数字档案信息长期安全存储探究

王偲璇

（云南电网有限责任公司文山供电局，云南 文山 663000）

摘 要：在档案管理信息化建设工作逐渐得到落实的过程中，档案信息管理逐步实现网络化、数字化，信息传播载体由传统的纸质形式转向数字音频、数字视频、数字网络等。而数字档案信息储存、检索等功能提高了档案管理工作效率，推动了档案管理的现代化发展步伐。但是在数字档案信息长期存储的过程中会受到很多因素的影响，弱化了档案管理的安全性，需要采取合理选购数字档案载体、做好数字档案迁移工作、健全法律法规等方式，构建数字档案信息安全存储模式，通过应用可信时间戳技术、抗合谋指纹技术、WORM存储技术等先进科学技术提升安全风险防范水平，强化数字档案信息长期存储的可靠性。

关键词：数字档案信息 长期安全存储 构建安全防护体系

中图分类号：G270.7 **文献标识码：**A **文章编号：**1003-9082（2022）03-0028-03

信息技术在很多行业得到广泛应用，开展信息化建设工作能够改变档案的存在形式，即纸质档案电子化。在档案管理中应用数字化技术可以为文件资料的利用带来更多便利，但是网络环境具有开发性、不确定性，增加了病毒侵入、信息篡改的概率，给数字档案信息长期存储带来安全威胁。为了避免出现以上问题，应该加大资金投入力度，积极引进先进的软件、硬件设施，构建完善的安全防护体系，提升数字档案信息长期储存安全防护水平，为档案管理工作的有序落实奠定良好的基础。

一、数字档案信息长期安全存储中存在的主要问题

1.硬件的使用缺乏可靠性、安全性

数字档案在长期保存的过程中涉及硬件安全问题，即给系统正常运行带来支撑的物理设备，包含存储设备、数据和管理服务器、路由器、交换机等，以上设备的安全等级、工作性能直接影响系统的稳定性，决定了数据长期储存的质量。通常情况下，存储设备、服务器等硬件设施内部设置了安全备份功能，可以为数据信息的保存和利用提供基础安全保障，但是在各类外界因素的影响下，容易引发以上设备的故障问题，如火灾、雷电等，除此之外，还有工作人员操作不规范等，给数据信息的安全存储带来不良影响[1]。

2.计算机应用系统存在安全缺陷

开展数字档案信息存储、管理工作的过程中，离不开计算机操作系统、数据库及其他应用软件的使用，同时需要可靠的备份机制。针对操作系统而言，避免不了存在一些薄弱环节会遭到病毒的侵袭，对计算机系统造成攻击、破坏，尤其在用电单位的经营管理中，涉及机密文件，会增加电力系统的安全风险。而对于系统的应用软件来说，如果没有按照相关要求进行定期升级，也会弱化安全防护屏障的实际作用。在计算机应用系统的数据库中，数据具有可访问性特点，在传递、利用的过程中，容易被拷贝，并且数据信息在大量存储的过程中，体现出较强的聚生性，分散性的信息很难体现实际价值，但是集聚性信息能够发挥重要作用。由于数据库在安全防护及应用的过程中有着一定的矛盾性，虽然可以利用软件、硬件设施建立系统防护屏障，但如果设置安全防护层过多，会阻碍数据信息的利用，给数据使用人员带来不便。

3.档案数据的存取存在安全风险

与纸质载体相比较而言，现代化储存技术虽然能够为数据信息的储存和利用创造便利条件，但是依然会受到外界环境因素的影响，如磁带的使用寿命为3～5年，光盘的使用寿命也在30年以内，同时此类存储设备会受到磁场、环境温湿度等方面的影响，一定程度上缩短使用寿命。由于计算机语言的更新速度较快，为了保证计算机系统的使用能够保持与时俱进，需要不断地进行不同语言之间的互换，而在替换的过程中会体现出不适应性，导致一些原有的信息无法还原，弱化了数据信息的真实性。且数字档案在使用的过程中，离不开计算机设备，一旦因实际需要进行设备的更新，很容易改变数据记录存储的格式，导致数字档案无法实现正常浏览，各类数据难以有效读取。

4.安全技术与管理机制缺乏先进性

数据库安全技术与网络技术之间存在密切联系，数据库安全技术主要针对网络风险开发，立足于应用安全问题提升安全防范技术水平，可见安全技术需要依靠出现的风险问题进行升级，体现出较强的滞后性。在数据安全领域及信息系统的实际运行中，利用信息加密、数字水印、电子

签名、身份认证等技术能够提升安全防护水平，但是由于技术不够完善，弱化了系统的安全控制能力。在传统的纸质档案管理时期，针对档案管理制定了完善的制度，使得很多纸质档案资料得以长期保存，为重要文件需求者提供信息保障。但是在数字档案储存、管理的过程中，缺少健全的制度体系，致使档案资料的利用不够规范，引发文件不完整、被窃取等风险。

二、解决数字档案信息长期存储中安全问题的有效途径

1.合理购入数字档案载体，科学选择读取设备

在选择数字档案载体的过程中，应避免购入属于技术不成熟阶段的电子档案载体，同时使用技术相对完善的数据信息读取设备，此类设备不仅具备较强的可靠性，还有助于节约资金支出。此外，选择的数字档案载体不能处于技术淘汰期，虽然此类设备在成本方面占据一定优势，但是容易引发在使用过程中的不兼容问题，即设备无法读取载体的内容，反而会造成资源浪费。为此，应该保证数字档案载体和读取设备的兼容性，保障硬件设备的安全性，提高档案资料利用效率，提升数字档案存储水平。

2.更新数字档案管理软件，强化系统的适用性

在数字档案存储系统中，除了必要的硬件设施，技术成熟的软件也是不可或缺的构成部分，为了避免出现系统软件方面的缺陷，需要合理选择软件类型，避免使用处于测试时期的软件，同时认真辨别选择的软件是否已经被行业淘汰。开展软件购入工作时，应该优先选用能够应用在多个系统中的软件，以防出现软件与系统不兼容等问题。虽然可以利用升级BIOS软件版本适应系统，或者采用引进新型电子档案读取设备的方式实现对数字档案的存储，但是由于在硬件方面存在不配套的情况，难以保证以上方法的适用性，强化软件选择的合理性是最为有效的途径[2]。

3.做好档案迁移与载体转换，强化信息存取能力

由于部分档案资料载体形式容易受到外界因素的影响，给实际存储寿命带来不良影响，需要增强数字档案合理迁移意识，同时科学选择载体转换方式。首先，有序开展新型信息读取设备与旧型档案载体的兼容性测试工作，只有顺利通过测试达到100%兼容的程度才能投入使用，同时应保证旧型档案载体能够实现档案信息的继续保存，避免更换载体或者进行迁移。其次，一旦新型信息存取设备无法达到对旧型档案载体的100%兼容，则需要开展载体转换、档案迁移工作，在落实相关工作的过程中，需做好旧型档案信息读取设备的储备工作，从而确保在任何情况下都能完成旧型档案信息的读取。最后，如果购入的新型计算机系统无法实现对旧型档案信息的读取，且旧型信息读取设备不能继续使用，应采用新信息读取设备或者旧读取设备与E1转换设备连接的方式，包括IDE/SATA接口转换设备，能够达到延长旧型信息存储设备寿命的目的。

4.健全数字档案管理法律法规，加强安全标准建设

通过分析与数字档案管理相关的法律法规，明确数字档案信息管理缺少完善的法律保障，依靠通用的信息管理法律法规无法实现对档案资料的有效保护。有关部门应增强法律法规完善意识，构建健全的法律体系，为数字档案管理提供坚实基础。制定法律法规的过程中，需立足于规范性的角度进行分析，确保各项规章制度的可行性，加强基础管理与技术管理的有机结合，及时做好法律法规的修订工作，确保能够符合实际要求、满足基本需求，为数字档案信息系统的安全建设提供合理依据，强化数字档案管理的标准化、实效性。开展数字档案信息长期存储工作的过程中，离不开安全存储设备、先进的服务器，应始终坚持在线备份、离线备份相结合的基本原则，为了提升计算机系统的病毒防范水平，需要及时做好病毒库更新，选择使用两种以上的广谱杀毒软件，强化系统的病毒防御、查杀能力，强化安全技术与管理工作的先进性[3]。

三、提升数字档案信息长期安全存储风险防范水平

1.立足于技术层面强化防护

1.1增强可信时间戳技术运用意识

为了达到长期安全存储数字档案信息的目的，需要增强可信时间戳技术应用意识。此种技术具体指由权威可信时间戳服务中心签发的可以证明数据的电子文件，是一种具备较强法律效力的电子凭证，体现出可验证、完整性等特点，可信时间戳技术的应用目的是验证电子文件产生的准确时间，避免发生电子文件被篡改等风险。利用可信时间戳技术能够为数字档案的收集、移交、存储、利用等环节提供安全防护，确保数字档案可以得到法律的保护[4]。

1.2提高对抗合谋指纹技术的重视

由于公共网络具有开放性特点，使得档案信息被篡改、盗用的风险有所增加，为了提升安全保障水平，应该加强对抗合谋数字指纹技术的合理运用。如果用户提出档案使用申请，档案管理部门可以依据对用户身份的验证生成相应的指纹信息，之后向数字档案中进行嵌入，并向用户发送经过指纹嵌入的档案，为数字档案做好标识，同步完成数据中用户指纹信息的录入。在此基础上，审计部门可以有针对性地开展数字档案流通监管工作，及时发现存在的违法行为，一旦出现违规利用数字档案的问题，审计部门

可以通过调取数据库中的指纹信息在短时间内锁定违规操作人员。通过以上工作的落实，能够减少数字档案的违法传播，降低长期存储过程中的安全风险[5]。

1.3加强对WORM存储技术的研究

在数字档案长期存储的过程中，受到多种因素的影响，容易导致数据被删除、被篡改，为了减少此类情况的发生，应该加强对WORM存储技术的有效利用，针对WORM存储技术而言，具体指数据资料一旦被写入系统中，只能进行读取操作，不能在后期存储和使用的过程中进行修改和删除，体现出一次性写入的特点，可以应用在很多方面，如个人征信记录保存、数据加密、电子凭证、视频监控等，有效强化了数据存储的安全性。在先进的F2-safe硬盘式WORM储存器的使用过程中，即使出现设备丢失的情况，也无须考虑内部数据信息泄露的情况，因为只有拥有合法认证身份的人才能成功登录设备，在科研机构、政府部门、金融保险等领域，F2-safe有着广泛应用，且得到高度认可[6]。

2.立足于物质层面强化防护

2.1加大档案管理资金、资源投入力度

在部分企业或者事业单位中，给予档案管理方面的资源支持不够充足，不仅会掣肘各项工作的顺利开展，还会影响到数字档案长期储存过程中的安全性。有关部门需要加大资金、资源投入力度，在内部资金管理中引入数字档案信息安全风险防范，确保相关工作能够拥有持续性的经费支持。档案管理部门应该依据电力行业的实际发展情况，积极组建内部资金安全监管机构，主要负责实时监察各项资金的应用方向。此外，为了拓展数字档案管理的资金获取渠道，应该鼓励企业或者单位设立专项基金，让数字档案管理拥有坚实的基础，有利于档案部门的稳定有序发展。

2.2提升档案管理人员的综合素质

档案管理人员是数字档案长期存储过程中的重要基础力量，为了提升数字档案存储过程中的管理水平、安全防护能力，应该增强管理人员的安全知识学习意识，定期参加安全培训，了解数字档案信息安全防护的重要性。针对现有的管理人员应该开展信息安全相关的讲座、竞赛及其他类型的活动，帮助其熟练掌握安全防护知识，并且能够做到实际工作中的灵活运用，体现安全防护工作的价值。为管理人员提供继续教育的机会，合理调整内部组织结构，做好档案管理部门不同岗位的更新，合理利用岗位乱换机制，降低数字档案管理人员泄漏重要信息的几率。此外，为了保证档案管理人才队伍的先进性，应该建立严格的人才聘用机制，不仅能要求应聘人员具备岗位相关的专业能力，还要有高学历水平、丰富的管理经验，并且能够熟悉数字档案信息存储系统的软件、硬件设备，从而为档案管理提供助推力[7]。

结语

在档案管理工作中包含很多内容，且具备复杂性特点，需要合理明确数字档案信息管理流程，主要有采集、归类、存储、管理等。有关部门应该提高对数字档案信息长期存储方面的重视，从软件、硬件设施的角度出发，增强现代化建设意识，做好信息读取设备和载体更新工作，保证与计算机系统之间有着较强的兼容性，避免出现浪费资源的情况。与此同时，及时更新病毒库，合理选择广谱杀毒软件，在数字档案信息储存系统中建立安全防护屏障，强化原始档案的完整性、可靠性。为了让数字档案信息管理工作拥有合理依据，需要建立完善的管理机制，同时增强法律法规健全意识，确保档案利用行为的合法性、规范性，提升数字档案信息存储过程中的安全监督水平[8]。

参考文献

[1]王红娜.浅谈数字档案信息长期存取面临的问题及解决措施[J].神州,2018(18):2.

[2]贾明军.数字档案系统的安全防范之我见[J].山东档案,2019(2):3.

[3]聂云霞,方璐,曾松.数字档案信息安全风险与防范策略探讨[J].档案与建设,2017(4):5.

[4]杨建军.企业数字档案馆建设制度体系架构之我见[J].机电兵船档案,2019(3):6.

[5]杨涛.数字档案信息长期安全存储问题探讨[J].黑龙江史志,2014(14):2.

[6]张嘉.云存储环境下数字档案信息资源安全保障研究[J].办公室业务,2020(7):2.

[7]丁晓阳.数字档案长期存储问题探究及解决方案[J].信息记录材料,2018,19(6):2.

[8]杨重高.数字档案资源的安全存储[J].中国档案, 2014(11):4.