# 数字图书馆信息安全管理依从标准的选择*

茆意宏　黄水清

**摘　要**　信息安全管理标准是组织建立并实施信息安全管理体系的指导性准则。ISO 27000 系列标准是通用的、普适性的信息安全管理国际标准,适用于所有行业。数字图书馆信息安全管理不仅是技术问题,更是管理问题。按照数字图书馆信息安全管理标准的遴选原则,最合适的依从标准应该选择 ISO 27000。图 1。参考文献 21。

**关键词**　数字图书馆　信息安全管理　标准

**分类号**　G251

**ABSTRACT**　Information security management standards are guidelines for the organization and implementation of information security management systems. ISO 27000 series of standards is general and universal international standards for information security management, suitable to all industries. Information security management of digital library is not only a technical issue, but also an issue of management. Based on the analysis of the characteristics of digital library, the authors choose a suitable ISO 27000 standard for information security management of digital library. 1 fig. 21 refs.

**KEY WORDS**　Digital library.　Information security management.　Standard.

**CLASS NUMBER**　G251

从 20 世纪 90 年代开始,信息安全更多地是一个管理问题的理念被越来越多的业界人士所接受,一批与信息安全有关的规范陆续产生,一些国家和国际组织还制定了若干信息安全管理国家标准和国际标准。数字图书馆作为一种特定类型的组织,其信息安全管理工作也应遵循这些标准与规范。本文将介绍信息安全管理标准的概念及发展简况,并对国内外知名的信息安全管理标准与规范进行比较。在此基础上,结合数字图书馆的特点,选定数字图书馆信息安全管理的依从标准。

## 1　信息安全管理标准的概念与内容

信息安全是信息系统在实现互联、互用、互操作过程中提出的安全需求,因此迫切需要技术和管理标准来规范系统的设计和实现。如同质量管理过程中有 ISO 9000 与环境管理过程中有 ISO 14000 一样,信息安全管理标准是信息安全管理实践的必然产物,也是信息安全管理过程的共同原则。

信息安全管理标准是组织建立并实施信息安全管理体系(Information Security Management System,简称为 ISMS)的指导性准则,主要目的是为组织实施有效的信息安全管理所需的控制提供通用的规则[1]。信息安全管理标准提供了有效实施信息安全管理的建议,规范了信息安全管理的方法和程序。依据信息安全管理标准,用户可以制定出适合自己的安全管理计划和实施步骤,为所在组织发展、实施和评估有效的安全管理实践提供参考依据[2]。

信息安全管理标准的内容主要由两部分构成:风险评估和建立在评估基础上的风险控制。在风险评估方面,依据信息安全管理标准规定

* 本文系国家社会科学基金"数字图书馆信息安全管理与评价"(编号 07BTQ005)研究成果之一。

的方法与原则,组织可以对其所拥有的资产进行识别,同时明确各项资产安全责任的归属,对资产存在的脆弱性与面临的安全威胁进行规范的评估。在风险控制方面,信息安全管理标准规定了针对组织及信息系统中的内容进行管理和控制的规则,这些内容与人员、流程、实体安全以及一般意义上的安全管理有关[3]。

没有标准就没有规范,没有规范就无法生产出在信息安全方面有保证的满足社会需求的产品,无法形成信息安全产业的规模化。信息安全管理标准是一种多学科、综合性、规范性很强的标准,其目的在于保证信息系统的安全运行。信息安全管理标准可以规范人们的安全防范行为,提高组织内外各类人员的信息安全意识及组织的整体信息安全水平。

## 2　国内外主要的信息安全管理标准

对信息安全标准的研究最早出现在20世纪60年代的西方发达国家。60年代后期,以大型机为代表的计算机系统在多种场合得到应用,世界上最早的计算机网络也在这一时期萌芽,信息安全管理有了最初的动因与需求。

### 2.1　国外的信息安全管理标准

在业界有影响的国外信息安全管理标准,均诞生于欧美发达国家,其中的部分标准或为国际标准化组织接受成为国际标准,或在某些领域成为业界的操作规范,起到事实上的行业标准的作用。这些标准与规范包括美国审计总署的GAO/AIMD－99－139风险评估指南[4]、美国国家标准与技术研究所(NIST)的风险管理框架[5]、卡内基·梅隆大学软件工程研究所(CMU/SEI)的OCTAVE(Operationally Critical Threat, Asset, Vulnerability Evaluation)方法[6]、澳大利亚和新西兰联合开发的风险管理标准AS/NZS 4360:1999[7－8]、国际标准化组织的ISO 27000标准系列。

上述标准是目前在业界得到广泛应用的普适性的信息安全管理标准。此外,国外还有一些与信息安全管理有关的其他标准和操作指南。它们或者在某个历史时期产生过重大影响,或者在某个特定的领域为了某个特定的目的得到广泛应用,如系统安全工程能力成熟模型(SSE-CMM)[9]、可信计算机系统评估准则(TCSEC)[4]、信息安全技术标准(ITSEC)[4]、可信计算机产品评估准则(CTCPEC)[10]、信息技术安全性评估通用准则(CC)[11]、美国信息技术安全联邦准则(FC)[4]。

当前,世界上最著名的信息安全管理标准是国际标准化组织的ISO 27000系列标准。ISO 27000系列标准所针对的是组织的资产,其核心是ISO 27001与ISO 27002,适合于任何规模和行业的组织,尤其适合于信息安全影响关键的组织[12－13]。ISO 27000的前身——英国标准BS 7799,自1998年颁布后就在全世界范围内得到广泛的认可,有40多个国家和地区开展了BS 7799信息安全管理体系的认证。ISO 27000标准公布后,已为更多的国家和地区所接受。截至2010年1月21日,已有80多个国家与地区开展了ISO 27000信息安全管理体系的认证工作,全球通过ISO 27001认证的组织已经达到6037家,其中日本最多,达到3378家[14]。

已开发和规划中的ISO 27000系列标准包含:

- ISO/IEC 27000:2009 概况与术语
- ISO/IEC 27001:2005 信息安全管理体系要求
- ISO/IEC 27002:2005 信息安全管理体系最佳实践
- ISO/IEC 27003 信息安全管理体系实施指南(正在开发)
- ISO/IEC 27004 信息安全管理度量和改进(正在开发)
- ISO/IEC 27005:2008 信息安全风险管理指南
- ISO/IEC 27006:2007 信息安全管理体系审核认证机构要求
- ISO/IEC 27007 信息安全管理体系审核指南

上述标准或指南,相互支持和参照,共同为组织实施信息安全最佳实践和建立信息安全管

理体系而发挥作用。

ISO 27000 系列标准是通用的、普适性的信息安全管理国际标准。为了照顾各行业的不同特点,ISO 还计划针对不同行业开发一组标准,已完成的有电信行业的 ISO/IEC 27011,正在开发的有电子政务行业的 ISO/IEC 27012。

### 2.2 国内的信息安全管理标准

从 20 世纪 90 年代末开始,我国先后公布了一系列的国内信息安全标准与法规。公安部、国家保密局、国家密码管理局、国务院信息化工作办公室等制定、颁布了一批信息安全的行业标准,国家信息安全标准化委员会相继转化了一批国际信息安全管理标准。我国信息安全标准在这些标准化组织的有效领导下取得了长足的进步[2]。

1999 年 9 月 13 日,《计算机信息系统安全保护等级划分准则》(GB 17859 - 1999) 经国家质量技术监督局发布,并于 2001 年 1 月 1 日起实施,该准则是由公安部提出并组织制定的强制性国家标准[15]。

2001 年 3 月 8 日,国家质量技术监督局正式颁布了由 ISO/IEC 15408:1999(CC)转化而来的国家标准《信息技术 安全技术 信息技术安全性评估准则》(GB/T 18336 - 2001),并于 2001 年 12 月 1 日起实施[11]。

2007 年 6 月 22 日,公安部、国家保密局、国家密码管理局、国务院信息化工作办公室等四部委制定完成并审批通过了《信息安全等级保护管理办法》,将信息系统的安全保护等级划分为五级[16]。

目前,我国已完成信息安全管理体系国际标准 ISO/IEC 27001:2005 和 ISO/IEC 27002:2005 的转化工作,转化后对应的国家标准《信息技术 安全技术 信息安全管理体系 要求》(GB/T 22080 - 2008)和《信息技术 安全技术 信息安全管理实用规则》(GB/T 22081 - 2008)已于 2008 年 6 月发布,2008 年 11 月 1 日正式实施。此外,ISO 27000 系列标准中的《信息安全管理体系审核指南》系由我国提交,经批准已成为国际标准,标准号为 ISO/IEC 27007。在信息安全管理体系认证方面,截至 2010 年 1 月 21 日,我国获得信息安全管理体系认证证书的机构已有 205 家[14]。

## 3 数字图书馆信息安全管理标准遴选的原则

数字图书馆是一种特定的信息组织,也需要遵循信息安全管理标准。那么,如何选择和确定数字图书馆信息安全管理遵循的标准呢?

世界上现有的信息安全管理标准(或操作指南),可以从四个不同的角度进行分类:①有的是以信息产品或信息系统为保护对象,有的以整个组织为保护对象;②有的标准包括信息安全管理的风险评估与风险控制全部过程,有的标准只包括其中的部分环节;③有的只是某个地区、某个区域或某个国家的标准,有的则是由国际标准化组织制定的国际标准;④有的是适用于全行业的普适标准(或指南),有的只适用于特定的行业。

数字图书馆既可以从现有的通用信息安全管理标准中选择,也可以单独研发数字图书馆信息安全管理标准。能有专为数字图书馆量身定做的信息安全管理标准应是最理想的,不过目前世界上还没有出现这样的标准。主要原因在于数字图书馆行业的特殊性不够强,同时独立开发信息安全管理标准的成本代价太高,缺乏可行性。相比之下,选择国际通用的信息安全管理标准来直接使用或加以细化更为可行。比如信息安全管理标准 ISO 27011 与 ISO 27012 是 ISO 27001、ISO 27002 等标准分别在电信行业、政府机构领域的细化和补充,是在 ISO 27000 系列标准中作为特定行业的专业标准存在,其基本理念、原则与规范完全遵循 ISO 27000 的要求。数字图书馆信息安全管理目前虽不能像电信行业、政府机构那样发布自己的标准,但可以借鉴和模仿 ISO 27011 与 ISO 27012 的思路,从通用标准中选定一个依从标准,再为该标准应用于数字图书馆信息安全管理制定一些模板和准则,方便数字图书馆的具体实施。

作为一个信息组织,数字图书馆有设施(包

括软件、硬件和数据)、人员、用户及各种服务。数字图书馆信息安全管理的目的是保证数字图书馆的保密性、完整性和可用性,数字图书馆从现有信息安全管理标准中选定依从标准,须同时具备以下四个条件:标准以组织为保护对象;标准的内容包括信息安全管理过程,既有风险评估,也有风险控制;标准为通用标准,适用于所有行业;标准本身为国际标准,并在本国已被接受。按照这四个条件对前面介绍过的所有标准(或指南)进行过滤,符合第一个条件的信息安全管理标准(或指南)有 GAO/AIMD - 99 - 139、NIST 风险管理框架、OCTAVE 方法、AS/NZS 4360:1999、ISO 27000、国内的《信息安全等级保护管理办法》;符合第二个条件的有 NIST 风险管理框架、AS/NZS 4360:1999、ISO 27000;符合第三个条件的标准最多,有 GAO/AIMD - 99 - 139、NIST 风险管理框架、OCTAVE 方法、AS/NZS 4360:1999、ISO 27000、CTCPEC、TCSEC、ITSEC、CC(包括等同标准 GB/T 18336)、FC、GB17859 - 1999、国内的《信息安全等级保护管理办法》;符合第四个条件的标准只有 ISO 27000。

## 4　ISO 27000 对数字图书馆信息安全管理的适用性

按照数字图书馆信息安全管理标准的遴选原则,依次考察前面介绍过的所有信息安全管理标准,数字图书馆信息安全管理最合适的依从标准应该是 ISO 27000。

首先,ISO 27000 的保护对象为组织,包括完整的组织机构和组织机构中的某一部分。数字图书馆是一种特定的组织,由多个分支组织组成,同时包含信息系统、人员、用户、服务等多种成份,并且是建立在网络平台上的信息系统。ISO 27000 的原则与方法能够满足数字图书馆这种组织类型在信息安全管理方面的要求。

其次,ISO 27000 系列标准是一个完整的标准族,由多个标准组成,涉及信息安全管理体系建设的各个方面。ISO 27000 的核心是 ISO 27001 和 ISO 27002,这两个标准分别描述了组织的信息安全风险评估和风险控制的方法与流程,另外还有其他辅助性的标准,如术语、度量、认证机构、审核等。ISO 27000 系列标准的内容可以覆盖数字图书馆信息安全管理的全过程。

第三,ISO 27000 系列标准为通用标准,适合所有行业。ISO 27000 起源于 BS 7799,而 BS 7799 由英国贸易工业部立项、英国标准协会制定,业界、政府和商业机构共同倡导。BS 7799 的目的是提供一套开发、实施和测量的有效信息安全管理规则,并为贸易伙伴间的信任提供通用框架。在立项之初,BS 7799 就定位为跨行业的通用标准。ISO 27000 适用于所有的行业,同样也适用于数字图书馆。

第四,ISO 27000 是具有广泛影响的国际标准,并已转化为中国国家标准。目前,已经有 80 多个国家和地区开展了 ISO 27000 的认证工作。ISO 27001 的等同标准 GB/T 22080 - 2008 和 ISO 27002 的等同标准 GB/T 22081 - 2008 已正式公布并实施。同时,ISO 27000 系列标准中的 ISO/IEC 2007《信息安全管理体系审核指南》系由我国提交。我国数字图书馆信息安全管理选用 ISO 27000 作为依从标准,既符合业界习惯,也遵守了国家法令。

第五,ISO 27000 实施过程中采用的 PDCA 过程模式,可直接应用于数字图书馆信息安全管理。

PDCA 循环最早由美国质量统计控制之父休哈特(Shewhart)于 20 世纪 30 年代提出,后来由他的学生质量管理专家戴明(Deming)进行了改进。PDCA 是由英语单词 Plan(计划)、Do(执行)、Check(检查)和 Act(纠正)的第一个字母拼成的。PDCA 是全面质量管理所应遵循的科学程序。全面质量管理活动的过程,就是质量计划的制订和组织实现的过程,这个过程就是按照 PDCA 循环,通过周而复始地执行"Plan-Do-Check-Act"中的每一步骤,保证组织的最佳实践能够持续地被文档化、加强和改进[17]。ISO 27001 引入了 PDCA 过程模式作为建立、实施 ISMS 并持续改进其有效性的方法。在建立 ISMS 的过程中,PDCA 循环中的各个环节应作如下理解:P——策划,根据组织的商务运作需

求(包括顾客的信息安全要求)及有关法律法规要求,确定安全管理范围与策略,通过风险评估建立控制目标与方式,包括必要的过程与商务持续性计划;D——实施,按照组织的策略、程序、规章等规定的要求,也就是按照所选定的控制目标与方式进行信息安全控制;C——检查,根据策略、目标、安全标准及法律法规要求,对安全管理过程和信息系统的安全进行监视与验证,并报告结果;A——措施:对策略适宜性评审与评估,评价 ISMS 的有效性,采取措施,持续改进[18]。PDCA 循环周而复始,一个循环结束后即进入下一个 PDCA 循环;大环套小环,一环扣一环,小环保大环,推动大循环;阶梯式上升,每循环一次解决一部分问题,到新的循环又有新的目标与内容(如图 1)[19]。国内已有 9 篇研究 PDCA 应用于图书馆管理的文章,其中一篇直接讨论了将 PDCA 应用于数字图书馆管理的问题[20]。PDCA 应用于数字图书馆信息安全管理当无问题。

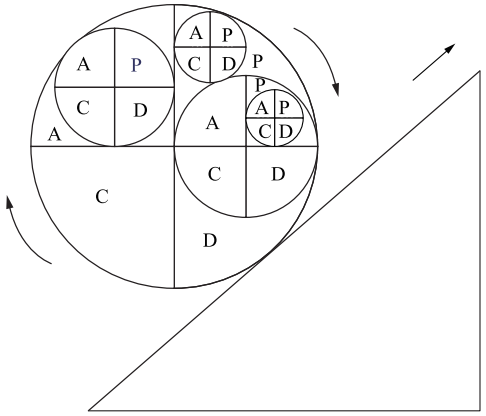


**图 1 PDCA 循环的基本模式**

第六,ISO 27000 提出的风险评估方法论与具体的风险评估方法,适用于数字图书馆信息安全的风险评估。

ISO 27001 提出的风险评估的方法论由三个步骤组成:定义组织的风险评估方法、识别风险、分析并评价风险。这样的三步骤流程在数字图书馆中运作起来并不困难,因为作为国际标准的 ISO 27001 提出的风险评估方法论本身就是普适性的。但 ISO 27001 没有提出实施风险评估的具体方法,在 BS 7799 的时代,实际的风险评估过程无一例外地直接引用 ISO 13335 - 3 的方法。现在 ISO 13335 - 3 已被国际标准化组织废止,其内容被纳入 ISO 27005,成为 ISO 27000 系列标准的组成部分。ISO 27005 中规定的资产、威胁、脆弱性识别及定性、定量风险估算方法运用于数字图书馆也不存在困难。

第七,ISO 27000 的控制目标与控制措施覆盖了信息管理的全过程,能满足数字图书馆信息安全管理控制的要求。

ISO 27002 将可以实施的安全控制划分为 11 个方面,包括 39 个控制目标、133 项控制措施,涉及信息安全的策动、组织、资产、人员、环境、通信、访问控制、系统、安全事故、业务连续性、政策法规的符合性,已包括了信息安全管理控制各个可能的方面,数字图书馆信息安全管理控制的控制域、控制目标与控制措施不可能超出 ISO 27002 的定义。因此,ISO 27002 能满足数字图书馆对信息安全管理控制的要求。

## 5 ISO 27000 应用于数字图书馆信息安全管理的基本思路

ISO 27000 系列标准理论上适用于任何组织,但是在其具体的推广与实施过程中,却存在许多困难。这是因为 ISO 27000 作为通用标准,要兼顾各种组织类型与安全需求,使得标准中规定的风险评估、风险控制等规定趋于原则性,当以 ISO 27000 标准为依据建立信息安全管理体系时操作难度较大。同时,各种组织的业务与资产差异性极大,安全等级要求不一,要把 ISO 27000 标准中原则性的规定落实到具体的信息安全管理体系,工作量巨大。此外,信息安全管理本质上是一个管理过程,组织的信息安全管理体系建立过程基本上等同于管理再造过程。这些原因造成 ISO 27000 实施周期长,费用高。类似数字图书馆这样规模的小型组织的 ISO 27000 认证,时间可能长达几个月甚至跨年度,费用高达几十万元。如果按照这种时间进度与资金耗费应用 ISO 27000 对数字图书馆实

施信息安全管理,建立数字图书馆的信息安全管理体系,估计国内大多数数字图书馆都难以接受。

数字图书馆是众多的组织类型中的一种。根据夏立新对数字图书馆特点的归纳[21],数字图书馆以数字化方式存储信息,以网状化方式组织信息,以智能化方式检索信息,以网络化方式传播信息,并以用户为中心开展服务。无论是前台还是后台业务,所有的数字图书馆都大体相同。数字图书馆以计算机和网络为平台,完成信息从采集、加工、存储到检索、传递的服务全过程。数字图书馆的工作基本相同,业务流程基本一致,或者说业务流程趋同。从信息安全管理的角度看,业务流程趋同是数字图书馆的最大优势,因为风险评估与风险控制都是从分析业务流程开始的。有什么样的业务,决定了需要什么样的安全级别,决定了有什么样的资产,也决定了资产将面临什么样的安全威胁及存在什么样的脆弱性,同时也决定了可供选择的可能的控制措施。

总之,应用 ISO 27000 这样的信息安全管理标准为数字图书馆建立信息安全管理体系时,数字图书馆反映出如下特点:业务流程趋同、安全等级要求相近、资产类型相似、威胁与脆弱性便于归纳、控制措施便于选择。基于数字图书馆信息安全管理的上述特点,我们便有可能为数字图书馆应用 ISO 27000 建立信息安全管理体系总结出某种模板。在这个模板中,包括了数字图书馆常见的业务,列出了数字图书馆各项业务可能用到的资产,和资产面对的安全威胁与脆弱性,及与之相关的信息安全控制措施。有了这个模板,数字图书馆信息安全的风险评估与风险控制一定程度上可以变成从列表中选择参数的过程。如此,则可能把应用 ISO 27000 对数字图书馆实施信息安全管理、建立信息安全管理体系的时间与经济成本控制在国内的数字图书馆界可接受的程度。

按照这个思路,将 ISO 27000 应用于数字图书馆信息安全管理,设计各数字图书馆建立信息安全管理体系时可借鉴的某种具体模式,面临着以下任务:

- 总结数字图书馆的业务流程;
- 归纳与数字图书馆各项业务相关的资产;
- 解决数字图书馆的资产估值问题;
- 解决资产的威胁估值问题;
- 解决资产的脆弱性估值问题;
- 建立数字图书馆信息安全的风险评估模型;
- 建立数字图书馆信息安全的风险控制模型;
- 解决数字图书馆风险控制的控制措施选择问题。

遵循上述思路,我们将 ISO 27000 系列标准应用于数字图书馆领域,在对国内数字图书馆与信息安全有关的各种现实情况进行调查的基础上,总结共同业务,得到数字图书馆的业务流程,建立了数字图书馆业务流程与资产关联表、数字图书馆资产—威胁—脆弱性对照表,计算和分析了数字图书馆面临的各项风险,提出了数字图书馆信息安全风险等级的划分方法,筛选得到数字图书馆信息安全管理的核心控制要素,确定了数字图书馆信息安全风险控制的目标,给出了数字图书馆控制措施的选择与实施,建立了数字图书馆信息安全的风险评估与风险控制的数学模型,形成了数字图书馆信息安全风险评估和风险控制模板。

**参考文献:**

[1] 科飞管理咨询公司. 信息安全管理概论:BS 7799 理解与实施[M]. 北京:机械工业出版社,2002.
[2] CEAC 国家信息化计算机教育认证项目电子政务与信息安全认证专项组,北京大学电子政务研究院电子政务与信息安全技术实验室. 信息安全管理基础[M]. 北京:人民邮电出版社,2008.
[3] 王英梅,王胜开,陈国顺,等. 信息安全风险评估[M]. 北京:电子工业出版社,2007.
[4] 科飞管理咨询公司. 信息安全风险评估[M]. 北京:中国标准出版社,2005.
[5] 严霄凤,高炽扬. 美国联邦信息安全风险管理框架及其相关标准研究[J]. 信息安全与通信

保密,2009 (2):40 - 44.
[6] Alberts C, Dorofee A. 信息安全管理[M]. 吴晞, 译. 北京:清华大学出版社,2003.
[7] 李菁,赵捷,应力. 信息安全风险评估标准与方法综述[J]. 上海标准化,2006(5):13 - 17.
[8] 余勇. 基于 AS/NZS 4360:1999 的信息安全风险管理[J]. 信息安全与通信保密,2003(7):71 - 73.
[9] 束红,苏国平,费翔. 信息安全相关标准的分析与研究[J]. 网络安全技术与应用,2005(3):60 - 62.
[10] 祁明,翟才忠. 全球信息系统与安全产品评估准则的建立与发展[J]. 现代计算机,2001(10):74 - 76.
[11] 洪宏. CC 标准及相关风险评估系统关键技术研究[D]. 西安:西安电子科技大学,2004.
[12] ISO/IEC 27001:2005, Information technology—Security techniques—Information security management systems—Requirements[S]. Genevan: International Organization for Standardization,2005.
[13] ISO/IEC 27002:2005. Information Technology-Security Techniques-Code of practice for information security management [S]. Genevan: International Organization for Standardization, 2005.
[14] ISMS International User Group. International Register of ISMS Certificates[OL]. [2010-01-21]. http://www. iso27001certificates. com.
[15] 马燕曹,周湛. 信息安全法规与标准[M]. 北京:机械工业出版社,2004.
[16] 公安部、国家保密局、国家密码管理局、国务院信息工作办公室. 信息安全等级保护管理办法(公通字[2007]43 号)[OL]. [2008-07-28]. http://www. mps. gov. cn/n16/n1282/n3493/n3793/n494630/494907. html.
[17] Eloff J H P, Eloff M M. Information security architecture[J]. Computer Fraud & Security, 2005(11):10 - 16.
[18] 苏一丹,李桂. 基于 BS 7799/ISO 17799 的企业信息安全管理体系的构建[J]. 信息安全与通信保密,2004(6):52 - 54.
[19] 万会龙. 扣紧企业管理薄弱环节——戴明环环环相扣的管理模式解读[J]. 施工企业管理,2009(6):70.
[20] 李融,韩毅. 基于 PDCA 的数字图书馆质量管理研究[J]. 大学图书馆学报,2003(3):12 - 15.
[21] 夏立新. 数字图书馆导论[M]. 武汉:湖北人民出版社, 2004.

**茆意宏** 南京农业大学信息科学技术学院副教授。通讯地址:江苏南京卫岗 1 号。邮编:210095。
**黄水清** 南京农业大学信息科学技术学院教授。通讯地址同上。

(收稿日期:2010-02-05)