

数据安全与治理

陈 庄 邹 航 张晓琴 编著
张峻峰 黄远江 刘红兵

清华大学出版社
北 京

内 容 简 介

本书密切结合我国大数据产业、数据安全产业的特点,全面系统地介绍了数据安全与治理的内涵、特点、方法、原理与技术。全书分为10章。其中,第1章介绍了数据安全与治理的基本概念,第5、6、7、9章介绍了数据安全的相关技术(含数据加密、数据脱敏、数据资产保护、数据审计),第3、4章介绍了数据治理的相关技术(含数据质量管控、数据采集),第2、8、10章介绍了数据安全治理的相关技术(含数据分类分级、数据资产交易、数据司法存证)。

本书在每章末均配置了复习题,在全书最后附有模拟试卷,题型包括单选题、多选题、判断题、简答题和论述题,以帮助读者检验其对知识点的掌握情况。

本书可作为高等学校大数据科学、大数据技术、大数据管理与应用、网络安全等相关专业本科生、研究生的教材或教学参考书,也可作为网络安全管理机构、信息产业管理部门相关管理人员的业务工作参考资料,还可作为大数据应用开发企业、数据安全企业的从业人员的培训教材。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

版权所有,侵权必究。举报:010-62782989, beiqinquan@tup.tsinghua.edu.cn。

图书在版编目(CIP)数据

数据安全与治理 / 陈庄等编著. —北京:清华大学出版社, 2022.6

ISBN 978-7-302-60353-5

I . ①数… II . ①陈… III . ①数据处理—安全技术 IV . ①TP274

中国版本图书馆 CIP 数据核字 (2022) 第 042234 号

责任编辑:高 岫

封面设计:周晓亮

版式设计:方加青

责任校对:马遥遥

责任印制:沈 露

出版发行:清华大学出版社

网 址: <http://www.tup.com.cn>, <http://www.wqbook.com>

地 址:北京清华大学学研大厦 A 座 邮 编:100084

社 总 机:010-83470000 邮 购:010-62786544

投稿与读者服务:010-62776969, c-service@tup.tsinghua.edu.cn

质 量 反 馈:010-62772015, zhiliang@tup.tsinghua.edu.cn

印 刷 者:北京富博印刷有限公司

装 订 者:北京市密云县京文制本装订厂

经 销:全国新华书店

开 本:185mm×260mm 印 张:15.5 字 数:367千字

版 次:2022年6月第1版 印 次:2022年6月第1次印刷

定 价:49.80元

产品编号:095020-01

前言

随着数字经济的快速发展，全球进入数据爆炸时代，数据在社会经济、民众生活中扮演着越来越重要的角色，并成为继土地、劳动力、资本、技术之后的第五大生产要素，成为政府、企事业单位的重要资产。

然而，数据成为资产是有前置条件的；否则，数据不仅不能释放出其资产价值，还有可能成为一种负担或负债。

数据成为资产的重要前置条件是数据治理能力强，主要体现在三个方面：一是数据本身的质量高，即数据具有完整性、及时性、准确性、一致性、唯一性、有效性等；二是数据权属机构要有系统的数据全生命周期管理策略，包括数据采集管理、数据存储管理、数据传输管理、数据处理管理、数据交换管理、数据销毁管理等；三是数据治理相关“政用产学研”机构要有科学的数据资产变现的数据运营商业模式，如数据资产确权、数据资产定价、数据资产监管、数据资产交易等。

数据成为资产的另一个前提条件是数据安全水平高，主要体现在两个方面：一是数据权属单位、数据运营公司、数据交易平台等数据相关机构必须遵守国家法律法规框架下开展数据管理、数据运营、数据交易等工作，即这些数据机构必须遵守《中华人民共和国数据安全法》《中华人民共和国密码法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》等数据安全的法律法规，且能经得起数据安全监管部门的网络安全审查，不能踩法律的黄线或红线；二是数据机构应该采用相应的数据安全技术（如数据分类分级技术、数据加密技术、数据脱敏技术、数据审计技术、数据司法存证技术等），确保数据全生命周期安全。

为了适应大数据产业、数据安全产业的发展形势，满足大数据专业、网络安全专业人才培养需求，我们组织了在数据安全治理领域具有丰富理论功底和实践经验的“产学研”团队，结合我们自身的研究成果，融合国内外学者近年来有关数据安全治理方面的研究论著和标准规范，编写了著作《数据安全与治理》，以期提升高校学生、研发机构、社会公众的数据安全治理意识，促进数据资产要素沿着安全之路快速健康发展。

本书密切结合我国大数据产业、数据安全产业的特点，全面系统地介绍了数据安全与治理的内涵、特点、方法、原理与技术。全书分为10章。其中，第1章介绍了数据安全与治理的基本概念，第5、6、7、9章介绍了数据安全的相关技术，第3、4章介绍了数据治理的相关技术，第2、8、10章介绍了数据安全治理的相关技术。

本书在每章末均配置了复习题，题型包括单选题、多选题、判断题、简答题和论述

题，以帮助读者检验其对每章知识点了解的情况；在全书最后精心编制了两套模拟试卷，以供读者综合测试其对知识的掌握情况。

本书免费配备了丰富的教学资源，包括电子课件和习题答案，可扫描右侧二维码获取。



教学资源

本书第1、2、4、5、8章由陈庄编写，第3章由黄远江编写，第6章由邹航编写，第7章由张峻峰编写，第9章由张晓琴编写，第10章由刘红兵编写，每章复习题及模拟试卷由陈庄编配，全书由陈庄总纂。

本书在编写过程中参考了大量文献，并尽可能详尽地罗列在每章后的参考文献中，但仍难免有遗漏，谨向被漏列的作者表示歉意，并向所有的作者表示诚挚的感谢；同时，还要感谢陈庄教授指导的重庆理工大学研究生王士伟、蔡明甸、丘嘉豪、赵源、王志坤、汪盼等同学，以及重庆邮电大学的研究生刘印全、张鑫、杨楚雄等同学，他们在收集文献资料、绘制插图初样、撰写部分章节初稿等方面做出了贡献。

本书可作为高等学校大数据科学、大数据技术、大数据管理与应用、网络安全等相关专业本科生、研究生教材或教学参考书，也可作为网络安全管理机构、信息产业管理部门相关管理人员的业务工作参考资料，还可作为大数据应用开发企业、数据安全企业的从业人员的培训教材。

由于作者水平有限，时间仓促，本书不妥之处在所难免，敬请读者批评指正。

编者
2022年4月

目 录

第 1 章 绪论	1
1.1 数据的概念	1
1.1.1 数据的定义及特征	1
1.1.2 数据的类别	2
1.1.3 数据的度量方法	4
1.1.4 数据、信息、知识、智慧之间的关系	4
1.2 数据安全的概念	5
1.2.1 数据安全的定义	5
1.2.2 数据安全的范围	5
1.2.3 数据安全 PA 体系	5
1.3 数据治理的概念	8
1.3.1 数据治理的定义	8
1.3.2 数据治理的特征	8
1.3.3 数据治理的体系结构	9
1.4 数据安全治理的概念	12
1.4.1 数据安全治理的定义	12
1.4.2 数据安全治理的本质	12
1.4.3 数据安全治理与传统数据安全的区别	13
1.4.4 数据安全治理体系	13
1.5 概念间的逻辑关系及本书框架结构	14
1.5.1 概念间的逻辑关系	14
1.5.2 本书框架结构	15
参考文献	16
复习题	16
第 2 章 数据分类分级技术	20
2.1 数据元素的概念	20

2.2	数据分类的概念、原则及方法	21
2.2.1	数据分类的概念	21
2.2.2	数据分类的基本原则	21
2.2.3	数据分类的基本方法	22
2.2.4	数据分类综合案例：铁路大数据分类	25
2.3	数据分级的概念、原则及方法	27
2.3.1	数据分级的概念	27
2.3.2	数据分级的基本原则	27
2.3.3	数据分级的基本流程	28
2.3.4	数据分级的基本方法	29
2.3.5	数据分级案例：金融数据分级	33
2.4	数据分类分级综合案例：个人信息分类分级	33
2.4.1	个人信息分类分级概述	33
2.4.2	个人信息分类分级结果	34
	参考文献	37
	复习题	37
第3章	数据质量管控技术	40
3.1	数据质量的概念	40
3.1.1	数据质量的定义	40
3.1.2	数据质量控制框架	40
3.1.3	数据质量问题产生的原因	41
3.1.4	数据质量管控的重要性	43
3.2	数据质量监控规则	44
3.2.1	完整性监控规则	44
3.2.2	及时性监控规则	44
3.2.3	准确性监控规则	45
3.2.4	一致性监控规则	45
3.2.5	唯一性监控规则	45
3.2.6	有效性监控规则	45
3.2.7	监控规则的技术实现方法	46
3.3	数据质量评价技术	50
3.3.1	数据质量评价方法	50
3.3.2	数据质量指标计算方法	50
3.4	数据质量管控技术	52
3.4.1	数据采集阶段	53
3.4.2	数据存储阶段	53

3.4.3 数据处理阶段	54
3.4.4 数据应用阶段	55
3.5 数据质量管控案例	56
3.5.1 项目背景介绍	56
3.5.2 大数据平台数据架构	56
3.5.3 数据质量管控技术实施	57
参考文献	59
复习题	59
第 4 章 数据采集技术	62
4.1 数据采集的概念	62
4.1.1 数据采集的定义	62
4.1.2 数据采集的原则	63
4.2 数据源	64
4.2.1 个人数据	64
4.2.2 组织数据	64
4.2.3 实体数据	65
4.2.4 数据库数据	65
4.2.5 网络数据	66
4.2.6 文献数据	66
4.3 数据采集技术简介	67
4.3.1 数据采集技术的分类	67
4.3.2 人工采集技术	67
4.3.3 半人工采集技术	71
4.3.4 自动采集技术	72
4.4 数据采集质量控制技术	74
4.4.1 数据采集质量控制原则	74
4.4.2 数据采集质量控制模式	74
4.4.3 数据采集质量评价方法	75
4.5 数据采集安全控制策略	75
4.5.1 数据采集安全控制要求	75
4.5.2 数据采集安全控制策略	76
4.6 数据采集综合案例：汽车数据采集及其安全控制策略	77
参考文献	78
复习题	79

第 5 章 数据加密技术	82
5.1 数据加密的相关概念	82
5.1.1 数据加密的概念	82
5.1.2 数据加密技术的组成	83
5.1.3 数据加密技术的作用	85
5.2 国外主要数据加密算法	85
5.2.1 DES 对称加密算法	85
5.2.2 AES 对称加密算法	87
5.2.3 RSA 非对称加密算法	88
5.2.4 MD5 散列算法	89
5.2.5 SHA1 散列算法	90
5.2.6 SHA2 散列算法	91
5.3 国内主要数据加密算法	92
5.3.1 SM2 公钥密码算法	93
5.3.2 SM3 散列算法	96
5.3.3 SM4 分组密码算法	97
5.3.4 SM9 椭圆加密算法	100
5.4 数据加密综合案例：商用密码技术在某政务系统中的应用	107
5.4.1 背景与现状	107
5.4.2 密码应用需求	109
5.4.3 密码应用技术框架	110
5.4.4 密码应用部署	112
参考文献	114
复习题	115
第 6 章 数据脱敏技术	118
6.1 数据脱敏的概念	118
6.1.1 数据脱敏的定义	118
6.1.2 数据脱敏的原则	118
6.1.3 数据脱敏的流程	119
6.1.4 数据脱敏与数据匿名化、数据去标识化间的关系	120
6.2 数据脱敏的类别	121
6.2.1 结构化数据脱敏	121
6.2.2 非结构化数据脱敏	122
6.3 敏感数据识别策略	123
6.3.1 敏感数据识别的概念	123

6.3.2	敏感数据源识别策略	124
6.3.3	敏感数据识别策略	124
6.4	数据脱敏方法	124
6.4.1	数据脱敏方法的类别	124
6.4.2	经典数据脱敏方法简介	125
6.4.3	现代隐私保护方法简介	127
6.5	数据脱敏产品及应用案例	129
6.5.1	数据脱敏产品总体架构	129
6.5.2	数据脱敏产品应用部署	132
6.5.3	数据脱敏产品在金融系统中的应用案例——某银行客户隐私数据 脱敏策略	133
	参考文献	134
	复习题	135
第 7 章	数据资产保护技术	138
7.1	数据资产的概念	138
7.1.1	数据资产的定义	138
7.1.2	数据资产的特征	139
7.1.3	数据资产的要素	140
7.2	数据资产管理的概念	140
7.2.1	数据资产管理的定义	140
7.2.2	数据资产管理的基本原则	141
7.3	数据资产管理策略	141
7.3.1	数据资产识别策略	142
7.3.2	数据资产确权策略	142
7.3.3	数据资产应用策略	142
7.3.4	数据资产盘点策略	142
7.3.5	数据资产变更策略	143
7.3.6	数据资产处置策略	143
7.4	数据资产价值评估技术	144
7.4.1	数据资产评估方法	144
7.4.2	数据资产评估体系	145
7.5	数据资产安全保护技术	150
7.5.1	数据资产安全保护的概念	150
7.5.2	数据资产安全保护权属体系	151
7.5.3	数据资产安全保护技术体系	153
7.6	数据资产保护综合案例：面向双碳服务平台的数据资产安全保护技术	153

7.6.1	双碳服务平台简介	153
7.6.2	双碳服务平台涉及的数据资产	154
7.6.3	面向双碳服务平台的数据资产安全保护系统	155
	参考文献	157
	复习题	158
第 8 章	数据资产交易技术	161
8.1	数据资产交易的概念	161
8.1.1	数据资产交易的定义	161
8.1.2	数据资产交易的主要特点	161
8.1.3	数据资产交易面临的问题	163
8.2	数据资产确权	164
8.2.1	数据资产确权的概念	165
8.2.2	数据资产确权的原则及路径	166
8.2.3	数据资产确权的方法	168
8.3	数据资产定价	169
8.3.1	数据资产定价的概念	169
8.3.2	数据资产定价的方法	170
8.3.3	数据资产定价案例	172
8.4	数据资产交易监管	173
8.4.1	数据资产交易监管的概念	173
8.4.2	数据资产交易监管原则	174
8.4.3	数据资产交易监管模式	174
8.4.4	数据资产交易监管内容	175
8.5	数据资产交易平台	178
8.5.1	数据资产交易平台的概念	178
8.5.2	数据资产交易平台的总体架构	179
	参考文献	181
	复习题	182
第 9 章	数据审计技术	186
9.1	数据审计的概念与作用	186
9.1.1	数据审计的背景	186
9.1.2	数据审计的概念	187
9.1.3	数据审计的作用	188
9.2	数据库审计技术	189

9.2.1	数据库审计的数据采集	189
9.2.2	数据库审计的事件审计	190
9.2.3	数据库审计的统计分析	191
9.3	主机审计技术	191
9.3.1	主机审计的数据采集	191
9.3.2	主机审计的事件审计	192
9.3.3	主机审计的统计分析	193
9.4	网络审计技术	193
9.4.1	网络审计的数据采集	193
9.4.2	网络审计的事件审计	195
9.4.3	网络审计的统计分析	195
9.5	应用审计技术	196
9.5.1	应用审计的数据采集	196
9.5.2	应用审计的事件审计	197
9.5.3	应用审计的统计分析	197
9.6	数据审计应用案例：面向高校校园网的网络审计系统	198
	参考文献	199
	复习题	200
第 10 章	数据司法存证技术	203
10.1	数据司法存证的概念	203
10.1.1	数据司法存证的背景	203
10.1.2	数据司法存证的定义	204
10.1.3	数据司法存证的基本原则	205
10.2	数据司法存证的基本要求	206
10.2.1	数据司法存证的总体要求	206
10.2.2	数据司法存证的具体要求	206
10.3	第三方数据存证平台	208
10.3.1	第三方数据存证平台的类别	208
10.3.2	第三方数据存证平台的基本功能	208
10.3.3	第三方数据存证平台的安全要求	211
10.3.4	第三方数据存证平台的相关技术简介	211
10.4	数据存证的司法实践	213
10.4.1	数据存证的法律效力	213
10.4.2	数据存证的司法证明力	215
10.4.3	数据存证的应用模式：以小贷业务为例	216
10.4.4	数据存证的主要应用场景	217

10.5 数据存证案例	219
10.5.1 知识产权案例	219
10.5.2 金融借贷案例	219
10.5.3 网络诈骗案例	220
参考文献	220
复习题	221
附录	224
附录 A 模拟试卷(一)	224
附录 B 模拟试卷(二)	230

第 1 章

绪 论

数据安全与治理是近年来大数据行业、网络安全行业交叉领域的新研究方向，涉及诸多新概念、新术语。本章将重点介绍数据、数据安全、数据治理、数据安全治理涉及的相关概念。

1.1 数据的概念

1.1.1 数据的定义及特征

1. 数据的定义

《中华人民共和国数据安全法》于 2021 年 6 月 10 日颁布，并于 2021 年 9 月 1 日正式实施。《中华人民共和国数据安全法》给出的数据定义是目前最权威的定义。本书采用该定义：数据是指任何以电子或者其他方式对信息的记录。

2. 数据的特征

数据定义所揭示的是数据的本质属性，但数据还存在许多由本质属性派生出来的相关特征，如普遍性、价值性（资产性）、共享性、交换性、时效性（实时性）、等级性（敏感性）等。

(1) 普遍性

数据的普遍性是指数据无处不在、无时不在。

数据普遍存在于自然界、经济社会中，无论是自然界的鸟语花香、风雨雷鸣、地震海啸，还是社会经济活动中的语言文字、机械工艺、建筑工程等，均可用数据来呈现。

(2) 价值性（资产性）

数据的价值性，又称资产性，指数据是一种类似土地、劳动力、资本、技术的有价值的资产。

数据是其权属机构（企事业单位）的重要资产，可通过数据交易平台进行交易，能为其权属机构带来丰厚的经济效益。

(3) 共享性

数据的共享性是指数据可由不同个体或群体（机构）在同一时间或不同时间共同享用。

数据只有进行了共享，其资产价值才能充分体现出来，才能避免“数据烟囱”“数据孤岛”现象，才能真正体现“体系化数据”对“科学决策”的重要支撑。

(4) 交换性

数据的交换性是指不同个体或机构之间将其权属数据互相进行交换。

数据交换与实物交换是有本质区别的：实物交换，一方有所得，必使另一方有所失；而数据在交换过程中，其原有数据一般不会丧失，而且还有可能同时获得新的数据。正是由于数据的交换性特点，才使数据生生不息，形成当今的数字经济态势。

(5) 时效性(实时性)

数据的时效性，又称实时性，是指数据具有时间特征。

数据时效性包括三层含义：一是指“数据产生→数据记录”的时间间隔，即传感设备或人工采集/更新数据的时间，该时间越短，其实时性就越高。二是指“数据记录→数据传递→数据处理→数据利用”的时间及其效率，该时间越短且其使用程度越高，其时效性越强。三是数据价值与数据所处的时间长度成反比，数据一经生成(记录)，其反映的内容越新，它的价值越大；反之，时间越长，其价值随之减小，一旦超过其“生命周期”，价值就会消失。

(6) 等级性(敏感性)

数据的等级性，又称敏感性，是指数据的敏感程度及其保护级别。

数据的等级性主要有两个作用：一是满足网络安全监管部分的数据安全审查；二是避免敏感数据的泄露。一般地，数据的等级可分为绝密级、机密级、秘密级、核心商密级、普通商密级、内部级、公开级等，也可按数据级别的高低分为 $n \sim 1$ 级。

1.1.2 数据的类别

依照数据的定义，按照不同的分类标准，数据可以划分为不同的类别。例如，从宏观的社会经济视角，按数据来源的不同可分为自然数据和社会数据两类；按数据记录内容的不同可分为经济数据、政务数据、文教数据、科技数据、管理数据、军事数据六类；按数据加工深度的不同可分为一次文献数据、二次文献数据、三次文献数据三类。图 1-1 所示为数据的类别。以下简要说明各类数据的基本内涵或特征。

(1) 自然数据

自然数据指自然界产生的各种数据，如山川、动植物、天体的状态与属性的记录。自然数据是认识自然界的媒介，人类利用这些数据开发利用自然物质，为人类社会创造财富，保护自然环境，改善生存条件。

(2) 社会数据

社会数据有两种解释：一种是指人类社会记录的各种事物的数据，如政治、经济、文化等社会活动；另一种是指投入社会交流的各种数据，有人类社会产生的，也有自然界产生的。社会数据都是用人类创造的各种符号表述和传递的，即经过人的思想加工，进入社会交流的各种数据。

(3) 经济数据

经济数据指经济活动中形成的数据，如国家经济政策法规、新技术开发与应用、生产销售、劳动人事、商业贸易、金融市场等数据。

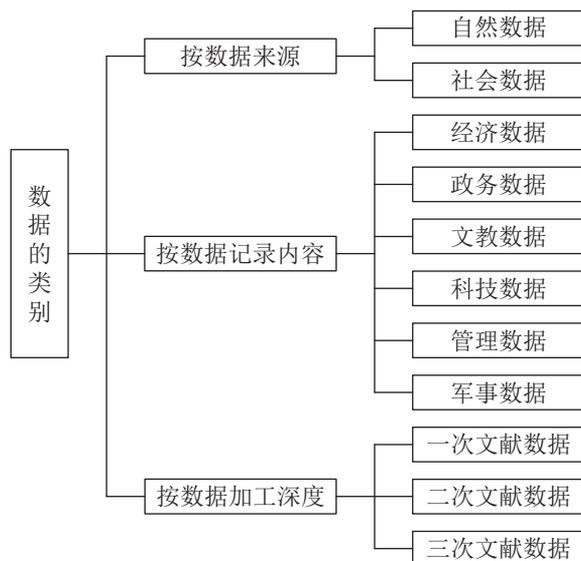


图 1-1 数据的类别

(4) 政务数据

政务数据指政府机关活动产生的数据，如方针政策、法规条令、政府决议、公报条约、国际交往、社会状况及日常活动等数据。

(5) 文教数据

文教数据指文教活动中形成的数据，如教育、体育、文学、艺术、出版发行等数据。

(6) 科技数据

科技数据指科学与技术活动中形成的数据，如科学技术成果、科研技术文献、知识产权等数据。

(7) 管理数据

管理数据指各种行业各个层次管理与决策活动中产生的数据，如人事、工资、计划、调度、财务、统计等内部与外部数据。

(8) 军事数据

军事数据指国防、战争等与军事活动有关的数据，如国防及军队的现代化建设、武器研制、战略战术研究、部队管理及作战等数据。

(9) 一次文献数据

一次文献数据指一切原始的数据，如决议、报告、记录、心得、经验、消息、创作、研究成果等数据。

(10) 二次文献数据

二次文献数据指对原始文献信息加工处理后的数据，如卡片、目录、索引、文摘等数据。

(11) 三次文献数据

三次文献数据指通过二次文献数据提供的线索，对某一范围内的一次文献信息进行分析、研究而加工生成的第三个层次的文献数据，如综述、述评、专题研究报告、百科全书等数据。

1.1.3 数据的度量方法

一般地，用来度量数据的度量方法是：按数据所占用计算机存储空间的大小进行度量。常用的存储单位有 bit(比特或位)、B(Byte, 字节)、KB(Kilobyte, 千字节)、MB(Megabyte, 兆字节)、GB(Gigabyte, 吉字节)、TB(Terabyte, 太字节)、PB(Petabyte, 拍字节)、EB(Exabyte, 艾字节)，其间的换算关系如下。

$$\begin{aligned} 1\text{B} &= 8 \text{ bit} & 1\text{KB} &= 2^{10}\text{B} = 1024\text{B} \approx 10^3\text{B} \\ 1\text{MB} &= 10^6\text{B} & 1\text{GB} &= 10^9\text{B} \\ 1\text{TB} &= 10^{12}\text{B} & 1\text{PB} &= 10^{15}\text{B} \\ 1\text{EB} &= 10^{18}\text{B} \end{aligned}$$

1.1.4 数据、信息、知识、智慧之间的关系

数据、信息、知识、智慧是数字经济时代的 4 个重要概念，它们之间既有联系，又有区别，人们对其既熟悉又容易混淆。通俗地讲，这 4 个概念可以解释如下。

- 数据是原始的、未解释的符号，是信息的记录。例如，日期、温度、流量、PM2.5 等。
- 信息是经过加工的、有意义的数，是数据间关系。例如，明日高温、后天有雾等。
- 知识是含有观点、发挥作用的信息，是对信息的理解。例如，高温防暑、雾大少驾等。
- 智慧是综合经验、进行创新的知识，是知识的运用。例如，厚德载物、难得糊涂等。

依据上述解释，数据、信息、知识、智慧之间的关系可由图 1-2 来描述。图中，若按其对社会的重要程度，其间的逻辑关系是：数据 ≤ 信息 ≤ 知识 ≤ 智慧；若按其数量多少情况，其间的逻辑关系是：数据 ≥ 信息 ≥ 知识 ≥ 智慧。

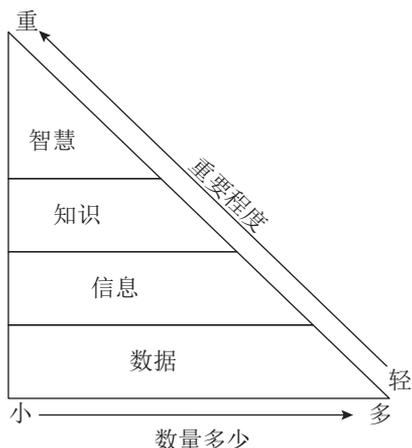


图 1-2 数据、信息、知识、智慧之间的关系

1.2 数据安全的概念

1.2.1 数据安全的定义

从技术角度，根据国家标准《信息安全技术 数据安全能力成熟度模型》(GB/T 37988—2019)，数据安全的定义是：通过管理和技术措施，确保数据有效保护和合规使用的状态。

从法律角度，根据《中华人民共和国数据安全法》，数据安全的定义是：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。

1.2.2 数据安全的范围

按照数据全生命周期过程，数据安全的范围包括数据采集、数据传输、数据存储、数据处理、数据交换、数据销毁 6 个数据过程阶段的安全。

- 数据采集阶段：是指组织内部系统中新产生数据及从外部系统收集数据的阶段。
- 数据传输阶段：是指数据从一个实体传输到另一个实体的阶段。
- 数据存储阶段：是指数据以任何数字格式进行存储的阶段。
- 数据处理阶段：是指组织在内部对数据进行计算、分析、可视化等操作的阶段。
- 数据交换阶段：是指组织与组织或个人进行数据交换（或交易）的阶段。
- 数据销毁阶段：是指对数据及数据存储媒体通过相应的操作手段，使数据彻底删除且无法通过任何手段恢复的阶段。

1.2.3 数据安全 PA 体系

按照国家标准《信息安全技术 数据安全能力成熟度模型》(GB/T 37988—2019)，数据安全 PA(Process Area, 过程域) 体系分为数据生存周期安全过程域和通用安全过程域两部分，共包含 30 个 PA。其中，数据生存周期安全过程域即为上述数据生命周期的 6 个数据过程阶段的安全，本书将其称之为数据生命周期安全过程域或数据生命周期安全，如图 1-3 所示。以下简要说明每一个过程域的内涵。

数据生命周期安全过程域					
数据采集安全	数据传输安全	数据存储安全	数据处理安全	数据交换安全	数据销毁安全
<ul style="list-style-type: none"> ●PA01 数据分类分级 ●PA02 数据采集安全管理 ●PA03 数据源鉴别及记录 ●PA04 数据质量管理 	<ul style="list-style-type: none"> ●PA05 数据传输加密 ●PA06 网络可用性管理 	<ul style="list-style-type: none"> ●PA07 存储媒体安全 ●PA08 逻辑存储安全 ●PA09 数据备份和恢复 	<ul style="list-style-type: none"> ●PA10 数据脱敏 ●PA11 数据分析安全 ●PA12 数据正当使用 ●PA13 数据处理环境安全 ●PA14 数据导入导出安全 	<ul style="list-style-type: none"> ●PA15 数据共享安全 ●PA16 数据发布安全 ●PA17 数据接口安全 	<ul style="list-style-type: none"> ●PA18 数据销毁处置 ●PA19 存储媒体销毁处置
通用安全过程域					
●PA20 数据安全策略规划	●PA21 组织和人员管理	●PA22 合规管理	●PA23 数据资产管理	●PA24 数据供应链安全	●PA25 元数据管理
●PA26 终端数据安全	●PA27 监控与审计	●PA28 鉴别与访问控制	●PA29 需求分析	●PA30 安全事件应急	

图 1-3 数据安全 PA 体系

- PA01 数据分类分级：基于法律法规及业务需求确定组织内部的数据分类分级方法，对生成或收集的数据进行分类分级标识。
- PA02 数据采集安全管理：在采集外部客户、合作伙伴等相关方数据的过程中，组织应明确采集数据的目的和用途，确保满足数据源的真实性、有效性和最少够用等原则要求，并明确数据采集渠道、规范数据格式及相关的流程和方式，从而保证数据采集的合规性、正当性和一致性。
- PA03 数据源鉴别及记录：对产生数据的数据源进行身份鉴别和记录，防止数据仿冒和数据伪造。
- PA04 数据质量管理：建立组织的数据质量管理体系，保证对数据采集过程中收集/产生的数据的准确性、一致性和完整性。
- PA05 数据传输加密：根据组织内部和外部的数据传输要求，采用适当的加密保护措施，保证传输通道、传输节点和传输数据的安全，防止传输过程中的数据泄露。
- PA06 网络可用性管理：通过网络基础设施及网络层数据防泄露设备的备份建设，实现网络的高可用性，从而保证数据传输过程的稳定性。
- PA07 存储媒体安全：针对组织内需要对数据存储媒体进行访问和使用的场景，提供有效的技术和管理手段，防止对媒体的不当使用而可能引发的数据泄露风险。存储媒体包括终端设备及网络存储。
- PA08 逻辑存储安全：基于组织内部的业务特性和数据存储安全要求，建立针对数据逻辑存储、存储容器等的有效安全控制。
- PA09 数据备份和恢复：通过执行定期的数据备份和恢复，实现对存储数据的冗余管理，保护数据的可用性。
- PA10 数据脱敏：根据相关法律法规、标准的要求及业务需求，给出敏感数据的脱敏需求和规则，对敏感数据进行脱敏处理，保证数据可用性和安全性间的平衡。
- PA11 数据分析安全：通过在数据分析过程采取适当的安全控制措施，防止数据挖掘、分析过程中有价值信息和个人隐私泄露的安全风险。
- PA12 数据正当使用：基于国家相关法律法规对数据分析和利用的要求，建立数据使用过程的责任机制、评估机制，保护国家秘密、商业秘密和个人隐私，防止数据资源被用于不正当目的。
- PA13 数据处理环境安全：为组织内部的数据处理环境建立安全保护机制，提供统一的数据计算、开发平台，确保数据处理的过程中有完整的安全控制管理和技术支持。
- PA14 数据导入导出安全：通过对数据导入导出过程中对数据的安全性进行管理，防止数据导入导出过程中可能对数据自身的可用性和完整性构成的危害，降低可能存在的数据泄露风险。
- PA15 数据共享安全：通过业务系统、产品对外部组织提供数据时，以及通过合作的方式与合作伙伴交换数据，执行共享数据的安全风险控制，以降低数据共享场景下的安全风险。

- PA16 数据发布安全：在对外部组织进行数据发布的过程中，通过对发布数据的格式、适用范围、发布者与使用者权利和义务执行的必要控制，实现数据发布过程中数据的安全可控与合规。
- PA17 数据接口安全：通过建立组织的对外数据接口的安全管理机制，防范组织数据在接口调用过程中的安全风险。
- PA18 数据销毁处置：通过建立针对数据的删除、净化机制，实现对数据的有效销毁，防止因对存储媒体中的数据进行恢复而导致的数据泄露风险。
- PA19 存储媒体销毁处置：通过建立对存储媒体安全销毁的规程和技术手段，防止因存储媒体丢失、被窃或未授权的访问而导致存储媒体中的数据泄露的安全风险。
- PA20 数据安全策略规划：建立适用于组织数据安全风险状况的组织整体的数据安全策略规划，数据安全策略规划的内容应覆盖数据全生命周期的安全风险。
- PA21 组织和人员管理：通过建立组织内部负责数据安全工作的职能部门及岗位，以及对人力资源管理过程中各环节进行安全管理，防范组织和人员管理过程中存在的数据安全风险。
- PA22 合规管理：跟进组织须符合的法律法规要求，以保证组织业务的发展不会面临个人信息保护、重要数据保护、跨境数据传输等方面的合规风险。
- PA23 数据资产管理：通过建立针对组织数据资产的有效管理手段，从资产的类型、管理模式方面实现统一的管理要求。
- PA24 数据供应链安全：通过建立组织的数据供应链管理机制，防范组织上下游的数据供应过程中的安全风险。
- PA25 元数据管理：建立组织的元数据管理体系，实现对组织内元数据的集中管理。
- PA26 终端数据安全：基于组织对终端设备层面的数据保护要求，针对组织内部的工作终端采取相应的技术和管理方案。
- PA27 监控与审计：针对数据生命周期各阶段开展安全监控和审计，保证对数据的访问和操作均得到有效监控和审计，以实现数据生命周期各阶段中可能存在的未授权访问、数据滥用、数据泄露等安全风险的防控。
- PA28 鉴别与访问控制：通过基于组织的数据安全需求和合规性要求，建立身份鉴别和数据访问控制机制，防止对数据的未授权访问风险。
- PA29 需求分析：通过建立针对组织业务的数据安全需求分析体系，分析组织内数据业务的安全需求。
- PA30 安全事件应急：建立针对数据的安全事件应急响应体系，对各类安全事件进行及时响应和处置。

1.3 数据治理的概念

1.3.1 数据治理的定义

数据治理 (data governance) 的概念源于企业的公司治理, 旨在保护其数据资产, 发挥其数据价值, 提高其市场竞争力。

国际多个数据治理知名企业 (机构) 均从自身从事的专业领域给出数据治理定义。例如: IBM 认为, 数据治理是指根据企业的管控政策, 利用组织人员、流程和技术相互协作, 使企业能将数据作为企业的核心资产来管理和应用; DAMA 认为, 数据治理是指对数据资产管理行使权力和控制的活动集合; Informatica 认为, 数据治理是指在组织范围内, 通过对流程、政策、标准、技术和人员进行职能协调和定义来将数据作为公司资产进行管理, 从而实现准确、一致、安全且及时的数据的可用性管理和可控增长, 以此制定更好的业务决策, 降低风险并改善业务流程。

目前, 国家标准《信息技术服务 治理 第5部分: 数据治理规范》(GB/T 34960.5—2018) 给出的数据治理定义是: 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。

1.3.2 数据治理的特征

数据治理的特征主要体现在基本要求、总体目标、主要任务三个方面。

1. 基本要求

数据治理应满足三个基本要求, 即行业监管要求、企业商业要求、管理体系要求。

- 行业监管要求: 数据治理应满足国家法律法规、行业监管部门的安全合规要求。
- 企业商业要求: 数据治理应满足企业的商业化要求, 包括数据产品化、数据资产化、数据价值化等要求。
- 管理体系要求: 数据治理应满足企业的数据生命周期管理体系及应用体系要求, 包括数据架构、数据模型、数据标准、数据质量、数据安全等体系建设要求。

2. 总体目标

数据治理的总体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。

- 运营合规: 建立符合法律法规和行业监管的数据运营管理体系, 保障数据及其应用的合规。
- 风险可控: 建立数据风险管控机制, 确保数据及其应用满足风险偏好和风险容忍度。
- 价值实现: 构建数据价值实现体系, 促进数据资产化和数据价值实现。

3. 主要任务

数据治理的任务是分析现状需求, 落地实施策略, 评估实施效果。

- 分析现状需求: 分析数据治理环境、数据资源现状、数据资产运营能力等。

- 落地实施策略：构建数据治理体系，制订数据治理方案、实施数据治理策略。
- 评估实施效果：制定数据治理评价体系、审计规范，评估数据治理的实施效果。

1.3.3 数据治理的体系结构

数据治理的体系结构如图 1-4 所示，它主要由顶层设计和核心治理领域构成。

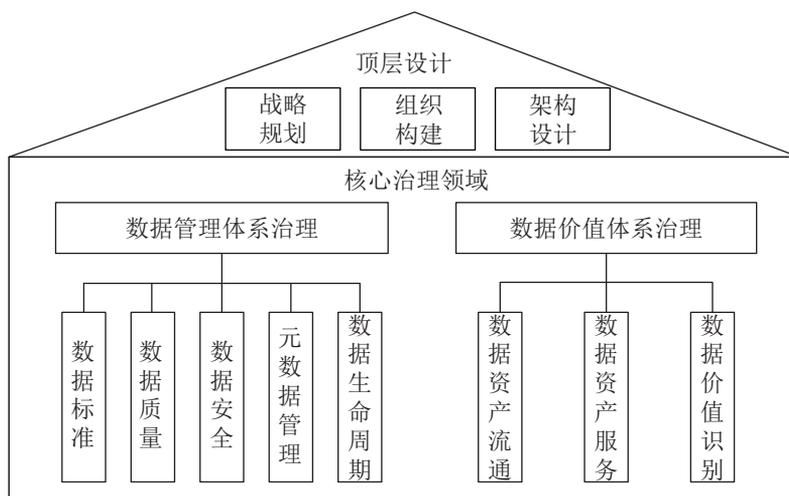


图 1-4 数据治理的体系结构

1. 顶层设计

顶层设计包括战略规划、组织构建、架构设计等工作内容。

(1) 战略规划

- 理解业务规划和信息技术规划，调研需求并评估数据现状、技术现状、应用现状和环境。
- 制定数据战略规划，包括（不限于）愿景、目标、任务、内容、边界、环境和蓝图等。
- 指导数据治理方案的建立，包括（不限于）实施主体、责权利、技术方案、管控方案、实施策略、实施路线等，同时，明确数据管理体系和数据价值体系。
- 明确风险源、符合性、绩效和审计等要求，监控和评价数据治理的实施并持续改进。

(2) 组织构建

- 建立支撑数据战略的组织机构和机制，明确相关的实施原则和策略。
- 构建决策和实施机构，设立岗位并明确角色，确保责权利的一致。
- 建立相关的授权、决策和沟通机制，保证利益相关方理解、接受相应的职责和权利。
- 实现决策、执行、控制和监督等职能，评估运行绩效并持续改进和优化。

(3) 架构设计

- 建立与战略一致的数据治理架构，明确技术方向、管理策略和支撑体系，以满足

数据管理体系、数据价值体系的治理要求。

- 评估数据治理架构的合理性和先进性，监督数据治理架构的推进情况。
- 评估数据治理架构的有效性，并持续改进和优化。

2. 核心治理领域

核心治理领域包括数据管理体系治理、数据价值体系治理。其中，数据管理体系治理包括数据标准、数据质量、数据安全、元数据管理、数据生命周期等治理内容；数据价值体系治理包括数据资产流通、数据资产服务、数据价值识别等治理内容。

(1) 数据标准

- 明确数据标准的内涵和范围，制定通用的数据规范，包括（不限于）数据分类、数据类型、数据格式和编码规则等，保证数据应用过程中的一致性。
- 建立数据标准的实施方案、计划及管理制度，推进数据标准化实施的落地。
- 建立数据标准化管理机构和机制，明确责权利和流程，开展数据标准化的实施。
- 持续开展数据标准的更新，以保证数据标准的先进性、前瞻性和技术层面的可执行性，满足数据应用发展需要。

(2) 数据质量

- 结合数据标准对数据质量进行分类管理，明确不同数据之间的关系和依赖性，制定数据质量管理目标。
- 建立数据质量管理机构和机制，定义数据质量管理的角色和责任，建立数据质量管理方法。
- 研发数据质量相关技术，支撑数据质量管理和数据质量的提升。
- 识别数据生命周期各个阶段的数据质量因素，构建数据质量评估框架，包括（不限于）数据的准确性、完整性、一致性、可访问性、及时性、相关性和可信度等。
- 采用定性评估、定量评估或综合评估等方法，评估和持续优化数据质量。

(3) 数据安全

- 明确数据安全的内外部监管和管理需求，制定数据安全管理的目标、方针和策略，并持续改进和优化，做到数据防泄露、防篡改和防损毁。
- 建立数据安全管理机构，明确数据安全管理的角色和责任，提升人员的意识、能力和素质。
- 建立数据安全分类分级规范，建立满足不同业务场景、不同级别的数据安全规范、保护机制，确保数据的保密性、完整性、可用性及数据的可追溯性。
- 构建数据安全视图，识别数据应用过程中的风险，并建立数据泄露应急响应、沟通协作和责任追究等安全管控机制。
- 建立数据应用过程中的数据授权、访问和审计机制。
- 定期开展安全审计和风险评估，对数据安全能力进行监督并持续改进和优化。

(4) 元数据管理

- 明确元数据的管理范围，构建元数据库。
- 建立完整的数据字典、数据模型、数据架构及其管理体系。

- 建立元数据管理机制，明确元数据的管理过程及角色、职责。
- 建立元数据创建、维护、整合、存储、分发、查询、报告和分析机制。
- 建立元数据管理的质量标准和评估指标，开展元数据绩效评估并持续改进。

(5) 数据生命周期

- 识别数据资源和数据资产运营状况，明确数据资源和数据资产的管理目标和策略。
- 识别数据生命周期的各个阶段(包括数据采集、数据传输、数据存储、数据处理、数据交换、数据销毁等)之间的关联关系，制定相应的管理策略，确保数据生命周期各个阶段数据的保密性、完整性和可用性。
- 确保数据生命周期的管理符合法律法规、行业监管等要求，保证数据的获取合法、存储完整、整合高效、分析有效、应用合规、归档可靠和销毁完全等。

(6) 数据资产流通

- 建立数据资产的识别方法和机制，建立数据资产价值评估指标，包括(不限于)数据的整体性、动态性、针对性、准确性、层次性、可度量性等，并开展数据价值评估。
- 遵循法律法规、行业监管和内部管控等内外部要求，明确可流通的数据权属、流通方式等。
- 结合数据分类分级管理机制，采用必要的技术手段对流通数据进行加密、脱敏等处理，确保数据的准确性、可用性、安全性和保密性。
- 采用必要的技术手段，保证数据资产及其流通过程中的安全，明确数据流通参与方的责任权利，保证数据权属合法清晰、流通方式合规、流通过程可靠。
- 确保数据流通过程的可追溯性，保存数据流通日志或记录，包括(不限于)时间戳、数据流通方式、参与者身份及数据内容描述等。
- 建立数据流通管理机制，符合法律法规、行业监管和内部管控要求。

(7) 数据资产服务

- 分析数据服务需求、现有资源和环境，明确数据服务内涵、范围、类型、团队和服务方式。
- 明确数据服务的内容和能力，制定数据服务目录、服务级别协议和服务办法。
- 建立数据服务管控流程，监督数据服务的安全性及合规性，并对服务过程进行审核和控制。
- 建立数据服务支持流程，通过标准化、自动化等方式支持数据服务的交付，满足服务需求。
- 构建数据服务管理机制，对数据服务的过程、质量和安全等进行管理，并持续改进和优化。
- 开展数据服务能力评价，定期对数据服务能力和价值进行评估、改进和优化，促进服务创新。

(8) 数据价值识别

- 分析业务视角和用户视角下的数据应用的需求，开展静态和动态场景识别，获取不同场景和应用下的数据价值识别和应用模型。

- 识别有效数据源，开展数据抽取、数据清洗、数据转换等预处理，并由此开展规律性、交互性、关联性分析。
- 融合业务、数据、算法和技术，挖掘数据及其之间的规律，提升数据价值识别能力。
- 构建数据价值识别的管理和应用机制，持续改进和优化数据价值识别流程。
- 建立数据安全和隐私保护机制，使数据价值识别符合法律法规和行业管理等要求。

1.4 数据安全治理的概念

1.4.1 数据安全治理的定义

数据安全治理主要包含两个层面的治理：一是国家宏观（广义）层面的数据安全治理；二是组织机构（含企事业单位）微观（狭义）层面的数据安全治理。以下从这两个层面分别给出数据安全治理的定义。

(1) 广义的定义

数据安全治理是指在国家数据安全战略指导下，为形成全社会共同维护数据安全和促进发展的良好环境，国家有关部门、行业组织、科研机构、企业、个人共同参与和实施的系列协同活动的集合。其中，协同活动包括完善相关政策法规、推动政策法规落地、建设与实施标准体系、研发并应用关键技术、培养专业人才等。

(2) 狭义的定义

数据安全治理是指在组织机构数据安全战略的指导下，为确保数据处于有效保护和合法利用的状态，组织机构内部多个二级部门协作实施的一系列活动的集合。其中，系列活动包括建立数据安全治理团队，制定数据安全相关制度规范，构建数据安全技术体系，建设数据安全人才队伍等。

1.4.2 数据安全治理的本质

本质上，数据安全治理包含“理”“治”“治理”三层含义，即先“理”后“治”再“治理”。其中，需要“理”的工作包括数据资源的内容类型、分布流向及不同场景下数据安全风险种类等；需要“治”的工作包括数据安全保障制度体系、监管机制、数据安全保护生态、国际数据安全规则等；需要“治理”的工作包括保障数据资源在安全可控的状态下充分发挥使用价值。

1.4.3 数据安全治理与传统数据安全的区别

数据安全治理与传统数据安全的区别主要体现在理念、对象、手段、融合等方面，如表 1-1 所示。

表 1-1 数据安全治理与传统数据安全的区别

对比内容	数据安全治理	传统数据安全
理念方面	数据分类分级、数据合规、数据安全流动	安全域划分、区域隔离
对象方面	企业内部人员，安全管控其数据操作行为	企业外部人员，防范其入侵
手段方面	数据安全技术(如加密、脱敏等)	边界防护技术(如防火墙等)
融合方面	数据安全产品与企业管理流程深度融合	管理与技术分离

1.4.4 数据安全治理体系

数据安全治理体系可以概括为“142”体系，即“1”个地基、“4”根柱子、“2”个目标，如图 1-5 所示。其内涵是：以数据全生命周期安全保护这“1”地基为基础(基础层)，以政策环境、产业生态、监督管理、跨境协作这“4”根柱子为支撑(支撑层)，最终实现数据有效保护、数据合法利用这“2”个目标(目标层)。

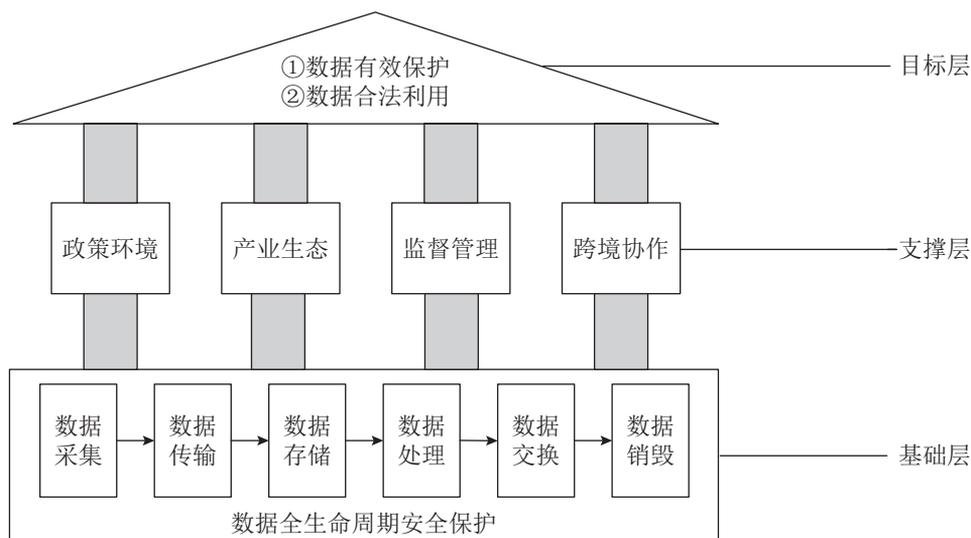


图 1-5 数据安全治理体系图

1. “1”个地基

数据全生命周期安全保护是数据安全治理体系的基础，必须采用相关技术、管理措施，确保数据在数据采集、数据传输、数据存储、数据处理、数据交换、数据销毁每个环节的安全。

2. “4”根柱子

政策环境、产业生态、监督管理、跨境协作这“4”根柱子是数据安全治理体系的重要支撑。

- 政策环境：包括数据安全法律法规、数据安全标准指南、数据安全管理制度等。
- 产业生态：包括数据安全战略规划、数据安全技术体系、数据安全产品体系、数据安全方案体系、数据安全服务体系、数据安全产融体系、数据安全人才体系等。
- 监督管理：包括数据安全监管机构、数据安全审查制度、网络安全(数据安全)执法行动等。
- 跨境协作：包括跨境数据分类(如个人数据、企业数据、国家数据等)管理、跨境数据分级(如核心高密级、普通高密级、内部级、公开级、国家涉密级等)管理、跨境数据交易规则、跨境数据合规性审查等。

3. “2”个目标

数据有效保护、数据合法利用是数据安全治理的两个目标。

- 数据有效保护：数据在“4”根柱子的支撑下，在数据全生命周期的数据采集、数据传输、数据存储、数据处理、数据交换、数据销毁诸环节，均能实现有效的安全保护。
- 数据合法利用：数据在“4”根柱子的支撑下，在数据全生命周期的数据采集、数据传输、数据存储、数据处理、数据交换、数据销毁诸环节所开展的所有工作，均能经得起数据安全监管部门、数据安全第三方审计机构的合法审查或合规审计。

1.5 概念间的逻辑关系及本书框架结构

1.5.1 概念间的逻辑关系

本章共包括数据、数据安全、数据治理、数据安全治理4个基本概念，从其定义视角，其间的逻辑关系如图1-6所示。其中，数据是大概念，数据安全与数据治理是数据的子集，数据安全治理则是数据安全与数据治理的交集。

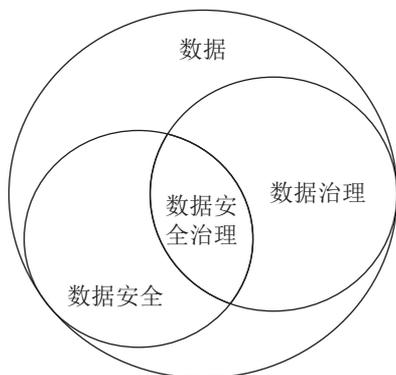


图 1-6 数据、数据安全、数据治理、数据安全治理间的逻辑关系

1.5.2 本书框架结构

本书共包括总论、数据安全、数据治理、数据安全治理、复习与考核5部分内容，共计10章，其框架结构如图1-7所示。其中，总论部分由第1章组成，数据安全部分由第5章(数据加密技术)、第6章(数据脱敏技术)、第7章(数据资产保护技术)、第9章(数据审计技术)四章组成，数据治理部分由第3章(数据质量管控技术)、第4章(数据采集技术)两章组成，数据安全治理部分由第2章(数据分类分级技术)、第8章(数据资产交易技术)、第10章(数据司法存证技术)三章组成，复习与考核则由每章末的复习题及全书最后的两套模拟试卷组成。

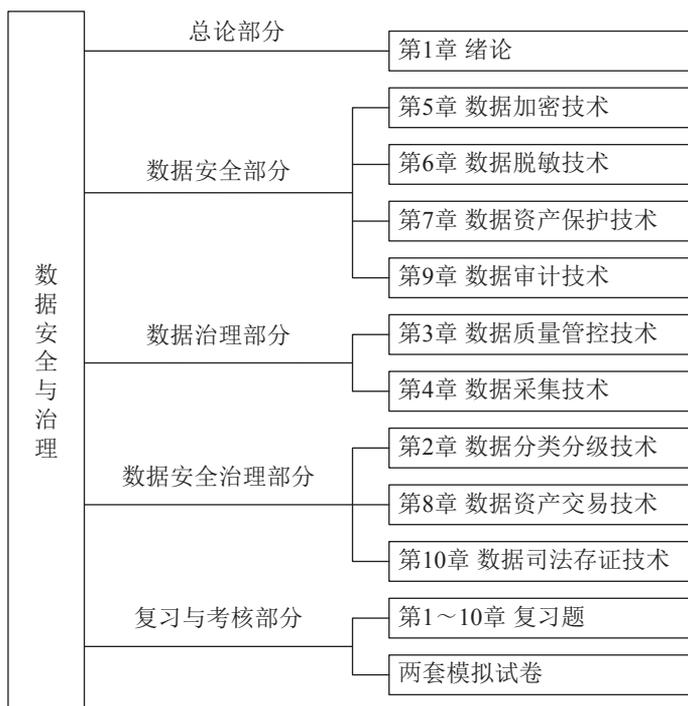


图 1-7 本书的框架结构

第1章 绪论，是本书的总论部分，重点阐述了数据、数据安全、数据治理、数据安全治理等相关概念及其内涵。

第2章 数据分类分级技术，是本书数据安全治理部分的重要内容，阐述了数据分类分级的概念、数据分类分级的原则、数据分类分级的流程和方法，给出了数据分类分级的相关案例。

第3章 数据质量管控技术，是本书数据治理部分的重要内容，阐述了数据质量的概念、数据质量监控规则、数据质量评价技术、数据质量管控技术，给出了数据质量管控案例。

第4章 数据采集技术，是本书数据治理部分的重要内容，阐述了数据采集的概念及技术、质量控制技术、安全控制策略，给出了数据采集综合案例。

第5章 数据加密技术，是本书数据安全部分的重要内容，阐述了数据加密的概念、

国外主要数据加密算法、国内主要数据加密算法，给出了数据加密综合案例。

第6章 数据脱敏技术，是本书数据安全部分的重要内容，阐述了数据脱敏的概念、数据脱敏的类别、敏感数据识别策略、数据脱敏方法、数据脱敏产品及应用案例。

第7章 数据资产保护技术，是本书数据安全部分的重要内容，阐述了数据资产的概念、数据资产管理的概念、数据资产管理策略、数据资产价值评估技术、数据资产安全保护技术，给出了数据资产保护综合案例。

第8章 数据资产交易技术，是本书数据安全治理部分的重要内容，阐述了数据资产交易的概念、数据资产确权、数据资产定价、数据资产交易监管、数据交易平台，给出了数据资产交易平台的总体架构。

第9章 数据审计技术，是本书数据安全部分的重要内容，阐述了数据审计的概念、数据库审计技术、主机审计技术、网络审计数据、应用审计技术，给出了数据审计应用案例。

第10章 数据司法存证技术，是本书数据安全治理部分的重要内容，阐述了数据司法存证的概念、数据司法存证的基本要求、第三方数据存证平台、数据存证的司法实践，给出了数据存证案例。

参考文献

- [1] 中华人民共和国第十三届全国人民代表大会常务委员会. 中华人民共和国数据安全法 [Z]. 2021.6.
- [2] 陈庄, 刘加伶, 成卫, 尹静. 信息资源组织与管理: 第3版 [M]. 北京: 清华大学出版社. 2020.
- [3] GB/T 37988—2019, 信息安全技术 数据安全能力成熟度模型 [S]
- [4] GB/T 34960.5—2018, 信息技术服务 治理 第5部分: 数据治理规范 [S]
- [5] DAMA International. DAMA 数据管理知识体系指南 [M]. 北京: 清华大学出版社, 2012.
- [6] 耿骞. 中国政务信息化发展报告 [M]. 北京: 北京邮电大学出版社, 2017.
- [7] 张莉. 数据治理与数据安全 [M]. 北京: 人民邮电出版社, 2019.
- [8] 数据安全治理专业委员会. 数据安全治理白皮书 3.0[R]. 2021.
- [9] T/ISC—0011—2021, 中国互联网协会. 数据安全治理能力评估方法 (团体标准) [S].
- [10] 中国信息通信研究院. 数据安全治理实践指南 (1.0) [S]. 2021.7.
- [11] 中国电子信息产业发展研究院. 数据安全治理白皮书 [R]. 2021.6.

复习题

一、单选题

1. 数据是指任何以电子或者其他方式对 () 的记录。

- A. 数据 B. 信息 C. 资产 D. 文本

二、多选题

1. 数据安全与治理涉及()等基本概念。
 - A. 数据
 - B. 数据安全
 - C. 数据治理
 - D. 数据安全治理
2. 数据的共享性没有充分体现,会出现()现象。
 - A. 数据江河
 - B. 数据烟囱
 - C. 数据孤岛
 - D. 数据湖泊
3. 数据按其等级性可分为()。
 - A. 绝密级
 - B. 机密级
 - C. 秘密级
 - D. 内部级
4. 数据按其来源的不同可分为()。
 - A. 政务数据
 - B. 经济数据
 - C. 自然数据
 - D. 社会数据
5. 数据按其加工深度的不同可分为()。
 - A. 零次文献数据
 - B. 一次文献数据
 - C. 二次文献数据
 - D. 三次文献数据
6. 数据存储单位 GB、TB、PB、EB 之间的换算关系是()。
 - A. $1\text{TB} = 10^3\text{GB}$
 - B. $1\text{PB} = 10^6\text{GB}$
 - C. $1\text{GB} = 10^3\text{TB}$
 - D. $1\text{EB} = 10^9\text{GB}$
7. 从技术视角,数据安全是指通过管理和技术措施,确保数据()状态。
 - A. 安全保护
 - B. 有效保护
 - C. 合规使用
 - D. 综合利用
8. 从法律视角,数据安全是指通过采取必要措施,确保数据处于()状态。
 - A. 安全保护
 - B. 有效保护
 - C. 合规使用
 - D. 合法利用
9. 数据安全范围包括()阶段的安全。
 - A. 数据采集
 - B. 数据处理
 - C. 数据交换
 - D. 数据销毁
10. 按照 GB/T 37988—2019,数据安全 PA(过程域)体系分为()过程域。
 - A. 数据采集
 - B. 通用安全
 - C. 数据生命周期
 - D. 数据销毁
11. 数据治理是指数据资源及其应用过程中相关()的集合。
 - A. 管控活动
 - B. 绩效
 - C. 风险管理
 - D. 数据管理
12. 数据治理的基本要求是满足()。
 - A. 法律法规要求
 - B. 行业监管要求
 - C. 企业商业要求
 - D. 数据管理体系要求
13. 数据治理应满足企业的商业化要求,包括()要求。
 - A. 数据产品化
 - B. 数据私有化
 - C. 数据资产化
 - D. 数据价值化
14. 数据治理的总体目标是保障数据及其应用过程中的()。
 - A. 运营合规
 - B. 风险可控
 - C. 价值实现
 - D. 目标达成
15. 数据治理的任务是()。
 - A. 制定数据规划
 - B. 分析现状需求
 - C. 落地实施策略
 - D. 评估实施效果
16. 数据的核心治理领域包括()治理。
 - A. 数据管理体系
 - B. 数据价值体系
 - C. 数据评价体系
 - D. 数据应用体系
17. 数据质量评估框架,包含数据的()。
 - A. 准确性
 - B. 完整性
 - C. 及时性
 - D. 一致性
18. 数据安全治理的目标是()。
 - A. 数据有效保护
 - B. 数据合法利用
 - C. 数据安全应用
 - D. 数据综合利用

19. 数据安全治理体系的重要支撑包括()。

- A. 政策环境 B. 监督管理 C. 跨境协作 D. 产业生态

三、判断题

1. 数据是指任何以电子或者其他方式对信息的记录。 ()
2. 数据普遍存在于自然界、经济社会中。 ()
3. 数据是一种类似土地、劳动力、资本、技术的有价值的资产。 ()
4. 数据不能进行交易。 ()
5. 将数据进行交换时,一方有所得,必使另一方有所失。 ()
6. 数据的价值与数据所处的时间长度成反比。 ()
7. 文献综述属于一次文献数据。 ()
8. 图书的索引卡片属于二次文献数据。 ()
9. 难得糊涂是一种智慧。 ()
10. 数据销毁阶段不存在数据安全问题。 ()
11. 数据治理应满足国家法律法规要求。 ()
12. 数据资产流通不属于数据价值体系治理的范畴。 ()
13. 数据安全治理应该先“理”后“治”再“治理”。 ()
14. 数据安全治理体系的基础是实现数据全生命周期安全保护。 ()

四、简答题

1. 简述数据的类别。
2. 简述数据、信息、知识、智慧之间的关系
3. 简述数据安全的概念和范畴。
4. 简述 PA10(数据脱敏)的重要性。
5. 简述数据治理的总体目标。
6. 简述数据治理的主要任务
7. 简述数据治理的体系结构。
8. 简述数据安全治理概念及其本质。
9. 简述数据安全治理与传统数据安全的区别。
10. 简述数据安全治理的体系结构。

五、论述题

依照你自己的经历或经验,论述本章涉及相关内容(如数据、数据安全、数据治理、数据安全治理等)的需求背景及其重要作用。