022年全球AI安全市场竞争格局 图表85：截至2022年10月全球AI安全相关技术专利来源国/地区（单位：项，%） 图表86：2010-2022年全球AI安全相关技术专利TOP10国/地区申请趋势（单位：项） 图表87：截至2022年全球AI安全主要企业兼并重组状况（单位：亿美元，万美元） 图表88：IBM公司发展历程 图表89：IBM公司基本信息表 图表90：2017-2021年IBM公司主要经济指标分析（单位：亿美元） 图表91：2021年IBM公司主营构



成（单位：亿美元，%） 图表92：IBM公司软件业务结构 图表93：2021年IBM公司区域销售收入分布（单位：亿美元，%） 图表94：IBM的人工智能三原则 图表95：IBM的AIF360 workflow 图表96：Meta Platforms公司发展历程 图表97：Meta Platforms公司基本信息表 图表98：2017-2021年Meta Platforms公司经营业绩情况（单位：亿美元） 图表99：Facebook（Meta）主要产品 图表100：2021年Meta Platforms公司主营构成（单位：亿美元，%） 图表101：2021年Meta Platforms公司区域销售收入分布（单位：亿美元，%） 图表102：Darktrace公司基本信息表 图表103：2020-2022财年Darktrace公司的经营情况（单位：亿美元） 图表104：DarkTrace公司的业务布局情况 图表105：DarkTrace公司的AI安全业务布局 图表106：DarkTrace公司的企业AI安全业务客户情况 图表107：全球AI安全发展趋势预判 图表108：2022-2027年全球AI安全市场规模预测（单位：亿美元） 图表109：2013-2021年CNVD收录漏洞情况（单位：个，%） 图表110：人工智能设计研发安全风险 图表111：人工智能应用失控风险危害 图表112：中国AI安全系统在设计上面临五大安全挑战 图表113：人工智能周期阶段风险地图 图表114：针对AI系统的攻击方法分析 图表115：人工智能新的攻击威胁攻击影响 图表116：中国人工智能算法模型安全隐患 图表117：人工智能系统的数据生命周期 图表118：人工智能自身面临的数据安全风险 图表119：人工智能应用导致的数据安全风险 图表120：人工智能应用加剧的数据治理挑战

详细请访问：<http://www.cction.com/report/202404/452600.html>