# 数字档案信息安全保存问题浅析

**摘　要：**文章从数字档案信息长期保存的标准和数字档案管理信息系统的安全管理两个方面，对数字档案信息安全保存问题进行分析。

**关键词**　数字档案信息　安全保存

◇张雪枫

随着档案信息化进程的加快，档案信息的数字化和网络化利用将更广泛、更深入，这必将进一步促进档案数字化工作的深入开展，但与此同时，数字档案信息在其形成、存贮和共享利用等环节也将存在各种类型和层次的问题，成为档案工作者亟待解决的问题之一。

一、数字档案信息长期保存的标准

将有价值的文件信息以稳定的格式储存在稳定的载体上并不能解决文件的长期保存问题。再稳定的格式也有过时的时候，再长久的载体也会腐坏，因而仍然需要随着科学技术发展对需要长期保存的文件进行新、旧数字平台之间的转换。但每种技术方案都各有优劣，所有的解决方案都只是部分地解决了问题，所以有必要确立选择评价技术方案的原则和标准，以尽快找到解决数字档案信息长期保存问题的理想策略。

1.评价选择的原则。首先，必须明确保存的目标和要求，这是选择技术方案的出发点和归宿点。具体来说，保存目标应包括保证信息载体的物理安全；保证信息内容的准确；保证信息的可理解；保证信息的可获取等。在讨论数字档案信息的保存要求时，需要了解相关问题：①为谁保存。从用户角度明确保存的要求，确定保存数字化信息是为了满足谁的需求、满足哪些方面的需求，有利于更好地平衡各方面的需求，并从整体规划和资源配置的角度考虑数字保存。②保存怎样的数字信息。保证信息的真实性、凭证性和可用性的必要特征；保证信息的易处理性。

2.理想策略的要求。根据以上保存要求明确一种理想的保存策略必须具有以下特点：①适用时间上的可延展性和适用范围上的包容性。一个理想的策略应该能提供一种可扩展、长期的方法，以保证在相当长的时间里数字档案信息的长期存取，并具有一定的进化升级能力，以便在保存对象、技术、要求发生变化时继续延用。另外，该策略应适用于所有文件种类和媒体类型。②使用中的简易性和灵活性。理想策略也应根据不同的保存要求提供不同代价的替代方案，以便将来可随时根据特定类型的文件、文件组合的要求改变保存方案。③最低风险和最大功能。理想策略要尽量避免翻译、转移的程序，以最小的人为干预，减少人力和数据丢失的可能。同时，转换后的文件要保留尽可能多的文件原始功能、外观等特征；给每个文件加以人为可识别的标签信息和元数据，以便于文件管理。④自身的可验证性。由于我们不仅是为现有技术条件下的数字信息提供保存方案，也要为将来可能出现的软硬件技术和信息类型作考虑，因而理想解决方案在技术上的可实现性应是能证明的。

二、数字档案管理信息系统的安全管理

数字档案信息的录入和维护主要依靠管理信息系统所提供的各项功能来完成，由于用户角色的不同、权限的差异，要求应用系统能够提供一套完整的用户安全管理策略，以保证档案信息的完整性和安全性。数字档案管理信息系统的安全管理主要体现在三个方面：一是要采用成熟先进的计算机应用系统运行结构；二是对系统用户按照工作需要进行角色和等级的区分；三是对档案数据的安全管理级别如保密、开放等状态按照相关法律法规进行多级安全管理，以区别不同类型用户的访问。

1.应用系统的体系结构。三层 BrowserServer 体系结构有着多层数据安全机制、日常维护工作量小、对客户端的运行环境要求较低、客户端物理位置可以灵活设置等诸多优点，因此，采用该系统结构无疑是一个明智的选择。安全防护措施主要包括：防火墙安全措施、应用系统的身份认证安全措施以及数据库管理系统的安全模型。

2.应用系统用户权限管理。系统用户权限的管理和角色分配与档案管理的业务功能、操作流程、档案数据的管理层次密切相关。一般情况下用户分 3 大类，即管理级用户、业务级用户和浏览级用户。管理级用户负责系统整体数据备份、日常维护、系统模块设置、用户定义及用户权限设置等；业务级用户负责各个业务岗位上数据的录入、修改、删除、统计、检索等功能，该类用户对系统中的数据具有完全的存取访问权限，每个用户的操作功能和访问数据内容的权限将根据其业务职能的不同而有所区别；浏览级用户主要是通过网络查询已经开放的档案信息，绝不允许对系统中的数字进行修改和删除。无论是哪一类用户，在访问系统的过程中主要是通过严格的身份认证技术来保证系统的安全性。因此，系统用户的安全管理也是非常重要的。

3.防病毒策略。第一，制定适合本系统的反病毒策略；第二，部署多层防御战略，在尽可能多的“点”采取病毒防护措施；第三，定期更新定义文件和引擎；第四，动态更新网络系统、桌面型计算机中的反病毒软件；第五，定期备份文件，检查从备份中恢复的数据；第六，预订电子邮件病毒警报服务，保证整个网络信息系统运行机制安全可控。为了保护数字档案信息的安全科学管理，数字档案馆使用网络病毒软件可以从两方面考虑：一是工作站；二是服务器。工作站是病毒进入网络的主要途径，为了防止病毒从工作站侵入，可以采用无盘工作站、带防病毒芯片的网卡、单机防病毒卡或网络防病毒软件。大多数防毒软件运行在文件服务器上，它可以同时对服务器和工作站进行查毒扫描、检查、隔离、报警，当发现病毒时，由网络管理员负责清除病毒。

[责编　赵晶莹]