大数据背景下档案数字化管理的安全风险防控策略

朱晴晴

上海大学 上海 200444

【摘　要】：在大数据时代背景下，档案管理从传统的纸质形态向数字化模式全面转变，数字化档案的高效利用与共享能力显著提升，但相应的安全风险也日益凸显，包括数据泄露、篡改、系统入侵、权限失控及技术老化带来的潜在隐患等。这些风险不仅威胁档案资源安全，也影响档案信息的真实性、完整性和可利用性，对政府部门、企事业单位及公共服务体系的运行造成潜在影响。本文从大数据时代档案数字化管理的特征出发，分析当前档案数字化在数据安全、平台建设、人员管理及法规体系等方面存在的主要风险，系统探讨安全风险形成的深层机制，并在此基础上提出权限分级管控、加密与备份体系建设、安全审查制度、技术防护体系建设及人员培训机制等综合防控策略。研究表明，档案数字化管理的安全防控应多维度协同推进，形成技术、制度、管理与文化融合的安全保障体系，以提高档案管理在大数据背景下的韧性和稳定性，为数字政府建设和智慧档案体系的发展提供理论与实践支撑。

【关键词】：大数据；档案数字化；安全风险；信息保护；防控策略

DOI:10.12417/2982-3846.25.03.016

引言

随着信息技术的高速发展，大数据成为推动社会治理现代化和组织管理数字化转型的重要动力。档案管理作为组织运行与历史记录的关键环节，其数字化建设不仅能够提升档案存储与利用效率，也为档案共享、开放和创新应用提供新的平台。然而，在数字化档案不断扩容、业务系统高度集成、数据流动性增强的背景下，安全风险随之增加，尤其是数据泄露、系统攻击和操作失误等风险在多起安全事件中得以体现。档案数字化管理往往涉及数据采集、加工、存储、传输与共享全链条，任何环节的风险都可能导致档案资源遭到破坏或滥用。因此，构建系统化的数字档案安全防控体系已成为档案管理部门和研究者关注的重点。当前研究虽然对档案信息安全提出了多种措施，但在大数据背景下面对的数据规模、复杂网络环境及跨系统协同机制，使传统安全模式面临挑战。本文旨在从风险识别、形成机制与防控策略三个角度展开研究，以期为档案数字化安全体系构建提供理论支撑与实践路径。

1 大数据背景下档案数字化管理的发展特征及安全风险概述

1.1 档案数字化管理呈现规模化、网络化与智能化特征

大数据环境下，档案数字化已经从简单的信息录入扩展为涵盖资源采集、智能识别、存储管理、开放共享等在内的系统化工程，其规模持续扩大、种类日益多样，同时呈现高度网络化特征。数字档案系统通过云平台、政务数据平台等进行联动，使档案管理突破时空限制，为跨部门业务协同提供支持。此外，人工智能、OCR 识别、自然语言处理等技术的应用，使档案管理从被动存储向智能提取、自动归档和智能检索演进，显著提高档案利用效率。然而，系统集成度越高，其安全风险也随之增加。多平台数据交互扩大了潜在攻击入口，智能算法在训练与应用过程中的数据依赖也增加了敏感信息暴露的风险，从而为档案安全管理带来新挑战。

1.2 档案数字化管理中数据泄露与篡改风险不断加剧

数字档案的数据结构整合和网络化存储，使得一旦发生数据泄露，影响范围远高于纸质档案时期。黑客攻击、内部操作人员违规下载和外部系统漏洞均可能导致敏感档案外泄。此外，大数据系统内部存在多层数据迁移与共享过程，档案在流动中的管控难度增加，若缺乏严格的访问控制机制或日志审查制度，篡改风险也随之上升。一旦档案信息被恶意更改，将严重破坏档案的真实性与权威性，甚至影响政府治理、公文决策或历史资料的可靠性。

1.3 技术系统老化、兼容性不足带来潜在运行风险

档案数字化过程中使用的系统与软硬件存在生命周期限制，随着技术更新速度加快，旧系统在存储容量、访问效率及安全防护上均可能面临不足。同时，档案数字化建设常采用多系统协同方式，不同系统的兼容性问题频繁出现，尤其在平台对接或数据迁移时可能出现格式损坏、内容丢失等风险。部分单位在实施档案数字化时未能同步升级安全防护设施，仍依赖过时的防火墙、杀毒软件等，使得系统面临更高的攻击风险。技术老化不仅影响档案管理效率，还可能导致系统瘫痪、数据丢失等严重后果。

2 档案数字化管理安全风险的形成机制分析

2.1 信息流动性增强导致数据保护难度上升

在大数据环境下，档案信息需在多部门、多平台之间频繁流转，数据开放共享的需求使档案系统不再是封闭环境。信息流动性在提高数据利用效率的同时，也让数据脱离原有的控制边界。一旦档案在流转过程中未采用加密传输，或系统间接口缺乏必要的安全协议，就可能被截获或篡改。此外，许多部门共享数据时对敏感等级划分不清，使得机密档案在未设定严格访问限制的情况下被大量人员接触，从而提高了安全风险。

2.2 人员管理不规范导致内部风险不可忽视

统计显示，档案数字化管理中的安全事件中相当比例来自内部人员。原因包括工作人员的信息安全意识薄弱、操作习惯不规范、缺乏严格的权限管理制度等。有些单位对档案数据库管理员、审核人员和普通使用人员未进行权限分级，导致一些不具备授权的人员能够访问敏感档案。此外，部分人员在工作中使用个人移动设备或社交软件传输档案文件，使信息泄露风险显著增加。因此，人员因素已成为档案安全管理的关键风险点。

2.3 制度建设滞后导致风险管控体系不完善

尽管国家陆续出台档案数字化相关政策，但许多单位在制度执行力度、流程规范性和监督机制等方面仍存在不足，例如档案安全责任不明确、敏感档案管理流程缺乏审核、应急处理机制不健全等。制度缺失导致档案管理无法形成闭环控制，一旦发生安全问题，难以及时定位责任环节，影响整体安全防护效率。此外，制度滞后使得新兴技术应用的风险缺乏法律依据与管理标准，不利于降低技术性安全隐患。

3 大数据背景下档案数字化管理的主要安全隐患识别

3.1 网络攻击风险呈现多样化与高频化趋势

黑客攻击形式正在不断更新，从传统的系统入侵演变为分布式攻击、勒索病毒、恶意脚本等多种方式。档案系统一旦暴露在互联网环境中，很容易成为攻击目标，尤其是利用系统漏洞或弱密码攻击更为常见。黑客可通过获取系统权限进行数据窃取、删除、病毒植入或控制系统设备，从而使档案管理面临严重威胁。

3.2 数据丢失与损坏风险影响档案完整性

数字档案依赖电子存储设备，然而设备老化、磁盘故障、电压不稳等都可能造成数据损坏。若未建立完善的备份机制，一旦发生事故，将造成不可逆信息丢失。同时，档案在格式转换、数据库升级或平台迁移过程中可能因格式兼容问题产生无法识别的数据，影响档案的完整性与可利用性。

3.3 隐私与敏感信息保护压力加大

数字档案中包含大量公民个人信息、重大项目资料及重要历史记录，属于高度敏感的数据类型。一旦泄露，可能引发社会舆情与法律风险。当前一些单位在档案处理过程中混淆公开档案与敏感档案的边界，使隐私保护存在漏洞。此外，在人工智能与数据挖掘技术应用过程中，算法训练可能无意间暴露敏感数据，进一步加大隐私保护压力。

4 档案数字化安全风险防控的技术路径

4.1 构建基于分级权限控制的档案访问管理体系

档案信息应根据内容性质、敏感等级和使用需求进行严格的权限分级。例如，将档案划分为公开级、内部级、限制级和机密级，并对不同级别设置不同的访问方式和授权流程。采用多因素认证、动态口令等方式增强访问安全性，并建立访问日志记录与审计制度，一旦发现异常操作可及时追踪来源。权限管控体系可有效减少内部违规访问带来的安全风险。

4.2 利用加密技术与多重备份提升档案数据安全性

在数据传输、存储和共享过程中应采用加密算法，例如 SSL、AES 等，实现数据在不同阶段的安全保护。同时，可采用冗余备份、异地备份、云备份等多重措施建立安全可靠的备份体系，提升档案数据在突发事件后的恢复能力。此外，通过数据指纹、防篡改技术等可进一步确保档案信息的真实性和可追溯性。

4.3 构建智能化安全防护平台提升实时监测能力

通过部署入侵检测系统（IDS）、入侵防御系统（IPS）、安全信息管理系统（SIEM）等，实现对异常访问、攻击行为及系统漏洞的实时监测及预警。人工智能技术可用于分析日志、识别异常模式，从而构建智能化安全防护体系。此外，应定期进行漏洞扫描与补丁更新，确保档案系统的安全性与稳定性。

5 档案数字化安全风险防控的管理策略

5.1 强化档案安全管理制度建设形成闭环管理机制

制度建设是档案安全管理的根本保障，需要围绕档案采集、加工、存储、使用与销毁等关键环节构建覆盖全流程的管理体系，使各项工作在统一标准下运行。制度内容应明确安全责任的分配方式，使不同岗位在档案处理过程中承担相应义务，并通过操作规范为工作人员提供可遵循的行为指引，让数据采集方式、权限设置、访问流程等关键环节具备一致性和可控性。风险评估机制的设置能够帮助机构及时识别潜在隐患，

对系统漏洞、人员操作偏差或外部威胁进行持续监测，使安全问题处于可预防的状态。应急预案在突发事件处理中发挥重要作用，使工作人员在面对数据泄露、系统攻击或设备故障等情况时能够迅速采取正确措施，降低风险扩散的可能。制度体系应随着技术发展和业务需求不断修订，使其始终适配最新的管理环境，保持有效性和前瞻性。通过制度化管理，档案安全流程能够达到规范化、可监控、可追溯的要求，使档案资源在全生命周期内得到稳定保护，为组织的信息安全建设提供长期支撑。

5.2 加强人员培训提升安全意识与管理能力

人员因素在档案安全管理体系中占据核心位置，任何疏忽都可能导致数据泄露、系统损坏或管理失序，因此强化工作人员的安全意识与专业能力十分必要。通过定期组织安全培训，使工作人员熟悉数据保护要求、密码管理规范以及违规操作的潜在后果，能够让其在实际工作中形成稳固的安全意识，减少因操作不当带来的风险。专业技术指导也能帮助员工理解更复杂的安全风险来源，使其在面对高风险场景时保持敏感度和判断力。信息技术能力的提升同样不可忽视，档案系统在数字化背景下更容易受到网络攻击、系统故障和硬件损坏等技术风险的影响，管理人员若缺乏相应能力，将难以在突发情况下作出正确处置。通过技能培训、应急演练和案例学习，使档案管理人员能够掌握系统维护、故障排查和应急响应的方法，在关键时刻保障档案数据的安全。

5.3 推动法律法规完善为档案安全提供制度保障

档案数字化过程中涉及大量敏感信息，安全风险的防控离不开法律法规的有效支撑。档案法、数据安全法和个人信息保护法为数字化管理提供了基本的制度框架，但在实际操作层面仍需针对档案管理特点进行细化，使数字化建设在合法合规的路径上稳步推进。法律条款的落地能够明确数据采集、存储、传输与使用的边界，为管理部门和技术人员提供行为准则，使数字化转型在安全要求上更具可执行性。行业标准与操作规范的建立同样具有重要意义，通过统一术语定义、流程要求、技术参数和安全控制措施，为档案管理提供结构化、系统化的指导，使不同机构在实施过程中保持一致的安全水准。规范体系的完善不仅有助于提升档案数据的安全性，也能推动行业整体形成成熟的管理模式，使档案数字化建设在风险可控的条件下不断发展，让档案资源在保障安全的前提下发挥更高的利用价值，为组织治理与社会服务提供更加可靠的信息支持。

6 结论

在大数据背景下，档案数字化管理在提高信息利用效率与资料保存能力的同时，也面临多维度、多层次的安全风险。通过对风险来源、形成机制及技术与管理防控路径的系统分析可见，档案安全保护需要技术手段、管理制度、法律法规及人员能力的综合支撑。未来，应进一步构建智能化、安全化的档案管理体系，实现档案资源的可靠保存、高效利用与长期安全保障，为数字政府、大数据治理及国家信息安全战略提供坚实支撑。

参考文献：

[1] 徐毅,孟荣荣,刘玮晗,等.数字化转型背景下电子档案及文件可信管理研究[J].2025(07):15-17.

[2] 宋香玉.数字化转型背景下档案管理的安全性与隐私保护策略研究[J].中原文化与旅游,2024(8):61-63.

[3] 仇海涛.数字化转型背景下档案信息安全管理问题探析[J].黑龙江史志,2023(10):119-120.

[4] 王瑞.数字化转型背景下档案信息安全问题分析[J].黑龙江档案,2024(4):25-27.

[5] 姜红霞.信息时代下档案管理风险识别及防范策略研究[J].山西档案,2023(1):132-134.

[6] 李娜.大数据背景下档案信息安全管理研究[J].档案管理,2020.

[7] 王蕊.数字档案室建设中的信息安全风险与对策[J].情报探索,2019.

[8] 张楠.数字化档案管理中的技术风险及管控策略[J].档案与建设,2021.

[9] 陈慧.信息时代档案安全管理面临的新挑战与策略[J].兰台内外,2018.

[10] 刘洋.数字档案安全防护技术研究进展[J].中国档案,2021.