数字图书馆信息安全管理

SHUZITUSHUGUANXINXIANQUANGUANLI

黄水清 著

南京大学出版社

数字图书馆信息安全管理

黄水清 著

南京大学出版社

图书在版编目(CIP)数据

数字图书馆信息安全管理 / 黄水清著. — 南京 : 南京大学出版社, 2011.8
ISBN 978-7-305-08761-5

Ⅰ. ①数… Ⅱ. ①黄… Ⅲ. ①数字图书馆—信息系统—安全管理 Ⅳ. ①G250.76

中国版本图书馆 CIP 数据核字(2011)第 171833 号

出版发行 南京大学出版社
社　　址 南京市汉口路 22 号　　邮　编 210093
网　　址 http://www.NjupCo.com
出 版 人 左　健

书　　名 数字图书馆信息安全管理
著　　者 黄水清
责任编辑 胥橙庭　　编辑热线 025-83686308

照　　排 南京南琳图文制作有限公司
印　　刷 赣榆县赣中印刷有限公司
开　　本 787×960　1/16　印张 25.75　字数 490 千
版　　次 2011 年 8 月第 1 版　2011 年 8 月第 1 次印刷
ISBN 978-7-305-08761-5
定　　价 60.00 元

发行热线 025-83594756　83686452
电子邮箱 Press@NjupCo.com
Sales@NjupCo.com(市场部)

* 版权所有,侵权必究
* 凡购买南大版图书,如有印装质量问题,请与所购图书销售部门联系调换

前　言

发端于20世纪90年代的数字图书馆的研究及实践在全球蓬勃发展，伴随着数字资源的积累与网络存取的开放性，数字图书馆的信息安全问题成为数字图书馆实践与研究中的热点和前沿问题。

国外的统计表明，70%的信息安全事件产生的原因并不是来自外界的病毒和黑客，而是来自内部的未授权访问，许多信息安全问题仅仅依靠产品和技术根本无法解决，而应依靠技术与管理的结合，所谓“三分技术七分管理”。因此，国外学者提出了信息安全管理与信息安全技术并举的观点，并在实践上加以贯彻执行，制定了一系列信息安全管理的规范与标准，如美国卡内基·梅隆大学的OCTAVE、美国审计总署的GAO/AIMD—98—68和GAO/AIMD—99—139、澳大利亚和新西兰的AS/NZS 4360、美国国家标准和技术学会的NIST风险管理框架、国际标准ISO27000系列等。特别是ISO27000系列国际信息安全管理标准的发布，得到多个国家的认可与接受，在各个行业得到应用，中国国家质量监督检查检疫局、国家标准化管理委员会已接受并转化为对应的中国国家标准。

数字图书馆的信息安全管理是数字图书馆管理的组成部分，数字图书馆信息安全管理体系的建设是数字图书馆各项业务与服务功能正常开展的前提与保证。数字图书馆信息安全管理的必要性自不待言，但在当前数字图书馆信息安全管理的理论研究与具体实践过程中普遍存在重概念轻实施、重技术轻管理的倾向。同时，由于信息安全问题专业性强，牵涉面广，信息安全管理体系建设工作量巨大，数字图书馆在实施过程中常有无所适从之感或畏难情绪。

本书试图将在企业和政府机构得到广泛应用的信息安全管理标准引入数字图书馆领域，从规范管理行为入手提升数字图书馆信息安全水平，为数字图书馆的信息安全问题提供理论上完备、现实中具操作性、实施过程简便易行的解决方案，改变数字图书馆信息安全过于依赖防火墙、反病毒、用户访问控制的状况，在不提升技术条件的前提下解决数字图书馆信息安全管理的现实问题，并为数字图书馆信息安全的风险评估与风险控制提供模板，降低数字图书馆信息安全管理体系建立与实施的难度，减少工作量。以上工作在数字图书馆领域尚属首次。

本书的目标是希望从理论和操作层面上解决信息安全管理标准应用于数字图书馆信息安全管理可能存在的障碍。理论层面上，将在国际上得到广泛认同的信

息安全管理标准引入数字图书馆信息安全管理，确定数字图书馆信息安全管理体系建立和实施的原则、方法和流程；操作层面上，提炼数字图书馆风险评估与风险控制的模板，降低数字图书馆信息安全管理的操作难度，减少数字图书馆信息安全管理体系建立与实施的工作量。

归纳起来，本书主要解决了以下三个方面的问题：

将在世界范围内得到广泛认同的信息安全管理标准引入数字图书馆领域，在对国内数字图书馆的信息安全现状进行调查的基础上，结合数字图书馆信息安全管理的实际需要，确定了 ISO27000 系列标准为数字图书馆信息安全管理的依从标准。这是本书解决的第一个主要问题。

在数据调查的基础上，根据数字图书馆信息安全管理的现实情况，设计了基于模糊数学的资产价值评估模型、基于“构建威胁场景”的威胁等级评估模型、基于 CVSS 的脆弱性评价模型、数字图书馆风险值计算模型、基于投资约束和风险防范策略的数字图书馆风险控制决策模型、风险评估与风险控制间的联动关系三维坐标系（含已施加控制措施的风险值计算模型）。这是本书解决的第二个主要问题。

以数字图书馆业务流程、资产、威胁、脆弱性的调查数据为基础，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，提出了数字图书馆信息安全风险等级的划分方法，构建了数字图书馆风险评估的模板。可将数字图书馆信息安全风险评估过程很大程度上简化为查表过程，降低了数字图书馆信息安全风险评估的难度，减少了工作量。在分析、提炼数字图书馆核心控制要素的基础上，确定了数字图书馆的风险控制目标和组织控制措施与技术控制措施的实施方法，构建了数字图书馆风险控制模板。这是本书解决的第三个主要问题。

本书是在国家社科基金项目“数字图书馆信息安全管理与评价”（项目编号 07BTQ005）最终研究报告的基础上修改而成。作者指导的研究生任妮、熊健、陈双喜参与了项目的全部研究工作，深圳大学图书馆赵洗尘、南京图书馆吴政、南京农业大学图书馆查贵庭、对外经济贸易大学图书馆邱小红和范利群、东莞图书馆李东来和叶少青、大连理工大学图书馆金玉玲、浙江省图书馆范沈姗、浙江工商大学图书馆朱小玲等参与了项目的数据调查或专家咨询工作，在此一并致谢！

由于时间与作者水平的关系，书中存在许多不足甚至是错误。如，书中对某大学的数字图书馆信息安全的风险评估与风险控制，既没有得到长时间运行的有效性验证，也没有得到第三方认证机构的确认（即获得认证证书），作者的研究团队目前还未能开发出完整的数字图书馆信息安全风险管理软件系统，对于数字图书馆信息安全管理工作的具体实施会带来不便。作者希望专家和读者对书中的不足和错误给予批评指正。

此为试读，需要完整PDF请访问：www.ertongbook.com

目 录

图目录

此为试读，需要完整PDF请访问：www.ertongbook.com

表目录

第一章 绪 论

从20世纪90年代起，数字图书馆的研究及实践在全球蓬勃发展。从美国的数字图书馆先导计划、美利坚记忆和NSDL计划，到欧盟的“欧洲图书馆”以及中国的多项数字图书馆工程项目，在新技术的开发与应用、资源的积累、相关标准的制订、服务环境的建设等各方面都已经取得了很大的成就。伴随着数字资源的积累与网络存取的开放性，数字图书馆的信息安全问题成为数字图书馆实践与研究中的热点和前沿问题。

在当前的实际工作中，数字图书馆信息安全问题有重概念轻实施、重技术轻管理的倾向。同时，由于信息安全问题专业性强，牵涉面广，信息安全管理体系建设工作量巨大，数字图书馆在实施过程中常有无所适从之感或畏难情绪。研究数字图书馆信息安全风险评估与风险控制，目的是为数字图书馆的信息安全问题提供理论上完备、现实中具操作性、实施过程简便易行的解决方案，改变数字图书馆信息安全管理过于依赖防火墙、反病毒、入侵检测的现状，在不提升技术条件的前提下解决数字图书馆信息安全管理的现实问题，促进数字图书馆事业的发展。

目前，国内外数字图书馆界对信息安全的概念与重要性已有了较清楚的认识。近年来，国内外对数字图书馆信息安全的研究主要集中在技术、管理与法律法规三个方面。目前国内的绝大部分研究都着重于技术，即计算机与网络安全技术在数字图书馆的应用。如：数据备份与软件更新、密码技术、杀毒软件、身份认证与访问控制、防火墙技术、漏洞扫描与检测等。管理方面，国内有研究者在分析管理的重要性的基础上，从人员管理、设备管理、灾难恢复制度、用户与员工的培训和监督方面提出了某些一般性的管理措施。国内也有学者强调了法律法规建设的重要性，并提出要加强执行力度。法律法规在国外的研究中被纳入管理的范畴，即管理措施应符合法律法规的要求、安全风险控制在法律法规许可范围内。总的来看，国内有关数字图书馆信息安全管理方面研究缺乏系统性，研究内容显得比较空泛，没有可操作的解决方案。

国外统计表明，70%的信息安全事件产生的原因并不是来自外界的病毒和黑客，而是来自内部的未授权访问，许多信息安全问题仅仅依靠产品和技术根本无法解决，而应依靠技术与管理的结合，所谓“三分技术七分管理”。因此，国外学者提出了信息安全管理与信息安全技术并举的观点，并在实践上加以贯彻执行，制定了

一系列的信息安全管理的规范与标准。如:美国卡内基·梅隆大学的 OCTAVE、美国审计总署的 GAO/AIMD—98—68 和 GAO/AIMD—99—139、澳大利亚和新西兰的 AS/NZS 4360、美国国家标准和技术学会的,NIST 风险管理框架、国际标准 ISO27000 系列等。特别是 ISO27000 系列国际信息安全管理标准的发布,得到多个国家的认可与接受,在各个行业得到应用,中国国家质量监督检查检疫局、国家标准化管理委员会已接受并转化为对应的中国国家标准。

数字图书馆的信息安全管理是数字图书馆管理的组成部分,数字图书馆信息安全管理体系的建设是数字图书馆各项业务与服务功能正常开展的前提与保证。数字图书馆信息安全管理的必要性自不待言,但在理论研究与具体实践过程中应既牢记其他行业"三分技术七分管理"的宝贵经验,又遵循国际国内强制性及得到广泛认可的各项推荐标准与规范。

基于其他行业信息安全领域的研究成果与实践经验,可以得出这样的结论:解决信息安全管理问题的主要出路在于管理体系,数字图书馆也是如此。数字图书馆可以在不提升技术水平的前提下依靠管理的改进大幅提高数字图书馆信息安全的层级、降低安全风险,并且针对数字图书馆这一特定类型的信息系统,可以制定出操作性很强的风险评估与风险控制模型,供数字图书馆使用。

将在企业和政府机构得到广泛应用的信息安全管理标准引入数字图书馆领域,从规范管理行为入手提升数字图书馆信息安全状况,改变数字图书馆信息安全过于依赖防火墙、反病毒的状况,并强调安全管理的操作性,为数字图书馆信息安全的风险评估与风险控制提供模板,降低数字图书馆信息安全管理体系建立与实施的难度,减少工作量。这就是本书的目标。为了实现这一目标,须将信息安全领域的标准和规范应用于数字图书馆这一业务趋同性很强的特定组织类型,设计数字图书馆信息安全风险计算和风险控制数学模型,在数据调查的基础上总结出数字图书馆风险评估与风险控制的模板,制定数字图书馆信息安全管理的方法和步骤,并用实际数字图书馆的信息安全管理实践验证模型、模板和方法的可行性。

为了从现实的数字图书馆信息安全管理工作中总结带普遍性的原则与规范,需要以国内建设情况较好的有典型性与代表性的数字图书馆为调查对象,针对数字图书馆建设现状,信息安全管理现状,数字图书馆业务流程,数字图书馆资产及估值、威胁及估值、脆弱性及估值、风险控制措施等方面进行数据调查。整个数据调查过程比较复杂,涉及的因素较多,某种意义上相当于对所有被调查的数字图书馆做一遍粗略的风险评估与风险控制措施筛选。

本书将数字图书馆定位于建立在传统的实体图书馆之上的数字图书馆部分。参与调查的数字图书馆应该属于某个已开展传统的图书馆服务的实体图书馆,在此前提下,该馆的服务理念和建设规划应该遵循数字图书馆的要求,拥有一定的数

字资源，并且已经开展相关的数字图书馆业务，这是数字图书馆信息安全管理调查对象的基本要求。

最终参与调查的数字图书馆为全国三十家已经建设有数字图书馆部分的公共图书馆和高校图书馆。其中，公共图书馆有省级馆、地市级馆和县级馆三种，高校图书馆有综合类、理工类、经济类、农林类、医药类等多种。数字图书馆建设需要大量的资金支持，因此调查对象选定为在数字图书馆建设方面有一定基础的发达地区的图书馆。调查范围覆盖了江苏、浙江、广东、辽宁、北京、上海四省和两直辖市，所处的城市包括南京、北京、上海、杭州、苏州、常熟、张家港、常州、广州、深圳、东莞、大连等，均为经济发达地区。

所有参与调研的图书馆除了保留有传统的采编、流通等图书馆业务外，都不同程度地开发建设有数字图书馆，并且开展了文献传递、特色数据库建设、参考咨询、馆际合作、个性化服务等活动和服务，工作重心逐渐向网络化、数字化方向转移。这些图书馆有各自自成体系的常规业务和特色业务，符合数字图书馆信息安全管理调查的基本要求。

参与调研的公共图书馆有 10 家，比例为 33.3%，高校图书馆有 20 家，比例为 66.7%。其中公共图书馆中，省级馆有 2 家，占全部参与调研的公共图书馆的 20%，地市级图书馆有 6 家，占全部参与调研的公共图书馆的 60%，县级市馆有 2 家，占全部参与调研的公共图书馆的 20%。

从地区分布来看，全部参与调研的图书馆中，来自辽宁的图书馆占 3.3%，来自浙江、上海的图书馆各占 6.7%，来自北京的图书馆占 13.3%，来自广东的图书馆占 20%，来自南京的图书馆占 30%，来自除南京以外的江苏其他地区的图书馆占 20%。

由于需要调查掌握的数据繁多，且许多数据即使数字图书馆的工作人员也没有现成答案，需要调查人员与被调查对象经过长时间的沟通、交流与探讨才能得出一个基本满意的答案，因此，数据调查过程不能采用简单的问卷发放、填写与回收的办法，而是多种调查方法的结合。具体来说，整个调查过程用到了走访与面谈、利用现代通信工具进行沟通、网站调查、现场考察、专家访谈、问卷填报等多种调查方法。

本书主要包括七个方面的内容：

(1) 对国内数字图书馆建设与信息安全管理现状的调研。

在梳理数字图书馆与信息安全管理相关概念及国内外研究现状的基础上，本书以经济发达、数字图书馆建设基础较好的北京、上海、广州、深圳、杭州、大连、南京及苏南地区的数字图书馆的调查数据为依据，对国内数字图书馆建设与信息安全管理的现状进行了阐述，统计了数字图书馆出现的安全事件与应对措施，分析了

此为试读，需要完整PDF请访问：www.ertongbook.com