国家信息化
计算机教育认证
CEAC
指定教材

北京大学
电子政务研究院认证
PCEG
指定教材

信息安全管理基础

■ CEAC国家信息化计算机教育认证项目电子政务与信息安全认证专项组
北京大学电子政务研究院电子政务与信息安全技术实验室　编著

人民邮电出版社
POSTS & TELECOM PRESS

国家信息化
计算机教育认证
CEAC
指定教材

北京大学
电子政务研究院认证
PCEG
指定教材

信息安全管理基础

■ CEAC国家信息化计算机教育认证项目电子政务与信息安全认证专项组
北京大学电子政务研究院电子政务与信息安全技术实验室　编著

人民邮电出版社
北　京

图书在版编目（CIP）数据

信息安全管理基础 / CEAC 国家信息化计算机教育认证项目电子政务与信息安全认证专项组，北京大学电子政务研究院电子政务与信息安全技术实验室编著. —北京：人民邮电出版社，2008.5

国家信息化计算机教育认证 CEAC 指定教材　北京大学电子政务研究院认证 PCEG 指定教材

ISBN 978-7-115-17634-9

Ⅰ. 信…　Ⅱ. ①C…②北…　Ⅲ. 信息系统—安全管理—教材　Ⅳ. TP309

中国版本图书馆 CIP 数据核字（2008）第 019150 号

国家信息化计算机教育认证 CEAC 指定教材

北京大学电子政务研究院认证 PCEG 指定教材

信息安全管理基础

◆ 编　　著　CEAC 国家信息化计算机教育认证项目电子政务与信息安全认证专项组

北京大学电子政务研究院电子政务与信息安全技术实验室

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

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：800×1000　1/16

印张：20

字数：484 千字　　2008 年 5 月第 1 版

印数：1 – 3 000 册　　2008 年 5 月北京第 1 次印刷

ISBN 978-7-115-17634-9/TP

定价：45.00 元

读者服务热线：(010)67132692　印装质量热线：(010)67129223

反盗版热线：(010)67171154

内容提要

为了推进我国信息化人才建设，CEAC 国家信息化培训认证管理办公室组织 IT 和培训领域的资深专家精心编写了国家信息化计算机教育认证系列教材。本书作为国家信息化计算机教育认证项目电子政务与信息安全培训认证专项的教材之一，以国际主流的安全技术为基础，详细介绍了信息安全涉及的安全理论知识与技术。

本书根据企事业单位和信息安全从业人员的实际需求，深入浅出地介绍了信息安全的物理安全、身份鉴别与认证、风险管理、安全管理策略等内容，并详细阐述了用户必须了解的安全法规和标准。

本书结构清晰，讲解详细，并在每章后配有丰富的思考与练习题。非常适合作为信息安全技术的标准培训教程，也可作为大中专院校、高职高专相应课程的教材和辅导教材，还可供读者自学使用。

CEAC 国家信息化计算机教育认证

北京大学电子政务研究院 PCEG 认证

指定教材

编委会

前　言

据国际权威机构调查，中国在信息化的软硬件环境的整体投资比重与某些同类发展中国家相比毫不逊色，但在电子商务与电子政务等实现应用方面却远远落在了后面。要想解决这一矛盾，教育培训是至关重要的一个环节。因为企业信息化、社会信息化的根本是人的信息化。

进入“十一五”后，我国信息网络安全建设与应用领域有了较大的发展，信息化建设的重点已经进入到网络信息应用、网络信息安全应用的高速发展阶段。此时，网络信息应用的安全隐患暴露了出来。究其根本，使用者自身的素质是安全问题的根本原因之一。

可喜的是，近年来大家对信息安全有了较全面、较深入的理解，使用者对网络安全、信息传输安全、信息安全管理也有了迫切的需要。顺应这种趋势，我们开展了 CEAC 国家信息化计算机教育认证项目——电子政务与信息安全培训认证专项（以下简称“CEAC 安全专项”），旨在培养更多的信息安全专业人才。

1. 项目背景

CEAC 安全专项是在信息产业部的领导下，在 CEAC 原有数据库、网络、政务等课程培训认证体系的基础上，结合武警部队网络与信息安全重点实验室、北京大学电子政务研究院等单位多年的研究、教学经验及现有部分培训认证体系，帮助企业和政府培养具有分析能力、设计能力、实现能力和解决问题能力的实用型信息化人才。

2. 项目特点

（1）专业教学体系

项目吸取原有培训资源，培训内容涵盖网络建设、数据库、电子政务、信息安全等工作中涉及的大部分知识。课程由浅入深，分层次、分步骤进行多元立体化教学，按照企事业单位的实际需求，以应用层、技术层、决策层分类设置课程。

(2) 应用与安全结合

CEAC 安全专项体现业务应用与信息安全的结合施教，在办公电子化、业务应用信息化的基础上，重点解决企事业单位信息网络安全的建设与管理问题。

(3) 理论与实训结合

为最大程度地将理论与应用相结合，使学员在学习基本知识的同时能进行同步操作实训，CEAC 安全专项专门开发了“电子政务实训平台”和“信息网络安全实训平台”，使学习结合实际，保障学习效果。

3. 认证体系（双证）

CEAC 按照国际规范，依托 Internet/Intranet 技术，建立了远程计算机考试模式。目前，在信息安全方面设置了 3 个级别的考试：“信息安全应用专家”、“信息安全技术专家”和“信息安全决策专家”。读者只要通过相应课程的考试并合格后，就可获得由信息产业部 CEAC 认证管理办公室和北京大学电子政务研究院联合颁发的培训认证证书。

4. 实训平台

CEAC安全专项开发实训平台的目的是帮助学员加深对相关理论知识的理解，模拟行业安全案例，生动直观地使学员掌握相关产品在实际环境中的技术应用。它包括以下几个部分。

- 防火墙实训平台：掌握市场主流访问控制类产品的应用方法。
- IDS 实训平台：掌握市场主流入侵检测产品的应用方法。
- VPN 实训平台：掌握市场主流 VPN 产品的应用方法。
- 网闸实训平台：掌握市场主流网闸隔离技术。
- 漏洞扫描实训平台：掌握市场主流漏洞扫描产品的应用。
- CA 实训平台：掌握市场主流身份认证与鉴别技术产品的应用方法。

5. 教学支撑

（1）教学资源包

课程方案配套开发“立体化教学支持资源包”，提供相关培训认证课程的现代教育技术支持手段，提供统一的教学资源，并规范课程教学过程，旨在帮助授课老师迅速把握课程的内容实质，提高备课和教学效率，也帮助学员更有效、迅速地掌握有关知识点、技能点，适应认证考试平台提供的技术支持。教学资源包内容如下。

- 教学大纲：课程纲要及授课重点。
- 教学教案：教师制定讲课计划、备课的主要参考手册。
- 教学素材：演示文档、案例。
- 实验手册：结合应用案例、利用实训平台模拟搭建应用环境的实验教学手册。
- 操作手册：实训平台设备操作说明。
- 试题库：模拟试题及考核内容，包括实训上机操作考核试题。
- 考试大纲：考核要点，复习指南。
- 考试系统：统一考试平台。

（2）施教机构：北京大学电子政务研究院

CEAC 安全专项借力北京大学电子政务研究院和武警工程学院多年研究培训经验，结合武警部队网络与信息安全重点实验室的先进技术支撑，以应用为先导，以安全为核心，组织专业授课教师进行培训和教学。

信息安全类教材严格按照国家信息化计算机教育认证项目的规划要求，由 CEAC 信息化培训认证管理办公室组织 IT 和培训领域的资深专家精心编著。教材以企事业单位的信息安全需求为依据，结合国际主流的信息安全技术，在强调培训结果实用有效的同时，还符合客观的培训学习的规律。

在编写信息安全类教材之前，我们经过了大量的培训实践。在培训中我们明显地感到，不同类型的用户对安全技术要求千差

万别，通过短短的几本书是无法满足他们的所有要求的。因此，我们归纳总结、精心挑选了那些最有价值和应用范围最广的技术，提供了大量具有代表性的示例和经验，希望能帮助用户熟练地掌握和使用这些技术，并能通过举一反三来提高学习效果。

严谨、求实、高品质是本系列教材追求的目标，尽管我们力求准确和完善，但由于时间紧迫，水平有限，书中难免会存在一些不足之处，衷心希望广大读者批评指正，并对教材的不足之处提出宝贵意见，我们将努力为您提供更完善的服务与支持。

CEAC 信息化培训认证管理办公室

武警部队网络与信息安全重点实验室

北京大学电子政务研究院

目　录

第1章

信息安全管理概述

本章要点

- ☆ 全球信息安全的发展形势
- ☆ 我国信息安全领域所面临的问题
- ☆ 信息安全的定义
- ☆ 信息安全管理系统的功能和作用

本章导读

本章通过分析全球信息安全发展形势，将举例说明信息安全所面临的一些主要的安全威胁。同时也将分析目前我国信息安全领域所面临的安全形势，指出我国网络安全存在的几大安全现状和威胁。通过对信息安全的举例分析后，本章最后将给出信息安全及信息安全管理的一些基本概念，并将重点给出信息安全管理系统的一些基本知识。

随着信息技术的发展，人们在享受信息技术带来的方便与高效的同时也面临着严重的信息安全的威胁。怎样保证信息被合法有效的利用，是目前信息安全技术所面临的一大课题。构建良好的信息安全管理策略是构建信息安全平台的前提条件。

1.1 全球信息安全发展形势

Internet 是信息传输的集中地，在上面充斥着大量有用和无用的信息。Internet 是一个庞杂的系统，其设计本身不可避免会出现很多不安全的因素。Internet 是一个开放式的网络，任何使用者都可能成为它的安全威胁者。

1.1.1 互联网骨干网络面临的安全威胁

Internet 主要由路由器和 DNS 服务器两大基本架构组成，其中路由器构成 Internet 的主干，DNS 服务器负责将域名解析为 IP 地址。攻击互联网骨干网络最直接的方式就是攻击互联网主干路由器和 DNS 服务器。如果一个攻击者能成功地破坏主干路由器用来共享路由信息的边界网关协议（BGP），或者更改网络中的 DNS 服务器，就会使 Internet 陷入一片混乱。为了寻找一些能够使主干路由器和 DNS 服务器彻底崩溃或者能够取得其系统管理权限的缓冲溢出或其他安全漏洞，恶意的高级攻击者通常会非常仔细地检查一些主干路由器和 DNS 服务器的服务程序代码和它们之间的通信协议的实现代码。路由代码非常复杂，目前已经发现并已修复了许多重要的安全问题，但是仍旧可能存在许多更严重的问题，并且很可能被黑客发现和利用。DNS 软件过去经常发生缓冲溢出这样的问题，在以后也肯定会发生类似的问题。如果攻击者发现了路由、DNS 或通信协议的安全漏洞，并对其进行大举攻击，那么大部分 Internet 将会迅速瘫痪。2002 年 8 月，互联网赖以运行的基础通信规则之一———ASN No.1 信令的安全脆弱性就严重威胁了互联网骨干网基础设施的安全。黑客利用 ASN No.1 信令的安全漏洞开发相应的攻击程序，关闭 ISP 的骨干路由器、交换机和众多的基础网络设备，可最终引起整个互联网瘫痪。ASN No.1 信令的安全脆弱性使得超过 100 家的计算机网络设备提供商将要为此付出代价，而弥补这些缺陷的投入将超过 1 亿美元。由于多个互联网通信协议都是基于 ASN No.1 计算机网络语言的，因此 ASN No.1 的脆弱性将广泛威胁通信行业。最为显著的例子就是造成 SNMP 协议多个安全漏洞。相同的问

题还影响至少其他 3 个互联网协议，在这里不做详细叙述。另外，随着黑客技术的发展，超级网络蠕虫、复杂的 DDoS 攻击（拒绝服务攻击）等无不威胁着整个互联网的安全。

1.1.2　根域名服务器面临安全威胁

全球共有 13 台根域名服务器。这 13 台根域名服务器的名字分别为“A”至“M”，其中有 10 台设置在美国，另外 3 台分别设置于英国、瑞典和日本。在根域名服务器中虽然没有每个域名的具体信息，但储存了负责每个域（如 COM、NET、ORG 等）的解析的域名服务器的地址信息，世界上所有互联网访问者的浏览器将域名转化为 IP 地址的请求（浏览器必须知道数字化的 IP 地址才能访问网站）理论上都要经过根服务器的指引后去该域名的权威域名服务器（authoritative name server，如 haier.com 的权威域名服务器是 dns1.hichina.com）上得到对应的 IP 地址，当然现实中提供接入服务的 ISP 的缓存域名服务器上可能已经有了这个对应关系（域名到 IP 地址）的缓存。根域名服务器是架构 Internet 所必需的基础设施。在国外，许多计算机科学家将根域名服务器称作“真理”（Truth），足见其重要性。

攻击整个 Internet 最有力、最直接，也是最致命的方法恐怕就是攻击根域名服务器了。早在 1997 年 7 月，这些域名服务器之间自动传递了一份新的关于 Internet 地址分配的总清单，然而这份清单实际上是空白的。这一人为失误导致了 Internet 出现最严重的局部服务中断，造成数天之内网页无法访问，电子邮件也无法发送。在 2002 年的 10 月 21 日美国东部时间下午 4:45，这 13 台服务器又遭受到了有史以来最为严重的也是规模最为庞大的一次网络袭击。此次受到的攻击是 DDoS 攻击，超过常规数量 30～40 倍的数据猛烈地向这些服务器袭来，并导致其中的 9 台不能正常运行，7 台丧失了对网络通信的处理能力，另外两台也紧随其后陷于瘫痪。此次事故发生的原因不在于根域名服务器本身，而在于 Internet 上存在很多脆弱的机器，这些脆弱的机器植入 DDoS 客户端程序（如特洛伊木马），然后同时向作为攻击对象的根域名服务器发送信息包，从而干扰根域名服务器的服务甚至直接导致其彻底崩溃。但是这些巨型服务器肯定存在漏洞，即使现在没有被发现，以后也肯定会被发现。而一旦被恶意攻击者发现并被成功利用，就会使整个互联网处于瘫痪之中。