可信数据空间标准化研究报告

（2025 版）

全国数据标准化技术委员会秘书处

二〇二五年八月

《可信数据空间标准化研究报告（2025 版）》

编写单位（排名不分先后）：

中国电子技术标准化研究院
北京大数据先进技术研究院
华为技术有限公司
中国联合网络通信集团有限公司
中电数据产业集团有限公司
上海芯超数据科技有限公司
国家数据发展研究院
浪潮云信息技术股份公司
领信数科信息技术有限公司
马上消费金融股份有限公司
西安交通大学
中国南方电网有限责任公司
四川省大数据中心
中国人寿保险股份有限公司
广西电网有限责任公司
人民数据管理（北京）有限公司
中央广播电视总台技术局
亚信科技（中国）有限公司
北京天融信网络安全技术有限公司
江西省大数据中心
东软集团股份有限公司
华控清交信息科技（北京）有限公司
京东科技信息技术有限公司
上海数据交易所有限公司
北京兴云数科技术有限公司
广州维视达数字科技有限公司
亚信科技（成都）有限公司
北京腾云天下科技有限公司
北京大学
浙江大学
中国电信集团有限公司
中国移动通信集团有限公司
云基华海信息技术股份有限公司
北京百度网讯科技有限公司
中国信息通信研究院
蚂蚁科技集团股份有限公司
中国移动通信有限公司研究院
上海零数众合信息科技有限公司
北京电子数智科技有限责任公司
大连理工大学
浙江蚂蚁密算科技有限公司
国网山东省电力公司
数据空间研究院
杭州数梦工场科技有限公司
华信咨询设计研究院有限公司
杭州金智塔科技有限公司
国家石油天然气管网集团有限公司科学技术研究总院分公司
北京华宇信息技术有限公司
上海金润联汇数字科技有限公司
杭州安恒信息技术股份有限公司
江苏中堃数据技术有限公司
上海临港北京大学国际科技创新中心
上海计算机软件技术开发中心
深圳市洞见智慧科技有限公司
煤炭科学研究总院有限公司
中电科大数据研究院有限公司

杭州锘崴信息科技有限公司
三六零数字安全科技集团有限公司
北京熠智科技有限公司
蓝象智联（杭州）科技有限公司
美林数据技术股份有限公司
中电信数智科技有限公司
杭州云象网络技术有限公司
神州数码信息服务集团股份有限公司
内蒙古自治区大数据中心
北京铜牛信息科技股份有限公司
深圳市尚数网科技有限公司
南方电网能源发展研究院有限责任公司
数巨有谱数据集团有限公司
北京数字认证股份有限公司
广州金域医学检验集团股份有限公司
飞腾信息技术有限公司
数篷科技（深圳）有限公司
广东省信息协会
广电运通集团股份有限公司
成都市标准化研究院
杭州安泉数智科技有限公司
北京建筑大学
新胜科技（上海）有限公司
全国组织机构统一社会信用代码数据服务中心
中移雄安信息通信科技有限公司
中电科数智科技有限公司
北京数安行科技有限公司
南京南瑞信息通信科技有限公司
数据易（北京）信息技术有限公司
软通智慧科技有限公司
北京市大数据中心
广州赛西标准检测研究院有限公司
西安航天飞邻测控技术有限公司
北京国金汇德工程管理有限公司
北京域智科技有限公司
中医内科学教育部重点实验室
渔翁信息技术股份有限公司
数智中医慢病防治北京市重点实验室
国信中健数字科技有限公司
第伍要素（上海）数据科技有限公司
清雁科技（北京）有限公司
北京品冠天成科技有限公司
北京华隐熵策数据科技有限公司
山西远大纵横科技有限公司

目 录

一、引言 1
（一）政策背景 1
（二）可信数据空间的概念、内涵 2
（三）标准化对可信数据空间的关键作用 3
二、国外可信数据空间发展现状及趋势 4
（一）欧盟可信数据空间发展现状 4
（二）美国可信数据空间发展现状 16
（三）日本可信数据空间发展现状 21
（四）国外可借鉴工作经验及趋势 25
三、我国可信数据空间发展现状及趋势 29
（一）可信数据空间技术能力发展现状 29
（二）可信数据空间应用发展现状 44
（三）我国可信数据空间发展建议及趋势 56
四、可信数据空间标准化现状 59
（一）可信数据空间国际标准化现状 59
（二）我国可信数据空间标准化现状 64
五、可信数据空间标准体系建设 68
（一）可信数据空间标准需求 68
（二）可信数据空间标准体系结构 71

（三）可信数据空间标准体系框架 73
（四）可信数据空间标准建设路径 74
（五）可信数据空间标准建设明细 76
六、下一步可信数据空间标准化工作考虑 85
（一）持续推进可信数据空间重点标准研制 85
（二）扎实做好可信数据空间标准宣贯推广 85
（三）打造可信数据空间标准应用服务生态 86
（四）推动可信数据空间国际对接互通 86

一、引言

（一）政策背景

近年来，全球主要经济体及区域性组织加速推进数据空间战略布局，数据空间已成为驱动全球数据要素流通与价值挖掘的核心载体。

数据空间 Dataspace 一词最早由 Michael Franklin 在 2005 年提出。2014 年德国提出“工业数据空间行动”。2016 年欧盟提出建立国际数据空间（International Data Space，IDS）倡议。2020 年欧盟发布《欧洲数据战略》，提出在工业、绿色、交通等领域构建“共同数据空间”，初步搭建起欧洲共同数据空间的总体框架。

2022 年 12 月，中共中央、国务院印发《关于构建数据基础制度更好发挥数据要素作用的意见》，明确了数据基础制度体系基本架构。2024 年 10 月，国家数据局开展数据基础设施先行先试，在 8 个城市部署可信数据空间建设任务，这是国家层面首次针对可信数据空间这一新型数据基础设施进行前瞻性的系统布局。2024 年 11 月，国家数据局印发《可信数据空间发展行动计划（2024—2028 年）》。2024 年 12 月，国家发展改革委、国家数据局、工业和信息化部印发《国家数据基础设施建设指引》，为贯彻落实党的二十届三中全会关于建设和运营国家数据基础设施，促进数据共享，明确了建设目标，做出部署要求，并明确将可信数据空

间作为数据基础设施的一种技术路线。2025 年 3 月，国家数据局和全国数据标准化技术委员会(以下简称“全国数标委”)联合发布国家数据基础设施建设参考架构、互联互通、用户身份管理、标识管理、接入连接器及数据目录描述等 6 项技术文件，指导各地方各行业各领域的数据基础设施建设，为推动形成横向联通、纵向贯通、协调有力的国家数据基础设施提供标准支撑。2025 年 4 月，全国数标委《可信数据空间技术架构》发布，明确了可信数据空间在国家数据基础设施中的定位，描述了可信数据空间作为一种数据流通利用基础设施的核心技术特征、最小功能集合以及关键业务流程。2025 年 7 月，国家数据局发布《2025 年可信数据空间创新发展试点名单的通知》，标志着我国可信数据空间从顶层设计迈向应用落地的关键一步。

（二）可信数据空间的概念、内涵

可信数据空间是基于共识规则，连接多方主体，实现数据资源共享共用的一种数据流通利用基础设施，是数据要素价值共创的应用生态，是支撑构建全国一体化数据市场的重要载体。可信数据空间作为 6 条技术路线之一，符合《数据基础设施 参考架构》确定的国家数据基础设施整体架构及基本约束，是流通利用设施层中的业务节点。

从上述定义来看，可信数据空间具有 3 个方面内涵。**一是**可信数据空间建设的基本条件是基于多方主体认同并遵

守的共同规则，规定了参与可信数据空间的各方主体资质要求及功能权限、数据流通客体及其授权方式、数据流通过程规范与控制方法等。**二是**可信数据空间是实现数据资源流通利用的一种数据流通利用基础设施。可信数据空间通过体系化的技术安排确保数据协议的确认、履行和维护，实现多主体间数据集聚、流通和利用。**三是**可信数据空间是数据要素价值共创的应用生态，作为一种数据应用生态，可信数据空间可支持多主体协同合作、资源整合以及场景创新，进而激发数据在生态体系中的价值实现。

（三）标准化对可信数据空间的关键作用

标准化对可信数据空间建设具有基础性、引领性作用，通过架构设计、功能技术、流程规则、应用服务、评价评估、安全保障等标准的研制，有利于凝聚政产学研用等各方力量，促进数据提供方、使用方、服务方、运营方、监管方等达成共识，**解决数据流通中的兼容性、互操作性和安全性等核心问题，避免数据孤岛，实现互联互通，避免在概念、功能上泛化，全面规范可信数据空间的建设、运营和管理**。

本研究报告通过系统梳理国内外可信数据空间政策制定、发展现状和趋势，以及标准化工作进展，结合可信数据空间标准研制实际需求，构建了可信数据空间标准体系框架，梳理出亟须研制的可信数据空间标准，并提出可信数据空间标准化建设的下一步工作考虑。本研究报告旨在为可信

数据空间标准化工作提供系统性支撑，聚焦于规范并促进数据的高效流通与可信使用。报告致力于探索可信数据空间标准化的方向与路径，推动可信数据空间建设，实现科学有序的顶层设计、多方协同的统筹推进；强化问题导向，确保标准化工作务实有效；突出应用牵引，激发技术与实践创新；坚持立足国内实践与开放国际合作相结合的原则，共同构建健康发展的可信数据空间生态。

二、国外可信数据空间发展现状及趋势

（一）欧盟可信数据空间发展现状

1.政策与法律环境

可信数据空间的概念由欧盟提出并发起，旨在构建和推广一个可信数据共享环境，在此环境中各组织能够共享数据，同时对其使用保持完全控制。当前，可信数据空间已经成为欧盟制造业转型的“加速器”，其理念和架构也在多个领域和成员间成功落地，在国际领域产生了很多可以借鉴的实例。

欧盟可信数据空间的构建源于其“数字主权”战略的深化。这一概念最初由德国弗劳恩霍夫协会在2014年提出，彼时该协会提出了“工业数据空间（Industrial Data Space, IDS）”的建设构想。随后，围绕这一构想，相关推进工作逐步展开：2015年发起“工业数据空间行动”，2016年成立工业数据空间协会，2018年该协会升级为如今的国际数据空间协

会（IDSA）。在政策环境上，2020 年，欧盟委员会发布《塑造欧洲数字未来》，该文件提出了通过建立“一个基于欧洲规则和价值观的欧洲数据空间”用来打造公平竞争的经济。同年，欧盟公布《欧洲数据战略》（European Data Strategy）旨在确保欧盟在数字化和人工智能方面成为全球引导者。通过充分利用数据驱动的创新来提升欧洲的竞争力和社会福利，将欧洲打造成全球最具吸引力、最安全和最具活力的数据经济体。并且计划在多个战略行业建立共同数据空间，如制造业、农业、医疗、交通、能源等。同时欧盟先后针对文化遗产、旅游、交通、健康和医疗等行业领域出台了相应细分领域的数据空间政策文件，对该领域共同数据空间的建设目标、支持措施、推进计划等提供了细化的指导，如《欧洲共同文化遗产数据空间建议》《迈向欧洲共同旅游数据空间：促进整个旅游生态系统的数据共享和创新》《创建欧洲共同交通数据空间》《欧洲健康数据空间条例》《医疗数据空间条例》等。2022 年，欧盟委员会发布《关于欧洲公共数据空间的欧盟委员会工作人员文件》，对相关的立法和财政举措进行了时间线上的梳理和汇总，在整体上反映出了欧洲各领域公共数据空间的发展实况。该文件中还计划建设欧洲交通数据公共空间、欧洲媒体数据公共空间等。2024 年，欧盟网络安全局发布《欧盟数据空间中的个人数据保护工程》，讨论了从个人数据保护工程角度，欧盟数据空间的设计和部

署。欧洲数据保护协会（EDPB）通过了其《2024-2027 行动计划》，该计划包含增强法律适用一致性、增强执法协调性、增强技术发展和交叉监管背景下的数据保护四个重点方面，为未来欧盟数据保护工作开展奠定基本方向。

在法律环境上，为了弥合欧盟各成员国在数据政策和实践方面的差异，欧盟出台立法，明确数据流通利用方式，降低各成员国数据共享的壁垒。欧盟委员会制定了一系列法规和政策，为数据空间的建设提供法律框架。早在 2018 年，欧盟便出台了具有里程碑意义的《通用数据保护条例》（GDPR）明确了数据保护的标准和要求，为个人数据的使用与保护设立了严格的标准。其他积极促进数据经济发展的法律举措还有《关于非个人数据自由流动条例》（FFD）、《开发数据指令》（ODD）、《高价值数据集实施法案》、《数据治理法案》（DGA）、《数字市场法案》（DMA）、《数字服务法案》（DSA）、《数据法案》（DA）和《网络安全法案》（CSA）、定义了数据共享的欧盟路径，确立了欧盟数据使用和管理的基本规则，并设立专门机构推动数据互联互通。在数据跨境方面，欧盟通过“内松外紧”法律体系，实现数据的跨境自由流通。2023 年，欧盟委员会批准了欧美间数据传输新协议《欧盟·美国 数据隐私框架》，旨在为欧盟公民的个人数据在美国的处理提供与欧盟法律相当的保护水平，解决跨大西洋数据传输中的隐私保护问题。

表 1 欧盟出台数据法律体系文件

（资料来源：根据公开资料整理）

政策名称	发布/生效时间	简介
《通用数据保护条例》（GDPR）	2018 年	对收集、传输、保留或处理涉及到欧盟所有成员国内个人信息的行为进行了约束
《关于非个人数据自由流动条例》（FFD）	2019 年	保障非个人数据在欧盟境内能够自由流动，并对数据本地化要求、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作了具体规定
《开放数据指令》（ODD）	2019 年	包含欧洲公共数据共享的一般规定。该指令不仅明确了公共数据的范围，将公共数据的概念延展至公共部门机构、公共服务运营商所控制的机构和受公共财政资助的研究数据三个门类。
《高价值数据集实施法案》	2022 年	基于《开放数据指令》，要求成员国以机器可读格式、免费提供六大类高价值数据（地理空间、环境、统计等）
《数据治理法案》（DGA）	2022 年	增强对数据共享的信任，设立数据互操作服务和数据利他组织 成立“欧洲数据创新委员会”（European Data Innovation Board, EDIB）作为 DGA 实施的顾问机构
《数字市场法案》（DMA）	2022 年	本立法的目的是确保数字领域的竞争性和公平性市场，使其他公司能够进入这些市场并在平衡、公平的竞争环境中竞争。
《数字服务法案》（DSA）	2022 年	作为 DMA 的补充措施提出，涵盖在线内容管理，澄清在线中介服务、托管服务和大型在线平台的责任和义

		务。
《数据法案》（DA）	2024 年	旨在促进公平的数据经济，通过明确数据访问和使用权利，消除工业等领域的数据壁垒，推动 B2B 和 B2C 数据共享，同时保护个人数据隐私。法案还规定了公共部门在紧急情况下获取数据的机制，保护中小企业免受不公平条款约束，并增强云服务市场的竞争力和数据跨境流动的安全性。
《网络安全法案》（CSA）	2024 年	承认托管安全服务在预防、检测、响应和恢复网络安全事件方面的重要性日益增加，该修正案将有助于提高托管安全服务的质量，培养值得信赖的网络安全服务商

2.建设现状

2020 年欧盟通过《欧洲数据战略》提出打造九大行业可信数据空间计划，并基于国际可信数据空间 IDS 的理念推进其在各领域的建设。欧盟已构建了以通用数据空间、行业数据空间和测试应用为核心的多层次可信数据空间推进体系。这一体系在战略规划、资金支持和行业推动下，成为欧盟数字基建的重要组成部分，进一步推动各个空间的互联互通和互操作，为数据流通和数字化转型提供了坚实基础。在通用数据空间上，该空间由数字欧洲计划等欧盟计划支持，欧盟和各成员国政府主导建设，覆盖战略、经济和公共利益领域。目前已有 14 个通用数据空间，其中 9 个项目源于 2020 年《欧洲数据战略》，5 个新增于 2022 年，通用数据空间的建立确保了关键领域的数据空间安全流通和高效管理，成为欧盟数

字主权的基石。在行业数据空间上，该空间基于欧盟战略框架，由各产业生态和行业主要参与者根据实际需求自发形成。这些空间普遍采用 IDS 技术框架，在能源、制造、农业等领域逐步形成数据共享与合作生态，推动产业协同和创新。从发展阶段来看，IDSA 将数据空间的进程划分为探索、筹备、实施、运营和规模化五个阶段，目前项目多处于筹备和实施阶段，数据空间整体发展进程由试点探索向建设运营阶段迈进。从资金来源来看，欧盟通过“数字欧洲”“地平线欧洲”等计划对数据空间相关项目提供资金资助。2021—2024 年欧盟已投入 12.77 亿欧元用于支持 14 个领域共同数据空间的开发，以及云到边缘基础设施和服务的建设。此外，欧盟委员会和其他专项基金也为法律、公共采购、电子政务和数据安全领域提供支持。

表 2 欧盟可信数据空间建设情况介绍

序号	数据空间项目分类	数据范畴	项目提出时间	参与方	资金来源	建设进展
1	农业数据空间	生产、土地使用、环境等农业数据	2020 年《欧洲数据战略》提出	欧盟成员国各公共部门、农民、机械公司、数据服务提供商	数字欧洲计划(Digital Europe)	正在进行治理和商业模式开发，预计 2024 年底部署操作性农业数据空间
2	能源数据空间	能源相关数据	2020 年《欧洲数据战略》提出	能源系统运营商、服务提供商	地平线欧洲(Horizon Europe)	正在进行部署准备，预计 2024 年启动第一个操作版本

3	研究与创新数据空间-EOSC	研究数据、开放科学实践	2020年《欧洲数据战略》提出，其中EOSC于2015年由欧盟委员会提出	欧盟成员国各公共部门、研究机构和社区	地平线欧洲(Horizon Europe)	核心组件已在操作环境中原型化，EOSC EU节点服务已于2023年采购
4	技能数据空间	技能和教育数据	2020年《欧洲数据战略》提出	公共就业服务、教育和培训机构	数字欧洲计划(Digital Europe)	正在进行部署准备，预计2024-2026年部署操作性技能数据空间
5	健康数据空间	电子健康数据	2020年《欧洲数据战略》提出	欧盟成员国各公共部门、研究人员、决策者	欧盟健康计划(EU4Health)	正在进行MyHealth@EU的扩展，Health Data@EU Pilot（EHDS）预计24年启动，以及其他相关项目和基础设施的部署
6	工业/制造数据空间	工业数据	2020年《欧洲数据战略》提出	制造业公司	数字欧洲计划(Digital Europe)	正在进行数据空间的部署准备，预计2023—2026年部署两个操作性制造数据空间
7	交通数据空间	交通和出行数据	2020年《欧洲数据战略》提出	物流业、城市管理者	数字欧洲计划(Digital Europe)	正在进行部署准备，预计2023—2026年部署操作性流动性数据空间
8	公共行政数据－法律数据空间	法律和案例法数据	2020年《欧洲数据战略》提出	法律从业者、公共行政部门	欧盟委员会	正在进行法律数据空间的建立，包括ELI标准的扩展和法律数据质量的提升
	公共行政数据－公	公共采购数据	Public Administratio	公共采购机构、中小	数字欧洲计划(Digi	正在进行公共采购数据空间的部署，

	共采购数据空间		ns Data Spaces，核心聚焦政府采购，2022年增加其他细分类目	企业	tal Europe)	预计2024年推出初始版本
	公共行政数据－电子政务	行政程序数据		公民、企业、公共当局	数字欧洲计划(Digital Europe)	正在进行一次性技术系统的建立，预计2023-2026年完成
	公共行政数据-安全数据空间创新	执法数据		执法机构	内部安全基金 (ISF)	正在进行安全数据空间的可行性研究和部署准备，预计2024年启动相关工作
9	金融数据空间	金融服务数据	2020年《欧洲数据战略》提出	金融机构、消费者	数字欧洲计划(Digital Europe)	正在开发中，包括金融数据访问框架和欧洲单一访问点 (ESAP)
10	语言数据空间	多模态语言数据和模型	2022年增加	行业、公民	数字欧洲计划(Digital Europe)	正在进行部署准备，预计2023—2026年部署操作性语言数据空间
11	媒体数据空间	媒体和音频视觉数据	2022年增加	媒体组织	数字欧洲计划(Digital Europe)	正在进行部署准备，预计2023—2026年部署操作性媒体数据空间
12	旅游数据空间	旅游相关数据	2022年增加	欧盟成员国各公共部门、旅游公司	数字欧洲计划(Digital Europe)	正在进行部署准备，预计2024年启动测试行动，2024—2027年部署操作性旅游数据空间
13	文化遗产数据空间	文化遗产资产的数字化数据	2022年增加	欧盟成员国各公共部门、文化机构、创意产业	数字欧洲计划(Digital Europe)	正在进行部署，计划2024年夏季推出操作性版本

3.技术架构与核心能力

技术层面，欧盟的数据空间架构代表包括 IDS、Gaia-X、Catena-X 等。IDS 以点对点形式实现主体之间的可信数据交换，在欧洲影响最广。基于此形成的联盟 IDSA（国际数据空间协会）将“数据空间”定义为虚拟空间，基于通用协议和格式以及安全可信的数据共享机制，为数据交换提供了一个标准化框架，其目标是确保数据主权，同时实现安全的数据共享和交易。在 IDS 参考架构模型（IDS-RAM）中数据提供商通过制定数据使用规则，明确数据访问的条件、目的和使用者，保留对数据的完全主权。同时，IDS 架构借助标准化连接器提供安全、标准化的数据交换环境，使数据使用者默认所访问的数据具有可靠性、高质量，并符合商定规则。

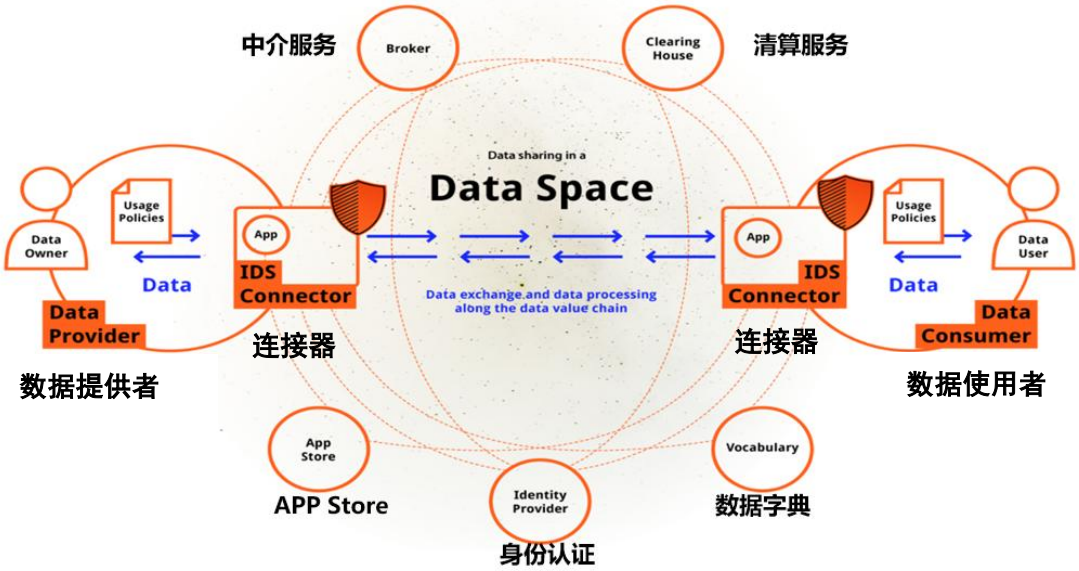

图 1 IDS 可信数据空间参考架构

如图 1 所示，数据空间主要包括五个主体：中介服务方、清算服务方、应用商店、身份认证者、数据字典，各主体基

于云上算力，通过连接器沿数据价值链进行数据交换与处理。其中，中介服务方提供分析/集成/清理或语义丰富等附加数据服务，提高交换数据质量；清算服务方提供数据交换和金融交易的清算和结算服务；应用商店提供可部署在 IDS 连接器中的应用程序，以执行转换、聚合或数据分析等任务；身份认证者创建、维护、管理和验证 IDS 参与者的身份信息；数据字典提供标准化描述符，使用共享词汇表在语义级上融合不同格式和协议类型的数据。IDS 连接器充当数据和服务的网关及应用程序和软件的可信环境，跟踪数据来源，允许参与者加入使用策略并强制执行。数据提供方保留对数据使用者、使用方式、时间、目的和价格的控制。

IDS 作为全球可信数据空间的通用参考架构，其主要功能包括，提供数据源认证和接入身份认证、提供数据资源目录以便快速检索、提供数据格式和协议转换软件、对敏感数据提供过滤和去标识化、提供算力和数据挖掘工具软件方便数据开发、支持明文计算和解密计算及同态加密计算、提供数据沙箱和数据流通安全合规管理、提供数据流通存证审计和交易清算结算服务。

Gaia-X 项目通过整合云提供商、可信数据空间和基础设施供应商构建安全可靠的跨域数据基础设施以打造统一的联邦数据生态系统，提升欧洲产业竞争力。Gaia-X 所有参与主体均需遵守统一标准以确保数据主权、互操作性和透明

度。截至 2024 年，Gaia-X 企业成员已超过 350 家。

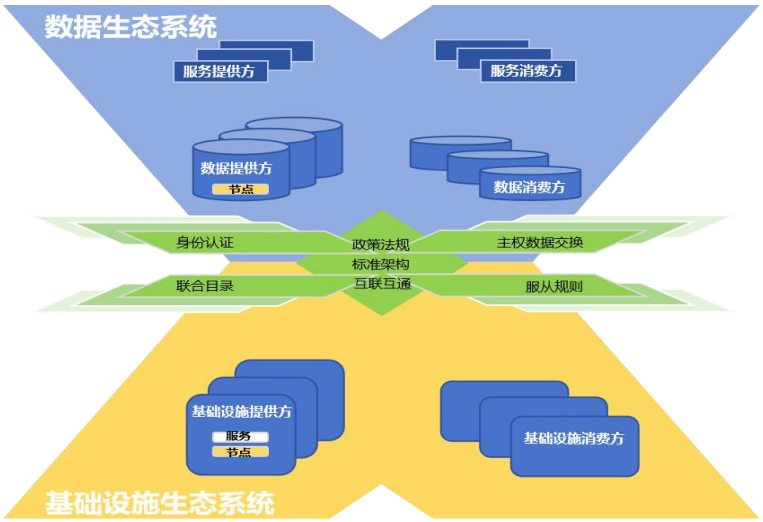

图 2 Gaia-X 系统架构

Gaia-X 聚焦欧盟的基础设施定义（偏 IaaS），IDS（偏 PaaS）定义了完整的可信数据空间方案，两者遵循相同的愿景，即保障数据主权为数据共享创建信任生态系统 IDS-RAM 架构满足了 Gaia-X 的落地需求，同时，Gaia-X 为 IDS 构建安全可靠的可信数据空间提供了广泛的云基础设施。当前国际可信数据空间标准 ISO/IEC JTC1/SC38 的 20151 可信数据空间标准，基础部分内容来自 IDS 的架构。

Catena-X 是欧洲开放协作式数据生态系统，该组织由德国发起，负责发展汽车领域的可信数据空间，目前近 200 家协会会员，包括众多欧盟以外的企业和协会，如 Ford，华为，宁德时代等。Catena-X 使用开源技术，基于各国监管法规和行业标准，面向全球汽车行业，打造开放的，标准的，去中心化的数据交换网络空间。

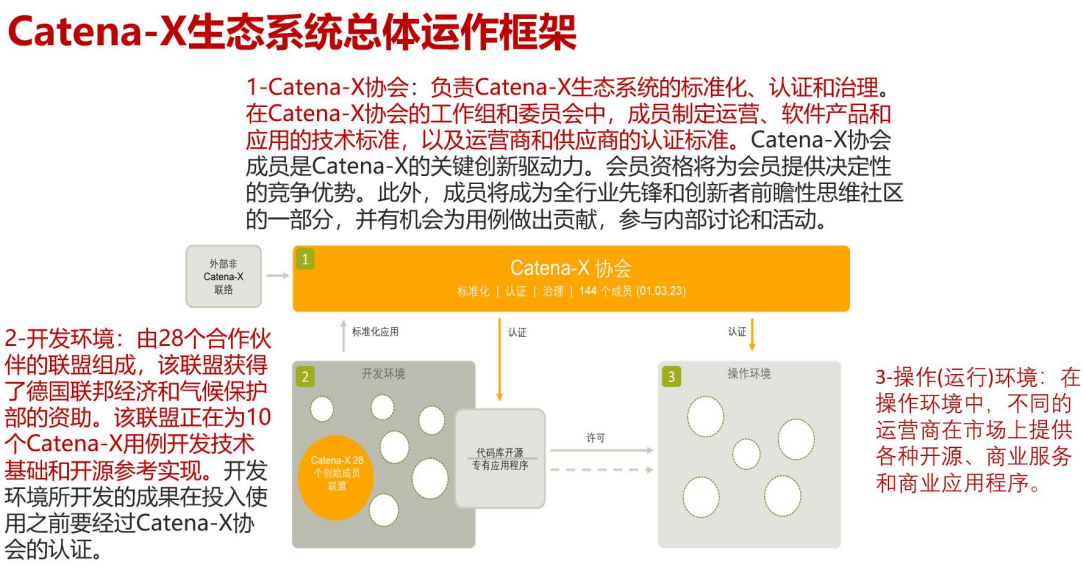

图 3 Catena-X 生态系统总体运作框架

4.相关参与方

数据持有者：数据的原始拥有者或管理者，负责数据的存储和维护。在欧盟数据空间中，数据持有者包括公共部门、私营企业、医疗机构、科研机构等。这些机构在各自的领域内生成和收集数据，并有权决定如何共享和使用这些数据。

数据用户：数据的需求方，其利用数据进行分析、研究、创新等活动。在欧盟数据空间中，数据用户可能包括企业、科研机构、政府部门、非政府组织等。这些用户通过访问和使用数据空间中的数据，提升自身的业务能力、推动技术创新或制定更科学的政策。

数据中介服务：根据《数据治理法案》的规定，数据中介服务（Ddata Intermediation Service）是指“通过技术、法律或者其他手段，在数量不确定的数据主体、数据持有人与数据使用者之间建立以数据共享为目的的商业关系，包括以行

使数据主体对个人数据的权利为目的的一项服务”。根据服务对象的不同，数据中介组织可分为以下三类：一是服务于数据持有人与数据用户之间的数据交易活动。其提供的服务形式多样，涵盖双边或多边的数据交换安排、搭建可实现数据交换或联合利用的平台或数据库、构建促使数据持有人与数据用户互联的特定基础设施等。同时，为保障上述服务的顺利开展，该类中介组织还会提供必要的技术支持及其他辅助手段。二是为个人行使数据权利提供中介服务，具体表现为在数据主体与数据用户之间的数据交互过程中发挥桥梁作用。其核心职责在于帮助数据主体有效行使《通用数据保护条例》（GDPR）所赋予的各项数据权利，例如数据访问权、更正权、删除权等。在实际操作中，常通过个人数据空间等方式，帮助数据主体将其个人数据从一个数据控制者安全、合规地转移至另一个数据控制者。三是为数据合作社内部交易提供中介服务。具体而言，该类中介组织会协助数据合作社成员在数据处理前做出充分知情的决策。

政府与监管机构：欧盟及其成员国政府在数据空间建设中发挥着关键作用，它们通过制定政策、法规和标准，为数据空间的健康发展提供指导和保障。同时，监管机构负责监督数据空间的运行，确保数据共享和使用的合法性和合规性。

（二）美国可信数据空间发展现状

1.政策与法律环境

在法律保障方面，颁布多项联邦及地方性法律，保护个人数据和隐私安全。2023 年生效的《加州隐私权法（CPRA）》、《弗吉尼亚州消费者数据保护法（VCDPA）》，以及联邦层面的部门法协同发力，保护个人数据隐私安全。《联邦数据质量法》要求政府机构确保所发布数据的准确性、完整性和及时性，从而为 B2G（Business-to-Government，企业对政府）数据共享提供高质量的数据来源。

在政策制定方面，《联邦数据战略（Federal Data Strategy, FDS）》作为首个政府级数据战略，规划了政府数据开发利用方向，但存在局限性，信息技术与创新基金会（ITIF）建议将其原则与政府优先事项紧密关联，推动联邦数据生态建设。《美国国际网络空间和数字政策战略》（2024 年）强调数字团结的理念，着重于网络空间的重要性。2025 年 1 月，白宫发布了一项行政命令，旨在提升美国在人工智能基础设施领域的领导地位，提出强化人工智能数据中心的建设。该数据中心旨在存储、管理、处理和传播计算机网络中的电子信息，能够容纳服务器、大型计算机、高性能计算设备等信息技术设备，构成一个或多个永久性或半永久性的结构。

2.建设现状

数据空间建设尚未形成统一的国家战略，但在政府、企业及国际合作层面取得多项关键进展，初步构建起数据互通

与共享机制，通过以下多维举措构建数据流通与价值释放体系。

明确数据权属。借助《加州消费者隐私法案》（CCPA）《数据安全管理法》（DSM）等立法，界定数据所有权、使用权及收益权，为数据的合法合规使用提供了法律依据。

统一标准与安全机制。政府推行开放数据政策，发布涵盖数据格式、元数据及 API（应用程序编程接口）标准等多个维度的标准规范，增强数据安全流通的效率。

构建完整数据生态。依托清晰权属与交换机制，数据驱动传统产业升级（如智能制造、精准农业）与新兴产业发展（如大数据分析、人工智能）。

政企协同，社会参与。政府鼓励私营部门与社会组织融入开放数据生态，引导医疗、金融等领域通过数据共享开发智能应用，拓展创新场景。

云平台主导数据汇聚。亚马逊网络服务（AWS）、谷歌云平台（GCP）、微软 Azure 等超大规模云服务商，构建了数据整合、流通环境，涉足数据共享与行业解决方案，影响全球数据格局。

数据经纪商驱动数据交易。碎片化监管环境催生数据经纪商，通过收集、分析、销售消费者与商业数据，形成服务于营销、风控等领域的数据产品体系。

此外，微软和亚马逊已加入 IDSA，并且亚马逊在数据空间实现技术方面借鉴 IDS 信任框架及 Gaia-X 信任框架定义安全规则，以数据空间协议规范传输、交换和访问，基于 Eclipse 数据空间组件建设连接器和 FIWARE TRUE 连接器，支持和管理数据流通的实现。

3.技术架构与核心能力

2005 年初在司法信息交换数据模型标准的基础上开发形成 NIEM（National Information Exchange Model）1.0 版本。NIEM 是一种由业务领域驱动的、基于标准的信息交换方式，在于解决不同领域之间以及同一领域内各级部门之间的信息共享问题，用于指导和管理信息交换的实施框架。NIEM 框架结构主要由技术框架、运用框架与管理框架三部分组成，至 2021 年底，已经发布了 5 个大版本、11 个小版本的模型框架。以开放标准与分散式体系为核心，联邦层面通过 NIST 的《数据参考模型》、OMB 的数据治理范本推动兼容标准与 API 互联互通；遵循 FAIR 原则（可寻找、可获取、可互操作、可重用）和 W3C 开放数据标准（如 DCAT 数据目录规范）提升不同来源数据的互操作性和可集成性；采用去中心化的治理模式，各机构保有对自身数据的控制权，通过标准化接口共享数据，数据在持有者之间直接交换。核心技术能力涵盖数据目录与元数据管理、数据 API 网关、身份认证与访问控制，以及隐私保护技术（如推动机构单点登录

与身份联邦）；数据权限管理以法律约束为主，正探索基于标签的自动化数据使用控制机制。

4.相关参与方

政府、行业协会、科研院所和第三方服务机构等多元协同，各主体分工明确，共同构建起数据要素市场生态基石。

政府是市场引导者与规则制定者。出台《联邦数据战略》《开放政府数据法案》明确市场发展路径，以《美国人工智能倡议》锚定技术创新方向；以资金支持、税收优惠鼓励市场投资；借助《加州消费者隐私法案》（CCPA）等法规，设立专门机构，保障市场合规。

行业协会是桥梁纽带。信息技术与创新基金会（ITIF）通过组织研讨会、国际合作论坛，聚焦数据共享中的知识产权、隐私安全等具体问题，推动跨主体信息互通，并促进国际合作，助力全球数据规则协调。

科研院所是创新源泉。斯坦福大学、加州大学伯克利分校等顶尖学府，凭借其领先的科研实力，与企业合作将科研成果转化为实际应用；开设专业课程、开展实习项目以及与业界合作，培养专业人才；参与国际合作，提升美国市场竞争力，推动全球数据要素市场繁荣发展。

第三方服务机构则是市场润滑剂。Acxiom 和 Experian 等数据经纪公司，提供数据清洗、分析等服务，定制解决方案助力企业营销；通过运营数据交易平台，搭建供需桥梁，

降低交易成本，推动数据流通与价值最大化。

（三）日本可信数据空间发展现状

1.政策与法律环境

日本可信数据空间的构建是在一系列国家战略、法律法规及治理准则的指导下进行的。这些顶层设计不仅明确了发展方向和核心原则，也为数据的高效、安全、可信流通与利用奠定了基础。日本的数据战略经历了从宏观框架到具体行动计划的迭代发展过程。其起点是2020年12月数据战略工作组发布的《数据战略》，随后在2021年6月经内阁会议通过了《综合数据战略》，进一步由2023年6月9日内阁批准的《数字社会实现重点计划》加以细化和落实。同年12月，针对人工智能出台了《公共及私人数据开发与合作行动计划》。2024年内阁批准的《数字社会实现重点计划2024年版》进一步强调了通过数据协作来强化数字产业基础和提升竞争力。在对外多边贸易协定上，将数据自由流通与信任（DFFT）原则纳入双边及多边贸易协定，如《美日数字贸易协定》和《日英全面经济伙伴关系协定》，清晰地表明了日本希望将这一理念转化为实际经济利益和具有约束力的承诺。此外，日本政府正通过数字厅和经济产业省（METI）积极制定《数据治理准则》，旨在构建一个统一的数据生态体系。这些准则聚焦于跨境数据的实际处理、数据安全，将重点从信息系统单元转向数据本身、数据成熟度以及人工智能

的利用等关键领域。在个人信息保护上，日本制定《个人信息保护法》（APPI）作为个人数据保护的法律基石。其核心条款对个人数据向境外的传输做出了限制。在网络安全上，制定《网络安全伴随数字化转型（DX with Cybersecurity）》《国家安全保障战略》（NSS）和《国家防卫战略》（NDS）强调加强网络防御能力，并支持私营部门防止信息泄露。这一系列文件的出台显示了日本政策的逐步深化和对新兴技术的快速响应。

2.建设现状

日本正通过多个并行且各具特色的项目，积极推进其可信数据空间的建设。这些项目不仅体现了国家战略的落地，也反映了不同领域对数据共享和利用的迫切需求。日本正积极推动数据空间的建设，关键举措包括用于跨领域数据联邦的 Data-EX、用于工业数据(最初侧重于电池追溯)的 Ouranos 生态系统，以及用于智能制造的互联工业开放框架（CIOF）。这些项目得到了政府战略和如战略创新推进计划（SIP）等资助计划的支持。

3.技术架构与核心能力

日本可信数据空间的构建，依赖于一套明确的技术原则和不断演进的架构体系。其核心在于如何在保障数据主权的前提下，实现高效、安全的数据互操作，并在此基础上催生新的数据价值。数据主权、互操作性和信任是日本数据空间

建设的三大基石。数据主权确保数据提供者对其数据保留权利和控制权，这是 Data-EX、Ouranos 生态系统和 CIOF 等项目的核心特征。互操作性旨在实现数据在不同国家、组织和系统间的顺畅连接与交换，而信任则通过安全和可靠的数据交易机制来保障。日本对这三大原则的持续强调是一种战略定位，旨在通过解决关键的商业顾虑来吸引参与者，从而在全球数据生态系统中建立差异化的竞争优势，创建一个有吸引力且可靠的数据驱动创新环境。核心技术架构参考如下：

（1）用于 Data-EX 的 CADDE（去中心化数据交换连接器架构），CADDE 是在 SIP 第二阶段为实现组织间安全高效的数据共享而开发的，并构成了 Data-EX 的基础。CADDE 采用联邦架构，支持去中心化的数据交换，允许在维护数据主权的同时，在各行业间发现和利用数据。Data-EX 则进一步扩展了 CADDE 的能力，构建了更广泛的数据交换基础设施。

（2）Ouranos 生态系统数据空间参考架构模型（ODS-RAM）与 ODS 协议，ODS-RAM 白皮书由经济产业省（METI）和信息处理推进机构数字架构设计中心（IPA DADC）于 2025 年 2 月发布，该模型包含一个分层结构。ODS-RAM 是一个面向服务的架构，分为四个松散耦合的层（Layer）和四个视角（Perspective），各自对应相关的角色、协议和服务模型，旨在解决数据互操作过程中的结构性问题。“构建模

块组合（Building-Block Portfolio）”（一种开源软件规范）作为 ODS 协议的参考实现。ODS-RAM 采用面向服务的松散耦合分层和多视角设计，旨在为多样化的工业用例提供灵活性和适应性，而非一种僵化的“一刀切”方案。松散耦合的层次结构意味着一个层次的变化不太可能导致其他层次的必要变化，从而促进了模块化和架构的便捷演进。其“四层四视角”结构，表明这是一个旨在系统性覆盖数据互操作性各个方面的综合模型。

（3）CIOF 技术框架，由产业价值链倡议（IVI）推出的互联工业开放框架（CIOF）基于 IVI 的“松散标准”、对等数据交换和数据所有权理念，推动数据共享。其架构涉及“超连接终端（Hyper Connection Terminals, HCT）”、“超连接服务器（Hyper Connection Server, HCS）”和“超连接管理器（Hyper Connection Manager, HCM）”，用于管理数据交换、字典和合约。CIOF 支持数据知识产权管理、质量保证和中小企业集成等用例。产业价值链参考架构（IVRA）则为 CIOF 提供了结构基础，包含业务层、活动层和规范层。CIOF 的设计强调“松散标准”和通过特定组件（如 HCT/HCS/HCM）管理的对等连接，这种务实的架构特别适用于多样化的制造场景，尤其是许多可能仍在使用遗留系统的企业。制造场所通常混合了新旧机器和 IT 系统。高度僵化的集中式数据交换标准在这种异构环境中难以实施。“松散标准”和对等方法允

许更灵活的集成，连接现有的“自动化孤岛”。

4.相关参与方

政府：日本政府通过公私合作伙伴关系（PPP）积极推动数据空间的发展。数字厅和经济产业省（METI）是领导这些工作的关键政府机构。Ouranos 生态系统被明确描述为公私合作的成果。

行业协会：日本的 Data-EX 由数据社会联盟运营，提供 Ouranos 的电池追溯平台 ABtC、由行业主导论坛 IVI。

技术路线运营商：日本丰田、松下等企业推动 Ouranos 工业数据与系统平台连接。

监管机构：日本个人信息保护委员会（PPC），独立于政府部门，直接依据法律授权开展工作。

（四）国外可借鉴工作经验及趋势

1.可信数据空间模式对比

从国外可信数据空间发展模式的对比来看，不同国家和地区因自身特点形成了差异化路径。

表 3 国外数据空间模式对比

国家/地区	驱动模式	核心参与者	技术发展重点	政策与管理方式	主要应用场景
欧盟	法规驱动的一体化建设	欧盟委员会、成员国、科研机构	依据 GDPR 引入隐私计算、区块链，构建“单一数据市场”	严格执行 GDPR，欧盟统一规划，成员国协同建设	跨境电商、医疗、工业数据流通
美国	市场主导的技术创	科技巨头、开源社区、	智能合约优化、跨链协同，融合	以法律监管为主（如 CCPA），	金融科技（跨境支付、实时

	新驱动	金融科技及互联网企业	人工智能、物联网等技术	行业协会制定标准、推动自律	结算）、人工智能
日本	战略导向的渐进式发展	政府、企业、科研机构、行业组织	数据安全、隐私保护，引进国际技术并本地化	国家数据战略指导，政府设工作组、提供资金，行业组织推动标准与交流	社会保障（社保信息整合）、制造业（供应链追踪）

欧盟是法规驱动的一体化建设模式，欧盟委员会、成员国及科研机构为核心力量，依据GDPR引入相关技术构建“单一数据市场”，通过法规强制和统一规划推进，应用于跨境电商等领域，旨在实现区域内数据的一体化流通与应用。

美国采用市场主导的技术创新驱动模式，核心参与者包括谷歌、微软等科技巨头以及以太坊基金会等开源社区，技术上聚焦智能合约优化、跨链协同并融合新兴技术，政策以法律监管为主，行业协会助力规范，应用集中在金融科技和人工智能领域，凭借市场力量推动技术创新与数据价值释放。

日本以战略为导向渐进式发展，在国家数据战略指引下，政府、企业、科研机构和行业组织共同参与，技术聚焦数据安全与隐私保护，政府主导规划并提供支持，应用于社会保障和制造业，注重稳步推进与国际技术的本地化结合。

2.国际可借鉴的工作经验及趋势

（1）顶层制度设计：政策引领与规则构建

国际可信数据空间建设以政策规范为核心驱动力，形成

“引导—保护—协同”的制度框架。德国通过发起“工业数据空间行动”并配套研究资金，推动 IDS 架构落地，构建工业领域数据治理基础；欧盟以《通用数据保护条例》（GDPR）为基石，建立数据跨境流动与隐私保护的高标准体系，强制规范数据处理全流程；美国则依托《加州消费者隐私法案》（CCPA）等法律群，形成细分领域的保护框架。日本与韩国则是通过构建一系列国家战略、法律法规及治理准则，明确可信数据空间的发展方向和核心原则。

对我国而言，需强化政策顶层设计，通过专项政策引导企业与科研机构突破可信计算、数字合约、使用控制等关键技术，建立“政策激励—企业创新—科研支撑”的协同机制，同步完善数据安全与隐私保护的法规体系，为数据空间建设提供制度保障。

（2）技术路径建设：架构创新与生态集成

国际技术实践呈现“互操作性架构+可信技术融合”的双轨模式。在架构层面，欧盟 Gaia-X 项目通过制定统一数据治理规则，推动跨国跨领域的数据协同；IDS 架构以共识性技术规范为基础，实现工业数据的安全交换与可信共享。在基础设施领域，美国 AWS、微软 Azure 等科技巨头依托全球数据中心与云计算服务，构建了支撑大规模数据处理的技术底座。

对我国而言，需构建“自主创新+兼容国际”的技术路径：

参考 IDS、Gaia-X 等架构的互操作协议，制定开放、安全的数据空间架构标准；重点突破使用控制等核心技术，推动区块链与数据沙箱等技术的模块化集成，形成兼具安全性与灵活性的技术体系。

（3）标准体系打造：标准化与生态化推进

国际标准体系打造上，通过构建以下几点推进可信数据空间标准生态的发展。一是打造技术协同体系，通过搭建开放科学数据合作平台，促进政府、企业、科研机构在数据技术研发、场景应用等领域的互联互通，推动产学研用深度融合。二是构建开源技术框架，以数据空间连接器为核心组件，基于开源技术构建数据查询、交换、监控审计等功能模块，遵循数据主权原则推动跨企业数据共享，培育数据驱动商业模式。三是建立共享激励机制，通过建立数据贡献回报体系，通过数据访问优先权、数据分析结果共享、服务费用减免等形式，激励企业与机构参与数据空间建设，形成“贡献—收益”良性循环。四是设立数据保护机制，通过设立独立数据保护委员会，由各地监管机构代表组成，统一实施数据保护规则，协调跨区域数据治理事务，确保数据流通合规性。

对我国而言，建立可信数据空间标准体系需囊括数据流通利用、规则制定、安全保障等内容。综上，国际经验表明，可信数据空间建设需以“制度—技术—生态”协同为核心，通过标准化、激励机制与跨域协作，推动数据空间从技术工具

向数字经济基础设施升级，为我国构建自主可控的数据治理体系提供参考范式。

三、我国可信数据空间发展现状及趋势

（一）可信数据空间技术能力发展现状

1.可信数据空间技术架构概述

可信数据空间是国家数据基础设施的一部分，符合国家数据基础设施整体架构及基本约束。可信数据空间包括可信数据空间服务平台以及与服务平台对接的接入连接器。在继承国家数据基础设施业务节点、接入连接器基本要求的基础上，可信数据空间结合自身技术特征进行了一定的功能扩展。

可信数据空间服务平台可具备身份管理、接入连接器管理、目录管理、数字合约管理、可信数据空间管理、数据使用控制、国际空间互通网关 7 个功能，其中身份管理、接入连接器管理、目录管理可复用区域/行业功能节点相关能力，并可在此基础上结合可信数据空间业务需求进行扩展。国际空间互通网关为可选功能，由服务平台按需建设。应按照“三统一”要求，保持身份、标识、目录与区域/行业功能节点的互联互通。可信数据空间服务平台应与其他流通利用业务节点互联互通，在实际数据流通利用业务过程中宜按需复用其他业务节点的功能，如：数据交易、开发应用中心、数据托管、存证审计等，也可根据实际业务需求，在服务平台上集

成相应功能。

接入连接器是可信数据空间各参与方加入可信数据空间生态的入口系统，支持数据提供方、数据使用方、数据服务方通过接入连接器提供数据、使用数据以及提供增值服务，是依据数字合约执行使用控制的系统载体。接入连接器加入可信数据空间时应遵循国家数据基础设施连接器相关技术要求，并采取扩展模式的接入连接器。其中需扩展的功能包括：数据交付、数据资源管理、数据产品管理、数字合约管理、数据使用控制 5 项功能。

下面本章将身份认证、数据标识、数据目录、互联互通、存证溯源、数字合约、使用控制、数据检索、空间管理、数据匿名化、隐私保护计算安全保障几个方面介绍我国可信数据空间技术发展现状及趋势。需要强调的是，以上技术需要通过标准化来统一接口、流程和要求，以确保技术的互操作性、规范性和可推广性。后续将通过制定相关技术标准来推动这些技术在可信数据空间中的落地，增强其权威性和公信力。最终，标准化的技术将成为可信数据空间建设的重要支撑，确保数据流通的安全、高效和合规。

2.身份认证技术

身份认证技术是指通过一系列技术手段验证主体（如个人、设备或系统）身份真实性的过程，通过验证用户提供的凭证与预存信息的匹配性，确保操作主体合法性的安全机

制。其本质是建立“信任链”，并确保身份信息不被伪造、冒用或篡改。它是信息安全体系中的基础环节，广泛应用于网络安全、数据访问控制、金融交易、政务服务等场景。我国在该技术领域主要采取以下几个技术路线：

（1）基于知识的认证，该认证方式属于较传统的认证方式，是用户通过记忆的信息证明身份方式。包括使用用户名/密码以及安全问题验证方式，例如各种 APP 登录、日常支付、密码找回等。该认证方式成本低，简单易用，但由于密码容易泄露或被暴力破解，安全信息也可能被猜测或窃取，因此安全性有限。

（2）基于拥有的认证，用户通过持有特定物理设备或数字凭证验证身份方式。包括动态口令（银行 U 盾、手机 APP）、短信/邮箱验证码、智能卡/USBkey、数字证书等方式。常见于银行、金融等行业，以及 CA 机构或商密厂家。

（3）基于生物特征的应用，该认证方式利用用户生理或行为特征以及做活体检测来验证身份，主要包括：指纹识别、面部识别、虹膜扫描、声纹识别、步态识别、眨眼/摇头动作检测、红外光血管扫描等。该认证方式唯一性强，安全性较高且用户体验便捷，但成本较高技术成熟度低，且生物信息一旦泄露不可重置。

（4）数字身份与匿名认证，该认证方式将实体身份转化为数字凭证，支持跨平台可信验证。匿名认证则是在不暴

露真实身份的前提下完成验证。应用包括 CTID 网证，公安部“互联网+可信身份认证平台”，将身份证加密为二维码（如微信“网证”）；嵌入公民身份信息的 eID 芯片卡，支持匿名可控的身份验证（如部分银行开户）该认证方式效率高安全性强，可有效减少明文信息暴露，支持隐私保护。

（5）基于度量值的应用身份认证，该认证方式通过可信根获取应用的真实度量值，再通过度量值关联应用程序的源码，从而实现对应用进行基于行为的身份认证。国外 CPU 可以支持上述能力，但会导致可信根被国外掌握。一些国产 CPU 也陆续支持了上述能力，可以将可信根从 CPU 中剥离，为各种 CPU 提供统一的可信根自主可控方案。

前期，全国数标委发布了《数据基础设施 用户身份管理和接入要求》技术文件，规范了统一用户身份的总体要求、身份信息构成、注册及认证流程、跨平台身份互联互通机制以及相关接口与安全管理要求，旨在保障接入主体、接入连接器及平台的身份可信，以实现用户身份的跨节点互联互通，支撑全网范围内的统一身份管理和明确的职责分工。

3.数据标识技术

标识是对主体、物品、信息内容、网络位置等对象进行唯一标记、识别、定位的信息符号。数据标识是对数据涉及的特定物理或逻辑对象的标识编码、标识赋码及标识解析，数据涉及标识对象包括机构、人、物品、数据产品、数据资

源、平台系统等。数据标识通过为数据涉及标识对象分配唯一标识符，实现快速准确的检索和定位，强化标识对象的可追溯性、可访问性，促进数据互联互通。从技术实现角度，数据标识可分解为标识编码、标识赋码及标识解析三个阶段。其中，标识编码是数据标识的起点，其核心是通过特定规则生成唯一、可解析的标识符，包括数据涉及标识对象编码规则设计、生成算法实现等；标识赋码是将编码后的标识符关联到数据涉及标识对象的过程，涵盖赋码载体选择、赋码流程控制、对象关联管理等；标识解析是通过标识符反向获取关联数据涉及标识对象的过程，包括解析协议、对象查询、权限控制等。目前，相对成熟标识体系有 Handle、OID、DOI、VAA 等，由于其管理机构、应用场景、服务目标的不同，体系方案各有侧重点，用于支撑相关具体场景的应用需求。

前期，全国数标委组织发布了《数据基础设施 标识要求》技术文件，构建了基于“全域功能节点－区域功能节点－行业功能节点－业务节点－接入连接器”的多层级分布式标识体系框架，制定了用于数据涉及标识对象的标识符编码规则，包括主体标识码、平台与接入连接器编码、数据产品与数据资源编码等，并明确了标识赋码和标识解析的相关要求。技术文件的发布实施，有效推动了数据标识体系建设进程，对建立全国统一的数据标识互认机制具有重要战略意

义。

4.数据目录技术

在可信数据空间中，数据目录作为数据资产展示窗口、数据交易的“撮合平台”、数据治理的“管理工具”、数据价值的“评估基准”和数据创新的“催化剂”，为数据价值流通提供基础支撑。技术实现上，数据目录系统通常包括元数据采集（自动采集与人工录入相结合）、元数据存储（采用关系型或图数据库）、元数据管理（提供增删改查和版本控制）、元数据服务（以 API 形式提供服务）和用户界面（提供交互窗口）等模块，采用微服务架构提高系统可扩展性和可维护性。

国内数据目录技术发展迅速，全国数标委发布了《数据基础设施 用户身份管理和接入要求》技术文件，规定了数据基础设施中数据资源和数据产品目录的描述要求、技术要求和安全要求。未来数据目录将不再是简单的数据资产登记簿，更多的综合元数据采集、数据血缘、数据标签、数据分类分级、数据发现等技术，为可信数据空间建设提供更加坚实的基础支撑。

5.互联互通技术

互联互通技术指的是利用标准化的接口、协议和机制，实现不同数据基础设施节点间无缝连接和数据流通的技术。其核心目标是消除数据孤岛，推动数据在可信数据空间中高

效、安全地流通，确保数据的可用性和互操作性。

在可信数据空间内，互联互通技术是数据要素市场化配置的核心支撑。它保障了数据基础设施各节点（包括区域功能节点、行业功能节点、业务节点等）间的信息同步和跨域协作，提升了数据流通的效率和安全性。通过互联互通技术，可以实现数据资源的统一目录管理、身份认证、数据传输和使用控制，进而构建全国一体化的数据市场，推动数据要素的高效利用和价值释放。

国内在互联互通技术的研究与应用方面已取得显著进展，特别是在数据基础设施的标准化和协议制定方面。全国数标委发布了《数据基础设施 互联互通基本要求》技术文件，规定了数据基础设施互联互通的技术要求、业务流程、能力要求和接口要求，详细描述了全域功能节点、区域/行业功能节点、业务节点以及接入连接器的功能框架及其互连互通方式。为实现数据基础设施的互联互通，国内正在实施“统一目录标识、统一身份登记、统一接口要求”的三统一原则，确保基础设施的互操作性。

国内正在增强数据基础设施的互联互通能力，包括南北向和东西向的互联互通。南北向互联互通涉及区域/行业功能节点与全域功能节点、业务节点、接入主体之间的连接。东西向的互联互通则包括不同区域/行业功能节点之间、不同全域功能节点之间、业务节点与接入主体之间的互联互通。

在东西向的互联互通方面，国内积极参与协议层级的国际标准研究。同时，在可信数据空间技术架构设计中预留了国际空间网关，以便未来与国际数据空间实现无缝对接。这一措施为国内数据基础设施与国际数据空间的互联互通提供了技术保障。国内正在加强与国际组织和其他国家的合作与交流，既可借鉴国际先进经验，也能为全球数据流通提供中国方案和技术支持。

这些进展表明，国内正在从数据、应用、底层互通协议多个层面逐步完善互联互通技术体系，以满足数据基础设施的互联互通需求，提升数据流通的效率和安全性。

6.存证溯源技术

存证溯源技术是一种结合区块链、密码学、时间戳以及数字水印等技术的数据管理、流通方案，旨在确保数据全生命周期的可追溯、可验证和不可篡改性。其核心目标是为数据生成、存储和流转的全生命周期提供不可篡改的证明，并在需要时能够追溯其来源和变更历史。

可信数据空间是保障数据安全流通与可信协作的关键基础设施，而存证溯源技术在其中扮演了确保数据全生命周期可追溯、可验证和不可篡改的核心角色。在可信数据空间中，数据在各类共享交付过程中，可能面临数据泄漏问题，使用“数字水印+区块链存证”技术、数据血缘+可信计算技术，可实现数据的“嵌入-流转-溯源”全流程可信记录，提升

证据法律效力。

存证溯源技术通过技术融合构建数据信任体系，已在金融、政务、供应链等领域展现显著价值。然而，在“大数据存储与信息溯源”方面，存在“数据实体海量增长、溯源效率低下”等现状，相关技术仍处于研究优化阶段。随着技术研发深入与应用场景拓展，其将成为数字经济时代数据要素安全流通的核心基础设施，为构建可信社会提供关键技术支撑。

7.数字合约技术

数字合约技术是以数字化形式描述的数据提供方、数据使用方、数据服务方等相关参与方对数据流通、使用等环节预期的承诺，包括但不限于数据的内容、使用者、使用方式、使用次数、使用范围、使用环境等。可信数据空间通过数字合约技术描述特定参与方对数据内容、使用方式、使用次数等流通利用行为的预期并达成共识。数字合约是可信数据空间执行使用控制的基础，数字合约通常以机器可解释的标记型语言，如 XML、JSON 等格式对数字合约的内容进行描述。使用控制识别、解释数字合约中对数据流通行为的“约束”，并基于“约束”在数据流通、使用过程中进行控制。

目前，大部分国内可信数据空间方案均采用国际数据空间 IDS 的数字合约技术。与此同时，国内高校、科研机构、领军企业等也在可信数据空间的数字合约技术上开展了积极创新，典型代表包括 4W2H 技术、数据语用技术等。交换

数据空间 EDS 将数字合约的控制策略分为：Who（使用者）、When（使用时间）、Where（使用环境）、What（数据内容）、How（使用方式）、How Much（使用次数）六大类、32 个子控制策略。北京大学基于数据在不同场景下的使用方式、目的及效用的数据语用原理，提出了数据语用标记语言 DPML（Data Pragmatic Markup Language），通过对数据、算法、环境等资源的输入、输出及交互关系的形式化描述，来对特定场景下数据的内容、使用方式、环境及输出进行约束。

8.使用控制技术

使用控制技术是一种依托动态策略引擎，对数据使用者的身份、行为、环境等多维度属性开展实时评估，进而实现对数据访问、分析、计算及处理等行为进行精细化管控的技术。该技术不仅聚焦于数据的访问权限，还对数据的使用方式、时间、范围等进行精准把控，以确保数据的使用过程契合预期的策略与规则。在可信数据空间中，使用控制技术是达成数据安全可信流通的核心手段之一。它突破了传统静态授权模式的束缚，能够依据数据使用者的实时状态和使用场景动态调整权限。

我国在使用控制技术方面覆盖但不限于数据内容、使用方式、使用频次、使用范围以及使用环境等多个关键维度，涉及多种使用控制策略。例如，对照欧盟 IDSA 初步提出的文件级控制粒度的 6 种基本策略，包括数据主权声明、目的

限制、留存期限控制、审计追踪、二次传播约束及合规性验证等，华为将其扩展至32种策略，分为Who（使用者）、When（使用时间）、Where（使用环境）、What（数据内容）、How（使用方式）、HowMuch（使用次数）六大类，新增动态水印、敏感操作拦截、使用次数或时长配额等，其高度精细化的策略分类能够精准满足不同应用场景下的数据使用需求，控制粒度达到字段级；同时，数鑫科技通过部署10项访问策略和11项使用策略，实现对数据全生命周期的使用控制，其中，访问策略包括限制能使用数据的相关方节点、允许或禁止对数据的使用、限制使用数据的相关方、限制能使用数据的相关方节点安全级别、限制能使用数据的时间窗口、限制能访问数据的最大次数、记录数据使用日志、访问需求要通知数据提供方、限制不能使用原始数据、数据被访问之前需满足合规性等，使用策略包括使用关系必须供需双方认可、限制相关方使用数据的上层应用系统、限制相关方使用数据的用途、限制多个数据联合使用的方法、限制相关方使用数据的字段、限制相关方存储原始数据、限制相关方使用数据前的加工处理方法、限制使用数据的范围（不可复制）、数据使用后必须删除（阅后即焚）、限定相关方不能分发原始数据给第三方、异常提醒等，控制粒度达到字段级。

由此可见，业界的积极探索也反映了对使用控制技术相关标准的迫切需求，当前全国数标委已经规划《可信数据空

间 数字合约技术要求》《可信数据空间 数据使用控制技术要求》并稳步开展相关标准工作，推进数据使用控制技术的规范、普及。

9.空间管理技术

空间管理技术是基于统一管理与调度机制，对数据空间内的计算、存储及网络资源进行优化配置与动态管理的专业技术。其核心目标是提升资源利用效率，保障系统安全性，满足不同应用场景对性能与安全的需求。该技术通过动态调整资源分配，确保数据处理任务高效执行，同时支持跨区域、跨行业的算力协同，为数据要素市场化提供技术支撑。

空间管理技术可通过逻辑隔离、物理隔离等技术方法，实现同一基础设施上构建不同数据空间，以降低成本与复杂度。空间管理技术主要针对可信数据空间中的数据存储、网络通信、计算资源、权限管理等。其中，逻辑隔离适用于资源利用率要求高的场景，依赖标识管理、网络分区、容器化部署与访问权限控制；物理隔离主要保障高敏感数据存储、计算与网络资源的独立使用，并在物理层严控访问权限。

10.数据匿名化技术

数据匿名化通过技术手段彻底消除所有直接和间接标识符，确保数据无法以任何方式关联到个体，避免了数据的重识别风险，使数据完全不可逆且无法重新识别个人，达到法律意义上的“非个人数据”，安全高效地使用数据。在可信

数据空间中，数据匿名化技术能够在不需要个人授权的前提下，实现数据的可信共享和高效利用，消除了数据资源持有方的顾虑，促进了数据的跨域流通和融合。匿名化技术不仅符合法律法规要求，还响应了社会对隐私保护的期待，为数据要素的市场化流通提供了可行性路径。

国内在数据匿名化技术方面已经取得了一定的进展。一方面，国家相继出台了《中华人民共和国个人信息保护法》《中华人民共和国数据安全法》等法律法规，明确了匿名化处理作为数据合规流通的重要路径之一。另一方面，相关标准和指南也在不断完善，例如拟研制的《数据匿名化流通实施及评估指南》等标准，为匿名化技术的实施提供了规范和指导。此外，国内企业和研究机构也在积极探索和应用匿名化技术，结合隐私计算、区块链等前沿技术，进一步提升了数据共享的安全性和可信度。

11.隐私保护计算技术

隐私保护计算指在保证数据提供方不泄露原始数据的前提下，对数据进行分析计算的一类信息技术，保障数据在产生、存储、计算、应用、销毁等数据流转全过程的各个环节中“可用不可见”。隐私保护计算不仅支撑了空间中数据的可信管控，而且支持跨主体、跨行业的数据联合挖掘，推动数据要素的高效流通与价值转化。常用方案包含多方安全计算、联邦学习、机密计算、可信计算、密态计算等。隐私保

护计算支撑数据提供方构建使用管控策略，保障提供方的数据持有权，约束数据使用方在不直接接触原始数据的前提下，以密文交互的形式对数据进行分析和建模。数据服务方侧如数据开发等，隐私保护计算能够打造可信开发利用环境，使得数据服务方在数字合约约定授权范围内和使用方式下对数据进行开发利用，有效管控数据泄露和非约定使用。

国内多家企业的隐私保护计算产品正融合联邦学习、安全多方计算、可信执行环境、可信计算、国家商用密码、图数据融合、安全 SQL 等多元技术，专注于加密算子和联邦学习算法、结合软硬件优势，打造满足复杂场景需求的全场景解决方案，平衡性能、安全与精度。某些企业将隐私保护计算与大模型相结合，为企业在数据利用和模型优化方面提供了新的途径和方法。某些企业实现大规模、低成本的数据流通，并进一步叠加密码学与可信硬件双重防护，推动产业从主体信任走向技术信任，实现数据全链路密态保障。

12.安全保障技术

（1）密码技术

国内密码技术发展势头强劲，《中华人民共和国网络安全法》《中华人民共和国数据安全法》等法规驱动企业强化密码技术的发展与应用。SSL/TLS、IPSec 等标准技术应用成熟，量子密钥分发、区块链存证等前沿技术处于世界领先地位，“京沪干线”量子通信网络与“墨子号”卫星等重大项目成

果瞩目，蚂蚁链在电子合同上链存证领域发挥重要作用，至信链为版权作品传输筑牢安全防线。产业生态中，一些企业推出 VPN、SD-WAN 等应用产品；产学研协同紧密，高校与科研机构在量子密码、区块链、碎片化多路传输等方向不断取得突破，推动我国密码技术迈向更高水平。

（2）日志审计技术

可信数据空间依托日志审计技术形成全链路管控体系。借助大数据关联分析技术构建多维审计模型实现行为追溯与责任界定，蚂蚁链摩斯平台在金融场景实践中，通过关联分析银行账户操作日志，成功识别某账户非工作时间高频调用信贷数据接口的异常行为，助力某银行拦截数十亿高风险贷款，模型预测效能提升 25%；某政务数据平台基于 Elastic search 搭建的日志审计系统，通过预设“同一 IP 地址短时间内多次访问”等规则，自动生成审计报告并推送监管部门，实现对《中华人民共和国个人信息保护法》的精准合规管控。

（3）分类分级技术

数据分类分级需要识别涉及的重要数据和核心数据，然后建立相应的数据安全保护措施。数据分类分级技术是通过结构化规则引擎或智能化分析手段，对数据进行特征识别、语义解析，根据国家相关法规形成标准化安全等级的体系化技术组合。

国内目前大部分分类分级产品都采用规则引擎技术做

敏感数据识别，识别敏感数据的规则包括数据标识符、正则表达式、关键字、词典、精确指纹、DNA、机器学习等。随着人工智能的进一步发展，部分厂商将人工智能融合到分类分级中，提升分类分级技术的智能化能力。部分厂商瞄准现行纸面上的数据分类分级体系难以有效匹配行业产业动态复杂实践的难点，基于大模型驱动的智慧引擎升级，实现政策法规与业务数据的精准映射。比如某企业的数据资产管理平台助力数据出海，通过 AI 智能数据对 PB 级数据进行分类分级，实现了 7 级分类与 5 个敏感级别的打标，出海数据打标正确率达到 85%以上，实现 90%以上数据自动识别，敏感数据标定效率提升 60%，形成对资产底数的梳理与管理、出境资产的审核评估、资产出境行为的监控等一系列安全管控。某企业数印技术支撑基础运营商，通过多模态大模型的自适应分类分级体系，在法规政策、行业场景拆解细化和动态语义理解基础上对未知数据类型进行智能推荐分类分级，帮助更好合规运营，升级数据治理工具箱。

（二）可信数据空间应用发展现状

我国可信数据空间应用实践呈现出多元化与多层次特征，目前在地方、行业、企业和跨境等各类可信数据空间中均有所涉及。其中，地方可信数据空间涵盖了区域、城市等类型可信数据空间，而个人可信数据空间实践仍有待探索实践。可信数据空间可以支持多方开展价值协同和业务合作，

形成多元主体共建共治共享的模式，打造可信数据空间发展的良好生态。这些实践不仅推动了数据要素的高效流通，还推动了一系列的技术与机制创新，进一步激发数据价值，促进全国一体化数据市场的构建。

1.地方可信数据空间应用发展现状

（1）发展现状

地方可信数据空间是面向特定区域或城市内多元主体，构建跨部门、跨行业的数据共享协同的环境，旨在整合和利用地方多源异构数据，构建安全、高效、可信的数据流通基础设施。其核心目标是打破地方内部各部门、各行业以及公共数据与社会数据之间的数据壁垒，促进数据要素在地方治理、公共服务、产业发展等领域的融合应用与价值释放。

多地已将城市数据空间纳入发展规划并启动试点。南京、青岛、成都、济南等地发布了城市数据空间建设方案，并形成首批示范成果。目前这些空间大多处于试点运营阶段，核心应用场景与数据集不断丰富。重庆等地也在探索跨区域数据共享机制，推进城市群协同。总体上，城市空间建设正逐步迈向成熟，典型项目开始产生示范效应。例如，江苏南京市依托公共数据交易平台和算力网络建设“南京城市可信数据空间”，融合了城市运行、生物医药、智能交通、绿色低碳等 12 个重点领域的数据资源。从典型场景看，主要集中在三类高频领域：一是公共数据流通与交易；二是城市

治理与决策支持；三是跨行业数据融合应用。这些实践表明，地方可信数据空间通过汇聚城市数据、制定统一标准、构建信任机制，有效促进了数据要素在城市范围内的深度融合与应用。然而，城市数据来源复杂、数据权属多元、数据安全与隐私保护要求高，仍需在技术标准、管理规范和运营模式上持续探索。

（2）建设模式

建设模式上，城市级数据空间多由地方政府或城市数据管理部门牵头建设，以公共数据为牵引，撬动城市内产业数据资源共享流通与融合利用，推进城市内数据资源开发利用、赋能城市全域数字化转型。部分地方采用政企合作模式，政府提供政策支持和公共数据资源，企业提供技术解决方案和运营服务，实现优势互补。

在技术架构方面，通常采用“一体化平台+分布式节点”的设计理念，以政务云为基座整合社会多源数据资源。城市级数据治理和共享平台（如数据湖、数据仓库、统一数据目录）构成系统基础，配合可信连接器、区块链技术和容器化数据沙箱，保障数据交换的可控性和可追溯性。

（3）运营模式

在运营模式上，地方可信数据空间通常以政府主导为主，运营场景多集中于民生相关的重点领域。数据提供方包括政务部门和产业企业，数据使用方为应用开发者和科研机

构，数据服务方提供存算资源和隐私服务，监管方落实合规要求。各方通过“多方共建共治”机制协同推进。在数据流通和安全保障方面，运营机制引入了隐私计算技术，实现公共数据与商业数据“可用不可见”，确保数据主体权益；通过链路加密和多节点部署，增强大规模数据交互的性能与安全性。同时，应用层引入城市大数据分析、人工智能引擎和数字孪生模型，推动数据的深度利用和价值转化。规则机制上，由市级数据主管部门牵头制定互联互通规范和收益分配规则，强调数据安全、隐私保护与成果回馈，确保数据在全生命周期内实现合规管理。

2.行业可信数据空间应用发展现状

（1）发展现状

行业可信数据空间主要由行业主管部门、头部企业或协会牵头发起，基于技术信任机制（如隐私计算、区块链）与制度信任体系（如规则、标准、法律）构建全链条数据共享的可信数据流通基础设施，实现“数据可用不可见、可控可追溯”，促进数据要素高效流通与价值释放。行业可信数据空间以行业通用数据标准和高价值数据为基础，通过建立统一规则、共建共享平台和多方协同机制，打通企业间、区域间的数据壁垒，提升全行业的数据互联互通水平与协同效率。其目标面向行业领域共性需求和痛点场景，解决行业内数据标准不统一、数据难共享、监管难落实、创新难协同等关键痛

点，支撑行业在智能制造、绿色低碳、合规监管、协同研发等核心场景中的数字化转型与集成创新，推动形成以数据驱动的行业级智能协同生态。

目前，我国多个行业已启动可信数据空间的试点建设，形成了以能源、医疗健康、制造与新材料等为代表的重点行业实践场景。部分行业空间已进入应用阶段，具备较强的规模化推广潜力。例如，南方能源行业可信数据空间在电网、交通、制造等多个领域推动能源数据共享与价值转化，已汇聚超 300 亿条数据，构建 4000 余项能源指标，支撑绿色低碳应用开发；医疗行业在医保、药品流通等方面建设可信数据空间，推动实现多主体间医疗数据的标准化共享和过程可控使用，提升了行业监管和协同诊疗能力；在制造与新材料领域，江苏苏州等地建设以“计算+实验+数据+AI”为核心的研发协同数据空间，支撑材料仿真与性能预测，提升了行业创新效率与成果转化率。从典型场景看，主要集中在三类高频领域：一是产业链数据共享与质量溯源，通过建立全行业标准体系和数据交换平台，实现上下游生产、物流、质检等关键数据的互通可控；二是行业协同创新与联合研发，依托共享数据支撑多机构协同攻关与模型共建；三是合规监管与风险防控，如通过空间实现排放数据、设备运行数据等的自动化采集与合规监管，提升行业治理现代化水平。行业可信数据空间作为推动产业链一体化协同、加强行业监管能力、

赋能数字化转型的重要基础设施，通过促进数据互信与要素协同，不仅提升了产业链效能和创新活力，更为行业集体竞争力的提升提供了有力支撑。目前行业数据空间整体仍处于培育阶段，多数项目处于规划或试点期，并面临行业标准体系不统一、平台互操作性不足、数据确权与收益分配机制不健全等问题，制约了跨区域、跨领域融合发展。因此，亟待推动标准体系建设、关键技术突破与规则机制创新，以提升其通用性与可复制性。

（2）建设模式

在建设模式上，通常以共性价值牵引，多主体联合打造共性应用场景赋能全行业转型。由行业主管部门、龙头企业或协会牵头发起，联合上下游企业、科研机构、标准组织及技术服务商共同参与，形成“主管推动、企业共建、平台支撑”的建设格局。部分项目采用“政府牵头+行业骨干+平台公司”三位一体的联合推进机制，确保建设方案契合行业实际需求与发展规划。例如，在能源、医药、新材料等领域，已形成由行业头部企业提供数据资源与场景牵引、科研机构提供技术方法论支撑、平台型企业提供数据基础设施和隐私计算能力的协同构建模式。此类模式有利于统一行业标准体系，推动形成跨组织、跨环节的共享机制。

在架构设计方面，行业数据空间建设通常采用分层解耦、联邦协作的理念，整体呈现联邦式分布架构，形成“横向

连接行业各类主体，纵向统筹数据生命周期”的分层分域结构。行业节点侧由参与方（企业、研究机构等）部署本地数据连接器，实现身份注册、权限校验及受控数据接入；行业统一平台侧集中提供数据产品发布、目录管理、交易监管与交付追踪等核心功能；可信传输通道则基于专网或可信计算环境构建可审计、可验证的安全流通网络。

关键技术方面，建设过程中往往需集成统一数字身份认证体系，确保行业上下游企业身份互认；通过行业数据总线、标准化协议实现跨企业数据交换；利用数据沙箱与隐私计算技术保护敏感数据；同时以区块链登记和智能合约管理共治规则，保障数据交换的可审计性和可信性。各行业还会搭建行业知识库、AI 模型库等共享资源，进一步促进跨企业协同创新。

（3）运营模式

在运营模式上，运营主体可由行业协会授权的专业平台公司承担，或由龙头企业设立专门的数据运营机构负责日常运行与平台维护。为保障多方参与和规则共识，多数行业空间建立联盟理事会或运营委员会，由数据提供方、使用方、服务商与监管方共同参与运营决策与规则制定。在规则机制上，通常由参与企业、行业协会和监管部门共同制定统一规则（数据上链规范、定价机制、分红激励等）。部分试点项目由政府部门主导建立数据准入与分配规则，企业则负责提

供计算沙箱、标识解析等基础设施。牵头机构/龙头企业负责制定行业标准和数据规则，数据提供方为行业内上下游企业，使用方同属行业生态（或相关行业），第三方服务方提供数据治理、计算等服务，监管方监督合规。例如医疗行业空间就由医疗机构、数据技术企业和监管部门共同签署合作协议。行业空间内部建立互惠机制，如数据贡献奖励、利益分成等，确保不同类型参与方互利共赢。

从运营支撑能力来看，行业数据空间的核心运营依赖于其底层架构的技术稳定性和安全性。数据使用普遍遵循严格的分级授权机制，采用“一场景一审批”的精细化管理方式，确保数据合规使用。为了保证系统运行安全，运营机构还需部署可信执行环境，提供硬件级安全隔离，防止数据在处理过程中被窥视或篡改。与此同时，采用零信任架构、多因素认证、细粒度权限管理等机制，有效防止非法访问。通过构建统一的数据目录与服务接口，提升运营平台对接能力，实现生态服务商（如数据服务商、算法方、应用方）灵活接入，支撑业务持续扩展。

3.企业可信数据空间应用发展现状

（1）发展现状

企业可信数据空间主要由企业（尤其是国有企业、龙头企业）主导建立，旨在联结自身及其上下游合作伙伴，构建可信数据流通利用基础设施。企业可信数据空间以高质量的

企业数据为基础，通过构建多方信任的数据共享环境，促进产业链与供应链的数字化协同，以解决数据协同策略难统一、数据使用难监控、事件发生难溯源等痛点问题。

目前，我国已有多家骨干企业投入企业可信数据空间试点建设，部分已商用，形成了以制造业、能源、金融、电子信息等行业为重点的企业级可信数据空间实践。各地亦在推进更多企业可信数据空间建设，如江苏首批9个企业类项目已入库启动，包括钢铁、新材料等领域。其应用场景主要集中在三大高频领域：一是供应链协同，例如长虹“虹雁”可信数据空间通过实现供应链数据可信采集与实时共享，将物料出入库信息同步时间从隔日压缩至秒级；二是研发协同，例如长安汽车通过数据共享加速了产品迭代；三是核心生产资料保护与共享，例如金太阳通过可信数据空间对设计图纸进行全生命周期的严格管控；华为则通过建立内部数据交换空间，支持各部门之间的敏感数据安全共享。这些实践表明，企业可信数据空间已在打通跨部门跨企业协同、提高供应链效率方面初见成效，显著提高了协同效率和数据价值。一方面，供应链各方可以实时共享关键数据，实现流程透明和协同决策；另一方面，企业通过可信数据空间实现合规数据流通和资产化，推动了业务创新。然而，目前尚未形成跨企业通用标准，这在一定程度上限制了其更大范围的互联互通。

（2）建设模式

在建设模式上，存在自主建设或联合打造两种模式。目前，以企业自主建设为主，部分项目则采用“龙头企业+科技公司”的联合开发模式，如中日友好医院作为医疗行业龙头，联合科技企业北电数智，共同开发并应用了智慧医院解决方案，提升了医疗服务效率和质量。

在技术实现层面，建设过程中均需采用分层与模块化相结合的服务化架构（涵盖数据接入层、控制层、服务层、应用层）并依赖统一身份认证、访问控制、全链路审计机制保障数据可控可追溯。同时，通过部署数据连接器与统一高速数据管道实现跨企业高效互联，并运用隐私计算、区块链等关键技术确保敏感数据的安全流通。

（3）运营模式

在运营模式方面，存在“企业主导、第三方平台支撑”或“自建空间、开放接入”等多种情况，并可成立由政府、企业等多方共治的联盟或委员会。通常，核心企业/运营机构负责建设和运营，数据提供方（核心企业或供应商）向空间注入数据，数据使用方（上下游合作伙伴）进行数据消费和分析，数据服务方提供隐私计算、交易服务等技术支持。这些主体通过联盟或协议形成分工：运营方制定规则、平台架构，提供方贡献数据，使用方在授权框架下获取价值，监管方监督合规与安全。在规则机制上，由核心企业或运营机构主导制定数据空间的各项规则，包括主体接入标准、数据接入标准、

数据使用协议、安全管理规范、收益分配等制度，保障各参与方公平权益。如长虹“虹雁”可信数据空间由长虹作为数据提供方，数鑫科技等为技术服务方，行业监管部门参与规则制定，深交所负责运营。

4.跨境数据空间应用发展现状

（1）发展现状

跨境可信数据空间是指在跨国或跨地区范围内，为促进安全、合规的数据流动而建立的协作网络。它通过统一规则和技术手段，实现不同法律区域间的数据互联互通。目标是降低跨境数据交换的合规成本和安全风险，促进跨国科研、贸易和服务创新。

目前，国内外各类探索尚以试点为主，实践案例尚处于探索阶段。如粤港澳大湾区已探索建立跨境数据传输与认证机制，在一定程度上实现了学历证书、税务等数据的跨境实时核验；深圳数据交易所通过可信数据连接平台，实现跨境传输供应链数据的加密传输和动态密钥管理，确保合规性；中国电信与国际数据空间组织（IDSA）合作，开发跨境流通解决方案，期望形成多方协作的全球数据生态；中国服务贸易协会牵头探索建立全球可信贸易服务平台，基于时空区块链等关键技术，集成货物流、资金流、合同流、信息流等贸易全流程数据要素，为国内外贸易参与方提供身份验证、信用评估、产品溯源、质量认证、贸易数据分析等各类贸易服

务。典型场景涵盖跨境贸易流通、金融服务、联合科研和公共服务。如跨境电商和供应链场景下共享关务、物流、信用数据以提高通关效率；跨境科研场景共享疫情、气候变化等全球数据加速研究进展；跨境金融场景实现银行间客户信用数据互认。总体来看，目前多为概念验证和初步示范，缺乏统一标准，核心挑战仍然是法律冲突的协调，规模化应用有待国际规则和技术逐步完善。

（2）建设模式

建设模式上，由政府、自贸区内跨国企业、国资企业、自贸区管委会等主导，参与方包括跨国企业、跨境服务商、金融机构、科研机构等，它们分别扮演数据提供方和使用方角色；技术和合规服务商提供跨境网络和合规控制。跨境可信数据空间的建设，需要依赖技术衔接、协议交互、规则互认、制度协同、审计监测等。目前，跨境可信数据空间建设实践方面，粤港澳大湾区通过在香港、澳门和内地分别布局信任锚节点，保障数据在不同法律体系间的互信流通。

在关键技术支撑方面，网络层面通过高速专线和境外节点构建安全高效的跨境通信通道；安全层面则依托端到端加密、动态监测与可信执行等手段，确保数据传输的完整性和机密性；合规层面则引入跨境身份认证与自动合规审查机制，使得不同国家法规能够在系统中自动执行，避免人为干预的风险。

（3）运营模式

运营模式上，由相关政府或自贸区充当运营者，发布数据跨境白名单和流通协议；跨境数据提供方（银行、物流、科研机构等）与数据使用方通过标准合同和授权机制达成数据共享；技术服务方和国际组织负责搭建互联互通设施（如跨境连接器）并协助开展跨国认证。技术服务提供方和国际组织则承担互联互通基础设施的搭建任务，例如开发跨境连接器、建立审计平台，并协助推动跨国认证机制的实施。此外，规则机制是支撑运营模式顺利运转的重要保障，需要在多方法律、文化和利益之间寻求协调与共识，最终构建出一个多边共识下的治理框架。该框架不仅保障数据流动的合规性，也促进多国监管间的信息互通与信任建立。

（三）我国可信数据空间发展建议及趋势

1.我国可信数据空间建设需要标准化支撑

当前，我国在地方、行业、企业及跨境层面均开展了可信数据空间建设探索，形成了各具特色的技术架构、治理模式与应用场景。整体来看，四类可信数据空间在应用边界、建设路径与技术策略上虽各具差异，但均围绕“可信、安全、合规、高效”这一核心目标展开建设。地方空间侧重城市治理和公共服务落地，行业空间强调产业链一体化协同，企业空间聚焦内部及供应链数据高效利用，跨境空间则面向制度互认与全球协作挑战。然而，从典型实践来看，仍面临标准不

统一、机制不健全等共性问题，难以支撑大规模协同与可持续运行，标准化已成为亟需突破的核心环节。因此，系统化推进各类可信数据空间之间的协同机制建设，推动统一技术标准、运营机制、安全能力的融合，已成为下一阶段可信数据空间发展的关键方向。

在技术架构方面，各类空间广泛采用分层解耦的模块化架构，集成连接器、隐私计算、区块链等关键技术，以实现数据可信流通。但不同场景下技术实现路径差异显著，缺乏统一规范，接口兼容性和互操作性较弱，制约了系统集成和空间互联。

在运营机制方面，企业、行业和地方多采取“主导方+多方参与”的共建共治模式，但运营职责边界不清晰，平台能力差异大，业务实施流程不清晰，运营体系亟需标准引导与制度支撑。

在安全保障方面，多数空间已部署统一身份认证、访问控制、审计追踪等能力，但在数据基础设施安全、数据流通利用安全等方面仍缺乏通用安全能力要求。

在评估评价方面，多数可信数据空间尚未建立系统绩效评估体系，缺乏针对数据质量、流通效率、安全合规、应用价值等维度的标准化评价方法，影响运行优化与政策支持。

实践表明，可信数据空间建设过程中各类关键环节均已暴露出对架构标准化、技术规范化、运营制度化、安全框架

化、评估指标化的强烈需求，这些实践痛点构成了我国可信数据空间标准体系建设的直接来源和现实基础，也为后续标准化工作的开展明确了方向。

2.我国可信数据空间发展趋势及建议

为加快构建统一规范、安全高效、开放协同的可信数据空间体系，全面释放数据要素价值，推动数字经济高质量发展，建议从以下五方面系统推进：

一是完善制度标准体系，夯实发展根基。制定全国统一的可信数据空间架构标准，明确技术规范、接口协议与数据使用边界，指导不同地方、行业、企业、跨境有序推进可信数据空间建设。同步推动运营、业务流程、安全等方面标准体系建设，鼓励多元主体参与共建共享，探索可持续的市场化运营模式。跨境方面，推动数据流动规则动态协调，参与多边机制，推动我国标准与国际接轨。

二是加强关键技术攻关，筑牢可信支撑底座。聚焦数字合约、可信管控、隐私计算、区块链等核心技术，加快科研突破和工程化落地，提升跨主体协同的可信性和效率。支持建设多层级数据空间底座平台与监管平台，强化算力调度、安全服务、身份认证与使用控制等关键支撑能力。推动标准化技术组件研发，降低不同空间的集成和复用门槛。鼓励国际技术互认合作，为我国标准“走出去”打通路径。

三是推动数据产品化与市场化，释放数据要素潜能。支持多参与主体将数据资源转化为标准化、可交易的数据产品。跨境方面，鼓励设立合规服务平台，降低企业跨境流通门槛，提升数据要素的国际配置效率。

四是构建协同开放的生态体系，提升系统集成效能。支持企业和地方开展跨主体、跨行业、跨区域、跨境的数据共享试点，推动可信空间之间的数据互联互通。推动地方整合数据平台资源，升级本地基础设施，在城市群或区域经济体范围内建立统一互通机制，探索“标准化+平台化+生态化”的区域协同路径。

五是深化示范应用与国际合作，增强全球影响力。积极对接 IDSA、Catena-X、Gaia-X 等国际标准框架，推动我国企业参与 ISO、IEC 等国际标准组织规则制定，构建“一带一路”背景下的数据合作示范工程,提升我国可信数据空间的全球参与度与话语权。

综上所述，我国可信数据空间的发展已开展试点探索并逐步走向体系化建设。应从顶层制度、关键技术、市场机制、生态协同与国际联动五个层面统筹推进，以标准化为抓手，构建覆盖地方、行业、企业、跨境多类型的可信数据空间体系，为我国数据基础设施建设提供坚实支撑。

四、可信数据空间标准化现状

（一）可信数据空间国际标准化现状

1.国际标准现状

目前，全球多个组织正在开展数据空间相关的标准化工作，具有代表性的如 ISO/IEC JTC 1/SC 32“数据管理与交换”、ISO/IEC JTC 1/SC 38“云计算和分布式平台”、ISO/IEC JTC 1/SC 41“物联网和数字孪生”等国际标准组织，CEN/CENELEC JTC 25“数据管理、数据空间、云和边缘”等欧洲标准组织，IDSA“国际数据空间协会”、IEEE-SA“IEEE 标准协会”、Catena-X“汽车产业协作式开放数据生态系统”等国际产业组织，以及 EDWG“Eclipse 数据空间工作组”等开源组织。

a、ISO/IEC JTC 1/SC 32 于 2020 年前后开展数据利用相关的国际标准研制，并成立了 WG 6 数据利用标准工作组，对数据使用、数据交换与数据共享等三个方面开展国际标准化。2024 年，在 WG 6 工作组的推进下，SC 32 研制并发布了 ISO/IEC 5207:2024《信息技术 数据利用 术语与用例》和 ISO/IEC 5212:2024《信息技术 数据利用 数据利用指南》。其中，ISO/IEC 5207:2024 统一了数据利用的术语，给出“数据使用、数据交换、数据共享”相关的基础词汇与定义；ISO/IEC 5212:2024 明确数据利用框架，以数据生命周期为主线，指导组织识别数据流程（内部或跨组织）与数据环境（法律、技术、市场等外部条件）。两项标准共同构成了“横向、跨域”的基础框架，适用于任何类型与规模的组织，旨在降低

数据利用合规风险、提升数据价值并促进标准化实践。当前，ISO/IEC JTC 1/SC 32/WG 6 的召集人由 IEC 副主席 Ian Oppermann 博士担任，秘书由中国专家担任。正在开展的国际标准研制包括“可信数据利用（使用、交换、共享）”、“数据利用评估”等。

b、ISO/IEC JTC 1/SC 38 早在 2014 年开始研究云计算和分布式系统相关的数据标准化，提出并开发了“云计算互操作性和可移植性”和“云服务与设备数据流、数据分类和数据使用”国际标准，对云计算相关的数据互操作和数据利用进行了规范。在此基础上，2018 年 SC 38 启动了数据共享相关的国际标准“云服务数据处理”和“数据共享协议框架”，为便利数据交换共享提供了标准基础。2022 年 SC 38 在研制“组织自主权和数字主权”国际标准的同时，讨论数据空间国际标准化需求，并于 2023 年立项了第一个数据空间国际标准 ISO/IEC 20151 Information technology - Cloud computing and distributed platforms - Dataspace concepts and characteristics《信息技术—云计算和分布式平台—数据空间概念和特征》统一规范数据空间基础概念与核心特征。目前，ISO/IEC 20151 的制定已进入送审阶段。在数据空间概念和特征国际标准的基础上，SC38 成员同意启动 ISO/IEC PWI 25850 数据空间用例研究，为探索和明确数据空间标准化需求提供基础。

c、ISO/IEC JTC 1/SC 41 基于 SC 38 开展的数据空间国际标准化，在 2025 年立项了一项数据空间国际标准 ISO/IEC 30152 IoT and digital twins – Guidance on the connection to data spaces《物联网和数字孪生-数据空间关联指南》。该标准将为数据空间中关联、集成数字孪生和物联网提供标准化技术指导。

d、欧洲标准化组织 CEN/CENELEC 于 2024 年成立了 JTC 25，旨在为欧洲数字主权建设和数据法案实施提供技术标准支撑。结合数据空间开源技术规范和 ISO/IEC 数据空间国际标准，JTC 25 启动了一系列基于数据空间的可信数据交易、数据目录、成熟度等标准项目，为通用欧洲数据空间建设提供统一的欧洲标准。

e、IDSA 发布了一系列数据空间技术规范，包括数据空间参考架构、设计原则、互操作性等，详见下表。

表 4 IDSA 标准清单

序号	标准英文名称	标准中文名称
1	IDS Reference Architecture Model	国际数据空间参考架构模型
2	IDSA Rulebook	IDSA 规则手册
3	Data Connector Report	数据连接器报告
4	Design Principles for Data Spaces	数据空间设计原则
5	Interoperability Framework in Energy Data Spaces	能源数据空间互操作性框架
6	Semantic Interoperability in Data Spaces	数据空间语义互操作性

7	Usage Control in the International Data Spaces	国际数据空间使用控制
8	Framework for the IDS Certification Scheme	国际数据空间认证计划框架

f、IEEE-SA 于 2024 年发布了 IEEE 3158 Trusted Data Matrix System Architecture《可信数据矩阵系统架构》，并正在制定 IEEE P3158.1 Testing and Performance of a Trusted Data Matrix System《可信数据矩阵系统的测试和性能》。此外，IEEE-SA 数字金融标委会正在制定 IEEE P3800 Standard for a Data Trading System 数据交易系统系列标准，采用了可信数据空间参考架构作为数据交易的基础。

g、Catena-X 的标准定义了如何在汽车生态系统内进行可互操作、可扩展的数据和信息交换。通过统一数据、接口和流程，形成一个可互操作的系统，使数据空间的所有参与者都可以轻松进行协作。Catena-X 标准主要包括数据格式、应用程序接口和界面、流程、安全标准，如 CX-0003 SAMM Aspect Meta Model《语义方面元模型》、CX-0012 Business Partner Data Pool API《业务伙伴数据池应用程序编程接口》、CX-0015 IAM & Access Control Paradigm for Users and Clients《用户和客户端的身份和访问管理和访问控制范例》、CX-0018 Dataspace Connectivity《数据空间连接》等。

h、为推动数据空间生态建设，Eclipse Foundation 于 2023 年成立数据空间工作组，为个人和组织提供基于开放标准的开源软件、规范和开放协作模型，支持可伸缩、模块化、可

扩展、面向产业的开源组件创建，用于构建、实现和推广数据空间。目前已开展数据空间组件、消息协议、身份信任协议、分布式声明协议等技术规范制定和开源实现。

2.国外可信数据空间可借鉴的标准化经验

在国际上，可信数据空间的核心理念是基于统一的基础设施架构，建设去中心化的共享交换模式，以低成本和低门槛向所有人开放，大幅提升了中小企业的广泛参与；并能够确保数据的隐私保护、安全可信，可信数据空间的平等互信、互操作性；基于多种便捷灵活的数据控制工具，以及泛连接的数据可信连接器，确保了可信数据空间的落地，成为广泛接收的产业标准。我国应在可信数据空间应在安全保障标准统一的前提下，在可信数据空间整体建设、互联互通、运营模式等方面加快标准研制进度。

（二）我国可信数据空间标准化现状

1.组织机制现状

2024 年，全国数标委（SAC/TC609）成立，从事数据领域国家标准化工作，筹建单位和业务指导单位为国家数据局，全国数标委的工作范围涵盖数据资源、数据技术、数据流通、智慧城市、数字化转型等基础通用标准，支撑数据流通利用的数据基础设施标准，以及保障数据流通利用的安全标准制修订工作。可信数据空间建设由国家数据局指导，标准化工作由全国数标委归口管理。同时，工业和信息化部等

行业主管部门也开展了行业数据空间的标准研制，部分行业标委会、地方团体等围绕特定领域，也开展了数据空间标准研究。

2.数据基础设施标准现状

2024年国家发展改革委、国家数据局、中央网信办、工业和信息化部、财政部、国家标准委联合印发《国家数据标准体系建设指南》加快构建数据标准体系，全面指导数据标准化工作开展，为制修订数据领域相关标准提供了重要指引。

为贯彻落实党的二十届三中全会关于“建设和运营国家数据基础设施，促进数据共享”的部署要求，紧密结合《国家数据基础设施建设指引》相关规划和发展目标，全国数标委秘书处已发布《数据基础设施 参考架构》等9项技术文件，并同步研制国家标准草案，针对数据基础设施参考架构、互联互通、用户身份管理、标识管理、接入连接器、数据目录描述、功能节点、接入管理、安全能力等提出标准化要求，引导地方、行业、企业按照“统一目录标识、统一身份登记、统一接口要求”推进国家数据基础设施建设。同时，全国数标委秘书处组织开展全国一体化算力网标准研究，推进公共传输通道网络传输服务能力、监测调度平台等方向标准研制，推动算力并网、算力资源管理与调度、算力多量纲计费、算力算效衡量、算力运营服务、算力监测接口、算力中心能力、

算力池化、算力安全等 9 个方向形成技术文件。通过构建数据基础设施标准体系，为构建横向联通、纵向贯通、协调有力的国家数据基础设施提供基础支撑。

3.可信数据空间标准制修订现状

国家标准方面，我国现行相关国家标准 2 项，技术文件 4 项；团体标准方面，共 4 项团体标准，发布时间都在近 2 年，统计情况见表 5。

表 5 我国可信数据空间标准统计

序号	标准名称	标准号	类型	发布时间	归口
1	可信数据空间 技术架构	TC609-6-2025-01	技术文件	2025	全国数据标准化技术委员会
2	可信数据空间 数字合约技术要求	TC609-6-2025-14	技术文件	2025	全国数据标准化技术委员会
3	可信数据空间 使用控制技术要求	TC609-6-2025-15	技术文件	2025	全国数据标准化技术委员会
4	可信数据空间 技术能力评价规范	TC609-6-2025-16	技术文件	2025	全国数据标准化技术委员会
5	智能制造 工业数据空间参考模型（修订中）	GB/T 42029-2022	国家标准	2022	工业和信息化部
6	自动化系统与集成 离散制造企业数据空间集成模型	GB/T 44063-2024	国家标准	2024	全国自动化系统与集成标准化技术委员会
7	可信数据空间一体机	T/SZBD 3-2025	团体标准	2025	深圳市大数据研究与应用协会
8	场景驱动的产品生态数据空间管理要求	T/AIITRE 21009-2024	团体标准	2024	中关村信息技术和实体经济融合发展联盟
9	场景驱动的跨企业产品生态数据空间 数据设计规范	T/AIITRE 21008-2024	团体标准	2024	中关村信息技术和实体经济融合发展联盟
10	制造业多价值链协同	T/CSTE 0435-2	团体	2023	中国技术经济

	数据空间概念模型	023	标准		学会

2025 年 4 月 30 日，国家标准层面首份可信数据空间技术文件《可信数据空间 技术架构》（TC609-6-2025-01），由全国数标委发布，旨在建立统一的可信数据空间技术架构，描述可信数据空间作为一种数据流通利用基础设施的核心技术特征、最小功能集合以及关键业务流程，为数据基础设施试点及地方、行业、企业数据空间的规划、建设、运营和管理提供参考依据。

2022 年，我国发布工业可信数据空间的国家标准 GB/T 42029-2022《智能制造 工业可信数据空间参考模型》，给出了工业可信数据空间参考模型框架和角色，描述了数据、应用、服务、软件和安全等功能构件，涵盖数据提供者、数据使用者、数据中介、数据服务商和认证机构等 5 种角色，适用于工业可信数据空间建设和应用，此标准正按照《可信数据空间 技术架构》开展修订工作。

团体标准方面，《制造业多价值链协同数据空间概念模型》（T/CSTE 0435-2023）聚焦电力装备制造、飞机制造、汽车制造、家用电器等离散型制造领域；中信联 2024 年发布的 2 项可信数据空间团标侧重于大规模定制化场景，规范了数据要求和管理要求；今年深圳市大数据研究与应用协会发布的《可信数据空间一体机》团体标准给出了可信数据空间一体机的硬件及主要参数、架构、功能，规定了可信数据

空间一体机的技术要求、试验方法、检验规则、标志、包装、运输和贮存，是地方响应国家可信数据空间政策的积极尝试。

3.我国可信数据空间标准化存在的问题

我国可信数据空间标准化组织建设相对完善，也具备了顶层政策指导，但处于初期起步，积极探索阶段。一是国家标准未成体系，目前尚无总体性国家标准，重点标准亟待研制。二是标准供应不足，可以看出近5年，可信数据空间行业、地方标准数量为零，反映出各行业、各地区存在“想建不会建”的困境。三是团体标准管理不规范，国家可信数据空间指导政策发布以来，很多机构开始了可信数据空间标准的研究，团体标准以速度快、效率高的特点，可以在新兴领域弥补部分国家标准缺失的空白，但真正备案可查的团体标准却寥寥无几，此类“标准”缺少征求意见、专家审查等环节，内容合理性、一致性存疑，对业内建设者造成困扰。

五、可信数据空间标准体系建设

（一）可信数据空间标准需求

我国的可信数据空间发展主要参考了国际上的应用模式，汇聚了数字合约与使用控制技术，构建了安全可靠的网络空间、可拓展的技术架构、全流程数据监测及系统互操作的基础环境，为多方主体提供了“可信赖”的数据流通及使用的基础设施。由于涉及的角色、技术种类众多且繁杂，在实

践中仍存在诸多问题，亟需统一的标准和规范。

一是架构标准化需求。可信数据空间是整体数据流通利用基础设施的业务节点，架构标准需要满足与其他类型的业务节点、区域/行业功能节点的连接要求，并且要覆盖城市、行业、企业等不同类型空间的建设要求。然而，由于技术路线、业务需求、成本考虑等多种因素影响，不同的可信数据空间在架构的设计上存在差异，将导致系统之间的兼容性差，难以实现数据资源共享共用。

二是技术选型与适配需求。可信数据空间平台应具备认证、使用控制、后台管理、统计清算等多种功能。但这些功能的具体实现和技术使用上却存在较大的差异，不同的可信数据空间平台、不同应用场景下采用不同的算法、模型或工具来处理数据，导致在处理结果可能存在较大的差异。提供可参考的技术选型与适配指引，将弥补传统技术路线短板将更有利于可信数据空间推广和服务体验。

三是空间集成与互操作需求。可信数据空间之间、物理空间与逻辑空间之间、各参与主体之间的数据资源共享共用依赖于统一的接口协议规范。由于连接器接口、数据格式、编码、命名等规范不一致，导致空间集成与互操作过程中需要进行复杂的转换和适配工作。这不仅增加了技术难度和成本，还可能引入错误和不一致性，影响可信数据空间的服务质量和可靠性，并增加了系统的复杂性和维护成本。

四是高效运营需求。可信数据空间建设应当满足不断变化的各方主体诉求和发展要求。运营主体需要借鉴主体识别、合约规则库建立、控制技术选型、生态体系建设、安全合规管理、场景适配的标准规范、参考架构和最佳实践，明确可信数据空间的管理目标和应用场景，结合典型应用提炼共性标准化需求，以确保数据的有效利用和价值最大化。

五是可信安全的运行需求。可信数据空间平台通过数字合约、使用控制和隐私保护计算等建立了跨主体、跨行业、跨区域的技术信任机制。这不仅增强了数据提供方敢于供数的信心，而且保障了数据使用方与服务方能够严格按照约定地用法用量去使用数据。为保障平台的安全稳定运行，必须制定涵盖安全要求、测试评价及安全保障技术的标准规范。进一步，在数据流通利用合作前，应先评价合作机构的信任度。对于信任度较低的机构间合作，应采取更严格的安全防控措施。此外，有必要制定可信管控能力、安全分级标准，以便根据数据流通场景和参与方信任度灵活选择合作模式，确保数据流通的安全性与高效性。

六是生态协同需求。可信数据空间需要构建开放互信的数据流通生态以促进多方协作。通过共识算法实现联盟链节点间数据一致性，并以收益分成等激励机制调动参与方积极性；统一数据格式、接口协议等技术标准，打通跨链数据流转通道以实现不同平台互认；清晰界定数据提供方、使用方、

监管方等角色的权责边界，引入第三方审计、认证中心等信任支撑角色，确保生态各环节有序运转，形成多方参与、标准统一、权责明确的协同发展格局。

七是国际协同需求。我国可信数据空间要与 IDSA、Gaia-X 等国际框架对齐和标准需求对齐，做到国内与国际协同建设及发展，满足跨境数据流通、数据共享与协作、信任机制构建、安全管理合作及关键技术联合研发，避免因标准差异导致的数据流通障碍和安全风险。

（二）可信数据空间标准体系结构

根据《国家数据标准体系建设指南》中数据标准体系的规划，数据基础设施标准以现有相关标准为主，强化基础设施互联互通、算力保障和流通利用标准建设，为数据资源、数据技术、数据流通、融合应用提供支撑。

基于可信数据空间建设现状，以及已有标准化基础，根据我国可信数据空间未来发展趋势，以《国家数据标准体系建设指南》《数据基础设施 参考架构》为指导，形成可信数据空间标准体系框架,属于国家数据标准体系中“数据基础设施－流通利用设施”标准，如图 4 所示。

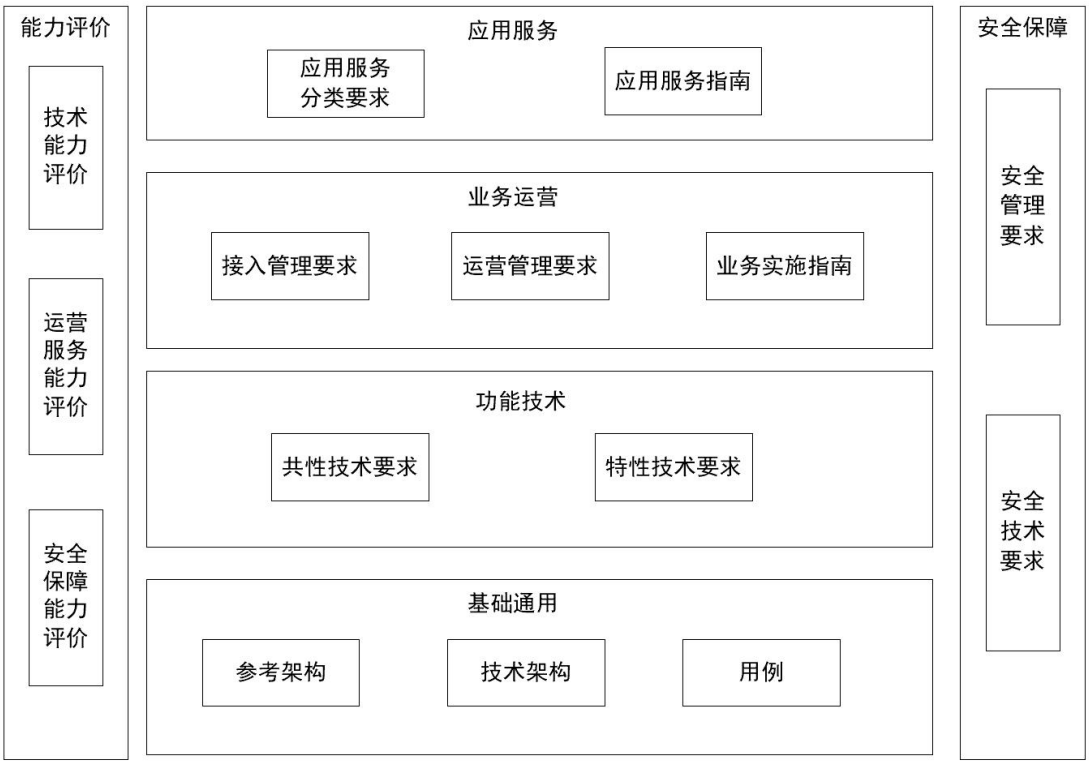

图 4 可信数据空间标准体系结构图

可信数据空间标准体系由 6 类标准组成，分别为基础通用标准、功能技术标准、业务运营标准、安全保障标准、能力评价标准和应用服务标准。

（1）基础通用标准

基础通用标准包括参考架构、技术架构及用例等，为后续拟制定标准研究奠定坚实基础。其中，参考架构规定数据基础设施整体的用户角色和架构功能；技术架构规定可信数据空间的功能特征、业务流程等；用例则涵盖了可信数据空间具体实践。

（2）功能技术标准

功能技术标准应促进数据资源交互、接口协议和互操作

规则，增强可信数据空间、接入连接器以及与其他数据流通利用业务节点之间的互操作性与兼容性，降低数据流通和应用的成本与风险。

（3）业务运营标准

主要针对可信数据空间平台的接入管理、运营管理、业务实施等运营环节的规则、要求等进行规范。

（4）安全保障标准

安全保障标准应遵从数据基础设施整体安全标准要求，从安全管理、安全技术等方面为标准体系建设提供安全保障。

（5）能力评价标准

可信数据空间能力评价定义了评价模型、评价指标、评价过程等内容，包括技术能力评价、运营服务能力评价、安全保障能力评价等方面。

（6）应用服务标准

应用服务标准用于将可信数据空间的应用服务模式分类，提供可信数据空间落地应用实践指南，支撑可信数据空间应用服务实践，促进可信数据空间的建设。

（三）可信数据空间标准体系框架

可信数据空间是国家数据基础设施的一部分，符合国家数据基础设施整体架构及基本约束，在继承国家数据基础设施业务节点及接入连接器基本要求的基础上，可信数据空间

结合自身技术特征进行了一定的功能扩展。同理，可信数据空间的标准体系在复用遵照数据基础设施参考架构整体标准体系的基础上，构建可信数据空间特有标准体系。

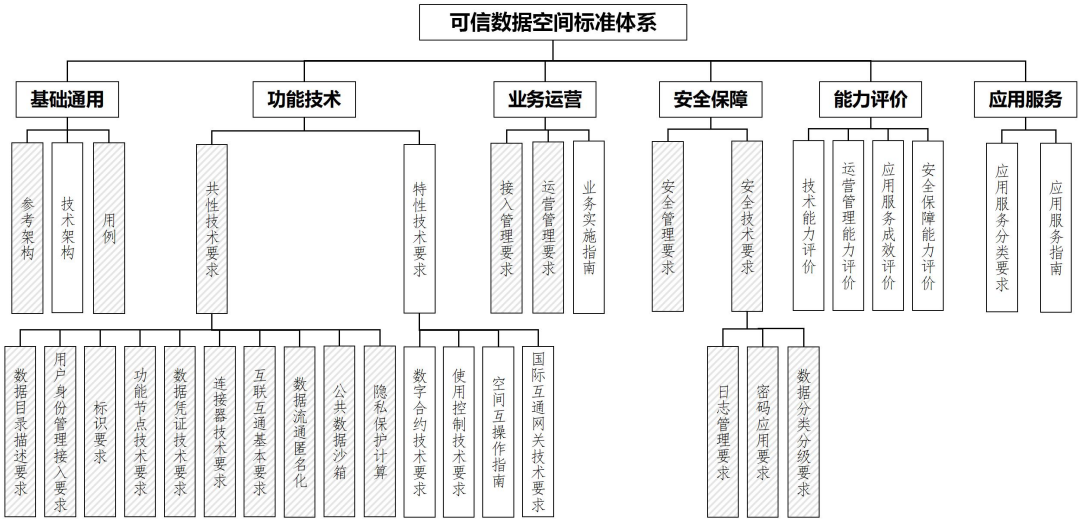

图 5 可信数据空间标准体系结构图

（四）可信数据空间标准建设路径

1.基础通用标准

基础通用标准包括参考架构、技术架构及用例等，为后续拟制定标准研究奠定坚实基础。可信数据空间的整体架构需符合数据基础设施参考架构。技术架构标准主要用于规范可信数据空间各功能模块和节点之间的逻辑关系和相互作用；可信数据空间作为数据基础设施的技术路线之一，其具体实践可体现在数据基础设施用例标准中。

2.功能技术标准

功能技术标准主要针对可信数据空间的功能和技术进

行规范，可信数据空间基于最前沿的数据技术建设，需要遵循三统一要求，具备互联互通互操作功能及数字合约、使用控制等技术能力。其中，共性技术要求为整体数据基础设施建设需遵循的整体要求，包括用户身份、数字目录、标识方面的三统一要求及互联互通、功能节点、数据凭证、数据流通匿名化、公共数据沙箱、隐私保护计算等方面的技术要求；特性技术要求标准规范可信数据空间核心关键技术要求，主要包括数字合约、使用控制、空间互操作、国际网关互通等标准。

3.业务运营标准

主要针对可信数据空间平台的接入管理、运营管理、业务实施等方面进行规范。其中，接入管理对应的标准包括接入主体、数据资源、数据产品及服务、技术工具的审核要求、审核操作流程、准入管理等规范；运营管理是对于可信数据空间日常运营管理的标准规范；业务实施指南对于用户角色、业务流程和业务管理要求等方面提出标准支撑。

4.安全保障标准

遵循整体数据基础设施的相关安全标准，主要包括安全管理要求和安全技术要求，聚焦可信数据空间的架构安全、运行安全和数据交互等方面安全，对于日志管理、密码应用等方面提出标准规范。

5.能力评价标准

主要用于规范可信数据空间技术能力、运营服务、安全保障等方面的能力评价，为可信数据空间的发展提供评价支撑。

6.应用服务标准

主要包括可信数据空间应用服务分类和指南，用于对各类型可信数据空间应用中的服务过程和方法提供指导，包括应用服务分类、指南等标准，促进可信数据空间与实体经济的深度融合。

（五）可信数据空间标准建设明细

序号	一级分类	二级分类	标准名称	标准范围	拟解决问题	备注
1	基础通用	参考架构	数据基础设施 参考架构	本标准主要针对数据基础设施参考架构，包括参与角色、活动、功能组件和它们之间的关系。	本标准拟提供一个体系架构，对于讨论数据基础设施需求、结构和操作是一种有效的工具，解决数据基础设施架构不明确的问题，可为数据基础设施系列标准的制定提供基础。	复用数据基础设施标准
2		技术架构	可信数据空间 技术架构	本标准规范了可信数据空间技术架构，适用于指导地方、行业、企业开展可信数据空间的规划、建设、运营和管理。	本标准拟解决技术架构不统一与互操作性不足的问题。	
3		用例	数据基础设施 用例	本标准适用于可信数据空间、数场、数据元件、数联网、区块链网络、隐私保护计算平台等数据基础设施的建设。	本标准旨在解决各技术路线建设思路不明的问题。	复用数据基础设施标准
4	功能技术	共性技术要求	数据基础设施 用户身份管理和接入要求	本标准规范了统一用户身份的构成要求、身份注册及验证、跨平台身份互联互通机制以及相关接口与安全管理要求，旨在保障接入主体、接入连接器及平台的身	本标准拟解决不同地区、不同组织用户身份标准不统一，跨地域、跨组织身份互认困难、身份重复认证等问题。	复用数据基础设施标准

				份可信，以实现用户身份的跨节点互联互通。		
5			数据基础设施 标识要求	本标准规定需要标识的特定物理或逻辑对象的表述要求，包括数据产品、数据资源、基础支撑平台、接入连接器、数据流通利用平台等。	本标准主要解决标识编码统一分配、管理问题，通过标识码统一规范，构建高效标识解析体系，促进各平台系统间数据可信流通。	复用数据基础设施标准
6			数据基础设施 数据目录描述要求	本标准规定了数据基础设施中数据目录的描述要求，包括数据目录的总体框架、技术要求、核心元数据、分类规则以及管理流程等内容。	本标准拟解决数据流通利用基础设施体系中数据产品及数据资源描述标准不流通不畅、统一管理困难等问题。	复用数据基础设施标准
7			数据基础设施 数据凭证技术要求	本标准规范数据基础设施中数据资产凭证、交易凭证结构、生成与验证机制，适用于数据基础设施中的凭证应用和管理。	本标准拟解决数据基础设施建设中凭证缺乏统一结构、生成与验证机制，难以交互的问题。	复用数据基础设施标准
8			数据基础设施 全域功能节点技术要求	本标准规范了全域功能节点在目录管理、标识管理、身份管理、运营管理、监测分析等方面的技术要求，适用于指导全域功能节	本标准拟解决全域功能节点建设中功能不清晰、一致性低、缺少技术规范等问题。	复用数据基础设施标准

				点的建设。		
9			数据基础设施 区域/行业功能节点技术要求	本标准规范了区域、行业功能节点在目录管理、标识管理、身份管理、运营管理、监测分析等方面的技术要求，适用于指导具备条件的省份按照标准化架构建设区域功能节点。	本标准拟解决区域、行业功能节点建设中功能不清晰、一致性低、缺少技术规范等问题。	复用数据基础设施标准
10			数据基础设施 互联互通基本要求	本标准规定了数据基础设施互联互通技术要求、业务流程、能力要求和接口要求，用于指导全域功能节点、区域功能节点、行业功能节点、业务节点以及接入主体之间开展信息同步、跨域协作等工作。	拟形成统一的互联互通框架和要求，推动各地区数据基础设施之间的规范互联。	复用数据基础设施标准
11			数据匿名化流通实施指南及评估指南	本标准规范了数据流通过程中匿名化处理的技术要求、操作规范，同时，提出了面向数据流通场景的匿名化效果评估方法，包括评估构成要素、评估流程，以及具体的评估方法和步骤，适用于企	本标准拟解决因匿名化标准缺失导致的数据流通合规性模糊、技术有效性不足，以及，因缺乏面向数据流通场景的匿名化判定规则、评估方法，导致数据流通场景中的匿名化效果无法认定的等问题。	复用数据流通匿名化标准

				业、公共机构等在数据流通场景下的匿名化实践和效果评估。		
12			数据基础设施 公共数据沙箱技术要求	本标准规范了公共数据沙箱的产品类型、应用场景、技术特性、安全功能、性能要求、兼容性要求、配套隐私存算系统要求、管理流程、测试方法、评估标准、术语解释。	数据接入、登记、采集、开发、利用、交易、流通、共享、交付、销毁等阶段的数据安全保护、数据隐私保护及数据管理控制。	复用数据基础设施标准
13			数据基础设施 隐私保护技术要求	本标准规范了数据基础设施中数据全生命周期安全和隐私防护，适用于数据基础设施中可信管控和安全保障能力建设，保障数据处理过程“可用不可见”。包括集合求交、隐匿查询、联合建模的功能、数据计算的机密性和正确性要求。	本标准拟解决多方数据协作中隐私保护与数据价值释放的矛盾，保障机密性与结果正确性。	复用数据基础设施标准
14		特性技术要求	可信数据空间 数字合约技术要求	本标准规范了可信数据空间服务平台中数据合约的技术要求，包括：合约描述语言要求、合约签署要求、合约备案要求、合约内	本标准拟解决可信数据空间中数字合约内容不清晰、描述不规范、签署流程不明确的问题。	

				容要求等，适用于可信数据空间服务平台中数字合约能力建设。		
15			可信数据空间 数据使用控制技术要求	本标准规范了可信数据空间服务平台中使用控制技术要求,包括:控制策略解释、控制策略执行、使用过程存证等，适用于可信数据空间服务平台中使用控制能力建设。	本标准拟解决可信数据空间中数据使用控制技术路径不清晰、功能组件不明确、跨域策略难协同的问题。	
16			可信数据空间 互操作指南	本标准主要规定了可信数据空间中不同可信数据空间之间的交互流程规范，包括统一数据模型、交互接口、语义、共享交换机制等，以及在该互操作协议下数据流通利用的安全、可信保障机制。	本标准旨在解决可信数据空间之间不同主体、系统之间的异构数据互操作问题，包括数据模型、交互接口、消息结构的标准化以及安全性、可信性等问题。	
17			可信数据空间 国际互通网关技术要求	本标准规范了可信数据空间与国际上其他数据空间进行数据流通利用时应提供的国际空间互通网关功能，适用于可信数据空间服务平台中国际空间互通网关能力建设。	本标准拟解决可信数据空间进行数据跨境数据流通利用时面临的若干问题。	

18	业务运营	接入管理	数据基础设施 接入管理要求	本标准规范了数据基础设施建设中各类系统、设备接入的要求，明确了业务节点、接入连接器接入区域/行业功能节点过程中的技术、管理、安全以及合规等方面要求。适用于指导各区域/行业功能节点运营主体开展接入管理，确保数据基础设施服务的普惠、高效和安全。	本标准拟解决数据基础设施接入各类系统、设备缺少明确要求的问题。	复用数据基础设施标准
19		运营管理	数据基础设施 运营管理要求	本标准规范了数据基础设施的管理、运营、服务等方面的基本要求，包括主体、技术、流程、跨域操作等，适用于各相关数据基础设施的全过程规划设计及运营管理。	本标准拟解决数据基础设施运营角色权责不清、运营模式不明的问题。	复用数据基础设施标准
20		业务实施指南	可信数据空间 业务实施指南	本标准规范了可信数据空间业务实施模式，明确可信数据空间的角色活动、业务流程、多角色协同机制、服务模式等。	本标准拟解决用户角色不清晰、业务架构不统一、业务流程碎片化、业务与技术脱节的问题。	
21	应用	应用服务	可信数据空间 应	本标准规范了可信数据空间的应	本标准拟解决各可信数据空间应用	

	服务	分类	用分类要求	用服务模式分类，适用于指导可信数据空间数据服务和应用的分类。	服务分类模式不一致的问题，明确各类应用服务的差异和边界。	
22		应用服务指南	可信数据空间 应用服务指南	本标准规范了可信数据空间的应用服务模式，适用于指导可信数据空间开展数据服务和应用拓展，助力可信数据空间在地方、行业、企业、跨境场景下的落地实践。	本标准拟解决建设可信数据空间时路径不明、缺乏差异化指导的问题，为各类应用场景提供清晰、具体的建设框架和实施方法。	
23	安全保障	安全管理要求	数据基础设施 安全能力通用要求	本标准规范了数据基础设施建设中的安全防护、管理等技术要求，适用于各相关数据基础设施运行全流程安全保障。	本标准拟解决数据基础设施安全防护不足、机制不完善的问题。	复用数据基础设施标准
24		安全技术要求	数据基础设施 运行日志管理技术要求	本标准规范了数据基础设施中支撑数据的收集、存储、管理、处理和分析等一系列运行活动的相关硬件、软件及网络等设备的日志要求，适用于运行日志管理相关技术在数据基础设施中的应用落地。	本标准拟解决数据基础设施中的日志管理技术实施问题。	复用数据基础设施标准

25			数据基础设施 密码应用技术要求	本标准规范了数据基础设施中密码应用技术要求，适用于密码应用相关技术在数据基础设施中的应用落地。	本标准拟解决数据基础设施中的密码应用技术实施问题。	复用数据基础设施标准
26	能力评价	技术能力	可信数据空间 技术能力评价规范	本标准规范了可信数据空间的技术能力评价体系，适用于组织对可信数据空间技术能力的监督和考核。	本标准拟解决可信数据空间技术能力评价标准不一致的问题。	
27		运营服务	可信数据空间 运营管理能力评价规范	本标准规范了可信数据空间的运营管理能力评价体系，给出运营管理能力评价模型、评价流程、评价内容、分析评价方法等。	本标准拟解决可信数据空间运营管理能力评价标准不一致的问题。	
28			可信数据空间 应用服务成效评价	本标准规范了可信数据空间的应用服务的成效评价模型，适用于组织对可信数据空间应用服务成效的监督和考核。	本标准拟解决可信数据空间应用服务成效评价标准不一致的问题。	
29		安全保障	可信数据空间 安全能力评价规范	本标准规范了可信数据空间的安全保障能力评价体系，给出安全防护能力评价要素、评价流程、评价内容、分析评价方法等。	本标准拟解决可信数据空间安全能力评价标准不一致的问题。	

六、下一步可信数据空间标准化工作考虑

（一）持续推进可信数据空间重点标准研制

持续完善可信数据空间标准编制组织机制，以全国数标委为依托鼓励政、产、学、研、用等多元主体参与标准制定工作。在整体规划下，围绕可信数据空间建设中基础通用、功能技术、业务运营、能力评价、应用服务和安全保障等方向，依据急用先行原则，加快推动国家标准的预研、立项及研制工作。建立国家、行业、区域、团体协同的标准优化体系，结合标准应用效果持续修正已发布标准，积极推动先进性、引领性、实施效果良好的行业标准、地方标准转化为国家标准，提升标准整体水平。建立动态优化迭代机制，同步开展可信数据空间技术能力等方面的试点验证，并根据验证结果，逐步对标准进行优化和调整，使其能够更好地应对实际应用中的各种情况。

（二）扎实做好可信数据空间标准宣贯推广

坚持标准与政策导向、技术创新、市场需求相结合，推动国家标准贯标工作，形成“标准研制－应用反馈－迭代优化”的闭环机制，以标准促应用、以应用验标准。积极开展标准解读与应用推广，系统地阐释标准制定的背景、技术考量和实践逻辑，通过案例解析和实施路径的说明，帮助业界准确理解标准的内涵，分层次，有节奏的推动标准的高效落地

和规模化应用。在重点地方、行业、企业，有计划的落地一批可信数据空间标准化建设试点项目，打造可复制、可推广的标准应用示范案例和最佳实践。开展标准化培训和咨询服务。针对关键地方、行业和企业，组织标准宣传和贯彻的讲座，提供个性化指导，协助企业掌握和执行标准，降低标准实践的试错成本，缩短标准落地的时间。组织区域性、行业性及全国性可信数据空间论坛、大赛、专项评比等活动，扩大标准的影响力，激发产业界实践动力。

（三）打造可信数据空间标准应用服务生态

鼓励各组织基于标准化框架开展联合研发、应用推广和商业模式创新等活动，形成多方参与、优势互补、互利共赢、协同发展的可信数据空间应用服务生态格局。聚焦可信数据空间标准化建设及发展需求，编制体系化培训教材，培育可信数据空间标准化服务应用技术人才，发展标准化服务专业能力认证体系，形成“教材支撑－人才培养－专业认证”标准化服务培育链条。以多元场景为牵引，促进标准与实践落地相结合，开展可信数据空间技术能力、应用服务能力等相关评测。积极培育并发展具备服务型、应用型、技术型及生态整合型能力的数据服务提供商，催生新产业、新业态、新模式、新应用、新治理，加快推动可信数据空间的繁荣和壮大。

（四）推动可信数据空间国际对接互通

积极推动数据领域国际标准化合作，深化与 ISO、IEC、

ITU 等国际标准组织以及 CEN、DIN、IDSA、Catena-X 等国外标准组织的交流与合作，逐步探索在可信数据空间、高质量数据集、数据利用、数据跨境合作等方向推广“中国方案”，尽快输出高质量国际标准成果，与国际标准组织、国外高水平标准组织深化沟通互动，促进标准国际互认；加强在数据标准领域的人才培养和交流，共同提升专家技术实力和标准化水平；建立并完善标准提案储备机制，通过举办国际论坛、开展技术路线图研究等方式，促进国内外标准互认，为全球数据治理体系注入中国动力。