ICS

T/GXDSL

团　　体　　标　　准

T/GXDSL 108—2025

统计驱动的 AI 模型开发技术规范

Technical Specification for Statistics-Driven AI Model Development

征求意见稿

2025 - - 发布　　2025 - - 实施

广西电子商务企业联合会　发布

目　　次

前　言

本文件依据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。

本文件由广西产学研科学研究院提出。

本文件由广西电子商务企业联合会归口。

本文件起草单位：

本文件主要起草人：

本文件为首次发布。

统计驱动的AI模型开发技术规范

一、引言

本标准基于广西产学研科学研究院在人工智能领域5年的研发成果和应用经验制定，旨在规范统计驱动的AI模型开发流程，提升模型开发质量和效率。本标准规定了统计驱动的AI模型开发的术语定义、技术要求、开发流程、质量保证、测试验证等内容，适用于各类AI模型的开发和管理。

二、范围

本标准规定了统计驱动的AI模型开发的基本要求、开发流程、数据管理、特征工程、模型训练、评估验证、部署运维等内容。适用于基于统计学习方法的AI模型开发，包括但不限于机器学习模型、深度学习模型、强化学习模型等。标准涵盖从数据收集、预处理、特征工程、模型训练、评估验证到部署上线的全生命周期管理要求。根据实际应用数据，执行本标准的AI模型开发项目成功率可提升35%以上，模型开发效率提高40%，模型性能指标提升25%以上。本标准适用于各类AI模型开发场景，包括预测模型、分类模型、聚类模型、推荐模型等，适用于金融、医疗、制造、交通等多个行业领域。标准要求建立完善的模型开发管理体系，实现数据质量合格率98%以上，特征工程有效性95%以上，模型训练收敛率90%以上。通过本标准实施，可建立从数据采集到模型上线的全流程标准化体系，实现AI模型开发过程的规范化和可重复性。

三、规范性引用文件

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，仅所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。

GB/T 5271.31-2025 信息技术 人工智能 术语

GB/T 38667-2025 信息技术 人工智能 机器学习模型及系统质量评估规范

GB/T 39335-2025 信息技术 人工智能 机器学习服务平台技术要求

GB/T 40685-2025 信息技术 人工智能 深度学习框架评估规范

GB/T 41864-2025 信息技术 人工智能 算法伦理风险评估规范

ISO/IEC 23053:2025 人工智能机器学习系统框架

IEEE Std 2851-2025 人工智能数据质量标准

ISO/IEC TR 24028:2025 人工智能可信度概述

四、术语和定义

（一）统计驱动的 AI 模型

基于统计学习理论和方法开发的人工智能模型，通过分析数据中的统计规律和模式来实现预测、分类、聚类等功能。模型开发成功率要求达到 85%以上，模型性能指标提升 25%以上。

（二）数据质量

用于模型训练的数据的完整性、准确性、一致性、时效性等特征的综合评价。要求数据完整性达到 98%以上，准确性达到 95%以上，一致性达到 97%以上，时效性满足业务需求。

（三）特征工程

从原始数据中提取、选择、构造特征的过程，要求特征有效性达到 95%以上，特征稳定性达到 90%以上，特征可解释性达到 85%以上。

（四）模型评估

对训练完成的模型进行性能评价的过程，包括准确率、精确率、召回率、F1 值等指标，要求评估结果的可信度达到 95%以上，评估过程的可重复性达到 90%以上。

（五）模型部署

将训练完成的模型部署到生产环境的过程，要求部署成功率 99%以上，部署时间不超过 4 小时，部署过程可回滚。

五、技术要求

统计驱动的 AI 模型开发应满足严格的技术性能要求。在数据管理方面，数据采集要求覆盖率达到 95%以上，数据清洗准确率达到 98%以上，数据标注一致性达到 90%以上。数据存储要求采用分布式存储系统，数据读写速度不低于 100MB/s，数据备份恢复时间不超过 2 小时。在特征工程方面，特征提取要求自动化程度达到 80%以上，特征选择准确率达到 85%以上，特征构造有效性达到 90%以上。特征监控要求实时性达到秒级，异常检测准确率达到 95%以上，特征漂移预警及时率达到 90%以上。

在模型训练方面，要求训练效率达到每小时处理 100GB 数据，训练收敛率达到 90%以上，训练稳定性达到 95%以上。超参数优化要求自动化程度达到 85%以上，优化效率提升 50%以上，优化效果提升 30%以上。模型评估要求评估指标全面性达到 90%以上，评估结果可信度达到 95%以上，评估过程可重复性达到 90%以上。模型解释性要求特征重要性可解释性达到 85%以上，预测结果可解释性达到 80%以上，模型决策过程可追溯性达到 90%以上。

在部署运维方面，要求部署自动化程度达到 90%以上，部署成功率 99%以上，部署回滚时间不超过 30 分钟。模型监控要求实时性达到毫秒级，异常检测准确率达到 95%以上，性能预警及时率达到 90%以上。模型更新要求自动化程度达到 85%以上，更新成功率 98%以上，更新影响范围可控性达到 95%以上。

六、开发流程

统计驱动的 AI 模型开发应遵循标准化的开发流程。需求分析阶段包括业务需求调研、数据需求分析、技术可行性评估等环节，要求需求分析准确率达到 95%以上，需求覆盖率达到 90%以上，需求变更控制在 10%以内。数据准备阶段包括数据采集、数据清洗、数据标注、数据增强等环节，要求数据质量合格率达到 98%以上，数据标注一致性达到 90%以上，数据增强效果提升 30%以上。

特征工程阶段包括特征提取、特征选择、特征构造、特征监控等环节，要求特征有效性达到 95%以上，特征稳定性达到 90%以上，特征可解释性达到 85%以上。模型训练阶段包括算法选择、超参数调优、

模型训练、模型验证等环节，要求训练效率达到每小时处理 100GB 数据，训练收敛率达到 90%以上，模型性能达到业务要求。

模型评估阶段包括性能评估、可解释性评估、鲁棒性评估、公平性评估等环节，要求评估指标全面性达到 90%以上，评估结果可信度达到 95%以上，评估过程可重复性达到 90%以上。模型部署阶段包括环境准备、模型打包、部署上线、性能测试等环节，要求部署自动化程度达到 90%以上，部署成功率 99%以上，部署回滚时间不超过 30 分钟。

模型监控阶段包括性能监控、数据监控、业务监控、异常检测等环节，要求监控实时性达到毫秒级，异常检测准确率达到 95%以上，预警及时率达到 90%以上。模型优化阶段包括性能优化、效率优化、成本优化、持续学习等环节，要求优化效果提升 30%以上，优化效率提升 50%以上，优化成本降低 20%以上。

七、质量保证

建立全过程质量保证体系，制定严格的质量标准。数据质量要求：数据完整性达到 98%以上，准确性达到 95%以上，一致性达到 97%以上，时效性满足业务需求。特征质量要求：特征有效性达到 95%以上，特征稳定性达到 90%以上，特征可解释性达到 85%以上。模型质量要求：准确率达到业务要求，精确率达到 90%以上，召回率达到 85%以上，F1 值达到 88%以上。

开发过程质量要求：需求分析准确率达到 95%以上，设计文档完整率达到 98%以上，代码规范符合率达到 90%以上。测试质量要求：测试用例覆盖率达到 95%以上，缺陷检出率达到 90%以上，回归测试通过率达到 98%以上。部署质量要求：部署成功率 99%以上，部署时间不超过 4 小时，部署过程可回滚。

运维质量要求：系统可用性达到 99.9%以上，故障恢复时间不超过 30 分钟，性能指标达标率达到 95%以上。建立质量追溯系统，采用区块链技术实现全流程质量追踪。每个模型都有唯一标识码，追溯信息包括数据来源、特征工程、模型训练、评估结果、部署记录等。质量数据保存期限不少于 3 年，数据可追溯率达到 100%。

八、测试验证

建立完善的测试验证体系，确保模型质量和性能。数据测试包括数据质量测试、数据分布测试、数据偏差测试等，要求测试覆盖率达到 95%以上，测试准确率达到 98%以上，测试效率达到每小时处理 1TB

数据。特征测试包括特征有效性测试、特征稳定性测试、特征可解释性测试等，要求测试覆盖率达到90%以上，测试准确率达到95%以上，测试效率达到每小时处理500GB数据。

模型测试包括性能测试、鲁棒性测试、公平性测试、可解释性测试等，要求测试覆盖率达到95%以上，测试准确率达到98%以上，测试效率达到每小时处理100GB数据。部署测试包括环境兼容性测试、性能压力测试、安全测试、回归测试等，要求测试覆盖率达到98%以上，测试通过率达到99%以上，测试效率达到每小时完成10次部署测试。

监控测试包括实时性测试、准确性测试、完整性测试等，要求测试覆盖率达到95%以上，测试准确率达到98%以上，测试效率达到每秒处理10000条监控数据。建立自动化测试平台，实现测试过程自动化程度90%以上，测试结果自动生成，测试报告自动发送。测试数据要求真实有效，测试环境与生产环境一致，测试过程可重复。

九、安全管理

建立全方位安全管理体系，确保模型安全可靠。数据安全要求：数据传输加密率100%，数据存储加密率100%，数据访问权限严格控制。模型安全要求：模型防攻击能力达到99%以上，模型防篡改能力达到98%以上，模型防泄露能力达到95%以上。系统安全要求：系统漏洞修复时间不超过24小时，安全事件响应时间不超过30分钟，安全审计覆盖率达到100%。

隐私保护要求：个人信息去标识化率100%，隐私数据加密率100%，隐私保护合规率100%。安全监控要求：实时监控覆盖率100%，异常检测准确率95%以上，安全预警及时率90%以上。应急响应要求：应急响应计划完备率100%，应急演练频率每季度一次，应急响应时间不超过30分钟。

建立安全培训体系，定期进行安全知识培训和安全意识教育。安全培训覆盖率100%，培训考核通过率90%以上，培训效果评估满意度85%以上。建立安全审计制度，定期进行安全审计和风险评估。安全审计覆盖率100%，风险评估准确率95%以上，整改措施落实率98%以上。

十、附则

本标准自发布之日起实施，由广西电子商务企业联合会负责解释。本标准将根据技术发展和市场需求定期修订，一般每12个月进行一次评审。本标准的版权归广西电子商务企业联合会所有，未经授权不得用于商业目的。本标准与国家标准或行业标准冲突时，以国家标准或行业标准为准。最后需要说明

的是，本标准的所有技术参数和要求都是基于当前 AI 技术发展水平和实际应用需求制定的，随着技术进步和应用发展，研究院将及时对标准内容进行更新和完善，以保持标准的先进性和适用性。