中国图书馆学报(双月刊)2000 年第 3 期
ZHONGGUO TUSHUGUANXUEBAO

●程小澜 陈 晔 胡 东 封学绛

图书馆计算机应用系统开放性与安全性的控制研究

摘 要 图书馆计算机应用系统中的开放性与安全性是相互对立又相互制约的。因此应对其进行综合控制,既要以最大限度的开放性为目的,又要时刻保持安全性的要求。有计划、有步骤地对图书馆的网络人员进行培训,全面提高其理论和知识水平,增强其系统操作能力是关键。参考文献 5。

关键词 图书馆计算机应用系统 开放性 安全性 控制研究
分类号 G250.72

ABSTRACT Openness and security in library computer application systems are mutually contradictory and restrictive. Therefore, we should have some control over them, paying attention to both openness and security. Among key factors is the training of library network administrators. 5 refs.

KEY WORDS Library computer application system. Openness. Security. Control
CLASS NUMBER G250.72

随着现代通信技术和计算机技术的迅速发展,越来越多的图书馆建立了图书馆自动化集成系统,由于其自身所特有的工作特性,构成了对安全性和开放性的双重要求。因此如何有效地控制系统的开放性和安全性,便成为摆在我们面前的十分重要的课题。笔者拟对构建浙江图书馆计算机应用系统的经验和教训进行总结,供大家参考。

1 构建应用系统的概况

浙江图书馆构建的计算机应用系统,已不再局限于传统图书馆业务的计算机化处理。从它所处理的业务可分为如下 7 个子系统:处理图书馆采访、编目、流通、检索等传统业务的子系统;图书馆读者 IC 卡智能管理系统;VOD 视频点播子系统;光盘数据库查询系统;因特网站及各类服务子系统;局部的办公自动化应用系统;人员培训及开发测试子系统。从软硬件设备的角度又可分为主机(服务器)系统、网络综合布线系统(PDS)、计算机网络系统、各类 PC 及外设组成的客户机应用子系统、不间断电源供应系统、操作系统、处理图书馆基础业务的集成系统、VOD 点播软件、网络监控系统、防火墙子系统等。该计算机应用系统已较为完善,它基本包含了当前图书馆自动化应用的诸多方面和形式。针对这些不同的应用与子系统,我们分别采取相应的措施来实现开放性与安全性的控制。主要采取两类措施,即技术手段和行政的规章制度。本文着重从技术措施方面加以阐述。

2 运用技术手段实现系统开放性与安全性的控制

2.1 系统开放性

2.1.1 系统开放性特征

开放性是当今计算机应用系统的普遍要求和趋势,也是图书馆自动化系统的发展方向。图书馆自动化系统的发展经历了从"单一"到"集成"的过程,最近几年又开始向以网络化、电子化、数字化为特征的数字图书馆方向开展。同时计算机应用系统体系结构的发展也经历了最初的主机多用户模式、客户—服务器模式以及到当前的浏览器—服务器模式,表现出应用系统越来越依赖于网络的建设与应用的趋势,且这两者是互相促进的。而这在本质上也是从封闭系统到开放系统的发展过程,因为网络化本身就体现了开放的含义。所以开放性的应用系统应是指其所产生的数据资源符合标准或通用格式;所建网络系统应遵循开放体系的标准,符合现行的网络标准与通讯协议;在多种硬件平台上能良好地运行,并保证能充分利用现有的设备和资源,又能满足业务量扩充和业务类型扩展的需要。具体体现在以下几个方面:

(1)标准的数据格式:在图书馆计算机应用系统中,各类数据库的开放性、标准化程度对整个应用系统的开放性有较大影响,因而在涉及建设各类数据库

时,需特别重视数据格式的标准与开放。

(2)开放的网络环境:电子计算机和数据通信网络的广泛应用是现代社会信息化的标志,图书馆作为"信息高速公路"的中转站在这方面显得尤为重要。一个开放的网络环境应符合各类现行的网络通讯协议,采用符合标准的各类网络产品,网络系统设计合理、结构清晰,具有良好的扩展性和可管理性,从而方便读者随时随地存取信息,实现图书馆之间、各种社会信息中心之间、地区之间、国家之间乃至世界范围内的信息资源共享。

(3)广泛的硬件支持:任何软件系统都必须运行在一定的硬件基础上,一个开放的系统应该能够在多种硬件平台上良好地运行,能够使图书馆现有的硬件发挥出最大的效用,且不必对硬件进行大量的重新投资。

(4)方便的系统功能:一个开放的图书馆管理系统应该让读者更多地参与到系统中来,向读者提供更为丰富多彩的系统功能,方便读者更加自主地获取和利用图书馆的资源,提供详尽的在线帮助和良好的人机界面,使读者更容易使用而不需任何专业培训或辅导。

2.1.2 系统开放性的控制

(1)数据标准的控制:尽可能选用通用的商品化数据库管理系统来构建各类数据库,且尽可能选购比较开放的有通用数据接口、界面友好的数据库。我馆经几年的积累,已建成约 25 万余条的书目数据,它可以从标准的 CNMARC 格式向其他数据库系统导入。因此在将这批数据向新采用的美国 INNOPAC 系统转入时,只需经编程预处理后,即顺利转入新系统。这正是由于我们在最初确定软件系统时,重视书目数据的标准而带来的便利。

(2)构建开放的网络环境:首先新建馆舍应考虑在基建过程中同步建设 PDS 系统。我们在新建馆舍时即选用美国 AMP 公司 ACO 系列产品。ACO 系列为模块式设计,十分灵活,只需更换接口模块就能适应不同的应用需求。根据新馆建筑平面面积较大,中心机房设置在地下一层建设物的中央位置,无法直接垂直布线,且许多区域到中心机房的距离超过 5 类线的使用极限值这一情况,我们采用在大楼两侧各放置井道,分别集中楼左右区域的走线,并在垂直干线上进行光纤与五类线的双备份。从而使大楼内计算机网络的物理链路在各工作区域中到处存在,而且配置、调整线路等管理工作极为便利,同时也增加了灵活性与可靠性。如此构建的 PDS 系统首先使我馆的网络环境在物理链路上具有良好的开放性。网络设备以选用美国 Bay Network 的产品为主,同时也采用了其他如 3 com, intel, cisco 的部分网络产品。在选用前做了一些彼此互操作、互兼容的测试,发现彼此能较好地互联,也证明了采用符合标准开放的产品具有较好的开放性。但应注意的是在一套彼此紧密联系的网络系统里,目前仍不赞成选用多厂商产品。网络系统采用 ATM、Fast switch ethernet 与 switch ethernet 混合使用,在主干交换机上配置 ATM 模块与 fast switch ethernet 模块,实现其他 ethernet 交换机与 ATM 的互联互通,从而在主干交换机内实现同一平台上不同类型网络的混接,在主干交换机上配置各类 LAN SERVER,实现以太网仿真。同时配置一些 Fast ethernrt switch,利用 PDS 系统中垂直主干的备份五类线,为一些重点应用区域提供备用链路。与外界的通讯采用 DDN 专线联通 Chinanet。馆内根据业务不同分为 6 个子网,通过配置支持 Layer3 switch 的交换机实现各子网间的路由。从而组建成以 ATM 为主干、Fast switch ethernet 为辅的全馆网络系统,实现 10M 交换到桌面,局部 25M ATM 到桌面,各主机服务器以 155M ATM 接入网络。这种配置在技术上较为先进,采用 ATM 技术能提供较高的带宽,特别是在大负载、大流量、多媒体应用的时候有极佳的性能,能针对不同网络应用提供相应的网络服务,网络服务的质量容易得到保证。快速以太网是一种非常成熟的技术,其设备优良,系列齐全,使用方便,可灵活根据应用环境配置设备,在更新或修复网络系统故障时较为方便。因而能很好地提供备用链路并满足其他在不断调整与发展变化中的业务需求。在网络协议以 TCP/IP 为主,也采用其他各类通用的网络协议。如此组建后的网络系统,其开放性、扩展性较好,能根据业务的局部调整与变化而改变,具有较好的灵活性。

(3)主机(服务器)系统:各类主机(服务器)在整个应用系统中充当重要的角色。服务器拥有系统中的各类数据资源与处理能力,提供各种服务。所以从开放系统的角度考虑,我们应选用档次高一些的,运行速度快的大型 UNIX 主机,并配以高容量、安全可靠的外存设备,如阵列等组建硬件主机系统。从性价、应用普及程度、技术支持和售后服务等角度考虑,我们选用了美国 SUN 公司 enterpcise 系列产品组建主机系统。同时购置一些 PC Server,以配合 UNIX 主

机,用于其他各类周边的服务。

(4)软件及软件中参数设置的考虑。开放的系统与各类软件的选用密切相关,在前述选购主机时也综合考虑了软件的开放性。首先,操作系统和系统服务软件应是开放的、高性能的和符合各类相关标准,有友好的界面和相对开放的应用开发环境,具有各类软件工具与支持软件包。我们所用的 SOLARS 操作系统在国内应用历史较长,有较多的应用开发经验和熟练的软件人才。在 PC 服务器上选用微软的 NT SERVER。NT 系统目前在国内应用也十分广泛,虽在系统健壮性方面较弱,但其友好的界面、丰富的支持软件与技术资料使它在非关键应用场合还是十分合适的。其他各类软件如防火墙、网管软件、因特网服务软件、光盘网络管理软件的选用也须重视其开放性、对各类标准的支持以及应用是否广泛深入等因素。

我馆选用的 INNOPAC 图书馆软件是一个由十几个模块组成的集成系统,它不仅支持传统图书馆业务的自动化功能,如编目、流通、采访等,同时有提供更为先进的图像、浏览器界面的 OPAC,WWW 支持等功能。为了更好地发挥系统本身的开放性特征,我们在业务参数设置中最大限度地利用了系统本身的自动和开放性的功能,把大量的以前面向馆员的业务程序提供给了读者自行处理,把馆员从一些繁琐的操作业务中解脱出来,从而有更多的精力去做深层次的信息服务。这样的业务参数设置主要体现在 OPAC (联机公共检索目录)和流通模块中。我们向读者提供了完全基于 Web 的 OPAC,读者只需了解基本的浏览器操作知识就能够轻松自如地检索所需的信息。在检索入口处我们不但提供了 8 个常用的检索途径如作者、题名、主题、索书号等,还设置了诸如检索历史和图书馆信息的辅助检索入口。在限制检索中,我们设置了语种限制、馆藏地限制和条件限制。其中条件限制又可细分为多个限制项,它们可以是出版年、出版者、资料类型、题名关键词、作者关键词和主题关键词等。在流通模块中我们目前已经把续借、预约等业务程序完全提供给读者自行处理,读者通过因特网连接到本馆主页就可以随时随地完成上述操作。同样是基于 Web 的浏览器界面使读者不需经过任何专业培训就能胜任,他们所要做的无非是个人身份验证而已。

2.2　系统安全性

安全性是指图书馆计算机集成系统内程序和数据的安全程度,即能否有效地防止不合法的访问使用程序和数据。安全性是评价一个图书馆集成系统的重要标志。我馆的集成系统主要从 3 个方面来考虑系统的安全性:系统中各设备在物理上应处于安全可靠的环境中;系统中软、硬件及网络系统安全可靠地正常运行,提供的各项业务与应用服务处于正常工作状态中;系统中的各类软件、数据资源处于安全可控制的环境中。

2.2.1　系统安全的必要性

(1)计算机网络安全的必要性。计算机网络由于其本身的复杂性,使得系统中任何一个硬件和软件模块存在的不安全缺陷都可导致整个系统的不安全。由于资源共享和网络扩展的需要,都会导致不法分子窃取他人秘密数据的机会增多。另外,病毒的传播愈来愈成为威胁计算机网络安全的问题,轻者使系统处理能力下降,重者使整个网络瘫痪。

(2)操作系统安全的必要性。操作系统是除计算机硬件外确保计算机安全的最基本的部件,因为它掌管着整个系统资源的使用权,其他软件都要通过操作系统才能获准使用某种资源。如果操作系统具有安全的控制策略和保护机制,便可以将非法入侵者拒之门外。

(3)数据库安全的必要性。图书馆自动化系统中最宝贵的资源是各类数据库,这些数据库凝聚了图书馆工作人员的大量心血,维系着图书馆日常工作的正常、有效地开展,动态地记录了读者利用图书馆的各种情况和信息,是图书馆需要重点保护的一种资源。随着图书馆自动化系统的服务与管理走向网络化,有效保证系统各数据源的安全是十分必要的。

2.2.2　系统安全性的控制研究

图书馆自动化系统的安全管理主要包括两部分:一是防止人为的入侵,即防止非法用户对网络系统、自动化系统的非法使用与合法用户的越权使用所造成的数据被非法窃取、篡改和破坏。二是防止意外事故,即防止系统数据丢失。在进行系统安全管理时,要评估安全要求和目标,制定系统安全策略,确定服务对象。

(1)计算机硬件的安全可靠性。对一些主要的应用应采用大型 UNIX 服务器或高端 PC Sever,并采用阵列、RAID 技术提高可靠性,对最为关键的应用采用集群、双机热备、设置备用设备等技术,合理配置各服务器上的服务内容,使得一台服务器硬件失败不会牵连其他服务的正常开展。

(2)计算机网络安全的控制。首先,我们选用了具有良好安全管理机制的运行环境 Windows NT,设定访问者及其相应访问类型。同时提高主干网络设备的可靠性,配置冗余电源、冷却装置时钟及冗余配置存贮。对网络的拓扑结构进行精心设计,对关键业务提供备用链路,防止出现单点失误。通过分析业务情况及网络的数据流量在时间与空间上的分布情况,合理配置各类路由与子网,从而大大减少网络上不必要的广播、查询等流量的出现。在与因特网连接处,设置防火墙软件,关闭对网络安全构成威胁的各类服务,对每一个进出系统的包进行查看、验证,以阻止非法侵入。将单纯内部业务处理的子网同因特网之间的路由隔断,以进一步提高系统的安全性,并减少不必要的网络流量。对各子网之间的路由也进行配置,以利系统安全。同时利用网管软件,分析、监控整个网络系统的运行,及时发现故障点以及各类网络非正常运行状态,在故障造成影响之前先行捕捉并排除。充分利用地址绑定、协议绑定等网络管理功能,细化并提升网络系统的安全性。

(3)操作系统的安全控制。操作系统需根据其所处位置、所处理的业务情况分别加以控制,如可分为外部网可访问的主机,馆内读者可访问的主机,馆内工作人员可访问的主机,以及馆内人事、财务等敏感主机。对于馆内人事、财务等主机因一般不与外界其他子网连通,故其安全控制主要针对内部人员,通过管理各级口令、权限来实现,而不对主机操作系统做特殊设置。对暴露在外部的主机其安全控制最为严格,在这类主机上对操作系统做特殊设置,如安装最小、干净、标准的操作系统、禁止使用用户账号、关闭所有不必要的服务程序、尽量使用只读文件系统,并使用工具软件检查系统的安全机制。在正常运行后,对该类主机做好备份,并保留好系统的日志。日常工作中经常分析日志,监测主机的运行。

(4)数据库的安全控制。我馆使用的 INNOPAC 图书馆软件,有一个集书目记录、馆藏记录、读者记录、书商记录等所有记录为一体的综合型数据库。浙江图书馆自动化集成系统旨在通过数据库结构定义、其他应用定义和程序算法设置各业务数据集,以防止图书馆集成系统用户以外的其他用户访问和使用本集成系统的程序和数据,防止本业务以外的其他人员使用和访问本业务功能和数据,以及防止本业务内的其他人员访问本人的数据。为此,我们设定的基本安全管理模式是将用户账号管理和用户权限设定相结合的方法。用户账号管理,既为分清每个人的工作责任提供了前提,也为每个人所负责的数据的安全创造了条件。而用户权限设定,可以保证每个业务人员只在其业务数据集内制作和处理数据,有效防止了有意或无意的数据非法访问。我们设定了 3 种保护方式。一是设定特定的终端机只执行那些特定的功能,例如只有设置在编目组,在编目组馆员众目睽睽之下才能改动书目。二是馆员依职务、权限设定可执行的系统功能。系统管理员先在系统设定可操作系统人员的代称及所能授权执行的功能,然后经授权可以操作系统的馆员可以自己决定自己的密码。之后,经授权可操作系统的馆员可以随时更改自己的密码而无需麻烦系统管理员,密码的变动不会影响到经授权的系统功能的执行。当那些功能已设定为某些特定馆员执行,馆员在终端机执行之前,必须先让系统确定是否可以执行;密码错误或未经授权的话,系统都会给予提示。三是以一独立的储存档储存什么时间、哪一台终端机、是谁来执行的变动。功能的执行、数据库的改动,则改动的记录会被储存在磁盘的处理档中,每一个处理档都会被复制到磁带上,由磁带可以追溯改动哪些资料,什么时间改动的,被谁改动的,及在哪一台终端机做的。另外,为了保护数据以防意外事件造成的破坏,如断电、火灾、机器故障等,我们专门为 INNOPAC 服务器配置了供电时间长达 8 小时的 UPS,坚持数据的日备份和定期的完全备份,并将备份的磁带放到远离机器的安全地方,以免有意外情况发生时和机器一同受损。

2.3 系统开放与安全性的统一控制

在技术实施时,开放性与安全性是互相对立的,越开放、越方便使用的系统相应会降低其安全性,而安全控制措施非常严格的系统其开放性相应变差。但从整体系统需求而言,它们又是相互依存的。因此,为了在提高开放性的同时相应提高安全程度,需对计算机应用系统的安全性与开放性进行综合控制。我们采用了前一种设计思想,以保证安全性。我们在系统建设至运行过程中,既以最大限度的开放性为目的,又时刻保持安全性的要求。在各业务环节的设置和访问权限的划定上,做到合理限定、有条不紊。同时,一直坚持管理控制从严的指导思想,禁止利用系统资源从事其他与业务无关的事情。并在客户端安装资源可控制的操作系统,以保证业务正常运行的前提下提高系统的整体安全性。对各项新的服务或业务采取逐步分期分批开放的方法,(下转第 80 页)

障社会由混沌到有序,从而顺利前进、健康发展的有力手段。而一切社会活动均遵循法制轨道运行,则是文明进步的重要标志。因此,必须尽快完善我国图书馆法制建设,依法治馆,使我国图书馆事业得以健康稳定地发展,以更好地迎接社会变革给图书馆带来的宝贵机遇和严峻挑战。

参考文献

1,11,14　李衍翎. 图书馆法的三个主要问题. 中国图书馆学报,1997(1)
2　陈静宇. 我国图书馆亟需立法. 图书馆建设,1996(2)
3,13,17　徐国定,陈德育. 图书馆法与图书馆事业. 四川图书馆学报,1992(2)
4,27,32　江向东. 国外图书馆立法实践给我们的启示. 图书馆论坛,1992(4)
5,20　李立新. 试论图书馆立法. 大学图书馆学报,1996(6)
6,9,12　裴成发. 图书馆法制建设论要之三:图书馆法属性研究. 图书馆建设,1996(1)
7,8,15,35　裴成发. 图书馆法制建设概说. 图书馆建设,1995(5)
10　董光荣,论日本图书馆法. 图书馆杂志,1989(4)
16,28,30,42　武守民. 关于我国图书馆立法的思考. 图书与情报,1996(2)
18　彭斐章. 世纪之交的思考 ——中国图书馆事业的昨天、今天与明天. 图书馆,1995(1)
19　范东洪. 我国图书馆立法刻不容缓. 情报杂志,1996(5)
21　刘德有. 适应市场经济新形势,深化图书馆事业的改革. 中国图书馆学报,1994(2)
22　万宗知. 我国图书馆立法初探. 图书馆员,1989(6)
23,38　谢建国. 进一步深化改革,加快图书馆立法建设. 浙江高校图书情报工作,1996(4)
24　赖宽标. 图书馆立法是图书馆事业延续和发展的重要保证. 广东图书馆学刊,1989(4)
25　李开胜. 立法是我国图书馆事业繁荣的根本保证. 中国图书馆学报,1995(5)
26　廖煊. 国外图书馆立法简况. 图书馆论坛,1995(6)
29,34　孟扬. 对美日图书馆法的比较分析. 图书馆理论与实践,1996(1)
31　罗力可. 论我国图书馆立法之必然. 图书馆,1995(6)
33　甘伟淑. 图书馆立法必须体现改革精神. 江苏图书馆学报,1994(5)
36　田文清,武旭. 关于图书馆立法的思考. 图书馆理论与实践,1993(3)
37　胡允珍. 对制定《图书馆法》几点思考. 图书馆建设,1996(1)
39　裴成发. 图书馆法应包含的权利、义务研究. 图书馆建设,1996(2)
40,41　谢友宁. 试论读者权益保护. 江苏图书馆学报,1997(3)

裴红艳　赖湘蓉　南开大学图书馆学系研究生。通讯地址:天津市。邮编 300071。

(来稿时间:1999-11-18。编发者:徐苇)

(上接第 45 页)使整个系统运行更加平稳。另外,素质优良的网管人员是图书馆网络系统正常运行的基本保障。有计划、有步骤地定期对图书馆的网络人员进行技术培训,全面提高其理论知识与业务水平,加强其对新知识、新技术的认识和掌握能力,增强其操作系统的能力,这是图书馆网络建设中使系统开放性与安全性得到良好控制的一个重要环节。

参考文献

1　Internet 防火墙与网络安全. 北京:机械工业出版社,纽约:西蒙与舒斯特国际出版公司,1998
2　我校数字图书馆的基本环境及其应用. 现代图书情报技术,1999(5)
3　浅析分网运行机制对图书馆自动化系统的保护. 现代图书情报技术,1999(2)
4　关于图书馆集成系统整体安全性的思考. 现代图书情报技术,1999(1)
5　现代图书馆信息管理系统的新要求 ——从美国威斯康辛大学图书馆系统的选择谈起. 现代图书情报技术,1999(4)

程小澜　浙江图书馆馆长,副研究馆员。通讯地址:杭州市曙光路 38 号。邮编 310007。

(来稿时间:1999-11-16。编发者:翟凤岐)