信息系统安全测评
理论与方法

黄洪韦勇胡勇著

科学出版社

信息系统安全测评理论与方法

黄 洪 韦 勇 胡 勇 著

科学出版社
北 京

内 容 简 介

本书是作者在信息安全测评领域多年经验的结晶，通过理论与实践相结合的方式，向读者介绍在信息安全测评中一些疑难问题的解决方法。读者读完本书之后，既可对信息安全测评工作有更深入的了解，也可参考本书提供的方法解决实际测评活动中可能会遇到的一些难题。

本书适合信息安全专业的学生和从业者阅读，特别是对信息安全测评行业的相关人员有很大的借鉴和参考意义，对普通读者深入地了解信息安全测评工作也有一定帮助。

图书在版编目(CIP)数据

信息系统安全测评理论与方法 / 黄洪，韦勇，胡勇著. — 北京：科学出版社, 2014.10

（计算机系统结构与应用技术研究丛书）

ISBN 978-7-03-042054-1

Ⅰ.①信… Ⅱ.①黄… ②韦… ③胡… Ⅲ.①信息系统-安全技术

Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字（2014）第 225427 号

责任编辑：杨 岭 孟 锐 / 封面设计：墨创文化

责任校对：赵桂芬 / 责任印制：余少力

科学出版社出版

北京东黄城根北街16号

邮政编码：100717

http://www.sciencep.com

成都创新包装印刷厂印刷

科学出版社发行 各地新华书店经销

*

2014 年 10 月第 一 版 开本：787*1092 1/16

2014 年 10 月第一次印刷 印张：9.5

字数：220 千字

定价：49.00 元

前　言

美国国家安全局前雇员斯诺登爆出的“棱镜门”事件让世界各国对信息安全问题更加重视，并纷纷通过颁布标准、实施有效的测评认证制度等方式，对信息技术产品、信息系统及服务实行严格的管理和控制。各国政府投入巨资，由国家主导，针对不同的信息安全需求和技术领域研究相应的测评技术和方法，并开发相应的工具，以建立有效的信息安全测评认证体系，从而保障本国信息安全。

我国正在实行信息安全等级保护制度，通过定级、测评、建设整改、监督检查等活动逐步建立重要信息系统的信息安全保障体系，测评在其中起着承上启下的重要作用，是获取安全建设需求、评价其整体安全状况的手段。然而，信息系统纷繁复杂、信息技术发展迅速，如何有效地对其进行安全测评是一个值得持续关注和研究的问题。本书通过对测评领域的数据安全测评、应用安全测评、整体测评、风险分析、态势感知、自动化测评等问题进行探讨，以期引起更多专家、学者、从业者和其他相关人员对信息安全测评中的相关技术问题的关注和思考，为建立高质量的安全测评技术体系贡献一份绵薄之力。

本书获得多个项目的支持，包括国家自然科学基金项目(No. 61303230)、四川省教育厅项目(No. 11ZB108)、西南科技大学博士基金项目(No. 13ZX7103、No. 11ZX7126)。编写团队由西南科技大学、四川大学的一线教师组成，他们都曾在信息安全领域长期从事信息安全研究与实践工作，具有丰富的经验。本书由黄洪、韦勇和胡勇博士执笔，其中黄洪博士(西南科技大学，曾任公安部信息安全等级保护评估中心测评部门的负责人)为主创作人，负责1、2、3、4、6、8、9章，胡勇博士(四川大学)负责第5章，韦勇博士(西南科技大学)负责第7章，魏蓉(西南科技大学)参与了修订。

感谢公安部信息安全等级保护评估中心的陶源、陈雪秀、张振峰、尚旭光、袁礼等和西南科技大学的黄晓芳、李波、孙海峰老师等对本书的帮助；感谢成都市锐信安信息技术有限公司的陈伟、祈志敏、邓跃良等在算法实验中给出的宝贵建议，作者受益匪浅；感谢国家信息中心软件评测中心的技术总监李刚、深圳职业技术学院的副教授谢朝海对本书的关注和支持。

感谢西南科技大学计算机科学与技术学院的韩永国院长、吴亚东副院长对本书的大力支持；感谢公安部信息安全等级保护评估中心的张宇翔主任、李明主任助理、朱建平研究员，以及国防科学技术大学的刘增良教授等领导专家在作者测评实践、科研活动中给予的指导和帮助，在此表示衷心的感谢。

最后要感谢在本书成稿过程中给予支持的同事、朋友和出版社的编辑，以及作者的家人在忙碌工作时给予的理解和支持。

由于信息技术发展很快、测评技术本身的时效性也很高，限于水平和经验，本书的

不足之处在所难免，望有关专家和读者批评指正，以利再版时修正，交流邮箱为 hong.huang@139.com，联系 QQ 为 10561955。

作　者

2014 年 6 月

目　录

第 1 章　信息系统安全测评概述

物理世界中，人们需要对高速公路、隧道、交通枢纽进行监测，对各种车辆进行年检，以保障鲜活、健康的城市动脉畅通无阻。而网络环境中高速发展的信息高速公路也同样需要保安全、促发展——对信息系统进行安全测评是解决这一问题的重要手段。

1.1　国内外现状与发展趋势分析

1.1.1　国内外现状分析

随着计算机网络的发展，其开放性、共享性和互连程度不断扩大，人们对信息系统的依赖程度不断增加，信息系统的重要性和对社会的影响也越来越大；另一方面，信息系统面临的威胁也越来越多，因而信息系统的安全保护问题显得越来越重要。在信息安全咨询、规划、设计、建设、测评、运维和应急响应等众多信息安全服务中，信息系统安全测评作为建立信息系统安全防护体系、实施合理防御的一项基础性工作，正在国际上兴起，在建立信息系统安全防护体系中发挥着越来越重要的作用。

在 20 世纪六七十年代，信息安全处于以计算机为对象的信息保密阶段时就有信息安全评估活动。1970 年，美国国防科学委员会委托兰德公司、迈特公司(MITIE)和其他与国防工业有关的公司，对当时的大型机、远程终端进行了研究分析，进行了一次较大规模的安全评估工作。1979 年，美国国家标准局(National Bureau of Standards，NBS)颁布了一个风险评估的标准——《自动数据处理系统(ADP)风险分析标准》(FIPS 65)。这个时期的主要工作特点是针对计算机系统的保密性问题提出要求，对安全评估也只关注保密性。

从 20 世纪 80 年代起，计算机系统形成了网络化应用，出现了初期的针对美国军方的计算机黑客行为。美国的审计总署(GAO)对美国国内主要由国防部使用的计算机网络进行了大规模的持续评估。1981—1985 年，美国国防部组织了很大的研究力量研究橘皮书。后来，在这个基础上，形成了一套包括橘皮书在内的 40 多个标准的彩虹系列。这就形成了美国早期的一套比较完整的从理论到方法的有关信息安全评估的准则[1]。1985 年 12 月，美国行政管理和预算局(Office of Management and Budget，OMB)颁布了《联邦信息资源管理政策》(美国行政管理与预算局第 A-130 文件)通告，提出政府信息的保护要建立一个安全级别，以应对计算机入侵带来的损失，并提出依据 1974 年的《隐私法》，进行安全评估，使金融风险和运营风险降到最低程度。1992 年美国联邦政府制定《美国信息技术安全联邦准则》(FC)。1993 年美国和欧洲四国(英、法、德、荷)、加拿大以及国际标准化组织(ISO)开始共同制定《信息技术安全性通用评估准则》(CC)[2]。1999 年

CC 成为国际标准 ISO/IEC 15408，大家逐步认识到了更多的包括保密性、完整性、可用性的信息安全属性，从关注操作系统安全发展到关注操作系统、网络和数据库安全。试图通过对安全产品的质量保证和安全评测来保障系统安全，但实际上仅奠定了安全产品测评认证的基础。

2000 年前后，由于国际范围内出现了大规模黑客攻击事件，信息战的理论逐步走向成熟，而且美国的军、政、经济和社会活动对信息基础设施的依赖程度达到了空前的高度，迫使美国又开始了对信息系统进行新一轮的评估和研究，产生了一些新的概念、法规和标准。1997 年美国国防部颁布了《国防部 IT 安全认证和认可过程》(DITSCAP)。修改后的 OMB A-130 要求，应该将风险评估作为基于风险的方法的一部分来为系统实现适当的、成本有效性更好的安全，用来评估系统风险性质和级别的方法中应该包括对风险管理主要因素的考虑：系统和应用的价值、威胁、脆弱性，当前或所建议的安全措施的有效性。在军方提出信息保障(Information Assurance，IA)概念的基础上，克林顿和小布什两任政府持续数年进行了国家信息安全保护计划和信息保障战略的研究。2002 年美国颁布了《联邦信息安全管理法案》。此外，美国国家标准和技术研究所(National Institute of Standards and Technology，NIST)先后发布了面向信息系统安全评估的一系列指南和标准。NIST 在 2000 年 11 月为 CIO(Chief Information Officer)委员会制定的《联邦 IT 安全评估框架》中提出了自评估的 5 个级别，针对该框架，NIST 颁布了《IT 系统安全自评估指南》(SP 800-26)，为三大类 17 项安全控制提出了 17 张调查表。从 2002 年 10 月开始，NIST 先后颁布了《联邦 IT 系统安全认证和认可指南》(SP 800-37)、《联邦信息和信息系统的安全分类标准》(FIPS 199)、《联邦 IT 系统最小安全控制》(SP 800-53)、《将各种信息和信息系统映射到安全类别的指南》(SP 800-60)等文档，试图通过信息安全测试评估加强联邦政府的信息安全[3]。

目前，相关后续文档仍在制定之中。随着对信息保障研究的深入，保障对象明确为信息和信息系统；保障能力明确来源于技术、管理和人员三方面；认识到 CC 和 FIPS 140-2 等标准仅适合安全产品的测评认证，对于信息系统则需要确立新的包括非技术因素的全面安全评估。到这一阶段，安全评估已经成为一种通用的方法学和基础理论，应用到广泛的信息安全实践工作之中。

我国在信息系统安全的研究与测试评估方面与先进国家和地区存在很大差距。公安部主持制定、国家质量技术监督局发布的中华人民共和国国家标准 GB 17895《计算机信息系统安全保护等级划分准则》在 1999 年正式颁布并实施[4]。该准则将信息系统安全分为 5 个等级：自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级。主要的安全考核指标有身份认证、自主访问控制、数据完整性、审计等，这些指标涵盖了不同级别的安全要求。该准则为我国信息安全产品的研制提供了技术支持，也为安全系统的安全测试评估提供了技术指导。另外一个比较重要的标准 GB 18336(等同于 ISO 15408－1999 标准)，存在只适合于信息安全产品测评而不太适合于信息系统安全测评的局限性。

对于信息安全测评的标准化工作，我国虽然起步较晚，但是近年来发展较快。成立于 1984 年的全国信息技术安全标准化技术委员会(CITS)，负责全国信息技术领域和与

ISO/IEC JTC1 相对应的标准化工作，目前下设 24 个分技术委员会和特别工作组，是一个具有广泛代表性、权威性和军民结合的信息安全标准化组织。该组织从 20 世纪 80 年代开始，本着积极采用国际标准的原则，转化了一批国际信息安全基础技术标准，制定了一批符合中国国情的信息安全标准，同时，对一些重点行业还颁布了一批信息安全的行业标准。据统计，我国从 1985 年发布了第一个有关信息安全方面的标准以来，到 2013 年年底共制定、报批和发布有关信息安全技术、产品、测评和管理的国家标准 70 多个，正在制定中的标准 50 多个，其中包括关于信息系统安全等级保护测评和风险评估指南方面的标准，这些标准已完成相关试点工作，已形成或即将形成国家标准，为我国开展信息安全测评工作奠定了标准方面的基础。

1.1.2　发展趋势分析

目前，各国进行的信息系统安全测评工作大致可以归结为具有固定指标的符合性安全测评和没有固定指标的安全测评两大类。具有固定指标的符合性安全测评比较典型的方式是利用 ISO 17799 进行的安全管理体系评估。我国主要采取信息系统安全等级保护测评方法(以下简称等级测评)，采用的标准是《信息系统安全等级保护基本要求》(GB/T 22239—2008)[5](以下简称《基本要求》)和《信息系统安全等级保护测评要求》(GB/T 28448—2012)[6](以下简称《测评要求》)；没有固定指标的安全测评方法比较典型的是风险评估。等级测评和风险评估各具优势，将其进行有机融合，充分发挥这两种方法的优点，是目前我国信息系统安全测评领域研究的一个热点问题。

1.2　等级测评工作分析

1.2.1　等级测评的目的和意义

(1)等级测评在本质上是一种标准符合性评定工作，在业务上是一项专业技术检测活动。根据《信息安全等级保护管理办法》(公通字［2007］43 号)(以下简称《管理办法》)的规定，信息系统按照《基本要求》等技术标准建设完成后，运营、使用单位或者其主管部门应选择符合规定条件的测评机构，依据《测评要求》等技术标准，定期对信息系统安全等级状况开展等级测评，以确定信息系统安全状况、安全保护制度和措施的落实情况。因此，等级测评这一技术活动，有助于人们判断当前信息系统的安全保护能力，确定信息系统的安全等级保护状况。

(2)等级测评可以发现信息系统存在的安全问题，有助于运营、使用单位对信息系统进行整改以提升信息系统的整体安全保护能力。在等级测评过程中，信息系统安全状况未达到安全保护等级要求的，运营、使用单位可以按照等级测评发现的问题，有针对性地提出整改方案，进行安全整改。这样就避免了此前进行安全整改的无目的性和无方向性，增强了针对性。因此，通过等级测评确定系统安全整改需求，然后进行信息系统整

改，有助于信息系统安全保障体系的建立，方便提升信息系统的整体安全保护能力。

(3)等级测评结果可以作为公安机关等管理部门进行安全监督、检查、指导的依据。《管理办法》规定信息系统运营、使用单位应接受公安机关、国家指定的专门部门的安全监督、检查、指导，如实向公安机关、国家指定的专门部门提供有关信息安全保护的信息资料和数据文件，其中包括对信息系统开展等级测评的技术测评报告。通过等级测评报告，公安机关可以更容易、更方便地进行检查，以便及时发现信息系统安全保护状况是否符合信息安全等级保护有关管理规范和技术标准要求，并及时通知运营、使用单位进行整改。

1.2.2 等级测评的范围和主要内容

等级测评的范围应该是全部定级对象，特别是三级以上信息系统。《管理办法》要求信息系统建设完成后，运营、使用单位或者其主管部门应选择符合规定条件的测评机构，依据《测评要求》等技术标准，定期对信息系统安全等级状况开展等级测评。第三级信息系统每年应至少进行一次等级测评，第四级信息系统每半年应至少进行一次等级测评，第五级信息系统应依据特殊安全需求进行等级测评。

等级测评的主要内容包括在确定的测评指标范围内进行现场测评(包括单元测评和整体测评)，综合分析，并给出等级测评报告等一系列内容。

测评指标范围可以确定对信息系统安全等级保护状况进行测试评估的单元测评内容的范围。包含的内容涉及信息系统安全技术和安全管理上的各个安全控制措施，是信息系统整体安全测评的基础。单元测评的测评指标直接指向《基本要求》相应等级的要求项，两者完全一致。

综合分析的一项主要内容是对信息系统的整体安全保护状况进行安全测评分析。等级测评报告应给出“符合”、“基本符合”或者“不符合”等测评结论。

1.2.3 等级测评执行主体

《管理办法》规定三级以上信息系统应选择符合下列条件的等级保护测评机构进行测评。

(1)在中华人民共和国境内注册成立(港澳台地区除外)。

(2)由中国公民投资、中国法人投资或者国家投资的企事业单位(港澳台地区除外)。

(3)从事相关检测评估工作两年以上，无违法记录。

(4)工作人员仅限于中国公民。

(5)法人和主要业务、技术人员无犯罪记录。

(6)使用的技术装备、设施应符合本办法对信息安全产品的要求。

(7)具有完备的保密管理、项目管理、质量管理、人员管理和培训教育等安全管理制度。

(8)对国家安全、社会秩序、公共利益不构成威胁。

1.2.4　等级测评的工作要求

开展等级测评的主要工作要求是依据标准，遵循原则，恰当抽样，保证强度，规范行为，减少风险。

依据标准，是指要依据等级保护的相关技术标准进行等级测评。相关技术标准主要包括《基本要求》和《测评要求》，其中《基本要求》解决测评的目标和内容等方面问题，《测评要求》解决测评的方法、实施过程和判定要求等方面问题。

遵循原则，主要是指在等级测评过程中，要遵循规范性、可控性、整体性、最小影响和保密性原则。遵循这些原则可以保证测评工作规范、科学、有效和合理，使风险最小化。

恰当抽样，是指对具体测评对象的抽样要恰当，既要避免重要的对象、可能存在安全隐患的对象没有被抽样，也要避免过多抽样，使工作量增大，不能按期完成测评任务。

保证强度，是指对被测系统应实施与其等级相适应的测评强度。不要用高等级的测评标准度量测评低等级的信息系统，使信息系统严重未达到标准要求；也不要用低等级的测评要求度量测评高等级的信息系统，使得不能恰当地评价信息系统的安全性，在信息系统面临实际威胁时，不能有效地保护其免受破坏。

规范行为，一方面是指等级测评的过程、流程要规范；另一方面是指测评人员的行为要规范，还有就是在等级测评实施过程中用到的方法、技术也要规范，确保测评的结果准确、可靠，不容易引起歧义。

减少风险，是指要充分估计测评可能给被测系统带来的影响，向被测系统单位揭示风险，要求其提前采取预防措施进行规避，同时，测评单位也应采取规范测评过程、及时与被测系统单位沟通等措施，尽量避免给被测系统和单位带来影响，特别是针对保密性要求高或连续性要求高的信息系统。

1.3　等级测评模型框架

为了描述等级测评的不同内容——现场测评的单元测评和整体测评以及非现场的综合分析等的相互关系以及它们使用的测评技术手段，引入等级测评模型。

根据《测评要求》等标准，等级测评是以单元测评为基础的。在单元测评的基础上，可以开展整体测评。《测评要求》介绍的整体测评主要以正向为主，包括安全控制间、层面间和区域间的相互作用的安全测评以及系统结构的安全测评。

整体测评还包括反向的整体测评，如通过漏洞扫描和渗透测试等方法对系统进行整体测评。综合分析则是根据整体测评的结果对信息系统的整体安全保护状况进行综合分析。它们之间的关系可用图 1-1 来表示。

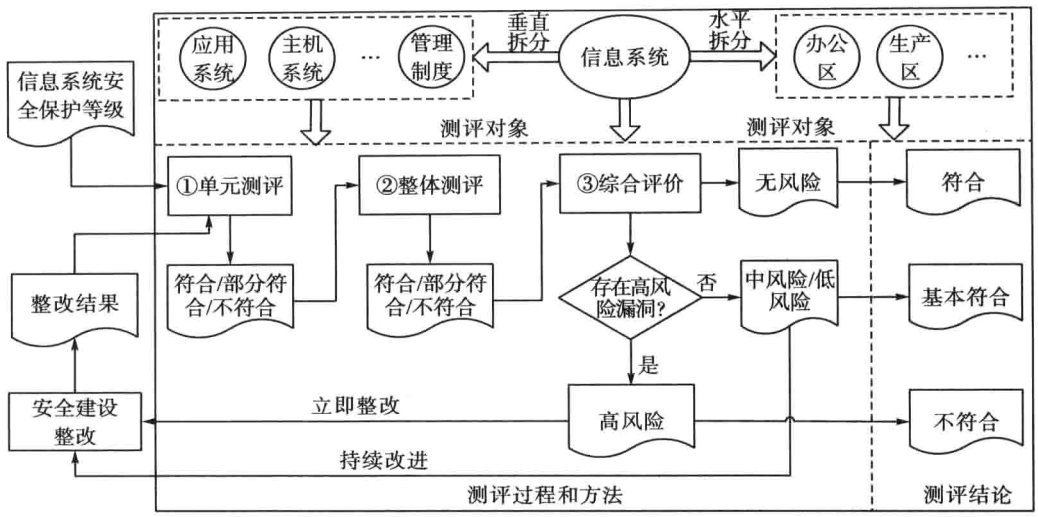

图 1-1 等级测评模型图

如图 1-1 所示，信息系统安全等级测评分为单元测评、整体测评和综合评价三个过程，其中单元测评是系统整体测评、综合评价的基础，综合评价采取风险分析和保护能力综合评价方法，综合评价可以帮助信息系统用户清楚地了解系统的安全现状，也可帮助决策人员对全国各行业信息系统的安全现状有一个比较全面、清晰的认识。

1.4 系统单元测评方法

单元测评由测评指标、测评对象、测评方法和测评证据等多种因素构成，用图 1-2 把这些因素关联起来构成单元测评模型。

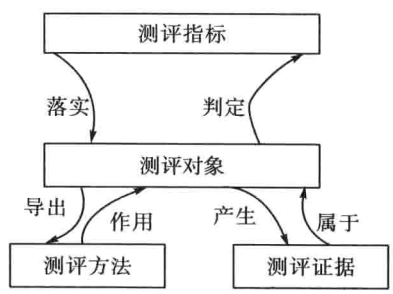

图 1-2 单元测评模型

单元测评模型把测评指标、测评对象、测评方法和测评证据联系在一起。在特定信息系统中进行单元测评就是判断该信息系统的安全保护状况是否符合相应测评指标的过程。但是由于信息系统是由不同层面上的不同组件(对象)构成的，所以需要把测评指标落实到特定的测评对象上。对于同一测评对象上的不同指标，可能需要用到不同的测评方法；对于落实在不同测评对象上的同一测评指标，同样可能需要用到不同的测评方法，因此，在这种意义上，测评指标和测评对象的结合可以导出测评方法。不同测评方法作

用到测评对象上就产生我们需要的、可以客观地反映出来的测评证据。属于不同测评对象的测评证据可以用来判定信息系统是否满足相应的测评指标。

(1)在测评模型上，测评指标既是单元测评的起点，也是单元测评的终点，测评指标起到统领全局的作用。因此，对于特定信息系统，正确选择测评指标对整个测评工作的成败起着关键作用。等级测评的测评指标是分层次的，具有层次体系结构。测评指标体系的最顶层是信息系统的整体安全保护能力要求，它也是信息系统不同等级的最基本要求。信息系统是否满足测评指标体系的最顶层要求是不能直接测评出来的，而是通过对下层测评结果的综合评价得到的。由于下层不同测评指标对上层测评指标的贡献大小是不一样的，所以在综合评价过程中，不同指标应该有不同的权重赋值。测评指标体系的最底层是《基本要求》的要求项，也是单元测评下的测评项。单个测评项的测评结果是可以直接依据测评证据使用优势证据法等判断出来的。

(2)在测评模型上，测评对象起着联系测评指标与测评方法、测评方法与测评证据、测评证据与测评指标的重要作用。测评对象既是在特定信息系统落实测评指标的落脚点，也是测评方法的作用对象，还是测评证据的依托对象。由于信息系统的复杂性，在进行等级测评时，往往需要对信息系统的构件进行抽样测评。抽样可以采用统计抽样方法，也可以采用非统计抽样方法。另一方面，构成信息系统的不同组件(对象)在信息系统中所起的作用、所处的位置的不同，决定了不同测评对象对不同层次测评指标的贡献也会不尽相同，即不同测评对象对不同层次测评指标的结论判定的权重是不一样的。因此，综合评判信息系统整体安全保护能力时，需要考虑测评对象所处的位置和所起的作用。

(3)测评方法是在特定测评对象上获取有效证据的具体方法。有时，在同一测评对象上对同一测评指标进行测评，可能会有多种方法。对这些不同的测评方法进行选择时，需要考虑测评强度，应选择能够保证与信息系统安全等级相适应的测评方法。

(4)测评证据具有客观性和时效性。客观性指测评证据是测评工作人员从信息系统观察到的、触摸到的、听到的实实在在的东西，是没有增加个人主观判断的、可以重复的客观事实。时效性指测评证据是当前信息系统的反映，如果信息系统的状态发生变化，构成组件发生变更，所取得的测评证据就有可能失效。

单元测评模型的提出有助于讨论在信息系统开展单元测评所涉及的关键技术，并能更好地展示这些关键技术在单元测评工作过程中的位置和作用。

1.5　系统整体测评方法

系统整体测评是建立在单元测评基础上的对信息系统整体安全状况进行分析的一种安全测评。系统整体测评可以从正向和反向两种不同的角度进行。

1.5.1　正向测评方法

正向是从保护的角度对信息系统进行整体安全测评，可以考察信息系统当前各种安全措施的关联互补情况，给出不同安全措施的关联对信息系统的安全保护能力构成的影