ICS 35.240
CCS L 67

T/EJCCCSE

团 体 标 准

T/EJCCCSE XXX—2025

AI 大数据应用平台信息技术安全开发运营技术规范

AI big data application platform information technology security development operation technology specification

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

2025－XX－XX 发布 2025－XX－XX 实施

中国商业股份制企业经济联合会 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××××提出。

本文件由中国商业股份制企业经济联合会归口。

本文件起草单位：

本文件主要起草人：

AI 大数据应用平台信息技术安全开发运营技术规范

1 范围

本文件规定了AI大数据应用平台信息技术安全开发运营的术语和定义、基本要求、运营要求、安全要求和维护要求内容。

本文件适用于AI大数据应用平台信息技术安全开发运营。

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。

GB/T 22080-2016 信息技术 安全技术 信息安全管理体系 要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

数据服务 data service

基于数据资源形成的具有规范化描述、对外提供访问地址、并可被重复调用的业务功能单元。

3.2

服务规约 service specification

描述某一类数据服务需遵循的通用接口规范。

4 基本要求

4.1 总体架构

数据服务运营管理总体架构包括服务管理层、服务网关层、服务运营层，满足GB/T 22080-2016的要求。

4.2 服务管理层

服务管理层应支持服务开发、服务目录管理、配置管理、数据源管理等统一的服务管理能力，具体要求如下：

——服务开发应支持用户自定义开发创建各种数据服务；

——服务目录管理应支持服务的生命周期管理、服务规约管理及服务列表管理；

——配置管理应提供服务分类管理及标签管理；

——数据源管理应支持结构化数据库的数据源适配以及数据资源管理。

4.3 服务网关层

服务网关层应支持服务访问通道的控制能力，是后端服务集成的载体，请求访问时应通过服务网关才能正常访问到服务本身，具体要求如下：

——应支持服务策略管理，包括但不限于流量控制策略、数据量控制策略、服务授权策略等；

——应支持服务的路由转发、服务限流等功能。

4.4 服务运营层

服务运营层应支持服务订阅、运营统计、服务评价等功能，具体要求如下：

——在服务提供前，支持服务使用者提出需求申请、订阅申请；

——在服务运行中，支持服务使用情况的统计分析；
——在服务使用后，支持对服务的效能进行量化的评价评估。

4.5 各层关系

服务管理层、服务网关层、服务运营层之间的关系如下：
——服务管理层用于服务的构建和管理，为服务网关层及运营层提供服务对象；
——服务网关层为服务管理层提供服务管控的载体，为服务运营层提供运营统计所需的日志数据；
——服务运营层为服务网关层提供策略管理依据，为服务管理层提供服务需求申请及服务评价，支撑服务管理层进行服务创建与升级优化。

5 运营要求

5.1 服务管理层

5.1.1 服务开发

服务开发支持多种服务开发方式，应提供可视化服务开发页面，支持对接服务构建引擎、对接结构化数据库服务开发、以及服务编排等开发方式，具体要求如下：
——服务基本信息。应支持服务基本信息的编辑，基本信息包括但不限于：服务名称、服务版本号、服务创建时间、服务类型、服务状态、服务地址、标签等；
——服务重建。应支持对创建失败的服务，按照创建策略重新进行创建；
——服务开发方式包括但不限于对接服务构建引擎、对接结构化数据库、服务编排，具体要求如下：

- 对接服务构建引擎。通过选择服务构建引擎提供的数据集，完成对数据集的设置，列表支持筛选数据集，展示数据集的详情和数据量。选定数据后，进行服务的输入参数与输出参数配置，并支持根据数据集字段进行数据范围控制；
- 对接结构化数据库。支持使用脚本编写，完成单表或者多表关联的数据服务开发，支持各类结构化数据库，通过解析脚本，完成输入输出参数以及数据筛选条件的配置；
- 服务编排。通过可视化界面将服务目录的服务作为编排对象，按执行顺序进行串联，上游服务的输出映射为下游服务的输入，支持配置编排服务的输入参数和输出参数，完成配置后形成新的编排服务。

5.1.2 服务目录

5.1.2.1 服务生命周期管理

服务生命周期管理范围包括自行开发服务及第三方服务，应支持服务生命周期基本管理功能，包括但不限于：服务注册、服务发布、服务启用、服务停用、服务上架、服务下架、服务注销、服务验证等，具体要求如下：
——服务注册。应支持将平台构建的服务注册到服务目录，注册信息包括但不限于：服务名称、服务版本号、服务地址、服务描述、服务分类、服务类型、请求方式、标签等；
——服务发布。应支持服务发布功能，实现数据服务共享展示；
——服务启停。应支持服务启停状态控制功能，实现对服务网关启停指令的下发；
——服务上架。应支持将已下架的服务进行上架，重新对外提供服务；
——服务下架。当服务信息发生变化或需要注销时，应支持将服务目录上的数据服务进行下架处理，下架的服务不再对外提供服务；
——服务注销。应支持对已下架的服务进行删除，实现服务注销；
——服务验证。应支持服务运行情况的验证，显示服务的运行状态，如正常、失败。

5.1.2.2 服务规约管理

服务规约用于服务注册到服务目录时进行服务引用和检测，包括服务功能、请求信息、响应信息和服务返回代码，服规约管理具体要求如下：

——应支持服务规约的导入、删除及查询；
——服务规约信息包括但不限于服务规约标识符、版本号、服务规约名称、简要情况、接口语言类型等；
——应支持接口定义及返回结果的格式验证规则导入；
——服务注册时可通过服务规约的验证规则进行服务验证，确保服务符合规约定义。

5.1.2.3 服务列表管理

服务列表管理范围包括自行开发服务及第三方服务，应支持将数据服务批量导入服务列表，并支持服务操作日志记录。

5.1.3 配置管理

5.1.3.1 分类管理

服务分类管理支持服务分类设置以及服务类型的查询、添加、编辑、删除、启停等管理功能，具体要求如下：
——应支持多级服务类型的查询、添加、编辑、删除、启停等；
——应支持服务类型的创建和编辑，服务类型信息包括但不限于服务类型名称、服务分类、说明、状态等；
——通过服务类型启停控制服务类型的状态，停用的服务类型不可在服务上引用。

5.1.3.2 标签管理

标签管理支持标签分类设置以及标签的查询、添加、编辑、删除、启停等管理功能，具体要求如下：
——应支持多级标签的查询、添加、编辑、删除、启停等；
——应支持标签的创建和编辑，标签信息包括但不限于标签名称、标签分类、标签说明、状态等；
——通过标签启停控制标签的状态，停用的标签不可在服务上引用。

5.1.4 数据源管理

5.1.4.1 数据源资源池

应支持统一的数据源资源池管理，通过建立数据源连接实现对接不同的数据源，具体要求如下：
——应支持数据源创建、编辑、连接、探查、删除等，数据源信息包括但不限于连接名称、数据库类型、说明、用户名、密码、IP 地址、端口号、数据库名称、来源信息等；
——已创建的数据源连接应支持通过连接功能测试连接状态，连接正常返回成功状态；
——针对连接正常的数据源，应支持通过探查功能发现系统中的数据表，选定数据表后采集数据表的元数据信息，实现数据资源的对接。

5.1.4.2 数据资源管理

数据资源管理可以通过数据源资源池探查自动生成，也可以手动生成。手动生成需要与已有的数据源资源池建立关联，引用数据源资源池的数据库信息。数据资源支持创建、编辑功能，具体要求如下：
——应支持数据资源手动创建功能，数据资源信息包括但不限于中文名称、英文名称、说明、标签、资源池、表结构、样例数据。其中，资源池源于数据源资源池中，表结构支持单个字段添加及批量导入，样例数据可以直接从数据源中抽取或手动导入；
——应支持数据资源编辑，可以对数据资源表及表结构信息进行修改。

5.2 服务网关层

5.2.1 策略管理

5.2.1.1 策略控制方式管理

策略控制方式包括单个策略控制和全局策略控制，具体要求如下：
——单个策略可以对特定服务及调用方进行策略控制；
——全局策略可以对每个服务进行基础限制。

5.2.1.2 流量控制策略管理

通过设置流量控制策略，可以对服务访问流量进行主动控制。流量控制策略包括瞬时流控、单日请求次数限制、请求总次数限制，具体要求如下：

——瞬时流量控制。支持设置瞬时控制时间及瞬时请求限额，服务访问时，当时间范围内的请求次数达到瞬时请求限额时，服务网关实施服务限制，即控制时间范围内的服务不可访问；

——单日请求次数限制。支持设置单日请求上限，达到上限后，当日内服务不可访问；

——请求总次数限制。支持设置请求总次数限制，达到上限后，服务不再支持访问。

5.2.1.3 数据量控制策略管理

通过设置数据量控制策略，可以对服务返回数据记录条数大小的请求进行控制。数据量控制策略包括数据查询单日量及总量限额、数据下载单日量及总量限额，具体要求如下：

——数据查询量达到限额时，服务网关应对查询服务进行当日或永久访问限制；

——数据下载量达到限额时，服务网关应对下载服务进行当日或永久访问限制。

5.2.1.4 服务授权策略管理

当服务订阅申请通过审批后，应生成服务授权策略，具体要求如下：

——应支持针对用户和应用进行授权；

——在用户或应用进行服务请求时，服务网关应使用服务授权策略进行鉴权。

5.2.1.5 白名单管理

白名单分为用户白名单和应用白名单，具体要求如下：

——应支持对白名单进行增删改查；

——白名单用户无需进行服务使用授权申请，可调用任意服务；

——白名单应用无需进行服务使用授权申请，可直接调用服务。

5.2.2 网关服务

5.2.2.1 路由转发

服务网关应支持接收服务访问请求，并根据服务访问地址和转发规则，自动对请求的服务进行转发。

5.2.2.2 服务鉴权

为保障服务请求安全性，应支持对不同维度的服务使用请求进行鉴权，包括用户鉴权与应用鉴权，具体要求如下：

——用户鉴权：服务访问时，服务网关根据服务请求的用户信息获得服务授权策略，基于授权策略进行鉴权，鉴权通过的请求可正常访问，鉴权失败的请求拒绝访问；

——应用鉴权：服务访问时，服务网关根据服务请求的应用信息获得服务授权策略，基于授权策略进行鉴权，鉴权通过的请求可正常访问，鉴权失败的请求拒绝访问。

5.2.2.3 服务限流

为保证服务请求量可控，服务网关应支持对服务请求执行限流。服务网关接收到服务请求后，根据策略管理中的各类策略进行策略验证，当达到策略管理中的限额参数时，对服务进行访问限制，如时间范围内限制访问、永久限制访问等。

5.2.2.4 统计日志

服务网关应对所有转发的服务请求记录服务历史调用日志。历史调用日志信息包括但不限于请求方信息、服务请求信息、请求转发信息、服务响应信息等，具体要求如下：

——请求方信息记录服务请求发起方的各类信息，包括但不限于请求 IP、用户信息、应用信息等；

——服务请求信息记录具体的服务请求参数，包括但不限于请求头、请求体、请求服务名称、URL、请求时间等；

——请求转发信息记录服务网关转发的情况，包括但不限于转发耗时、转发状态、失败原因等；

——服务响应信息记录服务响应请求的情况，包括但不限于响应状态、响应参数、返回结果、响应数据量、服务提供者等。

5.3 服务运营层

5.3.1 服务订阅

服务运营层支持服务需求申请、服务订阅申请、服务订阅管理等功能，具体要求如下：

——应支持在线发起服务需求申请，服务需求申请信息包括但不限于需求名称、需求描述、服务名称、服务描述等内容；

——应支持在线发起服务订阅申请，服务订阅申请信息包括但不限于服务名称、服务使用期限、服务使用人、服务调用应用、申请信息、使用限额等；

——应支持对已订阅服务进行查询、详情查看、续期、退订等管理操作，具体要求如下：

- 对于服务使用期限已过期的服务支持发起使用期限调整申请；
- 对于已申请的服务支持退订。

5.3.2 服务运营统计

服务运营统计提供完整的运营指标统计，通过多个维度的量化指标，对服务总体情况、服务使用情况、服务性能、服务稳定性、服务安全性等多维度进行统计展示，具体要求如下：

——服务总体情况统计，包括按时间统计服务注册数量、按服务分类统计服务数量及占比、按服务需求来源统计服务数量分布等维度；

——服务使用情况统计，包括按时间统计服务请求次数、按请求方组织机构统计分布比例、按服务请求统计访问量及占比热度排行、按服务及时间统计各类数据访问请求次数与数据返回量等维度；

——服务性能统计，包括服务超时响应总次数、超时响应服务请求占比、月平均服务超时响应次数、按时间维度及服务维度统计的平均响应次数、超时响应的请求次数、平均请求响应时间、超时请求响应次数等维度；

——服务稳定性统计，包括但按服务统计无故障运行时长、前三次累计服务故障持续时间、按时间统计服务故障次数排行、服务出现故障的总恢复和时间及平均恢复时间等维度；

——服务安全性统计，包括按时间统计服务授权及未授权请求的次数、按请求部门统计发起未授权请求次数、按时间统计等维度。

5.3.3 服务评价

5.3.3.1 服务评价是对服务价值的评估与反馈，评价管理具体要求如下：

——支持系统自动评价和使用人主观评价两种机制，根据主观评分和系统评分计算服务总评分；

——支持通过评价详情展示服务价值的具体评价情况，包括总分值、主观评分、系统评分以及主观评论等。

5.3.3.2 指标管理是对服务质量各项特性的评价指标进行管理，包括指标定义、评分规则设置、指标启停等，具体要求如下：

——支持对评价指标进行定义，包括但不限于可用性、安全性、可靠性、响应性等；

——支持对评分规则进行设置；

——支持对评价指标进行管理，包括评价指标停用和启用。

6 安全要求

6.1 基础设施安全

6.1.1 应建立资源隔离机制，保证计算、存储、网络资源的租户级隔离，防止非授权访问或资源抢占。

6.1.2 启用硬件级可信执行环境处理敏感数据，内存中数据不应被外部进程窃取。

6.1.3 采用加密传输协议保障节点间通信安全，不应明文传输认证信息或业务数据。

6.2 数据安全

6.2.1 验证数据源合法性，应对第三方数据提供方实施安全审计。
6.2.2 宜部署数据脱敏代理，在采集端对身份证号、手机号等敏感字段进行实时掩码或哈希处理。
6.2.3 应使用国密等强加密算法对静态数据加密，密钥由硬件加密机统一管理。
6.2.4 基于数据分类分级实施差异化访问控制，高敏感数据应允许经审批的安全沙箱环境访问。
6.2.5 应记录数据操作审计日志，包括访问者、操作类型、数据范围及时间戳，日志保留期≥180 天。
6.2.6 宜采用隐私计算技术（联邦学习、多方安全计算）进行跨域数据融合分析，避免原始数据出境。

6.3 模型安全

6.3.1 应通过代码扫描工具检测训练代码中的安全漏洞（如命令注入、路径遍历）。
6.3.2 在训练前对数据集进行投毒攻击检测，应识别异常样本注入风险。
6.3.3 验证模型文件的数字签名，模型完整性应未被破坏。
6.3.4 可部署模型水印技术，防止模型被非法复制或分发。
6.3.5 建立模型行为基线，应对输入数据分布偏移、对抗样本攻击进行实时告警。
6.3.6 宜定期进行模型反演攻击测试，评估成员推理攻击导致的数据泄露风险。

6.4 开发运营安全

6.4.1 在构建环节集成软件成分分析工具，应识别开源组件漏洞及许可证风险。
6.4.2 宜采用基础设施即代码安全扫描，禁止部署存在高危配置的云资源。
6.4.3 遵循最小权限原则，平台管理员、数据科学家、运维人员角色权限应分离。
6.4.4 可实施动态令牌认证，会话空闲超时时间应≤15 min。

6.5 安全运维

6.5.1 建立平台安全配置基线，应定期核查防火墙策略、端口开放状态及补丁更新情况。
6.5.2 宜部署驱动的异常行为分析系统，实时检测横向移动、暴力破解等攻击模式。
6.5.3 可制定数据泄露应急预案，并在半年内至少执行 1 次实战化攻防演练。

7 维护要求

7.1 日常维护

7.1.1 建立 7×24 h 自动化监控体系，应覆盖平台可用性、资源利用率、安全事件三要素。
7.1.2 宜部署异常检测引擎，主动识别流量突变、错误率飙升等隐形故障。
7.1.3 执行变更审批流程，基础设施、模型版本、关键配置的变更应经安全评估并留存回滚方案。
7.1.4 可实施蓝绿部署或金丝雀发布，业务更新期间服务应具有连续性。

7.2 故障响应

7.2.1 应制定分级应急预案，数据恢复 RTO≤2 h、RPO≤5 min。
7.2.2 建立跨部门应急协同机制，开发、运维、安全团队应定期开展断网演练或数据恢复演练。
7.2.3 可配置自动化熔断策略，当检测到大规模数据泄露或受到攻击时自动隔离受影响节点。

7.3 补丁管理

7.3.1 每季度核查安全配置基线，应包括操作系统内核参数、容器镜像漏洞、数据库权限清单。
7.3.2 宜采用基础设施即代码模板化管理配置，禁止生产环境手动修改。
7.3.3 建立漏洞闭环流程，高危漏洞应在 48 h 内修复或制定缓解措施。
7.3.4 可启用自动化补丁分发系统，非中断性补丁安装窗口应控制在业务低峰期。

7.4 数据维护

7.4.1 定期验证备份数据可恢复性，全量备份频率应≥1 次/周，增量备份频率应≥1 次/天。
7.4.2 实施数据生命周期自动化管理，应对超期暂存数据执行安全擦除。
7.4.3 应监控模型性能衰减，当预测准确率下降超过阈值时触发再训练流程。
7.4.4 可建立模型版本仓库，保留历史版本及训练数据集快照以备溯源审计。

7.5 运维能力保障

7.5.1 运维团队应持有安全认证比例≥80%，每年接受不低于 16 学时专项培训。
7.5.2 宜配置专职安全工程师，负责模型对抗防御、隐私泄露风险评估等专项工作。
7.5.3 应维护实时更新的运维知识库，含拓扑图、应急预案、故障排查手册等关键文档。
7.5.4 建立运维操作视频审计机制，高危操作应双人复核。