ICS 35.210
CCS L70

团　　体　　标　　准

T/ISC 0094—2025

基于大模型的智能体应用场景能力要求

Requirements of artificial intelligent agent application scenarios based on large scale model

（发布稿）

2025－12－26 发布　　2026－01－26 实施

中 国 互 联 网 协 会　　发 布

目　　次

前　　言 III
基于大模型的智能体应用场景能力要求 1
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
3.1 智能体 ai agent 1
3.2 大模型 large-scale model 1
3.3 强化学习 reinforcement learning 1
3.4 自然语言理解 natural language understanding 2
3.5 自然语言处理 natural language processing 2
3.6 自然语言生成 natural language generation 2
3.7 提示词 prompt 2
4 符号和缩略语 2
5 能力概述 3
6 模型接管层 3
7 核心能力层 3
7.1 知识接入 3
7.2 任务规划 4
7.3 任务执行 4
7.4 工具插件 4
7.5 记忆能力 4
7.6 学习能力 4
7.7 通信协议（可选） 5
8 认知交互层 5
8.1 对话能力 5
8.2 理解能力 5
8.3 生成能力 5
8.4 推理能力 5
9 应用场景层 6
9.1 知识智能体 6
9.2 分析智能体 6
9.3 风控智能体 6
9.4 客服智能体 7
9.5 营销智能体（消费侧） 7
9.6 营销智能体（企业侧） 7
9.7 办公智能体 8
9.8 财务智能体 8

9.9 人力智能体 8
9.10 研运智能体 8
10 安全服务层 9
10.1 服务能力 9
10.2 安全能力 9

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。

本文件由中国互联网协会提出并归口。

本文件起草单位：中国信息通信研究院、吉利汽车集团有限公司、天翼云科技有限公司、中移信息技术有限公司、中国移动集团有限公司、中国联合网络通信有限公司软件研究院、联通数字科技有限公司、中国第一汽车集团有限公司、中国电信集团有限公司、中国移动通讯集团浙江有限公司、中国移动通信集团江苏有限公司、中电信数智科技有限公司、北京搜狐新媒体信息技术有限公司、广州趣丸网络科技有限公司、北京车之家信息技术有限公司。

本文件主要起草人：徐恩庆、刘思颖、崔晨星、胡炜航、罗欧、刘昊、郑少斌、王爱娇、张巍、张瑞、张宝鑫、李文伟、郭艺娟、古英杰、张迪、马景耀、谭俊、陈子锋、卢辰、蔡丹丹、张晓京、杨德智、叶剑、赵新、仝飞、冼宜亮、高翔、吴健、陈韵、蒋汉卿、魏旭、奚天奇、武沛多、杨华锋、刘威辰、王栋、傅成彦、周琪山、余涛、李睿、杨林、殷娇、王上淇、杨经纬、尚啸、陈利明、邢驰、郭洪文、任少峰、杨玉涛。

基于大模型的智能体应用场景能力要求

1 范围

本文件规定了基于大模型的智能体应用场景能力要求，包括模型接管层、核心能力层、认知交互层、应用场景层、安全服务层等方面内容。

本文件适用于指导企业级用户规划实施并运维运营基于大模型的智能体应用使用，以及指导服务提供方设计、研发此类产品，也可作为第三方测评机构评估使用。

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。

[1] GB/T 41867-2022 信息技术 人工智能 术语

[2] GB/T 5271.28-2023 信息技术词汇 第28部分：人工智能

[3] GB/T 45288.1—2025 人工智能 大模型 第1部分：通用要求

3 术语和定义

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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。

3.1

智能体 ai agent

是一种能够感知其环境，并自主采取行动以实现特定目标的实体。

注：智能体通过感知、认知、规划、记忆和执行等内部能力，并运用学习、推理等方法，表现出适应环境的自主性与智能性。

3.2

大模型 large-scale model

大规模深度学习模型 large-scale deep learning model

基于大量数据训练得到，具有复杂计算架构，能处理复杂任务，且具备一定泛化性的深度学习模型。

注：参数量规模达到行业公认的大型模型标准，通常指参数量达到亿级或以上的深度学习模型。大模型训练使用的数据总量受参数量的影响，达到收敛的大模型的参数量的对数与其训练数据总量的对数成正比。

[来源：GB/T 45288.1—2025，3.1]

3.3

强化学习 reinforcement learning

一种通过与环节交互，学习最佳行动序列，使回报最大化的机器学习方法。

[来源：GB/T 41867—2022，3.2.25]

3.4

自然语言理解 natural language understanding

通过对功能单元从已传入的功能单元中的自然语言形式的文本或语音中的提取信息,并产生对给定文本或语音及其表示的描述。

[来源：GB/T 5271.28-2023，28.01.18]

3.5

自然语言处理 natural language processing

（系统）基于自然语言理解和自然语言生成的信息处理。

[来源：GB/T 41867-2022，3.3.16]

3.6

自然语言生成 natural language generation

将带有语义的数据转换为自然语言的任务。

[来源：GB/T 41867-2022，3.3.17]

3.7

提示词 prompt

提示语

使用大模型进行微调或下游任务处理时,插入到输入样本中的指令或信息对象。

[来源：GB/T 45288.1—2025，3.5]

4 符号和缩略语

下列符号和缩略语适用于本文件。

A2A：智能体对智能体协议（Agent-to-Agent）

ANP：智能体网络协议（Agent Network Protocol）

API：应用程序接口（Application Programming Interface ）

ASR：自动语音识别（Automatic Speech Recognition）

CRM：客户关系管理（Customer Relationship Management）

IVR：交互式话音应答（Interactive Voice Response）

MCP: 模型上下文协议（Model Context Protocol）

NLP：自然语言处理（Natural Language Processing）

OA：办公自动化（Office Automation

OCR：光学字符识别（Optical Character Recognition）

RBAC：基于角色的访问控制（Role-Based Access Control）

SDK：软件开发工具包（Software Development Kit）

TTS：语音合成（Text To Speech）

URL：统一资源定位符（Uniform Resource Locator）

5 能力概述

基于大模型的智能体应用场景能力要求包括模型接入和管理能力，以及知识接入、任务规划、任务执行、工具插件等核心能力层能力，以及对话能力、理解能力、生成能力、推理能力等认知交互层能力，以及多种智能体应用场景如知识智能体、分析智能体、营销智能体、客服智能体、财务智能体等，以及安全服务层等方面能力，参考架构如图1所示。

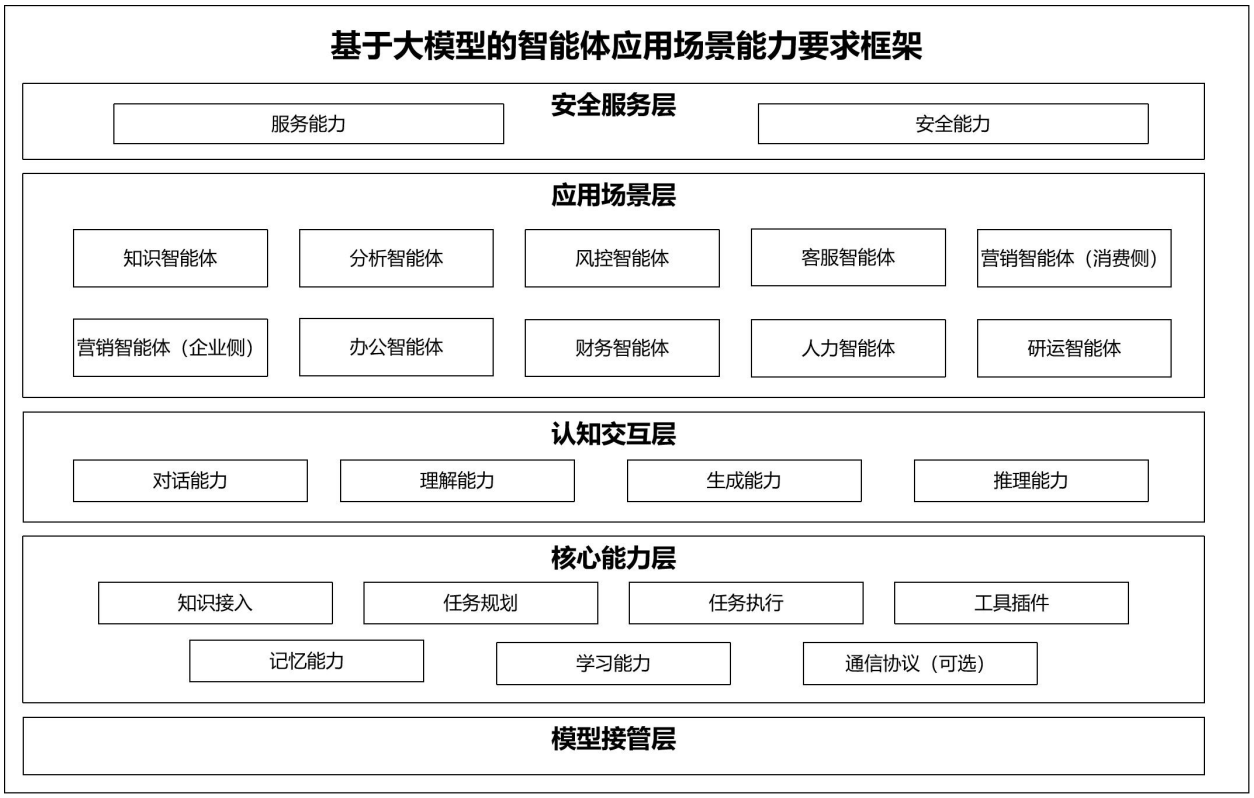

图 1 基于大模型的智能体应用场景能力要求框架

6 模型接管层

a) 应支持主流大模型的统一接入，允许通过配置界面实现模型选择、版本切换及参数调整；
b) 应支持基于应用场景的智能模型路由，能够结合环境感知、输入特征及模型能力动态选择最优模型；
c) 宜支持接入模型具备工具调用与思维链推理能力；

7 核心能力层

7.1 知识接入

a) 应具备多源异构知识统一接入能力，包括SQL/NoSQL数据库、RDF/OWL知识图谱、WORD/PDF/HTML/Markdown文档库及API服务等数据并行接入；
b) 应支持知识库全生命周期管理能力，包括知识的自动整理、更新、搜索、删除及版本管理等；
c) 应具备可扩展知识分类标签体系，支持依据预设标签对接入知识进行自动识别与归类；

d) 宜支持知识图谱技术的应用，支持对碎片化实体及其关系进行自动抽取、融合，并生成可视化知识网络呈现关联结构；
e) 宜提供多模态知识向量化服务，通过嵌入模型将文本、图像等映射至统一语义向量空间，并兼容主流向量数据库；

7.2 任务规划

a) 应具备任务理解能力，支持对用户输入任务目标的意图及关键信息准确识别；
b) 应具备任务分解能力，支持将复杂任务拆解为多个目标明确、步骤清晰的子任务；
c) 应具备路径规划能力，支持基于可配置参数将复杂任务生成最优原子操作序列；
d) 宜具备动态调整能力，支持依据实时数据与业务变化自适应调整已规划的任务路径；
e) 宜具备任务优先级评估能力，支持按紧急度、重要性等因素对任务进行优先级排序；

7.3 任务执行

a) 应具备任务执行能力，支持依据规划结果自主完成数据处理、文件操作、系统指令及网络请求等操作；
b) 应具备人机协作能力，支持任务执行过程中人工干预，包括补充任务数据、修改任务内容或打断任务进程等；
c) 宜具备跨系统协同能力，支持通过动态适配异构API接口与常规协议，实现与其他系统或智能体的任务级联与数据互通；
d) 宜具备状态监控能力，支持可视化实时展示任务进度、任务状态、资源占用及异常告警情况等；
e) 宜具备任务执行可解释性能力，对关键决策提供依据说明，引用外部知识时标注来源，有效抑制模型幻觉；

7.4 工具插件

a) 应支持调用AI工具，包括NLP（自然语言处理）、ASR（语音识别）、TTS（文本到语音）、图像识别、图片文字提取等常见AI工具组件即插即用；
b) 应支持调用信息增强插件、交互增强插件、服务增强插件等其他常见插件；
c) 应提供插件配置管理功能，支支持用户对插件进行新增、删除、查询及智能体分配操作；
d) 宜支持通过标准接口扩展工具能力，集成搜索引擎、数据库操作及自定义工具等；
e) 宜支持插件在线测试功能，支持对用户配置的工具进行即时调用验证并返回测试结果；

7.5 记忆能力

a) 应支持对历史交互记录的存储和检索功能，支持基于用户需求的关键信息快速定位与调用；
b) 应支持对情景信息的理解、记忆、查找能力，情景信息包括系统信息、用户画像、外部环境信息等智能体可感知的信息；
c) 宜支持短期记忆与长期记忆的分别加密存储，短期记忆宜覆盖最近10轮对话，长期记忆宜包括用户画像与偏好信息，并应支持用户自主删除；
d) 宜支持记忆有效期设置功能，具备自动清理过期对话痕迹的能力，以避免信息冗余和过时；
e) 宜支持记忆总结和提炼，基于用户特征生成个性化对话风格与内容；

7.6 学习能力

a) 应支持基于用户交互与任务执行数据，通过机器学习算法实现模型持续优化，提升语言理解、任务处理能力，并确保数据处理与模型输出符合数据安全及合规性要求；

b) 应支持用户反馈机制，能够根据用户对任务执行结果的评价（如满意、不满意、改进建议等），对自身行为和策略进行调整和优化；

7.7 通信协议（可选）

a) 宜兼容MCP协议，支持与符合该协议的MCP服务器进行通信；
b) 宜兼容A2A协议，支持与符合该协议的其他智能体进行通信；
c) 宜兼容ANP协议，支持与符合该协议的智能体进行通信；

8 认知交互层

8.1 对话能力

a) 应支持任务式对话、问答式对话及工具调用对话等多种对话类型，并实现各形态对话间的无缝切换；
b) 应具备智能问答能力，能够基于自然语言处理技术及知识库，精准理解用户问题并输出准确、简洁的答案；
c) 应支持单轮对话、多轮对话能力，在多轮对话中能够有效利用历史交互信息，保障对话的连贯性与逻辑性；
d) 宜支持会话状态的持久化与跨设备同步，并具备自动生成对话摘要的能力；
e) 宜支持上下文感知的问题推荐功能，能够基于当前问题或历史交互记录，自动生成多个候选扩展问题；
f) 宜支持意图澄清机制，在识别到用户意图模糊或信息不完整时，能够通过结构化提问主动明确用户需求；

8.2 理解能力

a) 应支持准确理解自然语言输入的意图和内容，包括语义理解、语法分析与意图识别，并支持对复杂对话场景及领域特定语言的解析；
b) 应支持对多轮对话中上下文信息的理解与利用，能够依据上下文语境进行智能推理，并生成连贯、准确的回应；

8.3 生成能力

a) 应支持文本生成能力，依据上下文主题、风格与字数约束等条件，生成输出符合场景需求的文本内容；
b) 宜支持代码生成能力，依据代码插件工具，可根据规划任务要求自动编写、调试并执行代码，完成执行类任务；
c) 宜支持图像生成能力，通过提示词驱动多模态模型，生成输出指定分辨率、风格与元素的合规图像；
d) 宜支持音视频生成能力，基于提示词与脚本模板，实时合成高清音视频，支持语音克隆、字幕同步等；

8.4 推理能力

a) 应支持基于知识推理，能够利用预定义的事实、规则、概念等，结合用户意图生成兼顾预期与知识参考的回复，以降低内容幻觉风险；

b) 应支持基于对话推理，能够利用预定义的事实、规则、概念等，结合用户意图生成兼顾预期与知识参考的回复，以降低内容幻觉风险；
c) 应支持基于数学逻辑计算推理，能够运用代数、几何、概率论等数学方法解决数学问题或验证逻辑命题；
d) 宜支持基于因果推理，通过分析因果关系进行推理，以预测事件的结果或推断事件的原因能力；
e) 宜支持基于深度推理，通过多步推理和复杂逻辑分析，解决复杂问题或理解复杂概念能力；

9 应用场景层

9.1 知识智能体

a) 应具备知识语义检索能力，支持对用户自然语言查询进行深层语义解析，并基于向量相似度计算实现语义匹配，可通过知识卡片、知识结构化及知识溯源等形式输出结果；
b) 应具备知识图谱检索能力，支持基于知识图谱的“实体-关系-属性”三元组结构，实现多维度、可推理的智能检索；
c) 应具备知识问答能力，支持基于对用户输入进行深度语义解析与检索，能够生成内容清晰、逻辑合理且标明引用出处的知识回复；
d) 应具备知识推荐能力，支持面向用户的个性化知识推荐能力，能够结合用户的行为、兴趣、意图及业务上下文动态调整推荐内容，优先推荐权威来源、最新内容、用户常用领域等；
e) 应支持知识问答的引用与溯源，提供一键访问源文档或片段级引用标识的能力，确保知识来源的可追溯性；
f) 宜具备知识混合检索能力，能够根据查询特征自动选择或组合语义、图谱与结构化检索方式，实现多策略融合的智能检索与结果召回；
g) 宜具备多模态知识检索能力，具备对文本、图像、音频、视频等信息的统一特征提取与跨模态语义关联能力，实现以文搜图、以图搜文等联合检索与多模态内容生成支持；

9.2 分析智能体

a) 应具备数据查询能力，支持自然语言问答交互方式提供业务数据查询、常见业务指标计算、数据异常检测等服务；
b) 应具备数据分析能力，针对多维度数据进行统计分析，能够快速解读数据特征和分布，智能生成可视化图表（如折线图、饼图、漏斗图），支持交互式上卷下钻分析；
c) 宜具备波动归因分析能力，能够基于关键指标历史趋势，结合知识库与外部数据，关联业务事件（如促销活动、系统故障），对指标波动原因进行拆解与归因；
d) 宜具备决策能力，支持根据业务场景需求（如经营分析、运营复盘），对业务关键指标进行趋势预测，智能生成决策建议与分析报告，支持多格式文档导出或链接形式分享；

9.3 风控智能体

a) 应具备合规审查能力，基于内外部合规知识库，对营销宣传、公示公告、制度协议等内容进行智能审核，识别不合规项并提供法规依据与整改建议；
b) 应具备内部操作审计能力，实时解析员工操作日志、权限变更、敏感数据访问等行为，识别越权、异常批量操作等内部威胁，生成可追溯的审计报告；
c) 应具备合规风险预测能力，基于历史处罚案例、监管动态、业务变更等数据，构建合规风险预测模型，构建风险预测模型，输出潜在违规场景及概率；

d) 宜具备交易风险实时监测能力，实时采集交易流水、账户行为、地理位置等多维数据，利用异常检测算法对欺诈、洗钱等高风险交易进行预警，并输出风险等级与处置建议；
e) 宜具备舆情分析能力，通过对内外部数据进行分析与抓取，识别企业相关的舆情信息，辅助企业掌握舆情动态；

9.4 客服智能体

a) 应具备多渠道接入与同步能力，支持多渠道接入包括企业微信、网页聊天窗口、电话IVR等，并实现对话内容的跨渠道状态同步；
b) 应具备客服咨询响应能力，支持基于自然语言理解与自然语言生成能力，实现对用户咨询的实时解析与响应，支持答案来源标注及多轮对话上下文跟踪，并可主动引导客户补充信息以精准理解需求；
c) 应具备情感识别与交互能力，支持语音与文本双向情感分析（如语调强度、关键词频率等），能够自动识别客户情绪，基于问题分类生成结构化安抚话术库，并智能匹配解决方案；
d) 应具备智能工单处理能力，支持从对话中自动提取工单关键信息，包括客户ID、问题类型、紧急程度等，并完成工单分派并生成全链路审计日志；
e) 宜具备智能质检能力，支持语音/文字质检多维度指标分析（如关键词出现频率、对话完整性等），提供可视化分析及问题归因功能，并支持服务评价与智能反馈生成；
f) 宜具备智能外呼能力，支持按预设规则自动发起外呼，实现语音识别与合成交互，能够基于客户历史行为预测潜在需求，动态优化外呼策略以提升接通率与转化成功率；

9.5 营销智能体（消费侧）

a) 应具备智能客户洞察能力，支持整合多源数据（如CRM系统数据、社交媒体交互数据等）构建360度用户画像，并基于动态聚类分析实现用户群体的划分与标签映射；
b) 应具备智能精准营销能力，支持通过多维度分析（如协同过滤算法、用户偏好预测模型等）生成产品/服务推荐与营销话术，实现官网内容智能排序与个性化分发；
c) 宜具备AI外呼与自动化触达能力，支持通过语音、短信等方式实现批量外呼，具备客户意图自动识别、外呼数据全量记录与效果可视化分析功能；
d) 宜具备营销效果追踪能力，支持对营销活动全流程核心指标进行监测统计与可视化展示，能够通过A/B测试对比不同营销策略的实施效果，并基于数据分析结果生成优化建议报告；
e) 宜具备智能营销培训能力，支持对客户经理进行多维度能力评价，提供模拟客户场景的对话演练环境，能够对客户经理的回复内容进行规范性、准确性和完整性评估；

9.6 营销智能体（企业侧）

a) 应具备行业趋势研判能力，支持自动化采集行业相关数据，构建行业景气度评估模型，生成景气指数曲线与周期预测图表，辅助判断行业周期阶段与发展趋势；
b) 应具备企业侧智能客户洞察能力，支持基于客户基本信息、采购及账务等数据进行分析，实现实现客户分级分类、价值分层与风险预警，识别潜在拓客机会；
c) 应具备智能营销商机推荐能力，支持通过大模型分析业务场景，提供个性化与场景化的线索及商机建议，包括历史相似商机与上下游关联商机推荐；
d) 宜具备智能营销策略生成能力，能够识别营销意图与诉求，基于输入背景与客户画像自动生成逻辑清晰的营销方案，内容涵盖公司介绍、行业分析、解决方案及相关案例；
e) 宜具备智能标书与合同能力，支持招投标文件解析与标书内容自动生成，可对投标文件进行智能检查与风险识别，并支持合同内容的生成与审核；

9.7 办公智能体

a) 应具备会议安排能力，支持自动协调参会时间、发送会议通知、生成会议纪要，并可将任务同步至OA系统或邮件等第三方平台；
b) 应具备邮件处理能力，支持邮件自动分类、关键信息提取、智能回复建议生成，并可将待办任务提交至工作通知列表；
c) 应具备文档管理能力，支持标准文档模板调用与自动生成、内容摘要提取与关键信息抽取，并提供关键词与语义检索功能；
d) 应具备员工问答助手能力，可基于企业知识库为公司制度、业务流程、合规要求等内容提供准确解答；

9.8 财务智能体

a) 应具备智能差旅报销能力，支持端到端差旅闭环管理，包括一键发起申请、智能差旅校验、自动比价订票、自动生成报销单、差旅成本可视化分析等；
b) 应具备智能发票识别能力，支持多票种OCR字段提取，可自动完成发票验真、查重与价税分离，并对异常票据进行实时预警；
c) 宜具备财报分析能力，可根据总账数据一键生成资产负债表、利润表、现金流量表及附注等财务报表，实现多维度钻取分析，对应收逾期、费用超标等风险进行识别并输出处置建议；
d) 宜具备资金预测能力，基于历史现金流、合同收付款计划、预算执行进度，滚动预测未来周资金缺口与盈余，自动生成融资或理财建议；
e) 宜具备税务管理能力，支持一键算税、自动申报、税负对标、优惠政策推送及留抵退税模拟测算等功能，确保税务合规与税负优化；

9.9 人力智能体

a) 应具备智能简历筛选能力，支持多格式简历批量解析与关键信息提取，实现简历画像与岗位需求的自动匹配；
b) 应具备智能面试安排能力，支持面试时间自动协调、多模态面试反馈整理及面试结果自动汇总；
c) 宜支持员工培训管理，能够基于岗位要求与绩效数据生成个性化学习路径，并提供情景化培训与效果追踪；
d) 宜具备组织洞察能力，支持人才盘点、继任梯队分析与离职预测，并生成可视化人力分析看板；

9.10 研运智能体

a) 应具备故障诊断能力，支持通过日志聚类与故障知识图谱定位异常根因，可基于历史解决方案或运维大模型匹配并执行修复操作；
b) 应具备环境变更管理能力，支持系统变更预检查、自动化测试上线、SQL稽核与风险评估，以及基础设施与应用服务的统一巡检；
c) 应具备代码辅助开发能力，支持根据自然语言描述生成Python、Java、SQL等语言的函数级代码；
d) 宜支持代码审查，具备静态代码分析与动态安全漏洞扫描能力，可检测代码缺陷与安全风险；
e) 宜具备系统性能优化能力，能够基于应用性能监控数据生成性能分析报告，并提供智能调参建议；

10 安全服务层

10.1 服务能力

a) 应支持将智能体能力以API、SDK等形式对外发布；
b) 应支持将智能体以浏览器插件形式对外发布；
c) 应支持将智能体以URL（网络链接）的方式对外发布；
d) 宜支持发布到第三方平台，如微信、抖音、飞书等开放平台；

10.2 安全能力

a) 应支持基于角色的访问控制（RBAC），能够根据业务需求定义角色权限并实现动态调整；
b) 应采用加密技术对存储与传输中的数据进行保护，防止未经授权的访问与泄露；
c) 应具备提示词注入与数据外泄的检测与防御能力，有效识别并阻断对抗性攻击；
d) 应支持确保个人身份信息和其他敏感数据全生命周期的安全处理，符合相关法律法规要求；
e) 应支持定期安全漏洞扫描与及时修复，有效防范潜在安全威胁；
f) 应具备安全审计追踪能力，完整记录智能体调用、配置变更、权限调整等关键操作日志；
g) 应支持内容安全治理，通过多级审核、权威验证与伦理审查确保生成内容的准确性、无偏见性与合规性。