# 基于图书馆业务的信息安全管理平台

□ 李留英 / 南京政治学院上海校区军事信息管理系 上海 200433

摘要：信息安全管理平台是提高图书馆安全管理的重要手段。文章分析了信息安全管理平台的发展现状，图书馆面临的安全威胁，提出利用大数据和云计算等技术构建基于图书馆业务的信息安全管理平台，讨论了其体系结构和主要功能，以保证图书馆业务的连续性和可用性。

关键词：基于业务，图书馆，安全管理平台
DOI：10.3772/j.issn.1673—2286.2014.02.007

为解决日益严重的信息安全问题，图书馆通过不断购置和部署不同厂家生产的安全设备和产品，包括防火墙系统、入侵检测系统、防病毒系统、漏洞扫描系统和终端安全管理系统等安全设备。这些安全设备虽然加强了网络安全性能，在使用中由于缺乏集中的全局性管理手段，实际的安全管理水平和工作效率不太理想。为有效发挥网络信息安全设备的效能，快速准确地掌握图书馆信息系统的整体运行状况，积极处理各类安全事件，必须建设相应的一体化安全管理平台。

## 1 信息安全管理平台概述

2000年开始，国内外陆续推出了安全管理平台产品，帮助企业分析和处理安全事件，评估资产风险，建立了一套应急响应流程。传统的信息安全管理平台（Security Operation Center，SOC）的定义：以资产为核心，以安全事件处理为关键流程，采用安全域划分的思想，建立一套实时的资产风险模型，协助处理员进行事件分析、风险分析、预警处理和应急响应处理的集中安全处理系统[1]。

总体而言，信息安全管理平台通过统一的技术方法，将全网中不同位置的IT资源、不同类型设备，不同安全系统进行安全域的划分，对海量异构网络与安全事件进行集中汇总、过滤、收集和关联分析，实现日志的集中、分析、审计与报告。同时通过集中的分析审计和评估，发现安全风险、潜在的攻击特征和安全态势发展趋势，形成统一的安全决策，以便对安全事件进行响应和处理，确保任何安全事件、事故得到及时的响应和处理，将安全事件对运行的影响降到最低。

信息安全管理平台使得各级管理员能够实现全网资产运行监控、事件分析与审计、风险评估与度量、预警与响应、态势感知，并可借助标准化的流程管理实现持续的安全运营。安全管理平台既是安全管理人员的工作平台，也是各级部门进行安全管理和安全实施的考核和决策平台[2]。

目前，一些企业和组织正在进行网络安全管理平台的研发工作。常见的产品如国外Check Point公司的Eventia Analyzer、Symantec公司的Security Management System等。国内代表性的安全管理平台主要有启明星辰公司的泰合安全管理平台、联想的网御安全管理平台、天融信公司的TopWAF等。

信息安全管理平台SOC正被越来越多的用户所接受，SOC已经成为继防病毒、Web安全网关、移动安全、下一代防火墙之后企业和部门在网络安全方面的最大投入。

但是，传统安全管理平台存在一定的缺陷，主要包括：（1）信息来源基本集中在网络和安全设备的日志，无法关注其余的IT资源的性能、故障、运行状态等信息，难于反映企业信息系统安全运营的实际情况。（2）安全事故发生后，安全管理人员一般可追踪到事件源IP，很难及时定位到具体的设备。（3）对终端的安全运行状况及实时响应无能为力。（4）内部信息保护存在缺陷，泄密事件时有发生。

随着先进持续性威胁（Advanced Persistent Threat，APT）以及工业控制系统遭受病毒等的各种复

杂攻击，需要更加智能的全局安全监控与分析系统来加强安全防护。信息安全管理平台应更强调安全运维和流程管理。随着云计算和虚拟化技术的逐步运用，安全管理平台将具备对云和虚拟化环境下的IT资源监控、分析能力。

## 2 图书馆面临的安全威胁

随着云计算、物联网技术的发展，很多图书馆开始尝试新的应用。如北京大学图书馆推出移动图书馆服务；北京邮电大学探索和研究利用物联网技术和云计算技术实现智能图书馆，为图书馆的工作人员和读者提供一个真实的基于物联网的智能图书馆；清华大学采用虚拟化技术实现图书资源的存储和优化等。

随着图书馆信息化程度的提高，其面临的信息安全威胁也日趋严重[4]，主要有以下几点。

（1）计算机病毒泛滥。图书馆的信息化和网络化，使图书馆感染病毒几率大增。一旦受病毒感染，可导致图书馆网络系统瘫痪，无法开展正常的图书信息服务，甚至造成图书馆大量珍贵数据的丢失。

（2）非法入侵。黑客利用网络协议、操作系统、软件漏洞实施非法入侵。其中，一些漏洞是网络协议、操作系统或应用软件本身所固有，如图书馆局域网ARP攻击就是利用了地址解析协议的漏洞；有些漏洞则是由于系统配置错误引起的，如将未加Shadow的用户密码以明码方式存放在某一目录之下。

（3）版权保护。图书馆将纸质资源转换成数字资源供读者使用，读者借助于网络可以将数字信息传输到世界各地，却出现了数字版权问题。如何保护版权，成为一个严峻的问题。

（4）数据备份。图书馆数字信息资源和文献信息资源是图书馆的核心资源。由于自然环境或意外事故等因素可造成图书馆信息资源的损失。为保证图书馆各类信息资源的安全，便于系统受到意外破坏时能尽快恢复工作，必须做好数据备份工作。

（5）个人隐私。利用手机等移动终端使用图书馆服务，是图书馆发展的趋势。目前，读者的移动终端中一般都会存储了个人隐私信息，一旦访问移动图书馆，就很容易受到网络攻击，导致个人隐私被窃取或者丢失。在移动图书馆服务过程中，如何保护用户的个人隐私以及图书馆的隐私信息，值得深思。此外，当图书馆将大量的用户信息存储在云平台上时，由于被离散地分布在云中不同的数据中心，增加了信息泄露的风险。

## 3 基于图书馆业务的一体化信息安全管理平台

随着数字图书馆的发展和图书馆服务模式的多样化，保障图书馆的业务安全性、可用性和连续性成为信息安全管理的首要任务。为此，需要从图书馆业务角度出发，构建全面的网络安全监控，实时采集图书馆业务系统的图书、设备等各种资产的信息，集中分析和审计各类安全事件，及时提供图书馆业务风险视图与应急响应处理方案，实现一个以图书馆业务为核心的安全处理、业务服务处理和运维处理的一体化管理平台。

### 3.1 基于图书馆业务的一体化信息安全管理平台的结构

目前，云计算技术已经逐步应用到图书馆，来扩充机房承载容量，搭建高性能存储，增强容灾能力，在线备份功能。面向图书馆业务的一体化信息安全管理平台必须充分借助图书馆的虚拟资源服务池。根据数字图书馆的B/S结构，面向图书馆业务的信息安全管理平台分为四层结构：分别是资源池、采集层、核心业务层和展现层。

第一层资源池。信息安全管理平台每天将接收大量的数据。为有效存储管理这些数据，需要扩展图书馆的私有云存储池，或采用虚拟化技术优化存储服务器，存储信息安全管理平台的各类信息资源；云存储解决了传统SOC面临的海量数据存储和处理带来的瓶颈。

第二层采集层，通过事件采集器、采集代理、摄像头或传感器，对图书馆支撑网络和系统上的资产、用户、各类安全设备获取事件日志信息。

第三层为核心业务层，实现信息安全管理平台的各类业务，如身份认证管理、风险管理、运维管理、预警管理、审计管理等。

第四层为展现层，提供各类事件、信息和操作信息等的可视化。包括实时列表、统计图表、信息仪表盘、地图等展示方式。

参考公安部的《安全管理平台产品检验规范》[4]，面向图书馆业务的一体化信息安全管理平台在保留传统信息安全管理平台优点的基础上，具有如下特点：

（1）海量信息的实时处理。实时采集图书馆资产、

不同安全设备的大量安全日志信息，采用大数据技术和人工智能技术进行实时智能关联分析。

（2）采用虚拟化技术管理图书馆的各类设备和资产，实现图书馆信息系统的运维处理管理。

（3）高效精准的应急响应和预警机制。

（4）监控对象、过程和结果的可视化展示，包括资产可视化、图书馆业务可视化、安全事件可视化、安全风险可视化等。

（5）良好的可扩展性和开放性，支持不同厂商不同类型设备。

## 3.2 基于图书馆业务的一体化信息安全管理平台的功能

（1）图书馆资产管理和业务运行监控

目前，RFID技术可以使图书馆的建筑环境、设备资产、文献资源关键数据能够被及时感知，通过智能手机的GPS、WiFi、Zigbee等技术能够感知和定位读者。为此，可充分利用图书馆已有的物联网系统和移动应用，对图书馆的各类移动终端、网络设备、安全设备、主机和服务器集群、数据中心、图书馆的各类业务系统、图书馆其他设施的温度、湿度、火灾和故障等信息进行采集和上报，实现7*24小时的全面运行监控。

安全事件发生后，能准确定位到事件相关的设备责任人、联系方式和物理位置等，安全管理人员能及时做出决策，采取响应措施，确保图书馆业务的正常开展。这种模式也便于日常的安全运行维护经验的积累和共享，便于日常运维工作的进行。

支持对安全设备和安全策略的统一配置和管理，能够对网络设备进行简单的命令操作，实现远程配置操作和维护。

（2）信息安全事件全程管理及流量管理

图书馆业务系统中运行着数量众多的移动终端、主机、服务器、存储设备、异构网络设备，多种安全设备如防火墙、防病毒、入侵检测系统，以及图书馆的应用系统等。大型的图书馆每天产生大量的日志和告警，以及几十到几百GB甚至上TGB级别的安全事件信息。需要花费大量的人力进行处理，传统的人工处理方法无法保证其精确性和实时性。

图书馆系统产生的安全事件包括有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他信息安全事件等[2]。为实现对安全事件的全程管理，需要对日志、告警和安全事件信息进行辨别、分析、规范化处理，形成统一的事件格式，包括事件严重等级、事件类型、来源和名称等，按照统一的标准对安全事件进行分类和分级，便于管理员快速地浏览所有安全事件，并形成告警。

采用大数据处理技术，结合安全事件关联分析方法，如基于因果的关联分析、基于规则的关联分析、基于漏洞的关联分析、基于攻击序列的关联分析、基于终端的关联分析等，分析海量安全事件之间的关系，排除无效安全事件，发现严重安全事件，减少漏报误报。

同时，通过监控各网络和网段的流量变化，根据一定的网络流量模型，通过有效的分析算法，发现网络的运行状态和网络异常流量行为。分析性能数据形成必要的报告，根据性能数据、故障信息、告警信息形成统计报表。

（3）智能业务风险分析和响应预警

依据信息安全等级保护原则，采用大数据技术和人工智能技术，对各安全监控点采集的海量数据进行智能分析，从中挖掘隐藏的安全问题，发现安全威胁信息。根据各监控点的资产信息、脆弱性统计信息以及安全威胁分布情况进行分析，评估安全风险，最终确定图书馆各业务点的安全风险等级。根据图书馆业务的重要性计算出整个图书馆的整体安全风险等级。在综合风险评估的基础上，向管理人员呈现相关风险报表。

通过智能化的业务风险管理，掌握图书馆信息系统的整体以及局部的风险状况，根据不同级别的风险状况，及时采取降低风险的防范措施，从而将风险降低到可接受的范围内。

依据信息安全管理平台制定的安全策略，及时调动有关资源做出响应处理，降低风险对图书馆系统的负面影响。响应方式包括对各种安全设备或图书馆的资产采取阻断攻击、改变配置等，以消除威胁。对无法自动处理的则可以通过邮件、短信等方式通知相关人员进行处理。

对风险结果形成的预警信息，及时传递到指定的安全管理人员，使安全管理人员掌握网络的最新安全风险动态，防患于未然，也为安全策略调整提供依据。如果安全事件的级别超过指定级别，自动产生预警信息，或手动创建预警信息。

（4）安全审计和趋势分析

支持各类安全审计功能，包括上网审计、邮件审

计、系统访问日志审计、加密文件使用审计、终端使用审计、防病毒审计、设施使用流程审计和图书馆业务流程审计等。图书馆中存在一些涉密文档，需要采取内部保护措施，通过大数据分析技术，挖掘故障数据和安全事件之间的内在联系，帮助管理员预测某些安全威胁发生的概率，以及下一个时间段可能出现的信息安全问题，以便提早预防和及时应对。同时提供基于天、周、月及特定时间段内的趋势分析，为领导决策服务。

（5）可视化展示

信息安全管理平台提供统一的Web登录界面，根据登录人员的身份展现不同的管理界面。同时提供多种Web显示方式，将各个部分的信息进行集中显示和发布，可支持报表、信息仪表盘、网络拓扑、电子地图等信息显示和发布方式。

基于报表的信息显示，是通过报表方式显示信息，简单明了，支持信息的检索、排序和查询。

基于信息仪表盘（Dashboard）显示，是通过整合数据和信息，以可视化的方式提高用户的判断、监控和决策，便于安全管理者轻松高效地监控整个图书馆的安全状况。

基于网络拓扑的信息显示，便于在逻辑层确定安全事件发生的区域和位置。

基于电子地图的信息显示，对具有多级结构的图书馆更加实用。通过与电子地图系统联动，可以定位安全事件发生的物理位置。

## 4 结语

随着物联网、云计算、移动网络的应用，图书馆在提供更加便捷服务的同时，也面临更多的安全威胁，需要加强图书馆的安全管理，提高信息安全管理水平和效率。本文在分析传统信息安全管理平台缺点的基础上，充分利用云计算、大数据和人工智能技术，构建面向图书馆业务的信息安全管理平台，以实现高效精确的安全管理，保证图书馆业务的连续性。

### 参考文献

[1] 李伟伟.面向业务的安全管理平台研究与实现[D].山东:曲阜师范大学,2012.

[2] 赖睿.运营商IP网安全管理平台SOC的设计与工程实现[D].陕西:西安电子科技大学,2012.

[3] 笪大伟.一种新型信息安全管理平台的设计与实现[D].北京:北京邮电大学,2008.

[4] MSTL_JUF_04-0190101-2006信息安全技术安全管理平台产品检验规范[S].公安部计算机信息系统安全产品质量监督检验中心,2006-01-01.

[5] 李伟伟,曹宝香.基于云计算的安全管理平台技术研究[J].电子技术,2013(5):8-10.

[6] 田燕,等.基于身份认证和访问控制的云安全管理平台[J].测控技术,2012,32(2):97-100.

### 作者简介

李留英（1972-），女，博士，南京政治学院上海校区军事信息管理系教授，硕士生导师，研究方向：信息安全、信息化。E-mail: lly003@vip.sina.com

Information Security Management Platform Based on Library Business

Li Liuying / Department of Military Information Management, Shanghai Branch of Nanjing Political College, Shanghai, 200433

Abstract: Information security management platform is an important means to improve the security management of the library. This paper analyzes the current development of information security management platform, security threats faced by the libraries, proposes to use big data and cloud computing technologies to build information security management platform based on library business, and discusses its architecture and main functions to ensure the continuity and availability of library service.

Keywords: Based on business, Library, Security management platform

（收稿日期：2014-01-08）