数字档案馆风险识别与安全管理方法探索
——评《云数字档案馆安全风险评估研究》

数字档案馆作为一种利用现代技术手段,承载文化遗产与机构记忆的核心基础设施作用越来越凸显,但同时也正面临着数据异构化、系统开放化与威胁动态化等安全挑战。数字档案馆的传统安全防护体系难以应对复合型网络攻击、数据篡改风险及隐私泄露隐患,尤其在云计算与人工智能技术深度融合背景下,数字资产的全生命周期安全管理亟需构建风险识别与防控体系框架。

《云数字档案馆安全风险评估研究》立足档案信息化发展前沿,以风险管理理论为基点,揭示了云数字档案馆安全风险的生成机制与演化特征。作者通过构建组织保障、业务管理、信息服务、技术实现四维风险评估指标体系,创新性地提出基于层次分析法与模糊评价模型的风险量化评估方法,形成覆盖风险识别、度量、预警的全流程管控机制。作者突破性地将生态系统理论引入档案安全研究领域,阐明云数字档案馆多主体协同、多要素耦合的复杂安全图景,并有针对性地设计出适配云环境特征的风险评估模型与判定标准。研究不仅完善了数字档案馆风险管理理论体系,更通过实证导向的指标权重测算与规范设计,为档案部门构建云上安全防护体系提供了可操作的技术路径。

书名:云数字档案馆安全风险评估研究
作者:徐华,薛四新
出版社:中国社会科学出版社
ISBN:9787520397797
出版时间:2022年2月
定价:76元

作者指出,数字档案馆的核心价值在于其承载信息的原始性与真实性,而数据篡改风险直接威胁这一根本属性。篡改行为不仅破坏档案的证据效力,更可能引发法律纠纷与信任危机,其技术本质在于数字对象的可编辑性与元数据完整性的脆弱性,需构建多层次防护体系。在技术防护层面,应采用基于密码学的完整性验证机制。通过数字签名技术对档案对象进行哈希运算,生成唯一标识符并与原始记录绑定,形成不可篡改的"数字指纹"。在管理策略方面,应实施严格的访问控制与审计机制。基于角色的访问控制模型细化权限颗粒度,将档案操作权限分解为读取、修改、删除等独立权限项,并建立最小特权原则下的动态授权机制。同时,构建三维审计体系,即操作审计记录用户行为的时间、对象与动作;内容审计通过差异比对工具自动检测档案变动;系统审计监控底层存储介质与网络传输的完整性。持续监控机制是风险管理的重要补充,需部署入侵检测系统,实时分析网络流量与系统日志,通过异常行为模式匹配识别潜在篡改尝试。结合人工智能技术构建行为基线模型,对用户操作习惯进行机器学习,实现偏离基线行为的自动告警,并定期开展渗透测试与红队演练,模拟真实攻击场景验证防护体系的有效性,形成"检测-响应-改进"的闭环管理流程。

笔者认为,数字档案的长期保存面临技术迭代、载体衰变与格式过时的三重挑战,构成独特的持续性风险,这一风险本质是数字档案生命周期管理中的技术异化问题,需建立前瞻性的保存策略体系。技术架构层面,应采用开放格式与标准化封装,优先选择国际标准化组织认可的非专有文件格式,如PDF等,确保内容与呈现的分离性。实施开放档案信息系统参考模型,构建包含提交信息包、存档信息包和分发信息包的标准化封装结构,通过元数据规范描述档案的技术特征与依赖关系,亦可采用通用磁盘格式等载体无关的存储规范,减少硬件依赖性。载体保护需贯彻"3-2-1"原则:保持3份数据副本,存储于2种不同介质,其中1份异地保存。结合磁带库、光盘库与云存储的优势,构建分级存储体系。对磁介质实施周期性再生迁移,通过专业设备检测磁性衰减并执行数据刷新;对光存储介质采用环境可控的冷存储方案,维持恒温恒湿条件;云存储服务需选择符合ISO 27001认证的提供商,并通过加密传输与分片存储保障数据主权。格式迁移管理是应对技术过时的核心机制,要求建立格式注册表与转换规则库,定期评估主流文件格式的市场占有率与技术发展趋势。采用无损转换工具保持内容与结构的完整性,对复杂格式(如CAD、多媒体文件)实施仿真迁移策略,通过虚拟化技术保留原始运行环境。持续维护体系应包含定期完整性检查与可访问性测试,通过校验和比对验证数据一致性,利用格式识别工具检测文件异常,且建立技术环境观察站,跟踪操作系统、播放器等依赖软件的版本演进,提前部署兼容性测试环境,最终形成由技术标准、管理流程与保障机制构成的立体化防护网络,实现数字档案从当前可读到未来可解的跨越。

总之,基于数字档案馆安全风险的作用机制,可构建覆盖技术、管理、法律多维度的动态防控框架,实现从风险识别到长效治理的闭环,保障数字档案产业可持续健康发展。

(陈晋/黑龙江省中医药科学院/副研究员)