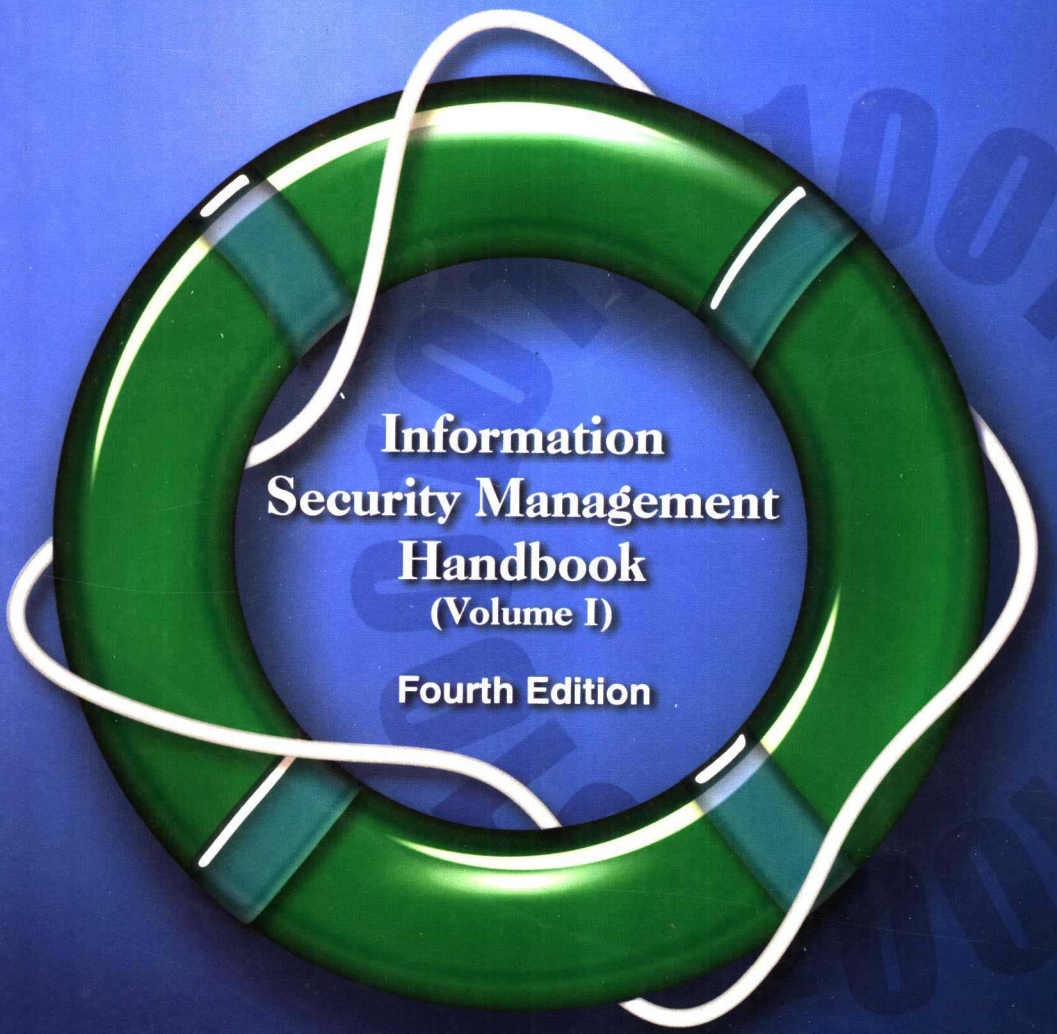

信息安全管理手册（卷I）（第四版）

[美] Harold F.Tipton Micki Krause 主编　　王卫卫 杨 波 等译

AUERBACH
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

电子信息科技专著出版专项资金资助出版

信息安全管理手册（卷I）

（第四版）

Information Security Management Handbook(Volume I)
Fourth Edition

[美] Harold F.Tipton　Micki Krause　主编
王卫卫　杨　波　等译

電子工業出版社
Publishing House of Electronics Industry
北京 • BEIJING

内 容 简 介

本手册共分 10 个部分。第一部分讨论访问控制系统和方法。第二部分叙述电信与网络安全问题。第三部分讨论安全管理的实现问题。第四部分讨论应用与系统开发安全问题。第五部分讨论密码学，主要是加密技术与实现。第六部分讨论安全结构与模型。第七部分讨论计算机操作安全问题。第八部分讨论业务连续性计划和灾难恢复计划。第九部分讨论法律、调查以及道德规范问题。第十部分讨论物理安全问题。

随着信息安全问题变得越来越复杂，拥有 CISSP 证书的人也越来越受到企业的欢迎。本手册的首要目的是作为应考 CISSP 的主要教材，也可以作为信息安全专业人员、研究人员的参考手册。本手册包括了 CISSP 考试要求的大部分内容，读者可以根据自己需要去单独学习每一章。

版权贸易合同登记号　图字：01-2002-5472

图书在版编目(CIP)数据

信息安全管理手册.1 卷：第 4 版/（美）泰普顿（Tipton,H.F.），（美）克劳斯（Krause,M.）主编；王卫卫，杨波译. —北京：电子工业出版社，2004.6

书名原文：Information Security Management Handbook(Volume I) Fourth Edition

ISBN 7-5053-9267-0

Ⅰ.信…　Ⅱ.①泰…②克…③王…　④杨…　Ⅲ.信息系统—安全管理—技术手册　Ⅳ.TN309—62

中国版本图书馆 CIP 数据核字（2003）第 095922 号

责任编辑：王春宁

印　　刷：北京民族印刷厂

出版发行：电子工业出版社　http://www.phei.com.cn

北京市海淀区万寿路 173 信箱　邮编　100036

经　　销：各地新华书店

开　　本：787×1092　1/16　印张：27.5　字数：694 千字

印　　次：2004 年 6 月第 1 次印刷

印　　数：5000 册　　定价：49.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

译 者 序

信息在当今社会中的地位和作用越来越重要，已成为社会发展的重要战略资源，信息技术改变着人们的生活和工作方式，信息产业已成为新的经济增长点，社会的信息化已成为当今世界发展的潮流和核心。与此同时，信息的安全问题也已成为世人关注的社会问题。

CISSP (Certified Information System Security Professional)的证书由 International Information Systems Security Certification Consortium （简称为 $(ISC)^2$）发布，其考试内容包括访问控制系统、密码学以及安全管理。目前拥有 CISSP 证书的人越来越受到企业的欢迎。本手册一方面是作为应考 CISSP 的主要教材，另一方面可以作为信息安全专业人员、研究人员的参考手册。

本手册共分 10 个部分，分别介绍访问控制系统和方法、电信与网络安全、安全管理的实现、应用与系统开发安全、密码学、安全结构与模型、操作安全、业务连续性计划和灾难恢复计划、法律及道德规范、物理安全。

参加本手册翻译的有王卫卫、杨波、王立明、符刚、刘秀英、王保仓、于志强、刘涛、吕锡香、程男男、赵志飞、魏凌波、胡明、王春松，由王卫卫统稿和审校。由于译者水平有限，错误在所难免，恳请读者批评指正。

前　言

本书不仅可以供信息安全专业人员作为参考手册，也可以供准备参加 CISSP 考试的人员作为复习资料。随着信息安全问题变得越来越复杂，企业也越来越需要拥有 CISSP 证书的人。

每年有几百人参加考试，但目前大约只有 2 500 人获得了国际信息系统安全证书联盟（ISC）[2] 颁发的 CISSP 证书。考前准备是至关重要的，因为应考者需要完全了解该领域的常用知识。信息安全管理手册（HISM）系列书已成为应考者的主要参考书。

本书涵盖了 CISSP 考试所需的大部分内容，读者可以根据自己的需要去单独学习每一章。

第一部分讨论访问控制问题和方法。访问控制包括所有机制：物理访问、逻辑访问与管理访问，目的是保证只允许特殊的授权者或授权过程使用或访问系统。

第二部分讨论电信与网络安全问题。包括两大主题：网络安全以及因特网、内部网、外域网安全问题，目的是保证通过电信传输的信息是完整、可靠的，同时电信媒体是可利用的。

第三部分讨论安全管理实践问题，包括安全意识、企业结构和风险管理。制定合理的安全管理策略、程序、底线和原则可以保证企业有合理、持久的安全性；对信息分类有利于保护敏感信息；安全意识培训可以帮助员工理解并遵守执行企业的安全策略和程序；了解企业结构有助于确定适当的信息安全功能；风险管理是有效利用企业资源的管理工具。

第四部分讨论应用与系统开发安全问题，包括系统与应用软件中可以利用和已经使用的各种控制，以及开发设计系统与应用软件的过程。

第五部分讨论密码学。主要包括从最基本的到最新的加密技术与实现，例如，密钥管理、Kerberos 以及 PKI。

第六部分讨论安全系统结构与模型。计算机结构部分主要讨论计算机的组织和配置以保证计算机安全，模型部分主要讨论维护系统与信息安全的一些概念，本部分还包括个人计算机与局域网（LAN）的安全问题。

第七部分讨论操作安全问题。包括围绕着操作者与系统管理权限的数据中心和分布式处理安全问题、计算资源的保护，以及对这些重要资源的威胁将会带来的影响.

第八部分讨论业务连续性计划和灾难恢复计划。本部分的术语非常多，但基本上可以归结为制定具体的协作行动计划以避免或减轻正常的业务信息处理功能遭到破坏时带来的影响。

第九部分讨论法律、调查以及道德规范问题。法律包括信息安全功能面临的法律和约束问题。调查包括成功地调查安全事件并保持证据的真实完整性所需要的原则和原理。道德规范讨论正确与错误行为之间的区别以及自愿做正确的事情。

第十部分讨论物理安全问题。物理安全包括为信息处理活动提供安全的环境，主要讨论如何防止对计算设备的非法的物理与技术访问。

目　录