中国图书馆学报(双月刊)1995 年第 1 期
ZHONGGUO TUSHUGUANXUEBAO

张晓源

论图书馆自动化系统的安全管理

ABSTRACT Dangerous factors that threaten the safety operation of automated library system are mainly from natural calamity, man-made inroads, environmental impact as well as poor management. Close attentions should be paid to these when the system is first set up.

SUBJECT TERMS Library automation--Safety management
CLASS NUMBER G258.94

目前,我国图书馆自动化建设已进入新阶段。仅以广东省为例,到 1993 年底,有近 30 家公共馆、40 家高校馆全面或部分实现了计算机管理。这两大系统的图书馆共拥有中小型、微型计算机和终端超过 700 台。已开发成功 3 种各具特色的图书馆自动化集成系统:中山图书馆的 **ZSLIAS**,深圳图书馆的 **ILAS** 和深圳大学的 **SULCMIS**;还有若干专门系统,如广州图书馆和深圳图书馆合作开发的视听资料管理系统(**AMMS**)。中山图书馆与佛山图书馆、石湾图书馆,深圳图书馆与蛇口图书馆的联网试验都分别获得成功。建立了若干数据库,如深圳图书馆等合作建立的 1985～1991 年中文图书数据库。1993 年 10 月,在佛山召开的广东省部分公共图书馆计算机联网会议,揭开了图书馆省级计算机联网的序幕。

1 图书馆自动化系统出现的安全问题

随着自动化系统在图书馆的普及和计算机联网,许多图书馆的自动化系统发生过各种故障和事故,有的甚至破坏了整个系统,造成巨大损失。例如:某省馆计算机系统硬盘出现故障先兆,经过售后服务部门检测后决定更换一个新硬盘。结果故障排除了,却发现由于更换硬盘而使近两个月的采编数据全部丢失,又没有任何磁带、磁盘备份可以补救。某市馆的流通子系统的借还功能块一天突然锁起,经检查,原因是某位流通管理员未经授权就私自利用读者管理用户权限进入该子系统的验证功能菜单并运行了这一功能。系统管理员虽发现并适当处理,但系统已给数千读者数据强制核证,停止了这些读者的借书权。某省馆安排一位大学毕业生负责开发某系统。3 年后,该人自动离职。经检查才发现,系统的原程序已支离破碎,所谓开发的新系统根本无法运行。

图书馆自动化系统安全问题有 3 种类型:系统被破坏、系统被非法使用、信息泄漏和丢失。必须实行和不断强化对自动化系统的安全管理,确保系统的正常运行。

2 安全问题来自图书馆自动化系统的脆弱性

作为高科技的图书馆自动化系统，会出现诸多安全问题是由图书馆自动化系统本身的脆弱性造成的。具体表现为：

计算机硬件虽然具有较高的可靠性，但这只能减少产品初期故障和推迟损耗故障的出现，而运行中的偶发故障是始终存在的。就计算机的制造过程来说，目前国内外市场存在多种类型：有原装和非原装、名牌机和杂牌机之分。非原版组装和杂牌，无论在零件、生产工艺、测试手段、质量控制等方面，还是在机器性能、使用寿命、维修服务等方面，都明显逊色。另外，整个硬件系统是由无数的电子元件组成的，其整体系统的可靠性依赖于全部元件的可靠性。即使单个元件有很低的故障率，系统整体出现故障的可能性仍会相对高。所有的硬件，基本上是高精密的电子、机械设备，对运行环境及负荷都有较严格的要求。如果环境条件差，或者超负荷工作，也会引起故障率增加。

计算机软件基本上属于树表加工系统，树表可以反映纵向的关系与属性，但难以控制横向侵入。目前国内图书馆自动化软件系统的开发者，对图书馆业务有较深认识，对软件业务功能的完善性较为重视，而对系统的安全性，则认识不够，软件设计中防止误操作、防止非法入侵的措施不足，缺乏完善的安全保护功能。各种计算机病毒的出现及流行，亦给软件带来很大的危害。

现代数据处理技术日趋复杂化，其特点是大批量、集中共享和联机。网络的普及、信息资源的共享性、软件和硬件知识的透明度、计算机使用方法的通用性，使系统在具有很强功能的同时，也有许多易被攻击的地方，为各种入侵创造了条件。

自动化对于大多数图书馆来说是新事物，普遍存在一个从认识、学习到掌握、熟悉的过程。各种人为失误都会出现，包括系统组成的各个部分，如系统规划、硬件选购、规范制度、人员管制等。这将形成很多危害系统安全的薄弱环节。

3 安全管理的概念和对象

图书馆自动化系统的安全管理，是指作为系统使用者的图书馆，针对威胁系统安全的种种危险因素和系统的薄弱环节，从系统设计、设备配置、软件程序、系统运行环境、人员的专业素质和职业道德、工作组织和岗位设置、规章制度、法律到社会环境等各个方面，采取规划、控制等一系列管理手段和措施，防止对自动化系统有意和无意的、人为和自然的任何形式的破坏、非法使用和信息泄漏，以及保障当系统遭到破坏后迅速恢复正常运行。

安全管理的对象包括与图书馆自动化系统有关的全部因素：硬件设备、操作系统、应用软件、系统环境、各种使用者（自动化专业人员、操作人员、数据录入人员）、各种数据源（磁带、磁盘、输出输入记录等）、管理人员（馆领导、系统管理人员、数据管理人员）、读者、非法入侵者和各种灾害。

4 影响系统安全的主要危险因素

由于系统所存在的脆弱性，使之很容易受到各方面危险因素的攻击。这些危险因素主要有：

自然危险因素。包括火灾、地震、水灾、雷击、动物入侵、盐雾、尘灾、风灾等。

人为危险因素。包括各种非法入侵、盗窃、破坏、操作失误、岗位素质不足、缺乏安全观念、职业道德水平低等。

管理危险因素。包括各种制度规范不健全、缺乏应急措施、实际管理不善、缺乏检查监督及有关岗位、有关法律不健全等。

硬件危险因素。包括设计配置不良、运行中逻辑出错、维护不善、维修不及时、零配件供应不足、通讯线路故障等。

软件数据危险因素。包括系统设计不良、缺乏安全控制功能、代码错、说明书错、数据错等。

环境危险因素。包括电气故障(电源质量差、停电、静电影响、磁场影响)、机房设计不当、机房辅助设备故障等。

5 安全管理的基本原则

通过对许多故障事故的分析,笔者认为,安全管理应该着重注意以下5个基本原则。

5.1 整体管理原则

安全管理的对象应该包括与自动化系统有关的全部因素。安全管理的实施过程应该包括系统生命周期中的全部阶段。例如在系统规划、方案实施、硬件配置、软件设计和程序开发、使用培训、系统运行等阶段,都必须实施安全管理。作为安全管理的责任者,应包括馆内与系统有关的全部人员。不单负责监督的人有责任,而是人人都要有安全管理的观念,谁主管谁负责,谁上岗谁负责。

5.2 预防为主原则

采取预防措施尤为重要。例如硬件系统的结构是否采用双机工作方式,应用软件是否采用分级用户控制等,最好在系统设计阶段,就有一个全面的考虑。预防的重点,一是系统设计。要求所设计的系统的行为是可以预测的。即在系统正常运行及出现故障时,人们能预测出系统对每个外来作用的响应。例如在应用软件中应有完善的防误操作功能,当发生误操作时,系统能发出相应的信息,提醒人们。二是要有计划、制度和应急方案。计划、制度和应急方案的制定应永远走在前面。建立图书馆自动化系统的同时,就应开始制定针对系统运行时可能出现的漏洞,预先制定出应急措施及工作人员的行为规范和操作规程。象"数据管理计划"、"事故处理堆积"、"系统恢复程序"都应事先筹划好。三是要确立工作岗位。注意对系统工作实行"任务划分"。象操作、核实、监督等任务,必须事先安排由多人分管。特别是某项活动的发起与批准或软件系统的开发应尽量避免交由一二个人来负责掌管。四是对系统中的关键部分、影响全局的部分,应该事先备份。如硬件应采用双机工作方式、廉价磁盘冗余阵列等;数据应每天进行磁带备份、操作实时打印等,并把重要的磁带和磁盘,一式二份分开存放在不同地点。

5.3 分级控制原则

系统应是可控制的,需要建立严格的分级控制体系。这样就意味着,只让那些需要的而又符合系统安全要求的东西传到其他部分去。控制的级别越高,管辖的范围越广,级别越低,操作越细致越具体。这样做,无论从宏观上还是从微观上都可以把整个系统置于控制之下。例如:——权限控制。就是给不同级别的用户或系统操作管理人员授予大小不等的权限。如流通管理员只能使用借还书部分的功能,但系统管理员却不一定有权去修改系统的程序,这部分的权力则只有系统程序员或主程序员才拥有。改变终端的物理联接,只有通过硬件系统员才能进行。调动设备,必须由馆领导决定。无论要发出什么级别的权限,有一点十分重要,这就是每一个权限的发出必须审慎,而且,只能给予用户最低限度的特权。

——功能控制。这是与权限控制配套的。系统每个部分,只能具有单一功能。如读者子系统,就不应具有采编功能。

——数据控制。数据控制包括:规定各种数据使用的标准和规范;限定各种数据的使用范围;确定各种数据的保密级别;严格控制数据的更改。

——人机接口控制。谁能联接到系统中来并能干些什么事,系统管理员都能从硬件、软件、数据等方面加以控制。

5.4 实时记录原则

实时记录,指必须随时把系统所发生的每一个有意义的活动记录下来。例如:软件程

序开发过程中需要把程序的每个修改版都打印出来；系统运行中需把每个用户的进入退出及工作情况等数据随时登记在磁盘的日志文件上。在硬件购进时，需要马上建立设备财产档案、工作档案和维修档案。在系统管理方面，系统员每天应按时填写工作日记。等等。

一个完善的系统，应该具有完备的实时记录机制。这样做可为改造、后援、补救工作提供资料；便于追踪和识别，确定责任；可以查看发生了什么事情。

记录可以采用多种载体形式，如书面文字形式、磁记录形式，可以由人来记录，也可由程序/机器自动进行。无论哪种实时记录机制，都应该为系统保留下最完整齐全的现场数据，所有工作数据都应得到保护。

5.5 监督原则

监督机制在图书馆自动化系统的整个生命周期内应始终存在。首先应对硬件和软件本身具有监督的功能，也就是说，系统的硬、软件应设置有监测部件/程序，随时监测着自身的运行状态。当出现异常现象时，必须能立刻检测出来，自动地加以适当处理，或报警引起管理人员注意。其次，必须设置一些监督组织和配备负责监督的人员，制定相应的监督制度或规程。要有人去检查记录，有人去监测业务活动。

6 安全防护结构

针对各种危害，图书馆自动化系统安全管理的防护结构，应该有5个安全防护层。

法律和社会管理防护层是利用法律、社会公共安全、社会教育、宣传舆论、社会管理和行政管理、馆际协作等手段来防范和制裁各种计算机犯罪、盗窃等社会灾害。是用来对付人员危险因素和管理危险因素的。它相当于整个社会的防护系统。其完善有赖于社会立法、公共安全工作、公民道德的提高，等等。

制度、规程、措施防护层是指：建立各项安全制度，组成一套有效的贯彻、执行、监督体系，确保各项制度的落实；制订人员、机房、设备、软件、资料、维护、维修、安全、值日、奖惩等一系列的管理制度，确保系统的安全营运。该防护层可以应付各类危险因素。

机房及附属设施防护层是指机房建设、数据载体贮存、电源、各种机房设施等。能提供系统的防火、防潮、防烟、防尘、防水、防磁、防静电，环境温度控制，净化电源，不间断供电，设备后勤保障等安全保障。它能对付各种天灾危险因素和环境危险因素，对人员危险因素如破坏、非法入侵和盗窃也有防护能力。

电子技术、软件技术防护层是指通过各种计算机硬件技术和软件技术，防止各种非法入侵、病毒感染、破坏、操作失误、软硬件故障等危险因素。

人员防护层包括了系统管理员、数据录入员、系统操作人员等与系统发生直接关系的员工，也包括人事保卫干部等非直接关系的员工。他们既是安全管理的对象，又是安全管理的责任者。从安全管理的规划到安全管理的执行，都要靠他们去做。它是最活跃、最具能动作用的防护层，与其他防护层结合，可以全面保障图书馆自动化系统的安全。

后4层是立足馆内的防护层。图书馆对它们有充分的能动作用，可以通过具体的方法、手段加强完善它们，以抵抗各种人为的和自然的入侵和危害。

从国内外图书馆界和其他行业的计算机应用实践来看，各类计算机信息系统的安全越来越被人们重视。本文对此作一些理论探讨，目的是为了引起图书馆界对图书馆自动化系统安全管理的重视，给从事图书馆自动化建设的有关人员和系统的实际使用者，以及对计算机信息系统的安全管理有兴趣的同行提供参考。

参考文献

1 王秀华. 关于计算机应用系统安全结构体系的探讨. 计算机世界周报，1993，(18)：25

（下转37页）

产业中各产业综合实力的体现，得到社会公众的认可。图书情报业在这方面受本产业综合实力的制约，相对较弱，但作为公益性较强的信息行业，其产品及服务的可信度较强，大有潜力可挖。

3 建议

图书情报业若想在市场经济的环境中继续生存与发展，首先应努力做到要根据市场经济规律办事，了解自己在信息产业中的地位及竞争能力，坚定以实力求生存的信心，确立以质求胜的竞争观念。其次要拓宽资金来源渠道，增强技术竞争力。图书情报业在信息产业中的技术竞争力相对薄弱与长期以来的资金严重不足有关。应拓宽资金来源渠道，变原来的一元化模式为多元化模式，以更多的经济投入来保证图书情报业技术设备的先进性，增强其技术竞争力。第三，要抓住机遇，发挥优势，尽快占有自己的市场。改革的浪潮将图书情报业推向了市场。关贸总协定将签订又为我们带来了新的社会需求和机遇。图书情报业应迅速加强有关方面的工作。

参考文献

1，2 杨列勋，何智勇. 信息产业的内部结构与外部关联. 情报学报，1993，(4)：276～283

3 汪廷炯. 关于科技情报体制改革。科技情报工作，1987，(5)

4 刘东维，薛曙光. 中国科技情报系统投资规模结构及其格局的演变。情报学报，1992，(2)：106～109

5 确保重点建设——1993 年国家重点项目建设情况。中国投资与建设，1993，(11)：18～20

6 同 5。1993，(7)：47

7 胡昌平. 论信息产业发展中的国际竞争与合作。情报学报，1993，(6)：445～451

相丽玲 1985 年毕业于山西大学图书情报学系，1990 年毕业于中国科技情报研究所，获管理学硕士学位。现为山西大学信息管理系讲师。已发论文数篇，专著 1 种。通讯地址：太原市，邮码 030006。

（来稿日期：1994-04-18。编发者：徐革。）

（上接 26 页）

2 王如起. MIS 整体系统的维护、更新、改造问题研究. 计算机世界，1993，(11)：121～123

3 彭钢. 单机银行门市业务系统的安全管理. 计算机世界月刊，1992，(2)：48～51

4 丁晓宁. 工业计算机容错概念及原理. 计算机世界月刊，1993，(5)：73～74

5 李学诗. 计算机系统安全技术. 武汉：华中工学院出版社，1987：8

6 [美]雷利·E·朗. 计算机与信息系统指南. 北京：电子工业出版社，1986：11

7 [美]R·P·费希尔. 信息系统的安全保密. 北京：科学出版社，1987. 12

8 刘尊全. 计算机病毒防范与信息对抗技术. 北京：清华大学出版社，1991. 5

9 翁朝曦、周源泉. 可靠性基础入门. 北京：中国统计出版社，1991. 4

10 广东省文化厅. 广东省文化厅关于建立广东省公共图书馆自动化网络的意见，1994

11 广东省高校图书情报工作委员会. 抓住机遇，为加速实现广东省高校图书馆现代化而奋斗. 图书馆论坛，1993，(5)：16～2

张晓源 现为广州图书馆副馆长、馆员。已发文 10 余篇，通讯地址：广州市中山四路 42 号，邮码 510055。

（来稿时间：1994-02-28。编发者：翟凤岐。）