政务信息安全管理与应用丛书

政务信息系统安全测评应用指南

刘海峰　李媛　毛东军　等　编著

中国质检出版社
中国标准出版社

| 政务信息安全管理与应用丛书 |

政务信息系统安全测评应用指南

刘海峰 李 媛 毛东军 张晓梅 钱秀槟 王春佳
赵章界 梁 博 胡 冰 李晨旸 杨泽明 刘 涛 ◉编著

中国质检出版社
中国标准出版社
北 京

内 容 提 要

本丛书从电子政务的固有特点出发，结合编者单位丰富的实践经验，围绕电子政务信息安全保障的重点领域，介绍了信息安全的实用技术方法。

本书为丛书的安全测评分册，以非涉密政务信息系统安全测评为主线，综合了风险评估、等级测评、验收测评等三种常见的安全测评方式的具体特点，全面覆盖了安全测评的标准法规、原理、技术、方法流程、工具等内容。

本书可为政务信息系统的运营单位、使用单位、安全服务机构、安全测评机构、重要行业的主管部门以及国家信息安全监管机构等的相关人员提供参考，从而为政务信息系统安全测评工作的顺利开展和完成提供相应的帮助。

图书在版编目（CIP）数据

政务信息系统安全测评应用指南/刘海峰，李媛，毛东军等编著．—北京：中国标准出版社，2013.8

ISBN 978-7-5066-7222-1

Ⅰ.①政… Ⅱ.①刘…②李…③毛… Ⅲ.①电子政务—管理信息系统—安全技术—评价—指南 Ⅳ.①D035.1-39

中国版本图书馆 CIP 数据核字（2013）第 177257 号

中国质检出版社
中国标准出版社出版发行

北京市朝阳区和平里西街甲 2 号（100013）
北京市西城区三里河北街 16 号（100045）

网址：www.spc.net.cn
总编室：（010）64275323 发行中心：（010）51780235
读者服务部：（010）68523946

中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

*

开本 787×1092 1/16 印张 15.5 字数 347 千字
2013 年 8 月第一版 2013 年 8 月第一次印刷

*

定价 45.00 元

丛书编委会

丛书序

中国正处在高速发展时期，随着人们生活水平的提高，社会对政府提出了越来越高的要求。利用信息技术对政府拥有的和需要的资源进行使用和管理，提高资源的使用效率和政府的办事效率，是建立服务型和经济型政府的必然选择。目前，我国大到中央政府，小到乡镇街道，都广泛开展了政府信息化应用，应用范围涵盖门户网站、日常行政办公系统、指挥高度系统、决策支持系统、行政审批系统以及网上报税等。这些信息化应用对促进政府职能转变、提高政府工作效率和办事水平、提供优质的政府服务等起到了非常重要的作用。

政府信息化带来巨大效益的同时，人口、交通、卫生、教育、税收、执法、统计等行政管理越来越依赖信息化手段，也使得政府掌握的各类资源面临着更多的威胁。这些威胁来自自然灾难和恶劣的自然环境、信息化设施设备和系统自身的故障以及人为的有意或无意的破坏等。对政府信息系统实施攻击的，不局限于个人，还包括具有强大攻击力的敌对势力，甚至敌对国家。另一方面，信息化应用天生就是不安全的，政府单位在建设信息系统时追求速度和节约成本的动力远远大于对安全的需求，这导致信息系统常常千疮百孔。两方面的因素结合起来，加上针对信息系统的攻击比传统攻击更加低廉和便捷，导致针对政府的信息安全攻击层出不穷。政府网站被黑，政府管理的公民隐私信息泄露，网上缴税系统瘫痪等，严重影响了政府的公信力和行政能力。

我国政府高度重视信息安全和保密工作。早在1994年，我国就发布了《中华人民共和国计算机信息系统安全保护条例》，对计算机信息系统安全等级保护、计算机信息系统安全专用产品销售等做出了具体规定。而2003年的《中共中央办公厅、国务

院办公厅转发〈国家信息化领导小组关于加强信息安全保障工作的意见〉的通知》（中办发［2003］27号）则对信息安全工作做出了全面部署。我国各级政府积极落实信息安全等级保护制度，开展网络信任、安全测评、安全预警、容灾备份、应急处置等工作，规范信息安全产品和服务的管理，加强信息安全和保密的监督检查。

作为我国首都，北京市积极贯彻落实国家信息安全和保密管理的政策法规和市委市政府领导的指示精神，努力把自身打造成信息安全一流的可信城市，保障首都安全，促进首都经济发展。北京高度重视信息安全工作的组织领导，成立了北京市网络与信息安全协调小组和北京市通信保障和信息安全应急指挥部；积极开展信息安全监督管理工作，进行多种形式的专项检查和联合检查；加强网络与信息安全应急体系建设，建立快速有效的分等级信息安全应急响应与处置机制；积极推进等级保护工作，加强信息系统建设方案的安全审查和建设完成后的安全测评与定级备案审查；加强基础设施建设，建立了北京市政务网络信息体系、北京市信息安全容灾备份中心、北京市通信保障和信息安全应急指挥平台、北京市政务信息安全监控预警系统等一批信息安全基础设施；完善信息安全法规政策和标准体系，发布了《北京市信息化促进条例》、《北京市公共服务网络与信息系统安全管理规定》等一系列政策法规和标准。北京在信息安全与保密管理方面取得了丰硕成果，为成功举办2008年奥运会与残奥会以及新中国成立60周年大庆做出了重要贡献。

本丛书总结了北京在信息安全基础设施建设和信息安全保障工作方面的理论研究成果和实践经验，希望能对未来北京市政务信息安全保障起到推动作用，同时也能对其他省市有参考和借鉴意义。

2011年11月

序

在经济全球化和社会信息化快速发展的大背景下，信息技术对经济社会发展的影响、带动作用日益凸显，成为推动经济社会发展和产业变革的重要力量，也已成为衡量一个国家或地区经济发展、社会进步的重要标志。政务信息化是信息技术在政府部门应用的一个重要方向，是政府部门加快转变职能、提高工作效率、增强其社会管理和公共服务能力的重要手段。

我国一直致力于电子政务信息资源共享平台的建设，截至目前，以“金字工程”、“数字城市”、“智慧城市”等为代表的顶层应用系统的发展已趋于成熟，为全面实现工业化和信息化深度融合提供了有力保障。随着政府在电子政务系统的投入不断增多，电子政务发展日新月异。但在一定范围内存在着“重建设、轻安全”的倾向。一些建成的系统虽然广泛部署各种网络安全技术和产品，对系统的安全性还是不能做到心中有数。电子政务信息系统的安全漏洞较多，病毒、木马、钓鱼僵尸网络、间谍软件、恶意软件的攻击等依然十分猖獗，APT 等新的攻击形式也层出不穷。因此，信息安全是当今政务信息化建设最引人关注的关键问题之一，没有信息安全的坚实保障，电子政务就难以有效推进与前行。

北京信息安全测评中心根据多年来的理论研究和测评实践，编写了《政务信息系统安全测评应用指南》一书，该书从对我国政务信息系统安全威胁与防护体系详细剖析入手，全面阐述了国内外信息安全测评发展与现状以及相关的政策文件及标准；从多个角度对政务信息系统安全测评进行了分类，并从技术和管理两方面详细介绍了测评工作内容；针对主要测评模式，结合测评中心工作实践就具体的测评流程和工作内容展开详尽讨论；最后，从提高测评结果质量的目的出发，讨论了安全测评质量管理相关要求，并简要介绍了信息系统安全测评常用工具。我认为这是一本理论系统、内容丰富、贴近实践的专业著作，拜读后感到获益匪浅。

“十二五”是我国电子政务建设的关键时期，也可能是政务信息系统安全问题的凸显期。政务信息系统的安全问题的解决，需要大家的共同努力和积极探索，希望本书能为进一步推动和深化政务信息系统安全测评工作提供有力帮助。

受本书编者的盛情相邀，以此为序。

崔书昆

2013年5月

前　言

政务信息系统是各有关部门和地方各级政府利用信息和网络通信技术，加强政府的管理，实现政务公开、提高效率、科学决策、改进和完善服务职能的重要手段。随着电子政务的深入发展和人们对信息依赖程度逐渐提高，电子政务的安全问题也越来越突出，电子政务信息系统中被发现的安全漏洞越来越多，针对电子政务信息系统的攻击更是层出不穷。缺乏安全保障的电子政务信息系统，就不能实现真正意义上的电子政务的功能。

目前，多数政务信息系统在建设上，一定范围内存在着“重建设、轻安全”的倾向。系统建设完成后对系统的安全性还不能做到心中有数。进行电子政务系统安全测评是掌握已投入或将投入使用的电子政务系统安全性的必要手段。近年来，随着《信息安全等级保护管理办法》、《关于加强国家电子政务工程建设项目信息安全风险评估工作的通知》、《国家电子政务工程建设项目管理暂行办法》等国家文件的相继出台，从国家机关到地方各级政府都已逐步开展了政务信息系统的安全风险评估、安全等级测评、安全验收测评等测评工作，对安全测评的重视程度显著提高，但是安全测评的质量和产生的效果仍然参差不齐。针对政务信息系统的安全测评，其测评对象往往是一个庞大的、错综复杂

的信息系统，因此需要采用系统的、科学和安全的测评方法，只有这样才能体现测评结果的客观性、科学性和公正性。

本书以非涉密政务信息系统安全测评为主线，综合了风险评估、等级测评、验收测评等三种常见的安全测评方式的具体特点，全面覆盖了安全测评的标准法规、原理、技术、方法流程、工具等内容。全书共分为9章。第1章阐述了信息系统安全的有关概念和背景，重点介绍了我国政务信息系统的发展及业务开展情况，分析了政务信息系统安全的基本特征和常见的安全威胁，提出一套综合的信息系统安全防护体系。第2章介绍国内外信息安全测评的发展与现状，重点分析了国外信息安全测评标准、信息安全管理体系标准的发展历程，国内信息安全测评的发展过程、现状及发展前景，同时总结性地提出了信息安全测评的重要原则。第3章介绍我国信息安全测评相关的政策文件及标准，包括国家政策文件、地方政策文件、行业政策文件，以及风险评估、等级保护、安全验收等相关的标准规范，这是从事信息安全测评工作的基础和指导。第4章介绍安全测评的分类，从测评目标、测评内容、实施方式等不同维度对安全测评进行了分类和测评内容描述，有助于全面理解安全测评工作和各个层面的具体测评内容。第5章介绍安全测评的模式和方法，主要围绕风险评估、等级测评和验收测评三种模式展开内容和方法概述。第6章介绍安全测评技术，从技术安全性测评和管理安全性测评两个方面描述了针对政务信息系统的安全测评技术，是风险评估、等级

测评、验收测评三种测评方式都需要实施的具体测评内容。第7章综合了当前相对独立的风险评估、等级测评、验收测评流程，介绍了这三类测评方式的通用测评流程和工作内容，并对测评各阶段的主要工作流程和任务等方面进行了详细描述。第8章介绍了安全测评质量管理，提出了质量管理和质量管理体系的建立需求，并重点介绍了安全测评质量管理的八个主要方面。第9章介绍安全测评中常用的测评工具。附录中提供了测评过程中重要的文档模板和典型案例等相关内容。

本书是在北京信息安全测评中心多年政务信息系统风险评估、等级测评、验收测评工作的具体实践基础上整理总结而成的成果，融合了最新的信息安全测评标准法规、方法和技术，可以为政务信息系统的运营单位、使用单位、安全服务机构、安全测评机构、重要行业的主管部门以及国家信息安全监管机构等的相关人员提供参考，从而为政务信息系统安全测评工作的顺利开展和完成提供相应的帮助。

由于水平有限，书中难免存在不足之处，欢迎广大读者批评指正。

编著者

2013年5月

目　录