档案信息安全防护技术应用与管理策略

陆丽忠

上海微小卫星工程中心，上海市，201304；

摘要：本论文聚焦于档案信息安全防护技术的应用与管理策略。首先阐述了档案信息安全的内涵和重要性，介绍了常见的安全防护技术类型。接着详细探讨了数据加密技术和访问控制技术在档案信息管理中的具体应用。分析了当前档案信息安全防护技术应用在技术和管理层面面临的挑战与不足。针对性地提出完善安全管理制度、加强人员培训与教育等管理策略。旨在为提升档案信息安全水平提供理论支持和实践指导，保障档案信息的完整性、保密性和可用性。

关键词：档案信息安全；防护技术；应用；管理策略

DOI：10.69979/3041-0673.26.01.084

在数字化浪潮席卷的当下，档案信息作为承载个人、企业乃至社会关键数据的重要载体，其价值愈发显著。但伴随着信息技术的迅猛革新，档案信息正遭遇网络攻击、数据泄露等多重安全隐患的挑战。如何强化档案信息安全防护技术的运用与管理，已然成为守护档案信息安全的核心要务。本文聚焦于深入剖析档案信息安全防护技术的实际应用状况，梳理其中存在的现实问题，并从管理层面探索切实可行的应对策略，力求为档案信息在复杂多变的网络环境中构建起坚实的保护屏障，确保这些重要数据能够得到妥善的保存与防护。

1 档案信息安全防护技术概述

1.1 档案信息安全的内涵与重要性

档案信息安全是指确保档案信息的完整性、保密性和可用性[1]。完整性意味着档案信息在存储和传输过程中不被篡改，保持其原始状态。保密性则要求档案信息仅被授权人员访问，防止敏感信息泄露。可用性保证档案信息在需要时能够及时、准确地被获取和使用。

档案信息安全具有极其重要的意义。对于个人而言，档案包含了个人的隐私信息，如医疗记录、教育背景等，保护这些信息安全是保障个人权益的基础。对于企业来说，档案信息涉及商业机密、客户数据等，安全的档案信息管理有助于维护企业的竞争力和声誉。在社会层面，政府机关的档案信息关系到国家的安全和社会的稳定，如政策文件、人口统计数据等。一旦档案信息安全受到威胁，可能导致个人隐私泄露、企业经济损失、社会秩序混乱等严重后果。

1.2 常见档案信息安全防护技术类型

常见的档案信息安全防护技术包括数据加密技术、访问控制技术、防火墙技术、入侵检测技术等。

数据加密技术是将档案信息进行编码转换，使得只有授权人员能够解密读取。常见的加密算法有对称加密算法和非对称加密算法。对称加密算法使用相同的密钥进行加密和解密，具有加密速度快的优点，但密钥管理较为困难。非对称加密算法使用公钥和私钥，公钥用于加密，私钥用于解密，提高了密钥管理的安全性。

访问控制技术用于限制对档案信息的访问权限。通过身份认证、授权等机制，确保只有经过授权的用户能够访问特定的档案信息。身份认证可以采用用户名和密码、数字证书、生物识别等方式。授权则根据用户的角色和职责，分配不同的访问权限。

防火墙技术是在内部网络和外部网络之间设置的一道屏障，阻止未经授权的网络访问。它可以根据预设的规则，对网络流量进行过滤和监控，防止外部攻击和恶意软件的入侵。入侵检测技术能够实时监测网络中的异常活动，发现潜在的安全威胁。它通过分析网络流量、系统日志等信息，识别入侵行为，并及时采取措施进行防范。

2 档案信息安全防护技术的应用

2.1 数据加密技术在档案信息中的应用

在档案信息管理中，数据加密技术的应用至关重要[2]。首先，在档案数据的存储阶段，对重要的档案信息进行加密存储可以有效防止数据在存储设备被盗或丢失时泄露。例如，对于企业的财务档案、研发资料等敏感信息，采用加密算法将其转换为密文形式存储在磁盘或数据库中。即使存储设备被非法获取，攻击者没有正确的密钥也无法解密读取其中的信息。

在档案数据的传输过程中，数据加密同样不可或缺。当档案信息在网络中传输时，如通过互联网从一个部门传输到另一个部门，或者从企业内部传输到合作伙伴的系统中，使用加密技术可以保护数据在传输过程中不被窃取或篡改。例如，采用 SSL/TLS 协议对传输的数据进行加密，确保数据在传输过程中的保密性和完整性。

此外，数据加密技术还可以用于保护档案信息的备份。定期对档案信息进行备份是保障数据安全的重要措施，但备份数据也需要进行加密处理。这样可以防止备份数据在存储或传输过程中出现安全问题，确保在需要恢复数据时能够得到完整、准确的档案信息。

2.2 访问控制技术在档案管理系统中的应用

访问控制技术在档案管理系统中起着关键作用。首先，身份认证是访问控制的基础。在用户登录档案管理系统时，系统会要求用户提供用户名和密码进行身份验证。为了提高安全性，还可以采用多因素认证方式，如结合短信验证码、指纹识别等。例如，在一些重要的政府档案管理系统中，除了用户名和密码外，还要求用户使用数字证书进行身份认证，确保只有合法的用户能够登录系统。

授权管理是访问控制的核心。根据用户的角色和职责，系统会为其分配不同的访问权限。例如，档案管理员可能具有对所有档案信息的管理权限，包括创建、修改、删除等操作；而普通用户可能只能查看部分公开的档案信息。通过精细的授权管理，可以确保每个用户只能访问其工作所需的档案信息，防止越权访问。

访问审计也是访问控制的重要环节。系统会记录用户的所有访问行为，包括登录时间、访问的档案信息、进行的操作等。通过对访问审计日志的分析，可以发现异常的访问行为，如频繁尝试登录、越权访问等，并及时采取措施进行防范。例如，当发现某个用户在非工作时间频繁尝试登录系统时，系统可以自动锁定该用户账号，并通知管理员进行调查。

3 档案信息安全防护技术应用面临的问题

3.1 技术层面的挑战

在技术层面，档案信息安全防护技术面临着诸多挑战[3]。首先，伴随信息技术的迅猛发展，黑客的攻击手段也在持续迭代升级。诸如零日漏洞攻击、高级持续性威胁（APT）等新型攻击技术，给档案信息安全构成了严峻挑战。零日漏洞指的是软件系统中尚未被发现和修复的安全漏洞，黑客能够利用这些漏洞实施攻击，而防护技术常常因漏洞的隐蔽性难以迅速响应。这类不断进化的攻击方式，凭借技术上的超前性和隐蔽性，让档案信息面临着更直接的安全风险，也对信息防护体系的实时性和精准性提出了更高要求。

其次，档案信息存储与处理环境正变得愈发复杂。当下，档案信息除了存储在传统的本地服务器和数据库中外，还大量存在于云服务器及移动设备里。这种分布式的存储处理模式，无疑加大了数据管理与安全防护的难度。就像云服务提供商的安全举措或许存在薄弱环节，使得存储在云端的档案信息面临安全隐患。此类多样化的存储环境，不仅让数据管理工作更具挑战性，也让档案信息安全防护需要应对更多元的风险，亟待更完善的管理与防护体系来保障档案信息的安全与稳定。

此外，不同的档案管理系统和应用程序之间的兼容性问题也给安全防护技术的应用带来了挑战。由于各个系统采用的技术标准和安全机制不同，在进行数据交互和共享时可能会出现安全漏洞。例如，当一个企业的档案管理系统与合作伙伴的系统进行数据对接时，可能因为双方系统的加密算法不兼容，导致数据在传输和共享过程中出现安全问题。

3.2 管理层面的不足

在管理层面，档案信息安全防护也存在一些不足之处。首先，安全管理制度不够完善。部分企业或机构缺乏明确的档案信息安全管理规范和流程，导致在档案信息的收集、存储、传输和使用过程中存在安全隐患。例如，没有明确规定档案信息的访问权限和操作流程，可能导致员工随意访问和修改档案信息。其次，人员安全意识薄弱是亟待解决的问题。不少员工对档案信息安全的重要性认知不足，缺乏必要的安全防护知识与技能。比如，部分员工会在公共网络环境中用未加密设备登录档案管理系统，或是随意将档案信息透露给外部人员，这些行为都为档案信息安全埋下了隐患。

在数据中心搭建高效的数据存储管理系统，可对传输而来的数据开展实时处理与分析。运用分布式存储技术，能提升数据存储的可靠性与可扩展性，同时构建数据备份机制，避免数据丢失情况发生。借助大数据分析技术对雨量数据进行深度挖掘，能够为气象预报和决策提供更具价值的信息。这种集存储、管理、分析于一体的系统架构，既保障了数据存储的安全稳定，又通过技术手段挖掘数据潜在价值，让雨量数据在气象领域发挥更大作用，为精准预报和科学决策奠定坚实的数据基

础。

4 档案信息安全管理策略

4.1 完善安全管理制度

完善安全管理制度是保障档案信息安全的基础[4]。首先，要建立健全档案信息安全管理的规章制度。明确档案信息的收集、存储、传输、使用和销毁等各个环节的安全要求和操作流程。例如，规定档案信息的收集必须经过严格的审批程序，确保收集的信息合法、合规；存储档案信息的设备必须定期进行安全检查和维护。

其次，构建档案信息安全管理责任制度至关重要。需清晰划定各部门及人员在安全管理中的职责与权限，将安全责任精准落实到具体岗位和个人。比如，档案管理员需承担档案信息日常管理与维护职责，切实做好信息安全存储、定期备份等工作；信息技术部门则要负责档案管理系统的网络安全防护，提供技术支持与系统升级服务；其他相关部门也应依据业务范畴承担相应的安全协同责任。通过这种责任到人的制度设计，避免管理盲区，形成各司其职、各负其责的安全管理格局，从责任层面为档案信息安全筑牢制度防线。

此外，构建档案信息安全应急响应制度同样关键。需制定完善的应急预案，清晰界定安全事件发生时的应急处置流程与各岗位责任分工。比如，当出现档案信息泄露情况，能第一时间启动预案，迅速采取封堵系统漏洞、切断信息传播路径等措施，阻止信息进一步扩散，同时及时联动技术部门、安全管理部门及相关责任人员，按照既定流程开展溯源调查、数据修复与善后处理工作，通过制度化的应急机制确保安全事件得到有序处置，将损失控制在最小范围，切实提升档案信息安全的风险应对能力。

4.2 加强人员培训与教育

加强人员培训教育是提升档案信息安全水平的核心举措[5]。首要任务是开展安全意识培训，可通过组织专题讲座、发放科普手册等形式，向员工深入讲解档案信息安全的重要意义，传授基础防范知识。比如教会员工设置高强度密码的方法，以及在公共网络环境下规避访问敏感信息的正确做法，从思想认知层面强化员工的安全防护意识，让安全理念真正融入日常工作习惯。其次，要进行专业的安全技能培训。针对不同岗位的员工，开展有针对性的安全技能培训。例如，对档案管理员进行档案管理系统的安全操作培训，使其能够熟练掌握系统的安全功能和操作方法；对信息技术人员进行网络安全技术培训，提高其应对网络攻击的能力。

此外，通过开展模拟安全事件演练也是提升员工实战应对能力的有效途径。可定期组织网络安全应急演练活动，设计贴近实际的攻击场景，让员工在模拟环境中学习如何快速响应安全事件，掌握信息防护、漏洞排查及应急处置的具体流程。这种演练不仅能增强员工的应急处理能力，还能在实战化场景中锻炼团队协作默契，让员工在亲身参与中深化对安全防护流程的理解，从而在面对真实安全威胁时能够更加从容、高效地采取应对措施，筑牢档案信息安全的人员防线。

5 结论与展望

本论文围绕档案信息安全防护技术的应用与管理策略进行了深入研究。阐述了档案信息安全的内涵和重要性，介绍了常见的安全防护技术类型，包括数据加密技术、访问控制技术等。接着详细探讨了这些技术在档案信息管理中的具体应用，如数据加密技术在档案存储和传输中的应用，访问控制技术在档案管理系统中的应用。未来，档案信息安全防护技术将不断发展和创新。随着人工智能、区块链等新技术的不断涌现，这些技术有望在档案信息安全领域得到广泛应用。例如，人工智能可以用于实时监测和分析网络安全态势，及时发现潜在的安全威胁；区块链技术可以用于保障档案信息的不可篡改和可追溯性。

参考文献

[1]金智智.智慧档案的信息安全提升策略[J].管理观察,2016,(06):46-48.
[2]周丹妮.用户体验视阈下数字档案信息服务创新研究[D].湘潭大学,2021.
[3]孟杰.档案数字化背景下加强档案管理工作的路径探讨[J].兰台内外,2023,(32):1-3.
[4]李莎莎.档案信息安全面临的挑战及策略研究[J].办公自动化,2020,25(14):57-58+19.
[5]张文娟.浅谈如何保障档案信息安全[J].办公室业务,2021,(16):81-82.

作者简介：陆丽忠，性别：男，民族：汉，籍贯：上海，学历：本科，当前职称：馆员，研究方向：档案管理与信息化，档案数据治理。