ICS 33.030
CCS M21

团　　体　　标　　准

T/CCSA 737—2025 （T/CAAAD 039—2025）

人工智能营销客服平台能力要求

Requirements for artificial intelligence marketing customer service platform

2025-12-01 发布　　2026-03-01 实施

中 国 广 告 协 会
中国通信标准化协会　　发 布

版权声明

邮箱：IPR@ccsa.org.cn　　digitalad@china-caa.org
电话：010-62302847　　010-65924878

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》的规定内容起草。

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。

本文件由中国通信标准化协会和中国广告协会共同提出并归口。

本文件起草单位：科大讯飞股份有限公司、中国信息通信研究院、华为技术有限公司、字节跳动有限公司、阿里巴巴集团控股有限公司、秒针信息技术有限公司。

本文件主要起草人：胡成春、冯庭好、朱岩、张亚兰、赵乃萱、胡俊英、胡春磊。

引　言

当前，人工智能技术在营销领域的应用日益广泛，特别是在客服平台的智能化发展方面，人工智能技术正发挥着不可或缺的作用。然而，随着客户交互方式的多样化与复杂化，现有的客服平台在能力要求上面临着诸多挑战。一方面，智能客服需要处理来自多渠道的数据，如文本、语音、视频等，要求平台具备强大的数据处理与分析能力；另一方面，客户体验的提升对智能客服的响应速度与准确性提出了更高的要求。此外，随着《中华人民共和国个人信息保护法》的实施，平台在数据安全与隐私保护方面也应严格遵循相关法律法规。

在智能客服平台的发展中，营销能力的强化不仅是技术进步的体现，更是助力企业实现商业目标的重要途径。作为客户互动的重要节点，智能客服平台已不再局限于被动响应需求，而是逐渐演变为精准营销的重要触点。通过深度学习算法、自然语言处理技术及数据挖掘能力的结合，客服平台能够洞察客户行为偏好，智能化推荐个性化服务与产品，实现从“服务”到“营销”的无缝衔接。同时，基于大数据分析的营销能力还能够帮助企业优化资源配置，提升客户生命周期价值。在竞争日益激烈的市场环境下，具备强大营销能力的智能客服平台，将成为企业在拓展客户关系、促进销售转化以及提升品牌忠诚度方面的重要支撑。

因此，有必要制定一个既符合国家数据安全与个人信息保护要求，又能满足不同行业和业务需求的《人工智能营销客服平台能力要求》标准。本标准旨在定义智能客服平台的能力架构、功能要求、接口规范以及安全要求。通过制定统一的能力要求，规范企业在智能客服平台的建设与运维中遵循标准化的流程，降低开发与维护成本，提升平台的整体服务水平与客户体验。

人工智能营销客服平台能力要求

1 范围

本文件规定了人工智能营销客服平台的能力架构、功能要求、接口规范以及安全要求。

本文件适用于面向企业客户的以人工智能能力为核心的营销客服平台，其他类型的智能客服系统亦可参考本文件。

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 45438—2025 网络安全技术人工智能生成合成内容标识方法

3 术语和定义

下列术语和定义适用于本文件。

3.1

人工智能营销客服平台 AI marketing customer service platform

人工智能营销客服平台是基于人工智能技术，通过多种数据处理与分析方式，提供自动化、智能化的客户服务与营销支持的平台。该平台能够通过语音识别、自然语言处理、图像识别、视频识别等技术手段，实现客户的精准需求识别、自动化问题解答、个性化营销推送等功能，以提升客户体验和营销效果。

3.2

自然语言处理 natural language processing

自然语言处理是人工智能的一个分支，旨在使计算机能够理解、解释和生成人类语言。自然语言处理在人工智能营销客服平台中用于分析和处理客户输入的文本或语音信息，生成相应的智能响应，广泛应用于自动应答系统、聊天机器人和情感分析等功能模块中。

3.3

大语言模型 large language model

大语言模型是基于深度学习技术，经过大量文本数据训练后，具备理解、生成自然语言能力的人工智能模型。大语言模型能够处理复杂的语义任务，如文本生成、翻译、问答、对话等。在人工智能营销客服平台中，大语言模型用于生成高质量的客户服务响应，支持自然语言处理、内容生成、智能应答等功能模块的实现。

3.4

聊天机器人　chatbot

聊天机器人是人工智能客服平台中通过预设规则或学习算法与客户进行对话的虚拟客服系统。聊天机器人能够模拟人类客服与客户进行交互，处理常见问题，提供即时解答，并引导客户完成特定任务。

3.5

个性化推荐　personalized recommendation

个性化推荐是基于客户的历史行为数据、偏好以及实时交互信息，通过人工智能算法为客户提供定制化产品、服务或内容的技术。在人工智能营销客服平台中，个性化推荐功能可用于精准推送适合客户需求的营销信息和解决方案，提升客户的满意度和转化率。

3.6

数据库　database

数据库是指用于组织、存储和管理数据的集合，可高效地执行数据的增删改查操作。在人工智能营销客服平台中，数据库用于存储与管理客户信息、交互记录、营销数据等关键业务数据。常见的数据库类型包括关系型数据库（如 MySQL、PostgreSQL 等）和非关系型数据库（如 MongoDB、Cassandra 等）。

3.7

向量数据库　vector database

向量数据库是一种专门用于存储、索引和检索高维向量数据的数据库。它支持对向量数据的快速相似性搜索，常用于处理自然语言处理、图像识别等需要高效查找相似特征的数据应用场景。在人工智能营销客服平台中，向量数据库可用于存储和检索嵌入表示（如文本、图像的向量表示），支持个性化推荐、语义搜索等功能的实现。

3.8

嵌入表示　embedding representation

嵌入表示是通过将高维数据（如文本、图像等）映射到低维向量空间中，以便机器能够更有效地处理和分析数据的表示形式。在人工智能营销客服平台中，嵌入表示用于表示客户输入的信息、产品特征等，以便在向量数据库中进行高效的相似性搜索和匹配。

3.9

联络中心　contact center

由传统呼叫中心演进而来，联络中心通过新技术的应用，使企业能通过如电话、短信、传真、视频、面对面、网络自动服务、电子邮件、聊天、交互式语音问答、语音机器人等多种渠道，提供多媒体客户接触服务。

4　缩略语

下列缩略语适用于本文件。

AI：人工智能（Artificial Intelligence）

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

DB：数据库（Database）

IVR：交互式语音应答（Interactive Voice Response）

IVVR：交互式视频应答（Interactive Voice and Video Response）

KG：知识图谱（Knowledge Graph）

LLM：大语言模型 （Large Language Model）

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

TTS：语音合成（Text to Speech）

VecDB：向量数据库 （Vector Database）

5 架构概述

5.1 平台技术架构

人工智能营销客服平台技术架构如图 1 所示，由基础设施层，平台能力层，平台应用层组成：

a） 基础设施层：负责组成系统网络资源、存储资源、计算资源及基础 AI 资源等；

b） 平台能力层：涵盖客服平台呼叫路由控制和媒体接入中心，负责接入语音和视频呼叫，并调度分配到后端的控制设备进行处理；

c） 平台应用层：提供自助服务及人工服务功能，并为业务开发者提供开发工具及统一的平台开放接口，包括但不限于知识库管理接口，软电话、IVR、IVVR、音视频、外呼、话务监控、管理及报表数据输出、路由调度等软件工具包和接口。

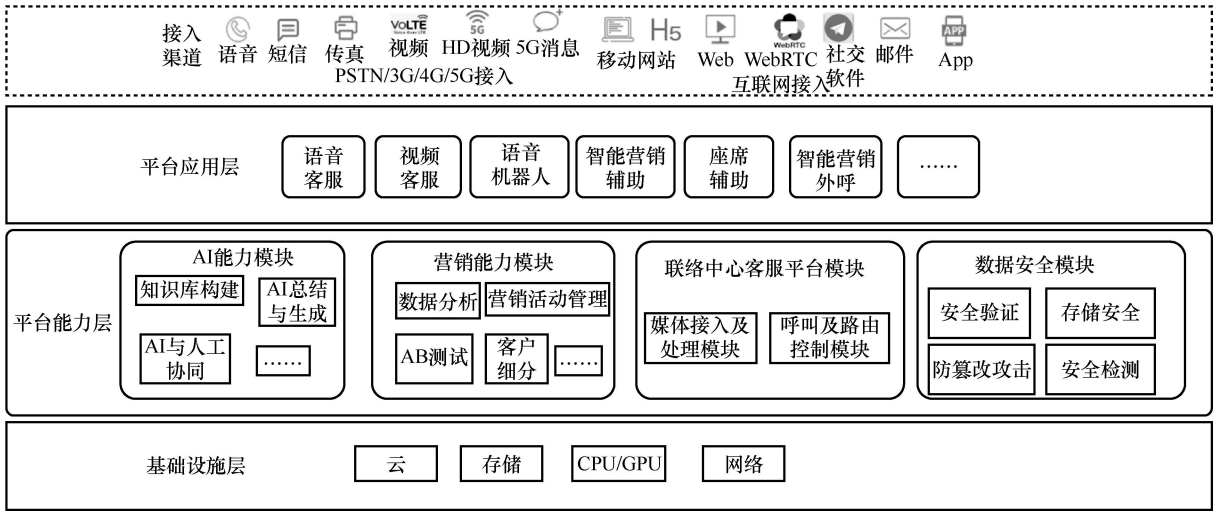

图 1 人工智能营销客服平台技术架构

5.2 服务流程

人工智能营销客服平台的总体业务流程如图 2 所示。

人工智能营销客服平台业务流程共涉及四个核心模块，包括离线知识库构建、客户请求预处理、知识库召回以及 AI 总结与生成。根据不同的功能和用途，这四个模块共同协作，构成了人工智能营销客服平台的智能化运行流程。

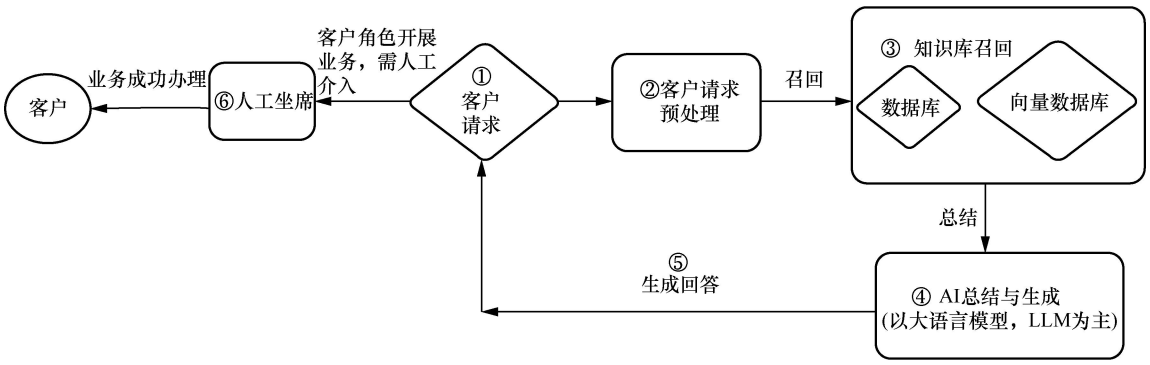

图 2　人工智能营销客服平台工作业务流程

5.2.1　离线知识库构建

该模块主要负责从各种数据源中收集和整理信息，生成涵盖产品、服务、常见问题等内容的离线知识库。知识库中的信息经过分类、分层处理，确保能够快速响应客户的多样化需求。

5.2.2　客户请求预处理

在客户发起请求后，系统首先对请求进行预处理，包括语音识别、文本解析、意图识别和情感分析等操作。通过对客户输入的标准化和语义分析，确保后续召回和生成模块能够准确理解并响应客户的需求。

5.2.3　知识库召回

在预处理后的客户请求基础上，系统通过检索和匹配技术，从离线知识库中快速召回与请求相关的内容。知识库召回模块通过优化的索引和搜索算法，确保能够高效找到最相关的答案或信息，供后续生成模块使用。

5.2.4　AI 总结与生成

该模块基于知识库召回的内容，结合 AI（主要是大语言模型，LLM，有些场景可能也会使用其他小模型）的能力，对客户请求进行总结与回答生成。AI 不仅可以生成准确的响应，还能够根据上下文信息提供扩展内容，确保客户得到详尽而精准的回答。

6　功能要求

6.1　智能平台功能要求

6.1.1　离线知识库构建功能要求

6.1.1.1　离线知识库的生成

离线知识库可在人工智能营销客服平台初始化时生成，并通过定期更新维护以确保内容的时效性。

知识库的内容应包括产品信息、常见问题解答（FAQ）、客户指南、行业知识等，并通过文本处理和分类算法进行整理与组织。

6.1.1.2 离线知识库的特性

离线知识库应具备以下特性：

a） 高覆盖性：知识库内容应覆盖客服可能涉及的所有话题与问题，确保全面性；

b） 准确性：知识库中的信息应经过审核和验证，确保提供给客户的内容准确无误；

c） 可扩展性：知识库结构应支持动态扩展，以便随着业务变化和客户需求增长，快速添加新内容；

d） 高速访问性：离线知识库应支持高效的检索与访问，以确保在客户请求时能够快速提供相关信息。

6.1.2 客户请求预处理功能要求

6.1.2.1 客户请求的解析

客户请求预处理模块在接收到客户请求后，应首先进行文本解析和清理，识别客户意图、提取关键词，并将请求格式化为标准化输入，便于后续处理环节的应用。

6.1.2.2 客户请求预处理的特性

客户请求预处理模块应具备以下特性：

a） 多样性：支持多种输入形式，包括文本、语音转文本等；

b） 实时性：能够实时解析客户请求，确保低时延处理；

c） 精确性：能够准确识别客户意图，减少误判和偏差；

d） 鲁棒性：对不完整或噪声信息具有较强的处理能力，能够从中提取有效信息。

6.1.3 知识库召回功能要求

6.1.3.1 知识库召回的执行

在客户请求预处理完成后，系统应根据解析结果在知识库中进行召回操作，检索与客户问题相关的条目，并将最相关的信息反馈给客户或交由 AI 进一步处理。

6.1.3.2 知识库召回的特性

知识库召回功能应具备以下特性：

a） 精准性：能够准确匹配客户问题与知识库中的相关条目，确保高相关性召回；

b） 效率性：在大规模知识库中高效检索，确保快速响应客户请求；

c） 多样性：支持不同类型的检索方法，如关键词匹配、语义搜索等，满足不同需求；

d） 可调优性：能够根据实际使用情况，通过调优算法提高召回结果的质量。

6.1.4 AI 总结与生成功能要求

6.1.4.1 AI 的生成能力

在知识库召回结果基础上，利用 AI 对复杂或多样化的客户请求进行总结与生成，通过深度学习模型生成个性化、自然语言化的响应内容，以提供更为智能化的客服服务。

6.1.4.2 AI 总结与生成的特性

AI 总结与生成功能应具备以下特性：

a） 准确性：应通过不断丰富知识库、提升客户意图识别准确性；

b） 自然性：生成的内容应具备高度的自然语言特性，使客户感受到流畅与人性化的对话体验；

c） 上下文理解：能够理解客户对话的上下文，确保生成内容的连贯性与逻辑性；

d） 定制化：支持根据企业需求进行定制和调优，生成特定风格或语气的内容；

e） 扩展性：支持持续学习和优化，能够随着客户互动数据的积累持续进行效果优化、升级；

f） 可标识：AI 生成内容应符合国家标准 GB 45438—2025，确保内容可识别、可追溯、可管理，并支持内容审核与合规追踪。

6.1.5 智能客服与人工客服协同功能要求

6.1.5.1 智能客服与人工客服协同的执行

人工智能营销客服平台宜支持智能客服与人工客服的无缝协同工作。当智能客服无法处理复杂问题时，系统宜能识别并自动将会话转交给人工客服，并在转交过程中保留完整的会话历史和上下文信息。

6.1.5.2 智能客服与人工客服协同的特性

智能客服与人工客服协同功能应具备以下特性：

a） 智能识别：系统应能够智能识别客户请求的复杂性，在适当时刻决定转交给人工客服；

b） 无缝转接：在智能客服与人工客服之间的转接过程中，应保证客户体验流畅，无需重复输入信息或描述问题；

c） 信息传递：在转接过程中，系统应将客户的所有历史会话记录、当前会话上下文、以及智能客服的分析结果一并传递给人工客服，以便人工客服快速理解问题并做出响应；

d） 灵活配置：系统应支持灵活配置转接规则，如根据客户的 VIP 级别、问题类型或当前客服负载情况，动态调整转接策略；

e） 明确标识：由人工客服转为智能客服时应通过法律法规规定的提示方式进行明确标识，避免引起客户混淆。

6.1.5.3 常规场景与极端场景下的人工客服依赖分析

为了更好地实现智能客服与人工客服的高效协同，应针对不同业务场景下对人工客服的依赖程度进行区分，明确各类场景下的策略设计与资源分配。

常规场景下的依赖特征：在大多数日常客户咨询场景中，如基础信息查询、常见问题答复、操作指引等，智能客服可实现高效应答并独立完成服务流程。在此类场景下，系统应优先由智能客服处理。降低对人工客服资源的消耗，仅在识别到客户反馈不满意或连续多轮未解决问题时，启动人工客服接入流程。

常规依赖策略包括：

a） 智能客服优先响应；

b） 设置容错轮数阈值后触发人工接入；

c） 通过客户满意度反馈判断是否转人工。

极端场景下的依赖特征：

当客户请求涉及高风险、高复杂度或突发事件（如交易异常、大规模故障、投诉升级、情绪激烈表达等）时，系统应快速判断为极端场景并优先转交人工客服处理。这类场景通常超出现有知识库覆盖范围或对响应速度、准确性要求极高，需依赖人工的灵活判断与应对能力。

极端依赖策略包括：

a） 建立高敏感度的异常识别模型，识别情绪波动、关键词触发等；

b） 配置“高优先级”人工接入通道；

c） 对高价值客户或重要事件配置人工客服专席支持；

d） 在突发场景下动态调整客服资源调度策略，确保人工客服响应优先级。

6.1.6 A/B 测试能力

系统应提供 A/B 测试功能，优化营销策略：

a） 测试设计：允许营销人员设计不同版本的营销内容；

b） 数据收集：收集各版本的效果数据；

c） 效果比较：比较不同版本的表现，确定最佳方案；

d） 自动应用：支持自动应用测试结果，提高效率。

6.1.7 客户生命周期管理

系统应根据客户不同的生命周期阶段，制定策略：

a） 阶段识别：识别客户所处的生命周期阶段；

b） 策略定制：根据阶段特点，定制营销策略；

c） 持续跟进：在不同阶段提供相应的支持和服务；

d） 关系维护：系统可根据客户所处不同阶段，制定自动化的维护策略，以增强客户忠诚度，延长生命周期。

6.2 智能推荐与营销引导功能要求

6.2.1 智能推荐的执行

AI 营销客服系统应具备智能推荐功能，通过分析客户行为数据和历史互动记录等数据，自动生成个性化推荐内容，如产品、服务或优惠信息，并适时推送给客户。

6.2.2 智能推荐的特性

智能推荐与营销引导功能应具备以下特性：

a） 个性化：推荐内容应基于客户行为数据和历史互动记录等数据，确保高匹配度和相关性；

b） 动态适应性：系统应能根据客户实时行为、意图变化，动态调整推荐内容和营销引导策略，以提升客户体验和营销效果；

c） 跨渠道一致性：智能推荐内容应在多渠道中保持一致，不论客户通过何种渠道访问，推荐的产品和服务信息应统一；

d） 透明度与可解释性：系统应提供推荐逻辑的可解释性，允许客户理解推荐的原因，并提供客户

选择的机会，如接受或拒绝推荐内容；

e） 合法性：推荐内容应确保属于合法、真实信息，不得存在虚假宣传、引人误解的内容。

6.2.3 数据分析与客户细分

系统宜具备强大的数据分析能力，通过对客户数据的深入分析，实现精准的客户细分：

a） 数据整合：系统应能对从多种渠道收集的客户数据，包括购买历史、浏览行为、社交媒体互动等，将其整合到统一的平台；

b） 客户细分：基于收集的数据，系统应能够对客户进行多维度细分，如按人口属性、行为特征、行为偏好等；

c） 预测分析：利用机器学习、统计模型等方法，系统应能预测客户未来的行为和需求，如购买意向、流失风险等；

d） 可视化报表：系统可根据常用分析需求，提供直观的分析报表和仪表盘，帮助营销人员理解客户特征和市场趋势。

6.2.4 营销活动管理

系统应支持营销活动的创建、管理和执行，提升营销活动的效率和效果：

a） 活动创建与设计：允许营销人员设计多种类型的营销活动，包括促销、新品发布、会员活动等；

b） 目标设定：支持设定明确的 KPI，如提升销售额、增加点击率等；

c） 预算与资源管理：能够管理活动预算，分配资源，跟踪花费；

d） 审批流程：支持活动的审批流程，确保活动内容和形式符合公司和法律要求；

e） 活动日程安排：设定活动的启动和结束时间，以及各项任务的时间节点。

6.2.5 营销流程自动化

系统应支持自动化重复性的营销任务，提高效率：

a） 任务自动执行：自动执行预设的营销任务，如发送跟进邮件等；

b） 流程编排：支持营销人员设计复杂的自动化流程；

c） 触发条件：根据客户行为或事件触发营销动作；

d） 监控与优化：实时监控自动化流程的效果，提供优化建议。

6.3 联络中心平台功能要求

6.3.1 概述

联络中心负责所有客户请求的媒体接入，呼入及呼出，以及路由控制，负责为整体客服平台提供统一的客户路由策略及媒体处理能力，提升客户体验。

6.3.2 呼叫及路由控制能力

智能客服呼叫及路由控制能力应满足以下功能要求：

a） 支持多种路由排队策略，包括但不限于根据客户维度、座席状态、座席技能等路由；

b） 路由排队系统支持溢出路由，包括技能组之间溢出路由、跨平台溢出路由、跨区域溢出路由等；

c） 宜支持自动外呼能力，宜支持预测、预览、预占用和 IVR 呼出，企业可根据业务需要、资源情况，选择适合的外呼策略；

d） 支持通话录音，录音宜满足 99.99%可靠性，录音数据保存期限应符合相关法律法规的规定；

e） 具备语音播放及控制能力，播放语音宜支持主流官方语言，如：汉语、英语等；

f） 具备座席管理能力，包括但不限于座席签发、修改、注销、删除等操作，并支持座席技能管理；

g） 具备自动化报表能力，宜能对呼叫、座席、路由等维度数据进行自动化报告；

h） 系统应支持灵活配置不同接入渠道的路由优先级与处理策略，适应业务需求变化。

6.3.3 媒体接入及处理能力

智能客服媒体接入及处理能力应满足以下功能要求：

a） 多种渠道接入：包括但不限于移动网站、App、5G 消息、Web 网站、VoLTE 视频接入、电话、邮箱等多种接入方式；

b） 多媒体接入：宜支持包括但不限于音频接入、视频接入、IVR 及 IVVR 接入；

c） 多媒体服务：宜支持多媒体服务（包括文字、图片、表情符号、语音、视频等）；

d） 音视频服务：宜支持 VoIP、VoLTE、WebRTC 等多种音视频通话能力，宜支持多人协同视频通话，宜支持音频通话和视频通话之间互相切换；

e） 单向视频外呼通话能力：宜支持在客户同意的前提下无缝切换成双向视频，切换期间不断线；

f） 远程协同：宜支持视频交互、桌面共享、白板、文档共享，支持视频场景下客户在线签名并保存等协同业务；

g） 体验一致性：无论哪种渠道接入，处理及响应体验一致；

h） 实时同步性：在多渠道交互中，系统应能实时同步客户会话记录，确保不同渠道的服务人员或系统模块可访问最新的会话历史。

6.3.4 开放性要求

宜支持基于联络中心平台开放接口，快速开发联络中心上层客服业务系统，支持灵活快捷构建智能化行业场景应用，宜具备如下能力：

a） 支持联络中心配置接口，供二次开发者使用创建、查询、修改、删除联络中心资源（技能、工号、IVR 流程等）配置；

b） 支持呼叫接续接口，供二次开发使用，含创建联络中心座席工作台、座席人员音频、视频及多媒体呼叫接续处理、座席状态控制；

c） 支持 IVR 编排接口，供二次开发使用，实现 IVR 流程编排；

d） 支持管理及报表接口，供二次开发使用，对联络中心的资源实时状态和呼叫实时及历史统计数据进行可视化管理；

e） 支持话单文件接口，供二次开发使用，获取联络中心原始话单；

f） 智能化能力接口，支持开发者基于开放接口实现智能语音导航、文本导航、智能推荐、意图识别等业务功能；

g） 联络中心监控能力接口，支持开发者基于开放接口实现联络中心实时和历史监控功能；

h） 系统应支持自动外呼能力接口，支持开发者基于开放接口实现自动外呼业务功能。

7 平台接口要求

7.1 综述

人工智能营销客服平台应提供一组标准化接口，以便于平台模块之间的交互以及与外部应用的集成。具体包括: 知识库状态相关接口（增删查改）、统一智能问答接口、知识库召回接口、AI 总结与生成接口等。

7.2 知识库状态相关接口

7.2.1 知识库新增知识接口

用于向知识库新增知识，见表 1。

public int newKnowledge（Knowledge knowledge）

表 1 知识库新增知识接口

参数	返回	说明
Knowledge：结构化知识	knowledgeId：唯一的知识 ID	

7.2.2 知识库知识删除接口

用于删除知识库中特定的知识，见表 2。

public boolean deleteKnowledge（int knowledgeId）

表 2 知识库删除知识接口

参数	返回	说明
knowledgeID：待删除的知识 ID	boolean: 是否删除成功	true 表示删除成功，false 表示删除失败

7.2.3 知识库知识查询接口

用于查询知识库中的知识，见表 3。

public Knowledge queryKnowledge（int knowledgeId）

表 3 知识库查询知识接口

参数	返回	说明
knowledgeID：待查询的知识 ID	Knowledge：查询到的结构化知识	如果查询失败或者未查询到，返回 null

7.2.4 知识库知识修改接口

用于修改知识库中的知识，见表 4。

public int modifyKnowledge（int knowledgeId, Knowledge updateKnowledge）

表 4　知识库修改知识接口

参数	返回	说明
knowledgeId：原始知识 ID updateKnowledge: 更新后的结构化知识	knowledgeId：更新后的知识 ID	

7.3　统一智能问答接口

该接口用于直接回答客户在智能客服系统中提出的各种问题，见表 5。

public String answer（String question）

表 5　统一智能问答接口

question：客户提出的问题	AI 营销客服系统经过综合处理响应客户的回答	该接口内部需要调用多个模块来综合作答

7.4　知识库召回接口

根据客户的问题，去知识库中召回与客户问题最相关的若干知识，见表 6。

public List<Knowledge> recall（String question）

表 6　知识库召回接口

参数	返回	说明
question：客户问题	List<Knowledge>：与客户问题最相关的知识列表	如果没有任何知识匹配客户问题，应该返回一个空列表

7.5　AI 总结与生成接口

该接口负责调用 AI 生成模块，基于客户输入和召回的知识内容，生成总结或进一步的营销话术，见表 7。

public String aiSummarize（String question, List<Knowledge> knowledge_list）

表 7　AI 总结与生成接口

参数	返回	说明
question：客户问题 knowledge_list：召回知识列表	AI 总结的回答话术	如果召回知识列表为空，则总结话术由 AI 自行判断回复

8　数据安全要求

8.1　安全验证

人工智能营销客服平台在接收到任何请求时，应首先执行安全验证流程，确保请求满足平台接口的

规范要求：

a） 平台应校验请求来源的合法性与可信度；

b） 只有在验证通过的前提下，系统才允许进一步处理请求并返回结果；

c） 验证机制应具备可扩展性，支持对新接入方的灵活配置与审查。

8.2 存储安全

平台应对涉及客户数据、知识库内容以及生成模型等相关信息的存储过程，提供全方位的安全保障：

a） 数据存储应满足完整性、机密性和可用性三大核心安全要求；

b） 所有数据必须采用强加密方式进行存储，防止被非法访问或篡改；

c） 与安全相关的证书、密钥等敏感信息，应使用安全加密机制进行存储管理，确保无法被窃取或破坏。

8.3 防篡改攻击

平台应具备完善的防篡改能力，以保障系统运行过程中的参数与配置不被恶意更改：

a） 应对涉及数据处理流程、生成算法、系统配置等要素实施完整性校验；

b） 所有运行参数与配置项应在执行期间持续保持有效性与一致性；

c） 防止外部实体或应用在未经授权的情况下对系统行为产生干扰或破坏，从而保障数据隐私与系统安全性。

8.4 安全检测

平台应具备对客户输入内容及生成输出的全流程安全检测能力，防止违法违规信息的生成与传播：

a） 系统可基于关键词识别、文本分类模型等技术，对客户输入内容进行实时分析；

b） 一旦发现明显诱导生成违法或不良信息的请求，应立即拦截响应，并返回安全提示信息；

c） 平台应具备多层处置手段，包括警示提醒、功能限制、暂停服务或终止服务；

d） 所有安全处置操作应自动记录，供后续溯源或审计。