信息系统安全保障评估

编著　吴世忠　江常青　林家骏

華東理工大學出版社
EAST CHINA UNIVERSITY OF SCIENCE AND TECHNOLOGY PRESS

信息系统安全保障评估

编著　吴世忠　江常青　林家骏

華東理工大學出版社
EAST CHINA UNIVERSITY OF SCIENCE AND TECHNOLOGY PRESS
·上海·

图书在版编目(CIP)数据

信息系统安全保障评估/吴世忠，江常青，林家骏编著. —上海：
华东理工大学出版社，2014.4
ISBN 978-7-5628-3189-1

Ⅰ. ①信… Ⅱ. ①吴… ②江… ③林… Ⅲ. ①信息系统—安全技术 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字(2011)第 255379 号

内容提要

本书主要介绍了信息安全模型、信息安全评估方法与标准；提供了可支持GB/T 20274的信息安全保障能力评估工具及其测评实例。

本书可供有关研究人员、工程人员阅读，也可作为研究生与大学高年级学生的教材与参考用书。

信息系统安全保障评估

编　　著 / 吴世忠　江常青　林家骏
责任编辑 / 李国平
责任校对 / 张　波
封面设计 / 裘幼华
出版发行 / 华东理工大学出版社有限公司
地　址：上海市梅陇路 130 号，200237
电　话：(021)64250306(营销部)
(021)64252712(编辑室)
传　真：(021)64252707
网　址：press.ecust.edu.cn
印　　刷 / 上海展强印刷有限公司
开　　本 / 710 mm×1000 mm　1/16
印　　张 / 12
字　　数 / 234 千字
版　　次 / 2014 年 4 月第 1 版
印　　次 / 2014 年 4 月第 1 次
书　　号 / ISBN 978-7-5628-3189-1
定　　价 / 48.00 元

联系我们：电子邮箱 press@ecust.edu.cn
官方微博 e.weibo.com/ecustpress
淘宝官网 http://shop61951206.taobao.com

序　言

如果将计算机、服务器、路由器及交换设备等信息技术产品比喻成网络空间的细胞，那么，由它们组合而成的信息系统无疑是网络王国的基本构成单元，犹如现实社会中的一家、一村、一镇、一城，是国家管理和社会稳定的重要环节。信息系统是信息化建设的主要内容，同样是信息安全工作的重点所在。美国将能源、交通、电力、食品、供水等事关国计民生的信息系统列为“国家关键基础设施”加以重点管理和保护，西方其他国家纷纷效法，先后制定专门的战略规划和保护计划，强化信息系统的安全保障。我国的党政军各部门和国有企事业单位的信息系统同样也是国家信息化建设的主流，在我国的信息安全保障体系建设工作中，也将民航、铁道、电力、海关、税务、银行、证券和保险等行业的网络系统，列为“重要信息系统”加以重点保护。可以说，信息系统的安全，是信息安全工作的关键所在和重中之重，对信息系统安全相关问题的研究和探索，自然成为信息安全理论和实践中的热点和重点。

然而，信息系统涉及硬件、软件、数据和人员等多种资源和要素，本身具有很高的集成性和复杂性。信息安全问题更是浓缩了太多的复杂性和不确定性。信息系统安全问题的复杂性和挑战性可想而知。为了科学、客观地规范和描述信息安全问题，国际社会一直在做不懈的努力，早在 1984 年，领先世界信息技术的美国就研究发布了著名的《可信计算机系统评估准则(TCSEC)》，这部俗称“橘皮书”的标准，对全球的信息安全工作产生了划时代的影响。英国、德国、法国、荷兰四国很快启动欧洲的相关标准工作议程，经过五年多的努力，于 1991 年正式推出欧洲统一的《信息技术安全评估准则(ITSEC)》。为了适应 INTERNET 发展普及带来的全球互联新形势，上述四国与美国、加拿大一道，又经五年多的时间和探索，共同推出了信息技术安全性评估的《通用准则(CC)》，成为西方发达国家评估信息安全的统一要求和工作规范。伴随着互联网飞速发展的势头，该标准经过三年的国际协调和技术评估后，于 1999 年正式成为国际标准 ISO/IEC15408，为信息安全界提供了全球通用的描述方法和评估框架。《通用准则(CC)》的面世，对信息安全工作而言，具有里程碑式的意义。由于该标准在结构上具有很好的开放性，其“安全功能要求”和“安全保证要求”可以根据具体的评

估对象和环境条件做进一步的细化和扩展。因而，在它的指导下，很快形成了一系列针对具体产品实现“保护轮廓(PP)”和“安全目标(ST)”，极大地促进了对信息技术产品的安全检测与评估工作。

中国信息安全测评中心作为我国为适应加入 WTO 的新形势，有效应对全球化、信息化带来的信息安全挑战而专门设立的专业化技术测试与评估机构，成立伊始就关注并跟踪国际上相关安全标准的动向与发展。《通用准则(CC)》一经国际标准化组织(ISO)批准，我们即启动相应的内容消化、文字翻译和技术验证工作，并于 2001 年正式等同采用为我国的国家标准 GB/T 18336—2001，直接应用于蓬勃兴起的信息安全行业，较好地满足了信息安全产品测评的现实需要。当然，产品安全只是信息安全的基础，由类别各异、品种繁多的产品构成的信息系统所面临的安全风险要比一种单一的产品复杂得多。如何将《通用准则(CC)》的指导思想和概念体系扩展到网络系统，很快成为一个新的现实问题。在“全国信息安全技术标准化委员会”的规划安排和指导下，测评中心牵头承担了研究制定我国《信息系统安全保障评估框架》标准的任务，我们在跟踪分析国际上相关标准研究动向的同时，以《通用准则(CC)》为基础，结合信息系统相关的安全标准和工作实践，研究归纳了信息系统安全保障模型的描述方法，从安全技术、安全管理和安全工程等方面，提炼确定了信息系统的通用安全保障要求，并据此建立了信息系统安全保障评估框架，该标准文本经信息安全技术标准化委员会评审后，分别于 2006、2008 年获得“国家标准化委员会”正式批准，成为我国的国家标准 GB/T 20274.1—2006，GB/T20274.2、3、4—2008。此后，根据我国信息系统安全建设和评估工作的实际，我们依据此标准，先后制定了《信息系统保护轮廓和安全目标产生指南》和《信息系统安全保障通用评估方法》，形成了针对信息系统安全评估工作的标准系列。从 2008 年至今，该系列标准在我国重要信息系统的安全性评估中得到实际运用和实践推广，特别是在对党政军关键信息网络的技术安全检查和国家重点行业、国有大型企事业单位的重要信息系统安全风险评估中发挥了应有的标准指导和工作支撑作用，本书即是该系列标准近五年来相关实践和理论工作的初步结论。

信息系统的安全问题本来就十分复杂，各种信息系统的互联互通和互操作更是将信息安全风险扩散、放大在网络空间，我们的实践与探索时间不长，理论归纳也远未完善，任何一项技术标准，都需要经过实践和时间的检验和考验，信息安全标准尤其如此，套用“实践是检验真理的唯一标准”这一至理名言，也可以说：实践是检验标准的唯一真理。我们将此项工作做一个阶段性的小结，目的就在于为该领域更深更广的实践探索和理论研究，提供实例和参考。

无论是技术标准的研究制定工作，还是信息系统的安全评估实践，均得到了国家信息安全各个管理部门和社会各界众多领导、专家和学者的大力支持和测评中心多个部门同事们的积极配合，所以在本书付梓之际，谨向支持和关心测评

中心技术安全标准制定和信息安全风险评估工作的部门、专家和同行们表示由衷的感谢。特别要向全国信息安全技术标准化委员会、工业和信息化部信息安全协调司、中国电子技术标准化研究院及信息安全领域的测评、认证机构表示诚挚的谢意。向参编本书的程华、王雨、袁文浩博士表示感谢。同时，要向华东理工大学出版社表达我们的敬意，他们对这部书稿的修改和编辑付出了极大的热情和耐心。

吴世忠

2013 年秋于北京

目　录

0 导论

随着信息技术的发展和广泛应用，人类对信息技术产品和系统的依赖越来越大，现代社会正常和可靠的运行越来越依赖于高度自动化的信息系统。从交通运输、电力供应、金融证券服务到衣食住行，信息系统正逐渐成为支撑社会运行的数字化神经中枢，无所不在的信息网络构成了国家关键信息基础设施，网络化社会已成为客观的现实。与此同时，这些重要的信息系统安全问题也日益突出。系统故障和中断，信息和数据被窃取，网络系统被攻破等事故常有发生，不仅造成经济上损失，还影响社会的稳定和秩序，甚至损害国家的安全与利益。

作为信息系统的运营者、使用者、主管部门等相关方都应该知道这些关键系统的安全，了解由大量、多样化的部件构成的复杂信息系统的安全程度。它们的安全风险在哪儿？风险有多大？可以信赖否？是否有足够的安全保障对抗将面临的风险？因而，如何测量和评价信息系统的安全性——信息系统安全评估，成为迫切又具有挑战性的问题。

信息系统安全评估类似其他测量(Measurement)要解决的问题一样，它包括三个方面的问题，第一，要明确评估的对象。在物理世界中，对象是物质的长度、质量和时间等。在信息系统安全中，对象可以是技术、产品、过程或系统及其特性。第二，要解决度量尺度的问题。在物理世界中，可以用米、千克、秒来度量长度、质量和时间。在信息系统安全中，度量安全的尺度是什么？基于安全漏洞的数量，漏洞的严重程度或者系统抗攻击的能力来度量，还是信息和系统的安全性质来度量，比如保密性、完整性、可用性等，或者从经济角度以信息资产可能造成的损失来度量。此外还有这些尺度是否实际可行，具有可操作性？特别是信息系统安全，它不仅要对其安全技术或机制进行测量，还必须对信息系统的使用及管理进行评估。例如，是否恰当正确地使用安全技术，以及有效使用安全措施的程度。第三，要解决如何检测和评估的问题。在信息安全中的检测，主要有检查、功能测试、渗透测试、审核、核查等手段来获得检测数据，而对于这些通过直接或间接检测获取的数据，结果是否可以量化，如何通过有效的评估方法达到对信息系统安全的整体安全评价，要研究和解决这些问题涉及面非常广，我们先简要回顾一下过去在这些方面的进展情况。

1. 信息安全评估对象及建模的问题

随着信息科学的理论和技术发展及其应用，对信息安全内涵与外延也有不同发展，信息安全评估的对象在广度和深度上也不断发生变化。从人类使用“消

息”(Message)进行通信开始,就存在信息保密问题。现代电子通信系统、计算机系统和信息系统等信息处理设施和技术的产生、演进和发展,人们对其安全的认识也逐步从通信安全(COMSEC:Communication Security)、计算机安全(COMPUSEC:Computer Security)、信息技术安全(ITSEC:Information Technology Security)发展到信息安全保障(IA:Information Assurance)。

20世纪以来,电话、电报、电传等远距离现代电子通信技术的发展应用,通信信息在信道上被拦截窃听、破译使得通信保密问题成为首先需要解决的问题。要保住秘密,简单地说有三种方法,一是看到了也看不懂,二是不该看的看不到;三是将秘密分拆、分散到不同地方,或隐藏在貌似正常的信息中。通信保密理论及密码学是用第一种方法来解决通信保密问题的核心技术。香农在1949年发表的《保密系统的通信理论》理论论证了信息在通信过程中的保密问题。相关的密码技术主要有对称密码与非对称密码(或公钥密码)。对称密码在加解密时使用相同的密钥,非对称密码使用公钥/私钥对分别进行加密与解密,密码技术还涉及密钥的分配与管理。基于计算机访问控制和信息流安全策略模型是第二种方法,通过自主访问控制,强制访问控制,基于角色的访问控制等技术对不同权限的主体和不同密级的信息进行访问控制。信息隐藏和数字水印技术是信息保密的第三种方法。

计算机与通信网络的技术融合发展进入了信息技术(IT)时代,安全问题也从仅关注信息和信息流发展到信息技术安全(IT Security),信息安全从关注保密性为主扩展到包括完整性和可用性在内的三性。经过加拿大、法国、德国、荷兰、英国和美国六个国家共同努力,在信息技术安全领域,产生了国际上公认评估信息技术安全标准即著名的“通用准则”(Common Criteria 简称为 CC),相应的国际标准 ISO/IEC 15408。我国将其作为国家标准 GB/T - 18336。CC 将安全功能要求与安全保证要求分开,“功能要求”是对产品希望提供的安全功能或特征的描述,“保证要求”是功能要求能够得到满足的程度。它提出了一种科学规范描述和表达信息技术产品或系统安全要求的方式。它将安全功能分为 11 大类,66 个子类,135 个组件。11 大类包括:FAU -安全审计、FCO -通信、FCS -密码支持、FDP -用户数据保护、FIA -标识与鉴别、FMT -安全管理、FPR -隐私、FPT -安全功能保护、FRU -资源利用、FTA - TOE 访问和 FTP -可信路径/通道。安全保证要求包括配置管理、分发和操作、开发过程、指导文件、生命期的技术支持、测试和脆弱性评估等 7 类。通过这些安全功能和保证要求产生用于描述某一种信息产品或技术的安全要求(简称保护轮廓 PP, Protection Profiles)和某一特定的产品或技术的安全要求(简称安全目标 ST, Security Target),这样可以更加科学规范并灵活地表达和描述信息技术或信息技术系统的安全性。但 CC 比较适合于信息技术安全产品或产品构成系统的评估,缺乏对管理和工程过程的安全要求。

自 20 世纪 90 年代后期以来，信息技术的广泛应用和信息社会化进程加快，信息安全内涵发生了新的变化，信息安全不仅是技术安全本身，更重要的是信息技术使用安全和信息系统安全管理方面的问题，这些问题包括从设计、实现到管理和使用的安全。在信息系统安全管理方面，在借鉴了 ISO 9000、PDCA 等通用管理思想基础上，诞生了许多信息安全管理的实践指南，如 ISO 17799、ISO 27000 系列、GASSP、ISO 13335 等。在信息系统安全工程方面，也产生了 SSE-CMM、ISSE 等，它们从安全工程过程、安全过程管理的角度不断增强和扩展了对信息系统安全的理解，提出对安全工程过程和管理的要求。在信息安全攻防方面，有基于防护-检测-响应(PDR)为基础的，与时间相关的 P2DR 是安全动态防护过程的概念模型。

尽管有众多的安全体系和描述信息安全的标准产生，但它们各自适用于信息系统安全的不同方面，从不同的角度来理解和解决不同的安全问题，各有所长，又各有所短。其中 GB/T 18336 主要适用于产品和产品系统，ISO/IEC 17799，ISO 13335 主要提供安全管理的最佳实践，缺少管理能力的评价，SSE-CMM，ISSE 主要用于提供信息系统安全设计和工程建设的持续改进能力。

信息系统是指用于收集、处理、存储、传输，显示、传播和清除信息的所有设施、组织、人员等部件的组合。从内涵来看信息系统比信息技术系统要广，它包括技术系统加上运行环境，这里的环境包括组织、管理及人。因而，信息系统安全保障不仅是技术安全问题，还是管理、运行及使用安全的问题。上面提到的各种已有安全体系和标准要关注于某一特定领域或方面，未能全面地解决信息系统安全保障的问题。1996 年，美国国防部在 DOD5 - 3600.1 指令中首次给出了“信息安全保障(IA)”的概念：为了确保信息及信息系统的可用性、完整性，身份鉴别性和不可否认性而采取的保护和保卫信息及信息系统的信息操作，包括以保护、检测和反应能力，为信息系统的恢复提供保障。在本书中，我们将在探讨信息系统安全保障的内涵与外延。通过对时间、空间、目标、能力等 4 个维度来研究信息系统安全保障。

2. 信息安全评估尺度问题

要对信息安全实施有效评估，需要在对信息安全进行建模和在描述的基础上，设计对信息安全进行度量的尺度。

信息安全不像物理领域，有长度、质量、热量等客观的度量尺度可以使用。从经典物理可以看出，针对不同的物理量有不同的度量尺度，在信息安全领域也应该针对不同的安全量设计不同的度量尺度。在信息安全领域，对于度量尺度的设计，度量尺度比较复杂，从不同角度进行度量有不同的度量尺度。对于安全管理通常采用安全审计的方式进行安全度量，符合性可以作为度量的尺度；对于安全技术通常采用渗透测试的方法进行安全度量，漏洞数量可以作为度量的尺度，而对于安全工程通常采用能力成熟度的方式进行安全度量，能力级别可以作

为度量的尺度，对于安全人员则通过能力评估的方式进行安全度量，能力等级可以作为度量的尺度。还有其他类似风险等级、业务影响、资产价值等都属于信息安全度量的度量尺度，根据度量对象的不同都可以归为上述四类参量。

度量尺度不仅仅是根据度量的对象来选取的，不同的评估方法其所采用的度量尺度也是会有差异的。在信息系统安全评估方面，尽管目前并没有形成形式化的评估理论，但存在着多种多样的信息系统安全评估的具体实践方式。主要的安全评估方式可以大致归结有安全审计、风险评估、能力成熟度、安全测评等四类。

(1) 安全审计

以审计概念为核心的安全评估思想认为存在关于安全的最佳实践(Best Practices)。以通过最佳实践的实施与否及其程度来测量 IT 系统的安全性。这一类相关的模型或指南包括：美国信息系统审计和控制协会的 COBIT、德国的 IT 基本安全保护手册、ISO 17799，还有美国审计总署的自动信息系统安全审计手册等。它们主要针对的是信息系统安全措施的落实和安全管理，是一种符合性的测量，是静态、瞬间的评估。

(2) 风险评估

风险评估模型是从风险管理角度进行安全分析。一般通过调查要保护的 IT 资产，假设这些资产存在的安全威胁、漏洞，以及这些威胁和漏洞对资产可能造成的影响进行评价，经过数学的概率统计得出对安全性的测量，大部分以可能产生的损失来量化。从而提出降低风险，将安全风险控制在可以接受的范围内的风险控制措施。风险分析是一种动态的、反复的评估。

(3) 能力成熟度

能力成熟度模型认为通过过程(Process)来保证安全。最著名的 SSE-CMM 系统安全工程能力成熟模型，其思想来源于卡耐基梅隆的软件工程能力成熟模型(SW-CMM)。它将安全能力划分为 5 个等级，从低到高，低等级是不成熟的、难以控制和重复的，中等级是可管理的、可控的，高等级是可量化、可测量的。能力成熟模型是一种动态的、螺旋式上升的模型。

(4) 安全测评

安全测评是从安全技术、功能、机制角度来进行安全评估。前面提到的橘皮书 TCSEC 标准提出了度量计算机安全特性的分级方法。TCSEC 定义了 7 个等级组成的 A、B、C、D 四个类别，类 A 中的级别 A1 是最高安全级别，类 D 中的级别 D1 是最低安全级别。类别用来度量提供安全保护的程度，每一个级别和类别都是在前一个基础上增加条款形成的。TCSEC 主要从安全功能角度来描述和度量安全级别。它比较适合于对计算机安全，特别是操作系统，进行安全度量，但不适合网络化的 IT 安全测量。CC 为安全技术的分级测量提供很好的方法，特别是信息安全产品。CC 定义了安全功能要求的类、族和部件结构划分。

用户可以从该结构中选择合适的条款来定义他们对产品的安全功能要求。CC也定义安全保证要求的类、族和部件结构划分，此外，安全保证要求使用评估保证级别(EAL)进行区分。

根据上面介绍，可以看出它们分别从不同角度不同侧面来度量安全：技术、管理、工程、人员。对信息安全可以从四个大的方面进行评估：

(a) 产品：建设系统的各种IT产品，包括由产品构成的技术系统；

(b) 工程：就是如何有效地建设安全的系统；

(c) 管理：如何运营管理使用好信息系统；

(d) 环境：人和组织方面因素。

安全尺度主要有四种，风险、能力成熟度、符合性和安全保证级。这些尺度又适用于不同的评估对象。产品/技术主要采用EAL等分级评估，安全过程/工程采用能力成熟度CMM，管理/服务采用符合性，环境(人、组织)也是符合性。

本书将在信息系统安全保障模型指导下，在综合考虑各种安全评估尺度基础上，通过安全保障控制措施和安全保障能力级来定义安全作为度量信息系统安全的尺度。

3. 如何检测和评估的问题

信息安全检测与评估方法主要有两大类，一类是风险评估方法，另一类是安全性评估方法。针对风险评估和审计的评估方法都可以融合和应用到风险和安全性评估方法中。

对于安全风险评估的方法有很多种，概括起来可分为三大类：定性分析方法、定量分析方法、半定量分析方法。

(1) 定性分析方法(Qualitative)

定性分析是最早被广泛采用的方法。定性分析技术大都基于判断、直觉和经验，因此可能由于直觉、经验的偏差而造成分析结果不准确，所以定性分析对风险分析人员有较高的要求，风险分析人员应具备丰富的风险分析经验。

定性分析通过列出各种资产、威胁、脆弱性的清单；然后分析威胁利用资产的脆弱性将对资产造成怎样的后果和影响，并对其发生的可能性进行判定；最后还要对资产的敏感程度、威胁-脆弱性对所造成的后果和影响的严重程度进行分级。

常见定性风险分析方法有HazOp、FEMA等。

(2) 定量分析方法(Quantitative)

定量分析方法是试图从数值上对安全风险进行分析的方法。定量分析过程有两个基本指标作为参考：事件发生的概率及事件造成的损失。

定量分析是在定性分析的逻辑基础上，给出各个风险源的风险量化指标及其发生概率，再通过一定的方法合成，得到系统风险的量化值。它是基于定性分析基础上的数学处理过程。定量的评估方法的优点是用直观的数据来表述评估

的结果客观，可以使研究结果更科学更严密、更深刻。有时，一个数据所能够说明的问题可能是用一大段文字也不能够阐述清楚的。但也存在为了量化，使本来比较复杂的事物简单化、模糊化了。有的风险因素被量化以后还可能被误解和曲解。现在发展较为成熟的方法有 PRA(概率风险评估)、Markov 分析方法、蒙特卡罗方法等。

(3) 半定量分析方法(Semi-Quantitative)

半定量分析方法是定性与定量相结合的综合评估方法。系统风险评估是一个复杂的过程，需要考虑的因素很多，有些评估要素是可以用量化的形式来表达，而对有些要素的量化又是很困难甚至是不可能的，所以在风险评估也是一切都是量化的风险评估过程是科学准确的。定性分析是量化定量分析基础和前提。在复杂的信息系统风险评估过程中，不能将定性分析和定量分析两种方法简单地割裂开来而是应该将这两种方法融合起来，采用综合的评估方法。

实际上，一项风险评估活动都不可能只用一种方法，而是根据具体情况，针对不同评估对象，采用多种评估方法的组合，才能使风险评估更完全、更客观。

安全性评估主要是针对安全功能(措施)正确性和有效性进行分析与评估，也可以定性或定量地评估。一直以来脆弱性分析和渗透性测试是对信息安全测试和评估的主要方法之一。这些以测试为主的评估方法主要是针对功能正确与否，以及功能的实现是否存在缺陷和漏洞，是一种技术性的安全功能强度和抗安全攻击能力的检测。

与 CC 相配套的通用评估方法(Common Evaluation Methodology，CEM)为信息技术安全评估提供新的方法。安全评估依赖相应的评估技术，主要包括：

(a) 处理和过程的分析检查；

(b) 正使用的处理和过程的检查；

(c) TOE 设计描述的相关性分析；

(d) TOE 设计描述与需求的不一致分析；

(e) 证明的验证；

(f) 指导性文档分析；

(e) 功能测试实现和提交的测试结果分析；

(g) 独立的功能测试；

(h) 脆弱性分析(包括缺陷假设)；

(i) 攻击渗透测试等。

IT 产品和系统的安全性评估结果由评估专家确认。确认的依据有三个方面：

(a) 广度：IT 产品和系统进行安全评估的范围；

(b) 深度：通过评估的设计和实现的水平；

(c) 强度：安全功能实现的结构化、形式化程度。

从系统建模(Modeling)仿真(Simulation)技术(简称 M&S)发展的验证(Verification)和证实(Validation)技术(简称 V&V)也可用于软件工程和信息安全的测试与评估。V&V 技术包括“验证”是检验产品是否已正确地实现了规格书所定义的系统功能和特性。验证过程提供证据表明相关产品与所有生命周期活动的要求(如机密性、完整性、可用性等)相一致。“证实”是确认信息系统是否满足用户真正需求的活动。常见的方法有评审、接口分析、语义分析、结构化分析、模型检测等。

除了前面提到的脆弱性分析、渗透性测试和基于 CC 的 CEM 以及 V&V 技术这些主要针对技术安全评估外,对于能力成熟度和符合性的评估方法有审计、符合性测试、SSAM、SCAMPI 等。

本书将风险和安全性联系起来评估作为出发点,提出基于证据理论和评估用例、基于系统安全性差距分析等评估方法。信息系统安全保障是信息安全风险评估的延伸,通过评估识别信息系统在运行中所面临的各种风险,并针对性地制定信息安全保障策略;在保障策略指导下,设计并实现信息安全保障架构或模型,采取保障措施,将风险减少至预定可接受的程度,最终实现对信息系统使命要求的保障。