信息安全系列教材

信息安全管理

主　编　王春东
副主编　杨　宏　赵俊阁

WUHAN UNIVERSITY PRESS
武汉大学出版社

信息安全系列教材

信息安全管理

主　编　王春东

副主编　杨　宏　赵俊阁

参　编　唐召东　楚丹琪　童新海　柴金焕

WUHAN UNIVERSITY PRESS

武汉大学出版社

图书在版编目(CIP)数据

信息安全管理/王春东主编;杨宏,赵俊阁副主编. —武汉:武汉大学出版社,2008.4
信息安全系列教材
ISBN 978-7-307-06064-7

Ⅰ.信… Ⅱ.①王… ②杨… ③赵… Ⅲ.信息系统—安全管理—高等学校—教材 Ⅳ.TP309

中国版本图书馆 CIP 数据核字(2007)第 204812 号

责任编辑:黄金文 责任校对:程小宜 版式设计:支 笛

出版发行:武汉大学出版社 (430072 武昌 珞珈山)
(电子邮件:wdp4@whu.edu.cn 网址:www.wdp.com.cn)
印刷:湖北金海印务公司
开本:787×1092 1/16 印张:14.375 字数:370 千字
版次:2008 年 4 月第 1 版 2008 年 4 月第 1 次印刷
ISBN 978-7-307-06064-7/TP·286 定价:26.00 元

信息安全系列教材

编　委　会

何明星，西华大学数学与计算机学院副院长，教授
代春艳，重庆工商大学计算机科学与信息工程学院
陈　龙，重庆邮电大学计算机科学与技术学院，副教授
杨德刚，重庆师范大学数学与计算机科学学院
黄同愿，重庆工学院计算机学院
郑智捷，云南大学软件学院信息安全系主任，教授
谢晓尧，贵州师范大学副校长，教授

华　东

徐炜民，上海大学计算机工程与科学学院，教授
楚丹琪，上海大学教务处，副教授
孙　莉，东华大学计算机科学与技术学院，副教授
李继国，河海大学计算机及信息工程学院，副教授
张福泰，南京师范大学数学与计算机科学学院，教授
王　箭，南京航空航天大学信息科学技术学院，副教授
张书奎，苏州大学计算机科学与技术学院，副教授
殷新春，杨州大学信息工程学院副院长，教授
林柏钢，福州大学数学与计算机科学学院，教授
唐向宏，杭州电子科技大学通信工程学院，教授
侯整风，合肥工业大学计算机学院计算机系主任，教授
贾小珠，青岛大学信息工程学院，教授
郑汉垣，福建龙岩学院数学与计算机科学学院副院长，高级实验师

中　南

钟　珞，武汉理工大学计算机学院院长，教授
赵俊阁，海军工程大学信息安全系，副教授
王江晴，中南民族大学计算机学院院长，教授
宋　军，中国地质大学（武汉）计算机学院
麦永浩，湖北警官学院信息技术系副主任，教授
亢保元，中南大学数学科学与计算技术学院，副教授
李章兵，湖南科技大学计算机学院信息安全系主任，副教授
唐韶华，华南理工大学计算机科学与工程学院，教授
杨　波，华南农业大学信息学院，教授

内 容 简 介

本书以信息安全专业的学生所应具备的知识体系为大纲进行编写的。全书主要介绍了信息安全管理的基本概念、信息安全管理体系、风险管理、安全规划及信息安全管理的实现，并详细列述了对环境、人员、软件、应用系统、操作和文档的安全管理，最后介绍了信息安全管理相关技术及法律、法规等有关内容。通过本书的学习，学生可对信息安全管理的体系、风险管理及信息安全相关技术有所了解，并明确信息安全管理所应包含的内容。

本书适合作为信息安全专业学生的教材，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。

序　言

21 世纪是信息的时代，信息成为一种重要的战略资源，信息的安全保障能力成为一个国家综合国力的重要组成部分。一方面，信息科学和技术正处于空前繁荣的阶段，信息产业成为世界第一大产业。另一方面，危害信息安全的事件不断发生，信息安全的形势是严峻的。

信息安全事关国家安全，事关社会稳定，必须采取措施确保我国的信息安全。

我国政府高度重视信息安全技术与产业的发展，先后在成都、上海和武汉建立了信息安全产业基地。

发展信息安全技术和产业，人才是关键。人才培养，教育是根本。2001 年经教育部批准，武汉大学创建了全国第一个信息安全本科专业。2003 年经国务院学位办批准，武汉大学又建立了信息安全的硕士点、博士点和企业博士后产业基地。自此以后，我国的信息安全专业得到迅速的发展。到目前为止，全国设立信息安全专业的高等院校已达 50 多所。我国的信息安全人才培养进入蓬勃发展阶段。

为了给信息安全专业的大学生提供一套适用的教材，武汉大学出版社组织全国 40 多所高校，联合编写出版了这套《信息安全系列教材》。该套教材涵盖了信息安全的主要专业领域，既有基础课教材，又有专业课教材，既有理论课教材，又有实验课教材。

这套书的特点是内容全面，技术新颖，理论联系实际。教材结构合理，内容翔实，通俗易懂，重点突出，便于讲解和学习。它的出版发行，一定会推动我国信息安全人才培养事业的发展。

诚恳希望读者对本系列教材的缺点和不足提出宝贵的意见。

编委会

2006 年 9 月 19 日

前 言

信息和数据安全的范围包括信息系统中从信息的产生直至信息的应用这一全部过程。我们日常生活中接触的数据比比皆是，考试的分数、银行的存款、人员的年龄、商品的库存量等等，按照某种需要或一定的规则进行收集，经过不同的分类、运算和加工整理，形成对管理决策有指导价值和倾向性说明的信息。随着信息化社会的不断发展，信息的商品属性也慢慢显露出来，信息商品的存储和传输的安全也日益受到广泛的关注。如果非法用户获取系统的访问控制权，从存储介质或设备上得到机密数据或专利软件，或根据某种目的修改了原始数据，那么网络信息的保密性、完整性、可用性、真实性和可控性将遭到破坏。如果信息在通信传输过程中，受到不同程度的非法窃取，或被虚假的信息和计算机病毒以冒充等手段充斥最终的信息系统，使得系统无法正常运行，造成真正信息的丢失和泄露，会给使用者带来经济或者政治上的巨大损失。

信息安全研究所涉及的领域相当广泛。从信息的层次来看，包括信息的来源、去向，内容的真实无误及保证信息的完整性，信息不会被非法泄露、扩散，保证信息的保密性。信息的发送和接收者无法否认自己所做过的操作行为而保证信息的不可否认性。从网络层次来看，网络和信息系统随时可用，运行过程中不出现故障，若遇意外打击能够尽量减少损失并尽早恢复正常，保证信息的可靠性。系统的管理者对网络和信息系统有足够的控制和管理能力，保证信息的可控性。网络协议、操作系统和应用系统能够互相连接，协调运行，保证信息的互操作性。准确跟踪实体运行达到审计和识别的目的，保证信息可计算性。从设备层次来看，包括质量保证、设备备份、物理安全等。从经营管理层次来看，包括人员可靠性、规章制度完整性等。由此可见，信息安全实际上是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

本书的撰写主要是基于当前市场上缺乏针对专业的、平衡的、综合性的信息安全管理和技术的书籍。我们希望编写一本专门面向信息安全专业学生的书籍来填补此空白。主要涉及信息安全的基础原理和基于此原理说明管理策略、技术方案和相关法律法规。

全书共分 11 章，第 1 章介绍了信息安全有关的概念和原则，第 2 章介绍了信息安全管理的体系，第 3 章从风险管理的角度讨论了信息安全管理，第 4 章阐述了信息安全的规划，第 5 章从技术和非技术两个方面整体上讨论了信息安全管理的实现，第 6~9 章则是从不同的方面详细阐述了信息安全的具体实现，第 10 章介绍了信息安全管理采用的技术，第 11 章介绍了相关的法律法规。

本书的编写是集体共同努力的结晶，在编写的过程中得到了武汉大学张焕国教授，天津理工大学的张桦教授、温显斌教授、王怀彬教授，南开大学贾春福教授的悉心指导。无论从大纲的研究，还是内容的确定上他们都给了我们很大的帮助和指导。在此谨向他们表示衷心的感谢。此外，还要感谢天津理工大学计算机科学与技术学院，感谢“天津市智能计算及软件技术重点实验室”以及“天津市软件与理论重点学科”对本书编写的支持和资助。

本书编者包括副主编天津理工大学的杨宏老师、武汉海军工程大学的赵俊阁老师，参编作者包括天津理工大学的唐召东老师、上海大学楚丹琪老师、北京电子科技学院童新海老师、天津外国语学院的柴金焕老师。其中王春东完成第 1、2 章，杨宏完成第 8、10、11 章，赵俊阁完成第 3 章，唐召东完成第 4、6 章，楚丹琪完成第 7 章，童新海完成第 9 章，柴金焕完成第 5 章。

由于作者水平有限，因此对于本书中出现的错误，希望读者提出宝贵的意见，以便我们再版时修改和完善，甚为感谢。

作　者

2007 年 11 月

目 录

第1章 信息安全管理简介

学习目标

- 认识信息技术的重要性并且理解由谁来负责保护机构的信息资产；
- 了解并掌握信息安全的定义和关键特性；
- 了解并掌握信息安全管理的定义和关键特性；
- 认识信息安全管理与普通管理的区别。

1.1 引 言

据美国FBI统计，美国每年因网络安全问题所造成的经济损失高达100多亿美元，还有日益增加的趋势。那么，信息安全问题主要是由哪些方面的原因引起的呢？一是技术因素，网络系统本身存在的安全脆弱性。二是管理因素，组织内部没有建立相应的信息安全管理制度。据有关部门统计，在所有的计算机安全事件中，约有52%是人为因素造成的，25%是由火灾、水灾等自然灾害引起的，技术错误占10%，组织内部人员作案占10%，仅有3%左右是由外部不法人员的攻击造成的。简单归类，属于管理方面的原因比重高达70%以上，这正应了人们常说的“三分技术，七分管理”的箴言。因此，解决网络与信息安全问题，不仅应从技术方面着手，更应加强网络信息安全的管理工作。

考虑如下情况，某工厂的前任网络管理员认为，他不仅具有破坏前任雇主的生产能力，而且还能毁灭所有的犯罪线索。这名受人信赖、有11年工龄的雇员负责公司内部的网络构建和维护，当他不再受到公司的重视并意识到将因表现和行为问题被解雇时，就在系统中设置了摧毁系统的软件定时炸弹。

该网络管理员被解雇3个星期后，工厂的工人和往常一样通过登录到中心文件服务器开始一天的工作，但是机器没有启动，而是在屏幕上出现一行信息，提示操作系统某个地方被锁住了。紧接着，服务器崩溃了。一眨眼的功夫，工厂所有的1 000个加工和生产程序都消失了，服务器再也不能恢复了。工厂经理要求用以前的程序集保持机器继续运转，不管是否下达过这样的命令，但是他必须保证机器运转。于是，工厂经理去取救助工具——备份磁带，磁带放在人力资源部的档案柜里，但是磁带不见了。于是他又去检查连接到文件服务器的工作站，至少大部分程序应该存储在本地的个人工作站上，然而这样的程序也没有找到。

被解雇的网络管理员是惟一负责文件服务器的维护、保护和备份的雇员，他的工作还没有人接手。系统崩溃后的这些天里，公司先后找了3个人试图恢复数据。系统崩溃5天后，工厂经理开始在部门内调换员工，关闭缺乏原料或者生产过剩的机器。他还采取措施，雇佣了一组程序员开始对丢失的1 000个程序中的某些部分进行重建。

公司的财务主管证实软件炸弹摧毁了所有的程序和代码生成器，这些程序和代码生成器