云计算环境下电子档案保密管理问题与应对措施

李姝睿　张梦妍　杨戈
北京强度环境研究所　100076

【摘　要】随着云计算技术在档案管理领域的广泛应用，电子档案的存储、传输与利用效率大幅提升，但保密管理面临诸多新挑战。本文通过分析云计算环境下电子档案保密管理的现状，梳理出数据安全风险、权限管理漏洞、技术依赖隐患、制度体系不完善等核心问题。针对这些问题，从技术防护、权限优化、自主创新、制度完善四个维度提出应对措施，旨在为提升云计算环境下电子档案保密管理水平提供参考，保障电子档案信息安全，推动档案管理在云端环境下安全高效发展。

【关键词】云计算；电子档案；保密管理；信息安全

Confidentiality Management of Electronic Archives in Cloud Computing Environment and Countermeasures by

Li Shurui　Zhang Mengyan　Yang Ge
Beijing Institute of Strength and Environment　100076

【Abstract】With the widespread adoption of cloud computing technology in archival management, the efficiency of electronic archive storage, transmission, and utilization has significantly improved. However, confidentiality management now faces new challenges. This paper analyzes the current status of electronic archive confidentiality management in cloud computing environments, identifying core issues such as data security risks, permission management vulnerabilities, technical dependency hazards, and incomplete institutional frameworks. To address these challenges, the paper proposes countermeasures from four dimensions: technical protection, permission optimization, independent innovation, and institutional improvement. The aim is to provide references for enhancing confidentiality management of electronic archives in cloud computing environments, ensuring information security, and promoting the safe and efficient development of archival management in cloud-based settings.

【Key words】cloud computing; electronic archives; confidentiality management; information security

引言

在数字化转型浪潮中，电子档案已成为各类组织信息存储与传承的重要载体。云计算凭借其高效的资源整合能力、灵活的扩展特性，逐渐成为电子档案管理的主流技术支撑。然而，云计算的分布式架构、多租户共享模式以及网络开放性，使电子档案保密管理面临前所未有的风险。一旦电子档案出现信息泄露、篡改或丢失，将给组织带来巨大的经济损失与信誉损害。因此，深入剖析云计算环境下电子档案保密管理存在的问题，探索科学有效的应对措施，对于维护电子档案安全、保障组织信息权益具有重要的现实意义和实践价值。

一、云计算环境下电子档案保密管理存在的问题

（一）数据存储与传输环节的安全风险

云计算环境下，电子档案多存储于云端服务器，数据传输依赖公共网络，这一过程存在显著安全风险。云端存储方面，服务商的物理服务器可能面临自然灾害、硬件故障等问题，若备份机制不完善，易导致电子档案丢失。同时，部分云服务商存在数据中心管理不规范的情况，内部人员可能非法访问或泄露电子档案。数据传输环节，公共网络的开放性使数据易被黑客拦截、窃取或篡改，尤其是未采用加密传输技术时，电子档案的保密性难以保障。此外，不同云服务平台间的数据迁移过程中，也可能因格式不兼容、传输协议漏洞等问题，引发数据泄露风险。

（二）用户权限管理体系存在漏洞

电子档案的保密管理离不开严格的权限控制，但云计算环境下多用户、多角色的访问模式，使权限管理难度大幅增加。部分组织未建立动态的权限分配机制，用户权限长期固定，当员工岗位变动、离职后，若未及时调整或收回权限，易出现权限滥用、越权访问的情况。同时，权限划分颗粒度较粗，无法根据电子档案的保密级别、用户职责精准分配访问权限，导致低权限用户可能接触到高保密等级的档案。此

外，身份认证方式单一，多依赖账号密码，易遭受暴力破解、钓鱼攻击，进而导致非法用户获取权限，威胁电子档案安全。

（三）对云服务技术的依赖引发隐患

当前，许多组织在电子档案管理中过度依赖第三方云服务提供商的技术支持，自身缺乏核心技术掌控能力，这一现象带来多重隐患。技术标准方面，不同云服务商的技术架构、接口协议存在差异，组织若长期依赖单一服务商，将面临“锁定效应”，后续更换服务商时，可能因技术不兼容导致电子档案无法正常迁移，影响档案的长期可用性。同时，若云服务商的技术更新不及时，无法应对新型网络攻击手段，将使电子档案暴露在安全风险中。此外，部分组织缺乏对云服务技术的监督与评估能力，难以准确判断服务商的技术安全性，无法及时发现并规避潜在风险。

（四）保密管理制度体系不完善

健全的制度是保障电子档案保密管理的基础，但目前部分组织的保密管理制度存在诸多缺陷。制度内容方面，未结合云计算环境的特点制定针对性条款，仍沿用传统电子档案管理的制度框架，对云端数据安全、权限管理、应急处置等关键环节的规定模糊，导致实际管理工作缺乏明确指引。制度执行层面，缺乏有效的监督考核机制，部分员工保密意识薄弱，未严格遵守制度要求，如随意分享云存储链接、使用非加密设备传输电子档案等行为屡禁不止。此外，跨部门协同管理机制缺失，档案管理部门与 IT 部门、业务部门之间沟通不畅，在云服务选型、技术维护、风险处置等工作中难以形成合力，影响保密管理效果。

（五）应急响应与灾难恢复能力不足

云计算环境下，电子档案面临的安全威胁具有突发性、复杂性，若缺乏完善的应急响应与灾难恢复机制，将无法及时控制风险、减少损失。应急响应方面，部分组织未制定针对云计算环境的安全应急预案，当发生数据泄露、系统瘫痪等突发事件时，工作人员无章可循，导致应急处置效率低下，扩大事故影响范围。同时，应急团队建设滞后，缺乏专业的技术人员，难以快速定位风险源头、实施有效处置措施。灾难恢复环节，部分组织未定期开展灾难恢复演练，对电子档案的备份策略缺乏有效性验证，当遭遇重大灾难时，无法及时恢复数据，导致电子档案长期不可用，严重影响组织的正常运营。

二、云计算环境下电子档案保密管理的应对措施

（一）强化数据安全技术防护能力

针对数据存储与传输的安全风险，需从技术层面构建全方位的防护体系。数据存储方面，选择具备完善备份机制的云服务商，采用“本地备份+云端备份”的双重备份策略，定期对电子档案进行备份，并验证备份数据的完整性与可用性。同时，要求云服务商采用加密存储技术，对电子档案进行 AES-256 等高强度加密处理，确保数据即使被非法获取也无法解密。数据传输环节，强制采用 SSL/TLS 等加密传输协议，避免数据在传输过程中被拦截篡改。此外，引入数据脱敏技术，对电子档案中的敏感信息进行处理，在不影响正常使用的前提下，降低信息泄露风险。

（二）优化用户权限管理机制

建立科学严谨的权限管理体系，是保障电子档案保密的关键。首先，实施动态权限分配，根据用户的岗位职责、工作需求以及电子档案的保密级别，实时调整用户权限，确保“按需授权、权限最小化”。员工离职或岗位变动时，通过自动化系统及时收回或调整权限，避免权限遗留问题。其次，细化权限划分颗粒度，将权限分为查阅、下载、修改、删除等不同类型，结合电子档案的保密等级，为不同用户分配精准权限，防止越权访问。最后，加强身份认证技术应用，采用“账号密码+动态口令+生物识别”的多因素认证方式，提高身份认证的安全性，有效防范非法用户登录。

（三）提升自主技术掌控与选型能力

减少对第三方云服务技术的过度依赖，需从技术自主与科学选型两方面入手。技术自主方面，加大研发投入，培养专业的 IT 技术团队，提升组织对云服务技术的理解与掌控能力，尤其是在数据加密、权限管理、安全监测等核心技术领域，逐步实现技术自主可控。同时，推动与高校、科研机构的合作，共同研发适配云计算环境的电子档案保密管理技术，降低对外部技术的依赖。云服务选型方面，建立科学的评估体系，从技术安全性、服务稳定性、数据迁移能力等维度，对云服务商进行全面评估，避免因单一选型导致的“锁定效应”。此外，签订详细的服务协议，明确云服务商的安全责任与数据保护义务，保障组织的合法权益。

（四）完善保密管理制度体系建设

构建适配云计算环境的保密管理制度，需从制度内容与执行监督两方面发力。制度内容上，结合云计算技术特点，修订完善电子档案保密管理相关制度，明确云端数据存储、传输、访问的安全要求，细化权限管理、应急处置、责任追究等条款，为实际工作提供清晰指引。同时，制定云服务选型规范、数据备份与恢复制度、安全事件应急预案等专项制度，形成覆盖电子档案全生命周期的制度体系。执行监督方面，建立健全监督考核机制，定期对制度执行情况进行检查，将员工的保密工作表现纳入绩效考核，对违反制度的行为严肃追责，提高制度的执行力。此外，加强跨部门协同，建立档案管理部门、IT 部门、业务部门联动机制，明确各部门在电子档案保密管理中的职责，形成管理合力。

（五）增强应急响应与灾难恢复能力

提升应急处置与灾难恢复水平，需从预案制定、团队建设、演练验证三方面推进。首先，制定针对性的安全应急预案，明确突发事件的响应流程、处置措施与责任分工，涵盖数据泄露、系统瘫痪、自然灾害等不同场景，确保突发事件发生时能够快速响应。其次，组建专业的应急响应团队，配备具备云计算、网络安全、档案管理等多领域知识的技术人员，定期开展专业培训，提升团队的应急处置能力。最后，加强灾难恢复演练，定期模拟不同类型的安全事件，检验应急预案的有效性与备份数据的可用性，根据演练结果优化应急预案与备份策略，确保在重大灾难发生时，能够快速恢复电子档案数据，减少损失。

三、云计算环境下电子档案保密管理的发展趋势

（一）人工智能技术深度赋能安全管理

未来，人工智能技术将在电子档案保密管理中发挥重要作用，实现安全管理的智能化升级。在安全监测方面，利用人工智能算法对电子档案的访问行为、数据传输情况进行实时分析，建立正常行为模型，当出现异常访问、数据异常传输等情况时，能够自动识别并发出预警，及时防范安全风险。在风险预测方面，通过人工智能对历史安全事件数据、网络攻击趋势进行分析，预测可能出现的安全威胁，提前采取防范措施，变被动应对为主动预防。此外，人工智能还可应用于身份认证领域，通过对用户的行为特征进行分析，实现更精准的身份识别，进一步提升访问控制的安全性。

（二）区块链技术助力数据安全保障

区块链技术的去中心化、不可篡改特性，将为云计算环境下电子档案的保密管理提供新的技术支撑。利用区块链技术构建电子档案的分布式存储系统，可避免因单一节点故障导致的数据丢失，同时去中心化的架构使数据难以被非法篡改，保障电子档案的完整性与真实性。在数据溯源方面，通过区块链记录电子档案的创建、修改、访问等操作信息，形成不可篡改的操作日志，便于追溯数据流转过程，一旦发生信息泄露，能够快速定位责任主体。此外，区块链技术可应用于电子档案的权限管理，通过智能合约自动执行权限分配与收回，提高权限管理的效率与安全性。

（三）合规化与标准化建设加速推进

随着数据安全相关法律法规的不断完善，云计算环境下电子档案保密管理的合规化要求将进一步提高。组织需严格遵守《数据安全法》《档案法》等法律法规，确保电子档案的管理工作符合法律要求，避免因合规问题引发法律风险。同时，行业层面将加快制定云计算环境下电子档案保密管理的标准规范，统一技术要求、管理流程与评估指标，推动不同组织、不同云服务商之间的协同合作，解决技术不兼容、管理不统一的问题。合规化与标准化建设的推进，将为电子档案保密管理提供更明确的方向，促进整个行业安全水平的提升。

（四）安全与效率的协同优化成为重点

在保障电子档案安全的前提下，提升管理效率将成为未来发展的重要方向。一方面，通过技术创新与流程优化，在加强保密管理的同时，减少不必要的操作环节，提升电子档案的访问与利用效率。例如，采用智能化的权限管理系统，实现权限的自动分配与调整，减少人工操作成本。另一方面，推动云服务技术与档案管理业务的深度融合，开发适配电子档案管理需求的云服务功能，如智能检索、自动分类等，在保障安全的基础上，提升电子档案的利用价值。安全与效率的协同优化，将实现电子档案保密管理与业务发展的双赢。

四、结论

本文深入分析了云计算环境下电子档案保密管理存在的数据安全风险、权限管理漏洞、技术依赖隐患、制度不完善、应急能力不足等问题，并针对性地提出强化技术防护、优化权限管理、提升自主技术能力、完善制度体系、增强应急恢复能力等应对措施，同时探讨了人工智能赋能、区块链应用、合规标准化、安全与效率协同的发展趋势。研究表明，云计算环境下电子档案保密管理需从技术、管理、制度多维度协同发力，才能有效应对安全挑战。未来，随着技术的不断创新与制度的持续完善，电子档案保密管理水平将逐步提升，为电子档案在云端环境下的安全高效管理提供有力保障，推动档案管理行业实现数字化、智能化、安全化发展。

参考文献

[1]刘嘉铭.数字化时代电子档案保密管理研究[J].中国管理信息化，2025，28（12）：150-152.
[2]张敏.浅谈如何做好电子档案管理的保密工作[J].兰台内外，2024，（17）：43-45.
[3]杨晓英.如何做好电子信息档案管理的保密工作[J].兰台内外，2021，（31）：34-36.
[4]杨戈.如何做好电子档案管理的保密工作[J].经营管理者，2021，（10）：100-101.
[5]侯桂明，吕颖君.新时代事业单位档案保密工作的强化策略[J].办公室业务，2021，（16）：99-100.