KH北京科海
25年·IT技术出版专家

"All·in·One·is·All·You·Need."

CISSP®
认证考试指南

-(第4版)-

CISSP All-in-One Exam Guide

Fourth Edition

完整覆盖**CISSP**认证考试的
10个专业领域

既是理想的考试学习工具
也可作为IT安全从业人员的技术参考

提供数百道练习题
并给出答案和详尽的解释

光盘内容：

- 数百道练习题及答案
- 作者亲自录制的视频培训教程
- 完整的原版电子书

McGraw Hill Osborne

（美）Shon Harris 编著
石华耀 张辉 段海新 译

科学出版社
北京科海电子出版社
www.khp.com.cn

CISSP认证考试指南（第4版）

CISSP All-in-One Exam Guide, Fourth Edition

（美）Shon Harris 编著

石华耀 张 辉 段海新 译

科学出版社

北京科海电子出版社

Shon Harris: CISSP All-in-One Exam Guide, Fourth Edition
ISBN：978-0-07-149787-9
Copyright© 2008 by McGraw-Hill Companies, Inc.
Original language published by The McGraw-Hill Companies, Inc. All rights reserved. No part of this publication may be reproduced or distributed by any means, or stored in a data base or retrieval system, without the prior written permission of the publisher. Simplified Chinese translation edition jointly published by Science Press and McGraw-Hill Education(Asia)Ca.

本书中文简体版由科学出版社和美国麦格劳-希尔教育（亚洲）出版公司合作出版，未经出版者预先书面许可，不得以任何方式复制或抄袭本书的任何部分。
本书封面贴有 McGraw-Hill 公司防伪标签，无标签者不得销售。

北京市版权局著作权合同登记号　图字：01-2009-0735

图书在版编目（CIP）数据

CISSP 认证考试指南/（美）哈里斯（Harris, S.）编著；石华耀，张辉，段海新译. —4 版. —北京：科学出版社，2009

ISBN　978-7-03-024286-0

Ⅰ. C…　Ⅱ. ①哈…　②石…　③张…　④段…　Ⅲ. 信息系统—安全技术—资格考核—自学参考资料　Ⅳ. TP309

中国版本图书馆 CIP 数据核字（2009）第 041559 号

责任编辑：刘秀青 / 责任校对：叶翠芹
责任印制：科　海 / 封面设计：林　陶

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

北京市艺辉印刷有限公司印刷

科学出版社发行　　各地新华书店经销

*

2009 年 5 月 第 一 版　　开本：16 开
2009 年 5 月第一次印刷　　印张：57.75
印数：0 001~3 000　　字数：1 405 000

定价：145.00 元（含 1CD 价格）
（如有印装质量问题，我社负责调换）

今年，我失去了我心中的英雄，我的祖父 George Fairbairn。他教会我许多书本上学不到，只有通过身边的楷模才能学习领悟的人生哲理：拥有正直、无私的爱、谦卑等美德是何等可贵，以及内在力量与勇气的重要性。

谨以此书献给我的祖父和为我提供极大支持的家人。我真的非常幸运，因为我的许多最好的朋友也正是我的家人，特别是我的母亲 Kathy Conlon 和丈夫 David Harris。

对本书第1版的赞誉

“没有这本书的帮助，我可能永远也拿不到CISSP证书。”

——Owen Creger，CISSP

“我向那些正在准备CISSP考试的人极力推荐这本考试指南，这本指南极大地帮助我全面理解了信息安全的概念、理论和实践。如今，虽然我通过了考试，我仍然不愿扔掉这本书，还把它当作一本工作中的参考指南。”

——Charles T. Danley，CCNA，CISSP，企业支持服务机构高级信息系统安全专家

“Shon 指出了一条学习捷径——你将以非常有效的方式获取所需的知识。我们公司90%的员工拥有CISSP 证书，他们100%都读过这本书。”

——Richard Hanson，RSA安全公司副总裁

“你的书清楚、精练、深入浅出，书中安排的方式使人集中于CISSP考试必备的关键知识点。无论是信息安全领域中的新手，还是资深的专家，在读完这本书之后，都会获取丰富的信息和知识。如果准备参加CISSP考试的人不读这本书，那么他们的信息安全藏书库中将缺少重要的一部分。”

——Daiel Sergile，CISSP，系统安全分析师，Cox Comminication Altanta公司

“Shon Harris的这本书是我准备CISSP考试的基础和关键。它覆盖了CISSP所有的CBK，难度恰如其分，有深度而又不失幽默，这使得本书信息丰富、生动有趣，最重要的是读者容易记住其中的内容。练习题是准备考试的重要内容，需要仔细地分析才能得到正确答案。我向许多同事都推荐过这本书，自己也定期翻阅。”

——David Heydecker，CISSP，BMC软件公司

“在找到这本书之前，准备CISSP考试令人望而生畏。这本书让我有机会在一本书里学到了10个所有安全领域（CBK）的知识，每章之后的提示和练习题使我可以测试自己掌握的程度。这本书的光盘包含的模拟考题可以测试我对全书信息的掌握。我购买并阅读了大量CISSP的书和其他一般性的安全书籍，对准备CISSP考试的安全专业人士来说，Shon写的这本书内容广泛、深入浅出，我极力推荐这本书。”

——Betty Prince，CISSP，资深信息安全分析师，社区安全合作组

此为试读，需要完整PDF请访问：www.ertongbook.com

内 容 简 介

本书完全覆盖 CISSP 考试的 10 个专业领域，囊括通过 CISSP 认证考试所需的全部信息，以及最新的修订内容。借助本书，读者可以全面把握 CISSP 认证的考试重点。

全书共分 12 章，每一章都从明确的学习目标开始，接着详细介绍该领域的考试重点，最后通过考试提示、练习题以及细致的解答进行总结。配书光盘包括 950 多道模拟考题和答案，以及 Shon Harris 讲授的密码学部分的视频培训教程。

本书权威而又不失详尽，是 CISSP 认证应试者的必备教材，对广大的 IT 安全从业人员而言，亦是理想的学习工具和技术参考资料。

作者简介

Shon Harris：MCSE、CISSP、Logical Security 总裁、安全顾问、美国空军信息战部门前工程师、技术总监和作者。她是两本 CISSP 畅销书的作者，并且与人合著了 *Hacker's Challenge:Test Your Incident Response Skills Using 20 Scenarios*，以及 *Gray Hat Hacking:The Ethical Hacker's Handbook*（均由 McGraw-Hill 出版）。Shon 曾为众多客户提供计算机和信息安全服务，包括 RSA、美国国防部、能源部、国家安全局（NSA）、美国银行、国防信息系统局（DISA）、BMC、西点军校等。

Information Security Magazine 认为 Shon 是信息安全领域最杰出的 25 位女性之一。

技术编辑简介

Joe Hoofnagle：CISSP，在信息安全领域拥有 12 年以上的从业经验，主要为私有和商业公司管理和开发安全程序。目前，Joe 是 Magellan Health Services 的信息安全服务主管。在这个职位上，他主要负责制定策略，并在计算机和网络取证分析、入侵检测、管理评估和风险分析等关键领域执行这些策略。作为一名策略家，Joe 创建和维护 Magellan 的安全风险模型和计算机取证程序，以满足联邦、州、立法和商业合约的苛刻要求。Joe 已与其他实现最佳安全实践的组织建立了协作关系。他是美国工业安全学会（ASIS）和高科技犯罪学会（HTCC）的成员。

Clement Dupuis：CD，CISSP，Security+，GCFW，GCIA，CEH，ECSA，CCSA，CCSE，以及 Vigilar 负责安全和渗透测试的资深安全导师。他还是一名国际知名的安全专家，经验丰富的培训专家和安全顾问，曾为微软、加拿大和美国国防部（DoD）、国防信息系统局（DISA）、海军陆战队、美国银行、摩根大通私人银行以及许多世界 100 强公司的员工提供培训。来 Vigilar 工作之前，Clement 受雇于 SANS，是该协会三名主要的课件开发人员之一。如今，作为通信和 IT 专家，他已经为加拿大国防部（DND）的陆军通信兵团服务 20 余年。

译者序

近年来，随着互联网的发展，黑客入侵、拒绝服务攻击、蠕虫病毒泛滥等安全事件越来越严重，同时计算机网络和信息安全也引起了社会各界越来越多的关注。但是长期以来，人们对信息安全的理解还是十分模糊的，特别是在企业中，经常无法明确安全管理的目标和任务。20 世纪 80 年代中期，人们开始认识到，亟需一种资格认证体系以规范信息安全行业，并证明从业人员的能力和资格，提高计算机安全行业及其从业人员的可信度。

信息系统安全专家认证（CISSP）是国际上信息安全领域中最权威的高级安全专业人员认证之一，1988 年由美国信息系统安全协会、加拿大信息处理协会、美国计算机安全研究所、爱达荷州立大学以及其他一些美国和加拿大的政府机构联合发起，后来成立了国际信息系统安全认证联盟$(ISC)^2$，负责为信息系统安全从业人员建立一套安全资格认证体系。这项认证面向信息安全领域的高级专业人员，全面考查待考人员的技术、管理、法律等各个方面的知识和能力。尽管$(ISC)^2$ 成立于北美，但它很快得到了国际上的广泛认可，为企业挑选高级安全管理人员和技术人员提供了有效的依据。

本书对准备参加 CISSP 认证考试的安全专业人员来说是一本不可多得的重要参考书之一。在本书中，身为 CISSP 的 Shon Harris 首先介绍了 CISSP 考试的特点、考试的形式、甚至考试的技巧；然后全面介绍了 CISSP 考试必备的所有 10 个公共知识体系（CBK），从安全管理、密码学、安全模型、安全通信、物理安全、灾难恢复、道德和法律等，几乎无所不包，写作风格深入浅出，非常适合 CISSP 考试“一英里宽，一英寸深”的特点。即使你不准备参加 CISSP 考试，本书也可以作为一本信息安全的教科书，供你全面了解信息安全的各个领域中最重要的知识点。

由于译者水平有限，时间有限，不足之处希望读者和专家批评指正。你的批评和建议是对本书价值的肯定和对我们工作的帮助。

译者简介

张辉，清华大学信息网络工程研究中心讲师，多年从事网络和安全领域的研究、开发和管理工作，在入侵监测、操作系统等方面有多年实践经验，在国内外重要学术会议和刊物上发表论文多篇。

段海新，CISSP，清华大学信息网络工程研究中心副教授，博士，主要从事网络和信息安全的教学、科研和管理工作，中国教育和科研计算机网紧急响应组（CCERT）负责人。

石华耀，自由翻译，多年从事计算机和本地化翻译工作，对计算机安全有较深的研究。译作包括:《WEB 渗透与防范的艺术 》（*The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws*）、《深入网络攻防》（*Crimeware: Understanding New Attacks and Defenses*）等。

推荐序（一）

作为一名计算机安全培训讲师和从业者，人们经常问我两个相同的问题：为更好地完成工作，我该如何学会计算机安全基础知识？我该如何及时了解最新的安全标准与实践？

第一起有记录的计算机“事故”发生于1958年；1966年，明尼苏达州联邦法院裁决，修改银行记录的行为属计算机犯罪。在20世纪60和70年代，人们并没有认真对待计算机安全，因为人们并不像今天这样需要计算机安全。1976年，FBI为它的员工制作了一个为期4周的计算机犯罪调查培训课程。而后在1977年，参议员Ribicoff提出了《联邦计算机系统保护法案》，该法案最终成为《1986年计算机欺诈与滥用法案》。1984年，*2600: The Hacker Quarterly*（其中包含如何攻击电信系统和计算机的指导）开始发行；随后，世界各地纷纷建立起为访问者提供非法软件的计算机安全站点（盗版软件站点）。20世纪80年代末，市场中出现新的安全产品，机构也开始认识到，它们需要一名“安全专家”帮助它们扩张传统的信息技术部门。

我提到FBI的培训课程和2600这份出版物，是因为这两个事件非常重要，人们由此开始收集和编纂一组与安全从业者有关的指导。回顾计算机安全的发展历程，有一件事情最为关键——对信息的控制。

在Morris蠕虫肆虐整个因特网之后大约20年，我们仍在设法修补系统，了解最新的供应商漏洞，并从同行那里获悉通过全球系统传播的潜在攻击。对任何一名IT专家而言，掌握新技术，了解相关商业需求以及保障其安全的有关安全知识，是一个充满挑战的任务。论及技术进步和变迁，人为因素仍然是最大的薄弱环节。

可喜的是，在提供行业最佳实践相关信息以及知识共享方面，我们已经取得了一些进展。国家安全局已授权59所大学成立“卓越中心”，以提供信息保障课程；每年都有更多的计划在开发和授权过程之中。如今，在提供其他IT和商业培训的同时，培训机构也同时提供安全培训。国家已经成立信息共享和分析中心（ISAC），为各个领域的关键基础设施提供保障。现在，国家标准与技术局（NIST）及其他组织正为企业赖以运营的技术制定安全技术标准。

Shon Harris于2001年开始撰写本书，旨在编纂一组最佳实践，同时为应试者通过CISSP考试提供指导。她很好地完成了这两项任务；有越来越多的IT专业人士开始使用这本畅销安全书籍来巩固他们的安全知识。我经常从此书中寻找上述问题的答案，并向学员推荐此书，建议他们将此书作为掌握安全知识的入门书籍。获得CISSP是一个值得追求的目标，但掌握本书讲述的知识也会使你成为一名更加成功的安全从业者。

Jeff Recor Security
卓越安全管理中心
德勤顾问公司

推荐序（二）

过去15～20年以来，信息安全已经从一个主要由政府机构、军队和金融机构提供的晦涩学科，发展为全世界大多数大中型公司所从事的主流活动。

在信息安全的发展过程中，有大量因素起到了推动作用。这些因素包括（部分列表）：

- 因特网的发展。无处不在的连通能力与匿名性共同给信息安全营造了一种复杂且充满挑战与威胁的前景。
- 绝大多数企业信息和知识产权不断被转换成数字格式，然后连接到因特网，这为那些希望获取这类信息的攻击者提供了大量攻击目标。
- 外包业务的迅速增长也要求公司彻底重新考虑外包服务提供商为保护他们的企业数据和知识产权所采取的控制措施。
- 同时，我们看到，各种法律层出不穷，这包括Sarbanes Oxley（SOX）、联邦健康保险法案（HIPPA）、金融现代化法案（GLBA）、加利福尼亚的SB1386、家庭教育权利和隐私法案（FERPA）、通信协助执法法案（CALEA）、OECD隐私指南，以及支付卡行业数据安全标准（PCI）。
- 这些法律，以及许多公司和政府实体（如ChoicePoint、美国银行、乔治亚州车辆管理局、CardSystems、La Salle Bank、ABN AMRO Mortgage Group和农业部）所经历的广为人知和令人尴尬的安全事件，使得人们的安全意识不断提高。

随着安全意识的提高，全世界对技术熟练、经验丰富的信息安全专业人员的需求也不断增加。在我看来，由于企业数据不断转换为电子形式、因特网提供的无所不在的连通能力，以及全球市场的激烈竞争，信息安全将面临日益严重、不断变化的威胁，因而这种需求不会很快萎缩。

准备进入信息安全领域的人经常问我："我如何才能成为信息安全从业者呢？我该从哪里起步呢？"我告诉他们，他们需要两点：对信息安全的全面了解，以及大量的实践经验。我还建议他们阅读并深入理解Shon Harris的CISSP认证考试指南，并获得CISSP证书。这是一个良好的开端，并应结合大量练习以及对本书中列出的信息安全原理和概念的实际应用。

作为Shon的朋友和同事，我感到非常荣幸。对于信息安全，她有着极其深入和全面的了解，这反映在你正在阅读的本书中。本最新版本对之前版本进行了更新和扩展。该书布局合理，浅显易懂，适合任何希望成为信息安全从业者的读者。我极力向大家推荐这本书。

Russell Walker

Warner Bros. Entertainment Inc.信息安全副总裁

致 谢

我要感谢 Sam Tomaino，在很多很多年以前，他给我讲解了计算机的工作原理。我要感谢 Dan Ferguson，因为他从来都没有因为我向他连珠炮式的发问而有什么抱怨，而且还培养了我永无止境的好奇心和求知欲。我要感谢我的父亲 Tom Conlon。这些人中的每一位都以各种方式帮助我编写了本书。

我还要感谢下列人士在我撰写第 4 版新增内容时提供的帮助：

- Burt Kaliski 博士，RSA Security 研究副总裁及该机构研究中心 RSA Laboratories 的首席科学家。感谢你回答了那些别人无法回答的问题！
- Dorothy Denning 博士，海军研究生院防御分析系教授。感谢你随时为我释疑解惑。
- David Miller，你的工作热情、忠诚和友谊一直激励着我；能够与 David 共事，我觉得非常庆幸。没有他，我永远无法尝到龙舌兰酒的美味。
- Allen Harper，他渊博的知识、完美的个性及真实的性格使他成为他周围所有人——包括我自己——的楷模。他是一名海军军官，曾志愿参加了战争（伊拉克巴格达）；我们全都感谢你为我们所做的贡献和牺牲，Allen。
- Clement Dupuis，他待人热情，乐于助人，是一位不可多得的导师和朋友。
- Jay Libove，他有着极其渊博的信息安全知识，真希望有一天我能够像他一样聪明。
- Mike Lester，他是我所认识的最聪明、最有趣的人；在我最需要他的时候，他总能出现在我身边。衷心感谢你，Sparky。我会努力让你了解一年有几个月，以及静电是如何产生的。
- Joe Hoofnagle，你总是在我需要帮助时出现，你是我的良师益友，是唯一通过电子邮件与我玩 Twister 的人。
- Jason Radar，在这本书的最终交稿期限来临之前，你为我提供了极大帮助。期待你成为我们 Logical Security 团队的一员！
- Tom 和 Kathy Conlon，我的父母。没有你们的爱和支持，我今天的生活将全然不同。

最特别的，我想要感谢我的丈夫 David Harris，谢谢他一直以来的支持和爱。没有他对我的坚定信心，我根本无法取得我目前的成就。

此为试读，需要完整PDF请访问：www.ertongbook.com

概 述

随着计算机犯罪的持续增多，计算机、信息和物理安全的重要性在以指数速率增长。过去几年来，由于 Web 站点被黑、拒绝服务攻击增多、信用卡信息被盗、公开可得的黑客工具日益复杂，以及如今病毒和蠕虫所造成的损失更大，人们已经迅速认识到计算机和信息安全的重要性。

许多公司不得不花费数百万美元来消除这些问题的影响，还要另外花费数百万美元购买设备、软件，聘请顾问，开展培训来保护他们的周边和内部网络。但是，在 2001 年 9 月 11 日之后，这类安全保障的必要性和紧迫性有了新的诠释。面对可以通过网络和无线电波实施的各种不同类型的攻击，政府、国家和社会的脆弱性慢慢地暴露出来。社会各界非常依赖各类计算资源和功能，而它们大多由公有和私营部门提供。这表示，即使政府有责任保护其公民，但是公民及为公民所有的公司必须更为安全，这样才能保护整个国家。

实际上，这种保护只有通过正确的教育和理解才能实现，而且必须专门落实这一点才能持续下去。编写本书旨在为许多不同的领域提供一个基础，这些领域组成了有效的安全保障。我们需要了解我们易于遭受的所有威胁和危险，还需要了解减轻这些脆弱性所必须采取的步骤。

目　录

此为试读，需要完整PDF请访问：www.ertongbook.com