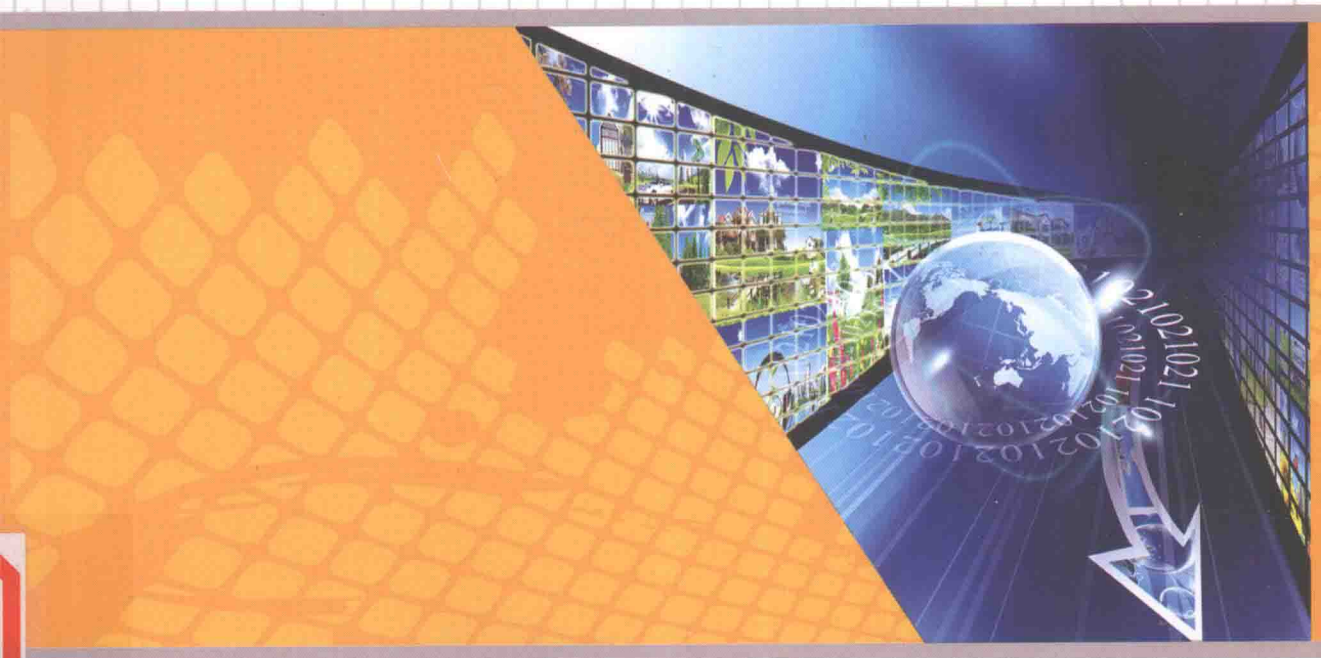
“十三五”普通高等教育本科部委级规划教材

计算机信息安全管理

COMPUTER INFORMATION SECURITY MANAGEMENT

魏红芹◎编著



中国纺织出版社

“十三五”普通高等教育本科部委级规划教材

计算机信息安全管理

COMPUTER INFORMATION SECURITY MANAGEMENT

魏红芹◎编著

中国纺织出版社

内容提要

本书立足于“技术与管理并重”的信息安全理念，从技术基础和综合管理两个方面对信息系统整体安全体系和综合管理方法进行分析和介绍，强调了信息安全的全局观。全书共分十三章，分别介绍了信息安全概论、安全立法、安全标准、软硬件信息安全、密码学、网络安全、安全审计和应急响应等内容，每章均配有引入案例、课后练习和扩展资料。

本书可作为信息管理、电子商务及计算机等专业本科生教材，也可供企业信息系统安全管理人员学习或培训使用。

图书在版编目（CIP）数据

计算机信息安全管理 / 魏红芹编著. -- 北京：中国纺织出版社，2016.9

“十三五”普通高等教育本科部委级规划教材

ISBN 978-7-5180-2759-0

Ⅰ. ①计… Ⅱ. ①魏… Ⅲ. ①电子计算机—安全技术—高等学校—教材 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字（2016）第 152505 号

策划编辑：顾文卓　　责任印制：储志伟

中国纺织出版社出版发行

地址：北京市朝阳区百子湾东里 A407 号楼　邮政编码：100124

销售电话：010—67004422　传真：010—87155801

http：//www.c-textilep.com

E-mail：faxing@c-textilep.com

中国纺织出版社天猫旗舰店

官方微博 http：//weibo.com/2119887771

北京通天印刷有限责任公司印刷　各地新华书店经销

2016 年 9 月第 1 版第 1 次印刷

开本：787×1092　1/16　印张：18.5

字数：315 千字　定价：48.80 元

高等院校“十三五”部委级规划教材经济管理类编委会

前言

计算机安全问题是伴随着计算机信息技术的发展而产生的，随着互联网的日益普及和各种信息技术在各行业得到越来越广泛的应用，整个社会对信息系统的依赖程度日益提高，安全问题也变得越来越复杂和重要。面对各种严重的计算机信息系统安全威胁，关于信息安全的研究日益得到人们的重视。目前，信息安全已经成为信息科学领域重要的研究课题，众多高等院校也相应开设了信息安全专业和系列课程。

本书主要面向信息管理与信息系统专业的学生。信管专业的主要培养目标之一就是为各类企业输送具有全面和系统的信息管理知识、兼顾技术与管理的综合性CIO型人才。而计算机及网络技术逐渐在安全管理方面暴露出的许多不足和缺陷，对信息技术的推广应用形成了严重的阻碍。各企事业和政府机关日渐关注信息安全问题，国家也成立了中央信息化和网络安全小组。这些都使得信息安全成为信管专业学生不可缺少的一个知识模块，国内外的很多高校都在该专业的教学计划中设置了信息安全相关课程。

现有的信息安全相关的教材普遍存在将管理和技术分隔开来的情况，有的侧重于介绍各种底层技术，有的侧重于介绍安全管理标准及制度等，其中技术类书籍种类要远多于安全管理类书籍。在相关专业的教学活动中也普遍存在“重技术轻管理”的现象。对于信息管理学生或在企业安全管理岗位工作的技术人员来说，管理的重要性应该不低于技术因素，甚至会更加重要。因此学生需要了解基本的技术，但也需要掌握基本的管理思想和方法，拥有“技术管理”的基本理念和能力。本书的主要目的是希望能相对全面地对信息安全的相关技术和管理方法进行介绍，使学生能够对信息安全的整体框架体系进行比较准确的把握。

基于以上考虑，本书共组织了十三章内容。第一章为计算机信息安全概论，介绍信息安全问题的起源、特点、发展历史和解决的基本思路，并构建了信息安全的技术框架；第二章从管理角度介绍安全立法和安全标准的基本情况；第三章和第四章分别介绍了软件和硬件安全的通用性问题；第五、六、七章则从三种特殊的软件——操作

系统平台、数据库、病毒出发，分别介绍了相应的安全问题和技术；第八章专门介绍了网络安全中面临的主要威胁和应对策略；第九章从古典密码学和现代密码学两个方面介绍了加密体系的结构和应用情况；第十章立足电子商务这个特殊的应用领域，介绍实际面临的安全问题和常用的安全协议；第十一章和第十二章分别介绍了安全审计和应急响应体系的内容；最后，第十三章分别给出了电子政务网站、电子商务网站和企业信息系统三种应用背景下的安全解决方案的设计方法和案例。其中，第三章到第十章侧重安全技术问题，第一、二、十一、十二和十三章侧重于安全管理。同时，为了便于学生拓展阅读，在附录中给出了国内外信息安全相关结构的信息和部分信息安全相关法律法规。

本书每章开始部分均有引入案例，教师可以借助这些案例使学生更好地理解该章内容的应用背景，也可以通过案例的讨论提高学生的学习兴趣。另外，学生可以借鉴章节关键知识点总结以及课后习题展开重点知识的学习和复习。另外，书中在每章最后还提供了一些拓展课外阅读的链接，主要是一些信息安全相关的网站。

本书中内容已被多次应用在东华大学管理学院信息系统和信息管理专业的《计算机信息安全》课程教学中，并且取得了较好的效果。本书在编写过程中得到了东华大学管理学院张科静等老师的热情支持，也得到了东华大学管理学院信息管理系其他各位老师的大力帮助，在此表示衷心的感谢。

计算机信息安全课程在各大高校的开设时间相对较短，对于课程的教学方法和教学内容，特别是针对信管专业的教学内容还在不断地探索之中。由于本人能力和水平所限，并且时间仓促，书中难免有错误和疏漏的地方，敬请读者批评指正。

魏红芹

第1章　计算机信息安全概论

【本章教学要点】

知识要点	掌握程度	相关知识
计算机安全问题产生	了解	计算机应用模式发展，计算机系统的脆弱性，信息安全问题的根源，信息安全的重要性
计算机信息安全概念	掌握	计算机信息安全基本定义，安全需求要素
计算机安全对策	掌握	实现全面信息安全的主要对策
计算机安全技术体系	了解	计算机信息安全技术体系框架构成

【本章技能要点】

技能要点	掌握程度	应用方向
计算机信息安全需求要素分析	掌握	针对具体应用系统进行安全需求分析
计算机安全基本观点	熟悉	采用正确的安全观点实现信息安全管理

【导入案例】

案例：全球IT安全风险调查报告

2011年6月17日，国际知名调查机构——B2B国际公司发布“全球IT安全风险调查”报告，指出全球约有91%的公司在过去的12个月内发生过至少一起IT安全事故。其中约有三分之一的公司曾丢失企业信息。据了解，此次调查由B2B国际公司与国际知名信息安全厂商卡巴斯基联合发起，全球11个国家，超过1 300名IT专业人员参与其中。

全球IT安全风险调查报告指出，最常见的安全威胁以病毒、间谍软件或其他恶意程序的形式出现。其中，约31%的恶意软件攻击会造成某种形式的数据丢失。而约有10%的公司表示会造成重要商业数据丢失。

在所有参与调查的公司中，仅70%的公司在企业中采取了完善的反恶意软件保护措施。另外还有3%的公司没有采取任何保护措施。不同国家的企业所采取的反恶意软件保护水平也不尽相同。在新兴市场国家，约有65%的公司采取了保护措施。而在英国和美国，采取保护措施的比例则分别高达92%和82%。尽管如此，大部分公司在过去

的12个月内，仍然遭受过至少一起IT安全事故。而且其中约有三分之一的公司曾丢失企业信息。

卡巴斯基市场情报和分析总监Alexander Erofeev在分析当前的企业安全状况时说："几乎超过一半以上的企业和组织都将网络威胁视为其所面临的三大风险之一，在企业中，IT安全策略的重要性甚至被视为高于财务策略、市场和人力资源策略，但这些企业和组织针对此类威胁所采取的态度却令人不解，造成这一现象的原因很可能是IT安全投入不足。"而在本次调查中也确实发现几乎每两家公司中，就有一家认为自己的IT安全预算不足，并且预计应该增加25%甚至更多的预算。

此外，根据相关研究和报告可以得知，目前小型企业的平均IT安全投入为8 055美元，中型企业的平均投入为83 200美元，而大型企业的平均投入则为3 263 476美元。

（查询详细报告，可登陆http://www.kaspersky.com/news?id=207576359）

【问题讨论】

1. IT安全对于企业和组织具有什么意义？
2. 企业如何规划IT安全预算才是恰当的？
3. 实现全面的IT安全需要哪些力量的参与？

计算机技术目前在社会各领域得到越来越广泛的应用，对各行业的发展提供了极大的推动作用，一般个人用户也藉由信息技术获得了许多的便利。然而任何的高新技术都是一把双刃剑，在我们获益于技术发展的同时，安全问题的存在也为信息系统各应用领域带来了极大的潜在威胁，甚至严重阻碍了信息技术的进一步推广普及。了解并应对这些信息安全问题成为人们不得不认真解决的问题之一。

计算机信息安全问题伴随信息技术的发展而产生，同时也需要借助其发展得到解决，因此了解人们使用计算机的方式变化是分析解决安全问题的一个有效途径。任何高新技术都要经历从简单到复杂，使用上却更加方便、可靠而逐渐成熟的过程，计算机信息技术也不例外。经过半个多世纪的发展，目前的信息技术以计算机技术为核心、融合传统的通信技术，已经成为广为人知的计算机网络技术。

1.1 计算机应用模式发展

回顾七十多年来的发展历程，按照技术主要涉及的使用人员、设备工具、信息数

据、方式方法和环境界面的不同，计算机应用模式主要经历了三个阶段：

主机计算（Mainframe Computing）

分布式客户机/服务器（Distributed Client/Server Computing）

网络计算（Network Computing）

1.1.1 主机计算模式

主机计算模式又可称为单机计算，也就是在一台机器或一台主机上带若干台终端及外部、外围设备，由一名或多名操作者操作，主要运算任务在一台机器的CPU上完成，也称主机—终端计算模式。这种模式的最大特点是系统软件、硬件的集中管理，系统最终用户可以分散，但是不需要进行软件、硬件的维护工作。这种模式用户界面单一，系统扩展性差，其处理逻辑如图1.1所示。主机计算模式是目前未联网PC机的主要工作方式。

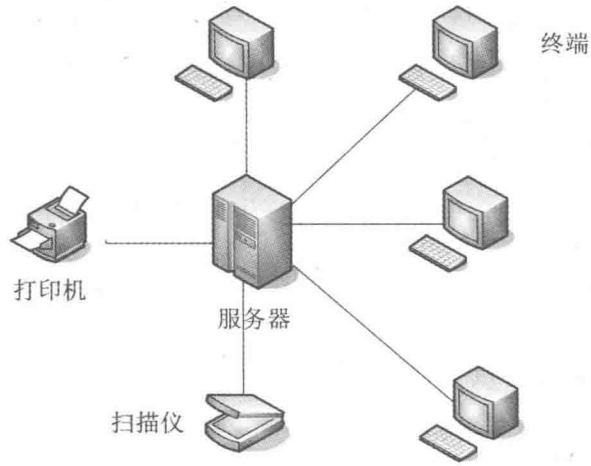


图1.1　主机—终端计算模式

计算机产生的最初十年，各种应用的发展是比较缓慢的，主要由少数专业人员使用机器语言、汇编语言来编写程序；第二个十年计算机的发展开始加快。几十年的发展，主机—终端计算机模式又可分为程序设计时代、结构化程序设计时代和软件工程时代。

1. 程序设计时代（1945 ~ 1955年）

这个时代的硬件处于电子管时代。当时注重的是硬件的性能和指标，程序的编写处于从属地位。程序设计的工具是机器语言、汇编语言，其方法追求编程技巧，追求效率高、内存省。人们仅根据需要来编制一些可以直接运行的程序，而不考虑系统地开发软件。这个时期计算机的应用主要限于科学计算，程序的总数量较少。相对较窄

的应用领域和较少的接触人员使得安全问题主要局限于系统本身的错误和故障等。

2. 软件时代（1955年～1970年）

这个时代硬件已广泛采用晶体管和小规模集成电路，计算机内存容量增大，运算速度加快，运行稳定性高。计算机产量急剧上升，程序需求量猛增。软件概念被提出，开始使用第二代语言，如FORTRAN、ALGOL、COBOL等编译系统。计算机的应用扩大到数据处理及过程控制等领域。各种系统及应用软件规模越来越大，结构也更加复杂。然而程序设计方法和软件开发技术没有重大突破，仍靠个人的“技艺”。使得软件产品开发的复杂需求与软件开发技术的能力之间产生尖锐的矛盾，从而产生所谓的“软件危机”。

3. 软件工程时代（1970年～现在）

20世纪60年代后期，因传统的软件开发方法不能适应大型软件的生产而导致的软件危机，使人们想到用工程化的方法来生产软件，把注意力集中到软件开发的方法、技术和原理上，从此软件生产开始进入软件工程时代。1972年到1975年提出软件生存周期模型，其后又把注意力集中到软件测试方面，提出了若干新的软件测试技术、测试方法、测试原理以及软件确认和验证的理论。1976年至1980年开始提出了若干处理需求定义方面的技术。80年代后，人们开始把软件工程各阶段的工具集成到一起，形成软件开发环境，更有效地支持软件开发的工程化，使软件产品质量和可靠性得到提高。

统计资料表明，计算机应用系统中的软件和硬件投资比例，在1955年是1∶9，1970年是1∶1，到1990年已经达到9∶1。软件危机的出路在于大量生产、高度重用、容易重组、易于维护，为实现这一目标而提出的结构化软件开发法、原型法技术和面向对象的开发模型等软件工程方法使手工劳动变为现代化生产，软件的开发规模和效率大增，也有效地使计算机技术和信息系统推广应用到更多的领域。与此同时，信息安全受到威胁的严重性及其重要性也随之提高。

1.1.2 分布式客户机/服务器计算模式

20世纪70年代兴起的IBM－PC机，由于结构简单技术公开，在个人数据处理、编写简单程序、编辑文档资料、进行游戏娱乐等方面有着广泛的应用，加之价廉物美、维护简单方便而得到了迅猛发展。随着硬件的不断降价、功能的不断提高，将若干处理机联结成计算机网络来完成原来需要大型机才能完成的任务，成为一种更具优势的选择。70年代的TCP/IP协议及相应的局域网LAN、广域网WAN和城域网MAN解决了异种机型、多操作系统、多方式通信的技术问题。分布式客户机/服务器（Client/

Server）计算模式如图1.2所示。

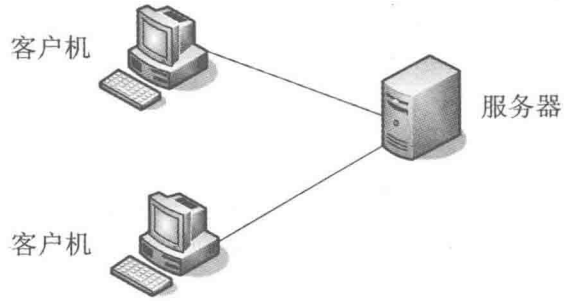


图1.2　分布式客户机/服务器计算模式

在分布式客户机/服务器计算模式中，前端客户部分（微机或工作站）通过应用程序运行服务器上的程序并得到结果，后端服务器部分（微机或大型机）运行客户机请求的应用程序，并将运行结果返回给客户机。客户机一端的客户程序尽量简单扼要，大量复杂的计算处理任务由服务器应用程序承担，并由服务器提供系统数据资源和文件服务，从而减少了数据传送和用户对数据文件的竞争。

按照企业业务模型建立的管理信息系统的框架是由多台资源服务器和多台客户站点构成的系统，客户端比较灵活，联网的计算机均可接入。服务器端则提供各种不同的服务。在这种计算模式中，虽然系统的安全主要集中在服务器环节，但连接的各客户端也会为系统引入各种潜在的危险因素。

1.1.3 互联网络计算应用

以因特网和内联网（Internet/Intranet）为代表的互联网计算模式实现了网络和网络的连接，极大地扩大了计算机的用途。由于若干LAN、WAN连成一片，各种通信、设备之间需要协议协调，广域网需要加装路由器和网关转接。信息按广播方式发出，路由器按指定的地点送达，接收方按协议收下。整个过程空前复杂，但取得了显著的网络效果。20世纪90年代末，世界各国纷纷建立自己的信息基础设施（GII，Global Information Infrastructure）和信息高速公路（ISH，Information Super-highway）。万维网上有各种各样的服务器，如浏览服务器、文件服务器、通信服务器、远程登录服务器、电子邮件服务器、索引服务器等等。用户之间、用户和服务器之间是以页面传递信息的。互联网的工作方式主要是浏览查询和计算处理，具体过程按TCP/IP协议。首先按格式写成主页，在本机上浏览解释执行，然后按主页内容制定的服务器地址URL向Web服务器请求HTTP，把URL换成服务器上的文件路径名，再送到服务器页面。若是HTML页面给用户的，则由Web服务器传回客户机，用户在自己的屏幕上看到结

果。这里，Web服务器充当客户使用互联网的中介。用户取得信息比计算的意义更大，计算机应用的样貌发生了深刻的改变，每个计算机用户都是无限资源网上的平等一员，他们需要的所有数据、资料、工具、软件，都可以在网上找到，并下载到本地机浏览使用、二次开发。互联网络计算模式如图1.3所示。

图1.3　互联网络计算模式

目前，网络化、信息化已经成为现代社会的一个重要特征，互联网络计算也成为目前最有发展前途的模式。网络的快速普及使得协同计算、资源共享、开放、远程管理、电子商务等成为可能。同时，开放的网络结构也使得计算机系统面临前所未有的安全危机。

纵览计算模式的发展历程，可以发现以微电子和半导体技术为基础的硬件，是软件发展的物质基础。软件和硬件两者互相促进、互相补充，相对来说软件更为关键，安全问题更为重要。计算机应用的几种计算模式是递次出现的，互联网式计算在我国方兴未艾，各种新的安全问题使得其既是机遇又是挑战。计算机技术目前正在进一步飞速发展，专业技术人员要掌握更精细的计算机通信、安全、保密技术，才能满足各个应用领域的需要。

1.2 计算机安全问题的产生

科技进步在造福人类的同时也带来了新的危害。从某种意义上讲，计算机信息技术的广泛普及，就像一个打开的潘多拉魔盒，使得新的邪恶与罪孽相伴而来。基于网