注册信息安全专业人员
资质认证培训教材

信息安全理论与技术

中国信息安全产品测评认证中心 编著

- 由信息安全专家精心编写与认真审校
- 全面覆盖了信息安全学科的知识要点
- 信息安全人员资质权威认证专业教材

人民邮电出版社
POSTS & TELECOM PRESS

注册信息安全专业人员
资质认证培训教材

信息安全理论与技术

中国信息安全产品测评认证中心 编著

人民邮电出版社

图书在版编目（CIP）数据

信息安全理论与技术/中国信息安全产品测评认证中心编著.
—北京：人民邮电出版社，2003.9
注册信息安全专业人员资质认证培训教材
ISBN 7-115-11525-7

I. 信… II. 中… III. 信息系统—安全技术—技术培训—教材 IV. TP309

中国版本图书馆 CIP 数据核字（2003）第 069941 号

注册信息安全专业人员资质认证培训教材
信息安全理论与技术

◆ 编　　著　中国信息安全产品测评认证中心
责任编辑　杨　璐

◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街 14 号
邮编　100061　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
读者热线　010-67132692
北京汉魂图文设计有限公司制作
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：28.25
字数：685 千字　　2003 年 9 月第 1 版
印数：1-4 000 册　　2003 年 9 月北京第 1 次印刷

ISBN 7-115-11525-7/TP・3563

定价：39.00 元

本书如有印装质量问题，请与本社联系　电话：(010)67129223

内容提要

本书主要针对“注册信息安全专业人员”认证培训，以注册信息安全专业人员所应具备的知识体系为大纲进行编写。全书以信息安全的主要理论为基础，注重理论、技术知识与实践应用的结合，详尽介绍了安全模型、安全体系结构、信息安全性技术评估、密码技术、访问控制、识别鉴别、审计监控、网络安全、系统安全、应用安全等领域的相关知识。通过对本书的学习，信息安全及相关行业的从业人员可以对信息安全体系框架、主要的信息安全技术、安全模型以及其他相关理论有较为全面的了解。

本书适合作为信息安全专业人员培训班的培训教材，也可供从事相关工作的技术人员和对信息安全感兴趣的读者阅读参考

注册信息安全专业人员资质认证培训教材

编委会

丛书序

随着我国社会信息化进程发展，计算机网络及信息系统在政府机构、企事业单位及社会团体的运作中发挥着越来越重要的作用。信息化水平的提高在带来巨大发展机遇的同时也带来了严峻的挑战。由于信息系统本身的脆弱性和日益呈现出的复杂性，信息安全问题不断暴露。信息安全既关系着个人的隐私，也关系着国计民生，乃至整个国家的安全与利益。信息安全问题已经倍受政府和社会的广泛关注和重视。在这样的大背景下，社会对信息安全专业人员的需求逐年增加。据统计，国内从事信息安全方面的专业人员仅有 3000 余人，社会需求与人才供给间还存在着很大差距；怎样培养信息安全的专门人才，并确保现有信息安全从业人员的职业素质等，将成为信息安全产业发展中需要迫切解决的重要问题。

人员认证概述

中国信息安全产品测评认证中心是经中央批准成立，代表国家开展信息安全测评认证的职能机构，“中华人民共和国国家信息安全认证”是目前国家对信息安全技术、产品、信息系统安全质量以及信息安全服务资质、人员资质的最高认可，由中国信息安全产品测评认证中心及其授权测评机构进行评估，由中国信息安全产品测评认证中心进行认证。本丛书是针对“注册信息安全专业人员认证”部分的培训教材。

“注册信息安全专业人员”（Certified Information Security Professional，简称 CISP）是指机构组织中负责信息系统（网络）建设、运行和应用管理的必备的专业性人才，其基本职能是为信息系统的安全提供技术和管理保障。对信息安全专业人员的认证和注册，是提高信息安全从业人员职业道德和技术水平、提升信息安全产业的竞争能力和强化国家信息安全管理的有效手段。

从书内容特色

本套丛书充分考虑“注册信息安全专业人员”培训学习的需要，以注册信息安全专业人员所应具备的知识体系为大纲，从信息安全的理论基础出发，兼顾理论学习与实践应用，较好地反映了信息安全学科的主要内容和基本特点，较为全面地覆盖了学科的知识要点。

为了使广大信息安全技术人员对信息安全有比较系统和全面的了解，本套丛书共分为以下 3 册：

《信息安全理论与技术》

《信息安全工程与管理》

《信息安全标准与法律法规》

内容涉及安全体系、密码技术、网络安全、系统安全、风险评估、安全策略、安全工程、信息安全管理、应急响应、国内外相关标准及法律等诸多方面，使相关从业人员对信息安全学科有一个较为全面的了解。

适用对象

本丛书适合作为培养信息安全专业人员的培训班教材，也适合从事信息安全工作的技术人员和广大对信息安全感兴趣的读者阅读参考。

关于作者

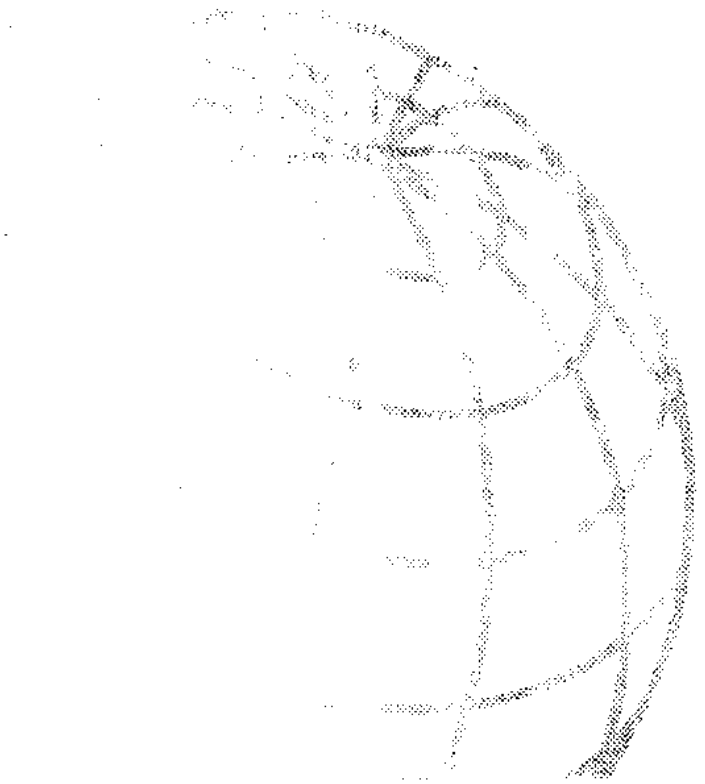
本丛书由中国信息安全产品测评认证中心组织编写，丛书的编写得到了何德全、周仲义、沈昌祥、蔡吉人几位院士的悉心指点，曲成义、方关宝、宁家骏、黄德根等专家更是为本书细心审校，业内相关人士尤其是首批 CISP 也给予了大力支持，在此一并表示感谢！

需要指出的是，由于丛书涉及内容较广，作者水平有限，书中难免会有疏漏之处，敬请专家和广大读者指正。

有关本丛书内容的更新更正以及参考资料信息，可查询：**http://www.cisp.org.cn**。

中国信息安全产品测评认证中心

2003 年 9 月



目 录

第 1 章　国内外信息安全现状与发展

2002 年是全球信息安全界极不平凡的一年。经历了“9.11”恐怖主义事件、美国经济快速下滑、阿富汗反恐战争、著名跨国大公司纷纷裁员、全球股市大幅下挫、大型企业集团会计丑闻不断、跨国投资大幅萎缩、世界油价急剧上扬等一系列冲击，全球 IT 产业在泡沫破灭中一片萧瑟。在如此复杂多变的国际背景下，国际信息安全产业却一枝独秀，逆势上扬。2001 年，美国发生的“9.11”恐怖事件彻底改变了全球对安全问题的思考方式，继美国“亡羊补牢”式的强化安全之后，各国均不同程度地在管理、技术和法规等方面加大了对信息安全的投入，并积极寻求国际合作，有效地推动了全球信息安全产业的发展，网络与信息安全的综合防范与管理对策正在形成之中。

2002 年也是中国信息安全界极为特殊的一年。在“以信息化带动工业化”成为国家发展战略的背景下，电子政务和信息安全保障体系成为十分热门的话题，尤为重要的是，2002 年中国先后发生了针对广播电视传播网络的破坏性事件、针对鑫诺卫星的恶意干扰事件、因技术故障引发的股市停市、首都机场进出港系统宕机事件以及多起网络安全事故。这些信息安全事件改变了中国信息安全问题的性质，使 2002 年真正成为了中国的信息安全年。中国政府高度重视网络等信息安全工作，强化管理，加强协调，统一指挥，沉着应对，成功地控制了信息安全风险，取得了网络与信息安全应急工作的胜利。在突如其来的现实需求面前，中国的信息安全产业却有些措手不及，步履蹒跚。炒得火爆的电子政务并没有如人所愿地拉动市场，而迫在眉睫的网络与信息安全问题却使刚刚起步的信息安全产业捉襟见肘。整个信息安全产业在经历了上半年的燥热之后，很快转入调整时期，在供求失调的严酷现实面前，不得不调整技术方向、市场策略和产品结构，为迎接 2003 年的市场大势作好准备。

1.1　国际信息安全现状

就全球的网络与信息安全发展来看，2002 年的最大特点是“9.11”恐怖事件后的反思和对应，从北美到西欧，从俄罗斯到亚洲，各国的网络与信息安全工作几乎都是围绕着“反恐”展开的，比往年更多了几分“火药味”。

1.1.1　“9.11”之后全球对信息安全的反思

“9.11”恐怖事件的发生，彻底改变了信息安全的传统概念。它将恶意破坏纳入了网络与信息安全的范畴，并由此引发了全球信息安全界的深层反思，从 2001 年 11 月到 2002

年 11 月，欧美各国先后召开了 20 多次大型的信息安全会议，每次会议均有专门议题讨论这种反思。综观今年全球信息网络安全的反思活动，主要有以下几方面的内容。

1. “9.11”恐怖事件对信息安全界的启示尤为重要

“9.11”事件后，各行各业都在反思同一个问题，那就是“9.11”事件对本行业的影响和启示，信息安全界也不例外，2002 年各国的政府、企业界和学术界都在从不同的角度分析这一问题。归纳各方的体会，“9.11”事件对全球信息安全的启示大致有以下几点。

首先，“9.11”事件使各国深刻地意识到：一个强大的国家可以成为个别人的攻击目标，对黑客行为的潜在危害绝不能低估。一直在全球寻找对手国的美国终于发现自己的对手并非多年来一直防范美国的某些国家，而是活跃于阿富汗山区的游击分子，同时更深刻地体会到他们的攻击是如此之快，成本是如此之低，效果是如此之大。信息安全界的人士普遍担心：恐怖分子除了传统意义上的野蛮之外，更多了几分狡猾，他们善于发现和利用发达国家社会结构中的缝隙、弱点和漏洞，这与网络上的黑客行为有异曲同工之处。各国日益依赖的网络基础设施极有可能成为别人的攻击目标，对网上攻击行为的破坏力绝不能低估。可以说“9.11”事件极大地刺激了全球的信息安全忧患意识。

其次，“9.11”事件使各国感到恐怖分子能够直接利用已有的先进技术发动攻击，因而再次重视对两用技术的管理与控制。信息技术作为具有双刃剑意义的两用技术，其发展与安全的微妙关系日益凸现。社会的网络化程度越高，其隐含的安全脆弱性就越大，这种“先进反而脆弱”的现象对安全管理的挑战越来越明显。如何防止先进技术被人为滥用已成为信息安全的重要问题。

第三，“9.11”事件使各国对社会依赖的网络设施的脆弱性深感忧虑。目前，支撑社会稳定和经济发展的大量基础设施都是自动化的、信息化的，都是在没有威胁、平平安安的环境中建设的，从使用方面考虑得多，从防破坏方面考虑得少。“9.11”事件使 4000 多人丧生，十多幢建筑物被毁，无论是在事发之后的紧急救援，还是后来的反恐之战，信息网络都发挥了十分突出和关键的作用。这种社会的神经一旦受到破坏，其后果不堪设想。

第四，“9.11”事件使各国政府深切意识到，在信息安全方面必须多方配合，协同应对。从“9.11”事件中猛醒的美国人在应对挑战面前较为团结，这给信息安全管理部门很大的启迪。2002 年内不仅各发达国家内部在网络与信息安全方面大大加强了各部门之间的协调，而且在国际层面上，不同国家之间也加紧了安全防范上的技术与管理工作。特别是在美国的反恐阵线中，各国在跟踪网上行为，加强网络防护，保护个人隐私和增强网络防范等方面进一步加强了协作，就是相当明显的动向。

最后，“9.11”事件使各国信息安全界认识到“安全是有成本的”。“9.11”事件后，人们对“不对称”的恐怖活动进行了大量投入产出分析，“攻易守难”是这种“新战争”的最显著特点之一。防范的成本相当高昂。曾有美国的专门机构从信息安全方面对世贸中心大厦中的商业公司的信息资源的损失情况组织过调查，结果表明，凡在信息安全上投入多的公司，其蒙受的损失要明显小得多，难怪“9.11”以后，美国经济转向萧条，IT 公司也厄运难免，唯有安全技术公司一枝独秀。这在一定程度上也反映了这种安全的成本观念。

2. 管理与技术的脱节仍是全球信息安全的通病

信息安全不仅仅是一个技术问题，在很大程度上还表现为管理问题，能不能对网络实

现有效的管理与控制是信息安全的根本问题之一。但长久以来，信息安全却一直被人们视为单纯的技术问题，归于信息技术部门独立处理，由此产生了以下几个方面的问题：

首先，信息安全策略难以在管理中实现。无论是政府部门还是公司或机构，大都将其信息安全策略集中于技术细节以及技术问题的解决，并将之纳入信息技术程序文件，属于技术性计划，而不考虑管理或商业风险的实质和机构的文化，由此导致了信息安全策略与管理工作的严重脱节，技术的解决方法无法支持整个管理程序的运转。虽然今年的全球调查结果表明形势有所改观，但这一问题仍然是目前影响信息安全的一个重要阻碍因素。另外，值得注意的是，根据国外的调查资料，目前只有 27%的机构将信息安全策略文件化，只有 14%的机构在设计信息技术项目的过程中建立了专门的文档，对如何处理信息安全问题做出了说明。

其次，信息技术的容灾恢复没有得到应有的重视。Ernst & Young 的“2002 年信息安全调查”显示，2002 年，重要商业系统网络中断现象增多，75%的商业机构经历了操作失效事件，而全球却只有 53%的机构制定了商业操作连续性计划。至今，许多机构仍然将“商业运行连续性计划”这一管理内容单纯地视为 IT“灾难恢复计划”，将保持商业持续性运行归结为信息技术的职责之一，45%的机构仍然将保持商业连续运行的费用列入信息技术的预算额中。事实也证明，在制定了信息技术灾难恢复计划的机构中，有 75%的单位同时取消了商业持续运行计划，而且这些商业持续运行计划只有 40%得到了执行，而 21%的机构则从未对计划的可行性进行过测试和验证。除此之外，有大约一半的机构都未就商业运行恢复的时间表达成一致，这也反映了商业需求与信息技术供应之间存在的差距。

再者，信息安全意识培训和教育力度不够。加强信息安全培训是信息安全策略以及程序得以实施和执行的重要基础。英国贸易工业部《2002 年信息安全问题调查报告》显示，大多数英国企业对信息安全标准 BS7799（即现在的 ISO17799）并不了解，并且只有 5.5%的企业宣称在信息安全实践中遵守了该标准。Ernst & Young 2002 年的调查结果也发现，各个机构在达到要求的计算机安全级别方面面临的最主要的挑战之一是其员工对信息安全的了解和意识不够。2/3 的被调查者认为员工对信息安全策略和程序的了解程度是实现信息安全的障碍之一，而接受调查的企业和机构中则只有不到一半设立了信息安全意识培训项目；2/3 的安全管理人员认为其机构的安全意识培训不到位，甚至是严重缺乏；50%的员工称其从未接受过任何形式的安全意识培训；1/3 的机构不要求其成员了解相关的安全政策和策略，10%的员工称他们从未阅读过公司的安全策略；90%的员工声称曾经打开或执行过带有病毒的电子邮件附件。对金融机构、医疗机构等涉及敏感信息的部门进行的员工信息安全保护意识调查结果也相当令人堪忧。

3. 网络与信息安全隐患与信息化发展同步增长

网络与信息安全问题随着网络基础设施的建设和互联网的迅速普及而激增，并随着信息网络技术的不断更新而愈显严重。

在过去一年多的时间里，全球互联网继续快速发展，互联网用户仍呈上升趋势。据美国 eMarketer 公司最新发表的全球调查报告，2001 年全球互联网用户总数达 4.459 亿（2000 年为 3.522 亿），预计到 2004 年，用户的总数将达到 7.091 亿。目前全球与互联网相联的主机约有 1 亿台，大约 30 亿个网页，2000 万个网址，而这一数字还在以每天 700 万的速度