信息科学与工程研究

Information Science and Engineering Research

Volume 2 Issue 1 March 2021 ISSN 2737-4815(Print) 2737-4823(Online)

NASS
NAN YANG ACADEMY OF SCIENCES

《信息科学与工程研究》为全球电子信息与工程同行发表有创见性的学术论文，介绍有特色的科研成果，探讨有新意的学术观点提供理想园地，扩大国际交流。以从事电子信息技术开发的科研人员、工程技术人员、各大专院校师生、计算机爱好者为主要作者和读者群体。本刊是一本拥有高水准的国际性同行评审团队的学术期刊出版物，编委鼓励符合本刊收稿范围的，有理论和实践贡献的优质稿件投稿。

为满足广大科研人员的需要，《信息科学与工程研究》期刊文章收录范围包括但不限于：

· 通信与安全
· 指导与传感技术
· 计算机网络
· 计算机应用技术
· 信息科学
· 电子通信工程

Nanyang Academy of Sciences Pte. Ltd.
12 Eu Tong Sen Street #07-169 Singapore 059819
Email: info@nassg.org
Tel: +65-65881289
Website: http://www.nassg.org

About the Publisher

Nanyang Academy of Sciences Pte. Ltd. (NASS) is an international publisher of online, open access and scholarly peer-reviewed journals covering a wide range of academic disciplines including science, technology, medicine, engineering,education and social science. Reflecting the latest research from a broad sweep of subjects, our content is accessible worldwide – both in print and online.

NASS aims to provide an analytics as well as platform for information exchange and discussion that help organizations and professionals in advancing society for the betterment of mankind. NASS hopes to be indexed by well-known databases in order to expand its reach to the science community, and eventually grow to be a reputable publisher recognized by scholars and researchers around the world.

Database Inclusion

Asia & Pacific Science Citation Index

Creative Commons

MyScienceWork

Google Scholar

Crossref

China National Knowledge Infrastructure

信息科学与工程研究

Information Science and Engineering Research

主　编

陈惠芳

浙江大学，中国

编　委

曾念寅　Nianyin Zeng

刘新华　Xinhua Liu

涂　锐　Rui Tu

李绍滋　Shaozi Li

刘士虎　Shihu Liu

马建伟　Jianwei Ma

朱昌明　Changming Zhu

 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.

 DOI: https://doi.org/10.36956/iser.v2i1.361

Preliminary Study on the Safety Maintenance of Computer Network System

Shengliang Wu

Changchun University of Finance and Economics, Changchun, Jilin, 130122, China

Abstract

With the development of the times, the Internet has become more and more popular, and the Internet has brought great convenience to people. However, because the Internet is an open, uncontrolled network, it is often attacked by computer viruses and hackers. It can cause computer and computer network data and files to be lost, and the system is paralyzed. Therefore, the security of computer network systems must be put in the first place.

Keywords

computer network; system security; maintenance; management

计算机网络系统安全维护初探

武胜良

长春财经学院，中国 · 吉林 长春 130122

摘　要

随着时代的发展，Internet 日益普及，网络已经给人们带来了极大的方便。但由于 Internet 是一个开放的，无控制机构的网络，经常会受到计算机病毒、黑客的侵袭。它可使计算机和计算机网络数据和文件丢失，系统瘫痪。因此，计算机网络系统安全问题必须放在首位。

关键词

计算机网络；系统安全；维护；管理

1 计算机安全的概念及其重要性

1.1 计算机安全的概念

从概念来讲，计算机安全就是通过各种先进的管理方法及技术手段，使计算机能够得到相应的保护，进而提高计算机网络的安全性，使计算机无论是从硬件上，还是从软件上，都能具有较高的安全性，从而使网络信息得到全面的保护，确保网络信息的机密性。计算机安全具体可划分为两个层面的安全，一种是硬件层面上的安全，另一种则是系统层面上的安全。

1.2 计算机安全的重要性

人们在生产生活中越来越依赖于计算机，这也使计算机网络安全变得日益重要，其直接关系到个人财产、隐私及人身安全。在中国社会发展中，计算机网络安全更是已经成为确保社会和谐稳定发展的关键所在。

计算机网络安全的重要性主要体现在以下几个方面：其一，只有确保计算机网络的安全，才能使计算机网络在安全的环境下得以正常使用，现阶段，人们在使用计算机时，经常需要将各种敏感信息存储至计算机网络中，如果计算机网络不够安全，便可能造成用户的信息被泄漏，进而对用户的切身利益造成严重侵害；其二，只有在计算机网络安全的前提下，才能使计算机网络的各项功能得以充分发挥，进而使人们能够通过计算机来进行更加高效的生产，在提高生产效率，计算机也能提升人们的生活品质，从而确保用户的相关信息不会发生泄漏或被他人利用。因此，无论是对个人来说，还是对组织来说，都要对计算机网络安全进行高度重视，使计算机网络能够真正高效、安全的应用于日常生产生活之中。

1.3 计算机工程安全隐患分析

1.3.1 病毒攻击

在计算机网络使用中，病毒攻击无时无刻不在发生着，这也使计算机病毒成为其网络安全的一大关键隐患。计算机

 DOI: https://doi.org/10.36956/iser.v2i1.361

网络所受到的违法攻击，都是以病毒作为其核心内容的，对于病毒来说，只要计算机网络中的代码发生改变，便可能会为计算机病毒提供可乘之机，从而使病毒入侵用户的计算机，对计算机的程序进行修改，使计算机无法得以正常运行，大大影响了计算机系统各种功能的发挥。比如，著名的熊猫烧香便是一种典型的计算机病毒，该病毒属于一种变种的蠕虫病毒，用户的计算机一旦中了这种病毒，便会出现频繁重启和蓝屏问题，同时其计算机中所有的 exe、pif、asp、com 等可执行文件均会出现熊猫烧香的文件，进而造成用户无法正常使用计算机，据统计，至少有数千家企业及政府机关受到感染，感染范围非常广泛，这给用户造成了巨大的经济损失，严重影响了社会的和谐稳定。可见，计算机网络病毒的攻击，已经成为计算机网络中的关键安全隐患。

1.3.2 WWW 欺骗技术

在计算机网络使用中，人们常常需要通过浏览器来访问某些网站，部分网站在进行访问时，都需要用户具有相应的访问权限，如果不具备访问权限，用户是无法对这些网站进行访问的。而不法分子为了窃取个人隐私及重要信息，便采取非法访问的方式，通过各种非法程序、含病毒软件来攻击这些网站，进而造成网站崩溃，导致用户无法正常访问这些网站，更对网站经营者造成巨大的经济损失。这种非法访问的方式，便是比较常见的 WWW 欺骗技术，该技术是通过 IE 浏览器来进行的，通过伪装某些 Web 站点，来欺骗不知情的用户对这些 Web 站点进行访问，当用户进入伪装的 Web 站点后，不法分子便会通过系统漏洞侵入到用户计算机中，窃取用户计算机中存储的敏感信息，从而给用户造成巨大损失。

1.3.3 系统安全性不高

除了病毒攻击与 WWW 欺骗技术以外，计算机网络系统的自身安全性，也同样是计算机网络关键安全隐患之一。人们在使用计算机网络获取信息时，是无法保证信息的准确性，而且计算机网络具有高度的共享性，这使计算机网络中存在着大量的共享信息，而用户在获取这些共享信息时，便难以保证计算机系统是否具有较高的安全性与实效性。信息共享能够为远程管理提供便利，不过其对用户的计算机却并没有较大的意义，反而会为不法分子提供入侵途径，一旦计算机用户在通过网络获取共享信息时，没有开启防火墙，便会大大增加其受到不法分子攻击的概率。

1.3.4 计算机操作不当

用户自身对计算机的操作行为不当，也可能成为计算机网络的关键安全隐患。不法分子为了获得不当利益，往往通过计算机来进行网络欺诈或窃取信息，这对中国社会的稳定和谐造成了巨大的不利影响。由于计算机网络的安全设置众多，而人们在使用计算机网络时却并没有了解这些安全设置的功能，更没有对其计算机安全有所重视，这也导致其在使用过程中可能会存在操作不当、误操作等行为，从而使计算机无法得到有效的安全防护，进而为不法分子对用户计算机的入侵提供了帮助。

1.4 计算机网络安全保障技术研究

1.4.1 防病毒技术

要想提高计算机网络的安全性，就必须要研究出更加先进的防病毒技术。用户可通过防病毒监控软件来进行病毒攻击检测，当软件检测到有病毒攻击用户计算机时，会自动发出预警信息，并提示用户进行有效应对。此外，用户还要定期更新病毒数据库，在访问网站或下载软件时，必须要了解网站与软件的安全性，尽可能地不要访问存在安全风险的网站和软件。防病毒技术主要分为三类，分别是防火墙技术、入侵检测技术以及 VPN 技术，其中，防火墙具有动态分组过滤、入侵检测、代理服务器以及 VPN 监视等多种功能。而入侵检测技术则能够检测计算机中正在进行的危险活动，并将这些危险活动完全隔离在某个分区中来进行限制，以此提高计算机网络的安全性。VPN 技术是在网络中建立一个 VPN 通道，并由 VPN 通道来进行机密数据和敏感信息的传输。VPN 技术中可结合数据加密技术、用户认证技术、密钥技术共同使用来提高计算机网络的安全性。

1.4.2 系统安全优化技术

在系统优化技术中，需要通过防火墙技术来进行系统安全防护，提高计算机网络系统的安全等级，通过防火墙技术，能够使系统对接收或下载的数据信息进行自动检测，一旦检测到数据信息含有安全风险，防火墙会自动提醒用户，并切断内网和代理服务器之间的联系，从而确保病毒无法传播到用户的计算机中。此外，在系统安全优化中，还能通过访问权限的控制来限制不具备访问权限的非法用户访问系统，用户在利用浏览器进行 Web 访问时，还可通过安全软件检测到存在安全风险的网站，并提醒用户不要试图访问。

 DOI: https://doi.org/10.36956/iser.v2i1.361

1.4.3 数据加密与访问控制技术

用户在使用计算机网络时，为了确保计算机在发送、传输和下载数据时不会被黑客所窃取，还可采取数据加密技术来对数据进行加密，对方在接收到数据后，要想查看数据，就必须要使用密钥来对这些数据进行解密，从而大大提高了数据信息的安全性，使不具有权限的人员即使截获了数据，也无法成功破译。访问控制技术也是计算机网络的重要安全保障技术，该技术能够对用户的访问权限进行设置，从而防止不具有访问权限的用户非法访问网站。并且，还可通过 VPN 网络的应用来建立 VPN 网络，从而大大提高了计算机网络的安全性。

2 计算机系统的脆弱性及安全维护

现如今，计算机在具体实践中日常生活中运用广泛，计算机系统是计算机的重要组成部分之一，和人们的生活息息相关。同时由于计算机系统的脆弱性，计算机系统容易面临安全威胁，就会造成信息的泄露，资料的丢失，从而严重影响人们的生活。因此，对计算机系统进行安全维护会减弱和避免此类影响，保障计算机的安全使用。

2.1 操作系统脆弱性的产生原因

2.1.1 系统的开发体系结构不安全

近年来，计算机技术可谓是迅猛发展，发展速度很快的同时自然会出现一些问题，计算机系统也是如此，仅有这么几十年的历史就已经不断地发创新，其热度可见一斑，但这么短短的几十年中，人们对于计算机系统开发的技术也不是十分的成熟，其过程也是十分坎坷，并不是一帆风顺的。因此，不成熟的技术开发出来的计算机系统就不可避免地存在漏洞。

2.1.2 应用进程管理机制存在缺陷

计算机系统作为一种运行程序，一定是以管理和执行为目的，这也是操作系统中的核心功能，但是这种机制是存在缺陷的，黑客就会利用这种缺陷进入计算机系统。如果黑客在远端执行一种访问进程，这些进程就会引发回应机制，如果说黑客把入侵软件通过此渠道植入操作系统中，那么就会非常的危险。还有，黑客们还常常利用人们所感兴趣的网站，人们在互联网上下载到本地的计算机上，这样黑客就可以合法的进行远程操控，这样，人们的电脑就成了黑客的“傀儡”，人们也就会在不知情的情况下受到损害。上述两种都是黑客利用计算机管理制度本身存在的缺陷来进入别人的电脑，从而侵害他人的利益。

2.2 完善操作系统的结构体系

首先具体实践中可以通过安装系统升级的补丁。系统的升级补丁可以更好地完善系统，通过这种对系统本身的改善和升级是最好的方法。那么如何完善这个系统结构体系，目前学界还正在有关这方面的研究。有些人指出，可以提供一种加密方式，当你建立一个文件夹时，它会自动加密，这样来说你的信息相对的就会更安全一些，如果有其他用户访问就会产生一些警告。安装杀毒软件给计算机系统一道屏蔽门

要想让计算机系统的安全得到有效维护，那么就一定要将病毒入侵的一系列防范工作做好。所以，为了让计算机病毒在系统中的进一步传播和扩散得到有效防止，则可在系统中将金山毒霸等一些正版杀毒软件加以安装，经过运行杀毒软件对计算机系统中存在的安全漏洞与木马病毒等进行定期查杀，便可以保证计算机系统不会再受到病毒的危害和干扰。

2.3 针对系统脆弱特性的意识层面解决方案

2.3.1 培养正确的计算机养护、操作习惯

在运行计算机系统之前，应当保证其处在比较安全的环境下，因此，要求人们定期对计算机进行除尘处理，同时注重将硬盘等各种硬件设备的防震与维护做好，禁止随意搬动计算机，并尽可能防止其与手机等磁场进行直接接触。此外，需保证计算机与外界设备的准确连接，而且还需将良好的安全意识加以树立，养成比较规范的操作习惯，对于来源不明的软件或者文件不可随意点击与下载，从而使计算机系统的安全运行得到有效保障。

2.3.2 建立计算机访问安全防护体系

现阶段，针对计算机网络安全防护体系来讲，其关键由安全性评价、上网保护与上网安全服务三个方面构成。在这之中，访问安全性评价通过防护漏洞与信息管理构成。安全防护主要包括病毒查杀与限制访问等。而为了让网络信息的安全可以得到有效保护，在部分网站将把 IP 地址进行隐藏，并将一些没有必要的访问端口关闭。黑客在入侵的时候，一般会对计算机端口进行扫描，因此，只要计算机用户安装了端口监视程序，那么在遇到入侵的时候，则会发出相应警告。

2.3.3 加强操作人员的思想管理与教育

上述提到的都是在国家管理或者是制度方面的建议，然

而还有一个非常重要的方面，那就是要加强操作人员的思想管理与教育，这虽然不是技术层面的，但是也很重要，如果不注重对个人思想意识的培养和提升，那么有再高端的防护技术也不能避免被黑客突破、利用。所以，要想不被黑客侵入，一方面应该从技术方面完善计算机系统，另一方面就是加强安全保护意识，只有两者的充分结合，才能最大限度地防止黑客的入侵，计算机系统才会真正的安全。

计算机系统安全已经成为各个领域高度重视的问题，黑客的攻击造成重要信息及资料的丢失，造成无法挽回的损失。因此，人们一定要养成备份的好习惯，规范操作行为，安装有效的杀毒软件，建立计算机系统的安全防护墙。总之，计算机系统的发展和完善是一个长期的过程，并不能一蹴而就，因此也不能急功近利，而且也不是一两个人就可以解决的，需要国家乃至全社会的共同努力，才能够完成。最后也希望具体实践中国家的网络计算机系统越来越完善，能更好地为人们服务。

3 结语

当前社会是一个计算机时代、信息时代和知识经济时代。随着信息化社会进程的不断加快，计算机网络技术已经在各行各业中得到了普及应用，随之而来的网络安全问题日益突出，对于网络管理与维护人员来说，必须要掌握好与网络安全相关的各项技术。论文简略地分析了当前网络时代计算机系统安全及网络安全等问题，提出了一些相应的防范措施。中国必将建立起一套完整的网络安全体系，特别是从政策上和法律上建立起有中国自己特色的网络安全体系。

参考文献

[1] 田小虎 . 计算机系统安全与计算机网络安全浅析 [J]. 现代商业 (35):188.

[2] 邱松 . 计算机网络信息系统安全防护分析 [J]. 计算机光盘软件与应用 ,2013(13):158-159.

[3] 李纳 . 计算机系统安全与计算机网络安全浅析 [J]. 科技与企业 ,2013(01):138.

[4] 余江涵 . 计算机网络信息系统安全问题的分析与对策 [J]. 智能城市 ,2017(01):62.

[5] 刘利 , 雷正桥 . 计算机网络系统安全维护策略初探 [J]. 科学咨询 (决策管理),2009:159.

 DOI: https://doi.org/10.36956/iser.v2i1.362

Technology and Products of Archives Management Information System

Guoping Zhang

Xi'an Traffic Engineering Institute, Xi'an, Shaanxi, 710300, China

Abstract

The Archives Management Information System (hereinafter referred to as AMIS) is the basic means to realize archives information management and information services. It is also one of the first application software systems for archives management business that archivists come into contact with at the beginning of the development of archives informatization work. At present, with the in-depth development of archives informatization work, some professional companies specializing in providing solutions for archives industry informatization applications have appeared on the market. At the same time, different brands of AMIS products have emerged. These products range from design concepts, R&D technologies, and safety guarantees, implementation methods, scope of application, after-sales service, and product functions, performance, and operating modes have their own characteristics.

Keywords

archives management information system; technology and products; information service; archives informationization

档案管理信息系统的技术与产品

张国平

西安交通工程学院，中国 · 陕西 西安 710300

摘　要

档案管理信息系统（以下简称 AMIS）是实现档案信息管理和信息服务的基本手段，也是开展档案信息化工作之初，档案工作者首先接触的面向档案管理业务的应用软件系统之一。目前，随着档案信息化工作的深入开展，市场上出现了一些专门提供档案行业信息化应用解决方案的专业公司，同时也出现了不同品牌的 AMIS 产品，这些产品从设计理念、研发技术、安全保障、实施方法、应用范围、售后服务以及产品的功能、性能、运行模式等方面都有其自己的特点。

关键词

档案管理信息系统；技术与产品；信息服务；档案信息化

1 AMIS 产品的设计策略分析

任何产品的研发都是依据市场和业务需求而开展工作的，这一点在业界已经达成共识。而在需求确定的情况下，由于系统设计策略的不同也会影响产品的推广应用范围。通过调研，我们总结出档案管理信息系统产品的两大设计策略，即定制策略和通用策略。

1.1 定制策略

定制策略是软件工程中快速原型法的典型应用，其特点是完全根据某一单位档案管理业务的需要进行个性化设计和开发，优点是研制出的产品能够很好地适应该单位的实际业务需要，功能模块清晰，开发任务明确，效率高，难度小，缺点是每个单位都有一个特定的产品版本，对于产品供应商而言售后服务工作量大，开发工作在低水平上重复。选择定制策略的条件是：

（1）业务模型相对固定，如专门针对人事档案管理业务开发一个管理信息系统，不考虑其他档案门类业务的信息化管理；或者是针对某个单位的业务管理模式开发一个相对固定的档案管理信息系统，因此在业务流程处理环节上存在一定的局限性。

（2）基于概念原型开发，选择某一单位的档案管理业务模型，通过快速原型法研制一个原型系统，对一些准备涉足档案信息化解决方案的单位或个人，逐渐深入行业领域是

 DOI: https://doi.org/10.36956/iser.v2i1.362

一个入门级的选择方案。

（3）选择自主开发 AMIS 的档案馆，其产品一般具有很强的针对性，但不具备将产品推广到其他单位使用的通用性，即开发的软件系统不作为商品对外销售。

1.2 通用策略

通用策略是为适应多元化业务发展的需要而出现的一种新的软件工程应用策略，目前在档案行业普遍采用，其特点是提前花费大量的时间在系统设计和实现阶段，旨在提供一个能够囊括档案行业多数业务功能和管理模式要求的通用产品，研发周期长，难度大，要求软件生产单位既懂技术又精通档案业务，开发出的产品通用性、灵活性、可扩充性等较强功能，便于推广应用。选择通用策略的前提是：

（1）研发单位在人力、物力和财力等方面实力雄厚，拥有专门的研发队伍。

（2）熟悉档案管理模式及其业务流程，并能适应业务发展的需求。

（3）及时跟踪新技术的发展，采用最新的支撑平台和现代技术。

（4）开发的产品主要用于市场化推广应用，形成产业化。

大部分自主开发的单位都采用定制策略，主要目的是将本单位的管理信息系统做到精细化管理和实用化操作，而商品化软件的开发则更倾向于采取通用策略，希望一次投入研发，能多次推广应用，并产生社会和经济效益。

单机版的 AMIS 产品大多是根据各单位业务需要进行定制开发的，虽然也有一些单机版的 AMIS 采用灵活设置数据库字段等功能，但其功能和界面都有局限性。而在网络的 AMIS 产品的调查中，大多是采用通用策略，只是通用的程度不一。有些软件产品在系统用户模型设置、数据字典、档案门类设置、系统数据库结构设计等方面实现了一定程度的灵活构建，有些单位则开发了相对通用的档案管理平台，不仅实现了数据字典、档案门类、数据库结构的通用灵活定制，而且在用户操作权限、系统个性化界面定制、档案业务处理界面中的维护字段、档案全过程业务管理流程（包括立卷、审核、移交、入库、库管、开放、转档、销毁、盘点）等方面也实现了灵活定义和设置，提供了一个通用的档案业务管理平台，可以根据用户的各种需求进行量体裁衣，实现个性化定制。

2 AMIS 产品功能和性能分析

AMIS 的功能和性能是衡量它是否实用、是否让客户满意的核心指标。

2.1 产品性能因素分析

产品性能决定产品能否被使用，直接影响产品性能的因素包括：

（1）所采用的开发平台自身的通用性、可扩展性和先进性以及生产该平台供应商的竞争力。像微软、Oracle，J2E 等一些知名的跨国公司，他们提供的研发平台在功能、性能、发展空间和市场竞争等指标上占有绝对优势。目前很多档案管理信息系统是基于微软的 Visual Stugio 平台开发的，但使用的版本高低不一。

（2）AMIS 本身的灵活性、可扩展性以及个性化定制能力。这主要取决于 AMIS 的设计思路和产品的实现方式，取决于 AMIS 是否容许用户按照自己的喜好和业务需要选择或修改界面、增加功能模块。一些单位研发的通用档案管理信息系统在这一点上考虑得比较周全，可以在一定程度上实现灵活可扩展的功能。

（3）实用、稳定和可靠是档案管理人员对档案管理信息系统最根本也是最基本的要求，同时也是 AMIS 必须保证的属性和特点。目前大多数市场化产品在这一点上的满足能力是比较好的，应该说目前的网络版软件基本上都可以满足档案馆用户的使用需求。

2.2 产品功能特点

AMIS 功能的比较主要从系统维护、系统定义、基础信息管理、档案业务管理和文档一体化等几个方面进行。

（1）系统维护功能。主要包括数据备份、数据恢复、数据装载、系统登录、系统帮助等一些支持系统运行的基本功能。目前大多数的 AMIS 都是依赖于所采用的数据库管理系统提供的功能来实现数据的备份、恢复、迁移、装载等功能，也有一些软件如 GE2000 在系统中提供了数据备份和恢复等功能。

（2）系统定义。主要包括系统框架、档案门类、档案数据库结构、用户模型、用户界面等功能的定义。清华通用档案管理信息系统、南大之星、飞狐灵通、广州邵林、GE2000 等软件产品可以在不同程度上支持系统的灵活定义；但一旦

 DOI: https://doi.org/10.36956/iser.v2i1.362

系统定义完成后，录入了数据，建议不要轻易修改系统的框架结构。这一点飞狐灵通和清华通用档案管理信息系统的功能比较强。

（3）基础信息管理。包括组织机构、实体分类、用户信息以及系统中使用的数据字典维护等功能，几乎所有的网络版软件系统都支持这一特定的应用模式，即通过对基础数据的一次录入，达到多次使用的效果，最重要的是保证了整个系统内部重要数据的一致性。

（4）档案业务管理功能。档案业务管理包括档案立卷、移交、审核、入库、库房管理、处理（如转出、转移、缩微处理、数字化处理等）、鉴定、盘点、销毁等全过程的业务管理功能，管理的内容既包括档案目录管理又包括全文信息管理，涉及的操作包括增加、修改、删除、查询、打印、统计等。而目前大多数产品在档案的库房管理功能模块上做得非常好，特别是在案卷级和文件级管理，以及封皮、脊背、目录打印等支持档案实物管理的功能上做得比较到位。而在支持档案业务全过程管理上，只有少数几个产品能够做到灵活配置，清华通用档案管理信息系统和飞狐灵通在这一点上领先于其他同类产品。

（5）文档一体化。文档一体化主要是指现行业务系统中流转文件的自动归档。但由于很多单位在进行信息化设计的过程中，特别是实施办公自动化较早的单位，没有将档案业务管理作为其中一个重要模块来实现。因此，才出现了档案行业的 AMISO 大多数 AMIS 基本上很难实现文件档案的一体化管理，但又必须将归档的电子文件纳入 AMIS 中进行管理。因此，普遍采用的一种方式是编写接口程序，而且需要针对不同的现行文件系统编写个性化的接口，这一点想做到通用比较难。除非像飞狐灵通和世纪科怡等公司将档案管理系统纳入办公自动化系统的全局中来考虑，才有可能在一定程度上实现文档一体化，但其前提条件是文件在办公业务中的管理思路与档案管理模式要一致，如文书档案、科技档案比较容易实现，而像高校中的学籍信息、财务信息、教务信息等以各种数据库格式存储的多元化形式的文件，很难实现归档前后的一体化管理。

（6）全文检索功能。在调研的十多种网络产品中，基本上都支持信息检索功能，但支撑的程度和实现的技术不太相同，有的是采用操作系统和数据库提供的功能来实现，有的是专门做检索引擎，有的采用了 OCR 技术实现了对规范图像文件（人工手写的扫描文件几乎无法识别）的全文检索。这些功能大大方便了用户的使用，但也提高了信息化的投入，因此各单位应根据资金实力和对检索能力的需求切合实际地进行购买。

（7）支持预警功能。通过系统给档案业务人员提供一定程度上的业务提示，如该动手立卷了，档案该入库了，档案保管期限到期了，档案该做密级鉴定了，借出的档案该归还了，以及实现一些对比统计等功能来提示档案管理人员，如库房的容量受到威胁，利用较高的档案应采取及时保护措施等，这些功能的开发有利于档案管理人员提高管理效率，开展精细化管理工作甚至支持辅助决策。目前已经有一些档案管理软件实现了支持预警的功能。

3 AMIS 产品运行架构和支持环境

稳定的网络环境和安全的基础设施是网络版 AMIS 的基本要求，由于 AMIS 的开发平台和运行架构不同将导致它所需要的支持环境也不尽相同。

（1）对服务器运行环境的支持。服务器硬件及其操作系统类型的选择和使用是根据 AMIS 的总体环境要求来决定的，如所采用的数据库管理系统以及服务器端软件系统的开发环境来决定。服务器类型的建立如文件服务器、数据库服务器、Web 服务器、邮件服务器等将根据整个系统的应用情况来进行部署，在资源紧张的情况下可以考虑一台机器拥有多个服务器的功能。

（2）对数据存储的要求，主要是考虑所采用的数据库管理系统、电子全文的存储以及备份存储介质的选择。前二者与 AMIS 的运行模式及对数据的存储要求有很大的关系，而数据备份介质及存储管理策略主要是依据各单位的执行情况进行综合考虑。

（3）客户端环境建立，客户端运行环境主要取决于 AMIS 采用的 C/S 或 B/S 运行模式来部署客户端的应用软件。如果采用 B/S 模式，则只需要在客户端安装浏览器就可以使用，不像采取 C/S 那样，必须安装客户端应用软件。

（4）对插件安装或者应用程序支持环境的安装要求。在使用过程中发现大多数档案管理信息系统能够支持多种类型的多媒体文件的管理，但如果在客户端浏览各种多媒体电子文件，需要安装相应的支持软件，如浏览后缀为 DOC，PDF，CAI，AVI，CAD 等文件的专用阅读器。

 DOI: https://doi.org/10.36956/iser.v2i1.362

4 AMIS 产品的安全保障措施

档案信息化系统建设过程中，安全体系也在不断得到完善和发展。AMIS 产品的安全保障措施就是系统安全体系的重要组成部分。

4.1 系统日志监控

系统日志监控能够辅助系统管理人员分析合法用户操作过程中存在的问题，主要用来记录什么时候、什么人采用哪台计算机做了什么样的操作，通过日志分析可以监控系统的使用状况，也可以在出现问题后及时查找原因。目前大多数系统记录的日志信息不是很全面，只能做到比较粗略的记录，为了支持更精细化的管理，有些产品在流程环节和操作功能等方面记录档案管理生命周期中的责任链相关信息，可以在更深程度上支持档案业务的规范化管理。

4.2 系统用户权限管理

根据不同的用户设置其对系统功能和数据的操作权限，大多数 AMIS 实现了对系统功能操作权限的控制，但并未细化到对系统数据操作权限的控制。

4.3 电子文件的安全管理

《电子签名法》的颁布实施，告诉档案管理人员必须做好接收电子档案的准备，必须准备和积累各类资源以面对电子档案归档过程中的安全管理和控制。目前大多数的 AMIS 在保障电子档案的安全、真实和完整等方面都采取了一定程度的措施，但在应对电子文件归档的安全措施上还没有下大功夫。有些软件产品在电子水印等方面正在做一些原型实验，也取得了初步的成效。

4.4 数据加密

大多数产品实现了对用户密码的加密，但像采用条码、磁卡、密钥等技术实现身份认证、采用生物识别技术对磁盘数据进行加密，以及实现对电子文件传输过程中的数据加密等措施使用得还非常少，甚至没有考虑数据加密的安全解决方案。这是目前 AMIS 产品最大的局限性。

5 AMIS 产品的分类

按系统运行模式可以将 amis 分为单机版和网络版，网络版又分为 C/S 和 B/S 两种运行模式。在调研过程中我们发现有的用户已经使用了网络版的档案管理信息系统，但仍然认为他录入的数据只归他自己一人使用，甚至认为数据存放在自己的客户机上；有的则以为机器能上网就是使用了网络版的软件系统等，存在一定程度的认识上的误区。究其原因，主要还是很多用户并不很了解单机版和网络版的根本区别。这里作简单说明。

一套单机版的软件只能在一台计算机上安装，而且它所采用的数据文件基本上都是文件级或桌面数据库，数据库本身不支持多用户的连接。如果一个单位有多个用户使用档案管理信息系统，则必须在多台机器上分别安装该软件系统及其数据库支持文件，而且这些用户录入的数据只能在本台机器上查看，在另外一台机器上的 AMIS 上无法查看到本机上录入的数据。另外单机版的数据集成起来形成资源共享是比较麻烦的，必须经过人工整合处理才能将多人录入的数据合并成一个大的资源库。而且在数据库合并的过程中也会由于各人录入数据格式甚至是定义的数据字典的不一致而难以处理，甚至无法处理。

正是为解决数据共享问题才出现了网络版的操作系统、网络版数据库管理系统以及网络版的档案管理信息系统。运行网络版 amis 的基本条件是服务器的操作系统及安装的数据库管理系统必须支持多用户操作（如 Unix，Linux，Windows2000 Server，Windows2003 Server 以及 SQL Server，Oracle），像安装 Windows98，Windows2000 Professional 以及 Windows XP 等操作系统的计算机不能作为 AMIS 的数据库服务器使用。

网络版的客户端也有一些基本配置要求，这主要取决于 AMIS 的运行结构，如果采用 Client/Server 模式，客户端必须安装应用程序才能运行，因此使用过程中整个应用系统维护的工作量比较大；而对于 Brow−ser/Server 运行模式的软件系统，则只需要多建一个 Web 服务器并安装 AMIS 的应用程序，客户端只需要安装浏览器就可以方便地进行操作，但这种方式的开发效率和应用效率相对较低，也有其多个方面的局限性。

网络版 AMIS 实际上是为多个业务部门建立了一个公共的网络平台和数据库环境，同时也为各个业务人员提供了一个协同工作的平台，因此要求大家按照约定的制度和标准进行规范化操作，要求使用该系统的所有用户不断提高自己的业务技能和技术知识，在考虑到本部门业务管理的同时，也应想到与其他业务部门之间的信息集成和资源共享的问题。

 DOI: https://doi.org/10.36956/iser.v2i1.362

目前市场上推广的各类档案管理信息系统产品按功能可分为以下五大类：

5.1 目录级档案管理

其主要特点是将档案的案卷目录和文件目录采用计算机方式管理起来，实现了档案目录信息的增加、修改、删除、查询、检索、统计、打印等基本功能。

这一类软件可以是单机版也可以是网络版，使用起来方便，易入门，用得好的单位能够通过该类软件的使用摆脱手工操作。这类软件的功能相对固定，有些可以实现灵活建库的功能，但很多单位在使用灵活建库的过程中，分类特别细，在检索时就出现了麻烦，虽然个别软件提供了跨库检索功能，但还是影响了系统的使用效率及业务人员的工作效率。

5.2 目录全文初级管理

其主要特点是不仅将档案目录信息管理起来，而且将档案目录对应的电子信息（如扫描的图像文件、移交的光盘等多媒体信息）一起对应起来并实现一体化管理，查询检索等功能主要是在档案目录级进行，有的可以在原文级实现简单的全文检索。

这类软件也有单机版和网络版（主要以 C/S 为主）两类，比较适合一些馆内存有电子信息的档案馆使用，以帮助理解全文检索的概念和初级使用，以及理解文件服务器的概念，为下一步选用更高级软件版本的用户奠定基础。

5.3 目录全文高级管理

这一类提供了基于文字识别、图像识别等技术的高级全文检索功能，对于目录管理、全文管理等一些基本功能实现得很好，一般都是网络版应用模式，既有 C/S 应用模式又有 B/S 应用模式，各用户可以根据本单位的情况建立文件服务器、Web 应用服务器、数据库服务器等，这一类软件的功能基本能够满足档案馆内部“目录 + 全文一体化”集成管理的需求。

5.4 集成化综合档案管理

前三类 AMIS 产品主要实现对库房档案信息的管理，而集成化综合档案管理这一类软件产品能够实现从档案的收集、整理、移交、入库、保管、档案处理（归档、转档、鉴定、开放、数字化等）到档案销毁全过程业务流程、档案目录和全文信息的综合管理，并能够实现多门类档案信息之间的跨库检索和统一一致的综合管理，即可以实现档案业务全过程的纵向集成管理和档案内部各部门之间信息的横向集成管理。

这一类软件提供的功能比较全，大多都包括从系统定义到业务流程的定制，甚至是个性化用户定制等功能，适合业务管理较为规范的档案馆使用。

5.5 集成平台级文档管理

集成平台级的文档管理不仅考虑到档案馆的业务，而且向外延伸到档案形成部门，主要功能是解决现行业务系统与档案管理的一体化集成问题，最终实现文档一体化管理。有些产品提供了办公自动化功能，并将该功能与档案管理业务相集成，有的则提供了集成接口功能，实现数据的迁移、转换、导入、导出等功能。

这一类软件将档案管理的业务向前延伸，旨在做到档案管理人员前端参与、全程监控的目的，但实施起来比较困难，因为该软件的应用不仅仅涉及档案部门，更重要的是要说服档案形成单位的工作人员在办公过程中采用该软件，而往往是归档单位已经采用了某一个办公自动化系统。因此对于这种情况，采用接口的方式进行数据迁移与转换是一种可操作的解决方案。

6 AMIS 产品的选型

实施档案信息化，产品选型非常关键。正确选择档案管理信息系统需要考虑以下三个主要问题。

6.1 档案馆信息化的应用需求和发展要求

选择档案管理信息系统的最终目的是要用起来，不仅当前能够用起来，而且要考虑业务扩展以后也能用起来，这一点是关键。因此，要求档案馆在选型过程中，不仅要对馆内所有的业务、管理、人员等的现状及存在的问题有一个充分的了解和认识，而且还需要结合全国档案事业及各档案馆的战略目标，考虑未来发展的需要。只有在充分认识到档案馆进一步发展的需要后，才能锁定需求，进行有效的选型。

6.2 信息技术和软件产品的现状与发展

涉足信息化，不了解信息技术、不熟悉软件产品是寸步难行的。信息技术的飞速发展推动了软件产品的更新换代，但也带来了“用跟不上变”的现实问题。因此，开展档案信息化建设，务实的同时，也必须经常关注和跟踪最新技术的发展，了解软件产品的运行特点和使用场合，才能在每一次

 DOI: https://doi.org/10.36956/iser.v2i1.362

面临产品选型时，作出客观的、切合实际的判断。

6.3 将产品与需求、技术与发展相结合，作出决策

在确定了档案馆的业务需求、认识了软件产品的使用要求之后，就需要将二者结合起来，综合平衡档案馆的人力、物力和财力，作出正确、合理的选择。

7 结语

软件和信息技术服务业是关系国民经济和社会发展全局的先导性产业，具有技术更新快、产品附加值高、资源消耗低等突出特点。论文查阅了行业相关数据，分析中国软件和信息技术行业目前的现状、未来的转变方式及发展机遇。在分析软件产业发展趋势的基础上提出了对软件产业发展的未来展望，认为目前 IT 领域硬件发展正逼近极限，而以移动智能终端操作系统为核心的产业生态体系的构建将成为未来竞争的焦点。

参考文献

[1] 郑柏杰 , 李志仁 . 档案管理信息系统 [J]. 信息技术 ,2000(03):17−18.

[2] 赵红梅 . 档案管理信息系统建设应注意的几个问题 [J]. 文学教育 : 中 ,2017(10):51−53.

[3] 曹玉林 , 武君胜 . 基于网络的档案管理信息系统的设计与研究 [J]. 计算机工程与设计 ,2009,30(006):1532−1535.

[4] 艾国生 , 王成义 . 网络化档案管理信息系统的运行模式 [J]. 兰台世界 ,2005:18−20.

 DOI: https://doi.org/10.36956/iser.v2i1.363

Research on Security System and Countermeasures of Mobile Communication System

Yuning Zhou

Huazhong University of Science and Technology, Wuhan, Hubei, 430074, China

Abstract

The conceptual security architecture framework (OSI/RM) proposed in the Open System Interconnection Reference Model defines five groups of security services: authentication services, confidentiality services, data integrity services, access control services, and non-repudiation services. The information security architecture based on the seven-layer protocol of the OSI reference model is a three-dimensional matrix composed of security attributes, OSI protocol layers and system components. It has important guiding significance for the information security architecture of the specific network environment. According to the characteristics of the mobile communication system, the paper gives the three-dimensional framework structure of the mobile communication system security system with reference to the 3G security domain structure and the OSI security system structure.

Keywords

mobile communication system; network security; system; countermeasures

移动通信系统的安全体系及对策研究

周宇宁

华中科技大学，中国 · 湖北 武汉 430074

摘　要

开放系统互联参考模型中提出的概念性安全体系结构框架（OSI/RM）定义了 5 组安全服务：认证服务、保密服务、数据完整性服务、访问控制服务、抗抵赖服务。基于 OSI 参考模型的七层协议之上的信息安全体系结构由安全属性、OSI 协议层和系统部件组成的三维矩阵，它对具体网络环境的信息安全体系结构有重要的指导意义。论文根据移动通信系统的特点，参考 3G 安全域结构和 OSI 的安全体系结构给出了移动通信系统安全体系的三维框架结构。

关键词

移动通信系统；网络安全；体系；对策

1 引言

随着电子信息技术的发展，各种网路技术不断融入到移动通信系统中，3G 移动通信系统得到广泛的应用，移动通信的用户也是越来越多，移动通信系统的网络安全问题已经受到人们的关注和重视，研究移动通信系统的网络安全问题对于提升通信安全具有十分重要的作用和意义。

2 移动通信系统的安全体系概述

安全服务轴（S）包括认证（鉴权）、访问控制、数据完整性、数据保密性和不可否认 5 个元素，各元素之间的关系是层次关系。安全需求轴（N）参照接口协议的分层和 OSI 参考模型的分层模型，包括物理层安全、链路层安全、控制层安全、用户层安全和管理层安全。安全域轴（F）由不同的安全域组成，安全域的划分由具体的安全策略确定。整个 TETRA 系统的安全域可以初步划分为网络接入域、网络域和用户域。

系统的任何一个安全措施都可以映射成这个三维空间的一个点，可以解释为每个安全措施都是在某个安全域内，为满足某个层次上的安全需求而提供的某种安全服务。

下面从安全服务、安全需求以及安全域三个方面详细讨论移动通信安全体系所涉及的要素和逻辑关系以及相关的安全技术。

3 安全服务

移动通信安全体系的安全服务包括认证和密钥管理服务、访问控制服务、数据完整性服务、数据保密性服务以及

 DOI: https://doi.org/10.36956/iser.v2i1.363

不可否认性服务等方面。各种安全服务之间存在相互依赖的关系，单独采用其中的一种安全服务无法满足移动通信系统的安全需求。这些安全服务之间的关系可以看成是一种层次关系。

其中实体 1 或实体 2 可以根据不同的安全域代表移动通信系统中不同的构件。例如，在用户域内可能分别代表安全模块和移动终端 . 在接入域内代表移动终端和网络基础设施，在网络域内则可以代表两个交换机或交换机和基站。所有的移动通信系统的安全服务都依赖主体与客体的身份标识和认证，主要实现的技术有系统和移动终端之间的鉴权协议、公钥基础设施和智能卡技术等 ; 访问控制是整个安全系统的核心，其目标是防止对任何资源进行非授权的访问，它对数据保密性和完整性所起的作用是十分明显的；数据的完整性和保密性确保数据在流通中不被篡改和窃取，它们是认证和访问控制有效性的重要保证，可以采用的技术包括空中接口加密和端到端加密等；不可否认服务是数字集群通信系统一个必不可少的安全服务，一般采用合法的监听来防止用户否认自己的通话。具体讨论如下。

3.1 认证服务和密钥管理

对一个实体进行鉴权就是接收到该实体的标识后证明该标识是真实的。在移动通信系统的接入域中，根据实际需要，鉴权可以是双向的，也可以是单向的。一般在移动终端接入网络或一次通话开始时需要鉴权，由系统的安全策略来决定鉴权的频度。密钥管理是产生、分发、选择、删除和管理在鉴权和加 / 解密的过程中使用的密钥的过程。没有发送和接收密钥的双方的双向鉴权就无法安全分发密钥。因此密钥管理和鉴权的关系非常紧密。

移动通信系统中的认证服务包括用户和网络之间签权、网络实体之间的认证以及在终端内安全服务模块和终端的认证等。密钥管理包括空中接口鉴权密钥的密钥管理、空中接口机密性和完整性服务的密钥管理、端到端保密通信的密钥管理等部分。

3.2 访问控制

访问控制的目标是防止对任何资源（这里主要是通信资源和信息资源）进行非授权访问。非授权访问包括未经授权的使用、泄露、修改、销毁以及颁发指令等。访问控制直接支持数据保密性、数据完整性、数据可用性以及合法使用的安全目标。在移动通信系统中访问控制的需求广泛存在，例如，为了保护系统基础设施，网络运营商需要：

防止对无线资源的非授权使用；

防止对服务的非授权使用；

对数据库需要进行访问控制；

对配置和网络管理需要进行访问控制；

终端的使能 / 禁用。

3.3 完整性服务

数据完整性是指接收方接收到的数据和发送方发送的数据保持一致。数据源鉴别用来检查数据源标识的真实性和发送该级别数据的资格。显然，只有在进行通信的双方进行鉴权后，数据完整性和数据源鉴别服务才有用。鉴权过程可用来提供安全参数和所需的密钥。

移动通信系统中的完整性服务主要是指信令数据的完整和数据源的鉴别功能，该服务可以确保和检查终端与核心网络之间的控制信息的完整性，并提供检查信息源的方法。

3.4 数据保密性服务

移动通信系统保密性服务的目的是保护敏感数据，防止存储在系统内和传输过程中的敏感数据被某个无权得到该数据的用户、实体或过程故意或偶然获得。一般采用加 / 解密来实现保密性服务。保密性服务需要和其他安全服务共同配合才能达到保护敏感数据的目的。例如，采用访问控制机制来防止对存储的数据和用来进行加解密的过程的非授权访问，在终端进行通信前需要进行鉴权，一般鉴权协议执行过程会产生进行空中接口加密的会话密钥。

移动通信系统的保密性服务不仅包括移动终端和核心网络之间（即空中接口）的语音、信令和数据保密，还包括端到端的语音和数据保密通信，以及用户标识和组标识的保密性服务等。其中用户标识的保密性服务是指，保证移动通信的个人用户标识或个人用户短标识不被非授权的个人、实体和过程获得 ; 组标识的保密性服务特指在集群移动通信系统中，组用户标识不被非授权的个人、实体和过程获得，而且保证从个人用户标识无法得到组用户标识，反之亦然，当然，组标识的保密可以通过部分信令的保密性服务来实现。

3.5 不可否认性服务

不可否认性服务的主要目的是保护通信用户免遭来自系统其他合法用户的威胁，而不是来自未知攻击者的威胁。具

 DOI: https://doi.org/10.36956/iser.v2i1.363

体是指，防止参与某次通信交换的一方事后否认曾经发生过本次交换。

在专有网络中经常采用合法的监听来防止用户否认自己的通话。一般某个组织管理者需要监听其组织内部的流量和通信，调度台用户需要监听其所管理的各个组的流量和通信，某个授权用户需要监听他所在的组或其他组的流量和通信情况。在某种程度上监听与机密性等安全服务有些对立，这需要系统的规划者、管理者和使用者合理设计、实施和使用这些安全服务。

4 安全需求

移动通信系统安全体系结构的 N 轴从下到上分别对应物理层、链路层、控制层、用户层和管理层。

相应的安全需求定义如下：

4.1 管理层

管理层位于安全需求的最上层，包括对安全威胁的管理和制定合理的管理标准。管理层对所有信息的安全负责，确定移动通信系统与其他系统连接时可能会暴露的漏洞，确定被保护的资源和使用的安全技术。

4.2 用户层

用户层安全提供事务处理的端到端安全。如果安全业务是应用层特有的，或者需要经过应用中继，则其安全性需要在本层上进行设置。移动通信系统中的端到端保密通信需求一般处在这个层面上。如果对通话内容进行端到端的保护，只有通信的端用户知道所用的密钥，则尽管信息经过了基站、交换机等中继系统，但因为这些中继系统对所用的密钥一无所知，因此也无法了解通信的内容。在其他基于用户层的应用中，如数据检索等需要保护特定服务的信息和处理，可能的安全服务包括验证、加密、数字签名、日志以及恢复机制等。有些安全服务，如不可抵赖只能在用户层实现。

4.3 控制层

负责网络过程。其中鉴权和用户管理等安全服务需要在该层的子网络接入功能中实现。

4.4 链路层

链路层主要保证数据在无线电线路上传输的正确性和安全性，一般采用 TDMA 帧同步、交织 / 去交织、信道编码、差错保护、空中接口加密等技术来实现。

4.5 物理层

移动通信系统的物理层由定时结构、无线电射频发射和接收等部分组成，其安全主要是防止物理通路的损坏、对物理通路的窃听和攻击干扰等。防止机房、电源、监控等场地设施和 UPS 周围环境的破坏，同时应具备对系统关键设备的备份手段。

5 安全域

5.1 网络接入域安全

网络接入域安全主要提供安全接入服务，包括用户身份保密性、用户认证、在网络接入信道和设备间传输数据的保密性和完整性、移动设备的鉴定。主要是通过临时身份号码来保证用户身份号码的保密性；采用基于对称密钥算法的双向认证协议来进行用户接入的认证和加密密钥与完整性密钥的协商。利用国际移动设备号来鉴别移动设备。

5.2 网络域安全

主要提供网络实体间（如交换机和基站之间，交换机和交换机之间）的认证、数据传输保密性和完整性、攻击信息的监视等安全机制。

5.3 用户域安全

主要提供终端安全服务模块（可能是终端内的模块或智能卡）与用户间的认证以及终端安全服务模块与移动终端间的认证。用户与终端安全服务模块间认证通常采用 PIN（个人识别码），而终端安全服务模块与移动终端间的认证通常采用共享秘密信息的方法。

6 移动通信系统的网络安全策略研究

6.1 移动通信系统的数据完整性研究

在执行密匙协商的过程中能够实现移动通信系统用户数据完整性的密匙协商，在用户和网络之间的安全模式协商机制能够实现完整性算法协商，而移动通信系统中的网络和 MS 之间的多数指令信息都需要提供完整性保护，在 3G 移动通信系统中为了确保用户和网络之间的信息指令不会被篡改，可以通过消息认证的方式来实现。

首先需要数据信息发送方将需要传递的数据信息使用完整性密匙将 F9 算法产生的消息认证码 MAC 附在发出数据信

 DOI: https://doi.org/10.36956/iser.v2i1.363

息的后面，数据信息接收方只需要将接收到的信息使用同样的方法得到 XMAC，然后将 XMAC 和 MAC 进行比较，如果两者相同，则表示数据信息的完整性，反之数据信息不完整。3G 移动通信系统数据信息的完整性主要表现在完整性算法协商、数据和指令的完整性以及完整性密匙协商三个方面。

6.2 移动通信系统的用户身份保密性研究

用户身份保密性主要涉及到以下几个主要方面。（1）用户身份的机密性，确保移动通信系统的用户的真实身份不会在无线链路中被盗用和窃听；（2）用户所处位置的机密性，确保所有移动通信系统的用户的即时位置在无线接入链路中使用窃听等手段来确定；（3）用户信息的不可追溯性，确保入侵移动通信系统的人无法通过无线接入链路得出用户的信息。移动通信系统为了确保用户身份的机密性，往往是通过设置常用的临时身份来识别用户身份，对于用户信息的可追溯性问题，系统可以应用不同的临时身份来识别和判断某一位用户的方法来解决，此外对于可能泄露用户身份的所有数据信息在无线接入链路上都应该采取加密措施，来提升信息传输和接受的安全性。

6.3 移动通信系统的认证系统

为了避免移动通信系统受到伪基站的攻击，提升移动通信系统的通信安全，可以采用双向认证方式，对 MS 和基站以及基站和 MS 进行认证，移动通信系统应该保证用户和网络之间建立的每一个连接的假设实体认证机制都能够发挥作用。双向认证鉴权向量的 5 个参数分别为期望相应、RAND、加密密匙、鉴权令牌和完整性密匙，其中完整性密匙能够对无线接入链路的数据的完整性提供有效保护，无疑增强了移动通信系统用户对网络测合法性的鉴权，大大确保网络安全。

6.4 移动通信系统数据保密性研究

3G 移动通信系统在密匙长度加长的同时，引入加密算法协商机制，提供基于端到端的全网加密方式，采用以交换设备为主的安全机制来确保数据信息在网络中的传输安全。3G 移动通信系统中的网络接入部分数据保密有加密密匙协商机制、机密算法协商机制、信息质量数据加密机制和用户数据加密机制四个方面。

7 结语

移动通信系统有确保自身信息传输和终端接入网络以及用户信息传递和接入网络的安全性，如何解决这些网络安全问题是影响移动通信系统发展的关键所在。

参考文献

[1] 谢磊 . 移动通信系统的网络安全问题研究 [J]. 信息通信 ,2013 (010):208.

[2] 张绍林 . 对移动通信系统中常见安全问题的思考 [J]. 中国新通信 ,2014 (011):56+57.

[3] 朱里奇 . 第三代移动通信系统 (3G) 安全性研究 [D]. 武汉 : 华中科技大学 ,2004.

[4] 黎杰文 . 超宽带无线通信系统中同步若干关键技术的研究 [D]. 重庆 : 重庆邮电大学 ,2008.

[5] 钱芳 . 移动通信系统的安全性研究 [J]. 计算机安全 ,2012 (004):25−28.

[6] 张振波 .4G 无线网络安全若干关键技术研究 [J]. 科技创业家 ,2014(05):7.

[7] 刘忠明 . 基于 3G 移动通信系统的安全问题研究 [J]. 信息与电脑 : 理论版 ,2013(006):67−68.

[8] 高建辉 , 祁建华 .3G 移动通信中的安全问题研究 [J]. 内江科技 ,2010(12):132−133.

[9] 范明钰 . 第三代移动通信系统的安全体系 [J]. 信息安全与通信保密 ,2000(03):1−4.

[10] 邓所云 , 胡正名 , 钮心忻 , 等 . 移动通信中的双向认证与密钥协商新协议 [J]. 北京邮电大学学报 ,2002,25(2):54−56.

[11] 安华萍 , 贾宗璞 .3G 移动网络的安全问题 [J]. 科学技术与工程 ,2005,5(6):375−378.

[12] 3G 移动通信系统的安全体系与防范策略 . 信息安全与通信保密 [J],2009(8):22−23.

 DOI: https://doi.org/10.36956/iser.v2i1.364

Exploring the Network Security Strategy of Archives Information

Haibo Liu

Hebei University of Technology, Tianjin, 300401, China

Abstract

Network security of archival information means that the hardware, software and data in the network system are protected from damage, change and leakage due to accidental or malicious reasons, the system runs continuously and reliably, and the network service is not interrupted. File information network security is the core content and key of file information security, and also the precondition of file information construction. It includes the operation security of archival information network and the information security of archival information network. Through various computer, network, password technology and information security technology (access control, communication encryption, identification and identification, anti-virus, etc.), the confidentiality, integrity and authenticity of information transmitted, exchanged and stored in the private network and public communication network of archival information are protected, and the transmission and content of archival information are controlled.

Keywords

security management strategy; archive work; information network; network technology

探究档案信息网络安全策略

刘海波

河北工业大学，中国 · 天津 300401

摘　要

档案信息网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。档案信息网络安全是档案信息安全的核心内容和关键，也是档案信息化建设的前提条件。它包括档案信息网络运行安全和档案信息网络上的信息安全。通过各种计算机、网络、密码技术和信息安全技术（访问控制、通信加密、识别和鉴别、防病毒等），保护在档案信息专用网络及公用通信网络中传输、交换和存储信息的机密性、完整性和真实性，并对档案信息的传播及内容具有控制能力。

关键词

安全管理策略；档案工作；信息网络；网络技术

1 访问控制技术

访问控制是网络安全防范和保护的主要策略，它的主要任务是保证网络资源不被非法使用和非常访问。它也是维护网络系统安全、保护网络资源的重要手段。各种安全策略必须相互配合才能真正起到保护作用，但访问控制可以说是保证网络安全最重要的核心策略之一。

1.1 入网访问控制

入网访问控制为网络访问提供了第一层访问控制。它控制哪些用户能够登录到服务器并获取网络资源，控制准许用户入网的时间和准许他们在哪台工作站入网。

用户的入网访问控制可分为 3 个步骤：用户名的识别与验证、用户口令的识别与验证、用户账号的缺省限制检查。三道关卡中只要任何一关未过，该用户便不能进入该网络。

对网络用户的用户名和口令进行验证是防止非法访问的第一道防线。用户注册时首先输入用户名和口令，服务器将验证所输入的用户名是否合法。如果验证合法，才继续验证用户输入的口令，否则，用户将被拒于网络之外。用户的口令是用户入网的关键所在。为保证口令的安全性，用户口令不能显示在显示屏上，口令长度应不少于 6 个字符，口令字符最好是数字、字母和其他字符的混合，用户口令必须经过加密。加密的方法很多，其中最常见的方法有：基于单向函数的口令加密，基于测试模式的口令加密，基于公钥加密方案的口令加密，基于平方剩余的口令加密，基于多项式共享

 DOI: https://doi.org/10.36956/iser.v2i1.364

的口令加密，基于数字签名方案的口令加密等。经过上述方法加密的口令，即使是系统管理员也难以得到它。用户还可采用一次性用户口令，也可用便携式验证器（如智能卡）来验证用户的身份。

网络管理员应该可以控制和限制普通用户的账号使用、访问网络的时间、方式。用户名或用户账号是所有计算机系统中最基本的安全形势。用户账号应只有系统管理员才能建立。用户口令应是每用户访问网络所必须提交的“证件”。用户可以修改自己的口令，但系统管理员应该可以控制口令的以下几个方面的限制：最小口令长度、强制修改口令的时间间隔、口令的唯一性、口令过期失效后允许入网的宽限次数。

用户名和口令验证有效之后，再进一步履行用户账号的缺省限制检查。网络应能控制用户登录入网的站点，限制用户入网的时间，限制用户入网的工作站数量。当用户对交费网络的访问“资费”用尽时，网络还应能对用户的账号加以限制，用户此时应无法进入网络访问网络资源。网络应对所有用户的访问进行审计。如果多次输入口令不正确，则认为是非法用户的入侵，应给出报警信息。

1.2 网络的权限控制

网络的权限控制是针对网络非法操作所提出的一种安全保护措施。用户和用户组被赋予一定的权限。档案信息网络控制用户和用户组可以访问哪些目录、子目参、文件和其他资源。可以指定用户对这些文件、目录、设备能够执行哪些操作。受托者指派和继承权限屏蔽（IRM）可作为其两种实现方式。受托者指派控制用户和用户组如何使用网络服务器的目录、文件和设备。继承权限屏蔽相当于一个过滤器，可以限制子目录从父目录那里继承哪些权限。我们可以根据访问权限将用户分为以下几类：①特殊用户（即系统管理员）；②一般用户，系统管理员根据他们的实际需要为他们分配操作权限；③审计用户，负责网络的安全控制与资源使用情况的审计。用户对档案信息网络资源的访问权限可以用一个访问控制表来描述。

1.3 目录级安全控制

网络应允许控制用户对目录、文件、设备的访问。用户在目录一级指定的权限对所有文件和子目录有效，用户还可进一步指定对目录下的子目录和文件的权限。对目录和文件的访问权限一般有 8 种：系统管理员权限（Supervisor）、读权限（Read）、写权限（Write）、创建权限（Create）、删除权限（Erase）、修改权限（Modify）、文件查找权限（File Scan）、存取控制权限（Access Control）。用户对文件或目标的有效权限取决于以下几个因素：用户的受托者指派、用户所在组的受托者指派、继承权限屏蔽取消的用户权限。一个网络系统管理员应当为用户指定适当的访问权限，这些访问权限控制着用户对服务器的访问。8 种访问权限的有效组合可以让用户有效地完成工作，同时又能有效地控制用户对服务器资源的访问，从而加强了网络和服务器的安全性。

1.4 属性安全控制

当用文件、目录和网络设备时，网络系统管理员应给文件、目录等指定访问属性。属性安全控制可以将给定的属性与网络服务器的文件、目录和网络设备联系起来。属性安全在权限安全的基础上提供更进一步的安全性。网络上的资源都应预先标出一组安全属性。用户对网络资源的访问权限对应一张访问控制表，用以表明用户对网络资源的访问能力。属性设置可以覆盖已经指定的任何受托者指派和有效权限。属性往往能控制以下几个方面的权限：向某个文件写数据、拷贝一个文件、删除目录或文件、查看目录和文件、执行文件、隐含文件、共享、系统属性等。网络的属性可以保护重要的目录和文件，防止用户对目录和文件的误删除、执行修改、显示等。

1.5 网络服务器安全控制

网络允许在服务器控制台上执行一系列操作。用户使用控制台可以装载和卸载模块，可以安装和删除软件等。网络服务器的安全控制包括可以设置口令锁定服务器控制台，以防止非法用户修改、删除重要信息或破坏数据；可以设定服务器登录时间限制、非法访问者检测和关闭的时间间隔。

1.6 网络监测和锁定控制

网络管理员应对网络实施监控，服务器应记录用户对网络资源的访问，对非法的网络访问，服务器应以图形或文字或声音等形式报警，以引起网络管理员的注意。如果不法之徒试图进入网络，网络服务器应会自动记录企图尝试进入网络的次数，如果非法访问的次数达到设定数值，那么该账户将被自动锁定。

1.7 网络端口和节点的安全控制

网络中服务器的端口往往使用自动回呼设备、静默调制

 DOI: https://doi.org/10.36956/iser.v2i1.364

解调器加以保护，并以加密的形式来识别节点的身份。自动回呼设备用于防止假冒合法用户，静默调制解调器用以防范黑客的自动拨号程序对计算机进行攻击。网络还常对服务器端和用户端采取控制，用户必须携带证实身份的验证器（如智能卡、磁卡、安全密码发生器）。在对用户的身份进行验证之后，才允许用户进入用户端。然后，用户端和服务器端再进行相互验证。

2 识别和鉴别

档案网络安全系统要具备识别和鉴别机制以面对网络上的各种攻击。识别就是分配给每个用户一个 ID 来代表用户和进程。鉴别是根据用户的私有信息来确定用户的真实性，防止欺骗。口令机制是最常用的鉴别方法。随着生物技术的发展，利用指纹、视网膜等可提高鉴别的强度。经常使用的还有数字签名等方法。

2.1 口令机制

口令是相互约定的代码，假定只有用户和系统知道。口令有时由用户选择，有时由系统分配。通常情况下，用户先输入某种标识信息，比如用户名或 ID 号，然后系统询问用户口令，绕口令与用户文件约定相匹配，用户即可进入访问。

作为安全防护措施，口令也有可能被攻破。攻击口令的方法主要有强力攻击，猜测一切可能的口令代码；猜测可能性较大的口令；窃取、分析系统通行字表；伪装成系统来询问用户可不可以。

对抗口令攻击通常采用加密、签名和令牌等办法。但最重要的是进行口令管理，包括选择、分发和更改等。

2.2 数字签名

在电子政务运行过程中，一个重要内容就是辨认发送者和接收者的身份并进行记录，以保证信息的真实性和不可抵赖性。

数字签名机制提供了一种鉴别方法，以解决伪造、抵赖、冒充和篡改等问题。数字签名采用一定的数据交换形式，使得双方能够满足两个条件：一是接受方能够鉴别发送方所宣称的身份；二是发送方以后不能否认它发送过数据这一事实。

在书面文件上签名是确认文件的一种手段，其作用：一是自己的签名难以否认，能够确认文件已签署的事实；二是签名不易仿冒，能够确认文件为真的事实。数字签名与书面文件签名有相同之处，采用数字签名，也能确认信息由签名者发送、信息自签发后到收到为止未被做过修改。

这样，数字签名就可以用来防止电子信息因易被修改而有人作伪，或假冒他人名义发送信息，或发出（收到）信件后又加以否认等情况发生。数字签名采用双重加密的方法来实现防伪、防抵赖，常见的数字签名主要有 3 种：RSA 算法、Rabin 算法和 DDS 算法。

2.3 数字水印

为了防止图像文件盗用，采用数字水印技术，将作者信息嵌入到图像中。数字水印的特点是即使数据的格式发生了变化，版权信息也不会丢失。例如，加入了数字水印的 JPEG 格式图像，将其转换为 BMP 格式后，数字水印的信息仍然不会丢失。这是因为版权信息并不是附加在原数据上的，而是嵌入到了原数据的当中。而且包含数字水印的数据看起来跟普通的数据完全一样，不影响图像的显示。

2.4 电子印章

对于一些须分发的文件，有时需要加盖印章，可采用自主产权的方法实现不可盗用的电子印章。印章图像的原稿事先保存到数据库中。当用印人在使用此印章时，先将须盖章的文件的检查和用印人信息、印章图像原稿制稿人信息作为水印加入印章图像原稿生成用印稿，然后将用印稿加到须盖章的文件中。使用文件时，将检查原稿制稿人、用印人信息以及文件的检查。这样，其他人即使采用图像编辑软件将印章图像取出，用在其他文件中，也无法通过印章鉴别系统的检查。

2.5 生物识别技术

生物识别技术是依靠人体的身体特征来进行身份验证的一种解决方案，由于人体特征具有不可复制的特性，这一技术的安全系统较传统意义上的身份验证机制有很大的提高。人体的生物特征包括指纹、声音、面孔、视网膜、掌纹、骨架等，而其中指纹凭借其无可比拟的唯一性、稳定性、再生性备受关注。

20 世纪 60 年代，计算机可以有效地处理图形，人们开始着手研究用计算机来处理指纹，自动指纹识别系统 AFIS 由此发展开来。AFIS 是当今数字生活中一套成功的身份鉴别系统，也是未来生物识别技术的主流之一，它通过外设来获取指纹的数字图像并存贮在计算机系统中，再运用先进的滤波、

 DOI: https://doi.org/10.36956/iser.v2i1.364

图像二值化、细化手段对数字图像提取特征，最后使用复杂的匹配算法对指纹特征进行匹配。时下，有关指纹自动识别的研究已进入了成熟的阶段。随着指纹识别产品的不断开发和生产，未来该项技术的应用将进入民用市场，服务大众。

除了指纹识别技术外，近年来视网膜识别技术和签名识别技术的研究也取得了骄人的成绩。视网膜识别技术分为两个不同的领域：虹膜识别技术和角膜识别技术。虹膜识别系统使用一台摄像机来捕捉样本，而角膜扫描的进行则是用低密度的红外线去捕捉角膜的独特特征。由于该项技术具有高度的准确性，它将被应用在未来军事安全机构和其他保密机关中。签名识别，也被称为签名力学识别（DSV：Danamic Signatuer Verification），它是建立在签名时的力度上的，分析笔的移动，例如加速度、压力、方向以及笔画的长度，而非签名的图像本身。签名力学的关键在于分出不同的签名部分，有些是习惯性的，而另一些在每次签名时都不同，DSV 系统能被控制在某种方式上去接收变量，此项技术预计在今后 10 年中会得到进一步发展和应用。

3 防火墙技术

防火墙是一种保护计算机网络安全的技术性措施，它是一个用以阻止网络中的黑客访问某个机构网络的屏障，也可称之为控制进 / 出两个方向通信的门槛。在网络边界上通过建立起来的相应网络通信监控系统来隔离内部和外部网络，以阻挡外部网络的侵入。目前的防火墙主要有以下 3 种类型：

3.1 包过滤防火墙

包过滤防火墙设置在网络层，可以在路由器上实现包过滤。首先应建立一定数量的信息过滤表，信息过滤表是以其收到的数据包头信息为基础而建成的。信息包头含有数据包源 IP 地址、目的 IP 地址、传输协议类型（TCP、UDP、ICMP 等）、协议源端口号、协议目的端口号、连接请求方向、ICMP 报文类型等。当一个数据包满足过滤表中的规则时，则允许数据包通过，否则禁止通过。这种防火墙可以用于禁止外部不合法用户对内部的访问，也可以用来禁止访问某些服务类型。但包过滤技术不能识别有危险的信息包，无法实施对应用级协议的处理，也无法处理 UDP、RPC 或动态的协议。

3.2 代理防火墙

代理防火墙又称应用层网关级防火墙，它由代理服务器和过滤路由器组成，是目前较流行的一种防火墙。它将过滤路由器和软件代理技术结合在一起。过滤路由器负责网络互联，并对数据进行严格选择，然后将筛选过的数据传送给代理服务器。代理服务器起到外部网络申请访问内部网络的中间转接作用，其功能类似于一个数据转发器，它主要控制哪些用户能访问哪些服务类型。当外部网络向内部网络申请某种网络服务时，代理服务器接受申请，然后它根据其服务类型、服务内容、被服务的对象、服务者申请的时间、申请者的域名范围等来决定是否接受此项服务，如果接受，它就向内部网络转发这项请求 o 代理防火墙无法快速支持一些新出现的业务（如多媒体）。现在较为流行的代理服务器软件是 ingate 和 Proxy Server。

3.3 双穴主机防火墙

该防火墙是用主机来执行安全控制功能。一台双穴主机配有多个网卡，分别连接不同的网络。双穴主机从一个网络收集数据，并且有选择地把它发送到另一个网络上。网络服务由双穴主机上的服务代理来提供。内部网和外部网的用户可通过双穴主机的共享数据区传递数据，从而保护了内部网络不被非法访问。

4 加密技术

信息加密的目的是保护网内的数据、文件、口令和控制信息，保护网上传输的数据。网络加密常用的方法有链路加密、端点加密和节点加密三种。链路加密的目的是保护网络节点之间的链路信息安全；端点加密的目的是对源端用户到目的端用户的数据提供保护；节点加密的目的是对源节点到目的节点之间的传输链路提供保护。用户可根据网络情况酌情选择上述加密方式。

信息加密过程是由形形色色的加密算法来具体实施的，它以很小的代价提供很大的安全保护。在多数情况下，信息加密是保证信息机密性的唯一方法。据不完全统计，到目前为止，已经公开发表的各种加密算法多达数百种。如果按照收发双方密钥是否相同来分类，可以将这些加密算法分为常规密码算法和公钥密码算法。

在常规密码中，收信方和发信方使用相同的密钥，即加密密钥和解密密钥是相同或等价的。比较著名的常规密码算法有：美国的 DES 及其各种变形，比如 Triple、DES、

 DOI: https://doi.org/10.36956/iser.v2i1.364

GDES、New DES 和 DES 的前身 Lucifer；欧洲的 IDEA；日本的 FEAL−N、LOKI−91、Skipjack，RC4、RC5 以及以代换密码和转轮密码为代表的古典密码等。在众多的常规密码中影响最大的是 DES 密码。常规密码的优点是有很强的保密强度，且经受住时间的检验和攻击，但其密钥必须通过安全的途径传送。因此，其密钥管理成为系统安全的重要因素。

在公钥密码中，收信方和发信方使用的密钥互不相同，而且几乎不可能从加密密钥推导出解密密钥。比较著名的公钥密码算法有：RSA、背包密码 AMcEliece 密码、diff−Hellman、Rabin、Ong−Fiat−Shamir、零知识证明的算法、椭圆曲线、EIGamal 算法等等。最有影响的公钥密码算法是 RSA，它能抵抗到目前为止已知的所有密码攻击。

PKI（Public Key Infrastructure，公开密钥基础设施）是一种遵循既定标准的密钥管理平台，它可以为各种网络应用透明地提供采用加密和数字签名等密码服务所必需的密钥和证书管理，从而达到保证网上传递信息的安全、真实、完整和不可抵赖的目的。PKI 可以提供会话保密、认证、完整性、访问控制、源不可否认、目的不可否认、安全通信、密钥恢复和安全时间等 9 项信息安全所需要的服务。在这个结构中，公开密钥密码算法居于中心地位，称其为 PKI0 利用 PKI，人们可以方便地建立和维护一个可信的网络计算环境，无须直接见面就能够确认彼此的身份，安全地进行信息交换。

完整的 PKI 系统有权威认证机构（CA）、数字证书库、密钥备份及恢复系统、证书撤销系统、应用接口（API）等基本构成部分。

CA 是 PKI 的核心，主要职责是颁发证书、验证用户身份的真实性。一般情况下，证书必须由一个可信任的第三方权威机构——CA 认证中心实施数字签名以后才能发布。而获得证书的用户通过对 CA 的签名进行验证，从而确定了公钥的有效性。

数字证书库是证书集中存储的地方，用户可以从此处获得其他用户可用的证书和公钥信息。数字证书库一般是基于 LDAP 或是基于 X.500 系列的，也可以基于其他平台。

密钥可能会由于一些原因而使密钥的所有者无法访问。密钥的丢失将导致那些被密钥加过密的数据无法恢复。为避免这种情况的出现，就需要 PKI 提供密钥备份与恢复的机制。

CA 签发证书来把用户的身份和密钥绑定在一起。那么，当用户的身份改变或密钥遭到破坏时，就必须存在一种机制来撤销这种认可。

一个完整的 PKI 必须提供良好的应用接口系统，以便各种应用都能够以安全、一致、可信的方式与 PKI 交互，确保所建立起来的网络环境的可信性，降低管理和维护的成本。

公钥密码的优点是可以适应网络的开放性要求，且密钥管理问题也较为简单，尤其可方便地实现数字签名和验证，但其算法复杂，加密数据的速率较低。尽管如此，随着现代电子技术和密码技术的发展，公钥密码算法将是一种很有前途的网络安全加密体制。

在实际应用中，人们通常将常规密码和公钥密码结合在一起使用，如利用 DES 或者 IDEA 来加密信息，而采用 RSA 来传递会话密钥。如果按照每次加密所处理的比特来分类，可以将加密算法分为序列密码和分组密码。前者每次只加密一个比特而后者则先将信息序列分组，每次处理一个组。

5 病毒防护技术

在网络环境下，计算机病毒有不可估量的威胁性和破坏力。档案信息网络系统中使用的操作系统一般均为 Windows 系统，比较容易感染病毒。因此计算机病毒的防范也是档案信息网络安全建设中应该考虑的重要环节之一。反病毒技术包括预防病毒、检测病毒和杀毒三种技术。

5.1 预防病毒技术

预防病毒技术通过自身常驻系统内存，优先获得系统的控制权，监视和判断系统中是否有病毒存在，进而阻止计算机病毒进入计算机系统和对系统进行破坏。这类技术有：加密可执行程序、引导区保护、系统监控与读写控制（如防病毒卡等）。

5.2 检测病毒技术

检测病毒技术是通过对计算机病毒特征（如自身校验、关键字、文件长度的变化等）进行分析，以确定病毒类型的技术。

5.3 杀毒技术

杀毒技术通过对计算机病毒代码分析，开发出具有删除病毒程序并恢复原文件的软件。反病毒技术的具体实现方法，包括对网络中服务器及工作站中的文件及电子邮件等进行频繁地扫描和检测。一旦发现与病毒代码库中相匹配的病毒代码，反病毒程序会采取相应处理措施，防止病毒进入网络进

 DOI: https://doi.org/10.36956/iser.v2i1.364

行传播扩散。

档案信息安全防范是通过安全技术、安全产品继承及安全管理来实现的，其中安全产品的继承便涉及如何选择档案信息安全产品。在进行档案信息安全产品选型时，要求档案信息安全产品能满足两方面的要求：一是安全产品必须符合国家有关安全管理的政策要求，针对相关的安全产品必须查看其是否得到相应的许可证，如密码产品满足国家密码管理委员会的要求，安全产品获得国家公安部颁发的销售许可证，安全产品获得中国信息安全产品测评认证中心的测评认证，安全产品获得原总参谋部颁发的国防通信网设备器材进网许可证，符合国家保密局有关国际联网管理规定以及涉密网审批管理规定。二是安全产品的功能与性能要求必须考虑产品功能、性能、运行稳定性以及扩展性，还必须考查安全产品自身的安全性。

参考文献

[1] 庄丽萍 . 档案信息网络安全管理策略 [J]. 科技档案 ,2006,04(4):11.

[2] 孙梅霞 . 高校档案信息网络安全与防护 [J]. 兰台世界 ,2009:46-47.

[3] 张照余 , 章丹 . 档案信息网络安全的法律保护 [J]. 广东档案 ,2002(001):34-35.

[4] 程茶 . 档案信息网络安全管理问题与对策研究 [J]. 档案天地 ,2015(S1):96-97.

[5] 张晓路 . 档案信息网络安全对策 [C]// 信息社会档案学理论与实践 .0.

[6] 罗为群 . 如何做好企业档案信息网络安全的可靠运行 [J]. 兰台世界 : 上旬 ,2010:66.

 DOI: https://doi.org/10.36956/iser.v2i1.365

Electronic Information Technology Development and Application Analysis

Boyu Shi

School of Electronic Engineering, Xi'an Vocational and Technical College, Xi'an, Shaanxi, 710077, China

Abstract

With the gradual progress of society, electronic information technology has been widely used in various industries and fields, especially in agriculture. The use of electrical information technology has produced agricultural information technology. The use of electronic information technology is responsible for agricultural production, management, decision-making, and storage. As well as processing, it can provide agricultural researchers and producers with technical consultation and automatic regulation and other related services. In addition, it is also widely used in various fields such as aviation and industry. In the new era, the development of electronic information technology is in a stage of rapid development. In the future development, the development of electronic information technology will progress towards a broader prospect.

Keywords

electronic information technology; development trend; application analysis

电子信息技术发展及应用分析

石博宇

西安职业技术学院电子工程学院，中国 · 陕西 西安 710077

摘　要

在社会逐渐进步之下，电子信息技术被广泛使用在各个行业和领域中，尤其是在农业方面，电气信息技术的使用产生了农业信息技术，使用电子信息技术对农业生产、管理、决策、存储以及处理，其能够为农业研究人员和生产者提供技术咨询和自动调控等相关的服务。此外，其还在航空、工业等各个领域都有广泛使用。在新时期下，电子信息技术的发展正处于快速发展阶段，在未来发展中，电子信息技术的还会朝着更广阔的前景而进步。

关键词

电子信息技术；发展趋势；应用分析

1 新时期电子信息技术发展现状

在最近几年中，随着电子信息企业的快速发展，中国江苏淮安经济技术开发区的电子信息产业年均产值一直保持在30% 以上的增幅，在全区规划总值的比重也上升到 64.7%。在当前的淮安经开区电子信息产业中，有很多企业具备完整的产业链条。但是纵观整个电子信息技术发展情况，当前行业的发展现状突显出以下一些问题。

1.1 发展水平相对落后

就中国目前电子信息技术的发展情况来看，电子信息技术的使用范围逐渐扩大，并且有着空前的发展前景，这让电子产品普及范围也逐渐扩大，提升了人们生活的便捷性。但是和一些发达国家相比，中国电子信息技术水平相对还比较落后。因为资金投入的力度较小，其中研发的力度也比较小，很多电子信息企业使用的核心技术还是来自国际。再加之中国电子信息技术发展较晚，没有形成大规模与集成化，这些都对电子信息技术的发展形成了阻碍。针对这些问题，中国需要尽快地推进标准管理，创新管理理念，对相关的资源进行整合。依据目前电子信息技术标准发展情况来看，涉及的范围十分广，综合性也比较强，在发展中要在大局观念上进行整体规划，才能够促使相关行业的共同发展。在电子信息技术发展中，要对各种资源进行整合，促使电子信息技术的发展。在发展中要对各行业未来发展趋势进行全面分析。依据标准化发展相关的需求，重视产品的专业性，提升产品的技术含量，这样才能够在全球化发展中，有效提升中国电子信息技术的影响力，将目前中国电子信息技术发展的阻碍逐

 DOI: https://doi.org/10.36956/iser.v2i1.365

个击破。

1.2 复合型人才缺乏

在教育改革力度不断加强之下，改革专业人才培养的需求逐渐提升，为社会的发展提供了关键的支撑。但是从整体情况上看，高水平、高科技的电子信息技术复合型人才十分稀少。这是中国电子信息技术发展现状中比较明显的一个问题。在行业的发展中，部分科研人员大量流失，这让新时期下电子信息技术发展有严重的人力资源缺乏问题。针对这个问题，行业内部和相关部门要一起合作，逐渐加强对信息技术复合型人才的培养，这样才能提升电子信息技术整体水平。通过对人才的培养，才能够提升行业的市场竞争力，逐渐缩短中国和一些发达国家之间的距离。

2 电子信息技术发展趋势

2.1 网络化

经济全球化背景之下，人们为了扩大商业影响力，加强市场竞争力，不断地创新技术，使用新型设备来对数据进行分析与收集，而在其中最关键的就在于移动通信网络的信号形成。从目前的技术发展情况来看，使用无线信息传播、联通与交互信息网络，必须要有地面基站和通信卫星的支撑。但是其中最关键的一点就在于电子信息技术的支撑，这项技术把电子、电磁和电路设备与信息技术结合，把电信号转换成为信息，让人们使用电信号与电子设备获得信息，并且分析信息 [1]。在生物科学和人工智能技术发展之下，未来的电子信息会呈现出网络化发展趋势，其中包含了物联网、虚拟情境网络等，这些都会是电子信息技术的主要发展趋势。这个时候，人们不仅可以使用互联网传递信息，运用物联网远程控制电子设备。同时还能使用生物信息网络和其他人进行信息共享，使用情境网络来学习，这样就提升了人们的生活和工作效率。

2.2 光电子与集成化

光电子是目前电子信息技术中的核心技术，目前电子信息技术的发展经历了两个十分关键的时期，主要是光电学和电子学。在未来的发展趋势中，光电学会成为电子信息技术研究的新阶段，能进行能量的传输和信息搭载。在实际运用中，光子学能够分成能量光子与信息光子两个部分。依据市场的需要，光电子信息产业和光电子成了新兴学科，所以在以后的发展中，光电子势必会成为电子信息技术中的一个主要技术趋势。在电子信息技术的发展中，怎样让系统集成化，集成电路制作技术是关键所在，其也在电子信息技术发展中占据了举足轻重的地位。目前，中国集成电路制造技术起步较晚，和国际技术有很大的差距。但是在电子产品中有十分广泛的运用，比如智能卡以及电脑中央处理器等，这些都是用集成电路制造技术进行的。在行业的发展中，微电子技术愈加成熟，在未来集成电路产品集成化会大幅度提升，芯片功能会更加完善，体积也会越小。

2.3 规模化与个性化

在未来的发展趋势中，产品个性化与规模化是技术的主要发展方向。电子信息技术发展中，实现规模化才能够达到成本最优和效益最大化。全球化环境中，跨国企业发展优势会更加明显，企业的产品质量也会在技术革新之下有所提升，这样让电子信息技术进行了创新，让个性化发展逐渐显著。就比如目前市场上比较常见的电子产品，OPPO 手机比较重视拍照和音乐方面的技术优势，苹果手机侧重于系统上的创新，华为有些手机注重游戏性能。在技术产品的不同创新过程中，电子信息技术的发展也更加个性化，这些都让企业在市场中可以占据自己的地位 [2]。在未来发展趋势中，一些发达国家的电子信息技术发展水平会更高，发展中国家则使用一些技术含量较低的产品，两者之间会形成一种落差性。而这种梯度式的发展模式，同样是电子信息技术发展中的一种趋势。

3 电子信息企业肩负社会责任，积极主动创新发展

大数据、云计算、物联网，是“互联网 +”时代的专有名词，也是其特色标志，这足以说明，“互联网 +”时代，是一个大融合的时代。要推动信息技术产业与其他产业的融合，譬如与农业的融合，与工业的融合，与服务业的融合等，必须坚持创新，加大研发力度和投入，注重技术应用性的提升，追求电子信息技术产品的智能化，实现制造的智能化和服务的智能化。

因为市场环境的原因，中国电子信息技术的发展现状中还存在水平落后与人才缺乏的现象，针对这些问题行业内部要引起重视，采取各种措施来克服阻碍。从目前电子信息技

 DOI: https://doi.org/10.36956/iser.v2i1.365

术的情况来看，智能化、个性化以及网络化都是这项技术的未来发展趋势。

4 电子信息技术在物联网中的应用阐释

电子信息技术作为一种先进技术手段，是支持物联网技术发展的重要基础技术，更是增强物联网运行效率的根本保障。物联网的各个环节供应都离不开电子信息技术，电子信息技术也推动着中国社会的进步和发展。客观来说，物联网和电子信息技术之间有着相互促进、相辅相成的作用，能够有效促进行业进步和发展。所以，想要确保物联网科学运行和高效发展，就需要广大工程师和设计师对电子信息技术在物联网当中运用的相关内容，进行密切的关注，为物联网技术的长效发展打下良好基础保障。

4.1 电子信息技术与互联网技术内涵概述

4.1.1 电子信息技术

电子信息技术在不断发展和进步的当下，以及渗透到了人们生活当中各个层面当中，在电子信息时代的当下，人们已经离不开电子信息技术。在中国社会经济不断发展的当下，电子信息技术已经在社会各个层面当中广泛运用，并且在人们生活与工作当中起到了重要作用。事实上来说，电子信息技术所涵盖的内容非常广泛，例如传感器技术、通信导航技术、互联网技术、数据传输技术等内容，都是电子信息技术的分支构成。电子信息技术在发展过程中，所附属衍生品也不断增多，不仅便捷了人们的生活，而且有效增强了人们工作效率，提升了整个社会的现代化发展水平。所以，电子信息技术运用水平的高低，直接决定着社会的发展进程 [3]。

4.1.2 物联网技术

物联网技术是在互联网基础上所衍生出的技术手段，物联网技术不仅具备感知功能，而且还具备了信息识别功能，物联网强大的功能性，可以将人、信息、物与物进行紧密联系，当这些技术被广泛运用之后，物联网自身的便捷性也逐渐提升。客观来说，物联网也是互联网技术的延伸和发展，其中最为主要的内容便是以互联网为根基数据交互传输内容，在互联网基础上，将各个货物的信息进行交互，实现了的物与物信息的交汇互通。物联网技术的诞生和发展，真正的促进了物与物、人与人、信息与信息之间交流，并且物联网体系也正是运用此种手段开展的物流沟通。但是值得注意的是，物联网信息一般私有性能相对较强，可以在一定程度上保护用户个人的隐私，物联网技术结构交互图。

4.2 电子信息技术在物联网中的应用途径

4.2.1 电子订货系统

在互联网不断发展和进步的当下，电子信息技术的表现形式是丰富多样的。电子信息技术贯穿在物联网技术当中各个环节和程序当中，其中电子订货系统作为互联网体系当中非常重要的技术手段，直接决定物联网信息交互的成败 [4]。通过电子信息技术的运用，能够最大程度上促进货物之间的交互和信息调配与信息查询。在电子订货系统的运作之下，可以实现配货、订货等工作的良好开展。电子订货系统可以有效降低经销商成本，保障货物配送效率，切实强化物联网的高效运行与流通。对于电子订货系统来说，需要一个健康、安全的互联网环境，切实有效地保障物联网用户们的信息以及财产安全。

4.2.2 条形码技术

条形码技术兴起相对较早，但是真正实现大面积运用还是在物联网技术不断发展之后，才真正地投入到了社会各个层次当中。条形码是一种能够将网络信息数据互传顺利实现的电子技术，借助各种形态的条形码把产品的信息组合在一起，进而将完整的商品信息形成，然后在借助对应的扫描设备扫描条形码，以此将其中的商品信息识别出来，最后由计算机处理识别信息 [5]。在物联网系统当中，条形码技术主要便是通过对商品信息的扫描和输入，来记载和核对商品信息的一种技术手段。通过条形码技术手段扫描条形码，可以及时获取商品信息，为商品入库、商品运输扫描、商品防伪等工作打下良好的基础保障，切实有效地强化了物联网运作的实际效率。

4.2.3 通信技术

通信技术是在人们日常生活当中运用最为常见的一种技术类型，例如人们日常生活所涉及的语音聊天、视频通话等。通信技术的类型多种多样，微信、QQ、计算机、传真、电话等；脸书、QQ、微信等软件不仅可以进行语音通话，还可以迅速传递文字、图书或一些相应的链接。在信息技术和互联网技术的大力支持下，通信技术跨越了时间、空间的隔阂，可以随时随地的保障世界各地人们之间的信息交互。随着科学技术的发展和进步，通信技术在物联网当中也起到了巨大

 DOI: https://doi.org/10.36956/iser.v2i1.365

的作用。例如，当前用户们在订购商品之前，为了详细的了解商品信息，便会利用通信技术手段来实现买方与卖方之间的信息交互传输。物联网能有效继承互联网技术信息传输的实时性与高效性，不仅有效降低了信息交互成本，而且利用互联网信息交互手段还能够实现信息交互效率，真正的增强了人们物联网消费体验。

4.2.4 卫星定位技术

卫星定位技术的主要原理便是利用 GPS 技术和 GIS 技术，通过卫星定位技术手段来积极获取地面信息。运用 GPS 在物联网中将商品的位置找到，也可以对商品进行指挥，选择商品的接收和运输方式，把一些合适的存放地点找到。在物联网货物运输工作当中，利用卫星定位技术可以科学合理的通过对运输路线规划、运输系统导航等形式，制定出物联网运输的最佳路线，切实为物联网运输提供良好便捷的基础保障 [6]。此外，卫星定位技术还能够有效地分析和了解商品的数量和位置等信息，消费者可以随时随地的把控货物信息，为物联网发展运营打下良好基础。

5 电子信息技术在物联网的发展建议

在中国电子信息技术不断发展和进步的当下，物联网工程的发展必须要紧紧把握时代发展的趋势，抓住电子信息技术发展的永恒动力，促进物联网领域的可持续发展。加快物联网信息化发展与运行，科学的建立以电子信息技术为支撑的互联网系统网站，真切的满足当前广大客户们对物联网的实际需求。将信息技术和互联网技术进行紧密融合，切实的在保障物联网信息交互的基础上，增强物流运输的实际效率。此外，还应该利用电子信息技术，构建起物联网的信誉度。客观来说，互联网以及物联网都是属于虚拟经济类别的内容，想要真正的获取广大消费者们的信任，还需要切实通过电子信息技术的安全管理手段，避免物联网当中的安全风险产生。相反，物联网的发展与电子信息技术的发展有着密切的联系，还应该及时把握当前市场当中人们对物联网的需求，在基础上创新原有的电子信息技术，确保物联网与电子信息技术的共同发展。

总而言之，物联网与电子信息技术有着极大地关联，物联网是在信息技术支撑之下所开展的信息交互系统。想要切实有效地促进物联网的长效发展，就应该详细的分析互联网当中的电系信息技术，充分地利用电子信息技术来发展物联网，确保物联网的可持续发展，为人们的生活提供更多便捷。

参考文献

[1] 杜佳 . 我国电子信息技术发展及应用分析 [J]. 信息通信 ,2014 (08):138.

[2] 蔡雯 . 电子信息技术在电力自动化系统中的实际应用分析 [J]. 电子制作 ,2016 (014):65.

[3] 宫晓琴 . 新时期电子信息技术在农业机械中应用分析 [J]. 河北农机 ,2013(04):57-58.

[4] 王重超 . 计算机电子信息技术工程管理与应用分析 [J]. 现代商贸工业 ,2018 (017):197-198.

[5] 沈天舒 . 电子信息技术应用特点及其发展趋势分析 [J]. 电子世界 ,2015 (024):31-32.

[6] 姜涛 . 计算机电子信息技术工程管理与应用分析 [J]. 电子技术与软件工程 ,2015:18-20.

 DOI: https://doi.org/10.36956/iser.v2i1.366

Research on Modern Electronic Control Technology of Automobile Electrical Appliances

Sen Jiang

Guizhou Transportation Vocational and Technical College, Guizhou, Guiyang, 550000, China

Abstract

Modern electronic control technology in automotive electrical appliances in its development direction and development field is mainly to help the automotive industry better develop and better popularize. In addition, in the development of electronic control technology, the electronic technology used in automotive electrical appliances has been compared it mostly appears in the more ordinary automobile industry. In the automotive field, the relatively high-end automotive industry often adopts relatively advanced electronic control technology, which is also in line with the market positioning of automobiles. However, in modern society, modern electronic control technology does not only appear in high-end automobiles, but also in ordinary. The automobile manufacturing industry has also introduced relatively advanced modern electronic control technology to help the better development and popularization of automobile electrical appliances, and also help the development of modern electronic control technology.

Keywords

electronic information technology; development trend; application analysis

汽车电器的现代电子控制技术研究

江森

贵州交通职业技术学院，中国 · 贵州 贵阳 550000

摘　要

汽车电器中的现代电子控制技术在其发展方向和发展领域里主要是帮助汽车行业更好的发展和更好地进行普及，此外在电子控制技术的发展当中，汽车电器中运用的电子技术已经比较多地出现在较为平常的汽车行业中。汽车领域，较为高端化的汽车产业往往会采用较为先进的电子控制技术，也符合汽车的市场定位，但在现代社会中，现代电子控制技术不仅仅只出现在高端化的汽车中，在平常的汽车制造业中也已经引进了相对较为先进的现代电子控制技术，以帮助汽车电器更好的发展和普及，也帮助了现代电子控制技术的发展。

关键词

电子信息技术；发展趋势；应用分析

1 汽车安全性的控制

汽车作为人们出行的交通工具之一，安全性是其首要注意的一点。在汽车的安全性上，主要体现在驾驶员驾驶和汽车行驶的安全性上，这其中对于驾驶员来说，汽车的安全性直接决定着汽车的使用稳定性和驾驶员对于驾驶汽车的放心程度，汽车作为交通工具之一，在公路行驶当中，需要极强的稳定性和安全性，包括在路段行驶中的高速度行驶模式下，是否能够平稳运行，或者驾驶员能否依靠自身驾驶技术将汽车更好的驾驶，这不仅取决于汽车驾驶员的驾驶技术，也取决于汽车本身的稳定性上。因此，对于汽车安全性能的控制是汽车电器中现代电子控制技术首要的发展方向和首要注意的问题之一。

2 汽车通信方面的控制

汽车导航在汽车领域里已经必不可少，也是现代社会人们最基本的生活要求，在汽车电器中，导航技术的先进程度将直接决定着汽车驾驶员对于汽车的驾驶体验，加上汽车的导航性能的好坏，也会决定着驾驶员对于路程的选择，在一定程度上能够体现出能否帮助驾驶员更好地进行驾驶，从生活层面上来讲，这将会提高人们出行的舒适度，也会帮助人们更好的选择出行路线以及能否在一定的时间段内到达目的地，保证出行的效率。

 DOI: https://doi.org/10.36956/iser.v2i1.366

3 现代电子控制技术在汽车电器中的研究

现代电子控制技术随着社会经济和科学技术的不断发展而逐渐被人们所重视，尤其现代电子控制技术在汽车领域里的使用，极大地方便了汽车行业对于汽车普及的力度，在汽车电器中的现代电子控制技术在使用性能上极大地改变了传统的汽车电器使用性能和使用方便性上，尤其处在现代社会中，汽车电器的整合程度以及汽车电子控制技术的集成度上，人们对其都有了较高的要求，所以，在汽车电器中，现代电子控制技术的应用将在很大程度上方便人们驾驶汽车以及在日常生活中对汽车的使用。

3.1 在汽车整体结构上运用现代电子控制技术

汽车的出现是为了方便人们出行，而汽车电器的出现是为了帮助人们更好的驾驶。因此，在汽车电器中，现代电子控制技术的运用使得汽车电器得以发展和提高，尤其在汽车的整体结构上运用现代电子控制技术，将会在最大程度上提高汽车的使用舒适度。汽车点火系统的基本功能是在接近压缩行程上止点时，在气缸内产生电火花，点燃压缩的可燃性混合气。点火系统的工作原理是在点火线圈中的一个绕组中反复通电、断电，在另一个绕组中感应出高电压。点火系统的设计要考虑的因素：燃烧室的结构、空燃比、发动机的转速范围、发动机的负荷、发动机的用途及排放法规等。在发动机管理系统中包括点火与燃油组合管理系统、废气排放控制及车辆控制系统等。涉及的控制方式包括闭环控制、爆燃控制及怠速控制。综合控制系统采用一个或多个控制单元（ECU），这些 ECU 之间通过控制器局域网（CAN）数据总线能够互相通信，采用集中控制的方式控制每个单元中做到它的最佳状态。实现全面的集中控制的优点可以使车载诊断（OBD）扩展到整车，节省修理时间和运行费用。随着科技的发展，人工智能和神经网络也应用到发电机管理系统中。此外，在现代电子技术的运用当中，结合相应的科学技术发展方向，将安全保障方面的技术以及方便驾驶方面的技术运用进去，将会大大提高驾驶体验和驾驶乐趣，使得驾驶汽车更加安全也更加可靠 [1]。

3.2 汽车具体功能上采用现代电子控制技术

汽车的使用是为了提高出行的效率，在汽车的具体功能上，包括转向、刹车、警报等方面运用现代电子控制技术，从根本上解决了汽车的使用困难，这其中，对于汽车的转向系统，运用现代电子控制技术，最突出的一点就是现代汽车电器中出现了汽车转向助力系统，可以帮助人们节省力气，实现高效率的转向。此外对于汽车刹车系统，在汽车行驶过程中，如果需要紧急刹车，驾驶员最普遍的一个做法就是紧紧踩住刹车，这将会使得汽车发生漂移，从而很容易发生交通事故，而现代电子控制技术的运用，将汽车刹车系统进行优化，做出了 ABS 汽车刹车系统。因此，在现代电子技术的运用当中，使得汽车电器的发展更迅速也更高效，极大地方便了人们的生活。

因此，在汽车电器的电子控制技术的发展中，电子控制技术得以实现的前提就是现代社会对于汽车电器的需求而来。此外，现代电子控制技术已经发展的相对成熟，较之传统的汽车电器，在使用的方便性以及效率性上都有所提高，极大地方便个改善了人们使用汽车和驾驶汽车的习惯。所以，现代电子控制技术在汽车电器中应用的重要性极大。

4 电动汽车核心控制器

大力发展新能源汽车、加快交通能源转型是实现汽车工业可持续发展的重要途径。如今，中国已经成为全球最大的新能源汽车市场，中国新能源车企业如何乘着政策东风在市场上站稳脚跟是决定中国汽车行业成败的关键。其中，在电动汽车核心控制器技术领域实现重大突破是重要环节。

4.1 电动汽车核心控制器发展现状

4.1.1 整车控制器

整车控制器（Vehicle Control Unit，简称 VCU）是实现整车控制决策的核心控制单元，对电动汽车的动力性、经济性、安全性及舒适性有很大影响。VCU 通过采集油门踏板、挡位、刹车踏板等信号来判断当前需要的整车工作模式（充电模式或行驶模式），采取闭环控制从而计算出当前车辆所需的实际转矩；负责整车网络中信息的组织与传输、网络状态的监控、网络节点的管理、信息优先权的动态分配以及网络故障的诊断与处理；对制动能量回馈进行控制。

目前整车控制器技术在国际已趋于成熟，各汽车电子零部件巨头如博世、法雷奥都纷纷进行整车控制器研发和生产。部分汽车设计公司，如 AVL、RICARDO，也为整车厂商提供整车控制技术方案，在电动汽车整车控制器领域也有不少成功案例。国产厂商大多已具备自主研发生产整车控制器并进行整车控制系统设计的能力，如比亚迪、北汽等企业均为自己配套。

 DOI: https://doi.org/10.36956/iser.v2i1.366

4.1.2 电机控制器

电机控制器（Motor Control Unit，简称 MCU），MCU 是控制主牵引电源与电机之间能量传输的装置。主要作用是控制驱动电机三相输入交流电的电压、电流、相序及频率来调校整车各项性能，完成对电动机转矩、转速、转向及能量回收的控制，保障车辆的基本安全及精准操控。

中国驱动电机已基本实现国产化，但电机控制器在功率密度、芯片集成设计、热管理设计等方面与国际差距较大。中国电力电子技术起步相对较晚，部分电机电控核心组件如 IGBT 芯片仍不具备完全自主生产能力，这使得中国电机控制器的功率密度水平和国际量产产品存在较大差距。以 IGBT 模块为例，作为新能源汽车驱动系统和直流充电桩的核心器件，其成本占新能源整车成本的 10%，占充电桩成本的 20%。中国作为世界上最大的功率半导体市场，占世界市场份额达 50% 以上，但中高端 IGBT 功率半导体主流器件，基本被欧美与日本等国际厂商垄断，如英飞凌、三菱、日立、东芝等。

4.1.3 电池管理系统

电池管理系统（Battery Management System，简称 BMS），是衔接电池组、整车控制器和驱动电机控制器的重要纽带，是动力电池组的核心技术，也是整车企业最为关注的核心技术。电池管理系统的主要任务是监测动力电池组的单体电压、温度、总电压和总电流的状态，与整车进行数据通信，预测电池的荷电状态，管控电池循环寿命，进行电池热管理及电芯均衡管理，对电池出现的故障进行诊断和报警，延长其使用寿命等功能。

国际比较早就开始研究电动汽车，且研究初期就比较重视 BMS 的研究。经过政府和各大企业几十年的努力，来自美、日、韩、德的诸多汽车行业巨头，如 SK、DENSO、LG Chem 等，已经占据电池管理系统领域的半壁江山。中国开始研究 BMS 起步较晚，在市场占有率上落后于国际产品。但在政府的大力支持、高校的努力推动下和企业的积极进取下，一大批像比亚迪、宁德时代、派司德科等优质企业已经在全球崭露头角。

4.2 电动汽车核心控制器发展趋势

4.2.1 整车控制器

随着电动汽车市场逐渐繁荣与成熟，新能源汽车供应链企业之间加强协作是未来的发展方向。整车控制器企业将与动力电池、电机、整车厂商等企业协同发展，在动力电池、驱动系统和整车之间寻求最佳方案。具备电动汽车整车控制技术的企业将逐渐发展成为方案提供商，专门进行软件层面的系统设计以及整车性能试验调试等。而硬件部分将逐渐趋于专业化，由专门的汽车电子企业研发生产。

4.2.2 电机控制器

电机控制器作为驱动电机系统的核心部件，其发展趋势主要集中在以下四个方面：一是高度集成化带来的安全性能提升。目前，电机控制器、车载充电机、DC/DC、电动空调系统等高压部件已经实现集成化，其高压安全、温度控制、电磁兼容等性能将更加严格；二是高功率密度化。依据各类车辆对动力性能的要求及车辆总布置的空间需要，提高电机控制器对电能的可承载能力、体积随分装向小型化发展是实现电机控制器高功率密度的重要途径；三是高压化。IGBT 的耐压能力也将由 650V 往更高的 750V 乃至 1200V 发展；四是电磁兼容性能提升，EMC 等级将会达到更高的 Class5 水平。

4.2.3 电池管理系统

目前，中国在 BMS 性能方面和国际顶尖水平相比，还存在不小差距，仍然是中国电动汽车发展的一块短板。其发展趋势主要有四大方面：一是电池状态估算技术的提升。利用建立更加可靠的电池模型、电池测试大数据等分析手段，补偿电池老化而导致的模型变化，优化充、放电控制算法，进一步提高 SOC、SOH 等技术精度；二是电芯均衡管理向非能量耗散型转化，提高能量的利用率；三是动力电池热管理由风冷技术向具有换热系数高、热容量大、冷却速度快的液冷技术发展；四是进一步升级 BMS 自诊断技术，提前预防 BMS 系统失效 [2]。

伴随着新能源汽车的进一步推广，新能源汽车产业也将迎来更大的发展契机。在展望新能源汽车快速发展的同时，也必须清楚地看到当前仍然还面临着的诸多重大挑战。中国新能源汽车企业要正确把握电动汽车三大核心控制器的发展方向，加大对技术创新和新产品研发的投入，以领先的技术、良好的品质引领新能源汽车行业发展潮流，为中国新能源汽车产业的快速发展提供可靠的保障。

5 关于汽车电子控制与智能交通相结合的思考及探索

5.1 现代汽车电子控制的技术

5.1.1 动力传动系统电子控制

汽车变速箱和发动机的电子控制技术是目前汽车动力系

 DOI: https://doi.org/10.36956/iser.v2i1.366

统的主要构成部分，而其电子控制技术的核心就是发动机缸内空燃比例与点火时间。而现代汽车电子控制技术不仅仅局限于此，还包括向电瓶补充电源、发动机的开启和停止还有极限转速的控制等重要的辅助功能。在变速箱的电子控制中，其技术核心主要体现在变速箱的自动变速上，这一功能就是现代汽车的重要标志。ECU（Electronic Control Unit），即电子控制单元，作为现代汽车发展的里程碑是智能汽车思考的核心工具，用通俗的话来讲 ECU 就是汽车的“大脑”。在汽车的行驶过程中，电子控制单元（ECU）可以接收到汽车的相关信息并将这些信息处理为电子信息，传感器可以对这些所传达的电子信息进行合理的判断，进而进行加速或限速等信息的传达并控制所执行元件和液压输出最终完成变速器换挡这一指令。除此以外，电子控制单元还可以对动力传感系统进行控制。电子控制单元一开始是单独控制系统，经过相关研究人员不断地研究与创新电子控制系统已逐渐向集成控制系统方向转变。而这种转变的最大优势就是可以更好地调节发动机和变速箱的配合，这样一来传感器的使用率就会降低进而就会使得换挡带来的动力损耗大大降低。通过大量的研究和数据表明在智能汽车的开发中电子控制单元的集成控制可以大大降低智能汽车的排放量，这样一来由汽车排放造成的对环境的破坏就会大大减小。除此以外，集成控制下的汽车在驾驶与变速的过程中都相对来说较为平稳顺利，这对减小驾驶成本有很大的帮助。ULSI 集成电路技术，即超大规模的集成电路技术可以通过 A/D 的转换提高汽车电子运算的精度，最高可达十倍以上，运算精度的大幅度提高为汽车的智能化提供了强有力的支撑。

5.1.2 车身系统的电子控制

关于车身系统的电子控制主要有两个部分组成，第一个部分是安全驾驶中的被动车载控制，第二个部分是常规性能的日常使用。第一个部分安全驾驶的被动性电子控制主要包含防盗系统的自动保护，以及安全气囊的实时启动等。而第二个部分常规性能的日常使用包含的系统就多而繁琐，不仅包括全车电灯的控制和车门锁的自动控制，还包括车内空调的控制以及汽车雨刷的控制等诸多方面。作为车身电子控制中提升驾驶安全的重要一环，安全气囊在汽车中的应用与开发对保障司机安全、提升行车驾驶安全有着相当重要的作用。其工作原理较为简单，在车辆行驶过程中发生碰撞的时候，传感器会对碰撞程度进行检测并传达到电子控制单元，再经由电子控制单元进行分析并判断是否应该开启气囊。若电子控制单元分析后决定应该开启气囊，那么就会发出点火的信号，点火的信号传递至点火器后点火器会及时点火让气囊进行迅速地膨胀以保障驾驶员的安全。接下来笔者将以汽车内的空调为例对其他常规电子控制进行简要的分析与介绍。电子控制单元可以对比驾驶室内外的气温，在感受到较大的温差时会对驾驶室内的气温进行智能化调节。当然，人为也可以在电子控制单元中预设温度要求，电子控制单元会根据要求对温度进行调节以达到人体最能接受的温度，给人带来极舒适的体验。

5.1.3 底盘系统的电子控制

底盘系统的电子控制主要包括车身电子稳定系统、制动防抱死系统和驱动轮防滑系统等主动防护系统也包括定速巡航和电子转向助力等电子控制，主要体现于外接悬挂的电子控制设备。车身电子稳定系统全称为 Electronic Stability Program，一般简称为 ESP，制动防抱死系统全称为 antilock brake system，一般简称为 ABS，驱动轮防滑系统全称为 AccelerationSlip Regulation，一般简称为 ASR。悬挂电子控制系统可以很大程度上促使车辆行驶中操控性和舒适程度的结合，它可以根据汽车行驶中的路况来对是否应该调节悬架的高度进行判断。车身电子稳定系统由两部分组成，其一是制动防抱死系统，其二就是驱动轮防滑系统，车身电子稳定系统主要负责分析传感器信息，进而对行进速度和转向命令等信息进行操作。在过度转向时会经由车身电子稳定系统发出偏离信息，然后再经由驱动轮防滑系统对车身电子稳定系统发出的命令进行调整，为汽车的稳定行驶带来物理上的保障。而电子转向助力能达到方向盘的最优控制，它是通过转矩转速控制和电子控制向方向盘施加压力实现的。定速循环系统非常适用于高速公路的驾驶，它与无级变速的理念非常接近而且可以让汽车在行驶中保证平均速度稳定的前提下实现最低油耗。通过定速循环系统在高速行驶的情况下，驾驶员要保持行驶的速度不变就不需要踩油门了。

5.2 电子控制与智能交通相结合

5.2.1 汽车智能化联网系统

所谓汽车智能化联网系统，具体实践中从字面上就不难看出是汽车本身和道路电子系统联网从而使汽车在驾驶的过

 DOI: https://doi.org/10.36956/iser.v2i1.366

程中方便地得到路况交通等多方面信息。汽车智能化联网系统中最为大众所熟悉的就是 ETC（Electronic Toll Collection）不停车收费系统。该系统将车辆自身的信息和道路交通信息通过联网以提高出行效率，除此以外还能很大程度上提高公路的利用率、减少人员浪费。现如今，驾驶员在行驶的过程中可以通过手机来缴费，大大减少了等待的时间从而很大程度上提高了出行效率。除此以外，GPS 定位系统还可以通过对道路交通的分析来对路线进行规划，很大程度上避免了堵车造成的不便 [3]。

5.2.2 交通服务系统地提升

电子控制与智能系统相结合可以有效促进交通服务系统的提升。交通服务系统利用无线电设备通过广播来报道车辆所在道路的信息，主要包括道路的交通拥堵状况和是否发生事故，如果该道路上有事故发生还会对事故发生的地点和方向进行报道。交通服务系统方便了驾驶员了解路况信息，也很大程度上避免了在发生事故的路段上重大连续事故。在驾驶员驾车行驶的过程中，驾驶员可以将自己所在路段的道路交通信息通过交通服务系统来传达给道路交通指挥部门，这样可以提高了信息的及时性同时也提高了交通信息的覆盖面。交通控制中心不仅可以采用红外线检测器对交通服务系统进行必要的管理，还可以利用视频监控系统对交通服务系统进行管理从而提升交通秩序。除此以外，在重点交通路段还设置了流量监控版和交通流预测感应设备从而为驾驶员提供实时的路段信息。

5.2.3 驾驶辅助功能系统

现如今自动驾驶系统构建还不够完善，但是有许多类似于自动泊车、停车辅助、限速信息和车道偏离系统的自动驾驶的衍生系统已经被越来越广泛的应用。这些系统在高级轿车中的应用非常广泛，例如宝马 7 系轿车。道路泊车系统的自动刹车和主动巡航可以通过摄像雷达技术的应用来实现，其系统主要利用道路信息的采集来判断车辆的停泊情况并将红外感应和雷达摄像技术融入其中。在认为判断不及时的情况下，道路泊车系统可以通过扫描信息对前方车距进行及时的判断并作出自动控制，这样就可以很大程度上提高了驾驶员道路行驶的安全性。常见的驾驶辅助功能系统还包括夜视辅助功能系统和车道偏离系统，这两类驾驶辅助功能系统主要通过影像传输来采集外界路况信息，该系统所采集的路况信息包括限速提示和车辆位置的信息，通过路况信息的采集驾驶员

扫描信息对前方车距进行及时判断在人为判断不及时的情况，系统做出主动判断和自动控制，这样的功能加强了道路行驶的安全性。夜视辅助功能系统和车道偏离系统，主要通过影像传输系统来完成对外界路况的信息采集。如限速提示和车辆位置信息，这样的功能使驾驶变得更为轻松快捷 [4]。

5.3 对汽车电控自动变速的控制

车速是汽车行驶过程中的重要参数，同时作为交通系统中的主要控制对象之一，在智能交通系统中需要对自动变速技术进行研究并对车速进行控制。下面笔者将电子控制液力自动变速器为例对汽车电控自动变速的控制进行分析和探讨。电子控制液力自动变速器是由传感器、自动换挡执行机构和 ECU 三个部分组成。传感器是将车速信息转化成电子信号然后传输到 ECU 当中，电子信号在 ECU 之中进行有效地处理后输出控制信号，控制信号被传输至电磁阀中进而有效进行油压回路的而控制。对于电子控制液力自动变速来说，它可以利用微机系统来进行控制，由传感器来提取与车速相关的信息并以此来对其进行控制，除此以外 ECU 的存储器会根据不同的情况来进行适应性调节以获得最佳的换挡规律，电子控制液力自动变速器还可以针对相关信息进行驾驶员的调用以保证最佳调速。在电子控制液力自动变速器的传动系统中可以实现软性链接，这主要是由于传动系统是利用液体工作机制的，软性链接可以在有效提升使用时间的同时大大降低噪声。换挡使用的行星齿轮系统主要是啮合齿轮组这样可以大大降低在换挡过程中出现的齿轮冲击现象，除此以外还能够实现自动操作汽车起步和换挡。

参考文献

[1] 张召晖 , 白晓刚 . 汽车电器现代电子控制技术研究 [J]. 中国科技投资 ,2016 (13):190.

[2] 宋秋红 , 李文萱 . 关于汽车电器的现代电子控制技术研究 [J]. 南国博览 ,2019(09): 386.

[3] 武明先 , 陈丹 . 汽车电器的现代电子控制技术探讨 [J]. 大众汽车 ,2014 (08):11+13.

[4] 郭策 , 张兴 . 汽车电器的现代电子控制系统应用研究 [J]. 引文版 : 工程技术 ,2016(02):260.

 DOI: https://doi.org/10.36956/iser.v2i1.367

Analysis on the Development Situation and Existing Problems of China's Agricultural Information Technology

Hongqian Li

Institute of Agricultural Remote Sensing and Information Technology Application, Zhejiang University, Hangzhou, Zhejiang, 310058, China

Abstract

With the development of information technology, agricultural information technology has also become an indispensable part of China's economic construction. Agricultural sensor technology, agricultural robot technology, agricultural Internet of Things technology, precision farming technology, agricultural information service technology, etc. constitute China's agricultural informatization technology, which can provide theoretical and practical support for the development of Chin's agricultural informatization. The paper briefly analyzes the current situation and existing problems of China's agricultural information technology development.

Keywords

China's agriculture; information technology; development situation; problems

浅析中国农业信息化技术发展现状及存在的问题

李洪倩

浙江大学农业遥感与信息技术应用研究所，中国 · 浙江 杭州 310058

摘　要

随着信息技术的发展，农业信息化技术也成为了中国经济建设中不可或缺的组成部分。农业传感器技术，农业机器人技术，农业物联网技术，精细农作技术，农业信息服务技术等组成了中国农业信息化技术，能够为中国农业信息化的发展提供理论与实际的支持。论文对中国农业信息化技术发展现状及存在的问题进行了简要的分析。

关键词

中国农业；信息化技术；发展现状；问题

1 引言

在中国，信息技术在农业领域的应用始于 20 世纪 70 年代末，比美国晚了近 30 年，但发展势头很好。短短 30 多年的时间里，中国农业信息技术经历了起步、普及、发展和提高几个阶段，与发达国家的差距正在逐步缩小，在某些地区有些技术应用已达到了国际水平。

2 中国农业信息技术发展阶段

2.1 起步阶段（1979—1985 年）

这一阶段，主要是利用计算机的快速运算能力，解决农业领域中的科学计算和数学规划问题。1979 年，江苏省农业科学院使用计算机对 78 头新淮猪、六千多头仔猪进行了 2 月龄断奶个体与繁殖力的相关和回归统计分析。1981 年，中国建立了第一个计算机农业应用专门研究机构——中国农业科学院计算中心，此后中国北京农业大学、中国农科院等单位相继研制出了农业统计分析和模型模拟软件包、模糊聚类分析程序等。1984 年，中国天津武清区等地已开始利用计算机技术和数学规划、系统分析技术方法，制定生产管理方案。

与此同时，一些单位开始了遥感、模拟模型、专家系统农业应用的探索性研究与试验。1979 年从其他国家引进遥感技术应用于全国土地资源调查。1983 年，中科院合肥智能所开始农业专家系统研发，高亮之等在美国发表了“苜蓿生产的农业气象计算机模拟模式（ALFAMOD）”。其后，中科院上海植物生理研究所推出了“水稻群体物质生产的计算机模拟模型”。

2.2 普及阶段（1986—1990 年）

这一时期，应用以农业数据处理、农业信息管理为主，农业专家系统成为热点，农业模拟研究也有所进展。

 DOI: https://doi.org/10.36956/iser.v2i1.367

中国农业信息数据库与管理信息系统建设起步较晚。1986 年，组建了农业农村部信息中心，并提出了《农牧渔业信息管理系统总体设计》方案。1988 年，中国农科院作物品种资源所初步建成了拥有 27 万份终止信息的中国作物种质资源信息系统（CGRIS），初步建成了《中国农业科技文献数据库》，实现了全国范围内共享检索服务。1990 年国家物价局信息中心研制了“农产品集市贸易价格行情数据库”收集了 35 个大中城市的 28 种大宗农副产品的集市贸易价格。

1985 年开始，中科院合肥智能所开发的砂姜黑土小麦施肥专家咨询系统，在中国安徽淮北平原十多个县得到较大规模推广，农业专家系统开始从实验室进入生产一线。此后，相继研制出了作物育种、田间管理和病虫害防治，以及鸡猪饲养管理、水利灌溉等多种农业专家系统，如中国农科院作物所的品种选育专家系统，植保所的黏虫测报专家系统，中国华中理工大学的园艺专家系统，中国浙江大学与中国农科院蚕桑所合作的家蚕育种专家系统，中国北京农业大学的农作制度专家系统，中国农科院畜牧所的畜禽饲料配方专家系统等，某些成果达到了国际水平。

中国农业模拟模型研究与应用始于 20 世纪 80 年代。1987 年，对中国四川省郫都区生猪生产系统进行了动态模拟研究。1988 年，运用系统动力学方法对中国陕西省紫阳县粮食供需系统的发展变化进行动态模拟，利用模拟模型评价了原规划方案，提出了更合理的发展方案。在作物生长模拟方面，比较成功的例子是中国江苏省农科院推出的水稻模拟模型 RICEMOD。中国农科院棉花研究所开发的棉花生产管理模拟系统也有一定的实用性，1990 年在中国山东、中国河南等地示范推广 3.5 万多公顷，每公顷增产皮棉 125kg。

2.3 发展阶段（1991—1995 年）

从 1990 年开始，科技部把农业专家系统等农业信息技术列入了 863 计划的重点课题，给予了重点支持。以智能化农业专家系统、农业系统模拟模型及实用 DSS（煤炭辅助决策系统）、GIS 为主要内容的研究在作物栽培、作物育种、畜禽饲养、农业生态环境控制等各农业领域得到了推广应用，网络开发也提到了议事日程。

90 年代，中国初步形成了一批有影响的农业专家系统。例如，中国吉林大学的“多媒体玉米生产专家系统”，中科院合肥智能所的“施肥专家系统”“水稻生产专家系统”，中国北京农林科学院的“小麦生产专家系统”，中国哈尔滨工业大学的“大豆生产专家系统”等。在国家的支持下，这些系统得到了进一步地完善。此外，中国辽宁农科院的水稻育种、施肥专家系统，中国华中理工大学的柑橘园艺专家系统，中国浙江大学的家蚕育种专家系统，中国江苏农科院的水稻模拟优化决策系统和疾病诊断专家系统也在农业生产实践中获得了应用，取得了比较明显的效益。

在作物模型研究方面，中国农科院农业气象所将引进的 CERES 玉米模型予以汉化，中国华南农业大学推出了水稻模拟模型 RSM，中国江苏省农科院采用 CERES 模型，系统地评价了全球气候变化对中国粮食生产的影响。

农业专家系统、农业模拟模型、农业管理信息系统的发展为农业煤炭辅助决策系统的开发奠定了基础，先后出现了一批主要服务于作物生产管理决策及用于农业宏观经济指导的农业管理煤炭辅助决策系统。例如，1992 年，中国江苏省农科院将作物模拟技术与水稻栽培的优化原理相结合，建成了水稻计算机模拟优化和决策系统 RCSODS，用户输入常年气候资料和水稻品种遗传参数，可以做出常年优化决策，根据当前苗情和未来天气预报，可以提出肥水和其他管理措施及对策。中国北京市农林科学院作物所利用人工智能技术和网络技术开发的“小麦管理计算机专家决策系统”，用于指导北京地区的小麦大田生产，经过 1994、1995 两年的实际应用和示范验证，使小麦产量增加 10%~15%，生产成本降低 5%~7%，效益提高 15%~20%。

2.4 提高阶段（1995 年以后）

随着微机价格不断下降、软件开发环境不断完善和提高，尤其是 Internet 的出现及其相关知识的普及，计算机网络工程的研究、开发和实施成为热点。中国计算机应用包括农业应用出现了第二次普及高潮，所不同的是人们已经把注意力集中在信息资源共享、计算机应用技术如何与生产实际相结合，既出成果又出效益等方面 [1]。

农业农村部 1994 年开始筹建的“中国农业信息网”，1996 年正式开通。中国农业科学院建立的“中国农业科技信息网”1997 年 10 月开始运行。同时各省市也相继建立了农业信息网站，多数省份成立了农业信息中心，已建成的一些大型农业信息资源数据库和管理信息系统通过网络得到了很好地利用。

 DOI: https://doi.org/10.36956/iser.v2i1.367

1996 年以来，中国选择北京、云南、安徽、吉林四个地区建立了首批智能化农业信息技术应用示范区，并逐步扩展到了全国 20 个省市，示范区以农业专家系统为突破口，累计示范应用面积 2000 万亩，辐射推广面积 1 亿亩。在不同起点和条件的示范区内，专家系统发挥了巨大作用，作物的产量得到了提高，农民的经济状况也有了改善。以中国吉林示范区为例，1996 年开始应用多媒体玉米生产智能系统 MIS-MAP，三年增产玉米 5000 万 kg，增收 5000 余万元。20 世纪末，中国开始 3S 技术综合农业应用试验，中国农业科学院草原研究所应用现代遥感技术和地理信息技术建立了“中国北方草地草畜平衡动态监测系统”，使中国草地资源管理进入了一个新阶段，将过去用常规方法需上百人 10 年完成的工作量缩短到了 7d，获得 1997 年国家科技进步二等奖。中国北京市农业局的 GPS 导航飞机防治麦蚜技术、基本农田地理信息系统（GIS）也先后取得了成功。此外中国北京、中国上海等地先后建立了精准农业示范区。

3 发展中的问题

中国农业信息技术虽发展很快，但仍然存在一些问题，总体来看有以下几个方面。

3.1 基础设施缺乏，地区之间参差不齐

与发达国家相比，中国在农业信息技术方面的资金投入相对不足，虽然已全面启动“金”字工程，加快了各种信息网及高速信息公路的建设，而且为此 2000 年国家拿出了 2000 万元专项资金，但对我们这样一个大国来说，这无异于杯水车薪，农业信息基础设施建设仍是薄弱环节。目前，计算机在农业基层系统中的普及率仍然很低，而且不同地区发展很不平衡，要在全国范围内达到乡镇、农户联网，尚有大量的工作要做 [2]。

3.2 信息资源建设滞后，难以满足实际需要

中国虽然建成了近三十个大型数据库，但总体来看，农业信息资源的建设规模和覆盖面小，地域和领域分布不均，缺乏统一规划与规范。虽有一千五百多个农业信息网站，但是网上综合性信息多，专业性信息少；简单堆砌的信息多，精心加工的信息少；交叉重复的信息多，有特色的信息少；目录数据库多，全文数据库少；自用数据库多，共用共享数据库少。目前，尚未有一个适合基层农民利用的数据库资源，与“路况差”相比，“无货可运”的问题更为严重。

3.3 基础研究乏力，低水平重复较为严重

作物生长模型等研究工作，虽然早在“七五”期间已经开始，但进展十分缓慢，这里有国家、地区的投入少，科研单位急功近利等原因，也与缺乏统一规划和引导，不同部门、单位之间未能相互协作有关。仅以棉花生长发育模拟模型研究为例，就有中科院动物所、中国北京农业大学、中国农科院棉花所、中国江苏省农科院等单位独立研究，而成果均为功能相似的初级产品。“八五”以来国家推出了 863-306 计划，加强了对农业信息技术研究和应用工作的引导与支持，但问题并未得到真正解决 [3]。例如，目前二次开发的一些所谓的专家系统，只不过是仅有简单查询功能的链接文件。

3.4 人才严重短缺，主体素质有待提高

农业信息技术开发应用中，人才与用户的素质是两个十分重要的因素。目前中国农业技术人员匮乏，以经济相对发达的中国上海为例，每万名农业劳动力中科技人员仅为 15 人，既懂信息技术又懂农业技术的复合型高级人才更为奇缺，农业信息系统技术研究开发力量薄弱，难以进行大项目的攻关。作为农业信息技术使用的主体，中国农民文化素质相对低下。以中国河北为例，农村劳动年龄内受教育人口就学率只有 4%，农业劳动力受教育程度为 6、7 年，从而导致信息意识差，对信息技术需求愿望低。

3.5 产业化程度低，市场机制远未形成

除中国黑龙江等地外，中国多数地区均为农户小规模分散生产经营，农业产业化程度很低，难以形成信息需求。农业信息技术研究及咨询主要还是对上服务，而直接面向农业生产、服务农户的技术研究尚为数甚少。研究内容单一，目标分散，适应面窄，缺乏多学科专业综合应用研究等也使得信息产业化难以形成。

4 加速中国农业信息技术发展进程

4.1 农业信息技术的作用与影响

目前，农业信息技术在发达国家已得到广泛应用，并已成为农业系统不可缺少的生产要素。发达国家的经验表明，信息技术的普遍应用，使农业生产在机械化的基础上实现了集约化、自动化和智能化，经营管理实现了科学化，提高了农业对市场的反应能力，增强了农业抵御自然灾害的能力。

 DOI: https://doi.org/10.36956/iser.v2i1.367

在中国，农业高度分散、生产规模小、时空变异大、量化规模化程度差、稳定性和可控程度低等行业性弱点更为明显。农业信息技术的应用对于农业现代化的推动和影响作用将更为突出，主要表现在以下几个方面。

4.1.1 推进农业生产的自动化和智能化

计算机自动测控、人工智能等技术的普遍应用，使农林牧副渔业的生产在机械化的基础上实现自动化和智能化。

4.1.2 增强农业生产管理的科学化

农业生产系统是一个复杂得多因子系统，受气象、土壤、作物及栽培管理技术等多种因素的影响。随着农业生产技术水平地提高，农业高新技术的应用，农作物和动物饲养对自然环境和条件的控制需要更加严密和精确。必须依靠监测、模拟模型、人工智能、3S 等信息技术去获取、处理、分析数据，选择管理措施。

4.1.3 促进农业生产的集约化与产业化

农业信息技术的应用将会极大地促进农业生产结构的进步和生产方式的变革。计算机网络、精细农业等技术在农业上的广泛应用，将使传统农业的粗放方式为集约方式所代替，把“千家万户的经营与千变万化的市场连接起来”，实现规模化、专业化与市场化经营，降低成本、提高效益。

4.4.4 增强市场竞争能力，减少经营风险

市场经济是信息引导的经济。准确、及时的市场信息能够有效地指导农业生产经营者的实践活动，帮助它们确定生产什么、生产多少、如何生产等问题，减少盲目性、趋同性，降低市场风险。尤其在中国加入 WTO 后，国际农产品市场竞争激烈，更要依靠信息技术，把握变化多端的市场，融入国际经济大环境之中。

4.1.5 有效利用农业资源，保障农业可持续发展

运用卫星遥感、地理信息、全球定位、空间分析等现代信息技术，可及时取得土壤、气候、植物和水等自然资源以及病虫草害、森林火灾发生变化的现实性资料，实现对农业生产和资源环境的有效监测和预警，促进资源和生态环境的合理利用与有效保护，达到优质、高产、高效、低耗，最终实现农业的可持续发展 [4]。

4.1.6 有利于农业新技术研究和推广

计算机网络、数据库等农业信息技术的应用拓宽了农业科研的信息渠道，提高了科研速度和水平，作为农业新技术的高度浓缩与传播载体，促进现代农业科学技术及成果的迅速推广和普及。而模拟仿真等技术的应用，则从根本上改变了农业科研的方式方法，大大缩短了农业科研的周期。

4.1.7 加强农业宏观经济管理

农业现代化不仅要求微观农业经济的优化，更要达到农业宏观经济的合理化，在市场经济体制下，国家和地区性的宏观指导就显得更加重要，农业系统的复杂性、动态性、模糊性和随机性决定了农业经济管理决策的复杂性。卫星遥感等技术可以及时获得作物生长信息，计算机网络等技术可以及时收集市场信息，管理信息系统和煤炭辅助决策系统可以快速对信息进行处理和分析，做出农业宏观发展的趋势预测，并提供相应对策。农业信息技术无疑是政府有效管理农业的重要手段。

4.2 发展中国农业信息技术的对策

目前，中国农业信息技术应用与发达国家的总体差距还是比较明显的，且不考虑工业方面的差距，仅以工业为标准来看，美国农业信息化强度高于工业 81.6%，而中国农业信息化强度则低于工业 288.9%。要缩小这一差距，迎头赶上，必须在以下几个方面采取相应对策。

4.2.1 加强政府的扶持、引导和示范推广

国家和各级政府必须加强宏观调控和政策引导，营造有利于农业信息技术研究、开发与应用的良好环境，要实行统一规划、统一管理、统一协调，利用国家重大计划和省、市政府的重大（点）攻关任务，加大政府拨款力度，集中人力、财力、物力等资源，进行协作攻关，提高研究效率和水平。要在税收、信贷、基金、计划项目拨款、技术设备与人才引进等方面制定和完善相应的鼓励和扶持政策，吸引更多的企业和团体加入农业信息技术应用领域。要加大政府宣传和服务力度，搞好引导示范，总结推广智能化农业示范工程的成功经验，结合各地区实际，开辟新的农业信息技术应用示范工程，如面向农户服务的农业综合信息网络服务体系的研究与示范，以信息技术为依托的农业科技咨询推广服务体系研究与示范等。

4.2.2 发展农业信息技术教育和培训

推进农业信息化，农民观念意识是基础，人才是关键。必须坚持普及培训和学历教育两手抓的方针。一方面要充分发挥高等农业院校的作用，扩大本科、硕士、博士层次的农业信

 DOI: https://doi.org/10.36956/iser.v2i1.367

息人才培养。高等农业院校要根据农业信息人才知识结构的要求，调整专业设置，建立新的课程体系。对于农科学生，要加强计算机应用能力培养，并把现代信息技术融入其专业课程中。对于计算机、信息等专业的学生，要加强农业技术基础教育，并结合农业应用领域，开设定向应用课程，培养既懂现代信息技术又懂农业科学技术的复合型高级人才，充实农业信息技术研发队伍。另一方面，要搞好现有农技人员、各级干部和农民的农业信息技术普及培训。依托农业系统已建立多年、覆盖全国的 2700 所农业广播学校的农村广播、电视远程教育培训网络和新建农村远程教育培训系统，开展远程多媒体教学。利用“三下乡”“志愿者”等活动，宣传普及农业信息技术知识，改变农民的观念和意识，奠定农业信息化的思想基础。

4.2.3 注重农业信息技术基础建设

要充分借鉴美国、法国、日本等发达国家的经验，明确国家的主体投资地位，加强农业信息技术基础性建设。首先，要做好农业信息体系结构建设。对中国计划体制下建立的四级农技推广体系进行必要的机制改革。大力支持多种形式的社会化信息服务组织，如农村专业协会、信息咨询机构、科技示范点等。充实农村信息员队伍，完善信息采集渠道，设立信息技术研究保障基金，形成多层次的农业信息技术研究、开发、应用推广、咨询服务体系及其相应的管理和保障体系。其次，要加快信息基础设施建设，重点发展现代化的宽带、高速农业信息网络。按照“集中、统一、规范、效能”的原则，建设统一兼容、资源共享、高效适用的各级网络中枢平台环境，形成全国统一、规范、畅通的信息网络体系。此外，不仅要“修路”，还要“造车、备货”，要改变“重硬轻软”的状况，加大信息资源开发的投入力度，有计划、有组织地实施农业自然资源信息、农业科技资源信息、农业政策法规、农产品市场信息、人才资源信息、世界农业科技文献资源信息等各类信息资源的建设工程。

4.2.4 抓好重点农业信息技术项目的开发和应用

要重视农业信息技术的应用开发研究，包括软件基础研究，系统结构和数据库结构研究，信息新技术应用研究。进一步明确“抓应用，促发展”的思路，国家和地方政府科技部门应结合实际需要，有选择性地确定一批具有应用前景的技术研究项目。组织一定的研究力量实施开发和应用推广。这些项目主要包括：应用型农业专家系统，精细农业生产管理系统，农业资源、生态环境监测预报系统，设施农业生产控制系统，虚拟农业系统以及农业经济管理煤炭辅助决策系统等。要重视对单项农业信息技术的整合与集成，提高农信息技术项目研究水平。

参考文献

[1] 王人潮 . 中国农业信息技术的现状及其发展战略 [C]// 中国数字农业与农村信息化发展战略研讨会 .2003.

[2] 史岳鹏 , 王猛 . 我国农业信息化发展的现状与趋势 [J]. 河南农业 ,2005, (08):43.

[3] 李洪利 . 浅析中国农业信息化技术发展现状及存在的问题 [J]. 商品与质量 ,2019(19):9.

[4] 苏希 SU, Xi,Scientech, 等 . 农业信息技术的发展与应用前景 [J]. 计算机与农业 : 综合版 ,2003.

 DOI: https://doi.org/10.36956/iser.v2i1.368

Analysis on the Digitalization Risk and Management of Archives in the Big Data Environment

Fen Xie

Shandong College of Electronics Technology, Jinan, Shandong, 250200, China

Abstract

Based on the understanding and grasp of the relevant situation of archive digitization, the thesis first briefly introduces archive digitization, then summarizes the various risks that exist, and conducts a preliminary exploratory analysis of related risk management measures.

Keywords

archive digitization; risk management; risk prevention; archive management

大数据环境下的档案数字化风险与管理浅析

谢奋

山东电子职业技术学院，中国 · 山东 济南 250200

摘　要

基于对档案数字化的相关情况的了解和掌握，论文首先对档案数字化进行了简要介绍，而后总结出存在的种种风险，并对相关的风险管理措施进行了初步的探索性分析。

关键词

档案数字化；风险管理；风险防范；档案管理

1 档案数字化风险的相关概念

1.1 风险

由风险因素、风险事故和损失三者构成的统一体被称为风险。风险是指在一定条件下和一定时期内，损失发生的不确定性。风险具有客观性、普遍性、必然性、可识别性、可控性、损失性、不确定性。

1.2 风险因素

风险因素是指引起或增加安全风险事故发生的机会或扩大损失幅度的条件，是风险事故发生的潜在原因；风险因素是指增加风险事故发生的频率或严重程度的任何事件。构成风险因素的条件越多，发生损失的可能性就越大，损失就会越严重。

影响损失产生的可能性和程度的风险因素有两类：有形风险因素和无形风险因素。有形风险因素是指导致损失发生的物质方面的因素。无形风险因素即非物资形态的因素，也会影响损失发生的可能性和受损的程度。无形风险因素包括道德风险因素和行为风险因素两种。道德风险因素是指人们以不诚实、或不良企图、或欺诈行为故意促使风险事故发生，或扩大已发生的风险事故所造成的损失的因素。行为风险因素是指由于人们行为上的粗心大意和漠不关心，易于引发风险事故发生的机会和扩大损失程度的因素。

1.3 风险识别与风险因素分析

通过感性认识和历史经验来判断或通过对各种客观的资料和风险事故的记录来分析，归纳和整理，从而找出各种明显和潜在的风险及其损失规律。

风险因素分析是指对可能导致风险发生的因素进行评价分析，从而确定风险发生概率大小的风险评估方法。一般思路：调查风险源→识别风险转化条件→确定转化条件是否具备→估计风险发生的后果→风险评价。

数字化的风险识别与分析是对数字化工作过程中客观存在的各种风险进行系统的识别和归类。探讨风险因素的具体体现，剖析风险复杂多变的深层原因。数字化外包风险识别与分析贯穿在整个项目实施过程中的各个环节，风险识别与

 DOI: https://doi.org/10.36956/iser.v2i1.368

分析是风险管理的第一步，也是风险管理的基础。通过风险的认知或理解，可以帮助预测在档案数字化各个环节中可能发生的何种质量问题、安全问题，并由此研究制定相应的防范与处置办法。

档案数字化风险分析的信息来源。风险分析是建立在丰富的资料和数据基础之上的，因此通过多种途径采集相关信息是风险分析的关键，获取信息的途径包括本部门数字化经验总结归纳；邀请专家进行会议讨论、交流和咨询；对当前采取的数字化安全策略和相关文档进行复查；制作问卷，向有数字化工作经验的单位或有承揽经验的数字化加工企业进行调查；对相关人员进行访谈；进行实地考察等。

风险分析过程一些关键的问题需要考虑。首先，要确定数字化过程中核心保护的对象与直接和间接价值；其次，数字化项目实施过程中面临哪些潜在威胁，导致威胁的问题所在，威胁发生的可能性；第三，研究核心保护对象存在哪些弱点可能会被威胁所利用，利用的容易程度又如何；第四，一旦风险事件发生，会遭受怎样的损失或者面临怎样的负面影响；最后，应该采取怎样的安全措施才能将风险带来的损失降低到最低程度。解决以上问题的过程，就是风险分析的过程。

1.4 档案数字化风险

档案数字化风险是指档案数字化整个过程中在质量、安全等方面可能出现的风险因素，这些因素可能会影响档案数字化目标的实现。

档案数字化加工是新时期档案工作者面临的一项重要工作。此项工作周期长、任务重、要求严，并且在实施过程中存在着各种危及档案安全的因素 [1-2]。

2 档案数字化风险的特征与分类

2.1 档案数字化风险的特征

2.1.1 客观性

风险的客观性表现在风险是一种不以人的意志为转移，独立于人的意识之外的客观存在。因为无论是自然界的物质运动，还是社会发展的规律，都由事物的内部因素所决定，由超过人们主观意识所存在的客观规律所决定。例如地震、台风、意外事故等，都是不以人的意志为转移的客观存在。因此，人们只能在一定的时间和空间内改变风险存在和发生的条件，降低风险发生的频率和损失程度。但是，从总体上说，风险是不可能彻底消除的。同样档案数字化风险也是无法完全回避的客观存在，档案数字化过程中不可能百分百达到预期目标。唯有主动通过科学有效的科学管理活动和技术措施控制其发生概率或减少其损失程度。正是风险的客观存在，决定进行档案数字化风险管理研究和实践的必要性。

2.1.2 普遍性

虽然档案数字化风险通过最后的质检结论与预期的偏差表现出来，但这种偏差是由多方面的因素引起的，数字化活动的每一个环节都可能导致风险因素的产生，风险因素分布广泛，涉及技术、制度、人员素质、设备、流程、管理等多个方面，任何一个方面的不健全、不完备都可能导致风险发生。因此，对档案数字化风险的控制，也就取决于对上述各种风险的控制。

2.1.3 连带性

数字化风险所造成的损失是多方面的，并且可能环环相扣，具有“多米诺骨牌”效应，并且一些风险造成的损失当时是难以察觉，只有在特定时期才表现出来。以数字化实体为例，数字化前处理中如果造成档案实体缺损，如不完整、不可读、不真实等，表现损失是在后续提供利用时，形成提供历史、文化等不真实、不确切、不完整信息，造成的利用满意度下降、不信任等损失，且难以用经济价值衡量。

2.1.4 可管理性

档案数字化工作所面临主要风险并非当前科技手段和管理措施难预测和管控的，如地震、洪灾、战争等，只存在于一定的局限性条件下（如：扫描场所未禁止携带水杯、手机等个人物品，就存在档案被水浸泡和手机拍照泄密的风险），但需要主动识别和预防，绝大多数风险可以通过系列措施，进行监控和管理 [3]。

2.2 档案数字化风险的分类

将档案数字化过程中所面临的风险进行科学分类，帮助认识各种风险的具体特点，有针对性的应对。在研究当中，有人将档案数字化过程中面临的风险归纳为安全保密风险、真实性风险、完整性风险，在此基础上进一步指出还包括可读性风险、资金风险；也有人直接分为两类：数字档案真实性和完整性面临的风险（包括信息迁移带来的风险、人为修改带来的风险、网络攻击带来的风险）和数字信息无法永久读出；或者数字档案信息资源风险、数字化信息存储风险。此外，还有人指

 DOI: https://doi.org/10.36956/iser.v2i1.368

出档案数字化项目风险应该包括组织环境风险、人力资源风险、质量监督风险、档案安全风险、外部因素风险。

划分风险的标准有多种，如按照损失的呈现时间可以划分为当前风险、短期风险、长期风险；按照风险的可控性可以划分为可控风险、不可控风险；按照损失的严重性可以划分为轻度风险、一般风险、严重风险；按照数字化流程可以划分为准备阶段风险、前处理阶段风险、数字化处理阶段风险、检查验收阶段风险；按照风险的影响方式可以划分为直接风险和间接风险等 [4]。

3 档案数字化风险管理的宗旨

档案数字化风险管理是将贯穿在整个项目实施过程各个环节中客观存在的各种风险进行系统的分析、识别、认识和归类，探讨风险因素的具体形式，剖析风险复杂多变的深层原因，明确风险管理的宗旨，明确风险管理的任务要求，采取相应措施，防范和控制各类风险的出现，确保档案及其信息的安全。根据风险的来源，结合数字化流程，以档案管理角度为出发点，形成项目风险列表，列出档案数字化外包工作流程中，可能出现威胁档案安全的因素以及可能造成的风险后果，建立科学的综合风险管理体系和具体的风险控制方法。档案数字化风险管理可以为开展数字化项目的决策者做出理性、客观、科学的安全管理决策提供依据，从而建立风险管理体系，避免出现重大决策失误和安全事故 [5]。

4 档案数字化风险管理的基本原则

4.1 事前管理、主动防御原则

最好的风险管理就是预防风险的发生。事前分析各种安全风险，采取全面防范、主动防御的办法建立起预警、保护、检测、反应、恢复的闭环反馈，主动发现和及时消除安全隐患，才能将各种安全危险“拒之门外”，提前防范和化解各种风险。从风险分析出发，及时预测和适应环境与技术的变化，并随环境与技术的变化主动采取各种防御措施，构建起整体的、动态的信息安全防御体系。

4.2 稳定协调、均衡防护原则

稳定协调、均衡防护原则要求确保各部分的风险防范水平基本一致，无明显薄弱环节或“瓶颈”。档案数字化是流程化的系统工程，包含数字化工作组织、各个加工阶段、数字化成果管理等多个工作环节，存在着多种风险因素，因风险因素间具有连带性和延续性，某个环节风险一旦发生，其他环节风险防范也无济于事。例如，在数字化扫描过程中纸质档案实体被人为恶意篡改，则后续图像处理、质检、保存各个环节风险防范如何严密，都无法改变档案受损的事实，后续严重的危害还将继续发生下去。

只有从基础设施、工作环境、系统功能抓起，全员、全面、全过程强化安全，保证各个环节风险防范都严密，没有“木桶效应”的短板，形成统一协调、责任明确、齐抓共管的态势，才能形成立体、全方位的档案数字化项目的整体安全 [6]。

4.3 适当防御、重视成本效益原则

这里的成本效益原则中的成本，是指数字化项目实施风险管理措施所要投入的时间成本、人力成本、设备成本、资金等。效益则是指资源（成本）投入所达到任务的成效。

安全管理应该实事求是，避免急于求成、铺张浪费脱离实际，造成不必要的资源浪费。确切分析各种风险事故发生的概率及其可能造成的损害，根据档案的实际价值及其风险系数确定防御。要有科学的规划和评估，从“投入”与“产出”的对比分析来看待“投入”（成本）的必要性、合理性，抓住防御重点，减少安全系统的规模和复杂性，提高系统的运行性能，即努力以尽可能少的成本付出，创造尽可能多的使用价值。

同时，档案数字化风险管理也是缜密、谨慎的工程，并非动辄以遵循成本效益原则为由简化风险管理的程序，即使确实需要运用成本效益原则也必须有必要的分析和论证。有时虽然要增加一定的费用开支，但能获取长期的效果。如：购置一台多功能智能监控设备或增加一套信息安全管理软件，较之其他功能单一设备需要增加开支，但因此可节省其他设备购置、维护费用，提高设备效率和安全系数，从而提高了风险管理的综合防御能力。因此这种成本观念可以说是“花钱是为了省钱”，都是成本效益观的体现 [7]。

5 档案数字化风险管理存在的问题

各级档案行政管理机构加强了数字化的监督、指导、检查工作，许多档案部门和档案数字化加工部门在组织实施档案数字化过程中设立专门机构和人员并且建章立制，通过培训教育、专项检查、签订协议、完善设施设备、加强日常管理等工作，进一步加强了档案数字化的风险防范与管理。

 DOI: https://doi.org/10.36956/iser.v2i1.368

虽然各级档案部门在档案数字化实施过程中都比较重视档案实体及其信息的安全问题，但总体上还存在着以下几个主要问题：

5.1 相关法规、标准不健全

由于相关标准还不够健全，很多工作缺少操作规范，同时中国对档案信息数字化方面的理论研究甚少，相关文献很有限，在业界也缺少系统可靠的理论指导和技术支撑。特别是涉及档案数字化过程中的安全管理、风险控制等相关规范及标准尚未建立，难以指导和规范档案数字化的安全管理工作。

5.2 风险管理意识淡漠

档案的安全管理与保护极其重要，业界已经认识到档案数字化过程中风险管理的重要性，但在实际数字化工作中相关风险管理研究还缺乏系统性，对潜在风险的评估和预警管理相对滞后，风险管理在实践中的应用不够，风险管理多为事后控制，缺乏主动性，缺乏风险管理整体策略。无论是组织档案数字化建设的档案部门还是数字化加工承揽企业方，风险意识都相对淡薄，风险管理制度不完善，特别是在风险管理控制、风险评估以及预警机制等方面的管理水平尚待提高 [8]。

5.3 忽视数字化安全风险管控工作

近年来，在档案部门大力推进档案数字化工作的过程中，档案信息安全隐患日益凸显，风险积聚。随着越来越多的档案部门开展档案数字化外包，在实施过程中各种档案安全风险正在不断叠加，将给档案管理造成较大损失，也带来较严重的社会影响。

参考文献

[1] 唐燕 . 浅析档案数字化项目的风险 [J]. 兰台世界 ,2011(21):63−64.

[2] 韩一静 . 档案数字化的风险及防范 [J]. 兰台世界 ,2009(2):23−24.

[3] 刘玉红 . 档案数字化项目风险问题研究 [J]. 黑龙江档案 ,2012(01):60.

[4] 万军 . 试论档案数字化风险与应对 [J]. 科技创新导报 ,2018,015(015):152+154.

[5] 李建朋 . 档案数字化面临的风险及其防控 [J]. 四川档案 ,2011(02):20−23.

[6] 朱丽梅 . 馆藏档案数字化风险应对研究 [J]. 档案与建设 ,2013(09):18−21.

[7] 张璐 . 浅谈档案数字化过程中的风险和对策 [J]. 机电兵船档案 ,2020,208(03):77−79.

[8] 谈胜祥 . 档案数字化风险警示与对策 [J]. 中国档案 ,2016(04):62−63.

 DOI: https://doi.org/10.36956/iser.v2i1.369

Analysis of Computer Network Security Technology

Chaofan Wu

Fujian Normal University, Fuqing, Fujian, 350300, China

Abstract

Based on the introduction of computer network security overview, the paper analyzes the reasons and methods of computer network security threats, and proposes preventive measures for computer network security.

Keywords

computer network; network security; prevention

计算机网络安全技术浅析

吴超凡

福建师范大学，中国 · 福建 福清 350300

摘　要

论文在介绍计算机网络安全概述的基础上，分析了计算机网络安全威胁产生的原因及方式，提出了计算机网络安全的防范措施。

关键词

计算机网络；网络安全；防范

1 计算机网络的潜在安全隐患

电子商务的网络环境包括 Intranet、Extranet、Internet 三种结构组成的网络环境，电子商务的网络安全涉及网络环境的各个方面。

企业内部的典型风险有：没有好的备份系统导致数据丢失；有外来磁盘携带的病毒攻击计算机系统；业务人员的误操作；删除了不该删除的数据，且无法恢复；系统硬件、通信网络或软件本身出故障。

如果企业的内部网连接上 Internet，则 Internet 本身的不安全性对企业内部信息系统带来的潜在风险主要有：外部非法用户潜入系统胡作非为，甚至破坏系统；数据丢失，机密信息泄漏；互联网本身固有的风险的影响；网络病毒的攻击。

Internet 的安全问题的主要原因之一在于 TCP/IP 和 UDP 的基本体系结构。

2 计算机网络安全体系

一个全方位的计算机网络安全体系包含网络的物理安全、访问控制安全、系统安全、用户安全、信息加密、安全传输和管理安全等。

在实施网络安全防范措施时应考虑以下几点：要加强主机本身的安全，做好安全配置，及时安装安全补丁程序，减少漏洞；要用各种系统漏洞检测软件定期对网络系统进行扫描分析，找出可能存在的安全隐患，及时修补；对敏感的设备和数据要建立必要的物理或逻辑隔离措施；安装防病毒软件，加强内部网的整体防病毒措施；建立详细的安全审计日志，以便检测并跟踪入侵攻击等。

3 常用的计算机网络安全技术

目前，常用的计算机网络安全技术主要有病毒防范技术、身份认证技术、防火墙技术和虚拟专用网 VPN 技术等。

3.1 病毒及黑客防范技术

计算机病毒是带有一段恶意指令的程序，一旦用户运行了被病毒感染的程序，它就会隐藏在系统中不断感染内存或硬盘上的程序。

黑客程序实际上是人们编写的程序，它能够控制和操纵远程计算机，一般由本地和远程两部分程序组成。考虑到黑

 DOI: https://doi.org/10.36956/iser.v2i1.369

客程序的危害性，把黑客程序也归于计算机病毒。

3.1.1 单机病毒

（1）单机病毒的种类

单机病毒就是以前的 DOS 病毒、Windows 病毒和能在多操作系统下运行的宏病毒。

DOS 病毒是在 MS-DOS 及其兼容操作系统上编写的病毒程序，例如以前著名的“黑色星期五”“DIR”等病毒。

Windows 病毒是在 Win3.x/Win9.x 上编写的纯 32 位病毒，例如 4 月 26 日危害全球的 CIH 病毒等。

宏病毒是利用 Office 特有的“宏”编写的病毒，它专门攻击微软 Office 系列 Word 和 Excel 文件。这种病毒不仅能运行在 Windows 环境，还能运行在 OS/2 或 MAC OS 上的微软 Office 软件中。例如“七月杀手”宏病毒，会在七月的任一天发作，发作时弹出“醒世恒言”对话框，要求用户选择“确定”或“取消”，如果按了“取消”，就会在 autoexec.bat 中增加一条删除 C 盘的命令，重新开机时，就会删除 C 盘上的全部数据。

（2）单机病毒的防范

考虑到每种杀毒产品都有其局限性，所以最好准备几套杀毒软件，用它们来交叉杀毒，杀毒软件还要及时升级；定期用杀毒软件检查硬盘，如果用的是 Win9.x（CIH 病毒对 WINNT 和 WIN2000 不起作用），每月的 26 号前一定要检查是否有 CIH 病毒，或者将系统日期跳过 26 号。C 盘最好是 FAT32 格式，容量大于 2G，这样设置的好处是，有利于提高系统运行速度，此外如果 C 盘被 CIH 病毒破坏了，只要它是 FAT32 格式，且容量大于 2G，用一般杀毒软件就可以将 C 盘上的数据恢复 98%。

CIH 病毒至少有 9 个变种，其中 V1.2 和 V1.3 在 4 月 26 号发作，V1.4 在每月的 26 号发作，还有的版本发作日期在 6 月 26 号。

3.1.2 网络病毒及其防范

网络病毒通常是指特洛伊木马和邮件病毒，因为是通过网络传播的，所以称为“网络病毒”。

（1）特洛伊木马病毒

特洛伊木马是一种黑客程序，与病毒有些区别，特洛伊木马本身一般并不破坏受害者硬盘上的数据，它只悄悄地潜伏在被感染的计算机里，一旦这台计算机上网，就可能大祸临头。木马、黑客病毒往往是成对出现的，即木马病毒负责侵入用户的电脑，而黑客病毒则会通过该木马病毒来进行控制。现在这两种类型都越来越趋向于整合了，一般的木马如 QQ 消息尾巴木马 Trojan.QQ3344，还有针对网络游戏的木马病毒如 Trojan.mir.PSW.60。值得注意的是，病毒名中有 PSW 或者什么 PWD 之类的一般都表示这个病毒有盗取密码的功能（这些字母一般都为“密码”的英文“password”的缩写）一些黑客程序有：网络枭雄（Hack.Nether.Client）等。

特洛伊木马病毒的防范方法是：不要轻易泄漏 IP 地址，下载来历不明的软件时要警惕其中是否隐藏了特洛伊木马，使用下载软件前一定要用特洛伊木马检测工具进行检查。

（2）邮件病毒

邮件病毒和普通病毒是一样的，只不过由于它们主要通过电子邮件传播，所以才称为“邮件病毒”，一般通过邮件中“附件”夹带的方法进行扩散，一旦你收到这类 E-mail，运行了附件中的病毒程序，就能使你的计算机染毒。这类病毒本身的代码并不复杂，比如 I love you 病毒，只要收到带有该病毒的 E-mail 并打开附件后，病毒就会按照脚本指令，将浏览器自动连接上一个网址，下载特洛伊木马程序，更改一些文件后缀为 .vbs，最后再把病毒自动发给 Outlook 通信薄中的每个人。

还有一个恶作剧，有人用 VBScript 编写了一个 HTML 文件，代码如下：

```
<script language="VBScript">
Dim WSHShell
Set WSHShell=CreateObject（wscript.Shell）
WSHShell.run（“c：\fbrmatd：”）
</script>
```

只要打开该网页，D 盘就被格式化了。预防办法是禁止 HTML 中脚本的运行（在浏览器的“工具 /Internet 选项 / 安全”中设置禁止 Java 或 Active X 的运行），当 IE 提示“该网页上的某个软件可能不安全，建议不要运行。

邮件病毒的防范方法是：不要打开陌生人来信中的附件，特别是“.exe”等可执行文件；养成用最新杀毒软件及时查毒的好习惯，不要急于打开附件中的文件，先将其保存在特定目录中，然后用杀毒软件进行检查；收到自认为有趣的邮件时，不要盲目转发，因为这样会帮助病毒的传播；对于通过脚本“工作”的病毒，可采用在浏览器中禁止 Java 或 Active X 运行的方法来阻止病毒的发作。

 DOI: https://doi.org/10.36956/iser.v2i1.369

（3）脚本病毒

脚本病毒的前缀是：Script。脚本病毒的共有特性是使用脚本语言编写，通过网页进行传播的病毒，如红色代码（Script.Redlof）o 脚本病毒还会有如下前缀：VBS、JS（表明是何种脚本编写的），如欢乐时光（VBS.Happytime）、十四日（Js.Fortnight.c.s）等。

（4）蠕虫病毒

蠕虫病毒的前缀是：worm 这种病毒的共有特性是通过网络或者系统漏洞进行传播，很大部分的蠕虫病毒都有向外发送带毒邮件，阻塞网络的特性。比如冲击波（阻塞网络）、小邮差（发带毒邮件）等 [1]。

3.1.3 网上炸弹及其防范

（1）IP 炸弹

IP 炸弹一般是指用专用的攻击软件（如 WinNuke、IGMPNuke 等）发送大量的特殊数据，对远程计算机中的 Windows 系统的漏洞进行攻击，造成对方的 Windows 蓝屏死机。当用户在聊天室聊天时，其 1P 地址很容易被别人查到，如果对方要发起攻击，只要用专用软件攻击用户的 IP 就可以了。

对付 IP 炸弹最好的办法是安装个人防火墙。个人防火墙实际上是一套程序，即对进出计算机的所有数据进行分析，切断非法连接。使用个人防火墙前一般要进行系统设置，进行“安全规则设置”。

（2）邮件炸弹

邮件炸弹的原理是向有限容量的信箱投入足够多或者足够大的邮件，使邮箱崩溃。这类炸弹很多，如 Nimingxin，Quickfyre mair Emailbomb、Upyours 系列、雪崩等。

防范邮件炸弹的方法有以下几种：①在邮件软件中设置好防范项目；②在邮件服务器上设置过滤器，防范邮件炸弹；③使用删除 E-mail 炸弹的工具；④谨慎使用自动回信。

3.2 身份识别技术

身份识别技术的基本思想是通过验证被认证对象的属性来达到确认被认证对象是否真实有效的目的。被认证对象的属性可以是口令、问题解答或者指纹、声音等生理特征，常用的认证技术有口令、标记法和生物特征法。

3.2.1 口令

传统的认证技术主要采用基于口令的认证方法。当被认证对象要求访问提供服务的系统时，提供服务的认证方要求被认证对象提交该对象的口令，认证方收到口令后，将其与系统中存储的用户口令进行比较，以确认被认证对象是否为合法访问者。

一般的系统都提供了对口令认证的支持，对于封闭的小型系统来说不失为一种简单可行的方法。

但是，传统的认证技术也有一些不足之处。用户每次访问系统时都要以明文方式输入口令，很容易泄漏；口令在传输过程中可能被截获；系统中所有用户的口令以文件形式存储在认证方，攻击者可以利用系统中存在的漏洞获取系统的口令文件；用户在访问多个不同安全级别的系统时，都要求用户提供口令，用户为了记忆的方便，往往采用相同的口令；只能进行单向认证，即系统可以认证用户，而用户无法对系统进行认证。

3.2.2 标记方法

标记是个人持有物，作用类似于钥匙，标记上记录着用于机器识别的个人信息。常用的标记有磁介质、智能卡。

3.2.3 生物特征法

每个人都有唯一且稳定的特征，如指纹、眼睛以及说话和书写等做事的标准方法。生物特征法是基于物理特征或行为特征自动识别人员的一种方法，其优点是严格依据人的物理特征并且不依赖任何迸被拷贝的文件或可被破解的口令，所以它是数字证书或智能卡的选择 [2]。

3.3 防火墙技术

3.3.1 防火墙概述

（1）防火墙的概念

防火墙是指一个由软件和硬件设备组合而成，处于企业或网络群体计算机与外界通道（Internet）之间，在内部网与外部网之间实施安全防范的系统，可被认为是一种访问控制机制，用于限制外界用户对内部网络访问及管理内部用户访问外界网络的权限，即确定哪些内部服务允许外部访问，以及允许哪些外部访问访问内部服务。

（2）防火墙的设计原则

防火墙的设计有以下两个原则：

第一，一切未被允许的就是禁止的。基于该准则，防火墙应封锁所有信息流，然后对希望提供的服务逐项开放，只有经过精挑细选的服务才被允许使用。其弊端是安全性高于

 DOI: https://doi.org/10.36956/iser.v2i1.369

用户使用的方便性，用户所能使用的服务范围受到很大限制。

第二，一切未被禁止的就是允许的。基于该准则，防火墙应转发所有信息流，然后逐项屏蔽可能有害的服务，从而可为用户提供更多的服务。其弊端是在日益增多的网络服务面前，网管人员疲于奔命，特别是受保护的网络范围增大时，很难提供可靠的安全防护。

（3）防火墙的实现技术

按照建立防火墙的主要途径，防火墙的实现技术可分为分组过滤、代理服务和应用网关。分组过滤技术是一种简单、有效的安全控制技术，它通过在网络间相互连接的设备上加载允许、禁止来自某些特定的源地址、目的地址、TCP 端口号等规则，对通过设备的数据包进行检查，限制数据包进出内部网络。分组过滤技术的最大优点是对用户透明，传输性能高。但由于安全控制层次在网络层和传输层，其安全控制的力度只限于源地址、目的地址和端口号，因而只能进行较为初步的安全控制，对于恶意的拥塞攻击、内存覆盖攻击或病毒等高层次的攻击手段则无能为力。

代理服务是运行于内部网络与外部网络之间的主机之上的一种应用。当用户需要访问代理服务器另一侧主机时，对符合安全规则的连接，代理服务器会代替主机响应，并重新向主机发出一个相同的请求。当此连接请求得到回应并建立起连接后，内部主机同外部主机之间的通信将通过代理程序将相应连接映射来实现。对于用户而言，似乎是直接与外部网络相连的，代理服务器对用户透明。由于给予代理服务的防火墙是在应用层实现的，所有它提供了较高的安全性和较强的身份验证功能。但是其透明性差，也离不开用户的合作。同时，它对网络性能的影响也较大。

应用网关技术是建立在网络应用层上的协议过滤，它针对特别的网络应用服务协议，即数据包分析并形成相关的报告。

3.1.2 防火墙的原理

防火墙是在专用网（Intranet）和 Internet 之间设置的安全系统，可以提供接入控制，可以干预这两个网络之间的任何消息传送。

（1）防火墙设计的基本原则

防火墙设计需要满足的基本原则如下：

①由内到外，或由外到内的业务流均经过防火墙；②只允许本地安全策略认可的业务流程通过防火墙；③尽可能控制外部用户访问专用网，应当严格限制外部人员进入专用网中；④具有足够的透明性，保证正常业务流通；⑤具有抗穿透攻击能力，强化记录、审计和报警功能。

（2）防火墙的组成

防火墙主要由 5 部分组成：即安全操作系统、过滤器、网关、域名服务和 E−mail 处理。有的防火墙可能在网关两侧设置内外过滤器。外过滤器保护网关不受攻击，而内过滤器在网关被攻破后提供对内部网络的保护。

安全操作系统可以保护防火墙的代码和文件免遭入侵者攻击；过滤器则执行由防火墙管理机构制定的一组规则，检验各数据组决定是否允许运行；应用网关可以在 TCP/IP 应用级上控制信息流和认证用户；域名访问使专用网的域名与 Internet 相隔离，专用网中主机的内部 IP 地址不至于暴露给 Internet 中的用户；函件处理能力保证专用网中用户和 Internet 用户之间的任何函件交换都必须经过防火墙处理。

（3）防火墙不能对付的安全威胁

首先，防火墙不能防止专用网内部用户对资源的攻击，它只是设在专用网和 Internet 之间，对其间的信息流进行干预的安全设施。

其次，如果专用网中有些资源绕过防火墙直接与 Internet 连通，则得不到防火墙的保护。

另外，从病毒防护来看，一般防火墙不对专用网提供防护外部病毒的侵犯。

（4）防火墙的分类

①分组过滤网关，按源地址和目的地址或业务（即端口号）卸包（组），并根据当前组的内容做出决定。管理者拟定一个提供接收和服务对象的清单，一个不接受访问或服务对象的清单，按所定安全政策实施允许或拒绝访问。

②应用级网关，在专用网和外部网之间建立一个单独的子网，它将内部网屏蔽起来。此子网有一个代理主机、一个路由器和一个较复杂的网关与内部网相连，另一个路由器和网关与外部相连。进出用户通过网关时必须在应用级上（要求特定的用户程序或用户接口）与代理主机连接 [3]。

③线路级网关，它使内部与外部网之间实现中继 TCP 连接。

3.1.3 防火墙产品

防火墙产品的用户主要分为个人用户、企业用户和政府部门用户。个人用户的安全需求基本上局限于防止网络病毒

 DOI: https://doi.org/10.36956/iser.v2i1.369

和“邮件炸弹”，一般的单机防火墙软件就能满足需求，而企业级用户和政府部门用户是安全产品最重要的应用对象。

（1）Checkpoint Firewall−1

Checkpoint 公司是一家专门措施网络安全产品开发的公司，是软件防火墙领域中的佼佼者，其旗舰产品 Checkpoint Firewall−1 在全球软件防火墙产品中位居第一。Checkpoint Firewall−1 是一个综合的、模块化的安全套件，它是一个基于策略的解决方案，提供集中管理、访问控制、授权、加密、网络地址传输、内容显示负载平衡等功能。其主要用在保护内部网络资源、保护内部进程资源和内部网络访问者验证等领域。

（2）Sonicwall 系列防火墙

Sonicwall 系列防火墙是 Sonic System 公司针对中小型企业需求开发的产品，并以其高性能和极具竞争力的价格受到中小企业和 ISP 公司的青睐 [4]。

（3）NetScreen 防火墙

NetScreen 公司推出的 NetScreen 防火墙是一种新型的网络安全硬件产品，把多种功能诸如流量控制、负载均衡、VPN 等集成到一起，优势在于采用了新的体系结构，可以有效地消除传统防火墙实现数据加盟时的性能瓶颈，能实现最高级别的 IP 安全保护。

（4）Alkatel intent Deices 系列防火墙

1999 年 6 月，阿尔卡特公司与 intent Deices 经过谈判达成协议，以 1.8 亿美元巨资收购 intent Deices 公司——一个业界具有重要地位的防火墙和 VPN 解决方案供应商。intent Deices 公司专门从事高性能计算机网络安全系统的设计、开发、销售和服务，其产品系列 intent Deices 1000/3000/5000 和 intent Deices 10K 分别适用于小型、中型、大型网络环境。其 中 intent Deices 3000>intent Deices 5000 及 intent Deices 10K 带有 VPN 功能，支持 VPN 用户。

（5）NAIGauntlet 防火墙

NAI 公司是全球著名的网络安全产品提供商，其产品包括网络检测、防火墙以及防病毒产品等。

3.4 虚拟专用网技术

虚拟专用网是用于 Internet 电子交易的一种专用网络，它可以在两个系统之间建立安全的通道，非常适合电子数据交换。在虚拟专用网中交易双方比较熟悉，而且彼此之间的数据通信量很大。只要交易双方取得一致，在虚拟专用网中就可以使用比较复杂的专用加密和认证技术，这样可以大大提高电子商务的安全性。

参考文献

[1] 庄建忠 . 计算机网络安全技术及策略浅析 [J]. 农业网络信息 ,2007 (08):91−93.

[2] 王宇光 . 计算机网络安全技术浅谈 [J]. 科技传播 ,2015,007 (021):114−115.

[3] 仉琦 , 缪超 , 张辉 . 计算机网络安全技术的影响因素与防范措施 [J]. 电脑迷 ,2017 (012):17.

[4] 罗小珠 . 浅析计算机网络安全的管理技术 [C]// 网络安全技术的开发应用学术会议论文集 .2002.

INFORMATION SCIENCE AND ENGINEERING RESEARCH

Nanyang Academy of Sciences Pte. Ltd.
Tel.:+65 65881289
E-mail:contact@nassg.org
Add.:12 Eu Tong Sen Street #07-169 Singapore 059819