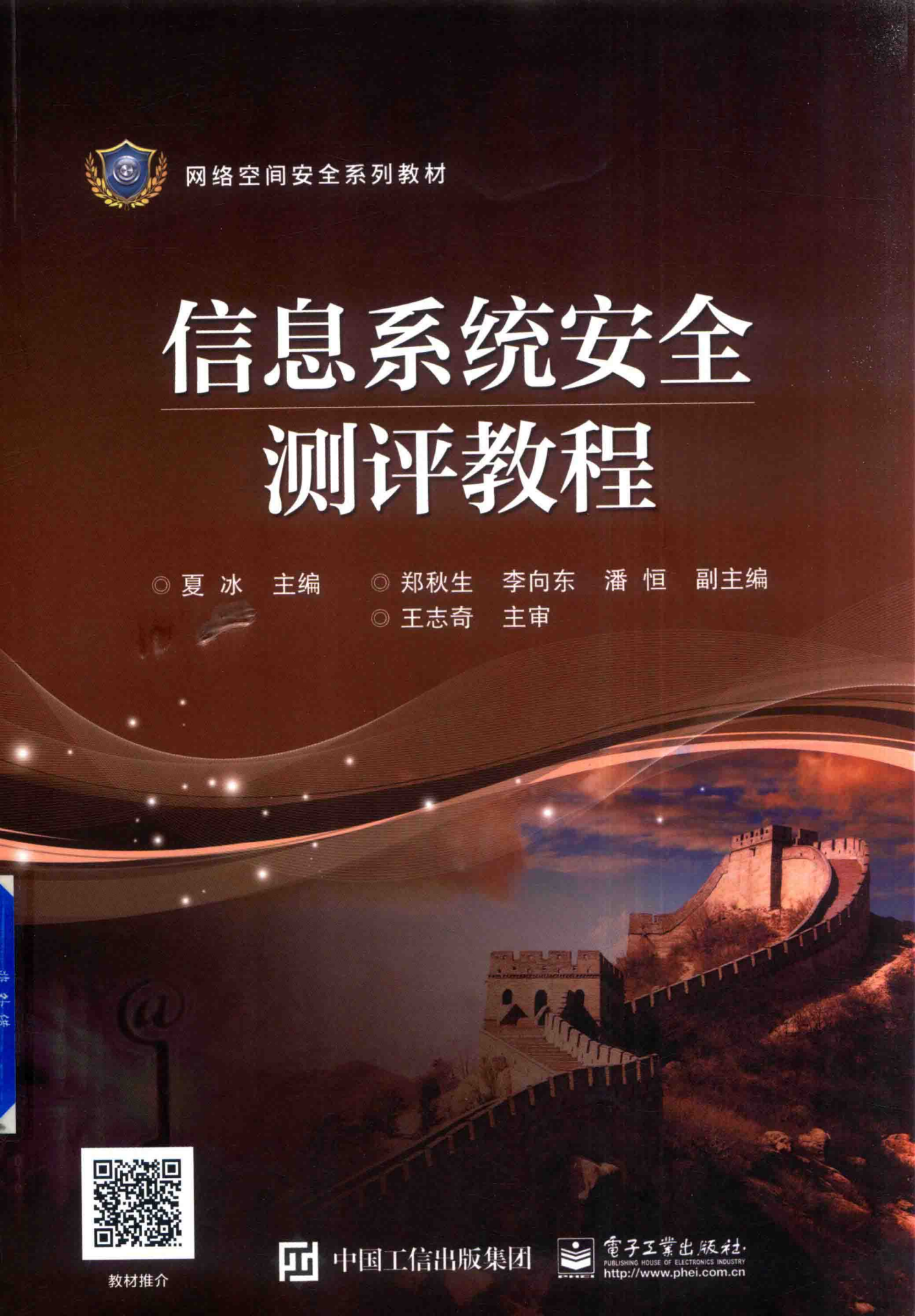
网络空间安全系列教材

信息系统安全测评教程

◎ 夏 冰 主编
◎ 郑秋生 李向东 潘 恒 副主编
◎ 王志奇 主审



教材推介

中国工信出版集团
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

网络空间安全系列教材

信息系统安全测评教程

夏　冰　主编

郑秋生　李向东　潘　恒　副主编

王志奇　主审

電子工業出版社

Publishing House of Electronics Industry

北京 · BEIJING

内 容 简 介

本书从应用流程和技术实现的角度介绍网络和信息系统安全测评工作，围绕信息系统安全要求、测评方法、测评技术、测评实施和测评案例展开。重点介绍了测评标准体系、传统信息系统安全通用要求、云计算安全扩展要求、物联网安全扩展要求、移动互联网安全扩展要求、工业控制系统安全扩展要求、测评对象选择、典型测评工具、安全检查技术、目标识别和分析技术、目标漏洞验证技术、测评结果分析量化和测评报告撰写。本书以网络安全等级保护为核心，给出详细具体、可操作性强、实用性高的等级保护和风险评估测评案例，供读者参考学习。

本书可供信息安全管理人员、信息安全专业人员、信息安全服务人员和等级保护测评工程师使用，也可作为信息安全、网络工程专业教材，网络安全培训教材和参考书。

图书在版编目（CIP）数据

信息系统安全测评教程 / 夏冰主编. —北京：电子工业出版社，2018.2
ISBN 978-7-121-33196-1

Ⅰ. ①信… Ⅱ. ①夏… Ⅲ. ①信息系统－安全技术－高等学校－教材 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字（2017）第 303184 号

策划编辑：章海涛
责任编辑：章海涛　　文字编辑：刘　瑀
印　　刷：三河市华成印务有限公司
装　　订：三河市华成印务有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：787×1092　1/16　　印张：16.75　　字数：407 千字
版　　次：2018 年 2 月第 1 版
印　　次：2018 年 2 月第 1 次印刷
定　　价：48.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：192910558（QQ 群）。

前　言

2017 年 6 月 1 日，《中华人民共和国网络安全法》（本书简称《网络安全法》）正式实施。《网络安全法》是我国网络空间安全的第一部网络安全基本大法，为今后网络安全工作的顺利开展给出了法律约束和指导。《网络安全法》第二十一条确定“国家实行网络安全等级保护制度”。网络运营者应当按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。因此，网络安全等级保护制度从信息安全保障工作的一项基本制度上升为国家法律。

自《网络安全法》出台以后，国家将信息系统安全等级保护变更为网络安全等级保护，后继配套的法律、法规会陆续出台。网络安全等级保护的基本要求主要从技术和管理两个层面展开。根据信息系统重要程度及受损害后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素划分，我国把信息系统安全保护等级分为五级，从低到高分别是第一级、第二级、第三级、第四级、第五级。国家信息系统安全保护等级越高，信息系统的安全保护能力也就越强。

网络安全等级保护的基本要求，是在传统信息系统安全等级保护基本要求的基础上，针对移动互联网、云计算、大数据、物联网和工业控制等新技术、新应用领域，加入了扩展的安全要求。为了便于网络运营者按照网络安全等级要求进行信息系统建设，国家出台 GB/T22239《网络安全等级保护基本要求》，采取“1+X”的保护要求，其中，“1”是指安全通用要求，“X”随着技术的发展而进行扩展。目前主要包括云计算安全扩展要求、移动互联网安全扩展要求、物联网安全扩展要求、工业控制安全扩展要求和大数据安全扩展要求。《网络安全等级保护基本要求》提出了各级信息系统应当具备的安全保护能力，并从技术和管理两方面提出了相应的措施，为信息系统建设单位和运营使用单位在系统安全建设中提供参照。

网络安全测评是衡量等级保护制度落实的有利抓手和标尺。《网络安全法》第三十一条规定“国家关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护”。第三十八条确定“关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估”，因此，如何确定信息系统建设单位和运营使用单位是否按照所定等级开展系统安全合规性建设，对应等级的安全保护保护能力是否满足，信息系统安全防护能力是否有效，这就需要对信息系统进行安全测评。为了便于等级保护测评工作的开展，国家出台 GB/T 28448《信息安全技术网络安全等级保护测评要求》、GB/T 28449《信息安全技术网络安全等级保护测评过程指南》，指导测评机构、测评人员、运行维护技术人员、安全服务人员、技术咨询人员等开展信息安全等级保护测评工作。以网络安全等级保护送审稿中的三级系统测评基本通用要求为例，共涉及 232 项指标，上千个检查要点内容。为了便于信息系统安全相关人员开展工作，本书编者依据多年的技术研究和教学工作经验编写了本书。

本书共 7 章，围绕信息系统安全测评的全过程展开。

第 1 章信息系统安全测评概述，主要讲述信息安全相关概念、信息安全管理和保障、信

息安全测评标准、信息安全等级保护、信息安全测评中的理论问题。

第 2 章信息系统安全通用要求，包括信息系统安全等级保护基本要求和网络安全等级保护安全通用要求。

第 3 章信息系统安全扩展要求，基于网络安全等级保护标准的送审稿，从概述、安全威胁、安全扩展要求角度介绍云计算、物联网、移动互联网和工业控制系统。

第 4 章信息系统安全测评方法，主要介绍测评流程、测评对象、测评工具、测评风险规避和常见测评问题。

第 5 章信息系统安全测评技术，主要从检查技术、目标识别和分析技术、目标漏洞验证技术三个角度，围绕常见的测评对象给出技术检查指导。

第 6 章信息系统安全测评实施与分析，基于等级保护测评，给出测评项结果分析与量化、风险评估结果分析与量化的实施过程。

第 7 章信息系统安全测评案例分析，主要帮助读者形成完整的测评报告，从等级保护测评报告和风险评估报告两个角度给出案例分析。

本书在实施分析和案例分析上，尽管采用的是信息系统安全等级保护标准，但是等级保护测评的核心并没有发生变化，信息系统测评的方法、策略、流程还是一样的。

本书编写由中原工学院信息系统测评技术课程组完成，得到河南省“网络工程专业教学团队”的资助。夏冰主编统稿并负责第 6 章的编写；潘恒负责第 1 章的编写；刘伎昭负责第 2 章的编写；倪亮和刘伎昭共同完成第 3 章；郑秋生、李向东共同完成第 4 章和第 5 章部分编写；冯国朋负责第 5 章的编写。夏冰、河南金鑫信息安全等级技术测评有限公司的蔡学锋，河南工业和信息化职业学院的杜昊凡共同完成第 7 章案例分析及附录的编写。在编写过程中，河南省网络安全保卫总队的王志奇调研员为本书的编写提供建设性的意见，在此表示感谢。

本书由河南省信息安全等级保护工作协调小组办公室组织编写。在编写过程中，得到了河南省公安厅网络安全保护总队的指导，得到了计算机信息系统安全评估河南省工程实验室、郑州市计算机网络安全评估重点实验室的研究支持和资金支持，得到了河南金鑫信息安全等级技术测评有限公司的技术支持。在出版过程中，电子工业出版社章海涛编辑做了大量协调工作，在此表示感谢。

由于作者水平有限，安全测评体系庞大复杂，书中无法包含全部要点且错误在所难免，欢迎读者批评指正。

作　者

目　录

第 1 章　信息系统安全测评概述

近年来，以网络为基础的信息系统建设，正深刻改变着人们的日常生活和工作方式。人们在充分享受便利的同时，其安全威胁也愈演愈烈。2013 年的“棱镜门”事件给全世界政府和人民都敲响了“防信息泄露”的警钟。而云计算、移动互联网及大数据等新技术对信息的获取、处理、存储等方式的改变，也使得企业敏感数据甚至国家机密更容易泄露，信息系统安全问题面临前所未有的严峻挑战。

1.1　信息安全发展历程

信息安全的发展经历了通信安全、计算机安全、网络安全、信息安全保障及网络空间安全的阶段。

早期的通信安全阶段，其主要威胁是对通信内容的窃听，因此主要通过通信技术和密码技术来解决数据的安全传输问题。在该阶段主要强调保证数据的机密性（Confidentiality）、完整性（Integrity）、可用性（Availability）。机密性是指信息不泄露给未授权的访问者、实体和进程，或被其利用。完整性是指信息在存储或传输过程中保持未经授权不能改变的特性，即对抗主动攻击，保持数据一致性，防止数据被非法用户修改和破坏。可用性是指信息可被授权者访问并按需求使用的特性，即保证合法用户对信息和资源的使用不会被不合理地拒绝。

20 世纪七八十年代，信息安全进入了计算机安全阶段。该阶段强调计算机软硬件及其所存储数据的安全，其主要威胁来自于对信息的非法访问等，强调基于访问控制策略的安全操作系统等安全措施。在这一阶段，出现了最早的安全评估标准，即 1983 年美国国防部发布的《可信计算机系统评估准则》（Trusted Computer System Evaluation Criteria，TCSEC）。

随着网络的普遍使用，信息安全进入了第三个阶段：网络安全。该阶段的主要威胁来自于网络入侵破坏等，主要采用防火墙、入侵检测、防病毒、漏洞扫描等工具来保证信息安全。1991 年，欧洲英、法、德、荷兰四个国家参考 TCSEC，制定了欧洲统一的安全评估标准《信息技术安全评估准则》（Information Technology Security Evaluation Criteria，ITSEC）。

1994 年，在美国联合安全委员会提交给美国国防部长和中央情报局长的一份《重新定义安全》的报告中，明确建议美国“应该使用风险管理作为安全决策的基础”。1996 年，美国国防部第 5-3600.1 号令第一次提出了信息安全保障的概念，由此进入了以风险控制、风险管理为核心的信息安全保障阶段。在这一阶段，信息安全从原有的强调技术措施，上升为技术和管理并重，认为安全不必要也不可能做到完美无缺、面面俱到，应在考虑安全成本的条件下，利用风险分析，使系统安全处于可控范围内。在测评标准方面，国际标准化组织（ISO）于 1996 年发布了最初的国际通用评估准则《信息技术安全性评估通用准则》（Common Criteria，CC）。

2008 年后，随着移动互联网的应用，虚拟网络世界已经和现实世界密不可分，于是出现了“网络空间”（Cyberspace）一词。同时，作为国家安全极为重要的一部分，工控安全也被

重视起来，信息安全发展到了网络空间安全阶段。

在信息安全发展的五个阶段中，安全测评的最早提出是以《可信计算机系统评估准则》（TCSEC）为标志的。但是，最初的 TCSEC 评估主要强调操作系统安全。在网络安全阶段，由 TCSEC 演变而来的 ITSEC、CC 等标准，主要是针对信息系统安全进行评估的。在第四阶段，即信息安全保障阶段，强调信息系统全生命周期的风险管理，其管理基础就是对信息系统从规划、设计、实施、运行维护、废弃等各阶段的风险评估。在该阶段除了上述的测评标准外，出现了信息安全管理标准，最早是英国的《信息安全管理实施细则》（BS 7799），后来发展为 ISO 27000 信息安全管理体系系列标准。

从信息安全的发展和信息安全测评标准的演变可见，信息系统测评作为风险评估的有效方法，是从信息安全第二个阶段开始出现并发展起来的，如表 1-1 所示。

表 1-1 信息安全发展历程

阶段	时间	主要特征	信息安全测评标准发展
通信保密	20 世纪 40～70 年代	解决数据的安全传输，强调信息的机密性、完整性、可用性	无
计算机安全	20 世纪 70～80 年代	强调基于访问控制策略的安全操作系统安全	《可信计算机系统评估准则》TCSEC 出现
网络安全	20 世纪 90 年代	主要威胁来自于网络入侵破坏等，主要采用防火墙、入侵检测、防病毒、漏洞扫描等工具来保证信息安全	《信息技术安全评估准则》ITSEC
信息安全保障	20 世纪 90 年代末	强调风险管理，技术和管理并重	《可信计算机系统评估准则》（CC） 《信息安全管理实施细则》BS 7799GB/T 17859 《计算机信息系统安全防护等级划分准则》
网络空间安全	21 世纪	涉及计算机、网络、云环境、工控系统等多层次、多维度安全问题，具有整体性；安全问题具有动态性、高复杂性，且具有共通性、国际化的趋势	我国 GB/T 18336—2001《信息技术安全性评估准则》及等级保护系列标准

1.2 相关概念

信息安全测评是信息安全管理的重要组成部分，更是保证系统“可信可靠”构建信息安全保障体系中的一个重要环节。信息安全管理是信息安全保障的要素之一。

作为信息系统安全管理、信息系统安全保障的重要组成，要理清信息系统安全测评的基本概念及其作用，必须将其放在信息安全管理、信息安全保障体系这样大的概念背景下来谈。因此，本节主要对信息系统安全、信息系统安全管理及信息系统安全保障等相关概念和理论进行简要介绍。

1.2.1 信息系统安全

1. 信息系统

信息是指有价值的数据。在信息产生、传输、存储、使用、销毁的整个生命周期里，需要各种载体。例如，常见的计算机、网络、人均是信息的载体。这些信息载体又处于相应实际的物理环境中。通俗来讲，信息系统就是信息及其所处环境。

信息系统不仅仅描述的是计算机软硬件，网络和通信设备，更是人和管理制度等的综合。因此，从信息系统组成的角度，将信息系统（Information System）定义为由计算机硬件、网

络和通信设备、计算机软件、信息资源、信息用户和规章制度组成的以处理信息流为目的的人机一体化系统；从过程的角度，将信息系统定义为输入输出的复杂系统，其复杂性体现在系统元素之间的耦合性（元素之间的关联强度）复杂；此外，系统一般是有输入和输出的，输入的变化会引起输出的变化，通常输入和输出之间是非线性关系，从安全的角度看，信息系统的输入和输出是主要风险来源。

2. 信息安全

在谈信息系统安全之前，首先明确下信息安全的定义。迄今为止，对于信息安全的概念尚无统一定义。但谈到信息的安全或信息系统的安全，普遍认同的是 1.1 节所述关于信息的三个安全属性，即机密性、完整性和可用性。随着技术的发展，从这三个基本安全属性中又扩展出可控性、抗抵赖性等其他性质。

3. 信息系统安全

信息系统安全有狭义和广义两种定义。狭义的信息系统安全是指信息及其所在系统能够保证信息的机密性、完整性、可用性、可控性、不可否认性等基本性质。广义的信息系统安全是从技术和管理两个方面能够保证信息及其所处环境的安全。具体技术方面包括物理安全、主机安全、网络安全、应用安全、数据安全及其备份恢复等；管理方面包括人员、制度、组织等方面的安全管理要求。可见，广义的信息系统安全不是单纯的技术问题，而是管理、技术、法律等问题相结合的产物。

1.2.2 信息系统安全管理

在信息安全发展之初，大家普遍认为信息安全是一个技术问题，当时的信息安全主要依赖各种密码技术的保护和防御。但是，随着各种威胁的不断增加，各国逐渐认识到，信息安全不是一个纯粹靠技术能够解决的问题，更多的安全事件是由于管理不善、操作失误等原因造成的。要实现信息安全目标，必须依靠强有力的信息安全管理。信息安全是一个动态的过程，需要人员、技术、操作三者紧密结合。

1. 信息安全管理概念

管理，是指为了达到特定目标，管理主体对被管对象进行的计划、组织、指挥、协调和控制等一系列活动。

信息安全管理（Information Security Management，ISM），是指为实现信息安全目标，管理主体对被管对象进行的计划、组织、指挥、协调和控制等一系列活动。

信息系统安全管理是指为了实现信息系统的安全目标，对信息系统的资产进行的计划、组织、指挥、协调和控制等一系列活动。

信息系统安全管理的被管对象是系统的资产，包括人员、软件、硬件、信息等，同时包括信息安全目标、信息系统安全组织架构和信息系统安全策略规则等。

2. 信息系统安全管理基本方法

信息安全管理基本方法有风险管理和过程方法两种。这两种方法都来自于管理学中的质量管理，而信息系统安全管理也主要依赖于这两种方法。

信息系统安全管理的目的是预防、阻止和减少信息系统中安全事件的产生。而要达到这一目标就是要将系统的安全风险降低到可控范围内。信息系统安全水平的高低遵循“木桶原理”。即：一只木桶的盛水量，取决于桶壁上最短的木板。因此，要控制安全风险，首先要了解信息系统中的最短板，也就是要进行风险要素识别和风险分析，了解系统中的脆弱点在哪里。

在风险管理中，风险评估是信息安全管理的基础，风险处理是信息系统安全管理的核心，控制措施是管理风险的具体手段。风险评估主要对系统的信息资产进行鉴定和估价，然后对系统资产面对的各种威胁和脆弱性进行评估，同时对已存在的或规划的安全控制措施进行界定。而风险处理是对风险评估活动识别出的风险进行决策，采取适当的控制措施处理不能接受的风险，将风险控制在可承受的范围。风险处理的最佳集合就是信息系统安全管理的控制措施集合。控制措施可以分为技术性措施、管理性措施、物理性措施和法律性措施等。

此外，过程方法也是信息系统安全管理的重要方法之一。其目的是通过识别信息系统中的关键和重点安全过程，并加以实施和管理，获得持续改进的动态循环，使得系统的信息安全水平得到显著提高。

ISO/IEC 27000:2009 将“过程”定义为将输入转化为输出的一组彼此相关的资源和活动。ISO/IEC 27001:2005 将“过程方法”定义为使组织的业务有效运作，需要识别和管理业务相关的活动。

在过程方法中，戴明环是管理学中的一个通用模型，也叫 PDCA 循环或质量环。PDCA 循环包括 Plan（计划）、Do（执行）、Check（检查）和 Action（行动）四个顺序步骤。由于 PDCA 循环不仅可以在质量管理体系中运用，也适用于一切循序渐进的管理工作。因此，它也是信息安全管理中基于过程方法常见的一种持续改进模型。

PDCA 模型有三个重要特点。

① P-D-C-A 四个步骤是按顺序进行的，且四个过程不是运行一次就结束，而是周而复始的进行。一个循环结束，解决一些问题，未解决的问题进入下一个循环，这样阶梯式上升。

② PDCA 模型中的 P-D-C-A 四个阶段，每个阶段又都可以按照 PDCA 循环进行，也就是说可以大环套小环，一层一层地解决问题。

③ 每次执行完 PDCA 循环，都要进行总结，提出新目标，再进行第二次 PDCA 循环。

信息安全管理体系（Information Security Management System，ISMS）就是基于过程方法的 PDCA 循环体。如图 1-1 所示。

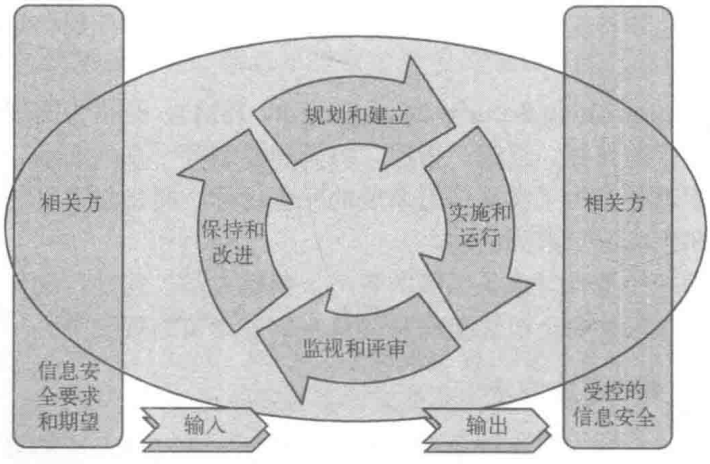


图 1-1　基于 PDCA 的信息安全管理体系

PDCA 循环是全面质量管理所应遵循的科学程序。全面质量管理活动的全部过程，就是质量计划的制订和组织实现的过程，这个过程就是按照 PDCA 循环，不停顿地周而复始地运转的。

3. 信息系统安全管理实施

上述信息系统安全管理听起来概念性比较强，但目前我国实际的实施主要有两种方法。一个是图 1-1 所示的建设基于 PDCA 和风险管理的信息安全管理体系；第二个是实施信息安全等级保护。

（1）信息安全管理体系

信息安全管理体系（ISMS）是一种常见的全面、系统的信息安全管理方法。它是一种基于风险管理和过程方法的管理体系，是由 ISO 27001 定义的，其前身是英国的 BS 7799-2 标准。ISMS 包括周期性的风险评估、内部审核、有效性测量、管理评审四个必要活动，以确保 ISMS 进入良性循环，持续自我改进。

目前，ISO 27000 标准族日益完善，已经开发和计划开发的标准有 60 余项，包括 ISO 27000《信息安全管理体系概述和术语》、ISO 27001《信息安全管理体系要求》、ISO 27002《信息安全控制措施实用规则》、ISO 27003《信息安全管理体系实施指南》等。

（2）信息安全等级保护

信息安全等级保护是对信息和信息载体按照重要性等级分级别进行全面、系统地管理的实施方法。根据《计算机信息系统安全保护等级划分规则》，计算机系统安全保护能力分为五个等级，分别是：第一级，用户自主保护级；第二级，系统审计保护级；第三级，安全标记保护级；第四级，结构化保护级；第五级，访问验证保护级。二级以上需要到公安机关备案，三级以上每年需要进行信息安全测评。信息安全等级保护工作包括定级、备案、安全建设和整改、信息安全等级测评、信息安全检查五个阶段。通过这五个阶段确保实现信息安全管理。

1.2.3 信息系统安全保障

1990 年，美国最早提出信息系统安全保障的概念，将信息安全的观念提升到“以预防、检测和反应能力的提高来确保信息系统的可用性、完整性、可鉴别性和不可否认性的全面保障阶段。”在此之前的信息安全重点是防御和保护，而信息安全保障强调的则是“防御保护、检测和响应”的综合。信息安全保障特别强调“检测和响应”，而检测响应的核心是风险管理，其基础是风险评估。

正如前文所提到的，在信息安全保障这一阶段，普遍的认同是，安全不必是完美无缺、面面俱到的，安全问题是一个成本问题，最佳的信息安全保障实际就是最佳的风险管理方式，信息安全测评是风险管理的有效手段。

我国信息安全保障工作起步较晚，先后经历了启动、逐步开展和深化落实阶段。

2001～2002 年，是我国信息安全保障工作的启动阶段。其标志是 2001 年国家信息化领导小组重组，网络与信息安全协调小组的成立。这一阶段的特点是，各种信息安全事件频繁发生，我国认识到信息安全不是一个局部的、技术性问题，信息安全是跨领域、跨部门、跨行业的问题，是一个关于国计民生、社会稳定和国家安全的问题。

2003～2005 年，是我国信息安全保障工作的逐步开展和积极推进阶段。其标志是 2003 年 7 月发布的《关于加强信息安全保障工作的意见》（中办发 27 号文件）。该文件明确了“积极防御、综合防范”的国家信息安全保障工作方针，提出了加强信息安全保障工作的总体要求和主要原则。在此阶段，各省（区、市）和有关部门陆续建立了网络与信息安全协调小组。信息安全等级保护、信息安全风险评估、网络信任体系建设、信息安全产品认证认可、信息安全标准制定、信息安全监控和信息安全应急处理等工作均取得了积极推进和明显进步。

2006 年至今，是我国信息系统安全保障深化落实阶段。围绕中办发 27 号文件，信息安全法律法规、标准化和人才培养工作取得新成果；信息安全等级保护和风险评估取得新进展。

1. 信息安全保障技术框架

目前，较成熟的信息安全保障框架主要是由美国国家安全局（NSA）制定的信息安全保障技术框架（Information Assurance Technical Framework，IATF），该框架主要为保护美国政府和工业界的信息与信息技术设施提供技术指南。

该框架的主要思想是深度防御，该框架强调人、技术、操作这三个核心要素，提出了信息保障依赖于人、技术和操作来共同实现组织职能和业务运作的思想，从多种不同的角度对信息系统进行防护。同时，IATF 关注四个信息安全保障领域，即本地计算环境、区域边界、网络和基础设施及支撑性基础设施。此基础上，对信息系统就可以做到多层防护，实现组织的任务和业务运作，如图 1-2 所示。

在 IATF 模型中，人是信息保障体系的第一位要素，需要对其进行意识培训、组织管理、技术管理、操作管理等；其次，技术是实现信息保障的重要手段，包括由防护、检测、响应、恢复等部分组成的一个动态技术体系；最后，操作也叫运行，构成安全保障的主动防御体系，是将各方面技术紧密结合在一起的主动的过程，主要包括风险评估、安全监控、安全审计、跟踪告警、入侵检测、响应恢复等。如图 1-3 所示。

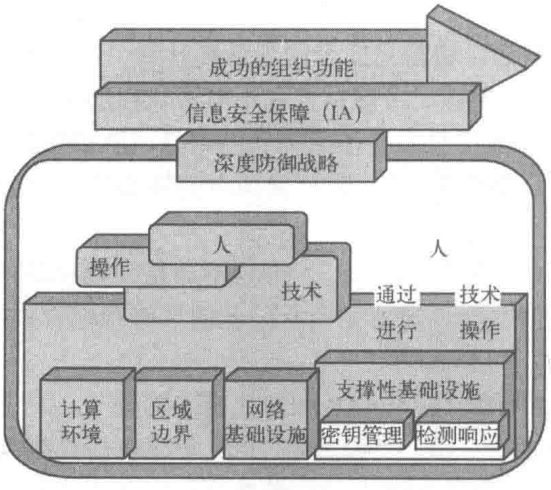


图 1-2　深度防御的信息安全保障技术框架

人员	技术	操作
培训	深度防御技术框架域	分析
意识	安全标准	监视
物理安全	获得IA/TA	入侵检测
人员安全	风险分析	警告
系统安全管理	证书与认证	恢复

图 1-3　IATF 三要素

IATF 定义的四个安全区域，分别是：

① 对计算机环境的保护：使用信息保障技术确保数据在进入、离开或驻留客户机和服

务器时具有保密性、完整性和可用性。

② 对区域边界的保护：这里的区域是指由单一授权通过专用或物理安全措施所控制的环境，包括物理环境和逻辑环境。而区域边界则是指区域的网络设备与其他网络设备的接入点。其主要保护方法是通过部署病毒、恶意代码检测、防火墙、入侵检测等设备对进出某区域（物理区域或逻辑区域）的数据流进行有效的控制与监视。

③ 对网络基础设施的保护：其目的是防止数据非法泄露，防止受到拒绝服务的攻击，以及防止受到保护的信息在发送过程中的时延、误传或未发送。

④ 支撑性基础设施建设：是为安全保障服务提供一套相互关联的活动与基础设施，主要包括密钥管理和检测响应两部分。

深度防御战略思想采用层次化保护策略，通过在主要位置实现适当的保护级别，同时为了降低保障成本，允许在不降低系统整体安全性的前提下，在适当的时候用低安全级的保障解决方案。

2. 信息系统安全保障模型

基于我国的实际信息安全保障需求，GB/T 20274.1—2006《信息安全技术信息系统安全保障评估框架第一部分：简介和一般模型》将信息系统安全保障定义为：在信息系统的整个生命周期中，从技术、管理、工程和人员等方面提出安全保障要求，确保信息系统的保密性、完整性和可用性，降低安全风险到可接受的程度，从而保障系统实现组织机构的使命。根据该定义，信息系统安全保障模型如图 1-4 所示。

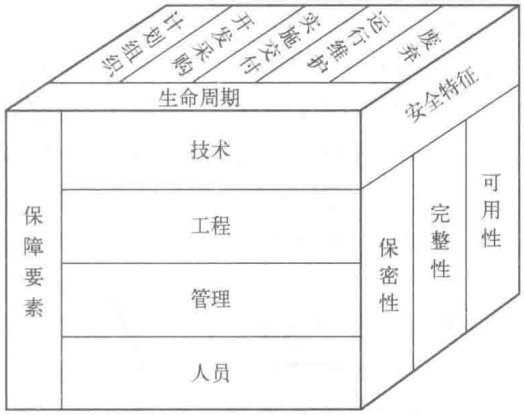


图 1-4 信息系统安全保障模型

信息系统安全保障模型是要保障信息系统在技术组织、开发采购、实施交付、运行维护到废弃整个生命周期中信息的保密性、完整性和可用性特征，从而实现和贯彻组织机构策略，并将风险降低到可接受程度。其保障要素包括技术、工程、管理和人员四部分。技术包括密码、访问控制、网络安全、漏洞及恶意代码防护等常见的安全技术；工程包括信息系统安全工程、安全工程能力成熟度模型等信息安全工程实现方法和模型；管理包括安全管理体系、风险管理、应急响应与灾难恢复等；人员包括对所有员工、信息系统岗位、安全专业人员的日常培训、管理等。

该模型提出保密性、完整性、可用性三个安全特征是信息系统安全要达到的基本要求；信息系统安全保障的生命周期是信息系统安全保障持续发展的动态特征；信息系统所处的运行环境、信息系统的生命周期和信息系统安全保障等概念的技术、工程、管理和人员等四个要素是综合保障，与 IATF 框架中的人、技术、操作有异曲同工之处。此外，该模型将风险和策略作为信息系统安全保障的基础策略，在生命周期、安全特征和保障要素中始终贯穿风险管理和策略部署。

1.3 信息系统安全测评作用

迄今为止，尚无对信息系统安全测评的统一定义。通俗地讲，信息系统安全测评，是一种合规性检测和评估活动，主要针对信息系统中可能存在的技术、管理等安全隐患，逐项对