档案信息安全面临的风险及对策

薛春晓
（山西省吕梁市汾阳市杏花村镇人民政府 山西 吕梁 032200）

摘 要 文中综合分析了档案信息安全的特征、面临的主要风险以及有效的防护对策。通过深入探讨档案信息的完整性、可用性和可追踪性，指出了档案信息在介质、信息、环境等方面面临的安全风险。针对这些风险，提出了提高安全防护意识，应用安全防护技术，创设安全防护环境，健全安全防护制度等对策，旨在为档案信息安全管理提供实用的参考和建议。

关键词： 档案信息安全；风险分析；防护对策
中图分类号 G271

Risks and Countermeasures Faced by Archive Information Security

XUE Chunxiao
（People's Government of Xinghua Village,Fenyang City,Lvliang,Shanxi 032200,China）

Abstract This paper comprehensively analyzes the characteristics of archival information security,the main risks faced and effective protection countermeasures. Through in-depth discussion of the integrity, availability and traceability of archival information,the security risks faced by archival information in media,information and environment are pointed out. In response to these risks,countermeasures such as improving security awareness,applying security protection technology,creating a security protection environment,and improving security protection systems are put forward,aiming to provide practical reference and suggestions for archival information security management.

Key words Archive information security,Risk analysis,Protective measures

0 引言

随着信息技术的快速发展，档案信息安全逐渐成为社会关注的焦点。档案信息作为历史和文化的载体，不仅承载着重要的数据和信息，还承担着传承文化，指导未来的重要任务。然而，随着技术的进步，各种安全风险日益增加，这对档案信息安全提出了更高的要求。本文旨在通过分析档案信息安全的特征，识别存在的安全风险，以提出有效的防护措施，为档案信息安全管理提供指导和帮助，确保档案信息的安全性和完整性。

1 档案信息安全的特征

档案信息安全是档案管理领域的重要工作，其核心在于确保档案数据的真实性、完整性、可用性和可追踪性。在数字化时代，档案信息安全不仅涉及传统的纸质档案，也包括电子档案。电子档案的安全保护关键在于确保档案数据的四性检验，避免病毒或非法人员的侵害，同时保障档案数据安全、可靠地传输与存储。

1.1 档案信息的完整性

档案信息的完整性是档案管理的核心要素，其意义在于确保档案资料在保存、使用过程中的真实性、可靠性和连续性。完整性的核心在于防止数据在未经授权的情况下被篡改、破坏或丢失[1]。此外，档案信息的完整性不仅关系到信息本身的准确性和可用性，还直接影响着信息的法律效力和历史价值。

在档案信息管理中，维护信息完整性的举措涵盖多个方面，其首要任务是确保档案材料在收集、存储、检索、传输、利用等各个环节中的安全性和准确性。对于电子档案而言，技术手段的应用尤为重要。例如，通过加密技术保护档案数据，不仅可以防止未经授权的访问，还能有效避免数据在传输过程中被篡改；数字签名技术则能确保数据的来源和完整性，使档案材料在法律和行政程序中具有更高的可信度。

在实践操作中，维护档案信息的完整性是一个持续的过程。随着技术的进步和管理方法的发展，档案管理者需要不断更新和完善保护档案完整性的方法和技术，确保档案资料能长期、稳定地服务于研究、决策和社会公众。同时，档案工作人员的专业素养和责任感也是确保档案信息完整性的重要因素。通过专业培训和实践经验积累，可提高档案工作人员在档案管理、风险识别和应对等方面的能力，是提高档案信息保护水平的关键。

作者简介：薛春晓（1982—），本科，研究方向为乡镇档案管理。

1.2 档案信息的可用性

档案信息的可用性指确保档案中的数据能及时、有效地被授权用户访问和利用。这不仅可以促进数据的高效检索及应用，还能增强档案管理系统的服务能力，提升数据的使用价值和工作效率。通过构建完备的电子档案管理体系，实现档案信息的智能化分类和快捷检索，可凭借几个关键词快速锁定关键信息，极大地提升数据的可访问性和操作便捷性[2]。

在该过程中，必须考虑信息安全和使用效率的平衡。划分数据访问层级与权限控制，精心设计权限分配流程，可确保不同级别的档案信息被相应的人员有效调阅。同时，需经常开展数据备份和灾难恢复演练，成立专门的数据管理团队，以负责备份工作，采用先进的存储技术，如云存储和远程备份，确保数据在系统崩溃或其他突发事件中仍能快速恢复，从而确保档案信息的可用性、稳定性和可靠性。

1.3 档案信息的可追踪性

档案信息可追踪性的重点在于确保档案数据的变更和操作都能实现准确的记录和溯源。这一特性对于防御安全威胁、辨识数据操作异常及维护数据的完整性和可靠性至关重要。在电子档案管理系统中，实施细致的数据操作日志，能追踪档案信息的查阅、编辑、传输、分享等操作，确保每次操作的透明度和可追踪性。

若想实现档案信息的高效追踪，则必须引入和融合尖端的技术工具与严格的管理措施。区块链技术正是这方面的典型应用，可通过其分布式账本的特性为每次数据操作提供时间戳和数字签名，确保记录的真实性和不可篡改性。同时，必须建立覆盖广泛的安全审计体系，对所有操作进行全面的监控，自动记录并保存修改、删除、新增等操作的详细信息。

2 档案信息安全面临的主要风险

在现代化管理中，档案信息安全面临着多方面的风险。这些风险不仅威胁着档案数据的安全性和完整性，还可能影响到档案信息的有效利用。本文详细分析了档案信息安全面临的主要风险。

2.1 介质安全风险

数字档案信息的介质安全是保障信息持久保存的重要条件，各种媒介的科技特性尤其关键。在选定存储介质时，需综合考量档案信息的可靠性、可用性、保护级别等。以光盘为例，档案级别MDISC采用无机材料，突破了普通光盘容易衰退的限制，降低了环境对数据的影响，赋予了档案百年甚至更长久的生命。同时，使用ISO/IEC 10995标准，即使在极端情况下，也能确保BLER（块错误率）处于可接受范围，持久保护档案信息的完整性。

闪存驱动器的进步也不容忽视。SanDisk Extreme Pro USB 3.1闪存驱动器强调读写速度与安全性，TLC NAND芯片配合AES 256位硬件加密，使得存储设备在提供快速的数据访问功能的同时，还能防范未经授权的入侵。其坚固的铝质外壳设计可抵御物理损坏，对移动存储介质进行了全面考虑[3]。

NAS系统对于扩展性和持久性十分重要，RAID配置在提供存储冗余的同时，也具有灵活性。例如，Synology NAS不仅能满足用户对存储空间的需求，在单个硬盘故障时也能保证数据的完整性，其可利用SHR技术优化存储，有利于数据庞大的档案系统的维护。

云存储标志着存储技术的新纪元，在AWS S3，Azure Blob Storage，Google Cloud Storage等云服务中，数据的多区域复制与自动加密为存储安全设立了新的标准。例如，某大型律所利用AWS S3来备份客户资料，其高达99.999%的耐久性和数据生命周期管理功能，体现了云存储在现代档案信息管理中的不可替代。

2.2 信息安全风险

在数字化浪潮的席卷下，信息安全风险时刻威胁着档案信息的安全。尤其是面对日趋复杂的网络威胁，如何构造安全屏障成了信息安全管理的核心挑战。入侵预防系统（IPS）的引入，保障了档案信息安全系统，它通过实时监测数据流，有效阻绝了潜在的入侵企图，提升了安全防护系统的主动性和智能性。

随着安全防护技术的发展，蜜网策略（Honeypot tactics）逐渐占据一席之地，它诱使攻击者陷入一个受控的网络环境中，有效分散了攻击者对真实系统的影响。在此基础上，区块链技术的引入为信息的真实性与不可篡改性提供了新的保障。数据一旦经过链上时间戳认证，其原始状态就会被牢牢锁定，保证了档案信息的原真性。

在应对不断变化的网络威胁时，端点检测和响应（EDR）解决方案日益重要。它通过在各终端收集与分析安全威胁信息，使得对于病毒、恶意软件的防护不仅限于识别和阻断，还能深入追踪与快速响应攻击行为。例如，某金融机构通过部署EDR，成功抵抗了一场精心策划的网络攻击，充分展现了ESR在数字资产保护中的作用[4]。

2.3 环境安全风险

档案信息安全不仅会受网络环境的影响，也会受自然和人为环境因素的影响，如火灾、洪水、操作失误等都可能对信息安全构成威胁。面对这些风险，技术与策略的结合为档案信息提供了另一层保障。在实际应用中，基于物联网技术的智能监测系统能适应各种环境，及时感应并预警如温度、湿度的异常变化，防范灾难的发生。

自动化的紧急响应程序已成为现代档案信息系统的重要组成部分。例如，一旦检测到火灾预兆，这些系统就能即刻激活消防系统，尽可能降低损失。在人为风险预防中，持续的培训与演练是减少操作失误的有效手段。例如，国立档案管理局通过定期的安全培训和模拟演练，使得每名工作人员都意识到自己在预防环境风险中的角色与责任，极大地提高了单位的整体应对能力。另外，将业务连续性规划（BCP）和灾难恢复规划（DRP）纳入日常管理实践，即便在不可预测的环境事件面前，档案信息管理系统也能迅速恢复运行。

通过这些技术和策略的融合，档案信息的环境安全防护得到了全方位的加固，即使在不利环境中，也能最大程度地减少损失，保障档案信息的安全性和完整性。

3 档案信息安全防护对策

维护档案信息安全，需要应用较为全面的策略和措施，如提高安全意识，应用先进技术，创设安全环境，建立完善的制度等。

3.1 提高安全防护意识

提高档案信息管理中的安全防护意识，是一个多层面、综合性的任务。在信息技术快速发展的背景下，档案信息安全受到多方面的挑战，提高安全意识尤为重要。组织需要定期举办针对性的安全知识培训，增强工作人员对档案信息保护的认识和理解。培训内容应涵盖信息安全的基本概念、网络威胁的识别以及防范网络攻击的策略。此外，还应强调个人和组织在维护信息安全方面的责任和义务，确保每位员工都能在日常工作中实践这些安全措施。通过这样的全面教育和实践，可有效提升整个组织在信息安全方面的防护能力，降低潜在的安全风险。

3.2 应用安全防护技术

引进和应用先进技术，是维护档案信息安全的关键因素。随着技术的不断进步，新的工具和方法不断出现，以加强档案信息的安全防护[5]。(1)机器学习和人工智能技术的整合，能帮助组织有效预测和防御持续性威胁(APT)。通过大数据分析，这些系统可以从海量数据中识别出异常模式，提前遏制安全威胁。(2)加密技术在档案信息安全中起到了至关重要的作用。现代加密算法，如 Elliptic Curve Cryptography(ECC)提供了强大而高效的加密手段，即使在计算资源受限的环境中，也能保证信息的保密性和完整性。(3)安全套接层(SSL)和传输层安全(TLS)协议的普及，确保了数据在传输过程中的私密性，有效预防了中间人攻击和数据劫持。

为实现更全面的安全策略，不断更新的技术标准(如 ISO 27001信息安全管理体系)已成为许多组织确立其信息安全措施的基石。这些标准不仅仅涉及技术层面，还包括政策、过程和人员方面，不断提升着档案信息系统的安全保护水平。通过积极应用这些先进技术和符合行业标准的体系，档案信息系统的安全性能得到有效加强，并为组织提供更强大的对抗信息风险的能力。

3.3 创设安全的防护环境

构建安全的防护环境，核心在于兼顾实体与虚拟两个领域。对物理层面而言，必须构建严密的物理访问控制系统，以确保档案存储地点的安全性。具体措施如下。(1)设计与建设恒温、恒湿的库房，满足冷却系统持久、稳定运行的硬性要求，保障档案免受极端温湿度变化的侵害。(2)落实全面防尘措施，包括高效过滤装置的安装与常态检查，避免灰尘微粒对档案的潜在损害。(3)建设防灾设施，确保档案在各类灾害情形下的安全性。

对网络层面而言，应围绕信息技术安全体系展开，重点如下。(1)选配与部署高效能的防火墙软件，强化对网络边界的防护，有效拦截恶意的网络入侵行为。(2)更新操作系统与应用软件，以修补安全漏洞。(3)定期进行网络安全演练与评估，通过模拟攻击场景来检测和强化网络防护体系的响应机制。

3.4 健全安全防护制度

安全防护制度是保障档案信息安全的坚实基础。依照《档案法》《保密法》等相关法律法规，并考虑具体的实际操作需求，组织机构应设立专门的档案信息安全防护工作领导小组。该小组的职责包括制定和执行一系列具体且有针对性的安全防护方案。制度管理的范畴较为广泛，包含身份验证、访问异常监控、信息内容的安全传输与下载等，旨在确保档案信息在整个处理流程中的安全性。

鉴于档案信息的多样性及其敏感程度，档案管理部门必须根据不同档案的保密级别实施相应的管理措施。这些措施应能全面、有效地覆盖档案信息安全管理的各个方面，确保每一环节都不出现安全漏洞。此外，应着重强化定期的安全审计和风险评估工作，通过这一过程，有效识别并及时解决安全防护体系中可能存在的漏洞和隐患。

为促进安全防护制度的不断完善，还应重视培养相关人员的安全意识。组织内部需定期开展有关档案信息安全及法律法规的培训，增强员工对安全防护的重要性的认识，并明确每位员工在维护信息安全中应承担的职责。通过建立健全的激励和问责机制，形成强有力的安全防护文化，进一步保障档案信息安全管理工作的落地执行，以适应不断变化的信息安全环境与挑战。

4 结语

档案信息安全是维护社会信息化健康发展的重要条件。本文全面分析了档案信息安全的特性、面临的风险和防护对策，指出了在现代信息化背景下，档案信息安全管理面临的复杂挑战。为保障档案信息的安全性，需要从提高安全防护意识，应用安全防护技术，创设安全防护环境，健全安全防护制度等多个方面进行综合施策。通过这些措施，可有效防范和减少安全风险，确保档案信息的完整性、可用性和可追踪性，促进档案信息安全管理的科学化、规范化。

参考文献

[1] 曹瑞萍.“十四五”时期档案信息安全管理面.的风险及应对策略[J].机电兵船档案，2023(3)：28-30.

[2] 陈万，王曙霞，刘震.浅析U盘病毒的攻防策略[J].电脑与电信，2019(3)：74-75，77.

[3] 姜峰.浅谈U盘和移动硬盘的使用与维护[J].中国现代教育装备，2019(7)：45-47.

[4] 宋艳红，程乐.基于云盘技术的高校档案管理系统设计[J].信息与电脑，2020(14)：97-99.

[5] 胡雪飞.电子档案信息安全管理初探[J].机电兵船档案，2020(4)：59-60.