基于硬件底层防御与软件应用层防护的信息安全实证研究——以江西省数字图书馆为例*[1]

黄珣 吴玉灵

【摘 要】:随着信息技术的迅猛发展和社会信息化程度的不断加深，网络信息安全问题日渐显现。本文采用问卷调研和实地走访的方法，对2013-2016年间江西省17家数字图书馆信息安全管理现状进行了调研分析，调研内容涉及信息安全问题、软件基础设施、硬件基础设施以及数据内容等，并对调研结果进行了数据分析。最后，从底层硬件到应用层软件，再到基于分布式云防御系统的角度提出了重视信息安全管理、健全信息安全保障制度、建立信息安全风险评估和应急处理体系等策略，从而有效保障数字图书馆的信息安全。

【关键词】:江西省数字图书馆；信息安全；策略

【中图分类号】：G250.76 **【文献标识码】**：A **【文章编号】**：1006-5024(2017)09-0157-06

DOI：10.13529/j.cnki.enterprise.economy.2017.09.026

一、引言

2016年起，国家网络安全宣传周于每年9月第三周在全国统一举行。中共中央政治局常委、中央书记处书记、中央网络安全和信息化领导小组副组长刘云山在2016年国家网络安全宣传周开幕式上强调，坚持网络安全和网络发展同步推进，让互联网更好地造福人民。

在图书馆领域，网络安全和信息安全从来都是如影随形的。随着互联网应用领域的拓展延伸和数字图书馆推广（图书馆自助借还服务、移动图书馆、图书馆微信平台、歌德电子书、信息检索资源库等数字应用服务的推广与普及）的不断深入，越来越多的读者和用户广泛参与其中，体验数字图书馆带来的便利。然而，也有一些不法分子试图攻击数字图书馆服务器，窃取相关资料信息，使得数字图书馆的信息安全问题日渐显现：数据信息欠完整；网络连接信号异常，无法访问目标服务器；服务器硬件故障；数据库服务器被入侵，信息数据资料被窃取等[1]。如何更好地解决数字图书馆信息化安全问题，保障数字图书馆的正常运行，是当下需要探讨的重要问题。

本文以江西省数字图书馆为例， 阐述其在不断适应时代技术发展潮流中出现的各种问题， 分析这些问题产生的原因，并提出相应的解决策略，为保障数字图书馆信息安全乃至整个图书情报行业信息安全提供借鉴。

二、江西省数字图书馆信息安全管理现状

近年来， 随着全媒体时代信息高速发展和江西省对数字文化的日益重视， 全省数字图书馆建设取得了长足进步， 无论是

[1] **基金项目**:江西省社会科学规划项目“江西省公共图书馆公益性数字文化服务体系构建研究”（项目编号：13TQ07）

作者简介：黄珣，江西省图书馆馆员，研究方向为图书情报及新闻传播；吴玉灵，江西省图书馆馆员，研究方向为数字图书馆建设。（江西南昌 330046）

在数字资源硬件方面还是在人才储备软件方面，都有了较大的提升，但是在信息安全管理方面还稍显不足。笔者采用调查问卷、电话访谈和现场走访相结合的方式对江西省 17 家数字图书馆进行了信息安全管理方面的调查， 以期通过调研和分析， 提出促进江西省数字图书馆信息安全管理的合理建议。

（一）调研对象及方法

参与调研的对象是江西省已经建设数字图书馆的公共图书馆和高校图书馆。其中，公共图书馆包含江西省图书馆和 11 个设区市图书馆，高校图书馆包含南昌大学图书馆、江西师范大学图书馆、江西财经大学图书馆等。由于江西省数字图书馆建设仍处于起步状态，因此，调查对象选定为数字图书馆建设方面有一定基础的相对较大的图书馆。参与调查的 17 家数字图书馆如表 1 所示。

表 1　参与调查的 17 家数字图书馆列表

公共图书馆		高校图书馆
江西省图书馆	南昌市图书馆	南昌大学图书馆
九江市图书馆	赣州市图书馆	江西师范大学图书馆
上饶市图书馆	宜春市图书馆	江西财经大学图书馆
景德镇市图书馆	抚州市图书馆	江西农业大学图书馆
吉安市图书馆	新余市图书馆	华东交通大学图书馆
鹰潭市图书馆	萍乡市图书馆	

（二）调研具体内容

调研内容主要涉及数字图书馆信息安全事件，从数据安装环境的硬件设施、数据安装环境的软件设施，以及数据内容的角度来分析数字图书馆的信息安全。

1. 信息安全事件调查。主要调查各馆在 2013-2016 年间发生的信息安全事件的内容、起数和信息安全技术人员数量、发现信息安全事件的途径、信息安全事件的原因和处理方式，以及一些建议意见等。

2.硬件设施分析。主要是关于各单位硬件设备的调研，包含防火墙、web 服务器、数字资源存储服务器、数据库服务器、流媒体服务器、UPS 电源设备、灾备设备等。

3.软件设施分析。主要涉及防病毒软件、服务器漏洞更新、服务器安全策略、数据资源访问认证系统、容灾备份恢复系统等应用软件。

4.数据内容分析。主要涉及数据资源的版权争议和数据内容与索引是否一致的真实性。

（三）调研结果及分析

1.江西省数字图书馆信息安全管理概况。综合分析调研反馈的数据后发现，12 家公共图书馆和 5 家高校图书馆均发生过信

息安全事件。事件类型主要包含：（1）硬件设备故障（服务器硬盘损毁、UPS 电源设备故障、接入层交换机设备故障、自助借还机设备模块故障等）；（2）软件系统故障（服务器 windows2003 操作系统故障、部分外购资源数据库系统故障、自助办证系统与自助借还系统故障、图书馆 ILAS3 自动化业务系统故障、平台资源加工业务系统故障等）；（3）数据内容出错（部分资源库中索引资源所对应的对象数据为空或出错）；（4）不可抗力因素（由于突发性意外断电以及其他因素引起的）。各安全故障类型具体所占比例见图 1。

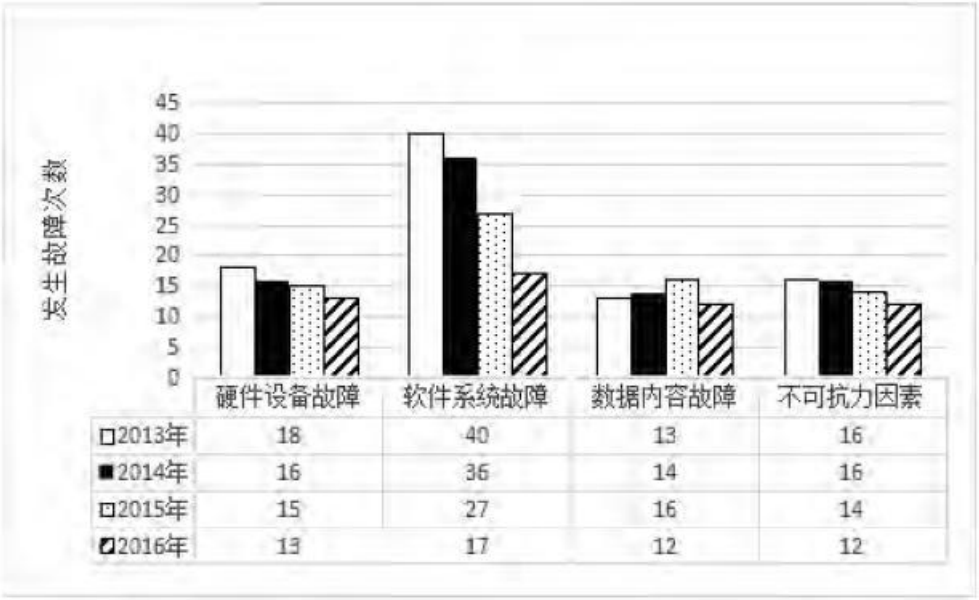

图 1 2013-2016 年江西省数字图书馆信息安全故障类型柱状图

2. 江西省数字图书馆信息安全硬件设施故障分析。数字图书馆的硬件设施包括：机房、服务器、局域网设备（包含防火墙、核心交换机、VPN 设备等）、存储设备、RFID、数字化设备、容灾设备等。被调查的 17 家数字图书馆中 58.8%采用 RAID 磁盘冗余阵列技术以提高数据的容错性， 35.3%表示不清楚，5.9%没有采用该技术。在是否设有灾备机房的调查中，仅有南昌大学图书馆、江西师范大学图书馆 2 家高校图书馆配备。经调查并综合分析可见，江西省高校图书馆信息安全建设在一些方面比公共图书馆更具优势。江西省公共图书馆与高校图书馆信息安全建设情况比较如图 2 所示。

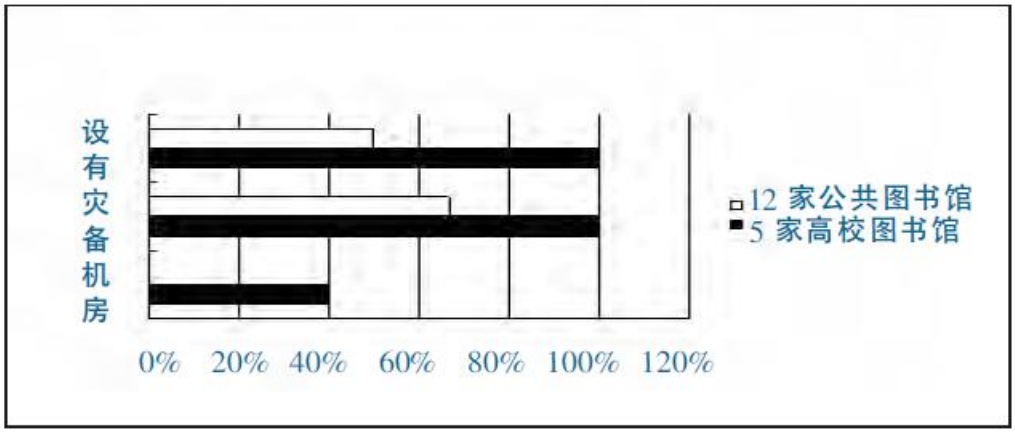

图 2 江西省数字图书馆信息安全建设部分情况比较(公共图书馆与高校图书馆)图

3.江西省数字图书馆信息安全软件系统故障分析。数字图书馆信息安全软件系统包括：服务器版防病毒软件； 统一资源定位符系统； 统一用户认证系统； 数字资源版权识别系统等。被调查对象中，有 76.5%已安装反病毒软件，23.5%没有安装；35.3%拥有容灾备份恢复系统，35.3%没有该系统，39.4%表示不清楚；64.7%拥有类似于数据资源访问用户认证系统，对数据的内容访问进行授权，从而协调数据资源的共建共享，35.3%没有该系统。调查结果显示，江西省数字图书馆信息安全软件系统建设正在得到重视，但仍不够完善。

4.江西省数字图书馆信息安全问题的发现。在 2016 年全年中， 通过在被调查的 17 家数字图书馆中抽样选取 50 起信息安全事件， 发现有 23 起是由本单位技术员定期检测发现；有 20 起是事后用户发现；有 4 起是相关部门告知；最后 3 起是意外发现。由此可见， 数字图书馆在信息安全事件防范方面仍处于被动的状态。江西省数字图书馆信息安全发现方式如图 3 所示。

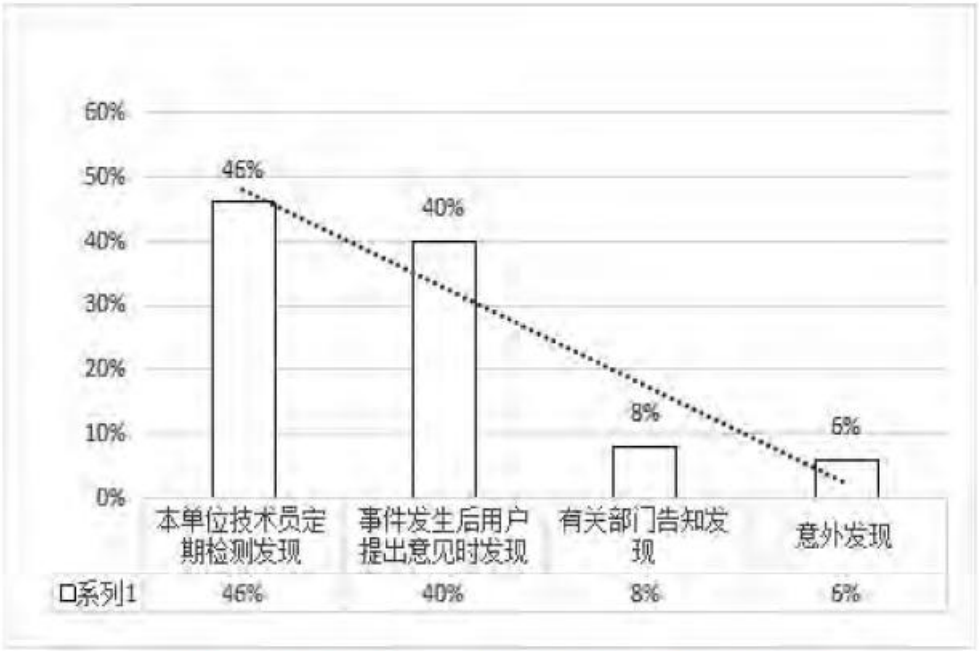

图 3 江西省数字图书馆信息安全问题发现方式

5. 江西省数字图书馆信息安全的处理。被调查的数字图书馆在发现信息安全事件后风险处理方式及对应比例为：有 46%自行解决、18%求助相关信息安全服务机构、18%向上级主管部门报告、6%向公安机关报案、12%求助网络信息安全公司。江西省数字图书馆信息安全风险处理方式如图 4 所示。

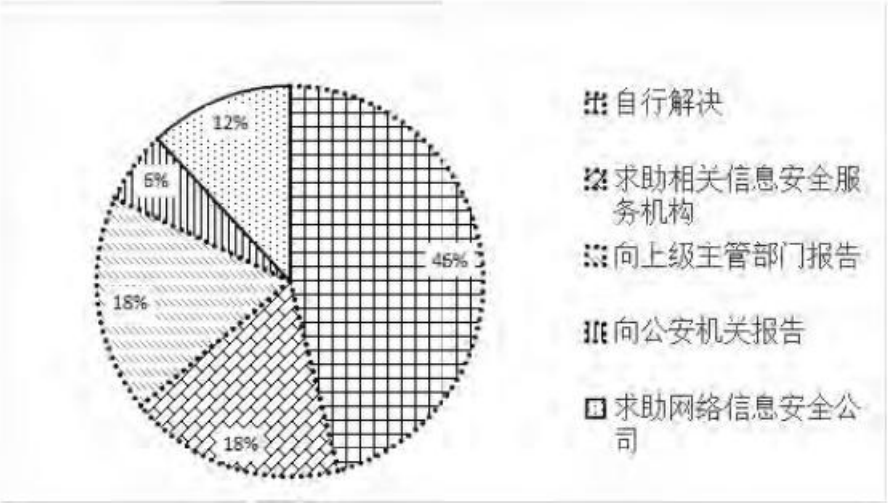

图 4　江西省数字图书馆信息安全风险处理方式

6.　江西省数字图书馆信息安全专业人才储备情况。信息安全专业人才储备和队伍建设是数字图书馆安全运行的重要保障。目前，江西省数字图书馆信息安全专业人才储备仍显不足。调查结果显示，被调查的 17 家数字图书馆仅有 2 家设立了专门的信息安全主管部门。82.4%的数字图书馆有技术人员负责信息安全，但他们大多属于兼职性质， 信息安全专业人才比较缺乏；17.6%的数字图书馆没有配备信息安全维护人员。江西省数字图书馆信息安全队伍建设情况如图 5 所示。

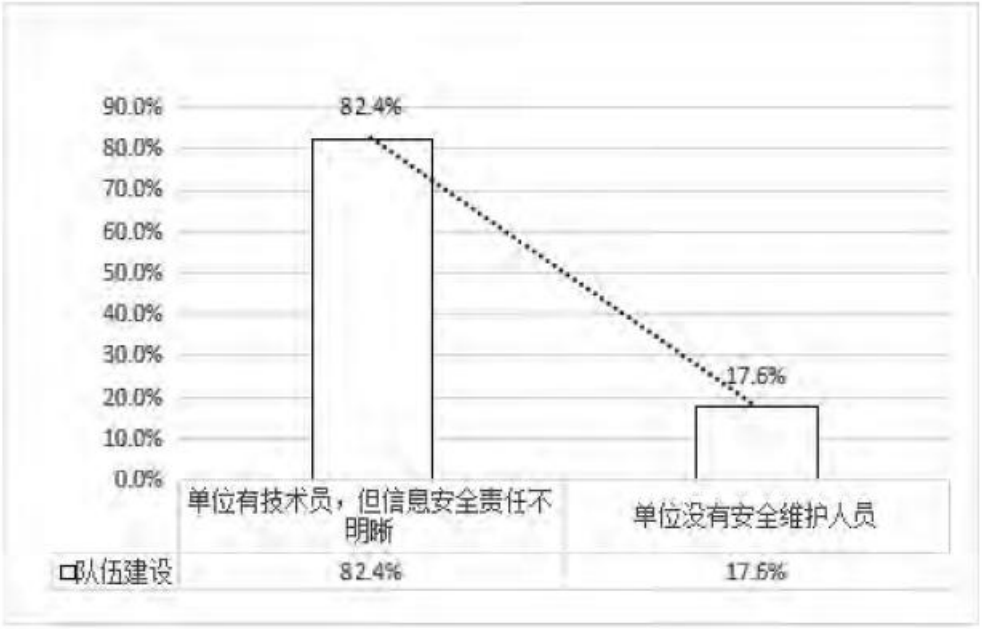

图 5　江西省数字图书馆信息安全队伍建设

7.　江西省数字图书馆信息安全制度建设情况。据调查表汇总显示，江西省数字图书馆信息安全制度还不够健全，17 家数字图书馆已建立信息安全制度的比例仅为 58.8%， 没有建立信息安全制度的为 41.2%， 但其中大部分已经具有建立信息安全制度来保障数字图书馆正常运行的意识。江西省数字图书馆信息安全制度建设情况如表 2 所示。

表 2　江西省数字图书馆信信息安全制度建设情况

是否建立	已建立	未建立		正在建立	打算建立	其他
图书馆数量	10	7	其中	3	3	1
所占比例	58.8%	41.2%		42.9%	42.9%	14.2%

三、影响江西省数字图书馆信息安全的因素

笔者通过实地调研， 对 2013-2016 年间江西省数字图书馆信息安全事件发生的原因进行了统计，主要有： 断电次数过多引起的存储服务器硬盘损毁（2013-2016 年占比均在 70%以上）；攻击者使用端口扫描程序入侵，修改管理权限（2013 年占比 88.2%，之后逐年减少）； 服务器使用远程维护后未及时关闭危险端口（或未指定 IP 段远程访问） 导致黑客入侵（2015 年占比最高，达到 94.1%）；未设置服务器安全策略（2013 年占比 70.6%，2016 年减少至 29.4%）等。根据 2013-2016 年信息安全事件发生原因统计数据可以看出，影响江西省数字图书馆信息安全的因素既有内部因素，也有外部因素。

（一）内部因素

1.防范意识薄弱。现代图书馆已发展至数字时代，而其信息安全意识发展却仍停留在传统图书馆时代。许多图书馆仍抱着“有防火墙=安全”的态度，缺乏“防黑防毒”的意识和警惕性，包括图书馆工作人员、读者和用户在内的人员大多对图书馆信息安全问题不够重视。因此，防范意识薄弱是导致信息安全事故发生的重要因素之一。另外，缺乏专业信息安全管理方面的人才也是不容忽视的。由于专业知识的局限，数字图书馆的管理人员往往只能处理日常系统的维护管理工作，在遇到突发性信息安全事件时，不能有效地运用专业技术手段及时处理和规避风险[2]。

2.管理制度不严。数字图书馆信息安全制度建立不完善、管理宽严不一是导致信息安全事件频发的重要原因之一。作为分布式系统之一的数字图书馆信息系统，具有物理分布、环境多变、分布式管理等特点。由于分布式管理，导致无法确保每台机器上的操作都受到适当的授权和限制的保护，不同的管理制度就有可能导致管理措施宽严不一。江西省部分数字图书馆就存在由于制度不全、对信息输入的授权和监督不明，导致存在安全漏洞且很难实现事后责任追究的问题[3]。

3.资金投入不足。江西省地处中部欠发达地区， 事业经费与沿海等发达地区相比差距较大，特别是现处于数字图书馆建设初期，已经非常有限的建设经费大多用于硬件设备购置方面，几乎没有用于信息安全维护的专项经费， 导致数字图书馆的安全系统不能及时更新换代以满足时代发展要求。

（二）外部因素

1.计算机恶意代码泛滥。计算机网络技术的飞速发展，在带来数字资源共享的同时，也为不法分子传播病毒、蠕虫、木马等恶意代码提供了途径。数字图书馆一旦感染恶意代码， 就有可能破坏被感染计算机数据、运行具有入侵性或破坏性的程序，从而破坏资源库的数据安全性和完整性。

2.网络黑客攻击入侵。数字图书馆是面向互联网的公共平台， 不可避免地会遭受到网络黑客的攻击。网络黑客常用的攻击手段有端口扫描、网络监听、IP 电子欺骗、拒绝服务攻击、缓冲区溢出等，他们有可能获得管理员权限对数字图书馆的资源进行删除、篡改，导致服务器运行速度减慢、网络瘫痪，从而影响读者和用户的正常登录及使用。

3.自然灾害。包括火灾、水灾、地震、闪电等在内的自然灾害同样可能破坏信息的存储、传输和使用。虽然这些自然灾害不可避免， 但管理人员可以通过建立灾难恢复计划、业务持续计划、紧急事件预案等方式，降低这些不可抗力造成的损失。

四、解决信息安全问题的对策

（一）重视信息安全管理

信息系统安全管理措施的实现依托于各种具体的安全控制管理措施。其中，物理安全是基础。要通过机房与设施安全、技术控制、环境与人身安全等来保证计算机系统有一个安全的物理环境。数据安全管理通过各种计算机、网络、密钥技术保证传输、交换和存储各环节中信息数据的机密性、完整性和真实性[4]。控制管理是保障。控制管理包含人员安全管理、软件安全管理、运行安全管理、技术文档安全管理等方面。此外，还要依赖信息安全管理的条件[5]，这些条件如图 6 所示。

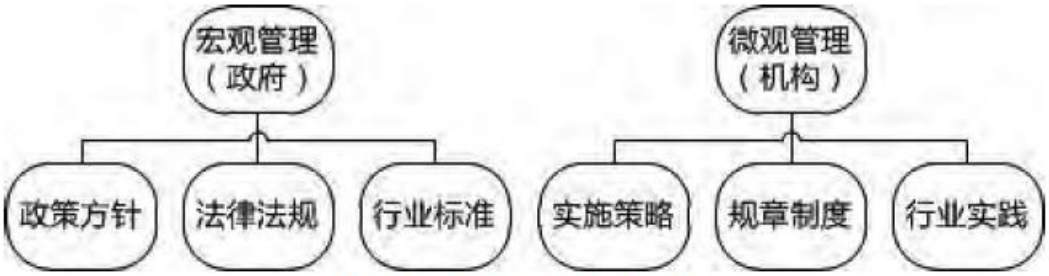

图 6　信息安全管理的条件

（二）健全信息安全保障制度

我国现有的中央网络安全和信息化领导小组这一具有最高权威机构的设立，打破了信息安全管理出现的条块分割、协作松散的局面，为建立信息安全相关法律法规和政策体系提供了条件。通过专门法律，依法打击网络犯罪，可以维护网络安全、规范个人信息的收集与利用、保护隐私权，同时还可以创设新的知识产权保护技术、建立互联网信息安全秩序[6]。

（三）建立信息安全风险评估和应急处理体系

信息安全系统风险评估是数字图书馆信息安全的基础性工作。立足于信息处理系统，从内因和外因两方面综合判断其可能面临的风险， 开展好信息安全系统风险评估，能够明确风险责任因素，在数字图书馆信息安全保障体系的建设中作出合理的决策，使信息安全策略保持一致性和持续性。在对风险进行评估和管理的同时，应加强对突发信息安全事件的预警处理能力，将损失降到最低。首先，在法律的保障下， 充分发挥政府作为应急组织者和指挥者的作用。同时，还要在社会连带责任思想的影响下，形成政府与社会成员合力的应急体系[7]。其次，依托业务连续性计划、业务恢复再继续计划、灾难恢复计划和拥有应急计划等重要信息技术。最后，通过实施业务影响分析、确定预防性控制措施、制定恢复战略计划、制定 IT 应急计划、进行有计划地测试、培训与配合以及不断维护和完善计划，真正构建应急处理体系。

信息技术的飞速发展促进了图书情报行业的发展，与此同时，也给处理海量信息资源的系统带来了挑战性和复杂性。发达国家愈加重视信息安全风险评估工作，提倡将风险评估纳入到制度中执行。当前，我国图书情报业数字图书馆信息安全必须加强风险评估工作，提高数字图书馆信息安全风险策略的匹配度。

（四）加强数字图书馆安全管理

1.建立防御型底层硬件设施

（1）加强服务器机房建设。通过定期采购先进硬件基础设施并建立规范化数字图书馆机房管理制度，对机房基础设施进行统一管理，如机房一体化监控设施、容灾备份设施等。

（2）通过对基础设施的评估来决定机房硬件基础设施的采购。在采购数字图书馆基础设备时， 需要对采购的对象进行性能评估。例如，存储设备需要关注其采用读写缓存、光纤连接数、集群模式控制器可扩展数等；灾备设备则需要模拟评估当灾难（如断电、火灾等）发生时其数据保护程度。

（3）基于硬件驱动控制权限构建底层系统防护。基于硬件级底层控制权限的系统防护为数字图书馆服务系统新增了一道安全防线，它拥有系统级最底层的权限，并在执行安全保护功能时不占用系统内存，比一般病毒程序拥有更高的优先权，能实时保护系统，常规病毒、恶意软件一般都无法破坏镶嵌在系统底层的 OS 防护功能。

2.建立防护型应用层软件设施

（1）建立数字图书馆服务器安全策略。对机房 web 服务器、FTP 服务器、数据库服务器建立相关安全策略。例如，关闭服务器不必要的服务端口、设置磁盘的访问权限、禁止远程修改注册表、禁用相关组件等操作。

（2）定期扫描修复服务器漏洞。常用的技术漏洞扫描工具有：①针对操作系统、典型应用软件等漏洞问题（Nessus 、绿盟极光、启明天境）。②针对网络端口（Namp）。③针对数据库漏洞安全（安信通、安恒）。④针对 web 漏洞（IBM Appscan、HP WebInspect WVS）。⑤针对网络数据流（WireShark、Ethereal）。

（3）利用“安全狗云安全中心平台”给予服务器全方位体检。通过“安全狗云安全中心”平台，结合云计算技术，对本馆数字图书馆基础设施进行网站安全扫描、网站安全监控、网页云防篡改、服务器（server 网络资源） 安全监控、安全告警、安全设置等全方位安全保护服务。

3.建立基于分布式云部署架构的云防御设施

基于分布式的云部署架构的云防御设施， 其被防御的设备资源隐藏在云端网络的后方， 攻击者无法直接接触到被防御的资源，起到隐藏源服务器 IP 的作用[8]。这样可以有效防御各类型大流量攻击和各类 CC 攻击，根据攻击大小动态伸缩防御体系，同时针对搜索引擎设置专用线路， 网站就算持续被攻击， 搜索引擎还是能通过对应的专线稳定快速访问到网站，从而保证不影响搜索引擎中网站的排名。云防御流程如图 7 所示。

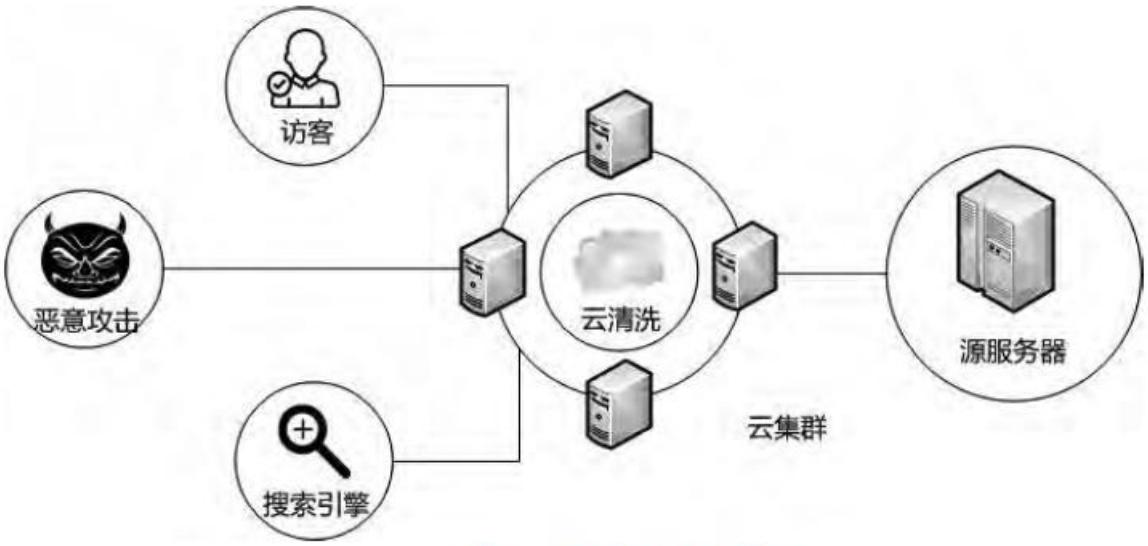

图 7　云防御流程示意图

4.加强信息系统安全新技术应用

我国信息安全技术的发展已经从通信级保密、计算机数据级保护 2 个阶段过渡到网络信息安全技术的研究发展阶段。目前主要有 Linux 安全增强技术、虚拟专网安全技术、网络安全物理隔离技术、数据库安全增强技术等。虽然我国信息安全技术起步较晚、产业化投入较少，但目前已有不少研发机构、高校及企业纷纷涉足信息安全技术研究和产品开发领域，信息安全技术将呈现由单一安全产品向安全管理平台转变，从静态、被动向动态、主动转变，由粗放型向量化型转变的趋势，新技术的研发与应用将为建立我国信息安全保障体系提供关键技术支撑[9]。

综上，针对今后可能发生的信息安全威胁，江西省数字图书馆只有采用先进的信息安全技术提升信息安全水平， 采用科学的管理方法打造一支有责任心的专业人才队伍，构建信息安全风险评估系统，才能增强自身的抗危险因素能力， 保障工作的稳定性和连续性， 从而加快数字图书馆乃至整个图书情报行业的发展。

参考文献：

[1] 姚晓丹.试论信息时代高校图书馆危机管理[J].兰州教育学院学报，2015，(12).

[2] 曹雪梅，高玲.谈数字图书馆网络信息安全[J].图书档案[J].科技创新与应用，2012，（1）.

[3] 鲍劼，李苏丰.大数据环境下图书馆信息安全问题与对策分析[J].科技情报开发与经济，2014，(12).

[4] 梁双.数字图书馆信息安全管理依从标准的选择[J].中国培训，2016，(24).

[5] 黄水清.数字图书馆信息安全管理的过程方法[J].图书情报工作，2013，(6).

[6] 李婵，张文德，蓝以信.数字图书馆信息系统安全动态风险评估模型[J].情报科学，2015，(5).

[7] 刘万国，张浩然，付希金.图书馆信息安全应用技术述评[J].现代情报，2010，（10）.

[8] 赵玉冬.云计算环境下数字图书馆信息安全问题及对策研究[A].《决策与信息》杂志社，北京大学经济管理学院.“决策论坛———决策理论与方法研究学术研讨会”论文集（下）[C].《决策与信息》杂志社，北京大学经济管理学院，2016.

[9] 郑德俊，任妮，熊健，黄水清.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）.