 DOI: https://doi.org/10.36956/iser.v2i1.360

Thoughts on Strengthening the Security System of Archives Information

Dong Li

Beijing University of Technology, Beijing, 100124, China

Abstract

The urgency of strengthening the information security system. Information is an important strategic resource for social development. Information technology and the information industry are changing traditional production, management and lifestyles, becoming new economic growth points. Digital archives information is an important type of archives information. Research on the digital archives information security system is of great significance to promote the construction of archives informatization and the development of archives, and to improve the national information security system.

Keywords

digital archive information; security guarantee; system

关于加强档案信息安全保障体系的思考

李栋

北京工业大学，中国 · 北京 100124

摘　要

加强信息安全保障体系的迫切性信息是社会发展的重要战略资源。信息技术和信息产业正在改变传统的生产、经营和生活方式，成为新的经济增长点。数字档案信息是档案信息的一种重要类型，研究数字档案信息安全保障体系问题，对于促进档案信息化建设和档案事业发展，完善国家信息安全保障体系具有十分重要的意义。

关键词

数字档案信息；安全保障；体系

1 引言

档案是国家的宝贵财富，是不可再生的重要信息资源，又具有一定的保密性，因此建立档案信息安全保障体系显得尤为重要。档案信息安全保障能力已经成为检验档案信息资源的保护能力、利用服务能力和档案事业软实力的重要指标。

档案信息安全，是指构建动态的档案信息安全保障体系，确保档案信息的真实性、完整性、保密性、可用性、可控性。要保证档案信息的安全，就必须考虑到硬件、软件、数据、人员、物理环境、人文环境等多方面要素。档案信息系统的复杂性、开放性及面临威胁的多样性，决定了其安全防护是一项整体性的、综合性的系统工程 [1]。

档案信息安全保障体系由档案信息安全法律法规体系、安全管理体系和安全技术体系三部分组成。

2 安全法律法规体系

信息安全首先需要建立档案信息安全法律法规体系，做到有法可依。该法律法规分布于档案专业的内部和外部。内部有涉及安全问题的档案法律法规，外部有涵盖档案管理的信息安全法律法规。

2.1 涉及安全问题的档案法律法规

《中华人民共和国档案法》是中国档案法律法规的基石，在《档案法》及其实施办法的基础上，近年来中国档案界陆续制定出一些关于或涉及档案信息安全的规章、标准和规范性文件。如国家档案局 2002 年颁发的《全国档案信息化建设实施纲要》和国家标准《电子文件归档与管理规范》中均有针对档案信息安全的具体规定；2013 年组织制定了《档案信息系统安全等级保护定级工作指南》（档办发〔2013〕5 号）

 DOI: https://doi.org/10.36956/iser.v2i1.360

以落实国家信息安全等级保护制度。很多地方和单位也颁发了档案信息安全保管方面的规章制度，如上海市档案局颁发的《上海市档案条例》《上海市档案信息化建设实施意见》中均有关于确保档案安全的条款。江苏省档案局颁发的《江苏省档案信息化建设保密管理办法》、黑龙江省档案局颁发的《黑龙江省档案信息化建设保密管理办法》等都专门针对档案信息化安全体系建设。

2.2 涵盖档案管理的信息安全法律法规

中国档案信息化建设尚处发展初期，专门针对档案信息安全制订的法律法规较少，档案信息安全法律法规体系的主要内容仍由涵盖或涉及档案信息安全的信息安全法规构成。这些综合性的信息安全法律法规为档案信息安全提供了基本的法律规范，也应列入档案信息安全法律法规知晓和执行的范畴，同时，对制定和完善档案信息化的专门法律法规具有依据和参考价值。

中国自 20 世纪 90 年代初开始重视信息安全的法律法规建设。1997 年 3 月修订的新刑法中开始加入了信息安全方面的内容。《刑法》第二百八十五条规定："违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役"。第二百八十六条规定："违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常进行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚"。第二百八十七条规定："利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚"。2009 年通过的《中华人民共和国刑法修正案（七）》中对于惩治网络"黑客"的违法犯罪行为也增加了相关条款于第二百八十五条之下："违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。""提供专门用于侵入、非法控制计算机信息系统的程序、工具，或者明知他人实施侵入、非法控制计算机信息系统的违法犯罪行为而为其提供程序、工具，情节严重的，依照前款的规定处罚"。这些条文从惩戒计算机犯罪的角度来保障网络系统的安全。作为国家最重要的法律之一，刑法条款对计算机犯罪具有相当的威慑力。

在行政法规与规章方面，国务院、各级地方政府陆续制订了一系列信息安全规范。其中，由国务院直接颁发的、具有指导性质的行政法规是《中华人民共和国计算机信息系统安全保护条例》（1994 年 2 月）、《中华人民共和国计算机信息网络国际联网管理暂行规定》（1996 年 2 月）、《信息网络传播保护条例》（2006 年 5 月）。工业和信息化部按照国务院要求进一步制定了《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法》（1998 年 2 月）、《通信网络安全防护管理办法》（2009 年 12 月）等。

国家公安部从网络系统安全保护和安全监控出发制定了《公安部关于对与国际联网的计算机信息系统进行备案工作的通知》（1996 年 1 月）、《计算机信息系统安全专用产品分类原则》（1997 年 4 月）、《计算机信息系统安全专用产品检测和销售许可证管理办法》（1997 年 12 月）、《计算机信息网络国际联网安全保护管理办法》（1997 年 12 月）、《计算机病毒防治管理办法》（2000 年 3 月）、《互联网安全保护技术措施规定》（2005 年 12 月）等文件。2007 年公安部与国家保密局、国家密码管理局、国务院信息化办公室共同制定了《信息安全等级保护管理办法》。国家保密局则从网上信息安全保密责任出发制定了《计算机信息系统保密管理暂行规定》（1998 年 2 月）、《计算机信息系统国际联网保密管理规定》（2000 年 1 月）。

归纳起来，国家和地方各级政府制定的有关信息安全的法规制度，主要是从机房建设的安全保护规范、通信设备进网认证制度、国际接口专线制度、国际联网经营许可证制度和接入登记制度、联网备案制度、安全等级制度、安全产品销售许可证制度、保护信息安全规章、网络利用限制和安全责任制、计算机病毒防治制度、安全报告制度、安全违规犯法惩治制度等方面对信息安全进行规范。

中国许多行业还根据自身的实际情况制定本行业的信息安全保护规章。例如，公安部和中国人民银行联合颁布了《金融机构计算机信息系统安全保护工作暂行规定》（1998 年 8

 DOI: https://doi.org/10.36956/iser.v2i1.360

月），以加强金融系统的信息安全保障；中国人民银行向银行金融业发布《网上银行系统信息安全通用规范》等。军队系统则根据《中华人民共和国计算机信息系统安全保护条例》第二十九条，“军队的计算机安全保护工作，按军队的有关法规执行”的要求，自 1989 年起先后发布了《军用通信设备及系统安全要求》《军队通用计算机系统使用安全要求》《军用计算机安全评估准则》《指挥自动化计算机网络安全要求》等规章，对军队信息系统的安全管理作出了严格的规范。

在上述安全法规的基础上，档案界加强了对档案信息安全的行政执法，认真查处档案信息安全隐患和档案违法案件。随着信息技术的不断发展，档案工作者应不断进行档案信息化安全管理的研究以及跟踪最新的安全技术，对档案信息化安全管理工作的效果进行及时的分析和评估，不断完善安全防范体系。在保障档案信息安全的过程中，逐渐健全档案信息安全管理制度，提高管理人员的安全意识以及管理水平，充分发挥档案工作人员、技术人员以及用户的积极作用，为推动中国档案信息化安全保障工作贡献力量 [2]。

3 安全管理体系

档案信息安全是基于技术的管理工程。从管理层面上讲，就是要确保档案信息的安全，必须在风险分析的基础上确立档案信息安全的策略、方针和目标，成立相应的管理机构，确立合理的管理机制，制定安全管理计划，分解安全管理职责，执行安全管理制度和管理标准，建立并实施完善的档案信息安全体系。因此，风险识别与风险评估是档案信息安全管理的基础，风险控制则是安全管理的最终目的。

3.1 档案信息安全系统管理模式

新的风险在不断出现，档案信息系统的安全需求也会随之不断变化，因此安全管理应是动态的、不断改进的持续发展的过程。档案信息安全管理模型可选择 PDCA 模式，即计划（Plan），执行（Do）、检查（Check）和行动（Action）的持续改进模式。采用 PDCA 管理模式，每一次的安全管理活动循环都是在已有的安全管理策略指导下进行，每次循环都会通过检查环节发现新的问题并采取行动予以改进，从而形成安全管理策略和活动的螺旋式提升。

信息安全管理 PDCA 持续改进模式把 PDCA 管理模式与安全要求、风险分析有机地结合在一起，考虑了信息安全中的非技术因素，同时加强了信息安全管理，具有广泛的适用性。

3.2 档案信息安全系统管理的具体实施

在档案信息安全管理模式中，档案信息安全管理中心是整个系统的核心，每一个环节都要定期地与档案信息安全管理中心进行安全信息交流，当档案信息安全管理中心认为有必要对其安全目标进行修改时，要及时向上级领导汇报，等待最终的定夺。

3.2.1 完善组织机构

有条件的档案部门可以成立档案信息安全管理中心，负责实施和监控整个档案信息安全管理活动。安全管理中的每一个环节都必须与安全管理中心进行信息交流，安全管理中心还具备评价数字档案信息安全管理体系运作情况的功能，可以对安全方针、安全制度和安全措施的实施结果进行调查，并分析这些安全举措对档案信息安全的影响，然后提出相应的改进方案。数字档案信息安全管理中心由部门领导、信息管理专家、信息技术专家和技术雄厚、人员稳定的开发队伍、有关的工作人员组成。

3.2.2 进行风险评估

根据最新的研究数据，在全部的计算机安全事件中，约有 60% 是人为因素造成，属于管理方面的失误比重高达 70% 以上，在这些安全问题中 95% 是可以通过科学的风险评估来避免的。

因此，档案部门必须清楚档案信息系统现有以及潜在的风险，充分评估风险可能带来的威胁和影响，这是档案信息化建设必须首先解决的问题，也是制定信息安全策略的基础与依据。进行风险评估，不只在明确风险，更重要的是为数字档案信息安全管理提供基础和依据。

风险评估是一项费时、需要人力支持以及相关专业或业务知识支持的工作。风险评估应遵循以下原则：

（1）安全、风险和成本均衡分析原则。即用最小的成本达到适度安全的需求。

（2）整体性原则。运用系统工程的原理进行网络信息安全的整体解决方案设计，以达到完整性的要求。

（3）可用性和易操作性原则。信息安全系统对于操作者应该是可用的，操作应该是简单易行的。

（4）适应性和灵活性原则。安全策略必须随着网络性能和安全需求的变化而变化，适应性强，易修改。

 DOI: https://doi.org/10.36956/iser.v2i1.360

3.2.3 制定安全策略

制定档案信息的安全策略，要在完善配套、科学合理的有关数字档案信息安全的法制和标准体系下，通过有效的信息安全技术和安全管理遏制来自外部和内部的攻击，增强安全防护能力和隐患发现能力，确保数字档案信息资源内容和信息载体的安全，达到所需的安全级别，具体安全策略可分为内部建设安全策略和网间互联安全策略等，循序渐进逐步加以完善，最终形成功能强大的数字档案信息安全管理体系。

制定安全策略时不能脱离实际，过于理论化或限制性太强的安全策略可能导致工作人员的漠视。因此在安全策略制定时必须遵循以下原则：越符合现状越容易推行，越简单越容易操作，改动越小越容易被接受。档案信息安全策略需要根据信息技术发展、自身的安全需求进行不断的修改和更新，以保证档案信息安全不受新的信息安全风险的影响。

3.2.4 开展数字档案信息安全管理培训

开展数字档案信息安全培训是档案信息安全管理体系的重要环节之一，特别是各关键岗位的人员，对档案信息的安全起到重要作用。在实际工作中，大部分档案信息安全问题都是由人为因素造成的。人本身就是一个复杂的信息处理系统，还会受到自身生理因素和心理因素的影响，受到技术熟练程度、责任心和道德品质等多方面的影响。因此对于档案部门工作人员的培训不应是“一次性”的活动，需要定期对人员进行安全策略及安全技术的“应知、应会”培训，尤其是安全策略更改或面临新的安全风险、部署新的安全解决方案之后，更要对其加强培训，以保证安全策略的有效程度。

3.2.5 贯彻执行管理决策

管理决策的贯彻执行必须依靠人来完成，虽然档案信息安全保障体系的建设涉及档案部门方方面面的因素，但归根结底的因素是“人”。没有机构人员的认可、理解与支持，就没有实施数字档案信息安全管理保障体系的前提；没有档案部门的有力组织协调，则很难保证信息系统建设的顺利进行；没有相关实施人员的互相配合和出色工作，无法使信息系统中各模块的信息无缝集成；没有具体业务人员及时准确地收集各种基础信息，就没有信息系统的输出；没有资深咨询顾问的正确指导，信息系统实施就难免多走弯路，甚至有可能失败。

3.2.6 持续完善管理体系

首先，确定待评价系统的边界和范围，明确评价的目的，以系统整体为立足点，总体分析各方面的效益与成本，及其与系统各构成部分的关系；其次，确定待评价系统的状态与所处的阶段，如可行性分析、总体设计、系统开发与运行等各阶段；再次，选择适当的评价方法，如结果观察法、类比一对比法、专家评价法或评分法等，确定适当的评价指标；最后，收集有关数据、资料进行分析、计算，得出评价结果，并将评价结果书面化。根据评价结果进行不断完善，提高档案信息安全管理体系及具体实施过程的有效性和效率，以满足自身、用户和其他相关方日益增长和不断变化的需求与期望。

目前，建立信息安全管理体系的方法已经制定为国际标准 USO/IEC 17799：《2000 信息安全管理实施细则》。中国在 2005 年 6 月颁布了相应的推荐性国家标准《信息技术信息安全管理实用规则》（GB/T 19716−2005）、《信息技术信息技术安全管理指南第 1 部分：信息技术安全概念和模型》（GB/T 19715.1−2005）、《信息技术信息技术安全管理指南》第 2 部分《管理和规划信息技术安全》（GB/T 19715.2−2005），这些标准主要参照了国际标准 ISO/IEC17799.ISO/IEC27001，ISO/IECTR13335 等。上述标准在管理策略、环境控制、组织结构、人员责任规范、操作程序以及技术手段上都提出了一系列指导性规范，各单位可参照上述国际和国家标准建立适合本单位的档案信息安全管理体系，保证档案信息的安全。

4 安全技术体系

目前，档案信息安全在技术方面主要采用信息加密技术、信息确认技术、访问控制技术、病毒防治技术、审计技术、防写技术等。

4.1 信息加密技术

加密是保障信息安全最基本、最经济的技术措施，也是大多数信息防护措施的技术基础。加密的作用是防止敏感的或有密级限制的信息在传输过程中泄密。

文件加密所采取的加密算法形形色色。据不完全统计，目前已经公开发表的加密算法多达数百种。电子文件加密的基本过程是：存储或传输前将原先借助相应的软件可以识读的数码序列（称为明文）通过数学变换（加密运算）变成无法识读的“乱码”（称为密文或密码）；利用时再通过数学

 DOI: https://doi.org/10.36956/iser.v2i1.360

变换（解密运算）将“乱码”还原成可以识读的数码序列。其中，加密运算和解密运算都是在一组密钥控制下进行的，密钥是控制加密算法和解密算法实现的关键数据。

密钥对非授权者是保密的，因此，可防止非法用户破解密钥而窃获文件内容。根据文件加密和解密时所使用的密钥是否相同，加密算法可以分为对称加密解密法和非对称加密解密法两种。

在对称加密解密法中，加密密钥和解密密钥是相同的，或者知道其中一个密码就可以方便地推算出另外一个密码，因此密钥必须绝对保密。问题是，在发送加密文件之前首先通过安全渠道将密钥分发到双方手中，其传递中很容易造成密钥泄漏。而且，如果某涉密文件分发的单位多，密钥的安全控制会有很大的难度。这种方法在对涉密文件进行静态管理时比较有效，如自己撰写的保密文件给自己使用，防止被人偷看。目前，Word.Excel 文件的加密就是采用对称加密解密法。然而，如果涉密文件需要传输，特别在大范围传播时，就需要用下面的方法。

非对称（又称双钥）加密解密法中，加密方和解密方使用的密钥是不相同的，密件经办人需预先准备两把钥匙，一把公钥，一把私钥。当发送密文时，发送者使用收文者的公钥，将文件加密后发给收文者，收文者收到密文后，用自己的私钥解密文件。由于只有拥有该私钥的收文者才能解密这份文件，所以文件的传递过程是安全的。

4.2 信息确认技术

对于纸质文件，以往用书面签署或签印的形式将责任者名或责任者特征（如指纹）固化到文件载体上，借助纸质文件载体与内容的不可分离性来证明文件内容的原始性和真实性，使文件具备法律效用。这种方法显然不适于不具有恒定载体的电子文件。对于虚拟流动的电子文件，信息确认技术起到了相当于签署纸质文件的作用。

信息确认技术是通过一定的技术手段防止文件的内容被非法伪造、篡改和假冒，同时用来确认文件的发出、接收过程及利用者身份和权限的合法性。完善的信息确认方案应能实现以下四个目标：

第一，合法的文件接收者能够验证其收到的档案文件是否真实；

第二，发文者无法抵赖自己发出了所发的文件；

第三，合法发文者以外的人无法伪造文件；

第四，发生争执时，具有仲裁的依据。

实现上述目标需要综合采用多种技术手段，目前，常用的有数字摘要技术、数字签名技术和数字水印技术。

4.2.1 数字摘要技术

文件的发送者采用某种特定算法（摘要函数算法）对发文进行运算，获得相应的摘要（即验证码），摘要具有这样的性质：如果改变发送文件的内容，即便只是其中一个比特，获得的摘要将发生不可预测的改变。摘要将作为发送文件的一部分附加在文件后一起发出，接收者则利用双方事先约定好的摘要算法对收到的文件作同样运算，并比较运算所得的摘要与随文件发送来的摘要是否一致，以此鉴定收到的文件是否在发送过程中受到篡改。如果摘要函数（相当于前面的密钥）仅为收发文件的双方所知，通过上述报文认证即可达到信息确认的上述四个目标。这种方法的缺点是：因收发文双方使用相同的摘要函数，因而，摘要函数本身的安全保密性是一个很大的问题，多次使用的摘要函数一旦被第三者窃获，报文认证便不再安全。

4.2.2 数字签名技术

随着中国《电子签名法》的生效，数字签名在法律与技术上走向成熟。数字签名是指数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据，而数据电文是指以电子、光学、磁或者类似手段生成、发送、接收或者储存的信息。

从技术上看，数字签名是非对称加密技术的一种，其基本原理类似于上述报文摘要技术。首先，签名者使用签名软件对拟发送的数据电文（电子文件）进行散列函数运算，生成报文摘要；然后，由签名软件使用签名者的私钥对摘要进行加密，加密后的报文摘要附着在电子文件之后，连同签名者从认证机构处获得的认证证书（用以证明其签名来源的合法性和可靠性）一同传送给文件接收者。文件接收者在收到上述信息后，首先使用软件用同样的散列函数算法对传来的电子文件进行运算，生成报文摘要，同时，使用签名者的公钥对传送而来的报文摘要进行解密，将解密后的报文摘要和接收者运算生成的报文摘要进行比较，如果两个摘要一样，就表明接收者成功核实了数字签名。在核实数字签名的同时，接收者的软件还要验证签名者认证证书的真伪，以确保证书

 DOI: https://doi.org/10.36956/iser.v2i1.360

是由可信赖的认证机构颁发的。经核实的数字签名向文件的接收者保证了两点：第一，文件内容未经改动；第二，信息的确来自签名者。

签名者所用的数字签名制作工具（公钥、私钥、散列函数、软件等），不是由签名者自行制作的，而是由合法成立的第三方电子认证服务机构在充分验证发文者真实身份后提供的。电子认证服务机构颁发的数字签名制作数据及认证证书相当于网上身份证，帮助收文、发文者识别对方身份和表明自身的身份，具有真实性和防抵赖功能。与物理身份证不同的是认证证书还具有安全、保密、防篡改的特性，可对电子文件信息的传输提供有效的安全保护[3]。

4.2.3 数字水印技术

数字水印类似于传统印刷品上的水印，用以鉴别电子文档的真伪。数字水印技术是日本电气公司于 1997 年投入使用的技术，它是在传输的文本、图像、音频、视频等电子文件中附加一个几乎抹不掉的印记，无论文件作何种格式变换或处理，其中水印不会变化。该印记在通常状态下隐匿不现，除非用特殊技术检测。

一旦这种水印遭到损坏，文件数据也会受到破坏。

上述信息确认技术的实质是，文件发送者将签署信息（加密运算方法）以不可分离的方式与文件内容（而不是纸质文件的载体）“编织”一体，使他人无法在不改变签署信息的前提下改变文件内容，或者相反（就像无法不改变载体而改变纸质文件上的内容一样），而收文者则通过验证其信息内容中的签署信息来证实文件内容的原始性和发文者的原真性。

4.3 访问控制技术

访问控制是信息系统安全防范和保护的主要策略，其任务是杜绝对系统内电子文件信息的非法利用和蓄意破坏。访问控制技术种类繁多，且相互交叉，目前主要有以下两类：

4.3.1 防火墙

防火墙是设置在被保护文件系统和外部网络之间的一道屏障，以防止发生不可预测的、潜在的、破坏性的侵入，它可通过监测、限制跨越防火墙的数据流，尽可能地对外屏蔽系统内部的信息、结构和运行状况，实现内部网络的安全保护。防火墙可分为外部防火墙和内部防火墙。前者在内部网络和外部网络之间建立一个保护层，以防止“黑客”的侵袭，挡住外来非法信息，并控制敏感信息被泄露；后者将内部网络分隔成多个局域网，以此控制越权访问。防火墙可以是一个路由器、一台主机，也可以是路由器、主机和相关软件的集合[4]。

电子文件系统在选择、使用防火墙时，应对防火墙所采用的技术、种类、安全性能及不足之处有充分认识：

（1）认真权衡防火墙的安全性能和通信效率，在文件安全和方便利用两者之间将安全放在第一位。

（2）对于中小型的文件管理系统，如果系统内外交换的信息量不是很大，信息重要程度属于一般，可以采用数据包过滤和代理服务型防火墙；而对于大型文件管理系统或信息安全要求较高的系统，可以考虑采用复合型防火墙。在系统安全和投资费用之间应进行权衡，不可不计代价地追求超出可能风险的安全性。

（3）对防火墙进行管理时，除了解防火墙的益处之外，还应了解防火墙自身的局限与不足。

（4）使用防火墙对外隔离时，不能忽视防火墙内部的管理，因为许多攻击来自内部。必要时可设置第二道防火墙，使内部网络服务器对内也被隔离（但这样会大大降低系统的效率）。

（5）为更好地保护文件管理系统，尽量考虑采用中国自主开发的防火墙产品。

（6）防火墙属于信息安全产品，国家规定实行强制认证，在文件管理系统中使用的防火墙必须是经国家认证的产品。

4.3.2 身份验证

为防止未经授权的用户操作文件管理系统中的各类资源，通常在用户登录或实施某项操作之前，系统将对其身份进行验证，并根据事先的设定来决定是否允许其执行该项操作。验证过程对用户而言就是要提供其本人是谁的证明。身份验证的方法很多，并且不断发展。但其验证对象有三：所知信息（如口令）、所持实物（如智能卡）、所具特征（如指纹、视网膜血管图、语音等）。口令是最普通的手段，但可靠性不高，智能化的“口令”是系统向被验证者发问的一系列随机性问题，以其回答来验证身份。以指纹、视网膜血管图、声波纹进行识别的可靠性较高，但需要使用指纹机等特征采集设备，代价较大。智能卡技术将逐步成为身份验证技术的首选方案。智能卡是密钥的一种媒体，性状如信用卡，由授权用户持有并由该用户赋予其一个口令或密码字。该密码与内部网络服务器上注册的密码一致。为提高身份验证的

 DOI: https://doi.org/10.36956/iser.v2i1.360

可靠性，可将上述三种手段结合起来使用。

4.4 病毒防治技术

即使采用防火墙、身份验证和加密技术，文件系统仍然可能遭到病毒的攻击。防治病毒包括两个方面：一是预防，在系统或载体未染毒之前采取有效措施，防止病毒感染；二是杀毒，在确认系统或载体已染毒后彻底将其清除。防毒是根本，杀毒则是补救措施，目前普遍使用的是以特征扫描为基础的杀毒软件。

文件网络环境下的防毒、杀毒需要注意以下几点：

（1）从客户机和服务器两个方面采取杀毒防毒措施°电子文件管理系统有的采用客户机 / 服务器模式，客户机、服务器都可能遭受病毒侵害，因此，必须同时展开防毒杀毒工作。作为局域网入口的工作站，不仅受病毒攻击的可能性更大，而且数量较多，管理分散，往往是最薄弱的环节，必须重点设防。对于功能简单的工作站尽可能设置成无盘工作站，并在所有工作站上都安装防病毒卡或芯片。服务器是整个网络的“中枢神经”，是网络信息资源的集中地，是防毒工作的重点。防止服务器被病毒感染的主要措施是：尽量少设超级用户；将系统程序设置为只读属性，对其所在的目录不授予修改权和管理权等 [5]。

（2）由于病毒不断变异，杀毒软件也不断升级，网络管理员与档案管理人员应注意及时更新杀毒软件的版本类型，选用最先进、可靠的防杀网络病毒软件。

（3）加强对网上资源的访问控制，防止非法用户进入网络，充分利用网络操作系统和文件管理系统所具有的安全管理功能。

防毒杀毒是一项系统工程，必须从管理和技术两方面着手，采取综合措施建立起完善的病毒防治体系。

4.5 审计技术

审计技术旨在记录电子文件运行处理的全部过程，抑制非法使用系统的行为。采用审计技术的电子文件管理系统将自动记录下系统运行的全部情况，形成系统日志。系统日志类似于飞机上的“黑匣子”，是系统运行的记录集，内容包括与数据、程序以及和系统资源相关的全部事件的记录，如机器的使用时间、敏感操作、违纪操作等。审计记录为电子文件真实性的认证提供了最基本的证据，借助系统日志，管理员可以分析出系统运行的情况，追踪事件过程，排除系统故障，侦察恶意事件，维护系统安全，优化对系统资源的使用。系统日志包括哪些内容必须根据文件系统的安全目标和操作环境个别设计。

4.6 防写技术

防写技术是保障电子文件内容不被修改所采取的安全技术，其目的是通过技术手段来固定处于静态的电子文件的内容信息。大多数文件管理系统具有将运行其中的文件属性设置为“只读”状态的功能，在只读状态下，文件内容只能读取，不能更改，除非具有高级权限的用户来更改文件的“只读”属性。另一个简单的技术手段是将文件内容刻录到 CD-R 光盘、WORM 磁盘等一次性写入存储介质上，这些不可逆式（无法改写已写入的内容）的存储载体有效防止了对静态电子文件内容的改动，保证了电子文件的真实性和完整性。

参考文献

[1] 宗文萍 . 档案信息安全保障体系建设研究 [J]. 档案学通讯 2006(01):51-54.

[2] 项文新 . 构建基于信息安全风险评估的档案信息安全保障体系必要性研究 [J]. 档案学通讯 ,2008(01):56-59.

[3] 张勇 . 数字档案信息安全保障体系研究 [D]. 苏州 : 苏州大学 ,2012.

[4] 陈亮 . 数字档案信息安全保障体系研究 [J]. 黑龙江史志 ,2015 (05):164.

[5] 王玉杰 , 苏卫东 . 档案信息化与档案信息安全保障体系建设 [J]. 机电兵船档案 ,2012(04):68-70.