XINXI ANQUAN CEPING
RENZHENG LILUN
YU SHIJIAN

Xinxi Anquan Ceping Renzheng Lilun Yu Shijian

信息安全测评认证
理论与实践

吴世忠 陈晓桦 李鹤田 李斌 等 编著

中国科学技术大学出版社
北京中电电子出版社

信息安全测评认证理论与实践

吴世忠　陈晓桦　李鹤田　李　斌　等　编著

中国科学技术大学出版社
北京中电电子出版社

内容简介

本书从理论和实践两个方面全面阐述了信息安全测评认证的技术、标准、体系等，为政府、行业和企业提供相关技术依据，为把握我国未来测评认证事业的发展方向提供良好的借鉴。该书适用于信息安全领域的管理者、从业者和研究人员。

图书在版编目（CIP）数据

信息安全测评认证理论与实践/吴世忠等编著. —合肥：中国科学技术大学出版社，2006. 6

ISBN 7-312-01969-2

Ⅰ. 信… Ⅱ. 吴… Ⅲ. ①信息系统—安全技术—评价②信息系统—安全技术—认证 Ⅳ. TP309

中国版本图书馆 CIP 数据核字（2006）第 056091 号

出版：中国科学技术大学出版社
（安徽省合肥市金寨路 96 号，230026）
北京中电电子出版社
（北京海淀区翠微东里甲 2 号为华大厦 4 层，100036）
责任编辑：邵祖英 高伟红
发行：中国科学技术大学出版社
印刷：北京华正印刷有限公司
经销：全国新华书店
开本：889mm × 1194mm 1/16
印张：15.5
字数：395 千字
版次：2006 年 6 月第 1 版
印次：2006 年 6 月第 1 次印刷
印数：1—3500 册
定价：69.00 元

序一

曲维枝

当今世界，以信息技术为代表的科技革命不断取得突破，信息化已经成为各国经济和社会发展的强大动力，无论是发达国家还是发展中国家，都在适应时代前进的潮流，把推进信息化作为增强综合国力和国际竞争力的战略选择。我国政府明确提出“信息化是覆盖现代化建设全局的战略举措”，把信息化建设提升到了国家发展战略的高度。

然而随着信息化进程的不断深入，日益突出的信息安全隐患和威胁，不仅对信息化建设产生了不利影响，而且影响到了我国政治、经济、文化、军事和意识形态的各个方面。为此党和政府高度关注信息安全问题，2003 年国家信息化领导小组第三次会议审议通过了《关于加强信息安全保障工作的意见》。2004 年 1 月，国家信息化领导小组又专门组织召开了全国信息安全保障工作会议，明确了信息安全保障工作的指导思想、基本原则和主要任务，为做好信息安全保障工作确定了大政方针、基本理念和总体思路。

信息安全测评认证工作是信息安全保障的基础性工作，也是目前加强信息安全保障的重点工作之一。信息安全测评认证是在信息技术广泛应用到国家生活的各个方面，信息安全产品和信息系统因其固有的敏感性和特殊性，对国家安全利益的影响越来越大的环境下产生和发展起来的。它对我国按国际惯例建立和实施有关信息安全产品、信息安全产品的市场准入制度、加强国家对技术安全的管理和确保网络与信息系统的安全运行等方面都起着十分重要的基础支撑作用；对广大用户采购信息安全产品，设计、建设、使用和管理安全的信息系统提供科学公正的专业指导；对信息安全产品的研究、开发、生产以及信息安全服务的组织等提供严格的规范引导和质量监督。因而信息安全测评认证体系的建立和运行，对我国信息安全保障工作和信息化建设具有十分现实的意义。

我国信息安全保障体系的研究刚刚开始，高度重视安全保障体系的研究和实践，乃是当务之急，刻不容缓。我国互联网上严峻的信息安全形势，以及国外信息安全方面的经验和教训等，都给我们提出了理论上和实践上的挑战，也为我们敲响了警钟。要有效地解决信息安全问题，都需要我们采用科学的方法和现实的态度，认真观察和分析信息安全问题的实质和特点，逐步建立起科学、合理而又适合中国国情的本土化的信息安全保障体系，为我国的信息化发展提供可靠的安全保障。

我国信息安全测评认证工作起步不晚，早在 1997 年，第一届国务院信息化工作领导小组就已将信息安全的测评认证工作纳入议事日程，在国家各有关部门的大力协助和共同支持下，我国参照国际通例，设立了专门的信息安全产品测评认证机构，制订了相关的技术安全标准，开展了针对主流信息安全产品的测评认证服务。经过近 8 年的探索和实践，积累了很多宝贵的经验，初步建立了能与国际接轨的测评标准，工作程序和测评方法，在信息技术产品安全，系统安全和信息安全服务等方面基本形成了服务能力，

基本上能满足现阶段对信息安全产品和信息系统进行测评认证的需要。随着国家信息化进程的加快和网络化应用的普及，无论是政府或是民间对信息安全测评认证的需求都将日益增加，正是基于这一现实需求，全国信息安全保障工作会议强调，要进一步加强和规范信息安全的测评认证工作。要按照客观独立、公开公正、诚实信用的原则，统一管理、监督和综合协调认证认可工作；要尽快制定、调整认证产品目录；对列入目录的产品，必须经国家认可的机构进行测评认证；要统一标准，实现互认，为信息安全产业发展创造一个良好的市场环境。

在全面贯彻落实中办［2004］27号文的精神，积极建设国家信息安全保障体系的过程中，对信息安全测评认证的理论和实践进行系统地阶段性总结，是一件非常有意义的工作。它将为我国信息安全测评认证不断完善认证体系、推行标准规范、制定技术标准、培育测评机构、加强研究开发、推进国际互认等方面的工作，提供有力的支持。

故尔，《信息安全测评认证的理论和实践》一书出版之际，谨对我国信息安全测评认证工作所取得的成绩表示祝贺，并祝我国的信息安全事业蓬勃发展、繁荣昌盛。

曲作孩

国务院信息化工作办公室常务副主任

序二

何德全

完备的质量认证制度是现代化的重要标志之一。是我国在现代化的进程中必须补好的一课。为什么这么说呢？我们可以做一个简单的历史回顾。西方国家在18世纪末、19世纪初开始了以蒸汽机为代表的技术革命，进入了以机器为基础的近代工业时期，这是大家所熟悉的。但人们往往忽略了19世纪末、20世纪初的又一次产业革命，即生产不再以一个个工厂为单位，而是实现了全面的社会化，出现了现代化大生产。在这个时期，西方在生产的组织管理上，在产品和质量认证中实现了社会化和现代化。在这次飞跃中，服务业异军突起。在不长的时间内，超过了工业，成为最占优势的产业部门。它包括科学技术研究和产品设计、金融和贸易等等。所有这些都有赖于完备的标准化和质量认证工作。这项工作在20世纪上半叶趋于完备和成熟。相比之下，我国在这方面还存在着较大的差距。这是由于我们的观念还停留在上次产业革命之前，所以一直缺乏质量认证的意识、文化和制度。

从20世纪后半叶开始，世界又进入了新的产业革命-信息化。在信息化时代，信息安全问题日趋严重，直接关系到国家安全和民族兴衰。信息技术产品能否保证安全，网络系统是否可靠，必须要有科学、客观和正确的技术评判。作为评判信息安全的手段和技术，信息安全测评认证体系的建立具有举足轻重的意义。这就迫使我们要迎头赶上，以跨越的精神，建设完备的质量认证体系。在这次跨越中，我们遇到了种种传统观念的干扰、小农经济思想的束缚和各方利益的冲撞，因此困难重重。面对这些困难，我们需要以坚持不懈的精神，克服种种困难，把质量认证工作抓上去。

国内外信息安全的理论和实践说明，建立完善的信息安全保障体系是进入信息网络化时代的主权国家捍卫自身安全的重要屏障，也是维护自身利益的主要手段。作为信息安全保障体系的重要组成部分，信息安全测评认证是确保信息安全良性发展的关键所在。

这些年来，我们国家和地方政府逐步建立了基本覆盖全国的信息安全产品测评认证组织体系，建立了一整套与国际接轨的国家信息安全测评认证标准、程序和方法，已基本具备了对信息技术产品安全性、信息系统安全性和信息安全服务资质进行测评和认证的能力，国家信息安全测评认证工作初见成效。

当前，需要进一步加强国家信息安全保障体系建设，应在信息安全测评认证工作中认真贯彻落实中央“坚持以人为本，全面、协调、可持续的科学发展观”，并借鉴国外的先进经验，走合适我国国情的发展道路，把信息安全综合管理中的质量监督、技术控制与产品市场准入、用户采购使用等环节，科学的规范起来。

《中国信息安全测评认证理论与实践》一书，对我国信息安全测评认证工作这些年的发展做了一个很好的总结，希望本书的出版能对我国信息安全测评认证工作起到积极的促进作用。

何德全

中国工程院院士

序三

周仲义

随着信息化的不断推进和互联网在全球范围的迅速发展和广泛应用，信息安全在信息技术的提高和对抗中不断得到发展和充实，信息安全的内容也由原来单一的保密通信扩展为计算机网络信息系统的安全。但同时，层出不穷的网络安全事件的发生，使网络安全问题成为人们关注的焦点。

信息系统中大量漏洞的存在，为黑客和网络犯罪人员提供了攻击的途径；由于我国的微电子技术水平与发达国家存在很大差距，致使信息化所需的不少关键技术设备必须从美国等发达国家引进，使境外垄断关键的信息技术或刻意布署隐蔽通道成为我国信息安全隐患；相关人员安全意识淡薄、安全技术水平较低、管理不善是信息安全发生的主观原因。此外，随着窃密手段的高技术化，网络入侵攻击、计算机病毒、窃听工具以及利用废旧磁介质获取信息等信息破坏的方法更是层出不穷。

如何增强信息产品的安全性，提高信息安全的防护能力，保障基础信息网络或重点信息系统的安全？如何确保计算机网络信息系统在存储、处理、传输信息数据的保密性、完整性和可用性，确保对授权合法用户的服务和限制非授权用户的服务？如何提高信息安全从业人员的总体素质和服务水平，创建健康安全的网络环境？如此等等一系列伴随着网络时代衍生的新问题困扰着人们。

现实表明，面对各种错综复杂的新形势、新问题，为使国家的信息化建设顺利进行，加强我国信息安全保障工作，开展信息安全测评认证具有十分重要的意义。

开展信息安全测评工作将最终达到通过国际贸易间通行的技术壁垒惯例，为国家信息安全保障体系建设提供有力技术基础支撑，阻击国外低水平产品的涌入，减低国家信息化带来的安全风险的目的。

开展信息安全测评认证可降低系统或网络的安全风险，有效保护系统运营单位的信息资产安全，使产品的研制和生产过程逐步走向规范化和标准化；通过对于系统的安全测评和认证可以对信息系统的安全要求、安全策略和安全机制等进行整体验证，提高信息系统整体安全保障能力；通过对现有网络结构与应用现状进行安全分析，对用户的安全风险与危害程度进行检测，提出相应的解决方案，对系统、对数据库和应用程序进行安全管理服务，对具有这些信息安全服务资质的公司、企业的认证保障其相关服务的有效性；对从事信息安全人员进行相关的专业知识教育和培养，并通过严格的标准流程进行信息安全专业人员认证，提升我国信息安全从业人员总体素质和专业水平。

毫无疑问，信息安全测评认证已经成为规范国家信息安全市场、提高国家信息安全综合能力和防范水平、推进国家信息化建设和与国际相关标准接轨的一项重要工作。正是基于这个原因，近年来，世界各国的信息安全测评认证工作均开展得相当蓬勃。在我国，从中办发［2003］27号文件中提出建立信息安全等级保护制度，实行相关信息安全领域重点保护政策，到去年全国的信息安全保障工作会议的隆重召开再到“国认证联［2004］57号文件提出“重要信息安全产品将实行强制性认证”，虽然信息安全测

评认证还是一项比较新的事业，起步较晚，但在8年多的时间里，在中央的高度重视下，信息安全测评认证工作已取得令人欣慰的成绩，并积累了大量宝贵的经验。

我们应该在国家的整体规划和统一指导下，用科学的发展观，正确处理安全与发展的关系，坚持管理和技术并重，坚持以人为本，勇于开拓创新。并借鉴国外信息安全测评认证工作的经验和教训，认真进行总结提高，为开拓我国信息安全测评认证工作的新局面，提高我国的信息安全保障能力，推进国家的信息化建设的全面发展而积极努力。

相信《信息安全测评认证的理论和实践》一书的出版，能为我们更充分地了解信息安全测评认证的历史发展提供一个开阔的窗口，为我国各级政府、部门、行业和企业提供相关的技术依据；为把握我国未来信息安全测评认证事业的方向提供良好的借鉴。

周仲义

中国工程院院士

序四

沈昌祥

信息是社会发展的重要战略资源，信息的安全已成为维护国家安全和社会稳定的一个焦点。随信息化发展而带来的层出不穷的网络安全事件造成的诸多危害，日益突出、备受关注，使网络信息安全成为急待解决、影响国家大局和长远利益、关系国家安全的重大战略问题。如果信息安全问题解决不好，将全方位地危及我国的政治、军事、经济、文化、社会生活的各个方面，使国家处于信息战、信息恐怖和高度经济金融风险的威胁之中。

目前我国信息与网络安全的防护能力处于发展的初级阶段，由于缺乏安全意识，许多应用系统处于不设防状态。经调查表明，目前我国与互联网相连的网络节点有95%都遭到过境内外黑客的攻击或侵入，其中银行、金融机构和政府网站是攻击重点。当前的信息与网络安全研究，处于忙于封堵现有信息系统的安全漏洞阶段。诸多实例表明，提高信息安全的技术能力，有效实现信息安全保障成为当务之急。

对于如何解决信息安全问题，几年来党中央和国家领导人对此一直是高度关注。党的十五届五中全会提出强化信息网络安全保障体系；中办发2003年27号文件中强调，必须坚持积极防御、综合防范的方针，从实际出发，重点保护基础信息网络和关系国计民生的重要信息系统，抓紧建立信息安全等级保护制度，制定相关管理办法和技术指南；在2004年全国信息安全保障工作会议上，黄菊同志又一次强调了实现信息安全等级保护是当务之急。可以看出，以分级分类为核心的等级保护已经成为国家信息安全保障体系中的一项基础性、制度性工作。等级保护是管理与技术并重的体现，对信息安全产品或系统进行检测、评估以及定级，其主要手段是通过专业的测评认证。

综合的来说，对于维护国家的信息安全、推动国家的信息化建设，信息安全认证认可工作具有非常重要的意义。维护信息安全，首要的是要拥有自主知识产权的信息安全产品和系统。但目前我国在信息技术上比较依赖国外，为使我国使用的产品和系统的安全性和可信程度心里有数，信息安全测评认证是头道防线，是预警和应急响应的基础，是国家信息化发展过程中重要的信息保障环节。信息安全的测评认证所依据的标准和程序对于指导产业界的技术研究、产品开发，规范信息化应用中的产品采购和安全保密，支持国家职能部门对信息安全的管理都起到技术规范和指南的作用，有利于我国信息安全民族产业的发展。

我国的信息安全测评认证工作发展已近10年历史，积累了大量宝贵的实践经验，有效推动了国家的信息化安全保障建设，其中也有一些教训值得借鉴，因此，对其进行全面总结是非常重要的。

当前，我国正在积极开展统一认证认可工作，信息安全测评认证工作正面临着大好的机遇，具有明显的政策支持优势。但作为一项比较新的事业，信息安全测评认证毕竟在我国起步较晚，必然会遇到很多管理和技术方面的挑战。欣闻《信息安全测评认证的理论与实践》即将出版，特此作序为贺。希望该书的出版能为我国信息安全测评工作者提供一个客观认识自我的全局视野，成为人们了解信息安全测评的良师益友和指导今后实际工作的有效指南。

沈昌祥

中国工程院院士

序五

蔡吉人

信息是社会发展的重要战略资源，国际上围绕信息获取和控制的斗争愈演愈烈，网络信息安全问题凸显出来，成为国家安全的重要组成部分。

由于我国的信息网络安全起步较晚，安全防护能力处于发展的初级阶段，与发达国家有较大的差距。国内许多信息网络应用系统尚处于不设防状态，存在着很大的风险性和危险性；有些重要的网络应用系统使用的安全设备是从国外直接引进的，难以保证安全利用和有效监控；国内的网络安全全面的研发力量分散，功能单一，基本处于封堵已发现的安全漏洞。要改变这种被动状态，必须加强信息网络安全研究，争取主动，未雨绸缪。

当前，我国信息网络安全面临着难得的发展机遇。中央高度重视信息网络安全问题，各部门提高了对自身网络安全的重视程度，纷纷制订发展规划，国内研究单位和企业已开发出一批满足社会需要的信息网络安全技术和产品，使我国的信息网络安全发展出现了前所未有的好形势。

加强信息安全保障建设，解决信息网络安全问题仅依靠技术是不够的，必须进一步制定相关的政策法规，提高信息网络安全管理水平，加强信息网络安全管理力度，普及信息网络安全教育，以化解信息网络风险。尤其是，要通过测评认证这一重要手段，为政府部门、社会用户、生产厂商和执法机关提供对信息技术“安全”、“可信”要求的技术保障，进一步提高我国信息安全产品的竞争力、服务质量和管理水平，促进经济和社会的发展。

我国的信息安全测评认证工作从诞生到发展已近10年，通过先期阶段的工作，积累了宝贵的实践经验，因此在信息网络飞速发展，电子政务、电子商务建设亟待加强的今天，必须高度重视信息安全测评认证工作，及时针对测评认证理论研究与实践探索做出阶段性的总结。

本书的编者中国信息安全产品测评认证中心，作为国家信息安全测评认证工作的职能部门，长期以来在国家信息安全测评认证建设工作中发挥了重要而积极的作用，他们对我国信息安全测评认证理论与实践的内涵具有深刻而全面的理解与把握。

很高兴看到《信息安全测评认证的理论与实践》一书的出版，该书及为我国各级政府、部门、行业和企业提供了信息安全测评认证科学、权威的理论依据和实践经验，具有很高的理论与实践指导意义，将会对我国信息安全保障建设工作起到积极的、重要的推动作用。

中国工程院院士

《信息安全测评认证理论与实践》编委会

目 录

第2篇 测评认证体系的组织与管理

第3篇 测评认证的规范与指南

第4篇 测评认证的实践与探索