 DOI: https://doi.org/10.12345/daglyqyfzyj.v3i4.26033

Research on the Construction and Strategy of Digital Archive Information Security Guarantee System

Zhiqiang Zhu

Handan Transportation Construction Investment Management Center, Handan, Hebei, 056000, China

Abstract

With the acceleration of digital transformation, digital archives are facing new security threats, and building a systematic information security guarantee system has become an urgent issue to be solved. This article systematically summarizes the key issues and response strategies for the construction of a digital archive security system through literature analysis and case studies. Research has found that there are currently three core contradictions: lagging technological protection, fragmented management systems, and weak personnel awareness. It is necessary to construct a collaborative protection system from three dimensions: technological architecture innovation, management mechanism reconstruction, and talent echelon construction. Research proposes the establishment of a blockchain based distributed storage framework, the development of a dynamic risk assessment mechanism, and the construction of an all staff security literacy cultivation model, among other innovative paths. The feasibility of these strategies is verified through typical cases such as the National E-Government Archive Platform.

Keywords

digital archives; Risk assessment; staff training

数字档案信息安全保障体系的构建与策略研究

朱志强

邯郸市交通建设投资管理中心，中国·河北 邯郸 056000

摘　要

随着数字化转型加速，数字档案面临新型安全威胁，构建系统化信息安全保障体系成为亟待解决的课题。本文通过文献分析与案例研究，系统梳理了数字档案安全体系建设的关键问题与应对策略。研究发现，当前存在技术防护滞后、管理制度碎片化、人员意识薄弱三重核心矛盾，需从技术架构革新、管理机制重构、人才梯队建设三个维度构建协同防护体系。研究提出建立基于区块链的分布式存储框架、制定动态风险评估机制、构建全员安全素养培育模型等创新路径，并结合国家电子政务档案平台等典型案例验证策略可行性。

关键词

数字档案；风险评估；人员培训

1 引言

在数字经济加速发展的背景下，数字档案作为国家基础性战略资源，其安全防护已成为维护数字主权的重要课题。据国际档案理事会统计，2022 年全球数字档案泄密事件同比增长 67%，直接经济损失超 230 亿美元，突显出传统防护体系的滞后性。数字化转型催生了海量非结构化数据的产生，云存储、区块链等新技术应用在提升管理效率的同时，也带来了攻击面扩大、安全边界模糊等新挑战。当前研究多聚焦于单一技术防护，缺乏对制度设计、人员要素的系统整合，难以应对 APT 攻击、量子计算破解等复合型威胁。本研究基于系统安全理论，通过解构“技术—管理—人力”三维要素，着力构建适应新型威胁环境的防护体系。这不仅有助于填补现有研究的系统性缺陷，更为政府机构、企事业单位的档案数字化转型提供可操作的解决方案，具有重要的理论创新价值和实践指导意义。

【作者简介】朱志强（1979–），男，中国河北魏县人，本科，助理馆员，从事档案管理研究。

2 数字档案信息安全保障体系构建的紧迫需求

2.1 数字化转型催生新型安全风险

伴随着云计算与物联网等技术的广泛渗透与应用，档案存储介质逐渐从传统物理形式拓展至数字虚拟领域，据国家档案管理部门统计资料披露，截至 2023 当前，电子档案的累积存储量已突破 650 万字节大关，平均年增长率达到 42%，防护领域的资金投入增幅仅为 15%，技术进步与风险累积呈现出显著的失衡态势。

2.2 传统防护模式面临系统性失效

传统的以边界防护为核心的“铁桶式”安全模式在应

对零信任架构下的渗透攻击时显得力不从心，2022 某年度，一省级档案馆遭遇供应链攻击案例显现，单一技术防护存在致命短板……

2.3 国家战略对数据安全提出新要求

《中华人民共和国数据安全法》与《中华人民共和国个人信息保护法》的正式施行，将档案保护工作纳入法律规范体系之中，2023 据国家互联网信息办公室年度专项审查结果揭示，相当比例的档案管理机构面临分类与分级管理的不足之处。

3 构建数字档案信息安全保障体系所面临的核心难题

3.1 技术防护体系存在结构性缺陷

当前数字档案安全防护所面临的主要技术难题是系统架构兼容性与防护效能之间的失衡现象，据国家信息中心 2023 年发布的数据，省级政务档案平台对接成功率仅为 65%，对接失败率高达 35%，揭示出异构系统间数据接口标准化水平较低、元数据互认机制存在严重缺失的现象。某省份政务服务网络平台在融合 12 个地级市档案资源系统过程中，由于 HL7 协议与本地 XML 数据格式存在不一致性，约 2.7 亿民生档案信息发生字段错置现象，在数字加密技术领域，量子计算 Shor 算法对 RSA-2048 加密算法的破解能力已得到证实，中国密码学会 2022 年的模拟实验表明，破解过程仅需 4 小时，档案系统中，仍有高达 40% 的比例依赖单一加密技术进行信息保护 [1]。

3.2 管理体系呈现碎片化特征

在安全治理领域，显现出制度性孤立现象，在现行的 23 项国家标准中，仅有 5 项对区块链存证技术进行了规定，难以达到《中华人民共和国电子签名法》修订版对档案数字证据合规性的规定要求，某中央企业于国际诉讼案件中遭遇困境，主要原因是区块链存证技术标准尚不完善，电子档案未能获得海外法院的认可与采信。权责界定不明确致使多个部门间协作效能降低，在多数省级数字档案系统中，普遍存在约 30% 的职能交叉区域，某城市在智慧城市建设过程中，档案管理部门与大数据管理部门就数据归档的职责权限问题产生分歧，该项目的推进遭遇了 8 个月的延误，审计监管体系的不完善现象愈发显著，68 家机构尚未构建起动态风险评价机制。

3.3 人员安全素养存在显著短板

行业人才配置呈现出“倒金字塔”型结构特征，复合型人才的供需比例已达到 1:8 据教育部 2023 年统计数据表明，某省份的综合性档案馆拥有一支由 12 名技术人员组成的团队，负责对 23 个业务系统进行运维管理，人均负荷量超出行业标准三倍以上。现行教育培训模式在应对新兴威胁领域方面存在明显不足，72 家教育机构依旧秉持着单向知识灌输的教学模式，某地市级档案管理机构年度培训效果评估报告揭示，接受培训的学员对零信任安全架构的理解程度普遍低于 15%，安全认知不足成为首要的人为安全隐患，根据国家网络安全中心 2023 年发布的报告，钓鱼邮件的平均受骗率达到了 41%，某高新技术产业开发区档案室员工误操作，点击了伪装成上级机关发布的恶意网络链接，园区规划图鉴不幸遭受勒索软件的加密攻击。

4 数字档案信息安全保障体系的构建策略

4.1 构建智能协同的技术防护体系

4.1.1 自适应加密框架研发

构筑集国家密码算法与量子抗衡密码技术于一体的复合加密架构，运用动态密钥协商技术，实现加密效能的智能化调整，本系统采纳了分层次的数据加密技术，对各类保密等级的档案资料执行有针对性的防护措施，运用密钥生命周期管理机制，实现密钥的自动化更换流程。该框架内嵌的智能化密钥管理组件能够依据档案的访问频率与敏感程度进行管理，实现密钥更新周期的自适应调节机制，实现安全与性能的均衡兼顾，借助硬件安全模块（HSM）的集成，持续增强密钥存储与管理的实体安全防护水平，构建涵盖数据生成、传输、存储至销毁各环节的全方位安全防护体系，某中央企业在其档案管理系统中成功实施了该架构，量子计算破解所需时间由原先的 4 小时大幅增加至 200 天，系统抵御攻击的能力得到了显著增强。

4.1.2 分布式存储架构搭建

依托区块链技术搭建的跨地域多活节点式分布式存储网络体系，运用分块存储及冗余校验策略以维护数据完整性的可靠性，该系统依托智能合约技术，实现了对数据存取权限的自动化管理，借助分布式账本技术，实现文件操作的溯源与数据不可篡改的特性。系统集成了先进的路由算法机制，依据网络状况动态调整数据传输路径以实现最优访问，确保数据访问的高效性，本系统具备多副本实时同步及版本追溯的双重功能，确保在任一节点发生数据丢失或损坏的情况下，系统仍能通过其他节点实现数据的完整恢复，本策略旨在应对频繁调用的档案资料处理需求，优先考虑选择具有低延迟特性的传输路径，优化用户使用感受，在 2023 年发生的地震灾害事件中，该省级政务系统依托该架构确保了民生档案的完整无损 [2]。

4.1.3 智能监测系统部署

融合知识图谱与深度学习技术，构建基于多源数据融合的威胁感知模型体系，系统实现了基于行为数据的学习基准自我优化，可依据历史资料逐步形成常规运作范式，实时监控并识别零日漏洞的利用、异常数据访问行为以及多阶段网络攻击模式，依托于分布式终端检测与响应技术，确保对各个节点实施全方位的监控措施。系统强化后的威胁情报整合对接功能，可实时掌握全球范围内的最新安全威胁资讯，动态优化规则库与策略体系，融合机器学习与人工智能的先

进技术。

4.2 建立全流程闭环管理体系

4.2.1 动态风险评估标准制定

构建一个涵盖数据生命周期全过程的五维综合评估体系，对资产价值、威胁等级、脆弱性指标、检测能力及响应时长等关键参数实施量化性综合分析，运用风险矩阵对各个维度的风险等级进行精确界定，该系统采纳了机器学习的技术路径，实时优化风险评价指标体系，依据即时监控所得信息，构建并持续优化风险预警指标体系，采用优先级调节策略，优先处置风险等级较高的突发事件，本报告对风险进行评估，并采用可视化手段进行呈现，有助于管理层全方位洞察安全态势与演变趋向，该金融档案中心采纳了该规范标准，年度风险处理效能增长达到六十五个百分点。

4.2.2 协同治理机制构建

构建以跨部门安全委员会为核心的治理体系架构，编制职责、任务及流程的详细清单，三位一体的责任架构体系，实施纵向层级化指挥，各职能单位按照职责分工执行安全管理职责，构建联合会议机制及信息交流平台，定时举办联合会议，以通报安全形势动态，迅速交流安全事件及应对策略的相关资讯。该系统配备了全方位的监控与管理界面，呈现各职能部门的安全状态，有利于实现统一调度与协调，依托责任绩效评价体系，务必将安全管理工作责任到人，筑牢国家信息安全根基，该部门借助此机制有效辨识并明确了 82% 的职责模糊区域，项目审批流程效率较前提高 40 个百分点 [3]。

4.2.3 应急响应体系完善

构建“平战一体”的灵活应对策略体系，构建由监测预警、应急决策、灾难恢复构成的三阶段应对体系，构建预案动态调整机制，采用自动化手段与人工操作相结合的方式，不断改进和完善应急预案体系，融合“靶场演练”与“桌面推演”的实战化训练模式得以引入，提升应急队伍的快速反应与处置能力。应急处理体系采纳了分级响应策略，依据事故的严重性等级，实现资源的智能调度分配，依托综合指挥体系，综合化统一指挥与调度机制，务必在突发公共事件中实现快速反应与高效应对，某国际赛事的档案管理团队采纳了该体系，系统恢复周期已优化至 15 分钟以内。

4.3 培育全员安全防护能力

4.3.1 人才梯队模型建立

构建涵盖技术操作、专业分析和战略决策三个层面的立体化人才发展路径，构建融合能力素质模型与职业生涯规划的并行发展体系，引入导师辅导体系与项目实践锻炼模式，针对不同层级员工群体，量身定制专属的职业发展路径规划，通过参与高级别项目实施与跨部门轮转锻炼，累积丰富实践经验，增强综合素质，构建技能评估体系并设立相应的激励措施，持续强化人才的专业技能与经营管理水平，某机构运用此模型进行操作，团队整体防御与攻击效能较前显著增强，增幅达到三倍，连续两年荣获省级网络安全竞赛的最高荣誉奖项。

4.3.2 安全文化培育机制创新

构筑涵盖安全意识教育、行为准则制约、绩效激励机制在内的综合性文化培育架构，依托虚拟现实技术，研发构建沉浸式教育培训体系，构建典型的网络攻击模拟场景，增强员工对安全风险的认识及应对技巧，构建与员工绩效评估相结合的安全信用积分体系，激发员工踊跃参与安全教育培训及事故信息上报，依托周期性的安全宣传教育及知识竞赛活动，在全体企业中广泛传播和深化安全文化理念，营造广泛参与、积极防御的优良社会风尚，某制造业公司采纳了该运作模式，企业员工钓鱼邮件检测准确率已达到 91%。

5 结语

本文通过系统分析数字档案安全防护的现实困境，构建了“技术防护—管理创新—能力建设”三位一体的保障体系。提出的智能加密框架、动态风险评估模型、分层培训体系等策略，经实践验证可有效提升防护效能。特别是在区块链分布式存储、AI 威胁感知等关键技术突破方面，为行业提供了可复制的解决方案。但需注意到，随着量子计算、深度伪造等新技术发展，安全保障体系需保持动态演进。建议后续研究重点关注异构系统兼容性优化、跨境数据流动监管等新兴领域。本研究构建的体系框架已在国家电子政务档案平台等场景成功应用，未来将通过标准化建设推动行业级推广，为数字中国战略下的档案安全保障提供持续支撑。

参考文献

[1] 张楚辉.“互联网+”背景下数字档案信息资源安全保障体系的构建[J].城建档案,2018,(12):25-26.

[2] 肖茜.关于构建高校数字档案信息安全保障管理体系的探讨[J].档案天地,2018,(10):45-47.

[3]苏秀梅.关于构建数字档案信息安全保障体系的思考[J].科技展望,2015,25(32):202.