2021年中国数据安全行业分析报告-行业全景调查与发展动向研究

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《2021年中国数据安全行业分析报告-行业全景调查与发展动向研究》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/hulianwang/552810552810.html

报告价格：电子版: 8200元　纸介版：8200元　电子和纸介版: 8500

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

根据《GB/T37988-2019信息安全技术 数据安全能力成熟度模型》国家标准，数据的生命周期分为采集、传输、存储、处理、交换和销毁六个阶段。数据安全体系包括边界安全、访问控制和授权、数据保护、审计监控等四个层面。

数据安全体系

体系

简介

具体内容

边界安全

授权合法用户访问大数据平台集群

身份认证：关注外部用户或者第三方服务对集群的访问过程中的身份鉴别，用户在访问启用安全认证的集群时，需通过服务所需要的安全认证方式。

网络隔离：大数据平台集群支持通过网络平面隔离的方式保证网络安全。

传输安全：关注数据在传输过程中的安全性，包括采用安全接口设计及高安全的数据传输协议，保证在通过接口访问、处理、传输数据时的安全性，避免数据被非法访问、窃听或旁路嗅探。

访问控制

定义可以访问、应用数据的用户

权限控制：包括鉴权、授信管理，即确保用户对平台、接口、操作、资源、数据等都具有相应的访问权限，避免越权访问；分级管理，即根据敏感度对数据进行分级，对不同级别的数据提供差异化的流程、权限、审批要求等管理措施。

审计管理：基于底层提供的审计数据，在权限管理、数据使用、操作行为等多个维度上对大数据平台的运转提供安全审计能力，确保及时发现大数据平台中的隐患点。

数据审计

数据溯源、数据使用和销毁路径跟踪

数据生命周期管理：追溯大数据平台中数据的来源，熟知数据使用、销毁情况，通过安全审计监测大数据系统中是否存在非法数据访问。安全审计的目的是捕获系统内的完整活动记录，且不可被更改，遵守“事前可管、事中可控、事后可查”，三大原则。

日志审计：对日志和审计记录做集中管理和分析。

数据保护

数据加密和脱敏；多租户隔离；数据侵权保护；容灾管理

数据加密：提供数据在传输过程及静态存储的加密保护，在敏感数据被越权访问时仍然能够得到有效保护。

用户隐私数据脱敏：提供数据脱敏和个人信息去标识化功能，提供满足国际密码算法的用户

数据加密服务。
多租户隔离：实施多租户访问隔离措施，实施数据安全等级划分，支持基于标签的强制访问控制，提供基于ACL的数据访问授权模型，提供全局数据视图和私有数据视图，提供数据视图的访问控制。
数据容灾：为集群内部数据提供实时的异地数据容灾功能。
数据侵权保护：利用区块链类似技术实现数据的溯源确权。数据来源：公开资料整理
一、优势分析
（1）泛数据安全为数据安全发展提供方法论和体系框架
除传统围绕数据的生命周期，安全领域还有一些产业与数据安全息息相关，具体包括数据安全治理、身份与访问管理（“零信任”体系）、隐私计算、云数据安全（SASE）等泛数据安全。泛数据安全为数据安全发展提供方法论和体系框架。
泛数据安全典型应用
典型应用
具体情况
数据安全治理
指从决策层到技术层，从管理制度到工具支撑，自上而下建立的数据安全保障体系和保护生态，包含国家宏观治理和企业组织内部微观自治两个层面。其中企业组织内部自治旨在规范企业组织数据全生命周期处理流程，保证数据处理活动的合规性和合法性。除具体相关技术产品外，数据安全治理多以咨询服务的形式体现。
身份与访问管理
主要指访问控制，即精选出来的一系列数据访问规则，主要包含身份验证与授权两个组成部分。身份验证是用于验证给定用户是否是其所声称的身份的一种技术，而授权技术是确定用户是否可以访问数据或执行其所尝试操作的技术。
“零信任”体系
零信任指一组以“信任从不被隐式授予，而是必须持续评估”为前提的概念和设计思想，而“零信任体系”是基于零信任的一种企业资源和数据安全端到端的保护方法，包含人和非人实体的身份标识、认证信息、访问管理、操作运维、端点管控、运行环境和互连基础设施等内容。
隐私计算
隐私计算体系通过融合多学科技术，使得两个或多个参与方可以在不泄漏各自数据的前提下进行联合计算，在保护数据安全的同时实现多源数据跨域合作，推进数据融合价值的挖掘。目前主流的隐私计算技术路径包含多方安全计算、联邦学习和可信计算三大方向。
云数据安全
云数据安全可从两个层面理解:一个层面为把用户在数据安全上需要使用到的所有的能力抽象化，以云服务的方式提供，以最简便的方式保证用户和开发者的数据安全;另一个层面为

云内应用的数据安全，这包括存储数据的敏感内容发现、数据流动的监控和保护、以及数据内容的安全分析等。

SASE

SASE（Secure Access Service Edge，安全访问服务边缘）是一个基于云化部署的网络和安全组件框架，包含了SD-WAN、云访问安全代理(CASB)、安全的web网关(SWG)、零信任网络访问(zTNA)、防火墙即服务（FWaaS)和远程浏览器隔离（RBI）等一套技术。SASE将身份作为安全架构的中心，确保通常以云服务形式提供的应用程序、服务、用户和机器对云和网络资源的安全访问。数据来源：公开资料整理

（2）数据安全战略由“被动”走向“主动”

传统网络安全防护多立足于边界防护，通过购买安全设备被动抵御外来数据侵略。基于防护对象的拓展和防护思想的转变，被动防御策略已无法适应当前的网络安全形势。伴随大数据分析、人工智能、安全情报收集等技术的逐渐成熟和发展，安全检测技术对安全态势的分析、预警和预测愈加准确，网络安全防御体系逐渐向自动响应、追查、威胁诱捕等方向的主动防御体系转变。

数据安全主动防护策略 数据来源：公开资料整理

（3）数据量快速攀升使得数据安全意识不断提升

数据显示，2020年，全球数据量达到了60ZB，其中中国数据量增速迅猛。预计2025年中国数据量将增至48.6ZB，占全球数据量的27.8%。数据量的增加，数据背后可被挖掘的信息也逐渐丰富，政府和企业开始逐渐意识到数据泄露的严重后果，对数据安全的重视程度日益提升。

2017-2025年全球数据量、增速及预测 数据来源：公开资料整理

2018-2025年中国数据量占全球数据量的比重 数据来源：公开资料整理

二、劣势分析

（1）技术仍待进步

国内外的大数据安全技术虽然已经取得了一定进步，但是面对层出不穷的新式大数据攻击，防护措施仍然显得不够充分。其原因是传统的安全防护观念以及技术无法满足大数据安全防护的需求。其中密文计算技术、数据泄露追踪技术的发展仍无法满足实际的应用需求，难以解决数据处理过程的机密性保障问题和数据流动路径追踪溯源问题。

（2）数据孤岛效应明显

企业各职能部门之间联系薄弱，现阶段数据孤岛效应明显。不管企业使用哪一种组织架构，数据的冗杂、前台与后台之间的接洽困难、业务与数据的孤立等问题，现阶段企业内、企业间数据割裂仍然是阻碍数据协作应用的重要障碍，不利于对数据安全的保障。

三、机遇分析

（1）勒索软件威胁日趋严重

自2016年起，勒索软件在全球范围内呈现爆发式增长，中国成为亚太地区受影响最严

重的国家之一。数据显示，2018年H1，中国恶意网站数量达226万个，主要分布在广东、上海、北京等一线城市。随着勒索软件威胁日趋严重，数据安全服务需求增长，成为推动行业发展的主要驱动力。

2018年上半年部分国家恶意网站地域分布 数据来源：公开资料整理

2018年上半年中国勒索软件感染地域分布（前十名省市） 数据来源：公开资料整理

（2）数据泄漏途径多元化

数据泄漏途径呈现多元化。数据泄露原因包括黑客的恶意攻击、内部工作人员的信息贩卖、第三方外包人员的交易行为、数据共享第三方的数据泄露、开发测试人员的违规等。社会及企业安全部门数据安全意识薄弱，以及传统网络安全体系老旧或安全策略的缺陷是导致数据泄露的主要原因。社会各界对数据资产安全的关注度与日俱增，减轻数据泄露为社会发展带来的影响，加强数据防护、抵御不法黑客恶意入侵成为行业发展动力。

国内部分数据泄露事件一览

分类

事件名称

事件时间

泄露人员

泄露数据规模

非法所得（元）

政府部门

南京公务员泄露居民信息

2018-01

内部人员，副主任科员刘某

82万条

-

国家宏观经济数据泄露

2010-2011

原国家统计局干部孙振等

多次泄露

-

教育

教育考试信息泄露

2016-08

黑客入侵

-

5万

医疗
疾控中心信息泄露
2016-07
黑客入侵
30个省的275例
-
上海新生儿信息外泄
2016-07
原上海疾控中心工作人员韩某等
20万新生儿信息
-
社保
篡改退休人员数据非法牟利
2010-2011
某市社保局退管中心蔡某等
-
280万
非法获得养老金
2005-2008
某区社保事业管理处副主任王某等
-
190.5万
其他
博士黑客贩卖公民信息
2018-04
某国有大型科技公司数据库员工
500余万条60G容量
-数据来源：公开资料整理

（3）政策支持

此前，我国前已颁布多部相关法律法规，《个人信息保护法》、《关保条例》、《数据安全法》将一步完善数据安全要求。

我国数据安全行业相关政策
日期
政策名称
制定部门

主要内容

2021.08.21

《中华人民共和国个人信息保护法》

全国人大常委会

一、个人信息保护法明确处理个人信息应当在事先充分告知的前提下取得个人同意，个人信息处理的重要事项发生变更的应当重新向个人告知并取得同意。同时，针对现实生活中社会反映强烈的一揽子授权、强制同意等问题，个人信息保护法特别要求，个人信息处理者在处理敏感个人信息、向他人提供或公开个人信息、跨境转移个人信息等环节应取得个人的单独同意，明确个人信息处理者不得过度收集个人信息，不得以个人不同意为由拒绝提供产品或者服务，并赋予个人撤回同意的权利，在个人撤回同意后，个人信息处理者应当停止处理或及时删除其个人信息。二、随着越来越多的企业利用大数据分析、评估消费者的个人特征用于商业营销。有一些企业通过掌握消费者的经济状况、消费习惯、对价格的敏感程度等信息，对消费者在交易价格等方面实行歧视性的差别待遇，误导、欺诈消费者。其中，最典型的就是社会反映突出的“大数据杀熟”“。对此，个人信息保护法明确规定：个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。三、个人信息保护法将生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息列为敏感个人信息。个人信息保护法要求，只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，方可处理敏感个人信息，同时应当事前进行影响评估，并向个人告知处理的必要性以及对个人权益的影响。

2019.06

《个人信息出境安全评估办法》

国家互联网信息办公室

明确网络运营者向境外提供在中国境内运营中收集的个人信息时需进行安全评估，极大地扩大了个人信息主体的权益，加强了出境数据非法利用的限制，保护个人数据安全

2019.05

《数据安全管理办法（征求意见稿）》

国家互联网信息办公室

维护国家安全、社会公共利益，保护公民、法人和其他组织在网络空间的合法权益，保障个人信息和重要数据安全

2018.04

《科学数据管理办法》

国务院办公厅

加强科学数据全生命周期管理，将数据安全放在首要位置，加强和规范科学数据管理，通过提升中国科学数据工作水平，为提高科技创新、保障国家数据安全提供支撑

2017.12

《信息安全技术大数据交易服务安全要求》
国家标准化管理委员会
有助于理清数据交易安全界限，促进数据交易行为合法合规，推动中国数据交易机构的安全建设，促进数据交易行为合法合规，促进全国数据要素有序流通，充分释放数据红利，助力“数字中国”建设
2017.08
《信息安全技术数据安全能力成熟度模型》
全国信息安全标准化技术委员会
帮助各行业、组织机构基于统一标准来评估其数据安全能力，发现数据安全能力短板，查漏补缺，促进大数据参与方的数据安全能力评估与提升，促进大数据在组织间的交换、共享与流转，发挥大数据的价值，促进中国大数据产业的健康发展
2016.11
《中华人民共和国网络安全法》
全国人民代表大会常务委员会
保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定的法律数据来源：公开资料整理

2021年3月22日，国家互联网信息办公室、工业和信息化部、公安部、国家市场监督管理总局四部门联合公开发布《常见类型移动互联网应用程序必要个人信息范围规定》，正式施行日期为2021年5月1日。明确了“必要个人信息”的定义，即“保障App基本功能服务正常运行所必需的个人信息，缺少该信息App即无法实现基本功能服务”。 常见类型移动互联网应用程序必要个人信息范围规定
类型
基本功能
必要个人信息
常见APP
地图导航类
定位和导航
位置信息、出发地、到达地。
百度地图、高德地图、苹果地图APP
网络约车类
网络预约出租汽车服务、巡游出租汽车电召服务
注册用户移动电话号码；乘车人出发地、到达地、位置信息、行踪轨迹；支付时间、支付金额、支付渠道等支付信息（网络预约出租汽车服务）。
滴滴、花小猪、嘀嗒、T3出行
即时通信类

提供文字、图片、语音、视频等网络即时通信服务
注册用户移动电话号码；账号信息：账号、即时通信联系人账号列表。
微信、QQ、钉钉、企业微信、Tim
网络社区类
博客、论坛、社区等话题讨论、信息分享和关注互动
注册用户移动电话号码。
微博、小红书、知乎、豆瓣、虎扑
网络支付类
网络支付、提现、转账等功能
注册用户移动电话号码；注册用户姓名、证件类型和号码、证件有效期限、银行卡号码。
支付宝、applepay、云闪付、银行官方APP
网上购物类
购买商品
注册用户移动电话号码；收货人姓名（名称）、地址、联系电话；支付时间、支付金额、支付渠道等支付信息。
淘宝、京东、拼多多、唯品会
餐饮外卖类
餐饮购买及外送
注册用户移动电话号码；收货人姓名（名称）、地址、联系电话；支付时间、支付金额、支付渠道等支付信息。
美团、饿了吗、盒马鲜生
邮件快件寄递类
信件、包裹、印刷品等物品寄递服务
寄件人姓名、证件类型和号码等身份信息；寄件人地址、联系电话；收件人姓名（名称）、地址、联系电话；寄递物品的名称、性质、数量。
菜鸟、丰巢、闪送、顺丰速运、圆通快递
交通票务类
交通相关的票务服务及行程管理（如票务购买、改签、退票、行程管理等）
注册用户移动电话号码；旅客姓名、证件类型和号码、旅客类型。旅客类型通常包括儿童、成人、学生等；旅客出发地、目的地、出发时间、车次/船次/航班号、席别/舱位等级、座位号（如有）、车牌号及车牌颜色（ETC服务)；支付时间、支付金额、支付渠道等支付信息。
12306、携程、去哪儿、飞猪
婚恋相亲类
婚恋相亲

注册用户移动电话号码；婚恋相亲人的性别、年龄、婚姻状况。
珍爱网、世纪佳缘、谈谈数据来源：公开资料整理

四、威胁分析

（1）核心软硬件垄断风险

我国数据安全行业产业链上游安全存储芯片、信息安全芯片等核心部件对国外产品依存度较高。未来，随着数据安全行业发展，信息安全芯片需求量将持续升高，而信息安全芯片自主生产力的缺失易导致数据安全行业面临核心软硬件垄断风险。

数据显示，我国信息安全芯片需求量由2013年的6.3亿颗增长至2017年的20.4亿颗，预计2021年我国信息安全芯片需求量将达59.69亿颗。
2013-2021年我国信息安全芯片行业需求量及预测 数据来源：公开资料整理

（2）人才缺口大

伴随我国数据安全行业发展，市场对人才需求量不断增加，尤其是一线和新一线城市地区，人才需求数量占全国需求总量60%以上。但由于我国网络信息安全行业起步较晚，网络安全人才短缺，数据安全行业面临专业人才缺乏威胁。同时，网络安全人才的缺乏使得相关职位薪酬的快速提升，导致企业雇佣成本较高。
2018年我国各地区网络安全人才需求占比情况 数据来源：公开资料整理（zlj）

（3）政策威胁

目前，我国数据安全行业仍存在基本法缺位、“数据主权”地位尚未确立，数据经营难有效监管等问题。“网络安全法”主要是针对网络层面的安全规范，但未能从数据信息全维度进行规范，相关配套政策文件法律层级低，要求较为分散，难以系统性解决数据安全保障问题。

本研究报告数据主要采用国家统计数据，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家统计局规模企业统计数据库及证券交易所等，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、PEST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。

【目录大纲】