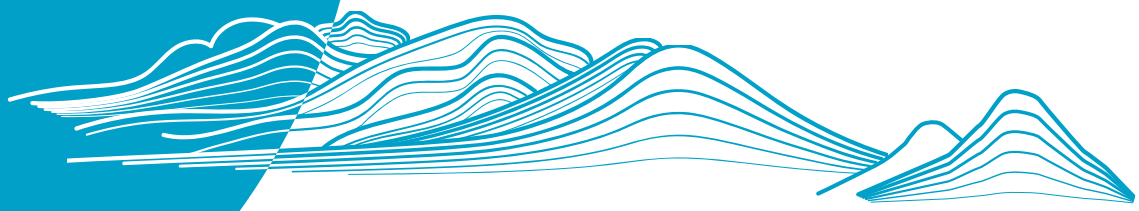
Hillstone
山石网科

数据安全治理
白皮书



www.hillstonenet.com.cn

前言

2020 年 4 月，中共中央办公厅、国务院办公厅发布《关于构建更加完善的要素市场化配置体制机制的意见》，明确表示数据成为重要生产要素。数据成为国家基础性战略资源、重要生产要素，对于推动经济高质量发展，助力国家经济体系现代化具有重要作用。

法律层面，随着《数据安全法》以及《个人信息保护法》的正式颁布及施行，企业对数据安全合规需求愈来愈强烈，企业数据安全体系建设、数据安全治理、数据安全保障的重要性不断提升。

2021 年 11 月 14 日，《网络数据安全管理条例（征求意见稿）》正式发布，落实并强化《网络安全法》、《数据安全法》和《个人信息保护法》等法律关于数据安全管理的规定，规范网络数据处理活动，保护个人、组织在网络空间的合法权益，维护国家安全和公共利益。

业务层面，企业数字化转型依托数据共享交换实现信息资源集约化、服务化和标准化供给，为现代化水平、产业升级和创新提供支撑，相互独立的业务将打破网络和安全的边界，走向融合。同时数据应用场景日益多元，整体业务环境更加开放，一方面需要防范内部人员和服务提供方被数据的价值吸引而恶意获取、处理和泄露数据，另一方面，需要防范外部访问人员恶意的数据窃取和数据破坏行为。基于以上，传统的基于边界的围栏式安全不能完全满足数据流动中的安全防护需求，企业亟需构建新的数据安全防护体系。

《数据安全治理白皮书》将与读者分享针对数字时代的数据安全问题，山石网科的思考和解决方式。

目录

Hillstone
山石网科

一、数字时代的数据战略

1.1 数字世界与数字经济背景下的数据价值

1.1.1 数字经济规模不断扩大

互联网时代的大背景下，“万物互联”成为社会经济发展的一大主题，新生技术与新生事务正影响着人们日常生活方式、工作习惯及思考模式。在信息化高速发展背景下，数字经济驱动着全球经济总量不断增长，全球经济数字化发展趋势愈加明显，传统产业加速向数字化、网络化、智能化转型升级，数字经济规模持续扩大。《中国互联网发展报告 2021》指出，2020 年中国数字经济规模达到 39.2 万亿元，占 GDP 比重达 38.6%，保持 9.7% 的高位增速，成为稳定经济增长的关键动力。

全球数字经济规模由 2018 年的 30.2 万亿美元扩张至 2019 年的 31.8 万亿美元，规模增长了 1.6 万亿美元，数字经济成为全球经济发展的新动能。有报告指出，“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。”

《中国互联网发展报告 2021》显示，中国数字产品化规模已经达到 7.5 万亿元，不断催生着新产品、新业态、新模式。与此同时，数字经济成为世界各国应对新冠肺炎疫情冲击、加快经济社会转型的重要选择。世界各国加快新型基础设施布局，以 5G、人工智能、物联网、工业互联网、卫星互联网为代表的新型基础设施逐步成为全球经济增长新动能。

数字经济总量增长离不开数据价值的加持，全球数据的“井喷式”生产为数据资源化奠定了基础。国际数据公司（IDC）发布的《数据时代 2025》显示，2025 年全球产生的数据将从 2018 年的 33ZB 增长到 175ZB，相当于每天产生 491EB 的数据。其中，中国数据量将增至 48.6ZB，占全球数据量的 27.8%，将成为全球最大的数据圈。规模如此之巨的存量与增量数据，势必带来巨大的数据安全风险。数字经济越发展，安全问题就越突出。在此背景下，世界各国纷纷采取行动，从战略规划、政策制定、立法执法等多个维度入手，形成了各具特色的治理理念和治理方案，对于完善我国数据安全治理体系、打造网络空间命运共同体具有重要借鉴意义。

1.1.2 数据成为新型生产要素

2019 年，党的十九届四中全会首次增列数据作为生产要素，2020 年 4 月 9 日，《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》（下称《意见》）正式公布。《意见》提出了土地、劳动力、资本、技术、数据五个要素领域改革的方向，提出加快培育数据要素市场。这是中央第一份关于要素市场化配置的文件，而数据作为一种新型生产要素也是首次正式出现在官方文件中。将数据增列为生产要素，有助于将我国超大规模数据和超大规模市场的优势双重叠加，抢抓数字经济全球竞争新赛

道优先权。

“数据”成为新生产要素，与劳动、资本、技术、土地一起构成新经济范式，全球从工业经济时代迈入数字经济时代。重视和利用数据要素的价值，已经成为社会各界的广泛共识和世界各国的重大战略抉择。数据要素市场是将尚未完全由市场配置的数据要素转向由市场配置的动态过程，目的是形成以市场为根本调配机制，实现数据流动的价值或数据在流动中产生价值。党中央、国务院高度重视数据要素市场的培育。2020 年 12 月，国家发展改革委、中央网信办、工业和信息化部、国家能源局联合发布《关于加快构建全国一体化大数据中心协同创新体系的指导意见》，指出以深化数据要素市场化配置改革为核心，加快构建全国一体化大数据中心协同创新体系。未来，从数据规模和量级看，一体化大数据中心所处理数据将是巨量的，其作为支撑数据流通与交易的基础设施，对我国构建全球领先的超大规模数据市场将起到重要支撑与推动作用。

1.2 国际数据战略现状

当前数据技术的应用与创新主要集中在欧美发达国家，大数据正逐渐引起公众意识形态的变革，甚至社会结构的深层调整，受到世界各主要国家和地区的广泛关注，纷纷从国家层面提出具体的数据发展战略。由于大数据技术应用发展迅速，随着存储设备、记录工具和分析技术的不断发展，其应用的深度与影响力也日新月异，各国大数据战略也是基于国家整体发展趋势进行布局。近期受疫情影响，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。

为了应对信息技术时代在数据方面的发展和挑战，近期美国和欧盟相继出台数据战略，探索未来数据发展之路。2019 年 12 月 23 日，美国白宫行政管理和预算办公室 (OMB) 发布《联邦数据战略与 2020 年行动计划》，以政府数据治理为主要视角，描述了联邦政府未来 10 年的数据愿景和 2020 年需要采取的关键行动。2020 年 2 月 19 日，欧盟委员会公布了《欧盟数据战略》，以数字经济发展为主要视角，概述了欧盟委员会在数据方面的核心政策措施及未来 5 年的投资计划，以助力数字经济发展。

图 重点国家或地区数据安全战略规划情况值

1.2.1 美国数据战略

美国政府长期秉持数据开放和数据自由流动相结合的数据治理理念。近年来，美国相继发布多份数据战略纲领性文件，初步建立了数据战略体系。美国数据战略的形成基于多方面因素，包括中美战略博弈外部环境的变化、保护关键数据的长期考量、提升高科技研发能力以及对私营部门的管理和规制等。美国数据战略内容丰富，主要涵盖数据的使用管理、规则和标准以及数据伦理等。美国在推行数据战略过程中，将面临诸多挑战。

美国是较早尝试对数字数据进行治理的国家，但政府并未出台成文的数据管理战略。随着国际环境的变化及对网络安全政策理念的调整，美国战略界逐步意识到数据在维护国家安全和国际竞争力方面的重要性，开始强化对数据使用和流动的规制。

美国政府围绕信息公开、个人隐私保护、信息安全、数据开放等数据问题颁布了大批法律法规和行政命令，1974 年《隐私法》、1967 年《信息自由法》、1967 年《信息自由法》、1976 年《阳光政府法》、1980 年《文书消减法》、OMB 备忘录《开放数据政策》、2002 年《电子政务法》，2012 年 3 月美国联邦政府推出《大数据研究和发展倡议》，同年 5 月，奥巴马政府发布了“构建 21 世纪数字政府”战略规划，通过 Data．gov 平台的建设吸引更多参与者加入，同时以行政管理和预算局牵头推进政府自身的公共数据开放。

2019 年 12 月，美国总统行政管理和预算办公室发布《联邦数据战略》(Federal DataStrategy，FDS)，同时发布的还有推进这一战略的《2020 年行动指南》，这是美国首次从联邦政府层面搭建数据治理方案的尝试。此后，包括美国国防部、情报部门及其他利益相关部门先后发布了各自的数据战略方案，以响应联邦政府的数据战略总体部署，这一战略体系的发展对美国数字经济与网络安全产生深远的影响。它以 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 9 月，美国国防部发布了《国防部数据战略》(DoD Data Strategy)，该战略要求包括国防部部长办公室、参谋长联席会议主席办公室、各军种以及联合作战司令部等军事部门应重视数据流通与数据安全，将国防部逐渐打造成“由数据驱动的机构”。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。

凭借这些战略规划，美国政府力图规范各部门使用和管理数据的方式。在上述已出台的数据战略中，既包括各机构数据治理制度化的细则，也提供了与其他部门相配合的具体方案。此外，美国主张对数据战略及时更新年度行动计划，按不同时间段对数据运用的侧重方面进行部署和调整。如果这一数据战略构想能够顺利推行，将在很大程度上降低美国政府在数据管理方面的行政成本。

美国政府已经充分认识到数字数据与信息所蕴含的经济、安全与科技价值，并将其视为重要的战略资源。为了争取在新一轮全球数据竞争中的优势地位，美国联邦先后出台了多项数据战略，美国的数据战略体系已初步形成。出台数据战略是美国政府对当前国际格局出现变化、中美关系发生质变以及美国数字技术相对优势不断缩小等客观局势的回应，体现了美国强化国内数据治理、掌控国际数据战略主导权的政策意图。在当前的国际政治环境下，如果美国数据战略仍将其政治和经济利益作为核心，并通过意识形态因素和零和博弈的政策手段予以强行推动，势必进一步加剧世界各国在数字领域的对抗。

1.2.2 欧盟数据战略

作为一个政治共同体，欧盟制定大数据战略的出发点与一般实体国家存在区别，其更强调技术导向的数据共享，消除成员国家间的信息屏障。2010 年 11 月欧盟通信委员会向欧洲议会提交了题为“开放数据：创新、增长和透明治理的引擎”的研究报告，围绕开放数据制定大数据相关战略，于 2011 年 11 月被欧盟数字议程采纳，作为“欧盟开放数据战略”部署实施。其核心在于促进成员国政府拥有的公共数据的开放度与透明度，通过数据处理、共享平台与科研数据基础设施建设，向全社会开放欧盟公共管理部门的所有信息，实现“泛欧门户”的成员国无障碍信息共享。

欧盟的战略目标是确保欧盟成为数据驱动型社会的榜样和领导者，以便商业和公共部门能利用数据更好地进行决策。为了实现

这一目标，欧盟必须在数据保护、公民基本权利、安全和网络安全等方面构建完善的法律框架，并建立欧盟内部市场，汇聚各种规模和不同行业基础的有竞争力的公司。为了在数据经济中跻身世界领先地位，欧盟必须立即有所行动，通过跟各成员国协商的方式，有效解决互联互通、数据存储、数据处理、计算能力和网络安全等一系列问题。此外，欧盟还必须进一步完善治理架构用于处理数据，并增加可供使用和重用的高质量数据库的数量。

2018 年 5 月，发布《通用数据保护条例》（General Data Protection Regulation，简称 GDPR），明确了个人数据的定义及适用范围，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。在数据保护方面，GDPR 是全球众多国家、地区制定数据保护条例的重要参考。

为应对未来发展，欧盟致力于平衡数据流动和广泛使用，希望通过建立单一的数据市场，确保欧洲在未来的数据经济中占据领先地位。在此背景，2020 年 2 月 19 日，欧盟委员会发布《欧洲数据战略》，全文包括背景介绍、关键点、愿景、问题、战略、国际路径、结论以及附录（欧洲战略部门和公共利益领域公共数据空间创建计划）等八个部分。主要内容为：一是指出欧盟具有发展数字经济的各项条件，二是对欧盟数据发展提出了明确的愿景目标，三是与欧盟其他战略措施一以贯之，四是通过各项重要举措推动战略落地实施。

1.3 国内数据战略现状

《经济学人》杂志曾提说，“数据之于 21 世纪，就像石油之于 20 世纪：它是发展和改变的动力”，正如 20 世纪围绕石油所爆发数次战争一样，《经济学人》预言，“未来，很多战争将围绕谁应该拥有数据和从数据中获利展开”。随着世界的数字化转型，人们日益意识到：以数据为关键生产要素的数字经济已不再是一种经济门类，它就是“经济”本身。数据由此成为各国博弈的新领域。2020 年见证了全球数据博弈的波诡云谲，从欧美之间“隐私盾”协议被欧洲法院判定无效到 TikTok 以数据安全为由被强令出售，再到美国“清洁网络”计划，可谓一夕数变，中国要对这些变数做足准备。

美欧的战略中都提到，全球各国均在迅速革新技术，争取在国家安全和国际竞争中的数据资源优势。美国数据空间的组织由私营部门负责，具有可观的集中效应。欧盟在个人数据保护问题上率先迈进，但各成员国之间的碎片化问题仍待解决。中国则将政府监管与大型科技公司对海量数据的强大控制权结合在一起，然而欧盟的报告中却诟病中国的个人得不到足够的安全保障。中国在数据安全方面其实一直有着自己的优势，比如基础设施条件优越，逐步推动数据安全人才培养等。

1.3.1 国内数据战略

当数据成为新型生产要素，数字经济迎来蓬勃发展，如何全方位构筑数据安全、为数字经济保驾护航，也被提升到了国家战略的高度。数据安全并不是单方面强调数据的绝对安全，关键在于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。放眼于国外，数据潜在价值的凸显，使得各国高度重视数据并围绕数据开展战略博弈，全球数据安全形势日益严峻；着眼于国内，高价值数据泄漏、个人信息滥用情况突出，新技术迭代衍生出新的风险，针对数据的攻击、窃取、劫持、滥用等手段不断推陈出新，经济、政治、社会等各领域面临巨大潜在影响。

2017 年 12 月，中国提出“要构建以数据为关键要素的数字经济”。2018 年 4 月，习近平总书记在全国网络安全和信息化工作会议上深入阐述了网络强国战略思想。2019 年 7 月，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”，数据安全上升到国家安全战略高度。

国家战略上，“十三五”规划中明确提出了“互联网＋”行动计划，“十四五”规划强调提高发展数字经济、加快培育发展数据要素市场，应把保障数据安全放到突出位置。2021 年 7 月 12 日，工业和信息化部（以下简称“工信部”）在其官网发布了《网络安全产业高质量发展 3 年行动计划（2021—2023 年）（征求意见稿）》，强调网络安全产业作为新兴数字产业，是维护国家网络

空间安全和发展的网络安全技术、产品生产和服务活动，是建设制造强国和网络强国的基础保障。

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。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。

2021 年 6 月 10 日，第十三届全国人民代表大会常务委员会第二十九次会议通过《中华人民共和国数据安全法》，自 2021 年 9 月 1 日起施行。《数据安全法》不仅关注了与数据安全保护息息相关的重大问题，同时也阐明了数据安全与发展的关系，明确了未来数据治理的方向。一是要开展数据领域国际交流与合作，参与数据安全相关国际规则和标准的制定，促进数据跨境安全、自由流动。二是要全面加强数据开放利用，推进数据开放利用技术和安全标准体系建设，建立健全数据交易管理制度。三是要建立分类分级数据保护制度，形成集中、统一、权威的数据安全机制，建立数据安全应急处理机制、数据安全审查制度、数据安全出口管制以及根据实际情况采取数据投资贸易反制措施等。四是明确数据安全保护义务，落实数据保护责任，加强数据安全风险监测、评估等。五是国家机关政务数据要建立健全数据安全管理制度，落实数据安全保护责任，及时、准确公开政府数据，构建统一、规范、互联互通、安全可控的政务数据开放平台，推动政府数据开放利用。

2021 年 8 月 21 日，全国人大常委会表决通过了《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》），这是我国首部针对个人信息保护的专门性立法．其主要亮点包括：一是明确立法依据是宪法中关于“尊重和保障人权，公民的人格尊严不受侵犯，公民的通信自由和通信秘密受法律保护”；二是进一步完善个人信息处理原则，即合法、正当、必要和诚信等，特别针对应用程序过度收集个人信息、“大数据杀熟”等做出有针对性的规范；三是完善个人信息跨境提供的规则；四是明确了敏感个人信息处理规则。

《国家安全法》、《网络安全法》、《数据安全法》以及《个人信息保护法》与其他规范形成配套组合，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。

为落实《网络安全法》、《数据安全法》、《个人信息保护法》等法律关于数据安全管理的规定，2021 年 11 月 14 日国家互联网信息办公室公布《网络数据安全管理条例（征求意见稿）》，条例意见稿分 9 章 75 条，条例除总则、法律责任和附则三章外，对一般义务、个人信息安全、重要数据安全、网络平台要求、数据跨境安全、监督管理责任机制等做了更进一步的说明。

数据安全法作为顶层设计，它确立了数据安全与利用的双重目标，但是，不论是“安全与利用”，还是“安全与自由”都存在难以化约的冲突，试图完美实现“既要又要”必然是不可能完成的任务，唯一可行的只有动态均衡一途。尽管我国数字经济的成就为世人瞩目，但也如麦肯锡《数字中国：为经济带来全球竞争力》报告所阐述，美国的数字化水平仍比我国高出 4.9 倍，我们还有很长的路要走。

同时中国积极参与区域性协议，作为数据经济大国和经济全球化的坚定主张者，中国在全球数据博弈中正经历着“攻守易型”的伟大转变，有责任也有能力通过全球数据规则，为全球数据博弈定规立制。基于此，中国积极开展国际交流与合作，参与数据安全相关国际规则和标准的制定。

1.3.2 中国数据安全律法体系

2015 年 7 月 1 日，我国正式颁布《国家安全法》，其中提出要“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”。2017 年 12 月，中共中央政治局就实施大数据战略的学习中，习近平总书记强调：大数据发展日新月异，我们应该审时度势、精心谋划、超前布局、力争主动，深入了解大数据发展现状和趋势及其对经济社会发展的影响，分析现在的成绩与问题，推动实施大数据战略，加快完善数字基础设施，推动资源整合与共享，保障数据安全，加快建设数字中国。

近几年，国家陆续出台相关法律政策，统筹发展和安全，推动数据安全建设，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》明确要求加强数据安全，《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》明确提出：保障国家数据安全，加强个人信息保护。随着《国家安全法》《网络安全法》《密码法》《民法典》《数据安全法》《个人信息保护法》“五法一典”出台，我国数据安全法制化建设不断推进，监管体系不断完善，安全由“或有”变“刚需”。结合顶层设计、法律法规，数据安全新监管同时体现对过程和结果的合规要求。数据处理者既应当从过程方面积极履行数据安全保护义务，也要对数据安全防护的最终结果负责。

《网络安全法》

《网络安全法》是我国第一部全面规范网络空间安全管理方面问题的基础性法律，是我国网络空间法治建设的重要里程碑，是依法治网、化解网络风险的法律重器，是让互联网在法治轨道上健康运行的重要保障。

《网络安全法第 10 条将数据安全目标明确为“维护网络数据的完整性、保密性和可用性”；第 21 条规定网络运营者（包括关键信息基础设施的运营者）的安全保护义务，明确提出要按照安全等级保护的制度“采取数据分类、重要数据备份和加密等措施，防止网络数据泄露或者被窃取、篡改；第 27 条则是要求任何人不得提供专门用于窃取网络数据的程序和工具；第 31 条从数据泄露可能造成的危害角度界定了关键信息基础设施的范围；第 34 条则提到关键信息基础设施的运营者还应当对重要系统和数据库进行容灾备份，同时制定网络安全事件应急预案，并定期组织演练。

个人信息保护方面，第 40 条明确将收集和使用个人信息的网络运营者，设定为个人信息保护的责任主体；第 41 条增加了对个人信息收集的“最少够用原则”；第 42 条增设了进行个人信息共享的条件；第 43 条增加了个人在一定情形下删除或更正其个人数据的权利；第 44 条在法律层面首次给予个人信息交易一定的合法空间。

在重要数据保护方面，第 51 条规定“国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作 "；第 52 条规定“负责关键信息基础设施安全保护工作的部门”，应当按照规定报送网络安全监测预警信息。

《数据安全法》

2021 年 6 月 10 日，十三届全国人大常委会第二十九次会议通过了数据安全法。这部法律是数据领域的基础性法律，也是国家安全领域的一部重要法律，将于 2021 年 9 月 1 日起施行。随着《数据安全法》的出台，我国在网络与信息安全领域的法律法规体系得到了进一步的完善。按照总体国家安全观的要求，《数据安全法》明确数据安全主管机构的监管职责，建立健全数据安全协同治理体系，提高数据安全保障能力，促进数据出境安全和自由流动，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益，让数据安全有法可依、有章可循，为数字化经济的安全健康发展提供了有力支撑。

《数据安全法》从各个方面提供了数据安全治理的指导思路，一是坚持以数据开发利用和产业发展促进数据安全，坚持维护数据安全与促进数据开发利用并重，互相促进。《数据安全法》的正式实施将为我国在国际数据经济市场中提供坚实有力的保障。

二是深化数据安全体制建设，在大数据时代背景下，政务、社会、城市数字化转型快速发展，依据本法建立数据安全管理制度，明确数据责任主体，从统一化及可落地性出发，结合现有数据业务建设需求和建设情况，遵从整体策略方针，全面优化管理体制，为我国数字化转型的健康发展提供法治保障，为构建智慧城市、数字政务、数字社会提供法律依据。

三是强化数据安全监管制约，《数据安全法》明确了数据管理者和运营者的数据保护责任，指明了数据保护的工作方向，对整个信息安全产业都带来了积极的影响，全面消除数据管理者和运营者在数据安全建设中的盲区，数据安全建设有法可依，数据安全事故造成的损失有法可惩，这对促进经济社会信息化健康发展，保护公民、组织的合法权益具有非常大的价值。

四是深度覆盖的全场景数据安全评估与防护要求，《数据安全法》特别指出“关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度”，提出对数据全生命周期各环节的安全保护义务，加强风险监测与身份核验，结合业务需求，从数据分级分类到风险评估、身份鉴权到访问控制、行为预测到追踪溯源、应急响应到事件处置，全面建设有效防护机制，保障数字产业蓬勃健康发展。

五是加大政务数据开放共享中的安全机制，《数据安全法》针对政务数据开发利用做出了明确的指示，要求省级以上人民政府

应当将数字经济发展纳入本级国民经济和社会发展规划，加强数据开放共享的安全保障措施，建立统一规范、互联互通、安全可控的机制，利用数据安全运营，提升数据服务对经济社会稳定发展的效果。

六是加大违法的处罚力度，《数据安全法》对数据安全违法行为赋予了多项处罚说明，对违反国家核心数据管理制度，危害国家主权、安全和发展利益的，由有关主管部门处二百万元以上一千万元以下罚款，并根据情况责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；构成犯罪的，依法追究刑事责任。

《个人信息保护法》

2021 年 11 月 1 日，《个人信息保护法》正式实施。它是我国第一部专门针对个人信息保护的法律。该法明确了个人信息的定义和处理规则，对个人和信息处理者双方的权利义务进行了细化，并建立了个人信息保护投诉、举报工作机制，全面系统地回应了关于个人信息安全的热点问题，堪称一把保护个人信息的“安全锁”。

首先，《个人信息保护法》确立了个人信息处理活动基本原则，个人信息保护法包括合法、正当、必要、诚信、目的限制、最小必要、质量、责任等原则。这些原则的根本目的就是要规范个人信息处理者的处理活动，保护个人信息权益。例如，依据第六条所确立的目的限制原则，处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。无论什么样的个人信息处理者为了何种处理目的，以何种方式实施个人信息处理活动，都应当遵循这些基本原则。

其次,《个人信息保护法》详细规定了告知同意规则,明确个人信息处理者处理个人信息前,必须以显著方式、清晰易懂的语言真实、准确、完整地向个人告知法律规定的事项,除非法律、行政法规规定应当保密或者不需要告知,或者告知将妨碍国家机关履行法定职责。如果个人信息处理者基于个人同意而处理个人信息，那么个人的同意必须是个人在充分知情的前提下自愿、明确地作出，个人信息处理者不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务。

同时，《个人信息保护法》对“大数据杀熟”“人脸识别”等问题予以回应，界定敏感个人信息并给予严格保护，专章规定个人在个人信息处理活动中的权利，对个人信息处理者的义务作出详细规定，明确违法行为处罚规定，规定民事责任制度以及民事公益诉讼。

《网络数据安全管理条例（征求意见稿）》

2021 年 11 月 14 日，国家互联网信息办公室（“网信办”）首次公布了《网络数据安全管理条例（征求意见稿）》（以下简称《条例》），并向社会公开征求意见。条例征求意见稿以《个人信息保护法》、《数据安全法》和《网络安全法》等法律为上位法，落实法律中提出的数据安全制度，执行上位法设立的制度，给出了这些制度的实施路径。进一步细化上位法的原则，对“合法、正当、必要”原则、告知事项、同意制度、数据出境这些关于个人信息和重要数据保护的规定做了细化。

《个人信息保护法》、《数据安全法》和《网络安全法》等法律法规之间相互关联，相互支持，强调了不同的安全防护点，但在具体落地和实践上，却都留有一定空白。值得关注的是，正是这一空白的存在，推动了《条例》的出台，为法律法规的具体落地提供了最佳实践方向与路径。

与以往网安行业相关政策法规内容不同的是，在《条例》中，明确对数据采取分类分级保护制度，数据分为一般数据、重要数据、核心数据等三个级别，不同级别的数据采取不同的保护措施。《条例》对重要数据的具体解释与定义，以及明确了如何对数据要素中的重要数据进行管理等内容也成为此次意见稿中值得关注的关键内容。

《条例》共有 9 章 75 条，很多条款是为了执行上位法设立的制度，给出了这些制度的实施路径，值得关注的是总则中对数据分类分级有专门的提及。按照惯例，《条例》首先对适用范围和基本定义做出明确，然后对监管部门及其职责、数据安全制度建设（包括分类分级保护制度、数据交易管理制度、数据安全管理制度、数据安全应急响应机制、安全审计制度等等）做出指示。

关于数据处理者，《条例》提出了总体要求、处理个人信息特别要求、处理个人信息强制性要求、处理重要数据的特别要求、处理跨境数据的特别要求等要求。对于网络数据的载体平台，尤其是互联网平台，《条例》提出了更多的义务。

《条例》作为三个数据安全相关上位法的具体落地条例，对数据安全来说有着重要意义，如果说《数据安全法》是为数据安全指明了目标，那《条例》则是告诉我们如何迈出第一步并为我们做了安全导航。

二、数据安全现状

随着 5G、大数据、云计算蓬勃发展，数据安全的重要性逐渐被政府、企业所认知。数字化进程的加速，也令企业面临更加复杂多样的网络安全、数据安全风险。同时，网络安全、数据安全建设落后于企业技术转型，也带来了沉重的代价。很多企业由于疏漏或行动紧迫性而未将网络安全、数字安全纳入决策流程，导致新的漏洞进入快速变化的环境，并持续威胁当下的企业。

近期随着《数据安全法》、《个人信息保护法》相继实施，信息安全从“互联网大蛮荒时代”“网安法时代”走向“大合规时代”。某咨询机构认为，“互联网大蛮荒时代”缺乏个人信息保护机制，个人信息保护工作基本等同于写一份隐私协议；而“网安法时代”为打补丁式合规；而“大合规时代”是将个人信息保护与数据安全融入企业文化、业务，视数据合规为企业竞争力，全面进行自上而下的治理。

2.1 数据安全面临的挑战

2.1.1 数据作为生产核心要素，泄露风险加剧

数字经济时代数据已成为发展的核心生产要素，是重要资产和基础战略资源。数据安全风险与日俱增，数据泄露、数据贩卖等数据安全事件频发，近些年，除电子商务、社交等领域的用户数据发生大规模泄漏之外，政务、医疗及生物识别信息等敏感数据，逐渐成为了数据泄露的重灾区。此外具有政治背景的境外黑客逐渐加大对我国关键信息基础设施攻击力度，试图获取我国机密重要数据，为个人隐私、企业商业秘密、国家重要情报等带来了严重的安全隐患。

2.1.2 互联网平台企业滥用个人信息

随着数据安全内涵的延伸和扩大，对数据合法合规地收集使用也成为了数据安全的重要组成。当前，由于互联网平台企业的业务大都由数据驱动，商业推广、精准营销、产品迭代等均依赖对数据的海量收集和开发利用，数据成为了平台企业发展和盈利的核心引擎。基于数据收集使用创新商业营收模式，实现利益最大化，成为了各个平台企业追逐的商业目标，由此也引发了个人信息滥采滥用程度加重、数据垄断乱象频发的数据安全风险。例如，移动应用强制授权、过度索权等问题严重，用户个人信息自主权丧失；

基于数据垄断优势进行“二选一”、“大数据杀熟”等，侵犯消费者权益。

2.1.3 数据跨境流动带来国家安全隐患

在大国博弈持续加剧的今天，数据作为国家重要的生产要素和战略资源，数据的跨境流动是数据价值发挥的关键，它不仅是跨国贸易和投资的重要载体，还是重要的跨国流通的商品。在 2005 到 2015 年的十年间，跨境数据流动使全球国内生产总值增长了约 10%，数据流所产生的附加值估计为 2.8 万亿美元，已经超过了货物贸易的贡献。Goldfarb 和 Tucker 已通过实证研究证明：数据跨境流动管控对经济全球化造成不利影响。2019 年，世行在其发布的《东亚数字经济创新：限制性数字政策重要吗？》报告中，梳理了东亚 15 国的数字经济法律政策，并使用定量研究的方法得出“数字限制指数”，直观展现出数据跨境管控与企业创新之间的负相关关系。我国改革开放的经验表明，经济全球化和自由贸易是全球发展繁荣的基石。正如李克强总理所言，在逆全球化的浪潮中，中国仍将坚定支持经济全球化，促进全球贸易和投资自由化便利化。

另一方面新技术新应用在极大促进生产力发展和为人民生活提供便利同时，也带来了安全方面的不确定性。以人脸识别技术为例，我国具有丰富的数据资源，且相较国外文化更易收集人脸数据，因此一旦我国独特的数据资源被他国获取，国外数据资源相对匮乏的短板会被迅速填补，从而实现反超，削弱我国的竞争优势。基于此，在数据“安全与自由流动”中，应避免日益频繁的跨境流动带来的潜在的国家安全隐患。

2.3 数据安全治理面临的困难

2.3.2 企业数据安全管理制度不完善

很多企业在进行数据安全治理时，注意力更多的集中在对外管理上，造成了“对外铁桶一块，对内千疮百孔”。数据安全管理要解决的最突出的问题之一就是敏感数据的泄露，但造成数据泄露的原因很多情况下都是由于企业内部人员导致的。比如，企业内部人员权限过高导致违规访问、内部人员绕开企业内容安全管控建设，直接登录系统进而窃取信息等。对企业员工内控的忽视是造成安全风险的重要原因。因此数据安全管理要落实到每一个参与数据安全执行的执行层面之上，甚至相关数据也会流转到最底层的员工身上。除了有管理之外，还应形成数据安全意识和数据安全防范的惯性，通过不断培训、学习、成长，最后让每一个人参与到发现、报告、初步处理、监督、改进数据安全事件中来，形成人人参与业务与安全的文化与局面。

2.3.3 数据权属争议大，管理责任不清

目前国家施行的法律法规通常都会要求明确数据责任，通过加大惩罚力度，来提升数据安全防范意识，规避“数据资产无人管、数据资产随意用”的现象，数据资产责任不清主要体现在如下两个方面：

一是数据资产未认责，数据资产体量大，且使用复杂，贯穿整个业务流程，涉及多个部门和岗位的人员，数据的所有权，使用权，安全责任等无法清晰划分；同一资产涉及多个部门或团队使用，且使用频率和重要性无法量化，导致资产认责工作无法开展；

二是管理角色的职责边界模糊，数据安全管理角色包括数据资产管理员、数据库管理员、安全审计员、安全 检测工程师、数据运维工程师、权限管理员等，一般情况下这些角色可能会由研发、运维、安全、运营人员来兼任，没有独立的团队或虚拟团队，导致权责不清，不利于整体提升数据安全防护能力。另外，一旦发生数据安全事件，很难开展追踪溯源工作。

2.3.3 数据安全技术措施零散

一是数据安全产品功能分散，现有的数据安全产品，大多都是单一数据安全功能，如：脱敏，加密，防泄密，企业部署了很多数据安全类产品，再加之企业数据分布也相对分散，导致各网络区域各数据安全产品间无法形成有效联动和整合机制，导致数据安

全管控能力分散，无法形成统一数据安全管控体系。

二是数据安全能力孤岛，由于组织内部的应用会按照部门划分，数据安全能力的建设也会以部门为单位开展，没有形成整体的防御体系，造成安全短板，容易被不法人员利用。 另外一个维度是角色和职责不明确，IT 各部门没有将安全责任进行清晰的划分，当发生数据安全事件时才考虑防护。即便是有主动建设的意愿，也是各自申请各自建设。

2.3.4 数据活动场景复杂，监管效能难提升

数据全生命周期涉及众多数据技术、数据处理主体，且数据流动范围广，从国家内部的数据流转到跨国界的数据传输，均增大了数据活动场景的复杂性，也提升了数据安全的监管难度。

一是互联网技术日新月异，实现数据安全监管全覆盖难度大。平台企业基于互联网技术进行数据的收集使用，并始终在技术和产品不断快速迭代中探索全新的数据处理模式，这对监管制度的革新速度提出了高要求。

二是数据处理环节繁杂众多，进行数据安全监管定责难度大。数据流通、应用及共享过程当中涉及众多数据处理主体，且由于数据具有低成本的复制特性，数据泄露源头往往难以确定，为数据泄露后安全事故的监管定责带来了困难。

三是跨境监管没有统一国际标准，开展数据跨境流动安全监管难度大。数据跨境流动可能导致国家关键数据资源流失，各国高度重视数据跨境流动监管这一国际性难题，但目前仍缺乏指导数据跨境流动监管的统一规范和国际规则，为我国建立数据跨境流动监管机制带来了一定挑战。

三、山石网科数据安全治理体系

十四五规划落地后，所有的企业都面临着一个相同的问题——如何安全的使用数据，创造更大的价值？那伴随而来，也就形成了企业在数据安全治理过程中的两个主要的驱动力：合规驱动以及结合自身战略的业务需求驱动。

合规驱动：在国家层面，以《网络安全法》、《数据安全法》、《个人信息保护法》为主的一系列法律法规，明确了组织在数据安全各个方面的合规要求；在各个行业层面，基于国家法律法规，以及各自行业特点，也都提出了更进一步的具体行业要求。

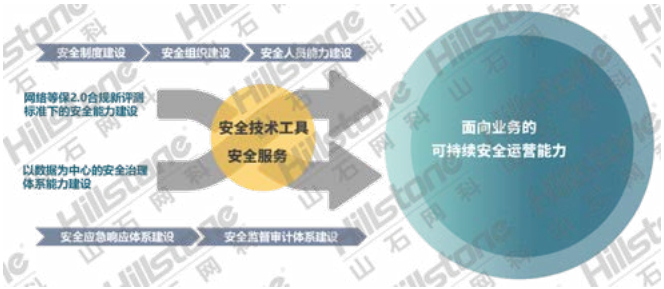
结合自身战略的业务需求驱动：伴随着数字化转型的浪潮，在人工智能、大数据、云计算、分布式计算等新型技术飞速发展的过程中，作为被定义为第五大生产要素的数据已经成为各个组织的核心资产，成为企业发展必不可少的战略性生产资料。众多企业将数据视为驱动其业务发展的创新战略资源。以企业战略和实际业务为导向，以数据为中心的安全治理，需要根据企业自身对风险的识别以及决策，做有针对性的数据安全能力体系建设。

3.1 数据安全体系建设目标

面对数据安全治理在法律法规、行业要求的合规层面，以及根据企业战略制定的数据安全治理愿景方针，结合其实际业务情况，以数据安全为中心，体系化的构建企业在其运行中需要的全面的安全能力。通过聚焦数据全生命周期，结合数据在整个企业业务中的流转状况，规划设计符合企业数据安全愿景的治理策略，不断的提升数据安全管理能力，夯实数据安全技术能力基座，依托于可持续安全运营体系，实现企业在使用数据创造价值的过程中风险可追溯。

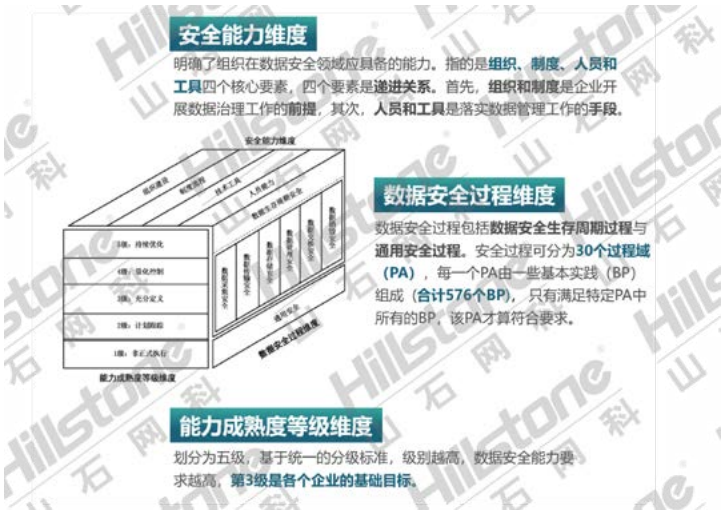
3.2 双维驱动数据安全建设

首先我们要提出山石的观点，数据安全治理永远不是从零开始的，它一定是基于企业现有的安全能力建设现状，通过以数据为中心的视角，对现有的体系进行扩展以实现对数据的安全治理管控。大多数企业在此前或多或少已有了一定的安全体系，基本上都是围绕着网络环境和信息系统开展的安全防护工作，主要聚焦在了网络安全和信息安全方面。而数据安全是以数据为中心，围绕着数据全生命周期进行建设以提高企业数据安全保障能力，所以通过企业对数据安全愿景的制定，由数据安全管理层根据企业的战略目标以及实际业务情况具体讨论建设方式。

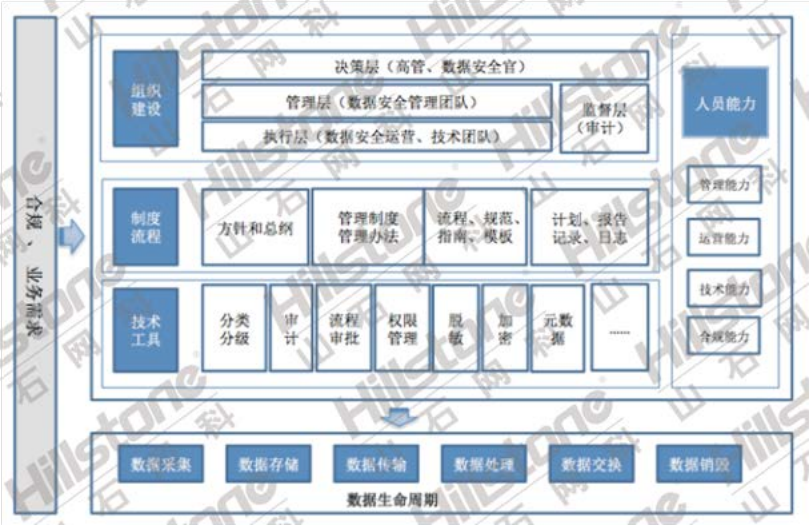


在设计整个的数据治理体系框架的过程中，山石是从两个维度进行思考。

第一个大维度是参考 DSMM（数据安全成熟度模型），对企业在数据安全建设中的所有控制点进行评估。DSMM 是一套围绕数据安全治理的能力分析模型，评估模型又包含了三个不同维度。维度一：能力成熟度等级：根据企业的战略方针、数据治理愿景，结合业务的实际情况，基于一套标准的分级方法，明确了组织在数据治理过程中各个能力域的能力建设目标。维度二：安全能力维度：从组织建设、制度流程、技术工具、人员能力四个关键能力方向，明确了在不同目标等级的前提下，组织应该具备的体系能力。维度三：数据生命周期安全：结合数据全生命周期以及通用安全过程，针对数据流转的不同阶段构建相关的安全过程域体系。



基于 DSMM（《数据安全能力成熟度模型》）标准能力的等级要求，一般数据安全能力建设的能力框架如下图所示。



第二个大维度是结合企业实际业务，根据其战略方针，更多的从场景层面出发，满足企业的数据安全目标和愿景。通过有效的数据分级分类，制定安全策略，打通技术能力基座与安全政策的对应关系，通过可持续的安全运营不断提高数据安全治理能力。

3.3 以数据为中心的安全治理体系

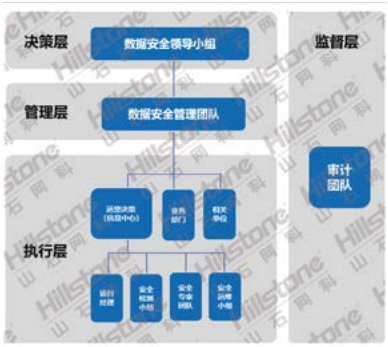
山石提出了以“制度规范体系”“技术防护体系”“运营管理体系”为核心，“监督审计体系”“应急响应体系”为支撑的数据安全治理五大体系架构。

其中通过制度规范体系建设，指引企业在技术防护体系中的构建方向，也指引着运营管理体系中的组织建设和人员能力建设的方向；同时，运营管理体系的建立也确保了制度规范体系的落地执行，和技术防护体系发挥实际作用；而技术防护体系作为关键工具，为制度规范体系和运营管理体系提供了实际的工具抓手。

3.3.1 自上而下的数据安全治理

无论是数据安全法还是关基条例，都要求数据安全治理要有专门的组织和人员负责，并定岗定责。在数据安全治理的过程中，成立专门的数据安全治理机构是首要条件。该组织结合企业的战略方针，制定符合自身的数据安全治理的政策，并落实和监督政策有效执行。

一般数据安全治理委员会会分为四个层面：决策层、管理层、执行层以及监督层。该机构一般由数据的利益相关者和专家构成，这个机构通常是一个虚拟的机构，但也可根据数据治理的战略形成一个固定组织。



数据安全治理委员会

该机构一般由数据的利益相关者和专家构成，这个机构通常是一个虚拟的机构，但也可根据数据治理的战略形成一个固定组织。

安全决策层：决策层是数据安全管理工作的决策机构，建议由数据安全负责人及其它高层管理人员组成，数据安全负责人是组织内数据安全的最终负责人。数据安全负责人应该可以参与到企业的业务发展决策，因为实际业务发展与数据安全是密不可分的关系。除数据安全负责人意外，其他管理人员对于数据安全的重视和决策也是必要的，需要有其他业务部门、研发部门、法务等高管共同组成，形成定期的例会机制，主要职责包括：

1. 制定组织的数据安全战略、愿景

2. 对数据安全的策略和规划，规章制度进行发布

3. 为企业的数据安全建设提供必要的资源支持

4. 对公司的重大数据安全事件进行协调以及决策

安全管理层：管理层是数据安全组织机构的第二层，基于组织决策层给出的策略，对数据安全实际工作制定详细方案，做好业务发展与数据安全之间的平衡。属于承上启下的部门，也是企业数据安全工作最重要的核心部门。

安全执行层：主要负责聚焦每一个数据安全场景，由信息科技部门、业务部门的数据安全接口人等、风险管理人员、数据负责人、数据安全合作伙伴（也可分为单独一层）组成。负责具体落实和执行数据安全决策。执行层与管理层是紧密配合的关系，对设定的流程进行逐个实现。

安全监督层：数据安全监督层负责定期的监督审核管理层、执行层、合作伙伴对数据安全政策的管理要求的执行情况，并向决策层进行汇报。监督层人员必须具备其独立性、做到权责清晰，不建议由其他管理层、执行层人员兼任。一般最佳实践建议由企业内部的审计部门担任。

3.3.2 制度规范体系建设

当数据安全治理委员会建立后，结合法律法规的合规要求，以及企业自身的数据安全治理愿景，首先确定公司的数据安全治理成熟度目标。在成熟度目标确定后，根据企业自身业务特点，可以参考 DSMM（数据安全成熟度模型）选定适合于本企业的安全过程域（Process Area）。针对选定的安全过程域中相关的规章制度基本实践（Basic Practice），可以得出企业自身在数据安全治理过程中的规章制度现状，以及差距分析。通过补齐、创建新制度，形成符合公司数据治理愿景的完整规章制度。

一般而言制度流程需要分层，层与层之间、同一层不同模块之间需要有关联逻辑，在内容上不能重复或矛盾。

- 一级文件：方针和总纲是面向组织层面数据安全管理的顶层方针、策略、基本原则和总的管理要求等。
- 二级文件：数据安全管理制度和办法，是指数据安全通用和各生命周期阶段中某个安全域或多个安全域的规章制度要求。
- 三级文件：数据安全各生命周期及具体某个安全域的操作流程、规范，及相应的作业指导书或指南，配套模板文件等。
- 四级文件：执行数据安全管理制度产生的相应计划、表格、报告、各种运行 / 检查记录、日志文件等，如果实现自动化，大部分可通过技术工具收集到，形成相应的量化分析结果，也是数据的一部分。

3.3.3 技术防护体系建设

通过规章制度体系建设，可以确定公司数据安全战略如何在企业落地。根据规章制度制定过程中对于安全过程域选择，可以确定在关键安全过程域中的技术需求。正如在前面描述中提出的主要观点“数据安全治理永远不是从零开始的”，企业或多或少的都已经完成了一些安全方面的建设，通过对数据安全治理的技术需求的确认，分析企业现有安全建设的基础技术能力，结合数据全生命周期以及通用安全需求，有针对性的进行技术能力补齐。

其中主要涵盖的有三个方面：

业务系统

企业的业务系统包括了前台应用、后台数据库和管理平台等。支撑数据的全生命周期（采集、存储、传输、处理、交换和销毁），几乎所有的数据安全技术工具都会对接并使用在这些业务信息系统上。

通用技术工具

通用技术工具是指绝大部分安全过程域都会使用到的技术工具，或者是数据安全管理的基础平台，或者是整合数据安全管理信息的门户网站等。比如身份和权限控制平台，所有业务系统和管理平台要进行统一控制。日志管理平台，需要采集所有业务系统和管理平台的操作日志，方便后续监控和审计。

特定阶段技术工具

针对企业战略选定的过程域适用的技术工具，只对接或者应用到部分的业务系统和管理平台。比如数据分类分级工具，对数据资产进行分类打标签。如数据安全接口管理，对数据库的接口调用进行安全管理。还比如一些数据脱敏技术，加密技术应用在了数据的存储和传输过程中。

3.3.5 运营管理体系建设

基于已经完成的规章制度体系建设，以及技术能力体系建设，根据企业数据安全治理战略选定的安全过程域，确定在组织建设以及人员能力建设方面的具体需求。

数据安全能力建设是一个系统工作，在开展组织架构的建设时，需要考虑组织层面的实体管理团队以及具体的执行团队，同时也要考虑虚拟的联动小组，其中相关业务部门、IT 部门、研发部门、HR、法务等部门都需要参与到数据安全的建设中。因为数据治理是一个自上而下的过程，数据安全管理委员会是最先建立的机构，其目的是明确数据安全的政策、落实和监督等工作，以确保数据安全能力建设的有效执行。通过完整体系建设的演进，基于选定的安全过程域，对组织建设提出了更加准确的要求，对整个数据

安全治理组织进行补全。

同时，数据安全治理也不只是一个单纯的技术类工作，更多的需要复合型工作能力，对于相关人员的能力也提出的更高的要求。数据安全人员能力主要包括了四个维度，数据安全管理能力、数据安全运营能力、数据安全技术能力和数据安全合规能力。

数据安全管理能力

目前大部分行业的企业还尚未正式开展数据安全体系建设，也较少有数据安全的专职职能岗位，对人员能力的培养也在初期。随着《数据安全法》的落地，以及企业实际业务对数据安全的需求，体系的建立与数据安全治理能力的提高成为了高优先级任务，数据安全管理能力是首要解决的问题。

数据安全运营能力

数据安全建设是一个不断持续改进的过程，需要在组织内持续性的落实数据安全的相关制度和流程，并基于组织的业务变化和技术发展不断的调整和优化，安全也是一个不断螺旋上升的过程，因此需要做好数据安全运营工作。

数据安全技术能力

数据安全的实现，需要技术和工具平台的支撑，来完成安全管控措施的构建，从而实现数据安全能力的建设。

数据安全合规能力

在数据安全领域，国内外越来越多的法律法规、标准逐步出台，合规工作成了数据安全领域建设的底线。

数据安全的人员能力建设会根据数据安全治理体系中的角色，有针对性的进行构建。对于不同角色的能力要求有侧重也有交叉。通过组织建设和人员能力的针对性构建，形成企业的安全运营能力，以保证企业数据安全治理目标的达成。同时数据安全运营能力也能反过来保障企业的规章制度落地，以及技术能力的有效使用。

3.3.6 应急响应体系建设

随着数据安全的三个核心体系建设完成，企业可以通过建设数据安全态势感知与预警平台，并与上级网络安全信息共享平台对接，构建应急预警平台。针对数据安全事件落实重大事件报告制度和突发数据安全事件应急响应制度，建立健全安全应急预案、应急处置工作指南和处置流程图。常态化开展数据安全攻防演练、应急演练、全员安全培训，组建专家队伍和支撑力量，提升全天侯、全场景、常态化、实战化的网络安全应急处置水平。

3.3.7 监督审计体系建设

企业需要针对数据全生命周期的各阶段的安全管理情况进行监控与审计，以保证数据安全治理可以有效、持续地产生价值。在监督审查体系中可以着重于以下几个方向，预警通报、安全监测和综合评价。

预警通报

通过迭代升级监测预警的技术平台，不断提升隐患时间发现的水平，提高数据安全态势感知能力。建立健全预警、通报、处置、整改、反馈闭环的工作机制，使得数据安全管理运营能力得到可持续的提高。

定期的数据安全审计和综合评估

定期开展数据安全专项审计工作，对规章制度体系，技术防范体系，以及数据安全运营体系的实际运转情况进行检查；同时要配合主管、监管部门开展重要数据处理活动审计工作，通过开放安全相关数据访问、提供技术支持等手段，对组织运作、技术系统、算法原理、数据处理等进行安全汇报，根据检查情况对企业的数据安全治理情况进行综合评估，确保数据安全运营的有效性和可持

续提升性。

四、以技术为抓手，落实体系建设

数据安全的建设，有了体系理论的指导和支撑，接下来就需要技术工具和安全服务作为抓手具体落地。数据安全技术能力与传统的网络安全能力存在重叠和区别，正如前文所说，数据安全能力需要基于现有的网络安全能力做扩展。

如何建立有效的数据安全技术防护体系，需要注意以下几点：

1. 数据需要做资产管理，包括数据 & 权限梳理、数据分类分级、形成数据资产台账或者数据资产地图；

2. 针对对全域数据类型（覆盖结构化数据和非结构化数据），提供全面的数据安全防护能力；

3. 需要对数据全生命周期各阶段进行安全防护；

4. 数据安全防护体系要基于分类分级清单做策略；

5. 数据安全防护设备需要做统一的安全管理

6. 需要关注用户行为分析和数据流向追踪；

7. 数据安全风险全景分析，对数据安全设备进行联动管控，进一步做到数据安全主动防御

综上所述，数据安全防护体系建设需要一个平台级的数据安全大脑，对数据资产进行可视化管理、对安全防护能力进行集中化管控、对安全运维 & 态势分析进行体系化建设，建立一个综合性数据安全治理平台。

数据安全能力是数据安全防护体系的基础，现阶段市场上大量的数据安全防护技术，本章对于纯数据安全部分相关能力做汇总介绍。具体如下：

4.1 数据资产管理

数据安全治理的前提是对当前资产状况有清晰的了解，只有对当前资产无缝管理，才能对数据进行全面的安全管控。通过资产梳理、敏感数据识别、数据分类分级、账号权限管控等手段，形成完整的数据资产地图。

4.1.1 数据资产梳理

资产梳理即资产的全量发现，做到资产的无缝管理。山石数据资产梳理技术能力支持多种数据自动发现，主动嗅探网内数据，可以指定 IP 段和端口的范围进行搜索自动发现与识别数据库。

明确数据的存储分布的基础上，掌握数据的业务访问情况。根据数据的业务访问情况制订针对业务系统的工作人员对敏感数据访问的权限策略和管控措施，并梳理不同的业务系统对敏感信息访问的基本特征，如访问的时间、IP、访问的次数、操作行为类型、数据操作批量行为等，在这些基本特征的基础上，完成数据管控策略的制定。

数据资产梳理需要对数据的权限进行持续扫描，获取其角色、对象等相关权限信息，直观的展示账户所拥有的权限，定位账户所拥有的高风险权限，便于对数据库账户进行管理。

4.1.2 敏感数据识别

数据资产梳理技术能力针对采集到的数据样本，基于内置规则匹配、语义算法、数据模型等技术手段，实现对个人敏感信息与重要数据的发现与定位。敏感数据识别需要对多种敏感数据对象进行发现识别，可实现如身份证号、电话号码、地址、邮箱、银行卡号、车牌号，护照号，军官证、位置信息等敏感数据的识别。此外，需支持自定义敏感对象识别规则，满足业务个性化检测需求。

4.1.3 数据分类分级

数据分类分级需要分两个步骤：数据分类和数据分级。

数据分类：从业务角度出发，在进行数据资产梳理后后，确定元数据属于相关业务范畴，按照一定的原则和方法进行区分并分类，建立一定的分类体系。业务范畴囊括的范围可大可小，是基于业务的梳理结果。

数据分级：数据分类，对于大多数组织 / 企业来说，更多是从满足监管要求的角度出发。需要按照一定的分级原则对分类后的数据进行定级，组织 / 企业中的数据有的密级程度高、有的低、有的可公开、有的不可公开，敏感等级不同的数据对内使用时受到的保护策略不同，对外共享开放的程度也不同。

4.2 数据库安全检测

数据库安全检测对访问数据库的行为、内容等进行采集、存储、分析，实现完全独立于数据库的检测审计能力，并生成合规报告，便于事故追根溯源，提高数据资产安全。对主流数据库系统的访问行为进行监控，让数据库的访问行为变得可见、可查。识别出数据库访问行为中的可疑行为并实时触发告警，及时调整数据库的访问权限进而达到安全保护的目的。直观的查看到每个数据库系统的整体运行情况，为数据库系统的调优提供有效的数据支撑。

4.3 数据备份与恢复

4.3.1 数据备份

数据备份是容灾的基础，是指为防止系统出现操作失误或系统故障导致数据丢失，而将全部或部分数据集合从应用主机的硬盘或阵列复制到其它的存储介质的过程。

数据备份包括以下备份方式：

- 定期磁带

远程磁带库、光盘库备份。即将数据传送到远程备份中心制作完整的备份磁带或光盘。

远程关键数据 + 磁带备份。采用磁带备份数据，生产机实时向备份机发送关键数据。

- 数据库

就是在与主数据库所在生产机相分离的备份机上建立主数据库的一个拷贝。

- 网络数据

这种方式是对生产系统的数据库数据和所需跟踪的重要目标文件的更新进行监控与跟踪，并将更新日志实时通过网络传送到备份系统，备份系统则根据日志对磁盘进行更新。

- 远程镜像

通过高速光纤通道线路和磁盘控制技术将镜像磁盘延伸到远离生产机的地方，镜像磁盘数据与主磁盘数据完全一致，更新方式为同步或异步。

数据备份必须要考虑到数据恢复的问题，包括采用双机热备、磁盘镜像或容错、备份磁带异地存放、关键部件冗余等多种灾难预防措施。这些措施能够在系统发生故障后进行系统恢复。但是这些措施一般只能处理计算机单点故障，对区域性、毁灭性灾难则束手无策，也不具备灾难恢复能力。

4.3.2 数据恢复

数据恢复，是指当计算机存储介质损坏，导致部分或全部数据不能访问读出时，通过一定的方法和手段将数据重新找回，使信息得以再生的技术。数据恢复技术不仅可恢复已丢失的文件，还可以恢复物理损伤的磁盘数据，以及不同操作系统的数据。数据恢复是计算机存储介质出现问题之后的一种补救措施，它既不是预防措施，也不是备份。

数据恢复包括以下分类：

1、软恢复（软件恢复）：

主要是恢复操作系统、文件系统层的数据。这种丢失主要是软件逻辑故障、病毒木马、误操作等造成的数据丢失，物理介质没有发生实质性的损坏。

2、硬恢复：主要针对硬件故障而丢失的数据，如硬盘电路板、盘体、马达、磁道、盘片等损坏或者硬盘固件系统问题等导致的系统不认盘，恢复起来一般难度较大。这时要注意不要尝试对硬盘反复加电，也就不会人为造成更大面积的划伤，这样还有可能能恢复大部分数据。

3、数据库系统或封闭系统恢复：

这部分系统往往自身就非常复杂，有自己的一套完整的保护措施，一般的数据问题都可以靠自身冗余保证数据安全。如 SQL、Oracle、Sybase 等大型数据库系统，以及 MAC、嵌入式系统、手持终端系统，仪器仪表等系统往往恢复都有较大的难度。

4、覆盖恢复：

恢复难度非常大，一般民用环境下因为需要投入的资源太大，往往得不偿失。但是在尖端的国防军事等国家统筹或者个别掌握尖端科技的硬盘厂商能做到，具体技术都涉及核心机密，无法探知。

4.4 身份鉴别

身份鉴别也称身份认证，是指对实体和其所声称的身份之间的绑定关系进行充分确认的过程，目的是为了确定该用户是否具有对某种资源的访问和使用权限，使数据访问策略安全可靠的运行。身份鉴别技术是为了防止攻击者假冒合法用户获得资源的访问权限，保证系统和数据的安全，以及授权访问者的合法利益。

目前比较流行的身份认证技术包括口令认证、双因素认证、生物特征认证等方式。

4.4.1 口令认证

口令认证是身份认证机制中最常用的技术。系统为每一个合法用户建立一个用户名 / 密码口令对，当用户登录系统或使用某项功能时，系统对用户输入的用户名、密码口令进行验证。口令密码机制无论是使用还是部署都非常简单，但从安全性上讲，用户名 / 密码方式是一种不安全的身份认证方式。

4.4.2 双因素认证

双因素认证就是将两种认证方法结合起来，进一步加强认证的安全性，使用最为广泛的双因素有：

动态口令 + 静态密码

USB KEY + 静态密码

4.4.3 生物特征认证

生物特征认证是指通过可测量的身体或行为等生物特征进行身份认证的一种技术。生物特征认证技术是目前最为方便和安全的识别技术，可以分为身体特征和行为特征两类；身体特征包括：指纹、掌型、视网膜、虹膜、人体气味、脸型、手的血管和 DNA 等；行为特征包括：签名、语音、行走步态等。

4.5 数据库访问控制

数据合规访问控制能力需要对全面的数据库通讯协议进行解析，通过 SQL 协议分析和 SQL 注入特征抽象技术，能快速有效的捕获异常行为特征，根据预定的 SQL 白名单策略决定让合法的 SQL 操作通过执行，对符合黑名单特征的可疑的非法违规操作进行阻断，从而形成一个数据库的外围防御圈 , 真正做到 SQL 危险操作的主动预防、实时审计。

4.5.1SQL 注入检测防护

SQL 注入是业务系统及数据库面临非常多的攻击风险，我们可以通过学习业务系统的 SQL 请求，在数据库层面识别 SQL 结构变化发现 SQL 注入行为，对 SQL 注入防护的一个高度互补，数据访问控制能力引擎通过对业务系统的 SQL 模板进行智能学习，并对学习干扰数据进行自动剔除，通过智能业务场景还原 web 层面的细微的 SQL 语句结构变更，并进行有效的智能业务关联分析，可以精准识别 web 层面的 SQL 注入攻击，让 SQL 注入攻击无处可藏。

4.5.2 数据库虚拟补丁加固

数据库虚拟补丁和日常了解的普通虚拟补丁又大同小异，主要是因为防护目标改变成了数据库，数据库虚拟补丁是专门针对数据库而设计的一款虚拟防护，当数据库存在漏洞没法升级的时候，黑客将很容易渗透到你的数据库并提权窃取篡改数据，如果加了一层虚拟补丁防护，将极大地提高数据业务系统的安全性。

4.5.3 拖库防护

拖库是黑客攻击业务系统的终极目标，一般可以通过根据黑客批量及遍历的大量拖库特征，对拖库行为中合法行为进行智能剔除，根据会话前后关联性及行为轨迹特征进行智能判断，智能识别拖库行为，及时阻断及时告警，阻止拖库事件发生。

4.5.4 撞库防护

撞库是因为数据库运维人员使用习惯的问题，大部分人在不同的应用上注册使用的是相同的用户名及密码，黑客成功拖库一个应用之后，使用对应的用户名和密码在其他应用进行尝试登陆的过程叫撞库，撞库又分为自动撞库和人工撞库两种方式。

一般可以通过针对撞库行为后台根据频率自动识别阻断，及时预警撞库行为，解决业务层面的极大风险威胁。

4.5.5 暴力破解防护

暴力破解分为应用系统暴力破解和数据库层暴力破解，主要是由于业务系统验证不合理和数据库配置不合理导致；

一般可以根据失败的频率及间隔进行精准的识别，从而抵御数据库暴力破解行为。

4.6 数据库漏洞检测

基于数据库漏洞攻击特征，在不误报的情况下，对漏洞特征精细化的设计，剔除可能误识别、误阻断的特征，安全检测防护绝不影响业务，避免非法人员利用已公开数据库漏洞对数据库进行攻击。

4.7 数据泄露防护

数据泄露防护（Data leakage prevention, 简称 DLP），是通过一定的技术手段，防止企业的指定数据或信息资产以违反安全策略规定的形式流出企业的一种策略。数据泄露防护根据保护的位置分为终端 DLP、网络 DLP、邮件 DLP 和存储 DLP 等。其中防护能力最强的终端 DLP 可以针对敏感数据泄露篡改等行为进行重点安全检测和防护，DLP 的基础内容识别技术包括关键字、正则表达式、指纹等为基础，结合自然语言处理、深度内容识别、机器学习等技术，以业务样本敏感数据为学习目标，通过语义相似度分析、用户行为基线分析深入了解每个数据操作的实际动作，对每个操作行为的各个特征采用快速自动建模技术，并通过内存级快速匹配算法自动智能检测违法的敏感数据泄露篡改行为，能精准智能的识别并阻断数据篡改的行为。

4.8 数据加密

数据加密技术是指一条消息通过加密密钥和加密函数转换成无意义的密文，接收者通过解密函数和解密密钥将密文还原成明文。数据加密技术可分为数据传输加密技术、数据存储加密技术、数据完整性的鉴别技术和密钥管理技术。

4.8.1 数据传输加密

数据传输加密可分为链路加密、节点加密和端到端加密。

链路加密

对于在两个网络节点间的某一次通信链路，链路加密能为网上传输的数据提供安全保证。对于链路加密（又称在线加密），所有消息在被传输之前进行加密，在每一个节点对接收到的消息进行解密，然后先使用下一个链路的密钥对消息进行加密，再进行传输。在到达目的地之前，一条消息可能要经过许多通信链路的传输。

节点加密

尽管节点加密能给网络数据提供较高的安全性，但它在操作方式上与链路加密是类似的：两者均在通信链路上为传输的消息提供安全性；都在中间节点先对消息进行解密，然后进行加密。因为要对所有传输的数据进行加密，所以加密过程对用户是透明的。

端到端加密

端到端加密允许数据在从源点到终点的传输过程中始终以密文形式存在。采用端到端加密（又称脱线加密或包加密），消息在被传输时到达终点之前不进行解密，因为消息在整个传输过程中均受到保护，所以即使有节点被损坏也不会使消息泄露。

4.8.2 数据存储加密

文件级加密

文件级加密可以在主机上实现，也可以在网络附加存储 (NAS) 这一层以嵌入式实现。对于某些应用来讲，这种加密方法也会引起性能问题在执行数据备份操作时，会带来某些局限性，对数据库进行备份时更是如此。特别是，文件级加密会导致密钥管理相当困难，从而添加了另外一层管理：需要根据文件级目录位置来识别相关密钥，并进行关联。

数据库级加密

当数据存储在数据库里面时，数据库级加密就能实现对数据字段进行加密。这种部署机制又叫列级加密，因为它是在数据库表中的列这一级来进行加密的。对于敏感数据全部放在数据库中一列或者可能两列的公司而言，数据库级加密比较经济。

由于数据库中数据的结构和组织都非常明确，因此对特定数据条目进行控制也就更加容易。用户可以对一个具体的列进行加密，如国家识别符列或工资列，而且每个列都会有自己的密钥。根据数据库用户的不同，企业可以有效地控制其密钥，因而能够控制谁有权对该数据条目进行解密。

介质级加密

介质级加密是一种新出现的方法，它涉及对存储设备 (包括硬盘和磁带) 上的静态数据进行加密。虽然介质级加密为用户和应用提供了很高的透明度，但提供的保护作用却非常有限：数据在传输过程中没有经过加密只有到达了存储设备，数据才进行加密，所以介质级加密只能防范有人窃取物理存储介质。另外，要是在异构环境使用这项技术，可能需要使用多个密钥管理应用软件，这就增加了密钥管理过程的复杂性，从而加大了数据恢复面临的风险。

嵌入式加密

嵌入式加密设备放在存储区域网 (SAN) 中，介于存储设备和请求加密数据的服务器之间。这种专用设备可以对通过上述这些设备、一路传送到存储设备的数据进行加密，可以保护静态数据，然后对返回到应用的数据进行解密。

应用加密

将加密技术集成在商业应用中是加密级别的最高境界，也是最接近“端对端”加密解决方案的方法。在这一层，企业能够明确地知道谁是用户，以及这些用户的典型访问范围。企业可以将密钥的访问控制与应用本身紧密地集成在一起。这样就可以确保只有特定的用户能够通过特定的应用访问数据，从而获得关键数据的访问权。任何试图在该点下游访问数据的人都无法达到自己的目的。

4.8.3 数据完整性的鉴别技术

数据完整性鉴别技术的目的是对介入信息传送、存取和处理的人的身份和相关数据内容进行验证，一般包括口令、密钥、身份、数据等项的鉴别。

数据完整性的鉴别技术包括：

信息摘录：对数据完整性保护的最基本思路是在综合相关因素的基础上为每个需要保护的信息生成一个唯一的附加信息，称为信息摘录。数据完整性保护能力有赖于信息摘录的生成和保护；

数字签名技术：数字签名是被保护信息以及发方已知的且收方可验证的保密信息的函数。它是签名方对信息完整性的一种承诺，它所保护的信息内容可能会被破坏，但任何对数据完整性的破坏都会被发现。数字签名包括盲签名、代理签名、群签名等签名技术；

数字水印：往目标数据中添加某些数字信息以达到版权保护等作用的技术。

4.8.4 密钥管理技术

密钥管理技术是指通过公开密钥加密技术实现对称密钥管理的技术，可以使相应的管理变得简单和更加安全，同时还解决了纯对称密钥模式中存在的可靠性问题和鉴别问题。管理密钥从产生到销毁的过程，包括密钥的产生、存储、分配、保护、更新、吊销和销毁等。在这一系列的过程中，都存在安全隐患威胁系统的密钥安全。

从密钥体制的不同上进行分类，密钥包括对称加密和非对称密钥。

保证密钥的安全基础：限制一个密钥的使用时间、密钥长度。

4.9 数据脱敏

数据脱敏是指对某些敏感信息通过脱敏规则进行数据的变形，实现敏感隐私数据的可靠保护。在涉及客户安全数据或者一些商业性敏感数据的情况下，在不违反系统规则条件下，对真实数据进行改造并提供测试使用，如身份证号、手机号、卡号、客户号等个人信息都需要进行数据脱敏。

数据脱敏分为静态数据脱敏和动态数据脱敏。

4.9.1 静态数据脱敏

静态数据脱敏，是数据的“搬移并仿真替换”，是将数据抽取进行脱敏处理后，下发给下游环节，随意取用和读写的，脱敏后数据与生产环境相隔离，满足业务需求的同时保障生产数据库的安全。

4.9.2 动态数据脱敏

动态数据脱敏，在访问敏感数据的同时实时进行脱敏处理，可以为不同角色、不同权限、不同数据类型执行不同的脱敏方案，从而确保返回的数据可用而安全。

4.10 数据安全溯源

数据安全溯源，主要是解决数据的流转或者泄露后的应对技术能力。一般是通过数据水印技术和数据溯源技术来实现。

4.10.1 数据水印

数据水印是一款对数据文件进行自动读取、识别、增加水印的专业数据安全产品，可自动发现源数据中的数据类型，并自动对数据增加仿真性水印，以应对数据泄露后的溯源查询和版权宣示。同时，对数据增加仿真性水印后，最大限度保证数据原始特征，逻辑及各类数据间的一致性、业务关联性。简单来说，数据水印技术实现了让数据泄露有迹可寻以及让数据所有权有据可查两大功能。

数据水印一般分为文档水印系统和数据库水印系统，其中数据库水印系统可以与脱敏结合使用，提高数据共享使用中的安全性和可追溯能力。

4.10.2 数据溯源

数据溯源定义为记录原始数据在整个生命周期内 (从产生、传播到消亡) 的演变信息和演变处理内容。

数据溯源追踪的主要方法有标注法和反向查询法。除此之外，还有通用的数据追踪方法，双向指针追踪法，利用图论思想和专用查询语言追踪法，以及文献提出以位向量存储定位等方法。

标注法

标注法是一种简单且有效的数据溯源方法，使用非常广泛。通过记录处理相关的信息来追溯数据的历史状态，即用标注的方式来记录原始数据的一些重要信息，如背景、作者、时间、出处等，并让标注和数据一起传播，通过查看目标数据的标注来获得数据的溯源。

反向查询法

通过逆向查询或构造逆向函数对查询求逆，或者说根据转换过程反向推导，由结果追溯到原数据的过程。反向查询法关键是要构造出逆向函数，逆向函数构造的好与坏直接影响查询的效果以及算法的性能，与标注法相比，它比较复杂，但需要的存储空间比标注法要小。

4.11API 数据安全防护

API （Application Programming Interface，应用程序接口）是一些预先定义的接口（如函数、HTTP 接口），或指软件系统不同组成部分衔接的约定。 用来提供应用程序与开发人员基于某软件或硬件得以访问的一组例程，而又无需访问源码，或理解内部工作机制的细节。

很多大数据平台和业务系统都是通过 API 开放服务方式，整合线上、线下资源，并为使用者提供数据服务。但是此种方式调用数据也存在严重的数据安全风险。

针对 API 的数据安全，一般是通过对 API 接口进行反向代理，实现内外隔离。使用 HTTPS 加密通道、强身份认证、黑白名单等技术来提高交互安全性。

4.11.1 数据销毁

数据销毁 , 计算机或设备在弃置、转售或捐赠前必须将其所有数据彻底删除，并无法复原，以免造成信息泄露，尤其是国家涉密数据。

常见的数据销毁方法：

- 覆写法

磁带是可以重复使用的，当前面的数据被后面一笔数据覆写过去时，就算可以透过软件进行数据还原，随着被覆写次数的增多，非结构性数据被复原，需要解读的时间也越久，企业就可以评估数据被复原的风险是否能够承担。其中，低程度的就是将磁带或磁盘完全覆写；高程度则可以参考美国国防部 DoD 5220-22-M 保安认证程序，结合数种清除与覆写程序，让硬盘每一个空间都被重复清除与覆写。

- 消磁法

磁盘或是磁带等储存媒体，都是磁性技术，若能破坏其磁性结构，既有的数据便不复存在。一般企业可以购买小型消磁机做单卷消磁，但消磁机磁波高，大量消磁委托专门公司较迅速安全。

- 捣碎法 / 剪碎法

破坏实体的储存媒体，让数据无法被系统读出，也是确保数据机密性与安全性。

- 焚毁法

几乎每一个需要汰换的储存媒体最终都会面临，藉由焚毁让数据真正化为灰烬，永久不复存在。

4.12 统一安全管理

统一安全管理平台综合运用统一策略管理、设备健康状态监控、全局性日志管理和报表统计等手段，解决网络安全状况不直观、安全策略管理乱、安全事件响应慢、安全故障定位难的问题。在技术上通过统一的界面实现对数据安全设备的统一管理，统一策略下发，从而解决了部署的多台安全设备总是“孤立”地进行安全检测和控制的难题，实现系统管理人员从全局角度对数据安全网络的安全状态有效监控，使安全孤岛形成合力和主动防御机制。

4.13 数据安全态势感知

数据安全态势感知，可针对用户访问行为进行分析建模，形成数据安全访问基线，从全网整体安全监测入手，再细化到数据信息资产以及安全数据的监测，实现全方位安全的态势感知。

数据安全态势感知一般采用大数据技术，实现事件的分布式采集、分析、存储和检索，对海量的日志数据、流量数据、数据包数据等做到实时关联分析、快速检索、高效统计，并以高度可视化的方式进行数据展现。

用户与实体行为分析

用户与实体行为分析，（User and Entity Behavior Analytics，简称 UEBA）。主要是以用户和实体为对象，结合规则以及机器学习模型，对用户行为进行分析和异常检测，尽可能快速地感知内部用户的可疑非法行为。

UEBA 聚焦于“异常用户”（即特权账号被盗用）和“用户异常”（即合法的人做不合法的事）。UEBA 对企业内部威胁的分析场景更有优势，更侧重于关注用户的行为，可以从另一视角去发现问题。

通常 UEBA 会与态势感知系统进行联动，针对外部数据和内部数据进行统一侦察分析，实现系统的多维度异常检测，对于将会产生的威胁进行及时告警，规避风险

4.14 隐私计算

隐私计算是指在保护数据本身不对外泄露的前提下实现数据分析计算的技术集合。目前主流的隐私计算技术主要分为多方安全计算、联邦学习、可信执行环境。

4.14.1 安全多方计算

安全多方计算指多个参与方各自持有隐私输入，各方希望共同完成对某问题的计算，而每个参与方除计算结果外均不能得到其他参与方的任何输入信息。

安全多方计算协议从适用性上说，分为通用安全多方计算协议和单一用途的安全多方计算协议。前者通过混淆电路（Garbled Circuit）等构造理论上可解决任意问题（即任意能以逻辑电路表达的函数），但效率相对较低，后者则针对某一类问题精心构造（如集合交集计算、模式匹配、数据挖掘等），效率相对较高。比如最早由 Lindell 等在 2000 年提出的保证隐私的数据挖掘（Privacy-Preserving Data Mining，PPDM）协议，就是在考虑各参与方输入数据的隐私的条件下，完成数据挖掘（如分类、聚类、关联规则挖掘）的安全多方计算协议。

在数据处理中，依据具体问题的不同，安全多方计算既可以单独使用，又可以与其他技术联合使用，作为高层隐私计算协议的组成部分。

4.14.2 联邦学习

联邦学习是一种分布式的机器学习方法，即参与方对本地数据进行训练后将更新的参数发往服务器进行聚合，得到总体参数的

学习方法。与传统机器学习技术相比，联邦学习旨在解决数据孤岛问题，保护本地数据隐私。

联邦学习可分为横向联邦学习（适用于参与方的数据具有相同特征空间和不同样本空间的场合）和纵向联邦学习（适用于参与方的数据具有相同样本空间和不同特征空间的场合），另外有学者提出了联邦迁移学习（适用于各个参与方的的数据的样本空间和特征空间均仅有少量重叠）。其中目前横向联邦学习相对更为成熟。

在数据处理的过程中，联邦学习可以让各个数据持有者在本地训练参数，这些参数通过同态加密和 / 或安全多方计算等方法进行聚合，进而得到聚合后的参数。

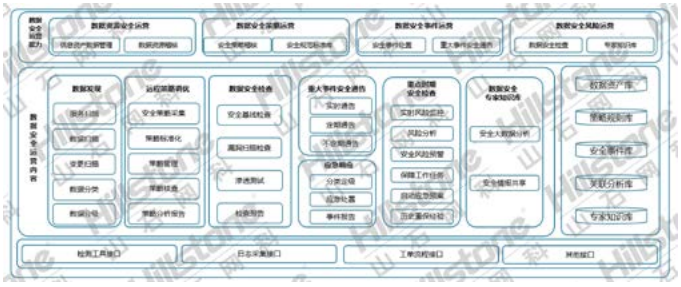
4.14.3 可信执行环境

可信执行环境是一种在相对不安全的主机环境中建立一个独立的、安全的、完全受控的计算环境的技术，需要特殊的 CPU 指令和主板硬件的支撑，以 ARM 的 TrustZone 和 Intel 的 SGX 为代表。在可信执行环境中，仅能运行经过认证的可信程序，而可信程序执行过程对于可信执行环境外的主机来说是不可见的。比如传统意义上的机密数据，如非对称加密体制中的私钥，就可以安全地放在可信执行环境中，而主机操作系统即便受到攻击，也无法获得位于可信执行环境中的私钥。

在数据处理的过程中，可信执行环境配合大数据算法程序监管措施，可以实现方滨兴院士提出的“数据不动程序动”的隐私计算实用落地策略。即在各数据持有方本地建立可信执行环境，数据使用方将算法程序提供给数据持有方，将数据使用方提供的算法程序运行在可信执行环境中，可信执行环境通过监管策略保证数据使用方最后仅能获得算法程序在数据上运行之后产生的模型数据。这样数据持有方的数据不会泄漏给数据使用方，而数据使用方也不用为算法程序设计全新的隐私计算协议。

五、以运营为保障，实现可持续数据安全

数字化转型下的数据安全体系设计，应通过建立数据安全运营中心实现对全域数据安全风险的监测、预警、通报和处置。



上图为全套的数据安全运营内容，依据这套内容，山石总结出了数据安全运营的关键步骤

5.1 数据安全制度规范、组织人员建设

5.1.1 数据安全组织建设

数据安全管理组织架构

一是数据安全管理组织架构，在完成数据安全管理流程梳理后，需结合数据安全现状对数据安全管理组织进行设计。

二是数据安全管理团队职责，根据安全管理现状，设立数据安全管理团队，负责安全管理工作。数据安全管理团队成员由各类专业技术人员组成，负责数据安全管理工作的日常管理、数据安全管理工作阶段性总结及汇报、与相关单位的沟通协调等工作。

数据安全运营组织架构

一是数据安全运营组织架构，在完成数据安全运营流程梳理后，需结合数据安全现状对数据安全运营组织进行设计。

二是数据安全运营团队职责根据安全管理现状，设立数据安全运营团队，负责大数据的安全运营工作。数据安全运营团队成员由各类专业技术人员组成，负责数据安全运营工作的日常管理、数据安全运营工作阶段性总结及汇报、与相关单位的沟通协调等工作。

数据安全监审团队架构

一是数据安全监审组织架构，数据安全监审是对大数据平台的日常业务活动、运营与保障、组织架构责任机制、关键控制环节和控制点等全生命周期的过程进行监审和稽核，确保各类数据活动符合法律法规和管理制度的要求，让各类作业得到有效的监管，防范和控制审计风险。完成数据安全监审流程梳理后，需结合数据平台数据安全现状对数据安全监审组织进行设计。

二是数据安全监审团队职责，根据安全现状，设立数据安全监审团队，负责安全监审工作。数据安全监审团队成员由数据安全监审方各类专业技术人员组成，负责数据安全监审工作的日常作业、数据安全监审工作阶段性总结及汇报、与相关单位的沟通协调等工作。

5.1.2 数据安全流程建设

参照国家、省有关政策导向，推进数据安全相关制度及流程编制、实施方案设计制定。数据安全流程是数据安全体系的指引和基础，可以从以下方面进行规划和建设，承建单位需结合实际需要进行优化和调整。

建立责任明确、程序清晰的数据安全组织架构，明确管理职责、工作程序和协调机制。针对不同类别和级别的数据制定管理控制原则，根据数据资产使用部门和角色、数据资产的分布、数据量级、访问权限、数据使用状况，有效的针对数据进行精细化的安全管控。

结合国家相关法律要求及行业标准规范制定数据安全策略和规划，建立健全数据安全治理过程的制度、流程、标准体系，对数据安全过程进行规范指导，保障实行数据安全规划、计划、实施、运行、督查的全过程管控。对数据安全制度、标准进行滚动式修订，持续夯实自身数据安全标准化管理基础。

建立数据安全工作和监督审计机制，监督数据安全工作有效开展，保障数据安全治理的策略和规范被有效执行和落地，快速发现异常行为和风险。

数据安全管理流程设计，包括但不限于权限管理、数据访问、事件及问题处理、应急管理等流程设计。

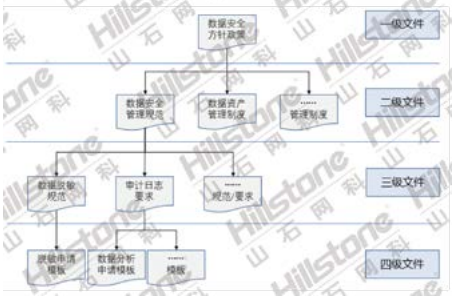
数据安全运营流程设计，包括但不限于系统上线流程、数据安全策略制定及发布、敏感数据操作等流程设计。

5.1.3 数据安全制度规范

根据当前数据安全保障体系的实施现状，结合最新的政策要求，为适应新时期的发展需求，应重新审视已编制规范的执行和运行情况，并根据一线的操作反馈，持续补充完善编制工作。针对已编制、待审的标准规范、技术规范等文件，提供编制、审核、跟

进以及相关的标准规范管理运营服务规范进行持续更新维护，推动待审标准规范修改完善。针对数据安全保障体系中尚未建立的相关规范制度，编制数据安全相关的规范制度，加快推动数据安全治理工作的开展。

建立覆盖各个层面的数据安全制度规范文件，数据安全制度规范文件的内容符合国家、省、市相关数据安全要求，并能明确每个控制点的落实要点、落实方法和执行责任人，制度规范文件内容应尽量与现有体系进行整合，还应保持与已有文件操持一致，防止冲突。数据安全制度的建设和执行，包括数据安全方针和总纲、数据安全制度、数据安全规范。



一级文件为方针政策、二级文件为制度规范、三级文件为操作明细、四级文件为基础模板，具体如下：

方针政策：明确数据安全工作的策略和方针，阐明数据安全的总体目标和范围，为数据安全体系其它文件的编制与具体措施的制订提供指导和支持。方针政策由决策层指导编制并发布，明确数据安全工作的总体方针和纲要，确定开展数据安全工作的目标和基本原则。

制度规范：在方针政策的框架下，明确制定基于数据场景的数据安全制度规范和管理办法，如数据安全人员管理制度、数据供应链安全管理制度、数据安全风险管理制度等，为数据安全体系中的流程、操作手册等的制订和评估提供直接依据。制度规范明确相关角色的权利和义务，面向相关对象（包括人、应用、工具）提出要求。

流程指南：基于制度规范提出的要求，形成具体的执行文件，梳理数据安全流程，拟定操作手册，如脱敏规范、审批流程、审计日志规范等，流程指南是指导技术落地的基础。

记录模板：记录模板是基础辅助类文件，由流程指南在执行过程中产生和沉淀而来，制定用以支撑各类制度规范和流程的表格，以及支持信息安全活动的记录文件。例如：数据权限申请模板、脱敏申请模板、流程审批模板等。

5.1.4 数据安全绩效评估

建立较为完整的数据安全管理考核指标体系，未形成制度化的考核机制，不利于持续优化改进数据安全管理工作。依据数据安全管理成效，持续改善评估流程，强化绩效评价机制。

数据安全管理方应根据业务要求，结合具体的考核标准，从三个方面加强单位绩效评估机制，并形成相应交付成果，例如：

1 制定单位绩效评估方案，明确评估频率、范围、时间、方法等。

2 制定绩效评估结果发布审核及反馈核查流程。

- 按照政数局要求，明确考核周期。
- 考核周期结束后的 15 天内，数据安全管理团队对考核指标完成情况进行评价，得出考核结果。
- 考核结果提交数据安全监审方及政数局进行审核。
- 审核完成后，发布考核结果。如对考核结果有异议，可在发布后的 5 个工作日内进行反馈，数据安全管理团队对反馈问题进行复核。

3 制定单位绩效评估指标及统计口径，最终绩效评估结果，为数据安全管理、数据安全运营、数据安全监审考核提供科学依据。

5.2 数据安全服务

5.2.1 数据安全咨询

重点课题研究支撑

梳理当前数据安全管理的发展规划和标准规范体系制定的现状，深入分析存在的问题，根据数据开发利用与开放共享的推进、数据管理的纵深服务需求以及国家政策的落实部署的需求，有针对性的甄选出行数据安全重点管控领域，协助制定数据安全管理发展规划编制以及相关指导意见的出台。

数据安全专项任务管控

在健全、强化咨询服务能力机制的基础上，根据管控的要求，处理各级安全管理部门组织的数据安全自查工作、现场安全检查工作。

另外，针对数据安全保障体系中，结合安全管理要求，对指导材料可用性把控、培训指导会议成效把控、进度通报指标合理性把控、

5.2.1 数据安全咨询

重点课题研究支撑

梳理当前数据安全管理的发展规划和标准规范体系制定的现状，深入分析存在的问题，根据数据开发利用与开放共享的推进、数据管理的纵深服务需求以及国家政策的落实部署的需求，有针对性的甄选出行数据安全重点管控领域，协助制定数据安全管理发展规划编制以及相关指导意见的出台。

数据安全专项任务管控

在健全、强化咨询服务能力机制的基础上，根据管控的要求，处理各级安全管理部门组织的数据安全自查工作、现场安全检查工作。

另外，针对数据安全保障体系中，结合安全管理要求，对指导材料可用性把控、培训指导会议成效把控、进度通报指标合理性把控、部门回访跟进指导问题把控、问题总结提升把控等进行专项任务管控服务。

数据安全政策咨询

对国家、省有关数据安全保障相关标准、规范、制度、办法等进行解读，并针对不同范围对象人群进行培训支撑，协助开展其他咨询、培训、出具报告的支撑服务。

5.2.2 数据安全常态化监测

日常数据安全监测管理

通过山石网科数据安全综合治理平台以及专业的安全运营人员人工监控和分析相结合的方式，对数据湖内各项数据进行全天、实时数据安全监控，监控内容包括：数据库风险监控、特权行为监控、应用行为监控、安全设备状态监控、安全策略联动监控等，第一时间发现数据存在的安全异常。

定期发布安全分析报告

以山石网科数据安全综合治理平台为抓手，对数据资产的安全情况进行常态化监测，通过数据资产的规模分布、运行现状、风险异常、整改进度进行定期的统计，分析当前阶段的安全风险重灾区，发现安全防护的薄弱点，针对性制定安全管理策略的计划和落实。并根据不同层级的用户需求，形成：

- 日常性安全监测报告
- 月度安全分析报告
- 季度安全分析报告

5.2.3 数据安全定期人工检查

根据数据安全内控要求，开展数据安全检查。围绕数据和业务流程，通过技术测试、管理检查、数据分析等多维度手段，进行安全检查的评估与分析，输出安全检查报告。同时，持续对检查结果予以整改意见，并对整改进度进行全流程的跟踪，最后根据整改依据和必要的复测验证，以确认整改完毕，关闭安全检查节点，完成闭环。

定期数据资产检查

一是资产梳理概述从数据安全管理与数据资产的相关性考虑，针对各类数据资产的动态变化进行技术上的识别与验证，包括但不限于：

（1）内网的数据资产，对现有内网数据资产进行技术上的主动发现，致力于对数据资产的管理，在技术手段上进行验证和发现，如识别发现未经授权的上下线资产、被遗弃和无人管理的幽灵资产等；

（2）互联网的数据资产，发现未经授权数据资产问题，如测试资产未经正式授权流程发布到互联网环境，开发人员误将研发代码、配置情况、路径等数据和信息发布到互联网代码共享平台等。

由于数据资产分配情况的繁杂多样，该部分的内容往往无法通过常规手段，手工进行及时梳理和管理，因此管理方将借用自动化手动资产发现工具，通过专业的分析人员，发现相关的数据资产，帮助进行数据资产的风险把控梳理。

定期数据安全检查

需定期开展的数据安全检查工作，检查的内容涵盖数据、基础设施安全和人员。

为保障数据安全，在原有平台环境中加强针对数据安全的防护体系建设，从数据资产发现、交换、共享、使用、销毁的过程中有针对性的进行数据安全防护。

通过前期数据资产发现及相关技术安全防护保障，结合实际业务情况建立数据风险管控平台对数据访问使用，尤其是内部数据使用行为进行数据风险控制。建立数据安全态势感知平台，有效监测风险数据安全行为、提供即时有效的数据安全运维管理能力，结合本地的特征库和数据访问行为提供态势感知安全报告和专家级的处理能力。

5.2.4 数据安全风险评估

从数据生命周期与数据应用场景两个维度中去关注数据安全所面临的各种威胁，包括数据合规、数据不可用（如数据异常丢失、勒索病毒）、数据未授权访问、数据泄露、数据篡改等。使用的工具：一是被动的数据安全调研，之所以说是被动的，是因为我们所接收的信息都是运维人员、研发人员、测试人员及业务人员基于我们问卷的一个反馈，既然是问卷当然存在着不足，比如错误反馈、遗漏反馈等等；二是由评估人员进行的主动的安全测评，比如现场检查、漏洞扫描、渗透测试等，评估人员会对前面的调研反馈进行验证核实并且基于调研去发现潜在的安全风险。

5.2.5 数据安全日常运营

数据安全情报通告

通过对 CNNVD、CNVD、SIC 等渠道收集到的威胁情报信息，结合国内外的数据安全形式、对于公开发布的安全情报中涉及已有业务的相关组件及相关类似功能可能发生的安全事件类型。

将由特定人员定期整理推送相关的通告，将收集到的漏洞情报进行集中式的报告，避免建设单位不及时更新信息库而造成的信

息滞后。

对于通告中涉及的漏洞信息的威胁级别、漏洞编号、来源、更新来源、影响范围、事件描述和应对措施。便于建设单位针对通告内容进行及时更新与防护，对于通告中涉及国内外的重大安全事件进行及时案例分析，避免同类安全事件的发生。

对于影响范围特别广或造成重大进行损失的安全事件，将作为典型案例，必要时须整理成为员工安全意识培训内容，用以提高员工安全意识建设。

数据安全巡检

数据安全运维人员应定期对各类资产进行全面安全巡检，使用技术检测和人工检查的手段，对各类资产的运行状态进行监控，对安全策略和安全日志进行检查，记录重点安全问题和异常情况，有针对性地提出通告及解决建议，提早预防、最大限度降低安全风险。

为防止在配置策略或升级补丁过程中出现系统异常的情况，在日常巡检过程中，也需定期对安全策略进行备份，以便在系统发生故障后能够迅速恢复正常。

数据安全运维处置

数据安全保障体系因其业务的持续性，需要进行长期性服务，建立完善的数据安全运营团队是必然选择。在原有的运维常规服务之上，数据安全处置运营主要包括以下内容：

1、数据安全运维

主要是数据安全措施的使用、运维，驻场或定期对数据安全产品的使用情况进行分析，并结合管理要求，持续进行管控措施策略和配置的优化，并定期输出数据安全运维报告和策略优化建议等。

通过已有的安全系统、工具和安全情报得到的有价值的安全信息，运维人员将安全信息用于发现问题，及时的更新策略和加强防护。结合人、工具、数据、流程实现数据安全运维。

2、应急预案与演练

按照相关要求，制定数据安全事件应急预案。并按照制定的应急规划，按照安全事件的危害程度、影响范围等对安全事件分级，定期进行应急预案演练。

由安全管理部门发起，根据相关的企业规章制度，配合完成相关的应急预案，并对演练中产生的攻击行为痕迹进行事后分析，根据分析结果及时调整业务的安全策略，演练的执行应按照企业的相关规章制度进行报备，并尽量避免影响业务系统用户的正常使用。

3、监测预警

围绕数据安全目标，依据相关安全标准，建立数据安全监测预警和安全事件通报制度，收集分析数据安全信息，对安全风险及时上报，包括按需发布数据安全监测预警信息等。

4、应急处置

相关方按照应急预案，在发生安全事件时，采取应急处置措施，向主管部门上报重大安全事件，定期对应急预案和处置流程优

化完善。

针对数据安全情报通告中的内容，按照业务实际需求对应急处置手册进行及时的更新。

在数据安全事件发生后，根据安全事件的影响和优先级，采取合适的恢复措施，确保信息系统业务流程按照规划目标恢复。

结合漏洞的危害等级、资产的重要性、威胁和漏洞情报（漏洞被利用的可能性）等维度对安全漏洞的风险等级进行重新排序，确定漏洞修复的优先级，筛选最重要的漏洞或数据产生最直接危害的漏洞，将结果上报给数据安全运营经理借助日常运维流程或通报下发流程推动进行优先修复。

数据安全策略优化

在业务运行中为加强数据的安全管理，保证数据全生命周期的数据流动安全，从数据采集、数据传输、数据存储、数据处理、数据共享、数据销毁这 6 个方面对数据全生命周期监管，实现对数据的监控和审计，以及数据安全策略动态优化。

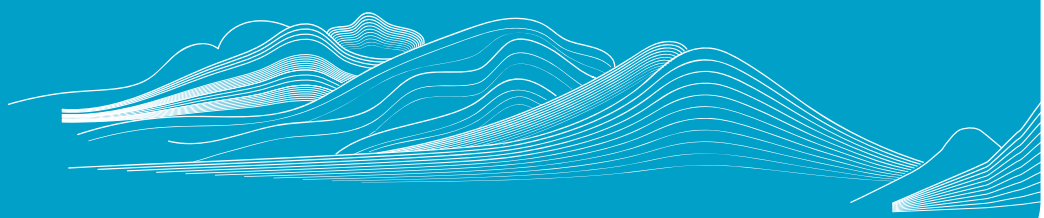
数据安全分析服务

结合山石网科数据安全综合治理平台的敏感数据地图、涉敏资产分析、数据使用分析、告警信息、用户行为模型等信息，由数据安全分析人员持续对数据使用过程中的安全风险进行深度挖掘，发现系统中的潜藏高危人员、高危敏感数据等隐患，同时定期按月报、季报上报给数据安全运营经理，再由数据安全运营经理基于事件级别进行分类推动数据安全运维人员、数据安全应急人员进行闭环处置工作。

5.2.6 数据安全应急响应

应急团队提供全天候的远程支持安全服务，可以根据网络管理员或系统管理员的初步判断是否与安全事件相关，通过远程咨询安全运营人员给出初步应急措施，确认需要信息安全专家或安全运营团队现场支持后，安全运营团队根据安全事件级别进行应急响应。

六、数据安全发展趋势展望



6.1 行业角度——政策利好，市场成长快、潜力高

一方面，国内外数据安全事件数量激增、数据安全已经成为各行业面临的最为严峻的考验，另一方面随着“数字中国”战略的深入推进，各地积极加快数字政府、数字经济建设步伐，数据安全逐渐成为各地基础共识，在国家立法层面，涉及数据安全的各项

法律法规及地方规范性文件密集出台，如《民法典》，《数据安全法》，《个人信息保护法》等政策法规，数据安全市场必将迎来高速发展。

6.2 市场角度——场景化数据安全将影响和牵引整个市场发展

云计算、大数据、信创等作为“新基建”中信息基础设施的重要组成，与应用场景相结合的安全防护也应运而生。一方面要解决关键软硬件的供应问题，另一方面要进一步提升系统和安全产品自身的安全性，信创作为国策会对数据安全市场造成很大的影响。

云计算环境下，数据安全流动问题凸出，面临黑客攻击、数据泄露、数据滥用、操作失误等内外部风险，数据安全已成为云上安全的防护重点。大数据平台造成数据高度集中，大数据平台自身安全性缺失等问题引起主管部门重视，大数据环境下的数据全生命周期安全、大数据平台自身安全等问题成为的数据经济发展的拦路虎，是未来市场建设和关注的重点。

6.3 技术角度——数据安全将与云、大数据等技术融合，隐私计算前景广阔

现有的数据安全技术更多是从数据库和数据平台的防护出发，没有深度的融入云环境和大数据环境中，安全设备的堆砌无法彻底解决数据安全问题还带来的投资和运维复杂的问题。利用云、大数据技术来解决云和大数据环境下的数据安全问题将成为数据安全技术发展的方向，如通过数据安全资源池提高资源使用率打破设备堆砌带来的问题；通过大数据技术解决海量数据安全日志分析等问题。

“数据”的确权、流通、共享利用，与“数据”的隐私保护、安全管控成为学术界和产业界共同关注的难题。隐私计算作为新兴的技术体系能够在保证数据安全可控的前提下，让数据得到共享利用。根据 IDC 的预测，到 2024 年，数据隐私、安全、放置、使用、披露要求方面的要求将迫使 80% 的中国大型企业在自主基础上重组其数据治理流程，数据治理、零信任与隐私计算、云与边缘安全成为企业的刚需。

6.4 用户需求角度——数据安全越来越引起重视，将是未来建设的重点

近年来，生产数据被勒索病毒加密、敏感数据被盗、隐私数据被泄露等问题使数据安全重要性越来越引起用户的重视，伴随着《数据安全法》等多个数据安全相关的法律法规的出台，只要涉及到数据处理的行业和场景都在积极开展数据安全工作，比如数字化程度比较高的金融行业、运营商行业、互联网行业，存储有大量个人信息和重要数据的政府单位、医疗机构等。毫无疑问地，数据安全将成为信息化建设过程中的重中之重。

参考文献

[1] 瞿晶晶 , 何雪莹 , 于新东 , 张涵 . 欧盟数据战略对长三角数字一体化发展的启示与建议 [J]. 科技中国 ,2021(10):69-71.

[2] 祁志伟 . 数字政府建设趋势及难题 [N]. 北京日报 ,2021-10-18(010).

[3] 邵晶晶 , 韩晓峰 . 国内外数据安全治理现状综述 [J]. 信息安全研究 ,2021,7(10):922-932.

[4] 赛迪译丛 . 联邦政府数据战略 [N]. 中国计算机报 ,2021-09-27(008).

[5] 郭云云 , 褚立文 . 欧洲议会通过《数据治理法》报告以推动建立“欧洲数据经济体”[J]. 互联网天地 ,2021(09):59.

[6] 陈天飞 .《数据安全法》正式实施，将会给数字营销行业带来哪些影响？ [J]. 国际品牌观察 ,2021(26):31-34.

[7] 石承泰 .《数据安全法》：让数据真正成为数字经济发展的流动血液 [J]. 国际品牌观察 ,2021(26):35-37.

[8] 杨楠 . 美国数据战略：背景、内涵与挑战 [J]. 当代美国评论 ,2021,5(03):76-92+123.

[9] 刘邦凡 , 臧梓健 . 我国数据安全治理研究 (2015—2020): 主题与演进趋势 [J]. 通信技术 ,2021,54(09):2190-2195.

[10] 瞿晶晶 , 陈秋萍 . 人工智能数据安全与法律治理 : 现状分析与发展建议 [J]. 华东科技 ,2021(09):56-59.

[11] 陈兰杰 , 李婷 . 基于战略三角模型的开放政府数据公共价值实现机制研究 [J]. 情报探索 ,2021(09):1-7.

[12] 王宇 . 大国博弈下的数据战略 [J]. 财富时代 ,2021(08):5.

[13] 魏亮 , 田慧蓉 . 网络安全发展综述 [J]. 信息通信技术与政策 ,2021,47(08):17-23.

[14] 黄欣荣 , 潘欧文 . “数字中国”的由来、发展与未来 [J]. 北京航空航天大学学报 (社会科学版),2021,34(04):99-106.

[15] 王伟洁 . 我国数据安全风险、治理困境及对策建议 [J]. 网络安全和信息化 ,2021(06):21-24.

[16] 杨洸 , 李东阳 , 宋旭 . 浅析大数据技术在公共信息安全领域的应用与发展趋势 [J]. 信息安全与通信保密 ,2020(12):93-102.

[17] 焦迪 . 新形势下数据安全发展分析 [J]. 网络安全技术与应用 ,2020(10):83-86.

[18] 赵博 . 基于大数据的战略预见研究 [D]. 中共中央党校 ,2016.

[19] 王世伟 . 论大数据时代信息安全的新特点与新要求 [J]. 图书情报工作 ,2016,60(06):5-14.

[20] 王斯妤 . 中国政府数据开放：现状问题与策略选择 [D]. 吉林大学 ,2016.

[21] 张弛 . 大数据时代中国出版产业链的重构 [D]. 华中科技大学 ,2015.

[22] 张兰廷 . 大数据的社会价值与战略选择 [D]. 中共中央党校 ,2014.

[23] 范生万 . 郭良主编 . 电子商务网络技术 [M]. 合肥：中国科学技术大学出版社 , 2012.02. 第 228 页

[24] 董文亮 , 陈思超 , 万燕珍 . 浅谈数据恢复技术的原理和硬盘数据恢复 [J]. 电脑迷 ,2018,(13):39.

Hillstone
山 石 网 科

中国·北京
北京市海淀区宝盛南路1号院20号楼5层
邮 编: 100192
电 话: +86(10)6299 7288
传 真: +86(10)6292 9388

中国·苏州
地 址: 苏州高新区科技城景润路
181号山石网科大厦
邮 编: 215153
电 话: +86(0512)6680 6966
传 真: +86(0512)6680 6206

销售与服务热线: 400-828-6655

Copyright © 2021，Hillstone Networks版权所有，保留所有权利。
Hillstone、Hillstone Networks标识、山石网科、StoneOS、StoneManager、Hillstone PnPVPN、UTM Plus均为Hillstone Networks所属商标。
所有其他商标和注册商标均为其各自公司的财产。
本文所包含信息可能会有所修改，恕不另行通知。如需最新信息请浏览Hillstone Networks网站(www.hillstonenet.com)。

科创板股票代码: 688030

官方微信

官方视频号