21世纪大学计算机基础规划教材

计算机信息安全

印润远 主编

- 系统介绍了计算机信息系统的日常数据维护、保密措施、病毒防治、防黑客入侵、侵害后的处理、数据受损后的恢复等。
- 本书通俗易懂、语言顺畅、概念清楚、内容新颖。
- 在阐述基本理论、基本方法的同时，力求实用和可操作性。

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

21 世纪大学计算机基础规划教材

计算机信息安全

印润远　主编
薛万奉　主审

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书主要内容包括：计算机信息系统安全概述、信息论与数学基础、信息加密技术与应用、数字签名技术与应用、黑客行径概述、鉴别与防御“黑客”入侵、入侵检测、防火墙技术与预防病毒。本书具有很强的实用性和指导性，内容新颖，通俗易懂。在阐述基本理论和、基本方法的同时，力求实用和可操作。

图书在版编目（CIP）数据

计算机信息安全 / 印润远主编. —北京：中国铁道出版社，2006.8
21 世纪大学计算机基础规划教材
ISBN 7-113-07081-7

Ⅰ.计… Ⅱ.印… Ⅲ.电子计算机－安全技术－高等学校－教材 Ⅳ.TP309

中国版本图书馆 CIP 数据核字（2006）第 103059 号

书　　名：计算机信息安全
作　　者：印润远
出版发行：中国铁道出版社（100054，北京市宣武区右安门西街 8 号）
策划编辑：严晓舟　秦绪好
责任编辑：苏　茜　赵　轩　王慧亮
封面设计：薛　为
封面制作：白　雪
印　　刷：河北省遵化市胶印厂
开　　本：787×1092　1/16　印张：14.25　字数：324 千
版　　本：2006 年 8 月第 1 版　　2006 年 8 月第 1 次印刷
印　　数：1～5 000 册
书　　号：ISBN 7-113-07081-7/TP・1827
定　　价：19.00 元

前　言

计算机自 1946 年在美国诞生以来，已经有了 60 多年的历史。目前，计算机和计算机技术的发展日新月异，其应用范围之广，已渗透到了社会的各个领域。上世纪 80 年代中期开始，随着计算机网络技术的成熟，信息的大量积累和广泛传播得以实现的。信息和物质、能源一样，成为人类社会赖以发展的三大重要资源，成为现代社会文明程度的衡量指标。信息技术是指获取、处理、传递、存储和利用信息的方法。计算机技术，使信息的形态数字化；而计算机网络技术，使信息的传输通信化。现代信息技术的重要特征是以数字化为基础、以光电信息存储技术为主要信息存储手段、以计算机技术为处理信息的核心、以网络通信为主的信息传递方法。

信息技术的革命性标志是实现信息快速传输和信息共享。随着我国国民经济信息化进程的推进，我国各行各业对计算机技术和计算机网络的依赖程度越来越高，这种高度依赖将使社会变得十分“脆弱”，一旦计算机网络受到攻击，不能正常工作，甚至全部瘫痪时，就会使整个社会陷入危机。人类对计算机技术和计算机网络的依赖性越大，计算机信息安全知识的普及要求就会越高。计算机类专业特别是应用型的计算机类专业和相近专业的学生学习计算机信息安全的课程，十分重要和必要。

Internet 已成为目前世界上应用最广泛的网络，但其开始构建时，无论在理论上、体系上或应用上都是没有严密地做好准备，特别是在服务、安全和通信等方面存在着诸多的问题。Internet 广泛应用以来，已经涉及到多起国家安全与主权的重大问题。因此，我们在因信息技术为国民生活带来巨大经济利益而欣喜的同时，必须居安思危，充分重视计算机的信息安全。

信息安全包括了设备的安全和数据的安全。设备安全涉及了计算机和网络的物理环境和基础设施。数据安全涉及的面较广，有日常的数据维护、保密措施、病毒防治、防黑客入侵、侵害后的处理、数据受损后的恢复等。其中安全法规、安全技术和安全管理，是计算机信息安全的 3 个部分。安全法规是实施计算机安全管理的准绳和依据；安全技术，也包括了标准，是信息安全的保证；安全管理是灵魂，人的因素是关键，是实现信息安全的有力保障。

《计算机信息安全》一书共分 9 章，包括计算机信息系统安全概述、信息论与数学基础、信息加密技术与应用、数字签名技术与应用、黑客行径概述、鉴别与防御“黑客”入侵、入侵检测、防火墙技术和预防病毒。

印润远教授毕业于上海交通大学，现任教于上海水产大学信息学院，是计算机科学和技术系的主任，从事网络方向的研究。印润远教授曾是组建上海水产大学校园网的技术和行政负责人，其编写的《计算机信息安全》一书，是多年来从事理论教学和科研实践的总结和结晶，具有很强的实用性和指导性。本书通俗易懂、语言顺畅、概念清楚、内容新颖；在阐述基本理论、基本方法的同时，力求实用和可操作性。本书作为应用型计算机专业和相近专业的教材很合适，既可以作为本科、高职高专和成人高校的教材，也可以作为计算机网络管理员、计算机信息安全管理员和计算机维护人员，甚至是计算机编程人员的参考书。

欢迎使用本书授课的老师们将教学情况反馈至信箱：rryin@shfu.edu.cn。也敬请各位读者指正书中的不足及疏漏，共同讨论计算机信息安全的相关技术及发展。

感谢中国铁道出版社的同仁们，对本书的出版和发行给予的支持，也感谢上海水产大学给予的支持。交通银行上海培训中心的韩炳兴高级工程师、上海市发展和改革委员会培训中心的童建初等，对于本书的相关章节提出了具有积极意义的建议，在此也表示感谢。

全国高等学校计算机教育研究会理事
华东高校计算机基础教学研究会理事　薛万奉
上海市计算机基础教育协会理事

2006年7月

目　录

第 1 章　计算机信息系统安全概述

自 20 世纪 40 年代计算机在美国诞生以来，计算机应用已逐渐在社会的各个领域中普及。20 世纪 80 年代中后期，随着计算机网络技术的成熟，计算机网络应用迅速普及，从而宣告了第三次工业革命浪潮的到来。第三次工业革命就是以通过计算机与通信系统实现信息快速传输和共享为标志的信息技术革命。伴随着我国国民经济信息化进程的推进和信息技术的普及，我国各行各业对计算机网络的依赖程度越来越高，这种高度依赖性将使社会变得十分“脆弱”，一旦计算机网络受到攻击，不能正常工作，甚至全部瘫痪时，就会使整个社会陷入危机。尤其是 Internet 广泛应用以来，已经涉及到多起国家安全与主权的重大问题。在为信息技术带来巨大经济利益而欣喜的同时，必须居安思危。

安全法规、安全技术和安全管理，是计算机信息系统安全保护的三大组成部分，它们相辅相成、相通互补。制订法规的根本目的或作用，在于引导、规范及制约社会成员的行为。安全法规以其公正性、权威性、规范性、强制性成为实施社会计算机安全管理的准绳和依据；有效的计算机安全技术是维护计算机信息系统的有力保障。安全保护的直接目标，是保障计算机信息系统的安全。

根据国内外大量的调查统计表明，人为或自然灾害所造成的计算机信息系统的损失中，管理不善所占的比例高达 70%以上。安全法规的贯彻、技术措施的实施都离不开强有力的管理。增强管理意识，强化管理措施，是做好计算机信息系统安全保护工作的有力保障，安全管理的关键因素是人。

同时，计算机信息系统安全又是动态的。攻击与反攻击、威胁与反威胁是一对永恒的矛盾，安全是相对的，没有一劳永逸的安全防范措施，计算机信息系统安全管理工作必须常抓不懈、警钟长鸣。

信息是人类社会的宝贵资源。功能强大的信息系统，是推动社会发展前进的加速剂和倍增器，它日益成为社会各部门不可缺少的生产和管理手段。信息与信息系统的安全，已经成为崭新的学术技术领域；信息与信息系统的安全管理，也已经成为社会公共安全工作的重要组成部分。

1.1　计算机信息系统及其安全的基本概念

为了深刻理解以后计算机信息系统及其安全保护的有关内容，本节首先介绍有关计算机信息系统及其安全的基本概念。

1.1.1　计算机信息系统

所谓计算机信息系统是指“由计算机及其相关的和配套设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统”。

信息是客观事物运动状态及运行方式的表征，能使我们由未知变为已知。信息按其内容的价值，大体上可分为三类：消息、资料和知识。消息可理解为单条信息的记录，例如报纸

上的消息报道；资料可理解为相关信息记录的集合，具有相对较大的参考价值，例如报刊文摘、统计报表；而知识则是在大量资料的基础上，经过分析研究所总结出来的客观规律或法则，这显然是人类文明进步的结晶，来之不易，例如论文、论著等。1996 年联合国教科文组织的“信息化与教育”把信息化社会的知识结构表述为图 1-1 所示的知识结构金字塔。

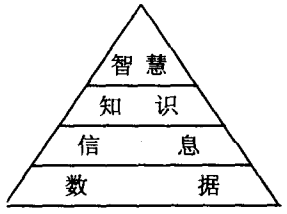

图 1-1 知识结构

在这知识结构的金字塔中，数据（Data）是信息的原材料，是一堆数字或符号的总括；信息（Information）是以某种目的组织起来，经加工处理并具有一定结构的数据的总括；知识（Knowledge）是经过整理、分析、评论和验证的信息；智慧（Intelligence）是经历客观现实验证而得到的充实的知识，是金字塔的顶端。

计算机系统的出现，是人类历史上相当重要的一次信息革命。它从 1946 年诞生至今，经历了科学计算、过程控制、数据加工、信息处理、人工智能等应用发展过程，功能逐步完善，现已进入普及应用的阶段。

计算机信息系统是一个人机系统，其基本组成是：计算机系统实体、信息和人。

所谓计算机系统实体，是指计算机系统的硬件部分，应包括计算机本身的硬件和各种接口，也应包括各种外部设备，还应包括形成计算机网络时应有的通信设备和线路、信道。

在计算机信息系统中，信息形成包括操作系统、数据库、网络功能及各种功能的应用程序。计算机系统实体，是在形成了计算机信息系统之后才有用的。计算机系统实体本身是有价的；而信息系统则是无价的，它的损害，往往是无法弥补、难以挽回的。

计算机信息系统的发展是要经过一个过程的。20 世纪 70 年代以来，大体上是计算机网络的开发、应用和发展阶段。网络技术应用，使得在空间、时间上原先分散、独立的信息，形成为相关密切的庞大的统计信息资源系统，网络资源共享，无可估量地提高了信息系统中信息的有效使用价值。

20 世纪 90 年代以来，多媒体技术蓬勃发展，这大大拓宽了计算机系统所处理的信息的范畴，使计算机信息系统在各行各业及日常生活领域的广泛应用，展现了令人鼓舞的前景。

1.1.2 计算机信息系统安全

计算机信息系统安全包括实体安全、信息安全及运行安全等几个部分。下面就这几个方面的内容作简单的说明。

1. 计算机信息系统实体安全

在计算机信息系统中，计算机及其相关的设备、设施（含网络）统称为计算机信息系统的实体，实体安全是指保护计算机设备、设施（含网络）以及其他媒体免遭地震、水灾、火灾、有害气体和其他环境事故（如电磁污染等）破坏的措施及过程。实体安全包括环境安全、

设备安全和媒体安全 3 个方面。

对计算机信息系统实体的威胁和攻击，不仅会造成国家财产的重大损失，而且会使信息系统的机密信息严重泄露和破坏。因此，对计算机信息系统实体的保护是防止对信息进行威胁和攻击的首要一步，也是防止对信息进行威胁和攻击的天然屏障。

2．计算机信息系统运行安全

计算机信息系统的运行安全包括系统风险管理、审计跟踪、备份与恢复、应急 4 个方面。系统的运行安全是计算机信息系统安全的重要环节，是为保障系统功能的安全实现，并提供一套安全措施来保护信息处理过程的安全，其目标是保证系统能连续、正常地运行。

3．计算机信息系统信息安全

所谓计算机信息系统的信息安全是指防止信息财产被故意的或偶然的非法授权泄漏、更改、破坏或使信息被非法系统辨识、控制。即确保信息的保密性、完整性、可用性和可控性。针对计算机信息系统中信息存在形式和运行特点，信息安全包括操作系统安全、数据库安全、网络安全、病毒防护、访问控制、加密与鉴别 7 个方面。

下面指出了对信息构成威胁的一些行为：

（1）对可用性的威胁

- 破坏、损耗或者污染
- 否认、拒绝或延迟使用或者访问

（2）对完整性的威胁

- 输入、使用或生成错误数据
- 修改、替换或重排序
- 歪曲（misrepresent）
- 否认（当成不真实的而拒绝）
- 误用或没有按要求使用

（3）对保密性的威胁

- 访问
- 泄露
- 监视或监听
- 拷贝
- 偷盗

为了更好的领会信息安全要素，下面列举了几个信息安全性遭到破坏的案例。

（1）可用性遭到破坏。用户的一个数据文件被别有用心的人移到了另一个文件中。该计算机用户在运行其应用程序时，由于在程序指定的子目录里数据文件已不存在，系统肯定要出错。

在这个事件中，信息的可用性被破坏，而信息的其他安全性要素（完整性、保密性）都没有遭到破坏。

（2）完整性遭到破坏。一个软件公司为了按期交货，将一个没有包含重要记账控制机制的应用程序提供给了一家客户，而该软件技术说明书里有这个控制机制。客户将该软件用