电子政务信息开放共享的安全保障

周玉建 吕艳丽
（科学技术部信息中心，北京 100862）

摘要：我国电子政务信息系统的建设取得了长足的发展，信息公开的推进赋予电子政务开放、协同、交互等特点，信息安全是根本保障。作为一项系统化工作，信息安全保障体系建设是信息系统安全稳定运行的关键。本文在分析已有网络安全保障模型的基础上，结合电子政务信息开放共享所面临的安全威胁，参考国家相关标准和要求，设计了一套以事件处置为核心的信息安全保障技术框架，并在科技部实际应用中得以检验。

关键词：信息安全保障；电子政务；开放共享；事件管理
中图分类号：TP309 **文献标识码：**A **DOI：**10.3772/j.issn.1674-1544.2016.03.012

Research on the Security of Information Open-Sharing of e-Government

ZHOU Yujian, LÜ Yanli
(Information Center of the Ministry of Science and Technology, Beijing 100862)

Abstract: The construction of e-government information system in China has made great progress, and information disclosure makes e-government open, cooperative and interactive, which is based on information security. Information security system construction is the key to the operation of information system. This paper analyzed the existing network security model, designed an information security technology framework in compliance with national policies and standards, which is based on security event management as the core and has been used in Ministry of Science and Technology (MOST) network.

Keywords: information security, e-government, open-sharing, security event management

1 引言

在信息化不断推进的今天，电子政务信息开放比任何时候更依赖网络，然而互联网自身的缺陷、漏洞的频发、安全监管的缺失等原因都导致电子政务面临技术、管理、立法等方面的安全威胁[1-2]。特别是电子政务信息系统涉及国防、公共安全、国家机密等内容，一旦信息被泄露并遭到破坏，政府部门甚至国家安全都会遭受损失。近年来，国家信息安全漏洞共享平台（CNVD）新增收录漏洞数量年均增长率在15% ～ 25%，针对漏洞的挖掘和利用研究日趋活跃[3]。2014年，CNVD收录并发布各类安全漏洞9163个，涉及电子政务的占1.9%。目前，我国的信息安全防护能力还有多个薄弱环节，网络安全研究的主要关注点还集中在漏洞的修补和拦截上，而解决以上问题的根本在于信息安全保障体系的建设[4]。安全保障工作也随之从网络、应用、数据等单点保障向系统化方向发展，成为一个系统的工程[5]。

为了提高我国信息系统的整体防护能力，国

作者简介：周玉建（1964—），男，科学技术部信息中心副主任，高级工程师，研究方向：电子政务；**吕艳丽***（1980—），女，科学技术部信息中心高级工程师，研究方向：网络安全。

收稿时间：2016年1月7日。

家相关部门成立了信息安全组织保障体系，制定和引进了《GB17895-1999计算机信息系统安全保护等级划分准则》、《ISO/IEC 17799-2000信息安全管理实施准则》、《BS 7799-2：2002信息安全管理体系实施规范》等信息安全标准，制定了《中华人民共和国计算机信息网络国际联网管理暂行规定》、《商用密码管理条例》等相关法律、条例和规定。

信息安全保障的研究最早开始于1995年。关于信息安全保障的定义主要有两类：一类是美国国防部给出的定义，即信息安全保障是以确保信息及信息系统可用性、完整性、身份鉴别性和不可否认性为目标而采取的操作，包括保护、检测、反应以及恢复能力；另外一类将信息安全保障作为一种较为全面和系统的规范和方法，为信息系统的动态组合提供运行环境。

目前，针对相关模型已经开展了广泛的研究。主要的信息安全保障模型是在闭环控制的动态网络安全理论模型的基础上发展起来的。其中，典型模型包括PDR模型与P^2DR模型。

PDR模型主要包括三部分：防护、检测和响应，如图1所示。该模型的攻击、防护、检测、响应等与信息安全相关的所有活动都要以消耗时间为代价，系统的安全性和安全能力是基于时间，而非永久性的，即若不考虑时间成本，任何防护措施都是可以被攻破的[6]。该模型表明，及时检测和响应、及时检测和恢复即为安全。

P^2DR模型主要包括四部分：安全策略、防护、检测和响应，如图2所示。该模型在PDR模型的基础上增加了安全策略，是基于健壮性和时间。该模型以安全策略为中心，在安全策略的控制下，利用防护工具和检测工具来分析和评估系统的安全状态，通过采取相应的响应措施降低系统的安全风险，提高安全性[7]。该模型从全局出发，强调系统的动态安全性，是一个螺旋上升的过程，安全防护在循环中得以提高。该模型表明安全防御的关键在于及时检测和响应。

研究者们基于以上模型根据自己的实际需求不断提出改进。张千里和陈光荣[8]提出P^2DR模型的基础上强调恢复工作，形成PDRR模型，即防护、检测、响应和恢复。赵战生[9]提出在PDRR 模型的基础上前面加上一个警告，后面加上一个反击，反映了六大能力，分别是预警能力、保护能力、检测能力、反应能力、恢复能力和反击能力。QU和YAN[10]扩展了P^2DR模型，给出了WP^2DR^2C模型，包括安全策略、防护、检测、响应、恢复、反击和警告。

随着电子政务信息开放共享模式的变化和发展，信息安全保障在数据处理、事件响应、管理机制等方面提出了新的要求，尽管以上模型提供了较为完整的解决思路，但仍然存在一定的局限性。

（1）欠缺管理因素。我国电子政务虽然呈现出良好的发展势头，但因为缺乏整体规划和统一标准，各自为政的局面较为普遍[1]，进而造成各电子政务信息系统安全管理能力参差不齐，建设及管理人员技术能力差异较大，在信息开放共享的大环境中，面临的安全风险也不尽相同。

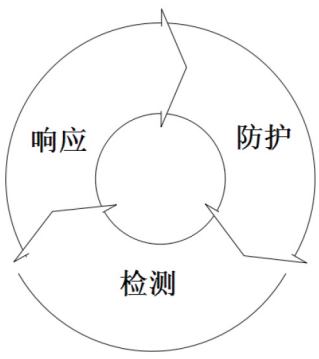

图1 PDR模型

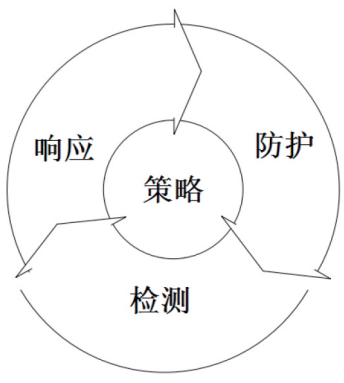

图2 P^2DR模型

PDR模型基于既定的攻防时间表运转，缺乏网络环境变化的适应性，攻击手段、防护人员等因素的变更会导致攻防时间的变化，降低模型的应用效果。P^2DR模型缺少评估和分析环节，导致策略的制定具有一定的盲目性。ISO 7498−2 标准指出，安全体系模型主要包括安全服务、安全机制和安全管理三部分[11]，充分考虑安全管理及安全服务才能保障电子政务的整体安全。

（2）流量剧增、攻击事件复杂度上升等因素，要求具有更高的监控和分析能力。电子政务应用的发展以及互联网应用的普及，使电子政务面向社会服务能力显著提高，产生的网络流量与发生的安全事件呈快速增长趋势，对安全事件响应和处理的及时性提出更高要求。科技部电子政务应用每天产生的网络流量达数百GB，发生的安全事件达上万件，在此应用环境中，依据PDR和P^2DR模型难以及时对安全事件作出响应。此外，网络攻击手段日益复杂，PDR和P^2DR模型中依靠安全设备不具备发现和处置复杂攻击的能力。

本文针对电子政务信息开放、协同、交互、服务等特点[12]，结合科技部电子政务运行中面临的实际安全威胁以及国家相关要求，探讨构建了一个较为完整和系统的信息安全保障技术框架，并在实际应用中得到检验。

2　信息安全保障技术框架

为了维护国家安全和社会稳定，全面提高信息安全保障能力和水平，我国提出实行电子政务基础设施的信息安全等级保护[13]，依据信息及载体的重要性对信息系统进行等级划分，在技术和管理上采用相适应的措施对不同等级的信息系统提供不同安全保护。

依据信息安全等级保护及相关标准[4，14−20]，本文给出了以管理制度、网络基础环境和安全基础环境以及安全事件风险管理互为支撑和反馈的信息安全保障技术框架（图3），管理制度、网络基础环境以及安全基础环境为安全事件风险管理的开展提供必要条件，安全事件风险的管控效果为管理制度、网络基础环境和安全基础环境的优化提供依据。

（1）信息安全管理制度。等级保护管理建设包括的内容较多，信息安全管理制度建设包括安全管理制度、安全管理机构、人员安全管理制度、系统建设管理制度、系统运维管理制度等。在制度制定中重点关注的内容包括管理制度的评审和修订的及时性、身份认证权限和设备撤销或收回的及时性、外部人员的管控到位情况、保密协议的签订情况等。

（2）网络基础环境。基础网络是承载电子政务信息系统运行的平台，其建设情况直接决定了整个信息系统的运行保障情况。网络基础环境的建设和管理包括网络设备的建设和管理、网络链路的建设和管理、通信质量保障措施的建立、网络接入合规性和合法性管控措施的建立以及对产生的网络流量的管理和分析。

（3）信息安全基础环境。信息安全基础环境是整个信息系统的安全运行情况的基础保障，通过在网络层、主机层、应用层和数据层部署所需的安全防范措施，制定相应的安全策略达到以下目标：在网络层实现入侵防范、访问控制、恶意代码防范、网络监控、网络审计等；在主机层实现身份鉴别、访问控制、安全审计、主机入侵防范、主机恶意代码防范、资源控制等；在应用层实现身份鉴别、访问控制、安全审计、资源控制等；在数据层实现备份与恢复、完整性保护、保密等。

（4）信息安全风险管理。围绕安全事件处置的生命周期，信息安全风险管理通过事前监控、事中处置和事后分析来发现网络安全异常现象、清除安全威胁以及改进运维和管理，是一个闭合的运转过程，如图4所示。

事前监控是对各网络和安全设备的运行状态、系统日志、安全日志、网络等进行实时采集和分析，以及时发现网络中的攻击、入侵、故障、病毒等异常网络安全现象。

事中处置是针对事前监控中发现的异常网络安全现象，深入分析相应的数据和日志，采用

图3　信息安全保障技术框架

操作系统和中间件安全检查、渗透测试、异常文件安全分析等技术手段定位威胁来源，明确事件原因，判断安全事件发展趋势以及可能造成的安全损失和对当前网络安全状态的影响。根据以上分析和判断结果，制定网络安全处置方案，调配所需的人财物等资源，修复和验证漏洞，清除威

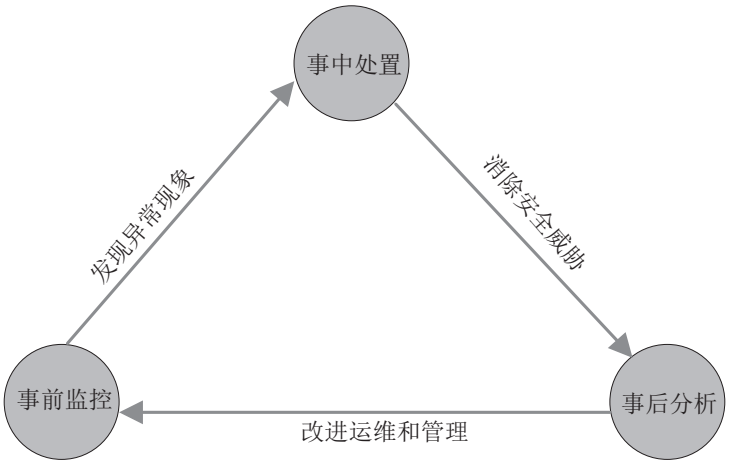

图4　信息安全风险管理流程

胁，实施相应的恢复和重建工作。

事后分析是及时检查、分析、修正、补充安全事件，针对引起安全事件的漏洞、文件或者突发的网络行为实施免疫处理，总结分析安全事件的处置经验，改进运维和管理方式，完善信息安全管理制度、网络基础环境和信息安全基础环境。

3　信息安全保障技术的实施

信息安全保障技术框架的指导思想和设计原则如下。

第一，构建纵深防御体系，实现层层保护。根据网络结构和信息系统业务流向设置多道安全防线，实现不同安全区域之间的保护以及网络边界、基础平台、主机及业务应用的多层次保护。

第二，实现网络安全集中管控，提高网络安全防御效能。通过集中管控方式，建立较为完善的网络安全数据体系和信息共享体系，提升网络安全防御能力，为管理员的防御决策部署和信息技术风险控制提供依据，并降低总体成本。

第三，统一规划统一设计，避免防御短板。在规划设计中，从提升网络安全整体保障能力出发，统筹考虑各单位或各部门之间的信息化发展的不均衡现象，制定完整的规划和设计方案，确保网络中各节点均可达到预期的信息安全防御能力。在实施过程中，可以根据具体的所涉及范围、技术特点以及经费预算等情况，以基础运行环境和重点应用、重点数据为核心分步实施。

科技部信息中心已依据本文给出的技术框架逐步建立了较为完善的科技部电子政务信息安全保障体系，并在近年来的运行中取得了较好的防护效果。

（1）门户网站、邮件等信息系统的安全防护体系符合国家要求。经过多年建设，科技部基础网络环境和安全防护能力均有了较大的提升，围绕门户网站、邮件等重要信息系统形成了一套包括带宽保障、访问控制、内容过滤、入侵防护、病毒防护、安全审计、安全值守在内的较为完善的安全保障体系，通过了信息安全等级测评，基本达到国家安全防护要求。

（2）安全漏洞的发现及预警能力增强。针对门户网站、邮件等重要信息系统的业务特点，建立了有效的信息安全值守和自查制度，每天对系统和设备运行情况、终端安全情况、网络安全情况进行监控和分析，并与渗透测试、主机安全检查、挂马检查等自查机制结合，提高漏洞的安全管理能力。在新的漏洞，如“心脏滴血”漏洞发布后，立即评估了漏洞影响范围，通知存在该漏洞的信息系统及时修补漏洞，并在网络监控中加强OpenSSL协议流量的监控和分析，将漏洞破坏遏制在萌芽状态。在安全值守发现某应用面临较多攻击或较高安全风险后，启动渗透测试、主机安全检查等进一步发现其可能存在的安全隐患。

科技部重要信息系统近年来运行平稳，全年

网络连通率达100%，重要信息系统的安全自查覆盖率达100%，监控覆盖率达100%，数据流量分析深入分析比例超过40%，全年监控发现并处理的安全事件超过300万件，自查发现的安全漏洞达数十个，实现安全责任零事故。

4 结论与展望

网络攻击不断呈现出分布式、协作式、复杂式的趋势，信息安全保障工作要不断完善和改进才能满足需求。根据网络安全态势发展趋势，本文的信息安全保障工作在以下几方面尚需提高。

（1）存在一定滞后性。目前，各安全技术和产品均是对已经发生的安全事件进行检测，一旦发现严重的安全事件，安全事件已经发生，管理员无法预先部署有效防御措施，安全破坏已经造成，损失无法弥补。

（2）准确性不高。安全检测系统发出警报存在虚警量大、误报率以及漏报率高，带来大量后续事件验证和评估工作，管理员无法根据其报警信息及时作出防御决策。

（3）缺乏对未知安全事件的防护。基于特征库和既定规则的机制使得安全防护系统不能识别攻击特征库中和已有规则库中不存在的安全事件，无法防御未知网络攻击。

电子政务信息系统是一个以计算机网络技术为基础，以共享、交流、协作为核心，以政务的信息流、工作流相对集成为基本结构的系统，在面向公众的服务中发挥着越来越重要的作用，但其根本是信息安全。本文针对电子政务开放共享所面临的安全威胁，从安全体系整体着手，构建了以安全事件处置为核心的安全保障体系，在实际应用中取得较好的效果。同时，针对网络安全态势的发展趋势，给出了下一步改进意见。

参考文献

[1] 孟薇.电子政务信息安全研究[D].天津：天津大学，2007.

[2] 于施洋. 对新时期我国电子政务发展几个问题的思考[J].电子政务,2008 (1): 44−49.

[3] 国家计算机网络应急技术处理协调中心. 2014年我国互联网网络安全态势综述[R].2015.

[4] 公安部信息安全等级保护评估中心. GB/T22239−2008 信息安全技术信息系统安全等级保护基本要求[S]. 2008.

[5] 沈昌祥.加强信息安全保障体系的思考[J].信息网络安全, 2002 (11): 11−14.

[6] 孟学军,石岗.基于PZDR网络安全体系结构[J].计算机工程,2004,30(4): 99−101.

[7] 陈运明.动态网络安全模型的系统研究[J].网络安全与技术应用,2005(5): 47−49.

[8] 张千里, 陈光英.网络安全新技术[M] .北京：人民邮电出版社, 2003.

[9] 赵战生.信息安全保障技术发展动态与印象[C]//中科院信息安全国家重点实验室会议报告, 2001.

[10] QU Zhaoyang, YAN Jia. The design of the network security model of active defense[C]. 4th International Conference on Wireless Communications, Networking and Mobile Computing, 2008: 1−4.

[11] ISO. ISO DIS 7498−2 information processing systems: open system interconnection reference model, part 2: security architecture[S] .1989.

[12] 赵鹏高.云南省电子政务信息安全保障体系建设研究[D] .昆明：云南大学, 2012.

[13] 国家信息化领导小组关于加强信息安全保障工作的意见(中办发[2003]27号) [R]. 2003.

[14] 刘春年, 娄策群. 电子政务概念解读[J]. 国外情报科学, 2004(5): 603−606.

[15] 公安部信息安全等级保护评估中心. GB/T22240−2008 信息安全技术 信息系统安全保护等级定级指南[S]. 2008.

[16] 公安部信息安全等级保护评估中心. GB/T 25058−2010 信息安全技术 信息系统安全等级保护实施指南[S]. 2010.

[17] 公安部第一研究所. GB/T 25070−2010 信息安全技术信息系统等级保护安全设计技术要求[S].2010.

[18] 北京思源新创信息安全资讯有限公司, 江南计算机研究所技术服务中心. GB/T 20269−2006 信息安全技术 信息系统安全管理要求[S]. 2006.

[19] 中国科学院研究生院国家计算机网络入侵防范中心, 中国电子技术标准化研究所. GB/T 24363−2009 信息安全技术 信息安全应急响应计划规范[S]. 2009.

[20] 国家信息中心, 公安部第三研究所, 国家保密技术研究所, 等. GB/T 20984−2007 信息安全技术信息安全风险评估规范[S]. 2007.