

档案馆数字资源安全管理体系设计与能力建设

秦哲君

拜泉县退役军人服务中心 黑龙江 齐齐哈尔 164700

摘 要：数字资源易于被复制、传播且具有较高的使用价值，在极大方便档案利用的同时也给档案馆带来前所未有的安全隐患。数据泄露、篡改、破坏甚至无法访问等都对档案的真实性、完整性、可用性和保密性构成严重威胁从而影响了档案的凭证作用以及历史传承的功能。因此，建设符合档案管理工作需求的数字资源安全保障机制并提高相关能力是新时代下档案事业发展的客观需要。本文基于档案学的基本观点，梳理了档案馆数字资源所面临的各种安全问题并提出了以“三重防护”的思想为基础，从制度、技术、管理和应急预案四个方面建立起一套完整的安全保障体系以及相应的能力建设措施以供国内各层级不同类型档案馆在进行数字化的过程中保护好自身的数字资源使其长期可信并且可使用。

关键词：档案；数字资源；安全管理体系；能力建设；档案安全

引言

数字化极大丰富档案的服务内容和服务效能，但同时也带来隐蔽性强、传播迅速、波及面广并且难以挽回的风险，比如勒索病毒、APT 攻击、工作人员失误或者设备故障等现象时有发生，而以往以发生后进行补救为主的防护方式显然已经不能适应形势发展变化的要求。档案馆所保存的数字资源除了具有普通数据的一般性质之外，还担负着保持档案真实性、证明力以及法律有效性的重要任务，一旦遭受破坏，会造成无法弥补的历史数据丢失和社会信任危机。因此，档案馆亟须建立覆盖整个数字资源生命周期的安全保障机制，这种保障机制要符合档案管理工作的要求，包括政策法规、技术和管理措施以及应急预案等方面内容，并配备相应的人力资源、专业技术力量以及工具设备等。对此进行探讨具有重大的理论意义和现实意义。

1 档案馆数字资源安全面临的挑战与风险分析

1.1 技术层面的脆弱性

档案馆数字资源的存储、管理和流动都离不开信息系统的支持，但是这些信息系统本身也有自身的不足之处。操作系统的缺陷、数据库或者中间件等底层软件中存在的未知的安全隐患（如 0day 漏洞），如果被黑客所掌握，则可以作为攻击点；云服务以及容器化虽然提高了资源使用的效率但也增加了暴露面以及对配置进行管理的难度。同时，档案数字资源还有一种特有的长期可读性的威胁叫作“数字黑暗时代”。如果不及时地进行格式转换、迁移或者仿真，即使数据载体完好无损，但

是在将来由于技术的变化也有可能无法阅读，造成档案信息事实上丢失的情况发生，而这种损失是比不上传统的纸质档案具有长久保存性的。因此档案馆需要把技术预见性考虑进安全保障中去。

1.2 网络空间的威胁态势

档案馆信息系统已普遍连接到互联网以及政府部门或者行业的专网，面临着越来越严重的网络安全问题。一些外部攻击者为了获利（例如勒索）、政治目的（例如获取机密的历史档案）或者其他原因，经常把档案馆视为他们的攻击对象。这些攻击方式有传统的病毒、木马，也有更为隐秘持久的 APT 攻击、使用社会工程学的方法进行鱼叉式网络钓鱼等^[1]。供应链安全也是一大问题，第三方软硬件供应商或者服务商的安全问题可能会给档案馆系统带来侧门进入的机会。而且更重要的是，档案数字资源的价值及其独特性使它们比一般的资料更容易受到高级持续性威胁的关注。

1.3 内部管理与人为因素

“堡垒最容易从内部被攻破”，内部威胁是档案馆数字安全最大的隐患。这既包括由于缺乏安全意识或者能力而做出的一些不当行为，比如误删除档案资料、错误设定权限、使用简单密码等；也包括一小部分人有意为之的数据窃取、篡改或者破坏。档案管理工作当中包含大量的机密信息和个人隐私等内容，在职员工有意为之的危害极大。而且管理上的漏洞例如缺少适当访问控制、权限分配混乱、无审计日志等都会使内部威胁加剧。档案单位所具有的多工种合作、长期保存的特点也

让权限管理以及行为审计变得更加困难。

1.4 法律法规与合规压力

国内外对数据安全和个人信息保护方面的立法日趋严格。我国《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等相关法律法规均对包括档案馆在内的所有数据处理者提出相应规定与要求。而作为负责保管历史文献资料并提供社会服务的单位,档案馆在进行数字化过程中更要保证其行为合法性,在涉及个人隐私、国家机密或者企业商业机密档案管理上面临的挑战更大,另外,《中华人民共和国档案法》以及《档案法实施办法》还就档案的真实性、完整性和可用性及保密问题做出特别说明。如果不合法不但会受到法律制裁而且会影响自身形象,也会使人们不再相信这个档案馆。

2 档案馆数字资源安全管理体系设计框架

依据“三重防护”理念(制度为纲、技术为基础、管理为关键),档案馆数字资源安全管理框架可以是一个由四个密切联系的部分构成的整体。这个框架以“保证数字档案的真实性、完整性和可用性以及保密性”为宗旨,分为四个部分分别是:(1)制度规范层:是基础部分,包括安全策略、规定、技术规范以及操作手册等,需要包含档案行业相关标准;(2)技术防护层:是核心部分,包括物理与环境安全、网络安全、主机安全、应用安全、数据安全以及备份恢复等,主要关注档案数据长久的安全问题;(3)管理运维层:是神经中枢,负责安全威胁分析、监控、人员管理、供应链管理和安全审计等工作,在档案工作中加强安全控制;(4)应急预案及不断优化层:是韧带,当出现安全事故时可以第一时间进行处理并且事后反思总结提高自身安全性。

3 安全管理体系的核心内容设计

3.1 制度规范层设计

制度规范层面是安全管理体系中的“宪法”,需要由上至下设计。一是要出台《档案馆数字资源安全总纲》,对安全工作提出总体要求、基本原则、机构设置以及各部门职责划分等,特别是要强调档案 RAID 原则实施情况;二是要有一系列一级规章制度,例如,《数字档案访问控制管理办法》《信息系统安全运维规程》《数字档案分类分级与保护办法》《安全事件应急预案》《第三方服务机构管理规定》等;三是对于每一个具体的操作都应有具体的标准作业程序(SOP),比如用户账号申请、数据备份、系统补丁升级等,以便做到操作有章可循;四是还要对这些规章制度定期检查

和改进制度,随着新技术出现以及档案工作的发展,不断对其进行完善^[2]。所有的制度性规定都要经过档案业务人员审阅,保证其符合档案管理工作基本标准。

3.2 技术防护层设计

从物理和环境安全角度出发,保证机房、档案库房等重要区域的安全,避免未经授权进入,安装消防、防水、防雷、温湿度监控等设备,保证档案数字资源载体所处环境的安全稳定。在网络层面,部署下一代防火墙(NGFW)、入侵检测/防御系统(IDS/IPS)、网络流量分析(NTA),划分不同区域,严格控制网络访问权限。对于主机与应用的安全问题,做好服务器、客户端等安全配置及补丁更新工作;做好档案管理系统等重要软件的安全检查以及漏洞测试,防止针对 Web 应用的攻击。数据安全最为重要,在整个生命周期中都应该受到充分重视:在收集时对涉及隐私的档案内容进行脱敏操作;在保存时使用高安全性加密方法(比如国密算法)对静止的数据进行加密;在传输过程中采用 SSL/TLS 等手段保护正在移动的信息;在使用时根据具体需求采取基于角色(RBAC)或者基于属性(ABAC)的访问控制方式^[3]。同时还需要建立健全的数据备份与恢复制度,在出现故障或者遭受攻击的情况下可以及时恢复档案数字资源并且定期进行恢复演练来检验备份的有效性。另外还要考虑到档案格式在未来仍然可以被读取的问题,定期对其进行评估并采取相应的转换或者模拟措施。

3.3 管理运营层设计

一方面要形成常态化安全风险评估机制,定期对信息系统、业务流程以及外部风险源进行检查,及时调整相应的安全防护手段及资源;另一方面需要设立专门的安全运营中心(SOC),对所有网络设备、日志以及用户的操作行为进行 7×24 小时监控、分析并预警,使安全管理更加直观,特别是对档案数据库和档案管理系统中的可疑活动给予高度关注。同时还要做到人人有责,做好人员背景调查和安全教育,按需分配最小权限,同时加强对账户的生命周期管理。档案管理部门还应更加重视对接触重要档案或者涉密档案的工作人员实行双人复核、岗位分离等制度。此外还要注意防范供应链安全风险,在选择第三方服务商时要对其安全情况进行严格考察,在签订合同时也要把安全条款写清楚,并对其所提供的产品进行安全测试以避免因为供应链问题而导致档案系统被植入木马或其他安全隐患。

3.4 应急响应与持续改进层设计

没有一劳永逸的安全防护,必须具备强大的应急响应

应能力和持续改进机制。一是应急响应：依据《安全事件应急响应预案》组建专业应急队伍。预案需明确针对不同类型网络安全事件（如数据泄露、勒索软件攻击、DDoS 攻击、档案篡改等）的处置流程、方法和联系人。定期开展应急演练，检验预案可行性并提升人员技能。特别要针对档案数字资源被加密或删除的场景设计专项演练，确保能够从备份中恢复完整、可用的档案内容。二是持续改进：每次发生安全事件或完成风险评估、审计后，均需进行详细的复盘总结（Post-Mortem），分析问题根源，并据此优化制度、技术和流程，实现安全管理水平的螺旋式上升。同时，建立档案数字资源安全知识库，积累案例和经验，形成组织记忆。

4 安全能力建设的关键路径

4.1 强化组织保障与领导力

档案馆应当设置专门的信息安全管理机构或者任命首席信息安全官（CISO），并由其向馆领导班子负责，具有决定权和资源调配权。馆领导班子应充分认识到数字安全对于档案工作的重要性，把数字安全列入档案馆的发展规划并提供必要的经费和其他方面的支持^[4]。“一把手”重视，才是做好这项工作的前提条件。此外，还要有跨部门的合作机制，在档案业务部门、技术部门以及保密部门之间进行有效的沟通与合作。

4.2 构建专业化人才队伍

档案馆一方面要积极引进或培养熟悉网络安全、数据安全、密码学及档案信息化技术的人才；另一方面要对所有档案工作人员进行分层次、分类别的定期培训，让管理者、技术人员、普通职工都了解自己所在岗位的安全要求，做到“人人都是安全员”。特别是要提高档案人员对 RAID 的理解以及在其业务中保护档案凭证性的认识。还要有必要的奖励与惩罚措施，以吸引优秀安全人才留在单位并且不断发展。

4.3 推动先进技术的融合应用

从技术能力方面来看，在技术选择上要根据实际情况量力而行，不能一哄而上。可以借鉴零信任（ZeroTrust）的思想改变档案馆网络访问模式，“永不信任，始终验证”，从而提高对档案系统的访问控制级别。通过人工智能（AI）、机器学习（ML）来识别大量的日志以及异常活动，做到智能的安全告警及防护。研究区块链技术用于保证档案元数据不可被篡改、建立可信存证链的作用，使档案数字资源具有法律效力。还要研究长期保存技术比如数字仿真、格式规范化转换等以防出现“数字黑暗时代”。技术的应用应符合档案工作需要，不能盲目。

5 结语

档案馆数字资源安全是关乎国家历史记忆保存完整性、文化自信根基及数字政府公信力问题。在日益复杂严峻安全环境下，建立基于“三重防护”基础上，包含制度、技术和管理与应急处置等方面内容并能够不断完善档案馆数字资源安全管理体系，已不是选择题，而是档案工作现代化必然要求。本论文提出思路是为了给档案馆提供一条思路：安全并非一个单位责任或一次投入就可以做到万无一失，而是一个需要全体人员共同参与、长期坚持、不断发展过程。只有让安全成为档案馆一种自觉意识和行为习惯，在这信息爆炸时代，才能保护那些记载过去、当下甚至未来珍贵数字档案不会消逝，从而服务于中国式现代化建设。

参考文献

- [1] 常愉. 档案馆数字资源安全管理体系设计与能力建设[J]. 山西档案, 2025, (12): 103-105.
- [2] 高康. 数字档案馆(室)建设中数据安全与隐私保护机制研究[J]. 办公室业务, 2025, (24): 100-102.
- [3] 刘殿强. 数字化转型背景下数字档案馆(室)的安全防护体系构建研究[J]. 兰台内外, 2025, (34): 36-38.
- [4] 杨鹏, 金波, 顾安清. 数字档案馆生态系统安全治理研究[J]. 图书情报工作, 2025, 69(14): 15-27.