模型上下文协议

连接协议 · 资源与工具接口

模型上下文协议是一种连接人工智能应用与外部系统的开放协议，用统一方式提供工具、资源和提示等能力。客户端负责使用这些能力，服务端负责暴露实际数据与操作接口。

01 工作方式

01 服务端声明可访问的资源和可调用的工具。

02 客户端发现能力，根据任务与授权发起请求。

03 服务端执行业务逻辑，返回结构化结果并保留日志。

02 场景应用

01 让智能体查询工单、读取知识库或获取数据字典。

02 为现有业务系统提供统一的人工智能工具接入方式。

03 边界与常见误区

01 模型上下文协议本身不保证数据正确、操作安全或业务规则完整。

02 身份认证、授权、输入校验和审计仍需系统实现。

03 接入模型上下文协议不意味着系统自动具备智能排程或自主决策能力。

04 来源与阅读说明

依据下列一手资料原创归纳；场景与工程建议为编辑整理，不是来源机构对本站服务的背书。

模型上下文协议官方文档 · 协议概述

https://modelcontextprotocol.io/docs/getting-started/intro