《数字图书馆安全管理指南》解读

赵 亮 刘 炜 徐 强

摘 要 对数字图书馆安全及信息安全的概念进行辨析,指出数字图书馆安全本质上就是一个信息安全问题。通过对国内外数字图书馆安全问题的研究以及对信息安全相关标准体系的详细考察,并通过对 ISO 15408、ISO 13335、ISO 27000、GB 17859 和 GB 20269 等信息安全领域几个重要的国际国内标准进行介绍,对《数字图书馆安全管理指南》的参考标准与指导思想进行说明,对指南的具体内容进行解读。图 5。参考文献 36。

关键词 数字图书馆 信息安全 标准 指南

分类号 G258.6

ABSTRACT By analyzing the concepts of digital library security and information security, the paper argues that digital library security is actually being part of the information security domain. With comprehensive investigation on researches about digital library security and standards framework of information security, including explaining some important international or national standards such as ISO 15408, ISO 13335, ISO 27000, GB 17859 and GB 20269 more clearly, the paper introduces the basis and all references used by *A Guide to Digital Library Security Management*. At last, the paper explains *the Guide to Digital Library Security Management* with more detailed information. 5figs. 36 refs.

KEY WORDS Digital library. Information security. Standards. Guide.

CLASS NUMBER G258.6

由上海图书馆主持编写的《数字图书馆安全管理指南》(以下简称《指南》),经过大半年的拟订修改,获得全国数字图书馆建设与服务联席会议成员审议通过,于2010年中国图书馆学会年会期间正式发布。《指南》明确了数字图书馆安全所涉及的概念定义,提出了数字图书馆安全管理中所需关注的相关要素,并从政策、过程、实施过程中的控制环节、资源与环境以及应急与处置等诸多方面提出了原则性的指导意见。本文将对《指南》进行解读,重点介绍有关数字图书馆安全管理的相关标准与规范以及《指南》制定的原则与思路,最后是对一些具体条款的解读。

1 数字图书馆安全概览

1.1 数字图书馆安全与模型

数字图书馆的安全问题是数字图书馆建设与服务中一个最重要的保障性难题,没有安全的保障,资源与系统得不到保护,有效的服务也难以为继。

从基本要素来说,数字图书馆具有资源、服务与网络三个要素。早期的数字图书馆安全研究更多关注资源安全与服务保障两个层面的问题。20世纪90年代中后期,国际上有许多针对数字图书馆建设与服务环境中安全问题的研究,如1997年至1998年著名的数字图书馆网刊D-Lib杂志刊发了一系列有关数字图书馆安全技术方面的文章。这一系列文章从保护资源内容与用户的主题出发,讨论了方方面面的问题,比如加解密技术[1]、保密技术与相关机制[2-3]、数字水印技术[4]、数字资源全球统一标识问题[5],甚至还包括对数字图书馆服务过程中的付费机制的讨论[6]以及对数字内容知识产权保护的技术解决方案的讨论[7],并且还对数字图书馆建设中的安全相关议题作了总结[8]。上述文章是早期数字图书馆研究与实践中有关安全

议题的标杆之作，也是少有的系统性讨论数字图书馆领域中安全问题的文章。20 世纪的数字图书馆安全相关议题强调的是内容资源的安全及用户访问控制。进入 21 世纪以来，海外的数字图书馆专业研究中有关安全的讨论，要么是深入到技术领域，进入专业信息技术领域专家们的研究范畴；要么是归入到管理范畴，更多地是从依从标准、适用规范的角度来讨论相关议题。例如，有关加解密及其他越来越复杂的安全技术，已经成为计算机行业专家研究的重点。在美国 911 事件之后，有关信息安全的技术研究更是信息技术领域研究中最重要的主题。

由于国内在数字图书馆建设方面与国际上有一定的时间落差，关注数字图书馆安全的研究文章大都见诸于 21 世纪初至今的图情专业期刊上。2005 年，李媛的《近五年来数字图书馆信息安全问题研究综述》一文对 2000—2004 年间有关数字图书馆安全议题的学术文章共计 119 篇进行了综合分析，对其研究内容以及一些趋势性的问题作了研判[9]。李媛提出，数字图书馆信息安全具有保密性、完整性、可用性、广泛性、动态性的特点，而解决数字图书馆信息安全问题的对策可以有技术手段、管理手段及法律和行政手段等。可以看出，国内相当多的图情研究者在关注技术问题的同时，已将眼光转向了信息安全领域的一些标准规范，引用了信息安全领域的相关定义与描述。郑德俊等统计了与数字图书馆信息安全有关的研究论文发文情况，发现有关文献呈逐年上升趋势，从 2000 年的 3 篇文献发展到 2009 年的 70 篇，表明数字图书馆信息安全问题是一个热点话题[10]。近年来，与国外同行研究特点相似，有关数字图书馆安全的纯技术性讨论往往是信息技术专业领域的研究重点，但国内图情业界对数字图书馆安全除了一些对技术与管理进行描述的泛泛之作外，更多地是关注如何运用信息技术领域的相应标准与规范来指导数字图书馆建设与服务中与安全相关的管理与实践，《数字图书馆信息安全管理依从标准的选择》[11]一文即为代表。

笔者接手编写《指南》的任务之后，查阅了大量文献，然后结合自身实践，理出了大致的思路结构（图 1）。但是经过进一步的学习研究之后发现，该大纲虽然具有一定的合理性与完整性，但全面性与规范性不足，在指导数字图书馆的信息安全实践工作时，难免挂一漏万；同时，这样的构架与行文对于实践的指导意义也偏弱一些。因此，我们重新整理思路，将直接解决数字图书馆安全管理的难题转变到找寻数字图书馆安全管理的所属领域，进而在这个领域范畴中找寻相关的标准、规范与参照指南。

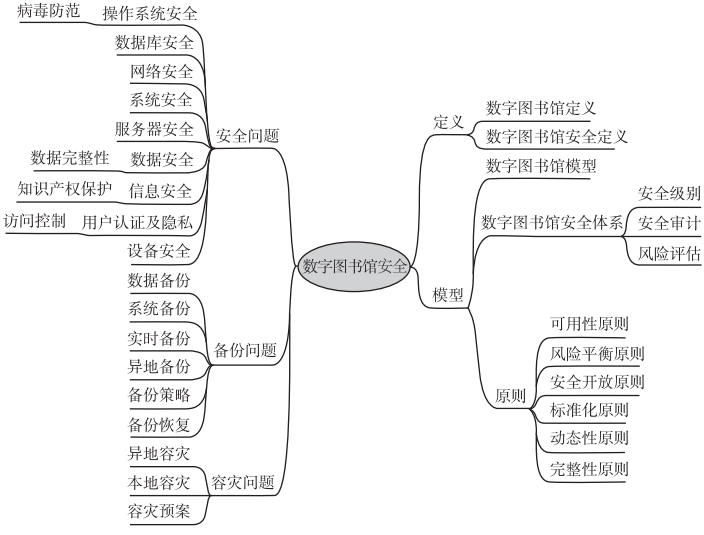

图 1　数字图书馆安全相关问题纲要

1.2 数字图书馆安全问题的本质就是信息安全问题

对于什么是数字图书馆的安全问题,文献[9]中引用了许多人的定义与讨论。有人认为"图书馆的信息安全目前主要指信息技术系统的安全和馆藏信息的安全。"[12]有人认为"网络安全是指为维护网络正常运转所采取的技术性和管理性措施。其目的是保证网络系统的硬件、软件、数据等不因无意的或故意的原因而出现故障或遭到破坏、变更或泄露,它包括硬件安全、软件安全、数据安全和运行安全等4个方面。"[13]也有人认为"数字图书馆的网络安全是一个系统概念,是指数字图书馆网络系统的各个组成部分不受偶然的或恶意的原因而遭到破坏、篡改和泄露,并且确保数字图书馆网络系统能连续正常运行的机制,其最终目的是要达到数字图书馆网络信息处理和传输过程中保持可靠的机密性、完整性、可用性、可控性和可审计性以及对信息处理传递行为的抗抵赖性。数字图书馆的计算机网络安全技术就是指为数字图书馆数据处理系统的建立和正常运行所采用安全管理和安全保护的技术。"[14]

如前所述,笔者认为数字图书馆具有对数字资源在网络环境下进行组织、管理、服务的技术形态特征。虽然它在实际应用中或多或少地更为关注数字信息内容的管理与服务,但它还是一个通常意义上的典型的信息系统。上面介绍的这些定义与论述,有的是从具体技术要素,有的是从系统观念来讨论数字图书馆安全问题的内涵外延,但无一例外地没有跨出信息系统的边界。数字图书馆所具有的网络环境下的服务与分布式架构的特点,也与通常的网络环境下的信息系统架构并无不同。因此,制定数字图书馆系统安全相关的策略,架构数字图书馆的安全技术体系,其实质就是一个信息安全问题。很多关于数字图书馆安全的论述就是直截了当地拿其当作信息安全问题来讨论[15]。我们在撰写《指南》时,也是基于这样的一个原则,在普遍意义上的信息安全标准、技术与方案基础上找寻合理的参照目标,藉以剪裁较为现实的实施指南。在后文中提到数字图书馆安全管理时,我们也采纳"数字图书馆信息安全管理指南"的说法。

2 信息安全概念与信息安全相关标准体系

2.1 信息安全概念

在最新的信息安全管理国际标准ISO 27000-2009[16]中对信息安全的定义是:"信息安全就是保持信息的保密性、完整性与可用性。"其中保密性(confidentiality)是指信息将不会被披露或被未授权的个人、实体或其他计算机处理进程所获取。完整性(integrity)是指要保护信息资产的准确与完整性。可用性(availability)是指信息能被经授权的实体可访问及使用。然而在GB/T 19715.1-2005[17](等同采用ISO 13335-1-1996[18])中对信息安全给出了包含保密性、完整性、可用性、可核查性、真实性、可靠性的定义。其中可核查性(accountability)是指确保可将一个实体的行动唯一地追踪到此实体的特性;真实性(authenticity)指确保主体或资源的身份是所声称身份的特性,适用于诸如用户、过程、系统和信息这样的实体;可靠性(reliability)是指与预期行为和结果相一致的特性。ISO 13335-1对信息安全作出了内涵更为丰富的定义,然而其内容的实际内涵很大程度上包含在ISO 27000-2009的定义之中。例如可核查性的内涵可以体现在保密性中,真实性可以体现在可用性中,而可靠性则可以体现在完整性中。另外,鉴于标准依从中从新的原则,我们还是采用2009年发布的ISO 27000-2009中的定义,取代1996年发布的ISO 13335-1中的定义,以保密性、完整性、可用性的原则来讨论信息安全的问题,这一定义也是绝大多数标准与指南所采用的通用说法。

2.2 信息安全技术标准体系

信息安全作为一个具有普遍性及行业应用特征的技术与系统要求,并不是一个研究性的课题对象,因此实现信息安全目标最好的方法

是参考或依从一些相关国际、区域、国内或行业标准等。我们在考虑参考或依从何种信息安全标准之前,有必要先考察一下与信息安全相关的整个标准体系。

从信息安全的实现要义来说,无非是预估或发现风险,然后加以防范与控制,从而实现信息安全的目标。但是,在信息安全相关的实践中,整个安全体系覆盖信息系统生命周期的各个阶段,包括设计、开发、实施、测试、运行、维护等。整个流程中涉及信息安全的方方面面,包括安全需求的定义、风险的评估、安全技术的采用、安全测评服务、安全机制的构建、安全的管理、安全产品及系统、安全的行业性应用与安全要求等。可以说,信息安全涉及的层面相当广泛,相应的安全标准也相当繁杂。

由于信息安全标准的复杂性,不同研究人员与机构都提出了自己的信息安全标准体系框架。黄元飞认为信息安全标准体系涉及基础标准、技术标准、应用标准、服务标准和管理标准等五类标准[19]。来自全国信息安全标准化技术委员会的林宁与吴志刚则认为我国信息安全标准体系已初步形成,该体系包括基础标准、技术与机制标准、管理标准和测评标准[20]。周鸣乐等人认为我国的信息安全标准体系包括基础标准、技术与机制、管理标准、评测标准、密码技术和保密技术等六类[21]。这一构架其实与林宁和吴志刚提出的标准体系框架是完全一致的,只是由于密码技术与保密技术在信息安全标准中占有一定的数量,因此也有研究者或管理机构将其从基础标准中分出来单列,以便于区分与管理。

关于信息安全技术标准体系,赵文等从现有的标准分类角度作了梳理和分析,认为国内现有的已发布或正在制订的信息安全正式标准、报批稿、征求意见稿和草案等大体上可以分为信息安全体系标准、信息安全机制标准、信息安全管理标准、信息安全工程标准、信息安全测评标准、信息系统等级保护标准和信息安全产品标准等七大类[22]。

综上分析,可以看出研究者在对信息安全技术相关标准的认识与结构定义上保持了相当的一致性。我们认为,可以将整个信息安全技术标准体系提炼为四大类,分别是基础类、技术与机制类、安全管理类以及应用类,四者之间的相互关系如图2所示。

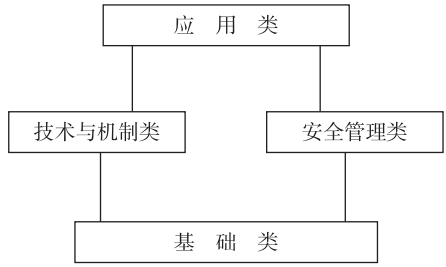

图2 各类标准之间的关系[21]

图2解析了信息安全标准之间的关系与内在逻辑。基础类标准包括对信息安全的一些最基本的技术与规范,如相关术语定义、有关信息安全的体系与模型定义、安全领域定义的整体要求与技术架构等,例如OSI安全体系结构标准以及其他网络基础架构中有关安全的结构等。技术与机制类标准则包括与信息安全相关的所有技术标准,包括技术类的具体要求、加密技术、保密技术(访问控制)、物理环境的安全规范、软件与应用系统的安全规范、标识与鉴别标准规范等。安全管理类标准则是关于指导整个信息安全技术实施的一些管理内容与实施手段的规定,如管理基础、管理要求、管理内容、管理实施等方面内容。管理类标准不仅仅是工程性管理层面的内容,同样也有对具体对象标的的管理内容,如数据管理的标准、网络管理的标准以及系统管理的标准等。应用类标准主要包括测评类标准,是对计算机系统、网络通信以及相关信息技术安全产品进行安全水平测定或评估的一类标准,包括评估的基础、评估的方法手段、产品与系统的测评等几个层面,也包括信息安全系统的等级划分与评估等。

在这四类标准中,基础类标准是信息安全的基石,也是所有其他标准的基础与出发点。技术与机制类标准则定义了信息安全技术实施中的一些适用技术、相应要求规范与实施标准,技术含量高,时效性很强,适用于提供安全

服务的公司、大型安全工程项目以及安全相关的产品开发与应用选择依从参照。安全管理类标准则可以看成是信息安全技术实施中的指导原则与实施指南,对如何实现信息安全的架构体系,对整个信息安全技术实施中的流程提出实施的模型、原则与具体建议。该类标准适用的对象面更广,可参照性更强,时效性也不太强。应用类标准大多与评测及产品相关,基本上限于为一些专业提供安全服务的实体或其他一些提供安全产品的第三方公司等参照选用。

从广义上讲,数字图书馆的安全管理需求与信息安全管理需求是一致的。首先,从自身的特点来说,数字图书馆更为强调数字化信息内容资源的管理以及对整个信息服务系统安全的关注,这些都没有超出一般意义上的信息安全领域,就是说没有超出信息安全技术标准体系的范畴。从理论上讲,整个信息安全技术标准体系都是数字图书馆安全应该参照或依从的标准规范,然而信息安全技术标准体系太过细致繁杂,有些标准的技术内容要求非常高,时效性非常强。其次,从安全的具体实施来说,往往有三分技术、七分管理的特点。安全技术固然重要,但安全管理的体系与相关制度的建设,以及人员的实际运作管理能力更为重要。因此在整个信息安全技术标准体系中,最需要参考的是信息安全技术基础及管理类的标准,严格说来,还仅仅是涉及到这些标准门类中很少的一部分。下面我们将重点介绍几个信息安全相关标准,从中寻找数字图书馆安全所应依从的最重要标准,并结合《指南》的立意与需求,提炼《指南》写作中最重要的素材内容。

3 信息安全管理相关标准

3.1 ISO 13335 信息技术安全管理指南

ISO/IEC 13335 信息技术安全管理指南(Guidelines for the Management of IT Security, GMITS)是于 1996 年起陆续发布的一项标准。它是 ISO/IEC JTC1 制定的技术报告,是一项信息安全管理方面的指导性标准,其目的是为有效实施信息技术安全管理提供建议和支持。

ISO/IEC 13335 有两个特点:一是更细致地提出了一些信息技术安全管理的具体措施;二是提出了一个以风险为核心的安全关系模型,定义了一些关键要素。ISO 13335 所定义的风险关系模型如图 3 所示。

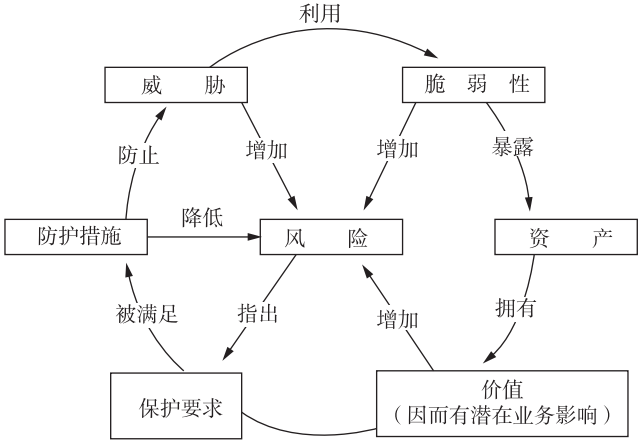

图 3 ISO 13335 所定义的风险关系模型[18]

图 3 清晰地说明了信息技术管理中风险控制相关的各要素之间的关系,它们的相互影响

与作用,以及如何通过不断完善的过程来更好地保护组织的资产并控制风险。风险管理应该是一个循环往复、不断改进的过程。

ISO/IEC 13335 - 1:1996 和 ISO/IEC 13335 - 2:1997 于 2005 年被等同采纳为中国国家标准,分别是 GB/T 19715.1 - 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与 GB/T 19715.2 - 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。而 ISO/IEC 13335 - 1:1996 和 ISO/IEC 13335 - 2:1997 本身已被新版的 ISO/IEC 13335 - 1:2004 信息技术 - 安全技术 - 信息和通信技术安全管理第 1 部分:信息和通信技术安全管理的概念和模型(Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management)所取代。另外 ISO/IEC 13335 - 3:1998 和 ISO/IEC 13335 - 4:2000 被 ISO 27000 标准族中的 ISO/IEC 27005:2008 信息技术 - 安全技术 - 信息安全风险管理指南(Information technology — Security techniques — Information security risk management)所替代,ISO/IEC 13335 - 5:2001 则被 ISO/IEC 18028 - 1:2006 信息技术 - 安全技术 - 信息技术网络安全第 1 部分:网络安全管理(Information technology — Security techniques — IT network security — Part 1: Network security management)所取代。因此原 ISO 13335 标准从"信息技术安全管理指南"(即 GMITS)转变到如今的"信息和通信技术安全管理"(即 MICTS),扩大了应用领域,但精简了整个标准体系。

3.2 ISO 15408 信息技术安全性评估准则

ISO/IEC 15408:1999 信息技术 - 安全技术 - 信息技术安全性评估准则(Information technology — Security techniques - Evaluation criteria for IT security),是第一个世界通用的信息技术安全评价标准,此标准也是现阶段最完善的信息技术安全评估标准。

1991 年欧盟颁布了信息技术安全评估准则(Information Technology Security Evaluation Criteria, ITSEC)。在此基础上,美国、加拿大、英国、法国等 7 国联合组织研制了"信息技术评估安全公共准则"(Common Criteria for Information Technology Security Evaluations)。1999 年 6 月 ISO 通过了 ISO/IEC 15408:1999(实际上由三部分组成,标准号分别为 15408 - 1、15408 - 2 和 15408 - 3),因它是由当初的 Common Criteria 演变而来,所以也通常被简称为 CC 标准。

CC 标准中讨论更多的是评估对象(Target of Evaluation, TOE),它专注于评估对象的安全功能,以及这些安全功能执行的是何种安全策略。它定义了安全属性,包括用户属性、客体属性、主体属性和信息属性,加强了完整性和可用性的防护措施,强调了抗抵赖性的安全要求,以及许许多多其他的安全要求。CC 标准还采用了安全工程的思想,通过对信息安全产品开发、评价、使用全过程的各个环节实施安全工程来确保产品的安全性,强调在信息技术产品与信息系统的整个生命周期确保安全性。CC 标准的许多条款与技术规定十分专业、细致与具体,适用于专业的安全服务商与安全产品生产厂商参照应用。

CC 标准也提出了自己的安全模型(图 4),这一安全模型与 ISO 13335 的风险管理关系模型有着异曲同工之妙。

2001 年,国内发布了等同采用 ISO/IEC 15408:1999 标准的 GB/T 18336 - 2001(依次分别为 GB/T 18336.1 - 2001[23]、GB/T 18336.2 - 2001、GB/T 18336.3 - 2001 三个标准)。2008 年,国内又发布了等同采用 ISO/IEC 15408:2005 的 GB/T 18336 - 2008(依次分别为 GB/T 18336.1 - 2008[24]、GB/T 18336.2 - 2008[25]、GB/T 18336.3 - 2008[26]三个标准)。CC 标准本身也在不断地发展,其最新版本分别是:ISO/IEC 15408 - 1:2009、ISO/IEC 15408 - 2:2008 和 ISO/IEC 15408 - 3:2008。

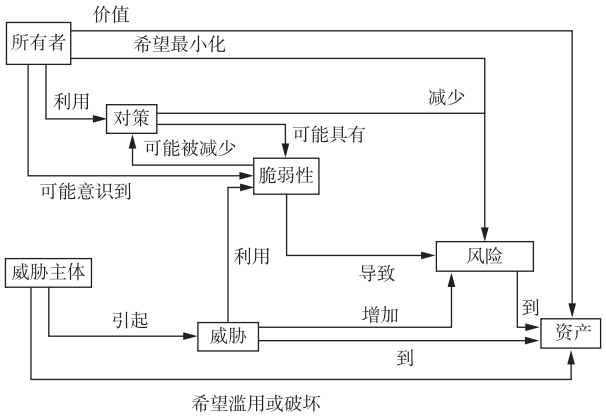

图 4 CC 标准中的安全概念和关系[23]

3.3 ISO 27000 系列信息安全管理系统

1993 年,由英国贸工部组织,许多企业参与编写了一个信息安全管理的文本"信息安全管理实用规则"(Code of practice for information security management)。这是著名的英国国家标准 BS 7799 的前身。1995 年,该文本被转化为英国国家标准,即 BS 7799 - 1:1995 信息安全管理实用规则。1998 年,英国又推出了 BS 7799 - 2:1998 信息安全管理体系规范(Specification for Information Security Management System),这就是后来俗称的 ISMS 名称的由来。

2000 年 12 月,BS 7799 - 1:1999 被采纳成为国际标准,即 ISO/IEC 17799:2000。但是 BS 7799 - 2 当时并未能够成为国际标准,后来 BS 7799 - 2 重新修订,推出了 BS 7799 - 2:2002。2005 年 ISO/IEC 发布了 ISO/IEC 17799:2000 的修订版本,即 ISO/IEC 17799:2005。同年,ISO/IEC 在 BS 7799 - 2:2002 基础上发布了 ISMS 规范要求标准,即 ISO/IEC 27001:2005。2007 年,ISO/IEC 17799:2005 也被重新更名为 ISO/IEC 27002:2005(内容不变),至此 ISO 27000 系列标准已经自成体系并得到了很好的发展。

源自 BS 7799 的信息安全管理体系规范及其实用规则是应用相当广泛,且在信息安全领域最具影响力的信息安全标准,ISO 27000 系列继承了这一血统并得到了很好的发展。除 27001、27002 以及不久前发布的 27000 以外,目前 ISO 27000 系列的后续标准形成了一个复杂而庞大的体系。这里主要介绍 ISO 27001 与 ISO 27002 标准。

ISO/IEC 27002:2005 信息技术 - 安全技术 - 信息安全管理实用规则(Information technology — Security techniques — Code of practice for information security management)[27] 是 2007 年为替代 ISO/IEC 17799:2005 标准而发布的,只是更改了相应的标准序号,内容并无变更,目的是使相关的标准都统一到 ISO 27000 标准系列之中。该标准包含 11 个主题,定义了 39 个控制目标、133 个控制措施。

ISO/IEC 27001:2005 信息技术 - 安全技术 - 信息安全管理体系 - 要求(Information technology — Security techniques — Information security management systems — Requirements)[28] 是建立信息安全管理体系(ISMS)的一套规范,其中详细说明了建立、实施和维护信息安全管理体系的要求,指出了实施机构应该遵循的风险评估标准。作为一套管理标准,ISO 27001 指导相关人员怎样去应用 ISO/IEC 27002:2005,最终目的还在于建立适合企业需要的信息安全管理体系。

ISO/IEC 27001:2005 采用过程方法来建立、实施、运行、监视、评审、保持和改进组织的

ISMS。它使用了一个被称为“规划(Plan)— 实施(Do) —检查(Check) —处置(Act)”(PDCA)的模型来应用这一过程方法(见图5)。该模型说明了ISMS如何把相关方的信息安全要求和期望作为输入,并通过必要的行动和过程,产生满足这些要求和期望的信息安全结果。

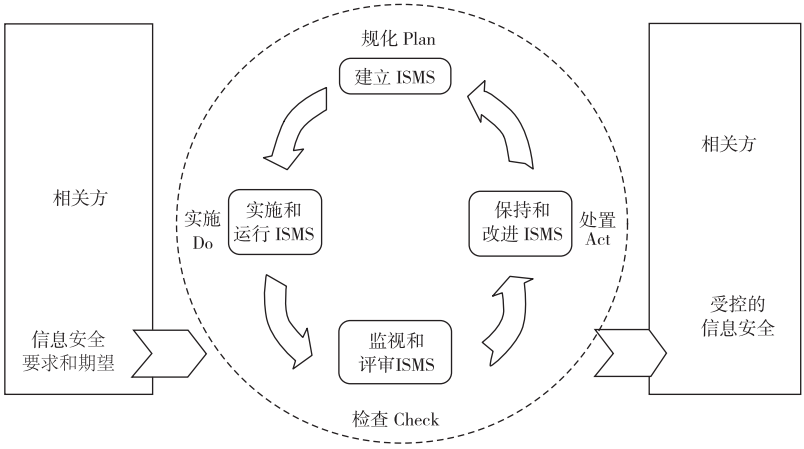

图5 应用于ISMS过程的PDCA模型[28]

2008年,国家标准化委员会发布了等同采用ISO/IEC 27001:2005的GB/T 22080-2008信息技术-安全技术-信息安全管理体系-要求[28]以及等同采用ISO/IEC 27002:2005的GB/T 22081-2008信息技术-安全技术-信息安全管理实用规则[27],后者同样替代了原等同采用ISO/IEC 17799:2000的GB/T 19716-2005。

3.4 GB 17859-1999 计算机信息系统安全保护等级划分准则

2007年,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部门,在2006年发布试行办法的基础上,正式发布了《信息安全等级保护管理办法》[29],要求各单位遵照执行。方法中提到信息系统的安全等级划分应依照由公安部主持制定、国家质量技术监督局发布的GB 17859-1999计算机信息系统安全保护等级划分准则[30]的标准予以执行。

GB 17859-1999与前面提到的其他等同采用国际标准的一些安全管理国家标准有显著的不同。GB 17859-1999是强制性国家标准,而其他标准都属于推荐标准。

3.5 GB/T 20269-2006 信息安全技术-信息系统安全管理要求[31]

2006年发布的GB/T 20269-2006可以看作是GB 17859-1999的一个具体实施指南,并且GB/T 20269-2006正是参照了ISO 13335及ISO 17799(即以后的ISO 27002)之后所编制出的一个国家标准,其安全理念模型和安全要素与所参照的这些国际标准保持一致,是这些在信息安全领域最具影响力的国际标准的本地化版本,更符合国内的现状与语境。

GB/T 20269-2006确定了信息安全管理要素,并且在GB 17859-1999所定义的每一个信息系统安全要求等级上都注明了各个管理要素的控制措施与强度,可以看作是国际标准要素与国内安全需求结合得很好的解决方案。

4 《指南》解读

4.1 《指南》编写的出发点

数字图书馆的安全问题是一个非常广泛及复杂的系统性问题。但是编写《指南》的立意是什么?它能起到什么作用呢?

笔者认为《指南》的编写可以起到如下作

用:①加强大家对数字图书馆安全管理概念的认识,增进对数字图书馆安全的重视,进行安全教育,普及安全理念,促使大家较全面地考虑安全问题。②通过《指南》简明扼要地普及安全管理的思想,使大家能认识到数字图书馆安全实践中管理胜于技术的观念。③在具体的数字图书馆建设与运行维护中,《指南》将指导大家的具体实践工作。④引导大家关注相应的信息安全规范标准,理解各种不同的安全模型,学习结合各种概念,根据具体的系统与项目要求、各单位的具体情况与人员及各种资源的具体情况,选择各自的依从标准或规范,从而有效地解决数字图书馆安全问题。⑤《指南》与数字图书馆联席会议所制定的其他指南一起,形成一个有机的整体,也是其他指南的有效补充。

4.2 《指南》的主要依从与参照标准

前面介绍了一些与信息安全相关的标准体系与重要标准,但哪些内容是我们编写《指南》最重要的参考或者说依从标准呢? 茆意宏和黄水清的《数字图书馆信息安全管理依从标准的选择》[11]一文对此作了很好的回答。该文有理有据地论述了数字图书馆信息安全管理依从标准的问题,认为"数字图书馆信息安全管理最合适的依从标准应该是 ISO 27000 标准系列",笔者对此结论完全赞同。

但是,选用 ISO 27000 标准族作为依从标准对数字图书馆信息安全管理来说显然是一个过大的帽子,我们必须在其中选择更合适精简的目标。经过仔细对照与评判,我们最后选择了 ISO 27002(即 GB/T 22081 - 2008)的内容作为《指南》文本的主要参照。因为 ISO 27002 本身具有一个安全系统架构与实施中的指南文本的性质,其内容与行文较符合数字图书馆安全管理指南文本的需要。当然,《指南》作为一个简单的文本,不可能照搬甚至是全盘采纳 ISO 27002 的纲要体系,我们根据自己的理解与选择,选取了其中的若干安全主题进行描述,在行文中主要参照其控制措施的部分。并且在实际行文中,《指南》还更多参考了比较本地化的 GB/T 20269 - 2006,该标准所描述的要素内容以及文本风格更易为我们的用户所接受。同时,《指南》也参照了 ISO 13335 标准族(即 GB/T 19715)、ISO 15408 标准族(即 GB/T 18336)以及 GB 17859 - 1999 的内容。

4.3 《指南》的特点

4.3.1 《指南》是融合参照各安全标准与实践的一个普及性的简要指南

《指南》的内容不仅仅参照了相关标准,也参照了国内外的研究成果,尤其是图情行业的一些论文著述,可以说,是一个混搭的文本。同时,考虑到国内数字图书馆事业实际发展状况与人员水准,《指南》在语言上力求简单平实。即使在参照各标准的相关描述、控制措施及其他内容时,也在文本上予以简化,力求更易为大家所接受。

4.3.2 《指南》简化了信息安全的描述与定义,简化了相关要求

《指南》中最重要的一个条款是对安全的定义与描述:

> 本指南中所称"数字图书馆安全管理",是指保护数字图书馆中的信息系统相关资产免受任何可能的威胁和损失,保持其中信息资源完整性和可用性并保障其实现所设定信息服务和其它功能的行为。数字图书馆中的信息系统相关资产可包含物理资源、软件资源与信息资源等。其中信息资源是指以数字形式发布、存取和利用的信息资源总和。

从该款规定可以看出,《指南》没有强调传统信息安全的保密性、完整性与可用性的定义,而是将其简化为信息系统与信息资源的安全,三性隐含其中。《指南》没有强调保密性,因为从字面意义上讲,保密性更容易使人联想起加密、解密与相关安全技术,而在数字图书馆建设中,保密性更多地体现在保护知识产权所有人的利益及保护用户的隐私等层面。

4.3.3 《指南》强调了区域合作与政策因素

数字图书馆从来就不是一个单一的实体,这是美国研究图书馆协会(ARL)在 1995 年给数字图书馆下的经典定义中的一条[32]。作为全国数字图书馆建设与服务联席会议这一合作组织的文件,《指南》在信息安全问题上更为强调区

域性的合作与协作。同时,安全与国家、地区或各系统的法规政策息息相关,政策性因素也是信息安全管理中不可忽视的一个部分。因此《指南》第三条作了如下规定:

在数字图书馆建设和服务过程中,应注意在全国或区域合作时统一协调信息安全政策与信息安全技术措施,加强在信息安全领域与其他合作方的交流。除了参照本指南,应遵守国家和地方各级有关部门与信息安全相关的法律、法规、条例、规章等,并根据自身实际情况进行补充完善。

4.3.4 《指南》强调安全是一个过程管理

安全不仅仅是对技术的关注,也不仅仅是简单的管理要素的堆积,而是一个系统工程,并且这个系统工程还是一个不断循环往复的过程。无论是 ISO 27001 所引用的 PDCA 模型还是 ISO 13335 所定义的风险管控关系,都直观地说明了这一点。因此,《指南》也将过程管理作为一个单独的要素专门列了出来,并强调安全管理是一个循环往复的过程,这里更多地参考了 ISO 13335 的一些描述。

4.3.5 《指南》的主体是描述需要关注的安全要素

《指南》的主体采用描述需要关注的安全要素的方式,除了过程管理外,还包括安全政策、访问控制、信息资源安全、备份与容灾、环境安全、应急响应与安全公告等内容。这些安全要素的选择与 ISO 27002 的安全主题相比有相当大的简化,在层次结构上也有自己的剪裁。在选择确定这些安全要素时,《指南》也参考了大量的国内研究[33-35]。

数字图书馆安全管理虽然说本质上就是一个信息安全管理的概念,但还是有其自身的一些个性与特点,比如在数字信息内容资源的组织管理、建设与服务上有着这个行业历史传承的一些属性和特点。因此《指南》将安全要素关注的重点落在信息资源上,无论是访问控制、信息资源安全以及备份与容灾都是围绕着这一点进行展开的。其他如信息安全领域非常关注的硬件与软件系统的安全,属于一般性问题,因而只是有所提及,没有作为完整的要素展开讨论。可以说,即使从关注的安全要素来看,《指南》文本也是简而又简。

在安全政策方面,《指南》强调安全是一个完整的体系,是一个系统工程。此外,安全策略的考虑必须基于风险平衡的原则。信息系统的构建与服务存在着不同的规模、不同的技术水平与特性以及不同的服务特点,数字图书馆的建设与服务也是如此。在考虑数字图书馆的安全问题时,不能不考虑我国各地区各类型数字图书馆目前的建设水平与现状,考虑成本支出的效益因素。对于信息安全而言,绝对的安全是不可能的。安全问题就像一个永远无法达致至善至美的远大理想一样,比较现实的做法一定是在给定的条件下达到最好的效果。

在一些安全要素的描述方面,《指南》有时分别从管理方法与实现技术两个层面给出建议的控制措施。例如《指南》第七条对访问控制的规定如下:

建立全面的用户访问控制管理,避免系统的未授权访问。并应明确告知用户其可访问的权限,明确其权利及所承担的责任。

应尽量关闭网络设备与主机系统不必要的服务端口,减少系统被非法利用与攻击的可能。利用应用与系统的分类采用不同的防护手段等级划分不同的防护区域,使外部非法访问内部服务器的可能降低。

规定第一款是利用相关管理制度与政策来进行安全控制,第二款就是如何采用具体的技术手段来进行控制。

另外,《指南》在有些要素的描述方面也充分体现了数字图书馆自身的特点。例如在第八条"信息资源安全"中指出,"信息资源包括购买信息、自建信息及购买的资源远程访问控制权限等",此处的"访问控制权限"就与第六条中的访问控制是完全不同的概念。这里指的是访问远程资源的权利,可以利用这项权利来为用户进行服务,这项权限也是一种资源,是《指南》规定需要进行安全保护的对象资源。

备份与容灾是数字图书馆安全管理工作中不可忽视的,因为没有将容灾工作做扎实而遭受很大损失的实例屡见不鲜。理论上备份应是

容灾手段中的一种,但为了便于理解,《指南》将备份与容灾分开,使其更接近我们平时的理解。备份被看作是一种对于信息资源数据的保存,而容灾则指的是系统的备份,以便在突发情况下能够迅速恢复系统正常运行。

对于环境安全要素的考虑,一开始并没有出现在《指南》文本中。但在《指南》几次征求意见的过程中,对于环境安全的要求屡屡被提及。笔者在调研国内的相关论文时,也发现物理安全是大家关注的重点,并且往往被列为首位。因此最终将环境要求要素也加入到《指南》中。这一条款同样是技术与管理并重,一是强调物理环境的安全,二是强调物理环境的管理,主要是人员的管理。

对安全事件的应急处置是我们实际工作中非常重视的一环,因此《指南》也参照 GB/T 20269 - 2006 的文本加上了应急响应与安全公告的条款。不仅强调了安全事件的应急响应,也强调如何在平时通过安全公告来做好安全事件的预防与预警。

5 《指南》的修订与完善

对于复杂的数字图书馆安全管理工作来说,不足 2000 字的《指南》只能算是一个起步,目的是让大家知道做好数字图书馆安全管理所要关注的一些基本出发点与总体原则,以及了解一些基本理念。

《指南》的编写本身应是一个不断完善的过程,不仅因为其需要根据大家的反馈而不断修订,同时也因为《指南》本身是在一定发展水平下对现有安全标准规范等进行剪裁的版本。如果我国的数字图书馆建设与发展水平上去了,人员水平也有了很大的变化,那是否就可以采用直接选择依从标准的方法来编写指南呢? 果真如此的话,《指南》就可以是一个完整的应用某个标准规范的指南了。此外,一些新的研究成果也可以为《指南》的完善所用,例如黄水清和任妮关于将 ISO 27002 用于数字图书馆信息安全风险控制管理的调查结果,及其对关键控制要素的建议[36],都可以作为今后完善《指南》的参照。

从目前的反馈来看,《指南》还有许多值得探讨之处。例如,对于信息安全中很重要的保密性定义的缺失是否合适? 很多人认为应加强用户信息的保护,加强对用户隐私问题的重视,而这就属于保密性的范畴。其次,《指南》并没有任何附录,而这对复杂的信息安全管理工作来说是不合适的。是否应该加上对于依从或参考标准的解释? 或者是否应该加上一些实践案例的收集作为附录? 这都需要作进一步的探讨。

参考文献:

[1] Gladney H M, Lotspiech J. Safeguarding digital library contents and users: Assuring convenient security and data quality[J/OL]. D - Lib Magazine, May 1997 [2010-10-25]. http://www.dlib.org/dlib/may97/ibm/05gladney.html.

[2] Gladney H M. Safeguarding digital library contents and users: Document access control[J/OL]. D - Lib Magazine, June 1997 [2010-10-25]. http://www.dlib.org/dlib/june97/ibm/06gladney.html.

[3] Kohl U, Lotspiech J, Kaplan M A. Safeguarding digital library contents and users: Protecting documents rather than channels[J/OL]. D - Lib Magazine, September 1997 [2010-10-25]. http://www.dlib.org/dlib/september97/ibm/09lotspiech.html.

[4] Mintzer F, Lotspiech J, Morimoto N. Safeguarding digital library contents and users: Digital watermarking[J/OL]. D - Lib Magazine, December 1997 [2010-10-25]. http://www.dlib.org/dlib/december97/ibm/12lotspiech.html.

[5] Gladney H M. Safeguarding digital library contents and users: A note on universal unique identifiers [J/OL]. D - Lib Magazine, April 1998 [2010-10-25]. http://www.dlib.org/dlib/april98/04gladney.html.

[6] Herzberg A. Safeguarding digital library contents: Charging for online content[J/OL]. D - Lib Magazine, January 1998 [2010-10-25]. http://www.dlib.org/dlib/january98/ibm/01herzberg.html.

[7] Gladney H M, Lotspiech J. Safeguarding digital library contents and users: Storing, sending, showing, and honoring usage terms and conditions [J/OL]. D - Lib Magazine, May 1998 [2010-10-25]. http://www.dlib.org/dlib/may98/gladney/05gladney.html.

[8] Gladney H M. Safeguarding digital library contents

and users: Interim retrospect and prospects[J/OL]. D-Lib Magazine, July/August 1998 [2010-10-25]. http://www.dlib.org/dlib/july98/gladney/07gladney.html.

[9] 李媛. 近五年来数字图书馆信息安全问题研究综述[J]. 图书馆学研究, 2005(12):10-15.

[10] 郑德俊,任妮,熊健,等. 我国数字图书馆信息安全管理现状[J]. 现代图书情报技术, 2010(7/8):27-32.

[11] 茆意宏,黄水清. 数字图书馆信息安全管理依从标准的选择[J]. 中国图书馆学报, 2010(4):54-60.

[12] 王东波. 数字环境下图书馆的网络安全隐患及防范[J]. 图书馆学研究, 2003(3):26-29.

[13] 贾宏. 高校图书馆网络安全体系的构建[J]. 图书馆学研究, 2003(4):25-27,31.

[14] 艾冰, 赵晓洪. 数字图书馆计算机网络的安全技术及其防护策略[J]. 太原师范学院学报(自然科学版), 2003(2):31-34.

[15] 杨木锐. 数字图书馆信息安全保障体系研究[D]. 长春:东北师范大学,2007.

[16] ISO/IEC 27000-2009. Information technology — Securitytechniques — Information securitymanagement systems — Overview andvocabulary[S].

[17] GB/T 1971 5.1-2005. 信息技术-安全技术-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[S].

[18] ISO/IEC 13335-1-1996. Information technology — Guidelines forthe management of IT Security — Part 1: Concepts and models for IT Security[S].

[19] 黄元飞. 信息安全标准化现状、问题和对策探讨[J/OL]. 通信技术与标准, 2004(11)[2010-10-25]. http://www.ptsn.net.cn/article_new/show_article.php?categories_id=28a66fa4-8bb4-2f31-09e0-44b1c08f3e7d&article_id=expert_b15c5eea-7bef-d8cb-2dd2-436ef6267b0e.

[20] 林宁, 吴志刚. 我国信息安全标准化概况[J]. 信息技术与标准化, 2006(8):6-8.

[21] 周鸣乐, 董火民, 李刚, 等. 信息安全标准体系研究与分析[J]. 信息技术与标准化, 2008(4):12-17.

[22] 赵文, 苏红, 胡勇. 信息安全标准关系分析[J]. 信息网络安全, 2009(11):48-50.

[23] GB/T 18336.1-2001(idt ISO/IEC 15408-1:1999). 信息技术-安全技术-信息技术安全性评估准则-第1部分:简介和一般模型[S].

[24] GB/T 18336.1-2008(idt ISO/IEC 15408-1:2005). 信息技术-安全技术-信息技术安全性评估准则-第1部分:简介和一般模型[S].

[25] GB/T 18336.2-2008(idt ISO/IEC 15408-2:2005). 信息技术-安全技术-信息技术安全性评估准则-第2部分:安全功能需求[S].

[26] GB/T 18336.3-2008(idt ISO/IEC 15408-3:2005). 信息技术-安全技术-信息技术安全性评估准则-第3部分:安全认证需求[S].

[27] GB/T 22081-2008(idt ISO/IEC 27002:2005). 信息技术-安全技术-信息安全管理实用规则[S].

[28] GB/T 22080-2008(idt ISO/IEC 27001:2005). 信息技术-安全技术-信息安全管理体系-要求[S].

[29] 信息安全等级保护管理办法[EB/OL]. [2010-10-25]. http://www.cspec.gov.cn/Upload/webnews/20070912_104716_765_158_%E7%AD%89%E7%BA%A7%E4%BF%9D%E6%8A%A4%E7%AE%A1%E7%90%86%E5%8A%9E%E6%B3%95070626%EF%BC%88%E5%8D%B0%E5%88%B7%E7%A8%BF%).doc.

[30] GB 17859-1999 计算机信息系统安全保护等级划分准则[S].

[31] GB/T 20269-2006 信息安全技术-信息系统安全管理要求[S].

[32] Realizing digital libraries-appendix II: Definition and purposes of a digital library[EB/OL]. [2010-10-25]. http://www.arl.org/resources/pubs/mmproceedings/126mmappen2.shtml.

[33] 徐宽, 刘万国, 房玉琦. 数字图书馆安全特点及影响因素研究[J]. 现代情报, 2008(11):84-86.

[34] 彭瑶. 数字图书馆的安全策略[J]. 重庆工学院学报, 2002(6):30-32.

[35] 董明浩. 论信息系统的安全与数字图书馆建设[J]. 科技情报开发与经济, 2006(22):67-69.

[36] 黄水清,任妮. 数字图书馆信息安全风险控制[J]. 现代图书情报技术, 2010(7/8):39-44.

赵 亮 上海图书馆系统网络中心副主任,副研究馆员。通讯地址:上海市淮海中路1555号。邮编:200031。

刘 炜 上海图书馆图情研究室主任,研究员。通讯地址同上。

徐 强 上海图书馆系统网络中心主任,副研究馆员。通讯地址同上。

(收稿日期:2010-11-17)