基于账号稽核智能体的智慧风控能力体系研究与实践

Research and Practice on Intelligent Risk Control Capabilities and System Based on Account Audit Agent

张晓东，高万江（中国联通广东分公司，广东 广州 510627）
Zhang Xiaodong，Gao Wanjiang（China Unicom Guangdong Branch，Guangzhou 510627，China）

摘　要：
落实账号精细管控是政策要求和电信行业的业务需求。现有的账号实名制合规体系，在账号管控上仍存在违规模型分散、违规实时监测难、处置碎片化、人工稽核慢、核查溯源滞后等痛点。以问题为导向，通过贯通“异常监测—违规溯源—安全运营”全链路，打造“AI Agent+RPA+大小模型”账号安全智能体，实现账号数据采集、违规行为建模、动态风险控制、自动稽核闭环，高危账号拦截从天缩至小时级，违规整改周期由15天压至5天内，人力稽核节省50%。

关键词：
账号安全风险管控；异常账号监测与闭环处置；多模态数据联动；账号AI智能体应用
doi：10.12045/j.issn.1007-3043.2025.12.013
文章编号：1007-3043（2025）12-0071-05
中图分类号：TN919
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
Implementing precise control over system accounts is a policy requirement and a business necessity in the telecommunications industry. there are still pain points in system accounts control, such as scattered violation models, difficulties in real-time monitoring of violations, fragmented handling, slow manual auditing, and lagging verification and traceability. By integrating the entire process from"anomaly monitoring to violation traceability to secure operation", it creates an "AI Agent+RPA+large and small models" system accounts security intelligence system, achieving closed-loop processes for system accounts data collection, violation behavior modeling, dynamic risk control, and automatic auditing. The interception time of high-risk system accounts has been reduced from days to hours, the violation rectification cycle has been compressed from 15 days to 5 days, and manual auditing has been saved by 50%.

Keywords：
System accounts security risk management and control; Abnormal accounts monitoring and closed-loop handling; Multi-modal data linkage; Accounts AI intelligent agent application

引用格式：张晓东，高万江. 基于账号稽核智能体的智慧风控能力体系研究与实践[J]. 邮电设计技术，2025（12）：71-75.

1 背景

1.1 实施背景

1.1.1 管理方面

为落实国家层面反诈相关法律法规要求，集团公司制定了内部信息系统操作规范[1]，严格规范各类业务系统操作人员的账号权限，明确要求信息系统工号100%落实“实名、实人、实操作”规范要求。

收稿日期：2025-11-17

1.1.2 业务方面

根据工信部2024年以来关于电话卡和用户个人信息安全管理的要求，省公司持续加强账号权限管理、账号数据运营、账号监控稽核和账号合规管理，实现对核心系统账号使用轨迹画像，沉淀异常检测分析方法，针对高风险账号、疑似账号的违规操作，实现异常操作的风险监测和违规行为的闭环处置。

1.1.3 技术方面

为满足当前反诈前端精细管控要求，实现及时发现、及时处置账号违规行为等管理目标，亟须对账号

管控系统的技术架构和监测处置技术进行升级改造[2]。

1.2 面临的挑战

1.2.1 缺少覆盖多场景的常态化账号异常监测

账号管理业务场景复杂，关键账号风险数据分散在多个业务系统[3]。一人多账号、一证多户等风险场景未全量纳入监测体系，盲区较多、异常行为发现滞后、涉诈溯源能力薄弱。

1.2.2 缺少常态闭环处置流程，安全运营点状化且不持续

账号安全运营呈现点状化、碎片化特征，难以实现常态化风险管控。风险评估与处置环节过度依赖人工经验，多通过邮件方式流转指令，经常出现反馈不及时、有头无尾等现象。

1.2.3 人工稽核耗时长、准确率低

账号操作日志依赖传统手段，多源异构数据未能有效整合，自动化识别和分类分级的准确率不高。缺少专业的数据安全风险排查工具，异常行为检测时延长，导致风险识别与处置效率低下，难以有效清除高发风险并遏制账号违规事件[4]。

2 解决思路

2.1 方案思路

围绕账号全生命周期风险管控“更快”和“更准”2个关键点，力争构建“账号创建→风险监控→异常处置→数据沉淀→账号终结”的敏捷管控体系。核心是在数据特征与AI算法的协同支撑下，构建智能化账号管控处置体系。

2.1.1 数据特征层面

基于集团数据湖和省分账号标签数据，运用AI技术融合新旧特征，形成包含“基础属性+业务指标+无监督算法输出”的多层次特征集合。通过无监督学习挖掘数据原生特征，再依托闭环迭代机制持续扩充特征宽表，形成“数据自驱动、业务反哺数据”的良性循环，为精细化稽核提供坚实特征支撑，推动运营策略从“经验驱动”升级为“数据预测驱动”[5]。

2.1.2 AI算法层面

依托企业AI智能体平台编排技防分析智能体[6]，通过多维特征融合模型开展异常账号分析。在实施时，整合时间（登录时长、非工作时操作）、空间（跨IP/跨域）、频次（高频操作）及业务（敏感查询）等18维度特征，结合DBSCAN、LightGBM算法及孤立森林等无监督算法构建检测模型，形成“数据采集—特征工程—指标建模—运营验证—特征迭代”的全链路闭环数据工程，提升稽核自动化与智能化水平。

业务流程如图1所示。

2.2 实施建设分析

2.2.1 体系架构

该体系包括构建基础数据集、异常账号稽核与账号风险管理等功能模块。基于能人账号轨迹数据，构建用户实体行为数据集，使用规则模型+算法模型对账号异常行为进行识别，调用RPA、大模型、流程编排、大模型问答等接口能力，实现对风险账号的处置与运营管理。体系架构如图2所示。

2.2.2 技术架构

本方案的技术架构如图3所示。本方案采用以Vue为主的前端页面，通过Nginx提供Websocket和Restful接口服务，使用Python搭建Agent技术框架，使用Mysql/PG作为数据存储，对接DeepSeek、千问、百川等大模型能力。

2.2.3 自动化流程

重构异常账号预警处置流程，解决人工处置效率低、响应滞后的问题，优化了以下2个流程[7]。

a）优化自动触发告警流程。通过“规则+算法模型”对账号行为进行异常稽核，自动进行弹窗预警。

b）优化自动化处置流程。根据预设规则（如红黄牌分级），触发账号禁用、权限降级等自动化操作，无需人工干预。

处置流程如图4所示。

3 实践成果

面向手机端和PC端业务核心业务系统账号权限和操作行为，构建统一稽核规则库。通过大小模型的深度融合进行账号异常操作行为的检测识别，具体包括构建多个小模型来识别账号异常数据自动进行打标；使用大模型构建AI Agent，基于多维度标签判定账号是否异常，主动发现疑似风险。与人工抽检模式相比，该方案的账号检查覆盖率达100%，监测效率提升40%以上，风险发现及时率提升到小时级。

3.1 形成基于多源数据集的多场景、全覆盖的异常账号监测体系

3.1.1 多源数据集完善与标签库构建

构建移动应用账号基础表、线上引流业务发展用户明细与汇总表、用户与订单开户行为日表等8个以

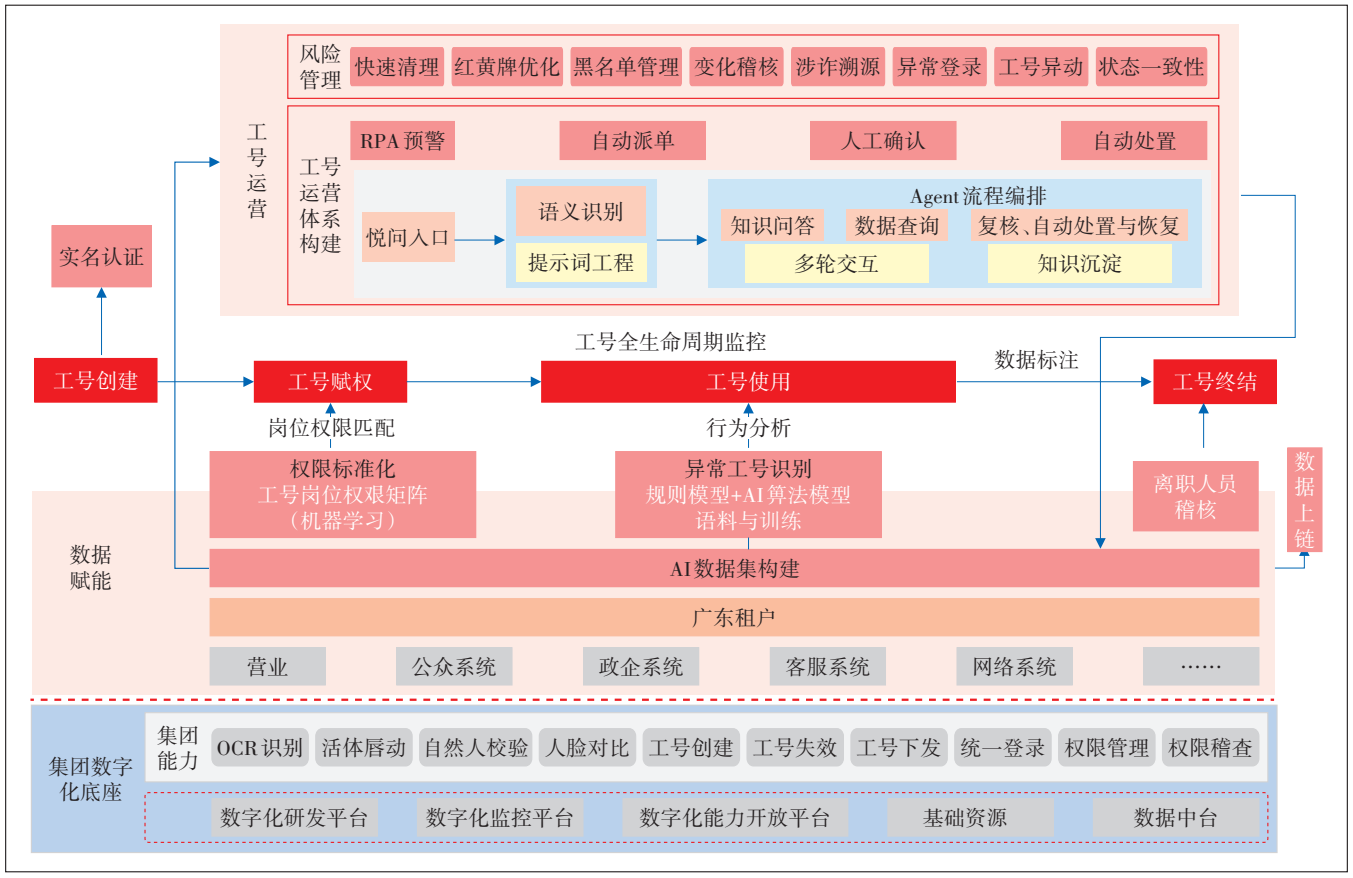

图1　业务流程

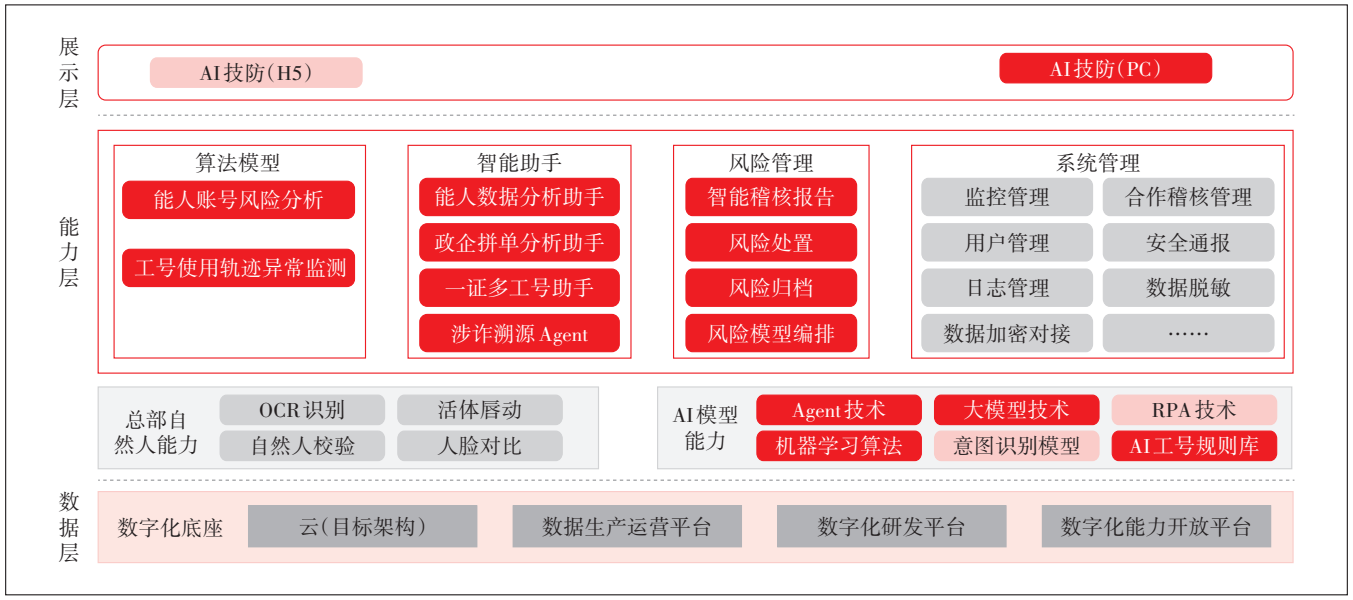

图2　体系架构

上的基础数据集，开发238项数据标签并构建异常操作行为标签库，将账号异常使用行为纳入常态检测和闭环管控[8]。

3.1.2　异常行为监测算法及模型

研发账号风险算法分析模型，使用机器学习算法对账号进行风险分析，每日对账号异常和风险场景进

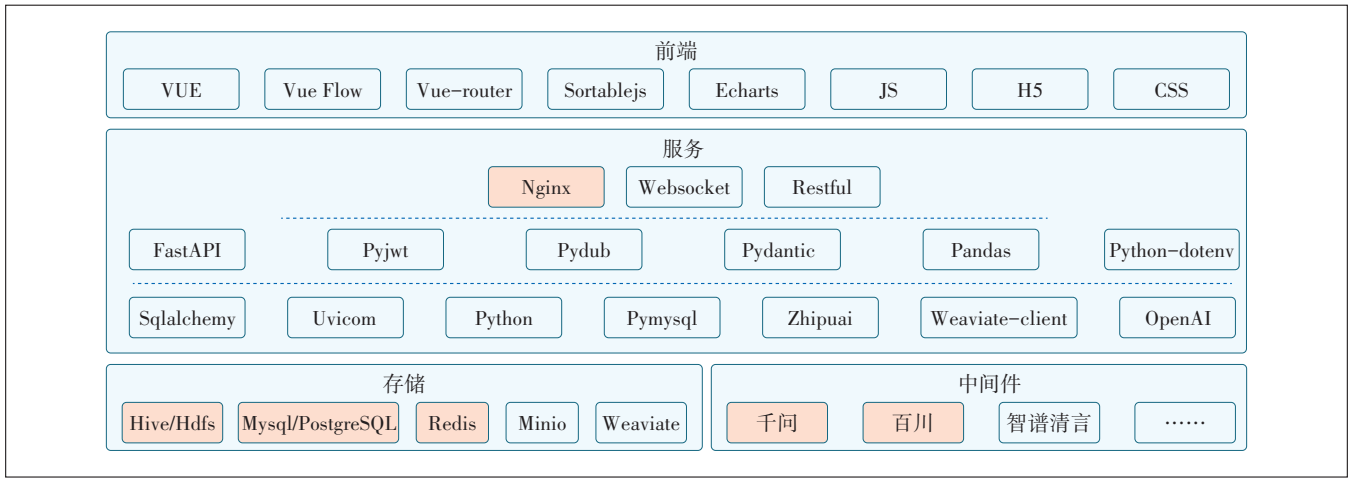

图3　技术架构

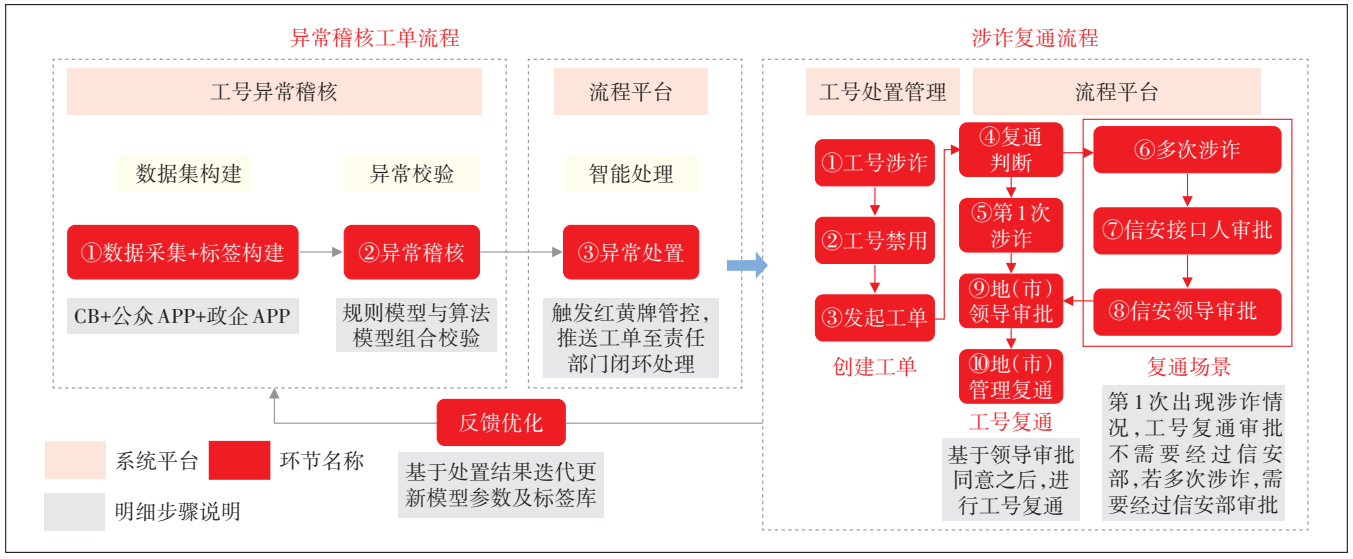

图4　异常账号预警处置流程

行稽核，确保账号100%纳入名单管控，并对风险账号进行常态管控[9]。

研发轨迹异常监测模型，结合账号的唯一性与位置、行为特征数据，为算法模型与分析提供支撑，提升异常识别准确率[10]。

3.1.3 账号异常操作信用评分“三维画像”

构建位置打点和账号行为数据集，首创“账号—位置—行为”多维标签库，设计账号动态信用组合评分体系，强化账号异常行为安全审计和违规稽核，实现高风险操作分钟级熔断。

3.2 构建常态化异常账号监测与闭环运营处置体系

3.2.1 构建新入网异常用户“红黄牌”预警引擎

预警引擎融合涉诈证件、高幼龄用户、频繁开销户、涉诈高危户籍地、涉诈高危交付地等28项高风险特征，每天自动对新入网异常用户风险进行打标并分类分级处置，对渠道网点违规率进行度量、溯源，并能一键生成核查整改和问责处置工单[11]。

3.2.2 打造用户异常入网和账号异常操作的全流程自动化处置机制

通过融入AI大模型、多场景异常检测小模型，实现检测能力常态化迭代升级训练。将涉诈风险号码和高危违规账号纳入常态检测和闭环管控，通过智能决策实现“预警—分析—处置”“查询—判定—处理”全流程自动化，报告一键生成，提升识别精准度和处置效率。

3.2.3 创新账号异常风险处置的全流程闭环管理与智能运营体系

实现从风险监测、识别到响应处置、反馈改进的

全流程闭环管理。采用区块链技术记录操作日志，确保数据不可篡改且全程可溯，增强透明度与信任度[12]。构建统一风险特征库，实时同步风险特征信息，各级部门可根据这些风险特征信息快速调整策略，精准地打击风险。

3.3 构建基于大小模型和智能体技术的AI Agent应用

3.3.1 开发能人账号数据分析助手

利用大模型构建AI Agent，使其理解用户数据分析意图。经过专门调优训练，让大模型对数据进行聚类、排序、排名并对数据的波动情况、相关性等进行分析，总结数据特征，降低数据使用门槛；代替人工取数，提升工作效率。

3.3.2 开发账号运营和管理智能体

依托智能体平台，建立账号规则知识库，构建多种场景的智能分析运营助手，如账号异常检测报告Agent、一证多卡运营助手、政企拼单运营助手、涉诈溯源Agent等，实现自动化运营，支撑对异常场景的运营处理和对涉诈的溯源。

4 运营成效

以打造“多模态数据联动+AI智能决策”的反诈体系为核心，贯通“大模型—小模型—AI智能体”三级引擎，提升了对诈骗电话的事前研判预警、事中快速关停、事后全面溯源的综合能力，形成了“全网一体、协同联动、技管融合、精准高效”的立体化防护网，实现账号安全与运营自动化双提升。

4.1 管理效益：筑牢业务安全防线，风险管控水平显著提升

新入网涉诈占比降至30%以下，高风险涉诈号码入网识别率达95%以上，高危账号违规操作下降60%以上，从源头防范电信业务安全风险。

4.2 业务效益：优化账号全流程运营，实现系统账号精细化稽核

建立标准化账号信用评分体系，按“高危—中危—低危”进行分级评价，并配套完善处置流程（含账号禁用、恢复流程），规范账号运营标准。支持自然语言自动转换为结构化查询语言，业务人员无需专业技术能力即可完成数据查询与分析，有效降低使用门槛。

4.3 经济效益：成本节约成效显著

累计节约人力成本40%以上、运营成本20%以上。通过账号管理人力集约、AI替代人工服务等智能化和自动化手段，全年总计节约成本700万元以上。

5 结束语

安全风险是相对的、动态的，智能化时代更是如此。在实践中，仍存在风险识别模型可解释性不足、跨平台兼容性较弱等关键挑战。未来研究将聚焦于联邦化协同学习、自适应威胁感知及隐私保护计算等核心技术，推动账号安全管理从“规则驱动”向“智能内生”的范式转化，该演进方向有望重塑企业级账号安全管理模式，并为构建智能社会的数字身份基础设施奠定重要技术基础。

参考文献：

[1] 胡凯鹏. 信息系统中的用户权限管理与访问控制优化策略分析[J]. 集成电路应用，2025，42(4)：250-251.
[2] 王晨，罗琼，潘梁，等. 基于可信AI和时空大数据的实时智能反诈系统研究与应用[J]. 电信工程技术与标准化，2022，35(12)：34-39.
[3] 覃锦端，王月兵，周杰，等. 基于动态风险评估机制的零信任IAM架构设计[J]. 信息安全研究，2023，9(12)：1190-1196.
[4] 陆勇，孙加萌. 基于大数据的日志分析技术及其在企业信息安全中的应用研究[J]. 中国高新科技，2022(18)：7-9.
[5] 何慧霞，武森，魏桂英，等. 混合属性数据深度无监督融合特征学习方法[J]. 计算机科学与探索，2024，18(7)：1852-1864.
[6] 李国鹏，吴瑞骐，谈海生，等. 面向大语言模型驱动的智能体的计划复用机制[J]. 计算机研究与发展，2024，61(11)：2706-2720.
[7] 叶张乐. AI智能体驱动安全防御从被动响应到主动预测的范式升级[J]. 中国安防，2025(6)：11-12.
[8] 李洪赭，江海涛，高艳苹，等. 基于贝叶斯层级模型的用户异常行为检测研究[J]. 通信技术，2024，57(6)：593-597.
[9] 高能，彭佳，王识潇. 零信任的安全模型研究[J]. 信息安全研究，2024(10)：886-895.
[10] 白雪，章帅，房礼国. 基于深度学习的用户和实体行为分析技术[J]. 信息工程大学学报，2024，25(6)：697-702.
[11] 孙加萌，宋文凯. 基于大数据的企业内部用户实体行为分析研究[J]. 中国新通信，2023，25(2)：53-55.
[12] 周黎. 基于区块链技术的防篡改审计系统设计[J]. 微型电脑应用，2021，37(12)：206-208.

作者简介：
张晓东，毕业于中山大学，工程师，硕士，主要从事数据安全、网络安全等相关工作；高万江，毕业于北京大学，工程师，硕士，主要从事数据安全、网络安全、信息安全和个人用户隐私保护工作。