清华大学计算机安全译丛

PEARSON
Prentice
Hall

安全策略与规程

Security Policies and Procedures

原理与实践
Principles and Practices

Sari Stern Greene 著
陈宗斌 等 译

PEARSON
Education

清华大学出版社

清华大学计算机安全译丛

PEARSON
Prentice
Hall

安全策略与规程

Security Policies and Procedures

原理与实践
Principles and Practices

Sari Stern Greene 著
陈宗斌 等 译

清华大学出版社
北京

EISBN: 0-13-186691-5

北京市版权局著作权合同登记号　图字：01-2007-5709 号

图书在版编目(CIP)数据

安全策略与规程——原理与实践/(美)格林(Greene, S. S.)著；陈宗斌等译. —北京：清华大学出版社，2008.10
书名原文：Security Policies and Procedures: Principles and Practices
ISBN 978-7-302-17962-7

Ⅰ. 安…　Ⅱ. ① 格… ② 陈…　Ⅲ. 信息技术－安全技术　Ⅳ. TP309

中国版本图书馆 CIP 数据核字(2008)第 093138 号

责任编辑：龙啟铭　李玮琪
责任校对：徐俊伟
责任印制：李红英

出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62776969, c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015, zhiliang@tup.tsinghua.edu.cn
印 装 者：北京鑫海金澳胶印有限公司
经　　销：全国新华书店
开　　本：185×230　　**印　张**：26　　**字　数**：629 千字
版　　次：2008 年 10 月第 1 版　　**印　次**：2008 年 10 月第 1 次印刷
印　　数：1～3000
定　　价：49.00 元

安全系列丛书

安全系列丛书是为将要从事信息技术安全职业的学员准备的一套丛书。这套丛书提供了来自业界专家的实践箴言，和对你手把手的培训。该丛书中的每本书，都列举了现实生活中大量的例子。这些例子能帮助你将所学到的知识应用到你的工作中去。以下是本书的几个关键元素，这些元素的目的是帮助学员解决学习过程中的一些问题。

本章目标：这些扼要、可行的目标概括了该章将涵盖哪些内容。

本章导论：每章开始先阐释一下每个主题的重要性，以及这些主题在整本书篇章结构中的地位。

实例：从书中提取出概念，而且展示这些概念是如何用在实际场所中的。

提示：和主题相关、但是超出了本书讨论范围的额外信息。

注意：不可忽视的、关键的信息。这些信息和上下文直接相关。

技能测试：每章末都附有习题，这些习题呼应该章目标，巩固相关的知识点。每章有四种题型：

- **多项选择题**：测验读者对该章内容的理解程度。
- **练习题**：围绕章节中出现的个别概念设计的简要、引导性的课程项目。
- **项目题**：综合一章内若干知识点的较长、引导性的课程项目。
- **案例研究**：运用该章中的知识点来解决问题的实际场景。

本系列丛书包括：

- 计算机安全基础
- 信息安全：原理与实践
- 防火墙与 VPN：原理与实践
- 安全策略与规程：原理与实践
- 网络防御与安全对策：原理与实践

“计算机安全”类图书还有：

书　名	书　号	定　价
密码学与网络安全	978-7-302-11490-1(翻译版)	43.00
	978-7-302-09967-3(影印版)	48.00
网络安全基础：应用与标准(第3版)	978-7-302-15435-8(翻译版)	39.00
	978-7-302-15451-8(影印版)	39.00
经典密码学与现代密码学	978-7-302-10740-8(翻译版)	35.00
	978-7-302-11156-6(影印版)	23.00
网络安全：加密原理、算法与协议	978-7-302-15259-0	39.00

译者序

随着 Internet 的迅速发展，信息安全正成为一个越来越受关注的话题。本书遵循由一般到具体、由理论到实践的原则阐述了当前国内外信息安全领域的相关主题，探讨了信息安全平台建设的理论基础和设计思路，并从实际应用出发探讨如何切实地落实信息安全工作。本书有助于组织构建符合 ISO 17799:2000 信息安全标准的系统，这个标准为开发信息安全策略和理解信息安全控制提供了一个框架。在全书中，我们都会引用 ISO 17799:2000 标准。

本书提供了信息安全思想的总体描述，以便企业管理人员能够更好地评估他们的公司在处理信息安全问题上的表现。同时本书也提供一些实用方法来协助各个公司改进其信息安全计划。

本书是按照为公司建立信息安全计划的步骤来组织内容的。本书分为三个部分。第 1 部分“策略简介”旨在为开发、引荐和实施策略提供基础。第 2 部分“信息安全策略的各个领域”探讨了 9 个安全领域的信息安全策略和规程。第 3 部分“合规性”是关于策略和规程遵从联邦规章以及行业最佳实践的实际应用。本书各章都配有相关的习题，以指导读者深入地进行学习。

本书可作为高等学校计算机及相关专业的教材，也可作为信息安全及管理人员的参考书。对于有志成为信息安全专业人员的人，掌握本书中介绍的信息是绝对必要的。

参加本书翻译的人员有陈宗斌、陈红霞、张景友、易小丽、陈婷、管学岗、王新彦、金惠敏、张海峰、徐晔、戴锋、张德福、张士华、张锁玲、杜明宗、高玉琢、王涛、申川、孙玲、李振国、高德杰、宫飞、侯经国、刘淑妮、张春林、李大成、程明、张路红、张淑芝、孙先国、刘冀得、梁永翔、张广东、郁琪琳、邵长凯、蒲书箴、潘曙光、刘瑞东、李军、焦敬俭。

由于时间紧迫，加之译者水平有限，错误在所难免，恳请广大读者批评指正。

关于作者

Sari Stern Greene(CISSP、MCSE、MCT、MCNE、MCNI、CTT、NSA/IAM)是 Sage Data Security 公司的总裁。在 Sage,Sari 领导一个经验丰富的安全从业人员团队。Sari 致力于提供信息安全服务,比如策略和规程开发、信息安全程序开发、风险和漏洞评估,以及金融、卫生保健和政府领域的灾难恢复/业务连续性计划。Sari 积极参与技术和安全社区。她是 MESDA 理事会中的一员,并且是 Maine ISSA 支部的创始会员。她还经常在安全大会和研讨会上发言,并且撰写了众多信息安全文章、教程和培训材料。你可以通过 sari@sagedatasecurity.com 与 sari 联系。

前言

根据 Per Internet 和 American Lift Project 的观点："在 2004 年末的某一天，大约有 7000 万美国成年人登录到 Internet 使用电子邮件、阅读新闻、访问政府信息、检查健康和医疗信息、参与拍卖、预订旅游行程、研究他们的家谱、赌博、寻找浪漫的合作伙伴，以及参加其他难以计数的活动"(www.pewinternet.org)。

我们生活在一个实在令人惊异的世界中，只要单击一下鼠标，就可以跨越各大洲和各种文化来共享各种思想。从意识形态的分歧到精密的远程外科手术，这种共享信息的能力对我们的世界产生了意义深远的、积极的影响。不过，真正的、正在发生的危险与内部连通性同样令人吃惊。我们的生活、公司和政府赖以存在的每一种信息基础设施的保密性、完整性和可用性都处于危险中。

信息安全在 21 世纪具有了新的含义。与安全从业人员一样，我们有义务设计、采用、影响和实现保护信息和信息系统免遭误用的环境。信息安全不仅仅限于一种活动和一种职业——它是公民的义务。就像组织、机构和政府一样，我们中的每个人都与信息息息相关。尊重这种信任是我们的工作。本书集中介绍如何实现这个目标。

全世界都在研究和讨论信息安全问题。国际标准化组织(International Organization for Standardization，ISO)开发和发布了称为 ISO 17799：2000 的信息安全标准——Code of Practice for Information Security Management(信息安全管理实施细则)。这份实施细则为开发信息安全策略和理解信息安全控制提供了一个框架。在本书中，我们会引用 ISO 17799：2000 标准。必须注意的是：我们把该标准用作一个框架，并且本书并没有构造成 ISO 17799：2000 的官方解释。选择实施该标准的组织应该从 ISO 购买完整的文档(www.iso.ch)。

本书读者对象

信息安全的职责不会落到单个角色身上。对于正在为商业、政府、学术界或卫生保健里的领导职位做准备的任何人，本书就是为他们编写的。在着手研究信息安全之前，学生应该理解商业世界中信息系统的作用、网络基础

设施设计，以及一些基本的安全概念。掌握本书中介绍的信息是将来的信息安全从业人员的必由之路。

本书概述

本书分为三个部分。第 1 部分“策略简介”旨在为开发、引荐和实施策略提供基础。第 2 部分“信息安全策略的各个领域”探讨了 9 个安全领域的信息安全策略和规程。第 3 部分“合规性”是关于策略和规程遵从联邦规章以及行业最佳实践的实际应用。

第 1 部分：策略简介

一项策略的目标是积极地影响行为。一种规程的目标是提供指导。影响行为和提供指导并不是信息安全所独有的。第 1 章“策略定义”首先讨论了有史以来的策略和规程。这种历史方法允许我们理解策略和规程在社会、政府和宗教领域当中所起的作用。在第 2 章“策略的元素”中，我们将把该知识应用于开发、引荐、采用、实施和维护策略。在此过程中，我们将探讨成功的策略和规程的重要元素和组件。

第 2 部分：信息安全策略的各个领域

信息安全的目标是保护信息资产以及处理、存储和传输信息的系统。本书重点关注的是开始策略和支持实现这个目标的活动。不过，在你可以开始编写策略之前，首先必须能够回答以下问题：我们在保护什么？我们在预防谁（和什么）？最大的风险领域是什么以及为什么？信息安全是一个非常广泛的主题。第 3 章“信息安全框架”讨论了这些问题，并介绍了 ISO 17799：2000 Code of Practice for Information Security Management（信息安全管理实施细则）。国际标准化组织发布的 ISO 17799：2000 文档已经成为开发安全策略和控制的广泛采用的框架。

我们将把第 2 部分的讨论建立在 ISO 17799：2000 的 9 个类别之上：

- 第 4 章：安全策略文档和组织的安全策略
- 第 5 章：资产分类
- 第 6 章：人员安全
- 第 7 章：物理和环境安全
- 第 8 章：通信和运营管理
- 第 9 章：访问控制
- 第 10 章：系统开发和维护
- 第 11 章：业务连续性管理

第 3 部分：合规性

信息安全的需求和重要性正快速地与日俱增。美国联邦政府已经认识到了这一点，并采用了各种规章，它们旨在保护个人隐私以及保护国家的关键基础设施。第 3 部分深入探讨了规章的影响以及合规性的要求。第 12 章“金融机构的合规性”和第 13 章“卫生保健领

域的合规性”研究了特定领域的信息安全要求。第 14 章“关键基础设施的合规性”重点关注教育、政府和上市公司的信息安全要求。最后一章即第 15 章“小企业的安全策略和规程”重点介绍开发和成功采用适合于小企业环境的信息安全策略和最佳实践。

补充信息

信息安全是一个动态领域。在本书中，你将发现我引用了许多补充的信息来源。我们鼓励你熟悉这些来源。本书还包含两个有用的附录：附录 A“信息安全从业人员的资源”和附录 B“雇员信息安全策略确认协议”。

本书约定

为了帮助你从本教材中学到最多的知识，我们在书中如下约定。

实际应用：关于实际应用

这些向读者介绍了如何获取本书中的理念并将其应用到工作中去。

参考：关于参考

这些方框提供了关于超出本书范围的主题的额外信息。

警告：关于警告

警告出现在正文的页边空白中。它们指示关键的、不应忘记的信息，这些信息与其周围的正文直接参与相关。

本书中的代码段和代码块都加有方框并带有编号，它们都可以从配套 Web 站点下载（www. prenhall. com/security）。

新的关键术语以粗体字形式表示。

当这个图标出现在页边空白的任意位置时，都可以在本系列书的配套 Web 站点（www. prenhall. com/security）上找到更多的信息。

教师和学生资源

教师资源仅提供给教师，需要这些资料的老师请与 longqm@tup. tsinghua. edu. cn 联系，它包含

- 教师手册。提供了教学提示、每章导言、教学目标、教学建议以及章末习题的答案。
- PowerPoint 幻灯片演示文稿。每章课件，用于教学。
- 题库：用 Prentice Hall 的 TestGen 软件可以使用这个 TestGen 兼容的题库文件。该软件在 www. prenhall. com/testgen 网站上可以免费下载。TestGen 是试题生成

器，可以以适合不同教学情形的各种形式打印。该程序提供许多选项，可以组织和显示题库和测验。它具有内置的随机数字以及文本生成器，通过计算机可以创建试题的多个版本，所提供的测试题可能比题问题更多。强大的搜索和排序功能，使用户能够轻松找到试题，以需要的方式安排它们。

本书配套网站

www. prenhall. com/security 是本书配套网站，这是一个 Pearson 学习工具，可以为学生和教师提供在线支持。其内容主要包括如下几方面。

- 交互式学习指南。这是基于 Web 的交互式测试，学生可以在这里方便地进行在线测试，自行检测是否掌握了本书的相关知识。
- 附加的 Web 工程和资源，练习每章所学的基本概念。

质量保证

我们想把我们的感谢延伸至质量保证团队，感谢他们对细节的注意以及他们对本书出版的付出。

技术编辑

Michael L. Denn
Network Security Technology,
Texas State Technical College

评审人

Carol Buser
Information Technology
Owens Community College

Jeanne Nelson Furfari
Information Systems Technology
New Hampshire Community Technical College,
Pease Emerging Technologies Campus

Hermann Gruenwald 哲学博士
University of Alaska, Anchorage

Charles D. Hamby
Computer Systems Technology
Matanuska—Sustina College

致谢

本书是团队工作的结晶。Sage Data Security 的同事和客户在本书写作过程中起到了重要作用。David Jacquet 和 John Hill Rogers 都做出了重大贡献。

我们的客户邀请我们分享他们的经验，他们是我们的灵感和知识持续不断的源泉。本书中介绍的绝大部分策略都是为我们的客户开发的。我们感谢他们这些年来一直提供他们的反馈意见以及他们的协作。一些早期的 ISO 策略开发工作得到了 ISO Security Solutions 产品的帮助。要查明关于他们的产品的更多信息，可访问 www. isosecuritysolutions. com。

编写一本书是一种独特的经历。我们的开发编辑 Chris Katsaropolous 和 Emilie Herman 给我们提供了专业的、极具耐心的指导，鼓励我们坚持下去。CEP 的 Tom Lewis、Ericka McIntyre 和 Megan Smith－Creed 把我们的原始材料转变成完成的副本。Steve Elliot 帮助我们联系上了 Prentice Hall。我们想对所有这些人说一声谢谢。

写作本书简直就是一项冒险活动。我永远感谢我的儿子 Max 和 Ben 以及我的丈夫 Eric，感谢他们的鼓励和奉献。

目录

第1部分 策略简介