ISSN：3078-8994
EISSN：3104-4492

# 人工智能审计场景下的数据隐私保护机制研究

刘子夜　刘琪琪

河北工程技术学院，河北 石家庄 050091

**摘　要：**随着人工智能的不断发展，其与审计的结合也越来越密切，有效突破了传统审计工作面临的数据处理效率低下、人工干预导致偏差、风险识别滞后的局限。但是人工智能审计也带来了超范围采集隐私数据、存储传输环节漏洞，数据脱敏不足以及审计成果归档环节的分级管控松散等数据安全问题。本文从审计数据采集、存储与传输、智能审计系统构建与处理以及审计资料归档这四大审计核心环节对数据安全问题进行分析，从技术防护、管理规范、合规管控三个维度，构建全流程、多层次的数据安全防护体系，防范数据泄露风险。

**关键词：**人工智能；审计；数据安全

## 0 引言

当前，随着数字经济全球化发展和人工智能技术不断迭代，审计工作已经处在从传统人工审计向以大数据、云计算为支撑的人工智能审计转型的关键阶段，智能审计已经成为审计数字化转型的重要趋势，并在政府审计、内部审计、社会审计领域得到实质性应用。其自动化采集、智能化处理、精准化识别风险、规范化存档的特性切实提高了审计质量与效率，也把审计工作推进到“事前预警、事中控制、事后整改”的全流程闭环管理。

但是智能审计在提升审计效能的同时，也突破了传统审计的数据安全管控边界。因此，数据安全问题成为了制约智能审计高质量发展的根本问题，也是目前审计学界和实务界都高度关注的议题。

## 1 智能审计带来数据泄露风险

数据采集、存储传输、模型与系统处理、成果归档是智能审计的四大核心环节，本文将系统分析各环节存在的数据泄露风险与关键泄露点。

### 1.1 数据采集与处理环节

在利用人工智能进行审计的流程中，数据采集是开展审计工作的首要环节，也是造成数据安全和隐私泄露的关键节点。人工智能审计可以利用智能算法从多个数据源头自动抓取和整合数据。在企业中，数据采集的范围涉及公司的财务系统、业务管理平台、内部办公系统、税务申报系统等公司的办公应用平台，收集的数据资料还包括银行、供应链上下游的资料、数据等，数据的来源复杂、类型多样且体量巨大。面对如此多的数据，人工审核管控难度大，只能依赖智能化的自动采集模式，但自动采集过程存在一定的不可控性，加剧数据安全风险和泄露隐患。从数据来源看，当前企业使用的业务平台多样且相互独立，数据接口的标准不统一，使智能审计平台在跨系统采集数据时无法制定严格的权限边界，容易出现超范围采集，抓取与审计无关的企业涉密信息、员工的隐私信息以及客户的敏感信息。同时，从合规授权和智能采集角度来看，人工智能的数据抓取往往存在数据采集授权流程不规范的问题。部分审计数据采集系统在未告知的情形下，盲目抓取企业半公开、未公开甚至涉密的经营信息；智能算法还会自动整合采集到的数据信息，使原本脱敏的数据信息整合成完整的数据图谱，间接造成信息泄露。

### 1.2 数据存储与传输环节

由于数据存储、传输是人工智能审计流程中连接数据收集、数据处理两个阶段的重要环节，故也是人工智能审计中产生审计数据泄露风险最突出、最关键的环节：审计数据从企业资金收支明细、往来账目等财务流水数据，到内部管控节点、审批记录、岗位职责权限、风险防控措施等多种内部控制数据，若其中任何部分泄露或被篡改，都会直接破坏审计工作的真实性、可靠性，甚至导致企业涉密信息泄露，进而带来财务风险、合规风险，损害企业利益。

在数据存储环节产生风险泄露的原因包括存储技术缺失和安全管理不到位。部分企业在存储审计数据时，放松警惕、未采用加密存储技术，将本地服务器存储、云端存储中的财务数据和内控数据直接以明文形式留存。在这种情况下，企业的审计人员、财务人员或者运维人员可以直接访问、私自拷贝、导出相关信息，获取核心审计数据；甚至存在企业内部人员对数据进行篡改以掩饰企业的违规操作。另外，如果存储设备存在系统漏洞、权限管理不严等，外部人员甚至可以通过入侵服务器、破解存储密码、植入病毒等方式非法获取存储的审计数

ISSN：3078-8994
EISSN：3104-4492

据，造成数据大规模泄露甚至智能审计程序瘫痪。

在数据传输环节主要是由于缺乏安全传输通道或传输过程管控不严，导致存在数据泄露风险。已采集的审计数据需要在采集端、存储端、审计处理端和各审计节点之间的流转，但是部分企业未建立起安全传输通道，财务、内控数据仍以明文形式进行传输，在传输过程中可能遭受黑客攻击或被无关人员非法拦截、窃取、篡改，导致数据泄露或审计数据失真。此外，内部审计人员由于安全意识淡薄，在数据传输或拷贝过程中未严格遵守相关规定，复制敏感数据，引发数据泄露。如果企业没有针对数据传输过程的全程监控，一旦发生数据泄露、篡改事件，可能导致无法及时追查问题环节，使风险影响的范围进一步扩大。

### 1.3 智能审计模型与系统处理环节

智能审计模型构建与系统梳理是智能审计实现自动化分析、识别风险和研判疑点的核心环节，该环节依托海量数据驱动模型运算，数据敏感性高，对安全防护的要求更为严格，也是造成数据泄露的重要环节。在审计模型的构建过程中，需要大量的基础数据进行训练、推理与迭代，会加载和存储被审计单位的财务数据、经营信息、内控流程以及交易流水等大量的敏感数据，如果未采取脱敏、隐私加密的处理，会导致模型逆向推理、提取参数、重构数据，进而得到原始训练数据和被审计对象的敏感信息，最终导致核心数据泄露。此外，部分企业将智能审计运算环境部署于公共云端平台，对智能审计处理系统未严格限制访问权限，将审计数据与普通的业务数据共同保管，其他云端服务商可能出现越权访问、违规调取隐私数据，严重威胁审计数据保密性和企业经营安全性。

### 1.4 审计成果归档环节

审计成果归档是智能审计的最后一个环节，而归档资料又集中体现了审计全过程细节及原始数据，因此管控不当必然会带来数据泄露风险。具体而言，人工智能环境下所生成的审计报告、审计工作底稿及电子证据材料中普遍夹杂着未脱敏的个人信息、企业商业秘密及财务核心数据，若归档存储环节没有严格贯彻数据分级分类保护及安全管控的要求，对存储资料中所含的敏感信息未及时、充分地脱敏、加密，可能发生企业、政府、事务所内部人员违规查阅、私自复制、外传泄露的问题。电子归档文件存储介质安全防护薄弱，纸质归档资料管理不规范，归档数据超期留存又未定时清理，种种因素叠加在一起，数据泄露风险大大增加，审计的公信力及数据安全合规性都直接受到影响。

## 2 人工智能审计场景下数据保护机制

针对人工智能审计各环节存在的数据泄露风险，本文从技术防护、管理规范、合规管控三个维度，构建全流程、多层次的数据安全防护体系，防范数据泄露风险。

### 2.1 数据采集环节改进措施

在数据采集环节，数据采集主体应严格落实最小权限采集和按需采集的原则，根据审计工作计划和工作方案明确数据的采集范围和边界，对跨系统的采集程序实行适当的授权审批控制，设置必要的采集白名单，降低超范围采集和抓取无关数据的可能性，确保只采集与审计目标相关的数据。对企业内部业务接口实行审计访问限流、对第三方接口也要采取加密方式进行数据传输，还可让审计人员全程参与接口测试和漏洞排查，留存相关的工作底稿，确保采集数据的真实性、完整性和安全性。对于采集授权，要严格履行审计告知义务，获得被审计单位的授权后再开展数据采集工作，在数据采集过程中严禁采集涉密数据、未经授权信息和敏感数据，防止出现审计执业风险。

### 2.2 数据存储与传输环节改进措施

在数据存储和传输环节，第一，要结合审计数据管理规范和信息安全保护规范，加密财务流水、内控流程数据等核心敏感审计数据，实现本地服务器、云端存储、中间数据库的全场景加密。审计人员还要对加密存储流程进行监督，留存加密审计记录，确保数据加密合规。第二，从数据的重要性、敏感程度出发，建立并实施审计数据分级分类存储机制，对核心审计证据、涉密审计数据实行物理或逻辑隔离存储，由专门的审计人员予以管控，审计人员要定期、不定期对数据的安全性、完整性做系统抽查，防止数据篡改或泄露，还要有计划地对存储设备进行安全检测与漏洞修复，保证数据的安全性。第三，建立审计专用安全传输通道，使审计数据实现加密传输，审计人员实时监控数据传输过程，对传输异常情况及时预警、即时处置。第四，建立审计数据传输全程日志记录与审计留痕机制，对传输数据的来源、去向、操作人、操作时间等信息完整记录，确保传输过程可追溯。同时加强对审计人员传输权加以严格控制，明令禁止私自截取、拷贝、外传审计数据，系统性防范内部审计人员违规操作风险。

### 2.3 智能审计模型与系统处理环节改进措施

在建立智能审计模型的过程中，审计人员参与模型脱敏技术应用的审核，对模型中存储的敏感审计数据处理效果进行检查，防范模型逆向推理导致的审计数据泄露。规范人工智能

ISSN：3078-8994
EISSN：3104-4492

审计模型训练数据管理，严禁将未脱敏的原始审计数据、审计证据直接用于模型训练，对模型训练过程进行审计监督，保留模型训练审计底稿。规范审计系统云端部署安全审计，审计人员和法务相关人员直接参与云端服务商的合规性审核，厘清云端服务商的数据访问权限、责任边界；同时，建立审计数据与普通业务数据的隔离机制，防范云端服务商在获取业务数据时越权访问、窃取审计数据，真正保障审计数据保密性。加强审计系统安全防护审计，定期进行系统漏洞扫描、病毒查杀，规范系统账号权限管理，做到审计人员账号专人专用、权限分级管控，避免账号共用等问题，确保所有操作都留有可追溯、可验证的系统安全审计记录。

### 2.4 审计成果归档环节改进措施

严格依照审计档案管理准则落实审计数据分级分类保护要求，审计人员对归档资料中的个人信息、企业商业秘密等必须做充分、规范的脱敏处理，对核心审计证据、审计报告、核查记录等敏感归档资料予以加密并设置查阅权限，明确不同等级归档资料的审计查阅权限、操作流程与审批程序，做到归档资料规范管理。在此基础上建立审计成果归档安全管理制度，实行分级查阅、操作留痕机制，审计人员直接承担归档资料的审核与管控责任，严禁未经审批违规查阅、复制、外传归档资料。同时规范电子审计归档文件存储介质管理，使用加密存储介质，定期做好存储介质的安全检测与备份；定期对电子归档文件的完整性、安全性进行检查，防范存储介质丢失、损坏带来的审计数据泄露。规范纸质审计归档资料管理，设立专门的审计档案库，指定专人专管，严格执行审计档案借阅、归还审批流程。最后，建立完整的审计归档数据生命周期管理机制，按照审计档案保管期限要求，及时、有序地对超期留存的归档数据进行清理、销毁，清理销毁过程实行双人复核、全程留痕，确保符合审计档案管理规范。

此外，还需定期对审计人员开展数据安全、审计合规管理培训，切实提高审计人员数据安全意识与执业素质，从根本上防范人为泄露、违规操作等审计执业风险。

## 3 结论

本文对智能审计的数据采集、存储和传输、智能审计模型构建与系统处理、审计成果归档四大核心环节中存在的数据泄露风险做了详细分析，并提出了针对性的防范措施，得出以下核心结论。

第一，虽然智能审计数字化、智能化转型显著提升了审计工作效率，但带来了数据泄露风险多元化、隐蔽性的新特点，因此数据安全管控已成为智能审计高质量发展的核心前提。智能审计涉及财务流水、内控流程、个人信息等敏感数据，数据的安全状态直接关系到审计结论的真实性、客观性及公信力，也直接关系审计机构执业的合规性和被审计单位的合法权益。

第二，智能审计各环节均存在数据泄露风险。数据采集环节存在超范围采集、接口安全漏洞问题，存储传输环节存在明文存储、未加密传输问题，智能审计模型构建与系统处理环节又存在数据脱敏不足、云端部署安全问题，以及审计成果归档环节管控松散、未做脱敏处理，这些问题共同构成了智能审计数据泄露的核心风险来源。

第三，防范智能审计数据泄露风险，必然要建立“技术防护 + 管理规范 + 合规管控”的全流程安全防护体系。通过落实最小权限采集、加密存储与传输、模型隐私加固、归档分级管控等措施，同时强化审计人员执业素养培训，才能真正防范各环节数据泄露风险，实现智能审计与数据安全的协同发展。

**参考文献：**

[1] 刘育红 . 人工智能技术在审计中的应用前景与挑战 [J]. 湖北经济学院学报 ( 人文社会科学版 ),2026,23(05):86-90.

[2] 韩天佩 , 杨寅 , 柯武敏 . 审计数智化转型：核心要素、逻辑框架与实现路径 [J]. 财会月刊 ,2026,47(09):82-88.

[3] 朱冬玲 . 智能审计技术在企业财务管理中的价值跃迁 [J]. 中国商界 ,2026,(07):96-97.

**作者简介**：刘子夜 (1995.03—)，女，汉族，河北张家口人，硕士，讲师，主要研究方向为审计、公司治理。

刘琪琪（1998.10—）女，汉族，河北衡水人，硕士，讲师，主要研究方向为审计。

**项目信息**：河北工程技术学院校级课题，课题名称《人工智能审计场景下的数据隐私保护机制研究》，（立项编号 2025HG50）。