ICS 35.240
CCS L 70

全国数据标准化技术委员会技术文件

TC609—6—2025—01

可信数据空间 技术架构

Trustworthy Data Space——Technology Architecture

（征求意见稿）

2025 年 4 月 18 日

全国数据标准化技术委员会 发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国数据标准化技术委员会（SAC/TC609）提出并归口。

本文件起草单位：中国电子技术标准化研究院、北京大数据先进技术研究院、中国信息通信研究院、北京大学、下一代互联网国家工程中心、中国移动通信集团有限公司、中国联合网络通信集团有限公司、中国电信股份有限公司数据发展中心、华为技术有限公司、浙江大学、上海芯超数据科技有限公司、深圳数鑫科技有限公司、北京大学上海临港国际科技创新中心、北京市大数据中心、电子科技大学、四川省大数据中心、国家电网有限公司大数据中心、四川长虹电器股份有限公司、中电数据产业集团有限公司、中电数创（北京）科技有限公司、蚂蚁科技集团股份有限公司、航天信息股份有限公司、数据空间研究院、国家信息中心、中国南方电网有限责任公司、浪潮云信息技术股份公司、西安电子科技大学、武汉达梦数据技术有限公司、三六零安全科技股份有限公司、杭州安恒信息技术有限公司、华为云计算技术有限公司、上海数据集团有限公司、太极计算机股份有限公司、北京数网链通科技有限公司、北京泰尔英福科技有限公司、杭州金智塔科技有限公司、汇数未来数据运营（杭州）有限公司、吉林省高速公路集团有限公司、蓝象智联（杭州）科技有限公司、星环信息科技（上海）股份有限公司、云上（南昌）大数据有限公司、浙江省大数据联合计算中心、中电云计算技术有限公司、中国移动通信有限公司研究院、中移动信息技术有限公司、联通数据智能有限公司、中国联通软件研究院、中国信通院江西研究院、浙江蚂蚁密算科技有限公司、杭州市大数据管理服务中心、杭州云象网络技术有限公司、天翼支付科技有限公司、中电福富信息科技有限公司、中国电信股份有限公司数据要素技术创新（海南）中心、中电信人工智能科技（北京）有限公司、国网山东省电力公司、江苏中堃数据技术有限公司、国网江苏省电力有限公司、中国交通建设集团有限公司、中国交通信息科技集团有限公司、数据易（北京）信息技术有限公司、上海零数众合信息科技有限公司、安徽中科晶格技术有限公司、广电运通集团股份有限公司、阿里云计算有限公司、深圳数据交易所、煤炭科学研究总院有限公司、新胜科技（上海）有限公司、成都市标准化研究院、哈尔滨工程大学、吉林省吉林祥云信息技术有限公司、普元信息技术股份有限公司、四川数通智汇数据科技有限公司、北京电子数智科技有限责任公司、国家工业信息安全发展研究中心、北京熠智科技有限公司、中移雄安信息通信科技有限公司公司、联通数字科技有限公司、中关村科学城城市大脑股份有限公司、中科斯欧（合肥）科技股份有限公司、福建省大数据集团有限公司、天津市天河数字产业科技有限公司、广西北部湾大数据交易中心有限公司、南方电网能源发展研究院、中国移动通信集团设计院有限公司、北京思特奇信息技术有限公司、中国联通智能城市研究院、北京天融信网络安全技术有限公司、中电科网络安全科技股份有限公司、数据要素社、北京数字认证股份有限公司、杭州数梦工场科技有限公司、中兴通讯股份有限公司、每日互动股份有限公司、杭州趣链科技有限公司、广州广电运通信息科技有限公司、中国信息协会、苏州数据资产运营有限公司、中启联信科技集团有限公司、山东未来集团有限公司、联通（广东）产业互联网有限公司、中国质量认证中心、北京华宇信息技术有限公司、联通数字科技有限公司、湖南天河国云科技有限公司、马上消费金融股份有限公司、中电科大数据研究院有限公司、奇点数联（北京）科技有限公司、中国民用航空西南地区空中交通管理局、重庆市质量和标准化研究院、成都久信信息技术股份有限公司、杭州高新区（滨江）区块链

与数据安全研究院、成都西南民航通信网络有限公司、广州维视达数字科技有限公司、北京数风科技有限公司、云基华海信息技术股份有限公司、金联汇通信息技术有限公司、杭州金智塔科技有限公司、山西远大纵横科技有限公司、长沙都正生物科技股份有限公司、湖南大数据交易所有限公司、深圳市华傲数据技术有限公司、临沂市大数据中心、公安部第三研究所、中国工业互联网研究院、浙江省数字经济发展中心、福建新世通律师事务所、广州金域医学检验集团股份有限公司、三未信安科技股份有限公司、北京金喻泽科技有限公司、豪尔赛科技集团股份有限公司、广州睿帆科技有限公司、北京腾云天下科技有限公司等。

可信数据空间 技术架构

1 范围

本文件规范了可信数据空间技术架构，明确可信数据空间在国家数据基础设施中的定位，可信数据空间的核心技术特征、最小功能集合以及关键业务流程。

本文件适用于地方数据基础设施试点及可信数据空间试点的规划、建设和运营、管理。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

NDI—TR—2025—01 数据基础设施 参考架构

NDI—TR—2025—02 数据基础设施 互联互通基本要求

NDI—TR—2025—03 数据基础设施 用户身份管理和接入规范

NDI—TR—2025—05 数据基础设施 接入连接器技术要求

NDI—TR—2025—06 数据基础设施 数据目录描述规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

可信 trustworthiness

可信，即可信赖，指“符合预期”，以技术可验证方式满足利益相关者期望的能力。可信数据空间中的可信是指数据流通及使用的可信赖，代表数据流通及使用的过程及结果符合相关参与方的行为预期。

[来源：ISO/IEC TS 5723:2022 3.1.1]

3.2

可信数据空间 trustworthy data space

可信数据空间是基于共识规则，联接多方主体，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。

3.3

数字合约 digital contract

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、使用等环节的预期，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。

3.4

使用控制 usage control

是指在数据的传输、存储、使用和销毁环节，通过集成在数据应用、算法和运行环境中的技术手段，确保相关参与方按照数字合约约定的使用策略对数据进行分析、计算和处理等，实现对数据使用的时间、地点、主体、行为和客体等因素的控制，从而保证对数据的使用符合预期。

3.5

数据资源 data resource

是指具有价值创造潜力的数据的总称，通常指以电子化形式记录和保存、可机器读取、可供社会化再利用的数据集合。可信数据空间中，数据资源需在连接器封装为数据产品进而登记、上架流通。

3.6

数据产品 data product

是指基于数据加工形成的，可满足特定需求的数据加工品。可信数据空间中，数据产品是从数据资源加工而来，是数据流通及使用的基本单元。数据产品的形式可以是数据集、文件或者API等。

4 概述

从定义角度，**可信数据空间是基于共识规则，联接多方主体，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。

从技术组成角度，**可信数据空间以数字合约、使用控制技术为核心，以数据跨主体流通使用的可信（符合预期）为目标**。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预期并达成共识；通过集成在特定软硬件环境中的使用控制技术对算法、应用进行控制和审计，实现数据访问、分析、计算等行为的管控，保证数据的流通利用过程符合预期。

从系统构成角度，**可信数据空间系统主要由可信数据空间服务平台和可信数据空间连接器组成**。其中可信数据空间服务平台是可信数据空间运营方运营可信数据空间的支撑平台，为可信数据空间参与方进行数据流通和使用的基础服务；可信数据空间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、使用方、服务提供方通过可信数据空间连接器提供数据、使用数据以及提供第三方增值服务，是实现依据数字合约进行控制的载体。

从生态关系上，可信数据空间是在连接器及服务平台上形成的数据流通要素和关系的集合，包括：提供方、使用方、服务方等参与主体，数据、算法、服务等可用资源，策略、合约、法规等共识规则。一套物理的可信数据空间系统应支持构建多个逻辑可信数据空间。不同的可信数据空间生态通常具有较强的共有业务属性、社会属性或群组关系，导致其中的参与主体、可用资源、共识规则各不相同。例如某领域供应链数据空间，参与方通常为供应链上下游企业；例如某医疗数据空间，参与方通常为医院、药物研发方、医学研究方等。

从应用场景角度，**可信数据空间可用于解决具体场景下数据流通利用中的信任问题，降低供方提供数据，需方使用数据的信任门槛**。例如，跨企业、跨行业的产业数据交换协同，跨领域、跨学科的科学数据共享分析等。在可信数据空间限定的参与主体、可用资源及共识规则下，利用可信数据空间技术能力，相关参与方之间能够达成对数据流通及使用预期的共识，使需方相信供方如约提供数据、供方相信需方如约使用数据，高效实现跨主体的数据可信流通及使用。

在与国家数据基础设施关系方面，**可信数据空间既是国家数据基础设施的架构派生也是国家数据基础设施的组成部分**。一方面，从技术架构角度，可信数据空间技术继承国家数据基础设施参考架构：可信数据空间服务平台在国家数据基础设施架构中的定位是业务节点，可信数据空间连接器的定位是接入连接器；同时，可信数据空间结合自身技术特征扩展了功能组件：可信数据空间服务平台中扩展数字合约、空间管理等部分，接入连接器扩展使用控制、签约履约等部分。另一方面，从互联互通的角度，可信数据空间系统是国家数据基础设施的一部分，需按照统一目录标识、统一身份登记、统一接口要求，接入区域/行业功能节点，实现与其他业务节点的互联互通，实现与其他数据基础设施互信互认及互操

作。可信数据空间用户可通过数据基础设施公共服务发现全域中各可信数据空间服务平台以及可信数据空间中的数据资源、产品，并按照各可信数据空间的业务规则加入、创建可信数据空间，获取可信数据空间服务。

可信数据空间形成的以数字合约、使用控制为核心的技术体系，具备以下典型特征：**安全可信的数据流通使用，**可信数据空间相关参与方在共识规则基础上，通过数字合约达成对流通使用行为预期的共识，并可在使用控制技术中融合区块链、数据沙箱、隐私保护计算、智能合约等技术，保证数据的流通和使用过程如约执行；**跨域跨空间的数据互联互通，**可信数据空间符合国家数据基础设施参考架构并与行业/区域业务节点对接，能够通过数据流通利用基础设施底座统一底座便捷、有效地发现、定位和使用其他区域及数据空间中的数据产品。**多方参与的数据价值共创**，可信数据空间在支持参与方之间数据可信流通的基础上，支持算力服务、人工智能服务、数据治理服务、数据开发服务等第三方服务及平台提供方加入可信数据空间生态，通过连接器提供增值服务，加速数据价值的挖掘、释放。

5　技术架构

5.1　概述

可信数据空间是国家数据基础设施的一部分，符合NDI—TR—2025—01确定的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、接入连接器基本要求的基础上，可信数据空间对其进行功能扩展，形成可信数据空间服务平台、可信数据空间连接器，整体架构见图1。

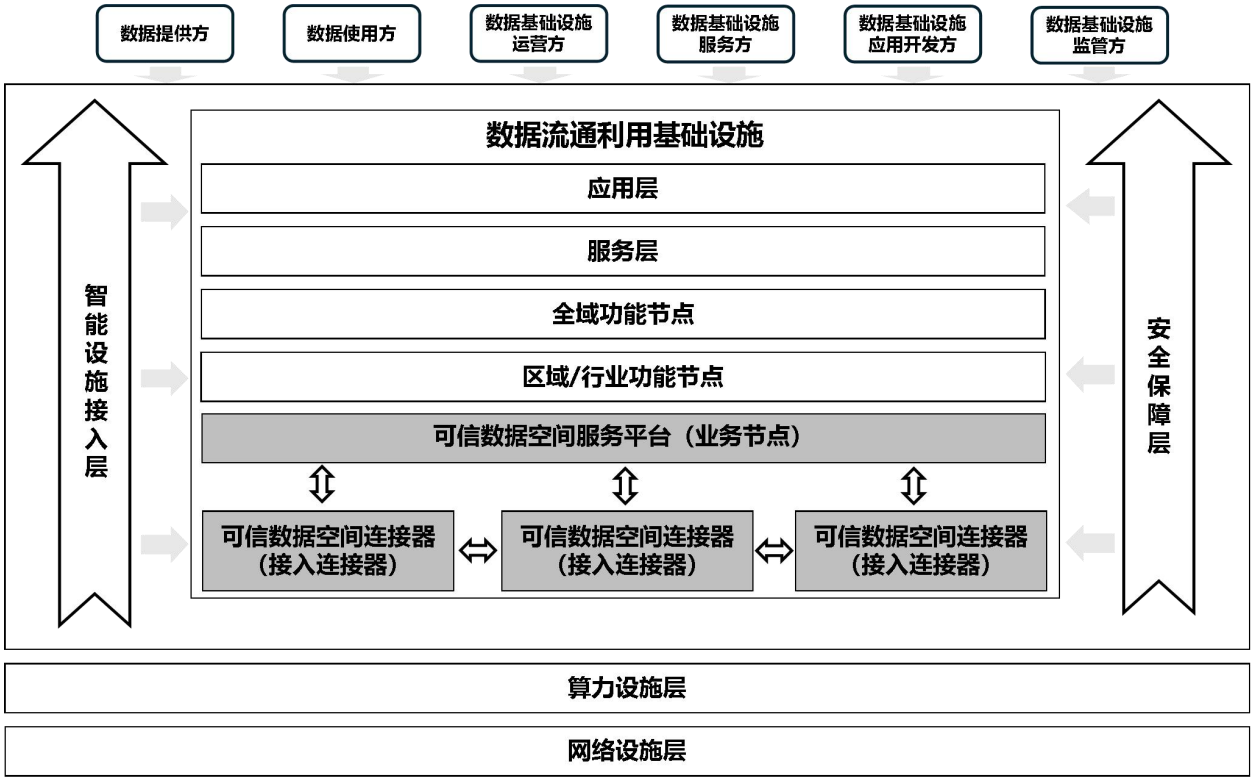

图 1　可信数据空间在数据基础设施中的位置

5.2　功能架构

5.2.1 概述

可信数据空间服务平台的身份管理、连接器管理、目录管理部分需满足数据流通利用基础设施业务节点基本要求，并与区域/行业功能节点对接；可信数据空间连接器继承数据基础设施接入连接器数据资源管理、身份管理、数据传输相关要求。

可信数据空间服务平台，向上连接区域/行业功能节点，并按照NDI—TR—2025—02、NDI—TR—2025—03、NDI—TR—2025—05确定的要求保持与区域/行业功能节点的身份、连接器、目录等信息的互通。向下连接可信数据空间连接器，数据提供方、数据使用方、第三方服务方通过可信数据空间连接器接入空间；提供方连接器通过接入数据源与本地的数据存储、汇聚、加工治理等数据系统对接；使用方数据应用系统通过连接器获取使用数据，完成价值化应用；第三方数据服务提供方，如：算力服务、智能化服务、数据交易服务、数据治理服务、隐私保护计算公共服务等其他第三方增值服务，通过连接器将服务系统接入可信数据空间并提供增值服务，服务提供方对于原始数据持有方来说是数据使用方，对于最终数据使用方来说是数据提供方，可利用连接器相关功能提供增值服务。

5.2.2 可信数据空间服务平台

可信数据空间服务平台包括身份管理、连接器管理、目录管理、数字合约管理、数据空间管理、审计清算、数据交易、数据开发、数据托管等功能，其中数据交易、数据开发、数据托管三部分功能（图中虚框）为可选功能，其他部分为可信数据空间应具备的功能。可信数据空间服务平台功能见图2。

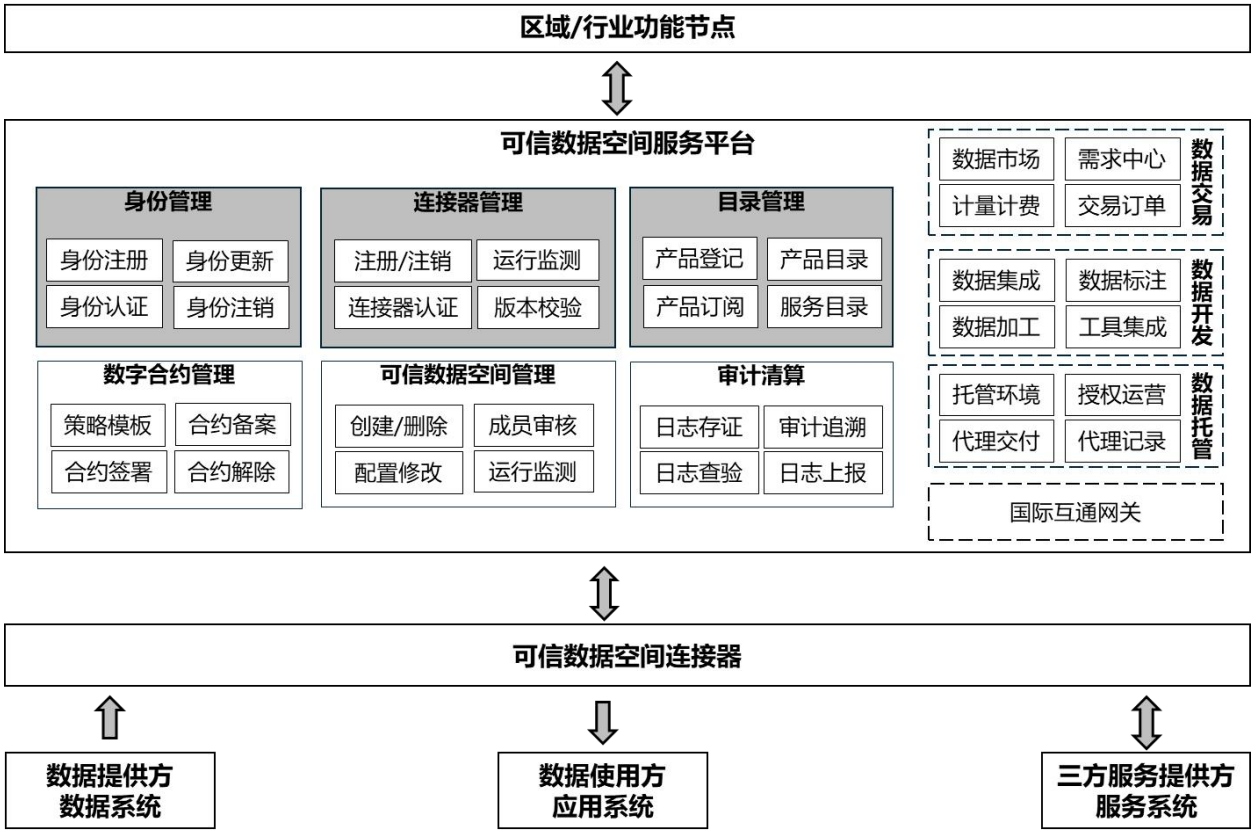

图 2 可信数据空间服务平台功能架构

5.2.2.1 身份管理

区域/行业功能节点为参与数据流通利用的企业/个人、数据流通利用平台等主体提供统一的身份注册、核验以及跨区域/行业身份互认和失效身份信息核验等服务。可信数据空间服务平台可以嵌套或调取接口等方式代理区域/行业功能节点面向空间中的各种用户提供身份注册、核验等服务。可信数据空间服务平台可以基于可信数据空间业务需求，在数据基础设施身份管理基础上拓展身份相关信息和管理要求。可信数据空间服务平台身份管理，应包含以下功能：

1) 身份注册：按照NDI—TR—2025—02确定的业务节点服务流程和要求、NDI—TR—2025—03确定的用户身份注册流程和要求，为数据基础设施新用户分配数字身份。用户可由可信数据空间服务平台代理完成注册，也可用在行业/区域功能节点中已注册的身份直接登录；
2) 身份认证：按照NDI—TR—2025—03确定的用户身份查询流程和要求，提供身份认证功能，支持确认可信数据空间中的用户身份。可信数据空间服务平台可以通过和区域/行业功能节点的交互，实现对数据基础设施所有已注册用户的身份认证；
3) 身份更新：允许可信数据空间用户更新身份信息，若更新的信息涉及NDI—TR—2025—03确定的用户信息相关内容，则需要按照NDI—TR—2025—02确定的业务节点服务流程和要求、NDI—TR—2025—03确定的用户身份更新流程和要求，将身份更新同步至区域/行业功能节点；
4) 空间身份注销：允许可信数据空间用户通过数据空间服务平台注销数据空间身份，注销后不影响用户在数据基础设施中的身份。

5.2.2.2 连接器管理

区域/行业功能节点为数据基础设施中的接入连接器提供注册、验证以及跨区域/行业接入连接器互认等服务。可信数据空间服务平台可以嵌套或调取接口等方式代理区域/行业功能节点面向空间中的连接器提供注册、核验等服务。可信数据空间服务平台可以基于可信数据空间业务需求，在数据基础设施接入连接器管理的基础上拓展连接器相关信息和管理要求。可信数据空间服务平台连接器管理，应包含以下功能：

1) 连接器注册/注销：按照NDI—TR—2025—02确定的业务节点服务流程和要求、NDI—TR—2025—03确定的接入连接器注册流程和要求，为数据基础设施新连接器注册并分配连接器身份信息。用户可由可信数据空间服务平台代理完成连接器注册，也可用在行业/区域功能节点中已注册的接入连接器直接访问可信数据空间。允许可信数据空间用户通过数据空间服务平台注销数据连接器身份，注销后不影响接入连接器在数据基础设施中的身份；
2) 连接器认证：按照NDI—TR—2025—05确定的接入连接器认证要求，服务平台支持对连接器进行身份认证。服务平台也可通过区域/行业功能节点，验证连接器身份；
3) 运行监测：按照NDI—TR—2025—05确定的接入连接器运行监测要求，收集、汇总连接器运行日志，监测可信空间中连接器的运行情况；
4) 能力适配：支持服务平台完成接入连接器与可信数据空间的业务能力适配，使其可满足可信数据空间的业务要求。同一物理连接器系统可接入不同逻辑可信数据空间，但需通过服务平台进行能力适配确保其满足空间业务规则。连接器能力配置的范围包括但不限于连接器在数据资源管理、数据产品管理、数字合约管理以及数据使用控制等方面。

5.2.2.3 可信数据空间管理

可信数据空间服务平台提供数据空间管理功能，支持面向数据流通利用场景，创建包含特定参与主体，数据资源及使用控制策略的逻辑可信数据空间，相关参与方可设置数据产品、服务仅该空间的参与方可见、可用。可信数据空间管理具体应包括如下功能：

1) 创建/删除：提供数据空间创建、删除等基本管理功能，允许数据参与方面向场景需求，基于限定的参与主体、数据资源及使用控制策略创建可信数据空间；按照NDI—TR—2025—02确定的业务节点登记流程和要求，上报可信空间基本信息；
2) 配置修改：允许可信数据空间创建者修改空间基本配置，包括：可信数据空间名称、可信数据空间描述、可信数据空间支持的使用控制策略等；按照NDI—TR—2025—02确定的业务节点服务流程和要求，上报可信空间基本信息；
3) 成员管理：提供可信数据空间成员管理功能，允许数据使用方、数据提供方、第三方服务提供方申请加入数据空间，并在可信数据空间管理方审批通过后授予参与方访问可信数据空间资源的权限；
4) 运行监测：提供可信数据空间运行状态监测基本功能，并与区域/行业功能节点实现互联互通，按照NDI—TR—2025—02确定的运行监测流程和要求，上报可信空间运行信息和业务信息。

5.2.2.4 目录管理

区域/行业功能节点为数据基础设施中的数据资源和产品提供登记服务，编制数据目录，并提供数据查询。可信数据空间服务平台可以嵌套或调取接口等方式代理区域/行业功能节点向空间中的数据资源、产品提供登记等服务。可信数据空间服务平台可以基于可信数据空间业务需求，在数据基础设施目录管理的基础上拓展目录相关信息和管理要求。可信数据空间目录管理，应包含以下功能：

1) 产品登记：支持可信数据空间运营方代理数据提供方将数据产品在行业/区域功能节点中进行数据登记，获取数据产品唯一标识；
2) 产品目录：支持数据提供方将数据产品上架至可信数据空间，确认数据产品的数据标识、登记信息、描述信息等元数据，审核通过后纳入可信数据空间数据目录。按照NDI—TR—2025—02确定的数据目录上报流程和要求向区域/行业功能节点同步目录信息。数据目录提供包括但不限于数据分类分级、场景、数据类型、使用策略等标签。数据目录应提供数据产品查询检索能力，包括查询本空间数据产品以及通过区域/行业功能节点，查询其他数据空间开放的目录及其他业务节点开放的数据目录；
3) 使用申请：提供数据产品使用申请功能，允许可信数据空间中的数据使用方通过连接器向所需使用的数据产品发出申请；
4) 服务目录：支持第三方服务提供方将所提供的数据服务发布至可信数据空间，记录数据服务的服务提供方、描述信息等元数据，审核通过后纳入服务目录，并提供服务的检索查询。

5.2.2.5 数字合约管理

提供数字合约管理的基本功能，协助数据提供方、使用方完成供需撮合及合约签署，应包含以下功能：

1) 策略模板：提供数字合约的策略模板，允许数据提供方、使用方选择模板中的一个或多个策略创建数字合约。策略模板中应包含多种使用控制策略，包括但不限于：限定数据内容、限定数据交付连接器、限定数据使用连接器、限定数据使用者、限定数据使用操作、限定数据使用次数、限定数据使用时长、限定数据可见范围、限定数据可用范围、数据使用时通知、数据使用后销毁等；不同逻辑可信数据空间可根据空间特征提供不同的策略模板。
2) 合约签署：提供合约签署功能，支持可信数据空间运营方作为中介，协助数据提供方、数据使用方完成合约协商及签署；支持通过门户或可信数据空间连接器的方式进行合约创建、协商、签署等流程。合约签订后可信数据空间服务平台按照NDI—TR—2025—02确定的数据交易控制指令流程和要求向数据提供方和使用方连接器下发数据交易控制指令，可信数据空间

服务平台应基于业务需求对相关信息进行拓展，以支持数字合约执行所必需的使用控制策略下发；

3) 合约备案：对可信数据空间中已签署的数字合约进行备案，支持已备案合约的查询；
4) 合约解除：允许合约签署双方解除通过可信数据空间服务平台签署的数字合约，并在合约备案模块标记合约的解除信息。

5.2.2.6 存证审计

允许可信数据空间运营方记录存证可信数据空间的业务执行、系统运行的日志，并提供审计服务。可信数据空间服务平台存证审计功能可采用传统的权威第三方存证，也可结合区块链、时间戳、数字签名和证书、哈希校验等技术，强化数据存证的可信。存证审计应包含如下功能：

1) 日志存证：合约生成、合约协商、合约签订、合约关闭等过程需要进行合约存证；数据发布、数据申请、数据使用过程中需要进行数据操作存证；
2) 日志查验：支持对已存证日志的查询、验证；
3) 审计追溯：支持与行业/区域功能节点对接，提供日志存证信息进行审计溯源、合规检查，支持可信数据空间监管方对可信数据空间运行情况进行监管。支持对数据使用控制是否符合电子合约进行审计；
4) 运行日志上报：支持与连接器对接，收集连接器的运行和业务信息。支持与行业/区域功能节点对接，将可信数据空间运行日志上报至功能节点。

5.2.2.7 数据交易

可信数据空间服务平台可提供数据交易相关功能系统，提高可信数据空间中数据提供方、数据使用方的数据交换意愿及供需匹配效率，可包含以下功能：

1) 数据市场：具备数据市场和需求中心功能，为供需撮合服务支撑，协助完成数据提供方和数据使用方之间的供需匹配；
2) 需求中心：允许数据使用方发布数据需求，并提供需求查阅功能；需求中心可与国家数据基础设施需求信息进行同步；
3) 计量计费：提供计量计费功能，基于可信数据空间中数字合约的签订及履行情况，对数据、应用、服务的使用进行计量计费，保障数据交易参与方权益；
4) 交易订单：管理、查询供需双方产生的数据交易订单。

5.2.2.8 数据开发

可信数据空间服务平台可提供数据开发模块，支持数据供需双方可根据数字合约约定在数据开发环境完成数据开发利用及交付，亦支持数据开发方基于可信数据空间中已有的数据产品，面向场景需求再次开发新的数据产品。数据开发模块可包括隐私保护计算、数据沙箱、可信执行环境等安全可信数据开发工具或环境。数据开发模块可包括以下功能：

1) 数据集成：支持将若干个已在可信数据空间中发布的数据产品集成开发为新的数据产品；
2) 数据标注：支持对已在可信数据空间中发布的数据产品进行标注，提高数据产品的机器可理解性及AI应用价值；
3) 数据加工：支持对已在可信数据空间中发布的数据产品进行二次加工，提高数据产品质量。
4) 工具集成：服务平台可提供各类数据开发工具，如：隐私保护算法、脱敏算法、匿名化算法、加解密算法、低代码开发工具、智能体开发框架、任务调度框架等，供数据开发方使用。

5.2.2.9 数据托管

可信数据空间服务平台可提供数据托管服务，允许数据提供方将数据产品交由服务平台托管运营，代替数据提供方完成其相关活动，可包括以下功能：

1) 托管环境：提供安全、可靠的数据产品存储、计算环境，允许数据提供方将数据产品汇聚、托管在服务平台中；
2) 产品授权：允许数据提供方在托管环境中对数据的申请、访问、使用进行授权；
3) 代理交付：允许数据托管服务方代替数据提供方自动完成合约协商、合约签订、数据交付等数据提供方活动；允许数据托管服务方提供数据交付网关或交付代理，提供代理交付服务；
4) 代理记录：应对托管数据的代理日志进行记录，供数据提供方进行查阅、审计。

5.2.2.10 国际空间互通网关

若可信数据空间，如：跨境数据空间，有与国际上其他数据空间，如：IDS、GAIA-X、Catena-X等，进行数据流通利用的需求。可信数据空间服务平台应提供国际空间互通网关功能，支持数据在不同国际数据空间之间的流通利用。

5.2.2.11 其他服务

可信数据空间服务平台可直接提供或通过连接器接入第三方服务的方式提供其他服务，包括算力、质量评估、数据合规、数据存储等。

5.2.3 可信数据空间连接器

可信数据空间连接器是用户接入可信数据空间服务平台、访问和使用可信数据空间资源的入口。可信数据空间连接器节点是国家数据基础设施的继承及扩展，其中身份管理、数据交付功能应符合NDI—TR—2025—05，并扩展数据产品管理、数字合约管理、数据使用控制三项功能。可信数据空间连接器功能见图3。

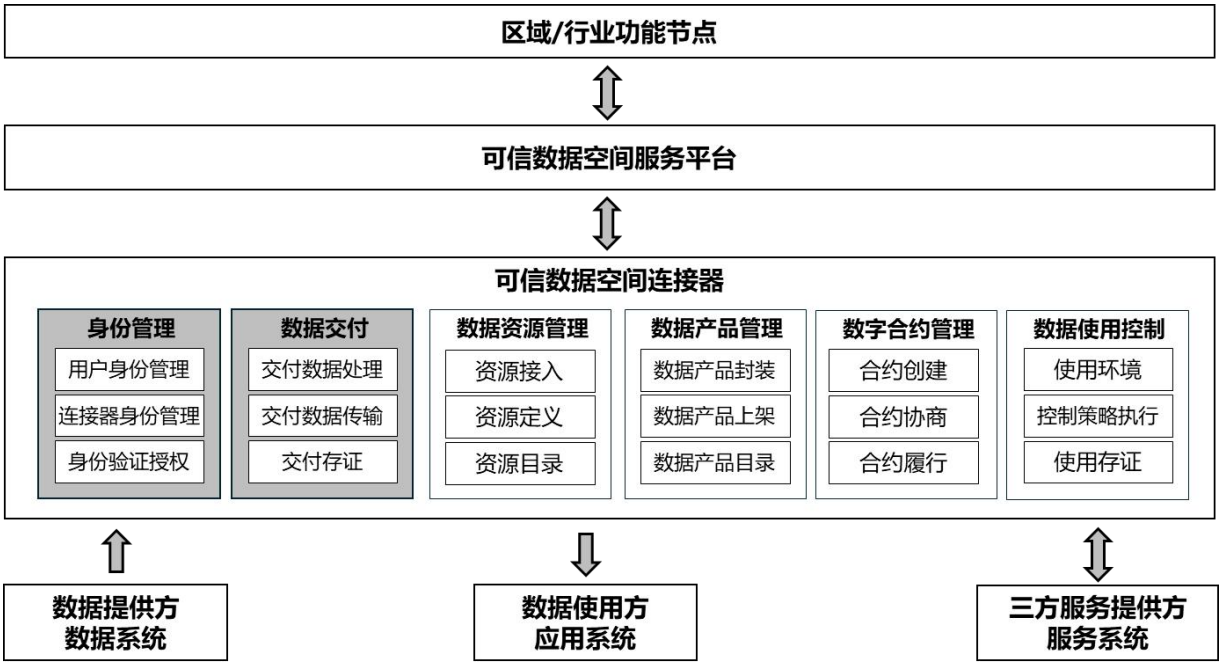

图 3 可信数据空间连接器功能架构

5.2.3.1 数据资源管理

支持数据提供方将数据系统中的数据资源接入可信数据空间连接器，作为形成数据产品的基础，应包括以下功能：

1) 资源接入：支持本地多样数据资源接入能力，包括但不限于对象存储、数据库、本地文件服务器；
2) 资源目录：对接入数据资源进行定义描述，通过数据资源目录进行数据资源管理；
3) 资源管理：数据提供方连接器具备数据源的删除、配置、修改等管理能力。

5.2.3.2 身份管理

按照NDI—TR—2025—05确定的连接器服务流程和要求、NDI—TR—2025—03确定的用户身份注册流程和要求，使用已有身份登录、使用连接器；支持连接器使用方管理用户身份、连接器身份信息，并具备身份验证能力，应包括如下功能：

1) 用户管理：提供连接器用户的管理、登录认证功能，管理连接器用户的身份信息；
2) 连接器身份：管理连接器的身份信息，如：连接器标识、连接器密钥、连接器能力等；
3) 身份验证及授权：支持数据提供方、数据服务方、数据使用方对与接入节点产生交互行为的主体进行身份核实并授予相应权限。

5.2.3.3 数据产品管理

支持数据提供方基于接入数据资源封装数据产品，并对本地数据产品进行管理，应包括以下功能：

1) 数据产品封装：基于接入数据资源，对数据资源配置数据使用策略及数据交付前的预处理策略，封装成数据产品；
2) 数据产品上架：支持数据提供方将已封装的数据产品上架到服务平台。也可支持点对点发送给特定的使用方连接器；
3) 数据产品目录：支持数据提供方维护本地数据产品目录，并提供本地数据产品的检索及使用申请服务。

5.2.3.4 数字合约管理

支持数据提供方、数据使用方通过连接器签订数字合约，并管理已签订的数字合约，也支持用户通过可信数据空间门户创建、协商合约，并下发到接入连接器。数字合约管理应包括以下功能：

1) 合约创建：在数据使用方发起产品使用申请时触发，由数据使用方连接器基于数据产品要求及服务平台策略模板创建，用户通过可信数空间门户创建后下发到接入连接器；
2) 合约协商：支持数据提供方、数据使用方、数据服务方之间就数据的使用策略形成的数字合约进行协商；数字合约协商可进行多轮，协商完成即签订数字合约；
3) 合约履行：数字合约签订完成，数据提供方和数据使用方依据合约内容触发数据交付和数据使用的履约操作。

5.2.3.5 数据交付

按照NDI—TR—2025—05确定的连接器服务流程和要求，完成数据交付。支持数据提供方通过可信数据空间连接器，按照数字合约要求交付原始数据、脱敏后数据或计算结果数据等，应包括以下功能：

1) 交付数据处理：基于数字合约要求，对提供方数据产品进行预处理，如对交付数据进行加密、脱敏或通过隐私保护计算、数据沙箱等方式交付计算结果；

2) 交付数据传输：支持数据提供方根据签订数字合约的要求将待交付数据传输给数据使用方连接器；
3) 交付存证：对数据的处理、传输等交付记录进行日志存证，并上报至存证审计系统及行业/区域功能节点运行监测，支持本地日志查验。

5.2.3.6 数据使用控制

支持数据使用方按照合约要求，在连接器上使用数据产品，应具备以下功能：
1) 使用环境：提供使用数据的软硬件环境，支持数据使用方按照数字合约要求，通过算法或应用使用数据提供方交付的数据产品；连接器可集成隐私保护计算、数据沙箱、数据匿名化等技术，增强数据使用的安全性；
2) 控制策略执行：与数据使用环境联动，确保对数据使用方的数据使用行为进行实时监测与控制，保证数据的使用符合数字合约要求；
3) 使用存证：连接器应将数据使用过程日志进行细粒度的存证，并按照要求上报给存证审计系统，并提供日志的查询及溯源服务。

5.3 交互关系

5.3.1 概述

可信数据空间交互关系描述了可信数据空间服务平台、可信数据空间连接器、区域/行业功能节点之间的系统接口及交互内容。分为南北向接口和东西向接口。其中南北向接口包括区域/行业功能节点与可信数据空间服务平台之间、区域/行业功能节点与可信数据空间连接器之间、可信数据空间服务平台与可信数据空间连接器之间的接口。东西向的接口指可信数据空间连接器之间的接口。

5.3.2 区域/行业功能节点与可信数据空间服务平台的交互

区域/行业功能节点与可信数据空间服务平台之间的接口应符合NDI—TR—2025—02对区域/行业功能节点与业务节点的互联互通规范。

区域/行业功能节点向可信数据空间服务平台提供身份注册、身份更新、身份注销、身份验证、身份信息查询等身份接口，数据资源登记、数据资源登记更新、数据资源登记撤销、数据产品登记、数据产品登记更新、数据产品登记撤销、数据产品上架、数据产品上架信息更新、数据产品下架、业务节点注册、业务节点更新、业务节点删除等登记接口，数据目录查询、业务节点目录查询等目录接口，标识解析、接入连接器地址上报等标识接口，运行监测和业务数据上报等监测接口。具体接口要求参见NDI—TR—2025—02。区域/行业功能节点与可信数据空间服务平台的接口见图4。

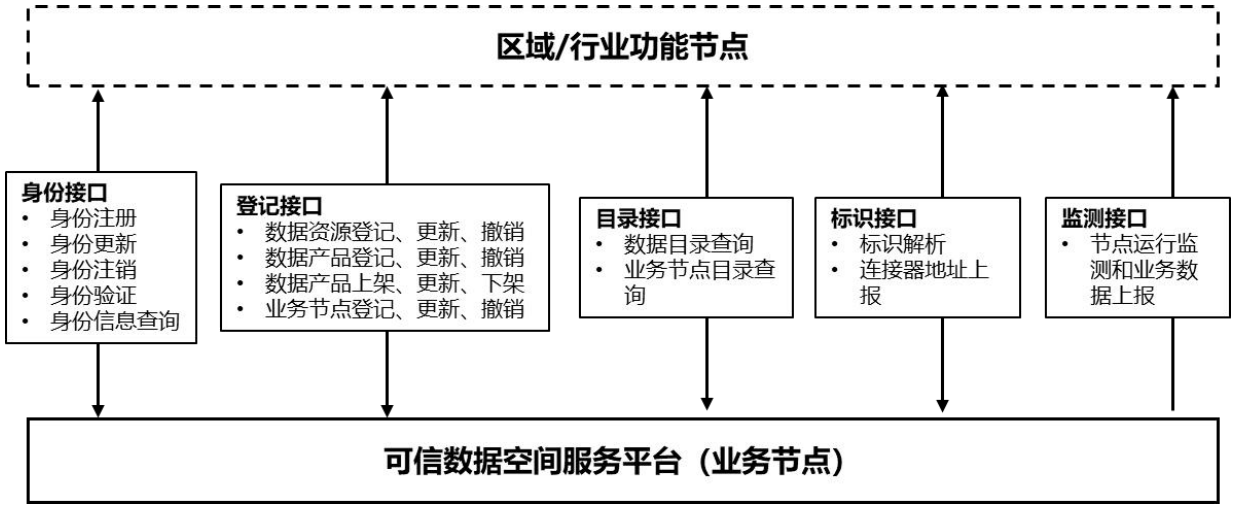

图 4　区域/行业功能节点与可信数据空间服务平台的接口示意图

5.3.3　区域/行业功能节点与可信数据空间连接器的交互

区域/行业功能节点与可信数据接入连接器之间的接口应符合NDI—TR—2025—02对区域/行业功能节点与接入主体的互联互通规范。

区域/行业功能节点向可信数据接入连接器提供身份核验、身份信息查询等身份接口，数据目录查询、业务节点目录查询等目录接口，标识解析、接入连接器地址上报等标识接口，运行监测和业务数据上报等监测接口。具体接口要求参见NDI—TR—2025—02。区域/行业功能节点与可信数据空间连接器的接口5。

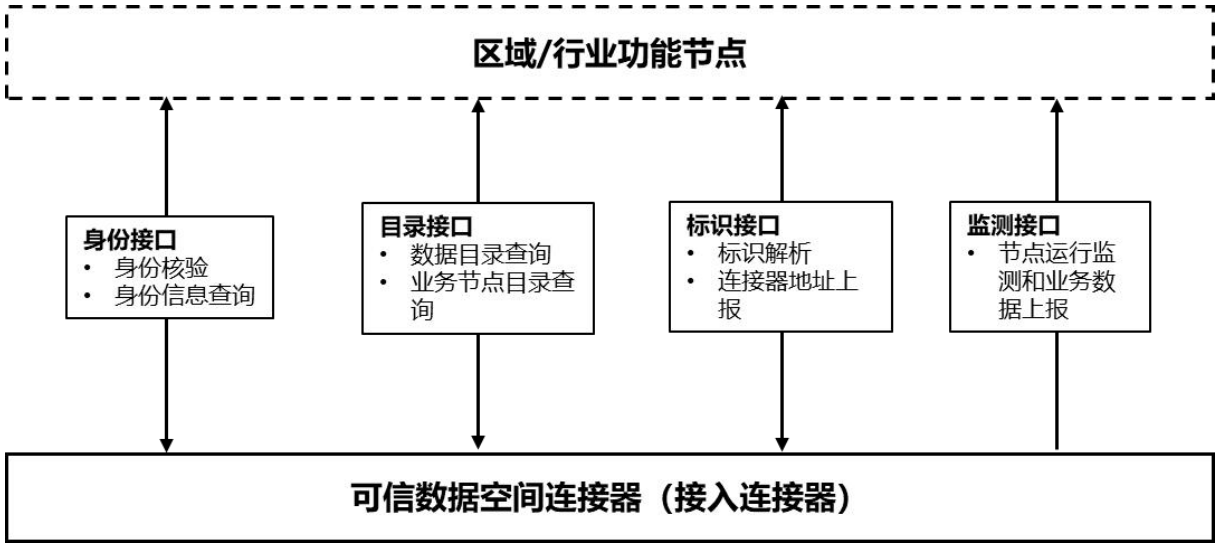

图 5　区域/行业功能节点与可信数据空间连接器的接口示意图

5.3.4　可信数据空间服务平台与可信数据空间连接器的交互

可信数据空间服务平台与可信数据空间连接器之间的接口应在符合NDI—TR—2025—02对业务功能节点与接入主体的互联互通规范的基础上进行拓展，拓展后的接口应包括身份接口、数据产品接口、

数字合约接口、使用控制接口、合规监测接口和连接器接口。可信数据空间服务平台与可信数据空间连接器的接口见图6。

可信数据空间服务平台可以嵌套或调取接口等方式代理区域/行业功能节点面向可信数据空间连接器提供统一身份注册、核验，接入连接器注册、核验，数据资源、产品登记等服务。

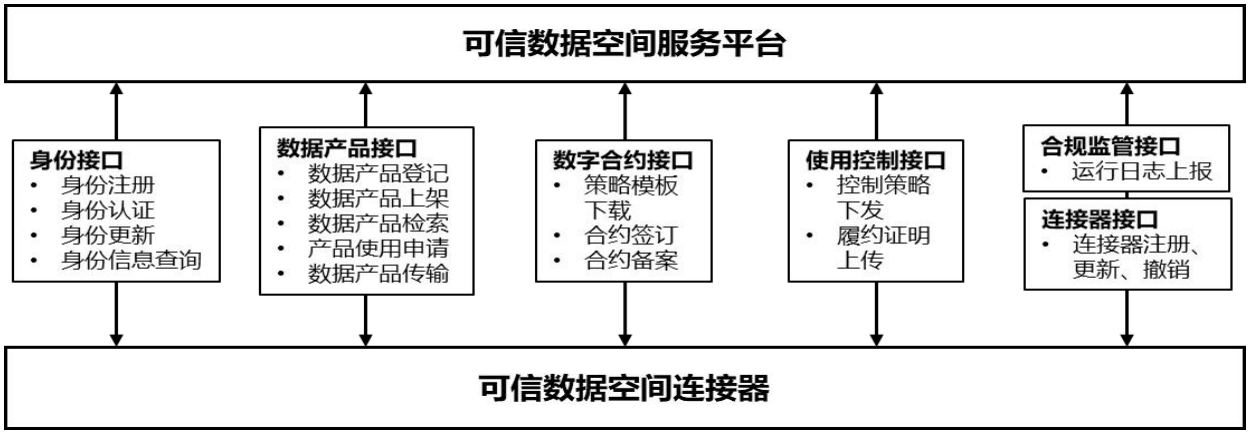

图 6　可信数据空间服务平台与可信数据空间连接器的接口示意图

5.3.4.1　身份接口

1) 身份注册：可信数据空间服务平台按照NDI—TR—2025—02确定的业务节点服务流程和要求，可以嵌套或调取接口等方式代理区域/行业功能节点面向可信数据空间连接器提供用户身份注册接口，并基于本平台业务需求进行必要的拓展；
2) 身份更新：可信数据空间服务平台按照NDI—TR—2025—02确定的业务节点服务流程和要求，可以嵌套或调取接口等方式代理区域/行业功能节点面向可信数据空间连接器提供用户身份更新接口，并基于业务需求进行必要的拓展；
3) 身份认证：可信数据空间服务平台向可信数据空间连接器提供符合NDI—TR—2025—03确定的用户身份查询流程和要求的接口，并基于业务需求进行必要的拓展；
4) 身份信息查询：可信数据空间服务平台按照NDI—TR—2025—02确定的业务节点服务流程和要求，可以嵌套或调取接口等方式代理区域/行业功能节点面向可信数据空间连接器提供用户身份查询接口，并基于业务需求进行必要的拓展。

5.3.4.2　数据产品接口

1) 数据产品登记：可信数据空间服务平台按照NDI—TR—2025—02确定的业务节点服务流程和要求，可以嵌套或调取接口等方式代理区域/行业功能节点面向可信数据空间连接器提供数据产品登记接口，并基于本平台业务需求进行登记请求、权属信息、合规检查等方面拓展；
2) 数据产品上架：可信数据空间服务平台向可信数据空间连接器提供数据产品上架接口。可信数据空间连接器向可信数据空间服务平台发起上架请求，携带数据产品上架的元数据及使用策略；可信数据空间服务平台对数据产品进行合规检查，检查通过后编入本空间数据目录；可信数据空间服务平台支持可信数据空间按照NDI—TR—2025—02确定的数据目录上报流程和要求向区域/行业功能节点同步目录信息；
3) 数据产品检索接口：可信数据空间数据产品上架后，可信数据空间连接器可通过数据产品检索接口查询本空间数据目录中上架的数据产品；数据产品检索接口按照NDI—TR—2025—02

确定的业务节点服务流程和要求应支持可信数据空间连接器通过可信数据空间服务平台检索全域数据目录、业务节点目录；

4) 数据产品使用申请接口：数据使用方可信数据空间连接器在可信数据空间服务平台数据目录查找需要的数据产品，并对本平台数据目录中上架的数据产品发起数据产品使用申请；可信数据空间服务平台和数据提供方可信数据空间连接器对数据使用方的数据使用请求进行审批；

5) 数据产品传输接口：可信数据空间服务平台可按照NDI—TR—2025—05确定的数据传输流程和要求，通过部署可信数据空间服务连接器完成向其他可信数据空间服务连接器的数据传输，支持服务平台的数据开发、数据托管等功能。

5.3.4.3 数字合约接口

1) 策略模板下载：可信数据空间连接器可从可信数据空间服务平台下载该空间支持的控制策略模板，并在此基础上创建数字合约；

2) 合约签订：可信数据空间服务平台向数据提供方或使用方可信数据空间连接器同步数字合约，双方进行合约签署，可信数据空间服务平台进行整体合约管理；合约信息中包括数据使用控制策略；

3) 合约备案：可信数据空间连接器向可信数据空间服务平台备案已签订的数字合约信息。

5.3.4.4 使用控制接口

1) 控制策略下发：可信数据空间服务平台按照NDI—TR—2025—02确定的数据交易控制指令获取流程和要求向可信数据空间连接器提供数据交易控制指令同步，并拓展使用控制策略相关内容；支持在执行合约中规定的策略时实时交互执行情况，并在异常情况下终止执行；

2) 履约证明上传：可信数据空间连接器按照使用控制策略执行完数字合约后，上传履约证明。

5.3.4.5 合规监管接口

1) 运行日志上报：可信数据空间连接器向可信数据空间服务平台上报本地运行日志。

5.3.4.6 连接器接口

1) 连接器注册、更新、撤销：可信数据空间服务平台按照NDI—TR—2025—02确定的业务节点服务流程和要求可以嵌套或调取接口等方式代理区域/行业功能节点面向可信数据空间连接器提供连接器注册、更新、撤销接口，并基于本平台业务需求进行必要的拓展。

5.3.5 可信数据空间连接器之间的交互

可信数据空间之间的接口应在符合NDI—TR—2025—05，接入连接器之间接口规范的基础上进行拓展，拓展后的接口应包括数字合约接口、数据目录接口、数据交付接口、使用控制接口。可信数据空间连接器之间的接口见图7。

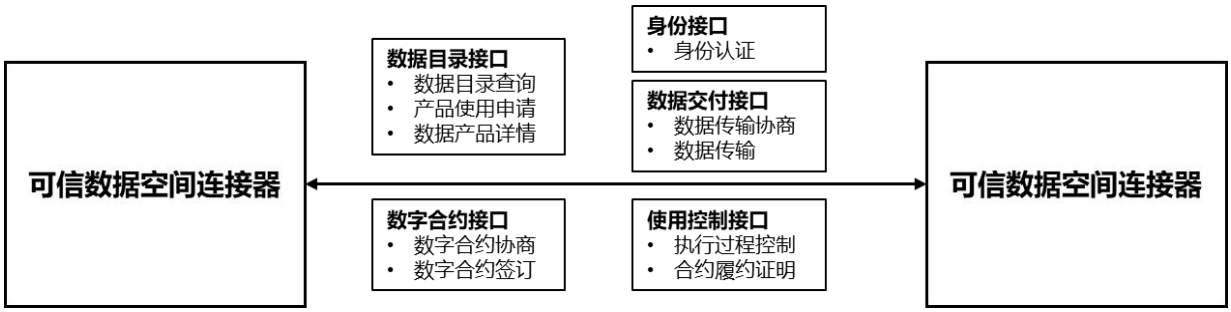

图 7　可信数据空间连接器之间的接口示意图

5.3.5.1　身份接口

1) 身份认证：可信数据空间连接器向其他连接器提供符合NDI—TR—2025—03确定的用户身份查询流程和要求的接口，并基于业务需求进行必要的拓展。

5.3.5.2　数字合约接口

1) 数字合约协商：数据提供方、数据使用方之间直接使用连接器进行数字合约的协商，确定数字合约内容；
2) 数字合约签订：数据提供方、数据使用方之间直接使用连接器签订数字合约。

5.3.5.3　数据目录接口

1) 数据目录查询接口：提供符合NDI—TR—2025—05中确定的数据产品目录查询流程和要求的本地数据产品目录查询，使用方连接器可通过该接口直接向提供方连接器获取数据目录信息；
2) 产品使用申请接口：提供产品使用申请接口，使用方连接器通过该接口直接申请使用提供方连接器中的数据产品；
3) 数据产品详情：提供数据产品详情查询接口，使用方连接器通过该接口查询指定数据产品的详细元数据。

5.3.5.4　数据交付接口

1) 数据传输协商：数据提供方和数据使用方连接器根据可信数据空间平台同步的交易控制指令建立互联，协商数据传输细节，如交付形式、协议、地址等；
2) 数据传输：按协商结果调用相关的传输协议或者传输工具交付数据。

5.3.5.5　使用控制接口

1) 执行过程控制：连接器提供策略执行过程控制接口，支持在执行合约中规定的策略时实时交互执行情况，并在异常情况下终止执行；
2) 合约履约证明：连接器向此次合约的参与方提供数字合约的执行完成证明；
3) 接入连接器的使用控制支持连接器与连接器之间的直接连接，也应支持通过可信数据空间服务平台使用控制接口中转完成不同连接器之间的使用控制信息传递。

6　业务流程

6.1　登记可信数据空间

可信数据空间作为业务节点接入数据基础设施体系中，登记相关服务信息后，可面向数据基础设施中的接入主体提供服务。主要流程见图8。

1) 可信数据空间运营方按照NDI—TR—2025—03确定的平台身份注册流程和要求完成平台身份注册；
2) 可信数据空间运营方按照NDI—TR—2025—02确定的业务节点登记流程和要求完成业务节点登记；可信数据空间运营方应在业务节点登记过程中登记可信数据空间限定的参与主体、数据资源及使用控制策略等基本信息；
3) 基于一个可信数据空间服务平台设施建立的多个可信数据空间可登记为一个业务节点，也可登记为各自独立的业务节点；登记为一个业务节点时，各可信数据空间服务统一管理、统一开展与区域/行业功能节点以及数据基础设施中其他接入主体的交互；登记为各自独立的业务节点时，各可信数据空间均需进行平台身份注册和业务节点登记，各可信数据空间自行开展与区域/行业功能节点以及数据基础设施中其他接入主体的交互。

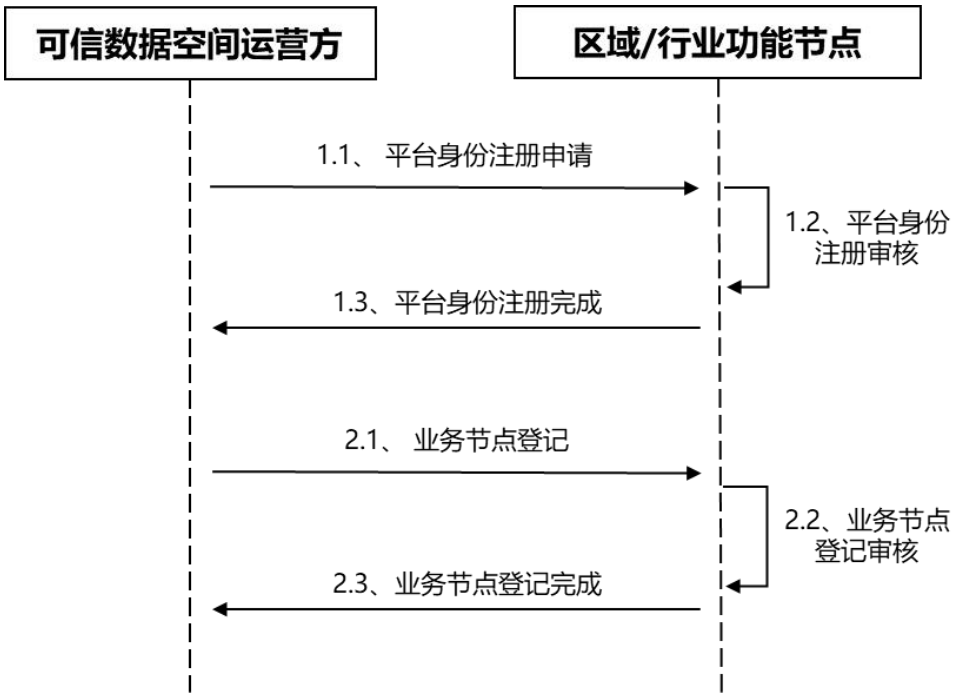

图 8　登记流程示意图

6.2　发现可信数据空间

可信数据空间作为业务节点接入数据基础设施体系后，数据基础设施中的接入主体可以通过业务节点目录或数据产品目录查询发现并访问可信数据空间。主要流程见图9。

1) 可信数据空间完成平台身份注册后，按照NDI—TR—2025—02确定业务节点登记流程和要求进行业务登记，并注明可信数据空间限定的参与主体、数据资源及使用控制策略等信息，区域/行业功能节点审核通过后将相关信息编入业务节点目录；
2) 可信数据空间按照NDI—TR—2025—02确定数据目录上报流程和要求完成数据目录上报，区域/行业功能节点审核通过后将相关信息编入数据目录；
3) 数据基础设施中的接入主体可以通过数据基础设施中的数据目录和业务节点目录发现可信数据空间业务节点或可信数据空间中的数据产品；

4) 数据基础设施中的接入主体可通过数据目录和业务节点目录提供地址、标识访问可信数据空间。

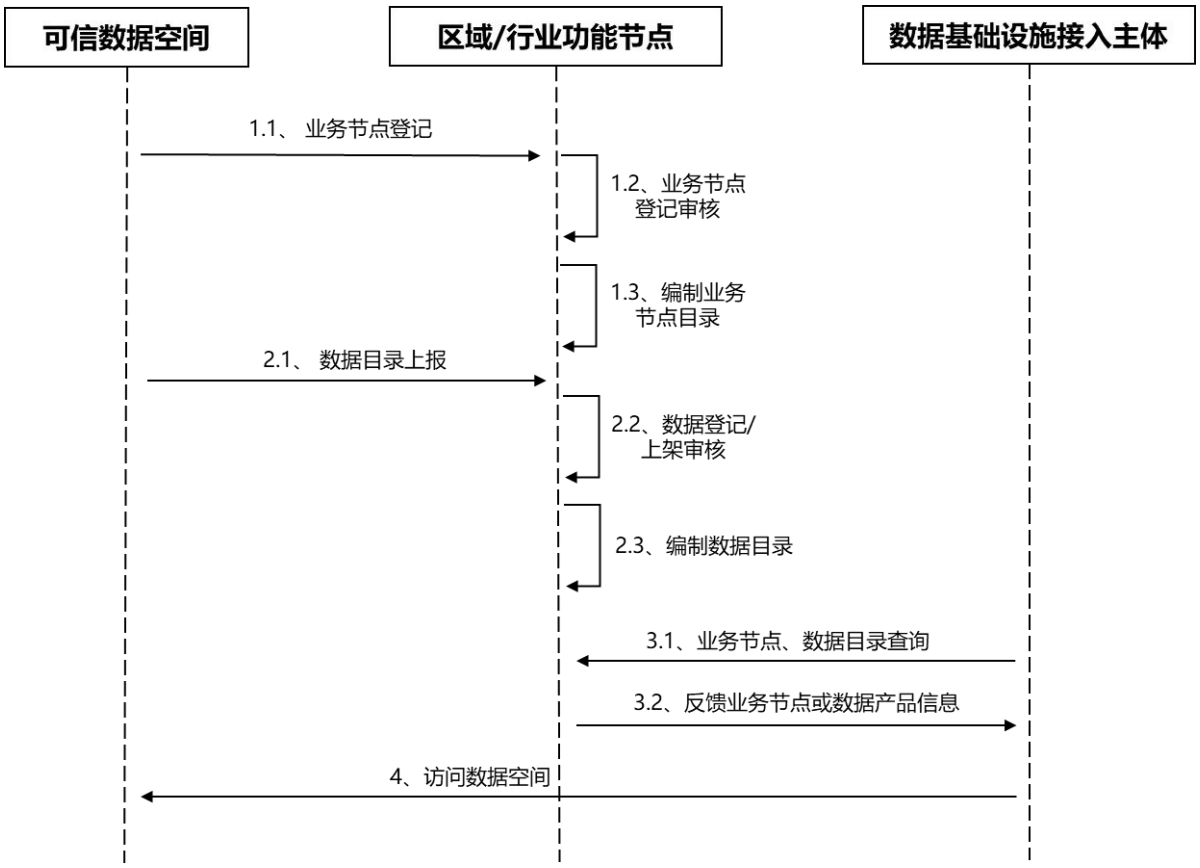

图 9　发现流程示意图

6.3　创建逻辑可信数据空间

数据基础设施中的接入主体在发现可信数据空间后，可在可信数据空间的业务规则允许下，在可信数据空间服务平台上创建新的逻辑可信数据空间。主要流程及建立多个逻辑可信数据空间的示意图见图10和图11。

1) 可信数据空间应按照NDI—TR—2025—03确定的登录流程和要求接受接入主体登录，按照登记的服务内容提供服务，不得隐瞒全局数据和业务服务信息，不得限制接入主体对其他业务节点和服务的自主选择；
2) 可信数据空间可根据业务规则审核登录的接入主体信息，并进行接入连接器能力检查和适配，确定接入主体和连接器符合可信数据空间规则要求后可为通过审核的接入主体注册可信数据空间账户；
3) 通过审核并获得账户的接入主体接入可信数据空间，在空间内开展数据流通利用；
4) 可信数据空间用户可按照可信数据空间服务平台的规则要求申请建立新的逻辑可信数据空间；新建可信数据空间应明确空间参与主体要求，数据资源及使用控制策略等；可信数据空间服务平台按照业务规则，在审核用户申请后完成新建数据空间的配置；新建可信数据空间需接入数据基础设施的，应符合可信数据空间登记的相关要求，具体内容见6.1。

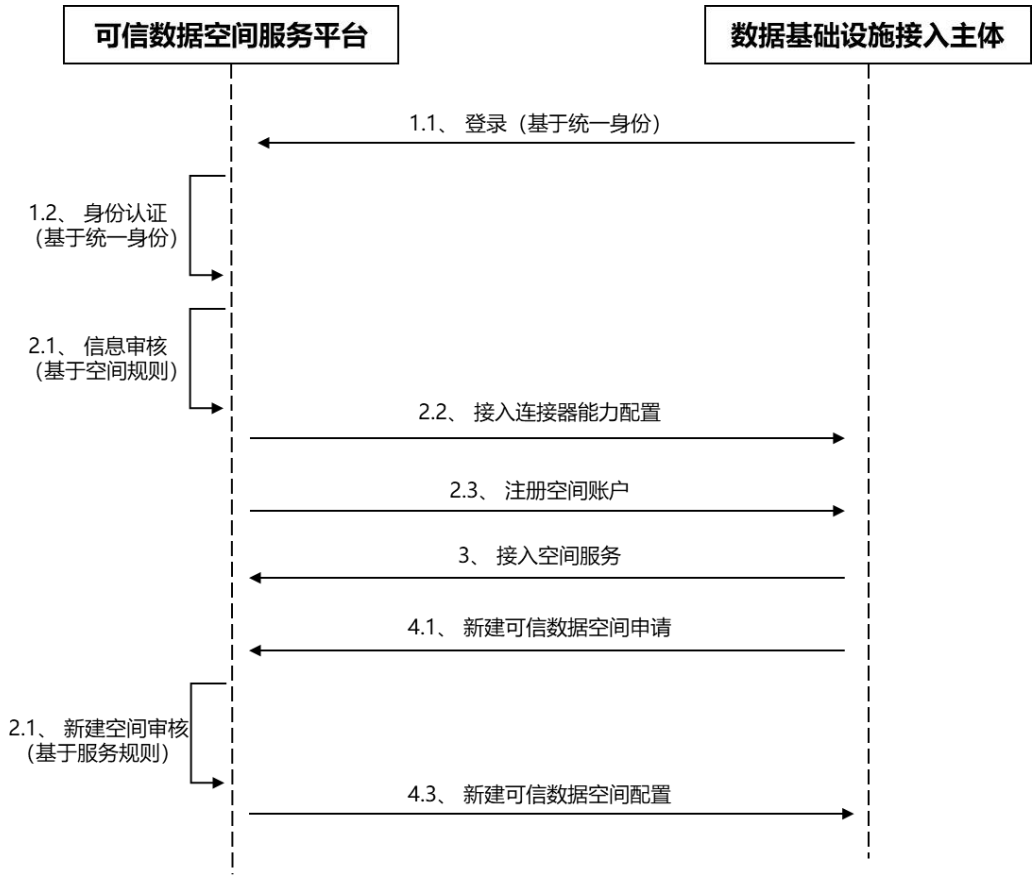

图 10　接入流程示意图

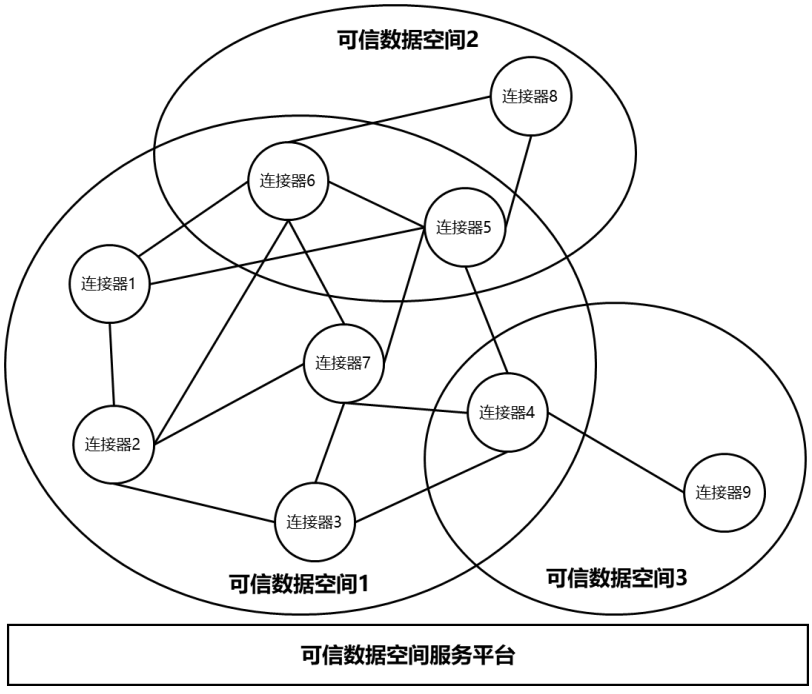

图 11　可信数据空间服务平台建立多个逻辑可信数据空间示意图

6.4 数据流通利用

在可信数据空间中，数据提供方和使用方可通过数据资源接入、数据产品上架、数据产品申请、合约签订、数据传输等业务流程，开展数据流通利用。主要流程见图12。

1) 数据提供方连接器将本地数据资源接入，形成本地数据产品，设施产品使用策略并纳入连接器本地数据目录进行管理；
2) 数据提供方向可信数据空间服务平台申请数据产品上架，按照NDI—TR—2025—06确定的登记、上架信息要求上传必要的信息。可信数据服务空间可以基于业务需求对相关信息进行拓展。可信数据空间服务平台审核通过后，纳入平台数据目录，并按照NDI—TR—2025—02确定的数据产品登记流程和要求向区域/行业功能节点申请数据产品登记。区域/行业功能节点审核通过后，可信数据空间服务平台按照NDI—TR—2025—02确定的数据上架登记流程和要求向区域/行业功能节点提交数据产品上架产品信息，完成数据产品在数据基础设施中的登记、上架；
3) 数据使用方连接器在平台数据目录查找需要的数据产品，并发起数据使用申请。平台和使用方连接器对数据使用方的数据使用请求进行审批；
4) 可信数据空间服务平台向数据提供方和使用方连接器下发合约，双方进行合约签署，平台进行整体合约管理；合约签订后可信数据空间服务平台按照NDI—TR—2025—02确定的数据交易控制指令流程和要求向数据提供方和使用方连接器下发数据交易控制指令，可信数据空间服务平台应基于业务需求对相关信息进行拓展，支持使用控制策略下发；
5) 提供方按照合约约定、协商结果交付数据；
6) 数据使用方连接器按照合约中的使用控制策略约束进行合规使用；
7) 在身份认证、数据流通、数据使用的整个过程中，数据提供方和数据使用方连接器需记录用户和操作日志，并将履约证明传至对方连接器以及可信数据空间服务平台。

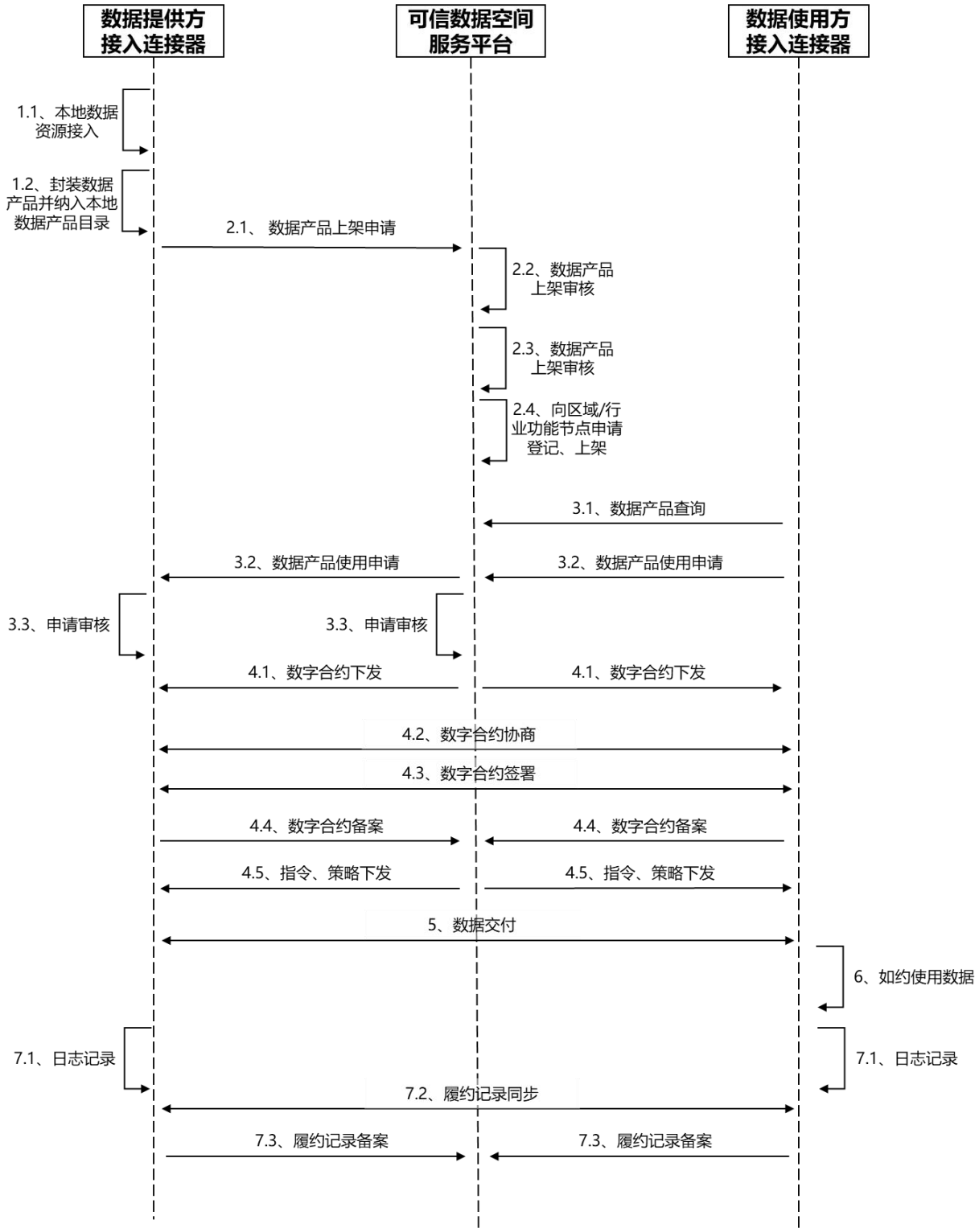

图 12　流通利用流程示意图

7　安全要求

7.1 概述

可信数据空间服务平台及连接器应满足国家数据基础设施业务节点、接入连接器相关规范中规定的安全要求，并在此基础上为可信数据空间的建设运营、数据的流通利用提供整体的安全保障。

可信数据空间的安全保障要求既可通过在可信数据空间服务平台、连接器中集成数据沙箱、区块链、隐私保护计算、数据匿名化等技术来实现，也可通过调用区块链公共服务平台、隐私保护公共服务平台或是其他第三方安全保障平台的技术能力来满足可信保障要求。区块链公共服务平台、隐私保护公共服务平台或是其他第三方安全保障平台通过可信数据空间连接器接入可信数据空间并提供安全保障服务。

7.2 数字合约安全

7.2.1 数字合约完整性

数字合约必须具备防篡改机制，确保其内容在生成、传输和存储过程中不被恶意修改，始终符合各参与方的初始约定和预期。

7.2.2 数字合约真实性

数字合约需通过可靠的身份验证和电子签名技术，确保参与方的身份真实且授权有效，同时达成共识，避免后续争议。

7.3 数据产品安全

7.3.1 数据安全分级

可信数据空间应支持对接入可信数据空间的数据产品进行安全等级划分，提供差异化的安全保障策略，应具备：数据敏感度评估、数据分类打标、分级策略管理等能力。

7.3.2 数据传输安全

可信数据空间应确保数据传输的安全，合理使用数据加密、数字签名、虚拟数据网络等技术，保障数据传输过程防窃听、防篡改。

7.3.3 数据存储安全

可信数据空间应提供或集成安全可靠的数据存储环境，允许数据提供方将数据存放于安全受控的环境内；合理使用数据加密、数字签名、访问控制、数据沙箱等技术，保障存储数据的完整性、隐私性、真实性。

7.3.4 数据计算安全

可信数据空间应提供或集成安全可靠的数据计算环境，允许数据使用方在安全和受控的环境下对数据进行分析处理；合理使用智能合约、可信执行环境、联邦学习、密态计算、零知识证明、安全多方计算等技术，保障数据计算过程的隐私性、完整性、真实性。

7.4 空间运营安全

7.4.1 运行维护安全

可信数据空间应具备安全运营、运维能力，保障可信数据空间的安全、合规运行，避免可信数据空间的运行数据、业务数据被窃取、滥用。

7.4.2 日志存证安全

可信数据空间应支持对可信数据空间中的数据流通及使用的详细日志进行安全存证及查证溯源，合理使用分布式账本等技术，保证日志存证的不可篡改。

7.4.3 合规审计安全

可信数据空间应对可信数据空间内的数据操作行为进行全流程监控与合规性验证，确保数据访问、操作留痕及异常行为可追溯。

参 考 文 献

[1] 《国家数据基础设施建设指引》
[2] 《可信数据空间行动计划》
[3] 《数据领域常用名词解释（第一批）》
[4] 《数据领域常用名词解释（第二批）》
[5] NDI—TR—2025—04 数据基础设施 标识管理规范