注册信息安全人员资质认证教材

HZ BOOKS 华章科技

Introduction to Information Assurance

信息安全保障导论

吴世忠 李斌 张晓菲 谢安明 编著

机械工业出版社
China Machine Press

Introduction to Information Assurance

信息安全保障导论

吴世忠 李斌 张晓菲 谢安明 编著

机械工业出版社
China Machine Press

图书在版编目（CIP）数据

信息安全保障导论 / 吴世忠等编著 . —北京：机械工业出版社，2014.8

ISBN 978-7-111-47420-3

I. 信… II. 吴… III. 信息系统 – 安全技术 IV. TP309

中国版本图书馆 CIP 数据核字（2014）第 164191 号

本书从我国国情出发，结合我国网络基础设施和信息系统安全保障的实际需求，以知识体系的全面性和实用性为原则，明确了信息安全专业人员应该掌握的信息安全技术的主体内容和相关的法律法规。

本书涵盖信息安全保障、技术、工程、管理、法律、法规及标准等领域知识。第 1 ~ 2 章，介绍了信息安全的背景、模型、现状、安全基础（密码学、TCP/IP）；第 3 ~ 7 章，从网络安全、终端安全、应用安全、数据安全、安全攻防几大方面讲解信息安全的深度防御策略；第 8 章介绍了信息安全技术的最新进展，为读者呈现前沿的安全技术概况。第 9 ~ 10 章介绍了信息安全的管理体系、信息安全的风险管理、基本的信息安全管理措施。第 11 ~ 12 章讲解了安全事件管理与应急响应、信息系统灾难恢复管理、信息安全工程原理以及信息安全工程实践方面的知识。第 13 章给出了信息安全法律、法规、政策与标准。

信息安全保障导论

吴世忠　等编著

出版发行：机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码：100037）
责任编辑：高婧雅　　责任校对：董纪丽
印　　刷：中国电影出版社印刷厂　　版　　次：2014 年 8 月第 1 版第 1 次印刷
开　　本：185mm × 260mm　1/16　　印　　张：16.75
书　　号：ISBN 978-7-111-47420-3　　定　　价：69.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991　88361066　　投稿热线：（010）88379604
购书热线：（010）68326294　88379649　68995259　　读者信箱：hzjsj@hzbook.com

前　言

随着信息化不断深入，信息安全已关乎到社会稳定、经济发展和公民权益，成为国家安全的重要组成部分。在整个信息安全保障工作中，人是最核心、最活跃的因素，信息安全保障工作最终也是通过人来落实。在信息安全保障工作中，除了信息安全专业人员外，广大网络和信息系统的使用人员也需要具备必要的安全意识和基本技能。因此，开展面向网络和信息系统使用人员的信息安全培训认证是建设我国信息安全保障体系必备的基础和先决条件，也是完善信息安全人才体系的基石。

中国信息安全测评中心依据中央赋予的职能，自2002年起，积极推动我国信息安全人才培养工作。一方面支持并配合国内多所大学开办了信息安全专业，有力促进了信息安全学历教育的开展；另一方面在原国务院信息化办公室的支持下，开创性地开展了信息安全职业教育与能力认证工作，面向社会提供“注册信息安全员”（CISM）培训服务。

指导书和知识体系是信息安全职业培训认证工作的核心因素。中国信息安全测评中心在全面考察国际知名信息安全职业教育知识体系的基础上，汇集国内诸多专家学者智慧，并汲取教学实践体验，在此基础上编撰了《信息安全保障导论》，与面向专业人员培训教材《信息安全保障》、《信息安全技术》一起，搭建有志掌握信息安全专业知识人士成长的阶梯。

本书以知识体系的全面性和实用性为原则，涵盖信息安全保障、技术、工程、管理、法律、法规及标准等领域知识，满足各岗位日常工作所需。这三本书主要面向国家部委、重要行业、科研院所及企事业单位的信息化从业人员，适用于信息技术产品研发测试、信息系统建设运维、信息系统使用人员等方面的操作人员、技术人员和管理人员。

这三本书在修订完善的过程中得到社会各界人士的关心与支持，在此表示衷心的感谢。

教材中不妥或错误之处恳请广大读者批评指正。

目　录

第 1 章

信息安全保障

信息安全的实质就是保护信息系统或信息网络中的信息资源免受各种类型的威胁、干扰和破坏。随着信息化的不断深入，信息已经成为社会发展的重要战略资源，信息安全对经济发展、国家安全和社会稳定的影响也日渐突出，各国纷纷重视信息安全保障工作，将其作为国家安全战略的重要组成部分。

1.1 信息安全保障背景

20 世纪 90 年代以来，信息技术不断创新，信息产业持续发展，信息网络广泛普及，信息化成为全球经济社会发展的显著特征。信息化与经济全球化相互交织，推动着全球产业分工深化和经济结构的调整。信息安全事件逐步增多，所造成的后果日益严重，信息化在国家发展中的重要作用和地位显著上升，信息安全已经得到世界各国的高度重视。

1.1.1 信息和信息安全

信息是一种消息，泛指人类社会传播的一切内容。在计算机系统中，信息通常以文字、声音、图像或数据的形式展现出来，它是按一定方式排列起来的、有意义的符号序列。

信息安全是一个广泛而抽象的概念，它关注的是信息自身的安全。信息安全的任务是保护信息财产，以防止不经意修改，或者未被授权者对信息的恶意泄露、修改和破坏，从而导致信息的不可靠或无法处理等现象。信息安全主要从 3 个方面描述，即信息的保密性（Confidentiality）、完整性（Integrity）和可用性（Availability），也称 CIA，它是信息安全的基本属性。

保密性，也称机密性，指的是对信息资源开放范围的控制，确保信息没有非授权的泄

露，不被非授权的个人、组织和计算机程序使用。需要保密的信息范畴十分广泛，它可以是国家秘密、企业或研究机构的核心知识产权或银行账号等个人信息。

完整性，有两层含义：一方面是指信息的完整性，即保证计算机系统中的信息处于完整或未受损坏的状态，确保信息没有遭到篡改和破坏；另一方面是指信息系统的完整性，即确保信息系统没有被更改或破坏。任何对系统信息的插入、窃取、篡改和伪造都是破坏系统信息完整性的行为，这种篡改和破坏可能是无意的错误，如设备故障、输入错误和软件瑕疵等，也可能是有意的更改或破坏，如攻击。

可用性是指保证信息或系统服务可以被授权实体访问，并按需要及时、正常地使用，防止由于人为或非人为的因素而拒绝合法用户对信息和服务的使用。

CIA 的形成侧重于信息和信息系统本身的安全性，当研究通信过程中数据的安全时，通信活动参与者的可信任问题也需要讨论，即要考虑数据是否确实来源于它声称的地方，数据的发送者是否可以否认其发出过这些信息等问题。此时，一般在 CIA 之外，还要求关注另外两个属性：可认证性（Authenticity）和不可否认性（Non-Repudiation）。

可认证性，也称作“可鉴别性”，通过对实体身份和数据来源的确认，保证两个或多个通信实体的可信，以及数据源的可信。

不可否认性，也称作“不可抵赖性”或“抗抵赖性”，主要用于网络信息的交换过程，保证信息交换的参与者都不能否认或抵赖曾发生的操作。

造成信息安全问题频发的因素很多，黑客攻击、病毒破坏、系统漏洞、运行错误和人为失误等都可以造成安全问题。信息安全问题出现的根本原因可以归纳为“内因”和“外因”两个方面。

内因是指信息系统自身存在漏洞，计算机程序是由人编制出来的，有可能考虑不周，造成信息系统不可避免地会存在漏洞，出现操作人员操作失误等情况。同时，信息系统运行的环境复杂，随着系统功能的不断增加，系统中会存在技术和管理方面的漏洞。

外因包括“环境因素”和“人为因素”两个方面。从自然环境的角度看，雷击、地震、火灾和洪水等自然灾害发生时，容易使信息系统所在机房和设备遭受破坏，电力、空调和电磁脉冲等出现问题时可能使信息系统出现软、硬件损坏，这些都会引发信息安全问题。从人为因素看，对一个信息系统而言，只要存在利益和兴趣，就可能有人想来盗取数据或破坏系统，这也是网络中存在黑客和犯罪团伙的原因。信息系统的外部攻击威胁可以分为个人层面威胁、组织层面威胁和国家层面威胁 3 种，如表 1-1 所示。

表 1-1 信息安全的外部攻击威胁

国家威胁	信息战士	巩固战略优势，制造混乱，进行目标破坏
	情报机构	搜集政治、军事，经济信息
组织威胁	恐怖分子	破坏公共秩序，制造混乱，发动政变
	工业间谍	掠夺竞争优势，恐吓
	犯罪团伙	施行报复，实现经济目的，破坏制度
个人威胁	社会型黑客	攫取金钱，恐吓，挑战，获取声望
	娱乐型黑客	以娱乐、吓唬人为乐，喜欢挑战

1.1.2 信息安全发展

信息安全的发展经历了通信安全（Communication Security，COMSEC）、计算机安全（Computer Security，COMPUSEC）、信息系统安全（Information Systems Security，INFOSEC）和信息安全保障（Information Assurance，IA）4 个阶段。

在计算机出现以前，信息安全保障的主要内容是通信保密。通信保密和通信安全的概念成熟于 20 世纪 40 年代到 70 年代，主要通过密码技术解决通信保密的问题，保证数据的保密性和完整性，多应用于军事和政府的信息系统。

随着计算机的广泛使用，20 世纪 80 年代到 90 年代计算机安全的理论和技术逐渐成熟。计算机安全阶段的主要安全目标是确保信息系统资产（包括硬件、软件、固件和通信、存储和处理的信息）的保密性、完整性和可用性。这个阶段的重要标志是 1985 年美国国防部发布《可信计算机系统评估准则》（Trusted Computer System Evaluation Criteria，TCSEC），也称“桔皮书”。

信息系统安全阶段，也称为“网络安全阶段”或“信息技术安全”（Information Technology Security，ITSEC）阶段。信息系统安全阶段综合了通信安全和计算机安全的特征，主要是保护信息系统，确保信息在存储、处理和传输过程中免受非授权访问，防止授权用户遭遇拒绝服务，以及检测、记录和对抗此类威胁的措施。信息系统安全阶段的主要安全目标是防范网络入侵和对抗网络攻击，为了抵御这些威胁，人们开始使用防火墙（Firewall）、防病毒软件和虚拟专用网（Virtual Private Network，VPN）等安全产品。这个阶段的重要标志是出现了国际标准《信息技术安全评估通用准则》（Common Criteria for Information Technology Security Evaluation）。

随着信息化的不断深入，信息化已经成为组织机构工作和生活不可或缺的一部分，人们逐渐认识到信息安全保障不能仅仅依赖于信息安全技术。信息系统是动态发展的，信息安全管理发挥着重要的作用，信息安全保障的概念逐渐形成和成熟。信息安全保障就是把

信息系统安全从技术扩展到管理，以动态安全的思想保障信息系统业务的正常、稳定运行。

上述 4 个阶段的主要特点如表 1-2 表示。

表 1-2 信息安全发展各阶段特点

阶段	年代	安全威胁	安全措施
通信安全	20 世纪 40 ~ 70 年代	搭线窃听、密码学分析	加密
计算机安全	20 世纪 70 ~ 90 年代	非法访问、 恶意代码、 脆弱口令等	安全操作系统设计技术
信息系统安全	20 世纪 90 年代	网络入侵、 病毒破坏、 信息对抗等	防火墙、防病毒、 漏洞扫描、 入侵检测、 VPN 等
信息安全保障	今天	黑客、恐怖分子、信息战、自然灾难等	技术体系、管理体系、信息安全工程、人员培训 / 教育、测评认证等

从信息安全发展阶段的计算机安全到信息安全保障，安全不再是单纯的技术问题。尤其是进入 21 世纪以后，信息安全的威胁来源发生了很大的变化。信息安全保障面对的不再是简单的病毒、木马和个人黑客，有组织的网络犯罪、网络恐怖主义、网络间谍和网络空间军事对抗等高级持续威胁（Advanced Persistent Threat，APT）的出现，使信息安全面临更加复杂、危险的局面。

2008 年以来，各国纷纷将信息和网络空间安全上升到国家安全的高度，从战略、组织结构、军事、外交和科技等方面加强信息安全保障。其中，美国的建设力度最大，速度也最快，其信息安全防御思想从单纯被动防御逐步转向“积极防御”，这种“积极防御”是指包含进攻与威慑在内的“先发制人”的安全防范战略和思想。与传统信息安全保障相比，信息安全新的发展趋势是将防御（Defense）、威慑（Offense）和利用（Exploitation）相结合，形成三位一体的“信息安全保障 / 网络空间安全”（Information Assurance/Cyber Security，IA/CS）。因此，也有研究者和文献将从 2008 年开始的信息安全发展阶段定义为“信息安全保障 / 网络空间安全”阶段。

1.2 信息安全保障概念和模型

信息技术发展到网络化社会阶段，信息安全作为一个日益重要而尖锐的问题，涉及面越来越广，众多因素和变量均处于“不确定状态”，在这种情况下只能维持一种动态、可控的安全状态，信息安全保障就是这样一种安全理念。

1.2.1 信息安全保障概念

信息安全保障的概念最早是由美国军方率先提出的，它强调了信息安全的保护能力，提出要重视提高系统的入侵检测能力、系统的事件反应能力，以及系统在遭到入侵后的快速恢复能力。它关注的是信息系统整个生命周期的防御和恢复。1998 年 5 月，美国政府颁发了《保护美国关键基础设施第 63 号总统令》，围绕信息保障，成立了一个全国性机构，加强对其国家关键基础设施，特别是信息基础设施保护的研究和实施。

在这一时期，其他国家也对信息安全进行了大量的研究。信息安全的属性由最早的保密性、完整性和可用性扩大到了保密性、完整性、可用性、可认证性和不可否认性 5 个方面；保障对象明确为信息、信息系统；保障能力明确来源于技术、管理和人员 3 个方面；关注局域计算环境、边界与外部连接、网络基础设施；以保护、检测、反应和恢复 4 个工作环节形成支撑条件，构建纵深防御体系。

简单地说，信息安全保障不仅仅是将信息安全技术产品和设备堆叠到信息系统建设中，而是综合考虑技术、管理、工程和人员等各种要素，保障信息系统业务和使命安全。除了要防止信息泄露、修改和破坏外，还应当检测入侵行为，计划和部署针对入侵行为的防御措施，同时采用安全措施和容错机制，在遭受攻击的情况下保证机密性、完整性、可用性、不可否认性和可认证性，修复信息和信息系统所遭受的破坏，这就是“信息安全保障”。

信息安全保障对安全的考虑远远超出技术本身的范畴，扩展到使用、管理、过程乃至法规和道德等。信息安全作为一个日益重要而尖锐的问题，涉及面越来越宽，涉及内容越来越多。众多因素和变量均处在“不确定”的状态，要在这种不确定的情况下实现安全，只能是维持一种动态、可控、可接受的风险管理状态，即通过各种综合手段和方法将安全风险控制在可接受的范围内。

同传统信息安全和信息系统安全的概念相比较，不难看出，信息安全保障的概念更加广泛。第一，它强调检测响应，是一种动态保护的概念。第二，它关注全局、系统性的防范功能，是一种系统保护的观点。第三，它注重使用、管理、规程和操作要求等方面，是一种保证条件的观点。第四，它对信息系统进行全生命周期的保护，是一种长期保护的观点。第五，它要求实现风险管控的目标，而不是彻底消除风险，这体现了安全经济学的观点。

1.2.2 信息安全保障相关模型

信息安全保障相关模型能准确描述安全的重要方面与系统行为的关系，提高对关键安全需求的理解层次，PDCA 模型和信息保障技术是信息安全管理和信息安全保障技术实施

过程遵循的方法和思想。

1. PDCA 模型

PDCA 循环又叫戴明环，它是管理学常用的一个过程模型（见图 1-1），由美国质量管理专家戴明（Edwards Deming）博士运用于持续改善产品质量的过程当中。随着全面质量管理理念的深入发展，PDCA 得以普及。

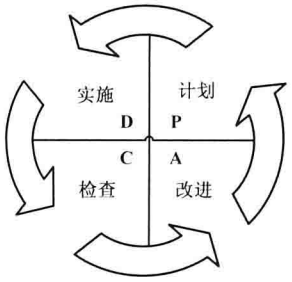

图 1-1　PDCA 戴明环过程模型

PDCA 由英语单词 Plan（计划）、Do（实施）、Check（检查）和 Act（改进）的第一个字母连接构成。P（Plan）是指依照组织的整体方针和目标，分析并控制风险，制定信息安全有关的安全方针、目标、指标、过程和程序。D(Do) 是指依据计划具体实施。C（Check）是指评估过程质量，并向决策者报告结果。A（Act）是指采取纠正和预防措施进一步提高过程质量。

PDCA 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，PDCA 循环即指按照这样的顺序进行质量管理，并且循环不止地进行下去的科学程序。全面质量管理活动的运转，离不开管理循环的转动，也就是说，改进与解决质量问题，赶超先进水平的各项工作，都要运用 PDCA 循环的科学程序。无论是提高产品质量，还是减少不合格产品，都要先提出目标，即质量提高到什么程度，不合格品率降低多少，需要有个计划，这个计划不仅包括目标，而且也包括实现这个目标需要采取的措施。计划制订之后，就要按照计划进行检查，看是否达到了预期效果，有没有达到预期的目标，通过检查找出问题和原因，最后要进行处理，将经验和教训制定成标准、形成制度。

在应用时，PDCA 模型按照 PDCA 的顺序依次进行，一次完整的 PDCA 可以看成组织在管理上的一个周期，每经过一次 PDCA 循环，组织的管理体系都会得到一定程度的完善，同时进入下一个更高级的管理周期，通过连续不断地 PDCA 循环，组织的管理体系能够得到持续的改进，管理水平将随之不断提升。

这种连续不断的 PDCA 循环，有 3 个特点。

（1）循序渐进，周而复始

每个 PDCA 循环按照 PDCA 的顺序依次进行，依靠实施者的力量来推动，像车轮一

样向前进，周而复始，不断循环，持续改进，如图 1-2 所示。

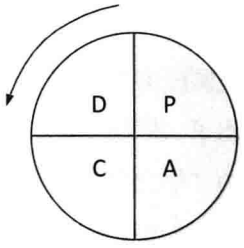

图 1-2 PDCA 循序渐进特征

（2）层层循环，环环相扣

各级质量管理都有一个 PDCA 循环，如此一来，形成一个大环套小环，一环扣一环，互相制约、互为补充的有机整体。在 PDCA 循环中，一般来说，上一级的循环是下一级循环的依据，下一级的循环是上一级循环的落实和具体化，如图 1-3 所示。

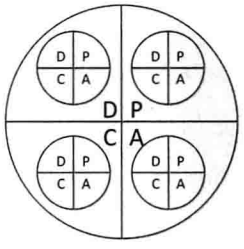

图 1-3 PDCA 层层循环特征

（3）不断循环，不断提高

每经过一次 PDCA 循环，都要进行总结，巩固成绩、改进不足，同时提出新的目标，以便进入下一次更高级的循环。因此，每个 PDCA 循环，都不是在原地周而复始运转，而是螺旋上升，每一次循环都有新的目标和内容，这意味着质量管理，经过一次循环，解决了一批问题，质量水平有了新的提高，如图 1-4 所示。

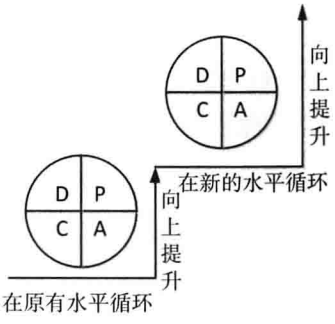

图 1-4 PDCA 的不断提高特征

PDCA 循环实际上是有效进行任何一项工作的合乎逻辑的工作程序。在质量管理中，PDCA 循环得到了广泛的应用，并取得了很好的效果，因此有人称 PDCA 循环是质量管理的基本方法。之所以将其称为 PDCA 循环，是因为这 4 个过程不是运行一次就完结，而是要周而复始地进行。一个循环完成，解决了一部分的问题，可能还有其他问题尚未解决，或者又出现了新的问题，再进行下一次循环。

PDCA 循环的 4 个阶段，体现着科学认识论的管理手段和工作程序。PDCA 管理模式的应用对提高日常工作的效率有很大的益处，它不仅在质量管理工作中可以运用，同样也适合于其他各项管理工作。

需要注意，随着 PDCA 模型的发展，有的研究文献使用 Policy、Do、Check 和 Adjust 这 4 个单词，表达策略、执行（实施）、检查和调整的概念，其缩写仍然是 PDCA，核心意思还是一致的。

2. 信息保障技术框架

信息保障技术框架（Information Assurance Technical Framework，IATF）是美国国家安

全局（National Security Agency，NSA）制定的，描述美国信息保障的指导性文件，为保护美国政府和工业界的信息与信息基础设施提供技术支持。

美国国家安全局于1998开始，研究信息安全保障框架历经数年。起初，美国国家安全局提出了“网络安全框架”1.0版本，1999年8月提出2.0版本，并正式将“网络安全框架”更名为“信息保障技术框架”（即IATF2.0版）。2000年，美国国家安全局发布IATF3.0版，将IATF的表现形式和内容通用化，使用范围不仅仅局限于美国国防部。2002年9月发布了IATF3.1版本，扩展了“纵深防御”，强调信息保障战略，并补充了语音网络安全方面的内容。

IATF要解决的问题主要有：如何定义信息保护的需求和解决方案；现有的何种技术能够满足信息保护需求；什么样的机构资源能够帮助获得所需的保护；当前有哪些信息保障产品和服务；对信息保障方法和技术的研究关注点应放在哪里等。虽然IATF最早是在军事需求的推动下组织开发的，但其内容和思想完全可以用于指导政府和各行各业的信息安全保障工作。

IATF认为，信息系统的安全不是仅靠一两种技术或者简单地设置几个防御设施就能实现的，它提出了深度防御战略（Defense in Depth），即应当通过在各个层次技术框架区域中实施保障机制，部署多层次纵深安全措施，才能在最大限度内降低风险，保护信息系统的安全。深层防御战略是IATF提出的信息保障的核心思想，IATF的整体框架如图1-5所示。

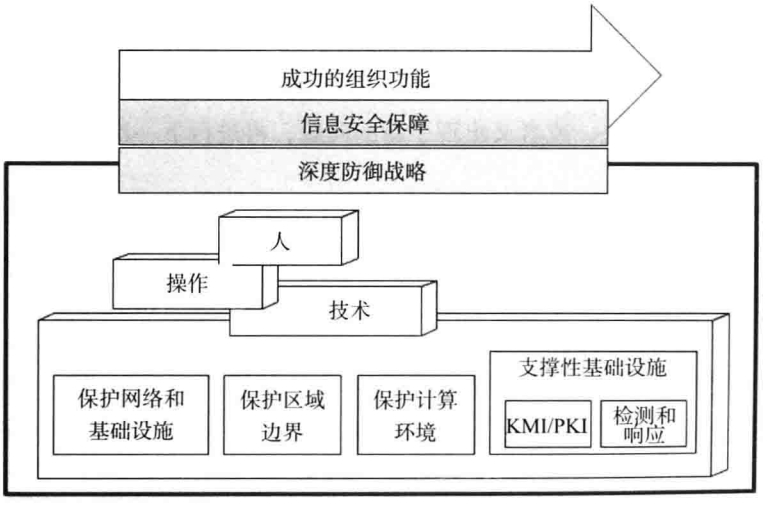

图1-5 IATF整体框架

IATF提出的深度防御战略可以从以下两个方面理解。