数据安全治理白皮书 5.0

中关村网络安全与信息化产业联盟

数据安全治理专业委员会　编著

2023

序一

Foreword

以大数据、云计算、人工智能、区块链、物联网等为代表的新技术与新应用的不断拓展，推动了产业数字化与数字产业化的巨大变革，数字经济发展成为推动整体经济增长的主要引擎之一。当前，数字经济发展的核心引擎，就是数据价值的发挥。数据作为数字经济建设关键要素，将对其他生产要素起到倍增器的作用，为经济转型发展提供新动力。

伴随数据要素化进程的高速发展，数据价值的不断凸显，数据安全风险也随之与日俱增，数据泄露、篡改、滥用等数据安全事件频发，造成对个人、组织、社会公共利益甚至国家安全的严重威胁和损害，极大地制约了数据共享流通使用。数据安全已成为数字经济时代最紧迫、最基础的问题，加强数据安全治理，统筹数据发展和安全防护，推动数据依法合理有效利用，已成为维护国家安全和提升国家竞争力的战略导向。

数字经济时代下，数据呈现体量大、种类多、传播广、变化快、可复制等特性，且与业务场景强关联，数据安全治理面临巨大挑战。如何统筹开发利用与安全防护，实现一体两翼发展，欲达到治理的最佳效果，必须坚持综合治理的原则，持续践行以下三个关键要素：一是一体化的治理理念，二是全维度的顶层设计，三是先进的技术体系。一体化的治理理念是实现数据安全治理高质量发展的核心，要把数据安全治理融入到整个国家和社会治理体系之中，构建政府负责、社会协同、公众参与、法治保障的数据安全社会治理体系，从单向的“通办”、“统管”转为多元、交互、协同的“共治”，共同织密织牢国家数据安全网。全维度的顶层设计是实现数据安全治理高质量发展的基础，国家层面要从职责分工、法律法规、政策制定和标准规范等方面做好国家层面的顶层设计，组织层面重点强调因地制宜、量身定制的治理目标，体现组织架构、管理体系和技术体系相融合的核心理念以及围绕全生命周期的场景化的治理方案。先进的技术体系是实现数据安全治理高质量发展的支撑，要从数据安全治理相关的基础理论到关键共性技术、再到应用技术进行全链条的创新研究，积极推动构建自主可控、先进实用的技术和产品体系。

本系列白皮书以理论联系实践为主导思想，以主册加各行业分册为呈现形式，从近年来我国数据战略及数据安全形势研判、数据安全治理概念与治理理念及框架、数据安全关键技术到多行业的场景化治理实践等多视角、多维度，较为系统、全面地对数据安全治理

相关内容进行了研究和探索，综合解读了监管政策法规及安全事件，梳理厘清了协同治理的相关概念与内涵，深入剖析了数据安全治理面临的挑战与治理方法论，整体架构了战略指导下的管理、技术、运营相结合的治理框架，体系化描述了各类监测与防护技术，列举了丰富的行业实践案例并建设性地提出了数据安全治理未来的发展和倡议。

“行远自迩，笃行不怠”，期待通过白皮书中围绕数据安全治理的理论探索与行业治理实践介绍，为数据安全治理相关人员带来具体的指引、参考和启迪，并付诸到实际治理工作当中，同时也期冀大家共同努力，持续探索数据安全治理之道，为加快推进数字中国建设保驾护航。

冯登国

中国科学院院士

序二

Foreword

《数据安全治理白皮书》（以下简称白皮书）历经五年多的发展与延续，已升级到 5.0 版本。白皮书与中国数据安全治理高峰论坛（以下简称高峰论坛）相伴相生，一路走来。2017 年首届高峰论坛开启，2018 年第二届高峰论坛发布《数据安全治理白皮书 1.0》，此后我们坚持每一届高峰论坛发布一版白皮书，只有 2020 年新冠黑天鹅降落人间停了一年，即便是 2021 和 2022 年疫情还未消散的时候，我们也依旧坚持着。

2017 年，安华金和在国内提出了“数据安全治理”这个概念，当时这个概念很新；业内大家主要谈的是网络安全，看待数据安全也大多基于等保与攻防的视角，由于缺乏法律法规作指引，只能贴着等保走。安华金和自 2009 年开始做数据安全，是国内最早一批专注于数据安全产品、技术研发的企业，积累了大量的实战经验，对于数据安全思考也比较多，逐步形成了对数据安全一些自己的认知。

最初我们聚焦在“数据库”安全，在与政府部委、企业数据中心客户的交流中，逐渐认识到用户真正关心的是如何保护数据库中的数据，以及数据在保障安全的基础上如何得到很好的利用，让价值得到充分释放。我们不断思考和实践如何达到安全与应用的平衡，在这个过程中领悟到两方面：一是应以数据为中心，在使用数据的基础上谈安全，结合不同的场景采取精准的数据安全防控措施；二是在促进数据流动的同时，要保证数据安全，应进行分类分级。我们思考并提炼出了一个词语来概括这些思想，即“数据安全治理”。而后看到国际上对此也有专门的描述，即“Data Security Governance”，发现我们的思考与国际同仁对于数据安全的看法不谋而合。

相较网络安全，数据安全的落地更专注，更要将组织、规范、技术整体统筹推进才有可能做好。2017 年，我们举办了第一届高峰论坛，众多行业用户与专家齐聚一堂，共同探讨数据安全。在这个过程中，我们认识到，需要对数据安全治理的概念归纳研讨做进一步深入的思考和表述，才能在业界的沟通中统一思想和话术。因此在 2018 年第二届高峰论坛召开前组织完成了《数据安全治理白皮书 1.0》的撰写并于峰会上奉献给大家，同时，在中关村网络安全与信息化产业联盟的支持下，牵头成立了联盟的数据安全治理专业委员会，持续的推进数据安全治理工作前行。就这样，高峰论坛和白皮书一直坚持到了现在。

2021 年 6 月，《中华人民共和国数据安全法》颁布施行，作为国家关于数据安全方

面的基础性法律，明确提出了“维护数据安全应当坚持总体国家安全观，建立健全数据安全治理体系，提高数据安全保障能力”，并把分类分级作为推进数据安全的基础工作，提出“国家建立数据分类分级保护制度”、“对数据实行分类分级保护”。2021 年 11 月，保护个人信息安全的专门法律《中华人民共和国个人信息保护法》正式颁布施行。在两个法律的基础上，国家互联网信息办公室于 2022 年 7 月发布了《数据出境安全评估办法》。《数据安全法》《个人信息保护法》《数据出境安全评估办法》分别从国家重要数据保护、个人隐私和权益保护、数据主权维护角度给出了行为指引。可以说，到 2022 年，我国数据安全治理的基础立法工作基本完成。

2022 年起，国家互联网信息办公室、工业和信息化部等相关部门陆续出台一系列规章和规范性文件，全国信安标委、行业管理部门加速推进标准化研究制定工作，随着各行各业数字化的推进，数据安全产业发展如火如荼。但我们在与客户沟通时发现，用户对于如何保障数据安全还是比较困惑。例如数据分类分级与个人信息保护相结合如何开展工作；与国家重要数据保护相结合如何开展工作；还有，分类分级后与数据安全管理的结合，也都存在许多的不确定性。《数据安全治理白皮书 5.0》在延续惯例对相关的新理论、新政策、新技术进行更新外，重点推出了行业落地实践集，对行业分类分级标准、数据安全建设要求、检查办法、具体化的建设落地案例等进行了介绍，共涵盖了七个行业。我们希望通过对各行业的治理实践进行归纳总结，为具体落实数据安全工作提供有价值的借鉴。在梳理行业实践总结时，我们发现，由于不同行业的数据安全工作进展参差不齐，行业间的相互借鉴、学习尤为重要。未来白皮书更新的重点之一也将是行业落地实践经验的汇集交流。

当下，数字经济成为人类新的经济增长方向，数字化、网络化、智能化在逐步改变人类生存环境，基于大规模数据学习的人工智能大有替代人类大脑决策之势；数据安全成为了人类基础安全保障的核心要素之一，数据安全的重要性前所未有。对此我们可以做的就是热烈拥抱他的到来。我们希望白皮书成为拥抱这一历史性变化的一个印迹，和大家一起见证数据安全与数字经济发展的相伴相行。

刘晓韬

中关村网络安全与信息化产业联盟数据安全治理专业委员会主任

北京安华金和科技有限公司董事长兼 CEO

前言

Preface

■ 数据安全新形势背景

近年来，我国数字经济持续快速发展，其产值占国内生产总值比重逐年高速增长，已成为推动经济增长的重要引擎。国家高度重视数据要素化市场配置改革进程，自 2022 年以来，党中央、国务院陆续印发了《“十四五”数字经济发展战略》《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》《数字中国建设整体布局规划》等一系列数字经济发展的战略性文件，我国在加快数据要素市场流通，创新数据要素开发利用机制。但是，数据在广泛流动释放价值的同时，也面临着被窃取、泄露、篡改、破坏、滥用的巨大威胁。新形势下的数据安全风险形态也呈现多样化、复杂化特点，造成对个人、组织、社会公共利益甚至国家安全的严重威胁和损害。为规范数据处理活动，保障数据依法有序自由流动，近年来，我国数据安全相关法律法规、部门规章持续密集发布，数据安全标准化研究制定工作加速推进，相关审查、评估、认证、审计等制度陆续推出，为各行各业落实数据安全治理、增强数据安全保障能力提供了具体指引和实施参考，持续推动了数据安全的有法可依、有章可循、有标可落。

■ 编写目标

在上述形势背景下，组织在数据收集、存储、使用、加工、传输、提供、公开等数据处理活动过程中，针对数据安全威胁与监管合规要求，无可避免地需要面对越来越多严峻和紧迫的数据安全挑战。大家都在思考如何在数据资产的开发利用、价值实现与安全保护、履行合规义务之间进行恰当平衡？如何在数据安全方面编制合理的制度策略和选取适宜的技术措施？如何在不断创新的数据应用场景中持续保护数据安全？为了帮助有关单位解决在开展数据安全治理时面对的众多困惑和难题，实现数据开发利用与安全防护一体两翼、平衡发展的目标，本白皮书在《数据安全治理白皮书 4.0》的基础上，根据最新进展分析当前我国数字经济战略发展与数据安全新形势新动态，厘清数据安全治理概念并诠释数据安全治理内涵，完善数据安全治理需求与框架，解读最新法律法规及标准等监管要求与技术规范，全面、系统介绍围绕数据生命周期的相关安全技术需求、安全技术工具与技术发展趋势，归纳 2022 年以来典型的数据安全事件与相关法律案件并进行分析，提出了数据

安全治理的未来展望和建议。同时，作为本白皮书的突出亮点，推出了典型行业数据安全治理实践篇。鉴于数据安全与业务场景的强关联性，践行场景化数据安全，面向政务、金融、医疗、电信、电力、教育、工业七大数字化转型相对比较领先的行业领域，由行业内治理专家及领军企业牵头，分别给出具备各行业特色的数据安全治理方案与落地实践案例。《数据安全治理白皮书 5.0》力图尽可能体系化、完整地梳理和总结当前与数据安全治理有关的各种资料和最新进展，持续深入探索“让数据使用有序而安全”的数据安全治理方案，以实现在数据要素释放价值的同时，坚守安全底线的目标。我们希望能为数据安全运营者、建设者提供指引，为服务支持者（安全服务机构、咨询机构、律师、法务等法律工作者）提供参考，期望为进一步推广、普及和完善数据安全治理的理念、方法、体系与实践添砖加瓦、贡献力量。

■ 读者对象

本白皮书主要面向以下几类读者：

组织内部数据安全治理相关人员：面向组织内部开展数据安全治理工作相关的决策人员、方案规划和实施人员、安全管理人员、技术培训人员，期望能够帮助他们更加深入全面地了解在数字化转型过程中正在和将要面对的数据安全威胁、风险和合规性要求以及行业内场景化治理实践，从而更积极主动地筹划和开展系统化的数据安全治理，确保能够有效应对新形势下的各种数据安全挑战。

数据安全治理相关产品 / 服务提供商：面向数据安全产业的方案及产品策划人员、安全治理咨询服务人员及项目实施人员，期望通过白皮书中对治理框架、技术应用与实践案例等内容的介绍为产品 / 服务提供商开展治理方案编制、产品研发和实施服务工作提供启迪与参考，以更好的服务用户。

数据安全治理相关服务支持者：对安全服务机构、咨询机构、律师、法务等法律工作者，期望通过对数据安全相关法律法规解读及相关法律案件分析介绍，给予他们在进行数据安全合规要求和建议工作中提供一定的借鉴参考。

此外，本白皮书对于数据安全相关政策法规和标准规范的编制人员、数据安全领域的研究人员，有关管理部门的专业人员等也具有一定参考价值。

■ 导读

整个白皮书由主册和典型行业数据安全治理实践篇构成，其中：

主册共分为五个正文章节和一个附录章节。

第一章 数据安全治理概念及内涵：对当前数据安全形势进行整体分析、梳理，厘清数据安全治理概念及内涵，诠释数据安全治理与相似概念的关系，梳理数据安全治理需求，进一步完善治理愿景、目标及理念。

第二章 数据安全整体框架：依据数据安全治理理念，围绕以数据为中心的治理体系不断演进、深化，组织在整体安全战略指导下，形成以数据分类分级为治理基石，数据安全管理体系、技术体系与运营体系为治理核心，监督评价体系为效能促进，形成更为完善、合理、全面的治理框架，并给出治理规划建设实施路径。

第三章 数据安全相关法律法规解读：在数据安全治理过程中，满足监管合规要求是重要驱动力之一，重点解读数据安全相关上位法及2022年以来新颁布的法律法规及技术标准等监管合规要求。

第四章 数据安全技术需求与主流工具：安全技术措施是数据安全治理的重要支撑，通过从需求和供给两侧对数据安全技术需求和安全技术工具进行全面性、系统化梳理与介绍，并对数据安全技术的发展趋势进行简述。

第五章 未来展望与倡议：面对数据安全治理实践涉及的管理、技术与运营过程中的问题，短期内尚无法有效解决的，以展望与倡议的形式予以表述，供行业内人士进行探讨。

附 录 作为本白皮书惯例，结合技术创新进一步对主流数据安全技术工具进行详述，对数据安全相关标准、国际数据安全政策法规进行介绍，并对近年以来重大数据安全事件与法律案件进行分析，为业内人士提供借鉴和参考。

典型行业治理实践篇

汇集了金融、政务、医疗、电信、电力、教育、工业七个领域，由行业内治理专家及领军企业牵头，从数据安全治理现状与需求、治理思路与内容、治理实践案例等多个维度论述各行业的数据安全治理实践，希望为各行业开展数据安全治理工作起到先行的示范作用。

■ 数据安全治理白皮书历史沿革

北京安华金和科技有限公司是在中国倡导数据安全治理理念的发起者和先行者，也是多年来推动数据安全治理理念在我国各行各业应用和实施的实践引领者。2017年，由安华金和联合国内网络和数据安全界的知名企业，发起成立了中国首个“数据安全治理小组”，并组织召开了首届中国数据安全治理高峰论坛。

2018年，在中关村网络安全与信息化产业联盟的支持和指导下，数据安全治理小组的成员单位共同发起成立全国首家数据安全领域的专业委员会—中关村网络安全与信息化产业联盟数据安全治理专业委员会。积极促进数据安全治理理念在我国的推广和普及，为我国数据安全领域的学术研究、技术创新、产业发展和人才培养提供了资源丰富的交流和支撑平台。成立当年，组织召开了第二届中国数据安全治理高峰论坛，并组织编撰《数据安全治理白皮书1.0》，首次提出数据安全治理的概念定义、治理理念及治理框架，强调业务需求与数据安全的平衡，在论坛上向社会公开发布。

2019年，第三届中国数据安全治理高峰论坛召开，《数据安全治理白皮书2.0》和《数

据安全治理建设指南》公开发布。在国家及行业高度重视数据安全及个人隐私安全的背景下，增加了数据安全相关法规和标准列表说明；补充了个人信息收集与隐私政策测评报告相关解读，扩展了各行业的数据安全治理实践，对数据库防勒索、透明加解密等数据安全相关热点技术进行了介绍，并更新了2019年重要的数据安全事件。

2021年，第四届中国数据安全治理高峰论坛隆重召开，《数据安全治理白皮书3.0》重磅发布。进一步诠释了“让数据使用更安全”的治理理念，分析了业内关注的数据安全与网络安全等概念的近似联系与区别，汇集了数据安全关键技术与前沿技术，解读了相关法律法规标准要求，整理了覆盖政务、金融、能源、教育、电信及医疗行业丰富的治理案例，成为数据安全行业较为全面且具有影响力的数据安全治理参考书。

2022年，由中关村网络安全与信息化产业联盟数据安全治理专业委员会主编，中国计算机学会计算机安全专业委员会、工业信息安全产业发展联盟、中关村网络安全与信息化产业联盟、北京工业互联网技术创新与产业发展联盟、中国电子商会自主创新与安全技术委员会指导，32家极具影响力的产学研机构共同参编的《数据安全治理白皮书4.0》于第五届中国数据安全治理高峰论坛上发布，白皮书分析研判了当时数据安全形势与动态，解读了相关法律法规监管要求，汇集了新形势下的数据安全治理主要实践案例及典型数据安全事件，尽可能全面、系统地整理总结了与数据安全治理有关的各类资料和最新进展。

组织架构

■ 主编方 / 出品方

中关村网络安全与信息化产业联盟数据安全治理专业委员会

北京安华金和科技有限公司

■ 指导单位

中国计算机学会计算机安全专业委员会

中关村网络安全与信息化产业联盟

工业信息安全产业发展联盟

北京工业互联网技术创新与产业发展联盟

中国电子商会自主创新与安全技术委员会

中国信息产业商会信息安全产业分会

中国网络安全产业联盟数据安全工作委员会

中国电力发展促进会网络安全专业委员会

■ 参编单位

国家计算机网络应急技术处理协调中心　国家信息技术安全研究中心　中国电子技术标准化研究院　中国信息安全测评中心　公安部第一研究所　公安部第三研究所　国家工业信息安全发展研究中心　中国软件评测中心　中国网络空间研究院　中国科学院软件研究所　中国科学院信息工程研究所　国家金融科技测评中心　国家卫生健康委医院管理研究所　北京市政务信息安全保障中心　天翼安全科技有限公司　暨南大学　国网智能电网研究院有限公司　福建省电子产品监督检验所　北京世辉律师事务所　光大科技有限公司　北京数字认证股份有限公司　北京安信天行科技有限公司　中国船舶集团有限公司第七〇九研究所　陕西省信息化工程研究院　北京市中伦律师事务所　西交苏州信息安全法学所　北京博遵律师事务所　泰和泰律师事务所　北京市中闻（上海）律师事务所　上海创同律师事务所　江西省信息中心　江苏省信息安全测评中心　山东省国土空间数据遥感技术研究院　山东省社会信用中心　烟台市大数据局　烟台市大数据发展集团有限公司　青岛市大数据发展管理局　智慧齐鲁（山东）大数据科技有限公司　联通数字科技有限公司　中国民生银行股份有限公司　工

银科技有限公司　中国工商银行安全攻防实验室　中金金融认证中心有限公司　北京国家金融科技认证中心有限公司　山东高速信联科技股份有限公司　晋商银行股份有限公司　江苏苏宁银行股份有限公司　东吴证券股份有限公司　南京证券股份有限公司　中电信数智科技有限公司　中移（苏州）软件技术有限公司　中国联合网络通信有限公司软件研究院　上海华东电信研究院（中国信息通信研究院华东分院）　西安电子科技大学杭州研究院　恒安嘉新（北京）科技股份公司　山东第一医科大学附属省立医院　江苏省人民医院　南京江北医院　中日友好医院　山东大学齐鲁医院　中南大学湘雅二医院　江苏省中医院　南方医科大学第七附属医院　东部战区总医院　临沂市人民医院　济南市康养事业发展中心　北京深思软件股份有限公司　华北电力大学　中国南方电网有限责任公司　国网大数据中心　中能融合智慧科技有限公司　中国人民公安大学　南开大学网络空间安全学院　电子科技大学网络空间安全研究院　北京科技大学　山东大学　山东财经大学　四川师范大学　华中科技大学　武汉理工大学　北京谷安天下科技有限公司　深圳市联软科技股份有限公司　北京锐安科技有限公司　湖北省电子信息产品质量监督检验院　山石网科通信技术股份有限公司　中电车联信安科技有限公司　天津太极风控网络科技有限公司　京信数据科技有限公司　北京智游网安科技有限公司　天九共享网络科技集团有限公司　青岛中元云册创新科技有限公司　昆仑太科（北京）技术股份有限公司　中邦网络安全技术（深圳）有限公司

致　谢

感谢以下人员为《数据安全治理白皮书 5.0》的编制付出的辛勤劳动。

编委会专家组组长

冯登国

指导专家（按姓氏笔画排序，排名不分先后）

于　锐　马民虎　王伟平　王才有　左晓栋　卢　卫　冯燕春　向小佳　刘龙庚　刘欣然
刘海峰　刘哲理　刘晓韬　刘紫千　严　明　李新社　李京春　李新友　李建彬　李　俊
李吉慧　李洪伟　杨　韬　肖革新　吴　兰　吴沈括　张　峰　张　力　张　涛　金　波
金　涛　单立坡　郝志强　胡红升　胡光俊　俞克群　姜　伟　姚相振　钱宗政　裴廷睿
衡反修

编审专家（按姓氏笔画排序，排名不分先后）

王晓光　王新锐　包国峰　刘曦泽　孙立淼　孙　岩　孙建国　李向锋　李安伦　李　斌
李　媛　杨帅锋　杨海峰　何延哲　何晋昊　张　敏　陈青民　陈　聪　林星辰　季亨卡
郝文江　胡　影　徐明迪　高　松　崔媛媛　蔚　晨　谭峻楠　魏　力

参编专家（按姓氏笔画排序，排名不分先后）

丁　莹　于建鹏　于　皓　马佑平　王　刚　王　玮　王　杰　王　迪　王美珍　王冠杰
王　峰　王浩宇　王海峰　王　翀　王逸君　王超毅　王斌君　王　普　王　蕾　王　巍
文　剑　尹晓东　邓鹏飞　左　芸　石聪聪　申浩文　田建彤　田　娜　田博文　史　辉
白旭东　白　倩　仝　鑫　朱元元　朱剑楠　朱洪涛　朱晓东　刘方斌　刘　杨　刘　畅
刘春雷　刘　洋　刘海丰　刘　翀　刘耜杭　刘　颖　衣军成　许智鑫　许道远　孙亚东
孙明明　孙晓童　苏　力　杜浩文　李　为　李永在　李　苏　李松涛　李　欣　李欣韦
李　波　李　振　李　莅　李　辉　李源鑫　李　静　李　睿　李潇莹　李德生　李　巍
杨　波　杨学颖　邱　杰　邱　峰　何黎明　宋士明　宋博强　初航正　张小亮　张永祯
张　兵　张　勇　张晓云　张晓娜　张　野　张　敏　张　瑞　张腾标　张　豪　张　澍
张耀峰　张　鑫　陈小春　陈江江　陈红松　陈志强　陈　虹　陈　钢　陈菲琪　范丽珺

范益天　范道峰　林　闯　金　晨　周　扬　周传玉　周　映　周剑涛　周　莉　周健雄
周爱昭　周　涛　官全龙　房海腾　赵宇博　柳彩云　钟　强　侯德智　施志晖　宫小茜
袁　成　袁　靖　夏杰峰　夏　瑛　顾飞飞　徐羽佳　徐　欢　徐　煦　栾秀梅　栾泽琳
高先周　高庆浩　高晨涛　高雅婷　高强裔　郭　莉　郭晓东　郭铮铮　郭超然　郭　腾
黄　进　黄　鹏　曹文洁　曹阿龙　龚伏兰　常景辉　梁明君　隆　峰　彭　远　彭建辉
葛　珊　葛菊平　董子娴　董　军　董　枫　韩　云　景慎旗　喻　英　程　娜　程　蕾
曾艳春　谢永红　谢航竞　雷嘉宾　阙秀震　廖怀学　魏　东　魏林锋

目录

Catalog

《数据安全治理白皮书 5.0》版本修订说明

《数据安全治理白皮书 5.0》版本中，针对以下内容进行修订完善与扩展：

1. 添加数据安全治理概念阐述，首次对“数据安全治理”概念进行了定义与诠释；

2. 基于当前数据安全发展形势，对当前国家数据战略、风险态势与监管举措等进行剖析；

3. 更新了数据安全治理实践过程中面临的新挑战与关键需求；

4. 进一步深化数据安全治理理念，健全数据安全治理框架，将个人信息保护明确纳入数据安全治理体系，并扩展治理框架中的监督评价体系介绍；

5. 添加数据跨境、数据交易、大数据处理与合作共享等典型、通用安全场景治理需求介绍；

6. 完善数据安全合规体系框架及相关法律间关系阐述，更新了 2022 年度以来最新的法律法规解读，对数据安全治理建设提供合规落地指引；

7. 基于数据安全技术在数据安全治理的关键支撑作用愈发显著，将数据安全技术体系独立成章，从技术需求到技术工具落地实践进行了体系化的整体介绍，并在附录中补充完善了数据安全相关产品与关键技术介绍；

8. 更新数据安全治理协同发展的未来展望和倡议；

9. 更新 2022 年度以来国内外重大数据安全事件归类分析与典型的数据安全相关法律案件分析；

10. 汇总最新的重要国家、行业与地方的数据安全相关标准列表；

11. 补充了国际数据安全政策与法规介绍；

12. 全文内容文字和段落结构优化；

13. 深入践行“场景化安全”，首次推出面向重点行业的数据安全治理实践集，形成数据安全治理主册加各行业分册的系列化丛书。

第一章　数据安全治理概念及内涵

当前，随着大数据、人工智能、区块链、云计算等新技术和产业的快速发展，数字化数据呈指数级增长，数据共享流通、开发利用的诉求愈发强烈。由于这类数据本身存在易于复制、确权困难的特点，数据在快速释放价值的同时，安全风险也与日剧增。

同时，在当前全球竞争格局加剧的形势下，数据安全已上升到国家安全战略。我国高度重视数据安全，持续出台相关法律法规，加强并健全系列监管举措，如何统筹数据开发利用与数据安全的平衡发展，促进和保障数据的有序流动，构建体系化、系统化的数据安全治理需求日益迫切。

1.1. 数据安全背景与形势

1.1.1. 数字化转型进入深水区

建立健全数字基础设施是打通内、外部循环经济体系的重要举措。我国信息化、数字化建设经过 20 余年的高速发展，已经在多点表现出全球领先的显著优势。数字革命是开启第四次工业革命的钥匙，数字经济是未来世界经济的火车头。执牛耳者，自当奋楫。促进数据共享流通使用，建成完善的数字基础设施，是“历史赋予的使命，时代要求的担当”。当前我国千行百业数字化转型进入深水区，数字经济已经成为助力经济增长的重要引擎。在这个大趋势中，加快培育壮大数据要素市场，充分发挥数据要素的放大、叠加、倍增作用，是贯彻落实新发展理念、构建新发展格局、推动我国经济转型的战略选择。

2022 年以来，我国围绕数字经济发展，在政策方面，国家陆续颁布了《关于构建数据基础制度更好发挥数据要素作用的意见》（以下简称“数据二十条”）、《数字中国建设整体布局规划》等纲领性文件。为持续推进数据要素化市场配置改革，2023 年国务院专门设立了国家数据局，负责协调推进数据基础制度建设，统筹数据资源整合共享和开发利用，统筹推进数字中国、数字经济、数字社会规划和建设。

1.1.2. 数据安全面临新挑战

伴随数据要素化进程的高速发展，数据广泛、实时流动，在释放数据价值的同时，数据安全威胁也日益严峻。除面临传统的泄露、窃取、破坏等安全威胁外，还呈现出如下新的风险态势：

数据跨境流动引发国家和公民安全隐患。随着经济全球化的发展，全球贸易往来、金融投资和技术交流日益频繁，在数据跨境传输、访问和使用过程中，跨境数据流动的种类、数量与频次持续大幅度上升，涉及的内容也不再局限于个人隐私信息，还包括国家安全、社会治理、企业商业机密等方方面面。伴随数据价值的攀升，数据被觊觎的风险也持续加大，由于技术漏洞、管理缺位和政策法规不完善等因素，海量的数据跨境流动带来了潜在的重大系统性风险，不仅会对个人隐私产生

严重影响，这些数据若被境外情报机关获取并用于对我国的战略分析，还会使得我国战略动作易被观察预测，产生国防安全的重大隐患。

滥采滥用个人信息并实施数据垄断。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资源。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，由此又加剧了个人信息滥采滥用、数据垄断乱象频发的数据安全威胁。

大数据杀熟与价格歧视。平台企业利用所掌握的数据以及大数据技术，对消费者的消费行为进行精准刻画，进而在用户不知情的情况下，对不同用户采取不同的价格机制与定价策略，从而最大程度上攫取利益。

信息茧房与视野窄化。算法推送技术导致推荐内容过于单调，它不仅让受众个体的视野被固化，会在受众当中形成分区，扩大了不同群体之间的知识鸿沟，甚至导致群体极化事件发生。

人工智能技术面临多重安全风险。一方面模型算法攻击挑战严峻，模型算法在深入挖掘数据价值的同时，被攻击、修改、窃取的风险也随之加剧，例如在网购平台推荐算法中，恶意混入误导性数据，导致推荐错误；以及利用人脸图片，欺骗人工智能系统，让其做出错误的判断。另一方面，基于人工智能的新型攻击凸显，基于人工智能具备的机器学习特性，会被黑客利用开展新型攻击。例如，针对具体人、具体场景，有针对性地生成钓鱼邮件，进行精准钓鱼；以及使用人工智能技术合成亲属语音，进行网络诈骗。再一方面，生成式人工智能引起新型数据泄露及滥用风险，伴随 ChatGPT 的兴起，生成式 AI 技术的商业化趋势已经来临，众多企业通过将文本理解分析，多模态检索等智能分析能力融入到在线服务、智能客服等产品和服务中，全面提升自身产品和服务的 AI 化，在此过程中，涉及的数据非法获取、数据泄露及恶意滥用等数据安全问题也日益凸显，例如：ChatGPT 不设限爬取、采集我国各大重要媒体、电商等平台中的敏感数据、用户行为轨迹等信息，深度训练分析我国社情民意，严重危害国家安全；以及在应用 ChatGPT 进行双向互动请求过程中，会被要求输入个人敏感信息、业务数据或涉及商业秘密等内容，加剧了数据泄露的风险。

1.1.3. 数据安全监管新举措

数据是经济发展的重要生产要素和核心引擎，数据安全已成为我国总体国家安全观的重要组成部分。“数据二十条”提出“统筹发展和安全，贯彻总体国家安全观，强化数据安全保障体系建设，把安全贯穿数据供给、流通、使用全过程，划定监管底线和红线。”《数字中国建设整体布局规划》提出“强化数字中国关键能力，筑牢可信可控的数字安全屏障。增强数据安全保障能力，建立数据分类分级保护基础制度，健全网络数据监测预警和应急处置工作体系。”

自 2022 年以来，为充分贯彻《数据安全法》《个人信息保护法》等上位法的总体要求，相关部门发布了多项数据安全规章、规范性文件、技术标准，以促进数据安全治理的落地实施，如国家互联网信息办公室出台了《数据出境安全评估办法》《个人信息跨境处理活动安全认证规范》《个人信息出境标准合同办法》等系列出境规则体系以及《数据安全管理认证实施规则》《个人信息保护认证实施规则》等认证相关部门工作文件。在技术标准方面，国家信安标委颁布了《信息安全技术

网络数据处理安全要求》《信息安全技术 移动互联网应用程序（App）收集个人信息基本要求》《信息安全技术 网络数据分类分级要求》（征求意见稿）等系列技术标准；在促进产业发展方面，工业和信息化部与国家互联网信息办公室等十六部门联合印发《关于促进数据安全产业发展的指导意见》，明确了数据安全产业发展的必要性、指导思想、基本原则和发展目标等顶层设计。由国家数据安全工作协调机制统筹协调，行业主管部门各司其职承担本行业、本领域的数据安全监管职责，网信部门、公安机关、国家安全机关依法依规承担各自职责范围内的数据安全监管职责的多方协同监管体系正在逐步形成并不断深入完善。

1.2. 数据安全治理概念和理解

自 2017 年 Gartner 首先在业界提出数据安全治理概念以来，国际国内对“数据安全治理”这一概念都有不同的诠释，但一直都没有给出一个标准化的公认定义。本白皮书从 1.0 到 4.0 版发布以来，本着求同存异的理念，也始终没有针对“数据安全治理”予以概念定义。伴随着数据安全治理的深入开展和广泛应用，在此版白皮书对“数据安全治理”的概念及涉及内涵尝试予以诠释，供业界探讨。

1.2.1. 数据安全治理概念

数据安全治理，顾名思义，可拆分为“数据安全”与“治理”，数据安全可理解为目标，治理可理解为手段。

首先看“数据安全”的定义，在《数据安全法》中明确将数据安全定义为“通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力”。

从核心立意来看，定义中核心强调的是数据开发利用与安全保护的统筹与平衡发展，一方面数字经济的发展必须在数据安全的前提下开展，没有数据安全，数字经济的发展将失去有效的控制支撑；另一方面，数据的开发利用是促进数据价值释放之必然，不能由于数据安全的过度保护制约数据的流动与共享开放。从防护措施来看，基于“统筹安全与发展”的数据安全核心立意，定义中强调了数据安全保护措施的必要性与持续性，必要性是指面向数据处理活动与场景化需求，采取按需、动态的管理和技术措施落实有效保护，持续性是指伴随数据围绕业务发展快速变化，相应的保护措施也需顺应变化，落实常态化运维，保持持续安全状态。

其次看“治理”的定义，“治理”对应的英文单词是“governance”（源自拉丁文或古希腊语“steering”一词，原意是“引领导航”），是指遵照具有共识的指导原则，通过协调和配合共同追求一致目标的过程。针对“治理”的概念，在全球治理委员会（CGG）中进一步解释为“个人与公私机构管理其自身事务的各种不同方式之总和；是使相互冲突或不同利益得以调和并且采取联合行动的持续的过程”，其中包含四个方面的特征，即：

（1）治理不仅仅是一整套规则条例，也不是一种活动，而是一个活动集合的过程；

（2）治理过程的基础不是简单的控制和支配，更重要的是协调；

（3）治理既涉及公共部门，也包括私人部门；

（4）治理不意味着只是一种固定的制度，而是持续的互动。

因此，治理更强调协调和合作，一般不应简单表述成一套严格的规则条例或正式制度，通常是以一种依托法规标准和协调机制，通过多组织、多部门横向协同配合与持续优化的过程，来实现行动目标。

最后，结合数据安全和治理的概念定义，从广义的社会层面和狭义的组织层面来理解数据安全治理：

从广义的社会层面治理来看，是指在国家整体数据安全战略指导下，依法依规整合多方相关单位共同参与、协同实施的一系列为实现既定目标活动的集合。其涉及的相关组织包括国家、行业、研究机构、组织及个人等多元实体。其核心活动包括持续建立健全相关法律法规、政策标准体系，创新数据安全关键技术，贯彻落实政策法规落地，培养专业人才，营造数据安全产业生态等。数据安全治理是以“让数据使用有序而安全”为愿景，构建形成全社会共同维护数据安全、促进数据开发利用和产业发展的良好环境，探索在我国易于落地的数据安全建设体系的过程。

从狭义的组织层面治理来看，数据安全治理是指从自身视角出发，多部门协作，推动合法合规使用数据的一系列活动的集合。其核心活动包括明确数据安全治理工作的团队及职责，规划制定相关制度规范，构建数据安全技术体系等。

源引国际咨询机构 Gartner（数据安全治理倡导者）的经典论述，“数据安全治理不仅仅是一套用工具组合的产品级解决方案，而是从决策层到技术层，从管理制度到工具支撑，自上而下贯穿整个组织架构的完整链条。组织内的各个层级之间需要对数据安全治理的目标和宗旨取得共识，确保采取合理和适当的措施，以最有效的方式保护信息资源。”，可进一步理解为依据顶层数据安全战略，从组织、人员、制度、工具等方面，内外部相关方协作实施的一系列治理活动集合，以确保数据安全。具体活动包括建立治理组织架构、建设和培养数据安全人员、制定数据安全制度规范、构建全生命周期技术防护体系等。类似的观点，微软提出了专门强调隐私、保密和合规的数据安全治理框架（DGPC），虽然没有明确指出数据安全治理的定义，但其核心思想指出：“数据安全治理理念主要围绕人员、流程、技术三个核心能力领域的具体控制要求展开，与现有安全框架体系或标准协同合作以实现治理目标，最终更好实现数据安全风险控制”。

在本白皮书中，更多强调的是狭义层面、面向组织的数据安全治理，通过治理活动，确保数据安全，推动发展与安全一体两翼、平衡发展。

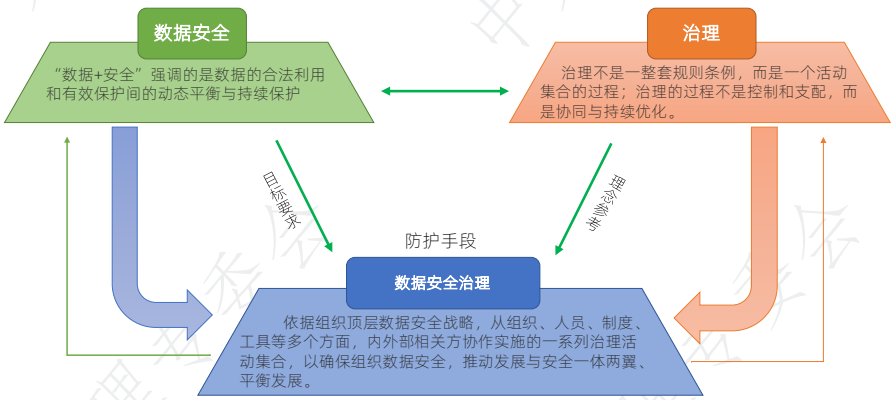


图 1-1　数据安全治理概念

1.2.2. 数据安全治理内涵

1.2.2.1. 数据安全治理内涵整体理解

通过对数据安全治理概念的梳理与理解，从多元共治、关注数据处理互动安全、重视管理与技术并举三个方面对关键要点的内涵进行解读：

（1）多元共治

与国家和社会治理的其他领域一样，数据安全治理面临的基本矛盾也是秩序与活力的矛盾，传统的数据安全防护体系主要偏向单纯的技术体系防护，如保密性、完整性、可用性等方面的技术防护措施，而对于社会伦理、法律合规、公共权益等问题关注度不够，鉴于数据安全的广泛性、普遍性与复杂性，面对数据安全领域的诸多挑战，需要整合国家、社会、组织及个人等多方主体资源，推动企业自治、政府监管、服务与市场调节形成合力，构建系统性、整体性、协同性的数据安全多元共治生态，更好地服务于数字经济发展，这也与《数据安全法》第九条中强调建立各方共同参与的工作机制相一致（“推动有关部门、行业组织、科研机构、企业、个人等共同参与数据安全保护工作”）。同样，对于治理主体而言，鉴于数据安全与业务的强关联性，数据开放流通与数据安全防护的天然矛盾，需要从战略层面出发，统筹安全与发展问题，协调解决业务、科技、审计、风控等各相关方的沟通障碍，统一数据安全共识、从管理和技术等多个方面，发挥各自优势，紧密配合，共同推进数据有序开发利用，促进数字化转型健康发展。

（2）关注数据处理活动安全

实施从以网络为中心转向以数据为中心的体系化安全保护策略。对数据进行有效识别并进行分类分级，针对数据的采集、传输、存储、提供、共享、公开、删除及销毁等处理活动进行梳理，根据不同的数据敏感等级以及数据处理活动状态，统筹规划与设置相应数据保护策略，实现不同级别数据的差异化、动态安全防护，有效贯彻落实数据的合法利用与有效保护，实现数据资产可知、流转可视、策略可管、风险可控，确保数据全生命周期安全。

（3）重视管理与技术并举

面对围绕数据处理活动的多方协同治理需求，组织在规划和开展数据安全治理工作时，需要依据数据安全治理的核心理念，从数据安全战略出发，明确各相关方的职权范围，制定相应的管理政策与流程，再通过技术措施落实安全防护策略。并能够根据安全形势、技术发展和演进趋势等的动态变化，对数据安全治理体系进行持续优化。在整体治理过程中，安全管理是安全技术的关键指导，安全技术是实现安全管理的基础支撑，通过管理和技术“双管齐下、深度融合”，解决数据安全保护问题。

1.2.2.2. 数据安全治理与社会治理的关系

随着信息技术和互联网的快速发展，超越传统意义上的数据储存、管理和分析能力的大数据在带来数据与信息处理方式的根本性变革的同时，也对社会治理产生了重要影响。2020 年 4 月 9 日，中共中央、国务院印发《关于构建更加完善的要素市场化配置体制机制的意见》，提出土地、劳动力、资本、技术、数据五个要素领域的改革方向和具体举措。数据作为一种新型生产要素写入中央文件

中，体现了互联网大数据时代的新特征。数据要素是数字经济时代的“石油”，数据流动能够活跃技术流、物质流、人才流、资金流，为数字经济创造价值。在这种背景下，数据安全就显得尤为重要。习近平总书记高度重视保障国家数据安全，强调“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”。因此，如何将数据安全治理融入社会治理，让二者相辅相成、相互促进，对于强化网络、数据等安全保障体系建设和推动数字经济发展具有重要意义。

一方面，社会治理是促进数据安全治理又好又快推进的关键环节。近年来，我国在筑牢数字安全屏障方面取得了众多瞩目的成绩，出台了包括国家安全法、网络安全法、密码法、数据安全法和个人信息保护法等在内的一系列法律法规，构筑起维护数据安全和促进数字经济持续健康发展的法律制度保障。但也要看到，在完善数据安全治理的过程中仍存在一些短板项，比如数据安全治理主体责任不明晰，企业数据安全治理流程及效果评价尚未形成统一标准，部分企业对数据安全不够重视，安全投入不足，层出不穷的新型网络攻击造成敏感数据泄露等。单纯依靠企业和个体自身的力量难以解决这些问题，必须加快探索构建起党委领导、政府负责、社会协同、公众参与、法治保障、技术支撑的数据安全社会治理体系，将数字安全治理从单向的“通办”、“统管”转为多元、交互、协同的“共治”。具体来说，首先，需要积极发挥政府和行业协会等主体作用，加强对数据安全治理规则、相关标准制定的组织引导，强化对企业数据安全的监督监管，确保关键领域和核心环节的数据安全。其次，进一步明确各类平台和企业等市场主体在数据安全治理方面的责任，提高居民个体维护自身数据安全的意识和积极性，同心协力维护数据安全，夯实数字经济持续健康发展的安全基础。最终，建立安全可控、弹性包容的数据安全治理制度，共同织密织牢国家数据安全网。

另一方面，尽管当前数据及其技术的融合应用在政府经济调节、市场监管、社会管理、公共服务、生态环境保护等各项工作中潜力无限。但由于数据作为新型的生产要素，具有体量巨大、类型众多、流通极快、易于编辑复制、多维复杂、不断裂变和虚拟性现实性紧密关联等新特点，传统的资源管理模式和安全防护手段难以完全适配和应对新技术带来的风险和挑战。因此，需要数据安全治理为社会治理模式创新提供有力的支撑和保障，并更好地赋能社会治理创新，推进政府治理体系和治理能力现代化：

第一，数据安全治理是促进社会治理体系变革的“牵引器”。数字化既是技术变革，也是组织与思想变革。数据已经成为连接社会万物的信息纽带，现实世界和虚拟世界之间的联系也变得越来越紧密。虚拟的数字印章和电子证照在现实世界得到普遍认可和使用，使得各类事务办理的效率大大提升；虚拟的数字货币在现实世界得到公开发行和推广，使得商品交易、货币流通和金融监管的成本大大降低。在这背后，离不开依托数据安全治理保障现实世界中不同利益主体的多样化安全需求，以及具备应对不同场景下的差异化条件的能力。举例来说，从行为规范角度，数据安全治理要求应用算法和数据必须保障虚拟空间的基本公共秩序，防止出现大数据杀熟、数字垄断、隐私泄露、数字欺诈等违法犯罪问题；从功能效用角度，要求算法、数据需要匹配现实世界的客观真实情况，避免产生算法偏见、算法歧视、“信息茧房”等消极负面影响；而从社会公益角度，算法和数据还应考虑人类群体的一般道德伦理，鼓励推广爱心通道、“适老”服务、弱势关怀等数字信息援助。总之，数据安全治理是进一步提升政府数字治理的文明程度，促进社会治理体系变革高质量前进的助推器。

我们应该通过数据安全治理合力建成共建、共享、共治的良好生态。

第二，数据安全治理是提升社会治理质量的“助推器”。当前，我国高度重视数字政府建设并取得了一系列成绩。从“推进数字政府建设”到“加强数字社会、数字政府建设”，深刻反映了国家对数据赋能社会治理的认识在不断深化。但我国是一个大国，地区的社会政治经济活动涉及诸多领域，具有范围大、规模大、情况复杂等特点。而过去的信息化建设模式千差万别，数据质量高低不一，脏数据、不完整数据等也层出不穷。因此决策者往往面临决策依据不充分、获取的信息不确定性大等问题。依托数据安全治理能够综合运用法律政策、技术手段、标准规范等各类工具，做到数据采集、存储、处理、共享、开放、开发利用等全链条数据活动的管理和监督，规范数据处理、提升数据质量、释放数据价值、防范安全风险，确保数据流通走向规范化、法律化、制度化轨道，实现从源头开始对数据质量层层把控，为共建共治共享提供安全、可信的载体、渠道和机制。使所掌握的数据真正的全样本、干净、有营养，能够实事求是地反映客观现实，基于高质量的数据进行建模、分析、决策和创新，必然事半功倍。

第三，数据安全治理是引导良好数字治理理念的“风向标”。数字技术在社会治理中的广泛应用，既有助于提升社会治理水平，也可能带来一系列非预期后果。由于数字技术本身并不足以保证社会治理的合法性、合理性和有效性。因此，我们需要依托数据安全治理构建社会治理数字化转型的坚实基础环境和有效约束空间。在社会治理现代化进程中，数据安全治理作为一种具有良好治理效果的重要方面，能有效促进社会治理参与者树立数据安全思维、转变治理观念、实现社会治理能力现代化的进步。所以应将数据安全治理紧密结合到社会治理决策、公共服务、社会监管以及社会民生保障等领域建设中，推进社会治理现代化。

以数据安全治理推动国家和社会治理的数字化转型是大势所趋，更是时代重任。目前，不论在理论还是实践层面，数据安全治理建设都处于初创阶段，还需要在治理技术创新、理论创新、制度完善等领域，进行深入探索和积极开拓，更好促进数字社会的健康发展。

1.2.2.3. 数据安全治理与数据治理的关系

数据治理是指从使用零散数据变为使用统一数据、从具有很少或没有组织和流程到企业范围内的综合数据流转、从尝试处理数据混乱状况到数据井井有条的一个过程；同时又作为组织中涉及数据使用的一整套管理行为，包括数据治理计划、监控、实施，通过对数据的梳理整合，利用数据驱动业务，实现企业增值。而数据安全治理则强调从战略层面形成由上而下贯穿组织总体架构的对数据安全治理目标的共识，关注数据处理全生命周期安全，重视管理与技术措施并举，并能够根据安全形势、技术发展和演进趋势等的动态变化，对数据安全治理体系进行持续优化。

目前，关于数据安全治理与数据治理的关系有两种主流的解读方式。一种以国际标准（ISO/IEC 38505）数据治理框架和国际数据管理协会（DAMA）的 DAMA-DMBOK 框架为代表，它们认为数据安全治理是整体数据治理的一个重要组成部分，数据安全治理是数据治理的一个子过程。另一种则认为数据治理和数据安全治理有一定的关联，但从本质上来说并没有直接的从属关系，二者是平行的方向，即数据安全治理可独立运作。

GB/T34960.5-2018《信息技术服务治理第 5 部分：数据治理规范》数据治理被明确定义为：“数

据资源及其应用过程中相关管控活动、绩效和风险管理的集合。”这项标准还进一步给出了数据治理的目标、任务和框架等：数据治理是“源于组织的外部监管、内部数据管理及应用的需求”；数据治理的目标是“保障数据及其应用过程中的运营合规、风险可控和价值实现”，“组织应通过评估、指导和监督的方法，按照统筹和规划、构建和运行、监控和评价以及改进和优化的过程，实施数据治理的任务”。

在数据治理的三点目标中，运营合规和风险可控是约束条件，价值实现是追求的结果，合规和风控既是使数据能最终实现价值的前提，同时又是必要的保障。为此，数据治理框架包含了数据管理和数据价值两套体系，前者统摄合规与风控，后者则支撑价值实现。在数据治理的框架下，数据安全是数据管理体系的重要组成部分，组织在实施数据治理的过程中，应“制定数据安全的管理目标、方针和策略，建立数据安全体系，实施数据安全管控，持续改进数据安全管理能力”。此处的数据安全概念相对狭义，基本仅限于为数据及其价值实现过程提供安全保障机制的范畴。

如果基于上述狭义的数据安全概念，将数据安全治理解读为以保护数据及其价值实现为目的而采取的风险评估和安全管控活动，那么，数据安全治理就可视作数据治理概念下专注于安全方面的子集。但从实际操作上来看，两者之间又有很大的不同：

（1）从发起部门来看

数据治理主要是由 IT 部门在驱动，而数据安全治理主要是由安全合规部门在驱动。当然两者的成功都要涉及到业务、运维和管理部门甚至公司最高管理决策层。

（2）从目标上看

数据治理的目标是数据驱动商业发展，管理企业的数据资产，提升企业数据资产价值。数据安全治理的目标是让数据的使用更安全，保障数据的安全使用和共享，实质也是保障数据资产价值和促进数据要素价值释放。

（3）从关注点上看

数据治理关注于数据本身的组织以及数据使用传输、业务支撑等场景下的质量、规范、流程与制度等，数据安全治理则关注于数据在整个生命周期可用性、完整性与机密性的安全保护。

（4）从工作内容产出上看

数据治理工作产出的一个核心成果就是数据质量提升，通过对数据进行清洗和规范的过程，获得高质量的数据。数据安全治理的重要产出包括完成对企业数据资产的分类分级，制定合规的安全访问策略并规划适宜的管控措施。

（5）从数据资产梳理上看

数据治理中的主要产出物是元数据，即赋予数据上下文和含义的参考框架。数据安全治理中的资产梳理，则要明确数据分类分级的标准，弄清敏感数据资产的分布、授权和访问状况。

（6）从结果看

数据治理是数据质量的提升，通过数据的清洗、规范，获得有价值的数据，而数据安全治理是基于数据分类分级实现数据的动态防护，保障数据有序流动。

尽管当前在数据治理中也在不断加强对数据安全方面的要求，但相对数据安全治理而言，数据治理中的安全实践还是常被置于从属角色，如同信息安全在信息化建设中的角色一样，不够系统和

深入。近年来，随着包括大数据在内的数据在数字化社会中的重要性不断提升，国家已将数据上升到新型生产资料和创新要素的高度，数据对安全形成影响的广度和深度已超越单纯为数据掌握者保护数据自身价值的范畴，例如对个人（数据主体）隐私保护的问题就牵涉到了社会伦理以及关于数据权益的法律认定，而数据出境等问题更是需要在国家安全层面全盘统筹考虑。

因此这里的数据安全治理将主要关注以保护数据及其价值实现过程安全为目标的风险管控活动，以达到数据开发利用与安全防护的“一体两翼，双轮驱动”的平衡发展。具体到合规性方面，则将以全面覆盖和满足国家关于数据安全的所有法律、法规、政策、规范和标准的要求为目标。数据安全治理工作既可在数据治理的框架下作为一个环节或子过程来开展，也可直接依照本书提出的数据安全治理框架独立实施。

1.2.2.4. 数据安全治理与数据安全管理的关系

“治理”如前述定义，是一种通过多组织、多部门横向协同和配合与持续优化，以达到通过治理有效平衡数据开发利用与数据安全保障的一体两翼平衡发展。

“管理”对应的英文单词则是“management”，是指为达到组织的既定目标而以人为中心对组织拥有的资源进行有效的决策、计划、组织、领导和控制的过程。更强调的控制和执行，通过自上而下的制度和规范的垂直管理落地，达到安全防护目标。通常会以形成制度和条例规范的形式加以表述和落实。

在数据安全范畴内，使用“数据安全治理”的概念比使用“数据安全管理”能够更好地适应当前的现实情况：一方面，人类正在全面跨入数据时代，为积极顺应这一势不可挡的历史潮流，国家和各层级的组织机构都迫切需要加强数据保护的意识，尽早启动和落实关于数据安全的准备和建设工作；另一方面，人类也仅是刚刚看到数据时代和数字化社会形态特征的端倪，数据无论是作为资产、生产资料，还是创新要素，都是方兴未艾的新事物，必然要经过一个认知逐渐深入和全面的复杂过程。因此，在这个过程中，鉴于数据安全与业务的紧密联系，数据安全的复杂性，使用治理而非管理的思路来指引数据安全建设，无疑拥有更好的灵活性、丰富性和包容性，因而也更有利于平衡对数据进行安全保护和在数据使用和价值挖掘方面激发创新。

1.3. 数据安全治理面临挑战与需求

数据安全治理覆盖管理、技术、运营、评估等多个方面，是一项需要多方联动的复合型、系统型工作。组织数据安全治理能力建设，围绕数据的产生、加工、使用、流通、销毁等环节，进行总体布局、全面规划，需要构建贯穿各层面的数据安全治理组织架构，全面梳理业务场景并设计体系化的安全制度流程，配合应用自动化工具、平台，实现数据安全治理“一盘棋”。同时，组织可通过搭建专业的人才梯队与培训机制，为数据安全管理工作持续积蓄力量。数据安全治理不仅限于解决当前的数据安全困境，还致力于数据安全长远发展，是一项长期工程。通过不断优化制度流程落地效果、提升技术与产品应用水平、强化人员安全意识与能力、明确未来数据安全治理发展方向等，实现数据安全治理的全生命周期闭环。数据安全治理工作的复杂性导致现阶段存在多方面的挑战无法满足。

1.3.1. 贯彻数据安全战略顶层规划需要布局

在顶层规划方面，伴随法律法规的颁布和各种政策文件的发布，国家数据安全的战略日趋明确，一是在数据安全供给侧，数据安全治理相关的隐私计算等核心关键技术要持续提升以逐步满足商用化需求，数据确权、数据公平交易、数字信任体系等技术也需完善，促进产学研深度融合，培育数据安全领军企业和数字化安全人才队伍，是落地国家整体战略规划的重要任务。二是数据安全治理关系业务开展、法规要求、技术建设、持续运营等多个维度，需要进行顶层规划，全面布局。

但是，面对各个环节的数据安全风险，组织当前缺乏落实国家数据安全顶层战略的方针，亦尚未形成一套规范的、行之有效的数据安全管理机制，导致在响应相关法律法规要求还存在很大的挑战。一是大部分企业不具备研究制定数据全生命周期安全治理的愿景、目标、领域、指导原则、责任模型和保护能力等水平，无法为数据安全建设提供统一指引。二是数据安全治理是需要综合考虑业务当前与未来发展需要，为保障数据安全所开展的一项系统工程，在为确保内部对数据安全治理的方针达成共识、合理配置数据安全工作任务与资源、如何评估投入产出比等方面，尚缺少有效的支持方法和评价依据。三是数据的动态性要求组织及时根据政策合规与制度规范提升需求，滚动修订数据安全的制度、流程、标准，保障数据安全的规划、实施、运行、监督的全程管控，持续提升数据安全能力，在管理和技术措施尚不完善的现状下，闭环管理落地困难。

1.3.2. 跨组织、部门全员协同治理需要加强

在组织协同方面，组织内部的数据与业务紧密联系，数据安全需随数据活动场景变化随需而变，数据处理活动涉及多个部门，内部组织和协调难度较大。主体多元、利益多元，组织内数据安全与发展、秩序与突破，诸多价值目标在这一问题上交织碰撞，如何满足内部和外部各方利益关系，实现数据开发利用和安全合规的平衡需求的满足度，成为保障数据的共享和开放的需求。从法律层面上讲，当前数据权属相关的法律法规和实施细则尚未颁布，在这样的前提下作为数据使用者如何向外部组织或者个人的数据所有者落实数据管理义务，是组织亟需解决的需求。从实际落地层面上讲，作为数据所有者，通过交换、共享、委托等处理活动对外提供的数据流出了自己可控的安全域，对于此类数据的防范属于自身技术防护的“盲区”。作为数据使用者，在使用数据中，如何落实外部组织或个人的数据所有者提出的数据安全管理义务，并提供合规性检测证明，以及网络安全事件发生后的安全取证、责任鉴定等对数据流转过程中的数据监管需求强烈。

由于数据作为特殊资产，其所有权和使用权分离的特性，导致在数据共享交换层面面临着无法满足其安全共享和开发的困境。在数据通过共享、交换等过程离开组织之后，数据的跟踪与溯源问题变得愈加困难。如何统筹各相关部门的治理授权和责任，落实数据从产生、使用到流转全生命周期中各环节责任主体，强化分行业和跨行业协同治理，完善分类、分级的安全管理要求以及追责机制等配套制度成为行业面临的共同挑战。

1.3.3. 个人信息合理利用与权益保护需要重视

在关注热点方面，对个人信息资源的合理利用和保护，是构建数字经济社会，繁荣数据要素市场的必由之路。各级组织在个人信息合理利用和开发过程中需要遵守众多的法律法规和标准，如《个人信息保护法》《欧盟通用数据保护条例（GDPR）》等，因此需要尽可能收集与之相关的各类法律法规和监管要求，确保他们在个人信息的合理利用过程中符合所有适用的法规和标准，同时，建立确保其拥有、使用和共享的个人信息得到保护、可追溯和可控制的技术手段、管理制度和运营机制，以符合监管要求，避免面临高额罚款和声誉损失。

但个人信息保护与合理利用间也存在较大矛盾和冲突，如何对个人信息的保护和利用做出合理规范还存在合规性、监管、个人隐私保护和个人信息治理等多方面的挑战。由于个人信息的规模和复杂性使得其安全治理变得非常困难，一方面组织的个人信息可能不准确或者存在噪音，这可能导致分析结果出现偏差或错误，进而影响个人权益；另外一方面，组织出于商业目的等，可能将数据交由第三方进行研究或分析，导致数据被滥用或不当使用，出现“大数据杀熟”或“算法歧视问题”，或者为了吸引用户粘性，制造“信息茧房”，束缚用户可接触的信息范围。

1.3.4. 面向行业特点的场景化治理需求凸显

在行业特性方面，数据安全治理的行业属性十分突出，是因为数据要素是在特定行业背景下产生的，反映了该行业相关的信息和现象。举例来说，教育行业的数据要素包括学生的学籍、学校的教务和实验记录等，这些数据要素反映了从学生入学到就业、学校教学和科研等特定需求和工作流程。同样，金融行业的数据要素包括交易记录、股票价格、汇率数据等，这些数据要素反映了金融行业的市场情况和交易活动。在不同行业间由于业务运转模式不同、数据特性和数据价值差异，导致其面临的网络安全威胁和行业监管差异化也非常大。因此，了解数据要素的行业属性对于正确理解和实施数据安全治理具有重要意义。在特定行业中，行业特定的场景也需要特定的技术和工具来处理和分析。

由于不同行业之间的信息化发展水平的不同，以及针对数据重要性的定义和认知差异较大，导致在数据安全治理中，无法使用通用的手段进行治理。针对数据运营者，面临着如何定义数据要素的行业属性并选择合适的技术和工具进行数据安全治理的挑战。而数据安全产品和数据安全服务企业方面，则面临着大量差异化行业的场景产生的复杂的数据形态，以及数据多来源、多协议、异构化、多模态、高并发的现象，研究和开发适合行业属性的数据治理工具的难度极大。其次，数据治理由单系统单领域走向跨系统全领域，开展行业级或区域级的数据安全治理工作中，跨层级、跨地域、跨系统、跨部门、跨业务成为显著特征，对数据治理方法和平台研制都带来了新的挑战。

本白皮书在编制数据安全治理主册的同时，面向政务、金融、医疗、电信、电力、教育、工业七个行业，同步推出行业数据安全治理实践篇，以为不同行业的用户在开展数据安全治理过程中提供参考和借鉴。

1.3.5. 数据分类分级自动化、精准化亟待解决

在基础支撑方面，实行数据分类分级是保障数据安全的前提，也是实施数据风险评估、数据安全策略制定、数据权限控制等数据安全治理过程中极为重要的一环。在实际进行数据分类分级的过程中，需要结合业务流程进行考虑，不同的部门或单位采用不同的数据分类标准，不同类型的数据可能存在交叉或重叠，并且数据分类分级是一个持续的过程，基于数据伴随业务处理活动的持续新增与变化，分类分级也需随之动态变更。然而目前缺乏分类分级的标准化工具，几乎所有情况下都需要人工对数据进行手动分类分级，导致效率及准确度低下。实现数据分类分级的自动化、精准化需要借助分类分级标准的统一及在此基础上研制自动化的工具来逐步解决。

1.3.6. 治理水平稽核评价体系需要建立健全

在治理评价方面，需要在促进数字经济发展与数据安全保护之间把握好动态平衡，持续探索构建原则性与灵活性相结合的新型监管体系。需要进一步完善数据安全测评标准体系，建立和完善数字技术应用审查机制，开展算法规制、标准制定、安全评估、伦理论证等工作。一方面，避免因监管的越位导致阻碍创新，影响数据资源的开发利用和数据依法有序的自由流动，另一方面，避免监管机构出现“监管迷茫”和“能力缺失”，在现实中演化为弱监管和慢监管甚至不敢和不会监管，造成监管的失位。

目前，针对组织的数据安全监管工作大多通过访谈评估、人工检查等形式开展，不可避免的面临着效率低下、难以量化和标准化的问题。针对敏感数据识别、异常行为监测、敏感数据泄露、非法越权访问、数据跨境传输、数据非法外联等核心检查内容，目前采用的漏洞扫描、流量探测、API接口分析等技术，也无法全面支撑自检查评估与第三方检查评估的监管实际工作需要，需要持续研究突破自然语言处理、数据血缘分析、算法合规性检测等技术在合规项解读、自动化检测、全链路流转监测等涉及监管的应用能力，提升数据安全检查、评估的自动化水平，实现以评促建，有效提升组织的数据安全治理水平。

1.4. 数据安全治理理念日趋成熟

在《数据安全治理白皮书 4.0》中，基于 Gartner 的数据安全治理架构（DSG），提出并诠释了数据安全治理的愿景、目标及核心理念。伴随数据安全治理的深入，围绕“让数据使用有序而安全”的治理愿景与“满足数据安全保护、合规性、敏感数据管理”的治理目标，面对数据安全治理的新形势、新挑战，进一步完善“个人信息保护与合理利用”的需求覆盖，突出“全员协同治理”的重要性，强调面向行业特点的“场景化安全”，健全从评估、建设、运营到监督评价的闭环治理体系。旨在持续推动数据开发利用与安全防护的一体两翼发展，并在我国易于落地的数据安全治理的体系化方法论。

（1）满足安全合规（Compliance）、数据发展与安全（Development and Security）、个人信息合理利用与保护（Privacy）三个需求目标；

（2）核心内容包括：数据分类分级（Classifying）、敏感个人信息识别（Identify）、风险评估（Risk Assessment）、场景化安全（Scene）；

（3）数据安全治理的建设步骤包括：组织构建、资产梳理、策略制定、过程控制、行为稽核和持续改善；

（4）核心安全框架为数据安全人员组织（Person）、数据安全使用的策略和流程（Policy&Process）、数据安全技术支撑（Technology）。

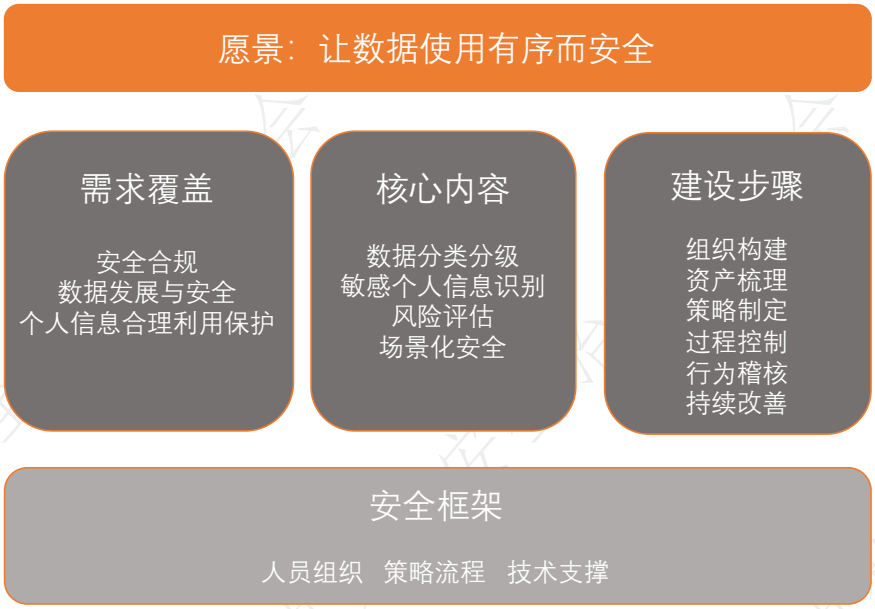


图 1-2 数据安全治理理念

1.4.1. 数据安全治理愿景

《网络安全法》“第三十三条 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用”，为关基信息系统安全技术措施落地应贯穿信息系统全生命周期提供依据。

《数据安全法》对数据的安全和发展在国家层面给出明确指示，“第十三条 国家统筹发展和安全，坚持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。”

《个人信息保护法》：“第一条 为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用，根据宪法，制定本法。”

根据以上三部法律相关条款，将治理愿景更加清晰地表述为以满足数据安全和个人信息保护的合规要求为基础，尽可能发挥数据价值，促进数据安全有序流动，提高全员安全意识，更好地为建设数字中国服务，不断提高数据安全治理水平。

1.4.2. 数据安全治理目标

（1）安全合规

国家层面对数据安全和个人信息保护更加重视，国家及行业涉及数据安全相关法律法规标准持续推出与完善，安全合规要求持续增加，监管力度不断加大，监管内容不断细化，面对众多的法律法规标准条文，需要围绕管理和技术要求进行解析，寻找合规途径，落实合规措施。

法律法规是指引数据安全建设的重要依据，应对解读的安全标准和规范的合规项进行落实，形成合规库，收录并拆解各类与数据安全相关的规范、标准，为数据安全管理提供参考及评估标准，并根据合规库中的合规项制定各类安全策略规则。

（2）数据发展与安全

数据作为新型生产要素，其强流动性是产生和释放数据价值的前提，针对数据广泛流动过程中可能产生的数据泄露、篡改、破坏、非法利用等风险，如何采取有效的防护手段，保障开发利用与安全防护的一体两翼、双轮驱动发展，促进数据有序流动是数据安全治理的关键目标。

（3）个人信息合理利用与保护

随着个人信息价值的凸显，个人信息收集乱象突出，个人信息泄露事件频发，个人信息滥用程度严重，极大地威胁了公民财产以及个人身份信息的安全，甚至危及国家安全。国家高度重视个人隐私保护，密集颁布系列法律、法规、标准保障个人信息安全。对个人信息进行有效治理，促进个人信息合理利用与保护个人隐私并重，成为又一关键目标。

1.4.3. 能力支撑框架设计

数据安全治理绝非是平地起高楼，与网络安全和数据治理既有紧密的关联性，又有面向数据的独特性，整体框架需要多体系间融合展开治理。

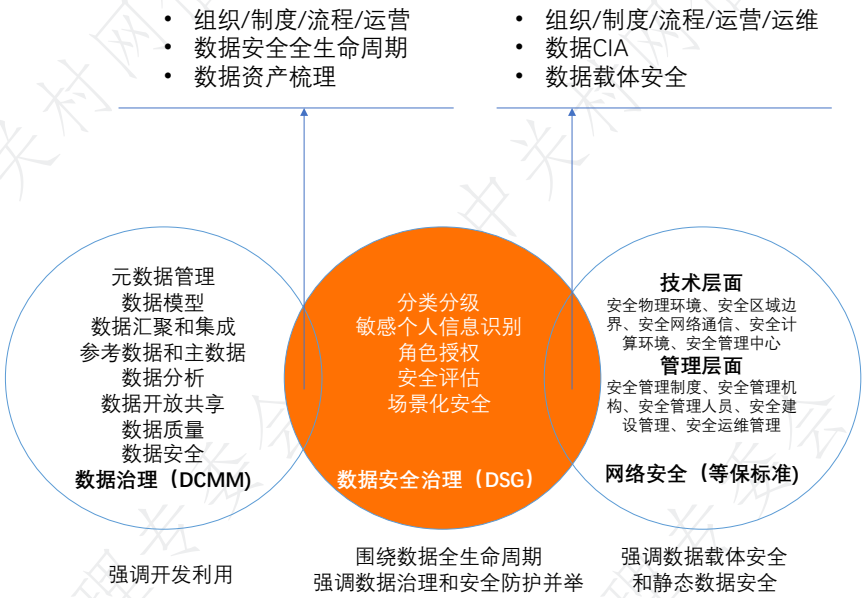


图 1–3　能力支撑推动数据安全治理框架设计

数据安全治理是以数据为中心，其核心思想是面向业务数据流转的动态、按需防护。

在防护技术上，仍需依托网络安全中面向网络、设备、应用等数据载体的静态防护能力，扩展面向数据流动的分类分级动态防护能力。

在安全管理上，在网络安全管理体系的基础上，补充、完善面向数据安全管理制度、策略和运营规范，形成围绕数据本身和数据载体的整体数据安全防护能力。

在与数据治理的关系方面，数据分类分级是基础，通过对数据资产的识别与梳理，与数据治理中的元数据管理进行集成打通，直接获取统一的数据标准，作为数据分类分级的资产标识，提高数据梳理准确性，避免重复工作，形成面向数据应用的数据治理体系与面向数据安全的场景化安全治理体系的融合与统一。

数据安全治理能力划分为“人员组织、策略流程、技术支撑”三个核心能力领域。

人员组织：建立数据安全治理团队，并明确团队中各成员的管理职责，团队组成依组织的具体情况，可以是实际存在的也可以是各部门成员组成的虚拟团队，是数据安全治理工作开展的基础资源保障。

策略流程：设定相关的管理制度、标准规范、管理策略及流程，并围绕策略流程，构建运营管控机制，以运营思路开展数据安全治理工作，充分考虑与网络安全管理的融合，实现“可持续化的数据安全治理能力”。

技术支撑：落实策略流程贯彻所涉及的数据全生命周期的数据安全防护技术建设，并融合数据治理和网络安全相关技术，形成完整的技术支撑体系。

组织内部通过专业的数据安全治理团队、明确的数据安全治理策略和流程、全面的数据安全运营机制、覆盖数据全生命周期的技术手段为支撑，围绕数据使用的业务场景活动，分析安全需求，同时加强数据安全宣传、培训、教育，提升数据资产的体系化保障能力。

组织一方面应遵守法律法规、国家和行业标准、借鉴行业数据安全最佳实践，另一方面要积极配合国家、行业主管单位和集团的数据安全检查，健全数据安全监督评价体系，这是多元治理的重要一环。

第二章　数据安全治理整体框架

依据数据安全治理理念，围绕以数据为中心的治理体系不断演进、深化，组织在整体安全战略指导下，形成以数据分类分级为治理基石，数据安全管理体系、技术体系与运营体系为治理核心，监督评价体系为效能促进，形成更为完善、合理、全面的治理框架。

2.1. 整体框架设计思路

数据分类分级与敏感个人信息识别可明确数据保护对象，是开展差异化、动态化数据安全治理的前提。数据安全管理制度体系是开展多元化安全治理工作的先导。数据安全技术体系是在数据处理活动中落实安全技术需求与工具支撑。数据安全运营体系将管理和技术体系进行有效衔接，实现持续化防护。通过管理、技术、运营体系三位一体、有机融合，数据安全治理形成以动态数据安全管控策略为中心，以管理体系为驱动，以运营体系为纽带、以技术体系为落地支撑的治理核心。数据安全监督评价体系则是指对数据安全治理情况进行总体的监督、稽核与评价，从而有效促进规模较大组织的治理水平提升。

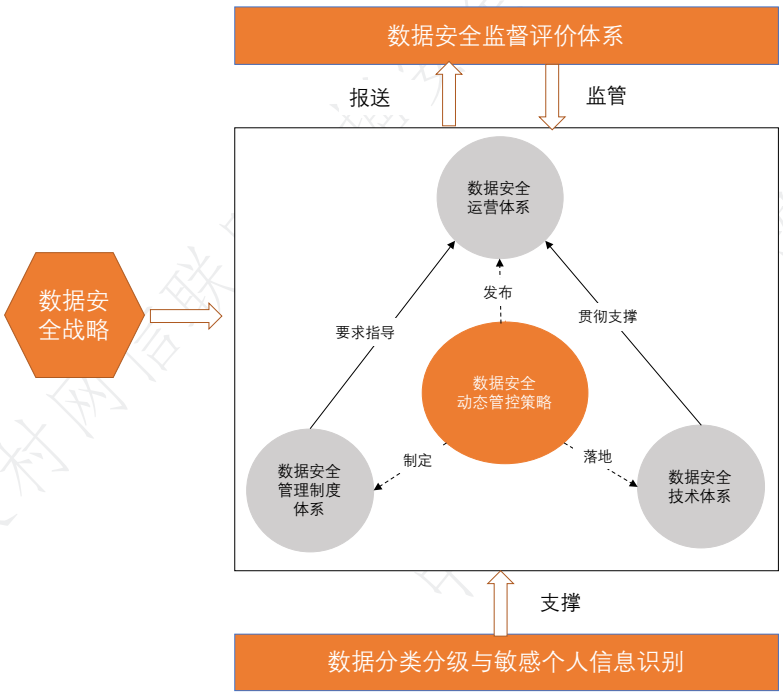


图 2–1　数据安全治理体系之间的联系

依据上述治理体系的构建思路，从数据安全战略出发，以数据分类分级与敏感个人信息识别为支撑，构筑数据安全管理体系、数据安全技术体系、数据安全运营体系与数据安全监督评价体系的整体数据安全治理体系框架。

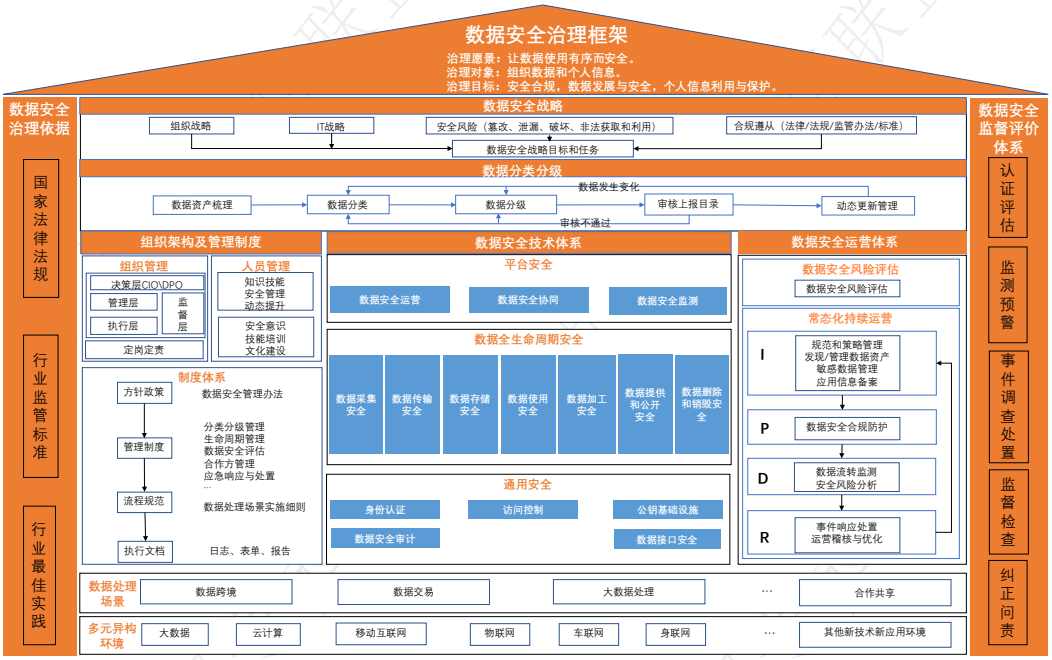


图 2–2　数据安全治理的总体框架

在数据安全战略方面，需要从组织战略、IT 战略、安全风险（篡改、泄露、破坏、非法获取和利用）、合规遵从（法律 / 法规 / 监管办法 / 标准），四个方面综合平衡考量，形成组织的数据安全战略目标和任务，指导整体数据安全治理建设。

数据分类分级是数据安全治理体系的基石，面向组织数据和个人信息，首先需开展数据资产的发现与梳理，然后基于识别备案的数据资产，落实从业务角度出发的数据分类标识以及从安全角度出发的数据定级标识，形成数据分类分级目录，最后对数据目录进行审核、发布，基于数据伴随业务处理活动的持续新增与变化，分类分级也需随之动态变更。

面向数据安全多元化治理特点，落实人员组织架构和管理制度体系，建立覆盖决策、管理、执行与监督等多层级的组织架构，各级部门协同配合工作，定岗定责落实治理行动；在人员管理维度，需注重能力的培养与提升，并加强安全意识教育；在管理制度维度，需围绕数据处理活动，构建从方针政策、管理制度、流程规范到执行文档的层级全面的制度集合，并伴随治理过程持续进行优化与调整。

在技术体系方面，基于分类分级成果，构建通用安全、数据全生命周期安全、平台安全的技术防护体系，明确各层级的安全技术保护要求。

在运营体系方面，展开定期或由特定数据处理场景触发的数据安全风险评估，基于经典 IPDR 理论，分别从识别、防护、监测与响应处置及优化四个维度出发，形成常态化、集中化、规范化的数据安全运营。实现事前预防、事中管控、事后审计溯源的持续、全面数据安全防护。

在监督评价体系方面，行业主管单位通过评估认证、监测预警、事件调查处置、监督检查、纠正问责等活动实现数据安全治理。

鉴于数据与业务的紧密联系，数据安全技术不能是孤立的和外挂的，应是嵌入的和内生的，在整个信息系统的规划组织、设计开发、实施交付、运行维护与系统废弃的全过程中，都需同步规划、

同步建设、同步使用，围绕数据跨境、数据流通交易、大数据处理、合作共享等众多典型数据处理场景，面向大数据、云计算、移动互联网、终端、物联网、车联网、身联网等复杂多元异构环境，方能真正实现数据使用的“贴身保镖”。

2.2. 规划数据安全战略

数据安全战略是推动数据安全整体工作的置顶要求，组织在实施数据安全治理工作之前，首先需要制定积极、有效的数据安全战略，并按战略要求指导数据安全防护体系建设，这对保障数据安全防护效果至关重要。

战略目标与总体任务设定应考虑提高安全价值的四个基本观点：经济、系统、长远、动态，符合经济学规律，如：安全成本（安全投资、安全投入）、安全收益（安全价值）和安全效益，用有限的安全投入实现最大的安全，在达到特定安全水平的前提下尽量节约安全成本。

组织的业务战略、IT 战略、风险容忍度和合规遵从是制定数据安全战略的关键要素，其中：

（1）业务战略：需要保持与业务发展战略、数字化转型战略的制定和实施统一。

（2）IT 战略：需要保持与整体的信息化战略同步。

（3）安全风险：对数据被篡改、泄露、破坏、非法获取和利用的安全风险容忍度。

（4）合规遵从：面临的法律、法规、监管办法、标准的合规要求。

在制定数据安全战略时，需要基于上述四个要素，充分考虑业务发展需求与风险、威胁、合规性的平衡，明确数据安全治理的总体目标、关键性原则、适用的对象和场景范围，阐明实现目标的主要战略以及所要遵守的相关合规性法律、法规及标准要求，形成基于目标的治理规划与任务。

其中，安全合规作为重要的数据安全治理驱动力，是指导数据安全治理建设的重要指引，也是业务开展的约束项，对相关法律、法规及标准的相关合规要求的详细解读参见“第三章 我国相关法律法规及标准解读”。

2.3. 开展数据分类分级

数据分类分级保护是我国数据安全管理基础制度之一。数据处理者应对数据进行分类分级，根据数据的密级和敏感程度制定不同的管理和使用策略，尽可能做到有差别和针对性的防护，避免敏感数据的防护不足，非敏感数据的过度防护。

分类是依照数据的来源、内容和用途对数据进行分类；分级是按照数据的价值、内容的敏感程度、影响和分发范围不同对数据进行敏感级别划分。

数据分为一般数据、重要数据、核心数据，不同级别的数据采取不同的保护措施。

国家对个人信息和重要数据进行重点保护，对核心数据实行严格保护。

分类分级更多是依据标准，对业务数据进行定义的过程，是一个研究审批的过程。数据处理者不应该只是形成一份数据资产清单就结束了，因为数据是动态和流动的，业务也是不断新增和变化的，分类分级清单也会不断变化，应建立符合分类分级和审核上报目录的闭环流程，并按照数据的敏感

程度和密级制定防护策略。

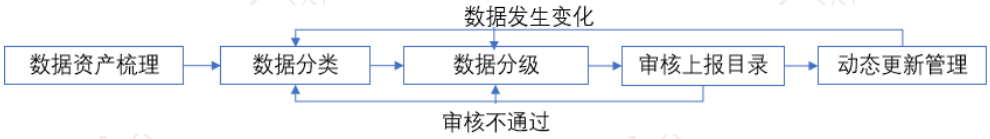


图 2–3　分类分级流程

个人信息处理的前提是敏感个人信息识别，识别是依据制定的分类分级标准，在业务处理流程中，更多依靠自动化的装备与系统进行标记或标签化的动作。综合个人信息的处理目的、处理方式以及可能对个人权益造成的影响等方面，判断构成敏感个人信息的处理行为，敏感个人信息包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

2.4. 组织架构及管理制度体系

2.4.1. 组织架构

数据安全治理需要从组织的战略层面出发，协调管理层、执行层等各相关方，打通不同部门之间的沟通障碍，统一内部数据安全共识，实现数据安全防护建设一盘棋，这也与《数据安全法》中强调建立各方共同参与的工作机制相一致。以安全合规为基础，数据开发利用与安全保护为目的，涉及国家、行业、组织及个人共同参与的多元化主体共同参与工作的数据安全治理需求愈发明确。

数据安全组织，就是数据安全治理策略从制定到落地，并持续优化改进的组织保障。数据安全组织架构建设和管理是数据安全治理工作开展的基础。以数据为中心，面向业务场景，纵、横向拉通各部门间的合作，合理定岗定责定员，明确职责分工，为数据安全治理的健康可持续发展提供支撑。

面向数据安全，组织内部通常设立数据安全治理委员会或数据安全治理小组来负责对数据安全治理工作的管理、执行和监督。团队职责在于对数据进行分类、分级、保护、使用和管理原则的制定。团队成员应包括内部的数据安全专家，以及所有与数据安全有关部门（如 IT 支持、人资、法律、财务、业务和市场、运营和维护、知识产权、风险管理、审计、保密等）的人员代表；在一些大型的组织中，因为数据安全正日益变成影响发展的重要因素，数据安全治理委员会或数据安全治理小组成员甚至会包括主管副总裁、董事会成员等高级管理人员。数据安全治理团队的成员同时也是数据安全制度的受众。他们是数据安全策略、规范和流程的执行者和被管理者，同时也是数据的使用者、管理者、维护者、分发者。只有将这些角色的人员代表纳入到团队中，才能使得在数据安全治理中制定的安全原则、安全措施和安全规范能够在具体执行中得到有效贯彻落实。

数据安全治理组织自上而下包含决策层、管理层、执行层，另外还存在一个贯穿整个数据安全治理过程的监督层对整个过程进行监督、审计。人员不应出现交叉，即一个人不可同时担任两个层级中的角色，避免出现因受利益和工作方便影响从而降低或绕过标准的情形。团队内部每个人应分配满足工作要求的最小权限，不可因管理因素而获得超出角色范围的权限。团队内部的关键岗位应设立“双人双岗，权限分离，互相监督”机制，即在工作过程中相同岗位应最少设立两名人员参与，

权限分离，互相监督，同时对结果负责。各层的岗位如下：

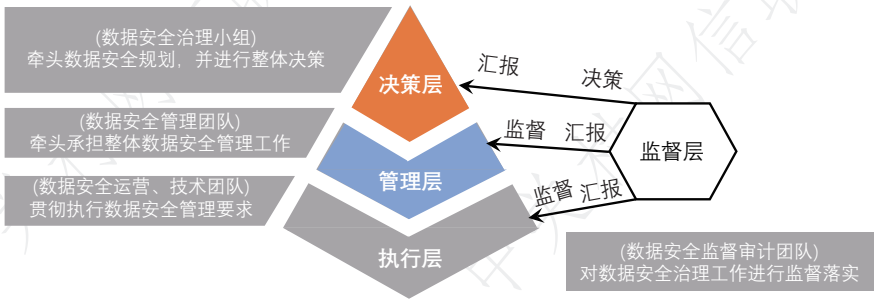


图 2–4　数据安全治理团队的职能架构

2.4.1.1. 决策层

决策层作为数据安全治理组织的顶层决策层，也是数据安全管理工作的决策机构，一般成员会包括组织内主管数据价值实现的最高负责人（如首席运营官、首席战略官等），或者信息安全方面的最高负责人（如首席信息官、首席信息安全官等），甚至可以考虑由负责推动数字化转型的高级副总裁、负责战略新兴业务拓展的高级副总裁来出任决策层的组长。比如：数据安全管理委员会领导小组建议由分管数据安全的高级管理层及相关部门负责人担任，并作为直接责任人，牵头数据安全规划，参与到业务发展决策，主要职责包括：

（1）制定组织的数据安全战略目标和任务；

（2）负责统筹、规划数据安全分级工作，并对其它数据安全建设提供必要的资源支撑；

（3）指导管理层数据安全工作的开展；

（4）负责对重大数据安全事项进行协调以及统筹决策；

（5）对数据安全策略和规划，制度与规范等进行发布；

（6）对组织开展和实施数据安全治理的体系目标、范围等进行决策。

2.4.1.2. 管理层

管理层在组织数据安全治理中具有举足轻重的地位，基于决策层给出的策略，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，保障数据安全全面落地工作，是开展数据安全工作最核心的部门或岗位，同时牵头承担单位整体数据安全管理工作，落实数据安全保护责任，对数据安全提出具体管理要求，一般由数据安全部门、数据资产管理或者数据治理部门牵头，协调各相关部门开展数据保护工作，监督数据安全管理制度和措施落地执行情况等，主要负责数据分级相关工作的组织、管理、审查、统筹协调等工作，具体如下：

（1）牵头对组织现有的数据资产进行梳理，调研分析数据使用部门与数据安全有关的业务需求、安全风险等；

（2）组织制定数据安全管理策略、规划、制度和规范，并推动在组织内的推广和落地实施；

（3）负责数据安全治理体系的建设、运营维护等工作；

（4）组织开展数据安全风险监测、预警与应急处置；

（5）组织开展数据安全教育宣贯培训，提升员工数据全保护意识与技能；

（6）对执行层进行管理，并提出数据安全要求；

（7）组织开展数据安全评估和审查；

（8）统筹建立数据安全应急管理机制；

（9）保持外部沟通，包括国家及行业监管、第三方咨询服务商（安全咨询、安全厂商）、测评机构（认证及认可机构、安全测评机构）；

（10）维护数据安全制度持续运转的保障工作，并及时做出更新、调整和优化，以更好适应和支撑业务发展。

2.4.1.3. 执行层

执行层与管理层是紧密配合的关系，面向组织的数据安全场景、数据安全分级工作等，执行层需要协助管理层详细了解并深入理解组织在业务开展过程中的各种数据安全需求，需要认真贯彻执行管理层提出的明确的数据安全要求，对设定的流程进行逐个实现，就数据安全执行情况和重大事项进行汇报，对管理层提出的数据安全操作规程等制度和方案的可行性和易用性，进行细致的分析和评估，并将结果反馈给决策层，以支撑后者做出明智、正确的决策。

数据安全制度正式发布实施后，执行层要在其日常例行工作中严格遵守数据安全操作规程，并积极发现和报告制度规范中的漏洞和潜在风险，促进管理层及时响应，尽快对数据安全的制度和措施做出更新、调整和优化。

执行层一般由业务部门、数据安全技术保护部门组成，考虑到数据应用场景不同，范围有可能扩充，比如：某金融单位执行层由科技、业务、法律合规、风险管理等部门具体数据安全岗位相关工作人员构成。他们是数据的使用者、管理者、维护者、分发者，同时也是数据安全策略、规范和流程的重要执行者和管理对象，负责落实数据安全标准，主导或协同实施数据安全防护和事件处置，落实数据安全运营工作，如：制定、发布和更新数据安全管理制度、规程与细则；组织开展数据分级工作，识别并维护数据资产清单；组织开展数据安全风险评估；制定个人信息保护政策和相关规程；监督内外部（合作方）数据安全管理情况等。

2.4.1.4. 监督层

数据安全治理工作的顺利开展，离不开各部门工作的协同配合，更离不开完善的监督审核机制，监督层人员必须具备独立性，不能与其它管理小组、执行小组等人员共同兼任，确保其审计核查工作不会受到来自其他三层，特别是管理层和执行层的相关利益或动机的影响和干扰，从而保证组织能够及时发觉其数据安全制度在落地执行层面的问题和风险。监督层负责定期将管理层、执行层数据安全工作情况进行监督，并向决策层进行汇报，对数据安全治理工作进行监督落实。监督层一般由风险管理、内控合规和审计部门组成。主要职责包括：

（1）定期对数据安全方面的制度、策略、规范等的贯彻落实和执行遵守情况进行考查与审核，并将结果汇报给决策层；

（2）对数据安全工具执行有效性监督；

（3）对数据安全风险开展监控与审计。

2.4.2. 人员管理

人员管理是组织管理的核心内容，管理的精要是将合适的人员配备到合适的职位上，并让其从事合适的工作，从而实现“人适其位，位得其人”，这也是数据安全管理体系的重要一环，主要体现在两方面：一方面是人员流动管理，另一方面是人员安全意识和综合素质培养管理。组织机构的数据安全策略、制度流程等的落实和推进离不开工作人员的参与和执行。由于组织机构内不同部门、不同层级及不同来源的员工，其工作难免需要在不同场景下直接或间接地接触数据资产，因此数据安全风险始终离不开工作人员本身，组织和人员管理部门需要联合人力资源部门在员工的招聘/引进、入职、转岗/调岗、离职等各个环节设置相应的风险控制措施，以降低个人本身问题所导致的数据安全风险。同时，在数据安全快速发展的时代大背景下，对人员的数据安全素质和安全意识提出了更高的要求，越来越多的组织赋予数据安全文化新的传承和使命。

2.4.2.1. 登记审查

随着数字化的不断发展，数据成为国家基础战略资源，面临窃取、泄露、篡改等多种风险，引发数据安全事件的因素有很多，有来自内部的缺陷，有来自外部的攻击，不管有意还是无意带来的数据安全事件，人都是关键因素。因此组织开展数据安全应加强人员登记、审查，统筹制定人员管理制度，明确数据使用、访问等管理措施，同时对数据安全管理机构负责人、关键岗位人员、接触个人信息或重要数据等人员进行资格审查，包括不限于身份、背景、专业资格和资质等，同时签署保密协议，日常落实审批和登记流程，明确数据访问范围、操作权限、人员调岗、离职保密要求、保密期限、违约责任等，定期审查其行为，有效约束其数据操作行为。另外，对数据安全人员履职情况留存相关工作记录，如数据安全管理人员数据安全管理监督检查记录，数据安全责任人数据安全事件信息报送记录等，以便待查和追溯。

2.4.2.2. 文化建设

数字经济时代，数据已经成为重要的基础性战略资源，更是企业的核心资产，不能把数据安全只当作专业人士或者专业工具的事，要建立数据安全教育培训制度，明确培训周期、培训对象、培训内容、考核评价等。定期组织数据安全培训工作，并留存相关记录（如培训计划、培训通知、培训课件、签到表、培训考核情况等相关记录文件）。例如，针对组织全员，培训内容包括但不限于数据安全意识、法律法规等；针对数据安全岗位人员，培训内容包括但不限于标准规范、技能培训、安全评估、应急响应、应急演练等。通过开展培训，宣传强化员工的数据安全意识，形成全员共同维护数据安全和促进发展的良好环境，把数据安全文化纳入企业文化体系，成为企业立身之本，发展之计。

2.4.2.3. 定岗定员

数据安全治理团队的职能架构确定后，如何制定出高质可行的操作规程和管理制度并实现这些制度规范的高效运作和部门职责的有效达成，就成为组织要面对和解决的首要问题。定岗定员、专

业化分工是解决问题、实现目标的基本方法。

定岗是指对数据安全职能架构中各个层次内的职责进行更细致的分工，将一系列相互间关联紧密的工作任务集合设定为一个岗位。定员则是指明确固定某一个或一组人承担某个岗位的任务和职责。定岗的本质是分工，定员的核心是明确职责，二者被共同用于在分工基础上为组织实现降低成本、提高效率的终极目标。

在数据安全治理实践中，定岗定员应特别注意遵循以下原则：

（1）不应出现人员跨层交叉

从上节对数据安全治理团队职能架构的介绍不难发现，决策层、管理层、执行层、监督层之间一方面存在着密切的配合与合作，另一方面也同时存在着相互制约与平衡。这些不同层间的相互制约与平衡是必不可少的，只有如此，才能有效降低人的主观因素中潜藏的负面影响。一旦有人在不同层内同时扮演多个角色，难免会出现因考虑个人相关利益而降低标准、通融迁就的情况。例如，如果一个人既在管理层内负责起草数据安全的技术实施方案，又在决策层内负责对方案的可行性进行审批，则难免会出现方案敷衍或滥用数据安全建设预算的问题；而如果有人同时出现在监督层和其他层，则监督层对后者的审计核查作用必然会大打折扣，甚至形同虚设。

（2）仅授予相关角色或人员完成岗位职责所需的最小权限

对于重要岗位或操作规程，应权限分离或安排多人互相监督，并对重要岗位人员开展背景调查，对重要数据的修改应安排不同人员分别进行操作、审批和复核，以防范内部人员对数据的违规篡改，例如，加密数据库的密码不应告知操作系统管理员，以防范后者用拖库的方法窃取数据等。

（3）信任要基于岗位职能和人员角色，而非人员身份

要培训员工树立和加强安全意识：在数据安全治理的职能框架下，默认不信任外部的任何人或设备，除非按照定岗定员的分工结果被授予了相应权限，否则即使是上级领导，也不能违反数据安全制度规定的操作规程，越权访问或使用敏感数据。

2.4.2.4. 提升考核

新的法律法规、行业标准的实施，和对已实施法律法规及行业标准的重新认识，都会触发安全人员进行重新解读，转化为新的安全管控策略；业务系统的变更需对涉及的数据资产进行重新分类分级，更新安全策略；安全事件的发生也会促进安全运营人员优化数据安全措施，不断提升。

（1）能力提升

●基本知识

掌握法律法规和标准、信息安全基础、数据安全策略、数据安全技术、数据安全检测评估认证等基本知识。

●基本技能

针对数据采集、传输、存储、处理、交换和销毁等生命周期各环节，能够采取措施保障数据安全。针对个人信息收集、存储、使用、共享、转让、公开披露、删除等环节开展个人信息安全保护和合规管理。

●岗位职责

根据数据安全管理、数据安全工程规划设计和实施建设、数据安全技术开发与运维、数据安全

监测与应急处置、数据安全评估等不同的岗位，提出具体要求。（可参考《数据安全工程技术人员国家职业标准》）

（2）人员考核

落实管理体系规范和流程，发挥技术体系监测和防护能力，需要常态化、完善的运营能力做支撑。

●日常运营

日常数据安全运营服务参照运营体系中的内容从数据安全摸底、数据安全策略的制定与升级、数据安全风险管理，以及数据安全策略优化等方面对数据安全开展全方位的工作。

●运营监管

通过可视化的运营监管能力，建设运营监测中心，帮助管理者全面掌握数据安全运营状况。

●服务保障

通过日常运营服务、专家服务、护网保障、重保服务、培训服务，实现数据安全常态化能力。

2.4.3. 管理制度

数据安全治理不仅要建立自上而下的覆盖四个层面的数据安全管理体系，制度更需要体系化建设，即面向内部组织人员和第三方组织，构建四级的管理制度体系，从而在管理层面形成完善的数据安全制度体系架构和各级制度文档，进而帮助组织快速落地数据安全治理体系建设。

图 2–5　管理制度建设思路

从上图可知，数据安全管理制度体系从上至下总共分为四级，每一级都作为上一层的支撑。一级文件是由决策层根据组织的发展目标、公司战略、业务需求，制定的数据安全管理方针、政策，应明确数据安全治理的目标重点，比如“以分类分级为基准，以权限控制为措施，管理与技术并重”的数据安全治理方针。二级文件是由管理层为了落实方针、战略制定的管理规范、标准，应建立数据安全管理制度、组织人员与岗位职责、应急响应、监测预警、合规评估、检查评价、教育培训等制度。三级文件一般由各执行环节的具体操作流程、手册组成，比如数据分类分级操作指南、数据安全治理能力评估、技术防护操作规范、数据安全审计规范等指导性文件。四级文件是各项具体制度执行时产生的过程性文档，一般包括申请表单、安全记录、安全报告、合同协议等内容。

面向组织顶层数据安全管理方针，考虑风险防范需求，满足合规需求为目标，以数据为中心，从资产管理入手，围绕数据生命周期保护要求，形成以下四级制度体系架构：

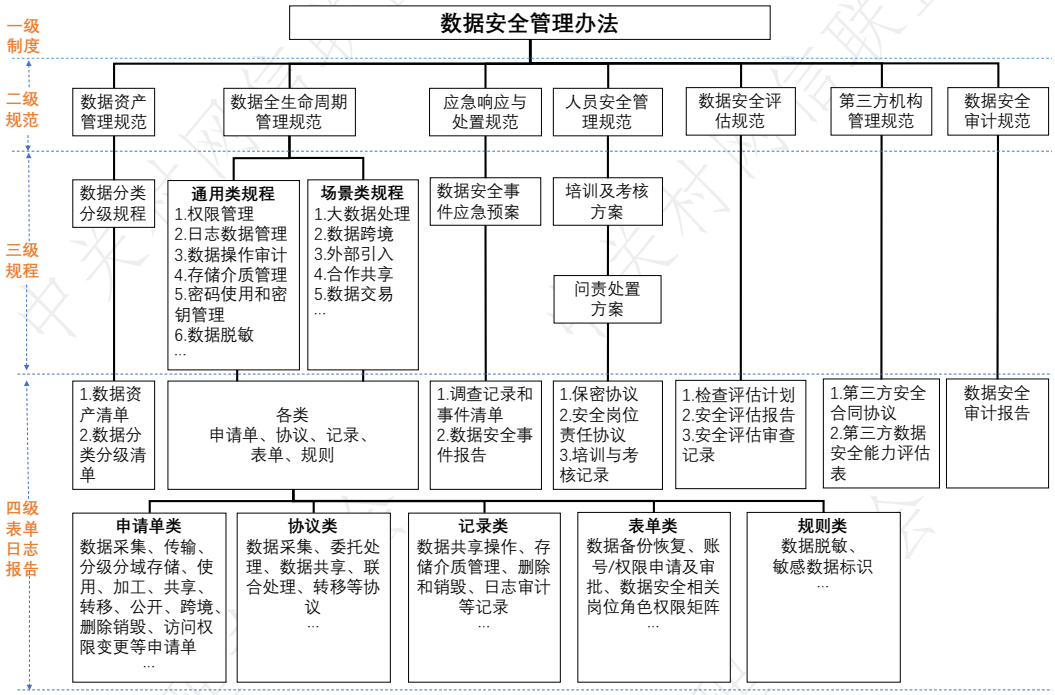


图 2-6　数据安全管理制度体系内容

如图 2-6 所示，一级数据安全管理办法：应按照国家数据安全与发展政策要求，根据自身发展战略，制定数据安全保护战略，明确管理责任分工，建立涵盖数据安全生命周期的管控机制，落实保护措施。

二级文档包括：

数据资产管理规范：应建立数据资产地图，以数据分类分级为基础明确数据保护对象，围绕数据处理活动实施安全管理。

数据安全评估规范：在开展数据委托处理、联合处理、转移、公开、集团内共享等对数据主体有较大影响，或处理敏感级及以上数据的业务活动时，事先开展数据安全评估，编制数据安全评估报告。根据数据处理目的、性质和范围，按照法律法规和伦理道德规范要求，分析数据安全风险和对数据主体权益影响，评估数据处理必要性、合规性，评估数据安全风险及防控措施有效性。建立数据安全评估、个人信息安全影响评估以及内外部数据安全检查与评估制度。

数据安全生命周期管理规范包括：

（1）数据采集要求：采集数据应坚持“合法、正当、必要”原则，明确数据采集和处理的目的、方式、范围、规则，保障采集过程的数据安全性、数据来源可追溯。

（2）外部数据采购要求：制定外部数据采购、合作引入的集中审批管理制度，统筹建立数据需求、安全评估、采集引入、数据运维、登记备案和监督评价管理机制，对数据来源的真实性、合法性进行安全审查，评估数据提供者的安全保障能力及其数据安全风险，明确双方数据安全责任及义务。

（3）数据跨境存储要求：中华人民共和国境内产生的数据原则上应在境内存储，国家或行业监督部门另有规定的除外。

（4）数据使用要求：开展数据清洗转换、汇聚融合、分析挖掘等数据加工活动时，当采用匿名

化等措施保护数据主体权益。数据汇聚融合衍生敏感级及以上数据，或导致数据安全级别变化的，及时评估、调整安全保护措施。数据使用不应超出数据采集时所声明的目的和范围。

（5）数据加工要求：目前数据使用业务场景的目的、范围、审批流程（含权限授予、变更、撤销等）、人员岗位职责等，在保障安全，数据合法正当使用的情况下开展数据利用。根据不同数据使用场景，明确安全管理要求，采用安全处理措施（如去标识化、匿名化、脱敏、数据访问控制等），并采取技术措施保证汇聚大量数据时不暴露敏感信息，降低数据敏感度及暴露风险。

（6）数据共享要求：明确对内、对外数据共享策略，评估数据共享使用的必要性、合规性、安全性、是否符合伦理道德规范要求，建立数据安全隔离的防火墙，并对共享数据进行有效保护。

（7）数据委托处理、外部共享要求：机构在委托数据处理、对外共享数据时，明确所涉数据外部使用和处理的条件、场景、方式。委托处理数据时，以合同协议方式约定委托的目的、期限、处理方式、数据范围、保护措施、双方的数据安全责任和义务，以及受托方返还或删除数据的方式等，对数据处理活动进行记录和审计，可对外公开披露的数据除外。

（8）数据联合处理要求：与第三方机构进行数据联合处理时，应以合同协议等方式予以明确，制定方案并采取有效保护措施，确保数据“可用不可见”，并以合同协议方式明确双方在数据处理过程中的数据安全责任和义务。

（9）数据转移要求：因兼并、重组、破产等需要转移数据，明确数据转移内容，通过协议、承诺等方式约定数据接收方面承接对应数据的安全保护义务，通过公告等告知数据主体。数据转移采用安全可靠方式进行，并确保过程可追溯。涉及敏感级及以上数据转移，向主管监管单位进行报告。

（10）数据公开要求：建立公开披露数据的审批机制，研判可能产生的影响，数据公开应在机构官方渠道进行发布，确保数据真实、准确、防篡改，记录审批和发布情况。敏感级及以上数据不得公开，国家法律法规另有规定或取得数据主体授权同意的除外。

（11）数据跨境要求：遵循“合法、正当、必要”原则建立数据出境评估与管控机制，评估出境数据内容、范围、安全级别、数据接收方的数据安全责任和保护能力等，编制出境报告。数据出境应采取妥善安全保护措施，避免数据泄露、篡改、破坏。核心数据不得出境。向境外提供在中华人民共和国境内运营中收集和产生的重要数据，应当按照国家相关政策要求通过数据出境安全评估。敏感级数据出境需获得数据主体授权同意。

（12）数据删除与销毁要求：按照国家、行业有关规定与数据主体的约定进行数据删除或匿名化处理，制定数据销毁管理制度。

应急响应与处置规范：制定应急响应与事件处置规范，建立完善的应急响应与事件处置和问责机制，做好应急预案。建立数据安全事件应急管理机制，建立机构内部协调联动机制，及时处置风险隐患及安全事件。建立数据安全事件报告机制，根据事件安全等级制定报告流程，发生数据安全事件时按照规定及时报告，同时按照合同、协议等有关约定履行客户及合作告知义务。发生数据安全事件或使用的网络产品和服务存在安全缺陷、漏洞时，应立即开展调查评估，及时采取补救措施，防止危害扩大。

人员安全管理规范：加强在人员录用及日常管理、人员培训和教育、关键岗位设置等方面的管理。

第三方机构管理规范：对参与本机构数据全生命周期过程中的第三方机构进行管理，确保不因与第三方机构合作或第三方应用接入而危害数据安全。建立第三方机构管理制度，对接入和涉及的第三方产品和服务进行专门的数据安全管理。

数据安全审计规范：制定数据安全审计规范，开展数据安全内部审计和分析，发现并反馈问题和风险，并对机构后续相关整改工作进行监督。开展外部审计相关的组织和协调工作。明确定期开展审计、监督检查与评价问责，督促问题整改。审计部门应每年至少开展一次数据安全审计，发生重大数据安全事件后应及时开展专项审计。

三级文档包括：

权限管理规程：建设分层分级的数据权限管控体系。

日志数据管理规程：明确日志的存储、分析、检查等要求。

数据分类分级规程：应制定本机构数据分级规程，识别并维护本机构数据资产清单，并标注相应的数据级别。

密码使用和密钥管理技术规程：建立合理、统一的密码使用和密钥管理技术规范和制度。

数据操作审计规程：明确一定级别以上数据的操作应当进行记录和审计。

数据脱敏技术规程：明确不同安全级别数据脱敏规则、脱敏方法和脱敏数据的使用限制，配置脱敏数据识别和脱敏效果验证服务组件或技术手段，确保数据脱敏的有效性和合规性。

数据存储介质管理规程：明确管理责任分工，建立存储数据安全管控机制，落实保护措施。

数据安全事件应急预案：制定数据安全事件应急预案，定期开展应急响应培训和应急演练。发生数据安全事件后，应立即启动应急处置、分析事件原因、评估事件影响、开展事件定级，按照预案及时采取业务、技术等措施控制事态。

数据安全培训及考核方案：组织开展数据安全宣贯培训，提升员工数据安全保护意识与技能。制定数据安全相关岗位人员的安全专项培训计划，并对培训结果进行评价、记录和归档，开展专业化培训和考核。

数据安全问责处置方案：建立数据安全责任制，明确各层级负责人的责任，明确违规和责任追究事项，落实问责处置机制。

四级文档包括：

各类申请表单：全生命周期数据使用申请单，比如：数据采集申请单、数据加工申请单等。

各类合同协议模板：全生命周期数据安全协议：数据采集协议、数据共享协议、数据联合处理协议等。

各类安全报告：在开展应急响应、安全审计过程中产生的安全报告，比如：数据安全审计报告、数据安全评估报告等。

各类安全记录：数据共享操作记录、存储介质管理记录、数据安全培训与考核记录、日志审计记录等。

清单要求：数据分类分级清单、数据资产清单、调查记录和事件清单、数据安全相关岗位角色权限清单等。

2.5. 数据安全技术体系

数据安全整体的技术体系面向数据的全生命周期进行构建，以覆盖全生命周期的数据采集安全、数据传输安全、数据存储安全、数据使用安全、数据提供安全、数据公开安全、数据删除和销毁安全技术为核心，以支撑生命周期各环节的通用安全技术为基石，以平台化的协同计算、安全监测与安全运营为总控，形成完备的识别、监测与防护的技术体系，支撑管理体系与运营体系的落地。具体的技术体系涉及的需求及安全工具介绍参见“第四章 数据安全技术需求与主流技术工具介绍”。

2.6. 数据安全运营体系

2.6.1. 规划思路

在数据安全治理体系的基础上，参照经典的 PDCA 模型，强化数据安全运营体系在数据安全治理中的轴心作用，有效上承管理制度体系，下接技术体系，落实数据流动性带来的持续、动态、闭环管理。

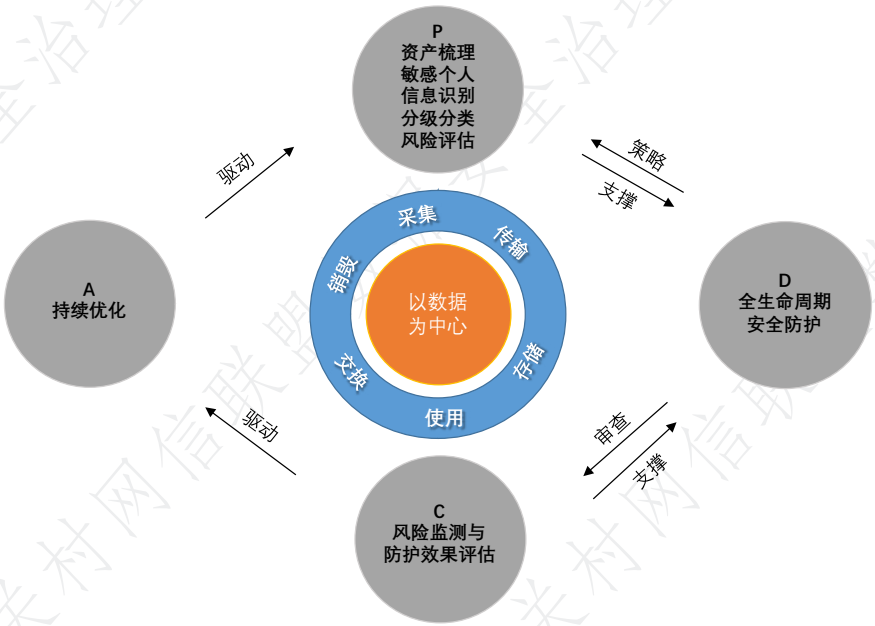


图 2-7　参照 PDCA 模型的运营体系规划思路

首先制定数据安全规划（P），通过对组织应遵循的法律法规和行业标准进行解读，结合业务情况，输出并持续更新数据资产分类分级知识库和数据安全合规库，并进行数据资产梳理及分类分级，摸清数据资产家底，评估风险暴露面缺陷，再依照合规性要求，针对风险点设定动态分级防护策略；然后落实全生命周期安全防护（D），依据规划制定的安全策略，面向不同级别的敏感数据对象，构建覆盖数据全生命周期节点的按需、动态防御技术能力体系；其次，开展风险监测与防护效果评估（C），实时监测数据安全运行风险，对安全事件进行响应处置，并对安全防护效果进行合规性综合评价；最后，根据风险监测和防护效果评估结果，结合业务变革，进行持续改善、优化（A），迭代驱动下

一个安全规划（P）。

2.6.2. 体系架构

管理制度和技术体系需要落地，离不开数据安全运营体系。数据安全运营体系主要包括两部分，一是定期或特定数据处理场景（数据跨境、数据交易等）触发的数据安全风险评估；二是常态化持续运营工作，依据I（识别）、P（防护）、D（监测）、R（响应）模型形成的一系列治理活动。数据安全运营要考虑“数据资产、安全策略、安全事件、安全风险”等关键因素，明确哪里做的好、好到什么程度，又有哪些做的不足、哪里需要改进和优化等等，不断地丰富和提升完整性和成熟度。

整体安全运营体系包括如下内容：

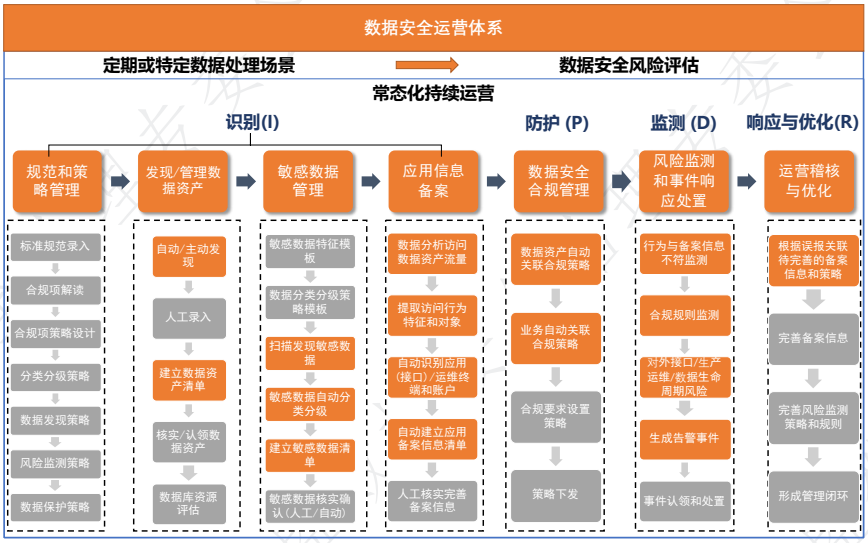


图 2-8　数据安全运营体系架构

如图 2-8 所示，具体内容如下：

（1）定期或特定数据处理场景触发的数据安全风险评估

数据安全风险评估的目的旨在掌握数据安全总体状况，发现存在的数据安全风险和违法违规问题，为进一步健全数据安全管理制度和技术措施，提高数据安全治理能力奠定基础。

从评估要素看，数据安全风险评估涉及数据、数据处理活动、业务、安全措施、数据安全风险等基本要素，开展数据安全风险评估应充分考虑要素间关系。

从评估对象看，数据安全风险评估主要围绕数据处理者的数据和数据处理活动，对可能影响数据保密性、完整性、可用性和数据处理活动合理性的安全风险进行分析和评价。数据安全风险分析主要涉及数据、数据处理活动、风险源、安全措施等基本要素。

从评估内容看，数据安全风险评估既包括涉及数据处理者、业务和信息系统的基本情况调研，也包括处理的数据、开展的数据处理活动情况识别，还包括数据处理活动、数据安全管理、数据安全技术、个人信息保护、重要数据处理等方面的评估内容。

从评估方法看，数据安全风险评估主要包括人员访谈、文档审核、系统核查、技术测试。其中：

●人员访谈是指评估人员采取调查问卷、现场沟通等形式对被评估方的数据、数据处理活动和数据安全实施情况等进行了解、分析和取证。

●文档审核是指评估人员通过对数据安全相关管理制度体系的完整性、健全性进行评估，包括管理办法，安全规范、流程机制及配套的表单 / 日志 / 报告等进行审核、查验、分析，全面梳理被评估方的数据安全实施情况。

●系统核查是指评估人员通过旁站查看被评估方数据安全相关网络、系统、设备的配置、功能或界面，验证数据处理系统和数据安全技术工具实施情况。

●技术测试是指评估人员通过手动测试或自动化工具进行技术测试，验证被评估方的数据安全措施有效性，发现可能存在的数据安全风险。

从实施流程看，数据安全风险评估主要包括评估准备、数据和数据处理活动识别、风险源识别、风险分析、评估总结五个阶段。风险沟通和评估过程文档管理需要贯穿于整个风险评估过程。其中：

●评估准备工作主要包括确定评估目标、明确评估范围、组建评估团队、展开评估前期调研。

●数据和数据活动识别工作主要包括数据发现、分类分级和数据处理活动的识别。

●风险源识别工作主要是指从数据处理活动风险、数据安全管理维度进行风险识别。

●风险分析工作主要是指对识别的各项风险进行归类，并从风险危害程度、发生可能性多个角度进行风险评价与定级。

●评估总结工作主要是指对评估结果进行分析总结，编制数据安全风险评估报告，并针对风险缺陷给出整改建议。

数据安全风险评估工作是持续性的活动，当被评估对象的政策环境、外部威胁环境、业务目标、安全目标等发生变化时，需要重新开展风险评估。

在涉及到个人信息处理活动的应用场景时，组织还应开展个人信息保护影响评估，检验个人信息处理的合法合规程度，判断对个人信息主体合法权益造成损害的各种风险，评估用于保护个人信息主体的各项防护措施的有效性。

个人信息保护影响评估的规模往往取决于受到影响的个人信息主体范围，数量和受影响的程度。通常，组织在实施该类个人信息安全影响评估时，个人信息的类型、敏感程度、数量，涉及个人信息主体的范围和数量，以及能访问个人信息的人员范围等，都会成为影响评估规模的重要因素。

可参考《个人信息保护法》第五十五条　有下列情形之一的，个人信息处理者应当事前进行个人信息保护影响评估，并对处理情况进行记录：

（一）处理敏感个人信息；

（二）利用个人信息进行自动化决策；

（三）委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息；

（四）向境外提供个人信息；

（五）其他对个人权益有重大影响的个人信息处理活动。

第五十六条　个人信息保护影响评估应当包括下列内容：

（一）个人信息的处理目的、处理方式等是否合法、正当、必要；

（二）对个人权益的影响及安全风险；

（三）所采取的保护措施是否合法、有效并与风险程度相适应。

个人信息保护影响评估报告和处理情况记录应当至少保存三年，可参考标准有 GB/T 39335-2020《信息安全技术 个人信息安全影响评估指南》,GB/T 35273-2020《信息安全技术 个人信息安全规范》，GB/T 41391-2022《移动互联网应用程序（APP）收集个人信息基本要求》，GB/T 39725-2020《信息安全技术 健康医疗数据安全指南》，JR_T 0171-2020 《个人金融信息保护技术规范》。

（2）常态化持续运营工作

1）识别（I）

●规范和策略管理

组织应调研相关的国内外数据安全相关监管要求、业界数据安全治理相关方法论和架构体系，作为数据安全治理优化工作的方法论和框架体系依据，形成数据分类分级策略、风险监测策略和数据保护策略。

●发现 / 管理数据资产

运用数据安全管理平台的自动发现工具，结合手工调研梳理，对数据资产进行持续维护，发现敏感数据库和敏感数据的位置和分布，统计重要数据，并对数据资产的归属部门、责任人、使用方等信息进行备案登记，形成数据资产列表。并对数据库资产进行安全评估，识别数据库资产的脆弱点。

●敏感数据管理

基于数据分类分级策略模板，借助敏感数据发现技术和数据自动分类分级工具，对新发现的数据资产进行分类分级识别与打标，快速建立数据分类分级清单，并进行人工核实确认。

●应用信息备案

收集分析数据资产访问流量，提取访问行为特征和对象，识别应用账号和运维账号，建立应用信息备案清单，并由人工进行备案信息核实完善。

2）防护（P）

●数据安全合规管理

梳理评估各级别数据资产在整个数据生命周期流动中的安全风险，借助数据安全管理平台的安全策略管理工具，针对风险设定各安全防护节点的防护策略，对数据安全进行合规管控。

特别强调的是涉及国家关键信息基础设施的单位，依据国家法律、行政法规和有关规定，要求其运营者应当使用商用密码落实数据保护，并需自行或者委托商用密码检测机构开展商用密码应用安全性评估。

3）监测（D）

●风险监测和事件处置

构建面向用户、终端、应用、数据的全链路数据安全风险监测能力，实现围绕数据全生命周期的统一流转监测与审计，并基于形成的数据流转视图，持续分析、研判数据流转风险，针对产生的安全事件告警，落实应急响应与事件处置与溯源取证。

4）响应与优化（R）

●运营稽核与优化

建立面向安全策略、安全风险、安全事件的 KPI 指标分析，对数据安全运营情况进行整体稽核，

根据稽核考核结果进行持续完善和优化。

2.6.3. 运营服务

组织落实管理体系规范和流程，发挥技术体系监测和防护能力，需要常态化、完善的运营能力做支撑。

日常数据安全运营服务参照运营体系中的内容从数据安全摸底、数据安全策略的制定与升级、数据安全风险管理，以及数据安全策略优化等方面对数据安全开展全方位的工作。

运营监管：通过可视化的运营监管能力，建设运营监测中心，帮助管理者全面掌握数据安全运营状况。

服务保障：通过日常运营服务、专家服务、护网保障、重保服务、培训服务，实现数据安全常态化能力。

（1）日常运营服务

数据安全运营是一个持续化运营的过程，在日常运营服务中需安排安全运营人员持续进行数据安全风险监测。建设集中化、日常化的数据安全运营业务流程，从数据安全摸底、数据安全策略的制定与升级、数据安全风险管理，以及数据安全策略优化等方面日常的数据安全运营工作。

新的法律法规、行业标准的实施，和对已实施法律法规及行业标准的重新认识，都会触发运营人员进行重新解读，转化为新的安全管控策略；业务系统的变更需对涉及的数据资产进行重新分类分级，更新安全策略；安全事件的发生也会促进安全运营人员优化数据安全措施，不断完善数据安全治理体系。

（2）应急保障服务

应急保障针对每年国内重大、重要事件，以及全网突发的重大安全事件提供应急支持服务。主要工作内容包含但不限于：制定数据安全应急方案、工作要求及相关制度；在事前为应急响应做好预备性的工作，做好数据备份；在安全事件发生后，按要求及时对异常的系统、网络进行分析，确定安全事件的各项技术细节，保留相关证据并制定进一步的响应策略；及时采取行动限制安全事件扩散和影响的范围，限制潜在的损失与破坏，保障系统正常运行，恢复受到毁损的数据；事后通过对有关安全事件或异常行为的分析结果，找出根源，明确相应的补救措施并协助完成彻底清除；协助恢复安全事件所涉及的系统，并还原到正常状态，使业务能够正常运行。

2.7. 数据安全监督评价体系

组织要服从和积极配合行业主管单位的数据安全监管，形成监督管理和自律管理相结合的数据安全治理体系，主要途径有评估认证、监测预警、事件调查处置、监督检查、纠正问责，这是多元治理的重要一环。

（1）评估认证

国家陆续推出数据安全管理、个人信息保护等认证制度，鼓励网络运营者通过认证方式规范网

络数据处理活动，加强网络数据安全保护，如APP安全认证、数据安全管理认证、个人信息保护认证等。组织还应在每年固定时间前向行业监管部门报送本年度数据安全风险评估报告，报告内容包括数据安全治理、技术保护、数据安全风险监测、事件处置、委托和联合处理、数据出境、数据安全评估与审查情况，数据安全投诉和处理情况。

（2）监测预警

行业监管单位通过数据安全风险评估报告、监测预警、通报处置机制，持续监测数据安全风险，向行业发布风险提示，制定行业数据安全事件应急预案，处置数据安全风险事件。与国家数据安全管理部门建立联防联控管理机制，建立信息共享平台，实施数据安全信息共享、风险和威胁监测、预警及数据安全事件处置。

（3）事件调查处置

数据安全事件是指由于管理控制不足导致数据被篡改、泄露、破坏、非法获取、非法利用等，对个人或组织合法权益、行业安全、国家安全造成负面影响的事件。根据其影响范围和程度，分为四级：特别重大事件、重大数据安全事件、较大数据安全事件、一般数据安全事件。行业监管单位对被监管单位的数据安全风险及防范能力进行评估，并纳入监管评价、评估体系，开展数据安全事件调查和处置。审计部门应每年至少开展一次数据安全审计，发生重大数据安全事件后应及时开展专项审计。

对违法个人信息处理活动向履行个人信息保护职责的部门进行投诉、举报。收到投诉、举报的部门应当依法及时处理，并将处理结果告知投诉、举报人。履行个人信息保护职责的部门应当公布接受投诉、举报的联系方式。

针对投诉举报事件，有关主管部门在履行数据安全监管职责中，发现数据处理活动存在较大安全风险的，可以按照规定的权限和程序对有关组织、个人进行约谈，并要求有关组织、个人采取措施进行整改，消除隐患。

（4）监督检查

国家通过数据安全审查、监督检查与违规处罚等相关制度落实监管，比如：2022年2月15日正式施行的《网络安全审查办法》将网络平台运营者开展数据处理活动影响或者可能影响国家安全等情形纳入网络安全审查，并明确掌握超过100万用户个人信息的网络平台运营者赴国外上市必须申报网络安全审查。同时国家还通过专项治理（协同打击）、“清朗”行动等系列专项行动，以及网络安全等级保护（基本要求）、关键基础设施保护（重点保护）、密码评估管理等系列测评开展监督检查。

（5）纠正问责

组织违反办法要求的，行业监管单位依法予以纠正，根据违规情况实施问责处置或行政处罚。具体措施包括：

- 采取监督监管措施，责令改正，给予警告。
- 对有关负责人、直接负责的主管人员和其他直接责任人员问责或处以罚款，包括禁止其在一定期限内从事数据安全保护工作、担任责任人。
- 对设计违规处理行为的系统及应用，责任暂停或者终止服务。
- 对涉及违规处理或产生重大风险、事件或案件的第三方机构，责令暂停或者停止与其开展合作，

必要时将有关情况移交司法机关。

2.8. 典型数据处理场景

数据安全治理的核心关注点在于场景化安全。

组织目前存在数据安全技术使用不够普及，比如：区块链、隐私计算、同态加密等对业务的支撑没有广泛应用，主要原因是技术人员与业务人员割裂，技术与业务缺乏深度结合。随着数据要素市场持续健全和深化，数据交易、数据出境等数据运用新模式持续涌现，不同用户基于业务、访问途径和使用需求，会产生不同的使用场景，一刀切、固化的防护方式已无法适应不同场景下安全防护要求。在保证数据被正常使用的目标下，基于不同的使用场景特点及时发现数据风险暴露面，数据安全技术与业务深度结合，制定相应的数据安全策略，使数据安全治理更具针对性，在个人和组织与数据有关的权益得到充分保护的基础上，依法推动数据合理有效利用和依法有序自由流动。

组织内的数据要跨部门、跨数据生命周期进行流转。比如：大数据的处理过程就包括数据抽取转换、数据传输、数据汇聚存储、数据加工生产、数据分发共享、用数访问。组织间的数据围绕合作共享、数据交易、数据跨境等众多数据运用新模式。

如图 2–9 所示围绕典型的数据使用场景，从不同用户、访问途径、使用需求、场景特点、安全策略五个方面，阐述有针对性的场景化数据安全治理思路。

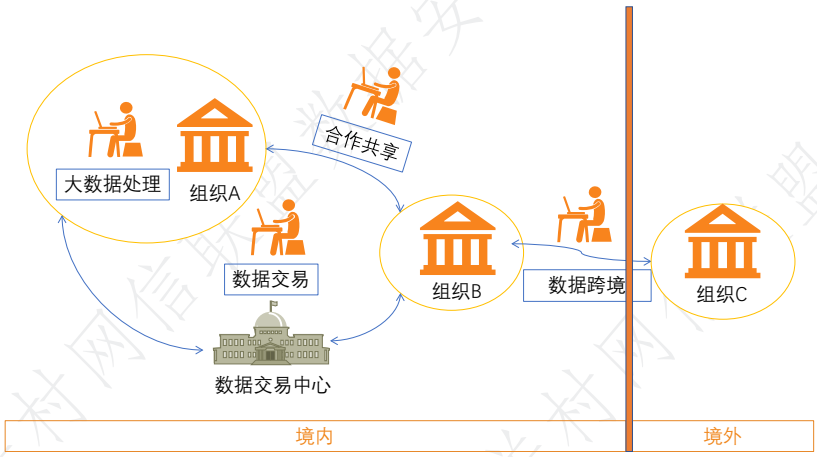


图 2–9　典型用数场景

2.8.1. 数据跨境

数据跨境场景主要是对从事跨境数据活动的数据处理者提出合规要求，个人信息处理者和境外接收方在跨境处理个人信息时应满足法律法规的规定，遵循合法、正当、必要的原则，重要数据境内存储，数据跨境要评估，同时做好个人信息保护，也要取得个人信息主体同意。

数据跨境主要的途径包括登录查询、拷贝复制、数据备份、WEB 服务、区块链、平台服务、数据迁移等。使用需求包括互联网跨境数据访问、境内访问路由至境外等、互联网数据推送与交换至境外、数据镜像至境外、数据迁移至境外、租用物理跨境专线至境外等。

数据处理者从事跨境数据活动应当按照国家数据跨境安全监管要求，建立健全相关技术和管理措施，明确数据接收方履行数据安全保护义务，保证数据安全。

虽然数据跨境传输是个法律问题，但是可以通过技术手段来降低风险。组织采用的安全策略包括通过技术手段进行个人信息脱敏，这将会大大降低数据跨境传输合规的风险。制定离境数据规范，明确离境评估机构要求进行安全评估，留存数据出境安全评估报告。同时在数据传输的过程中，要注意数据安全保护，与技术服务商签订业务合同能够有效划分责任，针对数据出境行为明确征求数据主体的授权也将有利于企业数据跨境传输合规。可参考的数据安全保护技术标准：GB/T 22239《网络安全等级保护基本要求》、GB/T 39786《信息系统密码应用基本要求》、GB/T 35274《大数据服务安全能力要求》，GB/T 37932《数据交易服务安全要求》，GB/T 41479《网络数据处理安全要求》等。

组织侧：采用境内存储、系统保护，产品和服务保护、传输过程保护，境外的同等保护；数据转移保护：完整性保护、机密性保护。

监管侧：

（1）检查数据跨境的合法性。检查跨境数据的分类分级（重要数据或一般数据）、数据跨境类型、方式等，以及用途、内容、数量、范围等是否合法必要正当；检查个人信息主体同意机制或匿名化处理情况。

（2）检查标准合规性。检查数据保护措施和风险控制、应急预案等，检查同等保护原则或情况，关注平台侧、网络侧、终端侧、边缘侧、边界侧等保护。

（3）持续监督数据跨境合法合规有效性。监督数据泄露事件处置、检查应急处置情况、损失评估和整改情况等。

2.8.2. 数据交易

数据交易场景交易主体要定期开展数据流通交易安全风险评估，不断健全完善数据流通交易安全管理机制，保障交易活动安全；强化全流程数据安全管理，切实保障数据安全；数据交易场所应当制定重大安全风险监测、风险警示、风险处置等风险控制制度以及突发事件应急处置预案，并报告主管单位；网信、公安、密码管理等部门在数据流通交易安全监督管理中，发现存在较大安全风险的，提出改进要求并督促整改。

在数据交易场景中，交易主体传输交易标的访问途径可以通过 API/SDK 接口、数据集、数据报告、算法模型、算力资源部署、数据系统部署及其他数据服务等方式进行交付。

交易主体采用云计算、区块链、联邦学习、多方安全计算等技术，建设安全可信的数据流通交易平台，构建数据流通交易基础设施环境，实现原始数据“可用不可见”、数据产品“可控可计量”、流通行为“可信可追溯”。

数据交易场景主要参与方包括交易用户、数据提供方、数据需求方、数据商、数据中介、交易标的、数据产品和服务、算力资源、算法工具，数据流通交易按照主体登记、标的登记、交易磋商、签订合同、交易结算、交易备案等流程组织实施。

数据交易场景安全策略以数据分类分级保护为基础，实施差异化安全管理要求，不同行业领域

安全策略不同。比如：工信领域鼓励要求企业按一般数据、重要数据、核心数据实施分级保护，金融领域二级数据优先考虑业务需求，四级数据优先考虑安全需求，四级及以上数据不应对外传输、汇聚融合、共享等。以保障数据安全过程安全为目标，明确安全管理基础规则。

破解数据流通交易的中数据安全问题，可以充分应用区块链、隐私计算等技术，从隐私保护技术、安防监管方面进行化解。

（1）利用区块链、隐私计算等新型技术实现数据“可用不可见”，有效管控数据计算价值使用的目的和方式，实现数据使用的事前评估和持续监督相结合、风险自评估与安全监督相结合，保障数据使用的安全与合法，破解数据滥用、隐私泄露、用户歧视等问题。

（2)改进提高监管技术和手段，建立数据交易平台，依托大数据技术建立健全违法线索线上发现、流转、调查处理等机制，提升分析预警、线上执法、信息公示等监管能力。同时，鼓励条件成熟的地区开展试点创新，以点带面提高数据交易流通安全保障能力。

监管方面，统筹各相关部门的治理授权和责任，落实数据从产生、使用到流转全生命周期中各环节责任主体，强化分行业和跨行业协同监管，完善追责机制等配套制度。

机制方面，在开展数据要素流通交易、跨境传输、争议解决等立法研究的基础上，建立数据流通交易负面清单制度，明确不能交易或严格限制交易的数据项，推动形成有规可循、安全可控的数据流通交易机制。

2.8.3. 大数据处理

大数据处理场景涉及大数据提供者、大数据使用者、大数据服务者（大数据平台提供者、大数据应用提供者和大数据服务协调者）五种角色。在开展数据处理活动应当依照法律、法规的规定，建立健全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护和敏感个人信息保护责任。

大数据处理场景是通过大数据平台组件进行访问，大数据流动（数据的产生、流动、处理等），用户个人数据收集和挖掘（逐步形成用户画像）；从事大数据相关产业的组织和个人访问，主要有大数据平台、大数据流动、大数据使用、大数据源数据使用和大数据隐私 5 个方面使用需求。

大数据处理场景应主要防止外部黑客攻击，满足合规性，敏感数据的安全管理和使用，采用安全策略包括大数据服务提供者应具有的基础安全能力、大数据服务生命周期安全能力以及大数据服务平台与应用相关的系统服务安全能力。大数据服务提供者在风险识别、安全防护、安全监测、安全响应和安全恢复环节的安全能力建设要求。

大数据安全评估：评估当前大数据平台、大数据流转、大数据使用等多种安全状态；

分类分级：结合业务对数据进行不同类别和密级划分，并制定不同的管理和使用原则，做到有差别和针对性的防护。

大数据授权控制：针对不同角色制定不同安全策略，常见的角色包括：业务人员（要进一步角

色细分）、数据运维人员、开发测试人员、分析人员、外包人员、数据共享第三方等。

大数据安全审计与稽核：行为审计分析、权限变化监控、异常行为分析、数据接口审计。

大数据使用安全控制：业务系统数据访问安全管控、大数据安全运维管控、开发测试环境数据安全使用、BI 分析数据安全管控、数据对外分发管控、数据内部存储安全。

2.8.4. 合作共享

数据合作共享场景对数据分发源单位和数据分发对象单位提出合规要求，仅靠书面合同难以实现对数据接收方的数据处理活动进行监控，极易造成数据滥用，要求委托方和受托方均应履行数据安全保护义务。

数据合作共享环节实现跨组织的数据授权管理和数据流向追踪，需要满足数据流动安全防护的需求，通过动态变化的视角分析和判断数据安全风险，构建以数据为中心、连续的数据安全防护。

在开展业务时数据需要对外共享，数据一旦对外分发共享，安全保护的责任主体变化，数据安全责任分不同场景以及过错情况等，承担责任不同，接收方与发送方均履行好各自承担的数据安全责任。比如：数据共享中的接收方在接收到数据后并没有对数据的安全保护起到应尽的责任，从而引发了数据二次扩散泄露事件。因此，对于数据分发后的安全性需要通过技术手段监管起来。

数据合作共享场景可以采用数据分发水印机制，对于将要发布到外界的数据预先进行水印处理，在水印中植入数据接收者的相关信息。嵌入原始数据中的水印是不可除的，并且能够提供完整的版权证据。在原始数据中嵌入水印标记信息不易察觉，不影响原始数据的可用性。从数据水印中溯源水印标记信息的能力。一旦发现泄露，可以通过提取泄露的数据样本对样本数据进行水印信息提取和分析。水印类型包括文本属性水印、伪行 / 伪列水印和仿真水印等，也可以采用数据脱敏，对数据中如：身份证号、银行卡号、电话号码等敏感数据进行脱敏处理，防止用户数据泄露。

2.9. 数据安全治理规划建设

从组织构建到持续改善是一个系统化的建设步骤，可有效指导数据安全治理全面建设的落地。

（1）组织构建

组建专门的数据安全团队，是作为数据安全治理建设的首要任务，是保证数据安全治理工作能够持续执行的基础。

（2）资产梳理

资产梳理是数据资产安全管理的第一步，通过资产梳理能够掌握数据资产分布、数据责任确权、数据使用流向等，使数据资产安全管理更全面。

（3）策略制定

掌握了数据资产概况后，需要制定安全策略作为数据资产管控的安全规则。

通过数据分类分级与重要数据识别，区分人员角色权限及场景，制定针对性的安全策略，能够实现对敏感数据进行分级管控，使数据在生命周期中安全流动。

（4）过程控制

策略制定后需要将安全规则落地，通过数据安全管理体系、技术体系、运营体系的有效配合，能够帮助组织进行数据资产安全管理的过程控制。

要对数据的访问过程进行审计，要判断这些数据访问行为过程是否符合所制定的安全策略；要对数据的安全访问状况进行深度评估，看在当前的安全策略有效执行的情况下，是否还有潜在的安全风险。

数据安全需要动态跟踪，持续改善。可通过资产梳理，持续掌握数据资产动态；通过预警演练，提升应急响应能力；通过数据安全评估，了解数据安全管控现状，持续优化安全策略等。

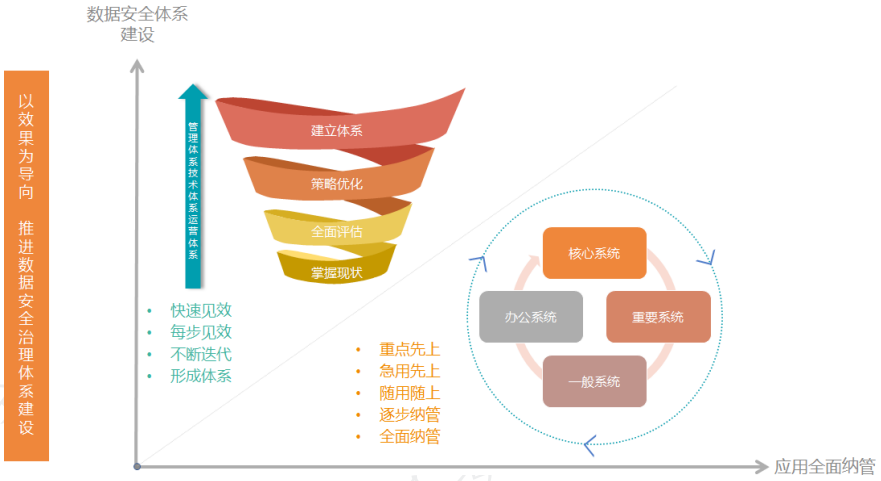


图 2–10　数据安全治理体系建设

依据上述指导性的建设步骤，数据运营者可根据组织的业务关注点、风险容忍度等实际情况，首先考虑核心业务且易实施、见效的防护手段先行实践，然后在治理深度上逐步构建形成体系化、全周期的数据安全防护体系，再在治理广度上逐步覆盖到数据运营全业务，并在过程中持续优化。

2.9.1. 数据安全治理整体建设思路

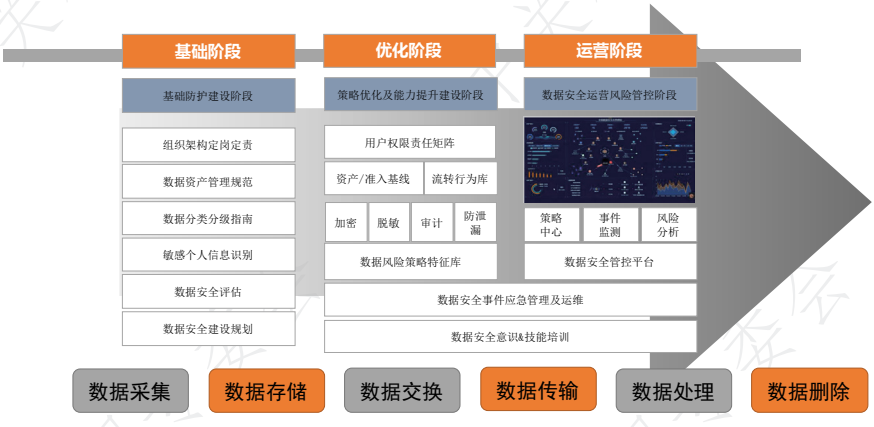


图 2–11　三阶段数据安全治理建设思路

数据安全治理规划建设，围绕收集、存储、使用、加工、传输、提供、公开等数据处理活动，分为三个阶段建设：

基础阶段－基础防护建设，主要以咨询服务为主，包括资产管理、数据分类分级、安全评估、管理制度建设、安全策略建设、方案规划。

优化阶段－策略优化及能力提升建设，主要以产品为主，依据管理流程和安全策略部署自动化防护工具，解决业务风险。

运营阶段－数据安全管控平台建设，主要基于管理流程、安全策略、业务场景和防护积累的经验，形成行为特征库、安全事件知识库、结合业务场景的积累，形成风险分析模型，建立数据安全管控平台，有监测、有预警、有管理、有控制、有审计、有运维、可感知。

2.9.2. 数据安全治理迭代式建设思路

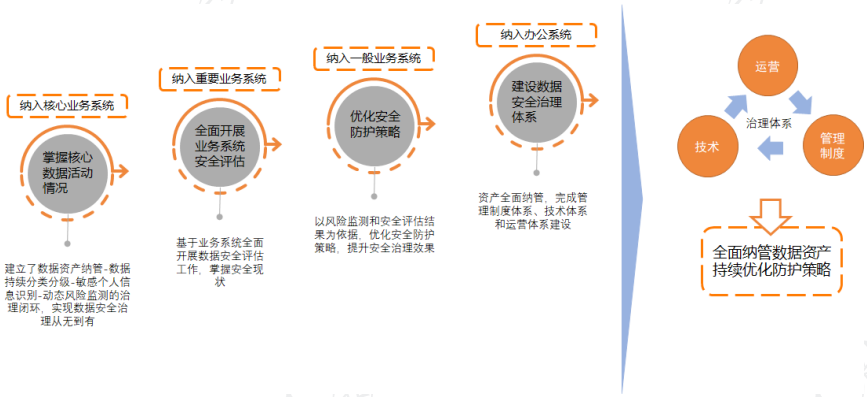


图 2-12　迭代式数据安全治理建设思路

在数据安全治理实践中，一次性建立完整的数据安全体系存在方案复杂、投入高、周期长，见效慢、效果不可控等问题，且各单位数据安全建设基础情况不一，宜循序渐进地开展数据安全治理建设工作。用户需坚持以业务数据资产为核心，基于当前的数据安全现状。数据安全治理体系的建设划分为多个阶段，并将管理＋技术＋运营的建设思想贯穿在每一个阶段的建设任务中，快速达成阶段性目标，再由前一个阶段的建设成果指导下一个阶段的建设目标，一步步证明路线选择的正确性，通过“小步快跑，不断迭代”的方式，横向形成应用全面纳管，纵向持续优化防护策略，逐步建成数据安全闭环管控体系。

第三章　我国相关法律法规及标准解读

2022 年以来，为推进《数据安全法》《个人信息保护法》的深入贯彻实施，国家、地方及各行业监管部门密集出台了围绕数据安全与个人信息保护的系列合规政策与办法，持续建立、健全覆盖建设、认证、评估、审计等数据安全合规监管体系与技术标准，为组织开展数据安全治理建设给出了细化的要求和指引。通过对数据安全相关法律、法规及标准的解读，帮助组织了解和梳理相关政策和标准内涵，保障数据安全治理过程中的有法可依，有章可循。

3.1. 数据安全合规整体体系框架

数据的开发利用必须要依法依规开展，满足合规要求是数据安全底线。通过对国内、国际数据安全相关的法律法规解读，了解监管层面对有序推动数据价值发挥的安全保障要求，为数据安全治理的开展奠定合规依据。

我国已经形成以法律、行政法规、部门规章及规范性文件、地方性法规、以及相关行业标准、指南等相结合的综合性数据安全监督评价体系。同时，数据安全监管也通过认证、评估、审计等抓手予以落实，做到事前、事中、事后全流程监管。目前已形成“数据安全管理认证”和“个人信息保护认证”等的认证、数据出境安全评估、个人信息处理的合规审计等制度。

《网络安全法》从法律层面保障了广大人民群众在网络空间的利益，有效维护了国家网络空间主权和安全，是国家基本法律；《数据安全法》是相关领域的基础性法律，《个人信息保护法》是我国关于保护个人信息的专门性法律，二者从法律层面提供了数据安全保障和个人信息保护。《网络安全法》《数据安全法》以及《个人信息保护法》共同构成了我国数据保护的基础体系，整体的法律法规脉络关系如下表所示：

表 3-1　数据安全相关法律法规关系脉络

层级	规范名称		
上位法	基本法律	基础性法律	专门性法律
	《网络安全法》	《数据安全法》	《个人信息保护法》
下位法	行政法规		
	《关键信息基础设施安全保护条例》《网络安全等级保护条例（征求意见稿）》《网络数据安全管理条例（征求意见稿）》		
部门规章	《网络安全审查办法》《数据出境安全评估办法》 《个人信息出境标准合同办法》《互联网信息服务算法推荐管理规定》		
规范性文件	《个人信息保护认证规则》《数据安全管理认证实施规则》（DSM） 《汽车数据安全管理若干规定（试行）》《工业和信息化领域数据安全管理办法（试行）》《网络产品安全漏洞管理规定》 《银行业金融机构数据治理指引》《国家健康医疗大数据标准、安全和服务管理办法（试行）》 ……		
地方性法规	《北京市公共数据管理办法》《深圳经济特区数据条例》《上海市数据条例》《浙江省公共数据条例》 《厦门经济特区数据条例》《重庆市数据条例》《吉林省促进大数据发展应用条例》 《四川省数据条例》《陕西省大数据条例》《辽宁省大数据发展条例》《安徽省大数据发展条例》 《广西壮族自治区大数据发展条例》《福建省大数据发展条例》《山西省大数据发展应用促进条例》 《山东省大数据发展促进条例》《贵州省政府数据共享开放条例》 ……		
标准、指南等	GB/T 35273-2020《信息安全技术 个人信息安全规范》 GB/T 41479-2022《信息安全技术 网络数据处理安全要求》 GB/T 41391-2022《信息安全技术移动互联网应用程序（App）收集个人信息基本要求》 GB/T 39335-2020《信息安全技术 个人信息安全影响评估指南》 GB/T 39204-2022《信息安全技术 关键信息基础设施安全保护要求》 GB/T 38667-2020《信息技术 大数据数据分类指南》 GB/T 37973-2019《信息安全技术 大数据安全管理指南》 GB/T 37964-2019《信息安全技术 个人信息去标识化指南》 GB/T 37932-2019《信息安全技术 数据交易服务安全要求》 GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》 GB/T 20984-2022《信息安全技术 信息安全风险评估方法》 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》 ……		

3.2. 重点推进工作

3.2.1. 数据安全认证机制完善数据安全监管体系

数据安全相关的认证包括“数据安全管理认证”（DSM）和“个人信息保护认证”（PIP），是对数据处理者和对个人信息处理者对数据安全和个人信息保护水平的认证。

对两项认证的具体内容分别论述如下：

（1）数据安全管理认证（DSM）

2022 年 6 月 9 日，国家市场监管总局、国家互联网信息办公室联合发布《关于开展数据安全管

理认证工作的公告》，正式宣告数据安全管理认证的启动，鼓励网络运营者通过认证方式规范网络数据处理活动，加强网络数据安全保护。

●认证目的

我国既有法律法规并未明确将 DSM 认证设置为强制性义务，而是鼓励网络运营者通过认证的方式规范网络数据处理活动，意义在于促进网络运营者数据安全建设规范化，加强数据安全的防护力度。认证推出势必会增强组织对数据安全落地的积极性，对于对暂不符合认证要求的，机构可要求认证委托人限期整改，促使认证对象加快数据安全标准建设内容。在认证有效期内，要求企业须持续接受机构监督，确保数据安全工作持续落到实处。

●认证依据

DSM 认证是按照《数据安全管理认证实施规则》来实施，此规则的制定依据是《中华人民共和国认证认可条例》。而认证认可条例所称的“认证”是指由认证机构证明产品、服务、管理体系符合相关技术规范、相关技术规范的强制性要求或者标准的合格评定活动。从数据处理全生命周期的安全技术要求（包括收集、存储、使用、传输、提供、删除、访问控制等），和安全管理要求（包括数据安全负责人、人力保障、事件应急处置）这两个维度来进行评估认证。

●认证对象

针对网络运营者的数据安全管理体系开展的认证活动，以验证网络运营者是否建立了有效的数据安全管理体系来进行网络数据的收集、存储、使用、加工、传输、提供、公开等处理活动。数据安全管理认证不是针对某个产品或服务的单独认证，而是对于企业管理体系的综合认证。

●认证依据

GB/T 41479–2022《信息安全技术 网络数据处理安全要求》及相关标准规范。

●认证模式与流程

数据安全管理认证的认证模式是“技术验证 + 现场审核 + 获证后监督”，具体流程如下图：

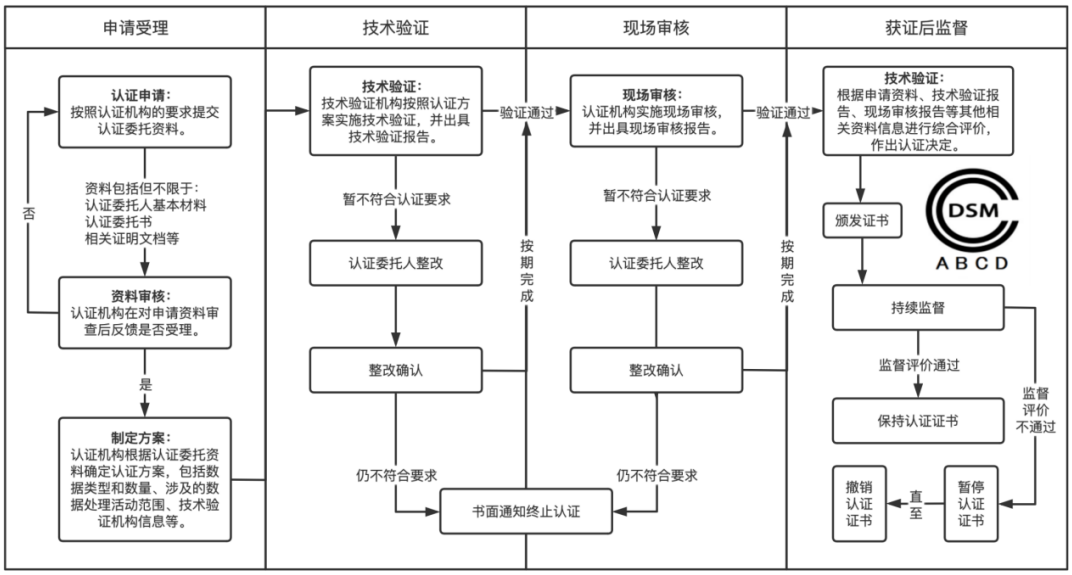


图 3–1　数据安全管理认证流程图

●证书期限

认证机构根据认证委托资料、技术验证报告、现场审核报告和其他相关资料信息进行综合评价，作出认证决定。对符合认证要求的，颁发认证证书，认证证书有效期为 3 年。不同于网络安全等级保护认证，不需要按照等级划分。

（2）个人信息保护认证（PIP）

2022 年 11 月 4 日，国家市场监督管理总局、国家互联网信息办公室发布《关于实施个人信息保护认证的公告》，正式宣告我国个人信息保护认证制度正式建立。《个人信息保护法》发布以来，落实法律要求的个人信息保护制度不断出台，由于个人信息特性及其处理活动的复杂性，《个人信息保护认证实施规则》将在落实《个人信息保护法》要求、支撑个人信息保护工作、促进个人信息合法有序利用等方面发挥重要作用。国家，鼓励个人信息处理者通过认证方式提升个人信息保护能力，同时要求从事个人信息保护认证工作的认证机构经批准后开展有关认证活动。

●认证目的

我国《个人信息保护法》《个人信息保护认证实施规则》系统规定了个人信息保护认证的适用范围、认证依据、认证模式、认证实施程序、认证证书和认证标志等内容，明确对个人信息处理者开展个人信息收集、存储、使用、加工、传输、提供、公开、删除以及跨境等处理活动进行认证的基本原则和要求。

根据是否包含跨境处理活动，个人信息保护认证可以划分为 PIP 认证（不含跨境处理活动）和 PIPCB 认证（包含跨境处理活动），这种划分实质体现了个人信息保护认证在合规能力证明和跨境提供制度的双重价值。

在《个人信息保护法》确定的“举证责任倒置”原则下，个人信息保护认证在证明个人信息处理者合规能力水平方面有着重要的作用。

个人信息保护认证细化和丰富了个人信息跨境提供制度，《个人信息保护法》首次将其规定为数据出境三种路径之一，符合认证申请条件的企业可通过该认证实现数据跨境传输。

●认证依据

个人信息处理者应当符合 GB/T 35273–2020《信息安全技术 个人信息安全规范》（以下简称“《个人信息安全规范》”）的要求，对于开展跨境处理活动的个人信息处理者，还应符合 TC260–PG–20222A《网络安全标准实践指南个人信息跨境处理活动安全认证规范》（以下简称“《跨境认证规范》”）的要求。

《个人信息安全规范》从个人信息安全基本原则、个人信息的收集、存储、使用、委托处理、共享、转让、公开披露，以及个人信息主体的权利、个人信息安全事件处理、个人信息安全管理要求等诸方面做出了相关要求。《跨境认证规范》主要针对个人信息跨境处理活动从基本原则、个人信息处理者和境外接收方的基本要求、个人信息主体权益保障等方面提出了要求。

●认证对象和范围

个人信息保护认证的对象是个人信息处理者开展的个人信息处理活动，认证申请主体应为个人信息处理者。个人信息处理活动包括个人信息收集、存储、使用、加工、传输、公开、跨境提供等，认证范围涵盖个人信息处理活动涉及的组织范围、业务范围、系统范围等，涉及个人信息处理活动

的组织管理、制度措施、技术处理等方面。

个人信息保护认证涉及数据跨境场景，个人信息处理者应梳理对照个人信息向境外提供的管理要求，选择适合自身情况的管理方式。对不属于评估范围的情形，个人信息处理者通过认证后可直接向境外提供；对属于评估范围的情形，认证结果可作为个人信息出境安全评估输入。

结合认证制度特点，适合采用认证方式满足向境外提供个人信息管理要求的个人信息处理者包括但不限于：1）向境外接收方持续提供个人信息的个人信息处理者；2）跨国公司或者同一经济、事业实体下属子公司或关联公司之间的个人信息跨境处理活动；3）落实法规标准要求，亟需加强个人信息跨境提供安全制度措施、规范开展个人信息处理活动的个人信息处理者；4）为向个人信息主体、境外接收方等明示个人信息处理达到相关标准要求的个人信息处理者。

●认证模式与流程

认证模式是“技术验证 + 现场审核 + 获证后监督”，具体流程如下：

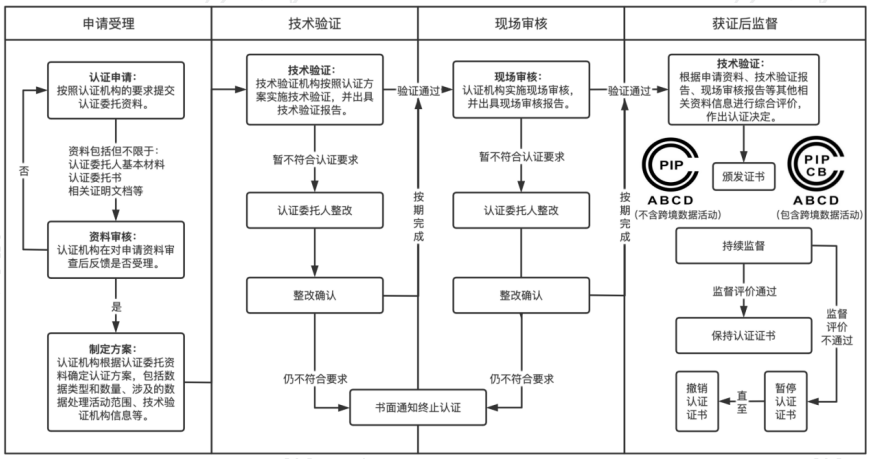


图 3–2　个人信息保护认证流程图

●认证时限及证书有效期

自认证受理之日起至作出认证决定所实际发生的工作日，包括认证申请资料审核时间、技术验证时间、现场审核时间、认证决定和证书批准以及制作时间，一般为 70 个工作日（不包含整改时间）。

认证证书有效期为 3 年。在有效期内，通过认证机构的获证后监督，保持认证证书的有效性。证书到期还需延续使用的，个人信息处理者应在有效期届满前 6 个月内向认证机构提出认证申请。认证机构采用获证后监督的方式，对符合认证要求的委托换发新证书。

●如何申请个人信息保护认证

个人信息处理者在认证申请时，应提交认证申请书、自评价表以及相关附件证明材料。为便于认证顺利开展，提高认证工作效率，申请认证的个人信息处理者可提前了解标准要求和认证流程、下载相应模板，如实、准确填报认证申请书、自评估表，准备好附件证明材料。个人信息保护认证范围与个人信息种类、数量、敏感程度以及个人信息处理情况、个人信息处理者组织管理等密切相关，不同业务场景的评价方法和指标不尽相同，需要企业的密切配合和充分沟通。

3.2.2.“三种路径”推动数据出境规则加快落地

2022 年，数据出境走向规范化，数据出境传输的规则、办法陆续出台，为涉及跨境服务的数据运营者构建了可落地实操的数据出境三种途径，即：（1）通过网信部门的数据出境安全评估；（2）经专业机构进行个人信息保护认证；（3）与境外接收方签订标准合同条款。

鉴于个人信息保护认证制度已于前文论述，以下主要对数据出境安全评估和数据出境标准合同进行说明。

2022 年 7 月 7 日，国家互联网信息办公室发布了《数据出境安全评估办法》（以下简称“《评估办法》”），办法于 9 月 1 日起施行。《评估办法》为数据出境安全评估在监管模式、评估范围、评估要求等方面提供了具有可操作性的依据。

（1）数据出境安全评估

在评估范围上，《评估办法》在第四条中明确以下主体在进行数据出境时必须通过数据出境安全评估：1）数据处理者向境外提供重要数据；2）关键信息基础设施运营者和处理 100 万人以上个人信息的数据处理者；3）自上年 1 月 1 日起累计向境外提供 10 万人个人信息或者 1 万人敏感个人信息的数据处理者。

在评估方式上，数据出境安全评估采取“风险自评估与安全评估相结合”的方式，在向网信部门申报安全评估前，需先进行数据出境风险自评估。

●数据出境风险自评估

自评估主要关注“数据出境的合法性、正当性、必要性”、“出境数据的重要程度”、“境外接收方的责任义务和数据安全能力”、“数据出境的风险”、“数据出境的法律文件”等内容。

●个人信息保护影响评估

《个人信息保护法》第 55 条明确向境外提供个人信息前，应当进行个人信息保护影响评估（“PIA”）。由此可知，《个人信息保护法》下个人信息出境前进行 PIA 属于强制性义务，无论企业适用《个人信息保护法》第 38 条中任何一个出境路径，都需进行 PIA。

在评估内容上，数据出境安全评估与风险自评估都会关注“数据出境的合法性、正当性、必要性”、“出境数据的风险”、“与境外接收方拟订立的法律文件”等的事项。但对于数据出境安全评估而言，境外接收方所在国家或者地区的数据安全保护政策法规及网络安全环境对出境数据安全的影响应是评估重点。与自评估事项的另一个显著区别在于，数据出境安全评估还会关注“守法情况”。

在监管模式上，《评估办法》构建了自上而下的数据出境逐级审查监管模式，第一步是省级网信部门的完备性查验，第二步则是国家网信部门组织国务院有关部门、省级网信部门、专门机构等开展的实质性安全评估。

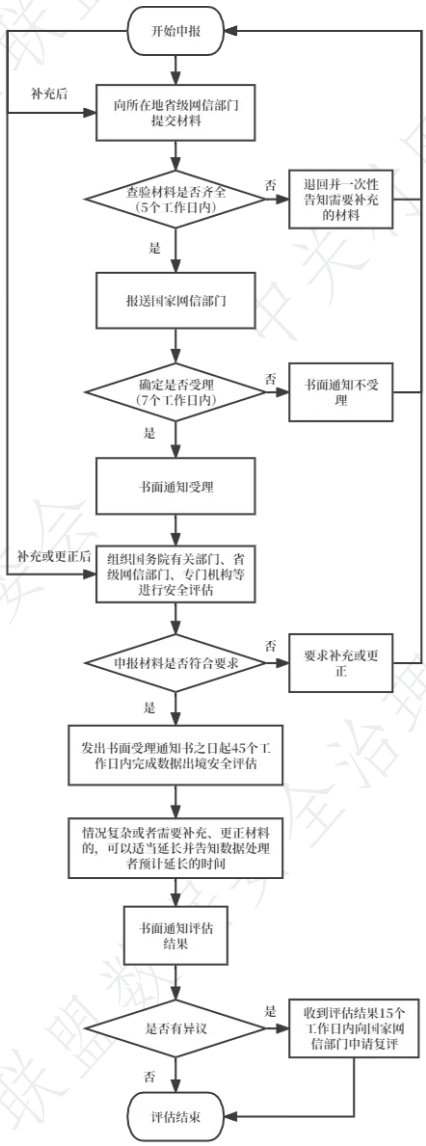


图 3-3　评估办法数据出境评估认证流程图

《评估办法》对数据出境安全评估的设定了 2 年的有效期，自安全评估结果出具之日起计算。2 年有效期的设定为企业开展数据出境活动提供了较为稳定的预期。有效期届满，需要继续开展数据出境活动的，应当在有效期届满 60 个工作日前重新申报评估。

（2）个人信息出境标准合同

2023 年 2 月 22 日，国家互联网信息办公室发布《个人信息出境标准合同办法》（简称“标准合同办法”）。该《标准合同办法》对标准合同具体适用条件、标准合同主要内容和备案要求等内容作出规定，并以附件形式提供了国家网信办制定的个人信息出境标准合同模板。

《标准合同办法》第四条明确提出采取标准合同方式向境外提供个人信息的个人信息处理者应当同时满足以下条件：（1）非关键信息基础设施运营者；（2）处理个人信息不满 100 万人的；（3）自上年 1 月 1 日起累计向境外提供个人信息不满 10 万人的；（4）自上年 1 月 1 日起累计向境外提供敏感个人信息不满 1 万人的。

在使用该标准合同文本时可以进一步关注下述事项：

●与其他出境相关的合同的关系

个人信息处理者可以与境外接收方约定其他条款，但不得与标准合同相冲突。而在实践中，其他法域的监管机构也规定了通过相应的标准合同文本管理跨境个人信息传输的相应场景和条件（例如欧盟 SCCs 等），因此跨国企业将会面临着协调不同法域标准合同文本的问题。

●关于适用委托处理的场景

《个人信息保护法》规定个人信息处理者和受托人的角色。个人信息处理者在个人信息处理活动中可以自主决定个人信息处理目的、处理方式，而受托人则是接受个人信息处理者委托而处理个人信息。标准合同模板中规定了个人信息处理者向境外接收方提供个人信息的模式，另标准合同模板在境外接收方义务中，规定了“受个人信息处理者委托处理个人信息”的义务，说明境外接收方可以是受托人的角色，接受委托处理个人信息。

●单独同意

标准合同模板在“个人信息处理者的义务”及境外接收方的义务中，均规定了“单独同意”的要求，与《个人信息保护法》的要求保持一致。

●责任承担

标准合同模板明确规定了“个人信息处理者”的义务、“境外接收方”的义务。在责任承担上，任何一方因违反标准合同而侵害个人信息主体享有的权利，应当对个人信息主体承担民事法律责任，且不影响相关法律法规规定个人信息处理者应当承担的行政、刑事等法律责任。双方依法承担连带责任的，个人信息主体有权请求任何一方或者双方承担责任。一方承担的责任超过其应当承担的责任份额时，有权向另一方追偿。

3.3. 法律

我国目前已形成以《网络安全法》《数据安全法》《个人信息保护法》三部法律为核心的法律架构，并分别从数据所承载系统的安全保障、数据本身的安全保护以及个人信息的安全保护的层面构建较为完整的数据安全保护体系。

3.3.1.《网络安全法》保障网络与信息安全

我国于 2016 年颁布并于 2017 年施行的《网络安全法》是我国网络安全管理方面的第一部基础性立法，旨在应对我国网络安全领域的严峻形势，以制度建设加强网络空间治理，规范网络信息传播秩序，惩治网络违法犯罪。《网络安全法》全面地规定网络与信息安全治理的基本规则，以网络运营者及关键信息基础设施运营者为主要规制对象，明确网络运行安全、网络信息安全、监测预警与应急处置等方面的义务。

近年来，各机构因网络安全防护能力薄弱进而导致的网络攻击、网络安全事件层出不穷、数据泄露及毁损危机凸显，由于网络安全的一大重要内容即是保障网络数据的完整性、保密性、可用性

的能力，因此《网络安全法》对于构建数据安全保障体系有着重要的意义。具体而言，《网络安全法》通过规定下述措施，以强化数据安全保障。

（1）保障网络运行安全

《网络安全法》第 21 条构建了网络安全等级保护制度，在保障网络系统安全的组织架构及管理体系上，《网络安全法》要求制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任。

在保障网络系统安全的技术体系上，《网络安全法》要求采取包括防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；采取数据分类、重要数据备份和加密等措施。

针对关键信息基础设施的运营者，《网络安全法》在第三章第二节中施加了更多的安全保护义务。而且，《网络安全法》第 37 条强化对关键信息基础设施运营者数据跨境传输的监管，提出数据本地化存储及跨境传输安全评估的要求，明确“关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定”。

（2）保障网络用户信息安全

在保障网络数据安全的总体要求上，《网络安全法》第 10 条提出保障网络数据完整性、保密性和可用性的要求；第 18 条强调了数据利用与数据安全之间的平衡，鼓励开发网络数据安全保护和利用技术。

在保障网络用户信息安全的管理体系上，《网络安全法》第 40 条要求建立健全用户信息保护制度。

在保障网络用户信息安全的技术措施上，《网络安全法》第 40、42 条重点要求对其收集的用户信息严格保密；采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。

同时，《网络安全法》第 47 条加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

3.3.2.《数据安全法》构建数据安全治理框架

由于数据安全已成为事关国家安全与经济社会发展的重大问题，为了有效应对数据这一非传统领域的国家安全风险与挑战，切实加强数据安全保护，维护公民、组织的合法权益，并发挥数据的基础资源作用和创新引擎作用，推进政务数据资源开放和开发利用，2021 年我国颁布并实施《数据安全法》。《数据安全法》作为数据安全领域的基础性法律，重点确立数据安全保护管理各项基本制度，构建起数据安全治理的框架，强调数据开发利用与保障数据安全并重的思路，将个人、企业和公共机构的数据安全纳入保障体系，确立了对数据领域的全方位监管。

（1）数据开发利用与数据安全并重

《数据安全法》在第 1 条立法目的中就将“保障数据安全，促进数据开发利用”纳入，强调数据开发利用与保障数据安全并重的思路。而且，《数据安全法》在第二章也对数据安全与发展进行专章规定，提出一系列促进数据开发利用的思路及措施，包括：国家统筹发展和安全，坚持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；国家实施大数据战略，推进数据基础设施建设，鼓励和支持数据在各行业、各领域的创新应用；国家推进数据开发利用技术和数据安全标准体系建设。国务院标准化行政主管部门和国务院有关部门根据各自的职责，组织制定并适时修订有关数据开发利用技术、产品和数据安全相关标准。国家支持企业、社会团体和教育、科研机构等参与标准制定；国家建立健全数据交易管理制度，规范数据交易行为，培育数据交易市场等。

（2）构建数据安全制度体系

由于不同维度的数据的价值不一，而且对于国家利益、社会利益、个人利益有着不同程度的影响，数据安全治理首先需要实施数据的分类分级保护，以避免因重要数据泄露、损毁带来影响国家安全、社会安全的严重后果。

鉴于此，《数据安全法》第 21 条确立了以数据分类分级为核心的安全制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。同时，《数据安全法》第 22 条要求建立相应的数据安全风险评估、报告、信息共享、监测预警机制及数据安全应急处置机制等。对于开展数据处理活动的主体，可以数据分类分级为基础，形成组织、管理、技术体系相融合的数据安全治理体系。

（3）实施全生命周期的数据安全保护

《数据安全法》第四章紧盯数据泄露、数据漏洞以及非法使用数据的风险，从数据处理的全生命周期提出合规要求，包括开展数据处理活动应当建立健全全流程数据安全管理制度；采取相应的技术措施和其他必要措施，保障数据安全；加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；不得窃取或者以其他非法方式获取数据等。

为了实现数据生命周期安全保护的要求，开展数据处理活动可采取集中策略管控能力与单点防护能力结合的防控措施，统一部署防护策略，在数据收集、存储、使用、加工、传输、提供、公开等数据处理活动中采取相适应的防护技术和能力。

（4）推进政务数据的安全与开放

《数据安全法》第五章推进政务数据的安全与开放，强调提升运用数据服务经济社会发展的能力。在保障政务数据安全方面，要求国家机关应当依照法律、行政法规的规定，建立健全数据安全管理制度，落实数据安全保护责任，保障政务数据安全；国家机关委托他人建设、维护电子政务系统，存储、加工政务数据，应当经过严格的批准程序，并应当监督受托方履行相应的数据安全保护义务。受托方应当依照法律、法规的规定和合同约定履行数据安全保护义务，不得擅自留存、使用、泄露或者向他人提供政务数据。

在推进政务数据开放方面，要求国家机关应当遵循公正、公平、便民的原则，按照规定及时、准确地公开政务数据；国家制定政务数据开放目录，构建统一规范、互联互通、安全可控的政务数据开放平台，推动政务数据开放利用。

3.3.3.《个人信息保护法》保障个人信息权益

相较于一般数据，个人信息因对个人权益的影响需要进行专门的保护。为了解决一些企业、机构甚至个人，从商业利益等出发，随意收集、违法获取、过度使用、非法买卖个人信息，利用个人信息侵扰人民群众生活安宁、危害人民群众生命健康和财产安全等问题，在保障个人信息权益的基础上，促进信息数据依法合理有效利用，2021 年颁布并施行的《个人信息保护法》是我国首部关于保护个人信息的专门性法律。这部法律以数据中的“个人信息”为主要规范对象，划定个人信息全生命周期处理的安全保护规则，以保护个人信息权益、促进个人信息合理利用。具体如下：

（1）个人信息全生命周期处理的防护

根据《个人信息保护法》，个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等的全生命周期，相应个人信息处理的风险也贯穿于个人信息处理的始终。例如，在个人信息采集传输阶段，因网络端口及传输通道的安全性问题而导致个人信息的毁损和丢失；在个人信息存储阶段，因未采取加密、脱敏存储而导致敏感信息的泄露；在个人信息使用阶段，因超权限的访问或者未经授权的使用而导致个人信息对外泄露、个人信息滥用；在个人信息销毁阶段，因未及时、有效销毁存储介质上的个人信息而导致的个人信息泄露等等。

鉴于此，《个人信息保护法》以第一章总则及第二章的一般规定划定了个人信息全生命周期处理的规则，要求个人信息处理应具备包括征得个人主体同意在内的合法基础，告知个人完整的个人信息处理事项。同时，《个人信息保护法》也对需要重点保护的敏感个人信息、风险程度较高的个人信息跨境提供予以特别规定。在《个人信息保护法》第二章第二节项下，对于处理敏感个人信息的，需具备具有特定的目的和充分的必要性及采取严格保护措施下方可处理，并且还要求取得个人的单独同意等；在《个人信息保护法》第三章项下，对于个人信息跨境提供，划定应当具备的条件，根据第 38 条，满足下列条件之一才可向境外提供个人信息，包括：（1）通过国家网信部门组织的安全评估；（2）经专业机构进行个人信息保护认证；（3）按照国家网信部门制定的标准合同与境外接收方订立合同等条件；（4）法律、行政法规或者国家网信部门规定的其他条件。

（2）明确个人信息处理者所应采取的组织措施及技术措施

在《个人信息保护法》第五章规定了个人信息保护的组织架构及管理体系，个人信息处理者应当承担个人信息保护的主要责任；在作为个人信息处理者的组织机构内部，要求制定内部管理制度和操作规程；合理确定个人信息处理的操作权限；指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督等，并对重要平台、大型个人信息运营者设定了额外个人信息保护义务。

在个人信息保护的技术措施上，要求采取措施防止未经授权的访问以及个人信息泄露、篡改、丢失，包括对个人信息实行分类管理；采取相应的加密、去标识化等安全技术措施。

（3）赋予个人充分的个人信息权利，保障个人信息权益

根据《个人信息保护法》第四章，我国赋予个人充分的个人信息权利，包括个人对其个人信息的处理享有知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理；个人有权向个人信息处理者查阅、复制其个人信息；个人有权请求个人信息处理者更正、补充不准确或不完整的个人信息；个人在特定情形下有权请求个人信息处理者删除个人信息；个人有权要求个人信息处理者对其个人信息处理规则进行解释说明等。

而且，《个人信息保护法》第 50 条要求个人信息处理者应当建立便捷的个人行使权利的申请受理和处理机制，并赋予个人可以在个人信息处理者拒绝个人行使权利的请求下向法院起诉的权利。上述做法充分保障了个人在其个人信息处理活动中的权益。

3.3.4. 网络安全、数据安全与个人信息保护的关系

数据天然具有流动性、可复制性等特点，导致在使用过程中存在易泄露、篡改和滥用等安全风险，为个人、企业乃至国家的利益和安全都带来了严峻的挑战。网络安全、数据安全和个人信息保护都绕不开数据话题，因此这些都是安全领域中要解决的基本问题，也是数字经济可持续发展、企业数字化转型成功实施和依托数字技术不断提升国家治理能力现代化水平的基本要求。

如前所述，我国围绕网络安全、数据安全及个人信息安全所构建的法律体系已经相对成熟；回归到三者关系的本质上，既有密切的联系，又有区别。首先，从层次和功能来看，三者都属于可被视为信息安全的子领域。具体来说，网络安全所保护的是数据所承载系统的运行，数据安全和个人信息安全都聚焦于数据本身的安全，数据安全宏观性地对数据保护和数据处理者提出制度要求，包括个人信息和非个人信息，个人信息安全将范围限缩为与个人密切相关的数据信息在更多具体场景的保护。从法律层面看，《网络安全法》对应网络系统的安全管理，《数据安全法》对应数据的安全管控，《个人信息保护法》对应个人信息的安全保障；《网络安全法》和《数据安全法》旨在维护国家安全、社会公共利益和组织权益，前者强调网络安全与网络空间的国家主权，后者侧重于数据安全以及基于数据安全所体现的国家安全。《个人信息保护法》以个人主体出发，为了维护公民个人的隐私、人格、人身、财产等权益，规范个人信息处理活动，促进个人信息有序开发利用。

从技术层面来看，三者有共性也有差异性。个人信息往往以结构化数据或非结构化数据形式存储在各类信息或数据库系统中，也会和其他类型的数据一样历经采集、存储、处理、传输、交换、销毁等阶段。在数据全生命周期的各个阶段也面临着和一般数据相似的完整性、可用性和保密性等方面的风险和挑战。因此，保护个人信息和保护一般数据的技术防护手段也高度相近，加密、脱敏、分类分级、安全评估等体系化的关键数据安全技术都能够有效地支撑个人信息保护业务；而为了实现个人信息安全和数据安全，网络安全作为其存储系统，必然需要在前述各阶段提升产品、服务的安全性。不同之处主要体现在数据处理者相较于个人信息处理者需要在数据交易及中介、数据分级分类、数据安全风险监控与报送等层面达到相应技术要求，网络运营者相较于前两者则更侧重网络安全等级制度、安全认证和检测、关键信息基础设施运营等层面的达到相应技术要求。

此外，从目标来看，三者具有共同的目标。网络安全、数据安全与个人信息保护都属于信息安

全的重要部分，都以保障信息资产的机密性、完整性和可用性为重心，即 CIA（Confidentiality，Integrity，Availability）三大原则。因此，数据安全治理需要三者协同作用。实现高度的信息安全离不开数据安全策略的实施、网络安全的持续保护和不断完善的个人信息保护制度、技术。在没有可靠数据安全措施的情况下，信息资产将面临更大风险，从而损害个人信息乃至整个组织的信息安全水平。

总之，网络安全、数据安全和个人信息保护是相辅相成的关系，三者涉及个人、企业、国家多个层面。个人是网络安全、数据安全和个人信息保护的最广泛参与者，需要加强对个人信息保护，保障个人的合法权益，维护人格尊严；企业是网络安全、数据安全和个人信息保护的关键主体，保障企业数据安全对于产业健康发展具有重要意义，企业层面要保证合法合规地搜集和利用个人数据，促进产业有序发展；网络安全、数据安全目前是网络空间安全的焦点，是事关国家安全与经济社会发展的重大问题，在国家层面要保障经济稳定和国家安全，维护国家网络空间安全和数据主权，才能为个人信息保护提供最坚实的基础。

3.4. 行政法规

3.4.1.《关键信息基础设施安全保护条例》实施关基重点保护

（1）重点防范关键信息基础设施风险

我国秉承“抓重点、保关键”的立法思路，2017 年 6 月 1 日生效的《网络安全法》第 31 条以列举的方式引入了关键信息基础设施的概念，列举了公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务 7 个重要行业和领域，并规定关键信息基础设施的具体范围和安全保护办法由国务院制定。

为配合《网络安全法》第 31 条的实施，2021 年 9 月 1 日生效的《关键信息基础设施安全保护条例》第二章专门规定了关键信息基础设施的认定程序，规定公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的主管部门、监督管理部门是负责关键信息基础设施安全保护工作的部门。保护工作部门制定关键信息基础设施认定规则，并根据该认定规则组织认定本行业、本领域的关键信息基础设施，及时将认定结果通知运营者，并通报国务院公安部门。通过制定《关键信息基础设施安全保护条例》，我国实施对关键信息基础设施的重点保护。

（2）重点强调对数据安全的保护

《网络安全法》《数据安全法》《关键信息基础设施安全保护条例》均对涉及关键信息基础设施的数据进行特别保护。《网络安全法》第 37 条强调关键信息基础设施运营者在中国境内收集个人信息和重要数据本地化存储及跨境数据传输安全评估的义务。《数据安全法》第 31 条也提出关键信息基础设施的运营者在中国境内运营中收集和产生的重要数据的出境安全管理适用于《网络安全法》的规定。

《关键信息基础设施安全保护条例》进一步强调对数据安全的保障，包括关键信息基础设施运营者应维护数据的完整性、保密性和可用性；履行个人信息和数据安全保护责任，建立健全个人信

息和数据安全保护制度；发生重要数据泄露、较大规模个人信息泄露等情形时，保护工作部门及时向国家网信部门、国务院公安部门报告的义务等。

《关键信息基础设施安全保护条例》明确规定了责任的落实，第十三条规定："运营者应当建立健全网络安全保护制度和责任制，保障人力、财力、物力投入。运营者的主要负责人对关键信息基础设施安全保护负总责，领导关键信息基础设施安全保护和重大网络安全事件处置工作，组织研究解决重大网络安全问题。"

用法令规定"主要负责人负总责"实行一把手负责制，在网安领域是第一次。

同时，为了进一步发现安全风险，《关键信息基础设施安全保护条例》第 17 条也要求运营者应当自行或者委托网络安全服务机构对关键信息基础设施每年至少进行一次网络安全检测和风险评估，对发现的安全问题及时整改，并按照保护工作部门要求报送情况。

3.4.2.《网络数据安全管理条例（征求意见稿）》细化数据安全治理规则

2021 年国家互联网信息办公室代国务院颁布《网络数据安全管理条例（征求意见稿）》，对《网络安全法》《数据安全法》《个人信息保护法》的规则予以进一步的细化，推动上述法律的进一步落地。

《网络数据安全管理条例（征求意见稿）》规定了数据安全的一般规则、个人信息保护、重要数据安全、数据跨境安全管理、互联网平台运营者义务等的重要内容，具体而言：

（1）要求数据处理者应当采取备份、加密、访问控制等必要措施，保障数据免遭泄露、窃取、篡改、毁损、丢失、非法使用，应对数据安全事件，防范针对和利用数据的违法犯罪活动，维护数据的完整性、保密性、可用性；按照网络安全等级保护的要求，加强数据处理系统、数据传输网络、数据存储环境等安全防护；

（2）细化取得个人同意的合规要求、个人信息处理规则等内容；

（3）重要数据安全，进一步明确数据安全管理机构的具体职责，并要求数据处理者履行制定数据安全培训计划、优先采购安全可信的网络产品和服务等义务；

（4）数据跨境安全管理，要求建立健全数据跨境安全相关技术和管理措施；

（5）要求互联网平台运营者对接入其平台的第三方产品和服务承担数据安全管理责任，利用人工智能、虚拟现实、深度合成等新技术开展数据处理活动，按照国家有关规定进行安全评估。

3.5. 部门规章及规范性文件

3.5.1. 数据安全的协同治理

数据安全对于各行各业都十分重要，在国家互联网信息办公室负责全国互联网信息内容管理工作、并负责监督管理执法的统筹协调下，各领域内各相关部门协同共治。

在网络和数据安全领域，国家网信部门负责统筹协调网络数据安全和相关监管工作。各地区、各部门在本地区、本部门工作中负责网络安全保护和监督管理工作，对收集和产生的数据及数据安

全负责；国务院电信主管部门、公安部门和其他有关机关在各自职责范围内承担数据安全监管职责；工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域网络数据安全监管职责；县级以上地方人民政府有关部门的网络数据安全保护和监督管理职责，按照国家有关规定确定。

以关键信息基础保护为例，参照《关键信息基础设施安全保护条例》和《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》，在国家网信部门统筹协调下，国务院公安部门负责指导监督关键信息基础设施安全保护工作；国务院电信主管部门和其他有关部门依照本条例和有关法律、行政法规的规定，在各自职责范围内负责关键信息基础设施安全保护和监督管理工作；省级人民政府有关部门依据各自职责对关键信息基础设施实施安全保护和监督管理。

网信部门、工信部门、公安部门以及金融、卫生等行业主管机构均在各自职责范围内颁布了数据安全治理的规章及规范文件。例如，国家互联网信息办公室、工信部等五部门发布《汽车数据安全管理若干规定（试行）》，国家互联网信息办公室、国家发改委等十三部门联合发布《网络安全审查办法》，国家互联网信息办公室发布《数据出境安全评估办法》、工信部发布《工业和信息化领域数据安全管理办法（试行）》、中国银行保险监督管理委员会发布《银行业金融机构数据治理指引》、国家卫生健康委员会发布的《国家健康医疗大数据标准、安全和服务管理办法（试行）》等。

3.5.2. 重要规章及规范性文件

（1）整体要求

总体规范上，2021 年 12 月 28 日，国家互联网信息办公室、国家发改委等十三部门联合发布《网络安全审查办法》（“《办法》”），适用于关键信息基础设施运营者采购网络产品和服务，网络平台运营者开展数据处理活动，影响或者可能影响国家安全的情形。《办法》规定了网络安全审查应考虑的国家安全风险因素，明确网络安全审查的具体流程。其中，在网络安全审查应考虑的国家安全风险因素中，特别考虑数据安全的因素，将“核心数据、重要数据或者大量个人信息被窃取、泄露、毁损以及非法利用、非法出境的风险”、“上市存在关键信息基础设施、核心数据、重要数据或者大量个人信息被外国政府影响、控制、恶意利用的风险，以及网络信息安全风险”纳入。

2021 年 10 月 29 日，国家互联网信息办公室发布《数据出境安全评估办法》，旨在规范数据出境活动，保护个人信息权益，维护国家安全和社会公共利益，促进数据跨境安全、有序流动。该办法明确需要申报数据出境安全评估的情形、数据出境风险自评估及数据出境安全评估所考虑的事项等。

（2）金融领域

2020 年 5 月 21 日，中国银行保险监督管理委员发布了《银行业金融机构数据治理指引》（“《指引》”），《指引》是为引导银行业金融机构加强数据治理，提高数据质量，充分发挥数据价值，提升经营管理水平，全面向高质量发展转变而制定的法规。《指引》共七章五十五条，其中明确了数据治理架构，要求确保数据治理资源充足配置，明确董事会、监事会和高管层等的职责分工，提出可结合实际情况设立首席数据官。《指引》还明确了监管机构的监管责任、监管方式和监管要求。

对于数据治理不满足有关法律法规和监管规则要求的银行业金融机构，要求其制定整改方案，责令限期改正；或与公司治理评价、监管评级等挂钩；也可依法采取其他相应监管措施及实施行政处罚。《指引》实施将进一步提升银行业金融机构的数据治理能力，同时也对数据合规提出了更高的要求。

2021 年 1 月，银保监会发布《中国银保监会监管数据安全管理办法（试行）》，该办法规范了银保监会监管数据安全管理工作，提高了监管数据安全保护能力，目的是建立健全监管数据安全协同管理体系，推动银保监会有关业务部门、各级派出机构、受托机构等共同参与监管数据安全保护工作，加强培训教育，形成共同维护监管数据安全的良好环境。

2021 年 9 月，中国人民银行发布了《征信业务管理办法》，并于 2022 年 1 月 1 日正式实施。明确征信机构采集个人信用信息应当采取合法、正当的方式，遵循最小、必要的原则，并明确告知信息主体采集信用信息的目的，取得信息主体本人同意。通过信息提供者取得个人同意的，信息提供者应当向信息主体履行告知义务。同时，该办法也设专章对信用信息整理、保存、加工进行了规定，明确了征信机构采集的个人不良信息保存期限等。

2022 年 1 月，中国人民银行印发《金融科技发展规划（2022–2025 年）》（“《规划》”），强调全面加强数据能力建设，在保障安全和隐私前提下推动数据有序共享与综合应用，充分激活数据要素潜能，有力提升金融服务质效。

2022 年 12 月，银保监会发布《银行保险机构消费者权益保护管理办法》，并于 2023 年 3 月 1 日正式实施。其中明确规定，银行保险机构应当建立消费者个人信息保护机制，完善内部管理制度、分级授权审批和内部控制措施，对消费者个人信息实施全流程分级分类管控。

2023 年 2 月，中国证券监督管理委员会发布《证券期货业网络和信息安全管理办法》，并将于 2023 年 5 月 1 日起施行。《证券期货业网络和信息安全管理办法》对证券期货业网络和信息安全监督管理体系、网络和信息安全运行、投资者个人信息保护、网络和信息安全应急处置、关键信息基础设施安全保护、网络和信息安全促进与发展、监督管理与法律责任等方面提出了要求。

（3）工业和互联网领域

2019 年 11 月，国家互联网信息办公室、工业和信息化部、公安部、市场监管总局联合制定了《App 违法违规收集使用个人信息行为认定方法》，该办法落实《网络安全法》等法律法规，明确 App 违法违规收集使用个人信息的主要情形，可以为监督执法提供参考，也可以为企业履责合规指明方向，为网民社会监督提供依据。

2021 年 3 月，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联合制定了《常见类型移动互联网应用程序必要个人信息范围规定》（“《个人信息范围规定》”），该规定明确了 39 类常见 App 的基本功能服务和必要个人信息范围，这些 App 覆盖了大众衣食住行、学习工作等日常生活主要方面。《个人信息范围规定》明确要求 App 运营者不得因用户不同意收集非必要个人信息，而拒绝用户使用其基本功能服务，在保障 App 正常运行的同时，保障了用户对 App 基本功能服务的使用权，以及对收集使用非必要个人信息的知情权和决定权。

2022 年 12 月 8 日，工业和信息化部印发《工业和信息化领域数据安全管理办法（试行）》（以下简称“《管理办法》”），自 2023 年 1 月 1 日起施行。该办法的发布标志着工业和电信数据迈向全面行业监管，对规范工业和信息化领域数据处理活动，加强数据安全管理，保障数据安全，促进

数据开发利用，保护个人、组织的合法权益，维护国家安全和发展利益起着重要指导作用。具体而言：

●规范工业和信息化领域数据处理活动

该办法对在工业和信息化领域对国家数据安全管理制度要求进行了细化：一是对基本概念进行了明确。《管理办法》第三条明确了工业和信息化领域数据处理者为工业和信息化领域数据处理者是指能够在工业和信息化领域数据处理活动中自主决定处理目的、处理方式的各类主体；数据范围包括工业数据、电信数据和无线电数据等。处理活动包括数据收集、存储、使用、加工、传输、提供、公开等。二是构建数据分类分级保护体系。《管理办法》第二章规定了对工业和信息化领域数据进行一般数据、重要数据和核心数据分级的“三分法”，并在法规层面对各类数据的范围进行了明确划定，并针对各类数据明确了安全保护要求。包括工业和信息化领域的数据范围、工业和信息化领域数据处理者；二是建立数据全生命周期安全管理制度。《管理办法》第三章针对不同级别数据，从数据收集、存储、使用、加工、传输、提供、公开等全命周期环节提出分级保护要求，并进一步规定了数据处理者的主体责任。

●加强数据安全管理，保障数据安全

一是构建工业和信息化领域数据安全监督评价体系。《管理办法》第四条、第五条、第六条明确工业和信息化部负责督促指导，各地方行业监管部门负责开展数据安全监管，对工业和信息化领域的数据处理活动和安全保护进行监督管理。从而构建了“工业和信息化部、地方行业监管部门”两级监管机制。二是明确重要数据和核心数据处理者安全保护义务。包括建立覆盖本单位相关部门的数据安全工作体系、明确数据处理关键岗位和岗位职责以及建立内部登记、审批等工作机制等。三是建立数据安全监测预警与应急管理机制。《管理办法》第四章要求工业和信息化部和地方行业监管部门分别建设国家层面的和本地区的数据安全风险监测预警机制，以及组织开展数据安全风险监测、预警信息发布、及时排查安全隐患等工作机制。

●促进数据开发利用

一是在自动化决策上，《管理办法》第十六条规定，工业和信息化领域数据处理者利用数据进行自动化决策的，应当保证决策的透明度和结果公平合理。使用、加工重要数据和核心数据的，还应当加强访问控制。二是在数据共享上，第十八条规定，工业和信息化领域数据处理者对外提供数据，应当明确提供的范围、类别、条件、程序等。提供重要数据和核心数据的，应当与数据获取方签订数据安全协议，对数据获取方数据安全保护能力进行核验，采取必要的安全保护措施。三是在数据出境上，《管理办法》第二十一条规定，重要数据和核心数据确需向境外提供的，应当依法依规进行数据出境安全评估。

●维护国家安全和发展利益

一是在数据分类上，《管理办法》将与国家安全相关的重点领域相关的数据作为重要数据和核心数据分类的标准。二是在数据共享上，《管理办法》第十九条规定，数据处理者应当在数据公开前分析研判可能对国家安全、公共利益产生的影响，存在重大影响的不得公开。三是规定了中央企业的数据安全保护义务。包括督促所属公司按照属地行业监管部门要求，履行重要数据目录备案、风险信息上报等，并且要求中央企业应当全面梳理汇总企业集团本部、所属公司的数据安全相关情况，

并及时报送工业和信息化部。

（4）交通运输领域

2022 年 8 月，交通运输部就《公路水路关键信息基础设施安全保护管理办法（征求意见稿）》公开征求意见，进一步细化了公路水路关键信息基础设施认定的考虑因素与责任部门，推动构建交通运输主管部门依法管理、运营者实施主动防护、社会力量共同参与的综合治理体系，更有效、更规范地推进公路水路关键信息基础设施安全保护工作。同年 3 月，工信部、公安部、交通运输部、应急管理部与国家市场监督管理总局联合发布《关于进一步加强新能源汽车企业安全体系建设的指导意见》。要求企业要依法落实关键信息基础设施安全保护、网络安全等级保护、车联网卡实名登记、汽车产品安全漏洞管理等要求。对车辆网络安全状态进行监测，采取有效措施防范网络攻击、入侵等危害网络安全的行为。

（5）医疗卫生领域

2022 年 8 月 29 日，国家卫生健康委、国家中医药局、国家疾控局印发《医疗卫生机构网络安全管理办法》。要求“各医疗卫生机构应履行数据安全保护义务，坚持保障数据安全与发展并重，建立健全个人信息保护和数据安全保护制度，建立本单位数据分类分级标准，加强数据全生命周期安全管理工作。”

（6）电力领域

2022 年 4 月 16 日，国家发展和改革委员会发布《电力可靠性管理办法（暂行）》，规定，电力企业应当落实网络安全等级保护、关键信息基础设施安全保护和数据安全制度，加强网络安全审查、容灾备份、监测审计、态势感知、纵深防御、信任体系建设、供应链管理等工作；同年 12 月，国家能源局发布《电力行业网络安全管理办法》及《电力行业网络安全等级保护管理办法》。对电力行业关键信息基础设施运营者的安保责任进行了细化规定，要求电力企业主要负责人对关键信息基础设施安全保护负总责，要明确一名领导班子成员作为首席网络安全官，专职管理或分管关键信息基础设施安全保护工作。国家能源局及其派出机构结合关键信息基础设施网络安全检查，定期组织对运营有第三级及以上网络的电力企业开展抽查。

（7）物流领域

2022 年 1 月，国家邮政局发布《快递市场管理办法（修订草案）》（征求意见稿），该草案特别增加了有关个人信息保护的相关规定，包括要求经营快递业务的企业应当建立用户个人信息安全管理制度和操作规程，处理用户个人信息活动符合法律、行政法规以及国务院邮政管理部门的规定，并要求快递企业应当合法处理用户个人信息，采取加密、去标识化等安全技术措施保护快递运单信息安全，不得完整显示自然人身份信息。

2023 年 2 月，国家邮政局发布《寄递服务用户个人信息安全管理规定》。根据《寄递服务用户个人信息安全管理规定》，寄递企业应当建立健全寄递服务用户个人信息安全保障制度和措施，明确企业部门、岗位的安全保护责任，合理确定寄递服务用户个人信息处理的操作权限，定期对从业人员进行安全教育和培训。寄递企业应当对快递电子运单单号资源实施全过程管理，并采用射频识别、虚拟安全号码、电子纸等有效技术手段对快递电子运单信息进行去标识化处理，防止运单信息在寄

递过程中泄露。

（8）广播传媒领域

2022 年 5 月 30 日，国家广播电视总局印发《广播电视和网络视听领域经纪机构管理办法》，明确要求广播电视和网络视听领域经纪机构、经纪人员收集、处理、使用个人信息，应当遵守国家有关法律规定，对于广播传媒领域落实《个人信息保护法》中个人信息保护的要求有着重要指导意义。

3.6. 地方性法规

我国各地方同样在不断探索数据安全治理的规则及模式，已出台的《深圳经济特区数据条例》《上海市数据条例》《浙江省公共数据条例》《贵州省大数据安全保障条例》等均在不断深化我国的数据安全治理的模式，提出了一些数据安全治理的新措施。

3.6.1. 创新数据安全治理新模式

《深圳经济特区数据条例》涵盖个人数据、公共数据、数据要素市场、数据安全等方面，可以认为是国内数据领域首部基础性、综合性立法。在个人数据部分，《深圳经济特区数据条例》明确规定自然人对其个人数据享有人格权益，细化个人信息处理、告知与同意、个人信息权利等的具体规则；在数据安全部分，《深圳经济特区数据条例》明确数据处理全流程记录、数据存储进行分域分级管理、重要系统和核心数据的容灾备份、建立数据销毁规程等的要求。

《上海市数据条例》涉及数据权益保障、公共数据、数据要素市场、数据资源开发和应用、浦东新区数据改革、长三角区域数据合作等重点内容，强调数据资源的利用与开发，以及数据资源的合作，并通过明确数据安全责任制、开展数据处理活动所应履行的义务、健全数据分类分级保护制度等保障数据安全。

此外，其他一些省市地区也制定了数据发展与安全促进相关的法律类文件。典型的包括《天津市促进大数据发展应用条例》《贵阳市大数据安全管理条例》《重庆市数据条例》《苏州市数据条例》等。

3.6.2. 提供公共数据治理的模式借鉴

上述地方性法规也突出对公共数据的处理的保护，明确公共数据共享、利用的规则。这也为相关政务大数据共享、政务数据安全检测及敏感数据防泄露等提供有益的指导。

《深圳经济特区数据条例》明确对公共数据进行分类管理，实行公共数据目录管理制度，推动公共数据的共享，以共享为原则，以不共享为例外，并构建公共数据共享、公共数据开放、公共数据利用的治理体系；《上海市数据条例》同样建立公共数据共享和开放的机制，也特别规定了公共数据授权运营的模式，提高公共数据社会化开发利用水平；《浙江省公共数据条例》全面规定公共数据平台、公共数据收集与归集、公共数据共享、公共数据开放与利用、公共数据安全等的内容，

促进公共数据应用创新，保护自然人、法人和非法人组织合法权益，保障数字化改革。

此外，《广东省首席数据官制度试点工作方案》提出的政府首席数据官和部门首席数据官也体现出地方在公共数据资源开发利用上的积极尝试与探索。

3.7. 国家标准、行业标准及相关指南

“安全发展，标准先行”，标准化工作是保障网络数据安全的重要基础。为落实国家出台的数据安全相关法律法规要求，围绕数据安全和个人隐私保护，全国信息安全标准化技术委员会及金融、电信、工业、互联网等重点行业、地区颁布了一系列的国家、行业、地方技术标准及相关指南，对法律法规中较为原则性的规定给予了具体的指导。从防止数据泄露、保护个人权益、提升数据安全治理能力等多方面、多角度，提出细化的保护要求与防护措施，对指导各行业组织合法、合规的开展数据安全治理工作，促进数据充分利用、有序流动和安全共享，推动数字经济发展具有重要意义。

网络数据安全标准体系包括基础共性、安全技术、安全管理、重点领域四大类标准：

（1）基础共性标准包括术语定义、数据安全框架、数据分类分级，相关标准为各类标准提供基础性支撑；

（2）安全技术标准从数据采集、传输、存储、处理、交换、销毁等数据全生命周期维度对数据安全关键技术进行规范；

（3）安全管理标准从网络数据安全保护的管理视角出发，指导行业有效落实法律法规关于网络数据安全管理的要求，包括数据安全规范、数据安全评估、监测预警与处置、应急响应与灾难备份、安全能力认证等；

（4）重点领域标准结合相关领域的实际情况和具体要求，围绕移动互联网、车联网、物联网、工业互联网、云计算、大数据、人工智能等重点领域指导行业有效开展网络数据安全保护工作。

具体内容参见附录 E：我国主要数据安全相关标准汇总。

第四章　数据安全技术需求与主流技术工具介绍

《数据安全法》《个人信息保护法》等正式实施以来，配套上位法的法律、法规、标准持续健全，围绕数据生命周期的安全技术需求也愈发明确、清晰，同时，保障数据安全的各类安全工具与相应技术也在不断创新发展，通过从需求和供给两侧对数据安全技术需求和安全技术工具进行全面性、系统化梳理与介绍，为组织践行数据安全治理的技术防护落地提供参考和指引。更进一步面向行业的场景化技术落地方案，可参见本白皮书配套的各行业分册中的详细介绍。

4.1. 数据安全技术需求介绍

数据安全技术体系框架覆盖平台安全、数据全生命周期安全、基础安全，结合组织自身使用场景的体系建设，要依照数据安全建设的方针总则，围绕数据处理活动各场景的安全要求，建立与制度流程相配套的技术能力，并形成平台化应用，发挥技术合力作用。通过持续对数据生命周期内各使用场景进行风险监测，评估现有数据安全控制措施的有效性及薄弱环节，对有问题的风险场景及时进行数据安全整改，优化数据安全相关制度流程，进而持续的提升数据安全防护能力。数据安全技术体系框架如图 4-1 所示：

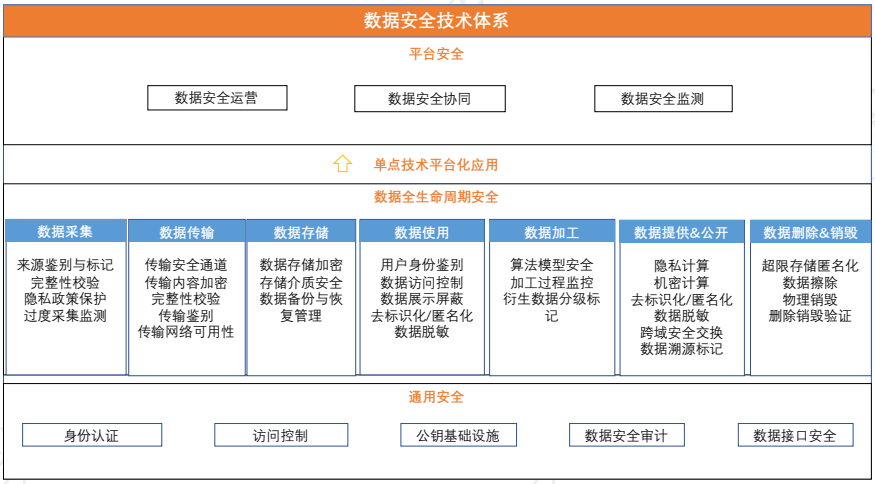


图 4-1　数据安全技术体系框架图

4.1.1. 平台化安全防护需求

单点技术向平台化融合发展趋势愈加强烈。围绕数据全生命周期，各阶段节点的单点防护技术手段已日益健全，但基于安全木桶效应，数据流转需要体系化防护。建立集中化、联动化的安全防护技术需求将这些单点技术进行有效串联，实现面向数据安全风险的动态、纵深防御已成业内共识。

当下，各类数据安全产品之间缺乏有效的联动和统一调度管理，安全风险应对能力难以得到真正提升，这促使数据安全厂商将单体产品安全能力聚合到数据安全管理平台（DSP）中，使其能够帮

助组织更好地进行数据安全建设。DSP 涵盖了各种场景下的数据安全保护需求，以数据发现和数据分类分级为基础，混合了多种技术来实现数据安全防护，例如：数据访问控制，数据脱敏，文件加密等，成熟的 DSP 也可能包含了数据活动监控和数据风险评估的功能。

此外，DSP 可以提高数据的可视性和控制能力，以确保个人、组织和政府之间的数据流动安全。DSP 能够帮助作出更明智的决策，并为组织提供更好的数据安全保护。因此，DSP 的设计理念如下：

（1）数据安全与业务和生产系统紧密结合

因为数据的价值必须在流动中得以体现，那么业务或生产系统就是决定数据如何流动的那一方；而数据安全建设究其根本，就是要保障数据在流动中被安全使用。

数据安全建设既依赖于业务又最终服务于业务，因而要在不影响业务本身的同时，通过简单易用的“一站式”操作完成。DSP 首先根据数据使用情况抽象出多个典型数据使用场景，比如：数据跨境、数据合作共享、数据交易、大数据处理等，形成完整的数据安全场景化解决思路。

（2）以数据分类分级为基础实现产品联动

正所谓不破不立，唯有打破通过“单品堆砌 + 独立功能点拼凑”的固有思维，才能解决由此带来的问题和制约，从而结合客户的真实业务场景构建行之有效的数据安全解决方案。在数据安全治理理念指导下的数据安全建设，要以数据分类分级为基础，即相关建设工作应围绕数据分类分级来展开，通过对数据资产发现、核实及其业务使用场景的备案，到对数据的敏感数据分布、分类分级、合规使用，再到对数据使用过程中可能面临的安全事件及后续风险、问题处置等。

（3）以工作台引导工作，可视化日常运营

针对数据安全的管理、运营与执行是一系列庞杂的工作过程，比如：当监管方明确工作任务方向和重点后，执行者又该在具体工作中通过怎样的业务流程、技术手段和安全策略进行落实？类似的问题在日常运营工作中比比皆是；而数据安全运营管控平台能够以日常运营工作台、待办事项工作台等可视化的方式，将日常运营工作规范化、流程化、指标化——以清晰的业务流程和数据统计，引导监管与执行人员“要做什么、先做什么、后做什么、怎么去做”等等，从而解决相关工作落地难的问题，在提高工作效率的同时，大大降低运营成本投入。

（4）管控与运营并举，运营提高安全能效

在安全能力建设的前期，“安全管控”无疑是建设的重点；而伴随安全管控手段的逐步完善，如何将安全管控日常化，如何在持续使用中完善并优化安全管控的措施和策略，使得前期对安全能力建设的投入发挥更大的能效价值，则成为后续建设的重点。通过构建数据安全平台，可将数据安全运营提升到一个全新的高度，即通过“运营”让安全监测与管控更具目的性，让用户不止于“可用”，还能让用户感到“好用”，并“持续地用起来”。

基于以上设计理念，DSP 产生三大技术需求。

数据安全运营的技术需求：以“更实用、可持续”为设计初衷，“一站式、体系化”的数据安全运营，在合规知识库基础上，可集合包括数据资产梳理、数据库防火墙、数据库审计、数据脱敏、数据库运维管理、数据库加密等在内的各类数据安全产品优势于一身，通过可视化的信息呈现与工作引导，实现全链路流转监测、风险分析研判与预警、安全事件处置与上报，“统一部署、统一监控、统一管理、统一运营”的数据安全日常化、可持续的运营管控目标。

数据安全协同的技术需求：一站式数据分析运算能力，具备敏感数据自动识别、数据自动分级分类管控、数据操作留痕审计、输出结果申报审核等功能的数据安全协同，全程加密传输、缓存和运算、隐私计算，跨部分、跨机构、跨行业的数据开放与共享，搭建统一规范、互联互通、安全可控的数据开放环境，多方协同全程加密传输、缓存和运算，保护数据的安全和隐私，促使数据流通价值最大化，安全合规的推动跨部门、跨机构、跨行业的数据开放与共享，实现了提供数据安全流通和共享的协同。

数据安全监测需求：面向数据安全监管机构和大型企业集团数据安全总体责任部门，依托国家数据安全法规、行业数据安全监管政策和企业数据安全总体策略，数据安全监测以数据安全评估、数据库审计、应用审计为基础，通过平台化的设备管理以及数据流转关联分析能力，打破应用和数据库安全监测的壁垒，实现以数据为中心，全面的数据分类分级安全合规监测。

4.1.2. 全生命周期安全防护需求

4.1.2.1. 数据采集安全

采集数据应坚持“合法、正当、必要”原则，明确采集和处理的目的、方式、范围、规则，数据采集安全主要是保障采集过程的数据完整性和数据来源可追溯，不得超范围采集数据。个人数据采集应按照“明确告知、授权同意”的原则实施，并建立保障个人知情权、决定权，采集敏感个人信息应遵循最小必要原则，业务停止相关采集活动应立即停止。

（1）来源鉴别与标记

数据收集源头的安全是数据价值利用的先决条件，在采集外部相关方数据的过程中，应对数据提供方的身份进行有效验证，需明确采集数据的目的和用途，确保数据源的真实性、有效性和最少够用等原则要求，并规范数据采集的渠道、数据的格式以及相关的流程和方式，并标记采集数据的来源，从而保证数据采集的合规性、正当性和执行上的一致性，符合相关法律法规要求。

（2）完整性校验

采取完整性校验算法对数据采集进行校验，防止数据在采集过程中被篡改和破坏，保护数据采集的完整性，应对数据收集设备进行持续的身份认证，对数据质量的一致性、完整性、准确性等属性进行监控和管理。

（3）隐私政策保护

个人信息处理者在采集敏感个人信息前，应在满足 GB/T 35273 中 5.1、5.2、5.3 和 GB/T 41391 收集的要求基础上，按照最小必要原则明确收集的敏感个人信息范围，收集的敏感个人信息应限于实现处理目的所必要的最小范围；应采取对个人权益影响最小的方式收集敏感个人信息；应仅在用户使用业务功能期间，收集该业务功能所需的敏感个人信息；如有法律明确规定或经公司内部评估确有必要收集敏感个人信息的，需在通过个人信息保护影响评估之后方可执行；收集个人敏感信息应按照业务核心功能或主要服务，进行分项收集。

（4）过度采集监测

针对组织数据和个人信息采集，检验其符合最小必要原则，判断其对组织数据和个人信息的主

体合法权益造成损害的各种风险，对采集数量进行监测，过度采集情况及时告警。

4.1.2.2. 数据传输安全

应明确数据传输相关安全管控措施，如：传输通道加密、数据内容加密、数据接口传输安全、数据传输终端身份鉴别等。对数据传输两端进行身份鉴别，确保传输双方可信任。采用校验技术保证数据在传输过程中的完整性，同时通过备份确保传输网络可用。

（1）传输安全通道

组织内外部在传输数据前，应评估传输通道的安全性，比如：从数据传输加密、传输完整性保护、网络可用性等方面进行评估，发现可能存在的数据传输安全风险和违法违规问题，根据数据分类分级传输管理规定和已有数据安全防护措施部署，设计相应的数据传输策略，选择传输安全通道。

（2）传输内容加密

根据法律法规、商业合同中的要求和业务性能的需求，明确组织机构内需要加密传输的数据范围和国家认可的加密算法，综合实现效果和成本，采取固定的数据加密模块，根据不同数据类型和级别进行数据加密处理，并定期审核并调整数据加密算法或根密钥。

（3）完整性校验

采取完整性校验算法对数据传输的发送和接收进行校验，保护数据传输的完整性，发现数据在传输过程中被篡改和破坏了，要有执行恢复控制的技术能力。

（4）传输鉴别

双向传输数据要对传输通道两端进行主体的身份鉴别和认证，部署独立的公钥 / 私钥对和数字证书，以保证各节点有效的身份认证。

（5）传输网络可用性

通过网络基础链路、关键网络设备的备份建设，实现网络的高可用性，从而保证数据传输过程的稳定性。

4.1.2.3. 数据存储安全

明确数据存储相关安全管控措施，针对不同类别级别的数据采取差异化安全存储保护措施，如：加密、访问控制等。针对存储介质提供有效的技术和管理手段，防止对介质的不当使用而引发的数据泄露风险。明确数据备份与恢复安全策略，建立数据备份恢复操作规程，保障数据的可用性和完整性。

（1）数据存储加密

存储作为 IT 数据基础设施的底座，对保障数据安全可靠尤为重要。数据库加密技术保障结构化数据存储安全，将明文数据经过加密钥匙（加密密钥）及加密函数转换，变成无意义的密文数据；以后需要获取数据内蕴含的信息时，要先将该密文数据经过解密函数、解密钥匙（解密密钥）处理，恢复成原来的明文数据，然后才能对数据及其内的信息加以使用。

（2）存储介质安全

基于组织机构的数据分类分级要求以及介质使用的要求，采取有效的介质净化工具对存储介质

进行净化处理，对介质访问和使用行为进行记录和审计；

（3）数据备份与恢复管理

明确数据备份与恢复的策略和操作规程，建立了用于数据备份、恢复的统一技术，并将具体备份的策略固化，保证相关工作的的自动化执行。建立备份数据的安全管理技术手段，对备份数据的访问控制、压缩或加密管理、完整性和可用性管理。

4.1.2.4. 数据使用安全

通过用户身份鉴别、数据访问控制、数据展示屏蔽、去标识化 / 匿名化、数据脱敏等技术手段，保障数据使用安全。开展数据清洗转换、汇聚融合、分析挖掘等数据加工活动时，应当采用匿名化等措施保护数据主体权益。数据汇聚融合衍生敏感级及以上数据，或导致数据安全级别变化的，应及时评估、调整安全保护措施。

（1）用户身份鉴别

通过用户身份鉴别识别数据的使用是否得到数据所有者的授权，使用流程是否合规。

（2）数据访问控制

数据在使用中发挥价值，但数据在使用过程中的流动性特征，极易导致数据泄露事件的发生。在数据使用阶段，应从数据内容识别和数据细粒度访问控制两个方面实施数据安全防护措施，对应用访问数据库的访问控制进行细粒度访问控制。

（3）数据展示屏蔽

在数据访问者读取数据的过程中，在应用系统开发的时候，加上数据屏蔽的代码，对敏感数据展示进行遮蔽。

（4）去标识化 / 匿名化

个人信息处理者对敏感个人信息的展示的时候，应对需展示的敏感个人信息采取去标识化处理等措施，降低敏感个人信息在展示环节的泄露风险，对于通过匿名化处理的敏感个人信息，应定期评估匿名化处理效果，确保个人信息在当前技术条件下不具备还原能力。

（5）数据脱敏

分为静态脱敏和动态脱敏，静态脱敏是在生产数据用于到测试环节时，要对其中的敏感数据进行脱敏，避免数据泄露。静态脱敏通常会涉及对较大数量的数据进行批量化的处理：静态脱敏系统首先从数据的原始存储环境（通常为生产环境）读入含有敏感信息的数据，然后在非持久化存储条件（系统内存）下按照脱敏策略、规则和算法对数据进行变形等脱敏处理，再将经过处理后的脱敏数据存储到新的目标存储环境中。

4.1.2.5. 数据加工安全

通过算法模型安全、加工过程监控、衍生数据分级标记保障数据加工安全。开展数据清洗转换、汇聚融合、分析挖掘等数据加工活动时，应采用匿名化等措施保护数据主体权益。数据汇聚融合衍生敏感级及以上数据，或导致数据安全级别变化的，应及时评估，调整安全保护措施。

（1）算法模型安全

采用多种技术手段结合以降低数据加工过程中算法模型安全风险，比如基于机器学习的重要数据自动识别、数据安全分析算法设计、推荐歧视等。

（2）加工过程监控

掌握数据安全防护措施部署情况，监控数据加工过程，发现可能存在的数据加工安全风险和违法违规问题。

（3）衍生数据分级标记

应对汇聚融合后产生的衍生数据重新开展数据安全定级工作，根据敏感程度打上分级标记，并采用相应级别的安全保护措施。

4.1.2.6. 数据提供和公开安全

通过隐私计算、机密计算、脱敏等技术保障数据提供和公开安全。建立公开披露数据的审批机制，研判可能产生的影响，数据公开应在官方渠道进行发布，确保数据真实、准确、防篡改，记录审批和发布情况。跨域安全交换同时做好数据溯源标记。

（1）隐私计算

数据提供和公开安全最好做到“数据可用不可见”。隐私计算是“隐私保护计算”的简称，它是一套包含人工智能、密码学、数据科学等众多领域交叉融合的跨学科技术体系。从技术机制来看，隐私计算主要分为三大技术路线，即安全多方计算（密码学）、联邦学习。

（2）机密计算

机密计算是针对数据在使用过程中的安全问题所提出的一种解决方案，其通过基于硬件的可信执行环境对使用中的数据进行保护，从硬件层面实现对数据以及隐私的保护。其中，可信执行环境被定义为提供一定级别的数据完整性、数据机密性和代码完整性保证的环境。

（3）去标识化 / 匿名化

见数据使用安全。

（4）数据脱敏

敏感数据提供和公开的时候，采用访问通道上的动态脱敏技术会监测和拦截数据访问请求，并根据请求中数据使用者的角色、权限、待访问数据的类别级别等信息，按照脱敏策略和规则实时对数据展示进行脱敏。

（5）跨域安全交换

应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信，应在网络边界根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信。

（6）数据溯源标记

数据一旦提供或公开给其他使用方或处理方，数据所有者可能全面失去数据的管理权和监督权，数据水印技术能够在一定程度上对二次传播的数据进行溯源标记，目前数据水印还不能从根本上阻断数据二次传播。

4.1.2.7. 数据删除和销毁安全

应按照国家、行业有关规定及与数据主体的约定进行数据删除或匿名化处理，制定数据销毁管理制度。对存储数据的介质或物理设备采取无法恢复的方式进行数据销毁与删除，明确数据销毁效果评估机制，验证数据删除结果。

（1）超限存储匿名化

敏感数据和敏感个人信息存储环境应具备时效性管理能力，应提供过期存储及其备份彻底删除方法和工具，能够验证个人信息已被删除或匿名化处理。

（2）数据擦除

通过数据覆盖等软件方法数据销毁或者数据擦除。数据擦除中的数据软销毁通常采用数据覆写法。数据覆写是将非保密数据写入以前存有敏感数据的硬盘簇的过程。使用预先定义的无意义、无规律的信息反复多次覆盖硬盘上原先存储的数据，就无法知道原先的数据是“1”还是“0”，也就达到了硬盘数据擦除的目的。

（3）物理销毁

涉及敏感数据和个人信息的存储介质销毁时，应采取专业的存储介质物理销毁设备进行物理销毁。硬盘数据销毁中的硬销毁则通过采用物理、化学方法直接销毁存储介质，以达到彻底的硬盘数据销毁 / 数据擦除的目的。

（4）删除销毁验证

对于通过匿名化处理的数据和敏感个人信息，应定期评估匿名化处理效果，确保个人信息在当前技术条件下不具备还原能力。数据覆写法处理后的硬盘可以循环使用，适应于密级要求不是很高的场合。处理后的硬盘仍有恢复数据的可能，这样就不能达到硬盘数据销毁 / 数据擦除的效力，因此该方法不适用于存储高密级数据的硬盘，这类硬盘必须实施硬销毁，才能保证彻底的硬盘数据擦除，防止涉密数据的流失。

4.1.3. 通用安全防护需求

通用安全防护技术是单点技术和平台技术的基础，主要采用身份认证、访问控制、公钥基础设施、数据安全审计、数据接口安全技术实现。

（1）身份认证

认证是对实体身份确认的过程，授权是为主体授予访问客体权限的过程，需要基于认证和授权动态重构业务访问控制的信任基础。身份认证与访问控制能力由认证、权限、审计、审批、环境感知和安全策略控制等服务，采用动态的访问控制技术提供，对应用、功能、服务、数据等核心资产的访问行为进行精细化访问控制，将用户、设备、应用和服务等的身份均统一抽象成主体身份，通过主体身份属性进行动态认证和鉴权，实现对数据“可用可见、可用不可见、不可用不可见”等状态的统一授权管理。

（2）访问控制

通过设置访问控制策略建立数据安全账户管理体系。包括用户注册、角色管理、权限和授权管

理及身份鉴别等措施；在系统集成商、供应商和外部服务提供商发生变更的情况下，更新访问权限等控制措施；明确职责定位，并在职责定位的基础上，采取最小权限和授权机制；限制组织内设备在外部信息系统中的使用；依据不同的访问级别，把供应链基础设施的接口，选择性地提供给系统集成商、供应商和外部服务提供商；使用自动化方式实现账户管理，包括进行包括通知变更、禁用过期账户、自行审核高危操作和超时自动注销等；从供应链角度，对组织与外部供应商互连的信息系统和操作任务进行核查和记录，包括了解与各类供方的组件/系统连接状况、共同开发和操作环境、共享的数据请求和检索事务等。

（3）公钥基础设施

公钥基础设施能够为数据生命周期防护涉及的身份认证、数据传输、数据存储、数据访问、数据应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系，简单来说，就是利用公钥理论和技术建立的提供安全服务的基础设施。

（4）数据安全审计

构建全链路数据安全审计能力，全链路数据安全审计综合采用数据库审计技术和应用系统安全审计技术，贯穿数据全生命周期各个阶段，覆盖用户访问、系统运维、开发测试、数据对外提供、数据出境等全部业务场景，通过可视化方式按数据分类分级全面分析、展示数据的分布、流动、命令执行成功/失败、风险事件等综合态势。

（5）数据接口安全

组织在建设开放系统、产业链生态或与第三方数据合作时，要实现自身与外部的安全风险隔离，与外部机构的数据交互应通过同意的外联平台或应用程序接口实施，依据“场景必需、最小权限”原则，采取有效措施对接口设计、开发、服务、运行等进行集中安全保护管理。组织向外部敏感数据，应当取得数据主体的单独同意。核心数据和重要数据不得提供外部访问服务，国家或行业监管部门另有规定的除外。

多行业数据开放渠道主要依托于 OpenAPI 这种方式，API 作为应用与数据服务的通信接口，应用场景广泛，已经成为攻击者窃取数据的重点攻击对象。近年来发生了很多重量级的 API 攻击事件，引发了社会各界的广泛关注，API 的监测和管控成为互联网数据流动场景的首要关注技术点。

- OWASP 组织分析调研 API 安全 TOP 10-2019，呈现 API 正面临的十大风险点。
- Salt Security 发布的《State of API Securiy,Q3 2022》，截止 2022 年 Q3，整体 API 流量 168%，恶意 API 流量 117%，受访者遭到 API 安全问题 94%。
- IBM Security X-Force 报告，其分析的数据安全事件中有三分之二是由不安全的 API 造成的。
- Gartner 提供的报告数据分析显示，在 2024 年 API 安全问题引起的数据泄露风险将翻倍。

4.2. 数据安全防护主流技术工具介绍

4.2.1. 技术工具功能及应用场景简介

整体技术工具集按类型总体划分为通用安全类、全生命周期防护类和安全运营与监测平台类三

大类。其中：通用安全类是对各数据生命周期环节技术防护的基础支撑技术，全生命周期防护类是覆盖各数据活动环节的安全防护技术，安全运营与监测平台类是对上述各类单点工具的建设与运行进行平台化的统一管控、统一运营、统一监测，形成事前预防、事中监控、事后审计的整体防护效果。各分类下安全技术工具构成及与安全技术需求的对应关系如下表 4-1 所示：

表 4-1　主流技术工具及与技术需求对应表

数据安全技术体系安全要求			工具名称
全生命周期安全域防护能力要求	数据采集	来源鉴别与标记 过度采集监测 完整性校验	数据安全采集工具
	数据传输	传输安全通道 传输网络可用性 完整性校验 双向传输鉴别 传输内容加密	VPN 光闸 数据防泄露系统
	数据存储	数据存储加密 存储介质安全 数据备份与恢复管理	数据防泄露系统 数据库加密系统 数据备份 / 恢复工具
	数据使用	用户身份鉴别 数据访问控制 数据展示屏蔽 去标识化 / 匿名化	统一身份认证系统 数据防泄露系统 数据零信任平台 数据库运维安全系统 数据库防火墙系统 数据脱敏系统
	数据加工 / 共享 / 公开	隐私计算 机密计算 去标识化 / 匿名化 数据溯源标记 数据脱敏 跨域安全交换	数据安全协同平台 机密计算平台 数据脱敏系统 数据水印工具 数据防泄露系统 跨域共享交换平台
	数据删除 / 销毁	超限存储匿名化 数据擦除 物理销毁 删除销毁验证	数据销毁工具 数据脱敏系统
通用安全要求		数据资产梳理与分类分级	数据资产梳理及分类分级工具
		身份认证	统一身份认证系统
		访问控制	
		密码基础设施	密码基础设施平台
		数据安全审计	数据库审计系统
		数据接口安全	API 监测
安全运营要求		数据安全一体化综合监测	数据安全监测平台
		数据安全策略运营	数据安全运营平台
		数据资产运营	
		数据安全风险运营	
		数据安全事件运营	
		检查评估	数据安全评估系统

具体的技术工具功能及应用场景简介如下：

4.2.1.1. 全生命周期安全防护类

（1）数据安全采集工具

数据安全采集工具能够实现对各类终端数据采集设备的接入和数据收集的监控和管理，实现对数据采集设备进行发现和识别、指纹管理、准入与访问控制、网络接入异常监控、数据采集合规分析、流量行文监控、信令白名单检查等功能。

数据安全采集工具可应用在各数据采集处理活动中。如在互联网个人数据采集方面，数据安全采集工具能够收集数据采集流量，分析互联网用户个人数据采集是否满足合法、合规要求，并对数据采集的终端进行身份认证，数据加密传输、过度采集监测等进行管控。

（详细介绍参见附录 B.1.1）

（2）数据防泄露系统（DLP）

数据防泄露（DLP，Data Leakage Prevention）系统又称为数据防泄露系统，或 DLP 系统。DLP 系统采用内容分析引擎，利用关键字、正则表达式、文件指纹、自然语言处理等数据识别技术，对使用和外发的文件进行解析与扫描，实时识别、监控、保护组织的敏感数据；对即将发生、正在发生的泄露敏感数据行为，按照预置策略及时阻断并告警，监视和保护静止、移动和使用中的数据并防止敏感数据传输到外部，有效避免数据泄露带来的安全风险，最终实现对敏感文件全生命周期的可知、可见、可控的一体化解决方案。

大部分 DLP 系统中的各项功能都采用了统一的内容识别技术引擎，根据不同的防护场景、不同的通道监测与管控技术划分为以下四类：

终端 DLP：对终端和外设中的敏感文件的内容识别与安全管控。

网络 DLP：对通过网络出口的外发敏感文件进行内容识别和安全管控。

邮件 DLP：对通过邮件系统传输的敏感文件进行专门的内容识别与安全管控。

存储 DLP：对存储在主机端存储设备的敏感文件进行内容识别和安全管控。

（详细介绍参见附录 B.1.2）

（3）数据库加密系统

数据库加密系统采用透明加解密、列加密等技术方式，实现对数据库中存储的明文数据进行加密存储、访问权限控制等功能。即使有人想对此类数据文件进行反向解析，所得到的也不过是没有任何可读性的“乱码”，有效避免了因数据库明文存储数据，被拖库而造成数据泄露的问题，从根本上保证数据的安全。

数据库加密系统可以应用在数据存储处理活动中。例如，组织的数据高度集中在数据中心，通过对数据库进行加密，能够有效的防止外部非法入侵窃取敏感数据、防止内部高权限用户窃取敏感数据、防止合法用户违规访问敏感数据等由数据明文存储引发的安全风险。

（详细介绍参见附录 B.1.3）

（4）数据备份 / 恢复工具

数据备份保护是保证数据安全的重要手段，通过备份与恢复有效规避数据丢失或者被窃取的影

响。数据备份包括应急容灾、副本管理、数据归档等内容。灾备架构既要能够解决复杂环境带来的脆弱性问题，同时具备多种灾备技术的统一管理，满足动态、敏捷和全面的要求。

灾备平台主要用于多种架构下的数据备份和恢复，包括本异地灾备场景、云上数据保护场景、云容灾场景、海量文件备份场景、防勒索病毒场景。

（详细介绍参见附录 B.1.4）

（5）统一身份认证系统（IAM）

统一身份认证系统是一套全面地建立和维护数字身份，并提供有效地、安全地进行 IT 资源访问的业务流程和管理手段，从而实现组织信息资产统一的身份认证、授权、访问控制和身份数据集中管理与审计。

统一身份认证系统建设的核心意义在于帮助组织进行应用系统的统一管理，从而提高数据资产的可管理性，也为组织实施进一步的安全保护措施提供支撑。

（详细介绍参见附录 B.1.5）

（6）数据零信任平台

零信任并非“没有信任”，而是“不再简单根据网络位置就判断对资源的访问权限”，而是“对何种网络位置，均从零开始依靠鉴别与验证建立信任”，从而实现纵深防护。保护数据是零信任策略的核心目标，其要求所有用户，无论位于网络内部还是外部，都需要经过身份验证、授权和持续验证，然后才能访问应用程序和数据，即以动态方式围绕每个连接进行防御，根据风险状态调整访问权限和其他特权。整个数据零信任平台一般由零信任客户端、零信任控制中心和零信任分析中心构成。

数据零信任平台能够应对因传统网络安全防护缺乏内部流量的检查、主机部署缺乏物理和逻辑上的灵活性、存在单点故障而带来的风险和威胁，因而能够有利于解决位于网络防护边界之外的远程用户和移动设备的安全接入问题，云上数据资产的安全认证与访问问题。

（详细介绍参见附录 B.1.6）

（7）数据库运维安全系统

数据库运维安全系统能够将数据库人员身份鉴别、安全策略、访问控制、审批流程管理等有效结合，解决运维账号共享与运维环境共享带来的运维身份不清问题，并且通过精准的 SQL 语句解析技术，建立细粒度的访问操作管控机制，实现对于违反安全策略的风险操作进行拦截、阻断。

数据库运维安全系统可以应用在数据使用处理活动中。例如，组织中存在大量的第三方运维、开发商驻场等人员，这些人员一般情况下具有高权限账户，一旦发生高危操作或越权访问，极易造成数据永久丢失、业务中断以及数据泄露等风险，通过部署数据库运维安全系统，可以实现拦截高危操作、防止账户越权访问数据等功能；另一方面，组织的数据库运维关系复杂，存在同一运维人员管理多个账户、多人共享账户等情况，无法针对人员进行最小全向控制并且一旦发生数据安全风险事件，无法有效定位责任人员，数据库运维安全系统能够通过多维身份认证和登录规则验证的双因素机制有效授鉴别运维人员身份，实现授权到人、审计到人、责任到人的溯源机制。

（详细介绍参见附录 B.1.7）

（8）数据库防火墙系统

数据库防火墙系统是基于数据库协议分析与控制技术的增强级数据库安全防护系统，能够主动、实时、全方位地保障数据库安全，使数据免受数据库漏洞、高危恶意操作及敏感数据泄露的威胁。面对来自外部的入侵行为，提供防 SQL 注入和数据库虚拟补丁技术。通过虚拟补丁，使数据库系统不依赖升级、打补丁，即可完成对主要漏洞的防护。

数据库防火墙系统可以应用在数据使用处理活动中。例如，大小写编码绕过、断包绕过、缓冲区溢出、协议不兼容、参数污染绕过、等价替换绕过等 SQL 注入攻击方式能够穿透传统网络边界防护产品、Web 应用程序输入校验、应用服务器的三层防护，造成刷库、拖库、撞库等数据库安全风险，通过部署数据库防火墙系统，能够基于精准的数据库协议解析技术和控制策略，有效防止 SQL 注入、XSS 攻击等攻击方式；另一方面，在面临端口扫描工具、协议扫描工具、漏洞扫描工具等黑客攻击前的暴露面探测时，能够通过数据库防火墙系统的防端口扫描、防协议扫描等功能，拦截具有端口扫描特征的 TCP/UDP 包、并对协议探测包的特征进行匹配，拦截具有协议探测包。

（详细介绍参见附录 B.1.8）

（9）数据脱敏系统

数据脱敏系统是面向敏感数据进行数据自动发现，按需对敏感数据采取泛化、随机化、抑制、扰乱、加密等一系列技术对源数据进行处理以屏蔽敏感数据，并最大程度保证脱敏后数据的一致性和业务的关联性，满足数据分析、测试开发、数据共享等场景下的数据安全性。数据脱敏系统根据数据脱敏的实时性和应用场景的不同，分为动态脱敏和静态脱敏。

数据脱敏系统可以应用在数据使用、数据共享 / 公开处理等多个活动中。例如，组织在数据开发测试时，需要使用业务环境中的真实数据进行测试，可以通过数据脱敏系统（静态）采用替换、变形等技术，对源数据中的敏感部分采用相同含义的数据进行替换，如身份证号码脱敏后仍然为有效的身份证信息；在组织进行数据分析时，需要保留数据之间的关联性和分析结果的准确性，可以通过数据脱敏系统（静态）采用抑制、泛化等技术，在脱敏后仍保留原有的数据关系与格式，确保数据脱敏后不会影响分析结果，如多个表格内相同人员的基本信息，脱敏后保持结果一致；另一方面，组织的运维人员、应用侧用户访问敏感数据时，可以通过数据脱敏系统（动态）采用替换、变形等技术，对源数据中的敏感部分采用相同含义的数据进行替换，如手机号脱敏后认为正常的手机联系方式。

数据安全技术发展始终处于对抗与反对抗的博弈中，经过脱敏的数据集仍可能受到隐私攻击的风险，攻击者可通过背景知识、网络公开的身份信息以及黑灰产等渠道获得具备关联信息的数据集，可从脱敏数据集中恢复出真实信息，通常这种攻击被统称为“重标识攻击”，近年来，反“重标识攻击”的防护技术也在不断发展，如通过“K- 匿名技术”有效防止数据链接攻击，通过“差分隐私技术”，防止集中数据的差分攻击。

（详细介绍参见附录 B.1.9）

（10）数据安全协同平台

目前不管是多方安全计算还是联邦学习技术，都只能解决单一的隐私计算，无法满足数据充分安全流通、释放数据价值的诉求。数据安全协同平台是将数据安全协同理念与各种隐私计算技术手段相融合，基于数据分类分级构建具备安全、合规及生态能力的数据共享、研究、利用与交易的平台。

整体平台由数据集市、数据安全发布体系与运算资源整合管理与任务调度体系构成，由发布者（数据持有方）在数据集市中通过发布者系统节点发布数据主题服务、参与数据协同任务，由订阅者（数据需求方）在数据集市中通过订阅者系统节点实现数据订阅与发起数据协同任务申请，由协同计算节点根据协同任务需求运用多方安全计算、联邦学习、隐私求交、匿踪查询、数据脱敏等技术实现数据安全共享与交易计算。并通过运算资源整合管理与任务调度体系实现对集市中各方成员的统一管理，计算资源的集中分配，数据共享的集中管控，从而最终达到“数据不出域、可算不可见”的安全共享与交易。

数据安全协同平台可以应用在数据的协同加工与数据价值共享等数据处理场景中。例如，政务数据共享场景下，通过协同平台打通政企之间的业务屏障，实现数据共享的统一管理审批，明文数据不出所在单位，全程加密传输、缓存和运算等效果，在数据共享过程中保护数据的安全和隐私，从而推进政务与金融、医疗、互联网等机构在联合风控、联合营销、联合分析等场景的安全应用，促进数据价值的极大释放。

（详细介绍参见附录 B.1.10）

（11）机密计算平台

机密计算是指在可信硬件支持下的隔离环境中运行安全计算任务，从而对安全计算任务的代码和数据进行保护。机密计算的保护可以让代码和数据免于特权软件（如操作系统、云虚拟机监控器 Hypervisor）的监视和修改。机密计算通过使用基于硬件的内存保护来改进敏感数据的隔离，能够使被加密的数据在内存中得到处理，降低数据暴露给系统其他部分的风险，从而降低敏感数据泄露的可能性，同时还能为用户提供更高程度的控制和透明使用。

通常，数据保护涉及三个方面：存储与备份时的数据安全保护主要通过加密实现；传输过程中的数据安全保护主要通过 TLS 和 HTTPS 等安全协议实现；使用时的数据安全保护需要对使用中的数据进行机密性和完整性保护。随着云计算、大数据等新型应用场景的发展，对使用中的数据进行保护已经成为一种趋势，机密计算技术重点解决的问题便是对使用时的数据进行安全保护。机密计算可以解决诸多应用场景中“信任”难题，比如多个不互信单位之间的数据融合与联合分析、区块链上的智能合约的机密性保护、公有云平台对外部或内部攻击的防御、高敏感信息（比如密码学材料、医疗档案等）的安全保护等。

（详细介绍参见附录 B.1.11）

（12）数据水印工具

数据水印工具通过对源数据中嵌入伪行、伪列等水印标记的技术方式，从而在数据进行分发后，能够实现对外发数据进行泄露溯源的功能。数据水印工具能够对外发数据行为流程化管理，具备事前数据发现梳理、申请审批、事中添加数据标记、自动生成水印、事后文件加密、外发行为审计、数据源追溯等功能，避免了因内部人员外发数据导致的数据泄露，无法对事件进行追溯，提高了数据传递的安全性和可追溯能力。

数据水印工具应用在数据共享 / 公开处理活动中。例如，组织内部需要将数据共享至其他部门或第三方公司 / 个人，可以通过数据水印工具在源数据中添加伪行、伪列的数据水印，一旦发现数据流传至互联网或其他环境中，可以根据水印信息快速溯源数据泄露源头，能够有效防止数据泄露的风险，

提高数据共享的安全性和可追溯能力；在需要进行数据实时交换应用场景中，可以通过 API 接口的方式调用数据水印工具向特定平台或系统提供数据时，嵌入水印，以保证数据的可追溯性。

（详细介绍参见附录 B.1.12）

（13）数据销毁工具

数据销毁工具是指采用各种技术手段将计算机存储设备中的数据予以彻底删除，避免非授权用户利用残留数据恢复原始数据信息，以达到保护关键数据的目的。数据销毁是数据处理全过程的最后一步，主要目的是将计算机或设备在弃置、转售或捐赠前彻底清除所存储的数据，并且无法复原，以免造成信息泄露，保障数据机密性。数据销毁主要分为数据介质物理销毁和逻辑销毁两种。

这种技术主要应用于重要或敏感以上数据的销毁处理。一般涉及商业秘密和大量个人信息的数据在使用完毕后，也应当进行销毁处理。

（详细介绍参见附录 B.1.13）

4.2.1.2. 通用安全防护类

（14）数据资产梳理及分类分级工具

数据资产梳理及分类分级工具通过协议解析、流量分析、敏感数据识别等技术，能够对目标环境中的数据资产进行全面清查、摸排，了解数据资产类型、数据资产分布、数据资产权限、数据资产使用等信息，形成数据资产清单、敏感数据清单。数据资产梳理及分类分级工具通过数据图谱、字段名分析 / 字段描述分析、表和字段自动关联统计、主从表智能关联、智能化行业数据分类分级知识库等核心能力，能够准确识别数据库中的表 / 字段的业务含义并与行业数据分类分级标准模板智能建立绑定关系，帮助组织实现智能、快速、便捷的数据分类分级工作。

数据资产梳理及分类分级工具是实现数据安全分类分级保护的核心基础能力。组织需要对数据进行分类分级管理，明确数据的类别和级别，能够进一步明确数据保护对象，有助于分配数据保护资源和成本，是建立完善的数据生命周期保护框架的基础，也是有的放矢地实施数据安全管理的前提条件。

（详细介绍参见附录 B.2.1）

（15）密码基础设施平台

密码基础设施平台通过数字证书作为载体，通过设施、技术、人员、策略、制度、审计的共同作用，实现对网络空间中各类实体的身份和密码机制进行管理，从而为数据安全提供身份的信任机制和数据的加密保护机制，为数据的加密保护提供支撑。

密码基础设施平台具备通用性，能够广泛地为各类业务系统提供数据安全防护。PKI 的基于第三方权威的第三方认证，能够保证各类业务活动中交互双方的身份真实性；PKI 的数字证书和电子签名，能够保证数据的完整性，保证数据不被篡改；PKI 的密钥管理，能够保证数据传递和流通过程在不被恶意窃取。

（详细介绍参见附录 B.2.2）

（16）数据库审计系统

数据库审计系统能对旁路镜像流量、虚拟化引流、远程登录、本地流量等多种访问操作数据库

方式进行全面审计监测，通过数据库议解析和深度 SQL 解析技术，实时感知数据库风险，并通过数据库行为建模，基于建模语句的波动情况，实现对数据库访问操作行为进行有效的分析和深入挖掘。

数据库审计系统具备通用性，可以帮助组织满足政策合规需求，完善数据安全体系，实现运维侧和应用侧对数据库访问操作全面监测审计，实时告警风险行为，并能够从行为、风险、语句、会话等多维度关联分析挖掘，对数据安全事件精准溯源及定责。

（详细介绍参见附录 B.2.3）

（17）API 监测系统

API 监测系统通过网络流量通讯协议分析和解析、流式计算引擎及高速匹配引擎等核心技术，能够实现应用接口自动发现、涉敏接口自动发现、敏感数据自动发现、接口弱点自动发现等功能，并能够实时监测敏感数据行为、追踪溯源风险事件，帮助组织快速梳理业务应用及接口资产，全面掌握敏感数据访问全貌，及时防控敏感数据行为风险，并通过与数据库审计等系统的配合，能够针对数据泄露事件进行有效溯源。

随着云计算、移动互联网的蓬勃发展，越来越多的应用开发深度依赖于 API 之间的相互调用，API 接口数量飞速增加。API 监测系统能够识别和梳理环境复杂的不同时期、不同业务的众多 Web 应用及 API 接口，帮助组织了解自身应用资产情况；并能够针对互联网用户的应用访问、内部用户的应用访问以及针对敏感数据共享与跨境等场景，发现 API 接口脆弱性，感知 API 接口风险，识别敏感数据访问流向，减少因 API 接口脆弱性等问题引起的数据泄露。

（详细介绍参见附录 B.2.4）

4.2.1.3. 安全运营平台类

（18）数据安全监测平台

数据安全监测平台是基于数据分析、用户行为分析、可视化分析等技术，从流量、日志等多个维度采集抽取数据，进行关联、分析，构建纵向贯通、横向融通的数据安全监测体系；及时发现、纳管数据库资产和应用资产，识别数据库和业务系统的脆弱性，绘制用户－终端－应用－接口－数据访问的全链路数据流转视图，进一步，基于敏感数据的流转情况，分析攻击特征，建立攻击者身份画像，研判分析安全风险并进行违规告警，同时对风险事件进行数据安全影响分析和追踪溯源，形成数据安全风险趋势预测。

数据安全监测平台的应用场景主要分为三种典型场景，第一种是监管机构对所管辖的单位进行数据安全监管，第二种是集团公司对下属各不同分、子公司开展数据安全监管，第三种是组织对本单位的数据安全整体态势进行监测，通过数据安全监测平台，低侵入性持续监测敏感数据流转情况，实时发现数据安全风险，并及时对安全事件进行预警与追踪溯源。

（详细介绍参见附录 B.3.1）

（19）数据安全运营平台

目前数据安全防护手段大多通过提供单一化的功能解决某个方面的问题和需求，这让不同数据安全产品之间的数据“孤岛”现象凸显，继而影响到数据安全建设在落地执行过程中的效率、质量乃至成本投入等诸多层面。

数据安全运营平台作为安全大脑，将管理体系、技术体系和运营体系有机融合，并把分散的数据安全产品能力进行整合，构成“平台化、体系化、可视化、实用化”的一套整体解决方案，帮助组织构建覆盖全生命周期、全领域的数据安全防控能力，形成对数据资产全链条防护；最终实现常态化、高效的数据安全资产运营、数据安全策略运营、数据安全风险运营、数据安全事件运营机制，不断提升安全运营团队能力。同时通过智能化手段，辅助安全运营人员，提升安全事件的分析和处置能力，从而不断丰富和提升数据安全建设的完整性与成熟度，帮助组织满足监管要求，杜绝敏感数据泄露等安全隐患。

数据安全运营平台通过对各数据安全设备 / 系统产生及上报的流量日志、事件日志及安全实事件等各类日志进行集中化大数据采集、汇聚、存储与归一化解析处理，形成标准化的统一数据格式，以作为支撑数据资产运营、数据安全策略运营、数据安全事件运营、数据安全风险运营的应用、分析、与可视化呈现的数据基础。通过用户实体分析技术（UEBA）实现将安全大脑的安全策略发布到各数据安全设备上，并关联端点、网络和应用的自动学习，构建组织的动态数据安全基线，实时监测数据在全生命周期的各处理活动中的安全风险；通过响应与处置自动化技术（SOAR），联动各数据安全防护产品能力，实现数据安全事件响应和处置，可以协同化、流程化的对一系列安全事件进行告警响应和处置；通过数据血缘技术，对数据安全风险进行详尽的追踪溯源。

（详细介绍参见附录 B.3.2）

（20）数据安全评估系统

面对数据安全多法并轨，技术标准并行的情况，目前组织在按合规要求开展数据安全评估工作时，面临评估工作内容繁多、交付周期长，评估服务从业人员门槛较高，评估项目经验难以沉淀实际痛点，数据安全评估系统基于风险评估开展特性，梳理标准评估实施作业流程，实现评估过程一体化线上统一管理。通过充分自定义的评估调研模板、全面覆盖的评估知识库，结合自动化的技术检测技术工具，智能辅助输出评估报告，以实现易管控、更快捷、可沉淀的标准化评估服务工具，降低数据安全评估服务资源投入，提高数据安全评估的效率与准确性。

数据安全评估系统能够面向数据出境、个人信息保护、数据安全能力成熟度以及安全技术措施专项等多样化场景，以及围绕金融、政务、医疗、企业等不同行业的合规性要求，基于底层的评估知识支撑体系，有效支撑统一化、标准化的自评估及第三方数据安全评估工作的落地，以更好的发挥评估人员的能效，准确高效的评估组织的数据安全管理差距并给出可行的整改建议。

数据安全评估涉及的自动化检测手段目前还仅限于数据库漏扫、API 接口扫描、数据调用链扫描等有限范畴，围绕数据处理活动全面的管理制度、技术措施及安全运营整体评估，仍需持续研究创新自然语言处理、密码算法检测、异常行为识别等人工智能技术在安全评估中的应用，以提高自动化评估检测水平。

（详细介绍参见附录 B.3.3）

4.2.2. 技术工具落地部署示意

上述各个数据安全技术工具需要部署并运行到组织的实际网络环境中，才能全面、综合的落地

整体数据安全保障。本白皮书力图基于较为普适化的网络逻辑拓扑，围绕涉及的互联网环境、办公环境、生产环境、开发测试环境等数据安全域，面向终端、网络、应用及数据存储部署相对应的安全技术工具，构建覆盖数据全生命周期流转场景的纵深防御体系，结合配套的管理策略与运营机制，有效防止外部攻击与内部泄露、滥用，保障数据安全有序流动，以给组织开展数据安全建设带来参考和指引。典型部署示意如下图 4-2 所示：

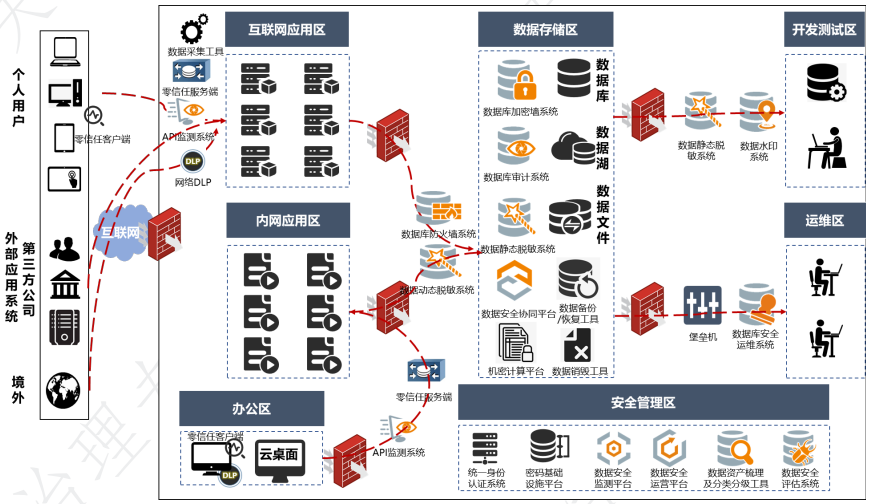


图 4-2　数据安全技术工具部署示意图

4.2.3. 技术发展趋势分析

随着信息技术的发展，支撑上述数据安全工具落地防护的安全技术也在不断创新，其演进趋势主要体现在技术能力供给全面化、技术应用模式多样化、多技术融合支撑体系化等方面，具体归纳总结为：

（1）基于 AI 的数据识别技术成为数据安全治理和安全防护的起点

对业务流中各阶段的数据进行识别，进而对各类不同数据的重要性、潜在风险进行分类分级，是数据安全治理和安全防护的依据。随着人工智能技术的发展，基于机器学习，能够大幅度提升数据识别的效率和准确性、全面性。典型的技术包括自然语言处理（NLP）、用户异常行为分析（UEBA）、知识图谱（KG）等。而对数据识别和分析的过程，也可以根据需要灵活部署在业务数据来的各个环节，例如基于前台流量的数据识别、基于数据库的数据识别等等。

（2）基于密码的数据主动防护技术成为数据安全治理的有力武器

密码技术一直是数据安全防护的重要手段，用来保证数据的完整性、机密性和可用性。随着互联网和密码学的发展，人们越来越多的在数据的采集、存储、传输、使用等生命周期活动中主动使用数据加密、数字签名等机制以及各类密码协议进行安全防护；同时，密码技术在数据安全领域的大量使用，也积极地推进了密码供给模式、密码应用模式和管理模式不断推陈出新，更加适应信息技术发展的需要。

（3）隐私计算技术成为保护数据跨域流通、安全开发利用的热点

数据只有充分流通、充分开发利用才能真正发挥数据的“生产要素”作用，创造更大的价值。

而数据的流通和开发利用就涉及到数据权益的确认、隐私和敏感数据的保护，这就需要隐私计算技术的支撑。隐私计算能够保证数据在隐私不泄露的前提下得到处理，例如对银行、社保、公安等数据融合分析以提升银行的风控水平。当前国内很多的研究机构、互联网厂商、金融机构都投入大量的资源进行隐私计算相关研究。从技术上看，隐私计算通常包括机密计算、安全多方计算、同态加密等技术路线，其中各种技术路线又有不同的适用场景。

（4）多技术协同配合提升数据安全治理和防护的有效性成为主流

从数据安全治理和数据安全防护的发展看，数据安全治理随着数据价值的不断提升和业务的多样化走向多层次、多维度的治理，而数据安全防护则随着信息技术发展增加数据安全防御纵深。这就需要多种数据安全相关技术协同配合，共同为数据安全治理和安全防护提供支撑。例如基于网络边界防护的网络安全技术、应用按需加密技术、数据库加密、磁盘加密、访问控制等技术或产品，在防止数据泄露的安全目标下，就需要发挥各自的安全能力统一规划实施。一种典型的思路是集中的策略管控系统作为“大脑”，而各类的设备、组件作为“执行引擎”执行策略，对数据进行保护。

（5）自动化评估成为数据安全治理以及数据安全防护的重要抓手

鉴于数据安全的重要性，国家层面和组织层面都非常重视数据安全评估，根据合规要求，需要定期（如一般每年）或针对重要数据处理活动场景（如委托加工，跨境等），需要对数据安全治理的有效性和数据安全防护的有效性进行合规性评估，才能确认数据安全治理和安全防护是能够达到预期要求，及时发现差距落实整改。但当前的评估手段主要依赖调研访谈、文档查验、旁站检测等人工手段，自动化评估水平相对较低，需要进一步创新发展自动化评估检测技术，推动数据安全合规评估的高效性、客观性和准确性。

第五章　未来展望与倡议

5.1. 未来展望

5.1.1. 治理能力创新

5.1.1.1. 以新技术防范和化解新业态的风险

移动通信、人工智能与量子计算等新技术发展不断推动社会发展进程的同时，相关创新技术应用带动海量数据流动，在数据处理过程引发的安全影响也愈发严峻。

随着 5G 通信技术的应用以及 6G 的研究，配合云计算、边缘计算、大数据等技术端融合发展，企业的数字化转型加速和普及，越来越多的设备和工具都具备了数据感知能力，企业可以通过互联网和物联网的技术手段，来获取来自在线或离线的数据，使得企业内部产生更多的数据。同时以字节跳动为代表的在线直播等社交媒体也成了企业获取消费者反馈和意见的重要途径，这些数据可以帮助企业更好地了解自己的受众和客户，进而改善产品和服务，提高客户满意度。各类海量数据呈现出主体多样化、处理活动丰富化、存储和应用环节离散化的特点未来将更加明显，数据安全风险随之也呈更加复杂化态势，给数据安全治理带来更大的挑战。

ChatGPT 的横空出世让大家对 AIGC（人工智能生成内容）技术有了更深的认识。人工智能技术自诞生起，就与数据相辅相成，ChatGPT 的成功，离不开大数据的帮助。ChatGPT 模型使用从各种来源收集的大型对话数据集进行训练，包括社交媒体、公共论坛以及其他我们暂未得知的渠道。庞大的数据训练，才使得 ChatGPT 具有我们今天看到的优秀性能。但这也意味着，模型实际上在不断地接触各种对话，其中可能包含相关的敏感信息。此类技术的应用和升级都可能伴随着新的对话和新的隐私泄露风险，如 ChatGPT 在 2023 年 3 月份暴露出用户对话数据和付款服务支付信息丢失，而三星员工直接将企业机密信息以提问的方式输入到 ChatGPT 中，导致三星半导体机密数据外泄。

量子技术的持续发展，量子计算机能够比传统计算机更快地处理信息，这可能彻底颠覆和完全破解现代信息和通信基础设施所依赖的数字加密系统，使得身份验证的安全与通信隐私在量子计算面前毫无安全保障，基于公钥加密的全球现存通信系统、安全设备等或都将面临巨大安全风险。除了实时攻击外，大量历史存量数据，通过量子计算技术也可以轻易获取仍处于敏感保护阶段的数据。

基于上述移动互联、人工智能、量子计算等新技术的不断发展，推动数据应用场景不断丰富化、多样化，促进数据要素价值高速释放，但同时带来的数据安全威胁也在持续加剧，对数据安全治理协同能力的创新需求也日益迫切，如从立法和政策引导角度，建立、健全面向人工智能算法安全、后量子加密防护、移动通信安全的管理要求与监管措施，从防护技术角度，深入研究与实践抗量子密码技术、人工智能算法监测技术、轻量级加密通信协议、区块链及隐私计算技术等安全技术创新，“魔高一尺，道高一丈”，通过对抗与反对抗的博弈，持续促进数据开发利用与安全防护的平衡发展。

5.1.1.2. 数据安全治理能力左移成为趋势

目前现有的数据安全工具一般多采用外挂模式，在事中和事后对数据威胁和泄露事件进行检测和防护，伴随数据的广泛流动，资产爆炸、边界模糊导致的安全暴露面过多，企业采用“被动合规”的模式已无法应对愈发严重的安全威胁。伴随法律法规的持续健全与数据安全风险的日益复杂，在合规和风险双重驱动下，企业的数据安全治理思路也在发生质的变化，将由“被动合规”转换为“主动治理”。需要在数据安全的风险源头进行及时管控与处置，基于数据全生命周期，对数据流动的轨迹、状态的变化进行记录，并依据数据本身的风险变化而做出细粒度的、动态的控制，构建一体化的数据安全治理体系。

基于以上的数据安全动态防护策略的需求，这就要求组织必须把数据安全能力从运维环节前置、左移到设计、编码阶段，将安全措施融入应用系统建设，遵循“三同步”原则，同步规划、同步建设、同步使用，由外挂安全转向内生安全架构。数据安全左移已成为数据安全未来演进中的一个核心方向，基于数据生命周期及内生安全架构开展数据安全治理，更早地识别并标记数据资产，界定数据权责，并在数据处理的第一现场持续对敏感数据处理和使用的过程进行追踪，横贯数据处理流转的整个环节，发掘数据风险的真正源头，及时施加细粒度的、动态的控制。同时，持续开展数据安全风险评估，更多地依托工具及产品为主导，利用自动化的方式进行风险评估，提高业务落地过程中的可执行性，并根据评估结果进行修正和升级。组织通过将数据安全能力左移，以更好的促进数据安全有序的使用、流通与交易。

5.1.2. 治理体系和制度健全

5.1.2.1. 数据安全治理框架升级保障数据流转安全

随着科技的不断发展，越来越多的数据被创造出来，并且需要在不同的场景下流转和共享，所以数据流转的场景的日趋丰富是一个不可避免的趋势。从个人信息来看，数据流转的丰富也为个人提供了更多的便利和可能性。例如，个人可以通过社交媒体平台与朋友分享自己的生活照片和视频，或者通过在线商店购买商品并享受更好的服务。从组织的角度来看，数据流转的丰富将带来更多的机遇和挑战。一方面，可以通过更好地管理和利用数据来提高生产效率、优化产品设计和提供更好的客户服务，从而提高市场竞争力；另一方面，数据生产要素化后，组织的相关数据在做好数据的安全基础上，通过交易或与其他企业进行数据共享和协作，也可以进一步提高收益。

随着新技术发展，未来元宇宙、自动驾驶、全息通信、智慧家居、远程医疗、数字孪生的智慧城市等场景将从实现 0 到 1 的突破，逐步落实为 1 到 N 的复制拓展，会进一步促进数据流转的场景更加丰富。在享受数据合作共享、流通、交易、跨境流转等场景带来的便利和好处的同时，我们应该认识到随着业务和数据处理活动的复杂化，不同应用间共享和共同处理数据，数据处理活动中存在模糊的边界，导致侵犯用户个人信息权益的事件屡屡发生。海量收集用户个人信息和记录用户行为，数据汇聚关联分析、智能化应用产生的影响，可能超出了单独企业主体能够承担风险的范围。随着 5G 和物联网的应用，以及新冠疫情大流行引发的数字化加速，急需一个连贯的、基础的数据安全治理框架来应对数据安全和隐私保护问题，确保数据流转的合法性和可靠性。

5.1.2.2. 法律法规标准趋于持续完善

近年来，以“三法三条例”为基础的数据安全相关的法律法规、政策、标准等频繁出台。金融、医疗、工业等不同行业领域以及多省市已经发布数据安全相关的条例和制度，这些已颁布、修订的法律，发布、实施的政策、标准等，一方面为组织开展数据安全治理工作，提升对重要数据和个人信息的保护能力提供了良好的指导参考依据；另一方面，也提出了合规的硬性要求。数据安全治理是个系统性工程，需要国家立法部门、政策制定部门、监管部门引导和组织数据处理相关单位相互协作，合力应对数字经济时代的数据安全风险和挑战，共同推动我国尽快建立、完善数据安全治理相关法律法规和标准体系，保障数字经济健康有序发展。

2023 年 1 月，工业和信息化部、国家网信办、发展改革委等十六部门发布《关于促进数据安全产业发展的指导意见》明确提出高质高效推进贯标工作，加大标准应用推广力度。积极参与数据安全国际标准组织活动，推动国内国际协同发展，以保证在数据安全关键治理环节、关键业务场景、特定行业要求方面进一步细化，明确数据安全治理各个活动指南以及数据安全评估方法和指标。标准和指南作为法律法规和政策落地实践的重要桥梁，可有效解决前述法律、法规的基本概念厘清、配套制度建立以及相关举措细则确定等问题。同时，目前全国多个省市都已经建立了数据交易市场，并出台了相关的数据安全管理条例、办法等，为数据的确权和合法流转建立了宏观规划，后期需要在实践中不断摸索不同地域、不同行业的数据确权的具体实施细则，并通过试点探索，不断调整和优化市场规则，以逐步建立一个健康、透明、公正的数据交易环境。

综上所述，可以预期未来在法律法规和标准体系建设会日趋完善，“数据”、“个人信息”、“网络数据”等基本概念将会日渐清晰。各部法律所涵盖的范围中出现重叠的部分，会在具体落地的管理办法中逐步明确何种场景下进行数据处理活动时的具体落地方案，数据所有权和数据加工新成果的责权界定等问题会逐步解决。

5.1.3. 治理全球化

5.1.3.1. 全球数据的流转与割裂并存

快速数字化正在影响生活的方方面面，包括人们互动、工作、购物和接受服务的方式，以及价值创造和交换的方式。作为数字经济驱动的产物，跨境数据流动正受到越来越多国家的重视，然而全球跨境数据流动的治理规则却变得日益复杂。跨境数据流动从过去关注技术问题和个人隐私保护问题，逐渐演变为一个包括国家安全、数据主权、经济要素等综合性议题，与此相关的政策制度建设也已成为各国间战略博弈的焦点。

从短周期来看，不同国家基于自身利益的诉求，纷纷通过加强数据管控来捍卫数字主权，突出网络与数据基础设施的自主性。以欧盟和美国为例，欧盟表现为对内部数据流动的支持，但对于数据跨境向境外传输，欧盟则有着严格的管控，设置了多条国际数据跨境传输与流动的条件和规范，并引入跨境数据流动认证新机制；而美国拥有全球范围内最多的互联网巨头，则希望能够无障碍地获得其他国家的数据，并且希望将本国法律的管辖权延伸至境外存储的数据。因此，全球数据安全的长臂管辖以及数据流动“朋友圈”扩充的相关治理规则体系高频更新，对企业全球业务发展带来

诸多挑战风险，跨境数据流动当中潜在的制度差异为跨国商业运营和数据资源开发利用带来了障碍，也决定了未来短时间内围绕数据跨境流动制度所产生的冲突难以避免。因此，各型组织应持续跟进欧美为代表的全球数据管理规则体系的最新动态，提前筹划，做好风险防范应对策略。

从更长的周期来看，世界范围内不同的数据治理模式的分化会威胁全球数字信息流动，导致跨国企业综合利用全球数据的成本和难度在不断提升，阻碍数字经济全球化。但是，全球数据的安全治理将有助于实现全球数据共享，开发有助于应对贫困、健康、饥饿和气候变化等重大全球发展挑战的公共产品，促进世界经济的复苏。因此，未来结合双边和多边机制、灵活对接跨境数据流动规则的全球数据安全治理模式必然出现，以实现积极应对新技术所带来的各种挑战，平衡经济自由与数据安全的关系。

5.2. 持续加强数据安全治理能力的倡议

5.2.1. 面向国家角度的倡议

5.2.1.1. 构建有中国特色的数据安全治理技术发展路径

开展数据安全治理必须立足我国信息环境的基本现状和未来的发展趋势，选准突破口，遵循国家的政策导向，坚持产业化推进，构建具有中国特色的自主可控技术发展路线。自主可控的数据安全技术的发展要以产业化为基础，结合信息化相关基础软硬件产品的研发、规模应用、服务保障体系等方面加强互动，推动数据安全相关产业协同快速发展，实现数据安全产业链上下游的有效结合。通过推进产业化成熟发展，广泛开展合作，认真分析用户需求，提供优质服务，真正使自主数据安全产品与技术在我国信息化和数据领域得到广泛应用。

希望通过政策的引导和技术的持续积累和发展，从企业、行业的不同视角，吸收国内外的成果经验，不断明确政府、企业、个人等不同角色的义务和权利，并在实践过程中，持续结合中国国情和技术发展路线趋势，以形成中国特色的数据安全治理技术发展路径。

5.2.1.2. 充分重视人工智能的应用和对抗

人工智能技术的发展，有效提升了数据收集管理能力和数据价值挖掘利用水平。在互相协同发展中，数据安全是人工智能安全的关键，数据质量和安全直接影响人工智能系统算法模型的准确性，进而威胁人工智能应用安全。但随着 ChatGPT 等更高水平的人工智能产品的发布，应充分认识到在人工智能应用中的数据安全问题。一是隐私泄露，人工智能技术需要大量的数据作为训练材料，如果这些数据被未经授权的人员访问，就可能导致个人隐私泄露，二是数据失控、偏见和歧视，由于数据的来源和处理方法可能存在偏见和歧视，人工智能技术的结果也可能存在偏见和歧视，这种情况可能会导致对某些人群的不公正对待或者歧视。近期 open AI 团队提出了广泛受益、长期安全、技术领导力和合作导向，四项关于今后人工智能发展的一些原则。同时，特斯拉 CEO 埃隆·马斯克率数百位科技行业高管在一封公开信中呼吁，所有人工智能实验室应立即暂停比 GPT-4 更强大的人工智能系统训练，以避免出现人类竞争性的人工智能系统会给社会和文明造成的潜在风险。

针对 ChatGPT 等生成式人工智能产品可能引发的风险，2023 年 4 月 11 日，国家网信办颁布《生成式人工智能服务管理办法（征求意见稿）》，对用于生成式人工智能产品的预训练、优化训练数据也进行了明确要求：一是要符合《网络安全法》《数据安全法》等法律法规的要求；二是不含有侵犯知识产权的内容；三是数据包含个人信息的，应当征得个人信息主体同意或者符合法律、行政法规规定的其他情形；四是能够保证数据的真实性、准确性、客观性、多样性；五是关于生成式人工智能服务的其他监管要求。

伴随人工智能技术的广泛应用和推广，深度赋能企业数字化转型，建议我国出台关于人工智能发展与伦理方面的相关数据安全倡议，重视数据隐私保护，限制数据滥用和挖掘，加强数据管理和监控，避免 AI 技术可能被滥用于网络钓鱼、宣传虚假信息甚至网络犯罪的威胁发生。

5.2.2. 面向学术和产业界的倡议

5.2.2.1. 协力推动数据安全人才培养

数据安全人才的短缺，尤其是复合型数据安全人才的奇缺，严重影响了产业的发展，因此需要高校、企业、政府等方面多方合作和支持，才能培养出更多能够应对复杂数据安全挑战的专业人才，为数据安全领域的发展和创新提供更强有力的支持。建议高校和各类教育培训机构，应增加数据安全相关的课程，邀请行业专家进行讲座和授课，让学生了解行业最新发展和趋势，通过联合培养、共建实验室、创建实习实训基地、线上线下结合等方式，培养实用型、复合型数据安全专业技术技能人才和优秀管理人才。企业可以提供实习和就业机会，让学生有机会接触和参与实际工作，加速学生的成长和发展。政府出台企业税收优惠、贷款、科研基金等政策和资金支持，鼓励企业进行数据安全人才培养；加强对数据安全行业的监管，规范行业发展，维护市场秩序和公平竞争环境，确保企业培养的人才能够发挥更大的效用。

政府、高校和企业各司其职，共同推进复合型数据安全人才的培养和发展，从政策、教育和市场等方面提供多层次的支持，为数据安全行业的人才培养和发展提供更强有力的保障。

5.2.2.2. 持续推动产学研一体化

数据安全的产学研一体化可以促进数据安全技术的创新和发展，加快技术的转化和应用。首先应加强产业界和学术界的合作，通过深度合作实现优势互补，共同推进数据安全技术的创新和发展；其次政府和社会应该给予创新型企业和团队更多的支持和鼓励，帮助他们实现技术创新和转化；最后，产业界和学术界需要积极探索数据安全技术的应用场景和商业模式，加速技术的转化和应用，政府应该为数据安全技术的应用提供更好的环境和政策支持。同时，发挥协会、联盟的作用，推动企业侧数据安全建设，将隐私计算等数据安全新技术可以在小范围内试点应用、落地，推动新型数据安全技术产品创新研发、融合应用。

总之，数据安全的产学研一体化需要政府、企业和学术界共同努力，加强合作和交流，共同推进数据安全技术的创新和应用。

5.2.3. 面向企业和组织的倡议

5.2.3.1. 企业持续完善数据治理职能机构和管理体系

数据领域的法律法规逐步健全完善，合规要求逐渐清晰明确。企业为了能够紧跟这些新举措新要求，亟需赋予关键角色来抓总和设置具体部门负责相关要求的落地，并依据业务实际设立岗位。如央企领域实行的首席合规官，一些大型互联网平台的隐私保护负责人，数据安全负责人等关键角色，对外响应主管监管部门、合作方、用户等要求，对内负责数据安全管理体系的建设。同时，赋予数据安全治理相关部门工作职责，对业务部门开展的数据处理活动进行把关，如事前的评估、审批，尤其是涉及跨境流动、权属转移等重要数据处理活动，并根据企业实际情况，不断修订和完善数据安全管理制度，按照规定向主管监管部门提交和审核。

未来，数据安全治理相关部门不仅仅是保障企业服务和网络的运行安全，还要为业务活动的合法合规、合理正当负责。因此，该部门要更为深入的参与到业务活动中，掌握更充分的话语权，才能更好的为业务保驾护航。

5.2.3.2. 企业采用透明和公正的算法和模型

随着互联网和社交媒体的普及，人们能够更容易地接触到各种信息，为了迎合用户，互联网和社交媒体往往通过算法和推荐系统向用户推送与其过去浏览行为相符合的信息，进而放大了用户的信息偏见，进而造成“信息茧房”的出现。同时，由于企业的趋利性、算法本身的设计缺陷、数据偏差等因素，可能出现针对用户的“算法歧视”，导致用户收到不公平对待。如企业可能出于商业目的，使用算法来做出决策，以最大化利润。算法本身的设计缺陷和数据偏差也可能导致歧视。如果算法的训练数据集本身存在偏差，例如数据集中缺乏某些人群的数据，那么算法可能无法准确地预测这些人群的行为，从而导致歧视。

随着互联网巨头的高覆盖面，尤其是数字平台型企业的全球范围和影响力日益扩大，使得任何一个国家都要考虑其算法和模型对公民利益和社会治理的挑战。因此倡议企业需要审慎设计和测试算法，在不涉及商业秘密的情况下，由大企业带头并联合更多的企业共同公开算法和模型，以确保其公正性和不歧视性。同时，政府和监管机构也需要加强对算法的监管和审查，确保其符合公正和道德标准，避免算法带来的不平等和歧视。

5.2.3.3. 持续加大数据安全治理投入

《关于促进数据安全产业发展的指导意见》提出，“到 2025 年，数据安全产业基础能力和综合实力明显增强，数据安全产业规模超过 1500 亿元”。从国内过去几年的数据安全产业发展态势看，政府、企业已经开始逐步加大数据安全投入，数据安全技术不断突破创新，数据安全企业快速发展，数据安全产业生态持续优化。但是，即便在数据安全投入较大的金融行业，仍在使用数据脱敏、数据加密等相对成熟的技术，未形成体系化的数据安全防护能力，在数据安全方面投入的主动性、积极性、充足性方面仍略显不足。

发展数据安全产业对于提高各行业、各领域数据安全保障能力，加速数据要素市场培育和数据

价值释放，夯实数字中国建设和数字经济发展基础有着重要意义。因此，一是建议主管部门加快推进数据安全合规落地，加大政策指导和监管力度，以查促改，督促相关数据运营单位加大数据安全方面的投入；二是政府部门应该以身作则，针对政务相关的大数据平台、城市数据中台、“东数西算”工程、数据交易所等典型场景，鼓励和支持创新技术产品深入应用，推进数据安全咨询、测评和培训服务业务广泛开展；三是应充分认识到每一种具体的业务应用场景都有其独特的数据安全需求，各个企业也应该结合自己实际需求，加大资金投入，支持数据加密、隐私计算、数据资产安全管理、数据安全监测监管等产品在典型场景深入应用，提升产业创新能力。

附录

A. 词汇表

数据：是指任何以电子或者非电子形式对信息的记录。（自《数据安全法》）

网络数据：通过网络收集、存储、传输、处理和产生的各种电子数据。（自《数据安全法》）

数据安全：通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。（自《数据安全法》）

数据处理：包括数据的收集、存储、使用、加工、传输、提供、公开等。（自《数据安全法》）

重要数据：指一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益的数据。（自《网络数据安全管理条例》（征求意见稿））

个人信息：以电子或者其他方式记录的能够单独或者与其他信息总结合识别特定自然人的各种信息，包括：姓名、出生日期、身份证号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。（自《民法典》）

敏感个人信息：一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。（自《个人信息保护法》）

组织：在本白皮书中所指的组织是指涉及数据处理（含个人信息处理）的企业、公共机构、行政机关或其他非法人机构。

去标识化：个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。（自《个人信息保护法》）

匿名化：个人信息经过处理无法识别特定自然人且不能复原的过程。脱敏是技术词汇，去标识化和匿名化是法律词汇。（自《个人信息保护法》）

安全评估：按安全标准及相应方法，验证某一安全可交付件与适用标准的符合程度及其安全确保程度的过程。（自 GB/T 25069-2022《信息安全技术术语》）

合规：对数据安全所适用的法律法规的符合程度。（自 GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》）

数据安全能力：组织在组织建设、制度流程、技术工具以及人员能力等方面对数据的安全保障。（自 GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》）

数据脱敏：通过一系列数据处理方法对原始数据进行处理以屏蔽敏感数据的一种数据保护方法。（自 GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》）

个人信息安全影响评估：针对个人信息处理活动，检验其合法合规程度，判断其对个人信息主体合法权益造成损害的各种风险，以及评估用于保护个人信息主体的各项措施有效性的过程。（自 GB/T 35273-2020《信息安全技术 个人信息安全规范》）

MPC：Multi-Party Computation，多方计算。使多个非互信参与方之间可以在数据相互保密的前

提下进行高效数据整合和计算，做到既使用多源数据进行指定的计算任务，又保证使用过程中数据不被泄露，包括数据使用方和计算任务执行平台都无法接触到原数据的明文，同时又能保证最终的计算结果与基于原数据明文的计算结果完全一致，真正实现数据的可用而不可见。

ChatGPT：ChatGPT 是一种用于优化对话的大型语言模型（Language Model），属于深度学习人工智能算法。据 OpenAI 介绍："ChatGPT 是一种对话式 AI（Artificial Intelligence），可运用自然语言连续对话，回答问题并挑战不正确假设。"

B. 数据安全主要产品与关键技术

针对本白皮书“第四章 数据安全技术需求与主流技术工具介绍”提到的系列化数据安全技术工具，对这些工具从概述、关键技术描述、应用场景等方面进行详细介绍。

B.1 全生命周期安全防护类

B.1.1 数据安全采集工具

数据安全采集工具能够对电脑、手机、服务器、各类传感器等进行接入和数据采集，通过对数据采集的流量进行解析和分析，实现数据采集设备的发现和识别、设备指纹管理、准入与访问控制、网络接入异常监控、数据采集合规分析、流量行为监控、信令白名单检查、和探查分析等功能。

数据安全采集工具采用 SM 国密加密通信技术，实现数据加密传输，防止数据泄露、被侦听或篡改，保障数据采集和传输过程中的安全。

数据采集设备发现和识别：对数据采集设备进行资产管理，管理设备的特征指纹、设备类型、用户、操作系统、品牌、厂商、IP/MAC 信息，形成“一机一档”管理体系。有新增前端设备，准入系统通过被动监测方式发现并更新设备特征指纹信息。

设备指纹管理：准入引擎内置指纹库，覆盖绝大多数终端类型，可通过指纹管理功能手动将该设备指纹提取进指纹库。

准入与访问控制：对接入的数据采集设备进行指纹认证，如发现接入的数据采集设备指纹信息与登记的设备指纹信息不符，则断开采集设备的网络连接，并通知管理员进行处置。

网络接入异常监控：数据安全采集技术包括仿冒检测能力，持续检测数据采集设备运行状态，当发现设备存在网络环境变更（如网络中断重新接入），或网络行为出现变更时触发仿冒确认过程，当发现设备硬件信息（MAC 地址）、指纹信息发生变化时，确认设备仿冒事件发生。当确认设备发生仿冒，准入系统需要通过连接重置的方式对设备网络流量进行限制或联动网络设备的方式直接切断设备网络连接。同时记录完整的发现及处置日志，满足合规审计要求。

数据采集合规分析：调研业务系统的目标和功能，梳理业务系统数据结构，通过数据采集的流量和日志信息，自动关联分析用户在系统上授权同意的相关操作行为与数据采集入库、数据在业务中使用、数据自动化决策等系统操作行为，生成《数据采集用户同意报告书》，向监管人员提供数据合法合规采集的相关监管报告，为监管人员评估数据采集、使用是否遵循用户同意原则提供数据支撑。整理系统要收集的敏感数据特征，通过数据识别技术，审计业务系统采集的各类敏感数据，发现未列入数据采集范围的敏感数据采集行为，生成《数据超范围采集报告书》，向监管人员提供数据合法合规采集的相关监测报告，为监管人员评估数据采集是否遵循必要、最小原则提供数据支撑。

流量行为监控：通过监测设备出入站流量，持续计算周期内设备使用上下行流量的平均值，当发现设备上下行流量波动超过阈值时及时告警并处置。

信令白名单检查：检查发向数据采集设备的控制信令内容，匹配信令白名单列表，只放行白名

单列表中允许放行的控制信令，阻断未登记在信令白名单列表中的控制信令传输到数据采集设备。

探查分析：根据运维人员策略配置，能够对发现的数据采集设备进行全方位、多维度的深入识别。通过设备指纹特征，资产库、自动学习等技术，发现其 IP/MAC、操作系统、设备类型、厂商、型号、序列号、开放端口、接入位置等信息。资产发现后可以对设备进行自动分类分组，并基于组织结构进行统计分析、基于类型和厂商进行统计分析、基于接入位置进行统计分析，生成图形化报表，支持快速信息筛选。

B.1.2 数据防泄露系统（DLP）

DLP 系统是结合了识别、监测、管控三类技术而形成的数据安全系统，其所能实现的功能便是将三类技术要素进行任意组合，对不同的数据内容通过不同的通道（与参与者）进行传输的行为进行区别化的管控。

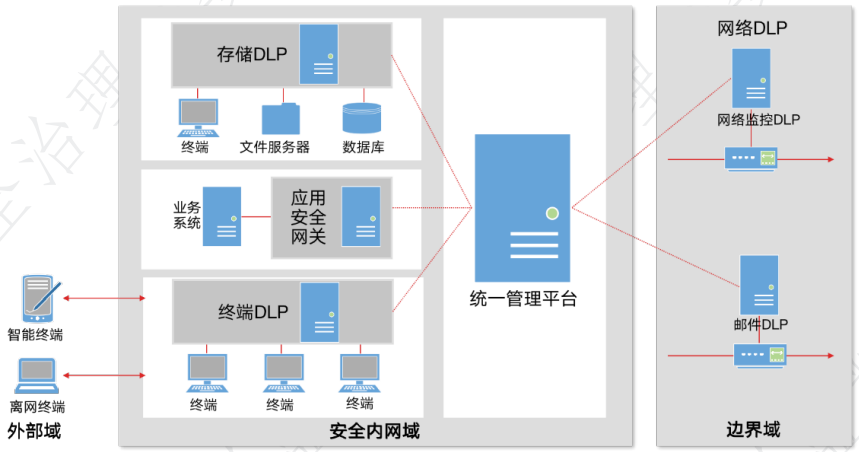


图 B-1　DLP 系统框架示意图

DLP 技术可分为常规 DLP 技术、内容指纹匹配技术、计算机视觉技术、高级语义分析检测技术等。

常规 DLP 技术：包括基于关键字的检测技术、基于正则表达式的检测技术、基于字典的检测技术、基于脚本的检测技术、基于数据标识符的检测技术，可实现一般数据的分析检测。

内容指纹匹配技术：包括索引内容指纹匹配技术、精确内容指纹匹配技术。索引内容指纹又称索引数据匹配（IDM），是用于对数据内容进行模糊匹配的算法技术。精确内容指纹又称精确数据匹配（EDM）用于对结构化数据（各类表格）进行精确匹配。

计算机视觉技术：是指对图像进行识别判断，并理解图像含义的技术，包括光学字符识别（OCR）、图章识别、物体识别、标志识别、人脸识别。

高级语义检测技术：是通过文本基本处理、高层语义分析进行语义分析。文本基本处理主要包括中文分词、语言模型、特征权重、核心词、关键词提取等一系列的方法，高层语义分析主要包括词向量和句向量分析、主题模型、深度神经网络以及文本分类等技术。

DLP 系统的核心功能包括：

实现敏感数据识别：采用关键字、正则表达式等基础规则匹配方法以及基于自然语言处理的智

能识别方法识别网络、终端、邮件等主体中的敏感数据，根据管控策略执行监控、阻断、审计等管控行为。

实现特殊人员标识：针对组织机构特殊人员管控要求，数据防泄露系统可以按照组织架构、用户账号、姓名等设置黑名单、放行白名单、审计白名单。

实现管控策略配置：用户结合企业的管理制度、组织架构、特殊要求，设置不同的匹配规则和匹配策略根据敏感数据管理的制度和手册，整理出违规行为处置流程、风险策略和事件策略，预先输入到数据防泄露中，提高安全事件处置效率。

实现监控保护审计：数据防泄露采用内容分析引擎，实时监听网络传输数据，分析网络信息包的副本，检测传输数据是否违反策略，自动记录敏感数据的使用情况。根据预先制定的安全策略，对敏感数据的扩散范围进行审计，对于审计出来的风险事件自动触发异常报警。

实现违规行为阻断：数据防泄露系统发现违规外发等行为，自动根据安全管控策略，阻断违规行为，防止敏感信息泄露，触发审计与告警。对于需要审批的违规行为，系统对其阻断后将自动进入审批流程，并且系统根据审批的结果来判断是否放行或者始终阻断。

实现安全态势评估：数据防泄露系统，根据数据安全风险评估模型，实时汇总各项指标数据，实时计算指标数值，根据模型计算规则，综合各项指标，实时评估风险范围和风险级别，及时掌握数据安全风险态势。根据风评报告模板，基于风险态势各项指标的总体数据与局部数据，自动生成风评报告，提升用户数据安全管控效率。

DLP 主要的应用场景包括：

终端安全管理场景：对入网后的终端设备还需进行安全加固，建立统一的安全基线，确保接入网络的终端设备是安全、可信的终端。主要通过补丁更新、防病毒软件安装、系统配置等技术，一方面实现终端标准化管控，一方面实现对终端行为的审计（包括敏感数据识别、敏感数据分类、数据分级阶段、敏感数据分布、敏感数据外发、敏感数据追踪、终端水印管理、屏幕录像审计、终端离线管控、终端外发审批、泄密追溯等功能）。

邮件防泄密场景：通过邮件外发数据是常见的泄密手段，所有的泄密事件中很多都是出自这个环节上，建议使用邮件防泄密网关来对邮件外发内容进行过扫描，发现违规外发情况，可以根据策略设定，向管理人员发送告警信息（以弹出消息框或者邮件形式）。

文档发布 / 数据交换场景：数据只有在不断的交换、传输的过程中，才能体现自身的价值；因此数据流转环节一定要“疏、通结合”，才能实现真正的安全可控。达到安全控制的同时，要给用户提供更加高效的数据交换通道：文档发布系统、数据交换系统。

B.1.3 数据库加密系统

数据库加密系统可对数据库中存储的数据在存储层进行加密，有效避免了因数据文件被拖库而造成数据泄露的问题，从根本上保证数据的安全。

对于数据库加密技术，从加解密位置区分，可以分为应用层加密、数据库中间件加密、数据库系统自身加密、数据库系统所依赖的文件系统加密以及存储硬件加密等不同技术路线。

应用层加密：在应用系统层的源代码中对敏感数据进行加密，加密后将密文存储到数据库中。

前置代理加密：类似于应用系统加密技术，前置代理加密技术也是在数据保存到数据库之前对敏感数据进行加密，并将密文存储到数据库中；而不同于前者的是，前置代理加密技术通常是以“前置代理加密网关”这种独立组件产品的形式实现的。

后置代理加密：是基于数据库自身能力的一种加密技术，可充分利用数据库自身提供的定制扩展能力实现数据的存储加密、加密后数据检索和应用透明等目标。

数据库透明加密：是一种对应用系统完全透明的数据库端存储加密技术，在数据库引擎的存储管理层增加一个数据处理过程，当数据由数据库共享内存写入到数据文件时对其进行加密；当数据由数据文件读取到数据库共享内存时对其进行解密。

数据库透明加密能够在无需数据库使用者改变访问接口甚至无需知情（透明）的情况下，使得数据库内存储的数据为经过加密的密文数据。这种技术的核心优点在于其对数据库使用者的高度友好性，几乎无需对使用数据库的已有应用（业务）系统进行任何改造和升级，就能实现对结构化数据的机密性进行有效保护。

透明数据加密技术凭借其自身的上述优势，几乎适用于全部有数据库加密需求的应用场景，尤其是在对数据加密透明化有要求，或需要对数据库超级用户进行数据访问权限控制，以及对数据加密后数据库性能有较高要求的场景中。

对数据进行透明加密可在不同层次、不同位置进行，下图展示了若干典型多层数据加密方案在透明性、性能影响、安全强度等方面的不同效果和表现。

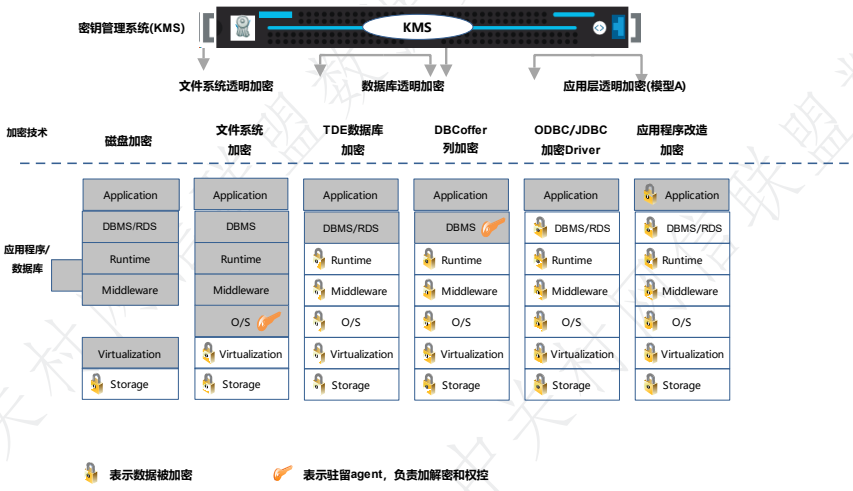


图 B–2　多层数据加密方案效果对比

（1）列加密

数据库列透明加密是按列对数据进行加密的，针对指定的列，采用指定的加密算法和密钥、盐值等进行加密处理。加密后的数据以密文的形式存储在 DBMS 的表空间中。

只有经过授权的用户才能看到明文数据，并且授权也是按列进行的，这种方式具备很好的灵活性和安全性。非授权用户，将无法读取（查询）加密列和更改加密列的数据。

权限管理上，数据库列透明加密采用了分权的机制，实现了三权分立，有效制约了数据库管理

员（DBA）这样的特权用户对数据的访问。同时这种保护又是透明的，不会对管理员的日常工作造成不便。

数据库列透明加密具有应用透明的特性，应用系统和外围维护工具无需改造，涵盖 SQL 语句透明、存储程序透明、开发接口透明、数据库对象透明、管理工具透明。

下图说明了列加密的数据处理机制：当明文数据到达数据库时，被列加密组件自动进行加密处理，之后数据以密文形式保存在数据文件中；在读取数据时，数据被列加密组件根据权限进行自动的解密处理。这些操作对应用都是透明的。

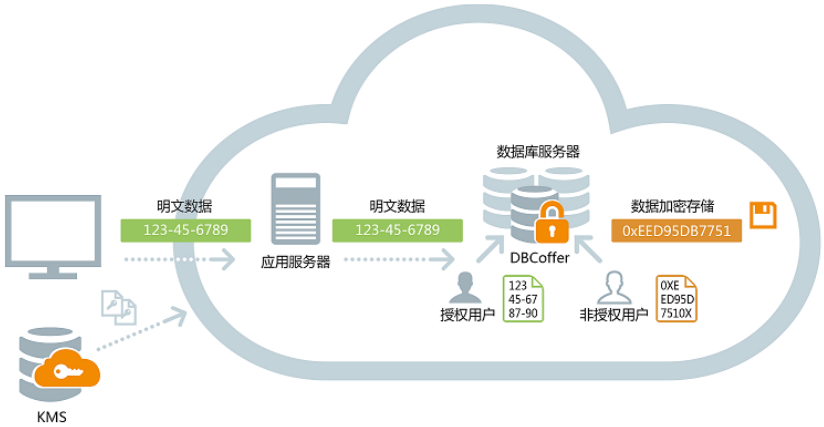


图 B–3　数据库列透明加密

（2）表空间加密

下图以 Oracle 数据库为例，说明了表空间透明加解密的关键机制：TDE 插件作为 Oracle 的插件，负责对数据存储时对数据进行加密处理；在数据从表空间读取时，负责对数据进行解密处理；并且根据读取数据的数据库账户，进行相应的权限控制。

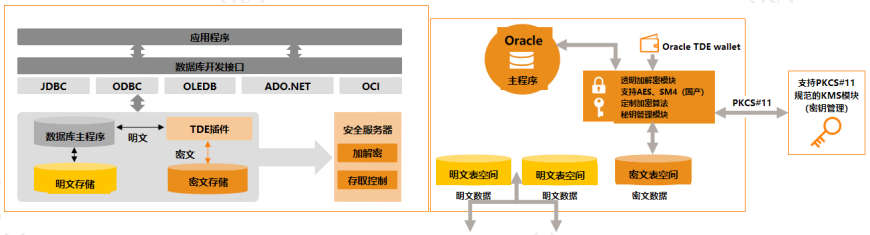


图 B–4　表空间（OracleTDE）加密技术

文件系统加密：是在操作系统的文件管理子系统层面上对文件进行加密，大多是通过对与文件管理子系统相关的操作系统内核驱动程序进行改造实现的。

磁盘加密：磁盘加密技术通过对磁盘进行加密以保障其内部数据的安全性，从实现上有软硬两种方式：软件方式的磁盘加密技术，大多是通过专用的磁盘加密软件对磁盘内容进行加密；而硬件方式的磁盘加密技术，在实现上则有两个思路：一种是针对单块硬盘的磁盘加密，一种是针对磁盘阵列或 SAN 存储设备的磁盘加密。

B.1.4 数据备份 / 恢复工具

随着灾备技术的演进与发展，数据与业务保护的架构可充分发挥云计算弹性、池化、资源综合利用的特点，利用分层分级数据捕获、系统高可用、分布式等相关灾备技术，建立统一架构、覆盖不同场景和不同灾备诉求的灾备平台，实现灾备资源弹性扩展和灾备服务能力的自由编排。

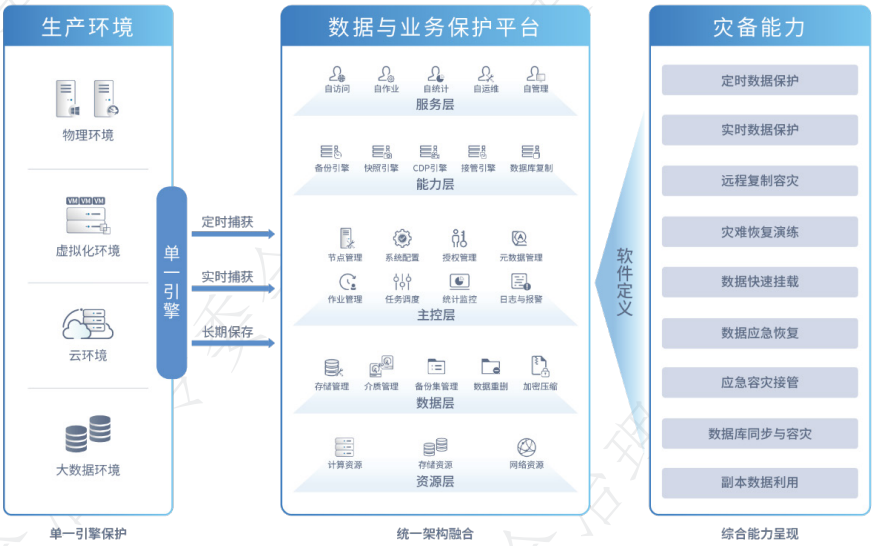


图 B-5　新一代数据与业务保护平台架构图

相对传统灾备系统，其关键技术包括：

单一引擎全面保护：为规避传统灾备系统针对不同 IT 环境、数据类型安装多个灾备引擎存在的模块化管理、资源占用、兼容性等一系列问题，平台采用单一灾备引擎获取数据，全面覆盖云、大数据、虚拟化、X86、小型机、国产化等不同 IT 环境和不同灾备对象的统一灾备或分级灾备保护的需求。

灾备能力融合：为确保灾备架构的灵活性、敏捷性，实现灾备能力可编排，灾备平台由统一资源层、数据层、控制层和服务层等构成，融合数据备份、数据快照、实时捕获、数据库复制、长期保存、容灾接管等灾备技术，通过软件授权控制方式，可灵活组合不同层级的灾备保护能力，满足业务工作负荷需要。

数据多元化利用：为最大化利用数据，降低副本数据存储空间，采用副本数据管理技术实现了从副本数据采集、安全传输、安全存储、数据索引、数据呈现到各种数据利用的统一管理，提高了数据的价值。

数据备份 / 恢复工具可面向用户生产环境提供定时备份、实时备份、应急接管等功能，覆盖包括本异地灾备、云上数据保护、云容灾、海量文件备份、防勒索病毒等场景，还可以进一步通过副本数据管理技术，满足用户开发测试、模拟演练等场景需求。

数据备份 / 恢复工具可运用在多个应用场景，具体如下：

本异地灾备场景：对于不同生产环境的用户，数据备份 / 恢复工具可提供备份、数据复制、应用接管、异地数据同步等功能，提供本异地的数据级和应用级灾备，满足等保合规、数据和业务保护需求。

云上数据保护场景：为保障云上数据安全，面向云虚拟主机、数据库数据、文件等，提供云上

数据备份与恢复、数据可用性校验，可以将云上数据备份至本地或云端，实现云上数据保护。

云容灾场景：对于业务上云的用户，通过构建云下或异构云间的容灾，采用实时数据复制、应急接管等，当云上业务中断时，可在本地或异构云上实现业务连续。

海量文件备份场景：面对用户海量非结构化数据的增长，基于数据备份/恢复工具分布式可扩展架构，实现海量备份任务的并发、数据的负载均衡，提升海量数据备份效率。

防勒索病毒场景：数据备份/恢复工具可提供 CDP 持续数据保护，当用户生产主机感染勒索病毒后，可在灾备平台选择任意时间点恢复数据，可有效防止勒索病毒攻击导致的数据丢失。

B.1.5 统一身份认证系统（IAM）

统一身份认证系统对数据安全的意义主要体现在三个方面：

首先，实现应用系统的单点登录 SSO，用户通过 IAM 访问门户首次认证登录成功之后，在系统设定的票据有效周期中，可多次访问组织内各业务应用，用户身份票据自动保持、传递，不再需要进行多次身份认证。单点登录为组织内应用系统提供了统一的入口，整合了组织资产，降低了由用户账号被窃导致的数据资产遗失等安全隐患。

其次，统一身份认证系统可设计完善的权限管理机制，进行严格的访问控制，避免了数据资源的过度访问导致的数据泄露，配合完善的安全审计规则，可实现数据访问事前事后的全面管理。

另外，统一身份认证系统通过构建完整可信的用户资源信息库，整合各应用系统的用户库，集中实现用户信息统一管理，并通过数据同步功能向应用系统同步，大大提高了组织数据资产的可管理性，也便于系统的安全审计。

统一身份认证系统的建设包括四个子域：身份数据、身份管理、访问执行及访问管理，通常分为身份管理、访问管理及门户三部分，集身份管理、身份认证、授权管理、应用资源访问控制及其安全审计于一体，构建多信息资源的应用整合和安全防护的安全基础服务平台。统一身份认证系统框架如图所示：

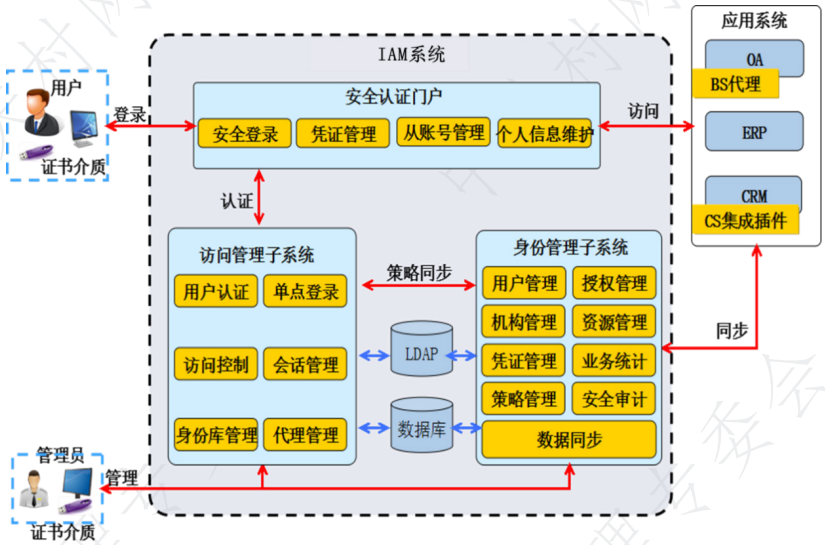


图 B-6　统一身份认证系统技术体系框架

安全认证门户：安全认证门户为用户集中展现可访问的应用列表，为用户提供统一的认证入口。认证门户能对用户所提供的数字身份凭证进行在线认证，识别用户身份的真实性，并通知各个应用系统，同时在门户中提供单点登录功能，实现门户与各应用系统之间进行一次性认证与登录。

身份管理子系统：身份管理子系统提供用户身份完整的生命周期管理、应用系统管理，身份管理子系统可以通过接口与业务系统进行用户信息同步，同时也可以为访问管理子系统提供用户信息，可以通过本系统进行行为审计查询。

访问管理子系统：访问管理子系统主要为用户提供集中的身份认证机制，采用数字证书技术进行身份鉴别，提供面对业务系统的访问控制机制，用户全行为流程进行跟踪审计。

统一身份认证系统的用户访问业务系统的流程如下图所示。统一身份认证系统建设后，每一用户拥有唯一的账户信息，用户访问应用系统时，将请求重定向到统一身份认证系统服务器，进行统一的身份认证和权限审核，认证通过后，即跳转进行业务访问，当用户需访问其权限范围内的其他应用系统时，无需再次进行身份认证。同时，通过基于机构、岗位、用户组和角色等不同维度的授权管理，灵活地实现对用户的权限控制，通过全面的用户行为数据收集，实现统一的安全审计，对用户的行为日志进行审计和综合分析。

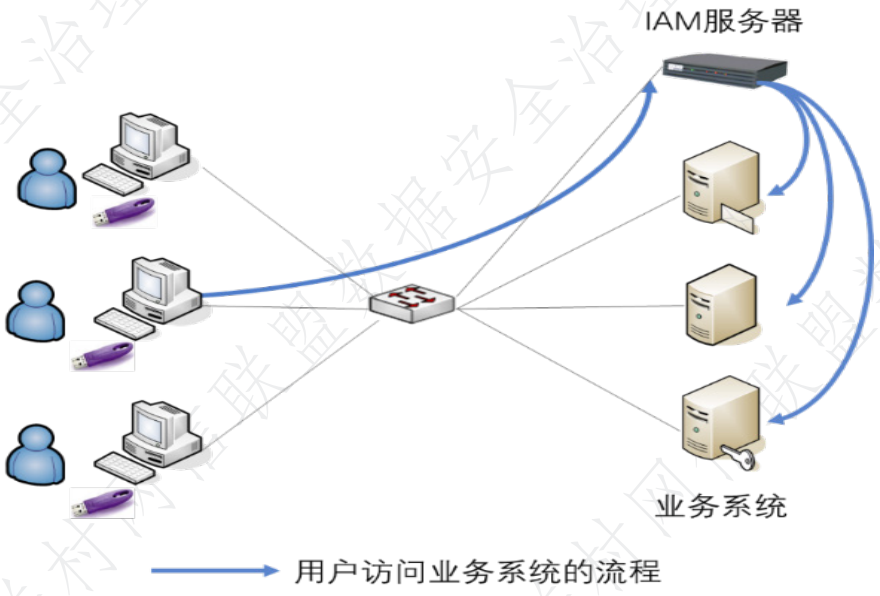


图 B-7　用户访问流程图

B.1.6 数据零信任平台

零信任架构主要针对传统安全防护的弊端而设计。传统网络安全防护大都通过在网络边界部署防火墙、IDS、入侵监测系统等防护设备，对企业网络层层防护，从外向内地将攻击拦截在外从而保障企业网络的安全。然而现在的网络架构和使用模式正在对这种基于边界的防护策略发起挑战：缺乏内部流量的检查、主机部署缺乏物理和逻辑上的灵活性、存在单点故障。比如：位于网络防护边界之外的远程用户和移动设备的接入，云上资产的访问与防护等问题，一旦某个单点被突破，就给了攻击者横行移动、进一步入侵的可能，传统防护策略逐渐显得力不从心。

而零信任架构的改变在于，“对何种网络位置，均从零开始依靠鉴别与验证建立信任”，从而实现纵深防护。因此，通过零信任，可以防止恶意用户在企业边界内部访问私有资源、防止数据泄露以及恶意操作。

与其他技术相比，零信任更像是一种体系，或者是是一种理念。融合“管理平台”+“安全组件”+“安全服务”的零信任逻辑架构如下图所示：

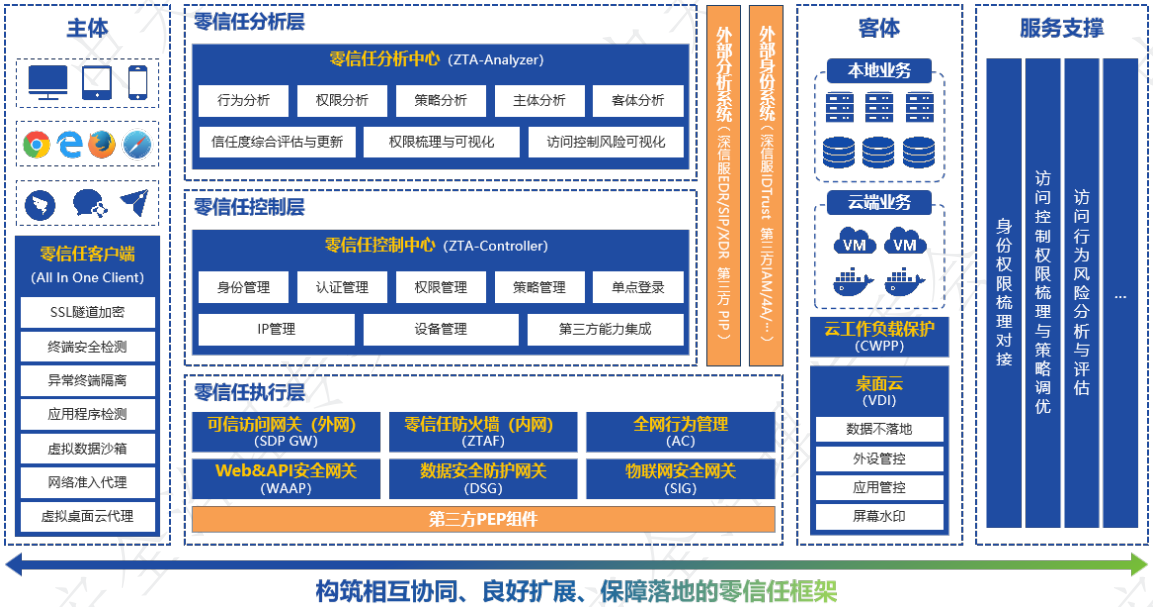


图 B–8　数据安全零信任架构图

统一管理平台打通端到端身份信息，实现全局风险研判与信任评估：管理平台部分可以进一步细分为“零信任分析中心”和“零信任控制中心”，零信任分析中心的主要职责是通过多维度获取的信息进行信任的评估，除了自身的分析模型与算法组件，还可以通过开放 API 与第三方分析系统进行对接，实现对访问行为和风险的持续评估；零信任控制中心主要职责是身份管理，以及根据分析中心的评估结果，生成动态的访问控制策略，向分散各处的、各种类型的安全组件进行下发，统筹全局的访问控制。

各种安全组件匹配用户端到端数据访问控制的场景需求：安全组件部分的核心职责是接收和执行管理平台的访问控制策略，其组成、形态、部署位置、功能选择等，可以随业务管控实际需求而定：（1）零信任一体化安全客户端，是零信任架构的重要组成部分，整合了安全基线核查、病毒与漏洞防护、网络安全接入、数据泄露防护等多种安全能力；（2）匹配不同业务场景的各类安全网关，包括外网访问、内网访问、数据中心服务间访问、物理网访问等等；（3）通过开放 API 接口实现异构厂商安全组件的按需灵活对接。

多样化的安全服务实现安全威胁的快速识别与处置：零信任不是“交钥匙工程”，系统和设备的堆砌无法达成既定目标，应该结合安全专家知识与云端分析能力，提供线上或线下多样化的安全服务（如账户与访问权限梳理、业务访问路径梳理、访问控制策略优化、风险分析与处置等），实现安全威胁的快速识别与处置。

“平台”+“组件”+“服务”的体系，最终构筑贯穿用户、终端、应用、连接、权限、数据，

构筑端到端的信任体系。完善的零信任系统，应该尽可能覆盖端到端业务运行流程，考虑如何在用户、设备、应用、连接、权限和数据等多个环节，落地“什么值得信任”这个关键的问题。核心的功能包括：（1）通过多维度的终端环境检查，确保访问数据的终端设备安全合规；（2）通过跨场景全局的统一身份管理与多因素认证方式，保证访问数据的用户其身份合法；（3）通过精细化权限控制，对数据的访问进行细粒度授权，防止越权、串权、滥权的访问；（4）根据数据重要程度和密级程度的不同，通过云桌面、终端数据沙箱、网络隔离、数据访问行为审计等技术手段，实现差异化数据泄密防护，保障数据安全；（5）通过持续信任评估，发现数据访问过程中行为的异常，进而生成动态的访问控制策略。

面向不同的应用环境、业务场景，零信任架构有多种灵活的实现方式和部署模式。面向远程办公、大数据中心、物联网等典型场景，按照访问主体和资源之间的关系，数据平面的访问代理重点考虑采用和被保护资源相结合的部署模式，搭建安全访问通道，对访问请求进行分流。控制平面的访问控制引擎负责指挥，按照“先认证后连接”原则，建立、维持有效连接，实施对资源的安全访问控制。在此过程中，持续开展安全监控评估，对应用场景中出现的安全威胁及时响应，消减风险。

针对远程办公应用场景：在零信任架构下，不再采用持续强化边界的思维，不区分内外网，针对核心业务和数据资产，梳理访问这些资产的各种访问路径和场景，在人员、设备和业务之间构建一张虚拟的、基于身份的逻辑边界，针对各种场景构建一体化的零信任动态访问控制体系，构建更安全的远程办公网络。

针对大数据中心场景：零信任架构通过微隔离技术，实现环境隔离、域间隔离、端到端隔离，根据环境变化自动调整策略，实现精细化隔离的网络安全策略及以身份为基础的逻辑边界，同时安全策略可以自适应调整。

针对物联网场景：借助边缘计算技术，解决终端的身份认证和访问控制价，允许身份可信、经过动态授权的物联设备入网，并动态监测，及时发现并处置假冒、伪造的非法连接。其核心思想是对物联设备建立身份指纹，由主体属性、环境属性和客体属性构成，通过持续主动扫描、被动监听检测、安全接入控制区等方式，对物联终端进行持续信任评估、访问控制，解决物联终端的身份仿冒和恶意访问。

B.1.7 数据库运维安全系统

在数据安全治理的过程中，不但要预防外部攻击造成的敏感信息泄露，同时也要关注内部环境中的数据使用安全，尤其是数据在运维过程中的安全。

传统的数据库运维管理方式存在着管理流程不完善、技术手段缺失、人员素质参差不齐等问题，使数据库运维面临：人员身份不明确导致的身份识别风险、密码安全管理难导致的密码泄露风险、运维行为不可控导致的访问操作风险、运维过程不透明导致的流程管控风险以及监控审计手段缺失导致的难以准确追踪溯源，定位责任人。

数据库运维安全系统主要为了规范内部人员的访问行为，特别是针对敏感数据的安全加固与访问控制，将运维人员身份鉴别、安全策略、访问控制、审批流程管理和审计追责有效结合，解决运

维账号共享与运维环境共享带来的运维身份不清问题，避免内部运维人员的误操作和恶意操作行为，确保运维行为在受控的范围内安全高效的执行。

数据库运维安全系统的核心功能主要包括：特权访问管理（PAM，Privileged Access Management）、密码代填（密码桥）和运维访问防绕过等功能。

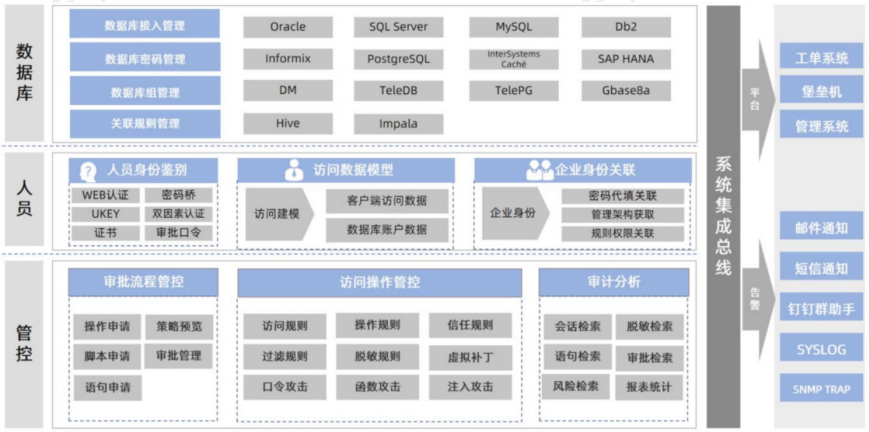


图 B-9　数据库运维安全系统架构图

账号发现和启用：提供发现，识别和启用特权账号的功能，包括支持周期性，临时或连续扫描发现的功能。还包括自动发现目标服务和系统（包括虚拟机）以进一步发现其中包含的特权账号的能力。

特权凭证管理：提供对组织和系统定义的特权账号凭证或机密（包括 SSH 密钥）进行管理和保护的核心能力。用户可通过生成，存储，轮换和检索等方式对凭证进行交互访问。还包括目标系统上服务和软件账号（即嵌入式账号）的轮换。这些功能至少需要能够通过 Web 控制台或 API 访问 PAM 工具。

特权会话管理：为特权访问会话提供会话建立，管理，录制和回放，实时监视，基于协议的命令过滤以及会话分离。包括使用 PAM 工具管理从凭证签出到签入期间的交互式会话的功能，即使在正常情况下，凭证不会向用户公开。此功能还可能涉及一些限制，例如在登录目标系统时允许 / 拒绝某些类型的命令和功能。

机密管理：此功能提供了针对非人类用例（例如机器，应用程序，服务，脚本，进程和 DevSecOps 流水线）的凭据（例如密码，OAuth 令牌，SSH 密钥等）进行访问管理的能力。它具有生成，存储，转换和向非人类实体提供凭据的能力（例如，通过 API）。还具有在不同的非人类实体之间交换机密和管理授权的信任代理能力。这些功能组合在一起支持动态环境的机密管理，并提供对 RPA 平台的支持。

日志和报告：此功能提供了将所有单个事件（包括更改和操作）记录为 PAM 操作的功能。为监视和确定风险事件的根本原因，并识别未经授权的访问，将单个事件基于用户，时间，日期和位置，并通过逻辑顺序关联与其他事件一起处理。提供事件数据库的审计和报告的功能，支持预建报告和临时报告。事件数据还必须包含来自特权会话的信息。利用特权账号活动的分析（基线、风险评分和告警），实现检测和异常标记。目的是为了更好地识别领先和滞后指标，从而识别特权访问异常，

以触发对告警的自动应对策略。

特权任务自动化：此功能提供针对多个系统上执行的特权操作，将与其相关的多步骤重复任务进行自动化的能力。使用常见IT系统和设备的可扩展的预配置特权操作库，在不同活动之间来回协调，并根据需要请求更多信息，同时通过对照策略和设置检查输入来提供防护。

特权提升和委派：此功能基于主机强制执行应用程序的允许/拒绝/隔离等控制策略，并允许授权的命令或应用程序在提升的特权下运行。管理员将使用非特权账号登录并根据需要提升特权。任何需要额外特权的命令都必须通过这些工具，从而有效地防止管理员执行不安全的活动。

相邻系统集成：此功能支持与相邻的安全和服务管理能力集成和交互，包括身份治理和管理（Identity Governance and Administration, IGA）、SSO、MFA和企业目录，对灵活的连接器和集成框架的支持，常规API访问，与IT服务管理（IT Service Management, ITSM）系统的集成，安全信息和事件管理（Security Information and Event Management, SIEM）系统，以及漏洞管理。

即时PAM方法：此功能提供按需特权访问，而无需共享拥有长期特权的账号。

密码代填（密码桥）：预先建立运维账号和数据库账号的映射关系表，当运维账号通过数据库连接工具（如SQL*Plus、PL/SQL Developer等）访问数据库时，密码代填技术会在数据库连接过程中按照映射关系表对账号、密码进行替换，实现运维账号直接访问数据库的效果。同时数据库账号不对运维人员暴露，增强了账号的安全性，解决了账号共用问题。

运维访问防绕过：通过数据库的logon触发器进行访问白名单控制。访问数据库的客户端设备，须先将其关键信息（IP地址、用户、客户端主机名等）进行备案注册，按照注册内容对触发器进行调整，实现客户端与数据库建立连接时的有效控制。试图绕过安全设备的访问行为，也会被认定为非授信的异常访问。只有在授信终端上使用授信客户端运维工具、运维账号、并通过合规的访问通道，才可对数据库进行运维操作，真正实现全方位的访问控制，保障安全无死角。

B.1.8 数据库防火墙系统

数据库防火系统是以风险策略为核心，以风险识别、风险评估、风险处置、风险分析为手段。帮助组织快速构建主动式安全防护体系，减少因风险事件造成的经济损失，节省漏洞的修复成本，降低投入到合规工作中人力成本。

数据库防火墙系统是基于数据库协议分析与控制技术的增强级数据库安全防护系统，能够提供虚拟补丁、防SQL注入攻击核心功能。

虚拟补丁，主动防护已知漏洞：虚拟补丁技术是系统通过协议解析技术，实时监控数据库漏洞攻击行为，防止利用已知漏洞对数据库发起的攻击，保障数据库安全与应用稳定。在数据库外围创建安全层，无需根据数据库厂商提供的补丁做数据库修复，也不需要停止服务和回归测试，使漏洞防御的实施更为轻量化和及时。

防护规则，全面感知防护风险：系统支持多种类型的防护规则，针对不同风险提供相应的防护规则，具体包括如下：

（1）注入攻击：提供SQL注入防护和XSS攻击防护规则，防止利用应用程序漏洞的注入攻击。

（2）操作规则：防止高危语句操作、批量数据篡改和大规模数据泄露等风险行为。

（3）访问规则：针对应用端信息、客户端信息、时间等条件限定非法账户登录行为。

（4）口令攻击：限定不同访问源和数据库账户的失败登录频次。

（5）语句规则：针对 SQL 语句模板设置访问控制规则。

（6）例外规则：可在每条风险防控规则中设置合规的例外访问操作，不拦截不审计。

（7）信任规则：针对信任操作行为及语句建立白名单不拦截，避免影响正常的业务行为。

（8）脱敏规则：配置脱敏规则及脱敏算法防止敏感数据泄露。

敏感数据，防止敏感信息外泄：关联 schema、表、字段等对象形成敏感数据组，基于与或关系并结合其他防护项建立敏感数据防护规则。限定敏感数据的访问时间、来源 IP 地址和访问账户，针对高危操作进行语句拦截或会话阻断。

应用关联，准确定位访问信息：基于应用会话捕获应用账户、应用登录 IP 及 URL 等关键防护信息，添加到防护规则进行风险行为管控，建立并完善应用关联防护体系。将业务信息和数据库操作行为进行关联，有效追溯应用系统的原始访问者和请求信息，对于应用端的数据库访问、操作行为，实施精确安全管控和防护。

防漏扫，抵御漏扫通过测评：对数据库漏洞扫描进行防御，防止漏扫工具扫描出漏洞，协助用户通过测评。

安全审计，关联分析追责溯源：从风险、语句和会话多个角度对风险行为进行审计。用户可基于风险模型进行风险行为的关联查询和深度挖掘，实现风险分析和问题追溯。

风险告警，实时告警及时处置：系统提供数据库风险告警能力，基于灵活的防护规则，对外部发起的数据库漏洞攻击、恶意的 SQL 注入行为、非法的业务登录、高危的 SQL 操作和过量的数据下载，提供实时的风险告警。

数据库防火墙系统的核心技术包括：

立体防护，阻断拦截审计告警：会话阻断，基于数据库安全防护规则，对高危会话进行强制阻断，禁止该会话的所有操作行为。语句拦截，比会话阻断更为细致的限制，只对风险语句进行拦截，不影响会话的整体操作。

精确防护，协议解析语法分析：准确的协议解析能力，是数据库安全防护的基础。由于串联防护的特殊性，任何误报、漏报都可能造成不可估量的损失。传统解析手段采用正则匹配和较为简单的协议解析技术来分析 SQL 语句，解析结果不准确，数据库通讯协议解析内容需要覆盖 SQL 语句、参数化语句句柄、SQL 参数、应答结果信息、结果集结构信息及结果集数据。

双向防护，黑白名单周密布防：通过学习模式及 SQL 语法分析构建动态模型，形成 SQL 黑白名单，放行 SQL 白名单语句，阻断 SQL 黑名单语句。

B.1.9 数据脱敏系统

数据脱敏系统是通过采用一系列数据脱敏技术对原始数据进行处理以屏蔽敏感数据的一种数据保护产品。数据脱敏的主要目的在于：（1）从源头加强敏感信息的保护，避免敏感信息在不可控的

网络空间中流转时被泄露，从信息源头进行阻断；（2）保留了原始数据的主要特征，如格式、类型、频率分布、唯一性等；（3）在一定程度上保证了数据的可用性，可做进一步的处理与分析。

数据脱敏系统的主要技术包括：泛化技术、随机化技术、抑制技术、扰乱技术、有损技术、差分隐私技术、K- 匿名化技术等。

泛化技术：是指在保留原始数据局部特征的前提下使用一般值替代原始数据，泛化后的数据具有不可逆性。

随机化技术：是指通过随机化修改属性的值，脱敏结果与原始数据产生明显区别，但服从数据的概率分布。

抑制技术：是指通过隐藏数据中部分信息的方式来对原始数据的值进行转换，又称为隐藏技术。

扰乱技术：是指利用加密、重排、均化、散列、替换、局部混淆等方式对原始数据进行修改。

有损技术：是指通过损失部分数据的方式来保护整个原始数据，适用于数据集的全部数据汇总后才构成敏感信息的场景。

差分隐私技术：是在发布数据前，对原始数据进行一些随机扰动，从而使得针对该数据集的攻击无法确定特定个体的信息。

K- 匿名化技术：通过概括和隐匿技术，发布精度较低的数据，使得同一个准标识符至少有 k 条记录，使观察者无法通过准标识符连接记录，不能判别出隐私信息所属的具体个体。K- 匿名算法按照泛化范围，可以分为全局算法和局部算法。

数据脱敏系统根据数据脱敏的实时性和应用场景的不同，分为数据动态脱敏和数据静态脱敏。

（1）数据动态脱敏

数据动态脱敏一般用在生产环境中，将敏感数据实时进行脱敏后用于应用访问等生产环境。动态数据脱敏旨在通过类似网络代理的中间件技术，按照脱敏规则对于外部申请访问的数据进行即时处理并返回脱敏后结果。数据动态脱敏通常会在数据对外提供查询服务的场景中使用，在降低数据敏感程度的同时，最大程度上降低了需求方获取脱敏后数据的延迟，请求实时产生的数据也能即时得到脱敏后结果。数据动态脱敏主要特点包括：

实时性：能够实时地对用户访问的敏感数据进行动态脱敏、加密和提醒。

多平台：通过定义好的数据脱敏策略实现平台间、不同应用程序或应用环境间的访问限制。

可用性：能够保证脱敏数据的完整，满足业务系统的数据需要。

图 B-10　数据动态脱敏框架示意图

（2）数据静态脱敏

数据静态脱敏一般用在非生产环境，将敏感数据从生产环境抽取并脱敏后用于培训、分析、测试、开发等非生产环境。数据静态脱敏旨在通过类似 ETL 技术的处理方式，按照脱敏规则一次性完成大批量数据的变形转换处理。数据静态脱敏通常会在将生产环境中的敏感数据交付至开发、测试或者外发环境时使用，在降低数据敏感程度的同时，能够最大程度上保留原始数据集所具备的数据内在关联性等可挖掘价值。数据静态脱敏主要特点包括：

适应性：即可为任意格式的敏感数据脱敏。

一致性：即数据脱敏后保留原始数据字段格式和属性。

复用性：即可重复使用数据脱敏规则和标准，通过定制数据隐私政策满足不同业务需求。

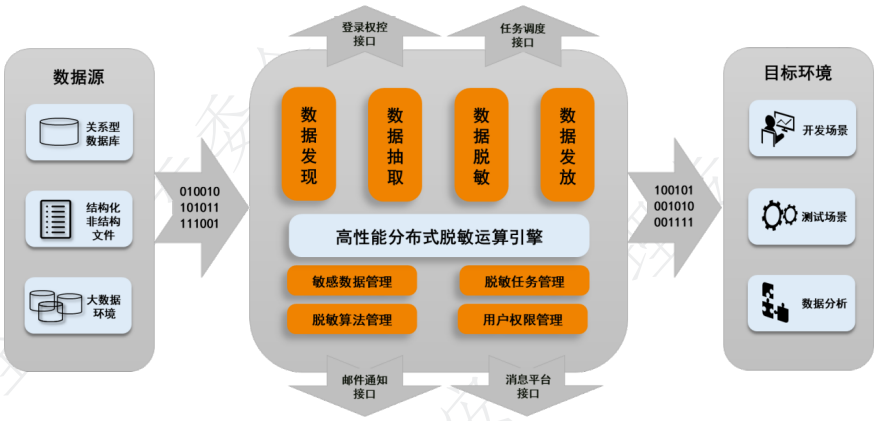


图 B-11　数据静态脱敏框架示意图

B.1.10 数据安全协同平台

如何解决数据流通与数据保护的矛盾，实现“数据不出域，可算不可见”，隐私计算技术兴起，但不管是多方安全计算（MPC）还是联邦机器学习(FL)平台，都只能解决单一的隐私计算问题。多个设备分别部署，各自本地数据无法同时共享，只能通过多次操作才能反复利用。因此，需要隐私计算技术手段和数据安全协同理念相结合，才能真正构建具备安全、合规及生态能力的数据共享、研究、利用及交易的平台。

基于数据安全共享技术的协同生态圈，应该涵盖了从基础资源管理到计算引擎再到数据服务和应用服务的多层架构，具有“高安全、高性能、高兼容”三大优势特性：一是无第三方参与联邦学习(FL)技术，解决多方联合建模中的第三方可信风险问题；二是隐私增强 MPP 引擎，相对于高并发大数据量性能速度优化提升，解决联合建模、多方安全计算中的通信性能问题；三是通过“MPC+FL”的双计算引擎，适配不同计算场景，并在一定标准内支持异构计算框架之间的互联互通。

数据安全协同生态圈的主要架构由数据集市和数据安全发布体系，以及运算资源整合管理与任务调度体系组成。

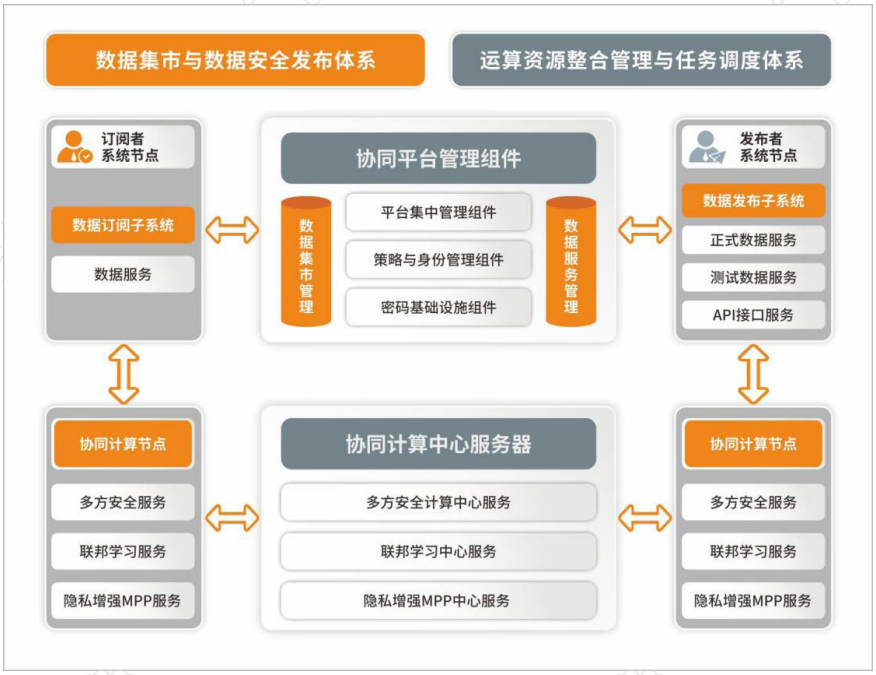


图 B–12　数据安全协同平台架构图

（1）数据集市和数据安全发布体系

数据集市和数据安全发布体系，可以由数据订阅者系统节点和数据发布者系统节点组成，各节点均部署自己的协同计算节点，用于进行多方安全计算、联邦学习计算和隐私增强计算等服务。其中发布者系统节点为该生态系统的数据持有方，负责管理本地用户的登录、数据主题的发布、发布数据和发布服务的维护、计算资源的管理、订阅请求的批准、数据协同任务的批准、数据协同任务的参与、协同结果的存储、本地数据处理过程日志的存储等。订阅者系统节点为该生态系统的数据需求方，负责管理软件负责管理订阅者成员、计算资源管理、数据订阅、数据协同任务申请、数据协同任务的执行监控等。

（2）协同计算节点

数据发布子系统和数据订阅子系统的协同计算节点，依托密码学基础算法库和人工智能算法库组成的计算引擎层，形成多方安全计算服务、联邦学习服务两类隐私计算服务，并通过隐私增强 MPP 服务形成大规模并行处理能力。其中：

●隐私计算引擎

隐私计算引擎由密码学基础算法库和人工智能算法库组成，包含秘密分享、姚式混淆电路、不经意传输、同态加密、多重签名、零知识证明等安全传输协议和数据密码分享方式；人工智能算法库将多种算法的集成适配，组成了联邦学习 FL 引擎、多方安全计算 MPC 引擎、隐私增强 MPP 引擎、去隐私化服务引擎等。

●隐私增强 MPP 服务

大规模并行处理的隐私增强引擎，可用来替代目前的计算节点中对于某些需要实时计算，并且计算任务量庞大、计算任务较复杂的应用场景，如多方安全计算无法解决的运算效率问题。它将任

务并行的分散到多个服务器和节点上，在每个节点上完成计算，大大提高运算效能，突出增强隐私计算优势。

（3）运算资源整合管理与任务调度体系

运算资源整合管理与任务调度体系为平台整体调度管理中心节点，由隐私计算平台管理组件（平台集中管理组件、策略与身份管理组件、密码基础设施组件）和协同计算中心服务器（多方安全计算中心服务、联邦学习中心服务、隐私增强中心服务）组成，负责管理整个平台的成员身份管理，计算资源信息协调和集中分配，日志追踪记录，各节点审批流程和规则制定和下发等。

（4）接口服务能力

可手写表达式自定义函数接口信息，针对接口安全采用公私钥 + 签名 + 证书管理，结合匿踪查询技术，参与方只需传递加密的参数，隐匿查询对象关键信息。可通过 OpenAPI 方式直接自定义算法对接第三方系统。且平台在隐私计算技术中引入分级分类概念，对上传数据自动标识等级、分类，对开放数据进行标准化、精细化管理。

基于数据安全共享技术的隐私计算平台无论在数据价值分享的过程中，还是数据协同过程中，都应为各组织机构数据流通提供安全体验，推进政务、金融、医疗、互联网等机构在联合风控、联合营销、联合分析等场景的数据安全和隐私保护需求，实现数据价值极大释放。以政务数据共享为例，通过隐私计算平台打通政企之间业务屏障，实现数据的安全共享。

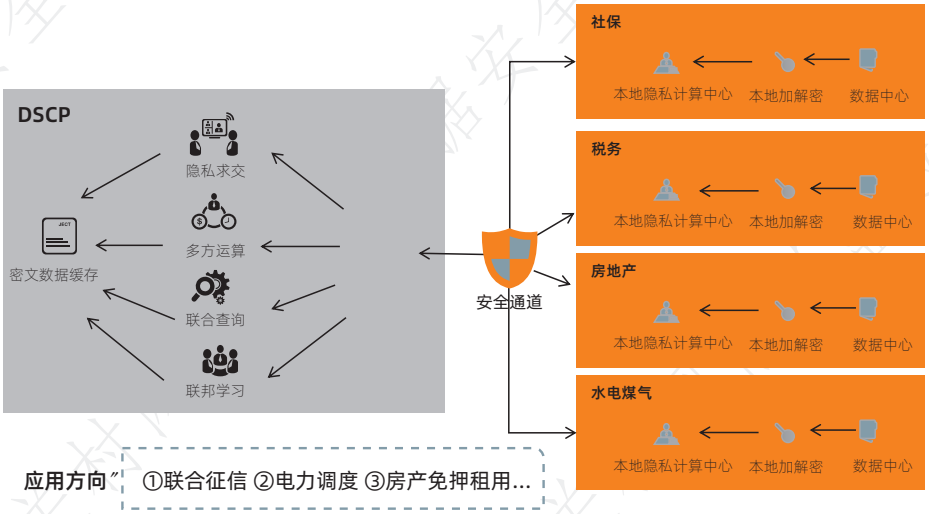


图 B–13　隐私计算应用场景图

整体数据安全共享技术中心服务可部署在政务中心，实现以下管控效果：

（1）国有企事业单位数据可以选择由政务中心数据部门统一管理审批；

（2）明文数据不出所在单位，全程加密传输、缓存和运算，保护数据的安全和隐私；

（3）各行各业综合使用政务服务，提升社会治理水平；

（4）其他机构，如金融机构使用数据，可以注册节点统一使用数据，简化线下申请和审批环节。

利用数据安全共享技术，既可以为政务中心构建全闭环安全体系，也可以形成覆盖事前、事中、事后的闭环安全隐私数据管控的生态系统。

事前防护可根据开放数据的敏感等级灵活设置安全共享策略：基于数据分类分级，对上传数据

自动标识等级、分类，对开放数据进行标准化、精细化管理，保证用户使用的数据统一标准、分类分级、安全可控，提升平台的使用数据质量。

事中监控可实时监测数据开发利用过程中的状态和风险：根据用户实际生产环境需求，多渠道多路径消息通知，对风险进行预警告知和处理，使用户可以根据告警内容准确、快速地做出响应，定位异常行为提升问题解决效率。

事后审计对整个数据流通过程进行全程审计和取证溯源：对用户行为和数据操作行为进行记录、分析和汇总，用来帮助事后生成数据报告、事故追根溯源，结合区块链技术算法上链、内容存证、日志存证等，全面保障和提高数据资产安全。

B.1.11 机密计算平台

机密计算通过 CPU 安全域隔离、完整性保护、虚拟化安全和安全操作系统等技术，为数据提供封闭的的处理环境，保证数据不被窃取、不被破坏。

CPU 安全域隔离是指在服务器 CPU 的不同安全域之间虚拟隔离资源，控制安全资源调配，实现不同业务场景下的安全隔离。隔离技术需要通过对不同安全域之间通信的数据完整校验、数据的安全检查及建立安全连接的方式来实现不同业务通信单元之间有效的安全隔离。

数据完整性保护是指对机密计算数据进行完整性检查和验证，保障数据的完整性，进而保证服务器运行在预期的状态，因此需要 CPU 的安全验证以及轻量级的可信链传递及度量方法，保证度量结果验证的时效性和准确性，实现系统或应用的安全启动和可信启动。

虚拟化安全是指基于虚拟化技术，实现对服务器的虚拟化隔离和安全增强。相较传统云服务器，需要提供低底噪、轻量级的虚拟化框架；需要基于虚拟化框架构建低时延、确定性的 OS 间安全隔离机制和 OS 内安全增强机制；需要增强 hypervisor 本身的安全保护，消减虚拟化攻击窗口。

安全操作系统是指可信应用程序层依赖的安全操作系统，支持额外的硬件安全特性（如 TPM、SGX enclave、TrustZone 等）等。需要提供协同的 OS 恶意代码检测和防范机制、统一的开放端口和 API 安全、应用程序的强安全隔离、可信执行环境的支持等关键技术，在保证操作系统自身的完整性和可信性的基础之上，保证其上运行的各类应用程序和数据的机密性和完整性。

机密计算技术架构一般包括硬件层、系统软件层、服务接口层、应用层和管理层五个层次。该技术通过软件和硬件相结合的方式构建数据保护能力，保证了执行的计算过程可控并且符合预期，消除了数据隐私泄露的风险，从而使用户能够相信计算的结果。

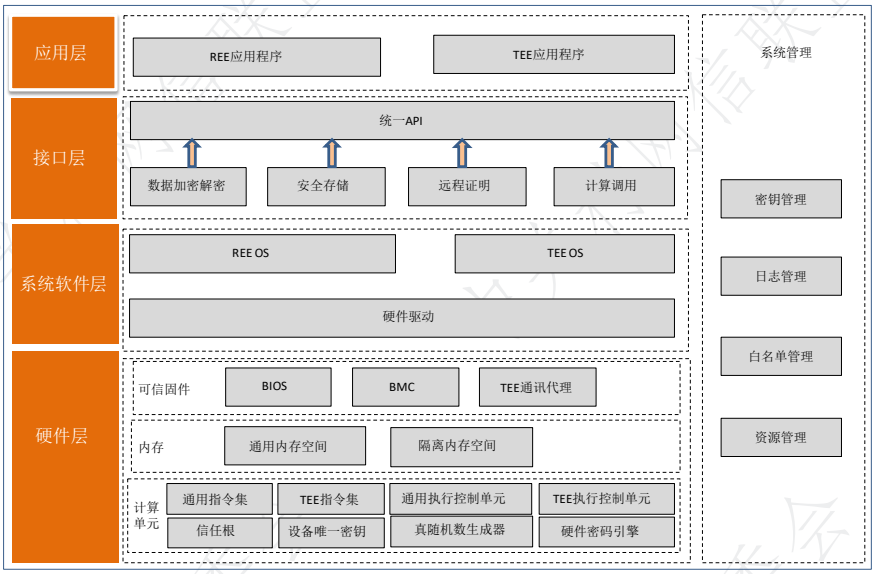


图 B–14　机密计算平台框架示意图

硬件层基于隔离机制实现受保护的资源不被开放系统访问，并提供基于硬件的安全功能，为机密计算提供受信任的硬件基础。

系统软件层为机密计算提供必要的硬件资源能力和基础服务。

接口服务层为上层应用程序提供统一的编程接口及机密计算原子服务接口，以屏蔽底层硬件架构和软件的开发接口差异，为用户调用机密计算服务提供易用性。

应用层直接面向用户的应用程序，用户通过应用程序执行计算操作。

管理层通过跨层交互为机密计算服务提供必要的管理模块，包括密钥管理、日志管理、白名单管理和资源管理，以满足不同业务场景和兼容不同可信架构。

机密计算平台通过结合密钥管理系统（KMS）和分布式部署的机密计算节点，以星形网络方式进行连接，各节点利用安全协议在 KMS 的统一管控下对业务数据执行计算，共同构建具有内生、敏捷、分布式、高效密态计算以及可统一管控特性的密码服务，支撑数据安全可控地流通与计算，实现数据价值的最大化。其架构如下图所示：

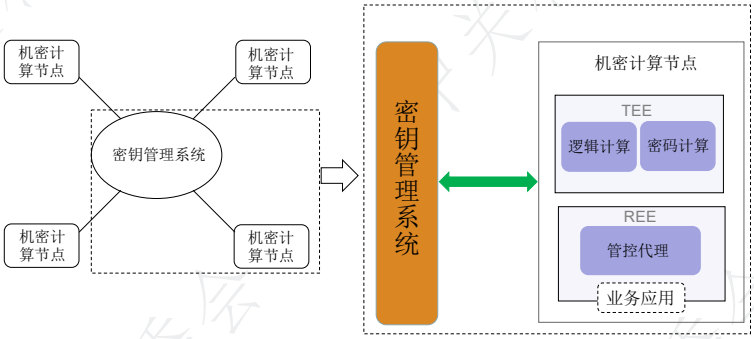


图 B–15　机密计算平台架构

机密计算使得将敏感工作外包到云中成为可能，它甚至引入了新的计算模式。例如，它支持安全和机密多方计算，在这种计算中，相互不信任的用户组可以进行联合计算和共享计算结果，而且不会向彼此或者他人泄露他们的隐私输入信息。机密计算以解决诸多应用场景中“信任”难题，其应用场景十分丰富，例如：

多个不互信组织之间的数据融合与联合分析、区块链上的智能合约的机密性保护、公有云平台对外部或内部攻击的防御、高敏感信息（比如密码学材料、医疗档案等）的安全保护等。

B.1.12 数据水印工具

数据水印工具是在从原始环境向目标环境进行敏感数据交换时，通过一定的方法向数据中植入水印标记，从而使数据具有可识别分发者、分发对象、分发时间、分发目的等因素，同时保留目标环境业务所需的数据特性或内容，当出现数据泄露事件时，可以从植入的数据水印信息中还原上述信息，从而达到追溯泄露途径、追责泄露人员目的的数据安全防护工具。数据水印应具有隐蔽性、可追溯性、确定性等特点，通过数据水印工具可以避免相同类型的数据泄露事件发生。

数据水印工具的主要工具包括定义伪行伪列字段规则、对数据进行字段规则配置、生成数据水印、嵌入数据水印、识别水印类型、解析水印信息、回溯分发内容等。

定义伪行伪列字段规则：根据敏感数据属性含义和数据类型进行定义；敏感数据属性定义会根据数据属性含义和数据类型结合，敏感数据属性往往具有明显的数据特征和数据类型；根据敏感数据属性的类型、值域范围及限定规则，抽象出敏感数据属性的规则，数据值型数据将通过正则表达式方式抽取数据属性规则，字符型属性可通过正则表达式方式或进行值域范围分解抽取数据属性规则。

对数据进行字段规则配置：选择指定的表，根据表中的已有字段属性分布情况，选择采用伪行或伪列方式嵌入水印信息；选择伪行时，对表中已有字段属性进行规则定义，选择字段属性配置对应的伪行字段规则；选择伪列时，直接配置对应的伪列字段规则。

水印数据的生成：据选择的字段规则，进行水印数据的生成；伪行或伪列水印处理根据字段规则配置生成数据行或数据列，生成的数据中对应规则配置的数值型数据按正则表达式构建数据值，并通过随机数值组合生成水印标记信息并嵌入到数据值中；字符型数据按值域范围获取数据字典数据构建数据值，并通过值域数据字典对应的数值编码生成水印标记信息并嵌入到数据值中。

水印数据的嵌入：伪行水印处理时，按照配置的数据行比例因子，在原始数据中按照一定的间隔比例将水印数据分散的插入到原始数据中；伪列水印处理时，对原始数据增加新的字段属性并根据配置生成字段名称，然后将伪列数据插入到对应的字段属性中。

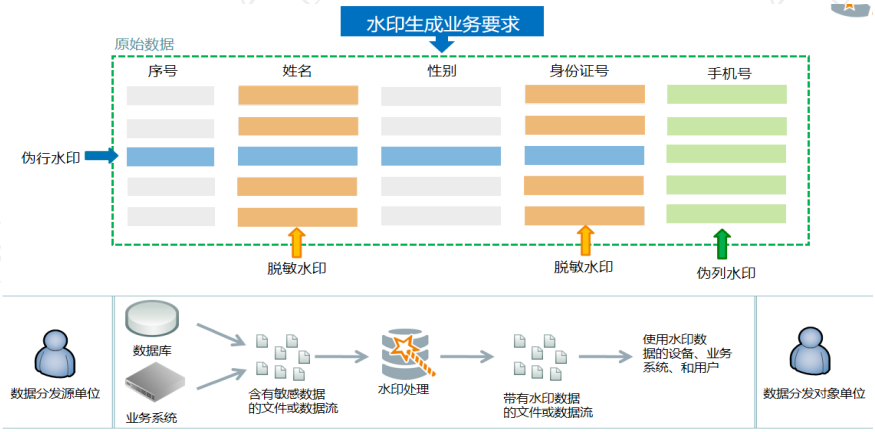


图 B–16　数据水印工具处理示意图

识别水印类型：通过对泄露数据分析，判断其中哪些字段为植入的水印信息的字段。

解析水印信息：通过对植入水印字段的解析，从中获取到水印代码内容。

回溯分发内容：指通过解析出的水印代码，查询映射码表，并获取分发者、被分发者、分发时间、用途的关键信息的步骤。

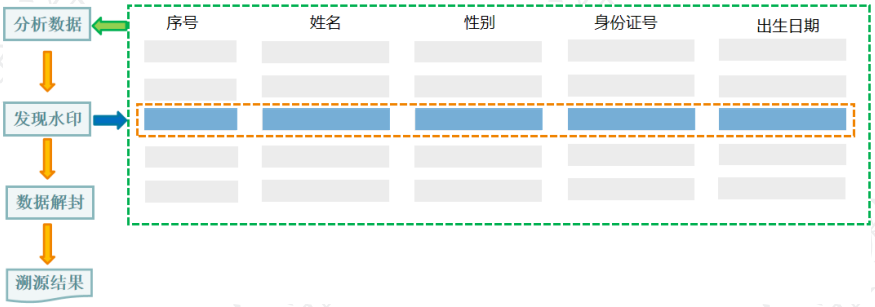


图 B–17　数据水印工具溯源处理示意图

数据水印工具的主要技术包括：伪行水印、伪列水印、脱敏仿真水印。

伪行水印：伪行水印指在对某些外发数据添加水印时，通过添加人为生成的若干整行信息，并从中挑选某些字段植入水印信息的技术。这些筛选的植入水印的字段一般常见于身份证、电话号、银行卡号、交易金额等字段。

伪列水印：伪列水印指通过对分发数据中，人为构造增加一列，并在其中植入水印的机制。

脱敏仿真水印：脱敏仿真水印指在增加行和列的情况下，通过对原始数据中某些字段按照一定的水印植入规则进行脱敏变形，产生的脱敏后数据植入了水印信息的技术。

B.1.13 数据销毁工具

数据销毁系统的主要特征包括：

保证数据彻底清除：在业务关闭或数据已无作用后，计算机或设备中所包含的敏感数据需要被彻底清除，防止被访问和获取。

保证数据无法还原：计算机或设备中被销毁的数据仍可不可以通过任何技术手段进行恢复。

保证销毁流程规范可靠：数据销毁过程和所采用的技术手段是规范的、可靠的。

数据销毁系统的技术主要分为数据介质物理销毁和逻辑销毁两种。

（1）数据介质物理销毁

数据介质销毁目前常用手段为物理消磁，消磁是磁介质被擦除的过程，销毁前硬盘盘面上的磁性颗粒沿磁道方向排列，不同的N/S极连接方向分别代表数据“0”或“1”，对硬盘施加瞬间强磁场，磁性颗粒就会沿场强方向一致排列，变成了清一色的“0”或“1”，失去了数据记录功能。但是消磁的彻底性存在疑问，并且磁场对环境有一定影响，并可能会伤害到操作人员。

其他物理销毁手段还有焚烧、熔炼、刀割盘片、滴盐酸或粉碎处理等。特别是消磁后仍达不到保密要求的磁盘或已损坏需废弃的涉密磁盘，以及曾记载过绝密信息的磁盘，应送专门机构作焚烧、熔炼或粉碎处理。

（2）逻辑销毁技术

逻辑销毁目前常用的方法是数据覆写法，将非保密数据写入以前存有敏感数据的存储位置的过程。

由于硬盘上的数据都是以二进制的“1”和“0”形式存储的，使用预先定义的无意义、无规律的信息反复多次覆盖硬盘上原先存储的数据，就无法知道原先的数据是“1”还是“0”，也就达到了硬盘数据清除的目的。根据数据覆写时的具体顺序，可将其分为逐位覆写、跳位覆写、随机覆写等模式，也可进行组合。覆写的次数与存储介质有关，也与数据敏感性有关，在不了解存储器实际编码方式的情况下，为了尽量增强数据覆写的有效性，需要正确确定覆写次数与覆写数据格式。

另外，值得注意的是，如果在覆写期间发生了错误或坏扇区不能被覆写，或软件本身遭到非授权修改时，处理后的硬盘仍有恢复数据的可能，这样就不能实现数据的彻底销毁。因此覆写技术不适用于存储高密级数据的硬盘，这类硬盘应实施物理损毁，才能保证彻底的硬盘数据擦除，防止敏感数据的流失。

数据销毁的基本流程包括：

（1）建立数据销毁清单，明确数据销毁范围；

（2）建立数据销毁规范或方案，确保以不可逆方式销毁数据及其副本内容；

（3）采取规范或方案中确定的技术手段开展数据销毁工作；

（4）建立数据销毁效果评估和审批制度。

数据销毁系统主要应用于重要或敏感以上数据的销毁处理。一般涉及商业秘密和大量个人信息的数据在使用完毕后，也应当进行销毁处理。

B.2 通用安全防护类

B.2.1 数据资产梳理及分类分级工具

数据安全治理的首要步骤是数据资产识别与数据分类分级，需要对数据的分布、位置、类型、

级别进行摸底梳理，明确保护对象后，在此基础上通过区分不同的访问者身份，制定不同的数据安全防护策略，采用相对应的安全防护技术，做到安全防护有的放矢，确保数据的“用”，“护”结合。

数据资产梳理及分类分级工具通过数据资产发现、数据特征识别、数据图谱分析、数据分类分级策略集生成、主从表自动关联与智能化行业数据分类分级知识库建立等功能，帮助组织识别数据资产，并智能、快速、便捷的实现数据分类分级。

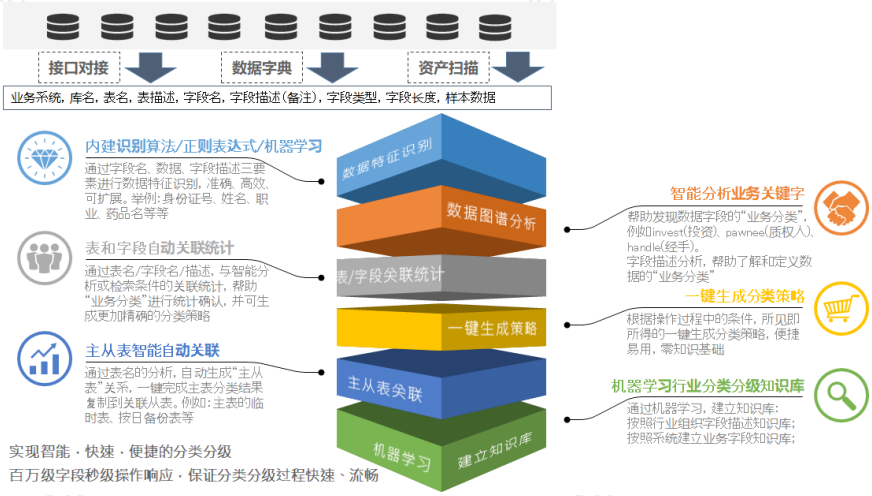


图 B-18　数据资产梳理及分类分级工具关键技术

数据资产发现：通过资产扫描、元数据接口对接、数据字典导入等方式，收集、发现数据资产，其中资产扫描方式是以任务形式对指定网段内的各类数据库进行嗅探，自动发现数据库资产并进行备案，再通过对指定数据库进行扫描，识别库中的表名、表描述、字段名、字段描述、字段类型、字段长度与样本数据；数据字典导入和接口方式可通过文件导入或与元数据系统的接口对接方式获取数据资产。

数据特征识别：对发现的数据资产，面向字段名、字段描述、数据样本三要素，通过敏感数据识别引擎进行自动化的敏感数据特征识别，与数据分类分级模板中明细分类建立映射关系，快速生成数据分类分级策略，完成数据资产分类分级的预处理。

数据图谱分析：针对敏感字段和字段描述，通过运用谓词切分与语义分析技术，帮助了解和定义数据的“业务分类”，进一步通过表和字段自动关联分析，对业务分类关键字进行钻取、分析、统计，帮助对“业务分类”进行统计确认，并与数据分类分级模板中的明细分类建立映射关系，生成更加精确的数据分类分级策略。

数据分类分级策略集生成：围绕数据特征识别与数据图谱分析中对“业务分类”还原操作形成的数据分类分级策略，进行梳理确认，所见即所得的一键形成数据分类分级策略集，并依据策略集中定义的映射规则，对未分类的数据资产进行策略匹配，对符合策略集的数据资产批量、自动化生成数据分类分级标签。

主从表自动关联：通过表名分析，自动形成主表与临时表、备份表等从表的关系，将主表数据分类分级结果自动转移同步到从表相同字段的标签上。

数据分类分级知识库：基于已分类分级的数据资产结果集，将结果中的表名、字段名、字段描述、数据特征等作为向量，进行机器学习建模，并根据知识库模型智能预测大规模数据的分类分级打标，实现数据自动分类分级，输出数据分类分级报告。并通过面向行业或系统的持续模型优化，形成数据分类分级模型知识库，向全自动数据分类分级迈进。

数据资产梳理及分类分级工具的主要技术包括：数据特征自动识别引擎、谓词切分与语义识别技术、知识库与匹配技术、机器建模与匹配技术等。

数据特征自动识别引擎：通过主动发起数据探测行为，对数据源或结构化文件中的数据进行分析，运用字段名、字段描述、内容关键字、正则表达式、自然语言识别等规则匹配，进行数据特征的智能识别，通过该技术，可以判断输入数据的特征是属于个人姓名、身份证号、手机/座机号、职业、地址、纳税人识别号等类型。

谓词切分与语义识别技术：数据分类分级所依托的重要因素，即为数据的业务属性，而数据的业务属性往往存在于字段的命名方式、字段描述或字段备注中，通过对这类数据基于文本上下文进行合理、准确的谓词切分，可以辅助人工进行判断，也为自动匹配数据分类分级规则提供了重要依据。

知识库与匹配技术：对于某个特定行业，其“专业术语”是可被枚举、收集的，在结合谓词拆分的基础上，可以将该行业所涉及的谓词进行充分的归纳记录整理，并按照法规与行业标准，对这些谓词与谓词组合“归属于”哪个数据分类分级结果进行收集统计，将收集统计结果形成行业知识库。当形成知识库后，对于相同命名规范和谓词切分的元数据成果，可以通过知识库自动匹配的机制，直接自动化生成初步数据分类分级结果，在此基础上再结合人工梳理，大幅度提升工作效率。

机器建模与匹配技术：通过引入机器学习，数学建模等技术，采用有监督学习模型，可以更进一步加速数据分类分级效率与自动化程度。对于遵循同样逻辑构造的大量数据，可先对其一小部分采用半自动数据分类分级技术先行处理，经过人工审核后，将这部分数据提交至机器学习引擎进行建模，反复训练达到较高匹配率后，该模型即为此场景下数据分类分级最佳匹配模型，并利用该模型完成后续数据的智能分类分级匹配。

B.2.2 密码基础设施平台

公钥基础设施 PKI（Public Key Infrastructure），是一种基于密码学而建设的基础设施，它能够为数据生命周期防护涉及的身份认证、数据传输、数据存储、数据访问、数据应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系。简单来说，PKI 就是利用公钥理论和技术建立的提供安全服务的基础设施。PKI 技术是信息安全技术的核心，也是电子商务的关键和基础技术。

PKI 公钥基础设施包括密钥管理服务、数字证书服务、时间戳服务。典型的 PKI 系统架构如下图所示：

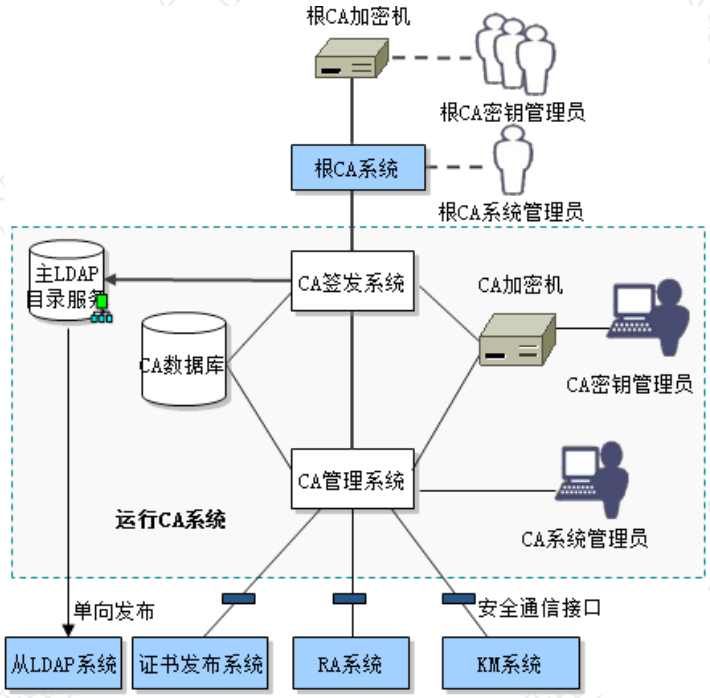


图 B–19　典型 PKI 系统架构

密钥管理服务：密钥管理系统对不同类型的密钥进行全生命周期的管理。包括密钥产生、密钥分发、密钥备份、密钥激活、密钥更新、密钥归档、密钥吊销、密钥销毁等，保证密钥不被非授权的访问、使用、修改和替换，不被非授权修改和替换。能够通过对密钥的管理控制，支撑数据加密和解密，从而实现数据安全防护。

数字证书服务：PKI 的核心是证书认证机构（CA）。CA 通过为各类实体签发数字来实现对身份的鉴别，并进行数字证书的生命周期管理，在认证或签名过程中确保实体身份的可信。具体功能包括：证书生命周期管理、注册审核服务、证书签发存储、证书撤销列表维护、证书在线查询服务和公钥证书下载服务。

时间戳服务：基于国家权威时间源和密码等技术，为信息系统提供精确可信的时间戳，为业务处理的抗抵赖性和可审计性提供有效支持。具体功能包括：时间同步和校准、时间戳签发、时间戳验证。

基于公钥基础设施，能够为为各类业务系统提供各种密码功能。最典型的包括数据加密服务、数字签名服务、身份鉴别服务。数据加密服务通常用于保证数据存储机密性保护、数据传输机密性保护，防止数据泄露；数字签名服务通常用于数据存储和传输完整性保护，防止数据被恶意篡改。

数据加密服务支持对称加密和非对称加密。其中，对称密码算法需要交互双方都拥有相同的密钥，对称加密的加密过程与解密过程使用相同的密钥，即加密和解密两方的密钥是“对称”的。这如同往一个上了锁的箱子里放物品，放入时需要用到钥匙打开，想要取出物品时需要用同样的钥匙开锁。其优势是运算速度快，适合加密大量数据，其劣势是需要安全完成密钥分发。

在使用非对称加密时，每个用户都有自己的一对公钥和私钥，需要跟谁秘密通信，只需用谁的公钥对消息进行加密，具有相应的私钥的人可以解密得到明文，而没有相应的私钥的人无法进行解密。公钥加密的速度一般比对称加密慢，主要用于运算数据的加密，例如，用公钥加密算法建立共享密钥。对称加密的加密过程与解密过程使用相同或容易互相推导得出的密钥，即加密和解密两方的密钥是“对称”的。这如同往一个上了锁的箱子里放物品，放入时需要用到钥匙打开，想要取出物品时需要用同样的钥匙开锁。

非对称密码技术的另外一个应用是数字签名。数字签名采用非对称密码算法和密码杂凑算法，实现数据内容的完整性保护，使各种数据不会被恶意篡改，从而保证的数据的可靠性。依托数字签名，还可以实现基于密码的身份鉴别，保证交互双方身份的真实可信。因此，数字签名功能大量用于保证数据的完整性，包括各类具备法律效率的电子凭据、交易报文。

利用公钥密码基础设施给各类用户签发的数字证书，可以通过证书的验证鉴别用户身份，从而为数据的访问控制提供依据。在实际业务中，大量的信息系统就采用数字证书作为系统登录手段。

近年来，随着量子计算的快速发展，后量子算法（PQC）的研制和应用被提上日程。目前广泛被接受的 PQC 算法包括 Dilithium 数字签名算法、Sphincs+ 数字签名算法、Falcon 数字签名算法以及 Kyber 公钥加密算法。PKI 公钥基础设施和基于 PKI 的各类新型系统向抗量子公钥算法迁移，成为了公钥基础设施以及相关应用所需要考虑的新问题。

B.2.3 数据库审计系统

数据库审计系统是基于数据库议解析和 SQL 解析技术的精准数据库安全审计系统。实现了对数据库访问行为的全面审计审计。可以用于安全合规、用户行为分析、运维监控、风控审计、事件追溯等及数据库安全相关的管理活动。

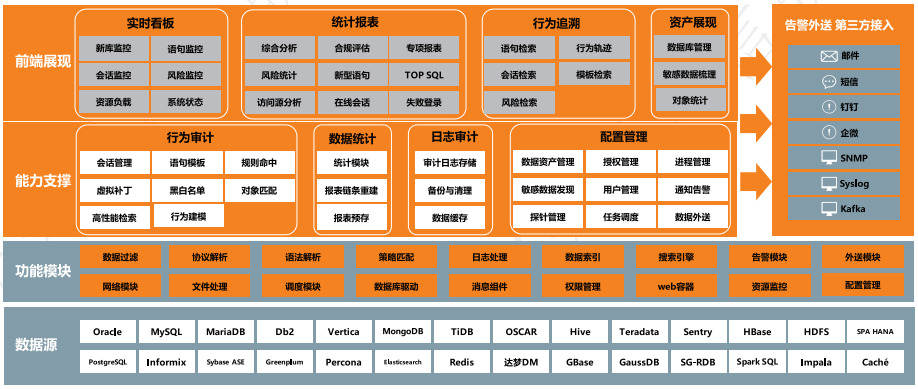


图 B–20　数据库审计系统框架图

数据库审计系统主要功能如下：

行为监测，数据库风险实时感知：针对异常访问登录、权限变更、高危操作、敏感数据访问、批量数据泄露、SQL 注入、数据库的漏洞攻击等访问操作行为进行规则配置。为事后追溯、风险触发奠定坚实基础。

行为建模，构建访问行为体系：在行为建模期，通过对访问操作行为不断学习，对 SQL 语句模板进行归类和完善，从而对数据库行为建模。基于建模语句的波动情况，进行有效的分析和深入的挖掘。

自动发现，自动识别自动审计：从全流量中识别数据库流量，智能分析出数据库信息，形成数据库资产清单，支持自动加入审计列表，全程免人工干预。自动发现网络内未知的数据库信息，在网络环境复杂、数据库资产不清晰情况下明细监管范围，帮助用户识别未登记数据资产。

日志管理，海量日志多态存储：采用在线、备份、外送三种存储机制及高压缩高性能处理技术，实现海量数据差异化存储，满足日志信息保留半年以上的要求。日志在线存储实现数据检索快速响应；日志备份存储支持高压缩比备份海量数据；日志备份后支持远程加密外送至服务器存储。

开放审计，外送数据二次分析：为便于第三方平台接收日志进行二次分析，提供数据对接 Syslog、对接 Kafka 传输的能力。

本地审计，本地访问行为全面审计：可以对本地回环访问和进程间通信访问进行完整，准确审计，实现全量的数据库本地行为记录。

数据库审计系统主要技术如下：

全面审计，信息安全尽在掌控：详细记录多项关键会话信息和语句信息，涵盖客户端信息、数据库信息、对象信息、SQL 语句信息、结果集信息、应身份信息等方面。支持旁路镜像审计、探针式数据采集、虚拟化引流、远程登录行为审计、本地流量采集、等多种来源。全面有效防护批量数据泄露、高危操作、口令攻击、敏感数据窃取、SQL 注入等风险行为。

精确审计，风险追溯坚实基础：区别于传统正则解析技术的局限性，数据库审计系统基于协议分析、完全 SQL 解析、参数化匹配、长语句解析、多语句解析，为审计记录、风险追踪提供了坚实的基础。协议分析和语法解析技术不受执行方式、语句长度及复杂度的影响。即使在超长语句、多层嵌套、多表关联等复杂场景下也不会造成误识别或漏识别。能够精确识别审计元素，准确分析操作类型和对象（存储过程、视图、函数、包、绑定变量），结合规则实现精确告警。

加密审计，加密流量“解密”审计：为满足用户数据使用安全及法律法规，系统针对 Oracle 高级安全加密、SSL、Kerberos 通讯链路加密进行解密审计，并且作为旁路引流审计的第三方产品，不会对加密传输有任何影响。

高性能审计，审计武功唯快不破：基于数据库协议解析能力，超大型审计记录分析运算入库时间小于 30 秒。基于全文检索能力，千亿级别数据规模单条记录查询响应时间小于 10 秒（千亿级数据秒级响应）。多途径实时有效的风险告警，将风险控制在最小范围内，防止风险进一步蔓延。多维度风险关联分析，审计的元素全面，强大的检索能力，使风险发生后能快速、准确定位。

高可靠审计，并发高压效果出色：可靠的审计引擎，保障业务高峰、并发高压下，风险命中依然快速及时、审计数据依然准确全面。系统自我监测和告警能力，监控审计是否丢包、高压下会话、SQL 语句是否超限，帮助用户实时掌握当前压力状况，及时调整或进行扩容。

B.2.4 API 监测系统

API 监测系统基于网络流量通讯协议分析和解析技术，可帮助组织快速梳理业务应用及接口资产。

全面掌握敏感数据使用状况，及时防控敏感数据行为风险，针对数据泄露事件进行有效溯源。

API 监测系统围绕着应用接口自动发现、敏感数据识别、应用账号发现、流式计算引擎及高速匹配引擎等核心功能，能够实现数据资产全面梳理、全面监测和全面可视的监测和审计。

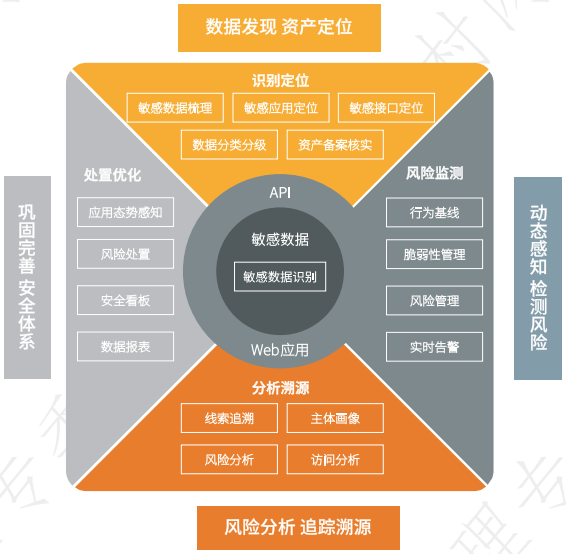


图 B-21　API 监测系统功能架构图

API 监测系统的主要功能如下：

流量解析：支持 HTTP 协议解析，完整还原 HTTP 事件的请求和返回内容；支持解析的内容格式包含：JSON，XML，HTML，JSONP，SOAP 等；支持对文件内容的识别，文件格式包括 xls，xlsx，doc，docx，txt，pdf，csv，zip，rar 等；支持以响应状态码或响应内容关键字过滤流量事件数据，对无效扫描流量进行过滤。

实时监测敏感数据行为：通过对用户环境网络流量的实时分析，实时监测发生的包含敏感数据的行为，并实时分析，对于命中敏感数据泄露风险规则的行为，实时报警；同步记录下所有发生敏感数据的行为，通过可视化敏感数据行为地图和行为画像的方式展示给用户，也为后续弱点分析，事件溯源等功能提供基础明细数据。

敏感数据自动发现：能够按照用户指定的一部分敏感数据规则或预定义的敏感数据特征，对网络流量中的数据进行自动的识别，发现敏感数据，并自动地根据规则对发现的敏感数据推荐最匹配的敏感算法，准确识别出敏感数据内容。

敏感数据分类分级：数据分类是数据保护工作中的一个关键部分，是建立统一、准确、完善的数据架构的基础，是实现集中化、专业化、标准化数据管理的基础。系统帮助用户实现敏感数据分类分级管理，确定数据重要性和敏感度。通过分类分级可以有针对性地采取适当、合理的管理措施和安全防护措施，形成一套科学、规范的数据资产管理与保护机制，从而在保证数据安全的基础上促进数据开放共享。

涉敏接口自动发现：通过对网络流量的分析，以及敏感数据的识别，能够帮用户自动发现用户环境中存在的大量接口里涉及敏感数据的接口，具体能够识别接口的 IP 地址、接口属于哪个应用、接口的功能类型、接口的资源类型、接口产生的敏感数据类型等。帮助用户了解自身环境里所有敏

感接口的分布情况，详细的了解每个涉敏接口的具体指标，帮助用户在解决敏感数据泄露问题时提供针对性接口情况。

接口弱点自动发现：自动发现弱点，对于用户复杂环境下的各种应用，以及每个应用下的大量不同类型的接口进行全面安全脆弱性检测，发现敏感数据泄露安全脆弱性较低的接口。弱点修复建议，针对已发现的弱点情况，基于多年积累的数据安全经验，提供有针对性的弱点修复建议，帮助用户提升应用接口安全程度。弱点统计分析及可视化展示，针对已发现的弱点情况，提供多条件的检索能力及各维度统计分析。包含弱点等级占比、弱点类型分布、弱点规则统计等。

梳理应用及接口资产：资产定位及自动发现，自动发现用户环境分布的应用及接口资产。并根据敏感数据流出的应用和接口，以及用户自身业务特性，对资产进行打标和分类。资产生命周期关注，对于应用和接口资产的状态持续关注。对于状态发生变化的资产，例如发生变更或长时间失活的资产，及时更新资产状态。

风险事件追踪溯源：针对已发生的某个风险事件，分析风险事件的疑似接口、疑似账户、疑似IP，为事件追责缩小范围，并提供原始证据链条。针对需要重点监控人员或重要数据，提供其行为轨迹画像作为定责的重要依据。可以根据多个疑似线索或风险事件，关联分析出共性特征，提供丰富证据素材。

API 监测系统的主要技术如下：

API 接口扫描技术：从镜像流量中进行深度分析，系统采集后，可自动生成 API 列表并且记录 API 的各项基本信息。依照 5W 原则——Who、Where、When、How、What，全面记录对 API 请求情况、请求的各种信息和返回值详细信息。包括请求时间、URL、源 IP、源端口、目的 IP 地址、目的端口、传输协议、访问请求方法、Referer、User-Agent、X-Forwarded-For、Cookie、响应状态码、响应时间等。

敏感数据发现技术：在执行任务过程中，对 API 的返回参数值的数据进行自动敏感识别。敏感扫描过程中，对返回参数中的数据样本采用零存储方案，数据不落地，不存在数据中间泄露风险。

B.3 安全运营平台类

B.3.1 数据安全监测平台

当前数据安全监管领域存在目标不统一、水平不一致、资源未整合等问题，而如何摸清各单位的安全，如何响应国家对关键信息基础设施安全监管的相关要求，深化网络安全监管机制创新，统筹网络空间安全监管防护资源，有效保障关键信息基础设施正常运行和不受侵害，是当前亟待解决的现实问题。

数据安全监测平台可采用“纵向贯通，横向融通”的建设思想，分地域、分行业，纵向贯通各级组织的数据安全态势，横向融通组织内部环境的全链路数据流转信息，实现数据安全综合监管一体化，加强日常监管，从监管角度判断企业数据安全合规情况，从行业角度判断数据安全风险趋势，从地区角度分析区域内数据安全总体态势，从集团公司角度俯视各不同分子公司数据安全态势，从单位内部监测数据全生命周期流转风险，从全局考虑和解决问题。

数据安全监测平台从多个维度抽取数据，并进行关联、分析，形成风险判断和违规告警，并对风险趋势进行预测，向被监管单位发布数据安全风险预警。

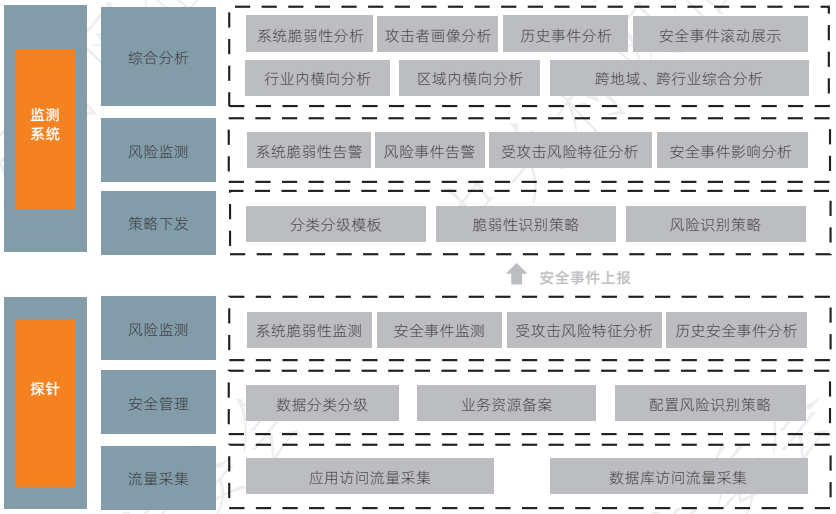


图 B–22　数据安全监测技术架构图

数据安全监测平台采用分布式系统架构设计，包括监测系统和探针。

监测系统向探针下发数据安全策略，及汇总探针上报的安全事件并进行分析，实时掌握被监管单位的数据安全现状，跟踪被监管单位数据安全事件的处置进度，并综合各监管单位的数据安全整体情况，按区域、行业、被监管单位、受攻击数据资产类型、安全事件数量、安全事件类型等条件进行综合分析，预测某一范围内的数据安全风险趋势。探针支持被监管单位按标准、规范进行数据分类分级、数据流转监测、制定数据风险监测策略及安全风险事件集中监测与响应处置。

监测平台涉及的关键技术包括如下几点：

全链路流转刻画：作为数据安全风险监测分析与溯源取证的基础，通过对应用访问流量和数据库访问流量的采集、解析，配合相关的日志信息，关联绘制覆盖数据全生命周期的流转视图。

风险关联分析：风险分析模型运行引擎对数据流转日志进行收集、存储、计算、挖掘和管理，并通过深度学习技术和数据建模技术，识别安全风险。模型引擎高效识别模型算子和数据资源，将算子调度到引擎组件服务中，并通过模型描述文件中描述的属性参数，调用本地数据资源和接口数据资源来运行生成模型结果。

用户行为分析：采用用户行为分析技术从网络流量中识别出数据安全风险，包括涉敏访问、业务数据未脱敏加密监测、超量访问、频次异常、非工作时间违规操作、密码泄露、批量导出等。

漏洞规则库：系统内置丰富的漏洞攻击库，匹配流量中的攻击行为特征，识别数据安全攻击事件。包括：数据库函数、SQL 命令特征、跨站攻击等。

可视化分析技术：通过可视化分析技术，以安全大数据为基础，辅助数据安全决策，从全局视角提升对安全风险的发现识别和响应处置能力。

数据安全监测平台可应用于以下监管场景：

（1）监管单位对所管辖的单位进行数据安全监管；

（2）集团公司对各不同分、子公司进行数据安全监管。

通过探针可实时查看本单位的数据安全整体态势，包括当前正在处置的数据安全事件、历史数据安全事件统计等。

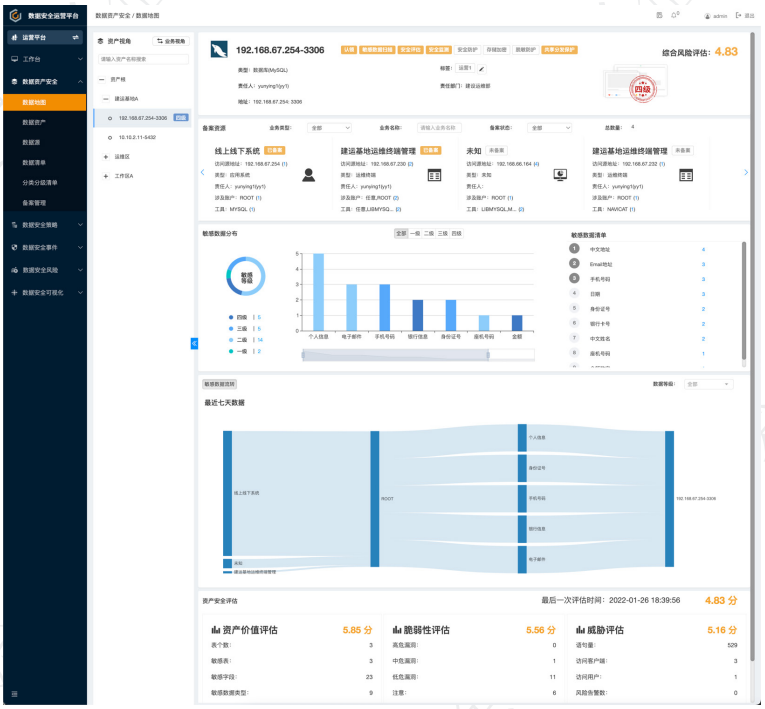


图 B–23　数据安全事件监测

监管单位对被监管单位下达数据安全监管策略，并实时汇聚、分析各被监管单位上报的数据安全事件，全面掌握数据安全整体态势。

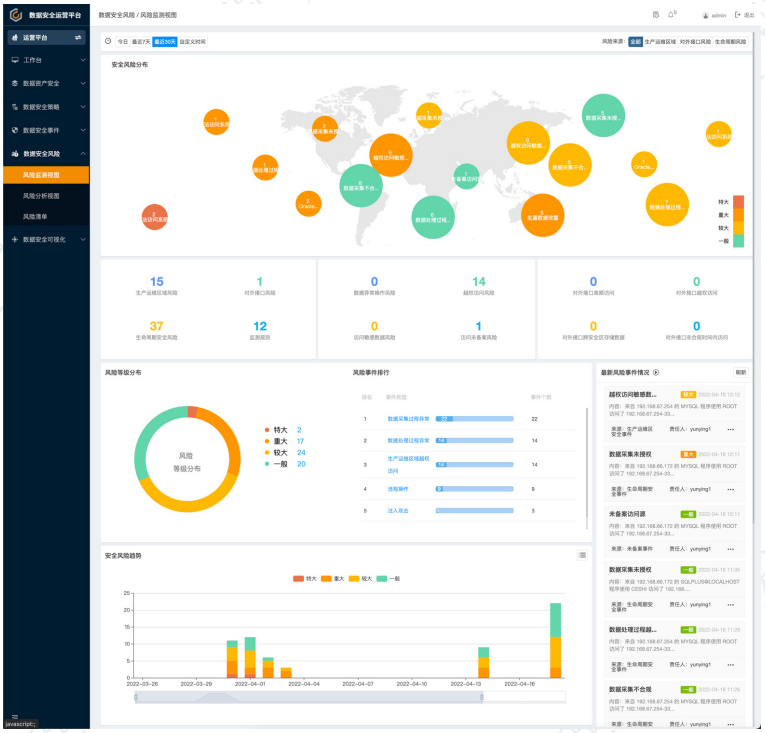


图 B–24　数据安全态势分析图

B.3.2 数据安全运营平台

面对因黑客攻击、内鬼泄密、操作失误、违规使用等导致的数据安全事件及各类隐患、风险、问题，单一化的功能只能解决客户在某个方面的问题和需求，这让不同安全产品间的数据“孤岛”现象凸显，在当前数据的价值利用与安全防护持续并行的需求下，将分散的安全产品能力进行整合，以“平台化、体系化、可视化、实用化”为出发点，提供具备一站式管理和常态化运营能力，对各类数据安全产品进行“统一部署、统一监控、统一管理、统一运营”，将为数据安全运营工作的开展提供有力的支撑。

数据安全运营技术为了满足项目需求建设，分为基础能力层、接口层、监测分析引擎层、安全管理和安全运营五个层次，如下图所示：

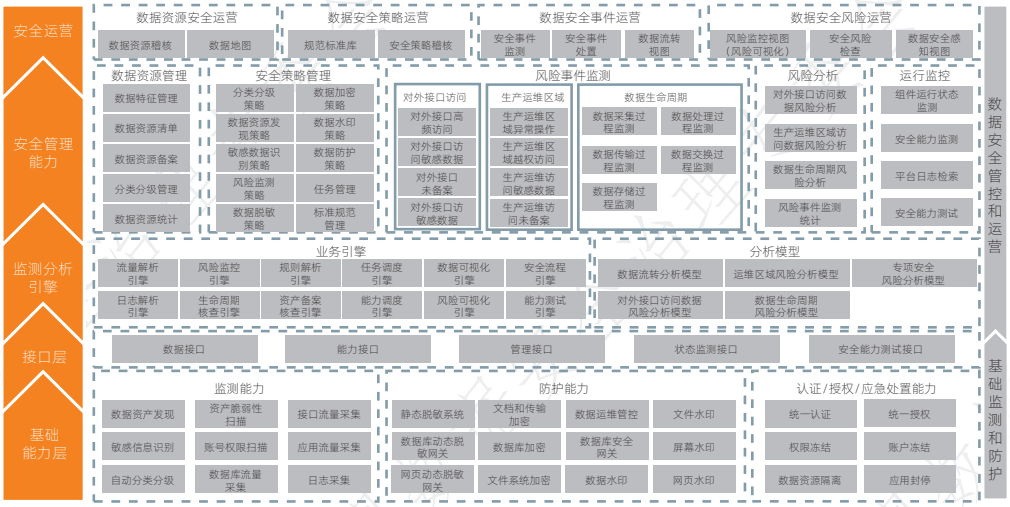


图 B–25　数据安全运营管控技术架构图

在用户可视化层横向分为数据安全运营和数据安全管理两层能力，纵向分为数据资源、数据安全策略、数据安全事件、数据安全风险共四个维度，另包含各组件的运行监控能力。

检测分析引擎层负责控制各类引擎来完成上层应用的各种功能。例如采集状态监控引擎，就是在收集日志后利用引擎做各种业务处理和相关数据分析，获得每个节点上对数据访问行为的状态监控。

接口层主要包含不同业务场景使用的五种接口。例如状态监测接口用于各个采集设备的工作情况，实时监控采集设备是否正常运行。策略配置接口是用于把规则向每台采集设备下放的，用于配置每台设备上对数据监控的策略。

最底层是基础能力层，主要为数据安全监测设备和探针、数据安全防护设备和探针，提供原始数据的输入。

数据安全运营平台主要包括以下核心功能：

数据资源安全运营：针对数据库资产及敏感数据的分布及流转状态进行实时呈现。

（1）数据资产视图

数据资产视图主要为对已注册的数据资产进行统计展现的结果，并进行相应的展现，展现过程

体现为数据资产总数，并根据资产的重要度不同进行分级展现。并可根据数据资产类型分布主要物理位置、逻辑地址作为展示内容，为用户做整体展现。

（2）敏感数据视图

敏感数据分布视图主要是基于敏感数据资产检测结果统计分析得出，采用多种维度、多种图表方式（比例图、趋势图、热度图等）进行展示，其中展示的内容包含敏感数据类型分布、敏感数据量展示、敏感数据属性展示、敏感数据类型分布主要物理位置、逻辑地址展示等。可针对非结构化数据、结构化数据进行独立展现。

（3）数据资产访问热度视图

数据资产热度视图主要是对于使用比较频繁的数据资产进行视图展示。可根据数据资产活跃度进行相应的展示，并提供高热资产视图、低热资产视图以及高热/低热数据资产的详细信息，能够快速了解到当前数据资产的访问频度。

（4）数据资产流向视图

数据资产流向视图用于对于数据资产与账号的访问关系视图。可通过账号访问的时间以及路径对数据资产的调用进行展示，并可根据时间范围进行选择。并建立全局数据资产流向展示，能够对某个数据资产或某个账号使用过的数据路径进行高亮展示，从而快速定位到账号在使用数据的业务流程，当出现异常访问时可给予相应的安全告警。

（5）数据资产账号应用视图

提供数据资产账号管理功能。可针对操作数据资产的账号进行全局管理，包括提供资产账号详表，内容包含账号、准入状态、资产名称、资产类型、来源方式、活跃度等。建立账号行为热图，可针对日常账号访问的频次、时间进行矩阵式排序，从而直观看到账号的使用情况。根据账号使用的基线分析，对于异常账号访问、异常操作访问进行管理，发现数据资产风险，并给予通报。

数据安全策略运营：建设数据安全策略管理中心，实现统一化数据防护策略管理。

（1）安全策略集中设置

集中展示各个数据安全组件状态，对各个数据安全组件涉及的识别类及防护类安全策略进行统一配置，形成安全策略集中管理，针对完成配置的各安全组件的策略，提供策略发布能力，将安全策略发布到相应的安全组件，以实现策略的落地执行。

（2）策略状态统计

能够根据单独的数据安全组件进行已添加策略、已执行策略、已失效策略等多个维度状态展示，并能够根据策略执行的成功率给出业务风险值参考等。

（3）安全策略核查

制定核查策略模板，基于模板，检验、核查数据安全策略设定的完备性及执行效果。

数据安全风险与事件运营：研判数据安全风险，并对安全事件进行响应处置及溯源。

（1）数据安全风险监测类视图

实时监测绘制数据安全风险相关视图，直观可视化呈现安全事件及风险趋势。

●数据安全管控全景图

数据安全管控全景图用于展现数据安全管控节点以及防护手段的逻辑架构图，对于数据安全组

件部署的位置、已执行的数据安全组件策略、已完成的策略结果等进行展现，并能够根据组件的类别进行单独展现。

●数据安全事件视图

数据安全事件视图根据用户环境实际的事件内容直观展现当前环境中出现的数据安全事件的统计结果，包含数据资产事件维度、应用事件维度、账号事件维度，并可根据不同的时间期限进行展示，让客户快速、便捷的看到数据安全事件。

●数据安全风险趋势视图

数据安全风险趋势视图适用于数据安全事件进行分类统计，并以曲线图展示，可根据不同的时间维度进行展示，也可根据不同的事件种类进行选择展示，并根据事件发生区间进行颜色区分，从而快速判断数据安全事件风险。

（2）数据安全事件响应处置与溯源

对各安全组件上报的安全事件按事件等级进行集中呈现，可钻取查看事件详情，并提供与工单、企业即时消息等系统的联动，进行统一告警通知，驱动针对安全事件的响应处置工作。当完成响应处置后，对安全事件记录处理人、处理结果，关闭安全事件，并依据事件典型性，定义处置措施标签集，记入事件处置知识库。针对指定的安全事件，提供事件关联功能，从数据资产流动路径分析角度出发，对安全事件涉及数据资产流转过程进行追踪溯源。

数据安全运营平台涉及的核心关键技术包括：

响应与处置自动化（SOAR）：SOAR 的核心能力包括编排、自动化、安全响应和威胁情报，SOAR 具备对第三方设备 / 系统接口对接能力、策略编排能力以及任务管理能力，支撑安全策略的发布与联动响应，通过预定义的策略形成标准化流程，将安全策略发布到对应安全设备，并对对不同类型的安全事件实现自动化响应。

数据血缘分析：针对数据流转过程中产生并记录的各种信息进行采集、处理和分析，对数据之间的血缘关系进行系统性梳理、关联、并将梳理完成信息进行存储及可视化，通过数据血缘分析，精准刻画数据流转路径，有效支撑流转风险分析与跟踪溯源。

用户异常行为分析（UEBA）：以用户为中心分析用户行为，关联端点、网络和应用及数据操作行为，并将这些数据与威胁情报相关联，通过自动学习正常行为，建立行为基线，来发现异常行为。UEBA 依赖高级安全分析方法实现免配置优化、自动发现异常行为。

数据安全运营平台针对政务、金融、能源、制造业、教育、医疗等行业的数据中心的数据安全运营工作进行全面的承载，将参与数据安全运营各角色的具体工作通过任务流转的方式全部纳入集中管理，形成从法律法规解读、数据库资产梳理、敏感数据发现、数据分类分级、防护策略统一下发、事件监测与处置、到策略稽核与完善的日常化、集中化、规范化、流程化的数据安全运营体系，推进组织数据安全运营各项工作的落地。通过安全运营技术的应用，实现数据安全的集中化管理，形成了数据风险趋势的全面感知，对数据安全事件整体态势做到心中有数，形成了强有力的管理抓手，全面提升组织数据安全管理能力和安全防护能力，保障数据安全稳定的使用和运行，为数据价值的充分挖掘和利用奠定坚实基础。

B.3.3 数据安全评估系统

数据安全风险评估，主要针对数据处理者的数据和数据处理活动进行风险评估，旨在掌握数据安全总体状况，发现存在的数据安全风险和违法违规问题，为进一步健全数据安全管理制度和技术措施，提高数据安全治理能力奠定基础。传统的数据安全风险评估采用现场访谈、问卷调查、现有业务检查的方式开展其检查项并不系统。在实施过程中仍面临以下问题：评估工作内容繁多、交付周期长、评估服务从业人员门槛较高、评估项目经验难以沉淀、评估服务难以标准化开展。

针对上述现状与问题，基于风险评估开展特性梳理标准实施流程，实现评估过程一体化线上统一管理。通过充分自定义的评估调研模板、全面覆盖的评估知识库，结合自动化的技术检测技术工具，智能辅助输出评估报告，实现易管控、更快捷、可沉淀的标准化评估服务工具，极大降低数据安全评估服务资源的投入。

整个数据安全风险评估技术总体架构，基于评估依据，自底向上由评估知识支撑体系层、评估方案层与风险评估过程层构成。

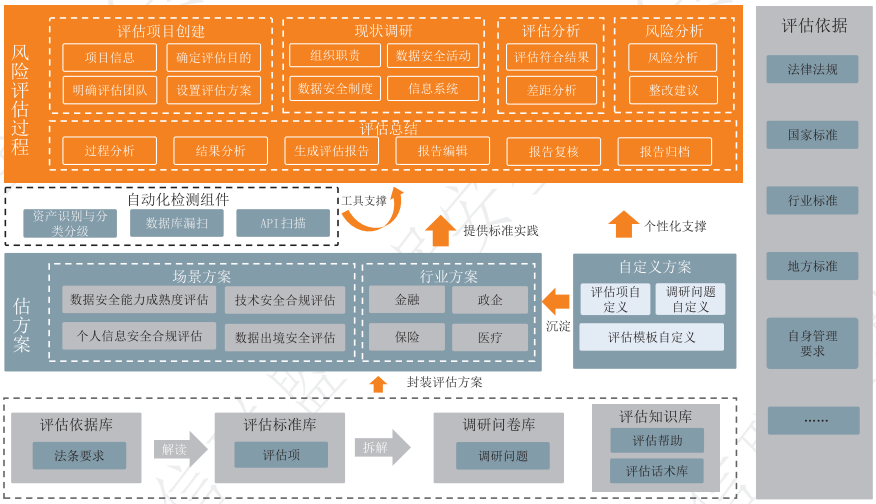


图 B–26　数据风险评估功能架构

在底层构建一套安全风险评估的底层知识支撑体系，首先对相应的合并评估所依据的法律法规、标准及自身规定进行法条要求分解，形成评估依据库，然后对各法条进行解读，生成系列评估项，形成评估标准库，其次，再对各评估项进行拆解，输出调研问题，形成调研问卷库，在各库形成过程中，逐步建立和不断完善评估帮助指引与评估话书库。

在评估方案层，依托底层的评估知识支撑体系，面向各类不同场景、不同行业的合规评估要求，结合个性化自定义方案，封装形成整体结构化的数据安全评估方案。

在上层的风险评估过程层，基于评估方案的标准实践支撑和个性化方案支撑，结合自动化的检测技术组件支撑，实现从评估项目建立、受评单位的现场调研、评估分析、风险评价到评估总结的数据安全评估全过程线上管理。

整体数据安全评估系统的核心功能包括：

评估项目管理：评估项目管理受评单位的基本信息、安全组织情况、数据安全活动、处理业务及业务系统等信息。项目列表可依据项目当前进展状态，快捷进入后续评估流程。同时，提供项目管理、安全评估等多维应用视角，为安全评估提供一种线上协作的高效评估作业模式。

评估方案：面向数据出境、个人信息保护、数据安全能力成熟度以及安全技术措施专项等多样化场景，以及面向金融、政务、医疗、企业等不同行业，依据合规性要求，基于底层的评估知识支撑体系，封装形成内置标准评估方案，标准方案未覆盖的评估场景可以通过自定义评估模板、评估项、调研问题等操作形成自定义方案。评估方案一方面支撑实际评估服务的开展，另一方面在实践评估服务完成后，也可将评估结果提取反馈到评估方案中，不断沉淀、完善评估方案。

评估知识库：建立围绕评估方案中各评估项在评估场景中的帮助指引，方便评估人员准确理解与把握评估项的内涵，构建各评估项涉及的多种评估问题与评估结果的评估话术库，指导评估人员的明确评估目的性、提高语言组织效率。

评估模板：基于国家法律、各地区各行业制度规范及各级标准要求，从数据安全合规评估、数据安全技术评估，数据安全管理评估三个方面解读评估要点并拆解佐证评估要点合规的调研问卷并整理提炼形成体系化的内置调研模板库。

系统中涉及的关键技术主要包括：

违规风险建模与识别技术：通过引入机器学习，风险特征建模等技术手段，对已知的常见的违规风险梳理为风险特征模型库，

知识库自动推荐：通过机器学习记录，基于评估场景、行业、评估要点的符合结果、评估顾问的使用记录等因素。在相似场景推荐引用频率较高的评估知识，并动态提供评估分析示例。可自动推荐机制能够高度个性化地预测评估知识库的引用。

合规性分析技术：在数据内容识别后，利用人工专家加自动研判模型，通过合规性评估，帮助企业识别违规、违法的数据使用行为，从而实现持续的安全运营能力。

文件属性识别技术：基于文件属性对文件进行识别，可识别文件的相似度及文件的 DNA 识别，基于识别结果可依据文件的内容特征快速定位，支持文件内容关键词、文件类型、文件作者等信息快速定位大量的佐证材料。

自动化的技术检测技术

（1）API 接口扫描

基于 http/https 协议解析，通过对 web 应用系统的流量进行旁路（镜像）采集和分析，识别应用及 API 资产及脆弱性，记录对应用系统的操作，可对 web 应用系统中的操作全审计，监视重点账号操作，监视重要业务模块的访问，发现异常操作和越权行为，哪些 API 会访问敏感数据、风险 API 进行标记，做到 API 风险提前预防和管控；同时可对业务系统安全性进行分析，检测常见 web 攻击行为和业务风险。

（2）数据库漏洞扫描

基于检测模块（黑盒检测 – 非授权检测、白盒检测 – 授权检测、渗透检测），通过读取数据库的信息与安全策略进行综合分析，在查出数据库中存在的漏洞后自动给出详细的漏洞描述、漏洞来

源及修复建议、并提供完整的数据库漏洞报告、数据库安全评估报告。用户据此报告对数据库进行漏洞修复，最大限度地保护数据库的安全。

（3）数据调用链扫描

调用链分析可以全面、准确的还原大数据场景下的数据流转关系，满足敏感数据内部流转监控的需求。通过代码插桩或代码注入等方式，实现覆盖主流数据处理组件的调用链监测，包括HTTP服务、数据库、消息系统、RPC服务等典型数据调用场景。

面向多样的评估场景，如“数据安全能力成熟度评估”、“个人信息安全合规评估”、“技术安全合规评估”、“数据出境安全评估”及各行业及自定义场景等，针对被评估单位的实际环境，充分运用数据安全风险评估系统，基于场景化的评估方案模板库，自动化的解读法条形成评估项，运用评估知识库，生成评估调研问卷，通过调研、访谈结合使用自动化检测技术工具，落实数据安全合规评估分析，发现数据安全治理差距，给出整改建议并智能输出数据安全评估报告，对组织自评估和第三方评估服务工作起到有效的自动化支撑作用。

C.2022 年以来重大数据安全事件归类分析

C.1 勒索软件持续带来数据安全威胁

勒索软件又称勒索病毒，是一种特殊的恶意软件，通过加密来阻止用户访问其文件、应用程序或系统，最终会要求用户缴纳赎金以取回对电脑的控制权。现在的勒索软件复杂且具有较强的侵入性，一旦被下载激活，它们可以迅速传播到整个组织中，使用户丧失使用能力并破坏整个业务的运营。

台达电子遭受 Conti 勒索病毒攻击：我国台湾地区电子产品制造公司台达电子 (Delta Electronics) 是电源组件供应商，生产的产品包括嵌入式电源、冷却风扇、电磁干扰滤波器和螺线管。其他产品包括电动汽车充电器、工业自动化解决方案和数据中心基础设施。2022 年 1 月 21 日，台达电子发布声明称，其受到一起勒索软件攻击，与 Conti 勒索软件团伙有关。虽然台达电子方面表示，公司已在第一时间发现了攻击，其安全团队进行了干预，对受感染系统采取措施，并开始恢复运营。但据知情人士透露，这次攻击实际情形非常严峻——台达电子 1500 多台服务器和 12000 多台计算机已被攻击者加密。台达电子未能及时恢复大部分系统，导致其官方网站长时间处于瘫痪状态，该公司只能使用一台替代的 Web 服务器与客户保持联系。据说 Conti 团伙要求台达电子支付 1500 万美元的赎金，为此，台达电子还与 Conti 勒索软件团伙就可能的付款进行了谈判，以换取密码并承诺数据不会遭到泄露。

哥斯达黎加遭到 Conti 勒索软件攻击：哥斯达黎加政府因勒索攻击宣布进入“国家紧急状态”，该事件是 2022 年最受关注的勒索攻击事件，针对该国的第一波勒索软件攻击始于 4 月初，勒索攻击致使其国家财政部陷入瘫痪，不仅影响了政府服务，还影响了从事进出口的私营部门。勒索软件组织 Conti 声称对此轮攻击负责，并要求哥斯达黎加政府支付 1000 万美元的赎金，后来这一金额又增加到 2000 万美元。5 月 31 日开始，另一波攻击使该国的医疗保健系统陷入混乱。这次与 HIVE 相关的攻击致使该国的医疗保健系统被非正常下线，直接影响了普通民众的生活。

非洲最大连锁超市遭勒索团伙敲诈，600GB 数据失窃：Shoprite 是非洲最大的连锁超市，业务遍布尼日利亚、加纳、马达加斯加、莫桑比克、纳米比亚、刚果民主共和国、安哥拉等国家，收入为 58 亿美元，拥有 149000 名员工。该公司在南非拥有 2943 家门店，为数百万客户提供服务。6 月 10 日，一场突如其来的勒索软件攻击令 Shoprite 猝不及防。事发后 Shoprite 并向斯威士兰、纳米比亚及赞比亚的客户发出警告，表示他们的个人信息可能因此受到损害。该公司在声明中表示，“我们已经修改身份验证流程、欺诈预防与检测策略来保护客户数据，并实施了额外的安全措施，以防止数据进一步丢失。对受影响网络区域的访问已被锁定。此次泄露的数据包括个人姓名和身份证号码，但不涉及财务信息或银行账号。”6 月 14 日，勒索软件团伙 RansomHouse 声称对此次攻击负责，并发布了一份据称从 Shoprite 窃取到的 600GB 数据的样本。而恶意攻击者称，受害者遇袭的主要原因是安全建设太差、保护不够充分。Shoprite 也不例外，该团伙在 Telegram 中嘲讽了这家零售商的安全习惯（比如用明文文本和原始图片保存大量个人数据）。

蔚来遭遇数据泄露，被勒索 225 万美元等额比特币：2022 年 12 月 20 日，网络上有人称破解了蔚来大量数据，包括蔚来内部员工数据 22800 条、车主用户身份证数据 399000 条。随后，蔚来官方

发布《关于数据安全事件的声明》，称 2022 年 12 月 11 日，蔚来公司收到外部邮件，声称拥有蔚来内部数据，并以泄露数据勒索 225 万美元等额比特币。在收到勒索邮件后，公司当天即成立专项小组进行调查与应对，并第一时间向有关监管部门报告此事件。经初步调查，被窃取数据为 2021 年 8 月之前的部分用户基本信息和车辆销售信息。

勒索软件攻击，是一个看似老生常谈却依然让全球企业为之惶恐的话题。随着勒索攻击体系的日益完善，有更多的人参与到勒索攻击中，勒索攻击造成的损失和后果不可估量，因此防范勒索攻击的重点在事前防御环节而非遭受攻击后的解密环节。用户应注意日常防范措施，针对重要的文档和数据，一定要定期做好数据备份；提高安全运维人员的职业素养，定期进行木马病毒查杀；提高人员安全意识，不点击来源不明的邮件、网站，不安装来源不明的软件，不插拔来历不明的存储介质等。而一旦中招，最佳方法不是屈服于勒索软件的要求，而是从备份中恢复系统和数据，并向执法和数据保护机构发出事件警报。其余的挣扎都是徒劳的，你的无能为力只会让勒索软件参与者变得越来越多，并且为他们提供勒索动力。

C.2 供应链攻击造成的数据泄露

许多公司花费时间和金钱来保护外围和内部系统，但很少关注第三方——包括供应商、合作伙伴、承包商和服务提供商的网络安全，网络供应链攻击因此趁虚而入。供应链攻击指的是对于供应链所发动的网络攻击。攻击者会将供应链作为攻击对象，先攻击供应链中安全防护相对薄弱的企业，再利用供应链之间的相互连接，如软件供应、开源应用等，将风险扩大至上下游企业，产生攻击涟漪效应和巨大的破坏性。供应链攻击的手段包括：利用第三方应用程序、利用开放源代码库中包含的漏洞等等。供应链攻击往往牵涉到更多的企业，且更具破坏性，甚至会给整个行业带来巨大的影响。

世界经济论坛最近发布的《2023 年全球网络安全展望》指出，供应链安全将是未来的重要挑战。近年来，针对软件供应链的安全攻击事件一直呈快速增长态势，造成的危害也越来越严重。

身份验证服务主要提供商 Okta 的网络遭到知名数据勒索组织 Lapsus$ 的攻击：当时表示，他们的目标并不是从供应商那里窃取数据，而是通过利用对 Okta 的访问权来攻击其客户。Lapsus$ 集团通过第三方分包商 Sitel 获得了对公司网络的访问权限，并且能够查看 Okta 的客户公司内部网络并执行管理操作。黑客的攻击行为发生在 2022 年 1 月 16 日至 21 日，并于 3 月下旬公开披露。Okta 表示有 366 家公司客户（约占 Okta 客户的 2.5%）受到安全漏洞的影响。

Comm100 聊天服务商在供应链攻击中被劫持传播恶意软件：总部位于加拿大的商业聊天提供商 Comm100 表示其在 51 个国家 / 地区拥有 15,000 名客户，遭到网络攻击，恶意攻击者破坏了供应商的基础设施并劫持了 Comm100 的实时聊天软件的安装程序。攻击者将安装程序修改为后门程序，得以部署其他恶意软件。此次攻击时间从 2022 年 9 月 27 日持续到 9 月 29 日上午，影响了北美和欧洲的工业、医疗保健、技术、制造、保险和电信行业的公司，有多少受害者在此次攻击中受到影响仍不得而知。

黑客入侵 Magento 供应链攻击软件供应商：由提供 Magento-WordPress 集成软件的公司 FishPig 开发的多个扩展在 8 月发生的供应链攻击中感染了恶意软件。攻击者破坏了供应商的基础设施，并

注入了恶意代码，将 Recoobe 恶意软件安装到 FishPig Magento Security Suite 和 FishPig WordPress Multisite 软件中，从而访问使用 FishPig 产品的网站。这次攻击影响了付费的 Fishpig 扩展，托管在 GitHub 上的免费扩展没有受到影响。

这些典型的供应链攻击案例对于企业带来的影响具有不可预测风险，企业现在需要准备更多，才能一定程度地避免供应链安全的复杂挑战。这对大型生产制造业尤为重要，比如企业将 IT 运维承包给第三方机构，还有涉及庞大供应链当中的任何一环。除了建立供应链安全审查机制，更要以安全合约为抓手，建立安全责任制，强化外部的安全风险管理，从合同签订之前到合同执行过程中一直到合同完成之后整个生命周期，并且在数字化环境下，需要得到领导充分的重视和支持，经多个业务和职能部门的协同来完成，过程更需要科学的方法。

C.3 云上存储的数据泄露

近年来，云计算技术得到了迅速发展和广泛应用，云计算服务具有高性价比、高灵活性、动态可扩展、专业安全服务保障等特点，有效助力了提升管理效率、节约成本、增强综合安全防护能力。与此同时，云计算服务也面临诸多挑战，如云计算技术基础平台安全性、云上数据的安全管理等安全风险问题，导致云平台数据安全事件层出不穷。

云存储平台，如谷歌 Drive、Dropbox 和 OneDrive，通常被用作硬件存储选项的替代方案，因为它们更方便。更重要的是，用户可以在任何时候使用登录详细信息访问云存储，这意味着用户不必依赖于单个设备来查看和使用数据。但是云存储平台很容易受到远程攻击，因为它们依赖软件来运行。虽然云存储提供商使用各种安全层来保护用户数据，但它们仍然是网络犯罪分子的主要目标。毕竟，任何有互联网连接的平台都有被黑客攻击的风险，云存储服务也不例外。

云存储公司 Dropbox 的源代码和个人信息被盗：2022 年 11 月 1 日，Dropbox 公司披露称数据遭泄露，恶意人员获得对员工和客户某些源代码和个人信息的访问权限。Dropbox 说明，该公司使用 GitHub 来托管公开与私有存储库，也通过 CircleCI 进行内部部署，10 月初便有许多员工收到伪装成 CircleCI 的网络钓鱼邮件，虽然该公司的系统会自动过滤可疑邮件，但仍有些网络钓鱼邮件进入员工信箱，这些邮件要求 Dropbox 员工访问一个伪造的 CircleCI 登录页面，以输入他们的 GitHub 用户名及密码，之后再要员工把硬件身份认证密钥所产生的一次性密码输入该恶意网页。据了解，黑客在取得员工的登录凭证之后，访问了该公司存放在 GitHub 上的 130 个存储库。遭暴露的源代码中包含开发人员使用的某些凭据。另外，被暴露的文件中还包括 Dropbox 员工、之前和当前客户、厂商和销售主管的“数千个”姓名和邮件地址。

微软或因云服务器配置错误暴露数万用户敏感信息：微软安全响应中心在当地时间 2022 年 10 月 20 日发布公告称：由于一台云服务器配置不当，导致某些客户的敏感信息遭暴露。在获悉该事件后，公司已经第一时间加固了相关服务器安全。微软表示，遭暴露的信息包括客户姓名、邮件地址、邮件内容、公司名称和电话号码等，而这些信息与受影响客户以及微软合作伙伴之间的业务存在关联性。这次数据暴露事故是因“维护人员对服务器的无意配置错误造成的，而非因安全漏洞引发，该端点设备也并未在微软生态中正式使用”。这起事件首先由安全公司 SOCRadar 发现并通过博客文

章发布。SOCRadar 指出：2022 年 9 月 24 日，该公司研发的内置云安全模块检测到，微软公司一个配置不当的 Azure Blob Storage 服务器中包含大约 2.4T 属于高级别云提供商的敏感数据。并称这些敏感信息可能与全球 111 个国家（地区）的超过 6.5 万个企业客户关联在一起，时间跨度从 2017 年起到 2022 年 8 月。一旦有黑客团伙访问了该服务器，就可利用相关信息，实施勒索、欺诈或在暗网出售等违法活动。

服务器配置不当已成为导致数据泄露的最常见的云安全问题之一。此次微软数据泄露就发生在 Azure Blob Storage 存储服务上，这种云端设备的配置漂移现象在现实中非常常见。它可能是由于某些用户拥有了过多特权，或者不具备专业的安全配置外部访问知识所引发。因此服务器的安全加固是必不可少的，比如限制连续密码错误的登录次数，是对抗密码暴力破解的重要手段，删除不需要的账户可以避免被攻击者利用，对权限进行合理的配置，关闭不需要的服务端口等，从而提升服务器的安全保护等级。

C.4 爬虫技术滥用非法获取数据

数据“爬虫”，是一种可以进行自动化访问并收集目标计算机信息系统数据的程序，设计初衷是为编纂网络搜索引擎，通过数据“爬虫”更新自身的网站内容或对其他网站进行索引。随着数字经济的快速发展与网络信息技术的普及应用，数据“爬虫”凭借着高效、可定制化、适用性等特点，已经成为当下运用最为广泛的技术方式之一。但随着互联网技术的发展，爬虫已经开始不守规矩了，经常肆意爬取网站私密数据，与此相关的各种热点事件层出不穷，反映了数字时代与数据流转利用和数据治理生态相关的诸多深层次问题。

某公司利用爬虫技术窃取 2.1 亿条简历数据：2022 年 2 月 8 日，北京某科技公司、王某某等人涉嫌侵犯公民个人信息罪，被告单位被判处罚金人民币 4000 万元，王某某被判处有期徒刑 7 年、罚金人民币 1000 万元。2015 年至 2019 年该公司组建专门爬虫技术团队，在未取得求职者和平台直接授权的情况下，秘密爬取国内主流招聘平台上的求职者简历数据，获取 2.1 亿余条个人信息。本案对被告单位判处的罚金数额、对被告人判处的刑期和罚金数额，均系近年来全国同类案件判罚最重案例。

首例短视频平台领域网络“爬虫”案件：2022 年 5 月 10 日，江苏省无锡市梁溪区人民法院以提供侵入计算机信息系统程序罪判处被告人丁某有期徒刑一年六个月，缓刑两年，并处罚金三万元。据悉，该案系全国首例短视频平台领域网络“爬虫”案件。

某快递公司利用爬虫窃取并售卖用户敏感信息：2022 年，国内某快递公司云仓电商仓库，被黑产团伙以应聘工作为由虚假入职，通过在其使用的工作电脑或面单打印机电脑上安装木马软件，对用户敏感信息数据进行窃取，并在数据交易市场上以单价 3 元进行售卖。

《网络数据安全管理条例（征求意见稿）》第十七条规定“数据处理者在采用自动化工具访问、收集数据时，应当评估对网络服务的性能、功能带来的影响，不得干扰网络服务的正常功能。自动化工具访问、收集数据违反法律、行政法规或者行业自律公约、影响网络服务正常功能，或者侵犯他人知识产权等合法权益的，数据处理者应当停止访问、收集数据行为并采取相应补救措施。”

一方面，相关部门应加大对平台的监管力度，另一方面，平台自身也应通过限制访问次数、提高人机识别技术等方法，有效拦截、识别恶意爬虫行为，从而加强对平台的安全防护，部署自动化安全防御工具，监测恶意行为，对未知的安全风险预警。对平台存储的敏感数据进行加密、脱敏处理或者前端页面加密展示，防止数据泄露对个人造成的严重威胁。

针对爬虫技术获取数据的手段，企业还需要定期组织各业务部门、技术部门等开展检查和评估，评估的内容包括：拟抓取的数据类型、数量、频次；拟抓取对象网站性质、类型；拟抓取对象网站是否具备 Robots 协议或反爬措施等。企业应当提前设置抓取内容的限制策略，注意审查抓取内容，避免因抓取个人信息、商业秘密等而构成违法犯罪。已经抓取的，则应当及时停止抓取行为并进行删除。

C.5 黑客入侵造成数据泄露

近年来，黑客组织出于政治、名誉甚至是利益的目的，纷纷精心策划各种形式的网络入侵计划，多数攻击活动具有极强的隐蔽性和针对性，通常会运用受感染的各种介质、供应链和社会工程学等多种手段实施先进的、持久的且有效的威胁和攻击，从医疗信息、账户凭证、个人信息、企业电子邮件到企业内部敏感数据等等，不一而足。

红十字会总部服务器遭不明黑客入侵：2022 年 1 月 19 日，总部设在日内瓦的红十字国际委员会对外称，存储该机构数据的服务器日前遭到不明来源的黑客侵入，来自世界各地至少 60 个“红十字会”和“红新月会”的 51.5 万份个人信息被窃，其中包括因冲突、迁移和灾难而同家人分离的人员、失踪人员和被拘禁人员的信息。

纽约市教育局数据泄露：2022 年 3 月 26 日，纽约市教育部证实 82 万学生的私人数据遭到黑客攻击。该漏洞源于对该市教育部门使用的软件 Illuminate Education 的攻击。黑客成功地获得了一系列学生的私人信息，包括姓名和生日。虽然违规事件发生在 1 月份，但教育部直到 3 月底才被告知暴露的学生数据。Illuminate 的声誉不仅受到了打击，近百万学生的家庭也可能面临持久的影响。

Uber 数据泄露：2022 年 9 月 15 日，全球最大共享汽车公司优步科技被一名 18 岁的年轻黑客入侵。黑客从暗网上购买了一名员工被盗的凭证，并将大量多因素身份验证（MFA）请求和虚假 IT 消息推送给这个员工，希望进入他的帐户。该员工被不间断的弹出窗口激怒，屈服并批准了请求，无意中引发了网络攻击，黑客利用特权帐户访问 Uber 的关键信息。

香港 3 家香格里拉酒店 29 万客户信息泄露：2022 年 10 月初，据香港媒体报道，香格里拉酒店集团的网络系统受到黑客攻击，其中 3 家位于中国香港，造成香港酒店 29 万个人资料泄露。香港安全专家表示：通过技术分析，黑客可能通过传送电邮，在超链接中加入“钓鱼程式”，窃取酒店系统内的资料。

台湾省 2300 万公民信息泄露：2022 年 11 月初，据台媒报道，台湾省政府系统遭黑客入侵，黑客在国外论坛公开出售 2300 万中国台湾民众数据，打包价 5000 万美元。

国内医疗机构 10 万条数据遭窃取：2022 年 10 月，经国内网警侦破，麻某利用自身黑客技术，在 2022 年 4 月侵入国内某医疗机构微信公众号系统窃取数据，半年多时间非法获取该计算机系统数

据 10 万余条，而后在境外黑客论坛兜售，非法获利 1500 美元。

西北工业大学邮件系统遭境外组织入侵：2022 年 6 月，西北工业大学发布《公开声明》称，西北工业大学电子邮件系统遭受网络攻击，有来自境外的黑客组织和不法分子向该校师生发送包含木马程序的钓鱼邮件，企图窃取相关师生邮件数据和公民个人信息。西安市公安机关对此高度重视，立即组织警力与网络安全技术专家成立联合专案组对此案进行立案侦查，初步判明相关攻击活动源自美国国家安全局下属的“特定入侵行动办公室”。本次调查还发现，在近年里，美国国家安全局下属的“特定入侵行动办公室”对中国国内的网络目标实施了上万次的恶意网络攻击，控制了数以万计的网络设备，包括：网络服务器、上网终端、网络交换机、电话交换机、路由器、防火墙等，窃取了超过 140GB 的高价值数据。

网络攻击者通过破译口令、IP 欺骗、DNS 欺骗等非法方式获得非法权限对被攻击的主机进行非授权操作，其手段多样、手法隐蔽，给用户造成巨大的经济损失，威胁社会和国家安全。因此，组织的数据安全管理面临着更高的要求和挑战，必须建立严格的安全保障体系，加强对数据访问权限的管控，对敏感数据进行加密处理，在网络中层层设防，让攻击者无缝可钻，无计可施。

C.6 内部员工泄露和删除数据

安全专家统计表明，组织在遭遇数据泄露事件时，有百分之八十的概率是出现在内部人员身上。内部人员利用合法获得的访问权对信息系统中的数据的机密性、完整性以及可用性造成负面影响，包括恶意的和非恶意行为。产生威胁的内部人员包括管理人员、管理员以及普通职员，包括离职人员泄露数据、为泄私愤删除数据、员工安全意识淡薄泄露数据等类型。

百度员工为发泄不满，刻意删改公司数据库被判刑：2022 年 6 月 8 日，根据北京法院审判网公布信息显示，百度一程序员为发泄对上司的不满，将公司数据库删改后被抓，判刑 9 个月。2020 年 8 月至 9 月，员工金某因对公司项目安排不满，将数据库的数据部分进行了篡改和删除，导致系统算法无法得出想要的结果，该行为严重影响了其部门工作的正常运转。同时，据公司同事证实，金某在商业质量效能部任职期间，由于对部门领导不满，使用隧道违规从外网接入百度 IDC 并对商业质量效能部 ff.baidu-int.com 平台数据库内表进行清空、篡改、锁定，造成严重后果。金某的行为一方面导致平台数据不一致或丢失，共计影响了五十多个项目使用平台的快捷操作能力；另一方面，数据库的异常变化也给用户带来了不良体验，对公司形象及经济利益造成了恶劣影响。

日本兵库县尼崎市丢失存 46 万市民信息 U 盘：2022 年 6 月 23 日，日本兵库县尼崎市称，存有该市 46 万余人个人信息的 U 盘于日前丢失。其中包含所有市民的姓名、住址、出生年月及纳税金额等。据悉，U 盘的丢失与和该市有合作关系的企业有关。该企业工作人员未经允许，擅自将市民信息复制至 U 盘进行数据移交，移交工作结束后并未删除数据，反而带着 U 盘去餐厅喝酒，随后将装有 U 盘的包丢失。

员工利用职务之便泄露客户信息被处罚：2022 年 11 月底，据公开的裁判文书显示，平安人寿六盘水中心公司内部人员利用职务之便泄露客户信息被处罚，多名涉事人员判处有期徒刑。涉案的公民信息高达 4 万余条。检察机关办案发现，有不少行业“内鬼”泄露个人信息，涉及通信、银行、

保险、房产、酒店、物业、物流等多个行业。

虽然组织将大量资源集中用于应对缓解外部威胁行为者，但内部风险可能对组织构成更大的威胁。组织内部的员工引起的数据安全事件，是所有事件中代价最高昂且最难检测到的事件。内部人员相比外部攻击者有显著的“优势”，他们不仅熟悉组织的政策、程序和技术，而且对内部的弱点了如指掌。恶意内部人员甚至可能是安全设备的策略配置者，因此内部威胁相对于外部威胁，检测极其困难，他们可以在实施恶意行为时规避相应的检测机制，事后删除日志以逃避追溯。组织除了对员工进行技术和制度制约，定期进行保密培训，提高员工的保密意识也尤为重要。

C.7 系统配置不当造成数据泄露

应用系统由于配置不当，没有考虑相关的安全隐患，造成相关的配置文件泄露。攻击者通过配置信息泄露获取敏感数据，为进一步攻击创造条件，设置通过泄露的配置直接控制数据库或网站。

大量美国和加拿大人的财务数据遭曝光：2022 年 1 月 12 日报道，Website Planet 的 IT 安全研究人员发现了一个配置错误的数据库，该数据库由位于佛罗里达州杰克逊维尔的运输行业商业信用报告机构 TransCredit 拥有。据称，该数据库包含客户敏感财务和个人数据，其中涵盖了加拿大和美国的货运和运输公司。该错误配置的数据库共暴露了 822,789 条记录，其中 600,000 条是客户的信用记录，其他暴露的信息包括：姓名、税号、电子邮件地址、银行信息、社会安全号码 (SSN)、内部登录 ID 和密码、EIN（雇主识别号码）等。

美国 Transact Campus 配置错误泄露 3 万多学生的信息：媒体 2022 年 6 月 15 日报道，SafetyDetectives 网络安全研究团队发现了一个配置错误的 Elasticsearch 服务器，该服务器暴露了 Transact Campus 应用程序的数据。根据他们的分析，该服务器已联网，无需密码即可访问数据。Transact Campus 是一家美国支付软件提供商，其软件解决方案主要用于促进高等教育机构的学生购买以及简化机构和学生的支付流程。SafetyDetectives 在报告中写道，服务器泄露的 5GB 数据库包含作为 Transact Campus 账户持有人的学生的详细信息。大多数受影响的个人是美国国民。暴露的数据包括学生的全名、电话号码、电子邮件地址、信用卡细节、交易明细、登录信息（用户名和密码）等。本次事件造成约 100 万条记录被泄露，涉及 30,000 至 40,000 多名学生的个人身份信息。值得注意的是，包括用户名和密码在内的登录数据以纯文本格式存储。另一方面，信用卡详细信息包括银行识别号，包括信用卡号的前六位和后四位、银行信息和卡的到期日期。此外，学生购买的膳食计划和膳食计划余额也是泄露数据的一部分。

服务器互联网暴露与配置问题是造成数据泄露与黑客入侵窃取数据的重要原因。作为拥有大量敏感信息的数据库，配置错误这种低级的安全问题不容小觑，必须采取一定的安全防御措施，可通过数据库安全加密技术对数据库中账号密码等基础安全配置进行加密操作，并配置合理的权限区分，利用数据库脱敏技术对数据进行变形操作，减少数据泄露给用户带来的损害。同时可以通过安装数据库漏洞扫描工具，定期扫描数据库，能够有效的找出数据库自身存在的安全漏洞和风险，并及时修复。

C.8 非法数据交易造成数据泄露

近年来，非法获取、买卖公民个人信息的案件时有发生，被贩卖的个人信息规模之大，触目惊心，已经严重影响到个人的生活，甚至人身安全。

2022 年 2 月，杭州市公安局滨江区分局接到线索：有人通过境外社交软件等渠道大量贩卖公民网络行为信息数据，涉嫌侵犯公民个人信息罪。该团伙通过注册公司与大量企业开展业务合作的形式，获取各种类型公民信息或其他关联信息，并通过组合加工的方式形成数据丰富、完整的公民个人信息进行出售。

2022 年 6 月 28 日，全国首家数据资源法庭——温州瓯海数据资源法庭依法审理并判决一起非法获取计算机信息系统数据罪，吴某利用技术手段非法获取某知名电商平台子账号数据并进行贩卖，从中牟利。因案涉商业秘密，经当事人申请，该案不公开开庭审理。

2022 年 8 月，有人在某黑客论坛上发帖以 4000 美元拍卖上海随申码数据库，声称其中包含 4850 万用户的上海随申码数据，其中包含自随申码推行以来，居住或到访过上海的所有人的身份证、姓名及手机号。发帖者为证实数据真实性，公开了 47 组样本数据，可以看到其中包含了用户的手机号码、姓名、身份证号、随申码颜色、UUID 多项信息。

某监测平台在 2022 年 11 月 15 日捕获到，国内某大型物流公司的用户快递面单信息数据遭到泄露，量级达每日上千条。泄露原因主要是快递站点工作人员进行面单拍摄，而后该人员在 Telegram 等交易平台，以每单 4 元的价格进行出售。

防范个人信息非法买卖，除了加大对非法收集、泄露、出售个人信息行为的打击力度，更要努力做到事前防范，提升自身的安全防范意识，尽力做到不使个人信息从自己手里泄露。对于所察觉的信息“黑市”交易行为及其人员，也应及时向执法部门举报，以公民群体力量织就严密的防范网络。

C.9 网络诈骗非法获取数据

近年来，电信网络诈骗犯罪多发高发形势严峻，在刑事犯罪案件中占据很大比重。数据显示，自 2021 年 4 月至 2022 年 7 月，全国共破获电信网络诈骗案件 59.4 万起。案件高发背后，非法泄露公民个人信息是网络犯罪链条中关键环节。

假借冬奥知识传播活动为名实施诈骗：2022 年 2 月，江苏南通警方侦破一起假借冬奥知识传播活动为名实施诈骗的案件。李某辉伙同汤某峰等人在没有取得冬奥组委会授权的情况下，开发“冬奥知识竞赛平台”，非法获取全国大中专院校在校学生的个人信息 350 余万条，骗取部分参与者缴纳证书工本费总计 1000 万余元。

一些非官方下载的 App，出现非授权、超范围采集使用个人信息等问题，存在用户个人信息泄露、滥用的风险，因此公众在使用相关 App 时，需提高风险防范意识，不轻易进行网上信息填写、网站注册。

C.10 儿童个人信息泄露

现如今，智能穿戴设备在生活中越发普及，儿童智能手表的功能也愈发强大，实时定位、高清双摄、人脸识别、视频通话、建立社群……家长们可以随时掌握孩子行踪，但一些穿戴型智能设备也在不断地采集、获取大量私密的个人信息，这些设备的安全性似乎很容易被忽视。

部分儿童产品违规收集个人隐私：央视财经频道的 3·15 晚会上，曝光了部分低配儿童智能手表存在的安全隐患。一项对此展开的专门测试发现：部分儿童智能手表可在用户不知情的情况下，劫持用户摄像头、麦克风、通讯录和定位信息，窃取用户隐私，通过手表能随时掌握孩子的一举一动，给孩子带来人身和财产安全隐患；部分儿童智能手表由于操作系统过于老旧，无需授权即可下载外部软件。一些恶意软件就能够轻松地拿到定位、麦克风、摄像头等多种敏感权限，轻易获取孩子的位置、人脸图像、录音等隐私信息，从而让使用者面临私密信息被暴露的风险。

手机 App 过度索取权限私自收集个人信息问题一度突出，工信部多次通报存在“APP 强制、频繁、过度索取权限”“违规收集个人信息”问题的软件。但少有人意识到的是：过度索取权限、违规收集个人信息的问题在儿童所能接触到的平板电脑、学习机、智能玩具、VR 游戏设备等领域同样泛滥。

某些短视频 APP 存在侵害儿童个人信息的行为：某科技公司运营的短视频 APP，存在侵害众多不特定儿童个人信息的侵权行为。这一短视频 APP 没有对儿童用户采取区分管理措施，默认用户点击“关注”后，就可以和儿童账户私信联系，获取地理位置、面部特征等个人信息。在没有征得儿童监护人授权同意的情况下，运用后台算法，向具有浏览儿童内容视频喜好的用户直接推送含有儿童个人信息的短视频，从而让犯罪分子有机可乘。

生产商、销售者不应该把未成年人当作商业手段，在研发面向未成年人的产品时安全永远高于创新。网络服务提供者要对青少年内容进行严格把控。同时家长要肩负起监护职责，不要纵容未成年人沉迷网络。2019 年 10 月 1 日，《儿童个人信息网络保护规定》正式实施，针对中华人民共和国境内通过网络收集、存储、使用、转移、披露不满十四周岁的儿童个人信息进行规范。《个人信息保护法》中也将不满十四周岁未成年人的个人信息作为敏感个人信息加以保护。真正实现儿童个人信息网络保护是多方参与、齐抓共管的过程，既依赖于法律规范、政府监管，也依赖于儿童监护人、行业组织以及社会公众在其中发挥的作用。

C.11 个人信息采集使用不当带来的权益侵害

2022 年度，工信部共发布 4 批《关于侵害用户权益行为的 APP 通报》，涵盖了违规收集使用、超范围收集个人信息，强制用户使用定向推送功能、APP 强制、频繁、过度索取权限、收集个人信息明示告知不到位、欺骗误导强制用户、应用分发平台上的 APP 信息明示不到位以及 SDK 违规收集个人信息等侵犯用户权益的行为。2022 年工信部还发布了 2 批《关于 APP 侵害用户权益整治“回头看”发现问题的通报》，分别针对违规推送弹窗信息、APP 过度索取权限等问题以及内存清理类、手机优化类 APP 进行重点监测，并对 2021 年发现问题的 APP 进行了抽测。此外，国家网信办还在 2022 年公布了一批侵犯个人信息合法权益的违法违规 App 的查处情况，主要围绕 APP 以强制、诱导、欺诈

等方式违法违规处理个人信息展开。除工信部以外，包括网信部门在内的监管部门亦开展了多样化的 APP 执法行动。

2022 年 8 月 3 日，银保监会办公厅下发《关于开展银行保险机构侵害个人信息权益乱象专项整治工作的通知》，要求全面梳理和排查银行业保险业在个人信息保护方面的问题和漏洞，深入整治侵害消费者信息权益乱象，督促银行保险机构建立健全消费者个人信息保护工作机制等。此次专项整治以银行保险机构自查为主，监管部门适时开展抽查和督导，整治的乱象包括个人信息的收集、存储、传输、查询、使用、提供、删除以及与第三方合作等方面，全面覆盖了与消费者个人信息处理相关的业务环节、员工行为和管理流程。

D.2022 年以来典型数据安全相关法律案件分析

D.1 中国知网因滥用市场支配地位行为，被罚 8760 万元

2022 年 6 月 24 日，为防范国家数据安全风险，维护国家安全，保障公共利益，依据《国家安全法》《网络安全法》《数据安全法》，按照《网络安全审查办法》，网络安全审查办公室对我国著名学术资源信息平台中国知网（以下简称“知网”）启动网络安全审查。2022 年 12 月 26 日，国家市场监管总局公布了对知网因滥用市场支配地位行为一案的调查结果，根据《反垄断法》相关规定，综合考虑知网违法行为的性质、程度、持续时间和消除违法行为后果的情况等因素，国家市场监管总局依法对知网上述垄断行为作出行政处罚决定：责令知网停止违法行为，并处以其 2021 年中国境内销售额 17.52 亿元 5% 的罚款，计 8760 万元。

知网在中国境内中文学术文献网络数据库服务市场具有很高的支配地位，其实施不公平高价、限定交易行为排除、限制了中文学术文献网络数据库服务市场竞争，侵害了用户合法权益，影响了相关市场创新发展和学术交流传播，构成《反垄断法》第二十二条第一款第（一）项、第（四）项禁止的“以不公平的高价销售商品”和“没有正当理由，限定交易相对人只能与其进行交易”的滥用市场支配地位行为。

D.2 上海 Z 网络公司陈某某等人非法获取计算机信息系统数据案

上海 Z 网络科技有限公司（以下简称“Z 公司”），公司是一家为本地生活商户提供数字化转型服务的互联网大数据公司，该公司涵盖在线开店、市场营销等多项业务，拥有 10 余项计算机软件著作权，还曾被评为高新技术企业。2019 年至 2020 年，该公司在未经授权许可的情况下，公司首席技术官陈某某指使多名技术人员，通过爬虫技术非法获取某外卖平台数据，造成该外卖平台直接经济损失 4 万余元，触犯了刑法第 285 条非法获取计算机信息系统数据罪，其情节适用 3 年以下有期徒刑或者拘役，并处或者单处罚金的法定刑档次。具体到本案的情况，检察机关认为涉案公司系初犯，且爬取的数据未涉及身份认证信息，没有二次兜售牟利等行为，犯罪情节较轻。同时，鉴于其属于成长型科创企业，陈某等人均认罪认罚，积极赔偿被害公司的经济损失并取得谅解，故依法启动涉案企业合规考察。2022 年 5 月，普陀区检察院依法对犯罪嫌疑单位 Z 公司、犯罪嫌疑人陈某某等 14 人作出不起诉决定。

这起首例数据合规不起诉案件的出炉带来了数据领域合规考察制度在应用层面的首次落地，与之伴随的，企业在从事数据处理活动上将面临更高、更加具体的合规要求。从事前合规控制违法成本的角度看，企业应当在日常经营活动中，将防范数据风险的意识落实到业务的细节处，建设常态化数据安全合规评估工作机制，提高数据安全意识，避免数据安全事件造成严重后果，导致不可预计的经济损失甚至被追究刑事责任。

D.3 公民非法买卖个人信息，判罚支付公共利益损害赔偿款 3.4 万元

杭州市上城区人民检察院诉孙某民事公益诉讼案中，被告孙某从 2019 年 2 月起以 34000 元的价格，将自己从网络购买、互换得到的 4 万余条含姓名、电话号码、电子邮箱等的个人信息，通过微信、QQ 等方式贩卖给案外人刘某。案外人刘某在获取相关信息后用于虚假的外汇业务推广。公益诉讼起诉人认为，被告孙某未经他人许可，在互联网上公然非法买卖、提供个人信息，造成 4 万余条个人信息被非法买卖、使用，严重侵害社会众多不特定主体的个人信息权益，致使社会公共利益受到侵害，据此提起民事公益诉讼。

杭州互联网法院经审理认为，民法典第一百一十一条规定，任何组织或者个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。被告孙某在未取得众多不特定自然人同意的情况下，非法获取不特定主体个人信息，又非法出售牟利，侵害了承载在不特定社会主体个人信息之上的公共信息安全利益。遂判决孙某按照侵权行为所获利益支付公共利益损害赔偿款 34000 元，并向社会公众赔礼道歉。判决后，当事人均服从法院判决未提起上诉，判决已生效。

本案系全国首例适用民法典的个人信息保护民事公益诉讼案，体现了法律对涉及社会公共利益的社会不特定民事主体个人信息的保护和重视，也体现了司法对不特定自然人个人信息保护路径的积极探索和有益创新。

D.4 滴滴公司违反数据安全相关规定，被网络安全审查行政处罚 80.26 亿元

2022 年 7 月 21 日，国家网信办依据《网络安全法》《数据安全法》《个人信息保护法》《行政处罚法》等法律法规，对滴滴公司处人民币 80.26 亿元罚款，对滴滴公司董事长兼 CEO 程维、总裁柳青各处人民币 100 万元罚款。经查明，滴滴公司共存在过度收集用户信息、未明确告知乘客情况下分析用户数据、频繁索取电话权限等 16 项违法事实，以及严重影响国家安全的数据处理活动、拒不履行监管部门的明确要求、阳奉阴违、恶意逃避监管等其他违法违规问题。

滴滴网络安全审查事件从 2021 年 7 月 2 日开始，至 2022 年 7 月 20 日作出处罚决定，经历了一年多的时间。经查实，滴滴公司的违法违规行为事实清楚、证据确凿、情节严重、性质恶劣，应当从严从重予以处罚。从滴滴事件可以看到，国家依法打击危害网络数据安全、侵害个人信息等违法行为，切实维护国家数据安全、保护个人信息和商业秘密的决心和力度。本案体现了监管部门治理网络安全、数据安全、个人信息保护等领域违法行为的决心，敲响了企业数据合规的警钟。

D.5 某征信机构错误关联个人企业信用信息致人失信，被判赔 9.1 万元

某征信机构在其运营的企业信用信息查询平台上，将与张某无关的大量信息错误关联至其名下及红彤彤公司，上述错误关联信息包括失信被执行人信息、限制高消费信息以及终本执行案件信息等。张某及红彤彤公司认为，该公司的上述行为侵害了其名誉权、个人信息权益，故提起诉讼。法

院对于该算法误判行为的技术中立抗辩意见予以反驳，并结合透明度规则和外观主义规则，最终判决支持张某及红彤彤公司的诉讼请求。广州互联网法院审理后判决，该征信机构在其平台官方网址、APP、微信公众号以及张某、红彤彤公司在该平台的主页内分别刊登对张某、红彤彤公司的致歉声明，声明内容需经法院审查，声明保留时间不少于十五日；此外向张某赔偿经济损失 30000 元，向红彤彤公司赔偿经济损失 30000 元；向张某、红彤彤公司赔偿律师费、公证费损失共计 31200 元，共 9.1 万元。

本案是广州互联网法院发布的《个人信息保护法》施行一周年个人信息保护典型案例之一，涉及的核心问题为“算法误判”问题，与之关联的案件还包括北京互联网审理的算法误判“杀猪盘”案以及杭州互联网法院审理的平台算法自动化决策案（(2020) 浙 0192 民初 3081 号）等。可以预见的是，随着算法监管的逐渐深入，算法应用过程中产生的算法误判等纠纷会逐渐增多，司法层面对于算法规制的裁判规则会愈发清晰，算法相关从业者应当予以重点关注。

D.6 广州一公司未履行数据安全保护义务被警方处罚 5 万元

从 2021 年 10 月下旬开始，广州市某公司陆续收到合作方驾校及当地运营部门投诉，有第三方人员冒充该公司工作人员，自称可以绕开该公司开发的“驾培平台”配套的车载终端打卡机制，让驾校学员在不到现场练车的情况下，在系统完成练车学时的累积，从而完成监管部门对驾考练车学时的严格要求。

广州警方经深入研判，挖出一作案团伙，抓获包括技术开发和代理在内的 3 名犯罪嫌疑人。该团伙通过技术手段非法破解“驾培平台”系统，将虚假的培训数据包发送至平台服务器，对学员的学时进行修改，以达到帮助学员快速完成培训和驾校快速盈利的目的。在刑事打击非法入侵驾培系统代刷学时案的同时，广州警方对此案进行“一案双查”。对上述公司的网络系统全面开展网络安全和数据安全检查。经查，公司开发的“驾培平台”存储了驾校培训学员的姓名、身份证号、手机号、个人照片等信息 1070 万余条，但该公司没有建立数据安全管理制度和操作规程，对于日常经营活动采集到的驾校学员个人信息未采取去标识化和加密措施，系统存在未授权访问漏洞等严重数据安全隐患。根据《中华人民共和国数据安全法》的有关规定，广州警方对该公司未履行数据安全保护义务的违法行为，依法处以警告并处罚款人民币 5 万元的行政处罚，开创了广东省公安机关适用《中华人民共和国数据安全法》的先例。

E. 我国主要数据安全相关标准汇总

“安全发展，标准先行”，标准化工作是保障网络数据安全的重要基础。为落实国家出台的数据安全相关法律法规要求，围绕数据安全和个人隐私保护，全国信息安全标准化技术委员会及金融、电信、工业、互联网等重点行业颁布了系列技术标准，对指导各行业组织合法、合规的开展数据安全治理工作，促进数据充分利用、有序流动和安全共享，推动数字经济发展具有重要意义。

E.1 国家标准汇总

序号	标准号	名称	实施时间	简介
1	GB/T42017-2022	信息安全技术网络预约汽车服务数据安全要求	2023/5/1	规定了网络预约汽车服务的收集、存储、使用、加工、提供、公开、出境等数据处理活动的安全要求。本文件适用于网络预约汽车服务提供者规范数据处理活动，也可为监管部门、第三方评估机构对网络预约汽车服务数据处理活动进行监督、管理、评估提供参考。
2	GB/T 42016-2022	信息安全技术网络音视频服务数据安全要求	2023/5/1	规定了网络音视频服务收集、存储、使用、加工、传输、提供、公开、删除等数据处理活动的全要求。本文件适用于网络音视频服务提供者规范数据处理活动，也可为监管部门、第三方评估机构对网络音视频服务数据处理活动进行监督、管理、评估提供参考。三
3	GB/T 42015-2022	信息安全技术网络支付服务数据安全要求	2023/5/1	规定了网络支付服务收集、存储、传输、使用、加工、提供、公开、删除、出境等数据处理活动的安全要求。本文件适用于网络支付服务提供者规范数据处理活动，也可为监管部门、第三方评估机构对网络支付服务数据处理活动进行监督、管理、评估提供参考。
4	GB/T 42014-2022	信息安全技术网上购物服务数据安全要求	2023/5/1	规定了网上购物服务的收集、存储、传输、使用、加工、提供、公开、删除、出境等数据处理活动的安全要求。本文件适用于网上购物服务提供者规范数据处理活动，也可为监管部门、第三方评估机构对网上购物服务数据处理活动进行监督、管理、评估提供参考。
5	GB/T 42013-2022	信息安全技术快递物流服务数据安全要求	2023/5/1	规定了快递物流服务收集、存储、传输、使用、加工、提供、公开、删除、出境等数据处理活动安全要求。本文件适用于快递物流服务提供者规范数据处理活动，也可为监管部门、第三方评估机构对快递流服务数据处理活动进行监督、管理、评估提供参考。
6	GB/T 42012-2022	信息安全技术即时通信服务数据安全要求	2023/5/1	规定了即时通信服务收集、存储、传输、使用、加工、提供、公开、删除、出境等数据处理活动安全要求。本文件适用于即时通信服务提供者规范数据处理活动，也可为监管部门、第三方评估机构对即时通信服务数据处理活动进行监督、管理、评估提供参考。

序号	标准号	名称	实施时间	简介
7	GB/T 41871-2022	信息安全技术 汽车数据处理安全要求	2023/5/1	规定了汽车数据处理者对汽车数据进行收集、传输等处理活动的通用安全要求、车外数据安全要求、座舱数据安全要求和管理安全要求。本文件适用于汽车数据处理者开展汽车数据处理活动，适用于汽车的设计、生产、销售、使用和运维，也适用于主管监管部门和第三方评估机构等对汽车数据处理活动进行监督、管理和评估。
8	GB/T 41817-2022	信息安全技术 个人信息安全工程指南	2023/5/1	提出了个人信息安全工程的原则、目标、阶段和准备，提供了网络产品和服务在需求、设计、开发、测试、发布阶段落实个人信息安全要求的工程化指南。适用于涉及个人信息处理的网络产品和服务（含信息系统），为其同步规划、同步建设个人信息安全措施提供指导，也适用于组织在软件开发生存周期开展隐私工程时参考。
9	GB/T 41807-2022	信息安全技术 声纹识别数据安全要求	2023/05/1	规定了数据处理者开展声纹识别数据处理的基本安全要求，并进一步明确了收集、存储、使用、提供、公开、删除等数据处理活动的安全要求，以及在不同处理活动下针对应用场景提出针对性的安全要求。涉及的主要法律法规：《民法典》第 1034 条，《个人信息保护法》第 28-30 条。
10	GB/T 41806-2022	信息安全技术 基因识别数据安全要求	2023/05/1	重点围绕个人信息处理的最小必要原则，规定了基因识别数据及关联信息的收集、存储、使用、加工、传输、提供、公开、删除等数据处理活动的安全要求。涉及的主要法律法规：《民法典》第 1034 条，《个人信息保护法》第 28-30 条，《人类遗传资源管理条例》。
11	GB/T 41773-2022	信息安全技术 步态识别数据安全要求	2023/05/01	重点围绕个人信息处理的最小必要原则，针对了当前步态识别数据滥采滥用、未采用有效的安全防范措施等突出问题，针对步态数据处理活动给出了安全要求。涉及的主要法律法规：《民法典》第 1034 条，《个人信息保护法》第 28-30 条。
12	GB/T 41479-2022	信息安全技术 网络数据处理安全要求	2022/11/01	规定了网络运营者开展网络数据收集、存储、使用、加工、传输、提供、公开等数据处理的安全技术与管理要求，适用于网络运营者规范网络数据处理，以及监管部门、第三方评估机构对网络数据处理进行监督管理和评估。涉及的主要法律法规：《个人信息保护法》《网络安全法》《数据安全法》。
13	GB/T 41400-2022	信息安全技术 工业控制系统信息安全防护能力成熟度模型	2022/11/1	本标准给出了工业控制系统信息安全防护能力成熟度模型，规定核心保护对象安全和通用安全的成熟度等级要求，提出了能力成熟度等级核验方法。
14	GB/T 41391-2022	信息安全技术 移动互联网应用程序（App）收集个人信息基本要求	2022/11/1	规定了 App 收集个人信息的基本要求，包括最小必要收集、必要个人信息、特定类型个人信息、告知同意、系统权限、第三方收集管理及其他要求，并给出了常见服务类型 App 必要个人信息范围和使用要求。

序号	标准号	名称	实施时间	简介
15	GB/T 39725-2020	信息安全技术 健康医疗数据安全指南	2021/07/01	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管理和技术措施。涉及的主要法律法规：《数据安全法》第 6 条、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（国办发〔2016〕47 号）等。
16	GB/T 39477-2020	信息安全技术 政务信息共享数据安全技术要求	2021/06/01	规定了政务信息共享过程中的数据安全技术要求以及相关基础设施的安全技术要求。涉及的主要法律法规：《数据安全法》第 42 条等。
17	GB/T 39335-2020	信息安全技术 个人信息安全影响评估指南	2021/06/01	提出了个人信息安全影响评估的基本原理和实施流程，适用于各类组织自行开展评估，或主管部门开展检查评估。涉及的主要法律法规：《个人信息保护法》第 55、56 条等。
18	GB/T 39204-2022	信息安全技术 关键信息基础设施安全保护要求	2023/05/01	该标准为运营者开展关键信息基础设施保护工作需求提供了强有力的保障。在网络安全等级保护的制度基础上，结合网络安全保障体系成果提出的可落地的安全保护要求。涉及的主要法律法规：《个人信息保护法》《网络安全法》《数据安全法》。
19	GB/T 38667-2020	信息技术 大数据 数据分类指南	2020/10/01	提供了大数据分类过程及其分类视角、分类维度和分类方法等方面的建议和指导。涉及的主要法律法规：《数据安全法》第 21 条。
20	GB/T 37988-2019	信息安全技术 数据安全能力成熟度模型	2020/03/01	给出了组织数据安全能力的成熟度模型架构，适用于组织开展数据安全能力建设，以及对组织数据安全能力进行评估。涉及的主要法律法规：《数据安全法》第 18、27 条等。 涉及的认证：“数据安全能力成熟度认证”等。
21	GB/T 37973-2019	信息安全技术 大数据安全管理指南	2020/03/01	提出了大数据安全管理基本原则，可指导组织开展大数据安全需求分析、数据分类分级、大数据风险评估等安全管理工作。 涉及的主要法律法规：《数据安全法》第 27、30 条等。
22	GB/T 37964-2019	信息安全技术 个人信息去标识化指南	2020/03/01	提出了个人信息去标识化的目标和原则，给出了去标识化过程和管理措施指导，适用于各类组织开展个人信息去标识化工作。涉及的主要法律法规：《个人信息保护法》第 51 条等
23	GB/T 37932-2019	信息安全技术 数据交易服务安全要求	2020/03/01	规定了数据交易服务所涉及的交易参与方、交易对象和交易过程的安全要求，可用于对数据交易服务机构进行安全评估。涉及的主要法律法规：《数据安全法》第 33 条等。
24	GB/T 35273-2020	信息安全技术 个人信息安全规范	2020/10/01	针对各类组织的个人信息处理活动，规范了开展收集、保存、使用、对外提供等个人信息处理活动应遵循的原则和安全要求。涉及的主要法律法规：《网络安全法》第 41-43 条，《个人信息保护法》等。
25	GB/T 31506-2022	信息安全技术 政务网站系统安全指南	2022/11/1	给出了政府网站采用云计算服务过程中，在规划准备、部署迁移、运行管理、服务退出等阶段的安全技术措施和安全管理措施。适用于为采用云计算服务，特别是社会化云计算服务的政务网站提供建设与运营指导。

序号	标准号	名称	实施时间	简介
26	GB/T 30283-2022	信息安全技术 信息安全服务分类与代码	2022/11/1	本标准描述了信息安全服务的分类与代码，主要包括信息安全咨询类、信息安全设计与开发类、信息安全集成类、信息安全运营类、信息的安全处理与存储类、信息安全测评与认证类及其他类七个方面。
27	GB/T 20984-2022	信息安全技术 信息安全风险评估方法	2022/11/1	描述了信息安全风险评估的基本概念、风险要素关系、风险分析原理、风险评估实施流程和评估方法，以及风险评估在信息系统生命周期不同阶段的实施要点和工作形式。
28	征求意见稿	信息安全技术 网络数据分类分级要求	征求意见	进一步落实了数据分级分类要求，阐明了数据分类分级的基本原则、数据分类分级框架和方法以及数据分类分级实施流程，并以附录形式详细介绍了数据分级要素识别常见考虑因素、影响对象考虑因素、影响程度参考示例等数据分类分级时所需关注的参考要点。涉及的主要法律法规:《数据安全法》第 21 条等。
29		信息安全技术 数据出境安全评估指南（征求意见稿）	征求意见	指南明确了数据出境安全评估是数据出境的路径之一，并对申报的相关流程进行了明确，包括数据出境的概念范围、数据出境安全评估的适用范围、重要数据的概念、数据出境安全自评估具体流程、不适用安全评估的数据如何出境等内容。涉及的主要法律法规:《网络安全法》第 37 条、《数据安全法》第 31 条、《个人信息保护法》第 38-43 条、《数据出境安全评估办法》等。
30		信息技术 大数据 数据治理实施指南	征求意见	本文件规定了数据治理实施过程框架，从规划、执行、评价及改进四个主体过程给出了开展数据治理活动的活动及内容。本文件适用于指导组织开展数据治理的实施工作
31		信息安全技术 重要数据识别指南（征求意见稿）	征求意见	指南明确了重要数据的定义、识别重要数据的基本准则、重要数据的识别要素和描述格式。涉及的主要法律法规:《网络安全法》第 21、37 条、《数据安全法》第 21、27、30、31 条、

E.2 行业标准汇总

序号	标准号	名称	实施日期	简介
1	YD/T 4058-2022	电信网和互联网安全防护基线配置要求和检测要求 大数据组件	2022/7/1	规定了电信网和互联网中所使用大数据服务在安全配置方面的基本要求及检测要求，特别是大数据采集组件、大数据处理组件、大数据存储组件及其基础设施、网络系统在安全配置方面的基本要求及检测要求。
2	YD/T 4057-2022	电信网和互联网大数据平台安全防护检测要求	2022/7/1	规定了大数据平台安全防护的检测范围、对象、环境、方式，并按照相应的安全防护等级给出测试方法，将大数据平台安全等级共分为 5 级。
3	YD/T 3954-2021	云服务用户数据保护能力参考框架	2022/04/01	规范了云计算服务提供者在提供云计算服务时应具备的用户数据安全保护能力，包括事前防范能力、事中保护能力和事后追溯能力。

序号	标准号	名称	实施日期	简介
4	YD/T 3956-2021	电信网和互联网数据安全评估规范	2022/04/01	规定了数据安全评估实施流程和数据安全相关管理及技术措施的评估要点。
5	YD/T 3865-2021	工业互联网数据安全保护要求	2021/07/01	规定了工业互联网数据安全保护的范围及数据类型、工业互联网数据重要性分级与安全保护等级划分方法，规定了低/中/高重要性数据在数据产生、传输、存储、使用、迁移及销毁阶段的具体安全保护要求。
6	YD/T 3867-2021	基础电信企业重要数据识别指南	2021/07/01	给出了基础电信企业重要数据的定义、识别规则、识别方法和重要数据安全保护实施指导，并给出了基础电信企业重要数据示例。
7	YD/T 3813-2020	基础电信企业数据分类分级方法	2021/01/01	规定了基础电信企业数据分类分级原则、数据分类工作流程和方法，数据分级方法，并给出基础电信企业数据分类分级示例。
8	YD/T 3806-2020	电信大数据平台数据脱敏实施方法	2021/01/01	本标准规定了电信大数据平台数据脱敏的指导原则、典型流程，对不同场景下的脱敏实施方法、脱敏算法选择给出了建议。
9	YD/T 3802-2020	电信网和互联网数据安全通用要求	2021/01/01	本标准规范了数据采集、传输、存储、使用、开放共享、销毁等数据处理活动及其相关平台系统应遵循的原则和安全保护要求,包括组织保障、制度建设、规范建立等管理性要求，以及规范执行相关配套技术性要求。
10	YD/T 3801-2020	电信网和互联网数据安全风险评估实施方法	2021/01/01	提供以数据为核心保护对象的面向应用场景的风险评估方法论，规定了电信网和互联网数据安全风险评估的基本原则、基本要素及各要素之间的关系、实施流程、风险分析模型与方法。
11	YD/T 3800-2020	电信网和互联网大数据平台安全防护要求	2021/01/01	准规定了大数据平台安全防护要求，包括大数据平台基础设施安全要求、平台安全要求、数据安全要求和安全管理要求。
12	YD/T 3797.2-2020	云服务用户数据保护能力评估方法 第2部分：私有云	2021/01/01	规定了云服务提供商在提供私有云平台时应具备的用户数据安全保护能力要求，包括事前防范能力、事中保护能力和事后追溯能力。
13	YD/T 3797.1-2021	云服务用户数据保护能力评估方法 第1部分：公有云	2022/04/01	规定了公有云云计算服务提供者在提供云计算服务时应具备的用户数据安全保护能力要求和评估方法进行规范，包括事前防范能力、事中保护能力和事后追溯能力。
14	YD/T 3746-2020	车联网信息服务用户个人信息保护要求	2020/10/01	规定了车联网信息服务用户个人信息保护的信息内容分类、敏感性分级和分级保护要求。
15	YD/T 3736-2020	电信运营商大数据安全风险及需求	2020/10/01	规定了电信运营商大数据通用安全风险及相关需求，包括安全风险、安全需求、防护架构、技术要求等方面的内容。
16	YD/T 3644-2020	面向互联网的数据安全能力技术框架	2020/07/01	定义了互联网行业的数据安全能力技术框架，该框架基于互联网行业的业务特点，在分析了覆盖数据全生命周期的数据安全威胁的基础上，提炼了数据安全能力建设的技术框架，并对框架内容进行了详细的描述。

序号	标准号	名称	实施日期	简介
17	JR/T 0223-2021	金融数据安全 数据生命周期安全规范	2021/04/08	规定了金融数嚣生命周期安全原则、防护要求、组织保障要求以及信息系统运维保障要求，建立覆盖数据采集、传输、存储、使用、删除及销毁过程的安全框架。
18	JR/T 0197-2020	金融数据安全 数据安全分级指南	2020/09/23	给出了金融数据安全分级的目标、原则和范围，以及数据安全定级的要素、规则和定级过程。
19	JR/T 0171-2020	个人金融信息保护技术规范	2020/02/13	将个人金融信息按敏感程度、泄露后造成的危害程度，从高到低分为 C3、C2、C1 三个类别；同时，规定了个人金融信息在收集、传输、存储、使用、删除、销毁等生命周期各环节的安全防护要求，从安全技术和安全管理两个方面，对个人金融信息保护提出了规范性要求。

E.3 地方标准汇总

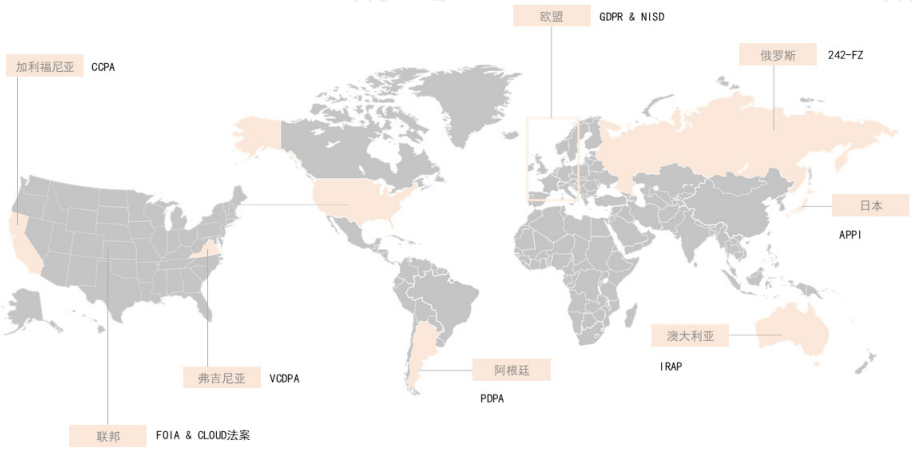
序号	标准号	名称	地点	实施日期	简介
1	DB11/T 2049-2022	政务大数据安全技术框架	北京	2022/04/01	提出了政务大数据安全技术框架，规定了政务大数据域安全要求、政务大数据域间协同安全要求以及基础设施安全要求等。适用于指导政务部门以及参与政务大数据处理活动的相关组织开展政务大数据安全技术体系规划、建设、监督与管理。
2	DB4403/T 271-2022	公共数据安全要求	深圳	2022/12/01	共九章，全面覆盖数据安全管理、技术及数据处理活动各环节，适用于公共管理和服务机构数据安全能力的建设、评估与监管，也适用于处理大量个人信息的服务平台数据安全能力的建设与评估。
3	DB4403/T 278.1-2022	公共基础信息数据元规范	深圳	2023/01/01	规定了人口、法人、房屋、电子证照、公共信用、地理空间等 6 个部分公共基础信息数据元应遵循的数据类型和格式、分类和属性；以及各数据源管理的指导原则、管理要素、相关角色和职责、归集管理和应用流程。
4	DB33/T 2488-2022	公共数据安全体系评估规范	浙江	2022/5/26	规定了大数据平台安全防护的检测范围、对象、环境、方式，并按照相应的安全防护等级给出测试方法，将大数据平台安全等级共分为 5 级。
5	DB11/T 2049-2022	政务大数据安全技术框架	北京	2022/04/01	提出了政务大数据安全技术框架，规定了政务大数据域安全要求、政务大数据域间协同安全要求以及基础设施安全要求等。适用于指导政务部门以及参与政务大数据处理活动的相关组织开展政务大数据安全技术体系规划、建设、监督与管理。

序号	标准号	名称	地点	实施日期	简介
6	DB31/T 1356.1—2022	公共数据资源目录	上海	2022/12/01	该目录分为三部分，分别为编制指南、元数据规范、编码规范。第一部分在于确定目录分类、编制过程，第二部分在于确定元数据描述方法以及不同种类元数据的描述，第三部分在于确定需要编码的元数据编码规则。
7	DB31/T 1311—2021	数据去标识化共享指南	上海	2021/10/01	通过“规范共享的数据内容、控制过程的安全有序、约束数据的有限使用”，使数据去标识化共享仍然遵循个人信息保护等的法律法规，以防范数据共享的风险，促进数据合法合规的共享和收集利用
8	DB1331/T 004—2022	雄安新区数据安全建设导则	河北	2021/07/01	规定了数据安全总体策略要求、数据安全建设总体要求、数据全生命周期安全技术要求、数据安全通用要求等方面内容，为雄安新区全区范围内党政机关和其他社会组织数据安全建设与发展明确总体框架、技术要求和通用要求。
9	DB2102/T 0041—2022	大数据标准体系框架	辽宁	2022/01/17	规定大数据标准体系框架，包括大数据标准体系总体要求、标准体系结构图以及分体系结构图等内容；适用于大数据业务相关的政府、企事业单位、科研院所以及相关组织机构等。

F. 国际数据安全政策与法规概述

在数字经济时代，数据安全是各行各业的运行关键，数据安全所带来的风险及损失也不可估量。例如，2022 年，在公共安全领域，美国新墨西哥州最大的县受到勒索软件攻击影响，多个公共事业部门和政府办公室系统下线，此次勒索软件攻击还致使监狱系统下线，严重危害到国家安全；在个人信息安全领域，中国的蔚来公司收到外部勒索邮件，发件人表示拥有数百万条蔚来内部数据，涉及车主身份证、贷款甚至亲密关系等极为隐私信息，并以泄露数百万条数据作为威胁，勒索 225 万美元等额比特币；在企业组织方面，2013 年 1 月，作为全球最大的社交媒体之一的推特，再次遭遇数据泄露。根据美国《华尔街日报》网站报道，超过 2.35 亿个推特账号的数据被泄露并发布在一个在线黑客论坛上，数据是完全公开，任何人都可以免费下载，其中包括账户名称、唯一 ID、创建日期、关注者数量和电子邮件地址等。

为应对突发多变的数据安全事件，各国均高度重视数据安全治理，严厉惩处造成数据安全后果的违规事件。例如，2022 年 7 月，中国国家互联网信息办公室对过度采集和滥用信息的滴滴公司，处以人民币 80.62 亿元罚款；2022 年 8 月，美国移动通信巨头 T-Mobile 同意支付 2021 年大规模数据泄露事件后的索赔、法律费用和管理费用，共计支付 3.5 亿美元。面对日益重要的数据与愈发严峻数据安全问题，全球各主要国家纷纷出台相关法律法规，通过各种组织措施和技术措施强化数据安全，推动数据开发利用、价值挖掘与安全防护的并举发展。迄今为止，全球近 60 个国家或地区出台了数据主权相关法律，并呈现不同的特征。但是，国际主流的数据安全管理思想较为统一：基于数据的重要程度，分类分级的开展数据跨境管理工作，并在既有的国际合作框架下探索数据跨境合作。



F-1　国际数据安全政策与法规

F.1 欧洲的政策和法律

（1）欧盟

欧盟对重要数据和个人信息等隐私数据的重视和立法保护一直走在世界前列。早在 1995 年，欧盟就在其《数据保护指令》中确立了数据跨境传输的基本原则，并对世界其他国家和地区的数据流动和保护产生了深远的影响。

2018 年 5 月 25 日，《通用数据保护条例》（GDPR）正式施行，适用于向欧盟民众提供商品和服务或收集并分析欧盟居民相关数据的组织。GDPR 重在保护数据主体的基本权利，规定了数据控制者和处理者应尽的保护数据主体权利的法定义务，以及监管部门和认证机构的法定义务。2018 年 10 月，欧盟颁布《联盟机构个人数据处理保护条例》，作为 GDPR 的补充，对欧盟机构在处理个人数据时应如何保护自然人提出基本要求，明确了数据主体的权利范围以及监管机关的职能和义务。2018 年 11 月，欧盟颁布《非个人数据自由流动条例》，对数据的本地化要求、主管当局的数据获取及跨境合作、专业用户的数据迁移等问题给出具体规定，并将服务提供商负担过度及市场扭曲等问题纳入考虑范畴，进一步完善了欧盟的数据治理框架。

《网络信息系统安全指令》（NISD）旨在加强基础服务运营商、数字服务提供商的网络和信息系统安全，并要求成员国及时转化为国内立法。NISD 和 GDPR 分别从安全防护和基本权利保障两个角度推行欧盟的网络和数据安全战略。

2019 年 6 月 27 日，《网络安全法案》正式施行，确立了欧盟的网络安全认证计划，指定了欧盟网络和信息安全署（ENISA）作为欧盟网络安全职能机构，确立了首份欧盟范围的网络安全认证计划，要求在欧盟境内采用的产品、流程和服务须满足该网络安全标准。

2020 年 2 月 19 日欧盟委员会推出《欧盟数据战略》，该战略勾画出欧盟未来十年的数据战略行动纲要。系统性地概括了欧盟未来在数据方面的核心政策举措和投资战略，包括构建统一的数据治理架构、加强数据基础设施建设、加大数据技能和素养投资、打造欧洲数据空间等。

2021 年 10 月，《欧盟数据治理法案》表决通过，该《法案》旨在“为欧洲共同数据空间的管理提出立法框架”。2021 年 9 月 15 日，欧委会提交《通向数字十年之路》提案，该提案以《2030 年数字指南针》”为基础，为保证战略的可持续性以及加强公民和企业对政策的支持和信任，为欧盟数字化目标的落地提供具体治理框架。

2022 年 4 月 6 日，欧洲议会通过了《数据治理法》，欧洲数据保护委员会（EDPB）公布了作为数据传输工具的行为准则的指南定稿，旨在促进数据在欧盟的共享，以使企业和初创公司获得更多的数据用于开发新的产品和服务，从而提高数据利用效率，确保重要数字服务市场的公平性和开放性；2022 年 7 月 18 日欧盟 27 个成员国一致宣布最终批准《数字市场法》（DMA）。DMA 中的规制对象主要针对大型数字服务提供者（即“守门人”），旨在明确大型数字服务提供者的责任，遏制大型网络平台企业的非竞争性行为。2022 年 10 月，《数字市场法案》《数字服务法案》在欧盟官方公报上正式刊发。前者作为欧盟传统反垄断执法的补充，对有重大影响力的数字公司施加更多义务和限制。后者则对网络平台、用户以及广告商等不同合规主体设置了不同合规义务，侧重对处在弱势地位的普通用户的权利进行保护。

（2）英国

1984 年，英国议会通过的首部《数据保护法》。该法提出个人数据保护的基础性原则，禁止数据主体未经注册持有个人数据，设立数据保护登记官和数据保护法庭，分别作为法令执行的监管机构和申诉机构。

2003 年，英国议会通过《隐私与电子通信条例（PECR）》，要求电子通信服务商保护终端用户信息，由信息专员负责监督执行。该条例是英国对欧盟《电子隐私指令（指令 2002/58/EC）》的落地实施，

同英国《数据保护法》和英国 GDPR 并驾齐驱，赋予公民在电子通信方面享有隐私权，保护消费者免受信息滥用和潜在网络犯罪的危害。

2018 年 5 月 10 日，《网络和信息系统安全法规》生效，是欧盟 2016 年 7 月 6 日颁布的《网络和信息系统指令》的英国版，是英国第一个以网络安全为重点的跨领域监管条例，旨在提高网络和信息系统的安全水平（包括网络和物理弹性），以保障基本服务和数字服务。

2021 年 1 月 1 日，英国通用数据保护条例（英国 GDPR）生效，涵盖了英国处理个人数据时的主要原则及权利和义务，并与 2018 年《数据保护法》并列，适用于向英国个人提供商品和服务和 / 或监控英国任何个人行为的任何组织。

英国政府为促进数据在政府、社会和企业间的流动，于 2020 年 9 月发布《国家数据战略》《战略》中明确指出了政府需优先执行的五项任务以促进英国社会各界对数据的应用：一是充分释放数据价值；二是加强对可信数据体系的保护；三是改善政府的数据应用现状，提高公共服务效率；四是确保数据所依赖的基础架构的安全性和韧性；五是推动数据的国际流动。五项任务发布以来，英国政府采取了一系列行动促进数据的高效合规应用，如颁布《政府数据质量框架》，助力公共部门提升数据管理效率以及建立数据市场部门等。2021 年 5 月，英国政府在官方渠道上发布《政府对于国家数据战略咨询的回应》，强调 2021 年的工作重心是“深入执行《国家数据战略》”，并表明将通过建立更细化的行动方案，全力确保战略的有效实施，由此可以看出英国政府利用数据资源激发经济新活力的决心。

（3）德国

1976 年，德国发布《联邦个人信息保护法》，采取统一的立法模式，对个人信息保护进行统一规范。具体内容包括个人信息保护的原则、监督机制损害赔偿制度、跨国传输机制等。

1977 年，德国发布《联邦数据保护法》，此后该法经过了多次修订，最后一次修订是在 2019 年。该法旨在通过数据保护以实现一般人格权的保护，规定了个人信息的知情权、同意权、使用权等。

2017 年 6 月 30 日通过了《联邦数据安全法》以落实对 GDPR 国内立法的承诺。德国数据安全执法采取了联邦 – 地方的两级架构，联邦数据保护与信息自由委员（BfDI）在联邦一级实施数据保护，而 16 个地区数据保护机构则在各自州的公共和私营部门执行数据保护法。所有监管机构会定期在德国数据保护会议（DSK）上举行会谈，发布详细的指导方针，进一步完善了德国的隐私法律框架。其中重要指南包括有关 Cookie 同意的指南、基于 GDPR 的罚金刑评估标准以及标准数据保护模型。此外，德国是首批实现卫生系统数字化的欧洲国家之一，《患者数据保护法》（PDSG）于 2020 年生效。

2021 年 1 月，德国政府发布《联邦数据战略》，旨在强化数据的应用和管理，并增强数据的安全保障能力。其具体内容涉及构建高效且可持续的数据基础设施、促进数据创新并负责任地使用数据、提高数据能力并打造数据文化、使德国成为数据先驱四个方面。

2021 年 5 月，德国颁布《IT 安全法》，旨在保护重要基础设施的数据安全，以加强国家安全。

德国较早通过明确立法对数据进行严格保护，通过制定《联邦个人信息保护法》《联邦数据保护法》《IT 安全法》《联邦数据战略》等法规和战略形成中央立法到地方立法、从一般立法到专门领域立法的全方位数据保护法律体系框架，这个体系在世界范围内同样具有领先性。同时，德国在数据保护领域长期致力于欧洲法律一体化的协调发展，深刻影响了欧洲乃至全球的数据立法进程。近

年来，德国对电子监控、个人信息存储、电子办公、工业互联网、视频会议等新兴技术发展带来的挑战予以高度关注，通过细化法律形式，强化数据安全风险管理。

为了协调德国《电信法》和《电信媒体法》长期以来与 GDPR 互动方面法律的不确定性，2021 年德国颁布了《电信和电信媒体数据保护法》（TTDSG）。TTDSG 实施了欧盟了《电子隐私指令》，该指令规范 cookie 的使用、电子邮件营销、数据缩小以及数据隐私的保护。TTDSG 主要规定数据保护原则在电信和电信媒体中的应用，该法要求电信服务提供商在使用 cookie 等跟踪技术前需获得有效的用户同意，这与欧盟《电子隐私指令》中的规范相呼应。

（4）法国

1978 年，《信息技术与自由法案》制定，这部法律是法国保护数据安全的起源法律之一。该方案明确阐述了信息技术发展与信息安全的关系，即："信息技术应该为每个公民服务。它的发展应在国际合作的背景下进行。它不得侵犯人的身份、人权、隐私及公共自由等。"在该法律的基础上，2018 年，法国政府通过了新版本的《法国数据保护法》，实现了法国数据保护有关法律与《通用数据保护条例》（GDPR）之间相互衔接的周延性。同年，法国《个人数据保护法》生效，该法案同样是以《信息技术、数据文件和公民自由法》为基础的，并且落实了 GDPR 的立法举措，目的在于保护公民的个人数据信息和重要数据安全。随着 2019 年 5 月 29 日为适用该法律而通过的第 2019–536 号法案的通过，法国国内数据保护立法得到进一步完善。该法令明确了法国数据保护机构的控制和制裁程序。

近年，为满足法国对国家安全的要求，相关的法律与法案又有了相应的更新。2021 年，关于防止恐怖主义和情报行为的第 2021–988 号法律对其第 48 和 49 条进行修订，对在国家安全需要处理的情况下为个人权利设定了例外；2022 年，关于刑事责任和国土安全的第 2022–52 号法律对其第 10、20 和 125 条进行了修改，并新设第 22–1 条，引入法国数据保护机构的简化制裁程序。

1994 年，为适应国际战略形势的变化，法国发表了冷战后的第一部国防白皮书，并把网络信息攻击视为未来 15 年最大的威胁之一，在此基础上，法国分别于 2008 年和 2015 年相继推出了《信息系统防御与安全：法国战略》和《法国国家数字安全战略》，体现出了法国对网络信息防护的重视。2018 年 2 月发布的《网络防御战略评论》更是明确提出了"'数字主权'是国家主权的组成部分"，数据安全的地位上升到新的战略高度。

（5）俄罗斯

2006 年，俄罗斯第一部关于数据与信息安全的联邦法律《信息、信息技术和信息保护法》颁布。该法认为信息可作为资产，信息资源是财产的组成部分和所有权的客体，相关主体的权利应当得到保障，因而对信息拥有者和信息系统运营者施加了其所需要承担的信息保护义务。此外，该法强调本地化数据存储，减少对境外网络的依赖。

同年 7 月，《俄罗斯联邦个人数据法》颁布，聚焦个人信息保护领域，旨在建立保护个人数据主体权利和自由的机制。其强调数据主权问题，在数据跨境流动方面，实行严格管控，要求处理者有义务确保个人数据接收国对个人数据主体的权利提供充分的保护。

2009 年，《不使用自动化设备进行个人数据处理规定》颁布，其主旨在于为执行"个人数据"联邦法，在不使用自动化工具的情况下处理个人数据的特殊性规定。

2012 年，《个人数据相关信息系统在处理个人数据过程中的防护要求》颁布，对个人数据信息系统进行分级，并制定相应的安全防护措施规范。

242-FZ(12.31.2014) 全称“关于阐明信息和电信网络中个人数据处理过程的俄罗斯联邦一揽子法律法案的修订”。该法案确认，自 2015 年 9 月 1 日起，被视为个人数据操作员的组织必须确保在收集个人数据时，俄罗斯公民的个人数据记录、系统化、保存、存储、修改（更新、更改）和提取操作是通过位于俄罗斯的数据库执行的。

2018 年 12 月俄罗斯发布《<俄罗斯联邦通信法>与<俄罗斯联邦关于信息、信息技术和信息保护法>修正案》，也被称为《主权互联网法》（Sovereignty Internet Law）。该法主要目的是保障俄罗斯对俄罗斯网络主权的控制权，包括域名自主、平台管控、主动断网等。

F.2 美国的政策和法律

F.2.1 联邦

（1）综合性立法

美国是世界上最早提出并通过法规对隐私权予以保护的国家，美国在 1974 年通过《隐私法案》（Privacy Act），对联邦行政部门收集、利用和保护个人数据作出规定，旨在保护公民隐私权和知情权，平衡政府保有个人信息的需求和个人隐私权保护之间的利益分歧。1986 年颁布《电子通讯隐私法案》，1988 年又制订了《电脑匹配与隐私权法》及《网上儿童隐私权保护法》（Children's Online Privacy Protection Act）。1990 年，美国国会颁布了《计算机匹配和隐私保护修正案》，明确了相关正当程序规定。1996 年颁布了《健康保险流通与责任法案》（HIPAA），该法案规范了健康信息的隐私和安全。1999 年颁布了《格雷姆－里奇－比利雷法案》（GLBA），该法案要求金融机构向客户解释其信息共享做法，并保护敏感数据。2020 年，美国司法部隐私和公民自由办公室编写了《1974 年隐私法概述》，为《隐私法案》的解释和应用提供了参考。

2018 年，美国国会通过了《澄清境外合法使用数据法案》（Clarifying Lawful Overseas Use of Data Act，以下简称“云法案”），云法案打破了以往跨国数据类证据调取过程中遵循的数据属地管辖模式，构建了一套全新的以数据控制者实际数据控制权限为衡量依据的标准框架。云法案单方面赋予了美国政府对全球绝大多数互联网数据的“长臂管辖权”，明确规定，无论服务提供者的通信、记录或其他信息是否存储在美国境内，只要相关通信内容、记录或其他信息为该服务提供者拥有、控制或者监管，均应当按照法令要求，保存、备份、披露。

2020 年 10 月，美国国防部发布了《国防部数据战略》（《DoD Data Strategy》），该战略是继 2019 年美国国防部发布的《国防部云战略》《国防部人工智能战略》和《国防部数字现代化战略》以后又一 IT（信息化）现代化领域指导性战略文件，其中提出国防部应加快向“以数据为中心”的过渡，强调通过数据融合实现军种联合、重视数据的安全性、强调数据全生命周期各个阶段的标准化处理能力。

2021 年，美国通过了《统一个人数据保护法》（Uniform Personal Data Protection Act，

UPDPA），旨在为各州隐私立提供一个可供参考的统一的立法模型。UPDPA 的主要内容包个人数据主体所持有的个人数据，个人数据主体的访问权和更正权，假名数据，兼容、兼容和禁止的数据实践，收集控制者、第三方控制者和实践者的责任，自愿共识标准，执行和规则制定。2021 年 12 月，根据《外国公司问责法案》（HFCAA）规定的监管机构如何界定将被摘牌的公司以及相应的退市程序，美国证券交易委员会（SEC）要求外国公司提供审计底稿供美国检查，不能提供审查的，可能在三年内被纽约证交所和纳斯达克摘牌。受到该法规影响的中概股超过 200 支。美国自 2002 年以来一直要求提供审计底稿，但中国大陆和中国香港一直拒绝检查。2022 年 3 月，SEC 再次公布新版规定征求意见稿，进一步加强要求上市公司关于网络安全风险管理、战略、治理和事件报告的披露，并使之标准化，其中明确了上市公司信息安全事件应在 4 天内披露。2022 年 3 月 –4 月，SEC 分五批将搜狐、百度、微博、富途控股等中概股列入预退市名单。

2022 年，美国还通过发布第一个综合性联邦隐私法案《美国数据隐私和保护法案》草案、《算法责任法案》草案等持续推动数据安全与隐私立法。

（2）针对性立法

●《联邦贸易委员会法案》：是美国于 1994 年制定的一部联邦消费者保护法，禁止不公平或欺骗性商业行为。由于缺乏任何综合性的联邦隐私法或专门针对线上服务的法律，联邦贸易委员会利用该法律，调查和纠正违反其通过执法逐渐形成的公平信息原则及其公布的指引的行为。

●《儿童在线隐私保护法》：于 1998 年颁布，对 13 岁以下儿童个人信息进行特殊保护。儿童网络隐私保护法旨在使家长能控制商业网站和线上服务对其子女数据的收集、使用和披露。

●《电话消费者保护法》：对收集和使用电话号码进行电话营销的行为进行监管，包括电话和短信。电话消费者保护法规定了私人诉讼权以及每条信息最高 1500 美元的法定处罚，且该权利被广泛用于集体诉讼。

●《控制非自愿色情与推销侵扰法》：该法以拒绝的方式，对为商业目的收集和使用电子邮件地址的行为进行监管。但在实践中，由于私人大多建立了拦截名单并使用拦截技术，因此该法律目前较少被运用。

●《格雷姆 – 里奇 – 比利雷法案》：对从事金融活动或提供金融产品的机构收集、使用、保护和披露非公开个人信息进行监管。

●《公平信用报告法》和《公平和准确信用交易法》：两部法案规定了金融领域中消费者报告机构和使用消费者报告的机构如何使用和披露消费者报告和信用卡账号。

●《健康保险携带和责任法案》：该法对广泛的医疗保健相关活动的隐私进行监管，健康信息包括包括与病人健康有关的医疗信息、医疗记录、与医疗服务提供者的对话、医疗账单信息等。

F.2.2 州

（1）加利福尼亚州

加利福尼亚州是美国第一个颁布了通用消费者隐私法律的州，于 2018 年颁布了《消费者隐私法》（CCPA），该法于 2020 年生效。加利福尼亚州消费者隐私法授予加利福尼亚州居民若干个人信息权利，

包括查阅权、数据可携带权、删除权等。加利福尼亚州消费并按规定披露相关信息等。该法被认为是全美目前最严格的隐私立法。

2020 年加利福尼亚州还颁布了《隐私权利法》（CPRA），该法将于 2023 年 1 月 1 日生效。该法对加利福尼亚州消费者隐私法进行了实质性修订，包括扩大加利福尼亚州消费者隐私法规定的个人信息保护权利和商业义务，特别是对于像精确地理位置数据这样的敏感信息以及规定数据最小化和目的限制的要求等。并且，《隐私权利法》还设立了一个新的州级机构，名为加利福尼亚州隐私保护局，负责执行隐私权利保护法。具体关注点如下：

●未来将继续出台法规以进一步细化 CPRA 的规定。CPRA 在 CCPA 的内容上进行了多处修改，但是 CPRA 的许多细节需要通过法规加以澄清和定义。其中，CPRA 要求加州出台相关法规以定义该法案中的一些条款，例如，建立约束更正权的规则，建立针对全面选择退出偏好标志及其他选择退出机制的技术要求，以及要求明确服务提供者和承包商（CPRA 中新定义的实体）在何种情况下能出于自身商业目的基于合同而使用个人信息。上述法规的制定将由加州总检察长办公室在未来陆续推出。

●成立加州隐私保护机构。CPRA 还将成立一个新的机构——加州隐私保护机构（California Privacy Protection agency，CPPA）来执行该法案。CPRA 如何被解释和执行将在很大程度上取决于 CPPA 的五人委员会由谁组成。其中两个席位（包括主席）将由州长任命，其余席位分别由总检察长、参议院规则委员会和议会发言人来任命。这些职位将在大约 90 天内确定。

●与 CCPA 的不同点。在敏感信息方面，CPRA 创造了一项新的敏感个人信息类别，它包含了精准地理位置信息，消费者的通信内容和的健康信息（前提是该等健康信息不属于《健康保险便携性和责任法案》(HIPAA) 或者其它有关例外所涵盖的范围）。值得注意的是，对于敏感个人信息的规定不适用于公开信息或者非用于分析消费者特点而收集或处理的敏感个人信息；在承包商方面，CPRA 将承包商定义为除了企业，服务提供者以及第三方以外的另一种受 CPRA 约束的实体。承包商与服务提供者的义务相似，并且都受到类似的合同限制，包括禁止出售个人信息、限制个人信息的处理方式，以及禁止混合数据等；此外，CPRA 还对“暗纹模式”做出了相关规定。根据 CPRA，“通过使用暗纹模式获得的协议不构成同意”。法案将暗纹模式定义为“一个被设计或操控的用户界面，其实质影响是颠覆或损害用户的自主权、决策或选择（未来将制定的法规会做出进一步定义的）”。不过，这个定义并不明确，可能会在之后的规则制定过程中引发重大争论。

（2）伊利诺伊州

伊利诺伊州设有关于生物识别信息的具体隐私法，即《伊利诺伊州生物识别信息隐私法》，该法保护消费者免于遭受因使用生物识别标识符和生物识别信息而引起的侵犯隐私、身份盗窃和经济损害等威胁。

（3）特拉华州

特拉华州未设制定通用隐私法律，但设有针对具体行业的隐私法，如《特拉华州网络隐私和保护法》，对服务对象或服务目的是以儿童为主要受众的互联网公司进行监管。

（4）纽约州

与加州不同，纽约州未制定通用隐私法，但设有针对具体行业的隐私法。例如，纽约州法律保护医疗保健数据的机密性，限制向第三方披露医疗记录。纽约州金融服务管理局也对金融服务和保

险企业规定了详细的网络安全要求，以保护非公开金融数据，其中包括关于书面政策、风险评估活动和网络安全方案设计的具体规定。

同时，《纽约州劳动法》规定，雇主负有防止非法披露其员工个人信息的一般义务。并且，纽约州法律还禁止为任何商业目的出售或发布学生信息。

（5）新泽西州

不同于加州，新泽西州未设通用隐私法，但设有针对具体行业的隐私法。例如，新泽西州颁布了《新泽西州遗传隐私法》，根据该法，收集个人遗传信息必须基于个人的知情同意，但在某些有限的情况下除外，如刑事调查和起诉。新泽西州的《防止身份盗窃法》禁止个人或企业公开披露个人社会安全号码的四个或四个以上的连续数字。

（6）佐治亚州

佐治亚州未制定通用隐私法，但设有针对具体行业的隐私法。如佐治亚州制定的《学生数据隐私、可访问性和透明度法案》对幼儿园至高中以及高中以上学生的数据进行保护。

（7）内华达州

内华达州制定了网络隐私法，规定消费者有权选择拒绝出售其个人数据。

（8）弗吉尼亚州消费者数据保护法（VCDPA）

弗吉尼亚州消费者数据保护法（VCDPA）是一项综合隐私法，即将于 2023 年 1 月 1 日开始由弗吉尼亚州总检察长（AG）执行。总检察长可以申请高达 7，500 美元的单次违规赔偿。VCDPA 为弗吉尼亚州消费者提供各种隐私权保护。受 VCDPA 监管的企业对这些消费者负有多项关键义务，包括提供披露，以类似方式响应通用数据保护条例（GDPR）消费者数据主体请求（DSR），以及遵守某些数据处理义务（例如，数据最小化原则，负责任的数据保全措施）。

F.3 其他国家的政策和法律

（1）澳大利亚

信息安全注册评估（IRAP）由澳大利亚网络安全中心（ACSC）管理，为针对澳大利亚政府政策和指南的独立评估系统安全提供了一个综合流程。IRAP 的目标是通过专注于存储、处理和传达信息的信息技术基础结构，最大限度地提高澳大利亚联邦、州以及当地政府数据的安全性。IRAP 提供了一个框架，用于认可来自私有和公共部门的个人，以便向澳大利亚政府提供网络安全评估服务，搭建了根据澳大利亚政府政策和指南对系统安全进行独立评估的综合流程。IRAP 的目标是通过专注于存储、处理和传达信息的信息技术基础结构，最大限度地提高澳大利亚联邦、州以及当地政府数据的安全性。

1988 年，与个人信息保护有关的澳大利亚《隐私法》颁布，该法适用于在澳大利亚处理个人信息的私人组织和大多数联邦政府机构，包括在澳大利亚开展业务过程中在澳大利亚处理个人信息的外国公司。针对澳大利亚人开展营销和与澳大利亚客户进行重复交易的外国公司可能被视为“在澳大利亚开展业务”。《隐私法》中没有数据控制者或数据处理者的概念，因而“数据控制者”和“数据处理者”之间没有责任或义务分配。为《隐私法》能够更好地实施，澳大利亚信息专员办公室制

定了相关指南，对有关数据安全等具体问题进行解释和指引。此外，澳大利亚还对某些与数据安全相关的行业部门，如金融服务、电信服务和医疗服务等，规定了额外的数据保护义务。

2018 年 2 月，澳大利亚正式实施隐私法修正案《数据泄露通知计划》。

（2）日本

2005 年 4 月 1 日，日本实施《个人信息保护法》(Act on the Protection of Personal Information, APPI)，该法在 2015 年、2020 年和 2021 年经过三次重大修订。现行 APPI 共八章，旨在就个人信息的正当处理，对其基本理念、政府制定的基本方针以及其他个人信息保护措施的基本事项作出规定，对国家及地方公共团体的职责等予以明确。同时，对个人信息处理业者应遵守的义务等作出规定，并设置了个人信息保护委员会（PPC）对个人信息处理者的行为进行统一监管，期在确保个人信息有效利用的同时，对个人的权利和利益加以保护。

在网络安全方面，2000 年《保护信息系统免受网络攻击行动计划》是日本在该领域首个政策文件，2013 年《网络安全战略》、2014 年《网络安全基本法》、2015 年《网络安全战略（第二版）》、2018 年《网络安全战略（第三版）》、2022 年，日本发布《网络安全战略》，构建了网络空间相关的法律框架，致力于构建“自由、公平、安全的网络空间”。

日本在跨境数据流动方面，限制性条件相对较少，只对涉及国家安全的敏感或关键数据进行监管。日本在参与多边和双边跨境协定谈判中更加务实，通过“大阪轨道”实现可信数据自由流动倡议。一方面，日本积极跟随美国的政策主张，参与 CBPR 体系；另一方面，日本积极对接 GDPR 框架，同时制定弥补差异的补充规则。日本推动美日欧三方建立数据安全联盟，旨在促进具有相当水平的数据安全和隐私保护的国家之间的数据有序流动，并且通过这种方式来限制中国的竞争优势。

（3）阿根廷

2000 年，阿根廷《个人数据保护法》生效，适用于阿根廷境内及互联网上的任何阿根廷个人数据处理，用以帮助保护个人数据隐私，并为用户提供对存储在公用和专用数据库和注册表中的任何信息的访问权限。

2022 年 11 月 10 日，阿根廷数据保护局公布了更新《个人数据保护法》的法案草案，此次更新旨在保护信息社会中的个人数据提供必要保障和建立促进阿根廷创新和经济发展的明确规则的决定性步骤。

（4）新加坡

新加坡《个人数据保护法》(PDPA)于 2014 年生效。随着时间的推移，最近一次修法是在 2021 年。该法现在包含了更具保护力的同意框架与更明确的离岸数据传输规则，新加坡使得其成为东南亚最严格的数据保护国家之一。PDRA 是新加坡最重要的数据保护法，内容包括明确了在新加坡境内收集、使用、披露和管理个人数据的要求。该法承认了个人保护其数据的各项权利，包括数据获取权和数据更正权，同时也承认了企业基于合理目的收集、使用和披露个人数据的需要。《2021 年个人数据保护条例》（PDPR）对 PDPA 进行了完善，该条例明确了个人保护其数据的各项权利，包括数据获取权和数据修改权，同时也承认了企业基于合理目的收集、使用和披露个人数据的需要，规定了个人信息的知情权或更正权行使的形式、方式和程序，以及明确可披露已故人士个人信息的权利人。

（5）韩国

2011 年 3 月 29 日，韩国颁布《个人信息保护法》（Personal Information Protection Act，PIPA），该法作为一部具有统一性、一般性和综合性的个人数据保护法律，对个人信息保护的基本原则、信息主体的权利以及信息的利用、收集等规则进行了规定。具体而言，PIPA 明确了数据跨境流动的多种渠道，建立了隐私政策审查机制，并引入了数据可携带权、对于自动化决策的拒绝权和解释权等多项权利。PIPA 规定，个人信息保护委员会（PIPC）是负责数据保护的主要机构，同时，韩国互联网与安全局（KISA）为接收个人信息泄露报告的专属机构。

2013 年，韩国实施《促进提供和使用公共数据法》，对有关提供公共机构持有和管理的数据以及激活其使用的事项进行了规定，强调公共机构主动公开数据，以促进数据的流通和使用，旨在实现“数字政府 3.0 运动”的目标。

2022 年，韩国实施《数据产业振兴和利用促进基本法》，以保护具有特定经济价值的数据，是全球首部规制数据产业的立法，内容涉及数据政策委员会的设立、数据经济商的培养以及相关争端解决机制的建立等内容。