数据安全白皮书

目录

1 全球新经济形态及主要经济体数据战略

1.1 全球新经济形态及主要经济特征 ---- 03
1.2 全球主要经济体数据战略 ---- 04
1.2.1 美国数据战略 ---- 04
1.2.2 欧盟数据战略 ---- 04
1.2.3 英国数据战略 ---- 05
1.2.4 中国数据战略 ---- 05
1.3 数据安全在数据产业生态中的战略意义 ---- 06

2 数据产业新生态的安全需求与挑战

2.1 数据产业新生态及发展趋势 ---- 07
2.2 数据产业新商业模式对数据安全的需求 ---- 08
2.3 产业升级和技术发展对数据安全提出了新挑战 ---- 08
2.3.1 人工智能领域 ---- 09
2.3.2 超算领域 ---- 10
2.3.3 数据中心 ---- 11
2.3.4 金融领域 ---- 12
2.3.5 工业互联网领域 ---- 12
2.3.6 医疗领域 ---- 12
2.4 数据安全对核心技术能力的诉求 ---- 13

3 数据安全的总体策略及治理思路

3.1 数据安全的总体策略 ---- 14
3.1.1 合法合规 ---- 14
3.1.2 安全与发展并重 ---- 14
3.1.3 以数据为中心构建安全体系架构 ---- 14
3.2 数据安全治理核心思想 ---- 15
3.3 数据安全治理的三个层面 ---- 16

4 数据安全的产业基础

4.1 数据存储介质 ---- 18
4.2 存储网络 ---- 19
4.3 数据存储软件系统 ---- 20
4.4 数据基础设施的绿色节能 ---- 21
4.4.1 介质节能 ---- 22
4.4.2 架构节能 ---- 22
4.4.3 算法节能 ---- 23

5 数据安全防护的关键技术

5.1 设备系统安全技术 ---- 25
5.1.1 可信启动 ---- 26

5.1.2 可信执行环境 ····· 26
5.1.3 操作系统内核的MAC ····· 26
5.1.4 操作系统内核完整性保护 ····· 26
5.1.5 芯片安全 ····· 26
5.2 密码学及隐私保护算法 ····· 27
5.3 认证和访问控制技术 ····· 29
5.4 关键业务的高可靠数据保护技术 ····· 30
5.5 数据安全管理技术 ····· 32
5.5.1 数据资产安全分析技术 ····· 32
5.5.2 数据安全审计 ····· 32
5.5.3 人工智能技术 ····· 34

6 我国数据安全法律法规体系

6.1 法律法规体系 ····· 35
6.1.1 现行法律法规梳理 ····· 35
6.1.2 《数据安全法（草案）》体系下的立法趋势洞察 ····· 36
6.2 组织保障体系 ····· 37
6.3 监管执行体系 ····· 38
6.4 数据安全评价体系 ····· 38

7 展望及倡议

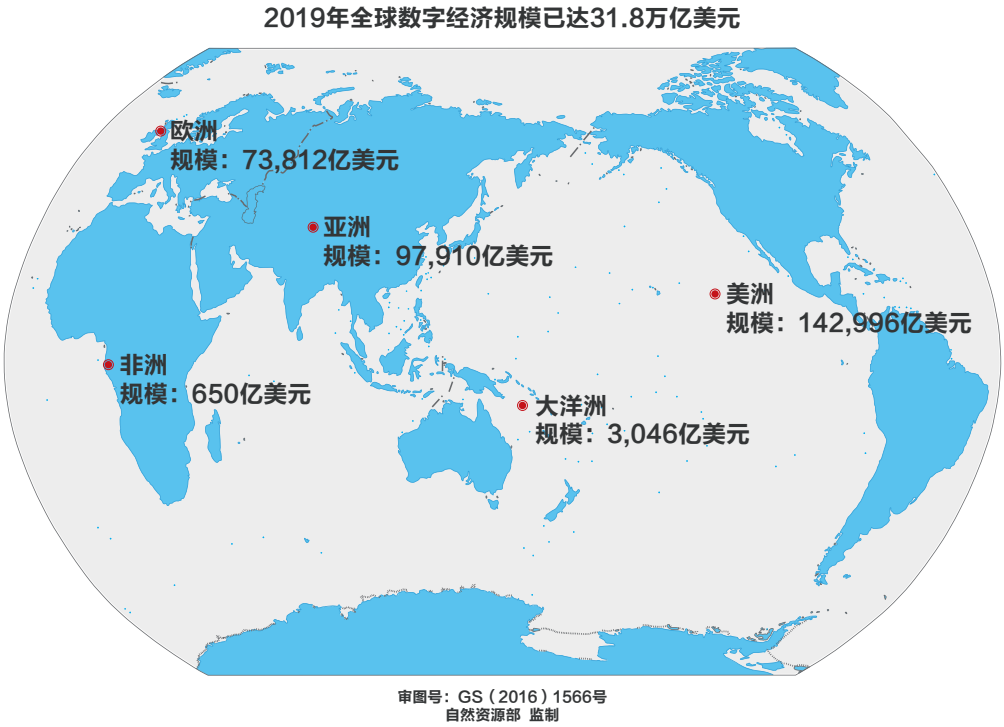
7.1 提升数据安全产业基础能力 ····· 43
7.1.1 加大普及全闪存数据中心力度 ····· 43
7.1.2 强化基础软件技术自主创新能力 ····· 43
7.1.3 促进数据产业绿色节能、高效发展 ····· 44
7.1.4 提升数据在产业应用中的价值变现能力，促进数据安全流通与治理 ····· 44
7.2 加快数据安全防护技术研究与应用 ····· 44
7.2.1 强化数据安全领域关键基础技术的研究与应用 ····· 44
7.2.2 重视核心业务数据的安全保护，确保数据高可靠、高可用 ····· 44
7.2.3 培养储备高素质数据安全人才队伍 ····· 45
7.3 提升法律法规在数据安全主权方面的支撑保障作用 ····· 46

01 全球新经济形态及主要经济体数据战略

1.1 全球新经济形态及主要经济特征

近年来，信息科技革命极大地改变了全球各经济体的经济社会发展。新一代信息技术不断涌现，正影响着各行各业变革和人们的日常生活。在信息技术支撑下，数字经济驱动着全球各经济体的经济总量不断增长。

>>> 图 1-1 2019年全球数字经济规模与分布 <<<



2019年，全球数字经济规模达到31.8万亿美元。从单一国家经济体看，美国走在全球数字经济前列，以13.1万亿美元排名全球第一。中国经过数十年的市场化发展，配以技术创新和模式创新，以5.2万亿美元的经济规模位列全球第二。德国、日本、英国、法国分列三至六名，数字经济规模合计超过3万亿美元。韩国、印度、加拿大、墨西哥、巴西、俄罗斯、新加坡、印度尼西亚、比利时等17国数字经济规模介于1000亿至8000亿美元之间，另有24国的数字经济规模不足1000亿美元。

随着科技的发展和新冠疫情的持续蔓延，以数据为核心的数字技术逐步成为经济发展的新驱动力，为数字经济的进一步发展带来新动能。例如，在新出行方式、个性化医疗、远程办公等驱动下的创新使更多的人受益。与此同时，持续增加的数据资源及其存储和处理技术的变化，将逐步成为一种潜在增长、可持续累积的社会资源。

据著名咨询机构IDC预测，2025年全球数据量将高达175ZB。其中，中国数据量增速最为迅猛，预计2025年将增至48.6ZB，占全球数据圈的27.8%，平均每年的增长速度比全球快3%,中国将成为全球最大的数据圈（数据圈指被创建、采集或是复制的数据集合）。

数据作为数字经济时代最核心、最具价值的生产要素，正在加速成为全球经济增长的新动力、新引擎，深刻地改变人类社会的生产和生活方式。5G联接、人工智能、云计算、区块链、产业互联网、泛在感知等ICT新技术、新模式、新应用无一不是以海量数据为基础，同时又激发数据量呈爆发式增长态势。随着数据量呈指数级增长，数据分析算法和技术迭代更新，数据创新应用和产业优化升级，数据对社会变革的影响更加深远。

1.2 全球主要经济体数据战略

近年来，全球发达经济体包括美国、欧盟、英国等纷纷把数据竞争力上升为国家战略高度。2020年，尽管受疫情影响，全球整体经济增长放缓，但“减少接触，远程办公”等疫情期间采取的一系列措施却推动数字经济势头发展地更加迅猛。各经济体更加重视数据竞争力，纷纷制定出台数据战略，宣誓数据安全和主权。在保护数据安全的前提下，承认数据价值、促进数据利用，力争在数据政策及标准制订等方面建立领导力。

1.2.1 美国数据战略

2019年12月，美国发布《联邦数据战略和2020年行动计划》，以2020年为起始点，规划了美国政府未来十年的数据愿景，核心思想是将数据作为战略资源来开发，通过确立一致的数据基础设施和标准实践来逐步建立强大的数据治理能力，为美国国家经济和安全提供保障。

2020年10月，美国发布《国防部数据战略》，提出其将加快向“以数据为中心”过渡，制定了数据战略框架，提出数据是战略资产、数据要集体管理、数据伦理、数据采集、数据访问和可用性、人工智能训练数据、数据适当目的、合规设计等八大原则和数据应当可见的、可访问的、易于理解的、可链接的、可信赖的、可互操作的、安全的等七大目标。

美国政府通过发布一系列数据战略，来促进美国内部机构数据的访问、共享、互操作和安全，使数据发挥更大的价值，支持更多创新算法应用，最终支持美国国家战略和数字现代化战略的实施。

1.2.2 欧盟数据战略

当前，欧盟面临着矛盾：一方面对他国关键数字技术（例如获取、交换和分析数据）有较强的依赖，另一方面在平台寡头经济的影响下需要保持其自由的、具有社会凝聚力的经济和社会模式。同时，当前国际紧张局势、贸易冲突和数字鸿沟加剧了这一矛盾。

因此，欧盟认为必须建立欧洲数据主权。2020年2月，欧盟发布了《欧盟数字化战略》《数据战略》《人工智能战略》，旨在建立欧盟数据平台的基础上，实现数据主权和技术主权，从而达到数字经济时代国家竞争力提升和领先。2020年6月，德国和法国合作启动欧洲数据基础架构GAIA-X项目，该项目被视为一个开放的数字生态系统摇篮，是欧洲国家、企业和公众联合建设的下一代数据基础设施。在该项目中，用户能在充分信任的环境中安全地收集、处理和共享数据。为确保GAIA-X项目能够长期运行，欧盟计划建立GAIA-X基金会，推进和建设欧洲范围的数据基础设施，细化联合数据基础设施所使用的参考架构，明确数据基础设施的技术要求及其规则体系。

欧盟非常注重信息数据流通与个人权利保护。2018年5月，发布《通用数据保护条例》（GDPR），明确了个人数据定义及适用范围，确定了数据保护的合法性基础、数据主体权利、数据控制者义务、数据流通标准、数据救济和处罚等。依据GDPR有关规定，欧盟对个人数据出境进行了高水平保护，并认为GDPR应该成为世界的标杆，并在实施数据战略中，力推让世界向欧盟看齐。与此同时，GDPR实际也是全球众多国家、地区制定数据保护条例的重要参考。

欧盟对数据中心减少能耗和碳排放也非常重视。要求数据中心遵循行为规范，必须实施节能最佳实践方案，满足采购标准，并且每年报告能耗。同时，要求数据中心设备提供商开发和提供高能效的服务器和低能耗的CPU，保证在降低能耗的情况下，具有相同的处理能力。

1.2.3 英国数据战略

一直以来，英国是欧盟数字标准规范最为积极的制定者和参与者。在脱欧之前，英国政府于2020年9月发布了《国家数据战略》，着眼于利用现有优势，促进政府、企业、社会团体和个人更好地利用数据，推动数字行业和经济的增长，改善社会和公共服务，并努力使英国成为下一代数据驱动创新浪潮的领导者。该《战略》还阐述了数据有效利用的核心支柱，确保数据可用性、安全可靠性。并确定了政府的优先行动领域，如释放经济的数据价值、确保有利于增长和可信赖的数据制度、改变政府对数据使用以提高效率和改善公共服务、确保数据基础设施的安全性和弹性、倡导国际间数据流动等。

1.2.4 中国数据战略

2017年12月，中国提出“要构建以数据为关键要素的数字经济。要切实保障国家数据安全，要加强关键信息基础设施安全保护，强化国家关键数据资源保护能力，增强数据安全预警和溯源能力”。2019年7月，在G20大阪峰会的数字经济特别会议上，中国提出“共同完善数据治理规则，确保数据的安全有序利用；要促进数字经济和实体经济融合发展，加强数字基础设施建设，促进互联互通；要提升数字经济包容性，弥合数字鸿沟”，“数据安全”已上升到了我国国家安全战略高度。

近年来，我国陆续发布了一系列数据及其安全相关的法律法规和标准规范，数据资产价值得到确认。政府部门、企业持续加大在数据治理、数据存储、数据保护、数据加密等方面的重视程度和投资力度。

2018年5月，全国信息安全标准化技术委员会发布《信息安全技术 个人信息安全规范》标准。针对个人信息安全问题，规范了个人信息控制者在收集、保存、使用、共享、转让、公开披露等信息处理环节中的行为，禁止了个人信息非法收集、滥用、泄漏等，保障了个人合法权益和社会公共利益。

2020年4月，发布《中共中央国务院关于构建更加完善的要素市场化配置体制机制的意见》，中央首次明确数据成为继土地、劳动力、资本、和技术之外的第五大生产要素。

2020年6月，12部委联合发布《网络安全审查办法》，推动建立国家网络安全审查工作机制。《办法》明确了关键信息基础设施运营者采购网络产品和服务，影响或可能影响国家安全的，应按照《办法》有关要求，进行网络安全审查，确保关键信息基础设施供应链安全，维护国家安全。

2020年8月，《数据安全法（草案）》公开发布，从法律层面清晰定义了数据活动、数据安全，提出国家将对数据实行分级分类保护、开展数据活动必须履行数据安全保护义务承担社会责任等，明确了在我国境内依法开展数据活动。2021年4月，《草案》进入十三届全国人大常委会二次审议。《数据安全法》正式发布指日可待，其将是数据要素国家战略的基本法，强调了数据安全是数字中国重要战略举措的根本保障，体现了国家对保障数字经济安全的决心与信心。

《国家安全法》《网络安全法》以及即将出台的《数据安全法》《个人信息保护法》与其他规范形成配套组合，将成为国家整体数据安全观的重要组成部分，为保护国家关键数据资源安全和个人信息数据安全提供了法律依据。

1.3 数据安全在数据产业生态中的战略意义

数据具有爆发式增长、海量集聚、取之不竭等特征，是数字经济的关键要素。数据已成为各经济体实现创新发展、重塑人们生活、乃至国家经济社会发展的重要支撑动力。数据安全包括数据存储、处理安全、所涉及技术和基础设施的安全以及数据权属带来的安全。在全球合作日益密切的背景下，数据安全对于提升用户信心、保护数据、促进数字经济发展至关重要。随着数据不断量变和质变，我们面临前所未有的数据安全问题；当数据量变和质变达到一定水平，其数据价值会随之增大，数据安全将在护航数字产业发展生态发挥关键作用。

02 数据产业新生态的安全需求与挑战

2.1 数据产业新生态及发展趋势

在新一轮科技革命和产业变革浪潮中，基于数据发展的数字经济已成为不可逆转的时代潮流。可以预见，未来几年全球数字经济仍将以高速增长态势驱动社会经济增长。数据产业创新演进升级，传统行业数字化转型大有可为，发达国家将通过强化技术创新巩固数据产业先发优势，发展中国家则将通过深化行业数字化努力实现赶超，数字经济领域的竞争将愈发激烈。

产业数字化已成为全球数字经济发展的主脉络。我国数字产业发展的关键是促进数字化技术在各个行业各个产业渗透和应用，催生新产业、新模式、新业态，释放数据产业经济活力。产业数字化不仅对数据的安全感知、安全存储、安全传输、安全处理等提出更大挑战，还对数据治理、服务平台、应用平台等带来新的安全需求。为构建完善的数据产业生态，建设新型数据基础设施势必需要：提高数据获取效率，打通数据流动通道，提供快速的数据分析能力，为行业用户提供一站式的服务，盘活数据资产，帮助各行业用户深度挖掘数据价值，实现转型和创新融合发展。

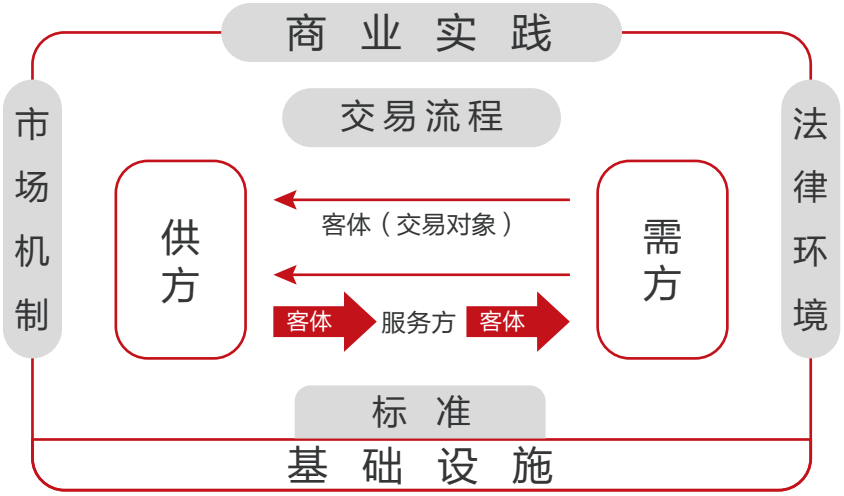
我国正处于从工业经济迈向数字经济的攻坚阶段，实体经济数字化、智能化转型需求越发迫切。数据技术日新月异，数据产业融合发展，相关政策持续完善，数据与实体经济融合发展正迈入前所未有的重大机遇期。在中国政府的高度重视和大力推动下，各部委相继出台大数据相关文件并加快落地实施，融合发展机制实施、资金支持、人才培养等政策保障持续强化，数据与实体经济融合发展的进程正在提速。

中国政府通过了《中共中央关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标的建议》，对“十四五”时期我国经济社会发展作出了贯彻新发展理念、构建新发展格局的重要部署，并作出了我国进入新发展阶段的重要判断。新发展理念的核心是创新，创新是发展的第一动力。随着数字经济蓬勃发展，数据保存量逐年倍增，建设创新、安全、绿色的数据基础设施将是支撑数据产业长期可持续发展的重要要素。

2.2 数据产业新商业模式对数据安全的需求

数据是二十一世纪的石油。近几年来，数据交易商业实践无论在广度上还是在深度上均有所突破，数据要素市场改革进一步加速了这个趋势的发展。数据产业发展服务于数字经济，需要建立在数据流通繁荣之上，围绕数据产业商业模式的创新至关重要。

>>> 图2-1 数据产业商业模式（源自:数据交易的商业模式《概要版》，2019）<<<



据《数据交易的商业模式》研究报告[1]，数据交易商业模式的框架主要由3+4+1要素构成。其中，3表示“数据交易的环境”“数据交易的基础设施”“法律环境和市场机制”，4表示“主体”“客体”“流程”和“标准”，1表示“数据交易的商业实践”。

经过多年探索和实践，当前市场存在直接交易模式、授权转移模式、数据市场模式、一般数据平台模式、具备授权和问责制数据平台模式、数据银行模式和数据信托模式7种数据交易商业模式。未来，可能还会产生更多的商业模式。但是无论何种商业模式创新，都需要建立在安全、高效的数据采集、存储、流通和交易基础之上。多样化的数据交易模式对数据安全提出了迫切需求，需要通过安全的信息基础设施、创新的技术手段、完善的法律法规来满足数据安全、隐私保护等高可用需求。

2.3 产业升级和技术发展对数据安全提出了新挑战

如前述，产业数字化已成为全球数字经济发展的主脉络。我国数字经济正处于快速发展阶段，尤其在抗击疫情的过程中，各行各业加快了数字化转型的步伐。据《中国数字经济发展白皮书（2020）》[2] 报告数据显示，2019年我国数字经济增加值规模占GDP比重提升到36.2%，数字经济在国民经济中的地位进一步凸显。

推动新型基础设施建设（以下简称新基建）是我国数字经济快速发展重要举措。从建设范畴看，新基建覆盖信息基础设施、融合基础设施和创新基础设施三类，分别对应产业、行业及科技。新基建的本质是建设信息数字化的基础设施，关键在于数据基础设施建设和传统基础设施的数字化转型，并以数据为中心，深度整合计算、存储、网络和软件资源，充分挖掘数据价值，加快数据共享和融合，使数据“存得下、流得动、用的好”。

1.数据交易的商业模式《概要版》，2019
2.中国信息通信研究院.中国数字经济发展白皮书（2020）[R].2020

随着新基建的持续推进，各行业对数据感知、存储、传输、处理等能力提出了更高要求。同时，数据特点也在不断演进，主要如下：

首先，海量、多元和非结构化成为数据新发展常态。数据环境呈现多样化、复杂化特征，大量文本、图片、视频等非结构化数据被产生、存储和使用。例如，在智慧城市场景中，各类传感设备采集的数据从单一内部小数据形态向多元动态大数据形态发展，产生的海量数据给数据安全存储、管理及使用带来压力。

其次，数据实时性处理变得更为迫切。随着新一代信息技术的快速发展，社会运行效率不断被优化和提升，企业新生业务对数据实时性要求日益增加。例如，在金融反欺诈风险评估、无人驾驶、工业检测、流程化制造等许多场景中，需要快速实时的数据安全采集、安全存储和安全分析处理。

第三，新型数字技术催生海量数据呈现多元化处理特征。在云计算、物联网、大数据、人工智能、区块链、边缘计算、5G等一系列新型数字技术对社会各个行业的渗透和场景中，产生海量数据，提出了多元化处理需求，这对数据中心应用更安全、高效支撑新型数字技术提出了挑战。例如，在无人驾驶场景下，原始图像数据处理就需要经过云计算、大数据、边缘计算、人工智能、5G等一系列新型数字技术的综合使用。

2.3.1 人工智能领域

据《人工智能数据安全白皮书（2019）》[3]，人工智能因其技术局限性和应用广泛性，给网络安全、数据安全、算法安全和信息安全带来风险，其中，数据安全是人工智能安全的关键。

人工智能快速发展的核心在于算法和数据，数据规模和质量对人工智能决策结果有着决定性的影响。同时，随着人工智能化水平的提升，在数据管理和数据挖掘方面将更容易引入数据安全风险。综合来看，人工智能领域涉及关键数据安全挑战主要有：

数据泄露风险

人工穿戴设备、视频采集设备等与人们日常生活息息相关，通过这些设备可以直接采集敏感个人信息（如人脸、指纹等），保护不当可能造成个人隐私泄露。

数据滥用风险

利用人工智能技术预测用户喜好和习惯，极大程度地提升了人们日常生活便利，改善了生活方式。但大数据“杀熟”、隐私跟踪等也频频发生，引发政府及公众对数据滥用的关注和担心。

3.中国信息通信研究院.人工智能数据安全白皮书（2019）[R].2019

数据治理挑战

随着互联网企业的业务国际化，全球搜索、位置定位、即时通信等软件在全球范围推广和应用，加剧了数据违规跨境流动风险。

2.3.2 超算领域

超算广泛应用于科学研究、气候气象、海洋科学、生物医药、油气勘探、工业创新、商业金融、社会公共服务等领域。由于涉及海量数据的存取和计算，同样面临各种数据安全挑战：

数据泄露风险

对于国家重大科技类任务，数据常常需要高度机密保护，不能随意访问，更不能对外泄露暴露。同时，要考虑数据销毁技术，避免恶意恢复数据。因此，需要更加全面的安全防护体系，其中，数据全生命周期加密、芯片级加密、可信执行环境等尤为重要。

数据高性能存储风险

各领域都迎来了数据量的爆发式增长。例如，一台L3级别的自动驾驶测试车，每天产生60TB的数据，多辆车产生的PB级热数据要求在24小时内完成数据处理，上百PB原始数据则需要存储30年以上，用于后续机器学习。同样的，基因测序和宇宙探索等场景下每天产生的热数据也需要提供每天级甚至小时级的快速处理能力，宝贵的原始数据则需要长期保存。

数据流通效率低

超算流程不同阶段可能用到文件、大数据、对象等不同的存储服务。而传统存储设备通常只支持一种存储类型，数据需要在不同存储设备间多次拷贝，会导致数据流通效率偏低。

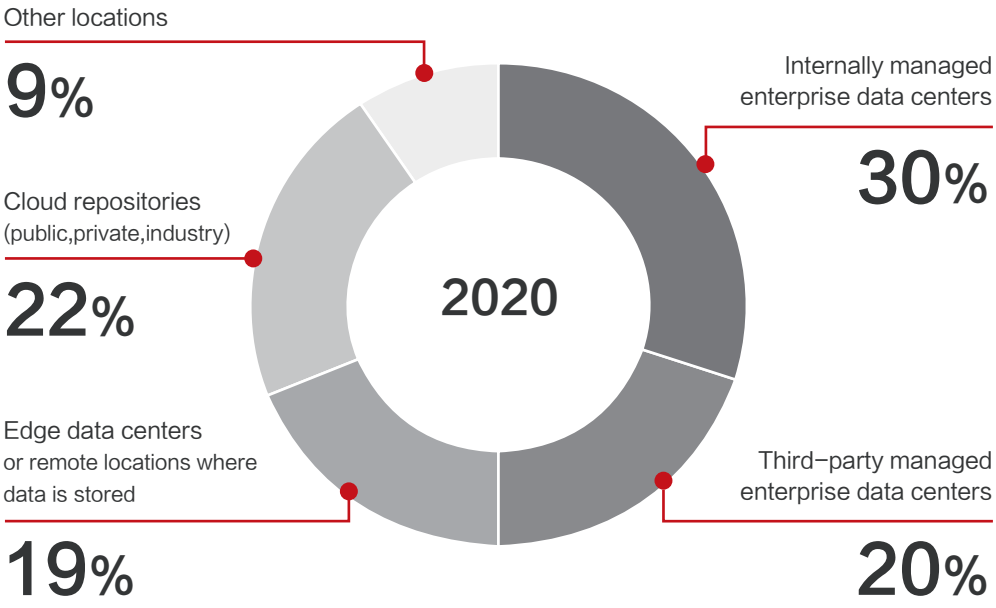
计算性能和自主创新风险

传统的计算型超算存在故障点多，索引无冗余，可靠性差等问题。同时，因其基于开源软件实现，存在不可信的安全风险。

2.3.3 数据中心

根据IDC的调研报告，目前企业50%的数据保存在自己的数据中心或者租用的第三方数据中心，另有22%保存在云服务商数据中心，19%保存在边缘数据中心[4]。随着我国数据中心使用增加，数据中心能耗大、效率低的问题日益突出，同时，由于数据交换更加频繁，核心业务数据、个人隐私数据保护等也面临更多安全风险：

图 2-2 存储在不同类别数据中心的分布



Source:The Seagate Rethink Data Survey,IDC,2020

业务中断、数据丢失风险

数据中心具有设备种类多、集中、自动化程度高的特点，且长时间不间断运行，容易出现因系统故障导致的业务中断风险，需要考虑数据的容灾保护（如两地三中心），保障业务连续性。同时，因恶意破坏或非恶意操作导致的数据丢失，需要考虑数据的本地或异地备份，保障数据完整可用。

数据破坏、泄露风险

数据中心为企业提供了大量的应用、服务和解决方案，已成为企业关键资源。数据中心一旦被恶意攻击成功，大量数据被破坏、窃取、泄露，将会对企业、个人及社会经济造成极大影响。

高能耗风险

2018年中国数据中心总用电量为1609亿kWh，占中国全社会用电量2.4%。预计2024年中国数据中心总用电量将达3000亿kWh，年均增长率10.6%[5]。能源是国家战略资源，是数据中心安全持续运行的保障。2019年我国企业数据存量约148EB，每年新增约35EB[6]，预估数据存储耗能为194亿kWh，约占我国数据中心总能耗的12%。随着数据分析需求不断增加、物联网设备逐渐普及以及云迁移活动的驱动，2020至2022年企业创建的数据量将每年增加42.2%[7]，数据存储所产生的能耗还将大幅增长。数据的计算和存储都将耗费电能，随着数据量加速井喷，如何有效借助技术创新降低数据中心每TB数据的计算、存储耗能将会是数据中心节能增效必须关切的问题。

4.The Seagate Rethink Data Survey, IDC, 2020
5.《点亮绿色云端：中国数据中心能耗与可再生能源使用潜力研究》华北电力大学，绿色和平组织，2019
6.IDC中国企业存储报告，存量以2014年~2019年容量之和计算
7.IDC，Rethink_Data_Report_2020

2.3.4 金融领域

金融是现代经济的核心，是国家重要的核心竞争力。对于金融业务，业务实时性要求很高，业务呈现高度数字化、信息化。数据安全关乎金融企业“生死存亡”。

《2018-2019 年度金融科技安全分析报告》[8] 表明，所有被调研企业均表示发生过不同类型的网络安全事件。其中，针对客户资料及企业重要业务数据的安全事件成为发生频率最高的安全事件类别，占比44%（其中，“客户资料”泄露和 “企业敏感信息泄露”各占一半）。关键数据安全成为持续影响金融科技企业最主要的网络安全风险，主要挑战有：

数据丢失风险

金融系统需要可靠的存储、完备的灾备系统。无论自然灾害、系统错误或是人为损坏，金融核心数据要实时可恢复，以避免造成严重金融损失。

数据泄露风险

随着金融业务的不断发展，线上服务更加丰富便捷。如何保障数据的安全使用，保护用户个人隐私信息，也成为金融领域的安全挑战之一。

数据完整性风险

交易记录等数据通常需要提供有效性追溯和防抵赖证明，这种高安全要求也是金融行业在数据安全方面区别其他行业的一个明显特征。

2.3.5 工业互联网领域

工业互联网日益成为提升制造业生产力、竞争力、创新力的关键要素。发达国家纷纷以工业互联网作为发展先进制造业的战略重点。与此同时，工业互联网面临的数据安全风险隐患日益突出。工业和信息化部发布《关于工业大数据发展的指导意见》，根据工业和信息化部的《意见》解读，工业数据已成为黑客攻击的重点目标，我国34%的联网工业设备存在高危漏洞，这些设备的厂商、型号、参数等信息长期遭恶意嗅探，仅在2019年上半年嗅探事件就高达5151万起。

目前工业数据安全责任体系建设正在推进，云计算、大数据、人工智能、5G等新技术新应用，进一步加剧了工业数据安全隐患。工业互联网数据安全防护面临以下两点关键挑战：

数据泄露风险

随着越来越多的工业控制系统与互联网、大数据平台连接，相对传统封闭的工业生产环境被开放，网络攻击面扩大，外部威胁更容易攻击到工业环境中，可造成重要工业数据泄露、勒索等严重后果。

数据全生命周期管理风险

因行业及企业间差异，数据接口规范、通信协议不统一，数据采集过程容易导致过度采集、隐私泄露等问题。工业数据传输、处理实时性要求高，工业互联网数据多路径、跨组织、跨地域的复杂流动，容易导致数据传输过程追踪溯源问题。

2.3.6 医疗领域

随着大数据、人工智能等新技术在医疗领域的渗透和应用，现代医学技术发展迅速，新兴重点领域如医学影像、辅助诊断、健康管理、疾病预测等对数据的依赖程度持续增加。从数据的角度出发，关键数据安全挑战有：

8.普华永道，中国信息通信研究院，平安金融安全研究院，2018-2019年度金融科技安全分析报告[R].2019.

数据泄露风险

医疗数据具有极强的隐私性，一旦泄露会对患者生活、工作带来负面影响。同时，大量医疗数据开始提供第三方开发测试使用，也容易造成个人隐私数据泄露。

涉及国家人类遗传资源、基因编辑等高价值生物数据的新兴的生物技术产业，一旦发生数据泄漏，后果也非常严重。

数据不可用风险

勒索软件攻击对医疗行业数据安全带来严重威胁。关键医疗数据、文件被勒索加密，如果不能及时恢复数据，将严重威胁患者的生命健康数据管理以及进一步的治疗。根据 Verizon 2019 年的数据泄露调查报告，针对医疗领域的勒索软件攻击连续两年占到其所有恶意软件事件的 70% 以上。

通过以上分析，数据安全对各行业/领域的生产与运营举足轻重，承载企业核心数据的关键信息基础设施都面临着共性的安全挑战。如何构建全方位的数据安全体系，保障数据的安全与合规有序流动，在数据全生命周期过程中确保数据不丢失、不泄露、不被篡改、业务永远在线、可追溯和隐私合规等，已成为数字经济时代对数据安全的核心要求。

2.4 数据安全对核心技术能力的诉求

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。从产业生态面临数据安全挑战看，各领域在数据全生命周期的不同阶段面临不同程度安全风险。因此，对数据安全提出如下（不限于）核心技术能力要求，通过构建和融合这些能力，可以系统化、端到端地全生命周期的保护数据安全。

>>> 表 2-1 数据安全核心技术能力诉求 <<<

数据生命周期	核心技术能力诉求
数据采集	数据分类和分级、身份认证、权限控制等
数据传输	身份认证、传输通道加密、敏感数据加密、密钥管理等
数据存储	软硬件数据加密、数据隔离存储、完整性保护/WORM、数据度量、数据容灾备份等
数据处理	访问控制、用户间隔离、防侧信道攻击、REE/TEE/SEE硬件隔离机制、日志审计等
数据交换	数据脱敏/水印等
数据销毁	安全擦除/消磁等
数据管理	数据可视化管理，数据安全策略管理等

03 数据安全的总体策略及治理思路

数据安全已经上升到国家主权的高度，是国家竞争力的直接体现，是数字经济健康发展的基础。数据安全不是单方面强调数据的绝对安全，关键在于维护数据安全性和促进数据开发利用并重，以数据开发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展。同时，我国高度重视数据安全的技术开发和管理管控，不断增强国际社会对中国信息技术的信任程度。数据安全核心价值可以简单概括为“以安全促可信，以可信促发展”。

3.1 数据安全的总体策略

3.1.1 合法合规

各国加强数据安全立法，保护涉及本国国家安全、公共安全、经济安全和社会稳定的重要数据及个人信息安全。为了维护开放、公正、非歧视性的营商环境，推动实现互利共赢、共同发展，无论企业还是个人，都应该严格遵守所在国法律法规，尊重他国主权、司法管辖权和对数据的安全管理权，并在此基础上，发展数据安全保护技术。

3.1.2 安全与发展并重

数据流通与交易有利于促进数据的融合挖掘，从而释放数据资源的价值。据估计，2014年，国际数据流动给全球经济增加了2.8万亿美元，预计到2025年将增至11万亿美元（麦肯锡全球研究所，2016年）[9]。然而，数据使用又必须明确数据保护的责任与义务,尤其是对个人隐私数据的保护。因此，需要辩证看待隐私保护、数据安全与数据共享利用效率之间的矛盾，以“数据安全与发展同步”为核心目标对数据进行开发和利用。

这势必要求从技术上打通数据孤岛，构筑开放、公正、安全、合作的数据价值流转环境，解决数据开放共享链条上多方的安全顾虑，促进数字经济健康发展，为社会的进步作出贡献。

3.1.3 以数据为中心构建安全体系架构

当前数据产业面临的威胁和风险不仅针对数据本身，也包括承载数据的关键信息基础设施，因此，我们需要以数据为中心，构建全方位的数据安全治理体系，保护数据资源，在风险可控的基础上实现数据的增值和自由流转。

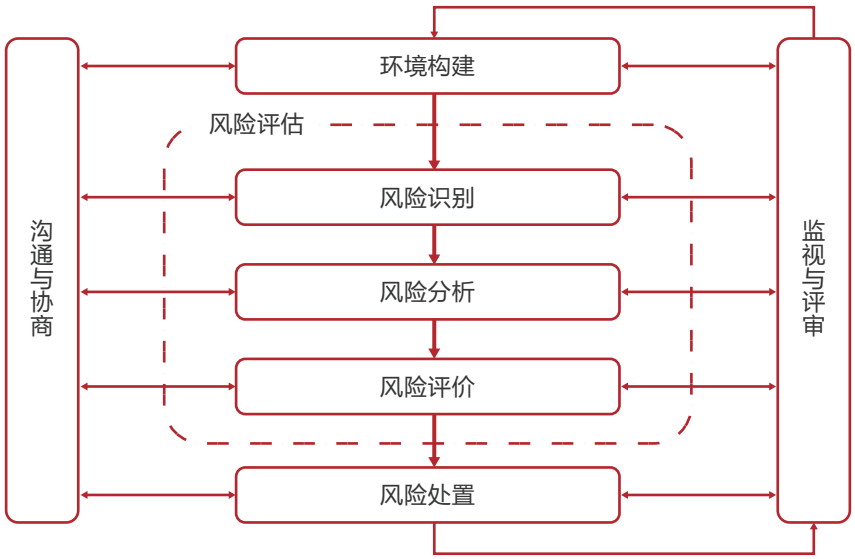
9.Measuring the economic value of data and cross-border data flows，OECD，26 Aug 2020.

3.2 数据安全治理核心思想

数据安全治理的理念正在被业界接纳，并且成为一种应对新产业生态数据安全挑战的重要指导思想。从本质上来说，数据安全治理理念与ISO 27001的基于风险的安全管理思路一致[10]，即数据安全方案和其他所有关键资产的安全方案设计一样，从资产面临的安全风险着手，对资产进行分类分级，实现精细化管理，以合理利用有限的投资实现资产风险可控。

数据安全治理能力建设并非单一产品或平台的构建，而是建设一个覆盖数据全部生命周期和使用场景的数据安全体系，需要从决策到技术，从制度到工具，从组织架构到安全技术通盘考虑。因此，在设计和部署具体安全方案之前，必须有详细的规划。在对国家法律法规、行业规范、企业现况进行详细分析的基础上，结合业务目标来构建数据安全治理的架构。在很多情况下，数据安全治理能力构建需要有一个长远目标和计划，需要分多骤、分阶段的逐步完成。

图 3-1 ISO 27001 风险治理流程



数据安全治理的第一步就是根据法律法规、商业战略、数据安全治理需求对数据进行分类。在分类之后，企业需要结合自身的实际情况对数据风险进行分级。

针对数据分级的评估维度，很多国际和国内的标准给出了参考意见。比如，美国国家标准与技术研究院（NIST）的《FIPS PUB 199》和《NIST SP800-122》建议使用可识别性、个人数据数量、字段敏感度、使用上下文、保密义务、访问要求存储位置六个关键因素来确定个人数据的价值并进行数据分级。

在数据分类和分级过程中，需要平衡精细化管理与落地实施。适合企业自身需求的数据分类分级方案应考虑以下因素：

- 数据分类分级应满足业务涉及有关国家法律法规及行业主管部门规定；
- 分类分级规则应避免过于复杂，以保证其在数据分级过程中的可行性；按照业界标准和实践，一般定级在3-5级为宜。

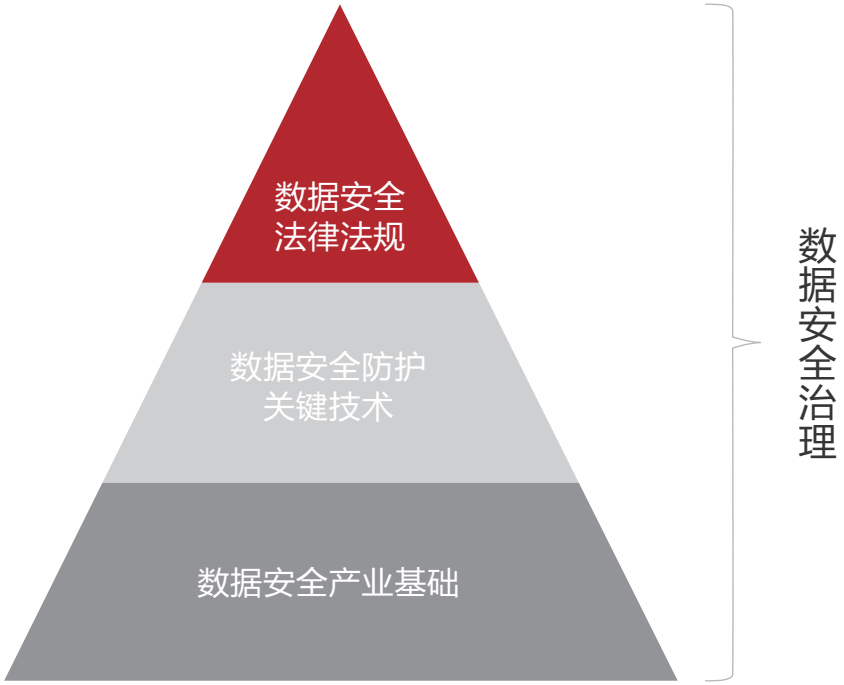
进行数据分级之后，就可以根据数据的类别和级别来制定配套安全策略以及安全技术方案，来保护数据全生命周期安全。

10.ISO 27001:2013 Information Security Management System, https://www.i2iso.com/portfolio/iso-27001-2013/.

3.3 数据安全治理的三个层面

基于数据安全治理核心思想，结合我国数据产业的实际情况，应对数据安全挑战，需要从数据安全的产业基础、数据安全防护的关键技术以及数据安全的法律法规建设三个方面来实现。

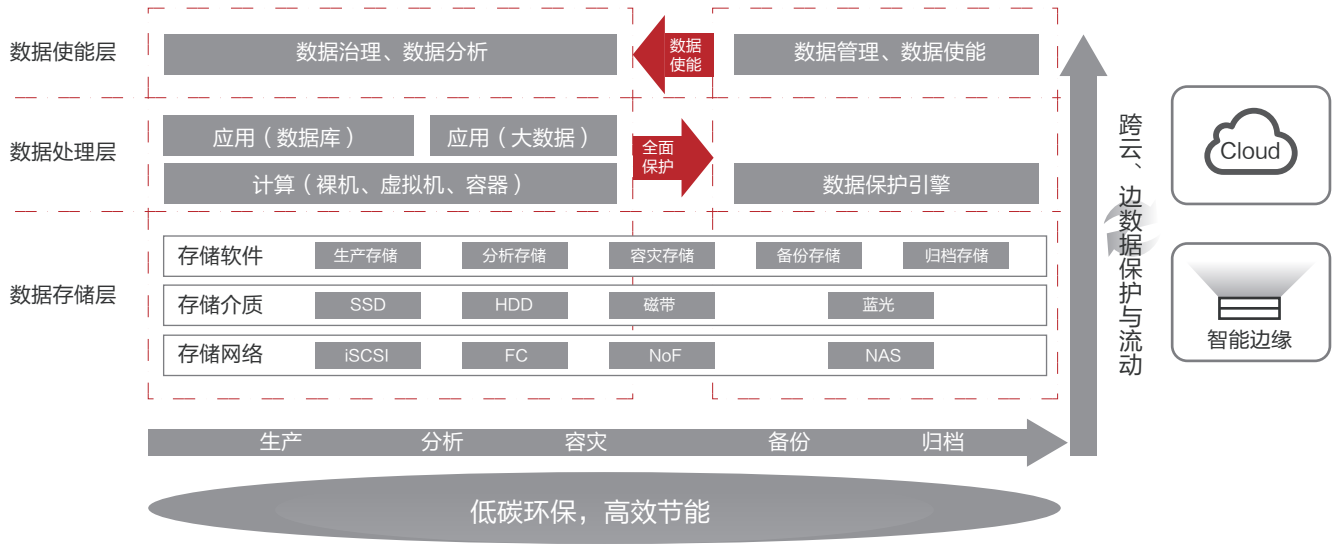
图 3-2 数据安全治理的三个层面



04 数据安全的产业基础

数据产业涉及到数据整个生命周期以及价值变现的全部过程的所有相关产业。具体包括数据采集、数据存储、数据传输、数据管理、数据分析、数据挖掘、数据价值评估和交易等。数据安全的存在意义是保证数据在全生命周期得到妥善保护，最终实现价值变现并促进数字经济健康发展。因此，没有安全健康的数据产业做支撑，数据和数字经济就是空中楼阁，数据安全就失去了依托。

>>> 图 4-1 数据安全的产业基础架构示意图 <<<



数据产业涉及到数据存储层、数据处理层和数据使能层。数据存储层是数据产业的核心层，主要包括存储网络、存储介质和存储服务，由相关存储设备的硬件和软件组成，是数据业务和配套安全方案的根基。经调研发现，我国在数据存储的介质自主化、存储网络技术自主化、抵御灾害突发事件、绿色环保的可持续发展等方面还有较大的提升空间。数据产业界同仁应当遵循安全和发展同步推进的原则，以确保数据安全为前提，大力发展数据产业，为建设数字经济强国和全面建成小康社会提供保障。

在数据安全存储的基础上，企业需要选择相应的数据库、大数据软件、分析工具以及相关的技术架构，对数据进行采集、存储、检索、加工、变换和传输。这个过程在数据处理层完成，从大量杂乱无章的、难以理解的数据中抽取并推导出有价值、有意义的数据，挖掘和开发出数据的价值。数据处理场景涉及到数据协同共享处理场景、数据跨网或跨境场景等，这类场景处理更多在于数据授权、审计跟踪、数据脱敏等。目前，我国已基本具备数据库和大数据产业基础，但距离国际领先水平还有较大差距。

数据使能层是指对数据治理、分析和管理过程。对于企业来说，数据流动起来才能给企业组织带来效益和价值。数据使能场景从数据使用和流动的角度进行提炼，包括内部数据使用、内外交互场景、业务系统安全防护、移动应用等场景。数据使能需要根据界定的数据安全治理业务对象，识别数据资产，发现和定位具体数据管理对象，可以是静态存储的数据库系统、文档存储系统，也可以是动态数据处理系统，包括数据接口API、传输数据的网络系统等。

总体来说，数据存储层以硬件能力为主，更需要通过技术创新构筑产业硬实力，这也是我国数据安全亟待提升的产业基础能力。数据处理层和数据使能层以软能力为主，需要大力发展和培育软件产业生态，共同应对产业挑战，数据安全的主要目标是保护个人隐私安全，防止数据泄露，确保数据安全流动共享。

4.1 数据存储介质

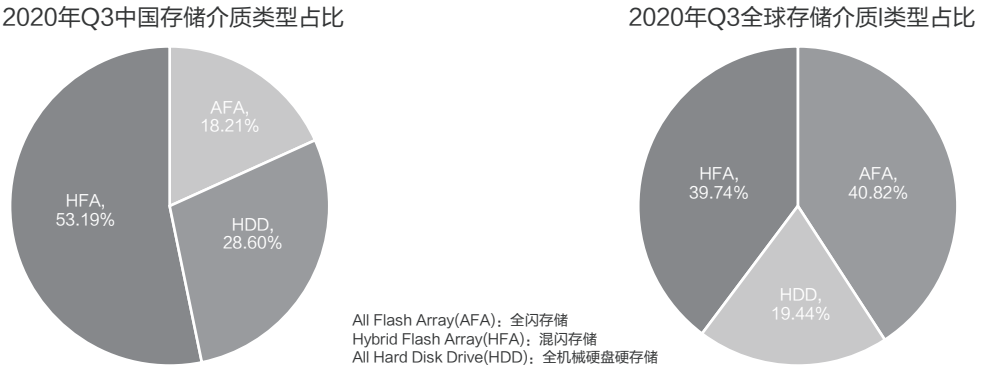
存储介质有磁、光、半导体等，在数据基础设施中以机械硬盘（HDD）和固态硬盘（SSD）为主。对于HDD，我国并无相关产业，也没有掌握核心技术。但是在SSD领域我国已经掌握了关键技术，如在SSD的控制器芯片方面，国内已有厂商推出了量产的产品。在SSD的NAND Flash颗粒方面，国内厂商的制造工艺和生产能力也逐渐成熟。在基于NVMe协议的SSD技术方面，国内厂商的产品也已经在政府、金融等行业开始使用，由此可见我国的SSD产业正处在快速发展的阶段，并且日趋成熟。

表4-1 存储介质供应风险

存储介质	掌握情况	风险情况	说明
半导体介质（SSD）	国内掌握NVMe接口SSD控制器和颗粒（NAND）的设计和制造技术	小	NVMe SSD介质可持续供应
磁盘介质（HDD）	国内无相关产业	大	可用半导体介质和光盘代替

从IDC　2020年的统计数据可以看出，全球使用全SSD的存储比例达到了40.8%，全HDD盘的占比不足20%，我国使用全SSD的存储比例为18.2%，全HDD盘的占比接近30%。在全球，SSD已逐渐成为数据基础设施中的主流存储介质，但是在我国，SSD的普及率还比较低。[11]

图 4-2 IDC存储介质类型占比



数据来源：2020Q3 IDC中国企业存储系统追踪报告

从Gartner的全球数据来看，企业关键系统存储SSD到2024年占比将达到100%，且成本持续降低，而企业级HDD在2023年将接近生命周期的EOL[12]。西数、希捷等厂商也放弃了对高性能HDD盘的研发投入，从而转向了SSD盘。

表 4-2 2020年Gartner企业SSD和HDD市场分析

	2017A	2018A	2019A	2020E	2021E	2022E	2023E	2024E
Mission-Critical Enterprise HDD Cost/GB	$0.130	$0.104	$0.089	$0.081	$0.073	$0.068	$0.063	EOL*
Storage-Class Enterprise-Grade SSD	$0.580	$0.358	$0.185	$0.182	$0.154	$0.146	$0.129	$0.104
Mission-Critical，performance-optimized HDDs spin at 10,000 rpm or 15,000 rpm,have SAS interfaces,and can be used in either servers to provide direct-attached storage or in external controller-based storage systems\Mission-critical HDDs will reach end-of-life(EOL)status during 2023.								

数据来源：Gartner（December2020）

11.2020年IDC中国企业存储系统追踪报告
12.2020年12月Gartner企业SSD和HDD市场分析

可以看出，全闪存已成为产业共识，加速“磁退硅进”已成为业界趋势，业界各主要厂商正在大力发展新一代闪存核心技术，并大力推动新型SSD在核心业务中的使用，越来越多的新基建也已经开始大规模采用全闪存产品。

4.2 存储网络

业务平台访问数据需要基于高速可靠的存储网络。过去传统的小型计算机系统接口协议（SCSI）一直是数据传输的主流协议，承载SCSI协议的技术主要有Fibre Channel（FC）和iSCSI（IP）两种方式。其中，FC传输协议主要涉及到FC接口卡（HBA）以及FC交换机两种产品，FC交换机的核心技术主要由国外厂商掌握，其全球市场占有率已经达到100%，我国无相关FC交换机产业，处于全面落后地位。相反，IP传输协议主要涉及到IP交换机和网卡产品，而这两种产品国内厂商都已经达到国际顶级水平。

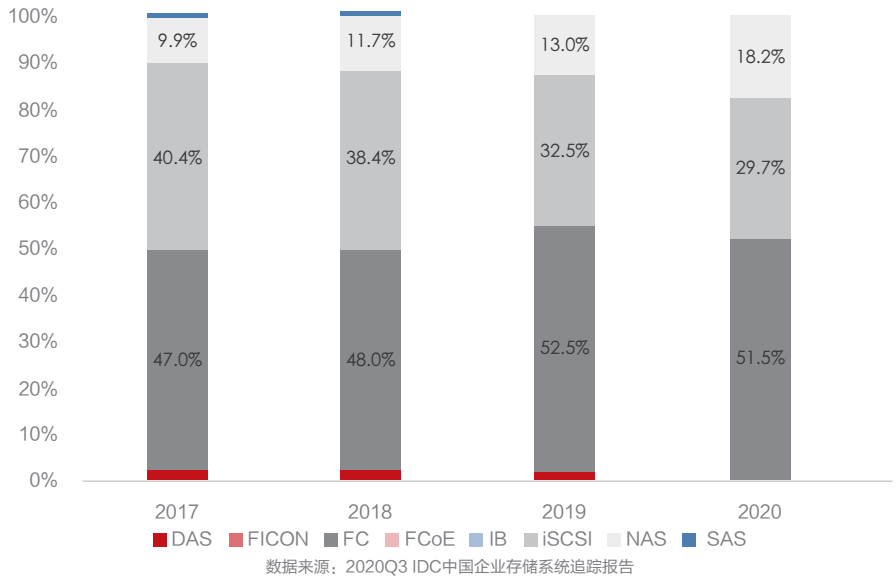
随着远程直接数据存取（RDAM）和非易失性存储器接口协议（NVMe）SSD的技术不断成熟，存储传输技术正在朝着NVMe over Fabric（NoF）等方向发展，并且NoF在传输性能和稳定性上已经超越了FC，业界一致认为NoF网络将取代传统的FC专用存储网络。我国在以太网和NVMe领域技术积累较多，供应链完整且具备一定市场竞争力，应尽快在存储网络接口和标准方面确定高速以太网和NoF的主导地位，避免在FC-SAN和SCSI接口产业链上的潜在风险。

>>> 表 4-3 存储网络供应风险 <<<

关键部件	掌握情况	风险情况	说明
Ethernet（IP）	国内产业成熟	小	已经掌握IP网络核心技术
Fiber Channel（FC）	国内无相关产业	大	可用存储IP网络替代

根据IDC分析报告[13]，在2020年有51.5%的存储网络使用了FC传输方式，有29.7%使用了iSCSI（基于IP），有18.2%使用了NAS（基于IP），FC和IP各自占据了一半的市场份额。但是，作为替代FC网络的NoF传输技术还未被IDC统计到相关数据，可见新型的NoF传输技术还处于大规模商用的初期阶段。

>>> 图 4-3 2017-2020年存储协议使用分析 <<<



数据来源：2020Q3 IDC中国企业存储系统追踪报告

13.IDC中国企业存储系统追踪报告 2020

当前是我国数据存储网络弯道超车的大好时机，应该大力推广新一代NoF高速存储网络，以适配NVMe SSD全闪技术。在接口和标准方面确定存储网络全IP化的主导地位，加速完成国内存储网络的技术升级。

4.3 数据存储软件系统

软件是数据基础设施中的重要组成部分。数据存储软件要满足系统“进不去”“看不了”“拿不走”“混不了”“赖不掉”“靠得住”等安全要求。

“进不去”：用户认证功能，确保非法用户无法访问数据。

“看不了”：数据脱敏和访问控制实现对系统和敏感数据的保护，确保不会被非法用户看到。

“拿不走”：数据加密和安全访问接入实现对关键数据的保护，确保非法窃取后，关键数据依然无法访问。

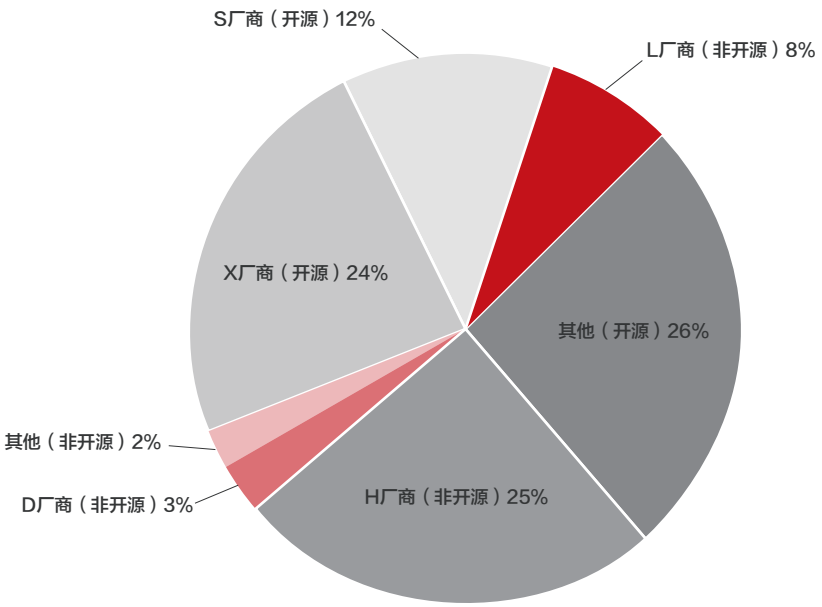
“混不了”：多租户隔离实现各用户使用数据时环境隔离，确保各类数据独立使用，不被非法混用。

“赖不掉”：系统审计、数据水印等功能实现对于用户操作的全程记录，确保行为的抗抵赖性。

“靠得住”：数据产品从设计、开发、认证等多个维度确保整个研发过程安全可信。

由于我国基础软件研发起步晚、技术积累不足，众多厂家不得不在其软件开发中广泛使用开源技术，比较有名的开源软件有RedHat、Lustre、Ceph等，这些开源软件提供了数据的处理、存储、管理等各方面的能力。在高性能计算（HPC）领域，开源软件Lustre被大量使用，而在分布式存储领域，Ceph也被很多厂商采用。从2019年IDC中国区分布式存储的市场分析[14] 可以看出，基于开源软件研发的存储占据了62%的市场份额，远大于基于自主软件研发的存储市场份额。

图 4-4 IDC 2019年中国区开源数据软件占比



数据来源：ICD 2019 中国区分布式存储市场报告

14.IDC 2019中国区分布式存储市场报告

开源软件带来了商业便利，但其可靠性低、存在安全隐患。由于大多数开源软件缺乏系统性的可信设计和验证，导致软件中存在大量安全漏洞，同时开源软件缺乏明确的安全责任主体，因此，使用开源软件存在安全风险的可能性比较大。Snyk2019年开源安全现状调查报告显示开源漏洞数量还在持续增长，81% 用户认为开发者负责开源软件的安全性，然而，只有 30% 的开源软件维护者认为自己具有高安全性意识。

构建我国自主的软件产业生态圈极为必要，鼓励国内数据软件厂商自主研发、掌握核心软件技术，并建立软件安全可信标准的认证实验室，推动数据软件产业高水平、安全发展。

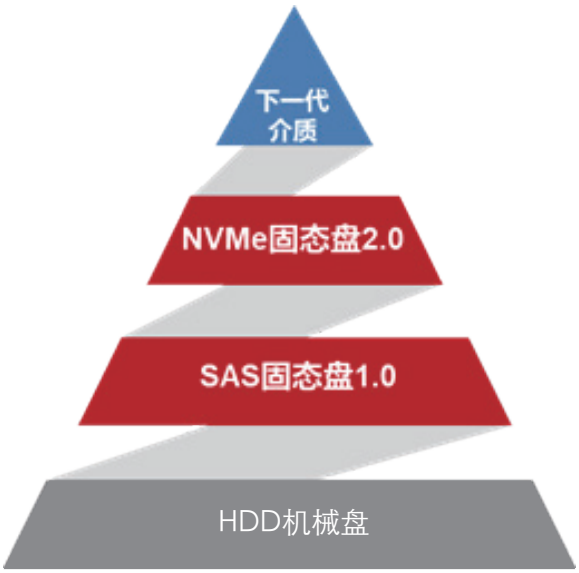
4.4 数据基础设施的绿色节能

据赛迪报告数据显示，我国数据中心数量从2012年的5.1万个发展到2019年的7.4万个，超大型、大型数据中心数量占比达到12.7%（引用来源）。数据的计算和存储都将耗费大量的能源，而提升数据中心能源利用效率主要有两个方向：一个是降低数据中心能源效率（PUE），PUE的降低代表了数据中心空调制冷等支撑设备的能耗占比降低。面对数字经济和数据量的快速增长，建设运营低PUE的数据中心是保障数据基础设施供应和绿色节能的第一步。另一个方向是提升IT设备的能源利用效率，数据中心IT设备高效节能是支持数字经济长远可持续发展、实施大数据战略和数据强国战略的重要保障。目前，有效降低数据中心每TB数据耗能的主要技术创新措施有：

4.4.1 介质节能

介质节能是利用半导体存储代替磁介质存储，硅进磁退方式节约能耗。存储介质是数据保存的关键部件。当前已经从HDD的磁盘介质演进到SSD的半导体存储介质。

图 4-5 数据存储介质发展示意



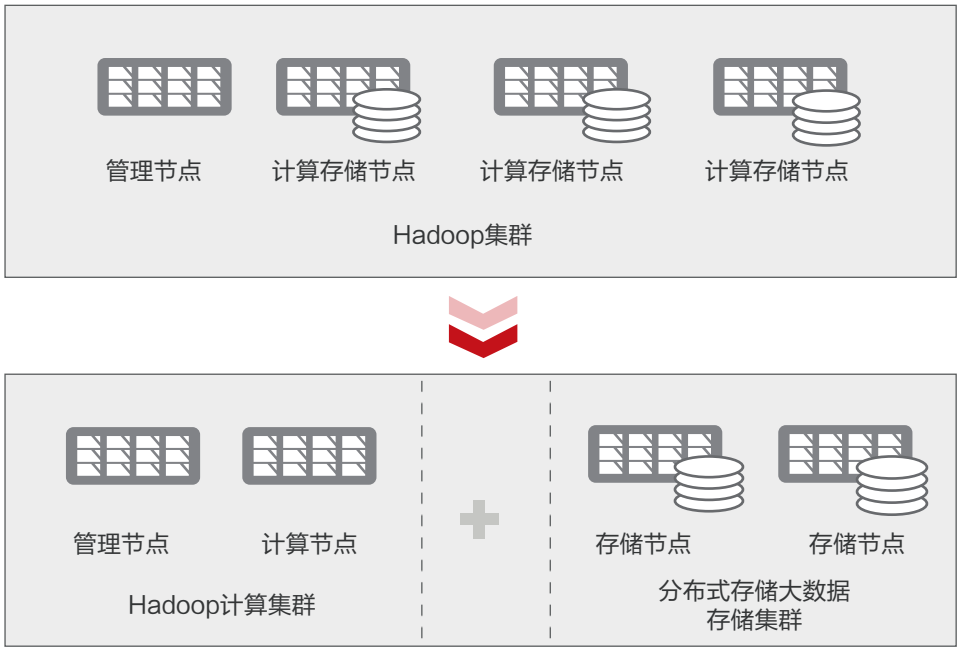
最常用的1万转SAS（1.2TB）HDD组成的存储系统典型功耗约10.6W/TB。SSD去掉了机械结构，增加了存储密度，能耗显著低于HDD，以常用的SSD（3.84TB）为例，其组成的存储系统典型功耗约5.3W/TB，可降低约50%能耗。目前，我国的数据中心还是以HDD为主，约75%的数据中心使用HDD，如果全部采用SSD，我国数据中心总能耗预计能降低近5~6%。

因此，在数据中心中推动计算资源闪存化和存储系统资源闪存化可以有效节能。建议数据中心通过部署配置全固态硬盘的存储型服务器和全固态硬盘的存储系统。

4.4.2 架构节能

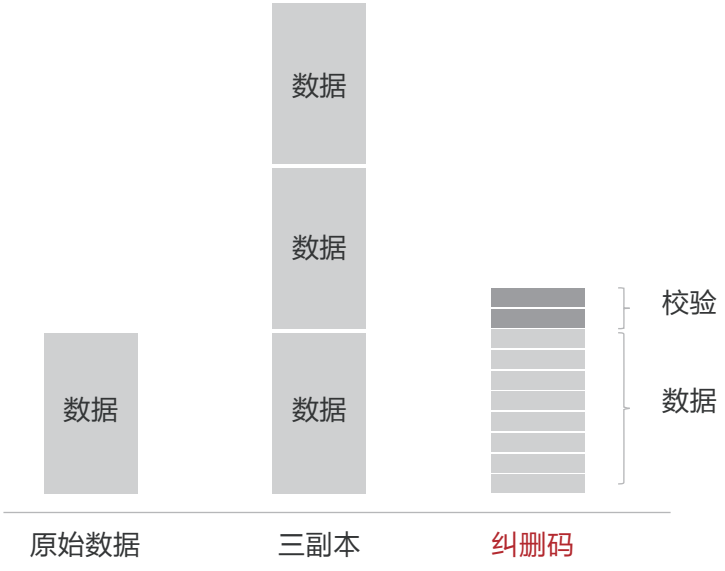
架构节能是通过存算分离架构，利用数据高密存储及纠删码技术来节约能耗。受限于散热和空间限制，普通的通用型服务器配备硬盘的数量有限，通常为1U10盘、2U24盘、4U36盘。而专门设计的高密存储型节点，能做到1U32盘、2U36盘、5U80盘、4U80盘、5U120盘，密度达到传统存储服务器的2~2.6倍，结合存算分离架构，相对使用通用型服务器，减少了节点CPU、内存及配套交换机，同等容量下带来能耗节约10%~30%。

图 4-6 大数据存算一体及存算分离示意



在大数据分析场景中，采用存算分离架构后，还可以利用数据纠删码（Erasure Code，EC）技术替代三次备份的方案，在实现同样可靠性等级的前提下把磁盘利用率从33%提升到91%，减少磁盘空间占用，节约能耗。

图 4-7 数据纠删码技术示意



4.4.3 算法节能

算法节能是利用数据重删压缩，相同空间存储更多数据的方式进行节能。借助闪存介质提升100倍性能。目前业界已经能够在数据库、桌面云、虚拟机等业务场景实现2~3.6的数据缩减率（重删压缩前数据总量/重删压缩后数据总量），相当于同样的存储空间能够储存2~3.6倍的数据，耗能节约50%以上。

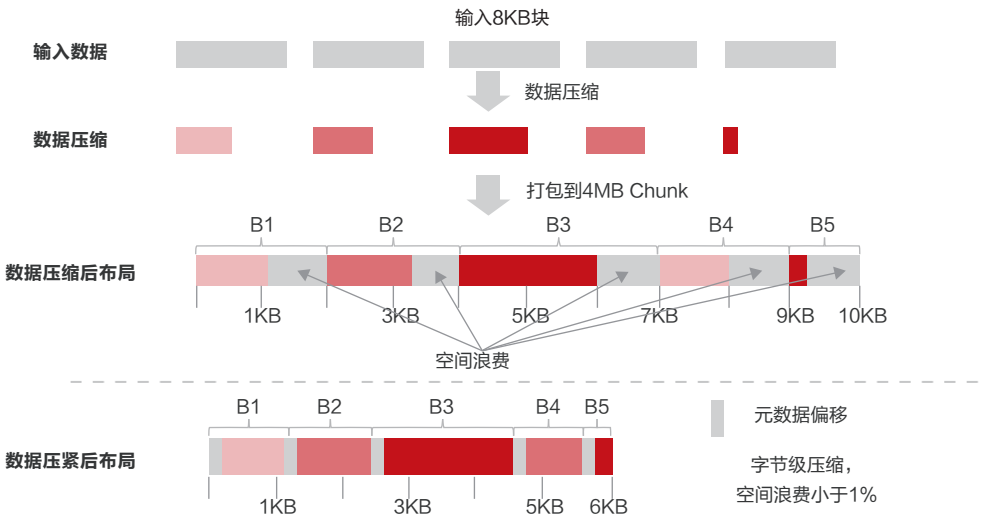
数据重删技术是通过利用定长重删、变长重删、相似重删算法来检查数据块，然后把相同数据删除的技术。

图 4-8 数据重删技术示意

重删场景	示意	定长重删	变长重删	相似重删
完全相同：整数据块		√	√	√
部分相同：sector偏移		×	√	√
部分相同：字节偏移		×	×	√
部分相同：任意修改		×	×	√

数据压缩、压紧技术是通过数据压缩、压紧算法把定长的数据块优化数据存储布局，节约存储空间。

图 4-9 数据压缩压紧技术示意



综合评估如上数据节能技术，为了应对数据的爆炸式增长，支撑企业更好的进行数据价值变现，建议在数据中心大规模普及全闪存及数据高密存储技术，节约数据中心数据存储耗能，使用同等电力情况下存储更多数据，来应对数字经济时代高速增长的数据存储需求。

05 数据安全防护的关键技术

数据安全防护关键技术是数据安全和隐私保护方案的基础。依据数据安全治理的理念，从软件到硬件，从网络边界到内部，从事前准备到事后追溯，几乎所有的安全技术都可以用在数据安全的防护上。受篇幅所限，本节将着重介绍以下几个关键技术领域：

- 设备系统安全

  防止攻击者利用设备软硬件的安全漏洞发起对数据的攻 击。数据越敏感，对承载其存储和使用的设备的系统安全性要求越高。

- 密码学及隐私保护算法

  在数据脱离系统安全机制保护的情况下，对数据安全和隐私提供保护。

- 认证和访问控制

  根据数据等级以及相关业务的配套安全策略，对访问者的身份和权限进行管控。

- 数据安全管理

  根据数据面临的风险，配置策略，构建对攻击快速感知和响应以及事后审计能力。

5.1 设备系统安全技术

从攻击的发展历史来看，基于系统的漏洞攻击是当前重要攻击手段。当一个操作系统甚至硬件的漏洞被攻击者利用时，攻击者就可能获得机会绕过安全机制，对系统数据进行攻击，进而造成严重的风险。一般来说，设备系统安全包括硬件的安全和操作系统的安全。而设备的系统安全能力构建有两个层面的考虑，即如何保证系统自身的完整性，以及如何支撑业务和数据的安全。常用的设备系统安全技术和设计理念如下：

5.1.1 可信启动

系统完整性保护的主要思路是基于硬件可信根，构建信任链，对系统进行完整性的度量，保证系统不被篡改。启动过程为链式关系，逐级进行签名校验，任何一级校验不过就视为启动出错。启动链完整性可以延伸到系统启动后的一些关键高权限应用，确保系统运行时具备基础的安全环境。

5.1.2 可信执行环境

可信执行环境（Trusted Execution Environment）可以为关键业务提供一个可信赖的安全执行环境，并且保护相关关键数据的机密性和完整性。可信执行环境的本质是隔离，典型的可信执行环境包括TrustZone，SGX等。可信隔离的方式包括处理器级隔离、特权模式隔离、软隔离，前两种方式依赖芯片提供特定支持，后者则是较容易在轻量级设备上部署。可根据不同场景的需要酌情选择。

5.1.3 操作系统内核的MAC

操作系统在运行过程中需要考虑防止黑客利用利用漏洞来提权。为了防范这种问题，操作系统应具备强制访问控制机制（Mandatory Access Control），典型的强制访问控制机制是SELinux。SELinux可以实现对系统资源的精细化访问控制。对于进程只赋予满足业务诉求的最小权限，对于系统服务进程等需要高权限访问系统资源的进程，需根据业务架构进行进程的分拆，只对关键核心进程保留高权限，其他无需高权限的进程仅保留满足业务需求的最低权限。

5.1.4 操作系统内核完整性保护

操作系统在运行过程中需要考虑防止黑客篡改内存中的内核代码。操作系统是设备资源管理的核心所在，负责绝大多数系统资源的管理和调度，也是为应用程序提供安全保障的最重要角色。操作系统本身代码规模庞大，在无法彻底消除漏洞的前提下，操作系统需具备一定的抵抗漏洞的韧性，降低操作系统漏洞被利用带来的危害性。

5.1.5 芯片安全

芯片安全包括芯片的自身安全和基于芯片的安全技术两个关键领域。芯片的自身安全保证了系统本身的安全可信，主要解决针对芯片和硬件的多种安全威胁，如新型侧信道攻击、以Rowhammer和骑士漏洞为代表的新型故障注入攻击和芯片级的后门与硬件木马。基于芯片的安全技术是以芯片和硬件为安全根，向上延伸出多种安全技术，自下而上的保障如固件、操作系统、软件等系统其它部分的安全，典型代表有可信计算技术、机密计算技术和密码学算法加速技术等。

众所周知，系统安全严重依赖于芯片和操作系统安全，芯片安全和操作系统安全一直都是学界的研究热点和业界难题，也是近年来大国间网络安全博弈的主要领域之一。因为芯片技术和操作系统本身具有的先进性和高技术门槛，基于芯片和操作系统的攻击一直高级黑客进行网络攻击和渗透的“杀手锏”。一直以来，每次针对芯片和操作系统的木马和安全事件都带来了较大的政治经济影响。如Shadow Brokers黑客组织在2020年泄露了NSA一些工具，其中名为DoublePulsar的后门程序可利用Windows系统（Windows XP，Windows Server 2003，Windows 7和8以及Windows 2012）部分漏洞进行恶意代码注入攻击[15]。

作为整个ICT基础设施的底座和基石，芯片的安全技术以及标准体系的发展和完善任重道远。

5.2 密码学及隐私保护算法

密码学体系是保护数据安全的关键技术手段，国际上为了确保密码学算法具备足够的强度并且被正确使用，进行了大量的研究、标准、以及法律工作。以我国为例，《中华人民共和国密码法》[16]《密码标准应用指南》[17]《商用密码管理条例全文》[18]等多部法律法规共同定义了密码算法和密钥保护的使用规范和实现方法。

密码学体系在数据存储、使用、传输等各个环节都发挥着重要的作用。在数据存储阶段，按照加密算法适用的不同层次，对数据的加密方案分为卷加密、文件系统加密、应用加密等。如IEEEP1619 “Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices”定义了卷加密的标准，其中AES-XTS作为一种重要的卷加密的密码算法。文件系统加密，如Windows的EFS，通过和文件系统的深度结合，实现用户无感知的加解密。应用加密指的是在数据落盘前，由应用负责对数据进行加密。不同层次的密码算法是相互补充的关系，多层次的加密体系互相配合，保证在存储介质即使被盗但是在密钥得到很好保护的情况下数据明文不被泄露。

15.Double Pulsar NSA leaked hacks in the wild, https://www.wired.com/beyond-the-beyond/2017/04/double-pulsar-nsa-leaked-hacks-wild/
16.《中华人民共和国密码法》，http://www.npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74.shtml.
17.《密码标准应用指南》，https://www.iteye.com/resource/zweib730-12275745
18.《商用密码管理条例全文》，http://m.law-lib.com/law/law_view.asp?id=477

与存储阶段的分层次的加密方式类似，传输阶段对数据的加密自下而上分为物理层加密、MAC层加密、网络层加密、传输层加密和应用层加密。目前，物理层加密主要集中在研究阶段，实际部署很少，主要分为基于密码算法的数字信号加密和基于调制解调或混沌理论的模拟信号加密两种手段。MAC层加密由思科公司提出并标准化为IEEE 802.1AE标准。该标准采用AES-GCM标准算法进行加密，密钥由上层协商或手动注入。网络层加密的协议以IPSec为代表，主要用于VPN等安全协议。传输层加密的代表协议是日常使用最多的TLS协议，是当前网络传输安全的重要基石，也是很多上层应用的重要组成部分。应用层加密主要与业务强相关，比如近期谷歌、脸书和思科联合推动的MLS协议就是一个应用层端到端加密消息的协议，里面代表性的密码算法包括使用TreeKem解决端到端加密协议中对大群组不友好的问题。同存储加密一样，传输的分层次加密各个层次之间是互补的关系且不可替代，每一层次应对的安全挑战不同，解决的安全问题不同，各个层次相互配合才能保护数据传输安全。在传输的加密设计过程中要考虑到数据的解密节点是否足够安全。如果数据流动过程中会经过不可信的设备，应考虑端到端加密的方案。当数据加解密被大规模使用以后，其带来的性能开销需要慎重的考虑。安全与效率永远是矛盾体，目前主要有两种手段来解决，一种是改进加解密算法，比如NIST现在正在进行的轻量化算法竞赛，另一种是通过硬件加速，可以使用专用硬件（比如ARM和X86都有提供的AES指令集或者苹果的Enclave芯片和谷歌的Titan芯片），也可使用通用平台的特殊特性（比如ARM和X86都提供的SIMD架构）。通过多种方式的配合可以缓解这个矛盾。

使用阶段的数据保护是数据安全的重要挑战，主要解决手段可以分为保护和脱敏。保护的基本思想还是基于数据加密。第一种保护方法是基于可信执行环境可以达到保护数据的目的。所有在可信执行环境内的运算和数据对外都不可见。第二种保护方法时基于密码学算法，比如同态加密、多方计算、可搜索加密等。以同态加密为例，同态加密允许在加密数据上进行运算，并得到加密的运算结果。攻击者无法在运算过程中得到数据。

脱敏的基本思想区别于传统数据安全，通过隐私保护算法将数据的敏感部分清洗掉，从而允许非敏感部分公开使用。隐私保护算法是解决数据的处理方和交换数据接收方可能泄露敏感数据的问题的重要技术手段。脱敏算法可以在保留数据原始特征的同时改变部分数值，防止数据的处理方或接收方因意外或有意的窃取敏感数据，同时又可以保证相关的业务处理不受影响。常用的算法包括：①泛化算法。考虑了多维属性之间的关联关系，防止从多个属性或多个数据集关联识别个人，泛化要达到的指标包括K-anonymity、L-diversity、T-closeness等；②差分隐私算法。通过增加随机的噪声，对个人的敏感信息进行匿名化处理。

数据脱敏技术在隐私合规场景下被广泛应用，比如AI模型训练、大数据统计等，即在保留数据意义和有效性的同时保持数据的安全性并遵从数据隐私规范。

密码学是安全解决方案的基础。密码算法的不当使用，或者使用有缺陷的密码算法，将造成严重的数据安全隐患。在国际上的密码学标准长期被西方管控，这对国家安全造成了严重的影响。2013年12月，据路透社披露，NSA通过买通RSA公司将有安全风险的Dual_EC_DRBG算法作为Bsafe设备中的首选随机数生成算法[19]。在我国有大量RAS用户，涉及通信、金融、制造业等行业重要用户，如中国电信、中国移动、中国联通、中国网通、中国银行、中国农业银行、中国工商行、中国建设银行、华为和海尔等。因此，加强对密码学的研究以及密码学系统和设备的有效管控是保护数据安全重点考虑的要素。

5.3 认证和访问控制技术

认证和访问控制是通用的安全技术。任何对数据的相关操作或者对访问数据的软硬件操作请求都必须经过认证，以确定其身份的合法性，进而通过访问控制来确定数据访问者有足够的权限。对于不同的访问控制系统，对数据访问者的身份的关注点可能也不同。比如根据不同的访问控制策略，访问控制系统可能需要判别对数据的请求是否来自一个合法的用户，是否来自一个合法的设备，或者来自合法的应用。相应的，一个认证体系可能需要对自然人，对设备，或者对应用进行认证。当前对用户的认证过程中除了传统的密码之外，往往还需要考虑基于生物特征或者硬件OTP（One Time Password）的方案来增加认证结果可信性，以应对目前越来越猖獗的基于社会工程学和盗取凭据的攻击手段。对于设备的身份认证，一般是基于提前部署的证书等凭据对设备的真实性进行校验。对于代码的认证，则一般是通过签名来对代码的合法性进行校验。

针对用户对数据安全访问服务的多样性，结合数据生命周期访问需求和特点，可以采用基于角色访问控制或者基于属性访问控制等方案来实现数据有效的管控。

当前，数据安全防护的场景复杂。特别是新冠疫情对企业运行及人们的工作方式产生了巨大的影响，越来越多的设备在企业的安全边界以外访问数据。在带来了工作便利的同时，也模糊了安全边界，增加了安全管控的难度。根据《电信和互联网行业数据安全治理白皮书（2020年）》统计，中国软件评测中心网安中心在电信和互联网行业的威胁监测中，发现80%的安全漏洞或问题与数据安全相关，其中非授权访问是主要的攻击手段，包括弱口令、授权绕过、未进行身份验证等。

为了缓解日趋严重的数据安全风险，业界正在数据存储、处理和传输的系统认证和访问控制设计中广泛引入零信任的理念，即无论是处于网络界限之内或是之外，系统都不应该自动信任任何人和设备。连接到组织系统的任何人和设备在获取访问权限之前，必须首先验证其身份和权证。根据Forrester2020年二季度关于零信任产业的统计数据[20]，零信任相关营收超过1.9亿美元的厂商已超过10家，零信任已进入规模化产业发展阶段。同时，美国政府和军队都将零信任的实施作为优先事项。2019年以来美国国防创新委员会、美国国家标准委员会等机构均发表了零信任相关的报告或标准。2021年5月，拜登政府上台后，发布《关于改善国家网络安全的行政命令》，要求美国联邦政府专项安全的云服务和零信任架构，并强制要求在特定时间内部署多因素认证和加密。同月，美国国防信息系统局（DISA）公开发布初始国防部（DoD）零信任参考架构，增强其网络安全并在数字战场上保持信息优势。2019年以来，我国先后发布了《关于促进网络安全产业发展的指导意见（征求意见稿）》《零信任安全技术一参考框架》《信息安全技术零信任 参考体系架构》等国家和行业标准，加强我国零信任架构部署和实施。

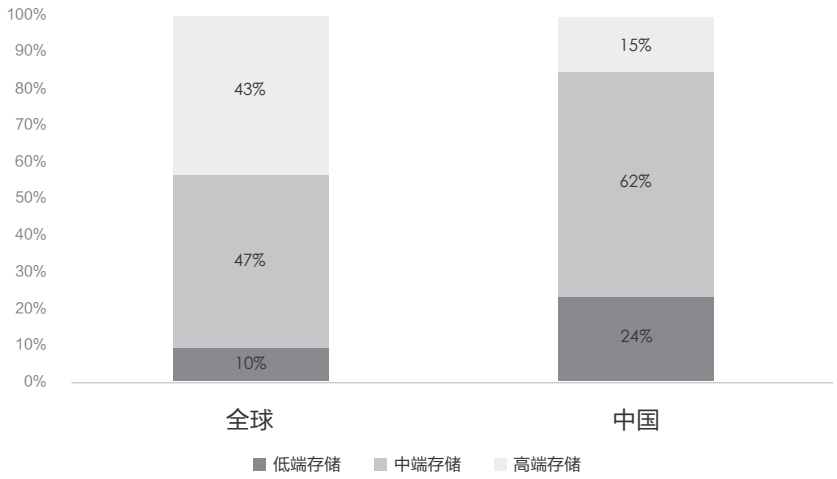
19.Exclusive: Secret contract tied NSA and security industry pioneer, https://www.reuters.com/article/us-usa-security-rsa-idUSBRE9BJ1C220131220
20.网络安全先进技术与应用发展系列报告 零信任技术（Zero Trust）（2020年）中国信通院

5.4 关键业务的高可靠数据保护技术

我国关键业务的数据保护特别是关系到国计民生的关键行业和核心数据保护水平还落后于发达国家。关键业务数据要求高可靠、高性能、高效能、高可信，需要通过高端存储和数据灾备保护来确保关键业务数据的安全性。

高端存储具有可靠性好、能效高、性能强等特点，适用于对业务连续性和安全可信有很高要求的关键业务场景。目前，我国数据存储市场仍以中低端为主，高端存储应用占比不到15%，而发达国家的高端存储应用占比达43%，建议我国大力提升高端存储占比，提升数据存储性能和安全性。

图 5-1 中国高端存储占比远低于发达国家



另外，虽然数据基础设施的资源和管理水平都有了较大提升，但是数据集中也引发了新的问题。由于故障域变得更大，任意一个小的设备故障或者灾难都可能会引发大面积的业务中断，甚至数据永久丢失。近年来发生了多起由于自然灾害，人为破坏等因素带来的数据丢失的案例。

我国政府非常重视对数据的保护，通过《网络安全法》及《关键信息基础设施安全保护条例（征求意见稿）》等相关立法，来要求金融、通信、能源、交通、水利等行业对关键数据基础设施进行容灾保护。2007年，发布国家级强制性标准《GB/T 20988-2007信息安全技术 信息系统灾难恢复规范》[21]，定义了灾难恢复能力等级。但是，该规范定义的系统恢复指标比较宽松，场景没有细化，不能适应当前智能时代对信息系统安全保护的要求，亟待修订完善。

21.GBT 20988《信息安全技术 信息系统灾难恢复规范》

>>> 表 5-1 灾难恢复能力等级划分 <<<

等级	恢复指标
1级-基本支持	信息系统2天以上恢复 允许1天至7天数据丢失
2级-备用场地支持	信息系统24小时以上恢复 允许1天至7天数据丢失
3级-电子传输和部分设备支持	信息系统12小时以上恢复 允许小于24小时数据丢失
4级-电子传输及完整设备支持	信息系统数小时-2天内恢复 允许小于24小时数据丢失
5级-实时数据传输及完整设备支持	信息系统数分钟-2天内恢复 允许小于30分钟数据丢失
6级-数据零丢失和远程集群支持	信息系统数分钟恢复 零数据丢失

数据来源：《信息安全技术 信息系统灾难恢复规范》

2019年，为了配套《网络安全法》实施，国家市场监督管理总局、中国国家标准化管理委员会联合发布《GB/T 22239-2019信息安全技术 网络安全等级保护基础要求》[22]，形成了新的网络安全等级保护基本要求标准，针对应用和数据安全，规范了基础设施灾备保护技术和管理要求。其中，技术要求按照四个等级进行规范和评估：

>>> 表 5-2 信息安全技术 网络安全等级保护灾备技术分级保护需求 <<<

级别	保护需求
一级	本地备份恢复
二级	本地备份恢复+异地定时备份恢复
三级	本地备份恢复+异地实时备份恢复+本地业务高可用
四级	本地备份恢复+异地实时备份恢复+本地业务高可用+异地业务高可用

数据来源：《信息安全技术 网络安全等级保护基础要求》

据调查，金融领域对信息系统要求非常高，虽然绝大部分核心业务建设了灾备体系，但是由于测评标准不完善，在测评过程中并未对容灾体系进行模拟切换演练。当灾难发生时，出现了“不敢切换”“不能切换”等情况，导致90%的灾备体系不具备真正的业务延续性，无法保证业务7*24小时不中断。而在运营商、医院等行业领域情况更加严重，只有不到10%的核心业务做了灾备。由此可见，我国数据基础设施的灾备体系还不太健全，大部分还是流于形式。

数据安全灾备保护的要求不仅仅是关注当前，更需要着眼未来。2020年，全球最大的开源代码社区Github宣布代码永久封存北极底下1000年，永久保护人类文明智慧结晶。我国从国家法规和行业管理办法层面，对核心关键业务数据的归档长久留存制定了相关保护管理法规和规范要求：在政府电子档案、金融会计档案、档案馆、司法档案、广电音视频资料、医疗病历影像、医

22.《信息安全技术 网络安全等级保护基础要求》GB/T 22239-2019

疗监管、油气勘探测绘等各个领域都有数据档案资产长期低成本保护诉求。《中国人民共和国档案法》中要求配置必要的设施，确保档案的安全；采用先进技术，实现档案管理的现代化；财政部国家档案局令《会计档案管理办法》规定银行会计档案的保管期限分为永久、定期两类，定期保管期限为10年和30年；《企业文件材料保管范围和档案保管期限规定》也明确了类似存储保护管理要求；《GB/T18894-2016电子文件归档与电子档案管理规范》规定，电子档案离线存储介质至少应制作一套，电子档案应满足保存三个副本，一份供查阅使用、一份封存保管和一份异地保存。

通过不断优化数据基础设施的灾备保护技术和管理体系，完善基础设施灾备体系建设，将进一步保障数字经济基础设施平稳健康发展。

5.5 数据安全管理技术

5.5.1 数据资产安全分析技术

数据安全治理的基础要求就是摸清被保护的数据资产。只有摸清数据资产底数，才可能对数据进行全面的、细粒度的安全管理。比如，为了判断系统中数据是否获得了有效地保护，首先需要了解在系统中特定数据如何被存储、存储位置、配套安全策略、业务内容及范围以及用户访问数据权限等。

数据资产梳理的关键技术首先是数据发现，即确定数据的存储分布状况，按照数据分类分级的规则，对数据打标签，形成完整的数据资产视图。这类技术可以大大降低数据资产梳理过程中的工作量，有助于对于数据的安全死角（比如数据处理过程中的中间数据、敏感数据）进行扫描，解决数据安全管理“灯下黑”的情况。在数据的存储分布情况的梳理基础上，可以进一步对数据访问、流动、共享进行梳理和分析，形成数据访问、传输和共享的流图。

结合安全合规策略，数据资产安全分析还可以对数据合规风险进行更全面的评估，判断数据是否已经根据特定合规的要求得到了有效的保护。对于存在风险的数据，可以结合检测和响应的能力进行修复。

5.5.2 数据安全审计

随着数据与业务逐渐独立，数据来源多样化，数据起源信息变得十分复杂。同时，数据处理过程中也容易受到内部和外部伪造、篡改、重放等攻击。数据在不同的业务之间流动和处理成为常态。在安全事件追溯过程中，数据安全责任主体增多，数据流动环节复杂度增大，安全事件审计确权确责难度加大。更不用说，数据分享经常是跨组织、跨安全系统边界进行。这些都使得攻击行为的追溯变的极为困难。因此，一个完善的数据安全审计方案需要慎重考虑数据整个生命周期。

数据采集阶段

数据采集阶段是数据生命周期的起点，数据分类和分级管理从这里开始。在这个阶段，对数据类别和级别进行标注会对后续数据处理产生重要影响，通常涉及元数据操作。数据采集阶段的审计重点工作之一确保元数据操作的可追溯性。通过对数据分类、加密、隔离等操作审计，确保对采集数据进行分类分级和防护的整个过程的追溯。

数据传输阶段

数据传输的安全审计需要重点关注传输安全策略的执行情况，对发送方和接收方的设备、接口、通讯协议以及加密方法等信息进行记录，及时发现传输过程中可能引发的敏感数据泄露事件，通过数据传输双方的日志信息可以发现异常传输的行为。

数据存储阶段

数据存储阶段的安全审计主要是对数据存储和读取的动作以及备份的行为进行审计。通过对数据操作主体、时间、操作类型的分析，发现数据访问者的可能异常行为并确保数据配套的存储安全策略得到正确的执行。

数据处理阶段

数据处理阶段的安全审计是对数据处理各个业务接口的操作记录进行审计，可以帮助发现数据处理当中的风险。另外，数据处理阶段的安全审计重点之一是关注脱敏处理过程，对敏感数据脱敏相关操作的记录进行审计，可以帮助发现机密信息或者个人数据隐私可能泄露的情况。

数据交换阶段

数据交换过程的安全审计是数据安全审计过程的重点。在数据共享阶段，需要对高价值的数据的导入、导出、共享操作进行持续监控，并且要审计和追溯交换数据是否已经脱敏，是否已经加密，或者保留有水印等。

数据销毁阶段

数据销毁阶段的安全审计重点关注对存储介质和数据的访问行为、数据销毁过程进行监控。相关审计信息应该包括数据删除的操作时间、操作人、销毁的方法、数据类型，操作结果等相关信息。

5.5.3 人工智能技术

人工智能是数据安全的倍增器，广泛应用到数据安全各个方面。在数据分类分级的过程中，基于人工智能的方案可以对更加复杂的上下文进行分析。在认证访问控制以及检测响应的过程中，基于人工智能的方案可以更有效地发现攻击者的异常行为，提高检测的精准度和系统应对攻击的响应能力。

根据《中国网络安全产业白皮书》[28]，当前人工智能与数据安全结合的越来越紧密，目前业界人工智能在数据安全领域成功的应用经验包括：

- 数据分类和合规分析：人工智能在敏感数据挖掘、图片文件内容实时监控和标记、数据防泄漏等方面都有很好的效果。比如：亚马逊推出 Amazon Macie Analytics 服务，可通过机器学习技术自动识别重要数据访问、复制、移动等可疑行为，并实施精准实时的修复措施，防范重要数据暴露及共享业务中的数据安全风险；Netapp推出了数据分类分级产品，利用人工智能提升了数据分类的精准程度，并且可以支持自动生成包括GDPR在内的多种法律法规的合规报告，提升了数据安全治理的效率；亚信安全的数据分类分级发现系统可以在数据块维度进行多任务并行处理，利用机器学习+语义分析生成训练　模型，提高数据分类速度和精度，并提供数据特性及变化趋势展示。

- 通过人工智能算法训练加密流量检测模型，对异常数据传输进行分析。思科的人工智能驱动的加密流量分析方案，使用机器学习算法，在分析初始数据包特征以及后续数据包长度与时序等的基础上识别加密后的异常流量。

- 借助机器学习技术来检测组织系统和网络中的异常行为，并根据异常信息来检测网络攻击，自动形成应对的操作，减少针对数据攻击的风险。目前IBM 推出 Resilient 事件响应平台，可提供响应流程定制功能，灵活编排响应活动并自动审计跟踪，实现对威胁事件的快速响应；Palo Alto Networks推出人工智能安全平台 Cortex，致力于打破网络、云端、终端数据孤岛，并支持对海量数据分析、威胁发现及响应策略快速编排。

人工智能在数据安全领域的应用有巨大的潜能，但同样存在巨大的安全风险。中国信通院的《人工智能白皮书（2018）》对人工智能安全面临的挑战进行了系统分析，比如目前很多人工智能算法在设计之初普遍未考虑相关的安全威胁，使得人工智能算法的判断结果容易被恶意攻击者影响，被污染的样本所误导，导致人工智能系统判断失准。人工智能缺乏道德规范约束，可能导致公众权益受到侵害。比如，2021年，我国315晚会上曝光部分商家利用人脸识别技术搜集顾客信息的违法行为。

因此，如何保证人工智能自身安全和监管人工智能使用，是业界需要慎重考虑的问题。

28.中国网络安全产业白皮书（2019年），中国信通院

06 我国数据安全法律法规体系

6.1 法律法规体系

作为数字化转型的关键与核心，数据对于数字经济的发展有着举足轻重的地位。数据安全问题给个人隐私保护、经济安全发展和国家安全带来挑战，各国亟需建立健全和完善数据安全法律法规体系。2020年9月，在“抓住数字机遇，共谋合作发展”国际研讨会上，我国提出了《全球数据安全倡议》，提出“秉持发展和安全并重的原则，平衡处理技术进步、经济发展与保护国家安全和社会公共利益的关系”，并呼吁各国应尊重他国主权、司法管辖权和对数据的安全管理权。因此，提出数据安全治理相关立法的中国方案，也成为践行《全球数据安全倡议》的题中之意。

6.1.1 现行法律法规梳理

在国家层面，2014年4月15日，在中央国家安全委员会第一次全体会议上首次提出“总体国家安全观”的重大战略思想，提出了“构建集政治安全、国土安全、军事安全、经济安全、文化安全、社会安全、科技安全、信息安全、生态安全、资源安全、核安全等于一体的国家安全体系”的要求。基于此，2015年颁布的《国家安全法》[23]第25条明确提出了“实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控”，将数据安全纳入国家安全的范畴。作为我国网络安全领域的首部综合性立法，《网络安全法》[24]于2017年正式施行，引入了网络数据的概念，将网络数据定义为“通过网络收集、存储、传输、处理和产生的各种电子数据”，提出了“维护网络数据完整性、保密性和可用性”“鼓励开发网络数据安全保护和利用技术”“防止网络数据泄露”等要求，并要求在中国境内收集和产生的个人信息和重要数据应当在境内存储。通过建立网络安全等级保护、关键信息基础设施保护以及数据本地化和跨境流动等制度，对数据及关键基础设施安全进行保护。国家互联网信息办公室于2017年4月发布了《个人信息和重要数据出境安全评估办法（征求意见稿）》，于2017年7月发布了《关键信息基础设施安全保护条例（征求意见稿）》，于2019年5月发布了《数据安全管理办法（征求意见稿）》，于2019年6月发布了《个人信息出境安全评估办法（征求意见稿）》。2018年6月中国发布了《网络安全等级保护条例（征求意见稿）》。上述配套制度均在研究制定中，尚未颁布实施。

在地方层面，吉林、山西、海南、贵州、天津等地相继出台了的本地大数据发展和应用相关条例，对大数据安全问题提出了原则性的规定。在本地大数据发展和应用的地方性条例的基础上，贵阳市于2018年10月颁布了《贵阳市大数据安全管理条例》，旨在保障该市辖区内大数据发展和应用的安全保护、监督管理及相关活动。该条例要求数据安全责任单位从制度、人员、系统设备等方面对大数据安全进行保护，并要求市政府建立联席会议制度推进解决大数据安全相关重大事项。天津市于2019年6月发布了《天津市数据安全管理办法（暂行）》，是全国首部数据安全相关的省级地方性专门规章。该办法提出了“数据运营者”的概念，对“数据运营者”提出了信息备案、落实安全管理制度和技术措施、建立系统资产安全规范和资产清单、指定数据安全管理部门岗位及人员、向境外提供数据时进行安全评估、合法采集、安全传输存储和访问、合规使用、信息通报和指定安全预案等的要求，同时明确了由市政府网信主管部门关于数据安全监督检查、数据安全信息通报、数据安全监测的职责，要求市政府统筹应对安全事件的职责。贵州省在贵阳市的实践基础上，于2019年10月出台了《贵州省大数据安全管理条例》。此外，宁波于2020年9月出台了《宁波市公共数据安全管理暂行规定》。另外值得注意的是，2020年，深圳特区公布了《深圳特区数据条例（征求意见稿）》，该条例在诸多方面进行了大胆的尝试，如设立了“数据权”，明确了公共数据作为新型国有资产，提出了各级政府设立数据工作委员会，建立决策协调机制等。但该《条例》同样也存在立法权限、混同隐私权和财产权、数据权利主体权利冲突等问题。目前上述条例仍在审议过程中。总而言之，各地政府就数据安全问题出台了地方性法规、规章及规范性文件超过14个，各地的数据安全相关制度基本基于《网络安全法》以及各地的大数据发展和应用条例，主要以地方政府及网信办作为主导力量，

23.《国家安全法》2015年7月
24.《网络安全法》2017年6月

关数据的运营方提出了从获取到存储再到使用的全生命周期安全管理要求。

在专项数据安全管理方面，国务院及各部委颁布了相关行政法规及各类规范性文件。在行政法规方面，出台了《科学数据管理办法》《档案法》《保守国家秘密法》《国务院办公厅关于促进和规范健康医疗大数据应用发展的指导意见》《促进大数据发展行动纲要》《国务院办公厅关于运用大数据加强对市场主体服务和监管的若干意见》《电信条例》等。在部门规范规章及规范性文件方面，科技部、工业和信息化部、国土资源部、财政部、教育部、农业农村部、交通部、国家税务总局、中国银保监会、中国人民银行、中国民航局、中国气象局、国家卫健委等部委均出台了对各自领域数据的管理相关的规范性文件。

在个人信息保护方面，我国出台了《民法典》《刑法》《电子商务法》、《消费者权益保护法》《居民身份证法》《基本医疗卫生与健康促进法》等法律法规，加强对个人信息保护。值得注意的是，《民法典》在总则部分明确规定，自然人的个人信息受法律保护，并要求获取他人个人信息的应确保信息的安全。同时，《民法典》通过专章的形式，将隐私权与个人信息保护列为《民法典》人格权编的重要内容，对个人信息的定义、处理个人信息的原则、自然人对本人个人信息的权利、信息处理者及国家机关和法定机构的安全保障义务进行了规定。其中，明确要求了信息处理者应当采取技术措施和其他必要措施，确保其收集、存储的个人信息安全，防止信息泄露、篡改、丢失，并在发生上述情形时告知自然人并向有关主管部门报告的义务。

总体来看，目前我国的数据安全相关的法律法规是基于《国家安全法》及《网络安全法》建立的，并在网络安全等级保障制度、关键信息基础设施保护制度以及数据本地化和跨境流动制度等中有所体现。各地围绕数据安全、数据跨境等问题积极探索。同时，在个人信息保护上，基本以《网络安全法》《民法典》及即将出台的《个人信息保护法》为主；在国家秘密、档案等相关特殊性质的数据，通过特定单行法律法规进行保护；而对于其他特定行业数据而言，则通过各部门规章由进行管理和保护。由此可以看出，在现行已颁布的法律法规体系下，数据安全相关法律法规还存在着交叉和空白，配套制度的细则尚未出台等问题。

6.1.2 《数据安全法（草案）》[25]体系下的立法趋势洞察

2020年7月，十三届全国人大常委会对《数据安全法（草案）》进行了第一次审议，并公开征求意见。2021年4月，十三届全国人大常委会进行了二次审议。该草案将“数据”定义为“以电子或非电子形式对信息的记录”，同时对数据安全的内涵进行了诠释，即“数据安全是指通过采取必要措施，确保数据处于有效保护和合法利用状态，以及保障持续安全状态的能力”。另外，该草案明确了中央国家安全领导机构负责数据安全工作的决策和统筹协调。

首先，通过相关定义我们不难看出，该草案填补《网络安全法》对于非电子数据保护的空白。同时，也是对呼应2020年3月国务院《关于构建更加完善的要素市场化配置体制机制的意见》中对于“加快培育数据要素市场”的要求，在第5条中规定了“鼓励数据依法合理有效利用”“促进以数据为关键要素的数字经济发展”，并在第二章以专章的形式对数据开发利用和数据安全产业发展进行了阐述。

25.《数据安全法（草案）》2020年7月

其次，草案第三章中提出了将建立数据分级分类保护制度、重要数据保护目录、数据安全审查制度、特定场景下的数据出口管制制度、数据安全风险预警机制和数据安全应急处理机制组成的数据安全制度。但对于上述数据安全相关制度，草案同样仅做了总体性规定，没有具体实施细则，还需相关部门进一步制定细则进行落地实施。

再次，草案第四章规定了数据处理者的数据安全保护义务。主要包括明确数据安全负责人和管理机构，开展风险监测和风险评估，发生数据安全事件时立即采取处置措施以及主动报告，以及境外司法或执法机构要求调取中国境内数据时应经中国主管机关批准等制度。其中，草案特别规定了从事数据交易中介服务的机构，需要要求提供方对数据来源进行说明，审核双方身份。

另外，草案第五章主要就政务数据的安全与开放进行了原则性的规定，并将管理公共事务职能的组织履行法定职责开展的数据处理活动纳入政务数据的安全与开发相关管理规定中。

最后，在法律责任层面，草案就数据处理者不履行数据安全保护义务的行为、数据交易中介服务机构不履行相关审核义务、国家机关不履行数据安全保护义务等行为的处罚进行了规定。

总体而言，在立法定位上，即将出台的《数据安全法》是数据安全领域的基础法律，与现行的《网络安全法》和即将要出台的《个人信息保护法》并行成为网络空间治理和数据保护的三驾马车，《网络安全法》负责网络空间安全整体的治理，《数据安全法》负责数据处理活动的安全与开发利用，《个人信息保护法》负责个人信息的保护。

在立法趋势上，根据现有的草案文本，《数据安全法》将“维护数据安全”与“促进数据开发利用”并重，建立“数据主权”的概念。一方面，通过数据分级分类保护、重要数据保护目录、数据安全风险预警机制、数据安全应急处置机制、数据活动国家安全审查机制，确立了数据安全保障的相关制度。另一方面，通过政务数据和公共事务管理部门数据开放，推进数据基础设施建设、数据安全标准体系建设、数据安全服务发展、数据交易管理制度健全等，促进数据开发利用。同时，通过要求相关主体在境外司法或执法机构要求调取境内数据时，向主管机关报告获批的义务的“阻断”机制，在他国就数据和数据开发利用技术相关贸易和投资对我国采取歧视性措施时的反制措施，对与履行国际义务和维护国家安全的属于管制物项的数据采取出口管制措施，确立了我国的数据主权概念。

根据以上定位和趋势，我们可以预见，未来《数据安全法》一方面需要通过厘清相关定义，处理好与《网络安全法》和《个人信息保护法》之间的管理界限；另一方面需要通过制定具体的实施细则、产业政策、操作指南，将数据安全保障制度、促进数据开利用的政策和落实数据主权的举措进行进一步落实。

6.2 组织保障体系

在现行数据安全相关法律法规体系下，《网络安全法》规定了数据安全的组织保障体系。

一方面，《网络安全法》明确了网络运营者的内部责任，要求网络运营者通过建立内部安全管理制度，确认安全负责人，通过内部组织来落实相关安全的保护责任。另一方面，在外部组织保障上，《网络安全法》明确了网信统筹，电信、公安和其他机关各自负责的监督管理体系。除监督管理的组织体系外，《网络安全法》同时鼓励企业、高校、行业组织参与相关标准制定，并鼓励通过社会化服务体系推动相关安全认证、检测和风险评估等服务的开展。

在具体的网络安全等级保护制度和关键信息基础设施制度方面，主要由公安部主要负责相关网络安全等级保护，并与国家网信部门共同统筹协调有关部门对关键信息基础设施进行风险监测、应急演练、信息共享等。在对网络安全应急机制机制和预案制定方面，由国家网信部门制定了《国家网络安全事件应急预案》，建立了国家网络安全事件应急工作机制，各省(区、市)、各部门、各单位根据本预案制定或修订本地区、本部门、本行业、本单位网络安全事件应急预案。在相关网络安全事件风险增大时，由省级政府有关部门采取相关措施加强监测、评估风险，并发布风险预警及减轻危害的措施。在相关数据跨境传输上，由国家网信部门会同国务院有关部门进行安全评估。

6.3 监管执行体系

根据《网络安全法》，国家网信部门负责统筹协调网络安全和相关监督管理工作，国务院电信主管部门、公安部门及其他有关机关依据有关法律、行政法规在各自职责范围内负责网络安全保护和监督管理工作。

目前而言，对于数据安全的监督与执行以APP治理和个人信息保护为主。网信办、公安部、工业和信息化部与市场监管总局四部门于2019年1月联合发布了《关于开展App违法违规收集使用个人信息专项治理的公告》，成立了专项治理工作组，在全国范围内开展APP违法违规收集和使用个人信息专项治理行动，通过群众举报获得相关线索并通过公开、约谈、下架等措施对违规收集个人数据的APP进行警告和处罚。此外，针对金融、教育等特定领域，相应的监管机构如银保监会、中国人民银行、 教育部等部门也开展了各自领域内数据相关问题的治理活动。

6.4 数据安全评价体系

以数据安全的视角来剖析国家通用信息安全标准，主要分为技术支撑类标准、信息系统安全类标准、以数据为中心的数据安全类标准。技术支撑类标准规范了通用安全支撑技术，可以直接用于数据安全保护，如密码技术类标准。信息系统安全类标准主要是从系统的视角来规范各种安全控制措施，如网络安全等级保护、云计算安全、数据库管理系统、灾难恢复、网络存储设备安全相关标准，其中诸多安全控制措施都对数据安全起到重要作用。以数据为中心的数据安全类标准通常从数据全生命周期来考虑各种数据安全保护需求，以此提出相关技术要求和管理规范。另外，以数据为中心的数据安全类标准中，有一部分标准是以个人信息安全为目标，围绕业务系统中对个人信息的采集、存储、处理、共享、转让等各个处理环节提出安全要求。

其中，以数据为中心的数据安全类标准是在全国信息安全标准化技术委员会（TC260）研制，如下表所示：

>>> 表 6-1 以数据为中心的数据安全标准 <<<

标准名称	主要内容概述
GB/T 37988-2019 数据安全能力成熟度模型	给出了数据安全能力的成熟度模型架构，规定了数据采集安全、数据传输安全、数据存储安全、数据处理安全、数据交换安全、数据销毁安全及通用安全的成熟度等级要求。目前该标准正在进行试点工作。
GB/T 35274-2017 大数据服务安全能力要求	给出了数据安全能力的成熟度模型架构，规定了数据采集安全、数据传输安全、数据存储安全、数据处理安全、数据交换安全、数据销毁安全及通用安全的成熟度等级要求。目前该标准正在进行试点工作。
GB/T 37932-2019 数据交易服务安全要求	规定了通过数据交易服务机构进行数据交易服务的安全要求，包括数据交易参与方、交易对象和交易过程的安全要求。
GB/T 37973-2019 大数据安全管理指南	提出了大数据安全管理基本原则，规定了大数据安全需求、数据分类分级、大数据活动的安全要求、评估大数据安全风险。
GB/T XXX 网络数据处理安全规范（送审稿）	规定了网络运行者利用网络开展数据收集、存储、使用、加工、传输、提供、公开等数据处理活动应遵循的规范和安全要求。
GB/T XXX 重要网络数据识别指南（征求意见稿）	提出了重要网络数据的识别过程和方法，描述了重要网络数据的特征。
GB/T XXX即时通信服务数据安全要求（征求意见稿）[还有网上购物、网络音视频、网络预约汽车、快递物流服务数据安全要求标准]	这一系列的数据安全要求标准主体思路比较一致，规定了即时通信/网上购物/网络支付/网络音视频/网络预约汽车/快递物流服务运营者收集、传输、存储、使用、共享、披露、删除、出境的数据安全要求。

个人信息保护系列国家标准主要包括以个人信息安全规范为核心的通用个人信息保护系列标准。通用个人信息保护系列标准在全国信息安全标准化技术委员会（TC260）研制，如下表所示：

>>> 表 6-2 通用个人信息保护系列标准 <<<

标准名称	主要内容概述
GB/T 35273-2020 个人信息安全规范	规定了开展收集、存储、使用、共享、转让、公开披露、删除等个人信息处理活动应遵循的原则和安全要求。
GB/T 37694-2019 个人信息去标识化指南	描述了个人信息去标识的目标和原则，提出了去标识化过程和管理措施。
GB/T 39335-2020 个人信息安全影响评估指南	给出了个人信息安全影响评估的基本原理、实施流程。
GB/T XXX 个人信息安全工程指南 (报批稿阶段)	描述了个人信息安全工程目标，给出了在需求分析、产品设计、产品开发、测试审核、发布部署、运行维护等系统工程阶段的个人信息保护实施指南。
GB/T XXX 个人信息告知同意指南（送审稿阶段）	提供了网络运营者在个人信息处理过程中告知的内容、机制，以及如何征得个人信息主体同意收集、使用、对外提供个人信息的指导和建议。
GB/T XXX 个人信息出境安全评估指南（送审稿）	提出了个人信息出境安全评估的框架、流程、要点和方法。
GB/T XXX 移动互联网应用（App）收集个人信息基本规范（报批稿阶段）	明确了移动互联网应用程序收集个人信息时应满足的基本要求，用以规范移动互联网应用程序运营者收集个人信息的行为。
GB/T XXX个人信息去标识化效果分级与评定（征求意见稿）	给出了个人信息去标识化效果分级评定的方法与指南。

从行业领域来看，金融、政务、交通、医疗、电信等重点行业领域都相继制定数据安全标准，整体数据安全治理思路与国家标准保持一致。主要在各行业领域结合业务场景进行了相应的细化，如下表所示：

>>> 表 6-3 行业领域数据安全标准 <<<

行业领域	标准名称	发布组织	主要内容概述
金融行业	JR/T 0171-2020 个人金融信息保护技术规范	政府	基于个人信息保护、数据分类分级下的差异化保护治理思路，对金融机构在开展业务中提出了全面的安全要求。这些标准后续将逐步应用落地，其中，JR/T 0171-2020 个人金融信息保护技术规范 已正式纳入“个人金融信息保护能力认证”，作为认证依据。
	JR/T 0197 金融数据分类分级指南		
	JR/T XXX 金融数据跨境安全要求》（送审稿）		
	JR/T XXX 金融数据安全 数据生命周期安全规范》（送审稿）		
政务行业	GB/T 39477-2020 信息安全技术 政务信息共享 数据安全技术要求	全国信息安全标准化技术委员会（TC260）	规范了政务信息共享数据安全要求技术框架，规定了政务信息共享过程中共享数据准备、共享数据交换、共享数据使用各阶段的数据安全技术要求以及相关基础设施的安全技术要求。其他诸如贵州、杭州等地市也发布了政务数据安全相关标准。
交通行业	GB/T 37373-2019 智能交通 数据安全服务	全国智能运输系统标准化技术委员会（TC268）	主要规定了智能运输系统安全支撑平台和数据安全服务内容。
医疗行业	GB/T 39725-2020 信息安全技术 健康医疗数据安全指南	全国信息安全标准化技术委员会（TC260）	给出了健康医疗数据控制者在保护健康医疗数据时可采取的安全措施。

电信行业	GB/T XXX 电信领域大数据安全防护实现指南》国家标准（送审稿阶段）	全国信息安全标准化技术委员会（TC260）	为电信企业大数据平台安全建设、大数据业务开展时安全防护能力的同步建设提供大数据安全防护实现指南。
	YD/T XXX电信网和互联网数据安全通用要求（送审稿）等系列数据安全标准	中国通信标准化协会（CCSA）	围绕工业和信息化部办公厅发布的《电信和互联网行业数据安全标准体系建设指南》，CCSA在研、发布了诸多关于电信和互联网行业领域的数据安全标准，电信网和互联网数据安全通用要求系列标准提出了全面的数据安全治理标准及相应的评估规范。

综上，我国数据安全及个人信息保护相关标准逐步建立健全，已形成数据分类分级、全生命周期安全、分级别差异化保护的通用数据安全治理思路。在执行落地方面，主要是有关部门在结合《App违法违规收集使用个人信息行为认定方法》《2020年电信和互联网企业网络数据安全合规性评估要点》等文件，对APP运营者、电信和互联网信息系统运营者进行个人信息、网络数据安全方面的监督管理。预计后续有关部门及第三方测评、认证机构会逐步以政策法规为纲领，将数据安全及个人信息保护相关国家、行业标准作为执行准则，对网络运营者进行数据及个人信息保护能力、信息系统落实情况的细化监管和评测。

07 展望及倡议

随着数字经济发展，不断产生的海量数据将成为国家战略支撑点。为了确保数据战略安全健康实施，护航经济发展，需要从政府、科研、产业界、学术界、行业应用等多方面加强对数据产业、数据安全的支撑。可以预见，《数据安全法》出台在即，将推动落实与数据安全保护相关的一系列措施，各行业宜围绕国家数据安全战略，提升数据安全产业基础能力，加快研究和应用数据安全防护技术，健全完善数据安全法律规范与标准，构筑数据安全战略国际领先，向国际推出数据安全中国方案。

7.1 提升数据安全产业基础能力

7.1.1 加大普及全闪存数据中心力度

全闪存已成为产业共识，加速“磁退硅进”已成为业界趋势。越来越多的新建数据基础设施已经开始大规模采用全闪存技术，配合全IP化高速互联系统架构及高速数据中心网络，建设全闪存数据中心。通过建设全闪存数据中心，一方面提升数据中心的性能、服务响应速度和并发能力，另一方面降低数据中心能耗，用绿色的数据发展绿色的经济，用绿色的经济再反哺绿色的技术，实现“数字经济”的健康循环发展。

结合我国目前全闪存数据中心发展现状，建议在十四五期间，我国分阶段按行业普及全闪存数据中心：

阶段一（2021年~2023年）：关系国计民生行业（如：政务、金融、电信、能源、交通、医疗等行业）的关键信息基础设施所在数据中心升级为全闪存数据中心，鼓励云服务提供商商普及全闪存数据中心。

阶段二（2024年~2025年）：其他行业新建及改造数据中心全面普及全闪存数据中心。

7.1.2 强化基础软件技术自主创新能力

数据基础设施的基础软件应自主可控，建议积极推动软件产业自主创新，鼓励国内数据软件厂商自主研发，掌握核心软件技术，推动数据软件产业高质量、安全发展。

软件系统性安全应经过可信设计和验证，以确保数据基础设施的安全可靠，排除安全隐患，特别是类似超算中心、人工智能中心等国之重器的基础软件系统，更应该确保高可靠、自主创新，建议国家建立软件安全可信标准的认证实验室，确保系统软件安全可信。

7.1.3 促进数据产业绿色节能、高效发展

绿色节能是国家战略发展方向，政府应加快整合数据相关全产业链基础设施，以PUE、WUE、机架利用率等指标为牵引，统一节能目标，制定节能措施，在鼓励采用风能、光能等绿色新能源的同时，还要采用高效节能的产品和技术。

数据中心、人工智能中心、超算中心等数据基础设施是耗能大户，2019年全国数据中心耗电量达1608亿度，超过三峡+葛洲坝总发电量，也超过了整个上海市全年用电量，应加快绿色节能转变进程，鼓励采用半导体闪存介质。半导体全闪存能耗仅为机械硬盘1/3，加快全闪存、高密度等高效、节能技术的发展和应用，可以有效实现绿色节能，确保数据能源安全，助力3060碳达峰、碳中和的社会整体目标。

7.1.4 提升数据在产业应用中的价值变现能力，促进数据安全流通与治理

当前各国纷纷从国家安全和产业应用角度，意识到数据作为生产要素和国家资源的重要性。对企业而言，虽然大数据业务场景众多，但尚未充分释放出应有的商业价值，数据变现能力亟待提升。

一要厘清自身拥有数据资源的价值。以电信运营商为例，一类是与用户行为息息相关的数据信息，包括用户浏览网页、网购等行为产生的数据等；另一类是在物联网场景下产生的数据，比如传感器收集的气候、污染数据、资产货运的跟踪数据等，也包括与智慧穿戴设备的大数据，如人体健康、生活习惯或运动等方面的数据。这些数据既是提升大数据变现能力的基础，也是其大数据变现的关键所在。

二要树立生态意识，推进数据产业发展。要实现海量数据更好地发挥价值，生态合作变得至关重要。企业要依托对自有数据、安全能力以及对开放运营的支撑，致力于让生态圈的。完善数据安全防护体系，通过对数据资产要素进行分类和分级保护，并通过更多合作伙伴一起做创新应用，将不同来源的数据进行整合、叠加，引入多维度智能分析，真正发挥大数据的商业价值。

三要重点防范数据安全风险，切实做好数据安全数据梳理、数据血缘分析、数据流转和跨境数据监测、权限控制、数据保护、安全审计、追踪溯源等综合技术保障。持续提升我国数据生产要素的全生命周期安全水平，使数据的全生命周期管理融入安全基因。关系国家民生、经济、文化等领域的企事业单位，应参与提升保障数据安全能力，助力关键信息基础设施和数据资产的安全建设中。

7.2 加快数据安全防护技术研究与应用

7.2.1 强化数据安全领域关键基础技术的研究与应用

建议政府、科研、产业、学术、行业应用等政产学研用把数据产业作为基础性和战略性产业。围绕数据全生命周期，构筑技术领先的、自主创新的数据基座，并坚持数据产业向安全可靠、绿色节能等方向发展，确保数据产业关键技术的可获得。

- 在芯片、操作系统、人工智能等方面，培养头部企业，推动在各行业和场景中广泛应用，形成良性的产业循环，最终从国家输血转变为造血。
- 加强密码技术基础研究，积极开展商用密码技术创新，促进密码技术的成果转化，缩小商用密码技术与国际先进密码技术（比如后量子密码）之间的技术差距。

7.2.2 重视核心业务数据的安全保护，确保数据高可靠、高可用

建议优化和提升《 GB/T 20988—2007 信息安全技术 信息系统灾难恢复规范》标准，对于关系到国计民生的核心业务，如政府机关、委办局、政务云、智慧城市、一体化大数据中心、人工智能试验区、国家实验室、省市区县公安、交警系统、金融核

参考《 GB/T 20988—2007 信息安全技术 信息系统灾难恢复规范》和《GB/T 22239-2019 信息安全技术 网络安全等级保护基础要求》，推荐采用以下灾备标准建设：

- 核心关键业务系统：从网络层、应用层、计算层和存储层等构建高可用能力，任一层故障的情况下，保证核心业务的同城或本地业务极致连续性，满足RPO=0、RTO<15min。同时可以支持扩展构建异地灾备中心，在发生区域灾难时，通过异地灾备中心恢复核心关键业务。
- 要业务系统：构建存储层高可用能力，保证重要业务数据零丢失。同时可以支持扩展构建异地灾备中心，在发生区域灾难时，通过异地灾备中心恢复重要业务。
- 普通业务系统：支持扩展构建异地灾备中心，在发生区域灾难时，通过异地灾备中心恢复重要业务。
- 所有业务系统均建设本地备份系统，核心关键业务数据归档做长期留存，同时核心关键和重要业务系统的备份数据可扩展复制到异地灾备中心。

7.2.3 培养储备高素质数据安全人才队伍

根据数据统计显示，未来十年我国信息安全人才总需求量为140万人，而当前仅仅有3万毕业生，人才缺口高达 98%，比如数据新介质领域、人工智能领域、密码学领域等，人才数量与质量、结构比例与市场需求不匹配。

针对数据产业人才总量缺口大，地域和行业分布差异大等问题，建议进一步完善数据产业人才培养机制。一是研究制定数据产业人才体系的发展规划，建立多层次、多元化的人才培养目标。二是鼓励高等院校科学设置课程体系，注重学科间的交叉融合，鼓励跨学科选修数据类课程，探索与产业机构建立联合培养机制，培养兼具专业理论与行业知识的复合型人才。三是进一步推动人事制度改革，鼓励地方政府引导企业完善人才激励机制，通过优化工资待遇、设置奖励基金等方式引进和留住高端专业人才，优化人才的地域和行业布局。四是鼓励地方政府、数据产业龙头企业、各行业协会搭建平台开展社会化培训，组织跨机构之间的人才交流机制，探索建立人才储备机制。

7.3 强化法律法规在数据安全主权方面的支撑保障作用

未来通过“三驾马车”的模式，从网络空间层面、个人数据层面和数据本身层面构建数据安全治理的基本制度框架。随着相关制度的逐步建立，从科学立法的角度需要关注以下几个方面的问题，保障法律法规的有效支撑。

首先，在立法层面，厘清“数据”“个人信息”“网络数据”等基本概念，并构建清晰关系是建立有效支撑的基础。在具体实践中，各部法律所涵盖的范围可能出现部分重叠，例如个人数据跨境，《数据安全法》《网络安全法》《个人信息保护法》都有相关规定，明确何种场景适用哪一部法律将对各种数据处理活动产生重大影响。

其次，在促进层面，除了《数据安全法》提出促进数字经济发展的大政方针外，还需要其他民事、商事法律的配套推进。如需要在《民法》层面厘清数字交易相关的法律关系。在《反不正当竞争法》《反垄断法》需对数据垄断等问题进行治理。在安全层面，相关的管制和管理措施的界限也需要进一步明确，例如在《数据安全法》中明确相关司法协助的要求后，是否会对我国企业“走出去”参与国际竞争产生影响，是否会引起对于侵犯个人权利的担忧。

再次，针对数据安全相关法律法规所引入的如数据分级分类制度、境外执法机关调取境内数据的报告制度、部分数据出口管制制度、外国歧视性措施的反制措施等制度，需要进一步细化相关制度和联动机制。建立一个统一的协调统筹机构，对相关制度进行统筹管理和执行。《数据安全法（草案）》第六条规定了“中央国家安全领导机构负责数据安全工作的决策和统筹协调”，因此相关部门的尽快建立相关举措细则，是在未来《数据安全法》颁布后亟需解决的问题。

最后，标准和指南作为法律法规和具体实践的重要桥梁，有望解决前述的基本概念厘清、配套制度建立以及相关举措细则确定等问题。在安全标准层面，通用的数据安全治理要求、个人信息保护相关标准已基本完备，但在一些数据安全关键治理环节、关键业务场景、关键网络产品和服务还有待进一步细化规范，提出数据安全实施指南或提出数据安全评价指标。例如，对网络存储设备提出相应的数据可靠性、可用性、保密性方面的数据安全评价指标，对云服务数据安全提出安全要求或实施指南。在具体产业政策的层面，鼓励相关产业政策的出台也有利于相关产业的发展，例如对相关数据安全基础设施产业进行扶持，推动各地政府就数据安全和可信产业项目进行实践探索，进一步推进相关数据安全法律法规落地实施，为相关行业发展树立标杆。

此外，作为践行《全球数据安全倡议》的重要内容，推动构建数据安全国际对话机制，建立全球性和区域性的数据安全合作体系，确立数据安全保护的国际标准和良好国际实践，探索数据安全全球治理和协调机制，也将有利于向世界贡献数据安全保护的中国方案。

参考文献：

编号	参考文献	出处
1	数据交易的商业模式研究报告《概要版》	上海玛娜数据科技发展基金会，2019.3
2	中国数字经济发展白皮书（2020）[R].	中国信息通信研究院, 2020
3	人工智能数据安全白皮书（2019）[R].	中国信息通信研究院, 2019
4	The Seagate Rethink Data Survey [R].	IDC, 2020
5	点亮绿色云端：中国数据中心能耗与可再生能源使用潜力研究[R].	华北电力大学, 绿色和平组织, 2019
6	中国企业存储报告[R].	IDC,2014-2019
7	Rethink_Data_Report_2020 [R].	IDC,2020
8	2018-2019 年度金融科技安全分析报告[R].	普华永道，中国信息通信研究院，平安金融安全研究院, 2019
9	Measuring the economic value of data and cross-border data flows [R].	OECD，2020
10	ISO 27001:2013 Information Security Management System [S].	ISO，2013
11	IDC中国企业存储系统追踪报告[R].	IDC, 2020
12	Gartner-Forecast Hard-Disk Drives [R].	Gartner, 2020.12
13	IDC中国企业存储系统追踪报告 [R].	IDC,2020
14	IDC 2019中国区分布式存储市场报告[R].	IDC,2019
15	Double Pulsar NSA leaked hacks in the wild	https://www.wired.com/beyond-the-beyond/2017/04/double-pulsar-nsa-leaked-hacks-wild/
16	中华人民共和国密码法	2019
17	密码标准应用指南[S].	GM/Y 5001-2020,密码行业标准化技术委员会, 2019

18	商用密码管理条例	1999
19	Exclusive: Secret contract tied NSA and security industry pioneer	https://www.reuters.com/article/us-usa-security-rsa-idUSBRE9BJ1C220131220
20	网络安全先进技术与应用发展系列报告 零信任技术（Zero Trust）（2020年）[R].	中国信通院, 2020
21	信息安全技术 信息系统灾难恢复规范 [S].	GBT 20988-2007, 全国信息安全标准化技术委员会, 2007
22	信息安全技术 网络安全等级保护基础要求[S].	GB/T 22239-2019, 全国信息安全标准化技术委员会, 2019
23	国家安全法	2015
24	网络安全法	2017
25	数据安全法（草案）	2020

国家工业信息安全发展研究中心
北京市石景山区鲁谷路35号
电话: +86 10 68636830
邮编: 100040
www.cics-cert.org.cn

华为技术有限公司
深圳龙岗区坂田华为基地
电话: +86 755 28780808
邮编: 518129
www.huawei.com